paloalto TECHDOCS

PAN-OS® 管理者ガイド

Version 10.2

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

June 6, 2022

Table of Contents

スタート ガイド

以下のトピックでは、新しい Palo Alto Networks の次世代のファイアウォールをデプロイする上で必要な手順について説明します。これらは、新しいファイアウォールをネットワーク統合する方法、および基本的なセキュリティポリシーをセットアップする方法の詳細を説明します。セキュリティ プラットフォーム機能を継続的にデプロイしてネットワーク セキュリティのニーズを満たすためのガイドについては、ファイアウォールのデプロイメントのベスト プラクティスを参照してください。

- 管理ネットワークへのファイアウォールの統合
- ファイアウォールの登録
- インターフェイスやゾーンを用いたネットワークのセグメント化
- 基本的なセキュリティ ポリシーのセットアップ
- ネットワーク トラフィックの評価
- 無料の WildFire 転送の有効化
- ファイアウォールのデプロイメントのベスト プラクティス

管理ネットワークへのファイアウォールの統合

すべての Palo Alto Networks ファイアウォールにはアウトオブバンド管理ポート（MGT）が用意されており、それを使用してファイアウォールの管理が可能です。MGT ポートを使用することによってファイアウォールの管理機能とデータ処理機能を分離するため、ファイアウォールへのアクセスが安全に守られ、パフォーマンスが向上します。Web インターフェイスを使用するときには、ファイアウォールを管理するためにインバンド データポートを使用する予定の場合であっても、MGT からすべての初期設定タスクを実行する必要があります。

ライセンスの取得や、ファイアウォールでの脅威シグネチャとアプリケーション シグネチャの更新などの一部の管理タスクでは、インターネットへのアクセスが必要です。MGT ポートへの外部アクセスを有効にしない場合は、必要な外部サービスにアクセスできるように（サービスルートを使用して）インバンド データポートをセットアップするか、定期的に手動で更新をアップロードするように計画する必要があります。

インターネットからまたは企業のセキュリティ境界内の他の信頼されていないゾーンから、管理インターフェイスへのアクセスを有効にしないこと。これは、専用管理ポート（*MGT*）を使用する場合でも、管理インターフェイスとしてデータ ポートを設定した場合でも適用されます。*firewall* を管理ネットワークに統合するときは、Adminstrative Access Best Practices に従って、*firewall* およびその他のセキュリティ デバイスへの管理アクセスを、攻撃の成功を防ぐ方法でセキュリティで保護していることを確認してください。

以下のトピックでは、新しいファイアウォールを管理ネットワークに統合し、基本的なセキュリティ設定をデプロイするために必要な初期設定手順の実行方法を説明します。

- 事業継続のためのアクセス戦略を決定する
- 管理ポリシーの決定
- 初期設定の実行
- 外部サービスへのネットワーク アクセスのセットアップ

以下のトピックでは、単一の *Palo Alto Networks* の次世代ファイアウォールをネットワークに統合する方法を説明します。ただし、冗長性を持たせるため、高可用性設定にファイアウォールのペアをデプロイすることを検討してください。

事業継続のためのアクセス戦略を決定する

事業継続計画には、停電などで通常の通信経路では接続できない場合に、ファイアウォールやPanoramaなどの重要なデバイスに接続する方法について規定する必要があります。帯域外（OOB）ネットワークに接続し、機器を管理できるため、主要なネットワークや電源がダウンした場合でも、ビジネスを継続することができます。事業継続性は、ネットワーク・アーキテクチャの中核的な検討事項であるべきです。

*OOB*ネットワークは、機器へのリモートアクセスや管理を安全に行うための方法で、主要な通信チャネルを使用しません。代わりに、*OOB* ネットワークは、プライマリ チャネルに障害が発生し、プライマリ ネットワークとは異なる電源がある場合に常に使用可能な個別の通信チャネルを使用します。ネットワーク アーキテクチャによっては、プライマリ ネットワークと *OOB* ネットワークの両方を使用して、日常業務でデバイスにアクセスして管理できます。

OOBネットワークは、プライマリアクセスネットワークと同時に故障する可能性のある電源やネットワークに依存しないようにする必要があります。デバイスへのOOBアクセスをどのように構築するかは、ネットワーク・アーキテクチャやビジネス上の考慮事項によって異なるため、接続性を確保するための「一律」の方法は存在しません。ただし、OOB アクセス ネットワークの目標を達成する方法を理解するのに役立つガイドラインがあります。

- **Power considerations** - OOB ネットワークには、通常のアクセス ネットワークで使用する電源とは異なる電源 (別の回路または保護またはバッテリ駆動のソース) を使用します。通常のネットワークへの電力が切れても、OOB ネットワークへの電力は失われません。

  電力配分装置 (PDU) コントロールを使用して、装置にリモートで電源をオン/オフします。

- **Secure connection method**—OOBネットワークに安全に接続するには、ターミナル・サーバー・デバイス、モデム、シリアル・コンソール・サーバーなど、さまざまな方法があります。OOB アクセスに使用できるセキュリティで保護されたネットワークの例としては、LTE、ダイヤルアップ、ブロードバンド (通常のブロードバンド ネットワークから完全に分離された) ネットワークなどがあります。使用する接続方法は、ビジネス ニーズとネットワーク アーキテクチャによって異なります。

  選択する方法に関係なく、接続は強力な暗号化と認証で安全である必要があります。firewall および Panorama への管理接続を保護する方法についてのアドバイスについては、Administrative Access Best Practices を参照してください。

  イーサネットLAN経由で強力な認証でSSHを使用してOOBネットワークにリモートで接続することも、シリアル接続を介してダイヤルインすることもできます。アウトバウンド接続はシリアルになります。

管理ポリシーの決定

Palo Alto Networks のファイアウォールは、ローカルで設定および管理するか、Palo Alto Networks の集中管理システムである Panorama を使用することによって一元管理することができます。ネットワークにファイアウォールが 6 台以上デプロイされている場合、Panorama を使用すると以下のメリットがあります。

- 設定、ポリシー、ソフトウェア、および動的コンテンツ更新の管理で、煩雑さや管理上の負荷を軽減できます。Panorama でデバイス グループとテンプレートを使用することにより、ファイアウォール固有の設定を各ファイアウォールでローカルに管理したり、すべてのファイアウォールまたはデバイス グループで共有ポリシーを適用したりすることで効果的に管理できます。
- すべての管理対象ファイアウォールからデータを集約し、ネットワーク上のすべてのトラフィックを可視化します。Panorama のアプリケーション コマンド センター（ACC）にはファイアウォール全体の統一レポートの一括管理画面が表示され、ネットワーク トラフィッ

ク、セキュリティ インシデント、および管理上の変更について一元的に分析と調査を行い、レポートを作成することができます。

以下の手順は、Web インターフェイスを使用してファイアウォールを管理する場合の方法を示しています。集中管理で Panorama を使用する場合は、最初に初期設定の実行を行い、ファイアウォールから Panorama への接続を確立できることを確認してください。それ以降は、Panorama を使用して一元的にファイアウォールを設定できます。

初期設定の実行

デフォルトでは、PA シリーズ ファイアウォールの IP アドレスは 192.168.1.1 で、管理者/管理者のユーザ名とパスワードが設定されています。セキュリティ上の理由により、他のファイアウォールの設定タスクを行う前に、これらの設定値を変更する必要があります。初期設定タスクは、ファイアウォールの管理で MGT インターフェイスを使用しない場合でもこのインターフェイスから実行するか、ファイアウォールのコンソール ポートへ直接シリアル接続を使用して実行する必要があります。

STEP 1 | ファイアウォールをインストールして電源を接続します。

デュアル電源のファイアウォール モデルである場合、*2* つ目の電源を接続して冗長性を確保します。お使いのモデルの詳細については、ハードウェア リファレンス ガイドを参照してください。

STEP 2 | ネットワーク管理者から必要な情報を入手します。

- MGT ポートの IP アドレス
- ネットマスク
- デフォルト ゲートウェイ
- DNS サーバー アドレス

STEP 3 | コンピュータをファイアウォールに接続します。

以下のいずれかの方法でファイアウォールに接続できます。

- コンピュータからコンソール ポートにシリアル ケーブルを接続し、ターミナル エミュレーション ソフトウェア (9600-8-N-1) を使用してファイアウォールに接続します。起動シーケンスが完了するまで 2、3 分待ちます。ファイアウォールの準備ができると、プロンプトがファイアウォールの名前に変わり、たとえば「**PA-220 login**」のように表示されます。
- コンピュータとファイアウォールの MGT ポートを RJ-45 Ethernet ケーブルで接続します。ブラウザで、**https://192.168.1.1** にアクセスします。

この *URL* にアクセスするには、コンピュータの *IP* アドレスを、*192.168.1.0/24* ネットワークでのアドレス *(192.168.1.2* など*)* に変更しなければならない場合があります。

STEP 4 | プロンプトが表示されたら、ファイアウォールにログインします。

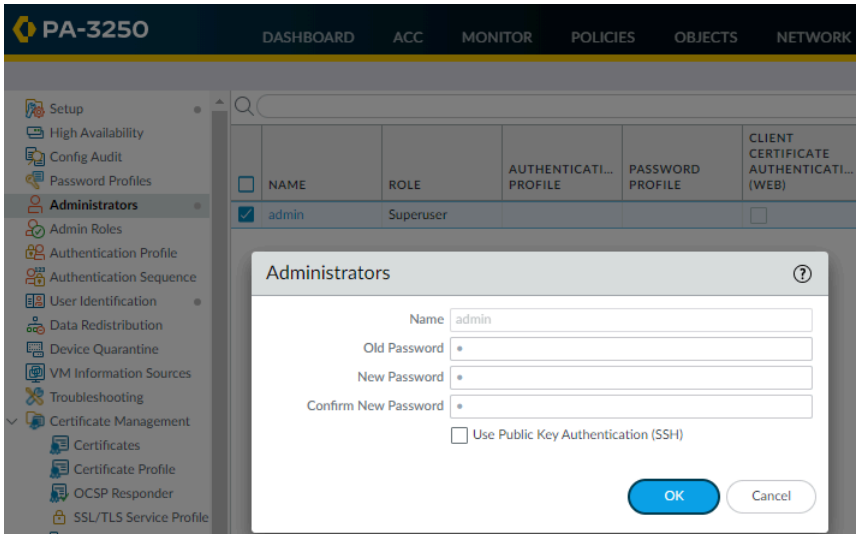
ログインには、デフォルトのユーザー名とパスワード（admin/admin）を使用する必要があります。ファイアウォールの初期化が開始されます。

STEP 5 | admin アカウントの安全なパスワードを設定します。

PAN-OS 9.0.4 で開始すると、事前定義済みのデフォルトの管理者パスワード *(admin/admin)* はデバイス初回ログイン時に変更されるようになっています。新しいパスワードは *8* 文字以上で、*1* 文字以上の小文字と *1* 文字以上の大文字、および数字または特殊文字 *1* 字を含める必要があります。

パスワードの強度を高めるために、必ずパスワード強度のベスト プラクティスに従い、パスワードの複雑さの設定を確認してください。

1. **Device**（デバイス） > **Administrators**（管理者）を選択します
2. **admin** ロールを選択します。
3. 現在のデフォルト パスワードと新しいパスワードを入力します。



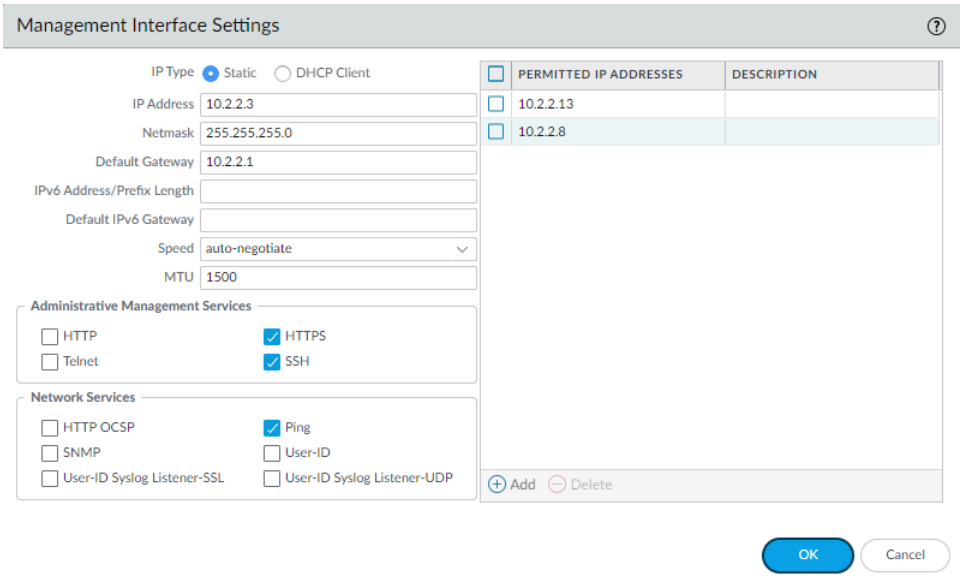
4. **OK** をクリックして、設定を保存します。

STEP 6 | MGT インターフェイスを設定します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Interfaces (インターフェイス)** を選択し、**Management (管理)** インターフェイスを編集します。
2. 次の方法でMGTインターフェイスのアドレス設定を行います。
   - MGTインターフェイス用に静的IPアドレスを設定するには、**IP Type** [IPタイプ]を**Static**[静的]に設定し、**IP Address**[IPアドレス]、**Netmask**[ネットマスク]、**Default Gateway**[デフォルトゲートウェイ]を入力します。
   - MGTインターフェイスのアドレス設定を動的に構成するには、**IP Type (IP タイプ)** を**DHCP Client (DHCP クライアント)**に設定します。この方法を使用するためには、DHCP クライアントとして管理インターフェイスを設定する必要があります。

   管理インターフェイスへの不正アクセスを防ぐために、管理者が *MGT* インターフェイスにアクセスできる***Permitted IP Addresses*** を追加するのが管理のベスト プラクティス です。
3. **Speed**[速度] を **auto-negotiate** に設定します。
4. インターフェイスで許可する管理サービスを選択します。

   Telnet と ***HTTP*** が選択されていないことを確認します。これは、これらのサービスでは平文が使用され、他のサービスほど安全ではなく、管理者の認証情報が漏洩する可能性があるからです。

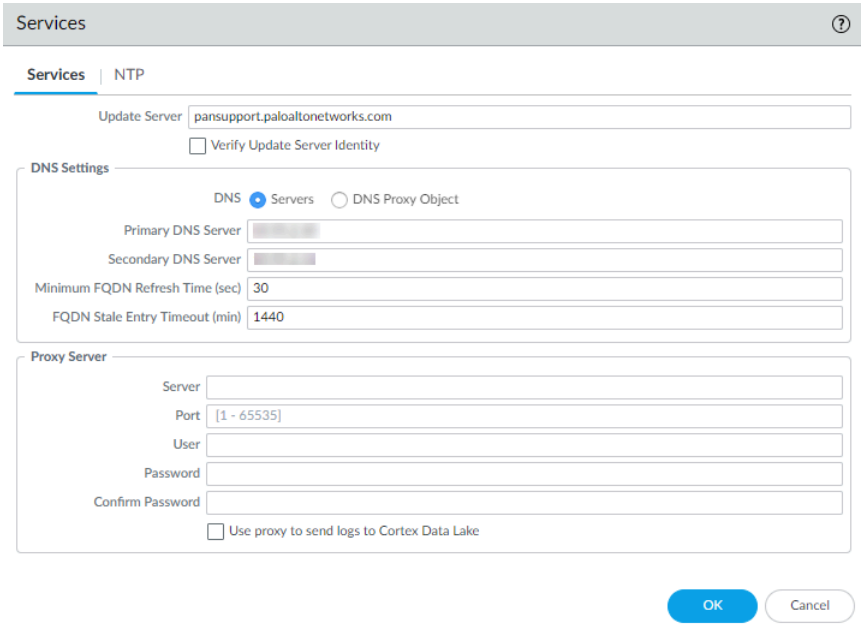


5. **OK** をクリックします。

STEP 7 | DNS、アップデート サーバー、およびプロキシ サーバーの設定を行います。

ファイアウォールで少なくとも *1* つの *DNS* サーバーを手動で設定する必要があり、設定しないとホスト名を解決することができなくなります。そのファイアウォールは、*ISP* などの別のソースからの *DNS* サーバー設定を使用しません。

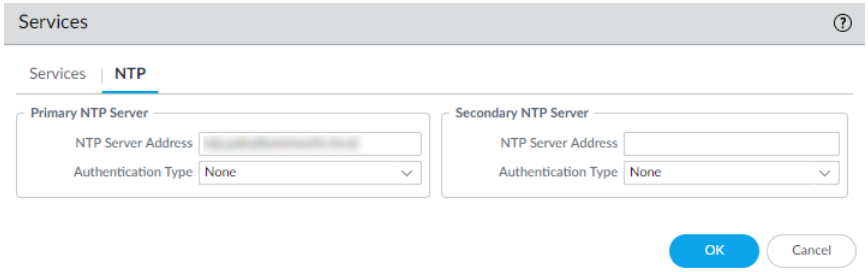
1. **Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）
   - マルチ仮想システム プラットフォームの場合は、**Global** [グローバル]を選択して Services [サービス]セクションを編集します。
   - 1 つの仮想システム プラットフォームの場合は、Services [サービス]セクションを編集します。
2. **Services** [サービス]タブの **DNS** で、以下のいずれかを選択します：
   - **Servers (サーバー)** — **Primary DNS Server (プライマリ DNS サーバー)** アドレスと **Secondary DNS Server (セカンダリ DNS サーバー)** アドレスを入力します。
   - **DNS Proxy Object (DNS プロキシ オブジェクト)** — ドロップダウンリストから、グローバル DNS サービスの設定に使用する **DNS Proxy (DNS プロキシ)** を選択するか、**DNS Proxy (DNS プロキシ)** をクリックして新しい DNS プロキシ オブジェクトを設定します。



3. **OK** をクリックします。

STEP 8 | 日時（NTP）の設定を行います。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）
   - マルチ仮想システム プラットフォームの場合は、**Global** [グローバル]を選択して Services [サービス]セクションを編集します。
   - 1 つの仮想システム プラットフォームの場合は、Services [サービス]セクションを編集します。
2. **NTP** タブでインターネット上のタイム サーバーの仮想クラスタを使用するには、**Primary NTP Server** [プライマリ NTP サーバー]にホスト名「`pool.ntp.org`」を入力するか、プライマリ NTP サーバー の IP アドレスを入力します。



3. （任意）**Secondary NTP Server** [セカンダリ NTP サーバー]のアドレスを入力します。
4. （任意）NTP サーバーからの時間の更新を認証するには、各サーバーの **Authentication Type** [認証タイプ]で以下のいずれかを選択します。
   - **None** [なし] – （デフォルト）NTP 認証を無効にします。
   - **Symmetric Key** [対称キー] – ファイアウォールで対象キー交換（共有のシークレット）を使用して時間の更新を認証します。
     - **Key ID**（キーID） – キーID（1～65534）を入力します。
     - **Algorithm** [アルゴリズム] – NTP 認証に使用するアルゴリズムを選択します（**MD5** または **SHA1**）。
   - **Autokey** [自動キー] – ファイアウォールで自動キー（公開鍵暗号）を使用して時間の更新を認証します。
5. **OK** をクリックします。

STEP 9 | （任意）全般的なファイアウォールの設定を行います。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して General Settings (一般設定) を編集します。
2. ファイアウォールの **Hostname**[ホスト名] を入力し、ネットワークの **Domain**[ドメイン] 名を入力します。ドメイン名は単なるラベルであるため、ドメインに参加するために使用されることはありません。
3. ログインしようとしているユーザーに対して、ファイアウォール管理機能にアクセスするには認証が必要であることを通知するテキストを **Login Banner** [ログイン バナー]に入力します。

   ウェルカムメッセージなどの入力は避け、簡潔に内容を通知することをお勧めします。さらに、法務担当者にバナーメッセージを確認してもらい、不正なアクセスを禁止する文言が適切かどうかよく確認してください。
4. **Latitude**（緯度） と **Longitude**（経度） を入力し、そのファイアウォールが世界地図上の正確な場所に配置されるようにします。
5. **OK** をクリックします。

STEP 10 | 変更をコミットします。

設定の変更を保存すると*IP*アドレスが変更されるため、*Web*インターフェイスへの接続が遮断されます。

Webインターフェイスの右上にある **Commit**[コミット] をクリックします。ファイアウォールが変更を保存するまでに最大90秒かかります。

STEP 11 | ファイアウォールをネットワークに接続します。

1. コンピュータからファイアウォールを切断します。
2. (PA-5450 を除くすべてのファイアウォール) RJ-45 Ethernet ケーブルを使用して、MGT ポートを管理ネットワーク上のスイッチ ポートに接続します。ファイアウォールからケーブルで接続するスイッチ ポートが auto-negotiation に設定されていることを確認します。
3. (PA-5450 のみ)Palo Alto Networks 認定の SFP/SFP+ トランシーバーとケーブルを使用して、MGT ポートを管理ネットワーク上のスイッチ ポートに接続します。

STEP 12 | ファイアウォールへの SSH 管理セッションを開きます。

PuTTY などの端末エミュレーション ソフトウェアを使用し、割り当てた新しい IP アドレスを使用してファイアウォールへの SSH セッションを開始します。

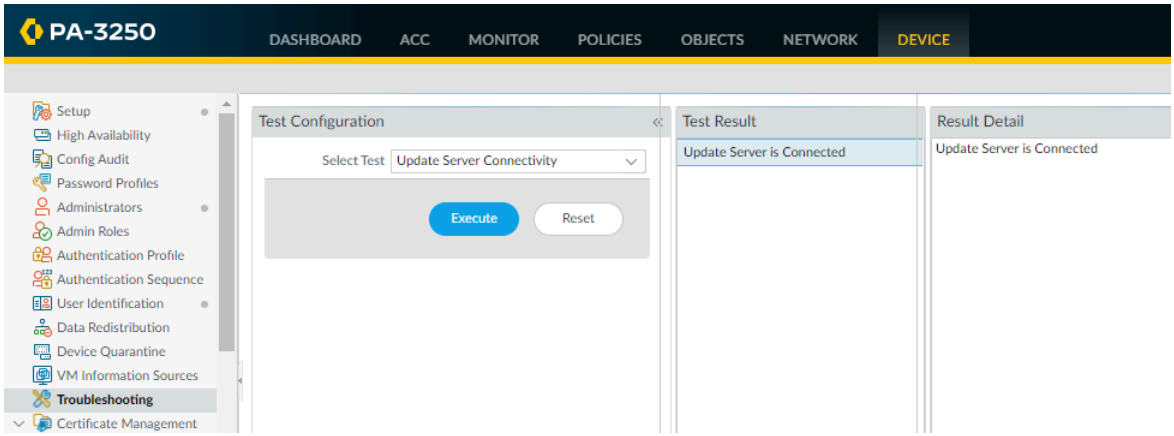
STEP 13 | Palo Alto Networks 更新サーバーなど、ファイアウォール管理に必要な外部サービスへのネットワーク アクセスを確認します。

以下のいずれかの方法でこの作業を行えます。

- MGT インターフェイスに外部ネットワークへのアクセスを許可しない場合は、必要なサービス アップデートを取得するようにデータ ポートをセットアップする必要があります。外部サービスへのネットワーク アクセスのセットアップに進んでください。
- MGT インターフェイスへの外部ネットワーク アクセスを許可する場合は、接続があることを確認し、Register the Firewall に進み、サブスクリプション ライセンスのアクティベーションします。

1. 以下の例に示すように、更新サーバー接続性テストを使用して Palo Alto Networks 更新サーバーへのネットワーク接続を検証します。

   1. **Device** > **Troubleshooting (**デバイストラブルシューティング**)** を選択し、Select Test (テストの選択) ドロップダウンから **Update Server Connectivity (**更新サーバー接続性**)** を選択します。
   2. 更新サーバー接続性テストを **Execute (**実行**)** します。



2. 以下の CLI コマンドを実行して、Palo Alto Networks 更新サーバーからファイアウォールのサポート資格に関する情報を取得します。

```
request support check
```

接続されている場合、更新サーバーはファイアウォールのサポート ステータスを伴うレスポンスを返します。ファイアウォールが登録されていない場合、更新サーバーは次のメッセージを返します。

```
Contact Us https://www.paloaltonetworks.com/company/contact-
us.html
Support Home https://www.paloaltonetworks.com/support/tabs/
overview.html
Device not found on this update server
```

外部サービスへのネットワーク アクセスのセットアップ

ファイアウォールは、デフォルトで MGT インターフェイスを使用して、DNS サーバー、コンテンツ更新、およびライセンス取得などのリモート サービスにアクセスします。管理ネットワークへの外部アクセスを不可能にしたい場合は、必要な外部サービスにアクセスできるようにインバンド データポートをセットアップし、さらに外部サービスにアクセスする際にファイアウォールがどのポートを使用するのか指定するためにサービスルートを設定します。

インターネットからまたは企業のセキュリティ境界内の他の信頼されていないゾーンから、管理へのアクセスを有効にしないでください。Adminstrative Access Best Practices に従って、ファイアウォールを適切に保護していることを確認します。

このタスクを行うには、ファイアウォールのインターフェイス、ゾーン、およびポリシーに精通しておく必要があります。これらのトピックの詳細については、インターフェイスとゾーンの設定および基本的なセキュリティ ポリシーのセットアップを参照してください。

STEP 1 | 外部サービスへのアクセスで使用するインターフェイスを決定し、それをスイッチまたはルーターのポートに接続します。

使用するインターフェイスには、スタティック IP アドレスが必要です。

STEP 2 | Web インターフェイスにログインします。

Web ブラウザーからのセキュア接続 (https) を使用して、初期構成 (https://<IP address>) 時に割り当てた新しい IP アドレスとパスワードを使用してログインします。証明書の警告が表示されますが、問題ありません。そのまま続行して Web ページを開きます。

STEP 3 | （任意）ファイアウォールは、Ethernet 1/1 ポートと Ethernet 1/2 ポート（および対応するデフォルトのセキュリティ ポリシーとゾーン）の間のデフォルトのバーチャル ワイヤー インターフェイスが事前設定されて出荷されます。このバーチャル ワイヤー設定を使用する予定がない場合は、定義する他のインターフェイスの設定と干渉しないようにするため、その設定を手動で削除する必要があります。

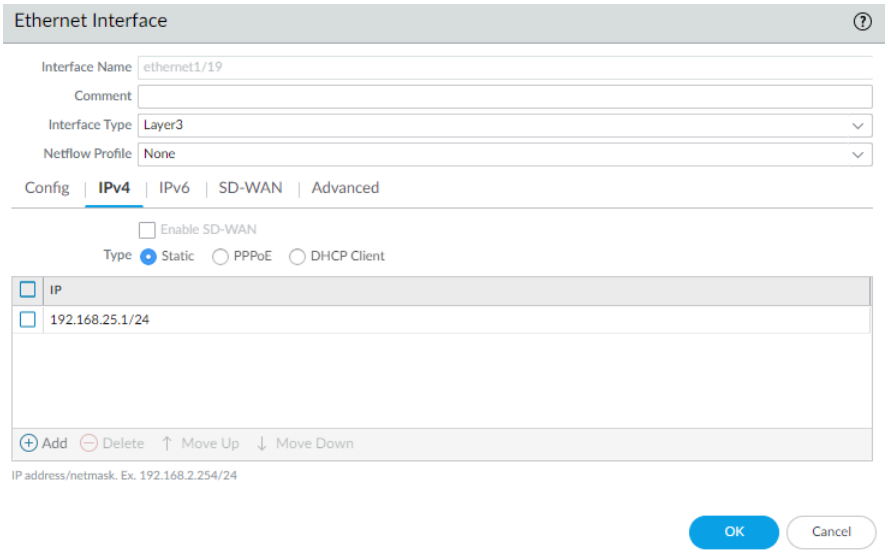
設定は以下の順序で削除する必要があります。

1. デフォルトのセキュリティ ポリシーを削除するには、**Policies (ポリシー)** > **Security (セキュリティ)** の順に選択してルールを選択し、**Delete (削除)** をクリックします。
2. デフォルトのバーチャル ワイヤーを削除するには、**Network (ネットワーク)** > **Virtual Wires (バーチャル ワイヤ)** の順に選択し、バーチャル ワイヤーを選択して **Delete (削除)**をクリックします。
3. デフォルトの信頼できるゾーンと信頼できないゾーンを削除するには、**Network (ネットワーク)** > **Zones (ゾーン)** の順に選択し、各ゾーンを選択して **Delete (削除)** をクリックします。
4. インターフェイス設定を削除するには、**Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択してから各インターフェイス（ethernet1/1 と ethernet1/2）を選択し、**Delete (削除)** をクリックします。
5. 変更を **Commit**（コミット）します。

STEP 4 | 管理サービスへの外部アクセスに使用する予定のインターフェイスを設定します。

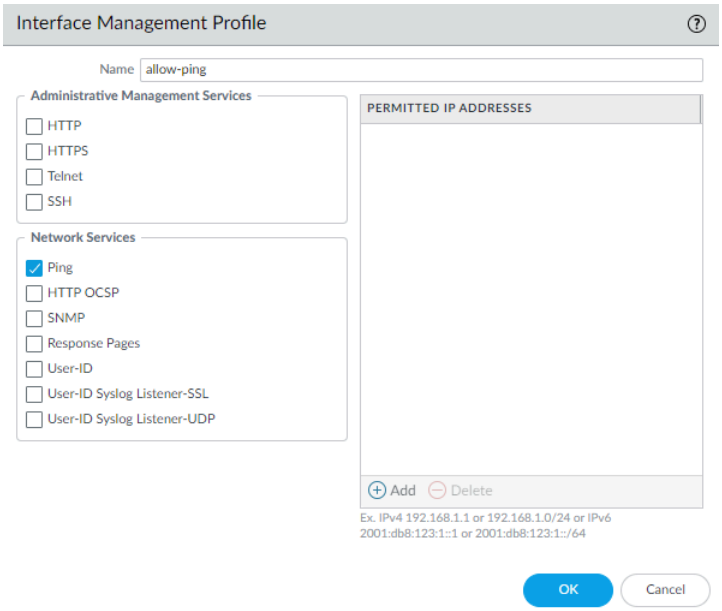
1. **Network (**ネットワーク**)** > **Interfaces (**インターフェース**)** の順に選択し、ステップ 1 でケーブルを接続したインターフェースに対応するインターフェースを選択します。
2. **Interface Type**（インターフェイス タイプ）を選択します。ここで選択するタイプはご使用のネットワーク トポロジに応じて異なりますが、この例では、**Layer3** [レイヤー 3]の場合の手順を示します。
3. **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。
4. Zone [ゾーン] ダイアログで新しいゾーンの **Name**[名前] （例：Management）を入力し、**OK** をクリックします。
5. **IPv4** タブを選択し、**Static**[静的] ラジオ ボタンを選択し、IP セクションの **Add**[追加] をクリックして、インターフェイスに割り当てる IP アドレスとネットワーク マスク

(「192.168.1.254/24」など) を入力します。このインターフェイスでは静的IPアドレスを使用する必要があります。



6. **Advanced** (詳細) > **Other Info** (その他の情報) の順に選択し、 **Management Profile** (管理プロファイル) ドロップダウン リストを展開して **New Management Profile** (新規管理プロファイル) を選択します。
7. プロファイルの **Name** [名前]（「allow_ping」など）を入力し、インターフェイスで許可するサービスを選択します。外部サービスへのアクセスを許可する目的の場合は、**Ping** のみをオンにして **OK** をクリックします。

許可するサービスにはファイアウォールへの管理アクセス権が付与されるため、このインターフェイスで許可する管理アクティビティに対応するサービスのみを選択してください。例えば、これらのプロトコルが平文で送信を行い、安全ではないため *HTTP* または *Telnet* を有効にしないでください。または、ウェブインターフェイスまたは *CLI* によるファイアウォール設定タスクで *MGT* インターフェイスを使用する場合は、*HTTP*、*HTTPS*、*SSH*、または *Telnet* を有効にしないことにより、このインターフェイスを介した不正アクセスを防止することができます (*HTTPS* あるいは *SSH* を有効にする場合は、***Permitted IP Addresses*** (アクセス許可 ***IP*** アドレス) で特定の *IP* アドレス セットへのアクセスを制限する必要があります)。詳細についてはインターフェイス管理プロファイルを使用してアクセスを制限を参照してください。



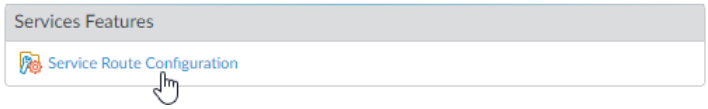
8. インターフェイス設定を保存するには、**OK** をクリックします。

STEP 5 | サービス ルートを設定します。

デフォルト設定では、ファイアウォールはMGTインターフェイスを使用して必要な外部サービスにアクセスします。ファイアウォールが外部サービスにリクエストを送信する際に使用するインターフェイスを変更するには、サービスルートを編集する必要があります。

この例では、グローバル サービスルートの設定方法について説明します。グローバル ベースではなく仮想システム ベースでの外部サービスへのネットワーク アクセスについての詳細は、仮想システムのサービスへのサービス ルートのカスタマイズを参照してください。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Services (サービス)** > **Global (グローバル)** を選択し、**Service Route Configuration (サービスルート設定)** をクリックします。



ライセンスをアクティベーションし、最新のコンテンツ更新とソフトウェア更新を取得する場合には、***DNS***、***Palo Alto Networks Services (Palo Alto Networks* サービス*)***、***URL Updates (URL* アップデート*)***、および ***AutoFocus*** のサービス ルートを変更できます。

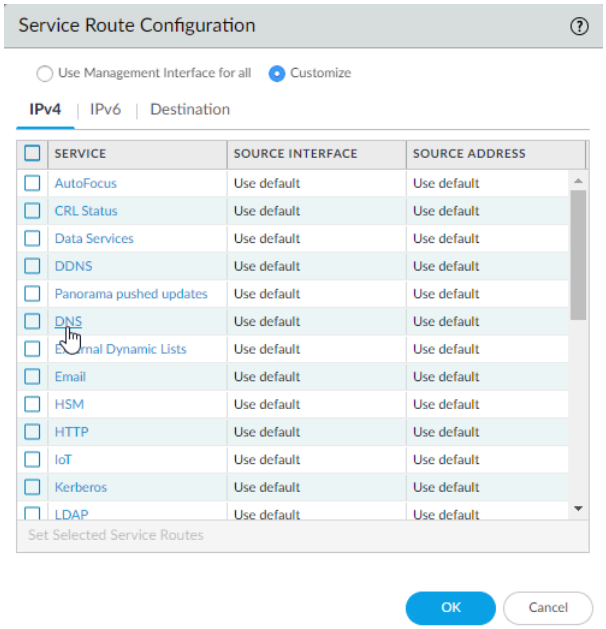
2. [カスタマイズ] ラジオ ボタンをクリックし、以下のいずれかを選択します。

   - 定義済みのサービスの場合は、**IPv4** または **IPv6** を選択し、サービスのリンクをクリックします。Source Address（送信元アドレス）のドロップダウンリストを制限するには、 **Source Interface**（送信元インターフェイス）を選択し、今設定したインターフェイスを選択します。次に、サービス ルートとして（そのインターフェイスから）送信元アドレスを選択します。

     選択したインターフェイスに複数の IP アドレスが設定されている場合、**Source Address**（送信元アドレス）ドロップダウン リストで IP アドレスを選択できます。

   - カスタム宛先のサービス ルートを作成するには、**Destination**（宛先）を選択して、**Add**（追加）をクリックします。**Destination**（宛先）の IP アドレスを入力します。このアドレスと一致する宛先アドレスを持つ着信パケットは、このサービス ルートに指定したSource Address（発信元アドレス）を発信元として使用します。Source Address（送信元アドレス）のドロップダウンを制限するには、**Source Interface**（送信元インターフェイス）を選択します。選択したインターフェイスに

複数の IP アドレスが設定されている場合、**Source Address**（送信元アドレス）ドロップダウン リストで IP アドレスを選択できます。



3. **OK** をクリックして設定を保存します。
4. 変更する各サービス ルートについて、上記の手順 5.2～5.3 を繰り返します。
5. 変更をコミットします。

STEP 6 | 外部へのインターフェイスおよび関連付けられたゾーンを設定し、ファイアウォールが内部ゾーンから外部ゾーンにサービス要求を送信することを許可するようにセキュリティ ポリシー ルールを作成します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択して、外部へのインターフェイスを選択します。**Interface Type**[インターフェイス タイプ] として **Layer3**[レイヤー 3] を選択し、**IP** アドレスを **Add**[追加] して（**IPv4** または **IPv6** タブ）、「Internet」など関連する **Security Zone**[セキュリティ ゾーン]（**Config**[設定] タブ）を作成します。このインターフェイスには静的IPアドレスが必要です。また、インターフェイス上で管理サービスをセットアップする必要はありません。

2. 内部ネットワークから Palo Alto Networks アップデート サーバーへのトラフィックを許可するセキュリティ ルールをセットアップするには、**Policies (ポリシー)** > **Security (セキュリティ)** の順に選択して **Add (追加)** をクリックします。

セキュリティポリシー ルールを作成する際、ポート ベースのルールではなくアプリケーション ベースのルールを利用し、ポート、プロトコル、回避戦略、採用する暗号化に関わらず、必ず正確に下層のアプリケーションを識別できるようにすることをお勧めいたします。***Service***[サービス]は常に***application-default*** に設定してください。この場合、更新サーバー（およびその他の*Palo Alto Networks*サービス）へのアクセスを許可するセキュリティポリシー ルールを作成します。

	NAME	Source ZONE	Destination ZONE	APPLICATION	SERVICE	ACTION
1	Palo Alto Networks Services	Management	Internet	paloalto-dns-security paloalto-logging-service paloalto-updates paloalto-wildfire-cloud	application-...	Allow

STEP 7 | NATポリシー ルールを作成します。

1. 内向きインターフェイスでプライベート IP アドレスを使用する場合は、そのアドレスをパブリックにルーティング可能なアドレスに変換するソース NAT ルールを作成する必要があります。**Policies (ポリシー)** > **NAT** の順に選択して **Add (追加)** をクリックします。少なくとも、ルールの名前を定義し（**General**[全般] タブ）、送信元と宛先のゾーン（この場合は Management [管理]から Internet インターネット）を指定し（**Original Packet**[元のパケット] タブ）、送信元アドレス変換の設定項目を定義して（**Translated Packet**[変換済みパケット] タブ）、**OK** をクリックする必要があります。
2. 変更をコミットします。

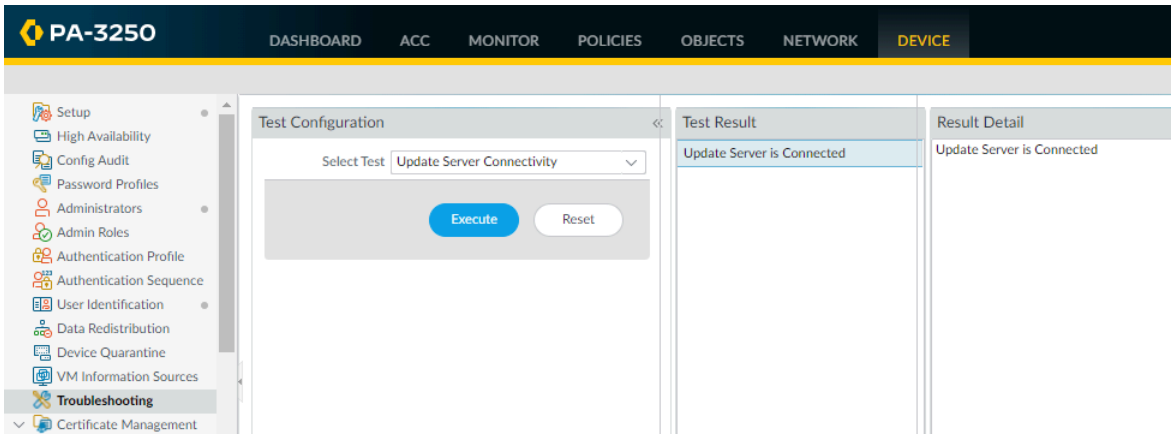
	NAME	Original Packet SOURCE ZONE	DESTINATION ZONE	SERVICE	Translated Packet SOURCE TRANSLATION	DESTINATION TRANSLATION
1	Source NAT	Management	Internet	any	dynamic-ip-and-port	none

STEP 8 | **Device (デバイス)** > **Troubleshooting (トラブルシューティング)** を選択して、**Ping** 接続テストを使用してデータポートから外部サービス (デフォルトゲートウェイを含む)、および **Update Server Connectivity (更新サーバー接続性)** テストを使用して Palo Alto Networks 更新サーバーに接続できることを確認します。この例では、Palo Alto Networks Update Server へのファイアウォール接続がテストされています。

必要なネットワーク接続があることを確認したら、Register the Firewall に進み、サブスクリプション ライセンスのアクティベーションします。

1. Select Test (テストの選択) ドロップダウンから **Update Server (サーバーの更新)** を選択します。

2. Palo Alto Networks Update Server の接続性テストを **Execute (実行)** します。



3. ファイアウォール CLI にアクセスし、以下のコマンドを実行して、Palo Alto Networks 更新サーバーからファイアウォールのサポート資格に関する情報を取得します。

```
サポートチェックをリクエストする
```

接続されている場合、更新サーバーはファイアウォールのサポート ステータスを伴うレスポンスを返します。ファイアウォールが登録されていないため、更新サーバーは次のメッセージを返します。

```
お問い合わせ https://www.paloaltonetworks.com/company/contact-us.html サポートホーム https://www.paloaltonetworks.com/support/tabs/overview.html Device not found on this update server
```

ファイアウォールの登録

サポート、ライセンスやサブスクリプションのアクティベーションを行う前に、ファイアウォールを登録しておく必要があります。しかし、ファイアウォールを登録する前に、まずはサポートアカウントを有効化する必要があります。アクティブなサポートアカウントをお持ちかどうかに応じて、次のいずれかの作業を行います：

- アクティブなサポートアカウントをお持ちでない場合は、新しいサポートアカウントを作成してファイアウォールを登録してください。
- すでにアクティブなサポートアカウントをお持ちの場合は、ファイアウォールの登録する準備ができています。
- 登録済みのfirewallで(任意) 初日設定の実行します。
- firewall が NPC (Network Processing Card) などのラインカードを使用している場合は、ファイアウォール ラインカードの登録します。

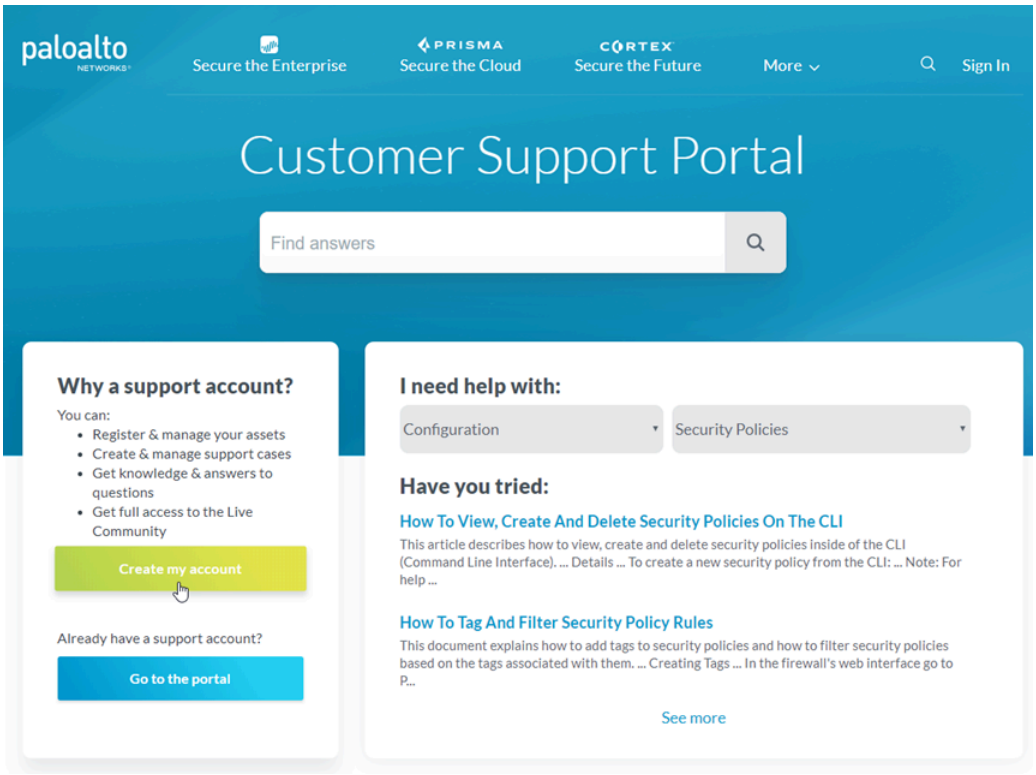
VM-Seriesファイアウォールの登録を行う際はVM-Series導入ガイドの指示を参照してください。

新しいサポートアカウントを作成してファイアウォールを登録

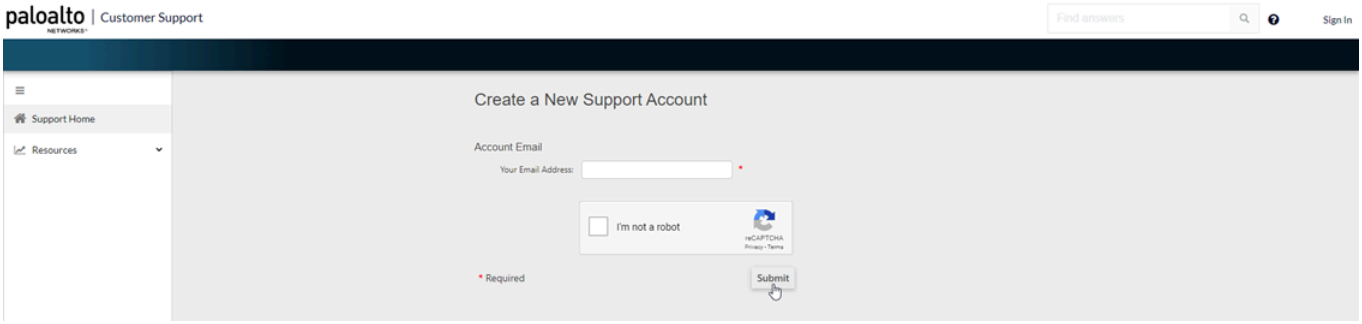
アクティブな Palo Alto Networks のサポートアカウントをまだ持っていない場合は、新しいサポートアカウントを作成する際にファイアウォールを登録する必要があります。

STEP 1 | Palo Alto Networks カスタマー サポート ポータルにアクセスします。

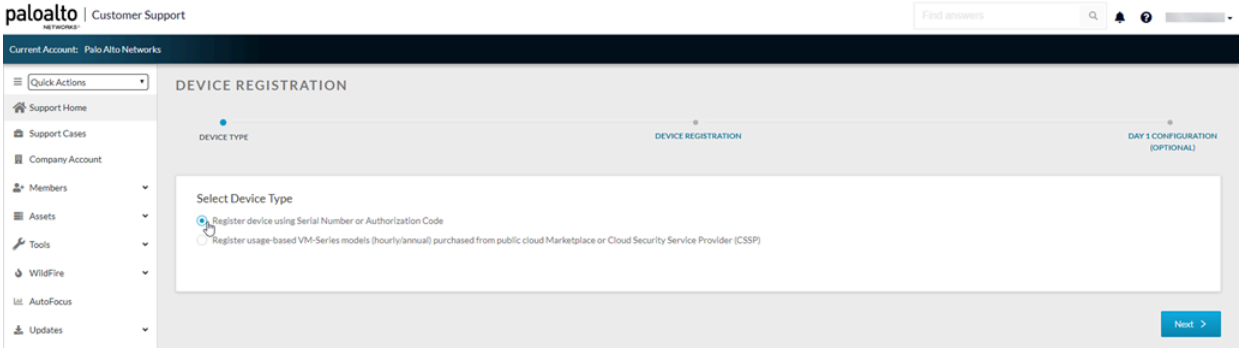
STEP 2 | **Create my account (**アカウントを作成**)** をクリックします。



STEP 3 | **Your Email Address (**お使いの **E** メールアドレス**)**を入力して、**I'm not a robot (**私はロボットではありません**)** をチェックし、**Submit (**送信**)** をクリックします。

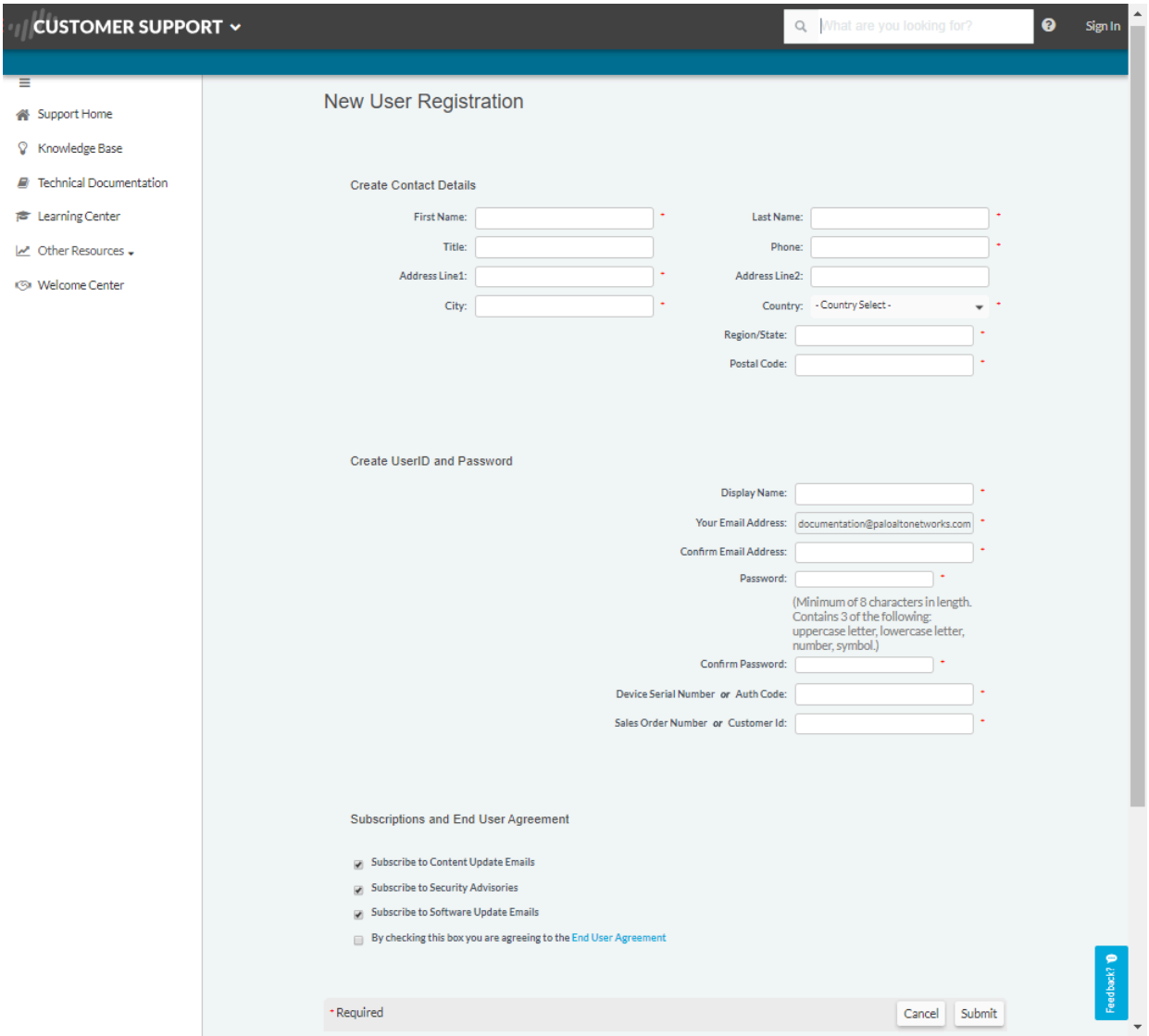


STEP 4 | **Register device using Serial Number or Authorization Code**（シリアル番号または認証コードを使用してデバイスを登録）を選択し、**Next**（次へ）をクリックします。



STEP 5 | 登録フォームを完成させます。

1. このアカウントを所有する組織内の担当者の連絡先を入力します。赤いアスタリスクが付いているのが必須フィールドです。
2. アカウントの UserID およびパスワードを作成します。赤いアスタリスクが付いているのが必須フィールドです。
3. **Device Serial Number**（デバイスのシリアルナンバー） または **Auth Code**（認証コード） を入力します。
4. **Sales Order Number**（販売受注番号） または **Customer Id**（顧客 **ID)** を入力します。
5. 最新のアップデートとセキュリティ情報のアラートを受け取るようにするには、**Subscribe to Content Update Emails (**コンテンツ更新 **E** メールの登録**)**、**Subscribe to Security Advisories (**セキュリティ アドバイザーの登録**)**、および **Subscribe to Software Update Emails (**ソフトウェア更新 **E** メールの登録**)** を選択します。
6. チェックボックスを選択し、エンドユーザー規約に同意して**Submit (**送信**)**します。



ファイアウォールの登録

すでにアクティブな Palo Alto Networks カスタマーサポートのアカウントをお持ちである場合は、以下の作業を行ってファイアウォールを登録します。

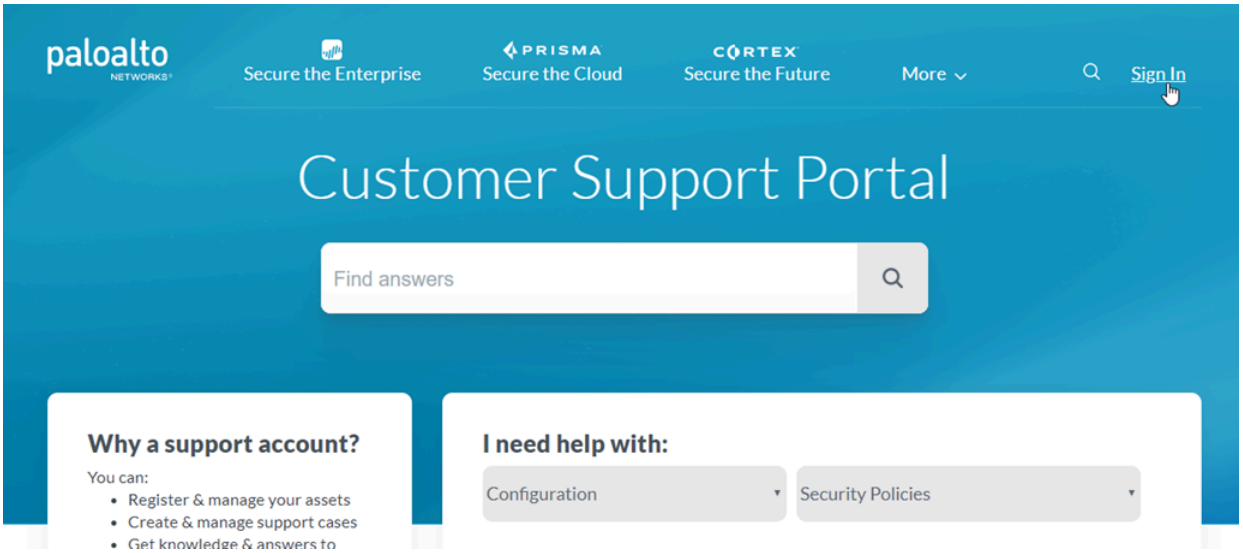
STEP 1 | ファイアウォール インターフェイスにログインします。

Web ブラウザーからのセキュア接続 (HTTPS) を使用して、初期構成 (https://<IP address>) 時に割り当てた新しい IP アドレスとパスワードを使用してログインします。

STEP 2 | シリアル番号を見つけ、クリップボードにコピーします。

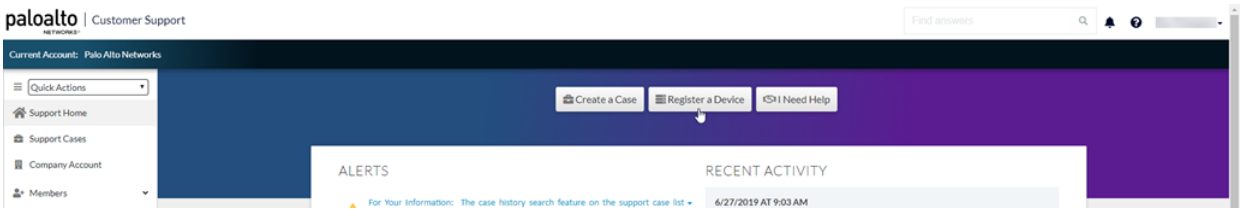
Dashboard [ダッシュボード]で、画面の General Information [一般的な情報]セクションに表示されている **Serial Number** [シリアル番号]を確認します。

STEP 3 | Palo Alto Networks カスタマーサポート ポータルに移動し、まだログインしていない場合は今すぐ **Sign In (**サインイン**)**します。

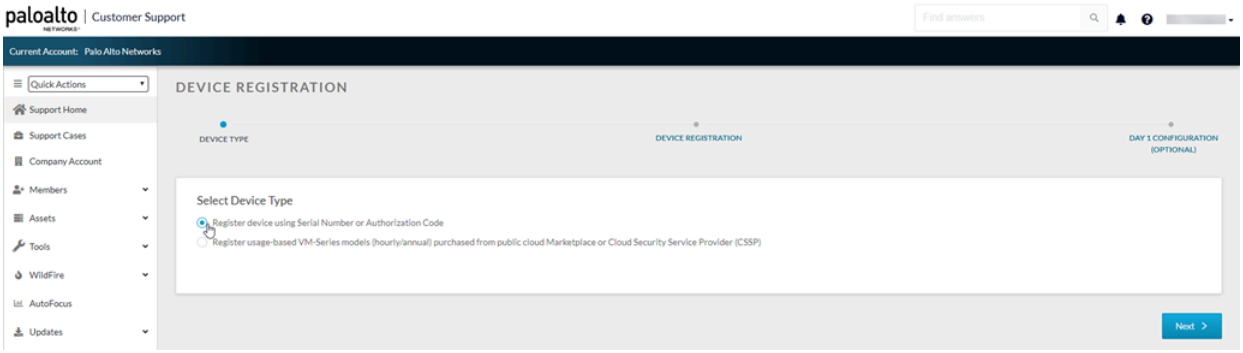


STEP 4 | ファイアウォールを登録します。

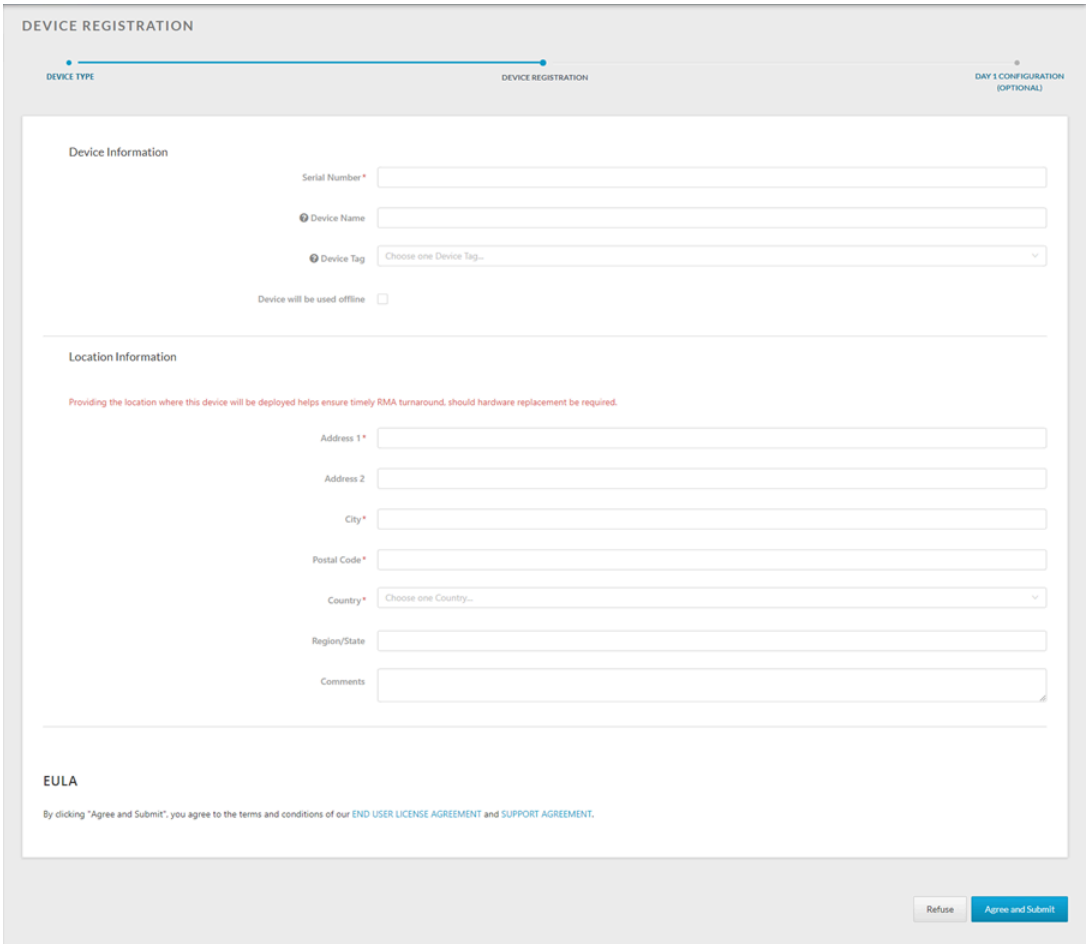
1. Support Home (サポートホーム) ページで、**Register a Device (デバイスの登録)** をクリックします。



2. **Register device using Serial Number or Authorization Code (シリアル番号または認証コードを使用してデバイスを登録)** を選択してから **Next (次)** をクリックします。



3. ファイアウォールの**Serial Number**[シリアル番号]（ファイアウォールのダッシュボードからコピー＆ペースト可能）を入力します。
4. （任意）**Device Name (デバイス名)**および**Device Tag (デバイスタグ)**を入力します。
5. （任意）デバイスをインターネットに接続しない場合は、**Device will be used offline (デバイスをオフラインで使用)**のチェックボックスを選択してから、使用する予定の**OS Release (OS リリース)**をドロップダウンリストで選択します。
6. ファイアウォールを導入する予定の場所を、**Address**（住所）、**City**（都市）、**Postal Code**（郵便番号）、**Country**（国）を含めて入力します。
7. エンドユーザー向け使用許諾契約（EULA）およびサポート規約をよく読み、**Agree and Submit (同意して送信)**します。



Devices（デバイス）で登録したファイアウォールのエントリを表示できます。

STEP 5 | (ラインカード付き Firewalls)firewall のラインカードのサポートを確実に受けるには、必ずファイアウォール ラインカードの登録してください。

(任意) 初日設定の実行

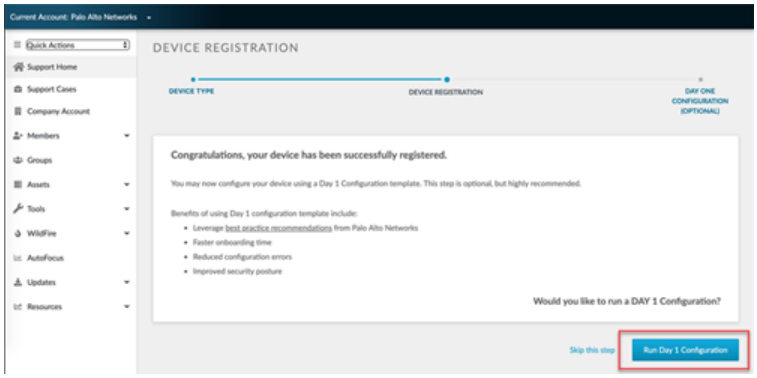
ファイアウォールを登録したら、初日設定を実行することができます。初日設定ツールには、残りの設定を構築するための開始点として使用できる、Palo Alto Networks ベストプラクティスによって通知された設定テンプレートが用意されています。

初日設定テンプレートの利点は次のとおりです。

- より速い実施時間
- 設定エラーの減少
- 改善されたセキュリティ体制

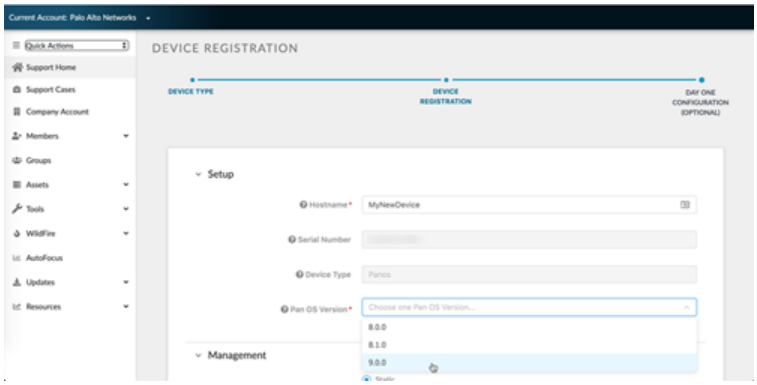
以下のステップに従い、初日設定を行います。

STEP 1 | ファイアウォールを登録した後に表示されるページから、**Run Day 1 Configuration (**初日設定の実行**)** を選択します。



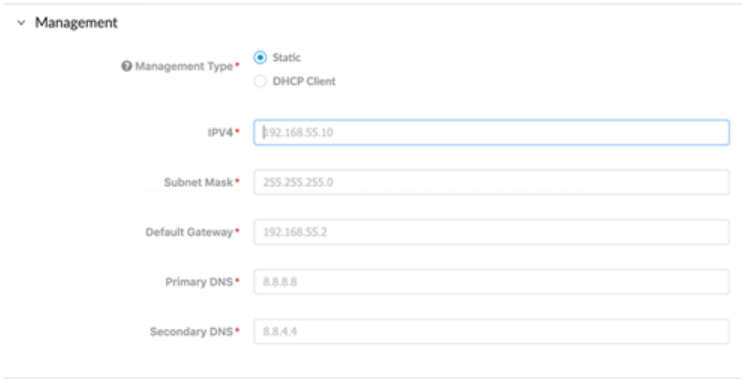
ファイアウォールをすでに登録したものの、初日設定を実行していない場合は、カスタマー サポート ポータルのホームページから***Tools***） **>** ***Run Day 1 Configuration***を選択して実行することもできます。

STEP 2 | 新しいデバイスの **Hostname (**ホスト名**)** と **Pan OS Version (Pan OS** バージョン**)** を入力し、必要に応じて **Serial Number (**シリアル番号**)** と **Device Type (**デバイスタイプ**)** も入力します。



STEP 3 | **Management (管理)** で、**Management Type (管理タイプ)** について **Static (静的)** あるいは **DHCP Client (DHCP クライアント)** を選択します。

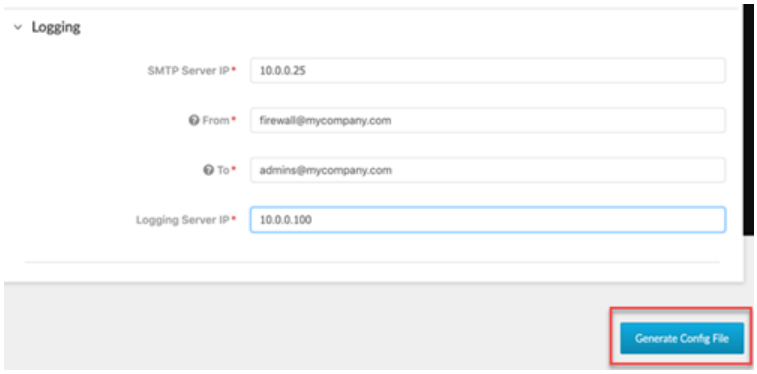
Static (静的) を選択した場合、**IPV4**、**Subnet Mask (サブネットマスク)**、および **Default Gateway (デフォルトゲートウェイ)** フィールドの各フィールドに入力する必要があります。



DHCP Client (DHCP クライアント) を選択すると、**Primary DNS (プライマリ DNS)** および **Secondary DNS (セカンダリ DNS)** を入力するだけで済みます。DHCP クライアントモードに設定されたデバイスは、管理インターフェイスがローカル DHCP サーバから IP アドレスを確実に受信するようにします。また、既知の場合はすべてのパラメータを入力します。

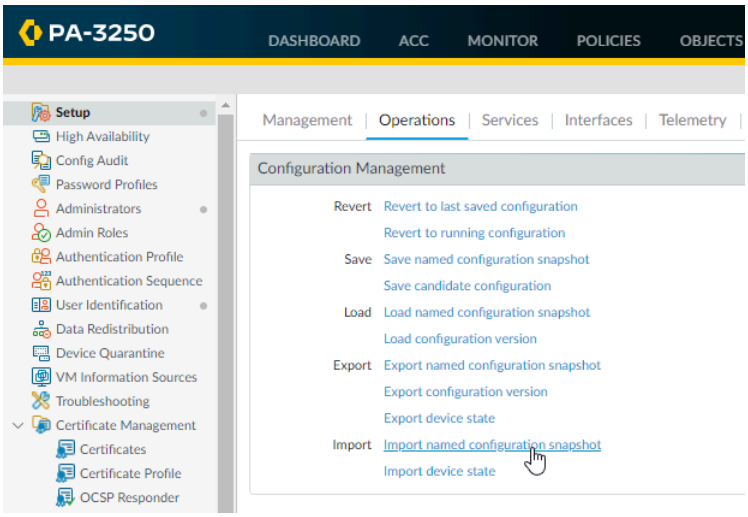
STEP 4 | **Logging (ロギング)** ですべてのフィールドに入力します。

STEP 5 | **Generate Config File (設定ファイルの生成)** をクリックします。



STEP 6 | ダウンロードした初日設定ファイルをファイアウォールにインポートして読み込むには：

1. ファイアウォール ウェブインターフェイスにログインします。
2. **Device**（デバイス） > **Setup**（セットアップ） > **Operations**（操作）を選択します。
3. **Import named configuration snapshot (**名前付き設定スナップショットのインポート**)** をクリックします。
4. ファイルを選択します。



ファイアウォール ラインカードの登録

次のファイアウォールでは、トラブルシューティングと返品のサポートを受けるために登録する必要があるラインカードを使用します。

- PA-7000 シリーズ ファイアウォール
- PA-5450 ファイアウォール

Palo Alto Networks Customer Support アカウントをお持ちでない場合は、新しいサポートアカウントを作成してファイアウォールを登録の手順に従ってアカウントを作成します。カスタマーサポート アカウントを作成し、ファイアウォールを登録した後、次の手順に戻ります。

STEP 1 | Palo Alto Networks カスタマーサポート ポータルに移動し、まだログインしていない場合は今すぐ **Sign In (**サインイン**)**します。

STEP 2 | >資産<2ライン カード/オプティクス/FRU を選択します。

STEP 3 | 登録コンポーネント。

STEP 4 | 登録の対象となるラインカードを表示するには、[販売受注番号 フィールドにラインカードの Palo Alto Networks 受注番号を入力します。

STEP 5 | **Serial Number** フィールドにシャーシのシリアル番号を入力して、ラインカードをファイアウォールに登録します。ファイアウォールの登録情報に基づいて、オートデータを自動入力する 場所情報 の下の情報を指定します。

STEP 6 | 法的条件に同意するには、同意して提出をクリックします。資産 > ライン カード/オプティクス/**FRU** の下に登録されたラインカードが表示されます。

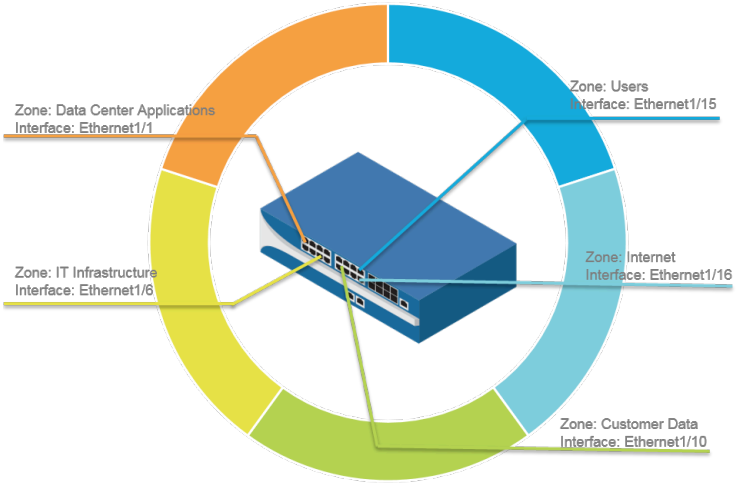
インターフェイスやゾーンを用いたネットワークのセグメント化

ファイアウォールでトラフィックを管理および制御するには、そのファイアウォールをトラフィックが通過する必要があります。物理的には、インターフェイスを介してトラフィックがファイアウォールを出入りします。ファイアウォールでは、パケットがセキュリティ ポリシー ルールと一致するかどうかに基づいてパケットの処理方法が決定されます。最も基本的なレベルでは、各セキュリティ ポリシー ルールで、トラフィックの送信元と送信先を特定する必要があります。Palo Alto Networks の次世代ファイアウォールでは、セキュリティ ポリシー ルールがゾーン間で適用されます。ゾーンとは（物理あるいは仮想）インターフェイスのグループ分けのことであり、これはファイアウォールに接続する、あるいはファイアウォールに制御されるネットワークの各領域を表します。セキュリティポリシーのルールによって許可されていれば、各ゾーン間以外をトラフィックが流れることはないため、これが最初の防御手段になります。ゾーンをより細かく作成することで、重要なアプリケーションやデータへのアクセスをさらに厳重に制御できるようになり、ネットワーク全体を移動するマルウェアに対する防御力も高まります。例えば、顧客情報を保存しているデータベースサーバーへのアクセスを、「Customer Data」というゾーンに区切ることができます。次に、特定のユーザーやユーザーグループだけが「Customer Data」ゾーンにアクセスできるようにするセキュリティ ポリシーを策定することで、このセグメントに保存されているデータへの不正な内部アクセスや外部アクセスを防ぐことができます。

- ネットワークのセグメント化により攻撃の入り口を減らす
- インターフェイスとゾーンの設定

ネットワークのセグメント化により攻撃の入り口を減らす

次の図は、ゾーンを使用してネットワークをセグメント化する際の最も基本的な方法を示しています。ゾーン（およびそれに対応する、各ゾーン間のトラフィックを許可するセキュリティポリシーのルール）をより細かく作成することで、ネットワークに対する攻撃の入り口をさらに減らすことができます。なぜなら、ゾーン内であればトラフィックは自由に流れることができますが（イントラゾーン トラフィック）、これがゾーン間となると、流れを許可するセキュリティポリシー ルールを定義していない限り、自由に流れることはできないからです。さらに、ゾーンを割り当てていないインターフェイスはトラフィックを処理できません。そのため、ネットワークをより細かなゾーンにセグメント化することで、重要なアプリケーションやデータへのアクセスをさらに厳重に制御できるようになり、悪意のあるトラフィックがネットワーク内で通信チャネルを確立するのを防止できるようになるため、ネットワークへの攻撃が成功する確率を下げることができます。



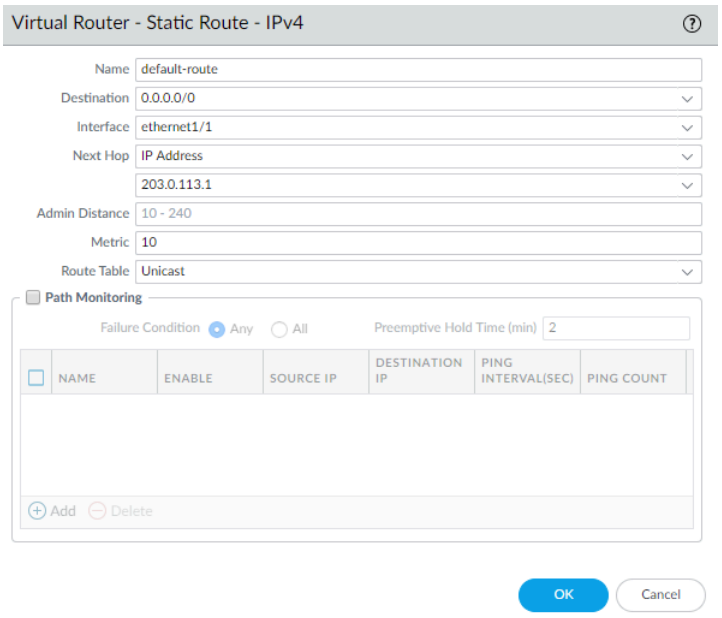
インターフェイスとゾーンの設定

ネットワークをどのようにセグメント化するか、またセグメント化を行うためにどのようなゾーンが必要か（さらに各ゾーンをマッピングするインターフェイスと併せて）判断したら、ファイアウォールのインターフェイスおよびゾーンの構成を開始できます。接続先のネットワークの各部分のトポロジをサポートするために、ファイアウォールの インターフェイス を構成します。レイヤー3のインターフェイスを構成してゾーンに割り当てるには、次の流れに従います。異なるタイプのインターフェイス展開を使用してファイアウォールを統合する方法の詳細については(たとえば、 仮想ワイヤ インターフェイス または レイヤ 2 インターフェイス)、PAN-OS ネットワーク管理者のガイドを参照してください。

ファイアウォールは、*Ethernet 1/1* ポートと *Ethernet 1/*（および対応するデフォルトのセキュリティ ポリシーと仮想ルーター）の間のデフォルトのバーチャル ワイヤー インターフェイスが事前設定されて出荷されます。このデフォルトのバーチャル ワイヤーを使用する予定がない場合は、定義する他の設定と干渉しないようにするため、手動でこの設定を削除し、変更をコミットしてから設定を続行する必要があります。デフォルトのバーチャル ワイヤーとその関連セキュリティ ポリシーおよびゾーンを削除する方法の詳細は、外部サービスへのネットワーク アクセスのセットアップの手順 *3* を参照してください。

STEP 1 | インターネット ルーターへのデフォルト ルートを設定します。

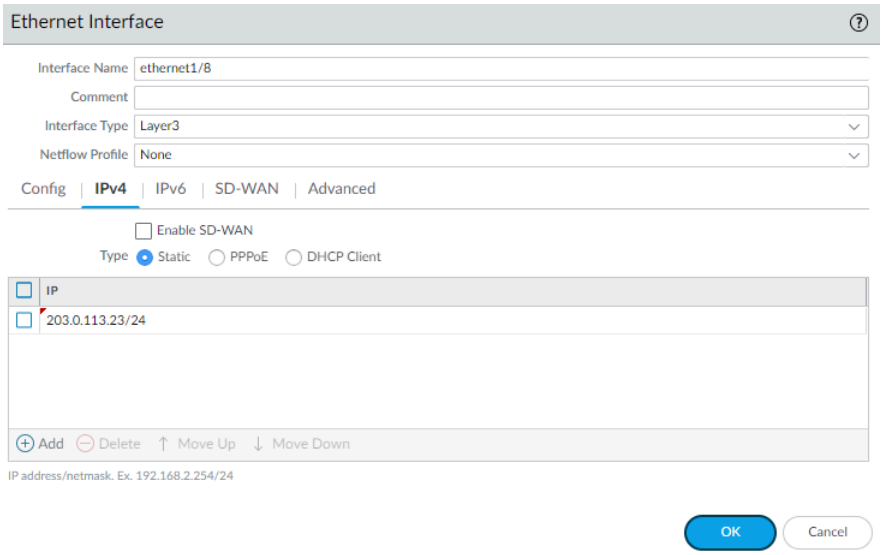
1. **Network (ネットワーク)** > **Virtual Router (仮想ルーター)** の順に選択し、**default (デフォルト)** リンクを選択して Virtual Router (仮想ルーター) ダイアログを開きます。
2. **Static Routes**[スタティック ルート] タブを選択して **Add**[追加] をクリックします。**Name** [名前]フィールドにルート名を入力し、**Destination** [宛先]フィールドにルートの宛先（例: 0.0.0.0/0）を入力します。
3. **Next Hop** [ネクスト ホップ]で **IP Address** [IP アドレス]ラジオ ボタンをクリックし、インターネット ゲートウェイの IP アドレスとネットマスク（例: 203.0.113.1）を入力します。



4. **OK** を 2 回クリックして仮想ルーターの設定を保存します。

STEP 2 | 外部インターフェイス (インターネットに接続するインターフェイス) を設定します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、設定するインターフェイスを選択します。この例では、Ethernet1/8 を外部インターフェースとして設定します。
2. **Interface Type**（インターフェイス タイプ）を選択します。ここで選択するタイプはインターフェイスのトポロジーに応じて異なりますが、この例では、**Layer3** [レイヤー 3]の場合の手順を示します。
3. **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウンから **New Zone**（新規ゾーン）を選択します。Zone [ゾーン] ダイアログの **Name**[名前] で「Internet」などの名前を付けて新しいゾーンを定義し、**OK** をクリックします。
4. **Virtual Router**（仮想ルーター）ドロップダウン リストで、**defaul**（デフォルト）を選択します。
5. IP アドレスをインターフェイスに割り当てるには、**IPv4** タブを選択してから IP セクションで **Add**（追加）をクリックし、インターフェイスに割り当てる IP アドレスとネットマスク（例: 203.0.113.23/24）を入力します。



6. インターフェイスの ping を有効にするには、**Advanced (詳細)** > **Other Info (その他の情報)** の順に選択し、**Management Profile (管理プロファイル)** ドロップダウンリストを展開して、**New Management Profile (新規管理プロファイル)** を選択します。**Name**[名前] フィールドにプロファイル名を入力し、**Ping** を選択してから **OK** をクリックします。
7. インターフェイス設定を保存するには、**OK** をクリックします。

STEP 3 | 内部ネットワークに接続するインターフェイスを設定します。

この例のインターフェイスは、プライベート *IP* アドレスを使用するネットワーク セグメントに接続します。プライベート *IP* アドレスは外部にルーティングできないため、NAT を設定する必要があります。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、設定するインターフェイスを選択します。この例では、ユーザーの接続先となる内部インターフェイスとしてEthernet1/15 を設定します。
2. **Interface Type**[インターフェイス タイプ] として **Layer3**[レイヤー3] を選択します。
3. **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。Zone [ゾーン] ダイアログの **Name**[名前] で「Users」などの名前を付けて新しいゾーンを定義し、**OK** をクリックします。
4. 以前に使用したのと同じ Virtual Router (仮想ルーター) を選択します。この例では default です。
5. IP アドレスをインターフェイスに割り当てるには、**IPv4** タブを選択してから IP セクションで **Add**（追加）をクリックし、インターフェイスに割り当てる IP アドレスとネットマスク（例: 10.16.0.0/22）を入力します。
6. インターフェイスの ping を有効にするには、先ほど作成した管理プロファイルを選択します。
7. インターフェイス設定を保存するには、**OK** をクリックします。

STEP 4 | データセンター アプリケーションに接続するインターフェイスを設定します。

機密性の高いアプリケーションやデータへの不正アクセスを防ぎ、マルウェアがデータセンター内を水平方向に移動する危険性を無くすために、きめ細かいゾーンを定義してください。

1. 設定するインターフェイスを選択します。
2. **Interface Type (インターフェイス タイプ)**ドロップダウン リストから **Layer3 (レイヤー3)**を選択します。この例では、データセンター アプリケーションへのアクセスを可能にするインターフェイスとして、Ethernet1/1を設定しています。
3. **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して **New Zone**（新規ゾーン）を選択します。Zone [ゾーン] ダイアログの

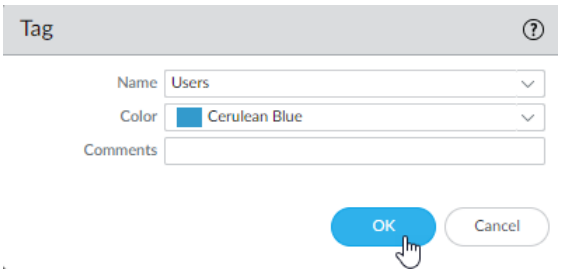
Name[名前] で「Data Center Applications」などの名前を付けて新しいゾーンを定義し、**OK** をクリックします。

4. 以前に使用したのと同じ Virtual Router (仮想ルーター) を選択します。この例では default です。
5. IP アドレスをインターフェイスに割り当てるには、**IPv4** タブを選択してから IP セクションで **Add**（追加）をクリックし、インターフェイスに割り当てる IP アドレスとネットマスク（例: 10.16.0.0/22）を入力します。
6. インターフェイスの ping を有効にするには、作成した管理プロファイルを選択します。
7. インターフェイス設定を保存するには、**OK** をクリックします。

STEP 5 | （任意）各ゾーンのタグを作成します。

タグがあれば、各ポリシールールを目視で識別しやすくなります。

1. **Objects (オブジェクト)** > **Tags (タグ)** を選択して **Add (追加)** します。
2. ゾーンの **Name**[名前] を選択します。
3. タグの**Color**[色]を選択して**OK**をクリックします。



STEP 6 | インターフェイスの設定を保存します。

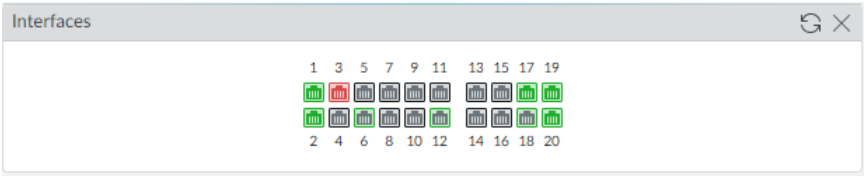
Commit（コミット）をクリックします。

STEP 7 | ファイアウォールを配線します。

ストレート ケーブルを使用して、設定したインターフェイスから対応するスイッチまたはルーターにネットワーク セグメントごとに接続します。

STEP 8 | インターフェイスがアクティブであることを確認します。

Dashboard[ダッシュボード]を選択し、構成したインターフェイスがInterfaces [インターフェイス]ウィジェットに緑色で表示されていることを確認します。



基本的なセキュリティ ポリシーのセットアップ

すでにいくつかのゾーンを作成して各インターフェイスに割り当てているため、セキュリティ ポリシーを作成することができます。セキュリティポリシー ルールによって許可されていない限り、ファイアウォールはトラフィックがゾーン間を流れることを許可しません。パケットがファイアウォールのインターフェイスに到達すると、ファイアウォールはパケットの属性をセキュリティポリシー ルールと照らし合わせ、発信元および宛先のセキュリティ ゾーン、発信元および宛先の IP アドレス、アプリケーション、ユーザー、サービスなどの属性に基づいてセッションをブロックするか許可するかを決定します。ファイアウォールは、インバウンド トラフィックをセキュリティポリシーのルールベースと (左から右へ、上から下へ) 照らし合わせて評価し、最初にマッチしたセキュリティルールで指定されているアクション (例：パケットを許可、拒否、あるいはドロップ) を実行します。つまり、セキュリティポリシーのルールベースにある各ルールは、より具体性の高いルールが上位に、より一般的なルールが下位になるよう並べて配置し、期待している通りのポリシーをファイアウォールが確実に適用するようにしなければなりません。

セキュリティポリシー ルールはパケットを許可しますが、これはトラフィックが脅威とは無関係であるということを意味しません。ファイアウォール が セキュリティ ポリシールールに基づいて許可したトラフィックをスキャンできるようにするには、各ルールにセキュリティ プロファイル (URL フィルタリング、アンチウイルス、アンチスパイウェア、ファイル ブロッキング、WildFire 分析など) もアタッチする必要があります (使用できるプロファイルは、購入したサブスクリプションによって異なります)。基本的なセキュリティポリシーを作成する際、事前定義済みのセキュリティ プロファイルを使用し、ネットワークへの侵入を許可するトラフィックの脅威が必ずスキャンされるようにします。必要に応じて、これらのプロファイルを環境に合わせて後からカスタマイズすることができます。

次の流れに従い、ネットワーク インフラストラクチャ、データセンター アプリケーション、およびインターネットへのアクセスを可能にする、基本的なセキュリティポリシーをセットアップします。これによりファイアウォールを正しく構成できていることを確認するために、ファイアウォールを起動・運転させることができます。ただし、この初期ポリシーは、ネットワークを十分保護することはできません。ファイアウォールの構成が正しく完了していることを確認し、ファイアウォールをネットワークに統合した後、最良のインターネット ゲートウェイのセキュリティポリシーの作成に進み、攻撃からネットワークを保護しつつアプリケーションのアクセスを安全に行えるようにするを作成する方法をご確認ください。

STEP 1 | （任意）デフォルトのセキュリティポリシー ルールを削除します。

デフォルトでは、「*rule1*」という名前のセキュリティ ルールがファイアウォールに含まれています。このルールでは、Trust ゾーンから Untrust ゾーンへのトラフィックがすべて許可されています。このルールを削除する、またはゾーンの命名規則を反映するようにルールを変更することもできます。

STEP 2 | ネットワーク インフラストラクチャのリソースへのアクセスを許可します。

1. **Policies**（ポリシー） > **Security**（セキュリティ） を選択してルールをクリックしますdd
2. **General**（全般）タブで、ルールの分かりやすい **Name**（名前）を入力します。
3. **Source (**送信元**)** タブで **Source Zone (**送信元ゾーン**)** を **Users (**ユーザー**)** に設定します。
4. **Destination (**宛先**)** タブで **Destination Zone (**宛先ゾーン**)** を **IT Infrastructure (IT** インフラストラクチャ**)** に設定します。

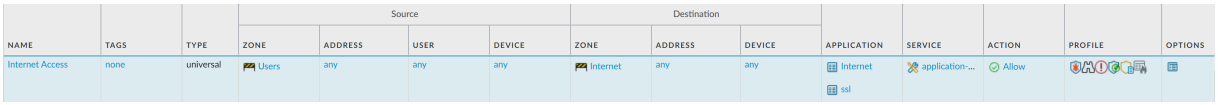
   Destination Address (宛先アドレス***)*** でアドレスオブジェクトを使用し、特定のサーバーあるいはサーバーのグループへのアクセスのみを許可してください。これは、頻繁に攻撃の対象となる *DNS* や *SMTP* といったサービスの場合は特に推奨される設定です。特定の宛先サーバーのアドレスにユーザーを制限することで、データの盗難を防止し、*DNS* トンネリングといった手法を用いてコマンド トラフィックやコントロール トラフィックが接続を確立するのを防ぐことができます。
5. 安全に有効化したいネットワークサービスの各アプリケーションを**Applications**[アプリケーション]タブで**Add**[追加]します。例えば、**dns**、**ntp**、**ocsp**、**ping**、および **smtp** を選択します。
6. **Service/URL Category**[サービス/URL カテゴリ] タブにある**Service**[サービス] は **application-default** のままにします。
7. **Actions** （アクション）タブで、**Action Setting**（アクション設定）を**Allow**（許可）に設定します。
8. **Profile Type (**プロファイル タイプ**)** を **Profiles (**プロファイル**)** に設定し、ポリシールールに付与する次のセキュリティ プロファイルを選択します。
   - **Antivirus (**アンチウイルス**)**については **default (**デフォルト**)**を選択します。
   - **Vulnerability Protection (**脆弱性保護**)**については **strict (**厳密**)**を選択します。
   - **Anti-Spyware (**アンチスパイウェア**)**については **strict (**厳密**)**を選択します。
   - **URL Filtering (URL** フィルタリング**)**については **default (**デフォルト**)**を選択します。
   - **File Blocking (**ファイル ブロッキング**)**については、**basic file blocking (**ベーシックなファイル ブロッキング**)**を選択します。
   - **WildFire Analysis (WildFire** 分析**)**については **default (**デフォルト**)**を選択します。
9. **Log at Session End**[セッション終了時にログを記録]が有効になっていることを確認します。セキュリティポリシー ルールと一致するトラフィックのみがログに記録されます。
10. **OK** をクリックします。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Network Infrastructu...	none	universal	Users	any	any	any	IT Infrastruct...	any	any	dns ntp ocsp ping smtp	application-...	Allow		

STEP 3 | 一般的なインターネットアプリケーションへのアクセスを有効にします。

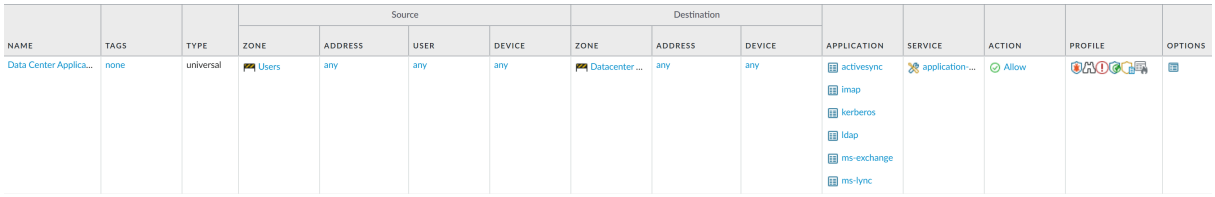
これは、ネットワーク上のトラフィックについての情報を収集できるようにする一時的なルールです。組織内のユーザーがアクセスすべきアプリケーションが明確になったら、許可するアプリケーションを吟味し、各ユーザーグループ用の、さらに細かなアプリケーションベースのルールを作成することができます。

1. **Policies (ポリシー)** > **Security (セキュリティ)** の順に選択し、ルールを **Add (追加)** します。
2. **General**（全般）タブで、ルールの分かりやすい **Name**（名前）を入力します。
3. **Source (送信元)** タブで **Source Zone (送信元ゾーン)** を **Users (ユーザー)** に設定します。
4. **Destination (宛先)** タブで **Destination Zone (宛先ゾーン)** を **Internet (インターネット)** に設定します。
5. **Applications (アプリケーション)** タブで **Application Filter (アプリケーション フィルタ)** を **Add (追加)** し、**Name (名前)** を入力します。正当なウェブベースのアプリケーションを安全に有効化するには、アプリケーションフィルタ内の **Category (カテゴリ)** を **general-internet (インターネット全般)** に設定し、**OK** をクリックします。暗号化されたサイトへのアクセスを有効にするには、**ssl**アプリケーションを**Add**[追加]します。
6. **Service/URL Category**[サービス/URL カテゴリ] タブにある**Service**[サービス] は **application-default** のままにします。
7. **Actions** （アクション）タブで、**Action Setting**（アクション設定）を**Allow**（許可）に設定します。
8. **Profile Type (プロファイル タイプ)** を **Profiles (プロファイル)** に設定し、ポリシールールに付与する次のセキュリティ プロファイルを選択します。
   - **Antivirus (アンチウイルス)**については **default (デフォルト)**を選択します。
   - **Vulnerability Protection (脆弱性保護)**については **strict (厳密)**を選択します。
   - **Anti-Spyware (アンチスパイウェア)**については **strict (厳密)**を選択します。
   - **URL Filtering (URL フィルタリング)**については **default (デフォルト)**を選択します。
   - **File Blocking (ファイル ブロッキング)**については **strict file blocking (厳密なファイル ブロッキング)**を選択します。
   - **WildFire Analysis (WildFire 分析)**については **default (デフォルト)**を選択します。
9. **Log at Session End**[セッション終了時にログを記録]が有効になっていることを確認します。セキュリティ ルールと一致するトラフィックのみがログに記録されます。
10. **OK** をクリックします。



STEP 4 | データセンター アプリケーションへのアクセスを有効にします。

1. **Policies (ポリシー)** > **Security (セキュリティ)** の順に選択し、ルールを **Add (追加)** します。
2. **General (全般)** タブで、ルールの分かりやすい **Name (名前)** を入力します。
3. **Source (送信元)** タブで **Source Zone (送信元ゾーン)** を **Users (ユーザー)** に設定します。
4. **Destination (宛先)** タブで **Destination Zone (宛先ゾーン)** を **Data Center Applications (データセンター アプリケーション)** に設定します。
5. 安全に有効化したいネットワークサービスの各アプリケーションを**Applications**[アプリケーション]タブで**Add**[追加]します。例えば、**activesync**、**imap**、**kerberos**、**ldap**、**ms-exchange**、および**ms-lync**を選択します。
6. **Service/URL Category**[サービス/URL カテゴリ] タブにある**Service**[サービス] は **application-default** のままにします。
7. **Actions** （アクション）タブで、**Action Setting**（アクション設定）を**Allow**（許可）に設定します。
8. **Profile Type (プロファイル タイプ)** を **Profiles (プロファイル)** に設定し、ポリシールールに付与する次のセキュリティ プロファイルを選択します。
   - **Antivirus (アンチウイルス)**については **default (デフォルト)**を選択します。
   - **Vulnerability Protection (脆弱性保護)** については **strict (厳密)** を選択します。
   - **Anti-Spyware (アンチスパイウェア)** については **strict (厳密)** を選択します。
   - **URL Filtering (URL フィルタリング)** については **default (デフォルト)** を選択します。
   - **File Blocking (ファイル ブロッキング)** については **basic file blocking (ベーシックなファイル ブロッキング)** を選択します。
   - **WildFire Analysis (WildFire 分析)** については **default (デフォルト)** を選択します。
9. **Log at Session End**[セッション終了時にログを記録]が有効になっていることを確認します。セキュリティ ルールと一致するトラフィックのみがログに記録されます。
10. **OK** をクリックします。



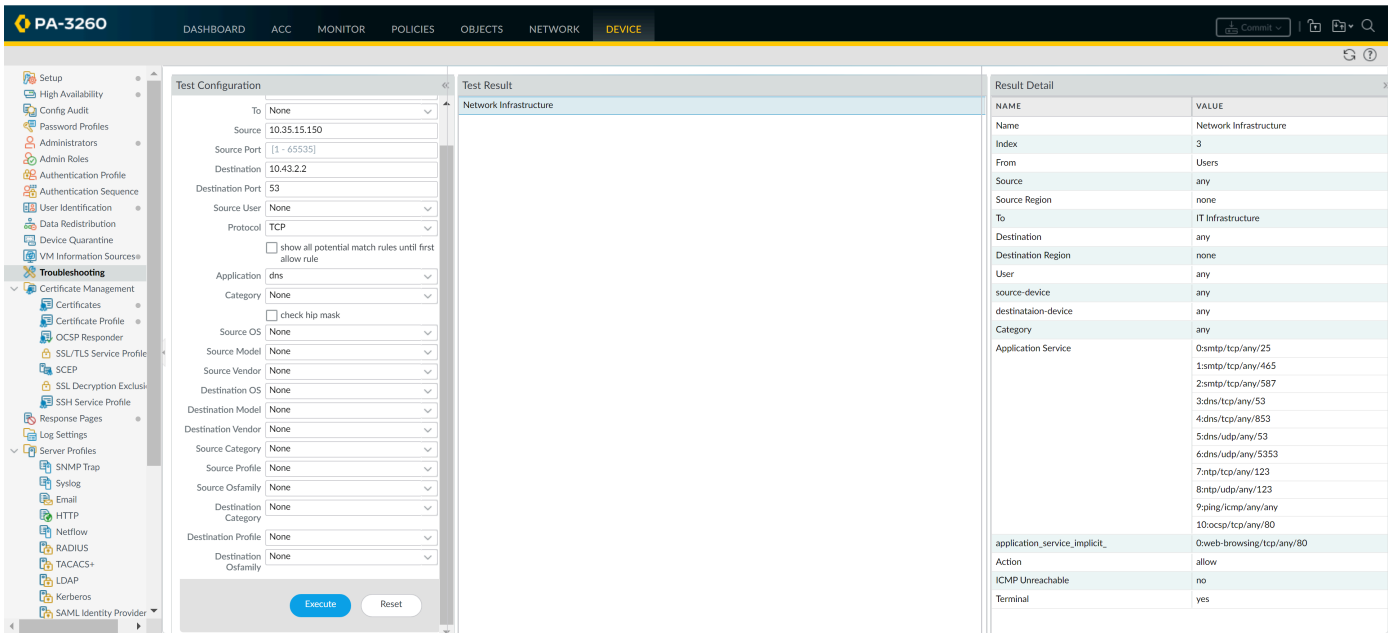
STEP 5 | ファイアウォールで現在アクティブな設定に対するポリシールールを保存します。

Commit（コミット）をクリックします。

STEP 6 | 基本ポリシーを効果的に設定できていることを確認するために、セキュリティポリシー ルールが評価されているかどうかテストし、どのセキュリティポリシー ルールがトラフィック フローに適用されているかを判断します。

例えば、DNSクエリをデータセンター内のDNSサーバーに送信する際、IPアドレスが10.35.14.150のユーザーゾーンにあるクライアントに適用されるポリシールールを検証する場合：

1. **Device** > **Troubleshooting** (デバイストラブルシューティング) を選択し、**Security Policy Match** (セキュリティポリシーマッチ)(**Select Test** (テストの選択)) を選択します。
2. **Source** (送信元) および **Destination** (宛先) IP アドレスを入力します。
3. **Protocol** (プロトコル) を入力します。
4. **dns** (**Application** (アプリケーション)) を選択します。
5. セキュリティ ポリシー マッチテストを **Execute** (実行) します。



ネットワーク トラフィックの評価

基本のセキュリティ ポリシーはこれで完了です。次に、アプリケーション コマンド センター（ACC）の統計およびデータ、トラフィック ログ、および脅威ログをレビューしてネットワークの傾向を観察します。この情報を利用し、より詳細なセキュリティポリシー ルールを作成する必要のある場所を特定します。

アプリケーション コマンド センターの使用と 自動相関エンジンの使用を行います。

ACC で使用頻度が最も高いアプリケーションと、リスクの高いネットワーク アプリケーションをレビューします。ACC では、ログ情報をグラフィカルに要約され、ネットワークを通過するアプリケーションと、それらを使用する (User-ID が有効な) ユーザー、およびコンテンツの潜在的なセキュリティへの影響が強調表示されるため、ネットワークの状況をリアルタイムに識別できます。この情報を利用して、不要なアプリケーションをブロックしながら、安全にアプリケーションを許可し有効にする適切なセキュリティ ポリシー ルールを作成できます。

ACC > **Threat Activity**（脅威アクティビティ）ウィジットには、ネットワーク上で侵入された可能性があるホスト、ログ、およびイベントを裏付ける一致の根拠が表示されます。

ネットワーク セキュリティ ポリシー ルールのどの部分を更新/修正し、変更を適用する必要があるかを判断します。

以下に例を示します。

- スケジュール、ユーザー、またはグループに基づいて、Webコンテンツを許可するかどうかを評価します。
- 特定のアプリケーションまたはアプリケーション内の機能を許可または制御します。
- コンテンツを復号化して検査します。
- 脅威や悪用をスキャンしてからコンテンツを許可します。

セキュリティポリシーの調整とカスタムセキュリティプロファイルの関連付けについてはセキュリティ ポリシー ルールの作成方法と セキュリティ プロファイルを参照してください。

「ログの表示」を行います。

特に、トラフィックおよび脅威のログを表示します（**Monitor**（監視） > **Logs**（ログ））

トラフィックのログは、セキュリティ ポリシーの定義およびログ トラフィックの設定の方法により異なります。ただし ***ACC*** の *Application Usage [アプリケーション使用率]*ウィジットでは、ポリシーの設定に関係なくアプリケーションおよび統計情報が記録されます。つまり、ネットワークで許可されているすべてのトラフィックが表示されるため、ポリシーで許可されているゾーン間トラフィックと、暗黙のうちに許可されているゾーン内トラフィックの両方が含まれています。

ログ ストレージの割り当てと有効期間の設定を行います。

AutoFocusインテリジェンス サマリーでログのアーチファクトを確認します。アーチファクトとは、ログに記録されたファイアウォール上のイベントに関連するアイテム、プロパティ、アクティビティ、あるいは挙動のことです。インテリジェンス サマリーにより、WildFireがアーチファクトを検知したサンプル数、セッション数が明らかになります。WildFire判定の情報（安全、グレイウェア、マルウェア）およびAutoFocusのマッチタグを使用して、ネットワーク内の潜在的なリスクを探します。

Unit 42（*Palo Alto Networks*の脅威インテリジェンスチーム）が作成した*AutoFocus*タグは、お客様のネットワーク内の脅威や、的を絞った最新のキャンペーンについての重要な情報を提供します。

AutoFocusインテリジェンス サマリーからAutoFocus検索を開始してアーチファクトを探し、グローバル、産業、およびネットワークレベルでそれがどの程度蔓延しているのか評価することができます。

ネットワーク ユーザーの Web アクティビティのモニターを行います。

URL フィルタリング ログをレビューして、アラートおよび拒否されたカテゴリ/URL をスキャンします。URL ログは、アラート、続行、オーバーライド、またはブロックといったアクションに関連付られている URL フィルタリング プロファイルを含むセキュリティ ルールにトラフィックが一致する場合に生成されます。

無料の WildFire 転送の有効化

WildFire は、未知のサンプル（ファイルやメール内リンク）を分析・実行し、サンプルが有害、フィッシング、グレイウェア、あるいは安全であるという判定を下すクラウドベースの仮想環境です。WildFireが有効な場合、Palo Alto Networksのファイアウォールは未知のサンプルを分析のためにWildFireに転送することができます。新種のマルウェアが見つかった場合、WildFire はそのマルウェアを検知するためのシグネチャを生成します。このシグネチャは、アクティブなWildFireサブスクリプションを有するすべてのファイアウォールで、リアルタイムに取得できるようになっています。これにより、いずれかのファイアウォールが発見したマルウェアを、すべての Palo Alto Networks の次世代のファイアウォールが検知・防御できるようになります。マルウェアのシグネチャは同じマルウェアの系統に属す複数の亜種にマッチすることも多いため、ファイアウォールがこれまでに出会ったことがない新しいマルウェアの亜種をブロックするようにします。Palo Alto Networks の脅威リサーチ チームはマルウェアの亜種から収集した脅威インテリジェンスを使用して、悪意のある IP アドレス、ドメイン、URL をブロックします。

Palo Alto Networksの次世代ファイアウォールには基本的なWildFireサービスが含まれているため、WildFireのサブスクリプションは必須ではありません。基本的なWildFireサービスを使用すれば、ファイアウォールがPEファイルを転送できるようになります。さらに、WildFireサブスクリプションをお持ちでなく、脅威防止サブスクリプションをお持ちの場合は、WildFireが特定したマルウェアのシグネチャを24～48時間ごとに受信できます（アンチウイルス アップデートの一部として）。

基本的なWildFireサービスでは利用できない次のようなWildFireの高度な機能を使用するには、WildFireサブスクリプションが必要になります。

- 最新の WildFire シグネチャをリアルタイムで取得します。
- 悪意のある PE (ポータブル実行可能ファイル)、ELF および MS Office ファイル、PowerShell およびシェル スクリプトが、WildFire インライン MLを使用してリアルタイムでネットワークに侵入するのを防ぎます。
- 最新のファイルタイプやメールリンクを分析のために転送します。
- WildFire API を使用します。
- WildFire アプライアンスを使用し、WildFire プライベート クラウドあるいは WildFire ハイブリッド クラウドをホストします。

WildFireサブスクリプションをお持ちの場合、先に進んでWildFire はじめにを用いてサブスクリプションを有効活用してください。あるいは、次の流れに従って基本的なWildFire転送を有効化してください。

STEP 1 | デファイアウォールが登録されており、有効なサポート アカウントと必要なサブスクリプションを保有していることを確認します。

1. Palo Alto Networks カスタマーサポート ポータル（CSP）にログインし、左側のナビゲーション ペインで**Assets (アセット)** > **Devices (デバイス)**を選択します。
2. ファイアウォールがリストにあることを確認します。一覧に表示されない場合は**Register New Device (新規デバイスの登録)**を選択し、ファイアウォールの登録に進みます。
3. (Optional)Threat Prevention サブスクリプションをお持ちの場合は、必ずサブスクリプション ライセンスのアクティベーションしてください。

STEP 2 | ファイアウォールにログインし、WildFire 転送設定を構成します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **WildFire** を選択し、General Settings (一般設定) を編集します。
2. **WildFire Public Cloud (WildFire パブリック クラウド)** フィールドを設定し、ファイルを次の場所にある WildFire グローバル クラウドに転送します。**`wildfire.paloaltonetworks.com`**.

   また、ロケーションや組織の条件に基づき、ファイルをリージョナル クラウドやプライベート クラウドに転送することもできます。
3. ファイアウォールが WildFire 分析のために転送する PE の **File Size Limits (ファイルサイズ制限)** を確認します。ファイアウォールが転送できる PE の **Size Limit (サイズ制限)** を、可能な上限値（10 MB）に設定します。

   WildFire のベストプラクティスとして、*PE* の ***Size Limit (サイズ制限)*** を限界値である *10 MB* に設定します。
4. **OK** をクリックして変更内容を保存します。

STEP 3 | ファイアウォールが分析のためにPEを転送できるようにします。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **WildFire Analysis (WildFire 分析)** を選択し、新しいプロファイル ルールを **Add (追加)** します。
2. 新しいプロファイル ルールに**Name**[名前]を付けます。
3. 転送ルールを **Add (追加)** してその **Name (名前)** を入力します。
4. **File Types (ファイルタイプ)** 列で **pe** ファイルを転送ルールに追加します。
5. PEをWildFireパブリック クラウドに転送するために、**Analysis**[分析]列で**public-cloud**を選択します。
6. **OK** をクリックします。

STEP 4 | 新しいWildFire分析プロファイルを、WildFireが許可するトラフィックに適用します。

1. **Policies (ポリシー)** > **Security (セキュリティ)** を選択し、基本的なセキュリティ ポリシーのセットアップの説明に従って、既存のポリシールールを選択するか、新しいポリシールールを作成します。
2. **Actions** （アクション）を選択し、Profile Settings （プロファイル設定）セクションで**Profile Type**（プロファイルタイプ）を**Profiles**（プロファイル）に設定します。
3. 先ほど作成した **WildFire Analysis (WildFire** 分析**)** プロファイルを選択し、このポリシールールによって許可されるすべてのトラフィックにそのプロファイル ルールを適用します。
4. **OK** をクリックします。

STEP 5 | ファイアウォールが WildFire に復号化された SSL トラフィックを転送することを許可します。

STEP 6 | WildFire のベストプラクティスを読んで実装し、WildFire の検知・保護機能を最大限活用できるようにします。

STEP 7 | 設定の更新を **Commit (コミット)** します。

STEP 8 | ファイアウォールが WildFire パブリック クラウドにPEファイルを転送していることを確認します。

Monitor (監視) > **Logs (ログ)** > **WildFire Submissions (WildFire** 送信**)** を選択し、WildFireがWildFire分析のために正しく送信したPEのログ エントリーを確認します。Verdict（判定）列で、WildFireがPEを有害、グレイウェア、あるいは安全と判断したことが確認できます。（WildFire はフィッシング判定をメールのリンクに割り当てるだけです）Action（アクション）列はファイアウォールが、サンプルを許可またはブロックしているかどうかを示します。Severity (重大度)列は、対象のサンプルが組織に及ぼす脅威の大きさを critical (重要)、high (高)、medium (中)、low (低)、information (通知) という値を使って示します。

STEP 9 | （脅威防止サブスクリプションのみ）脅威防止サブスクリプションをお持ちであり、かつWildFireサブスクリプションをお持ちでない場合でも、24～48時間ごとにWildFireシグネチャのアップデートを受信できます。

1. **Device**（デバイス） > **Dynamic Updates**（動的更新）を選択します。
2. ファイアウォールがアンチウイルス アップデートをダウンロード、インストールするようにスケジュール設定されていることを確認します。

ファイアウォールのデプロイメントのベスト プラクティス

これで、ネットワークにファイアウォールを統合し、基本的なセキュリティ機能を有効化することができました。高度な機能の設定を開始できます。以下に、考慮すべき推奨事項を示します。

- Adminstrative Access Best Practices に従って、管理インターフェイスを適切に保護するようにしてください。
- セキュリティポリシーのルールベースを推奨設定に従って構成し、アプリケーションを安全に有効化し、ネットワークを攻撃から保護します。ベストプラクティス ページに移動し、ファイアウォールのデプロイメントのセキュリティ ポリシーのベストプラクティスを選択します。
- 高可用性 構成 – 高可用性（HA）は、2 つのファイアウォールを 1 つのグループ内に配置して、ネットワーク上の単一障害点を回避するために 2 つのファイアウォールの設定およびセッション テーブルを同期する設定です。ファイアウォール ピア間のハートビート接続では、ピアがダウンした場合シームレスにフェイルオーバーを実行できます。2 つのファイアウォール クラスタを設定すると冗長性が得られるため、ビジネス継続性を確保できます。
- ユーザー識別子（User-ID）の有効化 – User-ID は Palo Alto Networks の次世代のファイアウォールの機能で、個々の IP アドレスの代わりにユーザーとグループに基づいてポリシーを作成し、レポートを実行できます。
- 復号化 の有効化 – Palo Alto Networks ファイアウォールでは、可視化、制御、および詳細なセキュリティのためにトラフィックを復号化および検査する機能を提供します。ファイアウォールで復号化を使用すると、悪意のあるコンテンツのネットワークへの侵入や、機密コンテンツが暗号化されたトラフィックまたはトンネルされたトラフィックとして隠ぺいされ、ネットワーク外に流出することを防止することができます。
- ネットワークをレイヤー 4 およびレイヤー 7 回避から保護するためのベスト プラクティスの指示に従います。
- 脅威インテリジェンスを Palo Alto Networks と共有–ファイアウォールが定期的にアプリケーション、脅威、デバイスの安全状態に関する情報を収集し、Palo Alto Networks に送信することを許可します。テレメトリーには、パッシブ DNS モニタリングを有効化し、実験的なテスト シグネチャがセキュリティポリシールール、ファイアウォール ログ、あるいはファイアウォールのパフォーマンスに影響を及ぼすことなくバックグラウンドで稼働するのを許可するオプションが含まれます。Palo Alto Networks がファイアウォールの脅威防止性能を改善するために使用するテレメトリーから収集されたインテリジェンスは、Palo Alto Networks のすべてのお客様にとって有益なものです。

サブスクリプション

ファイアウォールと連携するすべてのサブスクリプションとサービスについて学び、サブスクリプションライセンスをアクティブにすることから始めます。

- ファイアウォールで使用できるサブスクリプション
- サブスクリプション ライセンスのアクティベーション
- ライセンスの期限が切れるとどうなるか。
- Palo Alto Networks クラウド サービスの高度なアプリケーション ログ

Cortex XDR™ のような特定のクラウドサービスは、ファイアウォールと直接統合するのではなく、ネットワークアクティビティを可視化するために*Cortex Data Lake* に格納されたデータを使用します。拡張アプリケーション ロギングは、*Cortex Data Lake* サブスクリプションに付属する機能です。これにより、ファイアウォールは、*Cortex XDR* が異常なネットワーク アクティビティを検出するために特に使用するデータを収集できます。拡張アプリケーション ロギングをオンにすることは、Cortex XDR のベストプラクティスです。

ファイアウォールで使用できるサブスクリプション

次の Palo Alto Networks サブスクリプションは、特定のファイアウォールの機能をアンロックしたり、ファイアウォールが Palo Alto Networks のクラウド配信型のサービスを活用できるようにしたりするものです (あるいはその両方)。ここでは、ファイアウォールと共に使用するためにサブスクリプションが必要となる各サービスや機能を詳細に説明します。サブスクリプションを有効にするには、まずサブスクリプション ライセンスのアクティベーションする必要があります。アクティブになると、ほとんどのサブスクリプション サービスは Dynamic Content Updates を使用して、firewall に新しい機能や更新された機能を提供できます。

ファイアウォールで使用できるサブスクリプション	
IoTセキュリティ	IoT セキュリティ ソリューションは、次世代ファイアウォールと連携して、ネットワーク上の IoT デバイスのリアルタイム インベントリを動的に検出して維持します。AI と機械学習アルゴリズムにより、IoT セキュリティ ソリューションは、初めて遭遇した IoT デバイスタイプを分類する場合でも、高レベルの精度を実現します。そして、ご利用の IoT デバイス インベントリは常に最新の状態を維持します。IoT セキュリティは、IoT デバイス トラフィックを制御するためのポリシー推奨事項の自動生成、およびファイアウォール ポリシーで使用するための IoT デバイス属性の自動作成も提供します。 • IoT セキュリティを開始する
PAN-OS SD-WAN	PAN-OS ソフトウェアがすでに有する業界最先端のセキュリティに加えて、インテリジェントで動的なパス選択を提供します。Panorama によって管理される PAN-OS SD-WAN の実装には、次のものが含まれます。 • 設定の中央管理 • VPN トポロジの自動作成 • トラフィックの配布 • モニタリングとトラブルシューティング • PAN-OS SD-WAN を使い始める
Threat Prevention（脅威阻止）	脅威防止によって得られるもの： • アンチウイルス、アンチスパイウェア (コマンド アンド コントロール)、脆弱性保護。 • ネットワークを悪意のあるホストから守るために使用できるビルトイン外部動的リスト。 • 悪意のあるドメインに接続しようと試みる感染ホストを特定する機能。

ファイアウォールで使用できるサブスクリプション	
	• 脅威防止を開始する
Advanced Threat Prevention（高度な脅威防御）	Threat Prevention（脅威防御）に含まれるすべての機能に加えて、Advanced Threat Prevention（高度な脅威防御）サブスクリプションは、Palo Alto Networksによって収集された忠実度の高い脅威インテリジェンスでトレーニングされたディープラーニングモデルを活用して、すべてのネットワークトラフィックを検査することによって、回避的で未知のコマンドアンドコントロール(C2)脅威からネットワークを保護する、インラインc1loud-b1ased脅威検出および防止エンジンを提供します。 • Advanced Threat Prevention（高度な脅威防御）を使い始める
DNS セキュリティ	DNS セキュリティにクエリを送信する高度な DNS シンクホール機能、高度な予測分析および機械学習を使用して DNS シグネチャを生成する拡張可能なクラウドベースのサービス機能を提供します。このサービスでは、Palo Alto Networks が作成する、継続的に拡大する DNS ベースの脅威インテリジェンスをすべて利用できます。 DNS セキュリティをセットアップするためには、まずは脅威防止ライセンスを購入してインストールする必要があります。 • DNS セキュリティを開始する
URL フィルタリング	動的 URL カテゴリに基づいて、Web アクセスを制御するだけでなく、ユーザーがオンライン コンテンツとやり取りする方法も制御する機能を提供します。また、ユーザーが企業の認証情報を送信できるサイトを制御することで、認証情報の盗難を防ぐこともできます。 URL フィルタリングをセットアップするためには、サポートされている URL フィルタリング データベースである PAN-DB のサブスクリプションを購入してインストールする必要があります。PAN-DB では、PAN-DB パブリック クラウドまたは PAN-DB プライベート クラウドへのアクセス権限をセットアップできます。 *URL* フィルタリングはスタンドアロン サブスクリプションとして使用できなくなりました。*URL* フィルタリングに含まれるすべての機能は、詳細な *URL* フィルタリング サブスクリプションに含まれています。

ファイアウォールで使用できるサブスクリプション	
	• URL フィルタリングを開始する
高度な **URL** フィルタリング	高度な URL フィルタリングでは、クラウドベースの ML 駆動の Web セキュリティ エンジンを使用して、リアルタイムで Web トラフィックの ML ベースの検査を実行します。これにより、URL データベースと帯域外 Web クロールに依存して、標的型フィッシング、Web 配信マルウェアやエクスプロイト、コマンドアンドコントロール、ソーシャルエンジニアリング、その他の種類の Web 攻撃を含む、ファイルのない高度な Web ベースの攻撃を検出して防止できます。 • 高度な URL フィルタリングの使用を開始する
WildFire	基本 WildFire® サポートは脅威防御ライセンスの一部として含まれていますが、WildFire サブスクリプション サービスでは、直ちに脅威への対応が必要な組織を対象に強化サービスを提供することにより、頻繁な WildFire シグネチャ更新、高度なファイル タイプ転送 (APK、PDF、Microsoft Office、Java アプレット)、および WildFire API を使用したファイルのアップロード機能を有効にすることができます。WildFire サブスクリプションは、ファイアウォールがオンプレミスの WF-500 WildFire アプライアンスにファイルを転送する場合にも必要です。 • WildFireを開始する
オートフォーカス	ファイアウォールのトラフィックログについての分析結果を視覚的に表示します。また、AutoFocus ポータルで脅威インテリジェンスを使用することで、お客様のネットワークの潜在的な危険を特定することができます。アクティブなライセンスがあれば、ファイアウォールに記録されたログに基いてAutoFocus検索を利用することもできます。 • AutoFocus を開始する
Cortex Data Lake	クラウドベースの一元的なログ ストレージおよび集約を提供します。Cortex XDR、IoT セキュリティ、およびPrisma Access クラウドサービス、Traps 管理サービスを含め、他のいくつかのクラウド配信型のサービスをサポートするためにCortex Date Lake が必須、あるいは強く推奨されます。 • Cortex Data Lake の使用
GlobalProtectゲートウェイ	モビリティ ソリューションまたは大規模 VPN 機能を提供します。デフォルトでは、ライセンスなしで GlobalProtect ポータルとゲートウェイ（HIP チェックなし）を導入できます。GlobalProtect の高度な機能 (HIP チェックおよび関連コンテンツの更新、GlobalProtect Mobile App、IPv6 接続、または

ファイアウォールで使用できるサブスクリプション	
	GlobalProtect Clientless VPN) を使用する場合は、ゲートウェイごとに GlobalProtect ゲートウェイ ライセンスが必要です。 • GlobalProtect を開始する
仮想システム	これは永久ライセンスであり、PA-3200 シリーズのファイアウォールで複数の仮想システムのサポートを有効にするために必要です。さらに、PA-5200 Series、PA-5400 Series、および PA-7000 Series ファイアウォール でデフォルトで提供されている基本数を超えて仮想システムの数を増やしたい場合は、仮想システム ライセンスを購入する必要があります (基本数はプラットフォームによって異なります)。PA-220、PA-400 Series、PA-800 Series、PA-3400 Series、VM-Series firewallは仮想システムをサポートしていません。 • 仮想システムを開始する
エンタープライズ データ損失防止 **(DLP)**	不正なアクセス、不正使用、抽出、機密情報の共有に対するクラウドベースの保護を提供します。エンタープライズ DLP は、機械学習ベースのデータ分類、正規表現またはキーワードを使用した数百のデータ パターン、およびブール論理を使用して集合タイプをスキャンするデータプロファイルを使用して、保存中および移動中の機密データを正確に検出し、一貫したポリシーを適用する単一のエンジンを提供します。 • エンタープライズ データ損失防止の開始
SaaS セキュリティ インライン	SaaS セキュリティ ソリューションは Cortex Data Lake と連携して、ネットワーク上で使用されているすべての SaaS アプリケーションを検出します。SaaS セキュリティ インラインでは、何千もの Shadow IT アプリケーションとそのユーザーと使用状況の詳細を検出できます。SaaS セキュリティインラインでは、既存の Palo Alto Networks ファイアウォール全体で SaaS ポリシー ルールの推奨事項もシームレスに適用されます。App-ID クラウド エンジン (ACE) では、SaaS セキュリティ インラインも必要です。 • SaaS Security Inline の使用を開始する

サブスクリプション ライセンスのアクティベーション

これらのステップに従ってファイアウォール上で新しいライセンスをアクティベートします。

復号化ミラー 機能では、機能のロックを解除するために無料ライセンスを有効にする必要があります。これらの機能については、代わりに復号化機能の無料ライセンスをアクティベートの手順に従ってください。

STEP 1 | 購入したライセンスのアクティベーション コードを探します。

サブスクリプションを購入した場合は、各サブスクリプションに関連付けられているアクティベーション コードの一覧を示した電子メールを Palo Alto Networks カスタマー サポートから受信しています。この電子メールが見当たらない場合は、カスタマー サポートに連絡してアクティベーション コードを入手してから次に進んでください。

STEP 2 | サポート ライセンスのアクティベーション

有効なサポート ライセンスをお持ちでない場合、PAN-OSソフトウェアをアップデートすることはできません。

1. Webインターフェイスにログインし、**Device**（デバイス） > **Support**（サポート）を選択します。
2. **Activate support using authorization code**[認証コードを使用してサポートのアクティベーションを行う]をクリックします。
3. **Authorization Code**[認証コード] を入力し、**OK**をクリックします。

STEP 3 | 購入した各ライセンスをアクティベーションします。

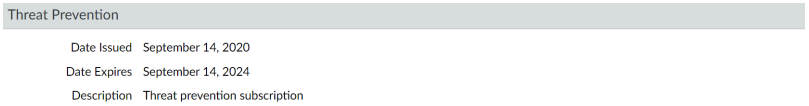
Device（デバイス） > **Licenses**（ライセンス）を選択し、次のいずれかの方法でライセンス/サブスクリプションのアクティベーションを行います：

- **Retrieve license keys from license server**（ライセンス サーバーからライセンス キーを取得） – カスタマー サポート ポータルでライセンスをアクティベートした場合は、このオプションを使用します。
- **Activate feature using authorization code** [認証コードを使用して機能のアクティベーションを行う] – ライセンスの認証コードを使用して購入したサブスクリプションを有効にする場合は、このオプションを使用します。該当の認証コードがサポート ポータルで以前にアクティベーションされていないことが前提になります。**Authorization Code**（認証コード）の入力を促されたら、認証コードを入力して **OK** をクリックします。
- **Manually upload license key**（ライセンス キーの手動アップロード） – ファイアウォールと Palo Alto Networks カスタマー サポート ポータルとのネットワーク接続が確立されていないまたは行えない場合は、このオプションを使用します。この場合は、インターネットに接続されたコンピュータでサポート サイトからライセンス キー ファイルをダウンロードしてから、ファイアウォールにアップロードする必要があります。

カスタマーサポートポータル*API*を使用してアクティベーションを自動化するには、 Activate Licenses のプロセスを参照してください。このプロセスは、ハードウェアと*VM-Series* ファイアウォールの両方で機能します。

STEP 4 | ライセンスが正常にアクティベーションされていることを確認します

Device（デバイス） > **Licenses**（ライセンス）ページで、ライセンスが正常にアクティベートされていることを確認します。たとえば、WildFire ライセンスをアクティベーションした後、ライセンスが有効なことを確認してください。



STEP 5 | （WildFire サブスクリプションのみ）WildFire サブスクリプションのアクティベーションを完了するためのコミットを実行します。

WildFire サブスクリプションのアクティベーションが完了したら、ファイアウォールが高度なファイル タイプの転送を開始するためのコミットが必要です。次のいずれかの作業を行います。

- 保留中の変更をすべてコミットします。
- WildFire 分析プロファイル ルールに、WildFire サブスクリプションで現在サポートされている高度なファイル タイプが含まれていることを確認します。ルールの変更が不要な場合は、ルールの説明を若干編集してコミットを実行します。

ライセンスの期限が切れるとどうなるか。

Palo Alto Networks のサブスクリプションは、ファイアウォールに Palo Alto Networks のクラウド配信サービスへの追加機能やアクセスを提供します。ライセンスが有効期限から 30 日以内になると、サブスクリプションが更新されるか期限切れになるまで、システム ログに警告メッセージが毎日表示されます。ライセンスの有効期限が切れると、一部のサブスクリプションは限られた容量で機能し続け、他のサブスクリプションは完全に動作を停止します。ここでは、各サブスクリプションの有効期限が切れたときに何が起こるかを確認できます。

ライセンスの有効期限の正確な瞬間は、翌日の午前 *12:00 (GMT)* の最初です。たとえば、ライセンスが *1/20* に終了する予定の場合、その日の残りの期間は機能します。*1/21* の午前 *12:00 (GMT)* に新しい日の開始時に、ライセンスの有効期限が切れます。すべてのライセンス関連機能は、ファイアウォール上で設定されたタイムゾーンに関係なく、グリニッジ標準時 *(GMT)* で動作します。

サブスクリプション	期限切れ時の動作
脅威防御	システム ログにアラートが表示され、ライセンスの有効期限が切れていることが示されます。 できること： • 新しいアプリケーションのみのコンテンツ更新を手動または自動スケジュールの一部としてインストールする場合を除き、ライセンスの有効期限が切れたときにインストールされたシグネチャを使用してください。使用する場合、更新によって既存の脅威シグネチャが削除され、それらに対する保護が受けられなくなります。 • カスタム App-ID™ と脅威シグネチャの使用および変更 できないこと： • 新しいシグネチャのインストール • シグネチャを以前のバージョンにロールバック
DNS セキュリティ	できること： • 有効な脅威防御ライセンスがある場合に、ローカル DNS シグネチャの使用 できないこと： • 新しい DNS シグネチャの取得
詳細な URL フィルタリング/URL フィルタリング	できること： • カスタム URL カテゴリを使用したポリシーの適用 できないこと：

サブスクリプション	期限切れ時の動作
	• キャッシュされた PAN-DB カテゴリの更新の取得 • PAN-DB URL フィルタリング データベースに接続します。 • PAN-DB URL カテゴリを取得します。 • 高度な URL フィルタリングを使用して、リアルタイムで URL 要求を分析します。
WildFire	できること： • 分析のための PEファイル の転送 • 有効な脅威防御サブスクリプションをお持ちの場合に、24 ～ 48時間ごとのシグネチャの更新の取得 できないこと： • WildFire のパブリック クラウドとプライベート クラウドを介した 5 分更新の取得 • SMTP および POP3 電子メールメッセージに含まれる APK、Flash ファイル、PDF、Microsoft Office ファイル、Java アプレット、Java ファイル（.jar および .class）、HTTP/HTTPS 電子メールリンクなどの高度なファイルタイプの転送 • WildFire API の使用 • WildFire アプライアンスを使用した、WildFire プライベート クラウドあるいは WildFire ハイブリッド クラウドのホスト
オートフォーカス	できること： • 3 カ月の猶予期間での、AutoFocus データを含む外部ダイナミック リストの使用 できないこと： • AutoFocus ポータルへのアクセス • AutoFocus Intelligence Summary（AutoFocus インテリジェンス サマリー）での、モニター ログまたは ACC アーティファクトの確認
Cortex Data Lake	できること： • 30 日の猶予期間のログ データの保存、およびその後の削除 • 30 日間の猶予期間が終了するまでの、ログの Cortex Data Lake への転送
グローバルプロテクト	できること：

サブスクリプション	期限切れ時の動作
	• Windows および macOS を実行するエンドポイント向けアプリの使用 • 単一または複数の内部/外部ゲートウェイの設定 できないこと： • iOS、Android、Chrome OS、およびWindows 10 UWP 向けの Linux OS アプリおよびモバイルアプリへのアクセス • 外部ゲートウェイ向けの IPv6の使用 • HIP チェックの実行 • クライアントレス VPNの使用 • 宛先ドメイン、クライアント プロセス、ビデオ ストリーミング アプリケーションに基づいて分割トンネリングを実行します。
VM-Series	VM-Series Deployment Guide を参照してください。
サポート	できないこと： • ソフトウェア更新の受信 • VM イメージのダウンロード • テクニカル サポートの利用

Palo Alto Networks クラウド サービスの高度なアプリケーション ログ

ファイアウォールは、Cortex XDRやIoT Securityなど、Palo Alto Networksのアプリやサービスのネットワーク アクティビティの可視性を高めるデータを収集することができます。これらの高度なアプリケーション ログは、Palo Alto Networks アプリケーションおよびサービスでの使用および処理用に厳密に設計されています。ファイアウォールや Panorama で強化されたアプリケーション ログを表示することはできません。ロギングサービスにログを送信するファイアウォールのみが、拡張アプリケーションログを生成できます。

以下の手順に従って、Cortex XDRおよびIoT Securityの拡張アプリケーションログのログ転送を有効にしてください。

- Cortex XDR
- IoTセキュリティ

Cortex XDR

高度なアプリケーション ログが収集するデータの種類には、DNS クエリのレコード、URL にアクセスするために使用される Web ブラウザまたはツールを指定する HTTP ヘッダー ユーザー エージェント フィールド、DHCP 自動 IP アドレス割り当てなどがあります。たとえば、Cortex XDR™ を利用すると、IP アドレスの代わりにホスト名を基準にして異常なアクティビティ発生時にアラートを発信できます。これにより、Cortex XDR を使用しているセキュリティ アナリストは、ユーザーの活動がロールの範囲内にあるかどうかを有意義に評価し、範囲外である場合は、行動を停止するための操作をより迅速に実行できます。

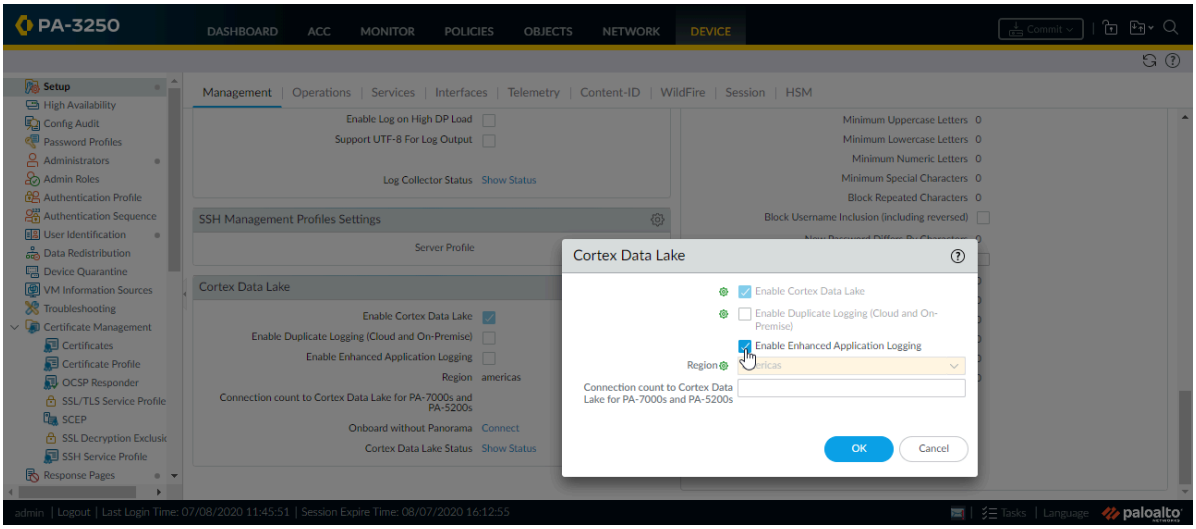
最も包括的な、高度なアプリケーション ログの利点を活用するには、User-ID を有効にする必要があります。Windows ベースの User-ID エージェントと PAN-OS 統合 User-ID エージェントのデプロイメントは、ファイアウォールの User-ID ログに反映されないデータが収集されますが、これはネットワーク アクティビティを特定のユーザーに関連付けるのに役立つます。

高度なアプリケーション ログを Cortex Data Lake に転送するには、高度なアプリケーション ロギングをグローバルに有効にしてから、セキュリティ単位のルールベースで有効にします（ログ転送プロファイルを使用する）。グローバル設定は必須であり、セッションベースではないトラフィック（ARP リクエストなど）のデータを取得します。セキュリティ単位のポリシールールの設定を強く推奨します。高度なアプリケーション ログの大半は、セキュリティ ポリシーの規則が適用するセッション ベースのトラフィックから収集されます。

STEP 1 | 高度なアプリケーション ロギングには Cortex Data Lake サブスクリプションが必要であり、User-ID も推奨されます。「Cortex Data Lake の開始」と「User-ID の有効化」のステップに移ります。

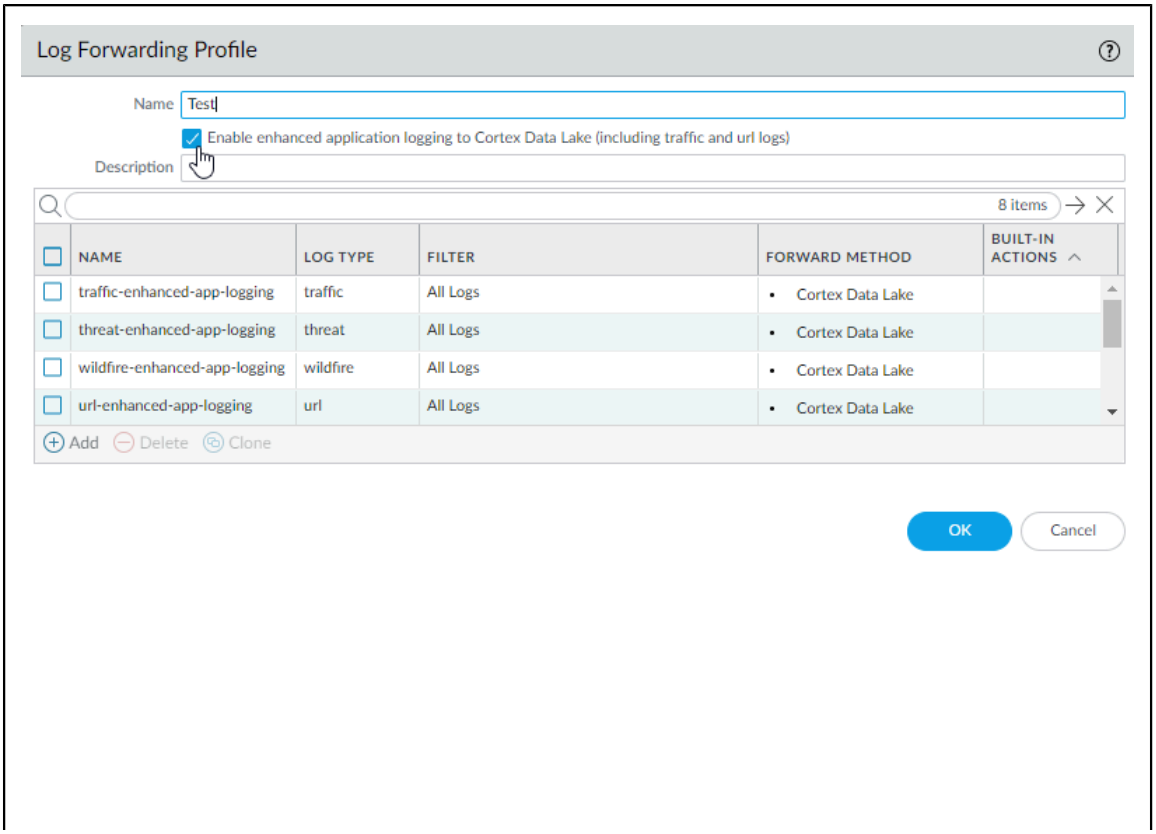
STEP 2 | ファイアウォール上で **Enable Enhanced Application Logging**（高度なアプリケーション ロギングの有効化）を行うには、 **Device**（デバイス） > **Setup**（セットアップ） >

Management（管理） > **Cortex Data Lake**を選択して、 Cortex Data Lake 設定を編集します。



STEP 3 | 拡張された可視性を必要とするトラフィックを制御するセキュリティ ポリシー ルールの高度なアプリケーション ログを引き続き有効にします。

1. **Objects (オブジェクト)** > **Log Forwarding (ログ転送)** を選択して、ログ転送プロファイルを **Add (追加)**するか変更します。
2. プロファイルを更新して、**Cortex Data Lake** への拡張アプリケーション ロギングを有効にします **(トラフィックと URL** ログを含む**)**。



ログ転送プロファイルで高度なアプリケーション ログを有効にすると、高度なアプリケーション ログに必要なログ タイプを指定する一致リストが自動的にプロファイルに追加されます。

3. **OK** をクリックしてプロファイルを保存し、必要な数のプロファイルを更新しぞ鋼します。
4. 更新したログ転送プロファイルがセキュリティ ポリシー ルールにアタッチされていることを確認し、ルールに一致するトラフィックのログ生成および転送をトリガーします。

   1. 各セキュリティ ポリシー ルールにアタッチされるプロファイルを見るには、**Policies**（ポリシー） > **Security**（セキュリティ）を選択します。
   2. ルールにアタッチされているログ転送プロファイルを更新するには、ルールを **Add**（追加）するか編集し、**Policies**（ポリシー） > **Security**（セキュリティ） > **Actions**（操作） > **Log Forwarding**（ログ転送）を選択してから、高度なアプリケーション ロギングで有効なログ転送プロファイルを選択します。

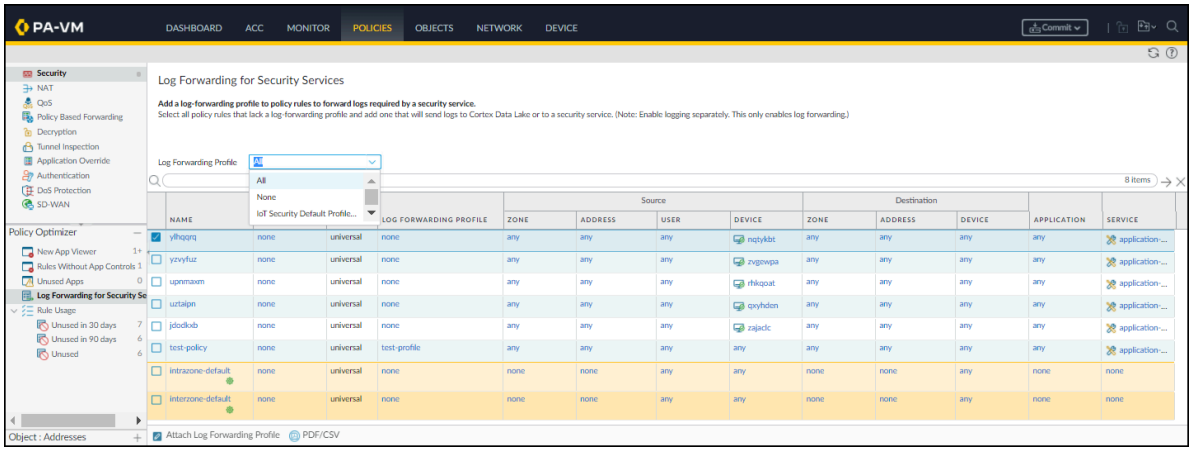
IoTセキュリティ

IoT Security のファイアウォール設定の 1 つには、Log Forwarding プロファイルを作成し、Security ポリシールールに適用することが含まれています。各ルールに個別にプロファイルを適用することもできますが、より簡単な方法は、定義済みのLog Forwarding プロファイルを選択し、まとめて複数のルールにそれを適用することです。次の手順では、定義済みの Log Forwarding プロファイルを Security ポリシー ルールに一括で追加するこの方法について説明します。

このワークフローを使用するには、Security ポリシー ルールを設定し、ルールでログを有効にし、拡張アプリケーションログのログサービスを有効にしておく必要があります。

STEP 1 | IoT Security の Log Forwarding プロファイルを Security ポリシー ルールに適用します。

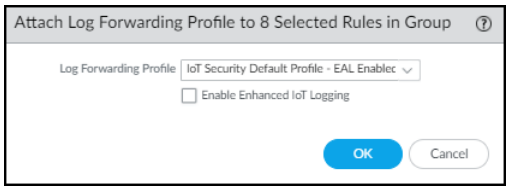
1. 次世代の firewall にログインし、[ポリシー オプティマイザ] セクションで **Policies** > **Log Forwarding for Security Services** を選択します。
2. すべての Security ポリシー ルール (Log Forwarding プロファイルを持つルールとそうでないルールを含む) を表示するには、[Log Forwarding プロファイル] で **All** を選択します。



3. ログをログ サービスに転送するルールを選択します。
4. **Attach log Forwarding Profile** をページ下部に表示します。
5. 既定の Log Forwarding プロファイルをルールに適用するには、**IoT Security Default Profile - EAL Enabled** および **OK** を選択します。

   既定のプロファイルは、拡張アプリケーション ログ (EAL) など、IoT Security に必要なすべてのログの種類を提供するように事前構成されています。

   IoT Security Default Profile で拡張アプリケーション ログ *(EAL)* が既に有効になっているため、***Enable Enhanced IoT Logging*** を行う必要はありません。



もしくは

EAL の転送を、まだ EAL を持たない既存の Log Forwarding プロファイルに追加するには、Log Forwarding Profile リストから EAL を選択し、**Enable Enhanced IoT Logging** を選択し、次に **OK** を選択します。

Enable Enhanced IoT Logging の場合、*PAN-OS* は選択した *Log Forwarding* プロファイル自体を更新し、同じ *Log Forwarding* プロファイルを使用するすべてのルールで拡張ログ転送を有効にします。

PAN-OS は、選択した Log Forwarding プロファイルを、まだプロファイルを持たないルールに追加し、以前に割り当てられたプロファイルをこのプロファイルに置き換えます。

STEP 2 | 変更を **Commit (コミット)** します。

ファイアウォールの管理

管理者は、Web インターフェイス、CLI、および API 管理インターフェイスを使用して、Palo Alto Networks のファイアウォールを設定、管理、およびモニタリングすることができます。特定のタスクまたは許可を特定の管理者に委任するために、管理インターフェイスに対するロールベースの管理アクセス権限をカスタマイズできます。

管理ネットワークとファイアウォール および Panorama 管理インターフェイスを保護する方法については、管理アクセスのベストプラクティス を参照してください。

- 管理インターフェイス
- Web インターフェイスの使用
- 設定バックアップ ファイルの管理
- ファイアウォール管理者の管理
- リファレンス：Web インターフェイス管理者のアクセス権限
- リファレンス：ポート番号の扱い
- ファイアウォールの工場出荷時設定へのリセット
- ファイアウォールのブート処理

管理インターフェイス

次のユーザーインターフェイスを使用すれば、Palo Alto Networks のファイアウォールを管理することができます。

インターネットからまたは企業のセキュリティ境界内の他の信頼されていないゾーンから、管理へのアクセスを有効にしないでください。管理者アクセスのベストプラクティス に従って、ファイアウォール を適切に保護していることを確認します。

- Web インターフェイスを使用すれば、設定を行って比較的容易にタスクを監視できます。このグラフィカル インターフェイスでは、HTTPS（推奨）あるいは HTTP を使用してファイアウォールにアクセスできます。これは、管理タスクを実行するための最適な方法です。
- コマンドラインインターフェイス（CLI）を使用すれば、SSH（推奨）、Telnet、あるいはコンソール ポートを介して次々とコマンドを入力していくことで、一連のタスクを実行できます。CLI は、2 つのコマンド モード（操作モードおよび設定モード）をサポートする必要最小限の機能を備えたインターフェイスで、それぞれにコマンドとステートメントの独自の階層があります。コマンドのネスト構造と構文に慣れると、CLI による応答時間が短縮され、効率良く管理を行えます。
- XML APIを使用して、内部的に開発された既存のアプリケーションやリポジトリの操作および統合を合理化します。XML API は、HTTP/HTTPS リクエストおよびレスポンスを使用して実装される Web サービスです。
- Panorama を使用し、ウェブベースで管理、レポート、および複数のファイアウォールのログ収集を行います。Panorama Web インターフェイスはファイアウォールの Web インターフェイスと似ていますが、一元管理を行える追加の機能があります。

Web インターフェイスの使用

以下のトピックでは、ファイアウォールの Web インターフェイスを使用する方法について説明します。Web インターフェイスの具体的なタブおよびフィールドの詳細は、Web インターフェイス リファレンス ガイドを参照してください。

- Web インターフェイスの起動
- バナー、本日のメッセージ、ロゴの設定
- 管理者ログインアクティビティ インジケーターを使用してアカウントの不正利用を検知
- 管理タスクの管理・監視
- ファイアウォールの設定変更をコミット、検証、プレビュー
- 選択的な構成変更のコミット
- 設定バンドル データのエクスポート
- グローバル検索を使用してファイアウォールあるいはPanoramaの管理サーバーを検索
- 設定変更を制限するためのロックの管理

Web インターフェイスの起動

Web インターフェイスにアクセスできるよう、以下の Web ブラウザがサポートされています。

- Internet Explorer 11+
- Firefox 3.6+
- Safari 5+
- Chrome 11+

次の各作業を行い、Web インターフェイスを立ち上げます。

STEP 1 | インターネットブラウザを起動し、URLフィールドにファイアウォールのIPアドレスを入力します(https://<IP address>)。

*Web*インターフェイスへのアクセスについて、管理（*MGT*）インターフェイスはデフォルト設定では*HTTPS*アクセスのみを許可するようになっています。他のプロトコルを有効にする場合は、***Device** (デバイス) > **Setup** (セットアップ) > **Interfaces** (インターフェイス)* を選択して ***Management** (管理)* インターフェイスを編集します。

STEP 2 | アカウントで使用する認証タイプに応じた方法で、ファイアウォールにログインします。ファイアウォールに初めてログインする場合は、ユーザー名およびパスワードでデフォルト値 **admin** を使用します。

- **SAML** – **Use Single Sign-On**（シングル サインオンの使用）をクリックします（シングル サインオン: SSO）。ファイアウォールが管理者の認証（ロールの割り当て）を行う場合は、**Username** (ユーザー名) を入力して **Continue** (続行) します。SAML アイデンティティ プロバイダ（IdP）が認証を行う場合、**Username** (ユーザー名) を入力せずに **Continue** (続行) します。どちらの場合でも、ファイアウォールによって IdP にリダイレクトされ、そ

こでユーザー名およびパスワードを入力するよう求められます。IdP への認証を行うと、ファイアウォールの Web インターフェイスが表示されます。

- 他のタイプの認証 – ユーザーの **Name**（名前）と **Password**（パスワード）を入力します。ログイン ページにバナーとチェック ボックスがある場合は、ログイン バナーを読み、**I Accept and Acknowledge the Statement Below**（次の内容に同意・承認します）を選択します。次に、**Login**（ログイン）をクリックします。

STEP 3 | 本日のメッセージを読み、**Close**[閉じる]をクリックします。

バナー、本日のメッセージ、ロゴの設定

ログインバナーとは、ログインページに追加することで管理者がログイン前に確認する必要がある情報を表示できる任意のテキストのことです。例えば、ファイアウォールの制限や許可されていない使用についてユーザーに通知するメッセージを加えたりすることができます。

ファイアウォール管理用の分類レベルといった重要な情報を管理者が見逃さないよう、Webインターフェイスの上部（ヘッダーバナー）および下部（フッターバナー）に、テキストがハイライト表示された色付きの帯を追加することができます。

ログイン後、 本日のメッセージダイアログが自動的に表示されます。このダイアログには、ソフトウェアやコンテンツリリースに関するPalo Alto Networksからの重要な情報を通知するメッセージが表示されます。また、管理者の業務に影響を与える可能性があるシステム再起動の実施といった情報を確実に管理者に通知できるよう、カスタムメッセージを1つ加える事もできます。

Webインターフェイスのログインページおよびヘッダーに表示されるデフォルトのロゴは、お客様の組織のロゴに変更することができます。

STEP 1 | ログインバナーを設定します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して General Settings (一般設定) を編集します。
2. **Login Banner**[ログインバナー]（最大3,200文字）を入力します。
3. （任意）管理者がバナーテキストの上にある**I Accept and Acknowledge the Statement Below**[次の内容に同意・承認します]のチェックボックスを選択しなければ**Login**[ログイン]ボタンが有効化しないようにするには、**Force Admins to Acknowledge Login Banner**[管理者にログインバナーの確認を求める]を選択します。
4. **OK** をクリックします。

STEP 2 | 本日のメッセージを設定します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して Banners (バナー) および Messages (メッセージ) 設定を編集します。
2. **Message of the Day**[本日のメッセージ]を有効化します。
3. **Message of the Day**[本日のメッセージ]（最大 3,200 文字）を入力します。

   メッセージを入力して***OK***をクリックすると、その後ログインする管理者や画面の更新を行ったアクティブな管理者に対し、新しいメッセージやアップデートされたメッセージが即座に表示されるようになります（コミットする必要はありません）。これにより、他の管理者の設定に影響を及ぼす可能性のある、間もなく実行予定のコミットについて通知を行うことができます。メッセージにて指定されているコミット時間に応じて、管理者は自身が行った変更を完了するか、保存するか、あるいはやり直すか検討することができます。
4. （任意）初回のログインセッションの後、管理者が任意で本日のメッセージを非表示にできるようにするには、**Allow Do Not Display Again**[以後、非表示にすることを許可]を選択します（デフォルト設定では無効な状態）。各管理者は、自分のログインセッションでのみメッセージを非表示にすることができます。この非表示オプションは、本日のメッセージ ダイアログのそれぞれのメッセージに対して独立して適用されるようになっています。
5. (任意) 本日のメッセージ ダイアログのヘッダー **Title (タイトル)** (デフォルト設定は `Message of the Day`) を入力します。

STEP 3 | ヘッダーおよびフッターバナーを設定します。

背景に明るい色を使い、それと対象的な色でテキストを表示することにより、管理者がバナーに気付いて内容を確かめる可能性が高まります。また、お客様の組織の分類レベルに対応した色を使用することもできます。

1. **Header Banner**[ヘッダーバナー]（最大3,200文字）を入力します。
2. （任意）ヘッダーおよびフッターで別々のバナーを使用するには、**Same Banner Header and Footer**[ヘッダーおよびフッターで同じバナーを使用]をクリアします（デフォルト設定で有効）。
3. ヘッダーバナーおよびフッターバナーが異なる場合、**Footer Banner**[フッターバナー]（最大3,200文字）を入力します。
4. **OK** をクリックします。

STEP 4 | ログインページおよびヘッダーのロゴを変更します。

ロゴ画像の最大サイズは、*128KB* です。サポートされるファイルの種類は *png* と *jpg* です。インターレースされたイメージ ファイル、アルファ チャネルを含むイメージ、および *GIF* ファイルの種類は *PDF* の生成に干渉するため、ファイアウォールはサポートしていません。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)** を選択し、Miscellaneous (その他) セクションで **Custom Logos (カスタム ロゴ)** をクリックします。
2. **Login Screen**[ログイン画面]のロゴおよび**Main UI**[メインUI]（ヘッダー）のロゴそれぞれに対して次の作業を行います。
   1. アップロードをクリックします。
   2. ロゴ画像を選択して**Open**[開く]をクリックします。

      拡大鏡のアイコンをクリックするとプレビューが表示され、*PAN-OS*により画像がどのようにトリミングされるか確認することができます。
   3. **Close**（閉じる）をクリックします。
3. 変更をコミットします。

STEP 5 | 希望した通りにバナー、本日のメッセージ、ロゴが表示されているかどうか確認します。

1. ログアウトしてログインページに戻ると、選択した新しいロゴが表示されます。
2. ログインに使用する認証情報を入力し、バナーを確認し、**I Accept and Acknowledge the Statement Below (次の内容に同意・承認します)**を選択して**Login (ログイン)**ボタンを有効化して最後に**Login (ログイン)**します。

   ダイアログに本日のメッセージが表示されます。Palo Alto Networksからメッセージは、同じダイアログの別のページに表示されます。各ページを移動する場合、ダイアログの側面に表示されている右向きと左向きの矢印をクリックするか、ダイアログ下部に表示されているページセレクターをクリックします。
3. （任意）自分で設定したメッセージやPalo Alto Networksからのメッセージをすべて**Do not show again**[以後表示しない]よう選択することができます。
4. 本日のメッセージ ダイアログを**Close**[閉じ]、Webインターフェイスにアクセスします。

   テキストや色を設定したヘッダーおよびフッターバナーが、Webインターフェイスの各ページに表示されます。Webインターフェイス用に選択した新しいロゴがヘッダーバナーの下に表示されます。

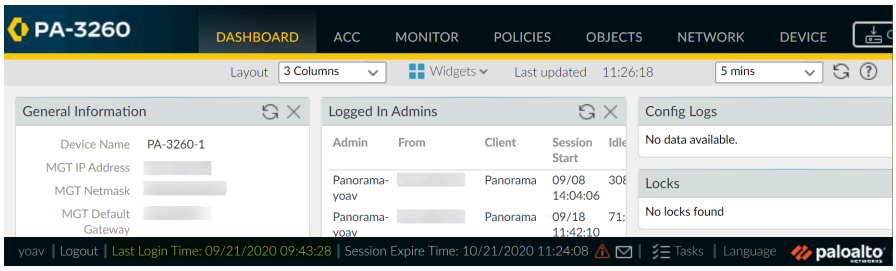
管理者ログインアクティビティ インジケーターを使用してアカウントの不正利用を検知

最終ログイン時間およびログイン失敗回数のインジケーターにより、Palo Alto Networksのファイアウォールあるいは Panorama管理サーバーで使用している自分の管理者アカウントの不正利用を発見する上で役立つ、視覚的な情報を得られます。最終ログイン情報を使用すれば自分の認証情報を使用して他人がログインしたことがあるかどうかが分かり、ログイン失敗回数インジ

ケーターを使用すれば自分のアカウントが総当たり攻撃のターゲットにされたかどうかを確認することができます。

STEP 1 | ログインアクティビティ インジケーターを確認し、自分のアカウントの最近のアクティビティを監視します。

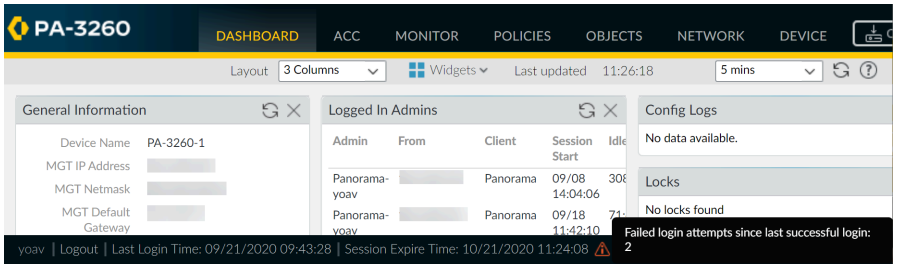
1. ファイアウォールあるいはPanorama管理サーバーのWebインターフェイスにログインします。
2. ウィンドウの左下に表示されている最終ログイン情報を確認し、タイムスタンプが前回自分がログインした時間と合致していることを確認します。



3. 最終ログイン時間情報の右側にある警告アイコンを探し、ログイン失敗回数を確認します。

   前回ログインに成功してから1回でもログインに失敗している場合は、ログイン失敗回数インジケーターが表示されます。

   1. 警告アイコンが表示されている場合、アイコンを合わせればログイン失敗回数が表示されます。

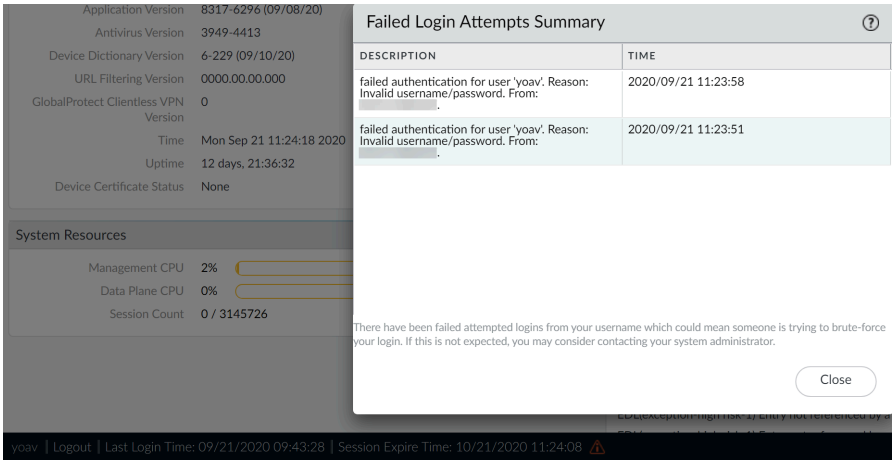


   2. 警告アイコンをクリックすると、失敗したログイン試行に関するサマリーが表示されます。これには、管理者アカウントの名前、ログイン失敗の理由、ソースIPアドレス、日時といった情報が含まれます。

      ログインおよびログアウトを正しく行うとログイン失敗回数が0に戻り、次回ログインする際にまた新たにログイン試行失敗があったかどうか確認することができます。

STEP 2 | ファイアウォールあるいは Panorama 管理サーバーに対して継続的にログインを試みているホストを特定します。

1. ログイン失敗の警告アイコンをクリックすると、失敗したログイン試行に関するサマリーが表示されます。
2. ログインを試みたホストのソースIPアドレスを特定・記録します。例えば、次の図は、複数回のログイン試行に失敗したことを示しています。



3. ネットワーク管理者と協力し、特定したIPアドレスを使用しているホストおよびユーザーを特定します。

   総当たり攻撃を行っているシステムを特定できない場合、アカウント名を変更して今後の攻撃を防ぐことも検討してください。

STEP 3 | アカウントに対する危険を検知した場合、次の作業を行います。

1. 自分が知らないところでアカウントが使用され、変更が加えられていないかどうか、**Monitor (監視)** > **Logs (ログ)** > **Configuration (構成)** を選択して設定変更を確認し、履歴をコミットします。
2. **Device (デバイス)** > **Config Audit** （設定監査） を選択し、現在の設定と、自分の認証情報を使用して設定が変更された疑いがある時点の直前の設定とを比較します。また、これはPanoramaを使用して実行することもできます。

   自分の管理者アカウントを使用して新しいアカウントが作成された場合、権限のないあらゆるアカウントに関する変更を検知するのにも設定監査が役立ちます。
3. 自分のアカウントを使用してログが削除された、あるいは不正に変更されたかどうか判別が難しい場合は、元の正しい設定に戻してください。

   以前の設定にコミットする前に、正しい設定が含まれていることをしっかり確認します。例えば、設定を戻すと最近加えた変更が反映されない可能性があるため、バックアップ設定をコミットした後でその変更を適用します。

   権限付きのアカウントに対する総当たり攻撃を防ぐ上で役立つ、以下のベストプラクティスに従ってください。

   - 認証プロファイルの*Failed Attempts [試行失敗回数]*および*Lockout Time (min) (ロックアウト時間（分）)*、あるいは管理インターフェイス用の*Authentication Settings (認証設定)*（***Device (デバイス)*** **>** ***Setup (セットアップ)*** **>** ***Management (管理)*** **>** ***Authentication Settings (認証設定)***）にて、ファイアウォールが権限付きのアカウントをロックするまでに許される試行失敗回数を制限します。
   - インターフェイス管理プロファイルを使用してアクセスを制限します。
   - 権限付きのアカウントには複雑なパスワードの使用を求めます。

管理タスクの管理・監視

タスク マネージャには、自分や他の管理者が行った操作（手動のコミットなど）や、前回のファイアウォールの再起動後にファイアウォールが開始した操作（定期レポートの生成など）についての詳細情報が表示されます。タスク マネージャを使用すれば、失敗した操作についてトラブルシューティングを行ったり、完了したコミットに関する警告について調査を行ったり、キューに並んでいるコミットの詳細情報を確認したり、保留中のコミットをキャンセルしたりすることができます。

また、システム ログを確認してファイアウォールのシステムイベントを監視したり、設定ログを確認してファイアウォールの設定変更を監視したりできます。

STEP 1 | Webインターフェイスの下部にある **Tasks**[タスク] をクリックします。

STEP 2 | 現在**Running**[実行中]（進行中）のタスクのみ、あるいは**All**[すべて]のタスク（デフォルト設定）を**Show**[表示]します。任意で、タスクを種類ごとに表示することができます。

- **Jobs**[ジョブ]—管理者が開始したコミット、ファイアウォールが開始したコミット、およびソフトウェアやコンテンツのダウンロードとインストール。
- **Reports**[レポート]—定期レポート。
- **Log Requests (**ログ リクエスト**)** —自分が**Dashboard (**ダッシュボード**)** あるいは**Monitor (**監視**)** ページにアクセスすることで発生したログ クエリ。

STEP 3 | 以下の中から選択して作業を行います。

- **Display or hide task details**（タスクの詳細を表示/非表示） — デフォルト設定では、タスク マネージャに各タスクの Type（タイプ）、Status（ステータス）、Start Time（開始時間）、Messages（メッセージ）が表示されます。タスクのEnd Time [終了時間]およびIDを確認するには、これらの列を表示するよう手動で設定を行う必要があります。列の表示/非表示を行うには、列の見出しにあるドロップダウンリストを開き、**Columns**[列]を選択し、必要に応じて列を選択/選択解除します。
- **Investigate warnings or failures**（警告あるいは失敗を調査） — タスク詳細情報にある Messages（メッセージ）列の項目を読みます。列に`Too many messages`[メッセージが多すぎます]と表示されている場合、Type [タイプ]列で対象の項目をクリックし、詳細な情報を表示します。
- **Display a commit description**[コミットの説明を表示]—コミットを設定する際に管理者が説明を入力している場合、Messages [メッセージ]列で**Commit Description**[コミットの説明]をクリックすることで説明を表示できます。
- **Check the position of a commit in the queue**（コミットのキュー内の順番をチェック） — Messages（メッセージ）列に、進行中のコミットのキュー内の順番が表示されます。
- **Cancel pending commits**[保留中のコミットをキャンセル]—保留中のコミットをすべてキャンセルするには**Clear Commit Queue**[コミット キューをクリア]をクリックします（定義済みの管理ロールでのみ使用可能）。コミットを個々にキャンセルするには、対象のコミットのAction [アクション]列にある**x**をクリックします（ファイアウォールがこのコミットをキューから取り除くまで、コミットはキューに残ったままになります）。進行中のコミットはキャンセルできません。

ファイアウォールの設定変更をコミット、検証、プレビュー

コミットとは、ファイアウォールの設定に加えた保留中の変更を反映させるプロセスのことです。管理者や場所に基づいてフィルタリングした保留中の変更をプレビュー、検証、コミットできます。特定の仮想システム、共有ポリシーおよびオブジェクト、または共有デバイスおよびネットワーク設定を場所（Location）にできます。

ファイアウォールはコミット作業をキューで処理するので、前回のコミットの進行中に新しいコミットを実行することができます。ファイアウォールは追加順にコミットを実行しますが、FQDN 更新など、ファイアウォールによって開始されるオートコミットを優先します。ただし、管理者が開始したコミットが既にキューの上限まで追加されている場合、ファイアウォールが保留中のコミットの処理を終えるまで待機してから、新しいコミットを開始する必要があります。保留中のコミットをキャンセルする、あるいは任意のステータスのコミットに関する詳細情報を表示する方法は、管理タスクの管理・監視を参照してください。

コミットを開始すると、変更を有効にする前にファイアウォールが変更の有効性を検証します。検証結果の表示画面には、コミットをブロックする状況（エラー）、あるいは通知が必要な状況（警告）が表示されます。例えばこの検証の結果、不正なルートの宛先が見つかり、コミットを続けるためには修正が必要になる場合があります。検証プロセスを利用すると、エラーを検出、修正してからコミットできます（実行中の設定は変更されません）。固定のコミット ウィンドウがあり、エラーなしでコミットを確実に実行したい場合に便利です。

管理対象ファイアウォールは、Panorama管理サーバーで有効にして管理すると、ローカルでコミットされた設定または Panorama からプッシュされた設定をローカルでテストして、新しい変更によって Panorama と管理対象ファイアウォール間の接続が切断されないことを確認します。コミットされた設定が Panorama と管理対象ファイアウォール間の接続を切断した場合、ファイアウォールは自動的にコミットに失敗し、設定は以前の実行中の設定に戻ります。さらに、Panorama 管理サーバーによって管理されているファイアウォールは、Panorama への接続を60分ごとにテストし、管理対象ファイアウォールが Panorama に正常に接続できなくなったことを検出した場合、設定を以前の実行中の設定に戻します。

コミット、検証、プレビュー、保存、復元操作は、前回のコミット後に加えた変更にのみ適用されます。前回のコミットよりも前の状態に設定を戻すためには、以前にバックアップした設定を読み込む必要があります。

複数の管理者が同時セッションで設定変更を行うのを防止する方法については、設定変更を制限するためのロックの管理をご参照ください。

STEP 1 | コミット、検証、プレビューを行う設定変更の範囲を設定します。

1. Webインターフェイスの上部にある **Commit**（コミット）をクリックします。
2. 以下のいずれかのオプションを選択します。
   - **Commit All Changes**（すべての変更をコミット）（デフォルト）— 管理権限があるすべての変更をコミットします。このオプションを選択すると、コミット スコープを手動で絞り込むことはできなくなります。代わりに、ログインに使用しているアカウントに割り当てられた管理者ロールによって、コミット スコープが指定されます。
   - **Commit Changes Made By**（指定対象による変更のコミット）— 管理者または場所によってコミット スコープを絞り込むことができます。ログインに使用しているアカウントに割り当てられた管理ロールによって、どの変更を絞り込めるかが決まります。

     他の管理者の変更をコミットするには、ログインに使用したアカウントにスーパーユーザー ロールが割り当てられているか、***Commit For Other Admins***（他の管理者に代わってコミット）権限が有効な管理者ロール プロファイルが割り当てられている必要があります。
3. （任意）管理者でコミット スコープを絞り込むには、**Commit Changes Made By**（指定対象による変更のコミット）を選択して、その横のリンクをクリックし、管理者を選択して **OK** をクリックします。
4. （任意）場所で絞り込むには、**Commit Changes Made By**（指定対象による変更のコミット）を選択し、コミット スコープから除外する変更をオフにします。

含めた設定変更、除外した設定変更の依存関係により検証エラーが発生する場合、すべての変更を含めてコミットを行います。例えば、仮想システムへの変更をコミットする場合、その仮想システムの同じルールベースのルールの追加、削除、位置変更を行ったすべての管理者の変更を含める必要があります。

STEP 2 | コミットにより反映される変更をプレビューします。

例えば変更内容をすべて覚えておらず、変更をすべて反映させて良いのか分からないと時はこのオプションが役立ちます。

Commit Scope (コミット範囲) で選択した設定を、ファイアウォールが実行中の設定と比較します。プレビュー ウィンドウには設定が横に並べて表示され、色分けによって、どの変更が追加であるか（緑）、変更であるか（黄）、削除であるか（赤）が示されます。

Preview Changes (変更をプレビュー) し、**Lines of Context (コンテクストの行数)** を選択します。これは、ハイライト表示された各差異の前後を示す、比較対象の設定ファイル中の行数です。この追加の行により、プレビュー結果をWebインターフェイスの設定内容に反映させやすくなります。変更のプレビューが完了したら、プレビューウィンドウを閉じます。

プレビュー結果は新しいブラウザ ウィンドウで表示されるので、ブラウザでポップアップを許可しておく必要があります。プレビュー ウィンドウが開かない場合は、ポップアップを許可する手順についてブラウザのドキュメントを参照してください。

STEP 3 | 変更をコミットする個別の設定をプレビューします。

設定のタイプや変更者など、変更の詳細について把握する場合は、これが役立つことがあります。

1. **Change Summary**（変更サマリー）をクリックします。
2. （任意）**Group By**（グループ化基準）により、列名（設定の **Type**（タイプ）など）によってグループ化します。
3. 変更のプレビューが完了したら、**Close**（閉じる）によって Change Summary（変更サマリー）ダイアログを閉じます。

STEP 4 | 確実にコミットが完了するよう、コミット前に変更内容を検証します。

1. **Validate Changes**（変更の検証）を行います。

   実際にコミットを行う際と同じエラーや警告がすべて結果に表示されます。
2. 検証結果で明らかになったエラーをすべて解決します。

STEP 5 | 設定の変更を Commit (コミット) します。

変更を **Commit (コミット)** し、それを検証・有効化します。

保留中（キャンセル可能）、進行中、完了済み、あるいは失敗したコミットについての詳細情報を確認する方法については、管理タスクの管理・監視を参照してください。

選択的な構成変更のコミット

構成の変更は頻繁に行われ、通常は、他にどのような構成変更が行われたかを認識していない複数の管理者によって行われます。どの構成オブジェクトをコミットするかを制御し、不完全な構成が ファイアウォール にコミットされるのを防ぐことが極めて重要です。保留中の設定変更をすべてコミットするのではなく、代わりにコミットする設定オブジェクトを選択することができます。選択的コミットが成功すると、システムログが生成されます。

特定のオブジェクトを選択してコミットすることができるため、コミットする準備ができていない構成変更を行う他の管理者を中断することなく、複数の管理者が構成変更を効率的に行うことができます。構成変更を選択的にコミットする機能を活用することで、定義された運用手順を維持しながら、運用範囲内で定義されていない独立した構成変更を正常に行うことができます。

STEP 1 | ファイアウォール Web インターフェイス にログインします。

STEP 2 | ファイアウォールの構成変更を行い、**Commit (コミット)** を実行します。

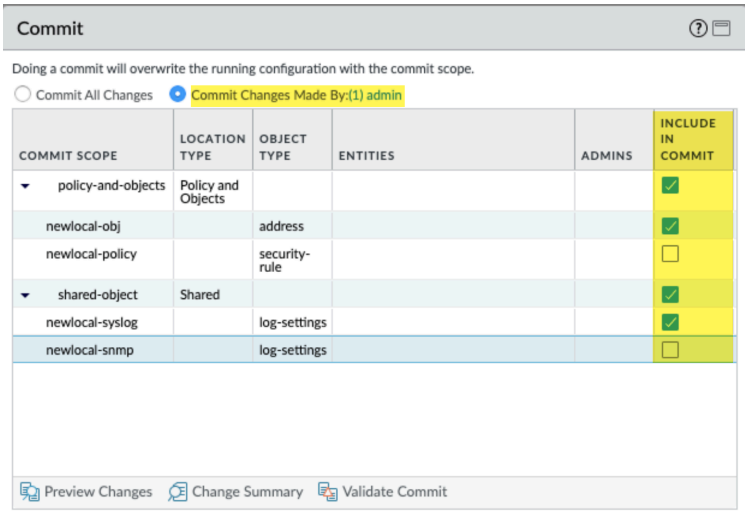
STEP 3 | コミット範囲を **Commit Changes Made By** に変更して、コミットする構成変更を選択します。

プッシュスコープには、現在ログインしている管理者の名前が表示されます。管理者名をクリックすると、コミットされていない構成変更を行った管理者のリストが表示されます。

STEP 4 | (オプション) 保留中の構成変更をプレビューして検証し、選択した構成オブジェクトをコミットすることを確認します。

STEP 5 | **[コミット]** します。

Commit Status (コミットステータス) ページには、コミットされた構成変更を行った管理者と、コミットされた構成変更の場所が表示されます。



設定バンドル データのエクスポート

Panorama™ およびファイアウォールからポリシー ルール、設定オブジェクト、IPS シグネチャをエクスポートして、外部監査法人への規制遵守を実証し、ファイアウォール設定の定期的レ

ビューを行い、ファイアウォール ポリシーに関するレポートを生成します。これにより、監査法人がファイアウォールやアプライアンスに直接アクセスしたり、スクリーンショットを撮ったり、XML API にアクセスして設定レポートを生成したりする必要がなくなります。Web インターフェイスから、ポリシー、オブジェクト、ネットワーク、ファイアウォール、および Panorama 設定の設定テーブルデータに加えて、アンチウイルス、アンチスパイウェア、および脆弱性保護のセキュリティ プロファイルのシグネチャ例外を、PDF または CSV ファイルのいずれかでエクスポートできます。

設定バンドルのエクスポートは印刷機能のように機能します。生成されたファイルを Panorama またはファイアウォールにインポートすることはできません。データを PDF ファイルとしてエクスポートし、テーブルの データが 50,000 行を超えると、データは複数の PDF ファイル (<report-name>_part1.pdf や <report-name>_part2.pdf など) に分割されます。データをCSV ファイルとしてエクスポートすると、そのデータは 1 つのファイルとしてエクスポートされます。これらのエクスポート形式を使用すると、レポート条件に一致するフィルタを適用し、PDF レポート内で検索して特定のデータをすばやく見つけることができます。さらに、設定テーブルのデータをエクスポートすると、イベントを記録するシステムログが生成されます。

STEP 1 | Web インターフェイスを起動して、エクスポートする必要がある設定データを識別します。

STEP 2 | 必要に応じてフィルタを適用して、エクスポートする必要のある設定データを作成し、**PDF/CSV** をクリックします。

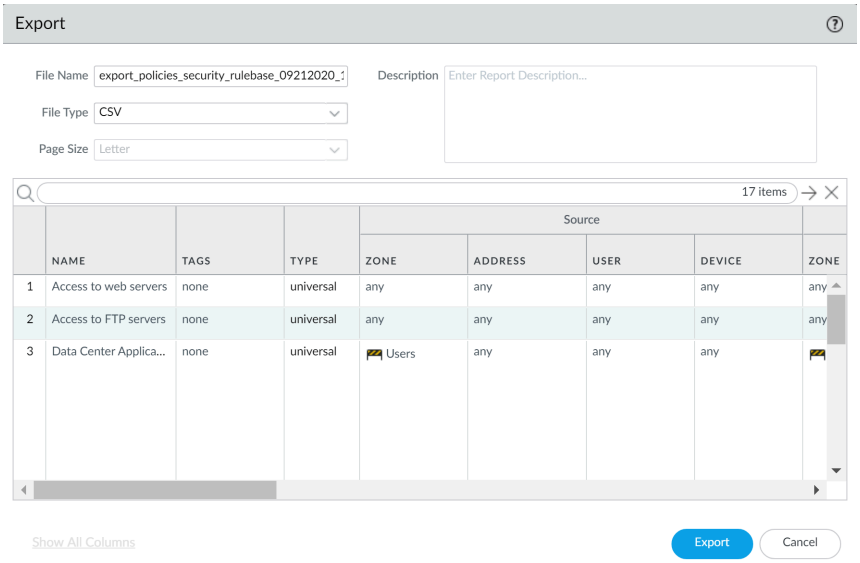
STEP 3 | 構成バンドルのエクスポート レポートを設定します：

1. **File Name**（ファイル名）を入力します。
2. **File Type**（ファイル タイプ）を選択します。
3. （任意）レポート説明を入力します。
4. 設定テーブルのデータが、適用したフィルタと一致することを確認します。

> ***Show All Columns***（すべての列を表示）を選択して、適用されたすべてのフィルタを表示します。

STEP 4 | 設定バンドル データを **Export**（エクスポート）します。

設定バンドルのエクスポートは印刷機能のように機能します。生成されたファイルを Panorama またはファイアウォールにインポートすることはできません。



STEP 5 | エクスポートしたファイルを保存する場所を選択します。

グローバル検索を使用してファイアウォールあるいはPanoramaの管理サーバーを検索

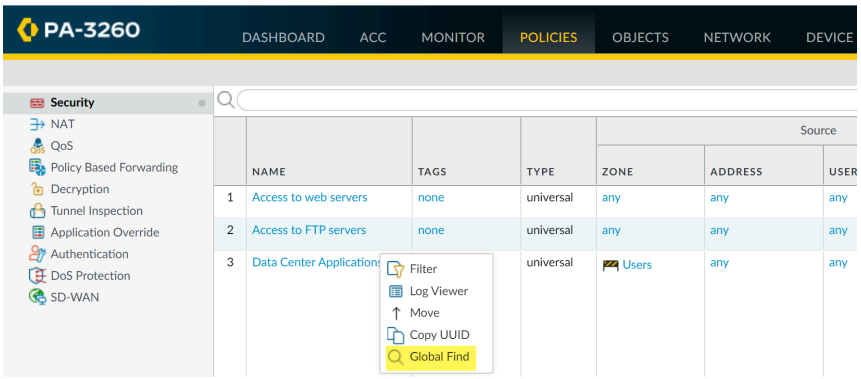
グローバル検索を使用すると、ファイアウォールまたは Panorama の候補設定に含まれる特定の文字列 (IP アドレス、オブジェクト名、ポリシールール名、脅威 ID、UUID、アプリケーション名など) を検索できます。設定オブジェクトおよび設定を検索するのに加え、管理者が実行した手動コミット、あるいはファイアウォールあるいは Panorama が実行した自動コミットのジョブ ID あるいはジョブ タイプに基づいて検索できます。検索結果はカテゴリー別に分類され、Web インターフェイスの設定場所へのリンクが表示されるので、当該文字列が出現するすべての場所を簡単に見つけることができます。検索結果は、検索語または文字列に依存したり、それらを参照する他のオブジェクトの識別にも役立ちます。たとえば、セキュリティ プロファイルを廃止する場合は、Global Find [グローバル検索]にプロファイル名を入力してプロファイルのすべてのインスタンスを見つけてから、各インスタンスをクリックして設定ページに移動し、必要な変更を行います。すべての参照が削除されたら、プロファイルを削除できます。依存関係のあるすべての設定項目に対してこの操作を実行できます。

動画をご覧ください。

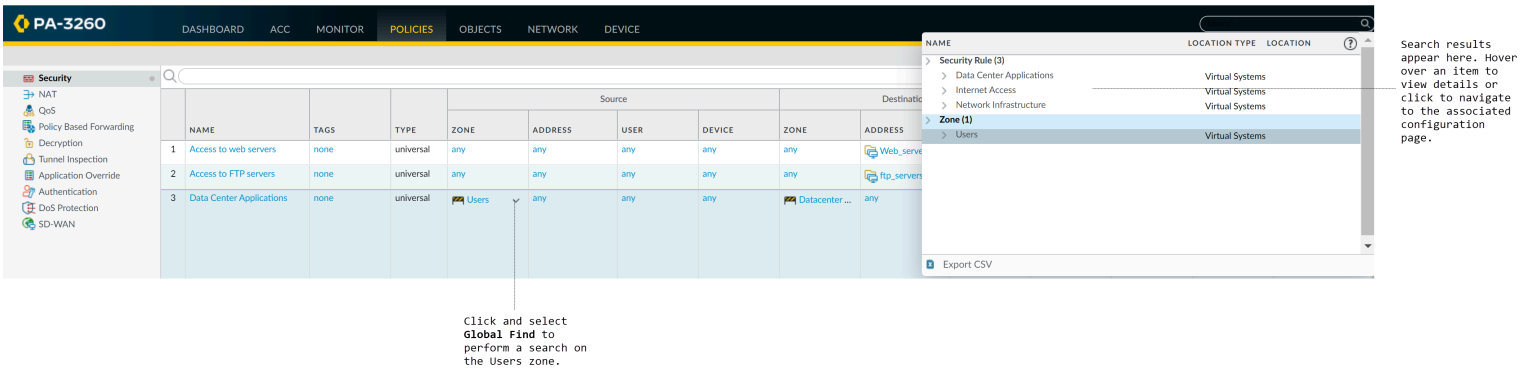
グローバル検索では、動的コンテンツ (ログ、アドレス範囲、割り当てられた *DHCP* アドレスなど) は検索されません。*DHCP* の場合、*DHCP* サーバー属性（*DNS* エントリなど）は検索できますが、ユーザーに割り当てられた個々のアドレスは検索できません。ユーザー/グループがポリシーで定義されていない場合、ユーザー *ID* で識別される個々のユーザーまたはグループ名も検索されません。一般に、ファイアウォールが設定に書き込む内容のみ検索できます。

グローバル検索を起動するには、Web インターフェイスの右上にある **Search** [検索]アイコンをクリックします。

設定エリア内でグローバル検索にアクセスするには、当該項目の横のドロップダウン リストをクリックして、**Global Find**[グローバル検索] を選択します。



たとえば、**Users(ユーザー)** という名前のゾーンで **Global Find(グローバル検索)** をクリックすると、そのゾーンが参照されている各場所の設定の候補が検索されます。以下の画面キャプチャは、ゾーン「Users (ユーザー）」の検索結果です:



検索のヒント:

- 複数の仮想システムが有効になっているファイアウォール上で検索を開始する場合、またはカスタム管理ロール タイプが定義されている場合は、管理者にアクセス許可が与えられ

ているファイアウォールのエリアの検索結果のみが返されます。同じことは Panorama デバイス グループにも当てはまります。

- 検索語に含まれるスペースは、AND 演算子として処理されます。たとえば、「**corp policy**」を検索すると、検索結果には設定に corp と policy の両方があるインスタンスが表示されます。
- 完全に一致するフレーズを検索するには、フレーズを引用符で囲みます。
- 5 つ以下のキーワードを入力するか、引用符で完全に一致する語句を使用してください。
- 前の検索を再実行するには、検索（Web インターフェイスの右上隅）をクリックします。最近実行した検索のリストが 20 件まで表示されます。リストの項目をクリックすると、その検索が再実行されます。この検索履歴は、管理者アカウントごとに固有のものです。
- UUID を検索するには、その UUID をコピー＆ペーストする必要があります。

設定変更を制限するためのロックの管理

設定のロックを使用すれば、自分が手動でロックを解除する、あるいはファイアウォールが自動的にロックを解除するまでの間に、他の管理者が候補構成を変更したり、設定変更をコミットしたりするのを防ぐことができます。このロックにより、同時ログインセッションにおいて相互に依存する設定や同一の設定に対して、管理者が衝突する変更内容を設定できなくなります。

ファイアウォールはコミットのリクエストをキューに並べ、管理者がコミットを開始した順番でコミットを実行していきます。詳細についてはファイアウォールの設定変更をコミット、検証、プレビューを参照してください。キューに並んでいるコミットのステータスを確認する方法については、管理タスクの管理・監視を参照してください。

現在のロックの詳細情報を表示します。

例えば、他の管理者がロックを設定したかどうかや、ロックの説明として入力されたコメントを確認することができます。

Web インターフェイスの上部にあるロック アイコンをクリックします。隣りにある数値は、現在のロック数を示します。

設定をロックします。

1. Web インターフェイスの上部にあるロック アイコンをクリックします。

   現在存在するロックが🔒あるいは🔓セットされていないかどうかによって、異なったロックアイコンが表示されます。

2. **Take a Lock**（ロックを選択）し、さらにロック**Type**（タイプ）を選択します。
   - **Config**（設定） – 他の管理者が候補設定を変更できないようにブロックします。
   - **Commit** （コミット） – 他の管理者が候補設定の変更をコミットすることを阻止します。
3. （仮想システムが複数あるファイアウォールのみ）得手の仮想システムで設定をロックする場合は**Location**[場所]を、あるいは**Shared**[共有]場所を選択します。
4. （任意）ロックをした理由が他の管理者にも分かるよう**Comment**[コメント]を入力しておくのが良いでしょう。
5. **OK**、**Close**（閉じる）の順にクリックします。

設定のロックを解除します。

スーパーユーザーまたはロックをセットした管理者のみが手動でロックを解除することができます。しかし、コミット操作の完了後、ファイアウォールが自動的にロックを解除します。

1. Web インターフェイスの上部にあるロック アイコンをクリックします。
2. リストからロックのエントリを選択します。
3. **Remove Lock**（ロック解除）、**OK**、**Close**（閉じる）の順にクリックします。

候補設定を変更するときにコミット ロックが自動的に適用されるように、ファイアウォールを設定します。この設定はすべての管理者に適用されます。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して General Settings (一般設定) を編集します。
2. **Automatically Acquire Commit Lock**(自動的にコミットをロック)を選択し、**OK**および**Commit**(コミット)をクリックします。

設定バックアップ ファイルの管理

ファイアウォール上の現在アクティブな設定はコミットしたすべての設定から成り、そのためアクティブな状態になっています。これにはネットワーク内の各トラフィックタイプをブロックあるいは許可するポリシールールなどがあります。候補設定は、現在アクティブな設定のコピー、および前回のコミット後に加えたアクティブでない変更から成ります。現在アクティブな設定あるいは候補設定の各バージョンのバックアップを保存することで、後で各バージョンを復元することが可能になります。たとえば、コミット検証の結果、修復したくなくなるほど多くのエラーが現在の候補設定に含まれていることが分かった場合、以前の候補設定を復元することができます。最初にバックアップを保存せずに、現在アクティブな設定に戻ることもできます。内部レビューまたは監査のために設定の特定の部分をエクスポートする必要がある場合は、設定テーブルデータをエクスポートできます。

コミット操作の詳細については、ファイアウォールの設定変更をコミット、検証、プレビューを参照してください。

- ファイアウォールの設定の保存およびエクスポート
- ファイアウォールの設定変更を元に戻す

ファイアウォールの設定の保存およびエクスポート

候補構成のバックアップをファイアウォールの永続ストレージに保存することで、後からそのバックアップを復元することができます（ファイアウォールの設定変更を元に戻すを参照）。これは、システムイベントや管理者のアクションによってファイアウォールが再起動した際に失われるおそれがある変更を保持したい場合に役立ちます。再起動後、ファイアウォールが running-config.xml というファイルに保存している、現在アクティブな設定の最新バージョンを PAN-OS が自動的に復元します。バックアップの保存は、現在実行中の設定よりも前のファイアウォールの設定に戻したい場合にも役立ちます。ファイアウォールが自動的に候補設定を永続的なストレージに保存することはありません。デフォルト スナップショット ファイル（.snapshot.xml）として、あるいは任意の名前のスナップショット ファイルとして、手動で候補設定を保存する必要があります。ファイアウォールはスナップショット ファイルをローカルに保存しますが、それを外部ホストにエクスポートすることができます。

前回のコミット後に加えた変更に戻すために、設定のバックアップを保存したり、再起動したりする必要はありません。***Config (設定) > Revert Changes (変更を元に戻す)*** を選択するだけで結構です（ファイアウォールの設定変更を元に戻すを参照）。

設定を変更して***OK***をクリックすると、ファイアウォールは候補設定を更新しますが、スナップショットのバックアップを保存することはありません。

さらに、保存しただけでは変更が反映されません。変更を有効化するには、コミットを実行します（ファイアウォールの設定変更をコミット、検証、プレビューを参照）。

*Palo Alto Networks*は、重要な設定をすべて、ファイアウォールの外部にあるホストでバックアップを取ることを推奨します。

STEP 1 | ファイアウォールが再起動した後も維持したい変更内容が含まれている候補設定については、バックアップ スナップショットをローカルに保存します。

これらの変更はまだコミットする準備ができていません（例えば、現在のログインセッションでは変更作業を完了できません）。

デフォルトのスナップショット ファイル（.snapshot.xml）を、すべての管理者が行ったすべての変更で上書きするには、以下のいずれかのステップを実行します。

- **Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)** を選択し、さらに **Save candidate configuration (候補構成の保存)**を選択します。
- スーパーユーザーのロール、あるいは他の管理者のために保存権限が有効である管理者ロール プロファイルが割り当てられている管理者アカウントを使ってファイアウォールにログインします。次に、Web インターフェイスの上部で**Config**（設定） > **Save Changes**（変更の保存）の順に選択し、**Save All Changes**（すべての変更を保存）および **Save**（保存）を選択します。

デフォルトのスナップショット ファイルを上書きせずに、すべての管理者が行ったすべての変更を含むスナップショットを作成するには、以下のステップを実行します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)** を選択し、さらに **Save named configuration snapshot (名前を付けて設定スナップショットを保存)** を選択します。
2. 新規または既存の設定ファイルの **Name**（名前）を指定します。
3. **OK**、**Close**（閉じる）の順にクリックします。

デフォルトのスナップショット ファイルのどの部分も上書きせずに、候補設定に対する特定の変更のみを保存するには、以下のステップを実行します。

1. 対象の設定を保存できるロール権限を持つ管理者アカウントを使ってファイアウォールにログインします。
2. Web インターフェイスの上部で **Config**（設定） > **Save Changes**（変更の保存）の順に選択します。

3. **Save Changes Made By**（指定対象による変更の保存）を選択します。
4. Save Scope を管理者毎にフィルターするには、**<administrator-name>** をクリックし、管理者を選択して **OK** をクリックします。
5. Save Scope（保存範囲）を場所でフィルタリングするには、除外する場所をクリアします。特定の仮想システム、共有ポリシーおよびオブジェクト、または共有デバイスおよびネットワーク設定を場所（Location）にできます。
6. **Save**（保存）をクリックし、新規または既存の設定ファイルの **Name**（名前）を指定して **OK** をクリックします。

STEP 2 | 候補設定、現在アクティブな設定、あるいはファイアウォールの状態情報を、ファイアウォールの外部にあるホストにエクスポートします。

Device (デバイス) > **Setup (セットアップ)** > **Operations (操作)** を選択してエクスポート オプションをクリックします。

- **Export named configuration snapshot**[名前を付けて保存した候補設定のスナップショットをエクスポート]–現在アクティブな設定、名前を付けて保存した候補設定のスナップショット、または前回インポートした設定（候補または実行中の設定）をエクスポートします。ファイアウォールは、指定した**Name**[名前]のXMLファイルとして設定をエクスポートします。
- **Export configuration version**[設定のバージョンをエクスポート]–現在アクティブな設定の**Version**[バージョン] を選択し、XMLファイルとしてエクスポートします。設定変更をコミットする際、ファイアウォールは必ず新しいバージョンを作成します。
- **Export device state**[デバイス状態をエクスポート]–ファイアウォールの状態の情報をバンドルとしてエクスポートします。現在アクティブな設定に加え、状態の情報には Panorama からプッシュされたデバイスグループ設定やテンプレート設定が含まれます。ファイアウォールがGlobalProtectポータルの場合、この情報には、証明書情報、サテライトの一覧、およびサテライト認証情報が含まれています。ファイアウォールまたはポータルを交換した場合、代替のものに状態のバンドルをインポートすることで、エクスポートしておいた情報を復元することができます。

ファイアウォールの設定変更を元に戻す

元に戻す操作を実行すると、現在の候補設定が別の設定に置き換えられます。変更を元に戻す操作が便利なのは、複数の設定に対する変更を手動で個々に取り消すのではなく、1 回の操作で取り消したいときです。

前回のコミット後にファイアウォールの設定に加えられた保留中の変更を元に戻すことができます。ファイアウォールでは、管理者やロケーションに基づいて保留中の変更をフィルタリングするオプションを利用できます。特定の仮想システム、共有ポリシーおよびオブジェクト、または共有デバイスおよびネットワーク設定を場所（Location）にできます。現在アクティブな設定よりも前の候補構成用のスナップショット ファイルを保存している場合（ファイアウォールの設定を保存・エクスポートを参照）、そのスナップショットに戻すこともできます。スナップショットを復元すると、最後のコミットより前に存在していた候補設定を復元できます。変更をコミットする際、ファイアウォールは現在アクティブな設定の新しいバージョンを自動的に保存するため、後でこれらのバージョンを復元することができます。

現在実行中の設定（ファイル名：running-config.xml）に戻します。

この操作では、前回のコミット以降に候補設定に対して加えた変更が取り消されます。

すべての管理者が行ったすべての変更を元に戻すには、以下のステップを実行します。

- **Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作), Revert to running configuration (現在アクティブな設定に戻す)** を選択し、**Yes (はい)** をクリックして操作を確定します。
- スーパーユーザーのロール、あるいは他の管理者のためにコミット権限が有効である管理者ロール プロファイルが割り当てられている管理者アカウントを使ってファイアウォールにログインします。次に、Web インターフェイスの上部で**Config**（設定） > **Revert Changes**（変更を元に戻す）を選択し、**Revert All Changes**（すべての変更を元に戻す）および **Revert**（元に戻す）を選択します。

特定の変更のみを候補設定に戻すには、以下のステップを実行します。

1. 対象の設定を元に戻すことができるロール権限を持つ管理者アカウントを使ってファイアウォールにログインします。

   コミット操作を制御する権限は、元に戻す操作も制御します。

2. Web インターフェイスの上部で **Config**（設定） > **Revert Changes**（変更を元に戻す）の順に選択します。
3. **Revert Changes Made By**（指定対象に基づいて変更を元に戻す）を選択します。
4. Revert Scope を管理者でフィルター処理するには、**<administrator-name>** をクリックし、管理者を選択して **OK** をクリックします。
5. Revert Scope（元に戻す範囲）を場所でフィルタリングするには、除外する場所をクリアします。
6. 変更に対して **Revert**（元に戻す）を実行します。

候補設定のデフォルトスナップショットを復元します。

これは、Webインターフェイスの上部にある **Config (設定)** > **Save Changes (変更の保存)** をクリックした際に作成/上書きされるスナップショットです。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)** を選択し、さらに **Revert to last saved configuration (前回保存した設定に戻す)** を選択します。
2. **Yes**（はい）をクリックして操作を確定します。
3. （任意）**Commit**[コミット]をクリックして現在アクティブな設定をスナップショットで上書きします。

ファイアウォールに保存されている、現在アクティブな設定の以前のバージョンを復元します。

設定変更をコミットする際、ファイアウォールは必ず新しいバージョンを作成します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)** を選択し、さらに **Load configuration version (設定のバージョンを読み込む)** を選択します。
2. 設定の **Version**（バージョン）を選択して **OK** をクリックします。
3. （任意）**Commit**[コミット]をクリックし、先ほど復元したバージョンで現在アクティブな設定を上書きします。

以下のいずれかを復元します。

- 名前を付けて保存した現在アクティブな設定（以前にインポートしたもの）。
- 名前を付けて保存した候補設定のスナップショット（デフォルトのスナップショットではない）

1. **Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)** を選択して **Load named configuration snapshot (名前を付けて保存した設定スナップショットを読み込む)** をクリックします。
2. スナップショットの **Name**（名前）を選択して**OK** をクリックします。
3. （任意）**Commit**[コミット]をクリックして現在アクティブな設定をスナップショットで上書きします。

以前に外部ホストにエクスポートした、現在アクティブな設定あるいは候補設定を復元します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)** を選択し、**Import named configuration snapshot (名前を付けて保存した設定スナップショットをインポート)** をクリックし、外部ホストにある設定ファイルを **Browse (参照)** し、**OK** をクリックします。
2. **Load named configuration snapshot**（名前を付けて保存した設定スナップショットを読み込む）をクリックし、先ほどインポートした設定ファイルの **Name**（名前）を選択して **OK** をクリックします。
3. （任意）**Commit**[コミット]をクリックし、現在アクティブな設定を先ほどインポートしたスナップショットで上書きします。

ファイアウォールからエクスポートした状態情報を復元します。

現在アクティブな設定に加え、状態の情報には Panorama からプッシュされたデバイスグループ設定やテンプレート設定が含まれます。ファイアウォールがGlobalProtectポータルの場合、この情報には、証明書情報、サテライトの一覧、およびサテライト認証情報が含まれ

ています。ファイアウォールまたはポータルを交換した場合、代替のものに状態のバンドルをインポートすることで情報を復元することができます。

状態情報をインポートします。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)** を選択し、**Import device state (デバイス状態をインポート)** をクリックし、状態バンドルを**Browse (参照)** して **OK** をクリックします。
2. （任意）**Commit**[コミット]をクリックし、インポートした状態情報を現在アクティブな設定に適用します。

ファイアウォール管理者の管理

管理アカウントによって、Palo Alto Networks ファイアウォールの管理者のロールおよび認証方式が指定されます。すべての Palo Alto Networks ファイアウォールにデフォルトの管理アカウント（admin）が事前設定されています。このアカウントには、ファイアウォールに対する読み取りと書き込みのフル アクセス権（スーパーユーザー アクセス権としても知られる）が付与されています。

ベスト プラクティスとして、ファイアウォールの管理機能またはレポート機能へのアクセス権を必要とするユーザーごとに別個の管理アカウントを作成します。これにより、無権限での設定からファイアウォールを保護する能力を高め、個々の管理者のアクションをログに記録することができます。管理者アクセスのベストプラクティス に従って、攻撃の成功を防ぎながらファイアウォール やその他のセキュリティ デバイスへの管理アクセスを確保していることを確認してください。

- 管理ロール タイプ
- 管理者ロール プロファイルの設定
- 管理認証
- 管理者アカウントおよび認証の設定
- 管理者のアクティビティの追跡を構成する

管理ロール タイプ

ロールにより、管理者のファイアウォールに対するアクセス権のタイプを定義します。管理者のタイプ：

- ロールベース – Web インターフェイス、CLI、または XML API のさまざまな機能領域へのアクセスをよりきめ細かく制御できるカスタムロール。たとえば、Web インターフェイスのファイアウォールとネットワークの設定領域へのアクセスを許可する管理者ロール プロファイルを操作スタッフ用に、またセキュリティ ポリシー定義、ログ、およびレポートへのアクセスを許可する別個のプロファイルをセキュリティ管理者用に作成できます。複数の仮想システムを持つファイアウォールでは、そのロールがすべての仮想システムまたは特定の仮想システムに対するアクセスを定義するかどうかを選択できます。製品に新しい機能が追加された場合は、各ロールを対応するアクセス権で更新する必要があります。ファイアウォールでは、新しい機能をカスタム ロール定義に自動的に追加することはありません。カスタム管理者ロール用に設定可能な権限の詳細は、次のレファレンスを参照してください：Web インターフェイス管理者のアクセス権限。
- 動的– ファイアウォールへのアクセス権を付与する、デフォルトで利用できるロール。新しい機能が追加されると、ファイアウォールによってダイナミック ロールの定義が自動的に更新されます。ユーザーが手動で更新する必要はありません。次の表に、ダイナミック ロールに関連付けられたアクセス権限の一覧を示します。

ダイナミック ロール	権限
スーパーユーザー	新しい管理者アカウントや仮想システムを設定できるなど、ファイアウォールに対する全アクセス権を持ちます。スーパーユーザー権限を持っていなければ、その他のスーパーユーザー権限を持つ管理ユーザーを作成することができません。
スーパーユーザー（読み取り専用）	ファイアウォールに対する読み取り専用のアクセス権を持ちます。
デバイス管理者	新しいアカウントまたは仮想システムの定義を除き、選択したファイアウォールに対する全アクセス権を持ちます。
デバイス管理者（読み取り専用）	パスワードプロファイル（アクセス不可）および管理者アカウント（ログイン中のアカウントのみ表示可能）を除き、ファイアウォール設定の全項目に対し読み取り専用のアクセスが許可されます。
仮想システム管理者	選択されたファイアウォールの仮想システムにアクセスし、仮想システムの特定の要素を作成・管理します。仮想システム管理者はネットワークインターフェイス、VLAN、バーチャル ワイヤ、仮想ルーター、IPSec トンネル、GRE トンネル、DHCP、DNS プロキシ、QoS、LLDP やネットワーク プロファイルにアクセスできません。
仮想システム管理者（読み取り専用）	選択されたファイアウォールの仮想システムおよび仮想システムの特定の要素への読み取り専用アクセス。読み取り専用の権限を持つ仮想システム管理者はネットワークインターフェイス、VLAN、バーチャル ワイヤ、仮想ルーター、IPSec トンネル、GRE トンネル、DHCP、DNS プロキシ、QoS、LLDP やネットワーク プロファイルにアクセスできません。

管理者ロール プロファイルの設定

管理者ロール プロファイルでは、管理アクセス権限を詳細に定義し、会社の機密情報とエンドユーザーのプライバシーを保護できます。

最小特権アクセスの原則に従って、管理者が作業を行うためにアクセスする必要がある管理インターフェイスの領域のみにアクセスできる管理者ロールプロファイルを作成し、管理者アクセスのベストプラクティスに従うようにします。

STEP 1 | **Device (デバイス)** > **Admin Roles (管理者ロール)** の順に選択し、**Add (追加)** をクリックします。

STEP 2 | ロールの識別に使用する **Name** [名前]を入力します。

STEP 3 | **Role** [ロール]の範囲として、**Device** [デバイス]または **Virtual System** [仮想システム]を選択します。

STEP 4 | **Web UI (ウェブ UI)** および **REST API** タブで、各機能領域のアイコンをクリックして、必要な設定に切り替えます：（Enable [有効化]、Read Only [読み取り専用]、Disable [無効化]のいずれか）**XML API** タブ選択の場合は、Enable [有効化] または Disable [無効化]にします。**Web UI** オプションの詳細は、Web インターフェイスのアクセス権限を参照してください。

STEP 5 | **Command Line** [コマンドライン]タブを選択し、CLI アクセス オプションを選択します。**Role** [ロール]範囲は、以下の使用可能なオプションを制御します。

- デバイス の役割:
  - **None**:CLI アクセスは許可されません(デフォルト)。
  - スーパーユーザ -フル アクセス。新しい管理者アカウントと仮想システムを定義できます。スーパーユーザのみが、スーパーユーザ権限を持つ管理者ユーザを作成できます。
  - **superreader**-完全な読み取り専用アクセス。
  - **deviceadmin** –新しいアカウントまたは仮想システムの定義を除くすべての設定に対するフルアクセス。
  - **devicereader** -パスワードプロファイル(アクセス権なし)と管理者アカウントを除くすべての設定に対する読み取り専用アクセス(ログインしたアカウントのみが表示されます)。
- 仮想システム ロール:
  - **None**：アクセスは許可されません (デフォルト)。
  - **vsysadmin**–特定の仮想システムにアクセスして、仮想システムの特定の側面を作成および管理します。静的および動的ルーティング、インターフェイス IP アドレス、IPSec トンネル、VLAN、仮想ワイヤ、仮想ルータ、GRE トンネル、DCHP、DNS プロキシ、QoS、LLDP、またはネットワーク プロファイルを含む、ファイアウォール レベルまたはネットワーク レベルの機能へのアクセスを有効にしません。
  - **vsysreader**：仮想システムの特定の側面に対する特定の仮想システムへの読み取り専用アクセス。静的および動的ルーティング、インターフェイス IP アドレス、IPSec トンネル、VLAN、仮想ワイヤ、仮想ルータ、GRE トンネル、DCHP、DNS プロキシ、QoS、LLDP、またはネットワーク プロファイルを含む、ファイアウォール レベルまたはネットワーク レベルの機能へのアクセスを有効にしません。

STEP 6 | **OK** をクリックしてプロファイルを保存します。

STEP 7 | ロールを管理者に割り当てます。ファイアウォール管理者アカウントの設定を参照してください。

管理者ロール プロファイルの構築例

この例では、潜在的な問題を調査するためにアクセスする必要があるセキュリティ オペレーション センター (SOC) マネージャーの管理者ロール プロファイルを示します。SOC Manager は

ファイアウォールの多くの領域への読み取りアクセスを必要としますが、一般的に書き込みアクセスは必要ありません。この例では、管理者ロール プロファイルの 4 つのタブをすべて取り上げ、各手順で、プロファイルが SOC マネージャへの特定のアクセス領域を有効または無効にする理由を説明します。

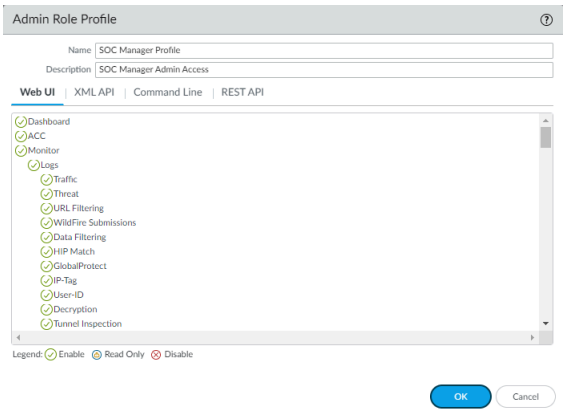
これは、架空の *SOC* マネージャーのプロファイルの例です。管理者が管理する機能と、その職務に必要なアクセス権に基づいて、管理者の管理者ロール プロファイルを設定します。不要なアクセスを有効にしないでください。同じ職務を共有する管理グループごとに、および固有の職務を持つ管理者に対して、別々のプロファイルを作成します。各管理者は、職務を遂行するために必要な正確なレベルのアクセス権を持ち、それ以上のアクセス権を持たなければなりません。

STEP 1 | Web UI アクセス許可を構成します。Web UI 画面の各切り取りでは、Web UI 権限の異なる領域が表示されます。アクセス許可は、Web UI のタブと他のアクションのアクセス許可の順に、ファイアウォール タブごとに表示されます。

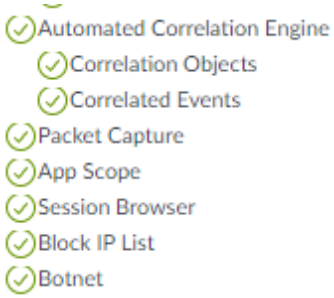
ファイアウォールの **[Dashboard]**、[**ACC**]、および [**Monitor** > **Logs**] 領域には、設定要素は含まれません。すべてのオブジェクトは情報提供用です（すでに読み取られているため、有効と無効を切り替えることができるだけです）。のみ)。SOC マネージャは潜在的な問題を調

査する必要があるため、SOC マネージャはこれらのタブの情報にアクセスする必要があります。

プロファイル名と説明により、プロファイルの目的を簡単に理解できます。この切り取りでは、 **Logs** のアクセス許可がすべて表示されるわけではありませんが、このプロファイルではすべての権限が有効になっています。

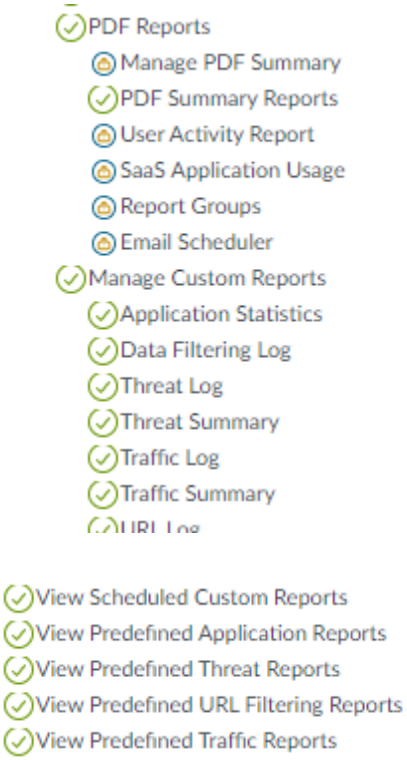


次の切り取りでは、 モニタ タブに、詳細情報のオブジェクトに対するアクセス許可が表示されます。SOC マネージャは、これらのツールを使用して潜在的な問題を調査するため、アクセスが必要です。

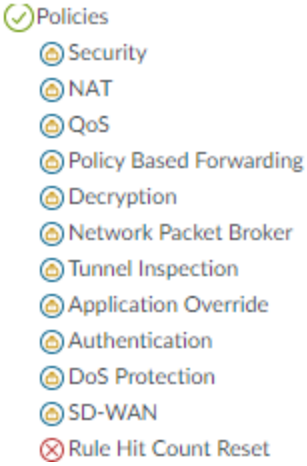


次の 2 つの切り取りは、PDF レポート、カスタムレポート、および事前定義済みレポートの権限を [監視] タブに表示します。SOC マネージャは情報を収集するために PDF レポートにアクセスする必要がありますが、この例では SOC マネージャは レポートを構成するため、アクセスは読み取り専用に設定されます (概要レポートは構成できません)。ただし、SOC Manager は特定の潜在的な問題を調査するためにカスタム レポートを管理する必要があるため、すべてのカスタム レポート (スニップに表示されていないレポートを含む) に対してフル

アクセス権限が付与されます。最後に、SOC マネージャは、潜在的な問題を調査するために事前定義されたレポートにアクセスする必要があります。

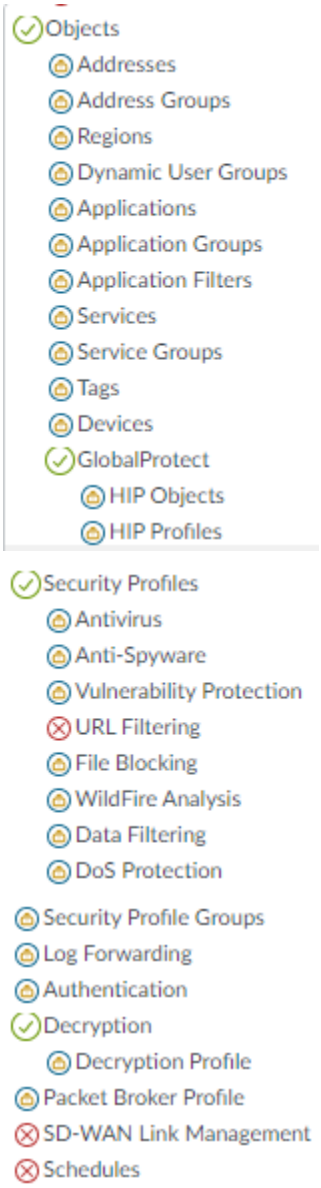


SOC マネージャは調査担当者であり、ファイアウォールを構成する管理者ではないため、 ポリシー タブのアクセス許可は読み取り専用になりますが、ルール ヒット カウントのリセットは例外です。ルールヒットカウントのリセットは SOC マネージャの義務の 1 つではない (また、ヒット カウントを変更すると、他の管理者に悪影響を与えたり混乱したりする可能性があります) ため、アクセスは無効になります。読み取りアクセスにより、SOC マネージャは、SOC マネージャが問題を引き起こした可能性のあるポリシーの構築を調査できます。



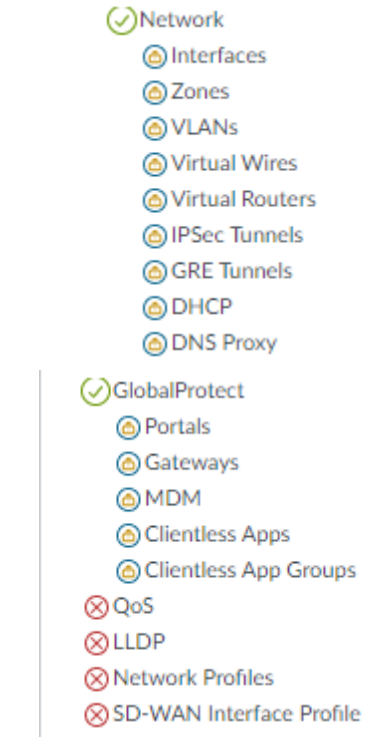
Objects タブのアクセス許可も読み取り専用であるため、SOC マネージャのジョブは構成を必要としないので、構成アクセス許可は割り当てられません。SOC マネージャの職務に含まれていないエリアについては、アクセスは無効になります。この例では、SOC マネージャ

は、**URL** フィルタリング、**SD-WAN** リンク管理、**Schedules**を除くすべてのオブジェクトのオブジェクト構成を調査するための読み取り専用アクセス権を持っています。

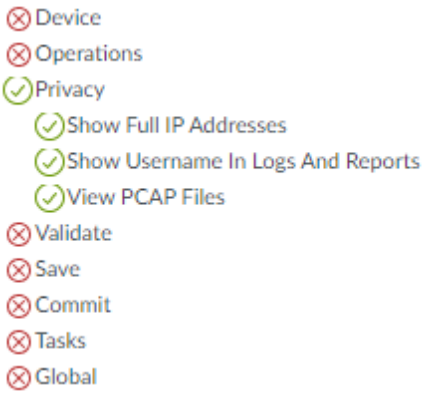


Network タブのアクセス許可の場合、SOC マネージャはオブジェクトを構成する必要はありませんが、問題を調査するために情報が必要な場合があるため、SOC マネージャが調査する必要がある領域に読み取り専用アクセスが割り当てられます。この例では、QoS、LLDP、

ネットワーク プロファイル、または SD-WAN インターフェイス プロファイルに対するアクセスは無効になっています。

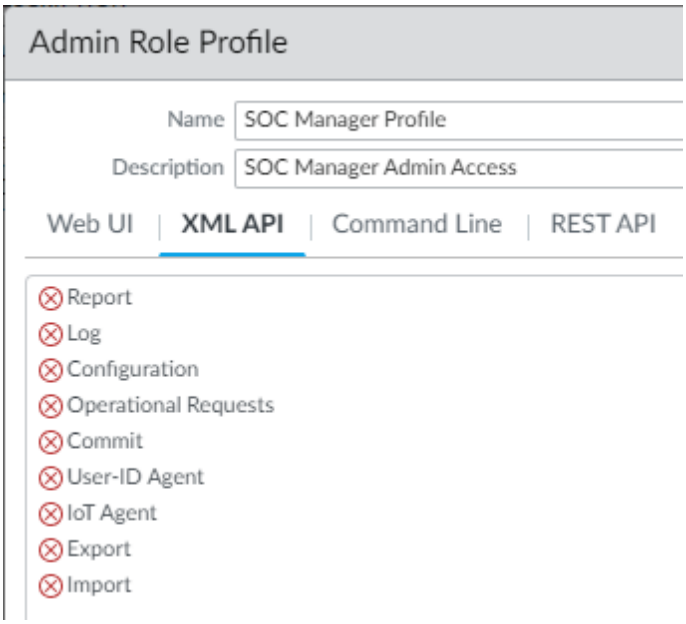


この例では、SOC マネージャーは調査目的で **Device** タブ機能にアクセスする必要がないため、**Device** タブのアクセス許可はすべてブロックされます。また、調査では、コミット アクションや残りのアクションへのアクセスは必要ないので、これらのアクセス許可もブロックされます。



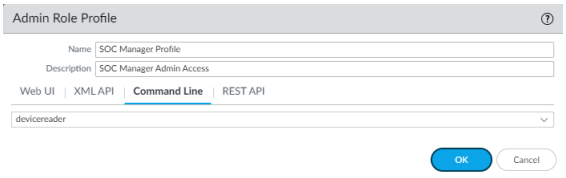
STEP 2 | XML API アクセス許可を構成します。

次の切り取りは、SOC マネージャーが XML API コマンドを使用してファイアウォールにアクセスしないため、SOC マネージャーのすべての XML API アクセス許可が無効になっていることを示しています。



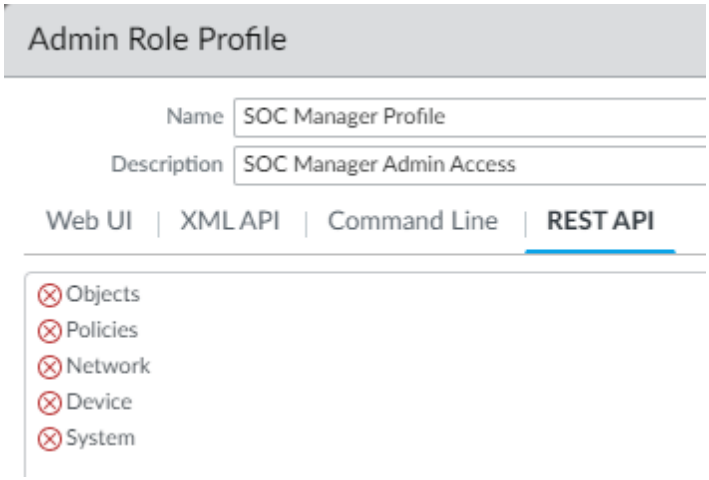
STEP 3 | コマンド ライン (CLI) のアクセス許可を設定します。

SOC Manager はログやその他の監視ツールにアクセスする必要があり、潜在的な問題を調査するために特定の設定を確認できる必要があるため、SOC マネージャのアクセス許可は読み取り専用です。ただし、SOC マネージャはファイアウォールを構成しないので、構成アクセス許可は割り当てられません。SOC マネージャーはパスワード プロファイルや他の管理アカウントにアクセスする必要がないため、アクセス レベルは **superreader** ではなく **devicereader** に設定されています。



STEP 4 | REST API アクセス許可を構成します。

SOC マネージャーは、REST API コマンドを使用してファイアウォールにアクセスしないので、すべての REST API アクセスが無効になります。



管理認証

ファイアウォール管理者には、次のタイプの認証と認可（ロールとアクセス ドメイン割り当て）を設定できます。

認証方式	認可方式	説明
ローカル	ローカル	管理者アカウント認証情報と認証メカニズムがファイアウォールに対してローカルです。ファイアウォールにローカルのユーザー データベースを使用するかどうかにかかわらず、アカウントを定義できます。ローカルのデータベースを使用する利点と欠点については、「ローカル認証」を参照してください。ファイアウォールを使用してロールの割り当てを管理しますが、アクセス ドメインはサポートされていません。詳細は、「ファイアウォール管理者用にローカルあるいは外部認証を設定」を参照してください。
SSH 鍵	ローカル	管理者アカウントはファイアウォールに対してローカルですが、CLI への認証は SSH 鍵に基づきます。ファイアウォールを使用してロールの割り当てを管理しますが、アクセス ドメインはサポートされていません。詳細は、「SSH 鍵ベースで CLI への管理者認証を設定する」を参照してください。
証明書	ローカル	管理者アカウントはファイアウォールに対してローカルですが、Web インターフェイスへの認証はクライアント証明書に基づきます。ファイアウォールを使用してロールの割り当てを管理しますが、アクセス ドメインはサポートされていません。詳細

認証方式	認可方式	説明
		は、「証明書ベース認証を Web インターフェイスに行う設定」を参照してください。
外部サービス	ローカル	ファイアウォールでローカルに定義する管理者アカウントは、多要素認証、SAML、Kerberos、TACACS+、RADIUS、LDAP のいずれかの外部サーバーで定義されているアカウントの参照として動作します。外部サーバーが認証を行います。ファイアウォールを使用してロールの割り当てを管理しますが、アクセス ドメインはサポートされていません。詳細は、「ファイアウォール管理者用にローカルあるいは外部認証を設定」を参照してください。
外部サービス	外部サービス	管理者アカウントは、SAML、TACACS+、RADIUS のいずれかの外部サーバーで定義されます。サーバーが認証と認可を両方とも行います。TACACS+ サーバーまたは RADIUS サーバーではベンダー固有属性（VSA）、SAML サーバーでは SAML 属性を認可用に定義します。PAN-OS は、ファイアウォールで定義した管理者ロール、アクセス ドメイン、ユーザー グループ、および仮想システムに属性をマップします。詳細は、以下を参照してください。 • SAML 認証の設定 • TACACS+ 認証の設定 • RADIUS 認証の設定

管理者アカウントおよび認証の設定

認証プロファイルをすでに設定済み（認証プロファイルおよびシーケンスの設定を参照）、あるいは管理者の認証においてそれが不要な場合は、ファイアウォール管理者アカウントの設定を行う準備ができています。そうでない場合、次にリストアップされている他のいずれかの作業を行い、特定の種類の認証のために管理者アカウントを設定します。

- ファイアウォール管理者アカウントの設定
- ファイアウォール管理者用にローカルあるいは外部認証を設定
- Web インターフェイスへの証明書ベースの管理者認証の設定
- CLI への SSH キーベースの管理者認証の設定
- API キーの有効期間を設定

ファイアウォール管理者アカウントの設定

管理者アカウントは、ファイアウォール管理者のロールおよび認証方法を指定します。ロールの割り当てと認証を行うのに使用するサービスによって、アカウントをファイアウォールに追加するのか、外部サーバーに追加するのか、あるいはその両方なのかが決まります（管理認証を参照）。ローカル ファイアウォール データベースあるいは外部サービスを使用する認証方法の場

合、管理者アカウントを追加する前に認証プロファイルを設定しておく必要があります（管理者アカウントおよび認証の設定を参照）。既に認証プロファイルを設定済み、あるいはファイアウォール データベースを使用せずに<18>ローカル認証</18>を行う場合は、次の作業を行い、ファイアウォール上で管理者アカウントを追加します。

ファイアウォールの管理機能またはレポート機能にアクセスする必要とするユーザーごとに個別の管理アカウントを作成します。これにより、ファイアウォール が許可なく設定されることから適切に保護し、個々の管理者のアクションをログに記録することができます。ファイアウォールやその他のセキュリティ デバイスへの管理アクセスを確実に保護し、攻撃が成功しないようにするため、

管理者アクセスのベストプラクティス に従っていることを確認してください。

STEP 1 | サポートされている管理者アカウントの数を変更します。

通常の動作モードまたは FIPS-CC モード で、ファイアウォールでサポートされる同時管理アカウント・セッションの合計数を構成します。最大 4 つの同時管理アカウント セッションを許可するか、または同時管理アカウント セッションの数を無制限にサポートするようにファイアウォールを構成できます。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して Authentication Settings (認証設定) を編集します。
2. [の最大セッション数] を編集して、すべての管理者アカウントとユーザー アカウントで許可される同時セッションの数 (範囲は **0** ~ **4**) を指定します。

   0 を入力して、無制限の数の管理アカウントをサポートするようにファイアウォールを設定します。
3. 管理アカウントの最大セッション時間 (分単位) を編集します。デフォルトは **720** 分です。
4. **OK** をクリックします。
5. **[コミット]** します。

また、ファイアウォール *CLI* に ログインして、サポートされる同時セッションの合計数を設定することもできます。

```
admin> configure
```

```
admin# set deviceconfig setting management admin-session
 max-session-count <0-4>
```

```
admin# set deviceconfig setting management admin-session
 max-session-time <0, 60-1499>
```

```
admin# commit
```

STEP 2 | **Device (デバイス)** > **Administrators**（管理者） を選択してアカウントを**Add**（追加）します。

STEP 3 | ユーザーの**Name** [名前]を入力します。

アカウントを認証する際にファイアウォールがローカルユーザーデータベースを使用する場合、データベースで指定したアカウントの名前を入力します（ローカル データベースにユーザーグループを追加を参照）。

STEP 4 | **Authentication Profile**（認証プロファイル）を選択するか、管理者の認証を複数設定している場合はシーケンスを選択します。

そのアカウントについて、ファイアウォールがローカルユーザーデータベースを使わずにローカル認証を行う場合は、**None (なし)**（デフォルト）を選択して **Password (パスワード)** を入力します。

STEP 5 | <60>Administrator Type</60> [管理者タイプ]を選択します。

ユーザーにカスタム ロールを設定している場合は、**Role Based**（ロール ベース）を選択し、管理者ロールの **Profile**（プロファイル）を選択します。それ以外の場合は、<67>Dynamic</67>[動的]（デフォルト）を選択してダイナミック ロールを選択します。ダイナミック ロールが**virtual system administrator**[仮想システム管理者]の場合、仮想システム管理者が管理できる仮想システムを追加（複数可）します。

STEP 6 | （任意）ファイアウォールがローカルユーザーデータベースを使用せずにローカルで認証を行う管理者用の **Password Profile (パスワード プロファイル)** を選択します。詳細についてはパスワードプロファイルの定義を参照してください。

STEP 7 | **OK**、**Commit (コミット)** の順にクリックします。

ファイアウォール管理者用にローカルあるいは外部認証を設定

ローカル認証と外部認証サービスを使用し、ファイアウォールにアクセスする管理者を認証できます。これらの認証方式では、ユーザー名とパスワードを入力するためのログイン ページなど、1 つ以上の認証チャレンジに応答することを管理者に要求します。

外部サービスを使用して認証と承認（ロールおよびアクセス ドメインの割り当て）の両方を管理する場合は、以下を参照してください。

- SAML 認証の設定
- TACACS+ 認証の設定
- RADIUS 認証の設定

Web インターフェイスへの証明書ベースの管理者認証の設定およびCLI への SSH キーベースの管理者認証の設定を行うことで、チャレンジレスポンス機構を使わずに管理者を認証することができます。

STEP 1 | （外部認証のみ）ファイアウォールが外部サービスに接続して管理者を認証する機能を有効化します。

サーバー プロファイルを設定します。

- RADIUS サーバー プロファイルを追加します。

  ファイアウォールが RADIUS を通じて マルチ ファクター認証（MFA）サービスを統合する場合は、RADIUS サーバープロファイルを追加する必要があります。このケースでは、MFA サービスがすべての認証要素（チャレンジ）を提供します。ファイアウォールがベンダーの API を通じて MFA サービスを統合する場合でも、最初の要素で RADIUS サーバープロファイルを使用できますが、追加の要素については MFA サーバープロファイルが必要になります。
- MFA サーバープロファイルを追加します。
- TACACS+サーバー プロファイルを追加します。
- SAML IdP サーバー プロファイルを追加します。Kerberos シングル サインオン（SSO）と SAML SSO を組み合わせることはできません。どちらか片方の SSO サービスのみを使用できます。
- Kerberosサーバー プロファイルを追加します。
- LDAP サーバー プロファイルを追加します。

STEP 2 | （ローカル データベース認証のみ）ファイアウォールのローカルにあるユーザーデータベースを設定します。

1. ユーザーアカウントをローカル データベースに追加します。
2. （任意）ユーザーグループをローカル データベースに追加します。

STEP 3 | （ローカル認証のみ）パスワードの複雑さおよび有効期限を設定します。

この設定によって攻撃者がパスワードを推定することが難しくなるため、ファイアウォールへの不正なアクセスを防止するのに役立ちます。

1. パスワードの複雑性をグローバルに定義し、すべてのローカル管理者の有効期限を設定します。パスワードの代わりにパスワードのハッシュを指定したローカル データベース アカウントには設定が適用されません（ローカル認証を参照）。

   1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して Minimum Password Complexity (パスワード複雑性) 設定を編集します。
   2. **Enabled**（有効）を選択します。
   3. パスワード設定を定義し、**OK** をクリックします。

2. パスワード プロファイルを定義します。

   グローバルなパスワード有効期限設定をオーバーライドする管理者アカウントにプロファイルを割り当てます。プロファイルは、ローカル データベースに関連付けられていないアカウントでのみ利用できます（ローカル認証を参照）。

   1. **Device (デバイス)** > **Password Profiles (パスワード プロファイル)** を選択してプロファイルを **Add (追加)** します。
   2. プロファイルを識別する **Name**（名前）を入力します。
   3. パスワードの有効期限設定を行い、**OK** をクリックします。

STEP 4 | （Kerberos SSO のみ）Kerberos キータブを作成します。

キータブは、ファイアウォールの Kerberos アカウント情報が含まれるファイルです。Kerberos SSO をサポートするには、ネットワークに Kerberos インフラストラクチャが必要です。

STEP 5 | 認証プロファイルを設定します。

管理者アカウントが複数のタイプのサーバーにかけて保存されている場合、各タイプの認証プロファイルを作成し、すべてのプロファイルを認証シーケンスに追加できます。

認証プロファイルおよびシーケンスの設定を行います。認証プロファイルで、認証サービスの **Type**（タイプ）および関連する設定を指定します。

- 外部サービス – 外部サービスの **Type**（タイプ）を選択し、その外部サービス用に作成した **Server Profile**（サーバー プロファイル）を選択します。
- ローカル データベース認証–**Type (タイプ)** を **Local Database (データベース)** に設定します。
- データベースを使わないローカル認証–**Type (タイプ)** を **None (なし)** に設定します。
- **Kerberos SSO**–**Kerberos Realm (Kerberos レルム)** を指定し、**Kerberos Keytab (Kerberos キータブ)** を **Import (インポート)** します。

STEP 6 | 認証プロファイルあるいは認証シーケンスを管理者アカウントに割り当てます。

1. ファイアウォール管理者アカウントの設定を行います。
   - **Authentication Profile**（認証プロファイル）または設定したシーケンスを割り当てます。
   - （ローカル データベース認証のみ）ローカル データベースに追加したユーザーアカウントの **Name (名前)** を指定します。
2. 変更をコミットします。
3. （任意）認証サーバー接続のテストを行い、ファイアウォールが認証プロファイルを使用して管理者を認証できることを確認します。

Web インターフェイスへの証明書ベースの管理者認証の設定

ファイアウォールの Web インターフェイスに対するパスワード ベース認証のより安全な方法として、ファイアウォールに対してローカルな管理者アカウントの証明書ベースの認証を設定できます。証明書ベースの認証では、パスワードの代わりにデジタル署名の交換と検証が行われます。

いずれかの管理者の証明書ベースの認証を設定すると、ファイアウォールのすべての管理者のユーザー名/パスワード ログインが無効になり、その後管理者がログインするには証明書が必要になります。

STEP 1 | ファイアウォールの認証局（CA）証明書を生成します。

この CA 証明書を使用して、各管理者のクライアント証明書に署名します。

自己署名ルート CA 証明書の作成を行います。

あるいは、エンタープライズ *CA* あるいはサードパーティ *CA* が提供する証明書および秘密鍵のインポートを行います。

STEP 2 | Web インターフェイスへのアクセスをセキュリティ保護するための証明書プロファイルを設定します。

証明書プロファイルの設定を行います。

- **Username Field** [ユーザー名欄]を**Subject** [サブジェクト] に設定します。
- CA Certificates [CA 証明書]セクションで、先ほど作成またはインポートした **CA Certificate** [CA 証明書]を **Add** [追加]します。

STEP 3 | 管理者の認証に証明書プロファイルを使用するようにファイアウォールを設定します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して Authentication Settings (認証設定) を編集します。
2. 管理者の認証用に作成した**Certificate Profile**[証明書プロファイル]を選択し、**OK**をクリックします。

STEP 4 | クライアント証明書の認証を使用するように管理者アカウントを設定します。

ファイアウォールの Web インターフェイスにアクセスする各管理者に対してファイアウォールの管理者アカウントを設定し、**Use only client certificate authentication (**クライアント証明書による認証のみ使用**)** を選択します。

エンタープライズ CA が生成したクライアント証明書を既にデプロイしている場合は、「ステップ 」に進んでください8。それ以外の場合は、ステップ 5 に進みます。

STEP 5 | 各管理者のクライアント証明書を生成します。

証明書の生成を行います。**Signed By**[署名者]のドロップダウンリストで、自己署名のルートCA証明書を選択します。

STEP 6 | クライアント証明書をエクスポートします。

1. 証明書および秘密鍵のエクスポートを行います。
2. 変更をコミットします。ファイアウォールが再起動し、ログイン セッションが終了します。その後、管理者は生成されたクライアント証明書のあるクライアント システムからのみ Web インターフェイスにアクセスできます。

STEP 7 | Web インターフェイスにアクセスする各管理者のクライアント システムにクライアント証明書をインポートします。

Web ブラウザのドキュメントを参照してください。

STEP 8 | 管理者が Web インターフェイスにアクセスできることを確認します。

1. クライアント証明書があるコンピュータのブラウザでファイアウォールの IP アドレスを開きます。
2. 入力画面が表示されたら、インポートした証明書を選択して **OK** をクリックします。ブラウザに証明書警告が表示されます。
3. ブラウザの例外リストに証明書を追加します。
4. **Login**（ログイン）をクリックします。ユーザー名やパスワードのプロンプトは表示されずに Web インターフェイスが表示されます。

CLI への SSH キーベースの管理者認証の設定

Palo Alto Networks ファイアウォールの CLI へのアクセスにセキュア シェル（SSH）を使用する管理者の場合、SSH キーによってパスワードよりも安全な認証方式が提供されます。SSH キーでは、ブルート フォース攻撃のリスクがほぼなくなり、2 要素認証（鍵とパスフレーズ）のオプションが提供され、ネットワーク上でパスワードが送信されることはありません。さらに、CLI にアクセスするための自動スクリプトも有効になります。

STEP 1 | SSH キー生成ツールを使用して、管理者のクライアント システムで非対称のキー ペアを作成します。

サポートされているキー フォーマットは、IETF SECSH と Open SSH です。サポートされているアルゴリズムは、DSA（1,024 ビット）と RSA（768 ～ 4096 ビット）です。

キー ペアを生成するコマンドは、SSH クライアントのドキュメントを参照してください。

公開鍵と秘密鍵は個別のファイルです。ファイアウォールがアクセスできる場所に両方のファイルを保存します。セキュリティ強化のため、パスフレーズを入力して、秘密鍵を暗号化します。ログイン中に、ファイアウォールによってこのパスフレーズのプロンプトが管理者に表示されます。

STEP 2 | 公開鍵の認証を使用するように管理者アカウントを設定します。

1. ファイアウォール管理者アカウントの設定を行います。
   - SSH キー認証が失敗した場合にフォールバックとして使用する認証方式を設定します。管理者の **Authentication Profile** [認証プロファイル]を設定している場合は、ドロップダウンリストでそのプロファイルを選択します。**None** [なし]を選択した場合、**Password** [パスワード]と **Confirm Password** [パスワードの確認]を入力する必要があります。
   - **Use Public Key Authentication (SSH)** (公開鍵認証（**SSH**）の使用) を選択し、**Import Key** (キーのインポート) を行い、先ほど生成した公開鍵を **Browse** (参照) して **OK** をクリックします。
2. 変更を **Commit** (コミット)します。

STEP 3 | ファイアウォールへの認証に秘密鍵を使用するように SSH クライアントを設定します。

管理者のクライアント システムでこのタスクを実行します。この手順は、SSH クライアントのドキュメントを参照してください。

STEP 4 | 管理者が SSH キー認証を使用してファイアウォール CLI にアクセスできることを確認します。

1. 管理者のクライアント システムのブラウザを使用して、ファイアウォールの IP アドレスに移動します。
2. 管理者としてファイアウォール CLI にログインします。ユーザー名を入力すると、以下の出力が表示されます（キー値は例です）。

```
Authenticating with public key “dsa-key-20130415”
```

3. プロンプトが表示されたら、キーの作成時に定義したパスフレーズを入力します。

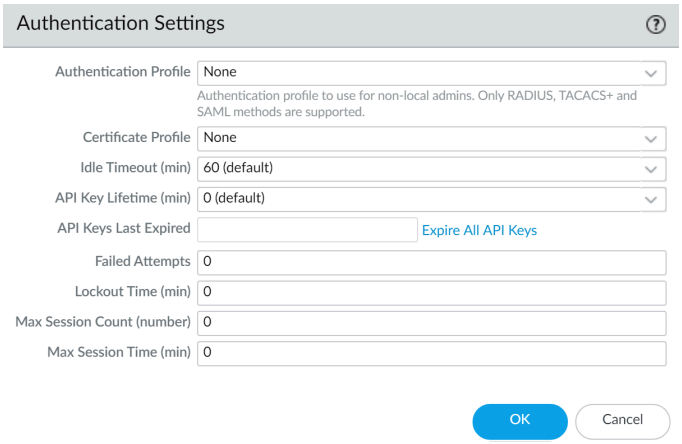
API キーの有効期間を設定

ファイアウォールおよび Panorama の API キーを使用すれば、XML API および REST API に対する API 呼び出しを認証できます。これらのキーはセキュリティにとって欠かせない ファイアウォールおよび Panorama へのアクセス権限を与えるため、API キーの有効期間を指定して定期的にキーを変えることがベストプラクティスになります。キーの有効期間を指定したら、API キーを再生成する際に各キーが一意のものになります。

キーの有効期間を設定して新しいキーを定期的に再生成することを求めるだけでなく、キーのセキュリティが破られた場合に現行のすべての有効な API キーを失効させることもできます。キーを失効すると、現行のすべての有効なキーが無効になります。

STEP 1 | **Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理）を選択します。

STEP 2 | 認証設定を編集して **API Key Lifetime (min) (API** キーの有効期間 **(分))** を指定します。

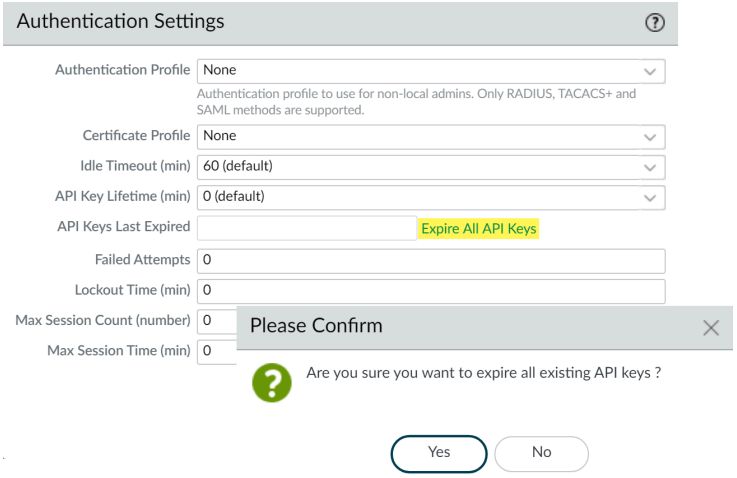


API キーの有効期間を設定して攻撃を防ぎ、意図しない漏洩の際のダメージを減らします。API キーの有効期間はデフォルトで 0 に設定されており、これはキーが失効しないことを示します。キーが必ず頻繁に変更され、一意のキーが再生成されるようにするには、1～525600 分の範囲で有効な期間を指定する必要があります。企業の監査およびコンプライアンス ポリシーを参照し、API キーの有効期間をどのように決定すべきか判断してください。

STEP 3 | 変更を **Commit**（コミット）します。

STEP 4 | (すべての API キーを失効させるには)**Expire all API Keys (**すべての **API** キーを失効**)** を選択して現在有効な API キーをリセットします。

キーの有効期間を設定したばかりの時点で、新しい条件を満たすためにすべての API キーをリセットしたい場合、すべての既存のキーを失効させることができます。



確定するとキーが失効され、**API Keys Last Expired**のタイムスタンプを見ることができます。

管理者のアクティビティの追跡を構成する

ファイアウォール Web インターフェイスと CLI で管理者のアクティビティを追跡し、ファイアウォール全体のアクティビティをリアルタイムで報告します。管理者アカウントが侵害されたと思われる理由がある場合は、この管理者アカウントが Web インターフェイスを通じて移動した場所や、管理者が実行した操作コマンドの履歴がすべてあるため、詳細な分析を行い、侵害された管理者が行ったすべての操作に対応できます。

イベントが発生すると、管理者が Web インターフェイスをナビゲートしたり、CLI で 操作コマンド が実行されるたびに、監査ログが生成され、指定された syslog サーバーに転送されます。実行されるナビゲーションまたは表彰ごとに、監査ログが生成されます。たとえば、新しい住所オブジェクトを作成する場合を考えます。**Objects** をクリックすると監査ログが生成され、次に [アドレス] をクリックすると 2 番目の監査ログが生成されます。

監査ログは syslog サーバに転送された syslog としてのみ表示され、ファイアウォール Web インターフェイスでは表示できません。監査ログは、syslog サーバーにのみ転送でき、Cortex Data Lake (CDL) に転送できず、ファイアウォール上にローカルに保存されません。

STEP 1 | ファイアウォール上の管理者アクティビティの監査ログを転送するように syslog サーバ プロファイルを設定します。

この手順は、ファイアウォール上の管理者のアクティビティを追跡するための監査ログを正常に保存するために必要です。

1. ファイアウォール Web インターフェイス にログインします。
2. syslog サーバー プロファイル を構成します。

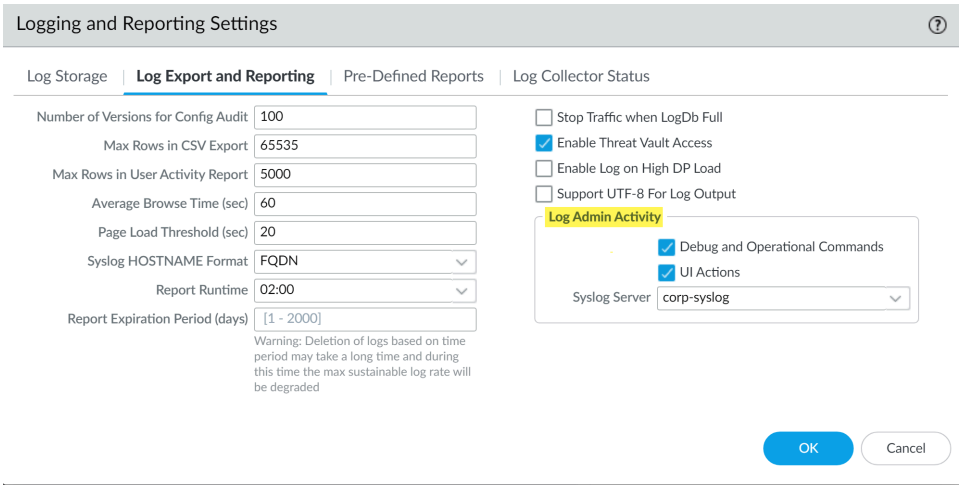
STEP 2 | 管理者のアクティビティの追跡を構成します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して Logging and Reporting Settings (ロギングおよびレポート設定) を編集します。
2. **Log Export** と **Reporting** を選択します。
3. [ログ管理アクティビティ] セクションで、追跡する管理者アクティビティを構成します。
   - 操作コマンド- 管理者が CLI で操作コマンドまたはデバッグコマンドを実行するか、Web インターフェイスから起動された操作コマンドを実行するときに監査ログを生成します。PAN-OS の操作コマンドとデバッグ コマンドの完全なリストについては、CLI 操作コマンド階層 を参照してください。
   - **UI Actions**- 管理者が Web インターフェイスを移動するときに監査ログを生成します。これには、構成タブ間のナビゲーションと、タブ内の個々のオブジェクトのナビゲーションが含まれます。

     たとえば、管理者が **ACC** から **Policies** タブに移動すると、監査ログが生成されます。さらに、管理者が **>**オブジェクト > **Addresses** から **Objects<** > タグ に移動すると>、監査ログが生成されます。

- **Syslog Server**- 監査ログを転送するターゲット syslog サーバー プロファイルを選択します。

4. **[OK]** をクリックします。
5. コミットを選択します。



リファレンス：Web インターフェイス管理者のアクセス権限

ファイアウォール全体または（複数の仮想システムをサポートするプラットフォーム上の）1 つ以上の仮想システムの権限を設定できます。その **Device** [デバイス]または **Virtual System** [仮想システム]の指定内で、動的管理者ロールと関連付けられた固定権限よりも詳細なカスタム管理者ロールの権限を設定できます。

詳細レベルで権限を設定することにより、下位レベルの管理者が特定の情報にアクセスできないようにすることができます。ファイアウォール管理者（ファイアウォールの管理者アカウントを設定を参照）、Panorama 管理者、または Device Group and Template (デバイス グループとテンプレート) 管理者（Panorama 管理者ガイドを参照）のカスタム ロールを作成できます。管理者ロールはカスタムロール ベースの管理者アカウントに割り当てます。また、単体あるいは複数の仮想システムを割り当てることも可能です。以下のトピックでは、カスタム管理者ロールに設定可能な権限について説明します。

- Web インターフェイスのアクセス権限
- Panorama Web インターフェイスのアクセス権限

Web インターフェイスのアクセス権限

ロールベース管理者が Web インターフェイスの特定のタブにアクセスできないようにする場合は、そのタブを無効にし、管理者が自分に関連付けられているロールベースの管理アカウントを使用してログインしたときにそのタブが表示されないようにすることができます。たとえば、操作スタッフ用に **Device**[デバイス] および **Network**[ネットワーク] タブへのアクセスのみを許可する管理者ロール プロファイルを作成し、セキュリティ管理者用に **Object**[オブジェクト]、**Policy**[ポリシー]、および **Monitor**[監視] タブへのアクセスを許可する別の管理者ロール プロファイルを作成することができます。

管理者ロールは、 **Device**（デバイス）または **Virtual System**（仮想システム）ラジオ ボタンで定義した通りに、**Device**（デバイス）レベルまたは **Virtual System**（仮想システム）レベルで適用できます。**Virtual System**（仮想システム）を選する場合、このプロファイルに割り当てられた管理者は割り当てられている仮想システムに制限されます。さらに、管理者が使用可能なタブは **Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス） > **Virtual Systems**（仮想システム）のみで、 **Global**（グローバル）タブは使用できません。

次のトピックでは、管理者ロール権限を Web インターフェイスのさまざまな部分に設定する方法について説明します。

- Web インターフェイスのタブへのアクセスを定義
- [Monitor] タブに対する詳細なアクセス権限の付与
- [Policies] タブに対する詳細なアクセス権限の付与
- [Objects] タブに対する詳細なアクセス権限の付与
- [Network] タブに対する詳細なアクセス権限の付与
- [Device] タブに対する詳細なアクセス権限の付与

- 管理者ロール プロファイルでのユーザーのプライバシー設定の定義
- コミットおよび検証機能への管理者アクセスの制限
- グローバル設定への詳細なアクセス権限の指定
- Panorama タブに対する詳細なアクセス権限の付与
- 操作設定へのきめ細かなアクセスを提供する

Web インターフェイスのタブへのアクセスを定義

以下の表に、管理者ロール プロファイルに割り当てることができるトップ レベルのアクセス権限の説明を示します（**Device (デバイス)** > **Admin Roles (管理者ロール)**）。Web インターフェイスのトップレベル タブにて、読込のみのアクセス権限を有効化、無効化、定義できます。

アクセス レベル	の意味	**Enable** [有効化]	読み取り専用	無効化
Dashboard（ダッシュボード）	**Dashboard** [ダッシュボード]タブへのアクセスを制御します。この権限を無効にすると、その管理者にはこのタブが表示されなくなり、Dashboard ウィジェットのいずれにもアクセスできません。	あり。	無し	あり。
ACC	アプリケーション コマンド センター（ACC）へのアクセスを制御します。この権限を無効にすると、**ACC** タブが Web インターフェイスに表示されなくなります。ACC へのアクセス権限を与えると同時にユーザーのプライバシーを守るには、**Privacy (プライバシー)** > **Show Full IP Addresses (完全 IP アドレスの表示)** オプションまたは **Show User Names In Logs And Reports (ログおよびレポート内のユーザー名の表示)** オプションを無効にすることができます。	あり。	無し	あり。
監視	**Monitor**[監視] タブへのアクセスを制御します。この権限を無効にすると、その管理者には **Monitor**[監視]タブが表示されなくなり、ログ、パケット キャプチャ、セッション情報、レポート、またはアプリケーション スコープのいずれにもアクセスできません。管理者が表示できるモニタリング情報をより詳細に制御するには、Monitor (監視) オプションを有効にしたままで、監視タブに対する詳細なアクセス権限の付与での説明に従ってタブ上	あり。	無し	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	の特定のノードを有効または無効にします。			
レポートを生成	**Policies**[ポリシー] タブへのアクセスを制御します。この権限を無効にすると、その管理者には **Policies** [ポリシー]タブが表示されなくなり、どのポリシー情報にもアクセスできません。たとえば、特定のタイプのポリシーへのアクセスを有効にする、またはポリシー情報への読み取り専用アクセスを有効にするなど、管理者が表示できるポリシー情報をより詳細に制御するには、**Policies (**ポリシー**)** オプションを有効にしたままで、ポリシータブに対する詳細なアクセス権限の付与での説明に従ってタブ上の特定のノードを有効または無効にします。	あり。	無し	あり。
オブジェクト	**Objects**[オブジェクト] タブへのアクセスを制御します。この権限を無効にすると、その管理者には **Objects**[オブジェクト] タブが表示されなくなり、オブジェクト、セキュリティ プロファイル、ログ転送プロファイル、復号プロファイル、またはスケジュールのいずれにもアクセスできません。管理者が表示できるオブジェクトをより詳細に制御するには、**Objects (**オブジェクト**)** オプションを有効にしたままで、オブジェクト タブに対する詳細なアクセス権限の付与での説明に従ってタブ上の特定のノードを有効または無効にします。	あり。	無し	あり。
Network（ネットワーク）	**Network**[ネットワーク] タブへのアクセスを制御します。この権限を無効にすると、その管理者には **Network**[ネットワーク] タブが表示されなくなり、インターフェイス、ゾーン、VLAN、バーチャル ワイヤー、仮想ルーター、IPSec トンネル、DHCP、DNS プロキシ、GlobalProtect、QoS 設定情報、またはネットワーク プロファイルのいずれにもアクセスできません。管理者が表示できるオブジェクトをより詳細に制御	あり。	無し	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	するには、**Network (ネットワーク)** オプションを有効にしたままで、ネットワーク タブに対する詳細なアクセス権限の付与での説明に従ってタブ上の特定のノードを有効または無効にします。			
Device（デバイス）	**Device**[デバイス] タブへのアクセスを制御します。この権限を無効にすると、その管理者には **Device** [デバイス]タブが表示されなくなり、ユーザー ID、高可用性、サーバー プロファイル、または証明書設定情報などのファイアウォール全体の設定情報のいずれにもアクセスできません。管理者が表示できるオブジェクトをより詳細に制御するには、**Objects (オブジェクト)** オプションを有効にしたままで、デバイス タブに対する詳細なアクセス権限の付与での説明に従ってタブ上の特定のノードを有効または無効にします。 ***Device**[デバイス] タブへのフル アクセス権限を有効にしていても、**Admin Roles**[管理者ロール] または **Administrators**[管理者] ノードに対するロールベース管理者のアクセス権限を有効にすることはできません。*	あり。	無し	あり。

[Monitor] タブに対する詳細なアクセス権限の付与

管理者が表示できる **Monitor** [監視]タブのエリアを、そのすべてではなく一部に制限したい場合もあります。たとえば、管理者の操作を、機密性の高いユーザー データが含まれていない設定およびシステム ログのみに制限する場合などです。管理者ロール定義のこのセクションでは管理者が表示できる **Monitor** [監視]タブのエリアを指定しますが、このセクションに含まれる権限を、ログやレポートでユーザー名を表示する権限を無効にするなどの privacy [専用]の権限と組み合わせることもできます。ただし、管理者ロールでユーザー名と IP アドレスの表示を無効にしても、システム生成のレポートにはユーザー名と IP アドレスが表示されます。したがって、管理者がユーザーの個人情報を一切表示することができないようにする場合は、以下の表に示す詳細に従って特定のレポートへのアクセス権限を無効にします。

以下の表に、**Monitor** [監視]タブのアクセス レベル、およびそのレベルで設定可能な管理者ロールの一覧を示します。

*Device Group and Template [デバイス グループとテンプレート]*ロールは、そのロールに割り当てられたアクセス ドメイン内にあるデバイス グループのログ データのみを表示できます。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
監視	**Monitor**[監視] タブへのアクセス権限を有効または無効にします。無効にすると、その管理者には、このタブとこのタブに関連付けられているログまたはレポートのすべてが表示されなくなります。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
ログ	すべてのログ ファイルへのアクセス権限を有効または無効にします。この権限を有効にしたままで、管理者に表示されないようにする特定のログを無効にすることもできます。1 つ以上のログに対するアクセス権限を与えると同時にユーザーのプライバシーを守るには、**Privacy (プライバシー)** > **Show Full IP Addresses (完全 IP アドレスの表示)** オプションまたは **Show User Names In Logs And Reports (ログおよびレポート内のユーザー名の表示)** オプションを無効にすることができます。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
トラフィック	管理者がトラフィック ログを表示できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
脅威	管理者が脅威ログを表示できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
URL フィルタリング	管理者が URL フィルタリング ログを表示できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
WildFire への送信	管理者がWildFireログを表示できるかどうかを指定します。これらのログは、WildFire サブスクリプションを持っている場合にのみ表示できます。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
データ フィルタリング	管理者がデータ フィルタリング ログを表示できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
HIP マッチ	管理者が HIP マッチ ログを表示できるかどうかを指定します。HIP マッチ ログは、GlobalProtect ライセンス (サブスクリプション) を持っている場合にのみ表示されます。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
グローバルな保護	管理者が GlobalProtect ログを表示できるかどうかを指定します。これらのログは、GlobalProtect ライセンス (サブスクリプション) を持っている場合にのみ表示されます。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
User-ID	管理者が User-ID ログを表示できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
GTP	モバイルネットワーク事業者が GTP ログを見ることができるかどうかを指定します。	firewall:あり。 Panorama：あり。	あり。	無し	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
		デバイス グループ/テンプレート：あり。			
トンネル検査	管理者がトンネル検査ログを表示できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
SCTP	モバイルネットワーク事業者が Stream Control Transmission Protocol (SCTP) ログを見ることができるかどうかを指定します。 *Panorama* およびデバイス グループ/テンプレートの *SCTP* ログ、カスタム レポート、または事前定義レポートへの管理者アクセスを制御する前に、*Panorama* 上で *SCTP* を有効にする必要があります（***Device***（デバイス） > ***Setup***（セットアップ） > ***Management***（管理））。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
設定	管理者が設定ログを表示できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：無し	あり。	無し	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
システム<:so>システム	管理者がシステム ログを表示できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：無し	あり。	無し	あり。
アラーム	管理者がシステム生成のアラームを表示できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
認証	管理者が認証ログを表示できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：無し	あり。	無し	あり。
自動相関エンジン	相関オブジェクトおよびファイアウォールで生成された相関イベント ログへのアクセス権限を有効または無効にします。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
相関オブジェクト	管理者が、相関オブジェクトを表示および有効化/無効化できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
相関されたイベント	管理者が相関イベントを表示および有効化/無効化できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
パケット キャプチャ	管理者が **Monitor** [監視]タブでパケット キャプチャ（pcap）を表示できるかどうかを指定します。パケット キャプチャは生のフロー データであり、そのためユーザーの IP アドレスが含まれている可能性があることに注	firewall:あり。 Panorama：無し デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	意してください。**Show Full IP Addresses**[完全 IP アドレスの表示] 権限を無効にしても pcap 内の IP アドレスが識別不能になることはないため、ユーザーのプライバシーの侵害が懸念される場合はパケット キャプチャ権限を無効にしてください。				
アプリケーション スコープ	管理者がアプリケーション スコープの可視化ツールと分析ツールを表示できるかどうかを指定します。アプリケーション スコープを有効にすると、**App Scope**[アプリケーション スコープ] のすべてのグラフに対するアクセス権限が有効になります。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
セッション ブラウザ	ファイアウォール上で現在実行中のセッションを管理者が参照およびフィルタリングできるかどうかを指定します。セッション ブラウザには生のフローデータが表示され、そのためユーザーの IP アドレスが含まれている可能性があることに注意してください。**Show Full IP Addresses**[完全 IP アドレスの表示] 権限を無効にしてもセッション ブラウザ内の IP アドレスが識別不能になることはないため、ユーザーのプライバシーの侵害が懸念される場合は **Session Browser**[セッション ブラウザ] 権限を無効にしてください。	firewall:あり。 Panorama：無し デバイス グループ/テンプレート：無し	あり。	無し	あり。
Block IP List ブロック IP リスト	管理者がブロックリストを表示（Enable あるいは Read Only）したり、リストの項目を削除（Enable）したりできるかどうか指定します。この設定を無効	firewall:あり。 Panorama：Context Switch UI (コンテキス	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	にすると、管理者はブロックリストを閲覧し足り、項目を削除したりできなくなります。	ト切り替え UI) 以下：あり。 テンプレート:あり。			
ボットネット	管理者がボットネット分析レポートを生成および表示できるか、またはボットネット レポートを読み取り専用モードで表示できるかどうかを指定します。**Show Full IP Addresses**[完全 IP アドレスの表示] 権限を無効にしてもスケジュール設定されたボットネット レポート内の IP アドレスが識別不能になることはないため、ユーザーのプライバシーの侵害が懸念される場合は **Botnet**[ボットネット] 権限を無効にしてください。	firewall:あり。 Panorama：無し デバイス グループ/テンプレート：無し	はい	はい	あり。
PDF レポート	すべての PDF レポートへのアクセス権限を有効または無効にします。この権限を有効にしたままで、管理者に表示されないようにする特定の PDF レポートを無効にすることもできます。1 つ以上のログに対するアクセス権限を与えると同時にユーザーのプライバシーを守るには、**Privacy (プライバシー)** > **Show Full IP Addresses (完全 IP アドレスの表示)** オプションまたは **Show User Names In Logs And Reports (ログおよびレポート内のユーザー名の表示)** オプションを無効にすることができます。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
PDF サマリーの管理	管理者が、PDF サマリー レポートの定義を表示、追加、または削除できるかどうかを指定します。読み取り専用アクセス権限を持っている場合、管理	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	者は、PDF サマリー レポートの定義を表示できますが、追加または削除することはできません。このオプションを無効にすると、管理者は、レポートの定義を表示したり、それらの定義を追加/削除したりすることができなくなります。				
PDF サマリー レポート	管理者が生成された PDF サマリー レポートを **Monitor (監視)** > **Reports (レポート)** で表示できるかどうかを指定します。このオプションを無効にすると、**Reports**[レポート] ノードに **PDF Summary Reports**[PDF サマリー レポート] カテゴリが表示されなくなります。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
ユーザー アクティビティ レポート	管理者が、ユーザー アクティビティ レポートの定義を表示、追加、または削除し、そのレポートをダウンロードすることができるかどうかを指定します。読み取り専用アクセス権限を持っている場合、管理者は、ユーザー アクティビティ レポートの定義を表示できますが、追加、削除、またはダウンロードすることはできません。このオプションを無効にすると、管理者はこのカテゴリの PDF レポートを表示することができません。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	はい	はい	あり。
SaaS アプリケーション使用率レポート	管理者が、SaaSアプリケーションの利用状況レポートを表示、追加、または削除できるかどうかを指定します。読み取り専用アクセス権限を持っている場合、管理者は、SaaSアプリケーションの利用状況レポートを表示できますが、追加または削除	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	することはできません。このオプションを無効にすると、管理者は、レポートの定義を表示したり、それらの定義を追加/削除したりすることができなくなります。				
レポート グループ	管理者が、レポート グループの定義を表示、追加、または削除できるかどうかを指定します。読み取り専用アクセス権限を持っている場合、管理者は、レポート グループの定義を表示できますが、追加または削除することはできません。このオプションを無効にすると、管理者はこのカテゴリの PDF レポートを表示することができません。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	はい	はい	あり。
電子メール スケジューラ	管理者が電子メール用のレポート グループをスケジュール設定できるかどうかを指定します。電子メールで送信される生成レポートには、**Privacy (プライバシー)** > **Show Full IP Addresses (完全 IP アドレスの表示)** オプションまたは **Show User Names In Logs And Reports (ログおよびレポート内のユーザー名の表示)** オプションを無効にしても除外されないユーザーの機密データが含まれている可能性があり、また管理者がアクセス権限を持っていないログ データが表示される可能性もあるため、ユーザーのプライバシーを守る必要がある場合は、**Email Scheduler (電子メール スケジューラ)** オプションを無効にしてください。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
カスタム レポートの管理	すべてのカスタム レポート機能へのアクセス権限を有効または無効にします。この権限を有効にしたままで、管理者が表示できないようにする特定のカスタム レポート カテゴリを無効にすることもできます。1 つ以上のログに対するアクセス権限を与えると同時にユーザーのプライバシーを守るには、**Privacy (プライバシー)** > **Show Full IP Addresses (完全 IP アドレスの表示)** オプションまたは **Show User Names In Logs And Reports (ログおよびレポート内のユーザー名の表示)** オプションを無効にすることができます。 要求時に実行されるレポートではなく、スケジュール設定されているレポートには、*IP* アドレスとユーザー情報が表示されます。この場合は、必ず該当するレポート エリアへのアクセスを制限してください。また、カスタム レポート機能では、管理者ロールから除外されているログに含まれているログ データを含むレポートの生成は制限されません。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
アプリケーション統計	管理者が、アプリケーション統計データベースからのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
データ フィルタリング ログ	管理者が、データ フィルタリング ログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
脅威ログ	管理者が、脅威ログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
脅威サマリー	管理者が、脅威サマリー データベースのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
トラフィック ログ	管理者が、トラフィックログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
トラフィック サマリー	管理者が、トラフィック サマリー データベースのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
URL ログ	管理者が、URLフィルタリング ログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
URL の概要	管理者が、トンネル サマリー データベースのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
HIP マッチ	管理者が、HIP マッチ ログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
グローバルな保護	管理者が、GlobalProtect ログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
WildFire ログ	管理者が、WildFireログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
GTP ログ	モバイル ネットワーク事業者が GTP ログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
GTP サマリー	モバイル ネットワーク事業者が GTP ログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
トンネル ログ	管理者が、トンネル検査ログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
トンネル サマリー	管理者が、トンネル サマリー データベースのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
SCTP Log SCTP ログ	モバイル ネットワーク事業者が SCTP ログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
SCTP Summary SCTP サマリー	モバイル ネットワーク事業者が SCTP サマリー データベースのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
User-ID	管理者が、User-ID ログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
認証	管理者が、認証ログのデータを含むカスタム レポートを作成できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
スケジュール設定されたカスタム レポートの表示	管理者が、生成するようにスケジュール設定されているカスタム レポートを表示できるかどうかを指定します。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
事前定義済みアプリケーション レ	管理者がアプリケーション レポートを表示できるかどうかを指定します。専用の権限は、**Monitor (監視)** > **Reports (レポート)** ノードに表示されるレポートに影響しないため、	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
ポートの表示	ユーザーのプライバシーを守る必要がある場合はこのレポートへのアクセス権限を無効にしてください。				
事前定義済み脅威レポートの表示	管理者が脅威レポートを表示できるかどうかを指定します。専用の権限は、**Monitor (監視)** > **Reports (レポート)** ノードに表示されるレポートに影響しないため、ユーザーのプライバシーを守る必要がある場合はこのレポートへのアクセス権限を無効にしてください。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
事前定義済み URL フィルタリング レポートを表示	管理者が URL フィルタリング レポートを表示できるかどうかを指定します。専用の権限は、**Monitor (監視)** > **Reports (レポート)** ノードに表示されるレポートに影響しないため、ユーザーのプライバシーを守る必要がある場合はこのレポートへのアクセス権限を無効にしてください。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
事前定義済み トラフィック レポートを表示	管理者がトラフィック レポートを表示できるかどうかを指定します。専用の権限は、**Monitor (監視)** > **Reports (レポート)** ノードに表示されるレポートに影響しないため、ユーザーのプライバシーを守る必要がある場合はこのレポートへのアクセス権限を無効にしてください。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
事前定義済み GTP レポートの表示	モバイルネットワーク事業者が GTP レポートを見ることができるかどうかを指定します。専用の権限は、**Monitor (監視)** > **Reports (レポート)** ノードに表示されるレポートに影響しないため、ユーザーのプライバシー	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	を守る必要がある場合はこのレポートへのアクセス権限を無効にしてください。				
View Predefined SCTP Reports 事前定義済みの SCTP レポートを表示	モバイルネットワーク事業者が SCTP レポートを見ることができるかどうかを指定します。専用の権限は、**Monitor (監視)** > **Reports (レポート)** ノードに表示されるレポートに影響しないため、ユーザーのプライバシーを守る必要がある場合はこのレポートへのアクセス権限を無効にしてください。	firewall:あり。 Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。

[Policies] タブに対する詳細なアクセス権限の付与

管理者ロール プロファイルで Policy オプションを有効にすると、定義するロールに対して、タブ内の特定のノードを有効または無効にしたり、読み取り専用アクセスを設定したりできます。特定のポリシー タイプへのアクセス権限を有効にすることにより、ポリシー ルールを表示、追加、または削除する権限を有効にできます。特定のポリシーに対する読み取り専用アクセス権限を有効にすると、その管理者は対応するポリシー ルール ベースを表示できるようになりますが、ルールを追加または削除することはできません。特定のタイプのポリシーに対するアクセス権限を無効にすることにより、管理者がポリシー ルール ベースを表示できないようにします。

特定のユーザーに基づいた（ユーザー名または IP アドレス）ポリシーは明示的に定義する必要があるため、完全な IP アドレスやユーザー名を表示する権限を無効にするプライバシーの設定はPolicy [ポリシー] タブには適用されません。したがって、ユーザーのプライバシー制限から除外されている管理者に対してのみ、Policy [ポリシー] タブへのアクセスを許可する必要があります。

アクセス レベル	の意味	**Enable** [有効化]	読み取り専用	無効化
セキュリティ	管理者にセキュリティ ルールの表示、追加、または削除を許可するには、この権限を有効にします。管理者が、ルールを表示できても変更できないようにする場合は、この権限を読み取り専用に設定します。管理者がセキュリティ ルールベースを表示できないようにするには、この権限を無効にします。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
NAT	管理者にNATルールの表示、追加、または削除を許可するには、この権限を有効にします。管理者が、ルールを表示できても変更できないようにする場合は、この権限を読み取り専用に設定します。管理者がNATルールベースを表示できないようにするには、この権限を無効にします。	あり。	はい	あり。
QoS	管理者にQoSルールの表示、追加、または削除を許可するには、この権限を有効にします。管理者が、ルールを表示できても変更できないようにする場合は、この権限を読み取り専用に設定します。管理者がQoSルールベースを表示できないようにするには、この権限を無効にします。	あり。	はい	あり。
ポリシー ベース フォワーディング	管理者にポリシーベース フォワーディング（PBF）ルールの表示、追加、または削除を許可するには、この権限を有効にします。管理者が、ルールを表示できても変更できないようにする場合は、この権限を読み取り専用に設定します。管理者がPBFルールベースを表示できないようにするには、この権限を無効にします。	あり。	はい	あり。
復号	管理者に復号化ルールの表示、追加、または削除を許可するには、この権限を有効にします。管理者が、ルールを表示できても変更できないようにする場合は、この権限を読み取り専用に設定します。管理者が復号化ルールベースを表示できないようにするには、この権限を無効にします。	あり。	はい	あり
ネットワークパケットブローカー	管理者がネットワーク パケット ブローカ ポリシー ルールを表示、追加、削除できるようにするには、この権限を有効にします。管理者が、ルールを表示できても変更できないようにする場合は、この権限を読み取り専用に設定します。管理	あり	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	者がインターフェイスでネットワーク パケット ブローカ ルールベースを表示しないようにするには、この特権を無効にします。			
トンネル検査	管理者にトンネル検査ルールの表示、追加、または削除を許可するには、この権限を有効にします。管理者が、ルールを表示できても変更できないようにする場合は、この権限を読み取り専用に設定します。管理者がトンネル検査ルールベースを表示できないようにするには、この権限を無効にします。	あり。	はい	あり。
アプリケーション オーバーライド	管理者にアプリケーション オーバーライド ポリシー ルールの表示、追加、または削除を許可するには、この権限を有効にします。管理者が、ルールを表示できても変更できないようにする場合は、この権限を読み取り専用に設定します。管理者がアプリケーション オーバーライド ルールベースを表示できないようにするには、この権限を無効にします。	あり。	はい	あり。
認証	管理者に認証ポリシールールの表示、追加、または削除を許可するには、この権限を有効にします。管理者が、ルールを表示できても変更できないようにする場合は、この権限を読み取り専用に設定します。管理者が認証ルールベースを表示できないようにするには、この権限を無効にします。	あり。	はい	あり。
DoS プロテクション	管理者に DoS プロテクション ルールの表示、追加、または削除を許可するには、この権限を有効にします。管理者が、ルールを表示できても変更できないようにする場合は、この権限を読み取り専用に設定します。管理者が DoS プロテクション ルールベースを表示できないようにするには、この権限を無効にします。	あり。	はい	あり
SD-WAN	管理者が SD-WAN ポリシー ルールを表示、追加、削除できるようにするには、	あり	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	この権限を有効にします。管理者が、ルールを表示できても変更できないようにする場合は、この権限を読み取り専用に設定します。管理者が SD-WAN ポリシー ルールベースを表示できないようにするには、この権限を無効にします。			

[Objects] タブに対する詳細なアクセス権限の付与

オブジェクトは、ルール定義を簡素化するために、IP アドレス、URL、アプリケーション、またはサービスなどの特定のポリシー フィルタ値をグループ化するコンテナです。たとえば、アドレス オブジェクトには、DMZ ゾーン内の Web サーバーやアプリケーション サーバーに固有の IP アドレスの定義が含まれています。

Objects [オブジェクト]タブ全体に対するアクセスを許可するかどうかを決定するときには、その管理者にポリシー定義の責任があるかどうかを判別してください。その責任がない場合、おそらくその管理者はタブにアクセスする必要がありません。ただし、その管理者が今後ポリシーを作成する必要がある場合は、このタブへのアクセス権限を有効にし、ノード レベルで詳細なアクセス権限を付与することができます。

特定のノードへのアクセス権限を有効にすることにより、対応するオブジェクト タイプを表示、追加、および削除する権限を管理者に付与します。読み取り専用アクセス権限が付与されると、管理者は、すでに定義済みのオブジェクトを表示できますが、オブジェクトを作成または削除することはできません。ノードを無効にすると、管理者は Web インターフェイスでそのノードを表示することができません。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
アドレス	管理者が、セキュリティ ポリシーで使用するアドレス オブジェクトを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
アドレス グループ	管理者が、セキュリティ ポリシーで使用するアドレス グループ オブジェクトを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
リージョン	管理者が、セキュリティ、復号、または DoS ポリシーで使用する地域オブジェクトを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
アプリケーション [applications]	管理者が、ポリシーで使用するアプリケーション オブジェクトを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
アプリケーション グループ	管理者が、ポリシーで使用するアプリケーショングループ オブジェクトを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
アプリケーション フィルタ	管理者が、繰り返し検索を簡単にするためのアプリケーション フィルタを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
Services（サービス）	管理者が、アプリケーションで使用可能なポート番号を制限するポリシー ルールを作成するときに使用するサービス オブジェクトを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
サービス グループ	管理者が、セキュリティ ポリシーで使用するサービス グループ オブジェクトを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
タグ	管理者が、ファイアウォールで定義されているタグを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
グローバルな保護	管理者が、HIP オブジェクトと HIP プロファイルを表示、追加、または削除できるかどうかを指定します。両方のタイプのオブジェクトへのアクセスを GlobalProtect レベルで制限できます。または、GlobalProtect 権限を有効にして HIP オブジェクトまたは HIP プロファイルへのアクセスを制限することにより、より詳細な制御を行うことができます。	あり。	無し	あり。
HIP オブジェクト	管理者が、HIP プロファイルの定義で使用される HIP オブジェクトを表示、追加、または削除できるかどうかを指定し	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	ます。HIP オブジェクトは、HIP マッチ ログも生成します。			
クライアントレス アプリケーション	管理者が、GlobalProtect VPN クライアントレス アプリケーションを表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
クライアントレス アプリケーション グループ	管理者が、GlobalProtect VPN クライアントレス アプリケーション グループを表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
HIP プロファイル	管理者が、セキュリティ ポリシーで使用されるか、または HIP マッチ ログの生成で使用される HIP プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
外部動的リスト	管理者が、セキュリティ ポリシーで使用するダイナミック ブロック リストを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
カスタム オブジェクト	管理者が、カスタム スパイウェアと脆弱性のシグネチャを表示できるかどうかを指定します。このレベルですべてのカスタム シグネチャに対するアクセス権限を有効または無効にしてアクセスを制限できます。または、カスタム オブジェクト権限を有効にして各タイプのシグネチャへのアクセスを制限することにより、より詳細に制御することができます。	あり。	無し	あり。
データ パターン	管理者が、カスタム脆弱性防御プロファイルの作成に使用するカスタム データ パターン シグネチャを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
Spyware	管理者が、カスタム脆弱性防御プロファイルの作成に使用するカスタム スパイウェア シグネチャを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
脆弱性が	管理者が、カスタム脆弱性防御プロファイルの作成に使用するカスタム脆弱性シグネチャを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
URL カテゴリ	管理者が、ポリシーで使用するカスタム URL カテゴリを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
セキュリティ プロファイル	管理者がセキュリティ プロファイルを表示できるかどうかを指定します。このレベルですべてのセキュリティ プロファイルに対するアクセス権限を有効または無効にしてアクセスを制限できます。または、セキュリティ プロファイル権限を有効にして各タイプのプロファイルへのアクセスを制限することにより、より詳細に制御することができます。	あり。	無し	あり。
Antivirus（アンチウイルス）	管理者が、アンチウイルス プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
アンチスパイウェア	管理者が、アンチスパイウェア プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
脆弱性防御	管理者が、脆弱性防御プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
URL フィルタリング	管理者が、URL フィルタリング プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
ファイル ブロッキング	管理者が、ファイル ブロッキング プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
WildFire分析	管理者が、WildFire 分析プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
データ フィルタリング	管理者が、データ フィルタリング プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
DoS プロテクション	管理者が、DoS プロテクション プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
GTP 保護	モバイル ネットワーク オペレーターが、脆弱性防御プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
SCTP Protection SCTP 保護	モバイル ネットワーク オペレーターが、Stream Control Transmission Protocol (SCTP) 防御プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
セキュリティ プロファイル グループ	管理者が、セキュリティ プロファイル グループを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
ログの転送	管理者が、ログ転送プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
認証	管理者が、認証適用オブジェクト を表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
Decryption Profile（復号化プロファイル）	管理者が、復号化プロファイルを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり
SD-WAN リンク管理	管理者がパス品質、SaaS 品質、トラフィック分布、およびエラー訂正プロファイルを追加または削除できるかどうかを指定します。	あり	無し	あり
Path Quality Profile (パス品質プロファイル)	管理者が SD-WAN パス品質プロファイルを表示、追加、または削除できるかどうかを指定します。	あり	はい	あり

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
SaaS Quality Profile SaaS 品質プロファイル	管理者が SD-WAN SaaS 品質プロファイルを表示、追加、または削除できるかどうかを指定します。	あり	はい	あり
トラフィック分散プロファイル	管理者が SD-WAN トラフィック配信プロファイルを表示、追加、または削除できるかどうかを指定します。	あり	はい	あり
Error Correction Profile エラーの修正プロファイル	管理者が SD-WAN エラー修正プロファイルを表示、追加、または削除できるかどうかを指定します。	あり	はい	あり
パケットブローカープロファイル	管理者が、復号化プロファイルを表示、追加、または削除できるかどうかを指定します。	あり	はい	あり。
スケジュール	管理者が、セキュリティ ポリシーを特定の日付または時刻範囲に制限するためのスケジュールを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。

[Network] タブに対する詳細なアクセス権限の付与

Network [ネットワーク]タブ全体に対するアクセスを許可するかどうかを決定するときには、その管理者に GlobalProtect 管理を含むネットワーク管理の責任があるかどうかを判別してください。その責任がない場合、おそらくその管理者はタブにアクセスする必要がありません。

Network[ネットワーク] タブへのアクセス権限は、ノード レベルで定義することもできます。特定のノードへのアクセス権限を有効にすることにより、対応するネットワーク設定を表示、追加、および削除する権限を管理者に付与します。読み取り専用アクセス権限が付与されると、管理者はすでに定義済みの設定を表示できますが、設定を作成または削除することはできません。ノードを無効にすると、管理者は Web インターフェイスでそのノードを表示することができません。

いくつかのルーティングアクセスレベルが表示され、デバイスで 高度なルーティング が有効になっている場合にのみ適用されます。この場合、論理ルーターが仮想ルーターに置き換わります。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
Interface（インターフェイス）	管理者が、インターフェイス設定を表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
ゾーン	管理者が、ゾーンを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
vlans	管理者が、VLANを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
バーチャル ワイヤー	管理者が、バーチャル ワイヤーを表示、追加、または削除できるかどうかを指定します。	あり。	はい	あり。
仮想ルーター	管理者が、仮想ルーターを表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり
routing	（Advanced Routing Engine）管理者がAdvanced Routing Engineのルーティングフィールドを表示、追加、変更、または削除できるかどうかを指定します。	あり	はい	あり
論理ルーター	（Advanced Routing Engine）管理者が論理ルーターを表示、追加、変更、または削除できるかどうかを指定します。	あり	はい	あり
RIP ルーティングプロファイル	（高度なルーティングエンジン）管理者がルーティングプロファイルを表示、追加、変更、または削除できるかどうかを指定します。	あり	はい	あり
BGP	（Advanced Routing Engine）管理者がBGPルーティングプロファイルを表示、追加、変更、または削除できるかどうかを指定します。	あり	はい	あり
BFD	（Advanced Routing Engine）管理者がBFDルーティングプロファイルを表示、追加、変更、または削除できるかどうかを指定します。	はい S	あり	あり
OSPF	（Advanced Routing Engine）管理者がOSPFv2ルーティングプロファイルを表	あり	はい	あり

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	示、追加、変更、または削除できるかどうかを指定します。			
OSPFv3IPv6	（Advanced Routing Engine）管理者がOSPFv3ルーティングプロファイルを表示、追加、変更、または削除できるかどうかを指定します。	あり	はい	あり
RIPv2	（Advanced Routing Engine）管理者がRIPv2ルーティングプロファイルを表示、追加、変更、または削除できるかどうかを指定します。	あり	はい	あり
フィルタ	（高度なルーティングエンジン）管理者がフィルターを表示、追加、変更、または削除できるかどうかを指定します。	あり	はい	あり
マルチキャスト	（Advanced Routing Engine）管理者がIPv4マルチキャストルーティングプロファイルを表示、追加、変更、または削除できるかどうかを指定します。	あり	はい	あり。
IPSec トンネル	管理者が、IPSec トンネル設定を表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
GRE トンネル	管理者が、GRE トンネル設定を表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
DHCP	管理者が、DHCP サーバー設定と DHCP リレー設定を表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
DNS プロキシ	管理者が、DNS プロキシ設定を表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
グローバルな保護	管理者が、GlobalProtect のポータル設定とゲートウェイ設定を表示、追加、変更できるかどうかを指定します。GlobalProtect 機能へのアクセス権限を完全に無効にできます。または、GlobalProtect 権限を有効にして、	あり。	無し	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	ポータル エリアかゲートウェイ設定エリアのいずれかに管理者ロールを制限することもできます。			
ポータル	管理者が、GlobalProtect ポータル設定を表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
ゲートウェイ	管理者が、GlobalProtect ゲートウェイ設定を表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
MDM	管理者が、GlobalProtect MDM サーバー設定を表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
デバイス ブロック リスト	管理者が、デバイス ブロック リストを表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
クライアントレス アプリケーション	管理者が、GlobalProtect クライアントレス VPN アプリケーションを表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
クライアントレス アプリケーション グループ	管理者が、GlobalProtect クライアントレス VPN アプリケーション グループを表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
QoS	管理者が、QoS 設定を表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
LLDP	管理者が、LLDP 設定を表示、追加、変更、または削除できるかどうかを指定します。	あり。	はい	あり。
ネットワーク プロファイル	デフォルト状態を設定して、以下で説明するネットワークの設定すべてを有効または無効にします。	あり。	無し	あり。
GlobalProtect の IPSec 暗号	**Network Profiles** (ネットワーク プロファイル) > **GlobalProtect IPSec Crypto**	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	(GlobalProtect IPSec 暗号化) ノードへのアクセスを制御します。 この権限を無効にすると、その管理者にはそのノードが表示されず、GlobalProtect ゲートウェイとクライアント間の VPN トンネルで認証および暗号化を行うためのアルゴリズムを設定することができません。 この権限を読み取り専用に設定すると、管理者は既存の GlobalProtect の IPSec 暗号プロファイルを表示できますが、プロファイルを追加または編集することはできません。			
IKE ゲートウェイ	**Network Profiles (**ネットワーク プロファイル) > **IKE Gateways (IKE** ゲートウェイ) ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **IKE Gateways**[IKE ゲートウェイ] ノードが表示されず、ピア ゲートウェイとの IKE プロトコル ネゴシエーションを実行するために必要な設定情報を含め、ゲートウェイを定義することができません。 権限状態を読み取り専用に設定すると、管理者は現在設定されている IKE ゲートウェイを表示できますが、ゲートウェイを追加または編集することはできません。	あり。	はい	あり。
IPSec 暗号	**Network Profiles (**ネットワーク プロファイル) > **IPSec Crypto (IPSec** 暗号) ノードへのアクセスを制御します。この権限を無効にすると、その管理者には**Network Profiles (**ネットワーク プロファイル) > **IPSec Crypto (IPSec** 暗号) ノードが表示されず、IPSec SA ネゴシエーションに基づいて VPN トンネルでの識別、認証、および暗号化のためのプロトコルおよびアルゴリズムを指定することができません。 権限状態を読み取り専用に設定すると、管理者は現在設定されている IPSec 暗号	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	設定を表示できますが、設定を追加または編集することはできません。			
IKE 暗号	デバイス間の情報交換の方法を制御して、保護された通信を確保します。IPSec SA ネゴシエーション（IKEv1 フェーズ 1）に基づいて VPN トンネルでの識別、認証、および暗号化のためのプロトコルおよびアルゴリズムを指定します。	あり。	はい	あり。
監視	**Network Profiles (ネットワーク プロファイル)** > **Monitor (監視)** ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Network Profiles (ネットワーク プロファイル)** > **Monitor (監視)**ノードが表示されず、IPSec トンネルのモニタリングに使用されるモニター プロファイルを作成または編集してポリシーベース フォワーディング（PBF）ルールのネクスト ホップ デバイスをモニターすることができません。 権限状態を読み取り専用に設定すると、管理者は現在設定されているモニター プロファイル設定を表示できますが、設定を追加または編集することはできません。	あり。	はい	あり。
インターフェイス管理	**Network Profiles (ネットワーク プロファイル)** > **Interface Mgmt (インターフェイス管理)** ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Network Profiles (ネットワーク プロファイル)** > **Interface Mgmt (インターフェイス管理)** ノードが表示されず、ファイアウォールの管理で使用するプロトコルを指定することができません。 権限状態を読み取り専用に設定すると、管理者は現在設定されているインターフェイス管理プロファイル設定を表示できますが、設定を追加または編集することはできません。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
ゾーン プロテクション	**Network Profiles** (ネットワーク プロファイル) > **Zone Protection** (ゾーン プロテクション) ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Network Profiles** (ネットワーク プロファイル) > **Zone Protection** (ゾーン プロテクション) ノードが表示されず、指定したセキュリティ ゾーンからの攻撃に対するファイアウォールの防御方法を決めるプロファイルを設定することができません。 権限状態を読み取り専用に設定すると、管理者は現在設定されているゾーン プロテクション プロファイル設定を表示できますが、設定を追加または編集することはできません。	あり。	はい	あり。
QoS プロファイル	**Network Profiles** (ネットワーク プロファイル) > **QoS** ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Network Profiles** (ネットワーク プロファイル) > **QoS** ノードが表示されず、QoS トラフィック クラスの処理方法を決める QoS プロファイルを設定することができません。 権限状態を読み取り専用に設定すると、管理者は現在設定されている QoS プロファイル設定を表示できますが、設定を追加または編集することはできません。	あり。	はい	あり。
LLDPプロファイル	**Network Profiles** (ネットワーク プロファイル) > **LLDP** ノードへのアクセスを制御します。この権限を無効にすると、その管理者には**Network Profiles** (ネットワーク プロファイル) > **LLDP** ノードが表示されず、ファイアウォール上のインターフェイスがリンク レイヤー検出プロトコル（LLDP）に参加できるかどうかを制御する LLDP プロファイルを設定することができません。 権限状態を読み取り専用に設定すると、管理者は現在設定されている LLDP プロ	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	ファイル設定を表示できますが、設定を追加または編集することはできません。			
BFDプロファイル	**Network Profiles** (ネットワーク プロファイル) > **Profile** (プロファイル) ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Network Profiles** (ネットワーク プロファイル) > **BFD Profile** (**BFD** プロファイル) ノードが表示されず、BFDプロファイルを設定できません。双方向転送検知（BFD：Bidirectional Forwarding Detection）プロファイルにより、BFDの設定を行って単体あるいは複数のスタティックルートまたはルーティング プロトコルに適用できるようになります。そのため、BFDは不正なリンクやBFDピアを検知し、極めて高速なフェイルオーバーを実現します。 権限状態を読み取り専用に設定すると、管理者は現在設定されている BFD プロファイルを表示できますが、BFD プロファイルを追加または編集することはできません。	あり。	はい	あり
SD-WAN インターフェイス プロファイル	**SD-WAN** インターフェイス プロファイル ノードへのアクセスを制御します。この特権を無効にすると、管理者は **SD-WAN** インターフェイス プロファイル ノードを表示したり、SD-WAN インターフェイス プロファイルを設定したりできなくなります。SD-WAN インターフェイス プロファイルは、ISP 接続の特性を定義し、リンク速度と、ファイアウォールがリンクを監視する頻度を指定します。 特権状態が読み取り専用に設定されている場合、現在設定されている SD-WAN インターフェイス プロファイルを表示することはできますが、追加または編集することはできません。	あり	はい	あり。

[Device] タブに対する詳細なアクセス権限の付与

Device (デバイス) タブへのアクセス権限を詳細に定義するためには、管理者ロール プロファイルを作成あるいは編集する際（**Device (デバイス)** > **Admin Roles (管理者ロール)**）に、**WebUI** タブの **Device (デバイス)** ノードのところまでスクロールします。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
Setup（セットアップ）	**Setup**[セットアップ] ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Setup (セットアップ)** ノードが表示されず、Management (管理)、Operations (操作)、Service (サービス)、Content-ID (コンテンツ ID)、WildFire、または Session (セッション) セットアップ情報などのファイアウォール全体のセットアップ設定情報にアクセスできません。 権限状態を読み取り専用に設定すると、管理者は現在の設定を表示できますが、変更を加えることはできません。	あり。	はい	あり。
管理	**Management**[管理] ノードへのアクセスを制御します。この権限を無効にすると、管理者はホスト名、ドメイン、タイムゾーン、認証、ロギングおよびレポート機能、Panorama 接続、バナー、メッセージ、パスワードの複雑さ設定やその他の設定を行えなくなります。 権限状態を読み取り専用に設定すると、管理者は現在の設定を表示できますが、変更を加えることはできません。	あり。	はい	あり。
業務	**Operations (操作)** および **Telemetry and Threat Intelligence (テレメトリーと脅威インテリジェンス)** ノードへのアクセスを制御します。この権限を無効にすると、管理者は次の操作を行えなくなります。 • ファイアウォールの設定の読込。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	• ファイアウォールの設定の保存およびやり直し。 この権限は ***Device*** **(**デバイス**)** **>** ***Operations*** **(**操作**)** オプションにのみ適用されます。保存および コミット権限は、管理者が ***Config*** **(**設定**)** **>** ***Save*** **(**保存**)** および ***Config*** **(**設定**)** **>** ***Revert*** **(**元に戻す**)**オプションを使って設定を保存したり元に戻したりできるかどうかを制御します。 • カスタム ロゴを作成します。 • ファイアウォール設定の SNMP モニタリングを設定します。 • 統計サービス機能を設定します。 • **Telemetry and Threat Intelligence (**テレメトリーおよび脅威インテリジェンス**)** の設定を行います。 事前定義済みのスーパーユーザーのロールを持つ管理者だけが、ファイアウォールの設定をエクスポート/インポートしたり、ファイアウォールをシャットダウンしたりできます。 事前定義済みのスーパーユーザーあるいはデバイス管理者のロールを持つ管理者だけが、ファイアウォールやデータプレーンの再起動を行えます。 特定の仮想システムへのアクセスのみ許可されているロールを持つ管理者は、**Device (**デバイス**)** > **Operations (**操作**)** オプションを通じてファイアウォール設定を読込、保存、復元することはできません。			
Services（サービス）	**Services**[サービス] ノードへのアクセスを制御します。この権限を無効にすると、管理者はDNSサーバー、更新サーバー、	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	プロキシサーバー、NTPサーバーのサービスを設定したり、サービスルートのセットアップを行ったりできなくなります。 権限状態を読み取り専用に設定すると、管理者は現在の設定を表示できますが、変更を加えることはできません。			
Content-ID	**Content-ID (コンテンツ ID)** ノードへのアクセスを制御します。この権限を無効にすると、管理者はURLフィルタリングやコンテンツIDを設定できなくなります。 権限状態を読み取り専用に設定すると、管理者は現在の設定を表示できますが、変更を加えることはできません。	あり。	はい	あり。
WildFire	**WildFire**ノードへのアクセスを制御します。この権限を無効にすると、管理者はWildFireの設定を行うことができなくなります。 権限状態を読み取り専用に設定すると、管理者は現在の設定を表示できますが、変更を加えることはできません。	あり。	はい	あり。
セッション	**Session**[セッション]ノードへのアクセスを制御します。この権限を無効にすると、管理者はTCP、UDPやICMPのセッション設定やタイムアウトの設定を行ったり、復号化やVPNセッションを設定したりできなくなります。 権限状態を読み取り専用に設定すると、管理者は現在の設定を表示できますが、変更を加えることはできません。	あり。	はい	あり。
HSM	**HSM** ノードへのアクセスを制御します。この権限を無効にすると、管理者はハードウェア セキュリティモジュールの設定を行うことができなくなります。 権限状態を読み取り専用に設定すると、管理者は現在の設定を表示できますが、変更を加えることはできません。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
高可用性（HA）	**High Availability**（高可用性）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **High Availability** [高可用性]ノードが表示されず、General [全般]のセットアップ情報や Link and Path Monitoring [リンクおよびパスのモニタリング]などのファイアウォール全体の高可用性設定の情報にアクセスできません。 この権限を読み取り専用に設定すると、管理者はファイアウォールの高可用性設定情報を表示できますが、設定手順を実行することは許可されません。	あり。	はい	あり。
Config Audit（設定監査）	**Config Audit**（設定監査）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Config Audit**（設定監査）ノードが表示されず、ファイアウォール全体の設定情報にアクセスできません。	あり。	無し	あり。
Administrators（管理者）	**Administrators**（管理者）ノードへのアクセスを制御します。この機能は、読み取り専用アクセスでのみ許可されます。 この権限を無効にすると、その管理者には **Administrators (管理者)** ノードが表示されず、自分の管理者アカウントに関する情報にアクセスできません。 この権限を読み取り専用に設定すると、管理者は自分の管理者アカウントの設定情報を表示できます。そのファイアウォールで設定されている他の管理者アカウントに関する情報は表示されません。	無し	はい	あり。
dmin Roles（管理者ロール）	**Admin Roles**（管理者ロール）ノードへのアクセスを制御します。この機能は、読み取り専用アクセスでのみ許可されます。 この権限を無効にすると、管理者には **Admin Roles (管理者ロール)** ノードが表示されず、管理者ロール プロファイル設	無し	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	定に関係するファイアウォール全体の情報にアクセスできません。 この権限を読み取り専用に設定すると、管理者はそのファイアウォールで設定されているすべての管理者ロールの設定情報を表示できます。			
Authentication Profile（認証プロファイル）	**Authentication Profile**（認証プロファイル）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Authentication Profile** (認証プロファイル) ノードが表示されず、管理者アカウントに割り当てることができる RADIUS、TACACS+、LDAP、Kerberos、SAML、マルチファクター認証（MFA）、またはローカル データベース認証の設定を作成または編集することができません。PAN-OS は認証プロファイルを使用してファイアウォール管理者および認証ポータルあるいは GlobalProtect のエンドユーザーを認証します。 この権限を読み取り専用に設定すると、管理者は **Authentication Profile** (認証プロファイル) 情報を表示できますが、認証プロファイルを作成または編集することはできません。	あり。	はい	あり。
Authentication Sequence（認証シーケンス）	**Authentication Sequence**（認証シーケンス） ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Authentication Sequence**（認証シーケンス）ノードが表示されず、認証シーケンスを作成または編集することができません。 この権限を読み取り専用に設定すると、管理者は **Authentication Profile** (認証プロファイル) 情報を表示できますが、認証シーケンスを作成または編集することはできません。	あり。	はい	あり。
仮想システム	**Virtual Systems**[仮想システム] ノードへのアクセスを制御します。この権限を無	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	効にすると、その管理者には仮想システムが表示されず、仮想システムを設定することができません。 権限状態を読み取り専用に設定すると、管理者は現在設定されている仮想システムを表示できますが、設定を追加または編集することはできません。			
共有ゲートウェイ	**Shared Gateways**[共有ゲートウェイ] ノードへのアクセスを制御します。仮想システムは、共有ゲートウェイを使用することによって共通の外部通信インターフェイスを共有できます。 この権限を無効にすると、その管理者には共有ゲートウェイが表示されず、共有ゲートウェイを設定することができません。 権限状態を読み取り専用に設定すると、管理者は現在設定されている共有ゲートウェイを表示できますが、設定を追加または編集することはできません。	あり。	はい	あり。
User Identification（ユーザー ID）	**User Identification**（ユーザー ID）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **User Identification (ユーザー ID)** ノードが表示されず、User Mapping (ユーザー マッピング)、Connection Security (接続セキュリティ)、User-ID Agents (User-IDエージェント)、Terminal Server Agents (ターミナル サーバー エージェント)、Group Mappings Settings (グループ マッピング設定)、または Authentication Portal Settings (認証ポータルの設定) などのファイアウォール全体のユーザー ID 設定情報にアクセスできません。 この権限を読み取り専用に設定すると、管理者はファイアウォールの設定情報を表示できますが、設定手順を実行することは許可されません。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
VM 情報ソース	VM インベントリを自動的に収集するファイアウォール/Windows User-ID エージェントを設定することができる、**VM Information Source**[VM 情報ソース] ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **VM Information Source**（VM 情報ソース）ノードが表示されません。 この権限を読み取り専用に設定すると、管理者は設定された VM 情報ソースを表示できますが、ソースを追加、編集、または削除することはできません。 この権限は、*Device Group and Template [デバイス グループとテンプレート]* 管理者に付与することはできません。	あり。	はい	あり。
証明書の管理	デフォルト状態を設定して、以下で説明する証明書の設定すべてを有効または無効にします。	あり。	無し	あり。
証明書	**Certificates**（証明書）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Certificates**（証明書）ノードが表示されず、デバイス証明書やデフォルトの信頼された証明機関 に関連した情報を設定したり、それらの情報にアクセスしたりすることはできません。 この権限を読み取り専用に設定すると、管理者はファイアウォールの証明書設定情報を表示できますが、設定手順を実行することは許可されません。	あり。	はい	あり。
証明書プロファイル	**Certificate Profile**（証明書プロファイル）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Certificate Profile**（証明書プロファイル）ノードが表示されず、証明書プロファイルを作成できません。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	この権限を読み取り専用に設定すると、管理者はそのファイアウォールで現在設定されている証明書プロファイルを表示できますが、証明書プロファイルを作成または編集することは許可されません。			
OCSP レスポンダ	**OCSP Responder**（OCSP レスポンダ）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **OCSP Responder (OCSP** レスポンダ**)** ノードが表示されず、ファイアウォールによって発行される証明書の失効状態の検証に使用されるサーバーを定義することはできません。 この権限を読み取り専用に設定すると、管理者はそのファイアウォールでの **OCSP Responder (OCSP** レスポンダ**)** 設定を表示できますが、OCSP レスポンダ設定を作成または編集することは許可されません。	あり。	はい	あり。
SSL/TLS Service Profile	**SSL/TLS Service Profile (SSL/TLS** サービス プロファイル**)** ノードへのアクセスを制御します。 この権限を無効にすると、その管理者にはそのノードが表示されず、SSL/TLS を使用するファイアウォール サービスの証明書およびプロトコル バージョンまたはバージョンの範囲を指定するプロファイルを設定することができません。 この権限を読み取り専用に設定すると、管理者は既存の SSL/TLS サービス プロファイルを表示できますが、プロファイルを追加または編集することはできません。	あり。	はい	あり。
SCEP	**SCEP** ノードへのアクセスを制御します。この権限を無効にすると、管理者はこのノードにアクセスできず、デバイス固有の証明書を発行するためのSCEP（simple certificate enrollment protocol）を指定するプロファイルを定義することができなくなります。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	この権限を読み取り専用に設定すると、管理者は既存のSCEPプロファイルを表示できますが、プロファイルを作成または編集することはできません。			
SSL 復号化例外	**SSL Decryption Exclusion (SSL** 復号化例外**)** ノードへのアクセスを制御します。この権限を無効にすると、その管理者はノードや SSL 復号化を表示できず、カスタム例外を追加できなくなります。 この権限を読み取り専用に設定すると、管理者は既存の SSL 復号化例外を表示できますが、作成または編集することはできません。	あり。	はい	あり
SSHサービスプロファイル	**SSL/TLS Service Profile (SSL/TLS** サービス プロファイル**)** ノードへのアクセスを制御します。この特権を無効にすると、管理者はノードを表示したり、Palo Alto Networks管理および高可用性（HA）アプライアンスへのSSH接続のパラメーターを指定するためのプロファイルを構成したりできなくなります。 この権限を読み取り専用に設定すると、管理者は既存の SSL/TLS サービス プロファイルを表示できますが、プロファイルを追加または編集することはできません。	あり	はい	あり。
応答ページ	**Response Pages**（応答ページ）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Response Page**（応答ページ）ノードが表示されず、要求された Web ページまたはファイルの代わりにダウンロードおよび表示されるカスタム HTML メッセージを定義することができません。 この権限を読み取り専用に設定すると、管理者はそのファイアウォールでの **Response Page (**応答ページ**)** 設定を表示できますが、応答ページ設定を作成または編集することは許可されません。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
ログ設定	デフォルト状態を設定して、以下で説明するログの設定すべてを有効または無効にします。	あり。	無し	あり。
システム<:so>システム	**Log Settings (ログ設定)** > **System (システム)** ノードへのアクセスを制御します。この権限を無効にすると、管理者には**Log Settings (ログ設定)** > **System (システム)** ノードが表示されず、ファイアウォールが Panorama あるいは外部サービス（Syslog サーバーなど）にどのシステムログを転送するのか指定できなくなります。 この権限を読み取り専用に設定すると、管理者はそのファイアウォールでの **Log Settings (ログ設定)** > **System (システム)** の設定を表示できますが、設定を追加・編集・削除することはできません。	あり。	はい	あり。
設定	**Log Settings (ログ設定)** > **Configuration (設定)** ノードへのアクセスを制御します。この権限を無効にすると、管理者には**Log Settings (ログ設定)** > **Configuration (構成)** ノードが表示されず、ファイアウォールが Panorama あるいは外部サービス（Syslog サーバーなど）にどの設定ログを転送するのか指定できなくなります。 この権限を読み取り専用に設定すると、管理者はそのファイアウォールでの **Log Settings (ログ設定)** > **Configuration (構成)** の設定を表示できますが、設定を追加・編集・削除することはできません。	あり。	はい	あり。
User-ID	**Log Settings (ログ設定)** > **User-ID** ノードへのアクセスを制御します。この権限を無効にすると、管理者には**Log Settings (ログ設定)** > **User-ID**ノードが表示されず、ファイアウォールが Panorama あるいは外部サービス（Syslog サーバーなど）にどの User-ID ログを転送するのか指定できなくなります。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	この権限を読み取り専用に設定すると、管理者はそのファイアウォールでの **Log Settings (ログ設定)** > **User-ID** の設定を表示できますが、設定を追加・編集・削除することはできません。			
HIP マッチ	**Log Settings (ログ設定)** > **HIP Match (HIP マッチ)** ノードへのアクセスを制御します。この権限を無効にすると、管理者には **Log Settings (ログ設定)** > **HIP Match (HIP マッチ)** ノードが表示されず、ファイアウォールが Panorama あるいは外部サービス（Syslog サーバーなど）にどのホスト情報プロファイル（HIP）マッチ ログを転送するのか指定できなくなります。HIP マッチ ログは、GlobalProtect エンドポイントに適用されるセキュリティ ポリシー ルールについての情報を提供します。 この権限を読み取り専用に設定すると、管理者はそのファイアウォールでの **Log Settings (ログ設定)** > **HIP** の設定を表示できますが、設定を追加・編集・削除することはできません。	あり。	はい	あり。
グローバルな保護	**Log Settings (ログ設定)** > **GlobalProtect** ノードへのアクセスを制御します。この権限を無効にすると、管理者には**Log Settings (ログ設定)** > **GlobalProtect**ノードが表示されず、ファイアウォールが Panorama あるいは外部サービス（Syslog サーバーなど）にどの GlobalProtect ログを転送するのか指定できなくなります。 この権限を読み取り専用に設定すると、管理者はそのファイアウォールでの **Log Settings (ログ設定)** > **GlobalProtect** の設定を表示できますが、設定を追加・編集・削除することはできません。	あり。	はい	あり。
製品連携	**Log Settings (ログ設定)** > **Correlation (相関)** ノードへのアクセスを制御します。この権限を無効にすると、管理者には **Log Settings (ログ設定)** > **Correlation (相関)**	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	ノードが表示されず、相関ログ転送を追加、削除、あるいは変更したりできず、さらにソースあるいは宛先 IP アドレスのタグ付けを行えなくなります。 この権限を読み取り専用に設定すると、管理者はそのファイアウォールでの **Log Settings (ログ設定)** > **Correlation (相関)** の設定を表示できますが、設定を追加・編集・削除することはできません。			
アラーム設定	**Log Settings (ログ設定)** > **Alarm Settings (アラーム設定)** ノードへのアクセスを制御します。この権限を無効にすると、管理者には **Log Settings (ログ設定)** > **Alarm Settings (アラーム設定)** ノードが表示されず、セキュリティポリシー ルール（あるいはルールのグループ）が設定期間内に何度もヒットした際にファイアウォールが生成する通知の設定を行えなくなります。 この権限を読み取り専用に設定すると、管理者はそのファイアウォールでの **Log Settings (ログ設定)** > **Alarm Settings (アラーム設定)** の設定を表示できますが、設定を編集することはできません。	あり。	はい	あり。
ログの管理	**Log Settings (ログ設定)** > **Manage Logs (ログの管理)** ノードへのアクセスを制御します。この権限を無効にすると、その管理者には**Log Settings (ログ設定)** > **Manage Logs (ログの管理)** ノードが表示されず、表示されたログをクリアすることができません。 この権限を読み取り専用に設定すると、管理者は **Log Settings (ログ設定)** > **Manage Logs (ログの管理)** 情報を表示できますが、いずれのログもクリアすることはできません。	あり。	はい	あり。
サーバー プロファイル	デフォルト状態を設定して、以下で説明するサーバー プロファイルの設定すべてを有効または無効にします。	あり。	無し	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
SNMP トラップ	**Server Profiles (サーバープロファイル)** > **SNMP Trap (SNMP トラップ)** ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Server Profiles (サーバープロファイル)** > **SNMP Trap (SNMP トラップ)** ノードが表示されず、システム ログ エントリで使用されるように 1 つ以上の SNMP トラップの宛先を指定することができません。 この権限を読み取り専用に設定すると、管理者は、**Server Profiles (サーバープロファイル)** > **SNMP Trap Logs (SNMP トラップ ログ)** 情報を表示できますが、SNMP トラップの宛先を指定することはできません。	あり。	はい	あり。
Syslog	**Server Profiles (サーバープロファイル)** > **Syslog** ノードへのアクセスを制御します。この権限を無効にすると、管理者には **Server Profiles (サーバープロファイル)** > **Syslog** ノードが表示されず、Syslog サーバーを指定することができません。 この権限を読み取り専用に設定すると、管理者は、**Server Profiles (サーバープロファイル)** > **Syslog** 情報を表示できますが、Syslog サーバーを指定することはできません。	あり。	はい	あり。
電子メール	**Server Profiles (サーバープロファイル)** > **Email** ノードへのアクセスを制御します。この権限を無効にすると、管理者には **Server Profiles (サーバープロファイル)** > **Email** ノードが表示されず、システムおよび設定ログ エントリの電子メール通知を有効にするために使用できる電子メール プロファイルを設定することができません。 この権限を読み取り専用に設定すると、管理者は **Server Profiles (サーバープロファイル)** > **Email** 情報を表示できますが、プロファイルを設定してメール サーバープロファイルを設定できません。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
HTTP	**Server Profiles (サーバープロファイル)** > **HTTP** ノードへのアクセスを制御します。この権限を無効にすると、管理者には**Server Profiles (サーバープロファイル)** > **HTTP** ノードが表示されず、任意のログ項目を HTTP の宛先に転送するために使用できる HTTP サーバープロファイルを設定することができません。 この権限を読み取り専用に設定すると、管理者は **Server Profiles (サーバープロファイル)** > **HTTP** 情報を表示できますが、プロファイルを設定して HTTP サーバープロファイルを設定できません。	あり。	はい	あり。
Netflow	**Server Profiles (サーバープロファイル)** > **Netflow** ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Server Profiles (サーバープロファイル)** > **Netflow** ノードが表示されず、NetFlow サーバー プロファイルを定義することができません。このプロファイルでは、エクスポートされたデータを受信する NetFlow サーバーおよびエクスポートの頻度を指定します。 この権限を読み取り専用に設定すると、管理者は **Server Profiles (サーバープロファイル)** > **Netflow** 情報を表示できますが、Netflow プロファイルを定義することはできません。	あり。	はい	あり。
RADIUS	**Server Profiles (サーバープロファイル)** > **RADIUS** ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Server Profiles (サーバープロファイル)** > **RADIUS** ノードが表示されず、認証プロファイルで識別される RADIUS サーバーの設定を行うことができません。 この権限を読み取り専用に設定すると、管理者は **Server Profiles (サーバープロファイル)** > **RADIUS** 情報を表示できます	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	が、RADIUS サーバーの設定を行うことはできません。			
TACACS+	**Server Profiles (サーバープロファイル)** > **TACACS+** ノードへのアクセスを制御します。 この権限を無効にすると、管理者にはそのノードが表示されず、認証プロファイルで参照される TACACS+ サーバーの設定を行うことができません。 この権限を読み取り専用に設定すると、管理者は既存の TACACS+ サーバー プロファイルを表示できますが、プロファイルを追加または編集することはできません。	あり。	はい	あり。
LDAP	**Server Profiles (サーバープロファイル)** > **LDAP** ノードへのアクセスを制御します。この権限を無効にすると、その管理者には**Server Profiles (サーバープロファイル)** > **LDAP** ノードが表示されず、認証プロファイルによる認証で使用する LDAP サーバーの設定を行うことができません。 この権限を読み取り専用に設定すると、管理者は **Server Profiles (サーバープロファイル)** > **LDAP** 情報を表示できますが、LDAP サーバーの設定を行うことはできません。	あり。	はい	あり。
Kerberos	**Server Profiles (サーバープロファイル)** > **Kerberos** ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Server Profiles (サーバープロファイル)** > **Kerberos** ノードが表示されず、ユーザーがドメイン コントローラに対してネイティブに認証できるようにする Kerberos サーバーの設定を行うことができません。 この権限を読み取り専用に設定すると、管理者は **Server Profiles (サーバープロファイル)** > **Kerberos** 情報を表示できま	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	すが、Kerberos サーバーの設定を行うことはできません。			
SAML アイデンティティ プロバイダ	**Server Profiles** (サーバープロファイル) > **SAML Identity Provider** (SAML アイデンティティ プロバイダ) ノードへのアクセスを制御します。この権限を無効にすると、管理者はノードを表示できず、SAML アイデンティティ プロバイダ（IdP）サーバープロファイルを設定できません。 この権限を読み取り専用に設定すると、管理者は **Server Profiles** (サーバープロファイル) > **SAML Identity Provider** (SAML アイデンティティ プロバイダ) 情報を表示できますが、プロファイルを設定して SAML IdP サーバープロファイルを設定できません。	あり。	はい	あり。
多要素認証	**Server Profiles** (サーバープロファイル) > **Multi Factor Authentication** (マルチ ファクター認証) ノードへのアクセスを制御します。この権限を無効にすると、管理者はノードを表示できず、マルチ ファクター認証（MFA）サーバープロファイルを設定できません。 この権限を読み取り専用に設定すると、管理者は **Server Profiles** (サーバープロファイル) > **SAML Identity Provider** (SAML アイデンティティ プロバイダ) 情報を表示できますが、プロファイルを設定して MFA サーバープロファイルを設定できません。			
ローカル ユーザー データベース	デフォルト状態を設定して、以下で説明するローカル ユーザー データベースの設定すべてを有効または無効にします。	あり。	無し	あり。
ユーザー	**Local User Database** (ローカル ユーザー データベース) > **Users** (ユーザー) ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Local User Database** (ローカル ユーザー データベース) > **Users** (ユーザー) ノードが表	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	示されず、リモート アクセス ユーザー、ファイアウォール管理者、および認証ポータル ユーザーの認証情報を格納するローカル データベースをファイアウォールにセットアップすることができません。 この権限を読み取り専用に設定すると、管理者は **Local User Database (**ローカル ユーザー データベース**)** > **Users (**ユーザー**)** 情報を表示できますが、認証情報を格納するローカル データベースをファイアウォールにセットアップすることはできません。			
ユーザー グループ	**Local User Database (**ローカル ユーザー データベース**)** > **Users (**ユーザー**)** ノードへのアクセスを制御します。この権限を無効にすると、その管理者には**Local User Database (**ローカル ユーザー データベース**)** > **Users (**ユーザー**)** ノードが表示されず、ローカル データベースにユーザー グループ情報を追加することができません。 この権限を読み取り専用に設定すると、管理者は **Local User Database (**ローカル ユーザー データベース**)** > **Users (**ユーザー**)** 情報を表示できますが、ローカル データベースにユーザー グループ情報を追加することはできません。	あり。	はい	あり。
Access Domains（アクセス ドメイン）	**Access Domain**（アクセス ドメイン）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Access Domain** [アクセス ドメイン]ノードが表示されず、アクセス ドメインを作成または編集することができません。 この権限を読み取り専用に設定すると、**Access Domain (**アクセスドメイン**)** の情報を表示できますが、アクセス ドメインを作成または編集することはできません。	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
スケジュール設定されたログのエクスポート	**Scheduled Log Export**（スケジュール設定されたログのエクスポート）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Scheduled Log Export (**スケジュール設定されたログのエクスポート**)** ノードが表示されず、ログのエクスポートをスケジュール設定してそのログを CSV 形式で FTP （File Transfer Protocol）サーバーに保存したり、または Secure Copy （SCP）を使用してファイアウォールとリモート ホスト間でデータを安全に転送したりすることができません。 この権限を読み取り専用に設定すると、管理者は **Scheduled Log Export Profile (**スケジュール設定されたログのエクスポート プロファイル**)** 情報を表示できますが、ログのエクスポートをスケジュール設定することはできません。	あり。	無し	あり。
ソフトウェア	**Software**（ソフトウェア）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Software**（ソフトウェア）ノードが表示されず、Palo Alto Networks が提供する最新バージョンの PAN-OS ソフトウェアを表示したり、各バージョンのリリース ノートを読んだり、リリースを選択してダウンロードおよびインストールすることができません。 この権限を読み取り専用に設定すると、管理者は **Software** （ソフトウェア）情報を表示できますが、ソフトウェアをダウンロードまたはインストールすることはできません。	あり。	はい	あり。
GlobalProtect クライアント	**GlobalProtect Client**（GlobalProtect クライアント）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **GlobalProtect Client**[GlobalProtect クライアント] ノードが表示されず、使用可能な GlobalProtect	あり。	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	リリースを表示したり、コードをダウンロードしたり、GlobalProtect アプリをアクティブにしたりすることができません。 この権限を読み取り専用に設定すると、管理者は **GlobalProtect Client (GlobalProtect** クライアント**)** リリースを表示できますが、アプリ ソフトウェアをダウンロードまたはインストールすることはできません。			
ダイナミック更新	**Dynamic Updates**（動的更新）ノードへのアクセスを制御します。この権限を無効にすると、管理者には **Dynamic Updates**（動的更新）ノードが表示されず、最新の更新を表示したり、各更新のリリース ノートを読んだり、アップロードおよびインストールする更新を選択したりすることができません。 この権限を読み取り専用に設定すると、管理者は使用可能な **Dynamic Updates (**動的更新**)** リリースを表示し、リリース ノートを読むことができますが、ソフトウェアをアップロードまたはインストールすることはできません。	あり。	はい	あり。
ライセンス	**Licenses**（ライセンス）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Licenses**（ライセンス）ノードが表示されず、インストール済みのライセンスを表示したり、ライセンスをアクティブにしたりすることができません。 この権限を読み取り専用に設定すると、管理者はインストール済みの **Licenses** [ライセンス]を表示できますが、ライセンス管理機能を実行することはできません。	あり。	はい	あり。
Support（サポート）	**Support**（サポート）ノードへのアクセスを制御します。この権限を無効にすると、管理者は **Support (**サポート**)** ノード、アクティブ サポートを表示できず、Palo Alto Networks の本番環境および	あり	はい	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	セキュリティ アラートにアクセスできません。 この権限を読み取り専用に設定すると、管理者は **Support (サポート)** ノードを表示し、本番環境アラートおよびセキュリティ アラートにアクセスすることができますが、サポートを有効化することはできません。			
マスターキーおよび診断	**Master Key and Diagnostics**（マスターキーおよび診断）ノードへのアクセスを制御します。この権限を無効にすると、その管理者には **Master Key and Diagnostics**（マスター キーおよび診断）ノードが表示されなくなり、ファイアウォールで秘密鍵を暗号化するためのマスター キーを指定することができません。 この権限を読み取り専用に設定すると、管理者は **Master Key and Diagnostics (マスター キーおよび診断)** ノードを表示し、指定されているマスター キーに関する情報を表示できますが、新しいマスター キー設定を追加または編集することはできません。	あり。	はい	あり
Policy Recommendation 推奨ポリシー	**IoT** および **SaaS** ポリシー ルールの推奨事項へのアクセスを制御します。これらの権限を無効にすると、管理者は無効にする権限に応じて、 ポリシー推奨 > **IoT** ノード、ポリシー推奨 > **SaaS** ノード、またはその両方を表示できません。 これらの特権を読み取り専用に設定すると、管理者はノードを表示できますが、ポリシールールのインポートや情報の編集はできません。	あり	はい	あり。

管理者ロール プロファイルでのユーザーのプライバシー設定の定義

管理者がどのようなエンドユーザーのプライベートなデータにアクセスできるのか定義するためには、管理者ロール プロファイルを作成あるいは編集する際（**Device (デバイス)** > **Admin Roles**

(管理者ロール)）に、**WebUI** タブの **Privacy (プライバシー)** オプションのところまでスクロールします。

アクセス レベル	の意味	**Enable** [有効化]	読み取り専用	無効化
専用	デフォルト状態を設定して、以下で説明するプライバシー設定すべてを有効または無効にします。	あり。	N/A	あり。
完全 IP アドレスの表示	無効にすると、Palo Alto ファイアウォールを通過するトラフィックによって取得された完全 IP アドレスは、ログまたはレポートに表示されません。通常表示される IP アドレスの代わりに、関連サブネットが表示されます。 ***Monitor (監視) > Reports (レポート)*** を介してインターフェイスに表示されるスケジュール設定されたレポート、およびスケジュール設定された電子メールで送信されるレポートには、この設定を無効にしても完全 ***IP*** アドレスが表示されます。このような例外があるため、***Monitor [監視]*** タブに表示される各設定を無効に設定することをお勧めします（*Custom Reports [カスタム レポート]*、*Application Reports [アプリケーション レポート]*、*Threat Reports [脅威レポート]*、*URL Filtering Reports [URL フィルタリング レポート]*、*Traffic Reports [トラフィック レポート]*、および *Email Scheduler [電子メール スケジューラ]*）。	あり。	N/A	あり。
ログおよびレポート内での	無効にすると、Palo Alto Networks ファイアウォールを通過するトラフィックによって得られたユーザー名は、ログまた	あり。	N/A	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
ユーザー名の表示	はレポートに表示されません。通常ユーザー名が表示される列は、空になります。 ***Monitor*** **(監視) > *Reports*** **(レポート)** を介してインターフェースに表示されるスケジュール設定されたレポート、および電子メール スケジューラ経由で送信されるレポートには、この設定を無効に設定してもユーザー名が表示されます。このような例外があるため、*Monitor* [監視] タブに表示される各設定を無効に設定することをお勧めします（*Custom Reports* [カスタム レポート]、*Application Reports* [アプリケーション レポート]、*Threat Reports* [脅威レポート]、*URL Filtering Reports* [URL フィルタリング レポート]、*Traffic Reports* [トラフィック レポート]、および *Email Scheduler* [電子メール スケジューラ]）。			
PCAP ファイルを表示	無効にすると、通常ならトラフィック ログ、脅威ログ、およびデータ フィルタリング ログに表示されるパケット キャプチャ ファイルは表示されません。	あり。	N/A	あり。

コミットおよび検証機能への管理者アクセスの制限

管理者ロール プロファイルを作成あるいは編集する際にコミット（および復元）、保存、および検証機能へのアクセスを制限するには（**Device (デバイス)** > **Admin Roles (管理者ロール)**）、**WebUI** タブで **Commit (コミット)**、**Save (保存)**、および **Validate (検証)** オプションのところまでスクロールします。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
コミット	デフォルト状態を設定して、以下で説明するコミットおよび元に戻す権限をすべて有効または無効にします。	あり。	N/A	あり。
Device（デバイス）	無効にすると、自分が行った変更も含め、あらゆる管理者がファイアウォールの設定に加えた変更を管理者がコミットすることも元に戻すこともできなくなります。	あり。	N/A	あり。
他の管理者のためにコミット	無効にすると、管理者は他の管理者がファイアウォールの設定に加えた変更をコミットしたり元に戻したりできなくなります。	あり。	N/A	あり。
Save（保存）	デフォルト状態を設定して、以下で説明する保存操作を行う権限をすべて有効または無効にします。	あり。	N/A	あり。
一部保存	無効にすると、自分が行った変更も含め、あらゆる管理者がファイアウォールの設定に加えた変更を保存することができなくなります。	あり。	N/A	あり。
他の管理者のために保存	無効にすると、管理者は他の管理者がファイアウォールの設定に加えた変更を保存できません。	あり。	N/A	あり。
検証	無効にすると、管理者は設定を検証できません。	あり。	N/A	あり。

グローバル設定への詳細なアクセス権限の指定

どのようなグローバル設定および管理者がアクセスできるのか定義するためには、管理者ロール プロファイルを作成あるいは編集する際（**Device (デバイス)** > **Admin Roles (管理者ロール)**）に、**WebUI** タブの **Privacy (プライバシー)** オプションのところまでスクロールします。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
Global	デフォルト状態を設定して、以下で説明するグローバルの設定すべてを有効または無効にします。事実上この設定は、こ	あり。	N/A	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	の時点ではSystem Alarms [システム アラーム] にのみ適用されます。			
システム アラーム	無効にすると、管理者は生成されるアラームを表示または確認できません。	あり。	N/A	あり。

Panorama タブに対する詳細なアクセス権限の付与

以下の表に、**Panorama** タブのアクセス レベルと、そのレベルで設定可能なカスタム Panorama 管理者ロールの一覧を示します。ファイアウォール管理者は、これらの権限のいずれにもアクセスできません。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
Setup（セットアップ）	管理者が、**Management (管理)**、**Operations and Telemetry (操作およびテレメトリー)**、**Services (サービス)**、Content-ID、**WildFire**、Session (セッション)、あるいは **HSM** など、Panorama のセットアップ情報を表示したり編集したりできるかどうかを指定します。 この権限の設定による影響は以下のとおりです。 • この権限を読み取り専用に設定すると、管理者は情報を表示できますが、編集することはできません。 • この権限を無効にすると、管理者は情報を表示または編集することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
高可用性（HA）	管理者が、Panorama 管理サーバーの高可用性（HA）設定を表示および管理できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、Panorama 管理サーバーの HA 設定情報を表示できますが、その設定を管理することはできません。 この権限を無効にすると、管理者は、Panorama 管理サーバーの HA 設定を表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。
Config Audit（設定監査）	管理者が Panorama 設定の監査を実行できるかどうかを指定します。この権限を無効にすると、管理者は Panorama 設定の監査を実行できません。	Panorama：あり。 デバイス グループ/テンプレート：無し	あり。	無し	あり。
Administrators（管理者）	管理者が Panorama 管理者のアカウント詳細を表示できるかどうかを指定します。 この機能へのフル アクセスを有効にすることはできません。有効にできるのは、読み取り専用アクセス権だけです（動的ロールを持つ Panorama 管理者だけが、Panorama 管理者を追加、編集、または削除できます）。 読み取り専用アクセス権限を持つ管理者は、自分のアカウントに関する情報を表示できますが、その他の Panorama 管理者のアカウントを表示することはできません。	Panorama：あり。 デバイス グループ/テンプレート：無し	無し	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	この権限を無効にすると、管理者は、自分のアカウントを含め、すべての Panorama 管理者のアカウントに関する情報を表示できません。				
dmin Roles（管理者ロール）	管理者が Panorama 管理者のロールを表示できるかどうかを指定します。 この機能へのフル アクセスを有効にすることはできません。有効にできるのは、読み取り専用アクセス権だけです（動的ロールを持つ Panorama 管理者だけが、カスタム Panorama ロールを追加、編集、または削除できます）。 読み取り専用アクセス権限を持つ管理者は、Panorama 管理者のロールの設定を表示できますが、管理することはできません。 この権限を無効にすると、Panorama 管理者のロールを表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	無し	はい	あり。
Access Domains（アクセス ドメイン）	管理者が、Panorama 管理者のアクセス ドメイン設定を表示、追加、編集、削除、またはコピーできるかどうかを指定します（この権限はアクセス ドメインの設定へのアク	Panorama：あり。 デバイス グループ/テンプレート：無し	あり。	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	セスのみを制御し、アクセス ドメインに割り当てられたデバイス グループ、テンプレート、およびファイアウォール コンテキストへのアクセスは制御しません）。 この権限を読み取り専用に設定すると、管理者は、Panorama のアクセス ドメイン設定を表示できますが、管理することはできません。 この権限を無効にすると、Panorama のアクセス ドメイン設定を表示または管理することができません。	*Device Group and Template* [デバイス グループとテンプレート]管理者が、アクセス ドメインに割り当てられたデバイス グループ、テンプレート、およびファイアウォール コンテキスト内の設定およびモニタリング データにアクセスできるように、管理者にアクセス ドメインを割り当てます。			
Authentication Profile（認	管理者が、Panorama 管理者の認証プロファイルを表示、追加、編集、削除、またはコ	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
証プロファイル）	ピーできるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、Panorama の認証プロファイルを表示できますが、管理することはできません。 この権限を無効にすると、管理者は Panorama の認証プロファイルを表示または管理することができません。				
Authentication Sequence（認証シーケンス）	管理者が、Panorama 管理者の認証シーケンスを表示、追加、編集、削除、またはコピーできるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、Panorama の認証シーケンスを表示できますが、管理することはできません。 この権限を無効にすると、管理者は、Panorama の認証シーケンスを表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。
User Identification ザー ID）	管理者が User-ID 接続セキュリティを設定したり、データ再配信ポイント（User-IDエージェントなど）を表示、追加、編集、削除したりできるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、User-ID 接続セキュリティおよび再配信ポイントの設定を表示でき	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	ますが、設定を管理できなくなります。 この権限を無効にすると、管理者は User-ID 接続セキュリティおよび再配信ポイントの設定を表示したり管理したりできなくなります。				
Managed Devices（管理対象デバイス）	管理者が、ファイアウォールを管理対象デバイスとして表示、追加、編集、または削除できるかどうか、およびそれらのファイアウォールでソフトウェアまたはコンテンツの更新をインストールできるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、管理対象ファイアウォールを表示できますが、それらのファイアウォールで更新を追加、削除、タグ付け、またはインストールすることはできません。 この権限を無効にすると、管理者は、管理対象ファイアウォールで更新を表示、追加、編集、タグ付け、削除、またはインストールすることができません。	Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。 （Device Group and Template [デバイス グループとテンプレート] ロールの場合は No[いいえ]）	あり。	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	デバイスのデプロイ権限を持つ管理者は、適用後も ***Panorama*** > ***Device*** (デバイス) ***Deployment*** (デプロイ) を選択し、管理対象のファイアウォールに更新コンテンツをインストールすることができます。				
Templates（テンプレート）	管理者が、テンプレートおよびテンプレート スタックを表示、編集、追加、または削除できるかどうかを指定します。	Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。（Device Group [デ	あり。	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	この権限を読み取り専用に設定すると、管理者は、テンプレートおよびスタック設定を表示できますが、管理することはできません。 この権限を無効にすると、管理者は、テンプレートおよびスタック設定を表示または管理することができません。	*Device Group and Template* [デバイス グループとテンプレート]管理者は、その管理者に割り当てられたアクセス ドメイン内にあるテンプレートおよびスタックのみを表示できます。	バイス グループ]とTemplate [テンプレート] 管理者の場合はNo[いいえ])		
Device Groups（デバイス グループ）	管理者が、デバイス グループを表示、編集、追加、または削除できるかどうかを指定します。	Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	この権限を読み取り専用に設定すると、管理者は、デバイス グループの設定を表示できますが、管理することはできません。 この権限を無効にすると、管理者はデバイス グループの設定を表示または管理することができません。	*Device Group and Template* [デバイス グループとテンプレート]管理者は、その管理者に割り当てられたアクセス ドメイン内にあるデバイス グループのみにアクセスできます。			
管理対象コレクタ	管理者が、管理対象コレクタを表示、編集、追加、または削除できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、管理対象コレクタの設定を表示できますが、管理することはできません。 この権限を無効にすると、管理者は管理対象コレクタの設定を表示、編集、追加、または削除することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	デバイスのデプロイ権限を持つ管理者は、適用後も ***Panorama*** > ***Device*** (デバイス) ***Deployment*** (デプロイ) オプションを使用し、管理対象のコレクタに更新コンテンツをインストールすることができます。				
コレクタ グループ	管理者が、コレクタ グループを表示、編集、追加、または削除できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、コレクタ グループを表示できますが、管理することはできません。 この権限を無効にすると、管理者はコレクタ グループを表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。
VMware Service Manager	管理者が、VMware Service Manager の設定を表示および編集できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は設定を表示できますが、関連する設定または操作手順を実行することはできません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	この権限を無効にすると、管理者は設定を表示したり、関連する設定または操作手順を実行したりすることができません。				
証明書の管理	Panorama の [証明書の管理] 権限のすべてについて、デフォルト状態を設定（有効または無効）します。	Panorama：あり。 デバイス グループ/テンプレート：無し	あり。	無し	あり。
証明書	管理者が、証明書を表示、編集、生成、削除、失効、更新、またはエクスポートできるかどうかを指定します。この権限により、管理者が HA キーをインポートまたはエクスポートできるかどうかも指定します。 この権限を読み取り専用に設定すると、管理者は、Panorama の証明書を表示できますが、証明書または HA キーを管理することはできません。 この権限を無効にすると、管理者は Panorama の証明書または HA キーを表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。
証明書プロファイル	管理者が、Panorama の証明書プロファイルを表示、追加、編集、削除、またはコピーできるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、Panorama の証明書プロファイルを表示できますが、管理することはできません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	この権限を無効にすると、Panorama の証明書プロファイルを表示または管理することができません。				
SSL/TLS Service Profile	管理者が、SSL/TLS サービス プロファイルを表示、追加、編集、削除、またはコピーできるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、SSL/TLS サービス プロファイルを表示できますが、管理することはできません。 この権限を無効にすると、SSL/TLS サービス プロファイルを表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。
ログ設定	ログ設定の権限すべてについて、デフォルト状態（有効または無効）を設定します。	Panorama：あり。 デバイス グループ/テンプレート：無し	あり。	無し	あり。
システム<:so>システム	管理者が、外部サービス（Syslog、電子メール、、SNMP トラップ、あるいは HTTP サーバー）へのシステム ログの転送を制御する設定項目を表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、システム ログの転送設定を表示できますが、管理することはできません。 この権限を無効にすると、管理者は設定を表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	この権限は、*Panorama* およびログコレクタが生成するシステム ログのみに関係します。コレクタ グループ権限（***Panorama*** > ***Collector Groups*** (コレクタ グループ)）は、ログコレクタがファイアウォールから受信するシステム ログの転送を制御します。***Device*** (デバイス) > ***Log Settings*** (ログ設定) > System (システム) 権限は、ファイアウォールから外部サービスに直接行うログ転送を制御します（ログコレクタの集約は行わない）。				
CONFIG コンフィグ	管理者が、外部サービス（Syslog、電子メール、、SNMP トラップ、あるいは HTTP サーバー）への設定ログの転送を制御する設定項目を表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、設定ロ	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	グの転送設定を表示できますが、管理することはできません。 この権限を無効にすると、管理者は設定を表示または管理することができません。 この権限は、*Panorama* およびログコレクタが生成する設定ログにのみ関係します。コレクタ グループ権限（***Panorama*** > ***Collector Groups***（コレクタ グループ）は、ログコレクタがファイアウォールから受信する設定ログの転送を制御します。***Device***（デバイス） > ***Log Settings***（ログ設定） >Config (設定) 権限は、ファイアウォールから外部サービスに直接行うログ転送を制御します（ログコレクタの集約は行わない）。				
User-ID	管理者が、外部サービス（Syslog、電子メール、、SNMP トラップ、あるいは HTTP サーバー）への	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	User-ID ログの転送を制御する設定項目を表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、設定ログの転送設定を表示できますが、管理することはできません。 この権限を無効にすると、管理者は設定を表示または管理することができません。				

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	この権限は、*Panorama* が生成する *User-ID* ログにのみ関係します。コレクタ グループ権限（***Panorama*** > ***Collector Groups*** (コレクタ グループ)）は、ログコレクタがファイアウォールから受信する *User-ID* ログの転送を制御します。***Device*** (デバイス) > ***Log Settings*** (ログ設定) > User-ID 権限は、ファイアウォールから外部サービスに直接行うログ転送を制御します（ログコレクタの集約は行わない）。				
HIP マッチ	管理者が、レガシー モードの Panorama 仮想アプライアンスから外部サービス（Syslog、電子メール、、SNMP トラップ、あるいは HTTP サーバー）への HIP マッチ ログの転送を制御する設定項目を表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、HIP マッ	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	チ ログの転送設定を表示できますが、管理することはできません。 この権限を無効にすると、管理者は設定を表示または管理することができません。 コレクタ グループ権限（***Panorama* > *Collector Groups* (**コレクタ グループ**)**）は、ログコレクタがファイアウォールから受信する *HIP* マッチ ログの転送を制御します。***Device* (**デバイス**) > *Log Settings* (**ログ設定**) >** HIP Match (HIP マッチ) 権限は、ファイアウォールから外部サービスに直接行うログ転送を制御します（ログコレクタの集約は行わない）。				
グローバルな保護	管理者が、レガシー モードの Panorama 仮想アプライアンスから外部サービス（Syslog、電子メール、、SNMP トラップ、あるいは HTTP サーバー）への GlobalProtect ログの転送を制御する設定項目を	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、GlobalProtect ログの転送設定を表示できますが、管理することはできません。 この権限を無効にすると、管理者は設定を表示または管理することができません。 コレクタ グループ権限（***Panorama* > *Collector Groups*** ***(***コレクタ グループ***)***）は、ログコレクタがファイアウォールから受信する *GlobalProtect* ログの転送を制御します。***Device*** ***(***デバイス***) > Log Settings (***ログ設定***) GlobalProtect*** 権限は、ファイアウォールから外部サービスに直接行うログ転送を制御します（ログコレクタの集約は行わない）。				
製品連携	管理者が、レガシー モードの Panorama 仮想アプライアンスから外部サービス（Syslog、電子メール、、SNMP ト	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	ラップ、あるいは HTTP サーバー）への相関ログの転送を制御する設定項目を表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、相関ログの転送設定を表示できますが、管理することはできません。 この権限を無効にすると、管理者は設定を表示または管理することができません。 コレクタ グループ権限（***Panorama* > *Collector Groups* (**コレクタ グループ**)**）は、*Panorama* モードの *Panorama* バーチャル アプライアンスあるいは *Panorama M-Series* アプライアンスからの相関ログの転送を制御します。				
トラフィック	管理者が、レガシー モードの Panorama 仮想アプライアンスから外部サービス（Syslog、電子メール、、SNMP トラップ、あるいは HTTP サーバー）へのトラフィック ログの転送を制御する設定項目を	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、トラフィック ログの転送設定を表示できますが、管理することはできません。 この権限を無効にすると、管理者は設定を表示または管理することができません。 コレクタ グループ権限（***Panorama* > *Collector Groups* (**コレクタ グループ**)**）は、ログ コレクタがファイアウォールから受信するトラフィック ログの転送を制御します。ログ転送権限（***Objects* (**オブジェクト**)** > ***Log Forwarding* (**ログ転送**)**）は、ファイアウォールから外部サービスに直接行うログ転送を制御します（ログコレクタの集約は行わない）。				
脅威	管理者が、レガシー モードの Panorama 仮想アプライアンスから外部サービス（Syslog、電子メール、、SNMP ト	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	ラップ、あるいは HTTP サーバー）への脅威ログの転送を制御する設定項目を表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、脅威ログの転送設定を表示できますが、管理することはできません。 この権限を無効にすると、管理者は設定を表示または管理することができません。 コレクタ グループ権限（***Panorama > Collector Groups*** **(**コレクタ グループ**)**）は、ログコレクタがファイアウォールから受信する脅威ログの転送を制御します。ログ転送権限（***Objects*** **(**オブジェクト**)** ***> Log Forwarding*** **(**ログ転送**)**）は、ファイアウォールから外部サービスに直接行うログ転送を制御します（ログコレクタの集約は行わない）。				

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
WildFire	管理者が、Panorama 仮想アプライアンスから外部サービス（Syslog、電子メール、または SNMP トラップ サーバー）への WildFire ログの転送を制御する設定項目を表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、WildFire ログの転送設定を表示できますが、管理することはできません。 この権限を無効にすると、管理者は設定を表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	コレクタ グループ権限（***Panorama*** > ***Collector Groups*** ***(***コレクタ グループ***)***）は、ログ コレクタがファイアウォールから受信する *WildFire* ログの転送を制御します。ログ転送権限（***Objects (***オブジェクト***)*** > ***Log Forwarding (***ログ転送***)***）は、ファイアウォールから外部サービスに直接行うログ転送を制御します（ログコレクタの集約は行わない）。				
サーバー プロファイル	サーバー プロファイルの権限すべてについて、デフォルト状態（有効または無効）を設定します。	Panorama：あり。 デバイス グループ/テンプレート：無し	あり。	無し	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	これらの権限は、*Panorama* あるいはログコレクタから収集するログの転送で使用されるサーバー プロファイルまたは *Panorama* 管理者の認証に使用されるサーバープロファイルにのみ関係します。***Device (デバイス)*** > Server Profiles (サーバープロファイル) 権限は、ファイアウォールから外部サービスへのログの直接転送、またはファイアウォール管理者の認証で使用されるサーバー プロファイルへのアクセスを制御します。				
SNMP トラップ	管理者が、SNMP トラップ サーバーのプロファイルを表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、SNMP トラップ サーバーのプロファイルを表示できますが、管理することはできません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	この権限を無効にすると、管理者は SNMP トラップ サーバーのプロファイルを表示または管理することができません。				
Syslog	管理者が、Syslog サーバーのプロファイルを表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、Syslog サーバーのプロファイルを表示できますが、管理することはできません。 この権限を無効にすると、管理者は Syslog サーバーのプロファイルを表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。
電子メール	管理者が、電子メール サーバーのプロファイルを表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、電子メール サーバーのプロファイルを表示できますが、管理することはできません。 この権限を無効にすると、管理者は電子メール サーバーのプロファイルを表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。
RADIUS	管理者が、Panorama 管理者の認証に使用される RADIUS サーバーのプロファイルを表	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、RADIUS サーバーのプロファイルを表示できますが、管理することはできません。 この権限を無効にすると、管理者は RADIUS サーバーのプロファイルを表示または管理することができません。				
TACACS+	管理者が、Panorama 管理者の認証に使用される TACACS+ サーバーのプロファイルを表示および設定できるかどうかを指定します。 この権限を無効にすると、管理者にはそのノードが表示されず、認証プロファイルで参照される TACACS+ サーバーの設定を行うことができません。 この権限を読み取り専用に設定すると、管理者は既存の TACACS+ サーバー プロファイルを表示できますが、プロファイルを追加または編集することはできません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。
LDAP	管理者が、Panorama 管理者の認証に使用される LDAP サーバーのプロファイルを表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、LDAP サーバーのプロファイルを表	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	示できますが、管理することはできません。 この権限を無効にすると、管理者は LDAP サーバーのプロファイルを表示または管理することができません。				
Kerberos	管理者が、Panorama 管理者の認証に使用される Kerberos サーバーのプロファイルを表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、Kerberos サーバーのプロファイルを表示できますが、管理することはできません。 この権限を無効にすると、管理者は Kerberos サーバーのプロファイルを表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。
SAML アイデンティティ プロバイダ	管理者が、Panorama 管理者の認証に使用される SAML アイデンティティ プロバイダ（IdP）サーバーのプロファイルを表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、SAML IdP サーバーのプロファイルを表示できますが、管理することはできません。 この権限を無効にすると、管理者は SAML IdP サーバーのプロファイルを表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
スケジュールされた設定のエクスポート	管理者が、Panorama のスケジュールされた設定のエクスポートを表示、追加、編集、削除、またはコピーできるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者はスケジュールされたエクスポートを表示できますが、管理することはできません。 この権限を無効にすると、管理者はスケジュールされたエクスポートを表示または管理することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	あり。	無し	あり。
ソフトウェア	管理者が、Panorama 管理サーバーにインストールされるソフトウェア更新に関する情報の表示、更新のダウンロード、アップロード、またはインストール、および関連付けられているリリース ノートの表示を実行できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、Panorama のソフトウェア更新に関する情報を表示し、関連付けられているリリース ノートを表示できますが、関連する操作は何も実行できません。 この権限を無効にすると、管理者は、Panorama のソフトウェア更新を表示したり、関連付けられているリリース ノートを表示したり、関連す	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	る操作を実行したりすることができません。 ***Panorama*** > Device Deployment (デバイスのデプロイ) > Software (ソフトウェア) 権限は、ファイアウォールにデプロイされる *PAN-OS* および専用のログ コレクタにデプロイされる *Panorama* ソフトウェアへのアクセスを制御します。				
ダイナミック更新	管理者が、Panorama 管理サーバー上にインストールされたコンテンツ更新（たとえば、WildFire の更新）に関する情報の表示、更新のダウンロード、アップロード、インストール、または逆戻り、および関連付けられているリリース ノートの表示を実行できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、Panorama のコンテンツ更新に関する情報を表示し、関連付けられているリリースノートを表示できますが、関連する操作は何も実行できません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	この権限を無効にすると、管理者は、Panorama のコンテンツ更新を表示したり、関連付けられているリリース ノートを表示したり、関連する操作を実行したりすることができません。 **Panorama** > Device Deployment (デバイスのデプロイ) > Dynamic Updates (動的更新) 権限は、ファイアウォールと専用ログ コレクタにデプロイされるコンテンツ更新へのアクセスを制御します。				
Support（サポート）	管理者が、Panorama のサポート ライセンス情報、製品のアラート、セキュリティ アラートの表示、サポート ライセンスのアクティベーション、およびケースの管理を実行できるかどうかを指定します。スーパーユーザーの管理者のみがテクニカルサポート ファイルを生成できます。 この権限を読み取り専用に設定すると、管理者は、Panorama のサポート情報、製品のアラート、およびセキュリティ アラートを表示できますが、サポート ライセ	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	ンスをアクティブにしたり、テクニカル サポート ファイルを生成したり、ケースを管理したりすることはできません。 この権限を無効にすると、管理者は、Panorama のサポート情報、製品のアラート、またはセキュリティ アラートの表示、サポート ライセンスのアクティベーション、テクニカル サポート ファイルの生成、またはケースの管理を行うことができません。				
デバイスのデプロイ	ライセンスおよびソフトウェア更新あるいはコンテンツ更新をファイアウォールおよびログコレクタにデプロイするのに関連するすべての権限のデフォルトの状態（有効あるいは無効）を設定します。 **Panorama** > ソフトウェアおよび **Panorama** > 動的更新 権限は、*Panorama* 管理サーバーにインストールされるソフトウェアおよびコンテンツ更新を制御します。	Panorama：あり。 デバイス グループ/テンプレート：あり。	あり。	無し	あり。
ソフトウェア	管理者が、ファイアウォールおよびログ コレクタにインストールされるソフトウェア更新に関する情報の表示、更新	Panorama：あり。 デバイス グループ/テンプレート：あり。	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	のダウンロード、アップロード、またはインストール、および関連付けられているリリース ノートの表示を実行できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、ソフトウェア更新に関する情報を表示し、関連付けられているリリース ノートを表示できますが、ファイアウォールまたは専用ログ コレクタに更新をデプロイすることはできません。 この権限を無効にすると、管理者は、ソフトウェア更新に関する情報を表示したり、関連付けられているリリース ノートを表示したり、ファイアウォールまたは専用ログ コレクタに更新をデプロイしたりすることができません。				
GlobalProtect クライアント	管理者が、ファイアウォール上の GlobalProtect アプリケーション ソフトウェア更新の表示、更新のダウンロード、アップロード、またはアクティベーション、および関連付けられているリリース ノートの表示を実行できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、GlobalProtect アプリケーションのソフトウェア更新に関する情報を表示し、関連付けられているリリース ノート	Panorama：あり。 デバイス グループ/テンプレート：あり。	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	を表示できますが、ファイアウォール上の更新をアクティブにすることはできません。 この権限を無効に設定すると、管理者は、GlobalProtect アプリケーションのソフトウェア更新に関する情報を表示したり、関連付けられているリリース ノートを表示したり、ファイアウォール上の更新をアクティブにしたりすることができません。				
ダイナミック更新	管理者が、ファイアウォールおよび専用ログ コレクタにインストールされるコンテンツ更新（たとえば、アプリケーション更新）に関する情報の表示、更新のダウンロード、アップロード、またはインストール、および関連付けられているリリース ノートの表示を実行できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、コンテンツ更新に関する情報を表示し、関連付けられているリリース ノートを表示できますが、ファイアウォールまたは専用ログ コレクタに更新をデプロイすることはできません。 この権限を無効にすると、管理者は、コンテンツ更新に関する情報を表示したり、関連付けられているリリース ノートを表示したり、ファイア	Panorama：あり。 デバイス グループ/テンプレート：あり。	はい	はい	あり。

アクセス レベル	説明	管理者ロールの使用可・不可	有効化	読み取り専用	無効化
	ウォールまたは専用ログ コレクタに更新をデプロイしたりすることができません。				
ライセンス	管理者が、ファイアウォールのライセンスを表示、更新、またはアクティブにすることができるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、ファイアウォールのライセンスを表示できますが、それらのライセンスを更新したり、アクティブにしたりすることはできません。 この権限を無効にすると、管理者は、ファイアウォールのライセンスを表示、更新、またはアクティブにすることができません。	Panorama：あり。 デバイス グループ/テンプレート：あり。	はい	はい	あり。
マスター キーおよび診断	管理者が、Panorama で秘密鍵を暗号化するためのマスター キーを表示および設定できるかどうかを指定します。 この権限を読み取り専用に設定すると、管理者は、Panorama のマスター キー設定を表示できますが、変更することはできません。 この権限を無効にすると、管理者は Panorama のマスター キー設定を表示または編集することができません。	Panorama：あり。 デバイス グループ/テンプレート：無し	はい	はい	あり。

操作設定へのきめ細かなアクセスを提供する

管理者がアクセスできる操作設定を定義するには、ファイアウォールの管理者ロール プロファイルを作成または編集するときに (デバイス > 管理者ロール)、**Web UI** タブの [操作] オプションまでスクロールします。

アクセス レベル	の意味	**Enable** [有効化]	読み取り専用	無効化
再起動	ファイアウォールを再起動します。ファイアウォールはすべてのユーザをログアウトし、PAN-OSソフトウェアとアクティブな設定をリロードし、既存のセッションを閉じてログに記録し、再起動を開始した管理者の名前を示すシステムログエントリを作成します。	あり	N/A	あり
テクニカルサポートファイルの作成	Palo Alto Networks サポートチームがファイアウォールで発生する可能性のある問題のトラブルシューティングに使用できる技術サポート システム ファイルを生成します。	あり	N/A	あり
Stats Dump ファイル を生成します。	ファイアウォールの過去 7 日間のネットワーク トラフィックを要約する一連の XML レポートを生成およびダウンロードします。	あり	N/A	あり
コアファイルをダウンロードする	ファイアウォールでシステム プロセス障害が発生した場合、プロセスの詳細と失敗の原因を含むコア ファイルが自動的に生成されます。このコアファイルをダウンロードして、Palo Alto Networks サポートケースにアップロードし、問題解決の詳細なサポートを受けることができます。	あり	N/A	あり
デバッグおよび管理 Pcap ファイルをダウンロードする	ファイアウォールでパケットキャプチャの失敗が発生した場合、ファイアウォールは、失敗した理由のデバッグと管理の詳細を含むパケットキャプチャ（pcap）ファイルを生成します。問題解決のサポートを受けるには、ファイルのダウンロード後に Palo Alto Networks サポートケースにアップロードします。	あり	N/A	あり。

Panorama Web インターフェイスのアクセス権限

Panorama のカスタム管理者ロールにより、Panorama でのオプションへのアクセス権限、および [デバイス グループとテンプレート] （**Policies**[ポリシー]、**Objects**[オブジェクト]、**Network**[ネットワーク]、**Device**[デバイス] タブ）へのアクセスのみを許可する権限を定義できます。

作成することができる管理者ロールは、**Panorama** と **Device Group and Template** [デバイス グループとテンプレート]です。CLI アクセス権限を **Device Group and Template** [デバイス グループとテンプレート]管理者ロール プロファイルに割り当てることはできません。CLI のスーパーユーザー権限を **Panorama** 管理者ロール プロファイルに割り当てると、そのロールを持つ管理者は、割り当てる Web インターフェイスの権限に関係なく、すべての機能にアクセスできます。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
Dashboard（ダッシュボード）	**Dashboard** [ダッシュボード]タブへのアクセスを制御します。この権限を無効にすると、その管理者にはこのタブが表示されなくなり、Dashboard ウィジェットのいずれにもアクセスできません。	あり。	無し	あり。
ACC	アプリケーション コマンド センター（ACC）へのアクセスを制御します。この権限を無効にすると、**ACC** タブが Web インターフェイスに表示されなくなります。ACC へのアクセス権限を与えると同時にユーザーのプライバシーを守るには、**Privacy (プライバシー)** > **Show Full IP Addresses (完全 IP アドレスの表示)** オプションまたは **Show User Names In Logs And Reports (ログおよびレポート内のユーザー名の表示)** オプションを無効にすることができます。	あり。	無し	あり。
監視	**Monitor**[監視] タブへのアクセスを制御します。この権限を無効にすると、その管理者には **Monitor**[監視]タブが表示されなくなり、ログ、パケット キャプチャ、セッション情報、レポート、またはアプリケーション スコープのいずれにもアクセスできません。管理者が表示できるモニタリング情報をより詳細に制御するには、Monitor (監視) オプションを有効にしたままで、監視タブに対する詳細なアクセス権限の付与での説明に従ってタブ上	あり。	無し	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	の特定のノードを有効または無効にします。			
レポートを生成	**Policies**[ポリシー] タブへのアクセスを制御します。この権限を無効にすると、その管理者には **Policies** [ポリシー]タブが表示されなくなり、どのポリシー情報にもアクセスできません。たとえば、特定のタイプのポリシーへのアクセスを有効にする、またはポリシー情報への読み取り専用アクセスを有効にするなど、管理者が表示できるポリシー情報をより詳細に制御するには、**Policies (**ポリシー**)** オプションを有効にしたままで、ポリシータブに対する詳細なアクセス権限の付与での説明に従ってタブ上の特定のノードを有効または無効にします。	あり。	無し	あり。
オブジェクト	**Objects**[オブジェクト] タブへのアクセスを制御します。この権限を無効にすると、その管理者には **Objects**[オブジェクト] タブが表示されなくなり、オブジェクト、セキュリティ プロファイル、ログ転送プロファイル、復号プロファイル、またはスケジュールのいずれにもアクセスできません。管理者が表示できるオブジェクトをより詳細に制御するには、**Objects (**オブジェクト**)** オプションを有効にしたままで、オブジェクト タブに対する詳細なアクセス権限の付与での説明に従ってタブ上の特定のノードを有効または無効にします。	あり。	無し	あり。
Network（ネットワーク）	**Network**[ネットワーク] タブへのアクセスを制御します。この権限を無効にすると、その管理者には **Network**[ネットワーク] タブが表示されなくなり、インターフェイス、ゾーン、VLAN、バーチャル ワイヤー、仮想ルーター、IPSec トンネル、DHCP、DNS プロキシ、GlobalProtect、QoS 設定情報、またはネットワーク プロファイルのいずれにもアクセスできません。管理者が表示できるオブジェクトをより詳細に制御	あり。	無し	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	するには、**Network (ネットワーク)** オプションを有効にしたままで、ネットワーク タブに対する詳細なアクセス権限の付与での説明に従ってタブ上の特定のノードを有効または無効にします。			
Device（デバイス）	**Device**[デバイス] タブへのアクセスを制御します。この権限を無効にすると、その管理者には **Device** [デバイス]タブが表示されなくなり、ユーザー ID、高可用性、サーバー プロファイル、または証明書設定情報などのファイアウォール全体の設定情報のいずれにもアクセスできません。管理者が表示できるオブジェクトをより詳細に制御するには、**Device (デバイス)** オプションを有効にしたままで、デバイス タブに対する詳細なアクセス権限の付与での説明に従ってタブ上の特定のノードを有効または無効にします。 ***Device** [デバイス]タブへのフル アクセス権限を有効にしていても、**Admin Roles** [管理者ロール]または **Administrators** [管理者]ノードに対するロールベース管理者のアクセス権限を有効にすることはできません。*	あり。	無し	あり。
Panorama	**Panorama** タブへのアクセスを制御します。この権限を無効にすると、その管理者には **Panorama** タブが表示されず、Managed Devices [管理対象デバイス]、Managed Collectors [管理対象コレクタ]、または Collector Groups [コレクタ グループ]などの Panorama 全体の設定情報にアクセスできなくなります。 管理者が表示できるオブジェクトをより詳細に制御するには、**Panorama** オプションを有効にしたままで、Panorama タブに対する詳細なアクセス権限の付与での説明に従ってタブ上の特定のノードを有効または無効にします。	あり。	無し	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
専用	管理者ロール プロファイルでのユーザーのプライバシー設定の定義に記載されているプライバシー設定へのアクセスを制御します。	あり。	無し	あり。
検証	無効にすると、管理者は設定を検証できません。	あり。	無し	あり。
Save（保存）	次に記載されている保存権限すべてを対象にして、デフォルトの状態（有効あるいは無効）を設定します（Partial Save (一部保存) および Save For Other Admins (他の管理者のために保存)）。	あり。	無し	あり。
• 一部保存	無効にすると、管理者はいずれかの管理者が Panorama 設定に加えた変更を保存できません。	あり。	無し	あり。
• 他の管理者のために保存	無効にすると、管理者は他の管理者が Panorama 設定に加えた変更を保存できません。	あり。	無し	あり。
コミット	次に記載されているすべてのコミット、プッシュ、復元権限をデフォルトの状態（有効あるいは無効）にセットします（Panorama、Device Groups (デバイス グループ)、Templates (テンプレート)、Force Template Values (テンプレートの値を適用)、Collector Groups (コレクタ グループ)、WildFire Appliance Clusters (WildFire アプライアンス クラスタ)）。	あり。	無し	あり。
• Panorama	無効にすると、自分が行った変更も含め、あらゆる管理者が行った設定変更を管理者がコミットすることも元に戻すこともできなくなります。	あり。	無し	あり。
• 他の管理者のためにコミット	無効にすると、他の管理者が行った設定変更を管理者がコミットすることも元に戻すこともできなくなります。	あり。	無し	あり

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
• すべての変更をプッシュ	無効にすると、管理者は管理者が行ったすべての構成変更をプッシュできません。	あり	無し	あり
• 他の管理者をプッシュする	無効にすると、管理者は別の管理者が行った構成変更を選択してプッシュすることはできません。	あり	無し	あり
• オブジェクトレベルの変更	無効にすると、管理者はプッシュする個々の構成オブジェクトを選択することはできません。	あり	無し	あり。
Device Groups（デバイス グループ）	無効にすると、管理者はデバイスグループに対する変更をプッシュできません。	あり。	無し	あり。
Templates（テンプレート）	無効にすると、管理者はテンプレートに対する変更をプッシュできなくなります。	あり。	無し	あり。
テンプレートの値を適用	この権限は、Push Scope Selection (プッシュ範囲の選択) ダイアログの **Force Template Values (**テンプレートの値を適用**)** オプションへのアクセスを制御します。 無効にすると、管理者はオーバーライドされたローカルのファイアウォール設定を、Panoramaがテンプレートからプッシュした設定で上書きすることができなくなります。	あり。	無し	あり。

アクセス レベル	の意味	Enable [有効化]	読み取り専用	無効化
	Force Template Values **(**テンプレートの値を適用**)**が有効な設定をプッシュする場合、ファイアウォールのオーバーライドされたすべての値がテンプレートの値で上書きされます。このオプションを使用する前にファイアウォールのオーバーライドされた値をチェックし、コミットによって予期せぬネットワークの障害が発生したり、これらのオーバーライドされた値によって問題が生じたりしないことを確認してください。			
コレクタ グループ	無効にすると、管理者はコレクタ グループに対する変更をプッシュできなくなります。	あり。	無し	あり。
WildFire アプライアンス クラスタ	無効にすると、管理者は WildFire アプライアンス クラスタに対する変更をプッシュできなくなります。	あり。	無し	あり。
タスク	無効にすると、管理者はタスク マネージャーにアクセスできなくなります。	あり。	無し	あり。
Global	グローバル設定への詳細なアクセス権限の指定に記載のグローバル設定（システムアラーム）へのアクセスを制御します。	あり。	無し	あり。

リファレンス：ポート番号の扱い

以下の表に、ファイアウォールおよびPanoramaが、相互の通信で、またはネットワーク上の他のサービスとの通信で使用するポートの一覧を示します。

- 管理機能で使用するポート
- HA で使用するポート
- Panorama で使用するポート
- GlobalProtect で使用するポート
- ユーザー ID で使用するポート
- IPSec に使用されるポート
- ルーティングに使用されるポート
- DHCP に使用されるポート
- インフラストラクチャに使用されるポート

管理機能で使用するポート

ファイアウォールおよび Panorama は次のポートを使用して管理機能を提供します。

Destination port	PROTOCOL	説明
22	TCP	クライアント システムからファイアウォールの CLI インターフェイスへの通信で使用します。
80	TCP	ファイアウォールが、OCSP レスポンダとして機能するときにオンライン証明書ステータス プロトコル（OCSP） 更新をリッスンするポート。
123	UDP	NTP 更新でファイアウォールが使用するポート。
443	TCP	クライアント システムからファイアウォールの Web インターフェイスへの通信で使用します。これは、仮想ネットワーク上の変更を追跡するためにVM監視を有効にすると、ファイアウォールと User-ID エージェントが更新を待機するポートです。 AWS 環境をモニタリングする場合、これは使用される唯一のポートです。 VMware vCenter/ESXi 環境をモニタリングする場合、デフォルトのリッスン ポートは 443 ですが、このポートは設定可能です。
4443	TCP	HTTPS の代替 SSL ポートとして使用されます。

Destination port	PROTOCOL	説明
162	UDP	ファイアウォール、Panorama、またはログ コレクタが SNMP マネージャへのトラップの転送に使用するポート。  *Palo Alto Networks* のファイアウォールでこのポートを開く必要はありません。このポートをリッスンするように *Simple Network Management Protocol*（*SNMP*）マネージャを設定する必要があります。詳細は、*SNMP* 管理ソフトウェアのドキュメントを参照してください。
161	UDP	ファイアウォールが、SNMP マネージャからのポーリング要求（GET メッセージ）をリッスンするポート。
514 514 6514	TCP UDP SSL	Syslog モニタリングの設定を行う場合にファイアウォール、Panorama、またはログ コレクタがログを Syslog サーバーに送信するために使用するポート、およびを行う場合にPAN-OS 統合ユーザー ID エージェントまたは Windows ベースのユーザー ID エージェントが認証 Syslog メッセージをリッスンするポート。
2055	UDP	NetFlow エクスポートの設定を行う場合にファイアウォールが NetFlow コレクタへの NetFlow レコードの送信で使用するデフォルトのポート。ただし、設定可能です。
5008	TCP	GlobalProtect モバイル セキュリティ マネージャが、GlobalProtect ゲートウェイからの HIP 要求をリッスンするポート。 サードパーティの MDM システムを使用する場合は、MDM ベンダーで必要とされるポートとは異なるポートを使用するようにゲートウェイを設定することができます。
6080 6081 6082	TCP TLS 1.2 TCP	User-ID™ 認証ポータルに使用されるポート: • NT LAN マネージャ (NTLM) 認証用 6080 • SSL/TLS サーバー プロファイルなしの認証ポータル用 6081 • SSL/TLS サーバー プロファイルを使用した認証ポータルの 6082
10443	SSL	ファイアウォールと Panorama が脅威に関するコンテキスト情報を提供したり、脅威調査をシームレスに Threat Vault と AutoFocus に移行するために使用するポート。

HA で使用するポート

高可用性（HA）ピアとして設定されるファイアウォールには、相互に通信して状態情報（HA1 制御リンク）を保持し、データを同期（HA2 データリンク）する機能が必要です。アクティブ/非アクティブ HA のデプロイの場合、ピア ファイアウォールは、セッションを所有する HA ピアにもパケットを転送する必要があります。HA3 リンクはレイヤー（MAC-in-MAC）リンクであり、レイヤー 3 アドレスまたは暗号化をサポートしていません。

Destination port	PROTOCOL	説明
28769 28260	TCP TCP	HA ピア ファイアウォール間のクリア テキスト通信用の HA1 制御リンクで使用されます。HA1 リンクはレイヤー 3 リンクのため、IP アドレスが必要です。
28	TCP	HA ピア ファイアウォール間の暗号化通信（SSH over TCP）用の HA1 制御リンクで使用されます。
28770	TCP	HA1 バックアップ リンク用のリッスン ポート。
28771	TCP	ハートビート バックアップで使用します。Palo Alto Networks では、HA1 または HA1 のバックアップ リンクでインバンド ポートを使用する場合、MGT インターフェイスでハートビート バックアップを有効にすることをお勧めします。
99 29281	IP UDP	セッションを同期するために HA2 リンクで使用して、HA ペア内のファイアウォール間で、テーブル、IPSec セキュリティの関連付け、および ARP テーブルを転送します。HA2 リンクのデータ フローは、（HA2 キープアライブを除いて）常に一方向であり、アクティブ ファイアウォール（アクティブ/パッシブ）またはアクティブ-プライマリ（アクティブ/アクティブ）からパッシブ ファイアウォール（アクティブ/パッシブ）またはアクティブ-セカンダリ（アクティブ/アクティブ）の方向に流れます。HA2 リンクはレイヤー 2 リンクであり、デフォルトで EtherType 0x7261 を使用します。 HA データ リンクは、IP（プロトコル番号 99）または UDP（ポート 29281）のいずれかを転送ポートとして使用するように設定することもできるため、HA データ リンクはサブネットをまたぐことができます。

Panorama で使用するポート

Panorama は次のポートを使用します。

Destination port	PROTOCOL	説明
22	TCP	クライアント システムから Panorama CLI インターフェイスへの通信で使用します。
443	TCP	クライアント システムから Panorama の Web インターフェイスへの通信で使用します。
444	TCP	Panorama および Cortex Data Lake 間の通信に使用します。
3978	TCP	Panorama と管理対象のファイアウォールあるいはコレクタ間の通信、およびコレクタ グループ内の管理対象コレクタ間の通信で使用されます。 • Panorama とファイアウォールの間の通信のため。この接続は、管理対象ファイアウォールから Panorama に開始され、ファイアウォールがログを Panoram に転送し、Panorama が設定変更をファイアウォールにプッシュする双方向データ交換を容易にします。コンテキストの切り替えコマンドは、同じ接続を使用して送信されます。 • ログ コレクタは、この宛先ポートを使用してログを Panorama に転送します。 • Panorama モードの M-Series アプライアンスでのデフォルトのログ コレクタとの通信、および専用ログ コレクタとの通信に使用されます。
28443	TCP	管理対象のデバイス（ファイアウォールおよびログコレクタ）が Panorama からソフトウェアおよびコンテンツ更新を取得するために使用します。 *PAN-OS 8.x* 以降のリリースを実行するデバイスのみ、このポートを介して更新コンテンツを取得できます。古いバージョンを実行しているデバイスについては、*Panorama* はポート *3978* を介して更新パッケージをプッシュします。
2876 （5.1 以降） 2826 （5.0 以降）	TCP TCP TCP	クリア テキスト通信を使用する Panorama HA ピア間の HA 接続および同期に使用します。通信は、どちらかのピアによって開始できます。

Destination port	PROTOCOL	説明
4916 （5.0 以前）		
28	TCP	暗号化通信（SSH over TCP）を使用する Panorama HA ピア間の HA 接続および同期に使用します。通信は、どちらかのピアによって開始できます。 ログ配信用のコレクタ グループ内のログ コレクタ間の通信で使用します。
2827 （6.0 以降） 4919 （5.1 以前）	TCP	ログ配信用のコレクタ グループ内のログ コレクタ間の通信で使用します。
2049	TCP	Panorama 仮想アプライアンスがログを NFS データストアに書き込むために使用します。
10443	SSL	Panorama が脅威に関するコンテキスト情報を提供したり、脅威調査をシームレスに Threat Vault と AutoFocus に移行するために使用するポート。
23000から23999の間	TCP、UDP、または SSL	Panorama および Traps ESM コンポーネント間の Syslog 通信に使用します。

GlobalProtect で使用するポート

GlobalProtect は次のポートを使用します。

Destination port	PROTOCO	説明
443	TCP	SSL トンネル接続のために、GlobalProtect アプリおよびポータル、あるいは GlobalProtect アプリおよびゲートウェイ間で使用されます。 また、GlobalProtect ゲートウェイは GlobalProtect アプリからホスト情報を収集し、ホスト情報プロファイル（HIP）チェックを行う際も、このポートを使用します。
4501	UDP	GlobalProtect アプリおよびゲートウェイ間の IPSec トンネル接続に使用されます。

さまざまなポートとアドレスの GlobalProtect へのアクセスを可能にするループバック インターフェイスの使用方法に関するヒントとして、GlobalProtect ポータル ページをどのポートからもアクセスできるように設定できるかどうかを参照してください。

ユーザー ID で使用するポート

User-ID は、ユーザーの IP アドレスとユーザー名およびグループ メンバーシップをマッピングできるようにする機能で、ユーザーまたはグループベースのポリシーを有効にし、ネットワークでのユーザー アクティビティを可視化することができます（たとえば、脅威の被害者になっている可能性があるユーザーまですばやくトラックダウンすることができます）。このマッピングを実行するため、ファイアウォール、User-IDエージェント（Windows ベース システムにインストールされているエージェントか、ファイアウォールで実行されている PAN-OS 統合エージェントのどちらか）、またはターミナル サーバー エージェントは、グループ マッピングおよびユーザーマッピングを実行するため、ネットワークのディレクトリ サービスに接続できるようになっている必要があります。また、ファイアウォールの外部システムでエージェントが実行されている場合、それらのエージェントでは、IP アドレスからユーザー名へのマッピングをファイアウォールに通信するため、ファイアウォールに接続できるようになっている必要があります。以下の表に、ユーザー ID での通信要件と、接続を確立するために必要なポート番号の一覧を示します。

Destination port	PROTOCOL	説明
389	TCP	ユーザー対グループのマッピングを行うため、ファイアウォールが LDAP サーバーへの接続（プレーンテキストまたは Start Transport Layer Security （Start TLS））に使用するポート。
3268	TCP	ユーザー対グループのマッピングを行うため、ファイアウォールが Active Directory グローバル カタログ サーバーへの接続（プレーンテキストまたは Start TLS）に使用するポート。
636	TCP	ユーザー対グループのマッピングを行うため、ファイアウォールが LDAP サーバーとの LDAP over SSL 接続に使用するポート。
3269	TCP	ユーザー対グループのマッピングを行うため、ファイアウォールが Active Directory グローバル カタログ サーバーとの LDAP over SSL 接続に使用するポート。
514 6514	TCP UDP SSL	User-ID を設定してユーザーマッピング用に Syslog 送信者を監視する場合に、User-ID エージェントが認証 Syslog メッセージをリッスンするポート。次のように、ポートはエージェントおよびプロトコルのタイプによって決まります。 • PAN-OS 統合 User-ID エージェント—SSL 用にポート 6514、UDP 用に ポート 514。

Destination port	PROTOCOL	説明
		• Windows ベースの User-ID エージェント—TCP および UDP の両方でポート 514。
5007	TCP	ファイアウォールが、User-ID または ターミナル サーバー エージェントからのユーザー マッピング情報をリッスンするポート。エージェントは、新規または更新されたマッピングを検出するといつでも、IP アドレスとユーザー名のマッピングをタイムスタンプと一緒に送信します。また、定期的にファイアウォールに接続し、既知のマッピングを更新します。
5006	TCP	User-ID エージェントが XML API 要求をリッスンするポート。この通信の送信元は、通常、API を呼び出すスクリプトを実行しているシステムです。
88	UDP/TCP	ユーザー ID エージェントが Kerberos サーバーに対する認証で使用するポート。ファイアウォールは最初に UDP を試行し、TCP にフォールバックします。
1812	UDP	ユーザー ID エージェントが RADIUS サーバーに対する認証で使用するポート。
49	TCP	ユーザー ID エージェントが TACACS+ サーバーに対する認証で使用するポート。
135	TCP	ユーザー ID エージェントが、Microsoft Remote Procedure Call（RPC）エンドポイント マッパーとの TCP ベースの WMI 接続を確立するために使用するポート。エンドポイント マッパーは、49152 ～ 65535 のポート範囲でランダムに割り当てられたポートをエージェントに割り当てます。エージェントは、この接続を使用して、Exchange Server または AD サーバーのセキュリティ ログ、セッション テーブルに対する RPC クエリを実行します。このポートは、ターミナル サーバーへのアクセスにも使用されます。 ユーザー ID エージェントは、クライアント システムに接続して Windows Management Instrumentation （WMI）プロービングを実行する場合にも、このポートを使用します。
139	TCP	ユーザー ID エージェントが、AD サーバーへの TCP ベースの NetBIOS 接続を確立し、セキュリティ ログとセッション情報に対する RPC クエリを送信できるようにするために使用するポート。

Destination port	PROTOCOL	説明
		ユーザー ID エージェントは、NetBIOS プロービング（Windows ベースのユーザー ID エージェントでのみサポート）でクライアント システムに接続する場合にも、このポートを使用します。
445	TCP	ユーザー ID エージェントが、ユーザーのログオン情報（印刷スプーラーおよび Net Logon）にアクセスする場合に、AD サーバーへの TCP ベースの SMB 接続を使用して Active Directory（AD）に接続する場合に使用するポート。
5985	HTTP	ユーザー ID エージェントが HTTP 経由の WinRM プロトコルでセキュリティログとセッション情報を監視する場合に使用するポート。
5986	HTTPS	ユーザー ID エージェントが HTTPS 経由の WinRM プロトコルでセキュリティログとセッション情報を監視する場合に使用するポート。
5009	TCP	ファイアウォールがターミナル サーバー エージェントへの接続に使用するポート。

IPSec に使用されるポート

ファイアウォールおよび Panorama は次のポートを使用して管理機能を提供します。

宛先ポート	PROTOCOL	説明
500	UDP	リモート IKE ピアと接続するために管理プレーン上の IKE によって使用されるポート。
4500	UDP	リモート IKE ピアと接続するために管理プレーン上の IKE によって使用されるポート。
4510	UDP	IKE に要求を送信するためにデータプレーンが使用するポート。
4511	UDP	`keymgr` に要求を送信するためにデータプレーンによって使用されるポート。

ルーティングに使用されるポート

ファイアウォールおよび Panorama は次のポートを使用して管理機能を提供します。

宛先ポート	PROTOCOL	説明
179	TCP	ピアに接続するためにBGPが使用するポート。
3784 3785 4784	UDP	ピアへの接続に BGP によって使用されるポート。
520	UDP	RIPv2 に使用されるポート。
89	IP	OSPF に使用されるポート。
103	IP	Protocol Independent Multicast（PIM）に使用されるポート。

DHCP に使用されるポート

ファイアウォールおよび Panorama は次のポートを使用して管理機能を提供します。

宛先ポート	PROTOCOL	説明
67 68 546 547	UDP	DHCP サーバーのリスニング ポートとして使用されるポート。

インフラストラクチャに使用されるポート

ファイアウォールと Panorama は、インフラストラクチャの機能に次のポートを使用します。

宛先ポート	PROTOCOL	説明
111	TCP / UDP	ポート マッパーとして使用されるポート。
23	TCP / UDP	Telnetアプリケーションプロトコルに使用されるポート。
69	TCP / UDP	TFTPに使用されるポート。
2049	TCP / UDP	ネットワークファイルシステム（NFS）に使用されるポート。
28260	TCP	内部プロセス用の内部 sysd IPC 通信で使用されるポート。

宛先ポート	PROTOCOL	説明
28261	TCP	内部プロセスを管理するために内部 マスター アプリケーションで使用されるポート。
動的	TCP / UDP	管理プレーンのホストデータプレーンファイルシステムに対する NFS 操作で使用される動的ポート。

ファイアウォールの工場出荷時設定へのリセット

ファイアウォールを工場出荷時設定にリセットすると、すべての設定とログが失われます。

STEP 1 | ファイアウォールへのコンソール接続を設定します。

1. コンピュータからコンソール ポートにシリアル ケーブルを接続し、ターミナル エミュレーション ソフトウェア (9600-8-N-1) を使用してファイアウォールに接続します。

   コンピュータが *9* ピン シリアル ポートを装備していない場合は、*USB*-シリアル ポート コネクタを使用してください。

2. ログイン認証情報を入力します。
3. 以下の CLI コマンドを入力します。

   debug system maintenance-mode

   ファイアウォールがメンテナンス モードで再起動します。

STEP 2 | システムを工場出荷時設定にリセットします。

1. ファイアウォールが再起動したら、**Enter** を押してメンテナンス モードのメニューに進みます。
2. **Factory Reset** [工場出荷時の設定にリセット]を選択し、**Enter** を押します。
3. **Factory Reset** [工場出荷時の設定にリセット]を選択し、**Enter** をもう一度押します。

   ファイアウォールが設定なしで再起動します。ファイアウォールにログインするためのデフォルトのユーザー名/パスワードは、admin/admin です。

   ファイアウォールで初期設定を実行し、ネットワーク接続を設定する方法については、管理ネットワークへのファイアウォールの統合を参照してください。

ファイアウォールのブート処理

ブート処理によりファイアウォールの構成プロセスやライセンス処理の速度が向上し、インターネットアクセスを使用する/使用しないネットワーク上で運転可能になります。このブート処理では、基本設定ファイル（init-cfg.txt）でファイアウォールを構成し、Panoramaに接続して完全な設定を入手できるようにするか、基本設定ファイルおよび任意のbootstrap.xmlファイルでファイアウォールを完全に構成するか、選択できるようになっています。

- USBフラッシュドライブのサポート
- サンプルファイル init-cfg.txt
- ファイアウォールのブート処理のためにUSBフラッシュドライブを準備
- USBフラッシュドライブを使用してファイアウォールのブート処理を行う

USBフラッシュドライブのサポート

ハードウェアベースのPalo Alto Networksファイアウォールのブート処理を行うUSBフラッシュドライブは、次のいずれかをサポートしている必要があります。

- File Allocation Table 32 (FAT32)
- Third Extended File System (ext3)

ファイアウォールは、USB2.0あるいはUSB3.0に接続できる次のフラッシュドライブによりブート処理を行うことができます。

サポートされている **USB** フラッシュドライブ
Kingston • Kingston SE9 8GB (2.0) • Kingston SE9 16GB (3.0) • Kingston SE9 32GB (3.0)
SanDisk • SanDisk Cruzer Fit CZ33 8GB (2.0) • SanDisk Cruzer Fit CZ33 16GB (2.0) • SanDisk Cruzer CZ36 16GB (2.0) • SanDisk Cruzer CZ36 32GB (2.0) • SanDisk Extreme CZ80 32GB (3.0)
Silicon Power • Silicon Power Jewel 32GB (3.0) • Silicon Power Blaze 16GB (3.0)
PNY

サポートされている USB フラッシュドライブ
• PNY Attache 16GB (2.0) • PNY Turbo 32GB (3.0)

サンプルファイル init-cfg.txt

ブート処理過程でinit-cfg.txtが必要になります。このファイルは、お客様がテキストエディタで作成する基本設定ファイルです。このファイルを作成するには、5 次のサンプル init-cfg.txt ファイル内のファイルでサポートされているパラメーターを参照します。指定する必要があるパラメーターは太字で示されています。

サンプル **init-cfg.txt**（静的 **IP** アドレス）	サンプル**init-cfg.txt**（**DHCP** クライアント）
type=static ip-address=10.5.107.19 default-gateway=10.5.107.1 netmask=255.255.25 address=2001:400:f00::1/64 ipv6-default-gateway=2001:400:f00::2 hostname=Ca-FW-DC1 panorama-server=10.5.107.20 panorama-server-2=10.5.107.21 tplname=FINANCE_TG4 dgname=finance_dg dns-primary=10.5.6.6 dns-secondary=10.5.6.7 op-command-modes=multi-vsys,jumbo-frame dhcp-send-hostname=no dhcp-send-client-id=no dhcp-accept-server-hostname=no dhcp-accept-server-domain=no	**type=dhcp-client** ip-address= default-gateway= netmask= ipv6-address= ipv6-default-gateway= hostname=Ca-FW-DC1 panorama-server=10.5.107.20 panorama-server-2=10.5.107.21 tplname=FINANCE_TG4 dgname=finance_dg dns-primary=10.5.6.6 dns-secondary=10.5.6.7 op-command-modes=multi-vsys,jumbo-frame dhcp-send-hostname=yes dhcp-send-client-id=yes dhcp-accept-server-hostname=yes dhcp-accept-server-domain=yes

init-cfg.txtファイルの各フィールドの内容は以下の表の通りです。typeは必須項目です。タイプが静的（static）の場合、IPアドレス、デフォルトゲートウェイおよびネットマスクの組み合わせ、あるいはIPv6アドレスおよびIPv6デフォルトゲートウェイの組み合わせが必須になります。

項目	の意味
type	（必須）管理IPアドレスのタイプ（staticあるいはdhcp-client）
IP アドレス	（IPv4静的管理アドレスの場合は必須）IPv4アドレス。typeがdhcp-clientの場合、ファイアウォールはこのフィールドを無視します。

項目	の意味
default-gateway	（IPv4静的管理アドレスの場合は必須）管理インターフェイス用のIPv4デフォルトゲートウェイ。typeがdhcp-clientの場合、ファイアウォールはこのフィールドを無視します。
ネットマスク	（IPv4静的管理アドレスの場合は必須）IPv4ネットマスク。typeがdhcp-clientの場合、ファイアウォールはこのフィールドを無視します。
ipv6-address	（IPv6静的管理アドレスの場合は必須）管理インターフェイスのプレフィックス長およびIPv6アドレス。typeがdhcp-clientの場合、ファイアウォールはこのフィールドを無視します。
ipv6-default-gateway	（IPv6静的管理アドレスの場合は必須）管理インターフェイス用のIPv6デフォルトゲートウェイ。typeがdhcp-clientの場合、ファイアウォールはこのフィールドを無視します。
hostname	（任意）ファイアウォールのホスト名。
panorama-server	（推奨）PanoramaプライマリサーバーのIPv4あるいはIPv6アドレス
panorama-server-2	（任意）PanoramaセカンダリサーバーのIPv4あるいはIPv6アドレス
tplname	（推奨）Panoramaテンプレート名。
dgname	（推奨）Panoramaデバイスグループ名。
dns-primary	（任意）DNSプライマリサーバーのIPv4あるいはIPv6アドレス
dns-secondary	（任意）DNSセカンダリサーバーのIPv4あるいはIPv6アドレス
vm-auth-key	（VMシリーズのファイアウォールのみ）マシン認証の認証キー。
op-command-modes	（任意）multi-vsysあるいはjumbo-frame、またはその両方を入力します（コンマ区切り）。ブート処理中に複数仮想システムおよびジャンボフレームを有効化します。
dhcp-send-hostname	（DHCPクライアント タイプのみ）値はDHCPサーバーによってyesあるいはnoに指定されます。yesの場合、ファイアウォールはそのホスト名をDHCPサーバーに送信します。

項目	の意味
dhcp-send-client-id	（DHCPクライアント タイプのみ）値はDHCPサーバーによってyesあるいはnoに指定されます。yesの場合、ファイアウォールはそのクライアントIDをDHCPサーバーに送信します。
dhcp-accept-server-hostname	（DHCPクライアント タイプのみ）値はDHCPサーバーによってyesあるいはnoに指定されます。yesの場合、ファイアウォールはそのホスト名をDHCPサーバーから受信します。
dhcp-accept-server-domain	（DHCPクライアント タイプのみ）値はDHCPサーバーによってyesあるいはnoに指定されます。yesの場合、ファイアウォールはそのDNSサーバーをDHCPサーバーから受信します。

ファイアウォールのブート処理のためにUSBフラッシュドライブを準備

USBフラッシュドライブを使用して物理的ファイアウォールのブート処理を行えます。ただし、これを行うには PAN-OS 7.1.0 以降のイメージを実行し、ファイアウォールの工場出荷時設定へのリセットを行う必要があります。セキュリティ上の理由から、ファイアウォールが工場出荷時のデフォルト設定になっている、あるいは個人的なデータがすべて削除されている状態の時しかブート処理を行えなくなっています。

STEP 1 | 注文完了メールに記載されている、サポート サブスクリプション用の認証コードおよびシリアル番号（S/N）を用意します。

STEP 2 | Customer Support [カスタマーサポート]ポータルで新しいファイアウォールのS/Nを登録します。

1. support.paloaltonetworks.com にアクセス、ログインし、**Assets**（アセット） > **Devices (デバイス)** > **Register New Device**（新規デバイスの登録） > **Register device using Serial Number or Authorization Code**（シリアル番号または認証コードを使用してデバイスを登録）を選択します。
2. ファイアウォールの登録に記載されている流れに従って作業を行います。
3. **Submit**（送信） をクリックします。

STEP 3 | Customer Support [カスタマーサポート]ポータルで認証コードのアクティベーションを行い、ライセンス キーを入手します。

1. support.paloaltonetworks.com にアクセスしてログインし、左側のナビゲーション ペインで**Assets (アセット)** > **Devices (デバイス)**を選択します。
2. 先ほど登録した各デバイス S/N について、**Action (アクション)**リンク（鉛筆のアイコン）をクリックします。
3. Activate Licenses (ライセンスのアクティベート) のところで**Activate Auth-Code (認証コードのアクティベート)**を選択します。
4. **Authorization code (認証コード)** を入力し、**Agree (同意する)**、**Submit (送信)** をクリックします。

STEP 4 | PanoramaにS/Nを追加します。

Panorama管理者ガイドのファイアウォールを管理デバイスとして追加のステップ1を完了させます。

STEP 5 | init-cfg.txtファイルの作成

ブート処理に使用するパラメーターを含む、必須のinit-cfg.txtファイルを作成します。各フィールドの説明はサンプルファイル init-cfg.txt にあります。

*init-cfg.txt*ファイルが無い場合、ブート処理に失敗し、ファイアウォールは通常のブート処理シーケンスに従ってデフォルト設定の状態で起動します。

各フィールドのキーおよび値の間にはスペースを含めません。管理サーバー側でパースを行う際にエラーが発生するため、スペースを入力しないようにしてください。

init-cfg.txtファイルを複数（各リモートサイト用に1ファイルずつ）使用する場合は、ファイル名の頭にシリアル番号を入力します。以下に例を示します。

0008C200105-init-cfg.txt

0008C200107-init-cfg.txt

シリアル番号が入力されたファイルが無い場合、ファイアウォールはinit-cfg.txtファイルを使用してブート処理を進めます。

STEP 6 | （任意）bootstrap.xmlファイルを作成します。

実運用中の既存のファイアウォールからエクスポートできる任意のbootstrap.xmlファイルには、完全なファイアウォール設定が含まれています。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)** > **Export named configuration snapshot (名前を付けて保存した設定スナップショットのエクスポート)**を選択します。
2. 保存済みの、あるいは現在アクティブな設定の**Name**[名前]を選択します。
3. **OK** をクリックします。
4. ファイル名を**`bootstrap.xml`**に変更します。

STEP 7 | カスタマーサポート ポータルでブート処理バンドルを作成・ダウンロード

物理的ファイアウォールの場合、ブート処理バンドルには/licenseおよび/configディレクトリのみが必要になります。

次のいずれかの方法でブート処理バンドルを作成・ダウンロードします。

- 方法 **1** を使用して各リモートサイト固有のブート処理バンドルを作成します（init-cfg.txt ファイルは一つだけです）。
- 方法 **2** を使用して複数サイト用のブート処理バンドルを一つ作成します。

方法**1**

1. ローカルシステムからsupport.paloaltonetworks.comにアクセスし、ログインします。
2. **Assets**[アセット]を選択します。
3. ブート処理を行うファイアウォールのS/Nを選択します。
4. **Bootstrap Container**[ブート処理コンテナ]を選択します。
5. **Select**[選択]をクリックします。
6. 作成したinit-cfg.txt ファイルをアップロードし、**Open (**開く**)** を実行します。
7. （任意）作成した bootstrap.xml ファイルを選択し、**Upload Files (**ファイルのアップロード**)** を行います。

   *bootstrap.xml*ファイルは、同一のモデルおよび*PAN-OS*バージョンのファイアウォールで使用する必要があります。
8. **Bootstrap Container Download**[ブート処理コンテナ ダウンロード]を選択し、**bootstrap_<S/N>_<**日付**>.tar.gz**という名前のtar.gzファイルをローカルシステムにダウンロードします。このブート処理コンテナには、そのファイアウォールに紐付けられているライセンス キーが含まれています。

方法**2**

トップレベルに2つのディレクトリがあるtar.gzファイルをローカルシステムに作成しますファイル名の頭にシリアル番号が付いたすべてのinit-cfg.txt ファイルとすべてのライセンスをインクルードします。

Customer Support [カスタマーサポート]ポータルからダウンロードしたライセンスキー ファイルの名前にはシリアル番号が含まれています。PAN-OSは、ブート処理中にそのファイル名のシリアル番号とファイアウォールのシリアル番号とを比較してチェックを行います。

STEP 8 | Secure Copy (SCP) あるいは TFTP を使用して、作成した tar.gz ファイルを (PAN-OS 7.1.0 以降のイメージを実行しているファイアウォールに) インポートします。

CLI にアクセスし、以下のいずれかのコマンドを入力します。

- **tftp import bootstrap-bundle file <path and filename>** から **<host IP address>**

  以下に例を示します。

  tftp import bootstrap-bundle file /home/userx/bootstrap/devices/pa5000.tar.gz from 10.1.2.3

- **scp import bootstrap-bundle from from <<user>@<host>：<path to file>>>**

  以下に例を示します。

  scp import bootstrap-bundle from userx@10.1.2.3:/home/userx/bootstrap/devices/pa200_bootstrap_bundle.tar.gz

STEP 9 | USBフラッシュドライブを準備します。

1. 前のステップで使用したファイアウォールに USB フラッシュドライブを挿入します。
2. 「**pa5000.tar.gz**」の部分をtar.gzファイルのファイル名に置き換えた上で、次のCLI操作コマンドを入力します。このコマンドにより、USBフラッシュドライブが初期化され、ファイルが回答され、さらにUSBフラッシュドライブの検証が行われます。

   request system bootstrap-usb prepare from pa5000.tar.gz
3. **y**を押して続行します。USBドライブの準備が完了すると、次のメッセージが表示されます。

   ```
   USB prepare completed successfully.
   ```
4. ファイアウォールからUSBフラッシュドライブを取り外します。
5. USBフラッシュドライブは必要な数だけ準備しておくことができます。

STEP 10 | USBフラッシュドライブをリモートサイトに配布します。

ブート処理バンドルを作成する際に 方法 2 を使用した場合、同じ USB フラッシュドライブのコンテンツを使用して複数のリモートサイトにあるファイアウォールのブート処理を行えます。このコンテンツは複数のUSBフラッシュドライブに入れたり、単体のUSBフラッシュドライブに入れて複数回使用したりすることができます。

USBフラッシュドライブを使用してファイアウォールのブート処理を行う

Palo Alto Networksのファイアウォール、およびブート処理ファイルが入ったUSBフラッシュドライブを入手すれば、ファイアウォールのブート処理を行うことができます。

*USB*フラッシュドライブは*ext4*ファイルシステムを使用してフォーマットされているため、*Microsoft*の*Windows*や*Apple*の*Mac OS*ではブート処理用*USB*フラッシュドライブを読み込むことができません。そのため、サードパーティ製のソフトウェアをインストールするか、*Linux*システムで*USB*ドライブを読み込む必要があります。

STEP 1 | ファイアウォールは工場出荷時のデフォルト状態、あるいは個人的なデータがすべて削除されている状態でなければなりません。

STEP 2 | お客様の組織の各拠点が確実に接続されるよう、イーサネットケーブルでファイアウォールの管理インターフェイス（MGT）を次のいずれかに接続します。

- 上流のモデム
- ルーターあるいはスイッチ機構のポート
- 壁面のイーサネット ジャック

STEP 3 | ファイアウォールのUSBポートにUSBフラッシュドライブを差し込み、ファイアウォールの電源を入れます。工場出荷時の状態のファイアウォールがUSBフラッシュドライブを使用してブート処理を開始します。

ファイアウォールの構成が完了すると、そのステータス ライトが黄色から緑に変わります。これで自動コミットが正しく完了しました。

STEP 4 | ブート処理の結果を検証します。ブートストラップ中、コンソールに基本ステータス ログが表示され、プロセスが完了したことを確認できるようになっています。

1. Panorama変数（panorama-server、tplname、and dgname）をinit-cfg.txtファイルに含めている場合、Panoramaが管理するデバイス、デバイスグループ、テンプレート名をチェックしてください。
2. Web インターフェイスにアクセスし、**Dashboard (ダッシュボード)** > **Widgets** > **System (システム)** を選択するか、CLI 操作コマンド **`show system info`** および **`show config running`** を使用し、システムの基本設定や構成を検証します。
3. **Device (デバイス)** > **Licenses (ライセンス)** を選択するか、CLI 操作コマンド **`request license info`** を使用してライセンスのインストール状況を確認します。
4. Panoramaの構成が終了していれば、Panoramaでコンテンツバージョンおよびソフトウェアバージョンを管理します。Panoramaの構成が終了していなければ、Webインターフェイスを使用してコンテンツバージョンおよびソフトウェアバージョンを管理します。

STEP 5 | (Panorama managed firewalls only)デバイス登録認証キーを作成し、firewallに追加します。

これは、ブートストラップを使って起動したファイアウォールをパノラマ管理に正常に追加するために必要です。デバイス登録認証キーの有効期間は有限であり、init-cfg.txt ファイルにデバイス登録認証キーを含めることはサポートされていません。

1. Panorama Web インターフェースにログインします。
2. **Panorama** > **Device Registration Auth Key** を選択し、 **Add** で新しい認証キーを追加します。
3. 認証キーを構成します。
   - **Name** –認証キーのわかりやすい名前を追加します。
   - **Lifetime**:キーの有効期間を指定して、認証キーを使用して新しいファイアウォールをオンボードできる期間を制限します。
   - **Count**–認証キーを使用して新しいファイアウォールをオンボードできる回数を指定します。
   - **Device Type** –この認証キーが つのファイアウォール のみを認証するために使用されることを指定します。

     デバイス登録認証キーをオンボードファイアウォール、ログコレクタ、および *WildFire* アプライアンスに使用するには、*[* 任意 *]*を選択できます。
   - (Optional) デバイス–認証キーが有効なファイアウォールを指定する 1 つ以上のデバイスシリアル番号を入力します。
4. **OK** をクリックします。
   プロンプトが表示されたら、[認証キーをコピー して 閉じる]をクリックします。
5. ファイアウォール Web インターフェイス にログインします。

   また、firewall CLI にログインして、デバイス登録認証キーを追加することもできます。

   ```
   admin> 認証キー セットの要求<auth key>
   ```
6. **[Device]** > **[セットアップ]** > **[管理]** の順に選択し、[Panorama 設定] を編集します。
7. 前の手順でコピーしたデバイス登録認証キーを貼り付け、**OK** をクリックします。
8. **[コミット]** します。
9. パノラマ Web インターフェイスにログインし、[パノラマ > 管理対象デバイスの > 概要] を選択して、ファイアウォールがパノラマに 接続 されていることを確認します。

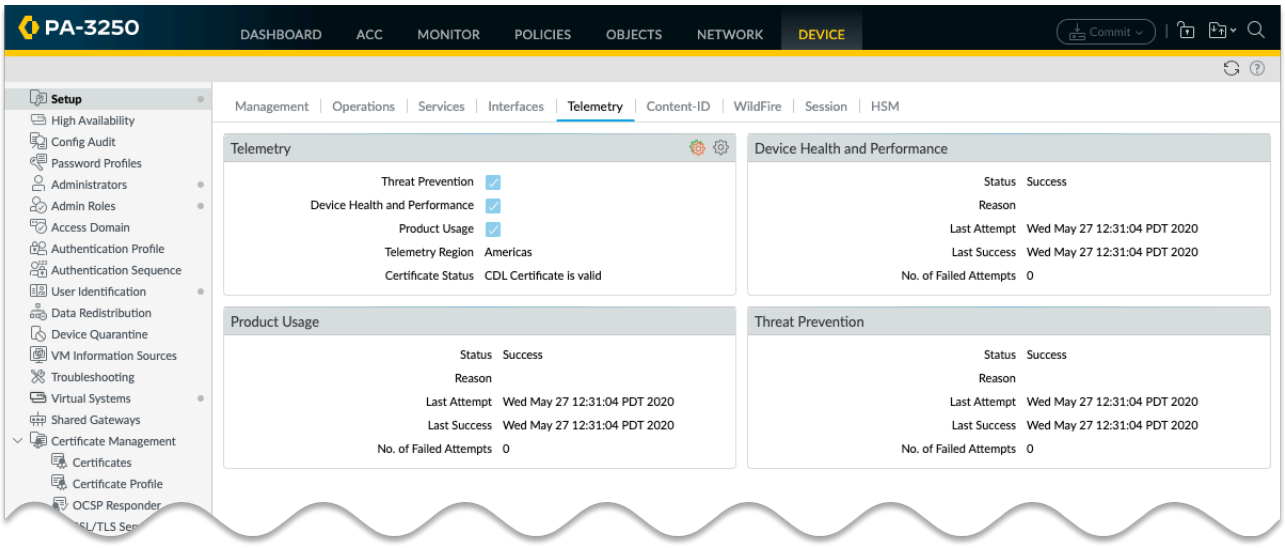
デバイスのテレメトリ

デバイスのテレメトリは、ご利用の次世代ファイアウォールまたは Panorama に関する情報を収集し、データを Cortex Data Lake にアップロードすることでその情報を Palo Alto Networks と共有します。このデータは、テレメトリ アプリケーションへの電力供給、および脅威インテリジェンスの共有に使用されます。

デバイスのテレメトリ概要

デバイスのテレメトリは、ご利用の次世代ファイアウォールまたは Panorama に関する情報を収集し、データを Cortex Data Lake にアップロードすることでその情報を Palo Alto Networks と共有します。このデータは、次世代ファイアウォールおよび Panorama の監視と管理を容易にするクラウドベースのアプリケーションであるテレメトリ アプリで利用されます。これらのアプリは、デバイスの状態、パフォーマンス、容量計画、および設定に対する可視性を向上させます。これらのアプリを通じて、Palo Alto Networks が提供する製品やサービスを最大限に活用することができます。

テレメトリ データは、脅威インテリジェンスの共有にも使用され、侵入防御の強化、脅威シグネチャの評価、PAN-DB URL フィルタリング、DNS ベースのコマンド アンド コントロール (C2) シグネチャ、および WildFire 内でのマルウェア検出の改善を提供します。



テレメトリデータは収集され、期間限定でデバイスにローカルに保存されます。このデータは、データの宛先リージョンを設定した場合にのみ Palo Alto Networks と共有されます。組織に Cortex Data Lake ライセンスがある場合は、Cortex Data Lake インスタンスが存在するのと同じリージョンにのみデータを送信できます。組織に Cortex Data Lake ライセンスがない場合、このデータを共有するには、デバイス証明書をインストールする必要があります。この場合、利用可能な任意のリージョンを選択できますが、プライバシーとデータ ストレージに関して適用されるすべての地域の法律に準拠する必要があります。

テレメトリ データが収集され、事前定義済みの収集間隔で Palo Alto Networks と共有されます。データのカテゴリを有効/無効にすることで、データを収集および共有するかどうかを制御できます。データの収集と送信の現在のステータスを監視することもできます。

最後に、ファイアウォールがテレメトリの目的で収集しているデータのライブ サンプルを取得できます。各メトリックのプライバシーへの影響など、Palo Alto Networks と共有できるすべてのテレメトリ メトリックの完全な説明については、PAN-OS デバイスのテレメトリ メトリック リファレンスガイドを参照してください。

テレメトリが有効になっている間、自動的に作成されたユーザー ***_cliadmin*** がダッシュボードの ***Logged in Admins*** の下に表示されることがあります。このユーザーは、テレメトリ コレクション専用に作成されます。

デバイスのテレメトリ収集および送信間隔

PAN-OS は、固定間隔でテレメトリのデータを収集し、送信します。収集はメトリック基準で定義され、以下の内の1つを設定できます。

- 20分ごと。
- 毎時間。
- 日毎。

テレメトリはデータ バンドルに収集されます。各バンドルは、データ送信の時点までに収集されたすべてのデータの集約です。これらのバンドルは、1 時間に 1 回発生する送信イベントまでデバイスに保存されます。バンドルが正常に Palo Alto Networks に送信されると、バンドルはデバイスから削除されます。

バンドルの Palo Alto Networks への送信時にエラーが発生すると、ファイアウォールは 10 分間待機してから送信を再試行します。ファイアウォールは、成功するか、新しいテレメトリ データを収集するためのストレージ スペースが必要になるまで、バンドルの送信を試行し続けます。

ファイアウォールは、定期的な送信間隔ごとに、そのイベントにスケジュールされたバンドルを送信することから始動します。これらのバンドルの転送が成功すると、ファイアウォールは、以前の送信イベントから保存した可能性のある失敗したバンドルを送信します。

デバイスのテレメトリの管理

デバイスのテレメトリを管理するために、以下の操作が可能です：

- デバイスのテレメトリを有効化する
- デバイスのテレメトリを無効化する
- デバイスのテレメトリが収集するデータを管理する
- デバイスのテレメトリ履歴を管理する

デバイスのテレメトリを有効化する

デフォルトでは、お使いのデバイスは Palo Alto Networks とデータを共有しません。共有が有効である場合、以下の方法ですべてのデバイスのテレメトリの共有を停止できます:**Device** > **Setup** > **Telemetry** (デバイスのセットアップのテレメトリ) で、**Enable Telemetry (**テレメトリを有効にする**)** チェックボックスをオフにしてから、変更内容をコミットします。

データが Palo Alto Networks と共有されるようにデバイスのテレメトリを有効にする方法は次の通りです:

STEP 1 | Cortex Data Lake を有効にします。

1. 組織に Cortex Data Lake ライセンスがなく、お使いのデバイスにデバイス証明書がインストールされていない場合は、デバイス証明書をインストールしてください。

   組織が Cortex Data Lake ライセンスを保有している場合は、ライセンスがアクティベート済みであることを確認してください。
2. ご利用のネットワークで、ファイアウォールがデータを Cortex Data Lake に送信できるように適切に設定されていることを確認してください。

STEP 2 | **Device (**デバイス**)** > **Setup (**セットアップ**)** > **Telemetry (**テレメトリ**)** の順に移動します。

STEP 3 | **Telemetry (**テレメトリ**)** ウィジェットを編集します。

STEP 4 | **Telemetry Destination (**テレメトリの宛先**)** で、リージョンを選択してください。ご所属の組織で Cortex Data Lake を使用している場合は、Cortex Data Lakeが使用するように設定されているリージョンを使用する必要があります。

STEP 5 | **OK** をクリックし、変更をコミットします。

デバイスのテレメトリを無効化する

次世代ファイアウォールが Palo Alto Networks とデータを共有するように設定されている場合は、次のようにしてこの共有を無効にすることができます：

STEP 1 | **Device (**デバイス**)** > **Setup (**セットアップ**)** > **Telemetry (**テレメトリ**)** の順に移動します。

STEP 2 | **Telemetry (**テレメトリ**)** ウィジェットを編集します。

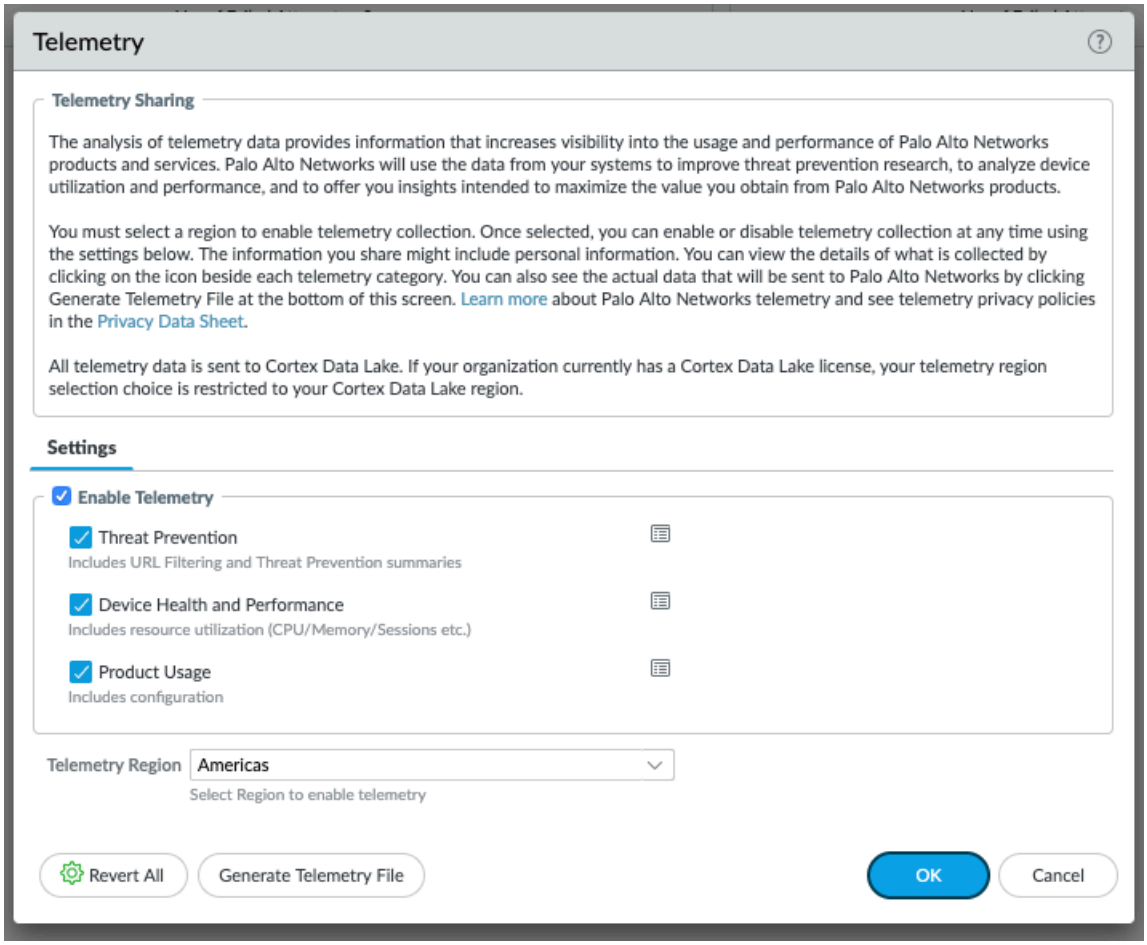
STEP 3 | **Enable Telemetry (**テレメトリを有効にする**)** チェックボックスをオフにします。

STEP 4 | **OK** をクリックし、変更をコミットします。

STEP 5 | 現在 Cortex Data Lake に保存されているテレメトリ データは、ファイアウォールがアップロードしてから1年後に自動的に削除されます。オプションとして、テレメトリの無効化後にこの期間のデータを Cortex Data Lake に残存させたくない場合は、サポート チケットを開示して Palo Alto Networks にテレメトリ データの消去を依頼してください。

デバイスのテレメトリを収集するデータを管理する

Device (デバイス) > **Setup (セットアップ)** > **Telemetry (テレメトリ)** を選択し、現在収集されたテレメトリのカテゴリを確認します。これらのカテゴリを変更するには、テレメトリ ウィジェットを編集します。ファイアウォールで収集しないカテゴリを選択解除し、**OK** をクリックしてから、変更内容をコミットします。



すべてのデバイスのテレメトリの共有を停止するには、***Enable Telemetry*** **(**テレメトリを有効にする**)** チェックボックスをオフにしてから、変更内容をコミットします。

履歴デバイステレメトリを管理する

Device Telemetry は PAN-OS 10.2 リリースで大幅に変更されました。10.0以前は、テレメトリのデータは脅威インテリジェンスの目的で主に利用ししていました。10.0の時点でも、脅威イン

テリジェンス メトリックは、デバイスによって収集されるデータの大部分を占めていますが、デバイスの状態、パフォーマンス、および設定に関連するデータも大量に収集されます。

つまり、PAN-OS 10.2 デバイス テレメトリは、以前のリリースで収集されたデータを拡張します。また、PAN-OS 10.2 は、テレメトリ データを以前のリリースとは異なるクラウドの場所に送信します。ただし、PAN-OS 10.0 を実行している次世代ファイアウォールには、これまでのテレメトリ サポートが引き続き存在します。唯一の違いは、10.2 デバイス テレメトリのユーザーインターフェイスでは、この履歴データ収集を管理できないことです。

既存の次世代 firewall があり、いずれかの履歴テレメトリ データ カテゴリが有効になっている場合、PAN-OS 10.2 にアップグレードしても、firewall はこの情報を収集して共有し続けます。このテレメトリ データ共有をオフにする場合は、次の CLI コマンドを使用します:

```
set deviceconfig system update-schedule statistics-service
 application-reports no set deviceconfig system update-schedule
 statistics-service threat-prevention-reports no set deviceconfig
 system update-schedule statistics-service threat-prevention-
information no set deviceconfig system update-schedule statistics-
service threat-prevention-pcap no set deviceconfig system
 update-schedule statistics-service passive-dns-monitoring no set
 deviceconfig system update-schedule statistics-service url-reports
 no set deviceconfig system update-schedule statistics-service
 health-performance-reports no set deviceconfig system update-
schedule statistics-service file-identification-reports no
```

10.2 firewallを使用していて、このテレメトリ共有がオフになっているが、このデータをPalo Alto Networksと共有したい場合は、次のようにして有効にすることができます。

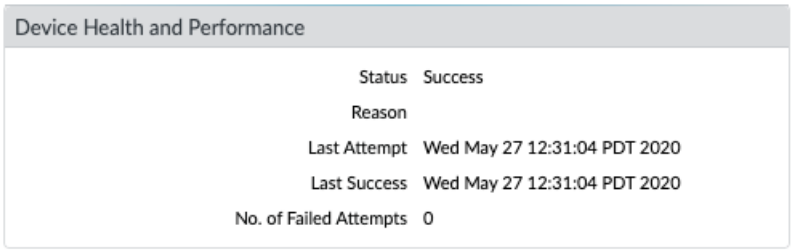
```
set deviceconfig system update-schedule statistics-service
 application-reports yes set deviceconfig system update-schedule
 statistics-service threat-prevention-reports yes set deviceconfig
 system update-schedule statistics-service threat-prevention-
information yes set deviceconfig system update-schedule statistics-
service threat-prevention-pcap yes set deviceconfig system
 update-schedule statistics-service passive-dns-monitoring yes set
 deviceconfig system update-schedule statistics-service url-reports
 yes set deviceconfig system update-schedule statistics-service
 health-performance-reports yes set deviceconfig system update-
schedule statistics-service file-identification-reports yes
```

次の CLI コマンドを使用して、デバイスがこの履歴テレメトリ データを収集および共有しているかどうかを確認できます:

```
show deviceconfig system update-schedule statistics-service
```

デバイスのテレメトリを監視する

PAN-OS には、各テレメトリのカテゴリの共有ステータスが表示されます。各メトリクス カテゴリのウィジェットは、**Device (デバイス)** > **Setup (セットアップ)** > **Telemetry (テレメトリ)** で使用可能です。

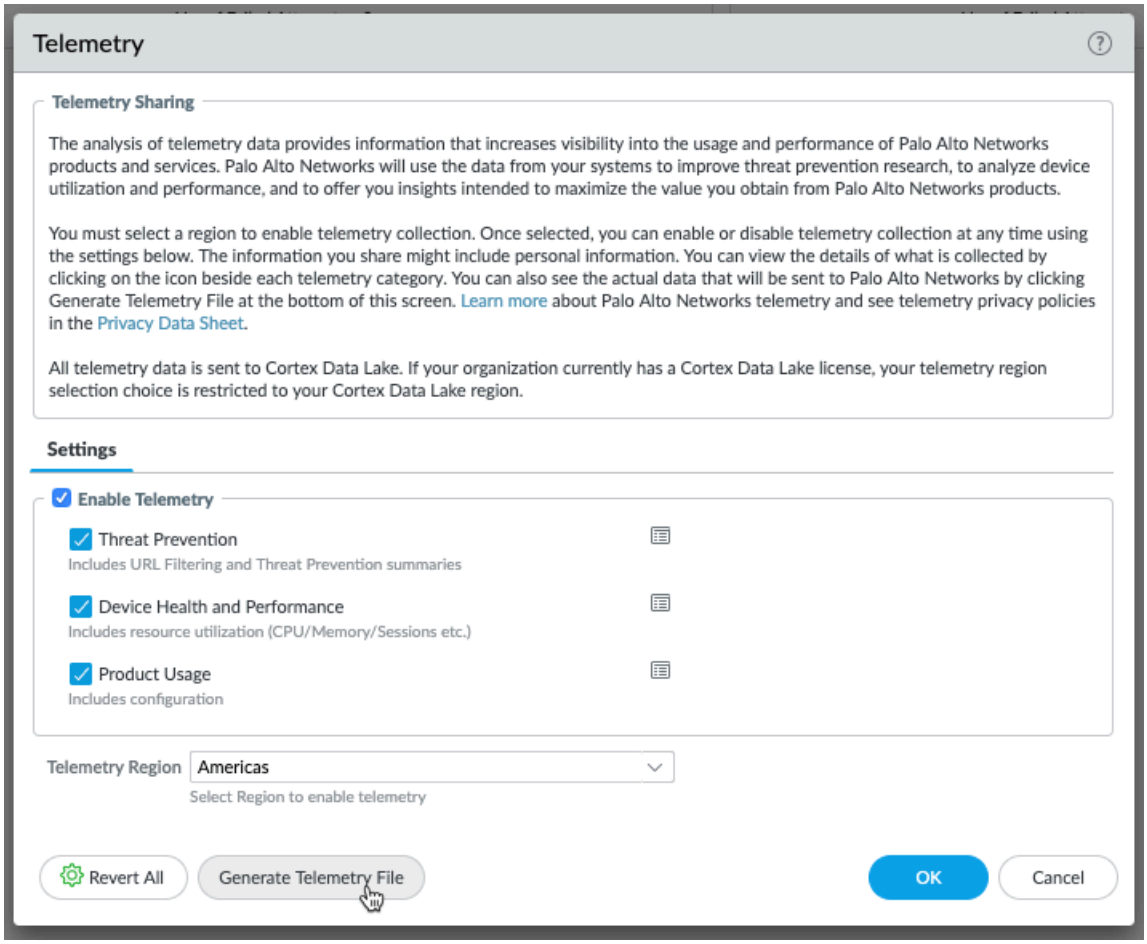


障害が発生した場合、デバイスは次の送信時に送信の試行を再試行します。問題が解決しない場合は、デバイスが Cortex Data Lake にデータを送信するように適切に設定されていることを確認してください:

- 組織が Cortex Data Lake ライセンスを保有している場合は、Cortex Data Lake ライセンスがアクティベート済みであることと、ご利用のファイアウォールが Cortex Data Lake で使用するように設定されていることを確認してください。
- ご所属の組織が Cortex Data Lake ライセンスを保有していない場合は、デバイス証明書をインストール済みであり、ご利用のネットワークが Cortex Data Lake へのトラフィックを許可するように設定されていることを確認してください。

デバイスのテレメトリを収集するデータのサンプルを取る

デバイス テレメトリが収集して Palo Alto Networks と共有するデータのライブ サンプルをダウンロードできます。これを行うには、**Device (デバイス)** > **Setup (セットアップ)** > **Telemetry (テレメトリ)** に移動し、**Telemetry (テレメトリ)** ウィジェットを編集します。次に、**Generate Telemetry File (テレメトリ ファイルの生成)** をクリックします。



データ収集は、ファイアウォールの速度に依存しますが、数分で完了します。プロセスが完了したら、**Download Device Telemetry Data (デバイスのテレメトリ データをダウンロード)** をクリックします。テレメトリ バンドルは圧縮された tar ボールであり、デフォルトのブラウザ ダウンロード ディレクトリに配置されます。

デバイスのテレメトリが収集し、Palo Alto Networks と共有するすべてのメトリックの説明は、PAN-OS デバイスのテレメトリ メトリック参照ガイドでご覧いただけます。

認証

認証は、正当なユーザーだけがアクセスできるようにユーザーの ID を確認することによって、サービスとアプリケーションを保護する方法です。いくつかのファイアウォール機能と Panorama 機能には認証が必要です。管理者は、ファイアウォールの Web インターフェイス、CLI、または XML API、および Panorama にアクセスするための認証を行います。エンドユーザーは、認証ポータルまたは GlobalProtect を介して認証を受け、さまざまなサービスやアプリケーションにアクセスします。スムーズなユーザーエクスペリエンスを確実なものにしつつ、ネットワークを保護し、既存のセキュリティ インフラストラクチャに対応するために、複数の認証サービスから選択できます。

パブリック キーのインフラストラクチャを使用している場合は、証明書をデプロイして、ユーザーがログインの問題に手動で対応することなく認証を有効にすることができます（「 証明書管理 」を参照）。あるいは、証明書に加えて、インタラクティブな認証を実装することもできます。その場合は、ユーザーが 1 つ以上のメソッドを使用して認証する必要があります。次のトピックでは、さまざまなタイプのインタラクティブ認証を実装、テスト、およびトラブルシューティングする方法について説明します。

認証タイプ

- 外部認証サービス
- 多要素認証
- SAML
- Kerberos
- TACACS+
- RADIUS
- LDAP
- ローカル認証

外部認証サービス

ファイアウォールおよび Panorama は外部サーバーを使用して、管理者による Webインターフェースへのアクセス、および 認証ポータルとGlobalProtect を通じてエンドユーザーが行うサービスあるいはアプリケーションへのアクセスを制御できます。この文脈においては、サービスがネットワークの内部にある（Kerberos など）か外部にある（SAML アイデンティティ プロバイダなど）かに関わらず、ファイアウォールあるいは Panorama のローカルにない認証サービスはすべて外部にあるとみなされます。ファイアウォールおよび Panorama が統合できるサーバーのタイプには、マルチ ファクター認証（MFA）、SAML、Kerberos、TACACS+、RADIUS、および LDAP などがあります。ファイアウォールおよび Panorama がサポートしているローカル認証サービスを使用することもできますが、通常は次の機能を提供する外部サービスの方が好まれます。

- 単一の外部 ID ストアですべてのユーザーアカウントを一元管理。サポートされているすべての外部サービスが、エンドユーザーおよび管理者に対してこのオプションを提供しています。
- アカウント認証の一元管理（ロールおよびアクセスドメインの割り当て）。SAML、TACACS+、および RADIUS が管理者に対してこのオプションをサポートしています。
- 一度限りの認証でユーザーが複数のサービスおよびアプリケーションにアクセスできるようになるシングル サインオン（SSO）。SAML および Kerberos が SSO をサポートしています。
- 極めて重要なサービスおよびアプリケーションを保護する、異なるタイプ（要素）から成る複数の認証チャレンジ。MFA サービスがこのオプションをサポートしています。

外部サービスを通す認証では、ファイアウォールがそのサービスに接続する方法を定義するサーバープロファイルが必要になります。このサーバープロファイルは、各アプリケーションおよび一連のユーザーに合わせてカスタマイズする設定を定義する認証プロファイルに割り当てます。例えば、Web インターフェイスにアクセスする管理者用の認証プロファイルを設定し、GlobalProtect ポータルにアクセスするエンドユーザー用に別のプロファイルを設定することができます。詳細については認証プロファイルおよびシーケンスの設定を参照してください。

多要素認証

マルチ ファクター認証の設定（MFA）を行い、極めて重要なサービスおよびアプリケーションにアクセスする際に各ユーザーが必ず複数の方法（要素）を使って認証を行うようにします。例えば、ユーザーがログイン用パスワードを入力した後、重要な経理文書にアクセスできるようになる前に、電話で受信する確認コードの入力を求めることができます。このアプローチは、攻撃者がパスワードを盗むだけですべてのサービスおよびアプリケーションにアクセスできるようになってしまうような状況を防ぐ上で役立ちます。もちろん、あらゆるサービスおよびアプリケーションでこのレベルの保護が必要になるわけではなく、ユーザーが頻繁にアクセスするあまりセンシティブではないサービスおよびアプリケーションについては MFA が不要な場合もあります。様々なセキュリティ要件を満たすために、特定のサービス、アプリケーション、エンドユーザーに基づいて MFA あるいは単一の認証要素（ログイン認証情報や証明書など）をトリガーする認証ポリシールールの設定を行えます。

使用する認証要素の数と種類を選択する際、ポリシー評価がどのようにユーザーエクスペリエンスに影響を与えるのか知っておくことが重要です。ユーザーがサービスあるいはアプリケーションをリクエストする際、ファイアウォールはまず認証ポリシーを評価します。リクエストが MFA が有効な認証ポリシールールにマッチすると、ファイアウォールはユーザーが最初の要素に対して認証を行えるよう、認証ポータルの Web フォームを表示します。認証が成功すると、追加の各認証要素のためにファイアウォールが MFA ログインページを表示します。2～4 つの要素の中からユーザーに 1 つ選択するよう求める MFA サービスもあり、これは利用できない要素がある場合に便利です。すべての要素に対して認証が成功すると、ファイアウォールはリクエストされたサービスあるいはアプリケーション用のセキュリティポリシーを評価します。

ユーザーの作業を滞らせる認証チャレンジの頻度を減らすために、最初の要素で Kerberos あるいは SAML シングル サインオン（*SSO*）を使用するよう設定します。

GlobalProtect 用の *MFA* を実装する方法は、マルチ ファクター認証の通知を活用するための GlobalProtect の設定を参照してください。

認証シーケンスで *MFA* 認証プロファイルを使用することはできません。

認証ポリシー 経由でエンドユーザーを認証する場合、ファイアウォールは、他のすべてのMFAプラットフォームに対してRADIUSまたはSAMLを介して統合するだけでなく、いくつかのMFAプラットフォーム（Duo v2、Okta Adaptive、PingID、およびRSA SecurID）と直接統合します。GlobalProtect ポータルとゲートウェイへのリモート ユーザー認証、および Panorama および PAN-OS Web インターフェイスへの管理者認証のために、ファイアウォールは RADIUS と SAML のみを使用して MFA ベンダーと統合します。

ファイアウォールでは、以下の MFA 要素がサポートされています。

要素	説明
プッシュ	エンドポイント デバイス（電話やタブレットなど）がユーザーに認証を許可あるいは拒否するよう求めます。

要素	説明
ショート メッセージ サービス（SMS）	エンドポイント デバイスの SMS メッセージが、ユーザーに認証を許可あるいは拒否するよう求めます。エンドポイント デバイスが、MFA ログインページに入力しなければならないコードを使うケースもあります。
音声	自動音声の電話により、電話のボタンを押す、あるいは MFA ログインページにコードを入力することでユーザーに認証を求めます。
ワンタイム パスワード（OTP）	エンドポイント デバイスが自動生成された英数字の文字列を提供し、ユーザーがそれを MFA ログインページに入力し、単一のトランザクションあるいはセッションを有効化します。

SAML

Security Assertion Markup Language（SAML） 2.0 を使用し、ファイアウォールあるいは Panorama Web インターフェイスにアクセスする管理者や、組織の内外にある Web アプリケーションにアクセスするエンドユーザーを認証することができます。各ユーザーが多くのアプリケーションにアクセスし、一つ一つに認証することがユーザーの生産性を損なわせるような環境では、SAML シングル サインオン（SSO）を設定し、一度のログインで複数のアプリケーションにアクセスできるようにします。同様に、SAML シングル ログアウト（SLO）により、ユーザーが一つのセッションからログアウトするだけで複数のアプリケーションのセッションを終了できるようにすることが可能です。SSO は、Webインターフェースにアクセスする管理者や、GlobalProtect あるいは認証ポータルを通してアプリケーションにアクセスするエンドユーザーが利用できます。SLO は、管理者、GlobalProtect のエンドユーザーが利用できますが、認証ポータルのエンドユーザーは利用できません。ファイアウォール上あるいは Panorama 上で SAML 認証を設定する際、管理者認証用の SAML 属性を指定できます。SAML 属性を使用すれば、ディレクトリ サービスを通じて管理者のロール、アクセスドメイン、ユーザーグループを素早く変更でき、これはファイアウォールあるいは Panorama で再度設定を行うよりも簡単です。

管理者は *SAML* を使用してファイアウォールや *Panorama* の *CLI* に認証することができません。

認証シーケンスで *SAML* 認証プロファイルを使用することはできません。

SAML 認証では、アプリケーションへのアクセスを制御するサービスプロバイダ（ファイアウォールあるいは Panorama）、およびユーザーを認証する PingFederate などのアイデンティティ プロバイダ（IdP）が必要になります。ユーザーがサービスあるいはアプリケーションをリクエストする際、ファイアウォールあるいは Panoramaはリクエストをインターセプトし、認証を行うためにユーザーを IdP にリダイレクトします。次に IdP がユーザーを認証し、認証の成功あるいは失敗を示す *SAML* アサーションを返します。認証ポータル エンドユーザーの SAML 認証は、認証ポータルを通してアプリケーションにアクセスするエンドユーザー用の SAML 認証について説明しています。

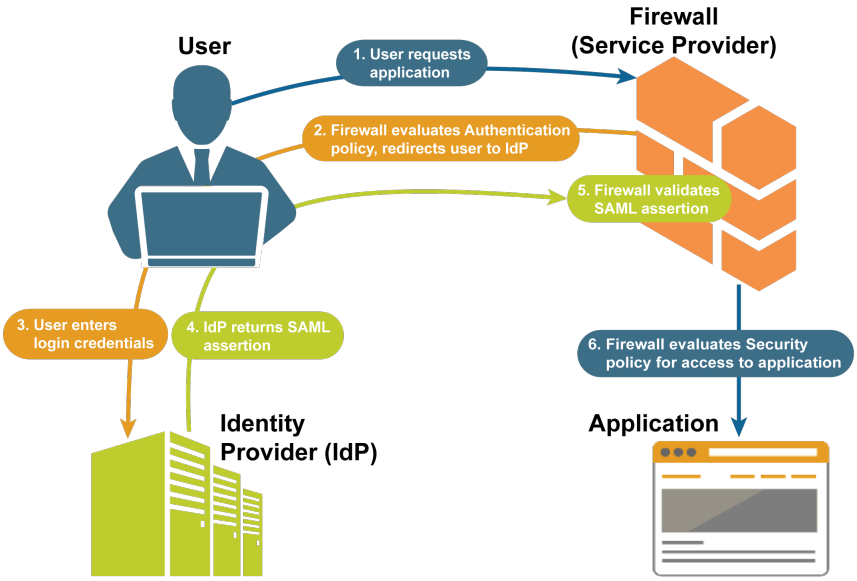


図 **1 :** 認証ポータル エンドユーザーの **SAML** 認証

Kerberos

Kerberos は、一意のキー（チケットと呼ばれる）を使用してお互いを特定し合うことで、安全でないネットワークをまたがって安全に情報を交換できるようにする認証プロトコルです。ファイアウォールおよび Panorama は、管理者およびエンドユーザーを認証する 2 種類の Kerberos 認証をサポートしています。

- **Kerberos** サーバー認証—Kerberos サーバー プロファイルを使用すると、ネイティブでユーザーが Active Directory ドメイン コントローラまたは Kerberos V5 準拠の認証サーバーの認証を受けることができます。この認証方法はインタラクティブであり、ユーザーにユーザー名およびパスワードを入力するよう求めます。設定の流れについては、Kerberos サーバー認証の設定を参照してください。
- **Kerberos** シングル サインオン（**SSO**）—Kerberos SSO をサポートするネットワークでは、ネットワークへの初回のアクセス時（Microsoft Windows へのログイン時など）にのみユーザーにログインを求めるプロンプトが表示されます。ユーザーは初回のログイン後、SSO セッションの期限が切れるまで再度ログインすることなく、ネットワークのブラウザ ベースのどのサービスにも（ファイアウォールの Web インターフェイスなど）アクセスできます。（SSO セッションの期間は Kerberos 管理者が設定します）。 Kerberos SSO ともう一つの外部認証サービス（TACACS サーバーなど）の両方を有効にした場合、ファイアウォールは最初に SSO を試行し、失敗した場合にのみ外部サービスにフォールバックして認証を行います。Kerberos SSO をサポートするためにはネットワークに以下が必要です。
  - Kerberos インフラストラクチャ（認証サーバー（AS）およびチケット保証サービス（TGS）を備えたキー配布センター（KDC）など）
  - ユーザーを認証するファイアウォールあるいはPanoramaごとの Kerberos アカウント。Kerberos キータブを作成するためにアカウントが必要です。キータブとは、ファイア

ウォールあるいはPanoramaのプリンシパル名およびハッシュされたパスワードを含むファイルです。SSO プロセスにはキータブが必要です。

設定の流れについては、Kerberos シングル サインオンの設定を参照してください。

Kerberos SSO は、*Kerberos* 環境の内部にあるサービスおよびアプリケーションに対してのみ利用できます。外部のサービスおよびアプリケーションに対して *SSO* を有効化する場合、SAML を使用します。

TACACS+

Terminal Access Controller Access-Control System Plus（TACACS+）は、中央のサーバーを通して一元的に本人確認および認証を行えるようにするプロトコルの一種です。TACACS+ はユーザー名およびパスワードを暗号化するため、パスワードのみを暗号化する RADIUS よりも安全です。また、UDP を使用する RADIUS と異なり、TACACS+ は TCP を使用するためより安定しています。エンドユーザーや管理者用の認証についてはファイアウォール上で、管理者用の認証については Panorama 上で TACACS+ 認証を設定できます。任意で、TACACS+ ベンダー固有属性（VSA）を使用して管理者の認証を管理できます。TACACS+ VSA を使用すれば、ファイアウォールおよび Panorama で再度設定を行うことなく、ディレクトリ サービスを通じて管理者のロール、アクセスドメイン、ユーザーグループを素早く変更できます。

ファイアウォールおよび Panorama は次の TACACS+ 属性および VSA をサポートしています。これらの VSA を TACACS+ サーバー上で定義するための各ステップについては、TACACS+ サーバーのドキュメントを参照してください。

名前	Value（値）
service	Palo Alto Networks 固有の VSA を識別するために必要な属性です。値を **PaloAlto** に設定する必要があります。
protocol	Palo Alto Networks デバイス固有の VSA を識別するために必要な属性です。値を **firewall** に設定する必要があります。
PaloAlto-Admin-Role	ファイアウォールのデフォルト（ダイナミック）管理ロール名またはカスタム管理ロール名
PaloAlto-Admin-Access-Domain	ファイアウォール管理者のアクセスドメインの名前（**Device (デバイス)** > **Access Domains (アクセス ドメイン)** ページで設定）。ファイアウォールに仮想システムが複数ある場合はこの VSA を定義します。
PaloAlto-Panorama-Admin-Role	Panorama のデフォルト（ダイナミック）管理ロール名またはカスタム管理ロール名

名前	Value（値）
PaloAlto-Panorama-Admin-Access-Domain	デバイス グループおよびテンプレート管理者のアクセスドメインの名前（**Panorama** > **Access Domains** (アクセス ドメイン) ページで設定）。
PaloAlto-User-Group	認証プロファイルの許可リストに含まれるユーザーグループの名前です。

RADIUS

Remote Authentication Dial-In User Service（RADIUS）は、広くサポートされているネットワークプロトコルであり、一元的な本人確認および認証を提供します。エンドユーザーや管理者用の認証についてはファイアウォール上で、管理者用の認証については Panorama 上で RADIUS 認証を設定できます。任意で、RADIUS ベンダー固有属性（VSA）を使用して管理者の認証を管理できます。RADIUS VSA を使用すれば、ファイアウォールおよび Panorama で再度設定を行うことなく、ディレクトリ サービスを通じて管理者のロール、アクセスドメイン、ユーザーグループを素早く変更できます。また、次の目的でファイアウォールが RADIUS サーバーを使用するように設定することもできます。

- GlobalProtect エンドポイントから VSA を収集します。
- マルチ ファクター認証を実装する。

認証リクエストを RADIUS サーバーに送信する際、その認証プロセスを開始したサービス（Web インターフェイスへの管理者アクセスなど）用の認証シーケンスに認証プロファイルが割り当てられている場合でも、ファイアウォールおよび Panorama はその認証プロファイルをネットワークアクセス サーバー（NAS ：network access server）の識別子として利用します。

ファイアウォールおよび Panorama は次の RADIUS VSA をサポートしています。RADIUS サーバーで VSA を定義するには、ベンダー コード（Palo Alto Networksのファイアウォールあるいは Panoramaは 25461）と、VSA 名および番号を指定する必要があります。一部の VSA は値が必要です。これらの VSA を定義するための各ステップについては、RADIUS サーバーのドキュメントを参照してください。

あるいは、Palo Alto Networks ファイアウォールと RADIUS サーバーが互いに通信するために使用する認証属性を定義し、それを RADIUS サーバーにインストールしてその属性を RADIUS バイナリデータにマッピングする、Palo Alto Networks RADIUS ディクショナリーをダウンロードすることもできます。

サーバー上のユーザーに対して動的管理者ロールを事前定義している場合は、小文字を使用してロールを指定します (例えば、***SuperUser*** ではなく、***superuser*** と入力します)。

Cisco Secure Access Control Server（*ACS*）上で詳細なベンダーオプションを設定する際、***Vendor Length Field Size*** (ベンダー長さフィールド サイズ) および ***Vendor Type Field Size*** (ベンダー タイプ フィールド サイズ) を両方とも ***1*** に設定する必要があります。定義していないと認証に失敗します。

名前	番号	値
管理者アカウント管理および認証用 VSA		
PaloAlto-Admin-Role	1	ファイアウォールのデフォルト（ダイナミック）管理ロール名またはカスタム管理ロール名
PaloAlto-Admin-Access-Domain	2	ファイアウォール管理者のアクセスドメインの名前（**Device (デバイス)** > **Access Domains (アクセス ドメイン)** ページで設定）。ファイアウォールに仮想システムが複数ある場合はこの VSA を定義します。
PaloAlto-Panorama-Admin-Role	3	Panorama のデフォルト（ダイナミック）管理ロール名またはカスタム管理ロール名
PaloAlto-Panorama-Admin-Access-Domain	4	デバイス グループおよびテンプレート管理者のアクセスドメインの名前（**Panorama** > **Access Domains (アクセス ドメイン)** ページで設定）。
PaloAlto-User-Group	5	認証プロファイルが参照するユーザー グループの名前
GlobalProtect エンドポイントから RADIUS サーバーに転送される VSA		
PaloAlto-User-Domain	6	これらの VSA を定義するときは値を指定しないでください。
PaloAlto-Client-Source-IP	7	
PaloAlto-Client-OS	8	
PaloAlto-Client-Hostname	9	
PaloAlto-GlobalProtect-Client-Version	10	

LDAP

Lightweight Directory Access Protocol（LDAP）は、情報ディレクトリにアクセスするための標準的なプロトコルです。エンドユーザー、およびファイアウォールと Panorama 管理者用に LDAP 認証の設定を行えます。

LDAP サーバーに接続するようファイアウォールを設定することで、IP アドレスだけでなくユーザーおよびユーザーグループに基づいてポリシールールを定義することも可能になります。流れについては、ユーザーをグループにマッピングおよびユーザーおよびグループ ベースのポリシーの有効化を参照してください。

ローカル認証

ファイアウォールおよび Panorama は管理者およびエンドユーザー用のローカル認証を提供しますが、外部認証サービスは一元的なアカウント管理を提供できるため、たいていの場合はこちらを優先します。しかし、組織が通常のアカウントのために予約しているディレクトリ サーバーを通じて管理しない特別なユーザーアカウントが必要になる場合もあります。例えば、ディレクトリ サーバーがダウンしている場合でもファイアウォールにアクセスできるよう、ファイアウォールに対してローカルのスーパーユーザー アカウントを定義する場合があります。そのようなケースでは、次のローカル認証方式を使用できます。

- （ファイアウォールのみ）ローカル データベース認証—ローカルデータベース認証の設定を行うには、ファイアウォールのトーカルで実行され、ユーザーアカウント（ユーザー名およびパスワード、あるいはパスワードのハッシュ）およびユーザーグループを含むデータベースを作成します。このタイプの認証は、プレーンテキストのパスワードを知らず、パスワードのハッシュだけを知っているケースで、既存の UNIX アカウントの認証情報を再利用するユーザーアカウントを作成する際に便利です。ローカル データベース認証は認証プロファイルに関連するため、異なるユーザーのグループが Kerberos シングル サインオン（SSO）やマルチ ファクター認証（MFA）など、別々の認証設定を必要とするようなデプロイ環境を実現することができます。（詳細については認証プロファイルおよびシーケンスの設定を参照してください）。認証プロファイルを使用する管理者アカウントの場合、パスワードの複雑度は 0、有効期限の設定 0 は適用されません。この認証方式は、ファイアウォール（Panorama ではなく）にアクセスする管理者、および認証ポータルあるいは GlobalProtect を通して、サービスおよびアプリケーションにアクセスするエンドユーザーに対する認証のために利用できます。
- データベースを使わないローカル認証—ファイアウォールあるいは Panorama のローカルで実行される、ユーザーおよびユーザーグループのデータベースを作成することなく、ファイアウォール管理者アカウントあるいはPanorama 管理者アカウントを設定できます。この方式は認証プロファイルと無関係なため、Kerberos SSO や MFA と組み合わせることはできません。ただし、これは個々のアカウントをグローバル設定とは異なるパスワードの有効期限設定に関連付けるパスワードプロファイルを許可できる唯一の認証方法です。（詳細については「パスワードの複雑さおよび有効期限の設定」を参照してください）

認証の導入計画

ファイアウォールにアクセスする管理者および認証ポータルを通じてサービスおよびアプリケーションにアクセスするエンドユーザー用の認証ソリューションを実装する際、事前に考慮すべき重要な項目は以下の通りです。

エンドユーザーおよび管理者の両方について、こちらを考慮してください。

- どうすれば既存のセキュリティ インフラを活用できますか？通常、既存のインフラストラクチャにファイアウォールを統合する作業は、ファイアウォール サービス専用の別のソリューションを新たにセットアップするよりも迅速かつ安価になります。ファイアウォールは、マルチ ファクター認証（MFA）、SAML、Kerberos、TACACS+、RADIUS、および LDAP と統合できます。ユーザーがネットワーク外のサービスおよびアプリケーションにアクセスする場合、SAML を使用してファイアウォールを内外両方のサービスおよびアプリケーションに対するアクセスを制御するアイデンティティ プロバイダ（IdP）と統合できます。
- どうすればユーザーエクスペリエンスを最適化できますか？ユーザーに手動で認証を行わせたくなく、かつ公開鍵インフラストラクチャがある場合は、証明書認証を実装できます。もう一つの選択肢として、Kerberos あるいは SAML シングル サインオン（SSO）を実装し、ユーザーが一度認証を行えば、その後は複数のサービスおよびアプリケーションにアクセスできるようにすることもできます。ネットワークにさらなるセキュリティが必要な場合、証明書認証をインタラクティブな（チャレンジとレスポンス）認証と組み合わせることができます。
- 組織が通常のアカウントのために予約しているディレクトリ サーバーを通じて管理しない特別なユーザーアカウントが必要ですか？例えば、ディレクトリ サーバーがダウンしている場合でもファイアウォールにアクセスできるよう、ファイアウォールに対してローカルのスーパーユーザー アカウントを定義する場合があります。そのような特別な目的を持つアカウント用にローカル認証を設定できます。

  外部認証サービスは、アカウント中央管理、信頼性の高い認証サービス、通常はログ記録およびトラブルシューティング機能を提供するため、通常はローカル認証よりも適しています。
- ユーザー アカウントのユーザー名は正しく書式設定されていますか。SAML、Kerberos、TACACS+、RADIUS、LDAP 認証を利用するには、すべてのユーザー

名が正規表現 Linux ログイン名ルールに従っている必要があります。ユーザー名は **[a-zA-Z0-9_]**という形式でなければなりません。**[a-zA-Z0-9_.-]{0,30}[a-zA-Z0-9_.$-]**。

これは、次の意味を意味します。

- ユーザー名の最初の文字は、英字の大文字または小文字、数字 (0 から 9)、または **_** (アンダースコア) または　**.** (ピリオド) のいずれかでなければなりません。
- 最初と最後の文字以外のユーザー名には、英字、数字 (0 ~ 9)、**_** (アンダースコア)、**.** (ピリオド)、または　が含まれます**>-** (ダッシュ)。最大長は、最初と最後の文字を除いて 30 文字です。
- ユーザー名の最後の文字は、英字の大文字または小文字、数字 (0 から 9)、または **_** (アンダースコア)、**.** (ピリオド)、**$**、または **-** (ダッシュ)。

正規表現 Linux ログイン名ルールに従うことは、PAN-OS 管理者にのみ必要です。これは、GlobalProtect およびキャプティブ ポータル ユーザには必要ありません。

エンドユーザーについてのみ、こちらを考慮してください。

- 他と比べてよりセンシティブなサービスおよびアプリケーションはどれですか？例えば、重要な財務文書に対しては、検索エンジンよりも強力な認証が必要になるかもしれません。極めて重要なサービスおよびアプリケーションを保護するために、マルチ ファクター認証の設定（MFA）を行い、極めて重要なサービスおよびアプリケーションにアクセスする際に各ユーザーが必ず複数の方法（要素）を使って認証を行うようにできます。様々なセキュリティ要件を満たすために、特定のサービス、アプリケーション、エンドユーザーに基づいて MFA あるいは単一の要素（ログイン認証情報や証明書など）による認証をトリガーする認証ポリシールールの設定を行います。攻撃面を減らす他の手段には、ネットワークのセグメント化 や許可されるアプリケーション用のユーザーグループなどがあります。

管理者についてのみ、こちらを考慮してください。

- すべての管理者アカウントの認証を外部サーバーを使って一元的に管理しますか？外部サーバー上でベンダー固有属性（VSA）を定義することで、ファイアウォールで再度設定を行うことなく、ディレクトリ サービスを通じて素早く管理ロールの割り当てを変更できます。また、VSA により、仮想システムが複数あるファイアウォールの管理者用にアクセスドメインを指定することもできます。SAML、TACACS+、および RADIUS は外部認証をサポートしています。

マルチ ファクター認証の設定

重要なサービスおよびアプリケーションを保護するためにマルチ ファクター認証（MFA）を使用するには、最初の認証要素のために Web フォームを表示し、さらにAuthentication Timestamps (認証タイムスタンプ) を記録するよう、認証ポータルの設定を行う必要があります。ファイアウォールはこのタイムスタンプを使用し、認証ポリシールールのタイムアウトを評価します。追加の認証要素を有効化するために、RADIUS あるいはベンダーの API を介して MFA ベンダーとファイアウォールを統合することができます。ファイアウォールは認証ポリシーの評価後にセキュリティポリシーを評価するため、両方のポリシータイプについてルールを設定する必要があります。

Palo Alto Networks はアプリケーションのコンテンツ更新を通じて、MFA ベンダーのサポートを提供しています。そのため、*Panorama* を使ってデバイスグループの設定をファイアウォールにプッシュする場合は、ファイアウォールに *Panorama* のものと同じアプリケーション更新をインストールし、ベンダーサポートの整合性を保つ必要があります。

MFA ベンダー *API* 統合は、認証ポリシーのみを使用するエンドユーザー認証でサポートされます。*GlobalProtect* ポータルまたはゲートウェイへのリモート ユーザー認証、または *PAN-OS* または *Panorama Web* インターフェイスへの管理者認証のために、*RADIUS* または *SAML* でサポートされている *MFA* ベンダーのみを使用できます。ベンダー *API* による *MFA* サービスは、これらの使用例ではサポートされていません。

STEP 1 | **Redirect (リダイレクト)** モードでConfigure Authentication Portal (認証ポータルの設定)を行って、最初の認証要素用の Web フォームを表示し、認証タイムスタンプの記録と、ユーザー マッピングの更新を行います。

STEP 2 | 次のいずれかのサーバープロファイルを設定し、最初の認証要素においてユーザーを認証するサービスにファイアウォールが接続する方法を定義します。

- RADIUS サーバー プロファイルを追加します。これは、RADIUS を通じてファイアウォールがMFA ベンダーと統合されている場合に必須になります。この場合、MFA ベンダーが最初とそれ以降のすべての認証要素を提供するため、次のステップ（MFA サーバープロファイルの設定）をスキップできます。ファイアウォールが API を通じて MFA ベンダーを統合する場合でも、最初の要素で RADIUS サーバープロファイルを使用できますが、追加の要素については MFA サーバープロファイルが必要になります。
- SAML IdP サーバー プロファイルを追加します。
- Kerberosサーバー プロファイルを追加します。
- TACACS+サーバー プロファイルを追加します。
- LDAP サーバー プロファイルを追加します。

たいていの場合、最初の認証要素については外部サービスが推奨されます。ただし、代わりにローカル データベース認証を設定することもできます。

STEP 3 | MFA サーバープロファイルを追加します。

このプロファイルは、ファイアウォールが MFA サーバーに接続する方法を定義します。最初の要素の後、各認証要素について、別々のプロファイルを追加します。ファイアウォールは、ベンダー API によって、これらの MFA サーバーと統合します。指定できる追加要素は 3 つまでです。各 MFA ベンダーは一つの要素を提供しますが、複数の要素の中からユーザーに要素を一つ選択させるベンダーもあります。

1. **Device (デバイス)** > **Server Profiles (サーバープロファイル)** > **Multi Factor Authentication (マルチ ファクター認証)** を選択してプロファイルを **Add (追加)** します。
2. MFA サーバーの識別に使用する**Name (名前)** を入力します。
3. サーバーへの安全な接続をセットアップするときにファイアウォールで MFA サーバー証明書を検証するために使用する **Certificate Profile (証明書プロファイル)** を選択します。
4. デプロイした **MFA Vendor (MFA ベンダー)** を選択します。
5. 各ベンダー属性の **Value (値)** を設定します。

   この属性は、ファイアウォールが MFA サーバーに接続する方法を定義します。各ベンダー **Type (タイプ)** の属性および値が異なっていなければなりません。詳細についてはベンダーのドキュメントを参照してください。
6. **OK** をクリックしてプロファイルを保存します。

STEP 4 | 認証プロファイルを設定します。

このプロファイルは、ユーザーが認証要素に答える順序を定義します。

1. **Device (デバイス)** > **Authentication Profile (認証プロファイル)** を選択してプロファイルを **Add (追加)** します。
2. 認証プロファイルを識別する **Name**（名前）を入力します。
3. 最初の認証要素の **Type (タイプ)**、対応する **Server Profile (サーバープロファイル)** を選択します。
4. **Factors (要素)**、**Enable Additional Authentication Factors (追加の認証要素を有効化)** を選択し、設定した MFA サーバープロファイルを **Add (追加)** します。

   ファイアウォールはリストの順番に従って上から順に MFA サービスを呼び出していきます。
5. **OK** をクリックして認証プロファイルを保存します。

STEP 5 | 認証適用オブジェクトを設定します。

このオブジェクトは、各認証プロファイルを認証ポータル方式と関連付けます。方式によって、最初の認証チャレンジ（要素）が透過的に行われるか、ユーザーの応答を求めるのかが決まります。

設定した **Authentication Profile** (認証プロファイル) を選択し、最初の要素に対して認証を行う方法をユーザーに伝える **Message** (メッセージ) を入力します。このメッセージは、認証ポータルの Web フォームに表示されます。

Authentication Method (認証方法) を ***browser-challenge*** に設定すると、*Kerberos SSO* 認証が失敗した場合のみ、認証ポータルの *Web* フォームが表示されるようになります。そうでない場合は、最初の要素に対する認証が自動的に行われ、ユーザーに *Web* フォームが表示されません。

STEP 6 | 認証ポリシールールを設定します。

ルールは、保護したいサービスおよびアプリケーション、認証が必要なユーザーにマッチしなければなりません。

1. **Policies (ポリシー)** > **Authentication (認証)** を選択してルールを **Add (追加)** します。
2. ルールを識別する **Name (名前)** を入力します。
3. **Source (送信元)** を選択し、特定のゾーンおよび IP アドレスを **Add (追加)** するか、**Any (すべて)** のゾーンあるいは IP アドレスを選択します。

   ルールは、指定した IP アドレスあるいは指定したゾーン内のインターフェイスから来るトラフィックにのみ適用されます。
4. **User (ユーザー)**を選択し、ルールを適用する送信元ユーザーおよびユーザーグループを選択あるいは **Add (追加)** います（デフォルトは **any (すべて)**です）。
5. **Source (宛先)** を選択し、特定のゾーンおよび IP アドレスを **Add (追加)** するか、**any (すべて)** のゾーンあるいは IP アドレスを選択します。

   IP アドレスは、アクセスを制御したいリソース（サーバーなど）にすることができます。
6. **Service/URL Category (サービス/URL カテゴリ)** を選択し、ルールによってアクセスを制御するサービスおよびサービスグループを選択あるいは **Add (追加)** します（デフォルトは **service-http**です）。
7. ルールによってアクセスを制御するURL カテゴリを選択あるいは **Add (追加)** します（デフォルトは **any (すべて)**です）。例えば、極めて重要な内部サイトを指定するカスタム URL カテゴリを作成することができます。
8. **Actions** （アクション） を選択し、作成した **Authentication Enforcement (認証適用)** オブジェクトを選択します。
9. サービスおよびアプリケーションに繰り返しアクセスする際に、ファイアウォールがユーザーに一度だけ認証を求める期間として、分単位で **Timeout (タイムアウト)** 期間（デフォルトは 60）を指定します。

   Timeout (タイムアウト)は、強固なセキュリティ（認証のプロンプトを表示する間隔が短い）とユーザーエクスペリエンス（認証のプロンプトを表示する間隔が長い）の間のトレードオフになります。データセンターなどの重要なシステムやセンシティブな領域へのアクセスが対象である場合、できるだけ頻繁に認証を行うのが最適な選択になるでしょう。ネットワークの境界やユーザーエクスペリエンスが重要なビジネスの場合は、認証の頻度を減らすことが最適な選択になるでしょう。
10. **OK** をクリックしてルールを保存します。

STEP 7 | MFA ログイン ページをカスタマイズします。

ファイアウォールはこのページを表示し、MFA 要素に対して認証を行う方法と認証状態（進行中、成功、失敗）をユーザーに伝えます。

1. **Device (デバイス)** > **Response Pages (応答ページ)** の順に選択し、さらに **MFA Login Page (MFA ログインページ)** を選択します。
2. **Predefined (定義済み)** の応答ページを選択し、ページをクライアントシステムに **Export (エクスポート)** します。
3. クライアント システムで、HTML エディタを使用してダウンロードした応答ページをカスタマイズして、一意のファイル名を付けて保存します。
4. ファイアウォールの MFA Login Page (MFA ログイン ページ) ダイアログに戻り、カスタマイズしたページを **Import (インポート)** し、**Import File (インポート ファイル)** を **Browse (参照)** して選択し、さらに **Destination (宛先)** （仮想システムあるいは **shared (共有)** 場所）を選択して **OK**、**Close (閉じる)** の順にクリックします。

STEP 8 | 認証が必要なサービスおよびアプリケーションへのアクセスをユーザーに許可するセキュリティポリシー ルールを設定します。

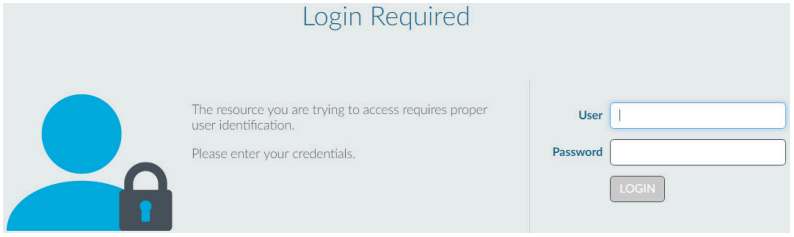
1. セキュリティ ポリシー ルールを作成します。
2. 変更をコミットします。

ファイアウォールの自動相関エンジンは複数の相関オブジェクトを使用し、*MFA* に関連してネットワーク上で発生したおそれがある認証情報の悪用イベントを検出します。イベントを確認するには、 ***Monitor (監視)*** > ***Automated Correlation Engine (自動相関エンジン)*** > ***Correlated Events (相関されたイベント)*** を選択します。

STEP 9 | ファイアウォールが MFA を適用することを確認します。

1. 認証ルールで指定されているいずれかのソース ユーザーとしてネットワークにログインします。
2. ルールで指定されているいずれかのものにマッチするサービスあるいはアプリケーションをリクエストします。

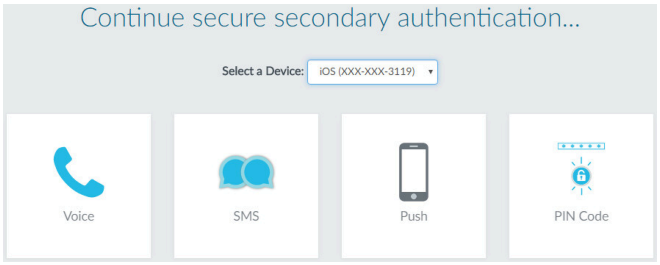
   ファイアウォールが最初の認証要素用に認証ポータルの Web フォームを表示します。このページには、認証適用オブジェクトで入力したメッセージが含まれています。以下に例を示します。



3. 最初の認証チャレンジで使用するユーザーの認証情報を入力します。

   そうすると、ファイアウォールが次の認証要素のために MFA ログインページを表示します。例えば、認証方法として音声、SMS、プッシュ通知、あるいは PIN コード

（OTP）のいずれかを選択するよう、MFA サービスに求められるかもしれません。プッシュを選択すると、認証を承認するよう、お使いの電話によって求められます。



4. 次の要素に対して認証を行います。

   認証が成功あるいは失敗したことを示すメッセージをファイアウォールが表示します。認証が成功すると、次の認証要素がある場合はファイアウォールが MFA ログインページを表示します。

   各 MFA 要素に対してこの手順を繰り返します。すべての要素に対して認証を済ませると、ファイアウォールはセキュリティ ポリシーを評価して、サービスあるいはアプリケーションへのアクセスを許可するかどうかを判断します。
5. 先ほどアクセスしたサービスあるいはアプリケーションのセッションを終了します。
6. 同じサービスあるいはアプリケーションのセッションを新しく開始します。必ず、認証ルールで指定した**Timeout (**タイムアウト**)** の期間内にこのステップを実行するようにしてください。

   再認証を行うことなく、ファイアウォールがアクセスを許可します。
7. **Timeout (**タイムアウト**)** の期間が過ぎるのを待ってから、同じサービスあるいはアプリケーションをリクエストします。

   ファイアウォールに再認証を求められます。

RSA SecurID とファイアウォールの間で MFA を設定する

マルチ ファクター認証では、複数の要素を使用して企業のアセットを保護し、ネットワーク リソースへのアクセスを許可する前にユーザーの身元を確認することができます。ファイアウォールと RSA SecurID Access クラウド認証サービスの間でマルチ ファクター認証（MFA）を有効にするには、最初に RSA SecurID サービスを設定して、複数の要素を使用してユーザーを認証するようにファイアウォールを設定する必要があるようにする必要があります。RSA SecurID Access Console で必要な設定を行った後、RSA SecurID と統合するようにファイアウォールを設定できます。

*Palo Alto Networks*の次世代ファイアウォールは、*RSA SecurID Access Cloud Authentication Service*と統合されています。*RSA SecurID* と *MFA API* との統合はクラウドベースのサービスでのみサポートされており、*2* つ目の認証要素がベンダー固有の *API* を使用するオンプレミスの認証マネージャーについては、*2* 要素認証をサポートしていません。この統合に必要な最小コンテンツ バージョンは、*752* および *PAN-OS 8.0.2* です。

- RSA SecurID Access Cloud 認証サービスの詳細を取得する

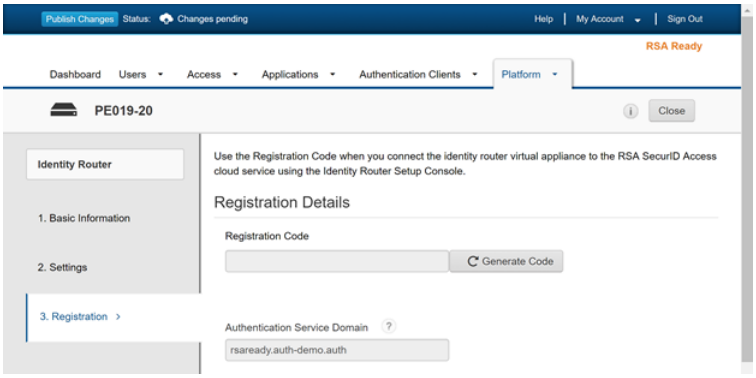
- RSA SecurID を使用して MFA のファイアウォールを設定する

RSA SecurID Access Cloud 認証サービスの詳細を取得する

ファイアウォールと RSA SecurID Access Cloud 認証サービスとの間でユーザー認証リクエストを安全に渡すには、まず RSA SecurID アクセス コンソールにアクセスし、RSA Access ID、認証サービス URL、およびクライアント API キーを設定する必要があります。ファイアウォールは認証してサービスと対話する必要があります。ファイアウォールには、IDA に対して認証するための RSA 承認または RSA トークン コード認証方式のいずれかを使用するアクセス ポリシー IDも必要です。

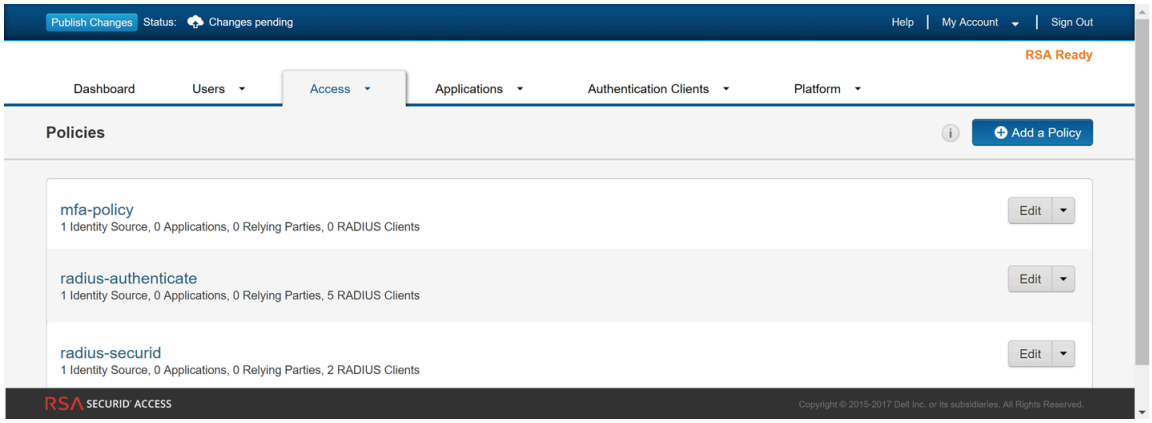
RSA SecurID API キーを作成する—RSA SecurID Access Console にログオンして、**My Account**（マイアカウント） > **Company Settings**（会社設定） > **Authentication API Keys**（認証 **API** キー）を選択します。新しいキーを **Add**（追加）して、**Save Settings**（設定を保存）と **Publish Changes**（変更のパブリッシュ）を行います。

ファイアウォールが必ず接続する **RSA SecurID Access** エンドポイント **API**（認証サービス ドメイン）を取得する—**Platform**（プラットフォーム） > **Identity Routers**（**ID** ルーター）を選択して、Identity Router（ID ルーター） を 1 つ選んで **Edit**（編集）し、**Authentication Service Domain**（認証サービス ドメイン）を書き留めます。この例では、https://rsaready.auth-demo.auth が対象です。



Access Policy ID を取得する—**Access**（アクセス） > **Policies**（ポリシー） を選択して、ファイアウォールを RSA SecurID サービスの認証クライアントとして機能させるアクセス ポリ

シー名を書き留めます。このポリシーは、RSA Approve または RSA Tokencode 認証方式のみを使用するように設定する必要があります。



RSA SecurID を使用して MFA のファイアウォールを設定する

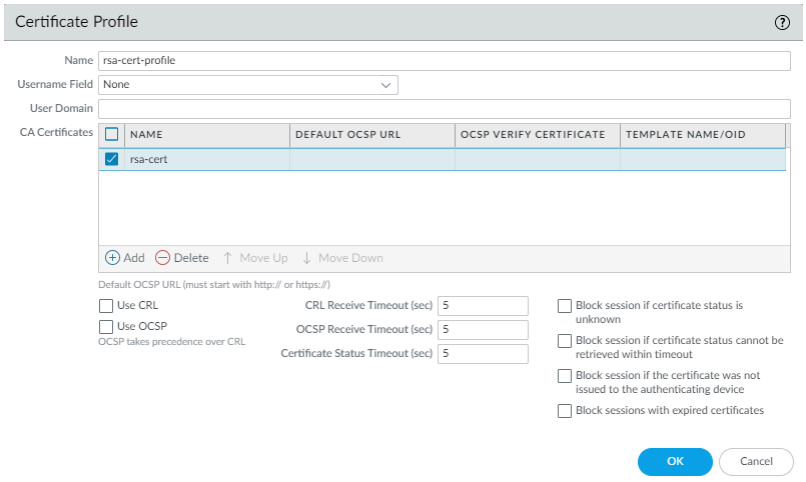
RSA SecurID アクセス クラウド認証サービスの詳細を取得後は、MFA 呼び出し時にユーザーに RSA SecurID トークンを要求するようにファイアウォールを設定できます。

STEP 1 | RSA SecurID Access エンドポイント API によって提供される SSL 証明書を信頼するようにファイアウォールを設定します。

1. RSA SecurID Access エンドポイントから SSL 証明書をエクスポートし、ファイアウォールにインポートします。

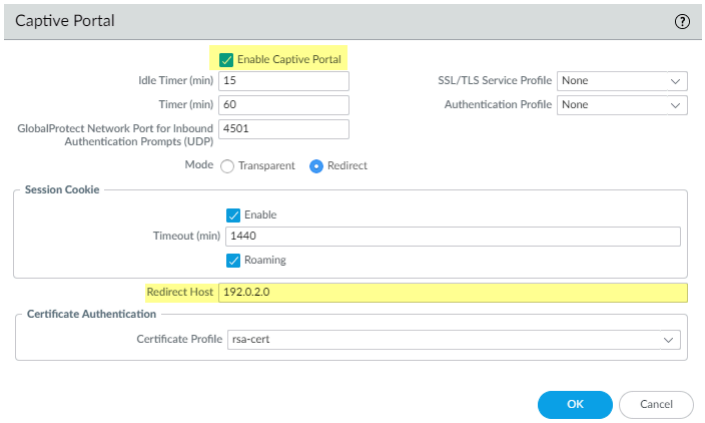
   ファイアウォールと RSA SecurID Access エンドポイント API 間の信頼を有効にするには、自己署名証明書または証明書の署名に使用された CA 証明書をインポートする必要があります。

2. 証明書プロファイルを設定して（**Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificate Profile**（証明書プロファイル）、**Add**（追加）をクリックします。



STEP 2 | Redirect (リダイレクト) モードで、認証ポータルを設定（**Device**（デバイス） > **User Identification**（ユーザー ID） > **Authentication Portal Settings**（認証 ポータル設定））すると、RSA SecureID への認証用 Web フォームが表示されます。リダイレクト ホスト

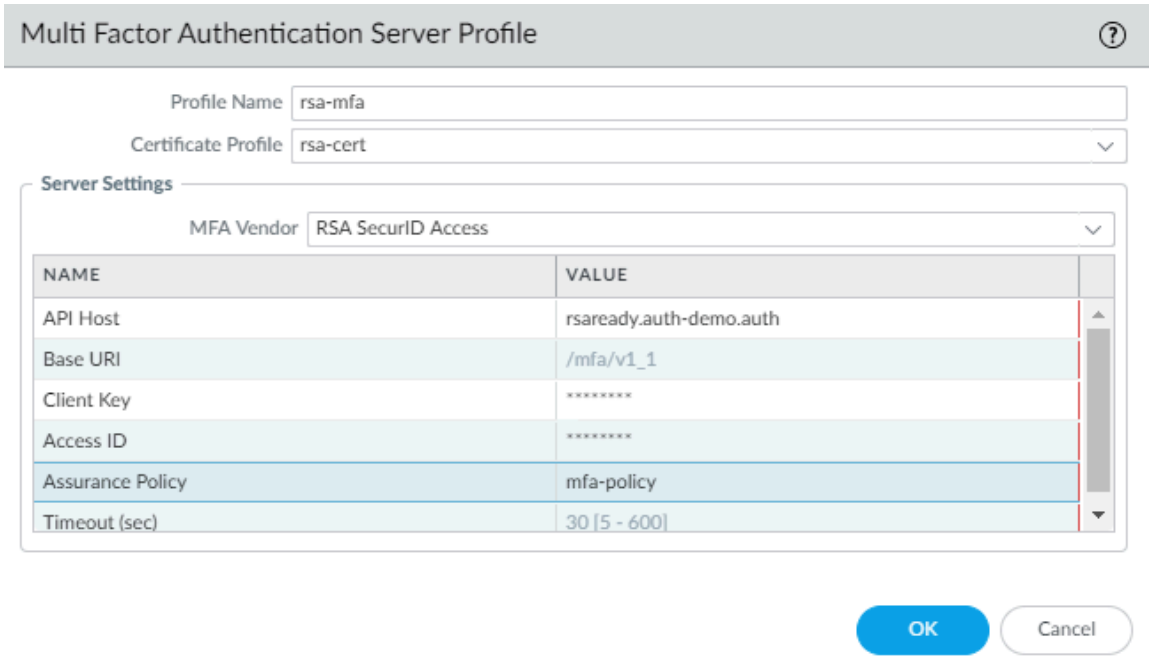
は、Web リクエストがリダイレクトされるファイアウォールのレイヤー 3 インターフェイスの IP アドレスに解決される IP アドレスまたはホスト名を、名前にピリオドを付けずに指定してください。



STEP 3 | マルチ ファクター認証サーバー プロファイルを設定して、どのようにファイアウォールを RSA SecurID クラウド サービスで接続するか指定して、（**Device**（デバイス） > **Server Profiles**（サーバー プロファイル） > **Multi Factor Authentication**（マルチ ファクター認証））、**Add**（追加）をクリックします。

1. MFA サーバー プロファイルの識別に使用する**Name (名前)** を入力します。
2. この例では、rsa-cert-profile の、先程作成した **Certificate Profile**（証明書プロファイル）を選択します。ファイアウォールは、RSA SecurID クラウド サービスとの安全な接続を確立するときにこの証明書を使用します。
3. **MFA Vendor**（**MFA** ベンダー）ドロップダウンリストで、**RSA SecurID Access** を選択します。

4. 「RSA SecurID アクセス クラウド認証サービスの詳細を取得」で記した各属性の **Value**（値）を設定します。
   - **API Host**（**API** ホスト）—この例では、ファイアウォールが接続する必要がある RSA SecurID Access API エンドポイントのホスト名または IP アドレス、rsaready.auth-demo.authを入力します。
   - **Base URI**（ベース **URI**） —デフォルト値（/mfa/v1_1）を変更しないでください
   - **Client Key**（クライアント キー）—RSA SecurID クライアント キーを入力します。
   - **Access ID**（アクセス **ID**）—RSA SecurID Access ID を入力します。
   - **Assurance Policy**（保証ポリシー）—この例の mfa-policy では、RSA SecurID アクセス ポリシー名を入力します。
   - **Timeout**（タイムアウト）—デフォルトは 30 秒間です。

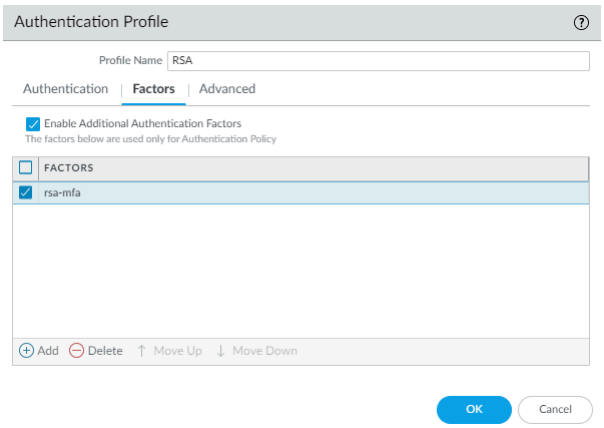


5. プロファイルを保存します。

STEP 4 | 認証プロファイルを設定して（**Device**（デバイス） > **Authentication Profile**（認証プロファイル））、**Add**（追加）をクリックします。

このプロファイルは、ユーザーが認証要素に答える順序を定義します。

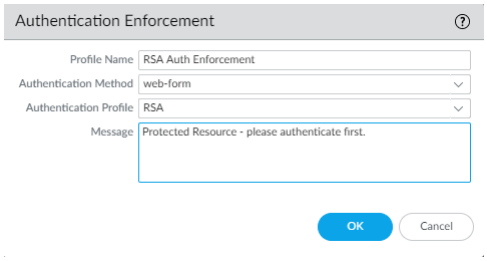
1. 最初の認証要素の **Type (タイプ)**、対応する **Server Profile (サーバープロファイル)** を選択します。
2. **Factors (要素)**、**Enable Additional Authentication Factors (追加の認証要素を有効化)** を選択し、この例の前で作成した rsa-mfa サーバー プロファイルを **Add (追加)** します。



3. **OK** をクリックして認証プロファイルを保存します。

STEP 5 | 認証適用オブジェクトを設定します。**Objects (オブジェクト)** > **Applications (アプリケーション)**を選択して**Add (追加)** をクリックします。

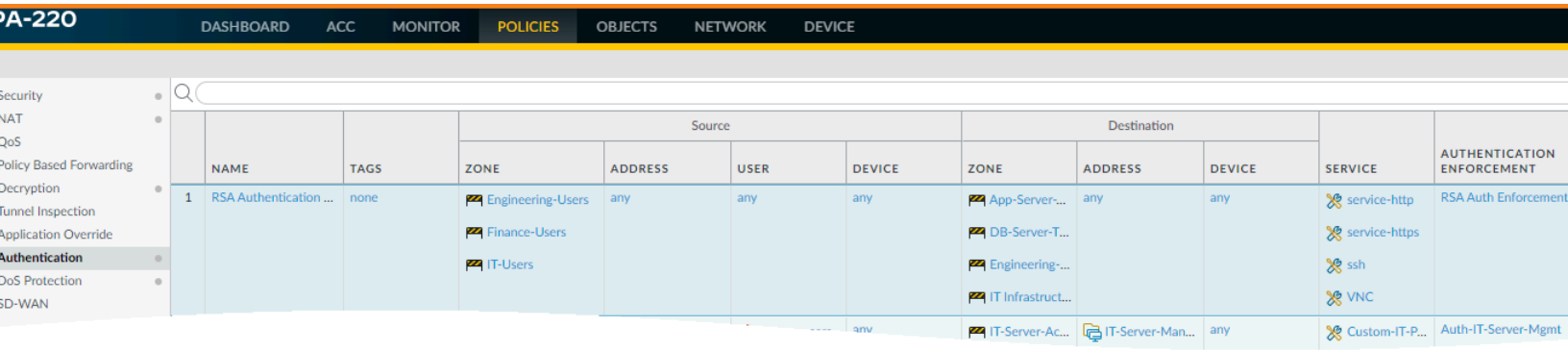
この例では、RSA という定義済みの認証プロファイルを選択してください。



STEP 6 | 認証ポリシールールを設定します。**Policies(ポリシー)** > **Applications (アプリケーション)**を選択して**Add (追加)**をクリックします。

認証ポリシー ルールは、保護するサービスとアプリケーションと一致している必要があります。認証する必要があるユーザーを指定し、認証プロファイルをトリガする認証適用オブジェクトを含めます。この例では、RSA SecurID Access は、RSA Auth Enforcement と呼ばれる認証オブジェクトが付属する HTTP、HTTPS、SSH、および VNC トラフィックにアクセス

するすべてのユーザーを認証します（**Actions**（操作）で、**Authentication Enforcement**（認証の適用）オブジェクトを選択します）。

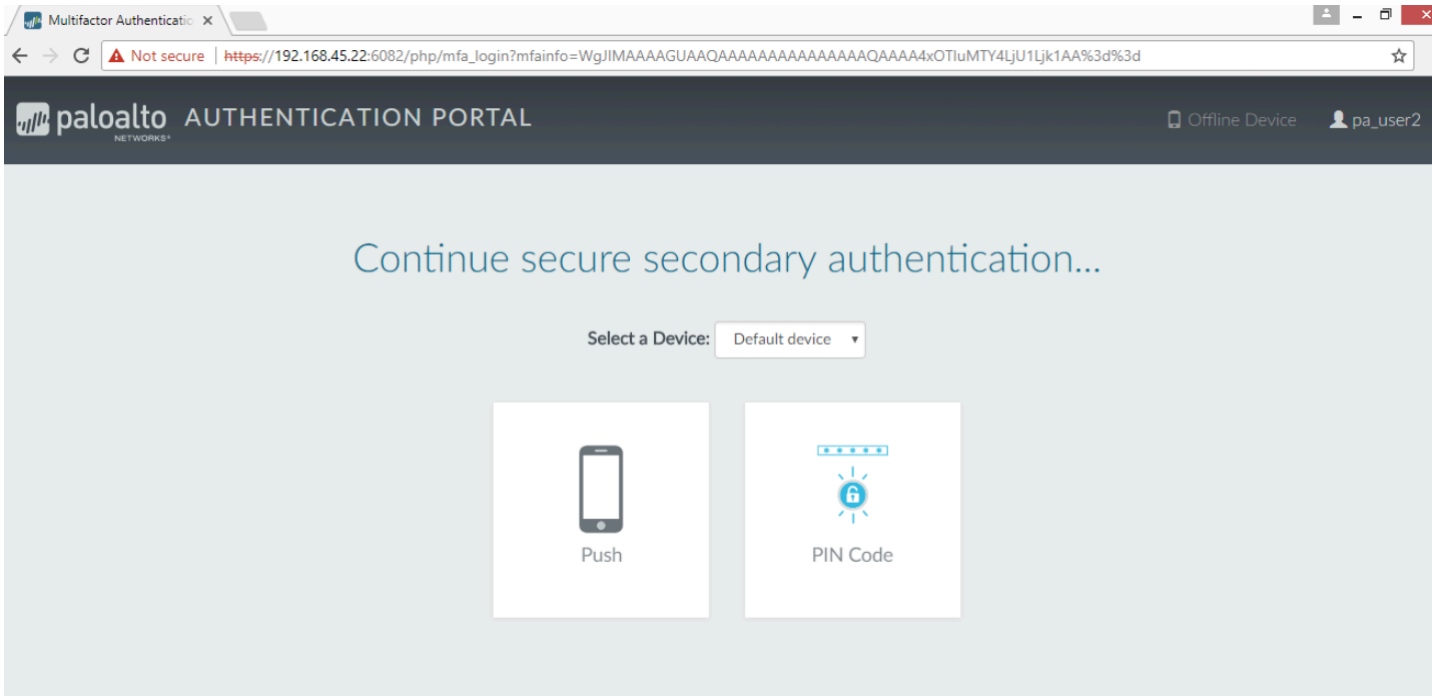


STEP 7 | ファイアウォールへの変更を **Commit**（コミット）します。

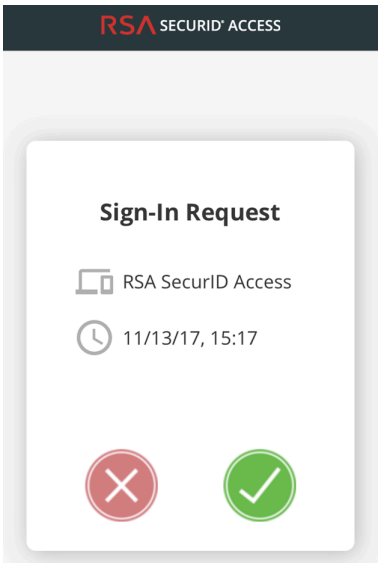
STEP 8 | 有効にしたプッシュまたは PIN コード認証方式を使用して、RSA SecurID を使用してネットワーク上のユーザーがセキュリティ保護されていることを確認します。

1. プッシュ認証

   1. ネットワーク上のユーザーに Web ブラウザを起動して Web サイトにアクセスするように要求します。前に定義したリダイレクト ホストの IPアドレスまたはホスト名を含む認証ポータル ページが表示されます。
   2. ユーザーが最初の認証要素の証明書を入力してから、2 次認証要素に進み、**Push**（プッシュ）を選択することを確認します。



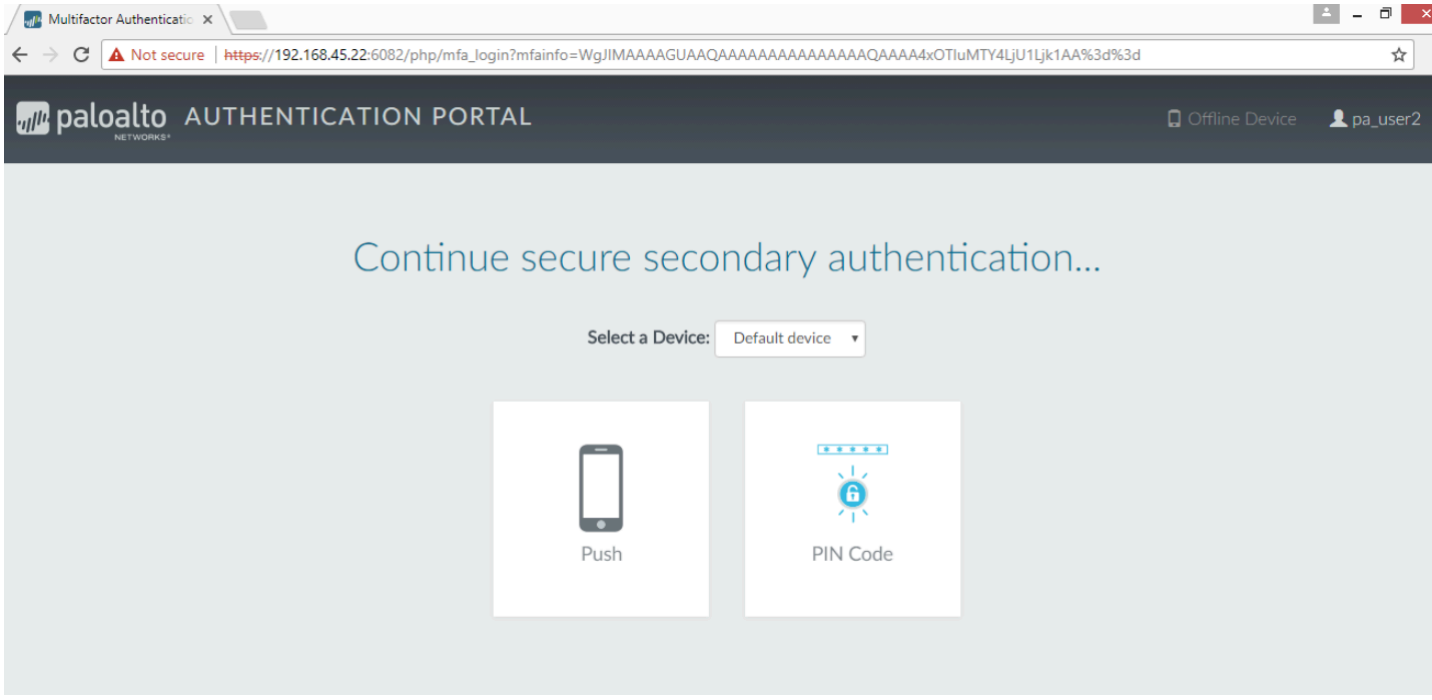
   3. ユーザーのモバイル デバイス上の RSA SecurID Access アプリケーションで **Sign-In request**（サインイン要求）を確認します。
   4. モバイル デバイス上でサインイン リクエストを**Accept**（承認）するようにユーザーに依頼し、ファイアウォールが認証の成功の通知を受信するのを数秒間待機します。ユーザーは、要求された Web サイトにアクセスできる必要があります。



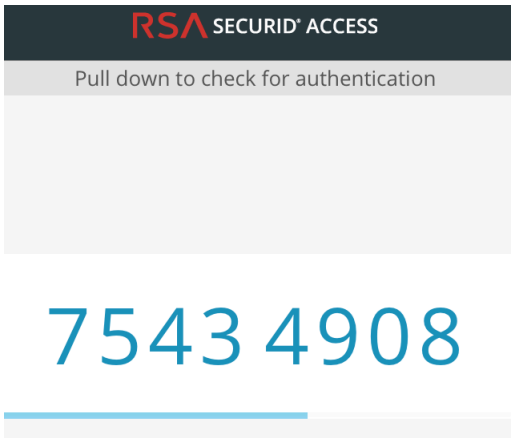
認証エラーをテストするには、モバイル デバイス上のサインイン要求を ***Decline***（拒否）します。

2. **PIN** コード認証

   1. ネットワーク上のユーザーに Web ブラウザを起動して Web サイトにアクセスするように要求します。前に定義したリダイレクト ホストの IPアドレスまたはホスト名を含む認証ポータル ページが表示されます。
   2. ユーザーが最初の認証要素の証明書を入力してから、2 次認証要素に進み、 **PIN Code**（**PIN** コード） を選択することを確認します。



3. **PIN** コード がユーザーのモバイル デバイスの RSA SecurID Access アプリケーションに表示されていることを確認します。



4. Web ブラウザの **Enter the PIN...**（**PIN** を入力...）プロンプトで PIN コードをコピーし、**Submit**（送信）をクリックします。ファイアウォールが正常な認証の通知を受け取るまで数秒間待ちます。ユーザーは、要求された Web サイトにアクセスできる必要があります。

Okta およびファイアウォール間の MFA を設定

マルチ ファクター認証では、複数の要素を使用して企業のアセットを保護し、ネットワーク リソースへのアクセスを許可する前にユーザーの身元を確認することができます。

ファイアウォールおよび Okta ID 管理サービス間の多要素認証（MFA）を有効化する方法：

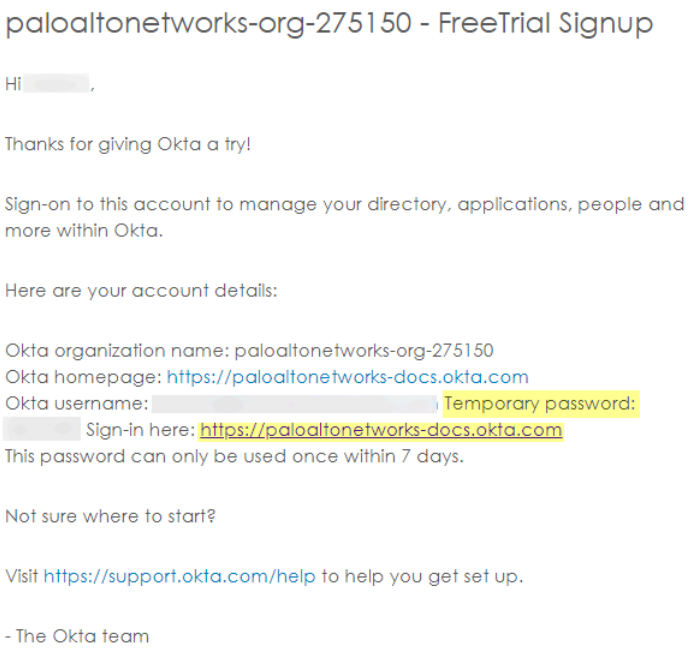
- Okta を設定
- Okta と統合するためにファイアウォールを設定
- Okta を伴う MFA を検証

Okta を設定

Okta 管理ポータルにログインしてユーザーアカウントを作成し、Okta MFA ポリシーを定義し、ファイアウォール上で Okta を伴う MFA を設定するのに必要なトークン情報を取得します。

STEP 1 | Okta 管理者ユーザーアカウントを作成します。

1. メールアドレスおよび名前を送信してから**Get Started (開始)**をクリックします。
2. 確認用メールに記載されているリンクをクリックし、そこに含まれている仮パスワードを使用して Okta 管理ポータルにログインします。



paloaltonetworks-org-275150 - FreeTrial Signup

Hi ,

Thanks for giving Okta a try!

Sign-on to this account to manage your directory, applications, people and more within Okta.

Here are your account details:

Okta organization name: paloaltonetworks-org-275150
Okta homepage: https://paloaltonetworks-docs.okta.com
Okta username: Temporary password:
Sign-in here: https://paloaltonetworks-docs.okta.com
This password can only be used once within 7 days.

Not sure where to start?

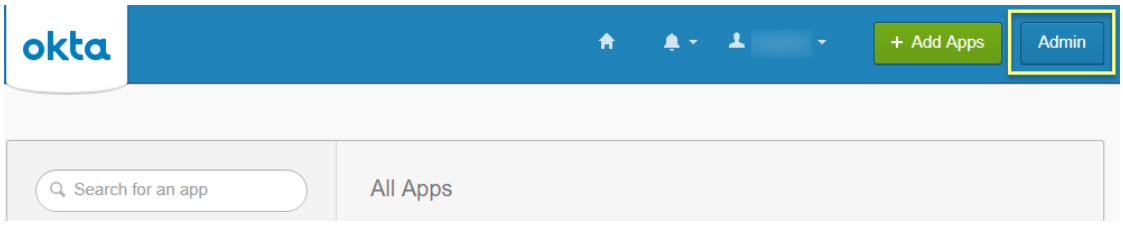
Visit https://support.okta.com/help to help you get set up.

- The Okta team

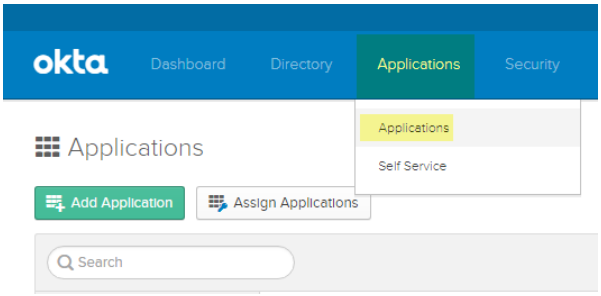
3. 小文字 1 文字、大文字 1 文字、数字を含み、ユーザー名で使われているどの文字も含まない最低 8 文字のパスワードを新規作成します。
4. パスワードを忘れた時のための質問を選択し、その回答を入力します。
5. セキュリティ用の画像を選択してから**Create My Account (アカウントを作成)**します。

STEP 2 | Okta サービスを設定します。

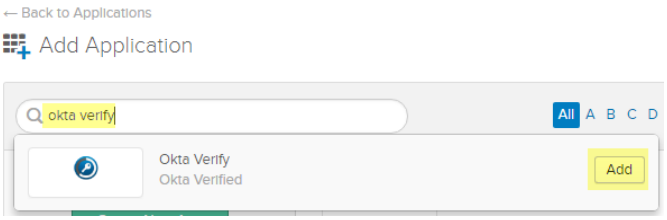
ログインし、*Okta* 管理ポータルにリダイレクトされない場合は、右上の***Admin*** *(*管理*)*を選択します。



1. Okta ダッシュボードで Okta 管理用認証情報を使用してログインしてから、**Applications (**アプリケーション**)** > **Applications (**アプリケーション**)**を選択します。

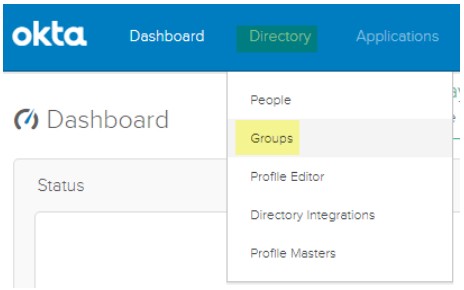


2. **Add Application (**アプリケーションの追加**)** を選択します。
3. **`Okta Verify`**を検索します。
4. **Add (**追加**)**、そして**Done (**完了**)**を選択します。

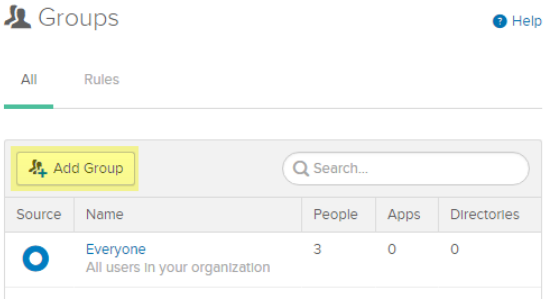


STEP 3 | 一つあるいは複数のユーザーグループを作成してユーザーをカテゴリー分け（例えば、デバイス毎、ポリシー毎、部課単位）し、Okta Verify アプリケーションを割り当てます。

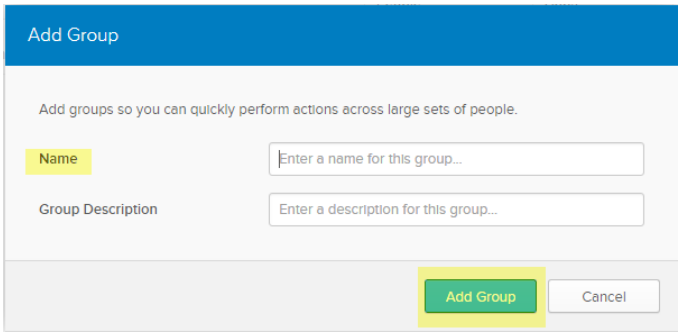
1. **Directory (ディレクトリ)** > **Groups (グループ)**を選択します。



2. **Add Group (グループの追加)**をクリックします。

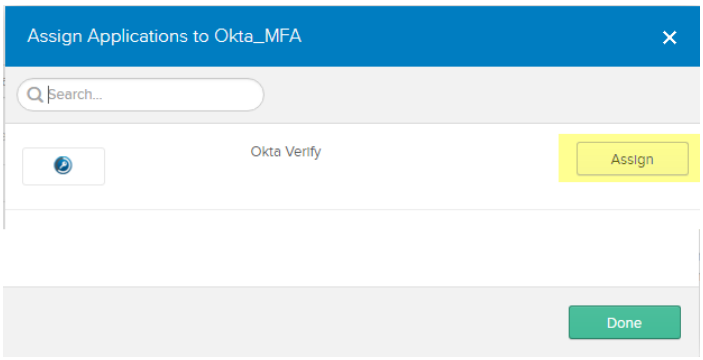


3. グループの**Name (名前)**、および任意で**Group Description (グループの説明)**を入力してから**Add Group (グループを追加)**します。



デフォルトのグループである***Everyone* (全員)**には、Okta を設定の最初のステップで設定した組織のすべてのユーザーが含まれます。

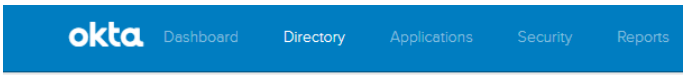
4. 作成したグループを選択し、さらに**Manage Apps (アプリの管理)**を選択します。
5. ステップ 2 で追加した Okta Verify アプリケーションを**Assign (割り当て)**ます。

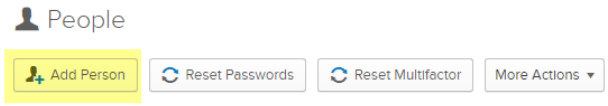


6. アプリケーションが**Assigned (**割り当て済み**)**になったら**Done (**完了**)**をクリックします。
7. MFA 用に Okta Verify アプリケーションを使用するすべてのグループに対してこの作業を繰り返します。

STEP 4 | ユーザーを追加してグループに割り当てます。

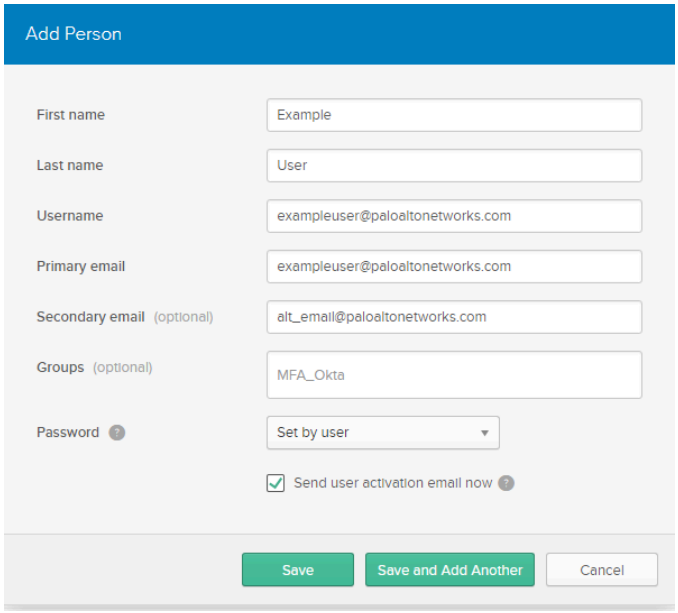
1. Okta ダッシュボードで**Directory (**ディレクトリ**)** > **People (**人々**)** > **Add Person (**人の追加**)**を選択します。





2. ユーザーの**First Name (**名**)**、**Last Name (**姓**)**、および**Username (**ユーザー名**)**を入力します。ユーザー名は、自動入力される**Primary email (**第一メール**)**、およびファイアウォー

ルで入力したユーザー名と一致しなければなりません。任意で、**Secondary Email (第 2 メール)**としてユーザーの代わりのメールアドレスを入力できます。



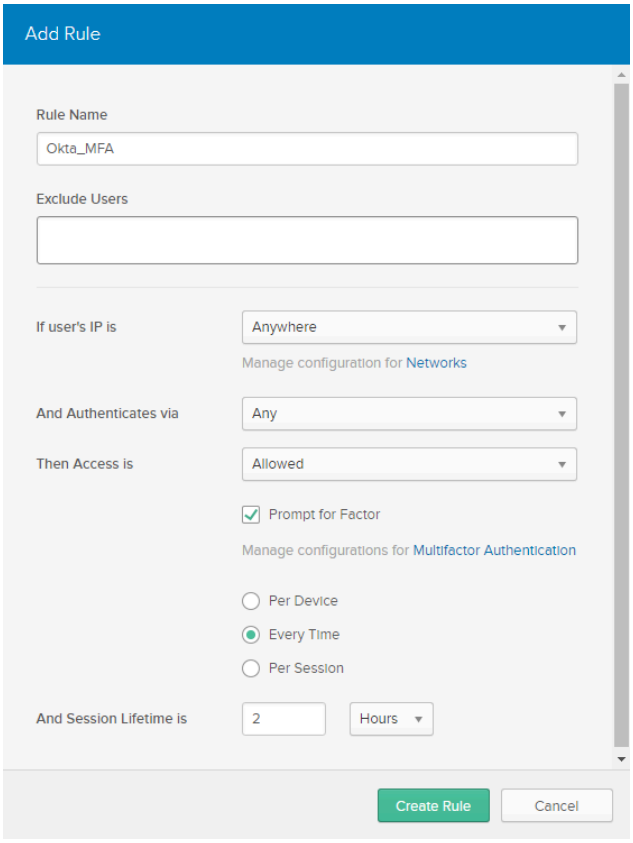
3. このユーザーに関連するグループあるいは**Groups (グループ)**の名前を入力します。入力を始めると、グループ名が自動補完されます。
4. **Send user activation email now (ユーザーにアクティベーション用メールを今すぐ送信)**にチェックを入れてから、**Save (保存)**して単一のユーザーを追加するか、**Save and Add Another (保存してさらに追加)**して別のユーザーに対して作業を行います。

STEP 5 | テスト ポリシーをユーザーに割り当てます。

1. **Security (セキュリティ)** > **Authentication (認証)** > **Sign On (サインオン)**を選択します。

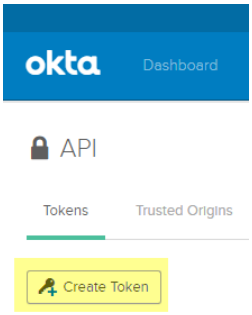
   MFA を使ってログインするようユーザーに求めない**Default Rule (デフォルトルール)**を持つ**Default Policy (デフォルト ポリシー)**があります。
2. **Rule Name (ルール名)**を入力し、MFA プロンプトを適用するための**Prompt for Factor (ファクター用プロンプト)**をチェックし、プロンプトのタイプ（**Per Device (デバイス単**

位)、**Every Time** (毎回)、あるいは**Per Session** (セッション単位)）を選択してから、さらに**Create Rule** (ルールの作成)を選択します。

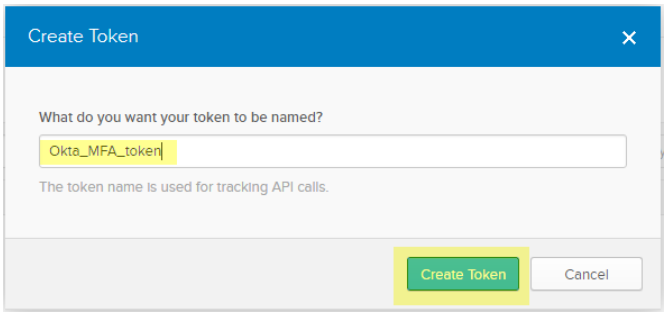


STEP 6 | Okta 認証トークンの情報は一度しか表示されないため、安全なところに記録しておいてください。

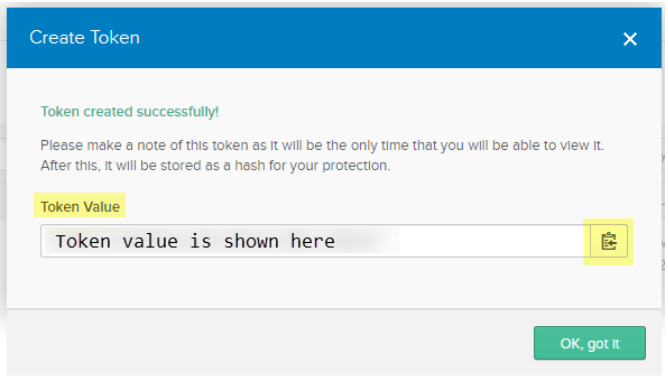
1. **Security (セキュリティ)** > **API** > **Tokens (トークン)**を選択します。
2. **Create Token (トークンの作成)**を選択します。



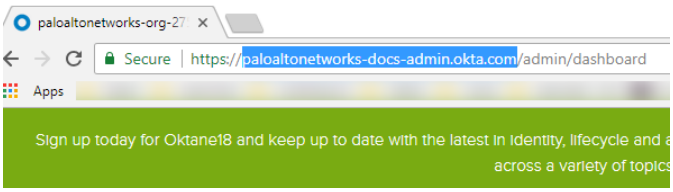
3. トークンの名前を入力してから**Create Token (トークンを作成)**します。



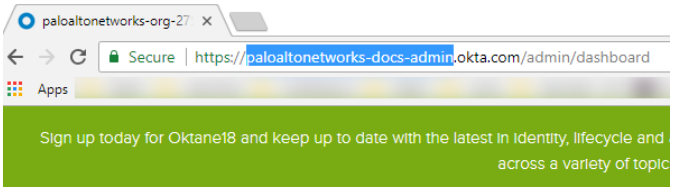
4. **Token Value (トークンの値)**をコピーします。
   クリップボードにコピー ボタンをクリックすると、Token Value をクリップボードにコピーできます。



5. Okta 管理ダッシュボードの URL のところで、**API host (API ホスト)**として使用する**`https://`**から**`/admin`**までの部分 URLをコピーします。



6. **Organization (組織)**として使用する際は、この URL のドメイン**okta.com**を省略します。



例えば、上記の Okta 管理ダッシュボードの URL の例では、**https://paloaltonetworks-doc-admin.okta.com/admin/dashboard**：

- The API ホスト名は **paloaltonetworks-doc-admin.okta.com**です。
- 組織は**paloaltonetworks-doc-admin**です。

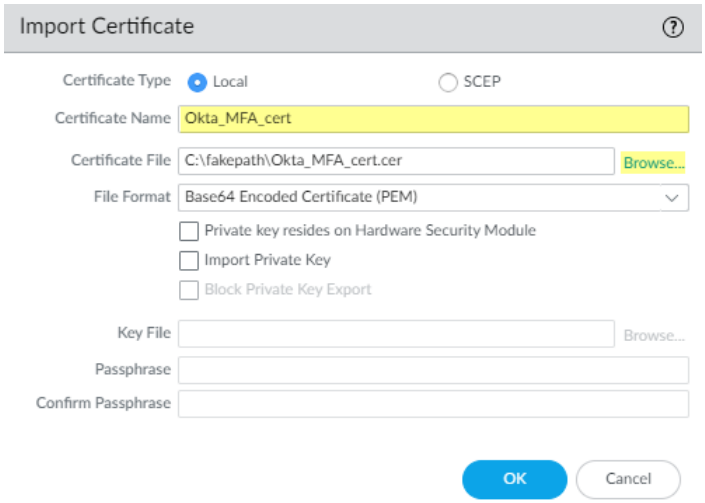
STEP 7 | Base-64 エンコーディングを使用して証明書チェーン内のすべての証明書をエクスポートします。

1. お使いのブラウザに応じて、次のいずれかの方法でチェーン内のすべての証明書をエクスポートします。
   - **Chrome**—**F12**を押してから**Security (セキュリティ)** > **View Certificate (証明書の表示)** > **Details (詳細)** > **Copy to File (ファイルにコピー)**を選択します。
   - **Firefox**—**Options (オプション)** > **Privacy & Security (プライバシーおよびセキュリティ)** > **View Certificates (証明書の表示)** > **Export (エクスポート)**を選択します。
   - **Internet Explorer**— **Settings (設定)** > **Internet Options (インターネット オプション)** > **Content (コンテンツ)** > **Certificates (証明書)** > **Export (エクスポート)**.を選択します。
2. Certificate Export Wizard (証明書エクスポート ウィザード) を使用してチェーン内のすべての証明書をエクスポートし、フォーマットとして **Base-64 encoded X.509 (Base-64 エンコードの X.509)**を選択します。

Okta と統合するためにファイアウォールを設定

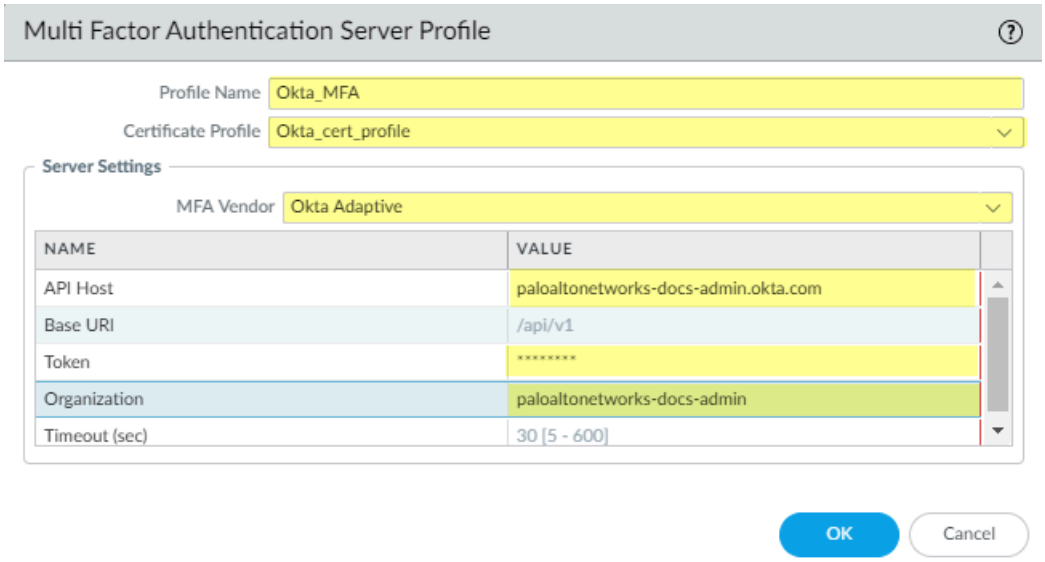
前提条件として、Okta を使って認証させたいすべてのユーザーをマッピングしていることを確認してください。

STEP 1 | ファイアウォールの証明書チェーン内のすべての証明書をImport（インポート）し、インポートした CA 証明書（ルートおよび中間）をCertificate Profile (証明書プロファイル)に追加します。



STEP 2 | Okta 用の多要素認証サーバープロファイルを追加します。

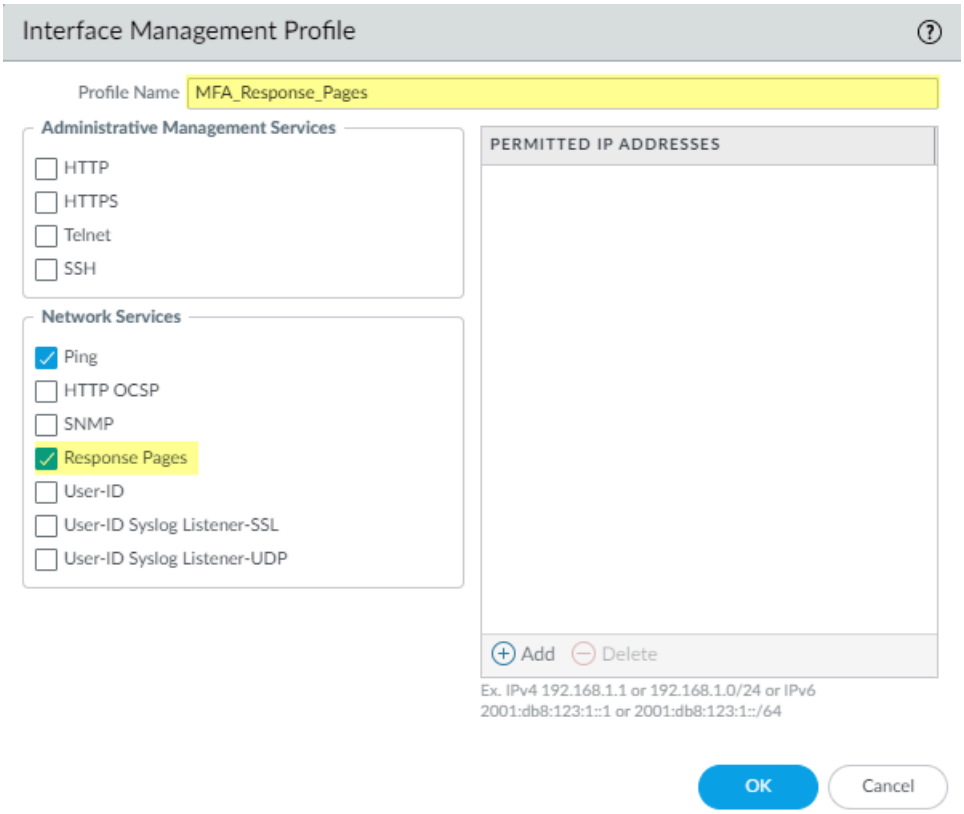
1. **Device (デバイス)** > **Server Profiles (サーバープロファイル)** > **Multi Factor Authentication (多要素認証)**を選択します。
2. MFA サーバープロファイルを追加します。



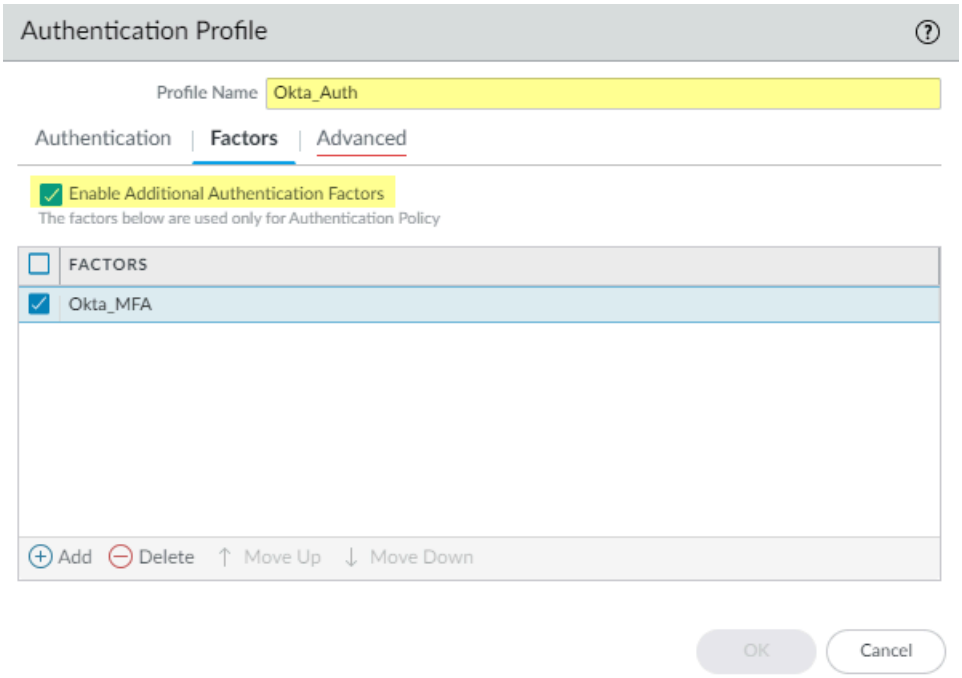
3. **Profile Name (プロファイル名)**を入力します。
4. Okta と統合するためのファイアウォールの設定のステップ 1 で作成した**Certificate Profile (証明書プロファイル)**を選択します。
5. **Okta Adaptive**を**MFA Vendor (MFA ベンダー)**として選択します。
6. Okta と統合するためのファイアウォールの設定のステップ 4 の**API Host (API ホスト)**、**Token (トークン)**、および**Organization (組織)**を入力します。

STEP 3 | **Redirect Mode (**リダイレクト モード**)**を使って、Configure Authentication Portal (認証ポータルの設定)を行い、ユーザーを MFA ベンダーの認証チャレンジにリダイレクトします。

STEP 4 | ユーザーを応答ページの認証チャレンジにリダイレクトするために、インターフェイス管理プロファイルで応答ページを有効化します。



STEP 5 | 認証プロファイルを作成し、MFA ベンダーを**Factor (要素)**として追加します（マルチ ファクター認証の設定、ステップ 3 を参照）。



STEP 6 | ソース ゾーン上のUser-ID の有効化を行い、識別されたユーザーに対し、MFA ベンダーを使って認証チャレンジに答えるよう求めます。

STEP 7 | MFA ベンダーを使用する認証適用オブジェクトを作成し、認証ポリシールールを作成します（認証ポリシーの設定のステップ 4 と 5 を参照）。

STEP 8 | 変更をコミットします。

Okta を伴う MFA を検証

STEP 1 | ユーザーが登録メールを受け取り、アカウントを有効化し、Okta Verify アプリを自身のデバイスにダウンロードしたことを確認します。

STEP 2 | ウェブサイトに移動すると、応答ページで認証チャレンジが求められます。

> *PKI* が割り当てられた組織の証明書ではなく自己署名証明書を使用している場合、クリックして認証チャレンジに進むようユーザーに求めるセキュリティ警告が表示されます。

STEP 3 | Okta 認証情報を使って応答ページにログインします。

STEP 4 | デバイスが認証チャレンジのプッシュ通知を受信することを確認します。

STEP 5 | 認証チャレンジを済ませたユーザーがデバイスで受け取ったプッシュ通知を承諾し、ページに正しくアクセスできることを確認します。

Duo およびファイアウォール間の MFA を設定

マルチ ファクター認証（MFA）では、複数の要素を使用して企業のアセットを保護し、ネットワーク リソースへのアクセスを許可する前にユーザーの身元を確認することができます。Duo ID 管理サービスを使ってファイアウォールの認証を行う方法は複数あります：

- GlobalProtect Gateway (GlobalProtect ゲートウェイ)およびRADIUSサーバープロファイルを使う、VPN ログイン用の 2 要素認証（PAN-OS 7.0 以降でサポート）。
- Authentication Portal (認証ポータル)およびMFA server profile (MFA サーバ プロファイル)を使う API ベースの統合（Duo Authentication Proxy (Duo 認証プロキシ) や SAML IdP が不要。PAN-OS 8.0 以降でサポート）。
- オンプレミス サーバー向けの SAML 統合（PAN-OS 8.0 以降でサポート）。

ファイアウォールおよび Duo 間の SAML MFA を有効化し、ファイアウォールへの管理者アクセスを保護する方法：

- Duo アクセス ゲートウェイを使って SAML MFA 用の Duo を設定
- Duo と統合するためにファイアウォールを設定
- Duo を伴う MFA を検証

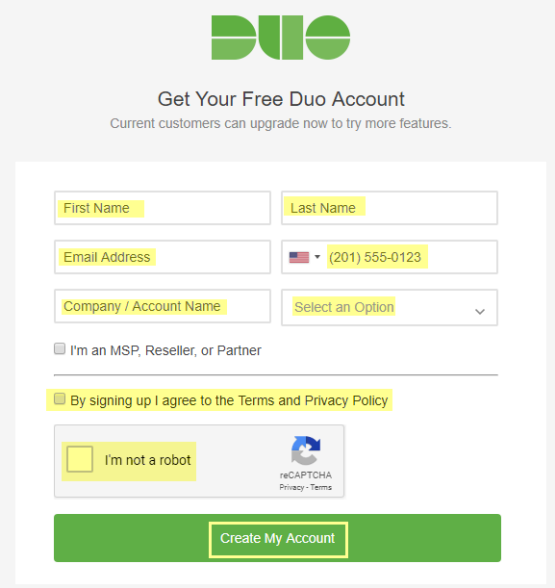
Duo アクセス ゲートウェイを使って SAML MFA 用の Duo を設定

開始する前に、DuoAccessGateway（DAG）を DMZ ゾーン内のオンプレミス サーバーにデプロイしていることを確認してください。

Duo 管理者アカウントを作成し、ユーザーがリソースにアクセスする前に認証を行うために Duo アクセス ゲートウェイを設定します。

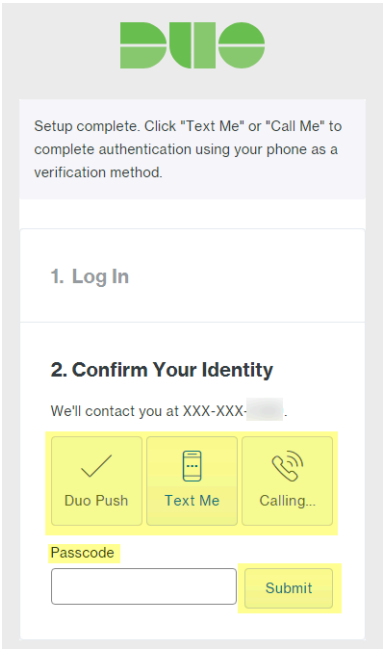
STEP 1 | Duo 管理者アカウントを作成します。

1. Duo アカウント作成ページで**First Name (名)**、**Last Name (姓)**、**Email Address (メールアドレス)**、**Cell Phone Number (電話番号)**、**Company / Account Name (企業/アカウント名)**を入力し、組織の従業員数を選択します。
2. 規約およびプライバシーポリシーに同意し、reCAPTCHA の質問に答えて**Create My Account (マイアカウントを作成)**します。



STEP 2 | Duo 管理者アカウントを確認します。

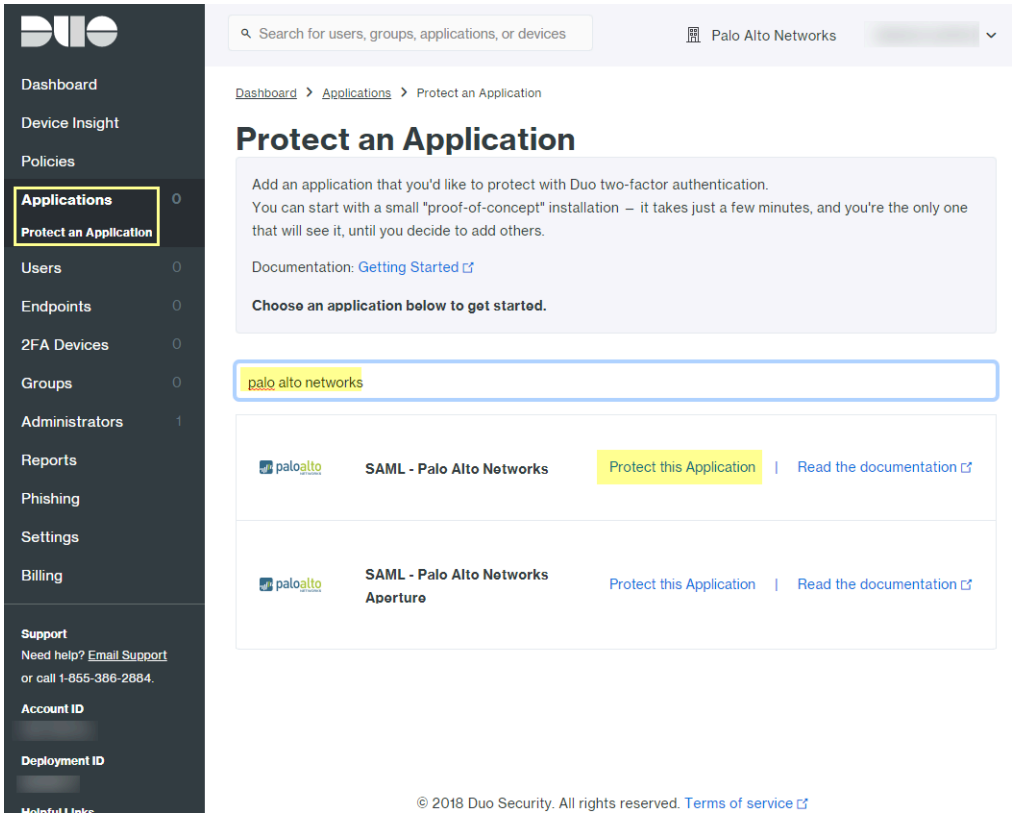
1. 本人確認方法を選択します（**Duo Push (Duo プッシュ)**、**Text Me (自分にテキスト送信)**、あるいは**Calling... (電話...)**）。
2. 受信した**Passcode (パスコード)**を入力し、**Submit (送信)**してアカウントを確認します。



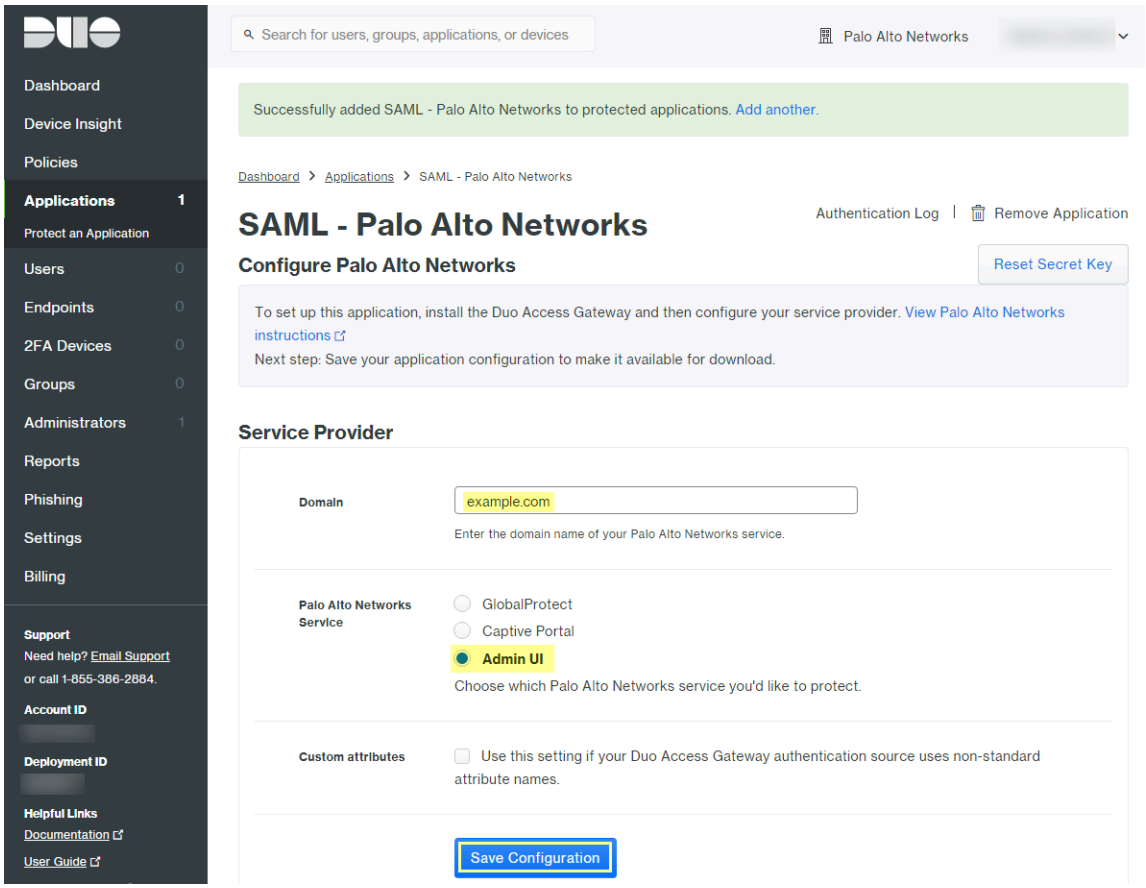
STEP 3 | SAML 用の Duo サービスを設定します。

構成を終えた後、ページ上部で構成ファイルをダウンロードします。

1. Duo 管理パネルで**Applications (アプリケーション)** > **Protect an Application (アプリケーションを保護)**を選択します。
2. **`Palo Alto Networks`**と入力してアプリケーションを検索します。
3. 結果の一覧から**SAML - Palo Alto Networks**を見つけ、**Protect this Application (このアプリケーションを保護)**します。

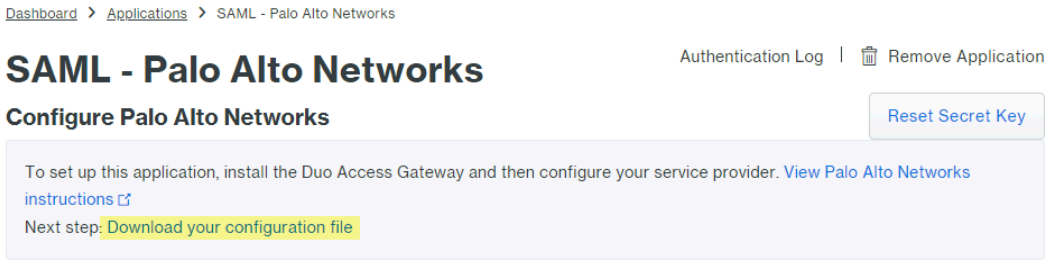


4. **Domain (ドメイン)**を入力します。
5. **Admin UI (管理 UI)**を**Palo Alto Networks Service (Palo Alto Networks サービス)**として選択します。
6. **Policy (ポリシー)**およびその他の**Settings (設定)**を行い、**Save Configuration (設定を保存)**します。



7. **Download your configuration file (**構成ファイルをダウンロード**)**します。

   ファイルをダウンロードするためのリンクは、ページの上部にあります。



STEP 4 | 構成ファイルを Duo アクセス ゲートウェイ（DAG）にアップロードします。

1. DAG 管理コンソールで**Applications (**アプリケーション**)**を選択します。
2. **Choose File (**ファイルを選択**)**をクリックし、ダウンロード済みの構成ファイルを選択してからそれを**Upload (**アップロード**)**します。
3. **Settings (**設定**)** > **Session Management (**設定管理**)**で**User agent binding (**ユーザーエージェントのバインド**)**を無効化してから**Save Settings (**設定を保存**)**します。

STEP 5 | DAG 管理コンソールで認証ソースとしてアクティブディレクトリあるいは OpenLDAP サーバーを設定し、メタデータ ファイルをダウンロードします。

1. DAG 管理コンソールにログインします。
2. **Authentication Source (認証ソース)** > **Set Active Source (アクティブ ソースのセット)**にて、**Source type (ソース タイプ)**（Active Directory (アクティブディレクトリ) あるいは OpenLDAP）および**Set Active Source (アクティブ ソースのセット)**を選択します。
3. **Configure Sources (ソースの設定)**で**Attributes (属性)**を入力します。
   - アクティブディレクトリの場合は**`mail,sAMAccountName,userPrincipalName,objectGUID`**を入力します。
   - OpenLDAP の場合は**`mail,uid`**を入力します。
   - カスタム属性はすべてリストの最後に追加し、各属性をコンマで区切ります。既存の属性は削除しないでください。
4. **Save Settings (設定を保存)**で設定を保存します。
5. **Applications (アプリケーション)** > **Metadata (メタデータ)**を選択してから**Download XML metadata (XML メタデータをダウンロード)**をクリックし、ファイアウォールにインポートすることになる XML メタデータをダウンロードします。

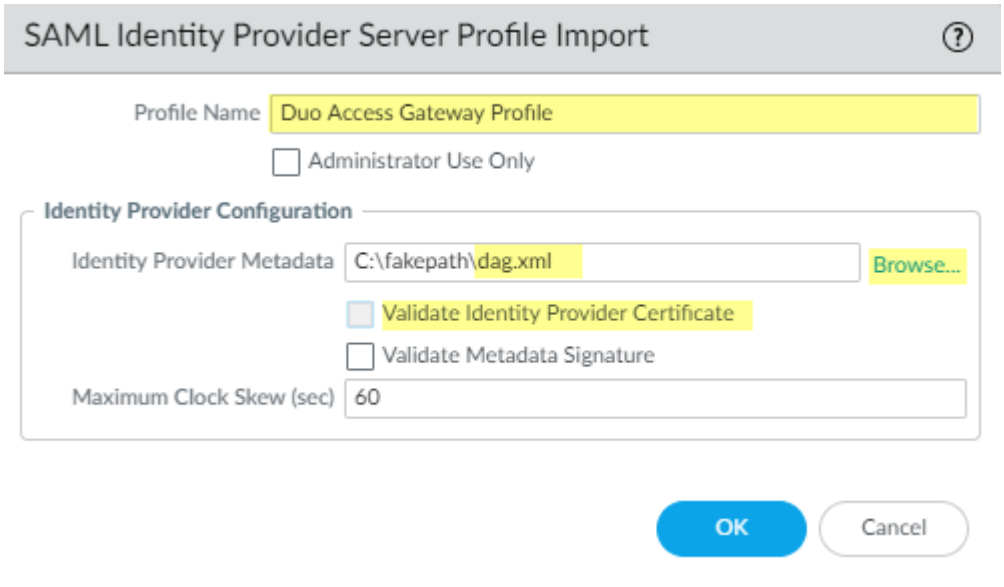
   ファイル名は dag.xml になります。ファイアウォールで Duo アカウントを認証するためのセンシティブな情報がこのファイルに含まれているため、ファイルを安全な場所に保管し、情報が漏れることがないようにしてください。

Duo と統合するためにファイアウォールを設定

STEP 1 | Duo メタデータをインポートします。

1. ファイアウォール インターフェイスにログインします。
2. ファイアウォール上で**Device (デバイス)** > **Server Profiles (サーバープロファイル)** > **SAML Identity Provider (SAML アイデンティティ プロバイダ)** > **Import (インポート)**を選択します。
3. **Profile Name (プロファイル名)**を入力します。
4. **Identity Provider Metadata** （アイデンティティ プロバイダ メタデータ）ファイル（**dag.xml**）を **Browse** （参照）します。
5. Duo Access Gateway が IdP の署名証明書として自己署名証明書を提供する場合、**Validate Identity Provider Certificate(アイデンティティ プロバイダ証明書の検**

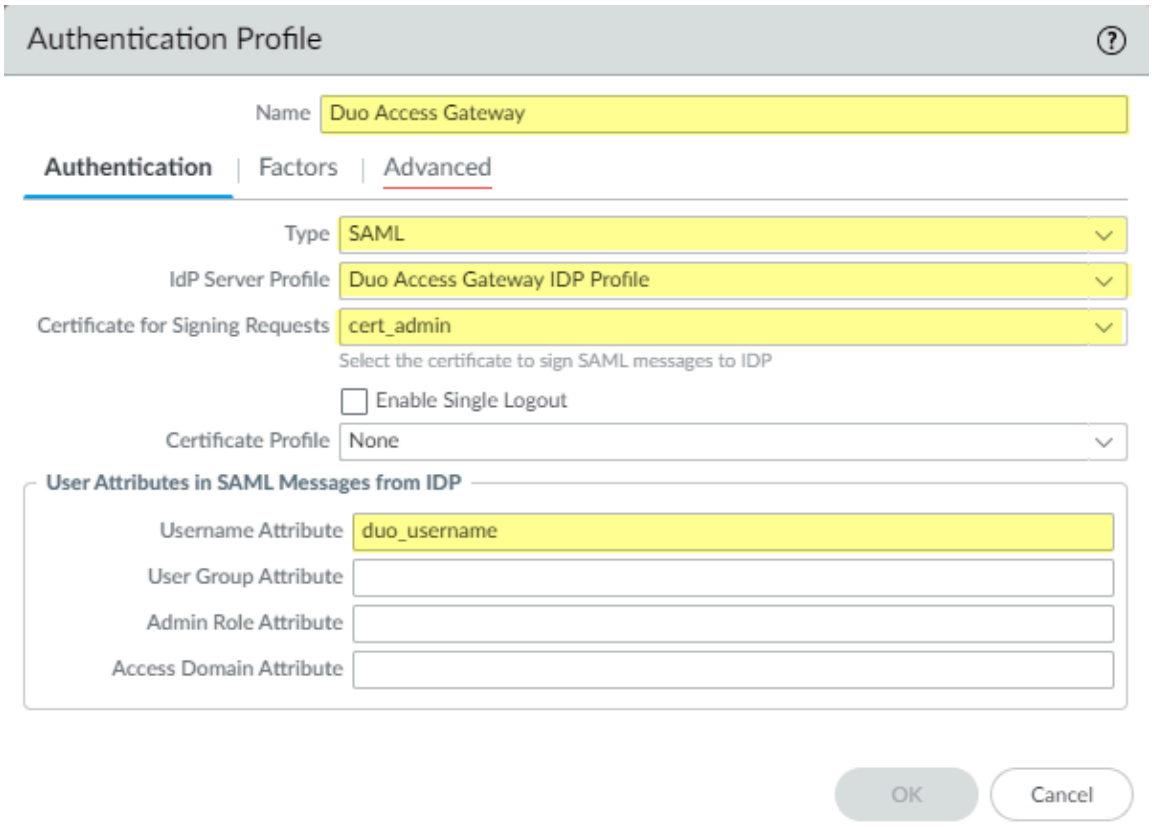
証)はできません。この場合、PAN-OS 10.2 を使用して CVE-2020-2021 への露出を軽減していることを確認してください。



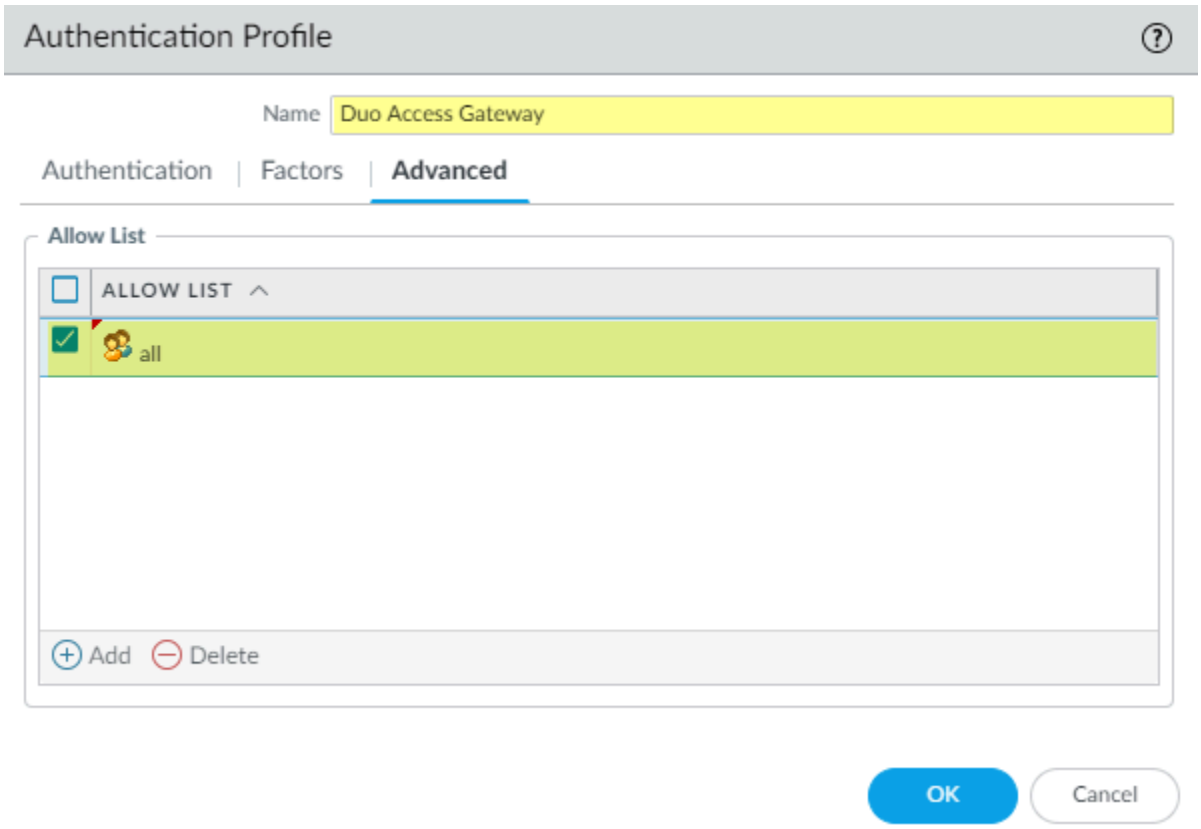
STEP 2 | 認証プロファイルを追加します。

認証プロファイルにより、Duo がアイデンティティ プロバイダとして管理者のログイン認証情報を検証できるようになります。

1. **Authentication Profile (**認証プロファイル**)**を**Add (**追加**)**します。
2. プロファイルの**Name (**名前**)**を入力します。
3. 認証**Type** （タイプ）として**SAML**を選択します。
4. **IdP Server Profile (IdP** サーバープロファイル**)**として**Duo Access Gateway Profile (Duo** アクセス ゲートウェイ プロファイル**)**を選択します。
5. **Certificate for Signing Requests (**署名要求する証明書**)**については、Duo アクセス ゲートウェイで SAML 通信に使用する証明書を選択します。
6. **`duo_username`** ユーザー名属性 として を入力します。

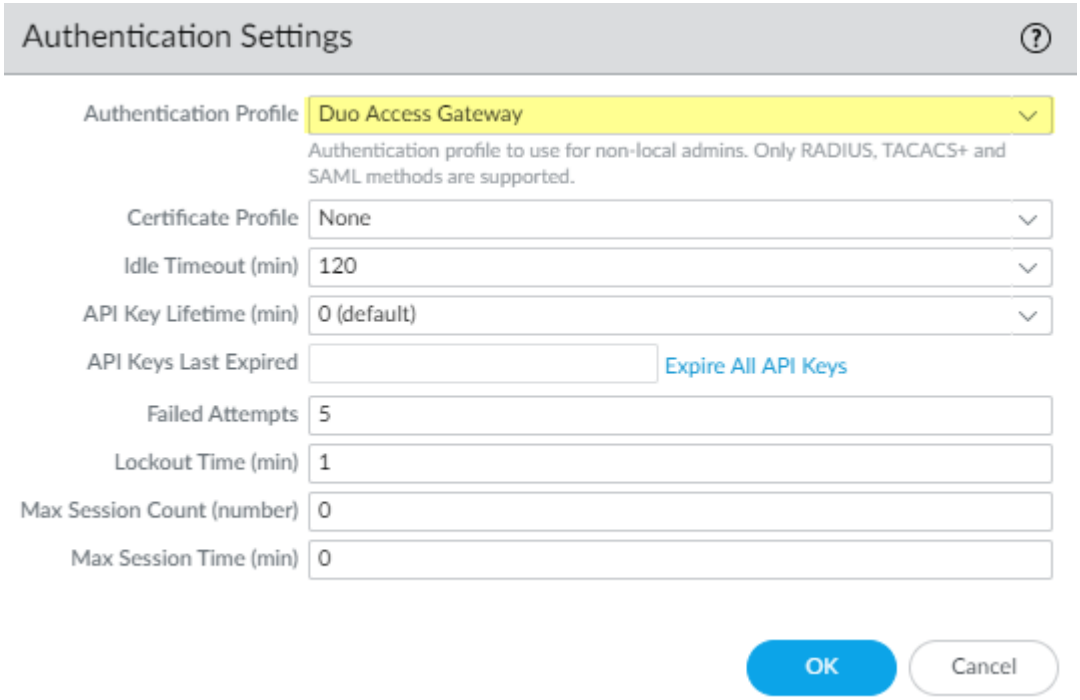


7. **Advanced (**詳細**)**を選択して許可リストを**Add (**追加**)**します。
8. **all (**すべて**)**を選択してから**OK**をクリックします。
9. 変更を **Commit**（コミット）します。



STEP 3 | ファイアウォールが Duo を伴う SAML 認証に使用する認証設定を指定します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して Authentication Settings (認証設定) を編集します。
2. **Duo Access Gateway (Duo アクセス ゲートウェイ)**を**Authentication Profile (認証プロファイル)**として選択してから**OK**をクリックします。



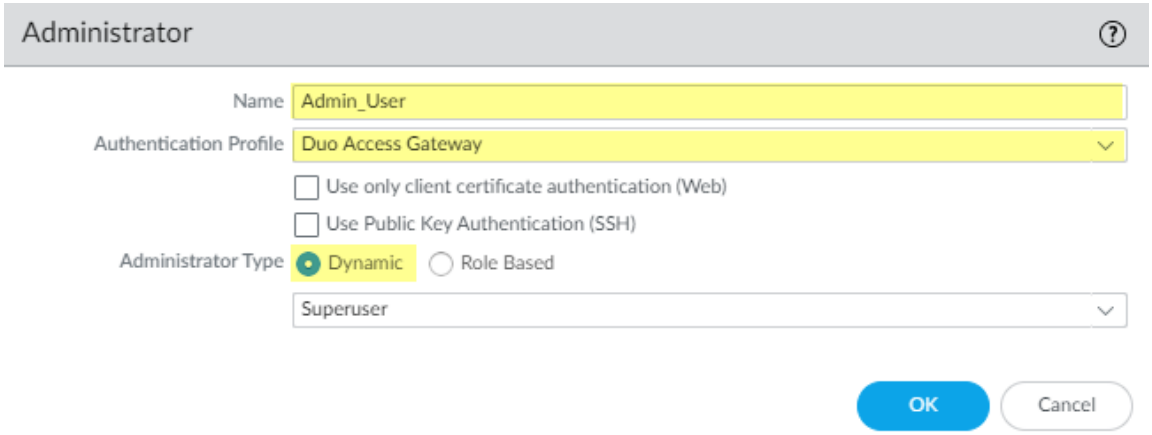
3. 変更をコミットします。

STEP 4 | Duo を使用してファイアウォールへの認証を行う管理者アカウントを追加します。

1. **Device (デバイス)** > **Administrators (管理者)** を選択してアカウントを **Add (追加)** します。
2. ユーザーの**Name** [名前]を入力します。
3. **Duo Access Gateway (Duo アクセス ゲートウェイ)**を**Authentication Profile (認証プロファイル)**として選択します。
4. **Administrator Type (管理者タイプ)**を選択してから**OK**をクリックします。

   ユーザーに対してカスタムロールを使用する場合は**Role Based (ロールベース)**を選択します。そうでない場合は**Dynamic (動的)**を選択します。管理者に Duno を伴う SSO を使

用したログインを要求するには、現在のすべての管理者に認証プロファイルを割り当てます。



Duo を伴う MFA を検証

STEP 1 | ファイアウォール上の Web インターフェイスにログインします。

STEP 2 | **Use Single Sign-on** （シングルサインオンの使用）および**Continue (続行)**を選択します。

STEP 3 | Duo アクセス ゲートウェイのログインページでログイン認証情報を入力します。

STEP 4 | 認証方法（プッシュ通知、電話、あるいはパスコードの入力）を選択します。

認証が成功したら、ファイアウォールの Web インターフェイスにリダイレクトされます。

SAML 認証の設定

SAML シングル サインオン（SSO）およびシングル ログアウト（SLO）を設定するには、ファイアウォールおよび IdP を相互に登録し、互いの通信を有効化する必要があります。IdP が登録情報を含むメタデータ ファイルを提供している場合、それをファイアウォールにインポートして IdP を登録し、IdP サーバープロファイルを作成することができます。サーバー プロファイルにより、IdP に接続する方法が定義され、IdP が SAML メッセージに署名するために使用する証明書が指定されます。また、証明書を使用してファイアウォールに SAML メッセージに署名させることもできます。ファイアウォールおよび IdP 間の通信を保護するには、証明書を使用する必要があります。

Palo Alto Networks は、すべての SAML トランザクションの機密性を確保するために、暗号化された SAML アサーションなどのような他のアプローチではなく、HTTPS を必須にしています。Palo Alto Networks は、SAML トランザクションで処理されるすべてのメッセージの整合性を保つために、暗号デジタル証明書が必要です。

次の各作業は、エンドユーザーおよびファイアウォール管理者用に SAML 認証を設定する方法を示しています。また、Panorama 管理者用に SAML 認証を設定することもできます。

SSO は、管理者、*GlobalProtect*、および認証ポータルのエンド ユーザーが使用できます。*SLO* は、管理者、および *GlobalProtect* のエンドユーザーが利用できますが、認証ポータルのエンドユーザーは利用できません。

管理者は *SAML* を使用してファイアウォールの *Web* インターフェイスとの認証を行うことができますが、*CLI* との認証を行うことはできません。

STEP 1 | IdP およびファイアウォールが SAML メッセージに署名するために使用する証明書を取得します。

証明書で鍵の用途の属性が指定されない場合、デフォルトではメッセージへの署名を含めてすべての用途が許可されます。この場合、任意の方法で証明書の取得を行えます。

証明書でキー利用属性が指定されている場合、属性の 1 つはデジタル署名です。デジタル署名はファイアウォールで生成する証明書では使用できません。この場合、証明書をインポートする必要があります。

- ファイアウォールが **SAML** メッセージに署名するために使用する証明書—企業用の証明書認証局（CA）あるいはサードパーティ CA の証明書をインポートします。
- **IdP** が **SAML** メッセージに署名するために使用する証明書（すべてのデプロイメントに必要）—IdP から証明書が含まれるメタデータ ファイルをインポートします（次のステップを参照）。IdP 証明書は、

  公開鍵アルゴリズム — RSA (1,024 ビット以上) および ECDSA (すべてのサイズ) のアルゴリズムに制限されます。FIPS/CC モードの firewall は、RSA (2,048 ビット以上) および ECDSA (すべてのサイズ) をサポートします。

  署名アルゴリズム — SHA1、SHA256、SHA384、および SHA512。FIPS/CC モードの firewall は、SHA256、SHA384、および SHA512 をサポートします。

STEP 2 | SAML IdP サーバー プロファイルを追加します。

サーバープロファイルは IdP をファイアウォールに登録し、接続方法を定義します。

この例では、IdP から SAML メタデータ ファイルをインポートし、ファイアウォールが自動的にサーバープロファイルを作成し、接続、登録、IdP 情報の入力を自動で行えるようにします。

IdP がメタデータ ファイルを提供しない場合、***Device*** *(*デバイス*)* > ***Server Profiles*** *(*サーバープロファイル*)* > ***SAML Identity Provider*** *(****SAML*** アイデンティティ プロバイダ*)* を選択し、サーバープロファイルを ***Add*** *(*追加*)* し、情報を手入力します（各値については *IdP* 管理者にご確認ください）。

1. SAML メタデータ ファイルを IdP から、メタデータをファイアウォールにアップロードできるクライアントシステムにエクスポートします。

   ファイルで指定された証明書は、前のステップで示した要件を満たす必要があります。ファイルのエクスポート手順については、IdP のドキュメントを参照してください。
2. Panorama™ 上で**Device**（デバイス） > **Server Profiles**（サーバプロファイル） > **SAML Identity Provider**（**SAML** アイデンティティ プロバイダ）または**Panorama** > **Server Profiles**（サーバプロファイル） > **SAML Identity Provider**（**SAML** アイデンティティ プロバイダ）を選択し、メタデータファイルをファイアウォールに**Import**（インポート）します。
3. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
4. **Identity Provider Metadata**（アイデンティティ プロバイダ メタデータ）ファイルを **Browse**（参照）します。
5. **Validate Identity Provider Certificate**（アイデンティティ プロバイダ証明書の検証）（デフォルト）を選択して、信頼のチェーンを検証し、オプションで IdP 証明書の失効ステータスを検証します。

   このオプションを有効にするために、認証局（CA）が IdP の署名証明書を発行する必要があります。IdP の署名証明書を発行した CA を含む証明書プロファイルを作成する必要があります。認証プロファイルで、IdP 証明書を検証するための SAML サーバ プロファイルおよび証明書プロファイルを選択します。

   IdP 署名証明書が自己署名証明書である場合、信頼チェーンはありません。 その結果、このオプションを有効にすることはできません。ファイアウォールは **Validate Identity Provider Certificate** *(*アイデンティティ プロバイダ証明書の検証*)* オプションを有効にするかどうかに関係なく、設定するアイデンティティプロバイダ証明書に対して SAML 応答またはアサーションのシグネチャを常に検証します。IdP が自己署名証明書を提供する場合は、PAN-OS 10.2 を使用して CVE-2020-2021への露出を軽減していることを確認してください。

   証明書を検証して、侵害されていないことを確認し、かつ、セキュリティを改善します。
6. ファイアウォールが IdP メッセージを検証する際に許容される、IdP およびファイアウォールのシステム時間の差（秒単位）として、**Maximum Clock Skew** *(*最大クロック

スキュー)を入力します（デフォルトは 60、範囲は 1～900）。誤差がこの値を超えると、認証が失敗します。

7. **OK** をクリックしてサーバー プロファイルを保存します。
8. サーバー プロファイルの Name（名前）をクリックしてプロファイル設定を表示します。インポートした情報が正しいことを確認し、必要に応じて編集します。
9. IdP メタデータをインポートする場合でも、IdP 情報を手動で入力する場合でも、SAML アイデンティティ プロバイダの署名証明書がサーバープロファイルの **Identity Provider Certificate**（アイデンティティ プロバイダ証明書）であり、IdP が署名済みの SAML 応答、アサーション、または 両方を送信することを常に保証します。

STEP 3 | 認証プロファイルを設定します。

このプロファイルは、一連のユーザーに対して共通の認証設定を定義します。

1. **Device (デバイス)** > **Authentication Profile (認証プロファイル)** を選択してプロファイルを **Add (追加)** します。
2. プロファイルを識別する **Name**（名前）を入力します。
3. **Type**（タイプ）を **SAML** に設定します。
4. 設定した **IdP Server Profile**（**IdP** サーバー プロファイル）を選択します。
5. **Certificate for Signing Requests**（署名要求の証明書）を選択します。

   ファイアウォールはこの証明書を使用し、IdP に送信するメッセージに署名します。エンタープライズ CA が生成した証明書をインポートするか、ファイアウォールあるいは Panorama で生成されたルート CA を使って証明書を生成することができます。
6. （任意）**Enable Single Logout**（シングル ログアウトの有効化）を行います（デフォルトでは無効）。
7. **Identity Provider Certificate (アイデンティティ プロバイダの証明書)** を検証するためにファイアウォールが使用する **Certificate Profile (証明書プロファイル)** を選択します。
8. IdP メッセージがユーザーを識別するために使用する **Username Attribute (ユーザー名属性)** を入力します（デフォルトは **`username`**）。

   ユーザーの動的管理者ロールを事前定義する場合、小文字を使用してロールを指定します *(例えば、**`SuperReader`*** ではなく、***`superreader`*** と入力します。*)IdP ID* ストアで管理者の認証を管理する場合は、***Admin Role Attribute (***管理者ロール属性*)*** および ***Access Domain Attribute (***アクセスドメイン属性*)*** も指定します。
9. **Advanced (詳細)** を選択し、この認証プロファイルで認証できるユーザーとユーザーグループを **Add (追加)** します。
10. **OK** をクリックして認証プロファイルを保存します。

STEP 4 | 認証が必要なファイアウォール アプリケーションに認証プロファイルを割り当てます。

1. 認証プロファイルを次の項目に割り当てます。
   - ファイアウォールのローカルで管理する管理者アカウント。この例では、作業の後半で SAML 設定を検証する前にファイアウォール管理者アカウントの設定を行います。
   - IdP ID ストアで外部的に管理する管理者アカウント。**Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)**を選択して Authentication Settings (認証設定) を編集し、設定した **Authentication Profile (認証プロファイル)** を選択します。
   - エンドユーザーが認証ポータルを通じてアクセスするサービスとアプリケーションを保護する、認証ポリシー ルール。認証ポリシーの設定を参照してください。
   - エンドユーザーがアクセスする GlobalProtect ポータルおよびゲートウェイ。
2. 変更を **Commit (コミット)**します。

   ファイアウォールは、SAML IdP サーバープロファイルに割り当てた **Identity Provider Certificate (アイデンティティ プロバイダ証明書)** を検証します。

STEP 5 | SAML メタデータ ファイルを作成し、IdP 上でファイアウォール アプリケーション (管理アクセス、認証ポータル、あるいは GlobalProtect) を登録します。

1. **Device (デバイス)** > **Authentication Profile (認証プロファイル)** を選択し、設定した認証プロファイルの Authentication (認証) 列で **Metadata (メタデータ)** をクリックします。
2. **Service (サービス)** ドロップダウンで、登録したいアプリケーションを選択します。
   - **management** （管理）（デフォルト） – Web インターフェイスへの管理者アクセス。
   - **authentication-portal** （認証ポータル） – 認証ポータルを介した、サービスおよびアプリケーションに対する、エンド ユーザーのアクセス。
   - **global-protect** – GlobalProtect を介したサービスおよびアプリケーションへのエンドユーザー アクセス。
3. （認証ポータルまたは GlobalProtect のみ）**Vsysname Combo (仮想システム名コンボ)** については、認証ポータル設定もしくは GlobalProtectポータルが定義されている、virtual system (仮想システム - vsys) を選択します。
4. 登録するアプリケーションに基づいて、インターフェイス、IP アドレス、あるいはホスト名を入力します。
   - **management (管理)**–**Management Choice (管理 オプション)** については **Interface (インターフェイス)**（デフォルト）を選択し、さらに Web インターフェイスへの管理アクセスを行うために有効なインターフェイスを選択します。デフォルトでは、MGT インターフェイスの IP アドレスが選択されています。
   - **authentication-portal (認証ポータル)**–**IP Hostname (ホスト名)** については、**Redirect Host (リダイレクト ホスト)** の IPアドレスあるいはホスト名を入力します（**Device (デバイス)** > **User Identification (ユーザー ID)** > **Authentication Portal Settings (認証ポータルの設定)** を参照）。

- **global-protect**—**IP Hostname (**ホスト名**)** については、GlobalProtect ポータルあるいはゲートウェイのホスト名あるいは IP アドレスを入力します。

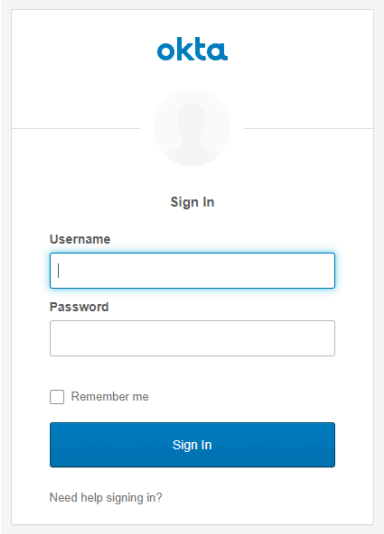
5. **OK** をクリックして、メタデータ ファイルをクライアント システムに保存します。
6. メタデータ ファイルを IdP サーバーにインポートしてファイアウォール アプリケーションを登録します。手順は、IdP のドキュメントを参照してください。

STEP 6 | ユーザーが SAML SSO を使用して認証できることを確認します。

例えば、ローカル管理者アカウントを使用し、Web インターフェイスへのアクセスで SAML を使用できることを確認できます。

1. ファイアウォールの Web インターフェイスの URL に移動します。
2. **Use Single Sign-On**（シングル サインオンの使用）をクリックします。
3. 管理者のユーザー名を入力します。
4. **Continue**（続行） をクリックします。

   認証を行うためにファイアウォールによって IdP にリダイレクトされ、ログインページが表示されます。以下に例を示します。



5. SSO ユーザー名とパスワードを使用してログインします。

   IdP 上で認証に成功したら、ファイアウォールに再びリダイレクトされ、Web インターフェイスが表示されます。
6. ファイアウォール管理者アカウントを使用して別の SSO アプリケーションへのアクセスをリクエストします。

   正常にアクセスできれば、SAML SSO の認証に成功したことになります。

Kerberos シングル サインオンの設定

Palo Alto Networks のファイアウォールおよびPanoramaでは、Web インターフェースにアクセスする管理者、および認証ポータルにアクセスするエンド ユーザーの認証にKerberos V5 Single Sign-On (シングル サインオン - SSO) がサポートされています。Kerberos SSO が有効な場合、ユーザーはネットワークに初めてアクセスした際だけログインを求められます（Microsoft Windows へのログインなど）。ユーザーは初回のログイン後、SSO セッションの期限が切れるまで再度ログインすることなく、ネットワークのブラウザ ベースのどのサービスにも（ファイアウォールの Web インターフェイスなど）アクセスできます。

STEP 1 | Kerberos キータブを作成します。

キータブは、ファイアウォールのプリンシパル名およびパスワードを含み、SSO プロセスで必要になるファイルです。認証プロファイルとシーケンス で Kerberos を構成すると、ファイアウォールは最初に Kerberos SSO ホスト名を確認します。ホスト名を指定すると、ファイアウォールはホスト名に一致するサービス プリンシパル名をキータブで検索し、そのキータブのみを復号化に使用します。ホスト名を指定しない場合、ファイアウォールは、Kerberos を使用して正常に認証できるまで、認証シーケンスの各キータブを試行します。

ファイアウォールに送信されたリクエストに *Kerberos SSO* ホスト名が含まれている場合、ホスト名はキータブのサービス プリンシパル名と一致する必要があります。そうしないと、*Kerberos* 認証要求は送信されません。

1. Active Directory サーバーにログインし、コマンド プロンプトを開きます。
2. 次のコマンドを入力して、GlobalProtect または Authentication Portal のサービス プリンシパル名 (SPN) を登録します (*<portal_fqdn>* および *<service_account_username>* は変数です)。

   setspn -s HTTP/*<portal_fqdn>* *<service_account_username>*
3. ファイアウォール用の Kerberos アカウントを作成します。各ステップについては、Kerberos のドキュメントを参照してください。
4. KDC にログインして、コマンド プロンプトを開きます。

5. 次のコマンドを入力します。ここで、*<portal_fqdn>*、*<kerberos_realm>*、*<netbios_name>*、*<service_account_username>*、*<password>*、および *<algorithm>* は変数です。

```
ktpass /princ HTTP <portal_fqdn>@<kerberos_realm> /mapuser
<netbios_name>\<service_account_username> /pass <password>/out
<filename>.keytab /ptype KRB5_NT_PRINCIPAL /crypto <algorithm>
```

<kerberos_realm> の値はすべて大文字にする必要があります (たとえば、***ad1.example.com*** ではなく ***AD1.EXAMPLE.COM*** と入力します)。

ファイアウォールがFIPS/CCモードの場合、アルゴリズムは***aes128-cts-hmac-sha1-96***または***aes256-cts-hmac-sha1-96***に設定されている必要があります。それ以外の場合、*des3-cbc-sha1* または *arcfour-hmac* も使用できます。*Advanced Encryption Standard* （*AES*）アルゴリズムを使用する場合は、*KDC* の機能レベルが *Windows* サーバー *2012* 以降でなければならず、ファイアウォール アカウントの *AES* 暗号化を有効にする必要があります。

キータブのアルゴリズムは、*TGS* がクライアントに発行するサービス チケットのアルゴリズムと一致している必要があります。サービス チケットで使用されるアルゴリズムは、*Kerberos* 管理者が決定します。

STEP 2 | 認証プロファイルおよびシーケンスの設定を行い、Kerberos、および一連のユーザーに対して共通であるその他のオプションを設定します。

- **Kerberos Realm** [Kerberos レルム]（レルムが大文字の場合を除き、通常はユーザーの DNS ドメイン）を入力します。
- ファイアウォール用に作成した **Kerberos Keytab (Kerberos** キータブ**)** を **Import (**インポート**)** します。

STEP 3 | 認証が必要なファイアウォール アプリケーションに認証プロファイルを割り当てます。

- Web インターフェイスへの管理者アクセス—ファイアウォール管理者アカウントの設定を行い、設定した認証プロファイルを割り当てます。
- 認証プロファイルによるサービスおよびアプリケーションへのアクセス—設定した認証プロファイルを認証適用オブジェクトに割り当てます。オブジェクトを設定する際、**Authentication Method (**認証方法**)** を **browser-challenge** に設定します。オブジェクトを認証ポリシールールに割り当てます。エンドユーザーの認証を設定する際の完全な流れについては、認証ポリシーの設定を参照してください。

Kerberos サーバー認証の設定

Kerberos を使用し、アクティブディレクトリ ドメイン コントローラあるいは Kerberos V5 と互換性のある認証サーバーに対し、エンドユーザーおよびファイアウォールあるいは Panorama 管理者をネイティブに認証することができます。この認証方法はインタラクティブであり、ユーザーにユーザー名およびパスワードを入力するよう求めます。

認証に *Kerberos* サーバーを使用する場合は、*IPv4* アドレスを使用してサーバーにアクセス可能でなければなりません。*IPv6* アドレスはサポートされません。

STEP 1 | Kerberosサーバー プロファイルを追加します。

このプロファイルは、ファイアウォールが Kerberos サーバーに接続する方法を定義します。

1. Panorama™ で **Device**（デバイス） > **Server Profiles**（サーバ プロファイル） > **Kerberos** または **Panorama** > **Server Profiles**（サーバ プロファイル） > **Kerberos**を選択し、サーバープロファイルを**Add**（追加）します。
2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
3. 各サーバーを **Add (追加)** し、**Name (名前)**（サーバーを識別するもの）、**Kerberos Server (Kerberos サーバー)** の IPv4 アドレスあるいは FQDN、さらに任意でサーバーとの通信に使用する **Port (ポート)** 番号（デフォルトは 88）を指定します。

   FQDN アドレス オブジェクトを使用してサーバーを識別し、後でアドレスを変更する場合は、変更をコミットし、新しいサーバー アドレスを有効にする必要があります。
4. **OK** をクリックして、プロファイルに対する変更を保存します。

STEP 2 | サーバー プロファイルを割り当てて認証プロファイルおよびシーケンスの設定を行います。

認証プロファイルは、一連のユーザーに対して共通の認証設定を定義します。

STEP 3 | 認証が必要なファイアウォール アプリケーションに認証プロファイルを割り当てます。

- Web インターフェイスへの管理者アクセス—ファイアウォール管理者アカウントの設定を行い、設定した認証プロファイルを割り当てます。
- 認証プロファイルによるサービスおよびアプリケーションへのアクセス—設定した認証プロファイルを認証適用オブジェクトに割り当て、そのオブジェクトを認証ポリシールールに割り当てます。エンドユーザーの認証を設定する際の完全な流れについては、認証ポリシーの設定を参照してください。

STEP 4 | 認証サーバー接続のテストを行い、ファイアウォールがユーザーを認証できることを確認します。

TACACS+ 認証の設定

エンドユーザーおよびファイアウォールあるいは Panorama 管理者用に TACACS+ 認証を設定できます。また、TACACS+ サーバーを使用し、ベンダー固有属性（VSA）を定義することで、管理者の認証を管理（ロールおよびアクセスドメインの割り当て）することができます。すべてのユーザーについて、ファイアウォールあるいは Panorama がサーバーに接続する際の方法を定義する TACACS+ サーバープロファイルを設定する必要があります。次に、共通の認証設定が必要な一連のユーザー毎に、 サーバープロファイルを認証プロファイルを割り当てます。認証プロファイルに対して何を行うかは、どのユーザーが TACACS+ サーバー認証を行うかによって決まります。

- エンドユーザー–認証プロファイルを認証適用オブジェクトに割り当て、そのオブジェクトを認証ポリシールールに割り当てます。作業の流れについては認証ポリシーの設定を参照してください。
- ファイアウォールあるいは **Panorama** のローカルで認証が管理される管理者アカウント–認証プロファイルをファイアウォール管理者あるいはPanorama 管理者アカウントに割り当てます。
- **TACACS+** サーバー上で認証が管理される管理者アカウント–次の各作業は、ファイアウォール管理者用の TACACS+ 本人確認および認証を設定する方法を示しています。Panorama 管理者の場合はPanorama 管理者用の TACACS+ 認証の設定を参照してください。

STEP 1 | TACACS+サーバー プロファイルを追加します。

このプロファイルは、ファイアウォールが TACACS+ サーバーに接続する方法を定義します。

1. Panorama™ で **Device**（デバイス） > **Server Profiles**（サーバ プロファイル） > **TACACS+** または **Panorama** > **Server Profiles**（サーバ プロファイル） > **TACACS+** を選択し、プロファイルを**Add**（追加）します。
2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
3. （任意）**Administrator Use Only**（管理者のみ使用）を選択し、管理者へのアクセスを制限します。
4. 認証要求がタイムアウトするまでの**Timeout (**タイムアウト**)** 時間を秒単位で入力します（デフォルトは 3、範囲は1～ 20）。
5. ファイアウォールが TACACS+ サーバーへの認証に使用する **Authentication Protocol (**認証プロトコル**)**（デフォルトは **CHAP**）を選択します。

   TACACS+ サーバーがサポートする場合は ***CHAP*** を選択します。このプロトコルは ***PAP*** よりも安全です。
6. 各 TACACS+ サーバーを **Add**（追加）して、以下を入力します。
   - サーバーの識別に使用する **Name**（名前）
   - **TACACS+ Server**（**TACACS+** サーバー） の IP アドレス あるいは FQDN。FQDN アドレス オブジェクトを使用してサーバーを識別し、後でアドレスを変更する場合は、変更をコミットし、新しいサーバー アドレスを有効にする必要があります。
   - **Secret**（シークレット）/**Confirm Secret**（再入力 シークレット）（ユーザー名とパスワードを暗号化するための鍵）
   - 認証要求用のサーバー **Port**（ポート）（デフォルトは49）
7. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 2 | TACACS+ サーバー プロファイルを認証プロファイルに割り当てます。

認証プロファイルは、一連のユーザーに対して共通の認証設定を定義します。

1. **Device (デバイス)** > **Authentication Profile (認証プロファイル)** を選択してプロファイルを **Add (追加)** します。
2. プロファイルを識別する **Name**（名前）を入力します。
3. **Type**（タイプ）を **TACACS+** に設定します。
4. 設定した **Server Profile**（サーバー プロファイル）を選択します。
5. **Retrieve user group from TACACS+**（**TACACS+** からユーザー グループを取得）を選択して、TACACS+ サーバーで定義された VSA からユーザー グループ情報を収集します。

   ファイアウォールは、認証プロファイルの許可リストで指定したグループに対し、グループ情報をマッチさせます。
6. **Advanced (詳細)** を選択し、Allow List (許可リスト) 内で、この認証プロファイルで認証できるユーザーとグループを **Add (追加)** します。
7. **OK** をクリックして認証プロファイルを保存します。

STEP 3 | すべての管理者に対して認証プロファイルを使用するようにファイアウォールを設定します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して Authentication Settings (認証設定) を編集します。
2. 設定した **Authentication Profile**（認証プロファイル）を選択し、**OK** をクリックします。

STEP 4 | 管理者用に、認証設定を定義するアクセスドメインおよびロールを設定します。

すでに TACACS+ サーバー上で TACACS+ VSA を定義済みである場合は、ファイアウォール上でロールおよびアクセスドメイン用に指定する名前が、VSA の値と一致しなければなりません。

1. 管理ユーザーが定義済みの（動的）ロールではなくカスタムロールを使用する場合は、管理者ロール プロファイルの設定を行います。
2. ファイアウォールが複数の仮想システムを持っている場合に、アクセスドメインを設定します—**Device (デバイス)** > **Access Domain (アクセスドメイン)** を選択し、アクセスドメインを **Add (追加)** し、そのアクセスドメインを識別する **Name (名前)** を入力し、管理者がアクセスする各仮想システムを **Add (追加)** し、**OK** をクリックします。

STEP 5 | 変更を **Commit (コミット)** し、ファイアウォール上でそれらを有効化します。

STEP 6 | 管理者を認証して承認するように TACACS+ サーバーを設定します。

これらの手順を実行するには、TACACS+ サーバーのドキュメントで各手順を参照してください。

1. ファイアウォールの IP アドレスまたはホスト名を TACACS+ クライアントとして追加します。
2. 管理者アカウントを追加します。

   Authentication Protocol（認証プロトコル）として ***CHAP*** を選択した場合、逆暗号化されたパスワードを使用してアカウントを定義する必要があります。定義していないと *CHAP* 認証に失敗します。
3. 各管理者のロール、アクセス ドメイン、ユーザー グループ用に TACACS+ VSA を定義します。

   ユーザーの動的管理者ロールを事前定義する場合、小文字を使用してロールを指定します *(*例えば、***SuperUser*** ではなく、***superuser*** と入力します。*)*

STEP 7 | TACACS+ サーバーが管理者の認証および承認を実行することを確認します。

1. TACACS+ サーバーに追加した管理者アカウントを使用してファイアウォールの Web インターフェイスにログインします。
2. 管理者に関連付けたロールに許可された Web インターフェイス ページにしかアクセスできないことを確認します。
3. **Monitor**（監視）タブ、**Policies**（ポリシー）タブ、**Objects**（オブジェクト）タブで、管理者に関連付けたアクセス ドメインに許可された仮想システムにしかアクセスできないことを確認します。

RADIUS 認証の設定

エンドユーザーおよびファイアウォールあるいは Panorama 管理者用に RADIUS 認証を設定できます。管理者の場合、RADIUS を使用してベンダー固有属性（VSA）を定義することで、認証を管理（ロールおよびアクセスドメインの割り当て）することができます。また、RADIUS を使用して管理者およびエンドユーザー用にマルチ ファクター認証（MFA）を実装することもできます。RADIUS 認証を有効化するには、ファイアウォールあるいは Panorama がサーバーに接続する際の方法を定義する RADIUS サーバープロファイルを設定する必要があります (以下のステップ 1 を参照)。次に、共通の認証設定が必要な一連のユーザー毎に、サーバープロファイルを認証プロファイルを割り当てます (以下のステップ 5 を参照)。認証プロファイルに対して何を行うかは、どのユーザーが RADIUS サーバー認証を行うかによって決まります。

- エンドユーザー–認証プロファイルを認証適用オブジェクトに割り当て、そのオブジェクトを認証ポリシールールに割り当てます。作業の流れについては認証ポリシーの設定を参照してください。

  また、認証プロファイルを *GlobalProtect* ポータルあるいはゲートウェイに割り当てることで、クライアントシステムを設定して RADIUS ベンダー固有属性（VSA）を *RADIUS* サーバーに送信することもできます。*RADIUS* 管理者はこれらの *VSA* に基づき管理タスクを実行します。

- ファイアウォールあるいは **Panorama** のローカルで認証が管理される管理者アカウント–認証プロファイルをファイアウォール管理者あるいはPanorama 管理者アカウントに割り当てます。
- **RADIUS** サーバー上で認証が管理される管理者アカウント–次の各作業は、ファイアウォール管理者用の RADIUS 本人確認および認証を設定する方法を示しています。Panorama 管理者の場合はPanorama 管理者用の RADIUS 認証の設定を参照してください。

STEP 1 | RADIUS サーバー プロファイルを追加します。

このプロファイルは、ファイアウォールが RADIUS サーバーに接続する方法を定義します。

1. Panorama™ で **Device**（デバイス） > **Server Profiles**（サーバ プロファイル） > **RADIUS** または **Panorama** > **Server Profiles**（サーバ プロファイル） > **RADIUS** を選択し、プロファイルを**Add**（追加）します。
2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
3. （任意）**Administrator Use Only**（管理者のみ使用）を選択し、管理者へのアクセスを制限します。
4. 認証要求がタイムアウトするまでの**Timeout (**タイムアウト**)** 時間を秒単位で入力します（デフォルトは 3、範囲は1～ 120）。

   サーバー プロファイルを使用してファイアウォールを *MFA* サービスと統合する場合、この時間を入力して、認証を行うのに十分な時間をユーザーに与えます。たとえば、*MFA* サービスがワンタイム パスワード（*OTP*）を要求する場合、ユーザーには自分のエンドポイント デバイスで *OTP* を確認し、*MFA* ログイン ページに *OTP* を入力するまでの時間が必要です。
5. **Retries**（再試行）を入力してください。
6. ファイアウォールが RADIUS サーバーへの認証に使用する **Authentication Protocol (**認証プロトコル**)**（デフォルトは **PEAP-MSCHAPv2**）を選択します。

   マルチ ファクター認証（MFA）環境でユーザーを認証するために使用する要素に応じて、適切な認証プロトコルを選択します。

   - ユーザー名、パスワード、およびプッシュ **(**自動的に **triggered out-of-band** 要求**)**:すべての認証プロトコルでサポートされています
   - プッシュ、パスワード、トークン、および **PIN (**パスワード、トークン、または **PIN** が一緒に提供されている場合**)**:PAP、GTC を使用した PEAP、PAP
   - ユーザー名、パスワード、トークン、および **PIN**、およびチャレンジレスポンス **(**パスワード、トークン、または **PIN** が一緒に提供されている場合**)** でサポートされています:PAP および PEAP と GTC でサポートされています

   EAP 認証方式 (PEAP-MSCHAPv2、GTC 付き PEAP、または PAP 付き EAP-TTLS) を選択した場合は、RADIUS サーバーが Transport Layer Security (TLS) 1.1 以降をサポートしていること、および RADIUS サーバーのルート認証局および中間認証局 (CA) が RADIUS サーバー プロファイルに関連付けられた証明書 profile に含まれていることを確認して

ください。EAP 方式を選択し、正しく設定された証明書プロファイルを RADIUS プロファイルに関連付けることができない場合、認証は失敗します。

7. 各 RADIUS サーバーを **Add**（追加）して、以下を入力します。
   - サーバーの識別に使用する **Name**（名前）
   - **RADIUS Server**（**RADIUS** サーバー） の IP アドレス あるいは FQDN。FQDN を使用してサーバーを識別し、後でアドレスを変更する場合は、変更をコミットし、新しいサーバー アドレスを有効にする必要があります。
   - **Secret (**シークレット**)**/**Confirm Secret (**再入力 シークレット**)** は、パスワードを暗号化するためのキーで、最大 64 文字の長さにすることができます。
   - 認証要求用のサーバー **Port**（ポート）（デフォルトは 1812）
8. **OK** をクリックしてサーバー プロファイルを保存します。

冗長性を確保するには、ファイアウォールで使用するシーケンスで複数の RADIUS サーバーを追加します。EAP 方式を選択した場合は、ユーザーが認証リクエストに正常に応答できるように、認証シーケンスを設定します。EAP を使用した代替認証方法はありません。ユーザーが認証リクエストに失敗し、別の認証方法を許可する認証シーケンスを設定していない場合、認証は失敗します。

STEP 2 | PEAP-MSCHAPv2 を GlobalProtect で使用中の場合、GlobalProtect ユーザーが変更済みで有効期限切れのパスワードを使用してログインできるようにするには、**Allow users to change passwords after expiry**（有効期限が切れた後にユーザーがパスワードを変更できるようにする）を選択します。

STEP 3 | (PEAP-MSCHAPv2、GTC 付属 PEAP、またはPAP 付属 EAP-TTLS 専用）サーバー認証後に作成される外部トンネル内の、ユーザーの識別情報を匿名化するには、**Make Outer Identity Anonymous**（外部アイデンティティを匿名化）を選択します。

チェーン全体が匿名ユーザーにアクセスできるように *RADIUS* サーバーを設定する必要があります。一部の *RADIUS* サーバー設定では、匿名の外部 *ID* はサポートされていない可能性があり、オプションをクリアする必要があります。クリアされると、*RADIUS* サーバーはクリアテキストでユーザー名を送信します。

STEP 4 | EAP 認証方式を選択した場合は、 証明書プロファイルを選択します。

STEP 5 | RADIUS サーバー プロファイルを認証プロファイルに割り当てます。

認証プロファイルは、一連のユーザーに対して共通の認証設定を定義します。

1. **Device (デバイス)** > **Authentication Profile (認証プロファイル)** を選択してプロファイルを **Add (追加)** します。
2. 認証プロファイルを識別する **Name**（名前）を入力します。
3. **Type**（タイプ）を **RADIUS** に設定します。
4. 設定した **Server Profile**（サーバー プロファイル）を選択します。
5. **Retrieve user group from RADIUS**（**RADIUS** からユーザー グループを取得）を選択して、RADIUS サーバーで定義された VSA からユーザー グループ情報を収集します。

   ファイアウォールは、認証プロファイルの許可リストで指定したグループに対し、グループ情報をマッチさせます。
6. **Advanced (詳細)** を選択し、Allow List (許可リスト) 内で、この認証プロファイルで認証できるユーザーとグループを **Add (追加)** します。
7. **OK** をクリックして認証プロファイルを保存します。

STEP 6 | すべての管理者に対して認証プロファイルを使用するようにファイアウォールを設定します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して Authentication Settings (認証設定) を編集します。
2. 設定した **Authentication Profile**（認証プロファイル）を選択し、**OK** をクリックします。

STEP 7 | 管理者用に、認証設定を定義するアクセスドメインおよびロールを設定します。

すでに RADIUS サーバー上で RADIUS VSA を定義済みである場合は、ファイアウォール上でロールおよびアクセスドメイン用に指定する名前が、VSA の値と一致しなければなりません。

1. 管理者が事前定義済みの（動的）ロールの代わりにカスタム ロールを使用する場合、管理者ロール プロファイルの設定を行います。
2. ファイアウォールに複数の仮想システムがある場合は、アクセス ドメインを設定します。
   1. **Device (デバイス)** > **Access Domain (アクセスドメイン)** の順に選択してアクセス ドメインを **Add (追加)** し、そのドメインを識別する **Name (名前)** を入力します。
   2. 管理者がアクセスする各仮想システムを **Add (追加)** し、**OK** をクリックします。

STEP 8 | 変更を **Commit (コミット)** し、ファイアウォール上でそれらを有効化します。

STEP 9 | RADIUS サーバーを設定し、管理者の本人確認と認証を行います。

これらの手順を実行するには、RADIUS サーバーのドキュメントで各手順を参照してください。

1. ファイアウォールの IP アドレスまたはホスト名を RADIUS クライアントとして追加します。
2. 管理者アカウントを追加します。

   RADIUS サーバー プロファイルで ***Authentication Protocol***（認証プロトコル）として ***CHAP*** を指定している場合、逆暗号化されたパスワードを使用してアカウントを定義する必要があります。定義していないと *CHAP* 認証に失敗します。
3. ファイアウォール（25461）のベンダーコードを定義し、各管理者のユーザーグループ、アクセスドメイン、ロール用の RADIUS VSA を定義します。

   ユーザーの動的管理者ロールを事前定義する場合、小文字を使用してロールを指定します (例えば、**SuperUser** ではなく、**superuser** と入力します。)

   ACS 上で詳細なベンダーオプションを設定する際、***Vendor Length Field Size (***ベンダー長さフィールド サイズ***)*** および ***Vendor Type Field Size (***ベンダー タイプ フィールド サイズ***)*** を両方とも ***1*** に設定する必要があります。定義していないと認証に失敗します。
4. EAP 方式を選択した場合、ファイアウォールはサーバーを検証しますが、クライアントは検証しません。クライアントの妥当性を確認するには、クライアントを IP アドレスまたはサブドメインで制限します。

STEP 10 | RADIUS サーバーが管理者の認証および承認を実行することを確認します。

1. RADIUS サーバーに追加した管理者アカウントを使用してファイアウォールの Web インターフェイスにログインします。
2. 管理者に関連付けたロールに許可された Web インターフェイス ページにしかアクセスできないことを確認します。
3. **Monitor**（監視）タブ、**Policies**（ポリシー）タブ、**Objects**（オブジェクト）タブで、管理者に関連付けたアクセス ドメインに許可された仮想システムにしかアクセスできないことを確認します。
4. **Monitor**（監視） > **Authentication**（認証）で、**Authentication Protocol**（認証プロトコル）を検証します。
5. 次のCLIコマンドを使用して、証明書プロファイルの接続と妥当性をテストします。

```
admin@PA-220 > test authentication authentication-profile
 auth-profile username <username> password <password>
```

LDAP 認証の設定

LDAP を使用し、認証ポータルを通じてアプリケーションあるいはサービスにアクセスするエンドユーザーを認証したり、Webインターフェースにアクセスするファイアウォールあるいは Panorama管理者を認証したりできます。

また、*LDAP* サーバーに接続し、ユーザーグループに基づいてポリシールールを定義することもできます。詳細についてはユーザー対グループのマッピングを参照してください。

STEP 1 | LDAP サーバー プロファイルを追加します。

このプロファイルは、ファイアウォールが LDAP サーバーに接続する方法を定義します。

1. Panorama™ で **Device**（デバイス） > **Server Profiles**（サーバ プロファイル） > **LDAP** または **Panorama** > **Server Profiles**（サーバ プロファイル） > **LDAP** を選択し、サーバープロファイルを**Add**（追加）します。
2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
3. （マルチ vsys のみ）プロファイルが使用可能な **Location**（場所）を選択します。
4. （任意）**Administrator Use Only**（管理者のみ使用）を選択し、管理者へのアクセスを制限します。
5. LDAP サーバーを **Add (追加)** します（最大 4 件）。各サーバーについて、**Name (名前)**（サーバーを識別するため）、**LDAP Server (サーバー)** の IP アドレスあるいは FQDN、およびサーバーの **Port (ポート)**（デフォルトは 389）を入力します。

   FQDN アドレス オブジェクトを使用してサーバーを識別し、後でアドレスを変更する場合は、変更をコミットし、新しいサーバー アドレスを有効にする必要があります。
6. サーバーの **Type (タイプ)** を選択します。
7. **Base DN**（ベース **DN**）を選択します。

   ディレクトリのベース DN を識別するには、**Active Directory Domains and Trusts(Active Directory** ドメインと信頼関係)Microsoft 管理コンソールスナップインを開き、トップレベル ドメインの名前を使用します。
8. **Bind DN** と **Password**（パスワード）を入力して、ファイアウォールを認証するための認証サービスを有効にします。

   Bind DN (バインド DN) アカウントには、*LDAP* ディレクトリを参照する権限が必要です。
9. **Bind Timeout (バインドのタイムアウト)** および **Search Timeout (検索タイムアウト)** を秒単位で入力します（デフォルトはどちらも 30）。
10. **Retry Interval**（再試行間隔）を秒単位で入力します（デフォルトは 60）。
11. **Require SSL/TLS secured connection**（**SSL/TLS**で保護された接続を要求）オプションを有効化する必要があります (デフォルトで有効)。サーバー ポートによってエンドポイントが使用するプロトコル：
    - 389（デフォルト） – TLS（具体的には、デバイスは StartTLS 操作を使用して、最初のプレーンテキスト接続を TLS にアップグレードします）
    - 636 – SSL
    - その他の任意のポート – デバイスはまず TLS を使用しようとします。ディレクトリ サーバーで TLS がサポートされていない場合は、SSL にフォールバックします。
12. （LDAP のみ）保護を強化するには、**Verify Server Certificate for SSL sessions**（**SSL** セッションのサーバー証明書を確認）オプションを有効化します。すると、エンドポイントは SSL/TLS 接続にディレクトリサーバーが提示する証明書を確認します。この検証を有効にする場合は、**Require SSL/TLS secured connection**（**SSL/TLS**で保護された

接続を要求）オプションを有効化する必要があります。進めるための確認において、証明書は次のいずれかの条件に合う必要があります。

- デバイス証明書のリストにある：**Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）。必要に応じて、証明書をデバイスにインポートします。
- 証明書の署名者は信頼できる証明機関のリストにあること：**Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Default Trusted Certificate Authorities**（デフォルトの信頼できる証明機関）

13. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 2 | サーバー プロファイルを割り当てて認証プロファイルおよびシーケンスの設定を行い、各種の認証設定を定義します。

STEP 3 | 認証が必要なファイアウォール アプリケーションに認証プロファイルを割り当てます。

- Web インターフェイスへの管理者アクセス–ファイアウォール管理者アカウントの設定を行い、設定した認証プロファイルを割り当てます。
- サービスおよびアプリケーションへのエンドユーザーのアクセス–エンドユーザーの認証を設定する際の完全な流れについては、認証ポリシーの設定を参照してください。

STEP 4 | 認証サーバー接続のテストを行い、ファイアウォールがユーザーを認証できることを確認します。

認証サーバーの接続タイムアウト

ファイアウォールあるいは Panorama にアクセスする管理者や、認証ポータルを通してサービスあるいはアプリケーションにアクセスするエンドユーザーを認証するために、ファイアウォールが外部認証サービスを使用するように設定できます。ファイアウォールが到達できない認証サーバーに何度も到達しようと試みることでリソースを無駄にしないようにするために、ファイアウォールが接続の試行を停止するまでのタイムアウト期間を設定することができます。このタイムアウトは、ファイアウォールが認証サーバーに接続する方法を定義するサーバープロファイルで設定します。タイムアウトの値を選択する際の目標は、ファイアウォール リソースを節約するというニーズを満たしつつ、認証サーバーがファイアウォールに素早く応答する方法に影響を与える通常のネットワーク遅延を損なわないように上手くバランスを取ることです。

- 認証サーバー タイムアウトを設定する際のガイドライン
- PAN-OS Web サーバー タイムアウトを変更
- 認証ポータルのセッション タイムアウトを変更

認証サーバー タイムアウトを設定する際のガイドライン

以下は、ファイアウォールが外部認証サービスへの接続を試みる際のタイムアウトを設定するためのガイドラインです。

- 特定のサーバー用にサーバープロファイルで設定したタイムアウトに加え、ファイアウォールにはグローバル PAN-OS Web サーバー タイムアウトがあります。このグローバル タイムアウトは、ファイアウォールの Webインターフェースあるいは PAN-OS XML API への管理者アクセス、および認証ポータルを通じたアプリケーションあるいはサービスへのエンドユーザー アクセスを認証する外部サーバーにファイアウォールが接続する際に適用されます。グローバル タイムアウトのデフォルト設定は 30 秒です（範囲は 3～125）。これは、サーバープロファイルが接続の試行において許可する合計時間と同じかそれより大きくなければなりません。サーバープロファイルの合計時間は、タイムアウトの値にリトライ数およびサーバー数を掛けたものです。例えば、RADIUS サーバープロファイルで 3 秒のタイムアウト、3 回のリトライ、4 つのサーバーを指定している場合、接続の試行に関してプロファイルが許可する合計時間は 36 秒（3 x 3 x 4）です。必要に応じてPAN-OS Web サーバー タイムアウトを変更します。

  認証が失敗していない限り、*PAN-OS Web* サーバー タイムアウトを変更しないでください。タイムアウトの設定が大きすぎると、ファイアウォールのパフォーマンスが下がったり、認証リクエストをドロップしてしまったりするおそれがあります。認証の失敗は認証ログで確認できます。

- ファイアウォールは、エンドユーザーが認証ポータルの Web フォームの認証チャレンジに答える際にかけられる時間を定義する認証ポータル セッション タイムアウトを適用します。Web フォームは、認証ポリシールールにマッチするサービスあるいはアプリケーションをユーザーがリクエストする際に表示されます。セッション タイムアウトのデフォルト設定は 30 秒です（範囲は 1 ～1,599,999）。これは、PAN-OS Web サーバーのタイムアウトと同じかそれより大きくなければなりません。必要に応じて、認証ポータルのセッション タイムアウトを変更します。PAN-OS WEB サーバーおよび認証ポータルのセッション タイムアウト

を増やすと、ファイアウォールのパフォーマンスが下がったり、認証要求をドロップしてしまったりするおそれがありますので、ご注意ください。

認証ポータル セッション タイムアウトは、ファイアウォールが *IP*アドレス - ユーザー名間マッピングを保持する期間を決定するタイマーとは関係がありません。

- タイムアウトは認証シーケンス毎に累積されていきます。例えば、2 つの認証プロファイルを使う認証シーケンスの場合を考慮します。ある認証プロファイルは 3 秒のタイムアウト、3 回のリトライ、4 台のサーバーを伴う RADIUS サーバープロファイルを指定します。もう一つの認証プロファイルは、3 秒のタイムアウトおよび 2 台のサーバーを伴う TACACS+ サーバープロファイルを指定します。その認証シーケンスでユーザーアカウントを認証するためにファイアウォールがかけられる最長の時間は、42 秒です（RADIUS サーバープロファイルに対して 36 秒、TACACS+ サーバープロファイルに対して 6 秒）。
- Kerberos サーバーのタイムアウトは、Kerberos サーバープロファイルで指定される各サーバー毎に 17 秒であり、これは設定できません。
- その他のサーバータイプでタイムアウトおよび関連設定を行う方法は、次を参照してください。
  - MFA サーバープロファイルを追加します。
  - SAML IdP サーバー プロファイルを追加します。
  - TACACS+サーバー プロファイルを追加します。
  - RADIUS サーバー プロファイルを追加します。
  - LDAP サーバー プロファイルを追加します。

PAN-OS Web サーバー タイムアウトを変更

PAN-OS Web サーバーのタイムアウトは、認証サーバープロファイルのタイムアウトに、そのプロファイルのリトライ数およびサーバー数を掛けた値以上でなければなりません。

認証が失敗していない限り、*PAN-OS Web* サーバー タイムアウトを変更しないでください。タイムアウトの設定が大きすぎると、ファイアウォールのパフォーマンスが下がったり、認証リクエストをドロップしてしまったりするおそれがあります。認証の失敗は認証ログで確認できます。

STEP 1 | ファイアウォール CLI にアクセスします。

STEP 2 | 次のコマンドを入力して、PAN-OS Web サーバーのタイムアウトを設定します。*<value>* は秒数です (デフォルトは 30、範囲は 3 ~ 125)。

```
> configure # set deviceconfig setting l3-service timeout <value>
 # commit
```

認証ポータルのセッション タイムアウトを変更

認証ポータルのセッション タイムアウトは、PAN-OS Web サーバーのタイムアウトと同じか、それより大きくなければなりません。詳細については認証サーバーの接続タイムアウトを参照してください。

PAN-OS Web サーバーおよび認証ポータルのセッション タイムアウトの値を増やすほど、認証ポータルからユーザーへの応答が遅くなります。

STEP 1 | **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** を選択して Session Timeouts (セッション タイムアウト) を編集します。

STEP 2 | 新しい **Authentication Portal (認証ポータル)** の値を秒単位で入力（デフォルトは 30、範囲は 1～1,599,999）して **OK** をクリックします。

STEP 3 | 変更を **Commit (コミット)**します。

ローカルデータベース認証の設定

ファイアウォールの Webインターフェースにアクセスする管理者を認証するため、および認証ポータルあるいは GlobalProtect を通じてアプリケーションにアクセスするエンドユーザーを認証するために、ファイアウォールのローカルにあるユーザーデータベースを設定できます。次の各作業を行い、ローカル データベースを使用するローカル認証を設定します。

一元的なアカウント管理を行えるというメリットがあるため、通常、ローカル認証よりも外部認証サービスの方が好ましい方法です。

データベースを使用しないローカル認証を設定することもできますが、それはファイアウォールあるいはPanorama 管理者用でしか行えません。

STEP 1 | ユーザーアカウントをローカル データベースに追加します。

1. **Device (デバイス)** > **Local User Database (ローカル ユーザー データベース)** > **Users (ユーザー)** を選択して **Add (追加)** をクリックします。
2. **Name**（名前）に管理者のユーザー名を入力します。
3. **Password**[パスワード]を入力し、さらに**Confirm Password**[パスワードの確認]を行うか、**Password Hash**[パスワード ハッシュ]を入力します。
4. アカウントを**Enable**[有効化]（デフォルト設定で有効）し、**OK**をクリックします。

STEP 2 | ユーザーグループをローカル データベースに追加します。

ユーザーがグループ メンバーシップを必要とする場合は必須です。

1. **Device (デバイス)** > **Local User Database (ローカル ユーザー データベース)** > **User Groups (ユーザーグループ)** を選択して **Add (追加)** をクリックします。
2. グループの識別に使用する **Name** [名前]を入力します。
3. グループのメンバーである各ユーザーを**Add**[追加]し、**OK**をクリックします。

STEP 3 | 認証プロファイルを設定します。

認証プロファイルは、一連のユーザーに対して共通の認証設定を定義します。認証**Type**[タイプ]を**Local Database**[ローカルデータベース]に設定します。

STEP 4 | 管理者アカウントあるいはエンドユーザー用の認証ポリシールールに認証プロファイルを割り当てます。

- **Administrators**—Configurea Firewall Administrator Account:

  この手順の前半で定義したユーザーの **Name** を指定します。

  アカウント用に構成した **Authentication Profile** を割り当てます。

- エンドユーザー—エンドユーザーの認証を設定する際の完全な流れについては、認証ポリシーの設定を参照してください。

STEP 5 | 認証サーバー接続のテストを行い、ファイアウォールがユーザーを認証できることを確認します。

認証プロファイルおよびシーケンスの設定

認証プロファイルは、ファイアウォールの Webインターフェースにアクセスする管理者、および認証ポータルまたは GlobalProtect 経由でアプリケーションにアクセスするエンドユーザーの、ログイン認証情報を検証する認証サービスを定義します。このサービスとして、ファイアウォールが提供するローカル認証あるいは外部認証サービスを使用できます。また、認証プロファイルは Kerberos シングル サインオン（SSO）などの各オプションも定義します。

一部のネットワークには、異なるユーザーおよびユーザー グループを対象とした複数のデータベース（TACACS+ および LDAP など）が存在します。そのようなケースでユーザーを認証するためには、認証シーケンス（ログイン時にファイアウォールあるいは Panorama が管理者を照合する認証プロファイルの順序）を設定します。ファイアウォールは、いずれかのプロファイルによって管理者の認証が成功するまで、各プロファイルを順番にチェックしていきます。ユーザーは、シーケンス中のすべてのプロファイルで認証が失敗した場合にのみ、アクセスが拒否されます。シーケンスは マルチ ファクター認証（MFA）および SAML を除き、ファイアウォールがサポートするあらゆる認証サービスに基づく認証プロファイルを指定できます。

STEP 1 | （外部サービスのみ）ファイアウォールが外部サービスに接続してユーザーを認証する機能を有効化します。

1. 外部サーバーをセットアップします。手順についてはお使いのサーバーのドキュメントを参照してください。
2. 使用する認証サービスのタイプに応じてサーバー プロファイルを設定します。
   - RADIUS サーバー プロファイルを追加します。

     ファイアウォールが *RADIUS* を通じて *MFA* サービスを統合する場合は、*RADIUS* サーバープロファイルを追加する必要があります。このケースでは、*MFA* サービスがすべての認証要素を提供します。ファイアウォールがベンダーの *API* を通じて *MFA* サービスを統合する場合でも、最初の要素で *RADIUS* サーバープロファイルを使用できますが、追加の要素については *MFA* サーバープロファイルが必要になります。

   - MFA サーバープロファイルを追加します。
   - SAML IdP サーバー プロファイルを追加します。
   - Kerberosサーバー プロファイルを追加します。
   - TACACS+サーバー プロファイルを追加します。
   - LDAP サーバー プロファイルを追加します。

STEP 2 | （ローカル データベース認証のみ）ファイアウォールのローカルにあるユーザーデータベースを設定します。

ファイアウォールのローカルにあるユーザー ID ストアに基づき、ローカル認証を設定したい各ユーザーおよびユーザーグループに対してこれらの各ステップを実行します。

1. ユーザーアカウントをローカル データベースに追加します。
2. （任意）ユーザーグループをローカル データベースに追加します。

STEP 3 | （Kerberos SSO のみ）Kerberos シングル サインオン（SSO）が第一認証サービスである場合は、ファイアウォール用の Kerberos キータブを作成します。

Kerberos キータブを作成します。キータブは、ファイアウォールの Kerberos アカウント情報が含まれるファイルです。Kerberos SSO をサポートするには、ネットワークに Kerberos インフラストラクチャが必要です。

STEP 4 | 認証プロファイルを設定します。

以下のいずれかまたは両方を定義します。

- **Kerberos SSO**—ファイアウォールは最初に SSO 認証を試行します。これに失敗すると、指定済みの認証 **Type (タイプ)** にフォールバックします。
- 外部認証あるいはローカル データベース認証—ファイアウォールがユーザーにログイン認証情報を入力するよう求め、外部サービスあるいはローカル データベースを使用してユーザーを認証します。

1. **Device (デバイス)** > **Authentication Profile (認証プロファイル)** を選択して認証プロファイルを **Add (追加)** します。
2. 認証プロファイルを識別する **Name**（名前）を入力します。
3. 認証サービスの **Type (タイプ)** を選択します。
   - マルチ ファクター認証を使用する場合、選択したタイプは最初の認証要素に対してのみ適用されます。**Factors (要素)** タブで、追加の MFA 要素に使用するサービスを選択します。
   - **RADIUS**、**TACACS+**、**LDAP**、**Kerberos** のいずれかを選択する場合は、**Server Profile (サーバー プロファイル)** を選択します。
   - **LDAP** を選択する場合は、**Server Profile (サーバープロファイル)** を選択して **Login Attribute (ログイン属性)** を定義します。アクティブディレクトリには、**sAMAccountName**の値を入力します。
   - **SAML** を選択する場合は、**IdP Server Profile (IdP** サーバープロファイル**)** を選択します。
   - クラウド認証サービス を選択した場合は、ファイアウォールと通信するように Cloud Identity Engine インスタンスを構成します。クラウド ID エンジンの詳細については、「クラウド ID エンジンの概要 」ガイドを参照してください。
4. Kerberos SSO を有効にする場合は、**Kerberos Realm** [Kerberos レルム]（レルムが大文字の場合を除き、通常はユーザーの DNS ドメイン）に入力し、ファイアウォールあ

るいはPanorama用に作成した **Kerberos Keytab**[Kerberos キータブ]を**Import**[インポート]します。

5. （MFA のみ）**Factors (要素)**、**Enable Additional Authentication Factors (追加の認証要素を有効化)** を選択し、設定した MFA サーバープロファイルを **Add (追加)** します。

   ファイアウォールはリストの順番に従って上から順に MFA サービスを呼び出していきます。

6. **Advanced (詳細)** を選択し、このプロファイルでにんしょうを行えるユーザーおよびグループを **Add (追加)** します。

   ローカル データベースから、あるいは ユーザー対グループのマッピングを設定している場合は LDAP ベースのディレクトリ サービス（Active Directory (アクティブディレクトリ) など）から、ユーザーおよびグループを選択できます。デフォルトでは、リストが空で、どのユーザーも認証されません。

   また、グループ マッピング設定で定義されているカスタム グループを選択することもできます。

7. (任意) ファイアウォールが認証リクエストをサーバーに送信する前にユーザー情報を修正するために、**Username Modifier (ユーザー名修飾子)** を設定します。

   - **%USERDOMAIN%\%USERINPUT%**—ソースにドメインが含まれていない場合 (例えば sAMAccountName を使用)、ファイアウォールはユーザーが指定する **User Domain (ユーザードメイン)** をユーザー名の前に追加します。ソースにドメインが含まれる場合、ファイアウォールはそのドメインを **User Domain (ユーザードメイン)** と置き換えます。**User Domain (ユーザードメイン)** が空の場合、ファイアウォールはリクエストを認証サーバーに送信する前に、ソースから受信したユーザー情報からドメインを削除します。

     LDAP サーバーは *sAMAccountName* のバックスラッシュをサポートしていないため、このオプションを使用して *LDAP* サーバーで認証しないでください。

   - **%USERINPUT%**—(デフォルト) ファイアウォールは、ソースから受信したフォーマットでユーザー情報を認証サーバーに送信します。
   - **%USERINPUT%@%USERDOMAIN%**—ソースにドメインが含まれていない場合、ファイアウォールはユーザー名の後に **User Domain (ユーザードメイン)** の値を追加します。ソースにドメインが含まれる場合、ファイアウォールはそのドメインを **User Domain (ユーザードメイン)** の値と置き換えます。**User Domain (ユーザードメイン)** が空の場合、ファイアウォールはリクエストを認証サーバーに送信する前に、ソースから受信したユーザー情報からドメインを削除します。
   - なし—**None （なし）** を手動で入力する場合：
     - LDAP および Kerberos サーバープロファイルの場合、ファイアウォールはソースから受信したドメインを使用して適切な認証プロファイルを選択してから、認証リクエストをサーバーに送信する際にドメインを削除します。これにより、認証シーケンスの間は **User Domain (ユーザードメイン)** を含めつつ、ファイアウォールがサーバーに認証リクエストを送信する前にドメインを削除することができます。例えば、LDAP サーバープロファイル、および samAccountName を属性とし

て使用している場合、このオプションを使用することで、ドメインではなくユーザー名だけを想定している認証サーバーにファイアウォールがドメインを送信しないようにすることができます。

- RADIUS サーバープロファイルの場合：
  - ソースがユーザー情報を **domain\username** の形式で送信する場合、ファイアウォールはユーザー情報を同じ形式でサーバーに送信します。
  - ソースがユーザー情報を **username@domain** の形式で送信する場合、ファイアウォールはユーザー情報を **domain\username** の形に正規化してからサーバーに送信します。
  - ソースがユーザー名だけを送信する場合、ファイアウォールは **domain\username** という形式で情報をサーバーに送信する前にユーザーが指定する **User Domain (ユーザードメイン)** を追加します。
- ローカル データベース、TACACS+、SAML の場合、ファイアウォールは、ソースから受信したフォーマットでユーザー情報を認証サーバーに送信します。

8. **OK** をクリックして認証プロファイルを保存します。

STEP 5 | 認証シーケンスを設定します。

ファイアウォールがユーザーの認証に複数の認証プロファイルを試行する場合は必須です。ファイアウォールはいずれかのプロファイルが正常にユーザーを認証するまで、上から順に各プロファイルを評価していきます。

1. **Device (デバイス)** > **Authentication (認証) Sequence** を選択して認証シーケンスを **Add (追加)** します。
2. 認証シーケンスを識別する **Name** [名前]を入力します。

   Use domain to determine authentication profile (ドメインを使用して認証プロファイルを決定) をオンにすることで、認証プロセスを高速化できます。ファイアウォールが、ログイン時にユーザーが入力したドメイン名を、シーケンスにある認証プロファイルの ***User Domain (ユーザー ドメイン)*** または ***Kerberos Realm (Kerberos レルム)*** と照合し、そのプロファイルを使用してユーザーを認証します。一致するものが見つからなかった場合、またはこのオプションを無効にしている場合は、ファイアウォールがプロファイルをシーケンスの上から順に試行します。
3. 各認証プロファイルを追加します。プロファイルの評価順序を変更するには、プロファイルを選択して **Move Up (上へ)** または **Move Down (下へ)** をクリックします。
4. **OK**[OK] をクリックして、認証シーケンスを保存します。

STEP 6 | ファイアウォール管理者用に管理者アカウントに、あるいはエンドユーザー用に認証ポリシーに対して認証プロファイルあるいはシーケンスを割り当てます。

- 管理者 – 管理者権限の管理方法に基づいて認証プロファイルを割り当てます。

  ファイアウォール内のローカルで管理される承認–ファイアウォールの管理者アカウントを設定する.

  SAML、TACACS+、または RADIUS サーバーで管理される承認 – **Device (デバイス) Setup (セットアップ) Management (管理)** を選択して、Authentication Settings (認証設定) を編集し、認証プロファイル.

  を選択します。

- エンドユーザー–エンドユーザーの認証を設定する際の完全な流れについては、認証ポリシーの設定を参照してください。

STEP 7 | 認証サーバー接続のテストを行い、ファイアウォールがユーザーを認証できることを確認します。

認証サーバー接続のテスト

テスト認証機能により、ファイアウォールあるいは Panorama が認証プロファイルで指定された認証サーバーと通信できるかどうかや、特定のユーザーの認証リクエストが成功するかどうかを確認できます。Web インターフェイスにアクセスする管理者や、GlobalProtect あるいは認証ポータルを通してアプリケーションにアクセスするエンドユーザーを認証する認証プロファイルをテストすることができます。候補設定で認証テストを実行し、コミットする前に設定が正しいかどうかを確認できます。

STEP 1 | 認証プロファイルを設定します。テストを行う前に認証プロファイルやサーバープロファイルの設定をコミットする必要はありません。

STEP 2 | ファイアウォール CLI にログインします。

STEP 3 | （仮想システムが複数あるファイアウォール）test コマンドがアクセスするターゲット仮想システムを定義します。

テスト認証コマンドがテスト対象のユーザーを特定できるようにするために、仮想システムが複数あるファイアウォールではこれが必須になります。

次を入力して対象の仮想システムを定義します。

```
admin@PA-3250> set system setting target-vsys <vsys-name>
```

たとえば、vsys2 にユーザーが定義されている場合は、次のように入力します。

```
admin@PA-3250> set system setting target-vsys vsys2
```

この ***target-vsys*** オプションは、ログイン セッション単位のものです。ログオフするとファイアウォールがこのオプションをクリアします。

STEP 4 | 認証プロファイルをテストするには、以下のコマンドを入力します。

```
admin@PA-3250> test authentication authentication-
profile <authentication-profile-name> username <username> password
```

たとえば、**bsimpson** という名前のユーザーの **my-profile** という認証プロファイルをテストするには、次のように入力します。

```
admin@PA-3250> test authentication authentication-profile my-
profile username bsimpson password
```

test コマンドを実行する際、認証プロファイルおよびサーバープロファイルの名前の大文字と小文字は区別されます。また、認証プロファイルにユーザー名修飾子が定義されている場合は、ユーザー名とともに修飾子も入力する必要があります。たとえば、名前が *bsimpson* でドメイン名が *mydomain.com* のユーザーに修飾子「*%USERINPUT%@%USERDOMAIN%*」を追加する場合は、ユーザー名に「*bsimpson@mydomain.com*」と入力します。これにより、確実にファイアウォールが認証サーバーに正しい認証情報を送信するようになります。この例では、*mydomain.com* が、認証プロファイルの ***User Domain (***ユーザー ドメイン***)*** フィールドに定義されているドメインです。

STEP 5 | テスト出力を表示します。

認証プロファイルが正しく設定されている場合は、出力に `Authentication succeeded` と表示されます。設定に問題がある場合は、出力に設定のトラブルシューティングに役立つ情報が示されます。

出力結果は、テストした認証タイプや問題の種類に関連するいくつかの要因によって異なります。たとえば、*RADIUS* と *TACACS+* では使用する基本ライブラリが異なるため、どちらのタイプにも存在する同じ問題から異なるエラーが生成されます。また、認証サーバー プロファイルで誤ったポートや *IP* アドレスを使用している場合などネットワークの問題がある場合は、具体的なエラーが出力されません。これは *test* コマンドが、ファイアウォールと認証サーバー間の最初のハンドシェークを実行できず、問題の詳細を判断できないためです。

認証ポリシー

認証ポリシーを使用すると、エンド ユーザーがサービスおよびアプリケーションにアクセスする前に、エンドユーザーの認証を行うことができます。ユーザーがサービスまたはアプリケーションを要求したとき（Web ページへのアクセス時など）、ファイアウォールが必ず認証ポリシーを評価します。一致する認証ポリシー ルールに基づいて、ファイアウォールは、ログインとパスワード、音声、SMS、プッシュ、またはワンタイム パスワード（OTP）認証のように、複数の方法（要素）を使用して認証するようにユーザーに求めます。第 1 の要素として、ユーザーは Authentication Portal Web フォームを通じて認証されます。その他の要素については、ユーザーはマルチ ファクター認証（MFA）ログインページを通じて認証されます。

GlobalProtect 用の認証ポリシーを実装する方法は、マルチ ファクター認証の通知を活用するための GlobalProtect の設定を参照してください。

すべての要素に対して認証を済ませると、ファイアウォールはセキュリティ ポリシーを評価して、サービスあるいはアプリケーションへのアクセスを許可するかどうかを判断します。

ユーザーのワークフローを中断する認証の問題が発生する頻度を減らすために、ユーザーが後でアクセスするのではなく、サービスやアプリケーションへの初期アクセスのみを認証するタイムアウト期間を指定できます。認証ポリシーは認証ポータルと統合され、タイムアウトの評価に使用されるタイムスタンプを記録し、ユーザーベースのポリシーとレポートを有効にします。

ファイアウォールが認証時に収集するユーザ情報に基づいて、User-ID は新しい IP アドレスとユーザー間のマッピングを作成します（マッピング情報が変更されている場合）。ファイアウォールは、追加と更新を記録する User-ID ログを生成します。また、ファイアウォールは、認証ルールに一致するリクエストごとに認証ログを生成します。一元的な監視を志向する場合は、User-ID または認証ログに基づいてレポートを構成し、他のログ タイプと同様に、Panorama または外部サービスにログを転送できます。

- 認証タイムスタンプ
- 認証ポリシーの設定

認証タイムスタンプ

認証ポリシー ルールを設定するときに、ユーザーがサービスおよびアプリケーションへの最初のアクセスに対してのみ認証するタイムアウト期間を指定できます。後続のアクセスでは許可されません。あなたの目標は、サービスとアプリケーションを保護する必要性とユーザーのワークフローへの中断を最小限にする必要性とのバランスをとるタイムアウトを指定することです。ユーザーが認証すると、ファイアウォールは、最初の認証チャレンジ（ファクター）のタイムスタンプと、追加のマルチ ファクター認証（MFA）ファクターのタイムスタンプを記録します。その後、ユーザーが認証ルールに一致するサービスとアプリケーションを要求すると、ファイアウォールは各タイムスタンプに関連するルールで指定されたタイムアウトを評価します。つまり、ファイアウォールは、タイムアウトが切れた場合に、ファクターごとに認証の問題を再発行します。ユーザーマッピングと認証タイムスタンプを再配布すると、すべてのファイアウォールがすべてのユーザーに対して一貫して認証ポリシーのタイムアウトを強制します。

ファイアウォールは、各 *MFA* ベンダーに個別のタイムスタンプを記録します。たとえば、Duo v2 と *PingID* サーバーを使用して *MFA* ファクターの課題を発行する場合、ファイアウォールは、*Duo* ファクターへの応答のタイムスタンプと *PingID* ファクターへの応答のタイムスタンプを記録します。

タイムアウト期間内に、1 つの認証ルールに対して正常に認証されたユーザーは、他のルールが保護するサービスまたはアプリケーションにアクセスできます。ただし、この移植性は、同じ認証要素をトリガするルールにのみ適用されます。たとえば、TACACS+ 認証をトリガーするルールに対して正常に認証されたユーザーは、アクセス要求が両方のルールのタイムアウト期間内であっても、SAML 認証をトリガするルールに対して再度認証する必要があります。

認証ポータルの設定（「認証ポータルの設定」を参照）で定義された各認証ルールとグローバルタイマーのタイムアウトを評価する場合、ファイアウォールは最初に有効期限が切れた設定に対して再認証を促すメッセージをユーザーに表示します。再認証時に、ファイアウォールはルールの新しい認証タイムスタンプを記録し、認証ポータル タイマーのタイムカウントをリセットします。したがって、異なる認証ルールに異なるタイムアウト時間を有効にするには、認証ポータル タイマーを任意のルールのタイムアウトと同じかそれ以上の値に設定します。

認証ポリシーの設定

以下の手順を実行し、Authentication Portal (認証ポータル) を通して各サービスにアクセスするエンドユーザー用の、認証ポリシーを設定します。作業を開始する前に、ユーザーがセキュリティポリシーによって、認証が必要なサービスおよび URL カテゴリへのアクセスが許可されていることを確認してください。

STEP 1 | Configure Authentication Portal (認証ポータルの設定) を行います。ユーザー認証でマルチファクター認証（MFA）を使用する場合、**Mode (モード)** を **Redirect (リダイレクト)** に設定する必要があります。

STEP 2 | ファイアウォールが次のいずれかのサービスを使ってユーザーを認証するよう設定します。

- 外部認証サービス—サーバープロファイルを設定し、ファイアウォールがサービスに接続する方法を定義します。
- ローカル データベース認証—各ユーザーアカウントをファイアウォール上のローカルユーザーデータベースに追加します。
- Kerberos シングル サインオン（SSO）—ファイアウォール用の Kerberos キータブを作成します。任意で、ファイアウォールが Kerberos SSO を第一認証サービスとして使用し、SSO が失敗した場合に外部サービスあるいはローカル データベース認証にフォールバックするように設定することができます。

STEP 3 | 同じ認証サービスと設定が必要な一連のユーザーおよび認証ポリシールールに対して、認証プロファイルおよびシーケンスの設定を行います。

認証サービスの **Type (タイプ)** および関連する設定を選択します。

- 外部サービス—外部サーバーの **Type (タイプ)** を選択し、そのサーバーのために作成した **Server Profile (サーバープロファイル)** を選択します。
- ローカル データベース認証—**Type (タイプ)** を **Local Database (データベース)** に設定します。**Advanced (詳細)** 設定で、作成した認証ポータル ユーザー、およびユーザーグループを **Add (追加)** します。
- **Kerberos SSO**—**Kerberos Realm (Kerberos レルム)** を指定し、**Kerberos Keytab (Kerberos キータブ)** を **Import (インポート)** します。

STEP 4 | 認証適用オブジェクトを設定します。

このオブジェクトは、各認証プロファイルを認証ポータル方式と関連付けます。方式によって、最初の認証チャレンジ（要素）が透過的に行われるか、ユーザーの応答を求めるのかが決まります。

1. **Objects (オブジェクト)** > **Authentication (認証)** を選択してオブジェクトを **Add (追加)** します。
2. オブジェクトを識別する **Name (名前)** を入力します。
3. 認証プロファイルで指定してある、その **Type (タイプ)** の認証サービスで使用する **Authentication Method (認証方法)** を選択します。
   - **browser-challenge**—最初の認証要素に対して、ユーザーに認証情報を入力させる代わりにクライアントのブラウザに応答させたい場合は、この方式を選択します。この方式では、認証プロファイルの Kerberos SSO を設定する必要があります。ブラウザ チャレンジが失敗した場合、ファイアウォールは **web-form** 方式にフォールバックします。
   - **web-form**—ユーザーがログイン認証情報を入力するための、認証ポータル Web フォームをファイアウォールに表示させたい場合は、この方式を選択します。
4. 設定した **Authentication Profile (認証プロファイル)** を選択します。
5. 初回の認証要素に対する認証方法をユーザーに伝えるのに、認証ポータルの Web フォームに表示する **Message (メッセージ)** を入力します。
6. **OK** をクリックしてオブジェクトを保存します。

STEP 5 | 認証ポリシールールを設定します。

同じ認証サービスと設定が必要な一連のユーザー、サービス、URL カテゴリ用のルールを作成します。

認証ポリシーがデフォルトの認証実施オブジェクト（たとえば、***default-browser-challenge***）を使用している場合、ファイアウォールは認証ポータルのタイムアウトを適用しません。認証ポータルのタイムアウト後、ユーザーに再認証を要求するには、デフォルト認証オブジェクトのルールを複製し、それをデフォルト認証オブジェクトの既存ルールの前に移動します。

1. **Policies (ポリシー)** > **Authentication (認証)** を選択してルールを **Add (追加)** します。
2. ルールを識別する **Name (名前)** を入力します。
3. **Source (送信元)** を選択し、特定のゾーンおよび IP アドレスを **Add (追加)** するか、**Any (すべて)** のゾーンあるいは IP アドレスを選択します。

   ルールは、指定した IP アドレスあるいは指定したゾーン内のインターフェイスから来るトラフィックにのみ適用されます。
4. **User (ユーザー)**を選択し、ルールを適用する送信元ユーザーおよびユーザーグループを選択あるいは **Add (追加)** います（デフォルトは **any (すべて)**です）。
5. ルールを適用するホスト情報プロファイルを選択あるいは **Add (追加)** します（デフォルトは **any (すべて)**です）。
6. **Source (宛先)** を選択し、特定のゾーンおよび IP アドレスを **Add (追加)** するか、**any (すべて)** のゾーンあるいは IP アドレスを選択します。

   IP アドレスは、アクセスを制御したいリソース（サーバーなど）にすることができます。
7. **Service/URL Category (サービス/URL カテゴリ)** を選択し、ルールによってアクセスを制御するサービスおよびサービスグループを選択あるいは **Add (追加)** します（デフォルトは **service-http**です）。
8. ルールによってアクセスを制御するURL カテゴリを選択あるいは **Add (追加)** します（デフォルトは **any (すべて)**です）。例えば、極めて重要な内部サイトを指定するカスタム URL カテゴリを作成することができます。
9. **Actions** （アクション） を選択し、作成した **Authentication Enforcement (認証適用)** オブジェクトを選択します。
10. サービスおよびアプリケーションに繰り返しアクセスする際に、ファイアウォールがユーザーに一度だけ認証を求める期間として、分単位で **Timeout (タイムアウト)** 期間（デフォルトは 60）を指定します。

    Timeout (タイムアウト)は、強固なセキュリティ（認証のプロンプトを表示する間隔が短い）とユーザーエクスペリエンス（認証のプロンプトを表示する間隔が長い）の間のトレードオフになります。データセンターなどの重要なシステムやセンシティブな領域へのアクセスが対象である場合、できるだけ頻繁に認証を行うのが最適な選択になるでしょう。ネットワークの境界やユーザーエクスペリエンスが重要なビジネスの場合は、認証の頻度を減らすことが最適な選択になるでしょう。

11. **OK** をクリックしてルールを保存します。

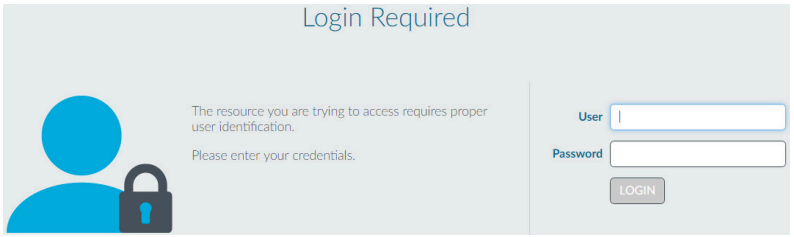
STEP 6 | （MFA のみ）MFA ログインページをカスタマイズします。

追加の MFA 要素がある場合にユーザーが認証できるよう、ファイアウォールがこのページを表示します。

STEP 7 | ファイアウォールが認証ポリシーを適用していることを確認します。

1. 認証ポリシールールで指定されているいずれかのソース ユーザーとしてネットワークにログインします。
2. ルールにマッチするサービスあるいは URL カテゴリをリクエストします。

   ファイアウォールが最初の認証要素用に認証ポータルの Web フォームを表示します。以下に例を示します。



   ファイアウォールが一つあるいは複数の *MFA* サービスを使用するように設定している場合は、追加の認証要素に対して認証を行います。

3. 先ほどアクセスしたサービスあるいは URL のセッションを終了します。
4. 同じサービスあるいはアプリケーションのセッションを新しく開始します。必ず、認証ルールで指定した**Timeout (**タイムアウト**)** の期間内にこのステップを実行するようにしてください。

   再認証を行うことなく、ファイアウォールがアクセスを許可します。
5. **Timeout (**タイムアウト**)** の期間が過ぎるのを待ってから、同じサービスあるいはアプリケーションをリクエストします。

   ファイアウォールに再認証を求められます。

STEP 8 | (任意) データおよび認証タイムスタンプの再配信 認証 ポリシーを適用する他のファイアウォールに対して、すべてのユーザーに一貫したタイムアウトを適用するようにします。

認証の問題のトラブルシューティング

ユーザーが Palo Alto Networks のファイアウォールあるいはPanoramaに対する認証に失敗した場合や、認証プロセスに予想以上の時間がかかる場合、認証に関連する以下の情報を分析すれば、失敗や遅延の原因を判断する手がかりが得られることがあります。

- ユーザー動作 – ユーザーが誤った認証情報を入力した後にロックアウトされていないか、多数のユーザーが同時にアクセスしようとしていないかなど
- システムまたはネットワークの問題 – 認証サーバーにアクセスできるかなど
- 設定の問題 – 認証プロファイルの許可リストにすべての対象ユーザーが記載されているかなど

以下の CLI コマンドは、上記の問題のトラブルシューティングに役立つ可能性のある情報を表示します。

タスク	コマンド
認証プロファイル（**auth-profile**）、認証シーケンス（**is-seq**）、または仮想システム（**vsys**）に関連付けられているロック中のユーザー アカウントの数を表示します。 ユーザーのロックを解除するには、次の操作コマンドを実行します。 `> request authentication [unlock-admin | unlock-user]`	`PA-220> show authentication locked-users { vsys <value> | auth-profile <value> | is-seq {yes | no} {auth-profile | vsys} <value> }`
認証イベントをトラブルシューティングするには、**debug authentication** コマンドを使用します。 **show** の各オプションを使用すると、認証要求の統計情報と現在のデバッグ レベルが表示されます。 • **show** は、認証サービス（authd）の現在のデバッグ レベルを表示します。 • **show-active-requests** は、認証要求、許可リスト、マルチ ファクター認証（MFA）リクエストのアクティブなチェック数を表示します。 • **show-pending-requests** は、認証要求、許可リスト、ロックされたユーザー	`PA-220> debug authentication { on {debug | dump | error | info | warn} | show | show-active-requests | show-pending-requests | connection-show | { connection-id | protocol-type { Kerberos connection-id <value> | LDAP connection-id <value> | RADIUS connection-id <value> | TACACS+ connection-id <value> | } connection-debug-on | { connection-id | debug-prefix | protocol-type { Kerberos connection-id <value> | LDAP connection-id`

タスク	コマンド
アカウント、MFA リクエストの保留中のチェック数を表示します。 • **connection-show** は、すべての認証サーバーまたは特定のプロトコル タイプの認証要求および応答の統計情報を表示します。 認証デバッグを有効または無効にするには、**connection-debug** オプションを使用します。 • authd のデバッグを有効にする場合は **on** オプション、無効にする場合は **off** オプションを使用します。 • すべての認証サーバーまたは特定のプロトコル タイプのデバッグを有効にする場合は **connection-debug-on** オプション、無効にする場合は **connection-debug-off** オプションを使用します。	**<*value*> | RADIUS connection-id <*value*> | TACACS+ connection-id <*value*> | } connection-debug-off | { connection-id | protocol-type { Kerberos connection-id <*value*> | LDAP connection-id <value> | RADIUS connection-id <value> | TACACS+ connection-id <value> | } connection-debug-on }**
証明書プロファイルの接続と有効性をテストします。	`PA-220> test authentication authentication-profile auth-profile username <username>password <password>`
Monitor（監視） > **Logs**（ログ） > **Authentication**（認証）で表示される **Authentication ID** （証明書 **ID**）を使用して、特定の認証のトラブルシューティングを行います。	`PA-220> grep <Authentication ID>`

証明書の管理

以下のトピックでは、Palo Alto Networks® のファイアウォールおよびPanoramaで使用する様々なキーや証明書、およびそれらの取得、管理方法を説明します。

- キーおよび証明書
- デフォルトの信頼された証明機関（CA）
- 証明書の失効
- 証明書のデプロイメント
- 証明書失効状態の検証の設定
- マスター キーの設定
- マスター キーの暗号化
- 証明書の取得
- 証明書および秘密鍵のエクスポート
- 証明書プロファイルの設定
- SSL/TLS サービス プロファイルの設定
- SSH サービス プロファイルの設定
- インバウンドの管理トラフィック用証明書の交換
- SSL フォワード プロキシ サーバーの証明書の鍵のサイズの設定
- 証明書の無効化および更新
- ハードウェア セキュリティ モジュールによるキーの安全確保

キーおよび証明書

Palo Alto Networks のファイアウォールおよびPanoramaでは、安全なコミュニケーション セッションでの両者間の信頼を確保するために、デジタル証明書を使用します。各証明書には、平文を暗号化したり、暗号化テキストを復号化したりするための暗号化キーが含まれています。また、発行者の ID を認証するためのデジタル署名も含まれています。発行者は、認証する側の信頼された認証局（CA）のリストに記載されている必要があります。必要に応じて、認証する側は発行者が証明書を無効化していないことを検証します（証明書の失効を参照）。

Palo Alto Networksのファイアウォールおよびでは、次のアプリケーションで証明書を使用します。

- 認証ポータルや多要素認証 (MFA)、ならびにファイアウォールまたは Panorama への Webインターフェースアクセス時のユーザー認証。
- GlobalProtect VPN （リモート ユーザーとサイト間または大規模）のデバイス認証。
- Internet Key Exchange （IKE）による IPSec サイト間 VPN のデバイス認証。
- 外部動的リスト (EDL) の検証。
- User-ID エージェントおよび TS エージェントのアクセス。
- インバウンドおよびアウトバウンド SSL トラフィックの復号化。

  ファイアウォールでは、ポリシー ルールを適用するためにトラフィックを復号化してから、最終的な宛先にトラフィックを転送する前にトラフィックを再暗号化します。アウトバウンド トラフィックの場合、ファイアウォールはフォワード プロキシ サーバーとして機能し、宛先サーバーとの SSL/TLS 接続を確立します。ファイアウォール自体とクライアント間の接続の安全性を確保するため、ファイアウォールでは署名証明書を使用して宛先サーバーの証明書のコピーを自動的に生成します。

以下の表では、Palo Alto Networksのファイアウォールおよびが使用するキーと証明書について説明します。ベスト プラクティスとして、各用途に異なるキーおよび証明書を使用します。

表 **1 : Palo Alto Networks** デバイスが使用するキー**/**証明書

キー/証明書の用途	説明
管理者アクセス	ファイアウォールあるいはPanoramaの管理インターフェイス（Web インターフェイスへの HTTPS アクセス）への安全なアクセスには、MGT インターフェイス（またはそのファイアウォールあるいはPanoramaが MGT を使用していない場合は、データプレーン上の指定インターフェイス）のサーバー証明書と、必要に応じて、管理者を認証する証明書が必要です。
認証ポータル	認証ポリシーが HTTPS リソースにアクセスするユーザーを識別する展開構成の場合、認証ポータルインターフェースのサーバー証明書を指定します。ユーザー認証のために証明書を使用するように認証ポータルを設定する場合（インタラクティブな認証の代わりに、あるいは追

キー/証明書の用途	説明
	加で）、クライアント証明書も展開します。認証ポータルの詳細については、認証ポータルを使用した IPアドレスとユーザー名のマッピングを参照してください。
フォワード トラスト	アウトバウンド SSL/TLS トラフィックでは、フォワード プロキシとして機能するファイアウォールが宛先サーバーの証明書に署名をした CA を信頼している場合、ファイアウォールでは、フォワード トラスト CA 証明書を使用して、クライアントに提示する宛先サーバー証明書のコピーを生成します。秘密鍵のサイズを設定する方法については、SSL フォワード プロキシ サーバーの証明書の鍵のサイズの設定を参照してください。セキュリティを強化するため、ハードウェア セキュリティ モジュールにキーを保存してください（詳細は、ハードウェア セキュリティ モジュールによるキーの安全確保を参照してください）。
フォワード アントラスト	アウトバウンド SSL/TLS トラフィックでは、フォワード プロキシとして機能するファイアウォールが宛先サーバーの証明書に署名をした CA を信頼しない場合、ファイアウォールでは、フォワード アントラスト CA 証明書を使用して、クライアントに提示する宛先サーバー証明書のコピーを生成します。
SSL インバウンド インスペクション	インスペクションおよびポリシー実施のためにインバウンド SSL/TLS トラフィックを復号化するキー。このアプリケーションでは、SSL/TLS インバウンド インスペクションの対象となるサーバーごとに秘密鍵をファイアウォールにインポートします。SSL インバウンド インスペクションを参照してください。

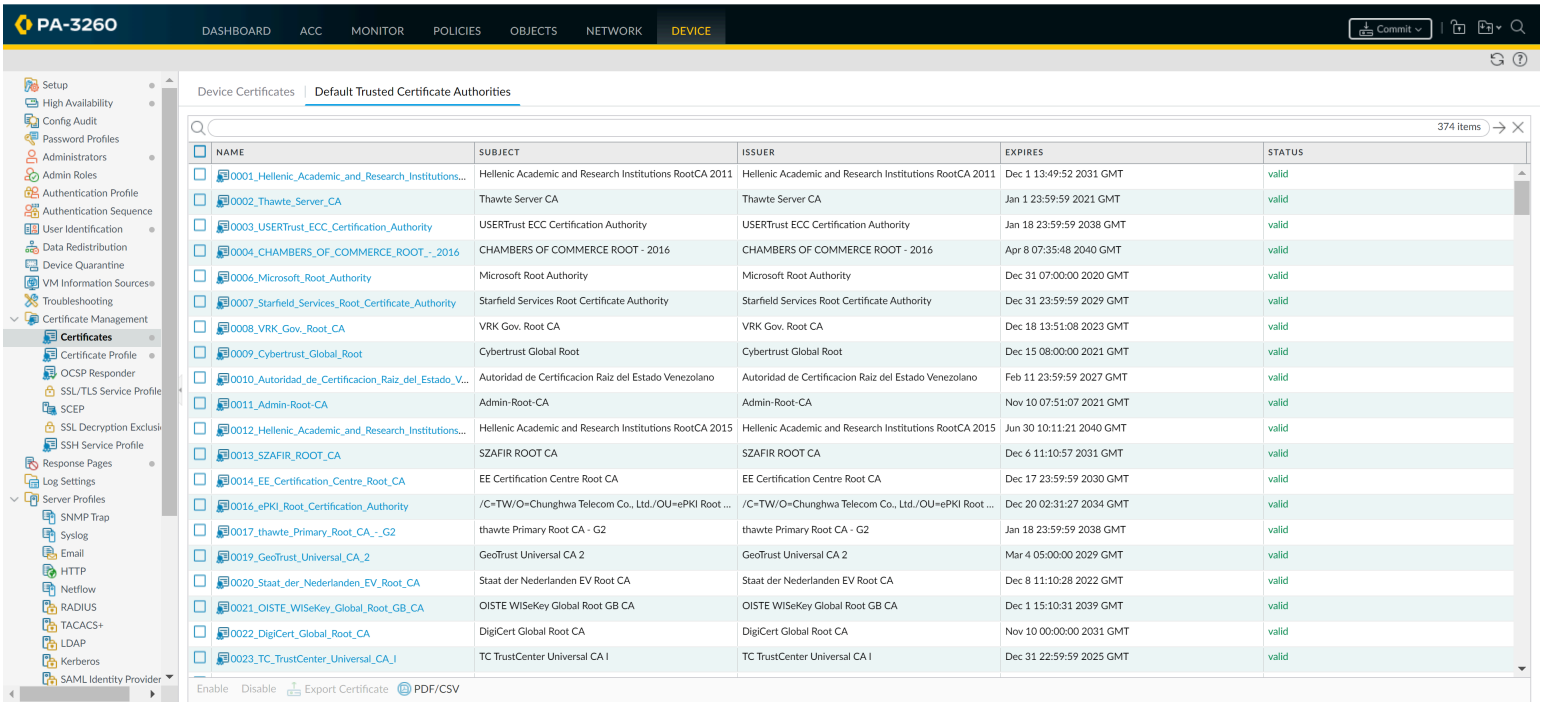
キー/証明書の用途	説明
	PAN-OS 8.0 から、ファイアウォールが楕円曲線 *Diffie-Hellman Ephemeral (ECDHE)* アルゴリズムを使用して厳格な証明書チェックを行うようになっています。つまり、ファイアウォールが中間証明書を使用する場合、*PAN-OS 8.0* 以降のリリースにアップグレードした後、*WEB* サーバーからファイアウォールに証明書をインポートし直し、サーバー証明書と中間証明書を組み合わせる必要があります *(*チェーン証明書をインポートします*)*。そうしなければ、チェーン中に中間証明書が存在する場合に *SSL* インバウンド インスペクションが失敗します。 チェーン証明書をインストールするには： **1.** メモ帳などのテキスト エディタで各証明書 *(.cer)* ファイルを開きます。 **2.** サーバー証明書の後に各署名者が続くようにして、それぞれの証明書を最初から最後までペーストします。 **3.** ファイルをテキスト *(.txt)* あるいは証明書 *(.cer)* ファイルとして保存します *(*ファイル名にはスペースを含められません*)*。 **4.** 組み合わせた *(*チェーン*)* 証明書をファイアウォールにインポートします。
SSL 除外証明書	SSL/TLS 復号化から除外するサーバーの証明書。たとえば、SSL 復号化を有効にしているが、ファイアウォールでトラフィックを復号化しないサーバー（HR システムの Web サービスなど）がネットワークに含まれている場合、該当する証明書をファイアウォールにインポートして、その証明書を SSL 除外証明書として設定します。復号化例外の管理を参照してください。
グローバルな保護	GlobalProtect のコンポーネント間のすべてのやり取りは、SSL/TLS 接続を介して実行されます。そのため、GlobalProtect デプロイメントの一環として、すべての GlobalProtect ポータル、ゲートウェイ、モバイル セキュリティ マネージャのサーバー証明書をデプロイします。必要に応じて、ユーザーを認証するための証明書もデプロイします。 *GlobalProtect* 大規模 VPN（LSVPN）機能では、*CA* 署名証明書が必要になります。

キー/証明書の用途	説明
サイト間 VPN（IKE）	サイト間 IPSec VPN デプロイメントでは、ピア デバイスは Internet Key Exchange （IKE）ゲートウェイを使用して安全なチャネルを確立します。IKE ゲートウェイでは、証明書または事前共有鍵を使用して、ピア同士が相互に認証を行います。ファイアウォールでの IKE ゲートウェイを定義する場合は、証明書またはキーを設定して、割り当てます。サイト間 VPN の概要を参照してください。
マスター キー	ファイアウォールでは、マスター キーを使用して、すべての秘密鍵とパスワードを暗号化します。ネットワークで秘密鍵を保存するための安全な場所が必要な場合は、ハードウェア セキュリティ モジュール（HSM）に保存されている暗号化（ラッピング）キーを使用して、マスター キーを暗号化できます。詳細についてはHSM を使用したマスター キーの暗号化を参照してください。
保護された Syslog	ファイアウォールと syslog サーバー間の安全な接続を有効にするための証明書。カスタム Syslog フィールドの説明を参照してください。
信頼されたルート CA	ファイアウォールが信頼する CA が発行したルート証明書の名称。ファイアウォールは自己署名ルート CA 証明書を使用して、他のアプリケーション（SSLフォワード プロキシなど）のための証明書を自動的に発行できます。 また、ファイアウォールが他のファイアウォールとの安全な接続を確立する必要がある場合、証明書を発行するルート CA が信頼されたルート CA のリストに含まれている必要があります。
デバイス間通信	Panorama、ファイアウォール、ログコレクタはデフォルトで、管理およびログ転送に使用する SSL/TLS 接続を行う際に、事前定義済みの一連の証明書を使用するようになっています。しかし、カスタム証明書をデプロイ環境内のデバイスにデプロイすることで、この接続を強化することができます。これらの証明書は、Panorama HA ピア間の SSL/TLS 接続を保護する目的でも使用できます。

デフォルトの信頼された証明機関（CA）

ファイアウォールは、デフォルトで最も一般的な信頼できる機関（CA）を信頼します。これらの信頼できる証明書プロバイダは、インターネットへの接続を保護するためにファイアウォールが必要とする証明書の発行を担当します。

ファイアウォールがデフォルトで信頼する CA のリストを閲覧、管理するには、**Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Default Trusted Certificate Authorities**（デフォルトの信頼された証明機関）を選択します。



組織が必要とする信頼できるエンタープライズ CA だけを追加できます—「証明書の取得」を参照してください。

証明書の失効

Palo Alto NetworksのファイアウォールおよびPanoramaでは、デジタル証明書を使用して、安全な通信セッションにおける両者間の信頼を実現します。証明書の失効状態を確認するようにファイアウォールやPanoramaを設定することで、セキュリティが強化されます。失効した証明書を提示する相手を信頼することはできません。証明書がチェーンの一部である場合、ファイアウォールあるいはPanoramaで失効状態を検証できないルート CA 証明書を除けば、そのファイアウォールあるいはPanoramaによってチェーンのすべての証明書の状態が確認されます。

さまざまな状況により、有効期限前に証明書が無効化されていることがあります。たとえば、名前が変更された場合や、サブジェクトと認証局間の関連付けが変更された（従業員の雇用が終了したなど）場合、秘密鍵の侵害が判明した、またはその疑いがある場合などです。このような状況では、証明書を発行した認証局が証明書を無効化する必要があります。

ファイアウォールおよびPanoramaでは、証明書の失効状態を検証するために以下の方法がサポートされています。両方の方法を設定すると、ファイアウォールあるいはPanoramaはまず OCSP の方法を試します。OCSP サーバーが使用できない場合は、CRL の方法を使用します。

- 証明書失効リスト (CRL)
- Online Certificate Status Protocol (OCSP)

PAN-OS では、証明書の失効状態の検証はオプションの機能です。認証ポータル、*GlobalProtect*、サイト間 *IPSec VPN* のユーザーおよびデバイス認証、およびファイアウォールあるいは *Panorama* への *Web*インターフェース アクセスを定義する証明書プロファイルでは、この機能を有効にして、証明書が無効になっていないことを確認するのがベストプラクティスです。

証明書失効リスト (CRL)

各認証局（CA）では公開リポジトリに証明書失効リスト（CRL）を定期的に発行しています。CRL では失効した証明書をシリアル番号で特定します。CA が証明書を無効化すると、次回の CRL の更新にその証明書のシリアル番号が含まれます。ファイアウォールは、識別エンコード規則 (DER) およびプライバシー強化メール (PEM) 形式の CRL をサポートします。

Palo Alto Networks ファイアウォールでは、ファイアウォールの信頼された認証局のリストに記載されているすべての認証局の最新発行の CRL をダウンロードして、キャッシュします。キャッシュは検証済みの証明書のみで実施されます。ファイアウォールで証明書の検証が行われたことがない場合、ファイアウォールのキャッシュには発行認証局の CRL は保存されていません。また、キャッシュが CRL を保存するのは、有効期限が切れるまでに限ります。

複数の *CRL* 分散ポイント *(CDP)* を設定しており、ファイアウォールが *CDP* に到達できない場合、ファイアウォールは残りの *CDP* をチェックしません。無効な *CRL* リクエストをリダイレクトするには、代替サーバーとしてDNS プロキシを設定します。

インバウンドおよびアウトバウンドの SSL/TLS トラフィックの復号化で使用される証明書の失効状態を検証するために CRL を使用するには、SSL/TLS 復号化に使用する証明書の失効状態検証の設定を参照してください。

ユーザーおよびデバイスを認証する証明書の失効状態を検証するために CRL を使用するには、証明書プロファイルを設定して、次のアプリケーション固有のインターフェイスにその証明書プロファイルを割り当てます：認証ポータル、GlobalProtect （リモート ユーザーとサイト間または大規模）、サイト間 IPSec VPN、あるいはPalo Alto Networksのファイアウォールや Panoramaへの Webインターフェース アクセス。詳細については、証明書の失効状態検証の設定 を参照してください。

Online Certificate Status Protocol (OCSP)

クライアントは、SSL/TLS セッションを確立するときに、オンライン証明書ステータス プロトコル（OCSP）を使用して、認証証明書の失効状態を確認できます。認証側のクライアントは OCSP レスポンダ（サーバー）に証明書のシリアル番号を含む要求を送信します。レスポンダは、証明書を発行した認証局（CA）のデータベースを検索して、状態（正常、無効化、または不明）を含む応答をクライアントに返します。OCSP の方法のメリットは、CRL の発行頻度（毎時、毎日、毎週）に依存することなく、状態をリアルタイムに検証できることです。

Palo Alto Networks ファイアウォールでは、ファイアウォールの信頼された認証局リストに記載されているすべての認証局の OCSP 状態情報をダウンロードして、キャッシュします。キャッシュは検証済みの証明書のみで実施されます。ファイアウォールで証明書の検証が行われたことがない場合、ファイアウォールのキャッシュには発行認証局の OCSP 情報は保存されていません。組織に独自の公開鍵基盤（PKI）がある場合、ファイアウォールを OCSP レスポンダとして設定できます（OCSP レスポンダの設定を参照）。

ファイアウォールが SSL フォワード プロキシとして機能している場合、証明書の失効状態を検証するために OCSP を使用するには、SSL/TLS 復号化に使用する証明書の失効状態検証の設定に記載されている手順を実行します。

次のアプリケーションでは、ユーザーやデバイスを認証するために証明書を使用します：キャプティブ ポータル、GlobalProtect （リモート ユーザーとサイト間または大規模）、サイト間 IPSec VPN、または Palo Alto Networks のファイアウォールや Panorama への Web インターフェイス アクセス。OCSP を使用して証明書の失効状態を検証するには、以下の手順を実行します。

- OCSP レスポンダを構成します（ファイアウォールを OCSP レスポンダとして構成している場合）。
- ファイアウォール上で HTTP OCSP サービスを有効化します（ファイアウォールを OCSP レスポンダとして構成している場合）。
- アプリケーションごとに証明書を作成または取得します。
- アプリケーションごとに証明書プロファイルを設定します。
- 該当するアプリケーションに証明書プロファイルを割り当てます。

OCSP レスポンダを使用できない状況に対処するには、CRL をフォールバック方法として設定します。詳細については、証明書の失効状態検証の設定 を参照してください。

証明書のデプロイメント

Palo Alto NetworksのファイアウォールあるいはPanoramaの証明書をデプロイする基本的なアプローチは以下のとおりです。

- **Obtain certificates from a trusted third-party CA**[信頼されたサードパーティ CA から証明書を取得する] — VeriSign、GoDaddy などの信頼されたサードパーティ証明書認証局（CA）から証明書を取得するメリットは、一般的なブラウザには、信頼されたルート証明書ストア内にある既知の CA のルート CA 証明書が含まれているため、エンド クライアントが証明書を信頼済みであることです。そのため、クライアントにファイアウォールあるいはPanoramaとの安全な接続の確立を要求するアプリケーションでは、クライアントにルート CA 証明書を事前にデプロイする必要がないように、クライアントが信頼する CA から証明書を購入します（このようなアプリケーションには GlobalProtect ポータル、GlobalProtect モバイル セキュリティ マネージャがあります）。 ただし、ほとんどのサードパーティ CA は署名証明書を発行することができません。そのため、このタイプの証明書は、ファイアウォールが証明書を発行する必要のあるアプリケーション（SSL/TLS 復号化および大規模 VPN など）には適していません。外部 CA からの証明書の取得を参照してください。
- **Obtain certificates from an enterprise CA**[エンタープライズ CA から証明書を取得する] — 独自の CA がある組織では、その CA を使用してファイアウォール アプリケーションの証明書を発行し、その証明書をファイアウォールにインポートできます。このメリットは、エンド クライアントがそのエンタープライズ CA を信頼済みである可能性が高いことです。必要な証明書を生成してファイアウォールにインポートするか、ファイアウォールで証明書署名要求（CSR）を生成して、署名を得るためエンタープライズ CA にその要求を送信します。この方法のメリットは、秘密鍵がファイアウォール外に出ないことです。また、エンタープライズ CA は、ファイアウォールが自動的に証明書を生成するために使用する署名証明書を発行することもできます（GlobalProtect 大規模 VPN または SSL/TLS 復号化を要求するサイトなど）。証明書および秘密鍵のインポートを参照してください。
- 自己署名証明書を生成 – ファイアウォールで自己署名ルート CA 証明書の作成を行い、その証明書を使用して他のファイアウォール アプリケーションの証明書を自動的に発行できます。

  この方法を使用して、アプリケーションの証明書を作成し、アプリケーションでクライアントにその証明書を信頼することを要求する場合、ルート *CA* 証明書がエンドユーザーの信頼済みのルート証明書ストアにないため、エンド ユーザーに証明書エラーが表示されます。これを回避するには、すべてのエンド ユーザー システムに自己署名ルート *CA* 証明書をデプロイします。手動で証明書をデプロイしたり、*Active Directory* の *Group Policy Object*（*GPO*）などの中央管理されたデプロイメント方法を使用したりできます。

証明書失効状態の検証の設定

証明書の失効状態を検証する場合、ファイアウォールはオンライン証明書ステータス プロトコル（OCSP）または証明書失効リスト（CRL）、あるいはその両方を使用します。これらの方法の詳細は、証明書の失効を参照してください。両方の方法を設定する場合は、ファイアウォールではまず OCSP を試行します。OCSP レスポンダを使用できない場合に限り、CRL 方法にフォールバックします。組織に独自の公開鍵基盤（PKI）がある場合、ファイアウォールを OCSP レスポンダとして機能するように設定できます。

以下のトピックでは、証明書の失効状態を検証するためのファイアウォールの設定方法を説明します。

- OCSP レスポンダの設定
- 証明書の失効状態検証の設定
- SSL/TLS 復号化に使用する証明書の失効状態検証の設定

OCSP レスポンダの設定

証明書の失効状態を検証するためにオンライン証明書ステータス プロトコル（OCSP）を使用するには、OCSP レスポンダ（サーバー）にアクセスできるようにファイアウォールを設定する必要があります。OCSP レスポンダを管理する組織は、サードパーティの認証局（CA）でも構いません。組織に独自の公開鍵基盤（PKI）がある場合、外部の OCSP レスポンダを使用するか、ファイアウォール自体を OCSP レスポンダとして設定できます。OCSP の詳細については証明書の失効を参照してください。

新しい証明書を生成する場合にのみ、*OCSP* 応答者 証明書プロファイル を構成します (**Device** > 証明書管理 > 証明書 。**OCSP** レスポンダー を指定して、ファイアウォールが適切な *URL* を持つ *[*機関情報アクセス *(AIA)]* フィールドに入力し、証明書プロファイルで新しい証明書を指定するようにします。証明書プロファイルを構成しても、既存の証明書またはルート *CA* の証明書プロファイルは上書きされません。

OCSP 検証を有効にするか、証明書プロファイル で証明書の *AIA* フィールドをオーバーライドできます。証明書プロファイル構成は、*GlobalProtect* などのファイアウォールでホストされているサービスに対して認証を行う証明書で使用される証明書検証メカニズムを決定します。

STEP 1 | 外部の OCSP レスポンダを定義するか、ファイアウォール自体を OCSP レスポンダとして構成します。

1. **Device (デバイス)** > **Certificate Management (証明書管理)** > **OCSP Responder (OCSP レスポンダ)** を選択して **Add (追加)** をクリックします。
2. レスポンダの識別に使用する **Name**[名前]（最大 31 文字）を入力します。名前では大文字と小文字を区別します。英字、数字、スペース、ハイフン、およびアンダースコアのみを使用し、一意である必要があります。
3. ファイアウォールに仮想システム（vsys）が複数ある場合は、証明書の **Location** [場所]（vsys または **Shared** [共有]）を選択します。
4. **Host Name**[ホスト名]フィールドに、OCSP レスポンダのホスト名（推奨）または IP アドレスを入力します。IPv4 あるいは IPv6 アドレスを入力できます。PAN-OS はこの値から URL を自動的に導出し、検証する証明書にその URL を追加します。

   ファイアウォール自体を OCSP レスポンダとして設定する場合、ホスト名は、ファイアウォールが OCSP サービスに使用するインターフェイスの IP アドレスに解決される必要があります。
5. **OK** をクリックします。

STEP 2 | OCSP レスポンダのインターフェイス用管理インターフェイスをファイアウォールに使用させたい場合、ファイアウォール上で OCSP 通信を有効化します。そうでない場合は、次のステップに進んで代替インターフェイスを構成します。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Interfaces**（インターフェイス） > **Management**（管理）を選択します。
2. [ネットワーク サービス] セクションで、[**HTTP OCSP** チェック ボックスをオンにし、[**OK** をクリックします。

STEP 3 | OCSP レスポンダのインターフェイスとして別のインターフェイスを使用するには、OCSP サービスで使用するインターフェイスにインターフェイス管理プロファイルを追加します。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **Interface Mgmt (インターフェイス管理)** を選択します。
2. **Add**[追加] をクリックして新しいプロファイルを作成するか、既存のプロファイル名をクリックします。
3. **HTTP OCSP** チェックボックスをオンにして **OK** をクリックします。
4. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、ファイアウォールが OCSP サービスに使用するインターフェイスの名前をクリックします。ステップ 1で指定した OCSP の **Host Name (ホスト名)** をこのインターフェイスの IP アドレスに解決する必要があります。
5. **Advanced (詳細)** > **Other info (その他の情報)** を選択し、設定したインターフェイス管理プロファイルを選択します。
6. **OK**、**Commit (コミット)** の順にクリックします。

証明書の失効状態検証の設定

認証ポータル、GlobalProtect、サイト間 IPSec VPN などのアプリケーション、ならびにファイアウォールあるいは Panorama への Webインターフェース アクセスでは、ファイアウォールや Panorama は、証明書を使用してユーザーおよびデバイスを認証します。セキュリティを向上させるため、デバイス/ユーザー認証のために使用する証明書の失効状態を検証できるようにファイアウォールあるいはPanoramaを設定することをお勧めします。

STEP 1 | アプリケーションごとに証明書プロファイルを設定します。

1 つ以上のルート CA 証明書をプロファイルに割り当てて、ファイアウォールによる証明書の失効状態の検証方法を選択します。

さまざまなアプリケーションが使用する証明書の詳細は、キーおよび証明書を参照してください。

STEP 2 | 関連アプリケーションに証明書プロファイルを割り当てます。

証明書プロファイルを割り当てる手順は、証明書を必要とするアプリケーションによって異なります。

SSL/TLS 復号化に使用する証明書の失効状態検証の設定

ファイアウォールは、インバウンドとアウトバウンドの SSL/TLS トラフィックを復号化して、トラフィックの脅威を検査します。トラフィックを許可するセキュリティ ポリシー ルールを作成し、そのルールにセキュリティ プロファイルを適用する際は、類似の復号ポリシー ルールを作成して、そのトラフィックを復号化します。トラフィックを復号化しない場合、ファイアウォールはセキュリティ プロファイルを使用してトラフィックを検査できません (見えないものを検査することはできません)。ファイアウォールは、トラフィックを転送する前にトラフィックを再暗号化します。(SSLインバウンド インスペクションおよびSSLフォワード プロキシを参照。) ファイアウォールは、以下のように、復号化で使用される証明書の失効状態を検証するように設定できます。

SSL/TLS 復号化証明書の失効状態検証を有効にすると、セッションの確立プロセスにさらに時間がかかります。セッションのタイムアウト前に検証が完了していない場合、サイトへの初回のアクセスの試行が失敗する可能性があります。このような理由から、検証はデフォルトで無効になっています。

STEP 1 | 失効状態要求のサービス固有のタイムアウト間隔を定義します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** の順に選択し、Session Features (セッション機能) セクションで、**Decryption Certificate Revocation Settings (復号化証明書失効の設定)** を選択します。
2. ファイアウォールがオンライン証明書ステータス プロトコル（OCSP）と証明書失効リスト（CRL）のどちらの方法を使用して証明書の失効状態を確認しているかに応じて、以下の手順のいずれかまたは両方を実行します。ファイアウォールが両方を使用してい

る場合、ファイアウォールはまず OCSP を試行します。OCSP レスポンダを使用できない場合は、CRL の方法を試行します。

- CRL セクションで、**Enable**[有効化] チェックボックスをオンにして **Receive Timeout**[受信の有効期限] に入力します。これは、ファイアウォールが CRL サービスからの応答を待機する期間（1 ～ 60 秒）です。
- OCSP セクションで、**Enable**[有効化] チェックボックスをオンにして **Receive Timeout**[受信の有効期限] に入力します。これは、ファイアウォールが OCSP レスポンダからの応答を待機する期間（1 ～ 60 秒）です。

ステップ 2 で指定した **Certificate Status Timeout (**証明書の有効期限**)** の値に応じて、ファイアウォールでは、一方または両方の **Receive Timeout (**受信の有効期限**)** 期間が経過するまでのタイムアウトを登録することができます。

STEP 2 | 失効状態要求の合計タイムアウト間隔を定義します。

Certificate Status Timeout[証明書の有効期限] を入力します。これは、ファイアウォールが任意の証明書状態サービスからの応答を待機し、ステップ 3 でユーザーが必要に応じて定義したセッション ブロック ロジックを適用するまでの期間（1 ～ 60 秒）です。**Certificate Status Timeout**[証明書の有効期限] は、以下のように OCSP/CRL の **Receive Timeout**[受信の有効期限] に関連付けられます。

- OCSP および CRL の両方を有効化する場合 – ファイアウォールは、**Certificate Status Timeout**[証明書の有効期限] の値または 2 つの **Receive Timeout**[受信の有効期限] の値の合計のいずれか小さい方の期間の経過後に、要求のタイムアウトを登録します。
- OCSP のみを有効化する場合 – ファイアウォールは、**Certificate Status Timeout**[証明書の有効期限] の値または OCSP の **Receive Timeout**[受信の有効期限] の値のいずれか小さい方の期間の経過後に、要求のタイムアウトを登録します。
- CRL のみを有効化する場合 – ファイアウォールは、**Certificate Status Timeout**[証明書の有効期限] 値または CRL の **Receive Timeout**[受信の有効期限] 値のいずれか小さい方の期間の経過後に、要求のタイムアウトを登録します。

STEP 3 | 証明書の状態が 不明 であるか、失効状態の要求がタイムアウトの場合のブロック動作を定義します。

OCSP または CRL サービスが 不明 という証明書の失効状態を返すとき、ファイアウォールで SSL/TLS セッションをブロックする場合は、**Block Session With Unknown Certificate Status**（証明書の状態が不明なセッションをブロックする）チェックボックスをオンにします。その他の場合は、ファイアウォールはセッションを続行します。

要求のタイムアウトが登録された後に、ファイアウォールで SSL/TLS セッションをブロックする場合は、**Block Session On Certificate Status Check Timeout** [証明書の状態のチェックがタイムアウトしたセッションをブロックします] チェックボックスをオンにします。その他の場合は、ファイアウォールはセッションを続行します。

STEP 4 | **OK**、**Commit (**コミット**)** の順にクリックします。

マスター キーの設定

各ファイアウォールおよび Panorama 管理サーバーには、設定に含まれるすべての秘密鍵およびパスワードを暗号化して保護するデフォルトのマスターキーがあります（SSL フォワード プロキシ復号化に使用する秘密鍵など）。

できるだけ早くデフォルトのマスター キーを変更して、暗号化で一意のマスター キーを使用するよう徹底します。

高可用性 (HA) 構成では、マスター キーが HA ピア間で同期されないため、両方のファイアウォールで同じマスター キーを使用する必要があります。同じマスター キーを使用しない場合、HA 同期が正しく機能しません。

Panorama を使用してファイアウォールを管理している場合は、Panorama とすべての管理対象ファイアウォールで同じマスターキーを構成するか、管理対象ファイアウォールごとに一意のマスターキーを構成できます。HA 構成の管理対象ファイアウォールの場合、HA ピアごとに同じマスターキーを設定する必要があります。ファイアウォールが Panorama™ 管理サーバーによって管理されている場合は、Panorama からマスター キーを管理する を参照してください。

必ずマスターキーは安全な場所に保存するようにしてください。マスターキーは復元できません。また、デフォルトのマスターキーを復元する唯一の方法は、ファイアウォールの工場出荷時設定へのリセットだけです。

STEP 1 | Backup the configuration (設定のバックアップ)を行います。

STEP 2 | (HA のみ) 設定の同期化を無効化する。

この手順は、新しいマスター鍵を ファイアウォール HA ペアにデプロイする前に必要です。

新しいマスター鍵を ファイアウォール HA ペアにデプロイする前に、設定の同期化を無効にする必要があります。Panorama で管理される ファイアウォール の場合、新しいマスターキーを展開する前に 設定の同期化 を無効にしないと、Panorama はプライマリ ファイアウォール への接続を失います。

1. **Device** > 高可用性 > 全般 を選択し、セットアップ を編集します。
2. 設定の同期化の有効化 を無効にし、**OK** をクリックします。
3. 設定の変更を **Commit (コミット)** します。

STEP 3 | **Device (デバイス)** > **Master Key and Diagnostics (マスター キーおよび診断)** の順に選択し、Master Key (マスター キー) セクションを編集します。

STEP 4 | すでにマスター キーがある場合は、**Current Master Key**[現在のマスター キー] に入力します。

STEP 5 | 新しい **New Master Key**（新規マスター キー）を定義して、**Confirm New Master**（マスター キーの確認）を定義します。キーは、厳密に 16 文字である必要があります。

STEP 6 | マスター キーの **Life Time (**ライフ タイム**)** を指定するには、キーが期限切れになるまでの期間を **Days (**日数**)** と **Hours (**時間数**)** またはいずれかで指定します。

現在のキーが失効する前に新しいマスター キーを設定する必要があります。マスター キーが失効すると、ファイアウォールまたは Panorama は自動的にメンテナンス モードで再起動されます。次にファイアウォールの工場出荷時設定へのリセットを行う必要があります。

デバイスが実行する暗号化の回数に応じて、***Lifetime (***有効期間***)*** を *2* 年以内に設定します。デバイスが実行する暗号化の回数が多いほど、***Lifetime (***有効期間***)*** は短く設定する必要があります。重要な注意点は、マスター キーを変更する前に、一意の暗号化を使い切ってしまわないようにすることです。各マスター キーは、マスター キー値と *Initialization Vector (*初期化ベクトル*; IV)* 値に基づいて、最大 2^{32} までの一意の暗号化を供給できます。一意の暗号化が 2^{32} に達すると、暗号化が繰り返され *(*一意ではなくなり*)*、セキュリティ リスクとなります。

マスター キーに***Time for Reminder (***リマインダーの時間***)*** の値 *(*次の手順を参照*)* を設定し、リマインダー通知が発生したら、マスター キーを変更します。

STEP 7 | マスター キーが失効する前にファイアウォールで失効アラームを生成するまでの **Days (**日数**)** および **Hours (**時間**)** を指定する **Time for Reminder (**リマインダーの時間**)** を入力します。ファイアウォールは System Alarms（システム アラーム）ダイアログを自動的に開いてアラームを表示します。

スケジュール済みメンテナンス ウィンドウで、有効期限が切れる前に新しいマスター キーを設定する時間が十分取れるよう、リマインダーを設定します。***Time for Reminder (***リマインダーの時間***)*** が期限に達し、ファイアウォールまたは *Panorama* が通知ログを送信したら、***Lifetime (***有効期間***)*** の有効期限切れを待たずに、マスター キーを変更します。グループ化されたデバイスの場合、すべてのデバイス *(Panorama* 管理のファイアウォールやファイアウォール *HA*ペアなど*)* を追跡し、グループ内にあるいずれかのデバイスでリマインダー値が期限に達したら、マスター キーを変更します。

失効アラームを表示するには、***Device***（デバイス）**>** ***Log Settings***（ログ設定）を選択し、*Alarm Settings*（アラーム設定）を編集して、***Enable Alarms***（アラームを有効化）します。

STEP 8 | **Auto Renew Master Key (**マスターキーの自動更新**)** を有効にして、マスターキーを自動的に更新するようにファイアウォールを構成します。**Auto Renew With Same Master Key (**同じマスターキーで自動更新**)** を設定するには、同じマスターキーを更新する **Days (**日数**)** と **Hours (**時間**)** またはいずれかを指定します。キー拡張により、ファイアウォールは動作し続け、ネットワークの保護を継続することができます。既存のマスター キーの有効期限がすぐに切れる場合、新しいキーを設定するための代替にはなりません。

マスター キーの自動更新には利点とリスクがあります。利点は、マスター キーの **Lifetime (**有効期間**)** を延ばせば、マスター キーの有効期限が切れる前にマスター キーを変更できない事態を防げることです。リスクは、デバイスがマスター キーで実行する暗号化の数が、マス

ター キーが生成できる一意の暗号化の数 (2^{32} の一意の暗号化) を超えると、暗号化が繰り返され、セキュリティ リスクが発生することです。

マスター キーの有効期限が切れた (自動更新せず、適時交換しない) 場合、デバイスはメンテナンス モードになります。

Auto Renew Master Key (マスター キーの自動更新)を有効にする場合は、デバイスが一意の暗号化を使い切らないように、合計時間 (有効期間と自動更新時間) を設定します。たとえば、デバイスが 2 年半でマスター キーの一意の暗号化の数を消費することが見込まれる場合、***Lifetime*** (有効期間) を 2 年間に設定し、***Time for Reminder*** (リマインダーの時間) を 60 日間に設定できます。***Auto Renew Master Key*** (マスター キーの自動更新)は 60～90 日間に設定し、***Lifetime*** (有効期間) の期限が切れる前に新しいマスター キーを設定する時間の余裕があるようにします。ただし、ベストプラクティスは、有効期限が切れる前にマスター キーを変更して、デバイスが暗号化を繰り返さないようにすることです。

キーの有効期限が切れた後に自動更新されるようにマスターキーを構成するときは、次に利用可能なメンテナンスウィンドウまでの日数を考慮してください。

STEP 9 | （任意）追加したセキュリティ用に、マスター キーを暗号化するために **HSM** を使用するかどうかを選択します。詳細についてはHSM を使用したマスター キーの暗号化を参照してください。

STEP 10 | **OK**、**Commit** (コミット) の順にクリックします。

STEP 11 | (HA のみ)設定の同期化 を再度有効にします。

1. **Device** > 高可用性 > 全般 を選択し、セットアップ を編集します。
2. 設定の同期化の有効化 を有効にして **OK** をクリックします。
3. 設定の変更を **Commit** (コミット) します。

マスター キーの暗号化

物理的および仮想的な Palo Alto Networks デバイスでは、AES-256-CBC または AES-256-GCM (PAN-OS 10.0で導入) 暗号化アルゴリズムを使用してキーやパスワードなどのデータを暗号化するようマスター キーを設定できます。AES-256-GCM は、AES-256-CBC よりも強力な暗号化を提供し、セキュリティ体制を改善します。また、組み込みの整合性チェックも含まれています。マスター キーは、設定された暗号化アルゴリズムを使用して、ファイアウォールと Panorama に保存されている機密データを暗号化します。暗号化アルゴリズムを AES-256-GCM に設定した場合でも、HSM を使用して、HSM に保存されている暗号化キーでマスターキーを暗号化できます。

マスター キーがデータの暗号化に使用するデフォルトの暗号化アルゴリズムは AES-256-CBC です。これは、PAN-OS 10.0より前のマスター キーと同じアルゴリズムです。Panorama を使用して ファイアウォール を管理する場合、管理対象の ファイアウォール は異なる PAN-OS で動作している可能性があり、PAN-OS 10.2 より前の PAN-OS で動作している ファイアウォール は AES-256-GCM をサポートしていないため、AES-256-CBC がデフォルトの暗号化レベルになります。Panorama が管理対象デバイスが使用できる最低レベルの暗号化を使用する必要があるのはこのためです。たとえば、一部の管理対象デバイスが PAN-OS 10.2 で動作し、一部のデバイスが以前のバージョンで動作している場合、Panorama は AES-256-CBC を使用する必要があります。ただし、すべての管理対象デバイスが PAN-OS 10.2 以降で動作している場合、Panorama とそのすべての管理対象デバイスは AES-256-GCM を使用できます。

Panorama とその管理対象デバイスで同じ暗号化レベルを使用し、ファイアウォール ペアで同じ暗号化レベルを使用します。デバイスをアップグレードして、可能な限り最強の暗号化アルゴリズムを使用するようにします。すべての *Panorama* 管理デバイスが *PAN-OS 10.0*を実行している場合は、すべてのデバイスで *AES-256-GCM* を使用します。異なる暗号化レベルを使用する管理対象デバイスまたはペアリングされたデバイスの設定は、同期しなくなる可能性があります。

暗号化アルゴリズムを AES-256-GCM に変更すると、デバイスは AES-256-CBC の代わりにそれを使用して機密データを暗号化します。あるアルゴリズムから別のアルゴリズムに変更する場合、次のいずれかを指定することもできます：

- 新しいアルゴリズムを使用して、既存の暗号化されたデータを再暗号化する。
- 既存のデータを古い暗号化アルゴリズムで暗号化したままにし、新しい (将来使用する) 暗号化にのみ新しいアルゴリズムを使用する。

デフォルトでは、暗号化アルゴリズムを変更すると、デバイスは新しいアルゴリズムを使用して、既存の暗号化されたデータを再暗号化し、新しいデータを暗号化します。*Panorama* を使用してデバイスを管理している場合、それらは異なるバージョンの *PAN-OS* 上にあり、最新の暗号化アルゴリズムをサポートしていない可能性があります。暗号化アルゴリズムを変更したり、すでに暗号化されているデータを再暗号化する前に、 *Panorama* とその管理対象デバイスがサポートする暗号化アルゴリズムを必ず理解してください。

- マスター キーの暗号化レベルの設定

- ファイアウォール HA ペアのマスター キーの暗号化
- マスターキーの暗号化ログ
- AES-256-GCM　用の固有のマスター キーの暗号化

マスター キーの暗号化レベルの設定

CLI を使用して、マスター キーの暗号化アルゴリズム レベルと、現在暗号化されているすべてのデータを新しい暗号化アルゴリズム レベルで再暗号化するかどうかを設定します。キーワードの順序に応じて暗号化レベルを変更したり、暗号化レベルを変更して以前に暗号化されたデータを再暗号化したりすることも可能です。

以下の操作 CLI コマンドは、暗号化レベルを変更し、指定した暗号化レベルで現在暗号化されているすべてのデータを自動的に再暗号化します。

```
admin@PA-NGFW>request encryption-level level <0|1|2>
```

以下の操作 CLI コマンドは、暗号化レベルを変更し、現在暗号化されているすべてのデータを新しい暗号化レベルで再暗号化するかどうかを指定します。

```
admin@PA-NGFW>request encryption-level re-encrypt <yes|no> level <0|
1|2>
```

キーワード	オプション
レベル	**0** = デフォルトのアルゴリズム (AES-256-CBC) を使用してデータを暗号化します **1** = AES-256-CBC アルゴリズムを使用してデータを暗号化します **2** = AES-256-GCM アルゴリズムを使用してデータを暗号化します ファイアウォールは、現在暗号化されているすべてのデータを再暗号化し、指定されたアルゴリズムを使用して新しい機密データを暗号化します。新しいアルゴリズムで既存の暗号化データを再暗号化しない場合は、コマンド文字列で **re-encrypt no** を指定します。これにより、ファイアウォールがすでに暗号化したデータを自動的に再暗号化するのを防ぎます。

キーワード	オプション
	AES-256-GCM は、*Panorama* とそのすべての管理対象デバイス (または *HA* ペアの両方のデバイス) が *PAN-OS 10.2* 以降を実行し、すべてのデバイスが *AES-256-GCM* を使用するように構成する場合にのみ使用してください。異なる暗号化レベルを使用する管理対象デバイスまたはペアリングされたデバイスは、同期しなくなる可能性があります。
再暗号化	**no** = 現在暗号化済みのデータは再暗号化しません。ファイアウォールは現在暗号化済みのデータを再暗号化しません。現在暗号化されているデータは、ファイアウォールがデータの暗号化に元々使用したアルゴリズムで暗号化されたままになります。ファイアウォールは、指定されたアルゴリズムだけを使用して、今後は機密データを暗号化します。 **yes** = 現在暗号化されているデータを指定されたアルゴリズムで再暗号化し、そのアルゴリズムを使用して、今後は機密データを暗号化します。

操作 CLI コマンド **show system masterkey-properties** を使用して、デバイスに現在設定されている暗号化アルゴリズム (レベル) を確認します。次に例を示します。

```
admin@PA-NGFW>show system masterkey-properties
```

```
Master key expires at: unspecified
Reminders will begin at: unspecified
Master key on hsm: no
Automatically renew master key lifetime: 0Encryption Level: 1{{{防御>防御<防御}>{防御>防御<防御}<{防御>防御<防御}}>{{防御>防御<防御}>{防御>防御<防御}<{防御>防御<防御}}<{{防御>防御<防御}>{防御>防御<防御}<{防御>防御<防御}}}
```

出力は、現在の暗号化レベルが1、つまりAES-256-CBCであることを示しています。

以前のバージョンの PAN-OS にダウングレードすると、デバイスは暗号化アルゴリズムをダウングレードされた PAN-OS バージョンがサポートするレベルに自動的に戻し、そのレベルを使用して暗号化されたデータを自動的に再暗号化して、必要に応じてデバイスがデータを復号化して使用できるようにします。たとえば、デバイスが PAN-OS 10.2 上にあり、暗号化アルゴリズムとして AES-256-GCM (以前のバージョンの PAN-OS ではサポートされていません) を使用していて、PAN-OS 9.1 にダウングレードした場合、デバイスは暗号化されたデータを PAN-OS 9.1 でサポートされている AES-256-CBC に再暗号化します。

ファイアウォール HA ペアのマスター キーの暗号化

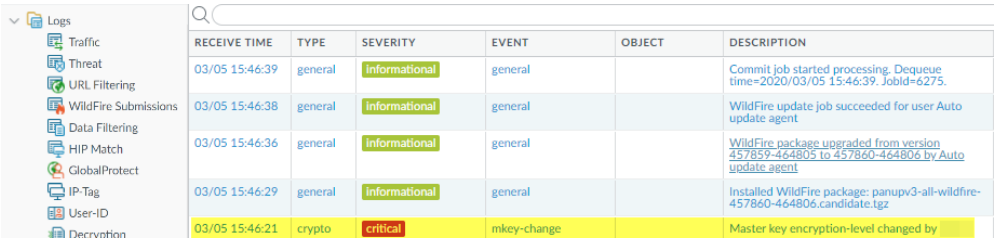
ファイアウォール高可用性 (HA) ペアで AES-256-GCM 暗号化レベルを使用するには、両方のファイアウォールが AES-256-GCM をサポートするよう PAN-OS 10.0 を実行しなければなりません。HA ペアのいずれかのファイアウォールが PAN-OS 10.0 以前のバージョンで動作している場合は、AES-256-GCM を使用できません。両方のファイアウォールが PAN-OS 10.0 の場合、どちらのファイアウォールも AES-256-CBC または AES-256-GCM の暗号化キーをデコードできるため、いずれの暗号化レベルも使用できます。ただし、同期が外れる可能性を回避するために、両方のファイアウォールで同じ暗号化レベルを使用する必要があります。

HA ペア内の両方のファイアウォールで *AES-256-GCM* 暗号化を使用します。*AES-256-GCM* または *AES-256-CBC* のどちらを使用する場合も、両方のファイアウォールで同じアルゴリズムを使用します。

両方のファイアウォールが PAN-OS 10.0 を実行している HA ペアでは、HA を無効にしてファイアウォールの暗号化レベルを変更する必要はありません。

マスターキーの暗号化ログ

マスターキーの暗号化アルゴリズム (レベル) を変更すると、ファイアウォールはシステム ログを生成します (**Monitor (監視)** > **Logs (ログ)** > **System (システム)**)。



システムログの中で、マスターキー暗号化に関するログのみを表示する場合は、**Type (タイプ)** crypto: **(subtype eq crypto)**のフィルタを作成します。

AES-256-GCM　用の固有のマスター キーの暗号化

マスター キーは、有限数の一意の暗号化のみを生成でき、一意の組み合わせがなくなると暗号化を繰り返す必要があります。ファイアウォールは、初期化ベクトル (IV) を使用した AES-256-GCM 暗号化アルゴリズムを使用して一意の暗号化を作成します。IV は任意の番号であり、暗号化を作成するために1回だけ使用して、各暗号化が一意であることを確認する必要があります。

マスター キーと IV を使用する各暗号化は、偽造攻撃を防ぐために一意である必要があります。ファイアウォールは、2 つ以上の異なる入力データセットにおいて、同一の IV と同一の鍵を使用して認証された暗号化が作成される確率が2^{32}以下であるという一意性の要件を満たしています。

IV がその一意の値をすべて実行すると、IV 値が繰り返されます。IV 値が繰り返される場合、同じマスター キーと繰り返される IV 値を使用してデータを暗号化すると、他のデータで以前に使用した暗号化と同じ暗号化と同じになります。システムが一意の暗号化を使い果たす前にマスター キーを変更して、ファイアウォールが複数の機密データで同じ暗号化 (マスター キーと IV

値の組み合わせ) を使用しないようにします。一意の暗号化の組み合わせを繰り返したり、再利用したりしないでください。

マスター キーをいつ変更する必要があるかを追跡するには、各アプライアンスでマスター キー **Lifetime (**有効期間**)** と **Reminder (**リマインダー**)** の値を設定します (**Device (**デバイス**)** > **Master Key and Diagnostics (**マスター キーおよび診断**)**を実行し、マスター キーを編集します)。マスター キー暗号化の予想量に基づいて値を控えめに設定し、すべての暗号化が一意であり、暗号化の組み合わせが繰り返されたり再利用されたりしないようにします。

証明書の取得

自己署名ルート CA 証明書の作成

自己署名ルート認証局（CA）証明書は、証明書チェーンで最上位の証明書です。ファイアウォールはこの証明書を使用して、他の用途のために証明書を自動的に発行できます。たとえば、ファイアウォールは、SSL/TLS 復号化や、GlobalProtect 大規模 VPN でのサテライトのための証明書を発行します。

ファイアウォールとの安全な接続が確立する場合、リモート クライアントは証明書を発行したルート CA を信頼する必要があります。信頼しない場合、証明書が無効であり（セキュリティ設定に応じて）接続をブロックする可能性があるという警告がクライアント ブラウザに表示されます。これを回避するため、自己署名ルート CA 証明書の生成後、クライアント システムにこの証明書をインポートします。

Palo Alto Networks のファイアウォールあるいは*Panorama*では、自己署名証明書を生成できます（ただし、*CA* 証明書に限ります）。

STEP 1 | **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択します。

STEP 2 | ファイアウォールに仮想システム（vsys）が複数ある場合は、証明書の **Location** [場所]（vsys または **Shared** [共有]）を選択します。

STEP 3 | **Generate**（生成）をクリックします。

STEP 4 | **Certificate Name** [証明書名]に「**GlobalProtect_CA**」などの名前を入力します。名前は大文字小文字を区別し、ファイアウォールでは最大 63 文字、Panorama では最大 31 文字を使用できます。英字、数字、ハイフン、およびアンダースコアのみを使用し、一意である必要があります。

STEP 5 | **Common Name**[共通名] フィールドに、証明書を使用するサービスを設定するインターフェイスの FQDN（推奨）または IP アドレスを入力します。

STEP 6 | ファイアウォールに仮想システム（vsys）が複数あり、どの vsys でも証明書を使用できるようにする場合は、**Shared** [共有]チェック ボックスをオンにします。

STEP 7 | **Signed By**[署名者] フィールドは空白のままにし、証明書を自己署名として指定します。

STEP 8 | （必須）**Certificate Authority** [認証局]チェック ボックスをオンにします。

STEP 9 | **OCSP Responder** [OCSP レスポンダ]フィールドは空白のままにします。ルート CA 証明書には失効状態検証が適用されません。

STEP 10 | **Generate**[生成]、**Commit**[コミット] の順にクリックします。

証明書の生成

Palo Alto NetworksのファイアウォールおよびPanoramaは、証明書を使用して、SSL/TLS 復号化、認証ポータル、GlobalProtect、サイト間 IPSec VPNなどのアプリケーションにおいて、ならびにファイアウォール/Panoramaへの Webインターフェース アクセスにおいて、クライアント、サーバー、ユーザー、およびデバイスを認証します。使用するたびに証明書を生成します（詳細はキーおよび証明書を参照）。

証明書を生成するためには、まず自己署名ルート CA 証明書の作成を行うか、あるいはインポート（証明書および秘密鍵のインポート）して署名します。証明書の失効状態を検証するためにオンライン証明書ステータス プロトコル（OCSP）を使用するには、証明書を生成する前に、OCSP レスポンダの設定を行います。

STEP 1 | **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択します。

STEP 2 | ファイアウォールに仮想システム（vsys）が複数ある場合は、証明書の **Location** [場所]（vsys または **Shared** [共有]）を選択します。

STEP 3 | **Generate**（生成）をクリックします。

STEP 4 | SCEP 証明書を GlobalProtect エンドポイントにデプロイしない場合を除き、**Certificate Type**（証明書タイプ）として**Local**（ローカル）（デフォルト設定）を選択します。

STEP 5 | **Certificate Name**（証明書名）を入力します。名前は大文字小文字を区別し、ファイアウォールでは最大 63 文字、Panorama では最大 31 文字を使用できます。英字、数字、ハイフン、およびアンダースコアのみを使用し、一意である必要があります。

STEP 6 | **Common Name**[共通名] フィールドに、証明書を使用するサービスを設定するインターフェイスの FQDN（推奨）または IP アドレスを入力します。

STEP 7 | ファイアウォールに仮想システム（vsys）が複数あり、どの vsys でも証明書を使用できるようにする場合は、**Shared** [共有]チェック ボックスをオンにします。

STEP 8 | **Signed By**[署名者] フィールドで、証明書を発行するルート CA 証明書を選択します。

STEP 9 | (Optional) **Block Private Key Export** にするかどうかを選択します。

この設定を有効にすると、export the certificate のときに秘密キーがエクスポートされないようにします。

この設定を有効にした場合、import the certificate の場合は、関連付けられた秘密キーを *Panorama* または他の *firewall* に手動でインポートする必要があります。*Panorama* によって管理される *firewalls* の場合、証明書のインポート先の管理対象 *firewalls* に構成変更を正常にプッシュするには、秘密鍵が必要です。

STEP 10 | （任意）**OCSP Responder** [OCSP レスポンダ]を選択します。

STEP 11 | 鍵生成の **Algorithm** [アルゴリズム]に、**RSA**（デフォルト）または **Elliptic Curve DSA**（ECDSA）を選択します。クライアント ブラウザおよびそれをサポートするオペレーティング システムでは、ECDSA をお勧めします。

PAN-OS 6.1 より前のリリースを実行しているファイアウォールでは、*Panorama*™ からプッシュした *ECDSA* 証明書が削除されます。また、これらのファイアウォールでは、*ECDSA* 認証局（*CA*）によって署名された *RSA* 証明書が無効になります。

ハードウェア セキュリティ モジュール（HSM）を使用して、SSL/TLS 複合に使用する ECDSA キーを保存することはできません。

STEP 12 | **Number of Bits** [ビット数]を選択して、証明書鍵の長さを定義します。数値が大きいほど安全性が高まりますが、処理に時間がかかります。

STEP 13 | **Digest** [ダイジェスト]アルゴリズムを選択します。セキュリティが高いオプションの順：**sha512**, **sha384**, **sha256** (default), **sha1**, と **md5**.

TLSv1.2 に依存するファイアウォール サービス（*Web* インターフェイスへの管理者アクセスなど）の要求時に使用するクライアント証明書に、ダイジェスト アルゴリズムとして ***sha512*** を含めることはできません。クライアント証明書でより低いダイジェスト アルゴリズム（***sha384*** など）を使用するか、ファイアウォール サービス用の CSSL/TLS サービス プロファイルの設定を行う際に、***Max Version***（最大バージョン）を ***TLSv1.1*** に制限する必要があります。

STEP 14 | **Expiration** [有効期限]に、証明書が有効である日数（デフォルトは 365）を入力します。

STEP 15 | （任意）証明書を使用するファイアウォールおよびサービスを一意に特定するための **Certificate Attributes**（証明書の属性）を **Add**（追加）します。

証明書のサブジェクト代替名 *(SAN)* フィールドをホスト名が決定し、証明書が保護するドメインを *SAN* が指定することを求めるブラウザが存在するため、***Host Name (***ホスト名*) (DNS* 名*)* 属性を追加する場合は、***Common Name (***共通名*)*と同じにすることが推奨されます。さらに *GlobalProtect* では、***Common Name (***共通名*)*と一致する ***Host Name (***ホスト名*)* が必要になります。

STEP 16 | **Generate** [生成]をクリックして、Device Certificates [デバイス証明書]ページで Certificate Name [証明書名]をクリックします。

ファイアウォールが属するタイムゾーンに関わらず、証明書が有効な時間や有効期限はグリニッジ標準時（*GMT*）で表示されます。

STEP 17 | ファイアウォールでの証明書の使用目的に該当するチェックボックスをオンにします。

たとえば、ファイアウォールが、外部 syslog サーバーへの syslog の転送を保護するためにこの証明書を使用する場合は、**Certificate for Secure Syslog (**保護された **Syslog** の証明書**)** チェック ボックスをオンにします。

STEP 18 | **OK**、**Commit (**コミット**)** の順にクリックします。

証明書および秘密鍵のインポート

組織に独自の公開鍵基盤（PKI）がある場合、組織の認証局（CA）からファイアウォールに証明書および秘密鍵をインポートできます。エンタープライズ CA 証明書（信頼されたサードパーティ CA から購入した大半の証明書ではなく）では、SSL/TLS 復号化または大規模 VPN などのアプリケーション用の CA 証明書を自動的に発行できます。

Palo Alto Networks のファイアウォールあるいは*Panorama*では、自己署名証明書をインポートできます（ただし、*CA* 証明書に限ります）。

すべてのクライアント システムに自己署名ルート *CA* 証明書をインポートするのではなく、エンタープライズ *CA* から証明書をインポートすることをお勧めします。これは、クライアントにエンタープライズ *CA* との信頼関係がすでにあり、デプロイメントが簡略化されるためです。

インポートする証明書が証明書チェーンの一部である場合、チェーン全体をインポートすることをお勧めします。

STEP 1 | エンタープライズ CA から、ファイアウォールが認証に使用する証明書と秘密鍵をエクスポートします。

秘密鍵をエクスポートする場合、転送用のキーを暗号化するパスフレーズを入力する必要があります。管理システムが証明書およびキー ファイルにアクセスできることを確認します。キーをファイアウォールにインポートするときは、同一のパスフレーズを入力してキーを復号化します。

STEP 2 | **Device** > **Certificate Management** > **Certificates** > **Device Certificates** (デバイス > 証明書の管理 > 証明書 > デバイス証明書)を選択します。

STEP 3 | ファイアウォールに仮想システム（vsys）が複数ある場合は、証明書の **Location** [場所]（vsys または **Shared** [共有]）を選択します。

STEP 4 | **Import**（インポート）をクリックして、**Certificate Name**（証明書名）を入力します。名前は大文字小文字を区別し、ファイアウォールでは最大 63 文字、Panorama では最大 31 文

字を使用できます。英字、数字、ハイフン、およびアンダースコアのみを使用し、一意である必要があります。

STEP 5 | すべての仮想システムで証明書を使用できるようにするには、**[共有]** チェックボックスをオンにします。このチェックボックスは、ファイアウォールが複数の仮想システムをサポートしている場合に限り表示されます。

STEP 6 | CA から受信した **Certificate File**[証明書ファイル] のパスと名前を入力するか、**Browse**[参照] してファイルを検索します。

STEP 7 | 以下の **File Format**[ファイル 形式] を選択します。

- **Encrypted Private Key and Certificate (PKCS12)**[暗号化された秘密鍵と証明書（PKCS12）] – これは、デフォルトで最も一般的な形式であり、キーおよび証明書が単一のコンテナに（**Certificate File**[証明書ファイル]）格納されています。ハードウェア セキュリティ モジュール（HSM）がこの証明書の秘密鍵を保存する場合、**Private key resides on Hardware Security Module**[秘密鍵はハードウェア セキュリティ モジュール上にあります] チェックボックスをオンにします。
- **Base64 Encoded Certificate (PEM)**[Base64 エンコード済み証明書（PEM）] – 証明書とは別にキーをインポートする必要があります。ハードウェア セキュリティ モジュール（HSM）がこの証明書の秘密鍵を保存する場合、**Private key resides on Hardware Security Module (**秘密鍵はハードウェア セキュリティ モジュール上にあります**)** チェックボックスをオンにして、次のステップをスキップします。その他の場合は、**Import Private Key (**秘密鍵のインポート**)** チェックボックスをオンにして、**Key File (**キー ファイル**)** に入力するか、キー ファイルを **Browse (**参照**)** して次のステップに進みます。

> (*Panorama managed firewalls*) 証明書の生成時に **Block Private Key Export** を有効にした場合 を有効にした場合>*Panorama* 管理サーバーから管理対象の *firewalls* に構成変更を正常にプッシュするには ***Import Private Key*** が必要です。

STEP 8 | 秘密鍵の暗号化に使用する **[パスフレーズ]** に入力して、再入力（確認）します。

STEP 9 | **OK** をクリックします。Device Certificates [デバイス証明書]ページに、インポートされた証明書が表示されます。

外部 CA からの証明書の取得

外部認証局（CA）から証明書を取得するメリットは、秘密鍵がファイアウォール外に出ないことです。外部 CA から証明書を取得するには、証明書署名要求（CSR）を生成し、CA にその要求をサブミットします。CA が指定の属性を持つ証明書を発行したら、その証明書をファイアウォールにインポートします。CA は、一般的な公開 CA またはエンタープライズ CA です。

証明書の失効状態を検証するため、Online Certificate Status Protocol（OCSP）を使用するには、CSR を生成する前に、OCSP レスポンダの設定を行います。

STEP 1 | 外部 CA の証明書を要求します。

1. **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択します。
2. ファイアウォールに仮想システム（vsys）が複数ある場合は、証明書の **Location** [場所]（vsys または **Shared** [共有]）を選択します。
3. **Generate**（生成）をクリックします。
4. **Certificate Name**（証明書名）を入力します。名前は大文字小文字を区別し、ファイアウォールでは最大 63 文字、Panorama では最大 31 文字を使用できます。英字、数字、ハイフン、およびアンダースコアのみを使用し、一意である必要があります。
5. **Common Name**[共通名] フィールドに、証明書を使用するサービスを設定するインターフェイスの FQDN（推奨）または IP アドレスを入力します。
6. ファイアウォールに仮想システム（vsys）が複数あり、どの vsys でも証明書を使用できるようにする場合は、**Shared** [共有]チェック ボックスをオンにします。
7. **Signed By** [署名者]フィールドで、**External Authority (CSR)** [外部認証局（CSR）]を選択します。
8. 該当する場合、**[OCSP** レスポンダ**]** を選択します。
9. （任意）証明書を使用するファイアウォールおよびサービスを一意に特定するための **Certificate Attributes**（証明書の属性）を **Add**（追加）します。

   Host Name (ホスト名**)*** 属性を追加する場合は、***Common Name (***共通名**)*** に一致させる必要があります *(*これは、*GlobalProtect* では必須です*)*。このホスト名が、証明書の *Subject Alternative Name [*サブジェクト代替名*]* フィールドに入力されます。
10. **Generate**（生成）をクリックします。**Device Certificates**（デバイス証明書）タブに状態が `pending`（保留）である CSR が表示されます。

STEP 2 | CA に CSR をサブミットします。

1. CSR を選択し、**Export** [エクスポート]をクリックして、ローカル コンピュータに .csr ファイルを保存します。
2. CA に .csr ファイルをアップロードします。

STEP 3 | 証明書をインポートします。

1. CA が CSR に応答して署名証明書を送信した後、**Device Certificates**[デバイス証明書] タブに戻り、**Import**[インポート] をクリックします。
2. CSR の生成に使用した **Certificate Name (**証明書名**)** を入力します。
3. CA が送信した PEM **Certificate File**[証明書ファイル] のパスと名前を入力するか、**Browse**[参照] してファイルを検索します。
4. **OK** をクリックします。**Device Certificates**[デバイス証明書] タブに状態が `valid`[有効] になっている証明書が表示されます。

STEP 4 | 証明書を設定します。

1. 証明書の **Name**[名前] をクリックします。
2. ファイアウォールでの証明書の使用目的に該当するチェックボックスをオンにします。たとえば、ファイアウォールが、外部 syslog サーバーへの syslog の転送を保護するためにこの証明書を使用する場合は、**Certificate for Secure Syslog (**保護された **Syslog** の証明書**)** チェック ボックスをオンにします。
3. **OK**、**Commit (**コミット**)** の順にクリックします。

デバイス証明書のインストール

次世代ファイアウォールは、デバイスのテレメトリや IoT などのクラウド サービスを活用できます。これを行うためには、デバイス証明書をインストールして、Palo Alto Networks の カスタマー サポート ポータル (CSP) でファイアウォールの認証に成功させ、これらのクラウド サービスを活用する必要があります。デバイス証明書が必要な状況は機能ごとに異なるため、機能のセットアップ ドキュメントに、これを行う必要があると記載されている場合にのみ、デバイス証明書をインストールしてください。

デバイス証明書のインストールは1度だけ必要です。デバイス証明書を使用するすべての機能は、ファイアウォールにインストールされている証明書がすでに存在する場合はそれを使用します。

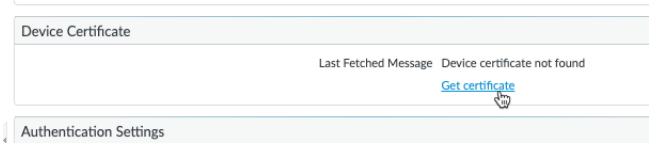
デバイス証明書は Panorama で管理されるファイアウォールにインストールすることができます。デバイス証明書を単一の次世代ファイアウォールに直接インストールする (つまりPanorama を使用していない)場合:

STEP 1 | ワンタイム パスワード（OTP）を生成します。

1. カスタマーサポート ポータルにログインします。
2. **Assets** > **Device Certificates**（デバイス証明書）および **Generate OTP**（**OTP**の生成）を選択します。
3. **Device Type**（デバイス タイプ）で、**Generate OTP for Next-Gen Firewalls (**次世代ファイアウォールの **OTP** を生成**)** を選択します。
4. **PAN OS** デバイスのシリアルナンバーを選択します。
5. **OTP** を生成して、OTP をコピーします。

STEP 2 | ご利用の次世代ファイアウォールに管理者ユーザーとしてログインします。

STEP 3 | **Device (**デバイス**)** > **Setup(**セットアップ**)** > **Management(**管理**)** > **Device Certificate(**デバイス証明書**)**の順に選択し、**Get certificate (**証明書を取得**)**します。



STEP 4 | 生成した **one-time password (** ワンタイム パスワード **- OTP)**を貼り付けて、 **OK** をクリックします。

STEP 5 | ご利用の次世代ファイアウォールは正常に証明書を取得し、インストールします。

SCEP を使用して証明書をデプロイする

エンタープライズ PKI に簡易証明書登録プロトコル（SCEP）サーバーがある場合は、SCEP プロファイルを設定して、一意のクライアント証明書の生成と配布を自動化できます。エンタープライズ PKI は SCEP クライアントからリクエストを受けた際にユーザー固有の証明書を生成し、その証明書を SCEP クライアントに送信します。つまり、SCEP のオペレーションは動的なものになります。その後、SCEP クライアントが証明書を透過的にクライアント デバイスへデプロイできるようになります。

GlobalProtect で SCEP プロファイルを使用して、各 GlobalProtect ユーザーにユーザー固有のクライアント証明書を割り当てることができます。この使用例では、GlobalProtect ポータルは、エンタープライズ PKI 内の SCEP サーバーに対する SCEP クライアントとして機能します。さらに、SCEP プロファイルを使用して、管理アクセスとデバイス間通信のために、また、他の Palo Alto Networks デバイスと Palo Alto Networks デバイスの相互認証のためにクライアント証明書を に割り当てることができます。

STEP 1 | SCEP プロファイルを作成します。

1. **Device** > **Certificate Management** > **SCEP**(デバイス > 証明書管理 > SCEP) の順に選択し、**Add**(追加) をクリックして新しいプロファイルを追加します。
2. SCEP プロファイルを識別する **Name**（名前）を入力します。
3. このプロファイルが複数の仮想システム容量のあるファイアウォール用であれば、仮想システムを選択するか、そのプロファイルを利用できる **Location**（場所）として **Shared**（共有）を選択します。

STEP 2 | （任意）SCEP ベースの証明書発行をより安全に行いたい場合は、各回の証明書要求について PKI およびポータルとの間に SCEP チャレンジレスポンス機能を設定します。

この機能の設定後はバックグラウンドで動作するため、追加の入力が必要になることはありません。

連邦情報処理標準（FIPS）に準拠するため、連邦情報処理標準（FIPS）に準拠するため、**Dynamic**（動的） SCEP要求を使用し、HTTPSを利用する**Server URL**（サーバーURL）を指定します。

以下のいずれかのオプションを選択します。

- **None**(なし) - （デフォルト）SCEPサーバーは証明書の発行前にポータルとのチャレンジを行いません。
- **Fixed**（固定） – PKI インフラストラクチャ内の SCEP サーバーから必須の登録パスワードを取得し、そのパスワードを Password（パスワード）フィールドに入力します。
- **Dynamic**（動的） – 任意のユーザー名およびパスワード（多くの場合は PKI 管理者の認証情報となります）と、ポータルのクライアントがこれらの認証情報を送信する SCEP **Server URL**（サーバー **URL**）を入力します。これは、証明書をリクエストする度にポータル用の OTP パスワードを透過的に生成する SCEP サーバーに認証するための認証情報を使用します。（各回の証明書要求の後、`The enrollment challengepassword is`（登録チャレンジパスワード）のフィールドの画面更新後にOTP の変更が表示されます） PKI はそれぞれの新しいパスワードをポータルへ透過的に受け渡し、また、証明書要求に対してそれらのパスワードを使用します。

STEP 3 | SCEP サーバーとポータル間の接続設定を指定し、ポータルがクライアント証明書をリクエスト・受信できるようにします。

証明書の**Subject**（サブジェクト）名でトークンを指定することで、クライアント デバイスまたはユーザーに関する補足的な情報を含めることができます。

ポータルは、SCEPサーバーへのCSRリクエストにトークンの値とホストIDを含めます。

1. PKI 内の SCEP サーバーにアクセスするためにポータルが使用する**Server URL**（サーバー **URL**）を設定します（例：`http://10.200.101.1/certsrv/mscep/`）。
2. SCEP サーバーを識別するための文字列（255 文字まで）を **CA-IDENT Name**（**CA-IDENT** 名）に入力します。
3. SCEP サーバーが生成する証明書に使用する **Subject**（サブジェクト）名を入力します。サブジェクトは、**<attribute>=<value>** の形式で識別される名前にして、共通名（CN）属性（**CN=<variable>**）を含める必要があります。CN は次のような動的なトークンをサポートしています。
   - `$USERNAME`—このトークンは、ポータルに特定のユーザーの証明書の要求を許可するために使用します。GlobalProtect でこの変数を使用するには、グループ マッピングの有効化も行う必要があります。ユーザーが入力したユーザー名は user-group マッピング テーブルの名前と一致する必要があります。
   - `$EMAILADDRESS`—このトークンは、特定の電子メール アドレスに関連付けられた証明書を要求するために使用します。この変数を使用するには、グループ マッピングの有効化を行い、Server Profile（サーバー プロファイル）の Mail Domains（メール ドメイン）セクションで **Mail Attributes**（メール属性）を設定する必要もあります。GlobalProtect がユーザーの電子メール アドレスを識別できない場合、一意の ID を生成してその値を含む CN を入力します。
   - `$HOSTID`—デバイスのみに対する証明書をリクエストするには、ホスト ID のトークンを指定します。ユーザーがポータルにログインしようと試みると、エンドポイントはホスト ID の値を含む、ユーザーを識別できる情報を送信します。GUID（Windows）、インターフェイスのMACアドレス（Mac）、Android ID（Androidデバイス）、UDID（iOSデバイス）、あるいはGlobalProtectが割り当てる一意の名前（Chrome）など、ホストIDの値はデバイスの種類によって異なります。
   - `$UDID`—UDID共通名属性を使用して、GlobalProtect のクライアントのデバイス UDID または Palo Alto Networks デバイス間の相互認証のデバイス シリアル番号に基づいて証明書を要求します。

   GlobalProtect ポータルがエージェントに SCEP 設定をプッシュする際、サブジェクト名の CN の部分は、証明書の所有者が持つ実際の値（ユーザー名、ホスト ID、または電子メール アドレス）に置き換えられます（例: **O=acme,CN=johndoe**）。

4. **Subject Alternative Name Type**（サブジェクトの別名タイプ）を選択します。

   *Subject Alternative Name (*サブジェクトの別名 - *SAN)* タイプのスタティックエントリを使用します。ファイアウォールは ***$ USERNAME***などのダイナミック トークンをサポートしていません。

   - **RFC 822 Name**（**RFC822** 名）— 証明書のサブジェクトまたはサブジェクト代替名拡張子に電子メールアドレス名を入力します。
   - **DNS Name**（**DNS** 名）— 証明書の検証に使用する DNS 名を入力します。
   - **Uniform Resource Identifier**（ユニフォームリソース識別子）— クライアントが証明書を取得する URI リソース名を入力します。
   - **None**（なし）— 証明書の属性を指定しません。

STEP 4 | （任意）証明書の暗号設定を行います。

- 証明書の鍵長（**Number of Bits**（ビット数））を選択します。

  ファイアウォールが FIPS-CC モードで鍵生成アルゴリズムが RSA の場合。RSA キーは 2,048 ビット以上でなければなりません。
- 証明書署名要求（CSR）用のダイジェスト アルゴリズムを示す **Digest for CSR**（**CSR** 用ダイジェスト）を選択します（sha1、sha256、または sha384）。

STEP 5 | （任意）許可される証明書の用途を設定します（署名用または暗号化用）。

- この証明書を署名のために使用する場合、**Use as digital signature**（デジタル署名として使用）のチェックボックスを選択します。これにより、デジタル署名の検証を行う際にエンドポイントが証明書に含まれる秘密鍵を使用するようになります。
- この証明書を暗号化のために使用する場合、**Use for key encipherment**（鍵の暗号化のために使用）のチェックボックスを選択します。これにより、SCEP サーバーが発行する証明書を通して確立された HTTPS 接続を経由して交換されたデータをクライアントのエンドポイントで暗号化する際に、証明書に含まれる秘密鍵を使用するようになります。

STEP 6 | （任意）ポータルが正しい SCEP サーバーに確実に接続されるようにするために、**CA Certificate Fingerprint**（**CA** 証明書フィンガープリント）を入力します。SCEP サーバーインターフェイスの Thumbprint（指紋）のフィールドからフィンガープリントを入手してください。

1. SCEP サーバーの管理 UI の URL を入力します (たとえば、**`http://<hostname or IP>/CertSrv/mscep_admin/`** など)。
2. Thumbprint（指紋）をコピーし、**CA Certificate Fingerprint**（**CA** 証明書フィンガープリント）に入力します。

STEP 7 | SCEP サーバーとファイアウォール間の相互 SSL 認証を有効にします。米国の連邦情報処理標準（FIPS）に準拠するためにこれが必須になります。Federal Information Processing Standard (連邦情報処理標準 - FIPS)

FIPS-CC の実施についてはファイアウォールのログインページおよびそのステータスバーに表示されます。

SCEP サーバーのルート**CA Certificate**（**CA** 証明書）を選択します。また、必要に応じて**Client Certificate**（クライアント証明書）を選択し、SCEP サーバーとファイアウォール間の相互 SSL 認証を有効にすることも可能です。

STEP 8 | 設定を保存・コミットします。

1. **OK** をクリックして設定を保存し、SCEP 設定を閉じます。
2. 設定を **Commit**（コミット）します。

ポータルが SCEP プロファイルの設定を使用して CA 証明書をリクエストしようと試み、それをファイアウォールがホストするポータルに保存します。正しく実行されると、CA証明書が**Device** > **Certificate Management** > **Certificates**(デバイス > 証明書管理 > 証明書)に表示されます。

STEP 9 | （任意）SCEP プロファイルの保存後にポータルが証明書の取得に失敗する場合、ポータルから手動で CSR を生成することができます。

1. **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択してから **Generate**（生成）をクリックします。
2. **Certificate Name**（証明書名）を入力します。この名前にはスペースを含められません。
3. お客様のエンタープライズ PKI に CSR を送信する際に使用する **SCEP Profile**（**SCEP** プロファイル）を選択します。
4. **OK** をクリックしてリクエストを送信し、証明書を生成します。

証明書および秘密鍵のエクスポート

Palo Alto Networks では、組織の公開鍵基盤（PKI）を使用して、証明書および秘密鍵を組織内に配布することをお勧めします。ただし、必要に応じて、証明書および秘密鍵をファイアウォールまたは Panorama からエクスポートすることもできます。以下の場合は、エクスポートした証明書および秘密鍵を使用できます。

- Web インターフェイスへの証明書ベースの管理者認証の設定
- GlobalProtect LSVPN コンポーネント間の SSL を有効にして 、ポータルとゲートウェイへの GlobalProtect エージェント/アプリケーション認証を設定する
- SSL 転送プロキシの復号化
- 外部 CA からの証明書の取得

STEP 1 | **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択します。

STEP 2 | ファイアウォールに仮想システム（vsys）が複数ある場合は、証明書の **Location** [場所]（特定の vsys または **Shared** [共有]）を選択します。

STEP 3 | 証明書を選択して、**Export** [エクスポート]をクリックし、**File Format** [ファイル形式]を選択します。

- **Base64 Encoded Certificate (PEM)** [Base64 エンコード済み証明書（PEM）] – デフォルトのフォーマットです。最も一般的で、インターネット上で一番広くサポートされています。エクスポートされたファイルに秘密鍵を含める場合は、**Export Private Key** [秘密鍵のエクスポート]チェック ボックスをオンにします。
- **Encrypted Private Key and Certificate (PKCS12)** [暗号化された秘密鍵と証明書（PKCS12）] – このフォーマットは PEM より安全ですが、PEM ほど一般的でなく、広くサポートされていません。エクスポートされたファイルには自動的に秘密鍵が含まれます。
- **Binary Encoded Certificate (DER)** [バイナリ エンコード済み証明書（DER）] – 他のフォーマットよりも多くの種類のオペレーティング システムでサポートされています。鍵なしで、証明書のみをエクスポートできます。その場合は、**Export Private Key** [秘密鍵のエクスポート]チェック ボックスをオフにして、パスフレーズのフィールドを無視します。

STEP 4 | **File Format** [ファイル フォーマット]が PKCS12 の場合、または PEM で **Export Private Key** [秘密鍵のエクスポート]チェック ボックスがオンの場合は、**Passphrase** [パスフレーズ]と **Confirm Passphrase** [パスフレーズの確認]に入力して秘密鍵を暗号化します。このパスフレーズは、証明書および鍵をクライアント システムにインポートするとき使用します。

(*Panorama* 管理 ファイアウォール) 証明書を 生成 または インポート するときに ***Block Private Key Export***[秘密鍵のエクスポートをブロック] を有効にした場合は、エクスポートされた証明書をインポートするときに必ず ***Import Private Key***[秘密鍵のインポート] と ***key File***[キーファイル] を追加する必要があります。これは、*Panorama* から証明書のインポート先であるマネージド ファイアウォール に構成変更を正常にプッシュするために必要です。

STEP 5 | **OK** をクリックして、証明書/キー ファイルをコンピュータに保存します。

証明書プロファイルの設定

証明書プロファイルは、認証ポータル、多要素認証 (MFA)、GlobalProtect、サイト間 IPSec VPN、外部動的リスト (EDL)検証、ダイナミック DNS (DDNS)、User-IDエージェントおよび TSエージェントのアクセス、Palo Alto Networks のファイアウォールあるいは Panorama への Webインターフェースを介したアクセスのユーザーおよびデバイス認証を定義します。プロファイルでは、使用する証明書、証明書の失効状態の検証方法、および状態によりアクセスを制限する方法を指定します。アプリケーションごとに証明書プロファイルを設定します。

証明書プロファイルのオンライン証明書ステータス プロトコル *(OCSP)* および証明書失効リスト *(CRL)* の状態検証を有効化し、証明書が無効になっていないことを確認することをお勧めします。*OCSP* サーバーが利用できない場合にファイアウォールが *CRL* を使用できるよう、*OCSP* と *CRL* の両方を有効化します。これらの方法の詳細については、証明書の失効 を参照してください。

STEP 1 | 割り当てる認証局（CA）証明書を取得します。

以下のいずれかの手順を実行して、プロファイルに割り当てる CA 証明書を取得します。少なくとも 1 つを割り当てる必要があります。

- 証明書の生成を行います。
- エンタープライズ CA から証明書をエクスポートし、それを ファイアウォール にインポートします (3 へのステップを参照)。

STEP 2 | 証明書プロファイルを特定します。

1. **Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificate Profile (証明書プロファイル)** を選択し、**Add (追加)** をクリックします。
2. プロファイルを識別する **Name**（名前）を入力します。この名前は、大文字と小文字が区別され、一意でなければならず、文字、数字、スペース、ハイフン、アンダースコアのみの、Panorama では最大 31 文字、ファイアウォールでは最大 63 文字で構成されます。
3. ファイアウォールに仮想システム（vsys）が複数ある場合は、証明書の **Location** [場所]（vsys または **Shared** [共有]）を選択します。

STEP 3 | 1 つ以上の証明書を割り当てます。

CA 証明書ごとに以下の手順を実行します。

1. CA Certificates [CA 証明書]表で、**Add** [追加]をクリックします。
2. **CA Certificate** [CA 証明書]を選択します。また、証明書をインポートする場合は、**Import** [インポート]をクリックして、**Certificate Name** [証明書名]に入力

し、**Browse** [参照]でエンタープライズ CA からエキスポートした **Certificate File** [証明書ファイル]を見つけて、**OK** をクリックします。

3. （任意）ファイアウォールで OCSP を使用して証明書の失効状態を検証する場合は、以下のフィールドを設定して、デフォルトの動作をオーバーライドします。ほとんどのデプロイメントでは、これらのフィールドは適用されません。

   - デフォルト設定では、ファイアウォールは証明書の「認証機関アクセス情報」（AIA）を使って OCSP レスポンダ情報を抽出します。AIA 情報をオーバーライドするには、**Default OCSP URL**（デフォルト **OCSP URL**）（**`http://`** または **`https://`** で始まる）を入力します。
   - デフォルトでは、ファイアウォールは **CA Certificate**[CA 証明書] フィールドで選択した証明書を使用して、OCSP 応答を検証します。検証に異なる証明書を使用するには、**OCSP Verify CA Certificate**（**OCSP** 検証 **CA** 証明書）フィールドでその証明書を選択します。

4. **OK** をクリックします。CA Certificates [CA 証明書] 表に割り当てられた証明書が表示されます。

STEP 4 | 証明書の失効状態および関連付けられているブロック動作の検証の方法を定義します。

1. **Use CRL**[CRLを使用] または **Use OCSP**[OCSPを使用]、あるいは両方を選択します。両方を選択している場合、ファイアウォールはまず OCSP を試行し、OCSP レスポンダが使用できない場合にのみ CRL を使用する方法にフォールバックします。
2. 検証方法に応じて、**CRL Receive Timeout**[CRL 受信の有効期限] または **OCSP Receive Timeout**[OCSP 受信の有効期限]、あるいはその両方に入力します。これは、ファイアウォールが CRL/OCSP サービスからの応答を待機する期間（1 ～ 60 秒）です。
3. **Certificate Status Timeout**[証明書の有効期限] を入力します。これは、ファイアウォールが任意の証明書状態サービスからの応答を待機し、定義したセッション ブロック ロジックを適用するまでの期間（1 ～ 60 秒）です。**Certificate Status Timeout**（証明書の有効期限）は、OCSP/CRL の **Receive Timeout**（受信の有効期限）と以下のように関連しています。

   - OCSP および CRL の両方を有効化する場合 – ファイアウォールは、**Certificate Status Timeout**[証明書の有効期限] の値または 2 つの **Receive Timeout**[受信の有効期限] の値の合計のいずれか小さい方の期間の経過後に、要求のタイムアウトを登録します。
   - OCSP のみを有効化する場合 – ファイアウォールは、**Certificate Status Timeout**[証明書の有効期限] の値または OCSP の **Receive Timeout**[受信の有効期限] の値のいずれか小さい方の期間の経過後に、要求のタイムアウトを登録します。
   - CRL のみを有効化する場合 – ファイアウォールは、**Certificate Status Timeout**（証明書の有効期限）値または CRL の **Receive Timeout**（受信の有効期限）値のいずれか小さい方の期間の経過後に、要求のタイムアウトを登録します。

4. OCSP あるいは CRL サービスが unknown (不明) という証明書失効状態を返した場合にファイアウォールにセッションをブロックさせるときは、**Block session if certificate status is unknown (**証明書状態が不明な場合にセッションをブロック**)** を選択します。その他の場合は、ファイアウォールはセッションを許可します。

5. OCSP または CRL 要求のタイムアウトが登録された後、ファイアウォールでセッションをブロックする場合は、**Block session if certificate status cannot be retrieved within timeout (**タイムアウト時間内に証明書状態を取得できない場合にセッションをブロック**)** を選択します。その他の場合は、ファイアウォールはセッションを許可します。
6. （**GlobalProtect** のみ）クライアント証明書の件名に含まれるシリアル番号属性が、そのクライアント エンドポイントについて GlobalProtect アプリが報告する host ID (ホスト ID) と一致しない場合にファイアウォールにセッションをブロックさせたい場合は、**Block sessions if the certificate was not issued to the authenticating device (**認証中のデバイスに対して証明書が発行されていない場合はセッションをブロック**)** を選択します。

STEP 5 | **OK** をクリックして **Commit (**コミット**)** します。

SSL/TLS サービス プロファイルの設定

Palo Alto NetworksのファイアウォールおよびPanoramaは、SSL/TLSサービス プロファイルを利用して、そのSSL/TLSサービスに対して使用できる証明書、およびプロトコルのバージョンを指定します。ファイアウォールおよび Panorama では、認証ポータル、GlobalProtectポータルおよびゲートウェイ、管理（MGT）インターフェースのインバウンド トラフィック、URL 管理者オーバーライド機能、User-ID™ syslog リスニング サービスに、SSL/TLS を使用します。プロトコル バージョンを定義することで、サービスを要求するクライアントとの通信の保護に使用できる暗号スイートを制限するプロファイルを使用できます。これによりファイアウォールあるいはPanoramaは、脆弱性が明らかになっているバージョンのSSL/TLSの使用を控えることができるようになるため、ネットワーク・セキュリティが向上します。指定された範囲外のバージョンのプロトコルがサービスリクエストに含まれている場合、ファイアウォールあるいはPanoramaは、サポートされているバージョンになるよう、接続のバージョンを上げるか下げるかします。

ファイアウォール サービスを要求するクライアント システムでは、*SSL/TLS* サービス プロファイルで指定されている証明書を発行した認証局（*CA*）証明書を証明書信頼リスト（*CTL*）に含める必要があります。これを含めない場合、ユーザーがファイアウォール サービスを要求したときに証明書エラーが発生します。ほとんどのサードパーティ *CA* 証明書がクライアント ブラウザにデフォルトで表示されます。エンタープライズまたはファイアウォール生成の *CA* 証明書が発行者の場合、その *CA* 証明書をクライアント ブラウザの *CTL* に適用する必要があります。

STEP 1 | 目的のサービスごとに、ファイアウォールで証明書を生成またはインポートします（証明書の取得を参照）。

SSL/TLS サービス プロファイルでは、*CA* 証明書は使用せず、署名付き証明書のみを使用します。

STEP 2 | **Device (デバイス)** > **Certificate Management (証明書管理)** > **SSL/TLS Service Profile (SSL/TLS サービス プロファイル)** を選択します。

STEP 3 | ファイアウォールに仮想システム（vsys）が複数ある場合は、プロファイルを使用できる **Location** [場所]（vsys または **Shared** [共有]）を選択します。

STEP 4 | **Add** [追加]をクリックして、プロファイルを識別する **Name** [名前]を入力します。

STEP 5 | 取得した **Certificate** [証明書]を選択します。

STEP 6 | サービスが使用できるプロトコルの範囲を定義します。

- **Min Version**[最低バージョン]では、許可するTLSの最も古いバージョン（**TLSv1.0**（デフォルト設定）、**TLSv1.1**、または**TLSv1.2**）を選択します。
- **Max Version**[最高バージョン]では、許可するTLSの最も新しいバージョン（**TLSv1.0**、**TLSv1.1**、**TLSv1.2**、または**Max**[最大]（現行の最新バージョン））を選択します。デフォルトは **Max** [最大]です。

ベストプラクティスとして、***Min Version***（最低バージョン）を***TLSv1.2*** に、***Max Version***（最高バージョン）を***Max***（最大）に設定します。

PAN-OS 8.0 またはそれ以降のリリースで実行する *FIPS/CC* モードのファイアウォールでは、***TLSv1.1***はサポートされている *TLS* バージョンの中で最も古いものです。***TLSv1.0*** は選択しないでください。

TLSv1.2 を使用するファイアウォール サービスを要求する場合、使用するクライアント証明書に *SHA512* をダイジェスト アルゴリズムとして含めることはできません。クライアント証明書でより低いダイジェスト アルゴリズム（*SHA384* など）を使用するか、ファイアウォール サービスの***Max Version***（最大バージョン）を ***TLSv1.1*** に制限する必要があります。

STEP 7 | **OK**、**Commit (コミット)** の順にクリックします。

SSH サービス プロファイルの設定

SSH サービス プロファイルにより、SSH パラメータをカスタマイズして、Palo Alto Networks 管理、およびhigh availability (高可用性 - HA)アプライアンスに対する、SSH 接続のセキュリティと整合性を強化できます。デフォルトでは、SSH はすべての暗号、キー交換アルゴリズム、およびメッセージ認証コードをサポートしているため、接続は攻撃に対して脆弱なままです。SSH サービス プロファイルを使用すれば、SSH サーバー サポートのアルゴリズムを制限できます。また、新しいホスト鍵を生成し、SSH セッション鍵の再生成と交換のために、データ量、時間、およびパケットベースのしきい値を指定することもできます。

SSH サーバー インスタンスに応じて、管理、またはHA SSH サービス プロファイルのいずれかを設定します。プロファイルは、ファイアウォール、または Panorama™ Webインターフェース(複数のファイアウォールまたはアプライアンスにまたがって設定を適用する場合)、または CLI から構成できます。

最大 *4* つの管理プロファイルと *4* つの *HA* サーバープロファイルを設定できます。

Collector Group (コレクタ グループ)内の各専用のログ コレクタ (ログ コレクタ モードの *M-series* または *Panorama* バーチャル アプライアンス) に対して同じ *SSH* 接続設定を使用するには、*Panorama*管理サーバから *SSH* サービス プロファイルを設定し、変更を *Panorama* に***Commit*** (コミット) してから、設定をログ コレクターに ***Push*** (プッシュ) します。また、*CLI* からこれらのステップを実行するには、***set log-collector-group <name> general-set management ssh*** コマンドを使用します。

- SSH 管理プロファイルを作成する
- SSH HA プロファイルを作成する

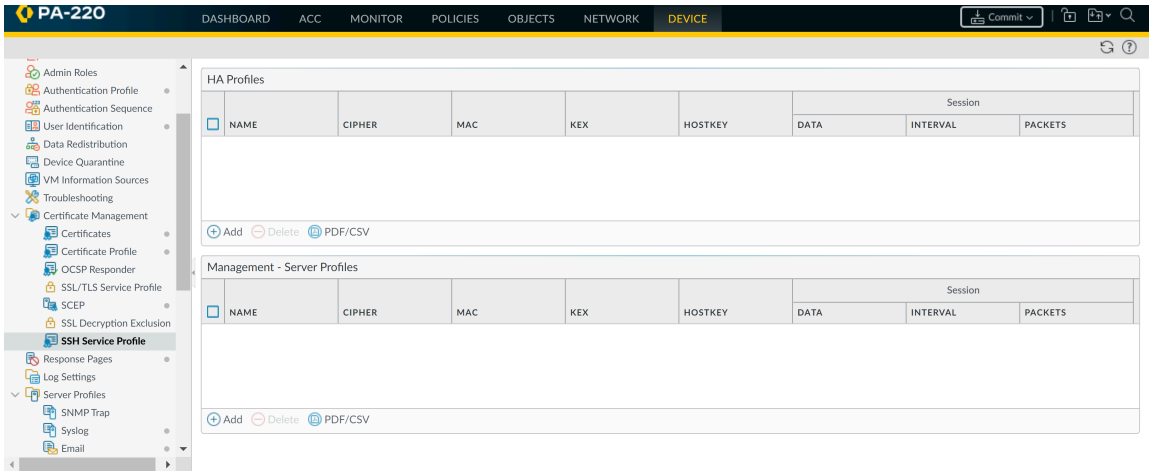
SSH 管理プロファイルを作成する

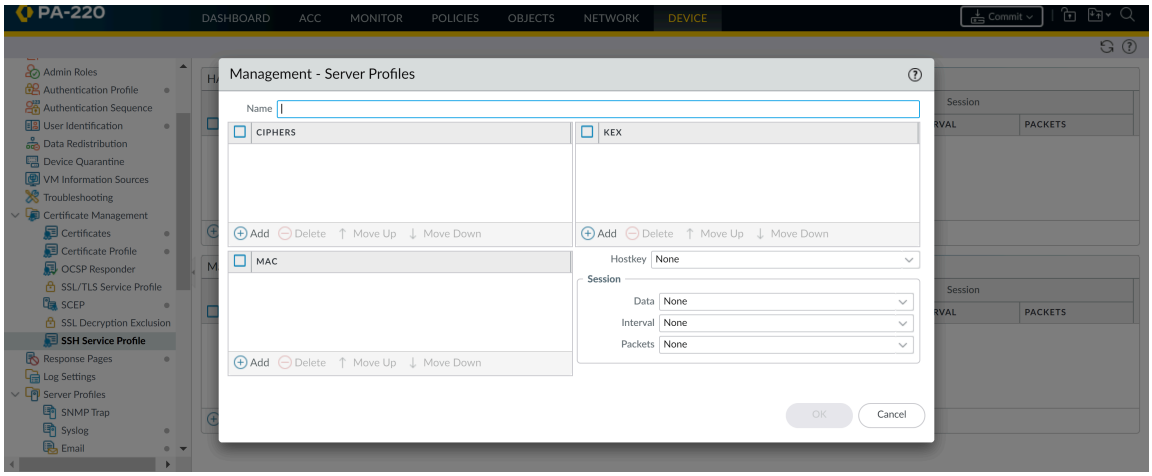
SSH 管理プロファイルを作成し、管理接続用に SSH 設定をカスタマイズする必要があります。

*CLI*から既存の管理プロファイルを設定するか、既存のプロファイルを更新する ことができます。

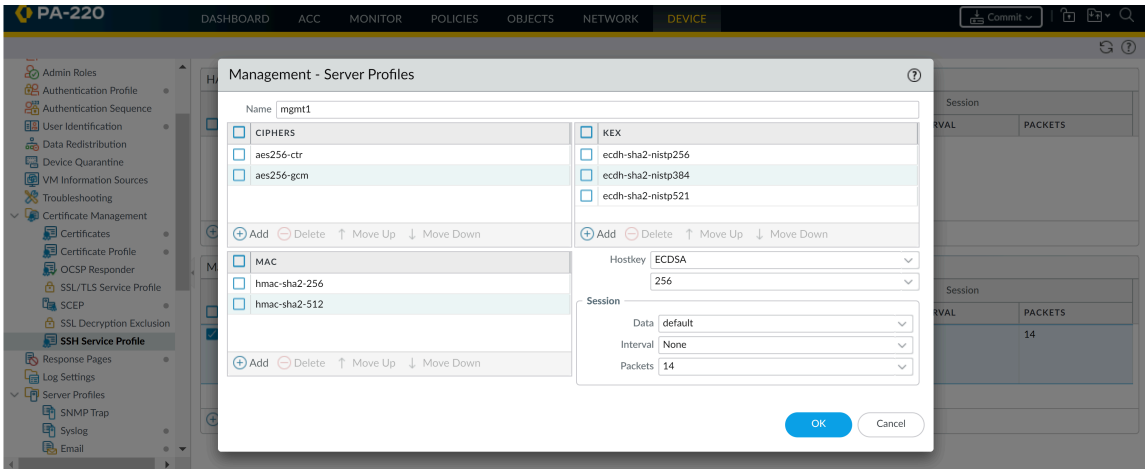
STEP 1 | 管理 - サーバ プロファイルを作成します。

1. **Device (デバイス)** > **Certification Management (証明書管理)** > **SSH Service Profile (SSH サービス プロファイル)** を選択します。
2. 管理 - サーバ プロファイルを**Add (追加)** します。





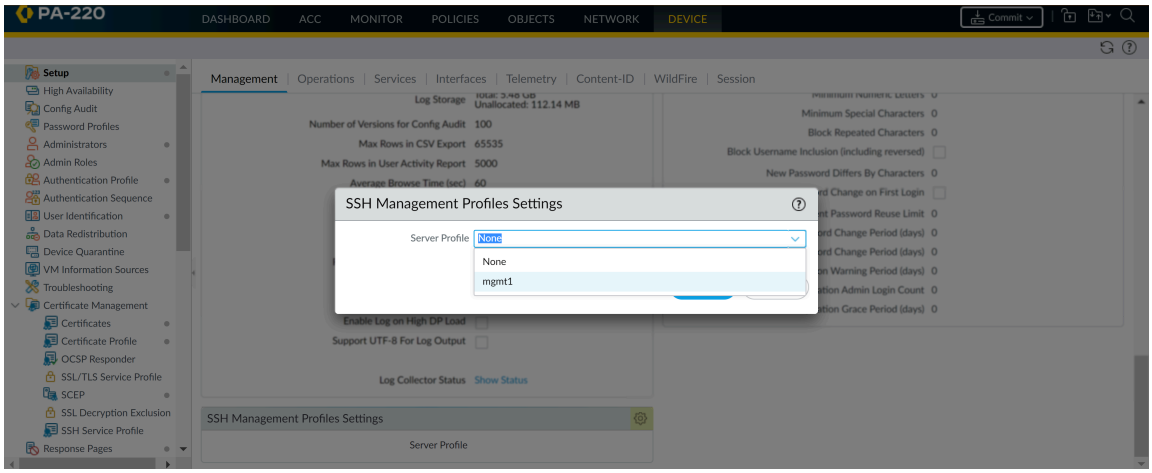
3. プロファイルを識別する **Name**（名前）を入力します。
4. (任意) プロファイルがサポートする、暗号、メッセージ認証コード、またはキー交換アルゴリズムを**Add (**追加**)** します。
5. (任意) **Hostkey (**ホストキー**)** とキーの長さを選択します。
6. (任意) SSH セッション鍵更新パラメータの値を入力します:**Data (**データ**)**、**Interval (**間隔**)**、および **Packets (**パケット**)**。



7. **OK**、**Commit (コミット)** の順にクリックします。

STEP 2 | 適用する管理プロファイルを選択します。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理）を選択します。SSH 管理プロファイル設定で、既存のプロファイルを選択します。



2. **OK** をクリックし、変更を **Commit**（コミット**)** します。 します。

STEP 3 | CLI から管理 SSH サービスを再起動して、プロファイルを適用します。

新しいプロファイルを適用するか、使用中のプロファイルに変更を加えるたびに、接続を再開する必要があります。この操作により、アプライアンスが再起動します。新しい設定はアクティブなセッションの影響を受けません。プロファイルは、後続の接続 (またはセッション) に適用されます。

1. admin@PA-3260> **set ssh service-restart mgmt**

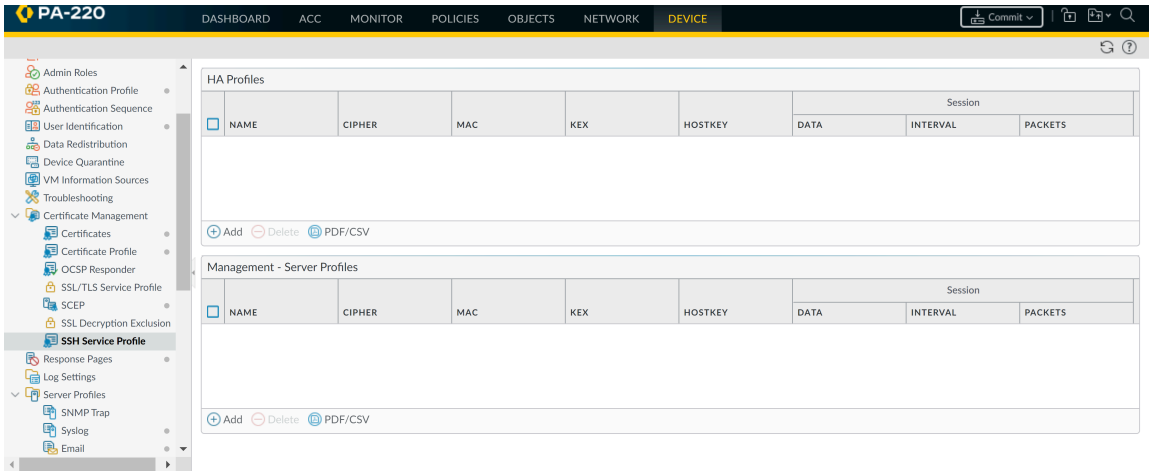
SSH HA プロファイルを作成する

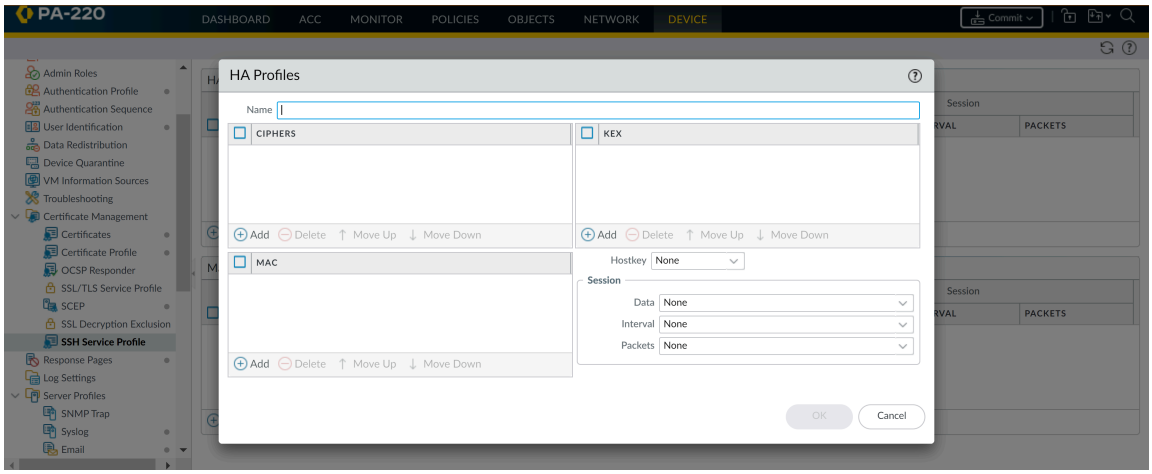
HAペア内のアプライアンス間の SSH 通信を保護するには、SSH HA プロファイルを作成する必要があります。プロファイルが作成可能になる前に、該当のアプライアンス間の HA 接続を確立させる必要があります。HA 接続がまだ確立していない場合は、コントロール リンク接続で暗号化を有効にし、HA キーをネットワーク上の場所にエクスポートして、その HA 鍵をピアにインポートする必要があります。(Configure Active/Passive HA (アクティブ/パッシブ HA を設定する)、または Configure Active/Active HA (アクティブ/アクティブ HA を設定する) を参照してください。)

*CLI*からHAプロファイルを設定するか、既存の HA プロファイルを更新する ことができます。

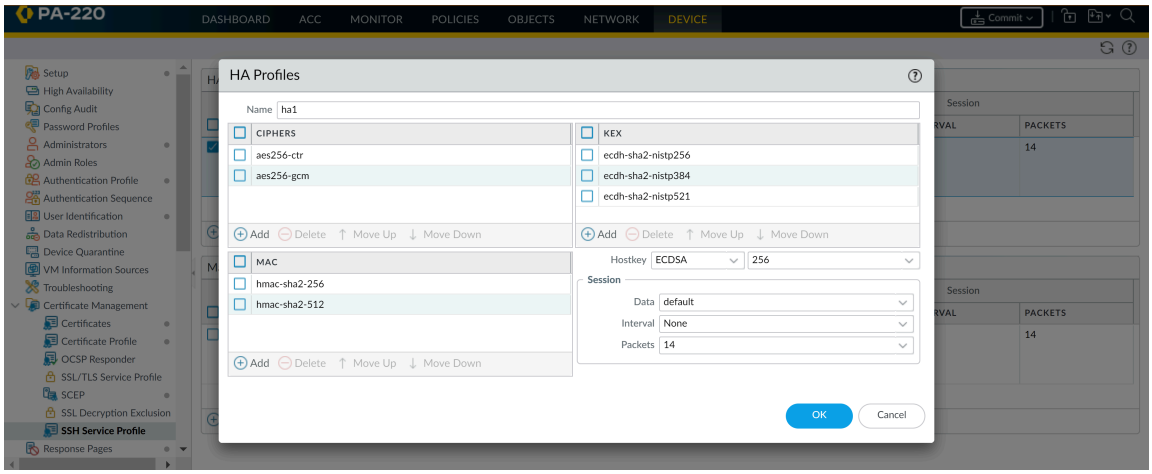
STEP 1 | HA プロファイルを作成します。

1. **Device (デバイス)** > **Certification Management (証明書管理)** > **SSH Service Profile (SSH サービス プロファイル)** を選択します。
2. HA プロファイルを**Add (追加)** します。





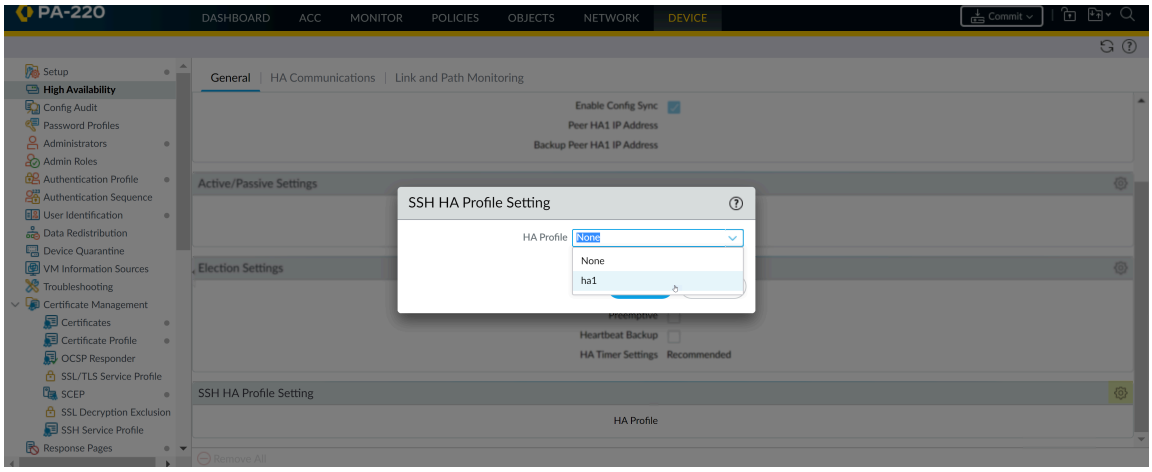
3. プロファイルを識別する **Name**（名前）を入力します。
4. (任意) プロファイルがサポートする、暗号、メッセージ認証コード、またはキー交換アルゴリズムを**Add (**追加**)** します。
5. (任意) **Hostkey (**ホストキー**)** とキーの長さを選択します。
6. (任意) SSH セッション鍵更新パラメータの値を入力します:**Data (**データ**)**、**Interval (**間隔**)**、および **Packets (**パケット**)**。



7. **OK**、**Commit (コミット)** の順にクリックします。

STEP 2 | 適用する HA プロファイルを選択します。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General** （全般）を選択します。SSH HA Profile Setting (SSH HA プロファイル設定) で、既存のプロファイルを選択します。



2. **OK** をクリックし、変更を **Commit**（コミット**)** します。 します。

STEP 3 | CLI から HA1 SSH サービスを再起動して、プロファイルを適用します。

新しいプロファイルを適用するか、使用中のプロファイルに変更を加えるたびに、接続を再開する必要があります。この操作により、アプライアンスが再起動します。新しい設定はアクティブなセッションの影響を受けません。プロファイルは、後続の接続 (またはセッション) に適用されます。

1. admin@PA-3260> **set ssh service-restart ha**

   *HA*ペア間の接続が確立されており、*SSH* サービスの再起動に伴うダウンタイムを最小限に抑えたい場合は、以下のコマンドを使用できます。*HA* 接続が確立されていない場合は、*SSH* サービスを再起動する必要があります。

   - *(HA1 Backup* が構成されている*) admin@PA-3260>* ***request high-availability session-reestablish***
   - *(HA1* バックアップ が設定されていないか、*HA1* バックアップ リンクがダウンしている*) admin@PA-3260>* ***request high-availability session-reestablish force***

     HA1 バックアップがない場合、ファイアウォール に *HA1* セッションの再確立を強制できます。これにより、*HA* ピア間に短時間の スプリットブレイン 状態が発生する可能性があります。*(HA1* バックアップが構成されている場合に ***force***（強制） オプションを使用しても効果はありません。

インバウンドの管理トラフィック用証明書の交換

ファイアウォールあるいはPanoramaの初回起動時、管理（MGT）インターフェイスおよび（ファイアウォールのみ）HTTPS管理トラフィックをサポートするその他のインターフェイスを介してWebインターフェイスやXML APIにアクセスする際にHTTPSを有効化するデフォルトの証明書が自動的に生成されます（詳細についてはインターフェイス管理プロファイルを使用してアクセスを制限を参照）。インバウンドの管理トラフィックのセキュリティを高めるため、このデフォルトの証明書を、お客様の組織用に発行された新しい証明書と入れ替えるようにしてください。

このデフォルトの証明書は閲覧・変更・削除することができません。

管理トラフィックを保護するためには、管理者アカウントおよび認証の設定も行う必要があります。

STEP 1 | ファイアウォールあるいはPanoramaを管理者のクライアントシステムに認証する証明書を取得します。

クライアントシステムがすでに信頼している証明書を使うことで、証明書のデプロイメントを簡素化することができます。そのため、企業用の証明書認証局（CA）から証明書および秘密鍵のインポートを行うか、外部 CA からの証明書の取得を行うことを推奨いたします。クライアントシステムの信頼されたルート証明書ストアには、すでに確実に信頼できる関連したルート CA 証明書がある場合が多くあります。

ファイアウォールあるいは*Panorama*で証明書の生成を行う場合、クライアントシステムの信頼されたルート証明書ストアにルート*CA*証明書が無いために、管理者は証明書エラーに遭遇します。これを回避するには、すべてのクライアントシステムに自己署名ルート *CA* 証明書をデプロイします。

証明書の入手方法に関わらず、***sha256***以上の***Digest*** *[ダイジェスト]*アルゴリズムでセキュリティを高めることを推奨いたします。

STEP 2 | SSL/TLS サービス プロファイルを設定します。

取得した **Certificate** [証明書]を選択します。

セキュリティを高めるために、インバウンドの管理トラフィック用の***Min Version****[最低バージョン]*（許可するもののうち最も古い*TLS*のバージョン）を***TLSv1.2***に設定することを推奨いたします。また、各ファイアウォールあるいは*Panorama*サービスについて、すべてのサービスでこのプロファイルを使い回すのではなく、各サービスで異なる*SSL/TLS*サービス プロファイルを使用することをお勧めします。

STEP 3 | SSL/TLSサービス プロファイルをインバウンドの管理トラフィックに適用します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して General Settings (一般設定) を編集します。
2. 先ほど設定した**SSL/TLS Service Profile** [SSL/TLS サービス プロファイル]を選択します。
3. **OK**、**Commit (コミット)** の順にクリックします。

SSL フォワード プロキシ サーバーの証明書の鍵のサイズの設定

SSLフォワード プロキシセッションでクライアントに応答する場合、ファイアウォールは宛先サーバーによって提示される証明書のコピーを作成し、それを使用してクライアントとの接続を確立します。デフォルト設定では、ファイアウォールは宛先サーバーによって提示される証明書と鍵のサイズが同じになっている証明書を生成します。ですが、ファイアウォールが生成した証明書の鍵のサイズは次の手順で変更することができます。

STEP 1 | **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** の順に選択し、Decryption Settings (復号化設定) セクションで、**SSL Forward Proxy Settings (SSL** フォワード プロキシ設定**)** をクリックします。

STEP 2 | **Key Size**[鍵のサイズ] を選択します。

- **Defined by destination host**（宛先ホストにより定義）—ファイアウォールは、生成する証明書で鍵のサイズおよびハッシュアルゴリズムを決定し、宛先サーバーの証明書に基づいてクライアントとの SSL プロキシ セッションを確立します。宛先サーバーが 1,024 bit (ビット- bit) RSA 鍵を使用する場合、ファイアウォールは、1,024 bit (ビット- bit) RSA 鍵を使用して証明書を生成します。宛先サーバーが 1,024 bit (ビット- bit)よりも大きい鍵のサイズを使用する場合（2,048 bit (ビット- bit)や 4,096bit (ビット- bit) など）、ファイアウォールは、2,048 bit (ビット- bit) RSA 鍵を使用する証明書を生成します。宛先サーバーが SHA-1 ハッシュアルゴリズムを使用する場合、ファイアウォールは、SHA-1 ハッシュアルゴリズムを使用して証明書を生成します。宛先サーバーが SHA-1 より強いハッシュアルゴリズムを使用する場合、ファイアウォールは、SHA-256 アルゴリズムを使用して証明書を生成します。これがデフォルトの設定です。
- **1024** ビット **RSA** :ファイアウォールは、宛先サーバー証明書のキー サイズに関係なく、1,024 ビットの RSA キーと SHA-256 ハッシュ アルゴリズムを使用する証明書を生成します。2013 年 12 月 31 日以降、公開認証局（CA）と一般的なブラウザでは、2048ビット未満のキーを使用するX.509証明書のサポートが制限されています。将来的にブラウザでは、このような鍵が提示された場合、セキュリティの設定に応じて、ユーザーに警告を表示したり、SSL/TLS セッション全体をブロックしたりする可能性があります。
- **2048-bit RSA** [2048 ビット RSA] — ファイアウォールは、宛先サーバーの証明書の鍵のサイズに関係なく、2048 ビットの RSA 鍵と SHA-256 ハッシュ アルゴリズムを使用する証明書を生成します。公開 CA と一般的なブラウザでは、1,024 ビット鍵よりも強固なセキュリティを提供する 2,048 ビット鍵がサポートされています。

鍵のサイズの設定を変更すると、現在の証明書キャッシュがクリアされます。

STEP 3 | **OK**、**Commit (コミット)** の順にクリックします。

証明書の無効化および更新

証明書の無効化

さまざまな状況により、有効期限前に証明書が無効化されていることがあります。たとえば、名前が変更された場合や、サブジェクトと認証局間の関連付けが変更された（従業員の雇用が終了したなど）場合、秘密鍵の侵害が判明した、またはその疑いがある場合などです。このような状況では、証明書を発行した認証局（CA）が証明書を無効化する必要があります。以下のタスクでは、ファイアウォールが CA である証明書を無効化する方法を説明します。

STEP 1 | **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択します。

STEP 2 | ファイアウォールで複数の仮想システムをサポートしている場合は、タブに **Location**[場所] ドロップダウンリストが表示されます。証明書が属している仮想システムを選択します。

STEP 3 | 無効化する証明書を選択します。

STEP 4 | **Revoke**[無効化] をクリックします。PAN-OS で直ちに証明書の状態が無効に設定され、オンライン証明書ステータス プロトコル（OCSP）レスポンダ キャッシュまたは証明書失効リスト（CRL）にシリアル番号が追加されます。コミットを実行する必要はありません。

証明書の更新

証明書の有効期限が切れた場合、または間もなく切れる場合、有効期間をリセットすることができます。外部認証局（CA）が証明書に署名し、ファイアウォールがオンライン証明書ステータス プロトコル（OCSP）を使用して証明書の失効状態を検証している場合、ファイアウォールは OCSP レスポンダ情報を使用して証明書の状態を更新します（OCSP レスポンダの設定を参照）。ファイアウォールが証明書を発行した CA である場合、ファイアウォールはその証明書を、古い証明書と属性が同じでシリアル番号が異なる新しい証明書に置き換えます。

STEP 1 | **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択します。

STEP 2 | ファイアウォールに仮想システム（vsys）が複数ある場合は、証明書の **Location** [場所]（vsys または **Shared** [共有]）を選択します。

STEP 3 | 更新する証明書を選択して、**Renew**[更新] をクリックします。

STEP 4 | **New Expiration Interval**[新しい有効期限間隔]（日数単位）を入力します。

STEP 5 | **OK**、**Commit (コミット)** の順にクリックします。

ハードウェア セキュリティ モジュールによるキーの安全確保

ハードウェア セキュリティ モジュール (HSM) はデジタル キーを管理する物理デバイスです。HSM では、デジタル キーの安全な保存と生成を提供します。HSM では、不正利用や潜在的な攻撃者からこれらを論理的および物理的に保護します。

Palo Alto Networksのファイアウォールあるいは Panorama と統合されている HSM クライアントにより、SSL/TLS 復号化で使用される秘密鍵のセキュリティが向上します（SSL フォワード プロキシおよび SSL インバウンド インスペクション）。また、マスター キーを暗号化するために HSM を使用できます。

以下のトピックでは、ファイアウォールあるいは Panorama と HSM を統合する方法を説明します。

- HSM との接続のセットアップ
- HSM を使用したマスター キーの暗号化
- HSM での秘密鍵の保存
- HSM デプロイメントの管理

HSM との接続のセットアップ

HSM クライアントは、PA-3200 Series、PA-3400 Series、PA-5200 Series、PA-5400 Series、PA-7000 Series、および VM-Series ファイアウォールおよび Panorama 管理サーバ (仮想アプライアンスと M-Series アプライアンスの両方) と統合されており、次の HSM ベンダーで使用できます。

- **nCipher nShield Connect**—サポートされているクライアントのバージョンは、PAN-OS のリリースによって異なります。
  - PAN-OS 10.2 は、クライアント バージョン 12.40.2 (古いアプライアンスではクライアント バージョン 11.50 までの下位互換性) をサポートします。
  - PAN-OS 9.1、9.0、および8.1は、クライアント バージョン12.30をサポートします。
  - PAN-OS 8.0 およびそれ以前のリリースは、クライアント バージョン11.62 をサポートします。
- **SafeNet Network**—サポートされているクライアントのバージョンは、PAN-OS のリリースによって異なります。
  - PAN-OS 10.2 は、クライアント バージョン 5.4.2 および 7.2 をサポートします。
  - PAN-OS 9.1 および 9.0 は、クライアント バージョン 5.4.2 および 6.3 をサポートします。
  - PAN-OS 8.1 は、クライアント バージョン 5.4.2 および 6.2.2 をサポートします。
  - PAN-OS 8.0.2 および、それ以降のPAN-OS 8.0 リリース（また、PAN-OS 7.1.10 および、それ以降の PAN-OS 7.1リリース）は、クライアント バージョン 5.2.1、5.4.2 および 6.2.2をサポートします。

HSM サーバー バージョンは、これらのクライアント バージョンと互換性がある必要があります。クライアント サーバー バージョンの互換性マトリックスについては、HSM ベンダーのドキュメントを参照してください。ファイアウォールまたは Panorama で、次の手順に従って SafeNet HSM サーバーと互換性のある SafeNet ネットワーク クライアントのバージョンを選択します。

HSM サーバーをアップグレードすると、*HSM* サーバーをダウングレードすることはできません。

- SafeNet Network HSMとの接続のセットアップ
- nCipher nShield Connect HSM との接続のセットアップ

SafeNet Client RPM Packet Manager をインストールします。

1. **Device**（デバイス） > **Setup**（セットアップ） > **HSM** を選択して、**Select HSM Client Version**（**HSM** クライアント バージョンの選択）を行います（ハードウェア セキュリティ操作設定 ）。
2. HSM サーバーのバージョンに応じて、**Version 5.4.2 (**バージョン **5.4.2)** (デフォルト) または **7.2** を選択します。
3. **OK** をクリックします。
4. （ファイアウォール上の HSM バージョンを変更する場合にのみ必須）バージョンの変更に成功すると、再起動して新しい HSM バージョンに変更するように指示されます。プロンプトが表示されたら、**Yes**（はい）をクリックします。
5. マスターキーがファイアウォール上にない場合、クライアントのバージョンのアップグレードは失敗します。メッセージを **Close**（閉じる）、マスターキーをファイアウォールのローカルにします。
   - ハードウェアのセキュリティ モジュール プロバイダを編集し、 **Master Key Secured by HSM**（**HSM** が保護するマスターキー）オプションを使用不可（クリア）にします。
   - **OK** をクリックします。
   - **Device (**デバイス**)** > **Master Key and Diagnostics (**マスター キーおよび診断**)** の順に選択し、Master Key (マスター キー) を編集します。
   - **Current Master Key**（現在のマスターキー）を入力します。同じキーを**New Master Key**（新規マスターキー）にしてから **Confirm New Master Key**（マスターキーの確認）を行うことができます。
   - **OK** をクリックします。
   - 最初の 4 つのステップを繰り返して **Select HSM Client Version**（**HSM** クライアント バージョンの選択）を行い、再起動します。

SafeNet Network HSMとの接続のセットアップ

Palo Alto Networks のファイアウォール（HSM クライアント）および SafeNet Network HSM サーバー間の接続をセットアップするには、サーバーの IP アドレスを指定し、ファイアウォールをサーバーに認証するためのパスワードを入力し、ファイアウォールをそのサーバーに登録する必要があります。HSM クライアントを設定する前に、HSM サーバー上のファイアウォール

のパーティションを作成し、ファイアウォール上の SafeNet ネットワーク クライアントのバージョンが SafeNet Network HSM サーバーと互換性があることを確認します（「HSM との接続の設定」を参照）。

HSM とファイアウォールが接続する前に、HSM はファイアウォールの IP アドレスに基づいてファイアウォールを認証します。そのため、DHCP を通して割り当てられる動的アドレスではなく、静的 IP アドレスを使用する用にファイアウォールの設定を行う必要があります。ファイアウォールの IP アドレスがランタイム中に変更されると、HSM の操作が停止します。

HSM 設定は、高可用性（*HA*）ファイアウォール ピア間では同期されません。そのため、ピアごとに個別に *HSM* を設定する必要があります。アクティブ/パッシブ *HA* 設定では、フェイルオーバーを 1 回手動で実行し、各 *HA* ピアを個別に設定して、*HSM* に対して認証する必要があります。この初回のフェイルオーバーを手動で行った後は、適切な機能のファイルオーバーに関するユーザーの操作は不要です。

STEP 1 | 各 SafeNet Network HSM 用の接続設定を定義します。

1. ファイアウォール Web インターフェイスにログインして、**Device (デバイス)** > **Setup (セットアップ)** > **HSM** を選択します。
2. Hardware Security Module Provider (ハードウェア セキュリティ モジュールのプロバイダー) 設定を編集し、**Provider Configured (設定済みのプロバイダー)** を **SafeNet Network HSM** に設定します。
3. 次のようにして各 HSM サーバーを **Add (追加)** します。高可用性（HA）HSM 設定には、少なくとも 2 つのサーバーが必要です。最大 16 個の HSM サーバーのクラスタを持つことができます。クラスタ内のすべての HSM サーバーは、同じ SafeNet バージョンを実行する必要があり、別途認証しなければなりません。SafeNet クラスタは、クラスタ全体でキーを複製する場合にのみ使用してください。また、SafeNet HSM サーバーを最大 16 台まで追加して、個別に機能させることもできます。
   1. HSM サーバーの**Module Name**（モジュール名）（最大 31 文字の ASCII 文字列）を入力します。
   2. HSM **Server Address (サーバー アドレス)** については IPv4 アドレスを入力します。
4. （HA のみ）**High Availability**（高可用性）を選択して、**Auto Recovery Retry (自動回復の再試行)**値（HSM クライアントが HSM サーバーへの接続を回復しようとしてから HSM HA ピア サーバーにフェイルオーバーする最大回数。範囲は 0～500、デフォルトは 0）を指定し、and enter a **High Availability Group Name**（高可用性グループ名）（最大 31 文字の ASCII 文字列）を入力します。

   2 つ以上の *HSM* サーバーを設定する場合は、***High Availability***（高可用性）を有効にすることがベストプラクティスです。それ以外の場合、ファイアウォールは追加の *HSM* サーバーを使用しません。
5. **OK** をクリックし、変更を **Commit (コミット)** します。

STEP 2 | （任意）ファイアウォールを管理インターフェイスを通して接続（デフォルト）したくない場合は、HSM に接続するためのサービスルートを設定します。

> *HSM* 用のサービスルートを設定する場合、***clear session all*** *CLI* コマンドを実行すると、既存のすべての *HSM* セッションがクリアされ、すべての *HSM* がダウンした状態になり、その後起動します。*HSM* を回復させるために必要な数秒の間は、すべての *SSL/TLS* 操作が失敗します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Services (サービス)** を選択して **Service Route Configuration (サービスルート設定)** をクリックします。
2. サービスルートを **Customize (カスタマイズ)** します。**IPv4** タブはデフォルトで有効になっています。
3. Service (サービス) 列の **HSM** をクリックします。
4. HSM 用の **Source Interface (ソース インターフェイス)** を選択します。
5. **OK** をクリックし、変更を **Commit (コミット)** します。

STEP 3 | HSM を認証するようにファイアウォールを設定します。

1. **Device (デバイス)** > **Setup (セットアップ) Setup Hardware Security Module (ハードウェア セキュリティ モジュールのセットアップ)** を選択します。
2. HSM **Server Name (サーバー名)** を選択します。
3. 認証と信頼証明書に対して **Automatic (自動)** または **Manual (手動)** を選択します。
4. ファイアウォールを HSM に対して認証するための **Administrator Password**（管理者パスワード）を入力します。
5. **OK** をクリックします。

   ファイアウォールは HSM に関する認証を試行し、状態のメッセージを表示します。
6. 再度 **[OK]** をクリックします。

STEP 4 | HSM サーバーでファイアウォールを HSM クライアントとして登録し、HSM サーバーのパーティションにファイアウォールを割り当てます。

> *HSM* に同じ *<cl-name>* が既に登録されているファイアウォールがある場合は、まず ***client delete -client <cl-name>*** コマンドを実行して重複登録を削除する必要があります。*<cl-name>* は削除する登録済みクライアント *(*ファイアウォール*)* の名前です。

1. リモート システムから HSM にログインします。
2. **client register -c *<cl-name>* -ip *<fw-ip-addr>*** CLI コマンドを使用してファイアウォールを登録します。*<cl-name>* は HSM で使用するためにファイアウォールに割り当てる名前で、*<fw-ip-addr>* はそのファイアウォールの IP アドレスです。
3. **client assignpartition -c *<cl-name>* -p *<partition-name>*** CLI コマンドを使用してパーティションをファイアウォールに割り当てます。*<cl-name>* は **client register** コマンドを使用してファイアウォールに割り当てた名

前、*<partition-name>* はこのファイアウォールに割り当てる以前に構成されたパーティションの名前です。

STEP 5 | HSM パーティションに接続するようにファイアウォールを設定します。

1. **Device**（デバイス） > **Setup**（セットアップ） > **HSM** を選択して、( )ディスプレイを更新します。
2. **Setup HSM Partition (HSM** パーティションのセットアップ**)**(ハードウェア セキュリティ操作設定)を行います。
3. HSM のパーティションに対するファイアウォールの認証を行う **Partition Password**[パーティション パスワード] を入力します。
4. **OK** をクリックします。

STEP 6 | （HA のみ）前述の認証、登録、パーティション接続の各ステップを繰り返し、別の HSM を既存の HA グループに追加します。

設定から *HSM* を取り除く場合、前述のパーティション接続作業を繰り返し、削除された *HSM* を *HA* グループから取り除きます。

STEP 7 | ファイアウォールと HSM の接続および認証を確認します。

1. **Device (**デバイス**)** > **Setup (**セットアップ**)** > **HSM** を選択し、認証および接続の Status (ステータス) を確認します。
   - 緑—ファイアウォールが正常に HSM に認証・接続されています。
   - 赤—ファイアウォールが HSM への認証に失敗したか、HSM へのネットワーク接続がダウンしています。
2. Hardware Security Module Status (ハードウェア セキュリティ モジュール状態) の以下の列を確認して、認証状態を特定します。
   - **Serial Number (**シリアル番号**)** — ファイアウォールが正常に HSM に認証された場合、その HSM パーティションのシリアル番号。
   - **Partition**（パーティション） — ファイアウォールに割り当てられた HSM のパーティション名。
   - **Module State**（モジュール状態） — HSM 接続の現在の状態。Hardware Security Module Status (ハードウェア セキュリティ モジュールの状態) に HSM が表示される場合、この値は常に `Authenticated` (認証済み) になります。

nCipher nShield Connect HSM との接続のセットアップ

Remote File System (リモート ファイル システム - RFS) をハブとしてセットアップし、nCipher nShield Connect HSM を使用する組織内のすべてのファイアウォール（HSM クライアント）用にキーデータを同期します。ファイアウォール上の nShield Connect クライアントのバージョンが nShield Connect サーバーと互換性のあるものであることを確認する方法については、HSM との接続のセットアップを参照してください。

HSM とファイアウォールが接続する前に、HSM は IP アドレスに基づいてファイアウォールを認証します。そのため、DHCP を通して割り当てられる動的アドレスではなく、静的 IP アドレ

スを使用する用にファイアウォールの設定を行う必要があります。（ファイアウォールの IP アドレスがランタイム中に変更されると、HSM の操作が停止します）。

HSM 設定は、高可用性（*HA*）ファイアウォール ピア間では同期されません。そのため、ピアごとに個別に *HSM* を設定する必要があります。アクティブ/パッシブ *HA* 設定では、フェイルオーバーを 1 回手動で実行し、各 *HA* ピアを個別に設定して、*HSM* に対して認証する必要があります。この初回のフェイルオーバーを手動で行った後は、適切な機能のファイルオーバーに関するユーザーの操作は不要です。

STEP 1 | 各 nCipher nShield Connect HSM 用の接続設定を定義します。

1. ファイアウォール Web インターフェイスにログインして、**Device (デバイス)** > **Setup (セットアップ)** > **HSM** を選択します。
2. hardware security module （ハードウェア セキュリティ モジュール - HSM)Provider(プロバイダー)の 設定を編集し、**Provider Configured (設定済みのプロバイダー)** を **nShield Connect** に設定します。
3. 次のようにして各 HSM サーバーを **Add (追加)** します。HA HSM 構成では、サーバーが 2 つ必要になります。
   1. HSM サーバーの **Module Name (モジュール名)** を入力します。31 文字以下の任意の ASCII 文字列を指定できます。
   2. HSM **Server Address (サーバー アドレス)** については IPv4 アドレスを入力します。
4. **Remote Filesystem Address (リモート ファイルシステムのアドレス)** に IPv4 アドレスを入力します。
5. **OK** をクリックし、変更を **Commit (コミット)** します。

STEP 2 | （任意）ファイアウォールを管理インターフェイスを通して接続（デフォルト）したくない場合は、HSM に接続するためのサービスルートを設定します。

HSM 用のサービスルートを設定する場合、***clear session all*** *CLI* コマンドを実行すると、既存のすべての *HSM* セッションがクリアされ、すべての *HSM* がダウンした状態になり、その後起動します。*HSM* を回復させるために必要な数秒の間は、すべての *SSL/TLS* 操作が失敗します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Services (サービス)** を選択して **Service Route Configuration (サービスルート設定)** をクリックします。
2. サービスルートを **Customize (カスタマイズ)** します。**IPv4** タブはデフォルトで有効になっています。
3. Service (サービス) 列の **HSM** をクリックします。
4. HSM 用の **Source Interface (ソース インターフェイス)** を選択します。
5. **OK** をクリックし、変更を **Commit (コミット)** します。

STEP 3 | HSM サーバーでファイアウォールを HSM クライアントとして設定します。

この手順では、nShield Connect HSMのフロント パネル インターフェースを使用する手順を簡単に説明します。詳細は、nCipher のドキュメントを参照してください。

1. nCipher nShield Connect HSM のフロント パネル ディスプレイにログインします。
2. 右側のナビゲーション ボタンを使用して、**System (システム)** > **System configuration (システム設定)** > **Client config (クライアント設定)** > **New client (新規クライアント)** を選択します。
3. ファイアウォールの IP アドレスを入力します。
4. **System (システム)** > **System configuration (システム設定)** > **Client config (クライアント設定)** > **Remote file system (リモート ファイルシステム)** を選択し、RFS をセットアップするクライアント コンピューターの IP アドレスを入力します。

STEP 4 | ファイアウォールからの接続を承諾するよう、RFS を設定します。

1. Linux クライアントから RFS にログインします。
2. **anonkneti** CLI コマンド (*<ip-address>* は HSM IP アドレス) を実行して、クライアントに対して HSM を認証する電子シリアル番号 (ESN) と K_{NETI}<ip-address> キーのハッシュを取得します。

   以下に例を示します。

   ```
   anonkneti 192.0.2.1
   ```

   ```
   B1E2-2D4C-E6A2 5a2e5107e70d525615a903f6391ad72b1c03352c
   ```

   この例では、B1E2-2D4C-E6A2 は、ESM であり、5a2e5107e70d525615a903f6391ad72b1c03352c は、K_{NETI} キーのハッシュです。
3. スーパーユーザー アカウントから以下のコマンドを使用し、RFS をセットアップします。

   ```
   rfs-setup --force <ip-address> <ESN> <hash-Kneti-key>
   ```

   <ip-address> は HSM の IP アドレス、*<ESN>* は電子シリアル番号、*<hash-Kneti-key>* は K_{NETI} キーのハッシュです。

   以下の例では、この手順で取得した値を使用します。

   ```
   rfs-setup --force 192.0.2.1 B1E2-2D4C-E6A2
    5a2e5107e70d525615a903f6391ad72b1c03352c
   ```
4. 次のコマンドを使用し、RFS 上の HSM クライアントの送信を許可します。

   ```
   rfs-setup --gang-client --write-noauth <FW-IPaddress>
   ```

   ここで、*<FW-IPaddress>* はファイアウォールIP アドレスです。

STEP 5 | ファイアウォールを HSM に認証します。

1. ファイアウォールの Web インターフェイスで **Device (デバイス)** > **Setup (セットアップ)** > **HSM** を選択し、さらに **Setup Hardware Security Module (ハードウェア セキュリティ モジュールのセットアップ)** を選択します。
2. **OK** をクリックします。

   ファイアウォールは HSM に関する認証を試行し、状態のメッセージを表示します。
3. **OK** をクリックします。

STEP 6 | **Device (デバイス)** > **Setup (セットアップ)** > **HSM** を選択し、さらに **Synchronize with Remote Filesystem (リモート ファイルシステムと同期)** を選択することで、ファイアウォールを RFS と同期します。

STEP 7 | ファイアウォールと HSM の接続および認証を確認します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **HSM** を選択し、認証および接続の Status (ステータス) を確認します。
   - 緑—ファイアウォールが正常に HSM に認証・接続されています。
   - 赤—ファイアウォールが HSM への認証に失敗したか、HSM へのネットワーク接続がダウンしています。
2. Hardware Security Module Status (ハードウェア セキュリティ モジュール状態)を確認し、認証状態を判断します。
   - **Name** （名前） — HSM の名前。
   - **IP address** （**IP** アドレス） — HSM の IP アドレス。
   - **Module State** （モジュール状態） — HSM 接続の現在の状態：`Authenticated` (認証済み) あるいは `NotAuthenticated` (未認証)。

HSM を使用したマスター キーの暗号化

マスターキーは、ファイアウォールおよび Panorama 上のすべての秘密鍵およびパスワードを暗号化します。セキュリティ要件で秘密鍵を安全な場所に保存する必要がある場合は、HSM 上に保存されている暗号化キーを使用してマスター キーを暗号化できます。その後、ファイアウォールあるいは Panorama は、ファイアウォールでパスワードまたは秘密鍵の復号化が必要になるたびに、HSM にマスター キーを復号化するように要求します。通常、HSM は、セキュリティを向上させるため、ファイアウォールあるいは Panorama とは別の高度に安全な場所に設置されます。

HSM では、ラッピング キーを使用してマスター キーを暗号化します。セキュリティを維持するために、このラッピング キーは定期的に変更（リフレッシュ）する必要があります。

以下のトピックでは、初めにマスター キーを暗号化する方法とマスター キーの暗号化を更新する方法を説明します。

- マスター キーの暗号化
- マスター キーの暗号化の更新

マスター キーの暗号化

特定のファイアウォールでマスター キーがこれまで暗号化されていなかった場合、以下の手順を使用してマスター キーを暗号化します。キーの初回の暗号化時、または、新規マスター キーを定義するか、暗号化する場合に、この手順を使用します。以前に暗号化されたキーの暗号化を更新する場合は、マスター キーの暗号化の更新を参照してください。

STEP 1 | **Device** > **Master Key and Diagnostics (**マスター キーおよび診断**)** を選択します。

STEP 2 | **Master Key (**マスター キー**)** フィールドで、ファイアウォールでのすべての秘密鍵とパスワードを暗号化するために現在使用されているキーを指定します。

STEP 3 | マスター キーを変更する場合、新規マスター キーを入力して、確認します。

STEP 4 | **HSM** チェックボックスをオンにします。

- **Life Time (ライフ タイム)**—マスター キーが期限切れになるまでの期間を日数と時間数で指定します（範囲は 1 ～ 730 日）。
- **Time for Reminder (リマインダーの時間)**—有効期限が迫っていることをユーザーに通知する時期を、期限切れまでの日数と時間数で指定します（範囲は 1 ～ 365 日）。

STEP 5 | **OK** をクリックします。

マスター キーの暗号化の更新

ベストプラクティスとして、キーを暗号化するラッピング キーを変更させ、定期的にマスター キーの暗号化を更新するようにしてください。この変更頻度はアプリケーションによって異なります。ラッピング キーは HSM 上にあります。以下のコマンドは、SafeNet Network および nCipher nShield Connect HSM で同じです。

STEP 1 | ファイアウォール CLI へログインします。

STEP 2 | 以下の CLI コマンドを使用して、HSM でマスター キーのラッピング キーを交換します。

```
> request hsm mkey-wrapping-key-rotation
```

HSM でマスター キーが暗号化されている場合、CLI コマンドでは、HSM で新しいラッピング キーを生成し、その新しいラッピング キーを使用してマスター キーを暗号化します。

HSM でマスター キーが暗号化されていない場合、CLI コマンドでは、今後使用するために HSM で新しいラッピング キーを生成します。

古いラッピング キーはこのコマンドでは削除されません。

HSM での秘密鍵の保存

セキュリティを強化するために、HSM を使用して、以下の SSL/TLS 復号化に使用する秘密鍵を保護できます。

- SSL 転送プロキシ – HSM に、SSL/TLS フォワード プロキシ操作で証明書を署名するフォワード トラスト証明書の秘密鍵を保存できます。保存後、ファイアウォールは、この操作中に生成する証明書を HSM に送信して署名を得てから、クライアントに証明書を転送します。
- SSL インバウンド インスペクション – HSM に、SSL/TLS インバウンド インスペクションを実行している内部サーバーの秘密鍵を保存できます。

DHE あるいは ECDHE キー交換アルゴリズムを使用してSSL 復号化のための Perfect Forward Secrecy（PFS）サポートを有効化する場合、HSM を使用し、SSL インバウンド インスペクション用の秘密鍵を保存することができます。また、TLSv1.3 を使用しない限り、SSLフォワード プロキシあるいは SSLインバウンド インスペクションの復号化に使用する ECDSA キーを HSM を使用して保存することもできます。TLSv1.3トラフィックの場合、PAN-OS は SSL フォワード プロキシの HSM のみをサポートします。SSL インバウンド検査用の HSM はサポートしていません。

STEP 1 | HSM 上で、復号化デプロイメントで使用する証明書および秘密鍵をインポートあるいは生成します。

HSM に証明書および秘密鍵をインポートまたは生成する手順については、HSM のドキュメントを参照してください。

STEP 2 | （nCipher nShield Connectのみ）nCipher nShield Remote File System (リモート ファイル システム - RFS) からファイアウォールにキー データを同期します。

SafeNet Network HSM との同期は自動で行われます。

1. ファイアウォール Web インターフェイスにアクセスして、**Device (デバイス)** > **Setup (セットアップ)** > **HSM** を選択します。
2. **Synchronize with Remote Filesystem**（リモート ファイルシステムと同期）（Hardware Security Operations（ハードウェア セキュリティ操作））。

STEP 3 | HSM に保存された鍵に対応する証明書をインポートします。

1. **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択し、**Import**（インポート）をクリックします。
2. **Certificate Name**[証明書名] を入力します。
3. **Browse (参照)** をクリックして、HSM 上の **Certificate File (証明書ファイル)** を選択します。
4. **File Format**[ファイル形式] を選択します。
5. **Private Key resides on Hardware Security Module (秘密鍵はハードウェア セキュリティ モジュール上にあります)** を選択します。
6. **OK** をクリックし、変更を **Commit (コミット)** します。

STEP 4 | （フォワード トラスト証明書のみ）SSL/TLS 転送プロキシで使用する証明書を有効にします。

1. ステップ 3 でインポートした証明書を編集用に開きます。
2. **Forward Trust Certificate (フォワード トラスト証明書)** を選択します。
3. **OK** をクリックし、変更を **Commit (コミット)** します。

STEP 5 | 証明書をファイアウォールに正常にインポートしたことを確認します。

手順 3 でインポートした証明書を見つけて、[キー] 列のアイコンを確認します。

- ロック アイコン – 証明書の秘密鍵が HSM にあります。
- エラー アイコン – 秘密鍵が HSM にないか、HSM が適切に認証または接続されていません。

HSM デプロイメントの管理

以下のタスクを実行して、HSM デプロイメントを管理できます。

HSM 設定を表示します。

Device（デバイス） > **Setup**（セットアップ） > **HA** を選択します。

HSM の詳細情報を表示します。

Hardware Security Operations（ハードウェア セキュリティ操作）セクションで **Show Detailed Information**（詳細情報を表示）を選択します。

HSM サーバーに関する情報、HSM HA 状態、および HSM ハードウェアが表示されます。

サポート ファイルをエクスポートします。

Hardware Security Operations（ハードウェア セキュリティ操作）セクションで**Export Support File** （サポート ファイルのエクスポート） を選択します。

カスタマー サポートがファイアウォールの HSM 設定に関する問題に対処する上で役立つテスト ファイルが作成されます。

HSM 設定をリセットします。

Hardware Security Operations （ハードウェア セキュリティ操作） セクションから **Reset HSM Configuration**（**HSM** 設定のリセット）を選択します。

このオプションを選択すると、すべての HSM 接続が削除されます。このオプションを使用した後は、すべての認証手順を繰り返す必要があります。

高可用性（HA）

高可用性（HA）は、2つのファイアウォールを1つのグループに、または最大16のファイアウォールを1つのHA クラスタ内に配置するデプロイメントで、ネットワーク上の単一障害点を回避するために2つの設定が同期されます。ファイアウォール ピア間のハートビート接続では、ピアがダウンした場合シームレスにフェイルオーバーを実行できます。HA をセットアップすると冗長性が得られるため、ビジネス継続性を確保できます。

- HA
- HA の概念
- アクティブ/パッシブ HA のセットアップ
- アクティブ/アクティブ HA のセットアップ
- HA クラスタリングの概要
- HA クラスタリングのベストプラクティスとプロビジョニング
- HA クラスタリングの設定
- HA1 SSH 鍵の更新およびキーのオプションの設定
- HA ファイアウォールの状態
- リファレンス：HA 同期
- CLI Cheat Sheet - HA

HA

2つの Palo Alto Networks ファイアウォールを HAペアとして設定するか、最大16のファイアウォールを HA クラスタのピア メンバーとして設定することができます。クラスタ内のピアは、HAペアまたはスタンドアロン ファイアウォールとすることが可能です。HA では、ペアのファイアウォールに障害が発生した場合に、代替ファイアウォールを使用できるようにすることで、ダウンタイムを最小限に抑えることができます。HAペアまたはクラスとのファイアウォールでは、専用またはインバンドの HA ポートをファイアウォール上で使用することにより、ネットワーク、オブジェクト、ポリシー設定などのデータを同期して、状態情報を管理します。管理インターフェイスの IP アドレスや管理者プロファイルなどのファイアウォール固有の設定、HA 固有の設定、ログ データ、およびアプリケーション コマンド センター（ACC）の情報は、ペア間で共有されません。

アプリケーションおよびログのビューを HAペア間で統合したい場合、Panorama という Palo Alto Networks の集中管理システムを使用する必要があります。Panorama 管理者ガイドのコンテキストスイッチ–ファイアウォールまたは Panoramaを参照してください。アクティブ/パッシブ HA の前提条件とアクティブ/アクティブ HA の前提条件に相談してください。Panorama を使用して HA クラスタ メンバーをプロビジョニングすることが強く推奨されます。HA クラスタリングのベストプラクティスとプロビジョニングに相談してください。

HAペアまたは HA クラスタの一方のファイアウォールで障害が発生した場合、ペアのもう一方のファイアウォールがトラフィックを保護するタスクを引き継ぎます。このイベントをフェイルオーバーといいます。フェイルオーバーが引き起こされる条件は、以下のとおりです。

- モニター対象となる 1 つ以上のインターフェイスに障害が発生した場合。(リンク モニタリング)
- ファイアウォールで指定する 1 つ以上の宛先に到達できない場合。(パス モニタリング)
- ファイアウォールがハートビート ポーリングに応答しない場合。（ハートビート ポーリングおよび Hello メッセージ)
- パケットパスヘルスモニタリングとして知られるように、重要なチップやソフトウェアコンポーネントが故障した場合。

Palo Alto Networks ファイアウォールでは、少数の例外を除いて、セッション同期および設定の同期と、ステートフルなアクティブ/パッシブまたはアクティブ/アクティブ高可用性をサポートします。

- Azure 上の VM-Series ファイアウォールおよびAWS 上の VM-Series ファイアウォールはアクティブ/パッシブ HA しかサポートしていません。

  AWS の場合、Amazon Elastic Load Balancing (ELB) サービスでファイアウォールをデプロイする場合は HA をサポートしていません (この場合、ELB サービスがフェイルオーバー機能を提供します)。
- Google Cloud Platform 上の VM Series ファイアウォールは HA をサポートしていません。

まず、HA Concepts と、HA クラスタリングを構成する場合はHA クラスタリングの概要について理解します。

HA の概念

以下のトピックでは、Palo Alto Networks ファイアウォールでの HA の動作について、その概念を中心に説明します。

- HA モード
- HA リンクおよびバックアップ リンク
- デバイス優先度およびプリエンプション
- フェイルオーバー
- アクティブ/パッシブ HA のための LACP および LLDP プレネゴシエーション
- フローティング IP アドレスと仮想 MAC アドレス
- ARP ロード共有
- ルート ベース冗長性
- HA タイマー
- セッション オーナー
- セッション セットアップ
- NAT in Active/Active HA Mode[アクティブ/アクティブHAモードのNAT]
- ECMP in Active/Active HA Mode[アクティブ/アクティブHAモードのECMP]

HA モード

HAペアのファイアウォールは、以下の 2 つのモードのうち 1 つでセットアップできます:

- アクティブ/パッシブ – 一方のファイアウォールがトラフィックをアクティブに管理し、もう一方のファイアウォールは同期を取って、障害が発生したときにアクティブ状態に移行できるよう備えます。このモードでは、両方のファイアウォールで同じ設定を共有し、パス、リンク、システム、またはネットワークに障害が発生するまでは、一方がアクティブにトラフィックを管理します。アクティブなファイアウォールで障害が発生すると、パッシブ ファイアウォールがアクティブ状態に移行し、シームレスに同じポリシーを引き継いで適用し、ネットワーク セキュリティを維持します。アクティブ/パッシブ HA は、バーチャル ワイヤーと、レイヤー 2 およびレイヤー 3 デプロイメントでサポートされています。
- アクティブ/アクティブ – ペアのファイアウォールの両方がアクティブな状態でトラフィックを処理し、セッションのセットアップやオーナーシップを同期的に操作します。両方のファイアウォールはセッションテーブルとルーティングテーブルを維持し、互いに同期します。アクティブ/アクティブ HA は、バーチャル ワイヤー モードとレイヤー 3 展開でのみサポートされます。

  アクティブ/アクティブ HA モードでは、ファイアウォールは DHCP クライアントをサポートしません。さらに、アクティブプライマリファイアウォールのみが DHCP リレーとして機能

します。アクティブセカンダリファイアウォールが DHCP ブロードキャストパケットを受信すると、それらをドロップします。

アクティブ/アクティブ設定はロードバランストラフィックではありません。ピアにトラフィックを送信すればロードシェアは可能ですが、ロードバランスは発生しません。両方のファイアウォールにロードシェアする方法としては複数の *ISP* とロードバランサーがあります。

アクティブ/パッシブまたはアクティブ/アクティブモードのどちらを使用するか決定する際には、以下の差を考慮してください。

- アクティブ/パッシブモードはデザインがシンプルで、ルーティングとトラフィックフロー問題をトラブルシュートするのがはるかに簡単です。アクティブ/パッシブモードはレイヤー 2 展開をサポートしますが、アクティブ/アクティブモードはサポートしません。
- アクティブ/アクティブモードには、より複雑なネットワークが可能な高度なデザインコンセプトが必要です。アクティブ/アクティブ HA の実行方法によって、適切なフェイルオーバーを提供するために、両方のファイアウォールでネットワーキングプロトコルを起動する、NAT プールを複製する、フローティング IP プロセスをデプロイするなどの追加設定が必要になることもあります。両方のファイアウォールはアクティブにトラフィックを処理しているので、ファイアウォールはレイヤー 7 コンテンツを実行するために、セッションオーナーとセッションセットアップの補助コンセプトを使います。各ファイアウォールが独自のルーティングインスタンスを必要とし、あなたが、常に両方のファイアウォールから、フル、リアルタイム冗長性を必要とする場合は、アクティブ/アクティブモードを推奨します。両方のファイアウォールはアクティブにトラフィックを処理しているので、アクティブ/アクティブモードのフェイルオーバーはアクティブ/パッシブモードより速く、ピークトラフィックフローをアクティブ/パッシブモードより良好に処理できます。

アクティブ/アクティブモードでは、*HA* ペアを使って、通常、*1*個のファイアウォールが処理できるものよりも多くのトラフィックを一時的に処理できます。しかし、*1*個のファイアウォールに障害が発生すると、全てのトラフィックが *HA* ペア内の残りのファイアウォールにリダイレクトされるので、これを基準にすることはできません。コンテンツインスペクションを有効にした状態で、残りのファイアウォールが、トラフィックロードの最大容量を処理できるようにデザインする必要があります。デザインが残りのファイアウォールの容量をオーバーサブスクライブすると、長い待ち時間やアプリケーション障害が発生することがあります。

ファイアウォールをアクティブ/パッシブモードでセットアップする方法の詳細は、アクティブ/パッシブ HA のセットアップを参照してください。ファイアウォールをアクティブ/アクティブモードでセットアップする方法の詳細は、アクティブ/アクティブ HA のセットアップを参照してください。

HA クラスタでは、すべてのメンバーがアクティブであると見なされます。パッシブ ファイアウォールの概念は、HA クラスターに追加した後もアクティブ/パッシブの関係を維持できるクラスタ内の HAペアを除いてありません。

HA リンクおよびバックアップ リンク

HA ペアのファイアウォールでは、HA リンクを使用してデータを同期し、状態情報を管理します。ファイアウォールの一部のモデルには、コントロール リンク（HA1）とデータ リンク（HA2）という専用の HA ポートがありますが、それ以外のモデルでは、インバンド ポートを HA リンクとして使用する必要があります。

- 専用の HA ポートを持つファイアウォールの場合は、これらのポートを使用してファイアウォール間の通信と同期を管理します。詳細は、「Palo Alto Networks ファイアウォール上の HA ポート」を参照してください。
- PA-220 および PA-220R ファイアウォールなど、専用の HA ポートを持たないファイアウォールの場合、ベストプラクティスとして、HA1 ポート用にmanagement port (管理ポート - MGT port) を使用し、HA1 バックアップ用にデータプレーン ポートを使用してください。

専用の *HA* ポートのないファイアウォールの場合は、環境に基づいて *HA1* および *HA1* のバックアップに使用するポートを決定し、どれが最も使用されず、最も混雑していないかを理解します。*HA1* を最適なインターフェースに割り当て、*HA 1*バックアップを他のインターフェースに割り当てます。

HA クラスタ内の HAピアは、スタンドアロン クラスタ メンバーと HAペアとの組み合わせにすることができます。HA クラスタ メンバーは HA4 リンクと HA4 バックアップ リンクを使用してセッション状態の同期を実行します。HA1 (コントロール リンク)、HA2 (データ リンク)、およびHA3 (パケット転送リンク) は、HA ペアではないクラスタ メンバー間ではサポートされていません。

HA リンクおよびバックアップ リンク	説明
コントロール リンク	HA1 リンクは、Hello、ハートビート、HA 状態、ルーティング用の管理プレーンの同期、User-ID などの情報交換に使用します。ファイアウォールはまた、このリンクを使用して設定の変更をペアと同期します。HA1 リンクはレイヤー 3 リンクのため、IP アドレスが必要です。 HA ピア間でハートビートを交換するために ICMP が使用されます。 HA1 に使用するポート—クリア テキスト通信には TCP ポート 28769 と 28260、暗号化通信（SSH over TCP）にはポート 28 を使用します。 HA1 リンクで暗号化を有効にすると、HA1 SSH 鍵の更新およびキーのオプションの設定することもできます。
データ リンク	HA2 リンクを使用して、セッション、テーブルの転送、IPSec SA、および ARP テーブルを HA ペアのファイアウォール間で同期します。HA2 リンクのデータ フローは（HA2 キープアライブを除き）常に単向性で、データがアクティブまたはアクティブ-プライマリ ファイアウォールからパッシブまたはアクティブ-セカンダリ ファイア

HA リンクおよびバックアップ リンク	説明
	ウォールに送られます。HA2 リンクはレイヤー 2 リンクであり、デフォルトで EtherType 0x7261 を使用します。 HA2 で使用するポート: HA データ リンクは、IP （プロトコル番号 99）または UDP （ポート 29281）のいずれかを転送ポートとして使用するように設定できるため、HA データ リンクはサブネットをまたぐことができます。
HA1 および HA2 バックアップ リンク	HA1 リンクと HA2 リンクの冗長性を実現します。専用バックアップ リンクが使用できない場合、HA1 と HA2 の両方の接続のバックアップリンクに帯域内ポートを使用できます。バックアップ HA リンクを設定する場合は、以下のガイドラインを考慮してください。 • プライマリ HA リンクとバックアップ HA リンクの IP アドレスを重複させることはできません。 • HA バックアップ リンクは、プライマリ HA リンクとは別のサブネット上になければなりません。 • HA1 バックアップと HA2 バックアップのポートは、異なる物理ポート上で設定する必要があります。HA1 バックアップ リンクでは、ポート 28770 と 28260 が使用されます。 • PA-3200 Series のファイアウォールは HA1-backup リンク用の IPv6 アドレスをサポートしていないため、IPv4 アドレスを使用してください。 *Palo Alto Networks では、HA1 または HA1 のバックアップ リンクにインバンド ポートを使用する場合、ハートビート バックアップ（MGT インターフェイスでポート 28771 を使用）を有効にすることをお勧めします。*
パケット転送リンク	アクティブ/アクティブ展開では、HA1リンクとHA2リンクに加え、専用のHA3リンクが必要です。ファイアウォールはこのリンクを使って、セッションセットアップおよび非対称トラフィックフロー時にパケットをピアに転送します。HA3 リンクは、MAC-in-MAC カプセル化を使用するレイヤー 2 リンクです。レイヤー 3 アドレシングや暗号化はサポートしていません。PA-7000 シリーズ ファイアウォールはNPC one-for-one 内部でセッションを同期します。PA-800 Series、PA-3200 Series、PA-3400 Series、PA-5200 Series、および PA-5400 Series firewall では、集約インターフェイスを HA3 リンクとして設定できます。集約インターフェイスは HA3 に冗長性を与えることもできますが、あなたは HA3 リンクにバックアップリンクを設定することはできません。PA-3200 Series、PA-3400 Series、PA-5200 Series、PA-5400 Series、および PA-7000 Series firewalls では、専用 HSCI ポートが HA3 リンクをサポートします。ファイアウォールは適切なパケットヘッダを HA3 リンクを通過する

HA リンクおよびバックアップ リンク	説明
	パケットに追加するので、このリンク上の MTU は転送する最大パケット長よりも大きくなければなりません。
HA4 リンクおよび HA4 バックアップ リンク	HA4リンクと HA4バックアップ リンクは、同じクラスタ ID を持つすべての HA クラスタ メンバー間でセッション キャッシュの同期を実行します。クラスタ メンバー間の HA4リンクは、レイヤー2 キープアライブ メッセージを送受信することでクラスタ メンバー間の接続障害を検出します。ファイアウォール ダッシュボード上の HA4 と HA4 バックアップ リンクのステータスを閲覧してください。

Palo Alto Networks ファイアウォール上の HA ポート

高可用性（HA）設定で 2 つの Palo Alto Networks® ファイアウォールの接続時に、HA リンクおよび Backup リンク の専用 HA ポートを使用することを推奨します。これらの専用ポートには、HA 制御および同期トラフィックに使用される HA1、HA1-A、および HA1-B というラベルの HA1 ポート、 HA セッション セットアップ トラフィックに使用される HA2 および高速シャーシ インターコネクト（HSCI）ポートがあります。PA-5200 シリーズのファイアウォールには、HA1 トラフィック用に設定できる AUX-1 および AUX-2 というラベルの多目的補助ポートがあります。

また、HA3 用の HSCI ポートを設定することもできます。これは、セッションの設定や非対称トラフィック フロー（アクティブ/アクティブ HA のみ）中にピア ファイアウォールへのパケット転送に使用されます。HSCI ポートは、HA2 トラフィック、HA3 トラフィック、またはその両方に使用できます。

HA1 および *AUX* リンクでは、管理プレーンにある機能の同期を提供します。管理プレーンの専用 *HA* インターフェイスを使用する方が、インバンド ポートを使用するより効率的です。これは、データプレーンを介して同期パケットを渡す必要がないためです。

ファイアウォールに専用の *HA* ポート*(PA-220* や *PA-400 Series* など*)*がない場合は、データポートを *HA* インターフェイスとして設定できます。ファイアウォールに専用の *HA* ポートがあり、専用の *HA* バックアップ ポートがない場合は、データポートを専用の *HA* ポートへのバックアップとして設定することもできます。

可能であれば、ネットワークに問題が発生した場合に発生する可能性のある *HA* リンクおよび通信の問題を避けるため、*HA* ペア内の *2* つのファイアウォール間で直接 *HA* ポートを接続してください（スイッチまたはルータを介さない）。

以下の表には専用 HA ポートの説明および HA リンクおよびバックアップ リンクへの接続方法を説明が記されています：

model	フロント パネル専用ポート

PA-800 Series ファイアウォール	• **HA1** および **HA2**—HA モードの両方で、HA1 および HA2 に使用する Ethernet 10Mbps/100Mbps/1000Mbps ポート。
	  • **HA1** トラフィックの場合—最初のファイアウォールの HA1 ポートをペアの 2 つ目のファイアウォールの HA1 ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	  • **HA2** トラフィックの場合—最初のファイアウォールの HA2 ポートをペアの 2 つ目のファイアウォールの HA2 ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。

PA-3200シリーズ ファイアウォール	• **HA1-A** および **HA1-B**—HA モードの両方で、HA1 およびトラフィックに使用する Ethernet 10Mbps/100Mbps/1000Mbps ポート。
	  • **HA1** トラフィックの場合—最初のファイアウォールの HA1-A ポートをペアの 2 つ目のファイアウォールの HA1-A ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	  • **HA1-A** 接続へのバックアップの場合—最初のファイアウォールの HA1-B ポートをペアの 2 つ目のファイアウォールの HA1-B ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	  障害または手動による再起動のためにファイアウォールのデータプレーンが再起動すると、*HA1-B* リンクも再起動します。これが発生し、*HA1-A* リンクが接続されているが設定されていない場合、スプリットブレイン状態が発生します。したがって、*HA1-A1* ポートと *HA1-B* ポートを接続して設定し、冗長性を提供し、スプリットブレイン障害を予防することを推奨します。
	  ファイアウォールの *SFP* ポートは、*PAN-OS* または *Panorama* を介して *HA1-A* および *HA1-B* ポートして再マッピングすることが可能です。
	• **HSCI** - HSCI ポートは、HA 設定の 2 つの PA-3200 シリーズ ファイアウォールを接続するレイヤー 1 SFP+ インターフェイスです。このポートは、HA2 接続、HA3 接続、またはその両方に使用します。
	  HSCI ポートで伝送されるトラフィックは、ルーティング不可能または切り替え可能ではない Raw レイヤー 1 トラフィックで

model	フロント パネル専用ポート
	す。したがって、HSCI ポートを直接相互に接続する必要があります（最初のファイアウォールの HSCI ポートから 2 番目のファイアウォールの HSCI ポートまで）。

PA-3400シリーズファイアウォール	• **HA1-A** および **HA1-B**—HA モードの両方で、HA1 およびトラフィックに使用する Ethernet 10Mbps/100Mbps/1000Mbps ポート。
	  • **HA1** トラフィックの場合—最初のファイアウォールの HA1-A ポートをペアの 2 つ目のファイアウォールの HA1-A ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	  • **HA1-A** 接続へのバックアップの場合—最初のファイアウォールの HA1-B ポートをペアの 2 つ目のファイアウォールの HA1-B ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	• **HSCI** - HSCI ポートは Layer 1 SFP+ インターフェイスで、HA 構成で 2 つの PA-3400 Series firewall を接続します。このポートは、HA2 接続、HA3 接続、またはその両方に使用します。
	HSCI ポートで伝送されるトラフィックは、ルーティング不可能または切り替え可能ではない Raw レイヤー 1 トラフィックです。したがって、HSCI ポートを直接相互に接続する必要があります（最初のファイアウォールの HSCI ポートから 2 番目のファイアウォールの HSCI ポートまで）。

PA-5200シリーズ ファイアウォール	• **HA1-A** および **HA1-B**—HA モードの両方で、HA1 およびトラフィックに使用する Ethernet 10Mbps/100Mbps/1000Mbps ポート。
	  • **HA1** トラフィックの場合—最初のファイアウォールの HA1-A ポートをペアの 2 つ目のファイアウォールの HA1-A ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	  • **HA1-A** 接続へのバックアップの場合—最初のファイアウォールの HA1-B ポートをペアの 2 つ目のファイアウォールの HA1-B ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	• **HSCI** - HSCI ポートは、HA 設定の 2 つの PA-5200 シリーズ ファイアウォールを接続するレイヤー 1 インターフェイスで

model	フロント パネル専用ポート
	す。このポートは、HA2 接続、HA3 接続、またはその両方に使用します。 *PA-5220* ファイアウォールの *HSCI* ポートは *QSFP+* ポートで、*PA-5250*、*PA-5260*、および *PA-5280* ファイアウォールの *HSCI* ポートは *QSFP28* ポートです。 HSCI ポートで伝送されるトラフィックは、ルーティング不可能または切り替え可能ではない Raw レイヤー 1 トラフィックです。したがって、HSCI ポートを直接相互に接続する必要があります（最初のファイアウォールの HSCI ポートから 2 番目のファイアウォールの HSCI ポートまで）。

PA-5200 シリーズファイアウォールの概要（続き）	• **AUX-1** および **AUX-2**—補助SFP+ ポートは、HA1、管理機能、または Panorama へのログ転送用に設定できる多目的ポートです。これらの機能のいずれかにファイバー接続が必要な場合は、これらのポートを使用します。
	  • **HA1** トラフィックの場合—最初のファイアウォールの HA1-A ポートをペアの 2 つ目のファイアウォールの HA1-A ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	  • **HA1-A** 接続へのバックアップの場合—最初のファイアウォールの HA1-B ポートをペアの 2 つ目のファイアウォールの HA1-B ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。

PA-5400シリーズファイアウォール (PA-5410, PA-5420, and PA-5430)	• **HA1-A** および **HA1-B** – イーサネット 1Gbps/10Gbps ポートは、両方の HA モード で HA1 トラフィックに使用されます。
	  • **HA1** トラフィックの場合—最初のファイアウォールの HA1-A ポートをペアの 2 つ目のファイアウォールの HA1-A ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	  • **HA1-A** 接続へのバックアップの場合—最初のファイアウォールの HA1-B ポートをペアの 2 つ目のファイアウォールの HA1-B ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	• **HSCI** – HSCI ポートは Layer 1 QSFP+ インターフェイスで、2 つの PA-5400 Series firewall を HA 構成で接続します。このポートは、HA2 接続、HA3 接続、またはその両方に使用します。
	
	HSCI ポートで伝送されるトラフィックは、ルーティング不可能または切り替え可能ではない Raw レイヤー 1 トラフィックで

model	フロント パネル専用ポート
	す。したがって、HSCI ポートを直接相互に接続する必要があります（最初のファイアウォールの HSCI ポートから 2 番目のファイアウォールの HSCI ポートまで）。

PA-5450ファイアウォール	• **HA1-A** および **HA1-B** – SFP/SFP+ 1Gbps/10Gbps ポートは、両方の HA Modes の HA1 トラフィックに使用されます。
	  • **HA1** トラフィックの場合–最初のファイアウォールの HA1-A ポートをペアの 2 つ目のファイアウォールの HA1-A ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	  • **HA1-A** 接続へのバックアップの場合–最初のファイアウォールの HA1-B ポートをペアの 2 つ目のファイアウォールの HA1-B ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	• **HSCI-A** および **HSCI-B** - HSCI ポートは Layer 1 QSFP+ インターフェイスで、HA 構成で 2 つの PA-5450 firewall を接続します。このポートは、HA2 接続、HA3 接続、またはその両方に使用します。
	HSCI ポートで伝送されるトラフィックは、ルーティング不可能または切り替え可能ではない Raw レイヤー 1 トラフィックです。したがって、次のようにこれらのポートを接続する必要があります：
	  • **HA2** および **HA3** トラフィックの場合–1 番目のファイアウォールの HSCI-A ポートを 2 番目のファイアウォールの HSCI-A ポートに直接接続します。
	  • **HSCI-A** 接続へのバックアップの場合–1 番目のファイアウォールの HSCI-B ポートを 2 番目のファイアウォールの HSCI-B ポートに直接接続します。

PA-7000シリーズ ファイアウォール	• **HA1-A** および **HA1-B**–HA モードの両方で、HA1 およびトラフィックに使用する Ethernet 10Mbps/100Mbps/1000Mbps ポート。
	  • **HA1** トラフィックの場合–最初のファイアウォールの HA1-A ポートをペアの 2 つ目のファイアウォールの HA1-A ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。
	  • **HA1-A** 接続へのバックアップの場合–最初のファイアウォールの HA1-B ポートをペアの 2 つ目のファイアウォールの

model	フロント パネル専用ポート
	HA1-B ポートに直接接続するか、スイッチまたはルーターを介してこれらのポートを接続します。 *NPC* データ ポートまたは管理（*MGT*）ポートで *HA1* を設定することはできません。 • **HSCI-A** および **HSCI-B**—HSCI ポートは、HA 設定の 2 つの PA-7000 シリーズ ファイアウォールを接続するレイヤー 1 QSFP+ インターフェイスです。このポートは、HA2 接続、HA3 接続、またはその両方に使用します。 HSCI ポートで伝送されるトラフィックは、ルーティング不可能または切り替え可能ではない Raw レイヤー 1 トラフィックです。したがって、次のようにこれらのポートを接続する必要があります： • **HA2** および **HA3** トラフィックの場合—1 番目のファイアウォールの HSCI-A ポートを 2 番目のファイアウォールの HSCI-A ポートに直接接続します。 *HA2* または *HA2/HA3* トラフィックの場合、*PA-7000* シリーズ ファイアウォールは *NPC* 間でセッションを*1*対*1*で同期させます。 • **HSCI-A** 接続へのバックアップの場合—1 番目のファイアウォールの HSCI-B ポートを 2 番目のファイアウォールの HSCI-B ポートに直接接続します。 *HA2* と *HA2-Backup* リンクは、*HSCI* ポートの代わりにデータプレーン インターフェースを使用するように設定できます。ただし、この方法で設定を行うと、*HA2* と *HA2-Backup* リンクの両方はデータプレーン インターフェースの使用が必須となります。*HA2*または *HA2-Backup* のいずれかにデータプレーン ポートと *HSCI* ポートが混在していると、コミットが失敗します。これは、*PA-7050-SMC*、*PA-7080-SMC*、*PA-7050-SMC-B*、および *PA-7080-SMC-B* に適用されます。

デバイス優先度およびプリエンプション

アクティブ-パッシブ HA ペアのファイアウォールにデバイス優先順位の値を割り当てることにより、アクティブ ロールを担うファイアウォールの優先性を示すことができます。トラフィックのアクティブな保護に HA ペアの特定のファイアウォールを使用する必要がある場合は、両方のファイアウォールでプリエンプティブ機能を有効にし、各ファイアウォールにデバイス優先順位の値を割り当てる必要があります。数値の小さい方のファイアウォール (つまり優先順位が高

い) が、アクティブに指定されます。もう一方のファイアウォールはパッシブ ファイアウォールです。

アクティブ-アクティブ HA ペアでも同様ですが、デバイス優先順位の値の割り当てにはデバイス *ID* が使用されます。同様に、デバイス ID の値がより小さいと、優先順位が高いことを示します。優先順位が高いファイアウォールはアクティブ-プライマリになり、ペアのファイアウォールがアクティブ-セカンダリになります。

デフォルトでは、ファイアウォールのプリエンプティブ機能が無効になっているため、両方のファイアウォールで有効にする必要があります。この機能を有効にすると、優先順位の高い（数値の低い方の）ファイアウォールが障害から回復した後に、そのファイアウォールをアクティブまたはアクティブ-プライマリ ファイアウォールとして再開させることができます。プリエンプションが発生すると、そのイベントがシステム ログに記録されます。

フェイルオーバー

HAペア (または HA クラスタ内のピア) の一方のファイアウォールで障害が発生した場合、そのピアがトラフィックを保護するタスクを引き継ぎます。このイベントをフェイルオーバーといいます。例えば、HA ペアのファイアウォールのモニター対象メトリックに障害が発生すると、フェイルオーバーが引き起こされます。ファイアウォールの障害を検出するためにファイアウォールが監視するメトリックは、以下のとおりです:

- ハートビート ポーリングおよび **Hello** メッセージ

  ファイアウォールは、Hello メッセージとハートビートを使用して、ピア ファイアウォールの応答状態と動作状態を確認します。設定した「*Hello* 間隔」で Hello メッセージがピアの一方から他方へ送信され、ファイアウォールの状態を確認します。ハートビートは、コントロール リンクを介した HA ピアに対する ICMP ping の一種で、ピアがこの ping に応答することで、ファイアウォールの接続および応答状態を証明します。デフォルトでは、ハートビートの間隔は 1000 ミリ秒です。ping は 1000 ミリ秒毎に送信され、ハートビートが 3 回連続で失敗した場合、フェイルオーバーが発生します。フェイルオーバーをトリガーする HA タイマーの詳細は、「HA タイマー」を参照してください。

- リンク モニタリング

  ファイアウォールが監視する物理インターフェースのグループ (リンク グループ) を指定できます。ファイアウォールはグループ内の各リンクの状態 (リンク アップまたはリンク ダウン) を監視します。リンク グループの障害状態を判定できます:グループ内の **Any (**任意の**)** リンク ダウンまたは **All (**すべての**)** リンク ダウンが、リンク グループ障害を構成します (ただし、必ずしもフェイルオーバーとは限りません)。

  複数のリンク グループを作成できます。したがって、リンク グループのセットの障害状態も判別できます: **Any (**任意の**)** リンク グループが失敗するか、**All (**すべての**)** リンク グループが失敗します。これにより、フェイルオーバーがいつトリガーされるかが決定します。デフォルトの動作では、**Any (**任意の**)**リンクグループ内の **Any (**任意の**)** リンクに障害が発生すると、ファイアウォールの HA 状態が非稼働（またはアクティブ/アクティブモードの暫定的な状態）に変わり、監視対象オブジェクトの障害を示します。

- パス モニタリング

  ファイアウォールが監視する IPアドレスの宛先 IP グループを指定できます。ファイアウォールは、ICMP ping を使用してネットワークを介したミッション クリティカルな IP アドレスへ

のフルパスを監視し、IPアドレスの到達可能性を確認します。デフォルトの ping 間隔は 200 ミリ秒です。10回の連続した ping (デフォルト値) が失敗した場合、IPアドレスは到達不能と見なされます。宛先 IP グループの IPアドレスの障害条件を指定します:グループ内の **Any (**任意の**)** IPアドレスに到達できないか **All (**すべての**)** IPアドレスに到達できません。バーチャル ワイヤ、VLAN、またはVirtual Router (仮想ルーター - VR)のパス グループに複数の宛先 IP グループを指定できます。パス グループ内の宛先 IP グループの障害条件を指定します:**Any (**任意**)**または **All (**すべて**)**で、これがパスグループの障害を構成します。複数のバーチャル ワイヤ パス グループ、VLAN パス グループ、およびVirtual Router (仮想ルーター - VR)パス グループを設定できます。

また、グローバルな障害状態を決定できます:**Any (**任意の**)** パス グループが失敗するか、**All (**すべての**)** パス グループが失敗します。これにより、フェイルオーバーがいつトリガーされるかが決定されます。デフォルトの動作では、**Any (**任意の**)** バーチャル ワイヤ、VLAN、またはVirtual Router (仮想ルーター - VR)パス グループの **Any (**任意の**)** 宛先IP グループで **Any (**任意の**)** IPアドレスの1つが到達不能になり、ファイアウォールが HA 状態を非作動 (またはアクティブ/アクティブモードの暫定状態) に変更し、監視対象オブジェクトの障害を示します。

上記のフェイルオーバーのトリガー条件に加えて、管理者がファイアウォールをサスペンド状態にした場合、またはプリエンプションが発生した場合も、フェイルオーバーが引き起こされます。

PA-3200 Series、PA-5200 Series、および PA-7000 Series のファイアウォールでは、内部ヘルス チェックに失敗したときにフェイルオーバーが引き起こされることがあります。このヘルス チェックは設定変更不可で、有効時は FPGA や CPU などの重要なコンポーネントに対して動作状態を監視します。さらに、プラットフォームには一般的なヘルスチェックが発生し、フェイルオーバーが生じます。

以下に、HA クラスタのメンバーである PA-7000シリーズ ファイアウォールでNetwork Processing Card (ネットワーク プロセッシング カード - NPC)に障害が発生した場合にどのような事が発生するかを説明します。

- HA クラスタリング セッション キャッシュ (他のメンバーのセッションのコピー) を保持するために使用されている NPC がダウンすると、ファイアウォールは機能しなくなります。これが発生した場合、セッション分散デバイス (ロードバランサーなど) はファイアウォールがダウンしていることを検出し、クラスターの他のメンバーにセッションロードを分散する必要があります。
- クラスタ メンバーの NPC がダウンし、その NPC でリンク モニタリングまたはパス モニタリングが有効になっていない場合、PA-7000シリーズ ファイアウォール メンバーはアップしたままですが、1つの NPC がダウンしているため容量が少なくなります。
- クラスタメンバーの NPC がダウンし、その NPC でリンク モニタリングまたはパス モニタリングが有効になっている場合、PA-7000シリーズ ファイアウォールは機能しなくなり、セッション分散デバイス (ロードバランサなど) はファイアウォールがダウンして、セッションの負荷をクラスタの他のメンバーに分散します。

アクティブ/パッシブ HA のための LACP および LLDP プレネゴシエーション

ファイアウォールが LACP または LLDP を使用する場合、フェイルオーバー時、これらのプロトコルのネゴシエーションはサブセカンドフェイルオーバーを防止します。しかし、パッシブファイアウォールでインターフェイスを有効化して、フェイルオーバー前に LACP と LLDP をネゴシエートすることができます。従って、パッシブまたは非稼働 HA 状態のファイアウォールは、LACP または LLDP を使用する隣接デバイスと通信できます。そうしたプレネゴシエーションはフェイルオーバーを加速します。

VM-Series ファイアウォールを除くすべてのファイアウォール モデルは、Ethernet または AE インターフェイスがレイヤー 2、レイヤー 3、またはバーチャル ワイヤー展開のいずれかであるかに応じて、プレネゴシエーション設定をサポートします。HA パッシブファイアウォールは、次の 2 つの方法のいずれかで、 LACP と LLDP パケットを処理します。

- アクティブ–ファイアウォールは インターフェイスに設定された LACP または LLDP を持っており、 それぞれ、LACP または LLDP プレネゴシエーションにアクティブに参加します。
- パッシブ–LACP または LLDP はインターフェイスに設定されておらず、ファイアウォールはプロトコルに参加しませんが、ファイアウォールのいずれかの側のピアが LACP または LLDP をプレネゴシエートすることをそれぞれ許可します。

以下の表は、Aggregate Ethernet (集約イーサネット - AE)、およびイーサネットインターフェースでサポートされている展開構成を示しています。

インターフェースの展開構成	AEインターフェース	イーサネットインターフェイス
レイヤー2 における LACP	Active	非サポート
レイヤー3 における LACP	Active	非サポート
バーチャルワイヤにおける LACP	非サポート	Passive
レイヤー2 における LLDP	Active	Active
レイヤー3 における LLDP	Active	Active
バーチャルワイヤにおける LLDP	Active	• LLDP が設定されている場合は Active。 • LLDP が未設定の場合は Passive。

プレネゴシエーションは、サブインターフェイスやトンネルインターフェイスでは、サポートされていません。

LACP あるいは LLDP プレ ネゴシエーションを設定する方については、(任意) アクティブ/パッシブ HA 用に LACP および LLDP プレ ネゴシエーションを有効化し、ネットワークが LACP あるいは LLDP を使用する場合にフェイルオーバーを高速化のステップを参照してください。

フローティング IP アドレスと仮想 MAC アドレス

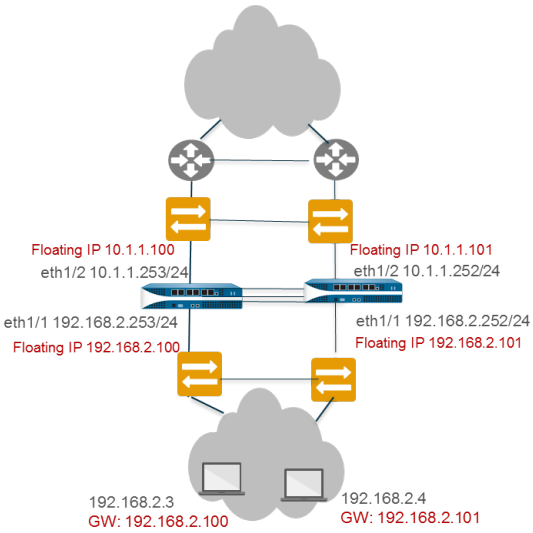
HA アクティブ/アクティブモードのレイヤー 3 展開では、リンクまたはファイアウォールに障害が発生した場合、1 つの HA ファイアウォールから別の HA ファイアウォールに移動するフローティング IP アドレスを割り当てることができます。フローティング IP アドレスを所有するファイアウォールのインターフェイスは、仮想 MAC アドレスを持つ ARP リクエストに応答します。

バーチャルルータ冗長プロトコル（VRRP）などの機能が必要な場合、フローティング IP アドレスを推奨します。フローティング IP アドレスは、VPN と送信元 NAT で使用でき、このようなサービスを提供するデバイスで障害が発生した場合に接続を持続させることができます。

下図のように、各 HA ファイアウォールインターフェイスは固有の IP アドレスとフローティング IP アドレスを持っています。インターフェイス IP アドレスはファイアウォールに対してローカルのままですが、フローティング IP アドレスは、ファイアウォールに障害が発生するとファイアウォール間を移動します。フローティング IP アドレスをデフォルトゲートウエイとして使用するようにエンドホストを設定します。これにより 2 つの HA ピアにバランストラフィックをロードできます。ロードバランストラフィックで、外部ロードバランサーを使うこともできます。

リンクまたはファイアウォールに障害が発生したり、パスモニタリングイベントがフェイルオーバーを生じたりした場合は、フローティング IP アドレスと仮想 MAC アドレスは機能ファイアウォールに移動します。（下図では、各ファイアウォールはそれぞれ 2 つのフローティング IP アドレスと仮想 MAC アドレスを持っています。それらは全てファイアウォールに障害が発生すると、移動します。） 機能中のファイアウォールは Gratuitous ARP を送信して、接続されたスイッチの MAC テーブルを更新し、フローティング IP アドレスと MAC アドレスのオーナーシップの変更を通知し、トラフィックを自分自身にリダイレクトします。

ファイアウォールの障害が復旧した後、デフォルトでフローティング IP アドレスと仮想 MAC アドレスは、フローティング IP アドレスが関連づけられているデバイス ID [0 または 1]で、ファイアウォールに戻ります。具体的には、ファイアウォールの障害が復旧すると、オンラインになります。現在アクティブなファイアウォールは、ファイアウォールがオンラインに戻るかどうか決定し、処理しているフローティング IP アドレスがネイティブで自分自身に属するか、他のファイアウォールに属するかをチェックします。フローティング IP アドレスが最初は他のデバイス ID に関連づけられていた場合は、ファイアウォールは自動的にそれを取り戻します。（このデフォルトの挙動の代替は、ユース ケース：アクティブプライマリファイアウォールにバインドされたフローティングIPアドレスをアクティブ/アクティブHAに設定する。



HA ペアの各ファイアウォールは、フローティング IP アドレスまたは ARP ロード共有 IP アドレスを持つインターフェイスごとに仮想 MAC アドレスを生成します。

仮想 MAC アドレス (PA-7000、PA-5200、PA-3200 Series ファイアウォール以外のファイアウォール上) のフォーマットは 00-1B-17-00-xx-yy です。ここで 00-1B-17 はベンダー ID (この場合、Palo Alto Networks の)、00 は固定、下図のように、xx はデバイス ID およびグループ ID、yy はインターフェイス ID です。

7	6	543210	76543210
Device-ID	0	Group-ID	Interface-ID

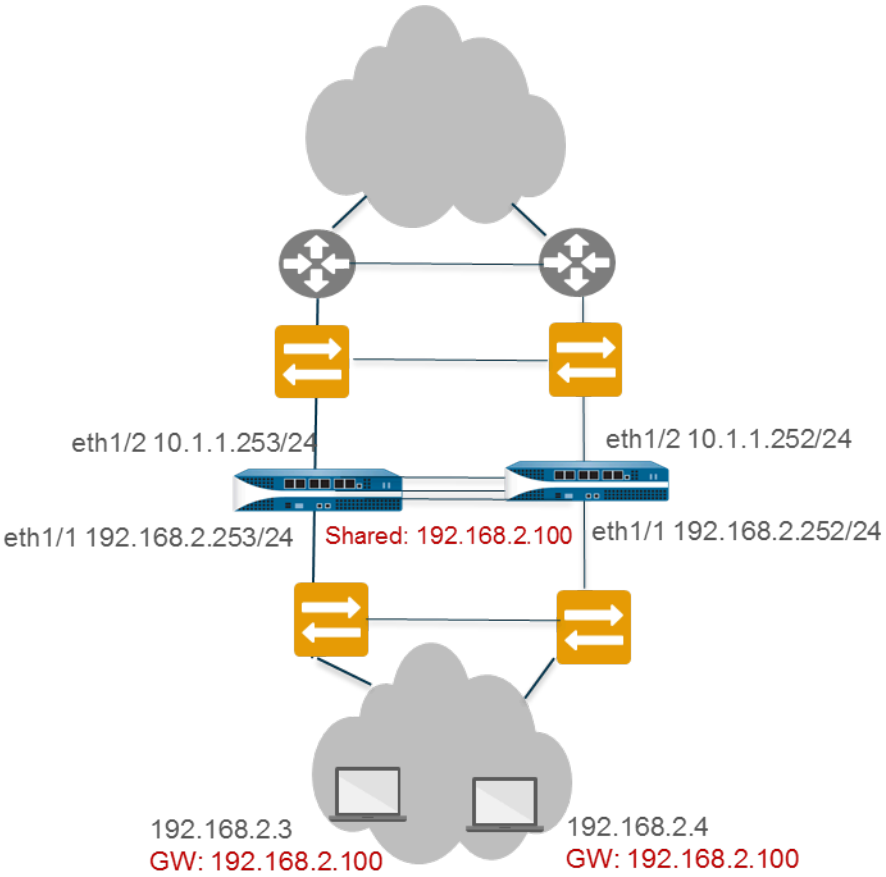
PA-7000、PA-5200、PA-3200 Series ファイアウォールの仮想 MAC アドレスのフォーマットは B4-0C-25-xx-xx-xx です。ここで B4-0C-25 はベンダー ID (この場合、Palo Alto Networks の)、次の 24 ビットは以下のようにデバイス ID、グループ ID、およびインターフェイス ID です。

765	4	321076	5432	1076543210
111	Device-ID	Group-ID	0000	Interface-ID

新しいアクティブファイアウォールが引き継ぐと、接続されたインターフェイスそれぞれの ARP を送信し、接続されたレイヤー 2 スイッチに仮想 MAC アドレスの新しい位置を通知します。フローティング IP アドレスの設定方法については、ユース ケース：フローティングIPアドレスをアクティブ/アクティブHAに設定する。

ARP ロード共有

レイヤー 3 展開とアクティブ/アクティブ HA 設定では、ARP ロード共有によってファイアウォールは IP アドレスを共有し、ゲートウェイサービスを提供できるようになります。ファイアウォールとエンドホストとの間にレイヤー 3 デバイスが存在しない時だけ ARP ロード共有を使います。つまりエンドホストがファイアウォールをデフォルトゲートウエイとして使うことになります。

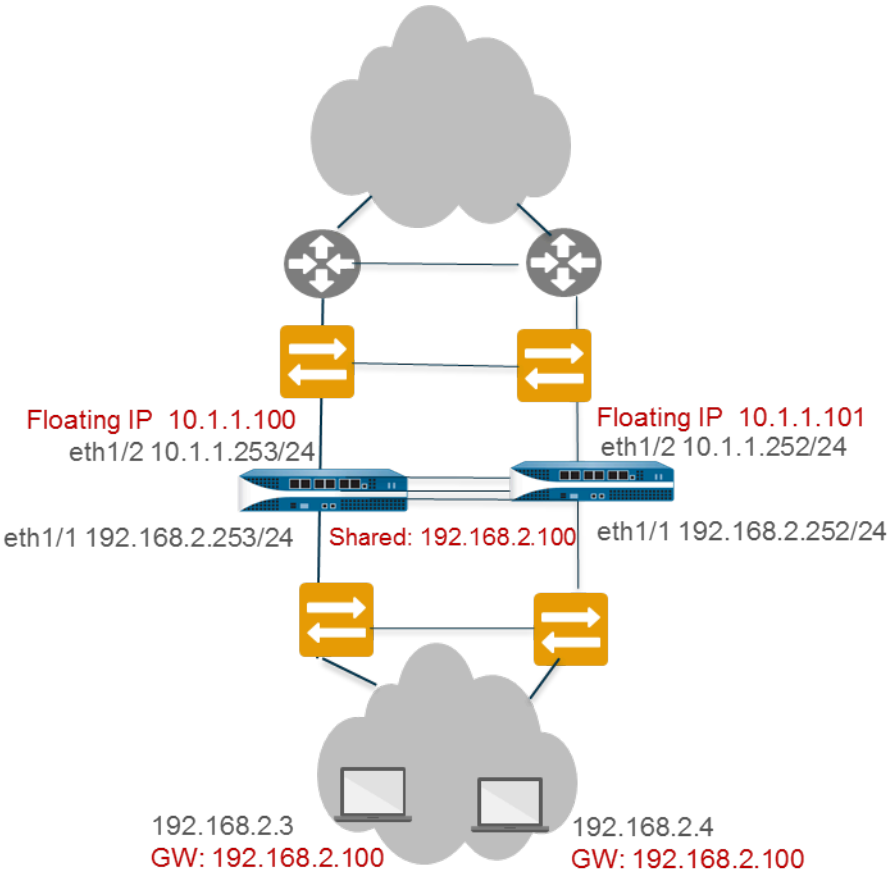


この例では、すべてのホストが 1 つのゲートウェイ IP アドレスで構成されています。ファイアウォールの 1 つがゲートウェイ IP アドレスの ARP 要求に仮想 MAC アドレスで応答します。各ファイアウォールは、共有 IP アドレスに生成された固有の仮想 MAC アドレスを持っています。ARP 要求に応答するファイアウォールを制御するロード共有アルゴリズムは設定を変更でき、ARP 要求の送信元 IP アドレスのハッシュまたはモジュロを計算することによって決定されます。

エンドホストがゲートウェイからARP応答を受信すると、MACアドレスをキャッシュし、ホストからの全てのトラフィックが、ARP キャッシュのライフタイムの間は、仮想 MAC アドレスで応答したファイアウォールを経由してルーティングされます。ARP キャッシュのライフタイムはエンドホストオペレーティングシステムに依存します。

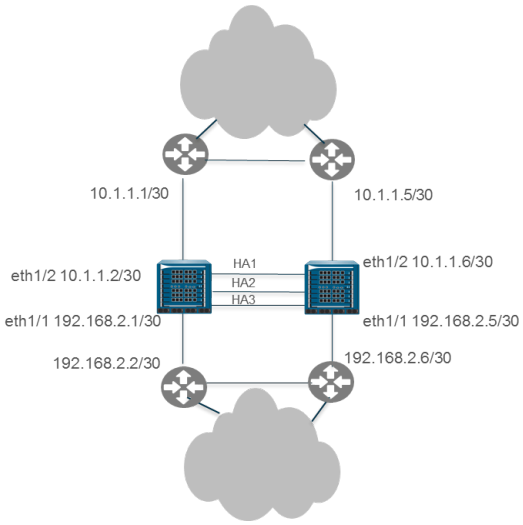
リンクまたはファイアウォールに障害が発生した場合は、フローティング IP アドレスと仮想 MAC アドレスは機能ファイアウォールに移動します。機能ファイアウォールは、gratuitousARP を送信して、接続されたスイッチの MAC テーブルを更新し、トラフィックを障害が発生したファイアウォールから自分自身にリダイレクトします。「ユース ケース：ARP ロード共有をアクティブ/アクティブ HA に設定します。

HA ファイアウォールの WAN 側のインターフェイスにフローティング IP アドレスを設定し、HA ファイアウォールの LAN 側のインターフェイスに ARP ロード共有のための共有 IP アドレスを設定できます。例えば、下図はアップストリーム WAN エッジルーターのフローティング IP アドレスと LAN セグメント上のホストの ARP ロード共有アドレスを示しています。



ルート ベース冗長性

レイヤー 3 インターフェイス展開とアクティブ/アクティブ HA 設定では、ファイアウォールはスイッチでなくルーターに接続されています。ファイアウォールはダイナミックルーティングプロトコルを使用して、最善のパス（非対称ルート）を決定し、HA ペアの間でロード共有します。その場合、フローティング IP アドレスは不要です。リンク、監視パス、またはファイアウォールに障害が発生したり、双方向送信検出 （BFD）がリンク障害を検出した場合、ルーティングプロトコル （RIP、 OSPF、または BGP）はトラフィックの機能ファイアウォールへのリルーティングを処理します。各ファイアウォールは固有の IP アドレスを設定します。IPアドレスは、設定されたファイアウォールに対してローカルのままで、ファイアウォールに障害が発生した場合、デバイス間を移動しません。ユース ケース：ルートベース冗長性をアクティブ/アクティブHAに設定する。



HA タイマー

高可用性（HA）タイマーは、ファイアウォール障害の検出を容易にし、フェイルオーバーをトリガーします。HAペアのタイマーの設定時に煩雑さを軽減するため、以下3種類のプロファイルから選択できます。**Recommended** [推奨]、**Aggressive** [アグレッシブ] および **Advanced** [高度]これらのプロファイルでは、特定のファイアウォール プラットフォームに最適な HA タイマー値が自動入力され、HA の導入速度を高めることができます。

通常のフェイルオーバー タイマー設定には **Recommended**（推奨）プロファイルを使用し、高速なフェイルオーバー タイマー設定には **Aggressive**（アグレッシブ）プロファイルを使用します。**Advanced**（詳細）プロファイルでは、ネットワーク要件に合わせてタイマー値をカスタマイズできます。

以下の表に、プロファイルに含まれる各タイマーと、異なるハードウェア モデルでの現在の事前設定値（Recommended (推奨)/Aggressive (アグレッシブ)）を示します。これらの値は、現時点でのものであり、以降のリリースでは変わる可能性があります。

HA クラスターのメンバーに影響を与えるタイマーについては、HA クラスタリングの設定で説明します。

タイマー	説明	PA-7000シリーズ PA-5200シリーズ PA-3200シリーズ	PA-800シリーズ PA-220 VM-Series	Panoramaバーチャル アプライアンス Panorama M-Series
モニター障害時ホールド アップ タイム (ミリ秒)	パス モニター障害またはリンク モニター障害の発生後、ファイアウォールがアクティブのままでいる時間。	0/0	0/0	0/0

タイマー	説明	PA-7000シリーズ PA-5200シリーズ PA-3200シリーズ	PA-800シリーズ PA-220 VM-Series	Panoramaバーチャル アプライアンス Panorama M-Series
	隣接するデバイスが偶発的にフラッピングすることによる HA のフェールオーバーを回避するためには、この設定をお勧めします。			
Preemption Hold Time (min)（プリエンプション ホールド タイム（分））	パッシブまたはアクティブ-セカンダリ ファイアウォールが、アクティブまたはアクティブ-プライマリ ファイアウォールとして引き継ぐまでに待機する時間。	1/1	1/1	1/1
ハートビート間隔 (ミリ秒)	HA ピアが ICMP（ping）形式のハートビート メッセージを交換する頻度。	1000/1000	2000/1000	2000/1000
プロモーション ホールド タイム (ミリ秒)	パッシブ ファイアウォール（アクティブ/パッシブ モードの場合）またはアクティブ-セカンダリ ファイアウォール（アクティブ/アクティブ モードの場合）が、HA ピアとの通信が失われた後でアクティブまたはアクティブ-プライマリ ファイアウォールとして引き継ぐまでに待機する時間。このホールド タイムは、ピアの障害宣言が行われた後に開始されます。	2000/500	2000/500	2000/500

タイマー	説明	PA-7000シリーズ PA-5200シリーズ PA-3200シリーズ	PA-800シリーズ PA-220 VM-Series	Panoramaバーチャル アプライアンス Panorama M-Series
追加のマスター ホールド アップ タイム (ミリ秒)	Monitor Fail Hold Up Time （モニター障害時ホールド アップ タイム、ミリ秒単位）と同じイベントに適用される時間間隔（範囲は 0 ～ 60000、デフォルトは 500）。追加の時間間隔は、アクティブ/パッシブ モードのアクティブ ファイアウォールおよびアクティブ/アクティブ モードのアクティブ-プライマリ ファイアウォールにのみ適用されます。両方のファイアウォールで同じリンク/パス モニターの障害が同時に発生した場合にフェイルオーバーを回避するためには、このタイマーをお勧めします。	500/500	500/500	7000/5000
Hello Interval (ms)（Hello 間隔（ミリ秒）	もう一方のファイアウォールの HA 機能が動作していることを確認するための Hello パケットの送信間隔（ミリ秒単位、範囲は8,000～60,000。デフォルトは8,000）。	8000/8000	8000/8000	8000/8000
Flap Max	フラップは、以下のいずれかが発生したときにカウントされます。	3/3	3/3	該当なし

タイマー	説明	PA-7000シリーズ PA-5200シリーズ PA-3200シリーズ	PA-800シリーズ PA-220 VM-Series	Panoramaバーチャル アプライアンス Panorama M-Series
	• プリエンプション対応のファイアウォールは、アクティブになってから 20 分以内にアクティブ状態を終了します。 • リンクまたはパスは、機能した後、10 分間起動に失敗します。 プリエンプションに失敗した場合、または機能しないループの場合、この値は、ファイアウォールがサスペンドされる前に許容されるフラップの最大数を示します（範囲 0 ～ 16、デフォルトは 3）。			

セッション オーナー

HA アクティブ/アクティブ設定では、両方のファイアウォールは同時にアクティブになりますが、これはパケットがそれらの間に配布されることを意味しています。こうした配布では、ファイアウォールは、セッションオーナーシップとセッションセットアップという 2 つの機能を充足しなければなりません。通常は、ペアの各ファイアウォールはこれらの機能のうち1つを実行し、それによって非対称ルーティング環境で発生しうる競合状態を回避します。

セッションのセッションオーナーを、エンドホストからの新しいセッションの最初のパケットを受信するファイアウォールにするか、アクティブプライマリ状態のファイアウォールにするか設定します。プライマリーデバイスが設定されているが、最初のパケットを受信するファイアウォールがアクティブプライマリ状態でない場合、ファイアウォールは HA3 リンクを経由してそのパケットをピアファイアウォール（セッションオーナー）に転送します。

セッションオーナーは、このセッションでの全てのレイヤー 7 処理 （App-ID、Content-ID、および脅威スキャン） を担当します。このセッションオーナーは、セッションのすべてのトラフィック ログの生成も行います。

セッションオーナーに障害が発生した場合、ピアファイアウォールがセッションオーナーになります。既存のセッションが機能ファイアウォールにフェイルオーバーし、このようなセッションでは、レイヤー 7 処理は利用できなくなります。ファイアウォールの障害が回復すると、デフォルトで、障害発生前に所有していた全てのセッションは最初のファイアウォールに戻ります。レイヤー 7 処理は再開しません。

セッションオーナーシップをプライマリデバイスに設定すると、セッションセットアップもデフォルトでプライマリデバイスに設定されます。

*Palo Alto Networks*は、各使用例に特段の規定がない場合は、セッションオーナーを最初のパケットに、セッションセットアップを*IP*モジュロに設定することを推奨します。セッションオーナーをファーストパケットに設定すると、*HA3* リンク上のトラフィックが減少し、データプレーンの負荷をピア間で分散することができます。

セッションオーナーとセッションセットアップをプライマリデバイスに設定すると、アクティブプライマリファイアウォールは全てのトラフィック処理を実行します。以下の理由のいずれかでこれを設定することもできます。

- パケット処理がファイアウォールに分割されないように、ログと *pcaps* をトラブルシューティングまたはキャプチャーしている。
- アクティブ/アクティブ *HA* ペアを強制的にアクティブ/パッシブ*HA*ペアのように機能させたい。「ユース ケース：アクティブプライマリファイアウォールにバインドされたフローティングIPアドレスをアクティブ/アクティブHAに設定するを参照してください。

セッション セットアップ

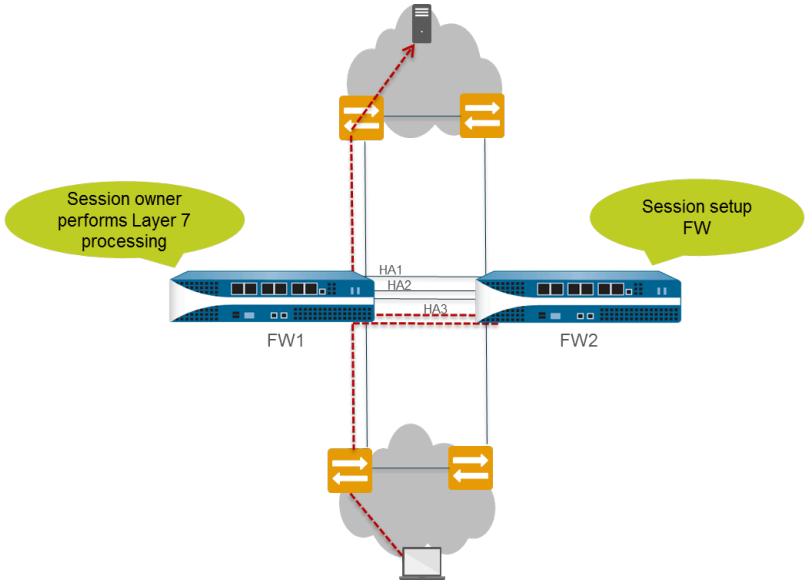
セッション セットアップ デバイスは、新しいセッションのセットアップに必要なレイヤー 2 からレイヤー 4 の処理を実行します。セッションセットアップファイアウォールもセッションオーナーの NAT プールを使って NAT を実行します。以下のセッションセットアップロード共有オプションのいずれかを選択して、アクティブ/アクティブ設定でセッションセットアップファイアウォールを決定します。

セッションセットアップオプション	説明
IP モジュロ	送信元IPアドレスのパリティに基づいて、セッションセットアップロードを分散させます。これはセッションセットアップを共有するための決定論的な方法です。
IP ハッシュ	ファイアウォールは、送信元と宛先のIPアドレスのハッシュを使って、セッションセットアップの責任を分散します。

セッションセットアップオプション	説明
プライマリ デバイス	アクティブプライマリファイアウォールは常にセッションをセットアップします。1個のファイアウォールのみが全てのセッションセットアップ責任を実行します。
最初のパケット	セッションの最初のパケットを受信したファイアウォールがセッションセットアップを実行します。

- セッションオーナーのロードとセッションセットアップ責任を共有したい場合は、セッションオーナーを最初のパケットに、セッションセットアップを *IP* モジュロにそれぞれ設定します。これらは推奨設定です。
- ログや *pcaps* をトラブルシューティングまたはキャプチャーしたい場合、あるいはアクティブ/アクティブ*HA*ペアをアクティブ/パッシブ *HA* ペアのように機能させたい場合は、セッションオーナーとセッションセットアップの両方をプライマリデバイスに設定し、アクティブプライマリデバイスが全てのトラフィック処理を行うようにします。ユース ケース：アクティブプライマリファイアウォールにバインドされたフローティングIPアドレスをアクティブ/アクティブHAに設定する。

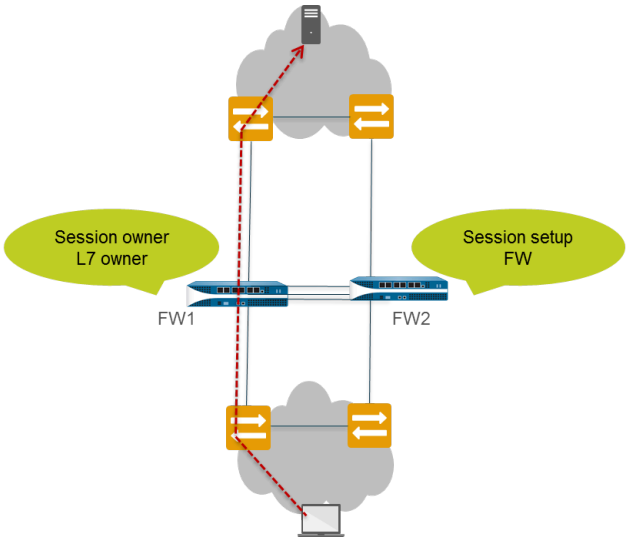
ファイアウォールは HA 3リンクを使って、必要に応じてセッションセットアップのためにパケットをピアに送信します。下図とテキストは、新しいセッションのためにファイアウォールFW1が受信するパケットのパスを説明しています。赤い点線は、パケットを FW2 に転送する FW1 と HA3 リンクを経由してパケットを FW1 に戻す FW2 を示しています。



1. エンドホストはパケットを FW1 に送信します。

- FW1 はパケットのコンテンツを検証して、既存のセッションに一致させます。一致するセッションがない場合、 FW1 は最初のパケットを受信したと見なし、セッションオーナーになります（**Session Owner Selection**[セッションオーナーの選択]が **First Packet**[最初のパケット]に設定されていると仮定する）。
- FW1 は校正済みセッションセットアップロード共有オプションを使用して、セッションセットアップファイアウォールを識別します。この例では、FW2 が設定され、セッションセットアップを実行しています。
- FW1 は HA3 リンク を使用して最初のパケットを FW2 に送信します。
- FW2 はセッションをセットアップし、そのパケットを FW1 に戻し、存在するのであればレイヤー 7 が処理します。
- 次に FW1 はパケットを出口インターフェイスから宛先に転送します。

下図とテキストは、既存セッションに一致するパケットのパスを説明しています。



- エンドホストはパケットを FW1 に送信します。
- FW1 はパケットのコンテンツを検証して、既存のセッションに一致させます。セッションが既存のセッションに一致するのであれば、FW1 はパケットを処理し、出口インターフェイスから宛先に送信します。

NAT in Active/Active HA Mode[アクティブ/アクティブHAモードのNAT]

アクティブ/アクティブHA設定において：

- それぞれのダイナミック IP （DIP） NAT ルール、ダイナミック IP、ポート （DIPP） NAT ルールをデバイス ID 0 または デバイス ID 1にバインドする必要があります。
- それぞれのスタティック NAT ルールを、デバイス ID 0、デバイス ID 1、both [両方]デバイス Id、またはアクティブな primary [プライマリ]ファイアウォールにバインドする必要があります。

従って、いずれかのファイアウォールが新しいセッションを生成する場合、バインドしたデバイス ID **0** またはデバイス ID **1** が、ファイアウォールと一致する NAT ルールを決定します。ルールの照合が行われるためには、デバイスバインドにセッションオーナーファイアウォールが含まれている必要があります。

セッションセットアップファイアウォールは NAT ポリシー照合を実行しますが、NAT ルールはセッションオーナーに基づいて評価されます。つまり、セッションは、セッション オーナーのファイアウォールに結合された NAT ルールに基づいて変換されることになります。NAT ポリシー照合を実行しつつ、ファイアウォールはセッション オーナーに関連付けられていないすべての NAT ルールを飛ばして進みます。

デバイス ID 1 のファイアウォールがセッションオーナーであり、セッションを作成するファイアウォールになる場合を例にとってみましょう。デバイスID 1 を持つファイアウォールが、セッションとNATルールを照合する際に、デバイス ID 0 にバインドされたすべてのルールを飛ばして照合を行います。NAT ルールのセッションオーナーとデバイス ID が一致するときだけ、ファイアウォールは NAT 変換を実行します。

通常は、ピアファイアウォールが異なる IP アドレスを使用して変換する場合に、デバイス固有の NAT ルールを生成します。

片方のピアに障害が発生した場合は、NAT 変換を含め、アクティブなファイアウォールが、障害が発生したファイアウォールのセッション同期用トラフィックの処理を続けます。送信元 NAT 設定では、1 つのファイアウォールに障害が発生した場合、

- NAT ルールの変換済み IP アドレスとして使用されるフローティング IP アドレスは生き残ったファイアウォールに移動します。従って、フェイルオーバーした既存のセッションは依然としてこの IP アドレスを使用します。
- 新しいセッションは全て、生き残ったファイアウォールが通常所有するデバイス固有の NAT ルールを使用します。つまり、生き残ったファイアウォールは、デバイス ID に一致する NAT ルールのみを使って新しいセッションを変換し、障害が発生したデバイス ID にバインドした NAT ルールはすべて無視します。

NATを伴うアクティブ/アクティブHAの例は以下のとおりです。

- ユース ケース：フローティングIPアドレスを使って送信元DIPP NATをアクティブ/アクティブHAに設定する
- ユース ケース：個別送信元NAT IPアドレスプールをアクティブ/アクティブHAファイアウォールに設定する
- ユース ケース：ARPロード共有を宛先NATでアクティブ/アクティブHAに設定する
- ユース ケース：ARPロード共有をレイヤー3の宛先NATでアクティブ/アクティブHAに設定する

ECMP in Active/Active HA Mode[アクティブ/アクティブHAモードのECMP]

アクティブ/アクティブHAピアに障害が発生した場合、そのセッションは新しいアクティブプライマリファイアウォールに移動し、そのアクティブプライマリファイアウォールは障害が発生したファイアウォールが使っていたのと同じ出力インターフェイスの使用を試行します。ECMP パスでそのようなインターフェイスが検出されると、同じ出力インターフェイスとパスを使用して

セッションが転送されます。同じインターフェイスを使用することが望ましいため、この動作は使用している ECMP アルゴリズムに関係なく実行されます。

どの ECMP パスも元の出力インターフェイスに一致しない場合のみ、アクティブ-プライマリファイアウォールは新しい ECMP パスを選択します。

アクティブ/アクティブピアで同じインターフェイスを設定していなければ、フェイルオーバーが発生すると、アクティブ-プライマリファイアウォールは FIB テーブルから次に最適なパスを選択します。その結果、既存のセッションは ECMP アルゴリズムに基づいて分散されない可能性があります。

アクティブ/パッシブ HA のセットアップ

アクティブ/パッシブ HA の前提条件

Palo Alto Networks ファイアウォールで高可用性をセットアップするには、以下の前提条件を満たすファイアウォールのペアが必要です。

- 同じモデル – ハードウェアまたは仮想マシンのモデルが、ペアの両方のファイアウォールで同じでなければなりません。
- 同じバージョンの **PAN OS** – 両方のファイアウォールで同じバージョンの PAN OS を実行していて、両方のアプリケーション、URL、および脅威データベースで最新の状態が保たれている必要があります。
- 同一のマルチ仮想システム機能－両方のファイアウォールは**Multi Virtual System Capability**[マルチ仮想システム機能]を有効または無効化する必要があります。有効化すると、各ファイアウォールには独自のマルチ仮想システムライセンスが必要になります。
- 同タイプのインターフェイス – 専用の HA リンク、またはインターフェイス タイプを HA に設定した管理ポートとインバンド ポートの組み合わせです。
  - HA ピア間の HA1 （コントロール）接続の IP アドレスを決定します。ピアが直結されている場合、または同じスイッチに接続されている場合は、両方の HA1 IP アドレスが同じサブネット上になければなりません。

    専用の HA ポートを持たないファイアウォールでは、管理ポートをコントロール接続に使用できます。管理ポートを使用すると、両方のファイアウォールの管理プレーン間の通信を直接接続できます。ただし、管理ポートはピア間で直結できないため、ネットワーク上にこれら 2 つのインターフェイスを接続するルートがあることを確認してください。
  - レイヤー 3 を HA （データ）接続の転送方法として使用する場合、HA2 リンクの IP アドレスを決定する必要があります。経路指定されたネットワークを介して HA2 接続の通信を行う必要がある場合は、レイヤー 3 のみを使用します。HA2 リンクの IP サブネットは、HA1 リンクのサブネットまたはファイアウォール上のデータ ポートに割り当てられたその他のサブネットと重複してはなりません。
- 同一ライセンス – ライセンスは各ファイアウォールに固有のため、ほかのファイアウォールと共有することはできません。そのため、両方のファイアウォールで同一のライセンスを取得する必要があります。両方のファイアウォールに同一のライセンスがない場合は、設定情

報を同期することや、等価性を管理してシームレスにフェイルオーバーすることができません。

最善の方法として、既存のファイアウォールがあり、*HA* 用に新しいファイアウォールを追加する場合、その新しいファイアウォールに既存の設定が存在する場合は、新しいファイアウォールでファイアウォールの工場出荷時設定へのリセットを実行することをお勧めします。これにより、新しいファイアウォールをクリーンな設定にすることができます。*HA* を設定したら、プライマリ ファイアウォールの設定を、新しく導入したクリーンな設定のファイアウォールに同期します。

アクティブ/パッシブ HA の設定ガイドライン

HA でアクティブ（PeerA）とパッシブ（PeerB）のペアをセットアップするには、いくつかのオプションは両方のファイアウォールで同一の設定にし、それ以外のオプションは各ファイアウォールで個別に（一致しないように）設定する必要があります。これらの HA 設定は、ファイアウォール間で同期されません。同期されるものと同期されないものの詳細については、リファレンス：HA 同期 を参照してください。

以下のチェックリストに、両方のファイアウォールで同一にする必要のある設定の詳細を示します。

- 両方のファイアウォールで HA を有効にする必要があります。
- 両方のファイアウォールで同じグループ ID の値を設定する必要があります。ファイアウォールは、設定したすべてのインターフェイスに対する仮想 MAC アドレスの作成にグループ ID の値を使用します。フローティング IP アドレスおよび仮想 MAC アドレスのところで、仮想 MAC アドレスの情報を確認します。新しいアクティブ ファイアウォールがタスクを引き継ぐと、接続された各インターフェイスから Gratuitous ARP メッセージを送信し、接続されたレイヤー 2 スイッチに仮想 MAC アドレスの新しい場所が通知されます。
- HA リンクとしてインバンド ポートを使用している場合、HA1 および HA2 リンク用のインターフェイスをタイプ HA に設定する必要があります。
- 両方のファイアウォールで HA モードを Active Passive (アクティブ パッシブ) に設定します。
- 必要に応じて両方のファイアウォールでプリエンプションを有効にします。ただし、デバイス優先順位は異なる値にする必要があります。
- 必要に応じて、HA1 リンク（HA ピア間の通信用）の暗号化を両方のファイアウォールで設定します。

- 使用中の HA1 と HA1 のバックアップ ポートの組み合わせに応じて、以下の推奨事項に基づき、ハートビート バックアップを有効にするかどうかを判断してください。

  管理インタフェースが*DHCP* アドレシング （***IP Type(IP***タイプ***)***が***DHCP Client(DHCP***クライアント***)***にセット） に設定されている場合、*HA* 機能 （*HA1* と *HA1* バックアップ） は管理インターフェースではサポートされません。*AWS* と *Azure* の場合は例外で、管理インターフェースは *DHCP* クライアントとして設定され、*HA1* および *HA1* バックアップリンクをサポートします。

  - HA1：専用の HA1 ポート

    HA1 バックアップ:専用の HA1 ポート

    推奨:ハートビート バックアップの有効化
  - HA1：専用の HA1 ポート

    HA1 バックアップ:インバンド ポート

    推奨:ハートビート バックアップの有効化
  - HA1：専用の HA1 ポート

    HA1 バックアップ:管理ポート(MGTポート)

    推奨:ハートビート バックアップを有効にしない
  - HA1：インバンド ポート

    HA1 バックアップ:インバンド ポート

    推奨:ハートビート バックアップの有効化
  - HA1：管理ポート(MGTポート)

    HA1 バックアップ:インバンド ポート

    推奨:ハートビート バックアップを有効にしない

以下の表に、各ファイアウォールで個別に設定する必要のある HA 設定を示します。ピア間で自動的に同期されないその他の構成設定の詳細については、リファレンス：HA 同期を参照してください。

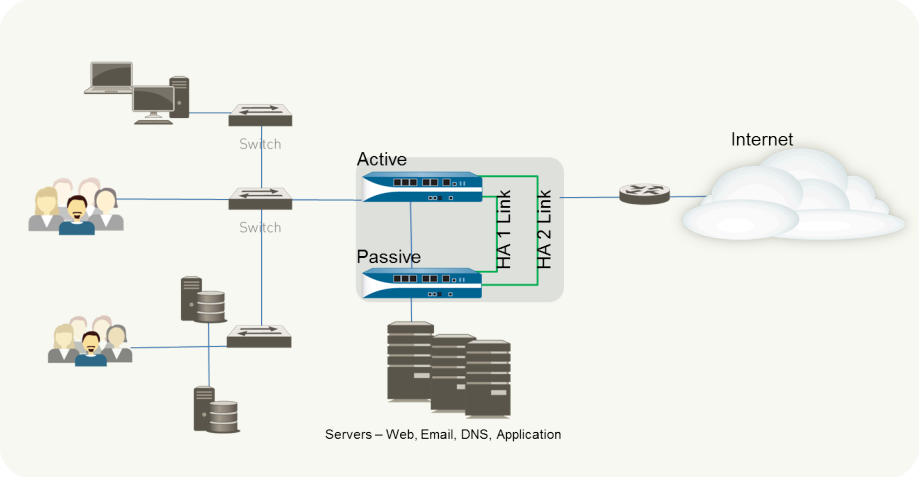
個別の設定	PeerA	PeerB
コントロール リンク	このファイアウォール（PeerA）に設定される HA1 リンクの IP アドレス。	このファイアウォール（PeerB）に設定される HA1 リンクの IP アドレス。
	専用の HA ポートを持たないファイアウォールでは、コントロール リンクに管理ポートの IP アドレスを使用します。	
データ リンク	デフォルトでは、HA2 リンクでレイヤー 2 の Ethernet が使用されます。	デフォルトでは、HA2 リンクでレイヤー 2 の Ethernet が使用されます。

個別の設定	PeerA	PeerB
データ リンク情報は、HA を有効にしてファイアウォール間のコントロール リンクを確立した後に、ファイアウォール間で同期されます。	レイヤー 3 接続を使用する場合は、このファイアウォール（PeerA）のデータ リンクの IP アドレスを設定します。	レイヤー 3 接続を使用する場合は、このファイアウォール（PeerB）のデータ リンクの IP アドレスを設定します。
デバイス優先順位（必須、プリエンプションが有効な場合）	アクティブにするファイアウォールの数値を、ピアよりも小さくする必要があります。そのため、PeerA をアクティブ ファイアウォールとして機能させる場合、デフォルト値の 100 をそのままにしておき、PeerB の値をこれよりも大きくします。 ファイアウォールが同じデバイス優先順位を持つ場合は、それらはタイブレーカーとしてHA1のMACアドレスを使用します。	PeerB がパッシブの場合、デバイス優先順位の値を PeerA よりも大きく設定します。たとえば、優先順位の値を 110 に設定します。
リンク モニタリング – このファイアウォールの主要トラフィックを処理する 1 つ以上の物理インターフェイスをモニターし、失敗条件を定義します。	モニターするファイアウォール上の物理インターフェイスを選択し、フェイルオーバーを引き起こす失敗条件（Any （いずれか）または all （すべて））を定義します。	このファイアウォール上でモニターする同様の物理インターフェイス群を選択し、フェイルオーバーを引き起こす失敗条件（all （すべて）または Any （いずれか））を定義します。
パス モニタリング – ファイアウォールで ICMP ping を使用して応答状態を確認できる、1 つ以上の宛先 IP アドレスをモニターします。	失敗条件（all （すべて）または Any （いずれか））、Ping 間隔、および Ping 数を定義します。相互接続されたネットワーク デバイスの可用性をモニターする場合は、特にこれらの定義が役に立ちます。たとえば、サーバーに接続されたルーターの可用性、サーバー自体への接続状態、またはトラフィック フロー中に存在するその他いくつかの主要デバイスへの接続状態をモニターする場合などです。	PeerB でも、モニターしてフェイルオーバーのトリガー条件を判断できる同様のデバイス群または宛先 IP アドレス群を選択します。失敗条件（all （すべて）または Any （いずれか））、Ping 間隔、および Ping 数を定義します。

個別の設定	PeerA	PeerB
	モニタリング中のノード/デバイスが応答していない可能性がある場合、特に負荷を受けている場合は、パス モニタリングの障害の原因となり、フェイルオーバーが引き起こされるため、このような状態がないかどうかを確認します。	

アクティブ/パッシブ HA を設定する

以下の手順は、下のトポロジの例に示すようなアクティブ/パッシブ導入で、ファイアウォールのペアを設定する方法を示したものです。



アクティブ/パッシブ HA ペアを設定するには、まずは 1 つ目のファイアウォールで、次の作業を完了させ、次に 2 番目のファイアウォールに対して各作業を繰り返します。

STEP 1 | HA ポートを接続して、ファイアウォール間の物理的な接続をセットアップします。

- 専用の HA ポートを持つファイアウォールの場合は、Ethernet ケーブルを使用して、ピアの専用の HA1 ポートと HA2 ポートを接続します。ピア同士を直結する場合は、クロスオーバー ケーブルを使用します。
- 専用の HA ポートを持たないファイアウォールの場合は、HA2 リンク用とバックアップ HA1 リンク用の 2 つのデータ インターフェイスを選択します。次に、Ethernet ケーブルを使用して、両ファイアウォール間でこれらのインバンド HA インターフェイスを接続します。

HA1 リンク用の管理ポートを使用して、ネットワーク全体を通じて管理ポート同士を接続できることを確認します。

STEP 2 | ping を管理ポートで有効にします。

ping を有効にすることで、管理ポートをハートビート バックアップの情報交換に使用できます。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択し、Management Interface Settings (管理インターフェイス設定) を編集します。
2. インターフェイスで許可されるサービスとして **[Ping]** を選択します。

STEP 3 | ファイアウォールに専用の HA ポートがない場合は、データ ポートを HA ポートとして機能するように設定します。

専用の HA ポートを持つファイアウォールの場合は、次の手順に進みます。

1. **Network (ネットワーク)** > **Zones (ゾーン)** の順に選択します。
2. 使用するポート上でリンクがアップになっていることを確認します。
3. インターフェイスを選択して、**Interface Type** （インターフェイス タイプ）を **HA** に設定します。
4. 必要に応じて、**Link Speed** （リンク速度）および **Link Duplex** （リンク デュプレックス）を設定します。

STEP 4 | HA モードとグループ ID を設定します。

1. **Device**（デバイス） > **High Availability**（高可用性） > **General**（全般）を選択し、Setup（セットアップ）セクションを編集します。
2. **Group ID** [グループ ID]を設定し、必要に応じてペアの **Description** [内容]を入力します。グループ ID は、ネットワーク上の各 HA ペアを一意に識別します。HA ペアが複数あり、同じブロードキャスト ドメインを共有している場合は、ペアごとに一意のグループ ID を設定する必要があります。
3. モードを **[アクティブ パッシブ]** に設定します。

STEP 5 | コントロール リンクの接続をセットアップします。

ここに示す例は、インターフェイス タイプを HA に設定したインバンド ポートです。

管理ポートをコントロール リンクとして使用するファイアウォールの場合、IP アドレス情報が自動的に入力されます。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General** （全般） の順に選択し、Control Link (HA1) (コントロール リンク (HA1)) セクションを編集します。
2. HA1 リンクとして使用するために配線した **Port (ポート)** を選択します。
3. **IPv4/IPv6 Address**（**IPv4/IPv6** アドレス） と **Netmask**（ネットマスク） を設定します。

   HA1 インターフェイスが個別のサブネットにある場合は、**Gateway**（ゲートウェイ）の IP アドレスを入力します。ファイアウォール同士を直結しているまたは同一の VLAN 上にある場合は、ゲートウェイのアドレスを追加しないでください。

STEP 6 | （任意）コントロール リンク接続の暗号化を有効にします。

この設定は一般に、2 つのファイアウォールが直接接続されていない場合、すなわちポートがスイッチまたはルーターに接続されている場合に、リンクを保護するために使用します。

1. 一方のファイアウォールから HA キーをエクスポートして、ピア ファイアウォールにインポートします。
   1. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書）
   2. **Export HA key**（**HA** 鍵のエクスポート）を選択します。ピアがアクセスできるネットワーク上の場所に、HA キーを Save （保存）します。
   3. ピア ファイアウォールで、**Device (**デバイス**)** > **Certificate Management (**証明書管理**)** > **Certificates (**証明書**)** の順に選択し、**Import HA key (HA** キーのインポート**)** を選択してキーを保存した場所を検索し、そのキーをピアにインポートします。
   4. 2 つ目のファイアウォールでこの作業を繰り返し、両方のデバイスの HA キーを交換します。
2. **Device (**デバイス**)** > **High Availability (**高可用性**)** > **General** （全般） の順に選択し、Control Link (HA1) (コントロール リンク (HA1)) セクションを編集します。
3. **Encryption Enabled (**暗号化を有効**)**を選択します。

   暗号化を有効にした場合、*HA* ファイアウォール の設定が完了した後、HA1 SSH 鍵の更新およびキーのオプションの設定できます。

STEP 7 | バックアップ コントロール リンクの接続をセットアップします。

1. **Device (**デバイス**)** > **High Availability (**高可用性**)** > **General** （全般） の順に選択し、Control Link (HA1 Backup) (コントロール リンク (HA1 Backup)) セクションを編集します。
2. HA1 バックアップ インターフェイスを選択し、**IPv4/IPv6 Address (IPv4/IPv6** アドレス**)** および **Netmask (**ネットマスク**)** を設定します。

   PA-3200 Series のファイアウォールは *HA1* バックアップ制御リンク用の *IPv6* アドレスをサポートしていないため、*IPv4* アドレスを使用してください。

STEP 8 | ファイアウォール間のデータ リンク接続（HA2）とバックアップ HA2 接続をセットアップします。

1. **Device (**デバイス**)** > **High Availability (**高可用性**)** > **General** （全般） の順に選択し、Data Link (HA2) (データ リンク (HA2)) セクションを編集します。
2. データ リンク接続に使用する **Port**（ポート） を選択します。
3. **Transport (**転送**)**の方法を選択します。デフォルトは **ethernet** で、HA ペアが直結されている場合、またはスイッチ経由で接続されている場合はこの方法が機能します。ネット

ワーク経由でデータ リンク トラフィックをルーティングする必要がある場合は、**IP** または **UDP** を転送方法に指定します。

4. 転送方法に IP または UDP を使用する場合は、**IPv4/IPv6 Address**（**IPv4/IPv6** アドレス）と **Netmask**（ネットマスク） を入力します。
5. **Enable Session Synchronization**（セッション同期を有効にする） が選択されていることを確認します。
6. HA ピア間の HA2 データ リンクのモニタリングを有効にするには、**HA2 Keep-alive**（**HA2** キープアライブ） を選択します。設定されているしきい値（デフォルトは 10000 ミリ秒）に基づいて障害が発生した場合、定義されているアクションが発生します。アクティブ/パッシブ設定の場合、HA2 キープアライブの障害が発生すると、「critical」レベルのシステム ログ メッセージが生成されます。

   HA2 Keep-alive（*HA2* キープアライブ）オプションは、*HA* ペアの両方のファイアウォールにも一方のファイアウォールのみにも設定できます。このオプションが一方のファイアウォールでのみ有効な場合、そのファイアウォールのみからキープアライブ メッセージが送信されます。もう一方のファイアウォールに、障害が発生したかどうかが通知されます。

7. **Data Link (HA2 Backup)** (データ リンク **(HA2** バックアップ**))** セクションを編集してインターフェイスを選択し、**IPv4/IPv6 Address (IPv4/IPv6** アドレス**)** および **Netmask (**ネットマスク**)** を追加します。

STEP 9 | コントロール リンクで専用 HA ポートまたはインバンド ポートを使用している場合は、ハートビート バックアップを有効にします。

管理ポートをコントロール リンクに使用している場合は、ハートビート バックアップを有効にする必要はありません。

1. **Device (**デバイス**)** > **High Availability (**高可用性**)** > **General (**全般**)** にて、Election Settings (選択設定) を編集します。
2. **Heartbeat Backup (**ハートビート バックアップ**)**を選択します。

   ハートビートをファイアウォール間で送信できるようにするには、ピア同士で管理ポートをルーティングできることを確認する必要があります。

   ハートビート バックアップを有効にすると、スプリット ブレインを防ぐこともできます。*HA1* リンクがダウンしてファイアウォールがハートビートを受信しなくなると、スプリット ブレインが発生します。ただし、そのファイアウォールはまだ機能しています。このような状況になると、各ピアは相手がダウンしていると判断して、実行中のサービスを開始しようとするため、スプリット ブレイン状態になります。ハートビート バックアップ リンクが有効にされていると、冗長なハートビートおよび *hello* メッセージが管理ポート経由で送信されるため、スプリット ブレインを防ぐことができます。

STEP 10 | デバイス優先順位を設定してプリエンプションを有効にします。

この設定が必要となるのは、特定のファイアウォールが優先的なアクティブ ファイアウォールに指定されていることを確認する場合のみです。詳細は、「デバイス優先度およびプリエンプション」を参照してください。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Election Settings (選択設定) を編集します。
2. **Device Priority** （デバイス優先順位）に数値を設定します。優先順位を高くするファイアウォールには、数値を小さく設定する必要があります。

   両方のファイアウォールの優先順位の値が同じ場合は、*HA1* コントロールリンクで最も小さい *MAC* アドレスのあるファイアウォールがアクティブ ファイアウォールになります。
3. **Preemptive**（プリエンプティブ）を選択します。

   アクティブ ファイアウォールとパッシブ ファイアウォールの両方でプリエンプティブを有効にする必要があります。

STEP 11 | （任意）HA タイマーを変更します。

デフォルトで、HA タイマー プロファイルは、ほとんどの HA デプロイメントに適した **Recommended (推奨)**プロファイルに設定されています。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Election Settings (選択設定) を編集します。
2. フェイルオーバーを高速でトリガーするには **[アグレッシブ]** プロファイルを選択し、設定でフェイルオーバーのトリガーにカスタム値を定義するには **[詳細]** を選択します。

   プロファイルに含まれる個々のタイマーの事前設定値を表示するには、***Advanced***（詳細）を選択して ***Load Recommended***（推奨をロード）または ***Load Aggressive***（アグレッシブをロード）をクリックします。お使いのハードウェア モデルの事前設定値が画面に表示されます。

STEP 12 | (任意) パッシブ ファイアウォールで設定している場合のみパッシブ ファイアウォールの HA ポートのリンクの状態を変更します。

パッシブ リンクの状態はデフォルトで *[*シャットダウン*]* が選択されています。*HA* を有効にすると、アクティブ ファイアウォールの *HA* ポートのリンク状態が緑に変わり、パッシブ ファイアウォールの *HA* ポートが停止して赤く表示されます。

リンク状態を **Auto** （自動）に設定すると、フェイルオーバーが発生した場合にパッシブ ファイアウォールがタスクを引き継ぐまでの時間を短縮できます。また、リンク状態をモニターすることもできます。

パッシブ ファイアウォールでリンク状態をアップにして、物理インターフェイスの稼働状態および配線状態を保つには、以下の手順を実行します。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Active Passive Settings (アクティブ パッシブ設定) を編集します。
2. **[パッシブ リンク状態]** を **[自動]** に設定します。

   Auto （自動）オプションを設定すると、フェイルオーバーが発生した場合にパッシブ ファイアウォールがタスクを引き継ぐまでの時間を短縮できます。

   インターフェイスの表示は（配線されていて稼働していることを示す）緑になっていますが、フェイルオーバーが引き起こされるまでは、すべてのトラフィックが破棄されます。

   パッシブ リンク状態を変更する場合、ファイアウォールのリンク状態のみに基づいて、隣接するデバイスからパッシブ ファイアウォールにトラフィックが転送されていないことを確認してください。

STEP 13 | HA を有効にします。

1. **Device**（デバイス） > **High Availability**（高可用性） > **General**（全般）を選択し、Setup（セットアップ）セクションを編集します。
2. **Enable HA**（**HA** の有効化）を選択します。
3. **Enable Config Sync** （設定の同期化の有効化）を選択します。この設定により、アクティブ ファイアウォールとパッシブ ファイアウォール間で設定が同期されるようになります。
4. **Peer HA1 IP Address** （ピア HA IP アドレス）に、ピアのコントロール リンクに割り当てられた IP アドレスを入力します。

   専用の HA ポートを持たないファイアウォールで、ピアが HA1 リンクに管理ポートを使用している場合は、ピアの管理ポートの IP アドレスを入力します。
5. **[バックアップ側 ピア HA1 IP アドレス]** を入力します。

STEP 14 | （任意）ネットワークが LACP あるいは LLDP を使用する場合にフェイルオーバーを高速化するために、アクティブ/パッシブ HA 用に LACP および LLDP プレ ネゴシエーションを有効化します。

アクティブモードでプレネゴシエーションを機能させる場合、プロトコルに*HA*プレネゴシエーションを設定する前にLACP と LLDP を有効にします。

1. ステップ 12でリンク状態を **Auto(自動)**に設定していることを確認します。
2. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** を選択します。
3. LACPアクティブプレネゴシエーションの有効化
   1. レイヤー2またはレイヤー3展開で、AEインターフェイスを選択します。
   2. **LACP** タブを選択します。
   3. **Enable in HA Passive State**[HAパッシブステートを有効にする]を選択します。
   4. **OK** をクリックします。

      Same System MAC Address for Active-Passive HA*[アクティブ/パッシブHAで同じシステムMACアドレス]* は選択できません。なぜなら、プレネゴシエーションは、アクティブおよびパッシブファイアウォールで固有のインターフェイス*MAC*テーブルを必要とするからです。
4. LACPパッシブプレネゴシエーションの有効化
   1. 仮想ワイヤ展開でEthernetインターフェイスを選択します。
   2. **Advanced**（詳細）タブを選択します。
   3. **LACP** タブを選択します。
   4. **Enable in HA Passive State**[HAパッシブステートを有効にする]を選択します。
   5. **OK** をクリックします。
5. LLDP アクティブプレネゴシエーションの有効化
   1. Layer 2、Layer 3、Virtual Wire 展開のいずれかで、Ethernetインターフェイスを選択します
   2. **Advanced**（詳細）タブを選択します。
   3. **LLDP** タブを選択します。
   4. **Enable in HA Passive State**[HAパッシブステートを有効にする]を選択します。
   5. **OK** をクリックします。

      仮想ワイヤ展開で *LLDP* パッシブプレネゴシエーションを許可する場合は、ステップ 14.e を実行しますが、*LLDP* 自体は有効にしないでください。

STEP 15 | 設定の変更を保存します。

Commit（コミット）をクリックします。

STEP 16 | 両方のファイアウォールの設定が完了したら、アクティブ/パッシブ HA でファイアウォールがペアになっていることを確認します。

1. 両方のデバイスで **Dashboard** にアクセスして、High Availability （高可用性）ウィジットを表示します。
2. アクティブ ファイアウォールで、**Sync to peer** （ピアと同期）リンクをクリックします。
3. 次のように、ファイアウォールがペアになっていて同期されていることを確認します。
   - パッシブ ファイアウォール: ローカル ファイアウォールの状態が **passive**、Running Config (実行コンフィグ) が **synchronized** と表示されます。
   - アクティブ ファイアウォールローカル ファイアウォールの状態が **active**、Running Config (実行コンフィグ) が **synchronized** と表示されます。

フェイルオーバー条件の定義

リンク・モニターまたはパス・モニターを使用してフェイルオーバー条件を定義し、HA ペアの firewall がフェイルオーバーする原因 (トラフィックを保護するタスクが以前にアクティブだった firewall からその HA ピアに渡されるイベント) を確立するには、以下のタスクを実行します。HA 概要は、フェイルオーバーを発生させる条件を説明しています。

仮想ルーター、VLAN、バーチャル ワイヤーごとに複数の IP パス グループを監視することができます。1つ以上の IP アドレスを使用して各パス グループを有効にし、それぞれに独自のピア障害条件を与えることができます。さらに、「any」または「all」の失敗チェックを使用してアクティブなファイアウォールのステータスを判別することにより、パス グループ レベルとより広範な仮想ルーターまたは VLAN またはバーチャル ワイヤー グループ レベルの両方でこれらの障害条件を設定できます。

PAN-OS 10.0にアップグレードすると、ファイアウォールは現在監視されている宛先 IP アドレスを新しく作成された宛先グループに自動的に転送し、そのグループにデフォルトのパス モニタリング名を付けます。新しい宛先グループは、パス グループ レベルで以前のフェイルオーバー状態を保持します。

VLAN パス監視は PAN-OS 10.0 のアクティブ/アクティブ HA ペアと互換性がないため、PAN-OS 10.2 にアップグレードする前に、アクティブ/アクティブ HA 内のすべての VLAN パス監視構成を削除してください。以前のアクティブ/アクティブ HA 構成を保持すると、オートコミットが失敗します。

パス監視を有効にする前に、仮想ルーター、VLAN、バーチャル ワイヤ、またはこれらの論理ネットワーク コンポーネントの組み合わせを設定する必要があります。仮想ルーターおよびバーチャル ワイヤでのパス監視は、アクティブ/アクティブおよびアクティブ/パッシブ HA 展開の両方と互換性がありますが、VLAN でのパス監視は、アクティブ/パッシブ ペアでのみサポートされます。

また、パス モニタリングを有効にする前に、以下の操作を行う必要があります。

- 仮想ルーター内の宛先 IP グループが到達可能かどうかを確認する。
- (パス モニタリングを有効にする予定の) VLAN に設定済みのインターフェースが含まれていることを確認する。

- 適切な宛先IPアドレスから ping を受信するために使用する送信元 IP アドレスを取得しする。

SNMPv3 を使用して *firewall* を監視している場合は、*SNMPv3* エンジン *ID* が *HA* ペア間で同期されることに注意してください。*SNMP*の設定方法については、 Forward Traps to an SNMP Manager*[SNMP*マネージャーにトラップを転送する*]*を参照してください。エンジン *ID* はファイアウォールのシリアル番号を使用して生成されるため、*VM-Series* ファイアウォールでは、各ファイアウォールに一意のエンジン *ID* を取得するために有効なライセンスを適用する必要があります。

STEP 1 | HA リンク モニタリングを設定するために、ファイアウォールから監視への物理インターフェースのグループを指定します (リンク アップまたはリンク ダウン)。

1. **Device** > **High Availability** > **Link and Path Monitoring**(デバイス) > (高可用性) > (リンクとパス監視) の順に選択します。
2. リンク モニタリング セクションで、**Name (名前)** ごとにリンク グループを **Add (追加)** します。
3. **Enabled**(有効) を選択して、リンク グループを有効にします。
4. リンク グループのインターフェースの **Failure Condition (失敗条件)**を選択します: **Any (指定なし)** (デフォルト) または **All (すべて)**。
5. **Interface (インターフェース)** を **Add (追加)** します。
6. **OK**をクリックします。

STEP 2 | （任意）ファイアウォールで設定した一連のリンク グループの失敗条件を変更します。

デフォルトでは、モニター対象のリンク グループのいずれかに障害が発生すると、ファイアウォールでフェイルオーバーが引き起こされます。

1. **Link Monitoring**（リンク監視） セクションを編集します。
2. **Failure Condition** （失敗条件）を **Any** （指定なし） または **All (すべて)** に設定します。
3. **OK** をクリックします。

STEP 3 | 仮想ワイヤ、VLAN、または仮想ルータ(または Advanced Routing Engine の場合は論理ルータ)の HA パス監視を設定するには、ネットワーク接続を検証するために firewall が ping を実行する宛先 IP アドレスを指定します。

1. Path Monitoring セクションで、**Add Virtual Wire Path**、**Add VLAN Path**、または **Add Virtual Router Path** (または Advanced Routing Engine の場合は **Add Logical Router Path** を選択します。
2. 仮想ワイヤ、VLAN、仮想ルータ パス グループ、または論理ルータ>パス グループに **Name** を入力します。
3. (バーチャル ワイヤ パスまたは VLAN パスのみ)仮想ワイヤまたは VLAN を介して宛先 IP アドレスに ping を実行するために使用する**Source IP (送信元IP)** アドレスを入力します。
4. **Enabled (有効)** を選択して、パス グループを有効にします。
5. このパス グループで障害が発生する**Failure Condition (障害条件)** を選択します。**Any (指定なし)** (デフォルト)は、このパス グループ内の1つ以上の宛先 IP グループが失敗し

たときに失敗を発行し、**All (**すべて**)** は、このパスグループ内のすべての宛先 IP グループが失敗したときに失敗を発行します。

6. **Ping Interval (ping** 間隔**)** をミリ秒単位で入力します。これは、宛先 IP アドレスに送信される ICMP メッセージ間の間隔です (範囲は200～60,000、デフォルトは200)。
7. 失敗を宣言する前に失敗する必要がある ping の**Ping Count (ping** カウント**)** を入力します (範囲は3～10、デフォルトは10)。
8. **Destination IP Group (**宛先 **IP** グループ**)** 名を **Add (**追加**)** し、入力します。
9. 1つ以上の **Destination IP (**宛先 **IP)** アドレスを ping に **Add (**追加**)** します。
10. 宛先 IP グループのパス モニタリングを有効にするには、**Enabled (**有効**)** を選択します。
11. この宛先 ＩＰ グループで障害が発生する**Failure Condition (**障害条件**)** を選択します:リストされている1つ以上の IP アドレスに到達できない場合に障害を発行する**Any (**指定なし**)** (デフォルト)、またはリストされているすべての IP アドレスに到達できない場合に障害を発行する **All (**すべて**)**。
12. **OK** を 2 回クリックします。
13. (Panorama のみ) 適切な Panorama テンプレートを選択して、パス監視設定をご利用のアプライアンスにプッシュします。

> 仮想ワイヤ、*VLAN*、または仮想ルータの *HA* パス監視は、*PAN-OS 10.0* 以降のリリースを実行している *firewall* にのみプッシュできます。*PAN-OS 10.0* より前のリリース *(9.1.x* や *9.0.x* など*)* を実行している *firewall* に構成をプッシュしようとすると、コミットが失敗するか、コミットによってパス・グループから宛先 *IP* アドレスが削除されることがあります。
>
> *1* つの *Destination IP Group* を含む *HA Path Groups* のみが、*PAN-OS 9.1* 以前のリリースを実行しているマネージド *firewall* でサポートされます。

> 異なる *PAN-OS* リリースを実行しているマネージド *firewall* の宛先 *IP* アドレスを *Panorama* から管理するには、*PAN-OS 10.0* 以降のリリースを実行しているマネージド *firewall* 用に別の template を作成し、*PAN-OS 9.1* 以前のリリースを実行しているマネージド *firewall* 用に別のテンプレートを作成します。これにより、複数の宛先 *IP* グループを作成した場合に宛先 *IP* アドレス構成をより正確に制御でき、管理対象の *firewall* が正常にフェイルオーバーされるようにすることができます。

STEP 4 | （任意）ファイアウォールで設定したすべてのパス グループの失敗条件を変更します。

デフォルトでは、モニター対象のパス グループのいずれかに障害が発生すると、ファイアウォールでフェイルオーバーが引き起こされます。

1. **Path Monitoring**（パス モニタリング） セクションを編集します。
2. アプライアンス上でパス モニタリングを有効にするには、**Enabled (**有効**)** を選択します。
3. つ以上の監視対象の仮想ルーター、VLAN、または仮想ワイヤーがダウンしたときにこのファイアウォールの障害を発行するには、**Failure Condition (**障害条件**)** を**Any (**指定なし**)** (デフォルト)に設定します。監視対象のすべての仮想ルーター、VLAN、またはバー

チャル ワイヤーがダウンしたときにこのファイアウォールの障害を発行するには、**All (すべて)** を選択します。

4. **OK**をクリックします。

STEP 5 | **Commit (コミット)**します。

フェイルオーバーの確認

HA の設定が正しく動作することをテストするには、手動でフェイルオーバーを引き起こして、ファイアウォールの状態が正しく移行することを確認します。

STEP 1 | アクティブ ファイアウォールをサスペンドにします。

Device (デバイス) > **High Availability (高可用性)** > **Operational Commands (操作コマンド)** を選択し、**Suspend local device (ローカル デバイスをサスペンド)** リンクをクリックします。

STEP 2 | パッシブ ファイアウォールがアクティブ ファイアウォールとしてタスクを引き継いでいることを確認します。

Dashboard の High Availability （高可用性）ウィジットで、パッシブ ファイアウォールの状態が **active** に変わっていることを確認します。

STEP 3 | サスペンドされたファイアウォールを稼働状態に戻します。プリエンプティブを有効にしている場合は、しばらく待ってからプリエンプションが発生していることを確認します。

1. 前の手順でサスペンドにしたファイアウォールで、**Device (デバイス)** > **High Availability (高可用性)** > **Operational Commands (操作コマンド)** の順に選択して、**Make local device functional (ローカル デバイスを稼働状態にする)** リンクをクリックします。
2. **Dashboard (ダッシュボード)** の High Availability (高可用性) ウィジットで、ファイアウォールがアクティブ ファイアウォールとしてタスクを引き継いでいることと、ピアがパッシブ状態に変わっていることを確認します。

アクティブ/アクティブ HA のセットアップ

アクティブ/アクティブ HA の前提条件

Palo Alto Networks ファイアウォールでアクティブ/アクティブ HAをセットアップするには、以下の前提条件を満たすファイアウォールのペアが必要です。

- 同じモデル — ハードウェアのモデルが、ペアの両方のファイアウォールで同じでなければなりません。
- 同じバージョンの **PAN OS** — ファイアウォールで同じバージョンの PAN OS を実行していて、両方のアプリケーション、URL、および脅威データベースで最新の状態が保たれている必要があります。
- 同一のマルチ仮想システム機能—両方のファイアウォールは**Multi Virtual System Capability**[マルチ仮想システム機能]を有効または無効化する必要があります。有効化すると、各ファイアウォールには独自のマルチ仮想システムライセンスが必要になります。
- 同タイプのインターフェイス — 専用の HA リンク、またはインターフェイス タイプを HA に設定した管理ポートとインバンド ポートの組み合わせです。
  - HAインターフェイスは静的IPアドレスのみで設定します。DHCPから得られたIPアドレスではありません（AWSがDHCPアドレスを使える場合は除く）。HA ピア間の HA1 （コントロール）接続の IP アドレスを決定します。ピアが直結されている場合、または同じスイッチに接続されている場合は、 HA1 IP アドレスが同じサブネット上になければなりません。

    専用の HA ポートを持たないファイアウォールでは、管理ポートをコントロール接続に使用できます。管理ポートを使用すると、両方のファイアウォールの管理プレーン間の通信を直接接続できます。ただし、管理ポートはピア間で直結できないため、ネットワーク上にこれら 2 つのインターフェイスを接続するルートがあることを確認してください。
  - レイヤー 3 を HA （データ）接続の転送方法として使用する場合、HA2 リンクの IP アドレスを決定する必要があります。経路指定されたネットワークを介して HA2 接続の通信を行う必要がある場合は、レイヤー 3 のみを使用します。HA2 リンクの IP サブネットは、HA1 リンクのサブネットまたはファイアウォール上のデータ ポートに割り当てられたその他のサブネットと重複してはなりません。
  - 各ファイアウォールはHA3リンク専用インターフェイスが必要です。PA-7000シリーズ、PA-5400シリーズ、PA-3400シリーズ、およびPA-3200シリーズのファイアウォールは、HA3にHSCIポートを使用します。HA3 のために PA-5200 Series ファイアウォールに HSCI ポートを使用させる、あるいはデータプレーン ポート上で集約インターフェイスを設定して HA3 の冗長性を確保できます。残存するプラットフォームでは、冗長性を持たせるために、データプレーン ポート上の集約インターフェイスを HA3 リンクに設定できます。

- 同一ライセンス – ライセンスは各ファイアウォールに固有のため、ほかのファイアウォールと共有することはできません。そのため、両方のファイアウォールで同一のライセンスを取得する必要があります。両方のファイアウォールに同一のライセンスがない場合は、設定情報を同期することや、等価性を管理してシームレスにフェイルオーバーすることができません。

  既存のファイアウォールがあり、*HA* 用に新しいファイアウォールを追加する場合、その新しいファイアウォールに既存の設定が存在する場合は、ファイアウォールの工場出荷時設定へのリセットを行うことをお勧めします。これにより、新しいファイアウォールをクリーンな設定にすることができます。*HA* を設定したら、プライマリ ファイアウォールの設定を、新しく導入したクリーンな設定のファイアウォールに同期します。ローカル*IP*アドレスも設定する必要があります。

アクティブ/アクティブ HA の設定

次の作業の流れは、アクティブ/アクティブ構成でファイアウォールを設定する基本的な流れを示しています。ただし、作業を開始する前に、アクティブ/アクティブ ユースケースの判断で、お客様のネットワーク環境により適した構成の例を確認してください。

HA ファイアウォール間にスイッチがある場合、*HA3* リンクを接続するスイッチ ポートが、*HA3* リンクで *MAC-in-MAC* カプセル化に関連したオーバヘッドを処理するには、ジャンボフレームをサポートする必要があります。

アクティブ/アクティブの設定を行うには、まずは 1 つ目のピアで、次に 2 番目のピアで各作業をを完了させ、各ピアに対して必ず異なるデバイス IDの値（0 あるいは 1）を設定するようにします。

STEP 1 | HA ポートを接続して、ファイアウォール間の物理的な接続をセットアップします。

各使用例で、ファイアウォールはハードウェア モデルが可能です。お使いのモデルに対応する*HA3*ステップを選択します。

- 専用の HA ポートを持つファイアウォールの場合は、Ethernet ケーブルを使用して、ピアの専用の HA1 ポートと HA2 ポートを接続します。ピア同士を直結する場合は、クロスオーバー ケーブルを使用します。
- 専用の HA ポートを持たないファイアウォールの場合は、HA2 リンク用とバックアップ HA1 リンク用の 2 つのデータ インターフェイスを選択します。次に、Ethernet ケーブルを使用して、両ファイアウォール間でこれらのインバンド HA インターフェイスを接続し

ます。HA1 リンク用の管理ポートを使用して、ネットワーク全体を通じて管理ポート同士を接続できることを確認します。

- HA3:
  - PA-7000 シリーズファイアウォールでは、1 番目のシャーシの 高速シャーシインターコネクト（HSCI-A） は 2 番目のシャーシの HSCI-A に直接接続され、1 番目のシャーシの HSCI-B は 2 番目のシャーシの HSCI-B に接続されます。
  - PA-5450 ファイアウォールで、最初のシャーシのHSCI-Aを2番目のシャーシのHSCI-Aに接続し、最初のシャーシのHSCI-Bを2番目のシャーシのHSCI-Bに接続します。
  - PA-5400 シリーズ ファイアウォール (HSCI ポートが 1 つある) で、最初のシャーシの HSCI ポートを 2 番目のシャーシの HSCI ポートに接続します。
  - PA-5200 Series ファイアウォール（HSCI ポートが 1 つあるもの）上で、1 番目のシャーシにある HSCI ポートを 2番目のシャーシの HSCI ポートに接続します。また、PA-5200 Series ファイアウォール上の HA3 用データポートを使用することもできます。
  - PA-3400 シリーズ ファイアウォール(HSCIポートが1つある)では、最初のシャーシのHSCIポートを2番目のシャーシのHSCIポートに接続します。
  - PA-3200 Series ファイアウォール（HSCI ポートが1つあるもの）上で、1 番目のシャーシにある HSCI ポートを 2 番目のシャーシの HSCI ポートに接続します。
  - 他のハードウェア モデルでは、HA3のデータプレーンインターフェイスを使います。

STEP 2 | ping を管理ポートで有効にします。

ping を有効にすることで、管理ポートをハートビート バックアップの情報交換に使用できます。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** にて、Management Interface Settings (管理インターフェイス設定) を編集します。
2. インターフェイスで許可されるサービスとして **[Ping]** を選択します。

STEP 3 | ファイアウォールに専用の HA ポートがない場合は、データ ポートを HA ポートとして機能するように設定します。

専用の HA ポートを持つファイアウォールの場合は、次の手順に進みます。

1. **Network (ネットワーク)** > **Zones (ゾーン)** の順に選択します。
2. 使用するポート上でリンクがアップになっていることを確認します。
3. インターフェイスを選択して、**Interface Type** （インターフェイス タイプ）を **HA** に設定します。
4. 必要に応じて、**Link Speed** （リンク速度）および **Link Duplex** （リンク デュプレックス）を設定します。

STEP 4 | アクティブ/アクティブHAを有効化し、グループIDを設定します。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Setup (セットアップ) を編集します。
2. **Enable HA**（**HA** の有効化）を選択します。
3. 両方のファイアウォールで同じ**Group ID**を入力します。ファイアウォールはグループIDを使って仮想MACアドレスを計算します（範囲は1～63）。
4. （任意）**Description (内容)** を入力します。
5. **Mode (モード)**は、**Active Active**を選択します。

STEP 5 | デバイス ID を設定し、同期を有効化し、ピアファイアウォールでコントロールリンクを特定します。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Setup (セットアップ) を編集します。
2. **Device ID (デバイス ID)** を次の通り選択します。
   - 最初のピアを設定する際、**Device ID (デバイス ID)** を **0** に設定します。
   - 2 番目のピアを設定する際、**Device ID (デバイス ID)** を **1** に設定します。
3. **Enable Config Sync** （設定の同期化の有効化）を選択します。2つのファイアウォール設定を同期させる場合に、この設定が必要です（デフォルトで有効になっています）。
4. **Peer HA1 IP Address (ピアHA1のIPアドレス)**– ピアファイアウォールのHA1コントロールリンクスのIPアドレスを入力します。
5. （任意） **Backup Peer HA1 IP Address (バックアップピアHA1のIPアドレス)**– ピアファイアウォールのHA1バックアップリンクのIPアドレスを入力します。
6. **OK** をクリックします。

STEP 6 | 障害復旧時に、下位デバイス ID を持つファイアウォールがアクティブプライマリファイアウォールをプリエンプトするかどうか決めます。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Election Settings (選択設定) を編集します。
2. **Preemptive (プリエンプティブ)**を選択し、いずれかのファイアウォールが障害から復旧した後に、下位デバイスIDのファイアウォールに自動的にアクティブプライマリオペレーションを再開させます。両方のファイアウォールは、発生するプリエンプションに**Preemptive (プリエンプティブ)**を選択します。

   復旧したファイアウォールを手動でアクティブプライマリファイアウォールにするまで、アクティブプライマリロールを現在のファイアウォールに残す場合は、**Preemptive (プリエンプティブ)** は選択しません。

STEP 7 | コントロール リンクで専用 HA ポートまたはインバンド ポートを使用している場合は、ハートビート バックアップを有効にします。

管理ポートをコントロール リンクに使用している場合は、ハートビート バックアップを有効にする必要はありません。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Election Settings (選択設定) を編集します。
2. **Heartbeat Backup (ハートビート バックアップ)**を選択します。

   ハートビートをファイアウォール間で送信できるようにするには、ピア同士で管理ポートをルーティングできることを確認する必要があります。

   ハートビート バックアップを有効にすると、スプリット ブレインを防ぐこともできます。*HA1* リンクがダウンしてファイアウォールがハートビートを受信しなくなると、スプリット ブレインが発生します。ただし、そのファイアウォールはまだ機能しています。このような状況になると、各ピアは相手がダウンしていると判断して、実行中のサービスを開始しようとするため、スプリット ブレイン状態になります。ハートビート バックアップ リンクが有効にされていると、冗長なハートビートおよび *hello* メッセージが管理ポート経由で送信されるため、スプリット ブレインを防ぐことができます。

STEP 8 | （任意）HA タイマーを変更します。

デフォルトで、HA タイマー プロファイルは、ほとんどの HA デプロイメントに適した **Recommended (推奨)**プロファイルに設定されています。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Election Settings (選択設定) を編集します。
2. **Aggressive (アグレッシブ)**を選択して、高速フェイルオーバーをトリガーします。Select **Advanced (詳細)**を選択し、お使いの設定でフェイルオーバーをトリガーするカスタム値を定義します。

   プロファイルに含まれる個々のタイマーの事前設定値を表示するには、***Advanced***（詳細）を選択して ***Load Recommended***（推奨をロード）または ***Load Aggressive***（アグレッシブをロード）をクリックします。お使いのハードウェア モデルの事前設定値が画面に表示されます。

STEP 9 | コントロール リンクの接続をセットアップします。

ここに示す例は、インターフェイス タイプを HA に設定したインバンド ポートです。

管理ポートをコントロール リンクとして使用するファイアウォールの場合、IP アドレス情報が自動的に入力されます。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Control Link (HA1) (コントロール リンク (HA1)) を編集します。
2. HA1 リンクとして使用するために配線した **Port (ポート)** を選択します。
3. **IPv4/IPv6 Address**（**IPv4/IPv6** アドレス） と **Netmask**（ネットマスク） を設定します。

   HA1 インターフェイスが個別のサブネットにある場合は、**Gateway**（ゲートウェイ）の IP アドレスを入力します。ファイアウォール同士を直結している場合は、ゲートウェイのアドレスを追加しないでください。

STEP 10 | （任意）コントロール リンク接続の暗号化を有効にします。

この設定は一般に、2 つのファイアウォールが直接接続されていない場合、すなわちポートがスイッチまたはルーターに接続されている場合に、リンクを保護するために使用します。

1. 一方のファイアウォールから HA キーをエクスポートして、ピア ファイアウォールにインポートします。
   1. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書）
   2. **Export HA key**（**HA** 鍵のエクスポート）を選択します。ピアがアクセスできるネットワーク上の場所に、HA キーを Save （保存）します。
   3. ピア ファイアウォールで、**Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificates (証明書)** の順に選択し、**Import HA key (HA** キーのインポート**)** を選択してキーを保存した場所を検索し、そのキーをピアにインポートします。
2. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Control Link (HA1) (コントロール リンク (HA1)) を編集します。
3. **Encryption Enabled (暗号化を有効)**を選択します。

   暗号化を有効にした場合、*HA* ファイアウォール の設定が完了した後、HA1 SSH 鍵の更新およびキーのオプションの設定できます。

STEP 11 | バックアップ コントロール リンクの接続をセットアップします。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Control Link (HA1 Backup) (コントロール リンク (HA1 バックアップ)) を編集します。
2. HA1 バックアップ インターフェイスを選択し、**IPv4/IPv6 Address (IPv4/IPv6** アドレス**)** および **Netmask (**ネットマスク**)** を設定します。

   PA-3200 Series のファイアウォールは *HA1* バックアップ制御リンク用の *IPv6* アドレスをサポートしていないため、*IPv4* アドレスを使用してください。

STEP 12 | ファイアウォール間のデータ リンク接続（HA2）とバックアップ HA2 接続をセットアップします。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Data Link (HA2) (データリンク (HA2)) を編集します。
2. データ リンク接続に使用する **Port**（ポート） を選択します。
3. **Transport (転送)**の方法を選択します。デフォルトは **ethernet** で、HA ペアが直結されている場合、またはスイッチ経由で接続されている場合はこの方法が機能します。ネットワーク経由でデータ リンク トラフィックをルーティングする必要がある場合は、**IP** または **UDP** を転送方法に指定します。
4. 転送方法に IP または UDP を使用する場合は、**IPv4/IPv6 Address**（**IPv4/IPv6** アドレス）と **Netmask**（ネットマスク） を入力します。
5. **Enable Session Synchronization**（セッション同期を有効にする） が選択されていることを確認します。
6. HA ピア間の HA2 データ リンクのモニタリングを有効にするには、**HA2 Keep-alive**（**HA2** キープアライブ） を選択します。設定されているしきい値（デフォルトは 10000 ミリ秒）に基づいて障害が発生した場合、定義されているアクションが発生します。HA2 キープアライブのエラーが発生すると、システムは設定に応じて、重大なシステム ログ メッセージを生成するか、スプリット データプレーンを発生させます。

   HA2 Keep-alive (HA2 キープアライブ*)* オプションは、*HA* ペアの両方のファイアウォールにも一方のファイアウォールのみにも設定できます。このオプションが一方のファイアウォールでのみ有効な場合、そのファイアウォールのみからキープアライブ メッセージが送信されます。もう一方のファイアウォールに、障害が発生したかどうかが通知されます。

   スプリット データプレーンにより、高可用性状態がアクティブ-プライマリおよびアクティブ-セカンダリとして維持されたまま、ピアの両方のデータプレーンが独立して動作するようになります。単一のファイアウォールのみがスプリット データプレーンとして設定されている場合、スプリット データプレーンがもう片方のデバイスにも適用されます。
7. **Data Link (HA2 Backup) (データ リンク (HA2 バックアップ))** セクションを編集してインターフェイスを選択し、**IPv4/IPv6 Address (IPv4/IPv6** アドレス**)** および **Netmask (**ネットマスク**)** を追加します。
8. **OK** をクリックします。

STEP 13 | パケット転送用にHA3リンクを設定します。

1. **Device (デバイス)** > **High Availability (高可用性)** > **Active/Active Config (アクティブ/アクティブ設定)** にて、Packet Forwarding (パケット転送) を編集します。
2. **HA3 Interface (HA3**インターフェイス**)**で、 アクティブ/アクティブのHAピア間のパケットの転送に使用しようとしているインターフェイスを選択します。それはレイヤー2転送が可能な専用インターフェイスである必要があります。 **Interface Type HA (**インターフェイスタイプ**HA)**に設定します。.
3. **VR Sync (VR** 同期**)** を選択して、HAピアに設定されたすべての仮想ルーターの同期を強制します。仮想ルーターが動的ルーティングプロトコル用に設定されていない場合は、

選択します。両方のピアが交換網を介して同じネクストホップルーターに接続されている必要があり、スタティックルーティングのみを使用している必要があります。

4. すべての物理インターフェイスで QoS プロファイル選択を同期するには、 **QoS Sync** を選択します。両方のピアのリンク速度が同様で、すべての物理インターフェイスで同じQoSプロファイルが必要な場合に選択します。この設定は、**Network**[ネットワーク]タブの QoS 設定の同期に影響します。QoS ポリシーは、この設定に関係なく同期されます。

STEP 14 | （任意） Tentative Hold Time （暫定的な状態の保留時間）を変更します。

1. **Device (デバイス)** > **High Availability (高可用性)** > **Active/Active Config (アクティブ/アクティブ設定)** にて、Packet Forwarding (パケット転送) を編集します。
2. **Tentative Hold Time (sec) (暫定的な状態の保留時間 (秒))** は、障害から回復した後、ファイアウォールが 暫定的な状態にとどまる秒数を入力します (範囲は 10～600、デフォルトは 60 です)。

STEP 15 | セッション オーナーの設定およびセッションのセットアップを行います。

1. **Device (デバイス)** > **High Availability (高可用性)** > **Active/Active Config (アクティブ/アクティブ設定)** にて、Packet Forwarding (パケット転送) を編集します。
2. **Session Owner Selection (セッションオーナーの選択)**で、以下のいずれかを選択します。
   - **First Packet (最初のパケット)**—新しいセッションで 最初のパケットを受信したデバイスがセッション オーナーとなります（推奨設定）。この設定によりHA3のトラフィックとピア間のロード共有トラフィックが最小化されます。
   - **Primary Device (プライマリデバイス)**—アクティブプライマリ状態のファイアウォールがセッションオーナーになります。
3. **Session Setup (セッションのセットアップ)**で、以下のいずれかを選択します。
   - **IP Modulo (IP モジュロ)**—ファイアウォールはパケットから得た送信元および宛先 IP アドレスに対して XOR 演算を実行し、その結果に基づいて、どちらの HA ピアがセッションをセットアップするのか決定します。
   - **Primary Device**（プライマリデバイス） — アクティブ-プライマリのデバイスがすべてのセッションを確立します。
   - **First Packet (最初のパケット)**—新しいセッションで最初のパケットを受信したファイアウォールがセッションセットアップを実行します。

     セッションおよびセッション セットアップの最初のパケットから開始した後、負荷分散に基づいて他のいずれかのオプションに変更できるようになります。
   - **IP Hash (IPハッシュ)**—ファイアウォールは、送信元または送信元と宛先のIPアドレスを組み合わせたハッシュを使って、セッションセットアップの責任を分散します。
4. **OK** をクリックします。

STEP 16 | HA仮想アドレスを設定します。

フローティング IP アドレスと仮想 MAC アドレスあるいは ARP ロード シェアリングを使用するためには、仮想アドレスが必要になります。

1. **Device (デバイス)** > **High Availability (高可用性)** > **Active/Active Config (アクティブ/アクティブ設定)** で仮想アドレスを **Add (追加)** します。
2. **Interface (インターフェイス)**を入力もしくは選択します。
3. **IPv4** または **IPv6** タブを選択し、**Add (追加)** をクリックします。
4. **IPv4 Address (IPv4** アドレス**)** あるいは **IPv6 Address (IPv6** アドレス**)** を入力します。
5. **Type (タイプ)**
   - 仮想IをフローティングIPアドレスにするには **Floating (フローティング)**を選択します。
   - 仮想 IP アドレスを共有 IP アドレスとして設定するには **ARP Load Sharing (ARP** ロード共有**)** を選択し、ARP ロード共有の設定までスキップします。

STEP 17 | フローティングIPアドレスの設定

1. アクティブ/アクティブHAペアをアクティブ/パッシブHAペアのように動作させるのでなければ、**Floating IP bound to the Active-Primary device (**フローティング**IP**をアクティブ**-**プライマリ**HA**デバイスに固定**)** は選択しないでください。
2. **Device 0 Priority (**デバイス**0**優先順位**)** と **Device 1 Priority (**デバイス**1**優先順位**)** では、それぞれデバイスID 0 とデバイス ID 1で設定するファイアウォールの優先順位を入力します。相対的優先順位は、設定したフローティングIPアドレス（範囲は0～255）を所有するピアを決めます。最低数値（優先順位が高い） のファイアウォールがフローティング IP アドレスを所有します。
3. **Failover address if link state is down (**リンク状態がダウンの場合アドレスをフェイルオーバー**)** を選択して、 インターフェイスのリンク状態がダウンの場合に、ファイルオーバーアドレスを使用します。
4. **OK** をクリックします。

STEP 18 | ARP ロード シェアリングを設定します。

デバイス選択アルゴリズムは、ARP要求に応答して、ロード共有を行うHAファイアウォールを決めます。

1. **Device Selection Algorithm (**デバイス選択アルゴリズム**)**で、以下のいずれかを選択します。
   - **IP Modulo (IP**モジュロ**)** — ARPリクエスト元IPアドレスのパリティに基づいて、ARPリクエストに応答するファイアウォールが選択されます。
   - **IP Hash (IP**ハッシュ**)** — ARPリクエスト元IPアドレスのハッシュに基づいて、ARPリクエストに応答するファイアウォールが選択されます。
2. **OK** をクリックします。

STEP 19 | フェイルオーバー条件の定義を行います。

STEP 20 | 設定を **Commit**（コミット）します。

アクティブ/アクティブのユースケースの決定

使用例のタイプを決めてから、アクティブ/アクティブ HA を設定する適切な手順を選択します。

ルート ベース冗長性、フローティング IP アドレスと仮想 MAC アドレス、またはARP ロード共有を使用している場合は、対応する手順を選択します。

- 「ユース ケース：ルートベース冗長性をアクティブ/アクティブHAに設定する
- 「ユース ケース：フローティングIPアドレスをアクティブ/アクティブHAに設定する
- 「ユース ケース：ARPロード共有をアクティブ/アクティブHAに設定する

レイヤー3アクティブ/アクティブ HA 展開をアクティブ/パッシブ展開のように動作させる場合は、以下の手順を選択します。

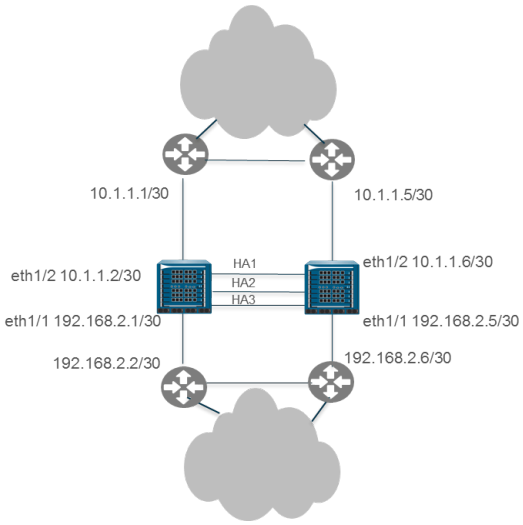
- 「ユース ケース：アクティブプライマリファイアウォールにバインドされたフローティングIPアドレスをアクティブ/アクティブHAに設定する

NAT in Active/Active HA Mode[アクティブ/アクティブHAモードのNAT]を構成する場合は、次の手順を参照してください。

- 「ユース ケース：フローティングIPアドレスを使って送信元DIPP NATをアクティブ/アクティブHAに設定する
- 「ユース ケース：個別送信元NAT IPアドレスプールをアクティブ/アクティブHAファイアウォールに設定する
- 「ユース ケース：ARPロード共有を宛先NATでアクティブ/アクティブHAに設定する
- 「ユース ケース：ARPロード共有をレイヤー3の宛先NATでアクティブ/アクティブHAに設定する

「ユース ケース：ルートベース冗長性をアクティブ/アクティブHAに設定する

以下のレイヤー 3 の例は、ルート ベース冗長性を使用するアクティブ/アクティブ HA 環境での 2 つのPA-7050 ファイアウォールですファイアウォールはOSPF領域に属します。リンクまたはファイアウォールに障害が発生した場合、OSPFはトラフィックを機能しているファイアウォールにリダイレクトすることによって冗長性を処理します。



STEP 1 | アクティブ/アクティブ HA の設定を行います。

ステップ 1 からステップ 15 を実行します。

STEP 2 | OSPF を設定する。

OSPFを参照してください。

STEP 3 | HAフェイルオーバー条件の定義

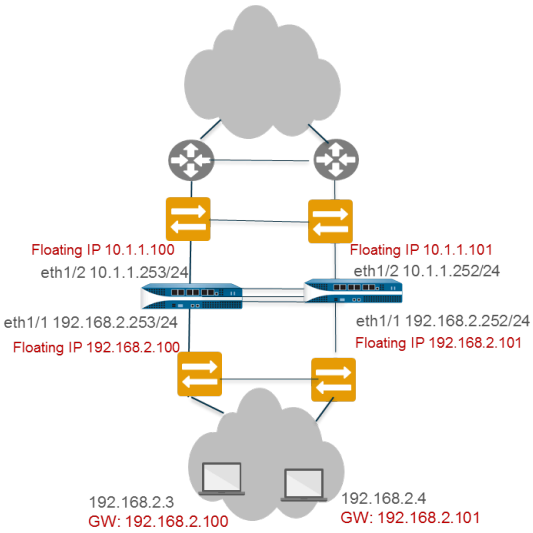
フェイルオーバー条件の定義を行います。

STEP 4 | 設定を **Commit**（コミット）します。

STEP 5 | ステップ 5 で、最初の firewall に Device ID **0** を選択した場合は、ピア firewall に Device ID **1** を選択する以外は、同じ方法でピア firewall を構成します。

「ユース ケース：フローティングIPアドレスをアクティブ/アクティブHAに設定する

このレイヤー3インターフェイスの例では、HAファイアウォールはスイッチに接続し、フローティングIPアドレスを使ってリンクやファイアウォールの障害を処理します。エンドホストは、1つのHAファイアウォールのフローティングIPアドレスであるゲートウェイで設定されています。フローティング IP アドレスと仮想 MAC アドレスを参照してください。



STEP 1 | アクティブ/アクティブ HA の設定を行います。

ステップ1からステップ15を実行します。

STEP 2 | HA仮想アドレスを設定します。

フローティング IP アドレスと仮想 MAC アドレスを使用するためには、仮想アドレスが必要になります。

1. **Device (デバイス)** > **High Availability (高可用性)** > **Active/Active Config (アクティブ/アクティブ設定)** で仮想アドレスを **Add (追加)** します。
2. **Interface (インターフェイス)**を入力もしくは選択します。
3. **IPv4** または **IPv6** タブを選択し、**Add (追加)** をクリックします。
4. **IPv4 Address (IPv4 アドレス)** あるいは **IPv6 Address (IPv6 アドレス)** を入力します。
5. **Type**（タイプ）で、仮想IPアドレスをフローティングIPアドレスにするには **Floating**（フローティング）を選択します。

STEP 3 | フローティングIPアドレスの設定

1. **Floating IP bound to the Active-Primary device**[アクティブプライマリ デバイスにバインドされた浮動 IP]は選択しないでください。
2. **Device 0 Priority (デバイス0優先順位)** と **Device 1 Priority (デバイス1優先順位)** では、それぞれデバイスID 0 とデバイス ID 1で設定するファイアウォールの優先順位を入力します。相対優先順位によって、構成したフローティング IP アドレスを所有するピアが決まります (範囲は 0 ~ 255)。最低数値（優先順位が高い） のファイアウォールがフローティング IP アドレスを所有します。
3. **Failover address if link state is down (リンク状態がダウンの場合アドレスをフェイルオーバー)** を選択して、 インターフェイスのリンク状態がダウンの場合に、ファイルオーバーアドレスを使用します。
4. **OK** をクリックします。

STEP 4 | PA-7000シリーズファイアウォール以外のファイアウォールでジャンボフレームを有効にします。

ステップ 19 の アクティブ/アクティブ HA の設定を実行します。

STEP 5 | フェイルオーバー条件の定義

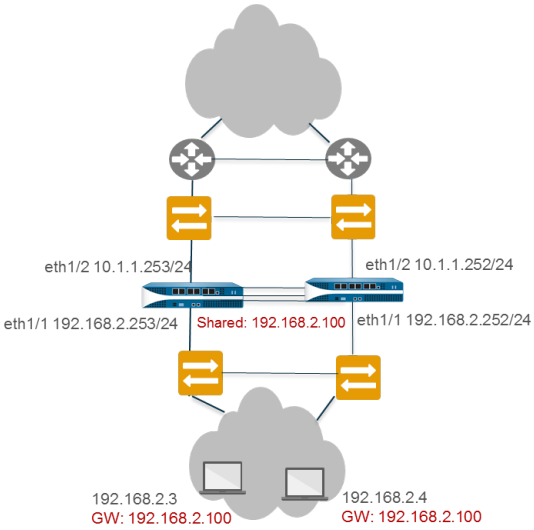
STEP 6 | 設定を **Commit**（コミット）します。

STEP 7 | 別のデバイス ID を選択するということ以外は同じやり方で、ピア ファイアウォールを設定します。

例えば、最初のファイアウォールにデバイスID **0** を選択した場合は、ピアファイアウォールにデバイスID**1**を選択します。

「ユース ケース：**ARP**ロード共有をアクティブ/アクティブ**HA**に設定する

この例では、レイヤー3のホストは、HAファイアウォールのゲートウェイサービスが必要です。ファイアウォールは、ARP ロード シェアリングが可能な 1 つの共有 IP アドレスで設定します。エンドホストは、HAファイアウォールの共有Pアドレスである同一のゲートウェイで設定されています。



STEP 1 | ステップ 1 ~ ステップ 15 の アクティブ/アクティブ HA の設定を実行します。

STEP 2 | HA仮想アドレスを設定します。

仮想アドレスはARP ロード シェアリングが可能な共有 IP アドレスです。

1. **Device (デバイス)** > **High Availability (高可用性)** > **Active/Active Config (アクティブ/アクティブ設定)** > **Virtual Address (仮想アドレス)** を選択して **Add (追加)** をクリックします。
2. **Interface (インターフェイス)**を入力もしくは選択します。
3. **IPv4** または **IPv6** タブを選択し、**Add (追加)** をクリックします。
4. **IPv4 Address (IPv4** アドレス) あるいは **IPv6 Address (IPv6** アドレス) を入力します。
5. **Type (タイプ)** では、両方のピアがARP ロード共有で仮想IPアドレスを使えるようにする**ARP Load Sharing (ARP**ロード共有) を選択します。

STEP 3 | ARP ロード シェアリングを設定します。

デバイス選択アルゴリズムは、ARP要求に応答して、ロード共有を行うHAファイアウォールを決めます。

1. **Device Selection Algorithm (デバイス選択アルゴリズム)**で、以下のいずれかを選択します。
   - **IP Modulo (IP**モジュロ) — ARPリクエスト元IPアドレスのパリティに基づいて、ARPリクエストに応答するファイアウォールが選択されます。
   - **IP Hash (IP**ハッシュ) — ARPリクエスト元IPアドレスのハッシュに基づいて、ARPリクエストに応答するファイアウォールが選択されます。
2. **OK** をクリックします。

STEP 4 | PA-7000シリーズファイアウォール以外のファイアウォールでジャンボフレームを有効にします。

STEP 5 | フェイルオーバー条件の定義

STEP 6 | 設定を **Commit**（コミット）します。

STEP 7 | 別のデバイス ID を選択するということ以外は同じやり方で、ピア ファイアウォールを設定します。

例えば、最初のファイアウォールにデバイスID **0** を選択した場合は、ピアファイアウォールにデバイスID**1**を選択します。

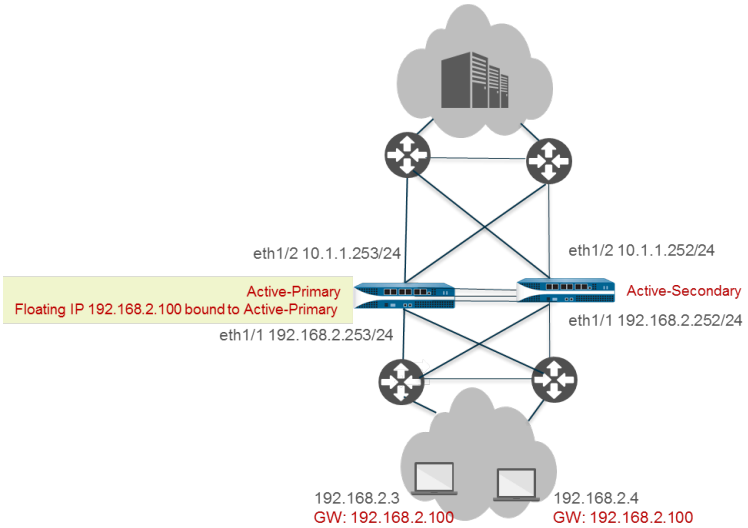
「ユース ケース：アクティブプライマリファイアウォールにバインドされたフローティング**IP**アドレスをアクティブ**/**アクティブ**HA**に設定する

ミッション クリティカルなデータセンターでは、両方のファイアウォールのパス障害を検出できるように、両方のレイヤー3HAファイアウォールをパスのモニタリングに参加させることができます。さらに、バインドされたデバイスIDに戻るフローティングIPアドレスでなく、復旧後、フローティングIPアドレスが復旧したファイアウォールに戻るタイミングをコントロールできます。（デフォルトの動作は、フローティング IP アドレスと仮想 MAC アドレスで説明しています）

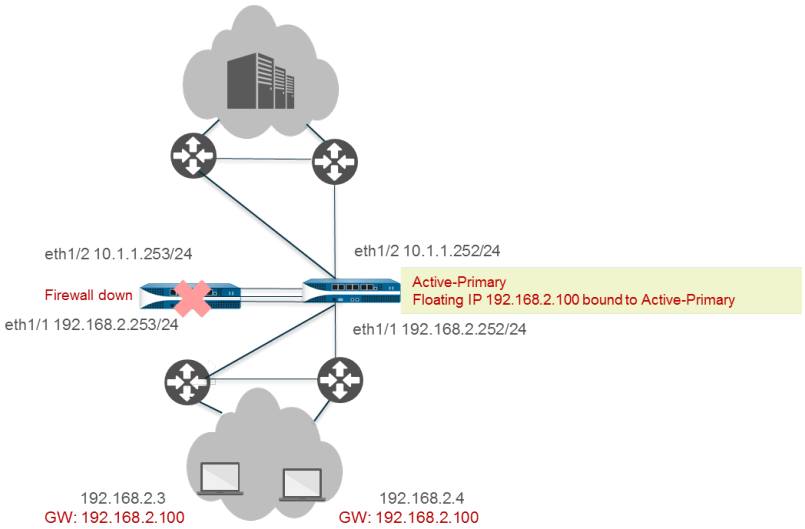
この使用例では、フローティングIPアドレス、ひいてはアクティブプライマリファイアウォールロールが復旧したHAピアに戻るタイミングをコントロールできます。アクティブ/アクティブHAファイアウォールは、アクティブプライマリ状態にあるいずれかのファイアウォールにバインドする1つのフローティングIPアドレスを共有します。1つのフローティングIPアドレスによってネットワークトラフィックは主に1つのファイアウォールに移動します。従って、このアクティブ/アクティブ展開機能はアクティブ/パッシブ展開に類似します。

この使用例では、 レイヤー3で機能する仮想PortChannels （vPCs） を有するCisco Nexus 7010スイッチはファイアウォールに接続します。レイヤー3スイッチ（ルーターピア）は、ルートをフローティングIPアドレスに設定してファイアウォールの north- south に設定する必要があります。ルーターピアのルートテーブルがフローティングIPアドレスへの最善のパスを持つようにネットワークを設定しなければなりません。この例は、フローティングIPアドレスへのルートは低メトリクス（フローティングIPアドレスへのルートが好ましい）を使い、トラフィックを受信するように適切なメトリクスを持った静的ルートを使用しています。静的ルートの代用としては、（OSPFを使っている場合）ネットワークをフローティングIPアドレスをOSPFルーティングプロトコルに再配信するようにデザインします。

下図は、当初はピアAであるアクティブプライマリファイアウォールにバインドされたフローティングIPアドレスです。左はファイアウォールです。



フェイルオーバー時、アクティブプライマリファイアウォール（ピアA）がダウンし、アクティブセカンダリファイアウォール（ピアB）がアクティブプライマリピアになると、フローティングIPアドレスはピアBに移動します（下図参照）。ピアBはアクティブプライマリファイアウォールのままであり、ピアAが復旧してアクティブセカンダリファイアウォールになってからもトラフィックはピアBに行きます。ピアAがアクティブプライマリファイアウォールになるのか、なるとすればそのタイミングを決める必要があります。



フローティングIPアドレスをアクティブプライマリファイアウォールにバインドすると、ファイアウォールが様々なHA ファイアウォール状態の間を移動する場合、フローティングIPアドレスオーナーシップを決定する方法をより多くコントロールできます。結果として以下のような利点が生じます。

- 両方のファイアウォールからパスモニタリングのためのアクティブアクティブHA設定が得られますが、ファイアウォールはアクティブパッシブHA設定のように機能します。なぜならフローティングIPアドレスに指向するトラフィックは常にアクティブプライマリファイアウォールに向かうからです。

両方のファイアウォールでプリエンプションを無効化すると、さらに以下のような利点が生じます。

- アクティブセカンダリファイアウォールがフラップアップまたはダウンする場合、フローティングIPアドレスはHAファイアウォールに往復しません。
- マニュアルでトラフィックを再度転送する前に、復旧したファイアウォールと隣接コンポーネントの機能をレビューできます。転送は都合のいいダウンタイムで実行できます。
- フローティングIPアドレスを所有するファイアウォールをコントロールできます。従って、アクティブプライマリファイアウォールの新規または既存のセッションはHA3リンクのトラフィックを最小化します。

- 各*HA*ピアがリンク障害とピアに対するフェイルオーバーを迅速に検出するように、フローティング*IP*アドレスをサポートするインターフェイスをモニターする*HA*リンクを設定することを強くおすすめします。両方の*HA*ピアは自分の機能をモニターするリンクを持つ必要があります。
- *HA*パスモニタリングはパスに障害が発生した場合、ファイアウォールがピアにフェイルオーバーを送信できるよう、各*HA*ピアに通知するように設定することを強くおすすめします。フローティング*IP*アドレスは常にアクティブプライマリファイアウォールにバインドしているので、パスがダウンしてパスモニタリングが不可能になってもファイアウォールは自動的にはピアにフェイルオーバーできません。

*NAT*はアクティブプライマリファイアウォールにバインドしたフローティング*IP*アドレスには設定できません。

STEP 1 | {31アクティブ/アクティブ HA53} の構成のステップ 1 からステップ 5 を実行します。

STEP 2 | （任意） プリエンプションの無効化

プリエンプションを無効にすると復旧したファイアウォールがアクティブプライマリファイアウォールになるタイミングを完全にコントロールできます。

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Election Settings (選択設定) を編集します。
2. **Preemptive**[プリエンプティブ] が有効になっている場合は、クリアします。
3. **OK** をクリックします。

STEP 3 | 手順 7 ~ 手順 14 の アクティブ/アクティブ HA の設定を実行します。

STEP 4 | セッション オーナーの設定およびセッションのセットアップを行います。

1. **Device (デバイス)** > **High Availability (高可用性)** > **Active/Active Config (アクティブ/アクティブ設定)** にて、Packet Forwarding (パケット転送) を編集します。
2. **Session Owner Selection**[セッションオーナーの選択]については、 **Primary Device**[プライマリデバイス]の選択をおすすめします。アクティブプライマリ状態のファイアウォールがセッションオーナーになります。

   または、**Session Owner Selection (セッション オーナー選択)** で **First Packet (最初のパケット)** し、**Session Setup (セッションのセットアップ)** で **Primary Device (プライマリデバイス)** あるいは **First Packet (最初のパケット)** を選択できます。
3. **Session Setup**（セッションセットアップ）で、Primary Device（プライマリデバイス）を選択します。 — アクティブ-プライマリのファイアウォールがすべてのセッションを確立します。これはアクティブプライマリファイアウォール上のすべてのアクティビ

ティを維持することから、。アクティブ/アクティブ設定をアクティブ/パッシブ設定のように動作させる場合の推奨設定となります。

非対称トラフィックがHAペアに行かないようにネットワークをデザインする必要があります。それを望まない場合にトラフィックがアクティブセカンダリファイアウォールに行く場合は、 ***Session Owner Selection*** *[セッションオーナーの選択]*と ***Session Setup****[セッションセットアップ]*を ***Primary Device*** *[プライマリデバイス]*に設定すると、トラフィックは*HA3* を通過して、セッションオーナシップとセッションセットアップのためにアクティブプライマリファイアウォールに到達するようになります。

4. **OK** をクリックします。

STEP 5 | HA仮想アドレスを設定します。

1. **Device (デバイス)** > **High Availability (高可用性)** > **Active/Active Config (アクティブ/アクティブ設定)** > **Virtual Address (仮想アドレス)** を選択して **Add (追加)** をクリックします。
2. **Interface (インターフェイス)**を入力もしくは選択します。
3. **IPv4** または **Ipv6** タブを選択して、**IPv4 Address (IPv4アドレス)**または **IPv6 Address (IPv6アドレス)** を **Add (追加)** します。
4. **Type**（タイプ）で、仮想IPアドレスをフローティングIPアドレスにするには **Floating**（フローティング）を選択します。
5. **OK** をクリックします。

STEP 6 | フローティングIPアドレスをアクティブプライマリファイアウォールにバインドします。

1. **Floating IP bound to the Active-Primary device**[アクティブプライマリ デバイスにバインドされた浮動 IP]を選択します。
2. **Failover address if link state is down (リンク状態がダウンの場合アドレスをフェイルオーバー)** を選択して、 インターフェイスのリンク状態がダウンの場合に、ファイルオーバーアドレスを使用します。
3. **OK** をクリックします。

STEP 7 | PA-7000シリーズファイアウォール以外のファイアウォールでジャンボフレームを有効にします。

STEP 8 | 設定を **Commit**（コミット）します。

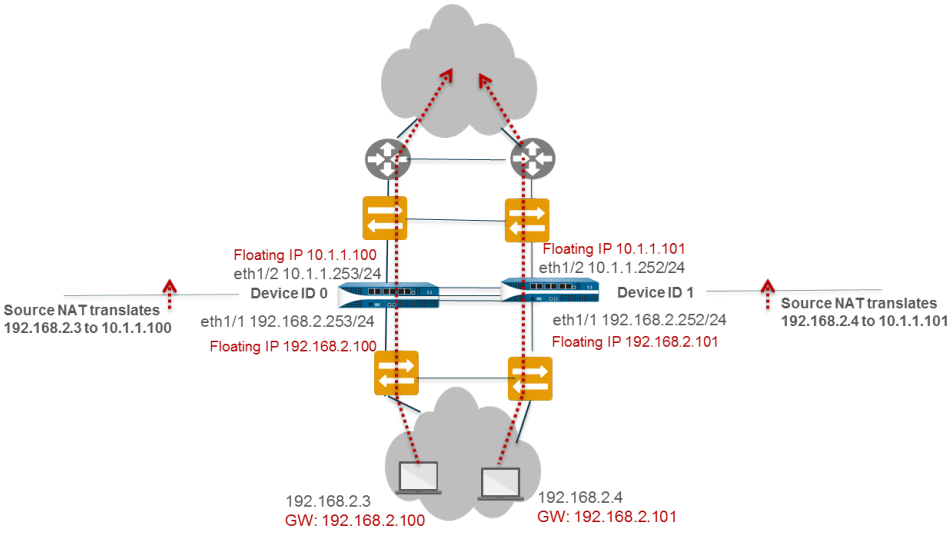
STEP 9 | 別のデバイス ID を選択するということ以外は同じやり方で、ピア ファイアウォールを設定します。

例えば、最初のファイアウォールにデバイスID **0** を選択した場合は、ピアファイアウォールにデバイスID**1**を選択します。

「ユース ケース：フローティングIPアドレスを使って送信元DIPP NATをアクティブ/アクティブHAに設定する

このレイヤー 3 インターフェイスの例では、送信元のアクティブ/アクティブ HA モードの NAT を使用します。レイヤー2スイッチはブロードキャストドメインを生成し、ユーザーはファイアウォールのnorth - south に全て到達できます。

PA-3050-1はデバイス ID 0を持ち、その HA ピアである PA-3050-2はデバイス ID 1を持ちます。この使用例では、NATは送信元IPアドレスとポート番号を、入口インターフェイスに設定されたフローティングIPアドレスに変換します。各ホストは、各ファイアウォールのEthernet1/1のフローティングIPアドレスであるデフォルトゲートウエイアドレスで設定します。この設定では2つの送信元NATルールが要求されます。両方のNATルールを1つのファイアウォールに設定し、ピアファイアウォールに同期しているとしても1つは各デバイスIDにバインドされています。



STEP 1 | PA-3050-2 (Device ID 1) で、{31アクティブ/アクティブ HA33} の設定のステップ 1 ~ ステップ 3 を実行します。

STEP 2 | アクティブ/アクティブ HA の有効化

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Setup (セットアップ) を編集します。
2. **Enable HA**（**HA** の有効化）を選択します。
3. 両方のファイアウォールで同じ**Group ID**を入力します。ファイアウォールはグループIDを使って仮想MACアドレスを計算します（範囲は1～63）。
4. **Mode (モード)**は、**Active Active**を選択します。
5. **Device ID (デバイス ID)** を **1** に設定します。
6. **Enable Config Sync**（設定の同期化の有効化）を選択します。2つのファイアウォール設定を同期させる場合に、この設定が必要です（デフォルトで有効になっています）。
7. **Peer HA1 IP Address (ピアHA1のIPアドレス)**– ピアファイアウォールのHA1コントロールリンクスのIPアドレスを入力します。
8. （任意） **Backup Peer HA1 IP Address (バックアップピアHA1のIPアドレス)**– ピアファイアウォールのHA1バックアップリンクのIPアドレスを入力します。
9. **OK** をクリックします。

STEP 3 | アクティブ/アクティブ HA の設定を行います。

ステップ6からステップ14を完了します。

STEP 4 | セッション オーナーの設定およびセッションのセットアップを行います。

1. **Device (デバイス)** > **High Availability (高可用性)** > **Active/Active Config (アクティブ/アクティブ設定)** にて、Packet Forwarding (パケット転送) を編集します。
2. **Session Owner Selection**（セッションオーナーの選択）では、 **First Packet**（最初のパケット）を選択します。–新しいセッションで 最初のパケットを受信したデバイスがセッション オーナーとなります（推奨設定）。
3. **Session Setup (セッションのセットアップ)** では、**IP Modulo (IP モジュロ)**を選択します。–送信元IPアドレスのパリティに基づいてセッションセットアップロードを分配します。
4. **OK** をクリックします。

STEP 5 | HA仮想アドレスを設定します。

1. **Device (デバイス)** > **High Availability (高可用性)** > **Active/Active Config (アクティブ/アクティブ設定)** > **Virtual Address (仮想アドレス)** を選択して **Add (追加)** をクリックします。
2. **Interface** [インターフェイス] eth1/1を選択します。
3. **Ipv4**を選択し、**IPv4 Address (IPv4 アドレス)** 10.1.1.101を **Add (追加)**します。
4. **Type**（タイプ）で、仮想IPアドレスをフローティングIPアドレスにするには **Floating**（フローティング）を選択します。

STEP 6 | フローティングIPアドレスの設定

1. **Floating IP bound to the Active-Primary device**[アクティブプライマリ デバイスにバインドされた浮動 IP]は選択しないでください。
2. **Failover address if link state is down (**リンク状態がダウンの場合アドレスをフェイルオーバー**)** を選択して、 インターフェイスのリンク状態がダウンの場合に、ファイルオーバーアドレスを使用します。
3. **OK** をクリックします。

STEP 7 | PA-7000シリーズファイアウォール以外のファイアウォールでジャンボフレームを有効にします。

STEP 8 | フェイルオーバー条件の定義を行います。

STEP 9 | 設定を **Commit**（コミット）します。

STEP 10 | 以下の変更を除いて、ピアファイアウォール PA-3050-1を同じ設定で設定します。

- **Device ID 0**[デバイスID 0]を選択します。
- HA仮想アドレス 10.1.1.100を設定します。
- **Device 1 Priority**[デバイス1優先順位]に、 255を入力します。**Device 0 Priority**[デバイス1優先順位]に、 0を入力します。

この例では、デバイス ID 0の優先値は低いので、優先順位は高くなります。従って、デバイス ID 0 （PA-3050-1）のファイアウォールのフローティングIPアドレス は10.1.1.100になります。

STEP 11 | PA-3050-1のままで、デバイスID 0に送信元NATルールを生成します。

1. **Policies (**ポリシー**)** > **NAT** の順に選択して **Add (**追加**)** をクリックします。
2. この例で デバイスID 0の送信元NATとなるルールに**Name**[名前]を入力します。
3. **NAT Type**[NAT タイプ] で **ipv4**（デフォルト）を選択します。
4. **Original Packet**[オリジナルパケット]の **Source Zone**[送信元ゾーン]で、 **Any**[いずれか]を選択します。
5. **Destination Zone**[宛先ゾーン]で、外部ネットワークに生成したゾーンを選択します。
6. **Destination Interface**[宛先インターフェイス]、 **Service**[サービス]、 **Source Address**[送信元アドレス]、および **Destination Address**[宛先アドレス]を **Any**[いずれか]に設定したままにします。
7. **Translated Packet**[変換済みパケット]の **Translation Type**[変換タイプ]で**Dynamic IP And Port** [動的 IP およびポート]を選択します。
8. もう **1** つの **Address Type** （アドレス タイプ） は Interface Address （インターフェイス アドレス） です。この場合、変換後アドレスはインターフェイスの IP アドレスにな

ります。フローティングIPアドレス10.1.1.100の**Interface**[インターフェイス]（この例ではeth1/1）と **IP Address**[IPアドレス]を選択します。

9. **Active/Active HA Binding (**アクティブ/アクティブ**HA**バインド**)** タブの **Active/Active HA Binding (**アクティブ/アクティブ**HA**バインド**)** で、 **0** を選択し、NAT ルールをデバイス ID 0にバインドします。
10. **OK** をクリックします。

STEP 12 | デバイスID 1に送信元NATルールを生成します。

1. **Policies (**ポリシー**)** > **NAT** の順に選択して **Add (**追加**)** をクリックします。
2. この例で デバイスID 1の送信元NATとなるポリシールールに**Name**[名前]を入力します。
3. **NAT Type**[NAT タイプ] で **ipv4**（デフォルト）を選択します。
4. **Original Packet**[オリジナルパケット]の **Source Zone**[送信元ゾーン]で、 **Any**[いずれか]を選択します。**Destination Zone**[宛先ゾーン]で、外部ネットワークに生成したゾーンを選択します。
5. **Destination Interface**[宛先インターフェイス]、 **Service**[サービス]、 **Source Address**[送信元アドレス]、および **Destination Address**[宛先アドレス]を **Any**[いずれか]に設定したままにします。
6. **Translated Packet**[変換済みパケット]の **Translation Type**[変換タイプ]で**Dynamic IP And Port** [動的 IP およびポート]を選択します。
7. もう **1** つの **Address Type** （アドレス タイプ） は Interface Address （インターフェイス アドレス） です。この場合、変換後アドレスはインターフェイスの IP アドレスになります。フローティングIPアドレス10.1.1.101の**Interface**[インターフェイス]（この例ではeth1/1）と **IP Address**[IPアドレス]を選択します。
8. **Active/Active HA Binding (**アクティブ/アクティブ **HA** バインド**)** タブの **Active/Active HA Binding (**アクティブ/アクティブ **HA** バインド**)** で **1** を選択し、NAT ルールをデバイス ID 1 にバインドします。
9. **OK** をクリックします。

STEP 13 | 設定を **Commit**（コミット）します。

「ユース ケース：個別送信元**NAT IP**アドレスプールをアクティブ/アクティブ**HA**ファイアウォールに設定する

ソース NAT in Active/Active HA Mode[アクティブ/アクティブHAモードのNAT]に IP アドレス プールを使用する場合は、各 firewall に独自のプールが必要であり、そのプールを NAT ルールの Device ID にバインドします。

アドレスオブジェクトとNATルールは同期しています（アクティブ/パッシブとアクティブ/アクティブの両方）。従って、HAペアのいずれか1つのファイアウォールで設定する必要があります。

この例ではIPアドレスプール10.1.1.140～10.1.1.150を持つアドレスオブジェクト名Dyn-IP-Pool-dev0を設定しています。この例ではIPアドレスプール10.1.1.160～10.1.1.170.を持つアドレスオブジェクト名Dyn-IP-Pool-dev1を設定しています。最初のアドレスオブジェクトはデバイスID0にバインドしています。第2アドレスオブジェクトはデバイスID1にバインドしています。

STEP 1 | HAファイアウォールで、アドレスオブジェクトを生成します。

1. **Objects (オブジェクト)** > **Addresses (アドレス)** の順に選択し、アドレス オブジェクトの **Name (名前)** を **Add (追加)** します（この例では Dyn-IP-Pool-dev0 ）。
2. **Type**[タイプ]で、 **IP Range**[IP範囲]を選択し、範囲 10.1.1.140～10.1.1.150を選択します。
3. **OK** をクリックします。
4. このステップを、 **IP Range**[IP範囲]10.1.1.160-10.1.1.170の別のアドレスオブジェクトDyn-IP-Pool-dev1でも繰り返します。

STEP 2 | デバイスID 0 に送信元NATルールを生成します。

1. **Policies (ポリシー)** > **NAT** を選択し、NATポリシールールに Src-NAT-dev0 などの **Name (名前)** を **Add (追加)** します。
2. **Original Packet**[オリジナルパケット]の **Source Zone**[送信元ゾーン]で、 **Any**[いずれか]を選択します。
3. For **Destination Zone**[宛先ゾーン]で、 Untrustのような送信元アドレスを変換したい宛先ゾーンを選択します。
4. **Translated Packet**[変換済みパケット]の **Translation Type**[変換タイプ]で、 **Dynamic IP and Port**[動的IPとポート]を選択します。
5. **Translated Address**[変換済みアドレス]で、デバイス ID 0 に属するアドレスプールに生成したアドレスオブジェクトを **Add**[追加]します。Dyn-IP-Pool-dev0.
6. **Active/Active HA Binding**[アクティブ/アクティブHAバインド] で **0** を選択して、NATルールをデバイスID 0にバインドします。
7. **OK** をクリックします。

STEP 3 | デバイスID 1に送信元NATルールを生成します。

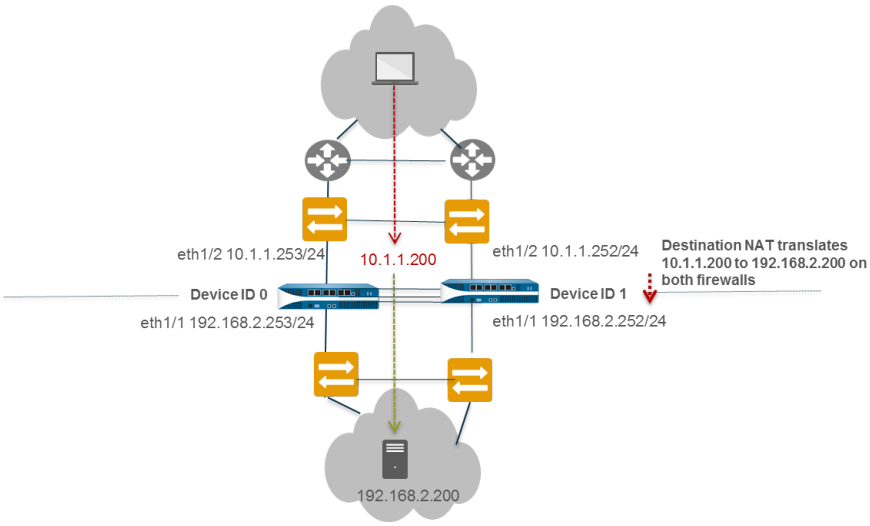
1. **Policies (ポリシー)** > **NAT** を選択し、NATポリシールールに Src-NAT-dev1 などの **Name (名前)** を **Add (追加)** します。
2. **Original Packet**[オリジナルパケット]の **Source Zone**[送信元ゾーン]で、 **Any**[いずれか]を選択します。
3. For **Destination Zone**[宛先ゾーン]で、 Untrustのような送信元アドレスを変換したい宛先ゾーンを選択します。
4. **Translated Packet**[変換済みパケット]の **Translation Type**[変換タイプ]で、 **Dynamic IP and Port**[動的IPとポート]を選択します。
5. **Translated Address**[変換済みアドレス]で、デバイス ID 1 に属するアドレスプールに生成したアドレスオブジェクトを **Add**[追加]します。Dyn-IP-Pool-dev1.
6. **Active/Active HA Binding**[アクティブ/アクティブHAバインド] で **1** を選択して、NATルールをデバイスID 1にバインドします。
7. **OK** をクリックします。

STEP 4 | 設定を **Commit**（コミット）します。

「ユース ケース：ARPロード共有を宛先NATでアクティブ/アクティブHAに設定する

このレイヤー 3 インターフェイスの例では、アクティブ/アクティブ HA モードの NAT および宛先 NAT を持つARP ロード シェアリング を使用します。両方のHAファイアウォールは、入口インターフェイスMACアドレスで宛先NATアドレスのARP要求に応答します。宛先NATはパブリック共有 IPアドレス （この例では 10.1.1.200）をサーバーのプライベートIPアドレス（この例では 192.168.2.200）に変換します。

HAファイアウォールが宛先 10.1.1.200の トラフィックを受信する場合、 両方のファイアウォールは、ネットワークの不安定化を招く恐れのあるARP要求に応答できます。リスクを避けるために、宛先NATルールをアクティブプライマリファイアウォールにバインドして、アクティブプライマリ状態のファイアウォールがARP要求に応答するよう設定します。



STEP 1 | PA-3050-2(Device ID 1)で、アクティブ/アクティブ HA の設定のステップ 1 ~ ステップ 3 を実行します。

STEP 2 | アクティブ/アクティブ HA の有効化

1. **Device (デバイス)** > **High Availability (高可用性)** > **General (全般)** にて、Setup (セットアップ) を編集します。
2. **Enable HA**（**HA** の有効化）を選択します。
3. 両方のファイアウォールで同じ**Group ID**を入力します。ファイアウォールは、Group ID を使用して仮想 MAC アドレスを計算します(範囲は 1 ~ 63)。
4. （任意）**Description (内容)** を入力します。
5. **Mode (モード)**は、**Active Active**を選択します。
6. **1**となるように、**Device ID**[デバイスID]を選択します。
7. **Enable Config Sync** （設定の同期化の有効化）を選択します。2つのファイアウォール設定を同期させる場合に、この設定が必要です（デフォルトで有効になっています）。
8. **Peer HA1 IP Address (ピアHA1のIPアドレス)**– ピアファイアウォールのHA1コントロールリンクスのIPアドレスを入力します。
9. （任意） **Backup Peer HA1 IP Address (バックアップピアHA1のIPアドレス)**– ピアファイアウォールのHA1バックアップリンクのIPアドレスを入力します。
10. **OK** をクリックします。

STEP 3 | ステップ 6 ~ ステップ 15 の でアクティブ/アクティブ HA の設定を実行します。

STEP 4 | HA仮想アドレスを設定します。

1. **Device (デバイス)** > **High Availability (高可用性)** > **Active/Active Config (アクティブ/アクティブ設定)** > **Virtual Address (仮想アドレス)** を選択して **Add (追加)** をクリックします。
2. **Interface** [インターフェイス] eth1/1を選択します。
3. **IPv4**を選択し、 **IPv4 Address (IPv4アドレス)** 10.1.1.200を**Add (追加)** します。
4. **Type (タイプ)** で、仮想IPアドレスを両方のピアがARP ロード共有のために使えるように **ARP Load Sharing (ARPロード共有)** を選択します。

STEP 5 | ARP ロード シェアリングを設定します。

デバイス選択アルゴリズムは、ARP要求に応答して、ロード共有を行うHAファイアウォールを決めます。

1. **Device Selection Algorithm**[デバイス選択アルゴリズム]で、 **IP Modulo**[IPモジュロ]を選択します。ARPリクエスト元IPアドレスのパリティに基づいて、ARPリクエストに応答するファイアウォールが選択されます。
2. **OK** をクリックします。

STEP 6 | PA-7000シリーズファイアウォール以外のファイアウォールでジャンボフレームを有効にします。

STEP 7 | フェイルオーバー条件の定義を行います。

STEP 8 | 設定を **Commit**（コミット）します。

STEP 9 | ピア firewall PA-3050-1 (Device ID 0) を、ステップ 2 で **Device ID 0** を選択する以外は同じ設定で設定します。

STEP 10 | PA-3050-1 （デバイス ID 0）のままで、宛先NATルールを生成し、アクティブプライマリファイアウォールがARP要求に応答できるようにします。

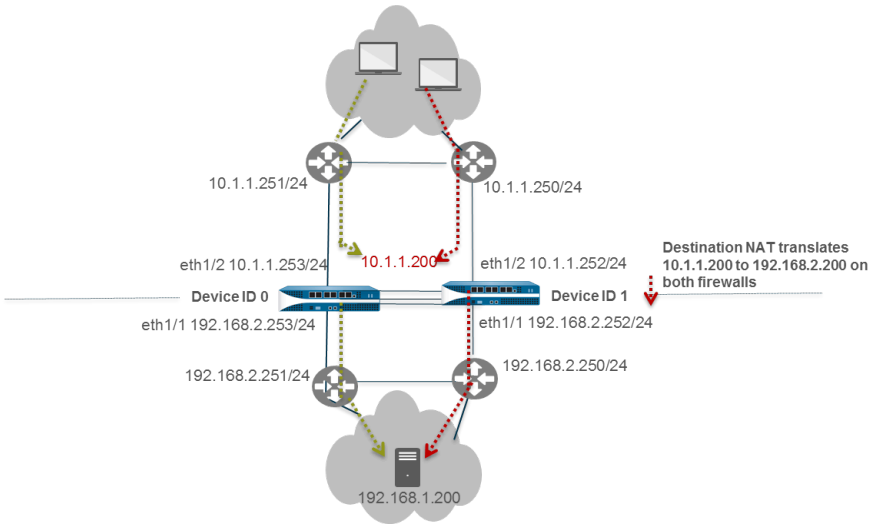
1. **Policies (ポリシー)** > **NAT** の順に選択して **Add (追加)** をクリックします。
2. この例でレイヤー2ARPの宛先NATとなるルールに**Name**[名前]を入力します。
3. **NAT Type**[NAT タイプ] で **ipv4**（デフォルト）を選択します。
4. **Original Packet**[オリジナルパケット]の **Source Zone**[送信元ゾーン]で、 **Any**[いずれか]を選択します。
5. **Destination Zone**[宛先ゾーン]で、外部ネットワークに生成したUntrustゾーンを選択します。
6. **Destination Interface**[宛先インターフェイス]、 **Service**[サービス]、および **Source Address**[送信元アドレス]を **Any**[いずれか]に設定したままにします。
7. **Destination Address**[宛先アドレス]で、 10.1.1.200を設定します。
8. **Translated Packet**[変換済みパケット]で、送信元アドレス変換は **None[**なし**]**のままにしておきます。
9. **Destination Address Translation**[宛先アドレス変換]で、宛先サーバーのプライベートIPアドレスを入力します。この例では 192.168.1.200です。
10. **Active/Active HA Binding (**アクティブ**/**アクティブ **HA** バインド**)** タブの **Active/Active HA Binding (**アクティブ**/**アクティブ **HA** バインド**)** で、**Primay (**プライマリ**)** を選択し、NAT ルールをアクティブプライマリ状態のファイアウォールにバインドします。
11. **OK** をクリックします。

STEP 11 | 設定を **Commit**（コミット）します。

「ユース ケース：**ARP**ロード共有をレイヤー**3**の宛先**NAT**でアクティブ**/**アクティブ**HA**に設定する

このレイヤー 3 インターフェイスの例では、アクティブ/アクティブ HA モードの NAT および ARP ロード シェアリング を使用します。PA-3050-1はデバイス ID 0を持ち、その HA ピアである PA-3050-2はデバイス ID 1を持ちます。

この使用例では、両方のHAファイアウォールは、宛先NATアドレスに関するARP要求に応答しなければなりません。トラフィックはuntrsutゾーンのいずれかのWANルーターからいずれかのファイアウォールに到達できます。宛先NATはパブリックフェイシング共有 IPアドレス をサーバーのプライベートIPアドレスに変換します。この設定では、1つの宛先NATアドレスをデバイスIDにバインドして、両方のファイアウォールがARP要求に応答できるようにする必要があります。



STEP 1 | PA-3050-2(Device ID 1)で、{31アクティブ/アクティブ HA33} の設定のステップ > ~ ステップ < を実行します。

STEP 2 | アクティブ/アクティブ HA の有効化

1. **Device (デバイス)** > **High Availability (高可用性)** > **General** （全般） > **Setup (セットアップ)** を選択して編集します。
2. **Enable HA**（**HA** の有効化）を選択します。
3. 両方のファイアウォールで同じ**Group ID**を入力します。ファイアウォールはグループIDを使って仮想MACアドレスを計算します（範囲は1～63）。
4. (オプション) 説明 を入力します。
5. **Mode (モード)**は、**Active Active**を選択します。
6. **1**となるように、**Device ID**[デバイスID]を選択します。
7. **Enable Config Sync** （設定の同期化の有効化）を選択します。2つのファイアウォール設定を同期させる場合に、この設定が必要です（デフォルトで有効になっています）。
8. **Peer HA1 IP Address (ピアHA1のIPアドレス)**– ピアファイアウォールのHA1コントロールリンクスのIPアドレスを入力します。
9. （任意） **Backup Peer HA1 IP Address (バックアップピアHA1のIPアドレス)**– ピアファイアウォールのHA1バックアップリンクのIPアドレスを入力します。
10. **OK** をクリックします。

STEP 3 | アクティブ/アクティブ HA の設定を行います。

ステップ 6 からステップ 15 を実行します。

STEP 4 | HA仮想アドレスを設定します。

1. **Device (デバイス)** > **High Availability (高可用性)** > **Active/Active Config (アクティブ/アクティブ設定)** > **Virtual Address (仮想アドレス)** を選択して **Add (追加)** をクリックします。
2. **Interface** [インターフェイス] eth1/1を選択します。
3. **IPv4**を選択し、 **IPv4 Address (IPv4**アドレス) 10.1.1.200を**Add (追加)** します。
4. **Type (タイプ)** で、仮想IPアドレスを両方のピアがARP ロード共有のために使えるように **ARP Load Sharing (ARP**ロード共有) を選択します。

STEP 5 | ARP ロード シェアリングを設定します。

デバイス選択アルゴリズムは、ARP要求に応答して、ロード共有を行うHAファイアウォールを決めます。

1. **Device Selection Algorithm**[デバイス選択アルゴリズム]で、以下のいずれかを選択します。
   - **IP Modulo (IP**モジュロ) — ARPリクエスト元IPアドレスのパリティに基づいて、ARPリクエストに応答するファイアウォールが選択されます。
   - **IP Hash**[IPハッシュ] — ARPリクエスト元IPアドレスと宛先IPアドレスのハッシュに基づいて、ARPリクエストに応答するファイアウォールが選択されます。
2. **OK** をクリックします。

STEP 6 | PA-7000シリーズファイアウォール以外のファイアウォールでジャンボフレームを有効にします。

STEP 7 | フェイルオーバー条件の定義を行います。

STEP 8 | 設定を **Commit**（コミット）します。

STEP 9 | ピア ファイアウォール PA-3050-1（デバイス ID 0）を、**Device ID (デバイス ID)** を **1** でなく **0** に設定する以外は同じように設定します。

STEP 10 | PA-3050-1 （デバイスID 0）で、デバイスID0とデバイスID1の両方に宛先NATルールを生成します。

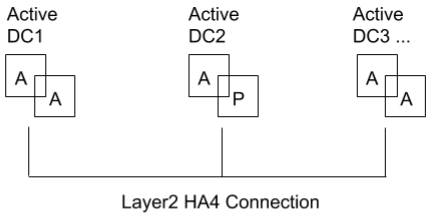
1. **Policies (ポリシー)** > **NAT** の順に選択して **Add (追加)** をクリックします。
2. この例でレイヤー3ARPの宛先NATとなるルールに**Name**[名前]を入力します。
3. **NAT Type**[NAT タイプ] で **ipv4**（デフォルト）を選択します。
4. **Original Packet**[オリジナルパケット]の **Source Zone**[送信元ゾーン]で、 **Any**[いずれか]を選択します。
5. **Destination Zone**[宛先ゾーン]で、外部ネットワークに生成したUntrustゾーンを選択します。
6. **Destination Interface**[宛先インターフェイス]、 **Service**[サービス]、および **Source Address**[送信元アドレス]を **Any**[いずれか]に設定したままにします。
7. **Destination Address**[宛先アドレス]で、 10.1.1.200を設定します。
8. **Translated Packet**[変換済みパケット]で、送信元アドレス変換は None[なし]のままにしておきます。
9. **Destination Address Translation**[宛先アドレス変換]で、宛先サーバーのプライベートIPアドレスを入力します。この例では 192.168.1.200です。
10. **Active/Active HA Binding (アクティブ/アクティブHAバインド)** タブの **Active/Active HA Binding (アクティブ/アクティブHAバインド)**で、**both (両方)** を選択し、NAT ルールをデバイス ID 0とデバイスID1の両方にバインドします。
11. **OK** をクリックします。

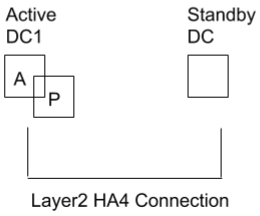
STEP 11 | 設定を **Commit**（コミット）します。

HA クラスタリングの概要

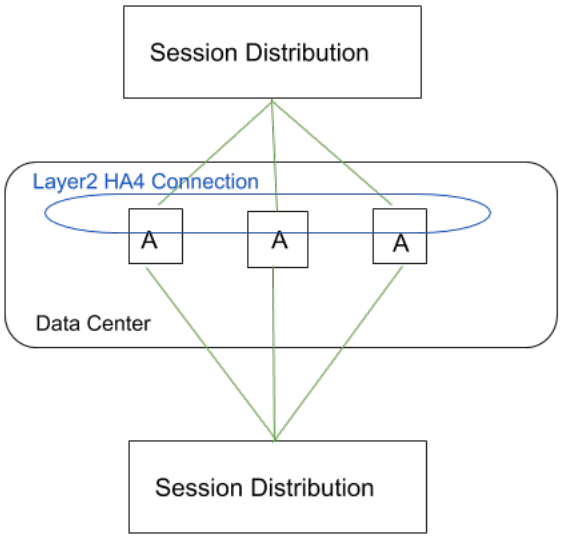
現在では、多くのPalo Alto Networks® ファイアウォール モデルが、最大16のファイアウォールのhigh availability (高可用性 - HA)クラスタ内のファイアウォール間のセッション状態の同期をサポートしています。HA クラスタ ピアはセッションを同期して、データセンターの障害や水平方向に拡張されたファイアウォールを備えた大規模なセキュリティ検査ポイントから保護します。ネットワークが停止したりファイアウォールがダウンしたりした場合、セッションはクラスタ内の別のファイアウォールにフェイルオーバーします。このような同期は、以下のユースケースで特に有用です。

1つ目のユースケースは、HAピアが複数のデータセンターに分散しているため、データセンター内またはデータセンター間に単一障害点がない場合です。2つ目のユースケースはマルチ データセンターで、一方のデータセンターがアクティブであり、もう一方がスタンバイ状態の場合です。





3つ目の HA クラスタリングのユースケースは水平スケーリングです。このユースケースでは、HA クラスタ メンバーを単一のデータセンターに追加して、セキュリティをスケーリングし、セッションの存続可能性を確保します。



HA クラスタはレイヤー3またはバーチャル ワイヤ デプロイメントをサポートします。クラスタ内の HAピアは、HAペアとスタンドアロン クラスタ メンバーの組み合わせにすることができます。HA クラスタでは、すべてのメンバーがアクティブであると見なされます。パッシブ ファイアウォールの概念は、HA クラスタに追加した後もアクティブ/パッシブの関係を維持できるHAペアを除いてありません。

すべてのクラスタ メンバーはセッション状態を共有します。新しいファイアウォールが HA クラスタに加入すると、クラスタ内のすべてのファイアウォールがトリガされ、既存のすべてのセッションが同期されます。HA4および HA4バックアップ接続は、同じクラスタ ID を持つすべてのクラスタ メンバー間でセッション状態を同期する専用のクラスター リンクです。クラスタ メンバー間の HA4リンクは、クラスタ メンバー間の接続障害を検出します。HA1 (コントロール リンク)、HA2 (データ リンク)、およびHA3 (パケット転送リンク) は、HAペアではないクラスタ メンバー間ではサポートされていません。

フェイルオーバーされていない通常のセッションの場合、セッション オーナーであるファイアウォールのみがトラフィック ログを作成します。フェイルオーバーしたセッションの場合、新しいセッション オーナー (フェイルオーバーされたトラフィックを受信するファイアウォール) がトラフィック ログを作成します。

HA クラスタリングをサポートするファイアウォール モデルと、クラスタごとにサポートされるメンバーの最大数は次のとおりです:

Firewall Model（ファイアウォール モデル）	クラスタごとにサポートされるメンバーの数
PA-3200シリーズ	6
PA-3400シリーズ	6

Firewall Model（ファイアウォール モデル）	クラスタごとにサポートされるメンバーの数
PA-5200シリーズ	16
PA-5400シリーズ	8
以下のカードを少なくとも1つ有する PA-7000 シリーズ ファイアウォール: PA-7000-100G-NPC、PA-7000-20GQXM-NPC、PA-7000-20GXM-NPC	PA-7080:4 PA-7050:6
VM-300	6
VM-500	6
VM-700	16

パブリック クラウドの展開では、HA クラスタリングはサポートされていません。HA クラスタリングの設定を始める前に、HA クラスタリングのベストプラクティスとプロビジョニングを検討してください。

HA クラスタリングのベストプラクティスとプロビジョニング

以下で紹介するのは、HA クラスタリングのプロビジョニング要件とベストプラクティスです。

- プロビジョニングの要件とベストプラクティス
  - HA クラスター メンバーは同じ firewall モデルで、同じ PAN-OS を実行している必要があります。®version.

    アップグレード時に、*firewall* メンバーは別のバージョンの *1* つのメンバーとセッションを同期し続けます。
  - Panorama を使用して HA クラスタ メンバーをプロビジョニングし、すべてのクラスタ メンバー間ですべての設定とポリシーの同期を維持することが推奨され、ベストプラクティスとなります。
  - ポリシー施行とコンテンツ検査機能を一貫するには、HA クラスタ メンバーに同じコンポーネントのライセンスを付与する必要があります。
  - ライセンスの不一致や機能の喪失を防ぐために、複数のライセンスが同時に期限切れになるようにしてください。
  - 一貫性のあるセキュリティを構築するには、すべてのクラスタ メンバーが同じバージョンの動的コンテンツ更新で実行されている必要があります。
  - HA クラスター・メンバーは、セッションが別のクラスター・メンバーに正常にフェイルオーバーするために、同じゾーン名を共有する必要があります。たとえば、リンクがダウンしているために「**internal**」という名前の入口ゾーンに向かうセッションがドロップされたとします。これらのセッションがクラスター内の HA firewall ピアにフェイルオーバーするには、そのピアに **internal** という名前のゾーンも必要です。
  - Client-to-server フローと server-to-client フローは、セキュリティ コンテンツ スキャンを実行するために、通常の (障害が発生していない) 条件下で同じ firewall に戻る必要があります。非対称トラフィックはドロップされませんが、セキュリティ上の目的でスキャンすることはできません。
- セッション同期のベストプラクティス
  - 専用の HA 通信インターフェイスは、データプレーン インターフェイス上で使用する必要があります。HSCI インターフェースは HA4 には使用されません。これにより、HA ペアとクラスター・セッション同期を分離して、セッション同期の帯域幅と信頼性を最大限に高めることができます。
  - HA4 は、データプレーン・インターフェースを使用する場合は、適切なサイズにする必要があります。これにより、クラスター・メンバー間でのベスト・エフォート・セッション状態の同期が保証されます。
  - HA4 通信リンク専用のクラスタ ネットワークを用意して、クラスタ メンバー間の適切な帯域幅と混雑のない低レイテンシ接続を確保することがベストプラクティスです。
  - ネットワークを設計し、トラフィック・エンジニアリングを実行して、firewall 間でセッションが正常に同期される前に、ネットワークがセッション所有者からクラスター・メ

ンバーにトラフィックを誘導する競合状態の可能性を回避します。レイヤー2 HA4接続には、HA メンバー間のタイムリーな同期を可能にするために、十分な帯域幅と低レイテンシが必要です。HA4 レイテンシは、ピアリング デバイスがクラスタ メンバー間でトラフィックを切り替えるときに発生するレイテンシよりも短くする必要があります。

  - 非対称フローを最小限に抑えるようにネットワークを設計します。セッション・セットアップでは、完全な TCP 3 方向ハンドシェークを表示するには、1 つのクラスター・メンバーが必要です。
- ヘルスチェックのベストプラクティス
  - クラスタ内の HA ペアでは、HA1、HA2、および HA4 の HA バックアップ通信リンクを使用して Active/Passive ペアを構成します。HA1、HA2、HA3、および HA4 の HA バックアップ通信リンクを使用してアクティブ/アクティブ・ペアを構成します。
  - すべてのクラスター メンバーに HA4 バックアップ リンクを構成します。

HA クラスタリングの設定

HA クラスタリング について学習し、HA クラスタリングのベストプラクティスとプロビジョニングに従って HA firewall をクラスターのメンバーとして構成します。

STEP 1 | インターフェースを HA インターフェースとして確立します (後ほど HA4 リンクとして割り当てるため)。

1. **Network (ネットワーク)** > **Interfaces (インターフェース)** > **Ethernet (イーサネット)** を選択し、さらにインターフェースを選択します (例「ethernet1/1」)。
2. **HA** 対象の **Interface Type (インターフェース タイプ)** を選択します。
3. **OK** をクリックします。
4. このステップを繰り返し、別のインターフェースを HA4 バックアップ リンクとして使用するように設定します。

STEP 2 | HA クラスタリングを有効化します。

1. **Device**（デバイス） > **High Availability**（高可用性） > **General**（全般）を選択し、Clustering Settings（クラスタリング設定）を編集します。
2. **Enable Cluster Participation (クラスター参加の有効化)** を行います。
3. **Cluster ID (クラスター ID)** を入力します。これはすべてのメンバーがセッション状態を共有できる HA クラスターの一意の数値 ID で、範囲は1～99です。
4. 簡潔で有益な **Cluster Description (クラスターの説明)** を入力します。
5. (オプション) **Cluster Synchronization Timeout (min) (クラスター同期タイムアウト) (分)**を変更します。これは、別のクラスター メンバーが (不明な状態で) クラスターの完全な同期を妨げている場合に、ローカル ファイアウォールがアクティブ状態になるまで待機する最大分数です。範囲は0～30で、デフォルトは0に設定されています。
6. (オプション) **Monitor Fail Hold Down Time (min) (モニター障害時ホールド ダウン タイム) (分)** を変更します。これは、ダウン リンクがバックアップされているかどうかを確認するために再テストされるまでの分数です。範囲は1～60で、デフォルトは1に設定されています。
7. **OK** をクリックします。

STEP 3 | HA4 リンクを設定します。

1. **HA Communications (HA 通信)** を選択し、Clustering Links (クラスタリングのリンク) セクションで、 HA4 セクションを編集します。
2. 最初のステップで設定したインターフェースを **HA** インターフェースとして選択し、HA4 リンクの **Port (ポート)** にします (例「ethernet1/1」)です。
3. ローカルHA4インターフェースの**IPv4/IPv6 Address (IPv4/IPv6** アドレス**)** を入力します。
4. **Netmask**（ネットマスク）を入力します。
5. (オプション) **HA4 Keep-alive (HA4** キープアライブ**) Threshold (ms) (しきい値) (ミリ秒)** を変更して、クラスター メンバーが機能していることを知るために、ファイアウォー

ルがクラスター メンバーからキープアライブを受信する必要がある時間枠を指定します。範囲は5,000～60,000であり、デフォルトは10,000に設定されています。

6. **OK** をクリックします。

STEP 4 | HA4 バックアップ リンクを設定します。

1. HA4 バックアップ セクションを編集します。
2. 最初のステップで設定したもう一つのインターフェースを **HA** インターフェースとして選択し、HA4 バックアップリンクの **Port (ポート)** にします。
3. ローカル HA4 バックアップ インターフェースの**IPv4/IPv6 Address (IPv4/IPv6** アドレス**)** を入力します。
4. **Netmask**（ネットマスク）を入力します。
5. **OK** をクリックします。

STEP 5 | ローカル メンバーと任意の HAペアの両方の HAピアを含む、HA クラスターのすべてのメンバーを指定します。

1. **Cluster Config (**クラスター設定**)** を選択します。
2. (サポートされているファイアウォール上) ピア メンバーの **Device Serial Number (**デバイスのシリアルナンバー**)** を**Add (**追加**)** します。
3. (Panorama 上) ドロップダウンリストから **Device (**デバイス**)** を**Add (**追加**)** して選択し、**Device Name (**デバイス名**)** を入力します。
4. クラスター内の HAピアの **HA4 IP Address (HA4 IP**アドレス**)** を入力します。
5. クラスタ内の HAピアの **HA4 Backup IP Address (HA4** バックアップ **IP**アドレス**)** を入力します。
6. 識別したピアで **Session Synchronization** を有効にします。
7. （任意）有益な**Description (**説明**)** を入力します。
8. **OK** をクリックします。
9. デバイスを選択して、**Enable (**有効化**)** します。

STEP 6 | リンクとパス モニタリングを使用して、Define HA failover conditions (HA フェイルオーバー条件を定義) します。

STEP 7 | **Commit (**コミット**)** します。

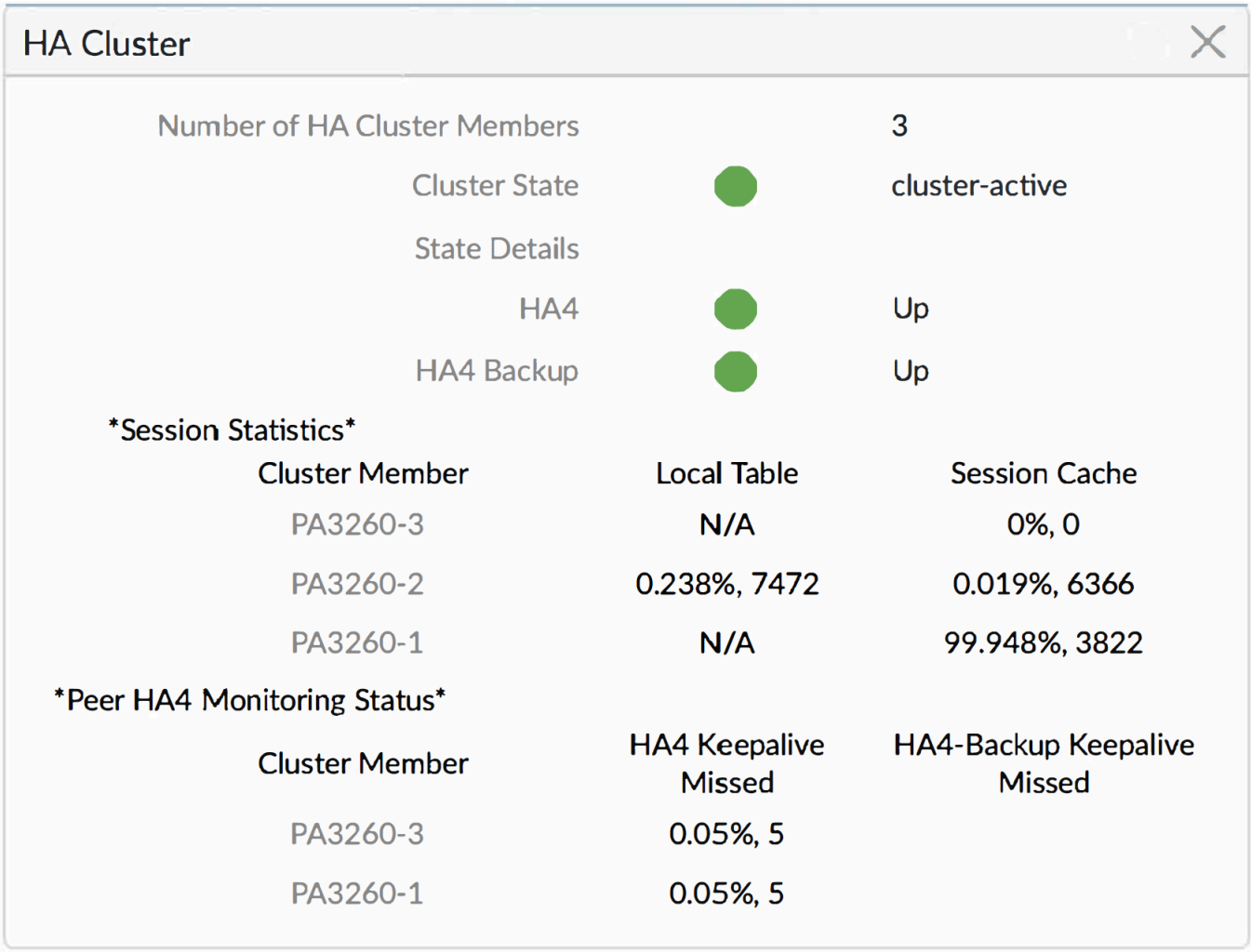
STEP 8 | (Panorama 専用) HA クラスター内の HA ファイアウォールのリストを更新します。

1. テンプレートで、**Device (**デバイス**)** > **High Availability (**高可用性**)** > **Cluster Config (**クラスター設定**)** を選択します。
2. 画面下部の**Refresh (**更新**)** をクリックします。

STEP 9 | UI 内の HA クラスター情報を表示します。

1. [**Dashboard(**ダッシュボード**)]**を選択します。
2. HA クラスター フィールドを表示します。上部のセクションには、クラスターの状態と HA4 接続が表示され、クラスターの状態が一目でわかります。HA4 および HA4 バックアップ インジケータは、以下のいずれかの色になります:緑色は、クラスター メン

バーのリンク ステータスが Up であることを示します。赤色は、すべてのクラスター メンバーのリンク ステータスが Down であることを示します。黄色は、一部のクラスター メンバーのリンク ステータスが Up で、他のクラスター メンバーのステータスが Down であることを示します。灰色は未設定を示します。中央のセクションには、ローカル セッションテーブルとセッション キャッシュ テーブルの容量が表示されるため、テーブルの容量を監視し、ファイアウォールのアップグレードを計画できます。下のセクションには、HA4 および HA4 バックアップ リンクの通信エラーが表示され、メンバー間の情報の同期で発生する可能性のある問題を示しています。



STEP 10 | CLI にアクセスして、HAクラスターとHA4 リンク情報を表示し、他の HA クラスタリング タスクを実行します。

HA クラスター フラップ統計情報を表示できます。*HA* デバイスがサスペンドから機能に移行し、その逆に移行すると、クラスタ のフラップ カウントがリセットされます。非機能保持時間が経過すると、クラスターのフラップ カウントもリセットされます。

HA1 SSH 鍵の更新およびキーのオプションの設定

すべての Palo Alto Networks ファイアウォールには、事前に設定されたSecure Shell (セキュアシェル - SSH) が付属しており、高可用性 (HA) ファイアウォールは、 SSH サーバーと SSH クライアントとして同時に機能することができます。アクティブ/パッシブ またはアクティブ/アクティブ HA を設定する際、HA ファイアウォール間の HA1 (コントロール リンク) 接続に対して暗号化を有効にできます。特にファイアウォールが同じサイトにない場合は、HAピア間の HA1 トラフィックを暗号化して保護することを推奨します。HA1 コントロール リンクで暗号化を有効にした後、以下の CLI を使用して、SSH サービスプロファイルを作成し、HA ファイアウォール間の接続を保護します。

SSH サービス プロファイルにより、デフォルトのホスト鍵タイプを変更したり、HA1 コントロール リンク用の新しい公開および秘密 SSH ホスト鍵のペアを生成したり、その他の SSH HA1 設定を設定したりできます。HAピアを再起動せずに、新しいホスト キーと設定済みの設定をファイアウォールに適用できます。ファイアウォールは、ピアとの HA1セッションを再確立して、設定の変更を同期します。また、HA1および HA1バックアップ セッションを再確立するためのシステム ログ (サブタイプは ha) も生成します。

以下の例は、暗号化を有効にして CLI にアクセスした後、HA1に対するさまざまなSSH設定を構成する方法を示しています。(SSH 管理サーバ プロファイルの例については、 SSH キーの更新と管理インターフェース接続のキーオプションの設定を参照してください。)

以下のタスクを実行する前に、暗号化を有効にする必要があり、暗号化が *HA*ペアで適切に機能している必要があります。

FIPS-CC モードで *HA1* コントロール リンクを設定している場合は、セッション鍵の自動キー再生成パラメータを設定する必要があります。

Collector Group (コレクタ グループ)内の各専用のログ コレクタ (ログ コレクタ モードの *M-series* または *Panorama* バーチャル アプライアンス) に対して同じ *SSH* 接続設定を使用するには、*Panorama*管理サーバから *SSH* サービス プロファイルを設定し、変更を *Panorama* に**Commit** (コミット) してから、設定をログ コレクターに **Push** (プッシュ) します。**`set log-collector-group <name> general-set management ssh`** コマンドを使用できます。

SSH サービス プロファイルを作成して、HA ファイアウォール間の SSH 接続をより細かく制御します。

この例では、設定を行わずに HA プロファイルを作成します。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles *<name>***
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. 新しいプロファイルが作成されたことを確認し、既存のプロファイルの設定を表示するには、次の手順に従います:

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles**

(任意) HA1 セッションに指定された暗号化暗号のみを使用するように SSH サーバを設定します。

デフォルトでは、HA1 SSH は、CLI HA セッションの暗号化に、サポートされているすべての暗号を許可します。1 つ以上の暗号を設定すると、SSH サーバーは接続中にそれらの暗号

のみをアドバタイズし、SSH クライアント (HAピア) が別の暗号を使用して接続を試みると、サーバーは接続を終了します。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ciphers ha-profiles <*name*> ciphers <*cipher*>**

   aes128-cbc—暗号ブロックチェーンを使用する AES 128 ビット暗号

   aes128-ctr—Counter Mode を使用する AES 128 ビット暗号

   aes128-gcm—GCM を使用する AES 128 ビット暗号 (Galois/Counter Mode)

   aes192-cbc—暗号ブロックチェーンを使用する AES 192 ビット暗号

   aes192-ctr—Counter Mode を使用する AES 192 ビット暗号

   aes256-cbc—暗号ブロックチェーンを使用する AES 256 ビット暗号

   aes256-ctr—Counter Mode を使用する AES 256 ビット暗号

   aes256-gcm—GCM を使用する AES 256 ビット暗号
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. (HA1 バックアップが設定されている) admin@PA-3250> **request high-availability session-reestablish**
6. (HA1 バックアップが設定されていないか、または HA1 バックアップリンクがダウンしている) admin@PA-3250> **request high-availability session-reestablish force**

   HA1 バックアップがない場合、ファイアウォールに *HA1* セッションの再確立を強制することで、*HA* ピア間に短いスプリットブレイン状態が発生する可能性があります。*(HA1* バックアップが設定されているときに ***force*** *(*強制*)* オプションを使用しても効果はありません。*)*
7. 暗号が更新されたことを確認する方法:

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles ciphers**

(任意) デフォルトのホスト鍵タイプを設定します。

HA1 制御リンクで暗号化を有効にした場合、変更しない限り、ファイアウォールはデフォルトのホスト鍵タイプの RSA 2048 を使用します。HA1 SSH 接続は、デフォルトのホスト鍵タイプのみを使用して HA ピアを認証します (暗号化セッションが確立される前)。デフォルトのホスト鍵タイプを変更できます。選択肢は、ECDSA 256、384、521、RSA 2048、3072、4096 です。RSA 鍵の長さをもっと長くしたい場合、または RSA よりも ECDSA を使用したい場合は、デフォルトのホスト鍵タイプを変更してください。この例で

は、デフォルトのホスト鍵タイプを 256 ビットの ECDSA 鍵に設定します。また、HA ピアを再起動せずに、新しいホスト鍵を使用して HA1 接続を再確立します。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> default-hostkey key-type ECDSA key-length 256**
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. admin@PA-3250> **request high-availability sync-to-remote ssh-key**

   HA 接続は *HA* ファイアウォール間ですでに確立されていなければなりません。ファイアウォールがまだ *HA* 接続を確立していない場合は、コントロールリンク接続で暗号化を有効にし、*HA* キーをネットワーク上の場所にエクスポートして、その *HA* キーをピアにインポートする必要があります。アクティブ/パッシブ HA の設定またはアクティブ/アクティブ HA の設定を参照してください。
6. (HA1 バックアップが設定されている) admin@PA-3250> **request high-availability session-reestablish**
7. (HA1 バックアップが設定されていないか、または HA1 バックアップリンクがダウンしている) admin@PA-3250> **request high-availability session-reestablish force**

   HA1 バックアップがない場合は、ファイアウォールに *HA1* セッションを再確立させることができます。これにより、*2* つの *HA* ピア間でスプリットブレイン状態が短時間発生します。*(HA1* バックアップが設定されているときに ***force*** *(*強制*)* オプションを使用しても効果はありません。*)*
8. ホストキーが更新されたことを確認する手順:

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles <*name*> default-hostkey**

(任意) HA1 制御リンクを介して SSH 用に選択した暗号のセットから暗号を削除します。

この例では、128 ビットキーを持つ AES CBC 暗号を削除します。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **delete deviceconfig system ssh profiles ha-profiles <*name*> ciphers aes128-cbc**
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. (HA1 バックアップが設定されている) admin@PA-3250> **request high-availability session-reestablish**
6. (HA1 バックアップが設定されていないか、または HA1 バックアップリンクがダウンしている) admin@PA-3250> **request high-availability session-reestablish force**

   HA1 バックアップがない場合は、ファイアウォールに *HA1* セッションを再確立させることができます。これにより、*2* つの *HA* ピア間でスプリットブレイン状態が短時間発生します。*(HA1* バックアップが設定されているときに ***force (***強制***)*** オプションを使用しても効果はありません。
7. 暗号が削除されたことを検証する手順:

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles <*name*> ciphers**

(任意) HA1 SSH サーバーがサポートする、セッション鍵交換アルゴリズムを設定します。

デフォルトでは、SSH サーバー (HA ファイアウォール) はすべての鍵交換アルゴリズムを SSH クライアント (HA ピアファイアウォール) にアドバタイズします。

ECDSA のデフォルトの鍵タイプを使用している場合は、*ECDH* 鍵アルゴリズムを使用することを推奨します。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> kex <*value*>**

   diffie-hellman-group14-sha1—SHA1 ハッシュを使用する Diffie-Hellman グループ 14

   ecdh-sha2-nistp256—SHA2-256 ハッシュを使用する、米国標準技術局 (NIST) P-256 に対する楕円曲線 Diffie-Hellman

   ecdh-sha2-nistp384—SHA2-384 ハッシュを利用する、NIST P-384 に対する楕円曲線 Diffie-Hellman

   ecdh-sha2-nistp521—SHA2-521 ハッシュを利用する、NIST P-521 に対する楕円曲線 Diffie-Hellman
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. (HA1 バックアップが設定されている) admin@PA-3250> **request high-availability session-reestablish**
6. (HA1 バックアップが設定されていないか、または HA1 バックアップリンクがダウンしている) admin@PA-3250> **request high-availability session-reestablish force**

   HA1 バックアップがない場合は、ファイアウォールに *HA1* セッションを再確立させることができます。これにより、*2* つの *HA* ピア間でスプリットブレイン状態が短時間発生します。*(HA1* バックアップが設定されているときに ***force*** *(*強制*)* オプションを使用しても効果はありません。
7. 鍵交換アルゴリズムが更新されたことを確認する方法:

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles**

(任意) HA1 SSH サーバーがサポートするメッセージ認証コード (MAC) を設定します。

デフォルトでは、サーバーはすべての MAC アルゴリズムをクライアントにアドバタイズします。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> mac <*value*>**

   hmac-sha1—SHA1 暗号ハッシュを使用する MAC

   hmac-sha2-256—SHA2-256 暗号ハッシュを使用する MAC

   hmac-sha2-512—SHA2-512 暗号ハッシュを使用する MAC
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. (HA1 バックアップが設定されている) admin@PA-3250> **request high-availability session-reestablish**
6. (HA1 バックアップが設定されていないか、または HA1 バックアップリンクがダウンしている) admin@PA-3250> **request high-availability session-reestablish force**

   HA1 バックアップがない場合は、ファイアウォールに *HA1* セッションを再確立させることができます。これにより、*2* つの *HA* ピア間でスプリットブレイン状態が短時間発生します。*(HA1* バックアップが設定されているときに ***force (***強制***)*** オプションを使用しても効果はありません*)*。
7. MAC アルゴリズムが更新されたことを確認する方法:

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles**

(任意) 既存の鍵を置き換えるために HA1 SSH 用の ECDSA または RSA ホスト鍵を再生成し、HA ピアを再起動せずに新しい鍵を使用して、HAピア間で HA1 セッションを再確立します。

HA ピアは、ホスト鍵を使用して互いに認証します。この例では、ECDSA 256 デフォルトホスト鍵を再生成します。

ホスト鍵を再生成しても、デフォルトのホスト鍵タイプは変更されません。使用しているデフォルトのホスト鍵を再生成するには、再生成時にデフォルトのホスト鍵のタイプと長さを指定しなければなりません。デフォルトのホスト鍵タイプではないホスト鍵を再生成しても、使用していない鍵が再生成されるだけなので効果はありません。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh regenerate-hostkeys ha key-type ECDSA key-length 256**
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. admin@PA-3250> **request high-availability sync-to-remote ssh-key**

   HA 接続は *HA* ファイアウォール間ですでに確立されていなければなりません。ファイアウォールがまだ *HA* 接続を確立していない場合は、コントロールリンク接続で暗号化を有効にし、*HA* キーをネットワーク上の場所にエクスポートして、その *HA* 鍵をピアにインポートする必要があります。アクティブ/パッシブ HA の設定またはアクティブ/アクティブ HA の設定を参照してください。
6. (HA1 バックアップが設定されている) admin@PA-3250> **request high-availability session-reestablish**
7. (HA1 バックアップが設定されていないか、または HA1 バックアップリンクがダウンしている) admin@PA-3250> **request high-availability session-reestablish force**

   HA1 バックアップがない場合は、ファイアウォールに *HA1* セッションを再確立させることができます。これにより、*2* つの *HA* ピア間でスプリットブレイン状態が短時間発生します。*(HA1* バックアップが設定されているときに ***force*** *(*強制*)* オプションを使用しても効果はありません。*)*

(任意) 鍵更新パラメータを設定して、HA1 コントロール リンク上の SSH に対してセッション鍵の自動キー再生成がいつ発生するかを設定します。

セッション鍵は、HAピア間のトラフィックを暗号化するために使用します。設定できるパラメータは、データ量 (Megabyte (メガバイト - MB))、時間間隔 (秒)、およびパケット数です。いずれかのキーの再生成パラメータが設定された値に達すると、SSH は鍵交換を開始します。

設定した 1番目のパラメータが、すぐにキーの再生成が発生する値に達することが確実でない場合は、2 番目または 3 番目のパラメータを設定できます。最初のパラメータが設定され

た値に到達すると、キーの再生成を促し、次にファイアウォールはすべてのキーの再生成パラメータをリセットします。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey data 32**

   キーの再生成は、前回のキーの再生成の後に送信されたデータ量 (Megabyte (メガバイト - MB)) の後に行われます。デフォルトは、使用する暗号に基づいており、範囲は 1GB から 4GB です。（範囲は 10MB ～ 4,000MB です）。あるいは、**set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey data default** コマンドを入力して、data パラメーターを、使用している個々の暗号のデフォルト値に設定することもできます。
3. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey interval 3600**

   鍵の再作成は、前回の鍵再作成の後に指定された時間間隔 (秒数) が経過した後に行われます。デフォルトでは、時間ベースのキー再生成は無効になっています (none に設定されています)。範囲は 10～3,600 です。
4. admin@PA-3250# **set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey packets 27**

   キーの再生成は、前回のキーの再生成に続いて、定義された数のパケット (2^n) が送信された後に行われます。たとえば、14 は、キー再生成が行われる前に最大 2^{14} パケットが送信されるように設定します。デフォルトは 2^{28} です。範囲は 12 ～ 27 (2^{12} ～ 2^{27}) です。あるいは、**set deviceconfig system ssh profiles ha-profiles <*name*> session-rekey packets default** と入力して、packets パラメータを 2^{28} に設定することもできます。

   トラフィックの種類とネットワーク速度に基づいて鍵の再設定パラメータを選択します (必要に応じて *FIPS-CC* の要件に加えます)。*SSH* のパフォーマンスに影響を与えるほどパラメータを低く設定しないでください。
5. admin@PA-3250# **commit**
6. admin@PA-3250# **exit**
7. (HA1 バックアップが設定されている) admin@PA-3250> **request high-availability session-reestablish**
8. (HA1 バックアップが設定されていないか、または HA1 バックアップリンクがダウンしている) admin@PA-3250> **request high-availability session-reestablish force**

   HA1 バックアップがない場合は、ファイアウォールに *HA1* セッションを再確立させることができます。これにより、*2* つの *HA* ピア間でスプリットブレイン状態が短時間発生します。*(HA1* バックアップが設定されているときに ***force*** *(*強制*)* オプションを使用しても効果はありません。*)*

9. 変更を確認する方法:

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh profiles ha-profiles <*name*> session-rekey**

プロファイルを選択して HA1 SSH サービスを再起動することにより、プロファイルを有効化します。

1. admin@PA-3250> **configure**
2. admin@PA-3250# **set deviceconfig system ssh ha ha-profile <*name*>**
3. admin@PA-3250# **commit**
4. admin@PA-3250# **exit**
5. admin@PA-3250> **set ssh service-restart ha**
6. 正しいプロファイルが使用されていることを確認する方法:

   admin@PA-3250> **configure**

   admin@PA-3250# **show deviceconfig system ssh ha**

HA ファイアウォールの状態

HAファイアウォールは以下の状態のいずれかになります。

説明における	HA ファイアウォール	説明
初期	A/P または A/A	デバイスが HA ペアに結合したときの一時的な状態。ファイアウォールはブートアップ後、ピアを検出し、ネゴシエーションが開始するまでこの状態にとどまります。HA ネゴシエーションが開始されていない場合、タイムアウト後にデバイスはアクティブになります。
アクティブ	A/P	アクティブ/パッシブ設定での有効なファイアウォールの状態
パッシブ	A/P	アクティブ/パッシブ設定でのパッシブファイアウォールの状態パッシブファイアウォールはネットワークを障害することなく、いつでもアクティブファイアウォールになれます。パッシブファイアウォールは他のトラフィックを処理しませんが、 • パッシブリンク状態autoが設定されている場合、パッシブファイアウォールはルーティングプロトコルを実行し、リンクとパス状態をモニターします。LACPとLLDPプレネゴシエーションを設定するとパッシブファイアウォールはそれぞれ LACP と LLDPをプレネゴシエートします。 • パッシブファイアウォールはフロー状態、ランタイムオブジェクトおよび設定を同期します。 • パッシブファイアウォールはhelloプロトコルを使ってアクティブファイアウォールの状態をモニターします。
アクティブ プライマリ	A/A	アクティブ/アクティブ設定では、User-ID エージェントに接続したファイアウォールの状態は DHCPサーバーと DHCPリレーを実行し、 NATと PBFルールをアクティブプライマリファイアウォールのデバイス IDに一致させます。この状態のファイアウォールは、セッションを所有し、セットアップできます。
アクティブ セカンダリ	A/A	アクティブ/アクティブ設定では、User-ID エージェントに接続したファイアウォールの状態は DHCPサーバーを実行し、NATと PBFルールをアクティブセカンダリファイアウォールのデバイス IDに一致させます。アクティブセカンダリファイアウォールの状態のファイアウォールはDHCPリレーをサポートしません。この状態のファイアウォールは、セッションを所有し、セットアップできます。

説明における	HA ファイアウォール	説明
仮	A/A	以下のうちのいずれかで生じたファイアウォール（アクティブ/アクティブ設定）の状態 • ファイアウォールの障害 • モニターしたオブジェクトの障害（リンクまたはパス） • ファイアウォールがサスペンドまたは非稼働状態のままである。 暫定的状態のファイアウォールは、ピアのセッションおよび設定を同期します。 • 仮想ワイヤ展開で、パス障害によりファイアウォールが暫定的状態に移行し、パケットを受信し転送する場合、ファイアウォールはパケットをHA3リンクを経由してピアファイアウォールに送信し、処理します。ピアファイアウォールはパケットを処理し、ファイアウォールへのHA3リンクを経由して送り返し、出口インターフェイスから送信します。この挙動は仮想ワイヤ展開の転送パスを保存します。 • レイヤー3展開で、暫定的状態のファイアウォールがパケットを受信する場合、ファイアウォールはそのパケットをHA3リンクを経由して送信し、ピアファイアウォールはそのセッションを所有またはセットアップします。ネットワークトポロジーにより、このファイアウォールはパケットを宛先に送るか、または暫定的状態のピアに送り返し、転送させます。 パスまたはリンク障害のクリアまたは暫定的状態からアクティブセカンダリ状態へのファイアウォール移行の障害が発生すると、 **Tentative Hold Time**[暫定的な状態の保留時間]がトリガーされ、ルーティング集束が発生します。ファイアウォールは近接ルーティングの確立を試行し、パケットを処理する前にそのルート テーブルを取り込みます。このタイマーを使用しない場合、ファイアウォールは回復時にただちにアクティブ-セカンダリ状態になり、必要なルートがないためパケットがサイレントで破棄されます。 ファイアウォールがサスペンド状態を終了すると、リンクがアップし、受信パケットを処理できるようになると **Tentative Hold Time** [暫定的な状態の保留時間]の間、暫定的状態に移行します。 **Tentative Hold Time range** （**sec**）[暫定的な状態の保留時間範囲 （秒）] は無効化できます（0秒）。範囲は 10～600で、デフォルトは 60です。

説明における	HA ファイアウォール	説明
非稼働	A/P または A/A	ファイアウォールが1つだけパケット送信VR syncまたはQoS syncに設定されているなど、データプレーン障害または設定不適合によるエラー状態 アクティブ/パッシブモードでは、暫定的状態としてリストアップされた原因の全てが非稼働状態を生じます。
サスペンド	A/P または A/A	デバイスが無効化されているため、データトラフィックを渡せず、HA 通信が引き続き発生するものの、デバイスは HA 選出プロセスに参加しません。HA を使用できる状態にするには、ユーザーによる作業が必要になります。

リファレンス：HA 同期

HA ペアの両方のピアで設定の同期化を有効にしている場合は、コミット時に、一方のピアに行った設定のほとんどがもう一方のピアに自動的に同期されます。設定の競合を避けるために、変更は常にアクティブ（アクティブ/パッシブ）またはアクティブ-プライマリ（アクティブ/アクティブ）ピアで行い、変更がもう一方のピアに同期されるまで待機してから、次の変更を行います。

コミットされた設定のみが*HA*ピア間で同期します。*HAsync*時のコミットキューの設定は同期できません。

以下のトピックは各ファイアウォールに個別に設定すべき設定を示しています（これらの選設定はHAピアと同期しません）。

- アクティブ/パッシブ HA で同期されない設定
- アクティブ/アクティブ HA で同期されない設定
- システムのランタイム情報の同期化

アクティブ/パッシブ HA で同期されない設定

アクティブ/パッシブ デプロイメントでは、HA ペアの各ファイアウォールで以下の設定を行う必要があります。下記の設定は、一方のピアからもう一方のピアに同期されません。

設定項目	アクティブ/パッシブで同期されない項目
管理インターフェイス設定	管理設定はすべて各デバイスで個別に設定する必要があります。以下に具体例を示します。 • **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** > **General Settings (一般設定)** —ホスト名、ドメイン、ログイン バナー、SSL/TLS サービスプロファイル (および関連する証明書)、タイム ゾーン、表示言語、日付、時間、緯度、経度。 • **Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理） > **Management Interface Settings**（管理インターフェイス設定）—IP タイプ、IP アドレス、ネットマスク、デフォルト ゲートウェイ、IPv6 アドレス/プレフィックス長、デフォルト IPv6 ゲートウェイ、速度、MTU、およびサービス（HTTP、HTTP OCSP、HTTPS、Telnet、SSH、Ping、SNMP、ユーザー ID、ユーザー ID Syslog リスナー SSL、ユーザー ID Syslog リスナー UDP
マルチ vsys 機能	PA-3200 Series、PA-3400 Series、PA-5200 Series、PA-5400 Series、および PA-7000 Series firewall でデフォルトで提供される基本の仮想システムの数を増やすには、ペアの各 firewall で Virtual Systems ライセンスをアクティブ化する必要があります。

設定項目	アクティブ/パッシブで同期されない項目
	各ファイアウォールで **Multi Virtual System Capability**（マルチ仮想システム機能）を有効にする必要があります（**Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理） > **General Settings**（一般設定））。
Panorama 設定	以下の Panorama 設定を各ファイアウォールで行います（**Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理） > **Panorama Settings**（**Panorama** 設定））。 • **Panorama** サーバー • **Disable Panorama Policy and Objects**（Panorama ポリシーとオブジェクトを無効にする）および **Disable Device and Network Template**（デバイスとネットワーク テンプレートを無効にする）
SNMP	デバイス > セットアップ > 業務 > **SNMP** のセットアップ
サービス	デバイス > セットアップ > サービス
グローバル サービス ルート	デバイス > セットアップ > サービス > サービス ルートの設定
テレメトリと脅威インテリジェンスの設定	デバイス > セットアップ > テレメトリと脅威インテリジェンス
データ保護	デバイス > セットアップ > **Content-ID** > データ保護の管理
ジャンボ フレーム	デバイス > セットアップ > セッション > セッション設定 > **Jumbo Frame** を有効にする
パケット バッファ保護	デバイス > セットアップ > セッション > セッション設定 > パケット バッファ保護 ネットワーク > ゾーン > パケット バッファ保護の有効化
フォワード プロキシ サーバーの証明書設定	デバイス > セットアップ > セッション > 暗号設定 > **SSL** フォワード プロキシ設定
HSM が保護するマスター キー	デバイス > セットアップ > **HSM** > ハードウェア セキュリティ モジュール プロバイダー > **HSM** が保護するマスター キー
ログのエクスポート設定	デバイス > スケジュール設定されたログのエクスポート

設定項目	アクティブ/パッシブで同期されない項目
ソフトウェア更新	ソフトウェア更新については、各デバイスに個別にダウンロードしてインストールすることも、一方のピアにダウンロードしてもう一方のピアに同期することもできます。各ピアに更新をインストールする必要があります（**Device**（デバイス） > **Software**（ソフトウェア））。
GlobalProtect エージェント パッケージ	GlobalProtect アプリの更新については、各ファイアウォールに個別にダウンロードしてインストールすることも、一方のピアにダウンロードしてもう一方のピアに同期することもできます。各ピアで個別にアクティベーションする必要があります（**Device**（デバイス） > **GlobalProtect Client**（**GlobalProtect** クライアント））。
コンテンツアップデート	コンテンツ更新については、各デバイスに個別にダウンロードしてインストールすることも、一方のピアにダウンロードしてもう一方のピアに同期することもできます。各ピアに更新をインストールする必要があります（**Device**（デバイス） > **Dynamic Updates**（動的更新））。
ライセンス/サブスクリプション	デバイス > ライセンス
サポート サブスクリプション	デバイス > サポート
マスター キー	マスター キーは、HA ペアの各ファイアウォールで同一でなければなりませんが、各デバイスで手動で入力する必要があります（**Device**（デバイス） > **Master Key and Diagnostics**（マスター キーおよび診断））。 マスター キーを変更する前に、両方のピアで設定の同期化を無効にして（**Device**（デバイス） > **High Availability**（高可用性） > **General**（全般） > **Setup**（セットアップ）、**Enable Config Sync**（設定の同期化の有効化）チェック ボックスをオフ）、キーを変更した後にもう一度有効にする必要があります。
レポート、ログ、およびダッシュボードの設定	ログ データ、レポート、ダッシュボードのデータおよび設定（列表示、ウィジット）は、ピア間で同期されません。ただし、レポートの設定は同期されます。
高可用性の設定	デバイス > 高可用性（**HA**）
ルール使用状況データ	ヒット数、作成日、変更日などのルール使用状況データは、ピア間で同期されません。各ファイアウォールのポリシールールヒットカウントデータを表示するには各ファイアウォールにログインするか、また

設定項目	アクティブ/パッシブで同期されない項目
	は HA ファイアウォールピアの情報を表示するには Panorama を使用しなければなりません。
SSL を介したデバイス管理および Syslog 通信専用の証明書	デバイス > 証明書の管理 > 証明書 デバイス管理または SSL を介した syslog 通信に使用される証明書は、HA ピアと同期しません。 管理インターフェイスに使用される証明書は同期されていませんが (異なる場合もあります)、証明書エントリの名前はアクティブ デバイスとパッシブ デバイスで同じである必要があります。
証明書プロファイルの証明書	デバイス > 証明書の管理 > 証明書プロファイル
デバイス管理専用の SSL/TLS サービス プロファイル	デバイス > 証明書の管理 > **SSL/TLS Service Profile** デバイス管理用の SSL/TLS サービス プロファイルは、HA ピアと同期しません。
Device-ID および IoT セキュリティ	IP アドレスからデバイスへのマッピングとポリシー ルールの推奨事項は、HA ピアと同期しません。

アクティブ/アクティブ HA で同期されない設定

アクティブ/アクティブ デプロイメントでは、HA ペアの各ファイアウォールで以下の設定を行う必要があります。下記の設定は、一方のピアからもう一方のピアに同期されません。

設定項目	アクティブ/アクティブで同期されない項目
管理インターフェイス設定	以下の管理設定を各ファイアウォールで全て個別に設定します。 • **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** > **General Settings (一般設定)** –ホスト名、ドメイン、ログイン バナー、SSL/TLS サービスプロファイル (および関連する証明書)、タイム ゾーン、表示言語、日付、時間、緯度、経度。 • **Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理） > **Management Interface Settings**（管理インターフェイス設定）–IP アドレス、ネットマスク、デフォルト ゲートウェイ、IPv6 アドレス/プレフィックス長、デフォルト IPv6 ゲートウェイ、速度、MTU、およびサービス（HTTP、HTTP OCSP、HTTPS、Telnet、SSH、Ping、SNMP、ユーザー ID、ユーザー ID Syslog リスナー SSL、ユーザー ID Syslog リスナー UDP）

設定項目	アクティブ/アクティブで同期されない項目
マルチ vsys 機能	PA-3200 Series、PA-3400 Series、PA-5200 Series、PA-5400 Series、および PA-7000 Series firewall でデフォルトで提供される基本の仮想システムの数を増やすには、ペア内の各 firewall で Virtual Systems ライセンスをアクティブ化する必要があります。 各ファイアウォールで **Multi Virtual System Capability**（マルチ仮想システム機能）を有効にする必要があります（**Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理） > **General Settings**（一般設定））。
Panorama 設定	以下の Panorama 設定を各ファイアウォールで行います（**Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理） > **Panorama Settings**（**Panorama** 設定））。 • **Panorama** サーバー • **Disable Panorama Policy and Objects**（Panorama ポリシーとオブジェクトを無効にする）および **Disable Device and Network Template**（デバイスとネットワーク テンプレートを無効にする）
SNMP	デバイス > セットアップ > 業務 > **SNMP** のセットアップ
サービス	デバイス > セットアップ > サービス
グローバル サービス ルート	デバイス > セットアップ > サービス > サービス ルートの設定
テレメトリと脅威インテリジェンスの設定	デバイス > セットアップ > テレメトリと脅威インテリジェンス
データ保護	デバイス > セットアップ > **Content-ID** > データ保護の管理
ジャンボ フレーム	デバイス > セットアップ > セッション > セッション設定 > **Jumbo Frame** を有効にする
パケット バッファ保護	デバイス > セットアップ > セッション > セッション設定 > パケット バッファ保護 ネットワーク > ゾーン > パケット バッファ保護の有効化
フォワード プロキシ サーバーの証明書設定	デバイス > セットアップ > セッション > 暗号設定 > **SSL** フォワード プロキシ設定
HSM 設定	デバイス > セットアップ > **HSM**

設定項目	アクティブ/アクティブで同期されない項目
ログのエクスポート設定	デバイス > スケジュール設定されたログのエクスポート
ソフトウェア更新	ソフトウェア更新については、各デバイスに個別にダウンロードしてインストールすることも、一方のピアにダウンロードしてもう一方のピアに同期することもできます。各ピアに更新をインストールする必要があります（**Device**（デバイス） > **Software**（ソフトウェア））。
GlobalProtect エージェント パッケージ	GlobalProtect アプリの更新については、各ファイアウォールに個別にダウンロードしてインストールすることも、一方のピアにダウンロードしてもう一方のピアに同期することもできます。各ピアで個別にアクティベーションする必要があります（**Device**（デバイス） > **GlobalProtect Client**（**GlobalProtect** クライアント））。
コンテンツアップデート	コンテンツ更新については、各デバイスに個別にダウンロードしてインストールすることも、一方のピアにダウンロードしてもう一方のピアに同期することもできます。各ピアに更新をインストールする必要があります（**Device**（デバイス） > **Dynamic Updates**（動的更新））。
ライセンス/サブスクリプション	デバイス > ライセンス
サポート サブスクリプション	デバイス > サポート
Ethernet インターフェイスの IP アドレス	Ethernet インターフェイスの設定は、IP アドレスを除いてすべて同期されます（**Network**（ネットワーク） > **Interface**（インターフェイス） > **Ethernet**）
ループバック インターフェイスの IP アドレス	ループバック インターフェイスの設定は、IP アドレスを除いてすべて同期されます（**Network**（ネットワーク） > **Interface**（インターフェイス） > **Loopback**（ループバック））。
トンネル インターフェイスの IP アドレス	トンネル インターフェイスの設定は、IP アドレスを除いてすべて同期されます（**Network**（ネットワーク） > **Interface**（インターフェイス） > **Tunnel**（トンネル））。
LACP システム優先順位	アクティブ/アクティブ デプロイメントでは、各ピアに一意の LACP システム ID が必要です（**Network**（ネットワーク） > **Interface**（インターフェイス） > **Ethernet** > **Add Aggregate Group**（集約グループの追加） > **System Priority**（システム優先度））。

設定項目	アクティブ/アクティブで同期されない項目
VLAN インターフェイスの IP アドレス:	VLAN インターフェイスの設定は、IP アドレスを除いてすべて同期されます（**Network**（ネットワーク） > **Interface**（インターフェイス） > **VLAN**）。
仮想ルーター	仮想ルーターの設定は、VR Sync （VR 同期）を有効にしている場合にのみ同期します（**Device**（デバイス） > **High Availability**（高可用性） > **Active/Active Config**（ アクティブ/アクティブ設定） > **Packet Forwarding**（パケット転送））。この設定を行うかどうかは、非対称ルーティングがあるかどうかなど、ネットワークの設計によって異なります。
IPSec トンネル	IPSec トンネル設定の同期は、仮想アドレスにフローティング IP アドレスを使用するよう設定しているかどうかによって異なります（**Device**（デバイス） > **High Availability**（高可用性） > **Active/Active Config**（アクティブ/アクティブ設定） > **Virtual Address**（仮想アドレス））フローティング IP アドレスを設定している場合は、これらの設定が自動的に同期されます。設定していない場合は、各ピアに個別に設定する必要があります。
GlobalProtect ポータル設定	GlobalProtect ポータル設定の同期は、仮想アドレスにフローティング IP アドレスを使用するよう設定しているかどうかによって異なります（**Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル））。フローティング IP アドレスを設定している場合は、GlobalProtect ポータル設定が自動的に同期されます。設定していない場合は、各ピアにポータルを個別に設定する必要があります。
GlobalProtect ゲートウェイ設定	GlobalProtect ゲートウェイ設定の同期は、仮想アドレスにフローティング IP アドレスを使用するよう設定しているかどうかによって異なります（**Network**（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ））。フローティング IP アドレスを設定している場合は、GlobalProtect ゲートウェイ設定が自動的に同期されます。設定していない場合は、各ピアにゲートウェイを個別に設定する必要があります。
QoS	QoS 設定は、**QoS Sync**（**QoS** 同期） を有効にしている場合にのみ同期します（**Device**（デバイス） > **High Availability**（高可用性） > **Active/Active Config**（アクティブ/アクティブ設定） > **Packet Forwarding**（パケット転送））。たとえば、リンクごとに帯域幅が異なる場合、またはサービス プロバイダからの遅延が異なる場合は、QoS 設定が同期しないようにすることができます。

設定項目	アクティブ/アクティブで同期されない項目
LLDP	アクティブ/アクティブ設定では、LLDP 状態または個別のファイアウォール データが同期されません（**Network**（ネットワーク） > **Network Profiles**（ネットワークのプロファイル） > **LLDP**）。
BFD	アクティブ/アクティブ設定では、BFD設定またはBDFセッション データが同期されません（**Network**（ネットワーク） > **Network Profiles**（ネットワークのプロファイル） > **BFD Profile**（**BFD** プロファイル））。
IKE ゲートウェイ	IKE ゲートウェイ設定の同期は、仮想アドレスにフローティング IP アドレスを使用するよう設定しているかどうかによって異なります（**Network**（ネットワーク） > **IKE Gateways**（**IKE** ゲートウェイ））。フローティング IP アドレスを設定している場合は、IKE ゲートウェイ設定が自動的に同期されます。設定していない場合は、各ピアに IKE ゲートウェイを個別に設定する必要があります。
マスター キー	マスター キーは、HA ペアの各ファイアウォールで同一でなければなりませんが、各デバイスで手動で入力する必要があります（**Device**（デバイス） > **Master Key and Diagnostics**（マスター キーおよび診断））。 マスター キーを変更する前に、両方のピアで設定の同期化を無効にして（**Device**（デバイス） > **High Availability**（高可用性） > **General**（全般） > **Setup**（セットアップ）、**Enable Config Sync**（設定の同期化の有効化）チェック ボックスをオフ）、キーを変更した後にもう一度有効にする必要があります。
レポート、ログ、およびダッシュボードの設定	ログ データ、レポート、ダッシュボードのデータおよび設定（列表示、ウィジット）は、ピア間で同期されません。ただし、レポートの設定は同期されます。
高可用性の設定	• デバイス > 高可用性（**HA**） • （例外は、同期している **Device**（デバイス） > **High Availability**（高可用性） > **Active/Active Configuration**（アクティブ/アクティブ設定） > **Virtual Addresses**（仮想アドレス）です。）
ルール使用状況データ	ヒット数、作成日、変更日などのルール使用状況データは、ピア間で同期されません。各ファイアウォールのポリシールールヒットカウントデータを表示するには各ファイアウォールにログインするか、または HA ファイアウォールピアの情報を表示するには Panorama を使用しなければなりません。

設定項目	アクティブ/アクティブで同期されない項目
SSL を介したデバイス管理および Syslog 通信専用の証明書	デバイス > 証明書の管理 > 証明書 デバイス管理または SSL を介した syslog 通信に使用される証明書は、HA ピアと同期しません。
証明書プロファイルの証明書	デバイス > 証明書の管理 > 証明書プロファイル
デバイス管理専用の SSL/TLS サービス プロファイル	デバイス > 証明書の管理 > **SSL/TLS Service Profile** デバイス管理用の SSL/TLS サービス プロファイルは、HA ピアと同期しません。
Device-ID および IoT セキュリティ	IP アドレスからデバイスへのマッピングとポリシー ルールの推奨事項は、HA ピアと同期しません。

システムのランタイム情報の同期化

次の表は、HA ピア間で同期されるシステム ランタイム情報をまとめたものです。

ランタイム情報	設定の同期化の有無		HA リンク	詳細:
	A/P	A/A		
マネジメント プレーン				
ユーザーからグループへのマッピング	あり。	あり。	HA1	
仮想システム間でのユーザーマッピング	あり。	あり。	HA1	
ユーザーと IP アドレスのマッピング	あり。	あり。	HA1	A/A 構成では、アクティブ プライマリ ピアのみが User-ID サーバーまたはエージェントに接続し、アクティブ セカンダリ ピアには接続しません。アクティブ プライマリ ピアが中断またはオフラインの場合、アクティブ セカンダリ ピアは User-ID サーバーまた

ランタイム情報	設定の同期化の有無		HA リンク	詳細:
	A/P	A/A		
				はエージェントに接続します。
DHCP リース（サーバーとして）	あり。	あり。	HA1	HA ピアの PAN-OS バージョンが一致しない場合、DHCP リース (サーバーとして) 設定情報は同期されません。
DNS キャッシュ	無し	無し	N/A	
FQDN 更新	無し	無し	該当なし	
IKE SA [Security Associations] (フェーズ 1)	いいえ	無し	該当なし	
Forward Information Base（FIB）（転送情報ベース（FIB））	あり	無し	HA1	
マルチキャストFIB（MFIB）	あり	無し	HA1	
PAN-DB URL キャッシュ	あり。	無し	HA1	このキャッシュは、データベースのディスクへのバックアップ時（8 時間ごと、URL データベースのバージョンが更新される時点）、またはファイアウォールの再起動時に同期されます。
コンテンツ（手動同期）	あり。	あり。	HA1	
PPPoE、PPPoE リース	あり。	あり。	HA1	
DHCP クライアントの設定およびリース	あり。	あり。	HA1	HA ピアの PAN-OS バージョンが一致しない場合、DHCP クライアント設定とリース設定情報は同期されません。

ランタイム情報	設定の同期化の有無		HA リンク	詳細:
	A/P	A/A		
SSL VPN Logged in User List （ユーザー リストに記録された SSL VPN）	あり。	あり。	HA1	
データプレーン				
セッション テーブル	あり。	あり。	HA2	• アクティブ/パッシブ ピアはICMPやホスト セッション情報を同期しません。 • アクティブ/アクティブ ピアは、ホスト セッション、マルチキャスト セッション

ランタイム情報	設定の同期化の有無		HA リンク	詳細:
	A/P	A/A		
				またはBFDセッション情報を同期しません。 ホスト セッションは、ファイアウォール インターフェースやGPトンネルに *ping* を実行する *ICMP* セッションなどの、ファイアウォール インターフェースの*1*つで終了するセッションです。
ARP テーブル	あり。	無し	HA2	
マルチキャストセッション テーブル	あり	無し	HA2	

ランタイム情報	設定の同期化の有無		HA リンク	詳細:
	A/P	A/A		
Neighbor Discovery（ND）（ネイバー検出（ND））テーブル	あり。	無し	HA2	
MAC テーブル	あり。	無し	HA2	
IPSec SA [Security Associations] (フェーズ 2)	あり	あり。	HA2	
IPSec シーケンス番号（アンチリプレイ）	あり。	あり。	HA2	
DoS ブロックリストのエントリ	無し	無し	N/A	
仮想 MAC	あり。	あり。	HA2	
SCTP アソシエーション	あり。	無し	HA2	

モニタリング

潜在的な問題を未然に防止し、問題が発生した場合の対応を促進するために、このファイアウォールは有益な情報を含むカスタマイズ可能なレポートを使用し、トラフィックとユーザーパターンに関するインテリジェンスを提供します。ファイアウォールのダッシュボード、アプリケーション コマンド センター（ACC）、レポート、およびログを使用してネットワーク上のアクティビティをモニターできます。ログをモニタリングして情報をフィルタリングし、事前定義されたビューまたはカスタマイズされたビューで構成されるレポートを生成できます。たとえば、事前定義されたテンプレートを使用してユーザーのアクティビティに関するレポートを生成したり、レポートとログを分析して、ネットワーク上での異常な振る舞いの意味を解釈したり、トラフィックのパターンに関するカスタム レポートを生成したりすることができます。視覚的に訴求する方法でネットワーク アクティビティを表示するために、ダッシュボードと ACC にはウィジット、グラフ、および表が含まれており、操作して関心のある情報を見つけることができます。さらに、モニターした情報を電子メール通知、Syslog メッセージ、SNMP トラップ、NetFlow レコードとして外部システムに転送するようにファイアウォールを設定できます。

Dashboard の使用

Dashboard[Dashboard] タブのウィジットには、ソフトウェアのバージョン、各インターフェイスの動作状態、リソース使用状況、脅威の最新エントリ（最大 10 個）、設定、システム ログなどのファイアウォールの一般的な情報が表示されます。使用可能なウィジットすべてがデフォルトで表示されますが、各管理者は必要に応じて個々のウィジットを削除および追加できます。ダッシュボードや個々のウィジットを更新するには、更新アイコン をクリックします。自動更新間隔を変更するには、ドロップダウン リストから間隔（**[1** 分**]**、**[2** 分**]**、**[5** 分**]**、または**[**手動**]**）を選択します。ダッシュボードにウィジットを追加するには、widget （ウィジット）ドロップダウンをクリックしてカテゴリを選択し、次にウィジット名を選択します。ウィジットを削除するには、タイトル バーの をクリックします。以下の表に、ダッシュボードのウィジットの説明を示します。

Dashboard のチャート	内容
上位のアプリケーション	セッション数が最も多いアプリケーションが表示されます。ブロック サイズでセッションの相対数を示し（マウス カーソルをブロックの上に移動すると数が表示されます）、色でセキュリティのリスクを示します（緑（リスク低）～赤（リスク高））。アプリケーションをクリックして、プロファイルを表示します。
上位のハイリスク アプリケーション	Top Applications [上位アプリケーション] と似ていますが、ここにはセッション数が最も多いハイリスク アプリケーションが表示されます。
General Information（一般的な情報）	ファイアウォール名、モデル、PAN-OS ソフトウェアのバージョン、アプリケーション、脅威、URL フィルタリング定義のバージョン、現在の日時、および最後に再起動したときからの経過時間が表示されます。
Interface Status	各インターフェイスが、有効 (緑)、無効 (赤)、または不明な状態 (グレー) であることを示します。
Threat Logs（脅威ログ）	脅威ログには、最新 10 エントリの脅威の ID、アプリケーション、および日時が表示されます。脅威 ID は、マルウェアに関する説明、または URL フィルタリング プロファイルに違反する URL を示します。
Config Logs（設定ログ）	設定ログの中から最新の 10 のエントリの、管理ユーザー名、クライアント（Web または CLI）、および日時が表示されます。
データ フィルタリング ログ	データ フィルタリング ログの中で、直近 60 分間に生成されたログの説明と日時が表示されます。

Dashboard のチャート	内容
URL Filtering Logs（URL フィルタリング ログ）	URL フィルタリング ログには、直近 60 分間に生成されたログの説明と日時が表示されます。
System Logs（システム ログ）	システム ログの中で、最新の 10 のエントリの説明と日時が表示されます。 ***Config installed*** エントリは、設定の変更が正常にコミットされたことを示します。
System Resources（システム リソース）	管理 CPU 使用率、データ プレーン使用率、およびファイアウォールで確立されたセッションの数を示すセッション カウントが表示されます。
ログインしている管理者	現在ログインしている各管理者の送信元 IP アドレス、セッション タイプ（Web または CLI）、およびセッションの開始時刻が表示されます。
ACC Risk Factor（ACC リスク ファクタ）	この 1 週間に処理されたネットワーク トラフィックの平均リスク ファクタ（1 ～ 5）が表示されます。値が大きいほどリスクが大きくなります。
高可用性（HA）	高可用性（HA）を有効にすると、ローカルおよびピアファイアウォールのHA状態–緑（アクティブ）、黄（パッシブ）、黒（その他）–が表示されます。HA についての詳細は、高可用性（HA）を参照してください。
ロック	管理者によって設定された設定ロックが表示されます。

アプリケーション コマンド センターの使用

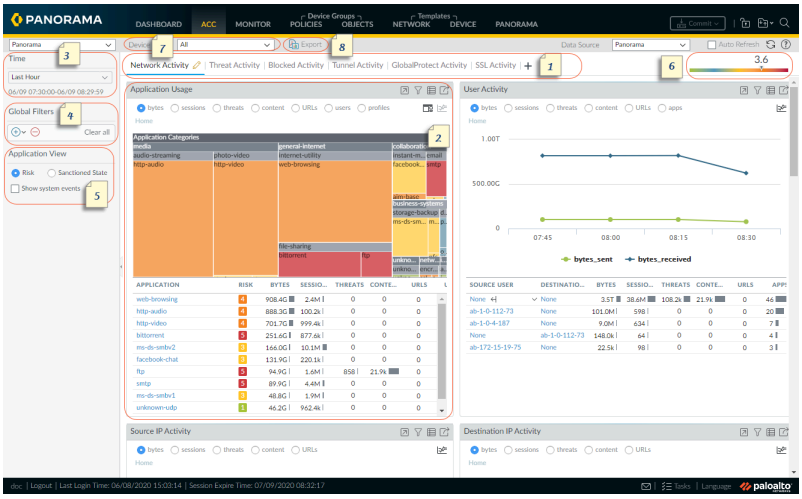
アプリケーションコマンドセンター(ACC)は、アプリケーション、ユーザー、URL、脅威、ネットワーを通過するコンテンツを分かりやすく表示するインタラクティブなグラフィックです。ACCはファイアウォールログを使って、トラフィックパターンと脅威に関する実行可能な情報を可視化します。ACC のレイアウトは、ネットワーク アクティビティ、脅威アクティビティ、およびブロックされたアクティビティのタブ表示で構成され、各タブには関連するウィジットによりネットワーク トラフィックが視覚的にわかりやすく表示されます。この図表形式の表現によりデータとの対話が可能になり、ネットワークで発生したイベントの関係性も可視化できるため、異常な状況を発見し、ネットワーク セキュリティ ルールの強化方法を見つけることができます。カスタム タブを追加し、自分にとって重要な情報にドリルダウンできるウィジェットを含めるなどして、ネットワーク ビューをパーソナライズできます。

ACC ウィジェットやエクスポートされた *ACC* レポートを含む *ACC* データは、***Log at Session End*** を有効にしたセキュリティ ポリシー ルールのデータを使用します。*ACC* でデータの一部が表示されない場合は、Traffic および Threat のログを確認して、修正が必要なセキュリティ ポリシー ルールを決定し、それらのセキュリティ ポリシー ルールに一致するすべての新しいログが *ACC* で表示できるようにします。

- ACC — 概要
- ACC のタブ
- ACC のウィジェット (ウィジットの説明)
- ACC のフィルタ
- ACC の操作
- 「ユース ケース：ACC — 情報検出のパス

ACC — 概要

ACC の概要を簡単に紹介します。



ACC — 概要		
	タブ	ACC には、ネットワーク トラフィックや脅威アクティビティ、ブロックされたアクティビティを可視化する事前定義されたタブが 3 つ含まれています。各タブの詳細は、「ACC のタブ」を参照してください。
	ウィジェット	各タブには、タブに関連付けられたイベントやトレンドを最適に表現する、デフォルトのウィジット セットが含まれます。ウィジットでは、以下のフィルタを使用してデータを調査できます。 • バイト（受信および送信） • sessions • コンテンツ（ファイルおよびデータ） • URL カテゴリ • 脅威（および数） 各ウィジェットの詳細は、「ACC のウィジェット」を参照してください。
	**Time** （時刻）	各ウィジットのチャートやグラフにはサマリー表示と履歴表示が用意されています。カスタム範囲を選択するか、事前定義済みの過去 15 分間～過去 90 日間 (または暦日の過去 30 日間) を選択できます。選択された期間は ACC のすべてのタブに適用されます。 データの表示に使用するデフォルトの期間は **Last Hour** [過去 1 時間]で、15 分間隔で更新されます。各間隔の日時は画面に表示されます。たとえば、11 時 40 分時点の時間範囲は「01/12 10:30:00-01/12 11:29:59」です。
	グローバル フィルタ	Global Filters （グローバル フィルタ）を使用すると、すべてのタブのすべてのウィジットにフィルタを設定できます。チャート/グラフには、選択されたフィルタを適用した後のデータが表示されます。フィルタの使用方法の詳細は、「ACC フィルタ」を参照してください。
	アプリケーション のビュー	アプリケーションのビューでは、ネットワークで使用中の許可されたアプリケーションと不許可のアプリケーション、またはネットワークで使用中のアプリケーションのリスク レベルで ACC ビューをフィルタリングできます。緑色は許可さ

ACC — 概要		
		れたアプリケーション、青色は不許可のアプリケーション、黄色は部分的に許可されたアプリケーションを示します。部分的に許可されたアプリケーションとは、許可状態が混在しているアプリケーションです。Panorama のデバイス グループ内の複数の仮想システムまたは 1 つ以上のファイアウォールで有効になっているファイアウォール上の 1 つ以上の仮想システムで許可されているなど、アプリケーションが矛盾して許可されているとタグ付けされていることを示します。
	**Risk Factor** [リスク ファクタ]	リスク ファクタ（1 = 最低～ 5 = 最高）は、ネットワーク上で使用されているアプリケーションに基づく相対的なリスクを示します。リスク ファクタではさまざまな要因を使用して関連付けられたリスク レベルが評価されます。たとえば、アプリケーションがファイルを共有できるかどうか、乱用されやすいか、ファイアウォールを回避しようとしているかなどがあります。また、ブロックされた脅威数によって確認される脅威のアクティビティとマルウェア、侵入されたホスト、マルウェアのホストまたはドメインへのトラフィックも要因として使用されます。
	送信元	ACC 表示に使用されるデータ。オプションは、ファイアウォールと Panorama で異なります。 ファイアウォールでは、複数の仮想システムが有効になっている場合、**Virtual System**（仮想システム）ドロップダウンリストを使用して、ACC の表示にすべての仮想システムからのデータを含めるか、選択した仮想システムのみを含めるかを変更できます。 Panorama では、**Device Group**（デバイス グループ）ドロップダウンを選択して、ACC の表示にすべてのデバイス グループのデータを含めるか、選択したデバイス グループのデータのみを含めるかを変更できます。 さらに Panorama では、**Data Source**（データ送信元）を **Panorama** のデータまたは **Remote Device Data**（リモート デバイス データ）に変更できます。**Remote Device Data** [リモート デバイス データ]は、すべての管理対象ファイアウォールが PAN-OS 7.0.0 以降である場合にのみ選択できます。特定のデバイス グループで表示をフィルタリ

ACC – 概要		
		ングする場合、**Panorama** のデータがデータ ソースとして使用されます。
	エクスポート	現在選択されているタブに表示されているウィジットを PDF としてエクスポートできます。PDF は、コンピュータの Web ブラウザに関連付けられたダウンロード フォルダにダウンロードされ、保存されます。

ACC のタブ

ACC には以下の事前定義済みのタブがあり、ネットワーク アクティビティ、脅威のアクティビティ、ブロックされたアクティビティが表示されます。

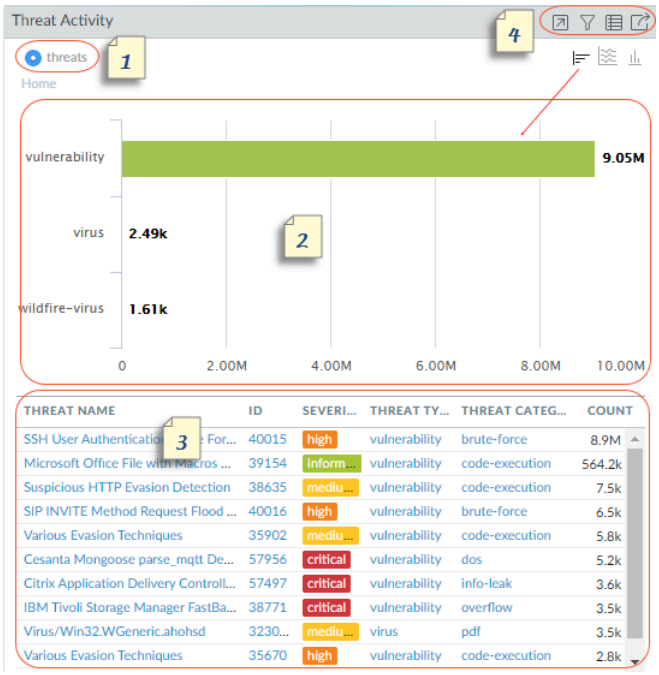
タブ	説明
ネットワーク アクティビティ	ネットワーク上のトラフィックおよびユーザー アクティビティの以下のような概要が表示されます。 • 使用率の高い上位のアプリケーション • トラフィックを多く生成している上位ユーザー（バイト、コンテンツ、脅威、またはユーザーがアクセスした URL の詳細を含む） • トラフィックの一致により最も使用されたセキュリティ ルール また、ネットワーク アクティビティを送信元または宛先のゾーン、領域、または IP アドレス別に表示したり、入力インターフェイスまたは出力インターフェイス別に表示したり、GlobalProtect ホスト情報（ネットワーク上で最もよく使用されたデバイスのオペレーティング システムなど）を表示したりできます。
脅威アクティビティ	ネットワーク上の脅威の概要が、最も顕著な脅威に焦点を当てて表示されます。たとえば、脆弱性、スパイウェア、ウイルス、有害なドメインまたは URL、上位の WildFire 送信（ファイル タイプ別およびアプリケーション別）、非標準ポートを使用しているアプリケーションなどです。このタブの Compromised Hosts（侵入されたホスト）ウィジット（ウィジットがサポートされるのは一部のプラットフォームのみ）は、より適切な視覚化手法で検出を補完します。Correlated Events （相関されたイベント）タブ（**Automated Correlation Engine**（自動相関エンジン） > **Correlated Events**（相関されたイベント））からの情報を使用して、ネットワーク上の侵入されたホストを送信元ユーザーまたは IP アドレス別に重大度の順番で集約して表示します。

タブ	説明
ブロックされたアクティビティ	主に、ネットワークに入ることを阻止されたトラフィックに関する情報を提供します。このタブのウィジットでは、拒否されたアクティビティをアプリケーション名、ユーザー名、脅威名、ブロックされたコンテンツ（ファイル ブロッキング プロファイルによってブロックされたファイルとデータ）別に表示できます。さらに、脅威、コンテンツ、URL のブロックで最も一致した上位セキュリティ ルールのリストも表示されます。
トンネル アクティビティ	トンネル検査ポリシーに基づいてファイアウォールで検査されるトンネル トラフィックのアクティビティが表示されます。トンネル ID、モニター タグ、ユーザー、トンネル プロトコル（Generic Routing Encapsulation（GRE）、General Packet Radio Service（GPRS）Tunneling Protocol for User Data（GTP-U）、非暗号化 IPSec など）に基づいて、トンネルの使用状況などの情報が表示されます。
GlobalProtect アクティビティ	GlobalProtect デプロイメントでのユーザー アクティビティの概要を表示します。情報には、ユーザー数とユーザーの接続回数、ユーザーが接続したゲートウェイ、接続の失敗回数と失敗の理由、認証方法の概要と使用された GlobalProtect アプリケーションのバージョン、および隔離されたエンドポイントの数が含まれます。 さらに、このタブには、隔離されたデバイス概要のチャートビューが表示されます。チャートの上部にある切り替えを使用して、GlobalProtect がデバイスを隔離する原因となった操作、GlobalProtect がデバイスを隔離した理由、および隔離されたデバイスの場所別に、隔離されたデバイスを表示します。
SSL アクティビティ	ファイアウォール上の TLS/SSL復号化アクティビティ概要を表示します。情報には、ネットワークでの復号化アクティビティの成功と失敗、プロトコル、証明書、バージョンの問題など復号化に失敗した理由、TLS バージョン、キー交換アルゴリズム、復号化されたトラフィックと復号化されていないトラフィックの量とタイプが含まれます。 ACC 情報を使用して、ネットワーク上での復号化の動作を評価し、復号化ログを使用して詳細をドリルダウンします。

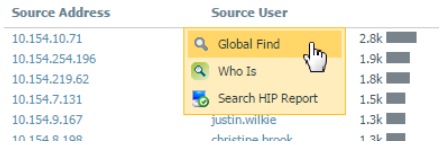
また、ACC の操作 を使用して、ネットワーク監視のニーズを満たすカスタムレイアウトとウィジェットを使用してカスタマイズされたタブを作成し、タブをエクスポートして別の管理者と共有することもできます。

ACC のウィジェット

各タブのウィジットはインタラクティブであるため、ACC フィルタを設定して各テーブルやグラフの詳細をドリルダウンしたり、タブに含まれるウィジットをカスタマイズして必要な情報に焦点を当てたりすることができます。各ウィジットの表示の詳細は、「ウィジット説明」を参照してください。



ウィジェット		
1	**View**	バイト、セッション、脅威、カウント、コンテンツ、URL、有害、安全、ファイル、アプリケーション、データ、プロファイル、オブジェクト、ユーザーでデータをソートできます。使用できるオプションはウィジェットによって異なります。
2	グラフ	グラフ形式の表示オプションとして、ツリーマップ、折れ線グラフ、横棒グラフ、積み上げ領域グラフ、積み上げ棒グラフ、およびマップがあります。使用できるオプションはウィジェットによって異なります。グラフとどのような対話ができるかも、グラフ タイプによって異なります。たとえば、非標準ポートを使用するアプリケーションのウィジェットでは、ツリーマップと線グラフを選択できます。 表示をドリルダウンするには、グラフをクリックします。クリックした領域がフィルタになり、選択対象を拡大し、選択対象のより詳細な情報を表示できます。

ウィジェット		
3	表	グラフの作成に使用されたデータの詳細がグラフの下の表に表示されます。表を操作するには以下のようないくつかの方法があります。 • 表内の属性に対してローカル フィルタをクリックして設定する。グラフが更新され、表がローカル フィルタを使用してソートされます。グラフと表に表示される情報は常に同期されます。 • 表の属性にカーソルを合わせて、ドロップ ダウンで選択可能なオプションを使用する。 
4	アクション	最大化してもっとデータを表示 – ウィジェットを拡大し、テーブルをより大きな画面スペースで、より見やすい情報で表示できます。 ローカル フィルタを設定 – ACC Filters を追加してウィジェット内の表示を絞り込むことができます。これらのフィルターを使用してウィジェットをカスタマイズします。これらのカスタマイズは、ログイン間で保持されます。 ログにジャンプ – ログに直接移動できます (**Monitor** > **Logs** > **<log-type>** タブ)。ログは、グラフがレンダリングされる期間を使用してフィルター処理されます。 ローカル フィルターとグローバル フィルターを設定している場合、ログ クエリは期間とフィルターを連結し、結合されたフィルター セットに一致するログのみを表示します。 **Export**[エクスポート] – グラフを PDF としてエクスポートできます。PDF はコンピュータにダウンロードされて保存されます。これは、Web ブラウザーに関連付けられている Downloads フォルダーに保存されます。

ウィジットの説明

ACC の各タブにはさまざまなウィジットのセットが含まれます。

ウィジット	説明
Network Activity（ネットワーク アクティビティ） – ネットワーク上のトラフィックおよびユーザー アクティビティの概要が表示されます。	
アプリケーションの使用状況	この表には、ネットワーク上で最も使用されているアプリケーションの上位 10 個が表示されます。ネットワーク上で使用されている残りのすべてのアプリケーションは集約され、「その他」として表示されます。グラフには、すべてのアプリケーションがアプリケーション カテゴリ、サブ カテゴリ、およびアプリケーション別に表示されます。ネットワーク上で使用されているアプリケーションをスキャンするには、このウィジットを使用します。帯域幅、セッション数、ファイル転送、最も多くの脅威のトリガ、URL のアクセスを使用して、最も重要なアプリケーションに関する情報を入手できます。 ソート属性: バイト、セッション、脅威、コンテンツ、URL 使用可能なチャート: ツリーマップ、面グラフ、棒グラフ、折れ線グラフ（使用可能なチャートは選択されたソート基準属性に応じて異なります）
User Activity（ユーザー アクティビティ）	生成したトラフィック量とコンテンツを取得するために消費したネットワーク リソースが最も多い、最もアクティブなユーザーの上位 10 が表示されます。バイト、セッション、脅威、コンテンツ（ファイルとパターン）、アクセスした URL でソートされた使用状況で上位のユーザーをモニターするには、このウィジットを使用します。 ソート属性: バイト、セッション、脅威、コンテンツ、URL 使用可能なチャート: 面グラフ、棒グラフ、折れ線グラフ（使用可能なチャートは選択されたソート基準属性に応じて異なります）
送信元 **IP** アクティビティ	ネットワーク上でアクティビティを開始したデバイスの上位 10 の IP アドレスまたはホスト名が表示されます。その他すべてのデバイスは集約され、「その他」として表示されます。 ソート属性: バイト、セッション、脅威、コンテンツ、URL 使用可能なチャート: 面グラフ、棒グラフ、折れ線グラフ（使用可能なチャートは選択されたソート基準属性に応じて異なります）
宛先 **IP** アクティビティ	ネットワーク上のユーザーによって最もアクセスされた宛先の上位 10 件の IP アドレスまたはホスト名が表示されます。 ソート属性: バイト、セッション、脅威、コンテンツ、URL

ウィジット	説明
	使用可能なチャート: 面グラフ、棒グラフ、折れ線グラフ（使用可能なチャートは選択されたソート基準属性に応じて異なります）
送信元領域	ネットワーク上でアクティビティが開始された世界の地域（組み込みまたはカスタム定義領域）の上位 10 件が表示されます。 ソート属性: バイト、セッション、脅威、コンテンツ、URL 使用可能なチャート: マップ、棒グラフ
宛先領域	ネットワーク上でユーザーがそのコンテンツにアクセスしている宛先地域（組み込みまたはカスタム定義領域）の上位 10 件が世界地図上に表示されます。 ソート属性: バイト、セッション、脅威、コンテンツ、URL 使用可能なチャート: マップ、棒グラフ
GlobalProtect ホスト情報	GlobalProtect えんとェントが実行されているホストの状態に関する情報が表示されます。ホスト システムは GlobalProtect エンドポイントです。この情報は、GlobalProtect アプリが送信したデータが、ファイアウォールに定義されている HIP オブジェクトまたは HIP プロファイルと一致したときに生成される HIP マッチ ログのエントリから取得されます。HIP マッチ ログがない場合、このウィジットは空白になります。HIP オブジェクトと HIP プロファイルを作成し、ポリシー一致条件として使用する方法の詳細は、「Configure HIP -Based Policy Enforcement （HIP ベースのポリシー適用の設定）」を参照してください。 ソート属性: プロファイル、オブジェクト、オペレーティング システム 使用可能なチャート: 棒グラフ
ルールの使用状況	ネットワーク上で最も多くのトラフィックを許可したルールの上位 10 件が表示されます。最もよく使用されるルールの表示、使用パターンのモニタリング、ルールがネットワークの保護に有効かどうかの評価を行うには、このウィジットを使用します。 ソート属性: バイト、セッション、脅威、コンテンツ、URL 使用可能なチャート: 折れ線グラフ
入力インターフェイス	ネットワーク内に入るトラフィックを許可するために最も使用されたファイアウォール インターフェイスが表示されます。 ソート属性: バイト、送信済みバイト、受信済みバイト 使用可能なチャート: 折れ線グラフ

ウィジット	説明
出力インターフェイス	ネットワーク外に出るトラフィックに最も使用されたファイアウォール インターフェイスが表示されます。 ソート属性: バイト、送信済みバイト、受信済みバイト 使用可能なチャート: 折れ線グラフ
送信元ゾーン	ネットワーク内に入るトラフィックを許可するために最も使用されたゾーンが表示されます。 ソート属性: バイト、セッション、脅威、コンテンツ、URL 使用可能なチャート: 折れ線グラフ
宛先ゾーン	ネットワーク外に出るトラフィックに最も使用されたゾーンが表示されます。 ソート属性: バイト、セッション、脅威、コンテンツ、URL 使用可能なチャート: 折れ線グラフ
Threat Activity [脅威アクティビティ] – ネットワーク上の脅威の概要が表示されます。	
侵入されたホスト	ネットワーク上の侵入された可能性が高いホストが表示されます。このウィジットでは、相関ログからイベントが要約されます。送信元ユーザー/IP アドレスごとに、一致をトリガーした相関オブジェクトと一致数が表示されます。これらは、相関されたイベント ログで照合された一致の証拠から集約されます。詳細は、「Automated Correlation Engine の使用」を参照してください。 PA-5200 Series、PA-7000 Series、および Panorama で使用可能。 ソート属性: 重大度（デフォルト）
有害な **URL** にアクセスしているホスト	ネットワーク上のホスト（IP アドレス/ホスト名）が有害な URL にアクセスした頻度が表示されます。これらの URL は、PAN-DB のカテゴリに基づいてマルウェアと認識されています。 ソート属性: 数 使用可能なチャート: 折れ線グラフ
有害なドメインを解決しているホスト	DNS シグネチャとの一致数が多いホスト、すなわち、有害な URL のホスト名またはドメインを解決しようとする回数が多いネットワーク上のホストの上位が表示されます。この情報は、ネットワーク上の DNS アクティビティの分析から収集されます。パッシブ DNS モニタリング、ネットワーク上で生成された DNS トラフィック、サンドボックスで確認されたアクティビティ（DNS シンクホールをファイアウォールに設定している場合）、Palo Alto Networks ユーザーがア

ウィジット	説明
	クセス可能な有害な DNS ソースに関する DNS レポートが利用されています。 ソート属性: 数 使用可能なチャート: 折れ線グラフ
脅威アクティビティ	ネットワークで確認された脅威が表示されます。この情報は、アンチウイルス、アンチスパイウェア、および脆弱性防御プロファイルでのシグネチャの一致と、WildFire によって報告されたウイルスに基づいています。 ソート属性: 脅威 使用可能なチャート: 横棒グラフ、面グラフ、縦棒グラフ
アプリケーション別の **WildFire** アクティビティ	生成した WildFire 送信数が最も多いアプリケーションが表示されます。このウィジットでは、WildFire 送信ログから有害判定および安全判定が使用されます。 ソート属性: 有害、安全 使用可能なチャート: 棒グラフ、折れ線グラフ
ファイル タイプ別の **WildFire** アクティビティ	ファイル タイプ別の脅威ベクトルが表示されます。このウィジットでは、生成した WildFire 送信数が最も多いファイル タイプが表示されます。WildFire 送信ログから有害判定および安全判定が使用されます。このデータが使用できない場合、ウィジットは空白になります。 ソート属性: 有害、安全 使用可能なチャート: 棒グラフ、折れ線グラフ
Applications using Non Standard Ports（非標準ポートを使用しているアプリケーション）	非標準ポートを使用してネットワーク内に入るアプリケーションが表示されます。ファイアウォール ルールをポートベースのファイアウォールから移行した場合、アプリケーションのデフォルト ポートを使用するトラフィックのみを許可するポリシー ルールを作成するには、この情報を使用します。必要に応じて、非標準ポートのトラフィックを許可する例外や、カスタム アプリケーションを作成します。 ソート属性: バイト、セッション、脅威、コンテンツ、URL 使用可能なチャート: ツリー マップ、折れ線グラフ
Rules Allowing Applications On Non Standard Ports（非標準ポートを使用す	非標準ポートを使用するアプリケーションを許可するセキュリティ ポリシー ルールが表示されます。グラフにはすべてのルールが表示されますが、表には上位 10 個のルールが表示され、残りのルールのデータは「その他」として集約されます。

ウィジット	説明
るアプリケーションを許可するルール）	この情報をもとに、アプリケーションがポート ホッピングをしているか、またはネットワークに忍び込もうとしているかを評価できるため、ネットワーク セキュリティのギャップを識別できます。たとえば、アプリケーションのデフォルト ポート以外のポートを使用するトラフィックを許可するルールがあるかどうかを検証できます。*application-default* ポートを使用する DNS トラフィックを許可するルールがあるとします（DNS の標準ポートはポート 53）。このウィジットでは、ポート 53 以外の任意のポートを使用してネットワークに入る DNS トラフィックを許可するルールが表示されます。 ソート属性: バイト、セッション、脅威、コンテンツ、URL 使用可能なチャート: ツリー マップ、折れ線グラフ
Blocked Activity（ブロックされたアクティビティ） — ネットワークに入ることができなかったトラフィックに焦点を当てます。	
ブロックされたアプリケーション アクティビティ	ネットワークで拒否されたアプリケーションが表示されます。また、ネットワークに入ることを阻止された脅威、コンテンツ、および URL を表示できます。 ソート属性: 脅威、コンテンツ、URL 使用可能なチャート: ツリー マップ、面グラフ、棒グラフ
ブロックされたユーザー アクティビティ	セキュリティ ポリシー ルールに適用されたアンチウイルス、アンチスパイウェア、ファイル ブロッキング、または URL フィルタリング プロファイルに一致したためにブロックされたユーザー要求が表示されます。 ソート属性: 脅威、コンテンツ、URL 使用可能なチャート: 横棒グラフ、面グラフ、縦棒グラフ
ブロックされた脅威	ネットワーク上で正常に拒否された脅威が表示されます。これらの脅威は、ファイアウォールのダイナミック コンテンツ更新により使用可能なアンチウイルス シグネチャ、脆弱性シグネチャ、および DNS シグネチャと一致しています。 ソート属性: 脅威 使用可能なチャート: 横棒グラフ、面グラフ、縦棒グラフ
ブロックされたコンテンツ	ネットワークに入るのをブロックされたファイルとデータが表示されます。このコンテンツがブロックされたのは、セキュリティ ポリシーがファイル ブロッキング セキュリティ プロファイルまたはデータ フィルタリング セキュリティ プロファイルで定義された基準に基づいてアクセスを拒否したためです。 ソート属性: ファイル、データ

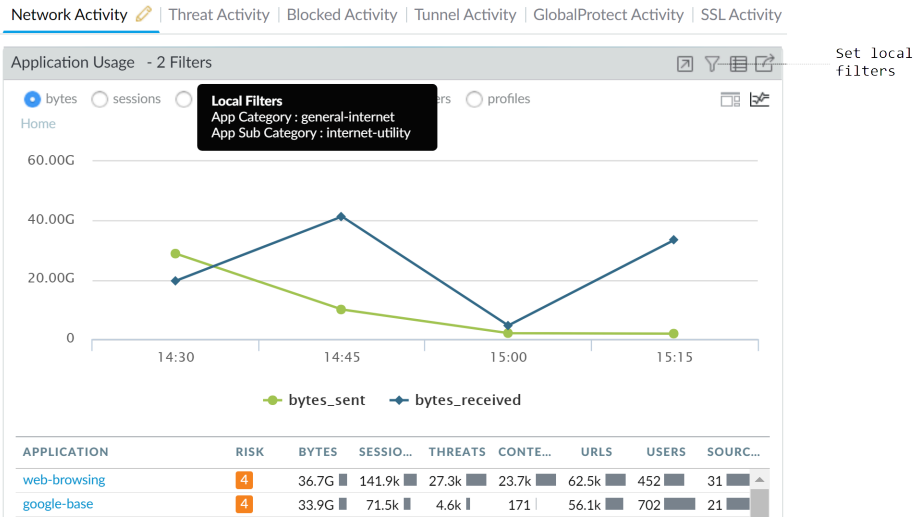
ウィジット	説明
	使用可能なチャート: 横棒グラフ、面グラフ、縦棒グラフ
アクティビティをブロックしているセキュリティ ポリシー	ネットワークに入るトラフィックをブロックまたは制限するセキュリティ ポリシー ルールが表示されます。このウィジットには、ネットワークへのアクセスを拒否された脅威、コンテンツ、および URL が表示されるため、ポリシー ルールの有効性評価に使用できます。このウィジットには、ポリシーに定義された拒否ルールによってブロックされたトラフィックは表示されません。 ソート属性: 脅威、コンテンツ、URL 使用可能なチャート: 横棒グラフ、面グラフ、縦棒グラフ
GlobalProtect Activity—GlobalProtect 展開でのユーザー アクティビティの情報を表示します。	
Successful GlobalProtect Connection Activity（成功した **GlobalProtect** 接続アクティビティ）	選択した期間の GlobalProtect 接続アクティビティのグラフビューを表示します。グラフの上部にあるトグルを使用して、ユーザー、ポータル、ゲートウェイ、および場所ごとの接続統計情報を切り替えます。 ソート属性：ユーザー、ポータル/ゲートウェイ、場所 使用可能なチャート: 棒グラフ、折れ線グラフ
Unsuccessful GlobalProtect Connection Activity（失敗した **GlobalProtect** 接続アクティビティ）	選択した期間における失敗した GlobalProtect 接続アクティビティのグラフビューを表示します。グラフの上部にあるトグルを使用して、ユーザー、ポータル、ゲートウェイ、および場所ごとの接続統計情報を切り替えます。接続の問題の特定とトラブルシューティングに役立つように、理由のチャートまたはグラフを表示することもできます。このグラフでは、ACC はエラー、送信元ユーザー、パブリック IP アドレス、および問題をすばやく特定して解決するのに役立つその他の情報を示します。 ソート属性：ユーザー、ポータル/ゲートウェイ、理由、場所 使用可能なチャート: 棒グラフ、折れ線グラフ
GlobalProtect Deployment Activity（**GlobalProtect** デプロイメント アクティビティ）	デプロイメントのチャートビューの概要を表示します。グラフの上部にあるトグルを使用して、認証方法、GlobalProtect アプリのバージョン、オペレーティングシステムのバージョンごとのユーザーの分布を表示します。 ソート属性：認証方法、globalprotect アプリのバージョン、OS 使用可能なチャート: 棒グラフ、折れ線グラフ
GlobalProtect 隔離アクティビティ	隔離されたデバイスのチャートビューの概要が表示されます。チャートの上部にあるトグルを使用して、GlobalProtect がデバイスを隔離

ウィジット	説明
	する原因となったアクション、GlobalProtect がデバイスを隔離した理由、および隔離されたデバイスの場所によって、隔離されたデバイスを表示します。 ソート属性: アクション、理由、ロケーション 使用可能なチャート: 棒グラフ、折れ線グラフ
SSL Activity (SSL アクティビティ**)**—ネットワーク内の SSL/TLS アクティビティに関する情報を表示。	
Traffic Activity (トラフィックアクティビティ**)**	SSL/TLS アクティビティを非 SSL/TLS アクティビティと比較して、セッションの総数またはバイト単位で表示します。
SSL/TLS Activity (SSL/TLS アクティビティ**)**	TLS バージョンおよびアプリケーションまたは SNI による成功した TLS 接続を表示します。このウィジェットは、より弱い TLS プロトコル バージョンを許可することにより、どの程度のリスクを負っているのかを理解するのに役立ちます。弱いプロトコルを使用するアプリケーションと SNI を特定することで、それぞれを評価し、ビジネス上の理由でアクセスを許可する必要があるかどうかを判断できます。ビジネス目的でのアプリケーションが必要ではない場合は、許可するのではなく、トラフィックをブロックすることをお勧めします。アプリケーションまたは SNI をクリックしてドリルダウンし、詳細情報を表示します。
Decryption Failure Reasons (復号化エラーの理由**)**	SNI による、証明書やプロトコルの問題などの復号化の失敗の理由を示します。この情報を使用して、復号化ポリシーまたはプロファイルの設定ミス、または弱いプロトコルまたはアルゴリズムを使用するトラフィックによって引き起こされる問題を検出します。失敗の理由をクリックしてドリルダウンし、SNI ごとのセッション数を分離するか、SNI をクリックしてその SNI の失敗を確認します。
Successful TLS Version Activity (正常に完了した **TLS** バージョンのアクティビティ**)**	セッションまたはバイトごとに、復号化されたトラフィックと復号化されていないトラフィックの量を示します。復号化されなかったトラフィックは、ポリシー、ポリシーの設定ミス、または復号化除外リストに含まれていることにより、復号化から除外される場合があります (**Device (**デバイス**)** > **Certificate Management (**証明書管理**)** > **SSL Decryption Exclusion (SSL** 復号化除外**)**)。
Successful Key Exchange Activity (正常に完了したキー交換のアクティビティ**)**	アプリケーションまたは SNI、アルゴリズムごとに成功した鍵交換アクティビティを示します。鍵交換アルゴリズムをクリックしてそのアルゴリズムのみのアクティビティを表示するか、アプリケーションまたは SNI をクリックしてそのアプリケーションまたは SNI の鍵交換アクティビティを表示します。

ACC のフィルタ

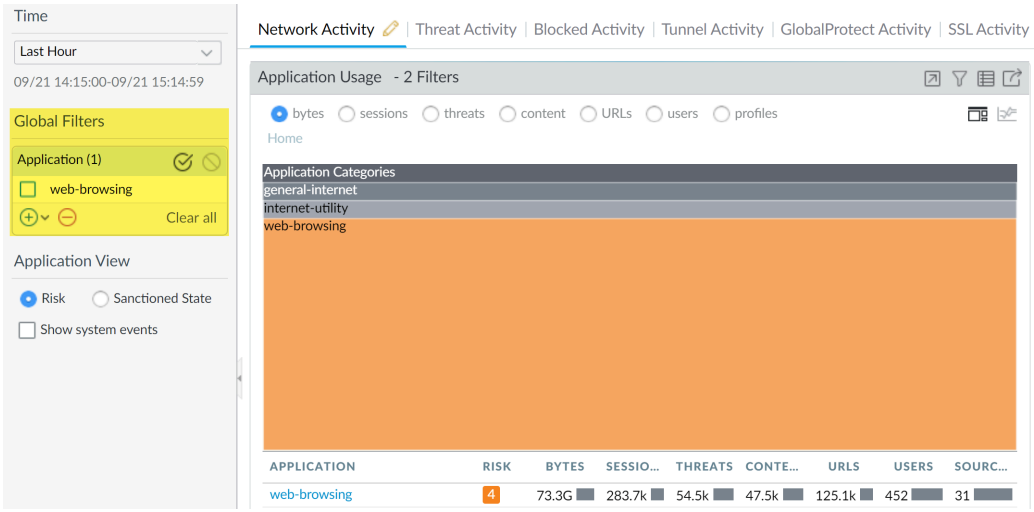
ACC のウィジットに含まれるグラフと表では、フィルタを使用して表示されるデータの範囲を絞り込み、特定の属性を分離し、情報を分析してさらに詳しく確認できます。ACC では、ウィジット フィルタとグローバル フィルタの同時使用がサポートされます。

- **Widget Filters**（ウィジット フィルタ） — ウィジット フィルタ（特定のウィジットでローカルに使用されるフィルタ）を適用します。ウィジット フィルタを使用すると、グラフを操作し、表示をカスタマイズできるため、情報を詳細までドリルダウンして、モニターする必要がある情報に特定のウィジットでアクセスできます。再起動後も持続するウィジット フィルタを作成するには、**Set Local Filter** [ローカル フィルタを設定]オプションを使用する必要があります。



- **Global filters**（グローバル フィルタ） — グローバル フィルタを ACC の全タブに適用します。グローバル フィルタを使用して、自分が現在注目しているデータを中心に表示し、関係のない情報を現在の表示から除外できます。たとえば、特定のユーザーとアプリケーションに関連するすべてのイベントを表示するには、ユーザー名とアプリケーションをグローバル

フィルタとして適用し、そのユーザーとアプリケーションに関連する情報のみを ACC 上のすべてのタブとウィジットに表示できます。グローバル フィルタは永続的ではありません。



グローバル フィルタの適用方法には次の 3 つがあります。

- **Set a global filter from a table**（表からグローバルフィルタを設定する） - 任意のウィジェット内の表から属性を選択し、その属性をグローバルフィルタとして適用します。
- **Add a widget filter to a global filter**[グローバルフィルタにウィジェットフィルタを追加する] - 属性にカーソルを合わせ、その右側にある矢印のアイコンをクリックします。これにより、ウィジェットで使用されているローカルフィルタの属性がグローバルに適用されるようになり、ACCの全てのタブの表示が変更されます。
- **Define a global filter**[グローバルフィルタを定義する] - ACCの**Global Filters**[グローバルフィルタ] ペインを使用してフィルタを定義します。

これらのフィルターの使用方法の詳細については、ACC の操作を参照してください。

ACC の操作

ACC 表示のカスタマイズおよび絞り込みを行うには、タブの追加・削除・エクスポート・インポート、ウィジットの追加と削除、ローカルおよびグローバル フィルタの設定、ウィジットの操作ができます。

タブを追加する。

1. タブ リストの横にある ＋ アイコンを選択します。
2. **View Name**[表示名] を追加します。この名前は、タブの名前として使用されます。最大 5 個のタブを追加できます。

タブを編集する。

タブを選択し、タブ名の横にある鉛筆アイコンをクリックして、タブを編集します。例:
Threat Activity

タブを編集すると、タブに表示されるウィジットを追加、削除、またはリセットできます。タブのウィジット レイアウトを変更することもできます。

タブをデフォルトのタブとして保存するには、を選択します。

タブのエクスポートとインポートを行います。

1. タブを選択し、タブ名の横にある鉛筆アイコンをクリックして、タブを編集します。
2. 現在のタブを .txt ファイルとしてエクスポートするには、アイコンを選択します。この .txt ファイルは他の管理者と共有できます。
3. 別のファイアウォール上でタブを新しいタブとしてインポートするには、タブ リストの横にある アイコンを選択し、名前を追加し、インポートアイコンをクリックして .txt ファイルを参照・選択します。

タブにどのウィジットが含まれているかを確認する。

1. タブを選択し、鉛筆アイコンをクリックしてタブを編集します。
2. **Add Widget (**ウィジェットを追加**)** ドロップダウンを選択し、チェック ボックスがオンになっているウィジットを確認します。

ウィジットまたはウィジット グループを追加する。

1. 新しいタブを追加するか、事前定義済みのタブを編集します。
2. **Add Widget**[ウィジェットの追加] から、追加したいウィジェットを選択します。最大12個のウィジェットを選択可能です。ウィジットを 2 列表示画面にドラッグ アンド ドロップできます。
3. (任意) 2列レイアウトを作成する場合は、**Add Widget Group**[ウィジットグループの追加] を選択します。ウィジットを 2 列表示画面にドラッグ アンド ドロップできます。ウィジットをレイアウトにドラッグすると、ウィジットをドロップするためのプレースホルダが表示されます。

ウィジット グループに名前を付けることはできません。

タブまたはウィジット グループ/ウィジットを削除する。

1. カスタム タブを削除するには、タブを選択して X アイコンをクリックします。 

   事前定義済みのタブを削除することはできません。

2. ウィジット グループ/ウィジットを削除するには、タブを編集し、ワークスペース セクションで、右側の X アイコンをクリックします。削除を取り消すことはできません。

タブのデフォルト ウィジットをリセットする。

事前定義済みのタブ（**Blocked Activity** [ブロックされたアクティビティ]タブなど）で、1 つまたは複数のウィジットを削除できます。レイアウトをリセットし、タブに含まれるウィジット セットをデフォルトに戻す場合、タブを編集し、**[ビューのリセット]** をクリックします。

面グラフ、棒グラフ、または折れ線グラフの詳細を拡大する。

拡大機能の動作を確認する。

選択された期間のデータをファイアウォールが取得します。たとえば、折れ線グラフを拡大すると、クエリが再度トリガーされ、選択された期間のデータをファイアウォールが取得します。単なる拡大表示ではありません。

表のドロップダウンを使用して属性に関する詳細情報を検出する。

1. 表の属性にカーソルを合わせて、ドロップ ダウンを表示します。
2. ドロップダウンをクリックして使用可能なオプションを表示します。
   - **Global Find** — 候補構成内の任意の場所で属性 (ユーザー名/IP アドレス、オブジェクト名、ポリシー ルール名、脅威 ID、またはアプリケーション名) への参照をグローバル検索を使用してファイアウォールあるいはPanoramaの管理サーバーを検索します。
   - **Value** [値] — 脅威 ID、アプリケーション名、またはアドレス オブジェクトの詳細を表示します。
   - **Who Is** [担当者] — IP アドレスのドメイン名（*WHOIS*）検索を実行します。この検索では、インターネット リソースの登録ユーザーまたは割り当て先が保存されているデータベースがクエリされます。
   - **Search HIP Report** [HIP レポートの検索] — ユーザー名または IP アドレスを使用して HIP マッチ レポート内の一致を検索します。

ウィジット フィルタを設定する。

表（グラフの下）で属性をクリックし、その属性をウィジット フィルタとして適用することもできます。

1. ウィジットを選択し、アイコンをクリックします。
2. アイコンをクリックして、適用するフィルタを追加します。
3. **Apply**[適用] をクリックします。このフィルタは、再起動後も持続します。

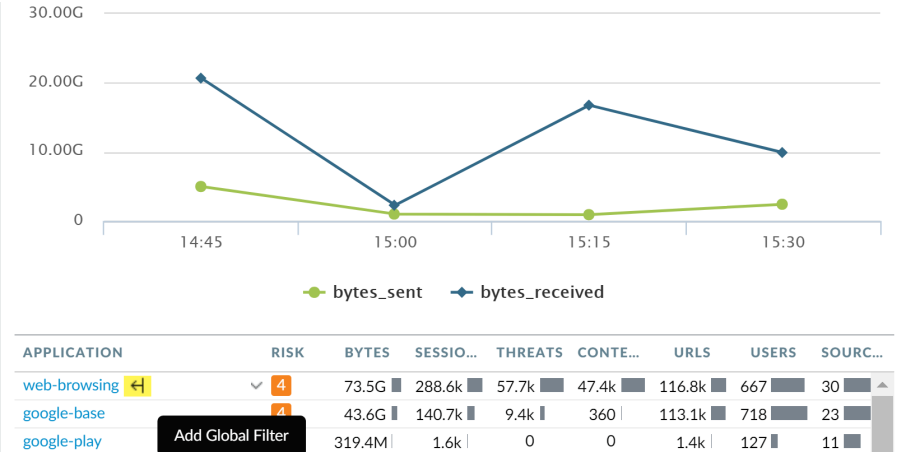
   アクティブなウィジット フィルタがウィジット名の横に示されます。

ウィジット フィルタを無効にする。

1. アイコンをクリックして、Setup Local Filters （ローカル フィルタの設定）ダイアログを表示します。
2. フィルタを追加し、Negate アイコンをクリックします。

表からグローバル フィルタを設定する。

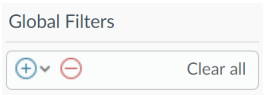
表の中の属性にカーソルを合わせ、その右側に表示される矢印をクリックします。



Global Filters（グローバル フィルタ）ペインを使用して、グローバル フィルタを設定します。

グローバル フィルタの動作を確認します。

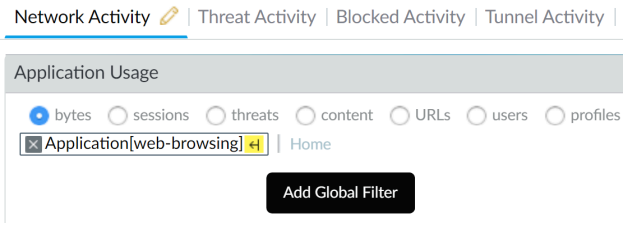
1. ACC の左側で **Global Filters** [グローバル フィルタ]ペインを見つけます。



2. アイコンをクリックして、適用できるフィルタのリストを表示します。

ウィジット フィルタをグローバル フィルタに昇格させる。

1. ウィジット内の任意の表で、属性のリンクをクリックします。これにより、属性がウィジット フィルタとして設定されます。
2. フィルタを昇格させてグローバル フィルタにするには、フィルタの右にある矢印を選択します。



フィルタを削除する。

アイコンをクリックして、フィルタを削除します。

- グローバル フィルタの追加Global filters[グローバルフィルタ]ペインにあります。
- ウィジットフィルタウィジット フィルタの場合: アイコンをクリックすると、Setup Local Filters [ローカル フィルタの設定]ダイアログが表示されます。ここで、フィルタを選択し、 アイコンをクリックします。

すべてのフィルタをクリアする。

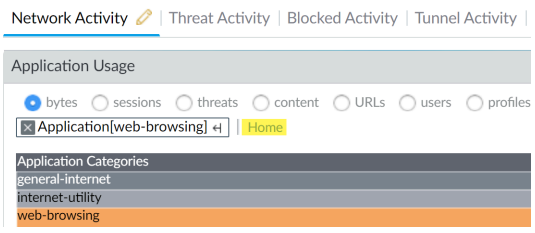
- グローバル フィルタの追加グローバル フィルタの場合: Global Filters[グローバル フィルタ] の下にある **Clear All** [すべてクリア]ボタンをクリックします。
- ウィジットフィルタウィジットを選択し、 アイコンをクリックします。次に、Setup Local Filters[ローカル フィルタの設定]ダイアログで **Clear All** [すべてクリア]ボタンをクリックします。

使用中のフィルタを表示する。

- グローバル フィルタの追加適用されているグローバルフィルタの数がGlobal Filters [グローバルフィルタ] の下の左ペインに表示されます。
- ウィジットフィルタウィジットに適用されているローカル フィルタの数がウィジット名の横に示されます。フィルタを表示するには、 アイコンをクリックします。

ウィジットの表示をリセットする。

- ウィジット フィルタを設定したか、グラフにドリルインした場合、ウィジットの表示をリセットするには、**Home** [ホーム]リンクをクリックします。

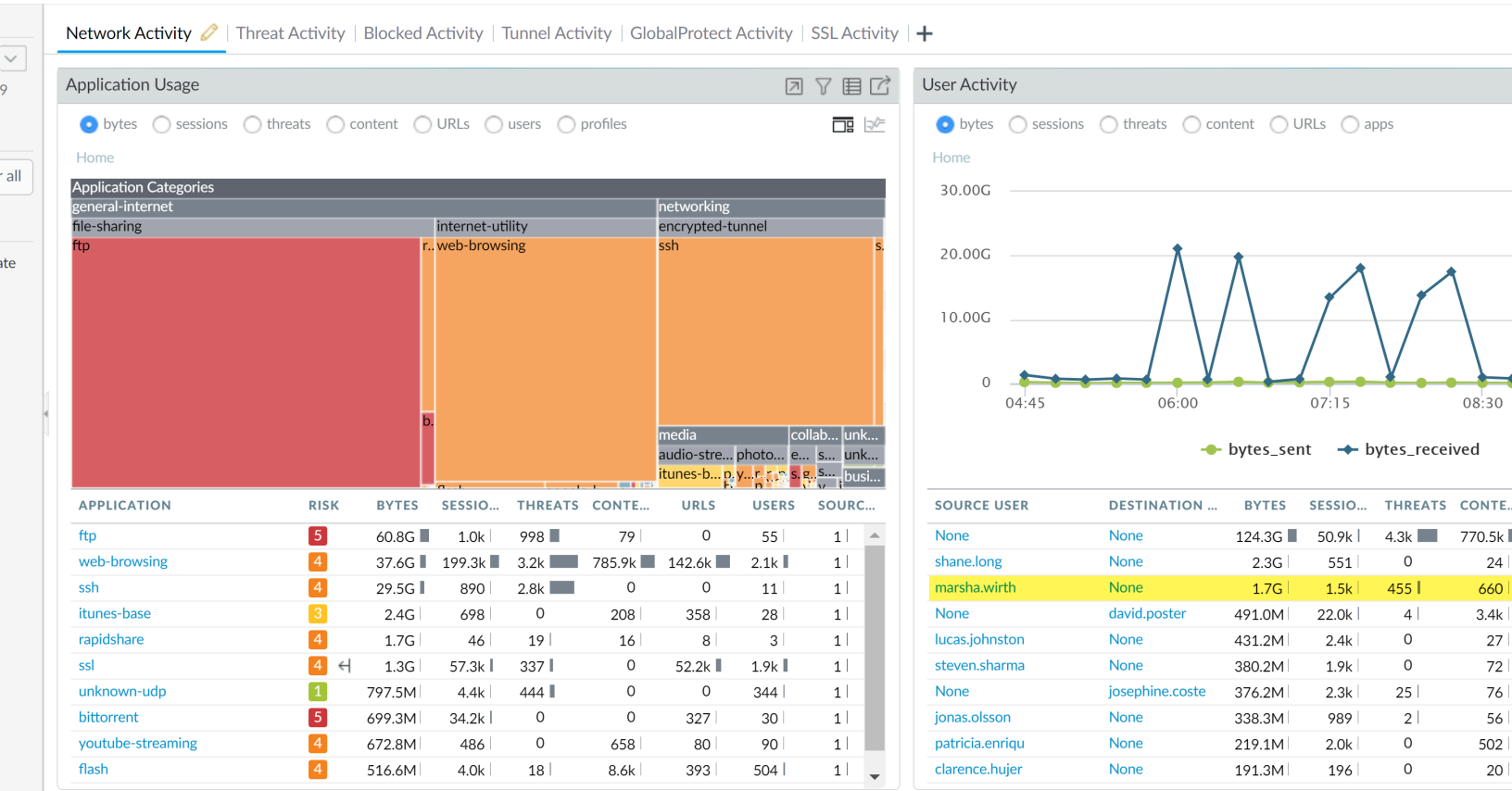


「ユース ケース：ACC — 情報検出のパス

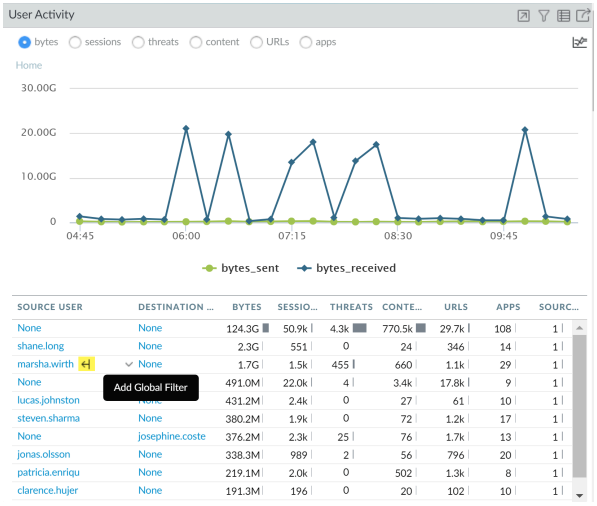
ACC には豊富な情報があり、ここを起点として使用して、ネットワーク トラフィックを分析できます。ACC を使用して関心のあるイベントを見つける例を見てみましょう。この例では、ACC を使用して、正当なユーザーにそのアクションについての責任があることを確認し、不正なアクティビティを検出および追跡し、さらにネットワーク上の侵入されたホストと脆弱なシステムを検出および診断する方法を説明します。

ACC のウィジットとフィルタを使用して、関心または懸念のあるイベントに基づいてデータを分析し、表示を絞り込むことができます。関心のあるイベントのトレース、タブの PDF としての直接エクスポート、生のログへのアクセス、追跡するアクティビティのパーソナライズした表示の保存ができます。これらの機能により、アクティビティをモニターし、有害なアクティビティに対してネットワークを強化するためのポリシーと対策を作成できます。このセクションでは、さまざまなタブにまたがるウィジェットのACC の操作、ウィジェットフィルターを使用したドリルダウン、グローバルフィルターを使用した ACC ビューのピボット、およびインシデント対応または IT チームと共有するための PDF のエクスポートを行います。

ACC > **Network Activity (**ネットワーク アクティビティ**)** タブを見ると、Application Usage (アプリケーション使用率) ウィジットと User Activity (ユーザー アクティビティ) ウィジットが表示されています。ユーザー アクティビティ ウィジェットは、過去 1 時間にユーザー Marsha Wirth が 154 MB のデータを転送したことを示します。これは、ネットワーク上の他のユーザーに比べてほぼ 6 倍の量です。過去数時間の傾向を確認するには、**Time** 期間を **Last 6 Hrs** に拡大し、マーシャのアクティビティは 1,500 セッションで 1.7 ギガバイトとなり、455 の脅威シグネチャがトリガーされました。



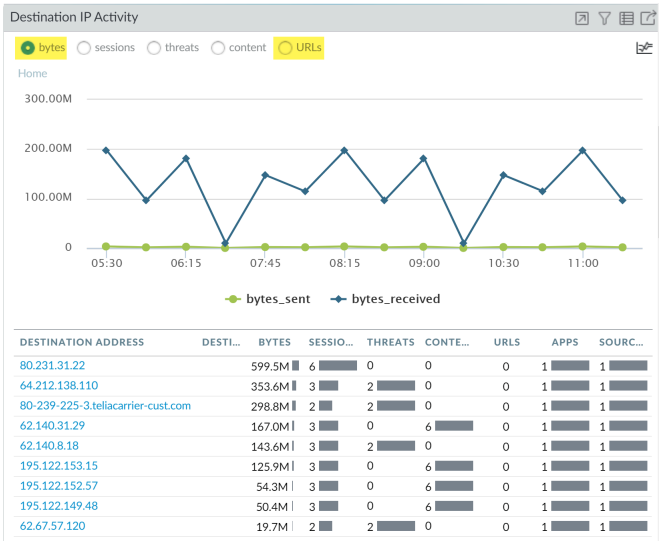
Marsha は大量のデータを転送したため、ユーザー名をグローバル フィルタ(ACC のフィルタ)として適用し、ACC 内のすべてのビューを Marsha のトラフィック アクティビティにピボットします。



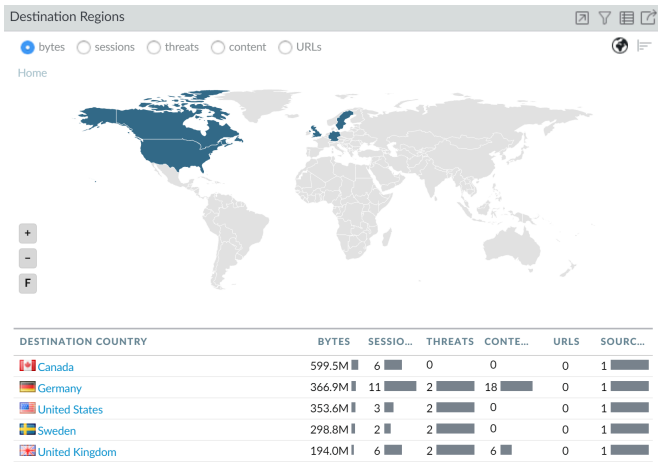
Application Usage （アプリケーション使用率）タブに、Martha が最も使用したアプリケーションが rapidshare であると表示されました。rapidshare は、スイスに本拠を置くファイル ホスティング サイトで、ファイル共有 URL カテゴリに属しています。詳細に調査するため、rapidshare をグローバル フィルタとして追加し、Marsha のアクティビティを rapidshare のコンテキストで表示します。

rapidshare の社内使用を認めるかどうかを検討します。このサイトへのアップロードを許可するべきでしょうか、または帯域幅を制限するための *QoS* ポリシーが必要でしょうか?

Marsha が通信した IP アドレスを表示するには、**Destination IP Activity** [宛先 IP アクティビティ]ウィジットを確認し、データをバイト別および URL 別に表示します。

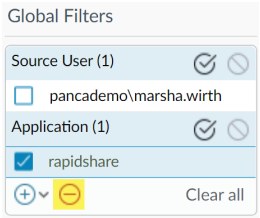


Marsha が通信した国を調べるには、**Destination Regions (宛先領域)** ウィジットで **sessions (セッション)** を基準にソートします。

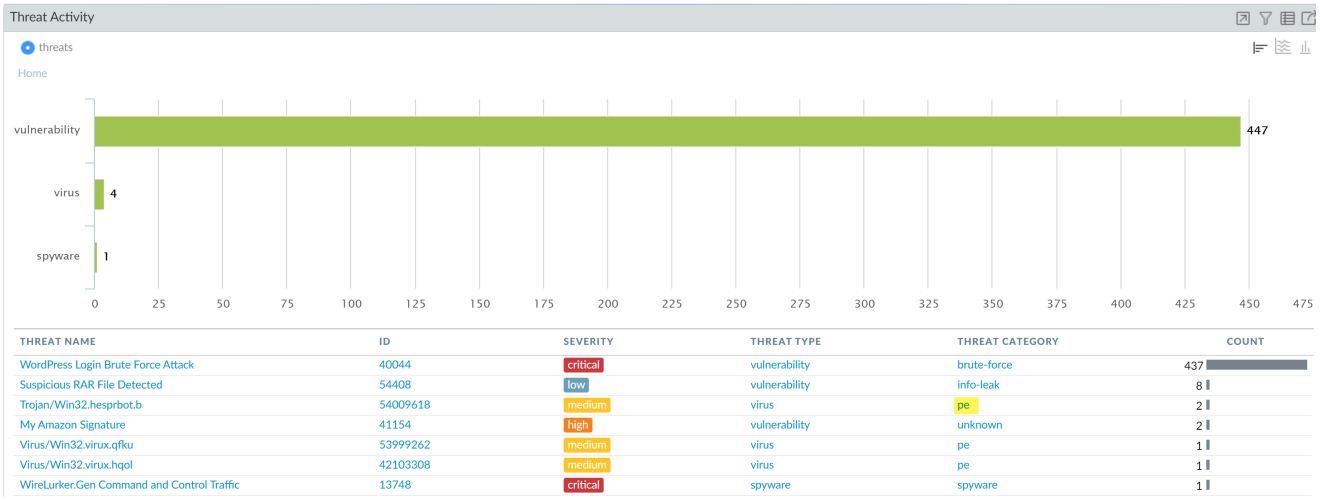


このデータから、ネットワーク上のユーザーである Marsha が、カナダ、ドイツ、スウェーデン、英国、および米国でセッションを確立したことを確認できます。彼女は各国とのセッションで2つの脅威を記録しました。

脅威という観点から Marsha のアクティビティを把握するために、rapidshare のグローバル フィルタを削除します。

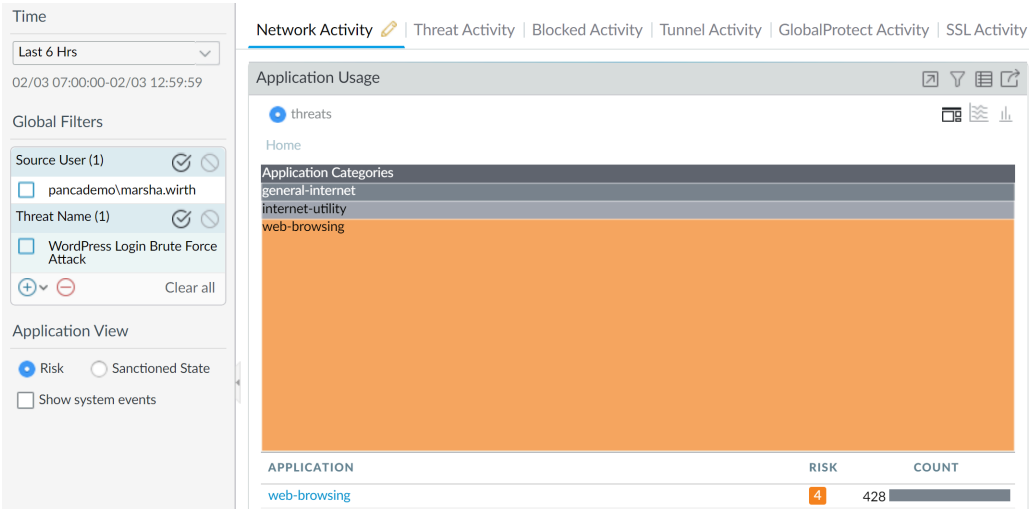


Threat Activity [脅威アクティビティ]タブの **Threat Activity** [脅威アクティビティ]ウィジットで、脅威を確認します。このウィジェットは、彼女のアクティビティがブルートフォース、情報漏洩、ポータブル実行可能(PE)、スパイウェア脅威カテゴリの452の脆弱性に対する一致を引き起こしたことを示しています。これらの脆弱性のいくつかは、重大度が「重要」に設定されています。



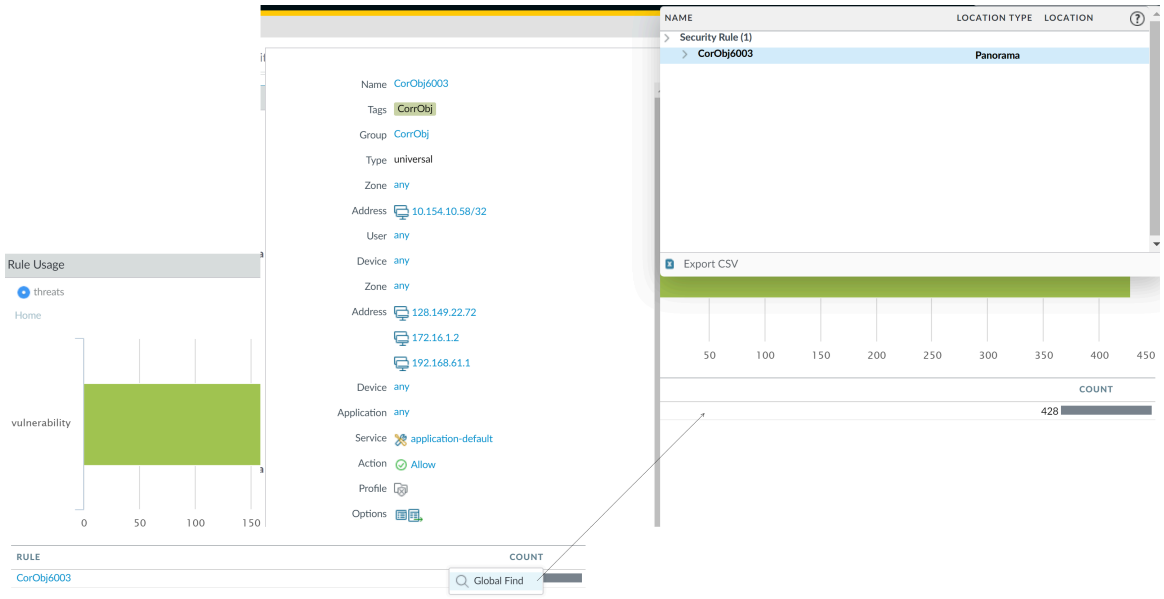
各脆弱性にさらにドリルダウンするために、グラフをクリックして調査の範囲を絞ります。クリックするごとに、ウィジットにローカル フィルタが自動的に適用されます。

名前で各脅威を調査するには、**WordPress** ログイン ブルート フォース攻撃 のグローバル フィルタを作成します。次に、**Network Activity** [ネットワーク アクティビティ]タブの **User Activity widget** [ユーザー アクティビティ]ウィジットを表示します。このタブは、Marsha の脅威アクティビティを表示するように自動的にフィルタリングされています（スクリーンショットのグローバル フィルタを参照）。



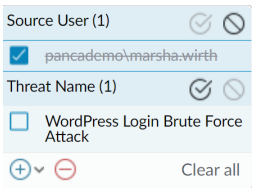
この Microsoft のコード実行脆弱性は、imap アプリケーションによって電子メールを介してトリガーされたことがわかります。これで、Martha に IE の脆弱性と電子メール添付ファイルの脆弱性があり、おそらくコンピュータにパッチを適用する必要があることが判明しました。**Blocked Threats** [ブロックされたアクティビティ]タブの **Blocked Threats** [ブロックされた脅威]ウィジットに移動してこれらの脆弱性のうちブロックされた数を確認できます。

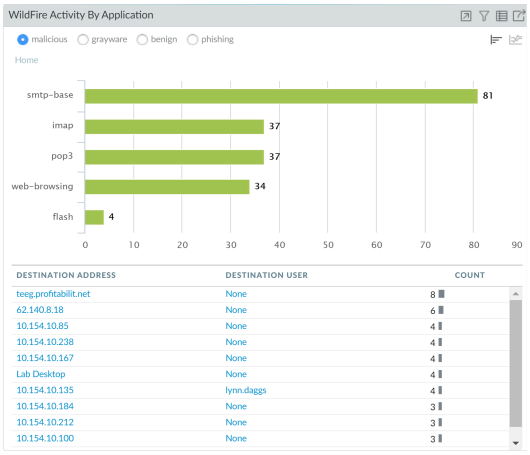
または、**Network Activity** [ネットワーク アクティビティ]タブの **Rule Usage** [ルールの使用状況]ウィジットを確認して、ネットワークに侵入した脆弱性の数と、このトラフィックを許可したセキュリティ ルールを調べ、**Global Find** [グローバル検索]機能を使用してそのセキュリティ ルールに直接移動することができます。



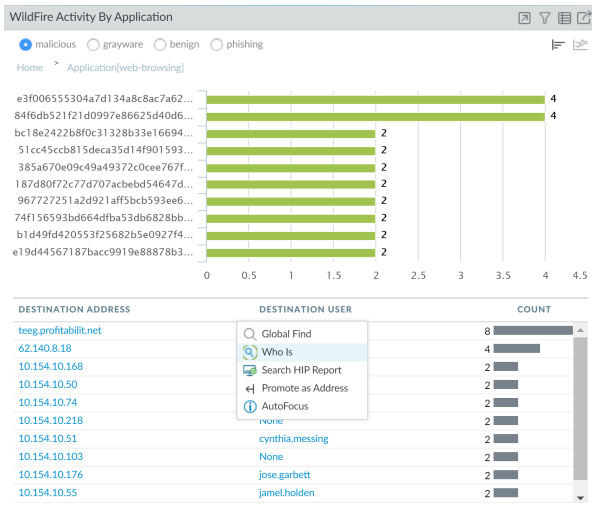
次に、Web ブラウジングを使用して標的となる宛先を攻撃する攻撃者を掘り下げ、攻撃を仕掛けます。これらの悪意のある IP アドレスを制限するようにセキュリティ ポリシールールを変更するか、ネットワーク リソースにアクセスできる IP アドレスをより狭く定義することを検討してください。

Web ブラウジングで脅威が記録されているかどうかを確認するには、**Threat Activity** タブの **WildFire** アクティビティ **(**アプリケーション **)** ウィジェットで Marsha のアクティビティを確認します。Marshaに悪意のあるアクティビティが存在していないのを確認できますが、他のユーザーがウェブブラウジングアプリケーションによって侵害されていないかどうかを確認するには、マーシャをグローバルフィルタとして否定し、Webブラウジング上の脅威を引き起こした他のユーザーを探します。





グラフで imap の棒をクリックし、imap に関連付けられたインバウンドの脅威にドリルインします。IP アドレスが誰に登録されているかを見つけるには、攻撃者の IP アドレスにカーソルを合わせ、ドロップダウンで **Who Is** [担当者]リンクを選択します。



この IP アドレスからのセッション数が多いため、**Blocked Activity (**ブロックされたアクティビティ**)** タブの **Blocked Content (**ブロックされたコンテンツ**)** ウィジットと **Blocked Threats (**ブロックされた脅威**)** ウィジットでこの IP アドレスに関連するイベントを確認します。**Blocked Activity** [ブロックされたアクティビティ]タブでは、ネットワーク上のホストが侵入されたときのコンテンツまたは脅威のブロックにポリシー ルールが有効であるかどうかを検証できます。

ACC の **Export PDF (PDF** のエクスポート**)** 機能を使用して、現在の表示をエクスポート（データのスナップショットを作成）し、問題対応チームに送信します。脅威ログをウィジットから直接表示する場合、アイコンをクリックしてログに移動することもできます。クエリが自動的に生成され、関連するログのみが画面上に表示されます（例は **Monitor (**監視**)** > **Logs (**ログ**)** > **Threat Logs (**脅威ログ**)**の場合）。

これで、ACC を使用してネットワーク データ/トレンドを確認し、最も多くのトラフィックを生成しているアプリケーションまたはユーザーと、ネットワークで確認された脅威の原因となっているアプリケーションの数を調べることができました。トラフィックを生成したアプリケーションやユーザーを識別し、アプリケーションがデフォルト ポートを使用したかどうか、トラフィックがネットワークに入るのを許可したのはどのポリシー ルールか、脅威がネットワーク上で横方向に拡散しているかどうかを判定できました。また、ネットワーク上のホストが通信している宛先 IP アドレスと地理位置も識別しました。調査結果を使用して、ユーザーとネットワークを保護できる明確な目標を持ったポリシーを作成できます。

アプリケーション スコープ レポートの使用

アプリケーション スコープ レポートには、問題の振る舞いを特定することができる可視化ツールと分析ツールが組み込まれており、アプリケーションの使用状況とユーザー アクティビティにおける変化、およびネットワークの帯域幅の大部分を使用しているユーザーとアプリケーションを把握し、ネットワークの脅威を特定することができます。

アプリケーション スコープ レポートを使用すると、異常な挙動または予期しない挙動が容易に確認できます。各レポートには、ネットワークの状況を示す、ユーザーがカスタマイズ可能なダイナミック ウィンドウがあります。チャートの線や棒にポインターを置いてクリックすると、その特定のアプリケーション、アプリケーション カテゴリ、ユーザー、または送信元に関する詳細情報を示したウィンドウが ACC で開きます。**Monitor (監視)** > **App Scope (アプリケーション スコープ)** のアプリケーション スコープのチャートには、以下の機能があります。

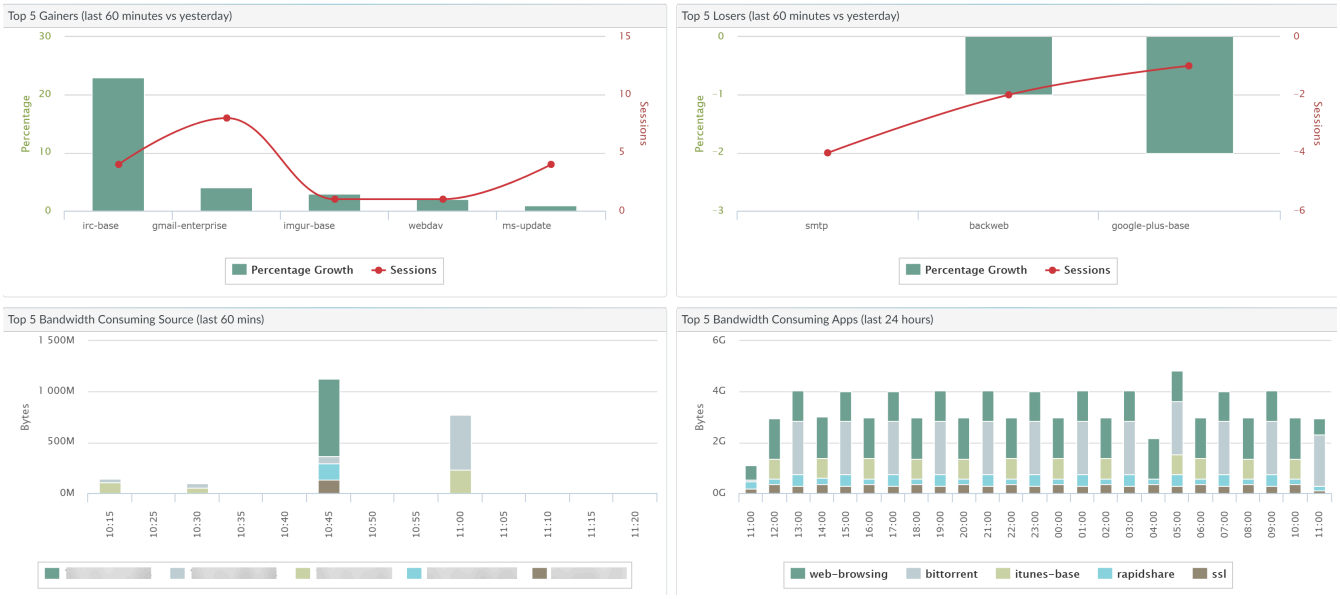
- レビュー対象のチャートの詳細のみを表示するように、凡例の属性を切り替えます。データをチャートに含めるか、またはチャートから除外する機能により、尺度を変更したり、情報をより詳細にレビューしたりすることができます。
- 棒グラフ内の属性をクリックし、ACC の関連セッションまでドリルダウンします。任意の棒グラフで、アプリケーション名、アプリケーション カテゴリ、脅威名、脅威カテゴリ、送信元 IP アドレス、または宛先 IP アドレスをクリックして属性に基づいてフィルタリングし、ACC で関連セッションを表示します。
- チャートまたはマップを PDF にエクスポートするか、またはイメージとしてエクスポートします。移植性を高め、オフライン表示を可能にするため、チャートおよびマップを PDF または PNG イメージとしてエクスポートすることができます。

以下のアプリケーション スコープ レポートを使用できます。

- サマリー レポート
- 変化モニター レポート
- 脅威モニター レポート
- 脅威マップ レポート
- ネットワーク モニター レポート
- トラフィック マップ レポート

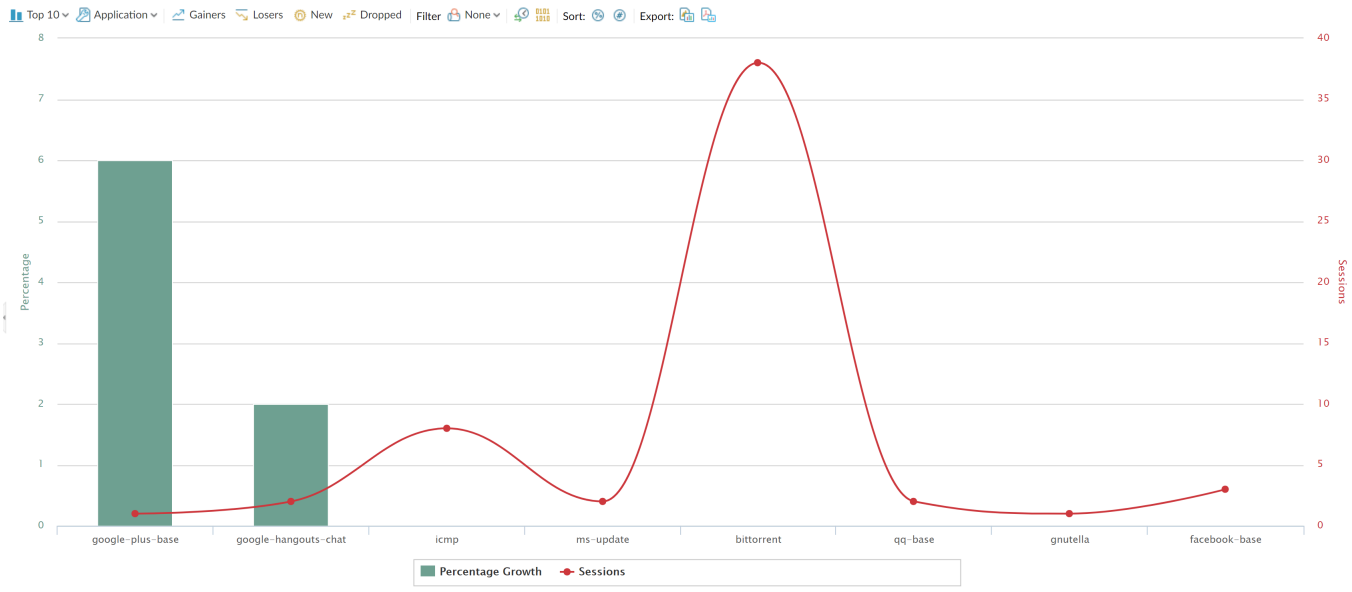
サマリー レポート

アプリケーション スコープ サマリー レポート（**Monitor (監視)** > **App Scope (アプリケーション スコープ)** > **Summary**）には、使用量が増加した、減少した、および帯域幅の占有量が多い上位 5 つのアプリケーション、アプリケーション カテゴリ、ユーザー、および送信元のチャートが表示されます。



変化モニター レポート

アプリケーション スコープ変化モニター レポート（**Monitor (監視)** > **App Scope (アプリケーション スコープ)** > **Change Monitor (変化モニター)**）には、指定した期間の変化が表示されます。たとえば、以下のチャートは、過去 24 時間と比較して直前の 1 時間に使用量が増加した上位のアプリケーションを示しています。上位のアプリケーションはセッション数によって決定され、パーセント別にソートされます。

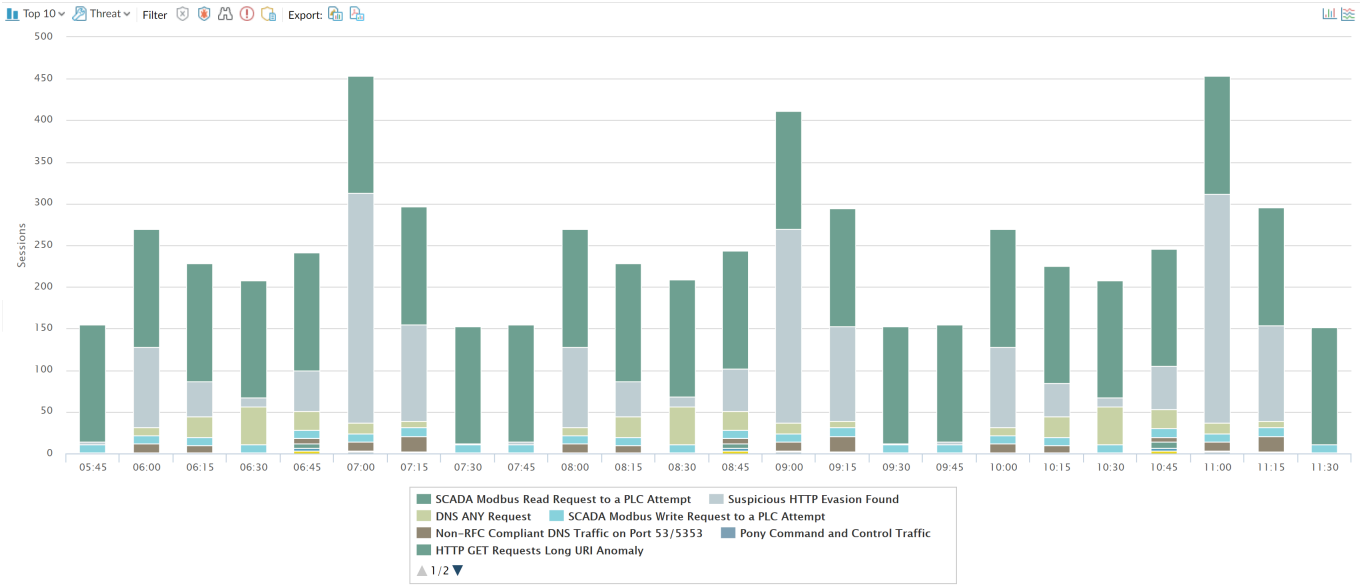


変化モニター レポートには、以下のボタンとオプションが表示されます。

ボタン	説明
トップ **10**	上位からいくつの項目を表に表示するかを指定します。
Application [アプリケーション**]**	レポートに含める項目を指定します。Application[アプリケーション]、Application Category[アプリケーションカテゴリ]、Source[送信元]、Destination[宛先]
増加アプリケーション	指定期間を比較し増加した項目を表示します。
利用が減ったアプリケーション	指定期間を比較し減少した項目を表示します。
新規	指定期間を比較し新たに検出された項目を表示します。
破棄	指定期間を比較し検出されなくなった項目を表示します。
フィルタ	フィルタを適用して、選択した項目のみを表示します。None (なし) を選択すると、すべてのエントリが表示されます。
	セッション情報またはバイト情報のどちらを表示するかを指定します。
ソート	パーセンテージまたは実増加のどちらでエントリをソートするかを指定します。
エクスポート	グラフを .png イメージまたは PDF としてエクスポートします。
比較	変化モニターの比較対象期間を指定します。

脅威モニター レポート

アプリケーション スコープ脅威モニター レポート（**Monitor (**監視**)** > **App Scope (**アプリケーション スコープ**)** > **Threat Monitor (**脅威モニター**)**）には、選択した期間にわたって上位を占める脅威の数が表示されます。たとえば、以下の図は、過去 6 時間における上位 10 件の脅威タイプを示しています。



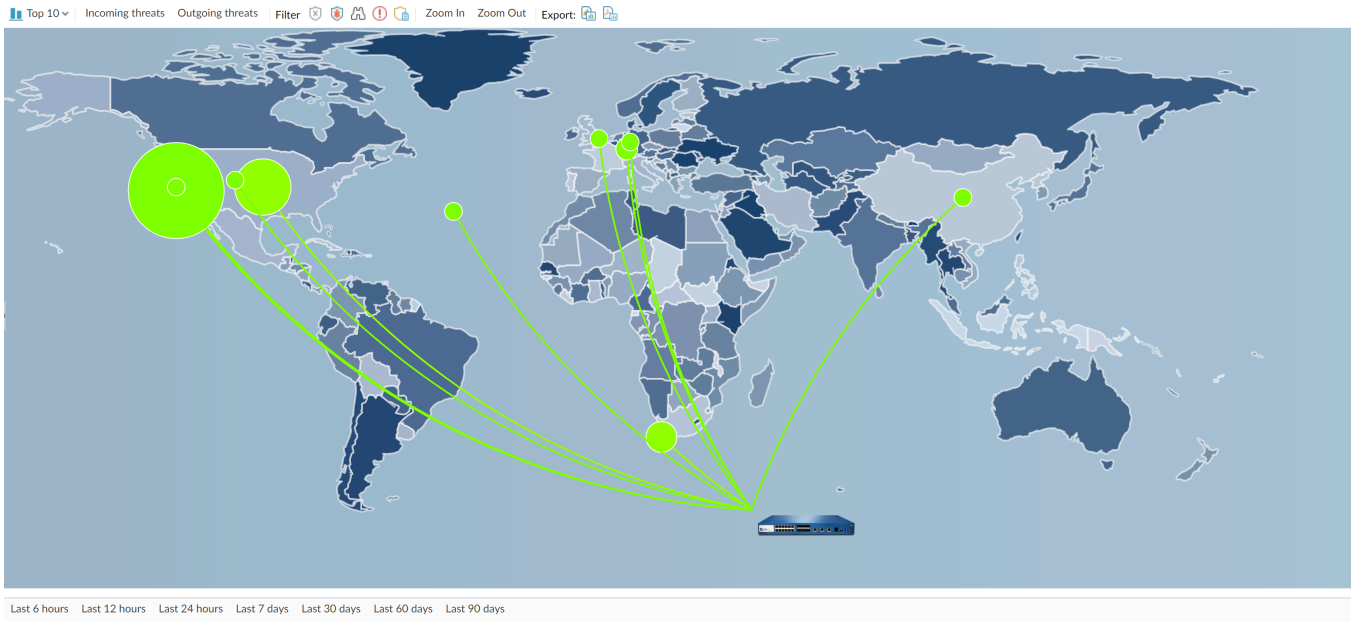
チャートの下の凡例のように、各タイプの脅威が色分けして示されます。脅威モニター レポートには、以下のボタンとオプションが表示されます。

ボタン	説明
トップ **10**	上位からいくつの項目を表に表示するかを指定します。
脅威	測定する項目を指定します。Threat[脅威]、Threat Category[脅威カテゴリ]、Source[送信元]、Destination[宛先]
フィルタ	フィルタを適用して、選択した種別の項目のみを表示します。
	情報を表示するグラフ（積み重ね棒グラフまたは積み重ね面グラフ）を指定します。
エクスポート	グラフを .png イメージまたは PDF としてエクスポートします。
	表示対象期間を指定します。

脅威マップ レポート

アプリケーション スコープ脅威マップ レポート（（**Monitor (監視)** > **App Scope (アプリケーション スコープ)** > **Threat Map (脅威マップ)**）には、重大度を含めた脅威の地理的ビューが表示されます。チャートの下の凡例のように、各タイプの脅威が色分けして示されます。

ファイアウォールでは、脅威マップを作成する場合にデバイス稼働場所を使用します。ファイアウォールでデバイス稼働場所の座標を指定していない場合（**Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)**の General Settings (一般設定) セクション）、そのファイアウォールは脅威マップ画面の最下部に配置されます。

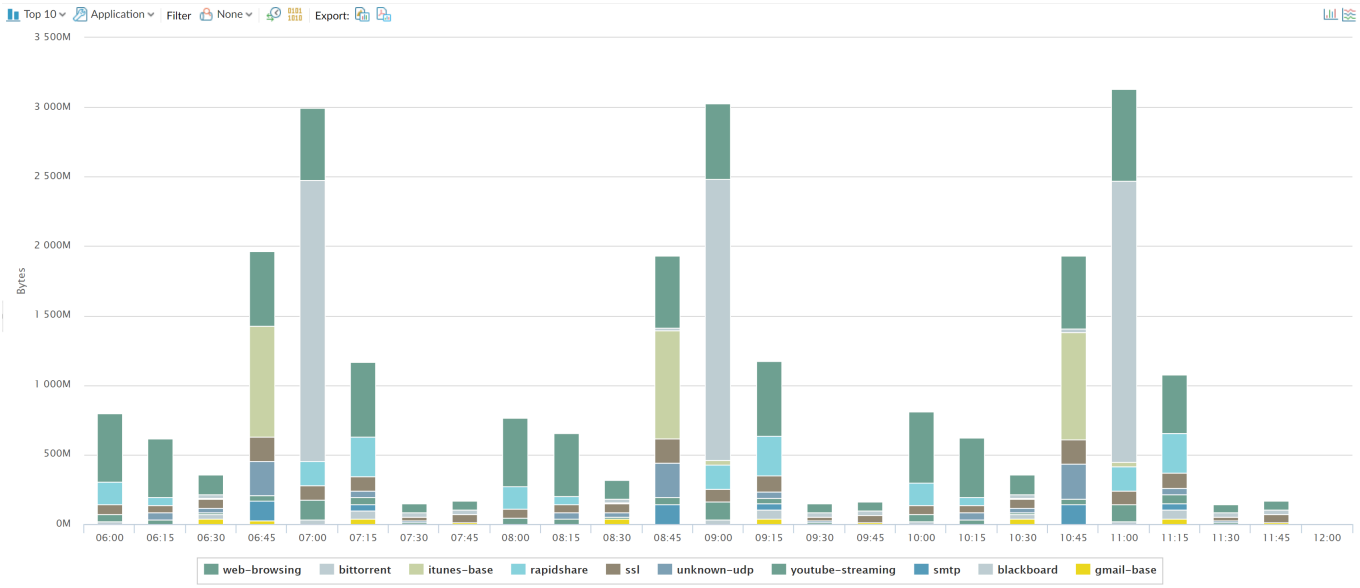


脅威マップ レポートには、以下のボタンとオプションが表示されます。

ボタン	説明
トップ **10**	上位からいくつの項目を表に表示するかを指定します。
受信した脅威	インバウンド方向（外部から）の脅威を示します。
送信した脅威	アウトバウンド方向（外部へ）の脅威を示します。
ファイル	フィルタを適用して、選択した種別の項目のみを表示します。
ズームインおよびズームアウト	マップを拡大および縮小します。
エクスポート	グラフを .png イメージまたは PDF としてエクスポートします。
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	表示対象期間を指定します。

ネットワーク モニター レポート

App Scope Network Monitor (アプリケーション スコープ ネットワーク モニター) レポート（**Monitor (監視)** > **App Scope (アプリケーション スコープ)** > **Network Monitor (ネットワーク監視)**）には、指定した期間にわたって複数のネットワーク アプリケーションによって占有されていた帯域幅が表示されます。図の下の凡例のように、各タイプのネットワーク アプリケーションが色分けして示されます。たとえば、以下の図は、セッション情報に基づく過去 7 日間のアプリケーション帯域幅を示しています。



ネットワーク モニター レポートには、以下のボタンとオプションがあります。

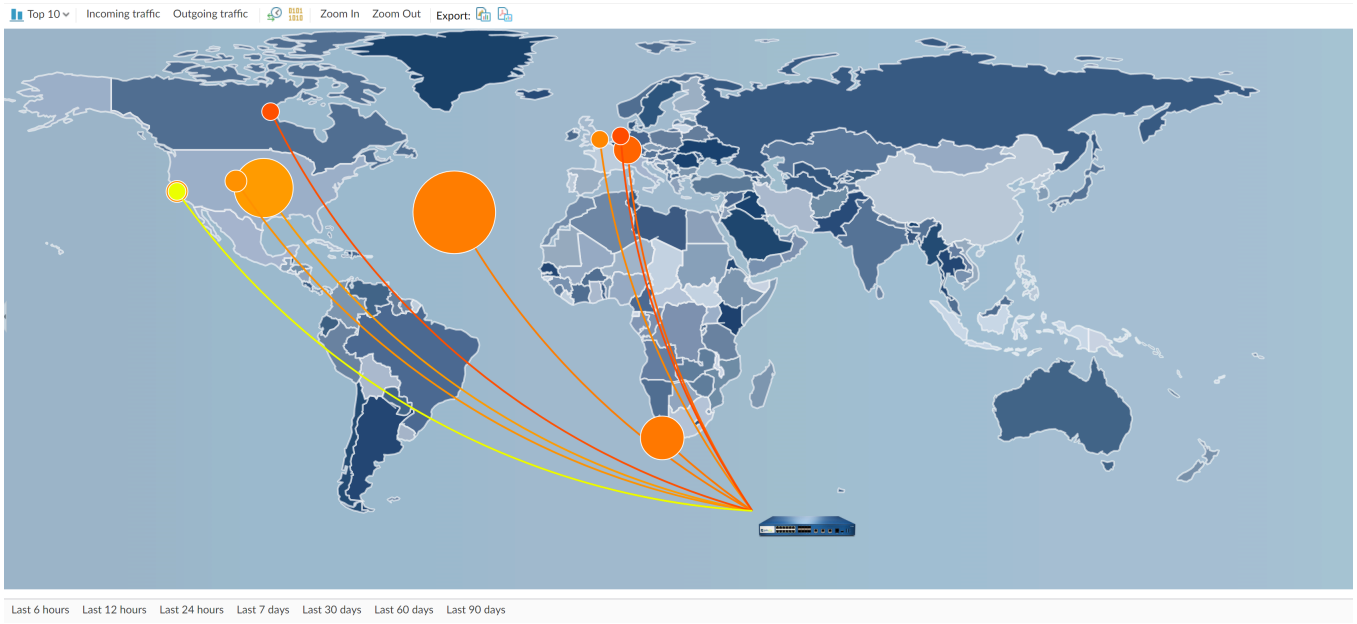
ボタン	説明
トップ **10**	上位からいくつの項目を表に表示するかを指定します。
Application [アプリケーション]	レポートに含める項目を指定します。Application[アプリケーション]、Application Category[アプリケーションカテゴリ]、Source[送信元]、Destination[宛先]
フィルタ	フィルタを適用して、選択した項目のみを表示します。**None**（なし）を選択すると、すべてのエントリが表示されます。
	セッション情報またはバイト情報のどちらを表示するかを指定します。
エクスポート	グラフを .png イメージまたは PDF としてエクスポートします。

ボタン	説明
	情報を表示するグラフ（積み重ね棒グラフまたは積み重ね面グラフ）を指定します。
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	変更措置が取られる期間を示します。

トラフィック マップ レポート

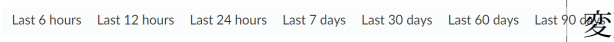
アプリケーション スコープ トラフィック マップ（**Monitor (監視)** > **App Scope (アプリケーション スコープ)** > **Traffic Map (トラフィック マップ)**）には、セッション数またはフロー数に応じて、トラフィック フローの地理的ビューが表示されます。

ファイアウォールでは、トラフィック マップを作成する場合にデバイス稼働場所を使用します。ファイアウォールでデバイス稼働場所の座標を指定していない場合（**Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)**, の General Settings (一般設定) セクション）、そのファイアウォールはトラフィック マップ画面の最下部に配置されます。



チャートの下の凡例のように、各タイプのトラフィックが色分けして示されます。トラフィック マップ レポートには、以下のボタンとオプションがあります。

ボタン	説明
トップ **10**	上位からいくつの項目を表に表示するかを指定します。
受信した脅威	インバウンド方向（外部から）の脅威を示します。
送信した脅威	アウトバウンド方向（外部へ）の脅威を示します。

ボタン	説明
	セッション情報またはバイト情報のどちらを表示するかを指定します。
ズームインおよびズームアウト	マップを拡大および縮小します。
エクスポート	グラフを .png イメージまたは PDF としてエクスポートします。
	変更措置が取られる期間を示します。

自動相関エンジンの使用

自動相関エンジンは、ファイアウォールのログを使用してネットワーク上の実行可能なイベントを検出する分析ツールです。このエンジンは、一連の関連する脅威イベントを相関付けます。これらのイベントは、組み合わせることで、ネットワーク上のホストが侵入されている可能性が高いことや、その他のより重大な結論を示します。ネットワーク上の侵入されたホストなど、リスクのある領域が特定されることで、ユーザーはリスクを評価し、ネットワーク リソースの悪用を防止するためのアクションを実行できるようになります。自動相関エンジンは、相関オブジェクトを使用してログを分析し、パターン マッチがあると、相関されたイベントを生成します。

以下のモデルは自動相関エンジンをサポートします。

- *Panorama – M-Series* アプライアンスおよびバーチャル アプライアンス
- *PA-7000* シリーズ ファイアウォール
- *PA-5450* ファイアウォール
- *PA-5200* シリーズ ファイアウォール
- *PA-3200* シリーズ ファイアウォール

- 自動相関エンジンの概念
- 相関オブジェクトの表示
- 相関されたイベントの解釈
- ACC での Compromised Hosts [侵入されたホスト]ウィジットの使用

自動相関エンジンの概念

自動相関エンジンは、相関オブジェクトを使用してログを分析し、パターン マッチがあると、相関されたイベントを生成します。

- 相関オブジェクト
- 相関されたイベント

相関オブジェクト

相関オブジェクトは定義ファイルです。照合するパターンや検索で使用するデータ ソース、パターンを検索する期間が指定されています。パターンは Boolean 構造の条件で、ファイアウォール上のアプリケーション統計、トラフィック、トラフィック サマリー、脅威サマリー、脅威、データ フィルタリング、URL フィルタリングなどのデータ ソース (またはログ) に対してクエリを発行します。各パターンには重大度評価とパターン マッチ回数のしきい値があり、定義された制限時間内にしきい値を超えた回数一致すると悪意のあるアクティビティであると示します。一致条件に適合すると、相関されたイベントがログに記録されます。

相関オブジェクトは、孤立したネットワーク イベントを関連付け、より重要なイベントを示すパターンを探します。これらのオブジェクトは疑わしいトラフィック パターンやネットワークの異常性 (怪しい IP アクティビティ、既知のコマンド アンド コントロール アクティビティ、既

知の脆弱性悪用、ボットネット アクティビティなど) を特定します。これらのアクティビティに相関関係が認められると、ネットワーク上のホストが侵害されている可能性が高くなります。相関オブジェクトは、Palo Alto Networks の脅威調査チームによって定義および開発され、週次ダイナミック更新でファイアウォールおよび Panorama に配信されます。新しい相関オブジェクトを入手するには、ファイアウォールに脅威防御ライセンスが必要です。Panorama で更新を取得するには、サポート ライセンスが必要です。

相関オブジェクトには静的または動的なパターンが定義されています。WildFire で観測されたパターンを含む相関オブジェクトはダイナミックで、WildFire で検出されたマルウェア パターンを、ネットワーク上のマルウェアで標的にされたホストから開始されたコマンドアンドコントロール アクティビティあるいはTraps で保護される Panorama 上のエンドポイントで発見されたアクティビティに関連付けることができます。例えば、ホストがファイルを WildFire クラウドに送信し、それが有害であると判定されたとき、相関オブジェクトはクラウド内で同じ挙動を示すネットワーク上の他のホストやクライアントを探します。マルウェアのサンプルが DNS クエリを実行し、マルウェア ドメインを参照した場合、相関オブジェクトはログを解析して類似のイベントを探します。ホスト上のアクティビティがクラウドの分析と一致すると、重大度の高い相関されたイベントがログに記録されます。

相関されたイベント

相関されたイベントは、相関オブジェクトに定義されたパターンとしきい値がネットワーク上のトラフィック パターンと一致した場合にログに記録されます。イベントを相関されたイベントの解釈およびグラフィカル表示を表示するには、「ACC での Compromised Hosts [侵入されたホスト]ウィジットの使用」を参照してください。

相関オブジェクトの表示

現在ファイアウォール上で利用できる相関オブジェクトを表示できます。

STEP 1 | **Monitor (監視)** > **Automated Correlation Engine (自動相関エンジン)** > **Correlation Objects (オブジェクト)**を選択します。リスト上のオブジェクトはすべてデフォルトで有効になっています。

TITLE	CATEGORY	STATE	DESCRIPTION
Multiple User from One Endpoint MFA Credential Theft	credential-theft-abuse	active	This correlation object detects multiple account abuse from a possibly compromised endpoint
WildFire C2	compromised-host	active	This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network.
WildFire and Traps ESM Correlated C2	compromised-host	active	This correlation object detects hosts that have received malware detected by WildFire or executed malware as seen by Traps, and have also exhibited command- and-control (C2) network behavior corresponding to the detected malware.
Single Account and Endpoint MFA Credential Theft	credential-theft-abuse	active	This correlation object detects activity from a possibly compromised user account from a single endpoint
Compromise Activity Sequence	compromised-host	active	This correlation object detects a host involved in a sequence of activity indicating remote compromise, starting with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain.
Exploit Kit Activity	compromised-host	active	This object detects probable exploit kit activity targeted at a host on the network. Exploit kits are identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
Single Account 1 FA Multiple Endpoints Credential Timeouts	credential-theft-abuse	active	This correlation object detects timed out attempts of first factor authentications from multiple endpoints using a single user account
Beacon Detection	compromised-host	active	This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.
Single Account and Endpoint MFA Credential Timeout	credential-theft-abuse	active	This correlation object detects timedout MFA authentication attempts from a single endpoint using single account
Multiple Endpoint MFA Credential Timeout Abuse	credential-theft-abuse	active	This correlation object detects timed out second factor authentications from multiple endpoints using a single user account
Multiple Endpoint MFA Credential Abuse	credential-theft-abuse	active	This correlation object detects activity from multiple endpoints using a single user account
Exploit Kit Delivering XOR obfuscated malware	compromised-host	active	This correlation object detects exclusive-or (XOR) obfuscated malware downloaded to a host. XOR obfuscation is a technique to evade detection by encrypting portions of a file in order to hide malicious code. This correlation object specifically identifies XOR obfuscated malware that is delivered to the host by an exploit kit. While the Exploit Kit Activity object detects exploit kits combined with either a malware download signature or a known command-and-control signature, this object is provided to specifically detect an event where XOR obfuscation malware inserted on a host by an exploit kit and to distinguish such an event from other exploit kit activities.
Single Account 1 FA Credential Abuse	credential-theft-abuse	active	This correlation object detects timed out first factor authentications from an endpoint using a single user account

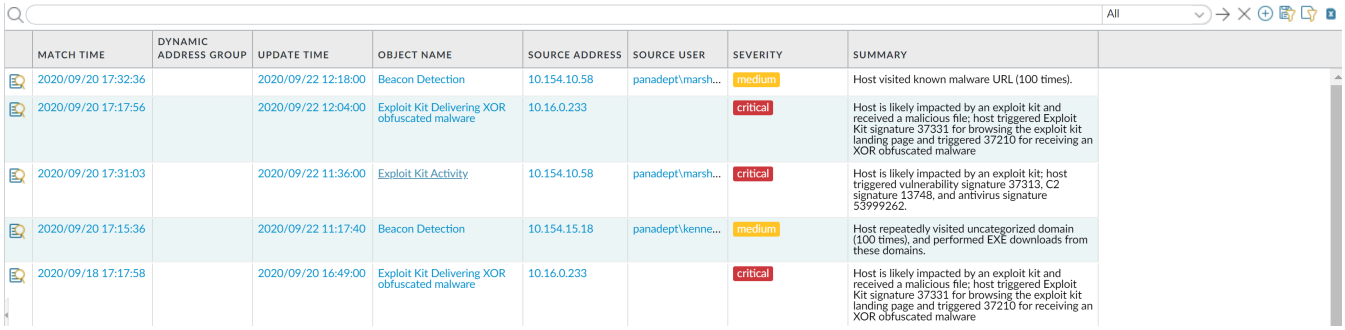
STEP 2 | 各相関オブジェクトの詳細を表示します。各オブジェクトでは、以下の情報が提供されます。

- **Name (名前)** と **Title (タイトル)**—名前とタイトルは、相関オブジェクトで検出するアクティビティのタイプを示します。Name [名前]列はデフォルトで非表示になっています。オブジェクトの定義を表示するには、Name [名前]列を表示して、名前のリンクをクリックします。
- **ID** — 相関オブジェクトを識別する一意の数値。この列もデフォルトで非表示になっています。ID は、6000 番台です。
- **Category (カテゴリ)** — ネットワーク、ユーザー、またはホストに与える脅威または損害の種類の分類。現時点では、すべてのオブジェクトがネットワーク上の侵入されたホストを識別します。
- **State (状態)** — 相関オブジェクトが有効（アクティブ）か無効（非アクティブ）かを示します。リスト上のオブジェクトはすべてデフォルトで有効（アクティブ）になっています。これらのオブジェクトは、脅威インテリジェンス データに基づいており、Palo Alto Networks 脅威調査チームによって定義されているため、ネットワーク上の有害なアクティビティを追跡および検出するためにオブジェクトは常時アクティブにしておきます。
- **Description (説明)** — ファイアウォールまたは Panorama でログを分析するための対象となる一致条件を指定します。有害なアクティビティまたは疑わしいホストの動作の加速または拡散を識別するために照合される、一連の条件を記述するものです。たとえば、**Compromise Lifecycle** [侵入ライフサイクル]オブジェクトは、3 ステップの拡散からなる完全な攻撃ライフサイクルに関与しているホストを検出します。このライフサイクルは、スキャンまたはプロービング アクティビティで開始し、悪用へと発展し、最終的にネットワークを既知の有害なドメインに接続します。

詳細については、自動相関エンジンの概念および自動相関エンジンの使用を参照してください。

相関されたイベントの解釈

Monitor (監視) > **Automated Correlation Engine (自動相関エンジン)** > **Correlated Events (相関されたイベント)** タブで、相関されたイベントごとに生成されたログを表示および分析できます。

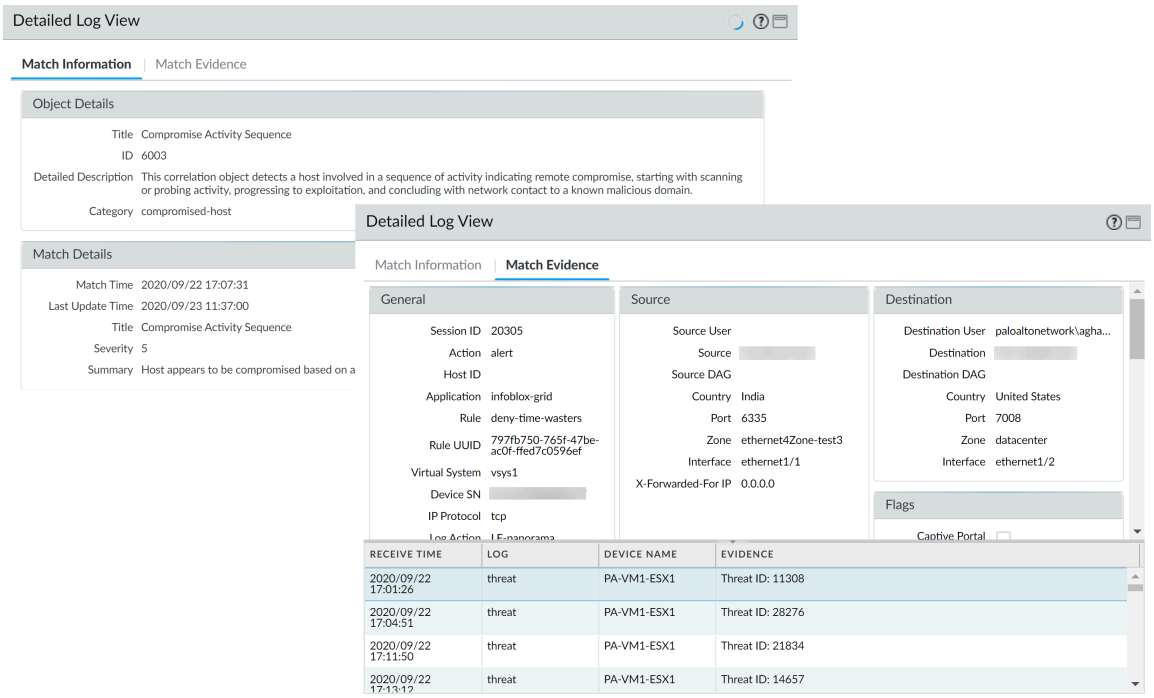


相関されたイベントには、次の詳細が含まれています。

項目	の意味
一致時間	相関オブジェクトが一致をトリガーした時間。
Update Time（更新時間）	一致に関する証拠でイベントが最後に更新された時刻。ファイアウォールが相関オブジェクトに定義されたパターンまたは一連のイベントに関する証拠を収集すると、相関されたイベント ログのタイム スタンプが更新されます。
Object Name（オブジェクト名）	一致をトリガーした相関オブジェクトの名前。
送信元アドレス	トラフィックの送信元であるネットワーク上のユーザー/デバイスの IP アドレス。
送信元ユーザー	ディレクトリー・サーバーからのユーザーおよびユーザー・グループ情報 (User-IDが使用可能になっている場合)。
重大度	一致の緊急性と影響を示す評価。重大度レベルは、損害や拡散パターンの程度と発生頻度を示します。相関オブジェクトは主に脅威の検出を目的としているため、通常、相関されたイベントは、ネッ

項目	の意味
電子メール、*SNMP*、または *syslog* メッセージを使用して目的の重大度レベルに対してアラートを送信するように *firewall* または *Panorama* を構成するには、モニタリングでの外部サービスの使用を参照してください。	トワーク上の侵入されたホストの識別に関連し、重大度は以下の意味を持ちます。 • **Critical**[重要] – 拡散パターンを示す相関イベントに基づいて、ホストが侵入されたことが確認されました。たとえば、WildFire によって有害と判定されたファイルをホストが受信し、WildFire サンドボックスでその有害ファイルのコマンド アンド コントロール活動として確認されたものと同じ活動がホストで示された場合、重要イベントがログに記録されます。 • **High** [高] – 複数の脅威イベント間の相関に基づいて、ホストが侵入された可能性が高いことを示します。たとえば、ネットワーク上の任意の場所で検出されたマルウェアが、特定のホストによって生成されたコマンド アンド コントロール アクティビティと一致する場合です。 • **Medium** [中] – 1 つまたは複数の疑わしいイベントの検出に基づいて、ホストが侵入された可能性があることを示します。たとえば、スクリプト化されたコマンド アンド コントロール アクティビティを示している既知の有害な URL への頻繁なアクセスがある場合です。 • **Low**[低] – 1 つまたは複数の疑わしいイベントの検出に基づいて、ホストが侵入されたと考えられることを示します。たとえば、有害な URL やダイナミック DNS ドメインへのアクセスがあった場合です。 • **Informational** [情報] – 集合体として疑わしいアクティビティの識別に役立つ可能性があるイベントを検出します。各イベントはそれ自体が必ずしも重要ではありません。
概要	相関されたイベントに関して収集された証拠を要約する説明。

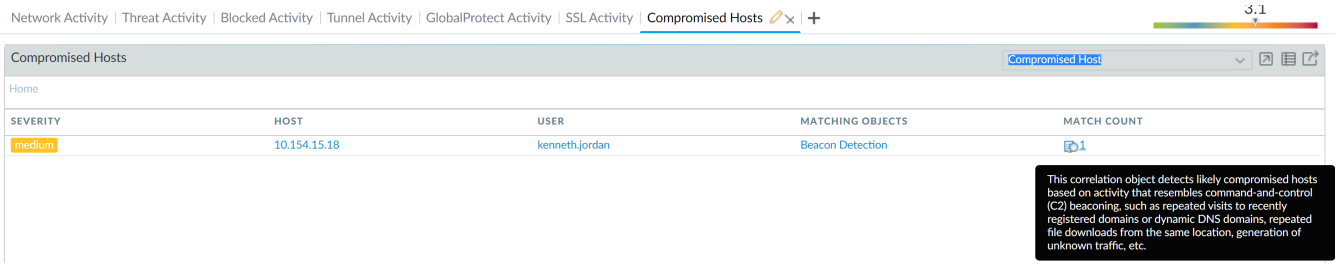
一致に関するすべての証拠が含まれる詳細ログ ビューを表示するには、 アイコンをクリックします。



タブ	の意味
Match Information（一致情報）	オブジェクトの詳細一致をトリガーした相関オブジェクトに関する情報を表示します。
	一致の詳細Match Details [一致の詳細]: 一致時間、一致の証拠の最終更新時間、イベントの重大度、イベントのサマリーを含む、一致の詳細のサマリー。
Match Evidence（一致の根拠）	相関されたイベントを裏付けるすべての証拠が表示されます。セッションごとに収集された証拠に関する詳細情報が表示されます。

ACC での Compromised Hosts [侵入されたホスト]ウィジットの使用

ACC > **Threat Activity** の侵害されたホスト ウィジェットは、相関されたイベントを集約し、重大度で並べ替えます。イベントをトリガーした送信元 IP アドレス/ユーザー、一致した相関オブジェクト、オブジェクトが一致した回数が表示されます。一致の証拠に関する詳細情報に移動するには、一致数のリンクを使用します。



詳細については、自動相関エンジンの使用とアプリケーション コマンド センターの使用を参照してください。

パケット キャプチャの実行

すべての Palo Alto Networks ファイアウォールでは、ファイアウォールの管理インターフェイスとネットワーク インターフェイスを通過するトラフィックのパケット キャプチャ（pcap）を実行できます。データプレーンでパケット キャプチャを実行する場合、ファイアウォールがすべてのトラフィックをキャプチャするようにハードウェア オフロードの無効化する必要がある場合があります。

パケット キャプチャを使用すると *CPU* に大きな負荷がかかるため、ファイアウォールのパフォーマンスが低下する可能性があります。必要な場合にのみ、この機能を使用してください。また、必要なパケットを収集した後は、この機能を必ずオフにしてください。

- パケット キャプチャのタイプ
- ハードウェア オフロードの無効化
- カスタム パケット キャプチャの実行
- 脅威パケット キャプチャの実行
- アプリケーション パケット キャプチャの実行
- 管理インターフェイスでのパケット キャプチャの実行

パケット キャプチャのタイプ

必要に応じて、有効にできるパケット キャプチャにはさまざまな種類があります。

- カスタム パケット キャプチャ – ファイアウォールはすべてのトラフィックのパケットか、定義したフィルタに基づいて特定のトラフィックのパケットをキャプチャします。たとえば、特定の送信元および宛先の IP アドレスまたはポートとの間でやりとりされるパケットのみをキャプチャするようにファイアウォールを設定できます。そうすることで、パケット キャプチャを使用して、ネットワーク関連の問題をトラブルシューティングできます。アプリケーション属性を収集してカスタム アプリケーション シグネチャを作成したり、Palo Alto Networks にアプリケーション シグネチャを要求したりすることもできます。カスタム パケット キャプチャの実行を参照してください。
- 脅威パケット キャプチャ – ファイアウォールは、ウイルス、スパイウェア、または脆弱性を検出するとパケットをキャプチャします。この機能は、アンチウイルス、アンチスパイウェア、および脆弱性防御のセキュリティ プロファイルで有効にします。パケット キャプチャを表示またはエクスポートするためのリンクが、脅威ログの 2 列目に表示されます。これらのパケット キャプチャによって、脅威を取り巻く状況が提供されるため、攻撃が成功したかどうかを判断したり、攻撃者が使用した方法について詳細を確認したりできます。誤検知や検出もれと思われる場合、このタイプの pcap を Palo Alto Networks に送信して脅威の再分析を依頼することもできます。脅威パケット キャプチャの実行を参照してください。
- アプリケーション パケット キャプチャ – ファイアウォールは、特定のアプリケーションおよび定義したフィルタに基づいてパケットをキャプチャします。パケット キャプチャ ルールに一致したトラフィックについて、パケット キャプチャを表示またはエクスポートするため

のリンクが、トラフィック ログの 2 列目に表示されます。アプリケーション パケット キャプチャの実行を参照してください。

- 管理インターフェイスパケット キャプチャ—ファイアウォールは管理インターフェイス (MGT) のパケットをキャプチャします。パケット キャプチャは、外部認証サービスへの firewall 管理認証、ソフトウェアおよびコンテンツの更新、ログ転送、SNMP サーバーとの通信、GlobalProtect および Authentication Portal の認証要求など、インターフェイスを通過するサービスのトラブルシューティングに役立ちます。管理インターフェイスでのパケット キャプチャの実行を参照してください。
- **GTP** イベントパケットキャプチャ—ファイアウォールは、GTP-in-GTP、エンドユーザ IP スプーフィング、および異常な GTP メッセージなどの単一の GTP イベントをキャプチャして、モバイルネットワークオペレータにとって GTP のトラブルシューティングを容易にします。モバイル ネットワーク保護プロファイルでパケット キャプチャを有効にします。

ハードウェア オフロードの無効化

Palo Alto Networks ファイアウォールのネットワーク データ ポートを通過するトラフィックのパケット キャプチャは、データプレーン CPU によって実行されます。管理インターフェイスを通過するトラフィックをキャプチャするには、管理インターフェイスでパケット キャプチャを実行する必要があります。この場合、パケット キャプチャは管理プレーン上で実行されます。

パケット キャプチャがデータプレーン上で実行されると、パケット キャプチャフィルタは、入力ステージによって、ファイアウォール、ドロップ、および出力キャプチャ ステージとは異なって使用されます。入力ステージでは、パケット キャプチャ フィルタを使用して、フィルタに一致する個々のパケットをキャプチャ ファイルにコピーします。パケット解析チェックに失敗したパケットは、キャプチャされる前に破棄されます。ファイアウォール、破棄、および出力キャプチャ ステージでは、同じパケット キャプチャ フィルタを使用して、フィルタに一致するすべての新しいセッションをマーキングします。セッション テーブルに記録されている各セッションは、クライアントからサーバーへの接続とサーバーからクライアントへの接続の両方を識別するため、フラグが付けられたセッションと一致するいずれかの方向のトラフィックはファイアウォール ステージと転送ステージ キャプチャ ファイルにコピーされます。同様に、フラグが設定されたセッションに一致するいずれかの方向に破棄されたトラフィック（受信ステージ後）は、破棄ステージ キャプチャ ファイルにコピーされます。

ネットワーク プロセッサを含むファイアウォール モデルでは、Palo Alto Networks によって特定の所定の基準を満たすトラフィックが、ネットワーク プロセッサによる処理のためにオフロードされる可能性があります。このようなオフロードされたトラフィックは、データプレーン CPU に到達しないため、キャプチャされません。オフロードされたトラフィックをキャプチャするには、CLI を使用してハードウェア オフロード機能をオフにする必要があります。

オフロードされる可能性のある一般的なトラフィックには、SSL/SSH トラフィック（暗号化されていないものは初期 SSL/SSH セッションの設定以外では有効に検査できません）、ネットワーク プロトコル（OSPF、BGP、RIP など）アプリケーションのオーバーライド ポリシー。ARP、すべての非 IP トラフィック、IPSec、および VPN セッションなど、一部のセッション タイプはオフロードされません。個別の SYN、FIN、および RST パケットは、オフロードされたセッション トラフィックであっても、決してオフロードされず、ネットワーク プロセッサによって認識されると常にデータプレーン CPU に渡されます。

以下のファイアウォールがハードウェアオフロードをサポートしています。*PA-3200 Series*、*PA-5200 Series*、*PA-7000 Series*。

ハードウェア オフロードを無効にするとデータプレーン *CPU* 使用率が上昇することがあります。データプレーン *CPU* 使用率がすでに高い場合、ハードウェア オフロードを無効にする前に、メンテナンス時間のスケジュールが必要になる場合があります。

STEP 1 | 以下の CLI コマンドを実行して、ハードウェア オフロードを無効にします。

```
admin@PA-7050>set session offload no
```

STEP 2 | ファイアウォールで必要なトラフィックをキャプチャしたら、以下の CLI コマンドを実行してハードウェア オフロードを有効にします。

```
admin@PA-7050>set session offload yes
```

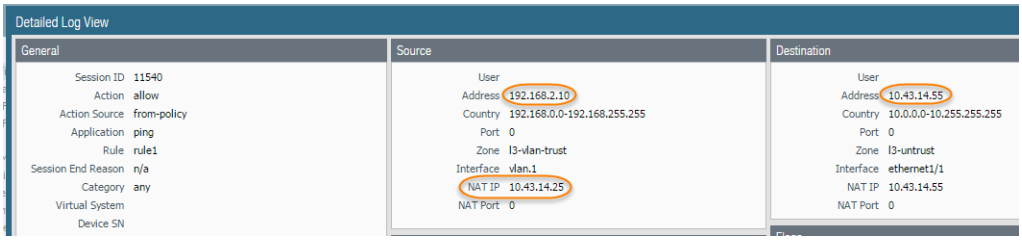
カスタム パケット キャプチャの実行

カスタム パケット キャプチャを使用すると、ファイアウォールでキャプチャするトラフィックを定義できます。すべてのトラフィックを確実にキャプチャするには、ハードウェア オフロードの無効化が必要な場合があります。

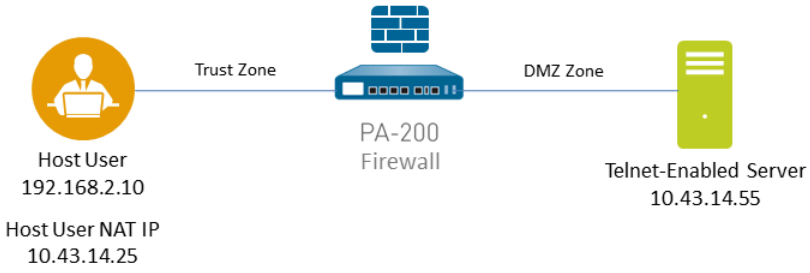
STEP 1 | パケット キャプチャを開始する前に、キャプチャするトラフィックの属性を識別します。

たとえば、2 つのシステム間のトラフィックの送信元 IP アドレス、送信元 NAT IP アドレス、および宛先 IP アドレスを判別するには、送信元システムから宛先システムに Ping を実行します。Ping が完了したら、**Monitor (監視)** > **Traffic (トラフィック)** に移動し、2 つのシステムのトラフィック ログを見つけます。ログの 1 列目にある **Detailed Log View** [詳細ログ

ビュー]アイコンをクリックし、送信元アドレス、送信元 NAT IP アドレス、および宛先アドレスを確認します。



以下は、パケット キャプチャを使用して、Trust ゾーンのユーザーから DMZ ゾーンのサーバーへの Telnet 接続の問題をトラブルシューティングする方法の例です。



STEP 2 | 関心のあるトラフィックのみをファイアウォールがキャプチャするように、パケット キャプチャ フィルタを設定します。

フィルタを使用することで、パケット キャプチャ内で必要な情報を容易に見つけることができます。また、ファイアウォールでパケット キャプチャを実行するために必要な処理能力を

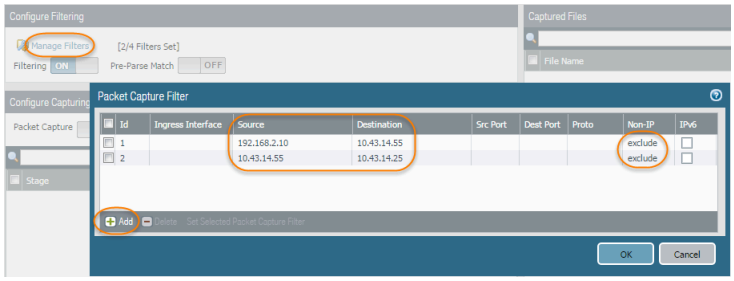
低減できます。すべてのトラフィックをキャプチャするには、フィルタを定義せずに、フィルタ オプションをオフのままにします。

たとえば、ファイアウォールに NAT を設定した場合、2 つのフィルタを適用する必要があります。1 つ目は、宛先 IP アドレスへの NAT 前の送信元 IP アドレスでフィルタリングし、2 つ目は宛先サーバーから送信元 NAT IP アドレスへのトラフィックをフィルタリングします。

1. **Monitor (監視)** > **Packet Capture (パケット キャプチャ)** を選択します。
2. 既存のキャプチャ設定をクリアするには、ウィンドウの下部で **Clear All Settings** [すべての設定をクリア]をクリックします。
3. **Manage Filters** [フィルタの管理]をクリックし、**Add** [追加]をクリックします。
4. **Id** で「1」を選択し、**Source (送信元)** フィールドに関心のある送信元 IP アドレス アドレス、**Destination (宛先)** フィールドに宛先 IP アドレス を入力します。

   たとえば、送信元 IP アドレス「**192.168.2.10**」と宛先 IP アドレス「**10.43.14.55**」を入力します。キャプチャをさらにフィルタリングするには、**Non-IP** [非 IP]を **exclude** に設定してブロードキャスト トラフィックなどの非 IP トラフィックを除外します。
5. 2 つ目のフィルタを**Add (追加)** し、**ID** で「2」を選択します。

   たとえば、**Source** [送信元]フィールドに「**10.43.14.55**」と入力し、**Destination** [宛先]フィールドに「**10.43.14.25**」と入力します。**Non-IP** [非 IP]ドロップダウン メニューで **exclude** を選択します。



6. **OK** をクリックします。

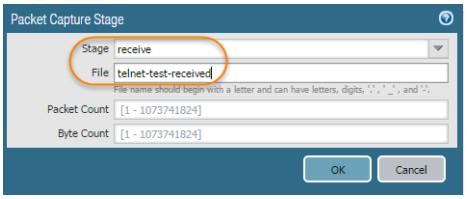
STEP 3 | **Filtering** [フィルタリング]を **On** [オン]に設定します。

STEP 4 | パケット キャプチャをトリガーするトラフィック ステージと、キャプチャしたコンテンツの保存に使用するファイル名を指定します。各ステージを定義するには、パケット キャプチャ ページで **Help** [ヘルプ]アイコンをクリックします。

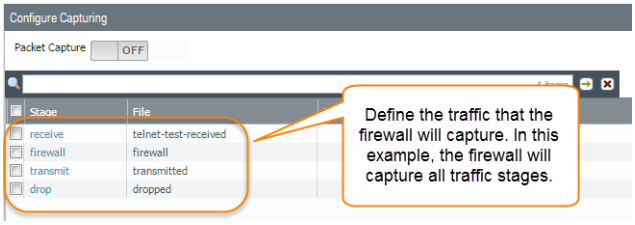
たとえば、すべてのパケット キャプチャ ステージを設定し、各ステージのファイル名を定義するには、以下の手順を実行します。

1. パケット キャプチャ設定に **Stage** （ステージ）を **Add** [追加]し、作成されるパケット キャプチャの **File** （ファイル）名を定義します。

   たとえば、**Stage** （ステージ）で **receive** を選択し、**File** （ファイル）名「telnet-test-received」を入力します。

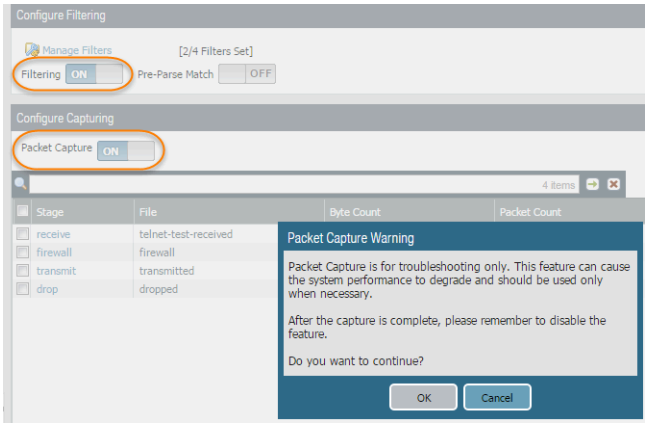


2. 引き続き、キャプチャする各**Stage (**ステージ**)** （**firewall**、**transmit**、**drop**）を **Add (**追加**)** し、各ステージに一意の **File (**ファイル**)** 名を設定します。



STEP 5 | **Packet Capture (**パケット キャプチャ**)** を **ON** に設定します。

システムのパフォーマンスが低下するおそれがあるという警告を、ファイアウォールあるいはアプライアンスが発します。**OK** をクリックして警告を確認してください。フィルタを定義する場合、パケット キャプチャはパフォーマンスにほとんど影響を与えませんが、分析するデータをファイアウォールでキャプチャしたら必ずパケット キャプチャを **Off** [オフ]にする必要があります。

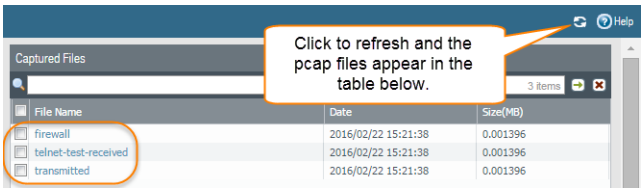


STEP 6 | 定義したフィルタに一致するトラフィックを生成します。

この例では、送信元システム（192.168.2.10）から以下のコマンドを実行して、送信元システムから Telnet 対応サーバーへのトラフィックを生成します。

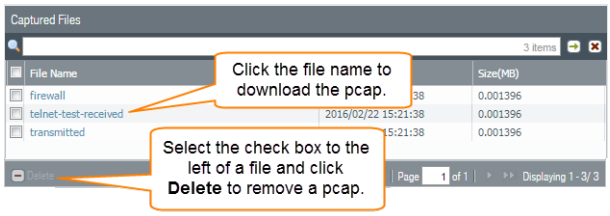
```
telnet 10.43.14.55
```

STEP 7 | パケット キャプチャを **Off** [オフ]にし、更新アイコンをクリックしてパケット キャプチャ ファイルを表示します。



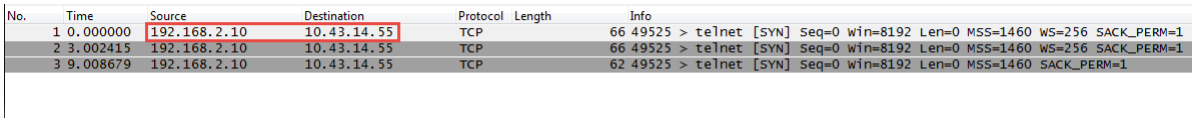
この場合、ドロップされたパケットがないため、ファイアウォールはドロップ ステージ用のファイルを作成しませんでした。

STEP 8 | File Name （ファイル名）列でファイル名をクリックして、パケット キャプチャをダウンロードします。



STEP 9 | Wireshark などのネットワーク パケット アナライザを使用してパケット キャプチャ ファイルを表示します。

この例では、received.pcap パケット キャプチャに、送信元システム（192.168.2.10）から Telnet 対応サーバー（10.43.14.55）への失敗した Telnet セッションが表示されています。送信元システムは、Telnet 要求をサーバーに送信しましたが、サーバーは応答しませんでした。この例では、サーバーで Telnet が有効になっていない可能性があるため、サーバーを確認します。



STEP 10 | 宛先サーバー（10.43.14.55）で Telnet サービスを有効にし、パケット キャプチャをオンにして新しいパケット キャプチャを実行します。

STEP 11 | パケット キャプチャをトリガーするトラフィックを生成します。

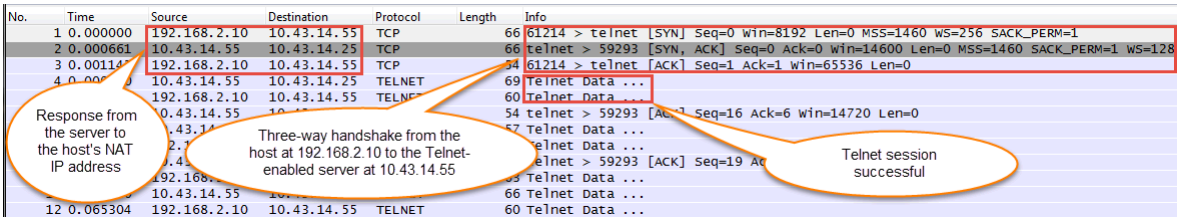
送信元システムから Telnet 対応サーバーへの Telnet セッションを再度実行します。

```
telnet 10.43.14.55
```


STEP 12 | received.pcap ファイルをダウンロードし、ネットワーク パケット アナライザで開いて表示します。

以下のパケット キャプチャでは、ホスト ユーザー（192.168.2.10）から Telnet 対応サーバー（10.43.14.55）への成功した Telnet セッションが表示されています。

NAT アドレス（*10.43.14.25*）も表示されています。サーバーは応答するとき、*NAT* アドレスに応答しています。図のように、ホストとサーバー間のスリーウェイ ハンドシェークによってセッションが成功したことが表示され、その後に *Telnet* データが表示されています。



脅威パケット キャプチャの実行

脅威を検出したらパケット キャプチャ（pcap）を実行するようにファイアウォールを設定するには、アンチウイルス、アンチスパイウェア、および脆弱性防御セキュリティ プロファイルでパケット キャプチャを有効にします。

STEP 1 | セキュリティ プロファイルでパケット キャプチャ オプションを有効にします。

セキュリティ プロファイルによっては、シングル パケット キャプチャ、または拡張キャプチャを定義できます。拡張キャプチャを選択した場合は、キャプチャの長さを定義します。これにより、ファイアウォールでキャプチャするパケットを増やすことができ、脅威に関する追加のコンテキストを得られます。

特定の脅威に対するアクションが許可されている場合、ファイアウォールは脅威ログをトリガせず、パケットもキャプチャしません。アクションがアラートである場合は、パケット キャプチャをシングル パケット キャプチャまたは拡張キャプチャに設定できます。すべてのブロッキングアクション（ドロップ、ブロック、およびリセットアクション）は、単一のパケットをキャプチャします。デバイス上のコンテンツ パッケージは、デフォルトのアクションを決定します。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** を選択し、サポートされているプロファイルのパケット キャプチャ オプションを以下のように有効にします。
   - **Antivirus** [アンチウイルス] – カスタムのアンチウイルス プロファイルを選択し、**Antivirus** [アンチウイルス]タブで **Packet Capture** [パケット キャプチャ]チェック ボックスをオンにします。
   - **Anti-Spyware** [アンチスパイウェア] – カスタムのアンチスパイウェア プロファイルを選択し、**DNS Signatures** [DNS シグネチャ]タブをクリックします。**Packet**

Capture [パケット キャプチャ]ドロップダウンで **single-packet** または **extended-capture** を選択します。

- **Vulnerability Protection** [脆弱性防御] — カスタムの脆弱性防御プロファイルを選択し、**Rules** [ルール]タブで、**Add** [追加]をクリックして新しいルールを追加するか、既存のルールを選択します。**Packet Capture** [パケット キャプチャ]を **single-packet** または **extended-capture** に設定します。

プロファイルにシグネチャの例外が定義されている場合は、***Exceptions (*例外*)*** タブをクリックします。シグネチャの ***Packet Capture (*パケット キャプチャ*)*** 列で ***single-packet*** または ***extended-capture*** を設定します。

2. （任意）いずれかのプロファイルで **extended-capture** を選択した場合、拡張パケット キャプチャの長さを定義します。
   1. **Device (**デバイス**)** > **Setup (**セットアップ**)** > **Content-ID** を選択し、コンテンツ ID 設定を編集します。
   2. **Extended Packet Capture Length** （**packets**）[拡張パケット キャプチャ長（パケット数）]セクションで、ファイアウォールがキャプチャするパケット数を指定します（1 ～ 50、デフォルトは 5）。
   3. **OK** をクリックします。

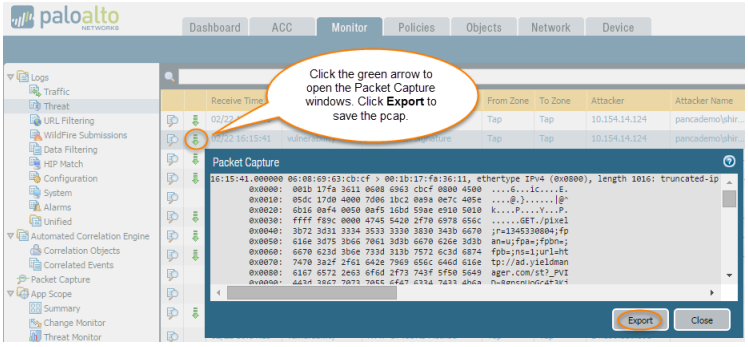
STEP 2 | （パケット キャプチャを有効にした）セキュリティ プロファイルをセキュリティポリシーのルールに追加します。

1. **Policies (**ポリシー**)** > **Security (**セキュリティ**)** を選択し、さらにルールを選択します。
2. **[**アクション**]** タブを選択します。
3. Profile Settings （プロファイル設定）セクションで、パケット キャプチャを有効にしたプロファイルを選択します。

   たとえば、**Antivirus** [アンチウイルス]ドロップダウンをクリックし、パケット キャプチャを有効にしたプロファイルを選択します。

STEP 3 | 脅威ログからパケット キャプチャを表示/エクスポートします。

1. **Monitor (**監視**)** > **Logs (**ログ**)** > を選択します
2. 関心のあるログ エントリの 2 列目にある緑のパケット キャプチャ アイコン をクリックします。パケット キャプチャを直接表示するか、システムに **Export** [エクスポート]します。



アプリケーション パケット キャプチャの実行

以下のトピックでは、ファイアウォールにアプリケーション パケット キャプチャの実行を設定する 2 つの方法を説明します。

- 不明なアプリケーションのパケット キャプチャの実行
- カスタム アプリケーション パケット キャプチャの実行

不明なアプリケーションのパケット キャプチャの実行

Palo Alto Networks ファイアウォールでは、ファイアウォールが識別できないアプリケーションが含まれるセッションのpacket capture (パケット キャプチャ - pcap)を自動的に生成します。通常、不明なトラフィック（tcp、udp、またはnon-syn-tcp）として分類されるアプリケーションは、まだ App-ID シグネチャがない市販のアプリケーション、ネットワーク上の内部アプリケーション、カスタム アプリケーション、または潜在的な脅威のみです。これらのパケット キャプチャを使用して、不明なアプリケーションに関連するより多くのコンテキストを収集したり、情報を使用してトラフィックに潜在的な脅威がないかどうか分析したりできます。セキュリティ ポリシーを使用してアプリケーションを制御したり、カスタム アプリケーション シグネチャを記述し、カスタムシグネチャに基づいたセキュリティ ルールを作成したりすることで、カスタム アプリケーションや不明なアプリケーションの管理を行うこともできます。アプリケーションが商用アプリケーションである場合、このパケット キャプチャを Palo Alto Networks に送信して App-ID シグネチャの作成を依頼することができます。

STEP 1 | 不明なアプリケーションのpacket capture (パケット キャプチャ - pcap)が有効であることを確認します (このオプションはデフォルトで有効です)。

1. 不明なアプリケーションのキャプチャ設定を表示するには、以下の CLI コマンドを実行します。

```
admin@PA-220>show running application setting | match “Unknown
 capture”
```

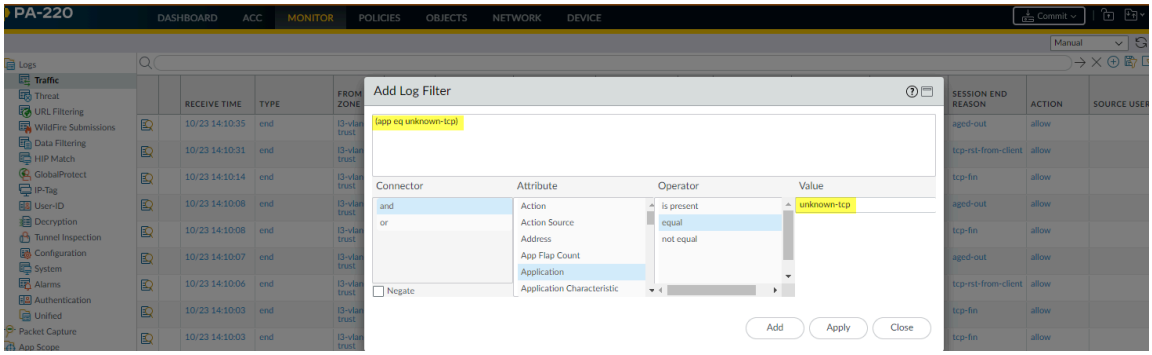
2. 不明なキャプチャ設定オプションがオフの場合は有効にします。

```
admin@PA-220>set application dump-unknown yes
```

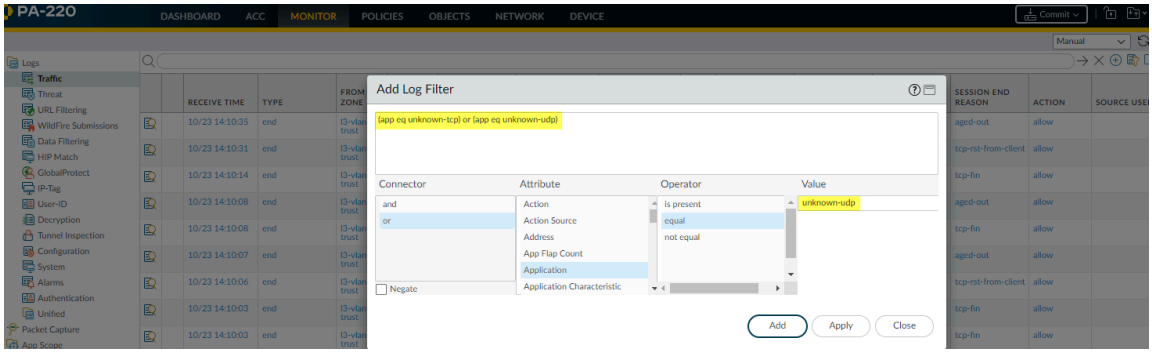
STEP 2 | トラフィック ログをフィルタリングして、不明な TCP と UDP アプリケーションを見つけます。

1. **Monitor (監視)** > **Logs (ログ)** > **Traffic (トラフィック)**を選択します。
2. **Add Filter (フィルタを追加)** をクリックし、フィルタの不明なTCP部分を作成してから (**Connector (コネクタ)** = “and”, **Attribute (属性)** = “Application”, **Operator (オペレータ)** =

“equal”、そして“unknown-tcp” を **Value (値)** として入力)、そして、**Add (追加)** をクリックして、クエリをフィルタに追加します。

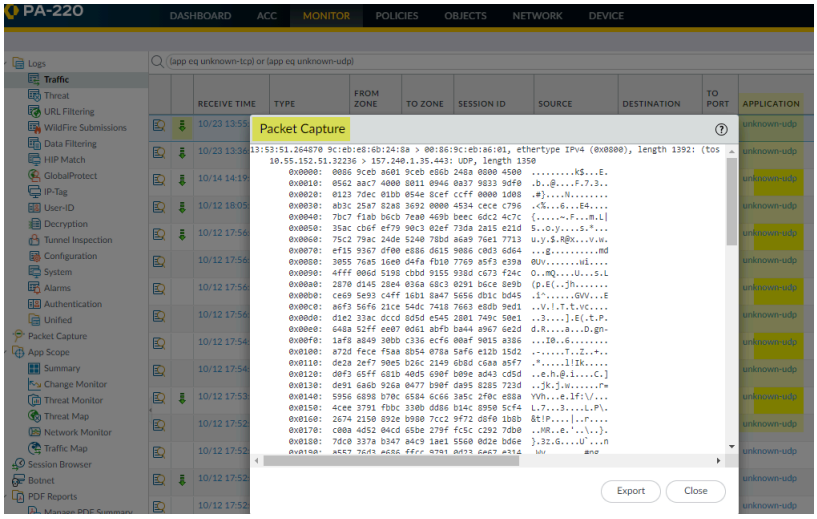


3. フィルタの不明な UDP 部分を作成してから、 (**Connector (コネクタ)** = “or”, **Attribute (属性)** = “Application”, **Operator (オペレータ)** = “equal”、そして“unknown-udp” を **Value (値)** として入力)、そして、**Add (追加)** をクリックして、クエリをフィルタに追加します。



4. **Apply (適用)** をクリックして、ログ画面のクエリ フィールドにフィルタを配置します。

STEP 3 | クエリフィールドの横にある **Apply Filter (フィルタの適用)** 矢印をクリックしてフィルタを実行し、packet capture (パケット キャプチャ - pcap)アイコンをクリックしてパケット キャプチャを表示するか、またはローカル システムに **Export (エクスポート)** します。



カスタム アプリケーション パケット キャプチャの実行

アプリケーション名および定義したフィルタに基づいてパケット キャプチャを実行するように Palo Alto Networks ファイアウォールを設定できます。パケット キャプチャを使用して、アプリケーションの制御に関する問題をトラブルシューティングできます。アプリケーション パケット キャプチャを設定するときには、App-ID データベースに定義されたアプリケーション名を使用する必要があります。Applipedia を使用するか、**Objects (オブジェクト)** > **Applications (アプリケーション)** でファイアウォールの Web インターフェイスを使用して、すべてのアプリケーションの App-ID を表示できます。

STEP 1 | PuTTY などの端末エミュレーション アプリケーションを使用して、ファイアウォールに SSH セッションを起動します。

STEP 2 | アプリケーション パケット キャプチャをオンにしてフィルタを定義します。

```
admin@PA-220>set application dump on application <application-name>
 rule <rule-name>
```

例えば、「ソーシャル ネットワーキング アプリケーション」というセキュリティ ルールに一致する linkedin-base アプリケーションのパケットをキャプチャするには、以下の CLIコマンドを実行します:

```
admin@PA-220>set application dump on application linkedin-base rule
 "Social Networking Apps"
```

送信元 *IP* アドレスや宛先 *IP* アドレスなど、他のフィルタを適用することもできます。

STEP 3 | パケット キャプチャ出力を表示して、正しいフィルタが適用されていることを確認します。パケット キャプチャを有効にすると、出力が表示されます。

以下の出力は、アプリケーション キャプチャ フィルタリングが、ソーシャル ネットワーキング アプリケーションのルールに一致するトラフィックの 1 linkedln-base のアプリケーションに基づいていることが確認できます。

```
Application setting:
Application cache             : yes
Supernode                     : yes
Heuristics                    : yes
Cache Threshold               : 16
Bypass when exceeds queue limit: no
Traceroute appid              : yes
Traceroute TTL threshold      : 30
Use cache for appid           : no
Use simple appsigs for ident  : yes
Use AppID cache on SSL/SNI    : no
Unknown capture               : on
Max. unknown sessions         : 5000
Current unknown sessions      : 7
Application capture           : on
Max. application sessions     : 5000
Current application sessions  : 0
Application filter setting:
    Rule                      : Social Networking Apps
    From                      : any
    To                        : any
    Source                    : any
    Destination               : any
    Protocol                  : any
    Source Port               : any
    Dest. Port                : any
    Application               : linkedin-base

Current APPID Signature
   Memory Usage               : 16768  KB (Actual 16440  KB)
      TCP 1 C2S               : regex 11898  states
      TCP 1 S2C               : regex 4549   states
      UDP 1 C2S               : regex 4234   states
      UDP 1 S2C               : regex 1605   states

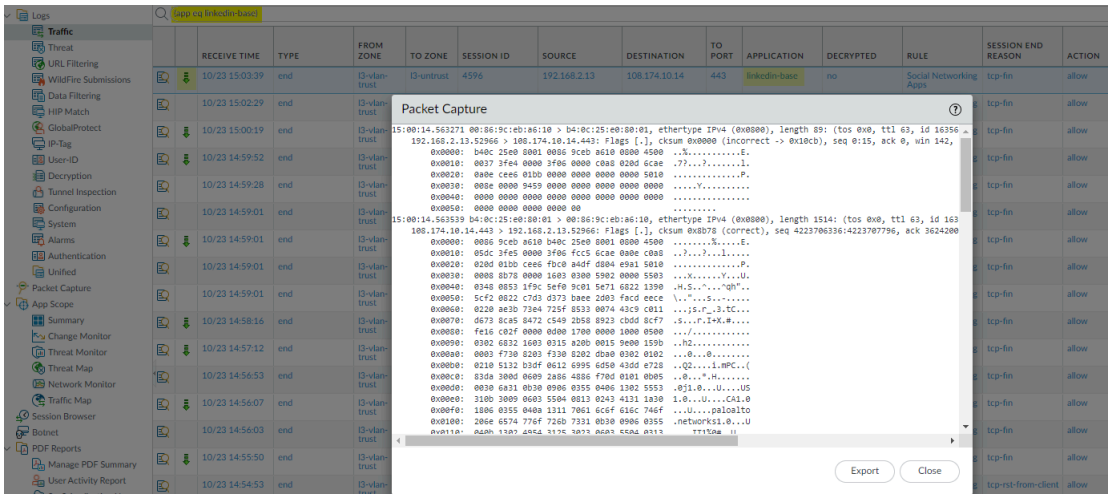
Alternate APPID Signature
   Memory Usage               : 16768  KB (Actual 16425  KB)
      TCP 1 C2S               : regex 11878  states
      TCP 1 S2C               : regex 4549   states
      UDP 1 C2S               : regex 4233   states
      UDP 1 S2C               : regex 1604   states
```

STEP 4 | Web ブラウザから linkedin.com にアクセスし、いくつかのLinkedIn タスクを実行して LinkedIn トラフィックを生成してから、 以下の CLIコマンドを実行してアプリケーション パケット キャプチャをオフにします:

```
admin@PA-220>set application dump off
```

STEP 5 | パケット キャプチャを表示/エクスポートします。

1. ファイアウォールの Web インターフェイスにログインし、**Monitor (監視)** > **Logs (ログ)** > **Traffic (トラフィック)** の順に選択します。
2. 関心のあるログ エントリにある、緑のパケット キャプチャ アイコン をクリックします。
3. パケット キャプチャを直接表示するか、コンピューターに **Export** [エクスポート]します。以下のスクリーン キャプチャには、linkedin-base のパケット キャプチャが表示されています。



管理インターフェイスでのパケット キャプチャの実行

tcpdump CLI コマンドにより、Palo Alto Networks ファイアウォールの管理インターフェイス（MGT）を通過するパケットをキャプチャできます。

プラットフォームごとに、***tcpdump*** でキャプチャされるデフォルトのバイト数が設定されています。*PA-220* ファイアウォールでは、各パケットから *68* バイトのデータがキャプチャされ、それを超える部分は切り捨てられます。*PA-7000 Series* のファイアウォール、および *VM-Series* ファイアウォールでは、各パケットから *96 byte (*バイト*)*のデータがキャプチャされます。***tcpdump*** でキャプチャするパケット数を定義するには、***snaplen***（*snap length*）オプションを使用します（範囲は *0* ～ *65535*）。***snaplen*** を *0* に設定すると、ファイアウォールでは、全部のパケットをキャプチャするために必要な最大長が使用されます。

STEP 1 | PuTTY などの端末エミュレーション アプリケーションを使用して、ファイアウォールに SSH セッションを起動します。

STEP 2 | MGT インターフェイスのパケット キャプチャを開始するには、以下のコマンドを実行します。

```
admin@PA-220>tcpdump filter “<filter-option> <IP-address>” snaplen
 length
```

たとえば、管理者が RADIUS を使用してファイアウォールへの認証を行ったときに生成されたトラフィックをキャプチャするには、RADIUS サーバー（この例では 10.5.104.99）の宛先 IP アドレスでフィルタリングします。

```
admin@PA-220>tcpdump filter “dst 10.5.104.99” snaplen 0
```

src （送信元 IP アドレス）、host、net でフィルタリングすることもできます。また、コンテンツを除外できます。たとえば、サブネットでフィルタリングしてすべての SCP、SFTP、および SSH トラフィック（ポート 22 を使用）を除外するには、以下のコマンドを実行します。

```
admin@PA-220>tcpdump filter “net 10.5.104.0/24 and not port 22”
 snaplen 0
```

> ***tcpdump*** がパケット キャプチャを実行するたびに、コンテンツが *mgmt.pcap* という名前のファイルに保存されます。このファイルは、***tcpdump*** を実行するたびに上書きされます。

STEP 3 | 関心のあるトラフィックが MGT インターフェイスを通過したら、Ctrl + C を押してキャプチャを停止します。

STEP 4 | 以下のコマンドを実行して、パケット キャプチャを表示します。

```
admin@PA-220> view-pcap mgmt-pcap mgmt.pcap
```

以下の出力には、MGT ポート（10.5.104.98）から RADIUS サーバー（10.5.104.99）へのパケット キャプチャが表示されています。

```
09:55:29.139394 IP 10.5.104.98.43063 > 10.5.104.99.radius:RADIUS,
 Access Request (1), id:RADIUS、アクセス要求（1）、ID：0x00 length:89
 09:55:29.144354 arp reply 10.5.104.98 is-at 00:25:90:23:94:98
 (oui Unknown) 09:55:29.379290 IP 10.5.104.98.43063 >
 10.5.104.99.radius:RADIUS, Access Request (1), id:0x00 length:70
 09:55:34.379262 arp who-has 10.5.104.99 tell 10.5.104.98
```

STEP 5 | （任意）SCP （または TFTP）を使用して、ファイアウォールからパケット キャプチャをエクスポートします。たとえば、SCP を使用してパケット キャプチャをエクスポートするには、以下のコマンドを実行します。

```
admin@PA-220>scp export mgmt-pcap from mgmt.pcap
 to <username@host:path>
```

たとえば、pcap を SCP 対応サーバー（10.5.5.20）の temp-SCP という一時フォルダにエクスポートするには、以下の CLI コマンドを実行します。

```
admin@PA-220>scp export mgmt-pcap from mgmt.pcap to
 admin@10.5.5.20:c:/temp-SCP
```

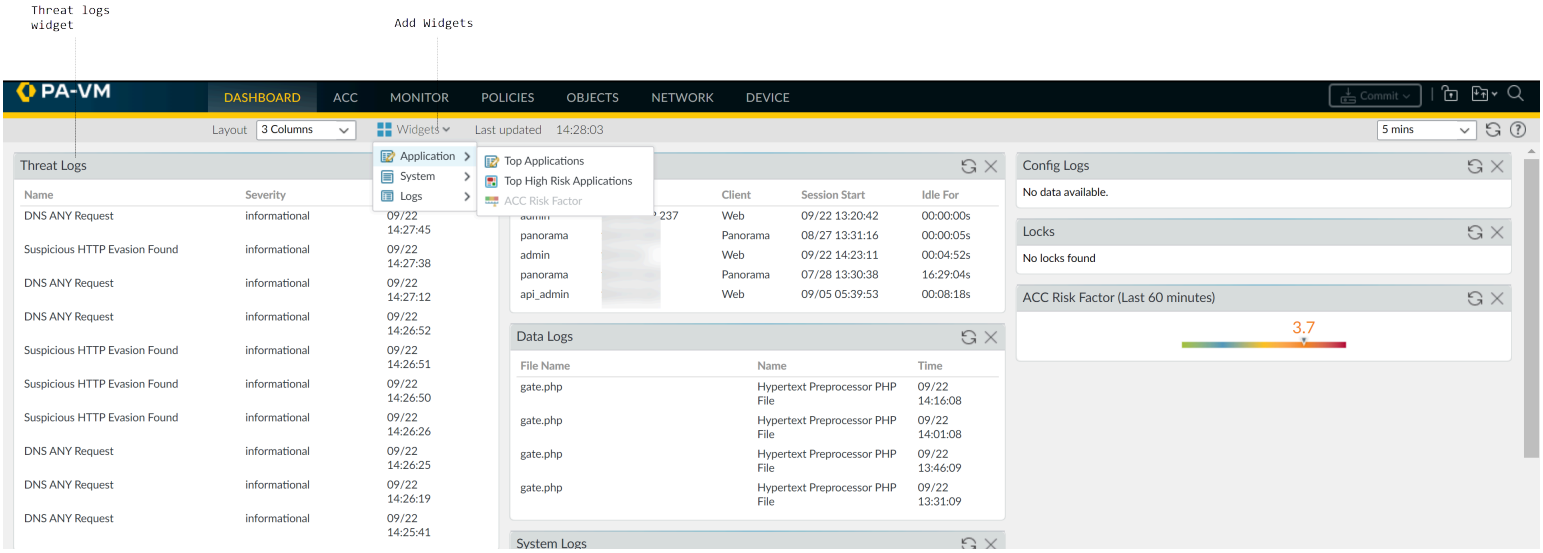
SCP サーバーのアカウントのログイン名とパスワードを入力すると、ファイアウォールはパケット キャプチャを SCP 対応サーバーの c:\temp-SCP にコピーします。

STEP 6 | これで、Wireshark などのネットワーク パケット アナライザを使用してパケット キャプチャ ファイルを表示できます。

アプリケーションと脅威のモニター

パロアルトネットワークスの次世代ファイアウォールはすべてApp-IDテクノロジーを搭載しており、プロトコル、暗号化、回避戦術に関係なく、ネットワークを通過するアプリケーションを特定します。その後、アプリケーション コマンド センターの使用でアプリケーションを監視することができます。ACC はさまざまなログ データベースのデータをグラフィカルに要約し、ネットワークを通過するアプリケーション、アプリケーションの使用者、および潜在的なセキュリティへの影響を強調表示します。また ACC は、App-ID が実行する連続的なトラフィック分類機能を使用して動的に更新されます。App-ID は、アプリケーションがポートまたは動作を変更した場合でもそのトラフィックを識別し続け、ACC に結果を表示します。さらに、URL カテゴリ、脅威、およびデータも視覚的に表示されるため、ネットワーク アクティビティの全体像を把握できます。ACC により、ネットワークを通過するトラフィックについての詳細な情報をごく短時間で収集し、その情報が反映された、より情報に則したセキュリティ ポリシーを作成することができます。

Dashboard の使用でネットワークも監視することができます。



コンテンツ配信ネットワーク インフラストラクチャ を確認して、ファイアウォール上のログイベントがセキュリティリスクを引き起こすかどうかを確認します。AutoFocus インテリジェンス サマリーは、お使いのネットワークログに関連したプロパティ、アクティビティ、挙動の頻度を示します。グローバルスケールでは、それらにリンクした WildFire 判定と AutoFocus タグを示します。AutoFocus サブスクリプションで、この情報を使うことにより、お使いのネットワークで特定の脅威を追跡するカスタマイズドAutoFocus アラートを作成できます。

ログの表示および管理

ログが自動的に生成されます。これはタイムスタンプされたファイルで、ファイアウォールのシステムイベントまたはファイアウォールがモニターするネットワークトラフィックイベントの監査証跡を提残します。ログエントリには *artifacts*が含まれます。これはログされたイベントのプロパティ、アクティビティ、挙動です。つまり攻撃者のアプリケーションタイプや IP アドレスなどです。各ログタイプは個別のイベントタイプの情報を記録します。例えば、ファイアウォールは、スパイウェア、脆弱性、ウイルス シグネチャに一致するトラフィックを記録するための脅威ログまたはポートスキャンやファイアウォールのホストスイープアクティビティに設定されたしきい値に一致するDoS攻撃を生成します。

- Log Types and Severity Levels（ログタイプと重大度レベル）
- ログの表示
- ログのフィルター
- ログのエクスポート
- ログ ストレージの割り当てと有効期間の設定
- SCP または FTP サーバーへのログのエクスポートのスケジュール

Log Types and Severity Levels（ログタイプと重大度レベル）

これらのログ ファイルは **Monitor (**監視**)** > **Logs (**ログ**)** ページで表示できます。

- トラフィック ログ
- Threat Logs（脅威ログ）
- URL フィルタリング ログ
- WildFire 送信ログ
- Data Filtering Logs（データ フィルタリング ログ）
- 相関ログ
- トンネル検査ログ
- Config Logs（設定ログ）
- System Logs（システム ログ）
- HIPマッチログ
- GlobalProtect ログ
- IP-タグ ログ
- ユーザー ID ログ
- 復号化ログ
- アラーム ログ
- 認証ログ
- 統合ログ

トラフィック ログ

トラフィックログは、各セッションの開始と終了のエントリを表示します。各エントリには、日付と時刻、送信元および宛先のゾーン、送信元および宛先のDynamic Address Group (ダイナミック アドレス グループ)、アドレスおよびポート、アプリケーション名、トラフィックフローに適用されるセキュリティルール、ルールアクション (「許可」、「拒否」、または「ドロップ」)、入口/出口 インターフェース、byte (バイト)数、およびセッション終了理由などが記載されます。

ダイナミック アドレス グループは、トラフィックが一致するルールにダイナミック アドレス グループが含まれている場合にのみログに表示されます。*IP*アドレスが複数のダイナミック アドレス グループに表示される場合、ファイアウォールは送信元 *IP* アドレスとともに最大*5*つのダイナミック アドレス グループをログに表示します

Type[タイプ] 列は、そのエントリがセッションの開始または終了のどちらのエントリなのかを示します。Action[アクション]列はファイアウォールが、そのセッションを許可、拒否またはドロップしたことを示します。「ドロップ」は、トラフィックをブロックしたセキュリティ ルールが適用されていずれかのアプリケーションが指定されたことを示し、「拒否」はルールが適用されてある特定のアプリケーションが識別されたことを示します。アプリケーションが識別される前にトラフィックが廃棄された場合 (あるルールにより特定のサービスのトラフィックがすべて廃棄された場合など)、そのアプリケーション列 は「該当なし」と表示します。

エントリの横の をクリックすると、セッションに関する詳細な情報（ICMP エントリを使用して同じ送信元と宛先間の複数のセッションを集約するかどうかなど）が表示されます（Count（繰り返し回数）列値は 1 より大きくなります）。

PAN-OS 10.2 で導入された 復号化ログが無効になっている場合、ファイアウォールは *HTTP/2* ログを トラフィック ログとして送信します。ただし、復号ログが有効になっている場合、ファイアウォールは *HTTP/2* ログをトンネル検査ログとして送信します *(*復号ログが無効になっている場合、*HTTP/2* ログはトラフィック ログとして送信されます*)*。したがって、*HTTP/2*イベントの場合はトラフィック ログではなくトンネル検査ログを確認する必要があります。

Threat Logs（脅威ログ）

トラフィックがファイアウォールのセキュリティルールに関連付けられているセキュリティ プロファイルの1つと一致すると、脅威ログはエントリを表示します。各エントリには、日付と時刻、脅威の種類(ウィルス、スパイウェアなど)、脅威の詳細やURL、送信元および宛先のゾーン、アドレス、送信元および宛先のダイナミック アドレス グループ、およびポート、アプリケーション名、アラーム アクション (「allow」または「block」)、重大度レベルなどが記載されます。

ダイナミック アドレス グループは、トラフィックが一致するルールにダイナミック アドレス グループが含まれている場合にのみログに表示されます。*IP*アドレスが複数のダイナミック アドレス グループに表示される場合、ファイアウォールは送信元 *IP* アドレスとともに最大*5*つのダイナミック アドレス グループをログに表示します

各脅威ログエントリの詳細を閲覧する

- 脅威エントリの横の をクリックすると、詳細な情報（そのエントリを使用して同じ送信元と宛先間の同じタイプの複数の脅威を集約するかどうかなど）が表示されます（Count （繰り返し回数）列値は 1 より大きくなります）。
- パケット キャプチャを実行するようにファイアウォールを設定している場合は、エントリ横の をクリックし、キャプチャーされたパケットにアクセスします。

以下の表に脅威の重大度レベルを要約して示します。

重要度	説明
Critical (極めて重大)	広範囲にデプロイされたソフトウェアのデフォルト インストールに影響するような深刻な脅威。サーバーの root が悪用され、弱点のあるコードが広範囲の攻撃者の手に渡ることになります。攻撃者は通常、特殊な認証資格証明や個々の被害者に関する知識を必要としません。また、標的がなんらかの特殊な機能を実行するように操作する必要もありません。
High（高）	重大度が Critical に変わる可能性があるものの、軽減要因が存在する脅威。たとえば、悪用するのが困難であったり、上位の特権が与えられることがなかったり、被害サーバー数が多くなかったりする場合です。 悪意があると判定された WildFire 送信ログの項目および許可するよう設定されたアクションは、High（高）としてログに記録されます。
Medium（中）	影響が最小限に抑えられる小さな脅威。たとえば、標的に侵入することのない DoS 攻撃や、攻撃者が被害サーバーと同じ LAN 上に存在する必要があり、標準以外の設定や隠れたアプリケーションにのみ影響するか、アクセスがごく限られている悪用などです。 • 既存の WildFire シグネチャの重大度に基づいて、悪意のある判定とブロックまたはアラートのアクションを含む脅威ログ エントリは、Medium（中）として記録されます。
Low（低）	組織のインフラストラクチャへの影響がわずかな警告レベルの脅威。通常、ローカルまたは物理的なシステムへのアクセスが必要であり、被害者のプライバシーや DoS の問題、情報漏洩などが発生することがあります。 • データ フィルタリング プロファイルの一致は、「低」としてログに記録されます。 • グレイウェア判定を含む WildFire 送信ログ エントリおよび何らかのアクションは、Low（低）としてログに記録されます。
Informational (通知)	厳密に脅威とはならなくても、存在する可能性がある深層の問題に注意を引くために報告される、疑わしいイベント。 • URL フィルタリング ログ エントリは Informational（通知）としてログに記録されます。

重要度	説明
	• 無害判定および何らかのアクションを含む WildFire 送信ログ エントリは、Informational（通知）としてログに記録されます。 • 何らかの判定と、ブロックおよび転送するよう設定されたアクションを含む WildFire 送信ログ エントリは、Informational（通知）としてログに記録されます。 • 何らかの判定をを含むログ エントリおよびブロックするよう設定されたアクションも、Informational（通知）としてログに記録されます。

URL フィルタリング ログ

URL filtering logs (**Monitor** > **Logs** > **URL フィルタリング**) は、Security ポリシー ルールで監視されている URL カテゴリへのトラフィックに関する包括的な情報を表示します。各セッションに記録される属性またはプロパティには、受信時刻、カテゴリ、URL、ゾーンからゾーンへ、ソース、およびソース ユーザー が含まれます。ログ・ビュー をカスタマイズして、最も関心のある属性のみが表示されるようにすることができます。firewall は、以下の場合に URL フィルタリング・ログ・エントリーを生成します。

- Traffic は、一致基準として URL カテゴリを持つ Security ポリシー規則を照合します。このルールは、トラフィックに対して次のいずれかのアクションを適用します: 拒否、ドロップ、またはリセット（クライアント、サーバー、両方）。
- Traffic は、URL Filtering Profile が添付された Security ポリシー規則と一致します。プロファイル内のカテゴリの Site Access は、`alert`、`block`、`continue`、または `override` に設定されます。

既定では、***allow*** に設定されたカテゴリは、*URL* フィルタリング ログ エントリを生成しません。例外は、 を構成した場合です。

許可しているが、より可視性を高めたいカテゴリへのトラフィックを *firewall* に記録する場合は、これらのカテゴリの ***Site*** アクセス を *URL Filtering* プロファイルで ***alert*** に設定します。

WildFire 送信ログ

ファイアウォールは、WildFire プロファイル設定（**Objects**（オブジェクト） > **Security Profiles**（セキュリティ プロファイル） > **WildFire Analysis**（**WildFire** 分析））に基づいて分析を行うため WidlFire クラウドにサンプル(ファイルおよび電子メールリンク)を送信します。WildFire がサンプルの動的/静的分析を終えると、ファイアウォールは転送するサンプルごとに WildFire 送信ログエントリを生成します。WildFire Submissions のログ エントリには、送信されたサンプルおよびそのサンプルの重大度に対する WildFire の判定をサンプル（許可またはブロック）の Firewall アクションが含まれます。

以下の表に WildFire 判定を要約して示します。

Verdict（判定）	説明
安全	エントリが WildFire 分析で安全と判定されたことを示します。安全と分類されたファイルは、安全でマルウェアの動作を示していません。
グレイウェア	エントリが WildFire 分析でグレイウェアと判定されたことを示します。グレイウェアと分類されたファイルは、直接のセキュリティ脅威とはなりませんが、他の迷惑な動作を示すことがあります。グレイウェアには、アドウェア、スパイウェア、ブラウザ ヘルパー オブジェクト（BHO）などがあります。
フィッシング	WildFire がリンクにフィッシングの分析の判定を割り当てたことを示します。フィッシング判定は、リンク先のユーザーが証明書のフィッシング詐欺行為を表示したことを示します。
悪意がある	エントリが WildFire 分析で悪意があると判定されたことを示します。悪意があると判定されたサンプルはセキュリティ上の脅威をもたらす恐れがありますマルウェアには、ウイルス、C2 (コマンドアンドコントロール)、ワーム、トロイの木馬、リモート アクセス ツール (RAP)、ルートキット、ボットネットなどがあります。マルウェアと識別されたファイルの場合、将来的な曝露を防止するためにシグネチャが WildFire クラウドによって生成および配布されます。 *C2* サンプルは、*WildFire* 分析レポートと、*WildFire* 分析データに依存する他の *Palo Alto Networks* 製品では *C2* に分類されます。ただし、その判定は、ファイアウォールによって悪意のあるものとして翻訳され、分類されます。

Data Filtering Logs（データ フィルタリング ログ）

データフィルタリングログでは、クレジット カード番号などの機密情報が、ファイアウォールによって保護されているエリアから流出するのを防止するのに役立つデータフィルタリングセキュリティ ポリシーのエントリが表示されます。データフィルタリングプロファイルの定義については、データのフィルタリングを参照してください。

このログ タイプには、ファイル ブロッキング プロファイルの情報も表示されます。例えば、ルールで .exe ファイルをブロックする場合、このログはブロックされたファイルを表示します。

相関ログ

ファイアウォールは、相関オブジェクトで定義されたパターンとしきい値がネットワーク上のトラフィック・パターンと一致する場合に、相関イベントをログに記録します。イベントのグラフィカル表示を相関されたイベントの解釈して表示するには、「ACC での Compromised Hosts [侵入されたホスト]ウィジットの使用」を参照してください。

以下の表に相関ログの重大度レベルを要約して示します。

重要度	説明
Critical（極めて重大）	拡散パターンを示す相関されたイベントに基づいて、ホストが侵入されたことが確認されました。たとえば、WildFire によって有害と判定されたファイルをホストが受信し、WildFire サンドボックスでその有害ファイルのコマンドアンドコントロール アクティビティとして確認されたものと同じアクティビティがホストで示された場合、重要イベントがログに記録されます。
High（高）	複数の脅威イベント間の相関に基づいて、ホストが侵入された可能性が高いことを示します。たとえば、ネットワーク上の任意の場所で検出されたマルウェアが、特定のホストから生成されたコマンドアンドコントロール アクティビティと一致する場合です。
Medium（中）	つまたは複数の疑わしいイベントの検出に基づいて、ホストが侵入された可能性があることを示します。たとえば、スクリプト化されたコマンドアンドコントロール アクティビティを示している既知の有害な URL への頻繁なアクセスがある場合です。
Low（低）	1 つまたは複数の疑わしいイベントの検出に基づいて、ホストが侵入されたと考えられることを示します。たとえば、有害な URL やダイナミック DNS ドメインへのアクセスがあった場合です。
Informational（通知）	集合体として、疑わしいアクティビティの識別に役立つ可能性があるイベントを検出します。各イベントはそれ自体が必ずしも重要ではありません。

トンネル検査ログ

トンネル検査ログは、トンネル セッション用のトラフィックログのようなものであり、非暗号化トンネル セッションのエントリを表示します。重複カウントを避けるために、ファイアウォールは内側のフローのみをトラフィックログに保存し、トンネル セッションをトンネル検査ログに送信します。トンネル検査ログのエントリには、受信時間（ログを受信した日時）、トンネル ID、監視タグ、セッション ID、トンネル セッションに割り当てられたセキュリティルール、セッションのバイト数、親セッション ID（トンネル セッション用のセッション ID）、送信元アドレス、送信元ユーザーおよび送信元ゾーン、宛先アドレス、宛先ユーザー、宛先ゾーンが含まれます。

PAN-OS 10.2 で導入された *Decryption* ログを有効にすると、*firewall* は *HTTP/2* ログを *Tunnel Inspection* ログとして送信します *(Decryption* ログが無効になっている場合、*HTTP/2* ログは *Traffic* ログとして送信されます*)* ため、*Traffic* ログではなく *Tunnel Inspection* ログで *HTTP/2* イベントを確認する必要があります。この場合、*HTTP/2* トラフィックの *App-ID* を取得するには、Tunnel Content Inspection (トンネル コンテンツ検査) を有効にする必要があります。

Detailed Log (詳細ログ) ビューをクリックし、使用するトンネル プロトコルなどといった項目の詳細情報と、トンネル コンテンツが検査済みかどうかを示すフラグを確認します。親セッションを持つセッションのみにトンネル検査済みフラグが設定されます。これは、セッションがトン

ネル内トンネル（2 レベルのカプセル化）に含まれていることを意味します。トンネルの最初の外部ヘッダにはトンネル検査済みフラグが設定されていません。

Config Logs（設定ログ）

設定ログはファイアウォール設定へのすべての変更エントリを記録します。各エントリには、日時、管理者のユーザー名、変更を行ったユーザーの IP アドレス、クライアントのタイプ（Web、 CLI または Panorama）、実行されたコマンドのタイプ、コマンドが成功したか失敗したか、設定パス、および変更前後の値が含まれています。

System Logs（システム ログ）

システムログはファイアウォールでのシステムイベントのエントリを表示します。各エントリには、日時、イベントの重大度、およびイベントの説明が含まれています。以下の表にシステム ログの重大度レベルを要約して示します。システム ログ メッセージとそれに対応する重大度レベルの部分的なリストについては、「System Log Events （システム ログ イベント）」を参照してください。

重要度	説明
Critical (極めて重大)	高可用性 (HA) フェールオーバーなどのハードウェア障害やリンク障害です。
High（高）	外部デバイス（LDAP サーバーや RADIUS サーバーなど）との接続の切断などの深刻な問題。
Medium（中）	アンチウイルス パッケージのアップグレードなどの中レベルの通知。
Low（低）	ユーザー パスワードの変更などそれほど重要ではない通知。
Informational (通知)	ログイン/ログオフ、管理者名やパスワードの変更、設定の変更、および重大度レベルに含まれない他のすべてのイベント。

HIPマッチログ

GlobalProtect Host Information Profile (HIP) matching によってネットワークを評価するエンドデバイスのセキュリティ状態に関する情報を収集できます(ディスク暗号化が有効か、など)。ファイアウォールは HIP ベースセキュリティルールにを準拠していることを基準に、特定のホストへのアクセスを許可または拒否します。HIP Match ログは、ルールに設定した HIP オブジェクトまたは HIP プロファイルに適合するトラフィック フローを表示します。

GlobalProtect ログ

GlobalProtect ログには、GlobalProtect に関連する以下のログが表示されます。

- GlobalProtect システム ログ

  GlobalProtect 認証イベント ログは、 **Monitor**（モニター） > **Logs**（ログ） > **System**（システム）に残ります。 ただし、GlobalProtect ログの **Auth Method**（認証方法） 列には、ログインに使用された認証方法が表示されます。
- LSVPN/サテライト イベント
- GlobalProtect ポータルおよびゲートウェイ ログ
- クライアントレス VPN ログ

IP-タグ ログ

IP-タグ ログには、送信元 IP アドレスがいつ、どのようにファイアウォールに登録、または登録解除されたか、またファイアウォールがどのタグをアドレスに付与したのかを示します。さらに、各ログ エントリでは 設定済みのタイムアウト (設定時)、および User-ID エージェント VM 情報ソースや自動タグ付けなど、IP アドレス-タグ間のマッピングの情報が表示されます。詳細については、IP アドレスおよびタグを動的に登録する方法を参照してください。

ユーザー ID ログ

User-IDログには IP アドレスからユーザー名へのマッピング情報と、マッピング情報のソースやユーザーが認証された時刻などの認証タイムスタンプに関する情報が表示されます。この情報を使用すると、User-ID および認証の問題をトラブルシューティングしやすくなります。たとえば、ファイアウォールが誤ったポリシー ルールをユーザーに適用している場合は、ログを参照して、そのユーザーが正しい IP アドレスにマッピングされているかどうか、およびグループの関連付けが正しいかどうかを検証できます。

復号化ログ

Decryption Logs (復号化ログ) には、デフォルトで失敗した TLS ハンドシェークのエントリが表示され、復号 ポリシーで有効にすると、成功した TLS ハンドシェークのエントリを表示できます。成功したハンドシェークのエントリを有効にする場合は、ログ用のシステム リソース (ログスペース) があることを確認してください。

復号化ログには、問題の復号のトラブルシューティングと監視を行うと解決に役立つ膨大な量の情報が含まれています。ログで有効にできる各種情報が62列あり、任意のログ (、虫眼鏡) を個別に選択して、単一の詳細ビューで詳細を表示できます。以下のような証明書、暗号化スイート、エラー情報を閲覧できます: サブジェクト共通名、発行者共通名、ルート共通名、ルート ステータス、証明書キーのタイプとサイズ、証明書の開始日と終了日、証明書シリアルナンバー、証明書の指紋、TLSバージョン、鍵交換アルゴリズム、暗号化アルゴリズム、ネゴシエートされた EC 曲線、認証アルゴリズム、SNI、プロキシタイプ、エラー情報 (暗号化、HSM、リソース、再開、プロトコル、機能、証明書、バージョン)、およびエラー インデックス (エラー情報詳細を取得するために検索できるコード)。

アラーム ログ

アラームとはファイアウォールが生成する、特定のイベントタイプ（暗号化や復号化の失敗など）の発生回数が、そのイベントタイプに設定されたしきい値を超えたことを示すメッセージです。アラームを有効化したり、アラームしきい値を設定するには、 **Device**（デバイス） > **Log Settings**（ログ設定）を選択して、アラーム設定を編集します。

アラームを生成する際、ファイアウォールはアラームログを作成し、システムアラームダイアログを開き、アラームを表示します。ダイアログを **Close** [閉じた]場合は、Webインターフェイスの下部に表示された**Alarms** [アラーム] () をクリックすることで再び開くことができます。ファイアウォールが特定のアラームのダイアログを自動的に開かないようにする場合は、Unacknowledged Alarms [未承認のアラーム] リストでそのアラームを選択し、**Acknowledge** [承認]します。

認証ログ

認証ログは、エンドユーザーが 認証ポリシー ルールによってアクセスが制御されているネットワークリソースにアクセスしようとしたときに発生する認証イベントに関する情報が表示されます。この情報を使用すると、アクセスの問題をトラブルシューティングしやすくなり、必要に応じて認証ポリシーを調整できるようになります。相関オブジェクトとともに認証ログを使用すると、総当たり攻撃など、ネットワークでの不審なアクティビティを特定することもできます。

必要に応じて、タイムアウト イベントをログに記録するように認証ルールを設定できます。これらのタイムアウトは、ユーザーがリソースに対して 1 回だけ認証すれば、その間リソースに何度でもアクセスできるという、その期間に関連します。タイムアウトの情報を見ることで、タイムアウトを調整するかどうか、どのように調整するかを決めることができます(詳細については、認証タイムスタンプを参照してください)。

システム ログには、*GlobalProtect* に関連する認証イベント、および *Web* インターフェイスへの管理者アクセスに関連する認証イベントが記録されます。

統合ログ

統合ログには、デフォルトで、トラフィック、脅威、URL フィルタリング、WildFire への送信、データフィルタリングログエントリが一つの画面で表示されます。統合ログビューによって、様々なログタイプを別々に検証するのではなく、それらの最近のエントリをまとめて検証したりフィルタをかけることができます。フィルターエリアで有効なクエリ () クリックして、統合ログビューにエントリを表示するログタイプを選択します。

統合ログビューは閲覧権限のあるログのエントリだけを表示します。たとえば、WildFire Submissions ログを表示する権限を持たない管理者は、統合ログを表示するときに WildFire Submissions ログ エントリを表示しません。これらのアクセス許可管理ロール タイプ定義します。

対象検索を実行するために *AutoFocus* でリモート検索をセットアップすると、検索結果が統合ログビューに表示されます。

ログの表示

ファイアウォールで様々なログタイプを表形式で表示できます。ファイアウォールはローカルに全てのログファイルを保存し、デフォルトで自動的に設定およびシステムログを生成します。他の種類のログのエントリの作成をトリガーするセキュリティ ルールの詳細については、Log Types and Severity Levels（ログタイプと重大度レベル）を参照してください。

ログを syslog メッセージ、電子メール通知、または Simple Network Management Protocol (SNMP) トラップとして転送するようにファイアウォールを構成するには、モニタリングでの外部サービスの使用を参照して下さい。

STEP 1 | 表示するログ タイプ を選択します。

1. **Monitor (監視)** > **Logs (ログ)**を選択します。
2. リストからログタイプを選択します。

   ファイアウォールは閲覧権限のあるログだけを表示します。たとえば、管理者アカウントに *WildFire Submissions* ログを表示する権限がない場合、ログ ページにアクセスするときに *firewall* にそのログ タイプは表示されません。権限は管理ロール タイプで定義されます。

STEP 2 | （任意）ログ列表示のカスタマイズ。

1. 列ヘッダーの右側にある矢印をクリックし、 **Columns**[Columns]を選択します。
2. リストから表示する列を選択します。ログは自動的に更新されて選択に一致するようになります。

STEP 3 | ログエントリの詳細を表示する。

- 特定のログエントリの spyglass ( )をクリックします。Detailed Log View [詳細ログ ビュー]はセッションの送信元と送信先ならびにログエントリに関連するセッションリストの詳細情報を持っています。
- （脅威ログのみ）エントリの隣にあるをクリックして、脅威のローカルパケットキャプチャーにアクセスします。ローカル パケット キャプチャを有効にするには、パケット キャプチャの実行を参照してください。
- （トラフィック、脅威、URL フィルタリング、WildFire 送信、統合ログのみ）ログ エントリの AutoFocus 脅威データを表示します。

  1. 「AutoFocus脅威インテリジェンスの有効化」を行います。

     *AutoFocus*に接続されておらず *PAN-OS 7.0* およびそれ以前のバージョンを実行しているファイアウォールのものを含む全ての *Panorama* ログエントリの *AutoFocus* 脅威データを表示できるように *Panorama* で *AutoFocus* を有効にします（***Panorama*** > ***Setup*** **(セットアップ)** > ***Management*** **(管理)** > ***AutoFocus***）。
  2. IP アドレス、URL、ユーザーエージェント、脅威名（サブタイプ：virus および wildfire-virus のみ）、ファイル名、あるいは SHA-256 ハッシュにカーソルを合わせてください。
  3. ドロップダウンリスト（）をクリックして **AutoFocus** を選択します。
  4. コンテンツ配信ネットワーク インフラストラクチャ .

次のステップ...

- 「ログのフィルター」を行います。
- 「ログのエクスポート」を行います。
- 「ログ ストレージの割り当てと有効期間の設定」を行います。

ログのフィルター

ログはそれぞれログエントリが表示する基準をセットできるフィルターエリアを持っています。ログのフィルター機能は特定のプロパティや属性を持つファイアウォールのイベントに注目するのに便利です。各ログエントリに関連するアーチファクトでログをフィルターします。

例えば、ルールの UUID でフィルタリングすれば、同じような名前のルールが多くある場合でも探している特定のルールを見つけやすくなります。ルールセットが非常に大きく、多くのルールが含まれている場合、ルールの UUID をフィルタとして使用することで、検索結果のページをたどることなく特定のルールを探せるようになります。

STEP 1 | （統合ログのみ）統合ログ表示に入れるログタイプを選択します。

1. 有効なクエリをクリックします ( )。
2. リスト (トラフィック、 脅威、 **url**、 データ、 **wildfire**)から1個以上のログタイプを選択します。
3. **OK** をクリックします。統合ログは更新され、選択したログタイプのエントリのみを表示します。

STEP 2 | フィルターフィールドにフィルターを追加する。

構文エラーを防ぐため、アーチファクト値がオペレーター（***has***または***in***など）と一致する場合、文字列を引用符で囲む必要があります。例えば、宛先国のフィルタリングを行い*INDIA*を検索する際に*Value[*値*]*として*IN*を使う場合は、フィルタを***(dstloc eq "IN")***と入力します。

- ログエントリで 1 個以上のアーチファクト(トラフィックに関連したアプリケーションタイプや攻撃者のIPアドレスなど)をクリックします。例えば、ログエントリの送信元 **10.0.0.25**とアプリケーション **web-browsing** [Web閲覧用]をクリックしてログの両方のアーチファクトを含むエントリのみを表示させます (AND検索)。
- フィルターフィールドに追加するアーチファクトを指定するには、 Add Filter （フィルタの追加）( )をクリックます 。
- すでに保存したフィルターを追加するには、Load Filter （フィルタをロード）( )をクリックします。

STEP 3 | フィルターをログに適用する。

Apply Filter （フィルタの適用） ( )をクリックします。ログは更新されてカレントフィルターに一致するログエントリのみ表示します。

STEP 4 | （任意）頻繁に使用するフィルターを保存します。

1. Save Filter （フィルタの保存）（)をクリックします。
2. フィルタの **Name** [名前]を入力します。
3. **OK** をクリックします。Load Filter [フィルタをロード]( )をクリックすると保存したフィルターを表示できます。

次のステップ...

- 「ログの表示」を行います。
- ログのエクスポートを行います。

ログのエクスポート

ログタイプのコンテンツをカンマ区切り値（CSV）フォーマットレポートにエクスポートできます。レポートにはデフォルトで最大2,000行のログを含むよう設定されています。

STEP 1 | レポート内の行数を指定します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択し、Logging and Reporting Settings (ロギングおよびレポート設定) を編集します。
2. **Log Export and Reporting** [ログのエクスポートとレポート] タブをクリックします。
3. **Max Rows in CSV Export**[CSV エクスポートの最大行数]の数を編集します(最大1048576 行)。
4. **OK** をクリックします。

STEP 2 | ログをダウンロードする

1. Export to CSV[CSV にエクスポート] ( ) をクリックします。ダウンロード状態を示す進捗バーが表示されます。
2. ダウンロードが終了したら、 **Download file**[ファイルをダウンロード]をクリックして、ログのコピーをローカルフォルダに保存します。ダウンロードしたログ内部の列ヘッダの詳細は、Syslog フィールドの説明を参照してください。

次のステップ...

SCP または FTP サーバーへのログのエクスポートのスケジュールを作成します。

ログ ストレージの割り当てと有効期間の設定

ファイアウォールは、有効期間が終了したログを自動的に削除します。ファイアウォールでは、ログ タイプのストレージ割り当てに達した場合、有効期間を設定していなくても、自動的にそのタイプのログを古い順に削除して領域を確保します。

手動でログを削除する場合は、***Device (デバイス) > Log Settings (ログ設定)*** の順に選択し、*Manage Logs (ログの管理)*画面で、タイプ別にログをクリアするリンクをクリックします。

STEP 1 | **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して Logging and Reporting Settings (ロギングおよびレポート設定) を編集します。

STEP 2 | **Log Storage (**ログ ストレージ**)** を選択して、各ログタイプに **Quota (%) (**割り当て**)** を入力します。パーセント値を変更するとダイアログが更新されて、対応する絶対値（割り当ての GB/MB 列）が表示されます。

STEP 3 | 各ログ タイプの **Max Days** (最大日数)（有効期間）を入力します（範囲は 1 ～ 2,000）。デフォルトではこのフィールドは空白（無期限）です。

ファイアウォールが、高可用性（*HA*）ペア間で有効期間を同期します。アクティブ *HA* ピアのみがログを生成するため、パッシブ ピアでは、フェイルオーバーが発生してログの生成を開始しない限り、削除するログはありません。

STEP 4 | **OK**、**Commit (**コミット**)** の順にクリックします。

SCP または FTP サーバーへのログのエクスポートのスケジュール

トラフィック、脅威、URL フィルタリング、データ フィルタリング、HIP マッチ、WildFire 送信の各ログの Secure Copy （SCP）サーバーまたは File Transfer Protocol （FTP）サーバーへのエクスポートをスケジュールできます。このタスクは、エクスポートするログ タイプごとに実行します。

CLI から Secure Copy （SCP）コマンドを使用して、ログ データベース全体を *SCP* サーバーにエクスポートし、さらに別のファイアウォールにインポートできます。ログ データベースは 以下のプラットフォームで実際にエクスポートまたはインポートするには大きすぎるため、これらのオプションはサポートされていません。*PA-7000 Series*ファイアウォール（すべての *PAN-OS* リリース）、*Panorama 6.0* 以降を実行している *Panorama* 仮想アプライアンス、および *Panorama M-Series* アプライアンス（すべての *Panorama* リリース）。

STEP 1 | **Device (**デバイス**)** > **Scheduled Log Export (**スケジュール設定されたログのエクスポート**)** を選択して **Add (**追加**)** をクリックします。

STEP 2 | [スケジュール設定されたログのエクスポート] の **[**名前**]** を入力し、**[**有効化**]** します。

STEP 3 | エクスポートする **[**ログ タイプ**]** を選択します。

STEP 4 | **[**エクスポートの開始予定時刻 **(**毎日**)]** を選択します。このオプションは、24 時間形式（00:00 ～ 23:59）で、15 分単位で指定します。

STEP 5 | **Protocol**[プロトコル] を選択してログをエクスポートします。**SCP** (secure) または **FTP**.

STEP 6 | **[**ホスト名**]** に、サーバーのホスト名または IP アドレスを入力します。

STEP 7 | **[**ポート**]** にポート番号を入力します。デフォルトでは、FTP ではポート 21、SCP ではポート 22 が使用されます。

STEP 8 | **[**パス**]** に、エクスポートしたログを保存するパスまたはディレクトリを入力します。

STEP 9 | サーバーにアクセスするための **Username** （ユーザー名）と、必要に応じて **Password** （パスワード）（および **Confirm Password** （パスワードの確認））を入力します。

STEP 10 | （FTP のみ）FTP パッシブ モード（ファイアウォールが FTP サーバーとのデータ接続を開始）を使用する場合は、**Enable FTP Passive Mode (FTP** パッシブ モードを有効にする**)** を選択します。デフォルトでは、ファイアウォールは FTP アクティブ モード（FTP サーバーがファイアウォールとのデータ接続を開始）を使用します。モードは、FTP サーバーのサポート内容とネットワーク要件に基づいて選択します。

STEP 11 | （SCP のみ） Click **Test SCP server connection**（**SCP** サーバー接続のテスト）をクリックします。接続を確立する前に、ファイアウォールが SCP サーバー用のホスト キーを承認する必要があります。

Panorama テンプレートを使用してログのエクスポート スケジュールを設定する場合、テンプレート設定をファイアウォールにコミットした後にこの手順を実行する必要があります。テンプレートのコミットが完了したら、各ファイアウォールにログインし、ログのエクスポート スケジュールを開いて、***Test SCP server connection***（***SCP*** サーバー接続のテスト）をクリックします。

STEP 12 | **OK**、**Commit (**コミット**)** の順にクリックします。

ブロックリストの監視

ファイアウォールにブロックリストへ IP アドレスを追加させる方法は 2 つあります。

- IP 接続をブロックするルールを持つ脆弱性保護プロファイルを設定し、ゾーンに適用するセキュリティポリシーにそのプロファイルを適用します。
- 分類化 DoS 保護プロファイルおよび Protect (保護) アクションを持つ DoS 保護ポリシールールを設定し、許可される最大の 1 秒あたりの接続数を指定ます。インバウンド パケットが DoS 保護ポリシーにマッチし、最大レートを超過しており、さらにブロック期間および分類化ポリシールールに送信元 IP アドレスを含めるように指定している場合、ファイアウォールはその攻撃的な送信元 IP アドレスをブロックリストに追加します。

上記のケースでは、パケットが CPU あるいは次のパケット バッファ リソースを使用する前に、ファイアウォールがハードウェア内のそのトラフィックを自動的にブロックします。攻撃トラフィックがハードウェアのブロック容量を超えた場合、ファイアウォールはソフトウェアの IP ブロック メカニズムを使用してトラフィックをブロックします。

ファイアウォールは脆弱性保護プロファイルあるいは DoS 保護ポリシールールに基づいて自動的にハードウェア ブロックリストのエントリを作成します（ルールにある送信元アドレスがハードウェア ブロックリストの送信元 IP アドレスになります）。

ブロックリストの各エントリの Type (タイプ) 列は、ハードウェア（hw）とソフトウェア（sw）のどちらによってブロックされたのかを示します。画面下部の表示：

- ファイアウォールがサポートする、ブロックされた IP アドレスの数のうち **Total Blocked IPs (ブロックされた IP の合計)** カウント。
- ファイアウォールが使用したブロックリストの割合。

ブロックリストのアドレスの詳細情報を確認するには、ソース IP アドレスにカーソルを合わせて下向きの矢印リンクをクリックします。Who Is リンクをクリックすると、そのアドレスについての情報を提供してくれる Network Solutions Who Is 機能が表示されます。

脆弱性保護プロファイルの設定の詳細については、「ブルート フォース シグネチャのアクションとトリガー条件のカスタマイズ」を参照してください。ブロックリストおよびDoS保護プロファイルの詳細については、「新規セッションのフラッド攻撃に対する DoS プロテクションの設定」を参照してください。

レポートの表示および管理

ファイアウォールのレポート機能により、ネットワークの状態の把握やポリシーの評価を行うことができ、ネットワークのセキュリティを保持してユーザーの安全性と生産性を確保することに注力できます。

- レポートのタイプ
- レポートの表示
- レポートの有効期間およびランタイムの設定
- 事前定義済みレポートの無効化
- カスタムレポート
- カスタム レポートの生成
- ボットネット レポートの生成
- SaaS アプリケーション使用率レポートを生成しています...
- PDF サマリー レポートの管理
- ユーザー/グループ アクティビティ レポートの生成
- レポート グループの管理
- 電子メールで配信するレポートのスケジュール設定
- レポートのストレージ容量を管理

レポートのタイプ

ファイアウォールには、事前定義済みレポートが組み込まれており、そのまま使用したり、特定のデータや実行可能なタスク用にニーズに合わせてカスタマイズしたり、事前定義済みレポートとカスタム レポートを組み合わせて必要な情報を編成したりできます。ファイアウォールでは、以下のタイプのレポートを作成できます。

- 事前定義済みレポート – ネットワーク上のトラフィックのサマリーを簡単に表示できます。一式の事前定義済みレポートには、アプリケーション、トラフィック、脅威、および URL フィルタリングの 4 つのカテゴリがあります。レポートの表示を参照してください。
- ユーザーまたはグループ アクティビティ レポート – 特定のユーザーまたはユーザー グループのアプリケーション使用量および URL アクティビティに関するレポートをスケジュール設定するか、またはオンデマンドで作成できます。レポートには、URL のカテゴリと、個々のユーザーの推定ブラウズ時間の計算結果が含まれます。ユーザー/グループ アクティビティ レポートの生成を参照してください。
- カスタム レポート – 含まれる条件と列に基づいてフィルタリングしたときの情報をそのまま表示するカスタム レポートを作成およびスケジュール設定します。また、クエリ ビルダーを組み込み、レポート データについてより具体的にドリルダウンすることもできます。カスタム レポートの生成を参照してください。
- **PDF** サマリー レポート – 脅威、アプリケーション、傾向、トラフィック、および URL フィルタリング カテゴリからの最大で 18 件の事前定義済みまたはカスタムのレポート/グラフ

を、1 つの PDF ドキュメントに集約します。PDF サマリー レポートの管理を参照してください。

- ボットネット レポート – 挙動ベースのメカニズムを使用して、ネットワーク内でボットネットに感染した可能性のあるホストを特定することができます。ボットネット レポートの生成を参照してください。
- レポート グループ – カスタム レポートと事前定義済みレポートをレポート グループにまとめ、1 人以上の受信者に電子メールで送信される単一の PDF にまとめます。レポート グループの管理を参照してください。

レポートは、要求時や定期的なスケジュールで生成できます。また、電子メール配信用にスケジュール設定することもできます。

レポートの表示

ファイアウォールでは、40 種類を超えるさまざまな事前定義済みレポートが毎日生成されます。それらのレポートは、ファイアウォールで直接表示できます。ほかに、カスタム レポートとサマリー レポートも表示できます。

ファイアウォールでは、レポートを保存するために約 200 MB のストレージが割り当てられます。この制限は、PA-7000 Series および PA-5200 Series のファイアウォールのみに再設定することができます。他のすべてのファイアウォールモデルでは、ファイアウォールが期間を超えるレポートを削除できるようにレポートの有効期間およびランタイムの設定ができます。ファイアウォールは、ストレージ制限に達すると、有効期間を設定していなくても、自動的にレポートを古い順に削除して領域を確保します。ファイアウォール上のシステム リソースを節約するもう 1 つの方法は、事前定義済みレポートの無効化にすることです。レポートを長期間保持するには、レポートをエクスポートするか (後述)、電子メールで配信するレポートのスケジュール設定をします。

他のレポートとは異なり、ユーザー/グループ アクティビティ レポートはファイアウォール上に保存できません。オンデマンドでユーザー/グループ アクティビティ レポートの生成するか、電子メール配信用にスケジュールする必要があります。

STEP 1 | (VM-50、VM-50 Lite、PA-200 ファイアウォールのみ) 事前定義済みレポートの生成を有効化します。

デフォルトでは、リソースを節約するために事前定義済みのレポートは *VM-50*、*VM-50 Lite*、および *PA-200* ファイアウォールで無効になります。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して **Logging and Reporting (ロギングおよびレポート作成)** を編集します。
2. **Pre-Defined Reports (事前定義済みレポート)** を選択し (チェック)、**Pre-Defined Reports (事前定義済みレポート)** を有効化します。
3. 生成したい事前定義済みレポートをチェック (有効化)して、**OK** をクリックします。
4. 設定の変更を **Commit (コミット)** します。
5. ファイアウォールCLIにアクセスして、事前定義済みレポートを有効化します。

   この手順は、ローカルの事前定義済みレポートおよび Panorama™ 管理サーバーからプッシュされた定義済みレポートに必要です。

```
admin> debug predefined-default enable
```

STEP 2 | **Monitor (監視)** > **Logs (ログ)**を選択します。

レポートはページ右側のセクション（タイプ）に分類されます。カスタムレポート、 アプリケーションレポート、 トラフィックレポート、 脅威レポート、 **URL** フィルタリングレポート、および **PDF** サマリーレポート.

STEP 3 | 表示するレポートを選択します。次にレポートページは前日のレポートを表示します。

他の日のレポートを表示するには、ページの右下にあるカレンダーから日付を選択し、レポートを選択します。別のセクションのレポートを選択すると、日付選択が今日の日付になります。

STEP 4 | レポートをオフラインで表示するには、レポートを PDF、CSV、または XML 形式にエクスポートします。ページの下部で、 **[PDF にエクスポート]**、**[CSV にエクスポート]**、または **[XML にエクスポート]** をクリックして、ファイルをプリントまたは保存します。

レポートの有効期間およびランタイムの設定

有効期限と実行時間は、すべてのレポートのタイプに適用されるグローバル設定です。新しいレポートを実行した後、ファイアウォールは有効期間が終了したレポートを自動的に削除します。

STEP 1 | **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)**の順に選択し、Logging and Reporting Settings (ロギングおよびレポート設定) を編集して、**Log Export and Reporting (ログのエクスポートとレポート)** タブを選択します。

STEP 2 | 24 時間表記で **Report Runtime (実行時間をレポート)** の時間を設定します（デフォルトは 02:00、範囲は 00:00（真夜中）～23:00）。

STEP 3 | **Report Expiration Period (**レポートの有効期間**)** を日数で入力します（デフォルトは失効なし。範囲は 1 ～ 2,000）。

ファイアウォールがレポート保存用に割り当てたストレージは変更できません。これは、約 *200 MB* に事前定義されています。ファイアウォールは、ストレージ上限に達すると、***Report Expiration Period*** （レポートの有効期間）を設定していなくても、自動的にレポートを古い順に削除して領域を確保します。

STEP 4 | **OK**、**Commit (**コミット**)** の順にクリックします。

事前定義済みレポートの無効化

ファイアウォールにはおよそ 40 種類の事前定義済みレポートが用意されており、それらが毎日自動的に生成されます。これらの一部または全部を使用しない場合は、選択したレポートを無効にして、ファイアウォールのシステム リソースを節約できます。

レポート グループまたは PDF サマリー レポートに、無効にする事前定義済みレポートが含まれていないことを確認してください。含まれていると、ファイアウォールはデータのない PDF サマリー レポートやレポート グループを表示します。

STEP 1 | **Device (**デバイス**)** > **Setup (**セットアップ**)** > **Management (**管理**)** を選択して Logging and Reporting Settings (ロギングおよびレポート設定) を編集します。

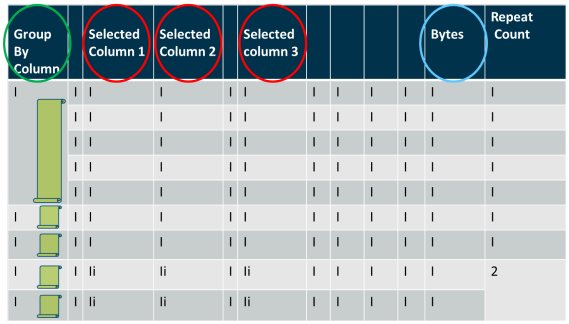
STEP 2 | **Pre-Defined Reports** （事前定義済みレポート）タブを選択し、無効にする各レポートのチェック ボックスをクリアします。すべての事前定義済みレポートを無効にするには、**Deselect All** （すべての選択を解除）をクリックします。

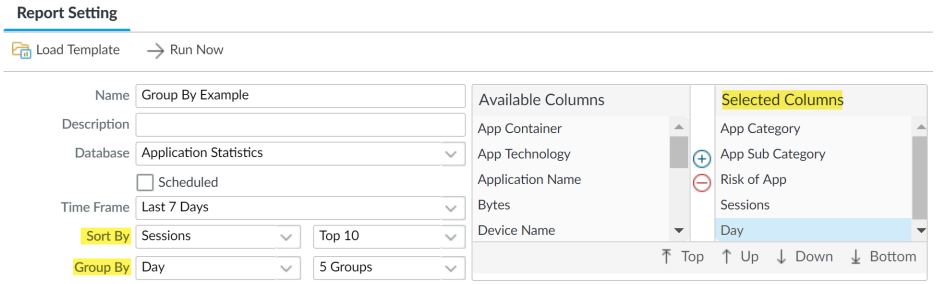
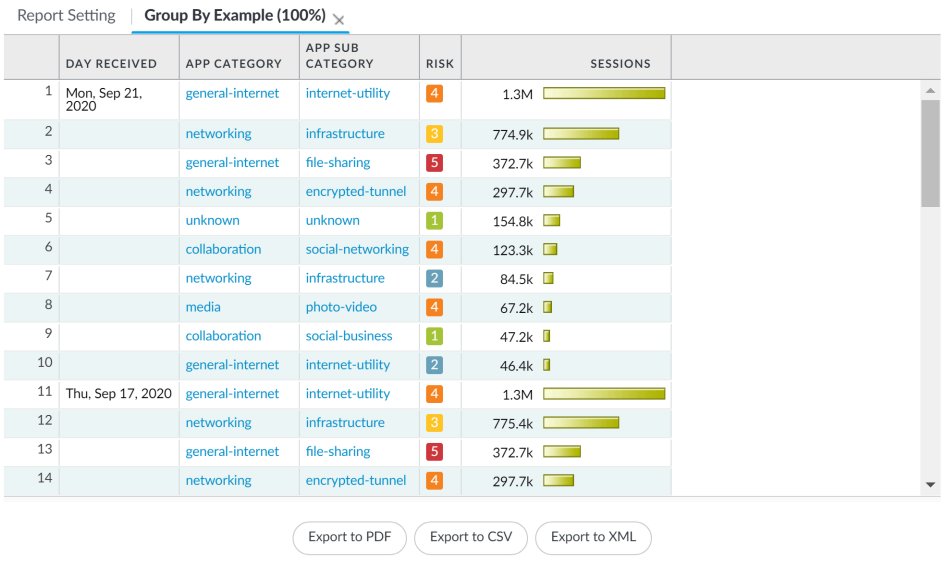
STEP 3 | **OK**、**Commit (**コミット**)** の順にクリックします。

カスタムレポート

確かな目的があるカスタム レポートを作成するには、脅威などの取得して分析したい重要な情報や各属性とともに、各脅威タイプに適用されるルールを把握できるようにルールの UUID でグループ化するなど、情報をカテゴリに分ける最適な方法を検討する必要があります。検討の結果を踏まえて、カスタム レポートで以下の選択を行います。

選択対象	説明
データベース	次のいずれかのデータベース タイプをレポートの基準にすることができます。 • サマリーデータベース—これらのデータベースは、アプリケーション統計、トラフィック、脅威、URL フィルタリング、およびトンネル検査ログで利用できます。ファイアウォールは、詳細ログを 15 分間隔で集約します。レポートを生成する際の応答時間を短くするために、ファイアウォールはデータを凝縮します。重複したセッションはグループ化されて繰り返しカウンターの数が増え、一部の属性（列）がサマリーから除外されます。

選択対象	説明
	• 詳細ログ—これらのデータベースはログをリスト化し、各ログ エントリのすべての属性 (列) を列挙します。 詳細ログに基づいたレポートは実行に時間がかかるため、絶対に必要な場合にのみ使用してください。
属性	一致条件として使用する列。属性は、レポートで選択可能な列です。[使用可能な列] のリストから、データを照合し、詳細情報を集約する（[選択した列]）ために選択基準を追加することができます。
ソート基準/グループ化基準	[ソート基準] および [グループ化基準] により、レポートのデータを整理/セグメント化できます。使用可能なソートおよびグループ化の属性は、選択したデータ ソースに応じて異なります。 Sort By （ソート基準）オプションでは、集約で使用する属性を指定します。ソート基準にする属性を選択しないと、レポートには集約情報なしで最初の N 件の結果が返されます。 Group By （グループ化基準）オプションにより、属性を選択し、その属性をデータをグループ化する場合のアンカーとして使用できます。レポート内のすべてのデータは、トップ 5、10、25、または 50 件のグループのセットで表示されます。たとえば、Group By （グループ化基準）として Hours （時間）を選択し、24 時間におけるトップ 25 件のグループを表示する場合、レポートの結果は 24 時間にわたり 1 時間単位で生成されます。レポートの最初の列は時間、それ以降の列は、管理者が選択したその他のレポート列です。
	以下の例は、レポートを生成するときに、[選択した列] および [ソート基準] / [グループ化基準] の基準がどのように関係するのかを示しています。  赤い円（上図）で囲まれた列は選択された列を示しています。これらの列は、レポートの生成で照合される属性です。データ ソースの各ログ エントリが解析され、これらの列が照合されます。選択した列について複数のセッションが同じ値を示す場合、それらのセッションは集約され、繰り返し回数（またはセッション数）が増えます。

選択対象	説明
	青の円で囲まれた列は、選択されたソート順序を示します。ソート順序（[ソート基準]）を指定すると、データは選択した属性を基準にしてソート（および集約）されます。 緑の円で囲まれた列は、[グループ化基準] の選択を示し、レポートのアンカーとして使用されます。**Group By**（グループ化基準）列は、トップ N 件のグループをフィルタリングするための適合基準として使用されます。次に、トップ N 件のグループのそれぞれについて、他のすべての選択した列の値がレポートに列挙されます。
	たとえば、レポートで以下のように選択されているとします  出力は以下のように表示されます。  レポートは [日] によってアンカーされ、[セッション] 別にソートされます。5 日分（[**5** グループ]）がリストに表示され、[過去 **7** 日間] の期間における最大トラフィックが表示されます。データは、選択した列（[カテゴリの追加]、[サプリケーション サブカテゴリ]、および [リスク]）について、各日の [トップ **5**] セッション別に列挙されます
タイム フレーム	データを分析するときの日付範囲。カスタム範囲を定義するか、過去 15 分～過去 30 日の範囲で期間を選択できます。レポート生成は、オ

選択対象	説明
	ンデマンドで実行するか、スケジュール設定して毎日または毎週単位で実行できます。
クエリ ビルダー	クエリ ビルダーにより、特定のクエリを定義して、選択した属性をさらに絞り込むことができます。**[and]** および **[or]** 演算子を使用してレポートで必要なもののみを表示し、次に、レポートのクエリに適合する、またはクエリを否定するデータを、含めたり除外したりできます。クエリを使用することで、より焦点を絞り込んだレポートを生成できます。

カスタム レポートの生成

ファイアウォールが直ちに（オンデマンド）あるいはスケジュールに従って（毎晩）生成するカスタム レポートを設定できます。カスタム レポートを参照し、目的に応じてカスタム レポートを作成するために使用できる選択肢を理解してください。

ファイアウォールがスケジュールされたカスタム レポートを生成した後で、設定を変更して将来の出力を変更すると、そのレポートの過去の結果が無効になる危険があります。スケジュール設定されたレポート設定を変更する必要がある場合は、新しいレポートを作成することをお勧めします。

STEP 1 | **Monitor (監視)** > **Manage Custom Reports (**カスタム レポートの管理**)**の順に選択します。

STEP 2 | **Add**[追加]をクリックし、レポートの **Name** [名前]を入力します。

事前定義済みテンプレートに基づいてレポートを作成するには、***Load Template***（テンプレートのロード）をクリックして、テンプレートを選択します。そのテンプレートを編集し、カスタム レポートとして保存できます。

STEP 3 | レポートで使用する **Database** （データベース）を選択します。

カスタム レポートを作成するごとに、ログ ビュー レポートが自動的に生成されます。このレポートには、カスタム レポートを作成するのに使用されたログが表示されます。ログ ビュー レポートでは、カスタム レポートと同じ名前が使用されますが、フレーズ（「ログ ビュー」）がレポート名に付加されます。

レポート グループを作成するときに、カスタム レポートと一緒にログ ビュー レポートを含めることができます。詳細については、レポート グループの管理を参照してください。

STEP 4 | レポートを毎晩実行する場合は、**[**スケジュール設定**]** チェック ボックスをオンにします。サイドの **Reports**（レポート）列でレポートが表示可能になります。

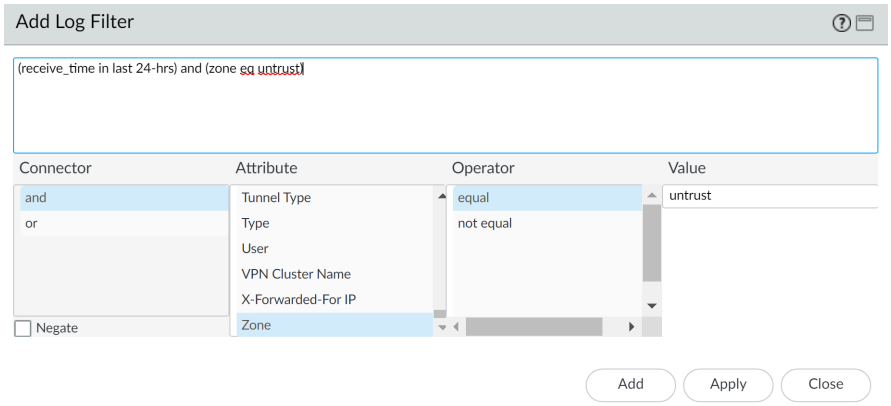
Panorama™ 管理サーバー上の *Cortex Data Lake* に保存されているログを使用してスケジュールされたカスタム レポートを生成するには、*Cloud Service* プラグイン *1.8* 以降のリリースが *Panorama* にインストールされている必要があります。

STEP 5 | フィルタリング基準を定義します。**Time Frame** (期間)、**Sort By** (ソート基準)の順序、**Group By** (グループ化基準)の設定を選択し、レポートに表示する列を選択します。

STEP 6 | （任意）選択基準をさらに絞り込む場合は、**[クエリ ビルダー]** 属性を選択します。レポート クエリを作成するには、以下を指定して、**Add**[追加] をクリックします。クエリが完成するまで、繰り返します。

- **Connector** （結合子） – 追加する式の前に置く結合子（and/or）を選択します。
- **Negate** – クエリを否定（除外）として解釈させるには、このチェック ボックスをオンにします。たとえば、過去 24 時間のエントリまたは Untrust ゾーンからのエントリを照合するように選択する場合に、Negate オプションを有効にすると、過去 24 時間以内ではなく、かつ Untrust ゾーンからではないエントリが一致します。
- **Attribute**（属性） – データ要素を選択します。使用可能なオプションは、選択したデータベースによって異なります。
- **Operator**[演算子] – 属性が適用されるかどうかを決定する基準を選択します (= など)。使用可能なオプションは、選択したデータベースによって異なります。
- **Value**（値） – 照合する属性値を指定します。

たとえば、（トラフィック ログ データベースに基づいた）以下の図は、トラフィック ログ エントリが過去 24 時間以内に「untrust」ゾーンから受け取られた場合に一致するクエリを示しています。



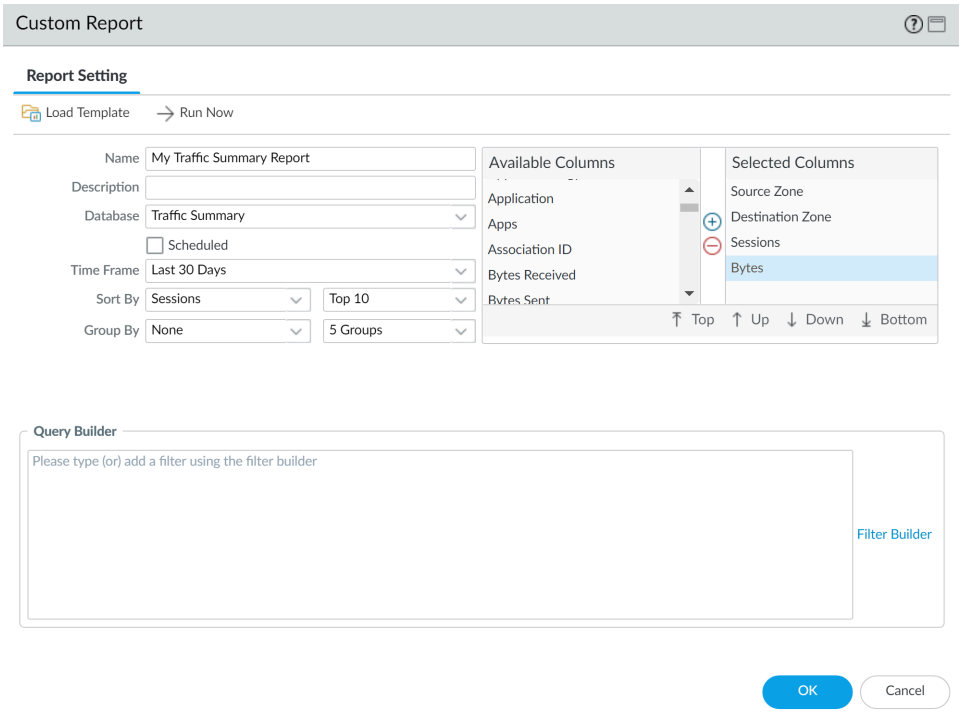
STEP 7 | レポート設定をテストするには、**Run Now**（今すぐ実行） を選択します。必要に応じて設定を変更し、レポートに表示する情報を変更します。

STEP 8 | **OK** をクリックしてカスタム レポートを保存します。

カスタム レポートの例

ここで、過去 30 日間のトラフィック サマリー データベースを使用する簡単なレポートをセットアップするとします。トップ 10 件のセッションごとにデータをソートし、これらの

セッションを週の曜日ごとに 5 つのグループにグループ化します。この場合、以下のようにカスタム レポートをセットアップします。



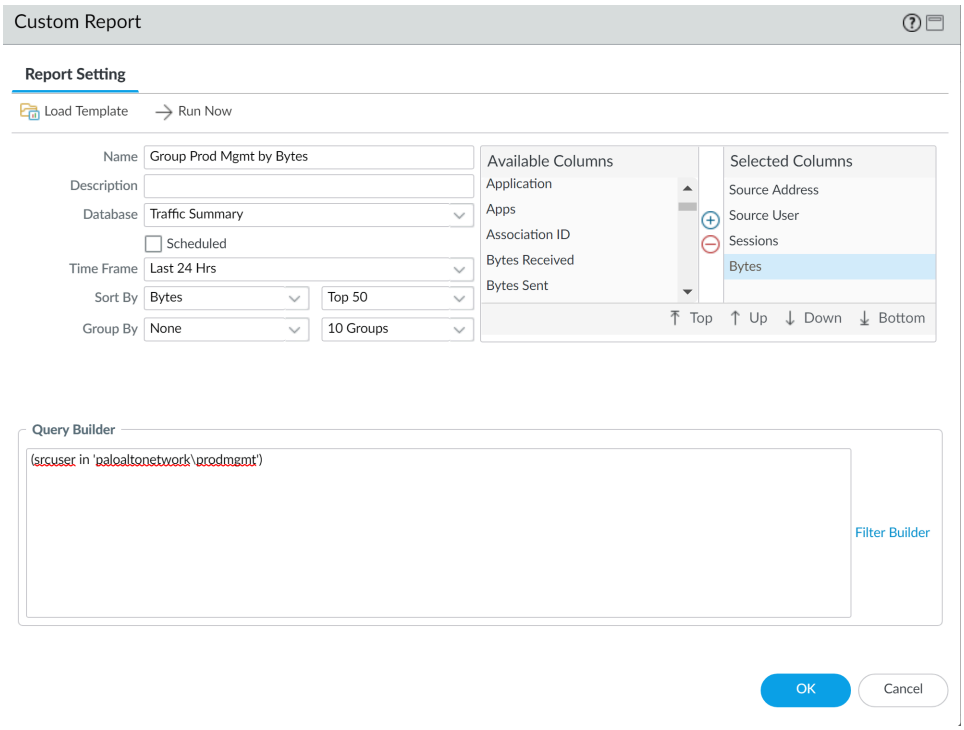
また、レポートの PDF 出力は以下のようになります。

My Traffic Summary Report

ca1demo.paloaltonetworks.com : 2016/01/25 10:34:39 - 2016/02/24 10:34:38

Source Zone	Destination Zone	App Category	Application	Sessions	Bytes
Tap	Tap	general-internet	web-browsing	74.54 M	2.47 T
Tap	Tap	networking	dns	52.03 M	28.93 G
Tap	Tap	networking	ssl	18.01 M	678.13 G
Tap	Tap	general-internet	bittorrent	9.80 M	1.62 T
Tap	Tap	general-internet	google-base	4.48 M	168.99 G
Tap	Tap	unknown	insufficient-data	4.45 M	31.30 G
Tap	Tap	collaboration	facebook-base	4.09 M	99.14 G
Tap	Tap	networking	ntp	4.07 M	3.29 G
Tap	Tap	collaboration	blackboard	2.84 M	186 G
Tap	Tap	collaboration	smtp	1.92 M	172.57 G
Tap	Tap	networking	icmp	1.36 M	320.49 M
Tap	Tap	general-internet	gnutella	1.17 M	17.84 G
Tap	Tap	collaboration	myspace-base	1.10 M	35.22 G
Tap	Tap	general-internet	ping	1.06 M	86.21 M
Tap	Tap	general-internet	flash	1.01 M	168.14 G

クエリ ビルダーを使用して、ユーザー グループ内のネットワーク リソースの上位消費ユーザーを表示するカスタム レポートを生成する場合は、以下のようにカスタム レポートをセットアップします。



このレポートには、製品管理ユーザー グループ内の上位ユーザーが、バイト数を基準にソートされて表示されます。

ボットネット レポートの生成

ボットネット レポートでは、ヒューリスティックで振る舞いベースのメカニズムを使用して、ネットワーク内でマルウェアまたはボットネットに感染した可能性のあるホストを識別できます。ボットネット アクティビティと感染したホストを評価するため、ファイアウォールでは、脅威、URL、およびデータ フィルタリング ログ内のユーザーおよびネットワークのアクティビティ データを、PAN-DB のマルウェア URL、既知のダイナミック DNS ドメイン プロバイダ、および過去 30 日以内に登録されたドメインのリストに相関付けます。こうしたサイトにアクセスしたホストに加え、Internet Relay Chat （IRC）サーバーと通信したホストや不明なアプリケーションを使用したホストを識別するようにレポートを設定できます。マルウェアの多くはダイナミック DNS を使用して IP のブロックを回避し、IRC サーバーの多くはボットを使用して自動化した機能を実行します。

ボットネット レポートを使用するには、ファイアウォールに脅威防御ライセンスと *URL* フィルタリング ライセンスが必要です。ボットネットレポートが使用する指標以外の追加の指標に基づいて、疑わしいアクティビティを監視する自動相関エンジンの使用があります。ただし、新しく登録されたドメインを指標として使用するツールは、ボットネット レポートのみです。

- ボットネット レポートの設定
- ボットネット レポートの出力の解釈

ボットネット レポートの設定

ボットネット レポートはスケジュールすることも、必要に応じて実行することもできます。ファイアウォールでは、24 時間ごとにスケジュールされたボットネット レポートを生成します。これは、振る舞いベースの検出では、その対象期間全体にわたって複数のログのトラフィックを相関付ける必要があるためです。

STEP 1 | ボットネットの可能性があるアクティビティを示すトラフィックのタイプを定義します。

1. **Monitor (監視)** > **Botnet** を選択し、ページの右側で **Configuration (構成)** をクリックします。
2. レポートに含まれるHTTPトラフィックのタイプごとの**Count**（カウント数）を**Enable**（有効化）します。

   Count [数]の値は、レポートでホストをより高い確度スコア（ボットネット感染の可能性がより高い）に関連付けるために最小限必要な、各トラフィック タイプのイベントの発生数を表します。イベント数が **Count** [数]より少ない場合、レポートにはより低い確度スコアが表示されるか、（特定のトラフィック タイプでは）ホストのエントリが表示されなくなります。たとえば、**Malware URL visit** [マルウェア URL へのアクセス]の **Count** [数]を 3 に設定した場合、既知のマルウェア URLに 3 回以上アクセスしたホストには、アクセス回数が 3 回未満のホストよりも高いスコアが設定されます。詳細は、ボットネット レポートの出力の解釈を参照してください。
3. 不明な TCP または不明な UDP アプリケーションが関与するトラフィックに関連付けられたホストをレポートに含めるかどうかを決定するしきい値を定義します。
4. IRC サーバーが関与するトラフィックを含めるには、**IRC** チェック ボックスをオンにします。
5. **OK** をクリックしてレポートの設定を保存します。

STEP 2 | レポートをスケジュールするか、必要に応じて実行します。

1. ページの右側で **Report Setting** [レポート設定]をクリックします。
2. **Test Run Time Frame** [ランタイム フレームのテスト] ドロップダウンでレポートの期間を選択します。
3. レポートに含める **No. of Rows (行数)** を選択します。
4. （任意）レポートに送信元/宛先 IP アドレス、ユーザー、ゾーンなどの属性別にフィルタをかける場合は、クエリ ビルダーにクエリを **Add**（追加）します。

   たとえば、IP アドレス 10.3.3.15 から開始されるトラフィックにはボットネット アクティビティが含まれる可能性がないことがあらかじめわかっている場合、「**`not (addr.src in 10.0.1.35)`**」をクエリとして追加し、そのホストをレポートの出力から除外します。詳細は、ボットネット レポートの出力の解釈を参照してください。
5. レポートを毎日実行する場合は **Scheduled** [スケジュール設定]を選択し、すぐにレポートを実行する場合は **Run Now** [今すぐ実行]をクリックします。
6. **OK**、**Commit (コミット)** の順にクリックします。

ボットネット レポートの出力の解釈

ボットネット レポートには、レポート設定時に疑わしいと定義したトラフィックに関連付けられたホストごとに 1 行が表示されます。レポートには、ホストごとに、ボットネット感染の可能性を示す 1 から 5 の確度スコアが表示されます（5 が最も高い可能性）。スコアは脅威重大度レベルに対応します。1: 情報、2: 低、3: 中、4: 高、5: 重要ファイアウォールは、以下の情報に基づいてスコアを設定します。

- **Traffic type**[トラフィック タイプ]– 特定の HTTP トラフィック タイプは、ボットネット アクティビティが含まれる可能性がより高くなります。たとえば、レポートでは、既知のマルウェア URL にアクセスするホストには、URL ではなく IP ドメインを参照するホストよりも高い確度を割り当てます（この両方のアクティビティが疑わしいと定義されている場合）。
- **Number of events** - 疑わしいイベントの数が多いホストは、>時に定義したしきい値 (**Count** 値) に基づいて、より高い信頼度スコアを持ちます。
- **Executable downloads**[実行可能なダウンロード] – レポートでは、実行可能なファイルをダウンロードしたホストにより高い確度を割り当てます。実行可能なファイルは多くの感染で使用されており、他の疑わしいトラフィック タイプと組み合せることで、侵入されたホストの調査に優先度を付けやすくなります。

レポート出力を確認するとき、ファイアウォールがボットネット アクティビティを評価するのに使用するソース（PAN-DB のマルウェア URL のリストなど）間にギャップがある場合があります。安全と見なしているトラフィックがこれらのソースで識別されることもあります。どちらの場合も補正するために、ボットネット レポートの設定時にクエリ フィルターを追加できます。

SaaS アプリケーション使用率レポートを生成しています...

SaaS アプリケーション使用率 PDF レポートは、2 つのパートからなるレポートで、SaaS アプリケーションのアクティビティをリスクおよび許可済み状態で簡単に調べることができます。許可されたアプリケーションは、ネットワークで使用することを正式に承認するアプリケーションです。SaaSアプリケーションは **Objects (オブジェクト)** > **Applications (アプリケーション)** のアプリケーション詳細ページで特性 SaaS=yes を持つアプリケーションです。他のすべてのアプリケーションは 非SaaS と見なされます。SaaS または 非 SaaS アプリケーションの区別を表示するには許可済みという事前設定済みのタグを付けます。この事前設定タグを持たないアプリケーションは、ファイアウォールおよび Panorama はネットワーク上で不許可となっているものと判断されます。

- レポートの最初の部分では、報告期間中に認可されたアプリケーションと認可されていないアプリケーションを比較し、使用状況、コンプライアンス、およびデータ転送による許可状態に基づいて上位のアプリケーションを一覧表示して、ネットワーク上の SaaS アプリケーションの重要な結果を示します。リスクの高いアプリケーションの使用状況を特定し調査するために、レポートの危険性の高いセクションのセクションには、達成された認証、過去のデータ侵害、IP ベースの制限のサポート、財政的実行可能性、および利用規約などの悪性ホスト特性を持つ SaaS アプリケーションが記載されています。また、ネットワークで使用するアプリケーションの合計数、アプリケーションが消費する帯域幅、およびアプリケーションを使うユーザー数、SaaS アプリケーションの大部分を使うトップ ユーザーグループ、制限付き/制限なしの SaaS アプリケーションを通して大量のデータを転送するトップ ユーザーグループに基づいた、制限付き/制限なしの SaaS アプリケーションの比較を閲覧できます。

レポートの前半は使用アプリケーション最大数、ユーザー数、アプリケーションサブカテゴリーに転送されたデータ量（バイト）の順にリストアップした上位 SaaS アプリケーションサブカテゴリーにも注目しています。

- レポートの後半部分には、レポート前半に記載された各アプリケーションサブカテゴリの SaaS および非 SaaS アプリケーションの閲覧に関する詳細な情報が含まれています。サブカテゴリー内のアプリケーションはデータを転送した上位ユーザー、上位ブロックまたはアラートファイルタイプ、および各アプリケーションの上位脅威の情報も含んでいます。さらに、このレポートセクションはファイアウォールが WildFire 分析のためにファイアウォールが送信した各アプリケーションのサンプルと 安全または有害と判定されたサンプル数を集計します。

このレポートの洞察を使ってビジネスクリティカルまたは認証 SaaS アプリケーションのリストを統合し、マルウェアの伝搬とデータ漏出の不要なリスクをもたらす恐れのあるアプリケーションの管理ポリシーを実行します。

定義済みの *SaaS* アプリケーション使用状況レポートは、特定の日にネットワーク上で実行されている上位 *100* の *SaaS* アプリケーション *(SaaS* アプリケーション特性 *SaaS=yes* を持つアプリケーション*)* を一覧表示する日次レポートの表示として引き続き使用できます。このレポートでは、認可済みと指定したアプリケーションの可視性は得られませんが、ネットワーク上で使用されているすべての *SaaS* アプリケーションの可視性が示されます。

STEP 1 | ネットワークでの使用を許可するアプリケーションに許可タグを付与します。

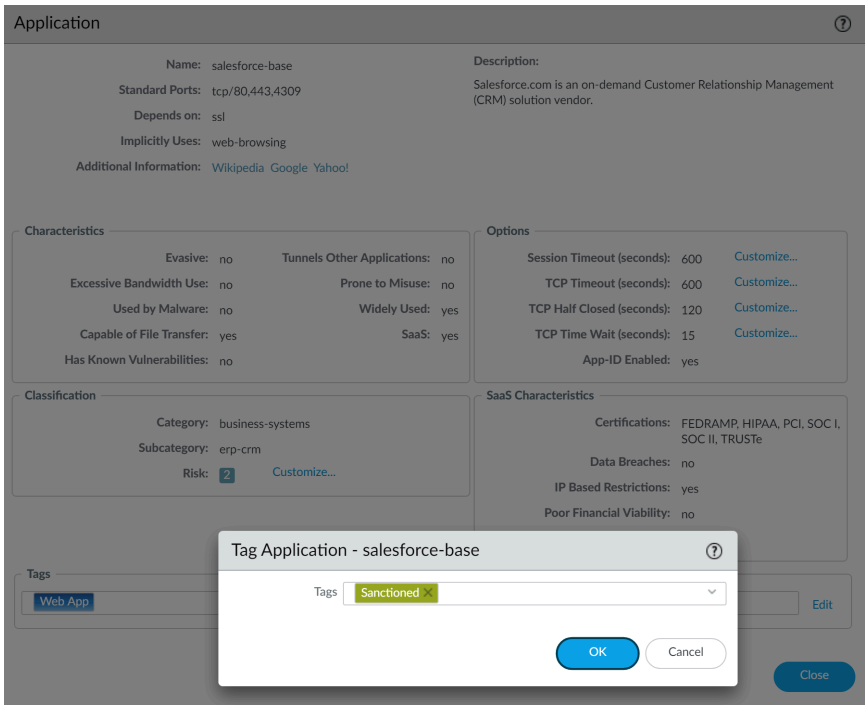
精確かつ情報が豊富なレポートを生成するためには、複数の仮想システムをもつファイアウォールや、*Panorama* 上のデバイスグループに属するファイアウォール全体で、許可されたアプリケーションに対するタグ付けを一貫させる必要があります。あるアプリケーションが一方の仮想システム上では許可されたアプリケーションとしてタグ付けされ、もう一方では不許可とされている場合、あるいは *Panorama* では親デバイスグループで不許可とされていて、子デバイスグループでは許可タグが付与されている場合（またはその逆）、*SaaS* アプリケーション使用状況レポートはアプリケーションが部分的に制限されていると報告し、結果が重複してしまいます。

例：Boxがvsys1で許可されていて、Google Driveがvsys2で許可されている場合、vsys1におけるGoogle Driveのユーザーは不許可のSaaSアプリケーションのユーザーとして計上され、vsys2におけるBoxのユーザーもまた不許可のSaaSアプリケーションのユーザーとして計上されてしまいます。レポートの主な内容として、ネットワーク上で2つの個別のSaaSアプリケーションが検出され、許可されたアプリケーションが2つ、不許可のアプリケーションが2つ、といったように記載されます。

1. **Objects (**オブジェクト**)** > **Application Filters (**アプリケーション フィルタ**)** を選択します。
2. アプリケーション**Name**[名]をクリックして、アプリケーションを編集し、タグセクションで **Edit**[編集]を選択します。

3. **Tag**[タグ]のドロップダウンリストから**Sanctioned**[許可済み]を選択します。

   事前定義された **Sanctioned**（許可済み）タグ（Sanctioned）を使用する必要があります。アプリケーションを許可したことを示すために別のタグを使用すると、ファイアウォールはタグを認識できず、レポートは不正確になります。



4. **OK**と**Close**[閉じる]をクリックして、全ての開いたダイアログを終了します。

STEP 2 | SaaS アプリケーション使用率レポートを生成しています...

1. **Monitor (監視)** > **PDF Reports (PDF レポート)** > **SaaS Application Usage (Saas アプリケーションの使用状況)** を選択します。
2. **Add**[追加]をクリックして、 **Name**[名前]を入力し、レポートの**Time Period** [期間]を選択します (デフォルトは **Last 7 Days**[過去7日間])。

   デフォルトでは、 レポートには、上位 *SaaS* と非 *SaaS* アプリケーションサブカテゴリーの詳細情報が含まれます。その結果、レポートのページ数とファイルサイズが非常に大きくなる可能性があります。ファイルサイズを小型化し、ページ数を *10* ページ以内にするには、***Include detailed application category information in report*** **(**レポートに詳細アプリケーションカテゴリ情報を含める**)** チェックボックスをクリアします。
3. レポートに **Include logs from (**次のログを含める**)**かどうか選択します。

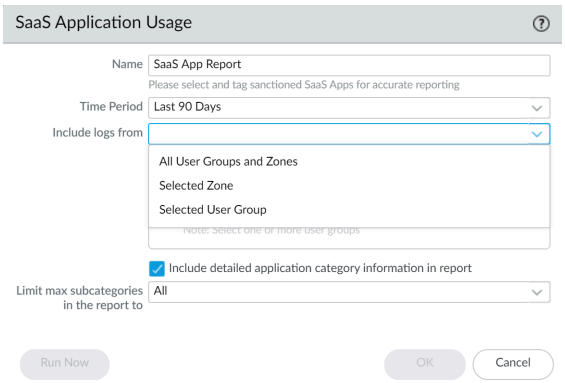
   PAN-OS 10.0.2 以降のリリースでは、*Cortex Data Lake* のログから生成されたレポートは、***Selected Zone*** **(**選択したゾーン**)** からのログのみを含めてサポートします。.

   - **All User Groups and Zones (**すべてのユーザーグループおよびゾーン**)**—ログで利用できるすべてのセキュリティ ゾーンおよびユーザーグループのデータがレポートに含まれます。

     レポートに特定のユーザーグループを含めたい場合は、**Include user group information in the report (**ユーザーグループ情報をレポートに含める**)** を選択し、**manage groups (**グループの管理**)** リンクをクリックして含めたいグループを選択します。選択されたユーザーグループ用のログをファイアウォールあるいは Panorama がフィルタリングできるよう、0～最大 25 のユーザーグループを追加する必要があります。含めるグループを選択する場合、レポートはすべてのユーザーグループを Others (その他) と呼ばれる単一のグループに集約します。
   - **Selected Zone (**選択したゾーン**)**—レポートは選択したセキュリティ ゾーンに基づいてデータをフィルタリングし、そのゾーンだけのデータを含めます。

     レポートに特定のユーザーグループを含めたい場合は、**Include user group information in the report (**ユーザーグループ情報をレポートに含める**)** を選択し、**manage groups for selected zone (**選択したゾーンのグループの管理**)** リンクをクリックし、レポートに含めたいそのゾーン内のユーザーグループを選択します。セキュリティ ゾーン内の選択されたユーザーグループ用のログをファイアウォールあるいは Panorama がフィルタリングできるよう、0 ～最大 25 のユーザーグループを追加する必要があります。含めるグループを選択する場合、レポートはすべてのユーザーグループを Others (その他) と呼ばれる単一のグループに集約します。

- **Selected User Group (選択したユーザーグループ)**—レポートは特定のユーザーグループのみに基づいてデータをフィルタリングし、その選択したユーザーグループのみを対象にした SaaS アプリケーションの使用率情報を含めます。



4. レポートにすべてのアプリケーション サブカテゴリを含める（デフォルト）か、あるいは上位の 10、15、20、25 カテゴリに **Limit the max subcategories in the report (レポートの最大サブカテゴリ数を制限)** するかを選択します（デフォルトはすべてのサブカテゴリ）。
5. **Run Now (今すぐ実行)** をクリックすれば、直近の 7 日間あるいは 30 日間分のレポートを必要なときに生成できます。レポートが新しいタブを開くので、ブラウザでポップアップブロッカーがオフになっていることを確認してください。
6. **OK** をクリックして変更内容を保存します。

STEP 3 | 「電子メールで配信するレポートのスケジュール設定」を行います。

直近の 90 日のレポートはメール配信用にスケジ.ュール設定されなければなりません。

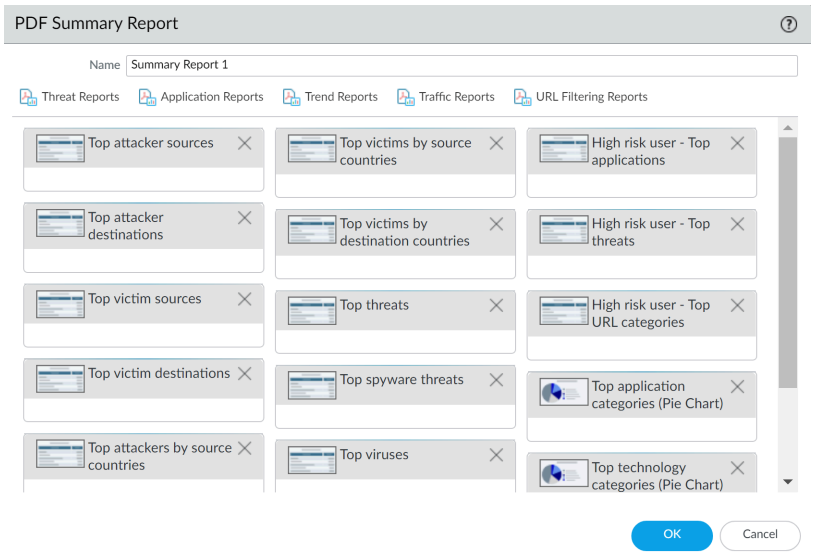
PA-220R および PA-800 Series のファイアウォールでは、SaaS アプリケーション使用状況レポートは PDF として電子メールに添付されるわけではありません。かわりに、電子メールにはリンクが記載されており、クリックすればウェブブラウザでレポートを開くことができます。

PDF サマリー レポートの管理

PDF サマリー レポートには、各カテゴリの上位 5 件（上位 50 件ではない）のデータに基づき、既存のレポートから集められた情報が含まれています。このレポートには、別のレポートでは表示されないトレンド チャートも表示されます。

STEP 1 | **[PDF サマリー レポート]** をセットアップします。

1. **Monitor** > **PDF Reports** > **Manage PDF Summary**(監視 > PDF レポート > PDF サマリーの管理) の順に選択します。
2. **Add**[追加]をクリックし、レポートの **Name** [名前]を入力します。
3. 各レポート グループのドロップダウンを使用し、1 つ以上の要素を選択して、PDF サマリー レポートを設計します。最大 18 個のレポート要素を含めることができます。



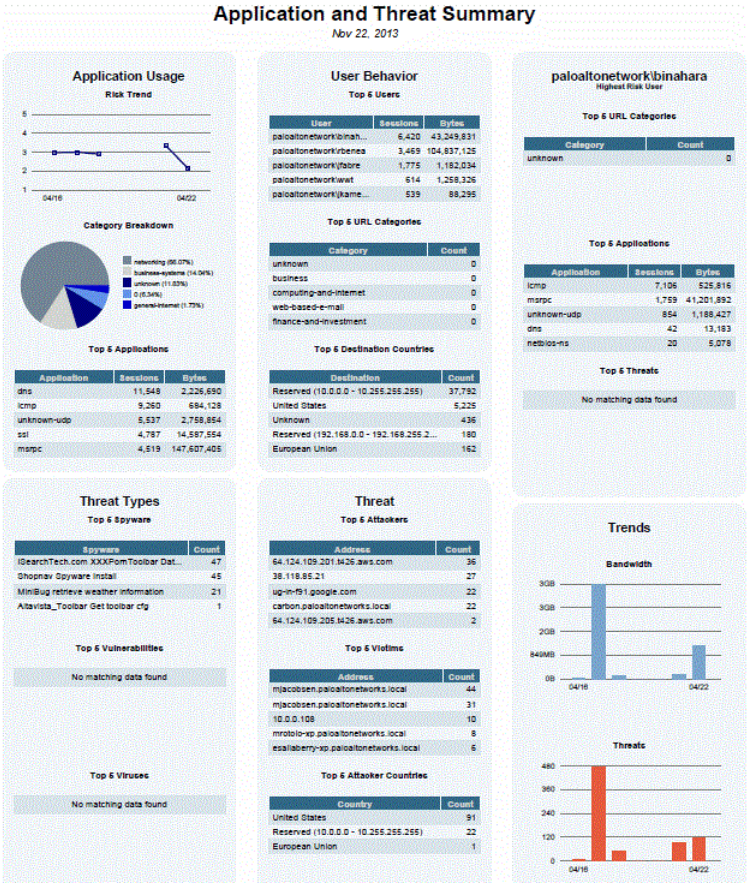
PDF サマリー レポートの事前定義済みウィジェット列に ***Top Threats***（上位の脅威） を選択すると、`top-attacks`として表示されます。

- レポートから要素を削除するには、**x** アイコンをクリックするか、該当するレポート グループのドロップダウンから選択をクリアします。
- レポートを再配列するには、アイコンをレポートの別のエリアにドラッグしてドロップします。

4. **[OK]** をクリックしてレポートを保存します。
5. 変更を **Commit**（コミット）します。

STEP 2 | レポートを表示します。

PDF サマリー レポート をダウンロードして表示するには、レポートの表示を参照してください。



以下のサマリー セクションは、以下の *PDF* サマリー レポート要素を参照しています。

- ***Top 5 Attacks***（攻撃のトップ *5*）*–op threats*（上位の脅威）要素を指します。
- ***Top 5 Threats***（脅威トップ *5*）*–High risk user - Top threats*（高リスク ユーザー-上位の脅威）要素を指します。
- 上位の脅威レポート*–Top threats*（上位の脅威）要素からの脅威の全リストを参照します。

ユーザー/グループ アクティビティ レポートの生成

ユーザー/グループ アクティビティ レポートには、個々のユーザーまたはユーザー グループの Web アクティビティが要約されます。両方のレポートには同じ情報が含まれています。例外として、**Browsing Summary by URL Category** （URL カテゴリ別ブラウザ サマリー）および **Browse time calculations** （ブラウズ時間の計算結果）はユーザー アクティビティ レポートにのみ含まれています。

firewall でUser-IDを構成して、ユーザーおよびユーザー・グループのリストにアクセスする必要があります。

STEP 1 | ユーザー/グループ アクティビティ レポートのブラウズ時間とログ数を設定します。

デフォルト値を変更する場合にのみ必要です。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)**の順に選択し、Logging and Reporting Settings (ロギングおよびレポート設定) を編集して、**Log Export and Reporting (ログのエクスポートとレポート)** タブを選択します。
2. **Max Rows in User Activity Report** （ユーザー アクティビティ レポートの最大行数）に、詳細なユーザー アクティビティ レポートでサポートされる最大行数を入力します（範囲は 1 ～ 1048576、デフォルトは 5000）。これにより、レポートで分析されるログの数が決まります。
3. ユーザーが Web ページを閲覧するのにかかる推定時間**Average Browse Time** [平均ブラウズ時間] を入力します（範囲は 0 ～ 300、デフォルトは 60）。平均ブラウズ時間が経過した後に行われた要求が、新しいブラウズ アクティビティと見なされます。この計算では、ユーザーがアクセスしたページのみを記録 (URL フィルタリング ログに記録されている) を基準として使用し、最初の要求の時刻 (開始時刻) から平均ブラウズ時刻までの間に読み込まれた新しい Web ページを無視します。たとえば、**Average Browse Time** （平均ブラウズ時間）が 2 分に設定されている場合は、ユーザーが Web ページを開いてそのページを 5 分間閲覧しても、そのページのブラウズ時間は 2 分になります。ファイアウォールはユーザーがあるページを閲覧する時間を判断できないため、このような動作が設定されています。平均ブラウズ時間の計算では、Web 広告やコンテンツ配信ネットワークとして分類されたサイトは無視されます。
4. **Page Load Threshold** （ページ ロードしきい値）に、ページ要素がページにロードされるまでの推定時間を秒単位で入力します（デフォルトは 20）。最初のページ ロードからページ ロードしきい値の間に発生する要求は、ページの要素と見なされます。ページ ロードしきい値の範囲外で発生する要求は、ページ内のリンクをユーザーがクリックしたものと見なされます。
5. **OK** をクリックして変更内容を保存します。

STEP 2 | ユーザー/グループ アクティビティ レポートを生成します。

1. **Monitor (監視)** > **PDF Reports (PDF レポート)** > **User Activity Report (ユーザー アクティビティ レポート)** の順に選択します。
2. **Add**[追加]をクリックし、レポートの **Name** [名前]を入力します。
3. レポートを作成します。
   - ユーザー アクティビティ レポート – **User (ユーザー)** を選択し、ユーザーの **Username (ユーザー名)** または **IP address (IP アドレス)** （IP アドレス）（IPv4 または IPv6）を入力します。
   - グループ アクティビティ レポート – **Group** （グループ）を選択し、ユーザー グループの **Group Name** （グループ名）を選択します。
4. レポートの **Time Period** （期間）を選択します。
5. （任意）必要に応じて、レポートに詳細な URL ログを含めるには、**Include Detailed Browsing (詳細なブラウジングを含める)** チェック ボックスをオンにします（デフォルトはオフ）。

   詳細な閲覧情報には、選択したユーザーまたはユーザー グループの大量の (何千もの) ログが含まれる可能性があり、その結果、レポートが非常に大きくなる可能性があります。
6. オンデマンドでレポートを実行するには、（今すぐ実行） をクリックします。
7. レポート設定を保存するには、**OK** をクリックします。ユーザー/グループ アクティビティ レポートの出力はファイアウォール上に保存できません。レポートの電子メール配信をスケジュールするには、「電子メールで配信するレポートのスケジュール設定」を参照してください。

レポート グループの管理

レポート グループを使用すると、レポートのセットを作成できます。システムはそのレポートのセットをまとめ、オプションのタイトル ページとすべての構成レポートが含まれる 1 つの集約された PDF レポートを送信することができます。

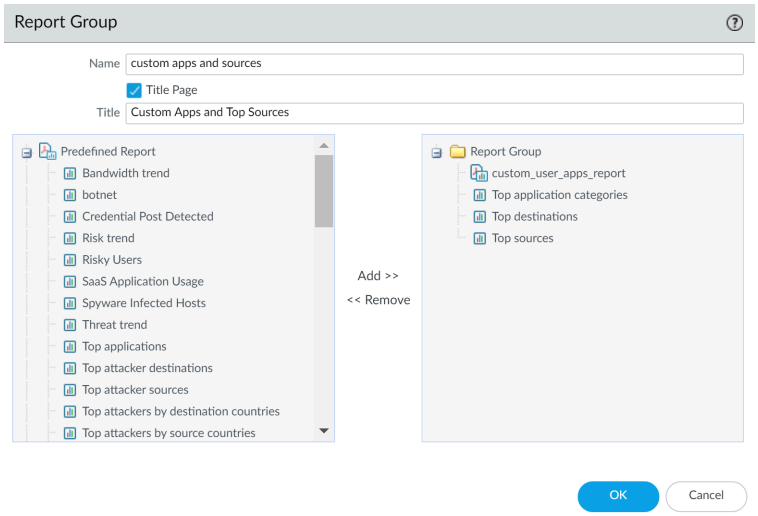
レポート グループをセットアップします。

レポートを電子メールで送信するためのレポート グループをセットアップする必要があります。

1. 電子メール サーバー プロファイルを作成します。

2. **[レポート グループ]** を定義します。レポート グループでは、事前定義済みレポート、PDF サマリー レポート、カスタム レポート、およびログ ビュー レポートを 1 つの PDF にまとめることができます。

   1. **Monitor (監視)** > **Logs (ログ)**を選択します。
   2. **Add** [追加]をクリックし、レポート グループの **Name** [名前]を入力します。
   3. （任意）**Title Page**（タイトル ページ）を選択して、PDF 出力の **Title**（タイトル）を追加します。
   4. レポートグループに含めるレポートを左側の列から選択して **[追加]** をクリックし、各レポートを右側のレポート グループに移動します。



   Log View[ログ ビュー] レポートは、カスタム レポートを作成するたびに自動的に作成されるレポート タイプで、カスタム レポートと同じ名前が使用されます。このレポートには、カスタム レポートの内容を作成するために使用されたログが表示されます。

   ログ ビュー データを含めるには、レポート グループを作成するときに Custom Reports（カスタム レポート） リストにカスタム レポートを追加し、次に **Log View**（ログ ビュー） リストから一致するレポート名を選択してログ ビュー レポートを追加します。レポートには、カスタム レポート データと、カスタム レポートの生成に使用されたログ データが含まれています。

   5. **OK** をクリックして設定を保存します。
   6. レポート グループを使用する方法については、電子メールで配信するレポートのスケジュール設定を参照してください。

電子メールで配信するレポートのスケジュール設定

レポートは、毎日配信されるか、特定の曜日に毎週配信されるようにスケジュール設定することができます。スケジュール設定されたレポートの実行は午前 2 時に開始され、スケジュール設定されたすべてのレポートが生成された後に電子メール配信が開始されます。

STEP 1 | **Monitor (監視)** > **PDF Reports (PDF レポート)** > **Email Scheduler (電子メール スケジューラ)** を選択して **Add (追加)** をクリックします。

STEP 2 | **Name** [名前]にスケジュールを識別する名前を入力します。

STEP 3 | 電子メールで配信する **[レポート グループ]** を選択します。レポート グループをセットアップするには、レポート グループの管理を参照してください。

STEP 4 | **Email Profile (**電子メール プロファイル**)** で、レポートの配信に使用する電子メール サーバー プロファイルを選択するか、**Email Profile (**電子メール プロファイル**)** リンクをクリックして電子メール サーバー プロファイルを作成します。

STEP 5 | **[**繰り返し**]** では、レポートを生成して送信する頻度を選択します。

STEP 6 | **Override Email Addresses**[電子メールアドレスの上書]フィールドでこのレポートを指定受信者だけに送信できます。このフィールドに受信者を追加すると、そのレポートは、電子メール サーバー プロファイルで設定されている受信者には送信されません。このオプションは、電子メール サーバー プロファイルで定義されている管理者または受信者以外の受信者の注意を喚起する場合に使用します。

STEP 7 | **OK**、**Commit (**コミット**)** の順にクリックします。

レポートのストレージ容量を管理

ファイアウォールにはデフォルトで、ファイアウォールが生成するレポート専用の 200MB のストレージが含まれています。特に PA-7000 Series および PA-5200 Series ファイアウォールなどの一部の場合では、新しいレポートを生成するためにレポート用のストレージ容量を増やす必要があるかもしれません。

STEP 1 | ファイアウォール CLI にアクセスします。

STEP 2 | ファイアウォールの現在のレポート用ストレージ容量を確認します：

コマンドの出力として、レポート用ストレージのサイズがバイト単位で表示されます。この作業では、ファイアウォールにデフォルトの 200MB のレポート用ストレージ容量があります。

```
admin@ISP-CONDOR-B(active)> request report-storage-size show

209715200
```

STEP 3 | レポート用ストレージ容量の拡張に向けてファイアウォールが十分なストレージを割り当てられることを確認します：

```
admin> show system disk-space
```

```
admin@ISP-CONDOR-B(active)> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        12G  8.9G  2.0G  83% /
none            7.9G   52K  7.9G   1% /dev
/dev/sda5        16G  8.5G  5.9G  59% /opt/pancfg
/dev/sda6        12G  5.8G  5.0G  54% /opt/panrepo
tmpfs           7.9G  247M  7.6G   4% /dev/shm
/dev/sda8        22G  8.7G   12G  43% /opt/panlogs
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/lcaas/ssl/private
```

STEP 4 | 必要に応じてレポート用ストレージ容量を増やします：

例えば、ここではレポート用ストレージのサイズを 1GB に増やします。

```
admin> request report-storage-size set size <0-4>
```

```
admin@ISP-CONDOR-B(active)> request report-storage-size set size 1

cfg.report-storage-size-gb: 1
```

STEP 5 | 前のステップで設定した量までレポート用ストレージ容量が増えているのを確認します：

```
admin> request report-storage-size show
```

```
admin@ISP-CONDOR-B(active)> request report-storage-size show

1073741824
```


ポリシー ルールの使用状況を表示する

セキュリティ、NAT、QoS、ポリシー ベースの転送（PBF）、復号化、トンネル検査、アプリケーション オーバーライド、認証、または DoS 保護ルールがトラフィックに一致する回数を表示して、環境やセキュリティのニーズが変化するにつれてファイアウォール ポリシーを最新の状態に保ちます。サーバーが廃止されたときや、サービスへの一時的なアクセスが不要になったときなど、過剰なプロビジョニング アクセスを悪用されないようにするには、ルール使用ヒット数データを使用して未使用ルールを特定して削除します。

ポリシー ルール使用状況データによって、ルール追加とルール変更を検証し、ルールが使用された時間枠を監視することができます。たとえば、ポートベースのルールをアプリベースのルールに移行する場合は、ポートベースのルールの上にアプリベースのルールを作成し、ポートベースのルールに一致するトラフィックを確認します。移行後、ヒット数データは、トラフィックがポートベースのルールではなくアプリベースのルールに一致しているかどうかを確認することで、ポートベースのルールを安全に削除できるかどうかを判断するのに役立ちます。ポリシー ルールのヒット数は、ルールがアクセスの強制に有効かどうかを判断するのに役立ちます。

ルール ヒット数データをリセットして、既存のルールを検証したり、指定された期間内にルールの使用状況を測定することができます。ポリシー ルールのヒット数データはファイアウォールや Panorama に保存されないため、ヒット数をリセット（クリア）した後はデータを利用できなくなります。

ポリシー ルールベースをフィルタリングした後、管理者は、ポリシー オプティマイザから直接ポリシー ルールを削除、無効化、有効化、およびタグ付けを行うことができます。たとえば、未使用のルールをフィルタリングしてから、そのルールを安全に削除するか、ルールベースに残すかを判断するためにタグを付けてレビューすることができます。管理者がポリシーオプティマイザから直接アクションを実行できるようにすることで、必要な管理オーバーヘッドを削減し、ルールのライフサイクル管理を簡素化し、ファイアウォールの過剰なプロビジョニングを防ぐことができます。

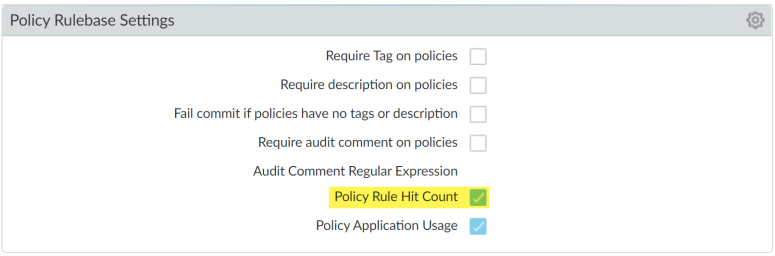
ルールのヒット数データは、高可用性 *HA* デプロイメントのファイアウォール間で同期されないため、各ファイアウォールのポリシー ルール ヒット数データを表示するには、各ファイアウォールにログインするか、または *Panorama* を使用して *HA* ファイアウォールピアに関する情報を表示する必要があります。

ポリシー ルールの使用状況データは、セキュリティ ポリシー ルールの最適化を使用して、最初に移行またはクリーンアップするルールを決定する場合にも役立ちます。

STEP 1 | 「Web インターフェイスの起動」を行います。

STEP 2 | **Policy Rule Hit Count (**ポリシールールのヒット数**)** が有効になっていることを確認します。

1. ポリシールールベース設定（**Device (**デバイス**)** > **Setup (**セットアップ**)** > **Management (**管理**)**）に移動します。
2. **Policy Rule Hit Count (**ポリシールールのヒット数**)** が有効になっていることを確認します。

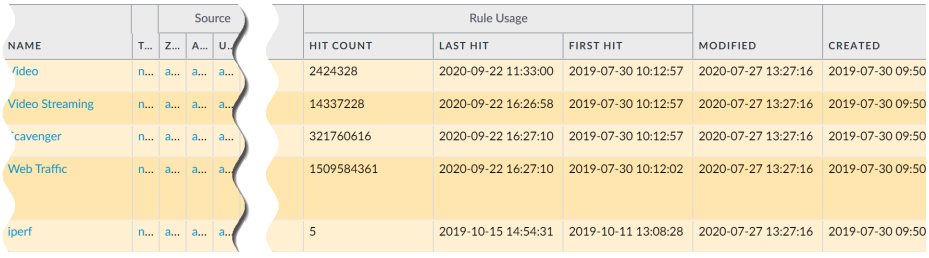


STEP 3 | **Policies (**ポリシー**)**を選択します。

STEP 4 | 各ポリシー ルールのポリシー ルール使用状況を表示します。

- ヒット数–トラフィックがポリシー ルールで定義した基準と一致した回数。手動でルールをリセットまたは名前を変更しない限り、再起動、データプレーンの再起動、およびアップグレードによって保持されます。
- 最終ヒット–トラフィックがルールと一致したときの最新のタイムスタンプ。
- 初回ヒット–トラフィックがこのルールに一致した最初のインスタンス。
- 編集–ポリシールールを最後に編集した日時です。
- 作成–ポリシールールが作成された日時です。

Panorama で *PAN-OS 8.1* を実行し、ポリシー ルール ヒット カウント設定が有効になっているときにルールが作成された場合、*PAN-OS 9.0* へのアップグレード時は、*First Hit (*最初のヒット*)* が作成日として使用されます。ポリシー ルール ヒット カウントの設定が無効なときに *PAN-OS 8.1* でルールを作成した場合、または *Panorama* で *PAN-OS 8.0* 以前のリリースを実行しているときにルールが作成された場合、*Panorama* が *PAN-OS 9.0* に正常にアップグレードされた日時が *PAN-OS 9.0* の作成日として使用されます。



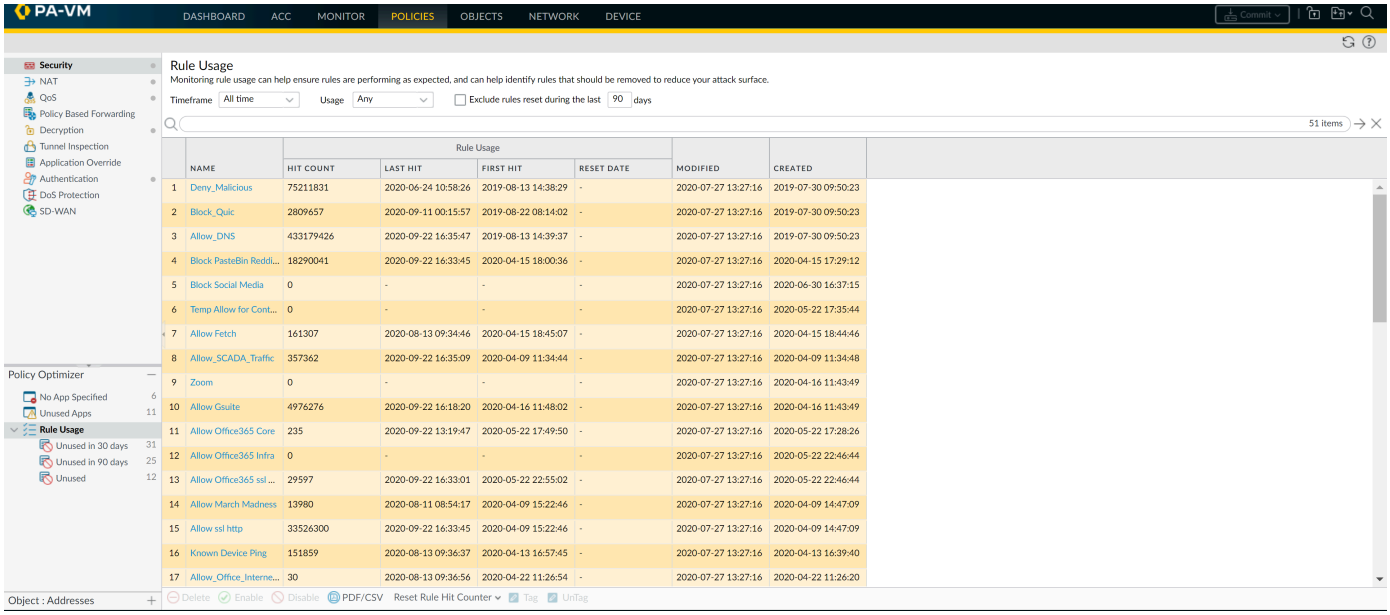
STEP 5 | Policy Optimizer ダイアログで、**Rule Usage**（ルール使用）フィルターを表示します。

STEP 6 | 選択したルールベースのルールをフィルタリングします。

ルール使用状況のフィルタを使用し、特定の期間でルール使用状況を評価します。たとえば、過去 *30* 日間の *Unused* (未使用) ルールを選択したルールベースでフィルタリングします。作成日や変更日など、他のルール属性を使用してルールの使用状況を評価することもできます。これにより、確認する一連の正しいルールをフィルタリングできます。ルールのライフサイクルを管理し、ネットワークへの攻撃の入り口を減らすためにルールを削除する必要があるかどうかを判断するためにこのデータを使用することができます。

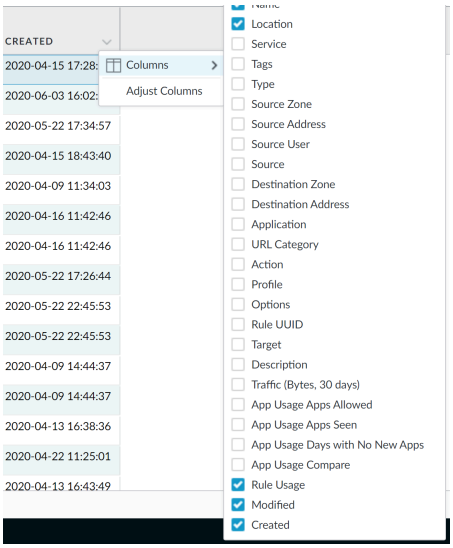
1. フィルタリングする **Timeframe** (時間枠) を選択するか、**Custom** (カスタム) 時間枠を指定します。
2. フィルタするルール **Usage** (使用状況) を選択します。
3. (オプション) ルールのルール使用状況データをリセットした場合は、過去 ***<number of days>*** 日間にリセットされたルールを除外する を確認し、ルールがリセットされてか

ら指定した日数に基づいてルールを除外するタイミングを決定します。指定した日数より前にリセットされたルールのみが、フィルタリング結果に含まれます。



4. （任意）ルールデータに基づいて検索フィルターを指定します。

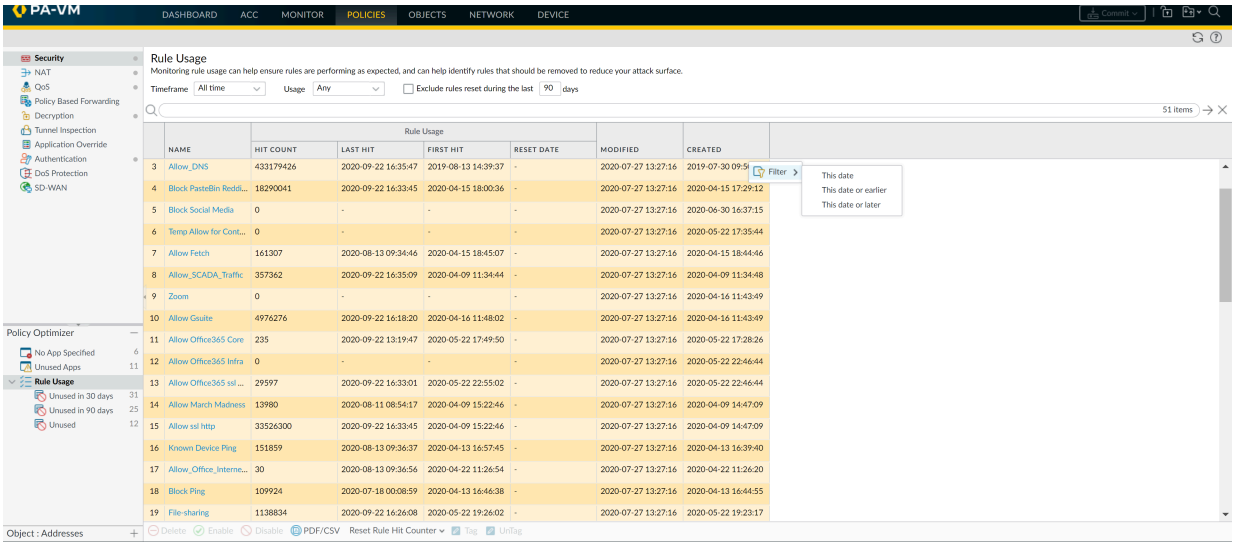
1. カーソルを列ヘッダーと**Columns**（列）に合わせます。
2. フィルタをかけたり表示したりする列を追加します。



3. **Filter**（フィルタ）でフィルタリングする列データにカーソルを合わせます。日付を含むデータの場合は、**This date (**現在の日付**)**、**This date or earlier (**現在の日付以

前)、または **This date or later** (現在の日付以降) の内どれを使用してフィルタリングするかを選択します。

4. フィルタの適用 (→)。



STEP 7 | 1つ以上の未使用のポリシールールへのアクションを実行します。

1. 1つ以上の未使用のポリシー ルールを選択します。
2. 以下のいずれかのアクションを実行します。
   - **Delete** (削除)—選択した1つ以上のポリシー ルールを削除します。
   - **Enable** (有効化)—無効な時、1つ以上の選択したポリシー ルールを有効にします。
   - **Disable** (無効化)—選択した1つ以上のポリシー ルールを無効にします。
   - **Tag** (タグ)—1つ以上のグループ タグを1つ以上の選択したポリシー ルールに適用します。ポリシールールにタグを付けるためには、グループタグが既に存在している必要があります。
   - **Untag** (タグ外し)—選択した 1 つ以上のポリシー ルールから 1 つ以上のグループ タグを削除します。
3. 変更を **Commit** (コミット) します。

モニタリングでの外部サービスの使用

外部サービスを使用してファイアウォールをモニターすると、重要なイベントに関するアラートの受信、専用の長期的なストレージを持つシステムへのモニターした情報のアーカイブ、サードパーティのセキュリティ モニタリング ツールとの統合が可能になります。外部サービスを使用する一般的なシナリオとして、以下のようなものがあります。

- 重要なシステム イベントまたは脅威について直ちに通知を受け取るためには、SNMP を使用した統計のモニター、トラップを SNMP マネージャに転送する、または電子メール アラートの設定を実行可能です。
- API を公開しているサードパーティのサービスに対して直接 HTTP ベースの API リクエストを送信して作業やアクションを自動化するために。例えば、定義済みの条件にマッチするログを転送して Service Now 上でインシデンス チケットを作成し、外部システムに頼ることなく Syslog メッセージ あるいは SNMP トラップを HTTP リクエストに変換します。HTTP リクエスト内の URL、HTTP ヘッダ、パラメータ、ペイロードを修正し、ファイアウォール ログの属性に基づいてアクションをトリガーできます。ログを HTTP(S) 宛先に転送を参照してください。
- ログの長期保管とファイアウォール監視の中央管理を行う場合は、Syslog 監視の設定を行い、ログ データを Syslog サーバーに送信できます。これにより、Splunk! や ArcSight などのサードパーティのセキュリティ モニタリング ツールとの統合が可能になります。
- ファイアウォール インターフェイスを通過する IP トラフィックのモニタリング統計を参照する場合は、NetFlow エクスポートの設定を行い、NetFlow コレクタで統計を表示できます。

ファイアウォールから直接外部システムへ、またはファイアウォールから Panorama への を行ってから、ログを各サーバーに転送するように Panorama を設定できます。ログの転送先を決定する際に考慮する要因については、「Log Forwarding Options [ログ転送オプション]」を参照してください。

NetFlow レコードを *Panorama* で集約することはできません。ファイアウォールから直接 *NetFlow* コレクタに送信する必要があります。

電子メール アラートの設定

電子メール アラートは、システム ログ、設定ログ、HIP マッチ ログ、相関ログ、脅威ログ、WildFire 送信ログ、トラフィック ログに設定できます。電子メール通知の送信に使用するプロファイルを分けることで、各ログ タイプをそれぞれ異なるサーバーに送信できます。可用性を高めるには、1 つのプロファイルに複数のサーバー（最大 4 個）を定義します。

ベストプラクティスとして、ファイアウォールが電子メールをサーバーに中継する前に、ファイアウォールが電子メール サーバーで認証することを要求するように*Transport Layer Security (*トランスポート レイヤー セキュリティ *-TLS)* を設定します。これにより、スパムやマルウェアの送信に使用される *Simple Mail Transfer Protocol (*シンプル メール トランスファー プロトコル *- SMTP)* リレーや、フィッシング攻撃に使用される電子メールのスプーフィングなどの悪意のある活動を防ぐことができます。

STEP 1 | (TLS 上の SMTP に対して必須) すでに実行済みである場合は、該当の電子メール サーバーの証明書プロファイルを作成します。

STEP 2 | **Device (**デバイス**)** > **Server Profiles (**サーバー プロファイル**)** > **Email (**電子メール**)**の順に選択します。

STEP 3 | 電子メール サーバ プロファイルを**Add (**追加**)** し、**Name (**名前**)** を入力します。

STEP 4 | 表示される読み取り専用ウィンドウで、電子メール サーバーを**Add (**追加**)** し、**Name (**名前**)** を入力します。

STEP 5 | ファイアウォールに複数の仮想システム（vsys）がある場合、このプロファイルを使用可能な **Location** [場所]（vsys または **Shared** [共有]）を選択します。

STEP 6 | (オプション)**Email Display Name (**電子メール表示名**)** を入力して、電子メールのFrom (送信者) フィールドに表示する名前を指定します。

STEP 7 | ファイアウォールが電子メールを送信する元の **From (**送信者**)** 電子メール アドレスを入力します。

STEP 8 | ファイアウォールが電子メールを送信する先の**To (**受信者**)** 電子メール アドレスを入力します。

STEP 9 | (オプション) 2 つ目のアカウントに電子メールを送信する場合は、**Additional Recipient(**追加の受信者**)** にアドレスを入力します。追加できる受信者は 1 名のみです。複数の受信者を追加する場合は、配布リストの電子メール アドレスを追加します。

STEP 10 | 電子メールの送信に使用する **Email Gateway**（電子メールゲートウェイ） の IPアドレスまたはホスト名を入力します。

STEP 11 | 電子メール サーバーへの接続に使用するプロトコルの**Type (**種類**)** を選択します:

- **Unauthenticated SMTP (**未認証の **SMTP)** — SMTP を使用して、認証なしで電子メール サーバーに接続します。デフォルトの **Port (**ポート**)** は 25 ですが、オプションで別のポー

トを指定出来ます。このプロトコルはSMTP over TLSと同じセキュリティを提供しませんが、このプロトコルを選択した場合は、次の手順をスキップしてください。

- **SMTP over TLS**—(推奨) TLS を使用して、電子メール サーバーに接続するための認証を要求します。次の手順に進み、TLS 認証を設定します。

STEP 12 | (SMTP over TLS 専用) TLS 認証を使用して電子メール サーバーに接続するようにファイアウォールを設定します。

1. (オプション) 電子メールサーバーへの接続に使用する **Port(ポート)** を指定します (デフォルトは 587 です)。
2. **TLS Version (TLS** バージョン**)** —TLS バージョン (**1.1** または **1.2**) を指定します。

   Palo Alto Networks では、最新の *TLS* バージョンの使用を強く推奨しています。
3. ファイアウォールと電子メール サーバーの**Authentication Method (**認証方法**)** を選択します:
   - **Auto (**自動**)** -ファイアウォールと電子メール サーバーが認証方法を決定することを許可します。
   - **Login (**ログイン**)** -ユーザー名とパスワードに Base64 エンコーディングを使用し、それらを別々に送信します。
   - **Plain (**プレーン**)** -ユーザー名とパスワードに Base64 エンコーディングを使用し、それらを一緒に送信します。
4. 電子メール サーバーで認証するには、**Certificate Profile (**証明書プロファイル**)**を選択します。
5. 電子メールを送信するアカウントの**Username (**ユーザー名**)** と **Password (**パスワード**)** を入力してから、**Confirm Password (**パスワードの確認**)** を選択します。
6. (オプション) ファイアウォールが電子メール サーバーで正常に認証できることを確認するには、**Test Connection (**接続のテスト**)**を選択します。

STEP 13 | **OK** をクリックして電子メール サーバー プロファイルを保存します。

STEP 14 | （任意）**Custom Log Format** [カスタム ログ フォーマット]タブを選択し、電子メール メッセージのフォーマットをカスタマイズします。さまざまなログ タイプでのカスタム フォーマットの作成方法については、『Common Event Format Configuration Guide』（英語）を参照してください。

STEP 15 | トラフィック ログ、脅威ログ、および WildFire 送信ログの電子メール アラートを設定します。

1. ログ転送プロファイルを作成する を参照してください。
    1. **Objects (オブジェクト)** > **Log Forwarding (ログ転送)** の順に選択して **Add (追加)** をクリックし、**Name (名前)** にプロファイルを識別する名前を入力します。
    2. ログ タイプごと、および重大度レベルまたは WildFire 判定ごとに、電子メール サーバー プロファイルを選択し、**OK** をクリックします。
2. ログ転送プロファイルをポリシー ルールおよびネットワーク ゾーンに割り当てるを参照してください。

STEP 16 | システム ログ、設定ログ、HIP マッチ ログ、および相関ログの電子メール アラートを設定します。

1. **Device**（デバイス） > **Log Settings**（ログ設定）を選択します。
2. システム ログと相関ログの場合、各重大度レベルをクリックし、**Email** [電子メール]サーバー プロファイルを選択し、**OK** をクリックします。
3. 設定ログと HIP マッチ ログの場合は、編集アイコンをクリックし、**Email** [電子メール]サーバー プロファイルを選択し、**OK** をクリックします。
4. **Commit**（コミット）をクリックします。

モニタリングのための Syslog の使用

Syslog は標準のログ転送メカニズムで、ルーター、ファイアウォール、プリンターなどのさまざまなベンダーのさまざまなネットワーク デバイスからアーカイブと分析そしてレポート作成のために、ログ データを集約できるようにします。Palo Alto Networks デバイスは、生成したすべてのログ タイプを外部の Syslog サーバーに転送できます。信頼性の高い保護されたログ転送には TCP または TLS（TLSv1.2 のみ）を使用し、保護されないログ転送には UDP を使用します。

- Syslog モニタリングの設定
- Syslog フィールドの説明

Syslog モニタリングの設定

Palo Alto Networks ファイアウォールでモニタリングのために Syslog を使用するためには、Syslog サーバー プロファイルを作成して、各ログ タイプのデバイス ログ設定に割り当てます。必要に応じて、Syslog メッセージで使用されるヘッダー フォーマットを設定し、TLSv1.2. を介した Syslog のクライアント認証を有効にできます。

CEF 形式の syslog イベント・コレクション の場合は、デフォルトの *syslog* 構成を編集する必要があります。デフォルトの *syslog* モニター構成は、*CEF syslog* イベント収集ではサポートされていません。

STEP 1 | Syslog サーバー プロファイルを設定します。

Syslog の送信に使用するプロファイルを分けることで、各ログ タイプをそれぞれ異なるサーバーに送信できます。可用性を高めるには、*1* つのプロファイルに複数のサーバー（最大 *4* 個）を定義します。

1. **Device (デバイス)** > **Server Profiles (サーバープロファイル)** > **Syslog** の順に選択します。
2. **Add** (追加)をクリックし、プロファイルの **Name** (名前)を入力します。
3. ファイアウォールに複数の仮想システム（vsys）がある場合、このプロファイルを使用可能な **Location** [場所]（vsys または **Shared** [共有]）を選択します。
4. Syslog サーバーごとに、**Add** [追加]をクリックし、ファイアウォールがそのサーバーへの接続に必要とする情報を入力します。
   - **Name** [名前] – サーバー プロファイルの一意の名前。
   - **Syslog Server**[Syslog サーバー] – Syslog サーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN)。

     FQDN を設定し、***UDP*** トランスポートを使用していて、ファイアウォールが *FQDN* を解決できない場合、ファイアウォールは既存の *IP* アドレス解決を ***Syslog Server (Syslog*** サーバー*)*** アドレスとして *FQDN* に対して使用します。
   - 転送 – Syslog サーバーとの通信方法として、**TCP**、**UDP**、または **SSL** (TLS) を選択します。**SSL** の場合、ファイアウォールは TLSv1.2 のみをサポートします。
   - **Port** （ポート） - Syslog メッセージを送信するときに経由するポート番号（デフォルトはポート 514 の UDP）。ファイアウォールと Syslog サーバーで同じポート番号を使用する必要があります。
   - **Format** [フォーマット]– 使用する Syslog メッセージ フォーマットを選択します。**BSD**(デフォルト)または**IETF**。従来、UDP 経由の場合は **BSD** フォーマット、TCP または SSL/TLS 経由の場合は **IETF** フォーマットが使用されています。
   - **Facility** [ファシリティ] - Syslog の標準値を選択します（デフォルトは **LOG_USER**）。実装されている Syslog サーバーの優先度（PRI）フィールドの計算で使用されます。PRI フィールドを使用して Syslog メッセージを管理する方法に対応する値を選択します。
5. （任意）ファイアウォールが送信する Syslog メッセージのフォーマットをカスタマイズするには、**Custom Log Format** [カスタム ログ フォーマット]タブを選択します。さまざまなログ タイプでのカスタム フォーマットの作成方法については、『Common Event Format Configuration Guide』（英語）を参照してください。
6. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 2 | トラフィック ログ、脅威ログ、および WildFire 送信ログの Syslog 転送を設定します。

1. ログを転送するためにファイアウォールを設定します。詳細は、Create a Log Forwarding profile（ログ転送プロファイルの作成）のステップを参照してください。
   1. **Objects (オブジェクト)** > **Log Forwarding (ログ転送)** の順に選択して **Add (追加)** をクリックし、**Name (名前)** にプロファイルを識別する名前を入力します。
   2. ログ タイプごと、および重大度レベルまたは WildFire 判定ごとに、**Syslog** サーバー プロファイルを選択し、**OK** をクリックします。
2. ログ転送プロファイルをセキュリティ ポリシーに割り当てて、ログの生成と転送をトリガーします。詳細は、Assign the Log Forwarding profile to policy rules and network zones（ポリシールールおよびネットワーク ゾーンにログ転送プロファイルを割り当て）のステップを参照してください。
   1. **Policies (ポリシー)** > **Security (セキュリティ)** を選択し、さらにポリシー ルールを選択します。
   2. **Actions**（アクション）タブを選択し、作成した **Log Forwarding**（ログ転送）プロファイルを選択します。
   3. **Profile Type**（プロファイル タイプ）ドロップダウンから、**Profiles**（プロファイル）または **Group**（グループ）を選択してから、ログの生成と転送をトリガーするために必要なセキュリティ プロファイルまたは **Group Profile**（グループ プロファイル）を選択します。
   4. トラフィック ログの場合は、**Log at Session Start**（セッション開始時にログ）および**Log At Session End**（セッション終了時にログ）チェックボックスの一方または両方を選択し、**OK** をクリックします。

   ログ転送プロファイルの構成とポリシー規則へのプロファイルの割り当ての詳細については、を参照してください。

STEP 3 | システム ログ、設定ログ、HIP マッチ ログ、および相関ログの Syslog 転送を設定します。

1. **Device**（デバイス） > **Log Settings**（ログ設定）を選択します。
2. システム ログと相関ログの場合、各重大度レベルをクリックし、**Syslog** サーバー プロファイルを選択し、**OK** をクリックします。
3. 設定ログ、HIP マッチ ログ、および相関ログの場合、**Syslog** サーバー プロファイルを選択し、**OK** をクリックします。

STEP 4 | （任意）Syslog メッセージ内のヘッダー フォーマットを設定します。

ログ データには、ログを生成したファイアウォールの一意の識別子が含まれます。ヘッダー フォーマットを選択することで、一部のセキュリティ情報およびイベント管理（SIEM）サーバーのログ データをより柔軟にフィルタリングおよびレポートできます。

これは、グローバル設定であるため、ファイアウォールで設定されているすべての Syslog サーバー プロファイルに適用されます。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して Logging and Reporting Settings (ロギングおよびレポート設定) を編集します。
2. **Log Export and Reporting**（ログのエクスポートとレポート）タブを選択し、Syslog HOSTNAME Format（Syslog のホスト名フォーマット）を以下から選択します。
   - **FQDN**[デフォルト] — 送信ファイアウォールで定義されているホスト名とドメイン名を連結します。
   - **hostname** — 送信ファイアウォールで定義されているホスト名を使用します。
   - **ipv4-address** [IPv4 アドレス] — ログの送信に使用されるファイアウォール インターフェイスの IPv4 アドレスを使用します。デフォルトでは、MGT インターフェイスです。
   - **ipv6-address** [IPv6 アドレス] — ログの送信に使用されるファイアウォール インターフェイスの IPv6 アドレスを使用します。デフォルトでは、MGT インターフェイスです。
   - **none** — ファイアウォールのホスト名フィールドを設定されないままにします。ログを送信したファイアウォールの ID はありません。
3. **OK** をクリックして変更内容を保存します。

STEP 5 | r TLSv1.2 を介した Syslog 通信を保護するための証明書を作成します。

Syslog サーバーがクライアント認証を使用する場合にのみ必要です。Syslog サーバーは、証明書を使用して、ファイアウォールに Syslog サーバーと通信する権限があることを確認します。

以下の条件が満たされることを確認します。

- 送信ファイアウォールで秘密鍵が使用可能である必要があります。秘密鍵は、ハードウェア セキュリティ モジュール（HSM）に保管できません。
- 証明書のサブジェクトと発行者を同じにすることはできません。
- 同じ信頼された認証局（CA）によって署名された証明書を Syslog サーバーと送信ファイアウォールに設定する必要があります。または、デバイスで自己署名証明書を生成し、その証明書をファイアウォールからエクスポートして、Syslog サーバーにインポートすることもできます。
- トラスト チェーンに含まれる各証明書がいずれかあるいは両方の拡張子を指定している場合、TLS を介する Syslog サーバーへの接続は、オンライン証明書ステータス プロトコル（OCSP）あるいは証明書無効リスト（CRL）を使って検証されます。しかし、OCSP や

CRL のエラーはバイパスできないため、必ず証明書チェーンが有効であり、OCSP あるいは CRL を使って各証明書を検証できることを確認してください。

1. **Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificates (証明書)** > **Device Certificates (デバイス証明書)** を選択して **Generate (生成)** をクリックします。
2. **[証明書名]** に証明書の名前を入力します。
3. **Common Name** [共通名]に、Syslog サーバーにログを送信するファイアウォールの IP アドレスを入力します。
4. **Signed by** [署名者]で、信頼された認証局、または Syslog サーバーと送信ファイアウォールの両方で信頼されている自己署名認証局を選択します。

   証明書は、**Certificate Authority** [認証局]と **External Authority** [外部認証局]（証明書署名要求（CSR））のどちらにもできません。
5. **Generate**（生成）をクリックします。ファイアウォールが証明書と鍵のペアを生成します。
6. 証明書名をクリックして編集し、**Certificate for Secure Syslog** [保護された Syslog の証明書]チェック ボックスをオンにし、**OK** をクリックします。

STEP 6 | 変更をコミットし、Syslog サーバーでログを確認します。

1. **Commit**（コミット）をクリックします。
2. ログを確認するには、Syslog 管理ソフトウェアのドキュメントを参照してください。また、Syslog フィールドの説明をレビューすることもできます。

STEP 7 | (オプション)FQDN の更新時に syslog サーバへの接続を終了するようにファイアウォールを設定します。

FQDN を使用して syslog サーバ プロファイルを設定すると、ファイアウォールは、FQDN 名が変更された場合に、デフォルトで syslog サーバへの接続を維持します。

たとえば、既存の syslog サーバーを別の FQDN 名を使用する新しい syslog サーバーに置き換えました。ファイアウォールで新しい FQDN 名を使用して新しい syslog サーバに接続する場合は、古い syslog サーバへの接続を自動的に終了し、新しい FQDN 名を使用して新しい syslog サーバへの接続を確立するようにファイアウォールを設定できます。

1. ファイアウォール CLI へログインします。
2. FQDN の更新時に syslog サーバへの接続を終了するようにファイアウォールを設定します。

```
admin> set syslogng fqdn-refresh yes
```

Syslog フィールドの説明

以下のトピックには、Palo Alto Networks ファイアウォールが外部サーバーに転送できる各ログ タイプの標準項目のリストと、重大度レベル、カスタム フォーマット、エスケープ シーケンスが含まれます。解析しやすくするため、カンマを区切り文字としており、各フィールドはカンマ区切り値（CSV）の文字列になっています。FUTURE_USE タグは、ファイアウォールで現在実装されていないフィールドに適用されます。

WildFire 送信ログは、脅威ログのサブタイプで、同じ *Syslog* フォーマットを使用します。

トラフィック ログの各フィールド

フォーマット:FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Source Address, Destination Address, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, Protocol, Action, Bytes, Bytes Sent, Bytes Received, Packets, Start Time, Elapsed Time, Category, FUTURE_USE, Sequence Number, Action Flags, Source Country, Destination Country, FUTURE_USE, Packets Sent, Packets Received, Session End Reason, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Action Source, Source VM UUID, Destination VM UUID, Tunnel ID/IMSI, Monitor Tag/IMEI, Parent Session ID, Parent Start Time, Tunnel Type, SCTP Association ID, SCTP Chunks, SCTP Chunks Sent, SCTP Chunks Received, Rule UUID, HTTP/2 Connection, App Flap Count, Policy ID, Link Switches, SD-WAN Cluster, SD-WAN Device Type, SD-WAN Cluster Type, SD-WAN Site, Dynamic User Group Name, XFF Address, Source Device Category, Source Device Profile, Source Device Model, Source Device Vendor, Source Device OS Family, Source Device OS Version, Source Hostname, Source Mac Address, Destination Device Category, Destination Device Profile, Destination Device Model, Destination Device Vendor, Destination Device OS Family, Destination Device OS Version, Destination Hostname, Destination Mac Address, Container ID, POD Namespace, POD Name, Source External Dynamic List, Destination

External Dynamic List, Host ID, Serial Number, Source Dynamic Address Group, Destination Dynamic Address Group, Session Owner, High Resolution Timestamp, A Slice Service Type, A Slice Differentiator, Application Subcategory, Application Category, Application Technology, Application Risk, Application Characteristic, Application Container, Tunneled Application, Application SaaS, Application Sanctioned State, Offloaded

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号 (serial)	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は TRAFFIC です。
脅威/コンテンツ タイプ (subtype)	トラフィック ログのサブタイプ。値は、「start」、「end」、「drop」、「deny」です • start — セッションが開始しました • end — セッションが終了しました • drop — アプリケーションが特定される前にセッションが廃棄され、そのセッションを許可するルールがありません。 • deny — アプリケーションが特定された後にセッションが廃棄され、そのセッションをブロックするルールがあるか、セッションを許可するルールがありません。
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
送信元アドレス (src)	元のセッション送信元 IP アドレス。
宛先アドレス (dst)	元のセッション宛先 IP アドレス。
NAT ソース IP (natsrc)	送信元 NAT を行った場合は、NAT 後の送信元 IP アドレス。
NAT 宛先 IP (natdst)	宛先 NAT を行った場合は、NAT 後の宛先 IP アドレス。
ルール名（rule）	セッションで一致したルールの名前。
送信元ユーザー (srcuser)	セッションを開始したユーザーのユーザー名。
宛先ユーザー (dstuser)	セッションの宛先となったユーザーのユーザー名。
アプリケーション (app)	セッションに関連付けられたアプリケーション。

フィールド名	説明
仮想システム (vsys)	セッションに関連付けられている仮想システム。
送信元ゾーン (from)	セッションの送信元だったゾーン。
宛先ゾーン (to)	セッションの宛先だったゾーン。
インバウンド インターフェイス (inbound_if)	セッションの送信元となったインターフェイス。
アウトバウンド インターフェイス (outbound_if)	セッションの宛先だったインターフェイス。
ログ アクション (logset)	セッションに適用されたログ転送プロファイル。
セッション ID (sessionid)	各セッションに適用される内部の数値識別子。
リピートカウント（repeatcnt）	5 秒以内に開始された、送信元 IP、宛先 IP、アプリケーション、サブタイプが同じになっているセッションの数です。
送信元ポート（sport）	セッションで使用された送信元ポート。
宛先ポート（dport）	セッションで使用された宛先ポート。
NAT ソース ポート（natsport）	NAT 後の送信元ポート。
NAT 宛先ポート（natdport）	NAT 後の宛先ポート。
フラッグ（flags）	セッションに関する詳細を示す 32 ビット フィールド。このフィールドは、以下のように、その値とログに記録されている値を AND 演算することによってデコードできます。 • 0X80000000—セッションにパケット キャプチャがあります（PCAP） • 0x40000000—クライアントが複数のパスを使用して宛先ホストに接続できるようにするオプションが有効です • 0x20000000 — サンプルが WildFire パブリッククラウド チャネルまたはプライベートクラウドチャネルを使用して分析のために送信されたかどうかを示します。 • 0x10000000—エンドユーザーによるエンタープライズ認証情報の送信を検出 • 0x08000000— 対象のフローの送信元が許可リストに記載されており、偵察行為防止の対象になっていません

フィールド名	説明
	• 0x02000000—IPv6 セッション • 0x01000000—SSL セッションが復号化されます（SSL プロキシ） • 0x00800000—セッションが URL フィルタリングによって拒否されます • 0x00400000—セッションで NAT 変換が実行されました • 0x00200000—セッションのユーザー情報が認証ポータルを通じて取得されました • 0x00100000—標準的でない宛先ポート上にアプリケーション トラフィックがあります • 0x00080000 — プロキシからの X-Forwarded-For 値は送信元ユーザー フィールドにあります • 0x00040000—ログは http プロキシ セッション内のトランザクションに対応します（プロキシ トランザクション） • 0x00020000—クライアントからサーバーへのフローがポリシーベース フォワーディングの対象になっています • 0x00010000—サーバーからクライアントへのフローがポリシーベース フォワーディングの対象になっています • 0x00008000—セッションはコンテナ ページ アクセスです（コンテナ ページ） • 0x00002000—セッションに、暗黙的なアプリケーションの依存関係処理のルールでの一時的な一致があります。PAN-OS 5.0.0 以降で使用できます。 • 0x00000800 — このセッションのトラフィックを転送するために対称リターンが使用されます • 0x00000400—復号化されたトラフィックがミラーポートを介してクリアテキストを送信しています • 0x00000100—外側のトンネルのペイロードを検査中です
IP プロトコル（proto）	セッションに関連付けられた IP プロトコル。
アクション（action）	セッションで実行されたアクション。値は以下のいずれかです。 • allow —セッションはポリシーによって許可されました • deny — セッションはポリシーによって拒否されました • drop — セッションはサイレントにドロップされました

フィールド名	説明
	• drop ICMP — セッションはサイレントにドロップされ、ホストまたはアプリケーションに ICMP 到達不能メッセージが表示されました • reset both — セッションは終了し、TCP リセットが接続の両端に送信されました • reset client — セッションは終了し、TCP リセットがクライアントに送信されました • reset server — セッションは終了し、TCP リセットがサーバーに送信されました
バイト (bytes)	セッションの合計バイト数 (送受信)
送信済バイト (bytes_sent)	セッションのクライアントからサーバー方向へのバイト数。
受信済バイト (bytes_received)	セッションのサーバーからクライアント方向へのバイト数。
パケット (packets)	セッションの合計パケット数 (送受信)。
開始時間（start）	セッションの開始時間。
経過時間 (elapsed)	セッションの経過時間。
カテゴリ（category）	セッションに関連付けられた URL カテゴリ (該当する場合)。
シーケンス番号（seqno）	64 ビットのログ エントリ識別子。各ログ タイプには、一意の番号空間があります。
アクション フラグ（actionflags）	ログが Panorama に転送されたかどうかを示すビット フィールド。
送信元（srcloc）	プライベート アドレスの送信元の国または内部領域。最大長は 32 バイトです。
宛先（dstloc）	プライベート アドレスの宛先の国または国内地域。最大長は 32 バイトです。
送信されたパケット（pkts_sent）	セッションのクライアントからサーバーへのパケット数。
受信したパケット（pkts_received）	セッションのサーバーからクライアントへのパケット数。

フィールド名	説明
セッション終了理由（session_end_reason）	セッションが終了した理由。複数の原因で終了した場合、このフィールドには優先度が最も高い理由のみが表示されます。有効なセッション終了理由の値は、優先度の高い順に以下のとおりです。 • threat — ファイアウォールが、リセット、ドロップ、またはブロック（IP アドレス）アクションに関連付けられた脅威を検出しました。 • policy-deny — セッションが、拒否またはドロップ アクションが指定されたセキュリティ ルールと一致しました。 • decrypt-cert-validation—失効、信用されていない発行者、未知の状態、状態検証タイムアウトなどの状況によりセッションがクライアント認証を実施またはセッションがサーバー証明書を実施する時に、SSL 送信プロキシ複合 または SSL インバウンド インスペクションをブロックするようにファイアウォールを設定したのでセッションが終了しました。サーバー証明書が type bad_certificate、unsupported_certificate、certificate_revoked、access_den または no_certificate_RESERVED (SSLv3 のみ)の致命的エラー アラートを生成する時にもこのセッションの終了理由が表示されます。 • decrypt-unsupport-param—セッションがサポートしていないプロトコルバージョン、暗号鍵またはSSHアルゴリズムを使用している場合、SSL送信プロキシ複合またはSSLインバウンドインスペクションをブロックするようにファイアウォールを設定したのでセッションは終了しました。unsupported_extension、 unexpected_message、または handshake_failureのタイプの致命的エラーアラートをセッションが発生すると、このセッション終了理由が表示されます。 • decrypt-error——ファイアウォールリソースまたは ハードウェアセキュリティモジュール (HSM) が利用できない時に、 SSL送信プロキシ複合またはSSLインバウンドインスペクションをブロックするようにファイアウォールを設定したのでセッションは終了しました。このセッション終了理由は、SSL エラーが発生した SSL トラフィックをブロックするようにファイアウォールを設定した場合、または復号化証明書検証および非サポート の終了理由にリストされている以外の致命的なエラー アラートを生成した場合にも表示されます。 • tcp-rst-from-client — クライアントが TCP リセットをサーバーに送信しました。

フィールド名	説明
	• tcp-rst-from-server — サーバーが TCP リセットをクライアントに送信しました。 • resources-unavailable — システム リソース制限が原因でセッションがドロップしました。たとえば、セッションの順序外パケット数が、フローまたはグローバル順序外パケット キューごとに許容される数を超えた場合などが考えられます。 • tcp-fin — 接続中の両ホストが TCP FIN メッセージを送信してセッションを閉じました。

	• tcp-reuse — セッションが再利用され、ファイアウォールが前のセッションを閉じました。
	• decoder — デコーダがプロトコル内で新しい接続を検出し（HTTP-Proxy など）、前の接続を終了しました。
	• aged-out — セッションがエージアウトしました。
	• unknown — この値は、以下の状況に適用されます。
	  • 上記の理由が適用されないセッションの終了（たとえば、`clear session all` コマンド）。
	  • セッション終了理由フィールドをサポートしない PAN-OS リリース（PAN-OS 6.1 より前のリリース）で生成されたログの場合、最新の PAN-OS リリースへのアップグレード後、またはログがファイアウォールにロードされると、値は **unknown** になります。
	  • Panorama では、セッション終了理由をサポートしない PAN-OS バージョンのファイアウォールから受信したログの値は、**unknown** になります。
	• n/a — この値は、トラフィック ログのタイプが **end** 以外の場合に適用されます。

デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。

フィールド名	説明
	API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
アクションの送信元（action_source）	アプリケーションを許可またはブロックするために実行されたアクションがアプリケーションまたはポリシーに定義されていたかどうかを示します。アクションは、セッションに対する「allow」、「deny」、「drop」、「reset- server」、「reset-client」、「reset-both」のいずれかになります。
送信元 VM UUID（src_uuid）	VMware NSX 環境のゲスト仮想マシンの送信元 UUID（Universally Unique Identifier）を識別します。
宛先 VM UUID（dst_uuid）	VMware NSX 環境のゲスト仮想マシンの宛先 UUID（Universally Unique Identifier）を識別します。
トンネル ID/IMSI (tunnelid/imsi)	International Mobile Subscriber Identity（IMSI）は、GSM/UMTS/EPS システム内の各モバイル サブスクライバに割り当てられる一意の番号です。IMSI は10進数（0～9）のみで構成され、最大桁数は 15 です。
モニタータグ/IMEI（monitortag/imei）	International Mobile Equipment Identity (IMEI) は、各モバイルステーション装置に割り当てられた 15 あるいは 16 桁の一意の数字です。
親セッション ID（parent_session_id）	内部でこのセッションをトンネル化するトンネルの ID。内側のトンネル（2 レベルのトンネリングの場合）あるいは内部コンテンツ（1 レベルのトンネリングの場合）のみに適用されます。
親開始時間（parent_start_time）	親トンネルのセッションが始まった年/月/日 時間:分:秒。
トンネル タイプ（tunnel）	GRE や IPSec などの、トンネルの種類。
SCTP アソシエーション ID（assoc_id）	2 つの SCTP エンドポイント間の関連付けのためのすべての接続を識別する番号。

フィールド名	説明
SCTP チャンク (chunks)	関連付けのために送受信された SCTP チャンクの合計。
送信済み SCTP チャンク (chunks_sent)	関連付けのために送信された SCTP チャンク数。
受信済み SCTP チャンク (chunks_received)	関連付けのために受信された SCTP チャンク数。
ルール UUID (rule_uuid)	規則を恒久的に識別するUUID です。
HTTP/2 接続(http2_connection)	次のいずれかの値を表示して、トラフィックが HTTP/2 コネクションを使用していたかどうかを識別します。 • ペアレントセッション ID—HTTP/2 コネクション • 0—SSL セッション
アプリ フラップカウント (link_change_count)	セッション中に発生したリンクフラップの数。
ポリシー ID (policy_id)	SD-WAN ポリシーの名前。
リンクスイッチ (link_switches)	最大 4 つのリンク フラップ エントリが含まれ、各エントリには、リンク名、リンクタグ、リンクタイプ、物理インターフェース、タイムスタンプ、読み取りbyte (バイト)、書き込みbyte (バイト)、リンク ヘルス、リンク フラップの原因が含まれます。
SD-WAN クラスタ (sdwan_cluster)	SD-WAN クラスタの名前。
SD-WAN デバイスタイプ (sdwan_device_type)	デバイスのタイプ (ハブまたはブランチ)。
SD-WAN クラスタタイプ (sdwan_cluster_type)	クラスタのタイプ (`mesh` または `hub-spoke`)。
SD-WAN サイト (sdwan_site)	SD-WAN サイトの名前。
ダイナミック ユーザー グループ名 (dynusergroup_name)	セッションを開始したユーザーを含むダイナミック ユーザー グループの名前。
XFF アドレス (xff_ip)	Webページをリクエストしたユーザーの IP アドレス、またはリクエストが通過した最後から2番目のデバイスの IP アドレス。リクエストが1つ以上のプロキシ、ロード バランサー、

フィールド名	説明
	またはその他のアップストリーム デバイスを通過する場合、ファイアウォールは最も新しいデバイスの IP アドレスを表示します。
ソース デバイスのカテゴリ (src_category)	Device-ID がトラフィックの送信元として識別するデバイスのカテゴリ。
送信元のデバイスのプロファイル (src_profile)	Device-ID がトラフィックの送信元として識別するデバイスのデバイスのプロファイル。
送信元のデバイス モデル (src_model)	Device-ID がトラフィックの送信元として識別するデバイスのモデル。
送信元のデバイス ベンダー (src_vendor)	Device-ID がトラフィックの送信元として識別するデバイスのベンダー。
送信元デバイス OS ファミリ (src_osfamily)	Device-ID がトラフィックの送信元として識別するデバイスのオペレーティングシステムの種類。
送信元デバイス OS バージョン (src_osversion)	Device-ID がトラフィックの送信元として識別するデバイスのオペレーティングシステムのバージョン。
送信元ホスト名 (src_host)	Device-ID がトラフィックの送信元として識別するデバイスのホスト名。
送信元 MAC アドレス (src_mac)	Device-ID がトラフィックの送信元として識別するデバイスの MAC アドレス。
宛先デバイスのカテゴリ (dst_category)	Device-ID がトラフィックの宛先として識別するデバイスのカテゴリ。
宛先デバイスのプロファイル (dst_profile)	Device-ID がトラフィックの宛先として識別するデバイスのデバイス プロファイル。
宛先デバイスのモデル (dst_model)	Device-ID がトラフィックの宛先として識別するデバイスのモデル。
宛先デバイスのベンダー (dst_vendor)	Device-ID がトラフィックの宛先として識別するデバイスのベンダー。
宛先 デバイス OS ファミリ (dst_osfamily)	Device-ID がトラフィックの宛先として識別するデバイスのオペレーティングシステムの種類。
宛先デバイス OS バージョン (dst_osversion)	Device-ID がトラフィックの宛先として識別するデバイスのオペレーティングシステムのバージョン。

フィールド名	説明
宛先ホスト名 (dst_host)	Device-ID がトラフィックの宛先として識別するデバイスのホスト名。
宛先 MAC アドレス (dst_mac)	Device-ID がトラフィックの宛先として識別するデバイスの MAC アドレス。
コンテナ ID (container_id)	アプリケーション POD がデプロイされる Kubernetes ノードの PAN-NGFW ポッドのコンテナ ID。
POD 名前空間 (pod_namespace)	保護されているアプリケーション POD の名前空間。
POD 名 (pod_name)	保護されているアプリケーション PODの名前。
送信元の外部ダイナミックリスト (src_edl)	トラフィックの送信元 IP アドレスを含む外部ダイナミックリストの名前。
宛先の外部ダイナミック リスト (dst_edl)	トラフィックの宛先 IP アドレスを含む外部ダイナミックリストの名前。
ホスト ID（hostid）	GlobalProtect がホストの識別のために割り当てる、一意の ID です。
ユーザーデバイスのシリアルナンバー (serialnumber)	ユーザーのマシンあるいはデバイスのシリアルナンバー。
送信元の動的アドレス グループ (src_dag)	元のセッション送信元のダイナミックアドレス グループ。
宛先のダイナミックアドレスグループ (dst_dag)	元の宛先送信元の動的アドレス グループ。
セッション オーナー (session_owner)	HA フェイル オーバー時にセッション テーブル データが同期された HA クラスタ内の同期元となる高可用性 (HA) ピア セッション オーナー。
高解像度タイムスタンプ (high_res _timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 この新規フィールドの形式は YYYY-MM-DDThh:ss:sssTZD です: • **YYYY**—西暦 • **MM**—2桁表記の月数 • **DD**—月の2桁の日 (01 ～ 31)

フィールド名	説明
	• **T**—タイムスタンプの開始のインジケータ • **hh**—24時間を使用した2桁の時間数 (00 ～ 23) • **mm**—2桁表記の分 (00 ～ 59) • **ss**—2桁表記の秒 (00 ～ 60) • **sss**—ミリ秒単位で1桁以上の桁数 • **TZD**—タイムゾーン指定子 (+hh:mm or -hh:mm) 高解像度タイムスタンプは、*PAN-OS 10.2* 以降のリリースを実行しているマネージドファイアウォール から受信したログでサポートされています。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*`1969-12-31T16:00:00:000-8:00`* というタイムスタンプを表示します。
A スライス サービス タイプ (nsdsai_sst)	ネットワーク スライス ID の A スライス サービス タイプ。
A スライス差別化要素 (nsdsai_sd)	ネットワーク スライス ID の A スライス差別化要素。
アプリケーション サブカテゴリ (subcategory_of_app)	アプリケーション構成プロパティで指定されたアプリケーション サブカテゴリ。
アプリケーションカテゴリ (category_of_app)	アプリケーション構成プロパティで指定されたアプリケーション カテゴリ。値を以下に示します。 • business-system • コラボレーション • 一般インターネット • メディア • networking • SaaS
アプリケーションテクノロジー (technology_of_app)	アプリケーション構成プロパティで指定されたアプリケーション テクノロジ。値を以下に示します。 • ブラウザベース • クライアント/サーバー • ネットワークプロトコル

フィールド名	説明
	• ピアツーピア
アプリケーションリスク (risk_of_app)	アプリケーションに関連付けられたリスク レベル (1 =最低から 5=最高)。
アプリケーション特性 (characteristic_of_app)	アプリケーションの適用可能特性のコンマ区切りリスト
アプリケーション コンテナ (container_of_app)	アプリケーションの親アプリケーション。
トンネリングされたアプリケーション (tunneled_app)	トンネリングされたアプリケーションの名前。
アプリケーション SaaS (is_saas_of_app)	SaaS アプリケーションの場合は 1、SaaS アプリケーションでない場合は 0 を表示します。
アプリケーション認可状態 (sanctioned_state_of_app)	アプリケーションが認可されている場合は 1、アプリケーションが認可されていない場合は 0 が表示されます。
オフロード (オフロード)	トラフィック フローがオフロードされている場合は 1 を表示し、トラフィック フローがオフロードされていない場合は 0 を表示します。

脅威ログの各フィールド

フォーマット：FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Source Address, Destination Address, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, IP Protocol, Action, URL/Filename, Threat ID, Category, Severity, Direction, Sequence Number, Action Flags, Source Location, Destination Location, FUTURE_USE, Content Type, PCAP_ID, File Digest, Cloud, URL Index, User Agent, File Type, X-Forwarded-For, Referer, Sender, Subject, Recipient, Report ID, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, FUTURE_USE, Source VM UUID, Destination VM UUID, HTTP Method, Tunnel ID/IMSI, Monitor Tag/IMEI, Parent Session ID, Parent Start Time, Tunnel Type, Threat Category, Content Version, FUTURE_USE, SCTP Association ID, Payload Protocol ID, HTTP Headers, URL Category List, Rule UUID, HTTP/2 Connection, Dynamic User Group Name, XFF Address, Source Device Category, Source Device Profile, Source Device Model, Source Device Vendor, Source Device OS Family, Source Device OS Version, Source Hostname, Source MAC Address, Destination Device Category, Destination Device Profile, Destination Device Model, Destination Device Vendor, Destination Device OS Family, Destination Device OS Version, Destination Hostname, Destination MAC Address, Container ID, POD Namespace, POD Name, Source External Dynamic List, Destination External Dynamic List, Host ID, Serial Number, Domain EDL, Source Dynamic Address Group,

Destination Dynamic Address Group, Partial Hash, High Resolution Timestamp, Reason, Justification, A Slice Service Type, Application Subcategory, Application Category, Application Technology, Application Risk, Application Characteristic, Application Container, Application SaaS, Tunneled Application, Application Sanctioned State, Cloud Report ID

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号（serial #）	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は THREAT です。
脅威/コンテンツ タイプ (subtype)	脅威ログのサブタイプ値は以下を含みます。 • data – データ フィルタリング プロファイルと一致するデータ パターン • file—ファイルブロッキングプロファイルと一致するファイルタイプ • flood – ゾーン プロテクション プロファイルによって検出されたフラッド • packet—ゾーンプロテクションプロファイルでトリガーされたパケットベース攻撃防御 • scan – ゾーン プロテクション プロファイルによって検出されたスキャン • Spyware —アンチスパイウェアプロファイルで検出したスパイウェア • url – URL フィルタリング ログ • ml-ウイルス —ウイルス対策プロファイルを介して WildFire インライン ML によって検出されたウイルス。 • virus—アンチウィルスプロファイルで検出したウィルス • Vulnerability —脆弱性防御プロファイルで検出した脆弱性バグ • 山火事 – ファイアウォールが WildFire 分析プロファイルごとにファイルを WildFire に送信し、その結果に基づいて判定 (マルウェア、フィッシング、グレーウェア、無害な情報) を WildFire の送信ログに記録すると、WildFire の判定が生成されます。 • wildfire-virus—アンチウィルスプロファイルで検出したウィルス
生成時間 (time_generated ま	データプレーンでログが生成された日時。

フィールド名	説明
たは cef-formatted-time_generated)	
送信元アドレス (src)	元のセッション送信元 IP アドレス。
宛先アドレス (dst)	元のセッション宛先 IP アドレス。
NAT ソース IP (natsrc)	送信元 NAT が実行された場合は、NAT 後の送信元 IP アドレス。
NAT 宛先 IP (natdst)	宛先 NAT が実行された場合は、NAT 後の宛先 IP アドレス。
ルール名（rule）	セッションで一致したルールの名前。
送信元ユーザー (srcuser)	セッションを開始したユーザーのユーザー名。
宛先ユーザー (dstuser)	セッションの宛先となったユーザーのユーザー名。
アプリケーション (app)	セッションに関連付けられたアプリケーション。
仮想システム (vsys)	セッションに関連付けられている仮想システム。
送信元ゾーン (from)	セッションの送信元だったゾーン。
宛先ゾーン (to)	セッションの宛先だったゾーン。
インバウンド インターフェイス (inbound_if)	セッションの送信元となったインターフェイス。
アウトバウンド インターフェイス (outbound_if)	セッションの宛先だったインターフェイス。
ログ アクション (logset)	セッションに適用されたログ転送プロファイル。
セッション ID (sessionid)	各セッションに適用される内部の数値識別子。
リピートカウント（repeatcnt）	5 秒以内に開始された、送信元 IP、宛先 IP、アプリケーション、コンテンツ/脅威タイプが同じになっているセッションの数です。
送信元ポート（sport）	セッションで使用された送信元ポート。
宛先ポート（dport）	セッションで使用された宛先ポート。

フィールド名	説明
NAT ソース ポート（natsport）	NAT 後の送信元ポート。
NAT 宛先ポート（natdport）	NAT 後の宛先ポート。
フラッグ（flags）	セッションに関する詳細を示す 32 ビット フィールド。このフィールドは、以下のように、その値とログに記録されている値を AND 演算することによってデコードできます。 • 0X80000000—セッションにパケット キャプチャがあります（PCAP） • 0x40000000—クライアントが複数のパスを使用して宛先ホストに接続できるようにするオプションが有効です • 0x20000000—判定を行うためにファイルが WildFire に送信されます • 0x10000000—エンドユーザーによるエンタープライズ認証情報の送信を検出 • 0x08000000— 対象のフローのソースが許可リストに登録されており、偵察保護の対象になっていません • 0x02000000—IPv6 セッション • 0x01000000—SSL セッションが復号化されます（SSL プロキシ） • 0x00800000—セッションが URL フィルタリングによって拒否されます • 0x00400000—セッションで NAT 変換が実行されました • 0x00200000—セッションのユーザー情報が認証ポータルを通じて取得されました • 0x00100000—標準的でない宛先ポート上にアプリケーション トラフィックがあります • 0x00080000 — プロキシからの X-Forwarded-For 値は送信元ユーザー フィールドにあります • 0x00040000 — ログは http プロキシ セッション内のトランザクションに対応します（プロキシ トランザクション） • 0x00020000—クライアントからサーバーへのフローがポリシー ベース フォワーディングの対象になっています • 0x00010000—サーバーからクライアントへのフローがポリシー ベース フォワーディングの対象になっています • 0x00008000 — セッションはコンテナ ページ アクセスです（コンテナ ページ）

フィールド名	説明
	• 0x00002000 – セッションに、暗黙的なアプリケーションの依存関係処理のルールでの一時的な一致があります。PAN-OS 5.0.0 以降で使用できます。 • 0x00000800 –このセッションのトラフィックを転送するために対称リターンが使用されます • 0x00000400–復号化されたトラフィックがミラーポートを介してクリアテキストを送信しています • 0x00000010–外側のトンネルのペイロードを検査中です
IP プロトコル（proto）	セッションに関連付けられた IP プロトコル。
アクション（action）	セッションに対して実行されたアクション。値は、「alert」、「allow」、「deny」、「drop」、「drop-all-packets」、「reset-client」、「reset-server」、「reset-both」、「block-url」です。 • alert – 脅威または URL が検出されましたが、ブロックされていません • allow– フラッド検出アラート • deny – フラッド検出メカニズムがアクティブにされ、設定に基づいてトラフィックを拒否します • drop– 脅威が検出され、関連付けられたセッションが廃棄されました • reset-client – 脅威が検出され、TCP RST がクライアントに送信されました • reset-server – 脅威が検出され、TCP RST がサーバーに送信されました • reset-both – 脅威が検出され、TCP RST がクライアントとサーバーの両方に送信されました • block-url – ブロックするように設定された URL カテゴリで照合が行われたため、URL 要求がブロックされました • block-ip–脅威が検出され、クライアント IP がブロックされます • random-drop–フラッドが検出され、パケットがランダムにドロップされました • sinkhole–DNS シンクホール起動 • syncookie-sent–syncookie アラート • block-continue（URL サブタイプのみ）–HTTP リクエストがブロックされ、続行確認のためのボタンが付いた Continue（続行）ページにリダイレクトされます • continue（URL サブタイプのみ）–継続要求が続行されたことを示す、block-continue URL 続行ページへの応答ブロック

フィールド名	説明
	• block-override（URL サブタイプのみ）–HTTP リクエストがブロックされ、ファイアウォール管理者からのパスコードが必要な管理オーバーライド ページにリダイレクトされます • override-lockout（URLサブタイプのみ）–送信元 IP からの管理上のオーバーライドパスコードの試行に失敗しました。IP が block-override リダイレクト ページからブロックされるようになりました • override（URLサブタイプのみ）–正しいパスコードが提供され、リクエストが許可されている block-override ページへの応答 • block（Wildfire のみ）–ファイルはファイアウォールでブロックされ、Wildfire にアップロードされました
URL/ファイル名 (misc)	可変長フィールドです。ファイル名は最大 63 文字です。URL は最大 1023 文字です サブタイプが url の場合の実際の URI サブタイプが file の場合のファイル名またはファイル タイプ サブタイプが virus の場合のファイル名 サブタイプが wildfire-virus の場合のファイル名 サブタイプが wildfire の場合のファイル名 該当する場合、サブタイプが脆弱である場合の URL またはファイル名 脅威カテゴリが `domain-edl` である時の URL ホストヘッダーの不一致が検出された場合のスプーフィングされた SNI ドメイン (一意の脅威 ID 86467 で識別)。
脅威/コンテンツ名 (threatid)	既知およびカスタム脅威に対する Palo Alto Networksの識別子。一部のサブタイプでは、説明の文字列にかっこで囲んだ 64 ビットの数値識別子が続きます。 • 8000 ～ 8099 – スキャン検出 • 8500 ～ 8599 – フラッド検出 • 9999– URL フィルタリング ログ • 10000 ～ 19999 – スパイウェア フォンホーム検出 • 20000 ～ 29999 – スパイウェア ダウンロード検出 • 30000 ～ 44999 – 脆弱性悪用検出 • 52000 ～ 52999 – ファイルタイプ検出 • 60000 ～ 69999 – データ フィルタリング検出

フィールド名	説明
	ドメイン EDL フィールドに値が入力されている場合、このフィールドに同じ値が入力されます。 以前のリリースで使用されていたウイルス検出の脅威 *ID* 範囲、*WildFire* シグネチャ フィード、および *DNS C2* シグネチャは、永続的でグローバルに一意の *ID* に置き換えられました。脅威/コンテンツ タイプ *(subtype)* および脅威カテゴリ *(thr_category)* フィールド名を参照し、更新されたレポート、フィルタ、脅威ログ、*ACC* アクティビティを作成します。
カテゴリ（category）	URL サブタイプの場合は、URL カテゴリです。WildFire サブタイプの場合、それはファイルの評決であり、"マルウェア"、"フィッシング"、"グレーウェア"、または '無害' のいずれかです。その他のサブタイプの場合、値は 「any」です。
重大度 (severity)	脅威に関連付けられた重大度。値は、「informational」、「low」、「medium」、「high」、「critical」です。
方向 (direction)	攻撃の方向（「クライアントからサーバーへ」、または「サーバーからクライアントへ」）を示します。 • 0 — 脅威の方向はクライアントからサーバーへ • 1 — 脅威の方向はサーバーからクライアントへ
シーケンス番号（seqno）	順次増分される 64 ビットのログ エントリ識別子。各ログ タイプには、一意の番号空間があります。
アクション フラグ（actionflags）	ログが Panorama に転送されたかどうかを示すビット フィールド。
送信元（srcloc）	プライベート アドレスの送信元の国または国内地域最大長は 32 バイトです。
宛先（dstloc）	プライベート アドレスの宛先の国または国内地域。最大長は 32 バイトです。
コンテンツ タイプ（contenttype）	サブタイプが URL の場合にのみ適用されます。 HTTP 応答データのコンテンツ タイプ。最大長は 32 バイトです。
PCAP ID （pcap_id）	パケット キャプチャ（pcap） ID は、脅威 pcap ファイルをそのフローの一部として取得された拡張 pcap と相関させるための ID を示す 64 ビット未署名整数です。すべての脅威ログには、値が 0 の

フィールド名	説明
	pcap_id （関連付けられた pcap なし）か、拡張 pcap ファイルを指す ID のどちらかが含まれます。
ファイル ダイジェスト（filedigest）	WildFire サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。 ファイルダイジェスト文字列には、WildFire サービスによって分析されるために送信されたファイルのバイナリ ハッシュが示されます。
クラウド（cloud）	WildFire サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。 クラウド文字列には、分析用ファイルのアップロード元となった WildFire アプライアンス（プライベート）または WildFire クラウド（パブリック）のいずれかの FQDN が示されます。
URL インデックス（url_idx）	URLフィルタリングおよび WildFire サブタイプで使用されます。 アプリケーションが TCP キープアライブを使用して接続が開いた状態を一定時間維持すると、そのセッションのすべてのログ エントリのセッション ID は同一になります。その場合、1 つの脅威ログ（およびセッション ID）に複数の URL エントリが含まれていると、url_idx がカウンタとなり、1 つのセッション内の各ログ エントリの順序を相関させることができます。 たとえば、ファイアウォールが分析のために WildFire に転送したファイルの URL を調べるには、WildFire 送信ログからセッション ID と url_idx を見つけ、URL フィルタリング ログで同じセッション ID と url_idx を検索します。セッション ID と url_idx が一致したログ エントリには、WildFire に転送されたファイルの URL が含まれます。
ユーザー エージェント（user_agent）	URL フィルタリング サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。 ユーザー エージェント フィールドでは、ユーザーが URL へのアクセスに使用した Web ブラウザ（Internet Explorer など）を指定します。この情報は、HTTP 要求でサーバーに送信されます。
ファイル タイプ（filetype）	WildFire サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。 WildFire 分析のためにファイアウォールが転送したファイルのタイプを指定します。
X-Forwarded-For（XFF）	URL フィルタリング サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。

フィールド名	説明
	HTTP ヘッダーの X-Forwarded-For フィールドには、Web ページを要求したユーザーの IP アドレスが保持されています。これによりユーザーの IP アドレスを特定することができ、特に、パケットヘッダーの送信元 IP アドレス フィールドのユーザー IP アドレスを独自のアドレスで置き換えるプロキシ サーバーがネットワーク上に存在する場合に役立ちます。
Referer （referer）	URL フィルタリング サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。 HTTP ヘッダーの Referer フィールドには、ユーザーを別の Web ページにリンクした Web ページの URL が含まれています。これは、要求された Web ページにユーザーをリダイレクト（参照）した送信元です。
送信者（sender）	電子メールの送信者の名前を指定します。
サブジェクト（subject）	電子メールの件名を指定します。
受信者（recipient）	電子メールの受信者の名前を指定します。
レポート ID（reportid）	Data Filtering および WildFire サブタイプのみ。他のすべてのタイプでは、このフィールドは使用されません。 ファイアウォール、WildFire クラウド、または WildFire アプライアンス上の分析要求を識別します。
デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。 API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。

フィールド名	説明
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
送信元 VM UUID（src_uuid）	VMware NSX 環境のゲスト仮想マシンの送信元 UUID（Universally Unique Identifier）を識別します。
宛先 VM UUID（dst_uuid）	VMware NSX 環境のゲスト仮想マシンの宛先 UUID（Universally Unique Identifier）を識別します。
HTTP メソッド (http_method)	URL フィルタリング ログのみ。Web リクエストで使用する HTTP メソッドを示します。ログに記録されるのは次のメソッドだけです：Connect、Delete、Get、Head、Options、Post、Put。
トンネル ID/IMSI (tunnel_id/imsi)	International Mobile Subscriber Identity（IMSI）は、GSM/UMTS/EPS システム内の各モバイル サブスクライバに割り当てられる一意の番号です。IMSI は10進数（0～9）のみで構成され、最大桁数は 15 です。
モニタータグ/IMEI（monitortag/imei）	International Mobile Equipment Identity (IMEI) は、各モバイル ステーション装置に割り当てられた 15 あるいは 16 桁の一意の数字です。
親セッション ID（parent_session_id）	内部でこのセッションをトンネル化するトンネルの ID。内側のトンネル（2 レベルのトンネリングの場合）あるいは内部コンテンツ（1 レベルのトンネリングの場合）のみに適用されます。
親セッションスタート時間 (parent_start_time)	親トンネルのセッションが始まった年/月/日 時間:分:秒。
トンネル タイプ（tunnel）	GRE や IPSec などの、トンネルの種類。
脅威カテゴリ（thr_category）	異なる種類の脅威シグネチャを分類化するのに使用する脅威カテゴリを示します。 ドメイン 外部ダイナミック リスト がログを生成した場合、`domain-edl` はこのフィールドを生成します。
コンテンツ バージョン（contentver）	ログが生成される際の、ファイアウォール上のアプリケーションおよび脅威のバージョンです。
SCTP アソシエーション ID（assoc_id）	2 つの SCTP エンドポイント間の関連付けのためのすべての接続を識別する番号。

フィールド名	説明
ペイロード プロトコル ID (ppid)	データ チャンクのデータ部分内のペイロードのプロトコルの ID。
HTTP ヘッダの挿入 (http_headers)	ファイアウォールの URL ログ エントリに挿入された HTTP ヘッダーを示します。
URL カテゴリ リスト (url_category_list)	ファイアウォールがポリシーの適用に使用した URL フィルタリングカテゴリを一覧表示します。
ルール UUID (rule_uuid)	規則を恒久的に識別するUUID です。
HTTP/2 接続 (http2_connection)	次のいずれかの値を表示して、トラフィックが HTTP/2 コネクションを使用していたかどうかを識別します。 • TCP コネクション セッション ID—セッションは HTTP/2 • 0—セッションは HTTP/2 ではありません
ダイナミック ユーザー グループ名 (dynusergroup_name)	セッションを開始したユーザーを含むダイナミック ユーザー グループの名前。
XFF アドレス (xff_ip)	Webページをリクエストしたユーザーの IP アドレス、またはリクエストが通過した最後から2番目のデバイスの IP アドレス。リクエストが1つ以上のプロキシ、ロード バランサー、またはその他のアップストリーム デバイスを通過する場合、ファイアウォールは最も新しいデバイスの IP アドレスを表示します。
ソース デバイスのカテゴリ (src_category)	Device-ID がトラフィックの送信元として識別するデバイスのカテゴリ。
送信元のデバイスのプロファイル (src_profile)	Device-ID がトラフィックの送信元として識別するデバイスのデバイスのプロファイル。
送信元のデバイス モデル (src_model)	Device-ID がトラフィックの送信元として識別するデバイスのモデル。
送信元のデバイス ベンダー (src_vendor)	Device-ID がトラフィックの送信元として識別するデバイスのベンダー。
送信元デバイス OS ファミリ (src_osfamily)	Device-ID がトラフィックの送信元として識別するデバイスのオペレーティングシステムの種類。
送信元デバイス OS バージョン (src_osversion)	Device-ID がトラフィックの送信元として識別するデバイスのオペレーティングシステムのバージョン。

フィールド名	説明
送信元ホスト名 (src_host)	Device-ID がトラフィックの送信元として識別するデバイスのホスト名。
送信元 MAC アドレス (src_mac)	Device-ID がトラフィックの送信元として識別するデバイスの MAC アドレス。
宛先デバイスのカテゴリ (dst_category)	Device-ID がトラフィックの宛先として識別するデバイスのカテゴリ。
宛先デバイスのプロファイル (dst_profile)	Device-ID がトラフィックの宛先として識別するデバイスのデバイス プロファイル。
宛先デバイスのモデル (dst_model)	Device-ID がトラフィックの宛先として識別するデバイスのモデル。
宛先デバイスのベンダー (dst_vendor)	Device-ID がトラフィックの宛先として識別するデバイスのベンダー。
宛先 デバイス OS ファミリ (dst_osfamily)	Device-ID がトラフィックの宛先として識別するデバイスのオペレーティングシステムの種類。
宛先デバイス OS バージョン (dst_osversion)	Device-ID がトラフィックの宛先として識別するデバイスのオペレーティングシステムのバージョン。
宛先ホスト名 (dst_host)	Device-ID がトラフィックの宛先として識別するデバイスのホスト名。
宛先 MAC アドレス (dst_mac)	Device-ID がトラフィックの宛先として識別するデバイスの MAC アドレス。
コンテナ ID (container_id)	アプリケーション POD がデプロイされる Kubernetes ノードの PAN-NGFW ポッドのコンテナ ID。
POD 名前空間 (pod_namespace)	保護されているアプリケーション POD の名前空間。
POD 名 (pod_name)	保護されているアプリケーション PODの名前。
送信元の外部ダイナミックリスト (src_edl)	トラフィックの送信元 IP アドレスを含む外部ダイナミックリストの名前。
宛先の外部ダイナミック リスト (dst_edl)	トラフィックの宛先 IP アドレスを含む外部ダイナミックリストの名前。

フィールド名	説明
ホスト ID（hostid）	GlobalProtect がホストの識別のために割り当てる、一意の ID です。
ユーザーデバイスのシリアルナンバー (serialnumber)	ユーザーのマシンあるいはデバイスのシリアルナンバー。
ドメイン EDL (domain_edl)	トラフィックのドメイン名を含む外部ダイナミックリストの名前。
送信元のダイナミックアドレス グループ (src_dag)	元のセッション送信元のダイナミックアドレス グループ。
宛先のダイナミックアドレス グループ (dst_dag)	元の宛先送信元のダイナミックアドレス グループ。
部分的ハッシュ (partial_hash)	機械学習の部分的ハッシュ。
高解像度タイムスタンプ (high_res timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 この新規フィールドの形式は YYYY-MM-DDThh:ss:sssTZD です: • **YYYY**—西暦 • **MM**—2桁表記の月数 • **DD**—月の2桁の日 (01 ～ 31) • **T**—タイムスタンプの開始のインジケータ • **hh**—24時間を使用した2桁の時間数 (00 ～ 23) • **mm**—2桁表記の分 (00 ～ 59) • **ss**—2桁表記の秒 (00 ～ 60) • **sss**—ミリ秒単位で1桁以上の桁数 • **TZD**—タイムゾーン指定子 (+hh:mm or -hh:mm)

フィールド名	説明
	高解像度タイムスタンプは、*PAN-OS 10.2* 以降のリリースを実行しているマネージドファイアウォールから受信したログでサポートされています。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*1969-12-31T16:00:00.000-8:00* というタイムスタンプを表示します。
理由 (reason)	データ フィルタリング アクションの理由。
正当化 (justification)	データ フィルタリング アクションの正当化。
スライス サービスの種類 (nssai_sst)	ネットワーク スライス ID の A スライス サービス タイプ。
アプリケーション サブカテゴリ (subcategory_of_app)	アプリケーション構成プロパティで指定されたアプリケーション サブカテゴリ。
アプリケーションカテゴリ (category_of_app)	アプリケーション構成プロパティで指定されたアプリケーション カテゴリ。値を以下に示します。 • business-system • コラボレーション • 一般インターネット • メディア • networking • SaaS
アプリケーション テクノロジー (technology_of_app)	アプリケーション構成プロパティで指定されたアプリケーション テクノロジ。値を以下に示します。 • ブラウザベース • クライアント/サーバー • ネットワークプロトコル • ピアツーピア
アプリケーションリスク (risk_of_app)	アプリケーションに関連付けられたリスク レベル (1 =最低から 5=最高)。
アプリケーション特性 (characteristic_of_app)	アプリケーションの適用可能特性のコンマ区切りリスト

フィールド名	説明
アプリケーション コンテナ (container_of_app)	アプリケーションの親アプリケーション。
トンネリングされたアプリケーション (tunneled_app)	トンネリングされたアプリケーションの名前。
アプリケーション SaaS (is_saas_of_app)	SaaS アプリケーションの場合は 1、SaaS アプリケーションでない場合は 0 を表示します。
アプリケーション認可状態 (sanctioned_state_of_app)	アプリケーションが認可されている場合は 1、アプリケーションが認可されていない場合は 0 が表示されます。
クラウド レポート ID (cloud_reportid)	(PAN-OS 10.2.0)ファイアウォールによって送信された DLP クラウド サービスによってスキャンされたファイルの一意の 32 文字の ID。 (PAN-OS 10.2.1 以降のリリース)ファイアウォールによって送信された DLP クラウド サービスによってスキャンされたファイルの一意の 67 文字の ID。 DLP クラウドサービスが既にスキャンして Cloud Report ID を生成したファイルに対して、同じ Cloud Report ID が表示されます。

URL フィルタリング ログ フィールド

フォーマット：FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Source Address, Destination Address, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, IP Protocol, Action, URL/Filename, Threat ID, Category, Severity, Direction, Sequence Number, Action Flags, Source Country, Destination Country, FUTURE_USE, Content Type, PCAP_ID, File Digest, Cloud, URL Index, User Agent, File Type, X-Forwarded-For, Referer, Sender, Subject, Recipient, Report ID, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, FUTURE_USE, Source VM UUID, Destination VM UUID, HTTP Method, Tunnel ID/IMSI, Monitor Tag/IMEI, Parent Session ID, Parent Start Time, Tunnel Type, Threat Category, Content Version, FUTURE_USE, SCTP Association ID, Payload Protocol ID, HTTP Headers, URL Category List, Rule UUID, HTTP/2 Connection, Dynamic User Group Name, XFF Address, Source Device Category, Source Device Profile, Source Device Model, Source Device Vendor, Source Device OS Family, Source Device OS Version, Source Hostname, Source MAC Address, Destination Device Category, Destination Device Profile, Destination Device Model, Destination Device Vendor, Destination Device OS Family, Destination Device OS Version, Destination Hostname, Destination MAC Address, Container ID, POD Namespace, POD Name, Source External Dynamic List, Destination

External Dynamic List, Host ID, Serial Number, Domain EDL, Source Dynamic Address Group, Destination Dynamic Address Group, Partial Hash, High Resolution Timestamp, Reason, Justification, A Slice Service Type, Application Subcategory, Application Category, Application Technology, Application Risk, Application Characteristic, Application Container, Tunneled Application, Application SaaS, Application Sanctioned State, Cloud Report ID

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号（serial #）	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は THREAT です。
脅威/コンテンツ タイプ (subtype)	脅威ログのサブタイプ。値は url です。
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
送信元アドレス (src)	元のセッション送信元 IP アドレス。
宛先アドレス (dst)	元のセッション宛先 IP アドレス。
NAT ソース IP (natsrc)	送信元 NAT が実行された場合は、NAT 後の送信元 IP アドレス。
NAT 宛先 IP (natdst)	宛先 NAT が実行された場合は、NAT 後の宛先 IP アドレス。
ルール名（rule）	セッションで一致したルールの名前。
送信元ユーザー (srcuser)	セッションを開始したユーザーのユーザー名。
宛先ユーザー (dstuser)	セッションの宛先となったユーザーのユーザー名。
アプリケーション (app)	セッションに関連付けられたアプリケーション。
仮想システム (vsys)	セッションに関連付けられている仮想システム。
送信元ゾーン (from)	セッションの送信元だったゾーン。
宛先ゾーン (to)	セッションの宛先だったゾーン。

フィールド名	説明
インバウンド インターフェイス (inbound_if)	セッションの送信元となったインターフェイス。
アウトバウンド インターフェイス (outbound_if)	セッションの宛先だったインターフェイス。
ログ アクション (logset)	セッションに適用されたログ転送プロファイル。
セッション ID (sessionid)	各セッションに適用される内部の数値識別子。
リピートカウント（repeatcnt）	5 秒以内に開始された、送信元 IP、宛先 IP、アプリケーション、コンテンツ/脅威タイプが同じになっているセッションの数です。
送信元ポート（sport）	セッションで使用された送信元ポート。
宛先ポート（dport）	セッションで使用された宛先ポート。
NAT ソース ポート（natsport）	NAT 後の送信元ポート。
NAT 宛先ポート（natdport）	NAT 後の宛先ポート。
フラッグ（flags）	セッションに関する詳細を示す 32 ビット フィールド。このフィールドは、以下のように、その値とログに記録されている値を AND 演算することによってデコードできます。 • 0X80000000—セッションにパケット キャプチャがあります（PCAP） • 0x40000000—クライアントが複数のパスを使用して宛先ホストに接続できるようにするオプションが有効です • 0x20000000—判定を行うためにファイルが WildFire に送信されます • 0x10000000—エンドユーザーによるエンタープライズ認証情報の送信を検出 • 0x08000000— 対象のフローのソースが許可リストに登録されており、偵察保護の対象になっていません • 0x02000000—IPv6 セッション • 0x01000000—SSL セッションが復号化されます（SSL プロキシ）

フィールド名	説明
	• 0x00800000–セッションが URL フィルタリングによって拒否されます • 0x00400000–セッションで NAT 変換が実行されました • 0x00200000–セッションのユーザー情報が認証ポータルを通じて取得されました • 0x00100000–標準的でない宛先ポート上にアプリケーショントラフィックがあります • 0x00080000 – プロキシからの X-Forwarded-For 値は送信元ユーザー フィールドにあります • 0x00040000 – ログは http プロキシ セッション内のトランザクションに対応します（プロキシ トランザクション） • 0x00020000–クライアントからサーバーへのフローがポリシーベース フォワーディングの対象になっています • 0x00010000–サーバーからクライアントへのフローがポリシーベース フォワーディングの対象になっています • 0x00008000 – セッションはコンテナ ページ アクセスです（コンテナ ページ） • 0x00002000 – セッションに、暗黙的なアプリケーションの依存関係処理のルールでの一時的な一致があります。PAN-OS 5.0.0 以降で使用できます。 • 0x00000800 –このセッションのトラフィックを転送するために対称リターンが使用されます • 0x00000400–復号化されたトラフィックがミラーポートを介してクリアテキストを送信しています • 0x00000010–外側のトンネルのペイロードを検査中です
IP プロトコル（proto）	セッションに関連付けられた IP プロトコル。
アクション（action）	セッションに対して実行されたアクション。値は、alert、allow、block-url、block-continue、continue、block-override、override-lockout、override です。 • alert – 脅威または URL が検出されましたが、ブロックされていません • allow– フラッド検出アラート • block-url – ブロックするように設定された URL カテゴリで照合が行われたため、URL 要求がブロックされました • block-continue–HTTP 要求がブロックされ、Continue ページにリダイレクトされ、続行を確認するためのボタンが表示されます。

フィールド名	説明
	• continue —Block-continue 要求の続行が許可されたことを示すブロック継続 URL 継続ページへの応答 • block-override —HTTP 要求はブロックされ、続行するために firewall 管理者からのパス コードを必要とする Admin オーバーライド ページにリダイレクトされます。 • override-lockout — ソース IP からの失敗した管理者オーバーライド パス コードの試行が多すぎます。IP が block-override リダイレクト ページからブロックされるようになりました • override —正しいパス コードが提供され、要求が許可されている Block-override ページに応答します
URL/ファイル名 (misc)	可変長フィールドです。URL の最大文字数は 1023 文字です。 サブタイプが url の場合の実際の URI。 Threat Category が `domain-edl` の場合の URL。
脅威/コンテンツ名 (threatid)	既知およびカスタム脅威に対する Palo Alto Networksの識別子。一部のサブタイプでは、説明の文字列にかっこで囲んだ 64 ビットの数値識別子が続きます。 • 8000 ～ 8099 — スキャン検出 • 8500 ～ 8599 — フラッド検出 • 9999— URL フィルタリング ログ • 10000 ～ 19999 — スパイウェア フォンホーム検出 • 20000 ～ 29999 — スパイウェア ダウンロード検出 • 30000 ～ 44999 — 脆弱性悪用検出 • 52000 ～ 52999 — ファイルタイプ検出 • 60000 ～ 69999 — データ フィルタリング検出 domain EDL フィールドにデータが入力されている場合、このフィールドには同じ値が入力されます。 以前のリリースで使用されていたウイルス検出、*WildFire* シグネチャ フィード、および *DNS C2* シグネチャの 脅威 *ID* 範囲は、永続的かつ グローバルな一意の ID に置き換えられています。脅威/コンテンツ タイプ *(subtype)* および脅威カテゴリ *(thr_category)* フィールド名を参照し、更新されたレポート、フィルタ、脅威ログ、*ACC* アクティビティを作成します。

フィールド名	説明
カテゴリ（category）	URL サブタイプの場合は、URL カテゴリです。WildFire サブタイプの場合、それはファイルの評決であり、"マルウェア"、"フィッシング"、"グレーウェア"、または '無害' のいずれかです。その他のサブタイプの場合、値は 「any」です。
重大度 (severity)	脅威に関連付けられた重大度。値は、「informational」、「low」、「medium」、「high」、「critical」です。
方向 (direction)	攻撃の方向を示します。 • クライアントからサーバー • サーバーからクライアント
シーケンス番号（seqno）	順次増分される 64 ビットのログ エントリ識別子。各ログ タイプには、一意の番号空間があります。
アクション フラグ（actionflags）	ログが Panorama に転送されたかどうかを示すビット フィールド。
送信元（srcloc）	プライベート アドレスの送信元の国または国内地域最大長は 32 バイトです。
宛先（dstloc）	プライベート アドレスの宛先の国または国内地域。最大長は 32 バイトです。
コンテンツ タイプ（contenttype）	HTTP 応答データのコンテンツ タイプ。最大長は 32 バイトです。
PCAP ID （pcap_id）	パケット キャプチャ（pcap） ID は、脅威 pcap ファイルをそのフローの一部として取得された拡張 pcap と相関させるための ID を示す 64 ビット未署名整数です。すべての脅威ログには、値が 0 の pcap_id （関連付けられた pcap なし）か、拡張 pcap ファイルを指す ID のどちらかが含まれます。
ファイル ダイジェスト（filedigest）	WildFire サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。 ファイルダイジェスト文字列には、WildFire サービスによって分析されるために送信されたファイルのバイナリ ハッシュが示されます。
クラウド（cloud）	WildFire サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。

フィールド名	説明
	クラウド文字列には、分析用ファイルのアップロード元となった WildFire アプライアンス（プライベート）または WildFire クラウド（パブリック）のいずれかの FQDN が示されます。
URL インデックス（url_idx）	アプリケーションが TCP キープアライブを使用して接続が開いた状態を一定時間維持すると、そのセッションのすべてのログ エントリのセッション ID は同一になります。その場合、1 つの脅威ログ（およびセッション ID）に複数の URL エントリが含まれていると、url_idx がカウンタとなり、1 つのセッション内の各ログ エントリの順序を相関させることができます。 たとえば、ファイアウォールが分析のために WildFire に転送したファイルの URL を調べるには、WildFire 送信ログからセッション ID と url_idx を見つけ、URL フィルタリング ログで同じセッション ID と url_idx を検索します。セッション ID と url_idx が一致したログ エントリには、WildFire に転送されたファイルの URL が含まれます。
ユーザー エージェント（user_agent）	ユーザー エージェント フィールドでは、ユーザーが URL へのアクセスに使用した Web ブラウザ（Internet Explorer など）を指定します。この情報は、HTTP 要求でサーバーに送信されます。
ファイル タイプ（filetype）	WildFire サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。 WildFire 分析のためにファイアウォールが転送したファイルのタイプを指定します。
X-Forwarded-For（XFF）	HTTP ヘッダーの X-Forwarded-For フィールドには、Web ページを要求したユーザーの IP アドレスが保持されています。これによりユーザーの IP アドレスを特定することができ、特に、パケット ヘッダーの送信元 IP アドレス フィールドのユーザー IP アドレスを独自のアドレスで置き換えるプロキシ サーバーがネットワーク上に存在する場合に役立ちます。
Referer （referer）	HTTP ヘッダーの Referer フィールドには、ユーザーを別の Web ページにリンクした Web ページの URL が含まれています。これは、要求された Web ページにユーザーをリダイレクト（参照）した送信元です。
送信者（sender）	電子メールの送信者の名前を指定します。
サブジェクト（subject）	電子メールの件名を指定します。
受信者（recipient）	電子メールの受信者の名前を指定します。

フィールド名	説明
レポート ID（reportid）	Data Filtering および WildFire サブタイプのみ。他のすべてのタイプでは、このフィールドは使用されません。 ファイアウォール、WildFire クラウド、または WildFire アプライアンス上の分析要求を識別します。
デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。 API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
送信元 VM UUID（src_uuid）	VMware NSX 環境のゲスト仮想マシンの送信元 UUID（Universally Unique Identifier）を識別します。
宛先 VM UUID（dst_uuid）	VMware NSX 環境のゲスト仮想マシンの宛先 UUID（Universally Unique Identifier）を識別します。
HTTP メソッド (http_method)	Web リクエストで使用する HTTP メソッドを示します。ログに記録されるのは次のメソッドだけです：Connect、Delete、Get、Head、Options、Post、Put。
トンネル ID/IMSI (tunnel_id/imsi)	International Mobile Subscriber Identity（IMSI）は、GSM/UMTS/EPS システム内の各モバイル サブスクライバに割り当てられる一意の番号です。IMSI は10進数（0～9）のみで構成され、最大桁数は 15 です。

フィールド名	説明
モニタータグ/ IMEI（monitortag/imei）	International Mobile Equipment Identity (IMEI) は、各モバイル ステーション装置に割り当てられた 15 あるいは 16 桁の一意の数字です。
親セッション ID（parent_session_id）	内部でこのセッションをトンネル化するトンネルの ID。内側のトンネル（2 レベルのトンネリングの場合）あるいは内部コンテンツ（1 レベルのトンネリングの場合）のみに適用されます。
親セッションスタート時間 (parent_start_time)	親トンネルのセッションが始まった年/月/日 時間:分:秒。
トンネル タイプ（tunnel）	GRE や IPSec などの、トンネルの種類。
脅威カテゴリ（thr_category）	異なる種類の脅威シグネチャを分類化するのに使用する脅威カテゴリを示します。 ドメイン 外部ダイナミック リスト がログを生成した場合、`domain-edl` はこのフィールドを生成します。
コンテンツ バージョン（contentver）	ログが生成される際の、ファイアウォール上のアプリケーションおよび脅威のバージョンです。
SCTP アソシエーション ID（assoc_id）	2 つの SCTP エンドポイント間の関連付けのためのすべての接続を識別する番号。
ペイロード プロトコル ID (ppid)	データ チャンクのデータ部分内のペイロードのプロトコルの ID。
HTTP ヘッダの挿入 (http_headers)	ファイアウォールの URL ログ エントリに挿入された HTTP ヘッダーを示します。
URL カテゴリ リスト (url_category_list)	ファイアウォールがポリシーの適用に使用した URL フィルタリングカテゴリを一覧表示します。
ルール UUID (rule_uuid)	規則を恒久的に識別するUUID です。
HTTP/2 接続 (http2_connection)	次のいずれかの値を表示して、トラフィックが HTTP/2 コネクションを使用していたかどうかを識別します。 • TCP コネクション セッション ID—セッションは HTTP/2 • 0—セッションは HTTP/2 ではありません

フィールド名	説明
ダイナミック ユーザー グループ名 (dynusergroup_name)	セッションを開始したユーザーを含むダイナミック ユーザー グループの名前。
XFF アドレス (xff_ip)	WebページをリクエストしたユーザーのIPアドレス、またはリクエストが通過した最後から2番目のデバイスのIPアドレス。リクエストが1つ以上のプロキシ、ロード バランサー、またはその他のアップストリーム デバイスを通過する場合、ファイアウォールは最も新しいデバイスの IP アドレスを表示します。
ソース デバイスのカテゴリ (src_category)	Device-ID がトラフィックの送信元として識別するデバイスのカテゴリ。
送信元のデバイスのプロファイル (src_profile)	Device-ID がトラフィックの送信元として識別するデバイスのデバイスのプロファイル。
送信元のデバイス モデル (src_model)	Device-ID がトラフィックの送信元として識別するデバイスのモデル。
送信元のデバイス ベンダー (src_vendor)	Device-ID がトラフィックの送信元として識別するデバイスのベンダー。
送信元デバイス OS ファミリ (src_osfamily)	Device-ID がトラフィックの送信元として識別するデバイスのオペレーティングシステムの種類。
送信元デバイス OS バージョン (src_osversion)	Device-ID がトラフィックの送信元として識別するデバイスのオペレーティングシステムのバージョン。
送信元ホスト名 (src_host)	Device-ID がトラフィックの送信元として識別するデバイスのホスト名。
送信元 MAC アドレス (src_mac)	Device-ID がトラフィックの送信元として識別するデバイスの MAC アドレス。
宛先デバイスのカテゴリ (dst_category)	Device-ID がトラフィックの宛先として識別するデバイスのカテゴリ。
宛先デバイスのプロファイル (dst_profile)	Device-ID がトラフィックの宛先として識別するデバイスのデバイス プロファイル。
宛先デバイスのモデル (dst_model)	Device-ID がトラフィックの宛先として識別するデバイスのモデル。

フィールド名	説明
宛先デバイスのベンダー (dst_vendor)	Device-ID がトラフィックの宛先として識別するデバイスのベンダー。
宛先 デバイス OS ファミリ (dst_osfamily)	Device-ID がトラフィックの宛先として識別するデバイスのオペレーティングシステムの種類。
宛先デバイス OS バージョン (dst_osversion)	Device-ID がトラフィックの宛先として識別するデバイスのオペレーティングシステムのバージョン。
宛先ホスト名 (dst_host)	Device-ID がトラフィックの宛先として識別するデバイスのホスト名。
宛先 MAC アドレス (dst_mac)	Device-ID がトラフィックの宛先として識別するデバイスの MAC アドレス。
コンテナ ID (container_id)	アプリケーション POD がデプロイされる Kubernetes ノードの PAN-NGFW ポッドのコンテナ ID。
POD 名前空間 (pod_namespace)	保護されているアプリケーション POD の名前空間。
POD 名 (pod_name)	保護されているアプリケーション PODの名前。
送信元の外部ダイナミックリスト (src_edl)	トラフィックの送信元 IP アドレスを含む外部ダイナミックリストの名前。
宛先の外部ダイナミック リスト (dst_edl)	トラフィックの宛先 IP アドレスを含む外部ダイナミックリストの名前。
ホスト ID（hostid）	GlobalProtect がホストの識別のために割り当てる、一意の ID です。
ユーザーデバイスのシリアルナンバー (serialnumber)	ユーザーのマシンあるいはデバイスのシリアルナンバー。
ドメイン EDL (domain_edl)	トラフィックのドメイン名を含む外部ダイナミックリストの名前。
送信元のダイナミックアドレス グループ (src_dag)	元のセッション送信元のダイナミックアドレス グループ。

フィールド名	説明
宛先のダイナミック アドレス グループ (dst_dag)	元の宛先送信元のダイナミックアドレス グループ。
部分的ハッシュ (partial_hash)	機械学習の部分的ハッシュ。
高解像度タイムスタンプ (high_res timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 この新規フィールドの形式は YYYY-MM-DDThh:ss:sssTZD です: • **YYYY**—西暦 • **MM**—2桁表記の月数 • **DD**—月の2桁の日 (01 ～ 31) • **T**—タイムスタンプの開始のインジケータ • **hh**—24時間を使用した2桁の時間数 (00 ～ 23) • **mm**—2桁表記の分 (00 ～ 59) • **ss**—2桁表記の秒 (00 ～ 60) • **sss**—ミリ秒単位で1桁以上の桁数 • **TZD**—タイムゾーン指定子 (+hh:mm or -hh:mm) 高解像度タイムスタンプは、*PAN-OS 10.1* 以降のリリースを実行している管理対象ファイアウォールから受信したログに対してサポートされています。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*`1969-12-31T16:00:00:000-8:00`* というタイムスタンプを表示します。
理由 (reason)	URL フィルタリング アクションの理由。
正当化 (justification)	URL Filtering アクションの正当性。
スライス サービスの種類 (nssai_sst)	ネットワーク スライス ID の A スライス サービス タイプ。
アプリケーション サブカテゴリ (subcategory_of_app)	アプリケーション構成プロパティで指定されたアプリケーション サブカテゴリ。

フィールド名	説明
アプリケーションカテゴリ (category_of_app)	アプリケーション構成プロパティで指定されたアプリケーションカテゴリ。値を以下に示します。 • business-system • コラボレーション • 一般インターネット • メディア • networking • SaaS
アプリケーションテクノロジー (technology_of_app)	アプリケーション構成プロパティで指定されたアプリケーションテクノロジ。値を以下に示します。 • ブラウザベース • クライアント/サーバー • ネットワークプロトコル • ピアツーピア
アプリケーションリスク (risk_of_app)	アプリケーションに関連付けられたリスク レベル (1 =最低から 5=最高)。
アプリケーション特性 (characteristic_of_app)	アプリケーションの適用可能特性のコンマ区切りリスト
アプリケーション コンテナ (container_of_app)	アプリケーションの親アプリケーション。
トンネリングされたアプリケーション (tunneled_app)	トンネリングされたアプリケーションの名前。
アプリケーション SaaS (is_saas_of_app)	SaaS アプリケーションの場合は yes 、SaaS アプリケーションでない場合は no を表示します。
アプリケーション認可状態 (sanctioned_state_of_app)	アプリケーションが認可されている場合は yes を表示し、アプリケーションが認可されていない場合は no を表示します。
クラウド レポート ID (cloud_reportid)	(PAN-OS 10.2.0)firewall によって送信された DLP クラウド サービスによってスキャンされたファイルの一意の 32 文字の ID。 (PAN-OS 10.2.1 以降のリリース)firewall によって送信された DLP クラウド サービスによってスキャンされたファイルの一意の 67 文字の ID。

フィールド名	説明
	DLP クラウドサービスが既にスキャンして Cloud Report ID を生成したファイルに対して、同じ Cloud Report ID が表示されます。

データ フィルタリング ログ フィールド

フォーマット：FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Source Address, Destination Address, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, IP Protocol, Action, URL/Filename, Threat ID, Category, Severity, Direction, Sequence Number, Action Flags, Source Country, Destination Country, FUTURE_USE, Content Type, PCAP_ID, File Digest, Cloud, URL Index, User Agent, File Type, X-Forwarded-For, Referer, Sender, Subject, Recipient, Report ID, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, FUTURE_USE, Source VM UUID, Destination VM UUID, HTTP Method, Tunnel ID/IMSI, Monitor Tag/IMEI, Parent Session ID, Parent Start Time, Tunnel Type, Threat Category, Content Version, FUTURE_USE, SCTP Association ID, Payload Protocol ID, HTTP Headers, URL Category List, Rule UUID, HTTP/2 Connection, Dynamic User Group Name, XFF Address, Source Device Category, Source Device Profile, Source Device Model, Source Device Vendor, Source Device OS Family, Source Device OS Version, Source Hostname, Source MAC Address, Destination Device Category, Destination Device Profile, Destination Device Model, Destination Device Vendor, Destination Device OS Family, Destination Device OS Version, Destination Hostname, Destination MAC Address, Container ID, POD Namespace, POD Name, Source External Dynamic List, Destination External Dynamic List, Host ID, Serial Number, Domain EDL, Source Dynamic Address Group, Destination Dynamic Address Group, Partial Hash, High Resolution Timestamp, Reason, Justification, A Slice Service Type, Application Subcategory, Application Category, Application Technology, Application Risk, Application Characteristic, Application Container, Tunneled Application, Application SaaS, Application Sanctioned State, Cloud Report ID

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号（serial #）	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は THREAT です。
脅威/コンテンツ タイプ (subtype)	脅威ログのサブタイプ。値はデータ、dlp、dlp-non-file、ファイルです。
生成時間 (time_generated ま	データプレーンでログが生成された日時。

フィールド名	説明
たは cef-formatted-time_generated)	
送信元アドレス (src)	元のセッション送信元 IP アドレス。
宛先アドレス (dst)	元のセッション宛先 IP アドレス。
NAT ソース IP (natsrc)	送信元 NAT が実行された場合は、NAT 後の送信元 IP アドレス。
NAT 宛先 IP (natdst)	宛先 NAT が実行された場合は、NAT 後の宛先 IP アドレス。
ルール名（rule）	セッションで一致したルールの名前。
送信元ユーザー (srcuser)	セッションを開始したユーザーのユーザー名。
宛先ユーザー (dstuser)	セッションの宛先となったユーザーのユーザー名。
アプリケーション (app)	セッションに関連付けられたアプリケーション。
仮想システム (vsys)	セッションに関連付けられている仮想システム。
送信元ゾーン (from)	セッションの送信元だったゾーン。
宛先ゾーン (to)	セッションの宛先だったゾーン。
インバウンド インターフェイス (inbound_if)	セッションの送信元となったインターフェイス。
アウトバウンド インターフェイス (outbound_if)	セッションの宛先だったインターフェイス。
ログ アクション (logset)	セッションに適用されたログ転送プロファイル。
セッション ID (sessionid)	各セッションに適用される内部の数値識別子。
リピートカウント（repeatcnt）	5 秒以内に開始された、送信元 IP、宛先 IP、アプリケーション、コンテンツ/脅威タイプが同じになっているセッションの数です。
送信元ポート（sport）	セッションで使用された送信元ポート。
宛先ポート（dport）	セッションで使用された宛先ポート。

フィールド名	説明
NAT ソース ポート（natsport）	NAT 後の送信元ポート。
NAT 宛先ポート（natdport）	NAT 後の宛先ポート。
フラッグ（flags）	セッションに関する詳細を示す 32 ビット フィールド。このフィールドは、以下のように、その値とログに記録されている値を AND 演算することによってデコードできます。 • 0X80000000—セッションにパケット キャプチャがあります（PCAP） • 0x40000000—クライアントが複数のパスを使用して宛先ホストに接続できるようにするオプションが有効です • 0x20000000—判定を行うためにファイルが WildFire に送信されます • 0x10000000—エンドユーザーによるエンタープライズ認証情報の送信を検出 • 0x08000000— 対象のフローのソースが許可リストに登録されており、偵察保護の対象になっていません • 0x02000000—IPv6 セッション • 0x01000000—SSL セッションが復号化されます（SSL プロキシ） • 0x00800000—セッションが URL フィルタリングによって拒否されます • 0x00400000—セッションで NAT 変換が実行されました • 0x00200000—セッションのユーザー情報が認証ポータルを通じて取得されました • 0x00100000—標準的でない宛先ポート上にアプリケーション トラフィックがあります • 0x00080000 — プロキシからの X-Forwarded-For 値は送信元ユーザー フィールドにあります • 0x00040000 — ログは http プロキシ セッション内のトランザクションに対応します（プロキシ トランザクション） • 0x00020000—クライアントからサーバーへのフローがポリシー ベース フォワーディングの対象になっています • 0x00010000—サーバーからクライアントへのフローがポリシー ベース フォワーディングの対象になっています • 0x00008000 — セッションはコンテナ ページ アクセスです（コンテナ ページ）

フィールド名	説明
	• 0x00002000 – セッションに、暗黙的なアプリケーションの依存関係処理のルールでの一時的な一致があります。PAN-OS 5.0.0 以降で使用できます。 • 0x00000800 –このセッションのトラフィックを転送するために対称リターンが使用されます • 0x00000400–復号化されたトラフィックがミラーポートを介してクリアテキストを送信しています • 0x00000010–外側のトンネルのペイロードを検査中です
IP プロトコル（proto）	セッションに関連付けられた IP プロトコル。
アクション（action）	セッションに対して実行されたアクション。値は、「alert」、「allow」、「deny」、「drop」、「drop-all-packets」、「reset-client」、「reset-server」、「reset-both」、「block-url」です。 • alert:一致するデータを含むトラフィックが検出されましたが、ブロックされていません • 許可 (DLP サブタイプのみ) - フラッド検出アラート • block (dlp および WildFire サブタイプのみ) – 検出されたがブロックされた一致するデータを含むトラフィック • block-continue (dlp サブタイプのみ):一致するデータを含むトラフィックがブロックされ、続行を確認するボタンがある [続行] ページにリダイレクトされます。 • continue (dlp サブタイプのみ) - ブロック継続要求の続行が許可されたことを示すブロック継続ページへの応答 • deny (dlp サブタイプのみ):フラッド検出メカニズムがアクティブになり、構成に基づいてトラフィックが拒否されます。
URL/ファイル名 (misc)	可変長フィールドです。ファイル名は最大 63 文字です。 サブタイプが dlp の場合のファイル名 Threat Category が **domain-edl** の場合の URL。
脅威/コンテンツ名 (threatid)	既知およびカスタム脅威に対する Palo Alto Networksの識別子。一部のサブタイプでは、説明の文字列にかっこで囲んだ 64 ビットの数値識別子が続きます。 • 8000 ～ 8099 – スキャン検出 • 8500 ～ 8599 – フラッド検出 • 9999– URL フィルタリング ログ • 10000 ～ 19999 – スパイウェア フォンホーム検出 • 20000 ～ 29999 – スパイウェア ダウンロード検出

フィールド名	説明
	• 30000 ～ 44999 — 脆弱性悪用検出 • 52000 ～ 52999 — ファイルタイプ検出 • 60000 ～ 69999 — データ フィルタリング検出 ドメイン EDL フィールドに値が入力されている場合、このフィールドに同じ値が入力されます。 以前のリリースで使用されていたウイルス検出、*WildFire* シグネチャ フィード、および *DNS C2* シグネチャの 脅威 *ID* 範囲は、永続的かつ グローバルな一意の ID に置き換えられています。脅威/コンテンツ タイプ *(subtype)* および脅威カテゴリ *(thr_category)* フィールド名を参照し、更新されたレポート、フィルタ、脅威ログ、*ACC* アクティビティを作成します。
カテゴリ（category）	URL サブタイプの場合は、URL カテゴリです。WildFire サブタイプの場合、それはファイルの評決であり、"マルウェア"、"フィッシング"、"グレーウェア"、または '無害' のいずれかです。その他のサブタイプの場合、値は 「any」です。
重大度 (severity)	脅威に関連付けられた重大度。値は、「informational」、「low」、「medium」、「high」、「critical」です。
方向 (direction)	攻撃の方向を示します。 • クライアントからサーバー • サーバーからクライアント
シーケンス番号（seqno）	順次増分される 64 ビットのログ エントリ識別子。各ログ タイプには、一意の番号空間があります。
アクション フラグ（actionflags）	ログが Panorama に転送されたかどうかを示すビット フィールド。
送信元（srcloc）	プライベート アドレスの送信元の国または国内地域最大長は 32 バイトです。
宛先（dstloc）	プライベート アドレスの宛先の国または国内地域。最大長は 32 バイトです。
コンテンツ タイプ（contenttype）	サブタイプが URL の場合にのみ適用されます。 HTTP 応答データのコンテンツ タイプ。最大長は 32 バイトです。

フィールド名	説明
PCAP ID （pcap_id）	パケット キャプチャ（pcap） ID は、脅威 pcap ファイルをそのフローの一部として取得された拡張 pcap と相関させるための ID を示す 64 ビット未署名整数です。すべての脅威ログには、値が 0 の pcap_id （関連付けられた pcap なし）か、拡張 pcap ファイルを指す ID のどちらかが含まれます。
ファイル ダイジェスト（filedigest）	WildFire サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。 ファイルダイジェスト文字列には、WildFire サービスによって分析されるために送信されたファイルのバイナリ ハッシュが示されます。
クラウド（cloud）	WildFire サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。 クラウド文字列には、分析用ファイルのアップロード元となった WildFire アプライアンス（プライベート）または WildFire クラウド（パブリック）のいずれかの FQDN が示されます。
URL インデックス（url_idx）	URLフィルタリングおよび WildFire サブタイプで使用されます。 アプリケーションが TCP キープアライブを使用して接続が開いた状態を一定時間維持すると、そのセッションのすべてのログ エントリのセッション ID は同一になります。その場合、1 つの脅威ログ（およびセッション ID）に複数の URL エントリが含まれていると、url_idx がカウンタとなり、1 つのセッション内の各ログ エントリの順序を相関させることができます。 たとえば、ファイアウォールが分析のために WildFire に転送したファイルの URL を調べるには、WildFire 送信ログからセッション ID と url_idx を見つけ、URL フィルタリング ログで同じセッション ID と url_idx を検索します。セッション ID と url_idx が一致したログ エントリには、WildFire に転送されたファイルの URL が含まれます。
ユーザー エージェント（user_agent）	URL フィルタリング サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。 ユーザー エージェント フィールドでは、ユーザーが URL へのアクセスに使用した Web ブラウザ（Internet Explorer など）を指定します。この情報は、HTTP 要求でサーバーに送信されます。
ファイル タイプ（filetype）	firewall が分析のために転送するファイルのタイプを指定します。

フィールド名	説明
X-Forwarded-For（XFF）	URL フィルタリング サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。 HTTP ヘッダーの X-Forwarded-For フィールドには、Web ページを要求したユーザーの IP アドレスが保持されています。これによりユーザーの IP アドレスを特定することができ、特に、パケットヘッダーの送信元 IP アドレス フィールドのユーザー IP アドレスを独自のアドレスで置き換えるプロキシ サーバーがネットワーク上に存在する場合に役立ちます。
Referer （referer）	URL フィルタリング サブタイプの場合のみ。それ以外のすべてのタイプではこのフィールドを使用しません。 HTTP ヘッダーの Referer フィールドには、ユーザーを別の Web ページにリンクした Web ページの URL が含まれています。これは、要求された Web ページにユーザーをリダイレクト（参照）した送信元です。
送信者（sender）	電子メールの送信者の名前を指定します。
サブジェクト（subject）	電子メールの件名を指定します。
受信者（recipient）	電子メールの受信者の名前を指定します。
レポート ID（reportid）	firewall、WildFireクラウド、またはWildFireアプライアンスの分析要求を識別します。
デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。 API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`

フィールド名	説明
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
送信元 VM UUID（src_uuid）	VMware NSX 環境のゲスト仮想マシンの送信元 UUID（Universally Unique Identifier）を識別します。
宛先 VM UUID（dst_uuid）	VMware NSX 環境のゲスト仮想マシンの宛先 UUID（Universally Unique Identifier）を識別します。
HTTP メソッド (http_method)	URL フィルタリング ログのみ。Web リクエストで使用する HTTP メソッドを示します。ログに記録されるのは次のメソッドだけです：Connect、Delete、Get、Head、Options、Post、Put。
トンネル ID/IMSI (tunnel_id/imsi)	International Mobile Subscriber Identity（IMSI）は、GSM/UMTS/EPS システム内の各モバイル サブスクライバに割り当てられる一意の番号です。IMSI は10進数（0～9）のみで構成され、最大桁数は 15 です。
モニタータグ/IMEI（monitortag/imei）	International Mobile Equipment Identity (IMEI) は、各モバイル ステーション装置に割り当てられた 15 あるいは 16 桁の一意の数字です。
親セッション ID（parent_session_id）	内部でこのセッションをトンネル化するトンネルの ID。内側のトンネル（2 レベルのトンネリングの場合）あるいは内部コンテンツ（1 レベルのトンネリングの場合）のみに適用されます。
親セッションスタート時間 (parent_start_time)	親トンネルのセッションが始まった年/月/日 時間:分:秒。
トンネル タイプ（tunnel）	GRE や IPSec などの、トンネルの種類。
脅威カテゴリ（thr_category）	異なる種類の脅威シグネチャを分類化するのに使用する脅威カテゴリを示します。 ドメイン 外部ダイナミック リスト がログを生成した場合、`domain-edl` はこのフィールドを生成します。
コンテンツ バージョン（contentver）	ログが生成される際の、ファイアウォール上のアプリケーションおよび脅威のバージョンです。

フィールド名	説明
SCTP アソシエーション ID（assoc_id）	2 つの SCTP エンドポイント間の関連付けのためのすべての接続を識別する番号。
ペイロード プロトコル ID (ppid)	データ チャンクのデータ部分内のペイロードのプロトコルの ID。
HTTP ヘッダの挿入 (http_headers)	ファイアウォールの URL ログ エントリに挿入された HTTP ヘッダーを示します。
URL カテゴリ リスト (url_category_list)	ファイアウォールがポリシーの適用に使用した URL フィルタリングカテゴリを一覧表示します。
ルール UUID (rule_uuid)	規則を恒久的に識別するUUID です。
HTTP/2 接続 (http2_connection)	次のいずれかの値を表示して、トラフィックが HTTP/2 コネクションを使用していたかどうかを識別します。 • TCP コネクション セッション ID—セッションは HTTP/2 • 0—セッションは HTTP/2 ではありません
ダイナミック ユーザー グループ名 (dynusergroup_name)	セッションを開始したユーザーを含むダイナミック ユーザー グループの名前。
XFF アドレス (xff_ip)	Webページをリクエストしたユーザーの IP アドレス、またはリクエストが通過した最後から2番目のデバイスの IP アドレス。リクエストが1つ以上のプロキシ、ロード バランサー、またはその他のアップストリーム デバイスを通過する場合、ファイアウォールは最も新しいデバイスの IP アドレスを表示します。
ソース デバイスのカテゴリ (src_category)	Device-ID がトラフィックの送信元として識別するデバイスのカテゴリ。
送信元のデバイスのプロファイル (src_profile)	Device-ID がトラフィックの送信元として識別するデバイスのデバイスのプロファイル。
送信元のデバイス モデル (src_model)	Device-ID がトラフィックの送信元として識別するデバイスのモデル。
送信元のデバイス ベンダー (src_vendor)	Device-ID がトラフィックの送信元として識別するデバイスのベンダー。
送信元デバイス OS ファミリ (src_osfamily)	Device-ID がトラフィックの送信元として識別するデバイスのオペレーティングシステムの種類。

フィールド名	説明
送信元デバイス OS バージョン (src_osversion)	Device-ID がトラフィックの送信元として識別するデバイスのオペレーティングシステムのバージョン。
送信元ホスト名 (src_host)	Device-ID がトラフィックの送信元として識別するデバイスのホスト名。
送信元 MAC アドレス (src_mac)	Device-ID がトラフィックの送信元として識別するデバイスの MAC アドレス。
宛先デバイスのカテゴリ (dst_category)	Device-ID がトラフィックの宛先として識別するデバイスのカテゴリ。
宛先デバイスのプロファイル (dst_profile)	Device-ID がトラフィックの宛先として識別するデバイスのデバイス プロファイル。
宛先デバイスのモデル (dst_model)	Device-ID がトラフィックの宛先として識別するデバイスのモデル。
宛先デバイスのベンダー (dst_vendor)	Device-ID がトラフィックの宛先として識別するデバイスのベンダー。
宛先 デバイス OS ファミリ (dst_osfamily)	Device-ID がトラフィックの宛先として識別するデバイスのオペレーティングシステムの種類。
宛先デバイス OS バージョン (dst_osversion)	Device-ID がトラフィックの宛先として識別するデバイスのオペレーティングシステムのバージョン。
宛先ホスト名 (dst_host)	Device-ID がトラフィックの宛先として識別するデバイスのホスト名。
宛先 MAC アドレス (dst_mac)	Device-ID がトラフィックの宛先として識別するデバイスの MAC アドレス。
コンテナ ID (container_id)	アプリケーション POD がデプロイされる Kubernetes ノードの PAN-NGFW ポッドのコンテナ ID。
POD 名前空間 (pod_namespace)	保護されているアプリケーション POD の名前空間。
POD 名 (pod_name)	保護されているアプリケーション PODの名前。
送信元の外部ダイナミックリスト (src_edl)	トラフィックの送信元 IP アドレスを含む外部ダイナミックリストの名前。

フィールド名	説明
宛先の外部ダイナミック リスト (dst_edl)	トラフィックの宛先 IP アドレスを含む外部ダイナミックリストの名前。
ホスト ID（hostid）	GlobalProtect がホストの識別のために割り当てる、一意の ID です。
ユーザーデバイスのシリアルナンバー (serialnumber)	ユーザーのマシンあるいはデバイスのシリアルナンバー。
ドメイン EDL (domain_edl)	トラフィックのドメイン名を含む外部ダイナミックリストの名前。
送信元のダイナミックアドレス グループ (src_dag)	元のセッション送信元のダイナミックアドレス グループ。
宛先のダイナミックアドレス グループ (dst_dag)	元の宛先送信元のダイナミックアドレス グループ。
部分的ハッシュ (partial_hash)	機械学習の部分的ハッシュ。
高解像度タイムスタンプ (high_res timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 この新規フィールドの形式は YYYY-MM-DDThh:ss:sssTZD です: • **YYYY**—西暦 • **MM**—2桁表記の月数 • **DD**—月の2桁の日 (01 ～ 31) • **T**—タイムスタンプの開始のインジケータ • **hh**—24時間を使用した2桁の時間数 (00 ～ 23) • **mm**—2桁表記の分 (00 ～ 59) • **ss**—2桁表記の秒 (00 ～ 60) • **sss**—ミリ秒単位で1桁以上の桁数 • **TZD**—タイムゾーン指定子 (+hh:mm or -hh:mm)

フィールド名	説明
	高解像度タイムスタンプは、*PAN-OS 10.1* 以降のリリースを実行している管理対象ファイアウォールから受信したログに対してサポートされています。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*1969-12-31T16:00:00:000-8:00* というタイムスタンプを表示します。
理由 (reason)	データ フィルタリング アクションの理由。
正当化 (justification)	データ フィルタリング アクションの正当化。
スライス サービスの種類 (nssai_sst)	ネットワーク スライス ID の A スライス サービス タイプ。
アプリケーション サブカテゴリ (subcategory_of_app)	アプリケーション構成プロパティで指定されたアプリケーション サブカテゴリ。
アプリケーションカテゴリ (category_of_app)	アプリケーション構成プロパティで指定されたアプリケーション カテゴリ。値を以下に示します。 • business-system • コラボレーション • 一般インターネット • メディア • networking • SaaS
アプリケーション テクノロジー (technology_of_app)	アプリケーション構成プロパティで指定されたアプリケーション テクノロジ。値を以下に示します。 • ブラウザベース • クライアント/サーバー • ネットワークプロトコル • ピアツーピア
アプリケーションリスク (risk_of_app)	アプリケーションに関連付けられたリスク レベル (1 =最低から 5=最高)。
アプリケーション特性 (characteristic_of_app)	アプリケーションの適用可能特性のコンマ区切りリスト

フィールド名	説明
アプリケーション コンテナ (container_of_app)	アプリケーションの親アプリケーション。
トンネリングされたアプリケーション (tunneled_app)	トンネリングされたアプリケーションの名前。
アプリケーション SaaS (is_saas_of_app)	SaaS アプリケーションの場合は yes 、SaaS アプリケーションでない場合は no を表示します。
アプリケーション認可状態 (sanctioned_state_of_app)	アプリケーションが認可されている場合は yes を表示し、アプリケーションが認可されていない場合は no を表示します。
クラウド レポート ID (cloud_reportid)	(PAN-OS 10.2.0)firewall によって送信された DLP クラウド サービスによってスキャンされたファイルの一意の 32 文字の ID。 (PAN-OS 10.2.1 以降のリリース)firewall によって送信された DLP クラウド サービスによってスキャンされたファイルの一意の 67 文字の ID。 DLP クラウドサービスが既にスキャンして Cloud Report ID を生成したファイルに対して、同じ Cloud Report ID が表示されます。

HIP マッチ ログの各フィールド

フォーマット：FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Source User, Virtual System, Machine Name, Operating System, Source Address, HIP, Repeat Count, HIP Type, FUTURE_USE, FUTURE_USE, Sequence Number, Action Flags, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Virtual System ID, IPv6 Source Address, Host ID, User Device Serial Number, Device MAC Address, High Resolution Timestamp

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号 (serial)	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は HIP-MATCH です。

フィールド名	説明
脅威/コンテンツ タイプ (subtype)	HIP マッチ ログのサブタイプ（未使用）。
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
送信元ユーザー (srcuser)	セッションを開始したユーザーのユーザー名。
仮想システム (vsys)	HIP マッチ ログに関連付けられた仮想システム。
マシン名 (machinename)	ユーザーのマシンの名前です。
オペレーティングシステム (OS)	ユーザーのマシンまたはデバイス（またはクライアント システム）にインストールされているオペレーティング システム。
送信元アドレス (src)	送信元ユーザーの IP アドレス。
HIP （matchname）	HIP オブジェクトまたはプロファイルの名前。
リピートカウント (repeatcnt)	HIP プロファイルが一致した回数。
HIP タイプ (matchtype)	hip フィールドが HIP オブジェクトまたは HIP プロファイルを表すかどうか。
シーケンス番号 (seqno)	64 ビットのログ エントリ識別子。各ログ タイプには、一意の番号空間があります。
アクション フラグ (actionflags)	ログが Panorama に転送されたかどうかを示すビット フィールド。
デバイス グループ階層 (dg_hier_level_1 ～ dg_hier_level_4)	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値

フィールド名	説明
	12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。 API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
仮想システム ID (vsys_id)	Palo Alto Networks のファイアウォール上の仮想システムの一意な識別子。
IPv6 システム アドレス (srcipv6)	ユーザーのマシンあるいはデバイスの IPv6 アドレス
ホスト ID（hostid）	GlobalProtect がホストの識別のために割り当てる、一意の ID です。
ユーザーデバイスのシリアルナンバー (serialnumber)	ユーザーのマシンあるいはデバイスのシリアルナンバー。
デバイス MAC アドレス (mac)	ユーザーのマシンあるいはデバイスの MAC アドレス。
高解像度タイムスタンプ (high_res_timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 この新規フィールドの形式は YYYY-MM-DDThh:ss:sssTZD です: • **YYYY**—西暦 • **MM**—2桁表記の月数 • **DD**—月の2桁の日 (01 ～ 31) • **T**—タイムスタンプの開始のインジケータ • **hh**—24時間を使用した2桁の時間数 (00 ～ 23) • **mm**—2桁表記の分 (00 ～ 59) • **ss**—2桁表記の秒 (00 ～ 60) • **sss**—ミリ秒単位で1桁以上の桁数 • **TZD**—タイムゾーン指定子 (+hh:mm or -hh:mm)

フィールド名	説明
	高精細タイムスタンプは、*PAN-OS 10.2* 以降のリリースを実行しているマネージド *firewalls* から受信したログでサポートされています。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*1969-12-31T16:00:00:000-8:00* というタイムスタンプを表示します。

GlobalProtect ログ フィールド

フォーマット:FUTURE_USE、受信時刻、シリアル番号、種類、脅威/コンテンツ タイプ、FUTURE_USE、生成時刻、仮想システム、イベント ID、ステージ、認証方法、トンネルの種類、送信元ユーザー、送信元領域、マシン名、パブリック IP、パブリック IPv6、プライベート IP、プライベート IPv6、ホスト ID、シリアル番号、クライアント バージョン、クライアント OS、クライアント OS、クライアント OS バージョン、リピート回数、理由、エラー、説明、ステータス、ロケーション、ログイン期間、ログイン期間 接続方法、エラーコード、ポータル、シーケンス番号、アクションフラグ、高Resタイムスタンプ、選択タイプ、応答時間、優先度、試行されたゲートウェイ、ゲートウェイ、デバイスグループ階層レベル1、デバイスグループ階層レベル2、デバイスグループ階層レベル3、デバイスグループ階層レベル4、仮想システム名、デバイス名、仮想システムID

フィールド名	説明
受信時間（receive_time）	management plane (管理プレーン - MP)でログが受信された時間。
シリアル番号 (serial)	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は GLOBALPROTECT です。
脅威/コンテンツ タイプ (subtype)	脅威ログのサブタイプ値は以下を含みます。 • data – データ フィルタリング プロファイルと一致するデータ パターン • fileーファイルブロッキングプロファイルと一致するファイルタイプ • flood – ゾーン プロテクション プロファイルによって検出されたフラッド • packet–ゾーンプロテクションプロファイルでトリガーされたパケットベース攻撃防御 • scan – ゾーン プロテクション プロファイルによって検出されたスキャン

フィールド名	説明
	• Spyware —アンチスパイウェアプロファイルで検出したスパイウェア • url — URL フィルタリング ログ • virus—アンチウィルスプロファイルで検出したウィルス • Vulnerability —脆弱性防御プロファイルで検出した脆弱性バグ • Wildfire —ファイアウォールが WildFire 分析プロファイルで WildFire にファイルを送信し、判定（ログ内容により有害、フィッシング、グレイウェア、安全）が WildFire 送信ログに記録される時に生成される WildFire 判定 • wildfire-virus—アンチウィルスプロファイルで検出したウィルス
生成日時（time_generated）	データプレーンでログが生成された日時。
仮想システム (vsys)	セッションに関連付けられているvirtual system (仮想システム - vsys)。
イベント ID (eventid)	イベントの名前を示す文字列。
ステージ (stage)	接続の段階を示す文字列（たとえば、 `before-login`（ログイン前）、`login`（ログイン）、または`tunnel` （トンネル））。
認証方式 (auth_method)	`LDAP`、`RADIUS`、または`SAML`などの認証タイプを示す文字列。
トンネル タイプ (tunnel_type)	トンネル タイプ（SSLVPN または IPSec のいずれか）。
送信元ユーザー (srcuser)	セッションを開始したユーザーのユーザー名。
送信元リージョン (srcregion)	セッションを開始したユーザーのリージョン。
マシン名（machinename）	ユーザーのマシンの名前。
公開 IP (public_ip)	セッションを開始したユーザーの公開 IP アドレス。
公開 IPv6 (public_ipv6)	セッションを開始したユーザーの公開 IPv6 アドレス。

フィールド名	説明
プライベート IP (private_ip)	セッションを開始したユーザーのプライベート IP アドレス。
プライベート IPv6 (private_ipv6)	セッションを開始したユーザーのプライベート IPv6 アドレス。
ホスト ID（hostid）	GlobalProtect がホストの識別のために割り当てる、一意の ID。
シリアル番号 (serialnumber)	ユーザーのマシンあるいはデバイスのシリアル番号。
クライアント バージョン (client_ver)	クライアントの GlobalProtect アプリケーションのバージョン。
クライアント OS (client_os)	クライアント デバイスの OS タイプ（WindowsやLinuxなど）。
クライアント OS バージョン (client_os_ver)	クライアント デバイスの OS バージョン。
リピートカウント（repeatcnt）	過去 5 秒以内に GlobalProtect が検出した、同じ送信元 IP アドレス、宛先 IP アドレス、アプリケーション、およびサブタイプを持つセッションの数。
理由 (reason)	隔離の理由を示す文字列。
エラー (error)	いずれかのイベントで発生したエラーを示す文字列。
説明 (opaque)	発生したイベントの追加情報。
ステータス (status)	イベントのステータス（成功または失敗）。
場所 (location)	管理者が定義した GlobalProtect ポータルまたはゲートウェイの場所を示す文字列。
ログイン期間 (login_duration)	ユーザーがログインからログアウトまで GlobalProtectゲートウェイに接続している時間の長さ (秒単位)。
接続手段 (connect_method)	GlobalProtect アプリケーションがゲートウェイに接続する手段を示す文字列（たとえば、`on-demand`（オンデマンド）または`user-logon`（ユーザーログオン））。
エラーコード (error_code)	発生したエラーに関連付けられた整数。

フィールド名	説明
ポータル (portal)	GlobalProtect ポータルまたはゲートウェイの名前。
シーケンス番号（seqno）	64 ビットのログ エントリ識別子。各ログ タイプには、一意の番号空間があります。
アクション フラグ（actionflags）	ログが Panorama に転送されたかどうかを示すビット フィールド。
ゲートウェイ選択方法 (selection_type)	ゲートウェイに接続するために選択された接続方法。 • 手動– GlobalProtectアプリケーションと手動接続したいゲートウェイ。 • 優先– GlobalProtectアプリケーションと接続したい優先ゲートウェイ。 • 自動– ゲートウェイに割り当てられた優先度と応答時間に基づいて、**Best Available (**利用可能な最良の**)** ゲートウェイに自動的に接続します。
SSL 応答時間 (response_time)	トンネルのセットアップ中にエンドポイントでミリ秒単位で測定される、選択されたゲートウェイの SSL 応答時間。
ゲートウェイ優先度(priority)	GlobalProtectアプリケーションが接続できる最高 (1)、高 (2)、中 (3)、低 (4)、または最低 (5) に基づくゲートウェイの優先順位。
ゲートウェイ試行回数 (attempted_gateways)	ゲートウェイ接続の試行ごとに収集されるフィールドと、ゲートウェイ名、SSL 応答時間、および優先度 (複数のゲートウェイ設定でのゲートウェイの優先度を参照)。各フィールドのエントリは、`g82-gateway,12,3` というように、コンマで区切られます。各ゲートウェイのエントリは、`g83-gateway,10,2;g84-gateway,-1,1` というように、セミコロンで区切られます。
ゲートウェイ名(gateway)	ポータル設定で指定されているゲートウェイの名前。
デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。

フィールド名	説明
	API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
仮想システム ID (vsys_id)	Palo Alto Networks のファイアウォール上の仮想システムの一意な識別子。

IP-タグ ログ フィールド

フォーマット:FUTURE_USE , Receive Time, Serial, Type, Threat/Content Type, FUTURE_USE, Generate Time, Virtual System, Source IP, Tag Name , Event ID, Repeat Count , Timeout, Data Source Name, Data Source Type, Data Source Subtype, Sequence Number, Action Flags, DG Hierarchy Level 1 , DG Hierarchy Level 2, DG Hierarchy Level 3, DG Hierarchy Level 4, Virtual System Name, Device Name, Virtual System ID, High Resolution Timestamp

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号 (serial)	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は IPTAG です。
脅威/コンテンツ タイプ (subtype)	HIP マッチ ログのサブタイプ（未使用）。
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
仮想システム (vsys)	HIP マッチ ログに関連付けられた仮想システム。
送信元 IP (src)	送信元ユーザーの IP アドレス。

フィールド名	説明
タグ名 (tag_name)	送信元 IP アドレスにマッピングされたタグです。
イベント ID (event_id)	イベントの名前を示す文字列。
リピートカウント（repeatcnt）	5 秒以内に開始された、送信元 IP、宛先 IP、アプリケーション、サブタイプが同じになっているセッションの数。
タイムアウト (timeout)	送信元 IP アドレスについて IP アドレス対タグのマッピングが失効するまでの時間。
データソース名 (datasourcename)	マッピング情報の収集元になるソースの名前。
データソース タイプ (datasource_type)	マッピング情報の収集元になるソース。
データソース サブタイプ (datasource_subtype)	データソース内の IPアドレス - ユーザー名間マッピングを識別するために使用するメカニズム。
シーケンス番号（seqno）	順次増分される 64 ビットのログ エントリ識別子。各ログ タイプには、一意の番号空間があります。
アクション フラグ（actionflags）	ログが Panorama に転送されたかどうかを示すビット フィールド。
デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、この構造に含まれていない共有デバイス グループ（レベル 0 ）を除いて、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。 API クエリ: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。

フィールド名	説明
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
仮想システム ID (vsys_id)	Palo Alto Networks のファイアウォール上の仮想システムの一意な識別子。
高精度タイムスタンプ (high_res timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 この新規フィールドの形式は YYYY-MM-DDThh:ss:sssTZD です: • **YYYY**—西暦 • **MM**—2桁表記の月数 • **DD**—月の2桁の日 (01 ～ 31) • **T**—タイムスタンプの開始のインジケータ • **hh**—24時間を使用した2桁の時間数 (00 ～ 23) • **mm**—2桁表記の分 (00 ～ 59) • **ss**—2桁表記の秒 (00 ～ 60) • **sss**—ミリ秒単位で1桁以上の桁数 • **TZD**—タイムゾーン指定子 (+hh:mm or -hh:mm) 高解像度タイムスタンプは、*PAN-OS 10.2* リリース以降で動作するマネージド ファイアウォールから受信したログに対応します。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*`1969-12-31T16:00:00:000-8:00`* というタイムスタンプを表示します。

User-ID ログの各フィールド

フォーマット：FUTURE_USER, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Virtual System, Source IP, User, Data Source Name, Event ID, Repeat Count, Time Out Threshold, Source Port, Destination Port, Data Source, Data Source Type, Sequence Number, Action Flags, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Virtual System ID, Factor Type, Factor Completion Time, Factor Number, FUTURE_USE, FUTURE_USE, User Group Flags, User by Source, High Resolution Timestamp

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号 (serial)	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は USERID です。
脅威/コンテンツ タイプ (subtype)	User-ID ログのサブタイプ。 値は、login、logout、register-tag、および unregister-tag です。 • login—ユーザーがログインしました。 • login—ユーザーがログアウトしました。 • register-tag—タグがユーザーに登録されたことを示します。 • unregister-tag—タグがユーザーに対して登録解除されたことを示します。
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
仮想システム (vsys)	設定ログに関連付けられている仮想システム。
ソース IP (ip)	元のセッション送信元 IP アドレス。
ユーザー (user)	エンドユーザを識別します。
データソース名 (datasourcename)	IP（ポート）対ユーザーのマッピングを送信する User-ID 送信元。
イベント ID (eventid)	イベントの名前を示す文字列。
リピートカウント（repeatcnt）	5 秒以内に開始された、送信元 IP、宛先 IP、アプリケーション、サブタイプが同じになっているセッションの数です。
タイムアウトのしきい値（timeout）	IP/ユーザーマッピングがクリアされるまでのタイムアウト。
送信元ポート（beginport）	セッションで使用された送信元ポート。
宛先ポート（endport）	セッションで使用された宛先ポート。

フィールド名	説明
データソース タイプ (datasource)	マッピング情報の収集元になるソース。
データソース タイプ (datasourcetype)	データソース内の IP/ユーザーマッピングを識別するために使用するメカニズム。
シーケンス番号 （seqno）	ログを生成したファイアウォールのシリアル番号。
アクション フラグ （actionflags）	ログが Panorama に転送されたかどうかを示すビット フィールド。
デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。 API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名 （vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。
デバイス名 （device_name）	セッションがログに記録されたファイアウォールのホスト名。
仮想システム ID (vsys_id)	Palo Alto Networks のファイアウォール上の仮想システムの一意な識別子。
ファクター タイプ (factortype)	マルチ ファクター認証の際にユーザーを認証するために使用するベンダー。
ファクター完了時間 (factorcompletiontime)	認証が完了した時間。
ファクター番号 (factorno)	第一認証（1）と追加の要素（2）のうちどちらなのかを示します。

フィールド名	説明
ユーザーグループフラッグ (ugflags)	ユーザーグループマッピング中に見つかったユーザーグループかどうかを表示します。サポートされている値は次のとおりです。 • 見つかったユーザグループ – ユーザをグループにマッピングできるかどうかを示します。 • 重複ユーザー – 重複ユーザーがユーザーグループで見つかったかどうかを示します。ユーザグループが見つからない場合は N/A を表示します。
ソース別ユーザー (userbysource)	IP アドレス-ユーザー名間のマッピングを介して送信元から受信したユーザー名を示します。
高解像度タイムスタンプ (high_res timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 この新規フィールドの形式は YYYY-MM-DDThh:ss:sssTZD です: • **YYYY**–西暦 • **MM**–2桁表記の月数 • **DD**–月の2桁の日 (01 ～ 31) • **T**–タイムスタンプの開始のインジケータ • **hh**–24時間を使用した2桁の時間数 (00 ～ 23) • **mm**–2桁表記の分 (00 ～ 59) • **ss**–2桁表記の秒 (00 ～ 60) • **sss**–ミリ秒単位で1桁以上の桁数 • **TZD**–タイムゾーン指定子 (+hh:mm or -hh:mm) 高解像度タイムスタンプは、*PAN-OS 10.2* 以降のリリースを実行している管理ファイアウォールから受信したログでサポートされています。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*1969-12-31T16:00:00:000-8:00* というタイムスタンプを表示します。

復号化ログのフィールド

フォーマット:FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, Config Version, Generate Time, Source Address, Destination Address, NAT Source IP, NAT Destination IP, Rule, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, Time Logged, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, IP Protocol, Action, Tunnel,

FUTURE_USE, FUTURE_USE, Source VM UUID, Destination VM UUID, UUID for rule, Stage for Client to Firewall, Stage for Firewall to Server, TLS Version, Key Exchange Algorithm, Encryption Algorithm, Hash Algorithm, Policy Name, Elliptic Curve, Error Index, Root Status, Chain Status, Proxy Type, Certificate Serial Number, Fingerprint, Certificate Start Date, Certificate End Date, Certificate Version, Certificate Size, Common Name Length, Issuer Common Name Length, Root Common Name Length, SNI Length, Certificate Flags, Subject Common Name, Issuer Subject Common Name, Root Subject Common Name, Server Name Indication, Error, Container ID, POD Namespace, POD Name, Source External Dynamic List, Destination External Dynamic List, Source Dynamic Address Group, Destination Dynamic Address Group, High Res Timestamp, Source Device Category, Source Device Profile, Source Device Model, Source Device Vendor, Source Device OS Family, Source Device OS Version, Source Hostname, Source Mac Address, Destination Device Category, Destination Device Profile, Destination Device Model, Destination Device Vendor, Destination Device OS Family, Destination Device OS Version, Destination Hostname, Destination Mac Address, Sequence Number, Action Flags

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号 (serial)	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は DECRYPTION です。
脅威/コンテンツ タイプ (サブタイプ)	復号化ログでは使用されない。
設定バージョン (config_ver)	ソフトウェア バージョン。
生成日時（time_generated）	データプレーンでログが生成された日時。
送信元アドレス (src)	元のセッション送信元 IP アドレス。
宛先アドレス (dst)	元のセッション宛先 IP アドレス。
NAT ソース IP (natsrc)	送信元 NAT を行った場合は、NAT 後の送信元 IP アドレス。
NAT 宛先 IP (natdst)	宛先 NAT を行った場合は、NAT 後の宛先 IP アドレス。
ルール(rule)	セッション トラフィックを制御するセキュリティ ポリシー ルール。

フィールド名	説明
送信元ユーザー (srcuser)	セッションを開始したユーザーのユーザー名。
宛先ユーザー (dstuser)	セッションの宛先となったユーザーのユーザー名。
アプリケーション (app)	セッションに関連付けられたアプリケーション。
仮想システム (vsys)	セッションに関連付けられている仮想システム。
送信元ゾーン (from)	セッションの送信元だったゾーン。
宛先ゾーン (to)	セッションの宛先だったゾーン。
インバウンド インターフェイス (inbound_if)	セッションの送信元となったインターフェイス。
アウトバウンド インターフェイス (outbound_if)	セッションの宛先だったインターフェイス。
ログ アクション (logset)	セッションに適用されたログ転送プロファイル。
ログ時間 (time_received)	ログが受信された時刻。
セッション ID (sessionid)	各セッションに適用される内部の数値識別子。
リピートカウント（repeatcnt）	5 秒以内に開始された、送信元 IP、宛先 IP、アプリケーション、コンテンツ/脅威タイプが同じになっているセッションの数。
送信元ポート（sport）	セッションで使用された送信元ポート。
宛先ポート（dport）	セッションで使用された宛先ポート。
NAT ソース ポート（natsport）	NAT 後の送信元ポート。
NAT 宛先ポート（natdport）	NAT 後の宛先ポート。

フィールド名	説明
フラッグ（flags）	セッションに関する詳細を示す 32 ビット フィールド。このフィールドは、以下のように、その値とログに記録されている値を AND 演算することによってデコードできます。 • 0X80000000—セッションにパケット キャプチャがあります（PCAP） • 0x40000000—クライアントが複数のパスを使用して宛先ホストに接続できるようにするオプションが有効です • 0x20000000—判定を行うためにファイルが WildFire に送信されます • 0x10000000—エンドユーザーによるエンタープライズ認証情報の送信を検出 • 0x08000000— 対象のフローの送信元が許可リストに記載されており、偵察行為防止の対象になっていません • 0x02000000—IPv6 セッション • 0x01000000—SSL セッションが復号化されます（SSL プロキシ） • 0x00800000—セッションが URL フィルタリングによって拒否されます • 0x00400000—セッションで NAT 変換が実行されました • 0x00200000—セッションのユーザー情報が認証ポータルを通じて取得されました • 0x00100000—標準的でない宛先ポート上にアプリケーション トラフィックがあります • 0x00080000 — プロキシからの X-Forwarded-For 値は送信元ユーザー フィールドにあります • 0x00040000—ログは http プロキシ セッション内のトランザクションに対応します（プロキシ トランザクション） • 0x00020000—クライアントからサーバーへのフローがポリシー ベース フォワーディングの対象になっています • 0x00010000—サーバーからクライアントへのフローがポリシー ベース フォワーディングの対象になっています • 0x00008000—セッションはコンテナ ページ アクセスです（コンテナ ページ） • 0x00002000—セッションに、暗黙的なアプリケーションの依存関係処理のルールでの一時的な一致があります。PAN-OS 5.0.0 以降で使用できます。 • 0x00000800 — このセッションのトラフィックを転送するために対称リターンが使用されます

フィールド名	説明
	• 0x00000400–復号化されたトラフィックがミラーポートを介してクリアテキストを送信しています • 0x00000100–外側のトンネルのペイロードを検査中です
IP プロトコル（proto）	セッションに関連付けられた IP プロトコル。
アクション（action）	セッションで実行されたアクション。値は以下のいずれかです。 • allow –セッションはポリシーによって許可されました • deny – セッションはポリシーによって拒否されました • drop – セッションはサイレントにドロップされました • drop ICMP – セッションはサイレントにドロップされ、ホストまたはアプリケーションに ICMP 到達不能メッセージが表示されました • reset both – セッションは終了し、TCP リセットが接続の両端に送信されました • reset client – セッションは終了し、TCP リセットがクライアントに送信されました • reset server – セッションは終了し、TCP リセットがサーバーに送信されました
Tunnel (トンネル)	トンネルのタイプ。
送信元 VM UUID（src_uuid）	VMware NSX 環境のゲストVirtual Machine (仮想マシン - VM)の送信元 UUID（Universally Unique Identifier）。
宛先 VM UUID（dst_uuid）	VMware NSX 環境のゲストVirtual Machine (仮想マシン - VM)の宛先 UUID（Universally Unique Identifier）。
ルールの UUID（rule_uuid）	規則を恒久的に識別するUUID です。
クライアントからファイアウォールのステージ (hs_stage_c2f)	クライアントからファイアウォールへの TLS ハンドシェークの段階。たとえば、Client Hello、Server Hello、証明書、クライアント/サーバー鍵交換など。
ファイアウォールからサーバーのステージ (hs_stage_f2s)	ファイアウォールからサーバーへの TLS ハンドシェークの段階。

フィールド名	説明
TLS バージョン (tls_version)	セッションに使用される TLS プロトコルのバージョン。
鍵交換アルゴリズム (tls_keyxchg)	セッションに使用される鍵交換アルゴリズム。
暗号アルゴリズム (tls_enc)	AES-128-CBC、AES-256-GCM、等のセッション データの暗号化に使用されるアルゴリズム。
ハッシュ アルゴリズム (tls_auth)	SHA, SHA256、SHA384 等のセッションに使用される認証アルゴリズム。
ポリシー名 (policy_name)	セッションに関連する復号ポリシーの名前。
楕円曲線 (ec_curve)	クライアントとサーバーがネゴシエートし、ECDHE 暗号スイートを使用する接続に使用する楕円暗号曲線。
エラー インデックス (err_index)	発生したエラーのタイプ:暗号、リソース、再開、バージョン、プロトコル、証明書、機能、または HSM。
ルート ステータス (root_status)	ルート 証明書のステータス (信頼されている、信頼されていない、未検査など)。
チェーン ステータス (chain_status)	チェーンが信頼されているかどうか。値を以下に示します。 • 未検査 • 信頼されていない • 信頼されている • 不完全
プロキシタイプ (proxy_type)	転送プロキシの転送、インバウンド検査の着信、復号化されていないトラフィックの復号化なし、GlobalProtect などの復号化プロキシの種類。
証明書シリアルナンバー (cert_serial)	証明書の一意の識別子 (証明書発行者により生成)。
証明書フィンガープリント (fingerprint)	x509 バイナリ形式の証明書のハッシュ。
証明書開始日 (notbefore)	証明書が有効になった時刻 (この時間より前には無効な証明書)。

フィールド名	説明
証明書終了日 (notafter)	証明書の有効期限が切れる時間 (この時間を過ぎると証明書は無効になります)。
証明書のバージョン (cert_ver)	証明書のバージョン (V1、V2、または V3)。
証明書のサイズ (cert_size)	証明書の鍵のサイズ。
Common Name (共通名 - CN)の長さ (cn_len)	サブジェクトのCommon Name (共通名 - CN)の長さ。
発行者のCommon Name (共通名 - CN)の長さ (issuer_len)	発行者のCommon Name (共通名 - CN)の長さ。
ルートのCommon Name (共通名 - CN) の長さ (rootcn_len)	ルートのCommon Name (共通名 - CN)の長さ。
SNI の長さ (sni_len)	サーバー名表示の長さ (hostname)。
証明書フラグ (cert_flags)	証明書フラグは7つの値を返すことができます: • セッション再開 (b_resume_session) • 証明書 (サブジェクト) のCommon Name (共通名 - CN)切り捨て (b_cert_cn_truncated) • 発行者のCommon Name (共通名 - CN)切り捨て (b_issuer_cn_truncated) • ルートのCommon Name (共通名 - CN) 切り捨て (b_root_cn_truncated) • サーバー名表示 (SNI) 切り捨て (b_sni_truncated) • 証明書の種類、RSA または ECDSA (b_cert_type) • 未使用 (padding3)
サブジェクトの Common Name (共通名 - CN) (cn)	ドメイン名 (証明書が保護するサーバーの名前)。

フィールド名	説明
発行者の Common Name (共通名 - CN) (issuer_cn)	証明書の内容を検証した組織の名前。
ルートの Common Name (共通名 - CN) (root_cn)	ルート Certificate Authority (認証局 - CA) の名前。
Server Name Indication (sni)	クライアントが接続しようとしているサーバーのホスト名。SNI を使用すると、サーバーは複数の Web サイトをホストし、各 Web サイトに一意の SNI があるため、同じ IPアドレスと TCP ポートで複数の証明書を提示できます。
エラー (error)	該当のイベントで発生したエラーを示す文字列。
コンテナ ID (container_id)	ファイアウォールがクラウド コンテナで実行されている場合にコンテナを識別する一意の英数字の文字列。
POD 名前空間 (pod_namespace)	Kubernetes ポッド名前空間の名前。
POD 名 (pod_name)	Kubernetes ポッドの名前。
送信元の外部ダイナミックリスト (src_edl)	トラフィックの送信元 IP アドレスを含む外部ダイナミックリストの名前。
宛先の外部ダイナミック リスト (dst_edl)	トラフィックの宛先 IPアドレスを含む外部動的リストの名前。
送信元のDynamic Address Group (ダイナミック アドレス グループ) (src_dag)	Device-ID がトラフィックの送信元として識別する Dynamic Address Group (ダイナミック アドレス グループ)。
宛先の Dynamic Address Group (ダイナミック アドレス グループ) (dst_dag)	Device-ID がトラフィックの宛先として識別する Dynamic Address Group (ダイナミック アドレス グループ)。
高解像度タイムスタンプ (high_res_timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 このフィールドの形式は YYYY-MM-DDThh:ss:sssTZD です:

フィールド名	説明
	• **YYYY**—西暦 • **MM**—2桁表記の月数 • **DD**—月の2桁の日 (01 ～ 31) • **T**—タイムスタンプの開始のインジケータ • **hh**—24時間を使用した2桁の時間数 (00 ～ 23) • **mm**—2桁表記の分 (00 ～ 59) • **ss**—2桁表記の秒 (00 ～ 60) • **sss**—ミリ秒単位で1桁以上の桁数 • **TZD**—タイムゾーン指定子 (+hh:mm or -hh:mm) 高解像度タイムスタンプは、*PAN-OS 10.2* 以降のリリースを実行しているマネージド *firewalls* から受信したログでサポートされています。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*`1969-12-31T16:00:00:000-8:00`* というタイムスタンプを表示します。
送信元 デバイスのカテゴリ (src_category)	Device-ID がトラフィックの送信元として識別するデバイスのカテゴリ。
送信元のデバイスのプロファイル (src_profile)	Device-ID がトラフィックの送信元として識別するデバイスのデバイスのプロファイル。
送信元のデバイス モデル (src_model)	Device-ID がトラフィックの送信元として識別するデバイスのモデル。
送信元のデバイス ベンダー (src_vendor)	Device-ID がトラフィックの送信元として識別するデバイスのベンダー。
送信元デバイス OS ファミリ (src_osfamily)	Device-ID がトラフィックの送信元として識別するデバイスのオペレーティングシステムの種類。
送信元デバイス OS バージョン (src_osversion)	Device-ID がトラフィックの送信元として識別するデバイスのオペレーティングシステムのバージョン。
送信元ホスト名 (src_host)	Device-ID がトラフィックの送信元として識別するデバイスのホスト名。

フィールド名	説明
送信元 MAC アドレス (src_mac)	Device-ID がトラフィックの送信元として識別するデバイスの MAC アドレス。
宛先デバイスのカテゴリ (dst_category)	Device-ID がトラフィックの宛先として識別するデバイスのカテゴリ。
宛先デバイスのプロファイル (dst_profile)	Device-ID がトラフィックの宛先として識別するデバイスのデバイス プロファイル。
宛先デバイスのモデル (dst_model)	Device-ID がトラフィックの宛先として識別するデバイスのモデル。
宛先デバイスのベンダー (dst_vendor)	Device-ID がトラフィックの宛先として識別するデバイスのベンダー。
宛先 デバイス OS ファミリ (dst_osfamily)	Device-ID がトラフィックの宛先として識別するデバイスのオペレーティングシステムの種類。
宛先デバイス OS バージョン (dst_osversion)	Device-ID がトラフィックの宛先として識別するデバイスのオペレーティングシステムのバージョン。
宛先ホスト名 (dst_host)	Device-ID がトラフィックの宛先として識別するデバイスのホスト名。
宛先 MAC アドレス (dst_mac)	Device-ID がトラフィックの宛先として識別するデバイスの MAC アドレス。
シーケンス番号（seqno）	順次増分される 64bit (ビット- bit) のログ エントリ識別子。各ログ タイプには、一意の番号空間があります。
アクション フラグ（actionflags）	ログが Panorama に転送されたかどうかを示すビット フィールド。
デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値

フィールド名	説明
	12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。 API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
仮想システム ID (vsys_id)	Palo Alto Networks のファイアウォール上の仮想システムの一意な識別子。
アプリケーション サブカテゴリ (subcategory_of_app)	アプリケーション構成プロパティで指定されたアプリケーション サブカテゴリ。
アプリケーションカテゴリ (category_of_app)	アプリケーション構成プロパティで指定されたアプリケーション カテゴリ。値を以下に示します。 • business-system • コラボレーション • 一般インターネット • メディア • networking • SaaS
アプリケーションテクノロジー (technology_of_app)	アプリケーション構成プロパティで指定されたアプリケーション テクノロジ。値を以下に示します。 • ブラウザベース • クライアント/サーバー • ネットワークプロトコル • ピアツーピア
アプリケーションリスク (risk_of_app)	アプリケーションに関連付けられたリスク レベル (1 =最低から 5=最高)。

フィールド名	説明
アプリケーション特性 (characteristic_of_app)	アプリケーションの適用可能特性のコンマ区切りリスト
アプリケーション コンテナ (container_of_app)	アプリケーションの親アプリケーション。
アプリケーション SaaS (is_saas_of_app)	SaaS アプリケーションの場合は 1、SaaS アプリケーションでない場合は 0 を表示します。
アプリケーション認可状態 (sanctioned_state_of_app)	アプリケーションが認可されている場合は 1 、認可されていない場合は 0 を表示します。

トンネル検査ログの各フィールド

フォーマット：FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, Generated Time, Source Address, Destination Address, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, Protocol, Action, Severity, Sequence Number, Action Flags, Source Location, Destination Location, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Tunnel ID/IMSI, Monitor Tag/IMEI, Parent Session ID, Parent Start Time, Tunnel, Bytes, Bytes Sent, Bytes Received, Packets, Packets Sent, Packets Received, Maximum Encapsulation, Unknown Protocol, Strict Check, Tunnel Fragment, Sessions Created, Sessions Closed, Session End Reason, Action Source, Start Time, Elapsed Time, Tunnel Inspection Rule, Remote User IP, Remote User ID, Rule UUID, PCAP ID, Dynamic User Group, Source External Dynamic List, Destination External Dynamic List, High Resolution Timestamp

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された月、日、時間。
シリアル番号 (serial)	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	セッションに関係するログのタイプ。開始あるいは終了。
脅威/コンテンツ タイプ (subtype)	トラフィック ログのサブタイプ。値は、「start」、「end」、「drop」、「deny」です

フィールド名	説明
	• start – セッションが開始しました • end – セッションが終了しました • drop – アプリケーションが特定される前にセッションが廃棄され、そのセッションを許可するルールがありません。 • deny – アプリケーションが特定された後にセッションが廃棄され、そのセッションをブロックするルールがあるか、セッションを許可するルールがありません。
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
送信元アドレス (src)	セッション中のパケットの送信元 IP アドレス
宛先アドレス (dst)	セッション中のパケットの宛先 IP アドレス
NAT ソース IP (natsrc)	送信元 NAT を行った場合は、NAT 後の送信元 IP アドレス。
NAT 宛先 IP (natdst)	宛先 NAT を行った場合は、NAT 後の宛先 IP アドレス。
ルール名（rule）	セッションで有効なセキュリティポリシー ルールの名前
送信元ユーザー (srcuser)	セッション中のパケットの送信元 User-ID
宛先ユーザー (dstuser)	セッション中のパケットの宛先 User-ID
アプリケーション (app)	セッションで使用されているトンネル プロトコル
仮想システム (vsys)	セッションに関連付けられている仮想システム。
送信元ゾーン (from)	セッション中のパケットの送信元ゾーン
宛先ゾーン (to)	セッション中のパケットの宛先ゾーン
インバウンド インターフェイス (inbound_if)	セッションの送信元となったインターフェイス。

フィールド名	説明
アウトバウンド インターフェイス (outbound_if)	セッションの宛先だったインターフェイス。
ログ アクション (logset)	セッションに適用されたログ転送プロファイル。
セッション ID (sessionid)	ロギング中のセッションのセッション ID
リピートカウント（repeatcnt）	5 秒以内に開始された、送信元 IP、宛先 IP、アプリケーション、サブタイプが同じになっているセッションの数です。
送信元ポート（sport）	セッションで使用された送信元ポート。
宛先ポート（dport）	セッションで使用された宛先ポート。
NAT ソース ポート（natsport）	NAT 後の送信元ポート。
NAT 宛先ポート（natdport）	NAT 後の宛先ポート。
フラッグ（flags）	セッションに関する詳細を示す 32 ビット フィールド。このフィールドは、以下のように、その値とログに記録されている値を AND 演算することによってデコードできます。 • 0x80000000 – セッションにパケット キャプチャがあります（PCAP） • 0x02000000 – IPv6 セッション • 0x01000000 – SSL セッションが復号化された（SSL プロキシ） • 0x00800000 – セッションが URL フィルタリングによって拒否されました • 0x00400000 – セッションで NAT 変換が実行されました（NAT） • 0x00200000 –セッションのユーザー情報が認証ポータルを通じてキャプチャされました • 0x00080000 – プロキシからの X-Forwarded-For 値は送信元ユーザー フィールドにあります • 0x00040000 – ログは http プロキシ セッション内のトランザクションに対応します（プロキシ トランザクション）

フィールド名	説明
	• 0x00008000 – セッションはコンテナ ページ アクセスです（コンテナ ページ） • 0x00002000 – セッションに、暗黙的なアプリケーションの依存関係処理のルールでの一時的な一致があります。PAN-OS 5.0.0 以降で使用できます。 • 0x00000800 – このセッションのトラフィックを転送するために対称リターンが使用されました
IP プロトコル（proto）	セッションに関連付けられた IP プロトコル。
アクション（action）	セッションで実行されたアクション。値は以下のいずれかです。 • allow – セッションはポリシーによって許可されました • deny – セッションはポリシーによって拒否されました • drop – セッションはサイレントにドロップされました • drop ICMP – セッションはサイレントにドロップされ、ホストまたはアプリケーションに ICMP 到達不能メッセージが表示されました • reset both – セッションは終了し、TCP リセットが接続の両端に送信されました • reset client – セッションは終了し、TCP リセットがクライアントに送信されました • reset server – セッションは終了し、TCP リセットがサーバーに送信されました
重大度 (severity)	イベントに関連付けられた重大度。値は、「informational」、「low」、「medium」、「high」、「critical」です。
シーケンス番号（seqno）	64 ビットのログ エントリ識別子。各ログ タイプには、一意の番号空間があります。このフィールドは、PA-7000 シリーズ ファイアウォールではサポートされていません。
アクション フラグ（actionflags）	ログが Panorama に転送されたかどうかを示すビット フィールド。
送信国 (srcloc)	プライベート アドレスの送信元の国または内部領域。最大長は 32 バイトです。
宛先国 (dstloc)	プライベート アドレスの宛先の国または国内地域。最大長は 32 バイトです。

フィールド名	説明
デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。 API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
トンネル ID (tunnelid)	検査されているトンネルの ID あるいはモバイル ユーザーの Mobile Subscriber Identity (IMSI) ID。
モニター タグ (monitortag)	トンネル検査ポリシー ルール用に設定したモニター名あるいはモバイル ユーザーの International Mobile Equipment Identity (IMEI) ID。
親セッション ID（parent_session_id）	内部でこのセッションをトンネル化するトンネルの ID。内側のトンネル（2 レベルのトンネリングの場合）あるいは内部コンテンツ（1 レベルのトンネリングの場合）のみに適用されます。
親開始時間（parent_start_time）	親トンネルのセッションが始まった年/月/日 時間:分:秒。
トンネル タイプ（tunnel）	GRE や IPSec などの、トンネルの種類。
バイト (bytes)	セッション内のバイト数。
送信済バイト (bytes_sent)	セッションのクライアントからサーバー方向へのバイト数。

フィールド名	説明
受信済バイト (bytes_received)	セッションのサーバーからクライアント方向へのバイト数。
パケット (packets)	セッションの合計パケット数 (送受信)。
送信されたパケット (pkts_sent)	セッションのクライアントからサーバーへのパケット数。
受信したパケット (pkts_received)	セッションのサーバーからクライアントへのパケット数。
最大カプセル化 (max_encap)	トンネル検査ポリシー ルール（最大トンネル検査レベルを超過するとパケットをドロップ）で設定されたカプセル化の最大レベル数をパケットが超過したためにファイアウォールがドロップしたパケット数。
未知のプロトコル (unknown_proto)	トンネル検査ポリシー ルール（トンネル内に未知のプロトコルがあればパケットをドロップ）で有効化された通り、パケットが未知のプロトコルを含むためにファイアウォールがドロップしたパケット数。
厳密なチェック (strict_check)	トンネル検査ポリシー ルールで有効化された通り、パケット内のトンネル プロトコル ヘッダがトンネル プロトコルのための RFC に準拠しないためにファイアウォールがドロップしたパケット数（**Drop packet if tunnel protocol fails strict header check**（トンネル プロトコルが厳密なヘッダーチェックに失敗したらパケットをドロップ））。
トンネルのフラグメント (tunnel_fragment)	フラグメンテーション エラーのためにファイアウォールがドロップしたパケット数。
作成されたセッション数 (sessions_created)	作成された内部セッションの数。
クローズされたセッション数 (sessions_closed)	作成されて完了/クローズされたセッション数。
セッション終了理由 (session_end_reason)	セッションが終了した理由。複数の原因で終了した場合、このフィールドには優先度が最も高い理由のみが表示されます。有効なセッション終了理由の値は、優先度の高い順に以下のとおりです。 • threat — ファイアウォールが、リセット、ドロップ、またはブロック（IP アドレス）アクションに関連付けられた脅威を検出しました。

フィールド名	説明
	• policy-deny — セッションが、拒否またはドロップ アクションが指定されたセキュリティ ルールと一致しました。 • decrypt-cert-validation—失効、信用されていない発行者、未知の状態、状態検証タイムアウトなどの状況によりセッションがクライアント認証を実施またはセッションがサーバー証明書を実施する時に、SSL 送信プロキシ複合 または SSL インバウンド インスペクションをブロックするようにファイアウォールを設定したのでセッションが終了しました。サーバー証明書が type bad_certificate、unsupported_certificate、certificate_revoked、access_denied、または no_certificate_RESERVED (SSLv3 のみ)の致命的エラーアラートを生成する時にもこのセッションの終了理由が表示されます。 • decrypt-unsupport-param—セッションがサポートしていないプロトコルバージョン、暗号鍵またはSSHアルゴリズムを使用している場合、SSL送信プロキシ複合またはSSLインバウンドインスペクションをブロックするようにファイアウォールを設定したのでセッションは終了しました。unsupported_extension、unexpected_message、または handshake_failureのタイプの致命的エラーアラートをセッションが発生すると、このセッション終了理由が表示されます。 • decrypt-error——ファイアウォールリソースまたは ハードウェアセキュリティモジュール (HSM) が利用できない時に、 SSL送信プロキシ複合またはSSLインバウンドインスペクションをブロックするようにファイアウォールを設定したのでセッションは終了しました。SSHエラーを有したり、decrypt-cert-validation and decrypt-unsupport-param 終了理由にリストアップされている以外の致命的エラーアラートを発生したSSLトラフィックをブロックするようにファイアウォールを設定した場合も、このセッション終了理由が表示されます。 • tcp-rst-from-client — クライアントが TCP リセットをサーバーに送信しました。 • tcp-rst-from-server — サーバーが TCP リセットをクライアントに送信しました。 • resources-unavailable — システム リソース制限が原因でセッションがドロップしました。たとえば、セッションの順序外パケット数が、フローまたはグローバル順序外パケット キューごとに許容される数を超えた場合などが考えられます。 • tcp-fin — 接続の一方または両方のホストが TCP FIN メッセージを送信してセッションを閉じました。 • tcp-reuse — セッションが再利用され、ファイアウォールが前のセッションを閉じました。

フィールド名	説明

	• decoder — デコーダがプロトコル内で新しい接続を検出し（HTTP-Proxy など）、前の接続を終了しました。
	• aged-out — セッションがエージアウトしました。
	• unknown — この値は、以下の状況に適用されます。
	  • 上記の理由が適用されないセッションの終了（たとえば、`clear session all` コマンド）。
	  • セッション終了理由フィールドをサポートしない PAN-OS リリース（PAN-OS 6.1 より前のリリース）で生成されたログの場合、最新の PAN-OS リリースへのアップグレード後、またはログがファイアウォールにロードされると、値は **unknown** になります。
	  • Panorama では、セッション終了理由をサポートしない PAN-OS バージョンのファイアウォールから受信したログの値は、**unknown** になります。
	• n/a — この値は、トラフィック ログのタイプが **end** 以外の場合に適用されます。

アクションの送信元（action_source）	アプリケーションを許可またはブロックするために実行されたアクションがアプリケーションまたはポリシーに定義されていたかどうかを示します。アクションは、セッションに対する「allow」、「deny」、「drop」、「reset- server」、「reset-client」、「reset-both」のいずれかになります。
開始時間（start）	セッションが始まった年/月/日 時間:分:秒。
経過時間 (elapsed)	セッションの経過時間。
トンネル検査ルール (tunnel_insp_rule)	クリアテキスト トンネル トラフィックに一致するトンネル検査ルールの名前。
リモートユーザー IP (remote_user_ip)	リモートユーザーの IPv4 あるいは IPv6 アドレス。
リモートユーザー ID (remote_user_id)	リモートユーザーの IMSI 識別子。利用できる場合、単一の IMEI 識別子または単一の MSISDN 識別子。
セキュリティ ルール UUID (rule_uuid)	規則を恒久的に識別するUUID です。
PCAP ID （pcap_id）	ファイアウォール上の pcap ファイルの場所を定義する一意のpacket capture (パケット キャプチャ - pcap) ID。

フィールド名	説明
ダイナミック ユーザー グループ名 (dynusergroup_name)	セッションを開始したユーザーを含むダイナミック ユーザー グループの名前。
送信元の外部ダイナミックリスト (src_edl)	トラフィックの送信元 IP アドレスを含む外部ダイナミックリストの名前。
宛先の外部ダイナミック リスト (dst_edl)	トラフィックの宛先 IP アドレスを含む外部動的リストの名前。
高解像度タイムスタンプ (high_res timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 この新規フィールドの形式は YYYY-MM-DDThh:ss:sssTZD です: • **YYYY**—西暦 • **MM**—2桁表記の月数 • **DD**—月の2桁の日 (01 ～ 31) • **T**—タイムスタンプの開始のインジケータ • **hh**—24時間を使用した2桁の時間数 (00 ～ 23) • **mm**—2桁表記の分 (00 ～ 59) • **ss**—2桁表記の秒 (00 ～ 60) • **sss**—ミリ秒単位で1桁以上の桁数 • **TZD**—タイムゾーン指定子 (+hh:mm or -hh:mm) 高解像度タイムスタンプは、*PAN-OS 10.2* 以降のリリースを実行しているマネージド *firewalls* から受信したログでサポートされています。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*`1969-12-31T16:00:00:000-8:00`* というタイムスタンプを表示します。
スライス差別化 (nssai_sd)	ネットワーク スライス ID の A スライス差別化要素。
スライスサービスタイプ (nssai_sd)	ネットワーク スライス ID の A スライス サービス タイプ。

フィールド名	説明
PDU セッション ID (pdu_session_id)	トンネル内の L4 セグメントのコレクションのセッション ID。
アプリケーション サブカテゴリ (subcategory_of_app)	アプリケーション構成プロパティで指定されたアプリケーション サブカテゴリ。
アプリケーションカテゴリ (category_of_app)	アプリケーション構成プロパティで指定されたアプリケーション カテゴリ。値を以下に示します。 • business-system • コラボレーション • 一般インターネット • メディア • networking • SaaS
アプリケーションテクノロジー (technology_of_app)	アプリケーション構成プロパティで指定されたアプリケーション テクノロジ。値を以下に示します。 • ブラウザベース • クライアント/サーバー • ネットワークプロトコル • ピアツーピア
アプリケーションリスク (risk_of_app)	アプリケーションに関連付けられたリスク レベル (1 =最低から 5=最高)。
アプリケーション特性 (characteristic_of_app)	アプリケーションの適用可能特性のコンマ区切りリスト
アプリケーション コンテナ (container_of_app)	アプリケーションの親アプリケーション。
アプリケーション SaaS (is_saas_of_app)	SaaS アプリケーションの場合は 1、SaaS アプリケーションでない場合は 0 を表示します。
アプリケーション認可状態 (sanctioned_state_of_app)	アプリケーションが認可されている場合は 1 、認可されていない場合は 0 を表示します。

SCTP ログの各フィールド

フォーマット：FUTURE_USE, Receive Time, Serial Number, Type, FUTURE_USE, FUTURE_USE, Generated Time, Source Address, Destination Address, FUTURE_USE, FUTURE_USE, Rule Name, FUTURE_USE, FUTURE_USE, FUTURE_USE, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Action, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, FUTURE_USE, FUTURE_USE, FUTURE_USE, FUTURE_USE, IP Protocol, Action, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Sequence Number, FUTURE_USE, SCTP Association ID, Payload Protocol ID, Severity, SCTP Chunk Type, FUTURE_USE, SCTP Verification Tag 1, SCTP Verification Tag 2, SCTP Cause Code, Diameter App ID, Diameter Command Code, Diameter AVP Code, SCTP Stream ID, SCTP Association End Reason, Op Code, SCCP Calling Party SSN, SCCP Calling Party Global Title, SCTP Filter, SCTP Chunks, SCTP Chunks Sent, SCTP Chunks Received, Packets, Packets Sent, Packets Received, UUID for rule, High Resolution Timestamp

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号 (serial)	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は SCTP です。
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
送信元アドレス (src)	元のセッション送信元 IP アドレス。
宛先アドレス (dst)	元のセッション宛先 IP アドレス。
ルール名（rule）	セッションで有効なセキュリティポリシー ルールの名前
仮想システム (vsys)	セッションに関連付けられている仮想システム。
送信元ゾーン (from)	セッションの送信元だったゾーン。
宛先ゾーン (to)	セッションの宛先だったゾーン。
インバウンド インターフェイス (inbound_if)	セッションの送信元となったインターフェイス。
アウトバウンド インターフェイス (outbound_if)	セッションの宛先だったインターフェイス。

フィールド名	説明
ログ アクション (logset)	セッションに適用されたログ転送プロファイル。
セッション ID (sessionid)	各セッションに適用される内部の数値識別子。
リピートカウント（repeatcnt）	5 秒以内に開始された、送信元 IP、宛先 IP、アプリケーション、サブタイプが同じになっているセッションの数です。
送信元ポート（sport）	セッションで使用された送信元ポート。
宛先ポート（dport）	セッションで使用された宛先ポート。
IP プロトコル（proto）	セッションに関連付けられた IP プロトコル。
アクション（action）	セッションで実行されたアクション。値は以下のいずれかです。 • allow — セッションはポリシーによって許可されました • deny — セッションはポリシーによって拒否されました
デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。 API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。

フィールド名	説明
シーケンス番号（seqno）	64 ビットのログ エントリ識別子。各ログ タイプには、一意の番号空間があります。
SCTP アソシエーション ID（assoc_id）	各 SCTP アソシエーションに適用される内部 56 ビット数値論理識別子。
ペイロード プロトコル ID (ppid)	このイベントをトリガしたデータ チャンク内のペイロード プロトコル ID（PPID）を識別します。PPID は Internet Assigned Numbers Authority（IANA）によって割り当てられます。
重大度 (severity)	イベントに関連付けられた重大度。値は、「informational」、「low」、「medium」、「high」、「critical」です。
SCTP チャンク タイプ (sctp_chunk_type)	コントロールやデータなど、チャンクに含まれる情報の種類を記述します。
SCTP イベント タイプ (sctp_event_type)	SCTP 保護プロファイルが SCTP トラフィックに適用されている場合に、SCTP チャンクまたはパケットごとにトリガーされるイベントを定義します。また、SCTP アソシエーションの開始または終了によってトリガされます。
SCTP 検証タグ 1 (verif_tag_1)	受信した SCTP パケットが現在の SCTP アソシエーションに属しているかどうかを検証し、endpoint2 を検証するためのアソシエーションを開始する endpoint1 によって使用されます。
SCTP 検証タグ2 (verif_tag2)	受信した SCTP パケットが現在の SCTP アソシエーションに属しているかどうかを検証し、endpoint1 を検証するための endpoint2 によって使用されます。
SCTP 原因コード (sctp_cause_code)	同じ SCTP アソシエーションの他のエンドポイントへのエラー条件の理由を指定するためにエンドポイントによって送信されます。
Diameter アプリ ID (diam_app_id)	イベントをトリガしたデータ チャンク内の Diameter アプリケーション。Diameter アプリケーション ID は Internet Assigned Numbers Authority（IANA）によって割り当てられます。
Diameter コマンド コード (diam_cmd_code)	イベントをトリガしたデータ チャンク内の Diameter コマンド コード。Diameter コマンド コード は Internet Assigned Numbers Authority（IANA）によって割り当てられます。

フィールド名	説明
Diameter AVP コード (diam_avp_code)	イベントをトリガしたデータ チャンク内の Diameter AVP コード。
SCTP ストリーム ID (stream_id)	イベントをトリガしたデータ チャンクを運ぶストリームの ID。
SCTP アソシエーション終了の理由 (assoc_end_reason)	アソシエーションが終了した理由。終了に複数の原因があった場合は、最も優先度の高い理由が表示されます。優先度の降順でセッションが終了する理由は、次のとおりです： • shutdown-from-endpoint （最高）–エンドポイント SHUTDOWN を送信します • abort-from-endpoint–エンドポントが ABORT を送信します • 不明（最下位）–関連が古くなった、または関連付けの終了理由が以前の理由の 1 つ（たとえば、セッションのすべてをクリアしている）でカバーされていません。
Op コード (op_code)	イベントをトリガしたデータ チャンク内 のMAP や CAP などのアプリケーション層 SS7 プロトコルのオペレーション コードを識別します。
SCCP 発呼側 SSN (sccp_calling_ssn)	イベントをトリガしたデータ チャンク内のシグナリング接続制御パート（SCCP）の発呼側サブシステム番号（SSN）。
SCCP 発呼側グローバル タイトル (sccp_calling_gt)	イベントをトリガしたデータ チャンク内のシグナリング接続制御パート（SCCP）のグローバル タイトル（GT）。
SCTP フィルタ（sctp_filter）	SCTP チャンクで一致したフィルタの名前。
SCTP チャンク (chunks)	アソシエーションの合計チャンク数（送受信）。
送信済み SCTP チャンク (chunks_sent)	アソシエーションの endpoint1（アソシエーションを開始する）-to-endpoint2 チャンク数。
受信済み SCTP チャンク (chunks_received)	アソシエーションの endpoint2-to-endpoint1 のチャンク数。
パケット (packets)	セッションの合計パケット数 (送受信)。
送信されたパケット（pkts_sent）	セッションのクライアントからサーバーへのパケット数。
受信したパケット（pkts_received）	セッションのサーバーからクライアントへのパケット数。

フィールド名	説明
ルールの UUID（rule_uuid）	規則を恒久的に識別するUUID です。
高解像度タイムスタンプ (high_res _timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 この新規フィールドの形式は YYYY-MM-DDThh:ss:sssTZD です: • **YYYY**—西暦 • **MM**—2桁表記の月数 • **DD**—月の2桁の日 (01 ～ 31) • **T**—タイムスタンプの開始のインジケータ • **hh**—24時間を使用した2桁の時間数 (00 ～ 23) • **mm**—2桁表記の分 (00 ～ 59) • **ss**—2桁表記の秒 (00 ～ 60) • **sss**—ミリ秒単位で1桁以上の桁数 • **TZD**—タイムゾーン指定子 (+hh:mm or -hh:mm) 高解像度タイムスタンプは、*PAN-OS 10.2* 以降のリリースを実行しているマネージド *firewalls* から受信したログでサポートされています。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*`1969-12-31T16:00:00:000-8:00`* というタイムスタンプを表示します。

認証ログの各フィールド

フォーマット:FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Virtual System, Source IP, User, Normalize User, Object, Authentication Policy, Repeat Count, Authentication ID, Vendor, Log Action, Server Profile, Description, Client Type, Event Type, Factor Number, Sequence Number, Action Flags, Device Group Hierarchy 1, Device Group Hierarchy 2, Device Group Hierarchy 3, Device Group Hierarchy 4, Virtual System Name, Device Name, Virtual System ID, Authentication Protocol, UUID for rule, High Resolution Timestamp, Source Device Category, Source Device Profile, Source Device Model, Source Device Vendor, Source Device OS Family, Source Device OS Version, Source Hostname, Source Mac Address

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号 (serial)	ログを生成したデバイスのシリアル番号。
タイプ（type）	ログのタイプを指定します。 値はAUTHENTICATIONです。
脅威/コンテンツ タイプ (subtype)	システム ログのサブタイプ。ログを生成するシステム デーモンを参照します。値は、「crypto」、「dhcp」、「dnsproxy」、「dos」、「general」、「global-protect」、「ha」、「hw」、「nat」、「ntpd」、「pbf」、「port」、「pppoe」、「ras」、「routing」、「satd」、「sslmgr」、「sslvpn」、「userid」、「url-filtering」、「vpn」です。
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
仮想システム (vsys)	セッションに関連付けられている仮想システム。
ソース IP (ip)	元のセッション送信元 IP アドレス。
ユーザー (user)	認証されるエンドユーザー。
ユーザー正規化 (normalize_user)	認証されるユーザー名の正規化バージョン（ユーザー名にドメイン名を追加するなど）。
オブジェクト (object)	システム イベントに関連付けられてたオブジェクトの名前。
認証ポリシー (authpolicy)	保護されたリソースへのアクセスを許可する前に、認証のためにポリシーが呼び出されます。
リピートカウント（repeatcnt）	5 秒以内に開始された、送信元 IP、宛先 IP、アプリケーション、サブタイプが同じになっているセッションの数です。
認証 ID (authid)	プライマリ認証と追加（マルチ ファクター）認証で一意の ID が与えられます。
ベンダー (vendor)	追加の要素認証を提供するベンダー。

フィールド名	説明
ログ アクション (logset)	セッションに適用されたログ転送プロファイル。
Server Profiles（サーバー プロファイル）（serverprofile）	認証に使用される認証サーバー。
説明（desc）	追加の Authentication（認証）情報。
クライアント タイプ (clienttype)	認証を完了するために使用されるクライアントのタイプ（認証ポータルなど）。
イベント タイプ (event)	認証試行の結果。
ファクター番号 (factorno)	第一認証（1）と追加の要素（2）のうちどちらなのかを示します。
シーケンス番号（seqno）	順次増分される 64 ビットのログ エントリ識別子。各ログ タイプには、一意の番号空間があります。
アクション フラグ（actionflags）	ログが Panorama に転送されたかどうかを示すビット フィールド。
デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。 API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。

フィールド名	説明
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
仮想システム ID (vsys_id)	Palo Alto Networks のファイアウォール上の仮想システムの一意な識別子。
認証プロトコル（authproto）	サーバーによって使用される認証プロトコルを示します。GTC 付属 PEAP 等
ルールの UUID（rule_uuid）	規則を恒久的に識別するUUID です。
高解像度タイムスタンプ (high_res_timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 この新規フィールドの形式は YYYY-MM-DDThh:ss:sssTZD です: • **YYYY**—西暦 • **MM**—2桁表記の月数 • **DD**—月の2桁の日 (01 ～ 31) • **T**—タイムスタンプの開始のインジケータ • **hh**—24時間を使用した2桁の時間数 (00 ～ 23) • **mm**—2桁表記の分 (00 ～ 59) • **ss**—2桁表記の秒 (00 ～ 60) • **sss**—ミリ秒単位で1桁以上の桁数 • **TZD**—タイムゾーン指定子 (+hh:mm or -hh:mm) 高精度タイムスタンプは、*PAN-OS 10.2* 以降のリリースを実行しているマネージド *firewalls* から受信したログでサポートされています。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*`1969-12-31T16:00:00.000-8:00`* というタイムスタンプを表示します。
送信元 デバイスのカテゴリ (src_category)	Device-ID がトラフィックの送信元として識別するデバイスのカテゴリ。
送信元のデバイスのプロファイル (src_profile)	Device-ID がトラフィックの送信元として識別するデバイスのデバイスのプロファイル。

フィールド名	説明
送信元のデバイス モデル (src_model)	Device-ID がトラフィックの送信元として識別するデバイスのモデル。
送信元のデバイス ベンダー (src_vendor)	Device-ID がトラフィックの送信元として識別するデバイスのベンダー。
送信元デバイス OS ファミリ (src_osfamily)	Device-ID がトラフィックの送信元として識別するデバイスのオペレーティングシステムの種類。
送信元デバイス OS バージョン (src_osversion)	Device-ID がトラフィックの送信元として識別するデバイスのオペレーティングシステムのバージョン。
送信元ホスト名 (src_host)	Device-ID がトラフィックの送信元として識別するデバイスのホスト名。
送信元 MAC アドレス (src_mac)	Device-ID がトラフィックの送信元として識別するデバイスの MAC アドレス。
地域（地域）	トラフィックの発信元の地理的リージョン。
ユーザー エージェント（user_agent）	HTTP 要求ヘッダーからの文字列　ユーザー・エージェント　。
セッション ID	トラフィック セッションを一意に識別する文字列。

設定ログの各フィールド

フォーマット：FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, Generated Time, Host, Virtual System, Command, Admin, Client, Result, Configuration Path, Before Change Detail, After Change Detail, Sequence Number, Action Flags, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Device Group, Audit Comment

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号 (serial)	ログを生成したデバイスのシリアル番号。

フィールド名	説明
タイプ（type）	ログのタイプを指定します。値は CONFIG です。
脅威/コンテンツ タイプ (subtype)	設定ログのサブタイプ。未使用
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
ホスト (host)	クライアント マシンのホスト名または IP アドレス
仮想システム (vsys)	設定ログに関連付けられた仮想システム
コマンド（cmd）	管理者によって実行されたコマンド。値は、「add」、「clone」、「commit」、「delete」、「edit」、「move」、「rename」、「set」です。
管理者（admin）	設定を実行する管理者のユーザー名
クライアント（client）	管理者によって使用されるクライアント。値は「Web」と「CLI」です
結果（result）	設定アクションの結果。値は、「Submitted」、「Succeeded」、「Failed」、「Unauthorized」です
設定パス（path）	発行された設定コマンドのパス。最大長 512 バイト
変更前の詳細 (before-change-detail)	このフィールドはカスタム ログの場合のみです。デフォルトのフォーマットには含まれません。 設定の変更前の完全な xpath が保持されています。
変更後の詳細 (after-change-detail)	このフィールドはカスタム ログの場合のみです。デフォルトのフォーマットには含まれません。 設定の変更後の完全な xpath が保持されています。
シーケンス番号（seqno）	順次増分される 64 ビットのログ エントリ識別子。各ログ タイプには、一意の番号空間があります。
アクション フラグ（actionflags）	ログが Panorama に転送されたかどうかを示すビット フィールド。
デバイス グループ階層	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）

フィールド名	説明
（dg_hier_level_1 ～ dg_hier_level_4）	には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。 API クエリ: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
デバイス グループ (dg_id)	Panorama™ 管理サーバーによって管理されている場合、ファイアウォールが属するデバイス グループ。
監査コメント (comment)	ポリシー ルール設定の変更に入力された監査コメント。

システム ログの各フィールド

フォーマット:FUTURE_USE, Receive Time, Serial Number, Type, Content/Threat Type, FUTURE_USE, Generated Time, Virtual System, Event ID, Object, FUTURE_USE, FUTURE_USE, Module, Severity, Description, Sequence Number, Action Flags, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, FUTURE_USE, FUTURE_USE, High Resolution Timestamp

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号 (serial)	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は SYSTEM です。

フィールド名	説明
コンテンツ/脅威タイプ (subtype)	システム ログのサブタイプ。ログを生成するシステム デーモンを参照します。値は、「crypto」、「dhcp」、「dnsproxy」、「dos」、「general」、「global-protect」、「ha」、「hw」、「nat」、「ntpd」、「pbf」、「port」、「pppoe」、「ras」、「routing」、「satd」、「sslmgr」、「sslvpn」、「userid」、「url-filtering」、「vpn」です。
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
仮想システム (vsys)	設定ログに関連付けられている仮想システム。
イベント ID (eventid)	イベントの名前を示す文字列。
オブジェクト (object)	システム イベントに関連付けられてたオブジェクトの名前。
モジュール（module）	このフィールドは、subtype フィールドの値が general の場合にのみ有効です。ログを生成するサブシステムに関する補足情報を提供します。値は、「general」、「management」、「auth」、「ha」、「upgrade」、「chassis」です。
重大度 (severity)	イベントに関連付けられた重大度。値は、「informational」、「low」、「medium」、「high」、「critical」です。
説明 (opaque)	イベントの詳細な説明。最大 512 byte (バイト)。
シーケンス番号（seqno）	64 ビットのログ エントリ識別子。各ログ タイプには、一意の番号空間があります。
アクション フラグ（actionflags）	ログが Panorama に転送されたかどうかを示すビット フィールド。
デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。

フィールド名	説明
	API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
高解像度タイムスタンプ (high_res_timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 この新規フィールドの形式は YYYY-MM-DDThh:ss:sssTZD です: • **YYYY**—西暦 • **MM**—2桁表記の月数 • **DD**—月の2桁の日 (01 ～ 31) • **T**—タイムスタンプの開始のインジケータ • **hh**—24時間を使用した2桁の時間数 (00 ～ 23) • **mm**—2桁表記の分 (00 ～ 59) • **ss**—2桁表記の秒 (00 ～ 60) • **sss**—ミリ秒単位で1桁以上の桁数 • **TZD**—タイムゾーン指定子 (+hh:mm or -hh:mm) 高解像度タイムスタンプは、*PAN-OS 10.2* 以降のリリースを実行しているマネージドファイアウォールから受信したログでサポートされています。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*`1969-12-31T16:00:00.000-8:00`* というタイムスタンプを表示します。

対比機能のあるイベント ログの各フィールド

フォーマット：FUTURE_USE、Receive Time (受信時間)、Serial Number (シリアル番号)、Type (タイプ)、Content/Threat Type (コンテンツ/脅威タイプ)、FUTURE_USE、Generated Time (生成時間)、Source Address (送信元アドレス)。Source User, Virtual System, Category, Severity, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Virtual System ID, Object Name, Object ID, Evidence

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された時間。
シリアル番号 (serial)	ログを生成したデバイスのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は CORRELATION です。
コンテンツ/脅威タイプ (subtype)	システム ログのサブタイプ。ログを生成するシステム デーモンを参照します。値は、「crypto」、「dhcp」、「dnsproxy」、「dos」、「general」、「global-protect」、「ha」、「hw」、「nat」、「ntpd」、「pbf」、「port」、「pppoe」、「ras」、「routing」、「satd」、「sslmgr」、「sslvpn」、「userid」、「url-filtering」、「vpn」です。
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
送信元アドレス (src)	イベントを開始したユーザーのIPアドレス
送信元ユーザー (srcuser)	イベントを開始したユーザーのユーザー名
仮想システム (vsys)	設定ログに関連付けられている仮想システム。
カテゴリ（category）	ネットワーク、ユーザー、またはホストに与える脅威または損害の種類を要約したもの。
重大度 (severity)	イベントに関連付けられた重大度。値は、「informational」、「low」、「medium」、「high」、「critical」です。
デバイス グループ階層（dg_hier_level_1 ～ dg_hier_level_4）	デバイス グループ階層内でのデバイス グループの位置を示す、一連の識別番号。ログを生成するファイアウォール（または仮想システム）には、デバイス グループ階層における各上位デバイス グループの識別番号が含まれます。共有デバイス グループ（レベル 0）はこの構造には含まれません。 ログの値が 12、34、45、0 の場合、デバイス グループ 45 に属し、上位デバイス グループが 34 および 12 であるファイアウォール（仮想システム）によってそのログが生成されたことを示します。値 12、34、または 45 に対応するデバイス グループ名を表示するには、以下のいずれかの方法に従います。

フィールド名	説明
	API query: `/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>`
仮想システム名（vsys_name）	セッションに関連付けられた仮想システムの名前。複数の仮想システムに対して有効化されたファイアウォールでのみ有効。
デバイス名（device_name）	セッションがログに記録されたファイアウォールのホスト名。
仮想システム ID (vsys_id)	Palo Alto Networks のファイアウォール上の仮想システムの一意な識別子。
オブジェクト名 (objectname)	一致した相関オブジェクトの名前。
オブジェクト ID (object_id)	システム イベントに関連付けられてたオブジェクトの名前。
イビデンス (evidence)	ホストが相関オブジェクトが定める条件に一致した回数を示すサマリーステートメント例えば、既知のマルウェア URL にアクセスするホスト(19回)

GTP ログの各フィールド

フォーマット：FUTURE_USE、受信時刻、シリアル番号、種類、脅威/コンテンツ タイプ、FUTURE_USE、生成時刻、送信元アドレス、送信先アドレス、FUTURE_USE、FUTURE_USE、ルール名、FUTURE_USE、FUTURE_USE、アプリケーション、仮想システム、送信元ゾーン、宛先ゾーン、受信インターフェイス、発信インターフェイス、ログ アクション、FUTURE_USE、セッション ID、FUTURE_USE、送信元ポート、宛先ゾーン、着信インターフェイス、発信インターフェイス、発信インターフェイス、ログ アクション、FUTURE_USE、セッション ID、FUTURE_USE、送信元ポート、宛先ポート、FUTURE_USE、FUTURE_USE、FUTURE_USE、プロトコル、アクション、GTP イベント タイプ、MSISDN、アクセス ポイント名、無線アクセス 技術、GTP メッセージ タイプ、エンド ユーザー IP アドレス、トンネル エンドポイント識別子 1、トンネル エンドポイント識別子 2、GTP インターフェイス、GTP の原因、重大度、サービス国 MCC、 サービスネットワークMNC、エリアコード、セルID、GTPイベントコード、FUTURE_USE、FUTURE_USE、ソースの場所、宛先の場所、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_トンネルID / IMSI、モニタータグ/IMEI、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTUR、FUTURE_USE、FUTURE_USE、FUTURE_USE、FUTURE_USE、Start Time、Elapsed Time、Tunnel Inspection Rule、Remote User IP、Remote User ID、UUID for rule、PCAP ID、High Resolution Timestamp、A Slice Service Type、A Slice Differentiator、Application Subcategory、 ア

プリケーションカテゴリ、アプリケーションテクノロジー、アプリケーションリスク、アプリケーション特性、アプリケーションコンテナ、アプリケーションSaaS、アプリケーション認可状態

フィールド名	説明
受信時間 (receive_time または cef-formatted-receive_time)	管理プレーンでログが受信された月、日、時間。
シリアル番号 (serial)	ログを生成したファイアウォールのシリアル番号。
タイプ（type）	ログのタイプを指定します。値は GTP です。
脅威/コンテンツ タイプ (subtype)	トラフィック ログのサブタイプ。値は、「start」、「end」、「drop」、「deny」です • start – セッションが開始しました • end – セッションが終了しました • drop – アプリケーションが特定される前にセッションが廃棄され、そのセッションを許可するルールがありません。 • deny – アプリケーションが特定された後にセッションが廃棄され、そのセッションをブロックするルールがあるか、セッションを許可するルールがありません。
生成時間 (time_generated または cef-formatted-time_generated)	データプレーンでログが生成された日時。
送信元アドレス (src)	セッション中のパケットの送信元 IP アドレス
宛先アドレス (dst)	セッション中のパケットの宛先 IP アドレス
ルール名（rule）	セッションで有効なセキュリティポリシー ルールの名前
アプリケーション (app)	セッションで使用されているトンネル プロトコル
仮想システム (vsys)	セッションに関連付けられている仮想システム。
送信元ゾーン (from)	セッション中のパケットの送信元ゾーン
宛先ゾーン (to)	セッション中のパケットの宛先ゾーン
インバウンド インターフェイス (inbound_if)	セッションの送信元となったインターフェイス。

フィールド名	説明
アウトバウンド インターフェイス (outbound_if)	セッションの宛先だったインターフェイス。
ログ アクション (logset)	セッションに適用されたログ転送プロファイル。
セッション ID (sessionid)	ロギング中のセッションのセッション ID
送信元ポート（sport）	セッションで使用された送信元ポート。
宛先ポート（dport）	セッションで使用された宛先ポート。
IP プロトコル（proto）	セッションに関連付けられた IP プロトコル。
アクション（action）	セッションで実行されたアクション。値は以下のいずれかです。 • allow —セッションはポリシーによって許可されました • deny — セッションはポリシーによって拒否されました
GTP イベント タイプ（event_type）	GTP 保護プロファイルのチェックが GTP トラフィックに適用されたときに、GTP メッセージによってトリガされるイベントを定義します。GTP セッションの開始あるいは終了によってもトリガーされます。
MSISDN（msisdn）	国コード、国内宛先コード、サブスクライバから成る、モバイル サブスクライバに関連するサービス ID。最大 15 桁の 10 進数の数（0～9）のみで構成されます。
アクセスポイント名（apn）	モバイルネットワーク内のパケット データ ネットワーク データ ゲートウェイ（PGW）/ゲートウェイ GPRS サポート ノードへの参照。必須の APN ネットワーク識別子および任意の APN 演算子識別子で構成されます。
ラジオ アクセス テクノロジー（rat）	ラジオ アクセスに使用されるテクノロジーの種類。例えば、EUTRAN、WLAN、Virtual、HSPA Evolution、GAN および GERAN です。
GTP メッセージ タイプ（msg_type）	GTP メッセージの種類を示します。
エンド IP アドレス（end_ip_adr）	PGW/GGSN によって割り当てられたモバイル サブスクライバの IP アドレス

フィールド名	説明
トンネル エンドポイント識別子1（teid1）	ネットワーク ノード内の GTP トンネルを識別します。TEID1 は GTP メッセージの最初の TEID です。
トンネル エンドポイント識別子2（teid2）	ネットワーク ノード内の GTP トンネルを識別します。TEID2 は GTP メッセージの 2 つ目の TEID です。
GTP インターフェイス（gtp_interface）	GTP メッセージの送信元となる 3GPP インターフェイス。
GTP 原因（cause_code）	ログ応答に含まれる GTP 原因の値であり、ネットワーク ノードによる GTP リクエストが承諾/拒否されたことについての情報を提供する情報エレメントを含みます。
重大度 (severity)	イベントに関連付けられた重大度。値は、「informational」、「low」、「medium」、「high」、「critical」です。
サービング ネットワーク MCC（mcc）	サービング コア ネットワーク演算子のモバイル国コード。
サービング ネットワーク MNC（mnc）	サービング コア ネットワーク演算子のモバイル ネットワーク コード。
市外局番（area_code）	地上波公共移動通信ネットワーク（PLMN）内のエリア。
セル ID（cell_id）	任意のエリアコード内のベース ステーション。
GTP イベント コード（event_code）	GTP イベントを説明するイベント コード。
送信国 (srcloc)	プライベート アドレスの送信元の国または内部領域。最大長は 32 バイトです。
宛先国 (dstloc)	プライベート アドレスの宛先の国または内部領域。最大長は 32 バイトです。
トンネル ID/IMSI (imsi)	International Mobile Subscriber Identity（IMSI）は、GSM/UMTS/EPS システム内の各モバイル サブスクライバに割り当てられる一意の番号です。IMSI は10進数（0～9）のみで構成され、最大桁数は 15 です。
監視タグ/IMEI (imei)	International Mobile Equipment Identity (IMEI) は、各モバイル ステーション装置に割り当てられた 15 あるいは 16 桁の一意の数字です。

フィールド名	説明
開始時間（start）	セッションの開始時間。
経過時間 (elapsed)	セッションの経過時間。
トンネル検査ルール (tunnel_insp_rule)	クリア テキスト トンネル トラフィックに一致するトンネル検査ルールの名前
リモートユーザー IP (remote_user_ip)	リモートユーザーが使用する IPv4 あるいは IPv6 アドレス。
リモートユーザー ID (remote_user_id)	リモートユーザーの IMSI 識別子。利用できる場合、単一の IMEI 識別子および/または単一の MSISDN 識別子。
ルールの UUID（rule_uuid）	ルールのユニバーサルに一意な ID です。
PCAP ID （pcap_id）	ファイアウォール上に保存された pcap ファイルを探すために使用する一意のパケット キャプチャ ID。
高解像度タイムスタンプ (high_res _timestamp)	management plane (管理プレーン - MP)でログが受信された時間 (ミリ秒)。 この新規フィールドの形式は YYYY-MM-DDThh:ss:sssTZD です: • **YYYY**—西暦 • **MM**—2桁表記の月数 • **DD**—月の2桁の日 (01 ～ 31) • **T**—タイムスタンプの開始のインジケータ • **hh**—24時間を使用した2桁の時間数 (00 ～ 23) • **mm**—2桁表記の分 (00 ～ 59) • **ss**—2桁表記の秒 (00 ～ 60) • **sss**—ミリ秒単位で1桁以上の桁数 • **TZD**—タイムゾーン指定子 (+hh:mm or -hh:mm) 高解像度タイムスタンプは、*PAN-OS 10.2* 以降のリリースを実行しているマネージド *firewalls* から受信したログでサポートされています。*PAN-OS 9.1* リリース以前で稼働する管理ファイアウォールから受信するログは、ログ受信時刻に関係なく、*1969-12-31T16:00:00:000-8:00* というタイムスタンプを表示します。

フィールド名	説明
A スライス サービス タイプ (nsdsai_sst)	ネットワーク スライス ID の A スライス サービス タイプ。
A スライス差別化要素 (nsdsai_sd)	ネットワーク スライス ID の A スライス差別化要素。
アプリケーション サブカテゴリ (subcategory_of_app)	アプリケーション構成プロパティで指定されたアプリケーション サブカテゴリ。
アプリケーションカテゴリ (category_of_app)	アプリケーション構成プロパティで指定されたアプリケーション カテゴリ。値を以下に示します。 • business-system • コラボレーション • 一般インターネット • メディア • networking • SaaS
アプリケーションテクノロジー (technology_of_app)	アプリケーション構成プロパティで指定されたアプリケーション テクノロジ。値を以下に示します。 • ブラウザベース • クライアント/サーバー • ネットワークプロトコル • ピアツーピア
アプリケーションリスク (risk_of_app)	アプリケーションに関連付けられたリスク レベル (1 =最低から 5=最高)。
アプリケーション特性 (characteristic_of_app)	アプリケーションの適用可能特性のコンマ区切りリスト
アプリケーション コンテナ (container_of_app)	アプリケーションの親アプリケーション。
アプリケーション SaaS (is_saas_of_app)	SaaS アプリケーションの場合は `1`、SaaS アプリケーションでない場合は `0` を表示します。
アプリケーション認可状態 (sanctioned_state_of_app)	アプリケーションが認可されている場合は `1`、アプリケーションが認可されていない場合は `0` が表示されます。

フィールド名	説明
アプリケーション サブカテゴリ (subcategory_of_app)	アプリケーション構成プロパティで指定されたアプリケーション サブカテゴリ。

Syslog の重大度

Syslog の重大度は、ログ タイプとコンテンツに基づいて設定されます。

ログ タイプ/重大度	Syslog の重大度
トラフィック	info
CONFIG コンフィグ	info
脅威/システム – Informational	info
脅威/システム – Low	通知
脅威/システム – Medium	Warning（警告）
脅威/システム – High	Warning（警告）
脅威/システム – Critical	Critical (極めて重大)

カスタム ログ/イベントのフォーマット

外部ログ解析システムと統合しやすくするため、ファイアウォールでは、ログ フォーマットをカスタマイズすることができます。また、カスタムの *Key:* を追加することもできます。値 属性ペアカスタム メッセージのフォーマットは、**Device (デバイス)** > **Server Profiles (サーバープロファイル)** > **Syslog** > **Syslog Server Profile (Syslog サーバー プロファイル)** > **Custom Log Format (カスタム ログ フォーマット)**で設定できます。

ArcSight Common Event Format （CEF）準拠のログ フォーマットを設定するには、『CEF Configuration Guide』（英語）を参照してください。

エスケープ シーケンス

カンマまたは二重引用符を含むフィールドは、二重引用符で囲みます。さらに、二重引用符が 1 つのフィールド内に含まれる場合は、別の二重引用符を前に付けてエスケープします。下位互換性を維持するため、脅威ログの「その他」フィールドは常に二重引用符で囲みます。

SNMP モニタリングおよびトラップ

以下のトピックでは、Palo Alto Networks ファイアウォール、Panorama、WF-500 アプライアンスによる SNMP の実装方法と、SNMP モニタリングおよび SNMP トラップ送信の設定手順を説明します。

- SNMP サポート
- SNMP マネージャを使用した MIB およびオブジェクトの探索
- ファイアウォールで保護されるネットワーク要素に対する SNMP サービスの有効化
- SNMP を使用した統計のモニター
- SNMP マネージャへのトラップの転送
- サポートされる MIB

SNMP サポート

SNMP マネージャを使用して、ファイアウォール、Panorama、WF-500 アプライアンスとそれらが処理するトラフィックのイベント駆動アラートおよび操作統計をモニターできます。統計とトラップは、リソース制限、システムの変更または障害、およびマルウェア攻撃の識別に役立ちます。ログ データをトラップとして転送することでアラートを設定し、また、SNMP マネージャからの GET メッセージ（要求）に応じて統計を送信できるようにします。トラップと統計にはそれぞれオブジェクト識別子（OID）があります。関連する OID は、Management Information Base （MIB）内に階層的にまとめられています。モニタリングを有効にするにはこの MIB を SNMP マネージャにロードします。

あるイベントが *SNMP* トラップジェネレーション（インタフェイスダウンなど）をトリガーする場合、ファイアウォール、*Panorama* 仮想アプライアンス、*M*シリーズアプライアンス、*WF-500* アプライアンスは*10*秒ごとに発生する全てのオブジェクトの定期的更新を待つのでなく、対応する *SNMP* オブジェクト（インターフェイス *MIB* など）を更新することによって応答します。これにより *SNMP* マネージャーはオブジェクトがイベントを確認する場合、最新の情報を表示できるようになります。

ファイアウォール、 Panorama、および WF-500 アプライアンスは SNMP バージョン 2c とバージョン 3 をサポートします。使用するバージョンは、ネットワーク内の他のデバイスがサポートしているバージョンと、ネットワーク セキュリティ要件に基づいて決定します。SNMPv3 は、SNMPv2c よりもセキュリティが強化され、システム統計へのアクセスをより詳細に制御できます。以下の表に、各バージョンのセキュリティ機能を要約して示します。SNMP を使用した統計のモニターおよびSNMP マネージャへのトラップの転送を行う際に、バージョンを選択し、セキュリティ機能を設定します。

SNMPバージョン	認証	メッセージのプライバシー	メッセージの整合性	MIB アクセスの詳細度
SNMPv2c	コミュニティ文字列	なし（クリアテキスト）	不要	デバイス上のすべての MIB に対する SNMP コミュニティ アクセス
snmpv3	エンジン ID、ユーザー名、および認証パスワード（パスワードの SHA ハッシュ）	SNMP メッセージの AES (128、192、または 256) 暗号化のプライバシー パスワード	あり	表示（特定の OID が含まれるか、除外されているか）に基づくユーザー アクセス

SNMP の実装 は、ファイアウォールがトラップを SNMP マネージャに転送すると共に、ログ コレクタにもログを転送するデプロイメントを示しています。または、ファイアウォール トラップを SNMP マネージャに転送するようにログ コレクタを設定できます。これらのデプロイメントの詳細は、一元的なロギングおよびレポートにおけるログ転送オプションを参照してください。すべてのデプロイメントで、SNMP マネージャは、直接、ファイアウォール、Panorama、WF-500 アプライアンスから統計を取得します。この例では、1 つの SNMP マネージャがトラップと統計の両方を収集しますが、ネットワークに適していれば、これらの機能に別個のマネージャを使用できます。

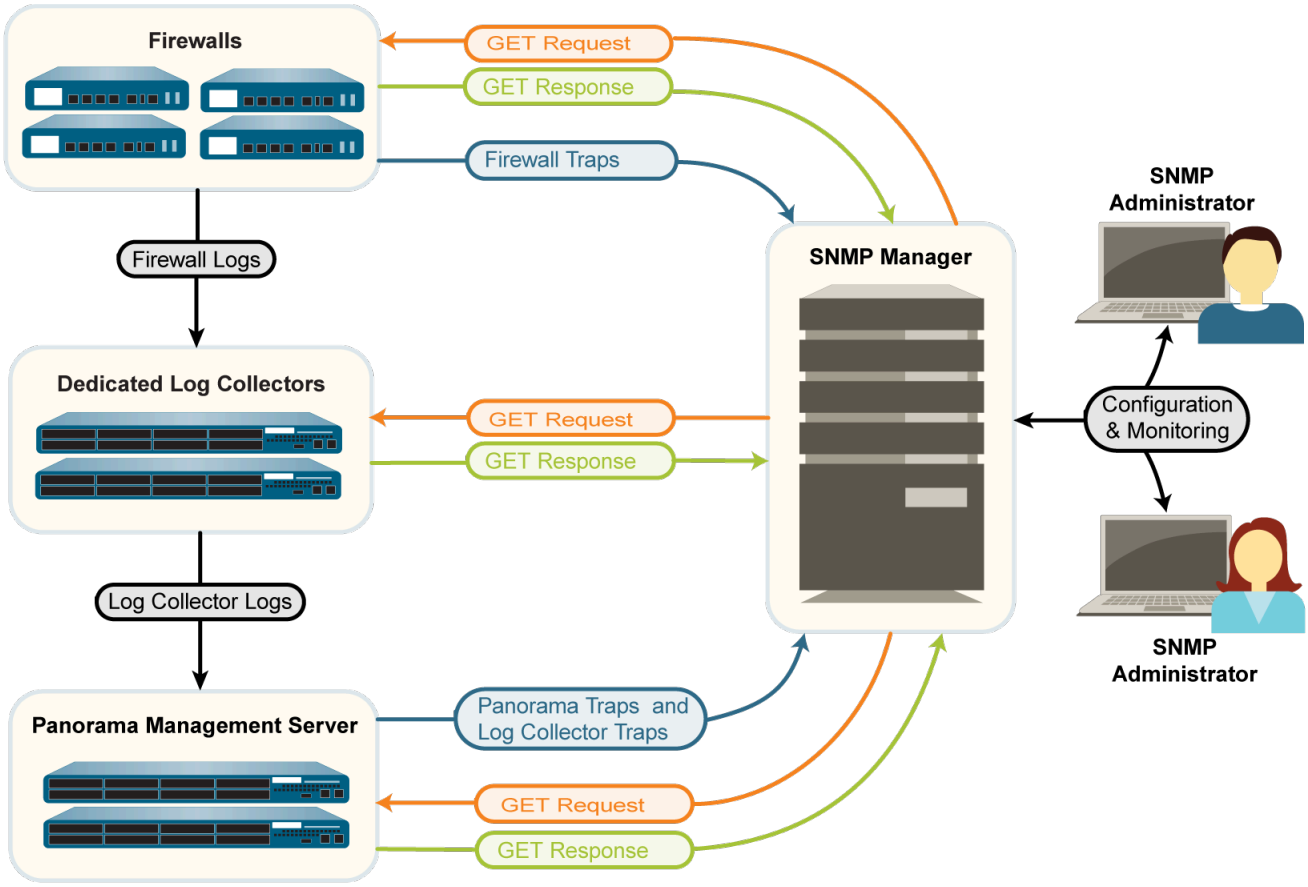


図 **2 : SNMP** 実行

SNMP マネージャを使用した MIB およびオブジェクトの探索

SNMP を使用して Palo Alto Networks ファイアウォール、Panorama、または WF-500 アプライアンスをモニターするには、まずサポートされる MIBを SNMP マネージャーにロードし、モニターするシステム統計およびトラップに対応するオブジェクト ID (OID) を判別する必要があります。以下のトピックでは、SNMP マネージャで OID と MIB を見つける方法の概要を説明します。これらのタスクを実行するための具体的な手順は、SNMP 管理ソフトウェアを参照してください。

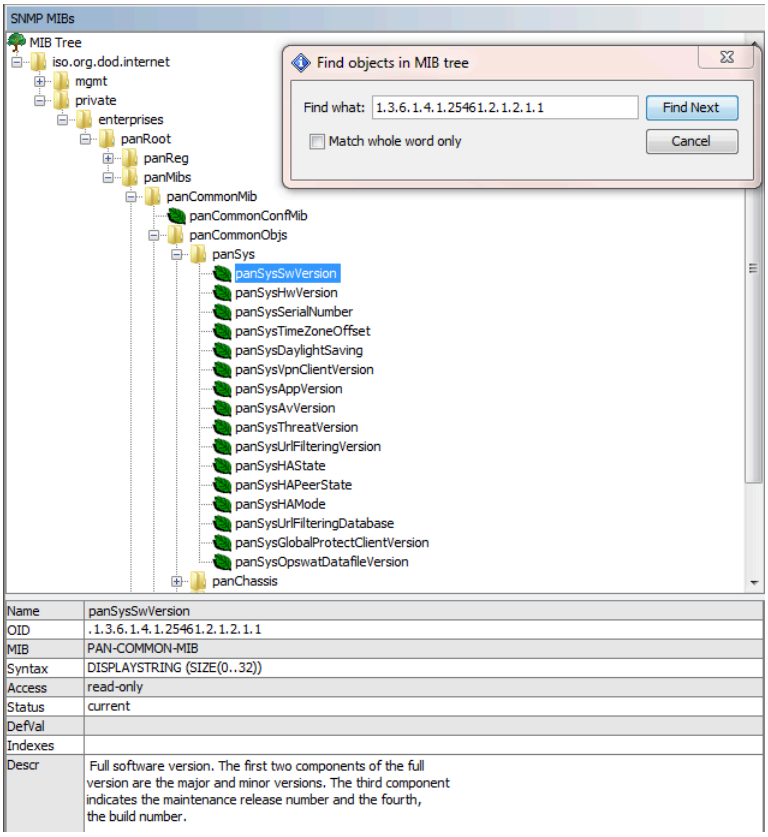
- 既知の OID が含まれる MIB の識別
- MIB の探索
- システム統計またはトラップの OID の識別

既知の OID が含まれる MIB の識別

特定の SNMP オブジェクト（デバイス統計またはトラップ）の OID がすでにわかっていて、類似のオブジェクトをモニターできるようにその OID を調べる場合、既知の OID が含まれる MIB を検索できます。

STEP 1 | すべてのサポートされる MIBをSNMPマネージャにロードします。

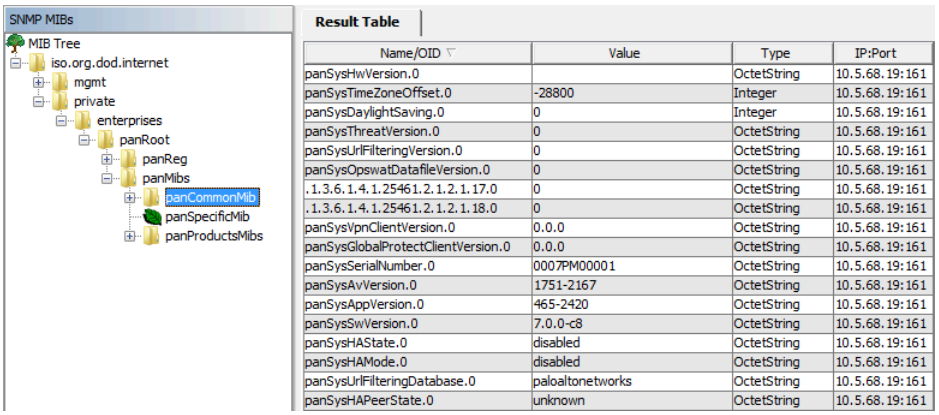
STEP 2 | MIB ツリー全体から既知の OID を検索します。検索結果には、その OID の MIB パスと OID に関する情報（名前、状態、説明など）が表示されます。同じ MIB の他の OID を選択して、それらに関する情報を表示できます。



STEP 3 | **(**Optional**)** は、そのすべてのオブジェクトを表示するMIB の探索があります。

MIB の探索

モニタリングが可能な SNMP オブジェクト（デバイス統計およびトラップ）を確認するには、特定の MIB のオブジェクトをすべて表示すると容易に確認できます。これを行うには、サポートされる MIBを SNMP マネージャーにロードし、目的の MIB で ***walk*** を実行します。Palo Alto Networks ファイアウォール、Panorama、 WF-500 アプライアンスでサポートされるトラップのリストを表示するには、panCommonEventEventsV2 MIB を探索します。次の例では、PAN-COMMON-MIB.myをwalkすると、特定の統計の OID とその値の次のリストが表示されます。



システム統計またはトラップの OID の識別

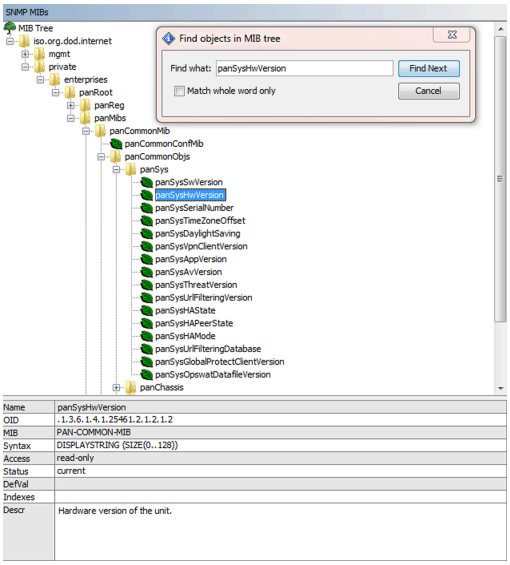
SNMP マネージャを使用して Palo Alto Networks ファイアウォール、Panorama、 WF-500 アプライアンス デバイスをモニターするには、モニターするデバイス統計とトラップの OID を把握しておく必要があります。

STEP 1 | サポートされる MIB を確認して、目的のタイプの統計がどの MIB に含まれているかを判別します。たとえば、PAN-COMMON-MIB.my には、ハードウェアのバージョン情報が含まれています。panCommonEventEventsV2 MIB には、Palo Alto Networks ファイアウォール、Panorama、 WF-500 アプライアンスでサポートされるすべてのトラップが含まれています。

STEP 2 | テキスト エディタで MIB を開き、キーワード検索を実行します。たとえば、PAN-COMMON-MIB で「**Hardware version**」（ハードウェア バージョン）を検索文字列として使用すると、panSysHwVersion オブジェクトが検出されます。

```
panSysHwVersion OBJECT-TYPE SYNTAX DisplayString (SIZE(0..128))
 MAX-ACCESS read-only STATUS 現在の記述 「ユニットのハードウェアバージョン」。 ::= {panSys 2}
```


STEP 3 | MIB ブラウザを使用して、識別されたオブジェクト名をMIB ツリーで検索し、その OID を表示します。たとえば、panSysHwVersion オブジェクトには1.3.6.1.4.1.25461.2.1.2.1.2.の OID があります。



ファイアウォールで保護されるネットワーク要素に対する SNMP サービスの有効化

Simple Network Management Protocol （SNMP）を使用して、Palo Alto Networks ファイアウォールのセキュリティ ゾーン内にあるネットワーク要素（スイッチやルーターなど）をモニターまたは管理する場合、それらの要素に対して SNMP サービスを許可するセキュリティ ルールを作成する必要があります。

Palo Alto Networks ファイアウォール、*Panorama*、 *WF-500* アプライアンスの *SNMP* モニタリングを有効にする場合は、セキュリティ ルールは必要ありません。詳細は、SNMP を使用した統計のモニターを参照してください。

STEP 1 | アプリケーション グループを作成します。

1. **Objects** > **Application Group**(オブジェクト > アプリケーション グループ) の順に選択し、**Add** (追加)をクリックします。
2. アプリケーション グループを識別するための **Name** [名前]を入力します。
3. **Add** [追加]をクリックし、「**snmp**」と入力し、ドロップダウンから **snmp** と **snmp-trap** を選択します。
4. **OK** をクリックしてアプリケーション グループを保存します。

STEP 2 | SNMP サービスを許可するセキュリティ ルールを作成します。

1. **Policies**（ポリシー） > **Security**（セキュリティ） を選択してルールをクリックしますd
2. **General** [全般]タブで、ルールの **Name** [名前]を入力します。
3. **Source** (送信元) タブと **Destination** (宛先) タブで、**Add** (追加) をクリックし、トラフィックの **Source Zone** (送信元ゾーン) と **Destination Zone** (宛先ゾーン) を入力します。
4. **Applications** [アプリケーション]タブで、**Add**[追加]をクリックし、作成したアプリケーション グループの名前を入力し、ドロップダウンからその名前を選択します。
5. **Actions** [アクション]タブで、**Action** [アクション]が **Allow** [許可]に設定されていることを確認し、**OK**、**Commit** [コミット]の順にクリックします。

SNMP を使用した統計のモニター

Simple Network Management Protocol （SNMP）マネージャが Palo Alto Networks ファイアウォールから収集する統計は、ネットワークの正常性（システムと接続）を測定し、リソース制限を識別し、トラフィックまたは処理負荷をモニターするのに役立ちます。統計には、インターフェイス状態（アップまたはダウン）、アクティブなユーザー セッション数、同時セッション数、セッション使用率、温度、システム アップタイムなどがあります。

SNMP マネージャに、（*SET* メッセージを使用した）*Palo Alto Networks* ファイアウォールの制御を設定することはできません。設定できるのは、（*GET* メッセージを使用した）ファイアウォールからの統計収集のみです。*Palo Alto Networks* ファイアウォールでの *SNMP* の実装方法の詳細は、「SNMP サポート」を参照してください。

STEP 1 | SNMP マネージャを、ファイアウォールから統計情報を取得するように設定します。

以下の手順では、SNMP マネージャで実行するタスクの概要を説明します。具体的な手順は、SNMP マネージャのドキュメントを参照してください。

1. SNMP マネージャを有効にしてファイアウォール統計を解釈するには、Palo Alto Networks ファイアウォールでサポートされたMIBをロードし、必要に応じてコンパイルします。
2. SNMP マネージャがモニターするファイアウォールごとに、ファイアウォールの接続設定（IP アドレスとポート）および認証設定（SNMPv2c コミュニティ文字列または SNMPv3 エンジン ID/ユーザー名/パスワード）を定義します。

   すべての *Palo Alto Networks* ファイアウォールがポート *161* を使用します。

   SNMP マネージャでは、複数のファイアウォールに対して使用する接続設定と認証設定は同じでも違っていてもかまいません。この設定は、ファイアウォールにSNMPを設定する際に定義したものと一致している必要があります（ステップ3を参照）。たとえば、SNMPv2c を使用する場合、ファイアウォール設定時に定義するコミュニティ文字

列が、SNMP マネージャでそのファイアウォールに対して定義するコミュニティ文字列と一致する必要があります。

3. モニターする統計のオブジェクト識別子（OID）を判別します。たとえば、ファイアウォールのセッション使用率をモニターする場合、MIB ブラウザにはこの統計がPAN-COMMON-MIB.myの OID 1.3.6.1.4.1.25461.2.1.2.3.1.0 に対応すると表示されます。詳細についてはSNMP マネージャを使用してMIB およびオブジェクトを探索をご覧ください。
4. SNMP マネージャを、目的の OID をモニターするように設定します。

STEP 2 | ファイアウォール インターフェイスで SNMP トラフィックを有効にします。

このインターフェイスが SNMP マネージャからの統計要求を受信します。

PAN-OS は、高可用性（*HA*）設定のファイアウォールについては、管理（*MGT*）インターフェイス設定を同期しません。*HA* ピアごとにインターフェイスを設定する必要があります。

ファイアウォールの Web インターフェイスで以下のステップを実行します。

- MGT インターフェイス上で SNMP トラフィックを有効にするには、**Device (デバイス)** > **Setup (セットアップ)** > **Interfaces (インターフェイス)** を選択し、**Management (管理)** インターフェイスを編集し、**SNMP** を選択して **OK** および **Commit (コミット)** をクリックします。
- 他のインターフェイスで SNMP トラフィックを有効にするには、SNMPサービスにインターフェイス管理プロファイルを作成し、それを SNMP 要求を受信するインターフェイスに割り当てます。インターフェイス タイプは Layer 3 Ethernet にする必要があります。

STEP 3 | ファイアウォールを、SNMP マネージャからの統計要求に応答するように設定します。

PAN-OS は、高可用性（*HA*）設定のファイアウォールについては、*SNMP* 応答設定を同期しません。*HA* ピアごとに設定する必要があります。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)** を選択し、Miscellaneous (その他) セクションで **SNMP Setup (SNMP セットアップ)** をクリックします。
2. SNMP の **Version**（バージョン）を選択し、認証値を以下のように設定します。バージョンの詳細については、SNMP サポートを参照してください。
   - **V2c** – **SNMP Community String** [SNMP コミュニティ名]を入力します。これは、SNMP マネージャおよびモニター対象デバイスのコミュニティを識別し、コミュニティ メンバーを相互認証するためのパスワードとして機能する文字列です。

     ベスト プラクティスとして、デフォルトのコミュニティ文字列 ***public*** はよく知られていて安全ではないため、使用しないことをお勧めします。
   - **V3** – 少なくとも 1 つの SNMP 表示グループと 1 つのユーザーを作成します。ユーザー アカウントと表示により、ファイアウォールがトラップを転送するとき

や SNMP マネージャがファイアウォール統計を取得するときに、認証、プライバシー、およびアクセス制御を実現できます。

- 表示 – 各表示は、ペアになっている OID とビット単位のマスクです。OID で MIB を指定し、マスク（16 進数形式）で、その MIB 内（一致部分を含む）または MIB 外（一致部分を含まない）でアクセスできるオブジェクトを指定します。最初のリストで **Add**（追加）をクリックし、表示グループの **Name**（名前）を入力します。グループの各表示について、**Add**（追加）をクリックし、表示の **Name**（名前）、**OID**、一致の **Option**（オプション）（**include**（含む）または **exclude**（除外））、および **Mask**（マスク）を設定します。
- **Users (ユーザー)**– 2 つ目のリストで **Add (追加)** をクリックし、**Users (ユーザー)** の下にユーザー名を入力し、ドロップダウンから **View (表示)** グループを選択し、SNMP マネージャへの認証に使用する認証パスワード（**Auth Password (認証パスワード)**）、SNMP マネージャへの SNMP メッセージの暗号化に使用する専用パスワード（**Priv Password (専用パスワード)**）を入力します。

3. **OK**、**Commit (コミット)** の順にクリックします。

STEP 4 | SNMP マネージャでファイアウォール統計をモニターします。

詳細については、SNMP マネージャのドキュメントを参照してください。

ファイアウォール インターフェイスに関連する統計をモニターする場合、*SNMP* マネージャのインターフェイス インデックスをファイアウォール *Web* インターフェイスのインターフェイス名と照合する必要があります。詳細については、SNMP マネージャおよび NetFlow コレクタのファイアウォール インターフェイス識別子を参照してください。

SNMP マネージャへのトラップの転送

Simple Network Management Protocol （SNMP）トラップを使用して、システム イベント（Palo Alto Networks ファイアウォールのハードウェアやソフトウェアの障害または変更）や直ちに注意が必要な脅威（ファイアウォール セキュリティ ルールと一致するトラフィック）に関するアラートを通知できます。

Palo Alto Networks ファイアウォールでサポートされるトラップのリストを表示するには、*SNMP* マネージャを使用して *panCommonEventEventsV2 MIB* にアクセスします。詳細についてはSNMP マネージャを使用してMIB およびオブジェクトを探索をご覧ください。

Palo Alto Networks のファイアウォールでの *SNMP* の実装方法の詳細は、SNMP サポートを参照してください。

STEP 1 | 受信するトラップを SNMP マネージャが解釈できるようにします。

Palo Alto Networks ファイアウォールのサポートされているMIBをロードし、必要に応じてコンパイルします。具体的な手順は、SNMP マネージャのドキュメントを参照してください。

STEP 2 | SNMP トラップ サーバー プロファイルを設定します。

このプロファイルで、ファイアウォールが SNMP マネージャ（トラップ サーバー）にアクセスする方法を定義します。プロファイルごとに最大 4 つの SNMP マネージャを定義できます。

必要に応じて、ログ タイプ、重大度レベル、および *WildFire* 判定ごとに別の *SNMP* トラップ サーバー プロファイルを設定できます。

1. ファイアウォール インターフェイスにログインします。
2. **Device (デバイス)** > **Server Profiles (サーバープロファイル)** > **SNMP Trap (SNMP トラップ)** の順に選択します。
3. **Add** (追加)をクリックし、プロファイルの **Name** (名前)を入力します。
4. ファイアウォールに複数の仮想システム（vsys）がある場合、このプロファイルを使用可能な **Location** [場所]（vsys または **Shared** [共有]）を選択します。
5. SNMP の **Version**（バージョン）を選択し、認証値を以下のように設定します。バージョンの詳細については、SNMP サポートを参照してください。
   - **V2c** – サーバーごとに、**Add** [追加]をクリックし、サーバーの **Name** [名前]、IP アドレス（**SNMP Manager** [SNMP マネージャ]）、および **Community String** [コミュニティ文字列]を入力します。このコミュニティ文字列は、SNMP マネージャおよびモニター対象デバイスのコミュニティを識別し、コミュニティ メンバーを相互認証するためのパスワードとして機能します。

     ベスト プラクティスとして、デフォルトのコミュニティ文字列 ***public*** はよく知られていて安全ではないため、使用しないことをお勧めします。
   - **V3** – サーバーごとに、**Add** [追加]をクリックし、サーバーの **Name** [名前]、IP アドレス（**SNMP Manager** [SNMP マネージャ]）、SNMP ユーザー アカウント（**User** [ユーザー]、SNMP マネージャに定義したユーザー名と一致する必要があります）、デバイスを一意に識別するために使用する **EngineID** [エンジン ID]（空白のままにするとデバイスのシリアル番号が使用されます）、サーバーへの認証に使用する認証パスワード（**Auth Password** [認証パスワード]）、サーバーへの SNMP メッセージの暗号化に使用する専用パスワード（**Priv Password** [専用パスワード]）を入力します。
6. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 3 | ログ転送を設定します。

1. トラフィック、脅威、および WildFire の各トラップの転送先を設定します。
   1. ログ タイプ、重大度レベル、または WildFire 判定ごとに、**SNMP Trap (SNMP トラップ)** サーバー プロファイルを選択します。
   2. Log Forwarding（ログ転送）プロファイルをポリシー ルールおよびネットワーク ゾーンに割り当てます。このルールおよびゾーンによって、トラップの生成と転送がトリガーされます。
2. システム、設定、User-ID、HIP マッチ、および相関ログの転送先を設定します。ログ（トラップ）タイプおよび重大度レベルごとに、**SNMP Trap (SNMP トラップ)** サーバー プロファイルを選択します。
3. **Commit**（コミット）をクリックします。

STEP 4 | SNMP マネージャでトラップをモニターします。

SNMP マネージャのドキュメントを参照してください。

ファイアウォール インターフェイスに関連するトラップをモニターする場合、*SNMP* マネージャのインターフェイス インデックスをファイアウォール *Web* インターフェイスのインターフェイス名と照合する必要があります。詳細については、SNMP マネージャおよび NetFlow コレクタのファイアウォール インターフェイス識別子を参照してください。

サポートされる MIB

以下の表は、Palo Alto Networks ファイアウォール、Panorama、WF-500アプライアンスでサポートされる Simple Network Management Protocol （SNMP）Management Information Base （MIB）の一覧です。MIB に定義されているオブジェクト（システム統計とトラップ）をモニターするには、これらの MIB を SNMP マネージャにロードする必要があります。詳細についてはSNMP マネージャを使用してMIB およびオブジェクトを探索をご覧ください。

MIB タイプ	サポートされる MIB
標準 – ほとんどの標準 MIB は、Internet Engineering Task Force （IETF）が管理しています。これらの MIB は IETF Web サイトからダウンロードできます。	MIB-II IF-MIB HOST-RESOURCES-MIB ENTITY-MIB ENTITY-SENSOR-MIB ENTITY-STATE-MIB

MIB タイプ	サポートされる MIB
Palo Alto Networks ファイアウォール、*Panorama*、*WF-500* アプライアンスは、これらすべての *MIB* のすべてのオブジェクト（*OID*）をサポートしているわけではありません。サポート対象 *OID* の概要については、「サポートされる *MIB*」リンクを参照してください。	IEEE 802.3 LAG MIB LLDP-V2-MIB.my BFD-STD-MIB
エンタープライズ – エンタープライズ MIB は、Palo Alto Networks の技術ドキュメント エンドポイントからダウンロードできます。	PAN-COMMON-MIB.my PAN-GLOBAL-REG-MIB.my PAN-GLOBAL-TC-MIB.my PAN-LC-MIB.my PAN-PRODUCT-MIB.my PAN-ENTITY-EXT-MIB.my PAN-TRAPS.my

MIB-II

MIB-II は、TCP/IP ベースのネットワークでのネットワーク管理プロトコルのオブジェクト識別子（OID）を提供します。システムとインターフェイスに関する全般情報をモニターするには、この MIB を使用します。たとえば、インターフェイス タイプ（ifType オブジェクト）別の帯域幅使用状況のトレンドを分析して、ファイアウォールがトラフィック量の急増に対応できるようにそのタイプのインターフェイスを追加する必要があるかどうかを判断できます。

Palo Alto Networks ファイアウォール、Panorama、WF-500アプライアンスでは、以下のオブジェクト グループのみをサポートしています。

オブジェクト グループ	説明
システム	ハードウェア モデル、システム アップタイム、FQDN、物理的な場所などのシステム情報を提供します。
インターフェイス	物理および論理インターフェイスの統計情報を提供します。たとえば、タイプ、現在の帯域幅（速度）、動作状態（アップ、ダウンなど）、破棄されたパケット数などです。論理インターフェイスのサポートには、VPN トンネル、集約グループ、レイヤー 2 サブインターフェイス、レイヤー 3 サブインターフェイス、ループバック インターフェイス、VLAN インターフェイスが含まれます。

この MIB は RFC 1213 に定義されています。

IF-MIB

IF-MIB は、インターフェース・タイプ (物理および論理) と、MIB-IIで定義されたものを超えるより大きなカウンター (64K) をサポートします。MIB-II で提供される統計以外のインターフェイス統計もモニターするには、この MIB を使用します。たとえば、PA-5200 シリーズ ファイアウォールの 10G インターフェイスなど、高速インターフェイス（2.2 Gps 超）の現在の帯域幅をモニターするには、MIB-II の ifSpeed オブジェクトではなく IF-MIB の ifHighSpeed オブジェクトを確認する必要があります。IF-MIB 統計は、ネットワークのキャパシティを評価する場合に便利です。

Palo Alto Networks ファイアウォール、Panorama、WF-500アプライアンスが IF-MIB でサポートするのは ifXTable のみです。これは、送受信されたマルチキャストおよびブロードキャスト パケット数、インターフェイスがプロミスキャス モードかどうか、インターフェイスに物理的なコネクタがあるかどうかなどのインターフェイス情報を提供します。

この MIB は RFC 2863 に定義されています。

HOST-RESOURCES-MIB

HOST-RESOURCES-MIB は、ホスト コンピュータ リソースの情報を提供します。CPU およびメモリの使用統計をモニターするには、この MIB を使用します。たとえば、現在の CPU 負荷（hrProcessorLoad オブジェクト）をチェックすると、ファイアウォールのパフォーマンス問題のトラブルシューティングに役立ちます。

Palo Alto Networks ファイアウォール、Panorama、WF-500アプライアンスでは、以下のオブジェクト グループを部分的にサポートしています。

オブジェクト グループ	説明
hrDevice	CPU 負荷、ストレージ容量、パーティション サイズなどの情報を提供します。hrProcessorLoad OID は、パケットを処理するコアの平均を提供します。

オブジェクト グループ	説明
	複数のデータプレーン (DPs) を有する PA-7000 と PA-5200 シリーズ ファイアウォールの場合は、個別のデータプレーン プロセッサの利用を監視できます。サービスの可用性の問題を回避するために、使用率が各 DP プロセッサの特定のしきい値に達したときにアラートを設定します。
hrSystem	システム アップタイム、現在のユーザー セッション数、現在のプロセス数などの情報を提供します。
hrStorage	使用中のストレージ量などの情報を提供します。

この MIB は RFC 2790 に定義されています。

ENTITY-MIB

ENTITY-MIB は、複数の論理および物理コンポーネントの OID を提供します。システムにロードされている物理コンポーネント（ファンや温度センサーなど）を判別し、モデルやシリアル番号などの関連情報を確認するには、この MIB を使用します。これらのコンポーネントのインデックス番号を使用して、 ENTITY-SENSOR-MIBおよび ENTITY-STATE-MIBでその動作状態を判別することもできます。

Palo Alto Networks ファイアウォール、Panorama、WF-500アプライアンスでは、以下のentPhysicalTable グループのみをサポートしています。

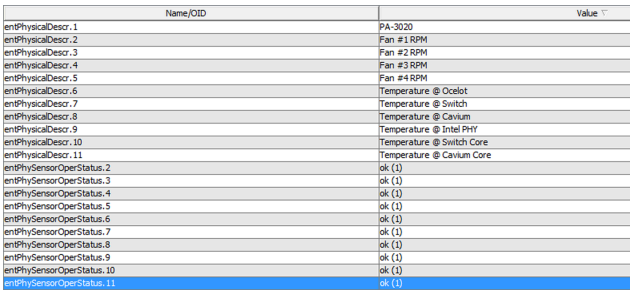
オブジェクト	説明
entPhysicalIndex	ディスク スロットとディスク ドライブを含む単一の名前空間。
entPhysicalDescr	コンポーネントの説明。
entPhysicalVendorType	sysObjectID (PAN-PRODUCT-MIB.my を参照) が使用可能な場合 (シャーシおよびモジュール オブジェクト)。
entPhysicalContainedIn	このコンポーネントが含まれるコンポーネントの entPhysicalIndex の値。
entPhysicalClass	シャーシ（3）、スロットのコンテナ（5）、電源（6）、ファン（7）、温度またはその他の環境それぞれのセンサー（8）、各ラインカードのモジュール（9）。
entPhysicalParentRelPos	兄弟コンポーネント内における、この「子」コンポーネントの相対的位置。兄弟コンポーネントは、entPhysicalContainedIn および entPhysicalClass オブジェクトのそれぞれについて同じインスタンス値を共有する entPhysicalEntry コンポーネントとして定義されます。

オブジェクト	説明
entPhysicalName	管理（MGT）インターフェイスでライン カードの命名が許可されている場合にのみサポートされます。
entPhysicalHardwareRev	コンポーネントのベンダー固有のハードウェア リビジョン。
entPhysicalFirwareRev	コンポーネントのベンダー固有のファームウェア リビジョン。
entPhysicalSoftwareRev	コンポーネントのベンダー固有のソフトウェア リビジョン。
entPhysicalSerialNum	コンポーネントのベンダー固有のシリアル番号。
entPhysicalMfgName	コンポーネントの製造元名。
entPhysicalMfgDate	コンポーネントの製造日。
entPhysicalModelName	ディスクのモデル番号。
entPhysicalAlias	ネットワーク マネージャがコンポーネントに指定したエイリアス。
entPhysicalAssetID	ネットワーク マネージャがコンポーネントに指定した、ユーザー割り当てのアセット追跡識別子。
entPhysicalIsFRU	コンポーネントがフィールド交換可能ユニット（FRU）かどうかを示します。
entPhysicalUris	コンポーネントの Common Language Equipment Identifier （CLEI）番号（URN:CLEI:CNME120ARA など）。

この MIB は RFC 4133 に定義されています。

ENTITY-SENSOR-MIB

ENTITY-SENSOR-MIB は、ENTITY-MIBでは定義されていないネットワーク機器の物理センサーのサポートを追加します。システムの物理コンポーネント（ファン、温度センサーなど）の動作状態をモニターするには、この MIB を ENTITY-MIB と併用します。たとえば、環境条件に起因する問題をトラブルシューティングする場合、ENTITY-MIB のエンティティ インデックス（entPhysicalDescr オブジェクト）を、ENTITY-SENSOR-MIB の動作状態値（entPhysSensorOperStatus オブジェクト）にマッピングできます。以下の例では、PA-3020 ファイアウォールのすべてのファンと温度センサーは動作しています。



Name/OID	Value
entPhysicalDescr.1	PA-3020
entPhysicalDescr.2	Fan #1 RPM
entPhysicalDescr.3	Fan #2 RPM
entPhysicalDescr.4	Fan #3 RPM
entPhysicalDescr.5	Fan #4 RPM
entPhysicalDescr.6	Temperature @ Ocelot
entPhysicalDescr.7	Temperature @ Switch
entPhysicalDescr.8	Temperature @ Cavium
entPhysicalDescr.9	Temperature @ Intel PHY
entPhysicalDescr.10	Temperature @ Switch Core
entPhysicalDescr.11	Temperature @ Cavium Core
entPhySensorOperStatus.2	ok (1)
entPhySensorOperStatus.3	ok (1)
entPhySensorOperStatus.4	ok (1)
entPhySensorOperStatus.5	ok (1)
entPhySensorOperStatus.6	ok (1)
entPhySensorOperStatus.7	ok (1)
entPhySensorOperStatus.8	ok (1)
entPhySensorOperStatus.9	ok (1)
entPhySensorOperStatus.10	ok (1)
entPhySensorOperStatus.11	ok (1)

システム プラットフォームが異なると、同じ *OID* が異なるセンサーを示す場合があります。対象プラットフォームで値と説明を照合するには、*ENTITY-MIB* を使用します。

Palo Alto Networks ファイアウォール、Panorama、WF-500アプライアンスでは、以下の entPhySensorTable グループのみをサポートしています。システムでは、温度（摂氏温度）センサーとファン（RPM）センサーのみをサポートしています。

ENTITY-SENSOR-MIB は RFC 3433 に定義されています。

ENTITY-STATE-MIB

ENTITY-STATE-MIBは、ENTITY-MIBが定義するもの以外にも、シャーシベースのプラットフォームにおけるコンポーネントの管理状態や運用状態など、物理コンポーネントの状態に関する情報を提供します。 この MIB は、ENTITY-MIB と組み合わせて、PA-7000 シリーズまたは PA-5450 ファイアウォールのコンポーネント（ラインカード、ファン トレイ、電源など）の動作状態を監視するために使用します。たとえば、脅威ログのログ転送に関する問題をトラブルシューティングする場合、ENTITY-MIB のログ処理カード（LPC）のインデックス（entPhysicalDesc オブジェクト）を ENTITY-STATE-MIB の動作状態値（entStateOper オブジェクト）にマッピングできます。運転状態値は数字を使って状態を表します。1:未知、2：無効、3：有効、4：試験PA-7000 シリーズと PA-5450 ファイアウォールは、この MIB をサポートする唯一の Palo Alto Networks ファイアウォールです。

ENTITY-STATE-MIB は RFC 4268 に定義されています。

IEEE 802.3 LAG MIB

IEEE 802.3 LAG MIB を使用して、リンク集約制御プロトコル (集約インターフェイス グループ内の LACP) が有効になっている集約グループのステータスを監視します。ファイアウォールは、LACP イベントをログに記録するとき、トラブルシューティングに役立つトラップも生成します。たとえば、このトラップにより、ファイアウォールと LACP ピア間のトラフィックの中断が、接続の切断によるものか、インターフェイス速度とデュプレックス値の不一致によるものかがわかります。

PAN-OS では、以下の LACP 用 SNMP テーブルを実装しています。

dot3adTablesLastChanged オブジェクト は、*dot3adAggTable*、*dot3adAggPortListTable*、および *dot3adAggPortTable* の最終変更日時を示しています。

表	説明
集約設定テーブル（dot3adAggTable）	このテーブルには、ファイアウォールに関連付けられているすべての集約グループに関する情報が含まれます。集約グループごとに 1 つのエントリがあります。 一部のテーブル オブジェクトには制限があります。これは、dot3adAggIndex オブジェクトで説明されています。このインデックスは、ローカル システムが集約グループに割り当てる一意の識別子です。包含するオブジェクトの下位管理対象オブジェクト間で集約グループ インスタンスを識別します。識別子は読み取り専用です。 *ifTable MIB*（インターフェイス エントリのリスト）は論理インターフェイスをサポートしていません。そのため、集約グループのエントリはありません。
集約ポート リスト テーブル（dot3adAggPortListTable）	このテーブルには、ファイアウォールの各集約グループに関連付けられているポートがリストされます。集約グループごとに 1 つのエントリがあります。 dot3adAggPortListPorts 属性には、集約グループに関連付けられているポートの完全なセットがリストされます。リスト内の各ビット セットがポート メンバーを表します。非シャーシ プラットフォームの場合、これは 64 ビット値です。シャーシ プラットフォームの場合、値は 8 個の 64 ビット エントリからなる配列です。
集約ポート テーブル（dot3adAggPortTable）	このテーブルには、ファイアウォールの集約グループに関連付けられているすべてのポートに関する LACP 設定情報が含まれます。ポートごとに 1 つのエントリがあります。このテーブルには、集約グループに関連付けられていないポートのエントリはありません。
LACP 統計テーブル（dot3adAggPortStatsTable）	このテーブルには、ファイアウォールの集約グループに関連付けられているすべてのポートに関するリンク集約情報が含まれます。ポートごとに 1 行があります。このテーブルには、集約グループに関連付けられていないポートのエントリはありません。

IEEE 802.3 LAG MIB には、以下の LACP 関連のトラップが含まれています。

トラップ名	説明
panLACPLostConnectivityTrap	ピアでファイアウォールへの接続が失われました。
panLACPUnresponsiveTrap	ピアがファイアウォールに応答しません。
panLACPNegoFailTrap	ピアとの LACP ネゴシエーションが失敗しました。

トラップ名	説明
panLACPSpeedDuplexTrap	ファイアウォールとピアのリンク速度とデュプレックス設定が一致しません。
panLACPLinkDownTrap	集約グループのインターフェイスがダウンしています。
panLACPLacpDownTrap	集約グループからインターフェイスが削除されました。
panLACPLacpUpTrap	集約グループにインターフェイスが追加されました。

MIB 定義については、IEEE 802.3 LAG MIB を参照してください。

LLDP-V2-MIB.my

リンク層検出プロトコル (LLDP) イベントを監視するには、LLDP-V2-MIB を使用します。たとえば、何らかの理由で破棄された LLDP フレームの数を調べるには、lldpV2StatsRxPortFramesDiscardedTotal オブジェクトを確認できます。Palo Alto Networks ファイアウォールは、LLDP を使用して隣接するデバイスとその機能を検出します。LLDP により、トラブルシューティングが容易になります（特に ping または traceroute ユーティリティでファイアウォールが検出されないバーチャル ワイヤー デプロイメントの場合）。

Palo Alto Networks ファイアウォールでは、以下を除くすべての LLDP-V2-MIB オブジェクトをサポートしています。

- 以下の lldpV2Statistics オブジェクト:
  - lldpV2StatsRemTablesLastChangeTimeIPv6
  - lldpV2StatsRemTablesInsertsIPv6
  - lldpV2StatsRemTablesDeletesIPv6
  - lldpV2StatsRemTablesDropsIPv6
  - lldpV2StatsRemTablesAgeoutsIPv6
- 以下のlldpV2RemoteSystemsData オブジェクト:
  - lldpV2RemOrgDefInfoTable テーブル
  - lldpV2RemTable テーブル内の lldpV2RemTimeMark

この MIB は RFC 4957 に定義されています。

BFD-STD-MIB

双方向送信検出 (BFD)MIB を使用してインターフェイス、データリンク、実際のエンジンなどの 2 つの転送エンジンの間の双方向パスの障害アラートをモニターおよび受信します。例えば、bfdSessState オブジェクトを確認して、転送エンジン間の BFD セッションを検証できます。Palo Alto Networks 導入環境下では、転送エンジンの1つがファイアウォールのインターフェイスとなり、他方が隣接して設定されたBFDピアとなります。

この MIB は RFC 7331 に定義されています。

PAN-COMMON-MIB.my

Palo Alto Networks ファイアウォール、Panorama、WF-500アプライアンスの以下の情報をモニターするには、PAN-COMMON-MIB を使用します。

オブジェクト グループ	説明
panSys	システムのソフトウェア/ハードウェア バージョン、ダイナミック コンテンツ バージョン、シリアル番号、HA モード/状態、グローバル カウンタなどのオブジェクトが含まれます。 グローバル カウンタには、サービス拒否（DoS）、IP フラグメンテーション、TCP 状態、ドロップされたパケットに関連するグローバル カウンタが含まれます。これらのカウンタを追跡することで、DoS 攻撃、システムまたは接続の障害、リソース制限から発生したトラフィックの異常をモニターできます。PAN-COMMON-MIB では、ファイアウォールのグローバル カウンタはサポートしていますが、Panorama のグローバル カウンタはサポートしていません。
panChassis	シャーシ タイプと M-Series アプライアンス モード（Panorama またはログ コレクタ）。
panSession	セッション使用状況に関する情報。たとえば、ファイアウォールまたは特定の仮想システム上のアクティブ セッションの総数などです。
panMgmt	ファイアウォールから Panorama 管理サーバーへの接続の状態。
panGlobalProtect	GlobalProtect ゲートウェイ使用率、最大許容トンネル数、アクティブ トンネル数。
panLogCollector	ロギング速度、ログ割り当て、ディスク使用状況、保持期間、ログの冗長性（有効あるいは無効）、ファイアウォールからログコレクタへの転送ステータス、ログコレクタから外部サービスへの転送ステータス、ファイアウォールからログコレクタへの接続ステータスを含む、各ログコレクタのロギング統計情報。
panDeviceLogging	ロギング速度、ディスク使用状況、保持期間、個々のファイアウォールから Panorama および外部サーバーへの転送ステータス、ファイアウォールからログコレクタへの接続ステータスを含む、各ファイアウォールのロギング統計情報。

PAN-GLOBAL-REG-MIB.my

PAN-GLOBAL-REG-MIB.my には、Palo Alto Networks エンタープライズ MIB モジュールのさまざまなサブツリーに対するグローバルな最上位 OID 定義が含まれます。ユーザーがモニターするオブジェクトは含まれておらず、必要になるのは他の MIB から参照される場合のみです。

PAN-GLOBAL-TC-MIB.my

PAN-GLOBAL-TC-MIB.my には、Palo Alto Networks エンタープライズ MIB モジュール内のオブジェクトのテキスト値に関する規則（文字長や許容される文字など）が定義されています。すべての Palo Alto Networks 製品がこの規則に従います。ユーザーがモニターするオブジェクトは含まれておらず、必要になるのは他の MIB から参照される場合のみです。

PAN-LC-MIB.my

PAN-LC-MIB.my には、ログ コレクタ（ログ コレクタ モードの M-Series アプライアンス）が実装する管理対象オブジェクトの定義が含まれます。ロギング率、ログ データベースの保存期間（日数）、ログ コレクタ上の各論理ディスク（最大 4 個）のディスク使用量（MB）をモニターするには、この MIB を使用します。たとえば、この情報を使用して、ログ コレクタをさらに追加するか、またはログを外部サーバー（Syslog サーバーなど）に転送してアーカイブするかを判断することができます。

PAN-PRODUCT-MIB.my

PAN-PRODUCT-MIB.my には、すべての Palo Alto Networks 製品の sysObjectID OID が定義されます。ユーザーがモニターするオブジェクトは含まれておらず、必要になるのは他の MIB から参照される場合のみです。

PAN-ENTITY-EXT-MIB.my

このMIB をサポートしている唯一の Palo Alto Networks ファイアウォールである PA-7000 シリーズまたは PA-5450 ファイアウォールの物理コンポーネント（ファントレイ、電源など）の電力使用量を監視するには、 PAN-ENTITY-EXT-MIB.my をENTITY-MIBと一緒に使用します。たとえば、ログ転送に関する問題をトラブルシューティングする際に、ログ処理カード（LPC）の電力使用量を確認することがあります。その場合、ENTITY-MIB の LPC インデックス（entPhysicalDescr オブジェクト）を PAN-ENTITY-EXT-MIB の値（panEntryFRUModelPowerUsed オブジェクト）にマッピングできます。

PAN-TRAPS.my

生成されたすべてのトラップとそれらに関する情報（説明など）の完全なリストを表示するには、PAN-TRAPS.my を使用します。Palo Alto Networks firewalls、Panorama、および WF-500 アプライアンスがサポートするトラップのリストについては、PAN-COMMON-MIB.my **panCommonEvents** > **panCommonEvents** > **panCommonEventEventsV2** オブジェクトを参照してください。

ログを HTTP/S 宛先に転送

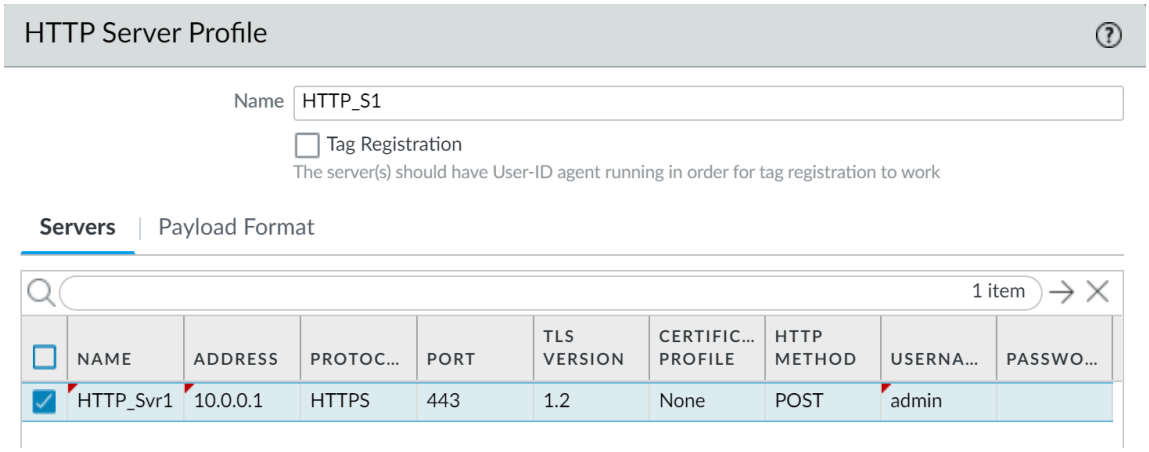
firewall と Panorama™ はログを HTTP/S サーバに転送できる。すべてのログを転送するか特定のログを転送するか選択し、イベントが発生した際に外部の HTTP ベースのサービスのアクションをトリガーすることができます。ログを HTTP サーバーに転送する場合、ファイアウォールが HTTP ベースの API リクエストをサードパーティのサービスに直接送信し、ファイアウォール ログの属性に基づいてアクションをトリガーするよう設定します。API を公開している任意の HTTP ベースのサービスと協働できるようファイアウォールを設定し、HTTP 要求の URL、HTTP ヘッダー、パラメータ、ペイロードを統合ニーズに合わせて変更できます。

STEP 1 | HTTP サーバープロファイルを作成し、ログを HTTP/S 宛先に転送します。

HTTP サーバプロファイルを使えば、サーバーにアクセスする方法を指定したり、HTTP/S の宛先に転送するログのフォーマットを定義したりできます。デフォルトでは、ファイアウォールは管理ポートを使用してログを転送します。ただし、**Device** > **Setup** > **Services** > **Service Route Configuration**.{ では、別のソース インターフェイスと IP アドレスを割り当てることができます。

1. **Device (デバイス)** > **Server Profiles (サーバプロファイル)** > **HTTP** を選択して新しいプロファイルを **Add (追加)** します。
2. サーバプロファイルの **Name**（名前）を指定し、**Location**（場所）を選択します。プロファイルは、すべての仮想システムで **Shared (共有)** することも、特定の仮想システムに所属させることもできます。
3. 各サーバーの詳細を**Add**（追加）します。各プロファイルにはサーバーを 4 個まで登録できます。
4. **Name (名前)** と IP **Address (アドレス)** を入力します。
5. **Protocol (プロトコル)**（**HTTP** または **HTTPS**）を選択します。デフォルトの **Port**（ポート）は 80 あるいは 443 のいずれかですが、このポート番号を変更し、HTTP サーバーがリッスンするポートにマッチさせることができます。
6. サーバーがサポートしている **TLS Version (TLS** バージョン**)**（**1.0**、**1.1**、または**1.2**（デフォルト））を選択します。
7. サーバーとの TLS 接続で使用する **Certificate Profile (**証明書プロファイル**)**を選択します。
8. サードパーティのサービスがサポートする **HTTP Method (HTTP** メソッド**)**（**DELETE**、**GET**、**POST**（デフォルト）、または**PUT**）を選択します。
9. （任意）必要であればサーバーへの認証に使う **Username (**ユーザー名**)** および **Password (**パスワード**)** を入力します。

10. （任意）**Test Server Connection (**サーバー接続のテスト**)** を選択し、ファイアウォールと HTTP/S サーバー間のネットワーク接続を検証します。

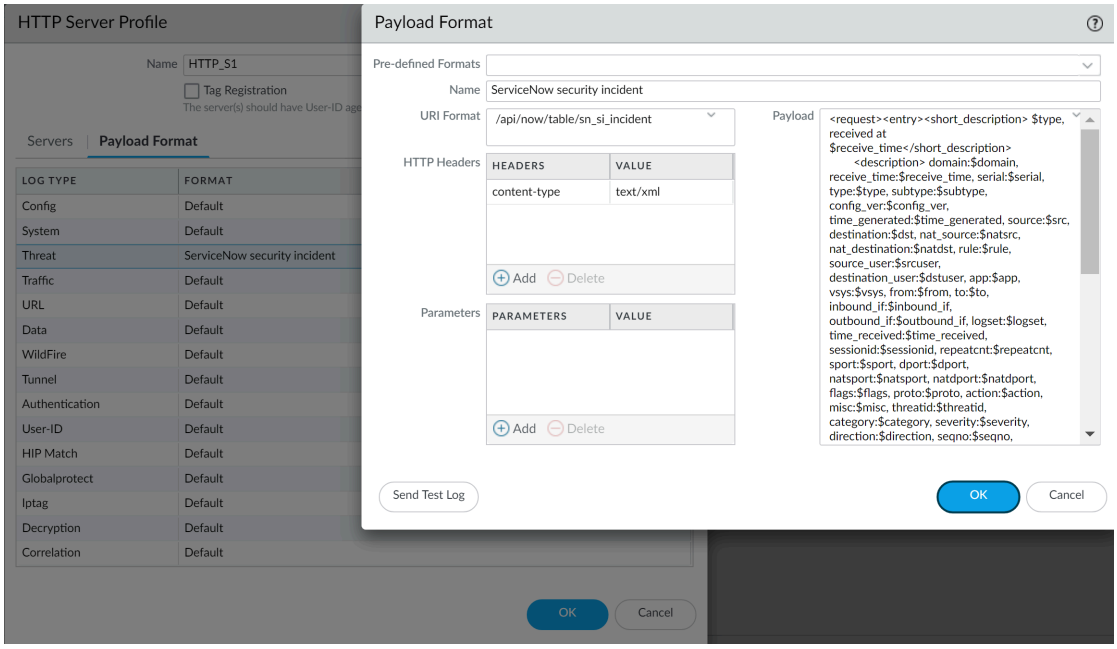


STEP 2 | その HTTP リクエストの **Payload Format (**ペイロードの形式**)** を選択します。

1. HTTP リクエストの形式を定義したい各ログ タイプ毎に **Log Type (**ログ タイプ**)** リンクを選択します。
2. **Pre-defined Formats (**定義済みのフォーマット**)**(コンテンツ更新を通して利用可能) を選択するか、カスタム フォーマットを作成します。

   カスタム形式を作成する場合、**URI** は HTTP サービス上のリソースのエンドポイントになります。ファイアウォールは、ユーザーが事前に定義した IP アドレスに URI を付加して、HTTP リクエストの URL を構築します。URI とペイロードの形式が、サードパーティ ベンダーが要求する構文に一致することを確認してください。選択したログ タイ

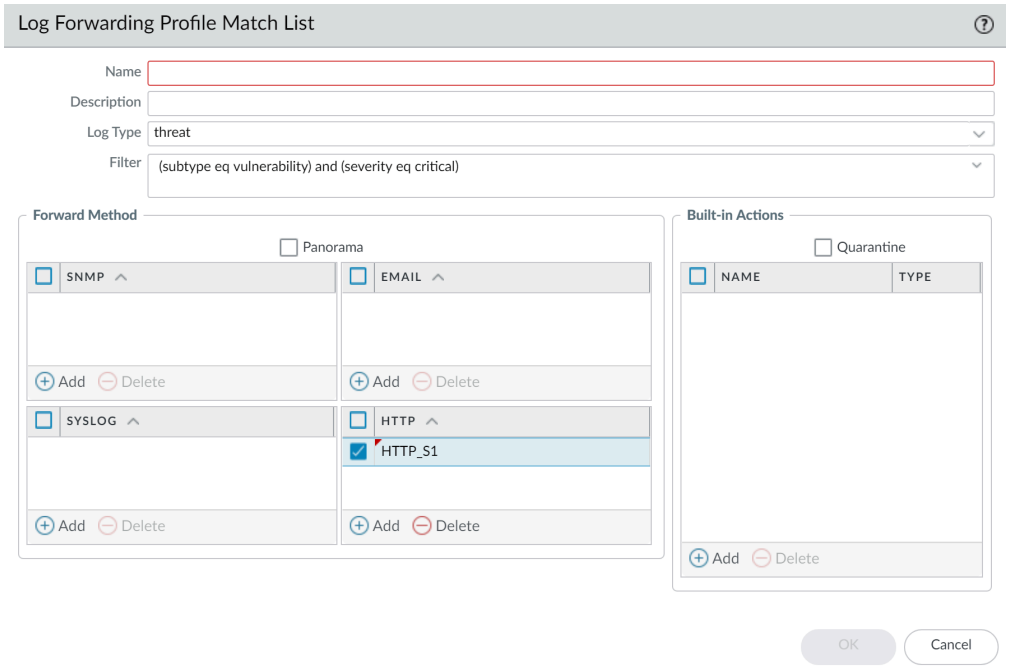
プでサポートされる任意の属性を HTTP ヘッダー、パラメータと値のペア、および要求ペイロード内で使用できます。



3. **Send Test Log (**テスト ログを送信**)** し、HTTP サーバーがそのリクエストを受信することを確認します。テスト ログをインタラクティブに送信する際、ファイアウォールはそのフォーマットをそのまま使い、変数をファイアウォール ログの値と置換することはありません。HTTP サーバーが 404 レスポンスを送信する場合、パラメータ用の値を提供し、サーバーがリクエストを正常に処理できるようにします。

STEP 3 | ファイアウォールが HTTP サーバーにログを転送する場面を決める一致条件を定義し、使用する HTTP サーバープロファイルを添付します。

1. ワークフローを開始したいログ タイプを選択します。
   - ユーザーアクティビティに関連するログ用に（たとえば、トラフィック、脅威、または認証ログ）、ログ転送プロファイル（**Objects (オブジェクト)** > **Log Forwarding (ログ転送)**）を追加します。
   - 構成ログやシステム ログなど、システムイベントに関連するログに対して **Device (デバイス)** > **Log Settings (ログ設定)** を選択します。
2. Log Type (ログ タイプ) を選択し、新しい **Filter Builder (フィルタ ビルダー)** を使って一致条件を定義します。
3. HTTP の宛先にログを転送するための HTTP サーバープロファイルを **Add (追加)** します。



NetFlow モニタリング

NetFlow は、ファイアウォールがインターフェイスに侵入する IP トラフィックに関する統計情報をエクスポートするために使用できる業界標準のプロトコルです。ファイアウォールは、その統計を NetFlow フィールドとして NetFlow コレクタにエクスポートします。NetFlow コレクタは、セキュリティ、管理、アカウント管理、およびトラブルシューティングの目的でネットワーク トラフィックを分析するために使用するサーバーです。すべての Palo Alto Networks ファイアウォールで NetFlow バージョン 9 がサポートされます。このファイアウォールでは、双方向ではなく、一方向の NetFlow のみをサポートします。ファイアウォールでは、インターフェイス上のすべての IP トラフィックに対して NetFlow 処理が実行されます。サンプリング NetFlow はサポートされていません。レイヤー 3、レイヤー 2、Virtualwire、tap、VLAN、ループバック、およびトンネルの各インターフェイスの NetFlow レコードをエクスポートできます。Ethernet の集約サブインターフェースの場合、グループ内でデータが流れる個々のサブインターフェースのレコードをエクスポートできます。NetFlow コレクターで firewall インターフェイスを識別するには、SNMP マネージャおよび NetFlow コレクタのファイアウォール インターフェイス識別子を参照してください。ファイアウォールは、スタンダードとエンタープライズ（PAN-OS専用）NegFlow のテンプレートをサポートしており、NetFlowコレクターがNetFlowフィールドを解読するために使用するものです。

- NetFlow エクスポートの設定
- NegFlow のテンプレート

NetFlow エクスポートの設定

NetFlow コレクタを使用して、ネットワーク トラフィックの入力ファイアウォール インターフェイスを分析するには、次の手順を実行して、NetFlow レコード のエクスポートを設定します。

STEP 1 | NetFlow サーバー プロファイルを作成します。

このプロファイルは、エクスポートされたレコードを受信する NetFlow コレクタを定義し、エクスポートのパラメータを指定します。

1. **Device (デバイス)** > **Server Profiles (サーバープロファイル)** > **NetFlow** を選択してプロファイルを **Add (追加)** します。
2. プロファイルを識別する **Name**（名前）を入力します。
3. NetFlow コレクタの要件に従って、ファイアウォールが NetFlow テンプレートを更新するレートを **Minutes**（分）（デフォルトは 30）および **Packets**（パケット）（エク

スポートされたレコード—デフォルトは 20）で指定します。どちらかのしきい値を超えると、ファイアウォールはテンプレートを更新します。

4. ファイアウォールがレコードをエクスポートする頻度として、分単位で **Active Timeout (**アクティブ タイムアウト**)** を指定します（デフォルトは 5）。
5. ファイアウォールで App-ID フィールドとユーザー ID フィールドをエクスポートする場合は、**PAN-OS Field Types (PAN-OS** フィールド タイプ**)** を選択します。
6. レコードを受け取る各 NetFlow コレクタ を **Add (**追加**)** します（プロファイル毎に 2 件まで）。コレクタ毎に次の項目を指定します。
   - コレクタを識別する **Name (**名前**)** を入力します。
   - **NetFlow Server (NetFlow** サーバー**)** のホスト名あるいは IP アドレス。
   - アクセス **Port (**ポート**)**（デフォルトは 2055）。
7. **OK** をクリックしてプロファイルを保存します。

STEP 2 | NetFlow サーバ プロファイルを、分析するトラフィックが受信しているファイアウォール インターフェイスに割り当てます。

この例では、プロファイルを既存の Ethernet インターフェイスに割り当てます。

1. **Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** > **Ethernet (**イーサネット**)** を選択し、インターフェイス名をクリックして編集します。

   レイヤー 3、レイヤー 2、*Virtualwire*、*tap*、*VLAN*、ループバック、およびトンネルの各インターフェイスの *NetFlow* レコードをエクスポートできます。集約イーサネット・インターフェースの場合、グループ内でデータが流れる個々のサブインターフェースのレコードをエクスポートできます。
2. 設定した NetFlow サーバープロファイル（**NetFlow Profile (NetFlow** プロファイル**)**）を選択し、**OK** をクリックします。

STEP 3 | **(PA-7000 Series**、**PA-5400 Series**、および **PA-5200** シリーズのファイアウォール に必要**)** ファイアウォールが NetFlow レコードを送信するために使用するインターフェイスのサービス ルートを設定します。

管理 (MGT) インターフェイスを使用して、PA-7000 Series、PA-5400 Series、および PA-5200 Series ファイアウォールから NetFlow レコードを送信することはできません。他のファイアウォール モデルの場合、サービスルートは任意項目です。すべてのファイアウォールについて、NetFlow レコードを送信するインターフェイスが、ファイアウォールがレコードを収集するインターフェイスと異なっていても構いません。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）を選択します。

2. （仮想システムが複数あるファイアウォール）次のいずれかを選択します。
   - **Global (グローバル)**—サービスルートがファイアウォール上のすべての仮想システムに適用される場合はこのオプションを選択します。
   - **Virtual Systems (仮想システム)**—サービスルートが特定の一つの仮想システムに適用される場合はこのオプションを選択します。**Location (場所)** を仮想システムに設定します。
3. **Service Route Configuration (サービスルート設定)** および Customize (カスタマイズ) を選択します。
4. インターフェイスが使用するプロトコル（**IPv4** あるいは **IPv6**）を選択します。必要な場合は、両方のプロトコル用のサービスルートを設定できます。
5. Service (サービス) 列で **Netflow** をクリックします。
6. **Source Interface (ソース インターフェイス)** を選択します。

   任意の、デフォルト、および ***MGT*** は、*PA-7000 Series*、*PA-5400 Series*、または *PA-5200 Series* ファイアウォールから *NetFlow* レコードを送信するための有効なインターフェイス オプションではありません。
7. **Source Address (送信元アドレス)**（IP アドレス）を選択します。
8. **OK** を2回クリックして変更内容を保存します。

STEP 4 | 変更をコミットします。

STEP 5 | NetFlow コレクタでファイアウォール トラフィックをモニターします。

NetFlow コレクタのドキュメントを参照してください。

統計をモニターする場合、*NetFlow* コレクタのインターフェイス インデックスをファイアウォール *Web* インターフェイスのインターフェイス名と照合する必要があります。詳細については、SNMP マネージャおよび NetFlow コレクタのファイアウォール インターフェイス識別子を参照してください。

NetFlow の配信に関する問題のトラブルシューティングを行うには、CLI コマンド **debug log-receiver netflow statistics** を使用します。

NegFlow のテンプレート

NetFlow コレクタは、テンプレートを使用してファイアウォールがエクスポートするフィールドを復号化します。ファイアウォールはエクスポートするデータのタイプに応じてテンプレートを選択します：IPv4またはIPv6トラフィック、NATを使用するかどうか、フィールドは標準のものかエンタープライズ固有(PAN-OS 固有) のものか。ファイアウォールは定期的に各テンプレートを更新して、（エクスポートされたデータのタイプが変わった場合は）どのテンプレートを使用するかを再評価し、選択したテンプレートのフィールドに変更があれば適用します。NetFlow エクスポートの設定を行う際、NetFlow コレクタの要件に従い、時間間隔およびエクスポートされたレコード数に基づいて更新頻度を設定します。どちらかのしきい値を超えると、ファイアウォールはテンプレートを更新します。

Palo Alto Networks ファイアウォールでは、以下の NetFlow テンプレートをサポートしています。

Template（テンプレート）	ID
IPv4 標準	256
IPv4 エンタープライズ	257
IPv6 標準	258
IPv6 エンタープライズ	259
NAT を使用する IPv4 標準	260
NAT を使用する IPv4 エンタープライズ	261
NAT を使用する IPv6 標準	262
NAT を使用する IPv6 エンタープライズ	263

以下の表に、ファイアウォールで送信できる NetFlow のフィールド、およびそれらを定義するテンプレートの一覧を示します。

Value	項目	説明	Templates（テンプレート）
1	IN_BYTES	IP フローに関連付けられているバイト数を示す、長さ N * 8 ビットの受信カウンタ。デフォルトで、N は 4 です。	すべてのテンプレート
2	IN_PKTS	IP フローに関連付けられているパケット数を示す、長さ N * 8 ビットの受信カウンタ。デフォルトで、N は 4 です。	すべてのテンプレート
4	PROTOCOL	IP プロトコル バイト。	すべてのテンプレート
5	TOS	入力インターフェイスに入るときの Type of Service バイトの設定。	すべてのテンプレート
6	TCP_FLAGS	このフローでのすべての TCP フラグの合計。	すべてのテンプレート

Value	項目	説明	Templates（テンプレート）
7	L4_SRC_PORT	TCP/UDP 送信元ポート番号（たとえば、FTP、Telnet、または同等のポート）。	すべてのテンプレート
8	IPV4_SRC_ADDR	IPv4 送信元アドレス。	IPv4 標準 IPv4 エンタープライズ NAT を使用する IPv4 標準 NAT を使用する IPv4 エンタープライズ
10	INPUT_SNMP	インターフェイスのインデックスを入力します。値の長さはデフォルトで 2 バイトですが、それより大きな値になることもあります。Palo Alto Networks のファイアウォールがインターフェイスのインデックスを生成する方法の詳細については、SNMP マネージャおよび NetFlow コレクタのファイアウォール インターフェイス識別子を参照してください。	すべてのテンプレート
11	L4_DST_PORT	TCP/UDP 宛先ポート番号（たとえば、FTP、Telnet、または同等のポート）。	すべてのテンプレート
12	IPV4_DST_ADDR	IPv4 宛先アドレス。	IPv4 標準 IPv4 エンタープライズ NAT を使用する IPv4 標準 NAT を使用する IPv4 エンタープライズ
14	OUTPUT_SNMP	インターフェイスのインデックスを出力します。値の長さはデフォルトで 2 バイトですが、それよ	すべてのテンプレート

Value	項目	説明	Templates（テンプレート）
		り大きな値になることもあります。Palo Alto Networks のファイアウォールがインターフェイスのインデックスを生成する方法の詳細については、SNMP マネージャおよび NetFlow コレクタのファイアウォール インターフェイス識別子を参照してください。	
21	LAST_SWITCHED	このフローの最後のパケットが切り替えられたときのシステムのアップタイム（ミリ秒単位）。	すべてのテンプレート
22	FIRST_SWITCHED	このフローの最初のパケットが切り替えられたときのシステムのアップタイム（ミリ秒単位）。	すべてのテンプレート
27	IPV6_SRC_ADDR	IPv6 送信元アドレス。	IPv6 標準 IPv6 エンタープライズ NAT を使用する IPv6 標準 NAT を使用する IPv6 エンタープライズ
28	IPV6_DST_ADDR	IPv6 宛先アドレス。	IPv6 標準 IPv6 エンタープライズ NAT を使用する IPv6 標準 NAT を使用する IPv6 エンタープライズ
32	ICMP_TYPE	ICMP （Internet Control Message Protocol）パケット タイプ。以下のように報告されます。 ICMP タイプ * 256 + ICMP コード	すべてのテンプレート

Value	項目	説明	Templates（テンプレート）
61	DIRECTION	フロー方向: • 0 = 入力 • 1 = 出力	すべてのテンプレート
148	flowId	観察ドメイン内で一意のフローの ID。IP アドレスやポート番号などのフロー キーが報告されないか、別個のレコードで報告される場合は、この情報要素を使用して、異なるフローを区別することができます。flowID はトラフィックおよび脅威ログのセッション ID フィールドに対応しています。	すべてのテンプレート
233	firewallEvent	以下のファイアウォール イベントを示します。 • 0 = 無視（不正）—使用されていません。 • 1 = フロー作成済み—NetFlow データのレコードは新しいフロー用です。 • 2 = フロー検知済み—NetFlow データのレコードはフロー終了用です。 • 3 = フロー拒否—NetFlow データのレコードは、ファイアウォール ポリシーが拒否したフローを示します。 • 4 = フロー アラート—使用されていません。 • 5 = フロー更新—NetFlow データのレコードは、NetFlow サーバープロファイルで設定された **Active Timeout (**アクティブ タイムアウト**)** の期間よりも長く持続する 長期持続フロー用に送信されます。	すべてのテンプレート
225	postNATSourceIPv4Address	この情報要素の定義は、パケットがインターフェイスを通過した後	NAT を使用する IPv4 標準

Value	項目	説明	Templates（テンプレート）
		のネットワーク アドレス変換時にファイアウォールによって生成された変更値を報告する点を除いて、sourceIPv4Address の定義と同一です。	NAT を使用する IPv4 エンタープライズ
226	postNATDestinationIPv4Address	この情報要素の定義は、パケットがインターフェイスを通過した後のネットワーク アドレス変換時にファイアウォールによって生成された変更値を報告する点を除いて、sourceIPv4Address の定義と同一です。	NAT を使用する IPv4 標準 NAT を使用する IPv4 エンタープライズ
227	postNAPTSourceTransportPort	この情報要素の定義は、パケットがインターフェイスを通過した後のネットワーク アドレス変換時にファイアウォールによって生成された変更値を報告する点を除いて、sourceTransportPort の定義と同一です。	NAT を使用する IPv4 標準 NAT を使用する IPv4 エンタープライズ
228	postNAPTDestinationTransportPort	この情報要素の定義は、パケットがインターフェイスを通過した後のネットワーク アドレス変換時にファイアウォールによって生成された変更値を報告する点を除いて、destinationTransportPort の定義と同一です。	NAT を使用する IPv4 標準 NAT を使用する IPv4 エンタープライズ
281	postNATSourceIPv6Address	この情報要素の定義は、パケットがインターフェイスを通過した後の NAT64 ネットワーク アドレス変換時にファイアウォールによって生成された変更値を報告する点を除いて、情報要素 sourceIPv6Address の定義と同一です。IPv6 ヘッダーの送信元アドレス フィールドの定義については、RFC 2460 を参照してください。NAT64 仕様については、RFC 6146 を参照してください。	NAT を使用する IPv6 標準 NAT を使用する IPv6 エンタープライズ

Value	項目	説明	Templates（テンプレート）
282	postNATDestinationIPv6Address	この情報要素の定義は、パケットがインターフェイスを通過した後の NAT64 ネットワーク アドレス変換時にファイアウォールによって生成された変更値を報告する点を除いて、情報要素 sourceIPv6Address の定義と同一です。IPv6 ヘッダーの宛先アドレス フィールドの定義については、RFC 2460 を参照してください。NAT64 仕様については、RFC 6146 を参照してください。	NAT を使用する IPv6 標準 NAT を使用する IPv6 エンタープライズ
346	privateEnterpriseNumber	これは、Palo Alto Networks を識別する一意のプライベート エンタープライズ番号です。25461.	IPv4 エンタープライズ NAT を使用する IPv4 エンタープライズ IPv6 エンタープライズ NAT を使用する IPv6 エンタープライズ
56701	App-ID	App-ID によって特定されるアプリケーションの名前。名前の最大長は 32 バイトです。	IPv4 エンタープライズ NAT を使用する IPv4 エンタープライズ IPv6 エンタープライズ NAT を使用する IPv6 エンタープライズ
56702	User-ID	ユーザー ID によって特定されるユーザー名。名前の最大長は 64 バイトです。	IPv4 エンタープライズ NAT を使用する IPv4 エンタープライズ

Value	項目	説明	Templates（テンプレート）
			IPv6 エンタープライズ NAT を使用する IPv6 エンタープライズ

SNMP マネージャおよび NetFlow コレクタのファイアウォール インターフェイス識別子

NetFlow コレクタ（NetFlow モニタリングを参照）または SNMP マネージャ（SNMP モニタリングおよびトラップを参照）を使用して Palo Alto Networks ファイアウォールをモニターする場合、インターフェイス インデックス（SNMP ifindex オブジェクト）によって、特定のフローを伝送したインターフェイスを識別します（SNMP マネージャのインターフェイス インデックスを参照）。一方、ファイアウォール Web インターフェイスは、インデックスではなくインターフェイス名を識別子として使用します（ethernet1/1 など）。NetFlow コレクタまたは SNMP マネージャに表示される統計がそれぞれどのファイアウォール インターフェイスに適用されるのかを理解するには、インターフェイス インデックスをインターフェイス名と照合できなければなりません。

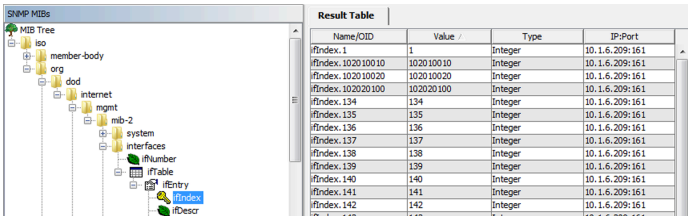


図 **3 : SNMP** マネージャのインターフェイス インデックス

ファイアウォールがインデックスの計算に使用する式を理解すれば、インデックスを名前と照合することができます。この式はプラットフォームとインターフェイス タイプ（物理または論理）によって異なります。

物理インターフェイスのインデックスの範囲は 1 ～ 9999 で、ファイアウォールでは以下のようにして計算します。

ファイアウォールのプラットフォーム	計算式	インターフェイス インデックスの例
VM-Series	管理ポート数 + 物理ポートのオフセット • 管理ポート数—これは 1 の定数です。 • 物理ポートのオフセット — これは物理ポート番号です。	VM-100 ファイアウォール、Eth1/4 = 1（管理ポート数） + 4（物理ポートのオフセット）= **5**
PA-220、PA-220R、PA-800 Series	管理ポート数 + 物理ポートのオフセット • 管理ポート数—これは5 の定数です。	PA-5200 シリーズのファイアウォール、Eth1/4 = 5（管理ポート数） + 4（物理ポートのオフセット）= **9**

ファイアウォールのプラットフォーム	計算式	インターフェイス インデックスの例
	• 物理ポートのオフセット – これは物理ポート番号です。	
PA-3200 Series、PA-5200 Series	管理ポート数 + 物理ポートのオフセット • 管理ポート数–これは 4 の定数です。 • 物理ポートのオフセット – これは物理ポート番号です。	PA-5200 シリーズのファイアウォール、Eth1/4 = 4（管理ポート数） + 4（物理ポートのオフセット）= **8**
PA-7000シリーズ	（最大ポート数 * スロット） + 物理ポート オフセット + 管理ポート数 • 最大ポート数–これは 64 の定数です。 • スロット – これは、ネットワーク インターフェイス カードのシャーシのスロット番号です。 • 物理ポートのオフセット – これは物理ポート番号です。 • 管理ポート数–これは5 の定数です。	PA-7000 シリーズのファイアウォール、Eth3/9 = [64 （最大ポート数）* 3（スロット）] + 9（物理ポート）+ 5（管理ポート数）= **206**

すべてのプラットフォームにおいて、論理インターフェイスのインデックスは、ファイアウォールが以下のようにして計算する 9 桁の数字です。

インターフェイスタイプ	範囲	9 桁	7 ～ 8 桁	5 ～ 6 桁	1 ～ 4 桁	インターフェイス インデックスの例
レイヤー 3 サブインターフェイス	101010001-199999999	Type:2	インターフェイス スロット：1-9 (01-09)	インターフェイス ポート：1-9 (01-09)	サブインターフェイス: サフィックス 1 ～ 999 （0001 ～ 9999）	Eth1/5.22 = 10000000（タイプ）+ 10000（スロット）+ 5000 （ポート）+ 2（サフィックス）= **101050022**

インターフェイスタイプ	範囲	9 桁	7 ～ 8 桁	5 ～ 6 桁	1 ～ 4 桁	インターフェイス インデックスの例
レイヤー 2 サブインターフェイス	101010001-199999999	type:2	インターフェイス スロット：1-9 (01-09)	インターフェイス ポート：1-9 (01-09)	サブインターフェイス: サフィックス 1 ～ 999 （0001 ～ 9999）	Eth2/3.6 = 10000000 （タイプ）+ 20000 （スロット）+ 3000 （ポート）+ （サフィックス）= **102030006**
vwire サブインターフェイス	101010001-199999999	type:2	インターフェイス スロット：1-9 (01-09)	インターフェイス ポート：1-9 (01-09)	サブインターフェイス: サフィックス 1 ～ 999 （0001 ～ 9999）	Eth4/2.312 = 10000000 （タイプ）+ 40000 （スロット）+ 2000 （ポート）+ 31 （サフィックス）= **104020312**
VLAN	200000001～200099999	type:2	00	00	VLAN サフィックス1-9999 (0001-9999)	VLAN.55 = 20000000 （タイプ）+ 5 （サフィックス）= **200000055**
ループバック	300000001 ～ 300009999	type:3	00	00	ループバックサフィックス：1-9999 (0001-9999)	Loopback.55 = 30000000 （タイプ）+ 5 （サフィックス）= **300000055**
トンネル	400000001 ～ 400009999	type:4	00	00	トンネル サフィックス：1-9999 (0001-9999)	Tunnel.55 = 40000000 （タイプ）+ 5 （サフィックス）= **400000055**
集約グループ	500010001 ～ 500089999	type:5	00	AE サフィックス1-8 (01-08)	サブインターフェイス: サフィックス 1 ～ 999 （0001 ～ 9999）	AE5.99 = 50000000 （タイプ）+ 5000 （AE サフィックス）+ 9 （サフィックス）= **500050099**

トランシーバーを監視する

物理アプライアンスまたはデバイスのトランシーバーのステータスを監視して、インストールとトラブルシューティングを容易にできます。表示可能な診断は、送信バイアス電流、送信電力、受信電力、トランシーバー温度、および電源電圧です。トランシーバーの監視をサポートするデバイスのリストについては、以下を参照してください。

- PA-800シリーズ
- PA-3200シリーズ
- PA-5200シリーズ
- PA-5450 Firewall
- PA-7000シリーズ

command line interface (コマンド ライン インターフェース - CLI) を使用して、トランシーバーの監視を実行します。使用可能なすべての CLI コマンドについては、以下の表を参照してください。

互換性のないトランシーバーでコマンドを実行すると、 *CLI* は読み取り不可能な診断情報に対して「*n/a*」を返します。

CLI	定義
`show transceiver <interface name>`	指定されたトランシーバーの概要が各診断の値と共に表示されます。 例: `admin@PA-7080> show transceiver ethernet11/25` CLI は、温度、電圧、電流、送信電力、および受信電力の値を返します。
`show transceiver-detail <interface name>`	ベンダー情報やリンク長など、より詳細なトランシーバー仕様を受け取ります。CLI は、より詳細な診断情報も提供します。
`show transceiver all`	すべてのアクティブなトランシーバーのリストと、それぞれの診断の概要を表示します。
`show transceiver-detail all`	デバイス内の各トランシーバーの包括的な詳細を取得します。

User-ID

IP アドレスとは対照的に、ユーザーの識別は効果の高いセキュリティ インフラに欠かせない要素です。誰がネットワーク上の各アプリケーションを使い、誰が脅威を伝搬した可能性があり、誰がファイルを転送中であるのか把握することで、セキュリティポリシーを強固なものにして、インシデントに素早く対応できるようになります。Palo Alto Networks のファイアウォールの標準機能である User-ID™ により、多彩なレポジトリに保存されているユーザー情報を活用できるようになります。以下のトピックでは、User-ID の詳細とその設定方法を説明します。

User-ID の概要

User-ID™ により、様々なテクニックを使用してネットワーク上のすべてのユーザーを識別したり、Microsoft Windows、Apple iOS、Mac OS、Android、Linux®/UNIX を含む様々なオペレーティングシステムやアクセス方式を使用して、あらゆるロケーションにいるユーザーを確実に識別したりできるようになります。IP アドレス以外の情報も含めてユーザーを把握することで、次のことを実現できます。

- 可視性–ユーザーに基づいたアプリケーション使用の可視性を向上することで、ネットワーク アクティビティのより適切な全体像を得られます。ネットワークに不審な、あるいは普段見かけないアプリケーションがあるのに気付いた際、User-ID の力が発揮されます。セキュリティチームは ACC あるいはログビューアを使用することで、アプリケーションやユーザーの性質、帯域幅およびセッションの消費量、アプリケーション トラフィックの送信元および宛先や、関連する脅威があるかどうかなどを認識することができます。
- ポリシー制御–ユーザー情報をセキュリティポリシールールと紐付けることで、ネットワークを横断するアプリケーションをさらに安全に有効化できるようになり、そのアプリケーションを使うビジネス ニーズを持つユーザーだけにアクセスを限定することができます。例えば、人材サービス（WorkdayやService Nowなど）にアクセスし得るSaaSアプリケーションなど、一部のアプリケーションはネットワーク上の既知のユーザーがすべて利用できなくてはなりません。しかし、もっと機密度の高いアプリケーションの場合、そのアプリケーションにアクセスする必要があるユーザーのみを許可することで、攻撃の入り口を減らすことができます。例えば、ITサポート担当者はリモート デスクトップ アプリケーションにアクセスする正当な理由がある場合がありますが、他の大抵のユーザーはそうではありません。
- ロギング、レポート、フォレンジック–セキュリティ インシデントの発生時には、IP アドレスだけでなくユーザー情報に基づくフォレンジック分析とレポートにより、そのインシデントの全体像をより正確に把握できます。例えば、事前定義済みのユーザー/グループ アクティビティを使用し、各ユーザーあるいはユーザーグループの Web アクティビティの概要を確認したり、SaaS アプリケーションの利用状況レポートを使用し、制限されていない SaaS アプリケーションを通じてデータの大部分を転送しているユーザーを確認したりできます。

ユーザーおよびグループ ベースのポリシーを実施するには、ファイアウォールで受信するパケットの IP アドレスをユーザー名にマッピングできる必要があります。User-ID には、このユーザー マッピング情報を収集するための多くのメカニズムが用意されています。たとえば、ユーザー ID エージェントは、サーバー ログのログイン イベントのモニター、認証サービスから送信された Syslog メッセージの受信とユーザー識別処理を行います。エージェントがマップしなかった IP アドレスのマッピングを識別するために、HTTP 要求を Authentication Portal ログイン画面にリダイレクトするように認証ポリシーを構成することができます。ユーザーマッピングのメカニズムを環境に合わせてカスタマイズでき、異なるサイトで別々のメカニズムを使用することまで可能です。これにより、すべてのユーザーに対し、あらゆるロケーションで、常にアプリケーションへのアクセスを安全に有効化できます。

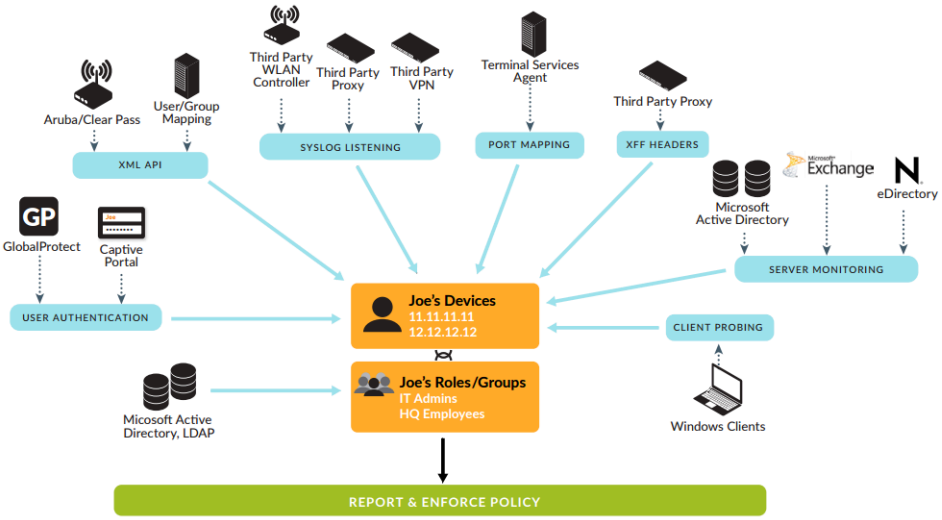


図 4 : User-ID

エージェントがマッピングしていない IP アドレスからの通信をユーザー識別させるためには、HTTP 要求をキャプティブ ポータルのログイン画面にリダイレクトするように設定することができます。ファイアウォールは、LDAP ディレクトリー・サーバーに直接接続するか、ディレクトリー・サーバーとの XML API 統合を使用して、Group Mapping（グループ マッピング）情報を収集します。

User-ID の動作についてはユーザー ID の概念を、User-ID のセットアップ手順についてはユーザー ID の有効化を参照してください。

ユーザー *ID* は、ファイアウォールが *IP* アドレスをユーザー名にマッピングする前にユーザーの送信元 *IP* アドレスに *NAT* 変換が適用される環境では機能しません。

ユーザー ID の概念

- Group Mapping（グループ マッピング）
- ユーザー マッピング

Group Mapping（グループ マッピング）

ユーザーまたはグループに基づいてポリシー ルールを定義するには、まず、ファイアウォールがディレクトリ サーバーに接続して認証を受ける方法を定義する LDAP サーバー プロファイルを作成します。ファイアウォールは、Microsoft Active Directory (AD)、Novell eDirectory、Sun ONE Directory Server を含む、さまざまなディレクトリ サーバーをサポートしています。サーバー プロファイルでは、ファイアウォールがディレクトリを検索して、グループのリストおよび対応するメンバーのリストを取得する方法をも定義します。ファイアウォールがネイティブでサポートしていないディレクトリ サーバーを使用している場合、XML API を使用してグループ マッピング機能を統合できます。その後、ユーザー対グループのマッピングおよびユーザーおよびグループ ベースのポリシーの有効化へのグループマッピング構成を作成できます。

個々のユーザーではなくグループ メンバーシップに基づいてポリシー ルールを定義すると、新しいユーザーがグループに追加されるたびにルールを更新する必要がなくなるため、管理が簡略化されます。グループ マッピングを設定するときに、ポリシー ルールで使用できるグループを制限できます。ディレクトリ サービスにすでに存在するグループを指定するか、LDAP フィルタに基づいてカスタム グループを定義できます。カスタム グループの定義は、新しいグループを作成したり、LDAP サーバー上の既存のグループを変更したりするよりも簡単に行うことができ、LDAP 管理者の介入も必要ありません。User-IDは、フィルタに一致するすべての LDAP ディレクトリ ユーザーをカスタム グループにマッピングします。例えば、マーケティング部門の請負業者がソーシャル ネットワーキング サイトにアクセスできるようなセキュリティポリシーが必要だとします。その部門の Active Directory グループが存在しない場合、LDAP 属性 Department が Marketing に設定されているユーザーに一致する LDAP フィルタを設定できます。ユーザー グループに基づいたログ クエリおよびレポートには、カスタム グループが含まれます。

ユーザー マッピング

ユーザーおよびグループの名前を知ることは、問題を解決するための出発点に過ぎません。また、ファイアウォールは、セキュリティー ルールを適切に適用できるように、どの IP アドレスがどのユーザーにマップされているかを知る必要があります。User-ID の概要は、ネットワーク上のユーザーとグループを識別するために使用されるさまざまな方法を示し、ユーザー マッピングとグループ マッピングが連携して、ユーザーおよびグループ ベースのセキュリティの適用と可視性を実現する方法を示します。以下のトピックでは、ユーザー マッピングのさまざまな方法について説明します。

- サーバー モニタリング
- ポート マッピング
- Syslog
- XFF ヘッダー

- ユーザー名 ヘッダの挿入
- 認証ポリシーおよび認証ポータル
- グローバルな保護
- XML API
- クライアントのプローブ

サーバー モニタリング

サーバー モニタリングを使用すると、ユーザー ID エージェント (ネットワーク内のドメイン サーバー上で実行される Windows ベースのエージェント、またはファイアウォール上で実行される PAN-OS 統合ユーザー ID エージェント) は、指定された Microsoft Exchange Server、ドメイン コントローラ、または Novell eDirectory サーバーのセキュリティ イベント ログのログイン イベントをモニターします。たとえば、AD 環境では、ユーザー ID エージェントを設定して、Kerberos チケットの付与または更新、Exchange サーバー アクセス(設定されている場合)、およびファイルと印刷サービスの接続のセキュリティ ログをモニターできます。これらのイベントをセキュリティ ログに記録するには、アカウントのログイン完了イベントを記録するように AD ドメインを設定する必要があります。さらに、ユーザーはドメイン内の任意のサーバーにログインできるため、すべてのユーザー ログイン イベントをキャプチャするには、すべてのサーバーに対してサーバー モニタリングをセットアップする必要があります。詳細については、Windows User-ID エージェントを使用したユーザー マッピングの設定またはPAN-OS 統合 User-ID エージェントを使用したユーザー マッピングの設定を参照してください。

ポート マッピング

Microsoft Terminal Server や Citrix 環境など、マルチ ユーザー システム環境の場合、多くのユーザーが同じ IP アドレスを共有します。このような場合、ユーザー対 IP アドレスのマッピング プロセスで、クライアントごとの送信元ポートの情報が必要となります。このタイプのマッピングを実行するには、Windows/Citrix のターミナル サーバー自体に Palo Alto Networks ターミナル サーバー エージェントをインストールし、さまざまなユーザー プロセスに対する送信元ポートの割り当てを仲介する必要があります。Linux ターミナル サーバーのようにターミナル サーバー エージェントをサポートしないターミナル サーバーの場合、XML API を使用して、ユーザー マッピング情報をログイン イベントおよびログアウト イベントからユーザー ID に送信できます。設定の詳細については、「ターミナル サーバー ユーザー向けのユーザー マッピング設定」を参照してください。

XFF ヘッダー

ネットワーク上のユーザーとファイアウォールの間にプロキシ サーバーがデプロイされている場合、ファイアウォールは、プロキシ サーバーの IP アドレスを、コンテンツを要求したクライアントの IP アドレスではなく、プロキシが転送する HTTP/HTTPS トラフィックの送信元 IP アドレスと見なすことがあります。多くの場合、プロキシ サーバーは、コンテンツを要求したクライアントまたは要求の送信元クライアントの実際の IPv4 または IPv6 アドレスが含まれているトラフィック パケットに、X-Forwarded-For （XFF）ヘッダーを追加します。このような場合、XFF からエンド ユーザーの IP アドレスを抽出して、User-ID がその IP アドレスをユーザー名にマッピングできるようにファイアウォールを設定できます。これにより、 XFF 値をポリシーに使用して、送信元ユーザーをログに記録し、ユーザーベースのポリシーを適用してから、プロキシ サーバーの背後にあるユーザーの Web ベースへのアクセスを安全にします。

ユーザー名 ヘッダの挿入

Palo Alto Networks ファイアウォールを使用してセカンダリ エンフォースメント デバイスを設定し、ユーザーベースのポリシーを実施する場合、セカンダリ デバイスにファイアウォールからの IP アドレスからユーザー名へのマッピングがない場合があります。ユーザーの身分証明をダウンストリーム デバイスに送信するには、プロキシなどの追加のデバイスの展開が必要になるか、ユーザーのエクスペリエンスに悪影響を及ぼすことがあります（たとえば、ユーザーが複数回ログインする必要がある）。ユーザーの発信トラフィックの HTTP ヘッダーにドメインとユーザー名をダイナミックに追加して、Palo Alto Networks ファイアウォールで使用するすべてのセカンダリ デバイスがユーザーの情報を受信し、ユーザーベースのポリシーを適用できるようにすることができます。トラフィックヘッダーにユーザー名とドメインを挿入することによりユーザーの身分証明を含むことで、ユーザーエクスペリエンスや追加インフラストラクチャの展開に悪影響を与えることなく、ユーザーベースのポリシーを適用できます。

認証ポリシーおよび認証ポータル

場合によっては、User-ID エージェントは、サーバー監視や他の方法（たとえば、ユーザーがログインしていないか、ドメイン サーバーがサポートしない Linux などのオペレーティング システムを使用している場合など）を使用して IP アドレスをユーザー名にマップすることはできません。ユーザー ID エージェントがユーザー マッピングを実行するために使用する方法に関係なく、機密アプリケーションにアクセスするときにユーザーが認証されるようにする場合があります。これらすべてのケースに対して、 認証ポリシーの設定と認証ポータルを使用して IP アドレスをユーザー名にマップするよう構成できます。認証ポリシー ルールに一致するすべての Web トラフィック（HTTP または HTTPS）は、認証ポータルから認証するようにユーザーに求めます。以下の 認証ポータルの認証方式 を使用できます:

- ブラウザ チャレンジ–ユーザーが応答しなければならないログイン要求の数を減らすには、Kerberos シングル サインオン認証を使用します。
- Web フォーム– マルチ ファクター認証、SAML シングル サインオン、 Kerberos、 TACACS+、RADIUS、LDAP、またはローカル認証を使用します
- クライアント証明書認証。

Syslog

ユーザーを認証するネットワーク サービスがすでに環境にある場合があります。これらのサービスには、ワイヤレス コントローラ 802.1x デバイス、Apple Open Directory サーバー、プロキシサーバー、およびその他のネットワーク アクセス制御（NAC）メカニズムなどが含まれます。これらのサービスがログインおよびログアウト イベントに関する情報を含む Syslog メッセージを送信するよう設定したり、User-ID エージェントがそのメッセージをパースするよう設定したりできますUser-ID エージェントはログイン イベントをパースして IP アドレスをユーザー名にマッピングし、ログアウト イベントをパースして古くなったマッピングを削除します。特に IP アドレスの割り当てが頻繁に変わる環境では、期限切れのマッピングを削除すると便利です。

PAN-OS 統合 User-ID エージェントおよび Windows ベースの User-ID エージェントはどちらも、Syslog 解析プロファイルを使用して Syslog メッセージをパースします。各サービスが異なるフォーマットでメッセージを送信するような環境では、各フォーマット用にカスタム プロファイルを作成し、複数のプロファイルを各 Syslog 送信者に割り当てることができます。PAN-OS 統合 User-ID エージェントを使用する場合、Palo Alto Networks がアプリケーション コンテ

ンツ更新を通して提供する事前定義済みの Syslog 解析プロファイルを使用することもできます。

User-ID エージェントが Syslog メッセージを解析するには、Syslog メッセージが次の条件を満たしている必要があります。

- 各メッセージは 1 行の文字列であること。改行として許可されている区切り文字は、改行 (**\n**) またはキャリッジ リターンと改行 (**\r\n**) です。
- 各メッセージの最大サイズは 8,000 byte (バイト)です。
- UDP 上で送信されたメッセージは 1 つのパケットに含まれること。SSL 上で送信されたメッセージは複数パケットにまたがることができる。1 つのパケットは複数のメッセージを含むことができる。

構成の詳細については、User-ID を設定してユーザーマッピング用に Syslog 送信者を監視を参照してください。

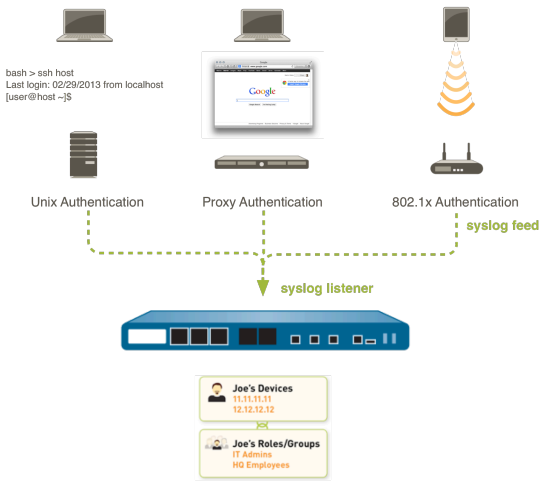


図 **5 :** ユーザー **ID** の **Syslog** との統合

グローバルな保護

モバイル ユーザーやローミング ユーザーの場合、GlobalProtect エンドポイントからユーザーマッピング情報がファイアウォールに直接提供されます。この場合、すべての GlobalProtect ユーザーは、ファイアウォールへの VPN アクセスのためのログイン認証情報を入力する必要があるアプリをエンドポイント上で実行しています。その後、このログイン情報は、可視化およびユーザーベース セキュリティ ポリシーの実施のために、ファイアウォール上のユーザー ID ユーザー マッピング テーブルに追加されます。GlobalProtect ユーザーがネットワークにアクセスするには認証が必要なため、IP アドレス対ユーザー名のマッピングは明確に分かります。これは、アプリケーションやサービスへのアクセスを許可するためにユーザーが誰であるかを知る必要がある機密環境では最適なソリューションです。GlobalProtect のセットアップの詳細は、『GlobalProtect 管理者ガイド』を参照してください。

XML API

認証ポータルおよびその他の標準的なユーザー マッピング方法は一部のユーザー アクセス タイプには機能しない場合があります。例えば、標準手法はサードパーティの VPN ソリューションから接続するユーザーや、802.1x 対応のワイヤレス ネットワークに接続するユーザーのマッピングを追加することはできません。その場合、PAN-OS XML API を使用して、ログインイベントをキャプチャーし、PAN-OS 統合 User-ID エージェントに送信できます。詳細は XML API を使用した User-ID へのユーザー マッピングの送信 を参照してください。

クライアントのプローブ

*Palo Alto Networks*は、高セキュリティネットワークでユーザ*ID*情報を取得する推奨方法ではないため、クライアントプローブを無効にすることを強くお勧めします。

Palo Alto Networksは、次の潜在的なリスクのためにクライアントプローブを使用することはお勧めしません。

- クライアントプローブはエンドポイントから報告されたデータを信頼するため、誤って構成された場合にセキュリティ リスクにさらされる可能性があります。外部の信頼されていないインターフェイスで有効にすると、クライアントプローブがクライアントプローブに送信され、ユーザー名、ドメイン名、パスワードハッシュなどの機密情報が含まれる場合、ネットワーク外の User-ID エージェント サービス アカウントが使用されます。サービス アカウントを正しく構成しないと、攻撃者が資格情報を悪用してネットワークに侵入してさらにアクセスする可能性があります。
- クライアント プロービングは、大部分のユーザーが内部ネットワーク上の Windows ワークステーション上に存在する古いネットワーク用に設計されており、様々なデバイスやオペレーティングシステム上のローミングやモバイル ユーザーベースをサポートする今日のモダンなネットワークには最適ではありません。
- クライアントプローブは、(マップされた IP アドレスの合計数に基づいて) 大量のネットワーク トラフィックを生成できます。

代わりに、Palo Alto Networksでは、ユーザーマッピングに次の代替方法を使用することを強くお勧めします。

- ドメイン コントローラや Syslog または XML API との統合など、分離された信頼できるソースを使用して、デバイスの種類やオペレーティング システムからユーザー マッピング情報を安全にキャプチャする。
- 認証ポリシーと認証ポータル を設定して、許可されたユーザーにのみアクセスを許可するようにします。

User-ID エージェントは、次の 2 種類のクライアント プローブをサポートします。

- NetBIOS プローブは、Windows ユーザー ID エージェントを使用します。
- 汎 OS 統合ユーザー ID エージェントまたは Windows ユーザー ID エージェントのいずれかを使用する WMI プローブ。

クライアントの調査はユーザー マッピングの方法としてはお勧めしませんが、それを有効にする予定の場合は、*Palo Alto Networks* は *NetBIOS* プローブを介して *WMI* プローブを使用することを強くお勧めします。

Microsoft Windows 環境では、Windows 管理インストルメンテーション (WMI) または NetBIOS プローブを定期的に使用してクライアント システムをプローブするように User-ID エージェントを構成し、既存のユーザー マッピングがまだ有効であることを確認したり、まだマップされていない IP アドレスのユーザー名を取得したりできます。

信頼できるゾーンでプローブを有効にすることを選ぶ場合、同じユーザーがまだログインしていることを確認するため、取得された各 IP アドレスがエージェントで定期的 (デフォルトでは 20 分ごとですが、これは設定可能です) にプローブされます。また、ユーザー マッピングが存在しない IP アドレスがファイアウォールで発生すると、アドレスがエージェントに送信されてプローブが直ちに行われます。

詳細については、「Windows ユーザ ID エージェント を使用してユーザ マッピングを設定する」または「PAN-OS 統合ユーザ ID エージェント を使用してユーザ マッピングを設定する」を参照してください。

ユーザー ID の有効化

IP アドレスとは対照的に、ユーザーの識別は効果の高いセキュリティ インフラに欠かせない要素です。誰がネットワーク上の各アプリケーションを使い、誰が脅威を伝搬した可能性があり、誰がファイルを転送中であるのか把握することで、セキュリティポリシーを強固なものにして、インシデントに素早く対応できるようになります。User-ID により、多彩なレポジトリに保存されているユーザー情報を活用し、可視性、ユーザーおよびグループベースのポリシー制御、ロギング、レポート、フォレンジックの改善のために役立てることができます。

STEP 1 | ユーザーベースのアクセス制御を必要とする要求を送信するユーザーを含む送信元ゾーンで、ユーザー ID を有効にします。

User-ID は信頼されたゾーンでのみ有効にしてください。外部の信頼されていないゾーン（インターネットなど）で *User-ID* およびクライアントによるプローブを有効にすると、保護されたネットワークの外にプローブが送信される可能性があります。これにより、*User-ID* エージェントのサービス アカウント名、ドメイン名、暗号化されたパスワード ハッシュの情報が漏洩し、保護されているサービスおよびアプリケーションに攻撃者が不正アクセスできるようになる場合があります。

1. **Network (ネットワーク)** > **Zones (ゾーン)** の順に選択し、ゾーンの**Name (名前)** をクリックします。
2. **Enable User Identification (ユーザー ID の有効化)** を行って **OK** をクリックします。

STEP 2 | ユーザーID エージェントの専用サービス アカウントを作成します。

ベストプラクティスとして、有効化する *User-ID* オプションをサポートするために必要となる最小限の権限だけを持ったサービス アカウントを作成し、サービス アカウントが悪用された際に攻撃の入り口が少なくなるようにします。

これは、ユーザーのログインおよびログアウト イベント用に Windows ベースの User-ID エージェントあるいは PAN-OS 統合 User-ID エージェントを使用して、ドメイン コントローラ、Microsoft Exchange Server、あるいは Windows クライアントを監視する予定である場合に必須になります。

STEP 3 | ユーザー対グループのマッピング。

これにより、ファイアウォールが LDAP ディレクトリに接続してグループ マッピング情報を取得できるようになるため、ポリシーを作成する際にユーザー名およびグループ名を選択できるようになります。

STEP 4 | IP アドレス対ユーザーのマッピング

ベストプラクティスとして、高セキュリティのネットワーク上でクライアント プロービングをユーザーマッピングの方法として有効化しないようにしてください。クライアントに対するプローブでは、大量のネットワーク トラフィックが生成される場合があり、設定に誤りがあるとセキュリティ上の脅威が発生する可能性があります。

これを行う方法は、ユーザーのロケーション、ユーザーが使用しているシステムの種類、ネットワーク上でどのようなシステムを使ってユーザーのログインおよびログアウト イベントを収集しているのかによって左右されます。ユーザー マッピングを有効化するには、一つ以上の User-ID エージェントを設定する必要があります。

- Windows ユーザー ID エージェントを使用したユーザー マッピングの設定を行います。
- PAN-OS 統合 User-ID エージェントを使用したユーザー マッピングの設定を行います。
- User-ID を設定してユーザーマッピング用に Syslog 送信者を監視を行います。
- ターミナル サーバー ユーザー向けのユーザー マッピング設定を行います。
- XML API を使用した User-ID へのユーザー マッピングの送信を行います。
- 「HTTP ヘッダーにユーザー名の挿入」を行います。

STEP 5 | ユーザーマッピングに含めるネットワーク、除外するネットワークを指定します。

ベストプラクティスとして、必ず *User-ID* に含める、あるいは除外するネットワークを指定してください。これにより、信頼できるアセットだけがプロービングされるようになり、不要なユーザーマッピングが意図せず作成されなくなります。

どのネットワークを含めるか除外するかを指定する方法は、 Windows ベースの User-ID エージェントまたは PAN-OS 統合 User-ID エージェントのどちらを使用しているかによって異なります。

STEP 6 | 認証ポリシーおよび認証ポータルを設定します。

ファイアウォールは認証ポータルを使用して、エンドユーザーが 認証ポリシー ルールにマッチするサービス、アプリケーション、または URL カテゴリを要求した際に、ユーザーを認証します。認証中に収集されたユーザー情報に基づき、ファイアウォールは新しいユーザーマッピングを作成するか、既存のマッピングを更新します。認証中に収集されたマッピング情報は、他の User-ID 方式を通じて収集された情報をオーバーライドします。

1. 認証ポータルの設定を行います。
2. 認証ポリシーの設定を行います。

STEP 7 | ユーザーおよびグループ ベースのポリシーを有効化します。

できる限りユーザーではなくグループに基づいてルールを作成します。これにより、ユーザー ベースが変更するたびにルールを更新(コミットが必要)し続ける必要がなくなります。

User-ID を設定すると、セキュリティ ルールの送信元および宛先を定義するときに、ユーザー名またはグループ名を選択できるようになります。

1. **Policies (ポリシー)** > **Security (セキュリティ)** を選択し、新しいルールを **Add (追加)** するか、既存のルールの名前を変更します。
2. **User (ユーザー)** を選択し、次のいずれかの方法で、ルールでマッチさせるユーザーおよびグループを指定します。
   - 一致基準としてユーザー/グループを選択する場合は、Source User (送信元ユーザー) セクションで **Add (追加)** をクリックすると、ファイアウォールのグループ マッピング機能により検出されたユーザーおよびグループのリストが表示されます。ルールに追加するユーザーあるいはグループを選択します。
   - 正常に認証されたかどうかに関係なく任意のユーザーと一致し、特定のユーザー名またはグループ名を把握する必要がない場合は、Source User [送信元ユーザー]リストの上にあるドロップダウンから **known-user** [既知のユーザー]または **unknown** [不明]を選択します。
3. 必要に応じてルールのその他の部分を設定し、**OK** をクリックして設定を保存します。セキュリティ ルールのその他のフィールドの詳細は、「基本的なセキュリティ ポリシーのセットアップ」を参照してください。

STEP 8 | セキュリティポリシールールを作成して信頼できるゾーン内で User-ID を安全に有効化し、User-ID トラフィックがネットワーク外に出ないようにします。

「インターネット ゲートウェイのセキュリティポリシーの推奨設定 」に従い、必ずエージェント（Windows エージェントおよび PAN-OS 統合エージェントの両方）がサービスを監視してファイアウォールにマッピングを配信しているゾーン内でのみ User-ID アプリケーション（`paloalto-userid-agent`）が許可されるようにします。具体的な内容は次のとおりです。

- エージェントが存在するゾーンおよび監視されているサービスが存在するゾーンの間（あるいは、エージェントをホストしている特定のシステムおよび監視されているサーバーの間の方がより好ましい）で `paloalto-userid-agent` アプリケーションを許可します。
- ユーザーマッピングを必要とするファイアウォールおよびエージェントの間、ユーザーマッピングを再配信しているファイアウォールおよびその情報を再配信しているファイアウォールの間で `paloalto-userid-agent` アプリケーションを許可します。
- インターネット ゾーンなど、すべての外部ゾーンで `paloalto-userid-agent` アプリケーションを拒否してください。

STEP 9 | ファイアウォールが X-Forwarded-For（XFF）ヘッダからユーザーの IP アドレスを取得するよう設定します。

ファイアウォールがインターネットおよびプロキシサーバーの間にある際、ファイアウォールに提供されるパケット内の IP アドレスは、ユーザーではなくプロキシサーバーのものです。その代わりにユーザーの IP アドレスが見えるようにするためには、ファイアウォールがユーザーマッピングで XFF ヘッダを使用するように設定します。このオプションが有効な場合、ファイアウォールがポリシーで参照されているユーザー名と IP アドレスをマッチさせ、その関連するユーザーおよびグループを把握・制御できるようになります。詳細は、「プロキシ サーバーを介して接続されたユーザーの識別」を参照してください。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Content-ID** の順に選択し、X-Forwarded-For Headers (X-Forwarded-For ヘッダー) 設定を編集します。
2. **X-Forwarded-For Header in User-ID (User-ID** 内の **X-Forwarded-For** ヘッダ**)** を選択します。

   Strip-X-Forwarded-For Header (X-Forwarded-For ヘッダーの除去**)** を選択しても、ポリシー ルールのユーザー属性では *XFF* ヘッダーの使用が無効になりません。ファイアウォールは、ユーザー属性に使用した後でのみ *XFF* 値をゼロに設定します。
3. **OK** をクリックして変更内容を保存します。

STEP 10 | high availability (高可用性 - HA) 設定を使用する場合は、同期を有効にします。

ベストプラクティスとして、*HA* 設定の ***Enable Config Sync***（設定同期の有効化）オプションを常に有効にして、グループマッピングとユーザーマッピングがアクティブ ファイアウォールとパッシブ ファイアウォールの間で確実に同期されるようにします。

1. **Device**（デバイス） > **High Availability**（高可用性） > **General**（全般）を選択し、Setup（セットアップ）セクションを編集します。
2. **Enable HA**（**HA** の有効化）を選択します。
3. **Enable Config Sync** （設定の同期化の有効化）を選択します。
4. **Peer HA1 IP Address (ピアHA1のIPアドレス)**– ピアファイアウォールのHA1コントロールリンクスのIPアドレスを入力します。
5. （任意） **Backup Peer HA1 IP Address (バックアップピアHA1のIPアドレス)**– ピアファイアウォールのHA1バックアップリンクのIPアドレスを入力します。
6. **OK** をクリックします。

STEP 11 | 変更をコミットします。

変更を **Commit (コミット)** し、それを有効化します。

STEP 12 | User-ID 設定の確認を行います。

ユーザーマッピングおよびグループ マッピングを設定した後、設定が正しく機能しており、ユーザーおよびグループによるアプリケーションとサービスに対するアクセスを安全に有効化・監視できることを確認します。

ユーザー対グループのマッピング

個々のユーザーではなくユーザー グループ メンバーシップに基づいてポリシー ルールを定義すると、グループ メンバーシップが変更されるたびにルールを更新する必要がなくなるため、管理が簡略化されます。各ファイアウォールまたは Panorama がすべてのポリシーで参照できる個別ユーザー グループの数はモデルによって異なります。詳細は、以下の互換性一覧を参照してください。

以下の手順により、ファイアウォールが LDAP ディレクトリに接続してグループ マッピング情報を取得できるようにします。その後、ユーザーおよびグループ ベースのポリシーの有効化を行えるようになります。

以下に、*Active Directory (AD)*環境でのグループ マッピングのベスト プラクティスを示します。

- ドメインが *1* つの場合、ファイアウォールを接続性が最も良いドメイン コントローラに接続する *LDAP* サーバー プロファイルを持つグループ マッピング設定が *1* つだけ必要です。冗長性を確保するために、ドメイン コントローラを *LDAP* サーバープロファイルに最大 *4* つまで追加できます。ドメインに複数のグループ マッピング設定を追加しても、単一のドメインではドメイン コントローラ *4* つを超える冗長性は確保できませんので、ご注意ください。
- 複数のドメインや複数のフォレストがある場合には、ファイアウォールを各ドメイン/フォレストのドメイン サーバーに接続する *LDAP* サーバープロファイルを持つグループ マッピング設定を作成する必要があります。異なるフォレスト内のユーザー名が一意になるようにする必要があります。
- ユニバーサルグループがある場合、先に *SSL* のポート番号*3268* または*3269* でグローバルカタログサーバーのルートドメインに接続する *LDAP* サーバー プロファイルを作成し、次にポート番号*389* でルートドメイン コントローラーに接続する別の *LDAP* サーバープロファイルを作成します。これにより、すべてのドメインとサブドメインでユーザーとグループの情報を利用できるようになります。
- グループ マッピングを使用する前に、ユーザーのセキュリティ ポリシーの ***Primary Username***（プライマリ ユーザー名）を設定します。この属性は、ポリシー設定、ログ、およびレポート内のユーザーを識別するためのものです。

STEP 1 | LDAP サーバー プロファイルを追加します。

このプロファイルでは、グループ マッピング情報の収集元となるディレクトリ サーバーへのファイアウォールの接続方法を定義します。

同じ識別名 *(DN)* または *LDAP* サーバーを使用する複数のグループマッピング設定を作成する場合、グループマッピング設定に重複するグループを含めることはできません *(*例：単一のグループ マッピング設定のインクルードリストに、 異なるグループマッピング設定を追加することはできない）。

1. **Device (**デバイス**)** > **Server Profiles (**サーバープロファイル**)** > **LDAP** を選択してサーバープロファイルを **Add (**追加**)** します。
2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
3. LDAP サーバーを **Add (**追加**)** します。プロファイルには、サーバーを 4 つまで追加できますが、同じ **Type** (タイプ)にする必要があります。各サーバーについて、**Name (**名前**)**（サーバーを識別するため）、**LDAP Server (**サーバー**)** の IP アドレスあるいは FQDN、およびサーバーの **Port (**ポート**)**（デフォルトは 389）を入力します。
4. サーバーの **Type (**タイプ**)** を選択します。

   選択内容（**active-directory (**アクティブディレクトリ**)** など）に基づいて、ファイアウォールは自動的に正しい LDAP 属性をグループ マッピング設定に入力します。ただし、LDAP スキーマをカスタマイズしている場合、デフォルトの設定を変更する必要があります。
5. **Base DN (**ベース **DN)** フィールドについては、ファイアウォールがユーザーおよびグループの検索を開始する LDAP ツリーの場所の識別名（DN）を入力します。
6. **Bind DN (**バインド **DN)** については、**Password (**パスワード**)** および **Confirm Password (**パスワードの確認**)** を入力し、LDAP ツリーにバインドする認証情報を入力します。

   Bind DN (バインド **DN)** は、完全修飾 LDAP 名（`cn=administrator,cn=users,dc=acme,dc=local` など）か、ユーザー プリンシパル名（`administrator@acme.local` など）にすることができます。
7. **Bind Timeout (**バインドのタイムアウト**)** および **Search Timeout (**検索タイムアウト**)** を秒単位で入力します（デフォルトはどちらも 30）。
8. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 2 | グループ マッピング設定のサーバー設定を指定します。

1. **Device (**デバイス**)** > **User Identification (**ユーザー **ID)** > **Group Mapping Settings (**グループ マッピング設定**)**の順に選択します。
2. グループ マッピング設定を **Add (**追加**)** します。
3. グループ マッピング設定の識別に使用する一意の**Name (**名前**)** を入力します。
4. 作成した LDAP **Server Profile** [LDAP サーバー プロファイル]を選択します。
5. (オプション) 更新間隔 (秒単位) を指定します。グループ マッピング設定の更新についてファイアウォールが LDAP ソースをチェックする頻度に基づいて、値 (範囲は 60～86,400、デフォルトは3,600) を入力します。LDAP ソースに多数のグループが含ま

れている場合、更新間隔が短かすぎると、すべてのグループをマッピングするのに十分な時間が確保できない可能性があります。

6. (任意)デフォルトでは、**User Domain** [ユーザー ドメイン]フィールドは空白になっています。空白のままにすると、ファイアウォールが、Active Directory (AD)サーバーのドメイン名を自動的に検出します。このフィールドに値を入力した場合、ファイアウォールがLDAPソースから取得したドメイン名はオーバーライドされます。ほとんどの設定では、値を入力する必要がある場合は、NetBIOS ドメイン名を入力します（たとえば、**`example.com`** ではなく **`example`**）。

   グローバル カタログを使用する場合、値を入力すると、このサーバーのすべてのユーザーとグループ（他のドメインのユーザーとグループを含む）のドメイン名が置き換えられます。

7. (任意)ファイアウォールで追跡する、グループ マッピングのグループをフィルタリングするには、Group Objects (グループ オブジェクト)セクションで、**Search Filter**（検索フィルタ）(LDAP クエリ)、**Object Class**（オブジェクト クラス）を入力します。

8. (任意)ファイアウォールで追跡する、グループ マッピングのユーザーをフィルタリングするには、User Objects (ユーザー オブジェクト)セクションで、**Search Filter**（検索フィルタ）(LDAP クエリ)、**Object Class**（オブジェクト クラス）（ユーザー定義）を入力します。

9. グループ マッピング設定が **Enabled (有効)** になっていることを確認します（デフォルトは有効）。

STEP 3 | （任意）ユーザーおよびグループのマッピング用に収集するユーザーおよびグループの属性を定義します。このステップは、ドメイン以外のディレクトリ属性に基づいてユーザーをマップする場合に必要です。

1. User-ID 送信元がユーザー名のみを送信し、かつ、そのユーザー名が組織全体で一意である場合は、**Device**（デバイス） > **User Identification**（ユーザー ID） > **User Mapping**（ユーザー マッピング） > **Setup**（セットアップ）を選択して、ファイアウォールによってグループマッピング中の LDAP サーバーから収集される一意のユーザー名がポリシーに関連付けられているユーザーと一致するかどうかを確認し、送信元プロファイル内のドメインがオーバライドされないようにするために、セットアップ セクションを **Edit**（編集）して **Allow matching usernames without domains**（ドメインが含まれていなくても **User-ID** ソースから収集したユーザー名を照合する）ようにします。

   このオプションを有効化する前に、マッピング情報を収集する *User-ID* ソース *(*GlobalProtectや認証ポータルなど*)* を含む *LDAP* グループのグループ マッピングを設定しておきます。変更をコミットすると、*User-ID* ソースはドメインなしのユーザー名を設定します。グループ マッピング中に収集されたユーザー名のみがドメインなしで照合できます。*User-ID* ソースがユーザー情報を複数の形式で送信し、このオプションを有効にする場合は、ファイアウォールによって収集された属性に固有のプレフィックスが付いていることを確認します。このオプションを有効にすると、ユーザーが正しく識別されるようにするには、グループ マッピングのすべての属性を一意にする必要があります。ユーザー名が一意でない場合、ファイアウォールはデバッグ ログにエラーを記録します。

2. **Device (デバイス)**、 > **User Identification (ユーザー ID)**、 > **Group Mapping Settings (グループ マッピング設定)**、 > **Add (追加)**、 > **User and Group Attributes (ユーザーおよびグループ属性)**、 > **User Attributes (ユーザー属性)**、を選択し、ユーザー識別のために収集したい **Directory Attribute (ディレクトリ属性)** を入力します。User-ID のソースからファイアウォールが受信する他のフォーマットをオーバーライドするログやレポートでユーザーを表し、ファイアウォール上でユーザーを識別する **Primary Username (プライマリ ユーザー名)**を指定します。

   サーバープロファイルの **Type (タイプ)**を選択する際、ファイアウォールはユーザーおよびグループ属性の値を自動的に補完します。User-ID 送信元が送信するユーザー情報に基づいて、正しい属性を設定する必要があります。

   - ユーザープリンシパル名 **(UPN)**: **`userPrincipalName`**
   - **NetBios** 名: **`sAMAccountName`**
   - 電子メール **ID**:該当の電子メールのディレクトリ属性
   - 複数の形式:User-ID ソースを有効にする前に、ユーザーディレクトリーからユーザーマッピング属性を取得します。

   プライマリユーザー名を指定しない場合、ファイアウォール はサーバープロファイルタイプごとに次のデフォルト値を使用します。

属性	アクティブディレクトリ	**Novell eDirectory** または **Sun ONE** ディレクトリ サーバー
プライマリ ユーザー名	`sAMAccountName`	`uid`
電子メール	`mail`	`mail`
代替 ユーザー名 1	`userPrincipalName`	None.
グループ 名	`name`	`cn`
グループ メンバー	`member`	`member`

3. （任意） **E-Mail**（電子メール）アドレス形式と最 3 つの **Alternate Username**（代替ユーザー名）形式を指定します。
4. **Device (デバイス)** > **User Identification (ユーザー ID)** > **Group Mapping Settings (グループ マッピング設定)** > **Add (追加)** > **User and Group Attributes (ユーザーおよびグループ属性)** > **Group Attributes (グループ属性)**を選択し、**Group Name (グループ名)**、**Group Member (グループ メンバー)**、**E-Mail (メール)**アドレスの書式を指定します。

   ファイアウォールが LDAP サーバーからディレクトリ属性を収集する前に、コミットする必要があります。

STEP 4 | ポリシー ルールで使用できるグループを制限します。

この作業は、ポリシー ルールを特定のグループに制限する場合にのみ必要です。**Group Include List (グループ含有リスト)**リストと **Custom Group**（カスタム グループ）リストの最大合計数は、グループ マッピング設定ごとに 640 エントリです。各エントリは、単一のグ

ループあるいはグループのリストにすることができます。デフォルトでは、グループを指定しないと、ポリシー ルールですべてのグループを使用できます。

作成したカスタム グループも、認証プロファイルの許可リストで使用できるようになります（認証プロファイルおよびシーケンスの設定）。

1. ディレクトリサービスから既存グループを追加します。
   1. **Group Include List (許可リストのグループ化)** を選択します。
   2. ポリシールールに含めたい利用可能なグループを選択し、Included Groups (含まれたグループ) に追加（⊕）します。
2. 既存のユーザー グループに一致しないユーザー属性に基づいてポリシー ルールを作成する場合、LDAP フィルタに基づいてカスタム グループを作成します。
   1. **Custom Group (カスタム グループ)** を選択してグループを **Add (追加)** します。
   2. 現在のファイアウォールまたは仮想システムにおけるグループマッピング設定の中で一意のグループの **Name**（名前）を入力します。

      Name (名前) に既存の AD グループ ドメインの識別名（DN）と同じ値があると、ファイアウォールは、その名前が参照されるすべての場所（たとえば、ポリシーやログ内）でカスタム グループを使用します。
   3. 最大 2,048 個の UTF-8 文字の **LDAP Filter** [LDAP フィルタ]を指定し、**OK**[OK] をクリックします。

      ファイアウォールは LDAP フィルタを検証しないため、正しいことを自分で確認する必要があります。

      LDAP ディレクトリ サーバーのパフォーマンスの低下を最小限に抑えるには、索引付けされた属性のみをフィルタに使用します。
3. **OK** をクリックして変更内容を保存します。

   カスタム グループをポリシーおよびオブジェクトで使用できるようにするには、コミットしなければなりません。

STEP 5 | 変更を **Commit (コミット)** します。

ファイアウォールが LDAP サーバーから属性を収集する前に、ポリシーとオブジェクトでカスタム グループを使用する前に、コミットする必要があります。

LDAP サーバーからグループマッピング情報を取得するようにファイアウォールを設定した後、取得するグループに基づいてポリシーを設定する前に、ファイアウォールによりグループ マッピングのキャッシュがリフレッシュされるのを待つか、手動でキャッシュをリフレッシュすることをお勧めします。どのグループが現在ポリシー内で使用できるのか確認するには、ファイアウォール CLI にアクセスして、***show user group*** コマンドを実行します。ファイアウォールが次にグループ マッピング キャッシュを更新する時期を決定するには、***show user group-mapping statistics*** コマンドを実行し、*Next Action* を確認します。キャッシュを手動で更新するには、***debug user-id refresh group-mapping all*** コマンドを実行します。

STEP 6 | ユーザーとグループのマッピングでユーザーが正しく識別されていることを確認します。

1. ファイアウォールがすべてのグループをフェッチしたことを確認するには、**Device**（デバイス） > **User Identification**（ユーザー **ID**） > **Group Mapping**（グループマッピング） > **Group Include List**（許可リストのグループ化）を選択します。
2. すべてのユーザー属性が正しく取得されたことを確認するには、次の CLI コマンドを使用します。

```
show user user-attributes user all
```

すべてのユーザーに対して、ユーザー プリンシパル名（UPN）、プライマリ ユーザー名、電子メール属性、および設定された代替ユーザー名の正規化形式が表示されます。

```
admin@PA-VM-8.1> show user user-attributes user all
```

```
Primary: nam\sam-user Email: sam-user@nam.com
```

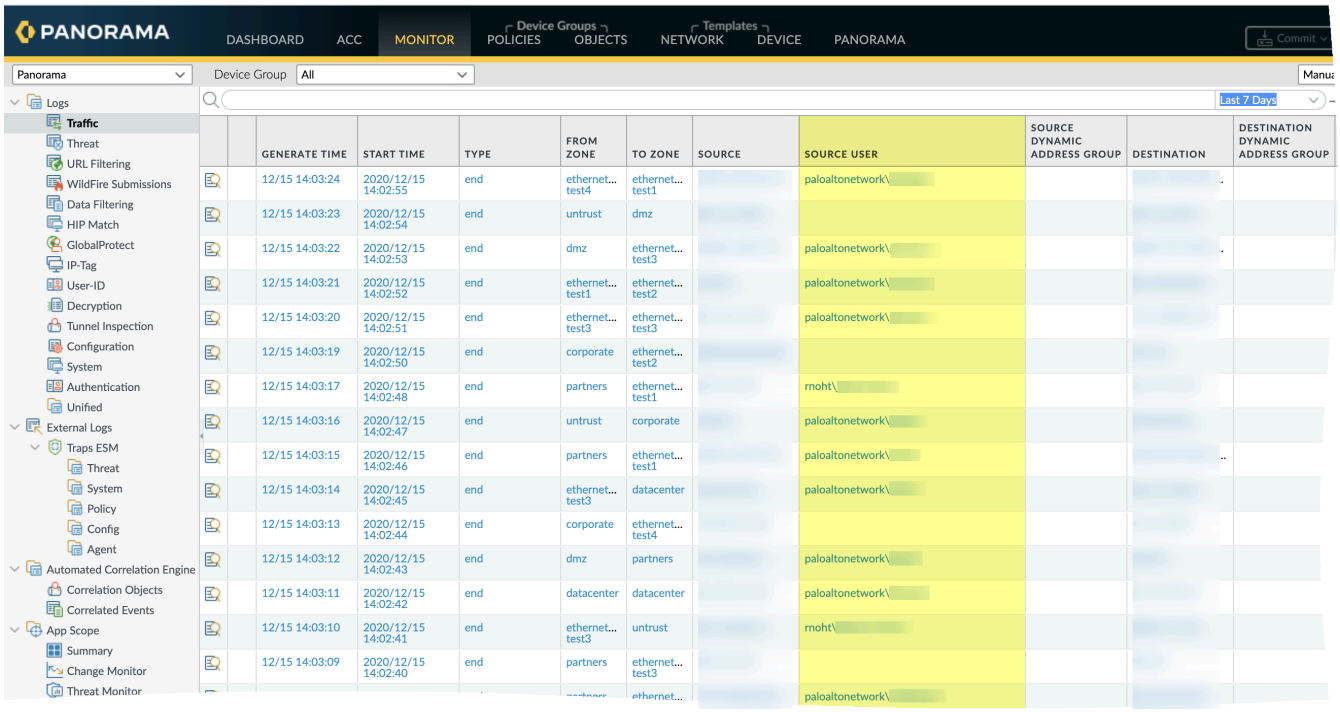
```
Alt User Names:1) nam.com\sam-user
```

```
2) nam\sam-user-upn
```

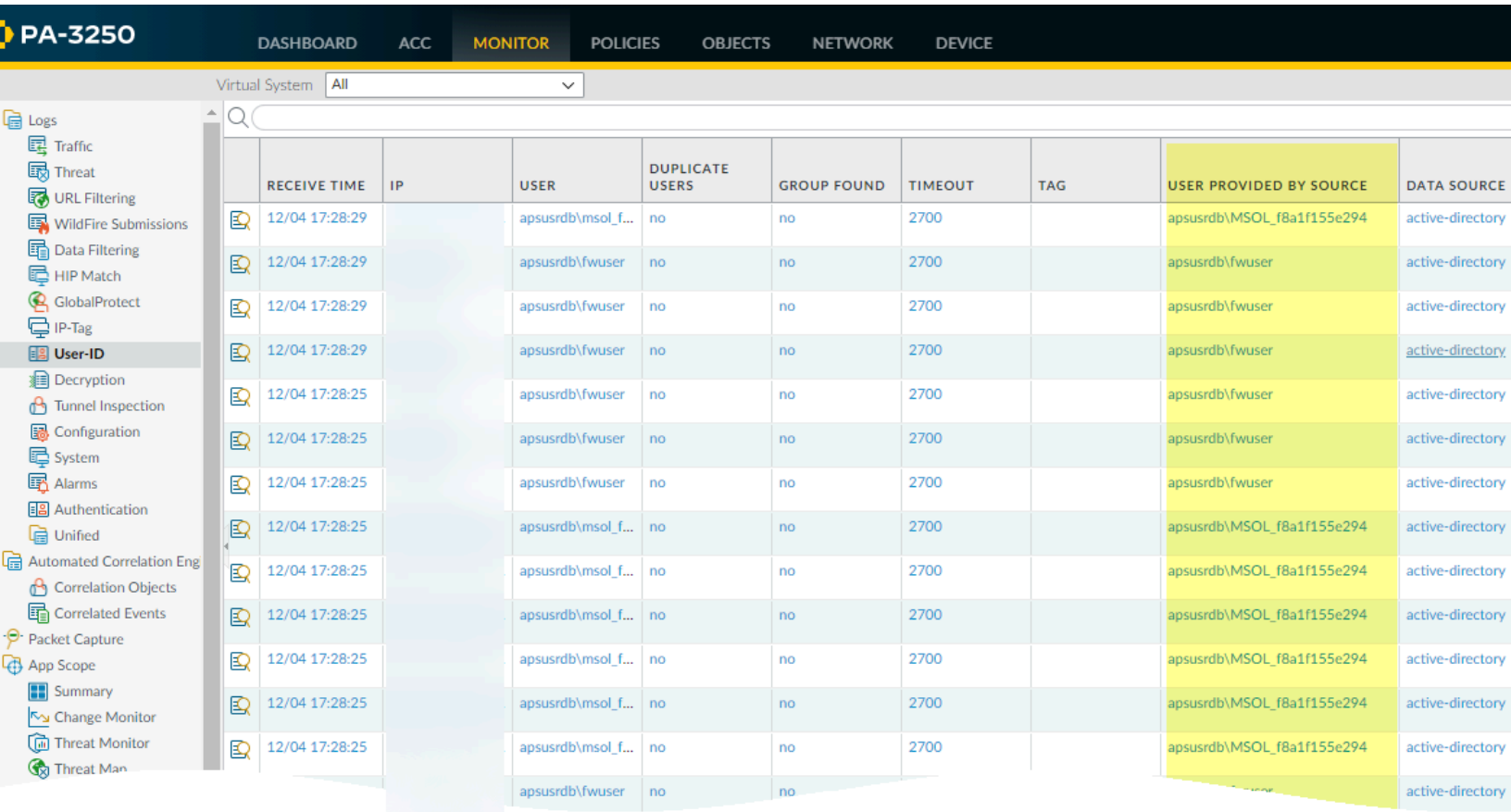
```
3) sam-user-upn@nam.local
```

```
4) sam-user@nam.com
```

3. ユーザー名が **Monitor**（監視） > **Logs**（ログ） > **Traffic**（トラフィック）の **Source User**（送信元ユーザー）列に正しく表示されることを確認します。



4. ユーザーが**Monitor**（監視） > **Logs**（ログ） > **User-ID** の **User Provided by Source**（送信元が提供したユーザー）列でに正しくマップされることを確認します。



IP アドレス対ユーザーのマッピング

User-ID は、IP アドレスをユーザー名にマッピングする様々な方法を提供します。ユーザーマッピングを設定する前に、ユーザーがどこからログインするのか、どのようなサービスにアクセスしているのか、どのようなアプリケーションやデータに対してアクセスを制御する必要があるのかを考えます。そうすることで、ユーザーを識別する上で最適な種類のエージェントや統合方法を把握できます。

計画が決まったら、必要に応じて次の方式のうち一つあるいは複数を使用してユーザーマッピングを設定し始め、ユーザーベースのアクセスを有効化し、アプリケーションおよびリソースに可視性をもたらします。

- ドメインログインしていない Linux クライアントなど、ドメインサーバーにログインしていないクライアントシステムのユーザーの場合、認証ポータルを使用して IP アドレスをユーザー名にマッピングできます。また、認証ポータルを認証ポリシーと併せて使用することで、最も機密性の高いアプリケーションやデータにアクセスした際、すべてのユーザに対する認証処理の実現が可能になります。
- Exchange サーバー、ドメイン コントローラ、eDirectory サーバー、または直接プロービングできる Windows クライアントにログインしたときにユーザーをマッピングするには、ユーザー ID エージェントを設定する必要があります。
  - PAN-OS 統合 User-ID エージェントを使用したユーザー マッピングの設定
  - Windows User-ID エージェントを使用したユーザー マッピングの設定
- Microsoft Terminal Server または Citrix Metaframe Presentation ServerやXenAppなど、Windows環境でマルチユーザーシステムを実行しているクライアントがある場合は、Palo Alto Networks ターミナル サーバー（TS）エージェントのユーザー マッピング設定。Windows 上で実行されていないマルチ ユーザーシステムについては、ユーザー ID XML API を使用したターミナル サーバーからのユーザー マッピングの取得を行えます。
- ワイヤレス コントローラ、802.1x デバイス、Apple Open Directory サーバー、プロキシ サーバー、その他のネットワーク アクセス制御(NAC)メカニズムなど、ユーザーを認証する既存のネットワーク サービスからユーザー マッピングを取得するには、User-ID を設定してユーザーマッピング用に Syslog 送信者を監視します。

  ファイアウォール上で *Windows* エージェントあるいは *PAN-OS* 統合 *User-ID* エージェントを設定してネットワーク サービスからの認証 *Syslog* メッセージをリッスンすることができますが、*TLS* を介した *Syslog* のリッスンをサポートしているのは *PAN-OS* 統合エージェントだけであるため、これが推奨される設定になります。
- 送信トラフィックのヘッダーにユーザー名とドメインを含めることで、ネットワーク内の他のデバイスがユーザーを識別し、ユーザーベースのポリシーを適用できるようにするために、HTTP ヘッダーにユーザー名の挿入できます。
- 仮想システム間でのユーザー ID マッピングの共有するために、仮想システムを User-ID ハブとして構成できます。
- 他の方法でマッピングできないその他のクライアントについては、XML API を使用した User-ID へのユーザー マッピングの送信を行えます。

- 大規模ネットワークは、ファイアウォールがユーザーおよびグループのマッピングのためにクェリする数 100 個の情報ソースを持つことができ、マッピング情報に基づいてポリシーを適用できる 多数のファイアウォールを持つことができます。ユーザー ID エージェントが収集する前に、マッピング情報を集約することによってユーザー ID の管理を簡略化することができます。マッピング情報を再配信するように、いくつかのファイアウォールを設定することによって、クエリープロセスでファイアウォールと情報ソースが使用するリソースを減らすこともできます。詳細については大規模ネットワークでのユーザー ID のデプロイを参照してください。

ユーザーID エージェントの専用サービス アカウントを作成

ユーザーが Exchange サーバー、ドメイン コントローラ、eDirectory サーバー、あるいは Windows クライアントにログインする際にユーザーをマッピングするために Windows ベースの User-IDエージェントあるいは PAN-OS 統合 User-IDエージェントを使用するには、エージェントが監視する各ドメイン内のドメイン コントローラ上の User-IDエージェント用に専用サービス アカウントを作成します。

User-IDエージェントは、セキュリティ イベントのログを基にユーザーをマッピングします。User-IDエージェントがユーザーを確実かつ正常にマッピングできるようにするために、ログオンの監査、Kerberos 認証サービスの監査、およびKerberos サービス チケット 運用の監査 イベントのログを生成するマッピングの送信元を検証します。少なくとも、送信元は以下のイベントのログを生成する必要があります:

- Logon Success (ログオン成功) (4624)
- Authentication Ticket Granted (認証チケット付与) (4768)
- Service Ticket Granted (サービス チケット付与) (4769)
- Ticket Granted Renewed (チケット付与更新) (4770)

サービス アカウントに必要な権限は、使用する予定のユーザー マッピングの方式や設定によって異なります。たとえば、PAN-OS統合User-IDエージェントを使用している場合、ユーザー セッションを監視するにはサービス アカウントにサーバー運用者権限が求められます。Windows ベースの User-ID エージェントを使用している場合、ユーザー セッションを監視するにはサービス アカウントのサーバー運用者権限は不要です。User-ID サービス アカウントが悪用されるリスクを軽減するために、必ずエージェントに最低限必要な権限だけを持つアカウントを設定するようにしてください。

- サポートされている Windows サーバーに Windows ベースのユーザー ID エージェントをインストールする場合は、 Windows ユーザー ID エージェントのサービスアカウントを設定します。
- ファイアウォールで PAN-OS 統合ユーザー ID エージェントを使用している場合は、 PAN-OS 統合ユーザー ID エージェントのサービスアカウントを構成します。

User-ID は、ユーザーマッピング情報を安全に収集するための方法を多く提供します。ローカル ネットワークにアタッチされた *Windows* デスクトップ上のユーザーのマッピングだけを必要とする環境用に設定された一部のレガシー機能では、権限付きのサービス アカウントが必要になります。権限付きのサービス アカウントが悪用された場合、ネットワークが攻撃にさらされることになります。ベストプラクティスとして、クライアントプローブ、セッションモニタリングなど、侵害された場合に脅威となる特権を必要とするレガシー機能の使用は避けてください。

Windows User-ID エージェント用サービス アカウントの設定

Windows User-ID エージェントがユーザー マッピングを収集するために監視するサービスと、ホストにアクセスできるように専用のアクティブディレクトリ（AD）サービスアカウントを作成します。エージェントが監視するドメイン毎にサービス アカウントを作成する必要があります。サービスアカウントに必要なアクセス許可を有効にしたら、Windows ユーザー ID エージェントを使用してユーザーマッピングを設定します。

次の作業は、全体のセキュリティを犠牲にすることなく、最適なやり方でユーザーを識別できるよう、必要なすべての権限を詳細に説明し、脅威を発生させ得る権限が必要な *User-ID* 機能はどれかを説明するものです。

STEP 1 | User-ID エージェント用の AD サービス アカウントを作成します。

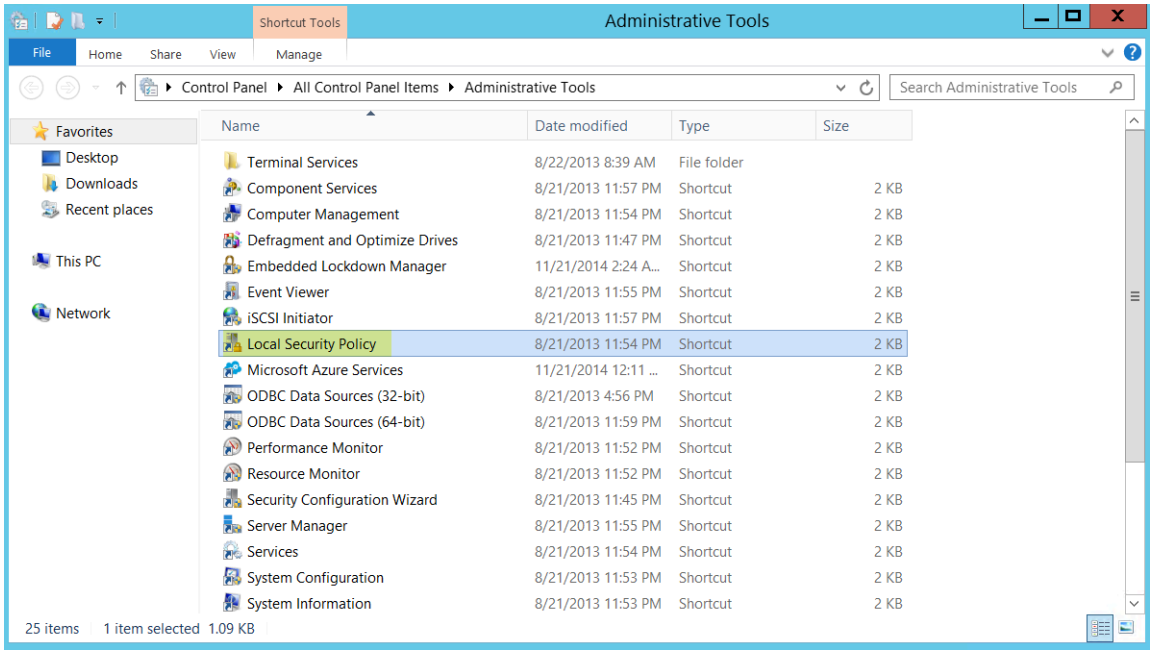
エージェントが監視するドメイン毎にサービス アカウントを作成する必要があります。

1. ドメイン コントローラにログインします。
2. Windows アイコン を右クリックし、**Active Directory Users** および **Computers** を **Search (検索)** してアプリケーションを起動します。
3. ナビゲーション ペインでドメインのツリーを開き、**Managed Service Accounts (管理対象サービス アカウント)** を右クリックして **New (新規)** > **User (ユーザー)** を選択します。
4. ユーザーの **First Name (名)**、**Last Name (姓)**、**User logon name (ユーザーログオン名)** を入力して **Next (次へ)** をクリックします。
5. **Password (パスワード)** および **Confirm Password (パスワードの確認)** を入力し、**Next (次へ)** をクリックして **Finish (完了)** します。

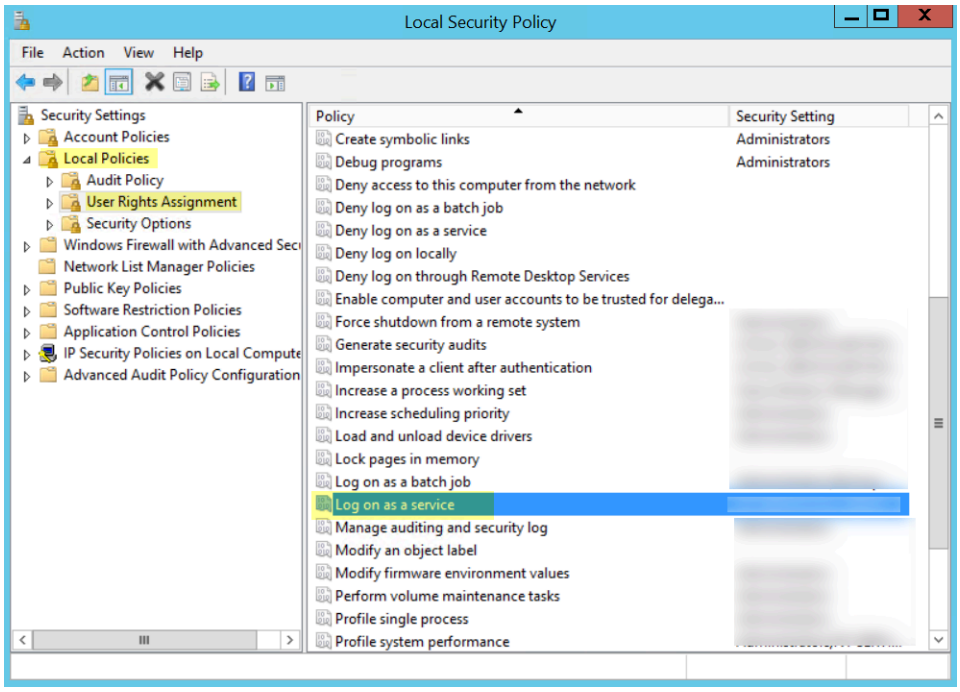
STEP 2 | サービスアカウントがサービスとしてログオンできるように、ローカルポリシーまたはグループポリシーを構成します。

サービスとしてログオンする権限は、エージェント ホストである Windows Server のローカルでのみ必要になります。

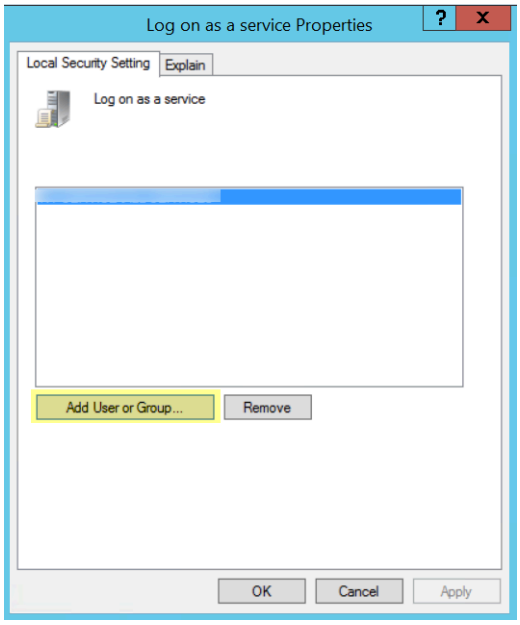
- ローカルで権限を割り当てるには：

1. **Control Panel** (コントロールパネル) > **Administrative Tools** (管理ツール) > **Local Security Policy** (ローカル セキュリティポリシー) を選択します。
2. 

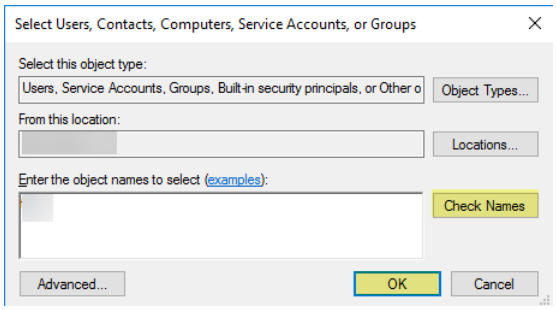
3. **Local Policies** (ローカルポリシー) > **User Rights Assignment** (ユーザー権限の割り当て) > **Log on as a service** (サービスとしてログオン)を選択します。



4. **Add User or Group** (ユーザーあるいはグループを追加)してサービス アカウントを追加します。

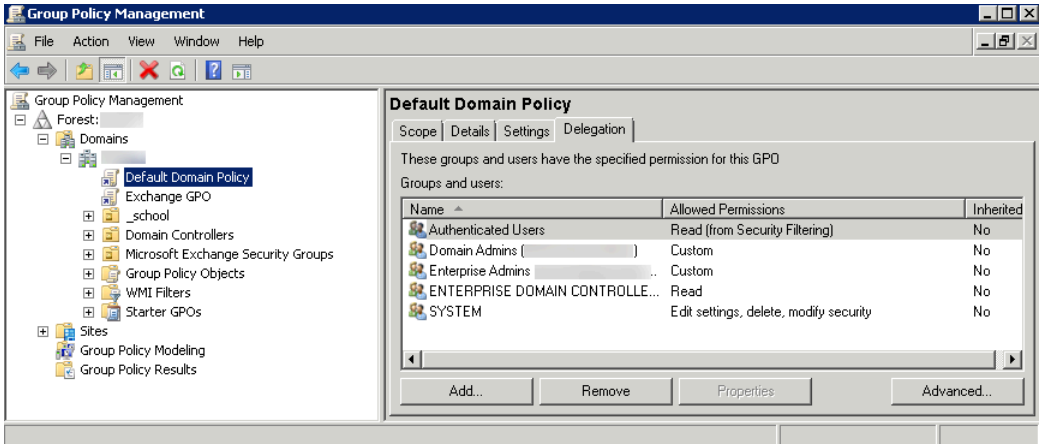


5. **Enter the object names to select** (選択するオブジェクト名を入力) (サービスアカウント名) を **domain\username** 形式で入力し、**OK** をクリックします。

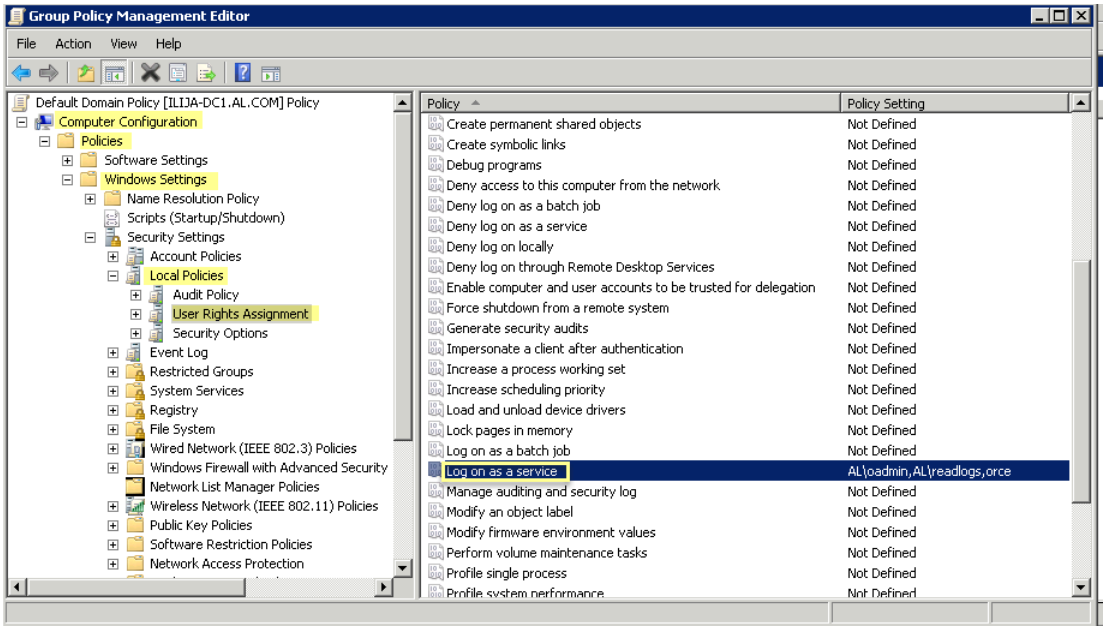


- Windows User-ID エージェントを複数のサーバーにインストールする場合、グループポリシーを構成するには、グループポリシー管理エディターを使用します。

  1. エージェント ホストである Windows サーバーに対して、**Start** > **Group Policy Management** > **<your domain>** > **Default Domain Policy** > **Action** > **Edit** を選択します。

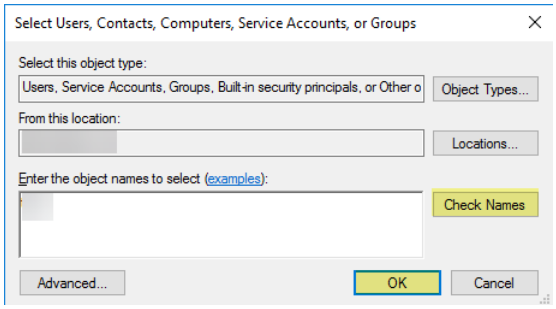


  2. **Computer Configuration** (コンピューター設定) > **Policies** (ポリシー) > **Windows Settings** (Windows 設定) > **Security Settings** (セキュリティ設定) > **Local Policies** (ローカルポリシー) > **User Rights Assignment** (ユーザー権限の割り当て) を選択します。



3. **Log on as a service (**サービスとしてログオン**)** を右クリックしてから **Properties (**プロパティ**)** を選択します。
4. **Add User** または **Group** をクリックしてサービス アカウントのユーザー名または組み込みグループを追加し、**OK** を 2 回クリックします。

   管理者には既定でこの特権があります。



STEP 3 | WMI を使用してユーザーデータを収集する場合は、監視対象サーバーで WMI クエリを使用できるように、DCOM 特権をサービスアカウントに割り当てます。

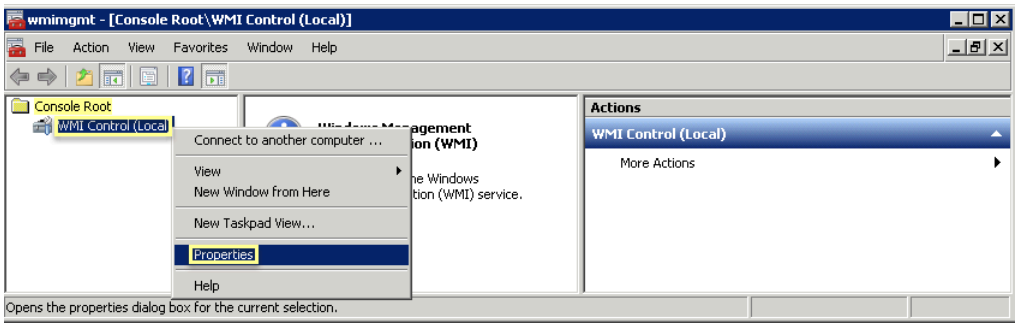
1. **Active Directory Users and Computers** > **<your domain>** > **Builtin** > **Distributed COM Users** を選択します。
2. **Properties (**プロパティ**)** > **Members (**メンバー**)** > **Add (**追加**)** を右クリックして、サービスアカウント名を入力します。

STEP 4 | WMI プロービングを使用する予定の場合、CIMV2 名前空間を読み取り、プロビジョニングするクライアント システムに必要なアクセス許可を割り当てるようアカウントを有効にします。

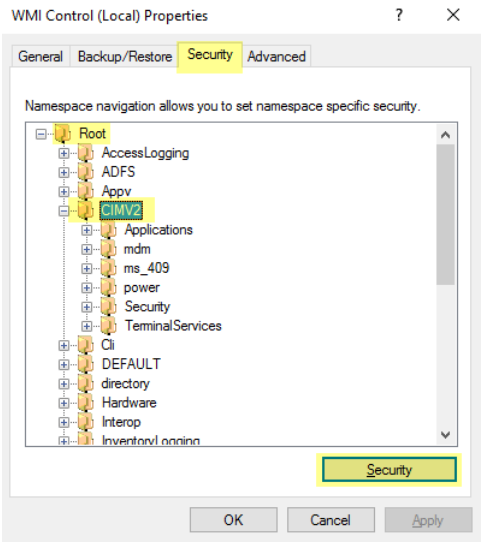
セキュリティの高いネットワークでは、クライアントに対するプローブを有効にしないでください。クライアントに対するプローブでは、大量のネットワーク トラフィックが生成される場合があり、設定に誤りがあるとセキュリティ上の脅威が発生する可能性があります。代わりに、分離性と信頼性の高いソース（ドメイン コントローラなど）から、*Syslog* や *XML API* との統合を介してユーザー マッピング情報を収集します。この方法には、（*Windows* クライアントだけでなく）すべてのデバイス タイプとオペレーティング システムから安全にユーザー マッピング情報をキャプチャできるという利点もあります。

User-ID エージェントがユーザーマッピング情報をプローブするクライアントシステム毎にこのタスクを実行します。

1. Windows アイコン を右クリックして **wmimgmt.msc** を **Search (検索)** し、WMI 管理コンソールを起動します。
2. コンソールのツリーで **WMI Control (WMI コントロール)** を右クリックし、**Properties (プロパティ)** を選択します。



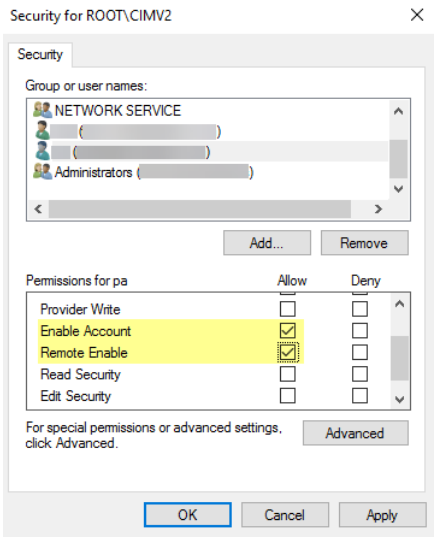
3. **Security (セキュリティ)** タブを選択してから、**Root (ルート)** > **CIMV2** を選択し、**Security (セキュリティ)** ボタンをクリックします。



4. 作成したサービスアカウントの名前を **Add** (追加) し、**Check Names** (名前を確認) で入力内容を確認し、**OK** をクリックします。

   Locations (場所) を変更するか、***Advanced*** (詳細) をクリックしなければアカウント名を照会できない場合があります。詳細は、ダイアログ ヘルプを参照してください。

5. **<Username>** のアクセス許可セクションでは、**Allow** に **Enable Account** と **Remote Enable** のアクセス許可があります。

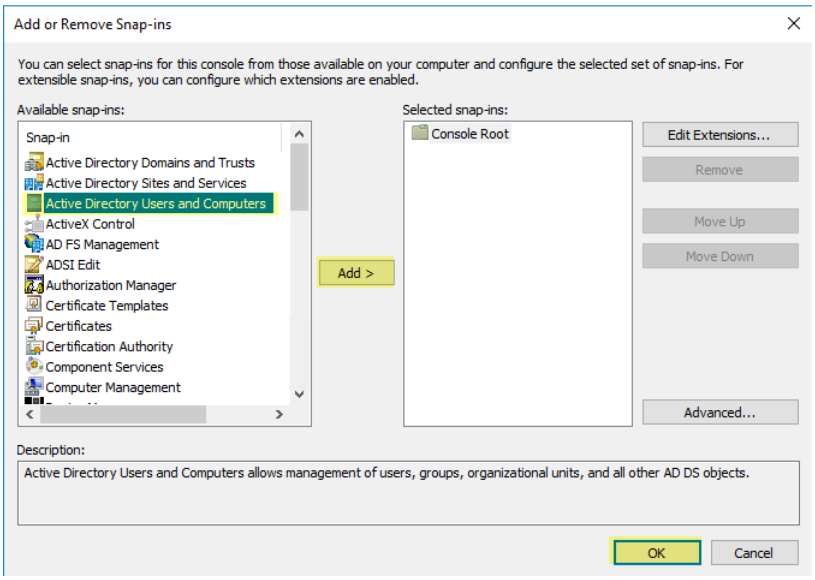


6. **OK** を 2 回クリックします。
7. ローカル ユーザーとグループの MMC スナップイン（lusrmgr.msc）を使用して、プローブされるシステム上のローカル DCOM（Distributed Component Object Model）ユーザーおよびリモート デスクトップ ユーザー グループにサービス アカウントを追加します。

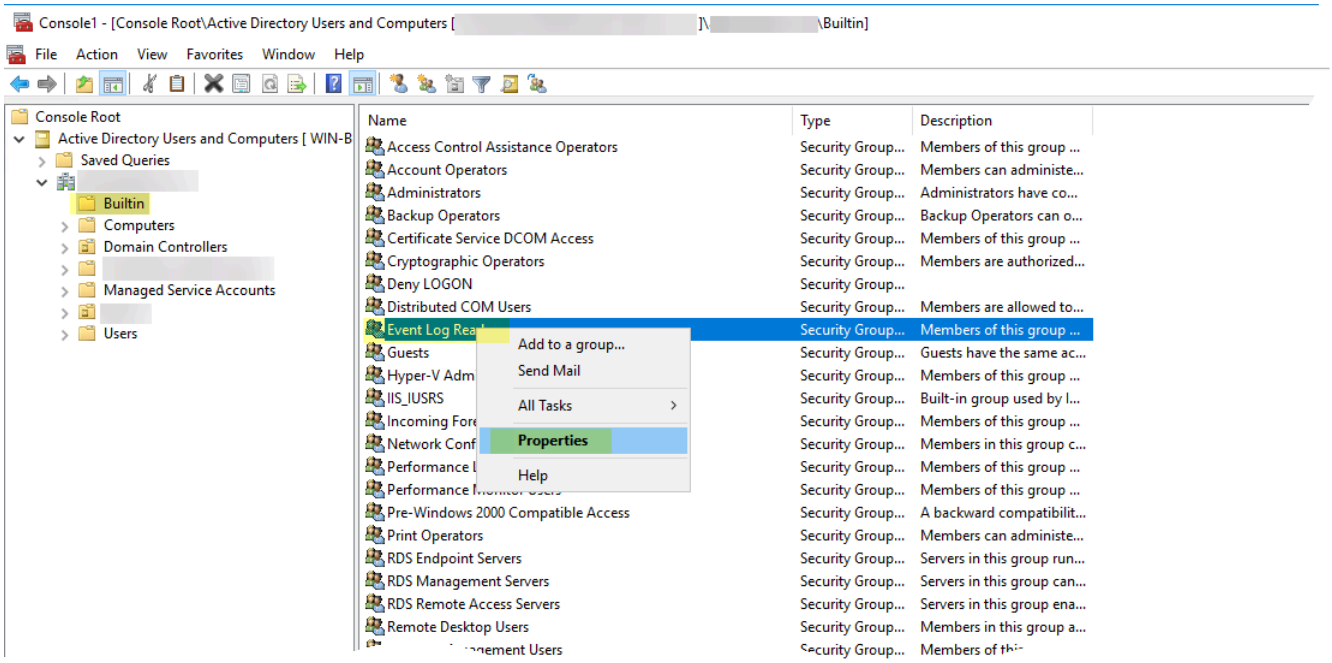
STEP 5 | サーバー モニタリングを使用してユーザーを識別する場合は、サービス アカウントを Event Log Reader 組み込みグループに追加して、サービス アカウントがセキュリティ ログ イベントを読み取れるようにします。

1. User-ID エージェントに読み取らせたいログを含むドメイン コントローラあるいは Exchange サーバー上、あるいはWindows ログ転送からイベントを受け取るメンバー サーバー上で **Start**（開始） > **Run**（実行）を選択し、**MMC** と入力します。
2. **File**（ファイル） > **Add/Remove Snap-in** （追加/除去スナップイン） > **Active Directory Users and Computers**（アクティブ ディレクトリ ユーザーおよびコンピュー

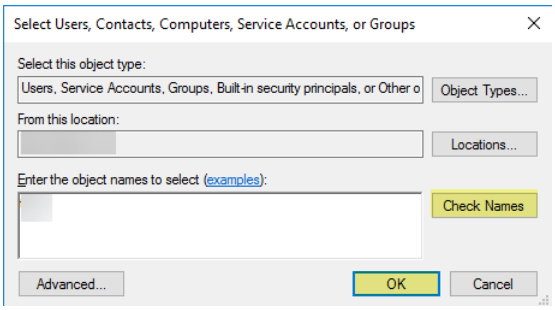
タ） > **Add**（追加）を選択し、**OK**をクリックして MMC を実行し、アクティブ ディレクトリ ユーザーとコンピュータースナップインを起動します。



3. ドメインの Builtin (ビルトイン) フォルダに移動し、**Event Log Reader (**イベントログ リーダー**)** グループを右クリックし、**Properties**（プロパティ） > **Members**（メンバー）を選択します。



4. サービスアカウントを **Add**（追加）してから、**Check Names**（名前を確認） をクリックして、適切なオブジェクト名があることを確認します。

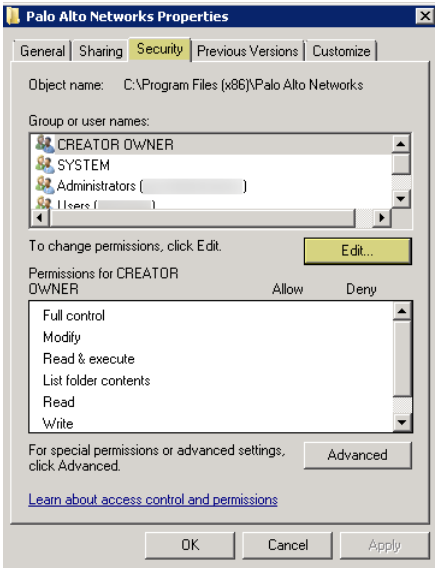


5. **OK**[OK] を 2 回クリックして設定を保存します。
6. ビルトインされたイベント ログ リーダー グループがサービス アカウントをメンバーとしてリストされることを確認します（**Event Log Readers**（イベントログリーダー）> **Properties**（プロパティ） > **Members**（メンバー））。

STEP 6 | アカウント権限をイントレーション フォルダに割り当て、サービス アカウントがエージェントのイントレーション フォルダにアクセスして設定の読み込みとログの書き込みを行えるようにします。

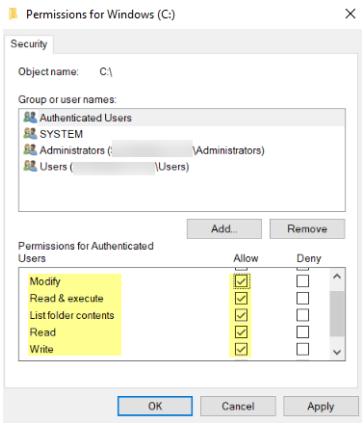
User-ID エージェント用に構成したサービスアカウントが、User-ID エージェントサーバー ホスト上のドメイン管理者またはローカル管理者でない場合にのみ、このステップを実行する必要があります。

1. Windows Explorer で、**`C:\Program Files(x86)\Palo Alto Networks`** に移動し、フォルダを右クリックして **Properties (プロパティ)** を選択します。
2. **[セキュリティ]** タブで、**[編集]** をクリックします。



3. User-ID エージェント サービス アカウントを **Add (追加)** し、**Modify (変更)**、**Read & execute(読み取りと実行)**、**List folder contents(フォルダの内容の一覧表示)**、**Read (読み**

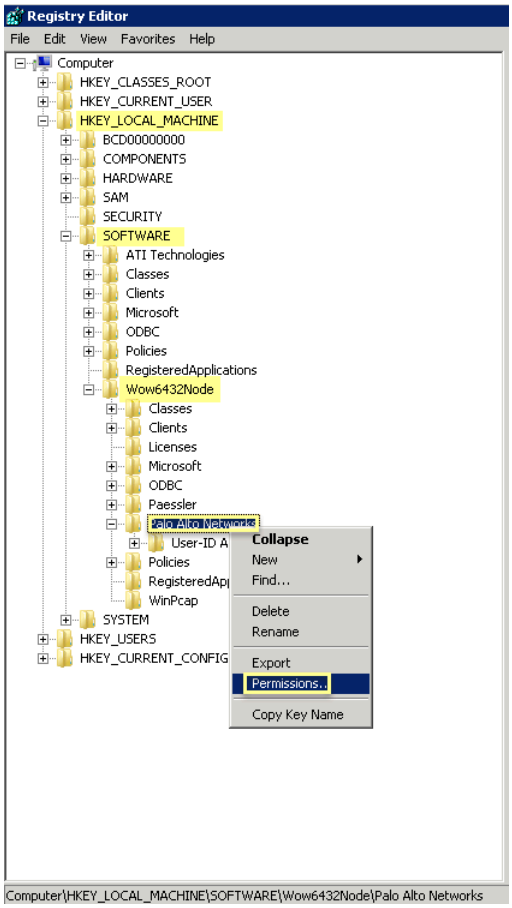
取り) および **Write** (書き込み) の権限を **Allow** (許可) し、**OK** をクリックしてアカウント設定を保存します。



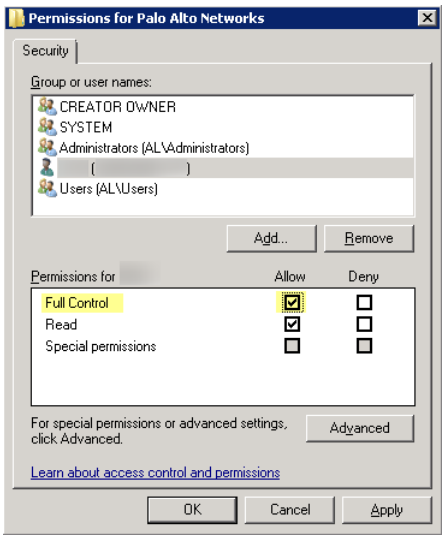
個々のアクセス許可を設定しない場合は、代わりに ***Full Control*** (フルコントロール) 権限を ***Allow*** (許可) します。

STEP 7 | エージェントが構成を変更できるようにするには (例えば、異なるログレベルを選択した場合)、サービスアカウントに User-ID エージェントレジストリサブツリーへのアクセス許可を与えます。

1. **Start (スタート)** > **Run (実行)** を選択し、**regedt32** を入力して、次のいずれかの場所にある Palo Alto Networks サブツリーに移動します：
   - **32** ビット システム—`HKEY_LOCAL_MACHINESoftwarePalo Alto Networks`
   - **64-**ビット システム—`HKEY_LOCAL_MACHINE\Software\WOW6432Node\PaloAlto Networks`
2. Palo Alto Networks**[Palo Alto Networks]** ノードを右クリックし、 **Permissions**[アクセス許可] を選択します。



3. User-ID サービス アカウントに **Full Control**[フル コントロール] を割り当て、 **OK**[OK] をクリックして設定を保存します。



STEP 8 | 不要なサービスアカウント権限を無効にします。

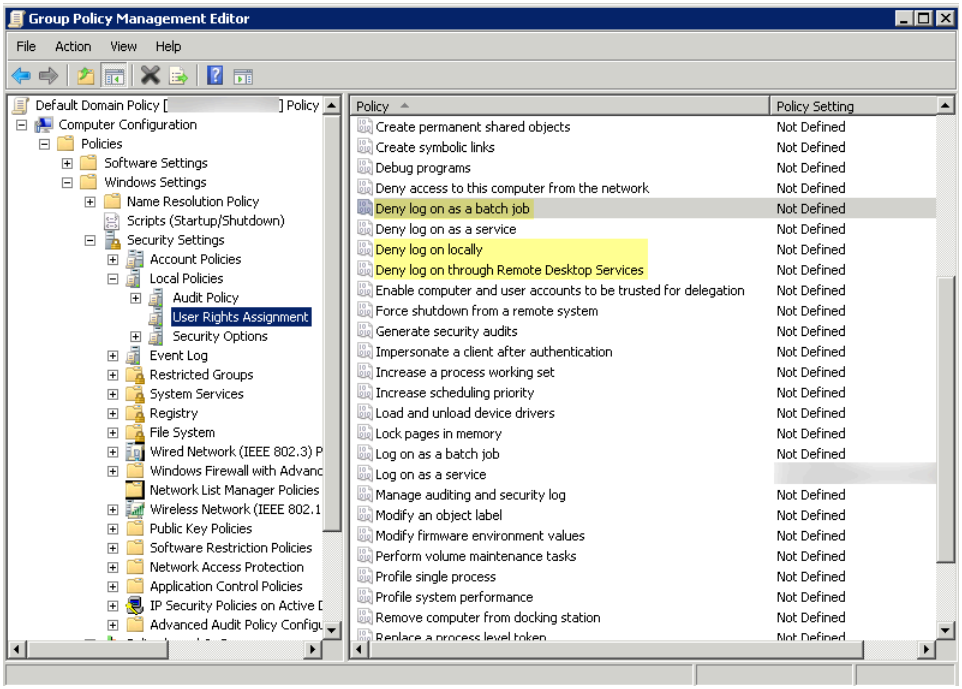
User-ID サービス アカウントに最低限必要なアカウント権限だけを持たせることで、アカウントが悪用された際に攻撃の入り口を減らすことができます。

User-ID アカウントが必要最低限の権限しか持たないようにするために、アカウントの次の権限を拒否します。

- **User-ID** サービス アカウントのインタラクティブ ログオンを拒否—User-ID サービス アカウントはアクティブディレクトリ セキュリティイベント ログを読み取ってパースする権限を必要としますが、サーバーあるいはドメインシステムにインタラクティブにログオンする能力は不要です。グループ ポリシーを使用して、あるいは管理対象のサービス アカウントを使用してこの権限を制限できます（詳細については Microsoft TechNet を参照）。

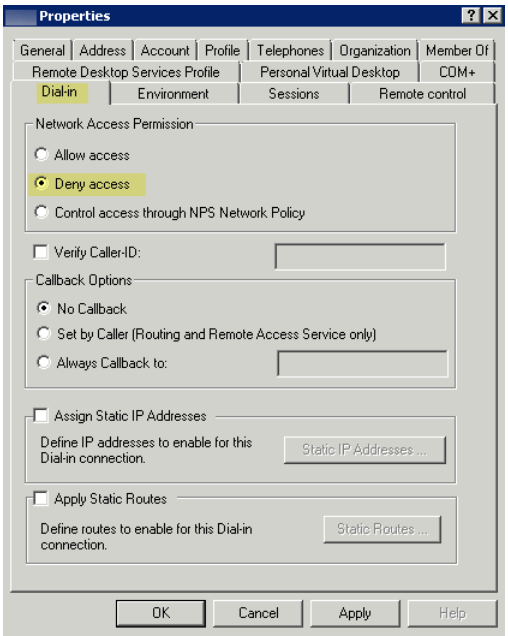
  1. 選択します **Group Policy Management Editor** > **Default Domain Policy** > **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **User Rights Assignment**.
  2. バッチ ジョブとしてのログオンを拒否する、ローカルでのログオンを拒否する、および **Remote Desktop Services** によるログオンを拒否するの場合は、**Properties**.

3. 選択します これらのポリシー設定を定義する > **Add User** または **Group** を選択してサービス アカウント名を追加し、**OK** をクリックします。



- **User-ID** サービス アカウントのリモート アクセスを拒否—攻撃者がアカウントを使用してネットワーク外部からネットワークにアクセスするのを防ぎます。

  1. 選択します **Start** > **Run** と入力し、**MMC** と入力し、**File** > **Add/Remove Snap-in** > **Active Directory Users and Computers** > **Users**.
  2. サービス アカウント名を右クリックし、**Properties**.
  3. 選択します **Dial-in**, then **Deny** the **Network Access Permission**.



STEP 9 | 次のステップとして、 Windows ユーザー ID エージェントを使用したユーザー マッピングの設定を行います。

PAN-OS 統合 User-ID エージェントのサービスアカウントを設定する

ユーザーマッピングを収集するために監視するサービスとホストにアクセスするには、PAN-OS 統合 User-ID エージェント専用のActive Directory (アクティブディレクトリ - AD) サービスアカウントを作成します。エージェントが監視する各ドメインにサービスアカウントを作成しなければなりません。サービスアカウントに必要なアクセス許可を有効にしたら、 PAN-OS 統合ユーザー ID エージェントを使用してユーザーマッピングを設定します。

次の作業は、全体のセキュリティを犠牲にすることなく、最適なやり方でユーザーを識別できるよう、必要なすべての権限を詳細に説明し、脅威を発生させ得る権限が必要な *User-ID* 機能はどれかを説明するものです。

STEP 1 | User-ID エージェント用の AD サービス アカウントを作成します。

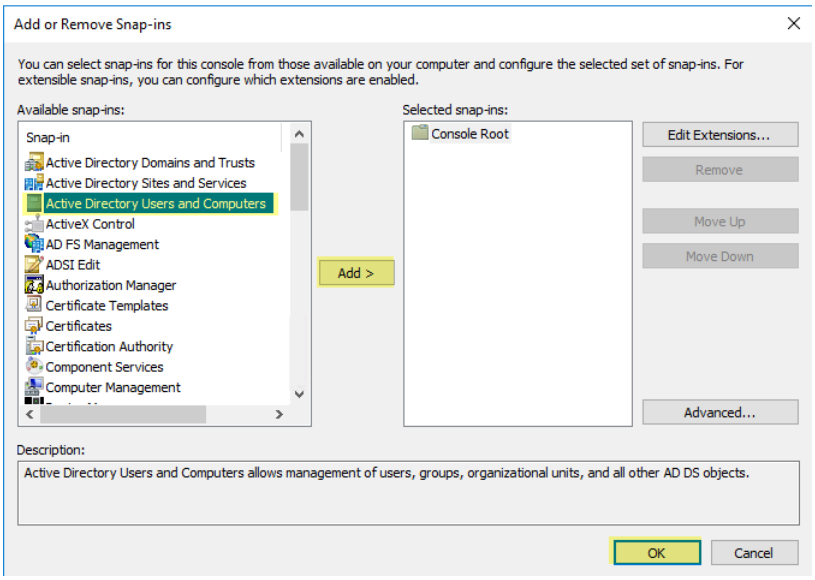
エージェントが監視するドメイン毎にサービス アカウントを作成する必要があります。

1. ドメイン コントローラにログインします。
2. Windows アイコン を右クリックし、**Active Directory Users** および **Computers** を **Search (検索)** してアプリケーションを起動します。
3. ナビゲーション ペインでドメインのツリーを開き、**Managed Service Accounts (管理対象サービス アカウント)** を右クリックして **New (新規)** > **User (ユーザー)** を選択します。
4. ユーザーの **First Name (名)**、**Last Name (姓)**、**User logon name (ユーザーログオン名)** を入力して **Next (次へ)** をクリックします。
5. **Password (パスワード)** および **Confirm Password (パスワードの確認)** を入力し、**Next (次へ)** をクリックして **Finish (完了)** します。

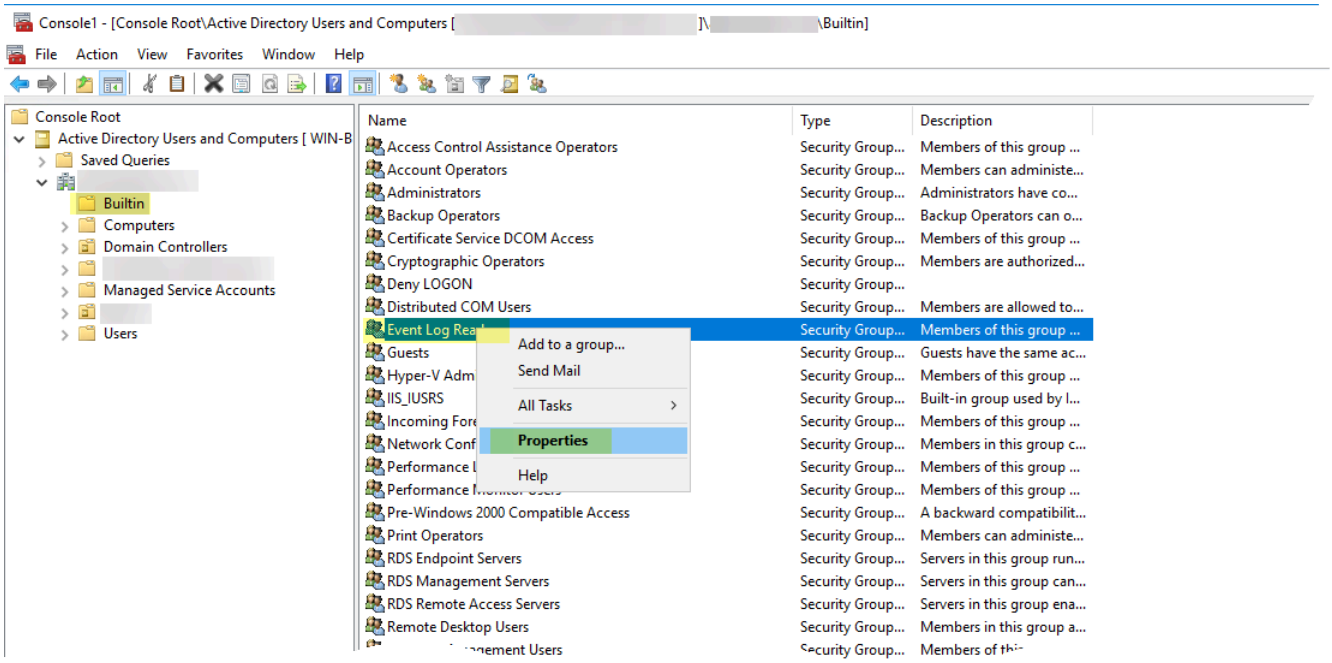
STEP 2 | サーバー モニタリングを使用してユーザーを識別する場合は、サービス アカウントを Event Log Reader 組み込みグループに追加して、サービス アカウントがセキュリティ ログ イベントを読み取れるようにします。

1. User-ID エージェントに読み取らせたいログを含むドメイン コントローラあるいは Exchange サーバー上、あるいはWindows ログ転送からイベントを受け取るメンバー サーバー上で **Start**（開始） > **Run**（実行）を選択し、**MMC** と入力します。
2. **File**（ファイル） > **Add/Remove Snap-in** （追加/除去スナップイン） > **Active Directory Users and Computers**（アクティブ ディレクトリ ユーザーおよびコンピュー

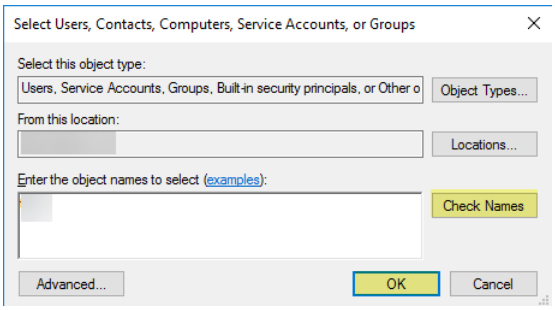
タ） > **Add**（追加）を選択し、**OK**をクリックして MMC を実行し、アクティブ ディレクトリ ユーザーとコンピュータースナップインを起動します。



3. ドメインの Builtin (ビルトイン) フォルダに移動し、**Event Log Reader (**イベントログ リーダー**)** グループを右クリックし、**Properties**（プロパティ） > **Members**（メンバー）を選択します。



4. サービスアカウントを **Add**（追加）してから、**Check Names**（名前を確認） をクリックして、適切なオブジェクト名があることを確認します。



5. **OK**[OK] を 2 回クリックして設定を保存します。
6. ビルトインされたイベント ログ リーダー グループがサービス アカウントをメンバーとしてリストされることを確認します（**Event Log Readers**（イベントログリーダー）> **Properties**（プロパティ） > **Members**（メンバー））。

STEP 3 | WMI を使用してユーザーデータを収集する場合は、監視対象サーバーで WMI クエリを使用できるように、DCOM 特権をサービスアカウントに割り当てます。

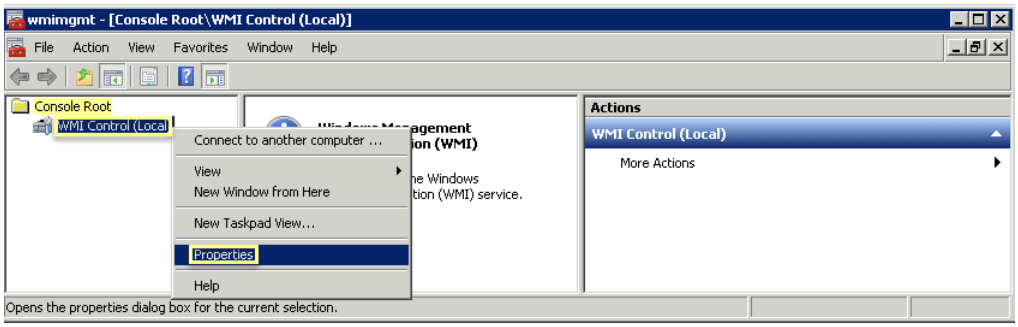
1. **Active Directory Users and Computers** > **<your domain>** > **Builtin** > **Distributed COM Users** を選択します。
2. **Properties (プロパティ)** > **Members (メンバー)** > **Add (追加)** を右クリックして、サービスアカウント名を入力します。

STEP 4 | WMI プローブの使用する予定の場合は、監視するドメイン コントローラの CIMV2 名前空間を読み取り、プロービングするクライアント システムに必要なアクセス許可を割り当てるようサービス アカウントを有効にします。

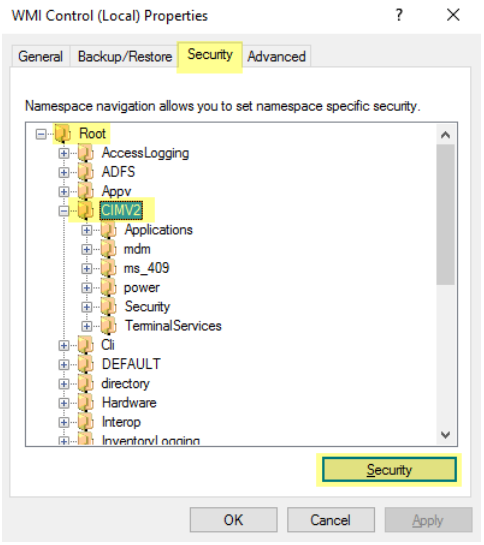
セキュリティの高いネットワークでは、クライアントに対するプローブを有効にしないでください。クライアントに対するプローブでは、大量のネットワーク トラフィックが生成される場合があり、設定に誤りがあるとセキュリティ上の脅威が発生する可能性があります。代わりに、分離性と信頼性の高いソース（ドメイン コントローラなど）から、*Syslog* や *XML API* との統合を介してユーザー マッピング情報を収集します。この方法には、（*Windows* クライアントだけでなく）すべてのデバイス タイプとオペレーティング システムから安全にユーザー マッピング情報をキャプチャできるという利点もあります。

User-ID エージェントがユーザーマッピング情報をプローブするクライアントシステム毎にこのタスクを実行します。

1. Windows アイコン を右クリックして **wmimgmt.msc** を **Search (検索)** し、WMI 管理コンソールを起動します。
2. コンソールのツリーで **WMI Control (WMI コントロール)** を右クリックし、**Properties (プロパティ)** を選択します。



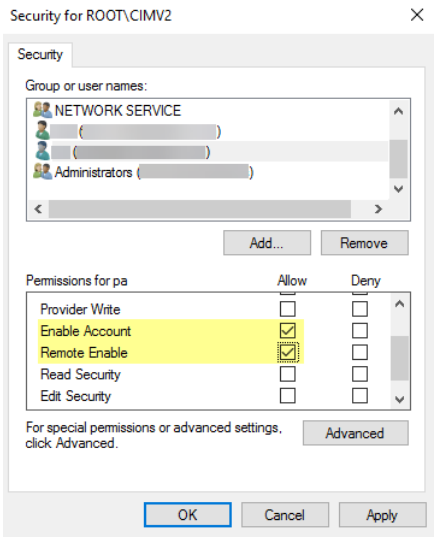
3. **Security (セキュリティ)** タブを選択してから、**Root (ルート)** > **CIMV2** を選択し、**Security (セキュリティ)** ボタンをクリックします。



4. 作成したサービスアカウントの名前を **Add** (追加) し、**Check Names** (名前を確認) で入力内容を確認し、**OK** をクリックします。

   Locations (場所) を変更するか、***Advanced*** (詳細) をクリックしなければアカウント名を照会できない場合があります。詳細は、ダイアログ ヘルプを参照してください。

5. **<Username>** のアクセス許可セクションでは、**Allow** に **Enable Account** と **Remote Enable** のアクセス許可があります。



6. **OK** を 2 回クリックします。
7. ローカル ユーザーとグループの MMC スナップイン（lusrmgr.msc）を使用して、プローブされるシステム上のローカル DCOM（Distributed Component Object Model）ユーザーおよびリモート デスクトップ ユーザー グループにサービス アカウントを追加します。

STEP 5 | (非推奨) エージェントがユーザーセッションを監視してユーザーマッピング情報を求めて Windows サーバーをポーリングするには、サーバーオペレーターの特権をサービスアカウントに割り当てます。

このグループはサーバーのシャットダウンと再起動を行う権限も持っているため、ユーザー セッションの監視がかなり重要な場合のみ、アカウントを割り当てるようにしてください。

1. **Active Directory** ユーザーとコンピューター > **<your domain>** > **Builtin** > **Server Operators Group** を選択します。
2. **Properties** (プロパティ) > **Members** (メンバー) > **Add** (追加) を右クリックして、サービスアカウント名を追加します。

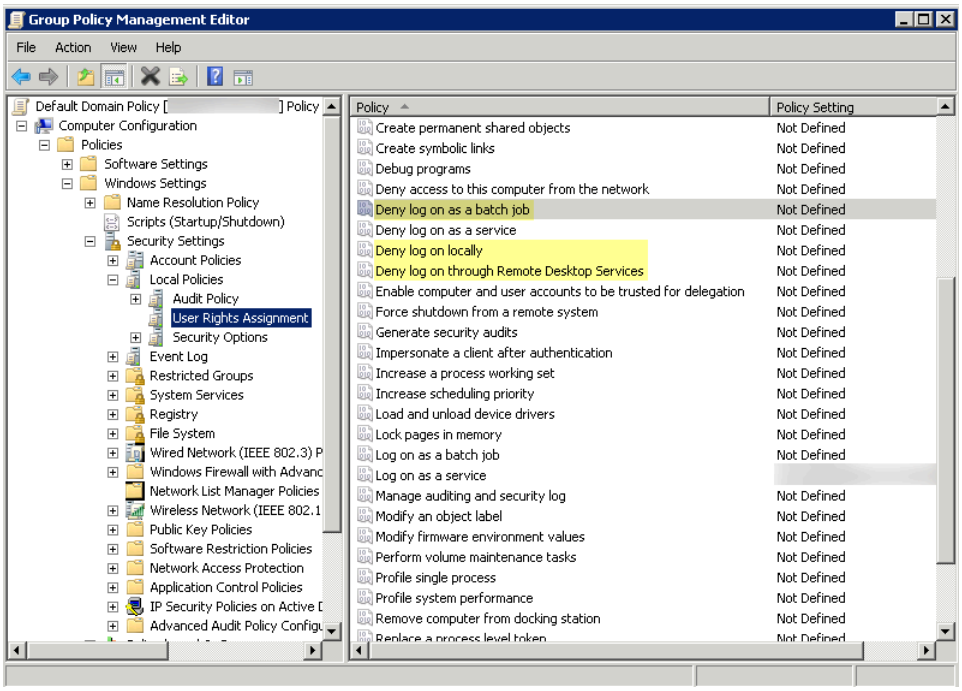
STEP 6 | 不要なサービスアカウント権限を無効にします。

User-ID サービス アカウントに最低限必要なアカウント権限だけを持たせることで、アカウントが悪用された際に攻撃の入り口を減らすことができます。

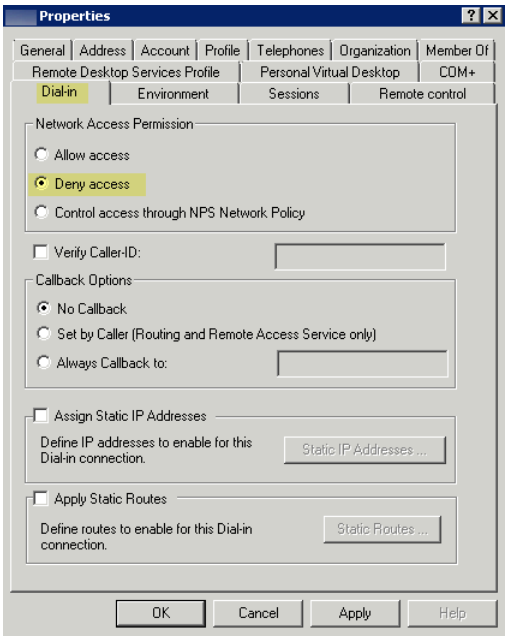
User-ID アカウントが必要最低限の権限しか持たないようにするために、アカウントの次の権限を拒否します。

- **User-ID** サービス アカウントのインタラクティブ ログオンを拒否—User-ID サービス アカウントはアクティブディレクトリ セキュリティイベント ログを読み取ってパースする権限を必要としますが、サーバーあるいはドメインシステムにインタラクティブにログオンする能力は不要です。グループ ポリシーを使用して、あるいは管理対象のサービス アカウントを使用してこの権限を制限できます（詳細については Microsoft TechNet を参照）。

  1. 選択します **Group Policy Management Editor** > **Default Domain Policy** > **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **User Rights Assignment**.
  2. バッチ ジョブとしてのログオンを拒否する、ローカルでのログオンを拒否する、および **Remote Desktop Services** によるログオンを拒否する を右クリックし、[プロパティを右クリックし、**[**これらのポリシー設定を定義する > **Add User or Group** を右クリックし、サービス アカウント名を追加し、[**OK** をクリックします。



- **User-ID** サービス アカウントのリモート アクセスを拒否—攻撃者がアカウントを使用してネットワーク外部からネットワークにアクセスするのを防ぎます。
  1. **Start** > **Run**, enter **MMC**, and select **File** > **Add/Remove Snap-in** > **Active Directory Users and Computers** > **Users**.
  2. サービス アカウント名を右クリックし、**Properties**.
  3. 選択します **Dial-in**, then **Deny** the **Network Access Permission**.



STEP 7 | 次のステップでは、 PAN-OS 統合 User-ID エージェントを使用したユーザー マッピングの設定を行います。

Windows User-ID エージェントを使用したユーザー マッピングの設定

多くの場合、ネットワーク ユーザーの大部分がモニタリング対象のドメイン サービスにログインできます。これらのユーザーに対して、Palo Alto Networks ユーザー ID エージェントはサーバーのログイン イベントをモニターし、IP アドレス対ユーザー名のマッピングを実行します。ユーザー ID エージェントを設定する方法は、環境の規模やドメイン サーバーの場所により異なります。ベスト プラクティスとして、User-ID エージェントは監視対象のサーバーの近くに配置します（つまり、モニター対象のサーバーと Windows User-ID エージェントの間に WAN リンクをはさまないようにします）。これは、ユーザー マッピングのトラフィックがエージェントとモニタリング対象サーバーの間で発生し、エージェントとファイアウォール間のトラフィック(最終更新以降のユーザーマッピングの差分情報)の量もごくわずかなためです。

以下のトピックでは、ユーザー ID エージェントのインストールと設定の方法、およびファイアウォールがエージェントからユーザー マッピング情報を取得するための設定方法について説明します。

- Windows ベースの ユーザー ID エージェントをインストール

- ユーザー マッピングのための Windows の User-ID エージェントの設定

Windows ベースの ユーザー ID エージェントをインストール

以下の手順では、ユーザー ID エージェントをドメイン内のメンバー サーバー上にインストールし、必要な権限が設定されたサービス アカウントをセットアップする方法を示します。アップグレードする場合、インストーラは古いバージョンを自動的に削除しますが、インストーラを実行する前に config.xml ファイルをバックアップしておくことをお勧めします。

Windows ベースの*User-ID*エージェントをインストールするためのシステム要件の情報、およびサポートされているサーバー *OS* バージョンに関する情報は、User-IDエージェントのリリース ノート、および Palo Alto Networks Compatibility Matrix (Palo Alto Networksの互換性一覧) を参照してください。

STEP 1 | ユーザー ID エージェントがユーザー マッピングを収集するためにモニターするサービスとホストにアクセスできるように専用のアクティブディレクトリ サービスを作成します。

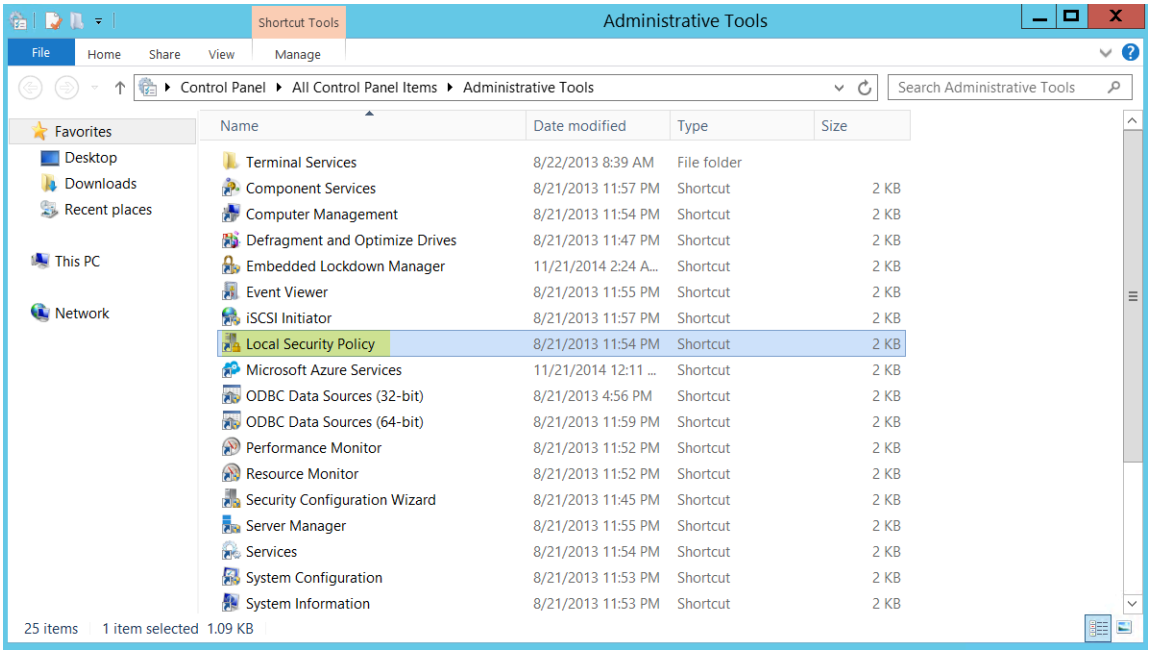
ユーザーID エージェントの専用サービス アカウントを作成し、必要な Windows User-ID エージェントの権限を付与します。

1. ローカルあるいはグループ ポリシーのいずれかを設定し、サービス アカウントがサービスとしてログオンできるようにします。
   1. Windows ベースの U1ser-ID エージェントを複数のサーバーにインストールする場合、グループ ポリシーを構成するには、エージェント ホストである Windows サーバーに対して **Group Policy Management** > **Default Domain Policy** > **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment** を選択します。
   2. Right-click **Log on as a service**, then select **Properties**.

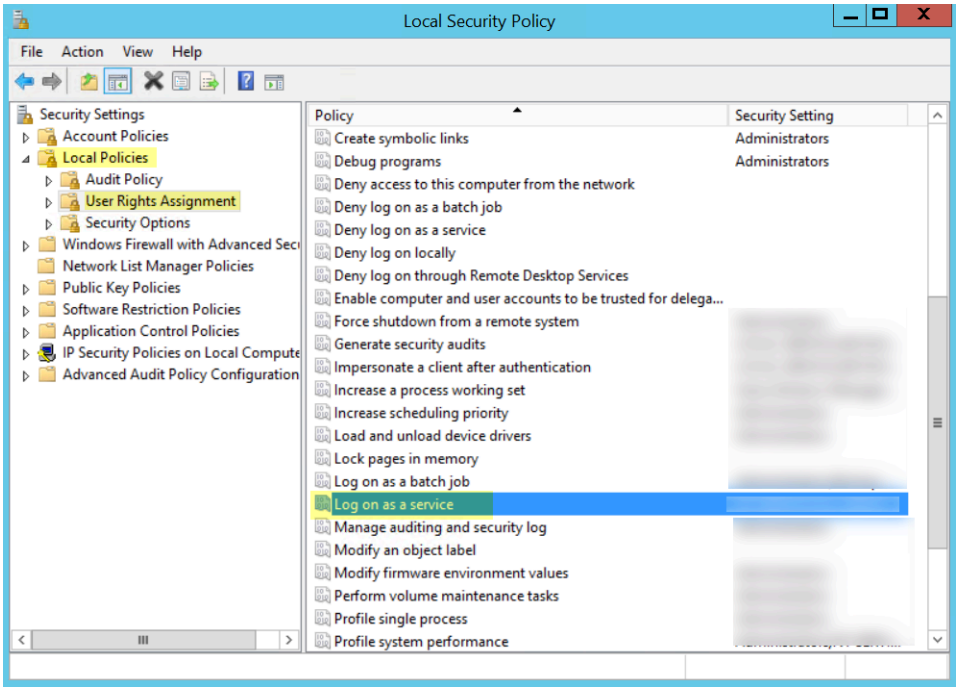
3. サービス アカウントのユーザー名または組み込みグループを追加します (管理者には既定でこの特権があります)。

   サービスとしてログオンする権限は、エージェント・ホストである*Windows*サーバ上でローカルにのみ必要です。*User-ID*エージェントを*1*つだけ使用している場合は、次の手順を使用して、エージェント・ホスト上でローカルに権限を付与できます。

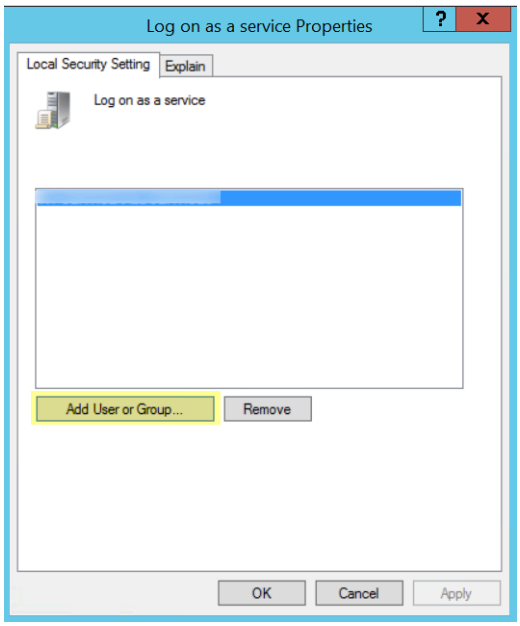
1. ローカルにアクセス許可を割り当てるには、**Control Panel** > **Administrative Tools** > **Local Security Policy**.



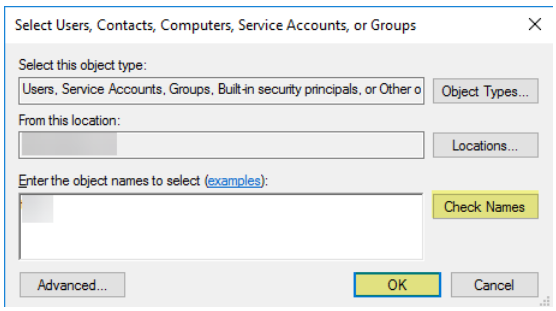
2. Select **Local Policies** > **User Rights Assignment** > **Log on as a service**.



3. **Add User or Group** を使用してサービス アカウントを追加します。



4. **domainusername** 形式でサービス アカウント名を 入力フィールドに入力し、**OK**.

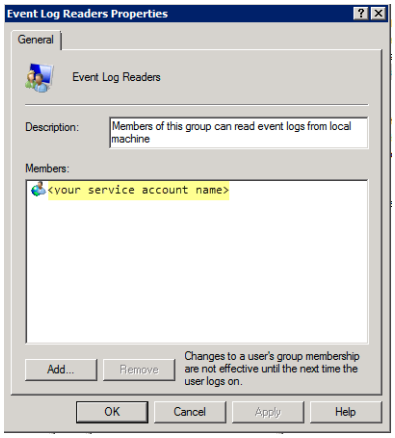


サービス アカウント名が有効であることを確認するには、**Check Names** をクリックします。

2. サーバー監視を使用してユーザーを識別したい場合、サービス アカウントを Event Log Reader (イベントログ リーダー) ビルトイン グループに追加し、セキュリティ ログイベントを閲覧する権限を有効化します。

   1. User-ID エージェントに読み取らせたいログを含むドメイン コントローラあるいは Exchange サーバー上、あるいはWindows ログ転送からイベントを受け取るメンバー サーバー上で MMC を実行して アクティブディレクトリ ユーザーおよびコンピューター スナップインを起動します。
   2. ドメインの Builtin (ビルトイン) フォルダに移動し、**Event Log Reader (**イベントログ リーダー**)**グループを右クリックし、**Add to Group (**グループに追加**)**を選択してプロパティのダイアログを開きます。
   3. **Add**[追加] をクリックし、User-ID サービスが使用するように設定したサービス アカウントの名前を入力し、**Check Names**[名前の確認] をクリックして正しいオブジェクト名であることを検証します。
   4. **OK**[OK] を 2 回クリックして設定を保存します。

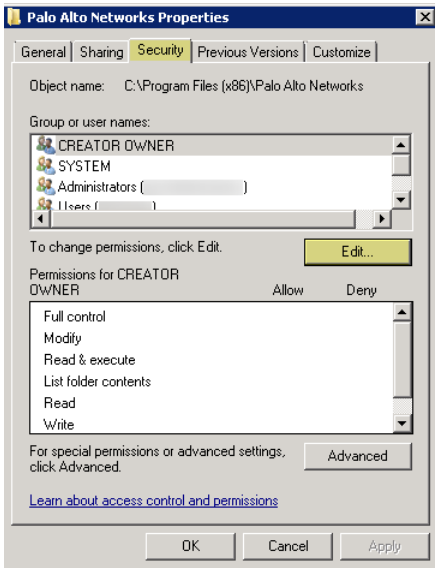
5. ビルトインされたイベント ログ リーダー グループがサービス アカウントをメンバーとしてリストアップすることを確認します。



3. アカウント権限をイントレーション フォルダに割り当て、サービス アカウントがエージェントのイントレーション フォルダにアクセスして設定の読み込みとログの書き込みを行えるようにします。

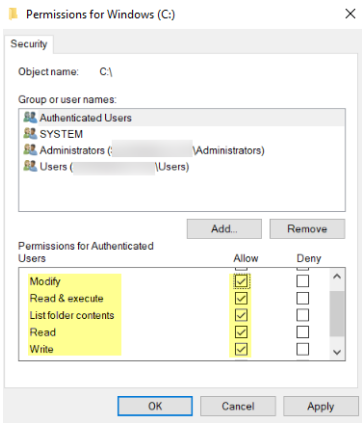
   User-ID エージェント用に構成したサービスアカウントが、User-ID エージェントサーバー ホスト上のドメイン管理者またはローカル管理者でない場合にのみ、このステップを実行する必要があります。

   1. 32-bit システムの場合、Windows Explorer で、**`C:\Program Files(x86)\Palo Alto Networks`** に移動し、フォルダを右クリックして **Properties** (プロパティ)を選択します。
   2. **Security** タブで、**Edit** をクリックします。



   3. User-ID エージェント サービス アカウントを **Add** (追加)し、**Modify** (変更)、**Read & execute** (読み取りと実行)、**List folder contents** (フォルダの内容の一覧表示)、**Read**

(読み取り)、および **Write** (書き込み)の権限を割り当て、**OK** をクリックしてアカウント設定を保存します。



サービス アカウントが *User-ID* エージェントのレジストリキーにアクセスできるようにする場合、***Full Control*** (全制御)権限を***Allow*** (許可)します。

4. ユーザー ID エージェントのレジストリ サブツリーにサービス アカウント権限を割り当てます。
   1. **regedt32** を実行し、以下の場所にある Palo Alto Networks サブツリーに移動します。`HKEY_LOCAL_MACHINE\Software\Palo Alto Networks`。
   2. Palo Alto Networks[Palo Alto Networks] ノードを右クリックし、**Permissions**[アクセス許可] を選択します。
   3. User-ID サービス アカウントに **Full Control**[フル コントロール] を割り当て、**OK**[OK] をクリックして設定を保存します。

STEP 2 | ユーザー ID エージェントをインストールする場所を決定します。

User-ID エージェントは、Microsoft Remote Procedure Calls（MSRPC）を使用してドメイン コントローラと Exchange サーバー ログを照会します。初回接続時に、エージェントはログから最新の 50,000 個のイベントをマップ ユーザーに転送します。後続の接続ごとに、エージェントはドメイン コントローラとの最後の通信よりも後のタイムスタンプでイベントを転送します。したがって、モニター対象のサーバーがあるサイトのそれぞれに、必ず 1 つ以上のユーザー ID エージェントをインストールします。

- ユーザー ID エージェントは、サポートされているいずれかの OS バージョンを実行しているシステムにインストールする必要があります。『互換性一覧』の「ユーザー ID エージェントのオペレーティング システム(OS)互換性」を参照してください。システムは、最小要件も満たしている必要があります (User-IDエージェントのリリース ノートを参照)。
- ユーザー ID エージェントをホストするシステムが、モニター対象のサーバーと同じドメインのメンバーであることを確認します。
- ベスト プラクティスとして、User-ID エージェントはモニター対象のサーバーの近くにインストールします(User-ID エージェントとモニター対象のサーバーの間のトラフィックは User-ID とファイアウォールの間のトラフィックより大きくなるため、エージェントをモニター対象のサーバーの近くに配置することで帯域幅使用が最適化されます)。

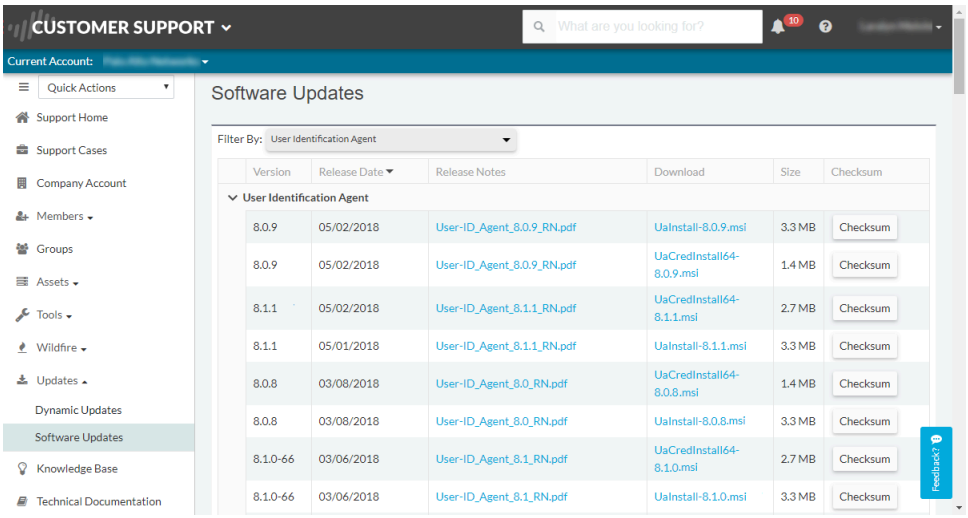
- ユーザーを最も包括的にマッピングするには、マップするユーザーの認証を処理するすべてのドメイン コントローラーを監視する必要があります。すべてのリソースを効率的にモニターするために、複数のユーザー ID エージェントをインストールする必要がある場合もあります。
- 認証情報検知に User-ID エージェントを使用している場合、それを読み取り専用ドメイン コントローラ（RODC）にインストールする必要があります。ベストプラクティスとして、この用途のために別のエージェントをデプロイメントするようにしてください。RODC にインストールされている User-ID エージェントを使用して IP アドレスをユーザーにマップしないでください。認証情報検知用の User-ID エージェントのインストーラーの名前は UaCredInstall64-x.x.x.msi です。

STEP 3 | ユーザー ID エージェント インストーラをダウンロードします。

ファイアウォール上で実行されている *PAN-OS* と同じバージョンのユーザー *ID* エージェントをインストールします。*PAN-OS* のバージョンと一致するバージョンの *User-ID* エージェントがない場合、 *PAN-OS* のバージョンに最も近い最新のバージョンのものをインストールしてください。

1. Palo Alto Networks カスタマー サポート ポータルにログインします。
2. **Updates**（更新） > **Software Updates**（ソフトウェア更新）を選択します。
3. **Filter By (**フィルタリング基準**)**を**User Identification Agent (**ユーザー **ID** エージェント**)**に設定し、インストールする User-ID エージェントのバージョンを、対応する Download (ダウンロード) 列で選択します。ファイル名は次の形式を使用します。`UaInstall-x.x.x.x.msi` (`x` はバージョン番号を表します)。たとえば、User-ID エージェントの 10.0 バージョンをダウンロードするには、**UaInstall-10.0.0-0.msi** を選択します。

   資格情報検出 にユーザー ID エージェントを使用している場合は、代わりに `UaCredInstall64-x.x.x.msi` ファイルをダウンロードします。資格情報の検出にユーザー ID を使用している場合は、`UaCredInstall64-x.x.x.msi` のみをダウンロードしてインストールします。
4. エージェントをインストールするシステムにファイルを保存します。



STEP 4 | 管理者としてインストーラを実行します。

1. Windows **Start**[スタート]メニューを開き、 **Command Prompt**[コマンドプロンプト]プログラムを右クリックして、 **Run as administrator**[管理者として実行]を選択します。
2. コマンド ラインから、ダウンロードした .msi ファイルを実行します。たとえば、.msi ファイルをデスクトップに保存した場合、以下のように入力します：

```
C:\Users\administrator.acme>cd Desktop
C:\Users\administrator.acme\Desktop>UaInstall-6.0.0-1.msi
```

3. デフォルトの設定を使用してエージェントをインストールするには、セットアップ プロンプトに従いします。既定では、エージェントは **C:**プログラム ファイル**(x86)Palo Alto Networks** にインストールされますが、**Browse** を別の場所にインストールできます。
4. インストール完了後、**Close**[閉じる] をクリックしてセットアップ ウィンドウを閉じます。

STEP 5 | 管理者としてユーザー ID エージェント アプリケーションを起動します。

Windows **Start (スタート)**メニューを開き、 **User-ID Agent (User-ID** エージェント**)**プログラムを右クリックして、**Run as administrator (**管理者として実行**)**を選択します。

アプリケーションのインストール、設定変更のコミット、アプリケーションのアンインストールを行うためには、管理者として *User-ID* エージェント アプリケーションを実行する必要があります。

STEP 6 | (任意)ユーザー ID エージェントがログインに使用するサービス アカウントを変更します。

デフォルトでは、エージェントは .msi ファイルのインストールに使用された管理者アカウントを使用します。アカウントを制限付きのアカウントに変更するには：

1. **User Identification (**ユーザー **ID)** > **Setup (**セットアップ**)** の順に選択し、**Edit (**編集**)** をクリックします。
2. **Authentication**[認証] タブを選択し、User-ID エージェントが使用するサービス アカウント名を **User name for Active Directory**[Active Directory 用のユーザー名] フィールドに入力します。
3. 指定したアカウントの **Password** [パスワード]を入力します。
4. User-ID エージェント構成の変更を**Commit**（コミット）し、サービス アカウントの証明書を使用してサービスを再起動します。

STEP 7 | （任意）Windows User-ID エージェントおよびファイアウォール間の相互認証に使用する独自の証明書を割り当てます。

1. 次のいずれかの方法を使用して、Windows User-ID エージェントの証明書を取得します。Privacy Enhanced Mail（PEM）形式のサーバー証明書とサーバー証明書の暗号化されたキーをアップロードします。
   - 証明書を作成して Windows User-ID エージェントにアップロードするためにエクスポートします。
   - 企業用の証明書認証局（CA）から証明書をエクスポートし、Windows User-ID エージェントにアップロードします。
2. Windows User-ID エージェントにサーバー証明書を追加します。
   1. Windows User-ID エージェントで **Server Certificate (**サーバー証明書**)** を選択し、**Add (**追加**)** をクリックします。
   2. CA から受信した証明書ファイルのパスと名前を入力するか、証明書ファイルを参照します。
   3. 秘密鍵のパスフレースを入力します。
   4. **(OK)** をクリックし、**(**コミット**)** をクリックします。
3. 証明書をファイアウォールにアップロードし、Windows User-ID エージェントの身元を検証します。
4. クライアント デバイスの証明書プロファイルを設定します（ファイアウォールまたは Pannorama）。
   1. **Device (**デバイス**)** > **Certificate Management (**証明書管理**)** > **Certificate Profile (**証明書プロファイル**)** を選択します。
   2. 証明書プロファイルの設定を行います。

      Windows User-ID エージェントおよびターミナル サーバー（*TS*）エージェントに対して割り当てられる証明書プロファイルは一つだけです。そのため証明書プロファイルには、*User-ID* エージェントおよび *TS* エージェントを接続するためにアップロードした証明書を発行した認証局がすべて含まれていなければなりません。
5. ファイアウォール上で証明書プロファイルを割り当てます。
   1. **Device (**デバイス**)** > **User Identification (**ユーザー **ID)** > **Connection Security (**接続セキュリティ**)** を選択し、編集ボタンをクリックします。
   2. 前のステップで設定した**User-ID Certificate Profile (User-ID** 証明書プロファイル**)**を選択します。
   3. **OK** をクリックします。
6. 変更をコミットします。

STEP 8 | Windows ベースの User-ID エージェントを使用する認証情報検知の設定を行います。

Windows ベースの User-ID エージェントを使用して認証情報の送信を検知して 証明書フィッシングの阻止を行うためには、Windows ベースの User-ID エージェント上に User-ID 認証情

報サービスをインストールする必要があります。このアドオンは読み取り専用ドメイン コントローラ（RODC）上でのみインストールできます。

ユーザー マッピングのための Windows の User-ID エージェントの設定

Palo Alto Networks Windows ユーザー ID エージェントは、ネットワーク上のサーバー (Active Directory サーバー、Microsoft Exchange サーバー、Novell eDirectory サーバーなど) に接続し、ログイン イベントのログを監視する Windows サービスです。エージェントはこの情報を使用して IP アドレスをユーザー名にマッピングします。Palo Alto Networks のファイアウォールはユーザー ID エージェントに接続してこのユーザー マッピング情報を取得します。これにより、 IP アドレスではなくユーザー名でのユーザー アクティビティへの可視性が得られ、ユーザーベースおよびグループベースのセキュリティ実施が可能になります。

ユーザー *ID* エージェントでサポートされるサーバー *OS* のバージョンの詳細は、『ユーザー ID エージェント リリース ノート』の「ユーザー *ID* エージェントのオペレーティング システム*(OS)*互換性」を参照してください。

STEP 1 | IP アドレス対ユーザーのマッピング情報を収集するためにユーザー ID エージェントがモニタリングするサーバーを定義します。

User-ID エージェントは最大100個(うち最大50個がsyslog senders)までのサーバーをモニターできます。

必要なマッピング情報をすべて収集するには、ユーザーがログインするすべてのサーバーに *User-ID* エージェントが接続し、ログイン イベントを含むすべてのサーバーのセキュリティ ログ ファイルをモニタリングできるようにする必要があります。

1. Windows **Start**[スタート]メニューを開いて、 **User-ID Agent**[ユーザーIDエージェント]を選択します。
2. **User Identification (ユーザー ID)** > **Discovery (検出)** の順に選択します。
3. 画面の **Servers**[サーバー]セクションで **Add**[追加] をクリックします。
4. モニター対象のサーバーの **Name**[名前] と **Server Address**[サーバー アドレス] を入力します。ネットワーク アドレスには、FQDN または IP アドレスを指定できます。
5. **Microsoft Active Directory**[サーバー タイプ](**Microsoft Active Directory**[Microsoft Active Directory]、**Microsoft Exchange**[Microsoft Exchange]、**Novell eDirectory**[Novell eDirectory]、または**Syslog Sender**[Syslog Sender])を選択し、**OK**[OK] をクリックしてサーバー エントリを保存します。モニター対象の各サーバーに対してこの手順を繰り返します。
6. (オプション) Dns ルックアップを使用してネットワーク上のドメイン コントローラを Windows ユーザー ID エージェントが自動的に検出できるようにするには、自動検出をクリックします。Windows User-ID エージェントで検出する新しいドメイン コント

ローラーがある場合は、新しいドメイン コントローラーを検出するたびに 自動検出 をクリックします。

自動検出で検出できるのはローカル ドメイン内のドメイン コントローラのみです。*Exchange* サーバー、*eDirectory* サーバー、および *Syslog* 送信元は手動で追加する必要があります。

7. （任意）ファイアウォールが設定済みサーバーに対してマッピング情報をポーリングする頻度を調整するには、**User Identification (ユーザー ID)** > **Setup (セットアップ)** の順に選択し、Setup (セットアップ) セクションの **Edit (編集)** を選択します。**Server Monitor**[サーバー モニタ] タブで、**Server Log Monitor Frequency (seconds)**[サーバー ログのモニター頻度(秒)] フィールドの値を変更します。ドメイン コントローラが古い環境やリンクの遅延が大きな環境の場合、このフィールドの値を 5 秒に増やします。

   Enable Server Session Read (サーバーセッションの読取りを有効化*)* の設定が選択されていないことを確認します。この設定では、すべてのユーザー セッションを読み取ることができるように *User-ID* エージェントにサーバー オペレータ権限のある *Active Directory* アカウントが必要です。代わりに、*Syslog* または *XML API* 統合を使用して、すべてのデバイス タイプとオペレーティング システム（*Windows* だけでなく）のログインおよびログアウト イベントをキャプチャするソース（ワイヤレス コントローラやネットワーク アクセス コントローラ（*NAC*）など）を監視します。

8. **OK** をクリックして設定を保存します。

STEP 2 | Windows User-ID エージェントが User-ID に含める、あるいは除外すべきサブネットワークを指定します。

デフォルト設定の User-ID は、監視中のサーバーにアクセスしているすべてのユーザーをマッピングします。

ベストプラクティスとして、必ず *User-ID* に含める、あるいは除外するネットワークを指定し、エージェントが内部リソースのみと通信を行い、不正なユーザーがマッピングされないようにしてください。組織内のユーザーがログインしているサブネットワークの *User-ID* のみを有効化する必要があります。

1. **User Identification (ユーザー ID)** > **Discovery (検出)** の順に選択します。
2. 設定済みのネットワークの Include/Exclude (許可/除外) リストに項目を **Add (追加)** し、その項目の **Name (名前)** を入力し、**Network Address (ネットワーク アドレス)** としてサブネットワークの IP アドレス範囲を入力します。
3. ネットワークを含めるか、除外するかを選択します。
   - **Include specified network (指定したネットワークを含める)**—ユーザーマッピングを指定したサブネットワークにログインしているユーザーのみに制限する場合は、このオプションを選択します。例えば 10.0.0.0/8 を含める場合、エージェントはユーザーをそのサブネットワークにマッピングし、他をすべて除外します。エージェントに他のサブネットワークに存在するユーザーをマッピングさせたい場合は、これらのステップを繰り返し、追加のネットワークをリストに追加してください。

- **Exclude specified network (**指定したネットワークを除外する**)**—追加して含めたサブネットワークのサブセットをエージェントに除外させたい場合のみ、このオプションを選択します。例えば 10.0.0.0/8 を含めて 10.2.50.0/22 を除外する場合、エージェントは 10.2.50.0/22 を除く 10.0.0.0/8 のサブネットワークにユーザーをマッピングし、10.0.0.0/8 の外部のサブネットワークをすべて除外します。

  許可プロファイルを一切追加せずに除外プロファイルを追加する場合、*User-ID* エージェントは、追加したサブネットワークだけでなく、すべてのサブネットワークを除外します。

4. **OK** をクリックします。

STEP 3 | (任意)エージェントが Novell eDirectory サーバーに接続するように設定した場合、エージェントがディレクトリを検索する方法を指定する必要があります。

1. **User Identification (**ユーザー **ID)** > **Setup (**セットアップ**)** の順に選択し、ウィンドウの Setup (セットアップ) セクションの **Edit (**編集**)** をクリックします。
2. **eDirectory** [eDirectory]タブを選択し、以下のフィールドを入力します。
   - **Search Base** [検索ベース]— エージェントによるクエリの開始点またはルート コンテキスト。（`dc=domain1,dc=example, dc=com`）.
   - **Bind Distinguished Name** [識別名のバインド] — ディレクトリにバインドするために使用するアカウント。例: `cn=admin,ou=IT, dc=domain1, dc=example, dc=com`.
   - **Bind Password** [バインド パスワード]— バインド アカウントのパスワード。エージェントは、暗号化したパスワードを設定ファイルに保存します。
   - **Search Filter**[検索フィルタ] — ユーザー エントリの検索クエリ(デフォルトは `objectClass=Person`)。
   - **Server Domain Prefix**[サーバー ドメイン プレフィックス] — ユーザーを一意に識別するためのプレフィックス。これは、名前空間に重複がある場合(たとえば他のディレクトリからの同じ名前の異なるユーザーなど)にのみ必要です。
   - SSL の使用 — eDirectory バインドに SSL を使用するには、このチェック ボックスをオンにします。
   - **Verify Server Certificate** — SSL 使用時に eDirectory サーバー証明書を検証する場合はこのチェック ボックスをオンにします。

STEP 4 | (強く推奨)クライアントのプローブを無効にします。

*Palo Alto Networks*は、高セキュリティネットワーク上でクライアントの調査を無効にすることを強く推奨します。クライアントプローブは、正しく設定されていない場合、セキュリティ上の脅威を引き起こす可能性があります。詳細については、「クライアントプローブ」を参照してください。

1. クライアントプローブ タブで、[**WMI** プローブを有効にする チェック ボックスが有効な場合はオフにします。
2. 有効になっている場合は、 **NetBIOS** プローブ を有効にする] チェック ボックスをオフにします。

Palo Alto Network では、ドメイン コントローラや Syslog または XML API との統合など、分離および信頼されたソースからユーザー マッピング情報を収集して、あらゆる種類のデバイスまたはオペレーティング システムからユーザー マッピング情報を安全にキャプチャすることを強くお勧めします。

クライアントプローブを有効にする必要がある場合は、*[**WMI** プローブを有効にする チェック ボックスをオンにし、[クライアント プローブ タブで選択します。この方法のセキュリティ上のリスクが生じ、ファイアウォールが他の方法でユーザー マッピングを取得できない場合は、[**NetBIOS** プローブを有効にする を有効にする] チェック ボックスのみをオンにします。次に、プローブされた各クライアントの *Windows* ファイアウォールにリモート管理例外を追加して、*Windows* ファイアウォールでクライアントのプローブが許可されるようにします。プローブされた各クライアント *PC* では、*Windows* ファイアウォールでポート *139* を許可し、ファイルとプリンタの共有サービスも有効にする必要があります。*

STEP 5 | 設定を保存します。

OK[OK] をクリックしてユーザー ID エージェントのセットアップ設定を保存し、**Commit** [コミット]をクリックしてユーザー ID エージェントを再起動し、新しい設定をロードします。

STEP 6 | （任意）サービス アカウントや kiosk アカウントなど、IP アドレス対ユーザー名のマッピングが不要な一連のユーザーを定義します。

タイトルを `ignore_user_list`、拡張子を .txt ファイルにして `ignore-user` リストをテキストドキュメントとしてエージェント ホストに保存し、エージェントをインストールしたドメインサーバーの User-ID エージェント フォルダに保存します。

無視するユーザー アカウントをリストします。リストに追加するアカウント数に制限はありません。各ユーザー アカウント名は、1 行ずつ指定する必要があります。以下に例を示します。

```
SPAdmin
SPInstall
```

```
TFSReport
```

アスタリスクをワイルドカード文字として使用して、複数のユーザーネームと一致させることが可能ですが、エントリの最後の文字としてのみ使用できます。例えば `corpdomain\it-admin*` は `corpdomain` のドメイン内で `it-admin`から始まるユーザー名をもつすべての管理者と一致します。また、`ignore-user` リストを使用すると、認証ポータルを使用して強制的に認証するユーザーを識別できます。

Ignore User (ユーザーを無視) リストにエントリを追加した後は、サービスへの接続を一旦停止し、再開する必要があります。

STEP 7 | ファイアウォールが User-ID エージェントと接続するように設定します。

ファイアウォールは、*User-ID* 認証情報サービスのアドオンを使用して企業認証情報の送信を検知する単体の *Windows* ベースの *User-ID* エージェントにのみ接続できます。認証情報フィッシング詐欺を防止するためにこのサーバーを使用する詳細な方法については、Windows ベースの User-ID エージェントを使用する認証情報検知を設定を参照してください。

ユーザー マッピングの取得のためにユーザー ID エージェントに接続する各ファイアウォールで、以下の手順を実行します。

1. **Device (デバイス)** > **Data Redistribution (データ再配布)** > **Agents (エージェント)** を選択し、**Add (追加)** をクリックします。
2. エージェントの **Name (名前)** を入力します。
3. **Add an Agent Using**（次を使用してエージェントを追加）で **Host and Port**（ホストおよびポート）を使用してエージェントを追加します。
4. **Host** [ホスト]に、User-ID エージェントがインストールされている Windows ホストの IP アドレスを入力します。
5. エージェントがユーザー マッピング要求をリッスンする **Port** [ポート]番号(1 ～ 65535)を入力します。この値は、ユーザー ID エージェント上で設定された値と一致する必要があります。ファイアウォールおよび新しいバージョンのユーザー ID エージェントでは、ポートはデフォルトで 5007 に設定されます。ただし、一部の古いバージョンのユーザー ID エージェントはデフォルトでポート 2010 を使用します。
6. **IP User Mappings**（**IP** ユーザー マッピング）を **Data type**（データ タイプ）として選択します。
7. 設定が **Enabled** [有効]になっていることを確認し、**OK** [OK]をクリックします。
8. 変更を **Commit**（コミット）します。
9. **Connected status (接続済みの状態)** が接続済み(緑色のライト)と表示されていることを確認します。

STEP 8 | ユーザー ID エージェントが IP アドレスをユーザー名に正しくマッピングしていることと、ファイアウォールがエージェントに接続できることを確認します。

1. User-ID エージェントを起動し、**User Identification**[ユーザー ID] を選択します。
2. エージェントの状態が、**Agent is running**[エージェントは実行中です] になっていることを確認します。エージェントが実行されていない場合は、**Start**[開始] をクリックします。
3. User-ID エージェントがモニター対象のサーバーに接続できることを確認するには、各サーバーの状態が**Connected**[接続済み] になっていることを確認します。
4. ファイアウォールが User-ID エージェントに接続できることを確認するには、接続済みデバイスそれぞれの状態が**Connected**[接続済み] になっていることを確認します。
5. User-ID エージェントが IP アドレスをユーザー名にマッピングしていることを確認するには、**Monitoring**[モニタリング] を選択し、マッピング テーブルにデータが入力されていることを確認します。特定のユーザーを **Search**[検索] したり、ユーザー マッピングをリストから **Delete** [削除]したりできます。

PAN-OS 統合 User-ID エージェントを使用したユーザー マッピングの設定

以下の手順では、ファイアウォール上の PAN-OS® 統合 User-ID™ エージェントを IP アドレスからユーザー名へのマッピングのために設定する方法を示します。統合 User-ID エージェントは、Windows ベースのエージェントと同じタスクを実行しますが、例外として NetBIOS クライアント プローブはサポートされていません(WMI プローブはサポートされています)。

STEP 1 | User-IDエージェントがユーザー マッピング情報を収集するためにファイアウォールが監視するサービスとホストにアクセスできるようにActive Directory (アクティブディレクトリ - AD) サービスを作成します。

ユーザーID エージェントの専用サービス アカウントを作成します。

STEP 2 | ファイアウォールでモニタリングするサーバーを定義し、ユーザーのマッピング情報を収集します。

ファイアウォールあたり監視対象サーバー最大100 個の範囲で、バーチャルシステム1個につき、50個を超える syslog sender は定義できません。

必要なマッピング情報をすべて収集するには、ファイアウォールはユーザーがログインしているすべてのサーバーに接続し、ログイン イベントを含むすべてのサーバーのセキュリティ ログ ファイルを監視できるようにする必要があります。

1. **Device (デバイス)** > **User Identification (ユーザー ID)** > **User Mapping (ユーザー マッピング)** の順に選択します。
2. サーバー（サーバー モニタリング セクション）を **Add**（追加）します。
3. サーバーの識別に使用する**Name**[名前]を入力します。
4. サーバーの**Type**[タイプ]を選択します。
   - **Microsoft Active Directory**
   - **Microsoft Exchange**
   - **Novell eDirectory**
   - **Syslog Sender**
5. (Microsoft Active Directory および Microsoft Exchange のみ) サーバー上のセキュリティ ログとセッション情報の監視に使用する **Transport Protocol (トランスポートプロトコル)** を選択します。
   - **WMI**—ファイアウォールと監視対象サーバーは、Windows Management Instrumentation (WMI) を使用して通信を行います。
   - **WinRM-HTTP**—ファイアウォールと監視対象サーバーは相互認証に Kerberos を使用し、監視対象サーバーはネゴシエートされた Kerberos セッション鍵を使用してファイアウォールとの通信を暗号化します。
   - **WinRM-HTTPS**—ファイアウォールと監視対象サーバーは HTTPS を使用して通信し、相互認証に基本認証または Kerberos を使用します。

   Windows Remote Management (WinRM) オプションを選択した場合は、WinRM を使用するサーバー監視の設定する必要があります。
6. (Microsoft Active Directory、Microsoft Exchange、および Novell eDirectory のみ) サーバーの **Network Address (ネットワークアドレス)** を入力します。

Kerberos で WinRM を使用している場合、完全修飾ドメイン名 *(FDQN)* を入力する必要があります。WinRM を基本認証で使用する場合、または ***WMI*** を使用してサーバーを監視する場合は、*IP* アドレスまたは *FQDN* を入力することができます。

WMI を使用してサーバーを監視するには、*IP* アドレス、サービスアカウント名 *(*すべてのサーバー監視が同じドメインにある場合*)*、または完全修飾ドメイン名 *(FQDN)* を指定します。*FQDN* を指定する場合は、*FQDN \sAMAccountName* 形式ではなく、*(DLN)\sAMAccountName* 形式のダウンレベル ログオン名を使用します。例えば、***example.com\user.services*** ではなく ***example\user.services*** を使用します。*FQDN* を指定すると、ファイアウォールは、*WMI* をサポートしない *Kerberos* を使用して認証を試みます。

7. (Syslog Sender only) サーバー **Type** として **Syslog Sender** を選択した場合、PAN-OS 統合 User-ID エージェントを Syslog リスナーとして設定します。
8. (Novell eDirectory のみ) 選択した **Server Profile (**サーバープロファイル**)** が **Enabled (**有効**)** になっていることを確認し、**OK** をクリックします。
9. （任意）DNS 検索を使用してネットワーク上のドメイン コントローラを自動的に**Discover**（検出）するようにファイアウォールを設定します。

   自動検出機能は、ドメイン コントローラの場合のみ有効です。*Exchange* サーバーや *eDirectory* サーバーをモニタリングする場合、手動でそれらを追加する必要があります。

STEP 3 | （任意）ファイアウォールが Windows サーバーに対してマッピング情報をポーリングする頻度を指定します。これは、前回のクエリが終了してから次のクエリが開始されるまでの間隔です。

ドメインコントローラが多くの要求を処理している場合、クエリ間の遅延が指定された値を超える場合があります。

1. **Palo Alto Networks User ID Agent Setup (Palo Alto Networks** ユーザー **ID** エージェントのセットアップ**)**を**Edit**（編集）します。
2. **Server Monitor(**サーバー モニタ**)** タブを選択し、**Server Log Monitor Frequency (**サーバー ログのモニター頻度**)**を秒単位で指定します(範囲は 1 ～ 3600、デフォルトは 2)。

ドメイン コントローラが古い環境やリンクの遅延が大きな環境の場合、この頻度を最低 5 秒に設定します。

Enable Session **(**セッションの有効化**)** オプションが有効でないことを確認します。このオプションでは、すべてのユーザー セッションを読み取ることができるように *User-ID* エージェントにサーバー オペレータ権限のある *Active Directory* アカウントが必要です。代わりに、*Syslog* または *XML API* 統合を使用して、すべてのデバイス タイプとオペレーティング システム（*Windows* だけでなく）のログインおよびログアウト イベントをキャプチャするソース（ワイヤレス コントローラや*Network Access Control (* ネットワーク アクセス制御 - *NAC)*デバイスなど）を監視します。

3. **OK** をクリックして変更内容を保存します。

STEP 4 | PAN-OS 統合 User-ID エージェントがユーザーマッピングに含める、あるいは除外すべきサブネットワークを指定します。

デフォルト設定の User-ID は、監視中のサーバーにアクセスしているすべてのユーザーをマッピングします。

ベストプラクティスとして、必ず含めるネットワーク、および任意で *User-ID* から除外するネットワークを指定し、エージェントが内部リソースのみと通信を行い、不正なユーザーがマッピングされないようにしてください。組織内のユーザーがログインしているサブネットワークのユーザーマッピングのみを有効化する必要があります。

1. **Device (**デバイス**)** > **User Identification (**ユーザー **ID)** > **User Mapping (**ユーザー マッピング**)** の順に選択します。
2. **Include/Exclude Networks (**ネットワークの許可/除外**)**にエントリを**Add**（追加）し、エントリの**Name**（名前）を入力します。エントリが**Enabled**（有効）であることを確認します。
3. **Network Address (**ネットワーク アドレス**)** を入力し、それを含めるか除外するかを選択します。
   - **Include (**許可**)**—ユーザーマッピングを指定したサブネットワークにログインしているユーザーのみに制限するこのオプションを選択します。例えば 10.0.0.0/8 を含める場合、エージェントはユーザーをそのサブネットワークにマッピングし、他をすべて除外します。エージェントに他のサブネットワークに存在するユーザーをマッピングさせたい場合は、これらのステップを繰り返し、追加のネットワークをリストに追加してください。
   - **Exclude (**除外**)**—このオプションを選択して、追加して含めたサブネットワークのサブセットを除外するようエージェントを設定します。例えば 10.0.0.0/8 を含めて 10.2.50.0/22 を除外する場合、エージェントは 10.2.50.0/22 を除く 10.0.0.0/8 のサ

ブネットワークにユーザーをマッピングし、10.0.0.0/8 の外部のサブネットワークをすべて除外します。

許可プロファイルを一切追加せずに除外プロファイルを追加する場合、*User-ID* エージェントは、追加したサブネットワークだけでなく、すべてのサブネットワークを除外します。

4. **OK** をクリックします。

STEP 5 | ファイアウォールで Windows リソースへのアクセスに使用する、アカウントのドメイン認証情報を設定します。この設定は Exchange サーバーとドメイン コントローラのモニター、および WMI プロービングに必要です。

1. **Palo Alto Networks User-ID Agent Setup (Palo Alto Networks** ユーザー **ID** エージェントのセットアップ**)**を**Edit**（編集）します。
2. **Server Monitor Account (**サーバーモニターアカウント**)** タブを選択して、User-ID エージェントがクライアントのプローブとサーバーのモニタリングに使用するサービスアカウントに **User Name (**ユーザー名**)** と **Password (**パスワード**)** を入力します。**`domain\username`** 構文を使用してユーザー名を入力します。
3. WinRM を使用してサーバーを監視している場合は、監視しているサーバーで認証するようにファイアウォールを構成します。
   - 基本認証で WinRM を使用する場合は、サーバーで WinRM を有効にし、基本認証を構成し、サービスアカウント **Domain's DNS Name (**ドメインの **DNS** 名**)** を指定します。
   - Kerberos で WinRM を使用する場合は、 Configure a Kerberos server profile(Kerberos サーバープロファイルを設定)していない場合は設定してから、**Kerberos Server Profile (Kerberos** サーバープロファイル**)** を選択します。

STEP 6 | （任意、非推奨）WMI プロービングを設定します（PAN-OS 統合 User-ID エージェントは NetBIOS プロービングをサポートしていません）。

セキュリティの高いネットワークでは、*WMI* プロービングを有効にしないでください。クライアントに対するプローブでは、大量のネットワーク トラフィックが生成される場合があり、設定に誤りがあるとセキュリティ上の脅威が発生する可能性があります。

1. **Client Probing (**クライアントプローブ**)** タブで、**Enable Probing (**プローブを有効化**)** します。
2. (任意) **Probe Interval (**プローブ間隔**)** を指定して、最後のプローブ要求の終了から、次の要求が開始されるまでの間隔 (分単位) を定義します。

   必要に応じて、値を大きくして、User-ID エージェントが学習したすべての IP アドレスをプローブするのに十分な時間を確保します (範囲は 1 ~ 1440、デフォルトは 20)。

   要求の負荷が高い場合、観測された要求間の遅延は指定された間隔を大幅に超える可能性があります。
3. **OK** をクリックします。
4. Windows ファイアウォールで、プロービング対象のクライアントごとにリモート管理の例外を追加することにより、クライアントのプロービングを許可することを確認します。

STEP 7 | (任意) kiosk アカウントなど、IP アドレス対ユーザー名のマッピングが不要な一連のユーザーアカウントを定義します。

クライアントではなく、ユーザー *ID* エージェントであるファイアウォールの無視ユーザーリストを定義します。クライアントファイアウォールで無視ユーザーリストを定義した場合、リスト内のユーザーは再配布中にマッピングされます。

Ignore User List（ユーザー リストを無視）タブ上で、ユーザー マッピングから除外するユーザー名を**Add**（追加）します。また、この設定を利用して、認証ポータルを使用して強制的に認証させるユーザーを識別できます。アスタリスクをワイルドカード文字として使用しte複数のユーザーネームと一致させることが可能ですが、エントリの最後の文字としてのみ使用できます。例えば **`corpdomain\it-admin*`** は `corpdomain` のドメイン内で `it-admin`から始まるユーザー名をもつすべての管理者と一致します。ユーザー マッピングから除外するエントリを最大 5,000 個まで追加することができます。

STEP 8 | 設定の変更を起動します。

OK、**Commit (**コミット**)** の順にクリックします。

STEP 9 | 設定を確認します。

1. ファイアウォール CLI にアクセスします。
2. 以下の CLI コマンドを入力します。

```
> show user server-monitor state all
```

3. Web インターフェースで **Device (デバイス)** > **User Identification (ユーザー ID)** > **User Mapping (ユーザー マッピング)** の順に選択して、サーバーのモニタリング用に設定したサーバーごとに、Status (状態) が `Connected` (接続済み) になっていることを確認します。

WinRM を使用するサーバー監視の設定

PAN-OS 統合ユーザー ID エージェントを設定して、Windows リモート管理 (WinRM) を使用してサーバーを監視することができます。WinRM プロトコルを使用すると、ユーザーイベントを IP アドレスにマッピングする際の速度、効率、およびセキュリティが向上します。PAN-OS統合User-IDエージェントは、Windows Server 2012 Active Directory (アクティブディレクトリ - AD)、およびMicrosoft Exchange Server 2012 以降の両方のバージョンで WinRM プロトコルをサポートします。

WinRM を使用してサーバー監視を構成するには、3 つの方法があります。

- 基本認証を使用して HTTPS 経由で WinRM を構成する:ファイアウォール はユーザ ID エージェントのサービス アカウントのユーザ名とパスワードを使用して監視対象サーバに対して認証を行い、ファイアウォール はユーザ ID 証明書プロファイルを使用して監視対象サーバを認証します。
- WinRM を HTTP 経由で Kerberos で構成する:ファイアウォール と監視対象サーバは相互認証に Kerberos を使用し、監視対象サーバはネゴシエートされた Kerberos セッション キーを使用して ファイアウォール との通信を暗号化します。
- WinRM を HTTPS 経由で Kerberos で構成する:ファイアウォール と監視対象サーバは HTTPS を使用して通信し、相互認証に Kerberos を使用します。

基本認証を使用して HTTPS 経由で WinRM を構成する

基本認証で HTTPS を使用するように WinRM を構成すると、ファイアウォールは SSL を使用して安全なトンネルでサービスアカウントの資格情報を転送します。

STEP 1 | 監視するサーバーのリモート管理ユーザーと CIMV2 特権で サービスアカウントを設定します。

STEP 2 | 監視している Windows サーバーで、WinRM で使用する Windows サーバーの証明書から拇印を取得し、WinRM を有効にします。

管理者特権を持つアカウントを使用して、監視するサーバーで *WinRM* を構成していることを確認します。セキュリティのベスト プラクティスとして、このアカウントは手順 *1* のサービス アカウントと同じアカウントにしないでください。

1. 証明書がローカルコンピューターの証明書ストアにインストールされていることを確認します (**Certificates (Local Computer) (**証明書 **(**ローカルコンピューター**))** > **Personal (**パーソナル**)** > **Certificates (**証明書**)**)。

   ローカルコンピューターの証明書ストアが表示されない場合は、Microsoft 管理コンソール (**Start (**スタート**)** > **Run (**実行**)** > **MMC**) を起動し、証明書スナップイン (**File (**ファイル**)** > **Add/Remove Snap-in (**スナップインの追加/削除**)** > **Certificates (**証明書**)** > **Add (**追加**)** > **Computer account (**コンピューターアカウント**)** > **Next (**次へ**)** > **Finish (**完了**)**) を追加します。
2. 証明書を開き、**General** > **Details** > **Show: <All>** を選択します。
3. **Thumbprint**（拇印）を選択し、コピーします。
4. WinRM を使用してファイアウォールが Windows サーバーに接続できるようにするには、コマンド **`winrm quickconfig`**を入力します。
5. **y** を入力して変更を確認して、出力に `WinRM service started` と表示されていることを確認します。

   WinRM が有効になっている場合、出力には、`WinRM service is already running on this machine` と表示されます。追加の必要な構成変更を確認するよう求められます。
6. WinRM が HTTPS を使用して通信していることを確認するには、コマンド ：**`winrm enumerate winrm/config/listener`** を入力し、出力に `Transport = HTTPS` と表示されていることを確認します。

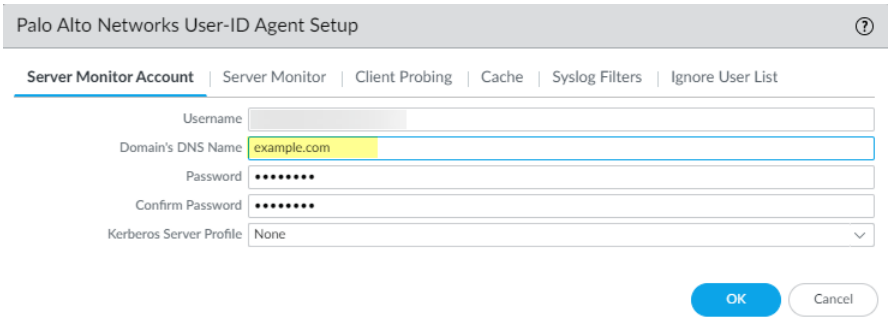
   デフォルトでは、WinRM/HTTPS はポート 5986 を使用します。
7. Windows サーバーのコマンド プロンプトから、次のコマンドを入力します: **`winrm create winrm/config/Listener?Address=*+ Transport=HTTPS @{ Hostname="<hostname>";CertificateThumbprint="Certificate Thumbprint"}`**。ここで、*hostname* は Windows サーバーのホスト名、*Certificate Thumbprint* は証明書からコピーした値です。

   コマンドプロンプト（*Powershell* ではなく）を使用し、証明書の拇印のスペースを削除して、*WinRM* が証明書を検証できることを確認します。
8. Windows サーバーのコマンドプロンプトから、コマンド

   ```
   c:\> winrm set winrm/config/client/auth @{Basic="true"}
   ```
9. **`winrm get winrm/config/service/Auth`** を入力して、`Basic = true` となっていることを確認します。

STEP 3 | PAN-OS 統合ユーザー ID エージェントと監視対象サーバー間の基本認証を有効にします。

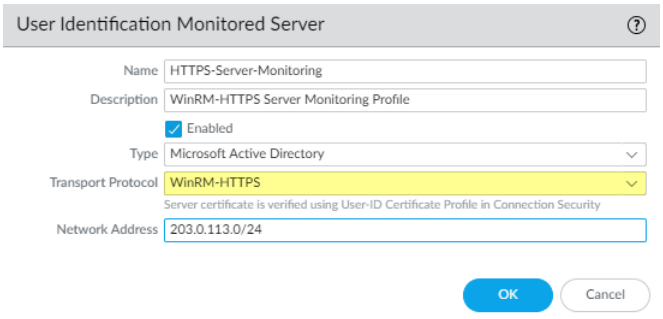
1. **Device (デバイス)** > **User Identification (User-ID)** > **User Mapping (ユーザーマッピング)** > **Palo Alto Networks User-ID Agent Setup (Palo Alto Networks User-ID エージェントの設定)** > **Server Monitor Account (サーバーモニターアカウント)** を選択します。
2. **`Domain\username`** 形式では、User-ID エージェントがサービスの監視に使用するサービスアカウント名に **User Name (ユーザー名)** を入力します。
3. サーバーモニターアカウントの **Domain's DNS Name (ドメインの DNS 名)** を入力します。



4. サービスアカウントの **Password (パスワード)** と **Confirm Password (パスワードの確認)** を入力します。
5. **[OK]** をクリックします。

STEP 4 | PAN-OS 統合 User-ID エージェント用に サーバー監視を設定します。

1. Microsoft サーバー **Type (タイプ)** (**Microsoft Active Directory (Microsoft アクティブディレクトリ)** または **Microsoft Exchange**) を選択します。
2. HTTPS 経由の Windows リモート管理 (WinRM) を使用してサーバー セキュリティ ログとセッション情報を監視するには、**Transport Protocol (転送プロトコル)** として **Win-RM-HTTPS** を選択します。

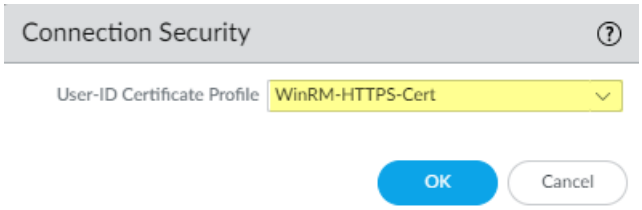


3. サーバーの IP アドレスまたは FQDN **Network Address (ネットワークアドレス)** を入力します。

STEP 5 | PAN-OS 統合 User-ID エージェントが WinRM-HTTPS を使用して監視対象サーバーと通信できるようにするには、Windows サーバーが WinRM に使用するサービス証明書のルート

証明書をファイアウォールに正常にインポートし、その証明書を User-ID 証明書プロファイルに関連付けていることを確認します。

1. **Device (デバイス)** > **User Identification (ユーザー ID)** > **Connection Security (接続セキュリティ)** を選択します。
2. **Edit**（編集）をクリックします。
3. **User-ID Certificate Profile (User-ID 証明書プロファイル)** に使用する Windows サーバー証明書を選択します。



4. **OK** をクリックします。

STEP 6 | 変更を **Commit (コミット)**します。

STEP 7 | 各監視対象サーバーのステータスが Connected (接続済み) であることを確認します (**Device (デバイス)** > **User Identification (ユーザー ID)** > **User Mapping (ユーザー マッピング)**)。

WinRM を HTTP 経由で Kerberos で構成する

WinRM を HTTP 経由で Kerberos で構成すると、ファイアウォールと監視対象サーバーは相互認証に Kerberos を使用し、監視対象サーバーはネゴシエートされた Kerberos セッション鍵を使用しファイアウォールとの通信を暗号化します。

Kerberos を使用した *WinRM* は、*aes128-cts-hmac-sha1-96* および *aes256-cts-hmac-sha1-96* 暗号をサポートしています。監視するサーバーが *RC4* を使用している場合、*Windows* アップデート をダウンロードし、監視するサーバーのレジストリ設定で *Kerberos* の *RC4* を 無効化しなければなりません。

STEP 1 | 監視するサーバーのリモート管理ユーザーと CIMV2 特権で サービスアカウントを設定します。

STEP 2 | 監視している Windows サーバーで WinRM が有効になっていることを確認します。

管理者特権を持つアカウントを使用して、監視するサーバーで *WinRM* を構成していることを確認します。セキュリティのベスト プラクティスとして、このアカウントは手順 *1* のサービス アカウントと同じアカウントにしないでください。

1. WinRM を使用してファイアウォールが Windows サーバーに接続できるようにするには、コマンド **`winrm quickconfig`**を入力します。
2. **`y`** を入力して変更を確認して、出力に `WinRM service started` と表示されていることを確認します。

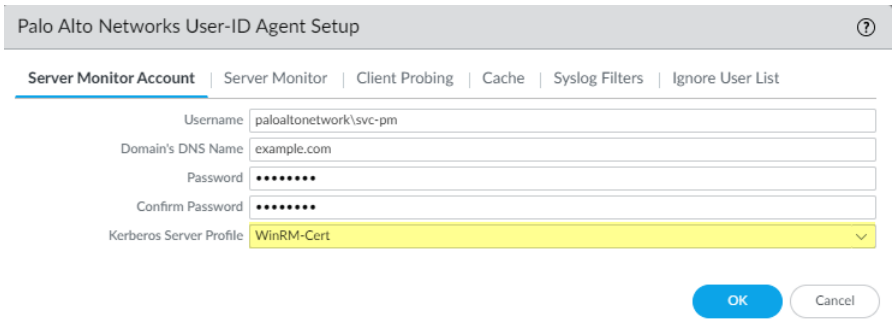
   WinRM が有効になっている場合、出力には、`WinRM service is already running on this machine` と表示されます。追加の必要な構成変更を確認するよう求められます。
3. WinRM が HTTPS を使用して通信していることを確認するには、コマンド ：**`winrm enumerate winrm/config/listener`** を入力し、出力に `Transport = HTTPS` と表示されていることを確認します。

   デフォルトでは、WinRM/HTTPS はポート 5985 を使用します。
4. **`winrm get winrm/config/service/Auth`** を入力して、`Basic = true` となっていることを確認します。

STEP 3 | PAN-OS 統合ユーザー ID エージェントと監視対象サーバーが Kerberos を使用して認証できるようにします。

1. initial configuration（初期設定）中にそうしなかった場合は、Kerberos ネゴシエーションが正常に行われるように日付と時刻 (NTP) を設定します。
2. ファイアウォールで Kerberos サーバープロファイルを設定して、サーバーで認証し、セキュリティログとセッション情報を監視します。
3. **Device (デバイス)** > **User Identification (User-ID)** > **User Mapping (ユーザーマッピング)** > **Palo Alto Networks User-ID Agent Setup (Palo Alto Networks User-ID** エージェントの設定) > **Server Monitor Account (サーバーモニターアカウント)** を選択します。
4. **`Domain\username`** 形式では、User-ID エージェントがサービスの監視に使用するサービスアカウント名に **User Name (ユーザー名)** を入力します。
5. サーバーモニターアカウントの **Domain's DNS Name (ドメインの DNS 名)** を入力します。

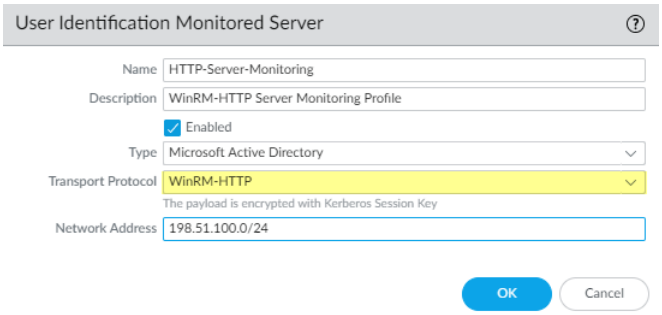
   Kerberos はドメイン名を使用して、サービスアカウントを探します。
6. サービスアカウントの **Password (パスワード)** と **Confirm Password (パスワードの確認)** を入力します。
7. ステップ 3.2 で設定した **Kerberos Server Profile (Kerberos サーバー プロファイル)** を選択します。



8. **OK** をクリックします。

STEP 4 | PAN-OS 統合 User-ID エージェント用に サーバー監視を設定します。

1. Microsoft サーバー タイプ (**Microsoft Active Directory** または **Microsoft Exchange**) を設定します。
2. HTTP 経由の Windows リモート管理 (WinRM) を使用してサーバー セキュリティ ログとセッション情報を監視するには、**Transport Protocol (転送プロトコル)** として **WinRM-HTTP** を選択します。



3. サーバーの FQDN **Network Address (ネットワークアドレス)** を入力します。

   Kerberos を使用している場合、ネットワークアドレスは完全修飾ドメイン名 (FDQN) でなければなりません。

STEP 5 | 変更を **Commit (コミット)**します。

STEP 6 | 各監視対象サーバーのステータスが Connected (接続済み) であることを確認します (**Device (デバイス)** > **User Identification (ユーザー ID)** > **User Mapping (ユーザー マッピング)**)。

WinRM を HTTPS 経由で Kerberos で構成する

Kerberos を使用して WinRM over HTTPS を構成すると、firewall と監視対象サーバーは HTTPS を使用して通信し、相互認証に Kerberos を使用します。

Kerberos を搭載した *WinRM* は、*aes128-cts-hmac-sha1-96* および *aes256-cts-hmac-sha1-96* 暗号をサポートしています。監視するサーバーが *RC4* を使用している場合は、監視するサーバーのレジストリ設定で、*Kerberos* 用の *Windows* update および disable *RC4* をダウンロードする必要があります。

STEP 1 | 監視するサーバーのリモート管理ユーザーと CIMV2 特権で サービスアカウントを設定します。

STEP 2 | 監視している Windows サーバーで、WinRM で使用する Windows サーバーの証明書から拇印を取得し、WinRM を有効にします。

管理者特権を持つアカウントを使用して、監視するサーバーで *WinRM* を構成していることを確認します。セキュリティのベスト プラクティスとして、このアカウントは手順 *1* のサービス アカウントと同じアカウントにしないでください。

1. 証明書がローカルコンピューターの証明書ストアにインストールされていることを確認します (**Certificates (Local Computer) (**証明書 **(**ローカルコンピューター**))** > **Personal (**パーソナル**)** > **Certificates (**証明書**)**)。

   ローカルコンピューターの証明書ストアが表示されない場合は、Microsoft 管理コンソール (**Start (**スタート**)** > **Run (**実行**)** > **MMC**) を起動し、証明書スナップイン (**File (**ファイル**)** > **Add/Remove Snap-in (**スナップインの追加/削除**)** > **Certificates (**証明書**)** > **Add (**追加**)** > **Computer account (**コンピューターアカウント**)** > **Next (**次へ**)** > **Finish (**完了**)**) を追加します。
2. 証明書を開き、**General** > **Details** > **Show: <All>** を選択します。
3. **Thumbprint**（拇印）を選択し、コピーします。
4. WinRM を使用してファイアウォールが Windows サーバーに接続できるようにするには、コマンド **`winrm quickconfig`**を入力します。
5. **y** を入力して変更を確認して、出力に `WinRM service started` と表示されていることを確認します。

   WinRM が有効になっている場合、出力には、`WinRM service is already running on this machine` と表示されます。追加の必要な構成変更を確認するよう求められます。
6. WinRM が HTTPS を使用して通信していることを確認するために、コマンド ：**`winrm enumerate winrm/config/listener`** を入力します。次に、出力に `Transport = HTTPS` と表示されることを確認します。

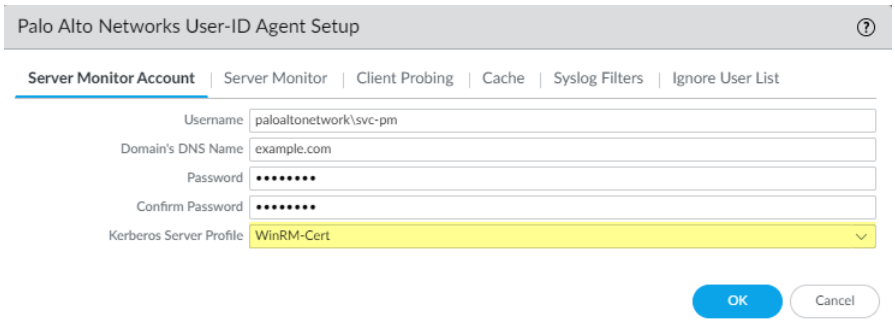
   デフォルトでは、WinRM/HTTPS は 5986 を使用します。
7. Windows サーバーのコマンド プロンプトから、次のコマンドを入力します: **`winrm create winrm/config/Listener?Address=*+ Transport=HTTPS @{ Hostname="<hostname>";CertificateThumbprint="Certificate Thumbprint"}`**。ここで、*hostname* は Windows サーバーのホスト名、*Certificate Thumbprint* は証明書からコピーした値です。

   コマンドプロンプト（*Powershell* ではなく）を使用し、証明書の拇印のスペースを削除して、*WinRM* が証明書を検証できることを確認します。
8. **`winrm get winrm/config/service/Auth`** を入力して、`Basic = false` および `Kerberos= true` となっていることを確認します。

STEP 3 | PAN-OS 統合ユーザー ID エージェントと監視対象サーバーが Kerberos を使用して認証できるようにします。

1. initial configuration（初期設定）中にそうしなかった場合は、Kerberos ネゴシエーションが正常に行われるように日付と時刻 (NTP) を設定します。
2. ファイアウォールで Kerberos サーバープロファイルを設定して、サーバーで認証し、セキュリティログとセッション情報を監視します。
3. **Device (デバイス)** > **User Identification (User-ID)** > **User Mapping (ユーザーマッピング)** > **Palo Alto Networks User-ID Agent Setup (Palo Alto Networks User-ID** エージェントの設定) > **Server Monitor Account (サーバーモニターアカウント)** を選択します。
4. **`Domain\username`** 形式では、User-ID エージェントがサービスの監視に使用するサービスアカウント名に **User Name (ユーザー名)** を入力します。
5. サーバーモニターアカウントの **Domain's DNS Name (ドメインの DNS 名)** を入力します。

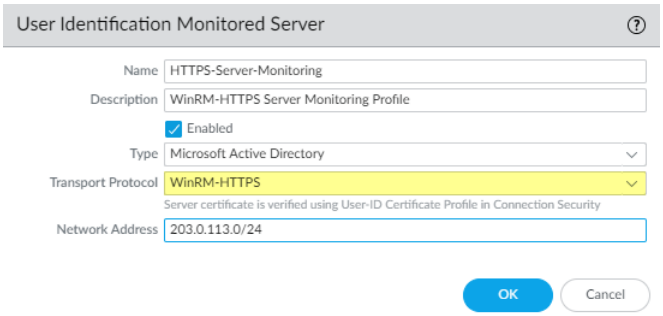
   Kerberos はドメイン名を使用して、サービスアカウントを探します。
6. サービスアカウントの **Password (パスワード)** と **Confirm Password (パスワードの確認)** を入力します。
7. ステップ 3.2 で作成した **Kerberos Server Profile (Kerberos サーバー プロファイル)** を選択します。



8. **OK** をクリックします。

STEP 4 | PAN-OS 統合 User-ID エージェント用にサーバー監視を設定します。

1. Microsoft サーバー タイプ (**Microsoft Active Directory** または **Microsoft Exchange**) を設定します。
2. HTTPS 経由の Windows リモート管理 (WinRM) を使用してサーバー セキュリティ ログとセッション情報を監視するには、**Transport Protocol (転送プロトコル)** として **Win-RM-HTTPS** を選択します。



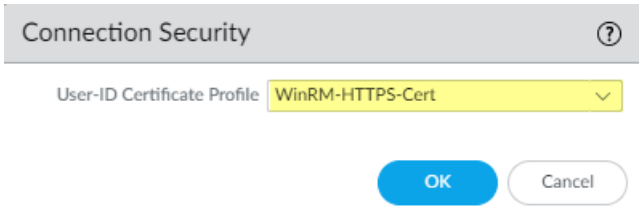
3. サーバーの FQDN **Network Address (ネットワークアドレス)** を入力します。

   Kerberos を使用している場合、ネットワークアドレスは完全修飾ドメイン名 (FDQN) でなければなりません。

STEP 5 | PAN-OS 統合 User-ID エージェントが WinRM-HTTPS を使用して監視対象サーバーと通信できるようにするには、Windows サーバーが WinRM に使用するサービス証明書のルート証明書をファイアウォールに正常にインポートし、その証明書を User-ID 証明書プロファイルに関連付けていることを確認します。

ファイアウォールは同じ証明書を使用して、すべての監視対象サーバーを認証します。

1. **Device (デバイス)** > **User Identification (ユーザー ID)** > **Connection Security (接続セキュリティ)** を選択します。
2. **Edit**（編集）をクリックします。
3. **User-ID Certificate Profile (User-ID** 証明書プロファイル**)** に使用する Windows サーバー証明書を選択します。



4. **OK** をクリックします。
5. 変更を **Commit (コミット)** します。

STEP 6 | 各監視対象サーバーのステータスが Connected (接続済み) であることを確認します (**Device (デバイス)** > **User Identification (ユーザー ID)** > **User Mapping (ユーザー マッピング)**)。

User-ID を設定してユーザーマッピング用に Syslog 送信者を監視

ユーザーを認証する既存のネットワーク・サービスから IP アドレスからユーザー名へのマッピングを取得するには、PAN-OS 統合 User-ID エージェントまたは Windows-based User-ID エージェントを構成して、これらのサービスからのSyslogメッセージを構文解析することができます。ユーザーマッピングを最新の状態に保つために、User-ID エージェントが Syslog メッセージをパースしてログアウト イベントを取得し、古くなったマッピングをファイアウォールに自動的に削除させることもできます。

- PAN-OS 統合 User-ID エージェントを Syslog リスナーとして設定
- Syslog リスナーとしての Windows User-ID エージェントの設定

PAN-OS 統合 User-ID エージェントを Syslog リスナーとして設定

PAN-OS 統合 User-ID エージェントを設定し、新しいユーザーマッピングを作成し、Syslog モニタリングを通じて古くなったマッピングを削除するためには、Syslog 解析プロファイルを定義する作業から開始します。User-ID エージェントはこのプロファイルを使用し、Syslog メッセージ内のログインおよびログアウト イベントを探します。*Syslog* 送信者（ユーザーを認証するネットワーク サービス）が異なる形式で Syslog メッセージを送信する環境の場合、各 Syslog フォーマット毎にプロファイルを設定します。User-ID エージェントが Syslog メッセージを解析するには、Syslog メッセージが特定の条件を満たしている必要があります（Syslogを参照）。この作業では、次のフォーマットの例を示します。

- ログイン イベント–`[Tue Jul 5 13:15:04 2016 CDT] Administratorauthentication success User:johndoe1 Source:192.168.3.212`
- ログアウト イベント–`[Tue Jul 5 13:18:05 2016CDT] User logout successful User:johndoe1 Source:192.168.3.212`

Syslog 解析プロファイルを設定した後、User-ID エージェントが監視する Syslog 送信者を指定します。

STEP 1 | 対象の Syslog 解析プロファイルに対する事前定義された Syslog フィルタがあるかどうかを確認します。

Palo Alto Networks では、いくつかの事前定義済みのプロファイルをアプリケーション コンテンツ更新で提供しています。事前定義済みプロファイルはファイアウォールでグローバルに適用されます。一方、カスタム プロファイルは 1 つの仮想システムのみに適用されます。

特定のコンテンツ リリースに含まれている新しい *Syslog* 解析プロファイルには、対応するリリース ノート内に説明があり、フィルタを定義するために使用する具体的な正規表現も記載されています。

1. 最新のアプリケーション更新あるいはアプリケーションおよび脅威更新をインストールします。
   1. **Device (デバイス)** > **Dynamic Updates (動的更新)** を選択して **Check Now (今すぐチェック)** します。
   2. 新しい更新コンテンツがあれば **Download (ダウンロード)** して **Install (インストール)** します。
2. どの定義済みの Syslog 解析プロファイルを利用できるのか判断します。
   1. **Device (デバイス)** > **User Identification (ユーザー ID)** > **User Mapping (ユーザー マッピング)** を選択し、Server Monitoring (サーバー監視) セクションで **Add (追加)** をクリックします。
   2. **Type (タイプ)** を **Syslog Sender (Syslog 送信者)** に設定し、Filter (フィルタ) セクションで **Add (追加)** をクリックします。必要な Syslog 解析プロファイルを利用できる場合は、カスタム プロファイルを定義するステップをスキップしてください。

STEP 2 | カスタム Syslog 解析プロファイルを定義し、ユーザーマッピングの作成・削除を行います。

各プロファイルは Syslog メッセージをフィルタリングし、ログイン イベント（ユーザーマッピングを作成するため）あるいはログアウト イベント（マッピングを削除するため）のいずれかを識別しますが、単一のプロファイルで両方を行うことはできません。

1. Syslog 送信者が生成した Syslog メッセージを確認し、ログインおよびログアウト イベントの構文を識別します。これにより、Syslog 解析プロファイルを作成する際の一致パターンを定義できるようになります。

   Syslog メッセージを確認する際、メッセージにドメイン名が含まれているかどうかも確認します。そうでなく、ユーザーマッピングがドメイン名を必要とする場合は、*User-ID* エージェントが監視する *Syslog* 送信者を定義する際（この作業の後半）に ***Default Domain Name*** **(**デフォルト ドメイン名**)** を入力します。

2. **Device (**デバイス**)** > **User Identification (**ユーザー **ID)** > **User Mapping (**ユーザー マッピング**)** を選択して Palo Alto Networks User-ID エージェント設定を編集します。
3. **Syslog Filters (Syslog** のフィルタ**)** タブを選択して、Syslog 解析プロファイルを **Add (**追加**)** します。
4. **Syslog Parse Profile (Syslog** 解析プロファイル**)** を識別する名前を入力します。
5. Syslog メッセージに含まれるログインあるいはログアウト イベントを見つける際に行うパースの **Type (**タイプ**)** を選択します。

   - **Regex Identifier (**正規表現識別子**)**–正規表現。
   - **Field Identifier (**フィールド識別子**)**–テキスト文字列。

   次の各ステップは、これらのタイプのパースを設定する方法を示しています。

STEP 3 | （正規表現識別子のパースのみ）正規表現の一致パターンを定義します。

Syslog メッセージで単独のスペースまたはタブが区切り文字として使用されている場合、**\s**(スペース)または**\t** (タブ)を使用します。

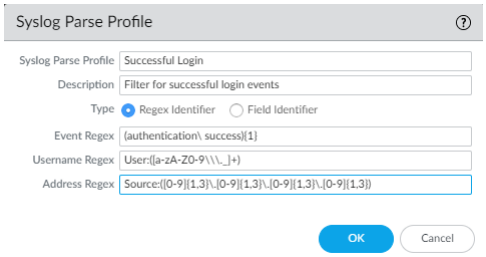
1. 探したいイベントのタイプに使用する **Event Regex** (イベント正規表現) を入力します。
   - ログイン イベント—メッセージ例の場合、正規表現 **(authentication\ success){1}** によって、文字列 `authenticationsuccess` の最初の **{1}** インスタンスが抽出されます。
   - ログアウト イベント—メッセージ例の場合、正規表現 **(logout\ successful){1}** によって、文字列 `logoutsuccessful` の最初の **{1}** インスタンスが抽出されます。

   スペースの前のバックスラッシュ（\）は、スペースを特殊文字として扱わないように正規表現エンジンに指示する標準の正規表現エスケープ文字です。
2. ユーザー名の始まりを識別する **Username Regex** (ユーザー名正規表現) を入力します。

   メッセージのサンプルでは、正規表現 **User:([a-zA-Z0-9\\\._]+)** は例のメッセージの文字列 `User:johndoe1` に一致し `johndoe1` をユーザー名として識別します。
3. Syslog メッセージの IP アドレス部分を識別する **Address Regex** (アドレス正規表現) を入力します。

   メッセージのサンプルでは、正規表現 **Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})** は、IPv4 アドレス `Source:192.168.3.212` に一致します。

   次の例は、正規表現を使用してログイン イベントを識別する Syslog 解析プロファイル全体の例です。



4. **OK** を 2 回クリックしてプロファイルを保存します。

STEP 4 | （フィールド識別子のパースのみ）文字列の一致パターンを定義します。

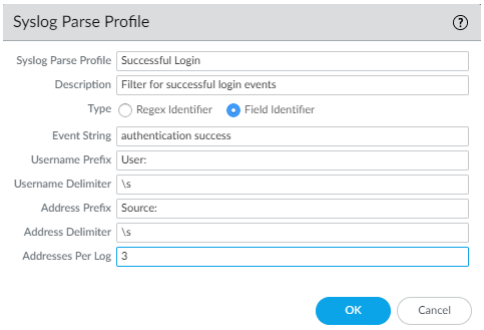
1. 探したいイベントのタイプに使用する **Event String (**イベント文字列**)** を入力します。
   - ログイン イベント–メッセージ例の場合、文字列 `authentication success` がログイン イベントを識別します。
   - ログアウト イベント–メッセージ例の場合、文字列 `logoutsuccessful` がログアウト イベントを識別します。
2. Syslog メッセージのユーザー名フィールドの先頭を識別する **Username Prefix (**ユーザー名プレフィックス**)** を入力します。このフィールドでは、\s（スペース）や \t（タブ）などの正規表現がサポートされません。

   このメッセージのサンプルでは、`User:` によってユーザー名フィールドの先頭を識別しています。
3. Syslog メッセージ内のユーザー名フィールドの終了を識別する **Username Delimiter (**ユーザー名の区切り文字**)** を入力します。1 つのスペースを示すには **\s**（メッセージ例を参照）、タブを示すには **\t** を使用します。
4. Syslog メッセージで IP アドレス フィールドの先頭を識別する **Address Prefix (**アドレスのプレフィックス**)** を入力します。このフィールドでは、\s（スペース）や \t（タブ）などの正規表現がサポートされません。

   このメッセージのサンプルでは、`Source:` によってアドレス フィールドの先頭を識別しています。
5. Syslog メッセージ内の IP アドレス フィールドの終了を識別する **AddressDelimiter (**アドレス区切り文字**)** を入力します。

   たとえば、区切り文字が行区切りであることを示すには、**\n** を入力します。

   次の例は、ログイン イベントを識別する一致文字列を使用する Syslog 解析プロファイル全体の例です。



6. **OK** を 2 回クリックしてプロファイルを保存します。

STEP 5 | ファイアウォールが監視する Syslog 送信者を指定します。

ファイアウォールあたり監視対象サーバー最大100 個の範囲で、バーチャルシステム1個につき、50個を超える syslog sender は定義できません。

ファイアウォールは、このリストにない送信者から受信した Syslog メッセージは破棄します。

1. **Device (デバイス)** > **User Identification (ユーザー ID)** > **User Mapping (ユーザー マッピング)** を選択し、Server Monitoring (サーバー監視) リストに項目を **Add (追加)** します。
2. 送信者を識別する **Name (名前)** を入力します。
3. 送信者プロファイルが **Enabled (有効)** になっていることを確認します（デフォルトは有効）。
4. **Type (タイプ)** を **Syslog Sender (Syslog 送信者)** に設定します。
5. Syslog 送信者の **Network Address**（ネットワークアドレス）（IP アドレス）を入力します。
6. **Connection Type (接続タイプ)** として **SSL**（デフォルト）あるいは **UDP** を選択します。

   ファイアウォールが *syslog* メッセージを受信するために使用する *TLS* 証明書を選択するには、***Device (デバイス) > User Identification (ユーザー ID) > User Mapping (ユーザー マッピング) > Palo Alto Networks User-ID Agent Setup (Palo Alto Networks ユーザー ID エージェントの設置アップ)*** を選択します。設定を ***Edit (編集)*** し、***Server Monitor (サーバー監視)*** を選択してから、ファイアウォールで *syslog* メッセージを受信するために使用する、*TLS* 証明書を含む ***Syslog Service Profile (Syslog サービス プロファイル)*** を選択します。

   PAN-OS 統合ユーザー ID エージェントは、SSL および UDP 上でのみ Syslog を受け入れます。ただし、UDP は信頼性の低いプロトコルであり、メッセージが信頼された Syslog 送信者から送信されたことを確認する方法がないため、UDP を使用して Syslog メッセージを受信する場合は注意が必要です。Syslog メッセージを特定の送信元 IP アドレスに制限することはできますが、それでも攻撃者によって IP アドレスがスプーフされ、不正な Syslog メッセージがファイアウォールに送信される可能性があります。

   トラフィックは暗号化されているため (*UDP はトラフィックを平文で送信するため*)、必ず *SSL* を使用して *syslog* メッセージを確認してください。*UDP* を使用する必要がある場合は、*Syslog* 送信者とクライアントの両方が専用の安全なネットワークにあることを確認し、信頼されていないホストからファイアウォールに *UDP* トラフィックが送信されないようにします。

SSL を使用して接続している Syslog 送信元は、アクティブな SSL 接続があるときだけ Status (状態) を Connected (接続済み) と表示します。UDP を使用している Syslog 送信元は、Status[状態] の値が表示されません。

7. 送信者がサポートする Syslog フォーマット毎に、Syslog パース プロファイルをフィルタ リストに **Add (追加)** します。識別を行うために設定する各プロファイルの **Event Type (イベント タイプ)** を選択します。（**login**（デフォルト）あるいは **logout**）を選択します。
8. （任意）Syslog メッセージにドメイン情報を含めず、ユーザーマッピングがドメイン名を必要とする場合は、**Default Domain Name (デフォルト ドメイン名)** を入力してマッピングを付加します。
9. **OK** をクリックして設定を保存します。

STEP 6 | ファイアウォールがユーザーマッピングを収集するために使用するインターフェイス上でSyslog リスナーサービスを有効化します。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **Interface Mgmt (インターフェイス管理)** の順に選択します。次に、インターフェイス管理プロファイルを編集するか、新しいプロファイルを **Add (追加)** します。
2. サーバー モニター リスト内の Syslog 送信元に定義したプロトコルに応じて **User-ID Syslog Listener-SSL (ユーザー ID Syslog リスナー SSL)** または **User-ID Syslog Listener-UDP (ユーザー ID Syslog リスナー UDP)**、あるいは両方を選択します。

   リスニング ポート（*UDP* は *514*、*SSL* は *6514*）は設定可能ではありません。リスニング ポートは管理サービスを通じてのみ有効にできます。
3. **OK** をクリックして、インターフェイス管理プロファイルを保存します。

   インターフェイス上でユーザー *ID Syslog* リスナー サービスを有効にした後でも、インターフェイスが *Syslog* 接続を受けつけるのは、ユーザー *ID* のモニター対象サーバー設定内に対応するエントリがある送信者からのみです。ファイアウォールは、このリストにない送信者から受信した接続やメッセージは破棄します。
4. ファイアウォールがユーザーマッピングを収集するために使用するインターフェイスにインターフェイス管理プロファイルを割り当てます。
   1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** を選択してインターフェイスを編集します。
   2. **Advanced (詳細)** > **Other info (その他の情報)** の順に選択し、追加したインターフェイス **Management Profile (管理プロファイル)** を選択し、**OK** をクリックします。
5. 変更を **Commit (コミット)**します。

STEP 7 | ユーザーがログインおよびログアウトを行う際にファイアウォールがユーザーマッピングを追加・削除することを確認します。

CLI コマンドを使用し、*Syslog* 送信者、*Syslog* メッセージ、ユーザーマッピングの詳細情報を表示できます。

1. 監視対象の Syslog 送信者がログインおよびログアウト イベント メッセージを生成する対象になるクライアントシステムにログインします。
2. ファイアウォール CLI へログインします。
3. ファイアウォールがログイン ユーザー名をクライアント IP アドレスにマッピングしたことを確認します。

```
> show user ip-user-mapping ip <ip-address>     IP address:
 192.0.2.1 (vsys1)
User:          localdomain\username
From:                  SYSLOG
```

4. クライアントシステムからログアウトします。
5. ファイアウォールがユーザーマッピングを削除したことを確認します。

```
> show user ip-user-mapping ip <ip-address> No matched record
```

Syslog リスナーとしての Windows User-ID エージェントの設定

Windows ベースの User-ID エージェントを設定し、新しいユーザーマッピングを作成し、Syslog モニタリングを通じて古くなったマッピングを削除するためには、Syslog 解析プロファイルを定義する作業から開始します。User-ID エージェントはこのプロファイルを使用し、Syslog メッセージ内のログインおよびログアウト イベントを探します。*Syslog* 送信者（ユーザーを認証するネットワーク サービス）が異なる形式で Syslog メッセージを送信する環境の場合、各 Syslog フォーマット毎にプロファイルを設定します。User-ID エージェントが Syslog メッセージを解析するには、Syslog メッセージが特定の条件を満たしている必要があります（Syslogを参照）。この作業では、次のフォーマットの例を示します。

- ログイン イベント–`[Tue Jul 5 13:15:04 2016 CDT] Administrator authentication success User:johndoe1 Source:192.168.3.212`
- ログアウト イベント–`[Tue Jul 5 13:18:05 2016 CDT] User logout successful User:johndoe1 Source:192.168.3.212`

Syslog 解析プロファイルを設定した後、User-ID エージェントが監視する Syslog 送信者を指定します。

Windows ユーザー *ID* エージェントは、*TCP* および *UDP* 上でのみ *Syslog* を受け入れます。ただし、*UDP* は信頼性の低いプロトコルであり、メッセージが信頼された *Syslog* 送信者から送信されたことを確認する方法がないため、*UDP* を使用して *Syslog* メッセージを受信する場合は注意が必要です。*Syslog* メッセージを特定の送信元 *IP* アドレスに制限することはできますが、それでも攻撃者によって *IP* アドレスがスプーフされ、不正な *Syslog* メッセージがファイアウォールに送信される可能性があります。*UDP* の代わりに *TCP* を使用することをお勧めします。どちらの場合も、*Syslog* 送信者とクライアントの両方が専用の安全な *VLAN* にあることを確認し、信頼されていないホストからユーザー *ID* エージェントに *Syslog* が送信されないようにします。

STEP 1 | まだ行っていない場合は Windows ベースの User-ID エージェントをデプロイします。

1. Windows ベースのユーザー ID エージェントをインストールします。
2. ファイアウォールが User-ID エージェントと接続するように設定します。

STEP 2 | カスタム Syslog 解析プロファイルを定義し、ユーザーマッピングの作成・削除を行います。

各プロファイルは Syslog メッセージをフィルタリングし、ログイン イベント（ユーザーマッピングを作成するため）あるいはログアウト イベント（マッピングを削除するため）のいずれかを識別しますが、単一のプロファイルで両方を行うことはできません。

1. Syslog 送信者が生成した Syslog メッセージを確認し、ログインおよびログアウト イベントの構文を識別します。これにより、Syslog 解析プロファイルを作成する際の一致パターンを定義できるようになります。

   Syslog メッセージを確認する際、メッセージにドメイン名が含まれているかどうかも確認します。そうでなく、ユーザーマッピングがドメイン名を必要とする場合は、*User-ID* エージェントが監視する *Syslog* 送信者を定義する際（この作業の後半）に ***Default Domain Name*** **(**デフォルト ドメイン名**)** を入力します。

2. Windows **Start**[スタート]メニューを開いて、 **User-ID Agent**[ユーザーIDエージェント]を選択します。
3. **User Identification (**ユーザー **ID)** > **Setup (**セットアップ**)** を選択してセットアップを **Edit (**編集**)** します。
4. **Syslog** を選択し、**Enable Syslog Service (Syslog** サービスの有効化**)** を行い、Syslog Parse (Syslog パース) プロファイルを **Add (**追加**)** します。
5. **Profile Name**[プロファイル名] と **Description**[内容] を入力します。
6. Syslog メッセージに含まれるログインおよびログアウト イベントを見つける際に行うパースの **Type (**タイプ**)** を選択します。
   - **Regex (**正規表現**)**—正規表現。
   - **Field (**フィールド**)**—テキスト文字列。

   次の各ステップは、これらのタイプのパースを設定する方法を示しています。

STEP 3 | （正規表現のパースのみ）正規表現の一致パターンを定義します。

Syslog メッセージで単独のスペースまたはタブが区切り文字として使用されている場合、**\s**(スペース)または**\t** (タブ)を使用します。

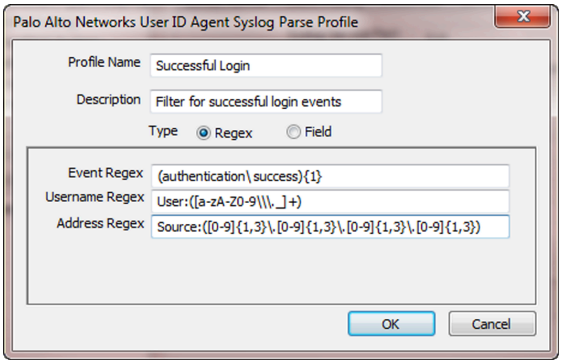
1. 探したいイベントのタイプに使用する **Event Regex (**イベント正規表現**)** を入力します。
   - ログイン イベント–メッセージ例の場合、正規表現 **(authentication\ success)** によって、文字列 `authentication success` の最初の **{1}** インスタンスが抽出されます。
   - ログイン イベント–メッセージ例の場合、正規表現 **(logout\ successful)** によって、文字列 **{1}** の最初の `logout successful` インスタンスが抽出されます。

   スペースの前の円記号は、スペースを特殊文字として扱わないように正規表現エンジンに指示する標準の正規表現エスケープ文字です。
2. ユーザー名の始まりを識別する **Username Regex (**ユーザー名正規表現**)** を入力します。

   メッセージのサンプルでは、正規表現 **User:([a-zA-Z0-9\\\._]+)** は例のメッセージの文字列 `User:johndoe1` に一致し `johndoe1` をユーザー名として識別します。
3. Syslog メッセージの IP アドレス部分を識別する **Address Regex (**アドレス正規表現**)** を入力します。

   メッセージのサンプルでは、正規表現 **Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})** は、IPv4 アドレス `Source:192.168.3.212` に一致します。

   次の例は、正規表現を使用してログイン イベントを識別する Syslog 解析プロファイル全体の例です。



4. **OK** を 2 回クリックしてプロファイルを保存します。

STEP 4 | （フィールド識別子のパースのみ）文字列の一致パターンを定義します。

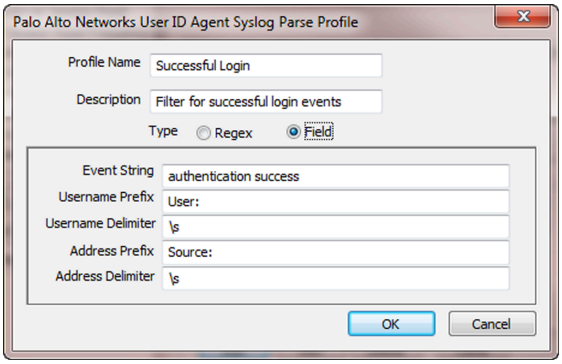
1. 探したいイベントのタイプに使用する **Event String (**イベント文字列**)** を入力します。
   - ログイン イベント–メッセージ例の場合、文字列 `authentication success` がログイン イベントを識別します。
   - ログイン イベント–メッセージ例の場合、文字列 `logout successful` がログアウト イベントを識別します。
2. Syslog メッセージのユーザー名フィールドの先頭を識別する **Username Prefix (**ユーザー名プレフィックス**)** を入力します。このフィールドでは、\s（スペース）や \t（タブ）などの正規表現がサポートされません。

   このメッセージのサンプルでは、`User:` によってユーザー名フィールドの先頭を識別しています。
3. Syslog メッセージ内のユーザー名フィールドの終了を識別する **Username Delimiter (**ユーザー名の区切り文字**)** を入力します。1 つのスペースを示すには **\s**（メッセージ例を参照）、タブを示すには **\t** を使用します。
4. Syslog メッセージで IP アドレス フィールドの先頭を識別する **Address Prefix (**アドレスのプレフィックス**)** を入力します。このフィールドでは、\s（スペース）や \t（タブ）などの正規表現がサポートされません。

   このメッセージのサンプルでは、`Source:` によってアドレス フィールドの先頭を識別しています。
5. Syslog メッセージ内の IP アドレス フィールドの終了を識別する **AddressDelimiter (**アドレス区切り文字**)** を入力します。

   たとえば、区切り文字が行区切りであることを示すには、**\n** を入力します。

   次の例は、ログイン イベントを識別する一致文字列を使用する Syslog 解析プロファイル全体の例です。



6. **OK** を 2 回クリックしてプロファイルを保存します。

STEP 5 | User-ID エージェントが監視する Syslog 送信者を指定します。

User-ID エージェントがモニターできるすべてのタイプのサーバー最大100個のうち、Syslog sender になりうるのは最大50個です。

ユーザー ID エージェントは、このリストにない送信者から受信した Syslog メッセージは破棄します。

1. **User Identification (ユーザー ID)** > **Discovery (検出)** を選択し、Servers (サーバー) リストに項目を **Add (追加)** します。
2. 送信者を識別する **Name (名前)** を入力します。
3. Syslog 送信者の**Server Address (サーバーアドレス)** を入力します（IP アドレスまたは FQDN）。
4. **Server Type (サーバータイプ)** を **Syslog Sender (Syslog 送信者)** に設定します。
5. （任意） **Default Domain Name**（サーバーのデフォルトのドメイン名を入力）して、現在のドメイン名を Syslog メッセージのユーザー名に上書きするか、Syslog メッセージにドメインが含まれていない場合はユーザー名に追加します。
6. 送信者がサポートする Syslog フォーマット毎に、Syslog パース プロファイルをフィルタ リストに **Add (追加)** します。各プロファイルを識別するために設定した **Event Type (イベント タイプ)**（**login**（デフォルト）あるいは **logout**）を選択し、**OK** をクリックします。
7. **OK** をクリックして設定を保存します。
8. User-ID エージェント設定に加えた変更を **Commit (コミット)** します。

STEP 6 | ユーザーがログインおよびログアウトを行う際に User-ID エージェントがユーザーマッピングを追加・削除することを確認します。

CLI コマンドを使用し、*Syslog* 送信者、*Syslog* メッセージ、ユーザーマッピングの詳細情報を表示できます。

1. 監視対象の Syslog 送信者がログインおよびログアウト イベント メッセージを生成する対象になるクライアントシステムにログインします。
2. User-ID エージェントがログイン ユーザー名をクライアント IP アドレスにマッピングしたことを確認します。
   1. User-ID agent (User-ID エージェント) で **Monitoring (モニタリング)** を選択します。
   2. フィルタ フィールドにユーザー名あるいは IP アドレスを入力し、**Search (検索)** し、リストがマッピングを表示することを確認します。
3. ファイアウォールが User-ID エージェントからユーザーマッピングを受信することを確認します。
   1. ファイアウォール CLI へログインします。
   2. 以下のコマンドを実行します：

      ```
      > show user ip-user-mapping ip <ip-address>
      ```

      ファイアウォールがユーザーマッピングを受信した場合、出力はおおよそ次のようになります。

      ```
      IPアドレス：     192.0.2.1 (vsys1) ユーザ: ローカルドメインユーザ
      名 差出人:           SYSLOG
      ```
4. クライアントシステムからログアウトします。
5. User-ID エージェントがユーザーマッピングを削除したことを確認します。
   1. User-ID agent (User-ID エージェント) で **Monitoring (モニタリング)** を選択します。
   2. フィルタ フィールドにユーザー名あるいは IP アドレスを入力し、**Search (検索)** し、リストがマッピングを表示しないことを確認します。
6. ファイアウォールがユーザーマッピングを削除したことを確認します。
   1. ファイアウォール CLI にアクセスします。
   2. 以下のコマンドを実行します：

      ```
      > show user ip-user-mapping ip <ip-address>
      ```

      ファイアウォールがユーザーマッピングを削除した場合、出力は次のようになります。

      ```
      一致するレコードがありません
      ```

認証 ポータルを使用したたIPアドレスとユーザー名のマッピング

ユーザーが認証ポリシールールに一致するWeb通信(HTTPまたはHTTPS)を開始すると、ファイアウォールは認証ポータルを通じて認証するようユーザーに要求します。これにより、極めて重要なアプリケーションやデータに誰がアクセスしているのか、正確に分かるようになります。認証時に収集されたユーザー情報に基づき、ファイアウォールがIPアドレスからユーザー名へのマッピングを新規に作成するか、そのユーザーの既存のマッピングを更新します。このユーザーマッピングの方式は、監視サービスなどの他の方法を通じてファイアウォールがマッピングを学習できない環境で役立ちます。例えば、Linuxクライアント上のユーザーなど、監視対象のドメインサーバーにログインしていないユーザーがいるかもしれません。

- 認証ポータルの認証方法
- 認証ポータル モード
- 認証ポータルの設定

認証ポータルの認証方法

認証ポータルは以下の方式を使用し、Web要求が認証ポリシールールに一致するユーザーを認証します:

認証方式	説明
Kerberos SSO	ファイアウォールは、Kerberosシングルサインオン（SSO）を使用して、透過的にユーザー認証情報を取得します。この方法を使用するには、ネットワークにKerberosインフラストラクチャ(Key Distribution Center (KDC)、認証サーバー、チケット発行サービスを含む)が必要です。ファイアウォールにKerberosアカウントが必要です。 Kerberos SSO認証に失敗した場合、認証ポリシーおよび認証ポータル設定に応じてファイアウォールはWebフォームまたはクライアント証明書の認証にフォールバックします。
Webフォーム	ファイアウォールは、認証を行うためにWeb要求をWebフォームにリダイレクトします。この方式の場合、マルチファクター認証（MFA）、SAML、Kerberos、TACACS+、RADIUS、あるいはLDAP認証を使用するように認証ポリシーを設定できます。ユーザーは自分のログイン認証情報を手動で入力する必要がありますが、この認証方法は、すべてのブラウザおよびオペレーティングシステムと連動します。
クライアント証明書認証	ファイアウォールは、有効なクライアント証明書をブラウザに要求してユーザーを認証します。この方法を使用する場合は、各ユーザーシステムのクライアント証明書をプロビジョニングし、ファイアウォールでそれらの証明書を発行するために使用

認証方式	説明
	する信頼された証明局(CA)証明書をインストールする必要があります。

認証ポータル モード

認証ポータル モードにより、ファイアウォールが Web 要求をキャプチャして認証を行う方法が定義されます:

モード	説明
透過	認証ポリシールールに従い、ファイアウォールがブラウザのトラフィックを遮断して元の宛先 URL になりすまし、HTTP 401 を発行して認証を呼び出します。ただし、ファイアウォールには宛先 URL の実際の証明書がないため、保護されたサイトへのアクセスを試みるユーザーのブラウザには証明書エラーが表示されます。したがって、このモードはレイヤー 2 やバーチャル ワイヤーのデプロイメントなど、絶対に必要な場合にのみ使用してください。
リダイレクト	ファイアウォールは不明な HTTP または HTTPS セッションをインターセプトし、認証を実行するために HTTP 302 リダイレクトを使用してファイアウォールのレイヤー 3 インターフェイスにリダイレクトします。より優れたエンドユーザー体験(証明書エラーなし)が提供されるため、このモードの使用をお勧めします。ただし、追加のレイヤー 3 設定が必要です。[リダイレクト] モードのもう 1 つの利点はセッション Cookie を使用できることで、タイムアウトが発生するたびに再度マッピングする必要なしに、ユーザーが継続して認証済みサイトを閲覧できます。ある IP アドレスから別の IP アドレス(企業 LAN から無線ネットワークなど)にローミングするユーザーは、セッションが開かれている限り IP アドレスが変化しても再認証する必要がないため、このモードが特に役立ちます。 Kerberos SSO 認証を使用する場合、ブラウザは信頼されたサイトにのみ認証情報を提供するため、リダイレクト モードを使用する必要があります。リダイレクトモードは、多要素認証を使用して Authentication Portal ユーザーを認証する場合にも必要です。

認証ポータルの設定

以下の手順では、PAN-OS統合User-IDエージェントを設定して、Authentication Policy (認証ポリシー)ルールに一致する Web 要求を、ファイアウォールのインターフェース（リダイレクト ホ

スト）にリダイレクトすることにより、Authentication Portal (認証ポータル) 認証をセットアップする方法を示します。

SSL Inbound Inspection（SSLインバウンド インスペクション）は、認証ポータルのリダイレクトをサポートしません。認証ポータルのリダイレクトと復号化を使用するには、SSL Forward Proxy（SSLフォワード プロキシ）を使用する必要があります。

認証ポータルを通じてユーザーがアクセスするアプリケーションには、その感度に基づいて、異なる認証方式と設定が必要になります。デフォルトおよびカスタム認証適用オブジェクトを使用し、すべての認証要件を満たすことができます。各オブジェクトは認証ルールを、認証プロファイルおよび認証ポータルの認証方法に関連付けます。

- デフォルトの認証適用オブジェクト—同じグローバル認証プロファイルを持つ複数の認証ルールを関連付け対場合は、デフォルトのオブジェクトを使用します。認証ポータルを設定する前にこの認証プロファイルを設定してから、それを認証ポータル設定に割り当てる必要があります。マルチ ファクター認証（MFA）が必要な認証ルールの場合は、デフォルトの認証適用オブジェクトを使用することができません。
- カスタム認証適用オブジェクト—グローバル プロファイルとは異なる認証プロファイルが必要な各認証ルールについては、カスタム オブジェクトを使用します。MFA を必要とする認証ルールの場合、カスタム オブジェクトが必須になります。カスタム オブジェクトを使用するには、認証ポータルの設定後（Configure Authentication Policy (認証ポリシーの設定) を行う際）に認証プロファイルを作成し、それをオブジェクトに割り当てます。

ユーザーが認証ポータルの Web Form (Web フォーム)、Kerberos SSOを通じて認証を行う場合のみ、認証プロファイルが必要になりますので、ご注意ください。代わりに、あるいはこれらの方法に加えて、次の作業の流れもクライアント証明書認証を実装する方法を示しています。

他のユーザー *ID* 機能 (ユーザー マッピングおよびグループ マッピング) を使用せずに認証ポータルを使用する場合は、*User-ID*エージェントを設定する必要はありません。

STEP 1 | ファイアウォールが Web 要求を受け入れたり、ユーザーを認証したり、ディレクトリ サーバーと通信してユーザー名を IP アドレスにマッピングしたりするために使用するインターフェースを設定します。

ファイアウォールが認証サーバーまたは User-ID エージェントに接続すると、デフォルトで管理インターフェイスが使用されます。ベストプラクティスとして、認証ルートサーバーまたは User-ID エージェントに接続するようにサービス ルートを設定することによって、管理ネットワークを分離します。

1. （MGT インターフェイスのみ）**Device (デバイス)** > **Setup (セットアップ)** > **Interfaces (インターフェイス)** の順に選択し、**Management (管理)** インターフェイスを編集し、**User-ID** を選択して **OK** をクリックします。
2. （MGT 以外のインターフェイスのみ）ファイアウォールがインバウンドの Web 要求やディレクトリ サーバーとの通信に使用するレイヤー 3 インターフェイスにインターフェイス管理プロファイルを割り当てます。インターフェイス管理プロファイルで、**Response Pages (応答ページ)** と **User ID (ユーザー ID)** を有効にする必要があります。

3. (MGT 以外のインターフェイスのみ)ファイアウォールがユーザーの認証に使用するインターフェイスのサービス ルートを設定します。ファイアウォールに複数の仮想システム(vsys)がある場合、サービス ルートはグローバルまたは vsys 固有になります。サービスには、**LDAP** および場合によっては以下が含まれている必要があります。
   - **Kerberos**、**RADIUS**、**TACACS+**、あるいは **Multi-Factor Authentication (**認証**)**—使用するすべての認証サービスについて、サービスルートを設定します。
   - **UID Agent (UID** エージェント**)**—ユーザーベースおよびグループベースのポリシーを有効にする場合にのみ、このサービスを設定します。
4. (リダイレクト モードのみ)レイヤー 3 インターフェイスの IP アドレスをリダイレクト ホストにマッピングする DNS アドレス(A)レコードを作成します。Kerberos SSO を使用する場合、同じマッピングを実行する DNS ポインタ(PTR)レコードを追加する必要もあります。

ファイアウォール インターフェイスからディレクトリ サーバーにアクセスできないネットワークの場合、Windows User-ID エージェントを使用したユーザー マッピングの設定を行う必要があります。

STEP 2 | ドメイン コントローラのアドレスを解決するように Domain Name System (DNS)が設定されていることを確認します。

正しく名前が解決されていることを確認するには、サーバーの FQDN を ping します。以下に例を示します。

```
admin@PA-220> ping host dc1.acme.com
```

STEP 3 | 認証ポータル証明書を信頼するようにクライアントを設定します。

リダイレクト モードで証明書エラーを表示せずにユーザーを透過的にリダイレクトする場合は必須。自己署名証明書を生成するか、または外部認証局(CA)によって署名された証明書をインポートできます。

自己署名証明書を使用するには、ルート CA 証明書を作成し、それを使用して認証ポータルに使用する証明書に署名します。

1. **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択します。
2. 自己署名ルート CA 証明書の作成を行う、あるいは CA 証明書をインポートします（証明書および秘密鍵のインポートを参照）。
3. 認証ポータルで使用するGenerate a Certificate (証明書の生成)を行います。以下のフィールドを設定します。
   - **Common Name** [共通名] – レイヤー 3 インターフェイスのイントラネット ホストの DNS 名を入力します。
   - **Signed By** [署名者] – 作成またはインポートした CA 証明書を選択します。
   - Certificate Attributes [証明書の属性] – **Add** [追加]をクリックして **Type** (タイプ)に **IP** を選択し、**Value** [値]に、ファイアウォールが要求をリダイレクトするレイヤー 3 インターフェイスの IP アドレスを入力します。
4. SSL/TLS サービス プロファイルを設定します。作成した認証ポータル証明書をプロファイルに割り当てます。

   SSL/TLS サービス プロファイルを割り当てない場合、ファイアウォールはデフォルトで *TLS 1.2* を使用します。別の *TLS* バージョンを使用するには、使用する *TLS* バージョンの *SSL/TLS* サービス プロファイルを設定します。
5. 証明書を信頼するようにクライアントを設定します。
   1. 作成またはインポートした CA 証明書をエクスポートします。
   2. 証明書を信頼されたルート CA としてすべてのクライアント ブラウザにインポートします。インポートはブラウザで手動で設定するか、または証明書を Active Directory (AD)のグループ ポリシー オブジェクト(GPO)の信頼されたルートに追加します。

STEP 4 | （任意）クライアント証明書認証を設定します。

クライアント証明書認証に認証プロファイルまたは認証シーケンスは必要ありません。認証プロファイル/シーケンスと証明書認証の両方を設定した場合、ユーザーは両方を使用して認証を受ける必要があります。

1. ルート CA 証明書を使用して、認証ポータルを通して認証を受ける各ユーザーのクライアント証明書を生成します。通常、この場合の CA は、ファイアウォールではなく、エンタープライズ CA になります。
2. ファイアウォールがアクセスできるシステムに、PEM 形式の CA 証明書をエクスポートします。
3. CA 証明書をファイアウォールにインポートします（証明書および秘密鍵のインポートを参照してください）。インポート後、インポートされた証明書をクリックし、**Trusted Root CA** [信頼されたルート CA]を選択して **OK**[OK] をクリックします。
4. 証明書プロファイルの設定を行います。
   - **Username Field** [ユーザー名フィールド]ドロップダウンから、ユーザー ID の情報を含む証明書フィールドを選択します。
   - **CA Certificates** [CA 証明書]リストで **Add** [追加]をクリックし、インポートした CA 証明書を選択します。

STEP 5 | （任意）Apple Captive Network Assistant 用の認証ポータルを設定します。

Apple Captive Network Assistant（CNA）を用いた認証ポータルを使用している場合のみ、このステップが必要になります。CNA を用いた認証ポータルを使用するには、以下の手順を実行します。

1. リダイレクト ホスト用の FQDN（IP アドレスだけでなく）を指定したことを確認します。
2. 指定された FQDN に対して公開署名証明書を使用するSSL/TLS サービス プロファイルを選択します。
3. 以下のコマンドを入力して、認証ポータル でサポートするリクエスト数を調整します: **set deviceconfig set ctd cap-portal-ask-requests *<threshold-value>***

   デフォルト設定では、ファイアウォールに認証ポータル用のしきい値が設けられており、要求の数が 2 秒毎 1 要求に制限されます。CNA が複数のリクエストを送ってこの上限を超過すると、TCP のリセットおよび CNA のエラーにつながるおそれがあります。推奨されるしきい値は 5 です（デフォルトは 1）。この値は、2 秒間に最大 5 件のリクエストを許可します。環境によっては別の値を設定する必要があるかもしれません。現在の値でリクエストの数に十分対応できない場合、値を増やしてください。

STEP 6 | 認証ポータル設定を設定します。

1. **Device (デバイス)** > **User Identification (ユーザー ID)** > **Authentivation Portal Settings (認証ポータルの設定)** を選択して設定を編集します。
2. **Enable Authentication Portal (認証ポータルを有効にする)** (デフォルトで有効)。
3. ユーザーが認証ポータルを通じて認証を行った後、そのユーザー用に IPアドレス - ユーザー名間マッピングを、ファイアウォールが保持する最大時間（分単位）に、**Timer (タイマー)** を指定します（デフォルトは 60、範囲は 1～1,440）。**Timer (タイマー)** の期限が切れた後、ファイアウォールは認証ポリシールールにある **Timeout (タイムアウト)** の評価に使用される、関連するすべての 認証タイムスタンプおよびマッピングを削除します。

   各認証ポリシー ルールにある認証ポータルの ***Timer (タイマー)*** および ***Timeout (タイムアウト)*** の値を評価する際、ファイアウォールは、先に期限が切れるいずれかの設定に対して再認証を行うよう、ユーザーに促します。再認証の際、ファイアウォールは認証ポータルの ***Timer (タイマー)*** の時間カウントをリセットし、そのユーザー用に新しい認証タイムスタンプを記録します。そのため、異なる認証ルールに対して異なる ***Timeout (タイムアウト)*** 期間を有効にするには、認証ポータルの ***Timer (タイマー)*** の値に、あらゆるルールの ***Timeout (タイムアウト)*** の値以上の値を設定します。

4. TLS 経由のリダイレクト要求用に作成した **SSL/TLS Service Profile** [SSL/TLS サービス プロファイル]を選択します。SSL/TLS サービス プロファイルの設定を参照してください。
5. **Mode** [モード](この例では **Redirect** [リダイレクト])を選択します。
6. （リダイレクト モードのみ）Web リクエストのリダイレクト先となるファイアウォール上のレイヤー 3 インターフェイスの IP アドレスに解決されるイントラネット ホスト名（名前にピリオドのないホスト名）として、**Redirect Host (リダイレクト ホスト)** を指定します。

   ユーザーが Kerberos シングル サインオン（SSO）で認証を行う場合、**Redirect Host**（ホストのリダイレクト）は、Kerberos キータブで指定したホスト名と同じにする必要があります。
7. 使用するフォールバック認証方法を選択します。
   - クライアント証明書認証を使用するには、作成した **Certificate Profile** [証明書プロファイル]を選択します。
   - インタラクティブあるいは SSO 認証でグローバル設定を使用するためには、設定した **Authentication Profile (認証プロファイル)** を選択します。
   - インタラクティブあるいは SSO 認証で認証ポリシールール固有の設定を使用するためには、認証ポリシーの設定を行う際に、認証プロファイルを認証適用オブジェクトに割り当てます。
8. **OK** をクリックして、認証ポータルの設定を **Commit (コミット)** します。

STEP 7 | 次のステップ...

ユーザーがサービスまたはアプリケーションをリクエストする際に、認証を開始するConfigure Authentication Policy (認証ポリシー ルールの設定) を行うまで、ファイアウォールがユーザーに対して認証ポータルの Web フォームを表示することはありません。

ターミナル サーバー ユーザー向けのユーザー マッピング設定

個々のターミナル サーバー ユーザーは同じ IP アドレスを持っているように見えるため、IP アドレスからユーザー名へのマッピングは、特定のユーザーを識別するのに十分ではありません。Windows ベースのターミナル サーバー上の特定のユーザーを識別するため、Palo Alto Networks ターミナル サーバー エージェント(TS エージェント)は各ユーザーにポート範囲を割り当てます。その後、TS エージェントは接続されているすべてのファイアウォールに、割り当てたポート範囲について通知します。これにより、ファイアウォールは IP アドレス対ポート対ユーザーのマッピング テーブルを作成し、ユーザーベースおよびグループベースのセキュリティポリシーを実施できるようになります。Windows 以外のターミナル サーバーに対しては、PAN-OS XML API を設定してユーザー マッピング情報を抽出します。次の値が両方の方法に適用されます。

- デフォルト ポート範囲：1025 から 65534 の間
- ユーザーあたりのブロック サイズ:200
- マルチユーザー システムの最大数:2,500

TS エージェントでサポートされるターミナルサーバーと、各ファイアウォールモデルでサポートされる TS エージェントの数についての情報は、 Palo Alto Networks Compatibility Matrix (Palo Alto Networks 互換性マトリックス) およびProduct Comparison Tool (製品比較ツール) を参照してください。

以下のセクションでは、ターミナル サーバー ユーザーのユーザー マッピング設定方法について説明します。

- Palo Alto Networks ターミナル サーバー（TS）エージェントのユーザー マッピング設定
- ユーザー ID XML API を使用したターミナル サーバーからのユーザー マッピングの取得

Palo Alto Networks ターミナル サーバー（TS）エージェントのユーザー マッピング設定

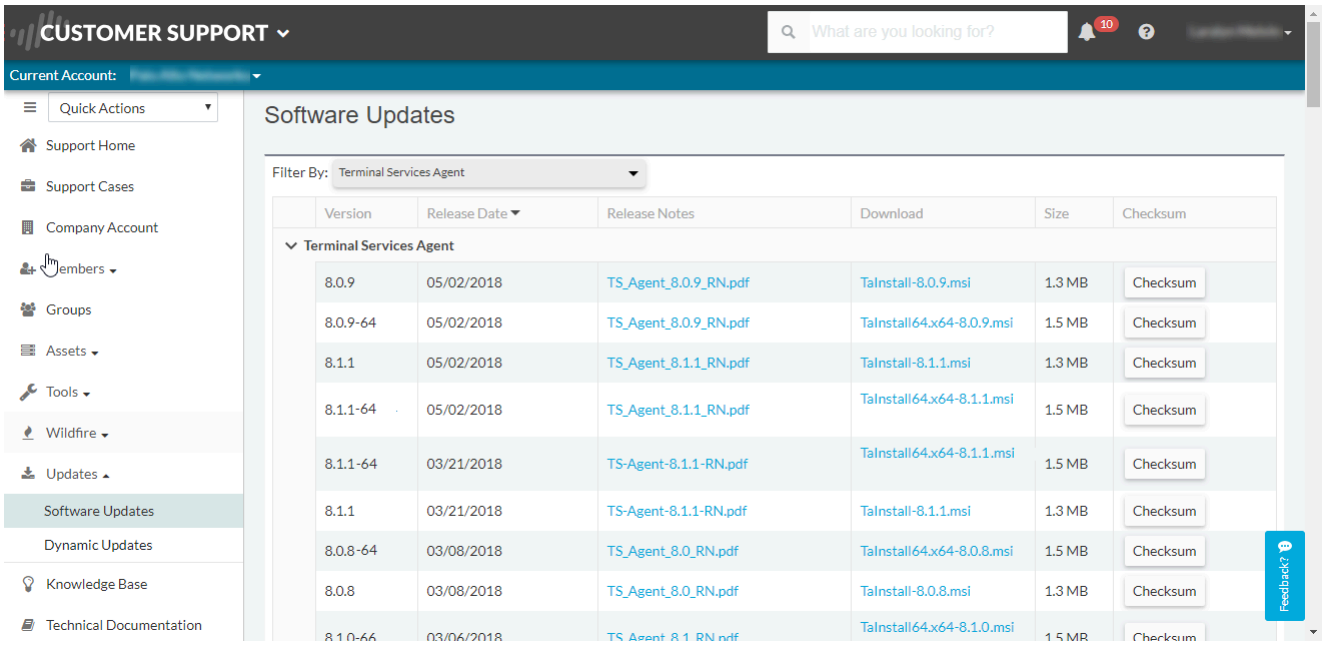
TS エージェントをターミナル サーバーにインストールおよび設定するには、以下の手順を実行します。すべてのユーザーを正しくマッピングするには、ユーザーがログインするすべてのターミナル サーバー上に TS エージェントをインストールする必要があります。

TS エージェント *7.0* 以降のバージョンを使用している場合、*TS* エージェント ホスト上のすべての *Sophos* アンチウイルス ソフトを無効化してください。それ以外の場合、ウイルス対策ソフトウェアは、*TS*エージェントが割り当てるソース・ポートを上書きします。

デフォルト値、範囲、およびその他の指定については、ターミナル サーバー ユーザー向けのユーザー マッピング設定を参照してください。*TS* エージェントでサポートされているターミナル サーバーと、各 ファイアウォール モデルでサポートされている *TS* エージェントの数については、Palo Alto Networks Compatibility Matrix を参照してください。

STEP 1 | TS エージェント インストーラをダウンロードします。

1. Palo Alto Networks カスタマー サポート ポータルにログインします。
2. **Updates**（更新） > **Software Updates**（ソフトウェア更新）を選択します。
3. **Filter By (**フィルタリング基準)を**Terminal Services Agent (**ターミナル サービス エージェント)に設定し、インストールするエージェントのバージョンを、対応する Download (ダウンロード) 列で選択します。たとえば、TS エージェント 9.0 をダウンロードするために、**TaInstall-9.0.msi** を選択します。
4. エージェントをインストールする予定のシステム上に `TaInstall.x64-x.x.x-xx.msi` ファイルまたは `TaInstall-x.x.x-xx.msi` ファイルを保存します(Windows システムが 32 ビット OS または 64 ビット OS のどちらを実行しているかによって適切なバージョンを選択する必要があります)。



STEP 2 | 管理者としてインストーラを実行します。

1. Windows **Start**（スタート）メニューを開き、 **Command Prompt**（コマンドプロンプト）プログラムを **Run as administrator**（管理者として実行）するために右クリックで起動します。
2. コマンド ラインから、ダウンロードした .msi ファイルを実行します。たとえば、`TaInstall-9.0.msi` ファイルをデスクトップに保存した場合、以下のように入力します。

```
C:\Users\administrator.acme>cd Desktop
C:\Users\administrator.acme\Desktop>TaInstall-9.0.0-1.msi
```

3. デフォルトの設定を使用してエージェントをインストールするには、セットアップ プロンプトに従いします。セットアップは `C:\ProgramFiles\P1alo A1lto Ne1tworks\`ターミナル サーバー エージェント にエージェントをインストールします。

   正しいポート割り当てを確保するには、デフォルトのターミナル サーバー エージェントのインストール フォルダーの場所を使用する必要があります。

4. インストールの完了後、**Close**（閉じる）をクリックしてセットアップ ダイアログを閉じます。

   既存の *TS* エージェントよりもドライバが新しい *TS* エージェントにアップグレードする場合、アップグレード後にシステムを再起動する必要があることを示すプロンプトがインストール ウィザードで表示されます。

STEP 3 | TS エージェントがエンド ユーザーに割り当てるポートの範囲を定義します。

System Source Port Allocation Range（システム送信元ポート割り当て範囲）および ***System Reserved Source Ports***（システム予約済み送信元ポート）は、非ユーザー セッションに割り当てられるポートの範囲を指定します。これらのフィールドの値がユーザー トラフィックに指定するポートと重複しないようにします。これらの値は、対応する *Windows* のレジストリ設定を編集することによってのみ変更できます。*TS* エージェントは、セッション *0* が発生させたネットワーク トラフィック用のポートを割り当てません。

1. Windows **Start**（スタート）メニューを開き、 **Terminal Server Agent**（ターミナル サーバー エージェント） を選択して、ターミナル サーバー エージェント アプリケーションを起動します。
2. エージェントを**Configure**（設定）（サイドメニュー）します。
3. **Source Port Allocation Range**（送信元ポート割り当て範囲）を入力します(デフォルトは 20,000 ～ 39,999)。これは、TS エージェントがユーザー マッピングに割り当てるポート番号の全範囲です。指定するポート範囲は **System Source Port Allocation**

Range（システム送信元ポート割り当て範囲）と重複しないようにする必要があります。

4. （任意）TS ポート エージェントがユーザー セッションに割り当てないようにする送信元ポート割り当て内のポートまたはポート範囲がある場合、それらを**Reserved Source Ports**（予約済み送信元ポート）として指定します。複数の範囲を含めるには、スペースを入れずにカンマを使用します（例:**2000-3000,3500,4000-5000**）.
5. ターミナル サーバー（**Port Allocation Start Size Per User**（ユーザーごとのポート割り当て開始サイズ））にログインしたときに各個人ユーザーに割り当てるポート数を指定します(デフォルトは 200)。
6. **[ユーザーごとのポート割り当て最大サイズ]** を指定します。これは、ターミナル サーバー エージェントが個人ユーザーに割り当てられる最大ポート数です。
7. ユーザーが割り当てられたポートを使い果たした場合に、そのユーザーからのトラフィックの処理を続行するかどうかを指定します。**Fail port binding when available ports are used up**（使用可能なポートを使い果たすとポート バインドに失敗する）オプションがデフォルトで有効で、これはすべてのポートが使用された場合には、アプリケーションはトラフィックの送信に失敗することを示します。ユーザーがポートを使い果たしてもアプリケーションを使い続けることができるようにするには、このオプションを無効（クリア）にしますが、そうすると、このトラフィックが User-ID で識別されない場合があります。
8. シャットダウンしようとしたときにターミナル サーバーが応答を停止した場合は、**Detach agent driver at shutdown**（シャットダウン時にエージェントドライバを切り離す）オプションを有効にします。

STEP 4 | （任意）TS エージェントおよびファイアウォール間の相互認証に使用する独自の証明書を割り当てます。

1. エンタープライズ PKI から TS エージェント用の証明書を取得するか、ファイアウォール上で生成します。サーバー証明書の秘密鍵を暗号化し、証明書を PEM ファイル形式でアップロードする必要があります。証明書をアップロードするために以下のいずれかのタスクを実行します。
   - 証明書の生成を行い、エクスポートします。
   - 企業用のCertificate Authority (認証局 - CA)から証明書をエクスポートします。

2. サーバー証明書を TS エージェントに追加します。
   1. TS エージェントで、**Server Certificate (**サーバー証明書**)** を選択し、新しい証明書を**Add (**追加**)**します。
   2. CA から受信した証明書ファイルのパスと名前を入力するか、証明書ファイルを参照します。
   3. 秘密鍵のパスワードを入力します。
   4. **OK** をクリックします。
   5. 変更を **Commit (**コミット**)**します。

   TS エージェントは、次の情報を含む自己署名証明書をポート *5009* 上で使用します:*Issuer:CN=Terminal Server Agent*、*OU=Engineering*、*O=Palo Alto Networks*、*L=Santa Clara, S=California*、*C=USSubject:CN=Terminal Server Agent*、*OU=Engineering*、*O=Palo Alto Networks*、*L=Santa Clara, S=California*、*C=US*
3. ファイアウォール用の証明書プロファイルを設定して割り当てます。
   1. **Device** （デバイス） > **Certificate Management** （証明書の管理） > **Certificate Profile** （証明書プロファイル）の順に選択し、証明書プロファイルの設定を行います。

      Windows User-ID エージェントおよび *TS* エージェントに対して割り当てられる証明書プロファイルは *1* つだけです。そのため証明書プロファイルには、*Windows User-ID* エージェントおよび *TS* エージェントを接続するためにアップロードした証明書を発行した認証局がすべて含まれていなければなりません。
   2. **Device (**デバイス**)** > **User Identification (**ユーザー **ID)** > **Connection Security (**接続セキュリティ**)** を選択します。
   3. **User-ID Certificate Profile**（**User-ID** 証明書プロファイル）として前のステップで設定した証明書プロファイルを選択（）し、編集します。
   4. **OK** をクリックします。
   5. 変更を **Commit (**コミット**)**します。

STEP 5 | ファイアウォールがターミナル サーバー エージェントと接続するように設定します。

ユーザー マッピングの取得のためにターミナル サーバー エージェントに接続する各ファイアウォールで、以下の手順を実行します。

1. **Device (デバイス)** > **User Identification (ユーザー ID)** > **Terminal Server Agents (ターミナル サーバー エージェント)** の順に選択し、新しい TS エージェントを**Add (追加)** します。
2. **[名前]** に、ターミナル サーバー エージェントの名前を入力します。
3. ターミナル サーバー エージェントがインストールされている Windows**Host (ホスト)** のホスト名または IP アドレスを入力します。

   ホスト名または IP アドレスは、静的 IP アドレスに対して解決しなければなりません。既存のホスト名を変更すると、変更をコミットして新しいホスト名を解決するときに TS エージェントがリセットされます。ホスト名が複数の IP アドレスに解決される場合、TS エージェントはリストの最初のアドレスを使用します。
4. (任意) 発信トラフィックのソース IP アドレスとして表示できる **Alternative IP Addresses (代替 IP アドレス)** のホスト名または IP アドレスを入力します。

   ホスト名または IP アドレスは、静的 IP アドレスに対して解決しなければなりません。最大 8 個の IP アドレスまたはホスト名を追加することができます。
5. エージェントがユーザー マッピング要求をリッスンする **Port**[ポート] 番号を入力します。この値は、 ターミナル サーバー エージェント上で設定された値と一致する必要があります。デフォルトでは、ポートは、ファイアウォールおよびエージェントで 5009 に設定されます。ファイアウォールで変更する場合は、ターミナル サーバー エージェントの **Configure**（設定） ダイアログの **Listening Port**（リスニング ポート）も同じポートに変更する必要があります。
6. 設定が **Enabled**[有効] になっていることを確認し、**OK**[OK] をクリックします。
7. 変更を **Commit (コミット)**します。
8. **Connected (接続済み)** の状態が接続済み(緑色のライト)と表示されていることを確認します。

STEP 6 | ターミナル サーバー エージェントが IP アドレスをユーザー名に正しくマッピングしていることと、ファイアウォールがエージェントに接続できることを確認します。

1. Windows **Start**[スタート]メニューを開いて、 ターミナル サーバー エージェントを選択します。
2. 接続リスト内の各ファイアウォールの **Connection Status** [接続状態]が `Connected`[接続済み] になっていることを確認することにより、ファイアウォールが接続できることを確認します。
3. ターミナル サーバー エージェントがポート範囲をユーザー名（サイドメニューの **Monitor**（モニター））に正常にマッピングしていることを確認し、マッピング テーブルにデータが入力されていることを確認します。

STEP 7 | (Windows 2012 R2 サーバーのみ) Microsoft Internet Explorer で ブラウザを使用する各ユーザーの Enhanced Protected Modeを無効にします。

この作業は Google Chromeや Mozilla Firefox などの他のブラウザでは必要ありません。

すべてのユーザーで *Enhanced Protected Mode* を無効にするには、Local Security Policyを使用します。

Windows サーバーでこれらのステップを実行します。

1. Internet Explorer をスタートします。
2. **Settings**（設定） > **Internet options**（インターネット オプション） > **Advanced**（詳細）を選択し、セキュリティ セクションにスクロールします。
3. **Enable Enhanced Protected Mode**（拡張保護モードの有効化）オプションを無効（クリア）にします。
4. **OK** をクリックします。

*Internet Explorer*では、 *Palo Alto Networks*は *Protected Mode*を無効にしないことを推奨します。 *Enhanced Protected Mode* とは異なります。

ユーザー ID XML API を使用したターミナル サーバーからのユーザー マッピングの取得

PAN-OS XML API は、標準 HTTP 要求を使用してデータを送受信します。API 呼び出しは、cURL などのコマンド行ユーティリティから直接行ったり、RESTful サービスをサポートする任意のスクリプトまたはアプリケーション フレームワークを使用して行うことができます。

非 Windows ターミナル サーバーがユーザー マッピング情報をファイアウォールに直接送信できるようにするには、ユーザーのログインおよびログアウト イベントを抽出するスクリプトを作成し、それを使用してユーザー ID XML API 要求フォーマットに入力します。その後、 cURL または wget を使用して XML API 要求をファイアウォールに送信するメカニズム、および安全な通信のためにファイアウォールの API キーを提供するメカニズムを定義します。ターミナル サーバーなどのマルチユーザー システムからユーザー マッピングを作成するには、以下の API メッセージを使用する必要があります。

- **<multiusersystem>** — firewall 上の XML API Multi-user System の構成を設定します。このメッセージにより、ターミナル サーバーの IP アドレスの定義が可能になります(これがそのターミナル サーバー上のすべてのユーザーの送信元アドレスになります)。さらに、**<multiusersystem>** セットアップ メッセージには、ユーザー マッピングに割り当てる送信元ポート番号の範囲と、ログイン時に個々のユーザーに割り当てるポートの数 (*block size* と呼ばれます) が指定されています。デフォルトのソース・ポート割り振り範囲 (1025-65534) とブロック・サイズ (200) を使用する場合は、**<multiusersystem>** セットアップ・イベントを firewall に送信する必要はありません。ファイアウォールは最初のユーザー ログイン イベント メッセージを受信したときに、自動的にデフォルト設定を使用して XML API マルチユーザー システム設定を生成します。
- **<blockstart>** — **<login>** および **<logout>** メッセージと共に使用して、ユーザーに割り当てられた開始ソース ポート番号を示します。その後、ファイアウォールはブロック サイズを使用して、ログイン メッセージ内の IP アドレスおよびユーザー名にマップする実際のポー

ト番号範囲を決定します。例えば、**<blockstart>** 値が 13200 で、マルチユーザー・システム用に構成されたブロック・サイズが 300 の場合、ユーザーに割り振られる実際のソース・ポート範囲は 13200 から 13499 です。ユーザーが開始した各接続は、割り当てられた範囲内で一意の送信元ポート番号を使用する必要があります。これにより、ファイアウォールは、IP アドレス対ポート対ユーザーのマッピングに基づいてユーザーを識別し、ユーザーベース、およびグループベースのセキュリティ ルールを実施できます。ユーザーが割り当てられたすべてのポートを使い果たすと、ターミナル サーバーは、firewall が IP アドレス-ポート-ユーザー マッピングを更新できるように、ユーザーに新しいポート範囲を割り当てる新しい **<login>** メッセージを送信する必要があります。さらに、1 つのユーザー名に同時に複数のポート ブロックをマップすることもできます。firewall は、**<logout>** パラメーターを含む **<blockstart>** メッセージを受信すると、対応する IP アドレス - ポート - ユーザー マッピングをマッピング テーブルから削除します。firewall は、ユーザー名と IP アドレスを含む **<logout>** メッセージを受信したが、**<blockstart>** は受信しない場合、そのユーザーをテーブルから削除します。また、firewall が IP アドレスのみの **<logout>** メッセージを受信すると、マルチユーザーシステムとそれに関連付けられたすべてのマッピングが削除されます。

ターミナル サーバーがファイアウォールに送信する *XML* ファイルには、複数のメッセージ タイプを含めることができます。メッセージはファイル内で特定の順序である必要はありません。ただし、複数のメッセージ タイプを含む *XML* ファイルを受信すると、ファイアウォールは、マルチユーザー システム要求を最初に処理し、次にログイン、その後にログアウトの順で処理します。

以下のワークフローは、PAN-OS XML API を使用してユーザー マッピングを非 Windows ターミナル サーバーからファイアウォールに送信する方法の例を示しています。

STEP 1 | ファイアウォールとターミナル サーバーの間の API 通信を認証するために使用される API キーを生成します。キーを生成するには、管理アカウントのログイン認証情報を提供する

必要があります。すべての管理者(XML API 権限を有効にしたロールベースの管理者を含む)が API を使用できます。

パスワード内の特殊文字は、*URL*パーセントエンコードにする必要があります。

ブラウザから、ファイアウォールにログインします。その後、ファイアウォールの API キーを生成するために、新しいブラウザ ウィンドウを開き、以下の URL を入力します。

```
https://<Firewall-IPaddress>/api/?
type=keygen&user=<username>&password=<password>
```

ここで、**<Firewall-IPaddress>** は firewall の IP アドレスまたは FQDN、**<username>** と **<password>** は firewall の管理ユーザー アカウントの資格情報です。以下に例を示します。

```
https://10.1.2.5/api/?type=keygen&user=admin&password=admin
```

ファイアウォールはキーを含むメッセージで応答します。以下に例を示します。

```
<response status="success">    <result>
       <key>k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg=</key>
    </result> </response>
```

STEP 2 | (任意)ターミナル サーバー エージェントが使用するポート範囲およびユーザーごとのポートのブロック サイズを指定するためにターミナル サーバーが送信するセットアップ メッセージを生成します。

ターミナル サーバー エージェントがセット アップ メッセージを送信しない場合、ファイアウォールは、最初のログイン メッセージの受信時に以下のデフォルト設定を使用して自動的にターミナルサーバー エージェント設定を作成します。

- デフォルト ポート範囲：1025 から 65534 の間
- ユーザーあたりのブロック サイズ:200
- マルチユーザー システムの最大数:1,000

以下に、サンプル セットアップ メッセージを示します。

```
<uid-message> <payload> <multiusersystem> <entry ip="10.1.1.23"
 startport="20000"          endport="39999" blocksize="100/"> </
multiusersystem> </payload> <type>アップデート</type> <version>1.0</
version> </uid-message>
```

ここで、`entry ip` はターミナル サーバー ユーザーに割り当てられる IP アドレスを指定し、`startport` および `endport` はポートを個別ユーザーに割り当てるときに使用するポートの範囲を指定し、`blocksize` は各ユーザーに割り当てるポート数を指定します。最大ブ

ロック サイズは 4000 で、各マルチユーザー システムは最大 1000 個のブロックを割り当てられます。

カスタムのブロック サイズやポート範囲を定義する場合、範囲内のすべてのポートが割り当てられ、ギャップや使用されないポートがないような値を設定する必要があります。たとえば、ポート範囲を 1000-1499 に設定すると、ブロック サイズを 100 に設定することはできますが、200 に設定することはできません。200 に設定した場合、範囲の最後に使用されないポートがあるためです。

STEP 3 | ログイン イベントを抽出するスクリプトを作成し、ファイアウォールに送信する XML インプット ファイルを作成します。

スクリプトで実施する割り当てのポート番号範囲が固定された境界を持ち、ポートの重複がないようにします。たとえば、ポート範囲が 1000-1999 でブロック サイズが 200 の場合、許容できる blockstart 値は 1000、1200、1400、1600、または 1800 です。blockstart 値に 1001、1300、1850 は許容できません。これらの値を使用すると、範囲内に使用されないポート番号が残るためです。

ターミナル サーバーがファイアウォールに送信するログイン イベント ペイロードには、複数のログイン イベントを含めることができます。

以下に、PAN-OS XML ログイン イベントの入力ファイル形式を示します。

```
<uid-message> <payload> <login> <entry name="acme\jjaso"
 ip="10.1.1.23" blockstart="20000"> <entry name="acme\jparker"
 ip="10.1.1.23" blockstart="20100"> <entry name="acme\ccrisp"
 ip="10.1.1.23" blockstart="21000"> </login> </payload> <type>アップデート</type> <version>1.0</version> </uid-message>
```

ファイアウォールはこの情報を使用してユーザー マッピング テーブルにデータを入力します。上の例で抽出されたマッピングに基づくと、ファイアウォールがソースアドレスおよびポートが 10.1.1.23:20101 のパケットを受信した場合、その要求はポリシー実施のためにユーザー jparker にマッピングされます。

各マルチユーザー システムは、最大 *1,000* 個のポート ブロックを割り当てられます。

STEP 4 | ログアウト イベントを抽出するスクリプトを作成し、ファイアウォールに送信する XML インプット ファイルを作成します。

ファイアウォールは、**blockstart** パラメータを含む **logout** イベント メッセージを受信すると、対応する IP アドレス対ポート対ユーザーのマッピングを削除します。**logout** メッセージにユーザー名と IP アドレスが含まれ、**blockstart** パラメータが含まれていない場合、ファイアウォールはそのユーザーに対するすべてのマッピングを削除します。**logout**

メッセージに IP アドレスのみが含まれている場合、ファイアウォールはそのマルチユーザー システムとすべての関連付けられたマッピングを削除します。

以下に、PAN-OS XML ログアウト イベントの入力ファイル形式を示します。

```
<uid-message> <payload> <logout> <entry name="acme\jjaso"
 ip="10.1.1.23" blockstart="20000"> <entry name="acme\ccrisp"
 ip="10.1.1.23"> <entry ip="10.2.5.4"> </logout> </payload>
 <type>アップデート</type> <version>1.0</version> </uid-message>
```

また、ファイアウォールから以下の *CLI* コマンドを使用してマルチユーザー システム エントリをクリアすることもできます。***clear xml-api multiusersystem***

STEP 5 | XML API を使用して割り当てられたポート ブロック範囲を実際にターミナル サーバーでユーザーに割り当てられた送信元ポートに一致させ、ユーザーがログアウトしたりポート割り当てが変更されたときにこのマッピングが削除されるように、動的に実行する方法が作成したスクリプトに含まれるようにします。

これを行う方法の 1 つは、Netfilter NAT ルールを使用して、ユーザー セッションを XML API を介して uid に基づき割り当てられた特定のポート範囲に隠すことです。たとえば、User-ID が jjaso のユーザーが送信元ネットワーク アドレス変換(SNAT)値 10.1.1.23:20000-20099 にマッピングされるようにするには、作成したスクリプトに以下が含まれている必要があります。

```
[root@ts1 ~]# iptables -t nat -A POSTROUTING -m owner --uid-owner
 jjaso -p tcp -j SNAT --to-source 10.1.1.23:20000-20099
```

同様に、作成したスクリプトによって、ユーザーがログアウトしたときやポート割り当てが変更されたときに IP テーブル ルーティング設定がダイナミックに SNAT マッピングを削除するようにする必要があります。

```
[root@ts1 ~]# iptables -t nat -D POSTROUTING 1
```

STEP 6 | セットアップ、ログイン、およびログアウト イベントを含む XML 入力ファイルを、ファイアウォールに送信するために wget または cURL メッセージにパッケージする方法を定義します。

wget を使用してファイルをファイアウォールに適用するには、以下のコマンドを実行します。

```
> wget --post file <filename> “https://<Firewall-IPaddress>/api/?type=user-id&key=<key>&file-name=<input_filename.xml>&client=wget&vsys=<VSYS_name>”
```

たとえば、wget を使用して、login.xml という名前の入力ファイルを 10.2.5.11 のファイアウォールにキー k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg を使用して送信する構文は以下のようになります。

```
> wget --post file login.xml “https://10.2.5.11/api/?type=user-id&key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&file-name=login.xml&client=wget&vsys=vsys1”
```

cURL を使用してファイルをファイアウォールに適用するには、以下のコマンドを実行します。

```
> curl --form file=@<filename> https://<Firewall-IPaddress>/api/?type=user-id&key=<key>&vsys=<VSYS_name>
```

たとえば、cURL を使用して、login.xml という名前の入力ファイルを 10.2.5.11 のファイアウォールにキー k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg を使用して送信する構文は以下のようになります。

```
> curl --form file@login.xml “https://10.2.5.11/api/?type=user-id&key=k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg&vsys=vsys1”
```

STEP 7 | ファイアウォールがターミナル サーバーからのログイン イベントを正しく受信していることを確認します。

ファイアウォールへの SSH コネクションを開き、以下の CLI コマンドを実行することによって設定を確認します。

ターミナル サーバーが **XML** を介してファイアウォールに接続していることを確認するには、以下のコマンドを実行します。

```
admin@PA-5250> show user xml-api multiusersystem Host Vsys
 Users Blocks ----------------------------------------
 10.5.204.43   vsys1      5         2
```

ファイアウォールが **XML** を介してターミナル サーバーからマッピングを受信していることを確認するには、以下のコマンドを実行します。

```
admin@PA-5250> show user ip-port-user-mapping all Global max host
 index 1, host hash count 1 XML API Multi-user System 10.5.204.43
 Vsys 1,  Flag 3 Port range:20000 - 39999 Port size: Start 200;
```



```
 max 2000 Block Count 100、Port Count 20000 20000-20199: acme
\administrator Total host:{{{防御>防御<防御}>{防御>防御<防御}<{防御>防
御<防御}}>{{防御>防御<防御}>{防御>防御<防御}<{防御>防御<防御}}<{{防御>防
御<防御}>{防御>防御<防御}<{防御>防御<防御}}}
```

XML API を使用した User-ID へのユーザー マッピングの送信

User-ID はユーザー情報をキャプチャする多くのユーザー マッピング情報取得手法を供給します。しかし、ユーザー情報をキャプチャするアプリケーションやデバイスの中にはネイティブには User-ID に統合できないものもあります。例えば、社内で開発したカスタム アプリケーションや標準的なユーザー マッピング手法をサポートしていないデバイスなどです。その場合、PAN-OS XML API を使用して、カスタム スクリプトを作成し、PAN-OS 統合 User-ID エージェントまたは直接、ファイアウォールに送信することができます。PAN-OS XML API は、標準 HTTP 要求を使用してデータを送受信します。API 呼び出しは、cURL などのコマンド ライン ユーティリティから直接実行できます。また、POST と GET 要求をサポートする任意のスクリプトやアプリケーション フレームワークを使用して実行することもできます。

外部システムがユーザー マッピング情報を PAN-OS 統合 User-ID エージェントに送信できるようにするには、ユーザーのログインおよびログアウト イベントを抽出するスクリプトを作成し、イベントを使用して PAN-OS XML API 要求フォーマットに入力します。その後、 例えば cURL を使用して XML API 要求をファイアウォールに送信するメカニズムおよび、安全な通信のためにファイアウォールの API キーを使用するメカニズムを定義します。詳細は、『PAN-OS XML API 使用ガイド』を参照してください。

ユーザーおよびグループ ベースのポリシーの有効化

ユーザー ID の有効化を行った後、特定のユーザーおよびグループに適用されるセキュリティポリシーを設定できるようになります。ユーザーベースのポリシー制御は、アプリケーション情報（どのカテゴリおよびサブカテゴリに属すか、基本となるテクノロジー、アプリケーションの特性など）も含めることができます。アウトバウンドあるいはインバウンドのどちらの方向でも、ポリシールールを定義して、ユーザーあるいはユーザーグループに基づいてアプリケーションを安全に有効化できます。

ユーザーベースのポリシーの例は次の通りです。

- 標準ポートで SSH、telnet、FTP などのツールを使用できるのは IT 部門のみにします。
- ヘルプ デスク サービス グループでの Slack の使用を許可します。
- すべてのユーザーが Facebook を閲覧できるものの、Facebook アプリの使用はブロックし、投稿できる人物をマーケティング担当者に制限します。

複数のアカウントのあるユーザーのポリシーの有効化

組織のユーザーに複数の責任がある場合、そのユーザーには複数のユーザー名(アカウント)があり、それぞれのユーザー名に特定のサービス セットにアクセスするための異なる権限が割り当てられている一方で、すべてのユーザー名で同じ IP アドレス(ユーザーのクライアント システム)を共有していることがあります。ただし、ユーザー ID エージェントは 1 つの IP アドレス(ターミナル サーバー ユーザーの場合は IP アドレスおよびポート範囲)を 1 つのユーザー名にのみマッピングしてポリシーを実施できますが、エージェントがマッピングするユーザー名は予測できません。ユーザーのすべてのユーザー名のアクセスを制御するには、ルール、ユーザー グループ、およびユーザー ID エージェントを調整する必要があります。

たとえば、ファイアウォールに、ユーザー名 corp_user の電子メールへのアクセスを許可するルールと、ユーザー名 admin_user の MySQL サーバーへのアクセスを許可するルールがあるとします。ユーザーは、同じクライアント IP アドレスからいずれかのユーザー名を使用してログインします。ユーザー ID エージェントが IP アドレスを corp_user に割り当てた場合、ユーザーが corp_user と admin_user のどちらでログインしても、ファイアウォールは、そのユーザーを corp_user として識別し、電子メールへのアクセスは許可しますが、MySQL サーバーへのアクセスは許可しません。一方、ユーザー ID エージェントが IP アドレスを admin_user にマッピングした場合、ファイアウォールは、ログインに関係なくそのユーザーを常に admin_user として識別し、MySQL サーバーへのアクセスは許可しますが、電子メールへのアクセスは許可しません。以下の手順では、この例の両方のルールを実施する方法を説明します。

STEP 1 | 個別のアクセス権限を必要とする各サービスのユーザー グループを設定します。

この例では、各グループは 1 つのサービス(電子メールまたは MySQL サーバー)を対象としています。ただし、通常は同じ権限を必要とする一連のサービスに対して各グループを設定します(基本的なすべてのユーザー サービスのグループとすべての管理サービスのグループなど)。

ユーザーが求めるサービスにアクセスできるユーザー グループがすでに組織にある場合、より制限の少ないサービスで使用するユーザー名をそれらのグループに追加するだけで済みます。この例では、電子メール サーバーでは MySQL サーバーよりも制限の少ないアクセスを必要としています。corp_user は、電子メールにアクセスするためのユーザー名です。そのため、電子メールにアクセスできるグループ(corp_employees)と、MySQL サーバーにアクセスできるグループ(network_services)に corp_user を追加します。

特定の既存のグループにユーザー名を追加することが組織の慣行に違反する場合、LDAP フィルタに基づいてカスタム グループを作成できます。この例では、network_services がカスタム グループで、以下のように設定するとします。

1. **Device (デバイス)** > **User Identification (ユーザー ID)** > **Group Mapping Settings (グループ マッピング設定)** の順に選択し、一意の **Name (名前)** のグループ マッピング設定を **Add (追加)** します。
2. LDAP **Server Profile** [LDAP サーバー プロファイル]を選択し、 **Enabled**[有効] チェックボックスがオンになっていることを確認します。
3. Custom Group [カスタム グループ] タブを選択し、Name [名前] が network_services のカスタム グループを Add [追加] します。

4. corp_user の LDAP 属性に一致する**LDAP Filter** [LDAP フィルタ]を指定し、 **OK** をクリックします。
5. **OK**、**Commit (コミット)** の順にクリックします。

> 後で、より制限の少ないサービスのグループの他のユーザーに、より制限の多いサービスにアクセスする追加のユーザー名を付与する場合、それらのユーザー名をより制限の多いサービスのグループに追加できます。このシナリオは、この逆のシナリオよりも一般的です。通常、より制限の多いサービスにアクセスできるユーザーは、より制限の少ないサービスにもアクセスできます。

STEP 2 | 設定したグループに基づいて、ユーザー アクセスを制御するルールを設定します。

詳細については、 「ユーザーおよびグループ ベースのポリシーの有効化」を参照してください

1. corp_employees グループに電子メールへのアクセスを許可するセキュリティ ルールを設定します。
2. network_services グループに MySQL サーバーへのアクセスを許可するセキュリティ ルールを設定します。

STEP 3 | ユーザー ID エージェントの無視リストを設定します。

これにより、ユーザー ID エージェントは、クライアント IP アドレスを、設定したルールに割り当てられているグループのメンバーであるユーザー名にのみマッピングします。無視リストには、それらのグループのメンバーでないユーザーのすべてのユーザー名が含まれている必要があります。

この例では、クライアント IP アドレスが corp_user にマッピングされるように、Windows ベースのユーザー ID エージェントの無視リストに admin_user を追加します。これにより、ユーザーが corp_user としてログインしているか、admin_user としてログインしているかに関係なく、ファイアウォールはユーザーを corp_user として識別し、設定した両方のルールを適用します(corp_user ユーザーはルールで参照されるグループのメンバーであるため)。

1. `ignore_user_list.txt` ファイルを作成します。
2. ファイルを開き、admin_user を追加します。

   後でユーザー名を追加する場合、各ユーザー名は 1 行ずつ指定する必要があります。
3. エージェントがインストールされているドメイン サーバーのユーザー ID エージェント フォルダにファイルを保存します。

> *PAN-OS* 統合ユーザー *ID* エージェントを使用する場合は、 「PAN-OS 統合 User-ID エージェントを使用したユーザー マッピングの設定」の指示を参照して無視リストを設定します。

STEP 4 | 制限されたサービスのエンドポイント認証を設定します。

これにより、エンドポイントでユーザーの認証情報を検証できるようになり、複数のユーザー名のあるユーザーのアクセスを有効にできます。

この例では、MySQL サーバーにサービス要求を送信するために、network_services グループのメンバーとして corp_user を許可するファイアウォール ルールを設定しました。今度は、認証されていないユーザー名(corp_user など)に応答するように MySQL サーバーを設定する必要があります。この応答では、認証されているユーザー名(admin_user)のログイン認証情報を入力するようにユーザーに求めます。

ユーザーが *admin_user* としてネットワークにログインすると、*admin_user* の認証情報を再度求められることなく *MySQL* サーバーにアクセスできます。

この例では、corp_user と admin_user の両方に電子メール アカウントがあるため、ネットワークにログインするときに入力したユーザー名に関係なく、電子メール サーバーから追加の認証情報を求められることはありません。

これでファイアウォールでは、複数のユーザー名のあるユーザーのルールを実施する準備ができました。

User-ID 設定の確認

ユーザーおよびグループのマッピングを設定し、セキュリティポリシーで User-ID を有効化し、認証ポリシーを設定した後、User-ID が適切に機能することを確認する必要があります。

STEP 1 | ファイアウォール CLI にアクセスします。

STEP 2 | グループ マッピングの動作を確認します。

CLI から以下のオペレーション コマンドを入力します。

```
> show user group-mapping statistics
```

STEP 3 | ユーザー マッピングの動作を確認します。

PAN-OS 統合ユーザー ID エージェントを使用している場合、CLI から以下のコマンドを実行すれば確認できます。

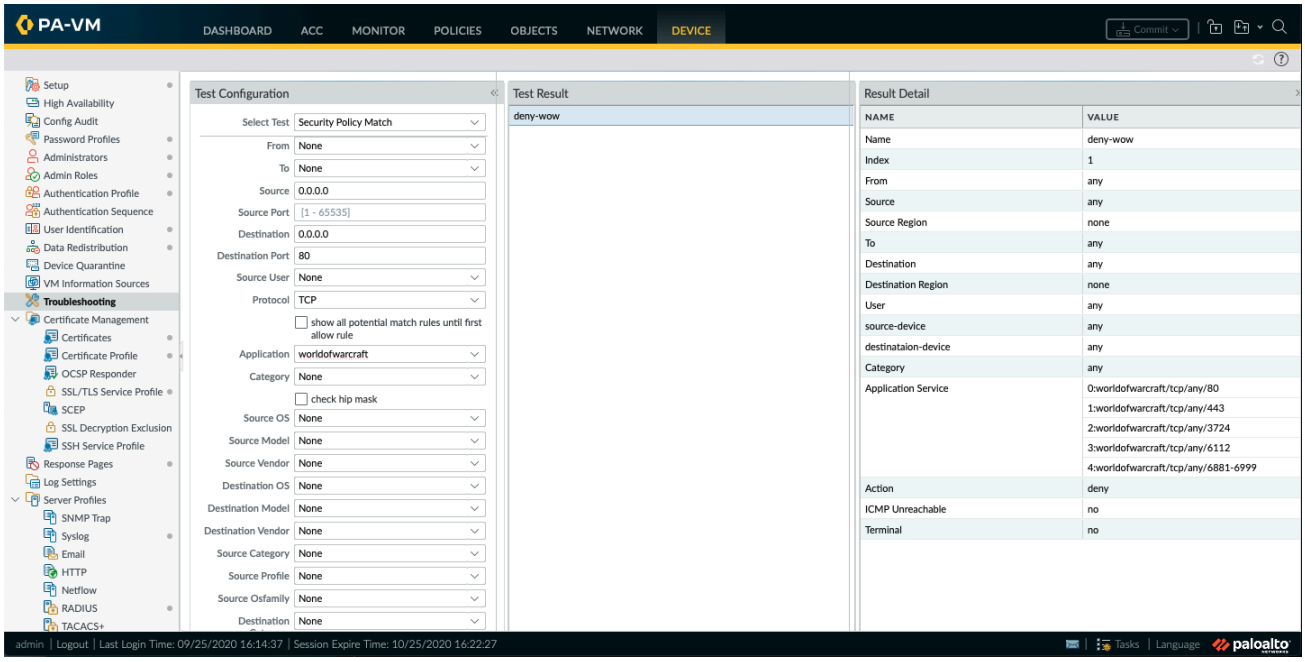
```
> show user ip-user-mapping-mp all
 IP              Vsys  From  User         Timeout (sec)
 ------------------------------------------------------
 192.168.201.1 vsys1 UIA   acme\george             210
 192.168.201.11 vsys1 UIA   acme\duane              210
 192.168.201.50 vsys1 UIA   acme\betsy              210
 192.168.201.10 vsys1 UIA   acme\administrator     210
 192.168.201.100 vsys1 AD    acme\administrator     748 Total:5
 users *:WMI probe succeeded
```

STEP 4 | セキュリティポリシー ルールをテストします。

- ユーザー ID が有効なゾーンのマシンからサイトやアプリケーションにアクセスして、ポリシーで定義したルールをテストし、トラフィックが予想どおりに許可または拒否されていることを確認します。
- また、実行コンフィギュレーションをトラブルシューティングして、ポリシーが正しく設定されているかどうかを判断することもできます。たとえば、World of Warcraft をプレイ

するユーザーをブロックするルールがある場合、以下の手順でポリシーをテストできます。

1. **Device (デバイス)** > **Troubleshooting (トラブルシューティング)** を選択し、Select Test (テストの選択) ドロップダウンから **Security Policy Match (セキュリティポリシー マッチ)** を選択します。
2. 送信元および宛先 IP アドレスとして **0.0.0.0** を入力します。これにより、任意の送信元および宛先の IP アドレスに対してポリシーマッチテストが実行されます。
3. Destination Port (宛先ポート) を入力します。
4. Protocol (プロトコル) を入力します。
5. セキュリティポリシー マッチ テストを **Execute (実行)** します。



STEP 5 | 認証ポリシーおよび認証ポータル設定をテストします。

1. 先ほどと同じゾーンから、Mac OS システムなど、ディレクトリのメンバーでないマシンより、ゾーン外部のシステムを ping します。ping は認証しなくても動作します。
2. 同じマシンからブラウザを開き、定義した認証ルールと一致する宛先ゾーンの Web サイトに移動します。認証ポータルのWebフォームが表示され、ログイン認証情報の入力を求められます。
3. 正しい認証情報を使用してログインし、要求したページにリダイレクトされていることを確認します。
4. また、以下の **test authentication-policy-match** 操作コマンドを使用して認証ポリシーをテストすることもできます。

```
> test authentication-policy-match from corporate to internet
 source 192.168.201.10 destination 8.8.8.8  Matched rule:
 'authentication portal' action: web-form
```

STEP 6 | ログファイルがユーザー名を表示していることを確認します。

ログ ページ（**Monitor (監視)** > **Logs (ログ)** > **Traffic (トラフィック)** など）を選択し、Source User (送信元ユーザー) 列にユーザー名が表示されていることを確認します。

STEP 7 | レポートがユーザー名を表示していることを確認します。

1. **Monitor (監視)** > **Logs (ログ)**を選択します。
2. ユーザー名を含むレポートタイプを選択します。例えば、 Denied Applications レポート、Source User コラムは アプリケーションへのアクセスを試行したユーザーのリストを表示しなければなりません。

大規模ネットワークでのユーザー ID のデプロイ

大規模ネットワークは、ファイアウォールが IP アドレスをユーザー名にマッピングしたり、ユーザー名をユーザーグループにマッピングするためにクェリする情報ソースを数百個持つことができます。ユーザー ID エージェントが収集する前に、ユーザーおよびグループ　マッピング情報を集約することによってユーザー ID の管理を簡略化することができます。それによって必要なエージェント数を減らすことができます。

大規模ネットワークはマッピング情報を使って、ポリシーを適用する多数のファイアウォールを持つこともできます。直接クエリでなく再配信によりマッピング情報を取得できるようにいくつかのファイアウォールを設定することによってクエリ プロセスでファイアウォールと情報ソースが使うリソースを減らすことができます。ユーザーがローカルソース（地域ディレクトリサービスなど）に認証を依存するが、リモートサービスおよびアプリケーション（グローバルデータセンター アプリケーションなど）にアクセスしなければならない場合は、再配信によってファイアウォールはユーザーベース ポリシーを適用できるようになります。

認証ポリシーの設定場合、firewall は認証チャレンジに対するユーザーの応答に関連付けられた認証タイムスタンプも再配布する必要があります。ファイアウォールはこのタイムスタンプを使用し、認証ポリシールールのタイムアウトを評価します。タイムアウトは、認証を成功させたユーザーが、タイムアウトの期間中に後で再度認証を行うことなくサービスおよびアプリケーションをリクエストできるようにします。タイムスタンプを再配信することで、最初にユーザーアクセスを許可したファイアウォールが、後でそのユーザーのアクセスを制御するファイアウォールと異なる場合でも、各ユーザーに対して一貫したタイムアウトを適用することができます。

複数の仮想システムを構成している場合、仮想システムを User-ID ハブとして選択することで、IP アドレス対ユーザー名のマッピングを複数の仮想システムで共有できます。

- 多数のマッピング情報ソースに User-ID を展開する
- データおよび認証タイムスタンプの再配信
- 仮想システム間でのユーザー ID マッピングの共有

多数のマッピング情報ソースに User-ID を展開する

Windows ログ転送およびグローバル カタログ サーバーを使用して、Active Directory (AD)ドメイン コントローラまたは Exchange サーバーの大規模なネットワークのユーザーとグループのマッピングを簡略化します。こうした方法によって、ユーザー ID エージェントが収集する前に、マッピング情報を集約することによってユーザー ID の管理を簡略化することができます。それによって必要なエージェント数を減らすことができます。

- Windows ログ転送およびグローバル カタログ サーバー
- 大規模 User-ID 展開のプランニング
- Windows ログ転送の設定
- 多数のマッピング情報ソースに User-ID を設定する

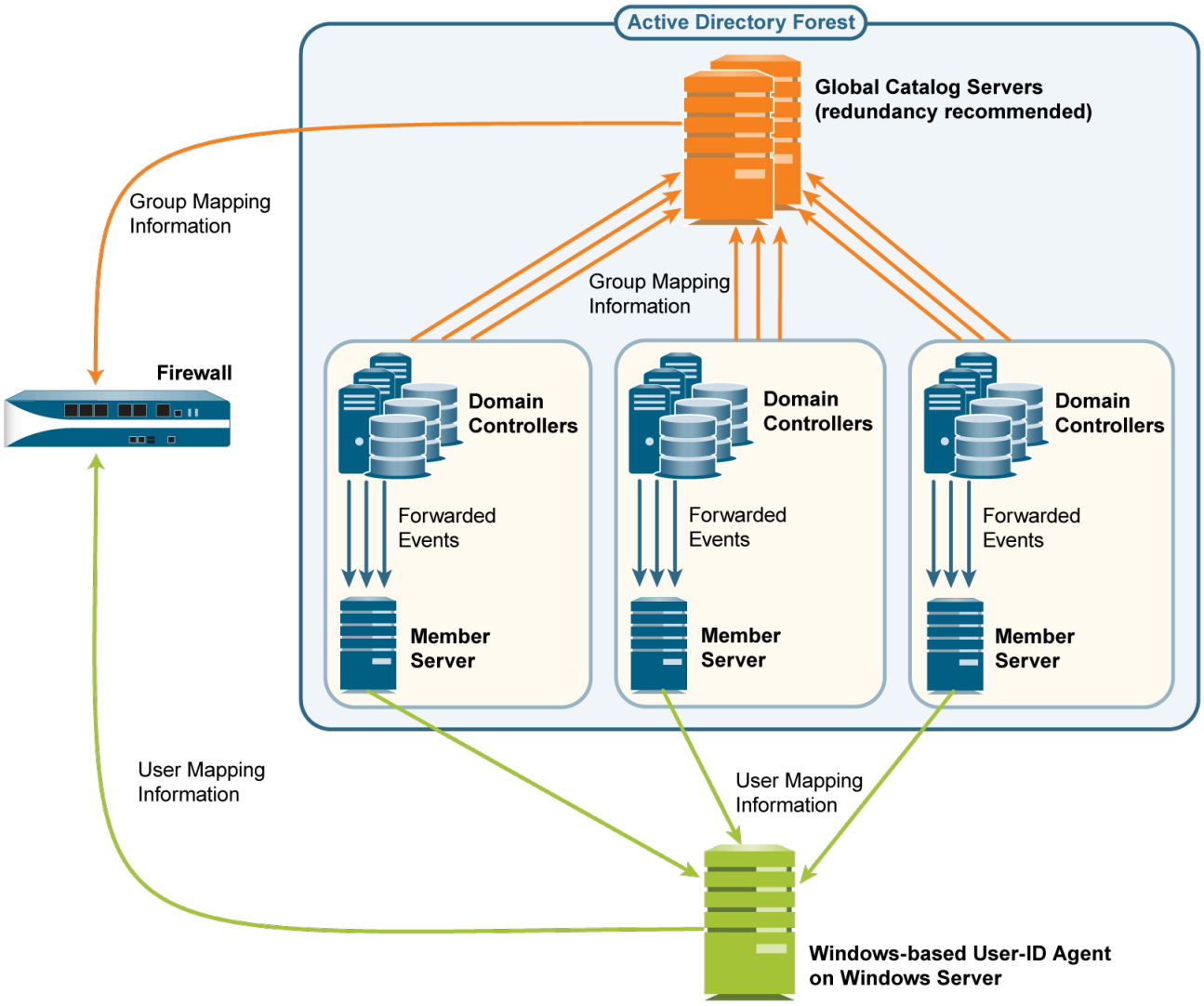
Windows ログ転送およびグローバル カタログ サーバー

ユーザー ID エージェントでモニターできるサーバーの最大数は 100 個であるため、何百もの AD ドメイン コントローラまたは Exchange サーバーのあるネットワークをモニターするには、ファイアウォールは複数のユーザー ID エージェントが必要になります。多数のユーザー ID エージェントを作成および管理する場合、管理上の負荷が大きくなります。特に、新しいドメイン コントローラの追跡が難しいネットワークの拡張ではその傾向が顕著になります。Windows ログ転送では、モニターするサーバー数を削減することで、管理上の負荷を最小限に抑えることができます。その結果、管理する必要があるユーザー ID エージェント数が減少します。Windows ログ転送を設定する場合、複数のドメイン コントローラが各自のログイン イベントを 1 つのドメイン メンバーにエクスポートします。ユーザー ID エージェントは、このドメイン メンバーからユーザー マッピング情報を収集します。

Windows Server バージョン *2012*、および *2012 R2* で *Windows* ログ転送を設定できます。*Windows* ログ転送は、*Microsoft* 以外のサーバーでは使用できません。

大規模なネットワークでグループのマッピング情報を収集するには、ドメイン コントローラからアカウント情報を受信するグローバル カタログ サーバーをクエリするようにファイアウォールを設定します。

以下の図は、ファイアウォールが Windows ベースのユーザー ID エージェントを使用している大規模なネットワークのユーザー マッピングおよびグループ マッピングを示しています。大規模 User-ID 展開のプランニングを参照して、この展開がネットワークに適しているかどうかを判断してください。



大規模 User-ID 展開のプランニング

ユーザー ID の実装で Windows ログ転送およびグローバル カタログ サーバーを使用するかどうかを決定する場合は、システム管理者と相談して以下を決定してください。

- ドメイン コントローラがログイン イベントをメンバー サーバーに転送するのに必要な帯域幅。帯域幅は、ドメイン コントローラのログイン頻度(1 分あたりのログイン数)と各ログイン イベントのバイト サイズを乗算したものです。

  ドメイン コントローラは、セキュリティログ全体を転送するのではなく、ユーザーマッピング プロセスがログインごとに必要とするイベントのみを転送します（Windows Server 2012 および MS Exchange では 4 つのイベント）。

- 以下のネットワーク要素で必要な帯域幅がサポートされているかどうか。
  - **Domain controllers (**ドメイン コントローラ**)** – イベントの転送に関連する処理負荷に対応できる必要があります。
  - **Member Servers (**メンバー サーバー**)** – イベントの受信に関連する処理負荷に対応できる必要があります。
  - **Connections (**接続**)** – ドメイン コントローラ、メンバー サーバー、およびグローバル カタログ サーバーの地理的な分散(ローカルまたはリモート)に左右されます。通常、リモート分散でサポートされる帯域幅の方が少なくなります。

Windows ログ転送の設定

Windows ログ転送を設定するには、Windows サーバーでグループ ポリシーを設定するための管理者権限が必要です。すべての ***Windows Event Collectors*** （ドメイン コントローラからログイン イベントを収集するメンバー サーバー）で Windows ログ転送を設定します。以下に、タスクの概要を示します。特定の手順については、Windows サーバーのドキュメントを参照してください。

STEP 1 | 各 Windows Event Collector で、イベント収集を有効にして、ドメイン コントローラをイベント ソースとして追加し、イベント収集クエリ(サブスクリプション)を設定します。サブスクリプションで指定するイベントは、ドメイン コントローラのプラットフォームによって異なります。

- **Windows Server 2012 (R2 を含む)**および **2016** または **MS Exchange** – 必要なイベントのイベント ID は、4768 (認証チケットが付与されました)、4769 (サービス チケットが付与されました)、4770 (付与されたチケットが更新されました)、4624 (ログオンに成功しました)です。

できるだけ迅速にイベントを転送するには、サブスクリプションの設定時に ***Minimize Latency***（遅延の最小化）を行います。

User-IDエージェントは、デフォルトの転送イベントの場所ではなく、Windows Event Collector 上のセキュリティ ログを監視します。イベント ロギング パスをセキュリティ ログに変更するには、各 Windows イベント コレクタで以下のステップを実行します。

1. Event Viewer を開きます：
2. **Security**（セキュリティ）ログを右クリックし、**Properties**（プロパティ）を選択します。
3. **Log path**（ログのパス）（デフォルトは **`%SystemRoot%\System32\Winevt\Logs\security.evtx`**）をコピーして、**OK** をクリックします。
4. **Forwarded Events**（転送イベント）フォルダを右クリックし、**Properties**（プロパティ）を選択します。
5. ログのパスの置き換えは、**Security**（セキュリティ）ログから値をコピーしてデフォルトの **Log path**（ログのパス）（**`%SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx`**）に貼り付けて、**OK** をクリックします。

STEP 2 | ドメイン コントローラの Windows リモート管理(WinRM)を有効にするグループ ポリシーを設定します。

STEP 3 | ドメイン コントローラの Windows イベント転送を有効にするグループ ポリシーを設定します。

多数のマッピング情報ソースに User-ID を設定する

STEP 1 | ログイン イベントを収集するメンバー サーバーで Windows ログ転送を設定します。

Windows ログ転送の設定を行います。この手順では、Windows サーバーでグループ ポリシーを設定するための管理者権限が必要です。

STEP 2 | Windows ベースのユーザー ID エージェントをインストールします。

メンバーサーバーにアクセスできる Windows Server 上に Windows ベースのユーザー ID エージェントをインストールします。ユーザー ID エージェントをホストするシステムが、モニター対象のサーバーと同じドメインのメンバーであることを確認します。

STEP 3 | メンバー サーバーからユーザー マッピング情報を収集するようにユーザー ID エージェントを設定します。

1. Windows ベースのユーザー ID エージェントを開始します。
2. **User Identification (ユーザー ID)** > **Discovery (検出)** の順に選択し、ドメイン コントローラからイベントを受信する各メンバー サーバーで以下の手順を実行します。
   1. Servers [サーバー]セクションで、**Add** [追加]をクリックし、**Name** [名前]にメンバー サーバーを識別するための名前を入力します。
   2. **Server Address** [サーバー アドレス]フィールドに、メンバー サーバーの FQDN または IP アドレスを入力します。
   3. **Server Type** [サーバー タイプ]で、**Microsoft Active Directory** を選択します。
   4. **OK** をクリックしてサーバー エントリを保存します。
3. 残りの User-ID エージェント設定を行います（Configure the Windows-Based User-ID Agent for User Mapping（ユーザー マッピングのための Windows ベースの ユーザー ID エージェントの設定）を参照してください）。
4. User-ID ソースが複数の形式でユーザー名を提供する場合は、 **Primary Username** の形式を指定します。

   プライマリ ユーザー名は、ファイアウォール上のユーザーを識別するユーザー名であり、ユーザー ID ソースが提供する形式に関係なく、レポートとログでユーザーを表します。

STEP 4 | LDAP サーバー プロファイルを設定して、ファイアウォールがグループ マッピング情報を取得するためにグローバル カタログ サーバー(最大 4 個)に接続する方法を指定します。

可用性の向上のために、*2* 個以上のグローバル カタログ サーバーを使用して冗長性を確保してください。

ローカル ドメイン グループ(サブドメイン)ではなく、ユニバーサル グループのグループ マッピング情報のみを収集できます。

1. **Device (デバイス)** > **Server Profiles (サーバープロファイル)** > **LDAP** の順に選択して **Add (追加)** をクリックし、**Name (名前)** にプロファイル名を入力します。
2. Servers [サーバー]セクションで、グローバル カタログごとに、**Add** (追加)をクリックしてサーバーの **Name** [名前]、IP アドレス(**LDAP Server** [LDAP サーバー])、および **Port** [ポート]を入力します。プレーンテキストまたは Start Transport Layer Security (Start TLS)接続の場合、**Port**（ポート）に 3268 を使用します。LDAP over SSL 接続の場合、**Port** [ポート]に 3269 を使用します。接続で Start TLS または LDAP over SSL を使用する場合、**Require SSL/TLS secured connection** [SSL/TLS で保護された接続を要求]チェック ボックスをオンにします。
3. **Base DN** [ベース DN]フィールドに、ファイアウォールがグループ マッピング情報の検索を開始する、グローバル カタログ サーバーのポイントの識別名(DN)を入力します(例: `DC=acbdomain,DC=com`)。
4. **Type**（タイプ）として、**active-directory** を選択します。

STEP 5 | LDAP サーバー プロファイルを設定して、ファイアウォールがドメイン マッピング情報を格納するサーバー(最大 4 個)に接続する方法を指定します。

ユーザー ID は、この情報を使用して、DNS ドメイン名を NetBIOS ドメイン名にマッピングします。このマッピングにより、ポリシー ルールで一貫性のあるドメイン/ユーザー名の参照を行うことができます。

可用性の向上のために、*2* 個以上のサーバーを使用して冗長性を確保してください。

この手順は、以下のフィールドを除き、前のステップでグローバル カタログ用に作成した LDAP サーバー プロファイルの場合と同じです。

- **LDAP Server** [LDAP サーバー] – ドメイン マッピング情報を格納するドメイン コントローラの IP アドレスを入力します。
- **Port** [ポート]– プレーンテキストまたは Start TLS 接続の場合、**Port** [ポート]に 389 を使用します。LDAP over SSL 接続の場合、**Port** [ポート]に 636を使用します。接続で Start TLS または LDAP over SSL を使用する場合、**Require SSL/TLS secured connection** [SSL/TLS で保護された接続を要求]チェック ボックスをオンにします。
- **Base DN** [ベース DN] – ファイアウォールがドメイン マッピング情報の検索を開始する、ドメイン コントローラのポイントの DN を選択します。値は、以下の文字列で始まる必要があります。`cn=partitions,cn=configuration` (for example, `cn=partitions,cn=configuration,DC=acbdomain,DC=com`).

STEP 6 | 作成した各 LDAP サーバー プロファイルのグループ マッピング設定を作成します。

1. **Device (デバイス)** > **User Identification (ユーザー ID)** > **Group Mapping Settings (グループ マッピング設定)**の順に選択します。
2. **Add** [追加]をクリックして、グループ マッピング設定を識別する **Name** [名前]を入力します。
3. **LDAP Server Profile** [LDAP サーバー プロファイル]を選択し、**Enabled** [有効]チェックボックスがオンになっていることを確認します。

   グローバル カタログおよびドメイン マッピング サーバーで、セキュリティ ルールで必要な数よりも多くのグループを参照している場合、***Group Include List*** *[許可リストのグループ化]*や ***Custom Group*** *[カスタム グループ]*リストを設定して、ユーザー *ID* がマッピングを実行するグループを制限します。
4. **OK**、**Commit (コミット)** の順にクリックします。

HTTP ヘッダーにユーザー名の挿入

Palo Alto Networks ファイアウォールを使用してセカンダリ エンフォースメント アプライアンスを設定し、ユーザーベースのポリシーを実施する場合、セカンダリ アプライアンスにファイアウォールからの IP アドレスからユーザー名へのマッピングがない場合があります。ユーザー情報をダウンストリーム アプライアンスに送信するには、プロキシなどの追加のアプライアンスの展開が必要になるか、ユーザーのエクスペリエンスに悪影響を及ぼすことがあります（たとえば、ユーザーが複数回ログインする必要がある）。HTTP ヘッダーでユーザーの ID を共有することにより、ユーザーのエクスペリエンスに悪影響を与えたり、追加のインフラストラクチャを展開したりすることなく、ユーザーベースのポリシーを適用できます。

この機能を設定するときは、URL プロファイルをセキュリティ ポリシーに適用し、変更のあるファイアウォールをコミットします。

1. 送信元ユーザーのグループ マッピングで、プライマリユーザー名のフォーマットでユーザーとドメインの値を入力します。
2. Base64 を使用してこの情報をエンコードします。
3. ペイロードに Base64 でエンコードされたヘッダーを追加します。
4. トラフィックをダウンストリーム アプライアンスにルーティングします。

ユーザーが特定のドメインにアクセスするときにのみユーザー名とドメインを含める場合は、ドメインリストを設定し、リスト内のドメインが HTTP 要求のホスト ヘッダーと一致する場合にのみファイアウォールがヘッダーを挿入します。

ユーザー情報をダウンストリーム アプライアンスと共有するには、まずユーザー ID を有効にし、グループマッピングを設定する必要があります。

ヘッダーにユーザー名とドメインを含めるには、*firewall* でユーザーの *IP* アドレスからユーザー名へのマッピングが必要です。ユーザーがマップされていない場合、*firewall* はヘッダー内のドメインとユーザー名の両方に対して *Base64* エンコードで *unknown* を挿入します。

HTTPS トラフィックのヘッダーにユーザー名とドメインを含めるには、まず decryption プロファイル を作成して HTTPS トラフィックを復号化する必要があります。

この機能は、転送プロキシ復号化トラフィックをサポートします。

STEP 1 | **URL Filtering Profile**（**URL**フィルタリング プロファイル）をCreate（作成）または編集します。

URL フィルタリング プロファイルのアクションがドメインのブロックである場合、ファイアウォールはヘッダーを挿入しません。

STEP 2 | 事前定義済みタイプを使用した HTTP ヘッダー挿入エントリを作成します。

プロファイルごとに最大 5 つのヘッダーを定義できます。

STEP 3 | ヘッダー **Type**（タイプ）として **Dynamic Fields**（ダイナミック フィールド）を選択します。

STEP 4 | ヘッダーを挿入する場所に**Domains**（ドメイン）を**Add**（追加）します。ユーザーがリスト内のドメインにアクセスすると、ファイアウォールは指定されたヘッダーを挿入します。

STEP 5 | 新しい **Header**（ヘッダー）を**Add**（追加）するか、 **X-Authenticated-User** を選択し編集します。

STEP 6 | ヘッダーの **Value**（値）フォーマット（（**$ domain**）****（**$ user**）または **WinNT**：**//**（**$ domain**）**/**（**$ user**）のいずれか）を選択するか、 （**$ domain**）および（**$ user**）ダイナミック トークンを使用して独自のフォーマットを入力します（たとえば、UserPrincipalNameの（**$ user**）**@**（**$ domain**））。

値ごとに同じダイナミック トークン（（***$ user***）または（***$ domain***））を *2* 回以上使用しないでください。

各値は最大512文字です。ファイアウォールは、グループ マッピング プロファイルのプライマリユーザー名を使用して、（**$ user**）および（**$ domain**）のダイナミック トークンを入力します。以下に例を示します。

- プライマリユーザー名が sAMAccountName の場合、（**$ user**）の値は sAMAccountName であり、（**$ domain**）の値は NetBios ドメイン名です。
- プライマリユーザー名が UserPrincipalName の場合、（**$ user**）はユーザーアカウント名（プレフィックス）、（**$ domain**）はDomain Name System（DNS）名です。

STEP 7 | （任意）ヘッダーを挿入するためのロギングを使用可能にするには、 Log（ログ）を選択します。

STEP 8 | HTTP または HTTP トラフィックのセキュリティ ポリシー ルールに URL フィルタリング プロファイルを適用します。

STEP 9 | **OK** を 2 回選択して、HTTP ヘッダー設定を確認します。

STEP 10 | 変更をコミットします。

STEP 11 | ファイアウォールの HTTP ヘッダーにユーザー名とドメインが含まれていることを確認します。

- **show user user-ids all** コマンドを使用して、グループマッピングが正しいことを確認します。
- **show counter global name ctd_header_insert** コマンドを使用して、ファイアウォールによって挿入された HTTP ヘッダーの数を表示します。
- ステップ 7 でログを設定した場合、挿入された Base64 エンコードされたペイロードのログを確認します（たとえば、**corpexample \ testuser** はログに **Y29ycGV4YW1wbGVcdGVzdHVzZXI =** として表示されます）。

データおよび認証タイムスタンプの再配信

大規模なネットワークでは、すべてのファイアウォールがマッピング情報ソースに直にクエリを送るよう設定する代わりに、再配信を通じて一部のファイアウォールだけがマッピング情報を収集するよう設定することで、リソースを合理的に使用できます。

Terminal Server (TS) エージェント以外の方法で収集したユーザー マッピング情報を再配信できます。グループ マッピングや HIP マッチ情報は再配信できません。

Panorama を使用してファイアウォールを管理し、ファイアウォールログを集約する場合、*Panorama* を に使用して User-ID 再配布 を管理できます。*Panorama*を活用することは、ファイアウォール間に追加の接続を作成してユーザー*ID*情報を再配布するよりも簡単なソリューションです。

認証ポリシーの設定を行う場合、ファイアウォールは、ユーザーがアプリケーションおよびサービスにアクセスするために認証を行う際に生成される認証タイムスタンプも再配信する必要があります。ファイアウォールはこのタイムスタンプを使用し、認証ポリシールールのタイムアウトを評価します。タイムアウトは、認証を成功させたユーザーが、タイムアウトの期間中に後で再度認証を行うことなくサービスおよびアプリケーションをリクエストできるようにします。タイムスタンプを再配信することで、ネットワーク内のすべてのファイアウォールに一貫したタイムアウトを適用できます。

ファイアウォールは、一度の再配信フローの一環としてデータおよび認証タイムスタンプを共有します。各情報タイプ毎に個別に再配信を設定する必要はありません。

- データ再配信のためのファイアウォール展開
- データの再配信を設定する

データ再配信のためのファイアウォール展開

大規模なネットワークでは、すべてのファイアウォールがデータ送信元に直にクエリを送るよう設定する代わりに、再配信を通じて一部のファイアウォールだけがデータを収集するよう設定することで、リソースを合理的に使用できます。データの再配信では、指定した種類の情報のみを、選択したデバイスのみに、きめ細かく再配信できます。サブネットと範囲を使用して、IP

ユーザー マッピングまたは IP タグ マッピングをフィルタリングし、ファイアウォールがポリシー適用に必要なマッピングのみを収集するようにもできます。

データの再配信は、単方向 (エージェントがクライアントにデータを提供)、または双方向にして、エージェントとクライアントの両方が同時にデータを送受信するようにできます。

データを再配信するには、以下のアーキテクチャ タイプを使用できます。

- 単一リージョンのハブ アンド スポーク アーキテクチャ:

  ファイアウォール間でデータを再配信するには、ベストプラクティスとしてハブ アンド スポーク アーキテクチャを使用します。この設定では、ハブ ファイアウォールは、Windows User-IDエージェント、Syslogサーバ、ドメイン コントローラ、その他のファイアウォールなどの送信元からデータを収集します。ハブ ファイアウォールからデータを収集するように、再配信クライアント ファイアウォールを設定します。

  たとえば、ハブ (復元性を考慮し、VM-50 のペアで構成する) は、ユーザー マッピングの User-ID 送信元に接続できます。ユーザー マッピングを使用してポリシーを適用するクライアント ファイアウォールが、データを受信するためハブに接続すると、ハブはユーザー マッピングを再配信できるようになります。

- 複数のリージョン向けのマルチハブおよびスポークアーキテクチャ:

  複数のリージョンにファイアウォールを導入していて、すべてのリージョンのファイアウォールにデータを配信し、ユーザーのログイン場所に関係なくポリシーを一貫して適用できるようにしたい場合は、複数のリージョンにマルチ ハブ アンド スポーク アーキテクチャを使用できます。

  まず、各リージョンのファイアウォールを、送信元からデータを収集するように設定します。このファイアウォールは、再配信のローカル ハブとして機能します。このファイアウォールは、そのリージョン内のすべての送信元からデータを収集して、クライアント ファイアウォールに再配信できるようにします。次に、クライアント ファイアウォールを、そのリージョンおよび他のすべてのリージョンの再配信ハブに接続するように設定して、クライアント ファイアウォールが全ハブからの全データを持つようにします。

  ベストプラクティスとして、ファイアウォールがデータの送受信両方を行う必要がある場合は、リージョン内で双方向の再配信を有効にします。たとえば、ファイアウォールが、リモート ユーザーの GlobalProtectゲートウェイとして、またローカル ユーザーのブランチ ファイアウォールとして機能している場合、ファイアウォールは、リモート ユーザー用に収集したユーザー マッピングをハブ ファイアウォールに送信し、ハブ ファイアウォールのローカル ユーザーのユーザー マッピングを受信する必要があります。

- 階層アーキテクチャ:

  データの再配信に、階層アーキテクチャを使用することもできます。たとえば、User-ID 情報などのデータを再配信するには、再配信シーケンスをレイヤーに編成します。各レイヤーには1つ以上のファイアウォールがあります。最下部レイヤーでは、ファイアウォールで実行されている PAN-OS 統合 User-ID エージェントと Windows サーバーで実行されている Windows ベース User-ID は IP アドレスをユーザー名にマッピングします。上位レイヤーは、下位レイヤーの最大 100 個の再配信ポイントからマッピング情報および認証タイムスタンプを受け取るファイアウォールを持っています。最上部レイヤー ファイアウォールはすべてのレイヤーからのマッピングおよびタイムスタンプを集約します。この展開により、最上部レイヤー ファイアウォールのすべてのユーザーにポリシーを設定し、下位レイヤー ファイア

ウォールが担当する、対応するドメインのユーザー サブセットに地域または機能別ポリシーを設定するオプションが提供されます。

このシナリオでは、ファイアウォールの3つのレイヤーが、マッピングとタイムスタンプをローカル オフィスからリージョナル オフィスに再配信してから、グローバル データセンターに再配信します。すべての情報を集約するデータセンター ファイアウォールは、それを他のデータセンター ファイアウォールと共有し、ネットワーク全体のユーザーに対してすべてのファイアウォールがポリシーを適用し、レポートを生成できるようにします。最下部レイヤー ファイアウォールのみが、User-ID エージェントを使用してクエリによってディレクトリ サーバーを求めます。

User-ID がクエリで求める情報ソースは、シーケンスにおいて最大 10 個のホップに加算しません。しかし、 マッピング情報をファイアウォールに送信する Windows ベース User-ID エージェントはカウントしません。またこの例では、最上部レイヤーは 2 つのホップを持っています。一方は 1 個のデータセンター ファイアウォールで情報を集約します。もう一方は情報を他のデータセンター ファイアウォールと共有します。

データの再配信を設定する

データの再配信の設定前：

- 再配信アーキテクチャのプランニング考慮すべきファクター：
  - どのファイアウォールがすべてのデータ タイプにポリシーを適用するのか？どのファイアウォールがデータのサブセットのために地域または機能別ポリシーを適用するのか？
  - すべてのデータ情報を集積するために再配信シーケンスが必要とするホップ数は？ユーザー マッピングの最大許容ホップ数は10で、IP アドレスからユーザー名へのマッピングおよび IP アドレスからタグへのマッピングの最大許容ホップ数は1です。
  - ユーザーマッピングの情報ソースをクエリするファイアウォールの数を最小化する方法は？クエリを行うファイアウォールの数が少なければそれだけファイアウォールとソースのプロセス負荷も低下します。
- 再配布エージェントがクライアントに再配布するデータを取得するデータ・ソースを構成します:
  - PAN-OS 統合ユーザーIDエージェントからのユーザー・マッピング または Windows ベースの User-ID エージェント
  - IP address-to-tag マッピング 動的アドレス・グループ
  - username-to-tag mappings for dynamic user groups
  - GlobalProtect for HIP-based Policy Enforcement
  - data for device quarantine (Panorama only)
- 認証ポリシーの設定を行います。

データ再配信は以下で構成されます：

- 情報を提供する再配信エージェント
- 情報を受信する再配信クライアント

データ再配信シーケンスのファイアウォールで以下の各作業を行います。

STEP 1 | 再配信クライアント ファイアウォール上で、ファイアウォール、Panorama、または Windows User-ID エージェントをデータ再配信エージェントとして設定します。

1. **Device (デバイス) > Data Redistribution (データ再配布) > Agents (エージェント)** を選択します。
2. 再配信エージェントを **Add (追加)** して、**Name (名前)** を入力します。
3. エージェントが **Enabled (有効)** になっていることを確認します。

STEP 2 | その **Serial Number (シリアルナンバー)** または **Host and Port (ホストとポート)** を使用するエージェントを追加します。

- シリアルナンバーを使用するエージェントを追加するには、再配信エージェントとして使用するファイアウォールの **Serial Number (シリアルナンバー)** を選択します。
- ホストとポートの情報を使用してエージェントを追加するには:

1. **Host** の情報を入力します。
2. ホストが **LDAP Proxy** であるかどうかを選択します。
3. **Port** を入力します (デフォルトは 5007、範囲は 1 ~ 65535)。
4. (複数の仮想システムのみ) **Collector Name** を入力して、再配布エージェントとして使用する仮想システムを特定します。
5. (複数の仮想システムのみ) 再配布エージェントとして使用する仮想システムの **Collector Pre-Shared Key** を入力して確認します。

STEP 3 | 再配信するためのエージェントの**Data Type (データ タイプ)**を1つ以上選択します。

- **IP** ユーザー マッピング—ユーザー ID の IP アドレスとユーザ名のマッピング。
- **IP Tags (IP タグ)** —ダイナミック アドレス グループの IP アドレスとタグのマッピング。
- **User Tags (ユーザー タグ)** —ダイナミック ユーザー グループのユーザー名とタグのマッピング。
- **HIP**—HIP オブジェクトとプロファイルを含むGlobalProtect の Host information profile (ホスト情報プロファイル; HIP) データ。
- **Quarantine List (隔離リスト)**—GlobalProtect が隔離対象として識別するデバイス。

STEP 4 | (複数の仮想システム専用) データを再配信できるコレクタとして仮想システムを設定します。

ファイアウォールがデータを受信しても再配信しない場合は、このステップをスキップしてください。

仮想システム内の情報を異なるファイアウォールや同一のファイアウォールに再配信できます。いずれの場合も、仮想システムは再配信シーケンスで*1*つのホップとしてカウントされます。

1. **Device (デバイス) > Data Redistribution (データ再配布) > Collector Settings (コレクタ設定)** を選択します。
2. **Data Redistribution Agent Setup (データ再配信エージェントのセットアップ)** を編集します。
3. このファイアウォールまたは仮想システムを User-ID エージェントとして識別する **Collector Name (コレクタ名)** および **Pre-Shared Key (事前共有鍵)** を入力します。
4. **OK** をクリックして変更内容を保存します。

STEP 5 | (推奨オプション) データの再配信に含めるネットワークと、データの再配信から除外するネットワークを設定します。

IP アドレスからタグへのマッピングまたは IP アドレスからユーザー名へのマッピングのいずれかを再配信する場合、ネットワークとサブネットワークを含めたり除外したりできます。

ベスト プラクティスとして、エージェントが内部リソースとのみ通信するように、含めるネットワークと除外するネットワークを常に指定してください。

1. **Device (デバイス) > Data Redistribution (データ再配信) > Include/Exclude Networks (ネットワークの追加/除外)**を選択します。
2. エントリを **Add (追加)** し、**Name (名前)**を入力します。
3. エントリが**Enabled**（有効）であることを確認します。
4. エントリを **Include (追加)** するか **Exclude (除外)** するか選択します。
5. エントリの **Network Address (ネットワーク アドレス)** を入力します。
6. **OK** をクリックします。

STEP 6 | ファイアウォールが他のファイアウォールに User-ID 情報をクエリする際に使用するサービスルートを設定します。

ファイアウォールが Windows ベースのユーザー ID エージェントからユーザーマッピング情報のみを受信する場合、または、他のファイアウォールからではなく情報ソース（ディレク

トリサーバーなど）からのみユーザーマッピング情報を直接受信する場合は、この手順をスキップしてください。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）を選択します。
2. （複数の仮想システムを有するファイアウォールのみ）**Global (**グローバル**)**（ファイアウォール全体のサービスルート用）または **Virtual Systems (**仮想システム**)**（仮想システム専用サービスルート用）を選択し、サービス ルートを設定します。
3. **Service Route Configuration (**サービスルート設定**)** をクリックし、**Customize (**カスタマイズ**)** を選択し、ネットワーク プロトコルに応じて **IPv4** あるいは **IPv6** を選択します。お使いのネットワークが両方を使っているのなら、両方のプロトコルのサービスルートを設定します。
4. **UID Agent**[UDI エージェント] を選択し、 **Source Interface**[ソースインターフェイス] と **Source Address**[ソースアドレス]を選択します。
5. **OK**[OK] を 2 度クリックすると、サービスルートの設定が保存されます。

STEP 7 | 他のファイアウォールから再配信するデータをクエリされた際にファイアウォールが応答できるようにします。

ファイアウォールがデータを受信しても再配信しない場合は、このステップをスキップしてください。

User-ID サービスを有効にしたインターフェイス管理プロファイルの設定を行い、そのプロファイルをファイアウォールのインターフェイスに割り当てます。

STEP 8 | (推奨オプション) エンタープライズ PKI からのカスタム証明書を使用して、再配信クライアントから再配信エージェントへの一意の信頼チェーンを確立します。

1. 再配信クライアント ファイアウォール上で、送信接続に使用するカスタム SSL 証明書プロファイル を作成します。
2. **Device (**デバイス**) > Setup (**セットアップ**) > Management (**管理**) > Secure Communication Settings (**セキュア通信の設定**)** を選択します。
3. 設定を **Edit (**編集**)** します。
4. **Customize Secure Server Communication**（セキュリティで保護されたサーバー通信のカスタマイズ） オプションを選択します。
5. サブステップ1で作成された**Certificate Profile (**証明書プロファイル**)**を選択します。
6. **OK** をクリックします。
7. **Data Redistribution (**データ再配信**)** の**Customize Communication (**通信のカスタマイズ**)** を行います。
8. 変更を **Commit (**コミット**)** します。
9. 次の CLI コマンドを入力して、証明書プロファイル (SSL 構成) が カスタム証明書 を使用していることを確認します: 再配布エージェントの状態 ***<agent-name>*** (*<agent-name>* は再配布エージェントまたは User-ID エージェントの名前です)。

STEP 9 | (推奨オプション) エンタープライズ PKI からのカスタム証明書を使用して、再配信エージェントから再配信クライアントへの一意の信頼チェーンを確立します。

1. 再配信エージェント ファイアウォールで、受信接続に使用するファイアウォールのカスタム SSL / TLS サービス プロファイルを作成します。
2. **Device (デバイス) > Setup (セットアップ) > Management (管理) > Secure Communication Settings (セキュア通信の設定)** を選択します。
3. 設定を **Edit (編集)** します。
4. **Customize Secure Server Communication**（セキュリティで保護されたサーバー通信のカスタマイズ） オプションを選択します。
5. ステップ1で作成した**SSL/TLS Service Profile (SSL/TLS** サービス プロファイル**)** を選択します。
6. **OK** をクリックします。
7. 変更を **Commit (コミット)**します。
8. 証明書プロファイル (`SSL config`) がカスタム証明書を使用していることを確認するには、次の CLI コマンドを入力します: **`show redistribution service status`**。

STEP 10 | エージェントがクライアントにデータを正しく再配信していることを確認します。

1. エージェントの統計 (**Device (デバイス) > Data Redistribution (データ再配信) > Agents (エージェント)**)を表示し 、**Status (ステータス)**を選択すると、クライアントのファイアウォールが受信したマッピングの数など、再配信エージェントのアクティビティの概要を表示されます。
2. **Connected (接続済み)** ステータスが **yes** であることを確認します。
3. エージェント上で、再配信のステータスを確認するには、CLI にアクセスし、次の CLI コマンドを入力します: **`show redistribution service status`**。
4. エージェント上で、再配信クライアントを表示するには、次の CLI コマンドを入力します: **`show redistribution service client all`**。
5. クライアント上で、再配信のステータスを確認するには、次の CLI コマンドを入力します: **`show redistribution service client all`**。
6. ファイアウォールが再配信エージェントからマッピングを受信したことを検証するには、User-ID ログ (**Monitor (監視) > Logs (ログ) > User-ID**) で**Source Name (ソース名)** を確認します。
7. クライアント上で、クライアント ファイアウォールがデータを受信していることを確認するには、IP-Tag ログ (**Monitor(監視) > Logs(ログ) > IP-Tag**) を表示します。
8. クライアント上で、次の CLI コマンドを入力し、ファイアウォールがマッピングを受信する`From`（送信者）が `REDIST`であることを確認します： **`show user ip-user-mapping all`**。

STEP 11 | (オプション) データの再配信のトラブルシューティングを行うには、トレースルートオプションを有効にします。

traceroute オプションを有効にすると、データを受け取る firewall は、データが通過したすべての firewall IP アドレスのリストである `<route>` フィールドにその IP アドレスを追加します。このオプションでは、再配信ルート内のすべての PAN-OS デバイスが PAN-OS バージョ

ン10.0を使用する必要があります。再配信ルート内の PAN-OS デバイスが PAN-OS 9.1.x またはそれ以前のバージョンを使用する場合、トレースルート情報はそのデバイスで終了します。

1. ソースが発信元である再配布エージェントで、次の CLI コマンドを入力します: **debug user-id test cp-login traceroute yes ip-address *<ip-address>* user *<username>*** (ここで、***<ip-address>*** は検証する IP address-to-username マッピングの IP アドレス、***<username>*** は検証する IP address-to-username マッピングのユーザー名です。
2. トレースルートを設定したファイアウォールのクライアントで、次の CLI コマンドを入力することで、ファイアウォールがデータを再配信することを検証します： **show user ip-user-mapping all**。

   ファイアウォールは、マッピング作成のタイムスタンプ(SeqNumber)と、ユーザーが GlobalProtect (GP User) を有するかどうかを表示します。

```
admin > show user ip-user-mapping-mp ip 192.0.2.0 IP
 address:192.0.2.0 (vsys1) ユーザ: jimdoe 差出人:REDIST タ
イムアウト:889s 作成日:11秒前 起源:198.51.100.0 シーケンス番
号:15895329682-67831262 GP User:ローカルHIPなし:No Route Node
 0:198.51.100.0 (vsys1) Route Node 1:198.51.100.1 (vsys1)
```

仮想システム間でのユーザー ID マッピングの共有

複数の仮想システムがある場合に User-ID ™ ソース構成を簡素化するには、単一の 仮想システム 上で、IP アドレス対ユーザー名マッピングおよびユーザー名とグループ間のマッピングをファイアウォール上の他のすべての仮想システムと共有するように User-ID ソースを構成します。

単一の仮想システムを *User-ID hub* として構成すると、ユーザーがアクセスしようとしているリソースに基づいてトラフィックが複数の仮想システムを通過する場合 (たとえば、学生が別の仮想システムによって管理される別の部門にアクセスするアカデミック ネットワーキング環境など) で、複数の仮想システム上でソースを構成する必要がなくなり、ユーザーマッピングが簡素化されます。

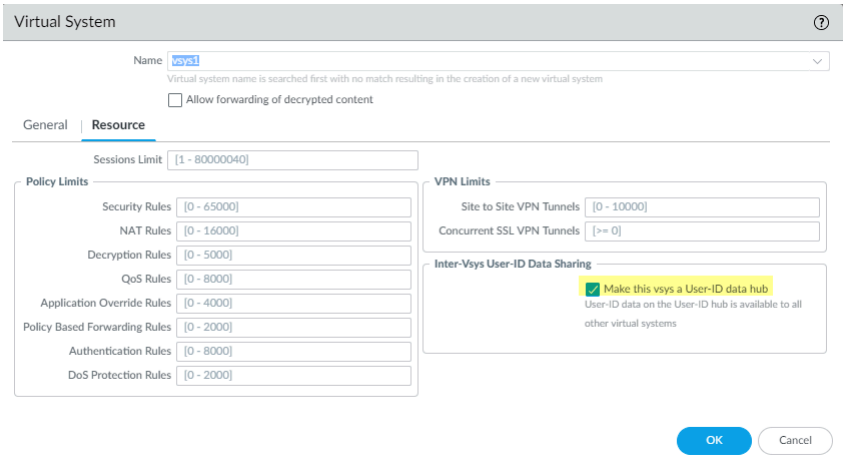
ユーザーまたはグループをマップするために、ファイアウォールはローカル仮想システムのマッピングテーブルを使用し、そのユーザーまたはグループにポリシーを適用します。ファイアウォールが、そのユーザーのトラフィックが発生した仮想システム上のユーザーまたはグループのマッピングを検出しない場合、ファイアウォールはハブに照会して、そのグループの IP アドレスからユーザー名への情報を取得します。ファイアウォールがユーザー ID ハブとローカル仮想システムの両方でマッピングを見つけると、ファイアウォールはローカルで学習したマッピングを使用します。ローカル ファイアウォール上のマッピングが仮想システム ハブのマッピングと異なる場合、ファイアウォールはローカル マッピングを使用します。

User-ID ハブを構成した後、virtual system (仮想システム - vsys)がユーザーベースのポリシー適用のためにユーザーを識別する必要がある場合、またはログあるいはレポートにユーザー名を表示する必要があり、送信元がローカルで使用できない場合、virtual system (仮想システム - vsys)は User-ID ハブでマッピングテーブルを使用することができます。ハブを選択すると、ファイアウォールは他のvirtual system (仮想システム - vsys)でマッピングを保持するため、ハブ上の

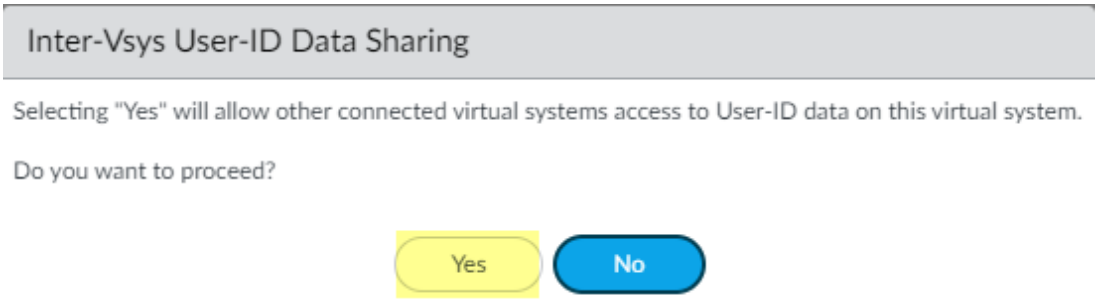
ユーザー ID ソースを統合することをお勧めします。ただし、特定のソースからのマッピングを共有したくない場合は、個々の仮想システムを構成して、ユーザーまたはグループのマッピングを実行できます。

STEP 1 | 仮想システム をユーザー ID ハブとして割り当てます。

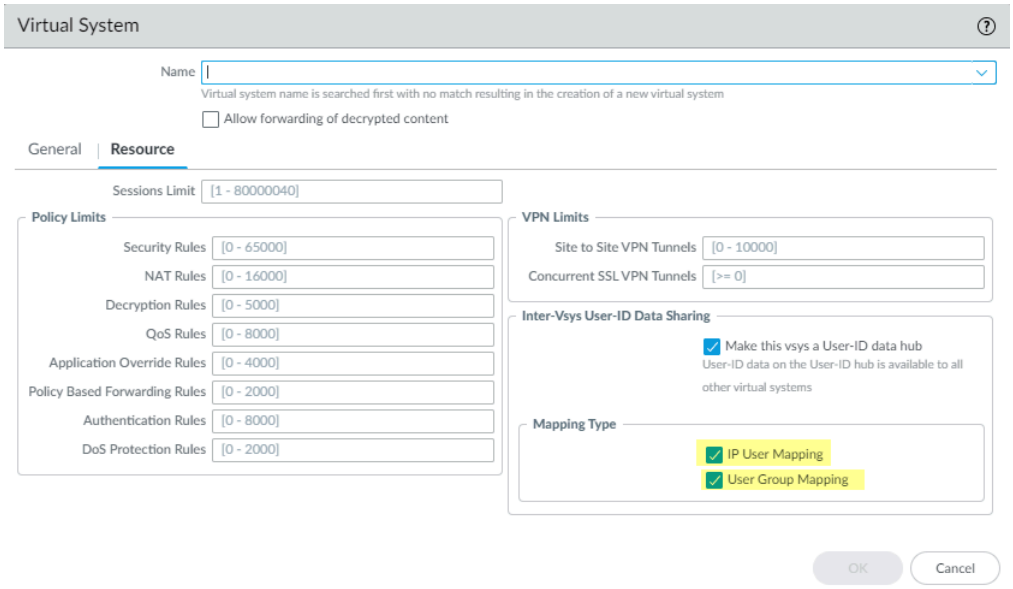
1. **Device (デバイス)** > **Virtual Systems (仮想システム)** を選択してから、ユーザー ID ソースを統合したvirtual system (仮想システム - vsys)仮想システムを選択します。
2. **Resource(リソース)** タブで、**Make this vsys a User-ID data hub (この vsys を User-ID データ ハブにする)** を行い、**Yes (はい)** をクリックし確認します。**[OK]** をクリックします。



STEP 2 | **Yes** をクリックして確定します。



STEP 3 | 共有する マッピングの種類 を選択し、**OK** をクリックします。



- **IP** ユーザー マッピング– IP アドレスとユーザー名のマッピング情報を他の仮想システムと共有します。
- ユーザー グループ マッピング– グループ マッピング情報を他の仮想システムと共有します。

マッピングタイプを少なくとも *1* つ選択する必要があります。

STEP 4 | ユーザー ID ソースを統合し、それらをユーザー ID ハブとして使用する仮想システムに移行します。

これにより、操作を簡単にするためのユーザー ID 構成が統合されます。サーバーをモニターし、他の仮想システムによって以前にモニターされていたエージェントに接続するようにハブを構成することにより、ハブは各仮想システムに個別に収集させるのではなく、ユーザーマッピング情報を収集します。特定のvirtual system (仮想システム - vsys)からのマッピングを共有したくない場合は、ハブとして使用されないvirtual system (仮想システム - vsys)上でそれらのマッピングを設定します。

仮想システムとファイアウォール間でプライマリユーザ名に同じ形式を使用します。

1. 不要または古くなっているソースを削除します。
2. Windows ベースあるいは 統合エージェント用のすべての設定と、および XML API を使用してユーザーマッピングを送信するすべてのソースを特定し、User-ID ハブとして使用したいvirtual system (仮想システム - vsys)にコピーします。

   ハブでは、現在仮想システムに構成されている任意のユーザー *ID* ソースを構成できます。ただし、ターミナル サーバー エージェントからの *IP* アドレスとポートからユーザー名へのマッピング情報は、*User-ID* ハブと接続されている仮想システム間では共有されません。

3. ユーザー ID がマッピングに含める、あるいは除外すべきサブネットワークを指定します。
4. **Ignore User List (**無視ユーザーリスト**)** を定義します。
5. 他のすべての仮想システムで、ユーザー ID ハブにあるソースをすべて削除します。

STEP 5 | 変更を **Commit (**コミット**)** して、ユーザー ID ハブを有効にし、統合されたソースに対するマッピングの収集を開始します。

STEP 6 | User-ID ハブがユーザーとグループをマッピング中であることを確認します。

1. **`show user ip-user-mapping all`** コマンドを使用して、IPアドレス - ユーザー名間マッピング、およびどのvirtual system (仮想システム - vsys)がマッピングを提供しているかを表示します。
2. **`show user user-id-agent statistics`** コマンドを使用して、どの仮想システムがユーザー ID ハブとして機能しているかを表示します。
3. 次の CLI コマンドを使用して、ハブがグループ マッピングを共有されていることを確認します。
   - `show user group-mapping statistics`
   - `show user group-mapping state all`
   - `show user group list`
   - `show user group name` *<group-name>*

App-ID

ネットワーク上のアプリケーションを安全に有効にするため、Palo Alto Networks の次世代ファイアウォールは、App-ID と URL フィルタリングによってアプリケーションと Web の両方の視点から、法律、規制、生産性、およびリソース使用に関するあらゆるリスクから保護します。

App-ID によってネットワーク上のアプリケーションに対する可視性が高まるため、アプリケーションの仕組みを知り、動作特性や相対リスクについて理解できます。このアプリケーションの知識を利用して、セキュリティ ポリシー ルールを作成および適用することにより、望ましいアプリケーションを有効にして、検査およびシェーピングを行い、望ましくないアプリケーションをブロックします。トラフィックを許可するポリシー ルールを定義すると、App-ID が追加の設定なしでトラフィックの分類を開始します。

新しいアプリケーション ID と変更された App-ID は、アプリケーションと脅威コンテンツの更新 の一部としてリリースされます - アプリケーションと脅威コンテンツの更新 のベスト プラクティス に従って、アプリケーションと脅威のシグネチャをシームレスに最新の状態に保ちます。

- App-ID の概要
- 合理化された App-ID ポリシー ルール
- App-ID および HTTP/2 検査
- カスタム アプリケーションや不明なアプリケーションの管理
- 新規および変更済みの App-ID の管理
- ポリシーでのアプリケーション オブジェクトの使用
- デフォルトのポートでアプリケーションを安全に有効化
- 暗黙的サポートを使用するアプリケーション
- セキュリティ ポリシー ルールの最適化
- App-ID クラウドエンジン
- SaaS アプリ ID ポリシーの推奨事項
- アプリケーション レベル ゲートウェイ
- SIP アプリケーション レベル ゲートウェイ（ALG）を無効にする
- HTTP ヘッダーを使用して SaaS アプリケーションのアクセスを管理する
- レガシー アプリケーションのカスタム タイムアウトを維持する

App-ID の概要

App-ID は、Palo Alto Networks のファイアウォールだけで使用できる特許取得済みのトラフィック分類システムで、アプリケーションで使用されるポート、プロトコル、暗号化（SSH または SSL）、その他のあらゆる回避技術に関係なく、アプリケーションが何であるかを判断します。App-ID は、複数の分類メカニズム（アプリケーション シグネチャ、アプリケーション プロトコル デコード、ヒューリスティクス）をネットワーク トラフィック ストリームに適用して、アプリケーションを正確に識別します。

App-ID は、ネットワークを通過するアプリケーションを以下のように識別します。

- トラフィックがポリシーに一致するかどうかによって、ネットワーク上で許可されるかが確認されます。
- 次に、一意のアプリケーション プロパティおよび関連するトランザクションの特性に基づいてトラフィックがアプリケーションを識別できるようにシグネチャが適用されます。シグネチャは、アプリケーションがデフォルト ポートで使用されているか、非標準ポートを使用しているかも指定します。ポリシーによってトラフィックが許可された場合、トラフィックは次に脅威がないかをスキャンされ、アプリケーションをより詳細に識別するためにさらに分析されます。
- App-ID が暗号化 (SSL または SSH) を使用中であると判断し復号ポリシー規則が設定されている場合、セッションは復号化され、復号化されたフローにアプリケーション シグネチャが再度適用されます。
- 次に、既知のプロトコルに対するデコーダによって、追加のコンテキストベースのシグネチャが適用され、プロトコルの内部にトンネリングしている可能性のある別のアプリケーション (たとえば、HTTP 上で使用される Yahoo! インスタント メッセンジャーなど) を検出します。デコーダはトラフィックがプロトコルの仕様に準拠していることを検証し、SIP や FTP などのアプリケーションのためにダイナミック ピンホールを開くことや NAT トラバーサルをサポートします。
- 特に回避的なアプリケーションや、先進のシグネチャやプロトコル分析でも特定できないアプリケーションに対しては、ヒューリスティック分析や行動分析を行ってアプリケーションの身元を特定することが可能です。

アプリケーションが識別されると、ポリシー チェックによってアプリケーションの処理方法が決定されます。たとえば、ブロックする、許可して脅威をスキャンする、無権限のファイル転送およびデータ パターンを検査する、QoS を使用してシェーピングを行うなどの処理があります。

合理化された App-ID ポリシー ルール

一つのポリシー ルールを使用して、共通の属性を持つ幅広いアプリケーションのセットを安全に有効にします (例えば、ユーザーに Webベースのアプリケーションへの幅広いアクセスを許可したり、すべてのエンタープライズ VoIP アプリケーションを安全に有効化します)。Palo Alto Networks は、共通の属性を持つアプリケーションを調査し、動的コンテンツ更新時にタグを介してこれを配信します。これにより、以下のことを行います:

- エラーを最小限に抑え、時間を節約します。
- 新しくリリースされたアプリケーションを処理するために、自動的に更新されるポリシーを作成するのに役立ちます。
- Policy Optimizer (ポリシー オプティマイザ) を使用して、App-ID ベースのルール セットへの移行を簡素化します。

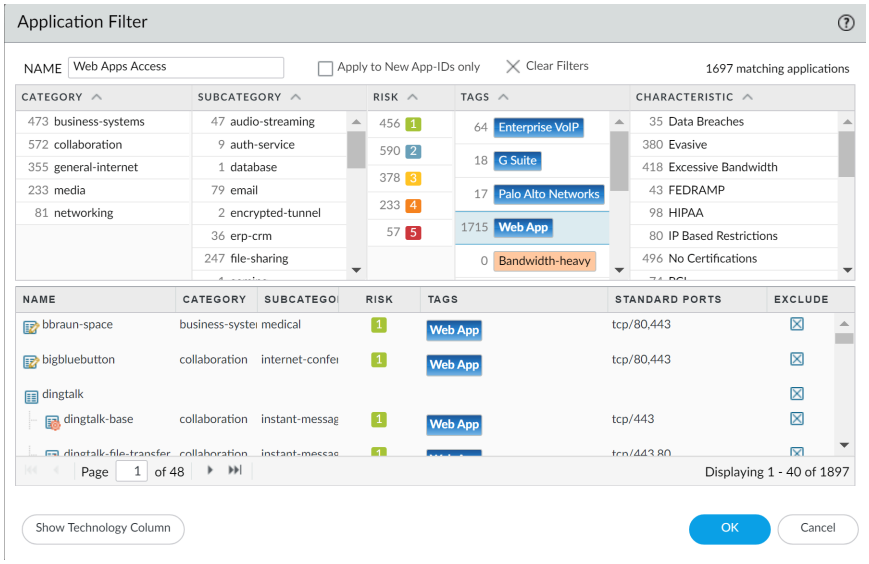
ファイアウォールは、タグベースのアプリケーション フィルタを使用して、新しいアプリケーションが追加されるたびにポリシー ルールを確認または更新しなくても、新しい App-ID と更新された App-ID を動的に適用できます。特定のタグからアプリケーションを除外することを選択した場合、新しいコンテンツ更新はそれらの除外を優先します。独自のタグを使用して、ポリシー要件に基づいてアプリケーション タイプを定義することもできます。

- タグを使用したアプリケーション フィルタの作成
- カスタム タグに基づくアプリケーション フィルタを作成する

タグを使用したアプリケーション フィルタの作成

STEP 1 | 1 つ以上のタグを使用してCreate an application filter（アプリケーション フィルタの作成）を行います。

複数のタグを選択した場合、フィルターに含まれるようにアプリケーションが両方のタグに一致する必要があります。



STEP 2 | （オプション）[除外] 列のチェック ボックスをオンにして、フィルターからタグを除外します。

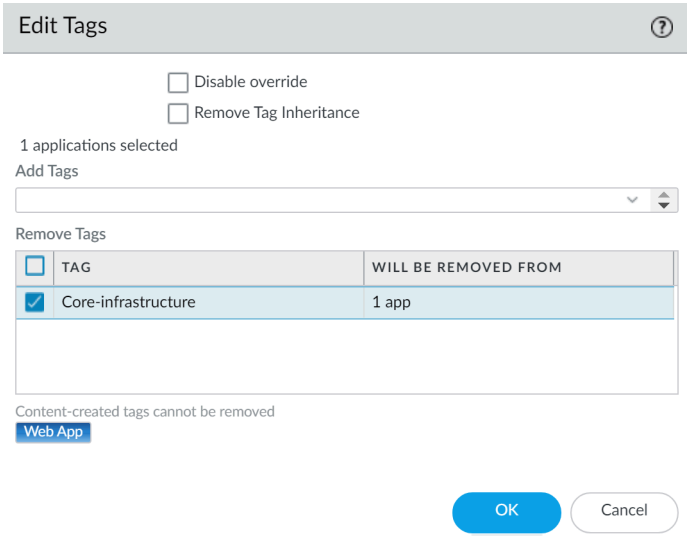
STEP 3 | Create a security policy rule（セキュリティ ポリシー ルールの作成）を行い、**Application**（アプリケーション）タブで新しいアプリケーション フィルタを**Add**（追加）します。

STEP 4 | 変更をコミットします。

カスタム タグに基づくアプリケーション フィルタを作成する

STEP 1 | タグを作成 して、App-ID に適用します。

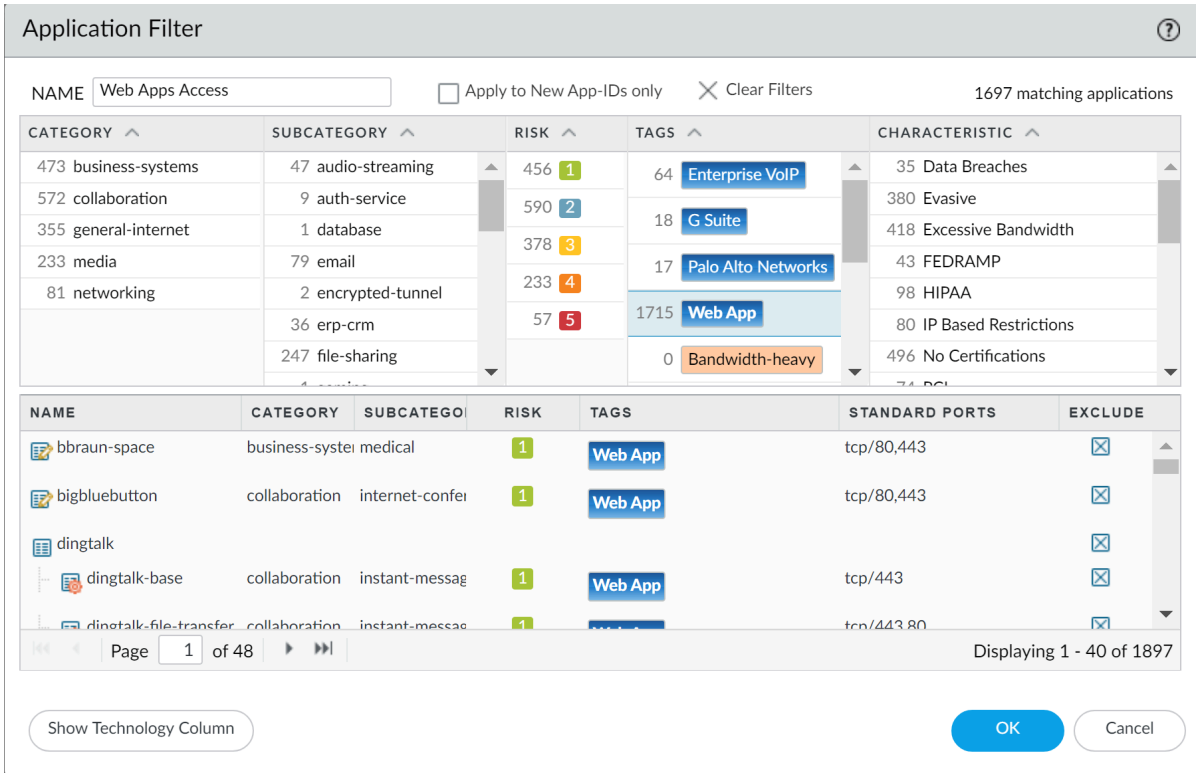
1. （任意）アプリケーションからタグを削除します。
2. アプリケーションをフィルタリングまたは検索してから、特定のアプリケーションを選択してタグを削除します。
3. **Edit Tags**（タグの編集）を行い、削除するタグを選択します。



4. **OK** をクリックします。

STEP 2 | 1 つ以上のタグを使用してCreate an application filter（アプリケーション フィルタの作成）を行います。

複数のタグを選択した場合、フィルターに含まれるようにアプリケーションが両方のタグに一致する必要があります。

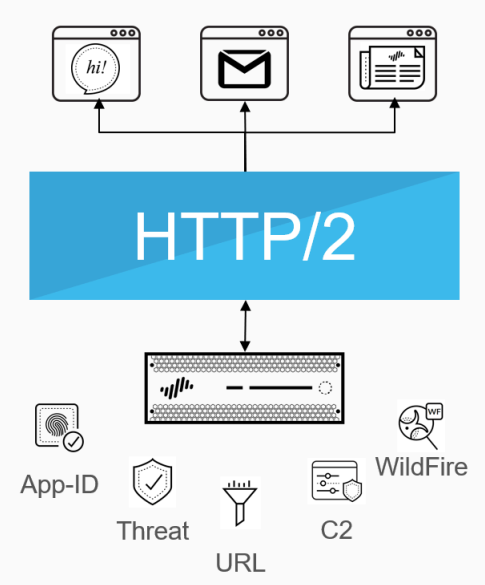


STEP 3 | Create a security policy rule（セキュリティ ポリシー ルールの作成）を行い、**Application**（アプリケーション）タブで新しいアプリケーション フィルタを**Add**（追加）します。

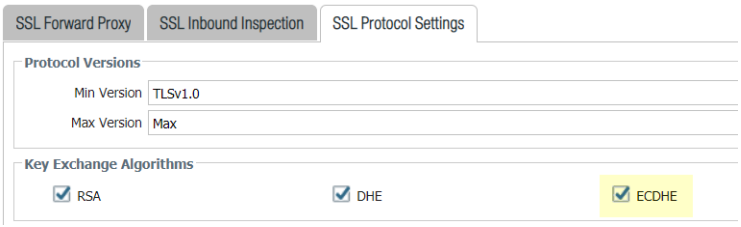
STEP 4 | 変更をコミットします。

App-ID および HTTP/2 検査

ファイアウォールで追加の設定を行うことなく、HTTP/2 を介して実行されるアプリケーションを安全に有効化できるようになっています。HTTP/2 を採用するウェブサイトが増え続けているため、ファイアウォールはストリーム バイ ストリームでセキュリティポリシー、すべての脅威検出、保護機能を適用することができます。この HTTP/2 トラフィックに対する可視性により、HTTP/2 を介したサービスを提供する WEB サーバーを保護しつつ、HTTP/2 で得られるスピードとリソースをユーザーが活用できるようになります。



SSL 復号化が有効な場合、ファイアウォールはデフォルトで HTTP/2 トラフィックを処理・検査します。HTTP/2 検査を正しく機能させるには、ファイアウォールが SSL セッションのキー交換アルゴリズムとして ECDHE (楕円曲線 Diffie-Hellman) を使用できるようにする必要があります。ECDHE はデフォルトで有効になっていますが、 **Objects (オブジェクト)** > **Decryption (復号化)** > **Decryption Profile (復号化プロファイル)** > **SSL Decryption (SSL 復号化)** > **SSL Protocol Settings (SSL プロトコル設定)**を選択してそれが有効であることを確認できます。

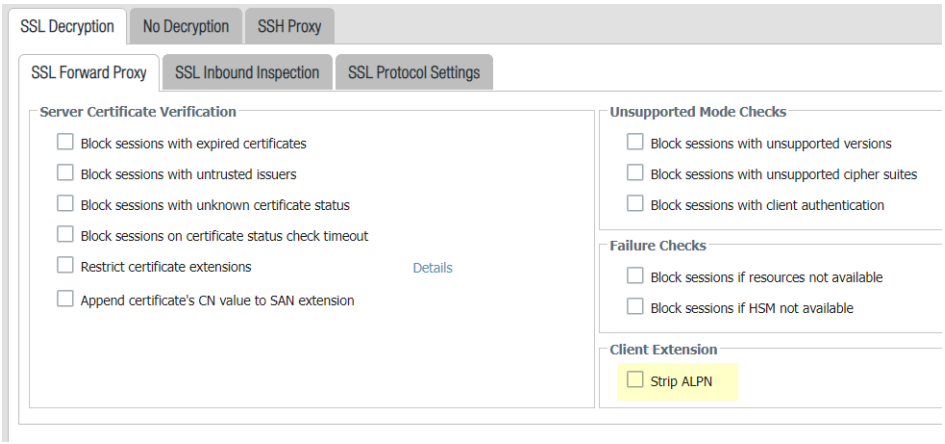


PAN-OS 10.2 で導入された *Decryption* ログが有効になっている場合は、Tunnel Content Inspection を有効にして、*HTTP/2* トラフィックのアプリ *ID* を取得する必要があります。

対象のトラフィックに対する検査、あるいはグローバルに HTTP/2 検査を無効化できます：

対象のトラフィックに対する HTTP/2 検査を無効化します。

ファイアウォールが ALPN (Application-Layer Protocol Negotiation) TLS 拡張に含まれるすべての値を削除するよう、指定する必要があります。HTTP/2 接続を保護するために ALPN が使用されています。この TLS 拡張用に指定されている値がない場合、ファイアウォールは HTTP/2 トラフィックを HTTP/1.1 にダウングレードするか、それを未知の TCP トラフィックに分類化します。



1. **Objects (**オブジェクト**)** > **Decryption (**復号化**)** > **Decryption Profile (**復号化プロファイル**)** > **SSL Decryption (SSL** 復号化**)** > **SSL Forward Proxy (SSL** 転送プロキシ**)**を選択してから、さらに **Strip ALPN (ALPN** を除去**)**を選択します。
2. 復号化プロファイルを復号化ポリシー (**Policies** > **Decryption**) にアタッチして、ポリシーに一致するトラフィックの HTTP/2 インスペクションをオフにします。
3. 変更を **Commit (**コミット**)** します。

HTTP/2 検査をグローバルに無効化します。

`set deviceconfig setting http2 enable no`。それから変更を **Commit (**コミット**)**します。ファイアウォールは HTTP/2 トラフィックを未知の TCP トラフィックに分類します。

カスタム アプリケーションや不明なアプリケーションの管理

Palo Alto Networks は、新しい App-ID シグネチャを識別するため、アプリケーションの更新を毎週提供しています。デフォルトでは、App-ID はファイアウォール上で常に有効になっており、一般的なアプリケーションを識別するために一連のシグネチャを有効にする必要はありません。通常、ACC およびトラフィック ログで不明なトラフィック（tcp、udp、non-syn-tcp）として分類されるのは、App-ID にまだ追加されていない商用のアプリケーション、ネットワーク上の内部アプリケーションやカスタム アプリケーション、または潜在的な脅威のみです。

時折、ファイアウォールは以下の理由でアプリケーションを不明であるとレポートする場合があります。

- 不完全なデータ – ハンドシェークは行われたが、タイムアウト前にデータ パケットが送信されなかった。
- 不十分なデータ – ハンドシェークの後に 1 つ以上のデータ パケットが送信されたが、アプリケーションを識別するのに十分なデータ パケットが交換されなかった。

不明なアプリケーションの処理方法には以下の選択肢があります。

- Unknown TCP、Unknown UDP、または送信元ゾーン、宛先ゾーン、および IP アドレスの組み合わせによって不明なアプリケーションを制御するセキュリティ ポリシーを作成します。
- Palo Alto Networks に App-ID を要求する – 不明なトラフィックに対して、ネットワークを通過するアプリケーションを検査および制御したい場合は、パケット キャプチャを記録できます。パケット キャプチャによってアプリケーションが商用のアプリケーションであることが判明した場合、このパケット キャプチャを App-ID 開発のために Palo Alto Networks に提案できます。内部アプリケーションである場合は、カスタム App-ID を作成したり、アプリケーション オーバーライド ポリシーを定義できます。
- カスタム アプリケーションの作成シグネチャを用いて、それをセキュリティ ポリシーに関連付けるか、カスタム アプリケーションを作成してアプリケーションオーバーライドポリシーを定義する - カスタム アプリケーションを使用すると、内部アプリケーションの定義 (特性、カテゴリ、サブカテゴリ、リスク、ポート、タイムアウト) をカスタマイズして、きめ細かなポリシー制御を実行し、ネットワーク上の不明なトラフィックの範囲を最小限に抑えることができます。また、カスタム アプリケーションを作成すると、**ACC** やトラフィック ログ内でアプリケーションを正しく識別でき、ネットワーク上のアプリケーションの監査やレポートに役立ちます。カスタム アプリケーションには、一意にアプリケーションを識別するシグネチャおよびパターンを指定し、アプリケーションを許可または拒否するセキュリティ ポリシーに関連付けられます。

  または、ファイアウォールが高速パスを使用してカスタム アプリケーションを処理する（App-ID を使用したレイヤー 7 検査ではなくレイヤー 4 検査）ようにするには、アプリケーション オーバーライド ポリシー ルール内でカスタム アプリケーションを参照できます。カスタム アプリケーションをアプリケーション オーバーライドに含めることによって、レイヤー 7 検査である App-ID エンジンによるセッションが処理されなくなります。ファイア

ウォールは、通常のステートフル インスペクション ファイアウォールとしてレイヤー 4 でセッションを処理し、アプリケーション処理時間を削減します。

たとえば、ホスト ヘッダー *www.mywebsite.com* をトリガーとするカスタム アプリケーションを作成した場合、パケットは最初に *web-browsing* と識別され、次にカスタム アプリケーション（web-browsing を親アプリケーションとする）に一致します。親アプリケーションが web-browsing であるため、カスタム アプリケーションはレイヤー 7 で検査され、コンテンツおよび脆弱性をスキャンされます。

アプリケーション オーバーライドを定義すると、ファイアウォールはレイヤー 4 での処理を停止します。ログ内での識別に役立つカスタム アプリケーション名がセッションに割り当てられ、トラフィックは脅威をスキャンされません。

新規および変更済みの App-ID の管理

新しい App-ID と変更された App-ID は、アプリケーションと脅威のコンテンツ更新 の一部としてファイアウォールに配信されます。新規および変更済みの App-ID により、ファイアウォールはセキュリティ ポリシーの精度を常に向上させることができますが、コンテンツ更新リリースがインストールされたときに発生するセキュリティ ポリシーの適用の変更はアプリケーションの可用性に影響します。このため、最新の脅威防止機能を利用可能になるようにコンテンツ更新を最適に配備する方法を考え、新規および変更済みの App-ID を最大限に活用するようにセキュリティ ポリシーを調整する必要があります。

新しい App-ID による既存のポリシー適用への影響を評価する場合、App-ID を無効（にして有効）にする場合、および安全を確保するためにポリシー ルールをシームレスに更新してから新たに識別されたアプリケーションを適用する場合は、以下のオプションを使用します。

- 新規および変更が加えられた App-ID を組み込むためのベストワークフロー
- コンテンツ リリースの新規および変更済みの App-ID を参照する
- 新規および変更済みの App-ID がセキュリティ ポリシーに与える影響を参照
- 重要な新規 App-ID が許可されていることを確認する
- 新しい App-ID の監視
- App-ID の無効化および有効化

また、コンテンツ更新時に提供されるアプリケーション タグを使用した合理化された App-ID ポリシー ルールを利用することもできます。

新規および変更が加えられた App-ID を組み込むためのベストワークフロー

このマスターワークフローを参照して、最初にアプリケーションおよび脅威のコンテンツの更新をセットアップし、新規および変更が加えられた App-ID をセキュリティ ポリシーに最適に組み込むようにします。コンテンツ更新をデプロイするために必要な項目をすべてこちらで紹介します。

STEP 1 | アプリケーションおよび脅威コンテンツの更新をデプロイする方法にビジネスニーズを合わせます。

アプリケーションと脅威コンテンツの更新の仕組みを理解し、 ミッション クリティカルまたはセキュリティ優先のいずれかの組織を特定します。これらのうちのどれがビジネスにとって最も重要かを理解することは、コンテンツの更新を最適にデプロイする方法を決定し、ビジネスニーズを満たすベストプラクティスを適用するのに役立ちます。おそらく、ファイアウォールのデプロイメント（データセンターまたは周辺）またはオフィスの場所（リモートまたは本社）に応じて、両方の方法を組み合わせて適用することができます。

STEP 2 | 組織のネットワーク セキュリティとアプリケーションの可用性要件に基づいて、のベストプラクティス (アプリケーションおよび脅威コンテンツ更新プログラム) を確認して適用します。

STEP 3 | セキュリティ ポリシー ルールを設定して、認証やソフトウェア開発アプリケーションなど、ネットワーク全体に影響を与える可能性のある新しい App-ID を常に許可するようにします。

新しい App-ID 特性は、最新のコンテンツ リリースで導入された App-ID にのみ一致します。セキュリティポリシーで使用すると、新しい App-ID に基づいてセキュリティ ポリシーを細かく調整し、重要なカテゴリになる App-ID（常に重要な新しい App-ID が許可されていることを確認する）を常に利用できるようになります。

STEP 4 | アプリケーションと脅威コンテンツの更新をデプロイするスケジュールを設定します。これには、必要なセキュリティ ポリシーの更新を行うまで App-ID の新しいインストールを遅らせるオプションが含まれています（**New App-ID Threshold (**新しい **App-ID** のしきい値**)**を使用）。

STEP 5 | コンテンツ更新のインストール スケジュールを設定したら、定期的にチェックインして、コンテンツ リリースの新規および変更された App-ID を確認するはずです。

STEP 6 | 次に、新規および変更済みの App-ID がセキュリティ ポリシーに与える影響を確認して、必要に応じてセキュリティ ポリシーを調整します。

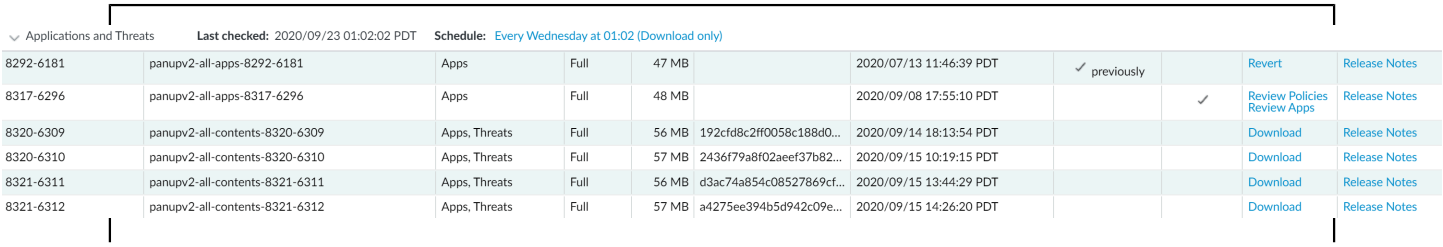
STEP 7 | 新規 App-ID を監視することで、ネットワーク上の新しい App-ID アクティビティを表示できるため、最も効果的なセキュリティ ポリシーの更新を行うことができます。

コンテンツ リリースの新規および変更済みの App-ID を参照する

ダウンロードされたコンテンツ更新とインストール済みのコンテンツ更新の両方に、更新に含まれる新規および変更済みの App-ID のリストが表示されます。完全なアプリケーションの詳細が提供され、重要なことに、ネットワーク全体に影響を与えるアプリケーション（LDAP や IKE など）の更新は、ポリシーのレビューに推奨されるものとして目立っています。変更済みの App-ID の場合、アプリケーションの詳細は、対象範囲がどのように拡張されるか、またはより正確になるかについても説明します。

STEP 1 | **Device (**デバイス**)** > **Dynamic Updates (**動的更新**)** を選択し、さらに **Check Now (**今すぐチェック**)** を選択して利用可能なコンテンツ更新を更新します。

STEP 2 | ダウンロード済みのコンテンツ リリースまたはインストール済みのコンテンツ リリースの場合は、**Actions**（操作）列の **Review Apps**（レビュー アプリ）リンクをクリックして、そのリリースの新しく特定されたアプリケーションや変更されたアプリケーションの詳細を表示します。

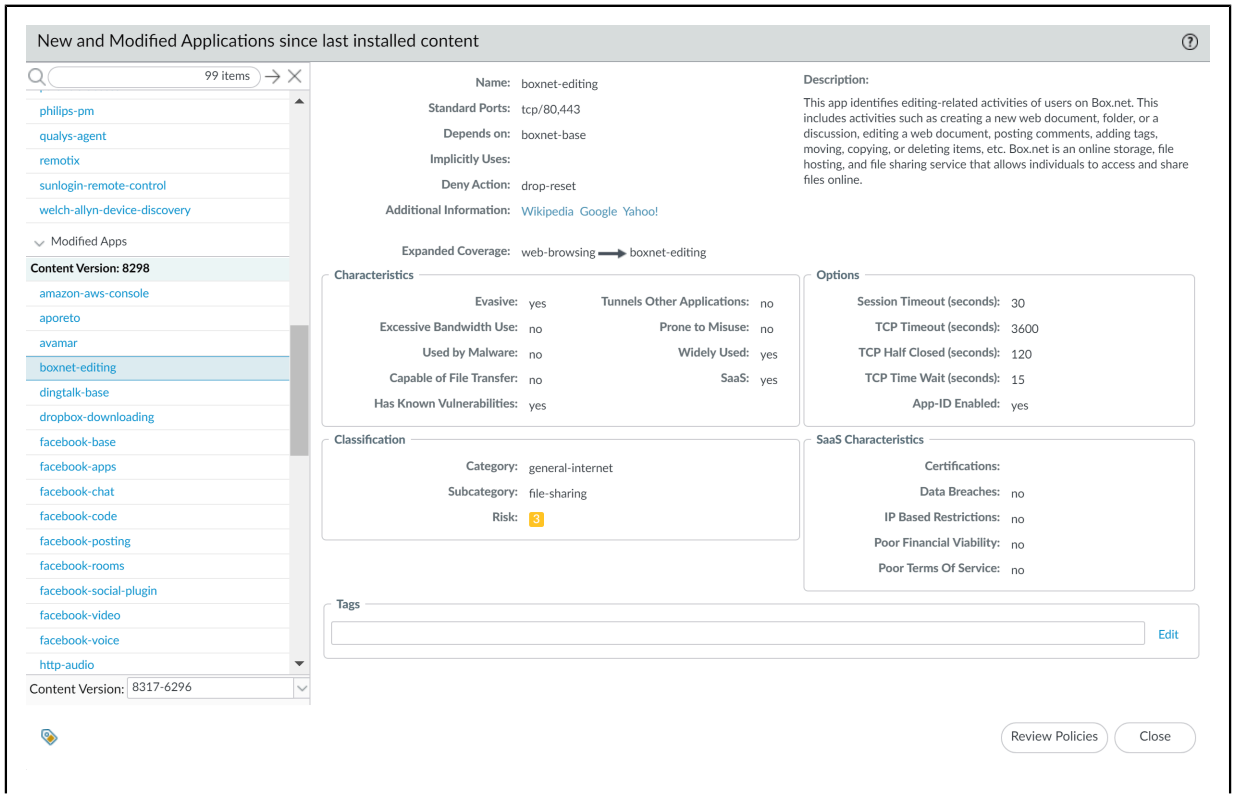


Applications and Threats **Last checked:** 2020/09/23 01:02:02 PDT **Schedule:** Every Wednesday at 01:02 (Download only)

8292-6181	panupv2-all-apps-8292-6181	Apps	Full	47 MB		2020/07/13 11:46:39 PDT	✓ previously		Revert	Release Notes
8317-6296	panupv2-all-apps-8317-6296	Apps	Full	48 MB		2020/09/08 17:55:10 PDT		✓	Review Policies Review Apps	Release Notes
8320-6309	panupv2-all-contents-8320-6309	Apps, Threats	Full	56 MB	192cfd8c2ff0058c188d0...	2020/09/14 18:13:54 PDT			Download	Release Notes
8320-6310	panupv2-all-contents-8320-6310	Apps, Threats	Full	57 MB	2436f79a8f02aeef37b82...	2020/09/15 10:19:15 PDT			Download	Release Notes
8321-6311	panupv2-all-contents-8321-6311	Apps, Threats	Full	56 MB	d3ac74a854c08527869cf...	2020/09/15 13:44:29 PDT			Download	Release Notes
8321-6312	panupv2-all-contents-8321-6312	Apps, Threats	Full	57 MB	a4275ee394b5d942c09e...	2020/09/15 14:26:20 PDT			Download	Release Notes

STEP 3 | このコンテンツのリリースは、最後のコンテンツ バージョン以降に導入または変更された App-ID を確認してください。

新規 App-ID と変更済み App-ID が別々に表示されます。完全なアプリケーションの詳細がそれぞれ提供され、ネットワーク全体に影響を及ぼすと Palo Alto Networks が予測する App-ID には、ポリシー レビューの推奨としてフラグが立てられます。



新しいポリシー適用で発生する可能性のある影響の評価に使用できる App-ID の詳細は、以下のとおりです。

- **Depends on**[依存] – アプリケーションを一意に識別するためにこの App-ID が依存するアプリケーション シグネチャの一覧を示します。**Depends On**[依存]フィールドに示されたいずれかのアプリケーション シグネチャが無効の場合、依存する App-ID も無効になります。
- **Previously Identified As**[以前の識別] – 新しい App-ID がインストールされる前にアプリケーションを照合して一意に識別していた App-ID の一覧を示します。
- **App-ID Enabled**（**App-ID** 対応） – コンテンツ リリースのダウンロード時にすべての App-ID が有効として表示されます。ただし、コンテンツ更新をインストールする前に App-ID シグネチャの手動による無効化を選択している場合を除きます。

変更された App-ID の場合、詳細には次の情報が含まれます：**Expanded Coverage**（拡張範囲）、**Remove False Positive**（誤検出の削除）、およびアプリケーション メタデータの変更。拡張範囲と誤検出の削除フィールドは、アプリケーションの対象範囲がどのように変更されたか（より包括的であるか狭められているか）を示し、時計アイコンは特定のアプリケーションの詳細が更新されるメタデータの変更を示します。

STEP 4 | 調査結果に基づいて、 **Review Policies**（ポリシーの確認）をクリックして、新しく変更された App-ID がセキュリティ ポリシーの適用にどのように影響するかを確認します。「新規および変更済みの App-ID がセキュリティ ポリシーに与える影響」を参照してください。

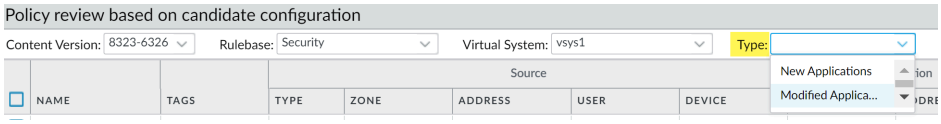
新規および変更済みの App-ID がセキュリティ ポリシーに与える影響を参照

新たに分類され、変更された App-ID は、ファイアウォールがトラフィックを強制する方法を変更する可能性があります。コンテンツの更新ポリシーレビューを実行して、新規および変更済みの App-ID がセキュリティ ポリシーにどのように影響するかを確認し、必要な調整を簡単に実行します。ダウンロードしたコンテンツとインストールしたコンテンツの両方について、コンテンツ更新ポリシーのレビューを実行できます。

STEP 1 | デバイス > ダイナミック更新

STEP 2 | コンテンツ リリースで導入または変更される各 App-ID の詳細については、「コンテンツ リリースの新規および変更された App-ID」を参照してください 。

STEP 3 | ダウンロードされたコンテンツ リリースまたは現在インストールされているコンテンツ リリースの場合は、Actions（操作）列の**Review Policies**（ポリシーの確認）をクリックします。**Policy review based on candidate configuration (**候補設定に基づくポリシー レビュー**)** ダイアログでは、**Content Version (**コンテンツのバージョン**)** 別にフィルタリングしたり、特定のリリースで追加された新規または変更済みのいずれかの App-ID を表示したりすることができます（また、**Rulebase (**ルールベース**)**、**Virtual System (**仮想システム**)**、および **Application**（アプリケーション）に基づいて新しい App-ID によるポリシーへの影響をフィルタリングすることもできます）。



STEP 4 | **Application (**アプリケーション**)** ドロップダウンから App-ID を選択して、現在アプリケーションに適用されているポリシー ルールを表示します。表示されるルールは、新しい App-ID がインストールされる前にアプリケーションと一致していた App-ID に基づきます（アプリケーションの詳細を表示して、新しい App-ID の追加前にアプリケーションが **Previously Identified As (**以前の識別**)** に該当していたアプリケーション シグネチャの一覧を示します）。

STEP 5 | ポリシー レビューで提供された詳細を使用して、App-ID がインストールされているとき、または App-ID を含むコンテンツ リリース バージョンが現在インストールされている場合に適用されるポリシー ルールの更新を計画すると、変更がすぐに反映されます。

Add app to selected policies（アプリを選択したポリシーを追加）または **Remove app from selected policies**（選択したポリシーからアプリケーションの削除）を行います。

重要な新規 App-ID が許可されていることを確認する

新しい App-ID は、特定のアプリケーションに属すると新たに識別されたトラフィックのポリシー適用の変更を引き起こす可能性があります。セキュリティ ポリシー適用への影響を軽減するには、新しい App-ID がインストールされたときに設定を変更することなく、常に最近デプロイされた App-ID が適用されるように、セキュリティ ポリシー ルールで **New App-ID**（新規 **APP-ID**）特性を使用できます。新しい App-ID 特性は、直前にインストールされたコンテンツ リリースの新規 App-ID と常に一致します。新しいコンテンツ リリースがインストールされると、新規 App-ID 特性は自動的に、そのコンテンツ リリース バージョンの新規 App-ID にのみ一致し始めます。

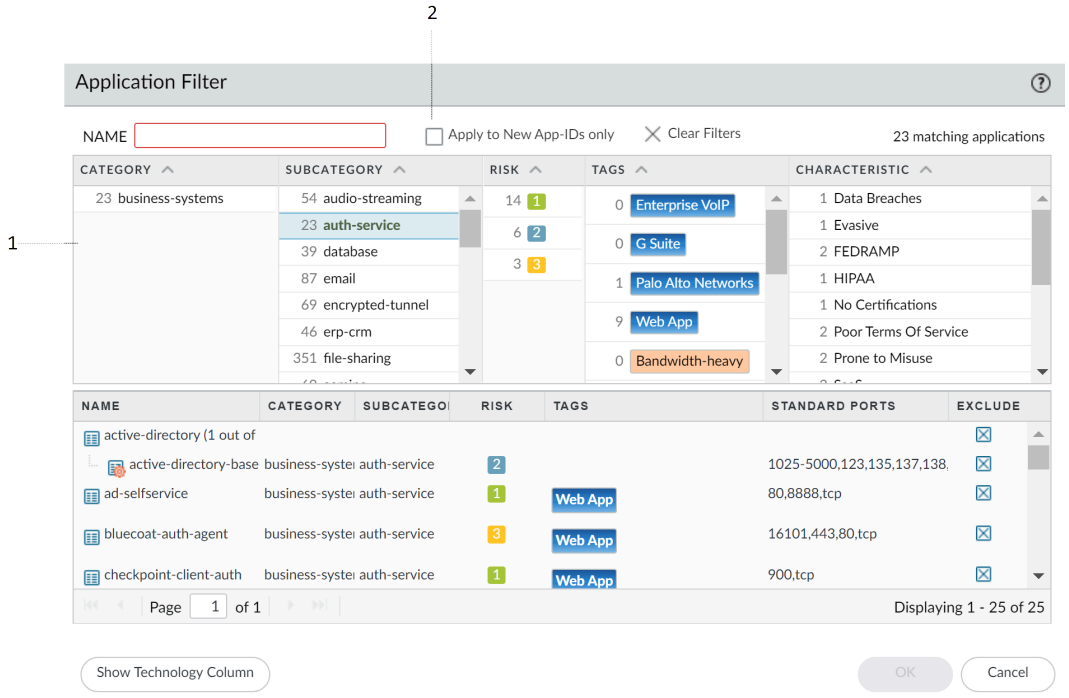
すべての新規 App-ID を適用するか、セキュリティ ポリシー ルールを対象にして、ネットワーク全体または重大な影響を及ぼす特定のタイプの新規 App-ID（認証またはソフトウェア開発アプリケーション限定の適用等）を適用することができます。App-ID リリースで重要なアプリケーションの拡張またはより正確な対象範囲がデプロイされても、ファイアウォールは引き続きそれらを許可するように、セキュリティ ポリシー ルールを **Allow**（許可）に設定します。

新規 App-ID は毎月リリースされるため、最新の App-ID を許可するポリシー ルールでは、新しく分類されたアプリケーションがセキュリティポリシー施行にどのように影響し、必要な調整を加えるかを調査するために、次に手動でコンテンツをインストールするまで、ファイアウォールがスケジュールに基づいてコンテンツの更新をインストールしない場合は 1 か月間の期間が与えられます。

STEP 1 | **Object (オブジェクト)** > **Application Filters(アプリケーション フィルタ)** を選択して新規アプリケーション フィルタを **Add (追加)** します。

STEP 2 | サブ カテゴリまたは特性に基づいて一定の可用性を確保したい新しいアプリケーションのタイプを定義します。たとえば、「認証サービス」というカテゴリを選択して、認証を実行またはサポートすることが分かっている新しくインストールされたアプリケーションが許可されていることを確認します。

STEP 3 | インストール直後に許可する新しいアプリケーションのタイプを絞り込んだ後でのみ、**Apply to New App-IDs only**（新規 **App-ID** のみに適用）を選択します。



STEP 4 | **Policies**（ポリシー） > **Security**（セキュリティ）を選択し、一致するトラフィックを許可するように設定されたセキュリティ ポリシー ルールを追加または編集します。

STEP 5 | **Application**（アプリケーション）を選択して、一致基準に従い、新しい **Application Filter**（アプリケーション フィルタ）をポリシー ルールに追加します。

STEP 6 | **OK** および **Commit (コミット)** をクリックして変更を保存します。

STEP 7 | 新しい App-ID でデプロイされた強制の変更を考慮してセキュリティ ポリシーを調整し続けるには：

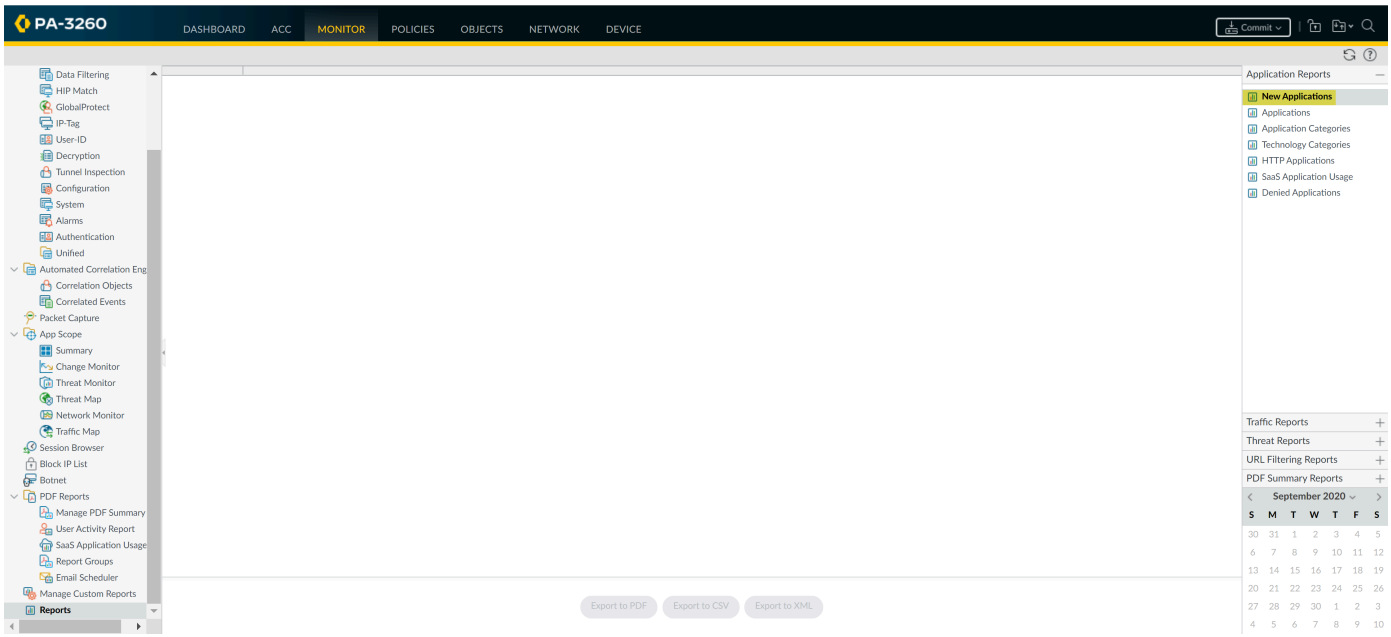
- 新規 App-ID を監視する—新規 App-ID のアクティビティを監視してレポートを取得します。
- コンテンツ リリースの新規および変更された App-ID を確認—新しくインストールされた App-ID が既存のセキュリティ ポリシー ルールにどのように影響するかを参照します。

新しい App-ID の監視

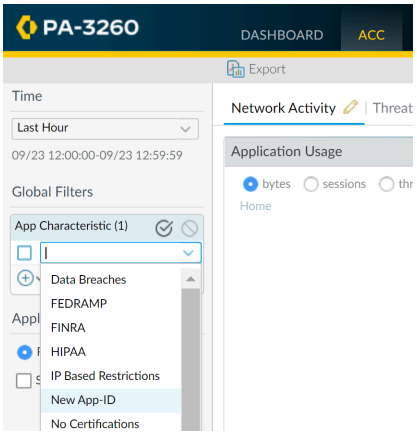
New App-ID（新規 **App-ID**）特性を使用すると、ネットワーク上の新しいアプリケーションを監視することができます。これにより、作成したいセキュリティ ポリシーの更新をより正確に評価できます。ACC の新規 App-ID 特性を使用して、ネットワーク上の新しいアプリケーションの可視性を取得し、新しく分類されたアプリケーションの動作を詳細にレポートします。ここでの学習内容は、最近分類された App-ID を実施するためにセキュリティ ポリシーを更新する方法についての正しい決定を下すのに役立ちます。ACC上で新規 App-ID 特性を使用している場合でもレポートを生成している場合でも（または常に重要な新しい App-ID が許可されていることを確認する）、新規 App-ID 特性は常に、直前にインストールされたコンテンツ リリースの 新規

App-ID にのみ一致します。新しいコンテンツ リリースがインストールされると、新規 App-ID 特性は自動的に、そのコンテンツ リリース バージョンの新規 App-ID にのみ一致し始めます。

新しいアプリケーション（最新のコンテンツ リリースでのみ導入されたアプリケーション）に関する詳細を含むレポートを生成します。



ACC を使用して新しいアプリケーションのアクティビティを監視します：**ACC** を選択し、**Global Filters**（グローバル フィルタ）で、**Application**（アプリケーション） > **Application Characteristics** > **New App-ID**（新規 **App-ID**）を選択します。



App-ID の無効化および有効化

最新の脅威防止のメリットを直ちに享受し、後で App-ID を有効にする予定で、特定のアプリケーションの App-ID を無効にする場合は、コンテンツ リリースに導入されたすべての App-ID を無効にすることができます。

App-ID を参照するポリシー ルールは、有効な App-ID のみに基づいてトラフィックが照合され適用されます。

特定の App-ID は無効にすることができず、ステータスは有効しか認められません。無効にできない App-ID には、他の App-ID （unknown-tcp など）が黙示的に使用する一部のアプリケーション シグネチャが含まれます。ベース App-ID を無効にすると、ベース App-ID に依存している App-ID も無効になることがあります。たとえば、facebook-base を無効にすると、他の Facebook App-ID がすべて無効になります。

コンテンツ リリースまたはスケジュール設定されたコンテンツ更新の App-ID をすべて無効にします。

このオプションにより脅威から保護することができますが、後で App-ID を有効にするオプションを与えることで、App-ID を定期的に無効にするのではなく、代わりにセキュリティ ポリシー ルールが 新規 App-ID を一時的に許可するように設定することを推奨します。このルールは常に、最新のコンテン ツリリースに導入された新規 App-ID のみを許可します。新規 App-ID を含むコンテンツの更新は月に 1 回しかリリースされないため、新しい App-ID を評価し、アプリケーションは影響を受けないことを確実にしつつ、必要に応じて新しい App-ID をカバーするようにセキュリティポリシーを調整する時間を用意してください。

- コンテンツ リリースに追加された新しい App-ID をすべて無効にするには、**Device (デバイス)** > **Dynamic Updates (動的更新)** の順に選択し、アプリケーションおよび脅威コンテンツ リリースを **Install (インストール)** します。プロンプトが表示されたら、**Disable new apps in content update** [コンテンツ更新での新しいアプリケーションの無効化]を選択します。チェックボックスをオンにすると、アプリケーションが無効になり、コンテンツ更新のインストールが続行されます。
- **Device (デバイス)** > **Dynamic Updates (動的更新)** ページで **Schedule (スケジュール)** を選択します。コンテンツ リリースのダウンロードおよびインストールの **Disable new apps in content update (コンテンツ更新での新しいアプリケーションの無効化)** を選択します。

一度に 1 つ以上のアプリケーションの App-ID を無効にします。

- 一度に 1 つ以上のアプリケーションを即座に無効にするには、**Objects (オブジェクト)** > **Applications (アプリケーション)** の順に選択します。1 つ以上のアプリケーションのチェック ボックスをオンにして、**Disable** [無効化]をクリックします。
- 1 つのアプリケーションの詳細を確認して、そのアプリケーションの App-ID を無効にするには、**Objects (オブジェクト)** > **Applications (アプリケーション)** の順に選択して、**Disable App-ID (App-ID の無効化)** を選択します。保留中の App-ID （App-ID を含むコンテンツ リリースがファイアウォールにダウンロードされているが、まだインストールされていない場合）とインストール済みの App-ID の両方を無効にする場合も、この手順を使用できます。

App-ID を有効にします。

以前に **Objects (オブジェクト)** > **Applications (アプリケーション)** を選択して無効にした App-ID を有効にします。1 つ以上のアプリケーションのチェック ボックスをオンにして、**Enable** [有効化]をクリックするか、特定のアプリケーションの詳細を開いて **Enable App-ID** [App-IDの有効化]をクリックします。

ポリシーでのアプリケーション オブジェクトの使用

アプリケーション オブジェクトを使用して、セキュリティ ポリシーがアプリケーションを処理する方法を定義します。

- アプリケーション グループの作成
- アプリケーション フィルタの作成
- カスタム アプリケーションの作成
- アプリケーションの依存関係を解決

アプリケーション グループの作成

アプリケーション グループとは、ポリシーで同じように処理される複数のアプリケーションを含むオブジェクトです。組織内で使用を明示的に許可するアプリケーションにユーザーがアクセスできるようにするときには、アプリケーション グループを使用すると便利です。制限付きのアプリケーションをグループ化することで、ルールベースを管理しやすくなります。サポートするアプリケーションに変更があった場合に、影響を受けるアプリケーション グループのみを更新することができ、個々のポリシー ルールを更新する必要がありません。

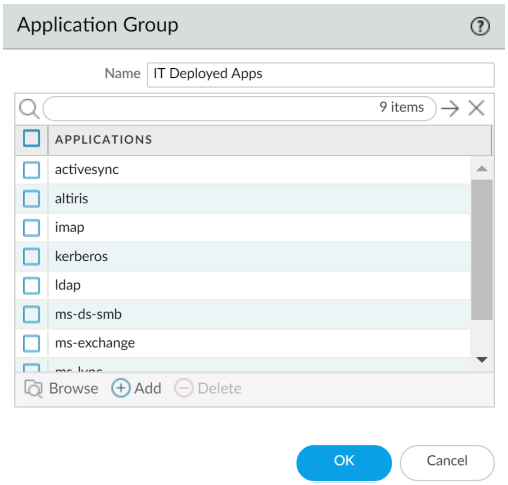
アプリケーションの分類方法を検討するときには、許可するアプリケーションへのアクセスをどのように制御するかを考慮します。そして、各ポリシーの目的に沿うようにアプリケーション グループを作成します。たとえば、一部のアプリケーションには IT 管理者のみがアクセスでき、他のアプリケーションは組織内の既知のすべてのユーザーが使用できるようにするとします。この場合、ポリシーの目的ごとに個別のアプリケーション グループを作成することが考えられます。アプリケーションへのアクセスはデフォルト ポートでのみ許可するのが一般的ですが、この方法の例外とするアプリケーションをグループ化して、別のルールでこれらのアプリケーションへのアクセスを制御します。

STEP 1 | **Objects (オブジェクト)** > **Application Filters (アプリケーション フィルタ)** を選択します。

STEP 2 | グループを **Add** [追加]して、そのグループの分かりやすい **Name** [名前]を付けます。

STEP 3 | （任意）**Shared** （共有）を選択すると、共有場所にオブジェクトを作成して、Panorama の共有オブジェクトとしてアクセスしたり、マルチ仮想システム ファイアウォールのすべての仮想システムで使用可能にしたりすることができます。

STEP 4 | アプリケーションをグループに **Add** [追加]して、**OK** をクリックします。



STEP 5 | 設定を **Commit**（コミット）します。

アプリケーション フィルタの作成

アプリケーション フィルタは、定義されたアプリケーション属性に基づいて動的にアプリケーションをグループ化するオブジェクトです。定義できる属性には、カテゴリやサブカテゴリ、テクノロジ、リスク ファクタ、特徴などがあります。この機能は、アクセスを明示的には許可しないが、ユーザーがアクセスできるようにするアプリケーションを安全に有効にする場合に役立ちます。たとえば、仕事に使うプログラム (Evernote、Google Docs、Microsoft Office 365 など) を従業員に自由に選択させるような場合です。これらの種類のアプリケーションを安全に有効にするには、**business-systems** カテゴリと **office-programs** サブカテゴリに照合するアプリケーション フィルタを作成することができます。新しいアプリケーション オフィス プログラムが出現して新しい App-ID が作成されると、これらの新しいアプリケーションが定義済みのフィルタと自動的に照合されます。フィルタに定義した属性と一致するアプリケーションを安全に有効にするためのポリシー ルールベースは変更する必要がありません。

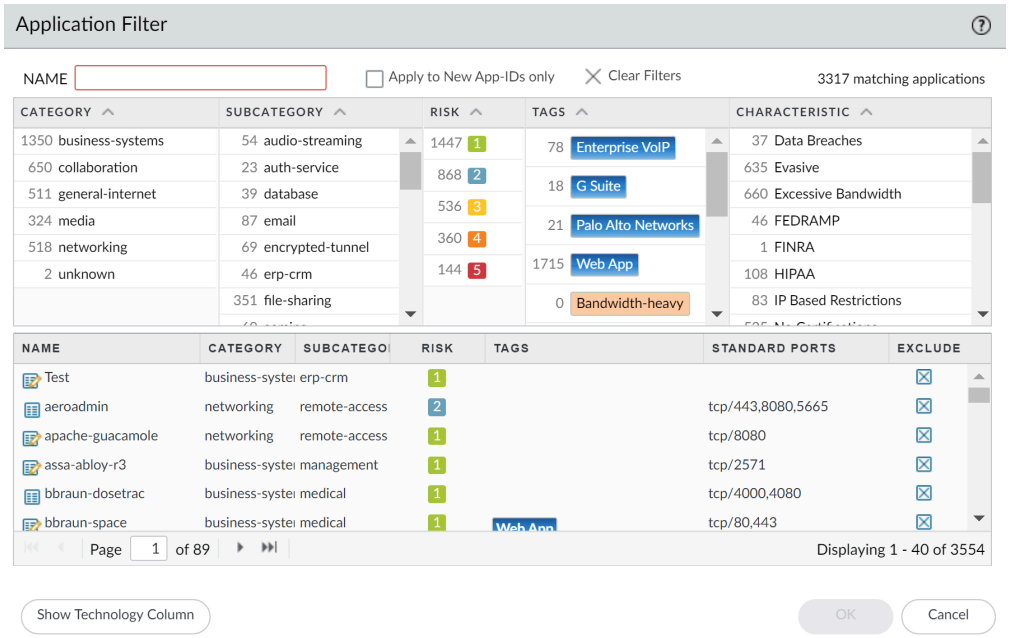
STEP 1 | **Objects (オブジェクト)** > **Application Filters (アプリケーション フィルタ)** を選択します。

STEP 2 | フィルタを **Add** [追加]して、そのフィルタの分かりやすい **Name** [名前]を付けます。

STEP 3 | （任意）**Shared** （共有）を選択すると、共有場所にオブジェクトを作成して、Panorama の共有オブジェクトとしてアクセスしたり、マルチ仮想システム ファイアウォールのすべての仮想システムで使用可能にしたりすることができます。

STEP 4 | Category [カテゴリ]、Subcategory [サブカテゴリ]、Technology [テクノロジ]、Risk [リスク]、Characteristic [特性]の各セクションから属性値を選択して、フィルタを定義します。値を選択していくうちに、ダイアログの下部の一致するアプリケーションのリストが絞り込

まれます。フィルタの属性を調整して、安全に有効にするアプリケーションの種類と一致したら、**OK** をクリックします。



STEP 5 | 設定を **Commit**（コミット）します。

カスタム アプリケーションの作成

アプリケーションを安全に有効にするには、すべてのポートのあらゆるトラフィックを常時分類する必要があります。App-ID を使用した場合、通常、ACC およびトラフィック ログで不明トラフィック（tcp、udp、non-syn-tcp）として分類されるアプリケーションは、App-ID にまだ追加されていない商用のアプリケーション、ネットワーク上の内部アプリケーションやカスタム アプリケーション、または潜在的な脅威に限られます。

App-ID がまだ設定されていない商用のアプリケーションの不明トラフィックが確認された場合は、こちらから新しい *App-ID*をリクエストしていただけます：http://researchcenter.paloaltonetworks.com/submit-an-application/.

内部のカスタム アプリケーションが不明トラフィックとして表示されないようにするには、カスタム アプリケーションを作成します。次に、ネットワーク上の不明なトラフィックの範囲を最小限にして、攻撃対象領域を縮小するために、これらのアプリケーションに対する詳細なポリシー制御を実施できます。また、カスタム アプリケーションを作成すれば、ACC やトラフィック ログでそのアプリケーションが正しくし識別されるため、ネットワーク上のアプリケーションの監査やレポートが可能になります。

カスタム アプリケーションを作成する場合は、アプリケーションの属性（特性、カテゴリ、サブカテゴリ、リスク、ポート、タイムアウト）を定義する必要があります。さらに、ファイアウォールがトラフィック フロー自体との照合に使用できるパターンまたは値（シグネチャ）も定義する必要があります。最後に、カスタム アプリケーションを、アプリケーションを許可または拒否するセキュリティ ポリシーに関連付ける（またはアプリケーション グループに追加したり、アプリケーション フィルタに照合したりする）ことができます。さらに、ワールド カッ

プ サッカーや全米大学バスケットボール トーナメントの ESPN3-Video など、関心の高い事項に関する一時的なアプリケーションを識別するカスタム アプリケーションを作成することもできます。

カスタム アプリケーション シグネチャを作成するための正しいデータを収集するには、パケット キャプチャとデータグラム生成についてよく理解しておく必要があります。作成されたシグネチャが大まかすぎる場合、他の類似のトラフィックも含まれてしまう可能性があります。定義が細かすぎる場合は、トラフィックがパターンに厳密に一致しないと検出を回避されてしまいます。

カスタム アプリケーションはファイアウォール上の別個のデータベースに保存され、このデータベースは毎週の *App-ID* の更新に影響されません。

プロトコルの内部にトンネリングされている可能性のあるアプリケーションをファイアウォールが検出できるようにするアプリケーション プロトコル デコーダとしては、コンテンツ リリース バージョン *609* の時点で、次のものなどがサポートされています：*FTP*、*HTTP*、*IMAP*、*POP3*、*SMB*、および *SMTP*。

以下は、カスタム アプリケーションの基本的な作成方法の一例です。

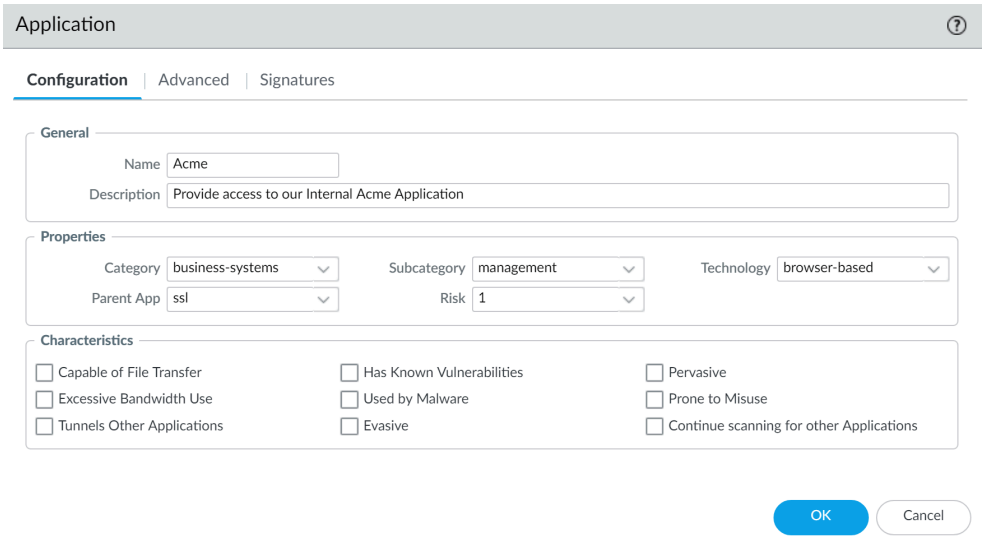
STEP 1 | カスタム シグネチャの作成に使用できる、アプリケーションに関する情報を収集します。

そのためには、アプリケーションについて理解し、アプリケーションへのアクセスをどのように制御するかを認識しておく必要があります。たとえば、ユーザーがアプリケーション内で実行できる操作（アップロード、ダウンロード、ライブ ストリーミングなど）を制限することが考えられます。あるいは、アプリケーションを許可したうえで、QoS ポリシー設定を適用することもできます。

- カスタム アプリケーション シグネチャのベースとなる、アプリケーションの一意の特性を見つけるためにアプリケーション パケットをキャプチャします。この方法の 1 つが、クライアント システム上でプロトコル アナライザ（Wireshark など）を実行して、クライアントとサーバー間のパケットをキャプチャすることです。アプリケーションでアップロードやダウンロードなどさまざまなアクションを実行して、その結果のパケット キャプチャ（PCAP）で各タイプのセッションを見つけられるようにします。
- デフォルトでファイアウォールはすべての不明トラフィックに対してパケット キャプチャを行うため、ファイアウォールがクライアントとサーバー間にある場合は、直接トラフィック ログから不明トラフィックのパケット キャプチャを表示できます。
- パケット キャプチャを使用して、パケット コンテキストで、アプリケーション トラフィックを一意に照合するシグネチャの作成に使用できるパターンまたは値を見つけます。たとえば、HTTP 応答またはヘッダー要求、URI パス、ホスト名に文字列パターンがないか探します。アプリケーション シグネチャの作成に使用できるさまざまな文字列コンテキストおよびパケット内で対応する値を見つける場所の詳細は、「カスタム脅威シグネチャの作成」を参照してください。

STEP 2 | カスタム アプリケーションを追加します。

1. **Objects (オブジェクト)** > **Applications (アプリケーション)** を選択して **Add (追加)** をクリックします。
2. **Configuration** [設定]タブに、カスタム アプリケーションの **Name** [名前]と **Description** [内容]を入力して、このアプリケーションを作成した理由が他の管理者にもわかるようにします。
3. （任意）**Shared** （共有）を選択すると、共有場所にオブジェクトを作成して、Panorama の共有オブジェクトとしてアクセスしたり、マルチ仮想システム ファイアウォールのすべての仮想システムで使用可能にしたりすることができます。
4. アプリケーションのプロパティと特性を定義します。



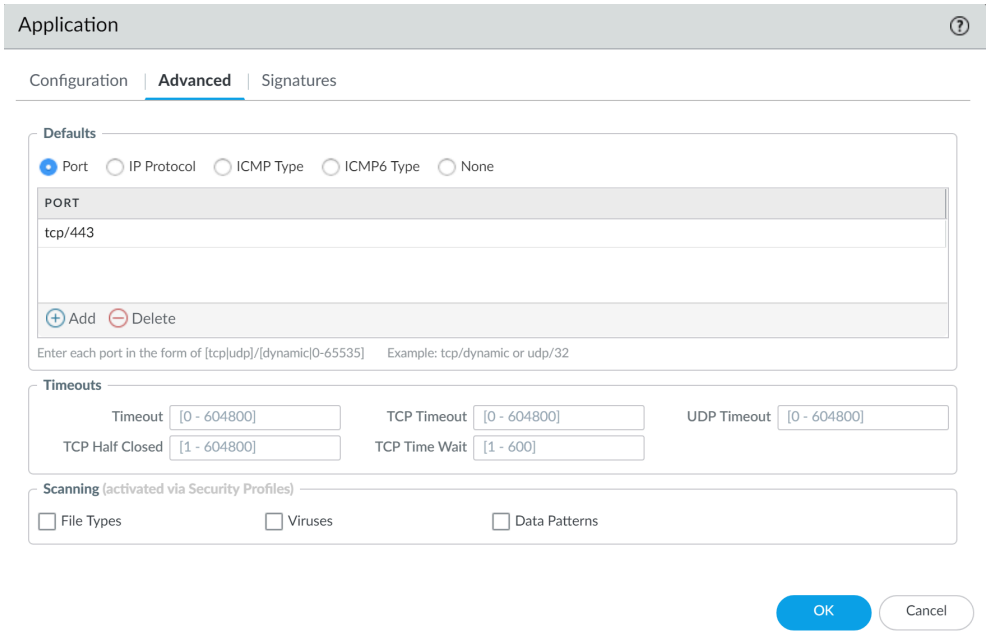
STEP 3 | 基本的なプロトコル、アプリケーションを実行するポート番号、タイムアウト値、トラフィックに実行可能にするスキャンのタイプなど、アプリケーションの詳細を定義します。

Advanced [詳細]タブで、ファイアウォールがアプリケーション プロトコルを識別できるように設定を定義します。

- アプリケーションが使用するデフォルトのポートまたはプロトコルを指定します。
- セッション タイムアウトの値を指定します。タイムアウト値を指定しない場合は、デフォルトのタイムアウト値が使用されます。
- アプリケーション トラフィックに実行する追加のスキャンのタイプを示します。

たとえば、SSL を介して実行するが、（SSL のデフォルト ポートである 443 ではなく）ポート 4443 を使用する TCP ベースのカスタム アプリケーションを作成する場合は、そのポート番号を指定します。カスタム アプリケーションのポート番号を追加すると、ファイアウォー

ルに追加ポートを開くのではなく、アプリケーションのデフォルト ポートを使用するポリシー ルールを作成できます。この方法により、セキュリティに対する姿勢が向上します。



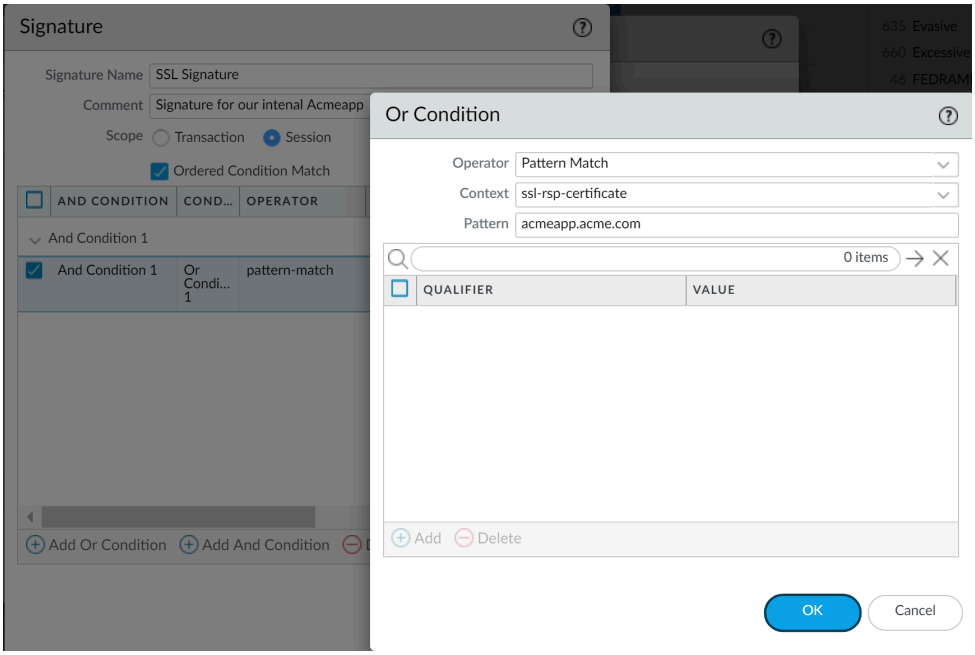
STEP 4 | ファイアウォールがトラフィックとアプリケーションとの照合に使用する基準を定義します。

パケット キャプチャから収集した情報を使用して、ファイアウォールがアプリケーション トラフィックのパターンの照合に使用できる一意の文字列コンテキスト値を指定します。

1. **Signatures** [シグネチャ]タブで、**Add** [追加]をクリックして、**Signature Name** [シグネチャ名]と任意の **Comment** [コメント]を定義し、このシグネチャをどのように使用するかについての情報を示します。
2. シグネチャの **Scope** [範囲]を指定します。つまり、シグネチャを **Session** [セッション]全体と照合するか、1 つの **Transaction** [トランザクション]と照合するかを設定します。
3. **Add And Condition**（And 条件の追加）または **Add Or Condition**（Or 条件の追加）をクリックして、シグネチャを定義する条件を指定します。
4. 使用する一致条件のタイプを定義する **Operator**（演算子）を選択します（**Pattern Match**[パターン マッチ]あるいは**Equal To**[等しい]のいずれか）。
   - **Pattern Match**（パターン マッチ）を選択した場合は、**Context** （コンテキスト）を選択し、正規表現を使用して選択したコンテキストと照合する **Pattern**（パターン）を定義します。任意で修飾子/値ペアを定義する場合は、**Add** [追加]をクリックします。**Qualifier** [修飾子]リストは、選択した **Context** [コンテキスト]に固有です。
   - **Equal To** （等しい）を選択した場合は、**Context**（コンテキスト）を選択し、正規表現を使用して、選択したコンテキストとの照合に使用するパケット ヘッダーのバイトの **Position**（位置）を定義します。**first-4bytes** と **second-4bytes** のいずれかを選

択します。**Mask** [マスク]の 4 バイト 16 進数（0xffffff00 など）と **Value** [値]の 4 バイト 16 進数（0xaabbccdd など）を定義します。

たとえば、ある内部アプリケーションのカスタム アプリケーションを作成している場合、以下のとおり、**ssl-rsp-certificate** というContext (コンテキスト) を使用して、サーバーからの SSL ネゴシエーションの証明書応答メッセージのパターン マッチを定義し、メッセージ内のサーバーの commonName と一致する**Pattern (パターン)** を作成することができます。



5. 一致する条件ごとに手順 4.c と4.dを繰り返します。
6. ファイアウォールがシグネチャの定義との照合を試行する順序が重要な場合は、**Ordered Condition Match** [順番が付けられた条件の一致]チェック ボックスがオンであることを確認してから、条件が適切な順番で評価されるように順序付けます。条件またはグループを選択して **Move Up** [上へ]または **Move Down** [下へ]をクリックします。グループ間で条件を移動することはできません。
7. **OK** をクリックして、シグネチャの定義を保存します。

STEP 5 | アプリケーションを保存します。

1. **OK** をクリックして、カスタム アプリケーションの定義を保存します。
2. **Commit**（コミット）をクリックします。

STEP 6 | トラフィックが予想どおりカスタム アプリケーションと一致することを検証します。

1. **Policies (ポリシー)** > **Security (セキュリティ)** の順に選択し、新しいアプリケーションを許可するセキュリティ ポリシー ルールを **Add (追加)** します。
2. ファイアウォールとアプリケーション間にあるクライアント システムからアプリケーションを実行して、トラフィック ログ（**Monitor (監視)** > **Traffic (トラフィック)**）をチェックし、トラフィックが新しいアプリケーションと一致していること（およびポリシー ルールに従って処理されていること）を確認します。

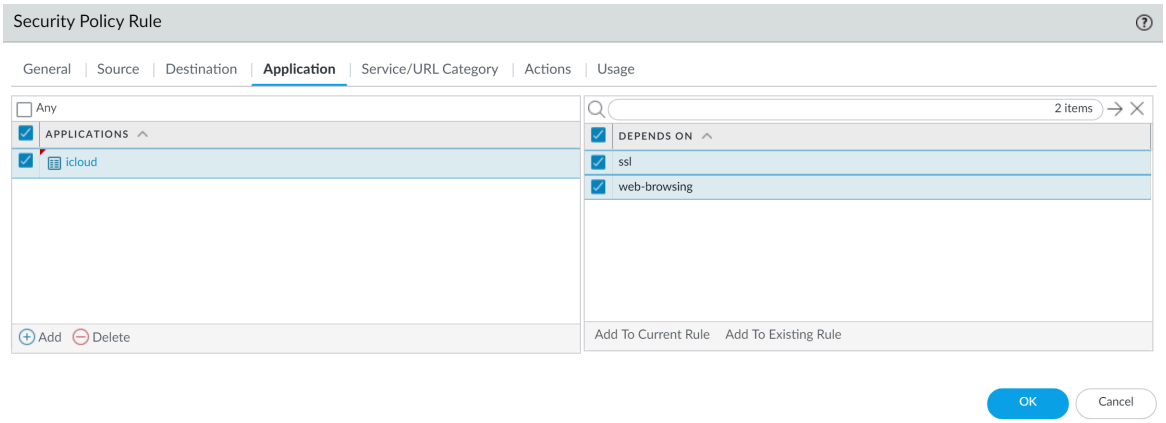
アプリケーションの依存関係を解決

新しいセキュリティ ポリシー ルールを作成するとき、およびコミットを実行するときに、アプリケーションの依存関係を確認できます。ポリシーにすべてのアプリケーションの依存関係が含まれていない場合、関連するセキュリティ ポリシー ルールに直接アクセスして、必要なアプリケーションを追加できます。

STEP 1 | セキュリティ ポリシー ルールを作成する。

STEP 2 | ルールが許可あるいはブロックするアプリケーションを指定します。

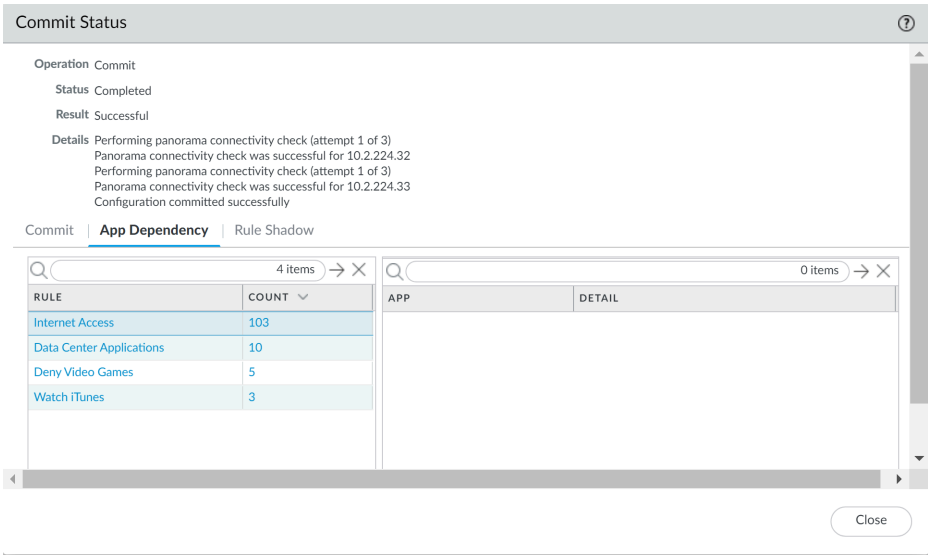
1. **Applications (アプリケーション)** タブで **Application (アプリケーション)** を **Add (追加)** し、安全に有効化します。複数のアプリケーションを選択する、あるいはアプリケーション グループやアプリケーション フィルターを使用することができます。
2. 選択したアプリケーションの依存関係を表示し、**Add To Current Rule**（現在のルールに追加）または**Add To Existing Rule**（既存のルールに追加）を行います。



3. 既存のルールに追加する場合は、**Select Rule**（ルールを選択）して、**OK** をクリックします。

STEP 3 | **OK** をクリックし、変更を **Commit (コミット)** します。

1. **App Dependency**（アプリの依存関係）タブでコミットの警告を確認します。



2. **Count**（カウント）を選択して、含まれていないアプリケーションの依存関係を表示します。
3. **Rule**（ルール）名を選択してポリシーを開き、依存関係を追加します。

   依存しているアプリケーションを解決しないと、アプリケーションはコミット時に警告を生成し続けます。
4. **OK** をクリックし、変更を **Commit (コミット)** します。

デフォルトのポートでアプリケーションを安全に有効化

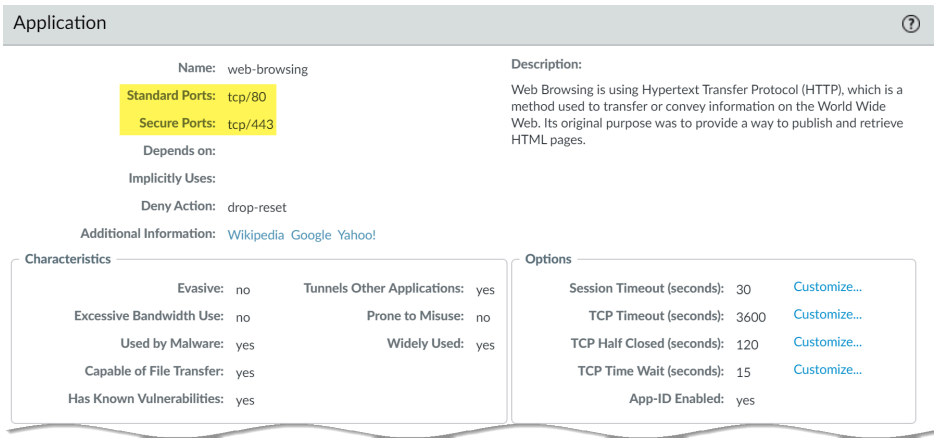
アプリケーションが通常のものでないポートで実行されている場合、従来型のポートベースの保護を攻撃者が回避しようとしている可能性が示唆されます。Application-default は、簡単にこの種の攻撃を回避して最も一般的に使用されているポート上でアプリケーションを安全に有効化する方法を提供する、Palo Alto Networks のファイアウォールの機能です。アプリケーション ベースのセキュリティ ポリシーのベストプラクティスである Application-default は、管理のオーバーヘッドを減らし、ポート ベースのポリシーが持つセキュリティの隙間を埋めてくれます。

- **Less overhead (少ないオーバーヘッド)**—アプリケーション対ポートのマッピングを調査・管理するのではなく、ビジネスニーズに基づいてシンプルなアプリケーション ベースのセキュリティポリシールールを書くことができます。当社は、App-ID を持つすべてのアプリケーションのデフォルトのポートを定義しています。
- **Stronger security (より強固なセキュリティ)**—デフォルトのポート上でのみアプリケーションを実行できるようにすることは、セキュリティのベストプラクティスになります。Application-default により、アプリケーションが予期せぬ挙動を見せている時に、セキュリティを損なわずに重要なアプリケーションを利用できる状態になります。

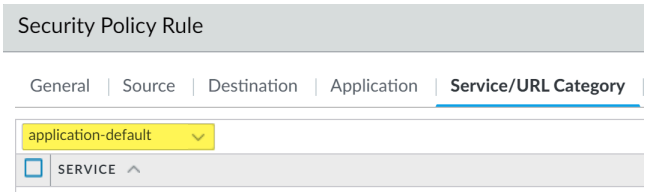
  さらに、アプリケーションが使用するデフォルトのポートは、アプリケーションが暗号化されている時と平文である時とで異なる場合があります。ポート ベースのポリシーでは、アプリケーションが暗号化に対応するために使用する可能性があるすべてのデフォルトのポートを開いておく必要があります。ポートを空けると、攻撃者がセキュリティポリシーをバイパスするために利用できるセキュリティの隙間を作ってしまうことになります。しかし、application-default は暗号化されたアプリケーション トラフィックと平文のアプリケーション トラフィックを区別します。つまり、暗号化されているかどうかに関わらず、アプリケーションのデフォルトのポートを強制することができます。

  例えば、application-default を使用しない場合、web-browsing のトラフィックを有効にするためにポート 80 と 443 を開く必要があります。両方のポートで平文のトラフィックと暗号化されたウェブ ブラウジングのトラフィックの両方を許可することになります。application-default をオンにすると、ファイアウォールは平文の web-browsing のトラフィックはポート 80 で、SSL トンネルのトラフィックはポート 443 で厳格に許可するようになります。

Applipedia にアクセスするか、**Objects (オブジェクト)** > **Applications (アプリケーション)** を選択することで、アプリケーションがデフォルトで使用するポートを確認できます。アプリケーションの詳細情報には、アプリケーションの標準的なポート (平文である場合に最も頻繁に使用するポート) が含まれています。また、web-browsing、SMTP、FTP、LDAP、POP3、IMAP の詳細情報にはアプリケーションの セキュア ポート (暗号化されているときにアプリケーションが使用するポート) も含まれています。



Policy (ポリシー) > **Security (セキュリティ)** を選択してルールを追加するか修正し、アプリケーションをデフォルトのポート上のみに制限します。



SSL 復号化と共にアプリケーション ベースのセキュリティポリシーの一部として *application-default* を使用することが、ベストプラクティスになります。さらに、*<45>Service (サービス)</45>* が *service-http* および *service-https* に設定された *web-browsing* のトラフィックを制御する既存のセキュリティポリシールールがある場合、その代わりに *application-default* を使用するためにそれらのルールを更新する必要があります。

暗黙的サポートを使用するアプリケーション

特定のアプリケーションを許可するポリシーを作成する場合、そのアプリケーションが依存する他のアプリケーションもすべて許可する必要があります。多くの場合、トラフィックが通過できるように依存アプリケーションへのアクセスを明示的に許可する必要はありません。ファイアウォールは依存関係を判断し、暗黙的にそれらを許可できるためです。この暗黙的サポートは、HTTP、SSL、MS-RPC、または RTSP に基づくカスタム アプリケーションにも適用されます。ファイアウォールが依存アプリケーションを時間内に判断できないアプリケーションに対しては、ポリシーを定義する際に依存アプリケーションを明示的に許可する必要があります。次のいずれかを使用して、アプリケーションベースのセキュリティポリシーワークフロー内からアプリケーションの依存関係を判別できます。

- ポリシー オプティマイザー
- タグを使用したアプリケーション フィルタの作成
- カスタム タグに基づくアプリケーション フィルタを作成する
- アプリケーションの依存関係を解決

必要に応じて、Applipediaも利用できます。

以下の表に、ファイアウォールが暗示的サポートに対応しているアプリケーションのリストを示します（コンテンツ更新 595 の時点）。

アプリケーション	暗黙的サポート
360-safeguard-update	http
apple-update	http
apt-get	http
as2	http
avg-update	http
avira-antivir-update	http, ssl
blokus	rtmp
bugzilla	http
clubcooee	http
corba	http
cubby	http, ssl

アプリケーション	暗黙的サポート
dropbox	ssl
esignal	http
evernote	http, ssl
ezhelp	http
Facebook	http, ssl
Facebook-chat	jabber
facebook-social-plugin	http
fastviewer	http, ssl
forticlient-update	http
good-for-enterprise	http, ssl
google-cloud-print	http, ssl, jabber
google-desktop	http
google-talk	jabber
google-update	http
gotomypc-desktop-sharing	citrix-jedi
gotomypc-file-transfer	citrix-jedi
gotomypc-printing	citrix-jedi
hipchat	http
iheartradio	ssl, http, rtmp
infront	http
instagram	http, ssl
issuu	http, ssl
java-update	http

アプリケーション	暗黙的サポート
jepptech-updates	http
kerberos	rpc
kik	http, ssl
lastpass	http, ssl
logmein	http, ssl
mcafee-update	http
megaupload	http
metatrader	http
mocha-rdp	t_120
mount	rpc
ms-frs	msrpc
ms-rdp	t_120
ms-scheduler	msrpc
ms-service-controller	msrpc
nfs	rpc
oovoo	http, ssl
paloalto-updates	ssl
panos-global-protect	http
panos-web-interface	http
pastebin	http
pastebin-posting	http
pinterest	http, ssl
portmapper	rpc

アプリケーション	暗黙的サポート
prezi	http, ssl
rdp2tcp	t_120
renren-im	jabber
roboform	http, ssl
salesforce	http
stumbleupon	http
supremo	http
symantec-av-update	http
trendmicro	http
trillian	http, ssl
Twitter	http
whatsapp	http, ssl
xm-radio	rtsp

セキュリティ ポリシー ルールの最適化

Policy Optimizer は、従来のセキュリティポリシールールベースを App-ID ベースのルールベースに移行するための簡単なワークフローを提供します。これにより、攻撃の入り口を減らし、アプリケーションを可視化して安全に有効にできるため、セキュリティが向上します。Policy Optimizer はポートベースのルールを識別するため、アプリケーションの可用性を損なうことなく、それらをアプリケーションベースの許可ルールに変換したり、ポートベースのルールから既存のアプリケーションベースのルールにアプリケーションを追加したりできます。また、オーバープロビジョニングされた App-ID ベースのルール (未使用のアプリケーションで設定された App-ID ルール) も識別されます。Policy Optimizer は、どのポートベースのルールを最初に移行するかの優先順位付け、使用していないアプリケーションを許可するアプリケーションベースのルールの特定、およびヒット数などのルール使用特性の分析を支援します。

ポートベースのルールをアプリケーションベースのルールに変換すると、許可リストに登録するアプリケーションを選択し、他のすべてのアプリケーションを拒否するため、ネットワークからの不要で悪意のあるトラフィックを排除することができるため、セキュリティ体制が向上します。アプリケーショントラフィックをデフォルトポートに制限する (Service を **application-default (**アプリケーションのデフォルト**)** に設定する) だけでなく、アプリケーションベースのルールに変換することで、回避的なアプリケーションが標準以外のポートで実行されるのを防ぐこともできます。

この機能は以下で利用することができます。

- PAN-OS バージョン 9.0 を実行し、App-ID が有効になっているファイアウォール。
- PAN-OS バージョン 9.0 を実行している Panorama。Panorama が **Policy Optimizer** 機能を使用するために管理するファイアウォールをアップグレードする必要はありません。ただし、**Rule Usage (**ルール使用状況**)** 機能 (ポリシールール使用状況のモニター) を使用するには、管理対象ファイアウォールで PAN-OS 8.1 以降が実行されている必要があります。管理対象ファイアウォールを Log Collector に接続する場合、それらの Log Collector も PAN-OS バージョン 9.0 を実行している必要があります。ログ プロセシング カード (LPC) を備えた管理 PA-7000 Series ファイアウォールは、PAN-OS 8.1（またはそれ以降）も実行できます。
- Cortex Data Lake との互換性のために、Cloud Services プラグイン 2.0 Innovation 以降をインストールした状態で PAN-OS 10.0.3 以降を実行している Panorama を使用してください。

PA-7000 Series ファイアウォールは、*2* つのロギングカード、*PA-7000 Series* ファイアウォールログ処理カード *(LPC)* と高性能 *PA-7000 Series* ファイアウォールログ転送カード *(LFC)* をサポートします。*LPC* とは異なり、*LFC* にはログをローカルに保存するためのディスクがありません。代わりに、*LFC* はすべてのログを *Panorama* や *syslog* サーバーなどの *1* つ以上の外部ログシステムに転送します。*LFC* を使用している場合、トラフィックログはローカルに保存されないため、*Policy Optimizer* のアプリケーション使用情報はファイアウォールに表示されません。*LPC*を使用する場合、トラフィックはファイアウォールにローカルに保存されます。そのため、*Policy Optimizer*のアプリケーション使用状況情報は、ファイアウォール上に表示されます。

この機能を使用して次を行います。

- ポートベースのルールをアプリケーションベースのルールに移行する—許可したいアプリケーションを選択して安全に有効にするため、トラフィックログを調べてアプリケーションをポートベースのルールに手動でマッピングする代わりに、Policy Optimizer を使用してポートベースのルールを特定し、各ルールに一致するアプリケーションを一覧表示します。従来のポートベースのルールをアプリケーションベースの許可ルールに変換すると、ビジネスアプリケーションがサポートされ、悪意のあるアクティビティに関連するアプリケーションをブロックすることができます。
- **Identify over-provisioned application-based rules** — ルールが広すぎると、ネットワーク上で使用しないアプリケーションが許可されるため、攻撃対象領域が増大し、悪意のあるトラフィックを誤って許可するリスクが高まります。

  未使用のアプリケーションを *Security* ポリシールールから削除して、攻撃対象領域を減らし、ルールベースをクリーンに保ちます。ネットワーク上で誰も使用しないアプリケーションを許可しないでください。
- **App-ID Cloud Engine**（**ACE**）アプリケーションをセキュリティポリシールールに追加する-SaaS セキュリティインラインサブスクリプションをお持ちの場合は、ポリシーオプティマイザの新しいアプリケーションビューアを使用して、セキュリティポリシーでクラウド配信のアプリ ID を管理できます。ACE のドキュメントでは、Policy Optimizer を使用してクラウド配信アプリケーション ID を可視化して制御する方法について説明しています。

  このセクションのポリシー オプティマイザーの例では、*SaaS* セキュリティ インライン サブスクリプションを持たないファイアウォールを示しているため、新しいアプリケーション ビューアーは表示されません。

従来のファイアウォールから *Palo Alto Networks* デバイスに設定を移行するには、アプリケーション ベースのポリシーに移行する際のベストプラクティスを参照してください。

ソートするとルールベース内のルールの順序が変わるため、**Security (セキュリティ)** > **Policies (ポリシー)** でセキュリティポリシールールをソートすることはできません。ただし、**Polices** > **Security** > **Policy Optimizer** では、Policy Optimizer にはルールの順序に影響を与えない並べ替えオプションが用意されているため、ルールを並べ替えて、最初に変換またはクリーンアップするルールに優先順位を付けることができます。過去 30 日間のトラフィック量、ルールに表示されるアプリケーションの数、新しいアプリケーションがない日数、および許可されているアプリケーションの数 (オーバープロビジョニングされたルールの場合) でルールを並べ替えることができます。

Policy Optimizer は、運用前のルール検証や既存ルールのトラブルシューティングなど、他の方法でも使用することができます。Policy Optimizer は、**Log at Session End (セッション終了時のログ)** のみを受け入れ、**Log at Session Start (セッション開始時のログ)** は無視して、一時的なアプリケーションがルールに含まれないようにすることに注意してください。

リソースの制約により、*VM-50 Lite* 仮想ファイアウォールは *Policy Optimizer* をサポートしていません。

- Policy Optimizer の概念
- ポートベースから App-ID ベースのセキュリティポリシールールに移行

- ルールコピー移行のユースケース：ウェブ閲覧および SSL トラフィック
- アプリケーションを既存のルールに追加
- 未使用のアプリケーションがあるセキュリティポリシールールを特定
- アプリケーション使用状況統計の高可用性
- Policy Optimizer を無効化する方法

Policy Optimizer の概念

この機能のサポートの詳細については、次のトピックを参照してください：

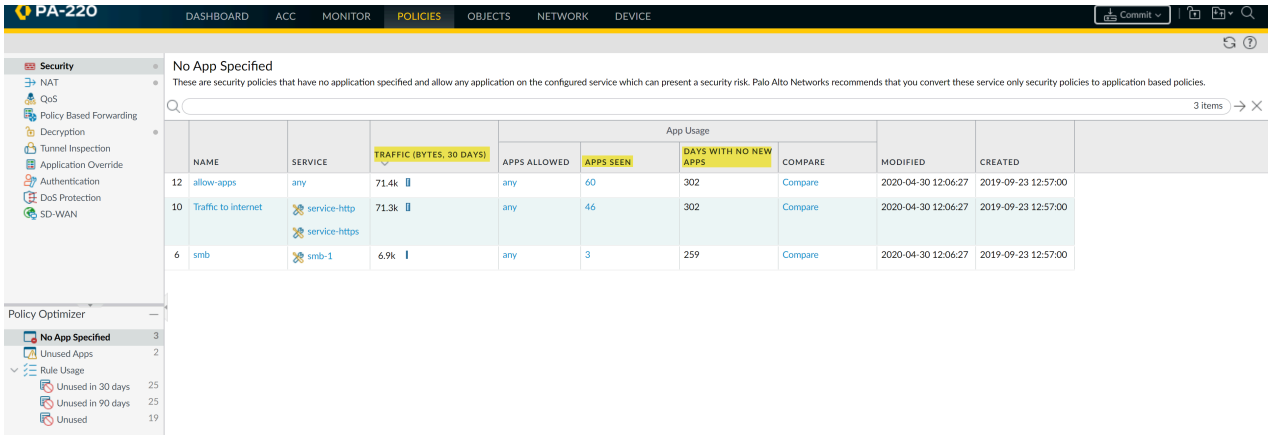
- セキュリティポリシールールの並べ替えとフィルタリング
- アプリケーションの使用状況データをクリア

セキュリティポリシールールの並べ替えとフィルタリング

セキュリティポリシールールをフィルタリングして、アプリケーションが設定されていないすべてのポートベースのルールを表示できます (**Policies (ポリシー)** > **Security (セキュリティ)** > **Policy Optimizer** > **No App Specified (アプリの指定なし)**)。また、アプリケーションが構成されているルールを表示することもできますが、トラフィックは構成済みのアプリケーションの一部にのみ一致します 。 ルールは過剰にプロビジョニングされ、ルールに表示されないアプリケーションが含まれます (**Policies** > **Security** > ポリシーオプティマイザー > 未使用のアプリ)。さらに、SaaS セキュリティインライン ライセンスがある場合は、新しいアプリ ビューアー を使用して、新しい App-ID クラウド エンジン (ACE) アプリケーションを表示したルールをフィルター処理できます (この方法については、ACE のドキュメントを参照してください)。フィルタ処理されたポリシールールをさまざまな種類の統計に基づいてソートし、ポートベースのルールからアプリケーションベースのルールに変換するルール、あるいは最初にクリーンアップするルールを優先することができます。

> ***Policies (ポリシー) > Security (セキュリティ)*** でルールをフィルタまたはソートすることはできません。ルールベースのポリシールールの順序が変わるためです。ポリシー > セキュリティ > ポリシーオプティマイザー > アプリケーション指定なし、ポリシー > セキュリティ > ポリシーオプティマイザー > .>アプリケーション***Policies*** > セキュリティ > ポリシーオプティマイザー > 新しいアプリ ビューア *(SaaS* インライン セキュリティ サブスクリプションを使用している場合*)* はルールベースのルールの順序を変更しません。

複数の列見出しをクリックすると、アプリケーションの使用状況の統計情報に基づいてルールを並べ替えることができます。さらに、ポリシー ルールの使用状況を表示するして、未使用のルールを特定して削除し、セキュリティ リスクを軽減し、ポリシー ルール ベースを整理しておくことができます。ルールの使用状況を追跡することにより、新しいルールの追加やルールの変更を迅速に検証し、操作やトラブルシューティングのタスクのルールの使用状況を監視することができます。



- **Traffic (Bytes、30 days)(**トラフィック **(**バイト、**30** 日間**))**—過去 30 日間におけるルールで見られたトラフィック量です。30 日間のウィンドウでは、デフォルトでリストの一番上に現在最もトラフィックの多いルールが配置されます (より長い時間枠は、トラフィックがそれほど多くなくても累積合計が大きい、リストの一番上に残る古いルールに重点が置かれます)。クリックすると順序が逆になります。
- **Apps Seen (**発見されたアプリ**)**—一番上に表示されているアプリケーションが最も多い、または最も少ないアプリケーションにルールを配置します。ファイアウォールがアプリケーション・データを自動的にパージすることはありません。

  ファイアウォールは、約 *1* 時間ごとに ***Apps Seen*** を更新します。ただし、アプリケーション トラフィックあるいはルールが大量にある場合、更新に *1* 時間以上かかる場合があります。アプリケーションをルールに追加した後、少なくとも *1* 時間待ってからトラフィック ログを実行し、アプリケーションのログ情報を確認します。
- **Days with No New Apps (**新規アプリがない日数**)**—新しいアプリケーションが最後にルールに一致してから最も日数が長い、または最も少ない日数でルールを適用します。

- (**Unused Apps (未使用のアプリ) のみ**) **Apps Allowed (許可されたアプリ)**– 一番上または一番上に設定されているアプリケーションが最も多いルールを一番上に配置します。

アプリケーション使用統計は、以下の基準を満たすルールのアプリケーションのみをカウントします。

- ルールのアクションは **Allow (許可)** する必要があります。
- ルールのログ設定は **Log at Session End (セッション終了時にログ)** にする必要があります (これがデフォルトのログ設定です)。一時的なアプリケーションのカウントを防ぐために、**Log at Session Start (セッション開始時にログ)** するルールは無視されます。
- 有効なトラフィックはルールと一致しなければなりません。例えば、アプリケーションを識別するのに十分なトラフィックがファイアウォールを通過する前にセッションが終了した場合、カウントされません。次のトラフィックタイプは無効であるため、Policy Optimizer の統計情報にはカウントされません。
  - データ不足
  - 該当なし
  - 非 syn-tcp
  - 不完全

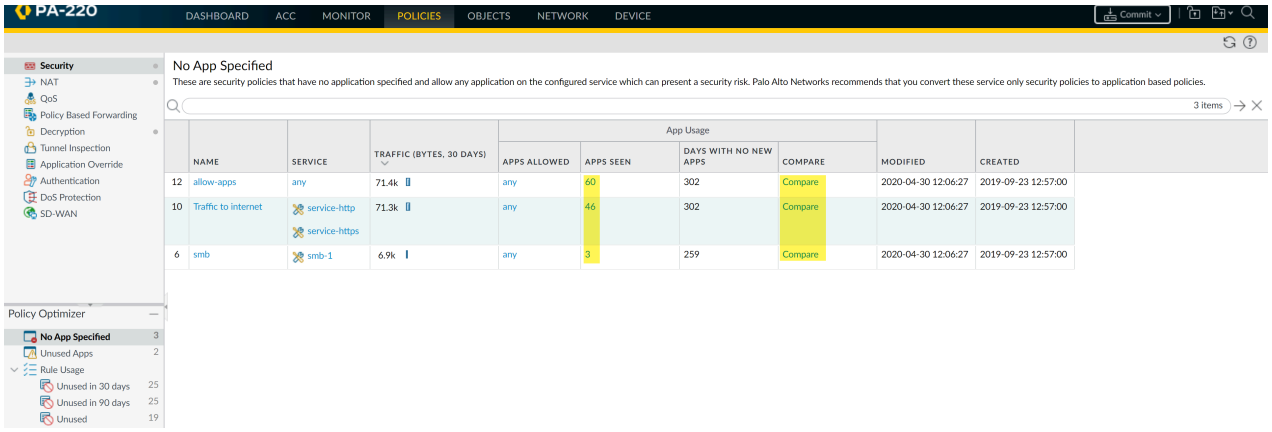
  トラフィックログ (**Monitor (モニター)** > **Logs (ログ)** > **Traffic (トラフィック)**) をフィルタリングして、これらのタイプの 1 つとして識別されたトラフィックを確認できます。例えば、すべてのトラフィックが未完了と識別されたことを確認するには、フィルタ **(app eq incomplete)** を使用します。

これらの基準が満たされていない場合、アプリケーションは **Apps Seen (発見されたアプリ)** などの統計情報にはカウントされず、**Days with No New Apps (新規アプリがない日数)** などの統計情報には影響せず、アプリケーションの一覧には表示されません。

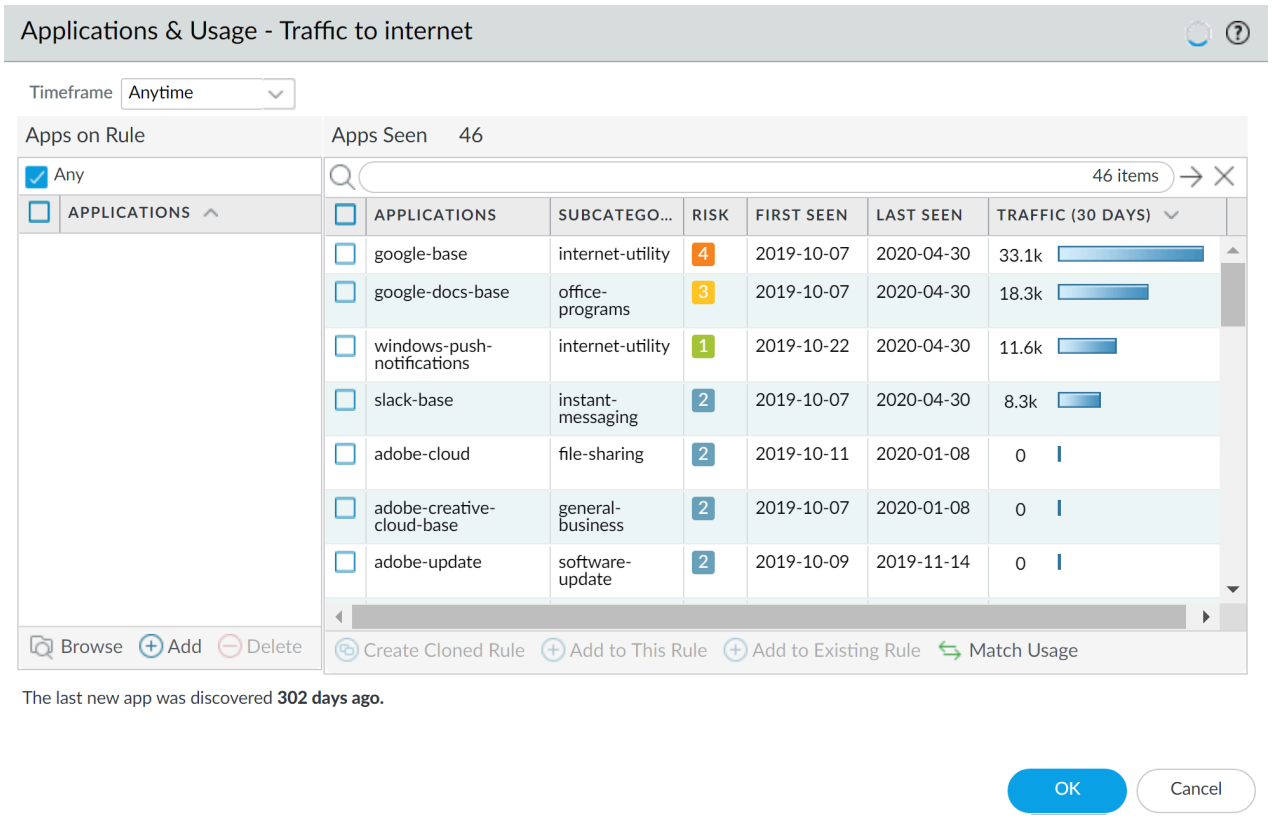
ファイアウォールは、ゾーン間デフォルトおよびゾーン内デフォルトのセキュリティポリシールールのアプリケーション使用統計を追跡しません。

ルールの *UUID* が変更されると、そのルールのアプリケーション使用統計情報はリセットされます。これは、*UUID* の変更によってファイアウォールがそのルールを別の (新しい) ルールとして認識するためです。

ルールに表示されているアプリケーションを表示して並べ替えるには、ルールの行で **Compare (比較)** をクリックするか、**Apps Seen (発見されたアプリ)** の番号をクリックします。



Policies (ポリシー) > **Security (セキュリティ)** > **Policy Optimizer** > **No App Specified (アプリの指定なし)** および **Policies (ポリシー)** > **Security (セキュリティ)** > **Policy Optimizer** > **Unused Apps (未使用のアプリ)** に表示されるルールについては、**Compare (比較)** または **Apps Seen (発見されたアプリ)** の番号をクリックすると、**Applications & Usage (アプリケーションおよび使用状況)** が表示され、ルールで表示されるアプリケーションの確認、および分類が可能です。**Applications & Usage** は、ポートベースから App-ID ベースのセキュリティポリシールールに移行と ルールから未使用のアプリケーションを削除する も参照できます。



6 つの **Apps Seen (**発見されたアプリ**)** 統計すべてでルールに表示されるアプリケーションをソートすることができます (**Apps Seen (**表示された見られたアプリ**)** はリアルタイムで更新されず、トラフィック量とルール数によっては更新に 1 時間以上かかります)。

- **Applications (**アプリケーション**)**—アプリケーション名のアルファベット順。ルールのサービス (サービスは **any (**任意**)** にすることはできません) に対して特定のポートまたはポート範囲を設定し、アプリケーション用の標準 (アプリケーションのデフォルト) ポートがあり、設定されたポートがアプリケーションデフォルトポートと一致しない場合は、黄色い三角の警告アイコンがアプリケーションの横に表示されます。
- **Subcategory(**サブカテゴリ**)**—アプリケーションコンテンツメタデータから派生した、アプリケーションのサブカテゴリ別のアルファベット順です。
- **Risk (**リスク**)**—アプリケーションのリスク評価に従います。
- **First Seen (**初回発見日**)**—ルール上でアプリケーションが初めて表示された日です。タイムスタンプ解決は日単位です (1 時間ごとではありません)。
- **Last Seen (**最終発見日**)**—ルール上でアプリケーションが最後に表示された日です。タイムスタンプ解決は日単位です (1 時間ごとではありません)。

- トラフィック **(30** 日間**)** —過去 30 日間にルールに一致したバイト単位のトラフィックがデフォルトのソート方法です。

Timeframe (時間枠**)** を特定の期間 **Anytime (**常時**)**、**Past 7 days (**過去 **7** 日間**)**、**Past 15 days (**過去 **15** 日間**)**、または **Past 30 days (**過去 **30** 日間**)** の統計を表示するように設定します。

Traffic (30 days) は常に過去 *30* 日間のトラフィックのみをバイト単位で表示します。***Timeframe*** を変更しても、***Traffic (30** 日**)*** バイトの測定値は変更されません。

列見出しをクリックすると表示順が変わり、同じ列をもう一度クリックすると順序が逆になります。例えば、**Risk (**リスク**)** をクリックして、アプリケーションを低リスクから高リスクに並べ替えます。もう一度 **Risk (**リスク**)** をクリックして、アプリケーションを高リスクから低リスクに並べ替えます。

ファイアウォールは、ポリシー オプティマイザーのアプリケーション使用状況の統計情報をリアルタイムで報告しないので、レポートの実行に代わるものではありません。

- ファイアウォールは、**Apps Allowed (**許可されたアプリ**)**、**Apps Seen (**発見されたアプリ**)**、ならびに **Applications & Usage (**アプリケーションおよび使用状況**)** に表示されているアプリケーションを、リアルタイムではなく、ほぼ 1 時間ごとに更新します。大量のトラフィックまたは大量のルールがある場合は、更新に時間がかかることがあります。アプリケーションをルールに追加したら、トラフィックログを実行する前に少なくとも 1 時間待ってからアプリケーションのログ情報を確認します。

  ファイアウォールは約 1 時間ごとに **Apps Seen (**発見されたアプリ**)** を更新します。ただし、アプリケーション トラフィックあるいはルールが大量にある場合、更新に 1 時間以上かかる場合があります。アプリケーションをルールに追加したら、トラフィックログを実行する前に少なくとも 1 時間待ってからアプリケーションのログ情報を確認します。
- ファイアウォールは、1 日に 1 回、真夜中のデバイス時刻で、**Applications & Usage (**アプリケーションおよび使用状況**)** の **Days with No New Apps (**新規アプリがない日数**)**、**First Seen (**初回発見日**)**、**Last Seen (**最終発見日**)** を更新します。
- 多数のアプリケーションが表示されているルールでは、アプリケーション使用状況の統計処理に時間がかかる場合があります。
- 多数のアプリケーションを含む多数のルールを含むセキュリティポリシールールベースの場合、アプリケーション使用状況の統計処理に時間がかかることがあります。
- Panorama が管理するファイアウォールの場合、アプリケーション使用状況データは、Panorama がファイアウォールにプッシュするルールについてのみ表示され、個々のファイアウォールでローカルに設定されたルールには表示されません。

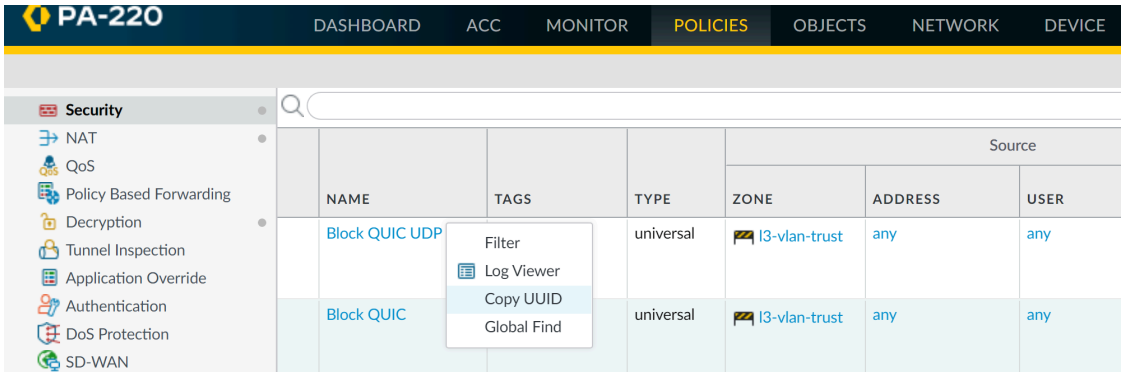
アプリケーションの使用状況データをクリア

CLI コマンドを使用して、個々のセキュリティポリシー ルールのアプリケーション使用状況データをクリアしたり、**Apps Seen (**発見されたアプリ**)** および他のアプリケーション使用状況データをリセットしたりすることができます。

STEP 1 | アプリケーション使用状況データをクリアしたいセキュリティポリシー ルールの UUID を検索します。

UI で UUID を探す方法は 2 つあります：

- **Policies (ポリシー)** > **Security (セキュリティ)** で、**Rule UUID (ルールの UUID)** 列から UUID をコピーします。
- **Policies (ポリシー)** > **Security (セキュリティ)** のルールの **Name (名前)** ドロップダウン メニューで **Copy UUID (UUID をコピー)** を選択します。



STEP 2 | UI から CLI に切り替えます。

UI で控えておいた UUID を使用してルールのアプリケーション使用状況データをクリアします：

```
admin@PA-VM>clear policy-app-usage-data ruleuuid <uuid-value>
```

ルールの UUID を値としてペーストするか入力し、コマンドを実行してルールのアプリケーション使用状況データをクリアします。

ポートベースから App-ID ベースのセキュリティポリシールールに移行

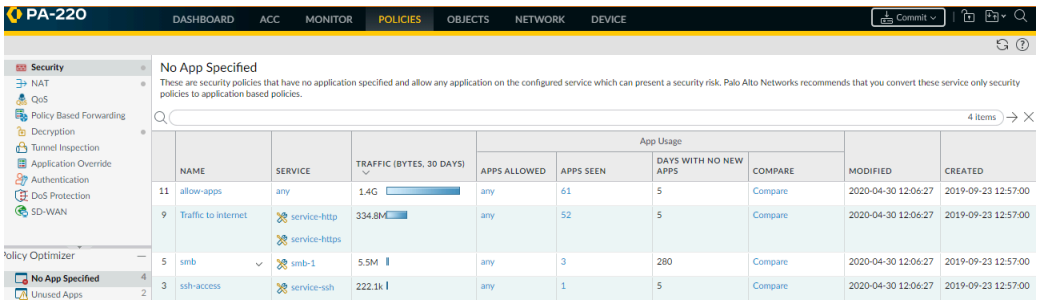
従来のファイアウォールから Palo Alto Networks の次世代ファイアウォールに移行する際、ポート上でアプリケーションを許可する大量のポートベースのルールを引き継ぐことになり、どのアプリケーションもオープンなポートを使用できるため、攻撃の入り口が増加します。Policy Optimizer はレガシーなポート ベースのセキュリティポリシー ルールに見られるすべてのアプリケーションを特定し、ルールで許可すべきアプリケーションを簡単に選択できるワークフローを提供します。ポートベースのルールからアプリケーション ベースのルールに移行して攻撃の入り口を減らし、ネットワーク上のアプリケーションを安全に使用できるようにします。Policy Optimizer を使用して新しいアプリケーションを追加する際にルールベースを保守します。

優先順位を付け、いくつかのポートベースのルールを一度にアプリケーション ベースのルールへと移行させます。徐々に変換していくことで、大きなルールベースを一度に移行する場合よりも安全性が高まり、新しいアプリケーション ベースのルールが必要なアプリケーションの確実な制御が容易になります。***Policy Optimizer*** を使用し、最初に変換するルールの優先順位を決めます。

従来のファイアウォールから *Palo Alto Networks* デバイスに設定を移行するには、アプリケーション ベースのポリシーに移行する際のベストプラクティスを参照してください。

STEP 1 | ポートベースのルールを特定します。

ポートベースのルールには設定済みの (許可された) アプリケーションがありません。**Policies (ポリシー)** > **Security (セキュリティ)** > **Policy Optimizer** > **No App Specified (アプリの指定なし)** には、すべてのポートベースのルールが表示されます (**Apps Allowed (許可されたアプリ)** が **any (すべて)**)。



STEP 2 | 最初に変換するポートベースのルールの優先順位を決めます。

Policies (ポリシー) > **Security (セキュリティ)** > **Policy Optimizer** > **No App Specified (アプリの指定なし)** では、ルールベースにおける順序を変えずにルールを並び替えることができ、またビジネス ゴールやリスクの許容度に基づいて変換するルールの優先順位を決める際に役立つ情報を閲覧できます。

- **Traffic (Bytes, 30 days) (トラフィック (バイト、30 日))**– (クリックして並び替えます)。 現在最も多くトラフィックにマッチするルールがリストの一番上に表示されます。これがデフォルトの順序です。
- **Apps Seen (発見されたアプリ)**– (クリックして並び替え) ポートベースのルールに正当なアプリケーションが大量にマッチする場合、アプリケーション、ユーザー、送信元および宛先を細かく定義した複数のアプリケーション ベースのルールで置き換えるべきかもしれません。例えば、単一のポートベースのルールが複数のデバイス上で異なるユーザーグループについて複数のアプリケーションのトラフィックを制御している場合、正当なユーザーおよびデバイスを持つアプリケーションをペアにするルールを個別に作成することで、攻撃の入り口を減らして可視性を高められます。(**Apps Seen (発見されたアプリ)** の数または **Compare (比較)** をクリックすると、ルールに一致したアプリケーションが表示されます)

  ファイアウォール は約 *1* 時間ごとに ***Apps Seen (発見されたアプリ)*** を更新します。ただし、アプリケーション トラフィックあるいはルールが大量にある場合、更新に *1* 時間以上かかる場合があります。アプリケーションをルールに追加した後、少なくとも *1* 時間待ってからトラフィック ログを実行し、アプリケーションのログ情報を確認します。

- **Days with No New Apps (新規アプリがない日数)**– (クリックして並び替え)。 ポートベースのルールに見られるアプリケーションが定まったら、ルールの成長度が高く、変換によって不意に正当なアプリケーションが除外されることがなく、ルールにマッチする新しいアプリケーションが今後は発生しない可能性が高くなります。最近変更されていない古

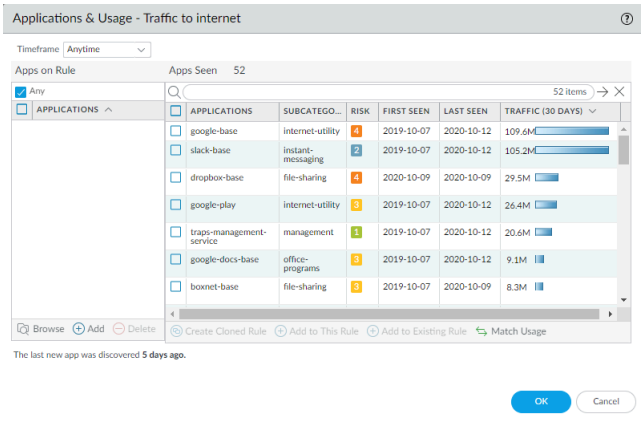
いルールはより安定している可能性が高いため、**Created** (作成) および **Modified** (変更) 日を使用すれば、ルールの成長度を判断しやすくなります。

- **Hit Count** (ヒット数)—選択した期間中に最もマッチが多いルールを表示します。ヒット カウンターをリセットするルールを除外し、日単位で除外期間を指定できます。最近ヒット カウンターがリセットされたルールを除外すれば、カウンターがリセットされたことを知らないために、ルールのヒット数が予想よりも少ないと誤解することがなくなります。

また、***Hit Count*** (ヒット数) を使用してポリシー ルールの使用状況を表示するを行い、未使用のルールを特定し削除することによって、セキュリティ リスクを軽減し、ルールベースを整理しておくことができます。

STEP 3 | 優先順位の高いルールから順に、ポートベースのルールで **Apps Seen** (発見されたアプリ) を確認します。

No Apps Specified (アプリの指定なし) で **Compare** (比較) あるいは **Apps Seen** (発見されたアプリ) の数をクリックして **Applications & Usage** (アプリケーションおよび使用状況) を開くと、特定の **Timeframe** (期間) 中にポートベースのルールにマッチしたアプリケーションが一覧表示され、各アプリケーションの **Risk** (リスク)、**First Seen** (初回発見日)、**Last Seen** (最終最後に表示日)、過去 30 日間のトラフィック量が表示されます。



過去 7、15、30 日、あるいはルールの存在期間 (**Anytime** (全期間)) に基づいてポートベースのルールの **Applications seen** (発見されたアプリケーション) をチェックできます。ルールを移行する際、**Anytime** (全期間) を使用すればルールにマッチしたアプリケーションの全体像を把握できます。

Apps Seen (発見されたアプリ) を検索したりフィルタリングしたりすることができますが、**Apps Seen** (発見されたアプリ) の更新には 1 時間以上かかるということにご注意ください。また、列の見出しをクリックすしても **Apps Seen** (発見されたアプリ) を並び替えることができます。例えば、**Traffic (30 days)** (トラフィック (30 日間)) をクリックすれば最新のトラフィックをリストの一番上に表示し、**Subcategory** (サブカテゴリ) をクリックすればサブカテゴリに基づいてアプリケーションを整頓することができます。

First Seen (初回発見日) と ***Last Seen*** (最終発見日) の精度は *1* 日であるため、ルールを定義した日は、これら *2* つの列の日付が同じになります。ファイアウォールがアプリケーション上でトラフィックを発見してから *2* 日後、日付の表示が変わります。

STEP 4 | アプリケーションをルールにコピーあるいは追加すれば、ルールで許可したいアプリケーションを指定できます。

Applications & Usage (アプリケーションおよび使用状況)では、次の 2 つの内いずれかの方法でポートベースのルールをアプリケーション ベースのルールに変換します：

- ルールをコピー—元のポートベースのルールを保持し、ルールベースでそのすぐ上にコピーしたアプリケーション ベースのルールを配置します。
- アプリケーションをルールに追加—元のポートベースのルールを新しいアプリケーションベースのルールで置き換え、元のルールを削除します。

> 既存のアプリケーションベースのルールがあり、ポートベースのルールからアプリケーションを移行する場合は、新しいルールをコピーしたり、アプリケーションを追加してポートベースのルールを変換したりする代わりに、アプリケーションを既存のルールに追加できます。

一部のアプリケーションは、四半期や *1* 年に一度など、定期的にネットワークに現れます。その最新のアクティビティを補足できるほど履歴がたまっていない場合、これらのアプリケーションが ***Applications & Usage*** (アプリケーションおよび使用状況) 画面に表示されない場合があります。

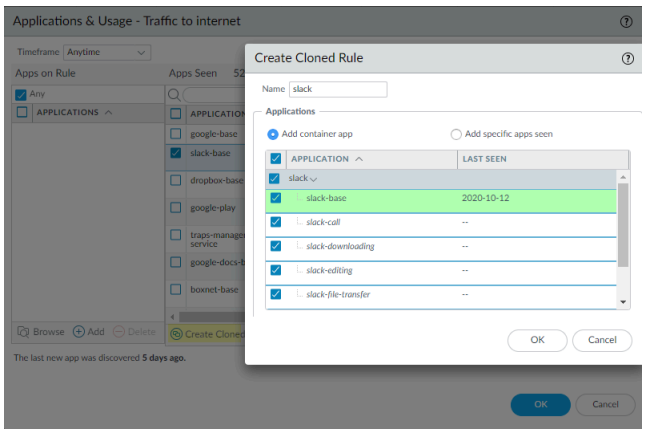
ルールをコピー、あるいはアプリケーションをルールに追加する際、元のルールは一切変更されません。元のルールの設定は、ルールに追加したアプリケーションを除いて同じままになります。例えば、元のルールのサービスが ***Any*** (すべて) のアプリケーションを許可していた、あるいは特定のサービスを指定していた場合、サービスを ***Application-Default*** (アプリケーション デフォルト) に変更し、許可されたアプリケーションを新しいルールのデフォルトのポートに限定する必要があります。

コピーを行うことは、特に **Applications & Usage** (アプリケーションおよび使用状況) にルールに一致する複数の既知のアプリケーションが場合、ルールを移行する最も安全な方法です(ルールコピー移行のユースケース：ウェブ閲覧および SSL トラフィックにこの例を示しています)。コピーを行うと元のポートベースのルールが保持されてコピーしたポートベースのルールの下にそれが配置され、コピーしたルールにマッチしないトラフィックはポートベースのルールを通るため、アプリケーションの可用性を損なうリスクがなくなります。正当なアプリケーションから来るトラフィックが合理的な期間中にポートベースのルールにヒットしなかった場合、それを削除してルールの移行を完了できます。

ポートベースのルールをコピーする方法：

1. **Apps Seen** (発見されたアプリ) でコピーしたルール内の任意の各アプリケーションの隣にあるチェックボックスをクリックします。**Apps Seen** (発見されたアプリ) の更新には 1 時間以上かかりますので、ご注意ください。
2. **Create Cloned Rule** (ルールのコピーを作成) をクリックします。**Create Cloned Rule** (ルールのコピーを作成) ダイアログで、コピーしたルールに **Name** (名前) を付け (この例では「slack」)、同じコンテナ内に他のアプリケーションを、必要な場合はアプリケーション

の依存関係を追加します。例えば、slack ベースのアプリケーションを選択してルールをコピーするには：



緑色のテキストが選択中のコピー対象のアプリケーションです。コンテナ アプリケーション (**slack**) はグレーの行にあります。イタリック体で列挙されているアプリケーションは、ルールで見つかっていないものの、選択中のアプリケーションと同じコンテナに存在するアプリケーションです。ルールで発見された個々のアプリケーションは通常のフォントで表示されます。ルールが後に壊れないようにするために、アプリケーションはデフォルトですべてのコピーされたルールに含まれます (コンテナ内のすべてのアプリケーションを追加する **Add Container App (**コンテナ アプリの追加**)** がデフォルトで選択されています)。

3. コンテナ内のすべてのアプリケーションを許可する場合は、**Add container app (**コンテナ アプリの追加**)** を選択したままにします。またこれにより、アプリケーションをコンテナ アプリに追加する際、自動的にルールに追加されるため、将来にも対応できるルールを作ることができます。

   アクセスをコンテナ内の一部のアプリケーションに制限する場合は、ユーザーへのアクセスを制限したい各アプリケーションの隣にあるボックスのチェックを外します。これによりコンテナ アプリのチェックも外れるため、後に新しいアプリケーションをコンテナで許可したい場合は、それらのアプリケーションを個別に追加する必要があります。

   コンテナ アプリのチェックを外すとすべてのアプリのチェックが外れ、コピーしたルールに含めるアプリを手動で選択することになります。

4. アプリケーションの依存関係が Application (アプリケーション) の下のボックスに表示されている場合 (この例ではありません)、チェックしたままにします。選択したアプリケーションを実行するには、それらのアプリケーションの依存関係が必要です。一般的な依存関係には **ssl** と **web-browsing** が含まれます。
5. **OK** をクリックしてルールベースにあるポートベースのルールのすぐ上に新しいアプリケーション ベースのルールを追加します。
6. 設定を **Commit**（コミット）します。

ルールをコピーして設定を **Commit (**コミット**)** すると、コピーしたルール用に選択したアプリケーションが元のポートベースのルールの **Apps Seen (**発見されたアプリ**)** リストから削除されます。例えば、ポートベースのルールに 16 件の **Apps Seen (**発見されたアプリ**)** があり、2 つのアプリケーションと 1 つの依存関係であるアプリケーションをコピーしたルール用に選択する場合、選択した 3 つのアプリケーションがポートベースのルールから削除されたため、ポートベースのルールに 13 件の **Apps Seen (**発見されたアプリ**)** が表示されます

(16-3 = 13)。コピーしたルールは **Apps on Rule (**ルールのアプリ**)** で 3 件の追加したアプリケーションを表示します。

コンテナ アプリを伴うルールのコピーを作成する場合は少し異なります。例えば、ポートベースのルールに 16 件の **Apps Seen (**発見されたアプリ**)** があり、1 つのアプリケーションとコンテナ アプリをコピーするルール用に選択します。コンテナ アプリには 5 つのアプリケーションと 1 つの依存関係のアプリケーションがあります。コピーした後、コピーしたルールは 7 件の **Apps on Rule (**ルールのアプリ**)** (個々のアプリケーション、コンテナ アプリ内の 5 つのアプリケーション、コンテナ アプリ用の依存関係のアプリケーション) を表示します。しかし、ポートベースのルールから削除されたのが個々のアプリケーション、コンテナ アプリ、コンテナ アプリの依存関係のアプリケーションだけであるため、元のポートベースのルールでは、**Apps Seen (**発見されたアプリ**)** に 13 件のアプリケーションが表示されます。

コピーとは異なり、アプリケーションをポートベースのルールに追加すると、新しいアプリケーション ベースのルールに置き換えられます。アプリケーションをルールに追加することはコピーを行うよりも単純な作業ですが、ルールに置くべきアプリケーションを見落とし、見落とされたものをカバーする元のポートベースのルールがルールベースに存在しなくなるため、リスクが高まります。しかし、少数のよく知られたアプリケーションに適用するポートベースのルールにアプリケーションを追加することで、素早くルールをアプリケーション ベースのルールに移行できます。例えば、TCP ポート 22 に向かうトラフィックだけを制御するポートベースのルールの場合、正当なアプリケーションは SSH だけであるため、アプリケーションをルールに追加しても安全です。

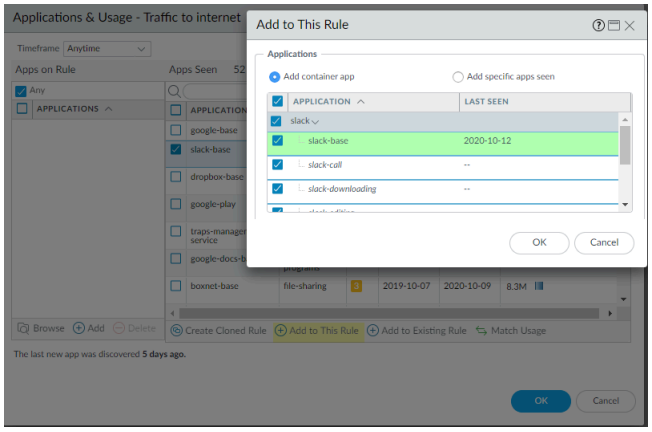
従来型のセキュリティポリシー ルールの ***Application (***アプリケーション***)*** タブを使ってアプリケーションを追加しても、***Apps Seen (***発見されたアプリ***)*** や ***Apps on Rule (***ルールのアプリ***)*** は変更されません。正確なアプリケーション使用状況情報を維持するため、ポートベースのルールをアプリケーション ベースのルールで置き換える際、***Apps Seen (***発見されたアプリ***)*** で ***Add to This Rule (***このルールに追加***)*** あるいは ***Match Usage (***使用状況と一致***)*** を使ってアプリケーションを追加します (あるいはその代わりにコピーしたルールを作成するか、アプリケーションを既存のアプリケーション ベースのルールに追加します)。

アプリケーションを追加してポートベースのルールをアプリケーション ベースのルールで置き換える方法は 3 つあります (**Apps Seen (**発見されたアプリ**)** の **Add to This Rule (**このルールに追加**)** および **Match Usage (**使用状況と一致**)**、**Apps on Rule (**ルールのアプリ**)** の **Add (**追加**)**):

- **Apps Seen (**発見されたアプリ**)** からアプリケーションを **Add to This Rule (**このルールに追加**)** します (ルールにマッチしたアプリケーション)。**Apps Seen (**発見されたアプリ**)** の更新には 1 時間以上かかりますので、ご注意ください。

  1. ルールの **Apps Seen (**発見されたアプリ**)** からアプリケーションを選択します。
  2. **Add to This Rule (**このルールに追加**)** をクリックします。**Add to This Rule (**このルールに追加**)** ダイアログで、同じコンテナ アプリ内の他のアプリケーションを追加し、必要

な場合はアプリケーションの依存関係を追加します。例えば、slack ベースをルールに追加するには：



Create Cloned Rule (ルールのコピーを作成) ダイアログと同様に、**Add to This Rule** (このルールに追加) にある緑色のテキストは、ルールに追加するために選択中であるアプリケーションです。コンテナ アプリ (**slack**) はグレーの行にあります。イタリック体で列挙されているアプリケーションは、ルールで見つかっていないものの、選択中のアプリケーションと同じコンテナに存在するアプリケーションです。ルールで発見された個々のアプリケーションは通常のフォントで表示されます。ルールが後に壊れないようにするために、アプリケーションはデフォルトですべてのコピーされたルールに含まれます (コンテナ内のすべてのアプリケーションを追加する **Add Container App** (コンテナ アプリの追加) がデフォルトで選択されています)。

3. コンテナ内のすべてのアプリケーションを許可する場合は、**Add container app** (コンテナ アプリの追加) を選択したままにします。またこれにより、アプリケーションをコンテナ アプリに追加する際、自動的にルールに追加されるため、将来にも対応できるルールを作ることができます。

   アクセスをコンテナ内の一部のアプリケーションに制限する場合は、ユーザーへのアクセスを制限したい各アプリケーションの隣にあるボックスのチェックを外します。これによりコンテナ アプリのチェックも外れるため、後に新しいアプリケーションをコンテナで許可したい場合は、それらのアプリケーションを個別に追加する必要があります。

   コンテナ アプリのチェックを外すとすべてのアプリのチェックが外れ、コピーしたルールに含めるアプリを手動で選択することになります。

4. アプリケーションの依存関係が Application (アプリケーション) の下のボックスに表示されている場合 (この例ではありません)、チェックしたままにします。選択したアプリケーションを実行するには、それらのアプリケーションの依存関係が必要です。

5. **OK** をクリックしてポートベースのルールを新しいアプリケーション ベースのルールで置き換えます。

Add to This Rule (このルールに追加) して設定を **Commit** (コミット) すると、追加しなかったアプリケーションは新しいアプリケーション ベースのルールが許可しなくなるため、**Apps Seen** (発見されたアプリ) から削除されます。例えば、ルールに 16 件の **Apps Seen** (発見されたアプリ) があり、3 つのアプリケーションを **Add to This Rule** (このルール

に追加) する場合、新しいルールは **Apps Seen** (発見されたアプリ) で追加した 3 つのアプリケーションしか表示しません。

コンテナ アプリで **Add to This Rule** (このルールに追加) する場合は少し異なります。例えば、ポートベースのルールに 16 件の **Apps Seen** (発見されたアプリ) があり、新しいルールに追加する 1 つのアプリケーションとコンテナ アプリを選択します。コンテナ アプリには 5 つのアプリケーションと 1 つの依存関係のアプリケーションがあります。ルールにアプリケーションを追加した後、新しいルールは 7 件の **Apps on Rule** (ルールのアプリ) (個々のアプリケーション、コンテナ アプリ内の 5 つのアプリケーション、コンテナ アプリ用の依存関係のアプリケーション) を表示します。しかし、個々のアプリケーション、コンテナ アプリ、コンテナ アプリの依存関係のアプリケーションがリストから削除されたため、**Apps Seen** (発見されたアプリ) に 13 件のアプリケーションが表示されます。

- ルールの **Apps Seen** (発見されたアプリ) をすべて一度にワンクリックでルールに追加します (**Match Usage** (使用状況と一致))。

  ポートベースのルールはすべてのアプリケーションを許可するため、***Apps Seen*** (発見されたアプリ) に不要な安全でないアプリケーションが含まれる場合があります。正当なビジネス上の目的を持つ少数のよく知られたアプリケーションがルールに見られる場合だけ、***Match Usage*** (使用状況と一致) を使ってルールを変換してください。*SSH* トラフィックだけを許可する *TCP* ポート *22* が良い例です。ポート *22* を開くポートベースのルールに見られるアプリケーションが *SSH* だけである場合、安全に ***Match Usage*** (使用状況と一致) できます。

  1. **Apps Seen** (発見されたアプリ) で **Match Usage** (使用状況と一致) をクリックします。**Apps Seen** (発見されたアプリ) の更新には 1 時間以上かかりますので、ご注意ください。**Apps Seen** (発見されたアプリ) のすべてのアプリケーションが **Apps on Rule** (ルールのアプリ) にコピーされます。
  2. **OK** をクリックしてアプリケーション ベースのルールを作成し、ポートベースのルールと置き換えます。

- ルールに入れたいアプリケーションが分かっている場合は、**Apps on Rule** (ルールのアプリ) で手動でアプリケーションを **Add** (追加) できます。しかし、この方法は従来型のセキュリティポリシー ルールの **Application** (アプリケーション) タブを使う場合と同じであり、**Apps Seen** (発見されたアプリ) や **Apps on Rule** (ルールのアプリ) は変更されません。正確なアプリケーション使用状況情報を維持するために、**Apps Seen** (発見されたアプリ) で **Add to This Rule** (ルールに追加)、**Create Cloned Rule** (ルールのコピーを作成)、または **Match Usage** (使用状況と一致) を使ってルールを変換します。

  1. **Apps on Rule** (ルールのアプリ) でルールに加えるアプリケーションを **Add** (追加) (あるいは **Browse** (参照)) して選択します。これは、**Application** (アプリケーション) タブでアプリケーションを追加するのと同じです。
  2. **OK** をクリックしてアプリケーションをルールに追加し、ポートベースのルールを新しいアプリケーション ベースのルールで置き換えます。

     この方法は ***Application*** (アプリケーション) タブを使ってアプリケーションを追加するのと同じであるため、アプリケーションの依存関係を追加するためのダイアログは表示されません。

STEP 5 | 各アプリケーション ベースのルールについて、**Service (サービス)** を **application-default** に設定します。

ビジネスニーズに基づき、アプリケーション (例えば、内部カスタム アプリケーション) を特定のクライアントおよびサーバー間の標準的でないポート上で許可する必要がある場合、必要なアプリケーション、送信元、宛先にだけ例外を認めます。アプリケーションのデフォルトのポートを使用するよう、カスタム アプリケーションを書き換えることを検討してください。

STEP 6 | 設定を **Commit**（コミット）します。

STEP 7 | ルールを監視します。

- コピーしたルール—元のポートベースのルールを監視し、アプリケーション ベースのルールが目的のトラフィックにマッチすることを確認します。許可したいアプリケーションがポートベースのルールにマッチする場合、それをアプリケーション ベースのルールに追加するか、それ用に別のアプリケーション ベースのルールをコピーします。長期間、ネットワークに入れたくないアプリケーションだけがポートベースのルールにマッチする場合、コピーしたルールは堅牢であり (制御したいアプリケーション トラフィックをすべて捕捉します)、安全に削除することができます。
- アプリケーションを追加したルール—少数のよく知られたアプリケーションを持つポートベースのルールだけを直接アプリケーション ベースのルールに変換するため、大抵の場合、ルールは最初から堅牢です。変換したルールを監視し、目的のトラフィックがルールにマッチすることを確認します。予想よりもトラフィックが少ない場合、ルールが必要なアプリケーションの一部を許可していない可能性があります。予想よりもトラフィックが多い場合、不要なトラフィックをルールが許可している可能性があります。ユーザーからフィードバックを得てください。ユーザーがビジネス上の目的で必要なアプリケーションにアクセスできない場合、ルール (あるいはベルのルール) が厳格過ぎます。

ルールコピー移行のユースケース：ウェブ閲覧および SSL トラフィック

TCP ポート 80 (HTTP ウェブブラウジング) および 443 (HTTPS SSL) でのウェブアクセスを許可するポートベースの規則では、どのアプリケーションがこれらのオープンポートを使用するかを制御できません。多くのウェブアプリケーションがあるため、ウェブトラフィックを許可する一般的な規則では何千ものアプリケーションを許可していますが、その多くはネットワーク上では不要です。

この使用事例では、すべてのウェブアプリケーションを許可するポートベースのポリシーを、必要なアプリケーションだけを許可するアプリケーションベースのポリシーに移行する方法を示します。そのため、許可することを選択したアプリケーションを安全に有効にできます。多くのアプリケーションを扱うルールの場合は、追加することでポートベースのルールが置き換えられるため、元のポートベースのルールをコピーする方が、ルールにアプリケーションを追加するよりも安全です。また、ポートベースのルールにも代わる **Match Usage (使用状況を一致)** させる場合は、そのルールで確認されているすべてのアプリケーションを許可することになります。これは、特にウェブ閲覧トラフィックでは危険です。

ルールをコピーすると、元のポートベースのルールが保持され、コピーされたルールがルールベースのポートベースのルールの真上に配置されるため、ルールを監視できます。コピーすると、ポートベースのウェブトラフィックルールなど、多数の異なるアプリケーションを参照するルールを複数のアプリケーションベースのルールに分割して、異なるグループのアプリケーションを異なる方法で処理することもできます。コピールールで許可する必要があるすべてのアプリケーションを許可していると確信できる場合は、ポートベースのルールを削除できます。

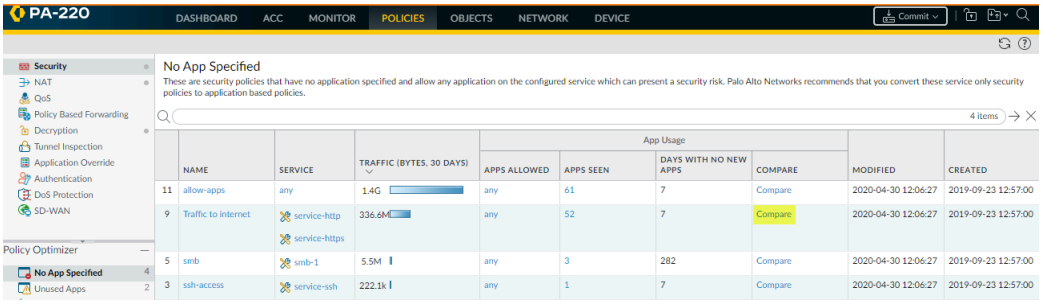
この例では、ポートベースのウェブトラフィックルールをコピーして、Webベースのファイル共有トラフィック用のアプリケーションベースのルール (ポートベースのルールに表示されるアプリケーショントラフィックのサブセット) を作成します。

この例は、 の新しい App Viewer を使用して *App-ID* クラウド エンジン *(ACE)* アプリケーションを複製する場合には適用されません (この方法の例については、 ACE のドキュメントを参照してください)。*ACE* には SaaS セキュリティ インライン ライセンスが必要です。

STEP 1 | **Policies (ポリシー)** > **Security (セキュリティ)** > **Policy Optimizer** > **No App Specified (アプリケーションの指定なし)** に移動し、ポートベースのルールを表示します。

STEP 2 | 移行するルールで **Compare (比較)** をクリックします。

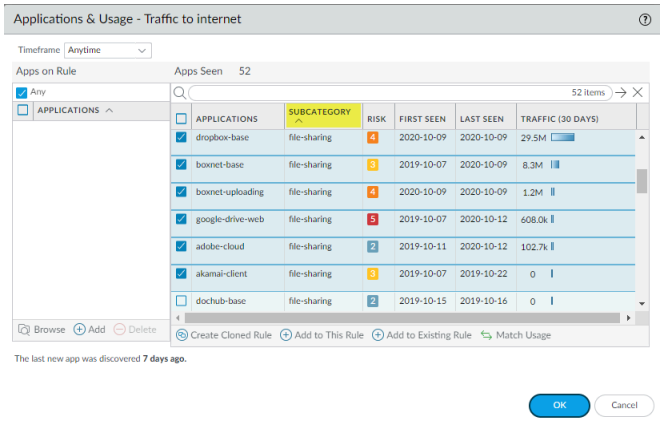
この例では、ウェブアクセスを許可するポートベースのルールは Traffic to internet と名付けられています。



STEP 3 | 並べ替えオプションを使用して、**Apps Seen (**発見されたアプリ**)** から許可するアプリケーションを確認して選択します。

> ***Apps Seen (***発見されたアプリ***)*** の数はほぼ毎時間更新されるため、表示されるアプリケーションの数が想定より少ない場合は、およそ *1* 時間後にもう一度確認します。ファイアウォールの負荷によっては、これらのフィールドが更新されるまでに *1* 時間以上かかることがあります。

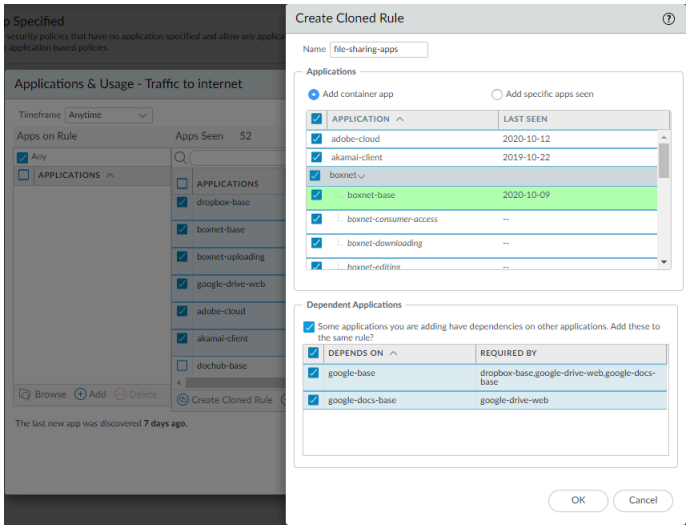
たとえば、**Subcategory (**サブカテゴリ**)** をクリックしてアプリケーションを並べ替えファイル共有サブカテゴリまでスクロールして、許可するアプリケーションを選択します。もしくは、ファイル共有アプリケーションをフィルタリング (検索) することもできます。



STEP 4 | **Create Cloned Rule (**複製されたルールを作成**)** を実行し、複製されたルールの **Name (**名前**)** を付けます (この例のファイル共有アプリケーション)。

Create Cloned Rule (ルールのコピーを作成**)** では、選択したアプリケーションが影付きの緑色、コンテナアプリケーションが影付きの灰色、コンテナ内の個別のアプリケーションがイタリック体、個別のアプリケーションが通常のテキストフォントで表示されま

す。**Applications** (アプリケーション) をスクロールすると、すべてのコンテナアプリケーションとその個々のアプリケーションが表示されます。



Create Cloned Rule (ルールのコピーを作成) には、選択したアプリケーションに依存するアプリケーションも表示されます。この例では、選択したアプリケーションの一部は実行のために google-base および google-docs-base アプリケーションを要求 します (**Required By**(が要求))。

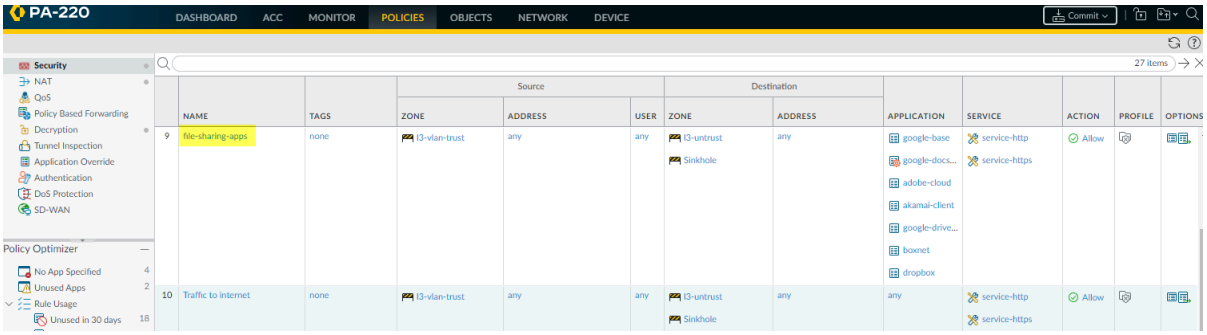
STEP 5 | コピーしたルールに含めるアプリケーションを選択します。

含めたくないアプリケーションである場合は、対応するボックスのチェックを外します。これにより、コンテナアプリケーションのチェックも外れます。コンテナアプリを含めない場合、新しいアプリがコンテナに追加されても自動的にルールに追加されることはありません。

コンテナアプリをオフにすると、コンテナ内にある個々のアプリケーションはすべてオフになり、手動で追加するアプリケーションを選択する必要があります。

STEP 6 | **OK** をクリックして、コピールールを保存します。

STEP 7 | **Policies** (ポリシー) > **Security** (セキュリティ) では、コピーされたルール (file-sharing-apps) は、元のポートベースのルール (インターネットへのトラフィック) の上のルールベースに挿入されます。



STEP 8 | 元のポートベースのルールのプロパティを継承するコピールールを編集するには、ルール名をクリックします。

STEP 9 | **Service/URL Category** (サービス/ **URL** カテゴリ) タブで、**Service** (サービス) から service-http と service-https を削除します。

これにより、**Service** (サービス) が **application-default** (アプリケーションのデフォルト) に変更され、アプリケーションが標準以外のポートを使用することを防ぎ、さらに攻撃の入り口を減らすことができます。

ビジネスニーズに基づき、アプリケーション (例えば、内部カスタム アプリケーション) を特定のクライアントおよびサーバー間の標準的でないポート上で許可する必要がある場合、必要なアプリケーション、送信元、宛先にだけ例外を認めます。アプリケーションのデフォルトのポートを使用するよう、カスタム アプリケーションを書き換えることを検討してください。

STEP 10 | **Source** (送信元)、**User** (ユーザー)、および **Destination** (宛先) タブで、適切な場所 (ゾーン、サブネット) にある適切なユーザーのみに適用されるようにルールを厳しくします。

たとえば、Web ファイル共有アクティビティを、Web 全体でファイルを共有するビジネス上の理由があるユーザーグループのみに制限することを決定できます。

STEP 11 | **OK** をクリックします。

STEP 12 | 設定を **Commit**（コミット）します。

STEP 13 | アプリケーションベースのルールで、ネットワーク上で許可したいアプリケーションのみが許可されるまで、ポートベースのウェブアクセスルールにおける他のアプリケーションカテゴリについてもこのプロセスを繰り返します。

許可するトラフィックが、元のポートベースのルールが不要になったことを確認するのに十分な時間だけヒットを停止した場合は、そのポートベースのルールをルールベースから削除できます。

アプリケーションを既存のルールに追加

場合によっては、ポートベースのルールで学習した (発見した) アプリケーションを既存のルールに追加することもあります。例えば、管理者がインターネットアクセスを許可するポートベースのルール (ポート 80/443 ルール) から、一般的なビジネス Web アプリケーション用のコピーしたアプリケーション ベースのルールを作成する可能性があります。後ほど、この管理者はインターネットアクセス ルールがより多くの一般ビジネスアプリケーションを発見していることに気づき、同じタイプのアプリケーション用の別のアプリケーション ベースのルールをコピーすると、不要なルールが作成されてルールベースが複雑になるため、それらの一部あるいはすべてをコピーしたアプリケーション ベースのルールに追加したいと考えます。

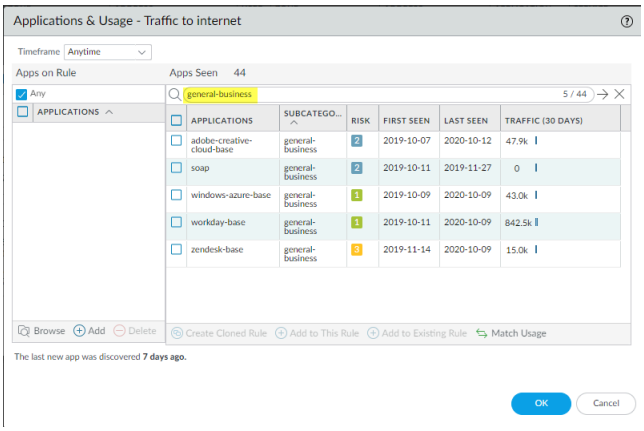
この例では、一般的なビジネス・トラフィックを制御するアプリケーション・ベースのセキュリティー・ポリシー・ルールが既に存在するか、ポート・ベースのインターネット・アクセス・ルールから複製されていることを前提としています (ルールコピー移行のユースケース：ウェブ閲覧および SSL トラフィック と同様)。この例では、ポートベースのインターネット アクセス ルールからアプリケーションベースのルールを複製し、新しいルールのサービスを application-

default に変更して、Web ベースのアプリケーションが非標準ポートを使用しないようにしました。

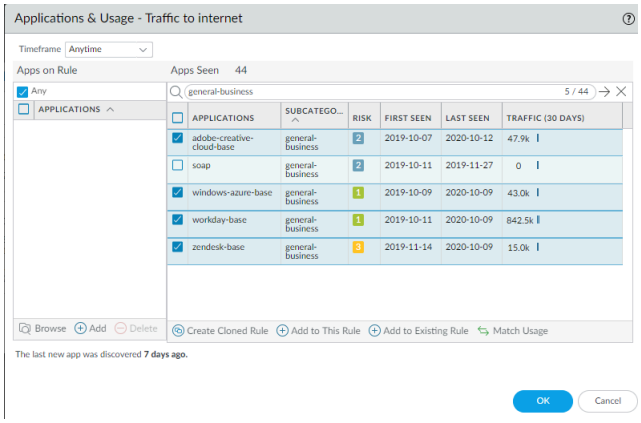
既存のアプリケーションベースのルールにアプリケーションを追加することに加えて、既存のポートベースのルールにアプリケーションを追加できます。この操作により、ポートベースのルールは、ルールに追加するアプリケーションのアプリケーションベースのルールに変換されます。これを行う場合は、ルールに移動し、サービスを *application-default* に変更して、アプリケーションが非標準ポートを使用しないようにします（ルールで設定されたサービスがアプリケーションと一致しない場合もあります）。

この例は、の新しい App Viewer を使用して *App-ID* クラウド エンジン *(ACE)* アプリケーションを既存のルールに追加する場合には適用されません (これを行う方法については、 ACE のドキュメントを参照してください)。*ACE* には SaaS セキュリティ インライン ライセンスが必要です。

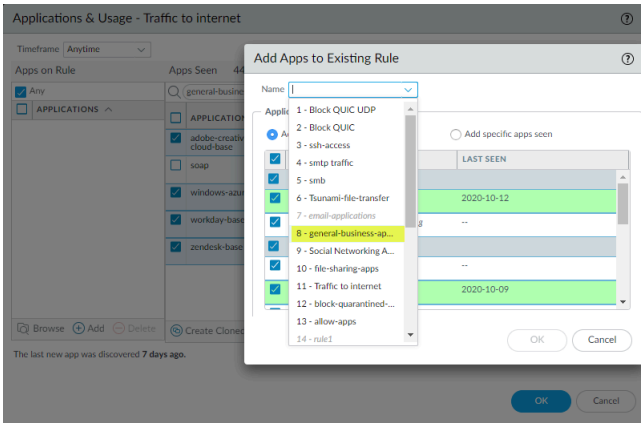
STEP 1 | ポートベースのインターネット アクセス ルールを確認すると、ルールが一般的なビジネスアプリケーションを認識しており、ビジネス目的でそれらの一部を許可する必要があることが分かります。



STEP 2 | 既存のルールに追加したい一般ビジネスアプリを選択します。



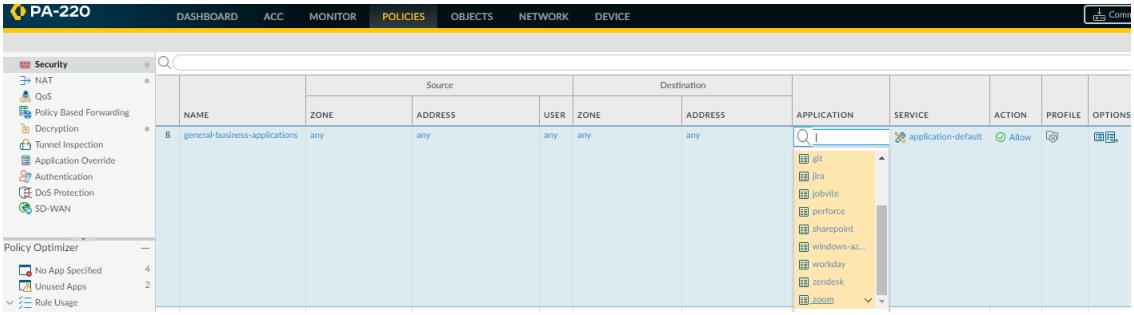
STEP 3 | **Add to Existing Rule** (既存のルールに追加) をクリックしてアプリケーションを追加したいルールの **Name** (名前)を選択します。この例では、**general-business-applications** (一般ビジネス アプリケーション)です。



STEP 4 | 選択したアプリケーションを **general-business-applications** (一般ビジネスアプリケーション) ルールに追加するには、**Add Apps to Existing Rule** (アプリを既存のルールに追加)で **OK** をクリックします。

STEP 5 | **Applications & Usage** (アプリケーションと使用状況) で**OK** をクリックします。

STEP 6 | 更新されたルールが、元のルール上のアプリケーションおよび先ほど追加したアプリケーションを制御するようになります。



未使用のアプリケーションがあるセキュリティポリシールールを特定

大量のアプリケーションを許可するアプリケーション ベースのセキュリティ ポリシー ルールがある場合、未使用のアプリケーション (ルールに存在しないアプリケーション) を除去してルールを整理し、ルールに一致するトラフィックに実際に存在するアプリケーションを許可するようにすることができます。未使用のアプリケーションを特定してセキュリティポリシールールから除去することは、攻撃の入り口を減らしてセキュリティを高められるため、ベストプラクティスになります。

STEP 1 | 未使用のアプリケーションがあるセキュリティポリシールールを特定します。

Policies (ポリシー) > **Security** (セキュリティ) > **Policy Optimizer** (ポリシー オプティマイザ) > **Unused Apps** (未使用のアプリ) は、ルールに一致し (表示され) ないアプリケーションで設定されたすべてのアプリケーションベースのルールを表示します。これは、これらのルールに

より、ネットワークで使用できないアプリケーションが許可されること (または、別のルールがルールをシャドウするため、ルールに一致すると予想されるトラフィックは、ルールベースの以前のルールに一致すること)を意味します。

> ***Apps Allowed*** **(**許可されたアプリ**)** および ***Apps Seen*** **(**発見されたアプリ**)** の数は約 *1* 時間毎に更新されるため、ルールでアプリケーションを設定して予想よりも ***Apps Allowed*** **(**許可されたアプリ**)** の数が少ない場合、*1* 時間後に再びチェックしてください。ファイアウォールの負荷によっては、これらのフィールドが更新されるまでに *1* 時間以上かかることがあります。

STEP 2 | 未使用のアプリケーションを伴うどのルールを優先して最初に変更するのか指定します。

Policies (ポリシー**)** > **Security (**セキュリティ**)** > **Policy Optimizer** > **Unused Apps (**未使用のアプリ**)**では、ルールベースにおける順序を変えずにルールを並び替えることができ、またビジネス ゴールやリスクの許容度に基づいて整理するルールの優先順位を決める際に役立つ情報を閲覧できます。

- **Apps Allowed (**許可されたアプリ**)** (許可リストのアプリケーションの数) と **Apps Seen (**発見されたアプリ**)** (ルールに実際に見られる許可されたアプリケーションの数) の差から、各ルールで設定されていながら、ルールに実際に見られないアプリケーションの数 (ルールの設定がどれだけ過剰かを示唆) を把握できます。**Apps Allowed (**許可されたアプリ**)** をクリックすればルールで許可されているアプリケーションに基づいて、**Apps Seen (**発見されたアプリ**)** をクリックすればルールに実際に見られるアプリケーションの数に基づいて並び替えを行うことができます。
- **Days with No New Apps (**新規アプリがない日数**)** (クリックして並び替え) には、新しいアプリケーションがルールに最後にヒットしてから経過した日数が表示されます。これはルールの成長度を示唆し、すでに発見されているアプリケーションは対象外になります。**Days with No New Apps (**新規アプリがない日数**)** が長いほど、新しいアプリケーションがルールにヒットする可能性が小さくなり、ルールがすべてのアプリケーションを許可している可能性が高くなります。
- また、**Created (**作成**)** および **Modified (**変更**)** 日も、ルールに見られないアプリケーションが後に見つかる可能性があるかどうか、ルールにヒットすることが予想されるすべてのアプリケーションをルールが見つけたかどうかを理解できるほど高い成長度をルールが持っているかどうかを判断するのに役立ちます。ルールが **Modified (**変更**)** されてからの経過時間が長いほど、ルールの成長度が高くなります。(**Created (**作成**)** および **Modified (**変更**)** が同じ場合、ルールは変更されていません)
- **Hit Count (**ヒット数**)**—選択した期間中に最もマッチが多いルールを表示します。ヒット カウンターをリセットするルールを除外し、日単位で除外期間を指定できます。最近ヒット カウンターがリセットされたルールを除外すれば、カウンターがリセットされたことを知らないために、ルールのヒット数が予想よりも少ないと誤解することがなくなります。

  > ***Hit Count*** を ポリシー ルールの使用状況を表示する.

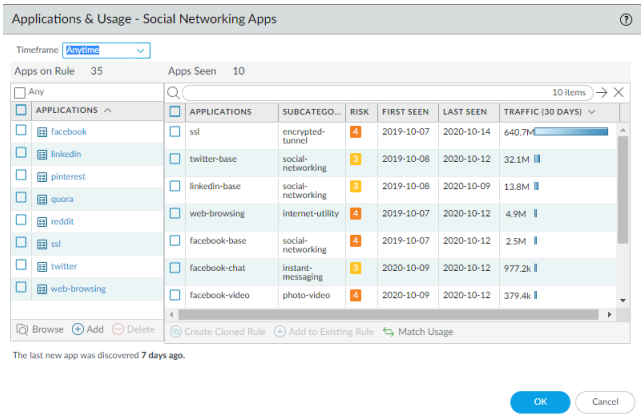
  に使うこともできます。

Traffic (Bytes, 30 days) (トラフィック **(**バイト、**30** 日**)** **)** をクリックし、過去 30 日間にルールが見つけたトラフィックの量に基づいて並び替えることができます。この情報を使用し、最

初に変更するルールの優先順位を決めることができます。例えば、**Apps Allowed** (許可されたアプリ) と **Apps Seen** (発見されたアプリ) の差が最も大きく、**Days with No New Apps** (新規アプリがない日数) が最も大きいルールを優先することができます。これらのルールは最も多く未使用のアプリケーションを持っており、成長度が高いためです。

STEP 3 | ルールの **Apps Seen** (発見されたアプリ) を確認します。

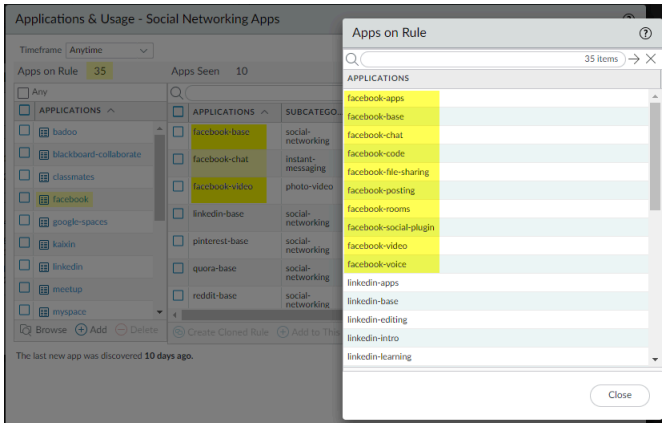
Unused Apps (未使用のアプリ) で **Compare** (比較) あるいは **Apps Seen** (発見されたアプリ) 列の数をクリックし、**Applications & Usage** (アプリケーションおよび使用状況) を開くと、ルールで設定されたアプリケーション (**Apps on Rule** (ルールのアプリ)) およびルールの **Apps Seen** (発見されたアプリ) が表示されます。



- **Apps Seen** (発見されたアプリ) の横にある数 (この例では 10) は、ルールに一致するアプリケーションの数です。ファイアウォールによる **Apps Seen** (発見されたアプリ) の更新には最低 1 時間以上かかりますので、ご注意ください。
- **Apps on Rule** (ルールのアプリ) の横にある数 (この例では 35) はルールで設定されているアプリケーションの数を示し、これはコンテナ アプリケーション内の各アプリケーションを数えることで計算されます (しかし、コンテナ アプリケーション自体は含みません。ルールでコンテナ アプリケーションを設定する場合、ルールはコンテナ アプリケーションの各アプリケーションを許可します)。**Applications** (アプリケーション) はルールで手動で設定したアプリケーションしか表示しないため、ルールでコンテナ アプリを設定する際、**Applications** (アプリケーション) には、コンテナ内のすべての各アプリケーションではなくコンテナ アプリしか表示されません (ルールで個々のアプリケーションも手動で設定していない限り)。そのため、**Apps on Rule** (ルールのアプリ) の表示数が、**Applications** (アプリケーション) リストのアプリケーション数と異なる場合があります。
- **Apps on Rule** (ルールのアプリ) の横にある数をクリックすると、ルールの各アプリケーションがすべて表示されます。

  この例では、ルールには 10 の**Apps Seen** (発見されたアプリ) (ルールと一致したアプリケーション) がありますが、35の **Apps on Rule** (ルールのアプリ) を許可します。**facebook** コンテナ アプリケーションはルール上で設定されており、ルールには、個別のアプリケーション facebook-base、facebook-chat、および facebook-video からのトラフィックが表示されます (**Apps Seen** (発見されたアプリ))。**Apps on Rule** (ルールのアプリ) の数をクリック

すると、**Apps on Rule** (ルールのアプリ) ダイアログが許可された各アプリケーションを表示しますが、コンテナ アプリケーション自体は表示しません。



ポップアップ ダイアログでアプリケーションを追加・削除することはできません。

ルール上の **Apps Seen** (発見されたアプリ) と **Apps on Rule** (ルールのアプリ) を比較します。ルール上のアプリケーションが使用されていない場合 (アプリケーションが表示されないか、**Apps Seen** (発見されたアプリ) で許可されたコンテナにアプリケーションが表示されない場合)、攻撃対象領域を減らすためにアプリケーションをルールから削除することを検討してください。期間を長くしなければ未使用だと誤解してしまうような、定期的 (四半期や一年に一度など) に使用するアプリケーションを考慮します。**Timeframe** (期間) は、ルールの **Apps Seen** (発見されたアプリ) の期間を有効化します。**Anytime** (すべて) を選択すると、ルールが存在する間に見つかったアプリケーションがすべて表示されます。**No App Specified** (アプリの指定なし) ダイアログにある **Created** (作成) あるいは **Modified** (変更) 日および定期的なイベント間の時間に応じて、定期的に使用されるアプリケーションをすべて確認できるほど長くルールがファイアウォール上に存在しないかもしれません。

STEP 4 | 未使用のアプリケーションをルールから削除します。

Apps on Rule (ルールのアプリ) でアプリケーションを手動で **Delete** (削除) (あるいは **Add** (追加)) するか、**Match Usage** (使用状況と一致) させてルールの **Apps Seen** (発見されたアプリ) を追加し、ルールで見つかったマッチするトラフィックが存在しないアプリケーションをワンクリックで削除します。

ルールから手動でアプリケーションを削除するにはアプリケーションを **Apps on Rule** (ルールのアプリ) で選択して **Delete** (削除) します。ルールから削除する前に、どのアプリケーションも定期的に使用しているものではないことを確認してください。(セキュリティ ポリシー ルールの **Application** (アプリケーション) タブでアプリケーションを追加または削除することもできます。)

Match Usage (使用状況と一致) は、ルールの **Apps Seen** (発見されたアプリ) を **Apps on Rule** (ルールのアプリ) に移動させ、未使用のアプリケーションがすべてルールから削除されます。

Policies > ***Security*** および ***No App Specified*** から ポートベースから App-ID ベースのセキュリティポリシールールに移行 にルールを複製できます。***Unused Apps*** (未使用のアプリ) から始まるアプリはコピーできません。

STEP 5 | 設定を **Commit**（コミット）します。

STEP 6 | 更新されたルールを監視し、ユーザーからのフィードバックを聴き、許可したいアプリケーションを更新されたルールが許可していること、定期的に使用するアプリケーションを意図せずブロックしていないことを確認します。

> ***Apps Allowed*** *(*許可されたアプリ*)* および ***Apps Seen*** *(*発見されたアプリ*)* の数は約 *1* 時間毎に更新されます。ルールから未使用のアプリケーションをすべて除去した後、ファイアウォールが表示を更新するまで、ルールが ***Policies*** *(*ポリシー*)* > ***Security*** *(*セキュリティ*)* > ***Policy Optimzer*** > ***Unused Apps*** *(*未使用のアプリ*)* のリストに残ります。ファイアウォールが表示を更新する際、***Apps Allowed*** *(*許可されたアプリ*)* と ***Apps Seen*** *(*発見されたアプリ*)* の数が同じである場合、ルールは ***Unused Apps*** *(*未使用のアプリ*)* 画面に表示されなくなります。ただし、ファイアウォールの負荷によっては、これらのフィールドが更新されるまでに *1* 時間以上かかることがあります。

アプリケーション使用状況統計の高可用性

2 つのファイアウォールを単一の高可用性 (HA) ペアとして構成する際、アプリケーション使用状況統計は、アプリケーション用にトラフィックログを生成するファイアウォールのローカルにあります。アプリケーション使用状況統計を閲覧できるかどうかは、HA 構成によっても異なります：

- アクティブ/パッシブ—アクティブ デバイスはアプリケーション使用状況統計を生成します。パッシブ デバイスがユーザートラフィックを発見しない場合、アクティブ デバイスだけがアプリケーション使用状況統計を表示します。パッシブ デバイスがトラフィックを発見する場合、パッシブ デバイスだけが発見したトラフィックからのアプリケーション使用状況統計を表示します。

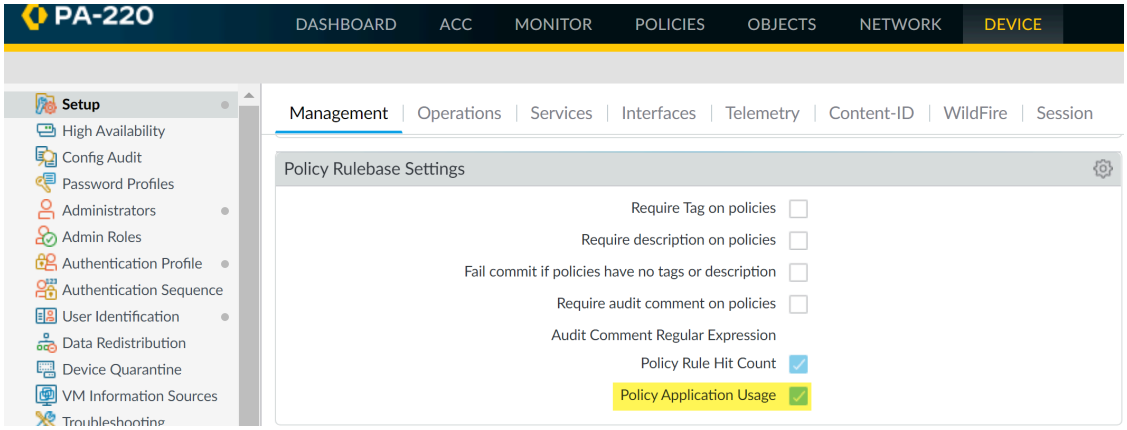
  フェイルオーバーの際、アプリケーション使用状況統計は新たにアクティブになったデバイス (フェイルオーバー前はパッシブだったデバイス) が生成するトラフィックログだけに基づきます。
- アクティブ/アクティブ—セッションを所有するデバイスがそのセッション用のトラフィックログを生成するため、セッションのアプリケーション使用状況統計はセッションを所有するデバイス上でのみ利用できます。あるアクティブ デバイスがセッションを所有している場合、他のアクティブ デバイスはそのセッションのアプリケーション使用状況統計を表示しません。

Policy Optimizer を無効化する方法

Policy Optimizer はデフォルトで有効になっています。Policy Optimizer はポートベースから App-ID ベースのセキュリティポリシールールに移行および未使用のアプリケーションがあるセキュリティポリシールールを特定を行って未使用のアプリケーションをルールから削除する際に役立つ多くの機能を提供しますが、任意でこの機能を無効化することもできます。

STEP 1 | **Device (**デバイス**)** > **Setup (**セットアップ**)** > **Management (**管理**)** > **Policy Rulebase Settings (**ポリシー ルールベース設定**)**に移動します。

STEP 2 | **Policy Application Usage** (ポリシー アプリケーションの使用状況)のチェックボックスを選択して機能を有効化でき、チェックボックスの選択を解除して機能を無効化できます。



App-ID クラウドエンジン

App-ID クラウド エンジン (ACE) は、ファイアウォールまたは Panorama が、Palo Alto Networks コンテンツ チームから特定の定義済みの App-ID を持たないアプリケーションのアプリ ID をクラウドからダウンロードできるようにする新しいサービスです。これらは、ファイアウォールが SSL、Web ブラウジング、不明 tcp、または不明 udp トラフィックとして識別するアプリケーションです。セキュリティ ポリシー ルールの ACE アプリ ID を使用して、これらのアプリケーションを可視化および制御し、ポリシー オプティマイザー を使用して、セキュリティ ポリシーでアプリケーションを追加および管理します。ACE アプリ ID は、他の種類のポリシー ルールでは使用できません。ACE:

- アプリケーションを識別および制御するために、既知の App-ID の数が大幅に増加します。ACE はアプリケーションの新しい App ID を定義すると、ファイアウォールで使用できるようになります。
- 新しい App-ID のファイアウォールへの可用性と配信を高速化します。
- セキュリティ ポリシー ルールでアプリケーション フィルタを使用することにより、アプリケーションのセキュリティ ポリシーへの追加を高速化し、自動化できます。
- 以前 ssl、Web ブラウジング、不明 tcp、または不明 udp として識別されていたアプリケーションの可視性を大幅に向上させます。

ACE には SaaS セキュリティ インライン サブスクリプションが必要です。*ACE* を使用する各アプライアンスには、有効なデバイス証明書がインストールされている必要があります。

PAN-OS 10.1 以降をサポートするすべてのハードウェア プラットフォームは *ACE* をサポートし、*ACE* を使用するすべてのアプライアンスには *PAN-OS 10.2* 以降が必要です。*Panorama* は、*SaaS* セキュリティ インライン ライセンスがインストールされていないファイアウォールや、*10.1* より前のバージョンの *PAN-OS* を実行するファイアウォールに対して *ACE* ベースのポリシーまたはオブジェクトをプッシュおよびコミットすることはできません。

ACE は、米国、*APAC*、および *EU GCP* リージョンでサポートされています。リージョンは、*CDL* リージョンに基づいて自動的に選択されます。

ファイアウォールが、お使いのリージョンに対して正しいコンテンツ クラウド *FQDN* (デバイス > ***Setup*** > コンテンツ***-ID*** > コンテンツ クラウド設定) を使用していることを確認し、必要に応じて *FQDN* を変更します。

- *US*—***hawkeye.services-edge.paloaltonetworks.com***
- *EU*—***eu.hawkeye.services-edge.paloaltonetworks.com***
- *APAC*—***apac.hawkeye.services-edge.paloaltonetworks.com***

ACE データ (トラフィック ペイロードを含む) は、選択したリージョンのサーバーに送信されます。お住まいの地域外のコンテンツ クラウド *FQDN* を指定すると (たとえば、*EU* リージョンに含まれているが、*APAC* リージョンの *FQDN* を指定した場合)、お住まいの国または組織のプライバシーと法的規制を破る可能性があります。

定義済みのコンテンツ配信アプリ ID は、新しいアプリケーションを毎月 1 回配信し、新しい App ID をインストールする前に分析して、セキュリティ ポリシー ルールに対して行う可能性のある変更を理解する必要があります。毎月のケイデンスと分析の必要性により、ポリシーにおける新しい App-ID の採用が遅くなります。Palo Alto Networks では、確認が必要な毎月のコンテンツ更新プログラムを通じて新しい App-ID を引き続き提供しますが、ACE は、次の 4 つの種類のいずれかとして最初に識別されるアプリケーションにオンデマンドの App-ID を提供することで、新しい App-ID の採用を改善します。

- **ssl** :暗号化されたSSLトラフィックは、最も一般的なタイプのネットワークトラフィックであり、ほとんどの専門家は総トラフィックの90%を超えていると主張しています。そのトラフィックを復号化しない場合、または復号化できない場合、ファイアウォールは実際の基盤となるアプリケーションとしてではなく、SSL としてしか識別できないことがよくあります。

- **Web** ブラウジング :ファイアウォールは、コンテンツ配信の App-ID が増え続ける量に追いついてはいられないほど多くのアプリケーションがあるため、暗号化されていない Web ブラウジング トラフィックを特定できません。
- **unknown-tcp** および **unknown-udp** :このトラフィックは、内部またはカスタム アプリケーションまたは不明な外部アプリケーションである可能性があります。特定の App-ID によってトラフィックを識別して、インテリジェントなアクセス決定を行い、トラフィックを制御および検査するための適切なセキュリティ ポリシー ルールを構築することが重要です。

ACE は、これらのアプリケーションを特定して識別し、それらを理解し、ポリシーで適切に制御できるようにします。

ACE アプリ *ID* は、他の種類のパブリック アプリケーションを識別せず、プライベート アプリケーションとカスタム アプリケーションを識別しません。*ACE* アプリ *ID* カタログには、定義済みのコンテンツ提供の *App-ID* が含まれていません。コンテンツ提供の *App-ID* は、コンテンツの更新で毎月到着します。

ファイアウォールが SSL、Web ブラウジング、不明 tcp、または不明 udp のトラフィックに遭遇すると、ファイアウォールは分析のために ACE にペイロードを送信します。ACE データベースに一致する App-ID がある場合、ACE は要求元のファイアウォールに App-ID を返します。ACE にトラフィックに対応する App-ID が存在しない場合、ACE は、ペイロードを機械学習 (ML) エンジンに送信します。ML エンジンは、ペイロードを分析し、ヒューマン コンテンツ チームと共に新しい App-ID を開発し、アプリケーションに関連しないトラフィックをドロップします。開発が完了すると、ML エンジンは新しい App-ID を ACE データベースにアップロードし、要求側のファイアウォール (およびその他のファイアウォール) は App-ID をダウンロードしてセキュリティ ポリシーで使用できます。

アプリケーションが *App-ID* を持つ *ACE* からアプリケーションを取得するのに数分かかる場合があり、新しい *App-ID* を開発する必要がある場合は、クラウド アプリケーションの検出がファイアウォール上でインラインではありません。ファイアウォールは、アプリケーション トラフィックを処理する判定を待機しません。ファイアウォールは、*ACE* から *App-ID* を受け取るまで、トラフィックを *SSL*、*Web* ブラウジング、不明 *tcp*、または *unknown udp* として処理し、新しい *App-ID* を受信してセキュリティ ポリシーで使用するまで、その方法でトラフィックを処理し続けます。

ACE が有効になっていて、*ACE* クラウドの *App-ID* がセキュリティ ポリシー ルールまたはアプリケーション グループで使用されている状態でファイアウォールまたは *Panorama* をダウングレードすると、ダウングレードは失敗します。失敗理由には、ダウングレードするために設定から削除する必要があるオブジェクトがリストされます。これらのオブジェクトを構成から削除し、 コミット 設定を行うと、ダウングレードは成功します。

- App-ID クラウド エンジンの展開の準備
- App-ID クラウド エンジンを有効または無効にする
- App-ID クラウド エンジンの処理と使用
- 新しいアプリ ビューアー (ポリシー オプティマイザー)

- ポリシー オプティマイザーを使用して App をアプリケーション フィルターに追加する
- ポリシー オプティマイザーを使用してアプリケーション グループにアプリを追加する
- ポリシー オプティマイザーを使用してルールに直接 Apps を追加する
- RMA ファイアウォール (ACE) を交換する
- ライセンスの有効期限または ACE の無効化による影響
- クラウド コンテンツロールバックによるコミットエラー
- App-ID クラウド エンジンのトラブルシューティング

App-ID クラウド エンジンの展開の準備

ファイアウォールで App-ID クラウド エンジン (ACE) を使用する前に、オンボーディングタスクがいくつかあります。ACE は、スタンドアロン ファイアウォールに展開することも、パノラマを使用して管理対象ファイアウォールに ACE を展開することもできます。

ファイアウォールが ACE を使用して、以前に SSL、Web ブラウジング、不明 tcp、および不明 udp トラフィックとして識別されたトラフィックに対して特定の App ID を提供できるようにするには、PAN-OS 管理者と SaaS セキュリティ管理者が連携して以下の作業を行う必要があります。

- ACE ファイアウォールを管理する Panorama アプライアンスを含む、ACE を使用する各アプライアンスに有効なデバイス証明書をインストールします。(PAN-OS管理者)。
- ACE を使用する各ファイアウォールで SaaS セキュリティ インラインをアクティブ化します。Panoramaはライセンスを必要としません。(SaaS セキュリティ管理者)
- ファイアウォールと ACE 間の通信用のサービス ルートを構成します。(PAN-OS管理者)。
- ACE を使用するファイアウォールを管理する Panorama アプライアンスで ACE を有効にします。(PAN-OS管理者)。

  ファイアウォールでは、*SaaS* セキュリティ インラインをアクティブ化した後、*ACE* が既定で有効になります。
- ACE トラフィックを許可するセキュリティ ポリシー ルールを作成します。(PAN-OS管理者)。
- ファイアウォールから Cortex データ レイク (CDL) へのログ転送を構成します。(PAN-OS管理者)。

次の手順の適切な手順で、*PAN-OS* 管理者は *SaaS* セキュリティ管理者に、展開が *SaaS* セキュリティ インラインのアクティブ化の準備ができていることを通知する必要があります。*SaaS* セキュリティ インラインをアクティブ化した後、*SaaS* セキュリティ インライン管理者は、*PAN-OS* デバイスで展開を完了する準備ができたことを *PAN-OS* 管理者に通知する必要があります。円滑な展開を実現するには、管理者間の通信が不可欠です。

要件:

- スタンドアロン ファイアウォール、Panorama アプライアンス、および管理対象ファイアウォールは、PAN-OS 10.1 以降を実行する必要があります。

- すべての ACE ファイアウォールは、SaaS セキュリティ インライン ライセンスを購入している必要があります。Panorama は、ACE ファイアウォールを管理したり、ACE 構成を管理対象のファイアウォールにプッシュしたりするためのライセンスを必要としません。
- すべての ACE アプライアンスは、お客様の地域に応じて、米国、APAC、または EU GCP リージョンに接続できる必要があります(リージョンは CDL リージョンに基づいて自動的に選択されます)。

  ファイアウォールが、お使いのリージョンに対して正しいコンテンツ クラウド FQDN (デバイス > **Setup** > コンテンツ**-ID** > コンテンツ クラウド設定) を使用していることを確認し、必要に応じて FQDN を変更します。

  - Default hawkeye.services-edge.paloaltonetworks.com デフォルト hawkeye.services-edge.paloaltonetworks.com
  - **EU – eu.hawkeye.services-edge.paloaltonetworks.com**
  - アジア太平洋–apac.hawkeye.services-edge.paloaltonetworks.com

  ACE データ (トラフィック ペイロードを含む) は、選択したリージョンのサーバーに送信されます。お住まいの地域外にある Content Cloud FQDN を指定した場合 (たとえば、EU リージョンにいるが、APAC リージョンの FQDN を指定した場合)、お住まいの国または組織のプライバシーおよび法的規制に違反する可能性があります。

PAN-OS 管理者は、手順の最初の つの手順を完了し、アクティブ化のために SaaS セキュリティ インライン管理者に渡します (Step 3)。ライセンス認証後、SaaS セキュリティ インライン管理者は、手順の残りの部分を PAN-OS 管理者に渡して PAN-OS デバイスで完了させます。

STEP 1 | ファイアウォールとPanorama(使用している場合)をオンラインにします。(PAN-OS管理者)。

STEP 2 | デバイス Certifcate を個々のファイアウォールにインストールして、クラウド サービスを使用したり、Panorama を 管理対象ファイアウォール にデバイス証明書をインストールしたりできます。(PAN-OS管理者)。

次のステップを *SaaS* セキュリティ管理者に渡します。

STEP 3 | ACE を使用するすべてのファイアウォールで SaaS セキュリティ インライン をアクティブにします。アクティベーションにより、ファイアウォール上で ACE が有効になります。(SaaS セキュリティ管理者)

Panorama は、*ACE* を使用するファイアウォールを管理するために *SaaS* セキュリティ インライン ライセンスを必要としません。管理対象ファイアウォールのみがライセンスを必要とします。ライセンスは、次の手順で示すように手動で取得する必要があります。

残りの手順を *PAN-OS* 管理者に渡します。

STEP 4 | 各ファイアウォールで SaaS セキュリティ インライン ライセンスを取得し、Panorama はライセンスを必要とせず、アクティブ化されていることを確認します。(PAN-OS管理者)。

SaaS Security 管理者のアクティベーションではファイアウォールのライセンスが設定されるため、カスタマーサポートポータルにアクセスしたり認証コードを取得したりする必要はありません。

1. デバイス > ライセンス > ライセンス管理 に移動し、[ライセンス サーバーからライセンス キーを取得 を選択してライセンスを取得します。
2. デバイス > ライセンス をチェックして、SaaS セキュリティ インライン ライセンスがアクティブであることを確認します。

STEP 5 | ファイアウォールが App-ID クラウド エンジンと通信できるように、データ サービス (データプレーン) サービス ルートを構成します。(PAN-OS管理者)。

この設定を *Panorama* から管理されたファイアウォールにプッシュできます。*Panorama* と管理対象ファイアウォールの両方で *PAN-OS 10.1* 以降を実行する必要があります。

既定では、ファイアウォールは管理インターフェイスをデータ サービス ルートのソース インターフェイスとして使用しますが、この手順の後半で示すように、クラウド サービスへの接続性を持つデータプレーン インターフェイスを **Source** インターフェイス および **Source Address** として構成することをお勧めします。

ファイアウォールの問題は、管理インターフェイスで明示的なプロキシが構成され、それをデータ サービス のルートに使用する場合、管理インターフェイスは、クラウド アプリケーションと署名を管理するナレッジ クラウド サービス (KCS) にのみ接続できることです。管理インターフェイスで明示的なプロキシが構成されている場合、アプリケーション ペイロードを既存の ACE App-ID に対してチェックし、判定を提供する検出クラウド サービス (DCS) に接続できません。KCS と DCS は、ACE クラウド内のサービスです。管理インターフェイスに明示的なプロキシが構成されている場合、ACE のデータ サービス ルートに対しては、すべてのサービスに接続できないため、このプロキシを使用できません。この場合、ファイアウォール上のデータプレーン インターフェイスを使用して、データ サービスに接続する必要があります。

Panorama はデフォルトで管理ポートを使用して *KCS* に接続し、*DCS* には接続しません。

デフォルトの管理インターフェイスを使用する代わりに、データプレーンインターフェイスでサービスルートを設定するには、次の手順を実行します:

1. デバイス > 設定 > サービス を選択し、サービス機能でサービス ルート構成 を選択します。
2. サービスルートを **Customize (カスタマイズ)** します。
3. **IPv4** プロトコルを選択します。
4. [サービス] 列の データ サービス をクリックして、[サービス ルート ソース ダイアログボックスを開きます。

5. ソース インターフェイス と ソース アドレス を選択します (これらは管理インターフェイスにできません)。

   送信元インターフェースにはインターネット接続が必要です。ベスト プラクティスは、クラウド サービスに接続できるデータプレーン インターフェイスを使用することです。ソース インターフェイスとアドレスの作成の詳細については、「インターフェイスを構成する と アドレス オブジェクト を作成する」を参照してください。
6. 送信元インターフェイスとアドレスを設定するには、[**OK** をクリックします。
7. **OK** をクリックして、サービス ルートの構成を設定します。
8. ポリシー > セキュリティ を選択し>、この手順で先に指定したソース インターフェイスから、**kcs.ace.ace.tpcloud>hawkeye.services-edge.paloaltonetworks.com<paloaltonetworks** (すべてのリージョンの)および {DCS サービスの FQDN アドレスへのトラフィックを許可する セキュリティ ポリシー ルール を追加します**>eu.hawkeye.services-edge.paloaltonetworks.com** (EU リージョン DCS サービス)、または **apac.hawkeye.services-edge.paloaltonetworks.com** (APAC 地域 DCS サービス)。

   また、新しいまたは既存のセキュリティ ポリシー 規則に次の つの FQDN を追加して許可します: **ocsp.paloaltonetworks.com** と **crl.paloaltonetworks.com** 証明書の検証を行います。

   最後に、次の つのアプリケーションを許可して、ACE トラフィックを許可するセキュリティ ポリシー 規則を追加または変更します: パロアルト**-ace**、パロアルト**-ace-kcs**、および**- dlp-service** です。

STEP 6 | hawkeye.services-edge.paloaltonetworks.com と kcs.ace.tpcloud.paloaltonetworks がファイアウォールで到達可能であり、パノラマ デバイス上で kcs.ace.tpcloud.paloaltonetworks に到達できることを確認します。(PAN-OS管理者)。

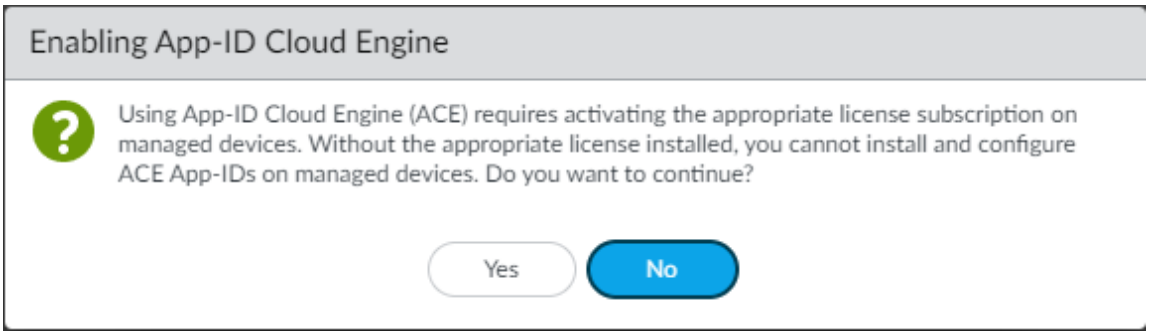
操作コマンド `admin@fw1>` クラウド とアプ `ID` の接続を表示 を実行します。出力は、接続が機能しているかどうか、およびライセンスがインストールされているかどうかを示します。

STEP 7 | (Panoramaのみ)ACE 対応ファイアウォールを管理する Panorama アプライアンスで ACE を有効にします。(PAN-OS管理者)。

ACE は Panorama ではデフォルトで無効になっています。

ACE が有効なファイアウォールがない管理対象グループに *ACE* 構成をプッシュする場合 *(*グループ内の一部またはすべてのファイアウォールで *ACE* が有効になっていない場合*)*、プッシュは失敗します。

1. **Panorama** > セットアップ > **ACE** > 設定 に移動します。
2. [編集 (⚙)] をクリックし、[無効にするアプリ **ID** クラウド エンジン*.* を選択解除します。
3. **OK** をクリックします。
4. **ID** クラウド エンジンを有効にする ダイアログが表示されます。



ACE を有効にするには、はい をクリックします。

5. 変更を **Commit**（コミット）します。

STEP 8 | App-ID カタログがダウンロードされるまで待ちます。(PAN-OS管理者)。

コンテンツ提供の App ID は 未満です。ACE カタログをダウンロードすると、ファイアウォール上に何千ものアプリケーションが表示され、**objects** > **Applications** をチェックするか、運用可能な CLI コマンド `show クラウド アプリ id クラウド アプリ データ アプリケーション`をすべて使用して を確認して新しいアプリ ID を確認できます。

STEP 9 | (Panoramaのみ)目的の構成を管理対象ファイアウォールにプッシュします。(PAN-OS管理者)。

STEP 10 | Cortex データ レイク (CDL) へのログ転送 を設定し、セキュリティ ポリシー ルールで正しいログ転送プロファイルを使用してログ転送を有効にします。(PAN-OS管理者)。

SaaS の可視性と SaaS アプリ ID ポリシー推奨 をサポートするには、SaaS セキュリティ インライン接続 から CDL が必要です。*SaaS* セキュリティ インラインが正しく機能するためには、少なくともトラフィック ログと *URL* ログを *CDL* に転送する必要があります。

App-ID クラウド エンジンを有効または無効にする

App-ID クラウド エンジン (ACE) は、Panoram では既定で無効になっており、SaaS セキュリティ インライン ライセンスがインストールされている場合はファイアウォールで既定で有効になっています。ACE 対応ファイアウォールを管理する Panorama アプライアンスで ACE を有効にする必要があります。

ACE を有効または無効にするには、次の手順を実行します。

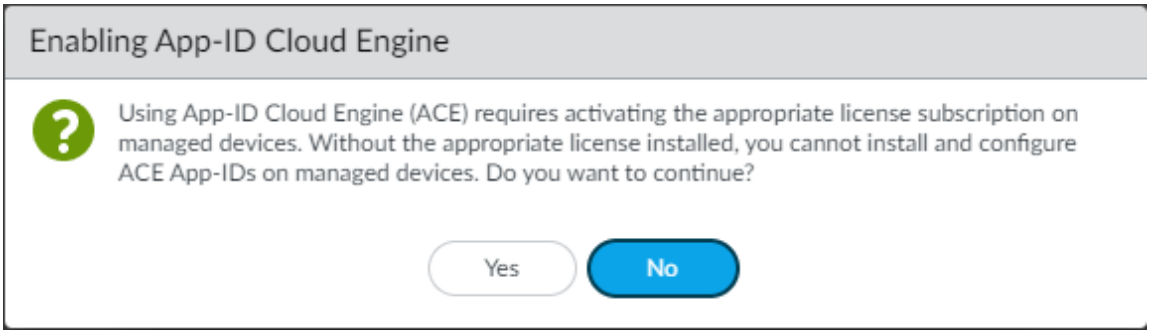
STEP 1 | ファイアウォールの デバイス > セットアップ > **ACE** > 設定 または Panorama の **Panoram** > セットアップ > **ACE** > 設定 に移動します。

STEP 2 | 編集 (⚙) をクリックし、ACE を有効にするには [を無効にする **App-ID** クラウド エンジン] をオフにするか、[を無効にするアプリ **ID** クラウド エンジン] を選択して ACE を無効にします。

ACE は既定で無効になっています。

STEP 3 | **OK** をクリックします。

STEP 4 | (ACE を有効にする場合のみ)ACE を有効にしている場合は、[を有効にするアプリ **ID** クラウド エンジン] ダイアログ ボックスが表示されます。



ファイアウォールまたは Panorama で管理されるファイアウォールに SaaS セキュリティ インライン ライセンスがインストールされている場合は、[はい] をクリックして ACE を有効にします。

STEP 5 | 変更を **Commit**（コミット）します。

App-ID クラウド エンジンの処理と使用

ファイアウォールで App-ID クラウド エンジン (ACE) アプリ ID がダウンロードされる場合、ファイアウォールがこれらの App-ID を処理する方法と、同じアプリケーションに対して定義済みのコンテンツ ベースの App-ID がある場合にファイアウォールが ACE アプリ ID をどのように処理するかを理解することが重要です。Palo Alto Networks コンテンツ チームは、定義済みのコンテンツ ベースの App-ID を開発し、 アプリケーション コンテンツの更新 を通じて、変更された App-ID を更新します (更新には有効なサポート契約が必要です)。

ACE には SaaS セキュリティ インライン ライセンスが必要です。ACE をサポートしないファイアウォールには、定義済みのコンテンツ ベースの App-ID しかありません。ACE アプリ ID カタログには、コンテンツ ベースのアプリ ID が含まれていません。

ACE アプリ *ID* は、セキュリティ ポリシー ルールでのみ使用できます。*ACE* アプリ *ID* は、他の種類のポリシー ルールでは使用できません。

- ファイアウォールが App-ID クラウド エンジンに最初に接続すると、ファイアウォールは使用可能な ACE アプリ ID のカタログをダウンロードし、セキュリティ ポリシーでそれらの App-ID を使用できます。完全な署名はダウンロードされません。このカタログを使用すると、ファイアウォールでアプリケーションが見たことがない場合でも、セキュリティ ポリシーで ACE App-ID を使用できます。ACE は、ファイアウォールが最新の ACE App-ID にアクセスできるように、定期的にカタログの更新をファイアウォールにプッシュします。

  アプリケーションが、ssl、Web ブラウジング、不明 tcp、または不明 udp として識別されるファイアウォールに到着し、ファイアウォールに署名がない場合、ファイアウォールはペイロードを ACE に送信します。ACE にトラフィックの App-ID がある場合、ACE は完全な署名をファイアウォールに送り返します。トラフィックが ACE 署名と一致しない場合、ACE は、マシン ラーニング (ML) エンジンにペイロードを送信します。ML エンジンは、ペイロードを分析し、ヒューマン コンテンツ チームと共に新しい App-ID を開発し、アプリケーションに関連しないトラフィックをドロップします。ML エンジンは新しい App-ID を ACE に送信し、ファイアウォールを要求すると、それをダウンロードしてセキュリティ ポリシーで使用できます。

  アプリケーションが *App-ID* を持つ *ACE* からアプリケーションを取得するのに数分かかる場合があり、新しい *App-ID* を開発する必要がある場合は、クラウド アプリケーションの検出がファイアウォール上でインラインではありません。ファイアウォールは、アプリケーション トラフィックを処理する判定を待機しません。ファイアウォールは、*ACE* から *App-ID* を受け取るまで、トラフィックを *SSL*、*Web* ブラウジング、不明 *tcp*、または *unknown udp* として処理し、新しい *App-ID* を受信してセキュリティ ポリシーで使用するまで、その方法でトラフィックを処理し続けます。
- ファイアウォールが ACE から App-ID を要求すると、ファイアウォールはトラフィックを保持せず、ACE から App-ID を受け取るまで通常どおりトラフィックを処理し続けます。
- ファイアウォールは、コンテンツ配信の App ID を処理するのとは異なる方法で、ACE からダウンロードされたクラウドの App ID を処理します。ファイアウォールは既存のセキュリティ ポリシーに従って ACE アプリ ID を使用するため、ファイアウォールにインストールする前に、新しい ACE アプリ ID がセキュリティ ポリシーにどのような影響を与えるかを調べる必要はありません。既存のセキュリティ ポリシー ルールは、セキュリティ ポリシーで ACE アプリ ID を明示的に使用するまで、新しい ACE アプリ ID を制御します。以下に例を示します。

  1. アプリケーションは「ssl」としてのみ識別され、SSL トラフィックを許可するセキュリティ ポリシー ルールがあるため、SSL ルールではそのアプリケーションが許可されます。
  2. ファイアウォールは SSL アプリケーションを認識し、ペイロードを ACE に送信します。
  3. ACE は実際のアプリケーションを識別します。アプリケーションが ACE データベースに存在する場合、ACE はその App-ID をファイアウォールに送信します。ACE に App-ID がない新しいアプリケーションの場合、ACE はペイロードを ML エンジンに転送します。ファイアウォールは、ML エンジンとヒューマン コンテンツ チームが App-ID を割り当てて ACE に送信するまで、App-ID を受け取りません。

4. Ssl トラフィックを許可するルールは、App-ID がもはや「ssl」ではない場合でも、新たに識別されたアプリケーションを許可します。(ただし、セキュリティ ポリシーで新しい ACE App-ID を使用する場合、そのポリシーによってトラフィックが制御されます。同様に、以前は Web ブラウジング、不明 TCP、および不明 udp として識別されたトラフィックは、セキュリティ ポリシーで ACE App-ID を使用するまで、これらの種類のトラフィックを制御するセキュリティ ポリシー ルールに従い続けます。

   ACE アプリ *ID* とは対照的に、*App-ID* が定義済みのコンテンツ提供の *App-ID* である場合、*SSL* トラフィックを許可するルールはアプリケーションと一致しなくなります。セキュリティ ポリシールールで明示的に許可されていない場合、ファイアウォールはそれをブロックします。

   この動作の例外は、別のセキュリティ ポリシー ルールが ACE によってトラフィックに与えられた App-ID を指定する場合です。特定の App-ID を持つセキュリティ ポリシー ルールは、より限定的でない ssl アプリ ID のルールよりも優先されます。実際の App-ID を指定するルールがブロック ルールの場合、SSL トラフィックを許可するルールがある場合でも、アプリケーションはブロックされます。より詳細な (細かい) App-ID を持つルールは、ファイアウォールが動作するルールです。

   この例では、既存のルールまたは複製されたルールに、直接または複製されたルールに、またはアプリケーション フィルタまたはアプリケーション グループを使用して、以前に *"ssl"* として識別されたアプリケーションのクラウド *App-ID* を追加すると、そのルールによってアプリケーションが制御されます。アプリケーションは別のルールで明確に識別されるため、*"ssl"* ルールはアプリケーションを制御しなくなりました。

新しい ACE App-ID をセキュリティ ポリシー ルールに明示的に追加しない場合、ファイアウォールは、ACE App-ID を使用する前にそれらのアプリケーションを制御し、SSL、Web ブラウジング、不明 TCP、または不明 UDP トラフィックとして識別されたのと同じルールで制御し続けます。たとえば、ファイアウォールが不明 TCP と識別されたアプリケーションを認識し、その後、その ACE App-ID をトラフィックに対して受信しても、セキュリティ ポリシー ルールでその ACE App-ID を使用しない場合、ファイアウォールは不明 TCP トラフィックを制御するルールを使用してそのトラフィックを制御します。 不明な TCP トラフィックを許可すると、トラフィックは許可されます。

- ファイアウォールは、キャッシュをチェックし、繰り返しデータをクラウドに送信し、評決を要求しないように、いくつかの情報をキャッシュします。ファイアウォールが ACE からの判定を待っている場合、ファイアウォールは同じアプリケーション データを 2 度転送しません。
- 特定のコンテナー アプリとその機能アプリケーションは、すべてのクラウド ベースの App-ID またはすべてのコンテンツ ベースの App-ID のいずれかです。1 つの App-ID 配信方法では、コンテナー アプリとそのすべての機能アプリを定義します。
- クラウドベース、コンテンツ提供、およびユーザー定義のカスタム App-ID 名が重複する場合、優先順位は次のようになります。

  1. カスタム **App ID** — これらの App-ID は他のすべての App-ID よりも優先され、同じ App-ID を持つ ACE アプリケーションをファイアウォールがダウンロードしようとすると、同

じファイアウォール上の 2 つのアプリケーションが同じ App-ID を持つことができないため、コミットは失敗します。

この場合、カスタム アプリケーションの名前を変更したり、カスタム アプリケーションが ACE アプリケーションと同じアプリケーションである場合は、カスタム アプリケーションを削除して ACE アプリケーションを使用できます。

2. コンテンツ ベースの定義済み **App-ID** – これらのアプリ ID は ACE クラウドの App-ID 定義よりも優先されます。
3. **ACE** クラウド アプリ **ID** - カスタムおよびコンテンツ ベースのアプリ ID は、ACE アプリ ID 定義よりも優先されます。

- App-ID がコンテナー アプリと一致する場合、ファイアウォールはコンテナー アプリの App-ID とその機能アプリをすべてダウンロードします。たとえば、ファイアウォールがFacebookコンテナアプリを取得した場合、Facebookベース、フェイスブックチャット、フェイスブック投稿などを取得します。
- ACE アプリ ID に対して次のいずれかのアクションを実行すると、ファイアウォールは、アプリケーションの以前の SSL、Web ブラウジング、不明 tcp、または不明 udp アプリ ID に基づく代わりに特定の ACE アプリ ID に基づいてアクションを実行するため、セキュリティ ポリシーがその ACE アプリ ID を処理する方法に影響します。
  - アプリケーション フィルター を作成して、ACE アプリ ID をセキュリティ ポリシーに自動的に追加します。

    アプリケーション フィルターを使用して、*ACE* アプリ *ID* をセキュリティ ポリシー ルールに自動的に追加します。新しい *App-ID* がアプリケーション フィルターと一致すると、ファイアウォールによって自動的にフィルターに追加されます。セキュリティ ポリシー ルールでアプリケーション フィルターを使用すると、そのルールによって、フィルターに自動的に追加された新しい *App-ID* のアプリケーション トラフィックが制御されます。つまり、アプリケーションフィルタは、*ACE*アプリ*ID*を自動的に保護するための「簡単なボタン」であり、最小限の労力で最大限のアプリケーションの可視性と制御を得ることができます。
  - アプリケーション グループ にアプリ ID を追加します。
  - ポリシー オプティマイザー を使用して、App-ID を複製されたルールまたは既存のルール、または既存のアプリケーション フィルタまたはアプリケーション グループに追加します。ポリシー オプティマイザーを使用すると、ポリシー オプティマイザー ツール内から直接新しいアプリケーション フィルタとアプリケーション グループを作成できます。ポリシー オプティマイザー の並べ替えツールとフィルター ツール を使用して、動作するルールに優先順位を付け、それらのルールに一致する ACE アプリ ID の数を評価します。
  - 新規または既存のセキュリティ ポリシー ルールに ACE アプリ ID を直接追加します。

  クラウドの App-ID をセキュリティ ポリシー ルールに直接追加するか、アプリケーション フィルターまたはアプリケーション グループを使用して追加すると、そのルールによってアプリケーションが制御されます。クラウド配信の App-ID を制御するためにこれらのアクションのいずれかを実行するまで、ファイアウォールは既存の ssl、Web ブラウジング、不明 tcp、または不明 udp セキュリティ ポリシールールを使用して ACE アプリケーションを制御します。

- アプリケーションフィルターを作成する場合は、ssl および Web ブラウジングをフィルターから除外します。ssl と Web ブラウジングは、すべてのブラウザーベースのクラウド アプリケーションと一致するため、ssl と Web ブラウジングを含むアプリケーション フィルターは、すべてのブラウザー ベースのクラウド アプリケーションに一致します。
- アクティブ/パッシブ高可用性:
  - Active ファイアウォールは、ACE カタログをパッシブ ファイアウォールと同期して、同一のカタログを持ちます。
  - パッシブ ファイアウォールは、ACE への接続をアクティブ なファイアウォールになるまで開始しません。
- アクティブ/アクティブ高可用性:各デバイスはカタログと署名を個別にフェッチするため、カタログと署名は同期されません。ただし、ピアでカタログが同期されていない場合、ACE App-ID がセキュリティ ポリシー ルールで参照されている場合は、コミットは失敗します。ピア HA ファイアウォールのカタログが同期していない場合は、更新がデバイスに届くまで数分待ってから、再び同期状態にします。
- Panorama は、管理対象ファイアウォールに対してすべての/プッシュ障害をコミットします。
  - 管理対象ファイアウォールには有効な SaaS セキュリティ インライン ライセンスが含まれていないため、ACE カタログはありません。この場合、プッシュされた構成から ACE オブジェクトを削除して、再試行してください。
  - 管理対象ファイアウォールと ACE 間の接続がダウンし、プッシュされた構成には、ファイアウォール上の ACE カタログにないアプリケーションが含まれます。この場合、ACE クラウドへの接続を確認し、必要に応じて接続を再確立して、ファイアウォールがカタログを更新できるようにします。

    運用 CLI コマンド は、クラウドと `appid` のクラウドへの接続を示す 、クラウド接続の状態と ACE クラウド サーバー URL を提供します。
  - Panorama の ACE カタログと管理対象ファイアウォールの ACE カタログが同期しなくて、ファイアウォールのカタログに含まれていない ACE アプリを含むプッシュされた構成が発生します。ファイアウォールと ACE 間の接続がアップしている場合、古くなったカタログは自動的に数分後に更新され、問題が解決されます。(5 分間待ってから、もう一度やり直してください。

    > *CLI* コマンド デバッグ クラウド *`appid`* クラウド-手動プル のチェック クラウド アプリ データ を使用して、カタログを手動で更新することもできます。
- ファイル ブロック、ウイルス対策、WildFire、DLP プロファイルなどの一部のセキュリティ プロファイルでは、プロファイルの一部としてアプリケーションを指定できます。コンテンツ提供の App-ID のみがセキュリティ プロファイルでサポートされます。ACE アプリ ID は、セキュリティ プロファイルではサポートされていません。ACE アプリ ID は、セキュリティ ポリシー ルールでのみ使用することを目的としています。

- ACE App-ID はセキュリティ ポリシーでのみサポートされるため、アプリケーションの上書き、ポリシー ベース転送(PBF)、QoS、または SD-WAN ポリシー ルールではサポートされません。

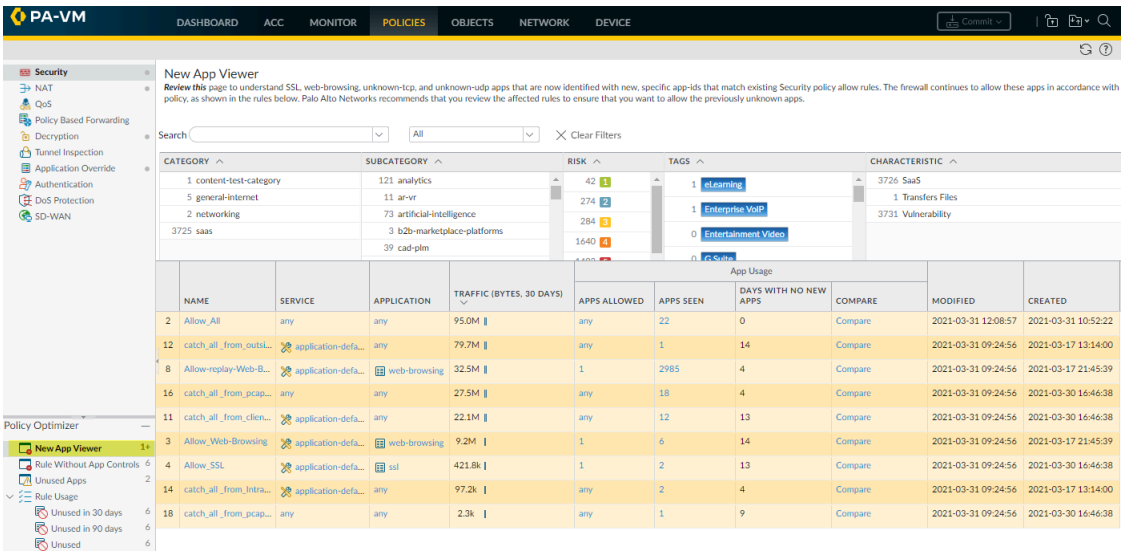
> アプリケーションの上書きまたは *PBF* ルールの構成で *ACE* アプリ *ID* を表示できません。ただし、*ACE App-ID* は *QoS* および *SD-WAN* ポリシー ルールの設定で表示 (選択可能) であり、ルールに適用されるアプリケーション グループまたはアプリケーション フィルタに存在する可能性があります。これらのルールで*ACEApp-ID*を使用する場合、ポリシーはアプリケーショントラフィックを制御せず、アプリケーショントラフィックに影響を与えません。*ACEApp-ID*が追加された場合でも、ルールは*ACEApp-ID*トラフィックには適用されません。ルールに。

新しいアプリ ビューアー (ポリシー オプティマイザー)

ポリシー オプティマイザー 新しいアプリ ビューアー は、ACE からダウンロードされたクラウドの App-ID と一致するセキュリティ ポリシー ルールを示しています。ポリシー オプティマイザーを使用して、新たに識別されたアプリケーションを管理し、複製されたルールまたは既存のルールに追加できます。**4>4>** > **Security** を選択して>、インターフェイスの ポリシー オプティマイザー 部分で 新しいアプリ< ビューアー を公開し、[新しいアプリ ビューアー<>8} を選択します。

画面の上部は オブジェクト > アプリケーション フィルタ に似ています。同様の方法で動作し、画面の下部に表示されるセキュリティ ポリシールールをフィルター処理します。カテゴリ、サブカテゴリなどでアプリケーションを許可するルールをフィルタリングできます。フィルター処理に使用できるカテゴリとサブカテゴリは、画面の下半分にリストされているルールの新しいアプリケーションと一致するものだけなので、そこにないアプリケーションのフィルタリングに時間を無駄にしません。

ルールをフィルター処理すると、画面の下部に、フィルター処理されたアプリケーションを含む規則のみが表示されます。フィルター内のアプリを表示していないルールは、リストから削除されます。(フィルタを削除すると、それらを再び表示できます)。



App が表示 列の数字をクリックして 、[アプリケーションと使用状況 ダイアログを開き、ファイアウォールがセキュリティ ポリシーでクラウドベースのアプリケーションを処理する方法を変更します。ACE アプリケーション フィルター、アプリケーション グループ、ポリシー オプティマイザーを使用するか、ACE アプリ ID を直接ルールに追加して、ACE アプリ ID をセキュリティ ポリシー ルールに追加します。クラウド配信の App-ID を制御するためにこれらのアクションのいずれかを実行するまで、ファイアウォールは引き続きトラフィックを ssl、Web ブラウジング、不明 tcp、または不明 udp トラフィックとして認識し、既存の ssl、Web ブラウジング、不明 tcp、または不明 udp セキュリティ ポリシー ルールを使用してアプリケーションを制御します。

ポリシー オプティマイザーを使用して App をアプリケーション フィルターに追加する

App-ID クラウド エンジン (ACE、およびコンテンツ提供の App-ID) から、新しいアプリケーション フィルターまたは既存のアプリケーション フィルターにアプリ ID を追加して、セキュリティ ポリシーでクラウドの App-ID を制御する方法を自動化します。新しい ACE App-ID がアプリケーション フィルタに一致すると、ファイアウォールによって自動的にフィルタに追加されます。セキュリティ ポリシールールでアプリケーション フィルタを使用すると、新しい ACE App ID がファイアウォールに到着し、フィルタに追加されると、ルールによって自動的に制御されます。

ACE は、以前に *SSL*、*Web* ブラウジング、不明 *tcp*、または不明 *udp* として識別されたアプリケーションに対して *App-ID* を提供します。

アプリケーション フィルタの使用は、次の理由からベスト プラクティスです。

- セキュリティ体制を改善します。アプリケーション フィルタは、より一般的な SSL、Web ブラウジング、不明 tcp、または不明 UDP ルールにトラフィックを一致させるのではなく、特定の種類のアプリケーション トラフィックを処理するように特別に設計したセキュリティ ポリシー ルールに新しい ACE App-ID を追加することを自動化します。
- 時間を節約します。ファイアウォール管理者は、ポリシーに新しい ACE App ID を自動的に追加し、管理者が作業を行う必要がないように、さまざまな種類のトラフィックを処理するようにアプリケーション フィルタを構成できます。

アプリケーションフィルターを作成する場合は、*ssl* および *Web* ブラウジングをフィルターから除外します。*ssl* と *Web* ブラウジングは、すべてのブラウザーベースのクラウド アプリケーションと一致するため、*ssl* と *Web* ブラウジングを含むアプリケーション フィルターは、すべてのブラウザー ベースのクラウド アプリケーションに一致します。

ポリシー オプティマイザー を使用して、ACE アプリ ID をアプリケーション フィルターに追加し、フィルターを複製または既存のルールに適用し、セキュリティ ポリシーで ACE アプリ ID を制御します。

STEP 1 | **2>policies** > セキュリティ に移動し、[ポリシー オプティマイザー > 新しいアプリ ビューアー を選択します。

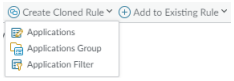
ファイアウォールが ACE App-ID でトラフィックを識別している場合、左側のナビゲーション ウィンドウに 新しいアプリ ビューアー の横に番号が表示されます。画面には、クラウドの App ID に一致するセキュリティ ポリシー ルールが表示されます。

STEP 2 | アプリケーションと使用状況 ダイアログで、ルールに一致するクラウド配信アプリケーションを表示するには、セキュリティ ポリシー ルールの **App** 見 の番号をクリックします。

STEP 3 | 既存のアプリケーション フィルタまたは新しいアプリケーション フィルタに追加するアプリケーションを選択します。

並べ替えおよびフィルタ は、**App Seen** 内のアプリケーションを、サブカテゴリ、リスク、過去 30 日間に見られたトラフィックの量、またはアプリケーションが最初または最後に見た時点で実行できます。

STEP 4 | **>**アプリケーションフィルタを選択するか<、アプリケーションの処理方法に応じて既存のルールに追加します。



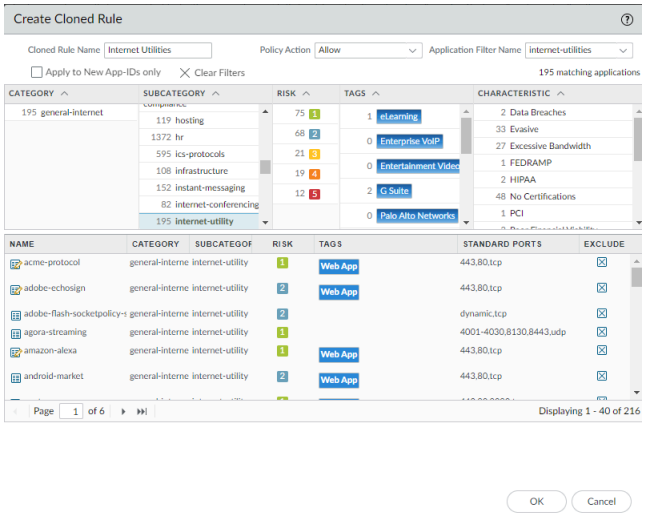
クローン作成ルール を使用して複製できるアプリケーションの最大数は、*1,000* 個のアプリケーションです。*1,000* を超えるアプリケーションを別のルールに移動する場合は、既存のルール に追加*]* を使用します。アプリケーションを新しいルールに移動する場合は、まずルールを作成します *(**Policies** >* セキュリティ*)* を作成してから、ポリシー オプティマイザーを使用してそのルールに追加します。

STEP 5 | 複製または既存のルールのアプリケーション フィルタを選択または作成します。ポリシー オプティマイザーを使用したアプリケーション フィルタ の作成は、**object** > アプリケーション フィルタ を使用してアプリケーション フィルタを作成する場合とほとんど同じです。

複製されたルールを作成:

1. クローンルール名（元のルールのすぐ上にあるセキュリティポリシールールベースに表示されるクローンルールの名前）を入力します。
2. ポリシー アクション (許可または拒否) を選択します。
3. メニューから アプリケーション フィルター名 を選択するか、新しいアプリケーション フィルターの名前を入力します。
4. フィルターを 新しいアプリ **ID** にのみ適用する にするか、すべての App-ID に適用するかを選択します。
5. カテゴリ、サブカテゴリ、リスク、タグ、特性値を使用して、アプリケーションフィルタに追加するアプリケーションのタイプをフィルタリングします。ファイアウォールは、

フィルタ条件を満たす新しいアプリケーションをアプリケーション フィルタに自動的に追加します。

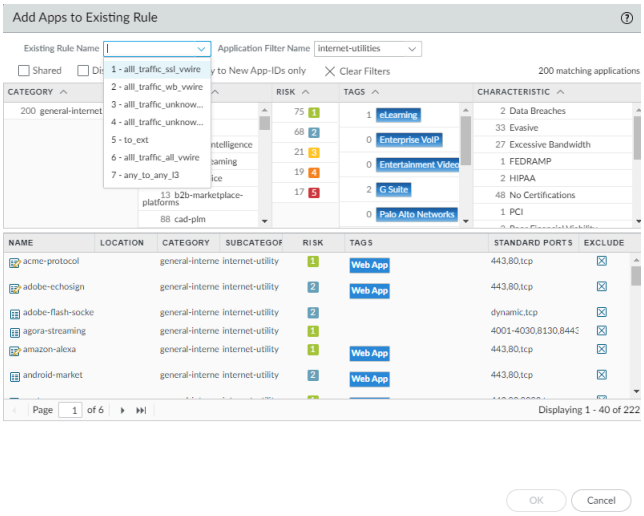


6. **OK** をクリックして、アプリケーションを新規または既存のアプリケーション フィルタに追加します。ファイアウォールには、アプリケーション フィルターの ステップ 3 で選択したアプリケーションが含まれています。
7. 変更を **Commit**（コミット）します。

既存のルールに追加:

1. 選択したアプリケーションをアプリケーション フィルターの既存のルールに追加するには、既存のルール名 を選択します。
2. メニューから アプリケーション フィルター名 を選択するか、新しいアプリケーション フィルターの名前を入力します。
3. アプリケーション フィルターが **Shared** かどうか、フィルターのアプリケーション特性の **disable** オーバーライド を行うかどうか、フィルターを 新しいアプリ **ID** にのみ適用する必要があるかどうか**<**、またはすべての **App-ID** に適用するかどうかを選択します。
4. カテゴリ、サブカテゴリ、リスク、タグ、特性値を使用して、アプリケーションフィルタに追加するアプリケーションのタイプをフィルタリングします。ファイアウォールは、

フィルタ条件を満たす新しいアプリケーションをアプリケーション フィルタに自動的に追加します。



5. **OK** をクリックして、アプリケーションを新規または既存のアプリケーション フィルタに追加します。ファイアウォールには、アプリケーション フィルターの ステップ 3 で選択したアプリケーションが含まれています。
6. 変更を **Commit**（コミット）します。

ポリシー オプティマイザーを使用してアプリケーション グループにアプリを追加する

App-ID クラウド エンジン (ACE、またはコンテンツ提供の App-ID) から新しいアプリケーション グループまたは既存のアプリケーション グループにアプリ ID を追加し、セキュリティ ポリシー ルールのアプリケーション グループを使用して、セキュリティ ポリシーでクラウド App ID を制御します。

ACE は、以前に *SSL*、*Web* ブラウジング、不明 *tcp*、または不明 *udp* として識別されたアプリケーションに対して *App-ID* を提供します。

ポリシー オプティマイザー を使用して、ACE アプリ ID をアプリケーション グループに追加し、グループを複製または既存のルールに適用し、セキュリティ ポリシーで ACE アプリ ID を制御します。

STEP 1 | **2>policies** > セキュリティ に移動し、[ポリシー オプティマイザー > 新しいアプリ ビューアー を選択します。

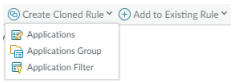
ファイアウォールまたは Panorama が ACE アプリ ID をダウンロードした場合、左側のナビゲーション ウィンドウに 新しいアプリ ビューアー の横に番号が表示されます。画面には、ダウンロードしたクラウドの App-ID と一致するセキュリティ ポリシー ルールが表示されます。

STEP 2 | アプリケーションと使用状況 ダイアログで、ルールに一致するクラウド配信アプリケーションを表示するには、セキュリティ ポリシー ルールの **App** 見 の番号をクリックします。

STEP 3 | 既存のアプリケーション グループまたは新しいアプリケーション グループに追加するアプリケーションを選択します。

並べ替えおよびフィルタ は、**App Seen** 内のアプリケーションを、サブカテゴリ、リスク、過去 30 日間に見られたトラフィックの量、またはアプリケーションが最初または最後に見た時点で実行できます。

STEP 4 | アプリケーションの処理方法に応じて、複製ルール または **[**既存のルールに追加**]**から**[{1<>**アプリケーション グループを選択します。



クローン作成ルール を使用して複製できるアプリケーションの最大数は、*1,000* 個のアプリケーションです。*1,000* を超えるアプリケーションを別のルールに移動する場合は、既存のルール に追加*]* を使用します。アプリケーションを新しいルールに移動する場合は、まずルールを作成します *(**Policies** >* セキュリティ*)* を作成してから、ポリシー オプティマイザーを使用してそのルールに追加します。

STEP 5 | 複製または既存のルールのアプリケーション グループを選択または作成します。アプリケーション グループの作成 ポリシー オプティマイザーを使用すると、**Objects** > アプリケーション グループ を使用してアプリケーション グループを作成するのと同様です。

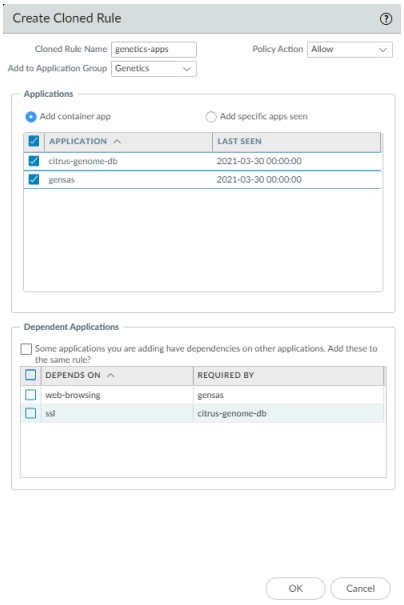
複製されたルールを作成:

1. クローンルール名（元のルールのすぐ上にあるセキュリティポリシールールベースに表示されるクローンルールの名前）を入力します。
2. ポリシー アクション (許可または拒否) を選択します。
3. **Add to Application Group** で、で選択したアプリケーションを追加するアプリケーション グループを選択します。
4. 追加コンテナー アプリ (既定) または 特定のアプリの表示 のみを選択します。

   コンテナー アプリを追加すると、そのコンテナー内のすべての機能アプリも追加されます。たとえば、「facebook」コンテナアプリを追加すると、Facebookベース、フェイスブックチャット、フェイスブック投稿などが追加され、コンテナに追加される将来のアプリケーションも追加されます。コンテナー アプリとその機能アプリは、アプリケーション グループを追加するセキュリティ ポリシールールの対象となります。コンテナー アプリを選択すると、コンテナーのアプリのセキュリティが実質的に将来的に保護され、自動化されるため、そのコンテナー内の新しいアプリをセキュリティ ポリシーに手動で追加する必要がなくなります。

   表示される特定のアプリのみを追加すると、選択したアプリケーションのみがアプリケーション グループに追加されます。同じコンテナー アプリ内の新しいアプリケーションがファイアウォールに到着した場合、アプリケーション グループはファイアウォールを制御しないので、新しいアプリの処理方法を手動で決定する必要があります。
5. アプリケーション グループに配置するアプリケーションが、他のアプリケーションを機能する必要がある場合もあります(依存します) 。このような場合、**> Cloned Rule** ダイアログ ボックスには 依存アプリケーション が含まれており、これらのアプリケーションを複

製されたルールに追加するかどうかを選択できます。選択したアプリケーションが正しく機能するように、依存アプリケーションをルールに追加します。

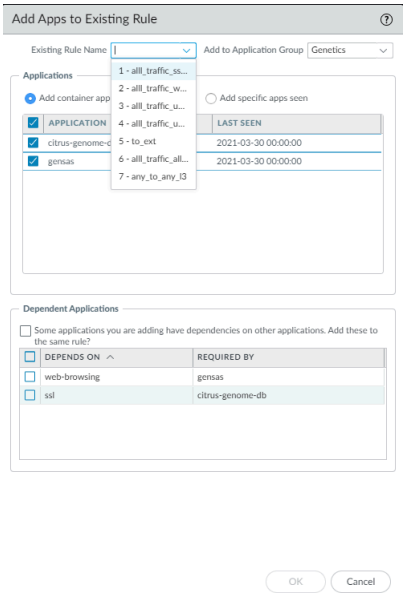


6. **OK** をクリックして、アプリケーションを新規または既存のアプリケーション グループに追加します。
7. 変更を **Commit**（コミット）します。

既存のルールにアプリを追加:

1. 選択したアプリケーションをアプリケーション グループの既存のルールに追加するには、既存のルール名 を選択します。
2. アプリケーション グループに追加 でアプリケーション グループを選択するか、新しいアプリケーション グループの名前を入力します。
3. ルールの複製と同様に、コンテナー アプリ または 特定のアプリを追加する を選択できます。コンテナー アプリを追加すると、コンテナー内のすべての機能アプリとそのコンテナーに追加される今後のアプリが追加されます。特定のアプリのみを追加すると、選択した特定のアプリのみが追加されます。
4. ルールの複製と同様に、場合によっては、アプリケーショングループに配置するアプリケーションは、機能するために他のアプリケーションを必要とします（依存します）。このような場合、アプリケーションを既存のルール に追加する] ダイアログ ボックスには 依存アプリケーション が含まれており、これらのアプリケーションを複製されたルールに

追加するかどうかを選択できます。選択したアプリケーションが正しく機能するように、依存アプリケーションをルールに追加します。



5. **OK** をクリックして、アプリケーションを新規または既存のアプリケーション グループに追加します。
6. 変更を **Commit**（コミット）します。

ポリシー オプティマイザーを使用してルールに直接 Apps を追加する

App-ID クラウド エンジン (ACE、またはコンテンツ提供の App-ID) を、複製または既存のルールに直接追加できます (ポリシー オプティマイザー です。ただし、アプリケーション フィルタ を使用して、ファイアウォールに到達した ACE App-ID を手動で追加するのではなく、セキュリティ ポリシーに自動的に追加することを検討してください。

ACE は、*ssl*、*Web* ブラウジング、不明 *tcp*、または不明 *udp* として以前に識別されたアプリケーションに対して *App ID* を提供します。

STEP 1 | **2>policies** > セキュリティ に移動し、[ポリシー オプティマイザー > 新しいアプリ ビューアー を選択します。

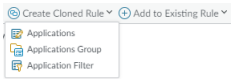
ファイアウォールまたは Panorama が ACE アプリ ID をダウンロードした場合、左側のナビゲーション ウィンドウに 新しいアプリ ビューアー の横に番号が表示されます。画面には、ダウンロードしたクラウドの App-ID と一致するセキュリティ ポリシー ルールが表示されます。

STEP 2 | アプリケーションと使用状況 ダイアログで、ルールに一致するクラウド配信アプリケーションを表示するには、セキュリティ ポリシー ルールの **App** 見 の番号をクリックします。

STEP 3 | 既存または複製されたセキュリティ ポリシールールに追加するアプリケーションを選択します。

並べ替えおよびフィルタ は、**App Seen** 内のアプリケーションを、サブカテゴリ、リスク、過去 30 日間に見られたトラフィックの量、またはアプリケーションが最初または最後に見た時点で実行できます。

STEP 4 | **Cloned rule** または 既存のルールに追加する から アプリケーション を選択します。



クローン作成ルール を使用して複製できるアプリケーションの最大数は、*1,000* 個のアプリケーションです。*1,000* を超えるアプリケーションを別のルールに移動する場合は、既存のルール に追加] を使用します。アプリケーションを新しいルールに移動する場合は、まずルールを作成します (***Policies*** > セキュリティ) を作成してから、ポリシー オプティマイザーを使用してそのルールに追加します。

STEP 5 | 選択したアプリケーションを複製されたルールまたは既存のルールに追加します。

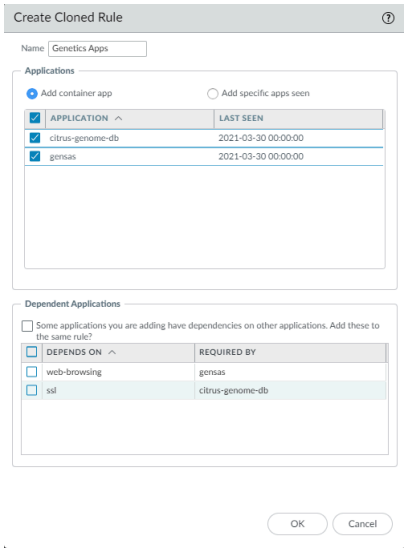
複製されたルールを作成:

1. 名前 (複製されたルールの名前) を入力します 元のルールのすぐ上のセキュリティ ポリシー ルールベースに表示されます)。複製されたルールには、元のルールと同じアクション (許可または拒否) があります。
2. 追加コンテナー アプリ (既定) または 特定のアプリの表示 のみを選択します。

   コンテナー アプリを追加すると、そのコンテナー内のすべての機能アプリも追加されます。たとえば、「facebook」コンテナアプリを追加すると、Facebookベース、フェイスブックチャット、フェイスブック投稿などが追加され、コンテナに追加される将来のアプリケーションも追加されます。コンテナーとその機能アプリは、複製するセキュリティ ポリシールールの対象となります。コンテナー アプリを選択すると、コンテナーのアプリのセキュリティが実質的に将来的に保護され、自動化されるため、そのコンテナー内の新しいアプリをセキュリティ ポリシーに手動で追加する必要がなくなります。

   表示される特定のアプリのみを追加すると、選択したアプリケーションのみが複製されたルールに追加されます。同じコンテナー アプリ内の新しいアプリケーションがファイアウォールに到着した場合、複製されたルールはファイアウォールを制御しないので、新しいアプリの処理方法を手動で決定する必要があります。
3. 場合によっては、ルールに追加するアプリケーションが、他のアプリケーションを機能する必要がある (依存する)。このような場合、**> Cloned Rule** ダイアログ ボックスには 依存アプリケーション が含まれており、これらのアプリケーションを複製されたルールに追加

するかどうかを選択できます。選択したアプリケーションが正しく機能するように、依存アプリケーションをルールに追加します。

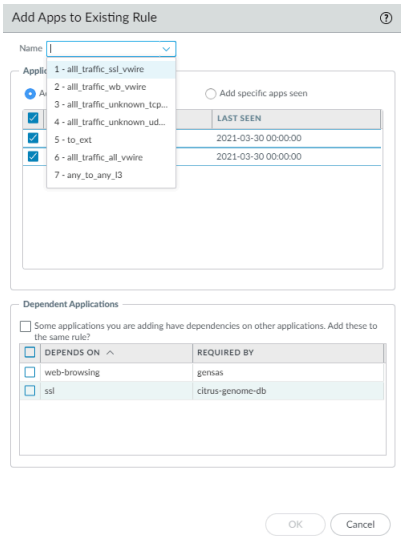


4. 複製されたルールにアプリケーションを追加するには、**OK** をクリックします。
5. 変更を **Commit**（コミット）します。

既存のルールにアプリを追加:

1. 選択したアプリケーションを追加する既存のルールの 名前 を選択します。
2. アプリケーションを追加するルールの複製と同様に、追加コンテナー アプリ または の特定のアプリを追加するかどうかを選択できます。コンテナー アプリを追加すると、コンテナー内のすべての機能アプリとそのコンテナーに追加される今後のアプリが追加されます。特定のアプリのみを追加すると、選択した特定のアプリのみが追加されます。
3. ルールのクローン作成と同様に、ルールに追加するアプリケーションが、他のアプリケーションを機能させる必要がある場合もあります。このような場合、アプリケーションを既存のルール に追加する] ダイアログ ボックスには 依存アプリケーション が含まれており、これらのアプリケーションを複製されたルールに追加するかどうかを選択できます。

選択したアプリケーションが正しく機能するように、依存アプリケーションをルールに追加します。



4. ［**OK**］をクリックして、既存のルールにアプリケーションを追加します。
5. 変更を **Commit**（コミット）します。

RMA ファイアウォール (ACE) を交換する

返品商品認証(RMA)がある場合に管理されたファイアウォールの設定を復元するには、次の手順を実行します。

- RMA ファイアウォールの交換を開始する前に を確認 .
- Panorama で、古いファイアウォールのシリアル番号を新しいファイアウォールのシリアル番号に置き換えます。
- ファイアウォール CLI で、ファイアウォールがオンラインで、ナレッジ サービスに接続されていることを確認し、ファイアウォールがクラウド アプリケーション カタログをダウンロードできるようにします。

  1. ファイアウォール CLI にアクセスします。
  2. 運用モードで、クラウドの App-ID 接続を確認します。

     ```
     admin @ vm1> show cloud-appid connection-to-cloud
     ```

     ファイアウォールがクラウドに接続されている場合、show コマンドは次のコマンドを返します。

     ```
     ACE Cloud サーバー: kcs.ace.tpcloud.paloaltonetworks.com:443Cloud 接続: 接続済み
     ```

     接続に関する情報も表示されます。ファイアウォールがクラウドに接続されていない場合は、DNS サービスが機能しているかどうかを確認し、ネットワークに関連するその他の問題がないかどうかを確認します。
- ファイアウォールが App-ID クラウドに接続されている場合、 交換後にファイアウォール構成を復元 。

ライセンスの有効期限または ACE の無効化による影響

ファイアウォールで App-ID クラウド エンジン (ACE) を有効にして ACE アプリ ID をファイアウォールにダウンロードし、アプリケーション フィルターやセキュリティ ポリシー ルールなどのオブジェクトでそれらの App-ID を使用する場合は、SaaS セキュリティインライン ライセンスの有効期限が切れた場合、または ACE を無効にした場合に何が起こるかを理解する必要があります。ACE と SaaS セキュリティ インライン ライセンスの有効期限を無効にすると、ダウンロードされた ACE アプリ ID、ACE アプリ ID のカタログ、ACE アプリ ID を制御するセキュリティ ポリシー ルール、ACE アプリ ID を含むオブジェクトの両方に影響します。特に明記されていない限り、効果は同じです。

- ACE アプリ ID はファイアウォール上に残りますが、ファイアウォールはセキュリティ ポリシーで ACE アプリ ID の適用を停止します。

  ACE アプリ ID を制御するセキュリティ ポリシー ルールは、ルールに表示されている場合でも ACE アプリ ID を制御しなくなりました。ファイアウォールで ACE が有効になる前に SSL、Web ブラウジング、不明 tcp、または不明 UDP の各ルールによって制御されていたトラフィックは、SaaS セキュリティ インライン ライセンスを更新してアクティブ化するか、ACE を再有効化するか、またはそれらのルールを変更するまで、これらのルールによって再び制御されます。
- ACE App-ID に基づくセキュリティ ポリシー ルールの適用は、ライセンスの有効期限が切れた 4 ~ 6 時間以内に停止します (ライセンスの状態を定期的にチェックするタイマーに基づく)。

  ACE App-ID に基づくセキュリティ ポリシー ルールの適用は、ファイアウォールで無効にする ACE をコミットした直後に停止します。

  > ***ACE*** を無効にすると、***SaaS*** セキュリティ インライン ライセンスが有効でアクティブな場合でも、変更をコミットするとすぐに ***ACE App-ID*** に基づくセキュリティ ポリシー ルールの適用が停止されます。
- ACE アプリ ID のカタログはファイアウォールと Panorama に残りますが、クラウド エンジンはカタログを更新しなくなりました。
- ファイアウォールから ACE への接続が機能しなくなります。ACE を再度有効にするか、SaaS セキュリティ インライン ライセンスを更新する場合は、カタログの更新をすべてダウンロードするのに時間がかかることがあります。
- SaaS セキュリティ インライン ライセンスの有効期限が切れると、ACE サービスは 4 ~ 6 時間以内に動作を停止します。

  > ***Panorama*** は ***SaaS*** セキュリティ インライン ライセンスを必要としないので、パノラマで有効期限が切れるライセンスはありません。ただし、管理対象ファイアウォールでライセンスの有効期限が切れると、***Panorama*** からそれらのファイアウォールに対する構成プッシュは、セキュリティ ポリシーまたはアプリケーション グループに ***ACE*** 構成が含まれている場合、失敗します。
- アプリケーション フィルターやアプリケーション グループなどのオブジェクトは変更されませんが、ACE アプリ ID が表示されている場合でも、それらのオブジェクトに配置した ACE アプリ ID は適用されなくなります。

- SaaS ポリシー勧告を使用している場合、ファイアウォールは SaaS ポリシーの推奨をプルできなくなるため、SaaS 管理者は新しいポリシーの推奨事項をファイアウォールにプッシュできません。ライセンスの有効期限が切れる前にダウンロードされたポリシーの推奨事項は構成に残りますが、適用されません (ライセンスの有効期限が切れたときや ACE が無効になったときに ACE App-ID で構成されたセキュリティ ポリシーと同じ動作)。

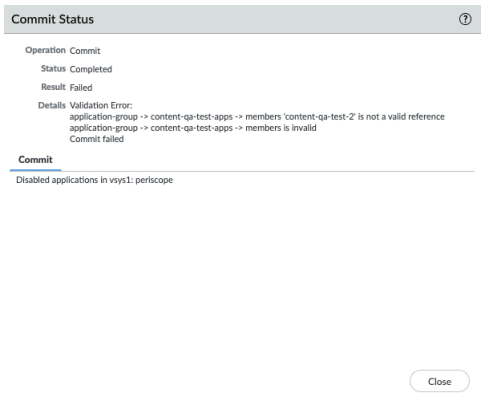
クラウド コンテンツロールバックによるコミットエラー

非常に可能性は低いですが、ACE App-ID は、不適切なメタデータやアプリケーションの問題のためにロールバック (元に戻す) 必要がある可能性があります。ACE が App-ID を元に戻す必要があり、それらの App-ID をセキュリティ ポリシー ルールで使用した場合 (直接またはアプリケーション グループ内)、コミット アクションは、アプリケーションがセキュリティ ポリシー ルールから削除され、オブジェクトから削除されるまで失敗します。

App-ID をロールバックする必要が出た場合、ACE は、最新のクラウドベースの App-ID、署名、メタデータ、カテゴリ、サブカテゴリ、およびタグを ACE カタログからすべて元に戻します。カタログから App-ID を削除すると、ファイアウォールから削除されるため、セキュリティ ポリシーで App-ID を使用するとコミットアクションが失敗します。

ACE がセキュリティ ポリシーでロールバックする必要があるアプリケーションを使用しなかった場合、構成に影響はなく、コミット操作は成功します。

ACE コンテンツのロールバック後に構成をコミットしようとすると、コミット失敗メッセージに、ACE が復帰したアプリケーションが一覧表示されます。 検証エラー の例のように、次の例を参照してください。



この問題を解決するには、ルールに直接追加されたか、アプリケーション グループを使用して追加されたかに関係なく、セキュリティ ポリシー ルールから一覧に表示されているアプリケーションを削除する必要があります。アプリケーションがアプリケーション グループで使用されている場合は、アプリケーション グループから削除します。

この例では、コンテンツ`-qa-test-2` は、アプリケーション グループ コンテンツ `qa-test-apps` で参照される、元に戻されたアプリケーションです。アプリケーション グループから コンテンツ `qa-test-2` を削除すると、コミット アクションは成功します。

App-ID クラウド エンジンのトラブルシューティング

このトピックでは、App-ID クラウド エンジン (ACE) の一般的なトラブルシューティング情報を提供します。

- アプライアンスに有効な SaaS セキュリティ インライン ライセンスが含まれるかどうかを確認するには、運用 CLI コマンド **show クラウド アプリ id 接続 -クラウド** を実行します。問題がある場合、コマンドはメッセージを返します。

  ACEエラー：ライセンスチェックに失敗しました。SaaSライセンスがインストールされ、activeCloud接続がインストールされているかどうかを確認します:失敗しました

  さらに、出力には、次の例の最後の接続が成功した時刻が表示されます。最後に正常に終了した **gRPC 接続:2021-05-20 16:00:00 -0800 PDT**

  ライセンスがインストールされていて、ACE への接続が良好な場合、コマンドは ACE クラウド サーバー接続の URL と状態 **Cloud 接続: connected** を、接続統計とデバイス証明書の状態 (証明書の有効期限を含む) と共に返します。
- Panorama は、管理対象ファイアウォールへのすべての/プッシュをコミットします。以下の条件のいずれかが存在することを確認し、それらを修復します。
  - 管理対象ファイアウォールに有効な SaaS セキュリティ インライン ライセンスがありますか?それでない場合、ACE カタログが存在せず、コミットの全て/プッシュ操作は失敗します。ACE App-ID を処理するためにファイアウォールを管理するかどうかに応じて、プッシュされた構成から ACE オブジェクトを削除して再試行するか、管理されたファイアウォールに有効な SaaS セキュリティインライン ライセンスをインストールして、カタログのダウンロードを待ちます。

    コンテンツ提供の *App ID* は *4000* 未満です。*ACE* カタログをダウンロードすると、ファイアウォール上に何千ものアプリケーションが表示され、***Objects > applications*** をチェックするか>運用可能な *CLI* コマンド ***show クラウド appid クラウド アプリ データ アプリケーション all*** を使用して新しいアプリ *ID* を確認できます。
  - 管理対象ファイアウォールと ACE の間の接続が切断されましたか?ACE クラウドへの接続を確認し、必要に応じて接続を復元します。

    運用 CLI コマンド 表示クラウド アプリ **id 接続 -クラウド** は、クラウド接続の状態と ACE クラウド サーバー URL を提供します。
  - Panorama の ACE カタログと管理対象ファイアウォールの ACE カタログが同期しなくて、ファイアウォールのカタログに含まれていない ACE アプリを含むプッシュされた構成が発生します。ファイアウォールと ACE 間の接続がアップしている場合、古くなったカタログは自動的に数分後に更新され、問題が解決されます。(5 分間待ってから、もう一度やり直してください。

    運用 *CLI* コマンド ***debug クラウド アプリ id クラウド 手動プル チェック-クラウド アプリ データ*** を実行して、カタログを手動で更新することもできます。

  - firewall はすべて PAN-OS 10.2 以降を実行していますか?(ACE アプリケーションおよびオブジェクトを参照する構成を、PAN-10 10.2 より前のバージョンを実行している firewall にプッシュすることは許可されていません。
- ACE 構成を持つ HA ペア (アクティブ/アクティブまたはアクティブ/パッシブ) で、操作コマンド **show session all** または **show session id <id>** を実行すると、ACE アプリケーションの出力にアプリケーション名ではなくグローバル App-ID 番号が表示されることがあります。ファイアウォールは、データ プレーンにクラウド アプリケーション データが含まれますが、アプリケーション名のみを表示します。それ以下の場合は、代わりにファイアウォールにアプリケーションのグローバル App-ID 番号が表示されます。
- 接続を ACE (gRPC 接続) にリセットするには、運用 CLI コマンド デバッグ クラウド アプリ **id** リセット接続 **-**クラウド を実行します。
- 運用 CLI コマンド 表示クラウド アプリ-データ アプリケーション を使用して、アプライアンスにダウンロードされた ACE アプリケーションを表示します。ダウンロードしたすべてのアプリまたは個々のアプリは、App-ID またはアプリケーション名で表示できます。
- 運用 CLI コマンド 表示クラウド **appid** 署名-**dp** 保留中要求 を使用して、ACE アプリ ID の保留中の要求を表示します。出力には、ファイアウォールが要求を ACE に送信した回数が含まれます (**tries** 。11 回の試行の後、送信操作はタイムアウトします。
- 操作可能な CLI コマンド **show** クラウド **appid** には、さらに便利なオプションがあります。

```
admin@PAN-ACE-VM-1> show cloud-appid ? > app-objects-in-policy
 Show application-filter/application-groups referred in policy >
 app-to-filtergroup-mapping Show application to matched filter and
 groups > application Show Application info for UI > application-
filter Show cloud apps in application-filters > application-group
 Show cloud apps in application-groups > cloud-app-data Show cloud
 application, container and metadata > connection-to-cloud Show
 gRPC connection status to cloud application server > ha-info Show
 statistics of cloud application high availability > overlap-appid
 Show duplicated applications in predefined content > signature-
dp Show cloud signatures and applications used on DP > task Show
 task on management-plane > transaction Show cloud application
 transaction > version Show Cloud-AppID version
```

- ACE のグローバル カウンターを表示するには、操作可能な CLI コマンド **show** カウンター グローバル フィルター値をすべてカテゴリ **cad** (**cad** は "クラウド アプリ識別" を表します。
- 共有メモリとの間で送受信されるパケットと、ACE、DLP、IoT などのサービスのセキュリティ クライアントとの間で送受信されるパケットの統計情報を表示するには、操作コマンド **show ctd** エージェント統計 を実行します。
- ユーザー インターフェイスを調べてアプリケーション フィルタに一致するアプリケーションの数が異なる場合、CLI を調べてみると、ファイアウォールがユーザー インターフェイスと CLI の一致するアプリケーションをカウントする方法が原因です。
  - **Objects** > アプリケーション フィルタ のアプリケーション フィルタを見ると、ファイアウォールが実際にそれらのアプリケーションを見て App-ID をダウンロードしたかどうか

に関係なく、ACE カタログ内のすべての一致するアプリケーションが表示され、数にはそれらのアプリケーションがすべて含まれます。

- `show cloud-appid` アプリケーションフィルター 操作コマンドを使用して CLI のアプリケーションフィルタを見ると、ファイアウォールが ACE アプリ ID をダウンロードした一致するアプリケーションの数のみがファイアウォールに表示されます。

このため、ユーザー インターフェイスは、同じアプリケーション フィルターの CLI よりも多くの一致するアプリケーションを表示する可能性があります。

ユーザー インターフェイスと *CLI* でアプリケーション グループを見ると、同じことがアプリケーション グループにも当てはまります。

- ACE アプリ ID は、セキュリティ ポリシーでのみサポートされています。ACE アプリ ID は、他のポリシーの種類ではサポートされていません。

  ただし、QoS または SD-WAN ポリシーを設定すると、ACE App-ID は表示され (選択可能)、ルールに適用されるアプリケーション グループまたはアプリケーション フィルタに存在する場合がありますが、QoS または SD-WAN ポリシーに追加してもアプリケーション トラフィックには影響しません。(QoS および SD-WAN ポリシーは、アプリケーション トラフィックを制御しません)。

SaaS アプリ ID ポリシーの推奨事項

SaaS アプリケーションの急増により、それらすべてを特定の App-ID に割り当て、それらのアプリケーションを可視化し、制御することが困難になります。SSL、Web ブラウジング、または「任意の」アプリケーションを許可するセキュリティ ポリシールールにより、ネットワークにセキュリティ リスクを引き起こす可能性のある、認可されていない SaaS アプリケーションが許可される場合があります。SaaSセキュリティ管理者は、これらのアプリケーションを可視化し、ファイアウォール上で制御するために、(ACE)が提供する特定のSaaS App-IDを持つセキュリティ ポリシールールをPAN-OSファイアウォール管理者に推奨することができます。PAN-OS 管理者は、SaaS セキュリティ インライン サブスクリプションを持つファイアウォールのルールをインポートできます。

SaaS ポリシーの推奨事項には、SaaS セキュリティ インライン サブスクリプションが必要です。***SaaS*** ポリシー推奨エンジンを使用する各アプライアンスは、生成してインストール に有効なデバイス証明書を作成してインストールするために、use Panorama を実行して、有効なデバイス証明書を生成およびインストールする必要があります。

SaaS セキュリティインライン接続 から ***Cortex*** データ レイク (CDL) は、***SaaS*** の可視性に必要です。 CDL へのログ転送 を構成し、セキュリティ ポリシー ルールで正しいログ転送プロファイルを使用してログ転送を有効にします。***SaaS*** セキュリティ インラインが正しく機能するためには、少なくともトラフィック ログと ***URL*** ログを ***CDL*** に転送する必要があります。

PAN-OS 10.2 以降をサポートするすべてのハードウェア プラットフォームは ***SaaS Policy Recommendation*** をサポートし、***SaaS Policy Recommendation*** を使用するすべてのアプライアンスには ***PAN-OS 10.2*** 以降が必要です。***Panorama*** は、***SaaS*** セキュリティ インライン ライセンスがインストールされていないファイアウォールや、***10.1*** より前のバージョンの ***PAN-OS*** を実行するファイアウォールに対して、***SaaS*** ポリシーの推奨事項をプッシュおよびコミットできません。

- ***SaaS*** セキュリティ管理者ガイド では、セキュリティ ポリシー ルールの推奨事項を作成し、ファイアウォールにプッシュする SaaS Security 管理者の手順について説明します。
- ***PAN-OS*** 管理者ガイド では、PAN-OS 管理者が SaaS セキュリティ管理者からポリシーの推奨事項をインポートおよび管理する方法について説明します。

SaaS Security 管理者は、新しいルールを作成し、アプリケーション、ユーザー、およびグループをルールに追加し、ルールのアクションを設定します。ルールアクションは許可またはブロックです。プッシュされたルールに対して他のアクションは許可されません。SaaS セキュリティ管理者は、適切なアプライアンスにルールをプッシュし、ルールがファイアウォール インターフェイスに表示されます (**Device** > ポリシー推奨事項 > **SaaS**

PAN-OS 管理者は、推奨される規則を評価し、ファイアウォールに実装するかどうかを決定します。PAN-OS 管理者がルールの実装を選択した場合、管理者はルールをファイアウォールにインポートし、ファイアウォールルールベース内のポリシールールの配置先を選択します。PAN-OS

管理者がポリシー推奨をインポートすると、ファイアウォールによって必要な HIP プロファイル、タグ、およびアプリケーション グループが自動的に作成されます(PAN-OS 管理者は手動で行う必要はありません)。

SaaS Security 管理者がポリシー推奨のセキュリティ プロファイルをプッシュし、それらのプロファイルがファイアウォールに存在しない場合、ファイアウォールのインポートは失敗します。プロファイルが既にファイアウォールに存在する場合、インポートは成功します。

SaaS セキュリティ管理者がポリシー ルールの推奨事項を更新すると、PAN-OS 管理者は更新プログラムを確認し、ファイアウォールにインポートします。SaaS セキュリティ管理者がポリシー ルールの推奨事項を削除すると、PAN-OS 管理者はそのアクションを確認し、ファイアウォール セキュリティ ポリシー ルールベースからルールを削除します。

SaaS セキュリティ インライン ライセンスの有効期限が切れると、ファイアウォールは *SaaS* ポリシーの推奨事項を引き出さなくなるため、新しい推奨事項は表示されません。ただし、既にインポートしたセキュリティ ポリシー ルールは引き続き機能します。

ACE を無効にすると、ファイアウォールは新しいクラウド アプリケーション署名と *App-ID* を受信しなくなり、新しい *ACE* アプリ *ID* に基づいて、ファイアウォールは *SaaS* ポリシーの推奨事項をインポートできません。

ACE 展開プロセス (クラウドへの接続、デバイス証明書のインストール、SaaS セキュリティ ポータルでのライセンスの有効化、Panorama およびファイアウォールへのプッシュなど) も SaaS ポリシーの推奨設定を行います。

すべてのアプライアンスを最新の脅威 コンテンツ更新プログラム に更新します。

この新機能のユーザー インターフェイスの追加には、次のものがあります。

- デバイス > ポリシー推奨 > **SaaS** は、SaaS 管理者からのポリシー推奨事項を表示し、ファイアウォール管理者が推奨 SaaS ポリシーをインポート、更新、削除、および制御できるようにします。このページの表示には、SaaS 管理者がポリシー用に構成したアプリケーション グループが含まれます。
- ロールベースのインターフェイス アクセス (**Device** > **Admin** ロール) は、SaaS ポリシーの推奨アクセス許可の **Web UI** タブに新しいオプションを持っています。デバイス > ポリシー推奨 > **SaaS**.
- SaaS ポリシーの推奨事項には、インターフェイスの **Tags** 列に表示される **SaaSSecurityRecommended** というタグが自動的に付けられます。

SaaS 管理者によってプッシュされた SaaS ポリシーの推奨事項をインポートおよび更新し、SaaS 管理者が削除した SaaS ポリシーの推奨事項を削除できます。

- SaaS ポリシーの推奨のインポート
- 更新された SaaS ポリシーの推奨事項をインポート

- 削除された SaaS ポリシーの推奨を削除する

SaaS ポリシーの推奨のインポート

SaaS セキュリティ管理者がセキュリティ ポリシー ルールの推奨事項を PAN-OS ファイアウォールにプッシュすると、PAN-OS ファイアウォール管理者はファイアウォール上でこれらのルールをインポートして、ポリシー推奨のアプリケーションを可視化して制御できます。

SaaS 管理者のポリシーの推奨事項とプッシュ手順については、*SaaS* セキュリティ管理者ガイドを参照してください。この手順では、PAN-OS 管理者がポリシーの推奨事項をインポートする方法を示します。

SaaS Security 管理者がポリシー推奨のセキュリティ プロファイルをプッシュし、それらのプロファイルがファイアウォールに存在しない場合、ファイアウォールのインポートは失敗します。プロファイルが既にファイアウォールに存在する場合、インポートは成功します。

STEP 1 | デバイス > ポリシー推奨 > **SaaS** と ポリシー推奨**<** > ポリシー推奨事項 > **SaaS** }は、SaaS 管理者からプッシュされたすべての SaaS ポリシー推奨事項を示します。Panorama から管理対象ファイアウォールにポリシーの推奨事項をプッシュします。

STEP 2 | **SaaS** ポリシーの推奨事項が最新であることを確認するために、 > **Device** > ポリシー推奨パノラマ > ポリシー推奨 > **SaaS**) を更新します。

Panorama から管理対象ファイアウォールにポリシーの推奨事項をプッシュする場合はいつでも、ファイアウォール上のページを更新 ( ) して、推奨事項が最新であることを確認します。

新しくプッシュされたポリシーの推奨事項が画面の上部に表示されます。**Active** 推奨事項 は **active** の値を示し、新しい更新プログラムが利用可能 は はい の値を示しています。

STEP 3 | 新しいポリシーの推奨事項を選択します。

一度に 1 つのポリシー推奨をインポートします。アプリケーション 列には、各ポリシーの推奨事項に対するアプリケーション グループが表示されます。グループの名前をクリックすると、そのグループ内のアプリケーションが表示されます。

Device 列には、SaaS 管理者がルールに対して構成したソース デバイスが表示されます。ソース デバイスの前に"SaaS" という用語が付きます。ソース デバイスは次のことができます。

- MCD:管理対象準拠デバイス
- MNCD:管理対象非準拠デバイス
- UMCD -アンマネージ 準拠デバイス
- UMNCD - 非準拠デバイス

たとえば、**SaaS - MCD** は、管理対象の準拠ソース デバイスを示します。

STEP 4 | インポート ポリシー ルール。

インポート ポリシー ルール ダイアログで、次の手順を実行します。

- **Name**- ルールの意図を説明する名前を使用して、インポートされたルールに名前を付けます。

  セキュリティ ポリシー ルールベースに既に存在するルール名を指定すると、インポートされたルールによって既存のルールが上書きされます。

- ルールの後- インポートされた SaaS ルールを配置する後のルールを選択します。ファイアウォールのルールベースと、新しいルールが既存のルールにどのような影響を与えるかを考えます。ルールを選択しない場合 (ルール選択なし)、そのルールはセキュリティ ポリシー ルールベースの一番上に配置されます。場合によっては、ルールを配置する場所ではありません。たとえば、QUIC プロトコルのブロックなど、特定のブロック ルールを常にルールベースの最上位にする必要があります。インポートされたルールの意図に注意し、既存のルールをシャドウしないように注意してください。

説明 は、SaaS 管理者がルールを作成したときに入力された説明に由来します。変更することも、そのままにすることもできます。

インポート プロセスでは、ポリシーの推奨事項でアプリケーションのアプリケーション グループが自動的に作成されます。アプリケーション グループの名前は、*SaaS Security* 管理者がルールに与えた名前から派生します。また、ファイアウォールは、*SaaS* 管理者がルールに適用した *HIP* プロファイルとタグも自動的に作成します。

STEP 5 | **OK** をクリックしてルールをインポートし、ルール後 で選択した位置にあるセキュリティ ポリシー ルールベースに追加します。

STEP 6 | "セキュリティ ポリシールールが正常に更新されました" というステータス メッセージが表示されたら、[**OK** をクリックします。

Location 列に、SaaS 管理者がルールをプッシュした vsys に対応するファイアウォール上のルールの場所 (vsys) が表示されるようになりました。

STEP 7 | インポートされたポリシー ルールがセキュリティ ポリシー ルールベース (セキュリティ > **Policies**) 内の指定された場所に存在し、ファイアウォールが関連付けられたオブジェクトを作成したことを確認します。

たとえば、セキュリティ ポリシールールを確認して、次の項目を確認します。

- ルールの ソース デバイス が設定され、[**Source** タブにルールのソース デバイスが表示されます。
- アプリケーション グループは、ルールの アプリケーション タブにデータを入力します。
- 関連付けられたプロファイルは、ルールに関連付けられます (**Actions** タブ)。

また、次の点も確認してください。

- **Objects** > アプリケーション グループ は、インポートされたアプリケーション グループを示しています。
- オブジェクト > **GlobalProtect** > **HIP** オブジェクト および オブジェクト > **GlobalProtect** > **HIP** プロファイル は、SaaS セキュリティ管理者からプッシュされた HIP 情報を表示します。

更新された SaaS ポリシーの推奨事項をインポート

SaaS セキュリティ管理者がセキュリティ ポリシー ルールの推奨事項を PAN-OS ファイアウォール (または Panorama) にプッシュすると、PAN-OS 管理者はこれらのルールをインポートして、ポリシー勧告でアプリケーションを可視化および制御できます。ただし、SaaS 管理者が、アプリケーションの追加や削除などによってルールを更新する場合は、ファイアウォールでルールも更新する必要があります。

SaaS Security 管理者が新規または更新されたアプリケーショングループ、*HIP* プロファイル、またはタグをプッシュすると、ファイアウォールはそれらのオブジェクトを自動的に作成または更新します。*SaaS Security* 管理者がポリシー推奨の更新を使用してセキュリティ プロファイルをプッシュし、それらのプロファイルがファイアウォールに存在しない場合、ファイアウォールのインポートは失敗します。プロファイルが既にファイアウォールに存在する場合、インポートは成功します。

STEP 1 | 更新（ ）デバイス > ポリシーの推奨事項 > **SaaS** （または **Panorama** > ポリシー 推奨事項 > **SaaS** ）を使用して、SaaS管理者がファイアウォールにプッシュした最新のSaaSポリシーの推奨事項をすべて表示できるようにします。

STEP 2 | 新しい更新プログラムが利用可能を確認します。

新しい更新プログラムが利用可能 列の値が いいえ の場合、ルールの更新はありません。値が はい の場合、SaaS 管理者は、ルールの更新をファイアウォールにプッシュしました。さらに、アクティブ推奨 は **active** の値を示します。

STEP 3 | [アプリケーション 列のアプリケーション グループ名をクリックして、ルールが制御する更新されたアプリケーションの一覧を表示します。

STEP 4 | 更新するポリシーの推奨事項を選択します。

一度に 1 つのポリシー推奨事項のみを更新します。

STEP 5 | ポリシールールをクリックしてポリシーをインポートします (ルールに更新がない場合、このオプションはグレー表示され、選択できません)。

ポリシールール のインポート] ダイアログが表示されます。名 は既に設定されているため、ルールが既にインポートされているため変更できません。後のルール もダイアログで変更することはできませんが、セキュリティ ポリシー ルールベースでルールの場所を変更する場合は、**Policies** > **Security** でセキュリティ ポリシー ルールの位置を変更するのと同じ方法で変更できます。説明を変更するか、そのままにしておくことができます。

STEP 6 | **OK** をクリックします。

STEP 7 | 変更の確認 で をクリックして更新されたルールをインポートします **(**変更されたルールをインポートしない場合は**no** をクリックします)。

ファイアウォールは、ルールに関連付けられたアプリケーショングループ、HIPプロファイル、タグに対して自動的に変更を行います。

削除された SaaS ポリシーの推奨を削除する

SaaS セキュリティ管理者がセキュリティ ポリシー ルールの推奨事項を PAN-OS アプライアンスにプッシュすると、PAN-OS 管理者はこれらのルールをインポートして、ポリシー推奨事項のアプリケーションを可視化および制御できます。ただし、SaaS セキュリティ管理者がルールを削除した場合は、そのルールを PAN-OS アプライアンスからも削除する必要があります。

SaaS セキュリティ管理者がルールを削除すると、**Active** 推奨事項 列に 削除 が表示されます (有効なルールの場合、値は **active** です。

STEP 1 | SaaS セキュリティ管理者 削除 のルールを選択します (一度に削除するルールは 1 つのみ選択できます)。

ポリシールール オプションは、ルールをインポートできなくなるため、グレー表示されています。

STEP 2 | 推奨マッピングの削除をクリックします。

これにより、ファイアウォール上のセキュリティ ポリシールールのローカル マッピングが削除されます。たとえば、場所、ユーザー、およびルールへのマッピングは削除されます。推奨マッピングの削除 ダイアログ ボックスにルールの場所が表示され、ルールが削除された場所がわかります。

STEP 3 | **OK** をクリックします。

STEP 4 | 変更の確認 ダイアログで、[はい をクリックして、ポリシー推奨データベースからルールを削除します。

このアクションは、ポリシーの推奨ルールリストからルールを削除するだけです。セキュリティ ポリシー ルールベースからルールは削除されません。ルールベースからルールを手動で削除する必要があります。

STEP 5 | **Status** ダイアログボックスが表示され、ポリシーの推奨マッピングが削除されたことが確認されますが、セキュリティ ポリシールールベースからルールを削除する必要があります。

STEP 6 | **2>2>**ポリシー > セキュリティ に移動し、セキュリティ ポリシー ルールベースからルールを削除します。

アプリケーション レベル ゲートウェイ

Palo Alto Networks のファイアウォールはトラフィックをポートやプロトコルによって分類せず、App-ID テクノロジを使用してアプリケーションを一意のプロパティやトランザクションの特性に基づいて識別します。ただし、一部のアプリケーションでは接続を確立するためにファイアウォールがダイナミックにピンホールを開き、セッションのパラメータを決定し、データ転送に使用するポートをネゴシエートする必要があります。これらのアプリケーションはアプリケーション レイヤーのペイロードを使用して、アプリケーションがデータ接続を開くダイナミック TCP または UDP ポートと通信します。そのようなアプリケーションに対して、ファイアウォールはアプリケーション レベル ゲートウェイ（ALG）として機能し、時間を限定して転送データまたは制御トラフィックのみのためにピンホールを開きます。また、ファイアウォールは必要に応じてペイロードの NAT 書き換えを実行します。

- *H.323*（*H.225* および *H.248*）ゲートキーパー ルーティング モードでは、*ALG* はサポートされていません。
- ファイアウォールが *SIP*（*Session Initiation Protocol*）に対して *ALG* として機能する場合、デフォルトではペイロードに対して *NAT* を実行し、メディア ポートのためにダイナミック ピンホールを開きます。環境で使用されている *SIP* アプリケーションによっては、*SIP* エンドポイントでクライアントに *NAT* インテリジェンスが組み込まれている場合があります。そのような場合、ファイアウォールがシグナリング セッションを変更しないように *SIP ALG* 機能を無効にする必要がある場合があります。*SIP ALG* を無効にした場合、*App-ID* がセッションを *SIP* と判断すると、ペイロードは変換されず、ダイナミック ピンホールは開きません。SIP アプリケーション レベル ゲートウェイ（ALG）を無効にするを参照してください。

dynamic IP and port (ダイナミック*IP*およびポート - *DIPP) NAT* を使用する場合、*Palo Alto Networks* ファイアウォール *ALG* デコーダは、*SIP* ヘッダー（*Contact* フィールドおよび *Via* フィールド）の下に *IP* およびポート（送信元アドレスおよび送信元ポート）の組み合わせを必要とし、上記ヘッダーを翻訳したり、それらに基づいて予測セッションを開いたりできます。

次の表は、IPv4、NAT、IPv6、NPTv6、および NAT64 ALG をリストし、ALG が各プロトコル（SIP など）をサポートしているかどうかをチェックマークで示しています。

App-ID	IPv4	NAT	IPv6	NPTv6	NAT64
SIP	✓	✓	✓	—	—
SCCP	✓	✓	✓	—	—
MGCP	✓	✓	—	—	—

App-ID	IPv4	NAT	IPv6	NPTv6	NAT64
FTP	✓	✓	✓	✓	—
RTSP	✓	✓	✓	✓	—
MySQL	✓	✓	—	—	—
Oracle/SQLNet/TNS	✓	✓	✓	✓	—
RPC	✓	✓	—	—	—
RSH	✓	✓	—	—	—
UNIStim	✓	✓	—	—	—
H.225	✓	✓	—	—	—
H.248	✓	✓	—	—	—

SIP アプリケーション レベル ゲートウェイ（ALG）を無効にする

Palo Alto Networks のファイアウォールは、SIP （Session Initiation Protocol）アプリケーション レベル ゲートウェイ（ALG）を使用して、NAT が有効になっているファイアウォールにダイナミック ピンホールを開きます。ただし、VoIP など一部のアプリケーションではクライアント アプリケーションに NAT インテリジェンスが組み込まれています。これらの場合、ファイアウォールの SIP ALG がシグナリング セッションと干渉し、クライアント アプリケーションが動作しなくなることがあります。

この問題に対する 1 つの解決策は、SIP に対してアプリケーション オーバーライド ポリシーを定義することですが、このアプローチでは、App-ID および脅威検出機能が無効になります。もっと良い方法は SIP ALG を無効にすることです。このアプローチでは App-ID や脅威検出は無効になりません。

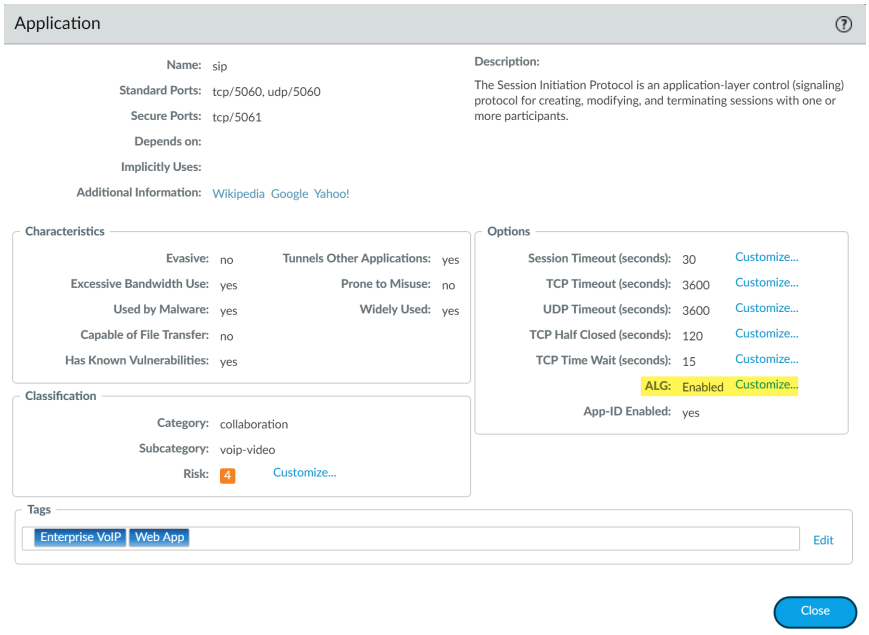
SIP ALG を無効にするには以下の手順を実行します。

STEP 1 | **Objects (オブジェクト)** > **Application Filters (アプリケーション フィルタ)** を選択します。

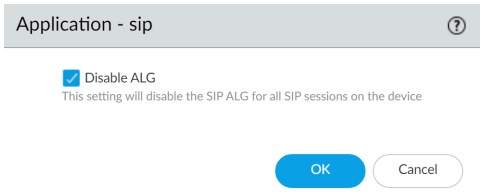
STEP 2 | **sip** アプリケーションを選択します。

Search [検索]ボックスに「**sip**」と入力すると、sip アプリケーションを検索できます。

STEP 3 | Application [アプリケーション]ダイアログ ボックスの Options [オプション]セクションで **ALG** の **Customize** [カスタマイズ...]を選択します。



STEP 4 | Application - sip（アプリケーション - sip）ダイアログ ボックスで **Disable ALG**（ALG の無効化）チェックボックスをオンにし、**OK** をクリックします。



STEP 5 | Application（アプリケーション）ダイアログ ボックスを**Close**（閉じる）で閉じ、変更を**Commit**（コミット）します。

HTTP ヘッダーを使用して SaaS アプリケーションのアクセスを管理する

不許可とされている SaaS アプリケーションの使用は、ユーザーがネットワーク外の機密情報を、通常は消費者バージョンのアプリケーションにアクセスすることによって送信する手段になります。ただし、特定の個人や組織に対してこれらのアプリケーションのエンタープライズ版へのアクセスを許可する必要がある場合、SaaS アプリケーションを完全にブロックすることはできません。

カスタム HTTP ヘッダーを使用すると、特定のエンタープライズ アカウントを許可しながら SaaS の消費者アカウントを許可することができます。多くの SaaS アプリケーションは、特定の HTTP ヘッダーに含まれる情報に基づいてアプリケーションへのアクセスを許可または禁止します。事前定義されたタイプを使用して HTTP ヘッダー挿入エントリを作成して、Google G Suite や Microsoft Office 365 などの一般的な SaaS アプリケーションへのアクセスを管理できます。Palo AltoNetworks® は、コンテンツ更新を使用して、これらのアプリケーションに固有の定義済みのルール セットを維持するとともに、新しい定義済みのルールセットを追加します。

また、HTTP ヘッダーを使用して、Palo Alto Networks が定義済みのルール セットを提供していないサービスへのアクセスを制限する SaaS アプリケーションへのアクセスを管理する場合は、カスタム HTTP ヘッダー挿入エントリを作成 することもできます。

市販の SaaS アプリケーションは常に SSL を使用するので、HTTP ヘッダー挿入を実行するには復号化が必要です。トラフィックがアップストリーム ファイアウォールによってまだ復号化されていない場合は、SSL 転送プロキシの復号化を使用してトラフィックを復号化するようにファイアウォールを設定できます。

この機能の使用に ***URL*** フィルタリング ライセンスは不要です。

HTTP ヘッダーを使用して SaaS アプリケーションを管理する方法の理解を深めるには、以下を参照してください：

- SaaS カスタム ヘッダーについて理解する
- 定義済みの SaaS アプリケーション タイプで使用されるドメイン
- 事前定義のタイプを使用した HTTP ヘッダー挿入エントリの作成
- カスタム HTTP ヘッダーの挿入エントリを作成する

SaaS カスタム ヘッダーについて理解する

始める前に、管理する SaaS アプリケーションで使用する予定のカスタム HTTP ヘッダーを理解しましょう。これらのヘッダーで達成できるものと、目標を達成するために指定する必要がある情報を理解する必要があります。

カスタム ヘッダーを使用する SaaS アプリケーションでは、必ずしもそれらを使用して種類のアカウントへのアクセスを制御するわけではありません。たとえば、Palo AltoNetworks® は、ネットワーク ユーザーが制限付きのコンテンツにアクセスできるかどうかを判断する、YouTube カスタム ヘッダーの事前定義されたサポートを提供します。

また、アクセスを制御する SaaS アプリケーションのドキュメントを読んで、そのアプリケーションに使用する必要があるヘッダーは何かを理解するとよいでしょう。

HTTP ヘッダーの挿入には、次の制限が適用されます。

- ヘッダー名の文字長：*100*
- ヘッダー値の文字長:*16K*。

一部の *SaaS* アプリケーションでは、これらの制限を超えるカスタム ヘッダー名を定義したり、カスタム ヘッダーに値を割り当てたりする可能性があることに注意してください。これらの状況はまれであるはずですが、*SaaS* アプリケーションがこれらの文字長制限の *1* つまたは両方を超える場合、次世代ファイアウォールはその *SaaS* アプリケーションへのアクセスを正常に管理できません。

次の表に、Palo Alto Networks が事前定義されたサポートを提供する SaaS アプリケーションに使用できるヘッダーを示します。各ヘッダーには、そのヘッダーに固有の詳細情報へのリンクも含まれています。

アプリケーション	ヘッダー	詳細情報
Dropbox	`X-Dropbox-allowed-Team-Ids`	www.dropbox.com/help/business/network-control 確認済みの Enterprise Dropbox アカウントへのアクセスを許可することができます。このヘッダーの値はビジネス アカウントのチーム IDで、Dropbox 管理コンソールのネットワーク コントロール セクションから取得できます。この機能を同じ場所から有効にする必要があります。 このヘッダーの管理の詳細、およびトラフィックを復号化できるように Dropbox クライアントを有効にする方法については、Dropbox アカウント担当者にお問い合わせください。
Google G Suite	`X-GooGApps-Allowed-Domains`	support.google.com/a/answer/1668854?hl=en ドメインの特定の Google アカウントへのアクセスを許可することができます。このヘッダーに付ける値は、ドメインとサブドメインです。 Google アプリケーションのヘッダーを正常に挿入するには、次の操作も必要になります:

アプリケーション	ヘッダー	詳細情報
		1. 次のカテゴリと URL を含む SSL 復号化プロファイル を作成します。 • ビジネスと経済 • コンピュータとインターネットの情報 • コンテンツ配信ネットワーク • インターネット通信とテレフォニー • 低リスク • online-storage-and-backup • search-engine • Web ベースの電子メール • drive.google.com • *.google.com • *.googleusercontent.com • *.gstatic.com 2. HTTP ヘッダー挿入は現在 HTTP/2 をサポートしていません。ヘッダーを挿入するには、適切な復号プロファイル内の **Strip ALPN** 機能を使用して HTTP/2 接続を HTTP/1.1 にダウングレードします。詳細については、App-ID および HTTP/2 検査を参照してください。 3. ファイアウォールはこのプロトコルのヘッダー挿入をサポートしていないため、Quick UDP インターネット接続 (QUIC) App-ID をブロックするルールを作成し、セキュリティ ポリシーの最上位に配置します。これを行うと、アプリケーションは前の手順でファイアウォールが処理した HTTP/2 over TLS の使用に戻ります。
Microsoft Office 365	`Restrict-Access-To-Tenants` `Restrict-Access-Context`	docs.microsoft.com/en-us/azure/active-directory/active-directory-tenant-restrictions ユーザーがアクセスできるようにするテナントのリストを `Restrict-Access-To-Tenant` に提供します。テナントに登録されているドメインを使用して、このリストのテナントを識別することができます。

アプリケーション	ヘッダー	詳細情報
		テナントの制限を設定しているディレクトリ ID を `Restrict-Access-Context` に指定します。ディレクトリ IDは Azure ポータルで検索できます。管理者としてサインインし、**Azure Active Directory**を選択してから、**Properties**（プロパティ）を選択します。
YouTube	`YouTube-Restrict`	support.google.com/a/answer/6214622?hl=en このヘッダーには、ユーザーに表示させたいビデオの種類に関する情報が表示されます。**Strict**（厳格）または**Moderate**（中）のいずれかの設定を指定できます。これらの異なる設定の詳細については、support.google.com/a/answer/6212415を参照してください。

定義済みの SaaS アプリケーション タイプで使用されるドメイン

SaaS アプリケーションは HTTPS を使用するため、このトラフィックにカスタム ヘッダーを挿入するには、カスタム ヘッダーを復号化する必要があります。カスタムヘッダーを復号化するためにファイアウォールで利用可能な転送プロキシ復号化を使用する場合は、トラフィックに関連するドメインを識別することによって復号化する特定の HTTPS トラフィックを特定する必要があります。次の表は、Palo AltoNetworks® が事前定義済みのルールを提供している各 SaaS アプリケーションの関連するドメインを示しています。

アプリケーション	ドメイン
Dropbox	`*.dropbox.com`
G Suite	`*.google.com` `gmail.com`

Microsoft Office 365	`login.microsoftonline.com`
	`login.microsoft.com`
	`login.windows.net`

YouTube	`www.youtube.com` `m.youtube.com`

アプリケーション	ドメイン
	youtubei.googleapis.com youtube.googleapis.com www.youtube-nocookie.com

事前定義のタイプを使用した HTTP ヘッダー挿入エントリの作成

STEP 1 | HTTPS トラフィックの復号化が済んでいるアップストリーム デバイスがない場合は、SSL 転送プロキシの設定の復号化を使用して復号化を設定します。

> *Dropbox* 用 *SSL* 暗号化を設定中の場合は、*Dropbox* クライアントも *SSL* トラフィックを許可するように設定する必要があります。こうした手順は、*Dropbox* 固有のものであり、これらの手順を入手するには *Dropbox* アカウント担当者にご連絡ください。

1. 管理中の SaaS アプリケーションのカスタム URL カテゴリ **Add**（追加）します（**Objects**（オブジェクト） > **Custom Objects**（カスタム オブジェクト） > **URL Category**（**URL** カテゴリ））。
2. カテゴリの **Name**（名前）を指定します。
3. 管理している、またはヘッダーにユーザー名とドメインを挿入する SaaS アプリケーションに固有のドメインを**Add**（追加）します。定義済みの SaaS アプリケーションのそれぞれに使用するドメインの一覧については、「事前定義された SaaS アプリケーションのタイプ」で使用されるドメイン」を参照してください。HTTP ヘッダーにユーザー名とドメインを含めるように firewall を構成する方法の詳細については、HTTP ヘッダーにユーザー名の挿入を参照してください。

   各ドメイン名は最大 254 文字まで入力することができ、エントリごとに最大 50 のドメインを識別できます。ドメイン リストはワイルドカードをサポートしています（たとえば、**`*.example.com`**）。ベストプラクティスとして、ワイルドカード（たとえば、**`*.*.*`**）をネストしないでください。また、同じ URL プロファイル内のドメインを重複させないでください。
4. SaaS アプリケーション管理の場合、Create a Decryption Policy Rule（復号化ポリシー ルールの作成）を行い、この手順に従って、以下を設定します。
   - **Service/URL Category**（サービス/**URL**カテゴリ） タブで、前のステップで作成した **URL Category**（**URL** カテゴリ）を **Add**（追加）します。
   - **Options**（オプション）タブ内で、make sure the **Action**（操作） が **Decrypt**（復号）に設定されていること、および **Type**（タイプ）が **SSL Forward Proxy**（**SSL** 転送プロキシ）に設定されていることを確認します。

STEP 2 | URL フィルタリングのプロファイルを編集/追加します。

STEP 3 | **URL Filtering Profile**（**URL** フィルタリングのプロファイル）ダイアログの **HTTP Header Insertion**（**HTTP** ヘッダーのルール）を選択します。

STEP 4 | エントリを **Add**（追加）します。

1. このエントリの**Name**（名前）（最大100文字）を指定します。
2. 事前定義済み**Type**（タイプ）を選択します。

   これにより、**Domains**（ドメイン）と **Headers**（ヘッダー）リストが表示されます。
3. 各**Header**（ヘッダー）に対して **Value**（値）を入力します。

   各ヘッダー値は、最大 16KB 文字にすることができます。
4. （オプション）ヘッダーの挿入アクティビティーのロギングを使用可能にするには、**Log**（ログ）を選択します。

   許可されたトラフィックはログに記録されないため、許可されたトラフィックのヘッダー挿入はログに記録されません。
5. **OK** をクリックして変更内容を保存します。

STEP 5 | Security Policy（セキュリティポリシー）ルールを**Add**（追加）または編集して、（**Policies**（ポリシー） > **Security**（セキュリティ））HTTP ヘッダー挿入 URL フィルタリング プロファイルを含めます 。

- SaaS アプリケーション管理の場合、このヘッダー挿入ルールを設定している SaaS アプリケーションにユーザーがアクセスするのを許可します。
- ユーザー名とドメインを HTTP ヘッダーに含めるには、HTTP または HTTPS トラフィックのセキュリティ ポリシー ルールに URL フィルタリング プロファイルを適用します。
  1. ステップ 2 で編集/作成したフィルタリングのプロファイルを選択します（**Actions**（操作） > **URL Filtering**（**URL** フィルタリング））。
  2. **OK** をクリックして保存して、変更を **Commit**（コミット）します。

STEP 6 | ファイアウォールがヘッダーを正しく挿入していることを確認します。

- Saas アプリケーション管理の場合、エンドポイントから、SaaS アプリケーションへのアクセスが期待どおりに機能していることを確認します。
  1. アクセスできると思われるアカウントまたはコンテンツにアクセスしてみてください。SaaSアカウントまたはコンテンツにアクセスできない場合、構成は機能していません。
  2. ブロックされると思われるアカウントまたはコンテンツにアクセスしてみてください。SaaSアカウントまたはコンテンツにアクセスできる場合、構成は機能していません。
  3. 前の手順の両方が期待どおりに機能する場合は、View Logs (手順 4.4 でログ記録を構成した場合) でき、記録された HTTP ヘッダー挿入アクティビティが表示されます

カスタム HTTP ヘッダーの挿入エントリを作成する

STEP 1 | HTTPS トラフィックを復号化しているアップストリーム デバイスがまだない場合は、SSL Forward Proxy を構成します。

1. **Add** は、管理している SaaS アプリケーションのカスタム URL カテゴリです (**Objects** > **Custom Objects** > **URL** カテゴリ)。
2. カテゴリの **Name**（名前）を指定します。
3. 管理中の SaaS アプリケーション固有のドメインを **Add**（追加）します。
4. 復号化ポリシーのルールを作成して、この手順に従って、以下を設定します：
   - **Service/URL Category**（サービス/URLカテゴリ） タブで、前のステップで作成した **URL Category**（**URL** カテゴリ）を **Add**（追加）します。
   - **Options**（オプション）タブ内で、make sure the **Action**（操作） が **Decrypt**（復号）に設定されていること、および **Type**（タイプ）が **SSL Forward Proxy**（**SSL** 転送プロキシ）に設定されていることを確認します。

STEP 2 | 編集または URL Filtering プロファイルを作成。

STEP 3 | URL Filtering Profile ダイアログで **HTTP Header Insertion** を選択します。

STEP 4 | エントリを **Add**（追加）します。

1. このカテゴリの **Name**（名前）を指定します。
2. **Type (タイプ)** として **Custom(カスタム)** を選択します。
3. ドメインを **Domains**（ドメイン）リストに **Add**（追加）します。

   最大 50 個のドメインを追加することができ、各ドメイン名には最大 256 文字まで使用でき、ワイルドカードがサポートされています（例：「*.example.com」）。

   HTTP ヘッダー挿入は、このリスト内のドメインが *HTTP* 要求の *Host* ヘッダーのドメインと一致すると発生します。
4. ヘッダーを **Headers**（ヘッダー）リストに **Add**（追加）します。

   最大 5 つのヘッダーを追加でき、各ヘッダーには最大 100 文字を含めることができますが、スペースを含めることはできません。
5. ヘッダーごとに、**Value** を入力します。

   各ヘッダー値は、最大 16KB 文字にすることができます。
6. (Optional) **Log** ヘッダーの挿入アクティビティ。
7. **OK** をクリックして変更内容を保存します。

STEP 5 | **Add** または Security policy 規則 (**Policies** > **Security**) を編集すると、ユーザーはこのヘッダー挿入規則を構成する SaaS アプリケーションにアクセスできます。

1. 手順 2 で編集または作成した URL Filtering プロファイル (**Actions** > **URL Filtering**) を選択します。
2. **OK** をクリックして保存して、変更を **Commit**（コミット）します。

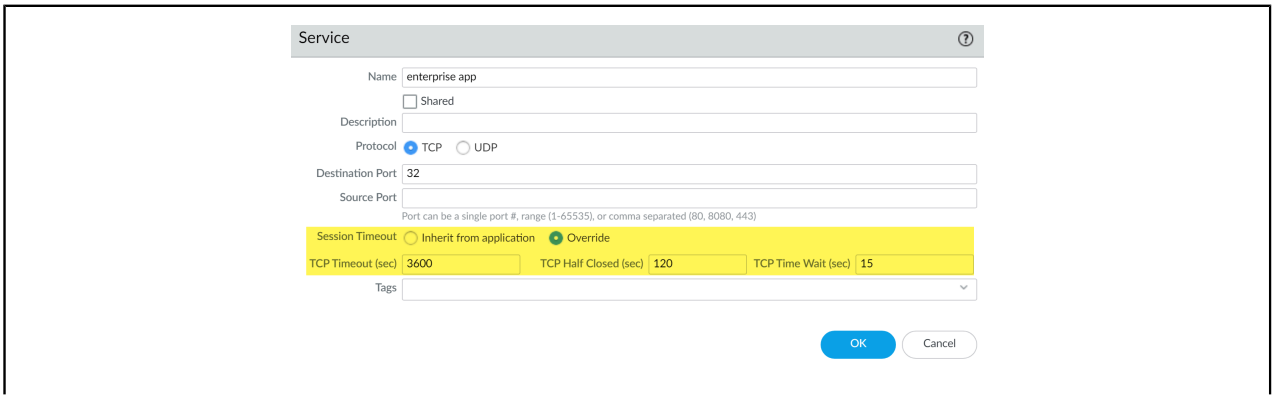
STEP 6 | SaaS アプリケーションへのアクセスが想定通りに機能していることを確認してください。ネットワークに接続されているエンドポイントから以下の作業を行います：

1. アクセス可能なアカウントまたはコンテンツへのアクセスを試行する。SaaS アカウントまたはコンテンツにアクセスできない場合は、設定が機能していません。
2. ブロックされると想定される、アカウントまたはコンテンツへのアクセスを試行します。SaaS アカウントまたはコンテンツにアクセスできる場合は、設定が機能していません。
3. 前の手順の両方が想定通りに機能する場合は、ログを表示できます（ステップ 4.6 でログを設定した場合）。記録された HTTP ヘッダー挿入アクティビティが表示されます。

データセンター アプリケーションのカスタム タイムアウトを維持する

ポートベースのポリシーからアプリケーションベースのポリシーに移行するときに、アプリケーションのカスタムタイムアウトを簡単に維持できます。このメソッドを使用して、App-ID をオーバーライドしたり (アプリケーションの可視性を失う)、カスタム App-ID を作成したり (時間と調査を費やす) 代わりに、カスタム タイムアウトを維持します。

開始するには、サービス・オブジェクトの一部としてカスタム・タイムアウト設定を構成します。



次に、ポリシー・ルールにサービス・オブジェクトを追加して、ルールが強制するアプリケーションにカスタム・タイムアウトを適用します。

次の手順では、カスタム・タイムアウトをアプリケーションに適用する方法について説明します。カスタム・タイムアウトをユーザー・グループに適用するには、同じ手順に従いますが、サービス・オブジェクトを、タイムアウトを適用するユーザー。

STEP 1 | **Objects**（オブジェクト） > **Services**（サービス）を選択して、サービス オブジェクトを追加するか変更します。

セキュリティポリシールールの一致基準を定義する時に、サービス オブジェクトを作成することもできます。**Policies**（ポリシー） > **Security**（セキュリティ） > **Service/URL Category**（サービス/URLカテゴリ）を選択して、該当のルールが強制するアプリケーションのトラフィックに適用されるように新しいサービス オブジェクトを **Add**（追加）します。

STEP 2 | 使用するサービスのプロトコル（TCP または UDP）を選択します。

STEP 3 | サービスで使用する宛先ポート番号またはポート番号の範囲を入力します。

STEP 4 | 以下のサービスに対するセッション タイムアウトを定義します。

- **Inherit from application**（アプリケーションから継承）（デフォルト）– サービス ベースのタイムアウトは適用されず、代わりにアプリケーションのタイムアウトが適用されます。
- **Override**（オーバーライド）–サービスに対するカスタム セッション タイムアウトを定義します。

STEP 5 | アプリケーションのタイムアウトを無効にしてカスタム セッションのタイムアウトを定義することを選択した場合は、次に進みます：

- **TCP Timeout**（**TCP** タイムアウト）値を入力して、データの送信が開始された後に TCP セッションを開いたままにできる最大時間を秒単位で設定します。これが期限切れになるとセッションが閉じます。値の範囲は 1 ～ 604800 であり、デフォルト値は 3600 秒です。
- **TCP Half Closed**（**TCP**半閉鎖） 値を入力して、最初の FIN パケットを受信してから、2 つ目の FIN パケットまたは RST パケットを受信するまで、セッションがセッション テーブル内に保持される最大時間（秒）を設定します。タイマーが期限切れになるとセッションが閉じます。値の範囲は 1 ～ 604800 であり、デフォルト値は 120 秒です。
- **TCP Wait Time**（**TCP** 待機時間） 値を入力して、2 つ目の FIN パケットまたは RST パケット受信後にセッションがセッション テーブル内に保持される最大時間（秒）を設定します。タイマーが期限切れになるとセッションが閉じます。値の範囲は 1 ～ 600 であり、デフォルト値は15秒です。

STEP 6 | **OK** をクリックしてサービス オブジェクトを保存します。

STEP 7 | **Policies**（ポリシー） > **Security**（セキュリティ）を選択して、ポリシー ルールを **Add**（追加） また変更して制御するアプリケーションのトラフィックを強制します。

STEP 8 | **Service/URL Category**（サービス/**URL**カテゴリ）を選択して、作成したばかりのサービス オブジェクトをセキュリティ ポリシー ルールに **Add**（追加）します。

STEP 9 | **OK** をクリックし、変更を **Commit (**コミット**)** します。

Device-ID

Device-ID の概要

2020 Unit 42 IoT Threat Report によると、平均的な企業におけるネットワーク接続デバイスの 30% が IoT です。これは、悪意のあるユーザーに悪用される可能性が多く、常にリスクが高まっている分野です。また、これらのデバイスを特定したら、古いオペレーティン グソフトウェアなどの脆弱性の問題からデバイスをどのように保護すれば良いのでしょうか？ファイアウォールでDevice-ID™を使用すると、ネットワーク上のイベントのデバイスコンテキストを取得し、それらのデバイスに対する推奨ポリシールールを取得し、デバイスに基づいてポリシールールを記述し、推奨に基づいてセキュリティポリシーを適用することができます。

User-ID がユーザー ベースのポリシーを提供し、App-ID がアプリケーション ベースのポリシーを提供する方法と同様に、Device-ID は、IPアドレスや場所の変更に関係なく、デバイスに基づくポリシー ルールを提供します。Device-ID を使用すると、デバイスにトレーサビリティを提供し、ネットワーク イベントを特定のデバイスに関連付けることにより、イベントがデバイスにどのように関連するかについてのコンテキストを取得し、時間の経過とともに変化する可能性のあるユーザー、ロケーション、または IPアドレスではなくデバイスに関連付けられたポリシーを書き込むことができます。Device-IDは、セキュリティ、復号化、サービス品質（QoS）、および認証の各ポリシーで使用することができます。

Device-ID 機能を firewall で使用できるようにするには、IoT Security サブスクリプションを購入し、IoT Security onboarding process 中に firewall を選択する必要があります。IoT Security サブスクリプションには、次の 2 種類があります。

- IoT セキュリティ サブスクリプション
- IoTセキュリティ - データレイク（DRDL）のサブスクリプションは必要としません。

最初のサブスクリプションでは、firewalls はデータ ログをログ サービスに送信し、ログ サービスは分析のために IoT Security に、ストレージ用に Cortex Data Lake インスタンスにストリーミングします。データレイクインスタンスは、新規または既存のインスタンスにすることができます。2 番目のサブスクリプションでは、firewalls はデータ ログをログ サービスに送信し、ログ サービスは分析のために IoT Security にストリーミングしますが、ストレージ用の Cortex Data Lake インスタンスにはストリーミングしません。IoT Security サブスクリプションと IoT Security (DRDL) サブスクリプションの両方が、IoT Security と Device-ID に関して同じ機能を提供することに注意することが重要です。

IoT Security への接続を許可するには、firewall にデバイス ライセンスが必要です。また、ログ サービスへの接続を許可するには、ログ サービス ライセンスが必要です。また、firewall では、IoT Security およびログ サービスに接続するときに、device certificate が自身を認証する必要があります。

ファイアウォールでPAN-OS 9.1.xを介して PAN-OS バージョン8.1.0を使用する場合、IoT セキュリティ ライセンスは、デバイスの分類、動作解析、および脅威解析を提供します。PAN-OS 10.0以降を使用している場合は、Devide-ID を使用して IPアドレスからデバイスへのマッピングを取得し、ネットワーク イベントのデバイス コンテキストを表示し、IoT セキュリティを使用してこれらのデバイスのポリシー ルールの推奨事項を取得し、レポートと ACC 内の透明性を向上します。

PAN-OS バージョン*10.0*以降を使用する どの*Panorama* またはファイアウォールでも デバイスベースのセキュリティ ポリシーを作成できます。セキュリティ ポリシーを施行するには、デバイスに有効な *IoT* セキュリティ ライセンスが必要です。

デバイスを識別して分類するために、IoT Security アプリは、firewall 上のログ、ネットワーク プロトコル、およびセッションからのメタデータを使用します。これには、デバイス識別子に関係のない個人情報や機密情報またはデータは含まれません。メタデータは、デバイスの予想される動作の基礎も形成します。これにより、そのデバイスに許可するトラフィックとプロトコルを定義するポリシー ルール推奨の基準が確立されます。

ファイアウォールが IoT Security からセキュリティ ポリシー ルールの推奨事項と IP アドレスとデバイスのマッピングをインポートすると、ファイアウォールは、自身を認証するために デバイス証明書 をエッジ サーバーに送信します。エッジ サーバーは、独自の証明書を送信してファイアウォールに対して認証を行います。ファイアウォールは、オンライン証明書状態プロトコル (OCSP) を使用して、TCP ポート 80 で HTTP を使用して次のサイトと照合してサーバーの証明書を検証します。

- ocsp.int-x3.letsencrypt.org
- isrg.trustid.ocscp.identrust.com
- crl.identrust.com

Panorama は、Panorama が IoT セキュリティからポリシー ルールの推奨事項をインポートするときに、エッジ サーバーの証明書を検証するために同じチェックを実行します。

IoT Security は、ネットワークにすでに存在する Palo Alto Networks ファイアウォールを使用してネットワーク内のデバイスを識別および分類した後、新しいデバイスやサード パーティ ソリューションを実装する必要がないため、Device-ID はこのデータを活用して、デバイスをポリシー ルールと照合し、ネットワーク イベントのデバイス コンテキストを提供できます。ファイアウォールまたは Panorama がトラフィック、アプリケーション、ユーザー、デバイス、および脅威に与える可視性を通じて、ネットワーク イベントを個々のデバイスまで即座に追跡し、それらのデバイスを保護するためのセキュリティ ポリシー ルールの推奨事項を取得できます。

PAN-OS 10.0 をサポートし、*Device-ID* と *IoT Security* アプリをサポートするすべての *firewall* プラットフォーム *(VM-50 series*、*VM-200*、*CN series* を除く*)*。

デバイスには、6つのレベルの分類 (「属性」とも呼ばれる) があります:

属性	例
カテゴリ	プリンター
プロファイル	シャーププリンター
Model	`MX-6070N`
OS バージョン	`ThreadX 5`
OS Family OS ファミリー	`ThreadX RTOS`

属性	例
ベンダー	株式会社SHARP

ネットワーク内のデバイスのポリシー ルールの推奨事項を取得するために、ファイアウォールはトラフィックを監視して拡張アプリケーションログ (EAL) を生成します。次に、firewall は EAL をロギング・サービスに転送します。IoT Security アプリは、分析のためにログ サービスからログを受信し、IP アドレスからデバイスへのマッピングを提供し、デバイス用の最新の ポリシー ルールの推奨事項 を生成します。IoT セキュリティアプリケーションを使用して、これらのポリシー ルールの推奨事項を確認し、これらのデバイスのセキュリティ ポリシーを作成できます。IoT セキュリティ アプリケーションでポリシー ルールをアクティベートした後、それらをファイアウォールまたは Panorama にインポートし、セキュリティ ポリシーをコミットします。

firewall は、ネットワーク上の DHCP ブロードキャストおよびユニキャストトラフィックを監視して、ネットワーク設定が動的に割り当てられたデバイスを識別できる必要があります。IoT Security は静的 IP デバイスもサポートしています。ファイアウォールが監視できるトラフィックが多いほど、デバイスに対するポリシー ルールの推奨事項がより正確になり、デバイスに対する IPアドレスからデバイスへのマッピングがより迅速かつ正確になります。デバイスが IP アドレスを取得するために DHCP トラフィックを送信すると、firewall はこのタイプの要求を監視し、ログ サービスに送信する EAL を生成し、IoT Security が分析のためにそれらにアクセスします。

L2 インターフェースのトラフィックを監視するには、そのインターフェースの *VLAN* を設定する必要があります。ファイアウォールがインターフェースを *DHCP* リレーの *L3* インターフェースとして処理できるようにすることで、トラフィックやパフォーマンスに影響を与えることなく *DHCP* ブロードキャスト トラフィックを監視できます。

ファイアウォールは、トラフィックに基づいてデバイスを検出し、それらのデバイスにセキュリティ ポリシーを適用する必要があるため、ファイアウォールは、デバイスからメタデータを収集するセンサーと、デバイスのセキュリティ ポリシーを施行するエンフォーサの両方として機能します。IoT セキュリティ アプリケーションは、DHCP トラフィックを送信するとすぐに新しいデバイスを自動的に検出し、最初の1週間以内にデバイスの95% を識別できます。

各アプリケーションには、ルールとしてファイアウォールまたは Panorama にインポートする個別の推奨事項があります。推奨事項をインポートすると、ファイアウォールまたは Panorama は、推奨事項からデバイスの動作を定義するために、少なくとも2つのオブジェクトを作成します:

- トラフィックが発生したデバイスを識別する送信元デバイスオブジェクト
- トラフィックの許可された宛先を識別する1つ以上の宛先オブジェクト。これは、デバイス、IPアドレス、またはfully qualified domain name (完全修飾ドメイン名 - FQDN)です

デバイスオブジェクトのいずれかが firewall または Panorama に既に存在する場合、firewall または Panorama は新しいデバイスオブジェクトを作成する代わりにデバイスオブジェクトを更新します。これらのデバイス オブジェクトは、Security、認証、復号化、および Quality of Service (QoS) ポリシー規則で使用できます。

さらに、ファイアウォールは、各ルールに 2 つの タグ を割り当てます。

- カテゴリ (ネットワーク デバイス - `TrendNet` など) を含むソース デバイスを識別するデバイス。
- ルールが IoT ポリシー ルールの推奨事項であることを示す 1 つ (`IoTSecurityRecommended`)。

firewall がルールに割り当てるタグは、マッピングが同期しなくなった場合にマッピングを復元する唯一の方法であるため、タグを編集または削除しないでください。

Device-ID の最適なデプロイメントと運用のために、以下のベストプラクティスをお勧めします:

- ネットワークの中央に配置されているファイアウォールに Device-ID を展開します。たとえば、大規模環境の場合は、IPアドレス管理 (IPAM) デバイスの上流にあるファイアウォールに Device-ID をデプロイします。小規模な環境の場合は、DHCP サーバーとして機能しているファイアウォールに Device-ID を展開します。
- 初期のデプロイメント時に、Device-ID がネットワークからメタデータを収集するのを少なくとも14日間許可します。デバイスが毎日アクティブでない場合、識別プロセスに時間がかかる場合があります。
- 最も重要なデバイスから最も重要でないデバイスの順にデバイスベースのポリシーを記述します。優先順位付け方法:
  1. Class (セキュリティで保護されたネットワーク デバイスを優先)
  2. 重要なデバイス (サーバーや MRI マシンなど)
  3. 環境固有のデバイス (火災報知器やバッジ リーダーなど)
  4. 消費者向け IoT デバイス (スマート ウォッチやスマート スピーカーなど)
- 内部ゾーンに対してのみ、ゾーンごとに Device-ID を有効にします。

Device-IDをデプロイする準備

ネットワークを Device-ID デプロイメント用に準備するには、次のデプロイメント前のタスクを完了して、ファイアウォールが拡張アプリケーションログ (EAL) を生成し、Cortex Data Lake に送信して、ポリシー ルール推奨の生成のために IoT セキュリティによる処理と分析を行えるようにします。

STEP 1 | ファイアウォールまたは Panorama のデバイス証明書が未インストールの場合はインストールしてください。

デバイス証明書は、ロギングサービスと IoT Security に接続するときにファイアウォールを認証します。

*Panoramaを使用して複数のファイアウォールを管理する場合、Palo Alto Networksでは、デバイスID展開のすべてのファイアウォールをPAN-OS 10.0以降のバージョンにアップグレードすることを強くお勧めします。**Device** を一致条件として使用するルールを作成し、Panorama が PAN-OS 9.1 以前のバージョンを使用するファイアウォールにルールをプッシュすると、**Device** がサポートされていないため、ポリシー ルールトラフィックの照合に問題が発生する可能性があるため、ファイアウォールは Device の一致条件を省略します。*

STEP 2 | デバイスライセンスとロギングサービスライセンスをファイアウォールにインストールします。

これを行うには、[デバイスライセンス] をクリックし、[ライセンス管理] セクションで [ライセンスサーバーからライセンスキーを取得する] を選択します。これにより、ロギングサービスと IoT Security のライセンスがファイアウォールにインストールされます。

ロギングサービスライセンスは、ファイアウォールがロギングサービスに接続することを許可します。

デバイスライセンスは、ファイアウォールが IoT Security に接続することを許可します。

STEP 3 | (L2 インスタンス専用) ファイアウォールが DHCP ブロードキャスト トラフィックを監視できるように、各 L2 インターフェースの VLAN インターフェースを作成します。

STEP 4 | (オプション) Device-ID および IoT セキュリティの必須のトラフィックを許可するために、サービス ルートを設定します。

デフォルトでは、ファイアウォールは管理インターフェイスを使用します。別のインターフェースを使用するには、以下の手順を完了します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Services (サービス)** を選択して **Service Route Configuration (サービスルート設定)** を選択します。
2. サービスルートを **Customize (カスタマイズ)** します。
3. **IPv4** プロトコルを選択します。

   Device-ID および *IoT* セキュリティは *IPv6* をサポートしません。

4. サービス列の **Data Services (データ　サービス)** を選択します。
5. **Source Interface (送信元インターフェース)** および **Source Address (送信元アドレス)** を選択します。
6. **OK** を 2 回クリックします。

STEP 5 | Device-ID および IoT セキュリティの必須のトラフィックを許可するために、Aoo-ID を使用します。

目的	App-ID
ポリシー ルールの推奨事項を取得し、IoT セキュリティ アプリとファイアウォールまたは Panorama 間のトラフィックを許可します。	**paloalto-iot-security**
すべての EACL とすべてのセッション ログのトラフィックを許可します。	**paloalto-logging-service**
IoT セキュリティの動的更新とデバイス ディクショナリの更新を取得します。	**paloalto-updates**

デバイス *ID* を使用するパロアルトネットワークスの次世代ファイアウォールとインターネットの間にサードパーティのファイアウォールがある場合は、次世代ファイアウォールが *iot.services-edge.paloaltonetworks.com: 443 (アメリカ地域、eu.iot.services-edge)* にある場合は、次世代ファイアウォールが *iot.services-edge*にアクセスできることを確認してください。欧州地域にある場合は*paloaltonetworks.com: 443*、アジア太平洋地域にある場合は*apac.iot.services-edge.paloaltonetworks.com: 443*。

STEP 6 | インターネットとPanoramaおよびPanoramaが管理する次世代ファイアウォールの間にサードパーティのファイアウォールがある場合は、デバイスIDとIoTセキュリティに必要なトラフィックを許可していることを確認してください。

目的	アドレス	TCPポート
(PAN-OS バージョン 10.0.3 以降)IoT セキュリティから IP アドレスとデバイスのマッピングとポリシー ルールの推奨事項を取得するデバイス ID を許可する地域 FQDN を受信します。	**Enforcer.iot.services-edge.paloaltonetworks.com**	443
(PAN-OS バージョン 10.0.0- 10.0.2 以降)IoT セキュリティからポリシー ルールの推奨事項と IP アドレスとデバイスのマッピングを受信することをデバイス ID に許可します。	アメリカ地域 **iot.services-edge.paloaltonetworks.com** 欧州地域 **eu.iot.services-edge.paloaltonetworks.com** アジア太平洋地域 **apac.iot.services-edge.paloaltonetworks.com**	443
（PAN-OS バージョン 10.0.0 以降）次世代ファイアウォールがアップデートサーバからデバイス辞書ファイルをダウンロードできるようにします。	**updates.paloaltonetworks.com:**	443
(PAN-OS バージョン 10.0.0 以降) Panorama にログのクエリをログサービスに送信させます。	アメリカ地域 **iot.services-edge.paloaltonetworks.com** 欧州地域 **eu.iot.services-edge.paloaltonetworks.com** アジア太平洋地域 **apac.iot.services-edge.paloaltonetworks.com**	443

目的	アドレス	TCPポート
(IoT セキュリティサブスクリプション + Cortex データレイク) Cortex データレイクにログを転送します。	Cortexデータレイクに必要なTCPポートとFQDNを参照してください。	

PAN-OS バージョン *10.0.0* ～ *10.0.2* は、デフォルトで南北アメリカリージョンのエッジサービス *FQDN* (`iot.services-edge.paloaltonetworks.com`) に接続します。これらの *PAN-OS* バージョンを実行しているファイアウォールが *EU* リージョン (`eu.iot.services-edge.paloaltonetworks.com`) またはアジア太平洋リージョン (`apac.iot.services-edge.paloaltonetworks.com`) の *FQDN* に接続するには、手動で設定する必要があります。*PAN-OS* バージョン *10.0.3* 以降では、ファイアウォールは *IoT Security* のオンボーディングプロセス中に設定されたリージョンに基づいて、使用する正しい *FQDN* を自動的に検出します。手動で設定する必要はありません。

STEP 7 | インターネットと次世代ファイアウォール（パノラマなし）の間にサードパーティのファイアウォールがある場合は、デバイスIDとIoTセキュリティに必要なトラフィックを許可していることを確認してください。

目的	アドレス	TCPポート
(PAN-OS バージョン 10.0.3 以降)IoT セキュリティから IP アドレスとデバイスのマッピングとポリシー ルールの推奨事項を取得するデバイス ID を許可する地域 FQDN を受信します。	**Enforcer.iot.services-edge.paloaltonetworks.com**	443
(PAN-OS バージョン 10.0.0- 10.0.2 以降)IoT セキュリティからポリシー ルールの推奨事項と IP アドレスとデバイスのマッピングを受信することをデバイス ID に許可します。	アメリカ地域 **iot.services-edge.paloaltonetworks.com** 欧州地域 **eu.iot.services-edge.paloaltonetworks.com** アジア太平洋地域 **apac.iot.services-edge.paloaltonetworks.com**	443
(PAN-OS バージョン 10.0.0 以降) 次世代ファイアウォールがアップ	**updates.paloaltonetworks.com:**	443

目的	アドレス	TCPポート
データサーバからデバイス辞書ファイルをダウンロードできるようにします。		
(IoT セキュリティサブスクリプション + Cortex データレイク) Cortex データレイクにログを転送します。	Cortexデータレイクに必要なTCPポートとFQDNを参照してください。	

STEP 8 | DHCP トラフィックのログを監視および生成するようにファイアウォールを設定してから、IoT セキュリティによる処理と分析のためにログを転送します。

- ファイアウォールが DHCP サーバーとして機能している場合:
  1. 拡張アプリケーションログを有効にします。
  2. Log Forwarding profileログ転送プロファイルを作成して、処理用にログを CDL に転送します。
  3. (PA-3200、PA-5200、PA-5450、またはPA-7000 ではサポートされていません) **DHCP** ブロードキャスト セッション オプションを有効にします (デバイス セットアップ > セッション > **Session** > **Session Settings**セッション設定
  4. セキュリティ ポリシーの ルールを作成して、**dhcp** を **Application (**アプリケーション**)** タイプとして許可します。
- ファイアウォールが DHCP サーバーではない場合、ファイアウォールが、クライアントから受信した DHCP トラフィックの EAL を生成できるように、インターフェースを DHCP リレー エージェント として設定します。
- DHCP サーバーがファイアウォールのインターフェースと同じネットワーク セグメント上にある場合は、DHCP サーバーの前にバーチャル ワイヤ インターフェースを配置して、パフォーマンスへの影響を最小限に抑えながら、ファイアウォールが最初の DHCP 交換ですべてのパケットの EAL を生成するようにします。
  1. 対応するゾーンを含む バーチャル ワイヤ インターフェースを設定して、**Multicast Firewalling (**マルチキャスト ファイアウォール設定**)** オプション (**Network (**ネットワーク**)** > **Virtual Wires (**バーチャル ワイヤ**)** > **Add (**追加**)**) を有効化します。
  2. バーチャル ワイヤ ゾーン間で DHCP サーバーとの間で DHCP トラフィックを許可するようにルールを設定します。ポリシーでは、サーバーが現在監視している既存のすべてのトラフィックを許可し、残りのルールと同じログ転送プロファイルを使用する必要があります。
  3. DHCP サーバーが IP アドレスを新しい要求へのリースとして割り当てる前にアクティブであるかどうかを確認できるようにするには、DHCP サーバーからサブネットの残りの部分への ping を許可するルールを設定します。
  4. トラフィックの一致のログを転送しない DHCP サーバーとの間のその他すべてのトラフィックを許可するルールを設定します。
  5. 1番目のバーチャル ワイヤ インターフェースを使用するように DHCP サーバー ホストを設定し、2番目のバーチャル ワイヤ インターフェースを使用するようにネットワーク

スイッチを設定します。ケーブル接続を最小限に抑えるために、DHCP サーバー ホストをファイアウォールに直接接続する代わりに、スイッチング インフラストラクチャで分離された VLAN を使用できます。

- タップ インターフェースを使用して、ネットワークの現在の設定またはトポロジが原因でファイアウォールが通常は監視しない DHCP トラフィックを可視化する場合は、ベストプラクティスとして次の設定を使用します。
  1. タップ インターフェース と、対応するゾーンを設定します。
  2. 残りのルールと同じログ転送プロファイルを使用する DHCP トラフィックに一致するようにルールを設定します。
  3. ファイアウォールのセッション負荷を最小限に抑えるには、他のすべてのトラフィックをドロップするルールを設定します。
  4. タップ インターフェースをネットワーク スイッチのポート ミラーに接続します。
- ネットワークトラフィックがファイアウォールから認識されないデバイスに関するデータを収集する場合は、カプセル化リモートスイッチドポートアナライザ（ERSPAN）を使用して、ミラーリングされたトラフィックをネットワークスイッチから汎用ルーティングカプセル化（GRE）トンネル経由でファイアウォールに送信します。

STEP 9 | セキュリティポリシールールにログ転送プロファイルを適用します。

IoT Security の定義済みログ転送プロファイルをルールに適用するか、既存のプロファイルを更新するか、新しいプロファイルを作成します。これにより、必要な種類のログがロギングサービスに転送されます。

Device-IDの設定

次のタスクを実行して、IP アドレスからデバイスへのマッピングとポリシー ルールの推奨事項を IoT セキュリティからファイアウォールまたは Panorama にインポートします。

Panorama を使用して複数のファイアウォールを管理する場合、*Palo Alto Networks* はデバイス *ID* 展開のすべてのファイアウォールを *PAN-OS 10.0* またはそれ以降のバージョンにアップグレードすることを強くお勧めします。デバイス　を一致条件として使用するルールを作成し、*Panorama* が *PAN-OS 9.1* 以前のバージョンを使用するファイアウォールにルールをプッシュすると、ファイアウォールはサポートされていないため、デバイス　の一致基準を省略し、ポリシー ルールトラフィックの一致に問題が発生する可能性があります。

STEP 1 | Hub上の IoT セキュリティ ライセンスをアクティベートする

1. 電子メールで受け取った指示に従って、IoT セキュリティ ライセンスをアクティブベートします。
2. ご利用の IoT セキュリティ アプリを初期化します。詳細については、IoTセキュリティを始める および IoTセキュリティのベストプラクティス を参照してください。
3. IoT セキュリティ ポリシーを適用するために使用するファイアウォールにライセンスを適用します。
4. ファイアウォールまたは Panorama でライセンスを更新します。

STEP 2 | IoT セキュリティ アプリで IoT セキュリティ ポリシーを定義します。

1. IoT セキュリティ アプリで、送信元デバイス オブジェクトを選択します。
2. 送信元デバイス オブジェクトの新しいポリシー ルールのセットを**Add (作成)** します。

   IoT セキュリティ アプリでセキュリティ ポリシーを作成する方法の詳細については、「セキュリティ ポリシーの推奨 」を参照してください。
3. 変更内容を確定するには、ポリシー ルールをアクティベートします。

STEP 3 | IP アドレスからデバイスへのマッピングとポリシー ルールの推奨事項をファイアウォールまたは Panorama にインポートします。

1. ポリシー ルールの推奨事項をインポートします。
   - ファイアウォールで、[デバイス > ポリシー推奨 > **IoT**] を選択します。
   - Panoramaの場合は、**Panorama** > ポリシー推奨 > **IoT** を選択し、ポリシー ルールを Panorama が管理する ファイアウォール にプッシュします。

   > ポリシーを ファイアウォール にプッシュした後、ファイアウォール で ポリシールールを同期して、ポリシー ルールの推奨とポリシー ルール のマッピングを作成する必要があります。

   ポリシー推奨を選択すると、ファイアウォールまたは Panorama が IoT セキュリティと通信して、最新のポリシー ルール推奨を取得します。ポリシー ルールの推奨事項は、ファイアウォールまたは Panorama にキャッシュされません。

   > *IoT Security* は、デバイスの信頼できる動作を使用してポリシー ルールの推奨事項を作成するため、ルールのデフォルトのアクションは *[許可]* です。

2. **Source Device Profile (**送信元デバイスのプロファイル**)** を選択します。
3. **Destination Device Profile (**宛先デバイスのプロファイル**)** と許可される **Applications (**アプリケーション**)** が正しいことを確認します。
4. ポリシー ルールにインポートする **Import Policy Rules (**ポリシー ルールのインポート**)** を選択します。
5. (Panorama 専用) ポリシー ルールをインポートするデバイス グループの **Location (**場所**)** を選択します。
6. ポリシー ルールの **Name**（名前）を入力します。
7. (Panorama 専用) **Destination Type (**宛先の種類**)** (**Pre-Rulebase (**プレ ルールベース**)** または **Post-Rulebase (**ポスト ルールベース**)**) を選択します。
8. ルールベースのルールの配置を定義するには、**After Rule (**ルール後**)** を選択します。
   - **No Rule Selection (**ルール選択なし**)**– 該当のルールをルールベースの一番上に配置します。
   - **Default One (**デフォルトの設定**)** – 該当のルールをリスト内のルールの後に配置します。

   > *Security policy (*セキュリティ ポリシー*)* で、*Device-ID* ルールは、デバイスに適用される既存のルールよりも前にある必要があります。

9. ポリシー ルールの推奨事項ごとにこのプロセスを繰り返して、各デバイス オブジェクトが必要な宛先にアクセスできるようにするルールを作成します。
10. **OK** をクリックし、変更を **Commit (**コミット**)** します。

STEP 4 | Device-ID を使用してデバイスを検出し、セキュリティ ポリシーを適用する各ゾーンで、Device-ID を有効にします。

デフォルトでは、Device-ID は、それを有効にしたゾーン内のすべてのサブネットワークをマップします。**Include List**（許可リスト） および **Exclude List**（除外リスト） でどのサブネットワークのデバイス ID をマップするかを変更できます。

ベスト プラクティスとして、送信元ゾーンで *Device-ID* を有効にしてデバイスを検出し、セキュリティ ポリシーを適用します。内部ゾーンに対してのみ *Device-ID* を有効にする必要があります。

1. **[Network]** > **[ゾーン]** の順に選択します。
2. Device-ID を有効にしたいゾーンを選択します。
3. **Enable Device Identification (デバイス ID を有効化する)** を実行してから、**OK** をクリックします。

STEP 5 | 変更をコミットします。

STEP 6 | セキュリティ ポリシー が正しいことを確認します。

1. **Policies (ポリシー)** を選択してから、ポリシー ルールの推奨事項から作成したルールを選択します。

   IoT セキュリティは、ソースデバイスオブジェクトを含む **Description (説明)** と **Tags (タグ)** を割り当てて、送信元デバイス オブジェクトを識別します。このルールはIoT セキュリティからの推奨事項です。

   デバイスのオブジェクト名は一意である必要があります。

2. **Source (送信元)** タブを選択してから、**Source Device Profile (送信元デバイスのプロファイル)** を確認します。
3. **Destination (宛先)** タブを選択して、**Destination Device Profile (宛先デバイスプロファイル)** を確認します。
4. **Application (アプリケーション)** タブを選択し、**Applications (アプリケーション)** を確認します。
5. **Actions (アクション)** タブを選択して、その**Action (アクション)** を確認します (デフォルトは **Allow (許可)**)。
6. Explore（エクスプローラ） を使用して、Cortex Data Lake がログを受信することを確認し、受信したログを確認します。

STEP 7 | IoT セキュリティ ポリシー ルールの推奨事項がないデバイス用にカスタム デバイス オブジェクトを作成します。

たとえば、ポリシー ルールの推奨事項を使用してラップトップやスマートフォンなどの従来の IT デバイスを保護することはできないため、セキュリティ ポリシーで使用するためにはこれらの種類のデバイスのデバイス オブジェクトを手動で作成する必要があります。カスタム デバイスオブジェクトの詳細については、「Device-IDの管理」を参照してください。

STEP 8 | デバイス オブジェクトを使用して、ポリシー ルールを適用し、潜在的な問題を監視および識別します。

次のリストには、デバイス オブジェクトの使用例がいくつか含まれています。

- セキュリティ、認証、QoS、および復号化ポリシー
- 復号化ログを使用して、障害と復号化するのに最も重要なアセットを特定します。
- ACC でデバイス オブジェクトのアクティビティを表示して、新しいデバイスとデバイスの動作を追跡します。
- デバイス オブジェクトを使用してカスタム レポートを作成します (インシデント レポートや監査用など)。

Device-IDの管理

必要に応じて次のタスクを実行し、推奨ポリシールールやデバイスオブジェクトの更新、もしくは推奨ポリシールールのマッピングを復元します。

STEP 1 | **New Updates Available (新規アップデートが利用可能)** 列で、推奨ポリシールール項目に **Yes** が表示された際、推奨ポリシールールを更新します。

デバイスが新機能を追加した場合、IoT Security は推奨ポリシールールを更新し、ファイアウォールまたは Panorama で許可する追加のトラフィックまたはプロトコルをアドバイスします。日次で IoT セキュリティの更新をチェックし、推奨ポリシールールをできるだけ早く更新する様にします。

1. IoT セキュリティ アプリケーションで、ポリシー ルールを **Edit (編集)** し、**Next (次へ)** をクリックします。
2. 新しい推奨事項を選択し、**Next (次へ)** をクリックします。
3. 変更を**Save**（保存）します。
4. ファイアウォールまたは Panorama で、**Import Policy Rules (ポリシー ルールのインポート)** をクリックしてから、**Yes (はい)** をクリックして、現在のルールに上書きすることを確認します。

   このアクションは、ルール自体ではなく、推奨ルールを上書きします。

5. (Panorama のみ) すべてのデバイス グループに対して、前のステップを繰り返し実行します。
6. 変更を **Commit (コミット)** します。

STEP 2 | デバイスディクショナリ内のデバイスオブジェクトについて、レビューや更新、およびメンテナンスを行います。

IoT セキュリティ推奨ポリシールールがないデバイス用に、デバイス オブジェクトを作成する必要があります。たとえば、ノートパソコンやスマートフォンなどの従来の*IT*デバイスは*IoT*セキュリティ推奨ポリシールールを使用して保護することが出来ないため、これらの種類のデバイスに対するデバイス オブジェクトを作成し、それらをセキュリティ ポリシーに適用して保護する必要があります。

1. オブジェクト > デバイス を選択します。
2. デバイス オブジェクトを **Add** (追加) します。
3. リストを **Browse** (参照) するか、キーボードを使用して **Search** (検索) します。

   検索結果には、複数タイプのデバイスオブジェクト属性を含めることができます (たとえば、**Category** (カテゴリ) と **Profile** (プロファイル) の両方）。
4. カスタム デバイス オブジェクトを追加するには、デバイス オブジェクトの **Name** (名前) を入力し、オプションで **Description** (説明) を入力します。

   デバイス オブジェクトごとに常に一意の名前を使用してください。推奨ポリシールールにあるデバイスオブジェクトの説明タグを変更しないでください。
5. (Panorama のみ) **Shared** (共有) オプションを選択し、このデバイスオブジェクトを他のデバイスグループで使用できるようにします。
6. デバイスオブジェクトの属性を選択します (**Category** (カテゴリ)、**OS** 、**Profile** (プロファイル)、**Osfamily**、**Model** (モデル)、および**Vendor** (ベンダー))。
7. **OK** をクリックして変更を確定します。

STEP 3 | 場合によっては (以前の設定を復元した場合等)、ポリシー ルール recommendation-to-policy ルール マッピングが同期しなくなる可能性があります。ポリシールールを Panorama から Panorama が管理するファイアウォールにプッシュした後、各ファイアウォールのマッピングも同期する必要があります。マッピングを同期する方法:

- ファイアウォールで、[デバイス > ポリシー推奨 > **IoT** > 同期ポリシールール を選択します。
- Panorama の場合は、**Panorama** > ポリシー推奨事項 > **IoT** > 同期ポリシールール を選択します。

ファイアウォールまたは Panorama は、ルールベース内のすべてのルールをスキャンし、ルールを IoT セキュリティ推奨ポリシールールとして識別するタグを確認し、送信元デバイスオブジェクト情報を取得して、ローカル ポリシールール推奨事項データベースを再入力が行われます。

STEP 4 | 不要になった推奨ポリシールールを削除します。

推奨ポリシールールが適用されなくなった場合は、推奨ポリシールールを削除できます。また、更新されたセキュリティポリシーを適用する場合も、推奨ポリシールールを削除する必要があります。

1. IoT セキュリティアプリケーションで、**Delete (削除)** を選択します。
2. **Mark as Removed (削除済みとしてマーク)** をクリックし、この推奨項目を削除対象に選択します。
3. マッピングを削除します。
   - ファイアウォールで、[デバイス > ポリシーの推奨事項 > **IoT** > ポリシー マッピング を選択します。
   - Panorama の場合<は、ポリシー推奨 > **IoT** > ポリシー マッピング を選択し、マッピングを削除する **Location** を選択します。
4. **Yes**（はい）をクリックして、マッピングの削除を確定します。
5. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。Panorama の場合は、**Policies (ポリシー)** > **Security (セキュリティ)** > **Pre-Rules/Post-Rules (プレ ルール/ポスト ルール)**を選択します。
6. 削除したい推奨ポリシールールを選択してから、**Delete (削除)** を選択します。
7. 変更を **Commit (コミット)** します。

STEP 5 | CLI コマンドを使用して、ファイアウォールと IoT セキュリティ間の問題をトラブルシューティングします。

Device-IDのCLIコマンド

以下のCLIコマンドを使用して、ファイアウォールとIoTセキュリティの間の問題のトラブルシューティングに関する情報を表示します。一般に、 **eal** を包含するCLIコマンドは送信データのカウンターを表示し、 **icd** を包含するCLIコマンドは受信データのカウンターを表示します。

例	コマンド
ファイアウォールとCortex Data Lake間の接続数やログ量などの、Enhanced Application Logging(高度なアプリケーションロギング;EAL)カウンターを表示します。	**show iot eal all**
ファイアウォールとCortex Data Lake間の接続に関する詳細を表示します。	**show iot eal conn**
PAN-OSのバージョンやシリアルナンバーなど、プレーン(データプレーンまたはmanagement plane(管理プレーン - MP))ごとのEALカウンターの概要を表示します。	**show iot eal dpi-eal**
プレーン(データプレーンまたは(データプレーンまたはmanagement plane(管理プレーン - MP))およびプロトコルごとにEALカウンターを表示します。	**show iot eal dpi-stats all**
EALカウンタをプロトコルごとに閲覧します。	**show iot eal dpi-stats subtype dhcp|http**
host information profile(ホスト情報プロファイル - HIP)一致レポートカウンターの概要を表示します。	**show iot eal hipreport-eal**
EALログ応答時間カウンターを表示します。	**show iot eal response-time**
ファイアウォールとIoTセキュリティアプリケーション間のエッジサービスへの接続の状態の詳細と、IPアドレスからデバイスへのマッピングおよびポリシー ルールの推奨事項のカウンターを表示します。	**show iot icd statistics all**
エッジサービスへの接続用のカウンターを表示します。	**show iot icd statistics conn**

例	コマンド
IPアドレス-デバイス間マッピングのカウンターを表示します。	**show iot icd statistics verdict**
ファイアウォールのすべての IPアドレス-デバイス間マッピングを表示します。	**show iot ip-device-mapping-mp all**
特定の IPアドレスの IP アドレス- デバイス間マッピングを表示します。	**show iot ip-device-mapping-mp ip *IP-address***
データ プレーン上の IP アドレスとデバイス マッピングのリストを表示します。	**show iot ip-device-mapping all**
management plane (管理プレーン - MP) の IPアドレス- デバイス間 マッピングを消去します。	**debug iot clear-all type device**
データ プレーン上の IP アドレスからデバイスへのマッピングをクリアします。	**clear user-cache all**

Threat Prevention（脅威阻止）

Palo Alto Networks®の次世代ファイアウォール脅威侵入防御サブスクリプションは、多面的な検出メカニズムを使用して、脅威のランドスケープの全範囲に対抗するために、コモディティの脅威や高度な永続的な脅威(APT)からネットワークを保護し、防御します。脅威防御ソリューションは、次の 3 つのサブスクリプションで構成されています。

- Threat Prevention:コア Threat Prevention サブスクリプションは、さまざまな Palo Alto Networks サービスから収集された悪意のあるトラフィック データから生成されたシグネチャに基づいています。これらのシグネチャは、コマンド アンド コントロール (C2)、さまざまな種類の既知のマルウェア、脆弱性の悪用など、特定の脅威に基づいてセキュリティ ポリシーを適用するために ファイアウォール によって使用されます。また、ファイアウォール の App-ID およびユーザー ID 識別テクノロジと組み合わせることで、コンテキスト データを相互参照して、きめ細かいポリシーを生成できます。脅威軽減ポリシーの一環として、既知または危険なファイルの種類と IP アドレスを特定してブロックすることもできます。これらのファイルの種類と IP アドレスは、防弾サービス プロバイダーや既知の悪意のある IP を指定するリストなど、事前に作成されたいくつかのカテゴリを使用できます。特殊なツールやソフトウェアを使用する場合は、独自の脆弱性シグネチャを作成して、侵入防御機能をネットワーク固有の要件に合わせてカスタマイズできます。
- Advanced Threat Prevention—高度な脅威防御 クラウド サービスは、インラインのディープラーニングと機械学習モデルを使用して、回避的でこれまでに見たことのない未知の C2 脅威をリアルタイムで実施します。超低レイテンシのネイティブクラウドサービスとして、この拡張可能で無限にスケーラブルなソリューションは、モデルトレーニングの改善により常に最新の状態に保たれます。Advanced Threat Prevention（高度な脅威防御） ライセンスには、Threat Prevention（脅威防御） に含まれるすべての利点が含まれています。
- DNS セキュリティ — 高度な DNS ベースの脅威から組織を保護するために設計された DNS Security クラウド サービス。DNS Securityは、高度な機械学習と予測分析をさまざまな脅威インテリジェンスソースに適用することで、強化されたDNSシグネチャセットを生成し、DNSリクエストのリアルタイム分析を提供して、新しく生成された悪意のあるドメインからネットワークを保護します。DNS Securityは、DNSトンネリング、DNS再バインド攻撃、自動生成を使用して作成されたドメイン、マルウェアホストなど、さまざまなC2脅威を検出できます。DNS Security は、完全な DNS 脅威カバレッジのために、Advanced Threat Prevention（高度な脅威防御） または Threat Prevention （脅威防御）サブスクリプションを必要とし、連携します。

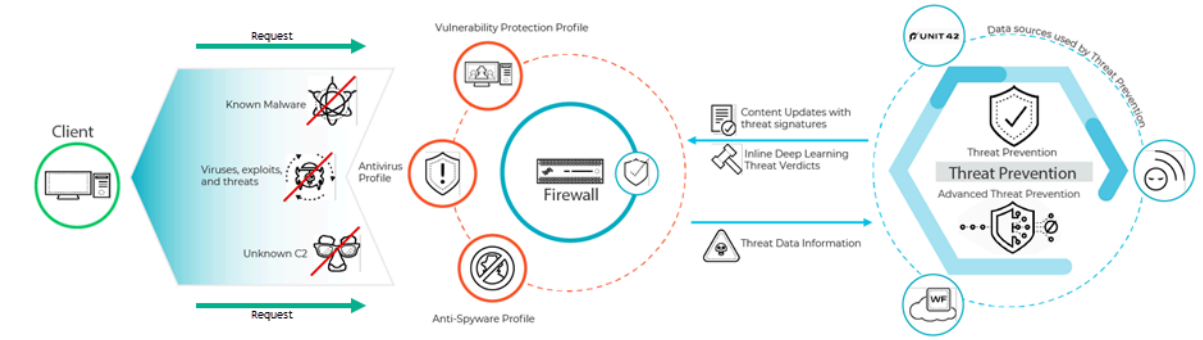
Palo Alto Networksの侵入防御サブスクリプションは連携して、攻撃プロセスのさまざまな段階でチェーンを傍受して切断し、ネットワークインフラストラクチャのセキュリティ侵害を防ぐための可視性を提供する包括的なソリューションを提供します。

- 脅威防御について
- 高度な脅威防御
- ネットワークをレイヤー 4 およびレイヤー 7 回避から保護するためのベスト プラクティス
- アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップ
- DNS セキュリティ

- DNS クエリを使用してネットワーク上の感染ホストを特定する
- データ フィルタリングのセットアップ
- 事前定義済みのデータ フィルタリング パターン
- データ フィルタリング プロファイルの作成
- インラインクラウド解析の設定
- WildFire インライン ML
- ファイル ブロッキングのセットアップ
- ブルート フォース攻撃の防御
- ブルート フォース シグネチャのアクションとトリガー条件のカスタマイズ
- 回避シグネチャの有効化
- Monitor Blocked IP Addresses（ブロックされた IP アドレスのモニター）
- 脅威シグネチャのカテゴリ
- 脅威例外の作成
- カスタム シグネチャ
- 脅威の詳細を把握して評価を実施
- 脅威インテリジェンスを Palo Alto Networks と共有
- 脅威防御リソース

脅威防御について

脅威防御は侵入防御システム (IPS) ソリューションで、ファイアウォール とクラウドで動作するコンポーネントを備えた多層防御システムを使用して、すべてのポートとプロトコルでマルウェア、脆弱性の悪用、およびコマンド アンド コントロール (C2) を検出してブロックできます。脅威防御クラウドは、Palo Alto Networksサービスからの脅威データを組み合わせて多数の検出サービスを実行し、それぞれが特定の識別可能なパターンを持つシグネチャを作成し、ファイアウォールによって、一致する脅威と悪意のある動作が検出されたときにセキュリティポリシーを適用するために使用されます。これらのシグネチャは、脅威の種類に基づいて分類され、一意の識別子番号が割り当てられます。これらのシグネチャに対応する脅威を検出するために、firewall は、異常な特性を示すネットワーク トラフィックを検査および分類する分析エンジンを操作します。シグネチャベースの検出メカニズムに加えて、Advanced Threat Prevention（高度な脅威防御）は、未知の回避的なC2脅威を防止するための補完的なインライン検出システムを提供します。Advanced Threat Prevention（高度な脅威防御） クラウドは、拡張可能なディープラーニングモデルを運用し、要求ごとにファイアウォールのインライン分析機能を有効にして、ゼロデイ脅威がネットワークに侵入するのを防ぎます。



ファイアウォール で使用される脅威シグネチャは、ウイルス対策、スパイウェア対策、脆弱性の 3 種類に大別され、対応するセキュリティプロファイルによってユーザー定義のポリシーを適用するために使用されます。

Palo Alto Networks がクラウド提供するセキュリティサービスは、それぞれのサービスに対して*WildFire*および*DNS C2*シグネチャと、脅威シグネチャの代わりにファイルタイプを指定できるファイル形式シグネチャも生成します。たとえば、署名の例外などです。

- ウイルス対策シグネチャは、ワーム、トロイの木馬、スパイウェアのダウンロードなど、さまざまな種類のマルウェアやウイルスを検出します。
- スパイウェア対策シグネチャは、侵害されたホスト上の C2 スパイウェアが、オートコールまたはビーコンを外部 C2 サーバーに送信しようとすることを検出します。
- 脆弱性シグネチャは、エクスプロイトシステムの脆弱性を検出します。

シグネチャには、デフォルトの重大度レベルと、関連するデフォルト・アクションがあります。たとえば、非常に悪意のある脅威の場合、[両方をリセット] の設定になります。この設定は、Palo Alto Networks のセキュリティに関する推奨事項に基づいています。

特殊な内部アプリケーションが存在する展開や、オープンソースの Snort ルールと suricata ルールが使用されているサードパーティのインテリジェンスフィードでは、専用の保護のために カスタムシグネチャ を作成できます。

Firewallsは、毎日のウイルス対策コンテンツと毎週のアプリケーションおよび脅威コンテンツの更新の2つのアップデートパッケージの形でシグネチャアップデートを受け取ります。ウイルス対策コンテンツの更新には、ウイルス対策およびスパイウェア対策のセキュリティ プロファイルで使用されるウイルス対策シグネチャと DNS (C2) シグネチャがそれぞれ含まれ、アプリケーションと脅威のコンテンツの更新には、脆弱性およびスパイウェア対策のセキュリティ プロファイルで使用される脆弱性シグネチャとスパイウェア対策シグネチャが含まれます。更新プログラム パッケージには、他のサービスやサブ機能によって活用される追加コンテンツも含まれています。詳細については、Dynamic Content Updates を参照してください。

高度な脅威防御

Advanced Threat Prevention （高度な脅威防御）は、既存の Threat Prevention（脅威防御） ライセンスと連携して動作する クラウドで提供されるセキュリティ サービスで、高度で回避的なコマンド アンド コントロール (C2) の脅威に対する保護を提供します。これにより、インライン検出器を使用したリアルタイムのトラフィック検査を使用して、未知の脅威を防ぐことができます。Advanced Threat Prevention（高度な脅威防御） クラウド のこれらのディープラーニング、ML ベースの検出エンジンは、高度な C2 およびスパイウェアの脅威のトラフィックを分析し、ゼロデイ脅威からユーザーを保護します。クラウドベースの検出エンジンを操作することで、ユーザーがアップデートパッケージをダウンロードしたり、リソースを消費する可能性のあるプロセス集約型の firewall-based アナライザーを操作したりすることなく、自動的に更新および展開される幅広い検出メカニズムにアクセスできます。クラウドベースの検出エンジン ロジックは、WildFireの C2 トラフィック データセットを使用して継続的に監視および更新され、Palo Alto Networks の脅威研究者による追加のサポートにより、高度に高速化された検出機能強化のための人間の介入を提供します。Advanced Threat Prevention（高度な脅威防御） ディープラーニングエンジンは、HTTP、HTTP2、SSL、不明 UDP、および未知の TCP アプリケーション上の C2 ベースの脅威の分析をサポートします。追加の解析モデルはコンテンツの更新によって提供されますが、既存のモデルに対する拡張機能はクラウド側の更新として実行され、ファイアウォールの更新は必要ありません。Advanced Threat Prevention（高度な脅威防御） は、セキュリティ プロファイル配下のアンチスパイウェアにある インライン クラウド 分析 で有効化および設定されます。

ネットワークをレイヤー 4 およびレイヤー 7 回避から保護するためのベスト プラクティス

以下に、ほとんどのレイヤー 4 攻撃およびレイヤー 7 攻撃をモニタリングし、ネットワークを保護するための推奨事項を示します。

- 最新の PAN-OS ソフトウェア バージョンおよびコンテンツ リリース バージョンにアップグレードして、最新のセキュリティ更新を使用してください。コンテンツとソフトウェア更新のインストールを参照してください。
- 悪意のある DNS 要求をシンクホールするDNS セキュリティの有効化 (Threat Prevention および DNS Security サブスクリプション ライセンスが必要)。Palo Alto Networks では、ご利用のアンチスパイウェア プロファイル内で、以下の DNS セキュリティ カテゴリ設定を使用するようお勧めします:

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
: Palo Alto Networks Content			
default-paloalto-dns		sinkhole	extended-capture
: DNS Security			
Command and Control Domains	default (high)	sinkhole	extended-capture
Dynamic DNS Hosted Domains	default (informational)	sinkhole	disable
Grayware Domains	default (low)	sinkhole	disable
Malware Domains	default (medium)	sinkhole	disable
Parked Domains	default (informational)	sinkhole	disable
Phishing Domains	default (low)	sinkhole	disable
Proxy Avoidance and Anonymizers	default (low)	sinkhole	disable
Newly Registered Domains	default (informational)	sinkhole	disable

  - ログの重大度設定の場合は、デフォルト設定を使用します。
  - ポリシーのアクションについては、すべてのシグネチャ送信元を **sinkhole (シンクホール)** に設定します。
  - packet capture (パケット キャプチャ - pcap) については、Command and Control Domains (コマンド アンド コントロール ドメイン) を **extended-capture (拡張キャプチャ)** に設定します。その他のすべてのカテゴリはデフォルト設定のままにします。

  関連するアンチスパイウェアの設定詳細については、インターネット ゲートウェイのアンチスパイウェア プロファイルのベストプラクティスを参照してください。
- アクティブな Advanced Threat Prevention サブスクリプションがある場合は、インライン クラウド分析 を有効にして、高度な C2 の脅威をリアルタイムでブロックします。各分析エンジンの既定のアクションは **alert** で、対応する脅威が検出されると脅威ログを生成しますが、Palo Alto Networks では、すべての分析モデル アクションを **Reset-Both** に設定することをお勧めします。これにより、一致するパケットがドロップされ、RST がクライアントとサーバーに送信し、接続が切断され、脅威ログエントリが生成されます。

- ファイアウォールがDNSプロキシとして振る舞うように設定し、回避シグネチャを有効にします。

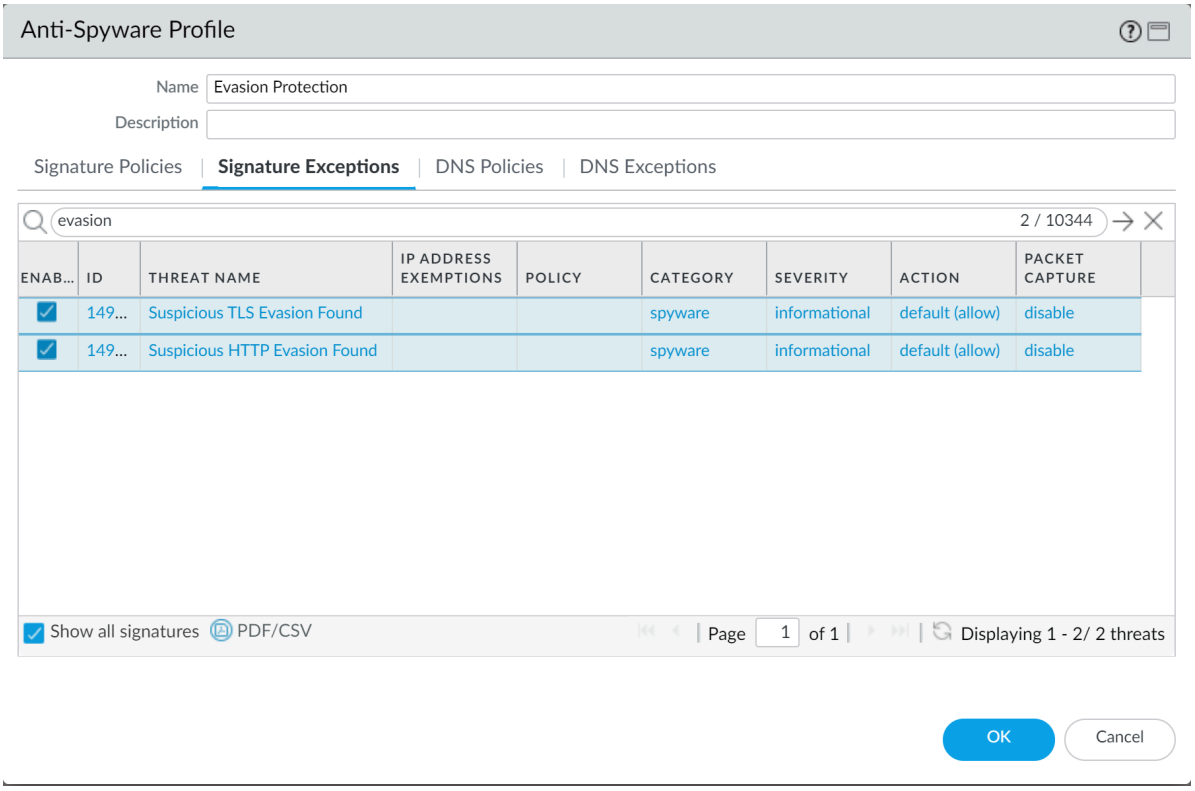
  DNS プロキシはファイアウォール セキュリティ ポリシー エンジンの一部ではありません。代わりに、ドメインから *IP* へのマッピングを管理しながら、 *DNS* ホスト名を解決するようファイアウォールに指示します。この指示は、*TLS/HTTP* 回避を防ぐのに不可欠です。

  - DNS プロキシ オブジェクトの設定を行います。

    DNS プロキシとして振る舞う際、ファイアウォールは DNS リクエストを解決し、今後の DNS クエリを効率よく迅速に解決するためにホスト名から IP アドレスへのマッピングをキャッシュします。
  - 回避シグネチャの有効化

    偽装された HTTP あるいは TLS リクエストを検知する回避シグネチャは、元の DNS リクエストで指定されているもの以外のドメインにクライアントが接続する際にアラートを送信できます。回避シグネチャを有効化する前に必ず DNS プロキシを設定するようにしてください。DNS プロキシがなくても、DNS 負荷分散構成における DNS サーバーが同じ DNS リクエストへの応答としてファイアウォールおよびクライアントに異なる IP アドレ

ス（同じリソースをホストするサーバーについて）を返す際にアラートをトリガーできます。

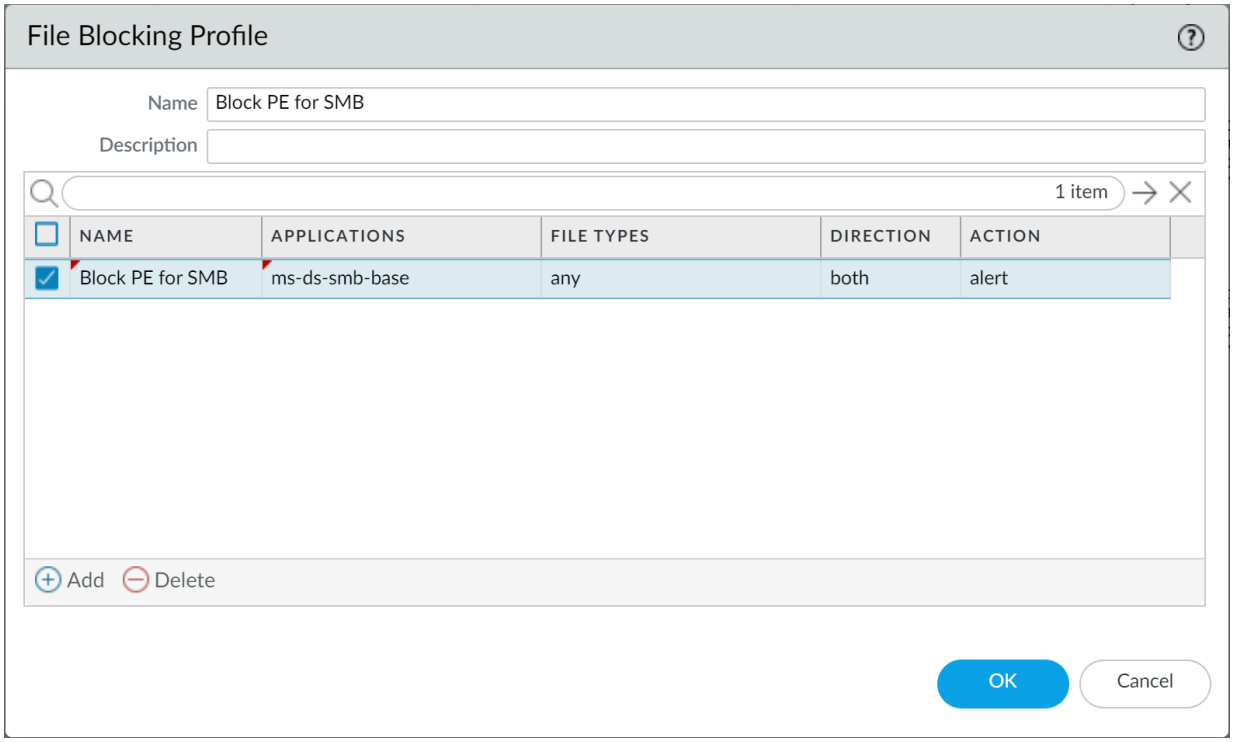


- Prisma Access を運用している展開、または内部 DNS サーバーのないネットワークの場合は、既定のシンクホール FQDN (sinkhole.paloaltonetworks.com) の代わりに Palo Alto Networks シンクホール IP アドレス (72.5.65.111) を使用するように DNS ポリシーを構成します。

  Anti-Spyware Profile によって使用される DNS シンクホールを使用すると、firewall は、指定されたシンクホール サーバーに対してシンクホール アクション用に構成されたカテゴリに一致するドメインの DNS クエリに対する応答を偽造し、侵害されたホストの識別を支援します。デフォルトのシンクホール FQDN が使用される場合、firewall は、内部 DNS サーバーが CNAME レコードを解決することを期待して、CNAME レコードを応答としてクライアントに送信し、クライアントから構成済みのシンクホール・サーバーへの悪意のある通信をログに記録し、容易に識別できるようにします。ただし、クライアントが Prisma Access を使用している場合、内部 DNS サーバーのないネットワークにいる場合、または CNAME を A レコード応答に適切に解決できない他のソフトウェアやツールを使用している場合、DNS 要求はドロップされ、脅威分析に不可欠な不完全なトラフィック ログの詳細が生成されます。
- サーバーについては、各サーバーで制限が加えられたアプリケーションのみを許可するセキュリティポリシー ルールを作成します。アプリケーションの標準的なポートがサーバー

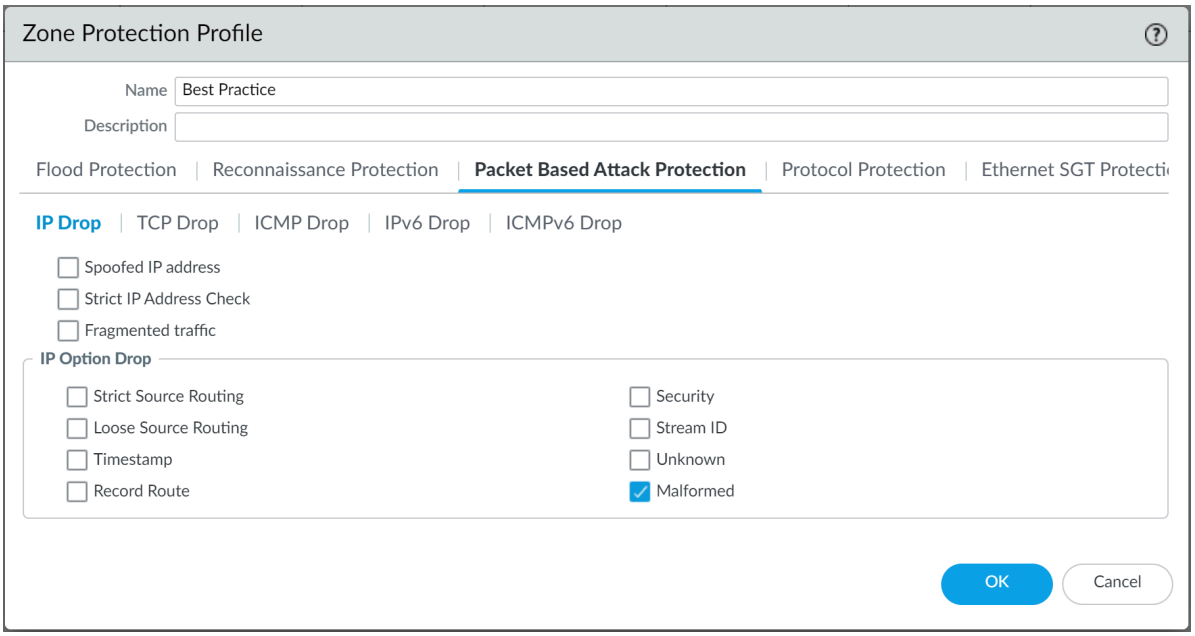
のリッスン ポートにマッチしていることを確認してください。例えば、SMTPトラフィックだけがメール サーバーへのアクセスを許可されるように、Application (アプリケーション) を **smtp** に設定し、Service (サービス) を **application-default** に設定します。サーバーが標準的なポートのサブネットだけを使用する場合（例えば、SMTP アプリケーションが 25 および 587 と定義された標準的なポートを持っていながら SMTP サーバーがポート 587 のみを使用する場合）、ポート 587 のみを含んだ新しいカスタム サービスを作成し、application-default の代わりにその新しいサービスをセキュリティ ポリシー ルールで使用してください。さらに、特定の送信元および宛先ゾーンや IP アドレス群にアクセスを制限するようにしてください。

- セキュリティ ポリシーを使用してすべての不明なアプリケーションおよびトラフィックをブロックします。通常、不明なトラフィックに分類されるのは、ネットワーク上の内部アプリケーションまたはカスタム アプリケーションおよび潜在的な脅威です。不明なトラフィックは、変則的で異常な非準拠のアプリケーションまたはプロトコルであるか、または非標準ポートを使用する既知のアプリケーションの可能性があり、どちらの場合でもブロックする必要があります。「カスタム アプリケーションや不明なアプリケーションの管理」を参照してください。
- ファイル ブロッキングのセットアップを行い、インターネットベースの SMB （Server Message Block）トラフィックの Portable Executable （PE）ファイル タイプが Trust ゾーンから Untrust ゾーンに通過するのをブロックします（ms-ds-smb アプリケーション）。



- PE (ポータブル実行可能ファイル)、ELF および MS Office ファイル、PowerShell およびシェル スクリプトの悪意のある亜種をリアルタイムでブロックする。WildFire インライン MLを有効にすると、firewallで機械学習を使用してファイルを動的に分析できます。このアンチウィルス保護の追加レイヤーは、WildFire ベースのシグネチャを補完し、シグネチャがまだ存在しないファイルのカバー範囲を拡大します。

- パケットベースの攻撃を防御するように設定されたゾーン プロテクション プロファイルを作成します（**Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **Zone Protection (ゾーン プロテクション)**）。
  - **Malformed (不正な形式の)** IPパケットをドロップするオプションを選択します（**Packet Based Attack Protection (パケット ベースの攻撃防御)** > **IP Drop (IPドロップ)**）。



  - **Mismatched overlapping TCP segment (重複する TCP セグメントの不一致)** をドロップするオプションを有効化します（**Packet Based Attack Protection (パケット ベースの攻撃防御)** > **TCP Drop (TCP ドロップ)**）。

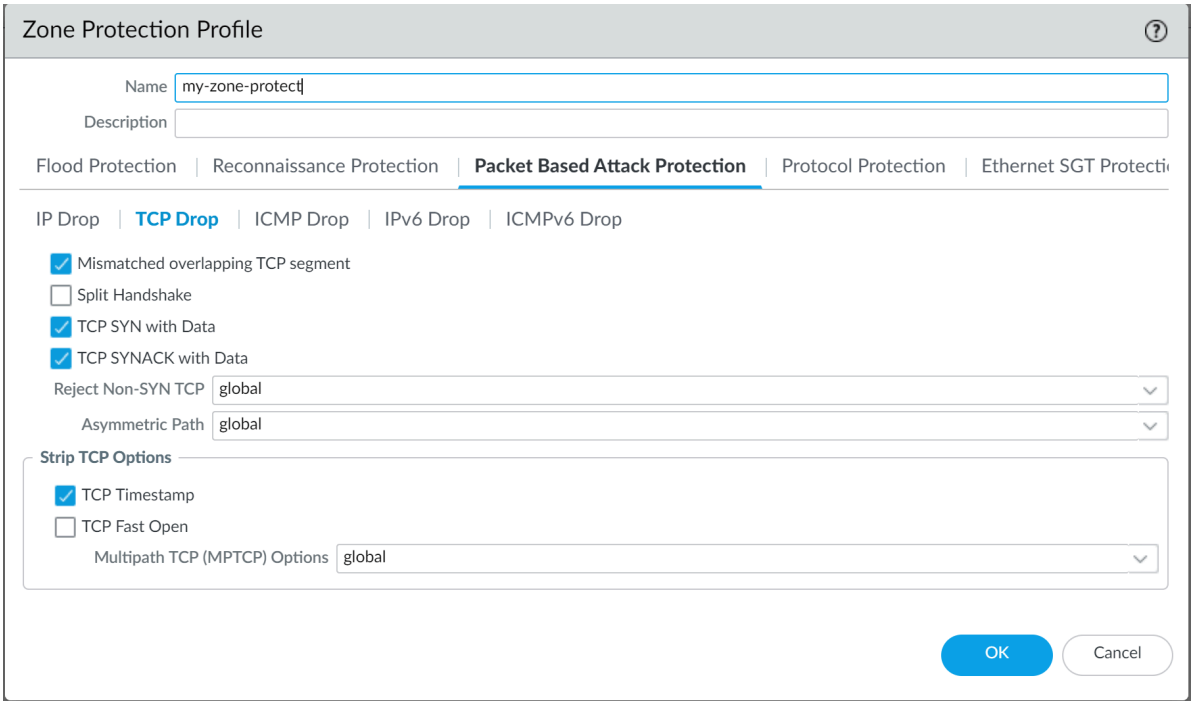
    重複するけれども異なるデータを故意に使用して接続を構築することにより、攻撃者は接続の意図を誤解させ、誤検出を故意に発生させようとすることができます。また、攻撃者は IP スプーフィングとシーケンス番号予測を利用してユーザーの接続をインターセプトし、接続を介して攻撃者のデータを挿入します。**Mismatched overlapping TCP segment (重複する TCP セグメントの不一致)** オプションを選択すると、不一致かつ重複したデータを持つフレームを PAN-OS に破棄させることができます。受信したセグメントは、別のセグメントに含まれている場合、別のセグメントの一部とオーバーラップしている場合、あるいは別のセグメントの全体を含んでいる場合に破棄されます。
  - **TCP SYN with Data (データを伴う TCP SYN)** および **TCP SYNACK with Data (データを伴う TCP SYNACK)** をドロップするオプションを有効化します（**Packet Based Attack Protection (パケット ベースの攻撃防御)** > **TCP Drop (TCP ドロップ)**）。

    3 方向ハンドシェイクの際にペイロードにデータを含む SYN および SYN-ACK パケットをドロップすることで、ペイロードに含まれるマルウェアをブロックし、TCP ハンドシェイ

クが完了する前に不正なデータの抽出を回避できるようになり、セキュリティが向上します。

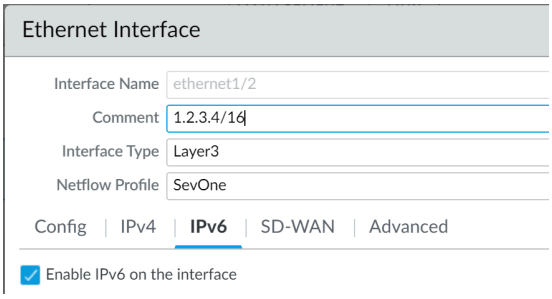
- ファイアウォールがパケットを転送する前に SYN パケットから TCP タイムスタンプを除去します（**Packet Based Attack Protection (**パケット ベースの攻撃防御**)** > **TCP Drop (TCP** ドロップ**)**）。

  SYN パケットの **Strip TCP Options - TCP Timestamp (TCP** ストリップのオプション**—TCP** タイムスタンプ**)** オプションを有効化すると、TCP 接続の両端の TCP スタックで TCP タイムスタンプがサポートされなくなります。これにより、同じシーケンス番号について複数のパケット上で異なるタイムスタンプを使用する攻撃を回避できます。

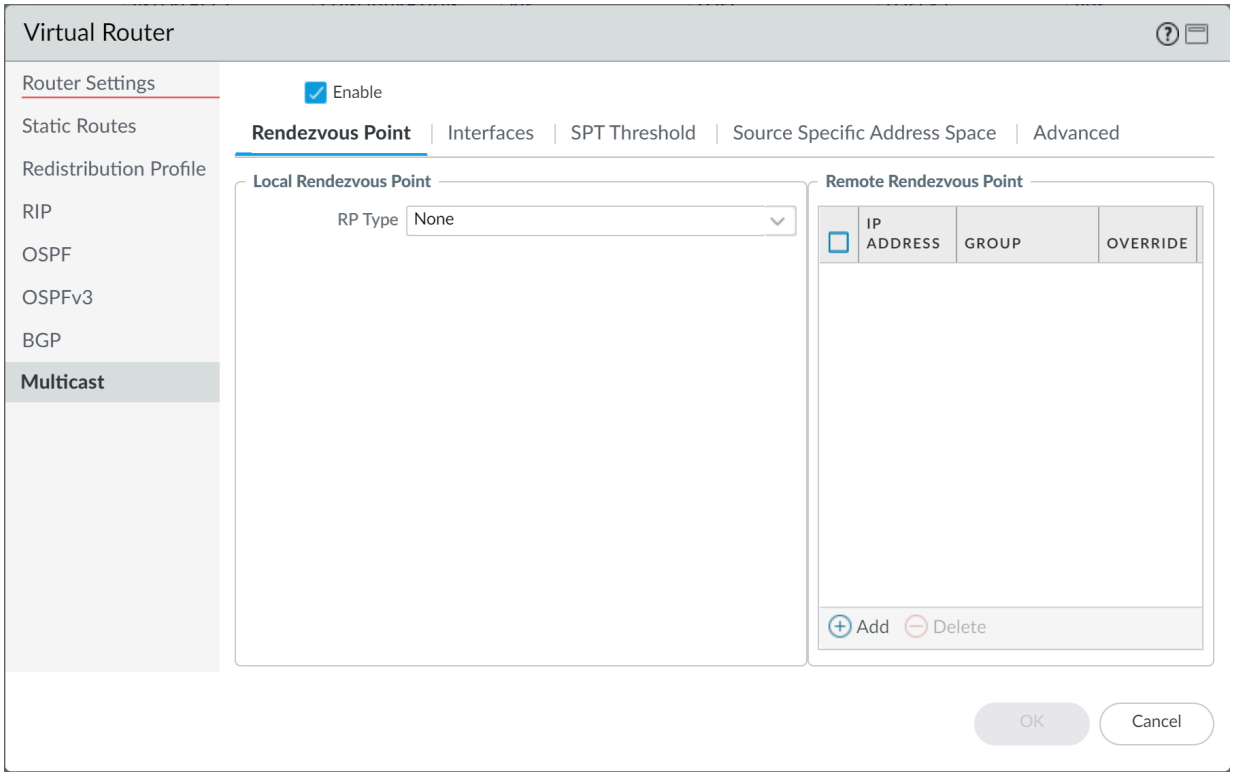


- ネットワークホスト上で IPv6 アドレスを設定する場合、IPv6 のサポートをまだ有効にしていないのであれば、必ず有効にしてください（**Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット) > IPv6**）。

  IPv6 のサポートを有効化することで、IPv6 ホストへのアクセスを許可し、さらに IPv4 パケットにカプセル化された IPv4 パケットをフィルタリングし、IPv6 over IPv4 のマルチキャスト アドレスがネットワークの偵察行為に悪用されるのを防ぐことができます。



- マルチキャスト トラフィックのサポートを有効にして、ファイアウォールがマルチキャスト トラフィックにポリシーを適用できるようにします（**Network (ネットワーク)** > **Virtual Router (仮想ルーター)** > **Multicast (マルチキャスト)**）。



- **Forward datagrams exceeding UDP content inspection queue (UDP** コンテンツ検査キューを超過するデータグラムを転送**)** および **Forward segments exceeding TCP content inspection queue (TCP** コンテンツ検査キューを超過するセグメントを転送**)** を無効化します (**Device (**デバイス**)** > **Setup (**セットアップ**)** > **Content-ID** > **Content-ID Settings (Content-ID** 設定)。

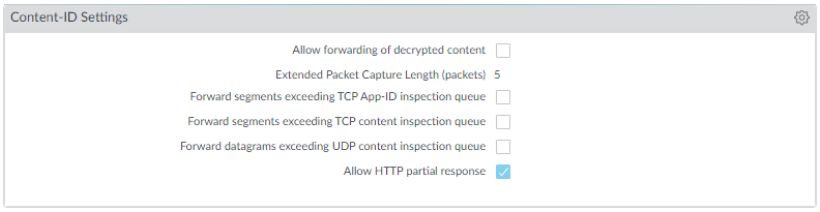
  デフォルト設定では、TCP または UDP コンテンツ検査キューが一杯になると、ファイアウォールはキュー制限 64 を超過した UDP データグラムあるいは TCP セグメントに対するコンテンツ検査をスキップします。このオプションを無効にすると、ファイアウォールが許可するすべての TCP および UDP データグラムに対して必ずコンテンツ検査が行われるようになります。例えば、ユースケースに合わせてファイアウォール プラットフォームが適切にサイジングされていないなどの特定の状況下でのみ、この設定を無効化するとパフォーマンスが影響を受ける場合があります。

- **Allow HTTP partial response (HTTP** 部分レスポンスの許可**)** を無効化します（**Device (**デバイス**)** > **Setup (**セットアップ**)** > **Content-ID** > **Content-ID Settings (Content-ID** 設定**)**）。

  HTTP 部分レスポンス オプションにより、クライアントはファイルの一部のみを取得することができるようになります。転送の途中経路にある次世代ファイアウォールが悪意のあるファイルの検知と破棄を行った場合、RSTパケットにてTCPセッションを強制終了します。ウェブ ブラウザが HTTP ヘッダー レンジ オプションを実装している場合、新しいセッションを開始してファイルの残りの部分だけを取得することで、最初のセッションのコンテクストが欠如しているためにファイアウォールが同一のシグネチャを再びトリガーするのを防ぐと同時に、ウェブ ブラウザがファイルを再構築して悪意のあるコンテンツを配信することができます。このオプションを無効にすると、これが発生しなくなります。

  HTTP部分応答の許可は、デフォルトでfirewallで有効になっています。これにより、最大限の可用性が提供されますが、サイバー攻撃が成功するリスクが高まります。最大限のセキュリティを確保するため、このオプションを無効にして、ファイアウォールが悪意のある活動によって元のセッションを終了させた後、Webブラウザがファイルの残りを取得するために新しいセッションを開始するのを防止します。HTTP 部分応答を無効にすると、RANGE ヘッダーを使用する HTTP-based データ転送に影響し、特定のアプリケーションでサービス異常が発生する可能性があります。HTTP 部分応答を無効にした後、ビジネス クリティカルなアプリケーションの動作を検証します。

  ビジネスクリティカルなアプリケーションでHTTPデータ転送の中断が発生した場合は、その特定のアプリケーションに対してApplication Overrideポリシーを作成できます。Application Override は App-ID (脅威とコンテンツの検査を含む) をバイパスするため、特定のビジネスクリティカルなアプリケーションに対してのみ Application Override ポリシーを作成し、ソースと宛先を指定してルールを制限します (最小特権アクセスの原則)。必要な場合を除き、Application Override ポリシーを作成しないでください。Application Override ポリシーの詳細については、「https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVLCA0 を参照してください。



- 重大度が「低」および「高」の脆弱性および異例のプロトコルをすべてブロックする脆弱性防御プロファイルを作成します。

  プロトコルの挙動が通常の適切な用途から外れたとき、プロトコルの異常が発生します。例えば、不正な形式のパケット、プログラムが不適切なアプリケーション、標準的でないポート上で実行されているアプリケーションはすべて、異常なプロトコルとみなされ、回避ツールとして使用される可能性があります。

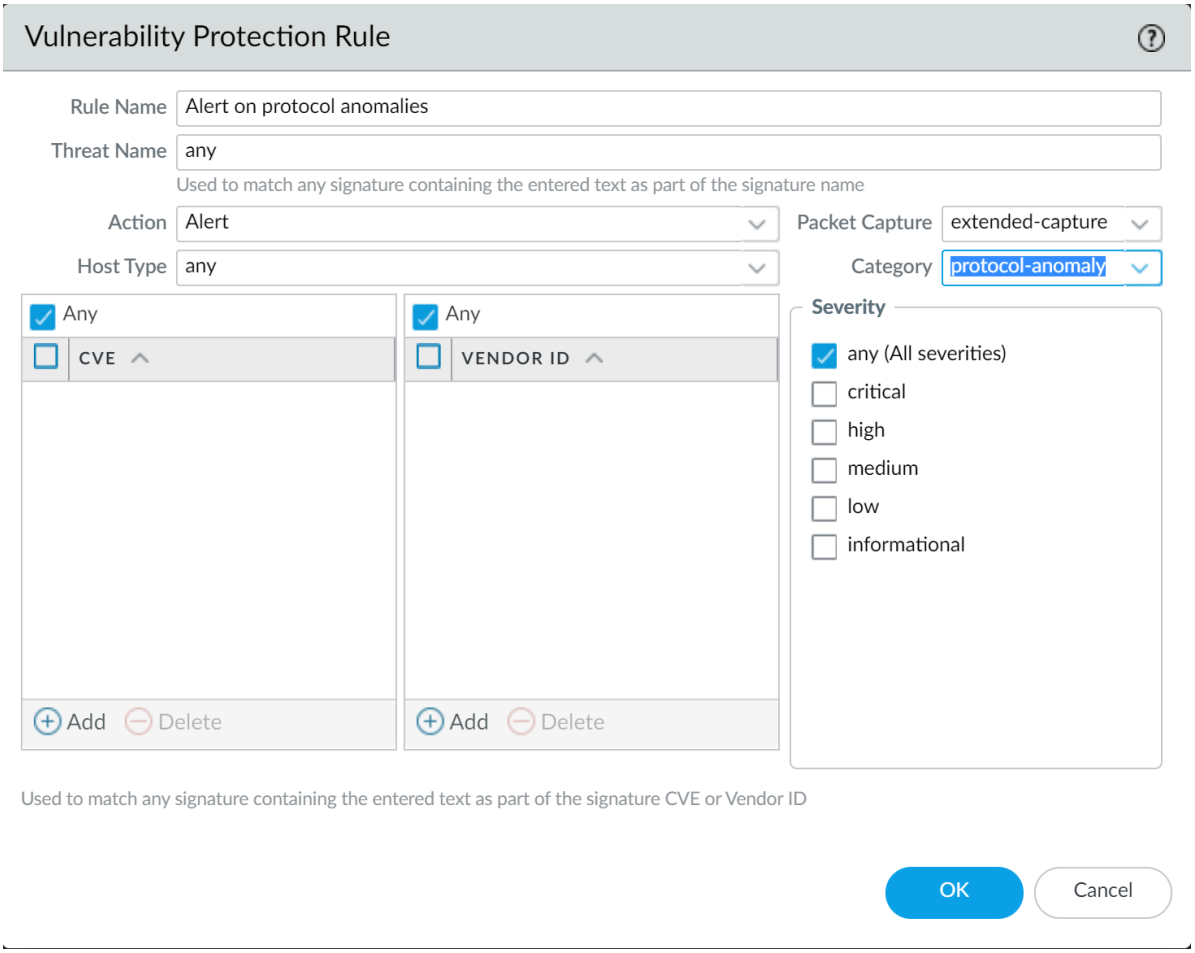
  ビジネスにおいてアプリケーションの可用性を最優先するミッション クリティカルなネットワークの場合、一定期間、特異なプロトコルに対するアラートを通知することから始め、重要な内部アプリケーションが標準的でない方法で確立されたプロトコルを決して使用しないようにします。特定の重要なアプリケーションが特異なプロトコルのシグネチャをトリガーすることが判明した場合、それらのアプリケーションを異例のプロトコルの適用から除外することができます。これを行うには、特異なプロトコルを許可する別のルールを脆弱性防御プロファイルに追加し、そのプロファイルを、重要なアプリケーションを出入りするトラフィックを実行するセキュリティ ポリシー ルールに付与します。

  重要な内部アプリケーションについて特異なプロトコルを許可する、脆弱性防御プロファイル ルール、およびセキュリティ ポリシー ルールが、上記、特異なプロトコルをブロックするルールにリストされていることを確認します。トラフィックはセキュリティポリシールールおよび関連する脆弱性保護プロファイル ルールに対して上から順に評価され、最初にマッチしたルールが適用されます。

  - 異例のプロトコルについてアラートを通知することから始めます。

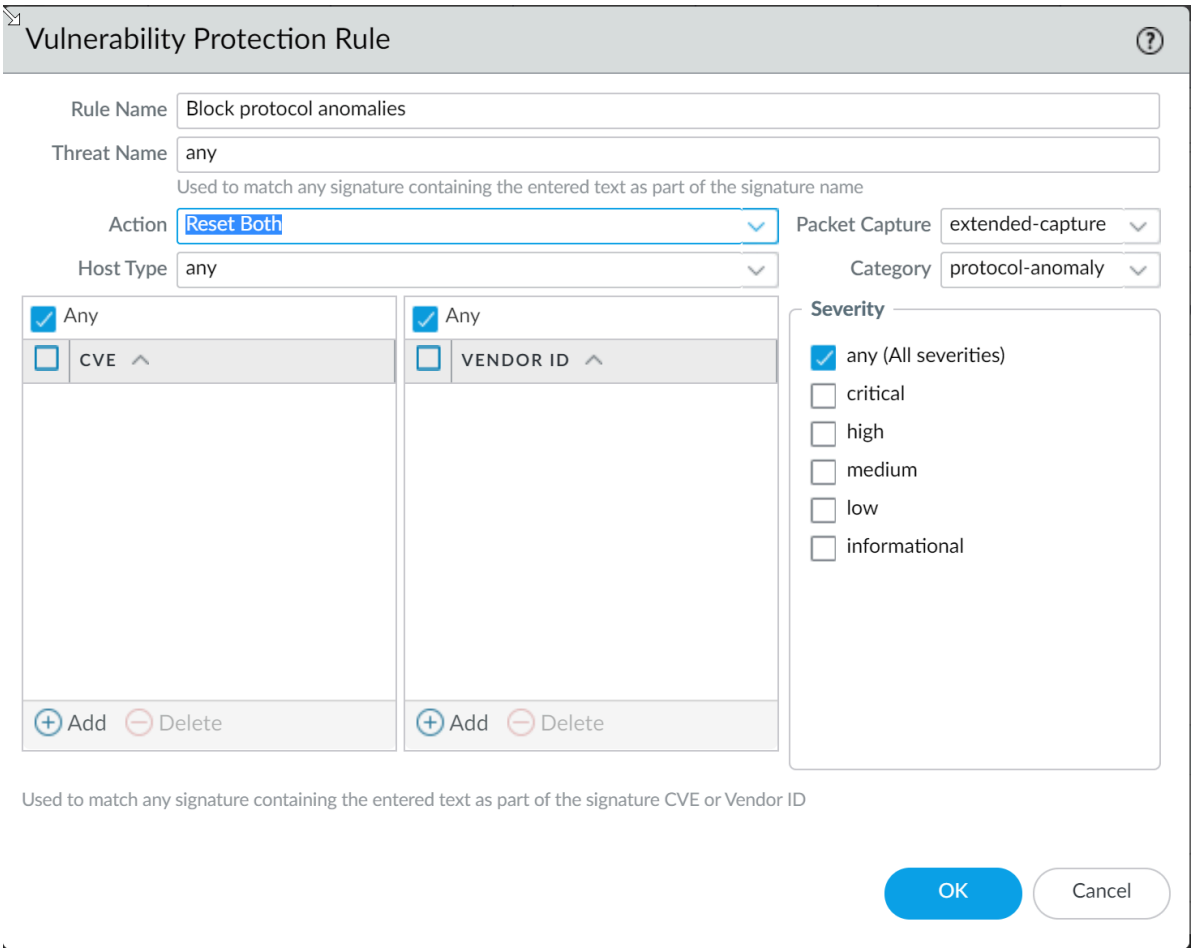
    Vulnerability Protection Profile (脆弱性保護プロファイル) ルールを作成し、**Action (アクション)** を Alert (アラート)に、**Category (カテゴリ)** を protocol-anomaly に、**Severity (重大度)** を Any (すべて) に設定します。トラフィックを監視し、標準的でない方法で確立されたプロトコルを使用している重要な内部アプリケーションがあるかどうか判断します。そうであることが分かった場合、該当するアプリケーションで特異なプロトコルの許可を

continue (続行) してから、その他すべてのアプリケーションについて、特異なプロトコルをブロックします。



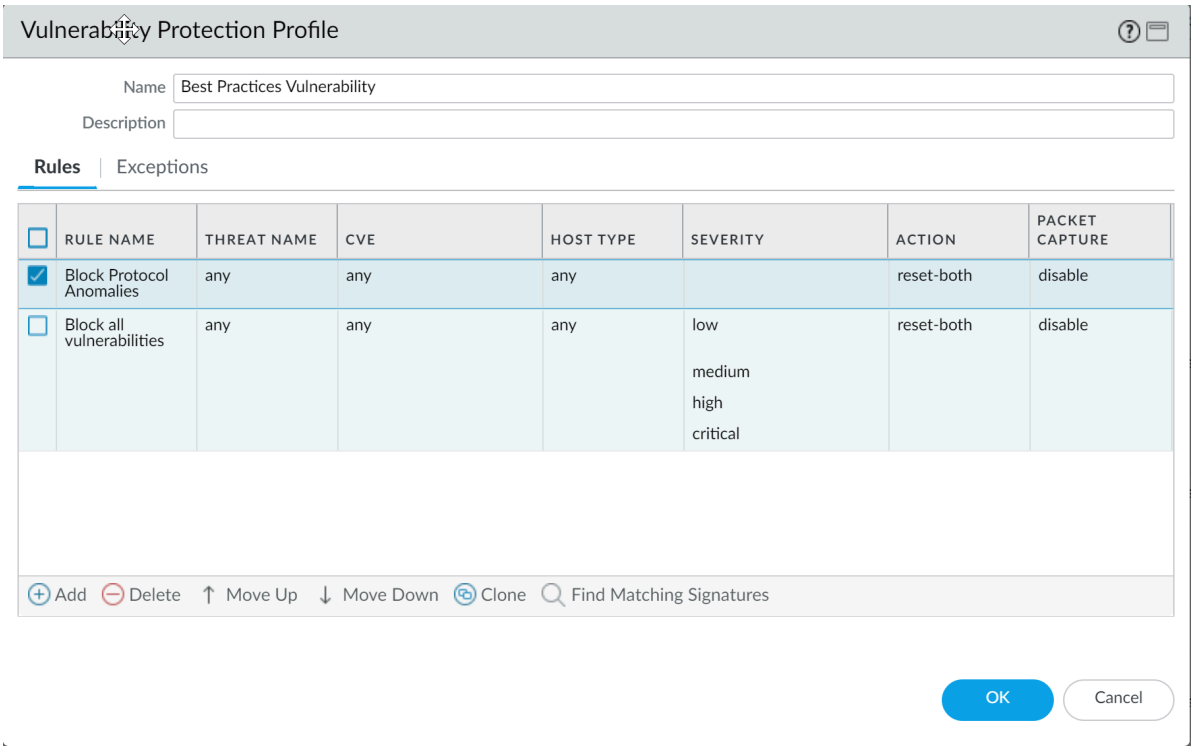
- 特異なプロトコルをブロックします。

  Vulnerability Protection Profile (脆弱性保護プロファイル) ルールを作成し、**Category (カテゴリ)** を protocol-anomaly に、**Action (アクション)** を Reset Both (どちらもリセット) に、**Severity (重大度)** を Any (すべて) に設定します。



- 必要に応じて、非標準的な方法で確立されたプロトコルを使用する重要なアプリケーションについて、特異なプロトコルを許可します。そうするには、特異なプロトコルを許可する Vulnerability Protection Profile (脆弱性保護プロファイル) ルールを作成します（**Action (アクション)** を Allow (許可) に、**Category (カテゴリ)** を protocol-anomaly に、**Severity (重大度)** を any (すべて) に設定）。重要なアプリケーションを出入りするトラフィックに適用されるセキュリティポリシー ルールに脆弱性保護プロファイル ルールを付与します。

- 重大度が「low」以上の脆弱性をすべてブロックする脆弱性防御プロファイルに別のルールを追加します。このルールは、特異なプロトコルをブロックするルールの後にリストアップする必要があります。



- 作業を続行し、以下のセキュリティ プロファイルをセキュリティ ポリシールールに関連付けて、シグネチャベースの防御を提供します：
  - 重大度が「low」以上のスパイウェアをすべてブロックするアンチスパイウェア プロファイル。
  - アンチウイルス シグネチャに一致するコンテンツをすべてブロックするアンチウイルス プロファイル。

アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップ

すべての Palo Alto Networks の次世代ファイアウォールには、セキュリティ ポリシーに適用できる事前定義されたアンチウイルス、アンチスパイウェア、および脆弱性防御プロファイルが付属します。事前定義されたアンチウイルス プロファイルは 1 つで、**default** と呼ばれ、プロトコルごとにデフォルトのアクション（HTTP、FTP、および SMB トラフィックのブロック、および SMTP、IMAP、POP3 トラフィックでアラート生成）を使用します。アンチスパイウェアおよび脆弱性保護用の事前定義されたプロファイルは以下の 2 つです。

- **default** – デフォルトのアクションがクライアントおよびサーバーのすべてのスパイウェア/脆弱性防御イベント（重大度 critical、high、および medium）に適用されます。low および informational イベントは検出しません。
- **strict** – ブロック応答がクライアントおよびサーバーのすべてのスパイウェア/脆弱性防御イベント（重大度 critical、high、medium）に適用され、low および informational イベントではデフォルトのアクションを使用します。

ネットワークに流れ込むトラフィックに脅威が含まれることのないようにするため、事前定義されたプロファイルを基本 Web アクセス ポリシーに関連付けます。ネットワーク上のトラフィックをモニターしてポリシー ルールベースを拡張し、その後、特定のセキュリティ ニーズに対応する詳細なプロファイルを設計できます。

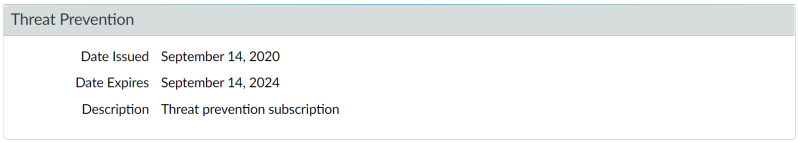
次の流れに従ってデフォルトのアンチウイルス、アンチスパイウェア、および脆弱性保護セキュリティ プロファイルをセットアップします。

Palo Alto Networks は、すべてのアンチスパイウェアおよび脆弱性保護シグネチャに対するデフォルトのアクションを定義しています。デフォルトのアクションを表示するには、***Objects* (オブジェクト) > *Security Profiles* (セキュリティ プロファイル) > *Anti-Spyware* (アンチスパイウェア)** あるいは ***Objects* (オブジェクト) > *Security Profiles* (セキュリティ プロファイル) > *Vulnerability Protection* (脆弱性保護)** を選択してから、プロファイルを選択します。*Exceptions* (例外) タブをクリックし、*Show all signatures* (すべてのシグネチャを表示) をクリックしてシグネチャのリストおよび対応するデフォルトの ***Action* (アクション)** を表示します。デフォルト アクションを変更するには、新しいプロファイルを作成し、***Action* (アクション)** を指定し、かつ/または個々のシグネチャ例外をプロファイルの ***Exceptions* (例外)** に追加します。

STEP 1 | 脅威防止サブスクリプションがあることを確認します。

脅威防止サブスクリプションでは、1 つのライセンスに、アンチウイルス、アンチスパイウェア、および脆弱性防御の全機能をバンドルしています。アクティブな脅威防止サブスクリプションを持っていることを確認するには、**Device** (デバイス) > **Licenses** (ライセンス) を

選択し、**Threat Prevention (**脅威防止**)** の有効期限が未来の日付になっていることをチェックします。



STEP 2 | 最新のコンテンツをダウンロードします。

1. **Device (**デバイス**)** > **Dynamic Updates (**動的更新**)** の順に選択し、ページの下部にある **Check Now (**今すぐチェック**)** をクリックして最新のシグネチャを取得します。
2. **Actions** （アクション） 列で **Download (**ダウンロード**)** をクリックして最新のアンチウイルス アップデートをインストールしてから、最新のアプリケーションおよび脅威更新を **Install (**インストール**)** します。

STEP 3 | コンテンツ更新のスケジュールを設定します。

更新プログラムの展開に関する重要な情報については、アプリケーションと脅威コンテンツ更新のベストプラクティスを参照してください。

1. **Device (**デバイス**)** > **Dynamic Updates (**動的更新**)** を選択して **Schedule (**スケジュール**)** をクリックし、**Antivirus (**アンチウイルス**)** および **Applications and Threats (**アプリケーションおよび脅威**)** のシグネチャ更新を自動的に取得します。
2. 更新の頻度およびタイミングを指定します。
   - **download-only**—ファイアウォールは、定義したスケジュールに従って最新の更新を自動的にダウンロードしますが、**Install (**インストール**)** は手動で行う必要があります。
   - **download-and-install**—ファイアウォールは、定義したスケジュールに従って更新コンテンツを自動的にダウンロードしてインストールします。
3. **OK** をクリックしてスケジュール更新を保存します。コミットは不要です。
4. （任意）更新コンテンツを利用できるようになってからファイアウォールがダウンロードを行うまでの最低時間を示す **Threshold (**しきい値**)** を定義します。例えば、**Threshold (**しきい値**)** を **10** に設定すると、スケジュールに関係なく、更新コンテンツを利用できるようになってから少なくとも 10 時間経過するまでの間、ファイアウォールが更新コンテンツをダウンロードしなくなります。
5. （HA のみ）ダウンロードおよびインストール後にピアがコンテンツ更新を同期できるようにする稼働かを、**Sync To Peer (**ピアと同期**)** で決定します（更新スケジュールはピア間で同期されません。両方のピアに対して手動でスケジュールを設定する必要があります）。

   次のように、**Sync To Peer (**ピアと同期**)** を行うかどうか、またその方法を判断するために HA デプロイメント環境に応じて考慮すべき事項が他にもあります。

   - アクティブ/パッシブ**HA**—ファイアウォールがコンテンツ更新のために MGT ポートを使用している場合、両方のファイアウォールが独立して更新コンテンツをダウンロードおよびインストールするようスケジュールを設定します。しかし、ファイアウォールがコンテンツ更新用にデータポートを使用している場合は、パッシブ ファ

イアウォールがアクティブになるまでの間、ファイアウォールは更新コンテンツのダウンロードもインストールも行いません。更新のためにデータポートを使用する際、両方のファイアウォールがスケジュールを同期した状態を保つためには、両方のファイアウォールで更新のスケジュール設定を行った後、**Sync To Peer (**ピアと同期**)** を有効化し、どちらかアクティブな方のファイアウォールが更新コンテンツをダウンロードおよびインストールしたら、それをパッシブ ファイアウォールにもプッシュさせるようにします。

- アクティブ/アクティブ**HA**—ファイアウォールがコンテンツ更新用に MGT インターフェイスを使用している場合は、両方のファイアウォールで **download-and-install** を選択しますが、**Sync To Peer (**ピアと同期**)** は有効化しません。ただし、ファイアウォールがデータポートを使用している場合は、両方のファイアウォールで **download-and-install** を選択し、**Sync To Peer (**ピアと同期**)** を有効化して、いずれかのファイアウォールがアクティブ-セカンダリ状態になった場合に、アクティブ-プライマリ ファイアウォールが更新コンテンツをダウンロードおよびインストールして、それをアクティブ-セカンダリ ファイアウォールにプッシュさせるようにします。

STEP 4 | （任意）アンチウイルス、アンチスパイウェア、および脆弱性保護用のカスタム セキュリティ プロファイルを作成します。

あるいは、事前定義済みのデフォルトあるいは厳格なプロファイルを使用することもできます。

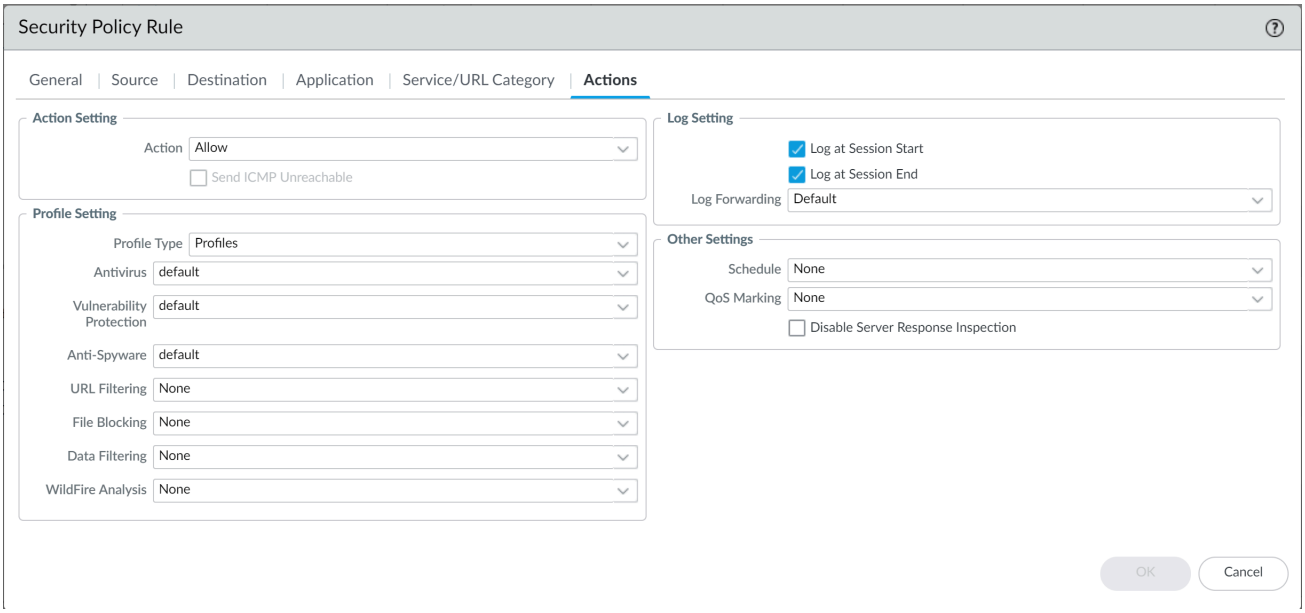
安全に ベストプラクティスとしてのセキュリティプロファイル へ移行し、最高のセキュリティ体制を整えます。

- カスタム アンチウイルス プロファイルを作成するには、**Objects (**オブジェクト**)** > **Security Profiles (**セキュリティ プロファイル**)** > **Antivirus (**アンチウイルス**)** を選択して新しいプロファイルを **Add (**追加**)** します。安全に目標を達成するために、アンチウイルス プロファイル移行ステップを利用してください。
- カスタム アンチスパイウェア プロファイルを作成するには、**Objects (**オブジェクト**)** > **Security Profiles (**セキュリティ プロファイル**)** > **Anti-Spyware (**アンチスパイウェア**)** を選択して新しいプロファイルを **Add (**追加**)** します。安全に目標を達成するために、アンチスパイウェア プロファイル移行ステップ を利用してください。
- カスタム 脆弱性保護プロファイルを作成するには、**Objects (**オブジェクト**)** > **Security Profiles (**セキュリティ プロファイル**)** > **Vulnerability Protection (**脆弱性保護**)** を選択して新しいプロファイルを **Add (**追加**)** します。安全に目標を達成するために、脆弱性プロテクション プロファイル移行ステップ を利用してください。

STEP 5 | セキュリティ プロファイルをセキュリティポリシールールにアタッチします。

脆弱性保護プロファイルを使用して接続をブロックするセキュリティポリシールールを持つファイアウォールを設定すると、ファイアウォールは自動的にそのハードウェア内のトラフィックをブロックします（ブロックされた IP アドレスの監視を参照）。

1. **Policies (ポリシー)** > **Security (セキュリティ)** を選択し、さらに変更したいルールを選択します。
2. **Actions** （アクション） タブで **Profiles (プロファイル)** を **Profile Type (プロファイル タイプ)** として選択します。
3. **Antivirus (アンチウイルス)**、**Anti-Spyware (アンチスパイウェア)**、および **Vulnerability Protection (脆弱性保護)** 用に作成したセキュリティ プロファイルを選択します。



STEP 6 | 変更をコミットします。

Commit（コミット）をクリックします。

DNS セキュリティ

DNS セキュリティは、DNS を使用する高度な脅威からネットワークを保護するための脅威防止サービスであり、継続的に進歩しています。このサービスは高度な機械学習と予測解析を活用し、リアルタイムの DNS リクエスト分析を提供し、C2 およびデータ盗難のために DNS を使うマルウェアを防止する目的に特化した DNS シグネチャを迅速に生成・配信します。これは拡張可能なクラウド アーキテクチャを組み合わせてスケーラブルな脅威インテリジェンス システムを利用できるようにし、ネットワークの保護を最新の状態に保ちます。

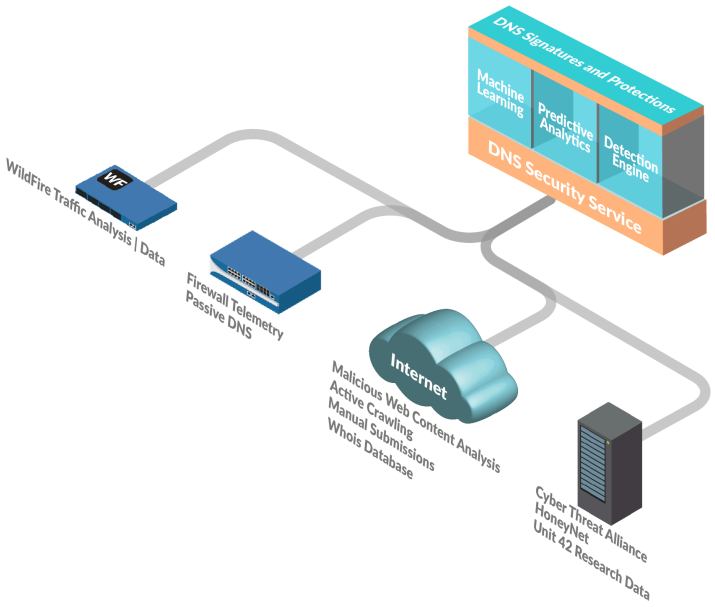
- DNS セキュリティについて
- クラウド配信型の DNS シグネチャおよび保護
- DNS セキュリティ分析
- DNS セキュリティの有効化
- DNS セキュリティ データの収集とログ記録

DNS セキュリティについて

アクティブな脅威防止ライセンスを持つお客様は、Palo Alto Networks が生成したドメインのリストを使用して、ファイアウォールが DNS リクエストをシンクホールするよう設定することができます。ローカルでアクセスするこれらのカスタマイズ可能な DNS シグネチャ リストはアンチウイルスおよび WildFire 更新に同梱されており、公表時点のポリシー適用および保護に最も関連する脅威が含まれています。DNS を使用する脅威をより良くカバーするために、DNS セキュリティ サブスクリプションは、ユーザーが高度な予測分析を使用してリアルタイムで保護を利用できるようにします。DGA/DNS トンネリング検出および機械学習などの技術を使用し、DNS トラフィックに潜む脅威を事前に特定し、制限なくスケーリングできるクラウドサービスで共有します。DNS シグネチャおよび保護はクラウドベースのアーキテクチャで保存されるため、様々なデータソースを使用して生成された、常に拡大するシグネチャのデータベースをフル活用できます。これによりリアルタイムで、DNS を使用する一連の脅威、新たに生成された悪意のあるドメインを防止することができます。将来の脅威と戦うために、DNS セキュリティ サービスの分析、検出、保護機能の更新を、コンテンツ リリースを通じて利用できるようになっています。

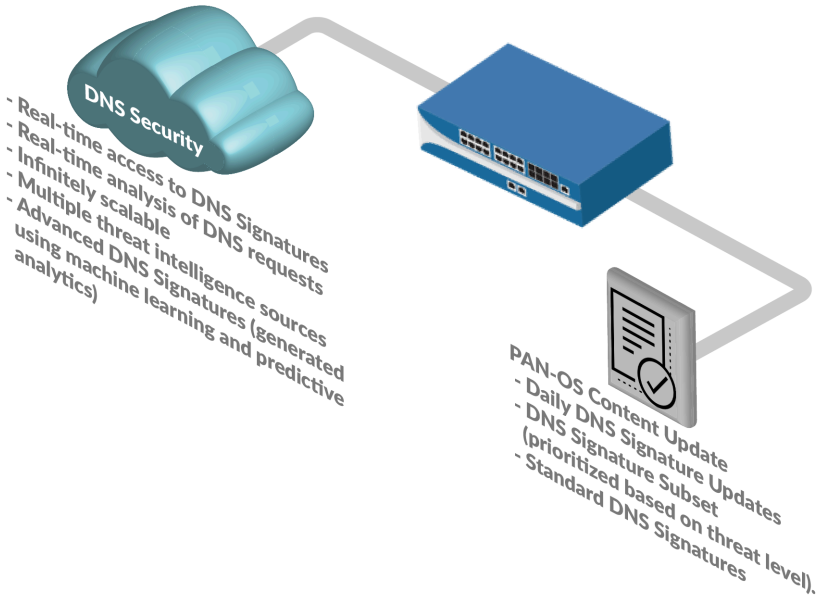
DNS セキュリティ サービスにアクセスするためには、有効な脅威防止ライセンスおよび DNS セキュリティ ライセンスが必要です。

次のワークフローは、DNS セキュリティ サービスが様々なデータソースを使用して DNS シグネチャを生成する方法を説明しています。



クラウド配信型の DNS シグネチャおよび保護

クラウドベースのサービスである DNS セキュリティを使用すれば、制限なくスケーリングできる DNS シグネチャおよび保護ソースを利用して、悪意のあるドメインから組織を守ることができます。Palo Alto Networks が生成するドメイン シグネチャおよび保護は、WildFire トラフィック分析、パッシブ DNS、アクティブ WEB クローリングおよび悪意のある Web コンテンツ分析、URL サンドボックス分析、Honeynet、DGA リバースエンジニアリング、テレメトリーデータ、whois、Unit 42 研究組織、Cyber Threat Alliance のようなサードパーティのデータソースを元にして生成されます。オンデマンドのクラウド データベースを使用すれば、高度な分析技術を使用して生成されたシグネチャを含む Palo Alto Networks の DNS シグネチャ一式やリアルタイムの DNS リクエスト分析を利用することができます。ダウンロードしてローカルで使用できる一連の DNS シグネチャ (アンチウイルスおよび WildFire 更新に同梱) には 100,000 件のシグネチャというキャパシティ制限が規定で備わっており、高度な分析を通じて生成されたシグネチャは含まれていません。毎日のように生成される大量の新しい DNS シグネチャにより良く対応するために、クラウドベースのシグネチャ データベースが、新たに追加された DNS シグネチャをユーザーが即座に利用できるようにします。更新をダウンロードする必要はありません。ネットワーク接続がダウンした、あるいは到達できない場合、ファイアウォールはオンボックスの DNS シグネチャ セットを使用します。



DNS セキュリティ分析

DNS セキュリティ サービスは、複数の DNSデータ ソースで予測分析と機械学習を使用して、リアルタイムの DNS 要求分析を操作します。これは、DNS ベースの脅威に対する保護を生成するために使用されます。DNS ベースの脅威には、セキュリティ ポリシー ルールにアタッチされたスパイウェア対策セキュリティ プロファイルの設定を通じてリアルタイムでアクセスできます。各 DNS 脅威カテゴリ (DNS シグネチャソース) を使用すると、特定のシグネチャ タイプのログ重大度レベルだけでなく、個別のポリシー アクションを定義できます。これにより、ネットワーク セキュリティ プロトコルに応じて、脅威の性質に基づいて特定のセキュリティ ポリシーを作成できます。また、Palo Alto Networks は、PAN-DB とAlexa からのメトリックに基づいて、明示的に許可されたドメインのリストを生成および維持します。これらの許可リストドメインは頻繁にアクセスされ、悪意のあるコンテンツがないことが分かっています。DNS セキュリティ カテゴリと許可リストは更新され、PAN-OS コンテンツ リリースを通じて拡張可能です。

AutoFocus を使用して、DNS セキュリティ クラウド サービスによって生成された組織の DNS 統計データを表示できます。これにより、利用可能な DNS カテゴリに基づいて、ネットワークを通過する DNS リクエストの内訳を説明する、高速かつ視覚的な評価が得られます。あるいは、トランザクション詳細に加えて、**test dns-proxy dns-signature fqdn *<domain>*** コマンドを使用するレイテンシと TTL などのドメイン情報を取得できます。

*PAN-OS 10.0*以降にアップグレードすると、*DNS* セキュリティ ソースが新しいカテゴリに再定義され、拡張されたきめ細かな制御が得られます。その結果、新しいカテゴリは以前に定義されたアクションを上書きし、デフォルト設定を取得します。新しく定義された *DNS* セキュリティ カテゴリに適したシンクホール、ログの重大度、およびパケット キャプチャの設定を必ず再適用してください。

DNS セキュリティ サービスは現在、次の DNS 脅威カテゴリの検出をサポートしています:

ユニバーサル脅威 *ID* 番号 (脅威ログでは *ID* として示されます) は、ドメインを分類するために *DNS Security* によって使用される特定の *DNS* 検出メカニズムにマップされます。これは、そのドメインが属する大まかな脅威のカテゴリとともに、正確なカテゴリ分けを示すものです。

- コマンドと制御ドメイン :C2 には、マルウェアや侵害されたシステムが使用する URL とドメインが含まれており、攻撃者のリモート サーバーと密かに通信して悪意のあるコマンドを受信したり、データを漏らしたり (DNS トンネリング検出や DGA 検出を含む)、またはターゲットの権限のある DNS サーバー上のリソースを枯渇させたり (NXNSattack など) します。
  - **DNS Tunnel Detection** (UTID:109001001/109001002) - DNS トンネリングは、DNS クエリと応答内の非 DNS プログラムおよびプロトコルのデータをエンコードするために攻撃者によって使用される可能性があります。これにより攻撃者は、ファイルを転送したり、システムにリモート アクセスしたりできるバック チャネルを開くことができます。DNS トンネリング検出は機械学習を使用して、ドメインの n-gram 頻度分析、エントロピー、クエリ レート、パターンなどの DNS クエリの挙動傾向を分析し、クエリが DNS トンネリング ベースの攻撃であることを示唆するかどうか判断します。これには、TriFive や Snugy など、検出を避けるために複数のドメインにわたってデータをゆっくりと浸透させる特定の次世代 DNS トンネリング マルウェアが含まれます。ファイアウォールの自動ポリシーアクションとこれを組み合わせることで、DNS トンネリングに隠されたデータ盗難や C2 を素早く検出し、定義したポリシールールに基づいて自動的にそれをブロックできるようになります。
  - **DGA Domain Detection** (UTID:109000001):ドメイン生成アルゴリズム(DGA)は、ドメインを自動生成するために使用され、通常は悪意のあるコマンド アンド コントロール(C2)通信チャネルを確立するコンテキスト内で大量に生成されます。DGA ベースのマルウェア (Pushdo、BankPatch、CryptoLocker など) は、多数の疑いのある疑いがある範囲内でアクティブな C2 サーバーの位置を隠すことによってドメインの数がブロックされないように制限し、時刻、暗号化キー、ディクショナリ名の派生スキーム、およびその他の一意の値などの要因に基づいてアルゴリズム的に生成できます。DGA が生成する大抵のドメインは有効なドメインとして解決されませんが、脅威を完全になくすためにはすべてを特定する必要があります。DGA 分析は、DGA で頻繁に使用される他の技術に対してリバース エンジニアリングを行って分析することで、人ではなく機械によってドメインが生成されたと考えられるかどうか判断します。その後 Palo Alto Networks はこれらの特性を使用して未知だった DGA ベースの脅威をリアルタイムで特定し、ブロックします。
  - **NXNSAttack** (UTID:109010007) -DNSプロトコルに存在するNXNSAttackの脆弱性は、すべての再帰DNSリゾルバーに影響を及ぼし、悪意のある攻撃者がDDOSのような増幅攻撃を開始して、脆弱な権威DNSサーバーの通常の動作を妨害する可能性があります。NXNSAttack は、再帰 DNS リゾルバーに無効な要求を大量に発行してサーバーをシャットダウンする可能性を強制することで、権限のある DNS サーバーに大量のトラフィックスパイクを発生させる可能性があります。
  - **DNS Rebinding** (UTID:109010009) - DNSリバインディング攻撃は、短いTTLパラメータで構成された攻撃者が管理するドメインにユーザーを誘い込み、ドメイン名の解決方法を操作して、ブラウザの同一生成元ポリシーを悪用し迂回させるものです。これにより、悪意のあるアクターは、プライベート ネットワーク内のリソースを攻撃またはアクセスするための仲介役としてクライアント マシンを使用できます。

  - **DNS Infiltration** (UTID:109001003) - DNS侵入には、悪意のある行為者が不正なA（IPv4）およびAAAA（IPv6）レコード要求への応答を通じて、微細なペイロードを隠し、解決できるようにするDNSクエリが含まれます。クライアントが複数のサブドメインを解決し、それぞれがエンコードされたコンポーネントを持つA/AAAAレコードを含む場合、それらに含まれるデータを統合して悪意のあるペイロードを形成し、クライアントマシンで実行することが可能です。ペイロードを実行した後、DNSトンネルを確立するためのセカンダリペイロードを導入したり、追加のエクスプロイトを行うことができます。
- ダイナミック**DNS**ホストドメイン （UTID：109020002) –ダイナミックDNS（DDNS）サービスは、ホスト名とIPアドレスのマッピングをほぼリアルタイムで提供し、静的IPが利用できないときに、特定のドメインにリンクしたIPアドレスの変更を維持することができます。これにより、攻撃者は DDNS サービスを使用してネットワークに侵入し、コマンド アンド コントロール サーバーをホストする IP アドレスを変更することができます。マルウェア キャンペーンとエクスプロイト キットは、ペイロード配布戦略の一部として DDNS サービスを利用する可能性があります。ホスト名インフラストラクチャの一部として DDNS ドメインを利用することにより、攻撃者は特定の DNS レコードに関連付けられた IP アドレスを変更し、検出をより簡単に回避できます。DNS セキュリティは、さまざまなソースからの DNS データをフィルタリングおよび相互参照して候補リストを生成し、さらに検証して精度を最大化することにより、悪用される DDNS サービスを検出します。
- **Malware Domains** –悪意のあるドメインは、マルウェアをホストおよび配布し、さまざまな脅威（実行ファイル、スクリプト、ウイルス、ドライブバイダウンロードなど）をインストールしようとするWebサイトを含む可能性があります。悪意のあるドメインは、外部ソースを介して悪意のあるペイロードをネットワークに配信するという点で C2ドメインと区別できますが、C2では、感染したエンドポイントは通常、リモート サーバーに接続して、追加の命令やその他の悪意のあるコンテンツを取得しようとします。
  - **Malware Compromised DNS** (UTID:109003001）-DNSを侵害するマルウェアには、一見すると本物のように見えるホスト名やサブドメインを生成し、実際には悪意のあるものを生成する、さまざまな手法があります。これには、データベース中心のセキュリティソリューションを偽装したり、誤解させたり、回避したりするために、既存の評判の良いホスト名を模倣した新しく観察されたホスト名が含まれます。これらは、データベースリストへの追加を先取りするために、一括して迅速に生成できます。ドメインシャドウイングは、通常、攻撃者がより一般的な攻撃によってドメインアカウントの制御を取得した後に続きます。これにより、ルートドメインが正当かつ有効であるにもかかわらず、攻撃の調整に使用される不正なサブドメインを作成するために必要なアクセスが提供され、ネットワークセキュリティを回避できる可能性が高くなります。
- **Newly Registered Domains** (UTID:109020001) - 新しく登録されたドメインは、TLD オペレータによって最近追加されたドメイン、または過去 32 日以内に所有権が変更されたドメインです。新しいドメインは正当な目的で作成できますが、大部分は C2サーバーとしての運用やマルウェア、スパム、PUP/アドウェアの配布などの悪意のある行動を促進するために使用されることがよくあります。Palo Alto Networks は、特定のフィード (ドメイン レジストリとレジストラ)を監視し、ゾーンファイル、パッシブ DNS、WHOIS データを使用して登録キャンペーンを検出することにより、登録されたばかりのドメインを検出します。
- **Phishing Domains** (UTID:109010001) –フィッシング ドメインは、フィッシングやファーミングによって正当な Web サイトになりすますことにより、個人情報やユーザーの資格情報などの機密データを送信させるようにユーザーを誘導しようとします。これらの悪意のある活動では、ソーシャルエンジニアリング キャンペーン (一見すると信頼できる送信元がユーザー

を操作して、電子メールまたはその他の形式の電子通信を介して個人情報を送信する)、または正当と思われる不正なサイトにユーザーを誘導する Web トラフィック リダイレクトを通じて実行する可能性があります。

- **Grayware Domains** (UTID:109010002) —(PAN-OS コンテンツ リリース 8290 以降のインストールで使用可能)。グレーウェアドメインは、通常、直接的なセキュリティ上の脅威をもたらすものではありませんが、攻撃のベクトルを容易にしたり、さまざまな望ましくない動作を引き起こしたり、単に疑わしい/不快なコンテンツを含む可能性があります。これらには、次のような Web サイトやドメインが含まれます。
  - ユーザーをだましてリモート アクセスを許可するようにします。
  - アドウェアやその他の未承諾のアプリケーション (暗号マイナー、ハイジャック犯、および PUP (望ましくない可能性のあるプログラム) など) が含まれています。
  - 高速フラックス技術によるドメイン識別隠蔽動作の展開 (**fastflux detection** - UTID:109010005).
  - DNSセキュリティの予測分析を通じて証明される悪意のある行動と使用法を実証 (悪意のある **NRD** - UTID:109010006).
  - Webページのアドレスを入力する際のユーザーのミスを利用する（**typosquatting domains**）。
  - 権威あるDNSサーバーのDNSレコードが不適切に設定されているか、または古く、削除またはその他の方法で修正されていないために、正当なソースから悪意のあるウェブサイトへトラフィックをリダイレクトする (ダングリング **DNS** - UTID:109010008).
  - 違法行為や詐欺を促進します。
  - ブロックリストを回避したり、悪意のあるWebサイトにトラフィックをルーティングすることでワイルドカードDNS攻撃を可能にするために使用できるワイルドカードDNSエントリを含む (ワイルドカードの悪用 - UTID: 109002001).
  - 収集したDNSデータから構築された確立されたベースラインプロファイルと比較して、異常な特性を持つDNSトラフィックの存在を示す (異常検出)。
  - 数ヶ月または数年前に登録され、休眠状態のままにされ、アクティブになったときに評判チェックをバイパスしている。これには、今まで見られなかった、または評価もされていないといった新たに観察されたドメインも含まれます (戦略的に古いドメイン - UTID:109002002).
- パークドメイン (UTID:109010003)—(PAN-OS コンテンツ リリース 8318 以降のインストールで利用可能) Parked ドメインは、通常、限られたコンテンツをホストする非アクティブな Web サイトであり、多くの場合、ホスト エンティティの収益を生み出す可能性のあるクリックスルー広告の形式で行われますが、一般にエンド ユーザーにとって有用なコンテンツは含まれていません。多くの場合、これらは正当なプレースホルダーとして機能するか、または単なる迷惑行為として機能しますが、マルウェアの配布の可能性のあるベクトルとしても使用される可能性があります。
- プロキシ回避とアノニマイザー（匿名化） (UTID:109010004)—(PAN-OS コンテンツ リリース 8340 以降のインストールで利用可能)Proxy Avoidance and Anonymizers は、コンテンツ フィルタリング ポリシーをバイパスするために使用されるサービスへのトラフィックです。アノニマイザー プロキシ サービスを介して組織のコンテンツ フィルタリング ポリシーを回避しようとするユーザーは、DNS レベルでブロックされます。

DNS セキュリティの有効化

DNS セキュリティを使用するドメイン クエリの DNS シンクホールを有効化するには、DNS セキュリティ サブスクリプションをアクティベートし、DNS セキュリティ サービスを参照するためにアンチスパイウェア ポリシーを作成 (または変更) し、各 DNS シグネチャ カテゴリのログ重大度とポリシー設定を設定し、プロファイルをセキュリティ ポリシー ルールに付与する必要があります。

STEP 1 | 「サブスクリプション ライセンスのアクティベーション」を行います。

STEP 2 | セキュリティ ポリシーの *paloalto-dns-security* App-ID が、DNS セキュリティ クラウド セキュリティ サービスからの のトラフィックを有効にする に構成されていることを確認します。

App-ID セキュリティ ポリシーを適用するように構成されたインターネットに接続する境界ファイアウォールを使用して、ファイアウォールの展開によって管理トラフィックがルーティングされる場合は、境界ファイアウォールで *App-ID* を許可する必要があります。これを行わないと、*DNS* セキュリティ接続ができなくなります。

STEP 3 | 定義されたシンクホールにマルウェア DNS クエリを送信するように、DNS セキュリティ署名ポリシー設定を構成します。

ドメイン許可リストとして外部動的リストを使用する場合、*DNS* セキュリティ ドメイン ポリシーの動作よりも優先されません。その結果、*EDL* のエントリと *DNS* セキュリティ ドメイン カテゴリに一致するドメインがある場合、*EDL* が許可のアクションで明示的に構成されている場合でも、*DNS* セキュリティで指定されたアクションは適用されます。*DNS* ドメインの例外を追加する場合は、アラート アクションを使用して *EDL* を構成するか、*DNS* 例外タブ *(手順 8)* にある *DNS* ドメイン/*FQDN* 許可一覧に追加します。

1. **Objects (オブジェクト) >** > **Security Profiles (セキュリティ プロファイル) >** > **Anti-Spyware (アンチスパイウェア)** を選択します。
2. 既存のプロファイルを変更あるいはプロファイルを作成するか、既存のデフォルト プロファイルの 1 つを選択してコピーします。
3. プロファイルに **Name (名前)** を付け、任意で説明を入力します。
4. **DNS Policies (DNS ポリシー)** タブを選択します。
5. **Signature Source (シグネチャ送信元)**列にある DNS セキュリティ見出しの下に、個別に設定可能な DNS シグネチャ送信元があり、個別のポリシー アクションとログの重大度レベルを定義できます。

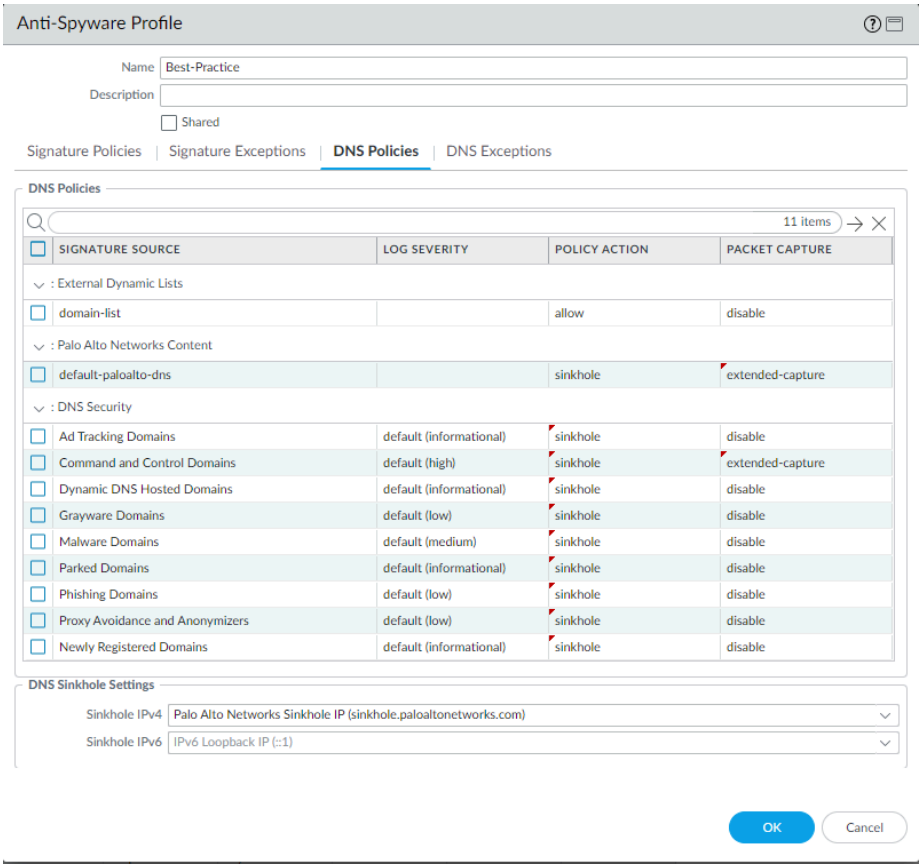
   Palo Alto Networks では、シグネチャ送信元のデフォルトの *DNS* ポリシー設定を変更して、最適なカバレッジを確保し、インシデントの応答と修復を支援することを推奨しています。ネットワークをレイヤー4 およびレイヤー7 回避から保護するためのベスト プラクティスで概説されているように、*DNS* セキュリティ設定を設定するためのベストプラクティスに従ってください。

   - ファイアウォールが DNS シグネチャに一致するドメインを検出したときに記録される、ログの重大度レベルを指定します。様々なログ重大度レベルの詳細情報は、Threat Severity Levels (脅威の重大度レベル) を参照してください。
   - DNS セキュリティ シグネチャ ソースの既知のマルウェア サイトに対して DNS ルックアップが行われる際に行うアクションを選択します。オプションは、許可、ブロック、シンクホール、またはデフォルトです。アクションがシンクホールに設定されていることを検証します。
   - DNS トラフィック検査を完全にバイパスするには、ポリシー アクションを **Allow** に設定し、対応するログ重大度を **None** に構成します。
   - （任意）**Packet Capture (パケット キャプチャ - pcap)** ドロップダウンリストにて、セッションの最初のパケットをキャプチャする場合は**single-packet**を、1～50の間で設定を行うには**extended-capture**を選択します。その後、packet capture (パケット キャプチャ - pcap) を使用してさらに解析できます。
6. **DNS Sinkhole Settings (DNS シンクホール設定)** セクションで **Sinkhole (シンクホール)** が有効になっていることを確認します。便宜を図るため、デフォルトのシンクホールのアドレス (sinkhole.paloaltonetworks.com) は Palo Alto Networks サーバーにアクセスする

よう設定されています。Palo Alto Networks はコンテンツ更新によりこのアドレスを自動的に更新する場合があります。

Sinkhole IPv4 または**Sinkhole IPv6**アドレスをネットワーク上のローカルサーバーまたはループバックアドレスに変更する場合は、ネットワーク上のローカル サーバーにシンクホールIPアドレスを設定を参照してください。

7. **OK** をクリックし、アンチスパイウェア プロファイルを保存します。



STEP 4 | アンチスパイウェア プロファイルをセキュリティポリシールールに適用します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. **Security Policy Rule (**セキュリティポリシー ルール**)** を選択するか、作成します。
3. **Actions (**アクション**)**タブで、**Log at Session End (**セッション終了時にログを記録**)**チェック ボックスをオンにして、ログを有効にします。
4. Profile Setting [プロファイル設定]セクションで**Profile Type**[プロファイルタイプ]ドロップダウンリストをクリックし、すべての**Profiles**[プロファイル]を表示します。**Anti-Spyware (**アンチスパイウェア**)** ドロップダウンリストで、新しい、あるいは修正したプロファイルを選択します。
5. **[OK]** をクリックしてポリシー ルールを保存します。

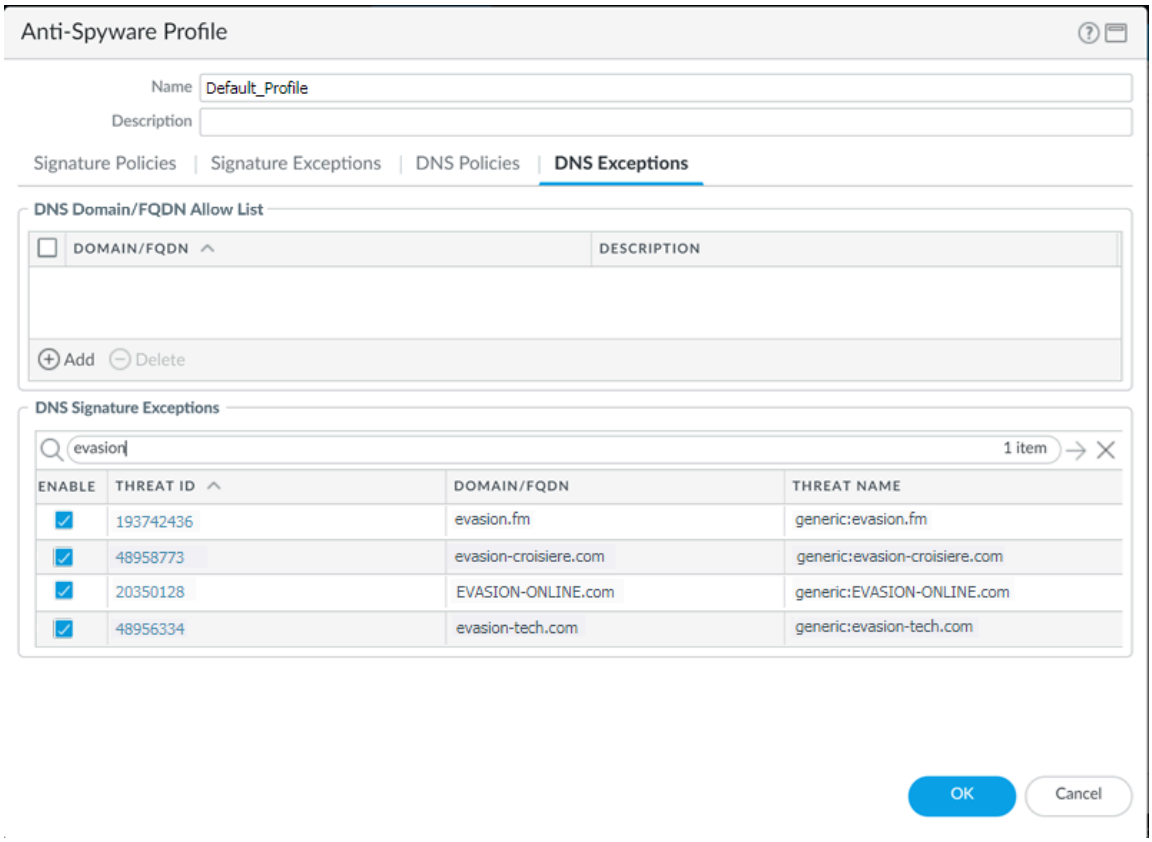
STEP 5 | ポリシー アクションが適用されているかどうかテストします。

1. 次のテスト　ドメインにアクセスして、特定の脅威タイプのポリシー　アクションが実施されていることを確認します。
   - C2—test-c2.testpanw.com
   - DNS Tunneling—test-dnstun.testpanw.com
   - C2—test-c2.testpanw.com
   - ダイナミック DNS—test-ddns.testpanw.com
   - マルウェア—test-malware.testpanw.com
   - 登録されたばかりのドメイン—test-nrd.testpanw.com
   - フィッシング—test-phishing.testpanw.com
   - グレイウェア—test-grayware.testpanw.com
   - パーク—test-parked.testpanw.com
   - プロキシ回避およびアノニマイザ—test-proxy.testpanw.com
2. ファイアウォール上のアクティビティを監視するには：
   1. **ACC**を選択し、URL Domain [URLドメイン]をグローバルフィルターとして追加し、アクセスしたドメインのThreat Activity [脅威アクティビティ]およびBlocked Activity [ブロックされたアクティビティ]を確認します。
   2. **Monitor (**監視**)** > **Logs (**ログ**)** > **Threat (**脅威**)** を選択し、`(action eq sinkhole)` でフィルタリングしてシンクホールされたドメインのログを確認します。

STEP 6 | トラフィックログで感染したトラフィックのホストを特定

STEP 7 | (任意) 誤検出がある場合、ドメイン シグネチャ例外を追加します。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **Anti-Spyware (アンチスパイウェア)** を選択します。
2. 変更するプロファイルを選択します。
3. 脅威シグネチャを除外したいアンチスパイウェア プロファイルを **Add (追加)** するか、既存のものを変更し、**DNSExceptions (DNS 例外)** を選択します。
4. 名前あるいは FQDN を入力し、除外する DNS シグネチャを検索します。
5. 適用から除外する DNS signature の各 **Threat ID** のチェックボックスをオンにします。
6. **OK** をクリックし、新しい、あるいは変更したアンチスパイウェア プロファイルを保存します。



STEP 8 | (任意) 許可リストを追加して、明示的に許可するDNS ドメイン/ FQDN のリストを指定します。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **Anti-Spyware (アンチスパイウェア)** を選択します。
2. 変更するプロファイルを選択します。
3. 脅威シグネチャを除外したいアンチスパイウェア プロファイルを **Add (追加)** するか、既存のものを変更し、**DNSExceptions (DNS 例外)** を選択します。
4. 新しい **FQDN Allow List (FQDN 許可リスト)** を **Add (追加)** するには、DNS ドメインまたは FQDN ロケーションおよび説明を指定します。
5. **OK** をクリックし、新しい、あるいは変更したアンチスパイウェア プロファイルを保存します。

STEP 9 | (任意) DNS セキュリティ サービスへのファイアウォールの接続を確認します。サービスに到達できない場合は、以下のドメインがブロックされていないことを確認してください: dns.service.paloaltonetworks.com.

ファイアウォールで以下の CLI コマンドを使用して、DNS セキュリティ サービスにファイアウォールが接続可能か確認します。

```
show dns-proxy dns-signature info
```

以下に例を示します。

```
show dns-proxy dns-signture info Cloud URL:
 dns.service.paloaltonetworks.com:443 Telemetry URL:
 io.dns.service.paloaltonetworks.com:443 Last Result:None
 Last Server Address:None Last Server Address:None Last Server
 Address:Interval 43200 sec Request Waiting Transmission:0 Request
 Pending Response:0 Cache Size:0
```

STEP 10 | (任意) レイテンシ、TTL、シグネチャのカテゴリなど、指定ドメインのトランザクション詳細を取得します。

ファイアウォール上で次のCLIコマンドを実行し、リストの詳細情報を表示します。

```
test dns-proxy dns-signature fqdn
```

以下に例を示します。

```
test dns-proxy dns-signature fqdn www.yahoo.com DNS
 Signature Query [ www.yahoo.com ] Completed in 178 ms
 DNS Signature Response Entries:2 Domain Category GTID TTL
 ------------------------------------------------------------------------------
 *.yahoo.com Benign 0 86400 www.yahoo.com Benign 0 3600
```

STEP 11 | （任意）DNS シグネチャ検索のタイムアウト設定を行います。接続の問題により、ファイアウォールが割り当てられた時間内にシグネチャの判定を取得できない場合、後続のすべ

ての DNS 応答を含む要求はパススルーされます。平均遅延をチェックして、要求が設定された期間内に収まることを確認できます。平均遅延が設定された期間を超える場合は、要求がタイムアウトしないように、平均遅延よりも高い値に設定を更新することを検討してください。

1. CLI で以下のコマンドを発行して、平均遅延を表示します。

```
show dns-proxy dns-signature counters
```

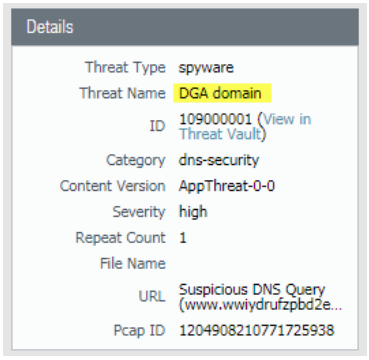
   デフォルトのタイムアウト値は 100 ミリ秒です。

2. 出力を下にスクロールして、シグネチャ クエリ API 見出しの下の遅延セクションに移動し、平均遅延が定義されたタイムアウト期間内であることを確認します。この遅延は、DNS セキュリティ サービスからシグネチャの判定を取得するのに平均してかかる時間を示します。さまざまな遅延期間の追加の待機時間統計は、平均以下と分かります。

```
Signature query API: . . . [latency ] : max 1870 (ms) min
 16(ms) avg 27(ms) 50 or less :47246 100 or less :113 200 or
 less :25 400 or less :15 else :21
```

3. 平均遅延が一貫してデフォルトのタイムアウト値を超えている場合は、要求を特定の期間内に収めるように設定を上げることができます。**Device**（デバイス）**> Content-ID** を選択し、**Realtime Signature Lookup**（リアルタイム シグネチャ ルックアップ）設定を更新します。
4. 変更を [コミット] します。

シンクホール化された DNS クエリを表示するには、firewall 脅威ログ (**Monitor > Logs** を参照し、リストからログの種類を選択します):



DNS セキュリティ データの収集とログ記録

DNS セキュリティ サービス は、ファイアウォール のセキュリティ ポリシールール、関連するアクション、およびドメイン検索を実行する際の DNS クエリの詳細に基づいて、サーバーの応答と要求情報を収集します。ファイアウォールは、補足 DNS データを DNS セキュリティ クラウド サーバーに転送し、Palo Alto Networks サービスによって使用され、より正確なドメイン情報 (プロバイダー ASN、ホスティング情報、位置情報識別など) を提供します。この補足データは DNS セキュリティ サービスを運用するために必要ではありませんが、強化された分析、DNS 検出、および予防機能を生成するためのリソースを提供します。このアクションは、収集後 30

秒以内に発生し、バッチ処理がファイアウォールのパフォーマンスに影響を与えません。ファイアウォールの負荷が高い場合、DNS データ収集は必要に応じてスケールダウンし、期待されるパフォーマンス レベルを維持します。

ファイアウォールは、次のデータ フィールドを送信できます。

項目	の意味
アクション	DNS クエリに対して実行されたポリシーアクションを表示します。
タイプ	DNS レコードの種類を表示します。
応答	DNS クエリのドメインが解決した IP アドレス。
応答コード	DNS クエリに対する応答として受信された DNS 応答コード。
送信元IP	DNS 要求を行ったシステムの IP アドレス。
送信元ユーザー	ファイアウォールの User-ID 機能が有効になっている場合は、DNS リクエスターの ID が表示されます。
Source Zone	セキュリティ ポリシールールで参照されている構成済みのソースゾーン。

DNS の拡張データ収集は、*DNS* 例外の許可リストに追加されたドメインに対してバイパスされます。

潜在的にユーザを識別するために使用できるデータフィールド（送信元 IP、送信元ユーザ、および送信元ゾーン）は、次の CLI コマンドを使用して自動送信から差し控えることができます。**set deviceconfig** 設定 **ctd cloud-dns-privacy-mask** はい。更新を有効にするには、コミット をコミットする必要があります。

DNS クエリを使用してネットワーク上の感染ホストを特定する

アンチスパイウェア プロファイルの DNS シンクホール アクションにより、既知の悪意あるドメインの DNS クエリあるいはカスタムドメインに対する応答をファイアウォールが偽装し、ネットワーク上のマルウェアに感染したホストを特定することができます。侵入されたホストは、コマンド アンド コントロール (C2) サーバーとの通信を開始する可能性があります。接続が確立されると、攻撃者は感染したホストをリモートから制御し、ネットワークにさらに侵入したりデータを漏洩させることができます。

Palo Alto Networks の DNS シグネチャ リストに含まれているあらゆるドメインにクエリするDNSは、Palo Alto Networks のサーバー IP アドレスにシンクホールされます。

ファイアウォールには、悪意のあるドメインおよび C2 ドメインを識別するために使用できる DNS シグネチャの送信元が 2 つあります。

- (脅威防止が必要) ローカル DNS シグネチャ–これはファイアウォールが悪意のあるドメインを識別するために使用できる DNS シグネチャの限定された、オンセットのセットです。ファイアウォールは、日々のウイルス対策アップデートの一環として新規の DNS シグネチャを取得します。
- (DNS Security 機能が必要)DNS セキュリティ シグネチャ - ファイアウォールは、Palo Alto Networks DNS Security クラウド サービスにアクセスして、DNS シグネチャの完全なデータベースに対して悪意のあるドメインをチェックします。DNS セキュリティのみが提供する特定のシグネチャは、ドメイン生成アルゴリズム (DGA) や DNS トンネリングなどの機械学習技術を使用した C2 攻撃を一意に検出することができます。

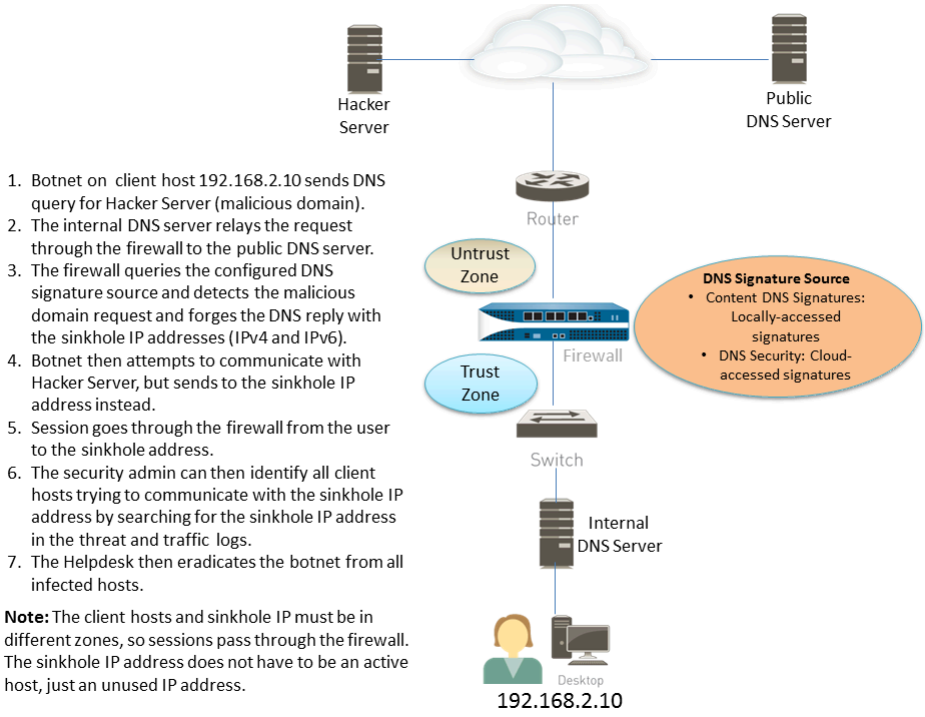
ローカル DNS シグネチャセットまたは DNS セキュリティシグネチャセット内のドメインへの DNS クエリは、Palo Alto Networks サーバーにリダイレクトされ、ホストは悪意のあるドメインにはアクセスできません。次のトピックでは、DNS シンクホールを有効にして、感染ホストを特定する方法について詳細にご説明します。

- DNS シンクホールの動作原理 を確認します。
- 「DNS シンクホールの設定」を行います。
- カスタムドメインのリスト用にDNS シンクホールを設定します。
- DNS セキュリティを有効にして、C2 ドメインをシンクホールします。
- ネットワーク上のローカル サーバーにシンクホール IP アドレスを設定します。
- 「悪意のあるドメインへの接続を試みた感染ホストを確認」を行います。

DNS シンクホールの動作原理

DNS シンクホール機能を使用すると、ファイアウォールが感染クライアントの DNS クエリを見ることができない状況（つまり、ファイアウォールが DNS クエリの発信元を確認できない状況）で、DNS トラフィックを使用して保護されたネットワーク上の感染ホストを特定できます。ファイアウォールがローカル DNS サーバーよりもインターネット側にある通常のデプロイメントでは、脅威ログは、実際の感染ホストではなくローカル DNS リゾルバをトラフィックの送信元として識別します。マルウェア DNS クエリのシンクホール処理では、この可視性の問題

を以下のようにして解決します。すなわち、クライアント ホストによる悪意あるドメインへのクエリに対する応答を偽装することで、悪意あるドメイン (たとえば、コマンド アンド コントロールなど) への接続を試みるクライアントが、デフォルトの Palo Alto Networks シンクホール IP アドレス (あるいはカスタムドメインのリスト用に DNS シンクホールを設定する場合は定義済みの IP アドレス) に接続を試みるように仕向けます。その後、感染ホストを簡単にトラフィック ログで特定することができます。



DNS シンクホールの設定

DNS シンクホールを有効化するためには、デフォルトのアンチスパイウェア プロファイルをセキュリティポリシー ルールに付与します (アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップを参照)。ユーザーが指定する Palo Alto Networks の DNS シグネチャ ソースに含まれているあらゆるドメインに対する DNS クエリは、Palo Alto Networks のシンクホール IP アドレスに解決されます。現在、この IP アドレスは IPv4—sinkhole.paloaltonetworks.com、およびループバック アドレス IPv6 address—::1 です。このアドレスは変更される場合があり、コンテンツ更新で更新される可能性があります。

STEP 1 | 外部動的リスト内のドメインのカスタム リスト用にDNS シンクホールを有効化します。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **Anti-Spyware (アンチスパイウェア)** を選択します。
2. 既存のプロファイルを変更するか、既存のデフォルト プロファイルの 1 つを選択してコピーします。
3. プロファイルの **Name**（名前） を入力し、**DNS Policies**（**DNS**ポリシー）タブを選択します。
4. **default-paloalto-dns** が **Signature Source (シグネチャ送信元)**にあることを確認します。
5. （任意）**Packet Capture (パケット キャプチャ)** ドロップダウンリストにて、セッションの最初のパケットをキャプチャする場合は**single-packet**を、1～50の間で設定を行うには**extended-capture**を選択します。その後、パケット キャプチャを使用してさらに分析できます。

STEP 2 | アンチスパイウェア プロファイルのシンクホール設定を確認します。

1. **DNS Policies (DNS ポリシー)** タブで、DNSクエリの**Policy Action**が **sinkhole(シンクホール)** になっていることを確認します。
2. DNS Sinkhole Settings (DNSシンクホールの設定) セクションで **Sinkhole (シンクホール)** が有効になっていることを確認します。便宜を図るため、デフォルトのシンクホールのIPアドレスはPalo Alto Networksサーバーにアクセスするよう設定されています。Palo Alto Networksはコンテンツ更新によりこのアドレスを自動的に更新する場合があります。

   Sinkhole IPv4 または**Sinkhole IPv6**アドレスをネットワーク上のローカルサーバーまたはループバックアドレスに変更する場合は、ネットワーク上のローカル サーバーにシンクホールIPアドレスを設定を参照してください。
3. **OK** をクリックし、アンチスパイウェア プロファイルを保存します。

STEP 3 | アンチスパイウェア プロファイルをセキュリティポリシールールに適用します。

1. **Policies (ポリシー)** > **Security (セキュリティ)** を選択し、セキュリティポリシー ルールを選択します。
2. **Actions** [アクション] タブで、**Log at Session Start** [セッション開始時にログ]チェックボックスをオンにして、ログを有効にします。
3. Profile Setting [プロファイル設定]セクションで**Profile Type**[プロファイルタイプ]ドロップダウンリストをクリックし、すべての**Profiles**[プロファイル]を表示します。**Anti-Spyware** [アンチスパイウェア]ドロップダウンリストで、新しいプロファイルを選択します。
4. **[OK]** をクリックしてポリシー ルールを保存します。

STEP 4 | ファイアウォール上のアクティビティを監視することで、ポリシーアクションが適用されていることをテストします。

1. **ACC**を選択し、URL Domain [URLドメイン]をグローバルフィルターとして追加し、アクセスしたドメインのThreat Activity [脅威アクティビティ]およびBlocked Activity [ブロックされたアクティビティ]を確認します。
2. **Monitor (監視)** > **Logs (ログ)** > **Threat (脅威)** を選択し、`(action eq sinkhole)` でフィルタリングしてシンクホールされたドメインのログを確認します。

カスタムドメインのリスト用にDNS シンクホールを設定

ドメインのカスタム リスト用のDNS シンクホールを有効にするには、そのドメインを含む外部動的リストを作成し、アンチスパイウェア プロファイルでシンクホール アクションを有効にし、そのプロファイルをセキュリティポリシー ルールに付与する必要があります。クライアントがリストに挙がっている悪意のあるドメインにアクセスしようとすると、ファイアウォールがパケット中の宛先IPアドレスをシンクホール用にデフォルトのPalo Alto Networksサーバーあるいはユーザー定義のIPアドレスに偽装します。

外部動的リストに含まれたカスタムドメインごとに、ファイアウォールはDNSベースのスパイウェア シグネチャを生成します。このシグネチャは Custom Malicious DNS Query <domain name> という名前で、重大度が中程度のスパイウェアです。各シグネチャは、 24 バイトのドメイン名のハッシュです。

各ファイアウォール モデルは、単体あるいは複数の外部動的リストで最大合計 50,000 のドメイン名をサポートしていますが、単体のリストでは最大数の制限がありません。

STEP 1 | 外部動的リスト内のドメインのカスタム リスト用にDNS シンクホールを有効化します。

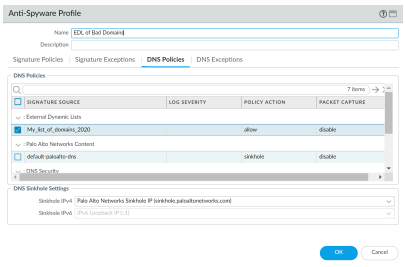
1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **Anti-Spyware (アンチスパイウェア)** を選択します。
2. 既存のプロファイルを変更するか、既存のデフォルト プロファイルの 1 つを選択してコピーします。
3. プロファイルの **Name** [名前]を入力し、**DNS Policies** [DNS ポリシー]タブを選択します。
4. **External Dynamic Lists (外部動的リスト)** シグネチャ送信元から EDL を選択します。

   次のタイプの外部動的リストをすでに作成済みの場合：ドメイン リストはここで選択できます。*URL*あるいは*IP*アドレスのタイプの外部動的リストを作成していても、このリストには表示されません。
5. アンチスパイウェア プロファイルの外部動的リストを設定します（外部動的リストにアクセスするためにファイアウォールを設定を参照）。**Type (タイプ)** のデフォルトの値は **Domain List (ドメイン リスト)** です。
6. （任意）**Packet Capture (パケット キャプチャ)** ドロップダウンリストにて、セッションの最初のパケットをキャプチャする場合は**single-packet**を、1～50の間で設定を行うには**extended-capture**を選択します。その後、パケット キャプチャを使用してさらに分析できます。

STEP 2 | アンチスパイウェア プロファイルのシンクホール設定を確認します。

1. **DNS Policies (DNS** ポリシー**)** タブで、DNSクエリの**Policy Action**が **sinkhole(**シンクホール**)** になっていることを確認します。
2. DNS Sinkhole Settings (DNSシンクホールの設定) セクションで **Sinkhole (**シンクホール**)** が有効になっていることを確認します。便宜を図るため、デフォルトのシンクホールのIPアドレスはPalo Alto Networksサーバーにアクセスするよう設定されています。Palo Alto Networksはコンテンツ更新によりこのIPアドレスを自動的に更新する場合があります。

   Sinkhole IPv4 (シンクホール **IPv4)** あるいは**Sinkhole IPv6 (**シンクホール **IPv6)** アドレスをネットワーク上のローカル サーバーあるいはループバック アドレスに変更する場合はネットワーク上のローカル サーバーにシンクホールIPアドレスを設定をご覧ください。



3. **OK** をクリックし、アンチスパイウェア プロファイルを保存します。

STEP 3 | アンチスパイウェア プロファイルをセキュリティポリシールールに適用します。

1. **Policies (**ポリシー**)** > **Security (**セキュリティ**)** を選択し、セキュリティポリシー ルールを選択します。
2. **Actions** [アクション] タブで、**Log at Session Start** [セッション開始時にログ]チェックボックスをオンにして、ログを有効にします。
3. Profile Setting [プロファイル設定]セクションで**Profile Type**[プロファイルタイプ]ドロップダウンリストをクリックし、すべての**Profiles**[プロファイル]を表示します。**Anti-Spyware** [アンチスパイウェア]ドロップダウンリストで、新しいプロファイルを選択します。
4. **[OK]** をクリックしてポリシー ルールを保存します。

STEP 4 | ポリシー アクションが適用されているかどうかテストします。

1. ドメイン リストに属する外部動的リスト エントリを表示し、リストに含まれるドメインにアクセスします。
2. ファイアウォール上のアクティビティを監視するには：

   1. **ACC**を選択し、URL Domain [URLドメイン]をグローバルフィルターとして追加し、アクセスしたドメインのThreat Activity [脅威アクティビティ]およびBlocked Activity [ブロックされたアクティビティ]を確認します。
   2. **Monitor (**監視**)** > **Logs (**ログ**)** > **Threat (**脅威**)** を選択し、`(action eq sinkhole)` でフィルタリングしてシンクホールされたドメインのログを確認します。

STEP 5 | 外部動的リストのエントリーが無視されるかスキップされるかを検証します。

ファイアウォール上で次のCLIコマンドを実行し、リストの詳細情報を表示します。

```
request system external-list show type domain name <list_name>
```

以下に例を示します。

```
request system external-list show type domain name
 My_List_of_Domains_2015 vsys1/EBLDomain:Next update
 at :Thu May 21 10:15:39 2015 Source : https://1.2.3.4/
My_List_of_Domains_2015 Referenced :Yes Valid :Yes Number of
 entries :3 domains:www.example.com baddomain.com qqq.abcedfg.com
```

STEP 6 | （任意）外部動的リストを必要な時に取得します。

更新されたリストを次の更新のタイミング（その外部動的リスト用に定義した**Repeat** [繰り返し]頻度）ではなくオンデマンドでファイアウォールに取得させるには、次のCLIコマンドを実行します。

```
request system external-list refresh type domain name  <list_name>
```

代わりに、ファイアウォールのインターフェイスを使用して Web　サーバーから外部動的リストを取得することもできます。

ネットワーク上のローカル サーバーにシンクホールIPアドレスを設定

デフォルト設定では、すべてのPalo Alto Networks DNSシグネチャに対してシンクホールが有効になっており、シンクホールIPアドレスはPalo Alto Networksサーバーにアクセスするよう設定されています。シンクホールIPアドレスをネットワーク上のローカル サーバーに設定したい場合はこのセクションの説明に従ってください。

悪意あるソフトウェアがIPv4 と IPv6 のどちらか一方または両方のプロトコルを使用して DNS クエリを実行する可能性があるため、IPv4およびIPv6アドレスの両方を取得してシンクホールIPアドレスとして使用する必要があります。シンクホール IP アドレスとセッションの開始を試みた感染ホストがファイアウォール経由でルーティングされるように、DNS シンクホール アドレスは、クライアント ホストと異なるゾーンに属している必要があります。

このシンクホール アドレスは、この目的のために予約する必要があります。このアドレスを物理ホストに割り当てる必要はありません。また、ハニーポット サーバーを物理ホストとして使用することで、悪意あるトラフィックをさらに詳しく分析することもできます。

以下に示す設定手順では、以下の *DNS* シンクホール アドレスを使用します。

IPv4 DNS シンクホール アドレス – *10.15.0.20*

IPv6 DNS シンクホール アドレス – *fd97:3dec:4d27:e37c:5:5:5:5*

STEP 1 | シンクホール インターフェイスとゾーンを設定します。

クライアント ホストが存在するゾーンからのトラフィックはシンクホール IP アドレスが定義されているゾーンにルーティングする必要があります。これにより、トラフィックがログに記録されます。

シンクホール トラフィックには専用のゾーンを使用します。このゾーンに、感染ホストからのトラフィックが送信されます。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** の順に選択し、シンクホール インターフェイスとして設定するインターフェイスを選択します。
2. **Interface Type**（インターフェイス タイプ） ドロップダウン リストで、**Layer3**（レイヤー **3**） を選択します。
3. IPv4 アドレスを追加するには、**[IPv4]** タブで **[スタティック]** を選択して、**[追加]** をクリックします。この例では、10.15.0.20 を IPv4 DNS シンクホール アドレスとして追加します。
4. **[IPv6]** タブで **[スタティック]** を選択し、**[追加]** をクリックして、IPv6 アドレスとサブネット マスクを入力します。この例では、fd97:3dec:4d27:e37c::/64 を IPv6 シンクホール アドレスとして入力します。
5. **OK** をクリックして保存します。
6. シンクホール用のゾーンを追加するには、**Network (ネットワーク)** > **Zones (ゾーン)** を選択して **Add (追加)** をクリックします。
7. ゾーンの **[名前]** を入力します。
8. **[タイプ]** ドロップダウン リストで、**[レイヤー 3]** を選択します。
9. **[インターフェイス]** セクションで、**[追加]** をクリックして、先ほど設定したインターフェイスを追加します。
10. **OK** をクリックします。

STEP 2 | DNS シンクホールを有効化します。

デフォルト設定では、すべてのPalo Alto Networks DNSシグネチャに対してシンクホールが有効になっています。シンクホール アドレスをローカル サーバーに変更するには、カスタムドメインのリスト用にDNS シンクホールを設定 の アンチスパイウェア プロファイルのシンクホール設定を確認のステップを参照してください。

STEP 3 | Trust ゾーンのクライアント ホストから Untrust ゾーンへのトラフィックを許可するセキュリティ ポリシー ルールを編集して、シンクホール ゾーンを宛先に含め、アンチスパイウェア プロファイルを添付します。

Trustゾーン内のクライアント ホストからUnTrustゾーンに向かうトラフィックを許可するセキュリティポリシールールを編集することで、感染ホストからのトラフィックを確実に識別できるようになります。シンクホール ゾーンをルールに宛先として追加することで、感染クライアントが偽の DNS クエリを DNS シンクホールに送信するようになります。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. クライアント ホスト ゾーンから Untrust ゾーンへのトラフィックを許可する既存のルールを選択します。
3. **[宛先]** タブで、シンクホール ゾーンを **[追加]** します。これにより、クライアント ホスト トラフィックがシンクホール ゾーンに流れるようになります。
4. **Actions** [アクション] タブで、**Log at Session Start** [セッション開始時にログ]チェックボックスをオンにして、ログを有効にします。これにより、Trust ゾーンのクライアント ホストからのトラフィックが、Untrust ゾーンまたはシンクホール ゾーンへのアクセス時にログに記録されるようになります。
5. **[プロファイル設定]** セクションで、DNS シンクホールを有効にした **[アンチスパイウェア]** プロファイルを選択します。
6. **OK** をクリックして Security (セキュリティ) ポリシールールを保存し、**Commit (コミット)** を実行します。

STEP 4 | 感染ホストを確実に特定できるようにするために、Trust ゾーンのクライアント ホストから新しいシンクホール ゾーンへのトラフィックがログに記録されていることを確認します。

この例では、感染したクライアント ホストは 192.168.2.10、シンクホールの IPv4 アドレスは 10.15.0.20 です。

1. Trust ゾーンのクライアント ホストでコマンド プロンプトを開き、以下のコマンドを実行します。

```
C:\>ping <sinkhole address>
```

以下の出力例は、DNS シンクホール アドレス 10.15.0.2 に対して Ping 要求を送信したときの結果です。この例では、シンクホール IP アドレスが物理ホストに割り当てられていないため、結果は、`Request timed out` になっています。

```
C:\>ping 10.15.0.20 Pinging 10.15.0.20 with 32 bytes of
 data:Request timed out.Request timed out.Ping statistics for
 10.15.0.20:Packets:Sent = 4, Received = 0, Lost = 4 (100%
 loss)
```

2. ファイアウォール上で、**Monitor (監視)** > **Logs (ログ)** > **Traffic (トラフィック)** の順に選択して、送信元が 192.168.2.10、宛先が 10.15.0.20 のログ エントリを探します。これ

により、シンクホール IP アドレスへのトラフィックがファイアウォール ゾーンを通過していることを確認できます。

ログを検索またはフィルタリングして、宛先が *10.15.0.20* のログのみ表示することもできます。それには、*[宛先]* 列で *IP* アドレス（*10.15.0.20*）をクリックします。すると、検索フィールドにフィルタ（*addr.dst in 10.15.0.20*）が追加されます。検索フィールドの右側の *Apply Filter*（フィルタの適用）アイコンをクリックして、フィルタを適用します。

STEP 5 | DNS シンクホールの設定が適切であることを検証します。

悪意のあるアプリケーションがホームを呼び出そうとする際に感染したクライアント ホストが実行するアクションを模擬的に行います。

1. ファイアウォールの現行のアンチウイルス シグネチャ データベースに含まれている悪意のあるドメインを探し、シンクホールのテストを行います。
   1. **Device (デバイス)** > **Dynamic (動的) Updates (アップデート)** を選択し、**Antivirus** セクションで現在インストールしているアンチウイルス データベースの **Release Notes (リリースノート)** リンクをクリックします。追加分のシグネチャ更新をリストアップしたアンチウイルス リリース ノートは、Palo Alto Networksサポート サイトのDynamic Update [動的更新]以下にもあります。
   2. リリース ノートの 2 列目で、特定のドメイン拡張子（たとえば、.com、.edu、.net など）を持つ行項目を探します。左側の列にドメイン名が表示されます。たとえば、アンチウイルス リリース 1117-1560 には、左側の列が "tbsbana" で、右側の列が "net" になっている項目が含まれます。

      以下に、リリース ノートのこの行項目の内容を示します。

      ```
      conficker:tbsbana 1 variants: net
      ```
2. クライアント ホストでコマンド プロンプトを開きます。
3. 既知の悪意あるドメインとして特定した URL に対して、NSLOOKUP を実行します。

   以下の例では、**track.bidtrk.com** という URL を使用しています。

   ```
   C:\>nslookup track.bidtrk.com Server: my-local-
   dns.local Address:10.0.0.222 Non-authoritative
    answer:Name: track.bidtrk.com.org Addresses:
    fd97:3dec:4d27:e37c:5:5:5:510.15.0.20
   ```

   悪意あるドメインに対する NSLOOKUP が、設定したシンクホール IP アドレス（10.15.0.20）を使用して偽造されている点に注目してください。このドメインは悪意ある DNS シグネチャと一致したため、シンクホール アクションが実行されています。
4. **Monitor (監視)** > **Logs (ログ)** > **Threat (脅威)** の順に選択して、対応する脅威ログ エントリを探し、NSLOOKUP 要求に対して正しいアクションが実行されたことを確認します。
5. **track.bidtrk.com** に対して Ping を実行します。シンクホール アドレスに対するネットワーク トラフィックが生成されます。

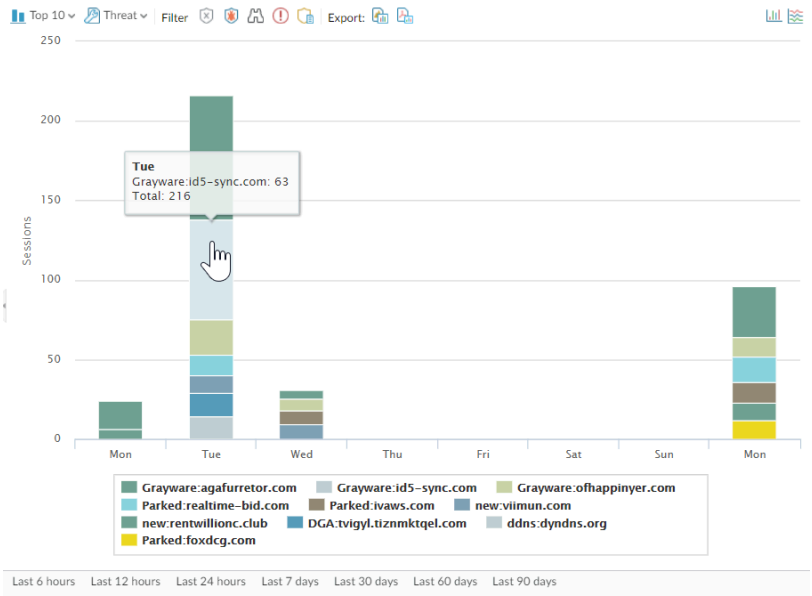
悪意のあるドメインへの接続を試みた感染ホストを確認

DNS シンクホールを設定して、悪意あるドメインへのトラフィックがシンクホール アドレスに向けて送信されることを確認したら、シンクホール アドレスへのトラフィックを定期的にモニターして、感染ホストを突き止め、脅威を排除する必要があります。

アプリケーション スコープを使用して感染したクライアント ホストを特定します。

1. **Monitor (監視)** > **App Scope (アプリケーション スコープ)** を選択し、さらに **Threat Monitor (脅威モニター)** を選択します。
2. 表示ページの上部にある **[スパイウェアの表示]** ボタンをクリックします。
3. 時間範囲を選択します。

   以下のスクリーンショットでは、疑わしい 3 つの DNS クエリのインスタンスが表示されています。これらは、テスト クライアント ホストが既知の悪意あるドメインに対して NSLOOKUP を実行したときに生成されたクエリです。グラフをクリックして、イベントの詳細情報を表示します。



シンクホール IP アドレス（この例では 10.15.0.20）に対してトラフィックを送信したすべてのクライアント ホストを明示するカスタム レポートを設定します。

SNMP マネージャ、*Syslog* サーバー、および（または）*Panorama* に転送して、これらのイベントのアラートを有効にしてください。

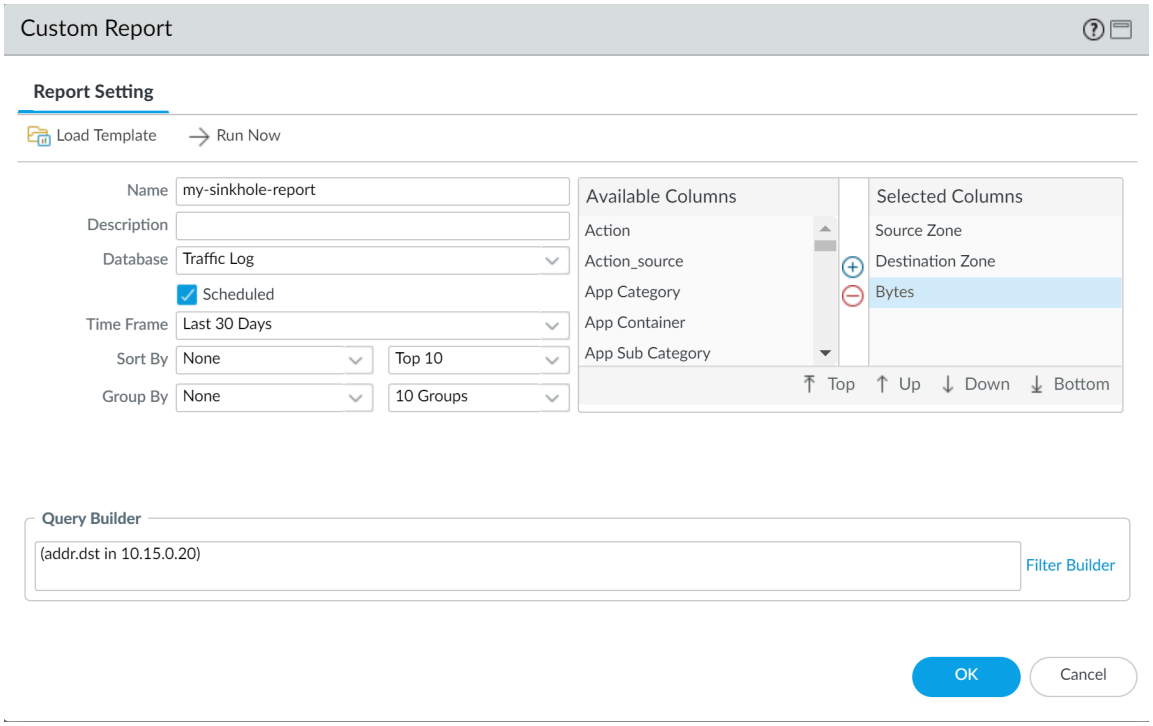
この例では、感染したクライアント ホストが、Palo Alto Networks DNS シグネチャ データベースに登録されている既知の悪意あるドメインに対して NSLOOKUP を実行します。すると、ローカルの DNS サーバーにクエリが送信され、その要求がファイアウォール経由で外部の DNS サーバーに転送されます。アンチスパイウェア プロファイルが設定されたファイアウォール セキュリティ ポリシーによって、このクエリが DNS シグネチャ データベースと照合され、シンクホール アドレス 10.15.0.20 および fd97:3dec:4d27:e37c:5:5:5:5 を使用して応答が偽造されます。クライアントがセッションを開始すると、アクティビティが送信元ホ

ストおよび宛先アドレスと一緒にトラフィック ログに記録されます。この時点で、宛先アドレスは偽造されたシンクホール アドレスに置き換わっています。

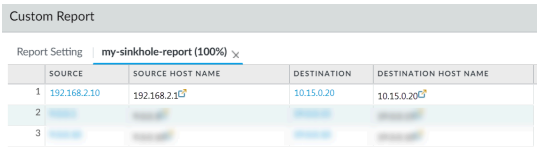
ファイアウォール上のトラフィック ログを確認することによって、シンクホール アドレスにトラフィックを送信しているクライアント ホストをすべて特定できます。この例では、送信元アドレス 192.168.2.10 から悪意ある DNS クエリが送信されたことがログから分かります。これで、感染ホストを見つけて排除できます。DNS シンクホール オプションがなければ、管理者には、クエリを実行したシステムとしてローカルの DNS サーバーしか見えず、感染したクライアント ホストは分かりません。仮にシンクホール アクションを使用して脅威ログに対するレポートを実行したとしたら、ログには、感染ホストではなく、ローカルの DNS サーバーが表示されます。

1. **Monitor (監視)** > **Manage Custom Reports (**カスタム レポートの管理**)**の順に選択します。
2. **Add**（追加） をクリックして、レポートに **Name**（名前） をつけます。
3. 以下のとおり、シンクホール アドレスへのトラフィックをキャプチャするカスタム レポートを定義します。
   - データベース – **[**トラフィック ログ**]** を選択します。
   - スケジュール設定 – **[**スケジュール設定**]** をオンにすると、レポートが毎晩実行されます。
   - 期間 – 30 日
   - 選択した列 – **[**送信元アドレス**]** または **[**送信元ユーザー**]**（User-ID を設定している場合）、および **[**宛先アドレス**]** を選択します。前者はレポート内の感染したクライアント ホストを識別します。後者はシンクホール アドレスです。
   - 画面下部のセクションで、シンクホール アドレス（この例では、10.15.0.20）へのトラフィックに対するカスタム クエリを作成します。**Query Builder**（クエリ ビルダー）ウィンドウに宛先アドレスを入力するか（**addr.dst in 10.15.0.20**）、各列で次の項目を選択して、**Add**（追加）をクリックします。結合子 = and、属性 = 宛先アド

レス、演算子 = in、値 = 10.15.0.20。**Add**（追加） をクリックしてクエリを追加します。



4. [今すぐ実行] をクリックしてレポートを生成します。シンクホール アドレスに対してトラフィックを送信したすべてのクライアント ホストがレポートに表示されます。これらは、感染している可能性が極めて高いホストです。これで、ホストを突き止めて、スパイウェアに感染していないかチェックできます。



5. スケジュール設定された実行済みレポートを表示するには、**Monitor (監視)** > **Reports (レポート)** を選択します。

データのフィルタリング

データ フィルタリング プロファイルを使用し、ネットワークの外に出るセンシティブな企業の機密情報を保護します。定義済みのパターン、組込設定、およびカスタマイズ可能なオプションを使用すると、特定のファイルプロパティ (文書タイトルや作成者など)、クレジットカード番号、各国の規制情報 (社会保障番号など)、サードパーティのデータ損失防止 (DLP) ラベルを含むファイルを簡単に保護できます。

- 定義済みデータパターン—クレジットカード番号を含む一般的なパターンを簡単にフィルタリングできます。事前定義されたデータフィルタリングパターンは、社会保障番号 (米国)、INSEE 識別番号 (フランス)、ニュージーランド内国歳入局識別番号など、世界各国からの特定の (規制) 情報も識別します。事前定義されたデータフィルタリングパターンの多くは、HIPAA、GDPR、グラム リーチ ブライリー法などの規格へ準拠することができます。
- **Azure Information Protection** および **Titus** データ分類の組み込みサポート—定義済みのファイルプロパティを使用すると、Azure Information Protection および Titus ラベルに基づいてコンテンツをフィルタ処理できます。Azure Information Protection ラベルはメタデータに格納されているため、ファイアウォールでフィルタリングする Azure Information Protect ラベルの GUID を把握していることを確認してください。
- データ損失防止 **(DLP)** ソリューション用のカスタムデータパターン—機密性の高いコンテンツを示すためにファイルプロパティを設定するサードパーティのエンドポイント DLP ソリューションを使用している場合は、カスタムデータパターンを作成して DLP ソリューションによってタグ付けされたファイルプロパティと値を識別します。データフィルタリングプロファイルはそのパターンに基づいて検出します。

データ フィルタリング プロファイルの作成

Data Filtering (データフィルタリング) プロファイルは、機密情報がネットワークを離れることがないようにすることができます。

まず、ファイアウォールでフィルタリングする情報の種類とフィールドを指定するデータパターンを作成します。次に、そのパターンをデータフィルタリングプロファイルに添付します。このプロファイルは、ファイアウォールがフィルタリングするコンテンツの適用方法を指定します。データフィルタリングプロファイルをセキュリティポリシールールに追加して、ルールに一致するトラフィックのフィルタリングを開始します。

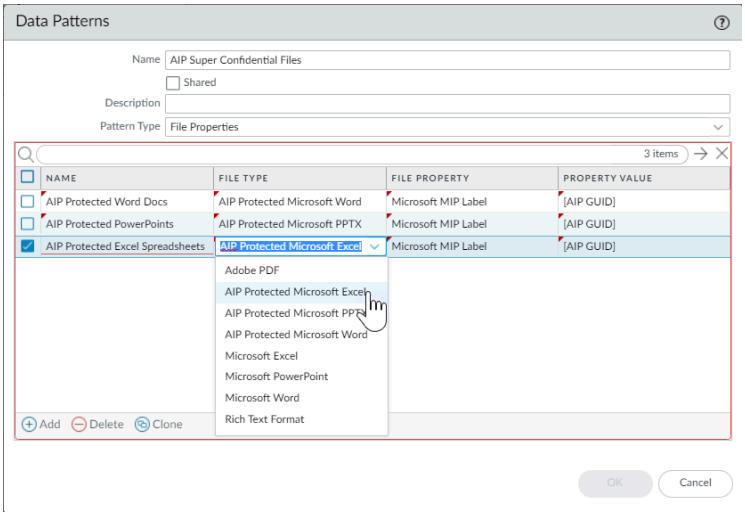
STEP 1 | フィルタリングしたい情報を検知する新しいデータパターン オブジェクトを定義します。

1. **Objects (**オブジェクト**)** > **Custom Objects (**カスタム オブジェクト**)** > **Data Patterns (**データ パターン**)** を選択して新しいオブジェクトを **Add (**追加**)** します。
2. 新しいオブジェクトに分かりやすい **Name (**名前**)** をつけます。
3. （任意）以下に対してデータ パターンを公開する場合は、**Shared (**共有**)** を選択します。
   - マルチ **vsys** ファイアウォール上のすべての仮想システム（**vsys**）—クリア（無効化）すると、**Objects (**オブジェクト**)** タブで選択された仮想システムでのみデータパターンを利用できます。
   - **Panorama** 上のすべてのデバイスグループ—クリア（無効化）すると、**Objects (**オブジェクト**)** タブで選択されたデバイスグループでのみデータパターンを利用できます。
4. （任意—Panorama のみ）管理者が、このオブジェクトを継承するデバイス グループのこのデータ パターン オブジェクトの設定をオーバーライドすることを防ぐには、**Disable override (**オーバーライドの無効化**)** を選択します。デフォルトでこのオプションはオフになっており、管理者は、このオブジェクトを継承するデバイス グループの設定をオーバーライドできます。
5. （任意—Panorama のみ）フィルタによってブロックされたデータを自動的に収集するア場合は、**Data Capture (**データ キャプチャ**)** を選択します。

   *Settings (*設定*)* ページの *Manage Data Protection (*データ保護の管理*)* にキャプチャしたデータを表示するためのパスワードを指定します（***Device (***デバイス***) > Setup (***セットアップ***) > Content-ID > Manage Data Protection (***データ保護の管理***)***）。
6. **Pattern Type (**パターン タイプ**)** を次のいずれかに設定します。
   - **Predefined Pattern (**定義済みパターン**)**—クレジットカード、社会保障番号、および HIPAA、GDPR、グラム・リーチ・ブライリー法などのいくつかのコンプライアンス基準での個人情報をフィルタリングします。
   - **Regular Expression (**正規表現**)**—カスタム データパターン用のフィルタです。
   - **File Properties (**ファイル プロパティ**)**—ファイル プロパティおよび関連する値に基づいてフィルタリングを行います。
7. データパターン オブジェクトに新しいルールを **Add (**追加**)** します。
8. このオブジェクト用に選択した **Pattern Type (**パターン タイプ**)** に従ってデータパターンを指定します。
   - 事前定義— **Name (**名前**)** を選択し、フィルタリングする事前定義データパターンを選択します。
   - 正規表現—分かりやすい **Name (**名前**)** を指定し、スキャンしたい単一の **File Type (**ファイル タイプ**)**（または複数のタイプ）を選択し、ファイアウォールに検知させたい具体的な **Data Pattern (**データ パターン**)** を入力します。
   - **File Properties (**ファイル プロパティ**)**—分かりやすい **Name (**名前**)** を指定し、スキャンしたい **File Type (**ファイル タイプ**)** および **File Property (**ファイル プロパティ**)** を

選択し、ファイアウォールに検知させたい具体的な **Property Value (**プロパティの値**)** を入力します。

- **Titus** 分類文書をフィルタリングするには：非 AIP 保護ファイルタイプのいずれかを選択し、**File Property (**ファイルプロパティ**)** を TITUS GUID に設定します。**Property Value (**プロパティ値**)** として Titus ラベル GUID を入力します。
- **Azure Information Protection** ラベル付きドキュメントの場合：リッチテキスト形式以外の任意の **File Type (**ファイルタイプ**)** を選択します。選択したファイルの種類に対して、**File Property (**ファイルプロパティ**)** を Microsoft MIP ラベルに設定し、**Property Value (**プロパティ値**)** として、 Azure Informatin Protect ラベル GUID を入力します。



9. **OK** をクリックしてデータパターンを保存します。

STEP 2 | データパターン オブジェクトをデータ フィルタリング プロファイルに追加します。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **Data Filtering (データ フィルタリング)** を選択し、データ フィルタリング プロファイルを **Add (追加)** あるいは変更します。
2. 新しいプロファイルに分かりやすい **Name (名前)** をつけます。
3. 新しいプロファイル ルールを **Add (追加)** し、ステップで作成したデータパターンを選択します。
4. そのデータパターンに基づいてフィルタリングしたい **Applications (アプリケーション)**、**File Types (ファイル タイプ)**、およびトラフィックの **Direction (方向)**（アップロードあるいはダウンロード）を指定します。

   選択するファイル タイプは、以前にデータパターン用に定義したファイル タイプと同じであるか、データパターンのファイル タイプを含むファイル タイプでなければなりません。例えば、データパターン オブジェクトおよびデータ フィルタリング プロファイルの両方を定義し、すべての *Microsoft Office* ドキュメントをスキャンすることができます。あるいは、データ フィルタリング プロファイルはあらゆる *Microsoft Office* ドキュメントをスキャンできますが、データパターン オブジェクトを *Microsoft PowerPoint* プレゼンテーションにのみマッチさせるように定義します。

   データパターン オブジェクトがデータ フィルタリング プロファイルにアタッチされており、設定したファイルの種類が 2 つの間で矛盾する場合、プロファイルはデータパターン オブジェクトにマッチしたドキュメントを正しくフィルタリングすることができません。
5. アラートをトリガーするまでのファイルのデータ パターン検出回数を指定するには、**Alert Threshold (アラートしきい値)** を設定します。
6. データ パターンがこの回数以上出現するファイルをブロックするには、**Block Threshold (ブロックしきい値)** を設定します。
7. このルールにマッチするファイルに対して記録する **Log Severity (ログの重大度)** を設定します。
8. **OK** をクリックして、データ フィルタリング プロファイルを保存します。

STEP 3 | データ フィルタリング設定をトラフィックに適用します。

1. **Policies (ポリシー)** > **Security (セキュリティ)**を選択し、セキュリティポリシールールを**Add**（追加）または変更します。
2. **Actions** （アクション） を選択して Profile Type (プロファイル タイプ) を **Profiles (プロファイル)** に設定します。
3. ステップ 2 で作成したデータ フィルタリング プロファイルをセキュリティポリシールールに適用します。
4. **OK** をクリックします。

STEP 4 | （推奨）ファイアウォールが終了させたセッションをウェブ ブラウザが再開するのを阻止します。

このオプションにより、ファイアウォールが検知後にセンシティブなファイルをドロップすると、ウェブ ブラウザがそのファイルを取得しようとしてセッションを再開することができなくなります。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Content-ID** を選択し、コンテンツ ID 設定を編集します。
2. **Allow HTTP partial response (HTTP** 部分レスポンスを許可)をクリアします。
3. **OK** をクリックします。

STEP 5 | ファイアウォールがフィルタリングしているファイルを監視します。

データ フィルタリング設定に基づいてファイアウォールが検知・ブロックを行ったファイルを表示するには、**Monitor (監視)** > **Data Filtering (データ フィルタリング)** を選択します。

事前定義済みのデータ フィルタリング パターン

HIPAA や GDPR、Gramm-Leach-Bliley Act などの規格に準拠するために、ファイアウォールには定義済みデータパターンが用意されています。これらのパターンを使用して、クレジットカードや社会保障番号などの一般的な種類の機密情報がネットワークから流出するのを防ぐことができます。

定義済みのデータパターンは、**Object (オブジェクト) > Custom Objects (カスタムオブジェクト) > Data Patterns (データパターン)** を選択し、新しいオブジェクトの **Add (追加)** をクリックして見つけることができます。次に、**Pattern Type (パターンタイプ)** を **Predefined Pattern (定義済みパターン)** に設定し、データパターンオブジェクトに新しいルールを **Add (追加)** します。**Name (名前)** の下に表示されるリストからデータパターンを選択します。

保護する情報の種類が事前定義パターンのリストに含まれていない場合、正規表現を使用してカスタムパターンを作成することができます。

以下は利用可能なデータパターンのリストです：

パターン	説明
クレジットカード番号	16 桁のクレジットカード番号
社会保障番号	ダッシュ付きの 9 桁の社会保障番号
社会保障番号 (ダッシュ区切りなし)	ダッシュなしの 9 桁の社会保障番号
ABA ルーティング番号	米国銀行協会ルーティング番号
AHV 識別番号	Swiss Alters und Hinterlassenenversicherungsnummer

パターン	説明
Codice Fiscale 識別番号	イタリア財政税コードカード識別番号
企業番号識別番号	日本国税庁法人番号
CUSIP 識別番号	統一セキュリティ識別手続委員会識別番号
DEA Registration Number	アメリカ米国薬物取締局登録番号
DNI 識別番号	Spanish Documento nacional de identidad Identification Number number
香港識別番号	香港居住者識別番号
INSEE 識別番号	フランス国立統計経済研究所識別番号
IRD 識別番号	ニュージーランド内国歳入局識別番号
MyKad 識別番号	マレーシア MyKad ID カード識別番号
マイナンバー識別番号	日本の社会保障と税番号システムの識別番号
NHI 識別番号	ニュージーランド国民保険検索番号
NIF 識別番号	スペイン納税者番号
NIN 識別番号	台湾の身分証明書番号
NRIC 識別番号	シンガポール国民登録 ID カード識別番号
納税者番号	インド国民向け納税者番号
PRC 識別番号	中華民国居住者識別番号
PRN 識別番号	大韓民国居住者登録番号
大韓民国住民登録	大韓民国居住者登録番号

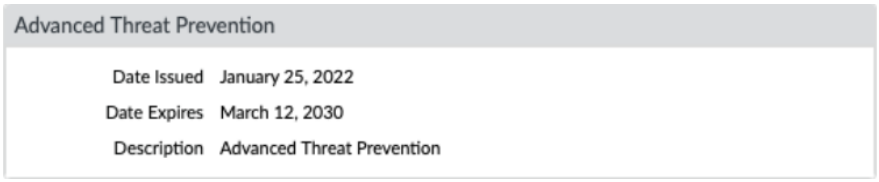
インラインクラウド解析の設定

Advanced Threat Preventionを有効にするには、インラインクラウド解析の設定で設定したスパイウェア対策プロファイルをセキュリティポリシールールに添付します。(基本的なセキュリティ ポリシーのセットアップ を参照)。

STEP 1 | PAN-OS Web インターフェイスにログインします。

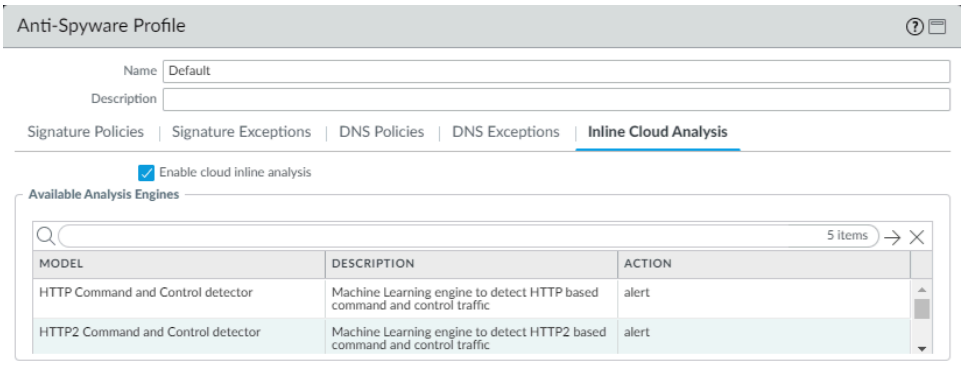
STEP 2 | インラインクラウド分析を利用するには、Advanced Threat Preventionのサブスクリプションが有効である必要があります。

現在アクティブなライセンスがあるサブスクリプションを確認するには、**Device** > **Licenses** を選択し、適切なライセンスが使用可能で有効期限が切れていないことを確認します。



STEP 3 | 新しい Anti-Spyware Security プロファイルを更新または作成して、インラインクラウド解析を有効にします。

1. 既存の **Anti-Spyware Profile** または **Add** を新しいもの (**Objects** > **Security Profiles** > **Anti-Spyware**) を選択します。
2. Anti-Spyware プロファイルを選択し、**Inline Cloud Analysis** および インラインクラウド解析を有効にするに進みます。



3. 対応する分析エンジンを使用して脅威が検出されたときに取る **Action** を指定します。以下のオプションを使用できます。

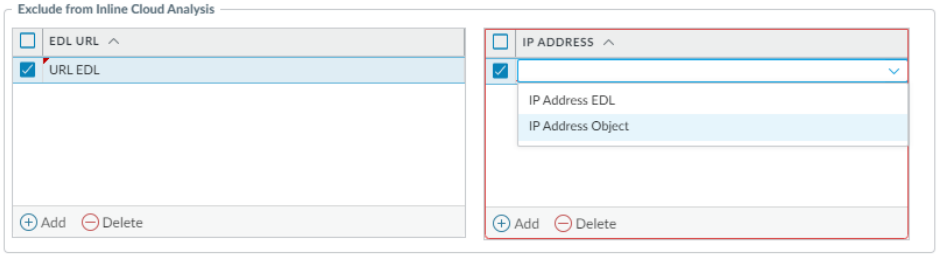
   各分析エンジンのデフォルトのアクションは ***alert*** ですが、*Palo Alto Networks* では、セキュリティ体制を最適にするために、すべてのアクションを ***Reset-Both*** に設定することをお勧めします。

   - **Allow** - 要求は許可され、ログ エントリは生成されません。
   - **Alert** - 要求が許可され、Threat ログ エントリが生成されます。
   - **Drop** - 要求を削除します。リセットアクションはホスト/アプリケーションに送信されません。
   - **Reset-Client** - クライアント側の接続をリセットします。
   - **Reset-Server** - サーバー側の接続をリセットします。
   - **Reset-Both** - クライアント側とサーバー側の両方で接続をリセットします。
4. **OK** をクリックして Anti-Spyware Profile 構成ダイアログを終了し、**Commit** をクリックして変更を行います。

STEP 4 | (Optional)Inline Cloud Analysis で誤検知が発生した場合は、Anti-Spyware プロファイルに URL や IP アドレスの例外を追加します。例外を追加するには、外部動的リスト (URL または IP アドレス一覧の種類) または **Addresses** オブジェクトを指定します。

1. **External Dynamic Lists** または [IP] **Addresses** オブジェクト例外を追加します。
2. **Objects > Security Profiles > Anti-Spyware** を選択します。
3. 特定の URL や IP アドレスを除外する Anti-Spyware プロファイルを選択し、**Inline Cloud Analysis** を選択します。
4. **Add** を追加する例外の種類に応じて、**EDL URL** または **IP アドレス** を選択し、既存の URL または IP アドレスの外部動的リストを選択します。使用可能なものがない場合は、

新しい external dynamic list を作成します。IP アドレスの例外については、オプションで **Addresses** オブジェクト リストを選択できます。



5. **OK** をクリックしてスパイウェア対策プロファイルを保存し、**Commit** に変更を保存します。

STEP 5 | Advanced Threat Prevention インライン クラウド分析サービスへの認証に使用される更新された firewall デバイス証明書をインストールします。インラインクラウド解析が有効なすべてのファイアウォールについて繰り返します。

STEP 6 | (Optional)インラインクラウド分析サービス要求を処理するために firewall によって使用される Cloud Content Fully Qualified Domain Name (FQDN) を設定します。既定の FQDN は hawkeye.services-edge.paloaltonetworks.com に接続し、最も近い cloud サービス サーバーに解決されます。自動サーバー選択をオーバーライドするには、データの常駐性とパフォーマンスの要件に最も適した地域の cloud コンテンツサーバーを指定します。

Cloud Content FQDN はグローバルに使用されるリソースであり、この接続に依存する他のサービスがトラフィックペイロードを送信する方法に影響します。

firewall がお住まいのリージョンに対して正しい Content Cloud FQDN (**Device** > **Setup** > **Content-ID** > **Content Cloud Setting**) を使用していることを確認し、必要に応じて FQDN を変更します。

- US—**us.hawkeye.services-edge.paloaltonetworks.com**
- EU—**eu.hawkeye.services-edge.paloaltonetworks.com**
- UK—**uk.hawkeye.services-edge.paloaltonetworks.com**

  英国を拠点とするクラウド コンテンツ *FQDN* は、*EU (eu.hawkeye.services-edge.paloaltonetworks.com)* にあるバックエンド サービスに接続することにより、*Advanced Threat Prevention* インライン *c1loud* 解析サービス サポートを提供します。
- APAC—**apac.hawkeye.services-edge.paloaltonetworks.com**

STEP 7 | (Optional)Advanced Threat Prevention cloud サービスへの firewall 接続の状態を確認します。

接続ステータスを表示するには、ファイアウォール上で次のCLIコマンドを実行します。

```
show ctd-agent status security-client
```

以下に例を示します。

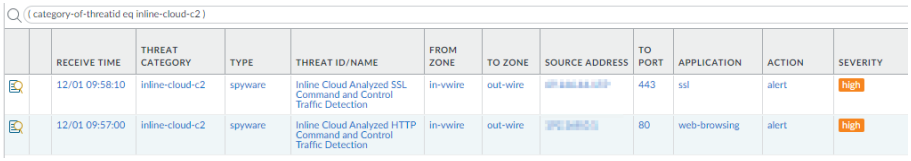
```
show ctd-agent status security-client ...Security Client AceMlc2(1)
 Current cloud server: hawkeye.services-edge.paloaltonetworks.com
 Cloud connection: connected ...
```

*CLI*出力は簡潔にするために短縮されています。

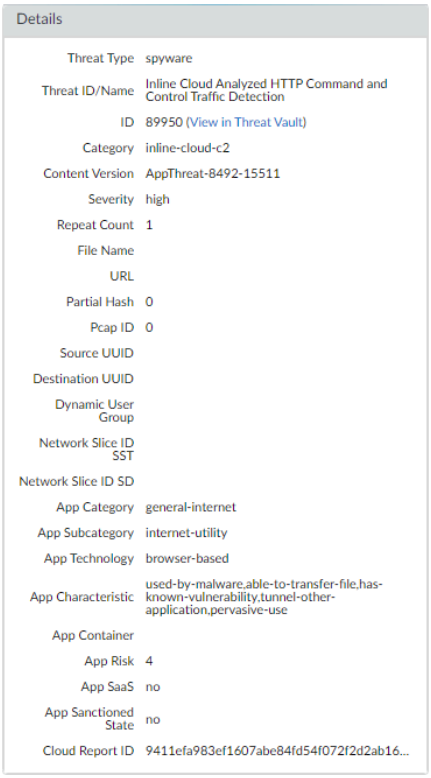
Advanced Threat Prevention クラウドサービスに接続できない場合、次のドメインがブロックされていないことを確認します。: hawkeye.services-edge.paloaltonetworks.com。

STEP 8 | (Optional)インラインクラウド分析を使用して検出されたC2脅威について、firewallのアクティビティを監視します。

1. **Monitor** > **Logs** > **Threat** を選択し、`( category-of-threatid eq inline-cloud-c2 )` でフィルター処理すると、Advanced Threat Prevention のインライン クラウド分析メカニズムを使用して分析されたログが表示されます。



2. ログ エントリを選択して、検出された C2 脅威の詳細を表示します。
3. 脅威 **Category** は、詳細ログ ビューの **Details** ペインの下に表示されます。インラインクラウド解析を用いて検知されたC2脅威は、脅威カテゴリがinline-cloud-c2となっています。



WildFire インライン ML

Antivirus プロファイルに存在する WildFire インライン ML オプションを使用すると、firewall データプレーンは、PE (ポータブル実行可能ファイル)、ELF (実行可能およびリンク形式)、MS Office ファイル、および PowerShell スクリプトとシェルスクリプトに機械学習をリアルタイムで適用できます。このアンチウィルス保護のレイヤーは、WildFire ベースのシグネチャを補完し、シグネチャがまだ存在しないファイルのカバー範囲を拡大します。各インライン ML モデルは、ファイルの高確率分類を定式化するためのデコーダ フィールドとパターンを含む、ファイルの詳細を評価することにより、特定のタイプの悪意のあるファイルを動的に検出します。この保護により、現在不明なものだけでなく、Palo Alto Networks が悪性であると識別済みの特性に一致する将来的な脅威の亜種にも拡張されます。脅威の状況における最新の変更に対応するために、インライン ML モデルがコンテンツ リリースを介して追加または更新されます。WildFire インライン ML を有効化できる前に、アクティブな WildFire サブスクリプションを保有している必要があります。

インライン ML ベースの保護を有効にして、URL フィルタリング設定の一部として、悪意のある URL をリアルタイムで検出します。詳細については、以下を参照してくださローカルインライン分類

***WildFire* インライン *ML* は、*VM-50* または *VM50L* バーチャル アプライアンスでサポートされていません。**

WildFire インライン ML の設定

WildFire インライン ML 設定を有効化するには、セキュリティ ポリシー ルールのためにインライン ML 設定で構成したアンチウイルス プロファイルをアタッチします (アンチウィルス、アンチスパイウェア、脆弱性防御のセットアップを参照)。

***WildFire* インライン *ML* は現在、*VM-50* または *VM50L* バーチャル アプライアンスでサポートされていません。**

STEP 1 | WildFire インライン ML を利用するには、Windows 実行可能ファイルを分析するためのアクティブな WildFireサブスクリプションがなければなりません。

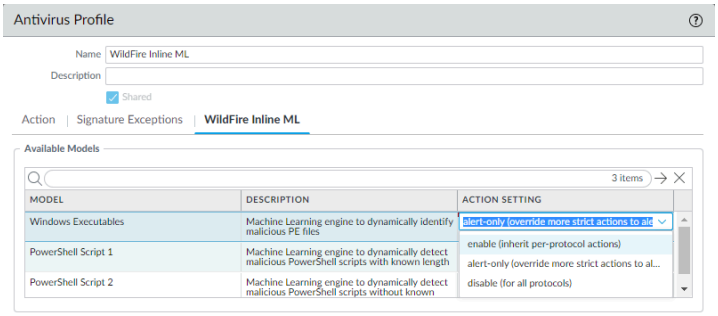
WildFireサブスクリプションがあることを確認します。現在ライセンスを持っているサブスクリプションを確認するには、**Device**（デバイス） > **Licenses(ライセンス)** を選択し、適切なライセンスが表示され、有効期限が切れていないことを確認します。

WildFire License

Date Issued	July 25, 2019
Date Expires	July 25, 2020
Description	WildFire signature feed, integrated WildFire logs, WildFire API

STEP 2 | リアルタイム WildFire インライン ML モデルを使用するには、アンチウイルス セキュリティ プロファイルを新規作成するか、既存のものを更新します。

1. 既存の **Antivirus Profile (**アンチウイルス プロファイル**)** を選択するか、アンチウイルス プロファイルを新規作成し (**Objects (**オブジェクト**) > Security Profiles (**セキュリティ プロファイル**) > Antivirus (**アンチウイルス**)**を選択し、新規プロファイルを**Add (**追加**)** します。
2. アンチウイルス プロファイルを設定します。
3. **WildFire Inline ML (WildFire** インライン **ML)** タブを選択し、各 WildFire インライン ML モデルの **Action Setting (**アクション設定**)** を適用します。この操作は、モデルベースごとの各プロトコル用に設定された WildFire インライン ML アクション設定を施行します。次の分類エンジンが使用可能です。
   - Windows実行可能ファイル
   - PowerShell スクリプト 1
   - PowerShell スクリプト 2
   - Executable Linked Format (PAN-OS コンテンツ リリース 8367 以降のインストールで利用可能)
   - MSOffice (PAN-OS コンテンツ リリース 8434 以降のインストールで利用可能)
   - Shell Scripts (PAN-OS コンテンツリリース 8543 以降のインストールで利用可能)



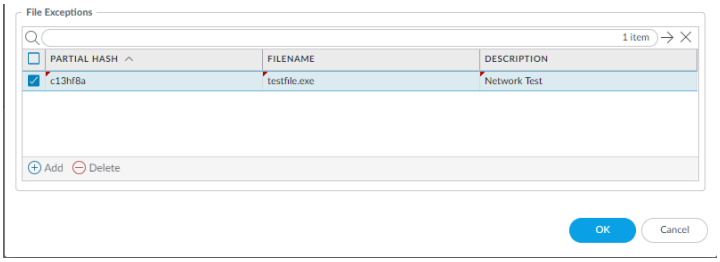
   - 有効にする**(**プロトコルごとのアクションを継承する**)** —WildFire は、**Action (**アクション**)** タブのデコーダ セクションの WildFire インライン ML アクション列内の選択内容に従ってトラフィックを検査します。
   - アラートのみ **(**より厳密なアクションをアラートにオーバーライドします**)**—WildFire は、**Action (**アクション**)** タブのデコーダセクションの WildFire インライン ML アクション列内の選択内容に従ってトラフィックを検査し、アラート (ドロップ、クライアントのリセット、サーバーのリセット、両方のリセット) アラートよりも高い重大度のアクションを上書きします。これにより、アラートを生成して脅威ログに保存しながら、トラフィックを通過させることができます。
   - 無効化**(**すべてのプロトコル用**)** —WildFire は、ポリシー アクションなしでトラフィックを通過させます。
4. **OK** をクリックして、アンチウイルス プロファイル設定ウィンドウを終了し、新しい設定を **Commit (**コミット**)** します。

STEP 3 | (オプション) 誤検知が発生した場合は、アンチウイルス セキュリティ プロファイルにファイル例外を追加します。これは通常、分析のために WildFire にファイルを転送していない

ユーザーに対して行われます。ファイルの例外の詳細を例外リストに直接追加するか、脅威ログからファイルを指定することができます。

WildFire のインライン *ML* を使用して分析されたファイルタイプを転送するように *WildFire* 分析セキュリティ プロファイルが設定されている場合、誤検知は受信時に自動的に修正されます。*WildFire*分析によって良性に分類されたファイルに対する*ml*-ウイルスアラートが引き続き表示される場合は、*Palo Alto Networks*のサポートにお問い合わせください。

- ファイルの例外を例外リストに直接追加します。
  1. 「**Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > Antivirus(アンチウイルス)**」を選択します。
  2. 特定のファイルを除外したい アンチウイルス プロファイルを選択してから、 **WildFire Inline ML (WildFire** インライン **ML)** を選択します。
  3. 施行から除外するファイルのハッシュ、ファイル名、および説明を追加します。



  4. **OK** をクリックしてアンチウイルス プロファイルを保存し、更新を **Commit (コミット)** します。
- 脅威ログ エントリからファイル例外を追加します。
  1. **Monitor (モニター) > Logs (ログ) > Threat (脅威)** を選択し、**ml-virus** 脅威タイプのログをフィルタリングします。ファイル例外を作成するファイルの脅威ログを選択します。
  2. **Detailed Log View (詳細ログ ビュー)** に移動し、**Details (詳細)** ペインにスクロールダウンしてから、**Create Exception (例外を作成)** を選択します。

  3. ファイル例外を追加するには、**Description (説明)** を追加して **OK** をクリックします。
  4. 新しいファイル例外は、**Objects(オブジェクト) > Security Profiles(セキュリティ プロファイル) > Antivirus(アンチウイルス) > WildFire Inline ML(WildFire** インライン **ML)** の **File Exceptions (ファイル例外)** リストにあります。

STEP 4 | （オプション）ご利用のファイアウォールの、インライン ML クラウド サービスへの接続ステータスを確認します。

接続ステータスを表示するには、ファイアウォール上で次のCLIコマンドを実行します。

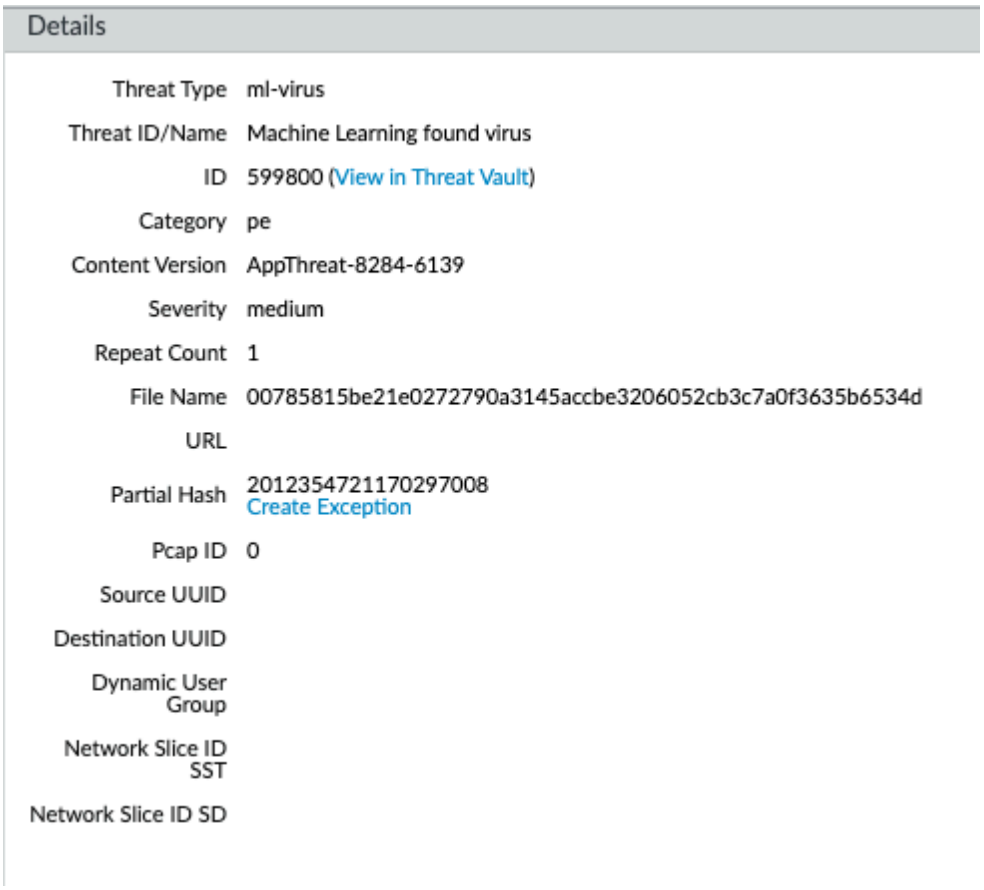
```
show mlav cloud-status
```

以下に例を示します。

```
show mlav cloud-status MLAV cloud Current cloud server:
 ml.service.paloaltonetworks.com Cloud connection: connected
```

インライン ML クラウド サービスに接続できない場合は、以下のドメインがブロックされていないことを確認してください: ml.service.paloaltonetworks.com.

WildFire インライン ML を使用して検出されたファイルに関する情報を見るには、脅威ログを確認します (**Monitor (モニター) > Logs (ログ) > Threat (脅威)** を選択し、リストからログ タイプを選択します)。WildFire インライン ML を使用して分析されたファイルには、脅威の種類 **ml-virus** というラベルが付けられます:



ファイル ブロッキングのセットアップ

ファイル ブロッキング プロファイルでは、ブロックまたはモニターする特定のファイル タイプを識別できます。ほとんどのトラフィックの場合 (内部ネットワークのトラフィックを含む)、脅威をもたらす既知のファイルや、アップロード/ダウンロードするメリットが無いファイルはブロックします。現在のところ、これにはバッチファイル、DLL、Javaクラスファイル、ヘルプファイル、Windowsショートカット（.lnk）、BitTorrentファイルが含まれます。さらに、ドライブバイダウンロード攻撃を防ぐためには、実行ファイルやアーカイブファイル (.zip や .rar) のダウンロード/アップロードを許可しつつも、ファイルを転送していることをユーザーが確実に分かるようにし、それまでは把握していなかった何かをブラウザがダウンロードしようとしていることに気付くようにする必要があります。一般的なウェブ ブラウジングを許可するポリシーの場合、ユーザーが知らないうちに悪意のあるファイルをダウンロードする危険性が高いため、ファイルのブロッキングをより厳重に行うべきです。このタイプのトラフィックでは、PE ファイルもブロックする厳しいファイルブロッキングプロファイルを使用します。

ファイル ブロッキングをセキュリティ ポリシールールに適用するには、独自のファイルブロッキングプロファイルを定義する方法と、以下のどちらかの事前定義プロファイルを選択する方法があります。コンテンツリリースバージョン 653 以降で使用可能な定義済みプロファイルをコピーならびに編集を行ってから、ファイルブロッキングプロファイルの安全な移行手順に従って、ベストプラクティスのファイルブロック設定に移行する際にアプリケーションの可用性を維持できます。

- **basic file blocking (**基本的なファイル ブロッキング**)**—比較的センシティブでないアプリケーションをトラフィックが出入りするのを許可するセキュリティポリシールールにこのプロファイルをアタッチし、頻繁にマルウェア攻撃キャンペーンに含まれる、あるいはアップロード/ダウンロードする意味がないファイルをブロックします。このプロファイルは PE ファイル（.scr、.cpl、.dll、.ocx、.pif、.exe）、Java ファイル（.class、.jar）、ヘルプファイル（.chm、.hlp）および .vbe、.hta、.wsf、.torrent、.7z、.rar、.bat などの悪意のある可能性があるファイル タイプをアップロードおよびダウンロードするのをブロックします。さらにこれは、ユーザーが encrypted-rar や encrypted-zip ファイルのダウンロードを試みた際にユーザーに確認を求めます。このルールは、他のすべてのファイル タイプに対してアラートを通知することで、ネットワークを出入りするすべてのファイル タイプに完全な可視性をもたらします。
- **strict file blocking (**厳格なファイル ブロッキング**)**—極めて重要なアプリケーションへのアクセスを許可するセキュリティポリシールールでは、この厳格なプロファイルを使用します。このプロファイルは他のプロファイルと同じファイル タイプをブロックするだけでなく、さらに flash、.tar、multi-level encoding、.cab、.msi、encrypted-rar、および encrypted-zip ファイルもブロックします。

これらの事前定義済みのプロファイルは、ネットワークの最適なセキュリティを実現できるように設計されています。ただし、これらのデフォルト プロファイルによってブロックされているアプリケーションを必要とする、ビジネスに不可欠なアプリケーションがある場合、必要に応じてプロファイルをコピーして修正することができます。必ず、リスクのあるファイル タイプをアップロードあるいはダウンロードする必要があるユーザーに対してのみ、その修正したプロファイルを使用するようにしてください。さらに、攻撃の入り口を減らすために、ユーザーがアップロードおよびダウンロードしているファイルが絶対に組織に脅威をもたらすことがないよう、他のセキュリティ対策も使用していることを確認してください。例えば、PE ファイルのダ

ウンロードを許可しなければならない場合は、必ず未知のファイルをすべて WildFire に送って分析を行っていることを確認してください。さらに、厳格な URL フィルタリング ポリシーを維持し、悪意のあるコンテンツをホストしていることが分かっているウェブサイトからユーザーがコンテンツをダウンロードできなくします。

STEP 1 | ファイル ブロッキング プロファイルを作成します。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **File Blocking (ファイル ブロッキング)** を選択してプロファイルを **Add (追加)** します。
2. ファイル ブロッキング プロファイルの **Name (名前)** に **Block_EXE** などと入力します。
3. （任意）**Description (説明)** に「ユーザーが **Web** サイトから **exe** ファイルをダウンロードできないようにする」などと入力します。
4. （任意）プロファイルを次のものと **Shared (共有)** することを指定します。
   - マルチ **vsys** ファイアウォール上のすべての仮想システム（**vsys**）—クリア（無効化）すると、**Objects (オブジェクト)** タブで選択された仮想システムでのみプロファイルを利用できます。
   - **Panorama** 上のすべてのデバイスグループ—クリア（無効化）すると、**Objects (オブジェクト)** タブで選択されたデバイスグループでのみプロファイルを利用できます。
5. （任意—Panorama のみ）管理者が、プロファイルを継承するデバイス グループのこのファイル ブロッキング プロファイルの設定をオーバーライドすることを禁止する場合は、**Disable override (オーバーライドの無効化)** を選択します。デフォルトでこのオプションはオフになっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。

STEP 2 | ファイル ブロッキングのオプションを設定します。

1. プロファイルを **Add (追加)** し、そのルールを定義します。
2. ルールの **Name (名前)**（**BlockEXE** など）を入力します。
3. **Any (すべて)** を選択するか、**web-browsing (ウェブ ブラウジング)** など、フィルタリングを行う単一あるいは複数の具体的な **Applications (アプリケーション)** を指定します。

   ウェブ ブラウザだけが、ユーザーが続行するために確認を行う応答ページ（続行プロンプト）を表示できます。他のアプリケーションを選択すると、ユーザーが続行するために確認を行えるプロンプトが表示されないため、そのアプリケーションのトラフィックがブロックされることになります。
4. **Any (すべて)** を選択するか、**exe** など、単一あるいは複数の具体的な **File Types (ファイルタイプ)** を指定します。
5. **Direction (方向)** を指定します（**download (ダウンロード)** など）。
6. **Action (アクション)** を指定します（**alert (アラート)**、**block (ブロック)**、あるいは **continue (続行)**）。例えば、実行ファイル（.exe）のダウンロードをユーザーに許可する前に確認を求める場合は、**continue (続行)** を選択します。あるいは、特定のファイル

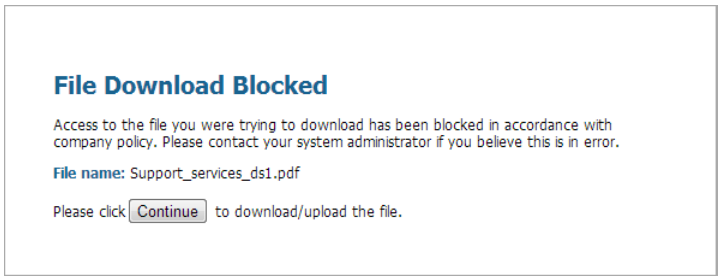
を **block (**ブロック**)** するか、ユーザーが実行ファイルをダウンロードする際にファイアウォールにただ **alert (**アラート**)** をトリガーさせるよう設定できます。

7. **OK** をクリックしてプロファイルを保存します。

STEP 3 | ファイル ブロッキング プロファイルをセキュリティ ポリシールールに適用します。

1. **Policies (**ポリシー**)** > **Security (**セキュリティ**)** を選択し、既存のポリシールールを選択するか、基本的なセキュリティ ポリシーのセットアップに従って新しいルールを **Add (**追加**)** します。
2. **Actions (**アクション**)** タブで、前のステップで設定したファイルブロッキングプロファイルを選択します。この例でのプロファイル名は **Block_EXE** です。
3. 設定を **Commit (**コミット**)** します。

STEP 4 | ファイル ブロッキング設定をテストするには、ファイアウォールの信頼されたゾーンのエンドポイント PC にアクセスし、信頼されないゾーンの Web サイトから実行ファイルのダウンロードを試みます。応答ページが表示されるはずです。**Continue (**続行**)** をクリックし、ファイルをダウンロードできることを確認します。また、ユーザーがダウンロードを続行できなくなるオプションとして、**alert (**アラート**)** や **block (**ブロック**)** などの他のアクションを設定することもできます。以下に、ファイル ブロッキングのデフォルト応答ページを示します。



STEP 5 | （任意）カスタム ファイル ブロッキング応答ページを定義します（**Device (**デバイス**)** > **Response Pages (**応答ページ**)**）。これにより、応答ページに表示される情報量を増やすことができます。会社のポリシーの情報やヘルプデスクの連絡先情報などを含めることができます。

continue (**続行**) アクションを使用するファイル ブロッキング プロファイルを作成する場合、選択できるアプリケーションは ***web-browsing*** のみです。その他のアプリケーションを選択すると、ユーザーには続行するためオプションが表示されないため、セキュリティポリシーに一致するトラフィックはファイアウォールを通過しません。さらに、*HTTPS* ウェブサイト用に復号化ポリシーを設定・有効化する必要があります。

ログをチェックし、この機能をテストする際に使用されたアプリケーションを確認します。たとえば、*Microsoft SharePoint* を使用してファイルをダウンロードする場合は、*Web* ブラウザを使用してそのサイトにアクセスするとしても、実際のアプリケーションは ***sharepoint-base*** または ***sharepoint-document*** です。（テスト時は、アプリケーションのタイプを ***Any (**すべて**)*** に設定すると効果的です）

ブルート フォース攻撃の防御

ブルート フォース攻撃は、同じ送信元または宛先 IP アドレスで大量の要求/応答を使用してシステムに侵入します。攻撃者は試行錯誤を繰り返す方法によって、チャレンジまたは要求に対する応答を推測します。

ファイアウォールの脆弱性防御プロファイルにはブルート フォース攻撃から保護するシグネチャも含まれています。各シグネチャには ID、脅威名、および重大度が設定されており、パターンが記録されるとトリガーされます。パターンは、トラフィックがブルート フォース攻撃として識別される条件と間隔を指定します。一部のシグネチャは、重大度がより低く、一致パターンを指定する別の子シグネチャと関連付けられています。パターンがシグネチャや子シグネチャと一致すると、シグネチャのデフォルト アクションがトリガーされます。

防御を適用するには、以下の手順を実行します。

- 脆弱性保護プロファイルをセキュリティポリシー ルールに適用します。アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップを参照してください。
- 新しいシグネチャを含むコンテンツ更新をインストールし、新たに出現した脅威から防御します。コンテンツ更新およびソフトウェア更新のインストールを参照してください。

ブルート フォース シグネチャのアクションとトリガー条件のカスタマイズ

ファイアウォールには、2 種類の事前定義されたブルート フォース シグネチャが含まれています。親シグネチャと子シグネチャです。子シグネチャはシグネチャに一致するトラフィック パターンの 1 回の発生です。親シグネチャは子シグネチャに関連付けられ、子シグネチャで定義されたトラフィック パターンに一致するイベントが指定された時間内に複数回発生した場合にトリガーされます。

通常、子シグネチャのデフォルト アクションは許可です。1 回のイベントだけで攻撃されたことにはならないためです。これにより、正当なトラフィックがブロックされず、また重要性の低いイベントについての脅威ログが生成されなくなります。Palo Alto Networks は、デフォルト アクションを変更する場合は必ず慎重に検討することをお勧めします。

多くの場合、ブルート フォース シグネチャが注目に値するイベントであるのは、その繰り返しパターンのためです。必要な場合は次のいずれかの作業を行って、ブルート フォース シグネチャ用のアクションをカスタマイズできます。

- ブルート フォース カテゴリ内のすべてのシグネチャのデフォルト アクションを変更するルールを作成します。トラフィックの許可、アラート、ブロック、リセット、または破棄のいずれかを選択できます。
- 特定のシグネチャに例外を定義します。例えば、CVE を検索したり、CVE 用の例外を定義したりできます。

親シグネチャの場合、トリガー条件およびアクションの両方を変更できます。子シグネチャの場合は、アクションのみを変更できます。

効果的に攻撃を軽減するために、ほとんどのブルート フォース シグネチャで *drop* アクションや *reset* アクションよりも *block-ip address* アクションを指定します。

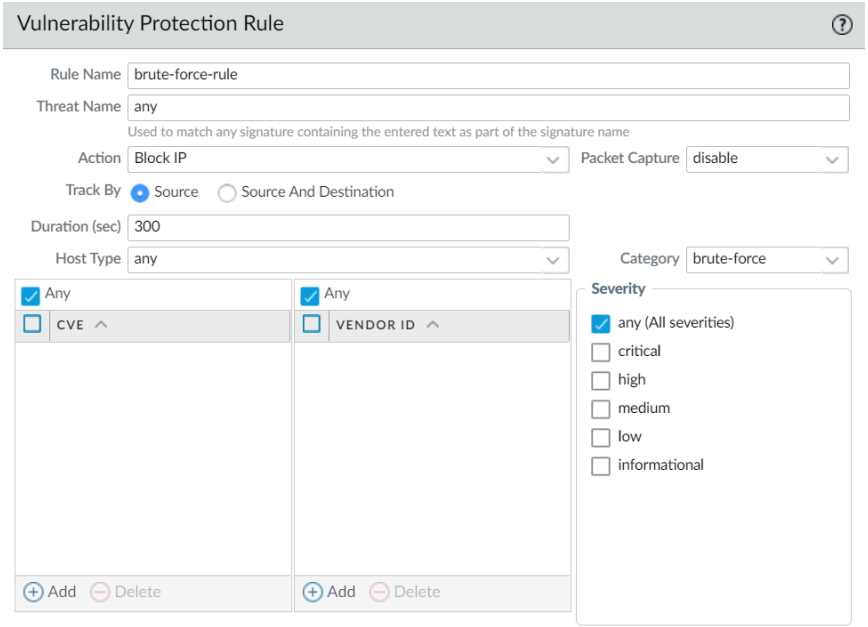
STEP 1 | 新しい脆弱性防御プロファイルを作成します。

1. **Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > Vulnerability Protection (脆弱性保護)** を選択してプロファイルを **Add (追加)** します。
2. 脆弱性保護プロファイルの **Name (名前)** を入力します。
3. （任意）**Description (内容)** を入力します。
4. （任意）プロファイルを次のものと **Shared (共有)** することを指定します。
   - マルチ **vsys** ファイアウォール上のすべての仮想システム（**vsys**）—クリア（無効化）すると、**Objects (オブジェクト)** タブで選択された仮想システムでのみプロファイルを利用できます。
   - **Panorama** 上のすべてのデバイスグループ—クリア（無効化）すると、**Objects (オブジェクト)** タブで選択されたデバイスグループでのみプロファイルを利用できます。
5. （任意—Panorama only） **Disable (無効化) override** to prevent administrators from overriding the settings of this Vulnerability Protection (脆弱性保護) profile in device groups that inherit the profileデフォルトでこのオプションはオフになっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。

STEP 2 | カテゴリ内のすべてのシグネチャのアクションを定義するルールを作成します。

1. **Rules (**ルール**)** タブで新しいルールを **Add (**追加**)** し、**Rule Name (**ルール名**)** を入力します。
2. （任意）具体的な脅威名を指定します（デフォルトは **any (**すべて**)**）。
3. **[**アクション**]** を設定します。この例では、**Block IP**[ブロックIP] に設定されています。

   脆弱性保護プロファイルで *IP* をブロックするように設定した場合、ファイアウォールはまずハードウェアを使用して *IP* アドレスをブロックします。攻撃トラフィックがハードウェアのブロック容量を超えた場合、次にファイアウォールはソフトウェア ブロック メカニズムを使用して残りの *IP* アドレスをブロックします。
4. **[**カテゴリ**]** を **[brute-force]** に設定します。
5. （任意）ブロック中の場合はブロックする **Host Type (**ホスト タイプ**)** を指定します。**server** あるいは r **client** (default is **any**).
6. 特定の署名のアクションをカスタマイズするには、「手順 3」を参照してください。
7. 親署名のトリガーしきい値をカスタマイズするには、ステップ 4 を参照してください。



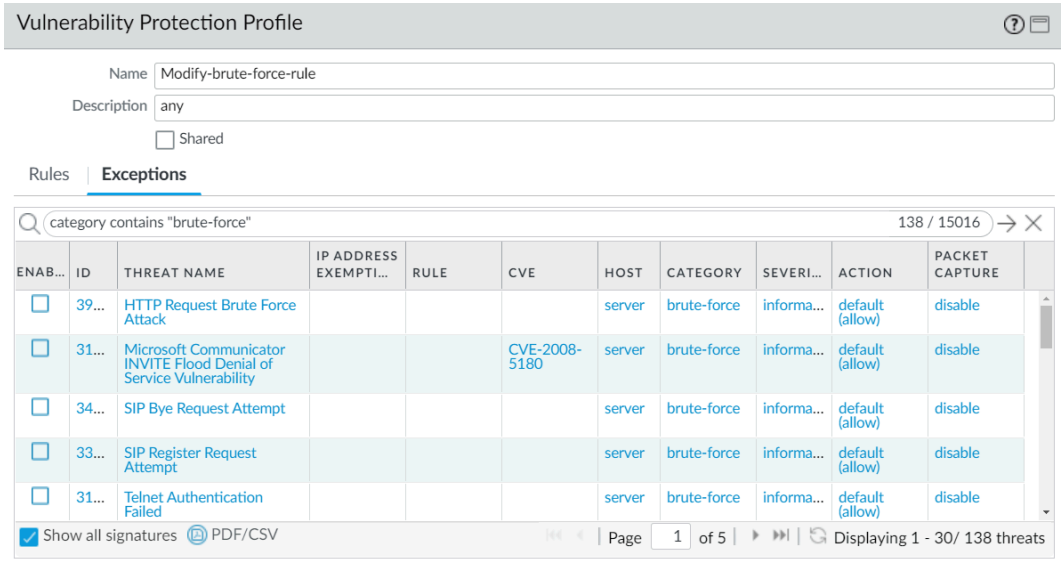
8. **[OK]** をクリックしてルールおよびプロファイルを保存します。

STEP 3 | （任意）特定のシグネチャのアクションをカスタマイズします。

1. **Exceptions (例外)** タブで **Show all signatures (**すべてのシグネチャを表示**)** し、修正したいシグネチャを探します。

   ブルート フォース カテゴリのすべてのシグネチャを表示するには、`category contains 'brute-force'`と検索します。

2. 特定のシグネチャを編集するには、Actions（操作）列の事前定義されたデフォルト アクションをクリックします。



3. アクションを設定します。**Allow (**許可**)**、**Alert (**アラート**)**、**Block Ip (**ブロック **IP)**、あるいは **Drop (**ドロップ**)**。**Block Ip (**ブロック **IP)** を選択した場合、以下の追加タスクを実行します。

   1. **[**日時**]** にアクションをトリガーするまでの時間を秒数で指定します。
   2. **Track By (**追跡区分**)** を指定するかどうか、**IP source (IP** 送信元**)** あるいは **IP source and destination (IP** 送信元および宛先**)** のどちらを使用して IP アドレスをブロックするかを指定します。

4. **OK** をクリックします。
5. 変更したシグネチャのそれぞれに対して、**[**有効化**]** 列のチェックボックスをオンにします。
6. **OK** をクリックします。

STEP 4 | 親シグネチャのトリガー条件をカスタマイズします。

編集可能な親シグネチャにはこのアイコンがついています。 .

この例では、検索条件はブルート フォース カテゴリおよび CVE-2008-1447 です。

1. シグネチャの時間属性および集約条件を編集（ ）します。
2. トリガーしきい値を変更するには、**seconds (秒)** あたりの **Number of Hits (ヒット数)** を指定します。
3. ヒット数（**Aggregation Criteria (集約条件)**）を **source (送信元)**、**destination (宛先)**、または**source-and-destination (送信元および宛先)** のいずれで集約するかを指定します。
4. **OK** をクリックします。

STEP 5 | この新しいプロファイルをセキュリティポリシー ルールに関連付けます。

1. **Policies (ポリシー)** > **Security (セキュリティ)**を選択し、セキュリティポリシールールを**Add**（追加）または変更します。
2. **Actions** （アクション） タブで、プロファイル設定の **Profile Type (プロファイル タイプ)** として **Profiles (プロファイル)** を選択します。
3. **Vulnerability Protection (脆弱性保護)** プロファイルを選択します。
4. **OK** をクリックします。

STEP 6 | 変更をコミットします。

1. **Commit**（コミット）をクリックします。

回避シグネチャの有効化

偽装された HTTP あるいは TLS リクエストを検知する Palo Alto Networks の回避シグネチャが、DNS リクエストで指定されているもの以外のドメインにクライアントが接続する際にアラートを生成できます。回避シグネチャは、ファイアウォールがさらに DNS プロキシとして動作してドメイン名のクエリを解決できるように設定されている場合のみ機能します。ベストプラクティスとして、次の各ステップを実施して回避シグネチャを有効化してください。

STEP 1 | ファイアウォールをクライアントおよびサーバー間で DNS プロキシとして動作できるようにします。

次の作業を含馬手、DNS プロキシ オブジェクトの設定を行います。

- ファイアウォールに DNS クエリをリッスンさせるインターフェイスを指定します。
- DNS リクエストを解決するためにファイアウォールが通信を行う DNS サーバーを定義します。
- 静的 FQDN から IP アドレスへのエントリーをセットアップし、ファイアウォールが DNS サーバーにアクセスすることなくローカルで解決できるようにします。
- 解決したホスト名から IP アドレスへのマッピングをキャッシュできるようにします。

STEP 2 | 最新のアプリケーションおよび脅威コンテンツ バージョン（コンテンツ バージョン 579 以降のもの）を入手します。

1. **Device**（デバイス） > **Dynamic Updates**（動的更新）を選択します。
2. 最新のアプリケーションおよび脅威コンテンツ更新を**Check Now**[今すぐチェック]して入手します。
3. アプリケーションおよび脅威コンテンツ バージョン 579（あるいはそれ以降）をダウンロードし、インストールします。

STEP 3 | 回避シグネチャにマッチしたトラフィックをファイアウォールがどのように扱うか定義します。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **Anti-Spyware (アンチスパイウェア)** を選択し、アンチスパイウェア プロファイル を **Add (追加)** あるいは変更します。
2. **Exceptions (例外)** を選択し、さらに**Show all signatures (すべてのシグネチャを表示)** を選択します。
3. キーワード`evasion`に基づいてシグネチャをフィルタリングします。
4. すべての回避シグネチャの**Action** [アクション]を、許可あるいはデフォルトのアクション以外のものに設定します（デフォルトのアクションは回避シグネチャが許可されるものです）。例えば、シグネチャ ID 14978 および 14984 の **Action (アクション)** を **alert (アラート)** あるいは **drop (ドロップ)** に設定します。
5. **OK** をクリックし、更新したアンチスパイウェア プロファイルを保存します。
6. アンチスパイウェア プロファイルをセキュリティポリシールールに適用します。**Policies (ポリシー)** > **Security (セキュリティ)** の順に選択し、適切なポリシーを選択して変更し、**Actions** （アクション） タブをクリックします。Profile Settings (プロファ

イル設定）で **Anti-Spyware (アンチスパイウェア)** の隣りにあるドロップダウンリストをクリックし、先ほど変更したアンチスパイウェア プロファイルを選択して回避シグネチャを強制します。

STEP 4 | 変更をコミットします。

Commit（コミット）をクリックします。

Monitor Blocked IP Addresses（ブロックされた IP アドレスのモニター）

ファイアウォールは、自身がブロックしている送信元 IP アドレスのブロックリストを維持します。ファイアウォールが送信元 IP アドレスをブロックする際（次のいずれかのポリシールールを設定する際など）、パケットが CPU あるいは次のパケット バッファ リソースを使用する前に、ファイアウォールがハードウェア内のそのトラフィックをブロックします。

- アクションが **Protect (保護)** である分類化 DoS 保護ポリシールール（新規セッションのフラッド攻撃に対する DoS プロテクションの設定に示されている通り、分類化 DoS 保護プロファイルに関連する分類化 DoS 保護ポリシーは、そのインバウンド接続が送信元 IP アドレス、宛先 IP アドレス、あるいは送信元および宛先 IP アドレスのペアにマッチすることを指定します）
- 脆弱性保護プロファイルを使用するセキュリティポリシー

ハードウェアIPアドレスブロッキングは、PA-3200 Series、PA-5200 Series、PA-5400 Series(PA-5450を除く)、およびPA-7000 Series firewallsでサポートされています。

ブロックリストを表示したり、ブロックリスト上の IP アドレスについての詳細な情報を取得したり、ハードウェアおよびソフトウェアがブロックしているアドレスの数を確認したりできます。ブロックすべきだと判断した場合は、リストの IP アドレスを削除可能です。リストにあるアドレスについての詳細情報のソースは変更できます。また、ハードウェアが IP アドレスをブロックする期間も変更できます。

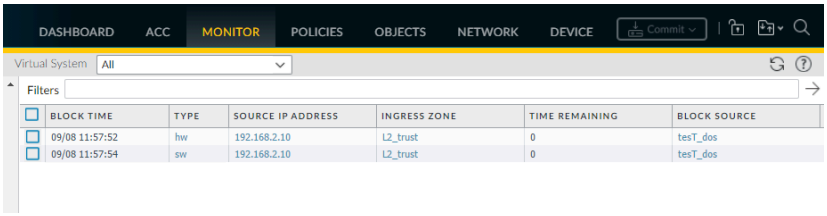
ブロックリストのエントリを表示します。

1. **Monitor (監視)** > **Block IP List (ブロック IP リスト)** を選択します。

   ブロックリストの各エントリの Type (タイプ) 列は、ハードウェア（hw）とソフトウェア（sw）のどちらによってブロックされたのかを示します。
2. 画面下部の表示を確認します：
   - ファイアウォールがサポートする、ブロックされた IP アドレスの数のうち **Total Blocked IPs (ブロックされた IP の合計)** カウント。
   - ファイアウォールが使用したブロックリストの割合。
3. 表示されたエントリをフィルタリングするには、列の値を選択（**Filters (フィルタ)** フィールドにフィルタが作成されます）し、Apply Filter (フィルタを適用) します

（→）。そうしない場合、ファイアウォールは最初の 1,000 件のエントリを表示します。

4. **Page (**ページ**)** 番号を入力するか、画面下部にある矢印をクリックして項目のページを進めます。
5. ブロックリストのアドレスの詳細情報を確認するには、ソース IP アドレスにカーソルを合わせて下向きの矢印リンクをクリックします。**Who Is** リンクをクリックすると、そのアドレスについての Network Solutions Who Is 情報が表示されます。



ブロックリストのエントリを削除します。

ブロックすべきでないと判断した *IP* アドレスがある場合は、エントリを削除します。その後、ファイアウォールにそのアドレスをブロックさせているポリシールールを修正します。

1. **Monitor (**監視**)** > **Block IP List (**ブロック **IP** リスト**)** を選択します。
2. 単一あるいは複数の項目を選択して **Delete (**削除**)** をクリックします。
3. （任意）**Clear All (**すべてクリア**)** を選択し、リストの全項目を削除します。

トラブルシューティングを行うために、ハードウェア IP アドレス ブロッキングを無効あるいは再度有効にします。

ハードウェア *IP* アドレス ブロッキングが無効になっていても、ファイアウォールは設定済みのソフトウェア *IP* アドレス ブロッキングをすべて実行できます。

```
> set system setting hardware-acl-blocking [enable | disable]
```

CPU およびパケット バッファのリソースを節約するために、ハードウェア *IP* アドレス ブロッキングは、*Palo Alto Networks* の技術サポートから無効にするよう求められない限り (トラフィック フローのデバッグを行っている際など)、有効な状態を保てるようにしてください。

ハードウェアによってブロックされた IP アドレスがブロックリストを残す秒数を調整します（範囲は 1～3,600、デフォルトは 1）。

```
> set system setting hardware-acl-blocking duration <seconds>
```

ハードウェアのブロック能力を超過するリスクを減らすには、ソフトウェア ブロックリストの各エントリよりもハードウェア ブロックリストの期間を短く保ちます。

IP アドレスの詳細情報を探すデフォルトのウェブサイトを、Network Solutions Who Is から別のウェブサイトに変更します。

```
# set deviceconfig system ip-address-lookup-url <url>
```

ハードウェアおよびソフトウェアによってブロックされた 送信元 IP アドレスのカウントを確認します（例えば、攻撃の頻度を見るなど）。

ハードウェア ブロック表およびブロックリストの IP アドレス エントリの合計数を確認します（ハードウェアおよびソフトウェアによってブロック）。

```
> show counter global name flow_dos_blk_num_entries
```

ハードウェアによってブロックされたハードウェア ブロック表の IP アドレス エントリの数を確認します。

```
> show counter global name flow_dos_blk_hw_entries
```

ソフトウェアによってブロックされたブロックリスト上の IP アドレス エントリの数を確認します。

```
> show counter global name flow_dos_blk_sw_entries
```

PA-7000 Series ファイアウォールのスロット毎のブロックリスト情報を表示します。

```
> show dos-block-table software filter slot <slot-number>
```


脅威シグネチャのカテゴリ

Palo Alto Networks の脅威シグネチャには 3 つの種類があり、いずれもファイアウォールがネットワーク トラフィックをスキャンする際に異なる脅威を検出するように設計されています：

- アンチウイルス シグネチャ–実行ファイル内のウイルスおよびマルウェア、ファイルの種類を検出します。
- アンチスパイウェア シグネチャ–感染したクライアント上のスパイウェアがユーザーの同意成しにデータを収集する、および/または離れた攻撃者と通信するコマンド アンド コントロール（C2）アクティビティを検出します。
- 脆弱性シグネチャ–攻撃者がエクスプロイトの対象にし得るシステムの欠陥を検出します。

シグネチャの重大度は検出されたイベントのリスクを示し、シグネチャのデフォルトのアクション（例：ブロックあるいはアラート）は、マッチするトラフィックに対して適用する Palo Alto Networks が推奨するアクションを示します。

アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップを行って脅威を検出した際に行うアクションをファイアウォールに対して指定します。また、デフォルトのセキュリティ プロファイルを使い、Palo Alto Networks の推奨事項に基づいて簡単に脅威をブロックし始めることができます。各シグネチャ タイプ、カテゴリー、特定のシグネチャについて、新しいプロファイルを作成あるいは編集する作業を進め、潜在的な脅威に細かく対応できます。

次の表は、すべてのシグネチャ カテゴリーをタイプ毎（アンチウイルス、スパイウェア、脆弱性）に一覧表示しています。また、各カテゴリーのシグネチャを提供するコンテンツ更新（アプリケーションおよび脅威、アンチウイルス、WildFire）も含まれています。また、Palo Alto Networks Threat Vault にアクセスして脅威シグネチャの詳細を把握することもできます。

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	説明
アンチウイルス シグネチャ		
apk	Antivirus [アンチウイルス] WildFire	悪意のある Android Application（APK）ファイル。
MacOSX	Antivirus [アンチウイルス] WildFire	次のような悪意のある MacOSX ファイル: • Apple ディスク イメージ (DMG) ファイル • Machオブジェクトファイル(Mach-O)は、実行可能ファイル、ライブラリ、およびオブジェクトコード • Apple ソフトウェア インストーラー パッケージ (PKG)

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	説明
Flash	Antivirus（アンチウイルス） WildFire または WildFire Private	Web ページに組み込まれている Adobe Flashアプレットおよびflashコンテンツ
jar	Antivirus [アンチウイルス] WildFire	Java アプレット（JAR/クラス ファイル タイプ）。
ms-office	Antivirus [アンチウイルス] WildFire または WildFire Private	ドキュメント（DOC、DOCX、RTF）、ワークブック（XLS、XLSX）、PowerPoint プレゼンテーション（PPT、PPTX）を含む Microsoft Office ファイル。これには、Office Open XML (OOXML) 2007+ ドキュメントも含まれます。
pdf	Antivirus（アンチウイルス） WildFire または WildFire Private	ポータブルドキュメントフォーマット（PDF）ファイル。
pe	Antivirus（アンチウイルス） WildFire または WildFire Private	Portable executable（PE）ファイルは Microsoft Windows システムで自動的に実行され、身元が確認できる場合のみ許可できます。これには次のようなファイル形式があります： • オブジェクトコード。 • フォント（FON）。 • システムファイル（SYS）。 • ドライバーファイル（DRV）。 • Windows コントロールパネルのアイテム（CPL）。 • DLL（ダイナミック リンク ライブラリ）。 • OCX（OLE カスタムコントロール、あるいは ActiveX コントロール用ライブラリ）。 • Windows スクリーンセーバー ファイル (SCR)。 • デバイスの更新および起動操作をサポートする、OS およびファームウェアの間で実行される Extensible Firmware Interface（EFI）ファイル。 • プログラム情報ファイル（PIF）。

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	説明
linux	Antivirus [アンチウイルス] WildFire	実行可能およびリンク可能な形式（ELF）ファイル。
アーカイブ	Antivirus [アンチウイルス] WildFire	Roshalアーカイブ（RAR）と7-Zip（7z）アーカイブファイル。
スパイウェア シグネチャ		
[Adware]	アプリケーションおよび脅威	好ましくない広告を表示するおそれのあるプログラムを検出します。一部のアドウェアはブラウザに変更を加え、頻繁に検索されるキーワードを Web ページ上でハイライト表示し、ハイパーリンクを付与します。これらのリンクは、ユーザーを広告サイトにリダイレクトさせます。また、アドウェアはコマンド アンド コントロール（C2）サーバーからアップデートを取得し、それをブラウザやクライアントシステムにインストールすることもできます。 このカテゴリーで新たにリリースされる保護はあまりありません。
autogen	Antivirus（アンチウイルス）	このペイロード ベースのシグネチャは、コマンド アンド コントロール（C2）トラフィックを検出し、自動生成されます。自動生成されたシグネチャは C2 ホストが未知である場合、あるいは急速に変化する場合でも C2 トラフィックを検出できるというのが重要です。
backdoor	アプリケーションおよび脅威	攻撃者がシステムへの不正なリモートアクセスを得られるようにするプログラムを検出します。
[Botnet]	アプリケーションおよび脅威	ボットネット アクティビティを示します。ボットネットとは、攻撃者が制御する、マルウェアに感染したコンピューター（ボット）のネットワークのことです。攻撃者はボットネットの全コンピューターに一元的に命令を出し、同時に一斉にアクション（例えば DoS 攻撃などを行う）を実行させます。
browser-hijack	アプリケーションおよび脅威	ブラウザ設定を変更しているプラグインやソフトウェアを検出します。ブラウザを乗っ取った攻撃者は、自動検索をコントロールしたり、ユーザーのウェブ アク

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	説明
		ティビティを追跡したり、その情報を C2 サーバーに送信したりする可能性があります。 このカテゴリーで新たにリリースされる保護はあまりありません。
クリプトマイナー	アプリケーションおよび脅威	(クリプトジャッキングまたはマイナーと呼ばれることもあります) ユーザーの知らないうちにコンピューティング リソースを使用して暗号通貨をマイニングするように設計された悪意のあるプログラムから生成されたダウンロードの試行またはネットワーク トラフィックを検出します。クリプトマイナー バイナリは、システム アーキテクチャを決定し、システム上の他のマイナー プロセスを強制終了しようとするシェル スクリプト ダウンローダーによって頻繁に配信されます。一部のマイナーは、悪意のある Web ページをレンダリングする Web ブラウザなど、他のプロセス内で実行します。
data-theft	アプリケーションおよび脅威	情報を既知の C2 サーバーに送信しているシステムを検出します。 このカテゴリーで新たにリリースされる保護はあまりありません。
dns	Antivirus（アンチウイルス）	悪意のあるドメインに接続するための DNS リクエストを検出します。 dns および dns-wildfire シグネチャは、同じ悪意のあるドメインを検出しますが、dns シグネチャは日次のアンチウイルス コンテンツ更新に、dns-wildfire シグネチャは 5 分毎に保護をリリースする WildFire 更新に含まれます。
dns-security	Antivirus（アンチウイルス）	悪意のあるドメインに接続するための DNS リクエストを検出します。 dns-security には、DNS Security サービスによって生成された固有の署名に加えて、dns および dns-wildfire からの署名が含まれています。
dns-wildfire	WildFire または WildFire Private	悪意のあるドメインに接続するための DNS リクエストを検出します。 dns および dns-wildfire シグネチャは、同じ悪意のあるドメインを検出しますが、dns シグネチャは日次のア

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	説明
		ンチウイルス コンテンツ更新に、dns-wildfire シグネチャは 5 分毎に保護をリリースする WildFire 更新に含まれます。
ダウンローダー	アプリケーションおよび脅威	（ドロッパー、ステージャー、ローダーとも呼ばれる） インターネット接続を使用してリモート サーバーに接続し、侵入先のシステムにマルウェアをダウンロードして実行するプログラムを検出します。最も一般的な使用例は、ダウンローダーがサイバー攻撃のステージ*1*の集大成として展開されることであり、ダウンローダーのフェッチされたペイロードの実行は、ステージ*2*と見なされます。シェルスクリプト (Bash、PowerShell など)、トロイの木馬、および PDFや Word ファイルなどの悪意のあるルアー ドキュメント (maldocs とも呼ばれます) は、一般的なダウンローダータイプです。
詐欺行為	アプリケーションおよび脅威	(フォームジャック、フィッシング、詐欺を含む) ユーザーの機密情報を収集するため悪意のある JavaScript コードが挿入されていると判断された侵害された Web サイトへのアクセスを検出します。(例えば：名前、住所、メール アドレス、クレジットカード番号、CVV、有効期限等) eコマース Web サイトの決済ページにある支払いフォームから。
hacktool	アプリケーションおよび脅威	悪意のある攻撃者が偵察を行ったり、脆弱なシステムを攻撃またはアクセスしたり、データを盗み出したり、コマンドと制御チャネルを作成して許可なくコンピュー タシステムを密かに制御したりする目的でソフトウェア ツールを用いて生成したトラフィックを検出します。これらのプログラムは、マルウェアやサイバー攻撃との関連度が高いです。ハッキング ツールは、Red team および Blue team の運用、侵入テスト、ならびに R&D で使用される場合、良識ある方法で展開される可能性があります。これらのツールの使用または所持は、意図に関係なく、一部の国では違法である可能性があります。
Keylogger	アプリケーションおよび脅威	攻撃者がキー操作を記録し、スクリーンショットを撮影してユーザーアクティビティを密かに追跡できるようにするプログラムを検出します。 キーロガーは様々な C2 手法を使用し、定期的にログおよびレポートを事前定義済みのメールアドレスある

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	説明
		いは C2 サーバーに送信します。キーロガーによる監視を通じて、攻撃者がネットワーク アクセスを可能にする認証情報を入手する可能性もあります。
networm	アプリケーションおよび脅威	自己増殖し、システムからシステムへと広がるプログラムを検出します。ネットワームは、共有リソースを使用し、あるいはセキュリティの不備を利用して目標のシステムにアクセスする可能性があります。
phishing-kit	アプリケーションおよび脅威	ユーザーがフィッシング キットのランディングページに接続しようとしているのを検出します（悪意のあるサイトへのリンクが記載されたメールの受信後が多い）。フィッシング サイトは、ユーザーをだまして認証情報を送信させ、攻撃者がその情報を盗んでネットワークへのアクセスを得られるようにします。 フィッシングキットのランディングページへのアクセスをブロックするだけでなく、Multi-Factor Authentication と 認証情報フィッシングの阻止 を有効にして、すべての段階でフィッシング攻撃を防御します。
post-exploitation	アプリケーションおよび脅威	攻撃者が侵入したシステムの価値を評価しようとするエクスプロイト後の段階を示唆するアクティビティを検出します。これには、システムに保存されているデータの重要性、さらにネットワークに侵入する上でそのシステムがどの程度重要かを評価することが含まれます。
webshell	アプリケーションおよび脅威	インプラントの検出やコマンドと制御の相互通信など、Web シェルと Web シェル トラフィックを検出します。Web シェルは、最初に悪意のある攻撃者によって侵害されたホストに埋め込まれる必要があり、ほとんどの場合、Web サーバーまたはフレームワークを標的にします。その後のWebシェルファイルとの通信により、悪意のある攻撃者がシステムに足場を確立し、Webサーバーユーザーのコンテキストでサービスとネットワークの列挙、データの漏えい、およびリモートコード実行を行うことができます。最も一般的な Web シェル タイプは、PHP、.NET、および Perl マークアップ スクリプトです。また、攻撃者はウェブシェルに感染した Web サーバー（インターネットに接

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	説明
		続されたサーバー、内部システムの両方）を利用し、その他の内部システムもターゲットにします。
spyware	アプリケーションおよび脅威	アウトバウンド C2 通信を検出します。これらのシグネチャは自動生成されるか、Palo Alto Networks の調査員が手作業で作成します。 スパイウェアおよび自動生成シグネチャの両方がアウトバウンド *C2* 通信を検出しますが、自動生成シグネチャはペイロード ベースであり、未知、あるいは急速に変化する *C2* ホストとの *C2* 通信を一意に検出できます。
脆弱性シグネチャ		
brute force	アプリケーションおよび脅威	ブルート フォース シグネチャは、一定期間に繰り返し生じる事象を検出します。正当なアクティビティが隔離される可能性もありますが、ブルート フォース シグネチャはアクティビティの正当性が疑わしくなるような頻度を示唆します。例えば、FTP ログインが一度失敗しても、悪意のあるアクティビティにはなりません。しかし、短期間に FTP ログインが多く失敗した場合、攻撃者が FTP サーバーへのアクセスを求めて組み合わせを変えながらパスワードを試していることが示唆されます。 ブルート フォース シグネチャのアクションおよび発動条件を調整できます。
code execution	アプリケーションおよび脅威	攻撃者が悪用し、ログイン済みのユーザーの権限でシステム上でコードを実行できるようにする、コード実行時の脆弱性を検出します。
code-obfuscation	アプリケーションおよび脅威	機能を維持したまま特定のデータを隠蔽するよう変更されたコードを検出します。難読化されたコードは読みづらい、あるいは判読不可能であるため、どのようなコマンドをコードが実行しているのか、どのプログラムとやり取りするよう設計されているのかをすぐに把握できません。最も多いのは、攻撃者がコードを難読化してマルウェアを隠蔽することです。それより頻度は落ちますが、プライバシー、知的財産を保護する、あるいはユーザーエクスペリエンスを向上させる

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	説明
		ために、正当な開発者がコードを難読化することもあります。例えば、ファイル サイズを減らしてウェブサイトの読み込み時間と帯域幅の消費量を減らす特定の難読化（ミニマイズ）があります。
dos	アプリケーションおよび脅威	攻撃者が目標のシステムを利用不可能にし、一時的にシステムおよびそれに従属するアプリケーションおよびサービスを中断させる、サービス拒否（DoS）攻撃を検出します。DoS 攻撃を行うために、攻撃者は目標のシステムに大量のトラフィックを送ったり、エラーを発生させる情報を送信したりします。DoS 攻撃は、サービスの正当なユーザー（従業員、会員、アカウント所有者など）やユーザーがアクセスできるリソースなどを奪います。
exploit-kit	アプリケーションおよび脅威	エクスプロイトキットのランディングページを検出します。エクスプロイトキットのランディングページには、複数のブラウザおよびプラグインに関して、一つあるいは多くの共通脆弱性識別子（CVE）をターゲットにする複数のエクスプロイトが含まれていることが多くあります。目標の CVE はすぐに変化するため、エクスプロイトキット シグネチャは CVE ではなくエクスプロイトキットのランディングページに基づいて発動します。 エクスプロイトキットを含むウェブサイトにユーザーがアクセスする際、エクスプロイトキットは目標の CVE をスキャンし、被害者のコンピューターに悪意のあるペイロードを密かに送り込もうとします。
info-leak	アプリケーションおよび脅威	攻撃者がエクスプロイトしてセンシティブあるいは占有情報を盗む可能性があるソフトウェアの脆弱性を検出します。通常、データを保護する包括的なチェックは存在しないため、情報流出が発生する可能性があり、攻撃者は巧妙なリクエストを送信して情報流出をエクスプロイトできます。
insecure-credentials	アプリケーションおよび脅威	ソフトウェア、ネットワークアプライアンス、および IoT デバイスの脆弱な、侵害された、製造元のデフォルトのパスワードの使用を検出します。
オーバーフロー	アプリケーションおよび脅威	リクエストのチェックが不適切であり、攻撃者がエクスプロイトする可能性があるオーバーフローの脆弱性を検出します。攻撃が成功すると、アプリケーショ

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	説明
		ン、サーバー、あるいはオペレーティングシステムの権限でリモートからコードを実行できる可能性があります。
phishing	アプリケーションおよび脅威	ユーザーがフィッシング キットのランディングページに接続しようとしているのを検出します（悪意のあるサイトへのリンクが記載されたメールの受信後が多い）。フィッシング サイトは、ユーザーをだまして認証情報を送信させ、攻撃者がその情報を盗んでネットワークへのアクセスを得られるようにします。 フィッシングキットのランディングページへのアクセスをブロックするだけでなく、Multi-Factor Authentication と 認証情報フィッシングの阻止 を有効にして、すべての段階でフィッシング攻撃を防御します。
protocol-anomaly	アプリケーションおよび脅威	プロトコルの挙動が通常の適切な用途から外れる、プロトコルの異常を検出します。例えば、不正な形式のパケット、プログラムが不適切なアプリケーション、標準的でないポート上で実行されているアプリケーションはすべて、異常なプロトコルとみなされ、回避ツールとして使用される可能性があります。あらゆる重大度の異例のプロトコルをブロックすることがベストプラクティスになります。
SQLインジェクション	アプリケーションおよび脅威	攻撃者が SQL クエリをアプリケーションのリクエストに含め、データベースからデータを読み取る、あるいはデータを変更する、よくあるハッキング技術を検出します。このタイプのテクニックは、ユーザーの入力情報のサニタイズが不十分なウェブサイトに対してよく利用されます。

脅威例外の作成

Palo Alto Networks は、脅威シグネチャの推奨されるデフォルトのアクション（ブロックやアラートなど）を定義しています。脅威 ID を使用することで、脅威シグネチャを適用対象から除外したり、脅威シグネチャに対してファイアウォールが取るアクションを変更したりできます。例えば、ネットワーク上で誤検出を引き起こす脅威シグネチャに対するアクションを変更することができます。

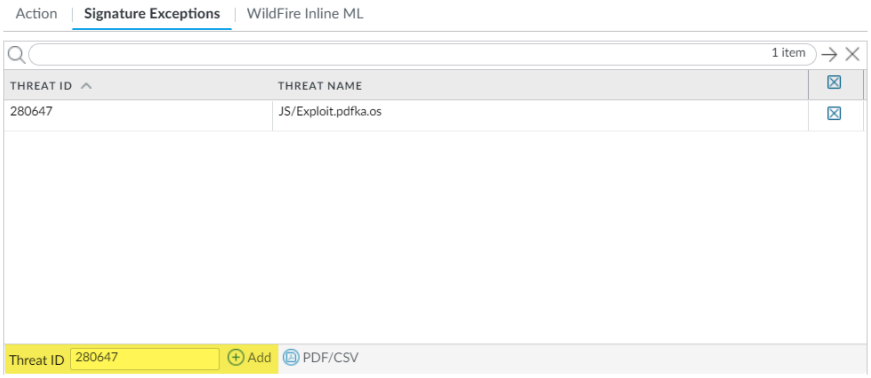
アンチウイルス、脆弱性、スパイウェア、および DNS シグネチャ用の脅威例外を設定し、脅威に対するファイアウォールの対応方法を変更します。しかし、作業を始める前に、ファイアウォールがデフォルトのシグネチャ設定に基づいて脅威を検知し、対処を行っていることを確認してください。

- アンチウイルス、脅威およびアプリケーション、WildFire シグネチャ更新の最新のものを取得します。
- アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップを行い、それらのセキュリティ プロファイルをセキュリティポリシーに割り当てます。

STEP 1 | アンチウイルス シグネチャを適用対象から除外します。

アンチウイルス プロファイルを使用してアンチウイルス シグネチャを適用対象から除外できますが、特定のアンチウイルス シグネチャに対するファイアウォールのアクションを変更することはできません。ただし、*Decoders* (***Objects** > **Security Profiles** > **Antivirus** > **<antivirus-profile>** > **Antivirus***) を編集することで、*firewall* がさまざまな種類のトラフィックで見つかったウイルスを強制するアクションを定義できます。

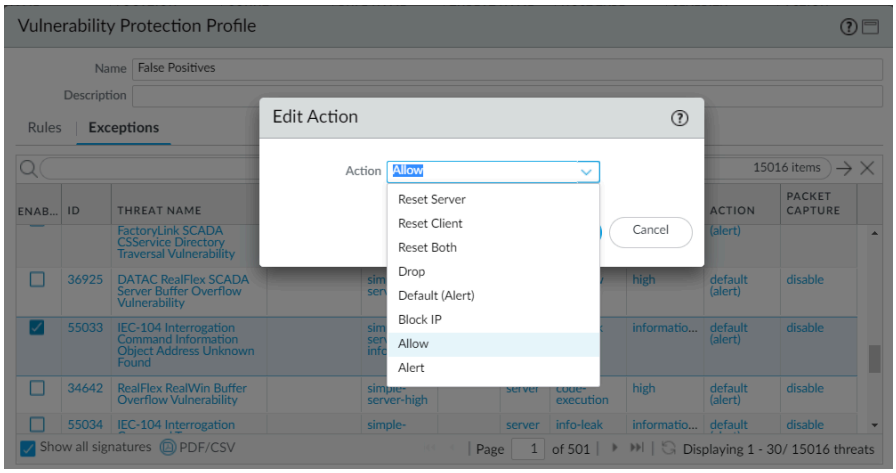
1. **Objects (オブジェクト) >** > **Security Profiles (セキュリティ プロファイル) >** > **Antivirus (アンチウイルス)** を選択します。
2. 脅威シグネチャを除外したいアンチウイルス プロファイルを **Add (追加)** するか、既存のものを変更し、**Signature Exception (シグネチャ例外)** を選択します。
3. 適用対象から除外したい脅威シグネチャの **Threat ID (脅威 ID)** を **Add (追加)** します。



4. **OK** をクリックしてアンチウイルス プロファイルを保存します。

STEP 2 | 脆弱性およびスパイウェア シグネチャに対する対処方法を変更します（DNS シグネチャを除きます。スパイウェア シグネチャの一種である DNS シグネチャに対する対処方法を変更する場合は、次のオプションまでスキップしてください）。

1. **Objects (オブジェクト) >** > **Security Profiles (セキュリティ プロファイル) >** > **Anti-Spyware (アンチスパイウェア)** あるいは **Objects (オブジェクト) >** > **Security Profiles (セキュリティ プロファイル) >** > **Vulnerability Protection (脆弱性保護)** を選択します。
2. 脅威シグネチャを除外したい既存のアンチスパイウェアまたは脆弱性防御プロファイルを **Add (追加)** するか変更してから、アンチスパイウェア保護プロファイルの **Signature Exceptions (シグネチャ例外)** または脆弱性防御プロファイルの **Exceptions (例外)** のいずれかを選択します。
3. **Show all signatures (すべてのシグネチャを表示)** してフィルタリングし、適用ルールを変更したいシグネチャを選択します。
4. 適用の仕方を変更したいシグネチャの **Enable (有効)**列にあるボックスにチェックを入れます。
5. この脅威シグネチャについて、ファイアウォールに適用させたい **Action (アクション)** を選択します。



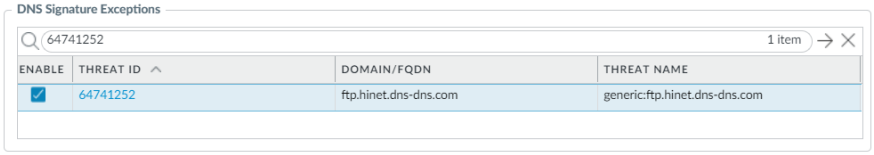
誤検出を引き起こすため、シグネチャを適用から除外したい場合は、**Action (アクション)** を **Allow (許可)** に設定します。

6. **OK** をクリックし、新しい、あるいは変更したアンチスパイウェアまたは脆弱性保護プロファイルを保存します。

STEP 3 | DNS シグネチャに対する対処方法を変更します。

デフォルト設定では、DNS シグネチャにシンクホールがあると検知された悪意のあるホスト名を DNS が検索します。

1. **Objects (オブジェクト) >** > **Security Profiles (セキュリティ プロファイル) >** > **Anti-Spyware (アンチスパイウェア)** を選択します。
2. 脅威シグネチャを除外したいアンチスパイウェア プロファイルを **Add (追加)** するか、既存のものを変更し、**DNS Exceptions (DNS 例外)** を選択します。
3. 施行から除外する DNS シグネチャの DNS 脅威 ID を検索し、該当するシグネチャのボックスを選択します:



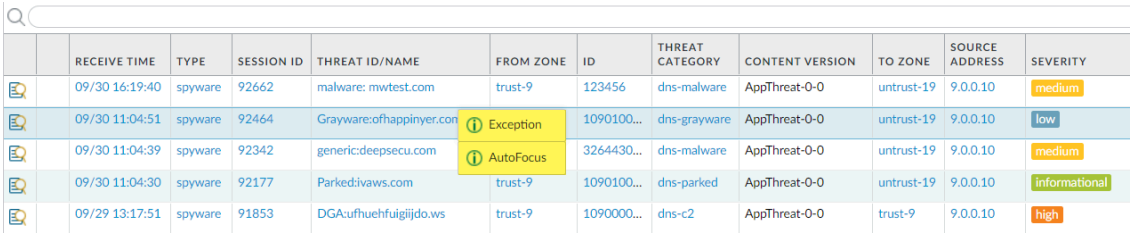
4. **OK** をクリックし、新しい、あるいは変更したアンチスパイウェア プロファイルを保存します。

カスタム シグネチャ

特定のトラフィックを検出してブロックするカスタム脅威シグネチャを作成できます。ファイアウォールが Panorama管理サーバーによって管理されている場合、ThreatID はファイアウォール上の対応するカスタム脅威にマップされ、ファイアウォールが設定済みのカスタム ThreatID を入力した脅威ログを生成できるようにします。詳細については、カスタム アプリケーションと脅威シグネチャのガイドをご覧ください。

脅威レポートの監視および取得

ファイアウォールに統合されている Threat Vault および AutoFocus の各機能により、ファイアウォールが検出する脅威の可視性が増し、組織のネットワーク トラフィックにどのようにアーチファクトが適合するのかについて、全体像をさらに深く知ることができるようになります（アーチファクトとは、ファイル、メールのリンク、あるいはセッションに関連するプロパティ、アクティビティや挙動のことです）。脅威についての文脈情報を即座に入手したり、脅威調査をファイアウォールから Threat Vault および AutoFocus にシームレスに切り替えたりすることができます。



さらに、脅威イベントの種類を分類する脅威シグネチャのカテゴリを使用して、特定の種類の脅威アクティビティにフォーカスしたり、カスタム レポートを作成したりできます。

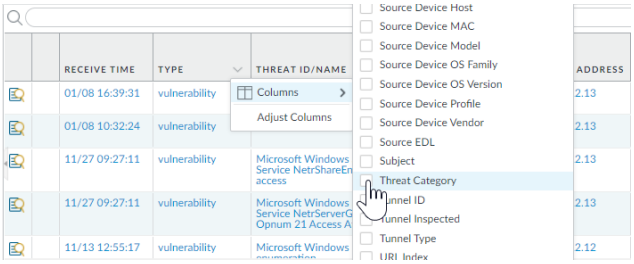
- 脅威カテゴリに基づいてアクティビティを監視し、カスタム レポートを作成
- 脅威シグネチャの詳細を把握
- ネットワーク トラフィックのための AutoFocus 脅威インテリジェンス

脅威カテゴリに基づいてアクティビティを監視し、カスタム レポートを作成

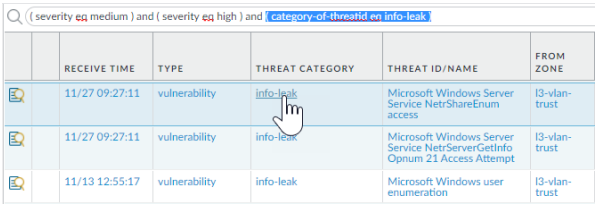
脅威カテゴリは異なる種類の脅威シグネチャを分類化し、理解しやすくすると共に、脅威シグネチャが検出した各イベントを関連付けます。脅威カテゴリは、より広汎な脅威シグネチャ タイプ（スパイウェア、脆弱性、アンチウイルス、および DNS シグネチャ）のサブネットです。脅威ログの各エントリは、記録された各イベントの **Threat Category (**脅威カテゴリ**)** を表示します。

脅威カテゴリで脅威ログをフィルタリングします。

1. **Monitor (監視)** > **Logs (ログ)** > 選択します。
2. Threat Category (脅威カテゴリ) 列を追加し、ログ エントリ毎に脅威カテゴリを閲覧できるようにします。

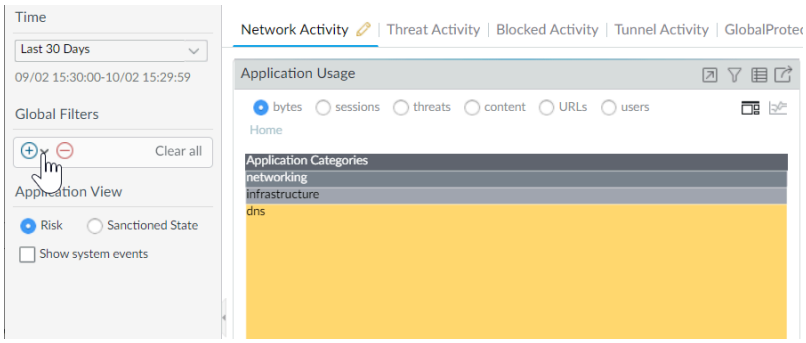


3. 脅威カテゴリに基づいてフィルタリングする方法：
   - ログ クエリ ビルダーを使用して Threat Category (脅威カテゴリ) の **Attribute (属性)** を持つフィルタを追加し、**Value (値)** フィールドに Threat Category (脅威カテゴリ) を入力します。
   - いずれかのログ エントリの Threat Category (脅威カテゴリ) を選択し、そのカテゴリをフィルターに追加します。

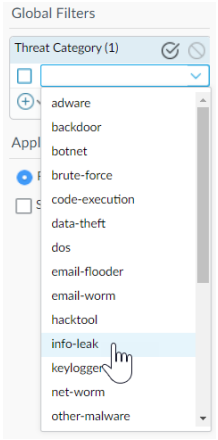


脅威カテゴリに基づいて ACC アクティビティをフィルタリングします。

1. **ACC** を選択し、脅威カテゴリをグローバルフィルターとして追加します。



2. 脅威カテゴリを選択し、すべての ACC タブをフィルタリングします。



脅威カテゴリに基づいてカスタム レポートを作成し、ファイアウォールが検出した特定のタイプの脅威についての情報を取得します。

1. **Monitor (監視)** > **Manage Custom (カスタム レポートの管理)** を選択し、新しいカスタム レポートを追加、あるいは既存のものを変更します。
2. カスタム レポートのソースとして使用する **Database (データベース)** を選択します。このケースでは、2 種類のデータベース ソース（サマリーデータベースおよび詳細ログ）のいずれかから **Threat (脅威)** を選択します。応答時間を短縮できるよう、サマリーデータベースのデータはレポート生成時に集約されます。詳細ログは生成により時間がかかりますが、各ログ エントリに関するすべてのデータを項目別に提供できます。
3. Query Builder (クエリ ビルダー) で、**Threat Category (脅威カテゴリ)** の属性を持つレポート フィルタを追加し、Value (値) フィールドで、レポートの基準にする脅威カテゴリを選択します。
4. 新しいレポート設定をテストするために **Run Now (今すぐ実行)** をクリックします。
5. **OK** をクリックしてレポートを保存します。

脅威シグネチャの詳細を把握

ファイアウォールの脅威ログは、脅威シグネチャ（アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップ）に基づいてファイアウォールが検知した脅威をすべて記録し、ACC がネットワークの上位の脅威についての概要を表示します。ファイアウォールが記録する各イベントには、関連する脅威シグネチャを特定する ID が含まれています。

脅威ログあるいは ACC エントリと共に見つかった脅威 ID を使用すれば、次のことが可能になります。

- 脅威シグネチャがセキュリティポリシーの例外として設定されているかどうか、簡単に確認（脅威例外の作成）。
- 特定の脅威に関する最新の Threat Vault の情報を見つける。Threat Vault はファイアウォールと統合されているため、ファイアウォール コンテキストで直に脅威に関する詳細を確認したり、新しいブラウザ ウィンドウで Threat Vault 検索を起動して、ファイアウォールがログに記録した脅威を確認したりすることができます。

シグネチャが無効化されている場合、新しいシグネチャに対してシグネチャ *UTID* が再利用される場合があります。

コンテンツ更新のリリースノートを読み、新規および無効化されたシグネチャに関する通知をご確認ください。対象のシグネチャが検出する行為を攻撃者が利用しなくなっている場合、対象のシグネチャが誤って許可するケースが多い場合、あるいは対象のシグネチャが他の類似のシグネチャと統合された（シグネチャの最適化）場合に、シグネチャが無効化されることがあります。

STEP 1 | ファイアウォールが Threat Vault に接続されていることを確認します。

Device（デバイス） > **Setup**（設定） > **Management**（管理）を選択し、**Logging and Reporting**（ロギングとレポート） 設定を編集して **Enable Threat Vault Access**（**Threat Vault** アクセスの有効化） を行います。Threat Vault へのアクセスはデフォルトで有効になっています。

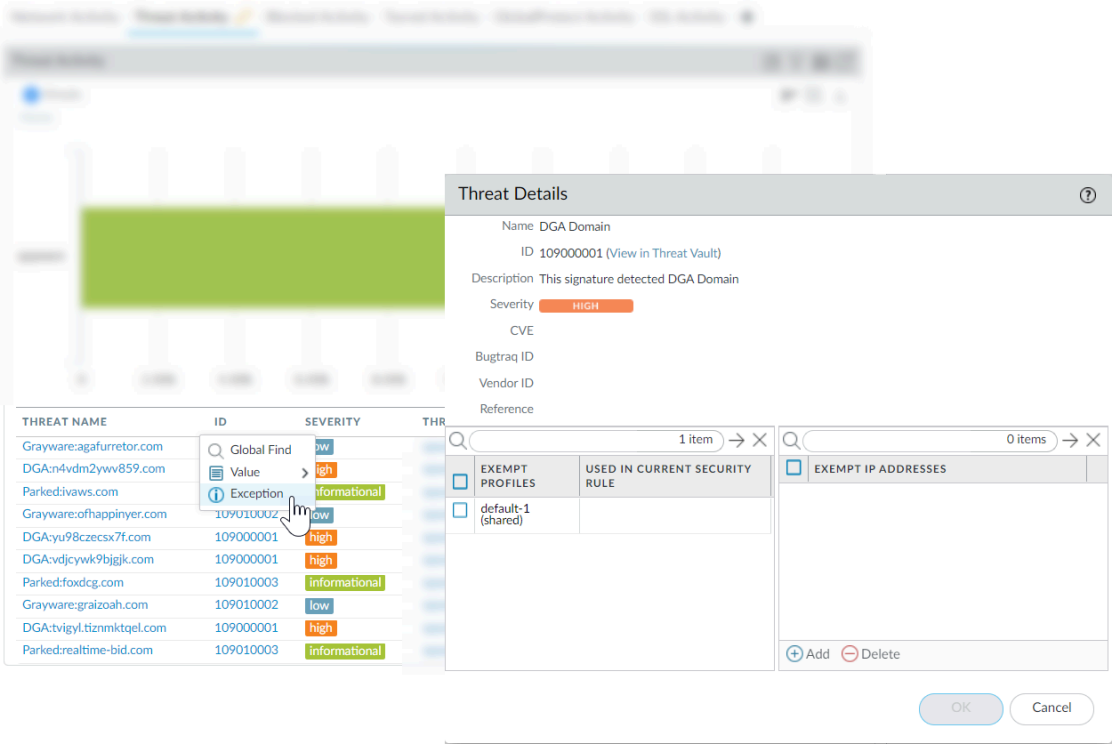
STEP 2 | ファイアウォールが検出した脅威の脅威 ID を探します。

- 脅威シグネチャに基づいてファイアウォールが検知する各脅威イベントを表示するには、**Monitor (**監視**)** > **Logs (**ログ**)** > **Threat (**脅威**)**を選択します。脅威エントリの ID は ID 列の一覧で確認したり、ログ エントリを選択し、脅威 ID を含むログの詳細を表示して確認したりできます。
- ネットワーク上の上位の脅威の概要を確認するには、**ACC** > **Threat Activity (**脅威アクティビティ**)** を選択し、Threat Activity (脅威アクティビティ) ウィジェットをチェックします。表示されている各脅威の脅威 IDが ID 列に表示されます。
- 脅威例外（つまり、その脅威シグネチャに対して定義されているデフォルトのアクションとは異なる方法でファイアウォールが脅威に対応）として設定できる脅威の詳細を表示するには、**Objects (**オブジェクト**)** > **Security Profiles (**セキュリティ プロファイル**)** > **Anti-Spyware/Vulnerability Protection (**アンチスパイウェア/脆弱性保護**)**を選択します。プロファイルを **Add (**追加**)** あるいは変更し、**Exceptions (**例外**)** タブをクリックして設定済みの

例外を表示します。例外が設定されていない場合、脅威シグネチャに基づいてフィルタリングしたり、**Show all signatures** (すべてのシグネチャを表示) を選択したりできます。

STEP 3 | **Threat Name** (脅威名) あるいは脅威 **ID** にカーソルを合わせてドロップダウンリストを開き、**Exception** (例外) をクリックし、脅威の詳細と、ファイアウォールがその脅威にどのように対処するよう設定されているのかを確認します。

例えば、ACC のチャートで上位の脅威に関する詳細を確認できます。



STEP 4 | その脅威に関する最新の **Threat Details** (脅威の詳細) を確認し、脅威 ID に基づいて Threat Vault 検索を起動します。

- 脅威の詳細表示には、脅威の最新の Threat Vault 情報、脅威を詳細に理解するために使用できるリソース、その脅威に関連する CVE が含まれています。
- Threat Vault 検索を新しいウィンドウで開き、Palo Alto Networks の脅威データベースに含まれている、この脅威シグネチャの最新情報を検索するには、**View in Threat Vault** (**Threat Vault** で表示) を選択します。

STEP 5 | 脅威シグネチャがセキュリティポリシーの例外として設定されているかどうか確認します。

- **Used in current security rule** (現在のセキュリティルールで使用中) 列が空である場合、ファイアウォールは推奨されるデフォルトのシグネチャ アクション（ブロックやアラートなど）に基づいて脅威に対処しています。
- **Used in current security rule** (現在のセキュリティルールで使用中) 列のどこかにチェックマークがある場合、セキュリティポリシー ルールが **Exempt Profiles** (除外プロファイル)

設定に基づき、その脅威用のデフォルト以外のアクション（許可など）を適用するように設定されていることが分かります。

Used in security rule column (セキュリティルール列で使用中**)** では、セキュリティポリシー ルールが有効かどうかは判断できません。分かるのはセキュリティポリシー ルールに脅威例外が設定されているかどうかのみです。指摘されたセキュリティポリシー ルールが有効になっているかどうか確認するには、***Policies (***ポリシー**) > Security (***セキュリティ**)** を選択します。

STEP 6 | 脅威例外をフィルタリングする IP アドレスを **Add (**追加**)** するか、既存の **Exempt IP Addresses** （除外 **IP** アドレス） を表示します。

関連するセッションがマッチする送信元あるいは宛先 IP アドレスを持っている場合のみ脅威例外を適用するには、除外する IP アドレスを設定します。その他のあらゆるセッションについては、デフォルトのシグネチャ アクションが脅威に適用されます。

ネットワーク トラフィックのための AutoFocus 脅威インテリジェンス

AutoFocusサブスクリプションがあれば、お客様のネットワーク内のアクティビティを、AutoFocusポータルで利用できる最新の脅威データと比較検討することができます。ファイアウォールとAutoFocusを接続することで次の機能を利用できるようになります。

- AutoFocus インテリジェンス サマリーで、ファイアウォールのログに記録されたセッションの分析結果を確認します。
- ファイアウォールのログにある分析結果を探す AutoFocus 検索を開きます。

AutoFocusインテリジェンス サマリーを使用すれば、お客様のネットワーク内あるいはグローバルなレベルでアーチファクトがどの程度蔓延しているのかが明らかになります。アーチファクトに対してリストアップされたAutoFocusタグとWildFire判定により、そのアーチファクトがセキュリティリスクを伴うかどうか判断できます。

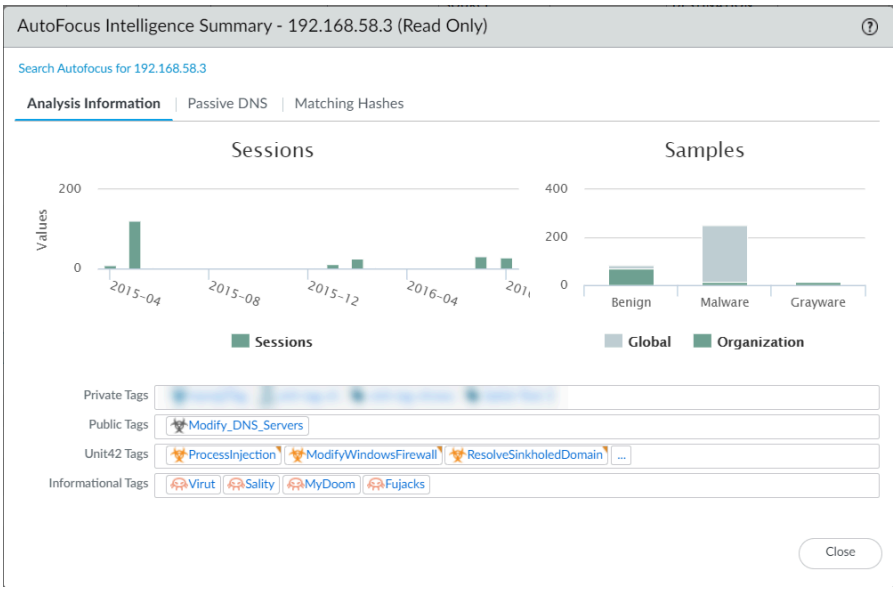
- AutoFocus インテリジェンス サマリー
- AutoFocus脅威インテリジェンスの有効化
- AutoFocus インテリジェンス サマリーのデータの表示と操作

また、***AutoFocus*** の結果に基づいてポリシーを適用することもできます:

- AutoFocus アーティファクト (IP アドレス、URL、およびドメイン) をエクスポートし、外部の動的リストで使用することもできます.
- AutoFocus マイナーを外部動的リストソースとして使用する.

AutoFocus インテリジェンス サマリー

AutoFocus インテリジェンス サマリーは、AutoFocus が 他のAutoFocus ユーザー、WildFire、PAN-DB URLフィルタリング データベース、Unit 42、およびオープンソースのインテリジェンスで収集した脅威インテリジェンスから抽出した成果物に関する情報の集中ビューを提供します。



AutoFocus インテリジェンス サマリー	
分析情報	分析情報のタブには、次の情報が表示されます 。 • セッション—ファイアウォールがアーティファクトに関連付けられたサンプルを検出したファイアウォールに記録されたセッション数。 • サンプル—アーティファクトに関連付けられ、WildFire の判定（良性、マルウェア、またはグレイウェア）でグループ化された組織サンプルとグローバル サンプルの比較。*Global*（グローバル）はすべての WildFire 送信のサンプルを意味します。一方、*organization*（組織）は組織が WildFire に送信するサンプルのみを意味します。 • 一致タグ—アーチファクトに一致する AutoFocus タグを表示します。AutoFocus タグはアーチファクトがマルウェアや 標的攻撃に関連していないかを表示します。
パッシブ DNS	Passive DNS（パッシブ DNS）タブには、アーチファクトを含むパッシブ DNS 履歴が表示されます。このパッシブ DNS 履歴は、AutoFocus のグローバル DNS インテリジェンスに基づいています。ネットワーク内の DNS アクティビティに限定されるものではありません。パッシブ DNS 履歴は以下から構成されます： • ドメイン リクエスト • DNS リクエストのタイプ • DNS リクエストで解決された IP アドレスまたはドメイン（プライベート IP アドレスは表示されません）。 • リクエストの作成回数

AutoFocus インテリジェンス サマリー	
	• リクエストが最初に表示された日時と最後に表示された日時
一致ハッシュ	一致ハッシュ タブには、最近検出された 5 つの一致するサンプルが表示されます。以下のようなサンプルがあります： • サンプルの SHA256 ハッシュ • サンプル ファイルのタイプ • WildFire がサンプルを分析して WildFire 判定を割り当てた日時 • サンプルの WildFire 判定 • WildFire がサンプルの WildFire 判定を更新した日時（該当する場合）

AutoFocus脅威インテリジェンスの有効化

AutoFocus ライセンスをアクティベートし、ファイアウォールが AutoFocus と通信できるようにします。セットアップが完了すると、ログまたは ACC アーティファクトのAutoFocus インテリジェンス サマリーを表示して、ネットワークおよび関連する脅威でのその拡散性を評価できます。

STEP 1 | AutoFocusライセンスがファイアウォール上でアクティベーションされていることを確認します。

1. **Device (デバイス)** > **Licenses (ライセンス)** の順に選択して、AutoFocus デバイス ライセンスがインストールされており、有効であることを確認します（有効期限をチェックします）。
2. firewallにライセンスが表示されない場合は、サブスクリプション ライセンスのアクティベーションしてください。

STEP 2 | ファイアウォールをAutoFocusに接続します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択し、AutoFocus 設定を編集します。
2. **AutoFocus URL**を入力します：

   `https://autofocus.paloaltonetworks.com:10443`
3. **Query Timeout**[クエリ タイムアウト]欄を使用し、ファイアウォールがAutoFocusに対し脅威インテリジェンスデータのクエリを行う際の試行継続時間を設定しま

す。AutoFocusポータルが指定した時間内に応答しない場合、ファイアウォールは接続を切断します。

クエリ タイムアウト値はデフォルトの*15*秒のままにしておくことをお勧めいたします。この時間中に処理が完了するよう、*AutoFocus*クエリが最適化されます。

4. **Enabled**[有効]を選択し、ファイアウォールがAutoFocusに接続できるようにします。
5. **OK** をクリックします。
6. 変更内容を**Commit**[コミット]し、再起動後もAutoFocus設定が維持されるようにします。

STEP 3 | AutoFocusをファイアウォールに接続します。

1. AutoFocusポータルにログインします。https://autofocus.paloaltonetworks.com
2. **Settings**[設定]を選択します。
3. 新規リモートシステムを**Add new**[追加]します。
4. ファイアウォールを識別できる分かりやすい**Name**[名前]を入力します。
5. System Type[システム タイプ]　として **PanOS**を選択します。
6. ファイアウォールのIP **Address**[IPアドレス]を入力します。
7. **Save changes**[変更内容を保存]をクリックしてそのリモートシステムを追加します。
8. Settings [設定]ページで再び**Save changes**[変更内容を保存]をクリックし、ファイアウォールが正しく追加されたことを確認します。

STEP 4 | ファイアウォールとAutoFocusの接続をテストします。

1. ファイアウォールで **Monitor (**監視**)** > **Logs (**ログ**)** > **Traffic (**トラフィック**)** を選択します。
2. AutoFocus でファイアウォール分析結果を評価できることを確認します。

AutoFocus インテリジェンス サマリーのデータの表示と操作

AutoFocus インテリジェンス サマリーとやり取りしてアーチファクトについての詳細情報を表示したり、アーチファクトの範囲を AutoFocus まで広げたりできます。AutoFocus タグは、アーチファクトが特定のタイプのマルウェアあるいは不審な挙動に関連しているかどうかを明らかにします。

STEP 1 | ファイアウォールが AutoFocus に接続されていることを確認します。

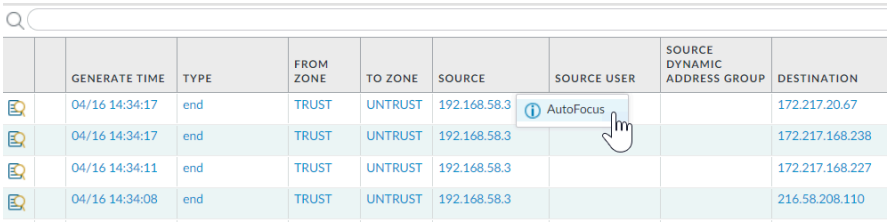
ファイアウォール上で AutoFocus脅威インテリジェンスの有効化を行います（アクティブな AutoFocus 脅威インテリジェンスが必要）。

STEP 2 | 調査するアーチファクトを探します。

次のタイミングで、アーチファクトについての AutoFocus インテリジェンス サマリーを表示できます。

- ログの表示（トラフィック、脅威、URL フィルタリング、WildFire への送信、データ フィルタリング、統合ログのみ）
- 外部動的リスト エントリを表示します。

STEP 3 | アーチファクトにカーソルを合わせてドロップダウンリストを開き、**AutoFocus** をクリックします。



AutoFocus インテリジェンス サマリーは、次のタイプのアーチファクトでのみ利用できます。

IPアドレス

URLプロテクションの

ドメイン

ユーザー エージェント

脅威名（サブタイプ ウイルスおよび WildFire ウイルスの脅威のみ）

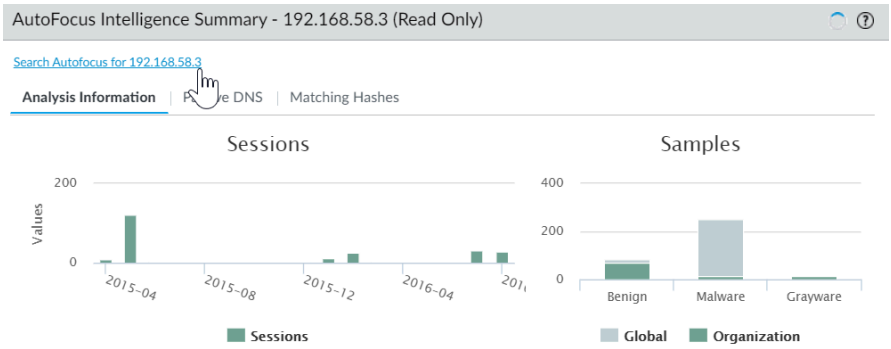
ファイル名

SHA-256ハッシュ

STEP 4 | AutoFocus 検索を起動し、開いた AutoFocus インテリジェンス サマリーの対象であるアーチファクトを検索します。

「AutoFocus インテリジェンス サマリー」ウィンドウの上部にある **Search AutoFocus for...** (次を対象にして **AutoFocus** を検索...) リンクをクリックします。検索結果には、そのアーチファクトに関連するサンプルがすべて含まれています。**My Samples** (マイサンプル) および

All Samples (すべてのサンプル**)** タブを切り替えつつ、サンプル数を比較して組織内のアーチファクトの浸透率を判断します。



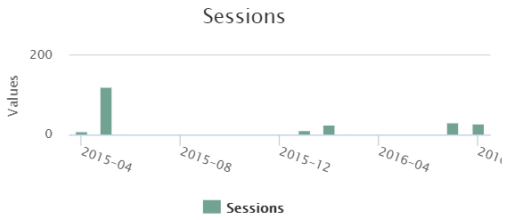
STEP 5 | AutoFocus 検索を起動し、AutoFocus インテリジェンス サマリーの他のアーチファクトを検索します。

次のアーチファクトをクリックし、組織内でそれらがどの程度普及しているのか判断します。

- Analysis Information (分析情報) タブ内の WildFire 判定
- Passive DNS (パッシブ DNS) タブ内の URL および IP アドレス
- Matching Hashes (一致するハッシュ) タブ内の SHA256 ハッシュ

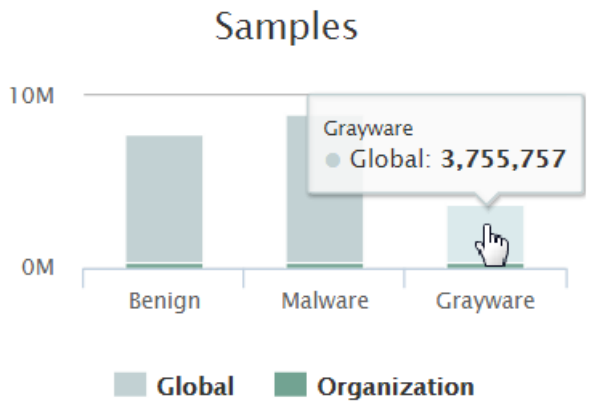
STEP 6 | 組織内のアーチファクトに関連するセッション数を月毎に表示します。

セッションのバーにカーソルを合わせます。



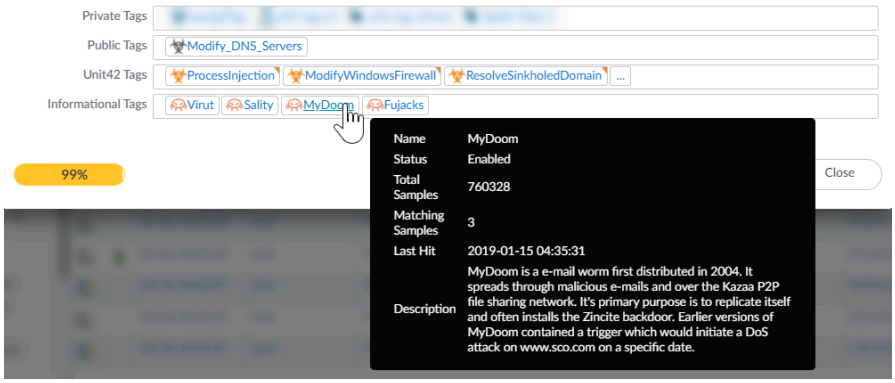
STEP 7 | アーチファクトに関連するサンプル数をスコープおよび WildFire 判定に基づいて表示します。

サンプルのバーにカーソルを合わせます。



STEP 8 | マッチする AutoFocus タブの詳細を表示します。

マッチするタグにマウス カーソルを移動すると、そのタグの説明や他のタグの詳細が表示されます。



STEP 9 | マッチするタグに関連するその他のサンプルを表示します。

一致タグをクリックすると、そのタグの AutoFocus 検索が起動します。検索結果には、タグにマッチしたサンプルがすべて含まれています。

Unit 42 タグは、直接的なセキュリティ リスクを引き起こす脅威やキャンペーンを識別します。Unit 42 一致タグをクリックすると、タグによって特定されるその脅威に関連するサンプルが、組織内にどの程度あるのか確認できます。

STEP 10 | アーチファクトに一致するタグをさらに見つけます。

アーチファクトに対する AutoFocus 検索を起動します。検索結果の Tags (タグ) 列にはアーチファクトの一致タグの詳細が表示され、頻繁にアーチファクトが検知される他のマルウェア、不審な挙動、脅威を及ぼすもの、エクスプロイト、キャンペーンを把握できます。

脅威インテリジェンスを Palo Alto Networks と共有

テレメトリーは、分析用のデータの収集と送信を行うプロセスです。ファイアウォールでテレメトリーを有効にすると、ファイアウォールは、アプリケーション、脅威、デバイスの安全状態に関する情報を含むデータを定期的に収集し、Palo Alto Networks に送信します。脅威インテリジェンスを共有することには、次のようなメリットがあります。

- ご自身や世界中のお客様に、強化された脆弱性およびスパイウェア シグネチャを提供。例えば、脅威イベントが脆弱性あるいはスパイウェア シグネチャをトリガーする際、ファイアウォールがその脅威に関連する URL を Palo Alto Networks 脅威リサーチ チームと共有し、その URL を悪意があるものとして適切に分類できるようになります。
- ネットワークに一切影響を与えることなく試験的な脅威シグネチャを素早くテスト・評価することで、すべての Palo Alto Networks のお客様に不可欠な脅威防止を素早く提供可能。
- PAN-DB URL フィルタリング、DNS ベースのコマンドアンドコントロール （C2）シグネチャ、および WildFire 内の精度とマルウェア検出機能が向上。

Palo Alto Networks は、テレメトリーから抽出された脅威インテリジェンスを使用して、これらのメリットをご自身や他の Palo Alto Networks のお客様に提供します。各ユーザーが共有するテレメトリーデータにより、すべての Palo Alto Networks ユーザーがメリットを得ます。テレメトリーはコミュニティ駆動の、脅威を阻止するためのアプローチです。Palo Alto Networks はユーザーのデータを他のお客様またはサードパーティ組織と共有しません。

テレメトリの利点、使用法、構成など、テレメトリの詳細については、「デバイスのテレメトリ」を参照してください。

脅威防御リソース

脅威防御のベストプラクティスに関する詳細は、以下の資料を参照してください：

- Creating Custom Threat Signatures（英語）
- ネットワークをレイヤー 4 およびレイヤー 7 回避から保護するためのベスト プラクティス
- URL フィルタリングのベストプラクティス
- ゼロトラストのベストプラクティス
- DoS およびゾーン プロテクションのベストプラクティス

Palo Alto Networks 製品で識別可能な脅威およびアプリケーションのリストを参照するには、以下のリンクを使用してください。

- Applipedia — Palo Alto Networks で識別できるアプリケーションについて詳細に説明しています。
- Threat Vault — Palo Alto Networks 製品で識別可能な脅威の一覧が掲載されています。脆弱性、スパイウェア、またはウイルスを条件にして検索できます。脅威についての詳細は、ID 番号の横にある詳細アイコンをクリックしてください。

復号

Palo Alto Networks のファイアウォールは、トラフィックを復号化および検査して脅威に対する可視性を確保し、プロトコル、検証、エラーのハンドリングを制御します。復号化は、ファイアウォールが設定済みのセキュリティ設定に従う形で暗号化されたトラフィックに対応できるよう、ポリシーを暗号化されたトラフィックに適用します。トラフィックを復号化すれば、悪意あるコンテンツのネットワークへの侵入や、機密コンテンツが暗号化されたトラフィックとして隠ぺいされてネットワーク外に流出することを防ぐことができます。復号化を有効にする手順には、復号化に必要な鍵および証明書の用意、復号化プロファイルおよびポリシーの作成、復号ポート ミラーリングの設定が含まれます。

復号の概要

SSL（Secure Sockets Layer）および SSH（Secure Shell）暗号化プロトコルは、2 つのエンティティ間（Web サーバーとクライアントなど）のトラフィックを安全に保護します。SSL および SSH はトラフィックをカプセル化し、データを暗号化します。これにより、データを復号化するキーとデバイス間の信頼を確立する証明書を持つクライアントとサーバー以外のエンティティにとって、データは意味のないものになります。次の目的で SSL および SSH トラフィックを復号化します：

- 暗号化されたトラフィックに隠れたマルウェアがネットワークに侵入するのを防ぎます。例えば、SSL 暗号化を使用するウェブサイトに攻撃者が侵入するとします。従業員がそのウェブサイトにアクセスし、知らないうちにエクスプロイトやマルウェアをダウンロードします。その後、マルウェアは感染した従業員のエンドポイントを使ってネットワーク内を横方向に移動し、他のシステムに侵入します。
- センシティブな情報がネットワークの外部に流出するのを防ぎます。
- 安全なネットワーク上で適切なアプリケーションが実行されていることを確認する。
- トラフィックを選択的に復号化します。例えば、金銭あるいはヘルスケアを扱うトラフィックを復号化から除外する復号化ポリシーおよびプロファイルを作成します。

Palo Alto Networks のファイアウォールの復号化はポリシーベースで、インバウンドとアウトバウンドの SSL および SSH 接続を復号化、検査、制御できます。復号化ポリシーにより、宛先、送信元、サービス、あるいは URL カテゴリ毎に復号化するトラフィックを指定したり、関連する復号化プロファイルのセキュリティ設定に従って特定のトラフィックをブロック、制限、転送したりすることができます。復号化プロファイルは SSL プロトコル、証明書の検証、エラーチェックを制御し、弱いアルゴリズムやサポートされていないモードを使用するトラフィックがネットワークにアクセスするのを防ぎます。ファイアウォールは、証明書とキーを使用してトラフィックをプレーンテキストに復号化し、次に App-ID およびセキュリティ設定（復号化、アンチウイルス、脆弱性、アンチスパイウェア、URL フィルタリング、WildFire、ファイル ブロッキングなどのプロファイル）をプレーンテキスト トラフィックに適用します。トラフィックの復号化と検査を行った後、プレーンテキスト トラフィックはファイアウォールを出るときにファイアウォールによって再暗号化され、プライバシーとセキュリティが確保されます。

ファイアウォールが提供する復号化ポリシー ルールには 3 つのタイプがあります：アウトバウンド SSL トラフィックを制御するSSL 転送プロキシ、インバウンド SSL トラフィックを制御するSSL インバウンド インスペクション、トンネル化された SSH トラフィックを制御するSSH プロキシです。復号化プロファイルをポリシールールに付与し、サーバー証明書、サポートされていないモード、エラーのチェックなど、細かなアクセス設定をトラフィックに適用できます。

SSL 復号化（転送プロキシおよびインバウンド インスペクションの両方）がファイアウォールを信頼できるサードパーティとして確立する際、また SSL/TLS 接続を保護するためにクライアントおよびサーバー間の信頼を確立する際に、証明書が必要になります。また、技術的な理由（証明書のピンニング、サポートされていない暗号、相互認証などの理由で復号化を妨げるサイト）でサーバーを SSL 復号化から除外する際も、証明書を使用します。SSH 復号化では証明書は必要ありません。

復号化のベストプラクティスのチェックリストを使って復号化のデプロイメントの計画、実装、保守を行います。

ハードウェア セキュリティ モジュール（HSM）をファイアウォールと統合すると、SSL フォワード プロキシ復号化および SSL インバウンド インスペクション復号化で使用される秘密鍵のセキュリティを強化できます。HSM を使用したキーの保存と生成、および HSM とファイアウォールの統合については、ハードウェア セキュリティ モジュールによるキーの安全確保を参照してください。

Decryption Mirroring を使用して、復号化されたトラフィックをプレーンテキストとしてサードパーティのソリューションに転送し、追加の分析とアーカイブを行うこともできます。

Decryption ミラーリングを有効にする場合は、機密情報を含むすべてのミラー化されたトラフィックが平文で転送されるため、ミラーリングできるトラフィックと、トラフィックをどこに、どのように保存できるかについて、地域の法律や規制に注意してください。

復号化の概念

復号化機能とサポートの詳細については、次のトピックを参照してください：

- 復号ポリシーのためのキーおよび証明書
- SSL 転送プロキシ
- SSL 転送プロキシの復号化プロファイル
- SSL インバウンド インスペクション
- SSL インバウンド インスペクション 復号化プロファイル
- SSL プロトコル設定 復号化プロファイル
- SSH プロキシ
- SSH プロキシ復号化プロファイル
- 復号化なしの復号化プロファイル
- 楕円曲線暗号（ECC）証明書用の SSL 復号化
- SSL 復号化のための Perfect Forward Secrecy（PFS）
- SSL 復号化とサブジェクト代替名（SAN）
- TLSv1.3復号
- 復号化されたセッションの高可用性サポート
- 復号化ミラーリング

復号ポリシーのためのキーおよび証明書

キーは数字列で、通常、ランダムな数字と大きな素数を使用した数学演算によって生成されます。キーは、暗号化されていないプレインテキストから暗号化された暗号文へ、暗号化された暗号文から暗号化されていないプレインテキストへと、文字列（パスワード、共有シークレットなど）を変換します。キーには対称キー（暗号化と復号化に同じキーを使用）と非対称キー（1 つのキーを暗号化に使用し、数学的に関連するキーを復号化に使用）があります。キーはあらゆるシステムで生成できます。

X.509 証明書は、クライアントとサーバーの間の信頼を構築し、SSL 接続を確立します。サーバーを認証するクライアント（またはクライアントを認証するサーバー）は、X.509 証明書の構造を知っているため、証明書内のフィールドから、FQDN や IP アドレス（証明書内では共通名または *CN* と呼ばれます）、または証明書が発行された組織、部門、ユーザーの名前など、サーバーに関する識別情報を抽出する方法を知っています。すべての証明書を認証局（CA）が発行する必要があります。CA はクライアントまたはサーバーを確認した後、証明書を発行し、秘密鍵を使用して署名します。

同じサブジェクトとキーを持つ *2* つの *CA*（***Device***（デバイス）> ***Certificate Management***（証明書管理）> ***Device Certificates***（デバイス証明書））があり、*1* つの *CA* の有効期限が切れている場合は、（カスタム）または期限切れの *CA* を無効（事前定義）にします。有効期限が切れた *CA* を削除または無効にしない場合、信頼できるチェーンで有効になっていると、ファイアウォールによって有効期限が切れた *CA* へのチェーンが構築され、ブロックページが表示されます。

復号化ポリシーをトラフィックに適用する際、サーバー証明書に署名した CA をファイアウォールが信頼する場合のみ、クライアントとサーバーの間でセッションが確立されます。信頼を確立するには、サーバーのルート CA 証明書がファイアウォールの証明書信頼リスト（CTL）内にあり、ファイアウォールがそのルート CA 証明書に含まれる公開鍵を使用して署名を確認する必要があります。その後、ファイアウォールは、フォワード トラスト証明書によって署名されたサーバー証明書のコピーを認証のためにクライアントに提示します。また、SSL フォワード プロキシのフォワード トラスト証明書としてエンタープライズ CA を使用するようにファイアウォールを設定することもできます。ファイアウォールの CTL にサーバーのルート CA 証明書が含まれていない場合、ファイアウォールは、フォワード アントラスト証明書によって署名されたサーバー証明書のコピーをクライアントに提示します。フォワード アントラスト証明書を使用すると、信頼されない証明書を持つサーバーがホストするサイトにクライアントがアクセスしたときに、サーバー証明書の警告画面が表示されます。

証明書の詳細は、証明書の管理を参照してください。

ファイアウォールが信頼する *CA* を管理するには、ファイアウォールの *Web* インターフェイスで、***Device (***デバイス*) > Certificate Management (***証明書管理*) > Certificates (***証明書*) > Default Trusted Certificate Authorities (***デフォルトの信頼された証明機関*)*** タブを使用します。

次の表は、Palo Alto Networks のファイアウォールが復号化に使用するさまざまなキーや証明書について説明しています。

復号化と併せて使用される証明書	説明
フォワード トラスト（SSL フォワード プロキシ復号化に使用）	クライアントが接続しようとしているサイトの証明書がファイアウォールが信頼する CA によって署名されている場合に、ファイアウォールが復号化通信開始時にクライアントに提示する証明書。信頼できるCAによってサーバー証明書が署名されている場合にファイアウォールがクライアンに提示するフォワード トラスト証明書を設定する方法については、SSL フォワード プロキシの設定を参照してください。 ファイアウォールは、デフォルトで、宛先サーバーの鍵のサイズに基づいてクライアント証明書で使用する鍵のサイズを決定します。しかし、SSL プロキシ サーバーの証明書の鍵のサイズの設定を行うことができます。セキュリティをさらに向上させるために、フォワード トラスト証明書に関連する秘密鍵をハードウェア セキュリティ モジュール上に保存することを検討してください（HSM での秘密鍵の保存を参照）。

復号化と併せて使用される証明書	説明
	ファイアウォールのフォワード トラスト *CA* 証明書に紐付いた秘密鍵（ファイアウォールのマスターキーではなく）を安全な場所にバックアップし、ファイアウォールに問題が発生しても、フォワード トラスト *CA* 証明書にアクセスできる状態を保ちます。セキュリティをさらに向上させるために、フォワード トラスト証明書に関連する秘密鍵をハードウェア セキュリティ モジュール上に保存することを検討してください（HSM での秘密鍵の保存を参照）。
フォワード アントラスト（SSL フォワード プロキシ復号化に使用）	クライアントが接続しようとしているサイトの証明書がファイアウォールが信頼しない CA によって署名されている場合に、ファイアウォールが復号化中にクライアントに提示する証明書。ファイアウォール上のフォワード アントラスト証明書を設定するには、SSL フォワード プロキシの設定を参照してください。
SSL インバウンド インスペクション	ネットワーク上のサーバーに向かうトラフィックの SSL インバウンド インスペクションを実行したいサーバーの証明書。サーバー証明書をファイアウォールにインポートします。

復号化と併せて使用される証明書	説明
	PAN-OS 8.0 から、ファイアウォールが楕円曲線 *Diffie-Hellman Ephemeral (ECDHE)* アルゴリズムを使用して厳格な証明書チェックを行うようになっています。つまり、ファイアウォールが中間証明書を使用する場合、*PAN-OS 8.0* 以降のリリースにアップグレードした後、*WEB* サーバーからファイアウォールに証明書をインポートし直し、サーバー証明書と中間証明書を組み合わせる必要があります *(*チェーン証明書をインポートします*)*。そうしなければ、チェーン中に中間証明書が存在する場合に *SSL* インバウンド インスペクションが失敗します。チェーン証明書をインストールするには： **1.** メモ帳などのテキスト エディタで各証明書 *(.cer)* ファイルを開きます。 **2.** サーバー証明書の後に各署名者が続くようにして、それぞれの証明書を最初から最後までペーストします。 **3.** ファイルをテキスト *(.txt)* あるいは証明書 *(.cer)* ファイルとして保存します *(*ファイル名にはスペースを含められません*)*。 **4.** 組み合わせた *(*チェーン*)* 証明書をファイアウォールにインポートします。

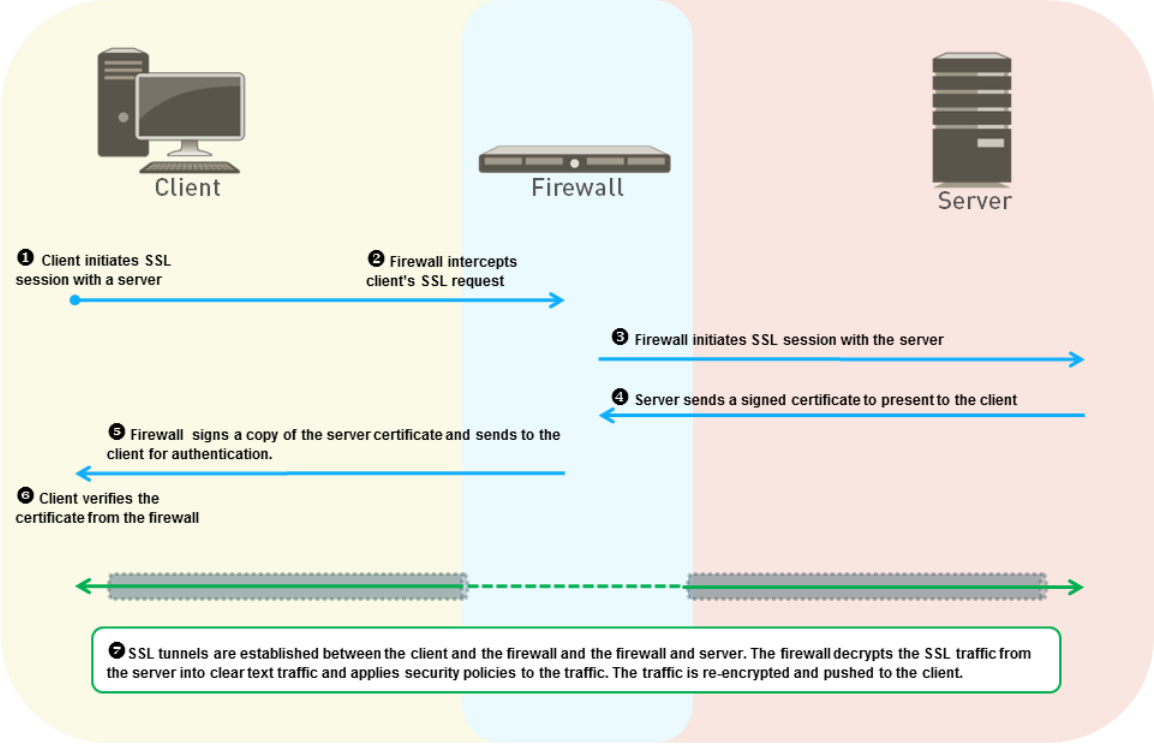
SSL 転送プロキシ

外部サイトに送信される SSL トラフィックを復号化するようにファイアウォールを設定すると、ファイアウォールはフォワード プロキシとして機能します。SSL フォワード プロキシ復号ポリシーを使用すると、内部ユーザーから Web への SSL/TLS トラフィックを復号化および検査できます。SSL フォワード プロキシ復号化はトラフィックを復号化し、ファイアウォールが復号化プロファイル、セキュリティ ポリシー、プロファイルをトラフィックに適用できるようにすることで、SSL で暗号化されたトラフィックに隠れたマルウェアが企業ネットワークに侵入するのを防ぎます。

SSL フォワード プロキシ復号化では、ファイアウォールが内部クライアントと外部サーバーの間に入ります。ファイアウォールは証明書を使い、サーバーに対して透過的にクライアントの、またクライアントに対して透過的にサーバーの代理となるため、クライアントはサーバーと直接通信しているとみなし（しかし、クライアントのセッションはファイアウォールとのもの）、ま

たサーバーはクライアントと直接通信しているとみなします（しかし、サーバーのセッションはファイアウォールとのもの）。ファイアウォールは証明書を使用して、クライアント-サーバー間の信頼されたサード パーティ（中間者）になります（証明書の詳細は、復号ポリシーのためのキーおよび証明書を参照）。

次の図は、このプロセスを詳細に示しています。SSL フォワード プロキシの設定の詳細は、SSL フォワード プロキシの設定を参照してください。



1. ネットワーク上の内部クライアントは、外部サーバーとの TLS セッションを開始しようと試みます。
2. ファイアウォールはクライアントの SSL 証明書要求をインターセプトします。安全なセッションが実際のサーバーではなくファイアウォールとの間で確立されているものの、ファイアウォールはクライアントに対して外部サーバーとして動作します。
3. その後、ファイアウォールはクライアントの SSL 証明書リクエストをサーバーに転送し、サーバーとのセッションを別途開始します。サーバーからはファイアウォールがクライアントのように見え、サーバーは中間者がいることを知らず、証明書の有効性を認めます。
4. サーバーは、クライアントに宛てた署名済みの証明書をファイアウォールに送信します。
5. ファイアウォールはサーバー証明書を分析します。ファイアウォールが信頼する CA によって署名され、設定済みのポリシーおよびプロファイルを満たすサーバー証明書であれば、ファイアウォールはそのサーバー証明書の SSL フォワード トラストのコピーを取り、それをクライアントに送信します。サーバー証明書が、ファイアウォールが信頼しない CA によって署名されていた場合、ファイアウォールはサーバー証明書の SSL フォワード アントラストのコピーを生成し、それをクライアントに送信します。ファイアウォールが生成してクライアントに送信する証明書のコピーには、元のサーバー証明書の拡張が含まれており、またそれは実際のサーバー証明書ではないため、*impersonation* (疑似)証明書と呼ばれます。ファイアウォールがサーバーを信頼しない場合、クライアントでは、接続しようとしているサイトが

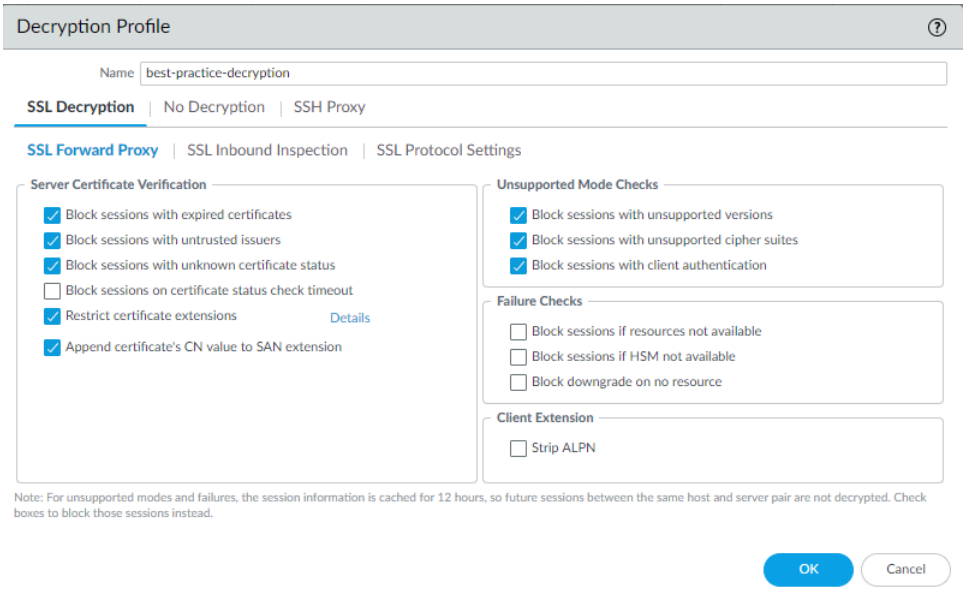
信頼されていないというブロック ページの警告メッセージが表示され、SSL 復号化のオプトアウトをユーザーに許可している場合は、クライアントはアクセスを続行するかセッションを終了するかを選択できます。

6. クライアントはファイアウォールの疑似証明書を検証します。その後、クライアントはサーバーとセッション キーの交換を始めますが、そこでもファイアウォールが証明書の場合と同様にプロキシとして機能します。ファイアウォールはクライアント キーをサーバーに送信し、クライアントのためにサーバー キーの疑似コピーを取ります。そこではファイアウォールが「目に見えない」プロキシの状態を保ち、クライアントおよびサーバーはお互いにセッションを確立していると信じますが、まだ 2 つの異なるセッション（一つはクライアントとファイアウォール間、もう一つはファイアウォールとサーバー間）が保たれています。これで、すべての関係者が必要な証明書とキーを持ち、ファイアウォールがトラフィックを復号化できる状態になります。
7. すべての SSL セッション トラフィックは、クライアントおよびサーバー間で透過的にファイアウォールを経由します。ファイアウォールは SSL トラフィックを復号化し、セキュリティ ポリシー、プロファイル、復号化プロファイルをトラフィックに適用し、トラフィックを再び暗号化してからさらに転送します。

SSL フォワード プロキシを設定すると、プロキシされたトラフィックは *DSCP* コード ポイントまたは *QoS* をサポートしません。

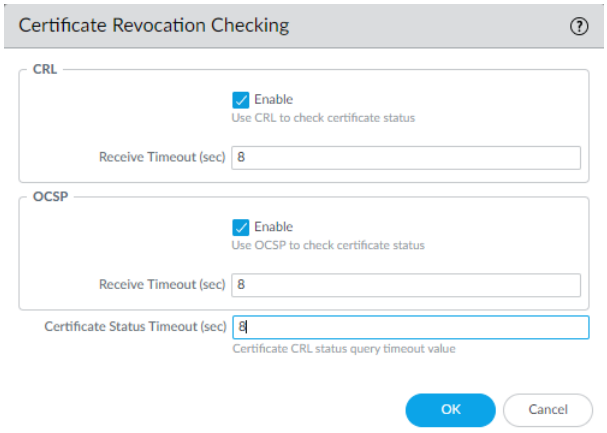
SSL 転送プロキシの復号化プロファイル

SSLフォワード プロキシの復号化プロファイル（**Objects (オブジェクト)** > **Decryption Profile (復号プロファイル)** > **SSL Decryption (SSL復号化)** > **SSL Forward Proxy (SSL** フォワードプロキシ**)**）は、プロファイルを付与するフォワードプロキシ復号化ポリシーで定義されている、アウトバウンド SSL/TLS トラフィックのサーバー検証、セッション モード チェック、およびエラーチェックを制御します。以下の図は、フォワードプロキシの復号プロファイル設定の一般的な推奨ベストプラクティスを示していますが、企業のセキュリティ関連のコンプライアンスルールや現地の法律、規制によっても設定が変わってきます。また、インターネット ゲートウェイ復号化プロファイルおよびデータセンター復号化プロファイルの具体的なベストプラクティスもあります。



サーバー証明書の確認：

- **Block sessions with expired certificates** (証明書が失効したセッションをブロック)—必ずこのボックスにチェックを入れ、失効した証明書を持つサーバーのセッションをブロックし、安全でない可能性のあるサイトへのアクセスを禁止してください。このボックスにチェックを入れなければ、ユーザーが悪意のある可能性のあるサイトに接してトランザクションを行うことができ、接続時に警告メッセージが表示されるものの、接続は拒否されません。
- **Block sessions with untrusted issuers** (発行者を信頼できないセッションをブロック)—必ずこのボックスにチェックを入れ、信頼できない証明書を持つサーバーのセッションをブロックしてください。信頼できない発行者は、UnTrust、リプレイ攻撃、その他の攻撃を行う可能性があります。
- 未知の証明書ステータスを持つセッションをブロック—サーバーの証明書失効状態から「unknown」のステータスが返ると、SSL/TLS セッションをブロックします。証明書ステータスは複数の理由で未知になることがあるため、一般的な復号化のセキュリティについては、このボックスにチェックを入れるとセキュリティが過剰になります。しかし、データセンターなどのセキュリティが強いネットワーク領域では、このボックスにチェックを入れることが合理的です。
- 証明書のステータスチェックがタイムアウトした際にセッションをブロック—強固なセキュリティと優れたユーザーエクスペリエンスのトレードオフになるため、ステータスチェックがタイムアウトした際にセッションをブロックするかどうかは、企業のセキュリティ コンプライアンスの内容によります。証明書ステータスの検証は、無効化サーバーの証明書無効リスト（CRL）を調べるか、あるいは発行者である CA が証明書を取り消し、証明書を信頼できないかどうかをオンライン証明書ステータス プロトコル（OCSP）を使って判断します。しかし、証明書が有効な場合でも、無効化サーバーの応答が遅く、セッションのタイムアウトにつながり、ファイアウォールがセッションをブロックしてしまう可能性があります。**Block sessions on certificate status check timeout** (証明書ステータスのチェックがタイムアウトした際にセッションをブロック)し、無効化サーバーの応答が遅い場合、**Device** (デバイス) > **Setup** (セットアップ) > **Session** (セッション) > **Decryption Settings** (復号化設定)を使用し、**Certificate Revocation Checking** (証明書失効チェック)をクリックすることで、デフォルトのタイムアウト値（5 秒）を別の値に変更できます。例えば、次の図のように、タイムアウト値を 8 秒に増やすこともできます。サーバー証明書は CRL Distribution Point（CDP）拡張子内に CRL URL を、認証機関アクセス情報（AIA）証明書拡張子内に OCSP URL を含んでいる可能性があるため、CRL および OCSP 証明書の失効チェックの両方を有効化してください。



- 証明書の拡張を制限—このボックスにチェックを入れると、サーバー証明書内の証明書の拡張が key usage および extended key usage に制限され、その他の拡張を持つ証明書がブロックされます。しかし、特定のデプロイ環境では他の証明書の拡張が必要になる場合があるため、他の証明書の拡張が必要でないデプロイ環境でのみこのボックスにチェックを入れてください。
- 証明書の **CN** 値を **SAN** 拡張に追加—このボックスにチェックを入れると、サブジェクト代替名（SAN）を使用するためにブラウザがサーバー証明書を求め、共通名（CN）に基づいてマッチする証明書をサポートしていない際、証明書が SAN 拡張を持っていない場合でも、ファイアウォールが SAN 拡張を（CN に基づいて）疑似（impersonation）証明書に追加するため、ユーザーはリクエストしたウェブ リソースにアクセスできます。

サポートされていないモード チェック。モードがサポート対象外であるセッションをブロックしない場合、安全でない可能性のあるサーバーに接続する際にユーザーに警告メッセージが届き、そのメッセージ内でクリックしながら進めることで、危険である可能性があるサイトにアクセスできるようになります。これらのセッションをブロックすることで、脆弱でリスクのあるプロトコル バージョンやアルゴリズムを使うサーバーに対して保護することができます：

- サポートされていないバージョンのセッションをブロックする - SSL プロトコル設定 復号化プロファイルを構成するときに、脆弱なプロトコルをブロックして攻撃対象領域を縮小できるように、ネットワーク上で SSL プロトコルの最小バージョンを指定します。必ずこのボックスにチェックを入れ、サポートしないことにした脆弱な SSL/TLS プロトコル バージョンを持つセッションをブロックしてください。
- サポートしていない暗号スイートのセッションをブロック—必ずこのボックスにチェックを入れ、ハンドシェイクで指定された暗号スイートをファイアウォールがサポートしていない場合にセッションをブロックするようにしてください。復号化プロファイルの**SSL Protocol Settings (SSL** プロトコル設定**)**タブで、ファイアウォールにサポートさせるアルゴリズムを設定します。
- クライアント認証を伴うセッションをブロック—ファイアウォールはクライアント認証を必要とするセッションを復号化できないため、クライアント認証が必要な重要なアプリケーションがない場合は、それをブロックしてください。ファイアウォールが双方向の復号化をする際、クライアントおよびサーバー証明書の両方が必要になりますが、クライアント認証が付属していると、ファイアウォールはサーバー証明書しか認識しません。そのため、クライアント認証を伴うセッションの復号化が妨げられます。このボックスにチェックを入れると、ファイアウォールはSSL復号化除外リスト（**Device (**デバイス**)** > **Certificate Management (**証明書管理**)** > **SSL Decryption Exclusion (SSL**復号化除外）に含まれるサイトからのセッションを除き、クライアント認証を伴うすべてのセッションをブロックします。

  クライアント認証でセッションをブロックするを使用しない場合、ファイアウォールがクライアント認証を使用するセッションを復号化しようとすると、ファイアウォールはセッショ

ンを許可し、サーバーのURL/IPアドレス、アプリケーション、およびDecryptionプロファイルを含むエントリをローカル復号化例外キャッシュに追加します。

クライアント認証を使用し、*SSL*復号化除外リストの事前定義済みサイトにないサイトからのネットワーク上のトラフィックを許可する必要がある場合があります。クライアント認証を伴うセッションを許可する復号化プロファイルを作成してください。アプリケーションをホストするサーバーにのみ適用する復号ポリシー ルールに、それを追加します。ログイン作業を完了するために多要素認証をユーザーに求めれば、セキュリティをさらに向上します。

失敗のチェック：

- リソースを使用できない場合にセッションをブロック—ファイアウォール処理リソースが利用できない時にセッションをブロックすると、ファイアウォールはトラフィックを復号化するためのリソースがない時にトラフィックをドロップします。リソースが不足しているためにファイアウォールが復号化を処理できない時にセッションをブロックしない場合、復号化したいトラフィックは暗号化されたままネットワークに入るため、検査されません。しかし、リソースを利用できない時にセッションをブロックすると、ユーザーが通常時にアクセスできるサイトが一時的にアクセス不可になるため、ユーザーエクスペリエンスが低下する可能性があります。このエラーチェックを実装するかどうかは、セキュリティ コンプライアンスの内容や、強固なセキュリティと比べてユーザーエクスペリエンスがどの程度重要かによって異なります。あるいは、復号化できるトラフィックを増やすために、処理能力の高いファイアウォール モデルを使用することをご検討ください。
- **HSM** を利用できない場合にセッションをブロック—ハードウェア セキュリティ モジュール（HSM）を使用して秘密鍵を保存する場合、使用するかどうかは、秘密鍵の取得元の制限、および HSM を利用できない場合に暗号化されたトラフィックをどのように扱うのかを定めるコンプライアンス規則によって異なります。例えば、秘密鍵の署名に HSM を使うことを求める企業は、HSM が利用できない場合にセッションをブロックします。しかし、これに関してそこまで厳重でない企業は、HSM が利用できない場合でもセッションをブロックしないという選択もできます。（HSM がダウンしている場合、ファイアウォールは HSM からのレスポンスをキャッシュしているサイトの復号化は行えますが、それ以外は復号化できません）この場合のベストプラクティスは、企業のポリシーによって異なります。ビジネスにとって HSM が不可欠であれば、高可用性（HA）ペアで HSM を実行してください（PAN-OS 8.1 は単一の HSM HA ペアで 2 つのメンバーをサポートしています）。
- リソースなしへのダウングレードをブロック—ファイアウォールが利用できる TLSv1.3 処理リソースがない場合に、ファイアウォールが TLSv1.3 から TLSv1.2 にダウングレードするのを防ぎます。ダウングレードをブロックする場合、ファイアウォールでTLSv1.3リソースが不足すると、TLSv1.2にダウングレードする代わりに TLSv1.3を使用するトラフィックがドロップされます。ダウングレードをブロックしない場合、ファイアウォールが TLSv1.3リソースを使い果たすと、ファイアウォールはTLSv1.2にダウングレードします。しかし、ファイアウォールが処理するリソースを利用できない時にダウングレードをブロックすると、ユーザーが通常時にアクセスできるサイトが一時的にアクセス不可になるため、ユーザーエクスペリエンスが低下する可能性があります。このエラーチェックを実装するかどうかは、セキュリティ コンプライアンスの内容や、強固なセキュリティと比べてユーザーエクスペリエンスがどの程度重要かによって異なります。TLS バージョンをダウングレードしたくない機密性の高いトラフィックの復号化を管理するために、個別の復号ポリシーとプロファイルを作成することを推奨します。

SSL インバウンド インスペクション

SSL インバウンド インスペクションを使用すると、クライアントからターゲットのネットワークサーバー（証明書があり、証明書をファイアウォールにインポートできる任意のサーバー）へのインバウンド SSL/TLS トラフィックを復号化および検査し、疑わしいセッションをブロックします。たとえば、悪意のある人物が Web サーバーの既知の脆弱性を悪用しようとしているとします。インバウンド SSL/TLS 復号化により、トラフィックの可視性が実現し、ファイアウォールが脅威に積極的に対処できるようになります。

SSL Inbound Inspection は SSL Forward Proxy と同様に機能しますが、ファイアウォールが内部クライアントからのアウトバウンド・トラフィックを復号化する代わりに、内部サーバーへのインバウンド・トラフィックを復号化する点が異なります。ファイアウォールは、外部クライアントと内部サーバー間の中間者プロキシとして機能し、セキュリティで保護されたセッションごとに新しいセッションキーを生成します。ファイアウォールは、クライアントとファイアウォールの間に安全なセッションを作成し、ファイアウォールとサーバーの間に別の安全なセッションを作成して、トラフィックを暗号化解除して検査します。

ファイアウォールで、SSL インバウンド検査を実行する各サーバーに対して、1 と秘密キーをインストールする必要があります。ファイアウォールは、SSL/TLS ハンドシェーク中にターゲット・サーバーによって送信された証明書が、Decryption ポリシー・ルール内の証明書と一致することを検証します。一致するものがある場合、ファイアウォールはサーバーの証明書をサーバー・アクセスを要求するクライアントに転送し、セキュア接続を確立します。

Web サーバーがサポートする TLS バージョンによって、サーバー証明書と鍵を ファイアウォールにインストールする方法が決まります。Web サーバーが TLS 1.2 および Rivest、Shamir、Adleman (RSA) または Perfect Forward Secrecy (PFS) 鍵交換アルゴリズム および中間証明書によって署名されているエンドエンティティ (リーフ) 証明書をサポートしている場合、証明書チェーン (単一ファイル) をファイアウォールにアップロードすることをお勧めします。チェーンをアップロードすると、クライアント側のサーバー証明書認証の問題を回避できます。

TLS 1.3 では、*RSA* 鍵交換アルゴリズムのサポートが除去されています。

ファイアウォールは、TLS 1.3 接続を TLS 1.2 接続とは異なる方法で処理します。TLS 1.3 ハンドシェーク中に、ファイアウォールはサーバーから受信したのと同じ証明書または証明書チェーンをクライアントに送信します。そのため、サーバー証明書と秘密鍵をファイアウォールにアップロードするだけで、Web サーバーを正しくセットアップすれば十分です。たとえば、サーバーのリーフ証明書が中間証明書によって署名されている場合、クライアント側のサーバー認証の問題を回避するために、証明書のチェーンをサーバーにインストールする必要があります。

複数の証明書のサポート

SSL Inbound Inspection ポリシー規則は最大 *12* 個の証明書をサポートし、ダウンタイムを発生させることなく保護された内部サーバーの証明書を更新できます。有効な証明書は、継続的な復号化のために、ポリシールールとサーバーに常に存在している必要があります。サーバー証明書の有効期限が切れたり、無効になったりする前に、新しい証明書を更新または取得する必要があります。次に、証明書と秘密鍵をファイアウォールにインポートし、*SSL Inbound Inspection* ポリシー・ルールに追加してから、同じ証明書を *Web* サーバーにインストールします。*Web* サーバー上で別の証明書がアクティブであるときに、ポリシー・ルールを新しい証明書で更新すると、ファイアウォールは、使用中の証明書に関係なく、サーバーへのトラフィックを復号化する準備をします。

新しい証明書を展開する準備ができたら、それを *Web* サーバーにロードし、正しくインストールしたことを確認します。新しい証明書をインストールしても、既存の接続には影響しません。ファイアウォールは、*Server Hello* メッセージの証明書が *Decryption* ポリシー規則の新しい証明書と一致することを確認します。一致しない場合、セッションは終了します。対応する Decryption log エントリは、セッション終了の理由をファイアウォールとサーバー証明書の不一致として報告します。成功したハンドシェイクをログに記録して、すべてのインバウンドインスペクションセッションで使用されているサーバー証明書を表示します。

また、ポリシー規則を作成して、さまざまなドメインをホストするサーバーへのトラフィックを検査し、各ドメインに独自の証明書を付けることもできます。

(*Panorama*™) *SSL Inbound Inspection* ポリシー規則における複数の証明書のサポートは、*PAN-OS 10.2* より前の *PAN-OS*® バージョンでは利用できません。*PAN-OS 10.2* を実行している *Panorama* 管理サーバーからの複数の証明書を含む *SSL Inbound Inspection* ポリシー規則を、以前のバージョンを実行しているファイアウォールにプッシュすると、管理対象ファイアウォールのポリシー規則は、アルファベット順にソートされた証明書リストからの最初の証明書のみを継承します。

*Panorama*から *Decryption* ポリシールールをプッシュする前に、*PAN-OS 10.1* 以前を実行しているファイアウォール用に異なる templates または device groups を設定して、正しいポリシールール と証明書を適切なファイアウォールに確実にプッシュすることをお勧めします。

SSL インバウンド インスペクションのトラフィック用のSSL プロトコル設定 復号化プロファイルを構成する際、異なるセキュリティ能力を持つ複数のサーバーに対して別々のプロファイルを作成します。例えば、*RSA* のみをサポートする一連のサーバーがある場合、*RSA* をサポートするための *SSL* プロトコル設定のみが必要になります。しかし、*PFS* をサポートするサーバー用の *SSL* プロトコル設定では、*PFS* をサポートする必要があります。サーバーがサポートしている最大レベルのセキュリティを利用できるように *SSL* プロトコル設定を構成しつつも、パフォーマンスをチェックし、強力なセキュリティ プロトコルおよびアルゴリズムに求められる大きなプロセス負荷にファイアウォール リソースが対応できることを確認します。

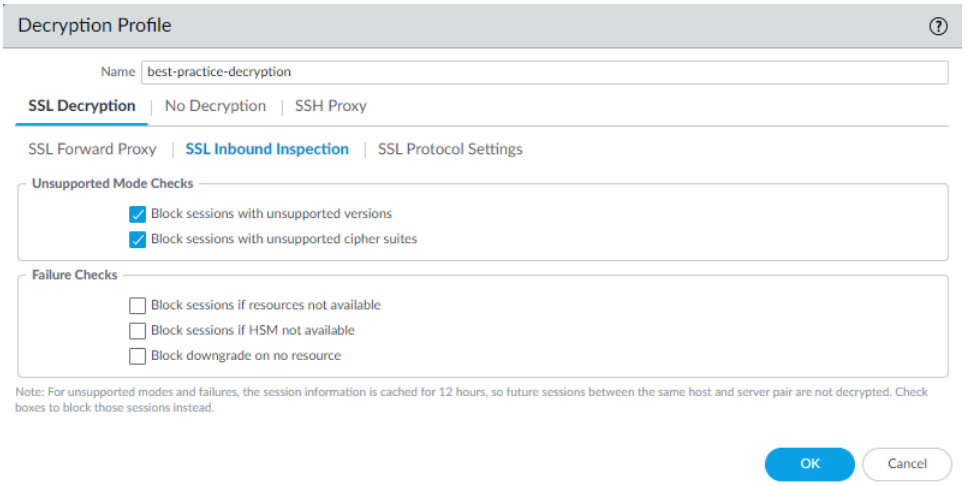
SSL Inbound Inspection は、セッションの再開をサポートしていません。

SSL インバウンドインスペクションを設定すると、プロキシされたトラフィックは *DSCP* コード ポイントまたは *QoS* をサポートしません。

内部サーバーを保護するには、SSL Inbound Inspection ポリシー規則を構成する手順に従います。

SSL インバウンド インスペクション 復号化プロファイル

SSL インバウンド インスペクション復号プロファイル（**Objects (オブジェクト)** > **Decryption Profile (復号プロファイル)** > **SSL Decryption (SSL復号化)** > **SSL Inbound Inspection (SSL**インバウンド インスペクション)は、プロファイルを付与するインバウンド インスペクション復号化ポリシーで定義されている、インバウンド SSL/TLS トラフィックのセッション モード チェックおよびエラーチェックを制御します。以下の図は、インバウンド インスペクション復号プロファイル設定の一般的なベストプラクティスを示していますが、企業のセキュリティ関連のコンプライアンスルールや現地の法律や規制によっても設定が変わってきます。



サポートされていないモード チェック。モードがサポート対象外であるセッションをブロックしない場合、安全でない可能性のあるサーバーに接続する際にユーザーに警告メッセージが届き、そのメッセージ内でクリックしながら進めることで、危険である可能性があるサイトにアクセスできるようになります。これらのセッションをブロックすることで、脆弱でリスクのあるプロトコル バージョンやアルゴリズムを使うサーバーに対して保護することができます：

1. サポートされていないバージョンのセッションをブロックする - SSL プロトコル設定 復号化プロファイルを構成するときに、脆弱なプロトコルをブロックして攻撃対象領域を縮小できるように、ネットワーク上で TLS プロトコルの最小バージョンを指定します。必ずこのボックスにチェックを入れ、サポートしないことにした脆弱な SSL および TLS プロトコル バージョンを持つセッションをブロックしてください。
2. サポートされていない暗号スイートのセッションをブロック—必ずこのボックスにチェックを入れ、ハンドシェークで指定された暗号スイートをファイアウォールがサポートしていない場合に、セッションをブロックするようにしてください。復号化プロファイルの**SSL Protocol Settings (SSL** プロトコル設定**)**タブで、ファイアウォールにサポートさせるアルゴリズムを設定します。

失敗のチェック：

- リソースを使用できない場合にセッションをブロック—ファイアウォール処理リソースが利用できない時にセッションをブロックすると、ファイアウォールはトラフィックを復号化するためのリソースがない時にトラフィックをドロップします。リソースが不足しているためにファイアウォールが復号化を処理できない時にセッションをブロックしない場合、復号化したいトラフィックは暗号化されたままネットワークに入るため、検査されません。しかし、リソースを利用できない時にセッションをブロックすると、ユーザーが通常時にアクセスできるサイトが一時的にアクセス不可になるため、ユーザーエクスペリエンスが低下する可能性があります。このエラーチェックを実装するかどうかは、セキュリティ コンプライアンスの内容や、強固なセキュリティと比べてユーザーエクスペリエンスがどの程度重要かによって異なります。あるいは、復号化できるトラフィックを増やすために、処理能力の高いファイアウォール モデルを使用することをご検討ください。
- **HSM** を利用できない場合にセッションをブロック—ハードウェア セキュリティ モジュール（HSM）を使用して秘密鍵を保存する場合、使用するかどうかは、秘密鍵の取得元の制限、および HSM を利用できない場合に暗号化されたトラフィックをどのように扱うのかを定めるコンプライアンス規則によって異なります。例えば、秘密鍵の署名に HSM を使うことを求める企業は、HSM が利用できない場合にセッションをブロックします。しかし、これに関してそこまで厳重でない企業は、HSM が利用できない場合でもセッションをブロックしないという選択もできます。（HSM がダウンしている場合、ファイアウォールは HSM からのレスポンスをキャッシュしているサイトの復号化は行えますが、それ以外は復号化できません）この場合のベストプラクティスは、企業のポリシーによって異なります。ビジネスにとって HSM が不可欠であれば、高可用性（HA）ペアで HSM を実行してください（PAN-OS 8.1 は単一の HSM HA ペアで 2 つのメンバーをサポートしています）。
- リソースなしへのダウングレードをブロック—ファイアウォールが利用できる TLSv1.3 処理リソースがない場合に、ファイアウォールが TLSv1.3 から TLSv1.2 にダウングレードするのを防ぎます。ダウングレードをブロックする場合、ファイアウォールでTLSv1.3リソースが不足すると、TLSv1.2にダウングレードする代わりに TLSv1.3を使用するトラフィックがドロップされます。ダウングレードをブロックしない場合、ファイアウォールが TLSv1.3リソースを使い果たすと、ファイアウォールはTLSv1.2にダウングレードします。しかし、ファイアウォールが処理するリソースを利用できない時にダウングレードをブロックすると、ユーザーが通常時にアクセスできるサイトが一時的にアクセス不可になるため、ユーザーエクスペリエンスが低下する可能性があります。このエラーチェックを実装するかどうかは、セキュリティ コンプライアンスの内容や、強固なセキュリティと比べてユーザーエクスペリエンスがどの程度重要かによって異なります。TLS バージョンをダウングレードしたくない機

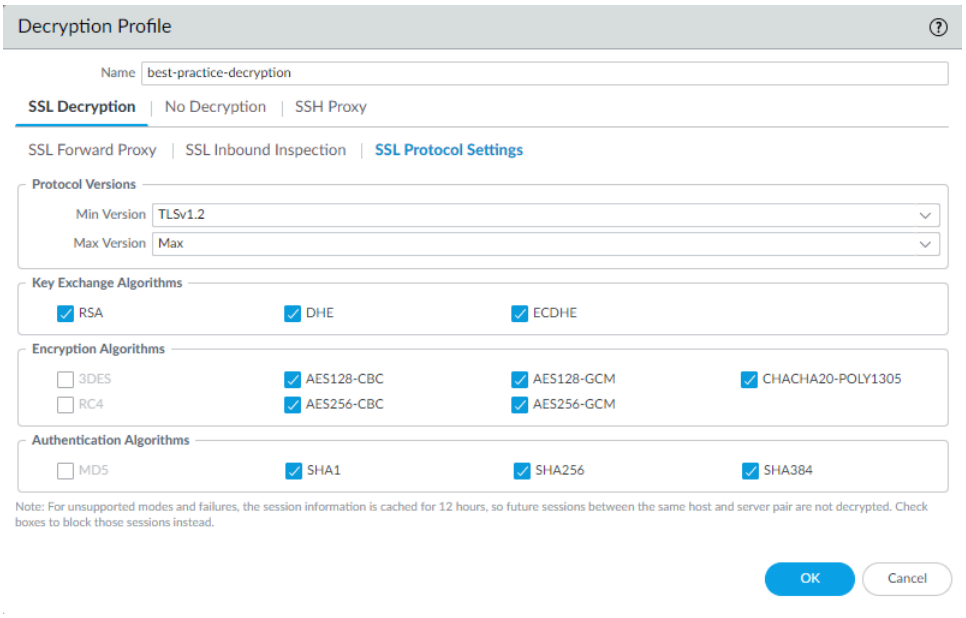
密性の高いトラフィックの復号化を管理するために、個別の復号ポリシーとプロファイルを作成することを推奨します。

SSL プロトコル設定 復号化プロファイル

SSL プロトコル設定（**Objects (オブジェクト)** > **Decryption Profile (復号化プロファイル)** > **SSL Decryption (SSL 復号化)** > **SSL Protocol Settings (SSL プロトコル設定)**）は、脆弱な SSL/TLS プロトコル バージョン、弱い暗号化アルゴリズム、弱い認証アルゴリズムを許可するかどうかを指定します。SSL プロトコル設定は、アウトバウンドの SSL 転送プロキシおよびインバウンドの SSL インバウンド インスペクションのトラフィックに適用されます。これらの設定は、SSH プロキシ トラフィックや、復号化しないトラフィックには適用されません。

次の図は、SSL プロトコル設定の一般的なベストプラクティスを示しています。また、インターネット ゲートウェイ復号化プロファイルおよびデータセンター復号化プロファイルの具体的なベストプラクティスもあります。

SSL インバウンド インスペクションのトラフィック用の *SSL* プロトコル設定を構成する際、異なるセキュリティ能力を持つ複数のサーバーに対して別々のプロファイルを作成します。例えば、*RSA* のみをサポートする一連のサーバーがある場合、*RSA* をサポートするための *SSL* プロトコル設定のみが必要になります。しかし、*PFS* をサポートするサーバー用の *SSL* プロトコル設定では、*PFS* をサポートする必要があります。保護対象のサーバーがサポートしている最大レベルのセキュリティを利用できるように *SSL* プロトコル設定を構成しつつも、パフォーマンスをチェックし、強力なセキュリティ プロトコルおよびアルゴリズムに求められる大きなプロセス負荷にファイアウォール リソースが対応できることを確認します。



プロトコル バージョン：

- **Min Version (最低バージョン)**を**TLSv1.2**に設定し、セキュリティを強化します（セキュリティ サポート TLSv1.2 に値するビジネス サイト）。サイト（あるいはサイト カテゴリー）が脆弱な暗号のみをサポートしている場合は、サイトを確認し、適正なビジネス アプリケーション

をホストしているかどうか判断してください。そうである場合は、サイトがサポートしている最も強力な暗号と一致する**Min Version (**最低バージョン**)**を持つ復号化プロファイルを構成し、その脆弱な暗号を許可するのを対象のサイトだけに制限する復号化ポリシー ルールにそのプロファイルを適用します。サイトが適正なビジネス アプリケーションをホストしていない場合、そのサイトをサポートするためにセキュリティを低下させないでください。弱いプロトコル（および暗号）には、攻撃者が悪用できる既知の脆弱性が含まれています。

そのサイトがビジネスにとって不要なサイト カテゴリーに属す場合、URL フィルタリングを使ってカテゴリー全体へのアクセスをブロックします。重要な古いサイトをサポートするために必要な場合を除き、弱い暗号化、または弱い認証アルゴリズムをサポートしないでください。例外を設ける場合は、対象のサイトに対してのみ脆弱なプロトコルを許可する復号プロファイルを個別に作成してください。TLSv1.1 のために大抵のサイトに適用するメインの復号化プロファイルを、一部の例外のためだけに弱体化させないでください。

Qualys SSL Labs SSL Pulseの *Web* ページには、世界中の最も有名な *150,000* のサイトで使用されている暗号およびプロトコルの割合に関する最新の統計情報が掲載されており、そこでトレンドを把握し、安全な暗号やプロトコルのサポートが世界中でどの程度浸透しているのか確認できます。

- **Max Version (**最大バージョン**)**は特定のバージョンではなく**Max (**最大**)**に設定し、プロトコルが改善される度に、ファイアウォールが自動的に最新かつ最高のプロトコルをサポートするようにしてください。インバウンド（SSL インバウンド インスペクション）あるいはアウトバウンド（SSL 転送プロキシ）トラフィックを制御する復号化ポリシー ルールに復号化プロファイルを付与する際、どちらの場合でも、弱いアルゴリズムを許可しないようにしてください。

  復号化ポリシーがモバイル アプリケーションをサポートしており、その多くが固定証明書を使用している場合は、***Max Version (***最大バージョン***)***を ***TLSv1.2*** に設定します。***TLS v1.3***は、以前の ***TLS*** バージョンでは暗号化されていなかった証明書情報を暗号化するため、ファイアウォールは証明書情報に基づいて復号の除外を自動的に追加できません。これは、一部のモバイル アプリケーションに影響します。したがって、***TLSv1.3***を有効にすると、そのトラフィックに対して復号化なしポリシーを作成しない限り、ファイアウォールが一部のモバイル アプリケーション トラフィックをドロップする可能性があります。

  ビジネスに使用するモバイル アプリケーションがわかっている場合は、それらのアプリケーション用に個別の復号ポリシーとプロファイルを作成して、他のすべてのアプリケーション トラフィックに対して ***TLSv1.3***を有効にできるようにすることを検討してください。

キー交換アルゴリズム：最小バージョンが TLSv1.3 に設定されていない限り、RSA と PFS (DHE と ECDHE) の両方の鍵交換をサポートするには、3 つのボックスをすべてオンのままにします (デフォルトです。TLSv1.3 は ECDHE のみをサポートします。

HTTP / 2 トラフィックをサポートするには、***ECDHE*** ボックスをオンのままにする必要があります。

暗号化アルゴリズム：最小プロトコル バージョンを TLSv1.2 に設定すると、古く弱い 3DES および RC4 アルゴリズムのチェックが自動で外れます（ブロックされます）。最小プロトコル バージョンを TLSv1.3 に設定すると、3DES、RC4、AES128-CBC、および AES256-CBC アルゴリズムは、自動ブロックされます。弱い TLS プロトコルを許可しなければならないトラフィックについては、個別の復号プロファイルを作成し、それをそのサイトのトラフィックにのみ適用し、適切なボックスの選択を解除してアルゴリズムを許可します。3DES または RC4 アルゴリズムを使用するトラフィックを許可すると、ご利用のネットワークが過度のリスクにさらされます。3DES または RC4 をブロックするとビジネスに不可欠なサイトにアクセスできなくなる場合は、そのサイト用の復号プロファイルとポリシーを個別に作成します。他のサイトの復号化を弱体化しないようにしてください。

認証アルゴリズム：ファイアウォールは、古い脆弱な MD5 アルゴリズムを自動でブロックします。TLSv1.3 が最小バージョンである場合、ファイアウォールは SHA1 もブロックします。ネットワークで MD5 認証トラフィックを許可しないでください。許可できる最も弱い認証アルゴリズムは SHA1 です。SHA1 を使う必要なサイトが存在しない場合、SHA1 トラフィックをブロックし、攻撃面をさらに減らしてください。

SSH プロキシ

SSH プロキシ設定では、ファイアウォールはクライアントとサーバーの間に存在します。SSH プロキシはファイアウォールがインバウンドおよびアウトバウンドの SSH 接続を復号化できるようにし、攻撃者が SSH を使用して好ましくないアプリケーションおよびコンテンツをトンネル化しないようにします。SSH 復号化には証明書が不要であり、ファイアウォールが起動時に SSH 復号化に使用するキーを自動生成します。システムの起動中、ファイアウォールは既存のキーがあるかどうかを確認します。存在しない場合、ファイアウォールがキーを生成します。ファイアウォールはこのキーを使用し、ファイアウォール上で設定されたすべての仮想システムの SSH セッションおよび SSH v2 セッションを復号化します。

SSH は、悪意のあるトラフィックを復号化から隠蔽できるトンネリングを許可します。ファイアウォールは SSH トンネル内のトラフィックを復号化できません。（**ssh**アプリケーションからのトラフィックを許可するセキュリティポリシー ルールとともに）アプリケーション**ssh-tunnel**用のセキュリティポリシー ルールを構成し、**Action (**アクション**)**を**Deny (**拒否**)**に設定することで、すべての SSH トンネルのトラフィックをブロックできます。

SSH トンネル セッションは、X11 Windows パケットおよび TCP パケットをトンネル化できます。単一の SSH 接続に複数のチャネルが含まれている場合があります。SSH 復号化プロファイルをトラフィックに適用する際、接続に含まれる各チャネルについて、ファイアウォールがトラフィックの App-ID を検証し、チャネルのタイプを識別します。チャネルには次のタイプがあります：

- session
- X11
- forwarded-tcpip
- direct-tcpip

チャネル タイプが session である場合、ファイアウォールはトラフィックを、SFTP や SCP などの許可された SSH トラフィックとして識別します。チャネル タイプが X11、forwarded-tcpip、

あるいは direct-tcpip である場合、ファイアウォールはトラフィックを SSH トンネル トラフィックとして識別し、それをブロックします。

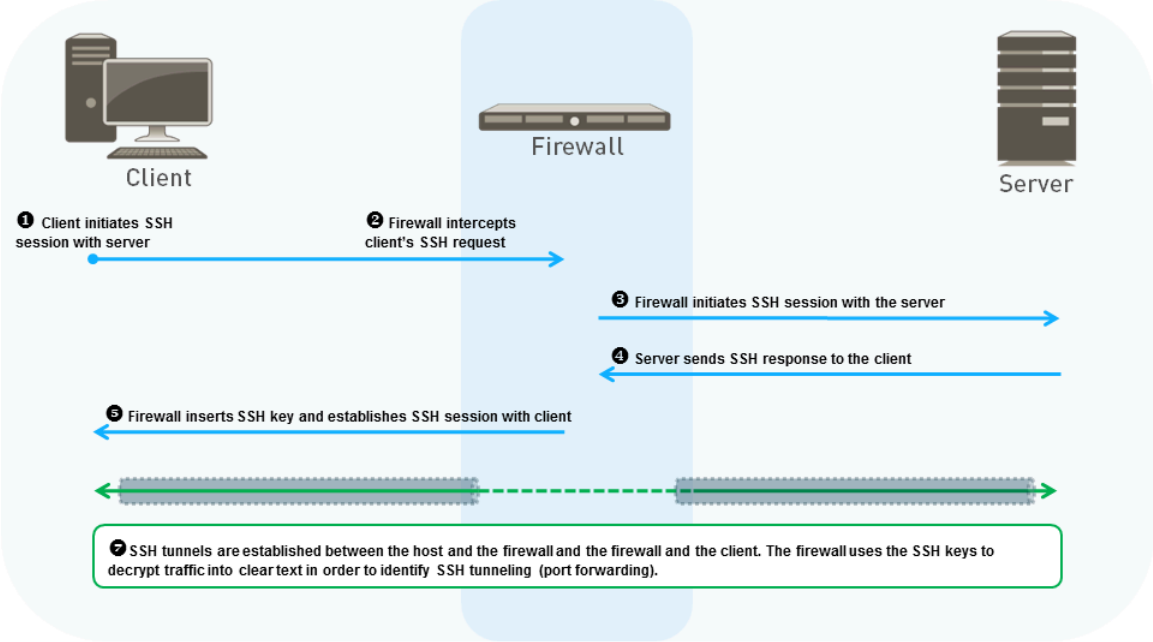
SSH の利用はネットワーク デバイスを管理する必要がある管理者だけに制限し、すべての *SSH* トラフィックのログを取り、マルチ ファクター認証の設定を行って、正当なユーザーだけが *SSH* を使ってデバイスにアクセスできるようにすることで、攻撃の入り口を減らすようにしてください。

ファイアウォールで*SSH Decryption*を有効にすると、*SSH*クライアントが公開鍵ベースの認証を使用しなくなったため、証明書を持つホストへの認証が失敗し、クライアントが秘密鍵を使用して復号化できる公開鍵を使用してハンドシェイクを完了できなくなります。ユーザー名とパスワード認証を使用して、*SSH* セッションを開始します。

鍵ベースの認証を使用する必要があるシステムの場合、*SSH Decryption* ポリシー規則を構成して、公開鍵認証を必要とするシステムを除外するようにします。*SSH Decryption* ポリシールールを編集するには:

1. ***Policies*** > ***Decryption*** に移動し、*SSH* 復号化を制御するポリシー規則を選択します。
2. ***Destination*** *(*宛先*)* タブを選択します。
3. ルールから除外するシステムの *IP* アドレスを追加します。
4. ***Negate*** を選択します。
5. ***OK*** をクリックします。
6. 変更を ***Commit***（コミット）します。

次の図は、SSH プロキシ復号化がどのように機能するのかを示しています。SSH プロキシ復号化を有効化する方法については、SSH プロキシの設定を参照してください。



1. クライアントは、セッションを開始するためにサーバーに SSH 要求を送信します。
2. ファイアウォールはクライアントの SSH 要求をインターセプトします。
3. ファイアウォールは要求をサーバーに転送し、サーバーとの SSH セッションを開始します。これにより、ファイアウォールが作成する 2 つの分割されたセッションのうち、最初のセッションが確立されます。各セッションは、分割されたSSH トンネルを確立します。
4. サーバーは、ファイアウォールがインターセプトする要求に応答します。
5. ファイアウォールは、SSH キーをサーバーの応答に挿入し、クライアントに転送します。これにより、ファイアウォールが作成する 2 番目の分割されたセッション (および分割されたSSH トンネル) が確立されます。
6. (図の「7」の最初の部分)ファイアウォールがサーバーとクライアントとの別々のセッションを確立した後、ファイアウォールはそれらの間のプロキシーとして機能します。
7. ファイアウォールは、クライアントとサーバー間のトラフィックをチェックして、正常にルーティングされているかどうか、またはSSHポートフォワーディング(SSHトンネリング)を使用しているかどうかを確認します。ファイアウォールが SSH ポートフォワーディングを識別する場合、ファイアウォールはトンネリングされたトラフィックをブロックし、設定された Security ポリシーに従って制限します。ファイアウォールはSSHポートフォワーディングのみを検査し、SSHトンネルでコンテンツと脅威の検査は実行しません。

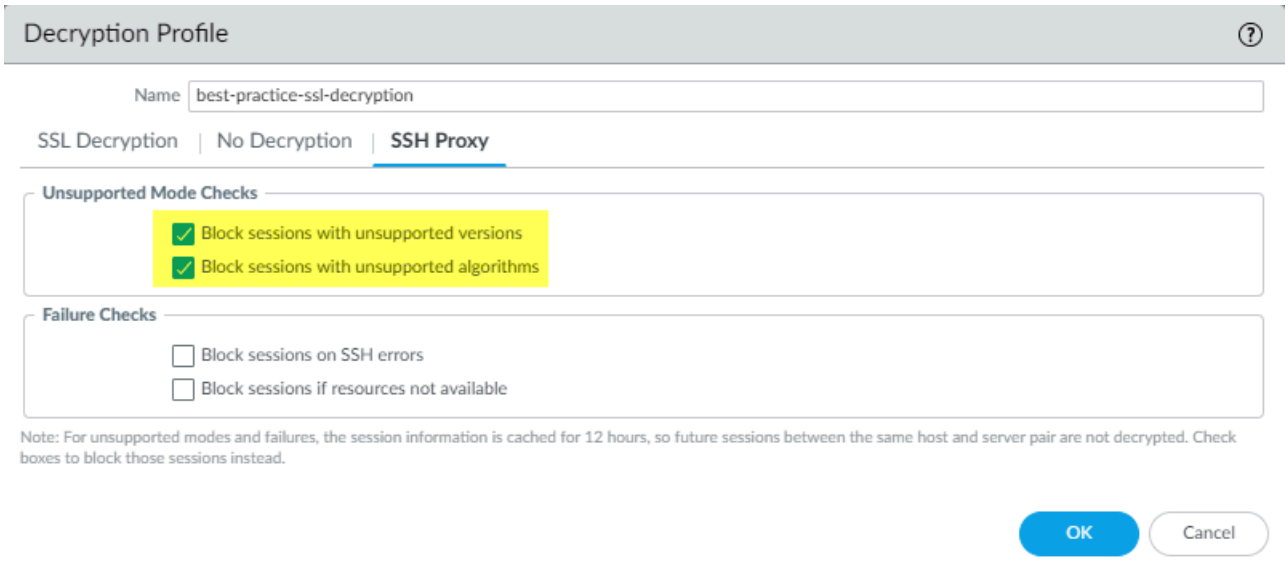
SSH プロキシを設定すると、プロキシされたトラフィックは *DSCP* コード ポイントまたは *QoS* をサポートしません。

SSH プロキシ復号化プロファイル

SSH プロキシ復号化プロファイル（**Objects (オブジェクト)** > **Decryption Profile (復号化プロファイル)** > **SSH Proxy (SSH プロキシ)**）は、プロファイルを付与する SSH プロキシ復号化ポリシーで定義されている、SSH トラフィックのセッション モード チェックおよびエラーチェックを制御します。次の図は、SSH プロキシ復号化プロファイル設定の一般的なベストプラクティス

を示していますが、企業のセキュリティ関連のコンプライアンス規則や現地の法、規制によっても設定が変わってきます。

ファイアウォールは *SSH* トンネル（ポート転送）に対してコンテンツおよび脅威検査を実行しません。しかし、ファイアウォールは *SSH* アプリケーションと *SSH* トンネル アプリケーションを区別します。ファイアウォールは *SSH* トンネルを識別すると、*SSH* トンネル トラフィックをブロックし、設定済みのセキュリティ ポリシーに従ってトラフィックを制限します。



サポートされていないモード チェック。ファイアウォールでは SSHv2 がサポートされています。モードがサポート対象外であるセッションをブロックしない場合、安全でない可能性のあるサーバーに接続する際にユーザーに警告メッセージが届き、そのメッセージ内でクリックしながら進めることで、危険である可能性があるサイトにアクセスできるようになります。これらのセッションをブロックすることで、脆弱でリスクのあるプロトコル バージョンやアルゴリズムを使うサーバーに対して保護することができます：

1. サポートされていないバージョンのセッションをブロック—ファイアウォールでは、一連のサポートされているバージョンが事前定義されています。このボックスにチェックを入れると、脆弱なバージョンのトラフィックがブロックされます。必ずこのボックスにチェックを入れて脆弱なプロトコル バージョンを持つセッションをブロックし、攻撃の入り口を減らすようにしてください。
2. サポートされていないアルゴリズムのセッションをブロック—ファイアウォールでは、一連のサポートされているアルゴリズムが事前定義されています。このボックスにチェックを入れると、脆弱なアルゴリズムのトラフィックがブロックされます。必ずこのボックスにチェックを入れてサポートされていないアルゴリズムを持つセッションをブロックし、攻撃の入り口を減らすようにしてください。

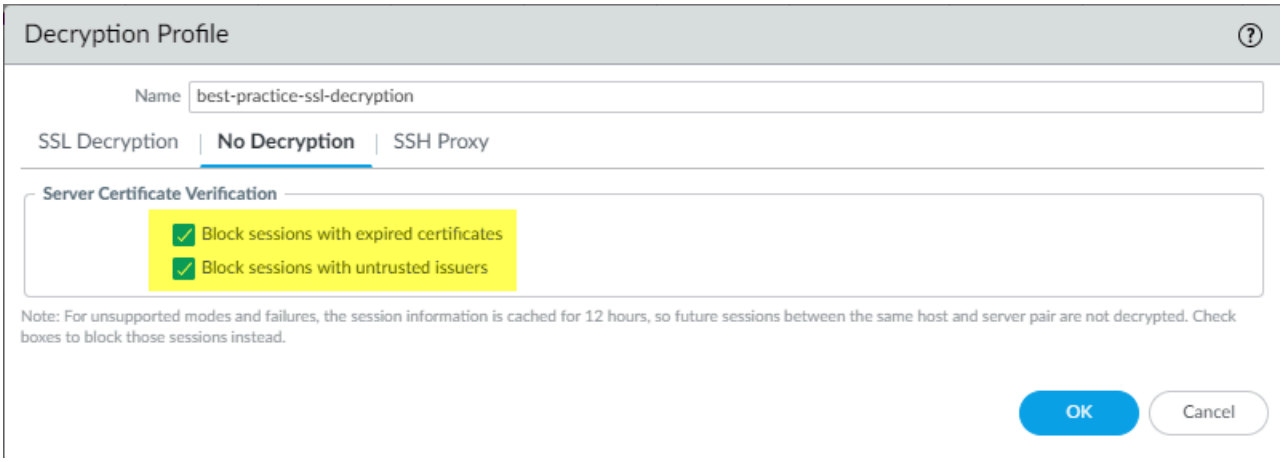
失敗のチェック：

- **SSH** エラー時にセッションをブロック—このボックスにチェックを入れると、SSH エラー発生時にセッションが終了します。

- リソースを利用できない場合にセッションをブロック—ファイアウォールが処理するリソースを利用できない時にセッションをブロックしない場合、復号化したい暗号化されたトラフィックが暗号化されたままネットワークに入り、危険な接続が可能になるおそれがあります。しかし、ファイアウォールが処理するリソースを利用できない時にセッションをブロックすると、ユーザーが通常時にアクセスできるサイトが一時的にアクセス不可になるため、ユーザーエクスペリエンスが低下する可能性があります。エラーチェックを実装するかどうかは、企業のセキュリティ コンプライアンスの内容や、強固なセキュリティと比べてユーザーエクスペリエンスがどの程度重要なビジネスなのかによって異なります。あるいは、復号化できるトラフィックを増やすために、処理能力の高いファイアウォール モデルを使用することをご検討ください。

復号化なしのプロファイル

復号化なしのプロファイル (**Objects (オブジェクト)** > **Decryption Profile (復号化プロファイル)** > **No Decryption (復号化なし)**) は、復号化しないことを選択したトラフィックに対してサーバー検証チェックを実行します。復号化から除外するトラフィックを定義する「復号化なし」復号化ポリシーに復号化なしのプロファイルをアタッチします。（サイトが証明書のピンニングや相互認証などの技術的な理由で復号化を妨げる場合、トラフィックの復号化を除外するためにポリシーを使用しないでください。代わりに、ホスト名を復号化除外リストに追加します） 次の図は、非復号化プロファイル設定の一般的なベストプラクティスを示していますが、企業のセキュリティ関連のコンプライアンス規則や現地の法、規制によっても設定が変わってきます。



- **Block sessions with expired certificates (証明書が失効したセッションをブロック)**—このボックスにチェックを入れ、失効した証明書を持つサーバーのセッションをブロックし、安全でない可能性のあるサイトへのアクセスを禁止してください。このボックスにチェックを入れなければ、ユーザーが悪意のある可能性のあるサイトに接してトランザクションを行うことができ、接続時に警告メッセージが表示されるものの、接続は拒否されません。
- **Block sessions with untrusted issuers (発行者を信頼できないセッションをブロック)**—このボックスにチェックを入れ、信頼できない証明書を持つサーバーのセッションをブロックしてください。信頼できない発行者は、UnTrust、リプレイ攻撃、その他の攻撃を行う可能性があります。

復号化しない *TLSv1.3* トラフィックの復号化ポリシーに復号化なしのプロファイルをアタッチしないでください。以前のバージョンとは異なり、*TLSv1.3* は証明書情報を暗号化するため、ファイアウォールは証明書データを可視化できません。そのため、期限切れの証明書や信頼できない発行者とのセッションをブロックできず、プロファイルは効果がありません。*(*これらのプロトコルは証明書情報を暗号化しないため、ファイアウォールは *TLSv1.2* 以前で証明書チェックを実行できますが、トラフィックに復号化なしのプロファイルを適用する必要があります。*)* ただし、復号化ポリシーがそのトラフィックを制御しない限り、ファイアウォールは復号化されていないトラフィックをログに記録しないため、復号化しない *TLSv1.3* トラフィックの復号化ポリシーを作成する必要があります。

（*TLSv1.2* 以前に適用）信頼されていない発行者とのセッションを許可することを選択し（推奨されません）、有効期限が切れた証明書でセッションをブロックする場合、信頼できる有効期限が切れた発行者とのセッションが発生するシナリオがあり、 誤ってブロックされる可能性があります。ファイアウォールの証明書ストアに有効な自己署名の信頼できる *CA* が含まれていて、サーバーが証明書チェーンで期限切れの *CA* を送信する場合、ファイアウォールは証明書ストアをチェックしません。代わりに、ファイアウォールは、信頼できる有効な代替トラストアンカーを見つけて、信頼できる自己署名証明書に基づくセッションを許可する必要がある場合に、期限切れの *CA* に基づいてセッションをブロックします。

このシナリオを回避するには、有効期限が切れた証明書によるセッションのブロックに加えて、信頼されていない発行者によるセッションのブロックを有効にします。これにより、ファイアウォールは証明書ストアをチェックし、自己署名された信頼できる *CA* を見つけて、セッションを許可します。

楕円曲線暗号（ECC）証明書用の SSL 復号化

ファイアウォールは楕円曲線デジタル署名アルゴリズム（ECDSA）証明書などのような ECC 証明書を使用してウェブサイトおよびアプリケーションから来る SSL トラフィックを自動的に復号化します。組織は ECC 証明書の使用に移行すれば強固な鍵の提供や証明書サイズの縮小などのメリットを得られるため、ECC で保護されたアプリケーションと Web サイト トラフィックへの可視性と安全使用を継続的に確保できます。

ECC 証明書を使用するウェブサイトおよびアプリケーションの復号化は、ファイアウォールにミラーリングされるトラフィックではサポートされていません。*ECC* 証明書を使用して復号化されたトラフィックは、ファイアウォールが復号化を行うために、直にファイアウォールを通る必要があります。

hardware security module （ハードウェア セキュリティ モジュール - HSM）を使用して、*ECDSA* 証明書に関連づけられた秘密鍵を保存することができます。*TLSv1.3*トラフィックの場合、*PAN-OS* は *SSL*フォワード プロキシ用のみに *HSM* をサポートします。*SSL* インバウンド検査用の *HSM* はサポートしていません。

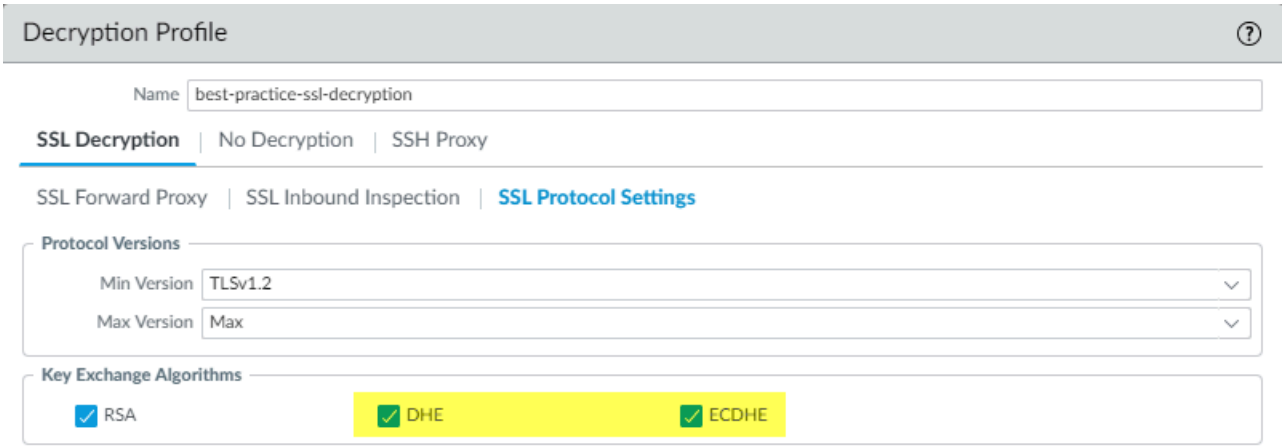
SSL 復号化のための Perfect Forward Secrecy（PFS）

PFS は、ある暗号化されたセッションが悪用された際に、他の複数の暗号化されたセッションにもそれが伝染するのを防ぐ安全な通信プロトコルです。PFS では、クライアントと接続を確立した安全なセッション毎にサーバーが一意な秘密鍵を生成します。サーバーの秘密鍵が感染すると、そのキーを使って確立された単一のセッションのみが脆弱になります。サーバーは一意のキーを生成してそれぞれと接続するため、攻撃者はそれ以前や以後のセッションから情報を取得することはできません。ファイアウォールは PFS キー交換アルゴリズムを使って確立された SSL セッションを復号化し、それ以前や以後のセッションを PFS で保護します。

Diffie-Hellman（DHE）ベースの PFS および楕円曲線 Diffie-Hellman（ECDHE）ベースの PFS のサポートは、デフォルトで有効になっています（**Objects (オブジェクト)** > **Decryption Profile (復号化プロファイル)** > **SSL Decryption (SSL 復号化)** > **SSL Protocol Settings (SSL プロトコル設定)**）。

DHE あるいは *ECDHE* キー交換アルゴリズムを使用して*SSL* 復号化のための *PFS* サポートを有効化する場合、ハードウェア セキュリティ モジュール（HSM）を使用し、*SSL* インバウンド インスペクション用の秘密鍵を保存することができます。

SSL インバウンド検査を構成し、*PFS* 暗号を使用する場合、セッション再開はサポートされません。

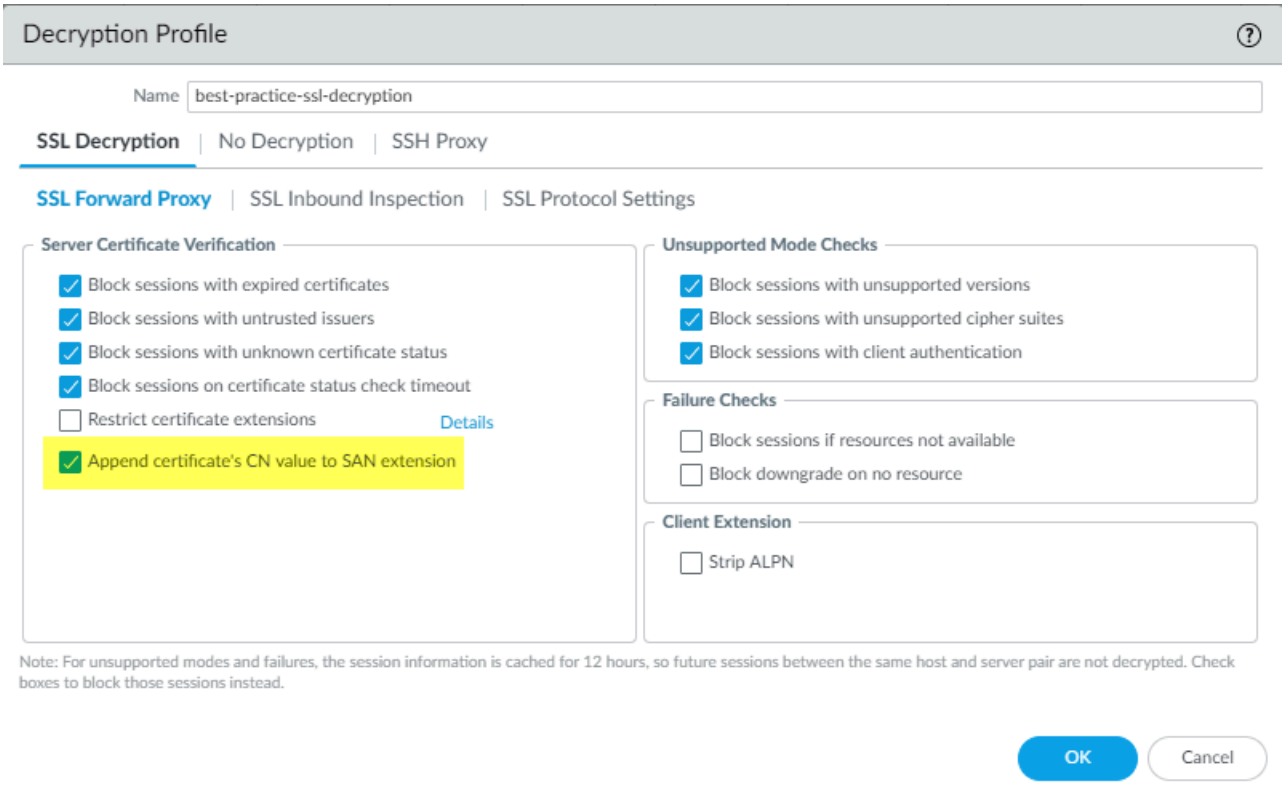


SSL 復号化とサブジェクト代替名（SAN）

一部のブラウザでは、サーバー証明書でサブジェクト代替名（SAN）を使用して証明書が保護するドメインを指定し、サーバー証明書の共通名（CN）に基づく証明書の照合はサポートされなくなりました。SAN を使用すると、単一のサーバー証明書で複数の名前を保護できます。CN は SAN よりも定義が厳密ではなく、ドメイン上の単一のドメインまたはすべての第 1 レベルのサブドメインのみを保護できます。ただし、サーバー証明書に 1 つの CN のみが含まれている場合、SAN を要求するブラウザは、エンドユーザーが要求された Web リソースに接続することを許可しません。ファイアウォールは、生成した偽装証明書に SAN を追加して、SSL 復号化中に信頼できる第三者として自身を確立することができます。サーバー証明書に CN のみが含まれている場合、SSL 復号化を実行するファイアウォールはサーバー証明書 CN を偽装証明書 SAN にコピーします。ファイアウォールは、SAN による偽装証明書をクライアントに提示し、ブラウ

ザはその接続をサポートすることができます。エンド ユーザーは必要なリソースに引き続きアクセスでき、ファイアウォールはセッションを復号化できます。

復号化された SSL トラフィックの SAN サポートを有効にするには、関連する復号ポリシーに添付されている復号プロファイルを更新します：**Objects**（オブジェクト） > **Decryption Profile**（復号プロファイル） > **SSL Decryption**（SSL復号化） > **SSL Forward Proxy**（SSL 転送プロキシ） > **Append Certificate's CN Value to SAN Extension**（証明書のコモンネーム (CN) 値を SAN 拡張項目に追加））を選択します。



TLSv1.3復号

TLSv1.3トラフィックの既知および未知の脅威を復号し、完全に可視化し、防止することができます。TLSv1.3は、TLS プロトコルの最新バージョンであり、アプリケーションのセキュリティとパフォーマンスを向上させます。TLSv1.3 復号化をサポートするには、最小プロトコル バージョンとして TLSv1.3 が構成されたか、Max または TLSv1.3 が最大プロトコル バージョンとして構成されている既存のおよび新しい Decryption ポリシー ルールに Decryption プロファイルを適用する必要があります。TLSv1.3 をサポートするように既存のプロファイルを編集できます。複合化 プロファイルで TLSv1.3 サポートを指定しない場合、PAN-OS はデフォルトで最大プロトコル バージョンとして TLSv1.2 をサポートします。ファイアウォールは、フォワード プロキシ、インバウンド インスペクション、復号化されたネットワーク パケット ブローカ トラフィック、および復号化ポート ミラーリングの TLSv1.3 復号化をサポートします。

TLSv1.3を使用するには、クライアントとサーバーが TLSv1.3暗号をネゴシエートできる必要があります。TLSv1.3をサポートしていない Web サイトの場合、ファイアウォールはサーバーがサポートしている古いバージョンの TLS プロトコルを選択します。

ファイアウォールは、TLSv1.3の以下の復号アルゴリズムをサポートしています：

- TLS13-AES-128-GCM-SHA256
- TLS13-AES-256-GCM-SHA384
- TLS13-CHACHA20-POLY1305-SHA256

復号されたトラフィックに適用する復号プロファイルでプロトコルの **Max Version (**最大バージョン**)** が**Max (**最大**)** として指定されている場合、プロファイルは TLSv1.3をサポートし、TLSv1.3をサポートするサイトで TLSv1.3を自動的に使用します。(TLSv1.3 をサポートするために、**Max Version** を **TLSv1.3.3** に設定することもできますが、TLS の次のバージョンがリリースされたら、プロファイルを更新する必要があります。**Max Version** を **Max** に設定すると、新しい TLS バージョンがリリースされたときに自動的にサポートされるようにプロファイルが将来にわたって保証されます。 PAN-OS 10.0にアップグレードすると、**Max Version (**最大バージョン**)**が **Max (**最大**)** に設定されているすべての復号プロファイルが **TLSv1.2** にリセットされ、ピニングされた証明書を使用するモバイル アプリケーションの自動サポートが提供され、そのトラフィックがドロップするのを防ぎます。

すべてのアプリケーションが TLSv1.3プロトコルをサポートしているわけではありません。復号のベストプラクティスに従い、TLS プロトコルの**Min Version (**最小バージョン**)** を **TLSv1.2** に設定し、**Max Version (**最大バージョン**)**設定を **Max (**最大**)** のままにします。ビジネス ニーズでより弱い TLS プロトコルを許可する必要がある場合は、より弱いプロトコルを許可する**Min Vversion (**最小バージョン**)** を使用して別の SSL 復号プロファイルを作成し、より弱い TLS プロトコルで許可する必要のあるトラフィックを定義する復号ポリシーにアタッチします。

復号ポリシーがモバイル アプリケーションをサポートしており、その多くがピニングされた証明書を使用している場合は、**Max Version (**最大バージョン**)**を **TLSv1.2** に設定します。TLS v1.3は、以前の TLS バージョンでは暗号化されていなかった証明書情報を暗号化するため、ファイアウォールは証明書情報に基づいて復号の除外を自動的に追加できません。これは、一部のモバイル アプリケーションに影響します。したがって、TLSv1.3を有効にすると、そのトラフィックに対して復号しないポリシーを作成しない限り、ファイアウォールが一部のモバイル アプリケーション トラフィックをドロップする可能性があります。ビジネスに使用するモバイル アプリケーションがわかっている場合は、それらのアプリケーション用に個別の復号ポリシーとプロファイルを作成して、他のすべてのトラフィックに対して TLSv1.3を有効にできるようにすることを検討してください。

特定のポリシーが *TLSv1.3* トラフィックのみを制御することがわかっている場合は、復号化しない *TLSv1.3* トラフィックに対して の復号化プロファイル を 復号化ポリシー にアタッチしないでください。以前の *TLS* バージョンからの変更点は、*TLSv1.3*が証明書情報を暗号化するため、ファイアウォールはそのデータを可視化できなくなり、期限切れの証明書または信頼できない発行者とのセッションをブロックできないため、プロファイルは効果がありません。*(*これらのプロトコルは証明書情報を暗号化しないため、ファイアウォールは *TLSv1.2*以前で証明書チェックを実行できます。そのため、トラフィックに復号なしのプロファイルを適用する必要があります。*)* ただし、すべてのタイプの復号されていないトラフィックをログに記録するには、復号ポリシーで成功および失敗した *TLS* ハンドシェイクのログ記録を有効にします *(*失敗した *TLS* ハンドシェイクのロギングはデフォルトで有効になっています*)*。

SSL プロトコル設定 復号化プロファイルでサポートされていないモードを許可すると、firewall によってトラフィックが自動的にローカル復号化例外キャッシュに追加されます。ファイアウォールは引き続き TLSv1.3から TLSv1.2にダウングレードされたトラフィックを復号して検査し、サーバーをキャッシュに追加するためにキャッシュに表示される**Reason (理由)** は TLS13_UNSUPPORTED です。

PAN-OS 10.2 から以前のバージョンにダウングレードすると、TLSv1.3 を **Min Version** または **Max Version** として指定する Decryption プロファイルは、サポートされている最高のバージョンに変更されます。たとえば、PAN-OS 10.2 から PAN-OS 9.1 にダウングレードすると、TLSv1.3 が TLSv1.2 に置き換えられます。PAN-OS 10.2 上の Panorama デバイスが古いバージョンの PAN-OS を実行するデバイスに構成をプッシュする場合、TLSv1.3 を **Min Version** または **Max Version** として指定した 複合化 プロファイルも、サポートされている最高のバージョンに変更されます。

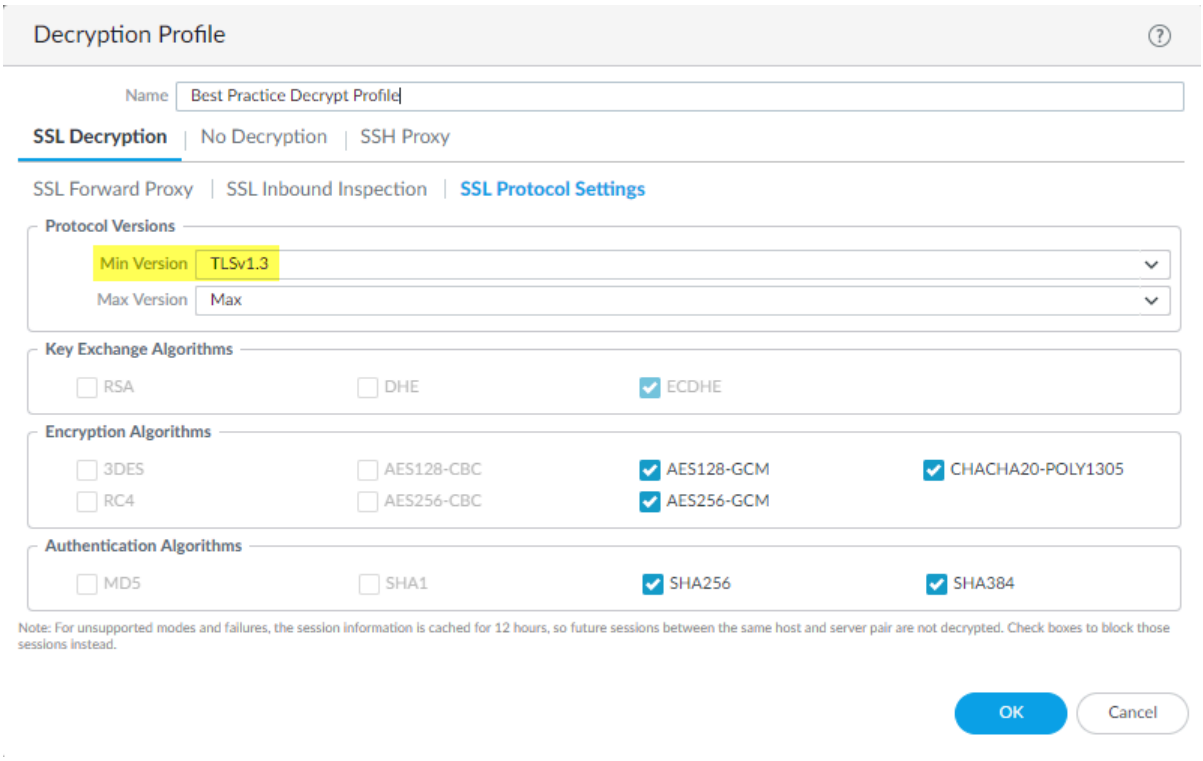
ハードウェア セキュリティ モジュール *(HSM)* を使用するお客様の場合、*PAN-OS* は *SSL* フォワード プロキシの場合のみ *TLSv1.3* をサポートします。*SSL* インバウンドインスペクションの *HSM* はサポートしていません。

TLSv1.3を最小許容プロトコルバージョンとして設定する SSL 復号プロファイルを設定して、最も厳しいセキュリティを実現できます。ただし、一部のアプリケーションは TLSv1.3をサポートしておらず、TLSv1.3が最小許容プロトコルである場合は機能しない可能性があります。TLSv1.3のみをサポートするアプリケーショントラフィックにのみ、TLSv1.3を最小バージョンとして設定するプロファイルを適用します。

1. 新しいSSL Decryption profile (SSL 復号プロファイル) を作成するか、既存のプロファイルを編集します(**Objects (オブジェクト)** > **Decryption (復号)** > **Decryption Profile (復号プロファイル)**)。

   プロファイルが新しい場合は、プロファイルの **Name (名前)** を指定します。
2. **SSL Protocol Settings (SSL** プロトコル設定**)** を選択します。

3. **Min Version (**最小バージョン**)** を **TLSv1.3** に変更します。



Max Version (最大バージョン**)**に**Max (**最大**)** を使用することで、プロファイルが制御するトラフィックが、利用可能な最も強力なプロトコル バージョンを使用できるようにします。**Min Version (**最小バージョン**)** は、トラフィックが使用できるプロトコルの最も弱いバージョンを設定します。最小バージョンを **TLSv1.3**に設定すると、トラフィックは TLSv1.3 (またはそれ以上) を使用する必要があり、より弱いプロトコルバージョンがブロックされます。(Decryption Policy Rule (復号ポリシー ルール)は、プロファイルが制御するトラフィックを定義します。)

TLSv1.3を **Min Version (**最小バージョン**)** として設定する場合は、Perfect Forward Secrecy (PFS) を使用する必要があり、より弱い鍵交換、暗号化、および認証アルゴリズムは使用できません。

4. 設定または変更する必要があるその他の復号プロファイル設定を構成します。
5. **OK** をクリックしてプロファイルを保存します。
6. プロファイルを適切な復号ポリシー ルールにアタッチして、適切なトラフィックに適用します。

高可用性は復号化されたセッションではサポートされていません

フェールオーバー後、ファイアウォールは復号化された SSL セッションの High Availability (HA) 同期をサポートしません。ファイアウォールは、復号化された SSL Forward Proxy、SSL Inbound Inspection、または SSH Proxy セッションを再開しません。ファイアウォールは、復号化ポリシーに基づいて、フェイルオーバー後に開始する新しいセッションを復号化します。

復号化ミラーリング

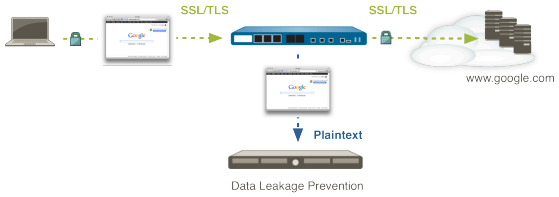
復号化ミラーリングは、ファイアウォールからの復号化されたトラフィックのコピーを作成して、NetWitness や Solera などのトラフィック収集ツールに送信します。このツールは、アーカイブや解析のためにpacket capture (パケット キャプチャ - pcap)を受信できます。フォレンジックや履歴調査の目的で、またはデータ漏洩防止（DLP）のために包括的なデータ キャプチャを必要とする場合は、無料のライセンスをインストールして機能を有効にすることができます。

ライセンスのインストール後、トラフィック収集ツールをファイアウォールのイーサネット インターフェースに直接接続し、**Interface Type**（インターフェースタイプ）を**Decrypt Mirror**（復号化ミラー）に設定します。ファイアウォールは、収集ツールを使用して TCP ハンドシェイクをシミュレートし、すべてのデータパケットを復号化して（平文として）インターフェースを介して送信します。

パブリック クラウド プラットフォーム向け *VM-Series*（*AWS*、*Azure*、*Google Cloud Platform*）、および *VMware NSX* では復号化ポート ミラーリングは使用できません。

一部の国では、SSL トラフィックの復号化、保存、検査、または使用が規制されていて、複合化ミラーリング機能を使用するにはユーザーの同意が必要な場合があります。さらに、ファイアウォールへの管理アクセス権を持つ悪意あるユーザーがこの機能を使用すると、暗号化されたチャネルを使用して送信されたユーザー名、パスワード、社会保障番号、クレジット カード番号などの機密情報を収集できる可能性があります。運用環境でこの機能を有効にしたり使用したりする前に、企業の審議会と協議することをお勧めします。

次の画像は復号化されたトラフィックをミラーリングするプロセスを示し、復号ポート ミラーリングの設定のセクションではこの機能のライセンスと有効化について説明します。



復号化をデプロイする準備

復号化をデプロイする際に最も時間がかかる作業は復号化ポリシーやプロファイルの設定ではなく、関係者と協力しつつ、復号化する、あるいは復号化しないトラフィックを判断し、ウェブサイトへのアクセスに関する変更内容についてユーザーに周知させ、秘密鍵基盤（PKI）の戦略を立て、段階的な優先順位を付けたロールアウトを計画するなどのデプロイの準備を行うことです。

デプロイメントの目標を設定し、復号化計画のベストプラクティスのチェックリストを確認し、推奨されるベストプラクティスを把握してください。ファイアウォール リソースが許容できる範囲で、重要なトラフィックから初めてできるだけ多くのトラフィックを復号化するというのが、ベストプラクティスの目標になります。

復号化ポリシー ルールを作成してデプロイする前に、ポートベースからアプリケーション ベースのセキュリティポリシールールへと移行します。ポート ベースのセキュリティポリシーに基づいて復号化ルールを作成し、それからアプリケーション ベースのセキュリティポリシーに移行する場合、アプリケーション トラフィックが標準的でないポートを使用できないようにするために、セキュリティポリシールールがアプリケーションのデフォルトのポートを使うことが多いため、その変更により、許可しようとしているトラフィックを復号化ルールがブロックしてしまうおそれがあります。例えば、ウェブ ブラウジング アプリケーション トラフィック（デフォルトのポート *80*）として識別されたトラフィックの背後に、*HTTPS* トラフィック（デフォルトのポート *443*）のような異なるデフォルトのポートを持つアプリケーションが存在するかもしれません。アプリケーションのデフォルトルールは、復号化されたトラフィックが「標準的でない」ポート（*80* ではなく *443*）を使用していると判断するため、*HTTPS* トラフィックをブロックします。復号化をデプロイする前に *App-ID* ベースのルールに移行すると、*POC* で復号化のデプロイメントをテストする際にセキュリティポリシーの設定ミスが見つかり、一般ユーザー用にロールアウトする前にそれを修正することになります。

復号化をデプロイする準備を行うには：

- 関係者と協力して開発：復号化のデプロイ戦略
- PKI ロールアウト プランの作成
- 復号化ファイアウォールのデプロイメントのサイジング
- 段階的な優先順位付きデプロイメント計画

関係者と協力して開発：復号化のデプロイ戦略

法務、経理、人事、重役、セキュリティ、IT/サポートなどの関係者と協力しつつ、復号化のデプロイ戦略を組み立てます。まずはトラフィックを復号化するために必要な承認を得て企業を保護します。トラフィックの復号化では、法的規制やビジネスニーズによって復号化できるものとできないものがどのように決まるのか、把握することも重要です。

復号化するトラフィックを判断し、優先順位を付けてください。暗号化されたトラフィックに含まれる潜在的な脅威に対して可視性を確保し、それらの脅威を防止するために、できるだけ多

くのトラフィックを復号化するというのがベストプラクティスになります。ファイアウォールのサイジングが適切でないために、復号化したいすべてのトラフィックを復号化できない場合は、最も重要なサーバー、リスクの大きいカテゴリー、あまり信頼されていないセグメントや IP サブネットを優先します。「このサーバーのセキュリティが破られたらどうなるか？」、「目標のパフォーマンスを達成するためにどの程度のリスクを取れるだろうか？」といったことを考えつつ、優先順位を決めます。

次に、証明書のピンニング、不完全な証明書チェーン、サポートされていない暗号化、相互認証などの技術的な理由でトラフィックが復号化を妨げるため、復号化できないトラフィックを判断します。技術的に復号化を解除するサイトを復号化すると、そのトラフィックがブロックされます。技術的に復号化を妨げるウェブサイトを評価し、そのサイトにアクセスするビジネス上の理由が本当にあるかどうかを検討します。サイトにアクセスする必要がない場合は、復号化を許可してブロックしてください。ビジネス上の目的でそれらのサイトのいずれかにアクセスする必要がある場合、それらを SSL 復号化Exclusion (除外)リストに追加して、復号化から除外します。SSL 復号化除外リストは、復号化を技術的に妨げるサイトのみに使用します。

金融、健康、政府関連のトラフィック、特定の重役のトラフィックなど、法、規制、個人的あるいは他の理由で復号化しないことにするセンシティブなトラフィックを判断します。これは復号化を技術的に妨げるトラフィックではないため、トラフィックを復号化から除外する際に SSL 復号化除外リストを使用しません。代わりに、ポリシー ベース復号化除外を作成し、復号化しないことにしたトラフィックを識別・制御し、復号化なしの復号化プロファイルをポリシーに適用し、証明書に問題のあるサーバーがネットワークにアクセスできないようにします。ポリシーベース復号化除外は、復号化しないことにしたトラフィックでのみ使用します。

復号化ポリシーを計画する際は、企業のセキュリティ コンプライアンス規則、コンピューターの使用規則、ビジネス ゴールを考慮してください。コントロールが厳格過ぎると、ユーザーが以前はアクセスできたビジネス以外のサイトにアクセスできなくなり、ユーザーエクスペリエンスが影響を受けるおそれがありますが、政府や金融機関の場合はそうする必要があるかもしれません。利便性、管理のオーバーヘッド、セキュリティにはトレードオフがつきまといます。復号化ポリシーが厳格なほどウェブサイトにアクセスできなくなる機会が増え、ユーザーの不満や、ルールベースの変更につながるかもしれません。

ユーザーが厳格な復号化ポリシーに対して最初は少し不満を持つかもしれませんが、その苦情によって、弱いアルゴリズムを使用している、あるいは証明書に問題があるためにブロックされている禁止された好ましくないウェブサイトに注意が向きます。ネットワーク上のトラフィックに対する理解を深めるツールとして苦情を利用してください。

各ユーザーグループや異なるユーザーに別々の復号化ポリシーが必要かもしれませんし、同じ復号化ポリシーをすべてのユーザーに適用できるかもしれません。例えば、他の従業員に適用する復号化ポリシーから重役を除外するかもしれません。また、従業員グループ、取引先、提携先、ゲストに異なる復号化ポリシーを適用するかもしれません。最新の法務および人事部のコンピューター使用規則を用意してすべての従業員、取引先、提携先、ゲスト、その他のネットワークユーザーに配布し、復号化をロールアウトする際に、脅威をスキャンするために自身のデータが復号化されるかもしれないということをユーザーに知らせます。

ゲストユーザーの扱い方は、どのようなアクセスが必要なのかによって異なります。ゲスト用の *VLAN* 、あるいはワイヤレス アクセスの場合は *SSID* を別け、ネットワークの他の場所から隔離します。企業ネットワークへのアクセスが不要なゲストはネットワークに入れないでください。そうなればトラフィックを復号化する必要もなくなります。企業ネットワークにアクセスする必要があるゲストについては、トラフィックを復号化します：

- 企業はゲストのデバイスをコントロールできません。ゲストのトラフィックは復号化してゲスト用のセキュリティポリシーを適用し、ファイアウォールがトラフィックを検査して脅威を防止できるようにしてください。これを行うには、認証ポータルを通じてゲストユーザーをリダイレクトし、*CA* 証明書のダウンロードおよびインストール方法を指示し、トラフィックが復号化されることをゲストに通知します。それを御社のプライバシーポリシーおよびコンピューター利用ポリシーに含めます。
- ゲストのアクセスを厳格にコントロールする復号化ポリシールールおよびセキュリティポリシールールを別途作成し、ゲストがアクセスする必要があるネットワーク内の領域にのみアクセスできるようにします。

各ユーザーグループの場合と同様に、どのデバイス、どのアプリケーションを復号化するのか判断します。今日のネットワークでは企業のデバイスだけでなく、BYOD デバイス、モバイル、リモートユーザーやその他のデバイスも使用されており、また取引先、提携先、ゲストのデバイスも含まれます。今日のユーザーは、許可されているサイト、許可されていないサイトの両方にアクセスしようと試みます。それらのトラフィックをどの程度復号化するのか判断する必要があります。

企業は *BYOD* デバイスをコントロールできません。ネットワークで *BYOD* デバイスを許可する場合、そのトラフィックを復号化し、他のネットワーク トラフィックに適用するのと同じセキュリティポリシーを適用し、ファイアウォールがトラフィックを検査して脅威を防げるようにします。これを行うには、*BYOD* ユーザーを認証ポータル経由でリダイレクトして、ダウンロード方法を指示して *CA* 証明書をインストールし、ユーザーに彼らのトラフィックが復号化されることを明確に通知します。*BYOD* ユーザーに対して、プロセスを教育し、それを御社のプライバシーポリシーおよびコンピューター利用ポリシーに含めます。

どのトラフィックをログに記録するのか判断し、どのトラフィックをログに記録できるのかを調査します。記録・保存できるデータの種類やデータを保存できる場所を定める現地の法律に注意してください。例えば、健康、金銭のデータなどの個人情報を記録したり保存したりすることを禁止する現地の法律があるかもしれません。

好ましくない証明書に対する対応を決めてください。例えば、証明書ステータスが未知であるセッションはブロックしますか？許可しますか？好ましくない証明書にどう対処するか決まれば、サーバー証明書の検証ステータスに基づいてどのセッションを許可するのかをコントロールする復号化ポリシーに付与する、復号化プロファイルの設定方法も決まります。

PKI ロールアウト プランの作成

公開鍵基盤（PKI）をロールアウトする方法を計画します。ネットワーク デバイスは、信頼されたサイトについては SSL フォワード トラスト CA 証明書を、信頼されていないサイトについては SSL フォワード アントラスト CA 証明書を必要とします。フォワード トラストおよびフォワード アントラスト証明書は個別に生成します（安全でない可能性があるサイトにユーザーがアクセスする際にアントラスト証明書に警告させる必要があるため、エンタープライズ ルート CA を使ってフォワード アントラスト証明書に署名しないでください）。Palo Alto Networks 次世代ファイアウォールが SSL 復号化用の CA 証明書を生成する方法は 2 つあります：

- エンタープライズ ルート **CA** から下位証明書として **SSL CA** 証明書を生成–既存のエンタープライズ PKI がある場合、これがベストプラクティスになります。ネットワーク デバイスはエンタープライズ ルート CA をすでに信頼しており、デプロイメントを開始する際に証明書の問題を回避できるようになるため、エンタープライズ ルート CA から下位証明書を生成することで、ロールアウトを簡単かつスムーズに行えるようになります。エンタープライズ ルート CA がない場合、入手することをご検討ください。
- ファイアウォール上で自己署名ルート **CA** 証明書を生成し、そのファイアウォール上で下位 **CA** 証明書を作成–エンタープライズ ルート CA がない場合、この方法で自己署名ルート CA 証明書と下位のフォワードトラストおよびアントラスト CA 証明書を入手できます。この方法では、すべてのネットワーク デバイスに自己署名証明書をインストールし、それらのデバイスがファイアウォールの自己署名証明書を認識できるようにする必要があります。証明書をすべてのデバイスにデプロイする必要があるため、この方法は大規模なデプロイよりも小規模なデプロイや、コンセプトの実証段階（POC）の検証に向いています。

フォワード アントラスト証明書をネットワーク デバイスの証明書トラスト リストにエクスポートしないでください！アントラスト証明書をトラスト リストにインストールすると、ファイアウォールが信頼していないウェブサイトをデバイスが信頼するようになるため、これが重要になります。さらに、信頼されていないサイトに対する証明書の警告がユーザーに表示されなくなり、サイトが信頼されていないことを知らないユーザーがサイトにアクセスし、ネットワークを脅威にさらしてしまうおそれもあります。

エンタープライズ ルート *CA* からフォワード トラスト証明書を生成する場合でも、ファイアウォール上で生成した自己署名証明書を使用する場合でも、各ファイアウォールに対して個別に下位フォワード トラスト *CA* 証明書を生成するようにしてください。個別の下位 *CA* を使用すれば柔軟性を確保でき、デバイス（あるいはデバイスのペア）をデコミッショニングする際に、他のデプロイメントに影響を与えることなく単一の証明書を無効化できるため、証明書を無効化する必要があるあらゆるケースで影響を減らすことができます。ユーザーに表示される *CA* のエラーメッセージには、トラフィックが経由しているファイアウォールについての情報が含まれるため、各ファイアウォールのフォワード トラスト *CA* を別けることで、問題のトラブルシューティングを行いやすくなります。すべてのファイアウォールで同じフォワード トラスト *CA* を使用すると、情報の精度が低下します。

別々のファイアウォールに対して異なるフォワード アントラスト証明書を使用するメリットはないため、すべてのファイアウォール上で同じフォワード アントラスト証明書を使用できま

す。秘密鍵のセキュリティをさらに高める必要がある場合は、秘密鍵を HSM に保存することをご検討ください。

ゲストユーザーに対して特別な対応を行いたいケースもあります。ゲストユーザーが企業ネットワークにアクセスする必要がない場合はアクセスを許可しないでください。そうすれば、ゲストユーザーのトラフィックを復号化したり、ゲスト アクセスをサポートするインフラストラクチャを作成したりする必要がなくなります。ゲスト ユーザーをサポートする必要がある場合、ゲスト トラフィックを復号化できるかどうか、法務部と相談してください。

ゲスト トラフィックを復号化できる場合、BYOD デバイスを扱う場合と同じようにゲストを扱います。ゲスト トラフィックを復号化して、その他のネットワークトラフィックに適用しているものと同じセキュリティポリシーを課します。そうするには、ゲストユーザーを認証ポータル経由でリダイレクトして、ダウンロード方法を指示して CA 証明書をインストールし、ユーザーにトラフィックが復号化されることを明確に通知します。それを御社のプライバシーポリシーおよびコンピューター利用ポリシーに含めます。さらに、ゲスト トラフィックをゲストがアクセスしなければならない領域に制限します。

法的な理由でゲスト トラフィックを復号化できない場合、ゲスト トラフィックを隔離し、ネットワーク内での横展開を防ぎます。

- ゲスト用に別のゾーンを作成し、ゲスト アクセスをそのゾーンに制限します。横展開を防ぐために、他のゾーンへのゲスト アクセスを許可しないでください。
- 許可されたアプリケーションだけを許可し、URL フィルタリングを使用してリスクのある URL カテゴリへのアクセスを防ぎ、最良のセキュリティ プロファイルを適用します。
- 復号化なしの復号化ポリシーおよびプロファイルを適用し、ゲストが未知あるいは失効した CA を持つウェブサイトにアクセスしないようにします。

すべての従業員、契約先、提携先、その他のユーザーは通常の企業のインフラを使用し、そのトラフィックを復号化して検査しなければなりません。

復号化ファイアウォールのデプロイメントのサイジング

暗号化されたトラフィックを復号化する際、ファイアウォールの CPU リソースを消費するため、スループットに影響が出るおそれがあります。通常、セキュリティが強固である場合（多くの SSL トラフィックを復号化し、また厳格なプロトコル設定を使用）、復号化により多くのファイアウォール リソースが消費されます。Palo Alto Networks の SE/CE と協力して、ミスがないようにファイアウォールのデプロイをサイジングしてください。復号化のリソース消費量に影響し、そのためファイアウォールが復号化できるトラフィックの量を左右する要素には、次のようなものがあります：

- 復号化する SSL トラフィックの量。これはネットワーク毎に異なります。例えば、マルウェアの侵入、ネットワークのエクスプロイト、不正なデータ移動を防止するために復号化しなければならないアプリケーションもあれば、現地の法や規制、ビジネス上の理由で復号化できないアプリケーションもあり、またクリアテキスト（暗号化されていない）であり復号化する必要がないアプリケーションもあります。復号化するトラフィックが増えるほど、必要なリソースも多くなります。
- TLS プロトコル バージョン。高いバージョンはより安全ですが、リソースを多く消費します。セキュリティを最大限に高めるために最大の TLS プロトコル バージョンを使用してください。

- キーのサイズ。キーのサイズが大きいほどセキュリティが向上しますが、キーの処理で消費するリソースも多くなります。
- キー交換アルゴリズム。Diffie-Hellman Ephemeral（DHE）、Elliptic-Curve Diffie-Hellman Exchange（ECDHE）などの Perfect Forward Secrecy（PFS）のその場限りのキー交換アルゴリズムは、Rivest-Shamir-Adleman（RSA）アルゴリズムよりも多くのリソースを消費して処理を行います。ファイアウォールがセッション毎に新しい暗号を生成しなければならない PFS キー交換アルゴリズムは、RSA キー交換アルゴリズムよりも安全ですが、新しいキーを生成するために多くのファイアウォール リソースを消費します。しかし、攻撃者がセッション キーを手に入れた場合、PFS は攻撃者がそれを使って同じクライアントおよびサーバー間で復号化を行うのを防止しますが、RSA にはそれができません。
- 暗号化アルゴリズム。キー交換アルゴリズムは、暗号化アルゴリズムが PFS と RSA のどちらなのかを決定します。
- 証明書の認証方法。RSA (RSA 鍵交換アルゴリズムではない) は、Elliptic Curve Digital Signature Algorithm (ECDSA) よりも少ないリソースを消費しますが、ECDSA はより安全です。

  鍵交換アルゴリズムと証明書認証方式の組み合わせは、***RSA*** および ***ECDSA*** benchmark tests に示すようにスループット・パフォーマンスに影響します。***PFS*** ではパフォーマンス コストが高い代わりに強固なセキュリティを得られますが、すべてのタイプのトラフィックで ***PFS*** が必要というわけではありません。ファイアウォール***CPU*** サイクルを節約するには、脅威を復号化して検査するトラフィックに ***RSA*** を使用しますが、これは機密性が高くありません。
- トランザクション平均サイズ。例えば、トランザクション平均サイズが小さいと、復号化でより多くの処理パワーを消費します。すべてのトラフィックでトランザクション平均サイズを計測してから、ポート 443（HTTPS で暗号化されたトラフィックのデフォルトのポート）上のトラフィックのトランザクション平均サイズを計測し、ファイアウォールに向かう暗号化されたトラフィックの割合と、総トラフィック、トランザクション平均サイズの相関性を把握します。異常に大きなトランザクションなど、異常値は省いてトランザクション平均サイズの精確な数値を得ます。
- ファイアウォール モデルおよびリソース。新しいファイアウォール モデルは古いモデルよりも高い処理能力を持っています。

これらの要素の組み合わせにより、復号化によってファイアウォールの処理リソースがどのように消費されるのかが異なってきます。ファイアウォールのリソースを最大限に活用するために、保護中のデータのリスクを把握してください。ファイアウォール リソースに問題があれば、優先度の高いトラフィックに対しては強力な復号化を使い、優先度の低いトラフィックに対しては処理量の小さい復号化を使用して復号化・検査を行い、空きリソースを増やしていきます。例えば、センシティブでない、あるいは優先度の低いトラフィックに対しては ECDHE や ECDSA の代わりに RSA を使用し、優先度の高いセンシティブなトラフィックに対して PFS ベースの復号化を行うために使用するファイアウォール リソースを確保します。（優先度の低いトラフィックを復号化・検査できますが、代わりに PFS ほど強力でないアルゴリズムを使えば必要なリソース消費量を減らすことができます） 各種のトラフィック タイプのリスクを把握し、それに従って対処することが重要です。

ファイアウォールのパフォーマンスを計測して現在利用できるリソースを把握すれば、復号化したいトラフィックを復号化するためにより多くのファイアウォール リソースが必要かどうか判

断しやすくなります。また、ファイアウォールのパフォーマンスを計測することで、復号化のデプロイ後にパフォーマンスを比較するためのベースラインも得られます。

ファイアウォールのデプロイメントをサイジングする際は、現在のニーズだけでなく未来のニーズも考慮してください。ガートナー氏は、2019 年を通じて 80% を超える企業の Web トラフィックが暗号化され、50% を超える新しいマルウェア キャンペーンが様々な形の暗号化を使用すると予測しています。トラフィックを復号化できる余地を確保しておいてください。Palo Alto Networks の担当者と協力し、そのファイアウォールのサイジングに関する実績を活用してファイアウォールの復号化のサイジングをサポートしてもらってください。

段階的な優先順位付きデプロイメント計画

制御された形で部分毎に復号化をロールアウトする準備を行います。復号化のデプロイメントをすべて一度にロールアウトしないでください。復号化が計画通りに機能していること、およびユーザーが作業の内容や理由を把握していることをテストして確認します。この方法で復号化をロールアウトすることで、予定通りに機能しないものがあった場合のトラブルシューティングを行いやすくなり、ユーザーが変更に対応しやすくなります。

復号化設定によりウェブサイトの利用可能性が変化する場合がかるため、関係者、従業員、取引先や提携先などのその他のユーザーに情報を伝えることが重要です。以前はアクセスできたウェブサイトにアクセスできなくなった際の対応方法、技術サポートに伝えるべき情報は何なのかを、ユーザーに理解させておく必要があります。問題を抱えたユーザーをサポートするためには、サポートスタッフがいつ、どのように、何がロールアウトされたのかを把握しておかなければなりません。一般ユーザーを対象にした復号化をロールアウトする前に：

- 復号化をサポートできる初期ユーザー、完全にロールアウトする際に疑問を抱えた他のユーザーをサポートできるユーザーを探します。部課のマネージャー協力を求め、トラフィックを復号化するメリットを伝えます。
- トラフィックを復号化することの重要性を理解している初期ユーザーおよびその他の従業員が各部課で行うコンセプトの実証段階（POC）試験をセットアップします。POC の参加者に変更点、および問題が発生した場合に技術サポートに連絡する方法を伝えます。このような方法により、POC の技術サポートと共に復号化の POC をサポートできる機会が得られ、本番のロールアウトを最もスムーズに行える方法を策定できるようになります。また、POC のユーザーと技術サポートがやり取りし合うことで、ポリシーやユーザーに情報を提供する方法を微調整できるようになります。

  POC を使用すると、何を最初に復号化するかという優先順位を検証できるため、全体で復号化を段階的に行うときに、POC エクスペリエンスによって、さまざまな URL カテゴリの復号化を段階的に行う方法を理解するのに役立ちます。ファイアウォールのサイジングが適切かどうか、あるいはアップグレードが必要かどうかを把握するために、ファイアウォールの CPU とメモリの使用に及ぼす復号化の影響を測定します。POC は、復号化が技術的に失敗する (復号化によってトラフィックがブロックされる) アプリケーションを明らかにし、Decryption Exclusion リストに追加する必要があるアプリケーションを明らかにすることもできます。

  POC を設定するときは、一般的なロールアウトの前に運用上の準備と手順を証明できるユーザー グループもセットアップします。

- 本番のロールアウト前にユーザーに情報を伝え、新しいユーザーが企業に参加した際の訓練方法を計画します。復号化をデプロイする際にこの段階が重要な理由は、復号化により、ユーザーが以前はアクセスできたが、安全でないためにアクセスできなくなるウェブサイトが生じる可能性があるためです。POC を経験することで、伝えるべき最も重要な内容を判断しやすくなります。
- フェーズごとの復号化これには複数の方法があります。優先順位が最も高いトラフィック（例えば、ゲームなど、悪意のあるトラフィックがありがちな URL カテゴリ）を最初に復号化してから、経験を得ながら復号化を増やしていくことができます。あるいは、より保守的な方法で、（問題が発生してもビジネスが影響を受けないよう）ビジネスに影響を与えない URL カテゴリ、例えばニュースフィードなどを最初に復号化することもできます。どのケースでも、復号化を段階的に導入する最適な方法は、いくつかの URL カテゴリを復号化し、ユーザーのフィードバックを取り入れ、レポートを発行して復号化が予定通りに機能していることを確認してから、徐々に復号化する URL カテゴリを増やしながら検証などの作業を繰り返すことです。Decryption Exclusions を作成して、技術的な理由でサイトを復号化できない場合、または復号化しないことを選択した場合に、サイトを復号化から除外するように計画します。

  Enable Users to Opt Out of SSL Decryption (ユーザは、復号化をやめてサイトに移動せずにセッションを終了するか、サイトに進み、トラフィックの復号化に同意するかのいずれかを可能にする応答ページを参照します)、それが何であるか、なぜユーザはそれを見ているのか、そしてユーザの選択肢は何なのかについてユーザに示します。
- ロールアウトの各段階を十分に評価できる、現実的なデプロイの予定を立ててください。

すべてのネットワーク トラフィックを確認できる位置にファイアウォールを設置し、暗号化されたトラフィックがファイアウォールを回避することで、予期せずにネットワークにアクセスできないようにしてください。

復号化するトラフィックの定義

復号化ポリシー ルールにより、ファイアウォールに復号化させるトラフィックと、プライバシーや現地の規制などの理由で復号化から除外するトラフィックを定義します。

復号化プロファイルを各復号化ポリシー ルールに付与し、プロファイルに応じて証明書チェック、セッション モード チェック、エラーチェック、プロトコルおよびアルゴリズムのチェックを有効化します。これらのチェックにより、証明書の発行者を信頼できないセッション、弱いプロトコル、暗号、アルゴリズム、証明書に問題があるサーバーなど、リスクのある接続を防ぎます。

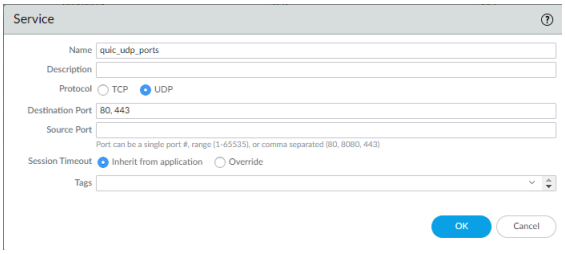
復号化デプロイメントのベストプラクティスのチェックリストを確認し、推奨されるベストプラクティスを把握してください。

マルウェア、フィッシング、ダイナミック DNS、未知、コマンド& コントロール、プロキシ回避・アノニマイザー、著作権侵害、エクストリミズム、新しく登録されたドメイン、グレイウェアおよびパークドなどの既知の危険な URLフィルタリング カテゴリをブロックします。ビジネス上の理由でこれらのうちいずれかのカテゴリーを許可しなければならない場合、それらを復号化して厳格なセキュリティ プロファイルをトラフィックに適用します。

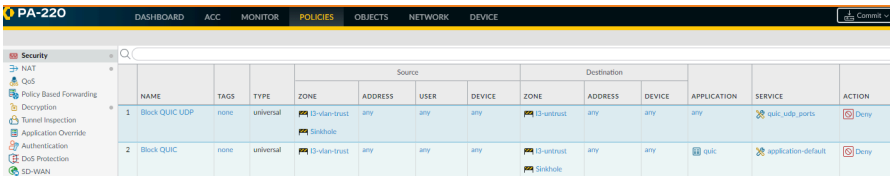
許可する場合に必ず復号化すべき URL カテゴリとしては、online-storage-and-backup、web-based-email、web-hosting、personal-sites-and-blogs、content-delivery-networks などがあります。

ビジネス上の理由で暗号化されたブラウザのトラフィックを許可する場合を除き、セキュリティポリシーでクイック *UDP* インターネット接続（*QUIC*）をブロックします。*Chrome* およびその他の一部のブラウザは *TLS* ではなく *QUIC* を使ってセッションを確立しますが、*QUIC* はファイアウォールが復号化できないプロプライエタリな暗号化を使用するため、危険があるトラフィックが暗号化されたトラフィックの状態でネットワークに侵入するおそれがあります。*QUIC* をブロックするとブラウザが *TLS* にフォールバックするため、ファイアウォールがトラフィックを復号化できるようになります。

UDP のサービスポート（*80* および *443*）で *QUIC* をブロックするセキュリティポリシールールを作成し、*QUIC* アプリケーションをブロックする別のルールを作成します。*UDP* ポート *80* および *443* をブロックするルールでは、*UDP* ポート *80* および *443* を含むサービス（***Objects***（オブジェクト） > ***Services***（サービス））を作成します。



サービスを使用して、*QUIC* をブロックする *UDP* ポートを指定します。*2* 番目のルールで、*QUIC* アプリケーションをブロックします。



- 復号化ポリシーの作成
- 復号化ポリシー ルールの作成

復号化ポリシーの作成

復号化プロファイルを使用すれば、復号化されたトラフィックおよび SSL 復号化から除外することにしたトラフィックの両方をチェックすることができます。（証明書のピンニングあるいはその他の理由でサーバーが SSL 復号化を技術的に妨げる場合、サーバーを復号化除外リストに追加します） 次の目的で要件に合わせて復号化プロファイルを作成します：

- 証明書が失効したセッションのブロック、信頼できない発行者、未知の証明書ステータス、証明書ステータスのチェックのタイムアウト、証明書の拡張子など、証明書ステータスに基づいてセッションをブロックします。
- サポートされていないバージョンや Cipher Suite を持つセッション、クライアント認証が必要なセッションをブロックします。
- 復号化を実行するためのリソース、あるいは証明書に署名するためのハードウェア セキュリティモジュールが利用できない場合にセッションをブロックする。
- SSL プロトコル設定内で、SSL 転送プロキシおよびSSL インバウンド インスペクション トラフィックに許可するプロトコル バージョン、キー交換、暗号化、認証アルゴリズムを定義します。

大抵のサイトに適用するメインの復号化プロファイルを弱体化させて脆弱なサイトに使用しないでください。そうせずに、サポートする必要がありながら、強力な暗号やアルゴリズムをサポートしていないサイト用に、個別の復号化プロファイルを一つあるいは複数作成します。また、異なる URL カテゴリに対して別々の復号化プロファイルを作成し、センシティブな情報を含まないトラフィック用にセキュリティとパフォーマンスのバランスを取ることもできます。しかし、復号化できるトラフィックはすべて復号化して検査するようにしてください。

作成した復号化プロファイルは復号化ポリシーに追加します。この復号化ポリシー ルールに一致するトラフィックに対し、ファイアウォールが復号化プロファイルの各設定を適用します。

Palo Alto Networksのファイアウォールにデフォルトの状態で含まれている復号化プロファイルを使用すれば、復号化されたトラフィックに対して推奨される基本的なプロトコルのバージョン、Cipher Suiteを利用できます。ただし、ベストプラクティスは、「SSL 転送プロキシの復号化プロファイル」、「SSL インバウンド インスペクション 復号化プロファイル」、および「SSL プロトコル設定 復号化プロファイル」で説明されているように、より厳密な復号化制御を有効にすることです。

攻撃者がエクスプロイトできる脆弱性が判明しているため、弱いプロトコルやアルゴリズムをサポートしないようにしてください。弱いプロトコルを持つ古いシステムを使用している重要な提携先や取引先があり、弱いプロトコルやアルゴリズムを許可しなければならない場合は、例外用の復号化プロファイルを別に作成し、対象のトラフィック（例えば、提携先の送信元 *IP* アドレス）にのみプロファイルを適用する復号化ポリシー ルールにそれを付与します。すべてのトラフィックに対して弱いプロトコルを許可しないようにしてください。

STEP 1 | 新しい復号化プロファイルを作成します。

Objects (オブジェクト) > **Decryption Profile (復号化プロファイル)** を選択し、復号化プロファイル ルールを **Add (追加)** あるいは変更し、そのルールに分かりやすい **Name (名前)** を付けます。

STEP 2 | （任意）ファイアウォール上のすべての仮想システム、あるいはあらゆる Panorama デバイスグループでそのルールを**Shared (共有)** することを許可します。

STEP 3 | （復号ミラーリングのみ）ファイアウォールがイーサネットInterface[インターフェイス]を使用するよう有効化を行い、復号化されたトラフィックのコピーおよび転送を行います。

このタスクとは別に、復号ポート ミラーリングの設定を行う各ステップに従います。ミラーリングを禁止していたり、ミラーリングできるトラフィックの種類を制限したりしている現地のプライバシー規制がないか注意してください。復号ポート ミラーリングには復号化ポート ミラーライセンスが必要になります。

STEP 4 | （任意）SSL トンネリングを使用したトラフィックやインバウンドトラフィックをブロック・制御します。

復号化プロファイルを復号化されたトラフィックに適用することは任意ですが、復号化プロファイルを常にポリシールールに適用してネットワークを暗号化された脅威から保護することがベストプラクティスになります。目に見えない脅威は防止できません。

SSL Decryption[SSL復号化]を選択します。

- **SSL Forward Proxy (SSL転送プロキシ)**を選択し、証明書を検証するための設定を行い、プロトコルのバージョンおよびCipher Suiteを指定し、SSL復号化済みのトラフィックに対して失敗のチェックを行うよう設定します。この設定は、SSLフォワード プロキシ復号化を行うよう設定された復号化ポリシー ルールにプロファイルが追加された場合にのみ有効になります。
- **SSL Inbound Inspection (SSL**インバウンド インスペクション**)** を選択して設定を行い、プロトコルのバージョンおよび Cipher Suite を指定し、SSL インバウンド トラフィックに対して失敗のチェックを行うようにします。この設定は、SSLインバウンド インスペクションを行う復号化ポリシー ルールにプロファイルが追加された場合にのみ有効になります。
- **SSL Protocol Settings (SSL** プロトコル設定**)** を選択し、プロトコル バージョン、復号化された SSL トラフィックに求める鍵交換、暗号化、認証アルゴリズムを制御する設定を行います。この設定は、SSLフォワード プロキシ復号化またはSSLインバウンド インスペクションを行うよう設定された復号化ポリシー ルールにプロファイルが追加された場合に有効になります。

ファイアウォールが *FIPS-CC* モードで、標準モードの管理サーバーである *Panorama* ™ 管理サーバーによって管理されている場合は、暗号化解除プロファイルをファイアウォール上でローカルに作成する必要があります。標準モードの *Panorama* で作成された暗号化解除プロファイルには、***3DES*** および ***RC4*** 暗号化アルゴリズムと ***MD5*** 認証アルゴリズムへの参照が含まれます。

STEP 5 | （任意）ポリシー ベース復号化除外を作成することにしたトラフィック（例：URLカテゴリ）をブロック・制御します。

復号化プロファイルを復号化しないことにしたトラフィックに適用することは任意ですが、復号化プロファイルを常にポリシールールに適用してネットワークを証明書が失効したセッションや発行者を信頼できないセッションから保護することがベストプラクティスになります。

Decryption を選択して復号化なしのプロファイルを構成し、有効期限が切れた証明書でセッションをブロックする および 信頼できない発行者とのセッションをブロックする ボックスをオンにして、復号化から除外されているトラフィックの証明書を検証します。ポリシーベースの例外は、復号化しないことにしたトラフィックのみを対象にして作成してください。サーバーが技術的な理由で復号化を妨げる場合、ポリシーベースの除外を作成せず、サーバーを SSL 復号化除外リストに追加してください（**Device (デバイス)** > **Certificate Management (証明書の管理)** > **SSL Decryption Exclusion (SSL 復号化除外)**）。

この設定は、特定のトラフィックに対する復号化を無効にする復号化ポリシー ルールに復号化プロファイルが追加された場合にのみ有効になります。

STEP 6 | （任意）復号化された SSL トラフィックのブロックと制御を行います。

SSH Proxy を選択して、SSH プロキシ復号化プロファイルを構成し、サポートされているプロトコル・バージョンを適用し、システム・リソースが暗号化解除の実行に使用できない場合にセッションをブロックするように設定を構成します。

この設定は、SSHトラフィックを復号化する復号化ポリシー ルールに復号化プロファイルが追加された場合にのみ有効になります。

STEP 7 | 復号化ポリシー ルールの作成を行う際に復号化プロファイルを追加します。

ファイアウォールは、復号化ポリシー ルールにマッチするトラフィックに対し、復号化プロファイルを適用し、プロファイルの設定を強制します。

STEP 8 | 設定を **Commit**（コミット）します。

復号化ポリシー ルールの作成

Decryption ポリシールールを作成して、firewall が復号化するトラフィックと、ファイアウォールで実行する復号化のタイプを定義します。SSL 転送プロキシ、SSL インバウンド インスペクション、あるいは SSH プロキシ復号化。Decryption ポリシー規則を使用して、Decryption Mirroring を定義することもできます。

STEP 1 | 新しい復号化ポリシー ルールを追加します。

Policies > **Decryption**, **Add** を新しい Decryption ポリシー規則として選択し、ポリシー規則に説明的な **Name** を指定します。

STEP 2 | ネットワークおよびポリシーオブジェクトに基いてトラフィックが一致するよう、復号化ルールの設定を行います。

- **Firewall security zones**[ファイアウォールのセキュリティゾーン]—**Source**[送信元]かつ/または**Destination**[宛先]を選択し、**Source Zone**[送信元ゾーン]かつ/または**Destination Zone**[宛先ゾーン]に基いてトラフィックを一致させるよう設定します。
- **IP**アドレス、アドレスオブジェクト、かつ/またはアドレスグループ—**Source (**送信元**)** かつ/または **Destination (**宛先**)** を選択し、**Source Address (**送信元アドレス**)** かつ/または **Destination Address (**宛先アドレス**)** に基いてトラフィックを一致させるよう設定します。あるいは、**Negate**[拒否]を選択して送信元アドレスのリストを復号化から除外します。
- **Users**[ユーザー]—**Source**[送信元]を選択し、トラフィック復号化の対象となる**Source User**[送信元ユーザー]を設定します。特定のユーザーあるいはグループのトラフィック、あるいは未知のユーザーやログオン前のユーザー（GlobalProtectに接続しているがログインしていないユーザー）といった特定の種類のユーザーに対して復号化を行うことができます。
- **Ports and protocols**[ポートおよびプロトコル]—**Service/URL Category**[サービス/URLカテゴリ]を選択し、サービスに基いてトラフィックを一致させるようルールを設定します。デフォルト設定では、ポリシールールはTCPおよびUDPポート上の**Any**[すべて]のトラフィックを復号化するように設定されています。サービスあるいはサービスグループを **Add (**追加**)** し、アプリケーションのデフォルトポート上でのみアプリケーションを一致させるよう、任意で **application-default** を設定することもできます。

アプリケーションの既定の設定は、ポリシーベースの復号化除外 を作成する場合に便利です。標準的なポート以外で検知されたアプリケーションの復号化は行いつつ、同じアプリケーションがデフォルトポートで実行されている場合は除外することができます。

- **URLs and URL categories**[URLおよびURLカテゴリ]—Service/URL Category [サービス/URLカテゴリ]を選択し、次の項目に基いてトラフィックを復号化します。
  - ファイアウォールがポリシー強化のために取得する、外部でホストされているURLのリスト（**Objects (**オブジェクト**)** > **External Dynamic Lists (**外部動的リスト**)**を参照）。
  - Palo Alto Networks は、 URL カテゴリを事前定義していますが、これにより許可されたトラフィックのカテゴリ全体を簡単に解読できます。個々のサイトではなくカテゴリに基づいてセンシティブなサイトを除外できるため、このオプションは、ポリシーベース復号化除外を作成する際にも役立ちます。例えば、カスタム URL カテゴリを作成して復号化を行いたくないサイトをグループ化できますが、定義済みの Palo Alto Networks の URL カテゴリに基づいて金融あるいはヘルスケア関連のサイトを復号化から除外したりすることも可能です。さらに、危険な URL カテゴリをブロックし、コンフォート ページの作成 を実行して、サイトがブロックされた理由を伝えたり、ユーザーが SSL 復号化をオプトアウトできるようにする を行うことができます。

    事前定義されている高リスクおよび中リスクの URL カテゴリを使用して、すべての高リスクおよび中リスクの URL トラフィックを復号する複合化ポリシールールを作成します。ルールベース (センシティブな情報を復号化しないように、すべての復号化の例外がこのルールに優先します) の下部にそのルールをセーフティーネットとして配置し、すべてのリスクのあるトラフィックを確実に復号化し検査します。ただし、アク

セスを許可している高リスクまたは中リスクのサイトに個人情報 (PII) が含まれていたり、復号化すべきではないその他のセンシティブ情報が含まれていたりする場合、これらのサイトをブロックしてプライバシーに関する問題を回避しながら、復号化されているリスクのあるトラフィックを許可することを避けるか、あるいはセンシティブなトラフィックに対応するための復号化禁止ルールを作成します。

- カスタム URL カテゴリ（**Objects (オブジェクト)** > **Custom Objects (**カスタム オブジェクト**)** > **URL Category (URL** カテゴリ**)**を参照）。たとえば、カスタム URL カテゴリを作成して、ビジネス目的でアクセスする必要があるが、最も安全なプロトコルとアルゴリズムをサポートしていないサイトのグループを指定し、カスタマイズされた Decryption プロファイルを適用して、それらのサイトのみに対してより緩やかなプロトコルとアルゴリズムを許可することができます (これにより、ほとんどのサイトで使用する Decryption プロファイルをダウングレードしてもセキュリティが低下することはありません)。

STEP 3 | マッチするトラフィックを復号化するか、トラフィックを復号化から除外するルールを設定します。

Options[オプション]を選択し、ポリシールールの**Action**[アクション]を設定します。

マッチするトラフィックを復号化する：

1. **Action** を **Decrypt** に設定します。
2. マッチするトラフィックに対してファイアウォールが実行する復号化の **Type (タイプ)** を設定します。
   - SSL Forward Proxy.
   - SSL インバウンド インスペクション。次に、**Add** は、インバウンド SSL トラフィックの宛先内部サーバーに対して **Certimatecate** を実行します。SSL Inbound Inspection ポリシー規則は、最大 12 個の証明書をサポートします。

   Decryption ポリシー規則を構成して、複数のドメインをホストする内部サーバーにバインドされた *SSL/TLS* トラフィックを復号化し、各ドメインに独自の証明書を持たせることができます。ファイアウォールは、要求された *URL* に対してサーバーが提示する証明書と一致するポリシー・ルール内の証明書を使用して、*SSL/TLS* 接続をネゴシエーションします。

   ダウンタイムを発生させずに保護された内部サーバーの証明書を更新するには、有効期限が切れる前に、または無効になる前に、新しいサーバー証明書を更新または取得します。次に、証明書と秘密鍵をファイアウォールにインポートし、*SSL Inbound Inspection* ポリシー・ルールに追加してから、同じ証明書を *Web* サーバーにインストールします。*Web* サーバー上で別の証明書がアクティブであるときに、ポリシー・ルールを新しい証明書で更新すると、ファイアウォールは、使用中の証明書に関係なく、サーバーへのトラフィックを暗号化解除する準備をします。SSL Inbound Inspection の構成 では、このプロセスについてさらに詳しく説明します。

   (Panorama™) SSL Inbound Inspection ポリシー規則における複数の証明書のサポートは、*PAN-OS 10.2* より前の *PAN-OS®* バージョンでは利用できません。*PAN-OS 10.2* を実行している *Panorama* 管理サーバーからの複数の証明書を含む *SSL Inbound Inspection* ポリシー規則を、以前のバージョンを実行している *firewall* にプッシュすると、管理対象 *firewall* のポリシー規則は、アルファベット順にソートされた証明書リストからの最初の証明書のみを継承します。

   パノラマから *Decryption* ポリシールールをプッシュする前に、*PAN-OS 10.1* 以前を実行しているファイアウォール用に異なる templates または device groups を設定して、正しいポリシールール と証明書を適切な *firewall* に確実にプッシュすることをお勧めします。

- SSH Proxy.

マッチするトラフィックを復号化から除外する：

Action (アクション) を **No Decrypt (復号化なし)** に設定します。

STEP 4 | （任意）**Decryption Profile (復号化プロファイル)** を選択し、ポリシールールにマッチするトラフィックに対して追加のチェックを行います。

復号化プロファイルを復号化されたトラフィックに適用することは任意ですが、復号化プロファイルを常にポリシールールに適用してネットワークを暗号化された脅威から保護することがベストプラクティスになります。目に見えない脅威は防止できません。

例えば、Decryption プロファイルをポリシー・ルールにアタッチして、サーバー証明書が有効であることを確認し、サポートされていないプロトコルまたは暗号を使用するセッションをブロックします。Decryption プロファイルを作成する には、**Objects** > **Decryption Profile** を選択します。

1. Decryption ポリシー ルールを作成するか、既存のルールを開いて変更します。
2. **Options (オプション)**、**Decryption Profile (復号化プロファイル)** の順に選択し、ルールに一致するトラフィックの各要素を制御し、ブロックします。

   一致するトラフィックにファイアウォールが適用するプロファイル ルール設定は、ポリシールールの**Action (アクション)**（Decrypt (復号化) またはNo Decrypt (復号化なし)）およびポリシールールの**Type (タイプ)**（SSL Forward Proxy (SSL転送プロキシ)、SSL Inbound Inspection (SSLインバウンド インスペクション)、SSH Proxy (SSLプロキシ)）によって異なります。これにより、さまざまな種類のトラフィックとユーザーに適用されるさまざまな種類の Decryption ポリシー規則で、さまざまな Decryption プロファイルを使用できます。
3. **OK** をクリックします。

STEP 5 | Configure Decryption logging(成功した TLS ハンドシェイクと失敗した TLS ハンドシェイクの両方をログに記録するかどうかを設定し、Decryption ログ転送を設定します)。

STEP 6 | **OK** をクリックしてポリシーを保存します。

STEP 7 | 次のステップを選択し、ファイアウォールがトラフィックを復号化する機能を完全に有効化します...

- SSL Forward Proxy を構成します。
- SSL Inbound Inspection を設定します。
- Configure SSH Proxy.
- 暗号化を解除しないトラフィックに対してポリシーベースの 復号化除外 を作成し、暗号化を解除しない 選択 し、固定された証明書や相互認証などの技術的な理由で復号化を破るサイトを SSL Decryption Exclusion リストに追加します。

SSL フォワード プロキシの設定

ファイアウォールにSSL 転送プロキシ復号化を実行させるには、クライアントとサーバーの間のセッションに対してそのファイアウォールが信頼された第 3 者（プロキシ）であることを証明するために求められる証明書をセットアップする必要があります。ファイアウォールは企業用の証明書認証局（CA）が署名した証明書あるいはファイアウォール上でフォワード トラスト証明書として生成された自己署名証明書を使用して、クライアントとの SSL セッションを認証できます。

- (ベスト プラクティス) エンタープライズ **CA** 署名証明書 : エンタープライズ CA は、SSL 復号化を必要とするサイトの証明書の署名にファイアウォールが使用できる署名証明書を発行できます。宛先サーバーの証明書に署名したCAをファイアウォールが信頼する場合、ファイアウォールはエンタープライズ CAによって署名が付与されたクライアントに宛先サーバーの証明書のコピーを送信できます。通常、すべてのネットワーク デバイスはすでにエンタープライズ CA を信頼しており（デバイスの CA トラスト ストレージにすでにインストールされているのが普通です）、エンドポイントに証明書をデプロイする必要がなく、ロールアウト プロセスをスムーズに行えるようになるため、これがベストプラクティスになります。
- 自己署名証明書—ファイアウォールは CA として機能し、SSL 復号化が求められるサイトの証明書に署名するためにファイアウォールが使用できる自己署名証明書を生成できます。ファイアウォールはサーバー証明書のコピーに署名し、それをクライアントに提示して SSL セッションを確立できます。また、この方法ではすべてのネットワーク デバイスに自己署名証明書をインストールし、それらのデバイスがファイアウォールの自己署名証明書を認識できるようにする必要があります。証明書をすべてのデバイスにデプロイする必要があるため、この方法は大規模なデプロイよりも小規模なデプロイや、コンセプトの実証段階（POC）の検証に向いています。

さらに、クライアントが信頼しないCAによってサーバーが署名されている場合にファイアウォールがクライアントに提示するフォワード アントラスト証明書をセットアップします。これを使用すると、信頼されない証明書を持つサイトにクライアントがアクセスしようとしたときに、証明書警告のプロンプトが表示されます。

エンタープライズ ルート *CA* からフォワード トラスト証明書を生成する場合でも、ファイアウォール上で生成した自己署名証明書を使用する場合でも、各ファイアウォールに対して個別に下位フォワード トラスト *CA* 証明書を生成するようにしてください。個別の下位 *CA* を使用すれば柔軟性を確保でき、デバイス（あるいはデバイスのペア）をデコミッショニングする際に、他のデプロイメントに影響を与えることなく単一の証明書を無効化できるため、証明書を無効化する必要があるあらゆるケースで影響を減らすことができます。ユーザーに表示される *CA* のエラーメッセージには、トラフィックが経由しているファイアウォールについての情報が含まれるため、各ファイアウォールのフォワード トラスト *CA* を別けることで、問題のトラブルシューティングを行いやすくなります。すべてのファイアウォールで同じフォワード トラスト *CA* を使用すると、情報の精度が低下します。

SSLフォワード プロキシ復号化に必要となるフォワード トラストおよびフォワード アントラストのセットアップを行った後、復号化ポリシー ルールを作成し、ファイアウォールに復号化させたいトラフィックを定義し、SSL 制御とチェックをトラフィックに適用する復号化プロファイルを作成します。復号化ポリシーは、ルールをクリア テキスト トラフィックにマッチさせ

る、SSL トンネル内のトラフィックを復号化します。ファイアウォールは、復号化ポリシーおよびファイアウォールのセキュリティポリシーに付与された復号化プロファイルに基づいてトラフィックをブロックおよび制限します。ファイアウォールは、トラフィックがファイアウォールを離れる際にトラフィックを再度暗号化します。

SSL フォワード プロキシを設定すると、プロキシされたトラフィックは *DSCP* コード ポイントまたは *QoS* をサポートしません。

STEP 1 | 適切なインターフェイスがバーチャル ワイヤー、レイヤー 2、またはレイヤー 3 インターフェイスのいずれかとして設定されていることを確認します。

Network (ネットワーク) > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** タブで設定されているインターフェイスを確認します。**Interface Type** [インターフェイス タイプ]列にはインターフェイスが **Virtual Wire** [バーチャル ワイヤー]、**Layer 2** [レイヤー 2]、または **Layer 3** [レイヤー 3]インターフェイスとして設定されているかが表示されます。インターフェイスを選択して、インターフェイスのタイプなどの設定を変更できます。

STEP 2 | 信頼できる CA がサーバー証明書に署名している場合にファイアウォールがクライアントに提示するフォワード トラスト証明書を構成します。エンタープライズ CA 署名付きの証

明書あるいは自己署名証明書をフォワード トラスト証明書として使用することができます。

（推奨されるベストプラクティス）エンタープライズ CA 署名付きの証明書をフォワード トラスト証明書として使用します。一意の名前を持つフォワード トラスト証明書を各ファイアウォール上で作成します：

1. エンタープライズ CA が署名および検証するための証明書署名要求 (CSR) を生成します。
   1. **Device** > 証明書の管理 > 証明書 を選択して、生成をクリックします。
   2. 証明書名 を入力します。各 ファイアウォール に一意の名前を使用します。
   3. 証明者 からドロップダウンで、**External Authority (CSR)**.
   4. (オプション) エンタープライズ CA で必要な場合は、証明書の属性 を追加して、国や部署などの ファイアウォール の詳細をさらに識別します。
   5. 生成 をクリックして CSR を保存します。保留中の証明書が デバイス証明書 タブに表示されるようになりました。
2. CSR をエクスポートします:
   1. デバイス証明書 タブに表示されている保留中の証明書を選択します。
   2. 証明書のエクスポート をクリックして証明書ファイルをダウンロードして保存します。

      秘密キーが ファイアウォール側に に安全に残るようにするため秘密鍵のエクスポート を未選択のままにしておきます。
   3. **OK**をクリックします。
3. エンタープライズ CA に証明書ファイルを提供します。エンタープライズ CA から、エンタープライズ CA 署名付きの証明書を受信した後、ファイアウォール上にインポートするエンタープライズ CA 署名付きの証明書を保存します。
4. エンタープライズ CA 署名付きの証明書をファイアウォールにインポートします。
   1. **Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificates (証明書)** の順に選択し、**Import (インポート)** をクリックします。
   2. 保留中の**Certificate Name (証明書名)**を正確に入力します。保留中の証明書が検証されるためには、入力する **Certificate Name** [証明書名]が保留中の証明書の名前と正確に一致する必要があります。
   3. エンタープライズ CA から受信した、署名された**Certificate File**[証明書ファイル] を選択します。
   4. **OK** をクリックします。キーおよび CA のチェック ボックスがオンの状態で、証明書が有効として表示されます。
5. 検証された証明書を選択し、**Forward Trust Certificate**（フォワード トラスト証明書）として有効にすることで、SSL フォワード プロキシ復号化に使用できるようにします。
6. **OK**をクリックし、エンタープライズ CA 署名付きのフォワード トラスト証明書を保存します。

自己署名付きの証明書をフォワード トラスト証明書として使用します：

1. 自己署名ルート CA 証明書を作成します。

2. 自己署名ルート CA 証明書をクリック（**Device (デバイス)** > **Certificate Management (証明書の管理)** > **Certificates (証明書)** > **Device Certificates (デバイス証明書)**）をクリックして**Certificate information (証明書情報)**を開いてから、**Trusted Root CA (信頼されたルート CA)**のチェックボックスをクリックします。
3. **OK** をクリックします。
4. 各ファイアウォールに対して新しい下位 CA 証明書を生成します：
   1. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書）
   2. ウィンドウの下部にある **Generate**[生成] をクリックします。
   3. **Certificate Name**（証明書名）を入力します。
   4. **Common Name**（共通名）に、「192.168.2.1」などの名前を入力します。これは、証明書に表示される IP または FQDN にする必要があります。この場合は、信頼できるインターフェイスの IP を使用します。このフィールドではスペースを使用しないでください。
   5. **Signed By (署名者)**フィールドで、作成した自己署名ルート CA 証明書と同じものを選択します。
   6. **Certificate Authority**[認証局] チェック ボックスをオンにして、ファイアウォールが証明書を発行できるようにします。このチェック ボックスをオンにすると、ファイアウォールで認証局（CA）が作成されてクライアントのブラウザにインポートできるようになるため、クライアントはそのファイアウォールを CA として信頼できます。
   7. 証明書を **Generate**[生成] します。
5. 新しい証明書をクリックして編集し、**Forward Trust Certificate (フォワード トラスト証明書)**のチェックボックスをクリックして対象の証明書をフォワード トラスト証明書として設定します。
6. **OK**をクリックし、自己署名付きのフォワード トラスト証明書を保存します。
7. この作業を繰り返し、各ファイアウォール上で固有の下位 CA 証明書を生成します。

STEP 3 | フォワード トラスト証明書をクライアントシステムの証明書ストアに配布します。

エンタープライズ CA 署名付きの証明書をSSLフォワード プロキシ復号化用のフォワード トラスト証明書として使用しており、さらにクライアントシステムがすでにローカルの信頼できるルートCAリストにエンタープライズ CAをインストールしている場合は、このステップを飛ばすことができます。（エンタープライズ トラスト ルート CA が署名しているため、

このクライアントシステムは、ファイアウォール上で生成された下位 CA 証明書を信頼します)

フォワード トラスト証明書をクライアント システムにインストールしない場合、ユーザーがアクセスする *SSL* サイトごとに証明書警告が表示されます。

GlobalProtectポータルとして設定されたファイアウォール上で：

このオプションは*Windows*および*Mac*クライアント*OS*バージョンでサポートされており、クライアントシステムにインストールする*GlobalProtect*エージェント*3.0.0*以降が必要になります。

1. **Network (**ネットワーク**)** > **GlobalProtect** > **Portals (**ポータル**)** の順に選択し、既存のポータル設定を選択するか、新しいものを **Add (**追加**)** します。
2. **Agent (**エージェント**)** を選択し、さらに既存のエージェント設定を選択するか、新しい物を **Add (**追加**)** します。
3. 自己署名のファイアウォールの信頼できるルート CA 証明書を Trusted Root CA (信頼できるルート CA) セクションに**Add (**追加**)**します。クライアントはファイアウォールの下位 CA 証明書を信頼するため、GlobalProtect がファイアウォールの信頼できるルート CA 証明書をクライアントシステムに配信した後、クライアントシステムがファイアウォールの下位 CA 証明書を信頼するようになります。
4. GlobalProtectポータルが自動的に証明書を配布してGlobalProtectクライアントシステムの証明書ストアにインストールするよう、**Install in Local Root Certificate Store**[ローカル証明書ストアにインストール]します。
5. **OK** を 2 回クリックします。

GlobalProtectなし：

ファイアウォールの信頼できるルート CA 証明書をエクスポートし、それをクライアントシステムにインポートできるようにします。証明書をハイライト表示し、ウィンドウ下部にある**Export (**エクスポート**)**をクリックします。PEM フォーマットを選択します。

Export private key (秘密鍵のエクスポート**)**のチェックボックスは選択しないでください！秘密鍵はファイアウォール上に残します。クライアントシステムにエクスポートしないでください。

ファイアウォールの信頼できるルート CA 証明書をクライアントが信頼できるよう、クライアントシステム上のブラウザの信頼できるルート CA リストに証明書をインポートします。クライアント ブラウザにインポートするときは、証明書を Trusted Root Certification Authorities (信頼されたルート証明機関) 証明書ストアに追加します。Windows システム上では、デフォルトのインポート場所は Personal （個人）証明書ストアです。また、Active Directory グループ ポリシー オブジェクト（GPO）などの中央管理デプロイメント オプションを使用することによってこのプロセスを簡略化することもできます。

STEP 4 | フォワード アントラスト証明書を構成します（すべてのファイアウォールで同じフォワード アントラスト証明書を使用します）。

1. 証明書ページの下部にある **Generate**[生成] をクリックします。
2. **Certificate Name**（証明書名）に、「my-ssl-fwd-untrust」などの名前を入力します。
3. **Common Name**（共通名）を、たとえば「192.168.2.1」に設定します。**Signed By**[署名者] は空白のままにします。
4. **Certificate Authority**[認証局] チェック ボックスをオンにして、ファイアウォールが証明書を発行できるようにします。
5. **Generate** [生成]をクリックして証明書を生成します。
6. **OK** をクリックして保存します。
7. 新しい「my-ssl-fwd-untrust」証明書をクリックして変更し、**Forward Untrust Certificate**（**Untrust** 証明書の転送） オプションを有効にします。

   フォワード アントラスト証明書をネットワーク デバイスの証明書トラスト リストにエクスポートしないでください！フォワード アントラスト証明書をクライアント システムにインストールしないでください。アントラスト証明書をトラスト リストにインストールすると、ファイアウォールが信頼していないウェブサイトをデバイスが信頼するようになるため、これが重要になります。さらに、信頼されていないサイトに対する証明書の警告がユーザーに表示されなくなり、サイトが信頼されていないことを知らないユーザーがサイトにアクセスし、ネットワークを脅威にさらしてしまうおそれもあります。
8. **OK** をクリックして保存します。

STEP 5 | （任意）ファイアウォールがクライアントに提示する SSL 転送プロキシ サーバー証明書用のキーサイズを設定します。ファイアウォールはデフォルトで、宛先サーバーの証明書の鍵のサイズに基づいて使用する鍵のサイズを決定します。

STEP 6 | 復号化ポリシー ルールの作成を行ってファイアウォールに復号化させるトラフィックを定義し、復号化プロファイルを作成してトラフィックを SSL で制御します。

復号化プロファイルは任意ですが、各復号化ポリシー ルールと共に復号化プロファイルを含め、ネットワーク内で脆弱なプロトコルやアルゴリズムが疑わしいトラフィックを許可しないようにすることがベストプラクティスになります。

1. **Policies (ポリシー)** > **Decryption (復号化)** を選択し、既存のルールを Add (追加) あるいは変更し、復号化するトラフィックを定義します。
2. **Options (オプション)** を選択し：
   - マッチするトラフィックを**Decrypt**[復号化]するためのルールの**Action**[アクション]を設定します。
   - ルール**Type**[タイプ]を**SSL Forward Proxy**[SSL転送プロキシ]に設定します。
   - （ベストプラクティスであるが任意）復号化されたトラフィックの各要素（例：証明書をチェックし、Cipher Suite およびプロトコル バージョンを指定するために復

号化プロファイルを作成する）を制御・ブロックするために、既存の**Decryption Profile (**復号化プロファイル**)**を選択します。

3. **OK** をクリックして保存します。

STEP 7 | ファイアウォールが復号化された SSL トラフィックを WildFire に転送することを許可します。

このオプションでは、アクティブな ***WildFire*** ライセンスが必要になり、WildFire ベストプラクティスになります。

STEP 8 | 設定を **Commit**（コミット）します。

STEP 9 | 次のステップを選択します：

- SSL 復号化のオプトアウトをユーザーに許可します。
- 復号化除外を設定し、特定の種類のトラフィックに対する復号化を無効化します。

SSL インバウンド インスペクションの設定

SSLインバウンド インスペクションを使用すれば、ネットワークサーバー（サーバー証明書をファイアウォールに読み込んでいれば、どのサーバーに対しても SSL インバウンド インスペクションを実施可能）に向かうインバウンド SSL トラフィックの復号化や検査を行うことができます。SSL インバウンド インスペクション復号化ポリシーが有効になっている場合、ポリシーによって識別されるすべての SSL トラフィックをファイアウォールがクリア テキスト トラフィックに復号化し、検査します。ファイアウォールは、ポリシーにアタッチされた Decryption プロファイルと、構成済みのウイルス対策、脆弱性対策、スパイウェア対策、URL フィルタリング、ファイル ブロックプロファイルなど、トラフィックに適用されるセキュリティ ポリシーに基づいてトラフィックをブロック、制限、または許可します。ベストプラクティスとして、シグネチャ生成やWildFire 分析を行うために、復号化された SSL トラフィックを転送するファイアウォールの機能を有効化します。

SSL インバウンド インスペクションの設定には、以下のものが含まれます。

- ターゲット・サーバー証明書を ファイアウォール にインストールする。
- SSL インバウンド インスペクション復号化ポリシー・ルールの作成。
- ポリシー ルールに復号化プロファイルを適用します。

SSL インバウンドインスペクションを設定すると、プロキシされたトラフィックは *DSCP* コード ポイントまたは *QoS* をサポートしません。

SSL Inbound Inspection（*SSL*インバウンド インスペクション）は、認証ポータルへのリダイレクトをサポートしません。認証ポータルのリダイレクトと復号化を使用するには、SSL Forward Proxy（SSLフォワード プロキシ）を使用する必要があります。

STEP 1 | 適切なインターフェイスが Virtual Wire、Layer 2、または Layer 3 インターフェイスとして設定されていることを確認します。

SSL インバウンド インスペクション に *Tap* モード・インターフェースを使用することはできません。

Network (ネットワーク) > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** タブで設定されているインターフェイスを確認します。**Interface Type** 列は、インターフェイスが **Virtual Wire**、**Layer 2**、または **Layer 3** インターフェイスに設定されている場合に表示されます。インターフェイスを選択して、インターフェイス タイプなどの設定を選択できます。

STEP 2 | ターゲット サーバー証明書がファイアウォールにインストールされていることを確認します。

Web インターフェイスで、**Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificates (証明書)** > **Device Certificates (デバイス証明書)** の順に選択すると、ファイアウォール上にインストールされている証明書が表示されます。

Web サーバーがサポートする *TLS* バージョンによって、サーバー証明書と鍵をファイアウォール にインストールする方法が決まります。

エンドエンティティ *(*リーフ*)* 証明書が *1* つ以上の中間証明書 *and* によって署名されている場合、*Web* サーバーが *TLS 1.2* と *Rivest*、*Shamir*、*Adleman (RSA)* または *Perfect Forward Secrecy (*PFS*)* キー交換アルゴリズムをサポートしている場合は、証明書チェーン *(1* つのファイル*)* を ファイアウォール にアップロードすることをお勧めします。チェーンをアップロードすることで、クライアント側のサーバー証明書認証の問題を回避できます。ファイル内の証明書は、次のように配置する必要があります。

1. エンドエンティティ *(*リーフ*)* 証明書
2. 中間証明書 *(*発行順*)*
3. *(*オプション*)*ルート証明書

Web サーバーが *TLS 1.3* 接続をサポートし、証明書チェーンがサーバーにインストールされている場合、リーフ証明書が中間証明書によって署名されている場合、サーバー証明書と秘密鍵のみを ファイアウォール にアップロードできます。SSL インバウンド インスペクション では、各ケースについてさらに詳しく説明します。

ターゲット サーバー証明書をファイアウォールにインポートするには、以下の手順を実行します。

1. **Device Certificates**[デバイス証明書] タブで、**Import**[インポート] を選択します。
2. 分かりやすい名前を **Certificate Name**（証明書名）に入力します。
3. **Certificate File**[証明書ファイル] で、ターゲット サーバーの証明書ファイルを参照し、選択します。
4. **OK** をクリックします。

STEP 3 | 復号化ポリシー ルールを作成する を使用して ファイアウォール が復号化するトラフィックを定義し、復号化プロファイルを作成する でトラフィックに SSL 制御を適用します。

復号化プロファイルはオプションですが、弱く脆弱なプロトコルやアルゴリズムがネットワーク上の疑わしいトラフィックを許可しないように、各 復号化 ポリシールールに 復号化 プロファイルを含めることをお勧めします。

1. **Policies (ポリシー)** > **Decryption (復号化)** を選択し、既存のルールを **Add (追加)** あるいは変更し、復号化するトラフィックを定義します。
2. **Options (オプション)** を選択し：
   - 一致するトラフィックに**Action**（アクション） として **Decryption (復号)** を設定します。
   - **Type**（タイプ） を **SSL Inbound Inspection**（**SSL** インバウンド インスペクション）に設定します。
   - インバウンド SSL トラフィックの宛先である内部サーバーに対して **Certificates**（証明書） を**Add**（追加） します。SSLインバウンド インスペクション ポリシー ルールは、最大 12 個の証明書をサポートします。

     復号ポリシー ルールを設定して、複数のドメインをホストする内部サーバーにバインドされた *SSL/TLS* トラフィックを復号化し、各ドメインに独自の証明書を持たせることができます。ファイアウォール は、要求された *URL* に対してサーバーが提示する証明書と一致するポリシー ルール内の証明書を使用して、*SSL/TLS* 接続をネゴシエーションします。

ダウンタイムを発生させずに保護された内部サーバーの証明書を更新するには、有効期限が切れる前に、または無効になる前に、新しいサーバー証明書を更新または取得します。次に、証明書と秘密鍵を ファイアウォール にインポートし、*SSL* インバウンド インスペクション ポリシー ルールに追加してから、新しい証明書を *Web* サーバーにインストールします。*Web* サーバー上で別の証明書がアクティブであるときに、ポリシー・ルールを新しい証明書で更新すると、ファイアウォールは、使用中の証明書に関係なく、サーバーへのトラフィックを暗号化解除する準備をします。

新しい証明書を展開する準備ができたら、それを *Web* サーバーにロードし、正しくインストールしたことを確認します。新しい証明書をインストールしても、既存の接続には影響しません。ファイアウォールは、*Server Hello* メッセージの証明書が 復号ポリシー ルールの新しい証明書と一致することを確認します。一致しない場合、セッションは終了します。対応する Decryption log（復号化ログ） エントリは、セッション終了の理由を ファイアウォール とサーバー証明書の不一致として報告します。成功したハンドシェイクをログに記録して、すべてのインバウンドインスペクションセッションで使用されているサーバー証明書を表示します。

*(Panorama™) SSL*インバウンド インスペクションポリシー ルールにおける複数の証明書のサポートは、*PAN-OS 10.2* より前の *PAN-OS®* バージョンでは利用できません。*PAN-OS 10.2* を実行している *Panorama* 管理サーバーからの複数の証明書を含む *SSL*インバウンド インスペクションポリシー ルールを、以前のバージョンを実行している ファイアウォール にプッシュすると、管理対象 ファイアウォール のポリシー ルールは、アルファベット順にソートされた証明書リストからの最初の証明書のみを継承します。

パノラマから 復号ポリシー ルールをプッシュする前に、*PAN-OS 10.1* 以前を実行しているファイアウォール用に異なる templates（テンプレート） または device groups（デバイスグループ） を設定して、正しいポリシールール と証明書を適切な ファイアウォール に確実にプッシュすることをお勧めします。

- （ベストプラクティスであるが任意）既存の復号化プロファイルを選択あるいは構成し、復号化されたトラフィックをブロックしたり、その様々な面を制御したりし

ます（例：アルゴリズムや Cipher Suite がサポートされていないセッションを終了させる復号化プロファイルを作成）。

> *SSL* インバウンド インスペクションのトラフィック用のSSL プロトコル設定 復号化プロファイルを構成する際、異なるセキュリティ能力を持つ複数のサーバーに対して別々のプロファイルを作成します。例えば、*RSA* のみをサポートする一連のサーバーがある場合、*RSA* をサポートするための *SSL* プロトコル設定のみが必要になります。しかし、*PFS* をサポートするサーバー用の *SSL* プロトコル設定では、*PFS* をサポートする必要があります。サーバーがサポートしている最大レベルのセキュリティを利用できるように *SSL* プロトコル設定を構成しつつも、パフォーマンスをチェックし、強力なセキュリティ プロトコルおよびアルゴリズムに求められる大きなプロセス負荷にファイアウォール リソースが対応できることを確認します。

3. **OK** をクリックして保存します。

STEP 4 | ファイアウォールが復号化された SSL トラフィックを WildFire に転送することを許可します。

> このオプションでは、アクティブな *WildFire* ライセンスが必要になり、WildFire ベストプラクティスになります。

STEP 5 | 設定を **Commit**（コミット）します。

STEP 6 | 次のステップを選択します...

- SSL 復号化のオプトアウトをユーザーに許可します。
- 復号化例外 を構成して、特定の種類のトラフィックの復号化を無効化します。

SSH プロキシの設定

SSH プロキシの設定には証明書は必要なく、SSH セッションの復号化に使用されるキーはファイアウォールの起動中に自動的に生成されます。SSH 復号化が有効な場合、ファイアウォールは復号化ポリシーおよび復号化プロファイル設定に基づき、SSH トラフィックを復号化し、SSH トラフィックをブロックあるいは制限します。トラフィックは、ファイアウォールから出力される際に再暗号化されます。

SSH プロキシを設定すると、プロキシされたトラフィックは *DSCP* コード ポイントまたは *QoS* をサポートしません。

STEP 1 | 適切なインターフェイスがバーチャル ワイヤー、レイヤー 2、またはレイヤー 3 インターフェイスのいずれかとして設定されていることを確認します。復号化は、バーチャル ワイヤー、レイヤー 2、またはレイヤー 3 インターフェイスのみで実行できます。

Network (ネットワーク) > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** タブで設定されているインターフェイスを確認します。**Interface Type** [インターフェイス タイプ]列にはインターフェイスが **Virtual Wire** [バーチャル ワイヤー]、**Layer 2** [レイヤー 2]、または **Layer 3** [レイヤー 3]インターフェイスとして設定されているかが表示されます。インターフェイスを選択して、インターフェイスのタイプなどの設定を変更できます。

STEP 2 | 復号化ポリシー ルールの作成を行ってファイアウォールに復号化させるトラフィックを定義し、復号化プロファイルを作成して SSL トラフィックにチェックを行います。

復号化プロファイルは任意ですが、各復号化ポリシー ルールと共に復号化プロファイルを含め、ネットワーク内で脆弱なプロトコルやアルゴリズムが疑わしいトラフィックを許可しないようにすることがベストプラクティスになります。

1. **Policies (ポリシー)** > **Decryption (復号化)** を選択し、既存のルールを Add (追加) あるいは変更し、復号化するトラフィックを定義します。
2. **Options (オプション)** を選択し：
   - マッチするトラフィックを**Decrypt**[復号化]するためのルールの**Action**[アクション]を設定します。
   - ルール**Type**[タイプ]を**SSH Proxy**[SSHプロキシ]に設定します。
   - （ベストプラクティスであるが任意）既存の復号化プロファイルを選択あるいは構成し、復号化されたトラフィックをブロックしたり、その様々な面を制御したりします（例：バージョンやアルゴリズムがサポートされていないセッションを終了させる復号化プロファイルを作成）。
3. **OK** をクリックして保存します。

STEP 3 | 設定を **Commit**（コミット）します。

STEP 4 | （任意）復号化除外に進み、特定の種類のトラフィックに対する復号化を無効化します。

復号化されていないトラフィックを検証するためのサーバー証明書設定

トラフィックが個人的、センシティブである、あるいは現地の法や規制の関係で復号化しないことにしたトラフィック用に、非復号化ポリシーを作成します。例えば、特定の重役のトラフィックや、個人情報を含む財務ユーザーおよび財務サーバー間のトラフィックを復号化しないという選択も可能です。（サイトが証明書のピンニングや相互認証などの技術的な理由で復号化を妨げる場合、ポリシーでトラフィックの復号化を除外しないでください。代わりに、ホスト名を復号化除外リストに追加します）

しかし、トラフィックを復号化しないといっても、復号化されていないあらゆるトラフィックをネットワークで許可することはできません。非復号化プロファイルを復号化されていないトラフィックに適用し、証明書が失効したセッションおよび発行者を信頼できないセッションをブロックするのがベストプラクティスになります。

STEP 1 | 復号化されていないトラフィックを識別する復号化ポリシー ルールの作成を行い、好ましくないセッションをブロックする復号化プロファイルを作成します。

1. **Policies (プロファイル)** > **Decryption (暗号化)**を選択し、復号化されていないトラフィックを識別するルールを Add (追加) するか、既存のものを編集します。
2. **Options (オプション)** を選択し：
   - ルールの**Action (アクション)**を**No Decrypt (復号化なし)**に設定し、ファイアウォールがルールにマッチするトラフィックを復号化しないようにします。
   - トラフィックは復号化されないため、ルールの**Type (タイプ)**は無視します。
   - (ベストプラクティスであるが任意) 既存の復号化されていないトラフィック用の復号化プロファイルを構成あるいは選択し、証明書の期限が切れたセッションおよび証明書の発行者を信頼できないセッションをブロックします。

   > ファイアウォールは暗号化された証明書情報を読み取ることができず、証明書チェックを実行できないため、復号化しない *TLSv1.3* トラフィックの復号ポリシーに復号化なしプロファイルを添付しないでください。ただし、復号ポリシーがそのトラフィックを制御しない限り、復号化されていないトラフィックはログに記録されないため、復号化しない*TLSv1.3*トラフィックの復号ポリシーを作成する必要があります。

STEP 2 | 設定を **Commit**（コミット）します。

STEP 3 | 次のステップを選択します：

- SSL 復号化のオプトアウトをユーザーに許可します。
- 復号化除外を設定し、特定の種類のトラフィックに対する復号化を無効化します。

復号化例外

復号化から除外できるトラフィックには 2 つのタイプがあります：

- 証明書のピニング、不完全な証明書チェーン、サポートされていない暗号、相互認証などのために技術的な理由で復号化を妨げるトラフィック (トラフィックを復号化しようとすると、トラフィックがブロックされます)。Palo Alto Networks は、デフォルトで SSL復号化を技術的に妨げることが知られている一連のアプリケーション、およびサービスを除外する事前定義済みの SSL復号化除外リスト（**Device (デバイス) > Certificate management (証明書管理) > SSL Decryption Exclusion (SSL 復号化除外)**）を提供しています。SSL 復号化除外リストに含まれておらず、復号化を技術的に妨げるサイトがあった場合、サーバーのホスト名を使ってそれらを手動でリストに追加することができます。ユーザーが対象のサイトを SSL 復号化除外リストに追加しない場合、ファイアウォールは復号化を技術的に妨げるアプリケーションやサービスを使うサイトをブロックします。

  復号 プロファイルで**Unsupported Modes (非サポート モード)** (クライアント認証、非サポートのバージョン、または非サポートの暗号スイートとのセッション) が許可されている場合、ファイアウォールは、ローカル SSL 復号化除外キャッシュ (**Device (デバイス) > Certificate Management (証明書管理) > SSL Decryption Exclusion (SSL復号化除外) > Show Local Exclusion Cache (ローカル除外キャッシュ表示)**) に、許可された非サポート モードを使用するサーバーとアプリケーションを自動追加します。サポートされていないモードをブロックすると、セキュリティが向上しますが、それらのモードを使用するアプリケーションとの通信もブロックされます。
- 金融サービス、健康および医療、軍事、政府関連のトラフィックなど、ビジネス、規制、個人的あるいは他の理由で復号化しないことにしたトラフィック。送信元、宛先、URL カテゴリ、サービスに基づいて、トラフィックを選択的に復号化から除外することができます。

アスタリスク（*）をワイルドカードとして使用して、ドメインに関連付けられた複数のホスト名の復号化除外を設定できます。アスタリスクは、キャレット (^) が URL カテゴリの例外に対して動作するのと同じように動作し、各アスタリスクは、ホスト名の1つの可変サブドメイン (ラベル) を制御します。これにより、具体的な除外と一般的な除外の両方を作成できます。以下に例を示します。

- mail.*.com は mail.company.com と一致しますが、mail.company.sso.com には一致しません。
- *.company.com は tools.company.com と一致しますが、eng.tools.company.com には一致しません。
- *.*.company.com は eng.tools.company.com と一致しますが、eng.company.com には一致しません。
- *.*.*.company.com は corp.exec.mail.company.com と一致しますが、corp.mail.company.com には一致しません。
- mail.google.* は mail.google.com に一致しますが、mail.google.uk.com には一致しません。
- mail.google.*.* は mail.google.co.uk と一致しますが、mail.google.com には一致しません。

例えば、ワイルドカードを使用して video-stats.video.google.com を復号化から除外し、video.google.com を復号化から除外しない場合は、*.*.google.com を除外します。

ホスト名の前にあるアスタリスクのワイルドカードの数に関係なく (ホスト名の前に非ワイルドカード ラベルがない場合)、ホスト名はエントリと一致します。例えば、*.google.com、*.*.google.com、*.*.*.google.com はすべて google.com と一致します。ただし、*.dev.*.google.com は、1 つのラベル（dev）がワイルドカードではないため、google.com と一致しません。

トラフィックに対する可視性を高め、できるだけ攻撃の入り口を減らすために、復号化の例外は必要最小限に留めてください。

- Palo Alto Networks の定義済みの復号化例外
- 技術的な理由でサーバーを復号化から除外
- ローカル復号化例外キャッシュ
- ポリシー ベース復号化除外の作成

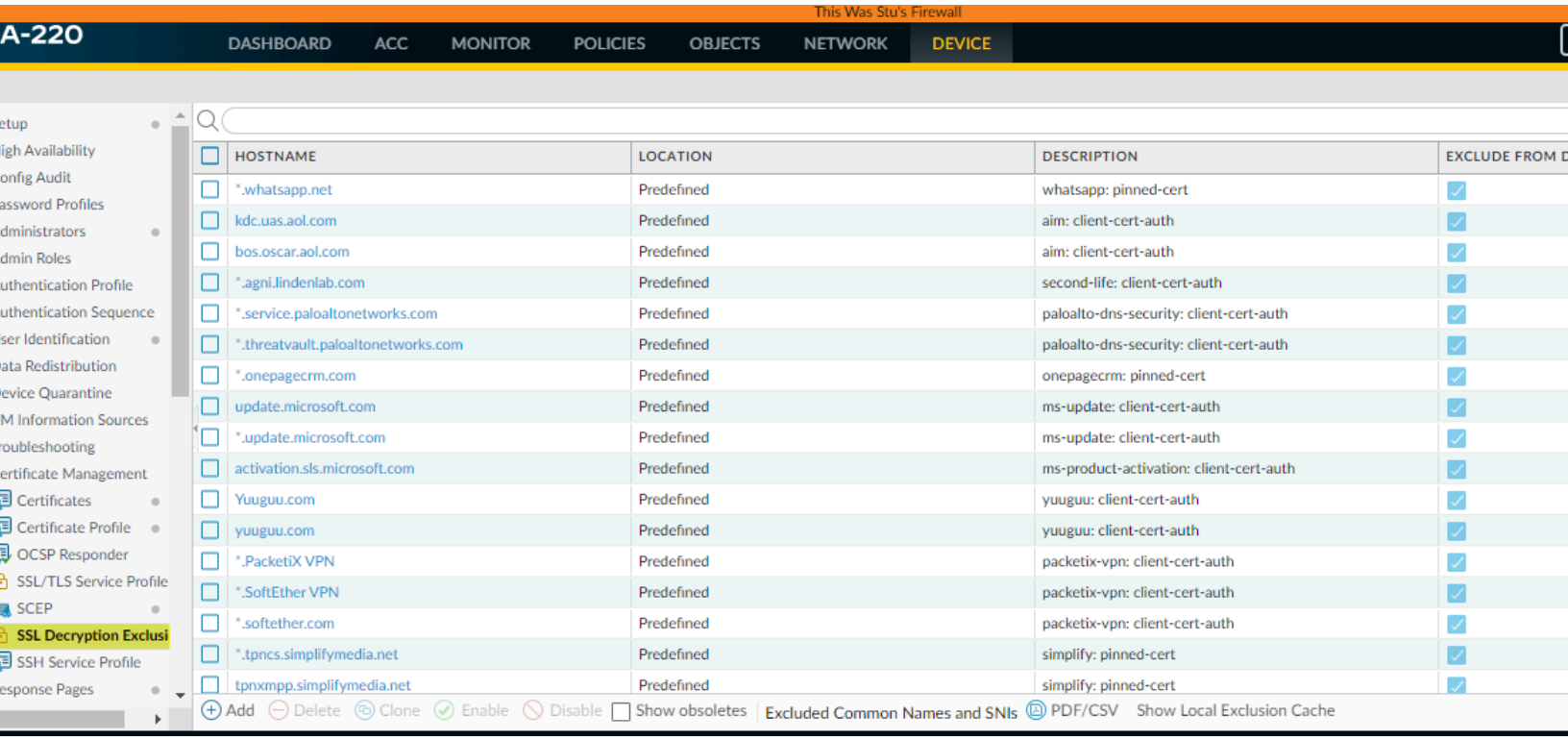
Palo Alto Networks の定義済みの復号化例外

ファイアウォールは、証明書のピンニングや相互認証などの技術的な理由で復号化を妨げ、頻繁に使用されるサイトを復号化から除外する事前定義済みの SSL 復号化除外リストを提供します。事前定義済みの復号化除外はデフォルトで有効になっており、Palo Alto Networks は、アプリケーションおよび脅威コンテンツ更新（あるいは、脅威防止ライセンスを持っていない場合はアプリケーション コンテンツ更新）の一部として、新規および更新された事前定義済みの復号化除外をファイアウォールに配信します。SSLファイアウォールは事前定義済みの除外にマッチするトラフィックを復号化せず、トラフィックを制御するセキュリティポリシーに基づいて暗号化されたトラフィックを許可します。しかし、ファイアウォールは暗号化されたトラフィックを検査したり、セキュリティポリシーを適用したりすることはできません。

SSL 復号化除外リストは、法律上の目的、規制上の目的、ビジネス上の目的、プライバシー上の目的、その他の意図的な目的のために復号化しないことにしたサイトに使用するものではありません。これは、復号化を技術的に妨げるサイトにのみ使用するものです (これらのサイトを復号化するとトラフィックがブロックされます)。復号化しないことにしたトラフィック (*IP* アドレス、ユーザー、*URL* カテゴリ、サービス、さらにゾーン全体など) に対し、ポリシー ベース復号化除外を作成します。

SSL 復号化除外リストに挙がったサイトのトラフィックは暗号化されたままになるため、ファイアウォールが検査を行ったり、トラフィックにさらにセキュリティを適用したりすることはありません。事前定義済みの除外は無効化できます。例えば、ファイアウォールが検査を行いセキュリティポリシーを適用できるアプリケーションおよびサービスのみを許可する厳格なセキュリティポリシーを強制するために、事前定義済みの除外を無効化することもできます。しかし、対象のサイトが SSL 復号化除外リストで有効化されていない場合、ファイアウォールは復号化を技術的に妨げるアプリケーションやサービスを使うサイトをブロックします。

Palo Alto Networks の定義済みの SSL 復号化除外をファイアウォール上で直に表示・管理できます（**Device (デバイス)** > **Certificate Management (証明書管理)** > **SSL Decryption Exclusions (SSL 復号化除外)**）。



Hostname (ホスト名)には、復号化を技術的に妨げるアプリケーションやサービスのホストの名前が表示されます。また、事前定義済みのリストに存在しない場合、ホストを**Add** (追加)して技術的な理由でサーバーを復号化から除外することもできます。

Description (説明)には、例えば**pinned-cert**（証明書のピンニング）、**client-cert-auth**（クライアント認証）など、ファイアウォールがサイトのトラフィックを復号化できなかった理由が表示されます。

ファイアウォールは、有効化されている事前定義済みの SSL 復号化除外が不要になった際、それをリストから自動的に取り除きます（アプリケーションが復号化をサポートすると、以前に復号化を妨げていたアプリケーションをファイアウォールが除去します）。**Show Obsoletes** (古くなったものを表示)は、もう不要になり、無効化された事前定義済みの除外がリストに残っているかどうかをチェックします。無効化された事前定義済みの復号化除外をファイアウォールがリストから自動的に削除することはありませんが、ユーザーが古い項目を選択して**Delete** (削除)することができます。

ホスト名のチェックボックスを選択してから**Disable** (無効化)をクリックすれば、事前定義済みのサイトをリストから削除できます。SSL 復号化除外リストは技術的な理由で復号化を妨げるサイトにのみ使用し、復号化しないことにしたサイトには使用しないでください。

技術的な理由でサーバーを復号化から除外

重要なアプリケーションやサービスが復号化によって技術的に壊される（トラフィックの復号化によって妨害される）場合、対象のアプリケーションあるいはサービスをホストしているサイトのホスト名を Palo Alto Networks の 事前定義済みの SSL 復号化除外リストに追加し、カスタム復号化除外を作成することができます。トラフィックが暗号化されたままであるため、ファイアウォールは SSL 復号化除外リストが許可するトラフィックに対して復号化、検査、およびセ

キュリティポリシーの適用を行いません。そのため、リストに追加するサイトは、ビジネスのために本当に必要なアプリケーションやサービスだけにしてください。例えば、ビジネス上欠かせない内部のカスタム アプリケーションの一部が復号化を妨げる場合がありますが、それらをリストに追加すれば、暗号化されたカスタム アプリケーションのトラフィックをファイアウォールに許可させることができます。

SSL 復号化除外リストは、法、規制上の目的、ビジネス上の目的、プライバシー上の目的、その他の意図的な目的のために復号化しないことにしたサイトに使用するものではありません。これは、復号化を技術的に妨げるサイトにのみ使用するものです。復号化しないことにしたトラフィック（*IP* アドレス、ユーザー、*URL* カテゴリ、サービス、さらにゾーン全体）に対し、ポリシー ベース復号化除外を作成します。

サイトが技術的に復号化を妨げる原因としては、証明書のピン留め、クライアント認証、不完全な証明書チェーン、サポートされていない暗号などがあります。HTTP 公開鍵ピンニング (HPKP) の場合、クライアントにエンタープライズ CA 証明書 (あるいは証明書チェーン) をインストールしていれば、HPKP を使用する大抵のブラウザが転送プロキシ復号化を許容します。

サイトを復号化から除外する技術的な理由が、不完全な証明書チェーンである場合、ブラウザの場合と異なり、次世代ファイアウォールが自動的にチェーンを修復することはありません。サイトを *SSL* 復号化除外リストに追加する必要がある場合、そのサイトが正当なビジネスのサイトであることを手作業で確認してから、不足しているサブ *CA* 証明書をダウンロードし、それらをファイアウォールに読み込んでデプロイします。

SSL 復号化除外リストにサーバーを追加すると、ファイアウォールは、クライアントの hello メッセージのサーバー名表示 (SNI) とサーバー証明書の共通名 (CN) の両方に対して、復号化除外を定義するために使用するサーバー ホスト名を比較します。SNI または CN のいずれかが SSL 復号化除外リストのエントリと一致する場合、ファイアウォールはトラフィックを復号化から除外します。

STEP 1 | **Device (デバイス)** > **Certificate Management (証明書管理)** > **SSL Decryption (SSL 復号化) Exclusions** を選択します。

STEP 2 | 新しい復号化例外を **Add (追加)** するか、既存のカスタム エントリを選択して変更します。

STEP 3 | 復号化から除外したいウェブサイトあるいはアプリケーションの **hostname (ホスト名)** を入力します。

ホスト名では大文字と小文字を区別します。

ドメインに関連付けられた複数のホスト名を除外するには、ワイルドカードを使用できます。ファイアウォールは、サーバーがドメインに一致する CN を提示するすべてのセッションを復号化から除外します。

各カスタム エントリのホスト名フィールドが一意であることを確認してください。事前定義済みの除外項目がカスタム エントリと一致する場合、カスタム エントリが優先されます。

STEP 4 | （任意）マルチ仮想システム ファイアウォールのすべての仮想システムで例外を共有するには、**Shared**（共有）を選択します。

STEP 5 | アプリケーションを復号化から除外します。あるいは、既存の復号化除外を修正している場合、このチェックボックスを解除することで、元々復号化から除外されていたエントリを復号化し始めることができます。

STEP 6 | **OK** をクリックして新しい例外項目を保存します。

ローカル復号化例外キャッシュ

ファイアウォールでは、サーバーをローカル復号化除外キャッシュに追加でき（**Device (デバイス)** > **Certificate Management (証明書の管理)** > **SSL Decryption Exclusion (SSL復号化例外)** > **Show Local Exclusion Cache (ローカル除外キャッシュを表示)**）、また、固定された証明書や非サポートの証明書などの技術的な理由で、トラフィックが復号化を中断した場合、トラフィックを12時間自動的に復号化から除外します。復号プロファイルが、非サポートのモード（クライアント認証、非サポートのバージョン、または非サポートの暗号スイートを使用したセッション）を許可し、許可されたトラフィックが非サポートのモードを使用する場合、デバイスはサーバーをローカル除外キャッシュへ自動的に追加し、復号化処理をバイパスします。ファイアウォールは、ローカル復号化除外キャッシュ処理によって許可された、暗号化されたままのトラフィックに対する復号化やペイロード部の検査は行いません。（非サポートのモードを許可する復号プロファイル適用により）復号化から除外するサイトが、ビジネスに必要なアプリケーションやサービスのサイトであることを確認してください。

非サポートのモードをブロックすると、それらのモードを使用してセキュリティを強化するアプリケーションとの通信が遮断されます。クライアント認証を使用するSSL/TLSトラフィックは、技術的に復号化が困難なため、一般的に複合化処理の対象外となります。このため、復号プロファイル設定において、非サポートのバージョンや、非サポートの暗号についてはブロックし、クライアント認証については許可することがベストプラクティスとなります。復号プロファイルがクライアント認証を許可している場合、クライアントが認証を必要とするサーバーとのセッションを開始すると、ファイアウォールがトラフィックを復号化できないため、トラフィックを遮断するかわりに、ファイアウォールはアプリケーションとサーバーをローカル除外キャッシュに追加して、トラフィックを許可します。

クライアント認証を使用しており、SSL復号化除外リストの事前定義済みサイトに無いサイトからのトラフィックを許可する場合は、クライアント認証を使用したセッションを許可する復号プロファイルを作成します。アプリケーションをホストするサーバーにのみ適用する復号ポリシー ルールに、プロファイルを追加します。ログイン作業を完了するために多要素認証をユーザーに求めれば、セキュリティをさらに向上します。または、サイトを *SSL*復号化除外リストに追加して、明示的な復号ポリシーを使用せずに復号化処理をスキップすることもできます。

ファイアウォールは、アプリケーション トラフィックを制御する復号ポリシーとプロファイルに基づき、ローカル SSL復号化除外キャッシュ エントリを追加します。復号プロファイルで**Unsupported Mode Checks (非サポートのモードのチェック)** をブロックしない場合、ファイアウォールは次の場合にローカルSSL復号化除外キャッシュにエントリを追加します。

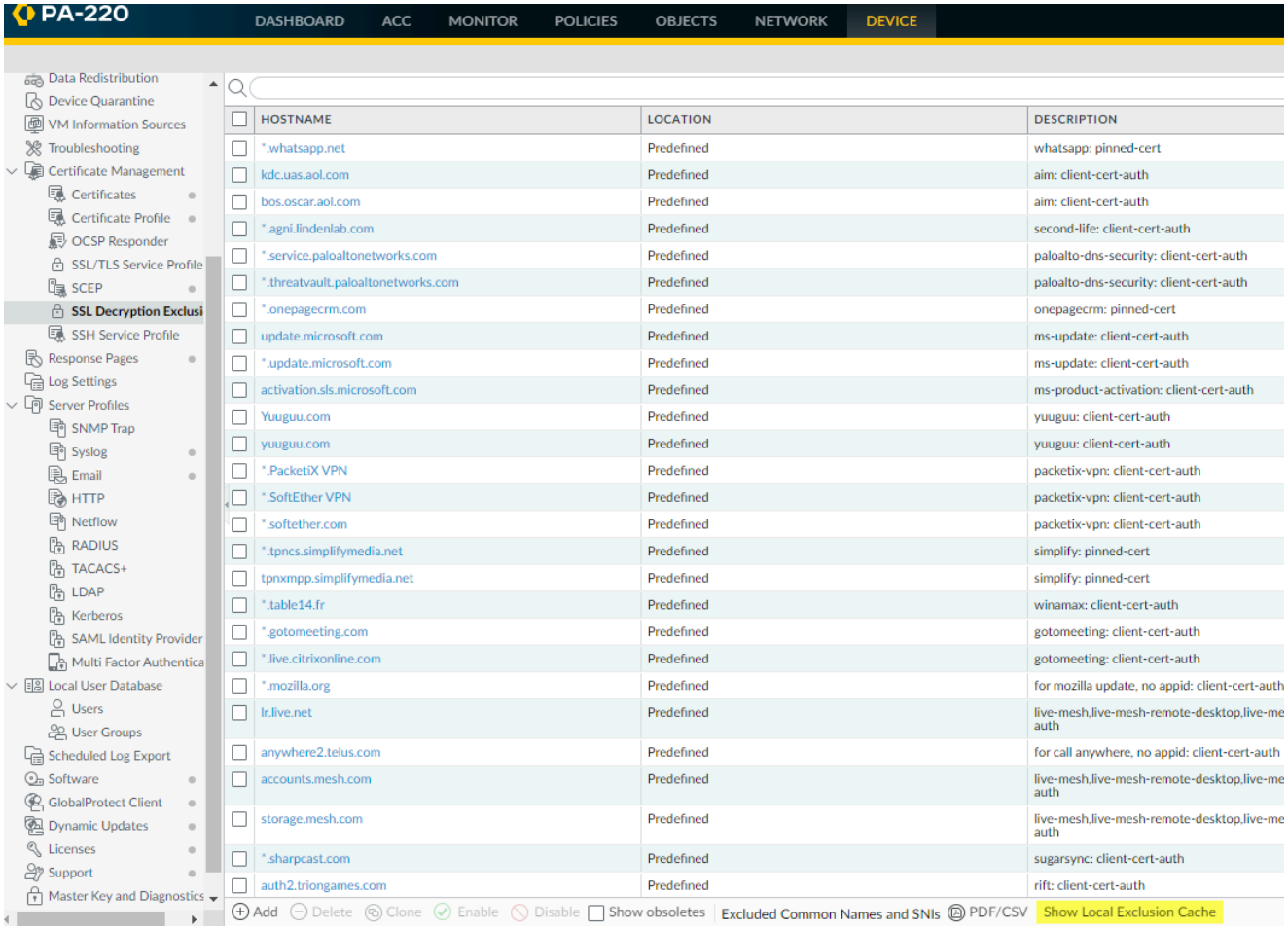
- クライアントは TLSv1.2 のみをサポートし、サーバーは TLSv1.3 のみをサポートする場合。ローカル キャッシュ内で、この除外に表示される理由は、SSL_UNSUPPORTED になります。

- クライアントは TLSv1.3 と TLSv1.2 をサポートし、サーバーは TLSv1.2 のみをサポートする場合。この場合、**Reason (理由)** 列には、TLS13_UNSUPPORTED が表示されます。

  サーバーをローカル *SSL*復号化除外キャッシュに追加する ***Reason (***理由*)* が、*TLS13_UNSUPPORTED* の場合、ファイアウォールはプロトコルを *TLSv1.2* にダウングレードし、トラフィックを復号化して検査します。
- クライアントが、サーバーがサポートしていない特定の暗号化スイートを通知した場合。
- クライアントが、サーバーがサポートしていない特定の楕円暗号化スイートを通知した場合。

ローカルキャッシュには、最大 1,024 エントリが保持されます。ローカル除外をローカル SSL復号化除外キャッシュに手動で追加することはできません (ただし、復号化除外を SSL復号化除外リストに手動で追加することは可能です)。

ローカル SSL復号化除外キャッシュを表示するには、スーパーユーザーまたは証明書管理の管理者アクセス権が必要です。表示するには、**Device (デバイス)** > **Certificate Management (証明書管理)** > **SSL Decryption Exclusion (SSL 復号化除外)** に移動し、画面下部付近の**Show Local Exclusion Cache (ローカルの除外キャッシュを表示)** をクリックします。ローカル除外キャッシュには、各エントリについて、アプリケーション、サーバー、キャッシュに含める理由、トラフィックを制御する復号プロファイルなどが表示されます。必要に応じて、ローカル除外キャッシュから特定エントリを手動で選択して削除することができます。



CLI を使用して、キャッシュされたエントリを削除することもできます。

```
clear ssl-decrypt exclude-cache [server <value>] [application
 <value>]
```

ローカルの除外キャッシュエントリが期限切れになる前 (12時間) に別ユーザが同じサーバーにアクセスしようとすると、ファイアウォールはセッションをキャッシュエントリと照合し、復号化をバイパスしてトラフィックを許可します。復号ポリシーまたはプロファイルを変更した場合、こうした変更はセッションの分類に影響を与える可能性があるため、ファイアウォールはローカル除外キャッシュエントリを消去します。キャッシュが一杯になった場合、ファイアウォールはあらたなエントリが登録されるタイミングで、最も古いエントリから削除を行います。

ポリシー ベース復号化除外の作成

ポリシー ベース復号化除外は、復号化しないことにしたトラフィックのみを対象にするものです。ポリシー ベース復号化除外は、トラフィックの送信元、宛先、サービス、URL カテゴリの任意の組み合わせに基づいて作成できます。復号化しないことにするトラフィックの例としては、次のようなものがあります：

- URL フィルタリング カテゴリ、金融サービス、健康および医療、政府など、個人を特定できる情報 (PII) やその他のセンシティブな情報が含まれるために復号化してはならないトラフィック。
- 重役、あるいはトラフィックを復号化してはならないその他のユーザーが送信元・宛先になるトラフィック。
- 金融サーバーなど、一部のデバイスは復号化から除外する必要があるかもしれません。
- ビジネスによっては、一部のアプリケーションよりもプライバシーやユーザーエクスペリエンスを重視する企業も存在します。
- 一部のトラフィックの復号化を禁止する法律または地域の規制。

  規制および法令遵守のためにトラフィックを復号化しない例としては、欧州連合(EU)の一般データ保護規則(GDPR)があります。EU GDPR は、すべての個人のあらゆる個人データを厳重に保護することを求めています。GDPRは、EU居住者の個人データを収集または処理する外国企業を含むすべての企業に影響します。

  規制やコンプライアンス規則が異なると、国や地域によって同じデータの取り扱いが異なる場合があります。通常、企業は情報を所有しているため、個人情報を社内のデータセンターで復号化できます。ベスト プラクティスは、できるだけ多くのトラフィックを復号化して、トラフィックを確認し、セキュリティ保護を適用できるようにすることです。

事前定義済みの URL カテゴリを使ってウェブサイトのカテゴリ全体を復号化から除外したり、カスタム URL カテゴリを作成してリストをカスタマイズし、復号化したくない URL を定義したり、外部動的リスト (EDL) を作成してリストをカスタマイズし、復号化したくない URL を定義したりすることができます。

IP アドレスが動的に変わる Office 365 のような環境、あるいは復号化から除外したい URL のリストを頻繁に変更するような環境では、URL カテゴリではなく EDL を使って除外する URL を指定するのが望ましいことが多くあります。カスタム URL カテゴリの修正を反映させるためには

Commit (コミット) が必要である一方、EDL を修正すると、**Commit (コミット)** せずに URL カテゴリが動的に変更されるため、動的な環境で EDL を使用すればサービスの中断が少なくなります。

許可する暗号化されたトラフィックを単一の復号化ポリシー ルールが制御できるよう、*EDL*、あるいは復号化しないことにしたすべてのカテゴリを含むカスタム *URL* カテゴリを作成します。非復号化プロファイルをルールに適用します。カテゴリを *EDL* やカスタム *URL* カテゴリに追加できるため、トラフィックを復号化から除外してルールベースを整理しやすくなっています。

セキュリティポリシールールと同じように、ファイアウォールはポリシーのルールベースの順序でインバウンド トラフィックをポリシー ルールと照らし合わせます。復号化除外ルールをルールベースの一番上に配置し、法や規制によって復号化できないトラフィックやセンシティブなトラフィックを不意に復号化しないようにします。

ポリシー ベース復号化除外を作成する場合は、こちらの順序で、次の除外ルールを復号化ルールベースのトップに配置することがベストプラクティスになります：

1. センシティブな宛先サーバー用の IP アドレスベースの除外。
2. 重役やその他のユーザーあるいはグループに使用する送信元ユーザーベースの除外。
3. 宛先 URL 用のカスタム URL あるいは EDL ベースの除外。
4. 金融サービス、健康および医療、政府など、カテゴリ全体の宛先 URL 用の、センシティブな事前定義済みの URL カテゴリベースの除外。

トラフィックを復号化するルールは、これらの復号化ルールベースのルールの後に配置してください。

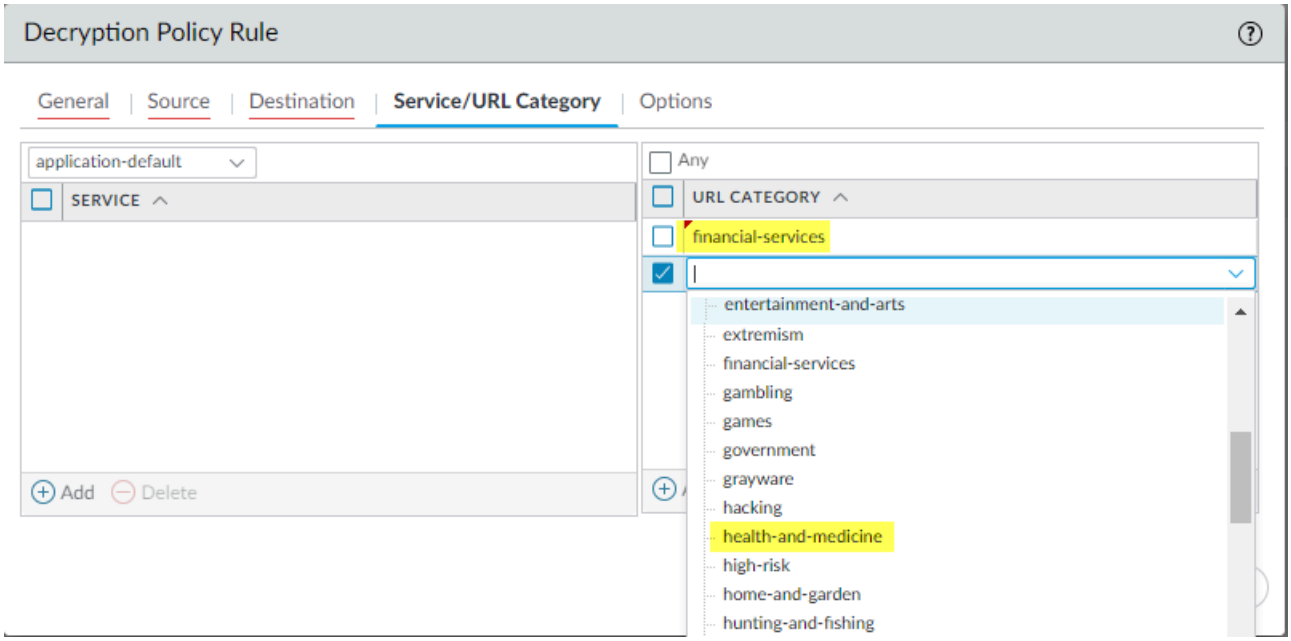
STEP 1 | マッチ条件に基いてトラフィックを復号化から除外します。

この例では、金融または医療関連と分類されるトラフィックを SSL フォワード プロキシ復号化から除外する方法を示します。

1. **Policies (**ポリシー**)** > **Decryption (**復号化**)** を選択し、復号化ポリシー ルールを **Add (**追加**)** あるいは変更します。
2. 復号化から除外するトラフィックを定義します。

   この例では:

   1. **Name**（名前）に、ルールの分かりやすい名前（たとえば「No-Decrypt-Finance-Health」など）を入力します。
   2. **Source (**送信元**)** および **Destination (**宛先**)** を **Any (**すべて**)** に設定すると、外部サーバーを宛先とするすべての SSL トラフィックにNo-Decrypt-Finance-Healthルールが適用されます。
   3. **URL Category**[URLカテゴリ]を選択し、financial-servicesおよびhealth-and-medicineのURLカテゴリを**Add**[追加]します。



3. **Options**[オプション]を選択してルールを**No Decrypt** [復号化なし]に設定します。
4. (ベストプラクティスであるが任意) 復号化なしプロファイルを作成してルールにアタッチすることで、ファイアウォールが復号化しないセッションの証明書を検証できるようにします。プロファイルを**Block sessions with expired certificates (**期限切れ証明書の

セッションをブロック)および **Block sessions with untrusted issuers (**発行元が信頼されていないセッションをブロック)に設定します。

例外: ファイアウォールは暗号化された証明書情報を読み取ることができず、証明書チェックを実行できないため、復号化しない *TLSv1.3* トラフィックの復号化ポリシーに復号化なしプロファイルを添付しないでください。ただし、復号化ポリシーがそのトラフィックを制御しない限り、復号化されていないトラフィックはログに記録されないため、復号化しない*TLSv1.3* トラフィックの復号化ポリシーを作成する必要があります。

5. **OK** をクリックして No-Decrypt-Finance-Health 復号化ルールを保存します。

STEP 2 | 復号化除外ルールを復号化ポリシー ルールベースの先頭に配置します。

ファイアウォールはルールベースの順序でインバウンド トラフィックに復号化ルールを適用し、トラフィックにマッチした最初のルールを強制します。

No-Decrypt-Finance-Health ポリシー（**Decryption (**復号化) > **Policies (**ポリシー)）を選択し、それがリストのトップに表示されるまで **Move Up (**上へ) をクリックするか、ルールをドラッグ アンド ドロップします。

STEP 3 | 設定を保存します。

Commit（コミット）をクリックします。

秘密鍵のエクスポートをブロック

PAN-OS または Panorama で証明書を生成またはインポートするときに、証明書の秘密鍵のエクスポートを永続的にブロックできます。PAN-OS デバイスからの秘密鍵のエクスポートをブロックすると、不正な管理者やその他悪意のある人物が鍵を悪用するのを防ぐため、セキュリティ体制が強化されます。証明書の管理を含むロールを持つ管理者は、秘密鍵のエクスポートをブロックできます。デバイスにすでに存在するキーをブロックすることはできません。キーをブロックできるのは、キー生成時、またはキーを PAN-OS にインポートする時のみです。

管理者が秘密鍵のエクスポートをブロックすると、スーパーユーザー管理者であっても、管理者がそのキーをエクスポートすることはできなくなります。PAN-OS アプライアンスから秘密鍵をエクスポートする必要がある場合は、秘密鍵のエクスポートをブロックするオプションを選択せずに、証明書とキーを再生成します。

旧バージョンの PAN-OS にダウングレードするには、最初に秘密鍵がブロックされている証明書を削除する必要があります。ダウングレードを試行する前に、秘密鍵がブロックされている証明書を削除しない場合、証明書の削除を求めるエラー メッセージが表示されます。それらの証明書を削除するまではダウングレードできません。ダウングレード後、必要に応じて、削除した証明書を再インポートまたは再生成します。

エンタープライズ *Public Key Infrastructure* (公開鍵インフラストラクチャ; *PKI*) を使用して、証明書と秘密鍵を生成する場合は、秘密鍵のエクスポートをブロックします。新しいファイアウォールと *Panoramas* には、エンタープライズ *Certificate Authority* (認証局 - *CA*) からインストールできるため、*PAN-OS* から証明書と秘密鍵をエクスポートする理由はありません。

ファイアウォールまたは *Panorama* に自己署名証明書を生成して、秘密鍵エクスポートのブロックを適用する場合、その証明書とキーは、他の *PAN-OS* アプリケーションにエクスポートできません。

秘密鍵のエクスポートをブロックしても、デバイス状態 (**Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)**) のエクスポートとインポートは可能です。デバイス状態のインポートとエクスポートには秘密鍵が含まれていますが、管理者はそれを読み取る、またはデコードすることはできません。

マスター キーが両方のファイアウォールで同一の場合、一方のファイアウォールの設定を、別のファイアウォールにインポートまたはロードできます。ファイアウォールでマスター キーが異なる場合、設定のインポートまたはロードは機能せず、証明書の読み取り中にコミットが失敗します。

- 秘密鍵を生成してブロックする
- 秘密鍵をインポートしてブロックする
- IKEゲートウェイの秘密鍵をインポートしてブロックする
- 秘密鍵ブロッキングを検証

秘密鍵を生成してブロックする

秘密鍵のエクスポートをブロックして、証明書の生成後の誤用を防ぎます。

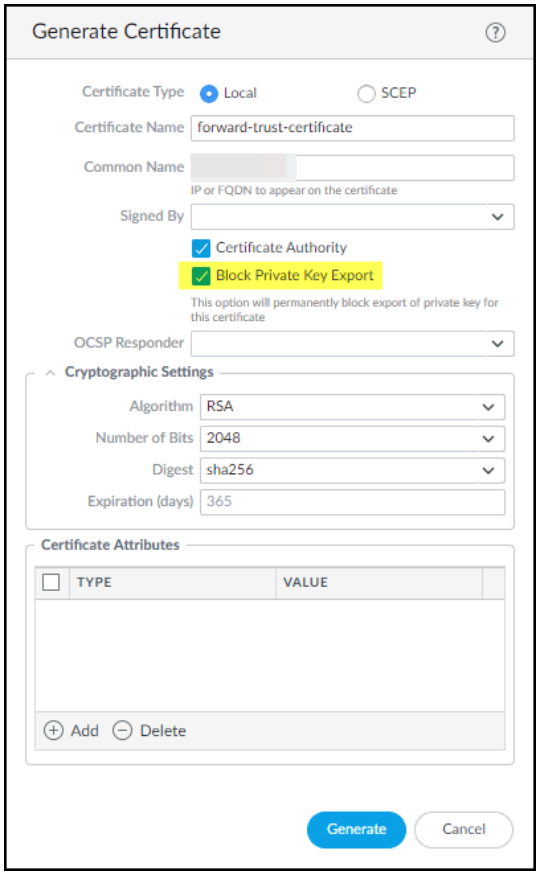
STEP 1 | **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択します。

virtual system (仮想システム - vsys)が複数ある場合は、証明書の **Location(場所)** または **Shared(共有)** を選択します。

STEP 2 | 証明書を **Generate**[生成] します。

STEP 3 | 証明書のエクスポートを防止するには、**Block Private Key Export (秘密鍵のエクスポートをブロック)** を選択します。

その他の証明書フィールドに関する情報については、Generate a Certificate (証明書の生成) を参照してください。



STEP 4 | **Generate(生成)** をクリックして新しい証明書を生成します。

また、操作用の *CLI* コマンドを使用して、証明書を生成し、その秘密鍵のエクスポートをブロックすることもできます:

```
admin@pa-220> request certificate generate block-private-key yes
```

上記の *CLI*コマンドには、表示されていない証明書やその他のパラメータを含めることもできます。

秘密鍵をインポートしてブロックする

秘密鍵のエクスポートをブロックして、証明書インポート後の誤用を防ぎます。

STEP 1 | **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択します。

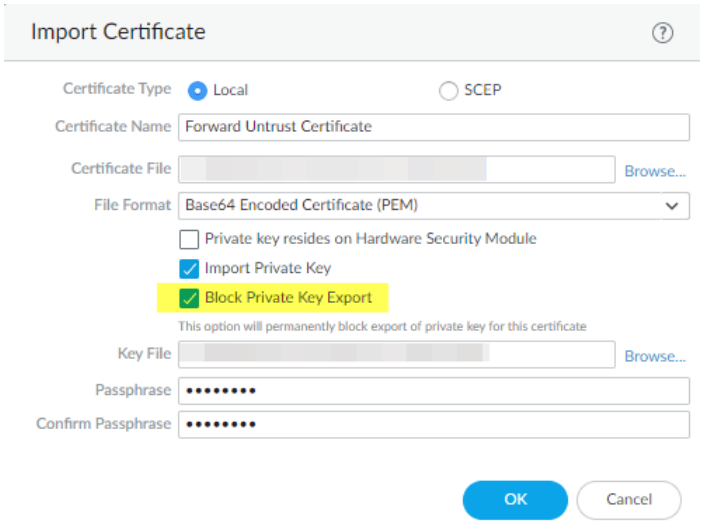
仮想システムが複数ある場合は、証明書の **Location** [場所] または **Shared** [共有]）を選択します。

STEP 2 | 証明書を **Import (インポート)** します。

STEP 3 | **Import Private Key (秘密鍵のインポート)** を選択して、秘密鍵のエクスポートをブロックするオプションをアクティベートします。

STEP 4 | 証明書のエクスポートを防止するには、**Block Private Key Export (秘密鍵のエクスポートをブロック)** を選択します。

その他の証明書のインポート フィールドに関する情報については、証明書と秘密鍵のインポート を参照してください。



STEP 5 | **[OK]** をクリックして、証明書をインポートします。

SCP 操作 CLI コマンドを使用して、証明書をインポート、または証明書の秘密鍵をインポートする場合でも、秘密鍵のエクスポートをブロックできます。

- ```
  admin@pa-220> scp import private-key block-private-key ...
  ```

上記の各 CLI コマンドには、送信元、証明書名、および表示されていないその他のパラメーターを指定するためのキーワードを含めることもできます。

SCP 操作 CLI コマンドを使用して証明書をエクスポートし、その秘密鍵を含める場合 (**scp** 証明書のエクスポート・パスフレーズは、証明書名**<phrase>**インクルード鍵**<1-65536>**形式 **<destination>**に<name>するためにリモート・ポート・<yes | no>に<der | pem | pkcs10 | pkcs12><されます)、証明書の秘密鍵がブロックされている場合、ブロックされた秘密鍵をエクスポートできないため、コマンドは失敗し、エラー・メッセージを返します。

IKEゲートウェイの秘密鍵をインポートしてブロックする

秘密鍵のエクスポートをブロックし、IKE ゲートウェイ認証用のための証明書の生成後の誤用を防止します。

STEP 1 | **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **IKE Gateway (IKE ゲートウェイ)** を選択します。

STEP 2 | IKE ゲートウェイを **Add (追加)** します。

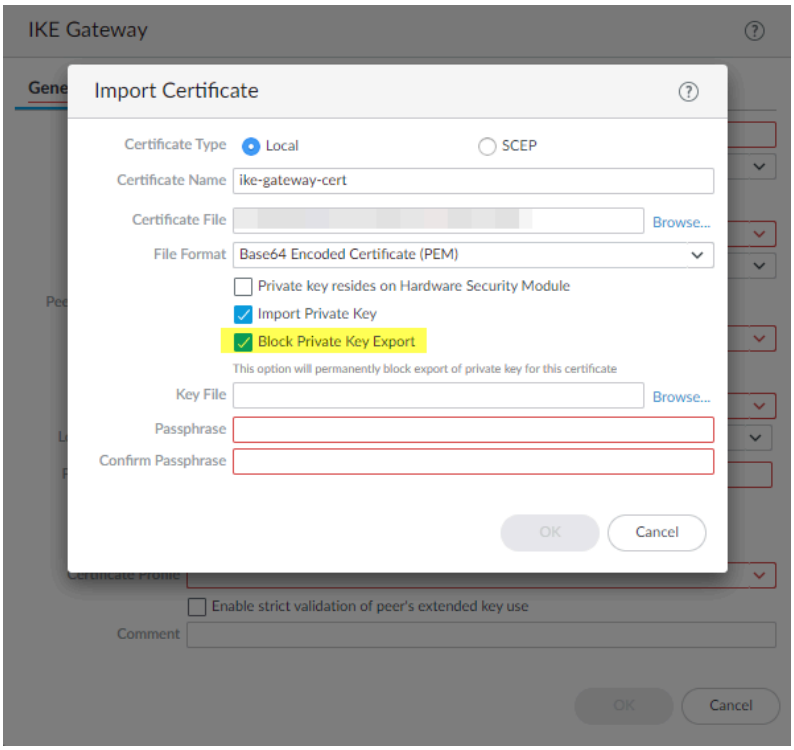
STEP 3 | **General (一般)** タブの **Authentication (認証)** で、**Certificate (証明書)** を選択します。

STEP 4 | **Local Certificate (ローカル証明書)** では、既存の証明書をインポートするか証明書を作成するかに応じて、**Import (インポート)** または **Generate (生成)** を選択します。

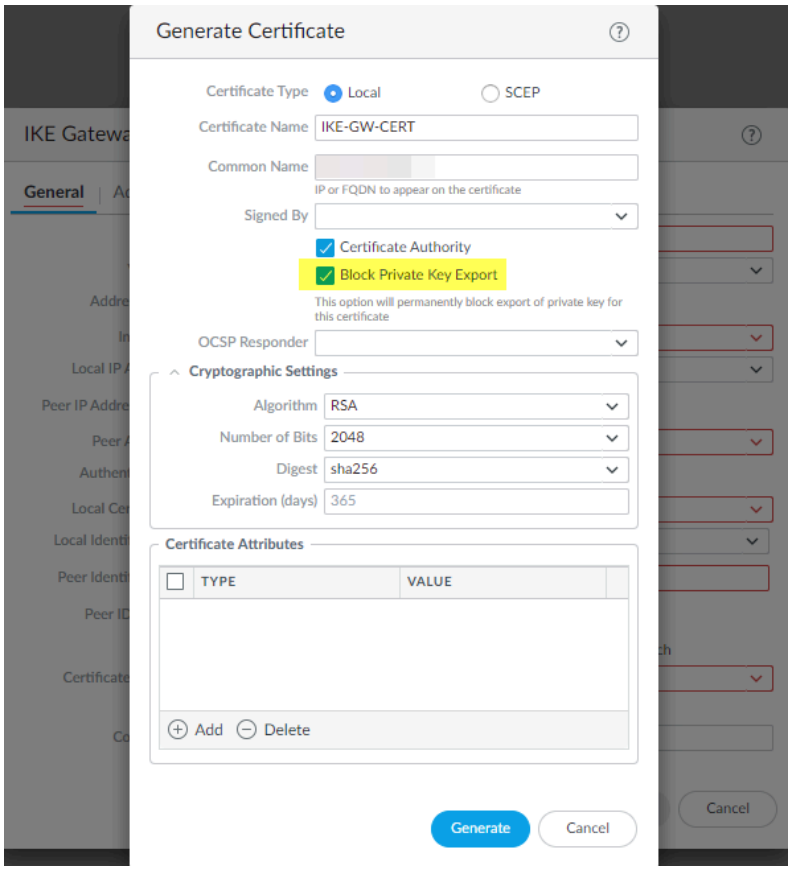
STEP 5 | 証明書情報を入力します。証明書をインポートする場合は、**Import Private Key (秘密鍵のインポート)** を選択し、**Block Private Key Export (秘密鍵のエクスポートをブロック)** チェックボックスにチェックを入れます。
  ```

STEP 6 | **Block Private Key Export (**秘密鍵のエクスポートをブロック**)** を選択して、キーのエクスポートを防止します。

証明書をインポートするには、**Passphrase (**パスフレーズ**)** を入力して確認し、**OK** をクリックします。



証明書を生成するには、**Generate (**生成**)** をクリックします。



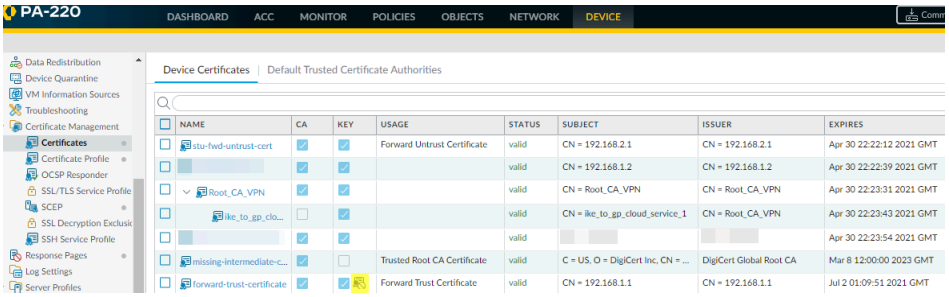
STEP 7 | **Passphrase (**パスフレーズ**)** を入力し確認してから、**OK** をクリックします。

秘密鍵ブロッキングを検証

秘密鍵のエクスポートがブロックされているかどうかは、複数の方法で確認できます。

Device (デバイス**)** > **Certificate Management (**証明書管理**)** > **Certificates (**証明書**)** > **Device Certificates (**デバイス証明書**)** の **Key (**キー**)** 列をチェックします。

この例では、forward-trust-certificate はブロックされます：



秘密鍵のエクスポートがブロックされている証明書をエクスポートしようとすると、**Export Private Key (**秘密鍵のエクスポート**)** チェックボックスが使用できなくなり、鍵をエクスポートできず、エクスポートできるのは証明書のみです。

以下の操作 CLI コマンドを使用して、エクスポートから秘密鍵がブロックされているデバイスまたは特定の Vsys のすべての証明書をリストアップします：

```
admin@pa-220> request certificate show-blocked <shared | vsys>
```

以下の操作 CLI コマンドを使用して、特定の証明書の秘密鍵のエクスポートがブロックされているかどうかを確認します：

```
admin@pa-220> request certificate is-blocked certificate-name
 <name>
```

証明書のエクスポートがブロックされている場合、コマンドは **yes** を返し、証明書がブロックされていない場合、コマンドは **no** を返します。

SSL 復号化のオプトアウトをユーザーに許可

プライバシーが重要な場面では、ファイアウォールが一定の Web トラフィックを復号化しているという内容をユーザーに警告し、トラフィックが復号化されると理解した上でサイトに進むか、セッションを終了してサイトへのアクセスをブロックするかどうかユーザーに選ばせたい場合があります。（サイトに進み、かつ復号化を回避するオプションはありません）

ファイアウォールは、復号ポリシーに適合する HTTPS サイトまたはアプリケーションをユーザーが初めて参照しようとするときに、ユーザーに対してセッションが復号化されることを通知する応答ページを表示します。ユーザーは、**Yes** [はい]をクリックして復号化を許可しサイトを訪問するか、**No** [いいえ]をクリックして復号化をオプトアウトし、セッションを終了することができます。復号化を許可する選択を行うと、次の24時間の間にユーザーがアクセスしようとしているすべてのHTTPSサイトにこの選択が適用され、その後ファイアウォールが再度応答ページを表示します。SSL復号化をオプトアウトしたユーザーは、指定された期間、リクエストしたウェブページあるいは他のどのサイトにもアクセスできなくなります。この指定された期間が過ぎ、次にユーザーがHTTPSサイトにアクセスしようとすると、ファイアウォールが再度応答ページを表示します。

ファイアウォールには、有効にすることができる事前定義された SSL Decryption Opt-out Page [SSL 復号オプトアウト ページ] が用意されてます。任意で、独自のテキストまたはイメージによってそのページをカスタマイズできます。しかし、ユーザーに復号化をオプトアウトさせないことがベストプラクティスになります。

サポートされている最大サイズを超えるカスタム応答ページは復号化されないか、ユーザーに対して表示されません。*PAN-OS 8.1.2* および古い *PAN-OS 8.1* リリースでは、復号化されているサイトのカスタム応答ページは *8,191* バイトを超えられません。*PAN-OS 8.1.3* 以降のリリースでこの最大サイズが *17,999* バイトに増加しました。

STEP 1 | （任意）[SSL 復号オプトアウト ページ] をカスタマイズします。

1. **Device** > **Response Pages** (デバイス > 応答ページ) の順に選択します。
2. **SSL Decryption Opt-out Page**[SSL 復号化オプトアウト ページ] リンクを選択します。
3. **Predefined**[事前定義済み] ページを選択し、**Export**[エクスポート] をクリックします。
4. 任意の HTML テキスト エディタを使用して、ページを編集します。
5. イメージを追加する必要がある場合は、エンド ユーザー システムからアクセス可能な Web サーバーでそのイメージをホストします。
6. そのイメージを指し示すように、HTML に行を追加します。以下に例を示します。

```
<img src="http://cdn.slidesharecdn.com/ Acme-logo-96x96.jpg?
1382722588"/>
```

7. 編集したページを新しいファイル名で保存します。ページが UTF-8 エンコーディングのままであることを確認してください。
8. ファイアウォールに戻り、**Device (デバイス)** > **Response Pages (応答ページ)** を選択します。
9. **SSL Decryption Opt-out Page**[SSL 復号化オプトアウト ページ] リンクを選択します。
10. **Import**（インポート）をクリックし、**Import File**（インポート ファイル）フィールドにパスとファイル名を入力するか、**Browse**（参照）をクリックしてファイルを指定します。
11. （任意）**Destination** [宛先]ドロップダウンリストから、このログイン ページが使用される仮想システムを選択するか、すべての仮想システムから利用できるように Shared [共有]を選択します。
12. **OK** をクリックしてファイルをインポートします。
13. インポートした応答ページを選択し、**Close**[閉じる] をクリックします。

STEP 2 | SSL 復号オプトアウトを有効にします。

1. **Device (デバイス)** > **Response Pages (応答ページ)** ページで、**Disabled (無効)** リンクをクリックします。
2. **Enable SSL Opt-out Page**[SSL オプトアウト ページを有効化] をオンにし、**OK** をクリックします。
3. 変更を **Commit**（コミット）します。

STEP 3 | サイトを参照しようとするときに、そのオプトアウト ページが表示されることを確認します。

ブラウザから、復号ポリシーと一致する暗号化されたサイトに移動します。

SSL 復号オプトアウトの応答ページが表示されることを確認します。

SSL 復号化を一時的に無効にする

場合によっては、SSL 復号化を一時的に無効にすることができます。例えば、急いで SSL 復号化をデプロイし、正常に機能しない部分があるものの原因が分からず、さらに検査すべきルールが大量にある場合、CLI を使って一時的に復号化を止め、分析を行って問題を解決する時間を確保できます。問題の解決後、CLI を使って再び SSL 復号化を有効化します。CLI を使って一時的に復号化を無効化し、再び有効化する際はコミット操作が不要であるため、ネットワーク トラフィックを中断することなく作業を行えます。

次の CLI コマンドは、コミットなしで一時的に SSL 復号化を無効化し、再びコミットなしで復号化を有効化します。

SSL 復号化を無効化するコマンドは、再起動後に構成に残ることはありません。一時的に復号化を止めてからファイアウォールを再起動すると、問題が解決されたかどうかに関わらず、復号化が再び有効になります。

SSL 復号化を無効にする

```
set system setting ssl-decrypt skip-ssl-decrypt yes
```

SSL 復号化を再び有効にする

```
set system setting ssl-decrypt skip-ssl-decrypt no
```

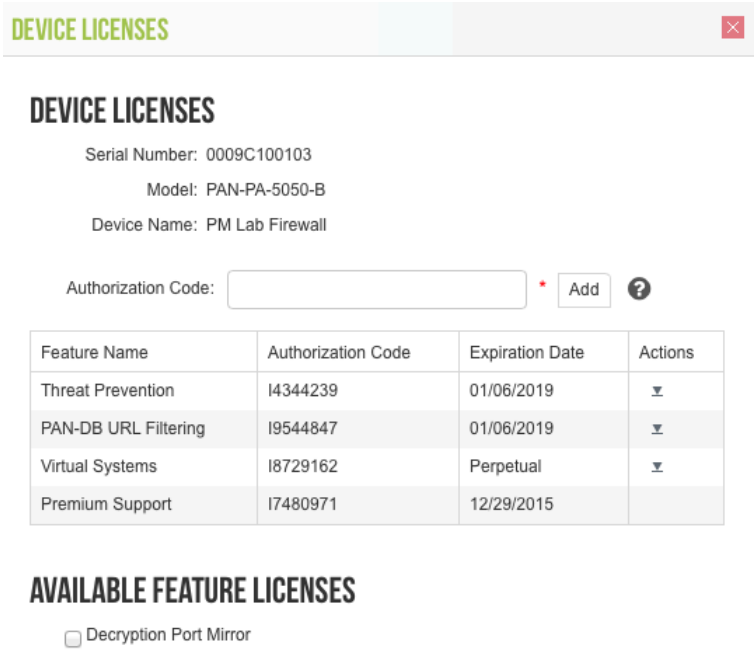
復号ポート ミラーリングの設定

復号ポート ミラーリングを有効にする前に、復号ポート ミラー ライセンスを取得し、インストールする必要があります。ライセンスは無料で、以下の手順によってサポート ポータルからアクティベーションできます。復号ポート ミラー ライセンスをインストールしてファイアウォールを再起動した後、復号ポート ミラーリングを有効にできます。

一部の国では、SSL トラフィックの復号化、保存、検査、または使用が規制されていて、複合化ミラーリング機能を使用するにはユーザーの同意が必要な場合があります。さらに、ファイアウォールへの管理アクセス権を持つ悪意あるユーザーがこの機能を使用すると、暗号化されたチャネルを使用して送信されたユーザー名、パスワード、社会保障番号、クレジット カード番号などの機密情報を収集できる可能性があります。運用環境でこの機能を有効にしたり使用したりする前に、企業の審議会と協議することをお勧めします。

STEP 1 | 復号ポート ミラーリングを有効にするファイアウォールごとにライセンスを要求します。

1. Palo Alto Networks のカスタマーサポート ウェブサイト サイトにログインし、**Assets (アセット)** タブに移動します。
2. ライセンスを取得するファイアウォールのエントリを選択し、**Actions**[アクション] を選択します。
3. **Decryption Port Mirror**[復号ポート ミラー] を選択します。法的通知が表示されます。
4. 潜在的な法的意味および要件を十分理解した上で、それでも復号ポート ミラーリングをセットアップしたい場合は**I understand and wish to proceed (**理解しました。続行します**)**をクリックします。
5. **Activate**(アクティベーション) をクリックします。



STEP 2 | 復号ポート ミラー ライセンスをファイアウォールにインストールします。

1. ファイアウォールの Web インターフェイスから、**Device (デバイス)** > **Licenses (ライセンス)** の順に選択します。
2. **Retrieve license keys from license server**[ライセンス サーバーからライセンス キーを取得] をクリックします。
3. ライセンスがファイアウォール上でアクティベーションされていることを確認します。

4. ファイアウォールを再起動します（**Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)**）。この機能は、PAN-OS を再ロードするまで設定できません。

STEP 3 | 復号化されたトラフィックを転送するファイアウォールを有効にします。この手順を実行するにはスーパーユーザーの権限が必要です。

仮想システムが **1** つのファイアウォールの場合**:**

1. **Device (デバイス)** > **Setup (設定)** > **Content-ID**の順に選択します。
2. **Allow forwarding of decrypted content**[復号化されたコンテンツの転送を許可] チェック ボックスをオンにします。
3. **OK** をクリックして保存します。

仮想システムが複数あるファイアウォールの場合**:**

1. デバイス > **virtual system (仮想システム - vsys)**の順に選択します。
2. 編集する仮想システムを選択するか、または **Add**[追加] を選択して新しい仮想システムを作成します。
3. **Allow forwarding of decrypted content**[復号化されたコンテンツの転送を許可] チェック ボックスをオンにします。
4. **OK** をクリックして保存します。

STEP 4 | 復号化ミラーリングに使用する Ethernet インターフェイスを有効にします。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)**を選択します。
2. 復号ポート ミラーリング用に設定する Ethernet インターフェイスを選択します。
3. **Interface Type**（インターフェイス タイプ）に **Decrypt Mirror**（復号化ミラー）を選択します。

   このインターフェイス タイプは復号ポート ミラー ライセンスがインストールされている場合にのみ表示されます。
4. **OK** をクリックして保存します。

STEP 5 | 復号化されたトラフィックのミラーリングを有効にします。

1. **Objects (オブジェクト)** > **Decryption Profile (復号化プロファイル)** の順に選択します。
2. **Decryption Mirroring** [復号化ミラーリング]に使用する **Interface** [インターフェイス]を選択します。

   Interface（インターフェイス）ドロップダウンリストには、次のタイプとして定義されているすべての Ethernet インターフェイスが含まれています：**Decrypt Mirror**[復号化ミラー]。
3. 復号化されたトラフィックをポリシー適用の前または後のどちらにミラーリングするかを指定します。

   デフォルトでは、ファイアウォールは、インターフェイスへのすべての復号化されたトラフィックをセキュリティ ポリシー検索の前にミラーリングします。これにより、イベントを再生して脅威を生成したりドロップ アクションのトリガーとなったトラフィックを分析できます。セキュリティ ポリシー適用の後の復号化されたトラフィックをミラーリングするには、**Forwarded Only**（転送のみ）チェック ボックスをオンにします。このオプションを指定すると、ファイアウォール内を転送されたトラフィックのみがミラーリングされます。このオプションは、復号化されたトラフィックを他の脅威検出デバイス（DLP デバイスや他の侵入防止システム（IPS）など）に転送する場合に役立ちます。
4. **OK** をクリックして復号プロファイルを保存します。

STEP 6 | （復号ポート ミラーリングが有効な）復号プロファイル ルールを復号ポリシー ルールに適用します。そのポリシー ルールに基づいて復号化されたすべてのトラフィックがミラーリングされます。

1. **Policies (ポリシー)** > **Decryption (復号化)** を選択します。
2. **Add**[追加] をクリックして復号ポリシーを設定するか、または既存の復号ポリシーを選択して編集します。
3. **Options (オプション)** タブで、ステップ4で作成した**Decrypt (復号化)**および**Decryption Profile (復号化プロファイル)**を選択します。
4. **OK** をクリックしてポリシーを保存します。

STEP 7 | 設定を保存します。

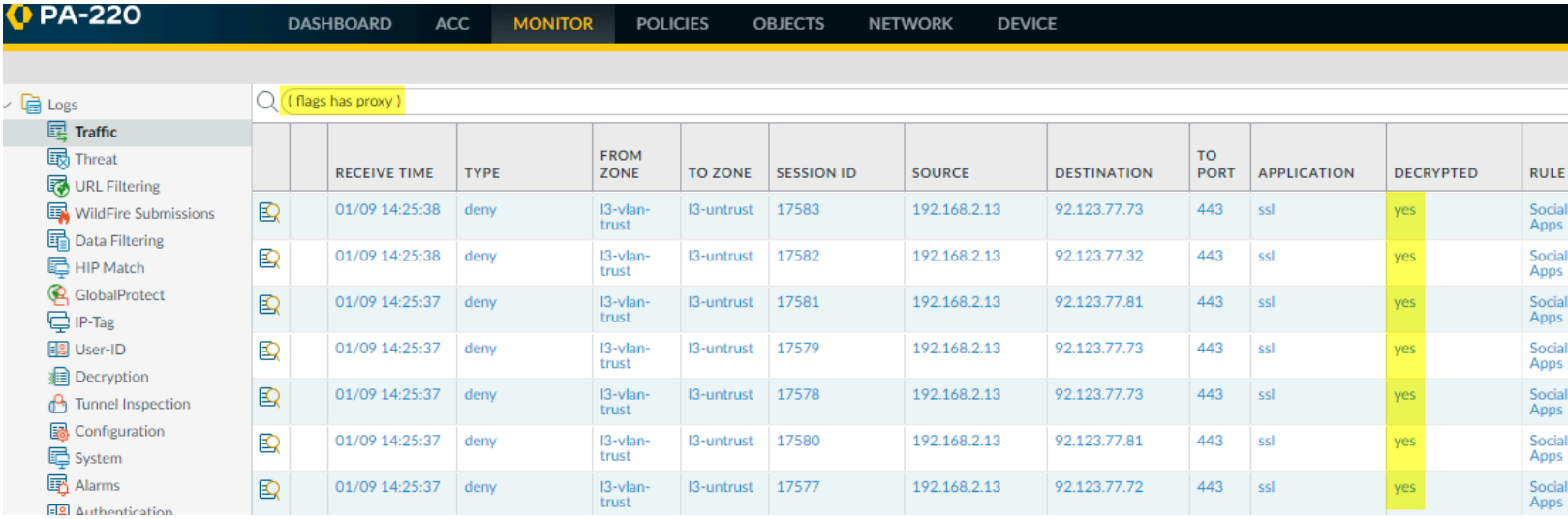
Commit（コミット）をクリックします。

復号化の検証

ベストプラクティスの復号化プロファイルを設定してトラフィックに適用した後、Decryption logs (復号化ログ) (PAN-OS 10.0 で導入) およびトラフィック ログの両方をチェックして、ファイアウォールが復号化する予定のトラフィックを復号化しており、復号化したくないトラフィックは復号化していないことを確認します。このトピックでは、トラフィック ログを使用して復号化を確認する方法を示します。さらに、デプロイ後の復号化のベストプラクティスに従ってデプロイメントを管理します。

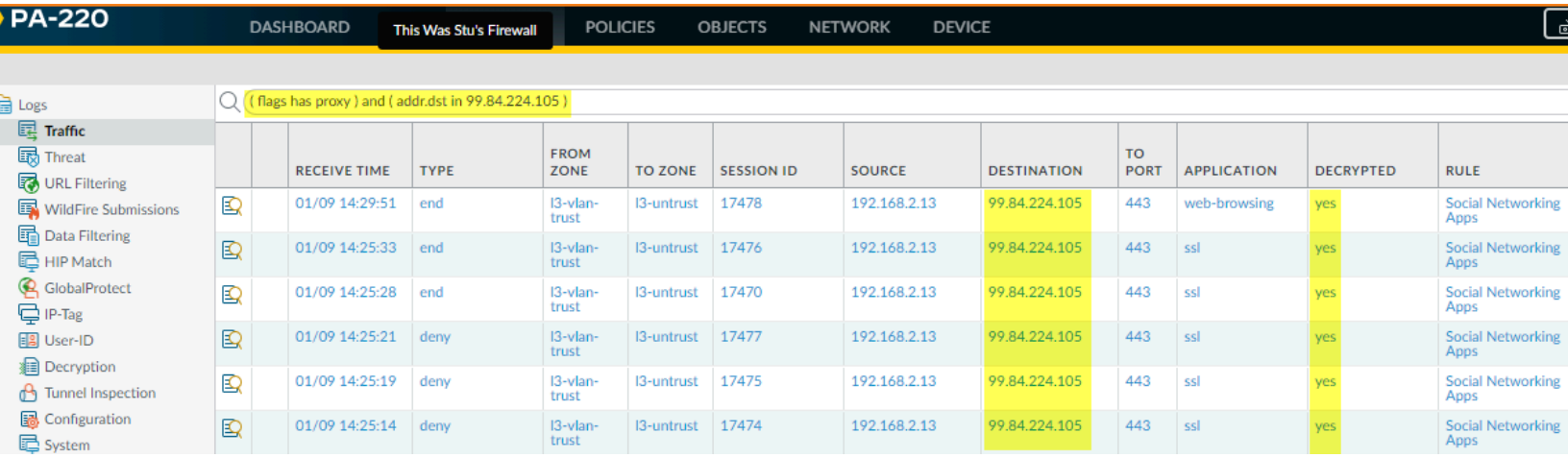
復号化されたトラフィック セッションの表示–フィルター**(flags has proxy)**を使用してトラフィックログをフィルタリング（**Monitor (**監視**)** > **Logs (**ログ**)** > **Traffic (**トラフィック**)**）します。

このフィルターは、SSL プロキシ フラグが立っている、つまり復号化されたトラフィックのログのみを表示します。すべてのログ エントリの**Decrypted (**復号化対象**)**列の値が yes になっています。



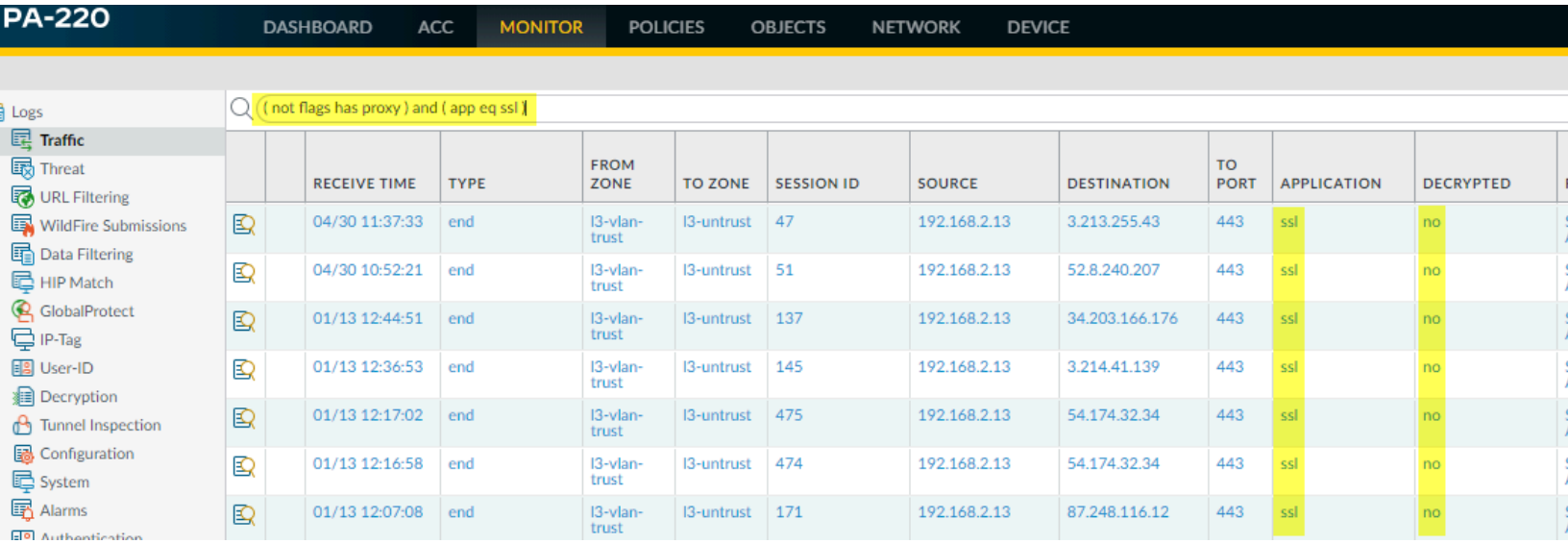
フィルターに語を追加することで、より細かくトラフィックをフィルタリングできます。例えば、フィルター**(addr.dst in 99.84.224.105)**を追加すれば、宛先 IP アドレス

99.84.224.105 に向かう復号化されたトラフィックのみをフィルタリングして表示できます：



復号化されていない **SSL** トラフィックの表示—フィルタ **(not flags has proxy)** および **(app eq ssl)** を使用してトラフィックログ (**Monitor (監視)** > **Logs (ログ)** > **Traffic (トラフィック)**) をフィルタリングします。

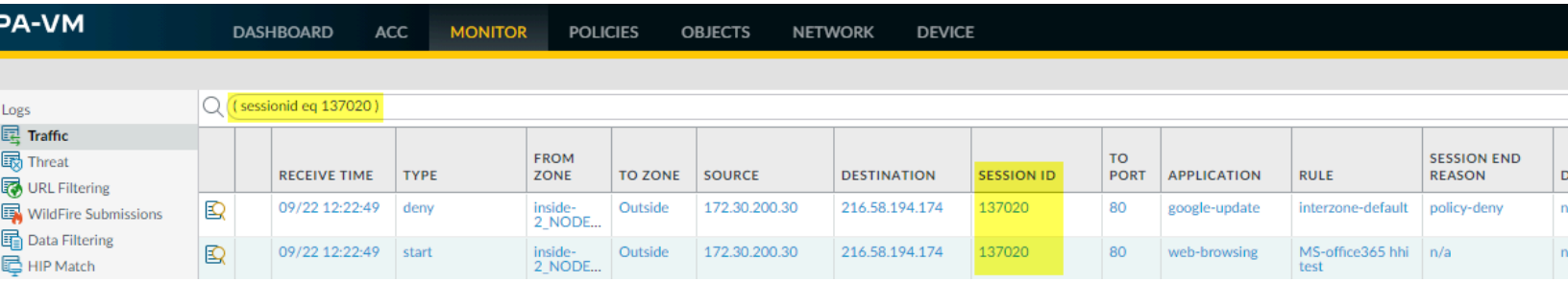
このフィルターは、SSL プロキシ フラグが立っていないログ（つまり暗号化されたトラフィックのみ）を表示します。トラフィックは SSL トラフィックになります。すべてのログエントリの**Decrypted (復号化対象)**列の値が**no (いいえ)**、**Application (アプリケーション)**列の値が**ssl**になります。



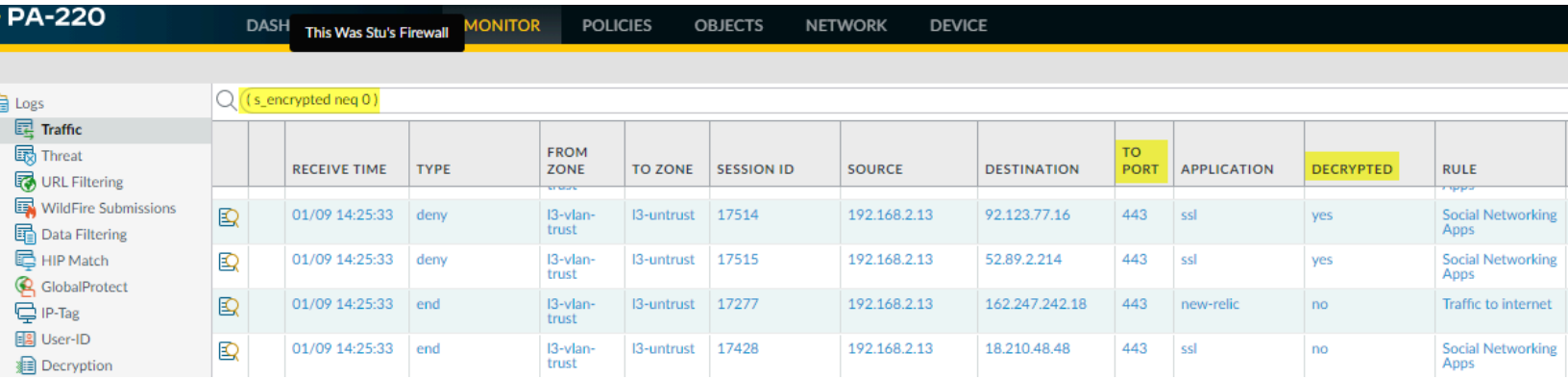
復号化されたトラフィックのログを閲覧する際と同様に、復号化しないトラフィックを細かくフィルタリングできるテキストを追加できます。

View The Log for a Particular Session (特定のセッションのログを表示**)**—特定のセッションのトラフィック ログを表示する場合は、セッション ID でフィルタリングします。

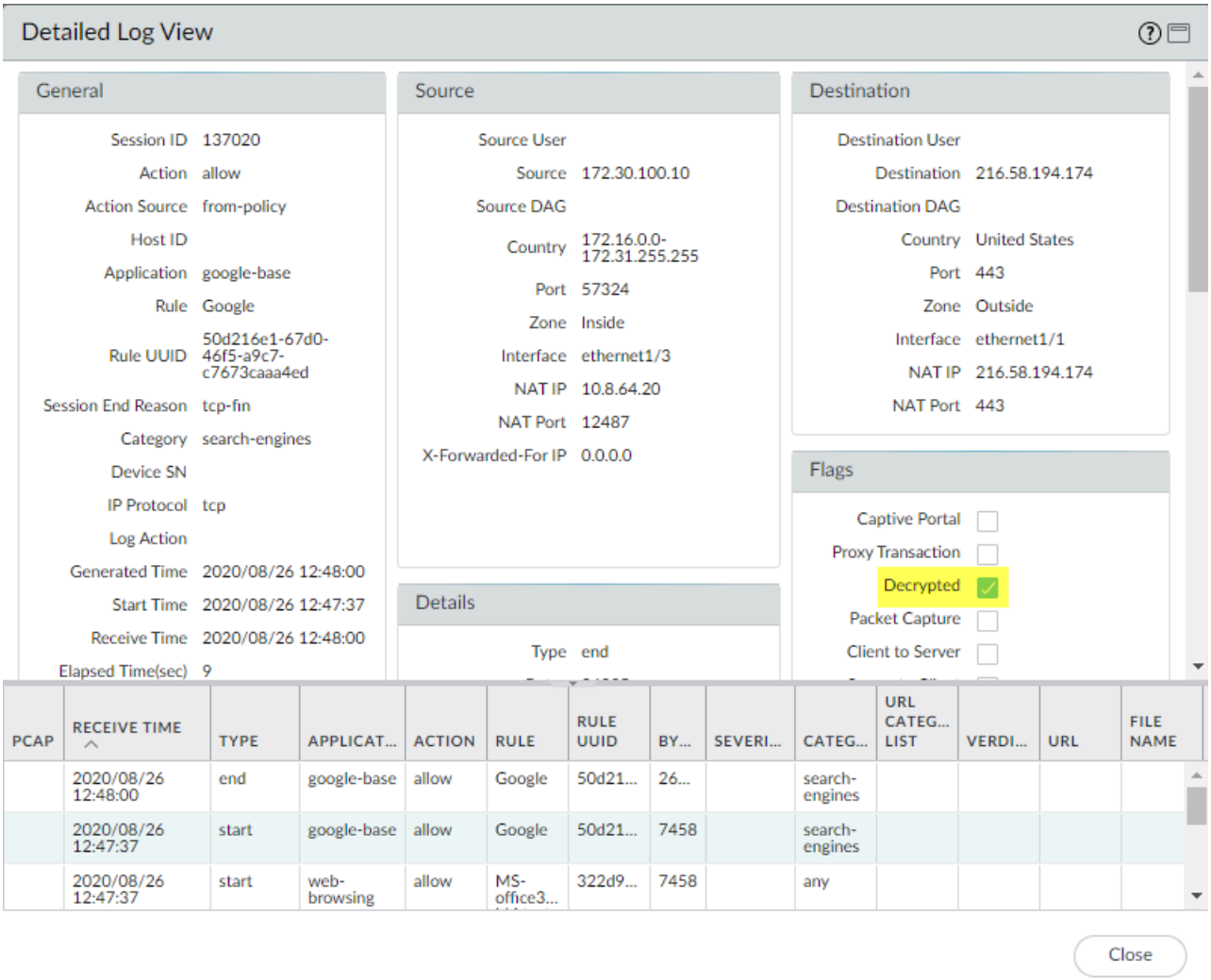
例えば、ID 137020 のセッションのログを表示するには、**`( sessionid eq 137020 )`**というテキストでフィルタリングします。前の画面にある通り、出力されたログの Session ID (セッション ID) 列に ID 番号が表示されます。Session ID (セッション ID) 列が表示されない場合は、その列を出力に追加してください。



View All TLS and SSH Traffic (すべての **TLS** と **SSH** トラフィックを表示**)**—トラフィック ログをフィルタして (**Monitor (**監視**)** > **Logs (**ログ**)** > **Traffic (**トラフィック**)**)、復号化および復号化されていない TLS および SSH トラフィックの両方を表示し、フィルタ **`(s_encrypted neq 0)`** を使用します:



詳細を確認–特定のログ エントリの詳細を表示するには、拡大鏡をクリックして詳細ログ ビューを表示します。例えば、セッション ID が 137020 の場合（前の箇条書きに記載）、詳細ログは次のようになります：



さらに**Decrypted (**復号化対象**)**フラグのボックスでも、トラフィックが復号化されていることが分かります。

また、復号化されたトラフィックの上流および下流のパケット キャプチャを取り、どのようにファイアウォールが SSL トラフィックを処理し、パケットに対してアクションを実行し、ディープ パケット インスペクションを行うのか確認できます。

復号のトラブルシューティングと監視を行う

トラブルシューティング ツールを使用すると、TLS トラフィックの可視性が向上するため、復号のデプロイメントを監視できます。これらのツールを使用すると、復号の問題をすばやく簡単に診断して解決し、復号の導入における弱点を強化し、復号の問題を修正してセキュリティ体制を向上させられます。例えば以下のことが可能です：

- サービス名識別 (SNI) とアプリケーションによって、復号化の失敗の原因となるトラフィックを識別する。
- 脆弱なプロトコルとアルゴリズムを使用するトラフィックを特定する。
- ネットワークでの成功と失敗した復号アクティビティを調べる。
- 個々のセッションに関する詳細情報を表示する。
- 復号の使用法とパターンをプロファイリングする。
- 詳細な復号の統計や、適用、失敗、バージョン、アルゴリズムなどに関する情報を監視する。

以下のツールは、TLS ハンドシェークを完全に可視化し、復号を導入するトラブルシューティングと監視に役立ちます:

- **ACC** > **SSL Activity (ACCのSSL** アクティビティ**)**—このタブの5つの ACC ウィジェット (PAN-OS 10.0で導入)は、復号の失敗、TLS バージョン、鍵交換、ならびに復号されたトラフィックおよび復号されていないトラフィックの量とタイプを含む、ネットワークでの成功および失敗した復号アクティビティに関する詳細を提供します。
- **Monitor** > **Logs** > **Decryption (Monitorの復号ログ)**—復号ログ (PAN-OS 10.0 で導入) は、復号ポリシー (復号しないトラフィックには復号なしのポリシーを使用) に一致する個々のセッション、ならびに GlobalProtectポータルまたは GlobalProtectゲートウェイ 設定での復号ログを有効にした際の GlobalProtect セッションに関する包括的な情報を提供します。アプリケーション、SNI、復号ポリシー名、エラーインデックス、TLS バージョン、鍵交換バージョン、暗号化アルゴリズム、証明書キー タイプ、およびその他の多くの特性など、情報を表示する列を選択します。列の情報をフィルタリングして、特定の TLS バージョンとアルゴリズム、特定のエラー、または調査するその他の特性を使用するトラフィックを特定します。デフォルトでは、復号ポリシーは失敗した TLS ハンドシェークのみをログに記録します。使用可能なログ ストレージに応じて、成功した TLS ハンドシェークもログに記録するように復号ポリシーを設定できます。
- **Local Decryption Exclusion Cache (**ローカル復号除外キャッシュ**)**—クライアント認証やピニングされた証明書などの技術的な理由で復号が出来ず、除外する必要があるサイトには、SSL Decryption Exclusion List(SSL復号除外リスト)とLocal Decryption Exclusion Cache(ローカル復号除外キャッシュ)の2つの仕組みがあります。SSL復号除外リストには、Palo Alto Networks が復号を技術的に失敗すると特定したサイトが含まれています。コンテンツ更新によりリストが最新の状態に保たれ、手動でサイトをリストに追加できます。ローカル復号除外キャッシュは、トラフィックに適用される復号プロファイルでサポートされていないモードを許可する場合、技術的な理由で復号を中断するローカル ユーザーが遭遇するサイトを自動的に追加し、それらを復号から除外します (サポートされていないモードがブロックされている場合、トラフィックはローカル キャッシュに追加されるのではなく、ブロックされます)。

- **Custom Report Templates for Decryption (**復号用のカスタム レポート テンプレート**)**—復号アクティビティ (PAN-OS 10.0 で導入) を要約する4つの事前定義済みのテンプレートを使用して、カスタム レポートを作成することができます (**Monitor (**監視**)** > **Manage Custom Reports (**カスタム レポートの管理**)**) 。

一般的なトラブルシューティング方法は、新しい ACC ウィジェットを使用して復号の問題を引き起こすトラフィックを特定し、新しい復号ログとカスタム レポート テンプレートを使用して詳細にドリルダウンし、そのトラフィックに関するコンテキストを取得することです。これにより、問題を以前よりも正確かつ簡単に診断できます。復号の問題とその原因を理解することで、次のような各問題を修正する適切な方法を選択できます:

- 復号ポリシー ルールの変更 (ポリシー ルールは、ルールが影響するトラフィック、そのトラフィックに対して実行されるアクション、ログ設定、およびトラフィックに適用される復号プロファイルを定義します)
- 復号プロファイルを変更する (復号ポリシー ルールが定義するトラフィックの許容可能なプロトコルとアルゴリズムに加えて、障害チェック、サポートされていない暗号やバージョンなどの項目のサポートされていないモードチェック、証明書チェックなど)
- 技術的な理由で復号を中断するサイトを SSL復号除外リストに追加する
- 従業員、顧客、およびパートナーが実際にアクセスする必要のあるサイトと、脆弱な復号プロトコルまたはアルゴリズムを使用している場合にブロックできるサイトに関するセキュリティの決定を評価する

目標は、復号できるすべてのトラフィックを復号し (復号のベストプラクティス)、それを検査することと、復号しないトラフィックを適切に処理できるようにすることです。

PAN-OS 10.0 にアップグレードすると、デバイスはログ スペースの1%を使用し、それを復号ログに割り当てます。> の 復号化ロギングの設定では、ログ・スペース割り振りを変更して、Decryption ログ用のスペースを増やす方法を示します。

PAN-OS 10.2 以降から PAN-OS 9.1 以前へダウングレードすると、PAN-OS 10.2 で導入された機能 (Decryption ログ、ACC の SSL Activity ウィジェット、カスタム レポート Decryption テンプレート) が UI から削除されます。復号ログへの参照もログ転送プロファイルから削除されます。さらに、Local Decryption Exclusion Cache は、PAN-OS 9.1 以前 CLI を使用してのみ表示できます (PAN-OS 10.2 では、ローカル キャッシュが UI に追加されました)。

PAN-OS 10.2 以降の Panorama から PAN-OS 9.1 以前を実行しているデバイスに構成をプッシュすると、Panorama は PAN-OS 10.0 で導入された機能を削除します。

- 復号化アプリケーション コマンド センター ウィジェット
- 復号化ログ
- 復号化のカスタム レポート テンプレート
- 復号化 トラブルシューティング ワークフロー例

復号化アプリケーション コマンド センター ウィジェット

PAN-OS 10.2 で導入された復号化 (**ACC** > **SSL Activity**) 用の Application Command Center (ACC) ウィジェットは、復号化ログ と連携して、復号化の問題を迅速かつ簡単に診断および解決するのに役立ちます。**SSL Activity (SSL** アクティビティ**)** ウィジェットを使用して、復号化されたセッションと復号化されていないセッションの数、さまざまな TLS プロトコル バージョンを使用す

るトラフィックの量、最も一般的な復号化の失敗の理由、そしてどのアプリケーションとサーバー名識別 (SNIs) が弱い暗号とアルゴリズムを使用するかなどの、ネットワーク復号化アクティビティの表示と分析を行います。次に、復号化ログを使用してセッションにドリルダウンし、問題を正確に診断して、適切なアクションを実行できるようにします。

PAN-OS 10.2 では、5 つの新しい復号化ウィジェットが導入されました。ウィジェットが提供する情報を使用して、誤って設定された復号化ポリシーとプロファイルを識別し、許可するトラフィックとブロックするトラフィックについて情報に基づいた決定を行います:

- **Traffic Activity (**トラフィック アクティビティ**)**-非 SSL/TLS アクティビティと比較した SSL/TLS アクティビティを、セッションの総数またはbyte (バイト)単位のトラフィック量で表示します。
- **SSL/TLS Traffic (SSL/TLS** トラフィック**)** –復号化されたトラフィックと復号化されていないトラフィックの量をセッション数またはトラフィック量(byte (バイト)単位)で示します。トラフィックが復号化されない原因には以下のものが含まれます:
  - 復号ポリシーがトラフィックに適用されていない。
  - 復号ポリシーが、トラフィックを意図的に復号化から除外した (非復号化ポリシーなど)。
  - 復号ポリシーが正しく設定されておらず、トラフィックは復号化されることを目的としていたがそうなっていない。
  - 該当のサイトは、 SSL 復号化例外リスト （ **Device (**デバイス**) > Certificate Management (**証明書管理**) > SSL Decryption Exclusion (SSL** 復号化例外**)**）内にあり、ピン留めされた証明書やクライアント認証などの技術的な理由で復号化に失敗したことをPalo Alto Networks が特定したサイトを含みます。これらのサイトに対して、ファイアウォールは復号化をバイパスします。
  - 該当のサイトは、ローカル復号化例外キャッシュにあります。このキャッシュには、ローカル ユーザーが遭遇する、技術的な理由で復号化を妨げるサイトが含まれています。

ACC は、次の3つのウィジェットに、復号ポリシーが制御するトラフィックからのデータのみを入力します。トラフィックに復号ポリシーを適用しない場合、そのトラフィックはこれらのウィジェットに入力されません。

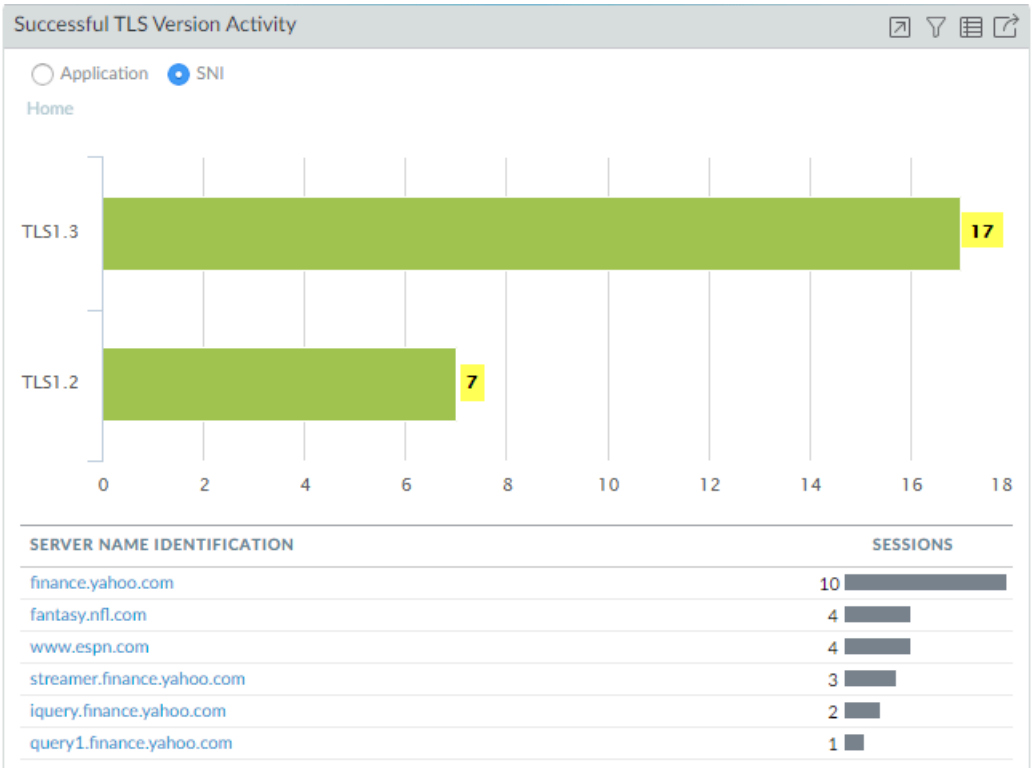
- **Decryption Failure Reasons (**復号化の失敗の理由**)** - SNI による復号化の失敗の理由 (プロトコル、証明書、バージョン、暗号、HSM、リソース、履歴書、または機能の問題) を示します。この情報を使用して、復号ポリシーまたはプロファイルの設定ミス、またはサポートされていない弱いプロトコルまたはアルゴリズムを使用するトラフィックによって引き起こされる問題を検出します。失敗の理由をクリックして、障害が発生した SNI ごとのセッション数をドリルダウンして分離するか、SNI をクリックして、その SNI のすべての復号化の失敗を確認します。
- **Successful TLS Version Activity (**成功した **TLS** バージョン アクティビティ**)**–アプリケーションまたは SNI の TLS バージョンごとに成功した TLS 接続を表示します (SNI は転送プロキシでのみ使用可能)。これにより、弱い TLS プロトコル バージョンを許可することで、どの程度のリスクが発生しているかを評価できます。弱いプロトコルを使用するアプリケーションと SNI を特定することで、それぞれを評価し、ビジネス上の理由でアクセスを許可する必要があるかどうかを判断できます。ビジネス目的でアプリケーションが必要ではない場合は、リスクを軽減するのではなく、トラフィックをブロックすることをお勧めします。TLS バージョンをクリックして、その TLS バージョンを使用した SNI またはアプリケーションをドリルダウン

して表示します。アプリケーションまたは SNI をクリックしてドリルダウンし、それらのアプリケーションまたは SNI セッションのうち各 TLS バージョンを使用した数を確認します。

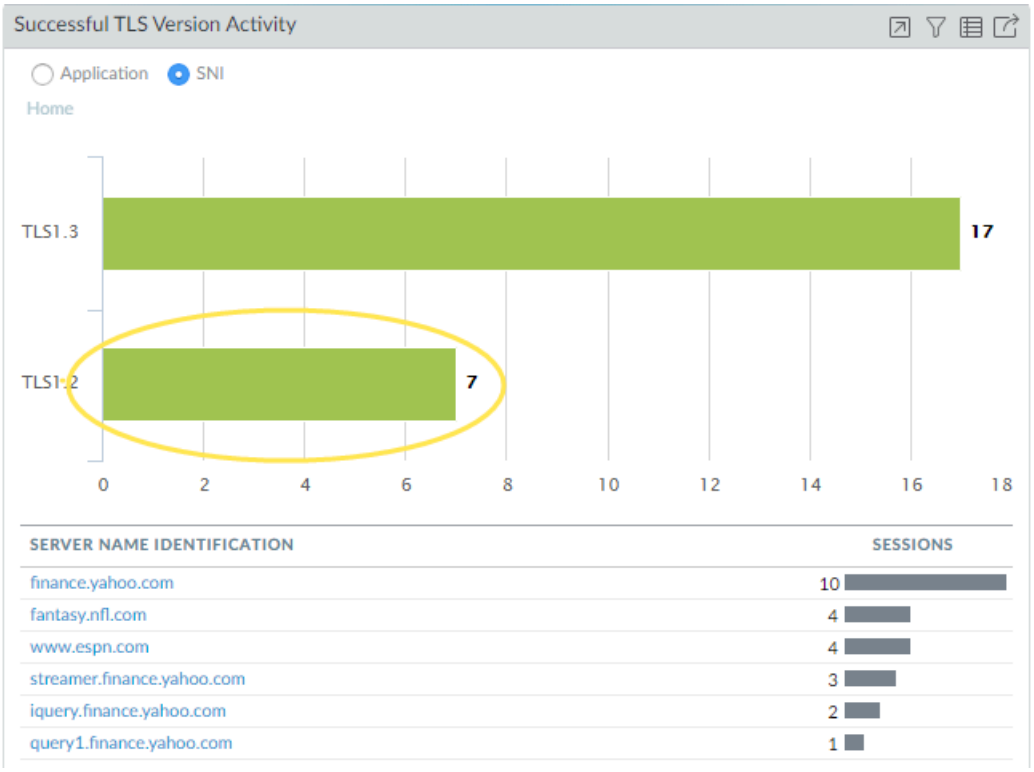
- **Successful Key Exchange Activity (**成功した鍵交換アクティビティ**)** – アプリケーションまたは SNI のアルゴリズムごとに成功した鍵交換アクティビティを示します (SNI は転送プロキシでのみ使用できます)。鍵交換アルゴリズムをクリックしてそのアルゴリズムのみのアクティビティを表示するか、アプリケーションまたは SNI をクリックしてそのアプリケーションまたは SNI の鍵交換アルゴリズム アクティビティを表示します。

以下の ACC データにドリルダウンする例は、成功した TLS バージョン アクティビティを調べる方法を示しています:

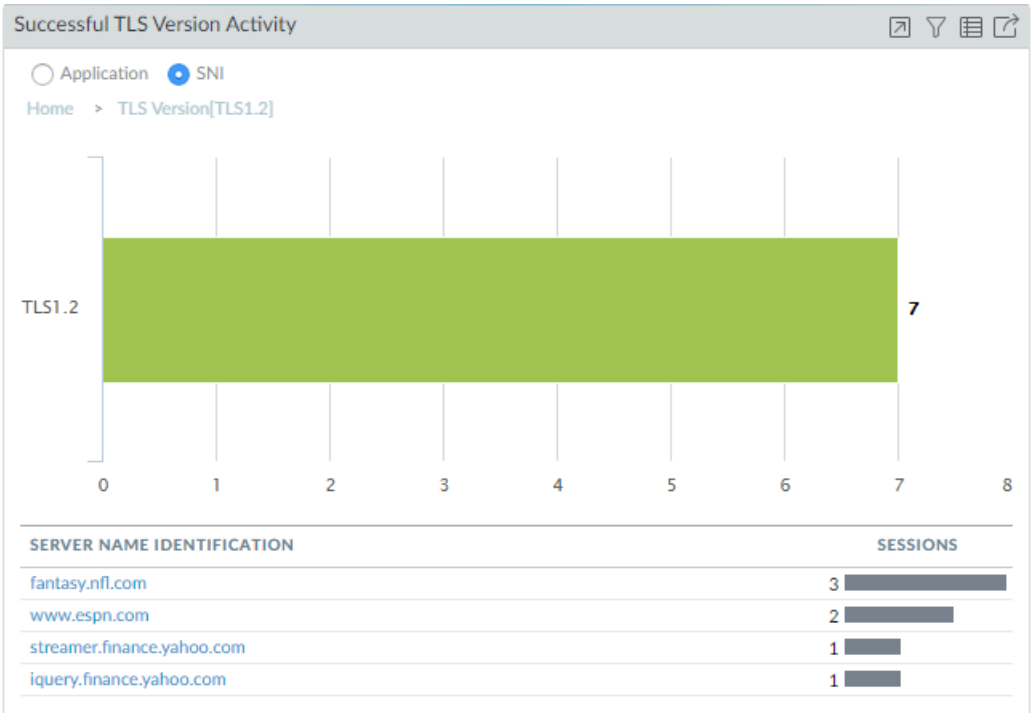
1. **Successful TLS Version Activity (**成功した **TLS** バージョン アクティビティ**)** ウィジェットは、17のセッションがTLSv1.3を使用し、7つのセッションがTLSv1.2を使用したことを示しています。SNI リストには、宛先 SNI と SNI ごとのセッション数が表示されます。



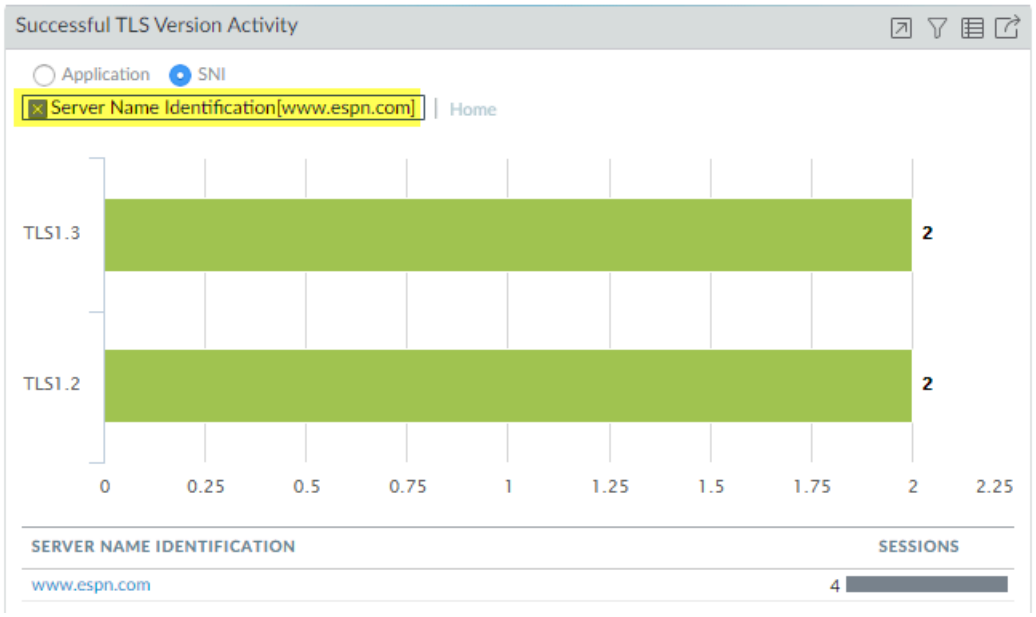
2. どの SNI が TLSv1.2を使用したかを確認するには、TLS1.2というラベルの付いた緑色のバーをクリックします。



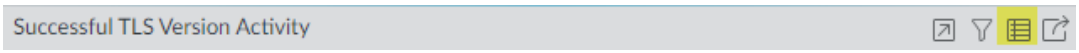
3. これで、7つの TLSv1.2セッションが4つのサーバーに分散されていることがわかります。



4. **Home (ホーム)** をクリックすると、ホーム画面に戻ります。ここで、www.espn.comをクリックすると、SNIは使用したTLSバージョンを表示します。4つのセッションのうち2つがTLSv1.3を使用し、2つが TLSv1.2を使用したことがわかります。



復号化ウィジェットの場合は、Jump to Logs (ログにジャンプ) アイコンをクリックして、ACC のデータに対応する復号化ログに直接ジャンプします:



前の例では、調査の任意の時点で、データの復号化ログにジャンプして、さらにドリルダウンすることができます。たとえば、TLSv1.2を使用した個々のセッションのログを調べて、TLSv1.3を使用しなかった理由を見つけることができます。

復号化 ACC ウィジェットは、Palo Alto Networks App-ID に基づいて復号化されたアプリケーションの名前を表示します。ACC にデータを入力する場合、ファイアウォールは Palo Alto Networks App-ID を持つアプリケーションのみを識別できます。つまり、ファイアウォールは、カスタム アプリケーションまたは App-ID を持たないアプリケーションを ACC に取り込むことはできません。コンテンツ更新によって、App-ID は定期的に更新されます。アプリケーションが不完全または不明として表示される可能性があるその他の理由は次のとおりです:

- ファイアウォールがアプリケーションを識別できるようになる前にセッションをドロップした。
- 復号化ログは、トラフィック ログに依存して、復号化ログ アプリケーション フィールドに入力します。ただし、トラフィック ログが60秒以内に完了しない場合、トラフィック ログはアプリケーションを復号化ログに入力せず、アプリケーションは不完全または不明として表示されます。

復号化ログ

復号化ログ (**Monitor (監視)** > **Logs (ログ)** > **Decryption (復号)**)は、復号化ポリシーに一致するセッションに関する包括的な情報を提供し、復号化の問題を正確かつ簡単に診断して解決できるようにそのトラフィックに関するコンテキストを取得するのに役立ちます。トラフィック

が復号化ポリシーに一致しない場合、ファイアウォールはトラフィックをログに記録しません。復号化しないトラフィックをログに記録する場合は、ポリシー ベースの復号化除外を作成し、TLSv1.2以前のトラフィックを管理するポリシーの場合は、復号化なしプロファイルをトラフィックに適用します。

PAN-OS は、次のタイプのトラフィックの復号化ログをサポートしています。

- フォワードプロキシ – いくつかのフィールドには、Root CA (信頼できる証明書のみ) やサーバー名識別 (SNI) など、フォワードプロキシ トラフィックの情報のみが表示されます。
- インバウンド インスペクション。
- 非復号化 (復号化ポリシーによって復号化から除外されたトラフィック)。

  セッションは暗号化されたままであるため、ファイアウォールに表示される情報は少なくなります。復号化されていない *TLSv1.3* トラフィックの場合、*TLSv1.3* は証明書情報を暗号化するため、証明書情報はありません。

- GlobalProtect – GlobalProtect ゲートウェイ、GlobalProtect ポータルおよび GlobalProtect クライアントレス VPN (client-to-firewall のみ) をカバーします。

  GlobalProtect は *TLSv1.3* をサポートしません。

- 復号化ミラー

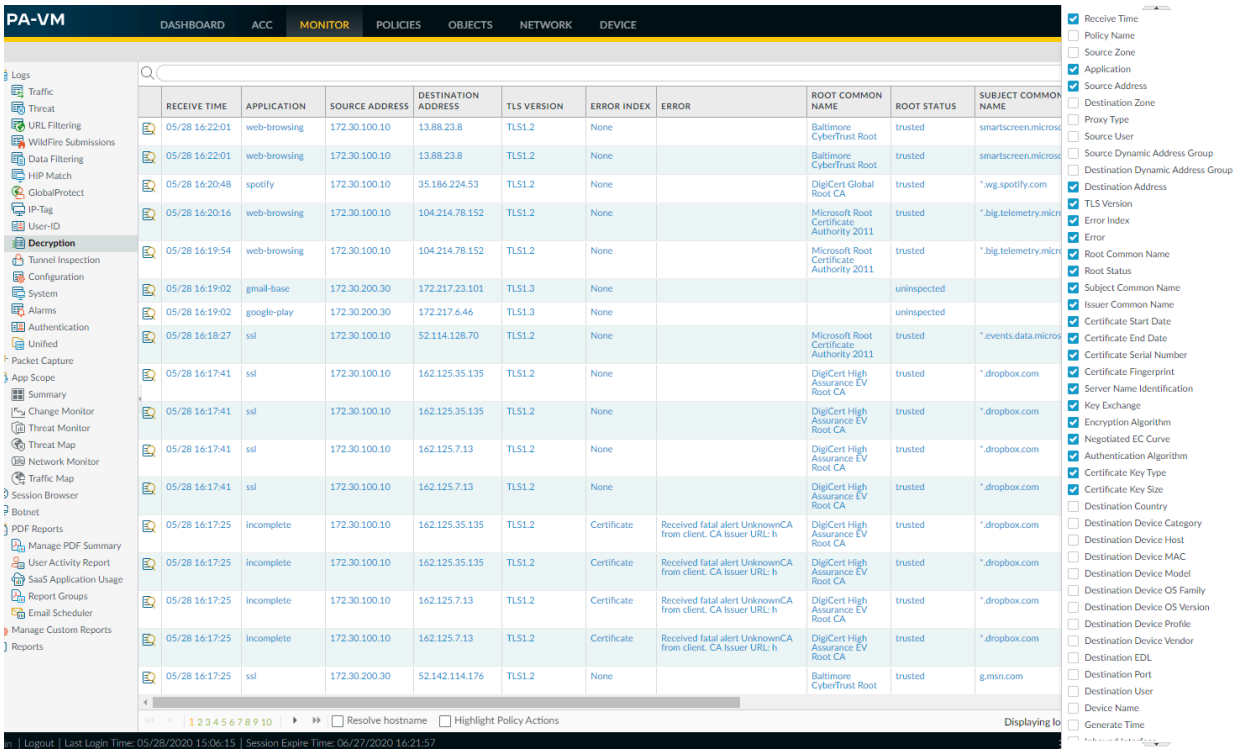
すべてのタイプのトラフィックがすべてのパラメーターをサポートしているわけではありません。プロキシ タイプおよび TLS バージョンによりサポートされていないパラメータ には、復号化トラフィックの種類ごとにサポートされていないパラメーターの完全なリストが記載されています。

フォワード プロキシ トラフィックのデータは、TLS ハンドシェークが成功したか失敗したかを基準にしています。TLS ハンドシェークが失敗した場合、ファイアウォールは、エラーの原因となったトランザクションのレッグ (クライアントからファイアウォール、またはファイアウォールからサーバー) のエラー データを送信します。TLS ハンドシェークを成功させるために、データは最初に正常に完了したレッグからのものであり、通常はクライアントからファイアウォールまでです。

ファイアウォールは、 SSL/TLS ハンドシェイク インスペクション でブロックされた *Web* トラフィックの復号化ログ エントリを生成しません。*SSL/TLS* 接続をリセットしてハンドシェイクを終了する際にファイアウォールが復号化を防止するため、これらのセッションは復号化ログに表示されません。ブロックされたセッションの詳細は、*URL* フィルタリング ログで確認できます。

復号化ログは、*SSH* プロキシ トラフィックではサポートされていません。また、セッション再開ログの証明書情報は利用できません。

デフォルトでは、ファイアウォールは失敗したすべての TLS ハンドシェーク トラフィックをログに記録します。必要に応じて、成功した TLS ハンドシェーク トラフィックをログに記録することもできます。アプリケーション、SNI、復号化ポリシー名、エラーインデックス、TLS バージョン、鍵交換バージョン、暗号化アルゴリズム、証明書キー タイプ、およびその他の多くの特性など、最大62列のログ情報を表示できます。



セッションの詳細ログ ビューを確認するには、虫眼鏡アイコン ( ) をクリックします。

復号化ログはトラフィック ログから各セッションの *App-ID* を学習するため、トラフィック ログを有効にして復号化ログに *App-ID* を表示する必要があります。トラフィック ログが無効な場合は、*App-ID* は ***incomplete*** *(*未完了*)* として表示されます。たとえば、*GlobalProtect* トラフィックの多くはゾーン内トラフィック *(Untrust* ゾーンから *Untrust* ゾーン*)* ですが、デフォルトのゾーン内ポリシーではトラフィック ログが有効になっていません。*GlobalProtect* イントラ ゾーン トラフィックの *App-ID* を表示するには、イントラ ゾーン トラフィックのトラフィックログを有効にする必要があります。

App-ID が ***incomplete*** *(*未完了*)* と表示されるもう*1*つの理由は、長いセッションの場合、トラフィック ログが完了する前にファイアウォールが復号化ログを生成する可能性があるためです *(*トラフィック ログは通常、セッションの終了時に生成されます*)*。そのような場合、*App-ID* は復号化ログに使用できません。さらに、*TLS* ハンドシェークが失敗してエラー ログが生成されると、ファイアウォールが *App-ID* を判別する前に失敗がセッションを終了するため、*App-ID* は使用できません。このような場合、アプリケーションは ***ssl*** または***incomplete*** *(*不完全*)* として表示されることがあります。

問題のトラブルシューティングを行うには、Decryption ACC ウィジェット (**ACC** > **SSL Activity**) を使用して復号化の問題を引き起こすトラフィックを特定し、Decryption ログと復号化のカスタム レポート テンプレートを使用して詳細をドリルダウンします。

復号化ログをストレージに転送するときは、復号化ログに機密情報が含まれているため、ログの転送とストレージを適切に保護するようにしてください。

復号化ログが有効になっている場合、ファイアウォールは *HTTP/2* ログをトンネル検査ログとして送信します (復号化ログが無効になっている場合、*HTTP/2* ログはトラフィック ログとして送信されます)。したがって、*HTTP/2* イベントの場合はトラフィック ログではなくトンネル検査ログを確認する必要があります。さらに、*HTTP/2* トラフィックの *App-ID* を取得するには、Tunnel Content Inspection (トンネル コンテンツ検査) を有効にする必要があります。

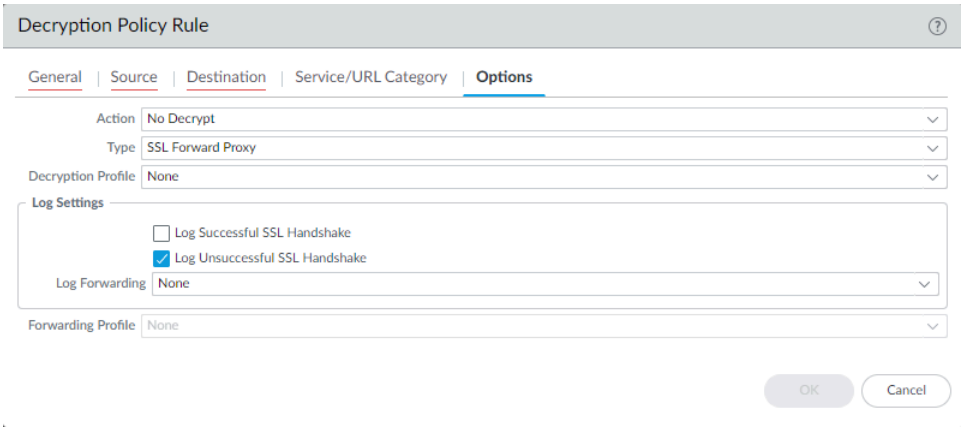
- 復号化ロギングの設定
- 修復未完了の証明書チェーン
- 復号化ログ エラー、エラー インデックス、ビットマスク

復号化ロギングの設定

ファイアウォールは、復号なしポリシーのセッションを含む、Decryption policy（復号ポリシー）によって管理されるセッションの復号化ログを生成します。ログに記録するトラフィックを制御する復号ポリシーで復号化ログを設定します。

STEP 1 | 復号ポリシーのログに記録する復号化トラフィックを設定します (**Policies (ポリシー)** > **Decryption (復号化)**)。

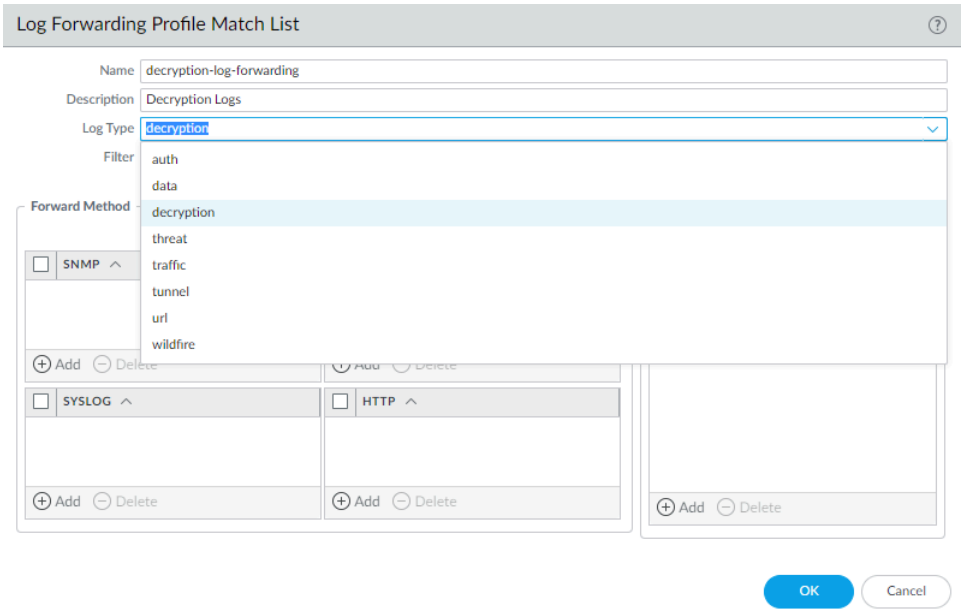
デフォルトでは、ファイアウォール は失敗した TLS ハンドシェイクのみをログに記録します:



成功したハンドシェークと失敗したハンドシェークをログに記録して、デバイスの利用可能なリソースで許可されている限りの復号化されたトラフィックを可視化します (プライベート トラフィックや機密性の高いトラフィックは復号化しないでください。復号化のベストプラクティスに従い、できるだけ多くのトラフィックを復号化します)。

STEP 2 | Log Forwarding profile (ログ転送プロファイル) を作成して、復号化ログをログ コレクター、他のストレージデバイス、または特定の管理者に転送し、復号ポリシー **Options (任意)**タブのログ転送フィールドでプロファイルを指定します。

復号化ログを転送するには、ログ転送プロファイル (**Objects (オブジェクト)** > **Log Forwarding**（ログ転送）)を設定して、復号化**Log Type (ログ タイプ)**とログの転送の方法を指定する必要があります。

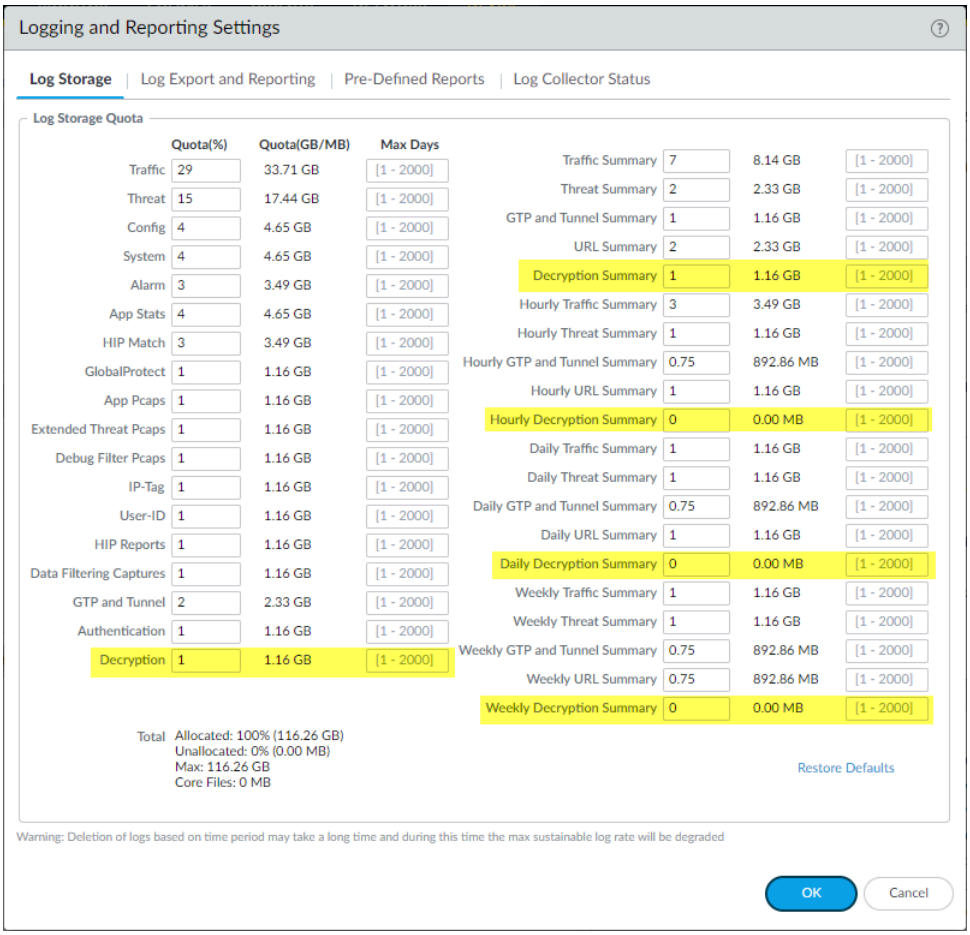


復号化ログを転送する場合は、機密情報が含まれているため、ログが安全に保存されていることを確認してください。

STEP 3 | 失敗した TLS ハンドシェークに加えて成功した TLS ハンドシェークをログに記録する場合は、ファイアウォール状の復号化ログのために、より大きなログ ストレージ容量クォータを設定します (**Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** > **Logging**

and Reporting Settings (ロギングとレポート作成の設定) > **Log Storage** (ログ ストレージ)
)。

デフォルトのクォータ (割り当て) は、復号化ログ用のデバイスのログ ストレージ容量の1パーセント、および一般的な復号化の概要用の1パーセントとなっています。時間単位、日単位、または週単位の復号化サマリーには、デフォルトの割り当てはありません。



多くの要因が復号化ログに必要なストレージの量を決定し、それらはデプロイメントによって異なります。たとえば、次の要素を考慮に入れてください:

- ファイアウォールをパススルーする TLS トラフィックの量。
- 復号する TLS トラフィックの量。
- 他のログの使用状況 (復号化ログに割り当てる容量を取得する必要があるログを評価します)。
- 成功した TLS ハンドシェークと失敗した TLS ハンドシェークの両方をログに記録する場合、失敗した TLS ハンドシェークのみをログに記録する場合に必要な容量よりも大幅に多くの容量が必要になる可能性があります。復号するトラフィックの量によっては、復号化ログがトラフィック ログまたは脅威ログと同じ容量を消費する可能性があり、デバイスの

容量がすでに満杯になっている場合は、それらの間でトレードオフが必要になる場合があります。

ログ クォータ合計割り当ては、使用可能なファイアウォール ログ リソースの*100%*を超えることはできません。

特定のデプロイメントの各ログ カテゴリに適切なクォータを見つけるために、実験が必要になる場合があります。失敗したハンドシェークのみをログに記録する場合は、デフォルトから開始するか、割り当てを2～3%に増やすことができます。成功したハンドシェークと失敗したハンドシェークの両方をログに記録する場合は、トラフィック ログに割り当てる復号化ログにスペースの約半分を割り当てることから始めることができます。復号化ログに割り当てるスペースを取得するログは、トラフィック、ビジネス、およびモニタリング要件によって異なります。

復号化ログ エラー、エラー インデックス、ビットマスク

復号化ログの **Error Index (**エラー インデックス**)** 列と **Error (**エラー**)** 列は、それぞれ復号化エラーのカテゴリと、詳細に関する情報を提供します。詳細ログビューのハンドシェークの詳細セクションで、エラーとエラー インデックス情報を表示することもできます (ログ エントリは をクリックします)。復号化ログ**Error Index (**エラー インデックス**)** は、以下のエラーカテゴリ 8 項目のいずれかを示します。

エラー インデックス	エラー (エラーインデックス表示向けの、想定されるエラー)
証明書	無効な証明書、有効期限切れの証明書、非サポートのクライアント証明書、OCSP/CRL チェックの失効と失敗、信頼されていない発行者 CA (不完全な証明書チェーンを含む、信頼されていないルートで署名されたセッション)、その他の証明書エラーなどのエラー。 サイトが完全な証明書チェーンを送信しなかったために *firewall* に中間証明書がない場合、見つからない証明書を見つけて 修復未完了の証明書チェーン にインストールできます。
暗号	以下の場合のサポートされていない暗号エラー: • クライアントは、ファイアウォールがサポートしているが、トラフィックに適用されている復号化プロファイルが非サポートの暗号を、ネゴシエートしようとしている。 • クライアントは、ファイアウォールで非サポートの暗号を、ネゴシエートしようとしている。 • (稀なケース) インバウンド インスペクションが有効になっており、サーバーの機能が復号化プロファイルの設定と一致していない。 エラーメッセージには、サポートされているクライアント暗号ビットマスク値と、サポートされている復号化プロファイル暗号ビットマスク値が含まれています。ビットマスク値を使用して、クライアントが使用を試みた暗号を

エラー インデックス	エラー (エラーインデックス表示向けの、想定されるエラー)
	識別し、このトピックで後述するように、復号化プロファイルがサポートする暗号値を一覧表示します。
機能	大きすぎる TLS ハンドシェークまたは不明なハンドシェイク、大きすぎる証明書チェーン (5つを超える証明書)、その他のサポートされていない機能などのエラー。
HSM	Hardware storage module (ハードウェア ストレージ モジュール; HSM) エラー、例えば不明な要求、設定に見つからないアイテム、要求のタイムアウト、その他の HSM エラーや障害など。
プロトコル	TLS ハンドシェークの失敗、秘密鍵と公開鍵の不一致、ハートブリード エラー、TLS 鍵交換の失敗、その他の TLS プロトコル エラーなどのエラー。プロトコル エラーは、クライアントがサポートするプロトコルをサーバーがサポートしていない場合、ファイアウォールがサポートしていない証明書タイプをサーバーが使用している場合、および一般的な TLS プロトコルエラーを示します。
リソース	メモリ不足などのエラー。
再開	セッション再開 ID とチケット、およびファイアウォール キャッシュ内のセッション再開エントリに関するセッション再開エラー、その他のセッション再開エラー。
バージョン	クライアントと復号化プロファイルのバージョン不一致、およびクライアントとサーバーのバージョン不一致に関するエラー。 エラー メッセージには、サポートされているクライアントと復号化プロファイルのバージョンを識別する、ビットマスク値が含まれています。ビットマスク値を使用して、クライアントが使用を試みた暗号を識別し、このトピックで後述するように、復号化プロファイルがサポートする暗号値を一覧表示します。

エラーに適したエラー説明カテゴリが存在しない場合、デフォルトのメッセージは ***General TLS protocol error (***一般 ***TLS*** プロトコル エラー***)*** です。

バージョンおよび暗号ログのエラー情報には、ビットマスク値が含まれており、これを操作 CLIコマンドを使用して実際の値に変換します。

- バージョン エラーのビットマスク値は、クライアントとサーバーが使用する TLS プロトコル バージョン間の不一致を識別し、またトラフィックに適用されるクライアントと復号化プロ

ファイル間の TLS プロトコルの不一致も識別します。バージョン エラー ビットマスクを変換する CLI コマンドは次のとおりです。

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version
 <bitmask-value>
```

このコマンドは、ビットマスクに一致する TLS バージョンを返します。

- 暗号エラー ビットマスク値は、クライアントと、トラフィックに適用される復号化プロファイルとの間の、暗号化その他の不一致を識別します。

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher <bitmask-
value>
```

このコマンドは、ビットマスクに一致する暗号を返します。

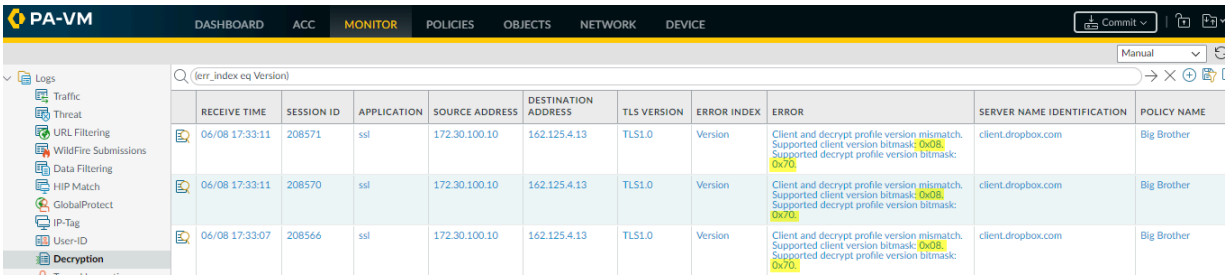
復号化ログをフィルタリングしてバージョンと暗号のエラーを検索し、エラーのあるセッションのビットマスク値を適切な CLI コマンドに接続し、エラーの原因となったプロトコルのバージョンまたは暗号の値を取得し、その情報を使用して、問題のサイトへのアクセスを許可したい場合に、復号化ポリシーまたはプロファイルを更新します。

- バージョンのエラー
- 暗号エラー
- ルート ステータス 「Uninspected (未検査)」

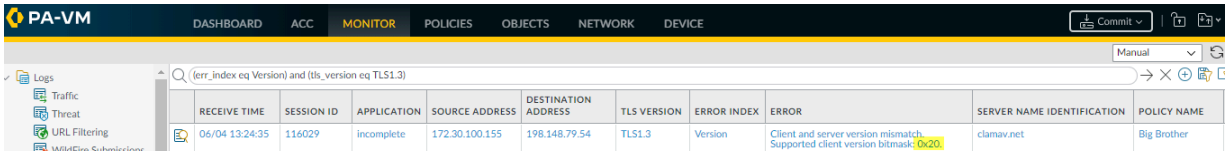
バージョンのエラー

バージョンの不一致エラーを特定して修正する方法:

1. フィルタ **(err_index eq Version)** を使用して復号化ログをフィルタし、バージョンのエラーを識別します。強調表示されている値はビットマスク値です。



復号化ログは、さまざまな方法でフィルタリングできます。たとえば、TLS v1.3バージョン エラーのみを表示するには、フィルタ **(err_index eq Version)** および **(tls_version eq TLS1.3)** を使用します。



2. CLI にログインし、ビットマスク値を検索します。最初のスクリーンショットのバージョン エラー (3つのセッションすべてで同じエラー) は、クライアントと復号化プロファイルの不一致に関する問題を示しています。サポートされているクライアントバージョンのビットマスクは 0x08 で、サポートされている復号化プロファイルのバージョン ビットマスクは 0x70 です。

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x08
```

```
TLSv1.0
```

この出力は、クライアントが TLSv1.0 のみをサポートしていることを示しています。

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x70
```

```
TLSv1.1
```

```
TSLv1.2
```

```
TLSv1.3
```

この出力は、復号化プロファイルが TLSv1.1、TLSv1.2、および TLSv1.3 をサポートしているが、TLSv1.0 はサポートしていないことを示しています。これで、問題はクライアントが非常に古いバージョンの TLS プロトコルのみをサポートしており、トラフィックを制御する復号化ポリシー ルールにアタッチされた復号化プロファイルが、TLSv1.0 トラフィックを許可しないことであると分かりました。

次にすることは、実行する対策の決定です。より安全な TLS バージョンを受け入れるよう、クライアントを更新できます。クライアントが何らかの理由で TLSv1.0 を必要とする場合は、ファイアウォールに引き続きトラフィックのブロックさせておくか、復号プロファイルを更新してすべての TLSv1.0 トラフィックを許可するか (非推奨)、または TLSv1.0 を許可する復号化ポリシーとプロファイルを作成して、それを TLSv1.0 を使用する必要があり、より安全なプロトコルをサポートできないクライアントデバイスにのみ適用することができます (トラフィック許可の最も安全なオプション)。

2 番目のスクリーンショットのバージョン エラーは、別の問題を示しています。クライアントとサーバーのバージョン不一致です。エラーは、サポートされているクライアント ビットマスクが 0x20 であることを示しています。

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x20
```

```
TLSv1.2
```

この出力は、クライアントが TLSv1.2 のみをサポートしていることを示しています。サーバーは TLSv1.2 をサポートしていないため、TLSv1.3 のみをサポートする場合もあれ

ば、TLSv1.1 以下 (安全性の低いプロトコル) のみをサポートする場合もあります。Wireshark または別のパケット解析ツールを使用して、サーバーがサポートしている TLS のバージョンを確認できます。サーバーのサポート対象に応じて、以下のことができます。

- サーバーが TLSv1.3 のみをサポートしている場合は、TLSv1.3 をサポートするように復号化プロファイルを編集できます。
- サーバーが TLSv1.1 以下のみをサポートしている場合は、ビジネス上の理由でそのサーバーにアクセスする必要があるかどうかを評価します。不要な場合は、セキュリティ強化のためトラフィックをブロックすることを検討してください。ビジネス目的でサーバーにアクセスする必要がある場合は、サーバーを作成するか、ビジネスでアクセスする必要のあるサーバーとサイトにのみ適用される復号化ポリシーにサーバーを追加します。安全性の低い TLS バージョンを使用したすべてのサーバーへのアクセスは、許可しないでください。

3. セッション トラフィックを制御する復号化ポリシーを検索するには、ログの **Policy Name (ポリシー名)**列を確認します (または、復号化ログの横にある虫眼鏡アイコンをクリックして、詳細ログ ビューの全般セクションの情報を表示します)。上記の例では、復号化ポリシー名は「BigBrother」です。復号化ポリシーとプロファイルを検索するには、**Policies (ポリシー)** > **Decryption (復号化)**に移動し、「Big Brother」という名前のポリシーを選択してから、**Option (オプション)** タブを選択します。**Decryption profile (復号化プロファイル)** には、復号化プロファイル名が表示されます。

   Objects (オブジェクト) > **Decryption (復号化)** > **Decryption Profile (復号化プロファイル)**に移動し、適切な復号化プロファイルを選択して、バージョンの問題に対処するように編集します。

暗号エラー

復号化ログを使用した暗号エラーの検出は、バージョン エラーの検出に似ています。ログをフィルタリングしてエラーを見つけ、エラー ビットマスクを取得します。次に、CLI に移動し、ビットマスクをエラー値に変換してから、適切に対処して問題を修正します。以下に例を示します。

1. フィルタ **(err_index eq Cipher)** を使用して復号化ログをフィルタし、暗号エラーを識別します。例えば、**Error (エラー)** メッセージ 「`Unsupported cipher`」 の暗号エラーを調査するとしましょう。サポートされているクライアント暗号ビットマスク:`0x80000000`。サポートされている復号化プロファイル暗号ビットマスク `0x60f79980`。

2. CLI にログインし、ビットマスク値を検索します。

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher
 0x80000000
```

```
CHACHA_PLY1305_SHA256
```

この出力は、ファイアウォールがサポートする暗号をクライアントがネゴシエートしようとしたことを示しています (ビットマスクがすべてゼロの場合 (`0x0000000`)、ファイアウォールがサポートしない暗号をクライアントがネゴシエートしようとした):

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-cipher
 0x80000000
```

```
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS13_WITH_AES_256_GCM_SHA384
TLS13_WITH_AES_128_GCM_SHA256
```

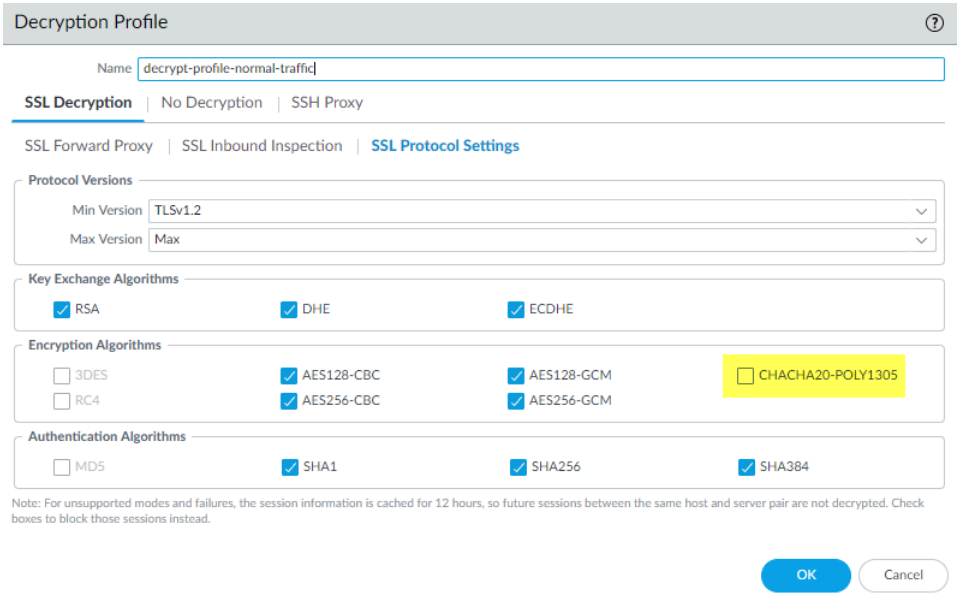
この出力は、トラフィックを制御する復号化プロファイルが多くの暗号をサポートしているが、クライアントが使用を試みている暗号はサポートしていないことを示しています。

ファイアウォールがトラフィックを許可および復号化するよう、この問題を修正するには、復号化プロファイルに欠落している暗号のサポートを追加する必要があります。

3. 復号化ログまたは詳細ログビューの**Policy Name (ポリシー名)** を確認して、トラフィックを制御する復号化ポリシーの名前を取得します。**Policies (ポリシー)** > **Decryption (復号化)** に移動し、ポリシーを選択します。**Options (オプション)** タブで、復号化プロファイルの名前を検索します。次に、**Objects (オブジェクト)** > **Decryption (復号化)** > **Decryption Profile (復号化プ**

ロファイル) に移動し、適切な復号化プロファイルを選択して、バージョンの問題に対処するように編集します。

この例では、復号化プロファイルは TLS13_WITH_CHACHA_POLY1305_SHA256 暗号をサポートしないため、クライアントは接続できません。



問題を修正するには、**CHACHA20-POLY1305** 暗号アルゴリズム オプション (**Max Version (最大バージョン)** 設定の **Max (最大)** は、プロファイルがすでに TLSv1.3 をサポートしており、認証アルゴリズム設定には SHA256 がすでに含まれていることを意味し、したがって、暗号アルゴリズムのサポートのみが欠けている) を選択してから、設定を **Commit (コミット)** します。設定のコミット後、復号化プロファイルは欠落している暗号をサポートし、トラフィックの復号化セッションは成功します。

firewall が暗号スイートをサポートしておらず、ビジネス目的でトラフィックを許可する必要がある場合は、そのトラフィックにのみ適用される *Decryption* ポリシーとプロファイルを作成します。*Decryption* プロファイルで、サポートされていない暗号スイートでセッションをブロックする オプション

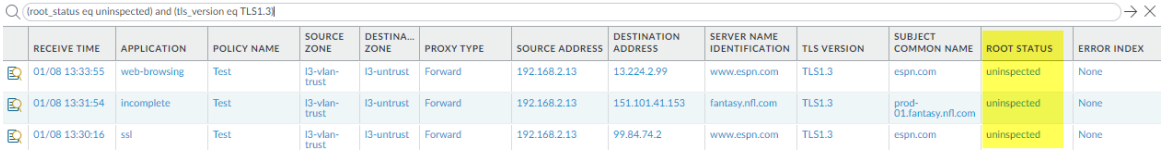
を無効にします。

ルート ステータス 「**Uninspected (未検査)**」

いくつかのケースで、**Root Status (ルート ステータス)** 列に表示される値が、**uninspected (未検査)** となる場合があります。ファイアウォールがルート ステータスを検査できなかった理由は、以下を含めいくつかあります。

- セッション再開。
- 非復号化ポリシーがトラフィックを制御したことでトラフィックが復号化されず、このためファイアウォールはトラフィックを復号化しなかった。
- ファイアウォールがサーバー証明書を検査する前に、復号化の失敗が発生した。

復号化ログ **(root_status eq uninspected)** と **(tls_version eq TLS1.3)** をフィルタして、ルート ステータスが未検査の復号化セッションを表示します。



修復未完了の証明書チェーン

RFC 5246 TLSv1.2標準では、認証済みサーバーが有効な認証チェーンを提供して、受け入れ可能な Certificate Authority (認証局 - CA) につながる必要がありますが、すべての Web サイトが完全な証明書チェーンを送信するわけではありません。復号化を有効にし、Decryption ポリシーで 信頼できない発行者とのセッションをブロックする を有効にする Forward Proxy Decryption プロファイルを適用すると、Web サイトのサーバーが firewall に提示する証明書リストに中間証明書がない場合、firewall は最上位 (ルート) 証明書への証明書チェーンを構築できません。このような場合、ファイアウォールがルート証明書へのチェーンを構築できず、欠落している中間証明書がないと信頼を確立できないため、ファイアウォールはクライアントにフォワードアントラスト証明書を提示します。

ファイアウォールのデフォルトの信頼された認証局ストアにのみ、ファイアウォールのルート証明書があります。

ビジネス目的で通信する必要のある Web サイトに1つ以上の欠落している中間証明書があり、復号プロファイルが信頼されていない発行者とのセッションをブロックしている場合、欠落している中間証明書を見つけてダウンロードし、信頼されたルートCA としてファイアウォールにインストールして、ファイアウォールが、そのサイトのサーバーを信頼するようにできます。(別の方法は、Web サイトのオーナーに連絡して、ハンドシェーク中に中間証明書を送信するようにサーバーを設定する依頼をすることです。)

復号プロファイルで信頼されていない発行者とのセッションを許可すると、発行者が信頼されていない場合でもファイアウォールはセッションを確立します。ただし、ベストプラクティスは、セキュリティ強化のため、信頼されていない発行者とのセッションをブロックすることです。

STEP 1 | 不完全な証明書チェーン エラーの原因となる Web サイトを見つけます。

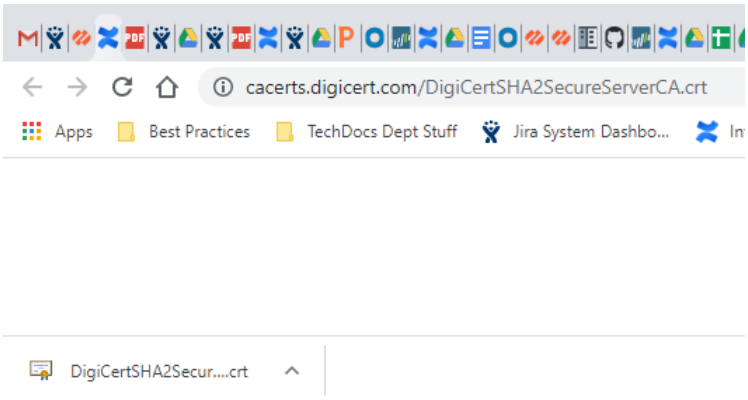
1. 復号化ログをフィルタリングして、証明書チェーンが不完全なために失敗した復号化セッションを特定します。

   フィルタ フィールド内で、クエリ **(err_index eq Certificate)** と **(error contains 'http')** を入力します。このクエリは、文字列「http」を含む証明書エラーのログをフィルタリングします。これにより、CA発行者URL (URI と呼ばれることが多い) を含むすべてのエラー エントリが検索されます。CA 発行者の URL は、CA 発行者のAuthority Information Access (認証局情報アクセス; AIA) 情報です。

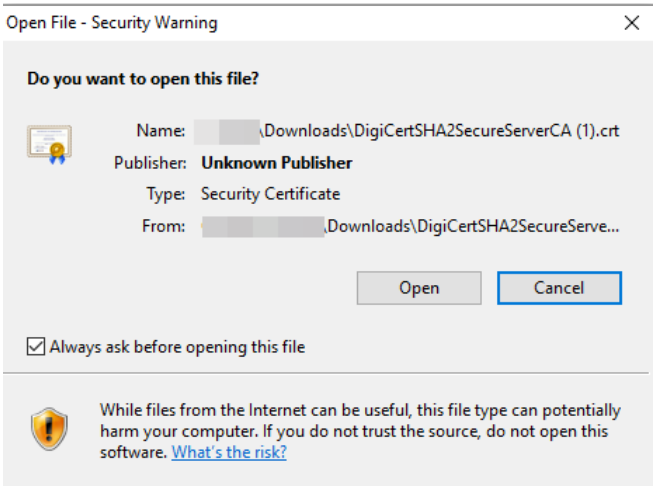
2. 以下で始まる**Error (エラー)** 列のエントリをクリックします: 「Received fatal alert UnknownCA from client. (クライアントから致命的なアラート UnknownCA を受信しました。)CA Issuer URL:」この後に URI が続きます。

ファイアウォールは、選択したエラーをクエリに自動的に追加し、完全な URI パスを表示します (完全な URI パスは、**Error (エラー)** 列で切り捨てられる場合があります)。

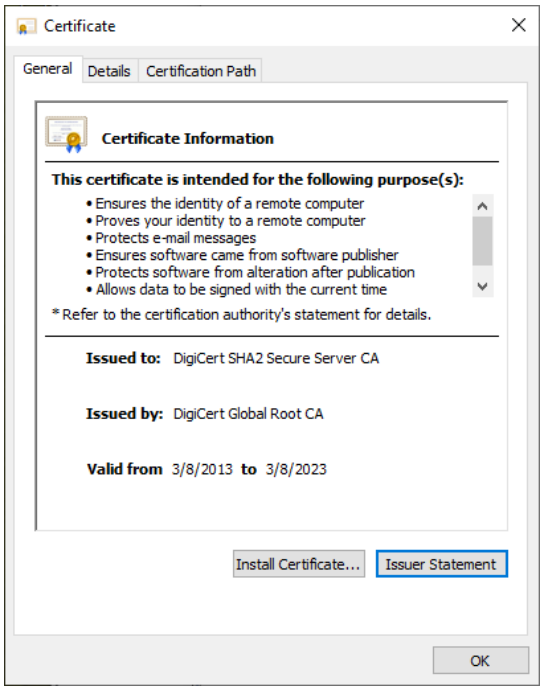
STEP 2 | URI をコピーしてブラウザに貼り付け、Enter キーを押して、不足している中間証明書をダウンロードします。



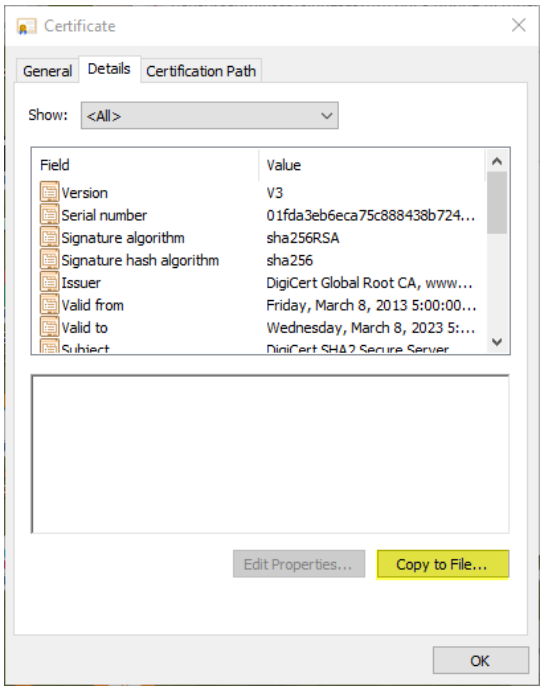
STEP 3 | 証明書をクリックしてダイアログボックスを開きます。



STEP 4 | **Open (開く)** をクリックして、証明書ファイルを開きます。



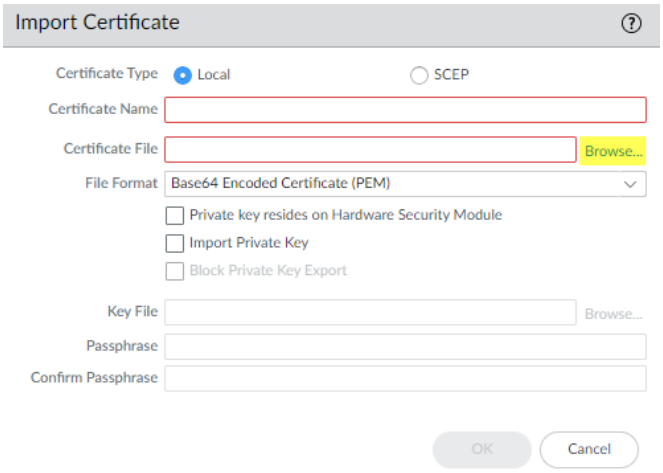
STEP 5 | **Details (詳細)** タブを選択してから、**Copy to File... (ファイルにコピー)**をクリックします。



エクスポートの指示に従います。証明書は、デフォルトのダウンロード フォルダとして指定したフォルダにコピーされます。

STEP 6 | 証明書をファイアウォールにインポートします。

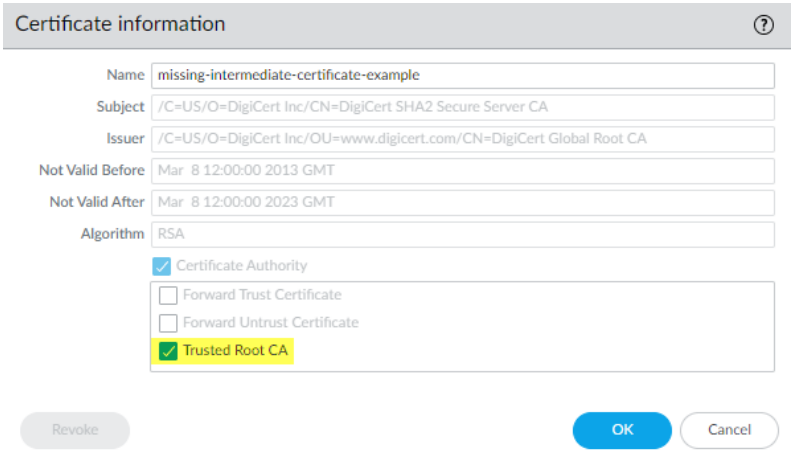
1. **Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificates (証明書)** の順に移動してから、**Import (インポート)** を選択します。
2. **Browse (参照)** から、欠落している中間証明書を保存したフォルダを選択します。**File Format (ファイル フォーマット)** は、**Base64 Encoded Certificate (PEM)**（**Base64** エンコード済み証明書 **(PEM)**）のままにしておきます。



3. 証明書に名前を付け、使用したいその他のオプションを指定して、**OK** をクリックします。

STEP 7 | 証明書がインポートされたら、**Device Certificates (デバイス証明書)** リストから証明書を選択して、Certificate Information (証明書情報) ダイアログを開きます。

STEP 8 | **Trusted Root CA (信頼されたルートCA)** を選択して、証明書をファイアウォール上で信頼されたルートCAとしてマークしてから、**OK** をクリックします。



Device (デバイス) > **Certificate Management (証明書管理)** > **Certificates (証明書)** > **Device Certificates (デバイス証明書)** で、インポートされた証明書が証明書リストに表示されるようになります。**Usage (使用状況)** 列をチェックして、ステータスが **Trusted Root CA Certificate (信頼されたルートCA 証明書)** であることを確認して、ファイアウォールが証明書を信頼されたルートCA と見なしていることを検証します。

STEP 9 | 設定を **Commit**（コミット）します。

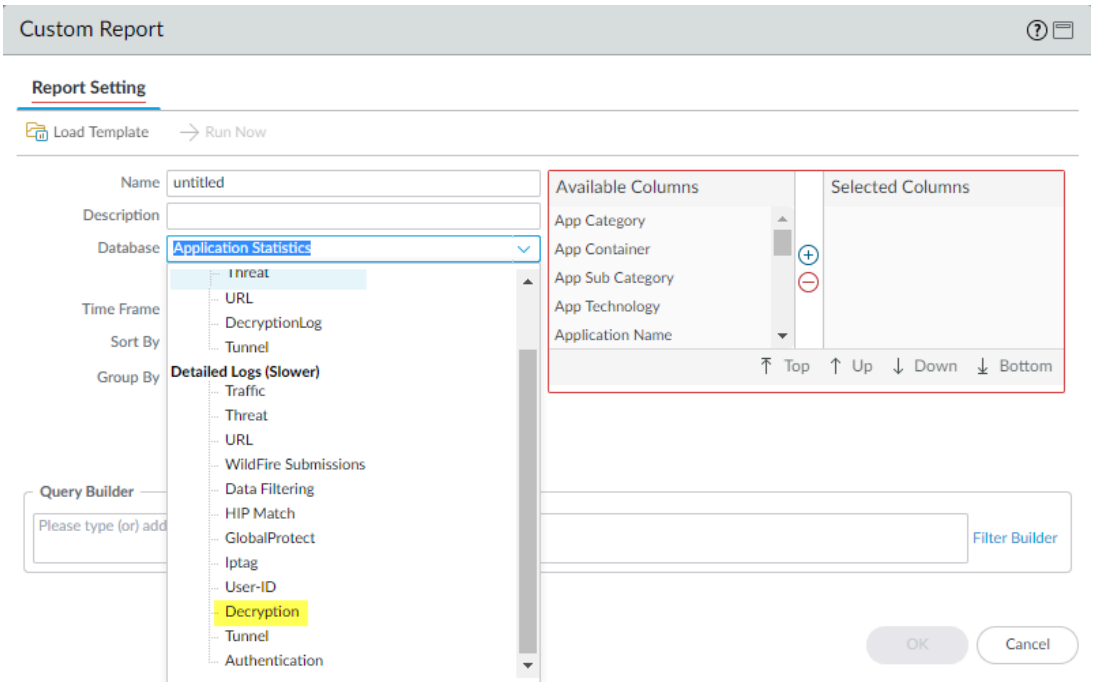
STEP 10 | これで、破損した証明書チェーンが修復されました。

信頼されていない CA 発行者ではなくなったため、ファイアウォールはトラフィックをブロックしません。欠落しているすべての中間証明書に対してこのプロセスを繰り返して、証明書チェーンを修復します。

復号化のカスタム レポート テンプレート

復号化ログ フィールドおよびカスタム テンプレートに基づく復号化イベントのカスタム レポートを作成して生成することができます。カスタム レポートに含めるログ フィールドを選択し、テンプレートを選択してログ クエリを絞り込みます:

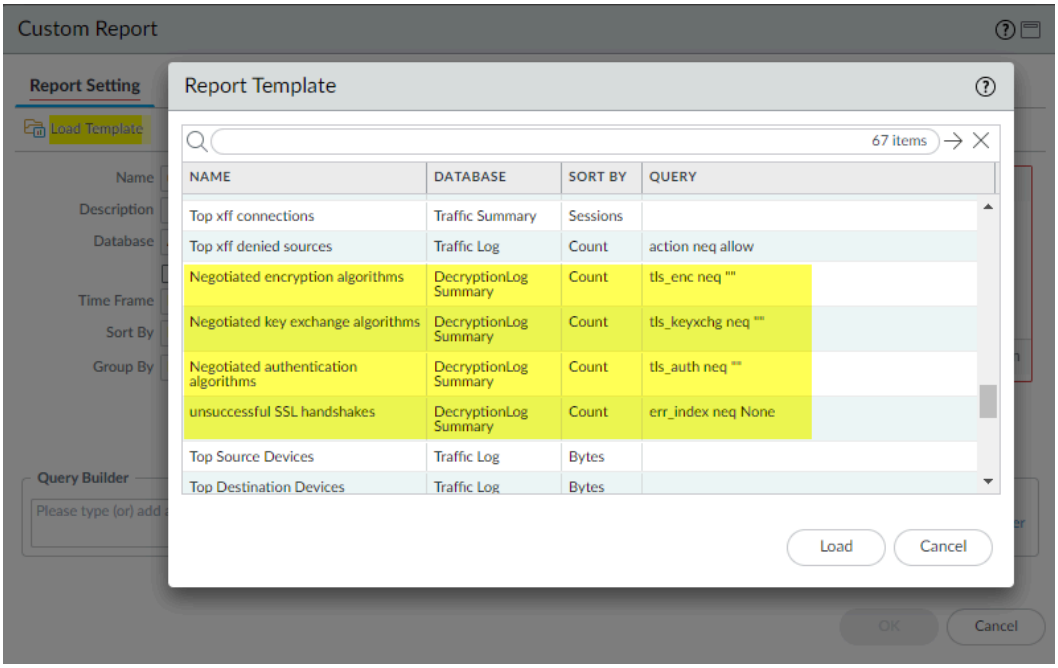
1. **Manage Custom Reports(** カスタム レポートの管理**)** を > 監視します。
2. カスタム レポートを**Add (**追加**)** します。
3. カスタム レポート内で使用する復号化 ログ フィールドを設定するには、**Decryption (**復号化**)** を **Database (**データベース**)** として選択します。



Available Columns (使用可能な列**)** リストは、復号化ログで使用可能な列と一致するように変更されます。カスタム レポートに含める列 (情報) を選択して追加します。カスタム レポートをさらに絞り込むことを望まない場合は、**OK** をクリックしてレポートを生成します。

4. 必要に応じて、クエリ ビルダーと PAN-OS 10.0 で導入された4つのテンプレートを使用して、カスタム復号化レポートの出力を調整します。テンプレートを選択してレポート出力を

フィルタするには、**Load Template (**テンプレートのロード**)** をクリックして、4つの復号化テンプレートから選択します:



Query (クエリ**)** 列には、各テンプレートが表すフィルター クエリが表示されます。目的のクエリを **Load (**ロード**)**、**OK** をクリックしてカスタム レポートを生成します。

プロキシ タイプおよび TLS バージョンによりサポートされていないパラメータ

復号化ログ フィールドには、各復号化プロキシ タイプの復号化セッション パラメータが表示されます。ただし、バージョンのサポート、TLS ハンドシェークの暗号化された部分、情報の可用性などの理由により、一部のパラメータはすべてのプロキシ タイプまたは TLS バージョンで使用できるわけではありません。次の表は、プロキシの種類とTLSのバージョン別に、サポートされていない復号化ログのパラメータを示しています。

プロキシ タイプ	非サポートのパラメータ	**TLS** バージョン
Forward Proxy (フォワードプロキシ)	Negotiated EC Curve (ネゴシエートされた楕円曲線)	TLSv1.3
Inbound Inspection (インバウンド インスペクション)	Server Name Identification (サーバー名識別情報) Root (ルート) Common Name (共通名 - CN)	すべて
	Negotiated EC Curve (ネゴシエートされた楕円曲線)	TLSv1.3

プロキシ タイプ	非サポートのパラメータ	TLS バージョン
No Decrypt(復号なし)(復号化ポリシールールの **No Decrypt (**復号なし**)** アクション)	Negotiated EC Curve (ネゴシエートされた楕円曲線) Server Name Identification (サーバー名識別情報)	TLSv1.2
	Negotiated EC Curve (ネゴシエートされた楕円曲線) Server Name Identification (サーバー名識別情報) Certificate Information (証明書情報) (全ての証明書情報フィールド、例えば、証明書の開始日、証明書の終了日、証明書キーの種類など)	TLSv1.3
ネットワークパケットブローカー	Negotiated EC Curve (ネゴシエートされた楕円曲線)	TLSv1.3
GlobalProtectポータル	Server Name Identification (サーバー名識別情報) Root (ルート) Common Name (共通名 - CN) 復号化ポリシー名 App-ID	すべて
GlobalProtectゲートウェイ	Server Name Identification (サーバー名識別情報) 復号化ポリシー名 App-ID	すべて
クライアントレス SSL VPN	Server Name Identification (サーバー名識別情報)	すべて
SSH	非サポートの復号化ログ	
Cleartext (平文)	非サポートの復号化ログ	

復号化 トラブルシューティング ワークフロー例

Application Comand Center (ACC) の 復号化ログ と SSL アクティビティ ウィジェット は、独立しても連携しても機能する強力な Decryption トラブルシューティング ツールを提供します。これらツールの使用方法を理解すると、さまざまな復号化の問題を調査して対処できます。

以下の例は、トラブルシューティング ツールを使用して、復号化の問題を特定、調査、および対処する方法を示しています。これらの方法を適用して、復号化デプロイメントで発生した問題のトラブルシューティングを行います。

- 復号化エラーの理由調査
- サポートされていない暗号スイートのトラブルシューティングを実行
- 脆弱なプロトコルと暗号スイートを識別する
- 信頼されていない CA 証明書を識別する
- 有効期限切れの証明書のトラブルシューティングを実行
- 失効した証明書のトラブルシューティングを実行
- ピン留めされた証明書のトラブルシューティングを実行

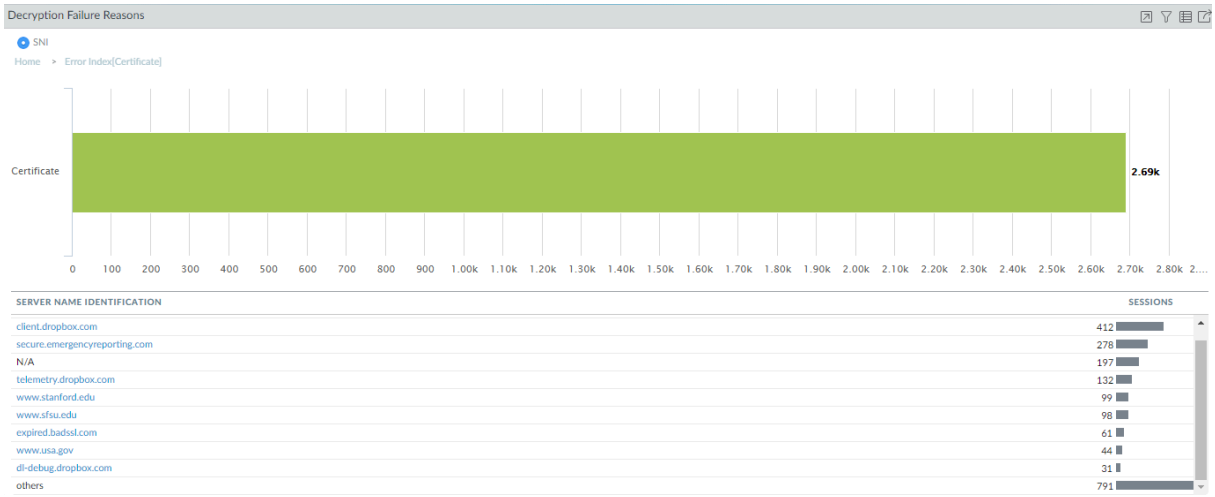
復号化エラーの理由調査

復号化エラーの最も一般的な理由は、TLS プロトコルエラー、暗号バージョン関連エラー (クライアントとサーバーのバージョンの不一致、およびクライアントと復号プロファイルのバージョンの不一致)、ならびに証明書エラーです。復号化エラーを調査するには、まず Application Command Center (アプリケーション コマンド センター - ACC) でエラーを特定し、次に復号化ログに移動して詳細に掘り下げます。

STEP 1 | **ACC** > **SSL Avtivity (SSL**アクティビティ**)** で調査を開始し、Decryption Failure Reasons (復号化エラーの理由) ウィジェットを確認します。

この例では、証明書エラーを調査します。同じプロセスを使用して、バージョンやプロトコル関連のエラーを調査できます。

STEP 2 | **Certificate (証明書)** の横にある緑色のバーをクリックして、証明書エラーが発生したホスト (SNI) と、証明書エラーの数が最も多いホストのリストを確認します。



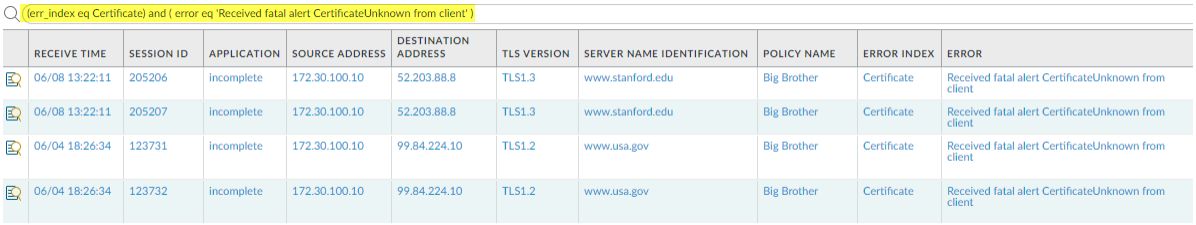
STEP 3 | **Monitor (監視)** > **Logs (ログ)** > **Decryption (復号化)** に移動して、ログを掘り下げます。

クエリ **(err_index eq Certificate)** を使用して復号化ログをフィルタリングし、証明書エラーが発生したすべての復号化セッションを表示します。

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	SERVER NAME IDENTIFICATION	POLICY NAME	ERROR INDEX	ERROR
06/08 13:22:11	205207	incomplete	172.30.100.10	52.203.88.8	TLS1.3	www.stanford.edu	Big Brother	Certificate	Received fatal alert CertificateUnknown from client
06/08 11:17:14	203671	ssl	172.30.100.10	52.9.173.94	TLS1.2	expired-isrgrootx1.letsencrypt.	Big Brother	Certificate	Expired server certificate. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:17:14	203669	incomplete	172.30.100.10	52.9.173.94	TLS1.2	expired-isrgrootx1.letsencrypt.	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:17:11	203666	incomplete	172.30.100.10	52.9.173.94	TLS1.2	expired-isrgrootx1.letsencrypt.	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:17:11	203663	incomplete	172.30.100.10	52.9.173.94	TLS1.2	expired-isrgrootx1.letsencrypt.	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:16:18	203598	ssl	172.30.100.10	52.9.173.94	TLS1.2	revoked-isrgrootx1.letsencrypt.	Big Brother	Certificate	OCSP/CRL check: certificate revoked. CA Issuer URL: http://cert.int-x3.letsencrypt.org/
06/08 11:16:18	203576	ssl	172.30.100.10	52.9.173.94	TLS1.2	revoked-isrgrootx1.letsencrypt.	Big Brother	Certificate	OCSP/CRL check: certificate revoked
06/08 11:16:18	203575	ssl	172.30.100.10	52.9.173.94	TLS1.2	revoked-isrgrootx1.letsencrypt.	Big Brother	Certificate	OCSP/CRL check: certificate revoked
06/04 18:26:34	123731	incomplete	172.30.100.10	99.84.224.10	TLS1.2	www.usa.gov	Big Brother	Certificate	Received fatal alert CertificateUnknown from client

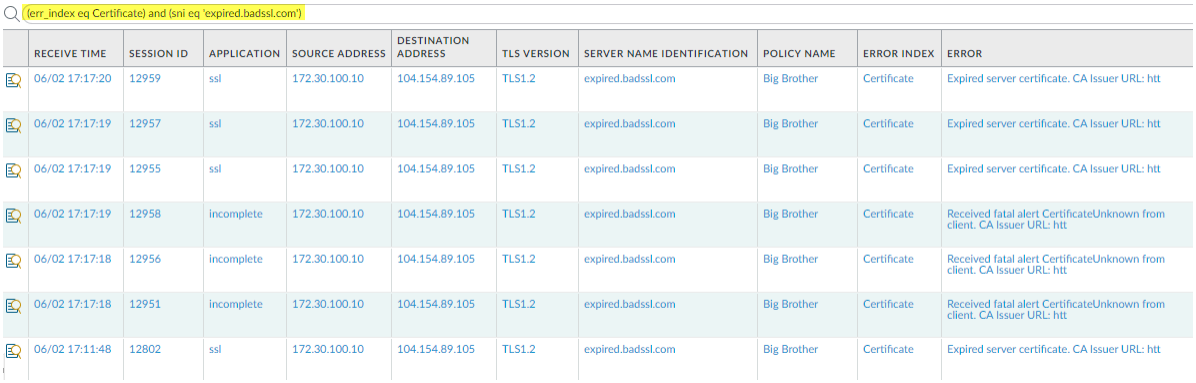
Error (エラー) 列には、証明書エラーの理由が表示されます。同じエラーが発生したすべての復号化セッションをフィルタリングするには、エラー メッセージをクリックしてクエリに追加してから、クエリを実行します。たとえば、クライアントからの致命的なアラートの受信に基づいてすべてのエラーを見つけるには、エラーをクリックすると、クエ

リ **(err_index eq Certificate)**、および **(error eq 'Received fatal alert CertificateUnknown from client')** が生成されます。


(err_index eq Certificate) and (error eq 'Received fatal alert CertificateUnknown from client')

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	SERVER NAME IDENTIFICATION	POLICY NAME	ERROR INDEX	ERROR
06/08 13:22:11	205206	incomplete	172.30.100.10	52.203.88.8	TLS1.3	www.stanford.edu	Big Brother	Certificate	Received fatal alert CertificateUnknown from client
06/08 13:22:11	205207	incomplete	172.30.100.10	52.203.88.8	TLS1.3	www.stanford.edu	Big Brother	Certificate	Received fatal alert CertificateUnknown from client
06/04 18:26:34	123731	incomplete	172.30.100.10	99.84.224.10	TLS1.2	www.usa.gov	Big Brother	Certificate	Received fatal alert CertificateUnknown from client
06/04 18:26:34	123732	incomplete	172.30.100.10	99.84.224.10	TLS1.2	www.usa.gov	Big Brother	Certificate	Received fatal alert CertificateUnknown from client

特定のホストが受信した証明書エラーをフィルタリングするには、エラーメッセージテキストを追加する代わりに、その SNI をクエリに追加します。たとえば、expired.badssl.comm の証明書エラーをすべて見つけるには、クエリ **(err_index eq Certificate)**、および **(sni eq'expired.badssl.com ')** を使用します。


(err_index eq Certificate) and (sni eq 'expired.badssl.com')

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	SERVER NAME IDENTIFICATION	POLICY NAME	ERROR INDEX	ERROR
06/02 17:17:20	12959	ssl	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Expired server certificate. CA Issuer URL: htt
06/02 17:17:19	12957	ssl	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Expired server certificate. CA Issuer URL: htt
06/02 17:17:19	12955	ssl	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Expired server certificate. CA Issuer URL: htt
06/02 17:17:19	12958	incomplete	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: htt
06/02 17:17:18	12956	incomplete	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: htt
06/02 17:17:18	12951	incomplete	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Received fatal alert CertificateUnknown from client. CA Issuer URL: htt
06/02 17:11:48	12802	ssl	172.30.100.10	104.154.89.105	TLS1.2	expired.badssl.com	Big Brother	Certificate	Expired server certificate. CA Issuer URL: htt

Error (エラー) 列には、expired.badssl.com に関連する各証明書エラーの具体的な理由が表示されます。

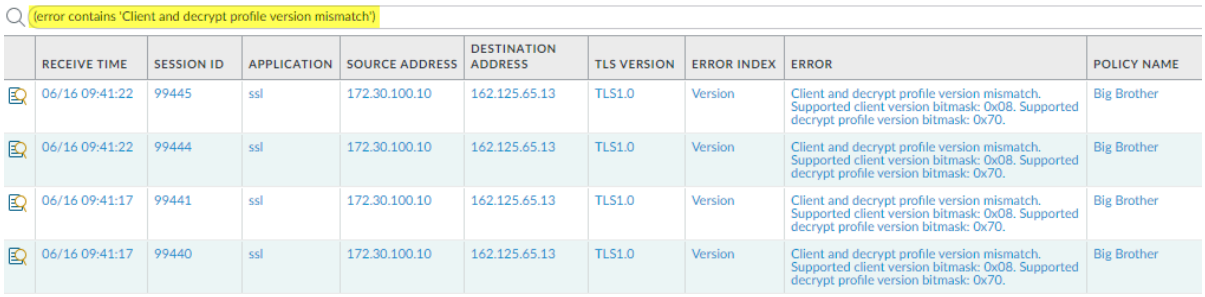
復号化エラーの原因となった証明書の問題の理由が判明すれば、それに対処できます。たとえば、証明書チェーンが不完全な場合、不完全な証明書チェーンを修復することができます。証明書が有効期限切れの場合、サイト管理者に通知するか、サイトにアクセスする必要がある場合は、ポリシーベースの例外を作成することで対処が可能になります。

サポートされていない暗号スイートのトラブルシューティングを実行

復号化ログでサポートされていない暗号スイートを特定してトラブルシューティングすることは、バージョン エラー調査の一つの側面であり、それ自体で調べる価値があります。

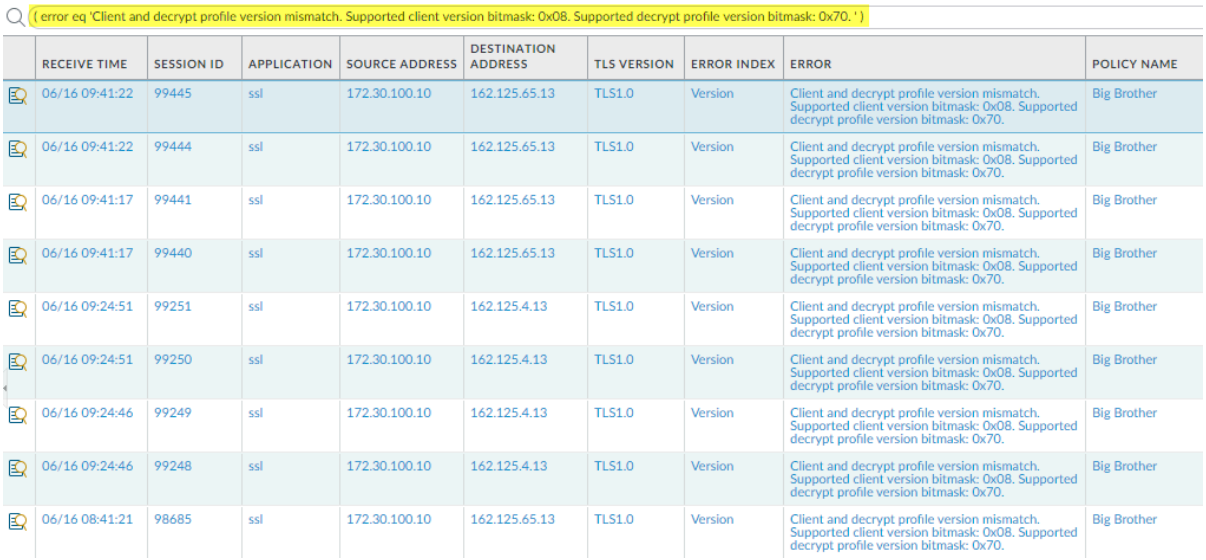
STEP 1 | 復号化ログ (**Monitor (監視)** > **Logs (ログ)** > **Decryption (復号化)**) で、クエリ **(error contains 'Client and decrypt profile mismatch'**を使用し、すべての暗号スイートバージョンの不一致を特定します。

これらの不一致のログをフィルタリングすると、クライアントと復号プロファイル暗号スイートのサポートが一致しない、すべてのインスタンスが検出されます。



RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME
06/16 09:41:22	99445	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:41:22	99444	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:41:17	99441	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:41:17	99440	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother

同じエラーが発生したすべての復号化セッションを見つけるには、エラー メッセージをクリックしてクエリに追加し、元のクエリを削除します。以下に例を示します:



RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME
06/16 09:41:22	99445	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:41:22	99444	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:41:17	99441	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:41:17	99440	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:24:51	99251	ssl	172.30.100.10	162.125.4.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:24:51	99250	ssl	172.30.100.10	162.125.4.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:24:46	99249	ssl	172.30.100.10	162.125.4.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 09:24:46	99248	ssl	172.30.100.10	162.125.4.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother
06/16 08:41:21	98685	ssl	172.30.100.10	162.125.65.13	TLS1.0	Version	Client and decrypt profile version mismatch. Supported client version bitmask: 0x08. Supported decrypt profile version bitmask: 0x70.	Big Brother

16進コードは、クライアントがサポートする正確なバージョンと、復号プロファイルがサポートする正確なバージョンを識別します。

STEP 2 | CLI にログインし、ビットマスク値を検索します。

エラーは、クライアントと復号プロファイルの不一致を示しています。サポートされているクライアント ビットマスクは0x08で、サポートされている復号プロファイル ビットマスクは0x70です:

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x08
```

```
TLSv1.0
```

この出力は、クライアントが TLSv1.0 のみをサポートしていることを示しています。

```
admin@vm1>debug dataplane show ssl-decrypt bitmask-version 0x70
```

```
TLSv1.1
```

```
TSLv1.2
```

```
TLSv1.3
```

この出力は、復号化プロファイルが TLSv1.1、TLSv1.2、および TLSv1.3 をサポートしているが、TLSv1.0 はサポートしていないことを示しています。これで、クライアントが古いバージョンの TLS プロトコルのみをサポートし、トラフィックを制御する復号ポリシー ルールにアタッチされた復号プロファイルがそのバージョンを許可しないことが分かりました。

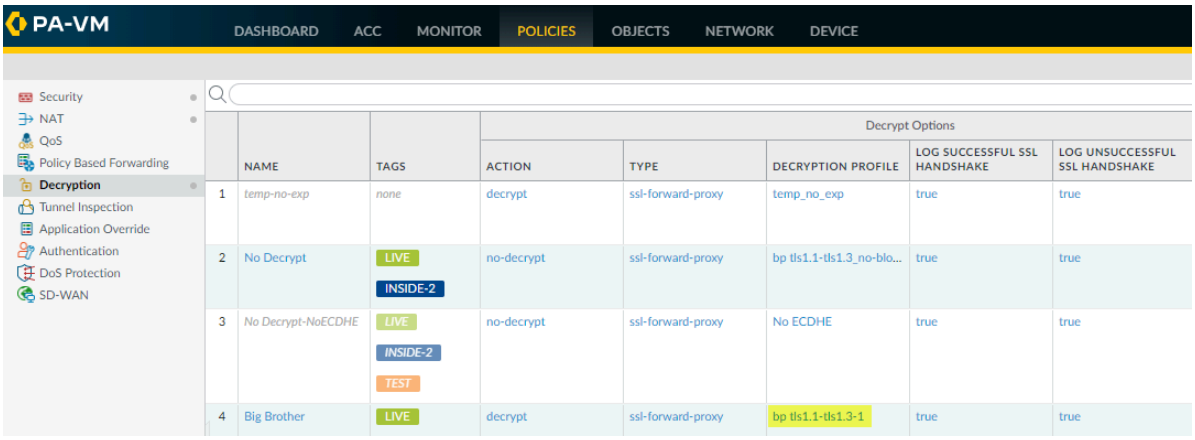
STEP 3 | 取るべきアクションを決定します。

より安全な TLS バージョンを受け入れるようにクライアントを更新できます。クライアントが何らかの理由で TLSv1.0 を必要とする場合は、ファイアウォールが引き続きトラフィックをブロックするようにするか、復号化プロファイルを更新してすべての TLSv1.0 トラフィックを許可するか (非推奨)、または復号化ポリシーを作成して TLSv1.0 を許可し、TLSv1.0 を使用する必要があり、より安全なプロトコル (トラフィックを許可するための最も安全なオプション) をサポートできないクライアントデバイスにのみ適用するプロファイルを続行できます。

STEP 4 | 復号化プロファイルの編集を選択する場合、セッション トラフィックを制御する復号ポリシーを検索するには、ログの **Policy Name (**ポリシー名**)**列を確認します (または、復号化ロ

グの横にある虫眼鏡アイコンをクリックして、詳細なログビューの全般セクションの情報を確認します)。

1. この例では、復号化ポリシー名は「Big Brother」であり、復号化プロファイルを見つけるには、**Policies (**ポリシー**)** > **Decryption (**復号化**)** に移動してから、**Decryption Profile (**復号化プロファイル**)** 列をチェックします。

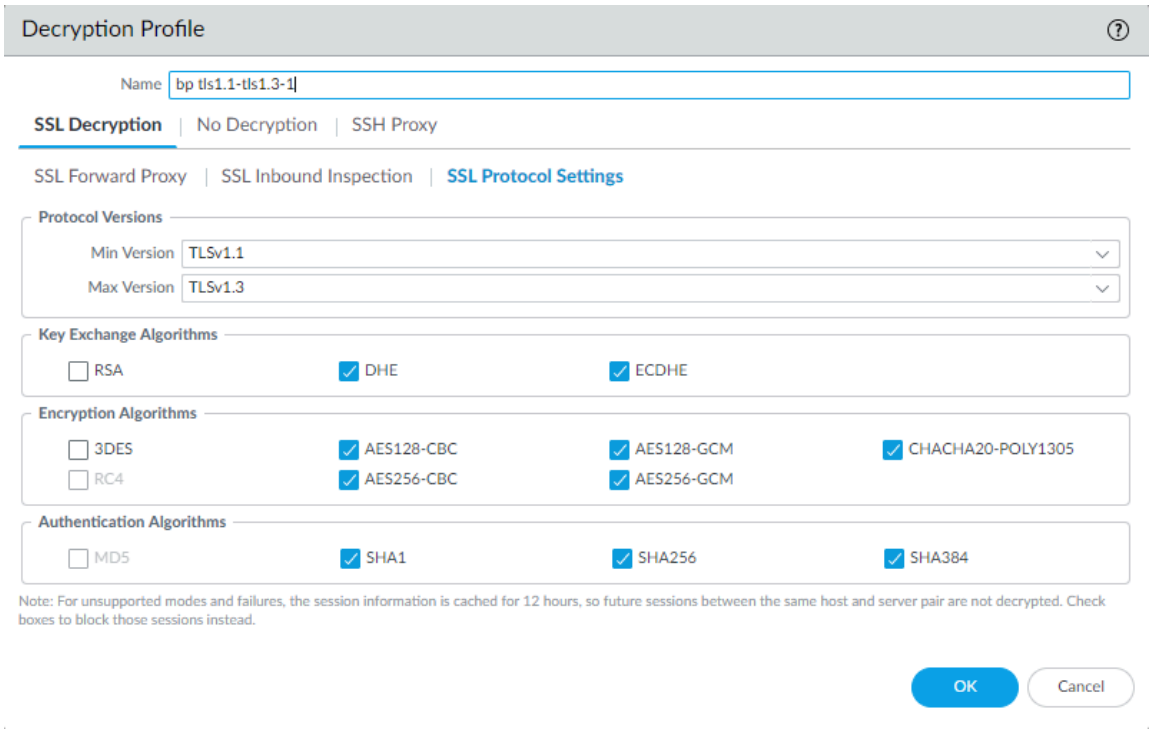


復号化プロファイル名は「**bp tls1.1-tls1.3-1**」です。「Big Brother」ポリシーを選択してから、**Options (**オプション**)** タブを選択して復号化プロファイルの名前を確認することもできます。

Objects (オブジェクト**)** > **Decryption (**復号化**)** > **Decryption Profile (**復号プロファイル**)**に移動し、適切な復号プロファイルを選択して、バージョンの問題に対処するように編集します。

2. **Objects (**オブジェクト**)** > **Decryption (**復号化**)** > **Decryption Profile**（復号プロファイル） の順に移動します。

bp tls1.1-tls1.3-1 復号化プロファイルを選択し、**SSL Protocol Settings (SSL** プロトコル設定**)** タブをクリックします。



プロファイルがサポートする最小の TLS プロトコル バージョン (**Min Version (**最小バージョン**)**) は TLSv1.1です。バージョンの不一致がブロックするトラフィックを許可するには、**Min Version (**最小バージョン**)** をTLSv1.0に変更します。しかし、より安全なオプションは、最新の TLS プロトコル バージョンを使用するようにクライアントを更新することです。クライアントを更新できない場合は、TLSv1.0トラフィックを許可する一般的な復号化ポリシーを適用する代わりに、該当のユーザー、デバイス、または送信元アドレスのみ (ならびに、ポリシーおよびプロファイルがこのトラフィックのすべてを制御するように、類似のユーザー、デバイス、または送信元アドレス) に適用される復号化ポリシーと復号化プロファイルを作成することができます。

脆弱なプロトコルと暗号スイートを識別する

脆弱な TLS プロトコルと脆弱な暗号スイート (暗号化アルゴリズム、認証アルゴリズム、鍵交換アルゴリズム、およびネゴシエートされた EC 曲線) は、セキュリティ耐性を弱め、強力な TLS プロトコルと強力な暗号スイートを使用した場合に比べて、悪意のあるユーザーによってエクスプロイトされやすくなります。

復号化ログエントリの5つのフィールドは、復号化セッションのプロトコルと暗号スイートを示します:

TLS VERSION	ENCRYPTION ALGORITHM	KEY EXCHANGE	AUTHENTICATI... ALGORITHM	NEGOTIATED EC CURVE
TLS1.2	AES_128_GCM	ECDHE	SHA256	secp256r1
TLS1.2	AES_256_GCM	ECDHE	SHA384	secp256r1

古く脆弱な TLS バージョンと暗号スイートを追跡し、セキュリティ耐性を損なう可能性のあるサーバーやアプリケーションとの接続を許可するかどうかについて、情報に基づいた決定を下せる様にします。

このトピックの例では、次の方法を示します:

- 安全性の低い TLS プロトコル バージョンを使用するトラフィックを特定する。
- 特定の鍵交換アルゴリズムを使用するトラフィックを識別する。
- 特定の認証アルゴリズムを使用するトラフィックを識別する。
- 特定の暗号化アルゴリズムを使用するトラフィックを特定する。

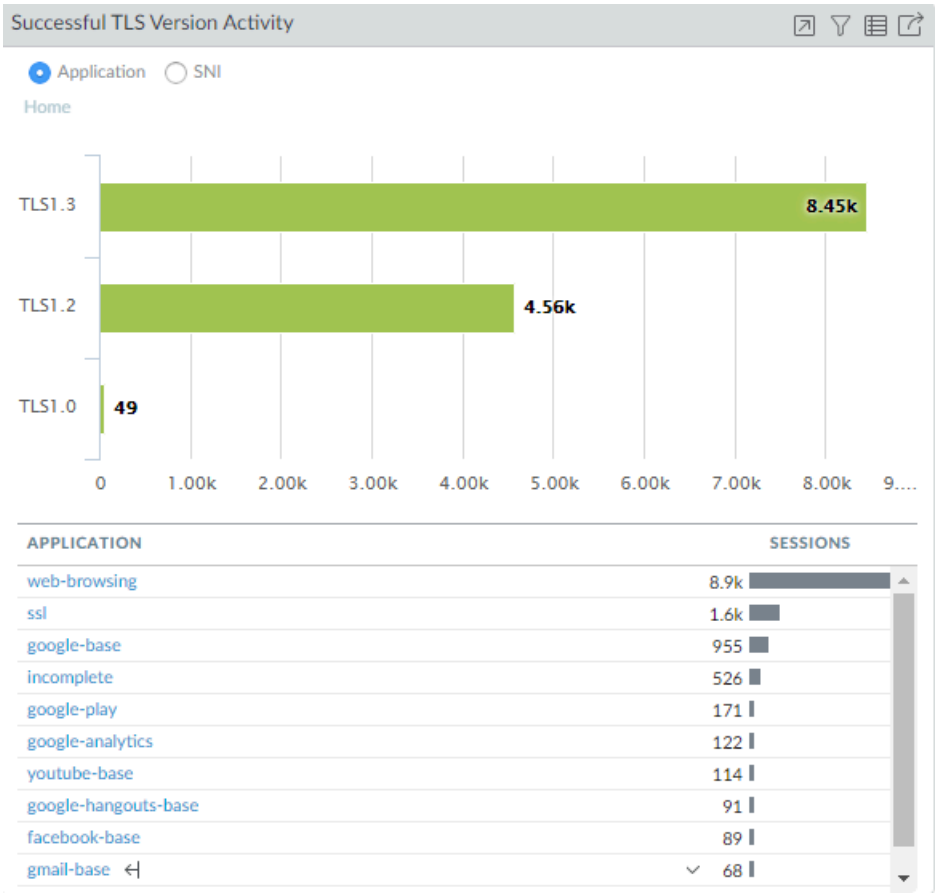
上記の例では、復号化トラブルシューティングツールをさまざまな方法で使用し、発生する可能性のある復号化の問題のトラブルシューティング方法を説明します。

Wireshark またはその他のパケットアナライザを使用し、クライアントまたはサーバーが問題を引き起こしたかどうか、*TLS* クライアントとサーバーのバージョン、およびその他の暗号スイート情報を再確認できます。このような確認は、バージョンの不一致やその他の問題の分析に有用です。

TLS Protocols (TLS プロトコル**)**—古く安全性の低いバージョンの TLS プロトコルを使用するトラフィックを特定して、脆弱なプロトコルを使用するサーバーやアプリケーションへのアクセスを許可するかどうかを評価できるようにします。

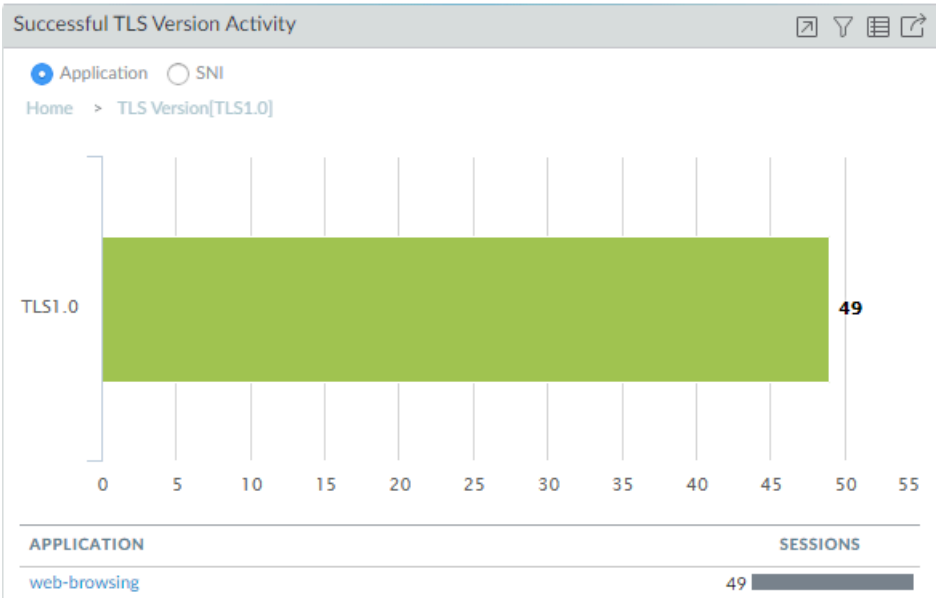
1. まず、Application Command Center (アプリケーション コマンド センター - ACC)をチェックして、ファイアウォールが脆弱なプロトコルを許可しているかどうかを確認す

るとともに (**ACC** > **SSL Activity (SSL** アクティビティ**)** > **Successful TLS Version Activity (**成功した **TLS** バージョン アクティビティ**)**)、アクティビティの全体像を取得します。



この例で成功する TLS アクティビティの大部分が TLSv1.2および TLSv1.3アクティビティです。ただし、許可された TLSv1.0トラフィックのインスタンスがいくつかあり

ます。番号**49**をクリックして、TLSv1.0アクティビティにドリルダウンし、どのアプリケーションが TLSv1.0接続を成功させているかを確認します:

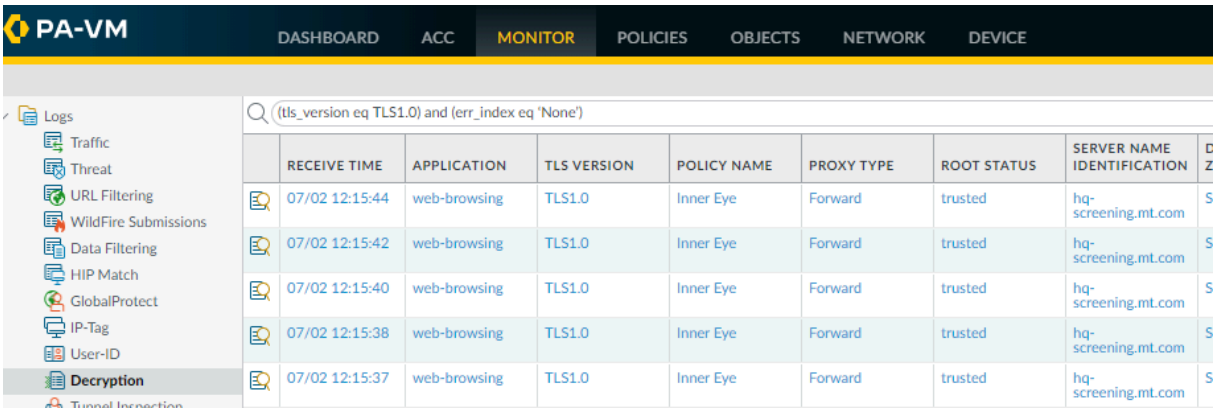


ファイアウォールが Web ブラウジングトラフィックとして識別されたトラフィックを許可していることがわかります。TLSv1.0 Web ブラウジングトラフィックとは何か、およびそれが許可される理由を理解するために、復号化ログへ移動します。

2. 復号化ログをフィルタリングして、TLSv1.0アクティビティの詳細を確認します。

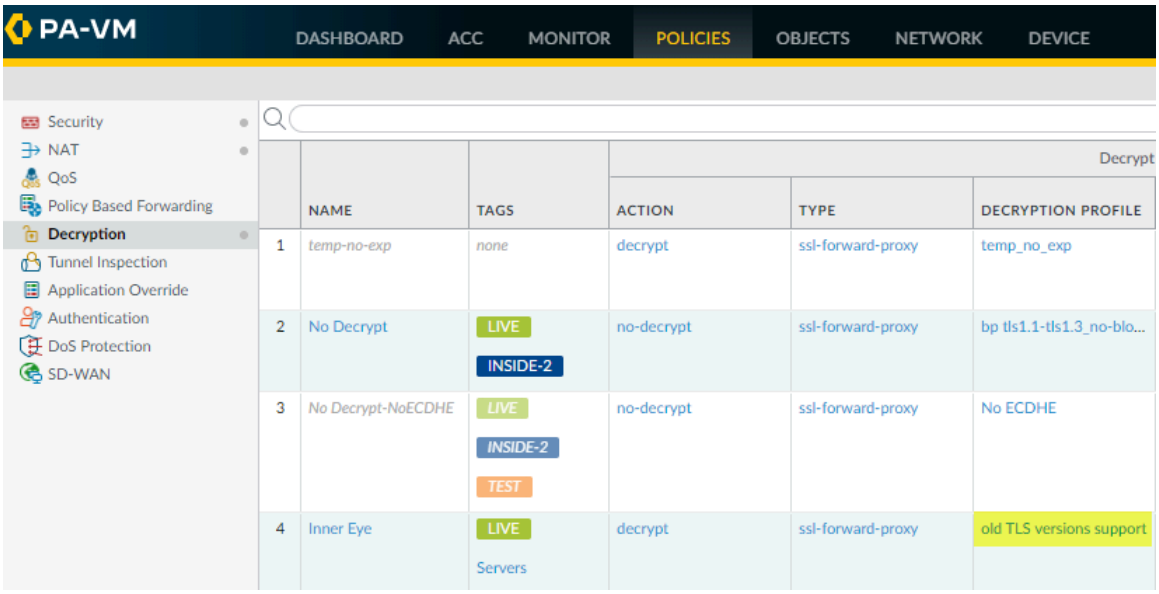
   クエリ **(tls_version eq TLS1.0)** および **(err_index eq'None')** を使用して、TLSv1.0復号化セッションが成功したことを示すログエントリを表示します。

   Decryption ログには、復号化ロギングの設定時に復号化ポリシーで成功した *TLS* ハンドシェイクのログ記録を有効にした場合にのみ、成功した *TLS* アクティビティが表示されます。成功した *TLS* ハンドシェイクのロギングが無効になっている場合、この情報を確認することはできません。（デフォルトでは無効）



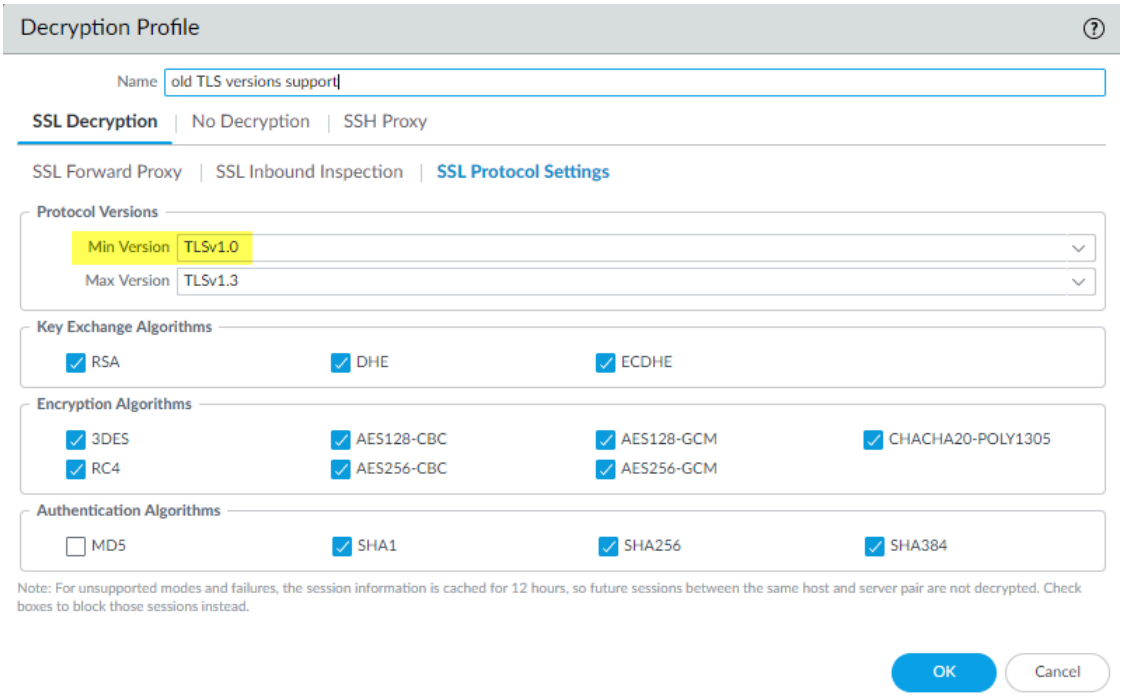
復号化ログには、トラフィックを制御する復号ポリシーの名前が「**Inner Eye**」であり、ホスト名が「**hq-screening.mt.com**」であることが示されています。これ

で、TLSv1.0を使用するサイトが分かったので、復号ポリシー (**Policies (ポリシー)** > **Decryption (復号化)**) をチェックして、トラフィックを制御する復号プロファイルを見つけ、トラフィックが許可された理由を知ることができます:



ポリシーに関連付けられている復号プロファイルは、古い **TLS** バージョンを許可していることがわかります。プロファイル (**Objects (オブジェクト)** > **Decryption (復号化)** >

Decryption Profile (復号プロファイル**)**) を表示し、SSL プロトコル設定内容を調査し、プロファイルで許可されているトラフィックを正確に確認します:



プロファイルでは TLSv1.0 トラフィックを許可しています。次の作業は、サイトへのアクセスを許可するか (ビジネス目的でアクセスする必要があるか)、それとも遮断するかを決定することです。

安全性の低いプロトコルを使用するトラフィックをファイアウォールで許可するもう1つの一般的なシナリオは、そのトラフィックが復号化されていない場合です。TLSv1.0トラフィックの復号化ログをフィルタリングするときに、**Proxy Type (**プロキシの種類**)** 列に値 **No Decrypt (**復号化なし**)** が含まれている場合、No Decryption (復号化なし) ポリシーがトラフィックを制御するため、ファイアウォールは復号化しないか、または

それを検査します。脆弱なプロトコルを許可したくない場合は、TLSv1.0トラフィックをブロックするように復号プロファイルを変更します。

復号化ログをフィルタリングして、脆弱なプロトコルを使用するアプリケーションやサイトを見つける数多く存在します。以下に例を示します:

- 成功した TLSv1.0ハンドシェークのみをフィルタリングする代わりに、クエリ **(tls_version eq TLS1.0)** を使用して、成功した TLSv1.0ハンドシェークと失敗したTLSv1.0 ハンドシェークの両方をフィルタリングする。
- クエリ **(tls_version eq TLS1.0)** および **(err_index neq 'None')** を使用して、失敗した TLSv 1.0 ハンドシェークのみをフィルタリングする。
- クエリ **(tls_version leq tls1.1)** を使用して、すべての安全性の低いプロトコル (TLSv1.1 以前のもの) をフィルタリングする。

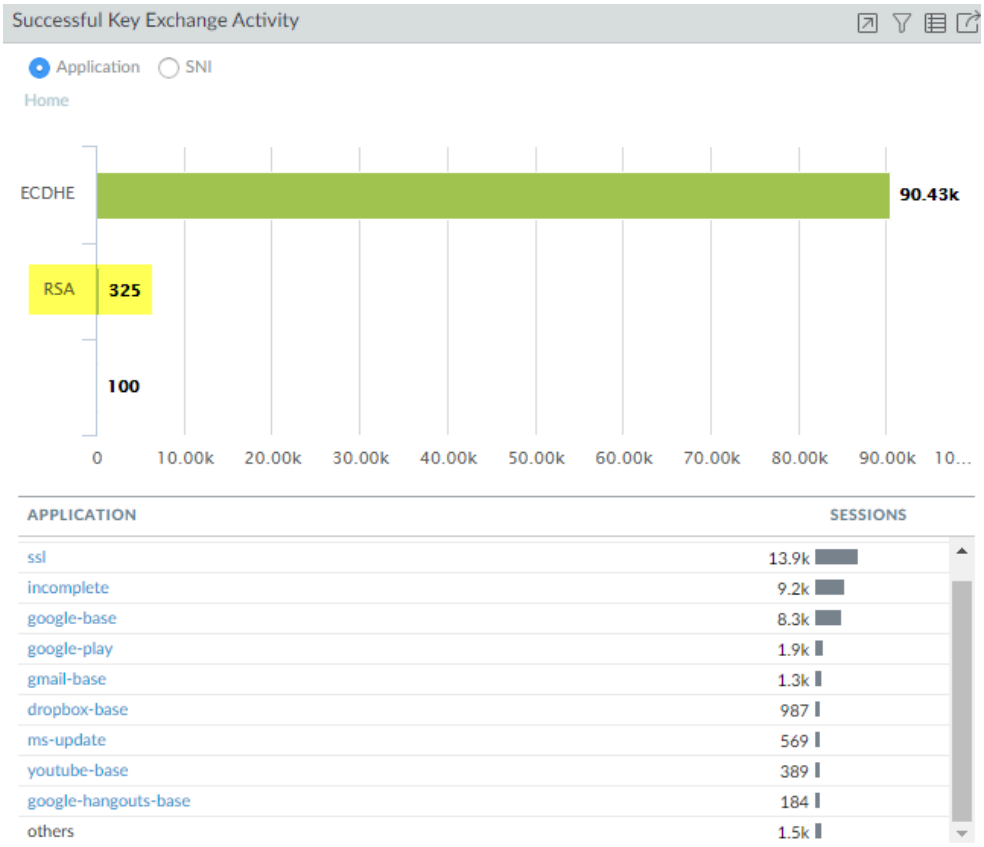
他の TLS バージョンのログをフィルタリングする場合、必要な操作は **TLS1.0** または **TLS1.1**を別の TLS バージョンに置き換えるだけです。

3. 脆弱な TLS プロトコルを使用するサイトに対して実行するアクションを決定します。
   - ビジネス目的でサイトにアクセスする必要がない場合、最も安全なアクションは、トラフィックを制御する復号ポリシーと復号プロファイルを編集して、サイトへのアクセスを遮断することです。復号化ログ **Policy Name (**ポリシー名**)** 列にはポリシー名が表示され、復号ポリシーには紐づけられた復号プロファイルが表示されます (**Options (**オプション**)**タブ)。
   - ビジネス目的でサイトにアクセスする必要がある場合は、そのサイト (またはそのサイトと他の同様のサイト) にのみ適用され、安全性の低いプロトコルを使用する他のすべてのトラフィックを遮断する復号ポリシーと復号プロファイルの作成を検討します。

Key Exchange (鍵交換**)**—安全性の低い鍵交換アルゴリズムを使用するトラフィックを特定します。

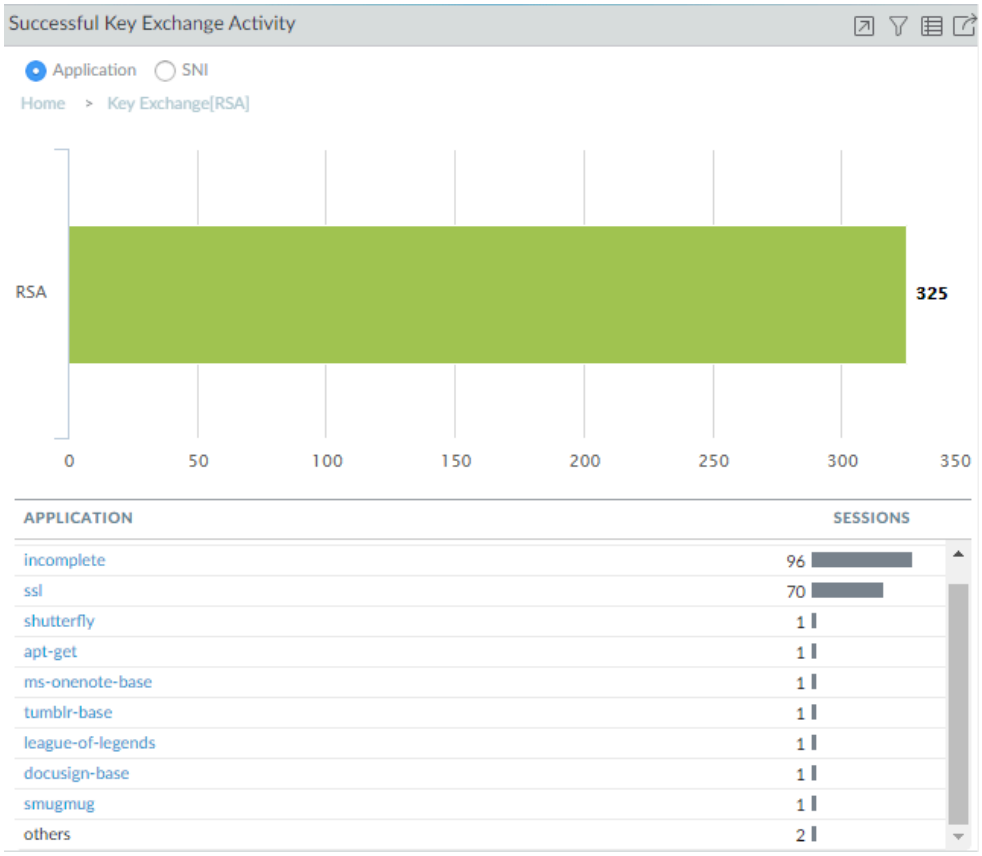
1. まず、Application Command Center (アプリケーション コマンド センター：ACC)をチェックし、ファイアウォールが許可する鍵交換アルゴリズムを確認するとともに

(**ACC** > **SSL Activity (SSL** アクティビティ**)** > **Successful Key Exchange Activity (**成功した鍵交換アクティビティ**)**)、アクティビティの全体像を把握します。

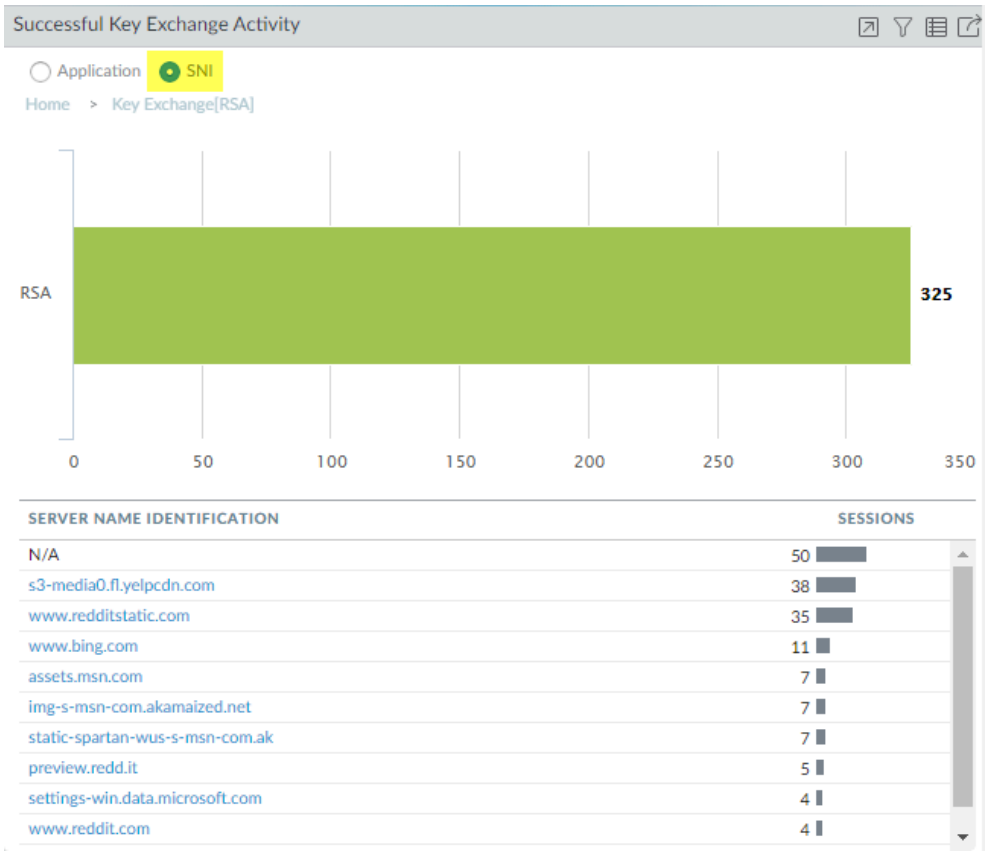


鍵交換の大部分は、安全な ECDHE 鍵交換アルゴリズムを使用しています。ただし、一部の鍵交換セッションは安全性の低い RSA アルゴリズムを使用し、一部は別の鍵アル

ゴリズムを使用します。たとえば、RSA 鍵交換を使用するトラフィックの調査を開始するには、番号**325**をクリックしてデータにドリルダウンします。



ドリルダウンすると、RSA 鍵交換を使用するアプリケーションが表示されます。**SNI** ラジオボタンをクリックして、SNI による RSA 鍵交換を表示することもできます:



この情報を利用して、ログに移動し、RSA 鍵交換の使用法に関する詳細なコンテキストを取得できます。

2. 復号化ログに移動し (**Monitor (監視)** > **Logs (ログ)** > **Decryption (復号化)**)、クエリ **(tls_keyxchg eq RSA)** を使用して RSA 鍵交換を使用する復号化セッション用にフィルタリングします:

	RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME
	06/04 09:29:50	92884	ssl	172.30.200.30	185.31.128.129	TLS1.2	None		No Decrypt
	06/04 09:29:50	92887	ssl	172.30.200.30	185.31.128.129	TLS1.2	None		No Decrypt
	06/04 09:29:44	92998	ssl	172.30.200.30	74.120.19.22	TLS1.2	None		No Decrypt
	06/04 09:29:24	92882	ssl	172.30.200.30	192.132.33.46	TLS1.2	Certificate	Expired server certificate	No Decrypt
	06/04 09:29:24	92880	ssl	172.30.200.30	192.132.33.46	TLS1.2	Certificate	Expired server certificate	No Decrypt
	06/04 09:29:23	92874	ssl	172.30.200.30	192.132.33.46	TLS1.2	Certificate	Expired server certificate	No Decrypt
	06/04 09:29:23	92873	ssl	172.30.200.30	192.132.33.46	TLS1.2	Certificate	Expired server certificate	No Decrypt
	06/03 22:30:11	36522	vudu	172.30.100.155	208.79.221.210	TLS1.2	None		Big Brother
	06/03 20:08:57	16896	ssl	172.30.200.30	66.117.28.86	TLS1.2	None		No Decrypt
	06/03 20:08:22	16947	ssl	172.30.200.30	185.31.128.129	TLS1.2	None		No Decrypt

ログの **Policy Name (ポリシー名)** 列から、 **No Decrypt (復号なし)** 復号ポリシーが、RSA 鍵交換を使用する大半のトラフィックを制御することが分かり、ファイア

ウォールがトラフィックを復号化せず、検査なしで許可していることが推測できます。トラフィックは復号化されていないため、ファイアウォールはアプリケーションを識別できず、**ssl** として識別します。RSA 鍵交換を使用するトラフィックを許可しない場合、トラフィックを制御する復号ポリシーに紐づけられている復号プロファイルを変更します。

クエリに追加して、ACC または最初の復号化ログ クエリで表示された特定の SNI またはアプリケーションの結果をさらにフィルタリングできます。

3. 安全性の低い鍵交換アルゴリズムを使用するトラフィックに対して実行するアクションを決定します。

   ビジネス目的でアクセスする必要がない限り、安全性の低い鍵交換プロトコルを使用するサイトへのアクセスを遮断します。こうしたサイトに対しては、そのサイト (またはそのサイトと他の同様のサイト) にのみ適用され、安全性の低い鍵交換アルゴリズムを使用する他のすべてのトラフィックを遮断する復号ポリシーと復号プロファイルを作成することを検討します。

復号化ログを使用して、安全性の低い古い認証アルゴリズムを使用するセッションを特定します。

復号化ログをフィルタリングし、安全性の低い古い認証アルゴリズムを特定します。

たとえば、SHA1アルゴリズムを使用するすべてのセッションを識別するには、クエリ **(tls_auth eq SHA)** を使用します:

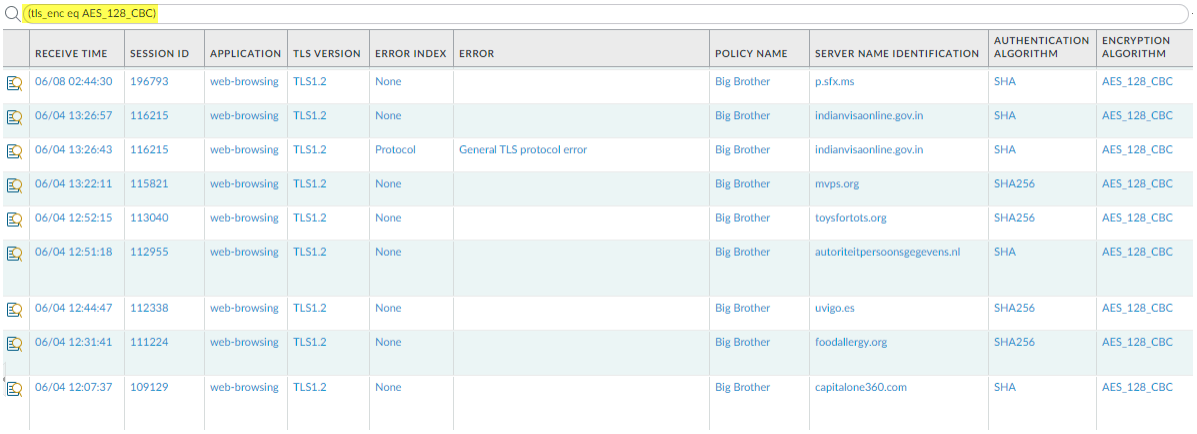

(tls_auth eq SHA)

	RECEIVE TIME	SESSION ID	APPLICATION	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME	SERVER NAME IDENTIFICATION	AUTHENTICATION ALGORITHM
	06/08 23:12:02	213635	ssl	TLS1.2	None		No Decrypt		SHA
	06/08 11:16:02	203438	incomplete	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 11:16:02	203439	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 11:15:01	203437	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 02:45:32	196795	incomplete	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 02:44:30	196794	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/08 02:44:30	196793	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA
	06/04 13:38:36	117329	web-browsing	TLS1.2	None		Big Brother	inegi.org.mx	SHA
	06/04 13:35:01	116980	web-browsing	TLS1.2	None		Big Brother	rupress.org	SHA

クエリに追加して、結果をさらにドリルダウンできます。たとえば、特定の SNI、鍵交換バージョン (RSA 鍵交換も使用する SHA1セッションのフィルタリングなど）、TLS バージョン、または復号化ログ列にあるその他の項目を追加できます。

復号化ログを使用して、特定の暗号化アルゴリズムを使用するセッションを識別します。

たとえば、AES-128-CBC 暗号化アルゴリズムを使用するすべてのセッションを識別するには、クエリ **(tls_enc eq AES_128_CBC)** を使用します:


(tls_enc eq AES_128_CBC)

	RECEIVE TIME	SESSION ID	APPLICATION	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME	SERVER NAME IDENTIFICATION	AUTHENTICATION ALGORITHM	ENCRYPTION ALGORITHM
	06/08 02:44:30	196793	web-browsing	TLS1.2	None		Big Brother	p.sfx.ms	SHA	AES_128_CBC
	06/04 13:26:57	116215	web-browsing	TLS1.2	None		Big Brother	indianvisaonline.gov.in	SHA	AES_128_CBC
	06/04 13:26:43	116215	web-browsing	TLS1.2	Protocol	General TLS protocol error	Big Brother	indianvisaonline.gov.in	SHA	AES_128_CBC
	06/04 13:22:11	115821	web-browsing	TLS1.2	None		Big Brother	mvps.org	SHA256	AES_128_CBC
	06/04 12:52:15	113040	web-browsing	TLS1.2	None		Big Brother	toysfortots.org	SHA256	AES_128_CBC
	06/04 12:51:18	112955	web-browsing	TLS1.2	None		Big Brother	autoriteitpersoonsgegevens.nl	SHA	AES_128_CBC
	06/04 12:44:47	112338	web-browsing	TLS1.2	None		Big Brother	uvigo.es	SHA256	AES_128_CBC
	06/04 12:31:41	111224	web-browsing	TLS1.2	None		Big Brother	foodallergy.org	SHA256	AES_128_CBC
	06/04 12:07:37	109129	web-browsing	TLS1.2	None		Big Brother	capitalone360.com	SHA	AES_128_CBC

クエリに追加して、結果をさらにドリルダウンできます。

他の古い暗号化アルゴリズムを見つけるためのクエリの例は次のとおりです: **(tls_enc eq DES_CBC)**、**(tls_enc eq 3DES_EDE_CBC)**、および**(tls_enc eq DES40_CBC)**。

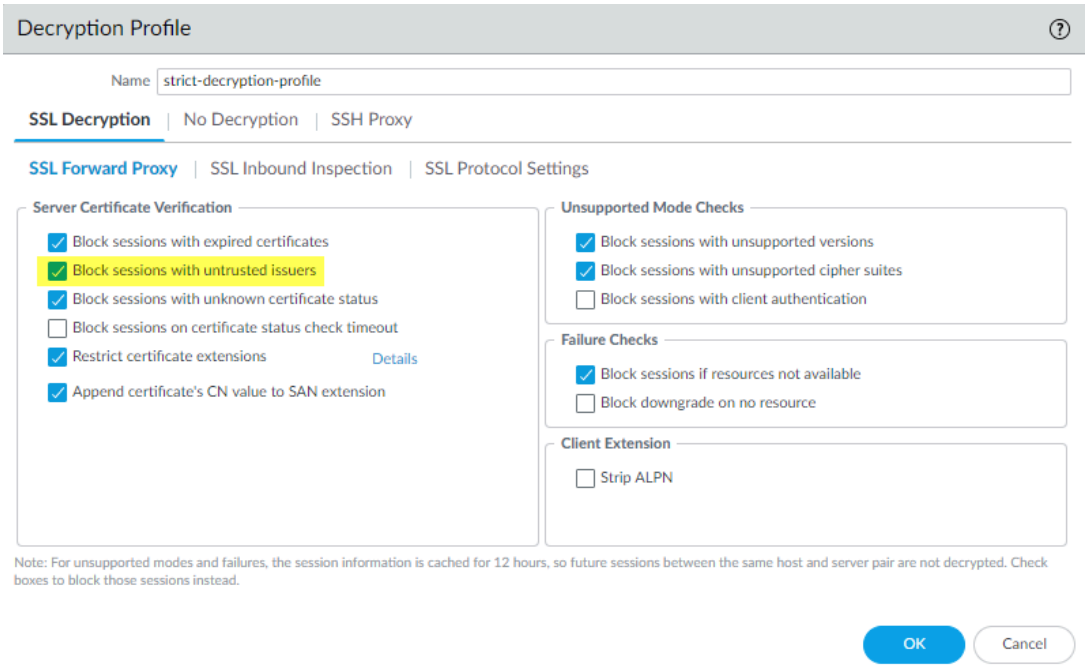
この方法とログ フィルタ ビルダーを使用して、ネゴシエートされた ECC 曲線や復号化ログにあるその他の情報を調査するためのクエリを作成します。

信頼されていない CA 証明書を識別する

信頼されていないCA 証明書を含むサイトは中間者攻撃、リプレイ攻撃、またはその他の悪意のあるアクティビティを示す可能性があるため、信頼されていない CA 証明書と、信頼されていないルートCA によって自己署名された証明書を含むサイトへのアクセスをブロックすることは、ベストプラクティスとなっています。

STEP 1 | 信頼されていない CA を含むサイトをブロックするために、フォワード プロキシ復号プロファイル内で **Block sessions with untrusted issuers (**発行者が信頼されていないセッション

をブロック) を実行していることを確認します (**Objects (オブジェクト)** > **Decryption (復号化)** > **Decryption Profiles (復号プロファイル)**)。



復号プロファイル内で信頼されていない発行者とのセッションをブロックすると、復号化ログ (**Monitor (監視)** > **Logs (ログ)** > **Decryption (復号化)**) はエラーをロギングします。

STEP 2 | ログをフィルタリングし、 クエリ**(error eq 'Untrusted issuer CA')**を使用して証明書が取り消されたために失敗したセッションを特定します。

(error eq 'Untrusted issuer CA')

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	POLICY NAME	SERVER NAME IDENTIFICATION
06/04 13:43:07	117709	ssl	172.30.100.155	184.172.23.30	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	dealscove.com
06/04 13:35:38	117074	ssl	172.30.100.155	204.236.227.206	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	foxsearchlight.com
06/04 13:17:10	115350	incomplete	172.30.100.155	69.163.152.152	TLS1.3	Certificate	Untrusted issuer CA	Big Brother	famfamfam.com
06/04 13:07:18	114451	ssl	172.30.100.155	52.209.190.138	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	bbva.com
06/04 12:52:46	113115	ssl	172.30.100.155	204.108.65.8	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	lausd.net
06/04 12:39:10	111870	ssl	172.30.100.155	34.90.228.231	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	dumpert.nl
06/04 12:23:05	110460	incomplete	172.30.100.155	75.119.204.133	TLS1.3	Certificate	Untrusted issuer CA	Big Brother	any.do
06/04 12:16:02	109894	ssl	172.30.100.155	217.21.43.35	TLS1.2	Certificate	Untrusted issuer CA	Big Brother	bsu.by
06/04 11:56:42	108205	incomplete	172.30.100.155	45.223.17.206	TLS1.3	Certificate	Untrusted issuer CA	Big Brother	imss.gob.mx

STEP 3 | (任意) Qualys SSL Labs サイトで証明書の有効期限日をダブルチェックします。

該当のホストの証明書情報を表示するには、**Hostname (ホスト名)** フィールドでサーバーのホスト名を入力し (復号化ログの **Server Name Identification (サーバー名識別情報)** 列)、**Submit (送信)** します。

有効期限切れの証明書のトラブルシューティングを実行

復号のベストプラクティスに従って、フォワードプロキシ復号プロファイル内またはNo Decryption(復号なし)のプロファイルで**Block sessions with expired certificates (**期限切れ証明書のセッションをブロック**)** を行った後、サーバーが期限切れの証明書を提示すると、ファイアウォールがセッションをブロックします。ただし、ビジネス上の理由でアクセスする必要のあるサイトで証明書の有効期限が切れると、そのサイトへの接続がブロックされ、理由が分からない場合があります。

復号ログを使用して、期限切れの証明書を確認したり、間もなく期限切れになる証明書を確認したりできるため、状況を把握して適切なアクションを実行できます。

STEP 1 | クエリ **(error eq 'Expired server certificate')** を使用して、証明書の期限切れエラーを見つけるため、復号ログをフィルタリングします。

(error eq 'Expired server certificate')

RECEIVE TIME	SESSION ID	APPLICATION	SOURCE ADDRESS	DESTINATION ADDRESS	TLS VERSION	ERROR INDEX	ERROR	SERVER NAME IDENTIFICATION	POLICY NAME
06/04 16:19:49	121352	incomplete	172.30.100.10	34.225.62.221	TLS1.3	Certificate	Expired server certificate	www.stanford.edu	Big Brother
06/04 13:43:26	117747	incomplete	172.30.100.155	104.197.149.89	TLS1.3	Certificate	Expired server certificate	phone.com	Big Brother
06/04 13:41:03	117572	incomplete	172.30.100.155	208.117.9.16	TLS1.3	Certificate	Expired server certificate	netcarshow.com	Big Brother
06/04 13:38:51	117379	ssl	172.30.100.155	69.172.200.184	TLS1.2	Certificate	Expired server certificate	royal.gov.uk	Big Brother
06/04 13:36:27	117150	ssl	172.30.100.155	107.21.104.61	TLS1.2	Certificate	Expired server certificate	www.uthscsa.edu	Big Brother
06/04 13:34:53	117004	incomplete	172.30.100.155	66.115.56.251	TLS1.3	Certificate	Expired server certificate	gunsamerica.com	Big Brother
06/04 13:33:17	116853	incomplete	172.30.100.155	34.107.140.234	TLS1.3	Certificate	Expired server certificate	skiplagged.com	Big Brother
06/04 13:32:45	116798	ssl	172.30.100.155	104.236.4.58	TLS1.2	Certificate	Expired server certificate	uploading.com	Big Brother
06/04 13:31:28	116655	incomplete	172.30.100.155	35.186.201.59	TLS1.3	Certificate	Expired server certificate	shared.com	Big Brother
06/04 13:29:32	116507	ssl	172.30.100.155	147.139.136.53	TLS1.2	Certificate	Expired server certificate	beautynesia.id	Big Brother
06/04 13:28:56	116426	incomplete	172.30.100.155	45.55.105.190	TLS1.3	Certificate	Expired server certificate	designbundles.net	Big Brother

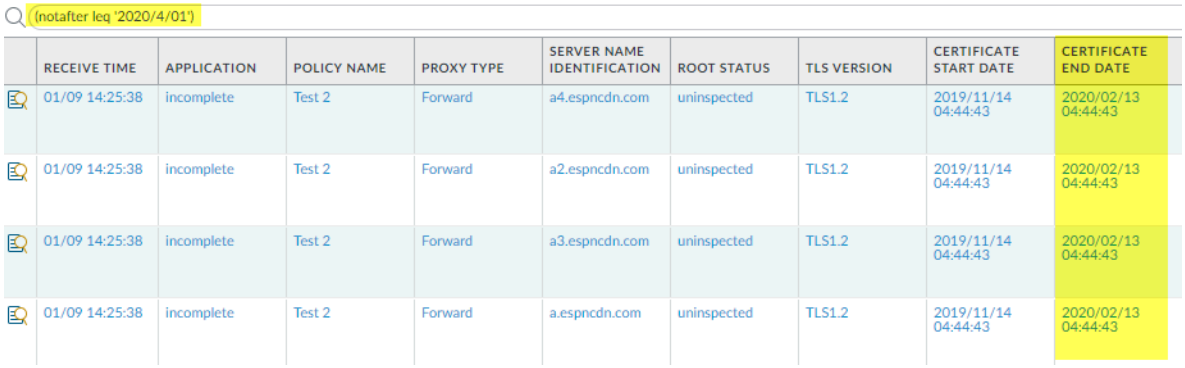
このクエリは、`Expired server certificate`(期限切れのサーバー証明書) エラーを生成するサーバーを識別します。ファイアウォールは、証明書が期限切れであることを理由に、これらのサーバーへのアクセスをブロックします。

STEP 2 | (オプション) Qualys SSL Labs サイトで証明書の有効期限日をダブルチェックします。

該当のホストの証明書情報を表示するには、**Hostname (**ホスト名**)** フィールドでサーバーのホスト名を入力し (復号ログの **Server Name Identification (**サーバー名識別情報**)** 列)、**Submit (**送信**)** します。

STEP 3 | 間もなく期限切れとなる証明書の終了日をクエリを使用して特定するため、復号ログ (**Monitor (監視)** > **Logs (ログ)** > **Decryption (復号)**) をフィルタリングします。

例えば、本日が2020年2月1日であり、サイトが証明書を更新しない場合に備えて、評価と準備に2か月を設けたい場合は、2020年4月1日以前に有効期限が切れる復号ログをクエリします (**notafter leq '2020/4/01'**):



Certificate End Date(証明書の終了日) 列には、Certificate（証明書）の有効期限が切れる正確な日付が表示されます。

STEP 4 | 証明書の有効期限が切れているサイトに対して実行するアクションを決定します。

- ビジネス目的でサイトにアクセスする必要がない場合、最も安全なアクションは、サイトへのアクセスを引き続きブロックすることです。
- ビジネス目的でサイトにアクセスする必要がある場合は、以下のいずれかのアクションを実行します:
  - 期限切れの証明書を使用しているサイトの管理者に連絡し、証明書を更新または書き換えする必要があることを通知する。
  - ビジネス目的で必要な期限切れの証明書を持つサイトにのみ適用される復号ポリシーと、期限切れの証明書を持つサイトを許可する復号プロファイルを作成する。ビジネス目的で不要なサイトにはポリシーを適用しないこと。サイトが証明書を更新したら、ポリシーから削除する。

失効した証明書のトラブルシューティングを実行

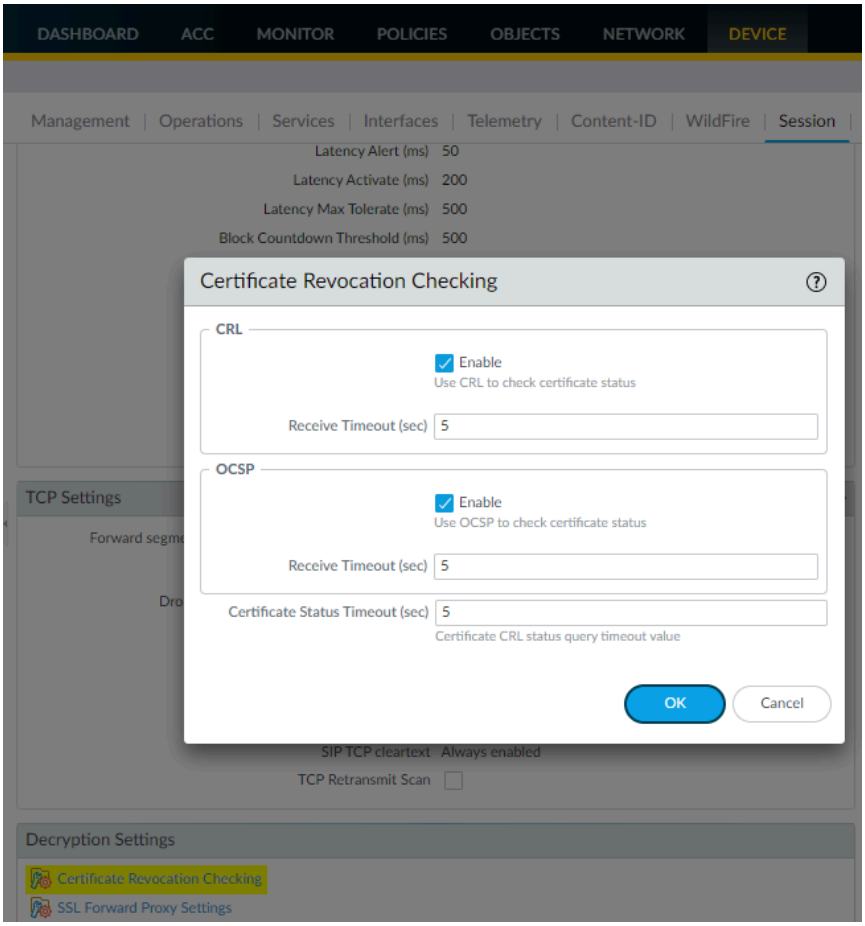
失効した証明書は有効ではありません。これは、サイトにセキュリティ上の問題があり、その証明書が信頼できないことを示している可能性があります。しかし、証明書が取り消される理由には害のないものもあります。

失効した証明書を信頼しないでください。証明書失効チェックを有効にして、失効した証明書を持つサイトへのアクセスを拒否します。

失効した証明書を使用してセッションをドロップし、失効した証明書のトラブルシューティングを行うには、証明書失効チェックを有効にする必要があります。証明書の失効チェックを有効にしないと、ファイアウォールは失効した証明書をチェックせず、サイトに失効した証明書があるかどうかがわかりません。

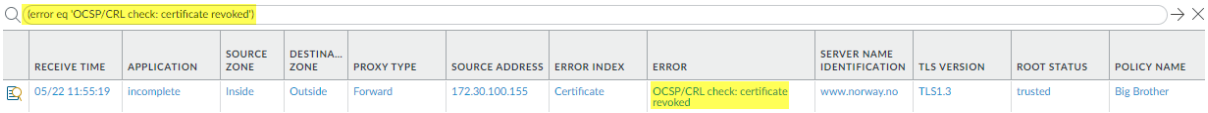
STEP 1 | 証明書失効チェックをまだ有効にしていない場合は、有効にします。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** > **Decryption Settings (復号設定)** に移動します。
2. OCSP および CRL 両方の証明書チェックを有効にします。



フォワードプロキシ復号プロファイルで**Block sessions on certificate status check timeout (証明書ステータス チェック タイムアウトのセッションをブロック)**が5秒では十分な時間がなく、タイムアウトによってブロックされるセッションが多すぎる可能性がある場合は、**Receive Timeout (sec) (受信タイムアウト（秒）)**をより長い時間に設定します。

STEP 2 | クエリ **(error eq 'OCSP/CRL check: certificate revoked')** を使用して証明書失効エラーを見つけるため、復号ログ (**Monitor (監視)** > **Logs (ログ)** > **Decryption (復号)**) をフィルタリングします。



STEP 3 | (オプション) Qualys SSL Labs サイトで証明書の有効期限日をダブルチェックします。

該当のホストの証明書情報を表示するには、**Hostname (ホスト名)** フィールドでサーバーのホスト名を入力し (復号化ログの **Server Name Identification (サーバー名識別情報)** 列)、**Submit (送信)** します。

ピン留めされた証明書のトラブルシューティングを実行

証明書のピン留めは、クライアントアプリケーションにサーバの証明書を既知のコピーと照合して検証させ、証明書が本当にサーバからのものであることを保証します。証明書をピン留めする目的は、クライアントとサーバー間のデバイスがサーバー証明書を別の証明書に置き換えるman-in-the-middle(仲介者- MITM) 攻撃から保護することです。

これにより、悪意のある攻撃者が接続を傍受して操作することは防止されますが、ファイアウォールがサーバー証明書の代わりに偽装証明書を作成してクライアントに提示するため、フォワードロキシ復号化も防ぐことができます。クライアントとサーバーを直接接続する1つのセッションの代わりに、フォワードプロキシは2つのセッションを作成します。1つはクライアントとファイアウォールの間、もう1つはファイアウォールとサーバーの間に作られます。これにより、クライアントとの信頼が確立され、ファイアウォールがトラフィックを復号して検査できるようになります。

ただし、証明書がピン留めされている場合、クライアントはファイアウォールの偽装証明書を受け入れないため、ファイアウォールはトラフィックを復号化できません – クライアントは、アプリケーションに固定されている証明書のみを受け入れます。

STEP 1 | 復号化ログ (**Monitor (監視)** > **Logs (ログ)** > **Decryption (復号化)**) をフィルタリングして、クエリ **(error contains 'UnknownCA')** を使用するピン留めされた証明書を探します。

(error contains 'UnknownCA')

	RECEIVE TIME	APPLICATION	PROXY TYPE	SOURCE ADDRESS	ERROR INDEX	ERROR	SERVER NAME IDENTIFICATION	TLS VERSION	POLICY NAME
	06/02 11:25:30	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
	06/02 11:16:53	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	telemetry.dropb...	TLS1.2	Big Brother
	06/02 11:15:52	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	dl-debug.dropbox.c...	TLS1.2	Big Brother
	06/02 11:15:52	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	dl-debug.dropbox.c...	TLS1.2	Big Brother
	06/02 11:09:03	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
	06/02 11:09:03	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother
	06/02 10:51:34	incomplete	Forward	172.30.115.10	Certificate	Received fatal alert UnknownCA from client. CA Issuer URL: h	d.dropbox.com	TLS1.2	Big Brother

アプリケーションは、サーバーの証明書の検証に失敗すると、TLS エラーコード (アラート) を生成します。アプリケーションが異なると、ピン留めされた証明書を示すために異なるエラーコードを使用する可能性があります。固定された証明書の最も一般的なエラー インジケータは、「UnknownCA」と「BadCertificate」です。より多くのピン留めされた証明書エ

ラーを探すには、**(error contains 'UnknownCA')** クエリの実行後、クエリ **(error contains 'BadCertificate')** を実行します。

Wireshark または他のパケット アナライザを使用して、エラーを再確認できます。*TLS* ハンドシェークの直後に接続を切断しているクライアントを探して、それがピン留めされた証明書の問題であることを確認します。

STEP 2 | ピン留めされた証明書の処理方法を決定します。

ビジネス目的でアクセスする必要がない場合は、ファイアウォールで引き続きアクセスをブロックできます。アクセスが必要な場合は、SSL 復号化除外リスト (**Device (デバイス)** > **Certificate Management (証明書管理)** > **SSL Decryption Exclusion (SSL復号化除外)**) に追加することで 技術的な理由でサーバーを復号化から除外実行できます。

ファイアウォールは、SSL復号化除外リストにあるサイトの復号化をバイパスします。ファイアウォールはトラフィックを検査できませんが、トラフィックは許可されます。

復号化機能の無料ライセンスをアクティベート

SSH トラフィック および SSL トラフィック (SSL インターネット トラフィック または SSL トラフィックを内部サーバー に復号化する場合は、ライセンスは必要ありません。ただし、復号ミラーリングを有効にするには、無料ライセンスをアクティブ化する必要があります。無料ライセンス要件により、この機能は、承認された担当者が故意に関連するライセンスをアクティブ化した後にのみ使用できます。

PAN-OS 10.1 では、復号化されたブローカー機能とフリー ライセンスがネットワーク パケット ブローカに置き換えられました (Networking 管理者ガイド) は、暗号化解除された *TLS* トラフィックと *TLS* 以外のトラフィックにブローカーの機能を拡張します。ネットワーク パケット ブローカー ライセンス も、カスタマー サポート ポータル からダウンロードおよびインストールできます。

Palo Alto Networks カスタマー サポート ポータルで次の手順を実行して、復号ミラーリング機能ライセンスをアクティブ化します。

STEP 1 | カスタマーサポート ポータルにログインします。

STEP 2 | 左側のナビゲーション ペインで**Assets (アセット)** > **Devices (デバイス)**を選択します。

STEP 3 | 復号化ポートのミラーリングを有効にするデバイスを探し、[**Actions** (鉛筆アイコン) を選択します。

STEP 4 | Activate Licenses（アクティブなライセンス）で、**Activate Feature License**（機能ライセンスの有効化）を選択します。

STEP 5 | 無料ライセンスを有効にする機能を選択します。復号化ポート ミラー

STEP 6 | 同意して提出。

STEP 7 | ファイアウォールに復号化ミラーリング ライセンスをインストールします。

1. **Device** > **Licenses (デバイス > ライセンス)**を選択します。
2. **Retrieve license keys from license server**（ライセンス サーバーからライセンス キーを取得）をクリックします。
3. **Decryption** ポート ミラー ライセンスがファイアウォールでアクティブになっていることを確認します。
4. ファイアウォールを再起動します（**Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)**）。暗号化解除ポートのミラーリングは、ファイアウォールがリロードされるまで構成に使用できません。

URL フィルタリング

Palo Alto Networks URLフィルタリングソリューションを使用すると、ユーザーがアクセスできるサイトを監視および制御し、ユーザーが有効な企業資格情報を送信できるサイトを制御することでフィッシング攻撃を防止し、GoogleやBingなどの検索エンジンの安全な検索を強制できます。

Palo Alto Networks URL Filteringソリューションについて

Palo Alto Networks URLフィルタリングソリューションであるAdvanced URL Filteringは、ユーザーがWebに安全にアクセスできるようにすることで、Webベースの脅威からネットワークを保護するサブスクリプションサービスであり、詳細なポリシーコントロールを提供して、オンラインコンテンツの対話方法とアクセス方法を正確に定義します。Advanced URL Filtering サブスクリプションは、URL 分類データベースを提供することにより、従来の URL Filtering サブスクリプションによって提供されるすべての機能を提供すると同時に、インライン ML ベースの Web セキュリティ エンジンを使用して回避的で未知の Web 脅威を防止する完全な Web コンテンツ検査という追加の利点ももたらします。

従来の ***URL Filtering*** サブスクリプション所有者は、ライセンス期間が終了するまで ***URL*** フィルタリング展開を引き続き使用できます。

URL カテゴリ、ユーザー、およびグループに基づいてサイトへのアクセスを制限するポリシー ルールを作成できます。(Advanced URL Filtering サブスクリプションを活用して組織の Web セキュリティ ニーズを満たすさまざまな方法については、「」を参照してください)。

Advanced URL Filtering を有効にすると、URL 要求は次のようになります。

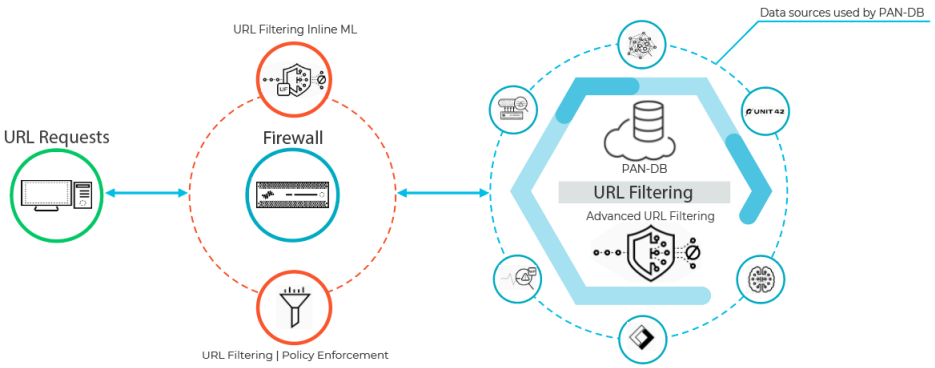
- 分類された何百万ものウェブサイトを含むPAN-DB URLデータベースと比較します。これらの URL カテゴリは、URL フィルタリング プロファイルで使用するか、一致条件として使用してセキュリティ ポリシーを適用できます。また、URLフィルタリングを使用して、ユーザーに安全な検索設定を適用したり、URL カテゴリに基づいて認証情報盗難の阻止を行ったりすることも可能です。
- クラウドベースのAdvanced URL Filtering検出モジュールを使用してリアルタイムで分析され、URLフィルタリングデータベースに現在存在しない新しい未知の脅威に対する保護を提供します。
- 未知の悪意のある Web ページをリアルタイムでブロックできる firewall ベースの分析ソリューションである local インライン分類 を使用して、フィッシングと悪意のある JavaScript がないか検査。

企業のネットワーク セキュリティ要件によって firewall によるインターネットへの直接アクセスが禁止されている場合、Palo Alto Networks は ***PAN-DB Private Cloud*** を備えたオフライン URL フィルタリング ソリューションを提供します。これにより、ネットワーク内の PAN-DB サーバーとして機能する 1 つ以上の M-600 アプライアンスに PAN-DB プライベートクラウドをデプロイできます。ただし、Advanced URL Filtering ソリューションにあるクラウドベースの URL 分析機能はサポートしていません。

アドバンスドURLフィルタリングの仕組み

アドバンスドURLフィルタリングは、サイトのコンテンツ、機能、および安全性に基づいて Web サイトを分類します。URL には、サイトが脅威にさらされる可能性を示すリスクカテゴリ（高、中、低）を含む最大 4 つの URL カテゴリを含めることができます。アドバンストURLフィルタリングのURLデータベースであるPAN-DBがサイトを分類するため、アドバンストURLフィルタリングを有効にしたファイアウォールはその知識を活用して、組織のセキュリティポリシーを実施することができます。PAN-DB データベースによって提供される保護に加えて、PAN-DBデータベースによる防御に加え、アドバンストURLフィルタリングでは、機械学習を用いたリアルタイム分析により、新しい脅威や未知の脅威に対する防御を実現します。これにより、URL フィルタリング データベースがコンテンツを分析して追加する機会が得られ、攻撃者が精密攻撃キャンペーンを開始できるオープン期間が提供される前に更新または導入された悪意のある URL に対する保護が提供されます。アドバンストURLフィルタリングは、リクエストごとにリアルタイムでURLを分析することで、データベースソリューションに特有のカバレッジのギャップを補います。高度な URL フィルタリングで使用される ML ベースのモデルは、さまざまな悪意のある URL、フィッシング Web ページ、および C2 を検出するために、トレーニングが行われ、継続的に更新されています。

特定の高度な脅威の存在を示すWebサイトは、クラウドベースのインライン深層学習システムで追加処理され、アドバンスドURLフィルタリングで使用されるMLモデルを補完するディテクターとアナライザーを介して処理されます。ディープラーニングによる検知は、より大きなデータセットを処理することができ、多層のニューラルネットワークによって、複雑な悪意のあるパターンや行動をよりよく識別することができます。アドバンストURLフィルタリングは、疑わしいWebリクエストを受信した際に、ファイアウォールからHTTPレスポンスデータを受け取ると、そのデータをさらにディープラーニングディテクターで分析し、回避的なゼロデイWeb攻撃に対するインライン防御を提供します。これには、未知のWebサイトからWebページのコンテンツを不正に取得するクローキングWebサイトが含まれます。具体的には、URLデータベースが対応できない悪意のあるコンテンツ、多段階攻撃、CAPTCHAチャレンジ、以前は見られなかったワンタイムURLなどが含まれます。回避可能な悪意のあるWebサイトは常に流動的であるため、Webサイトの分類に使用されるディテクターとアナライザーは、パロアルトネットワークスの脅威研究者が検出ロジックを改善する際に自動的に更新・展開され、管理者は更新パッケージをダウンロードする必要はありません。



ユーザーが Web ページを要求すると、ファイアウォールはユーザーが追加した例外と、サイトのリスク カテゴリの PAN-DB を照会します。PAN-DBは、ユニット42、ワイルドファイ

ア、パッシブDNS、Palo Alto Networksテレメトリデータ、サイバー脅威同盟からのデータからのURL情報を使用し、カテゴリを決定するために様々なアナライザを適用します。URLに危険性や悪意のある特徴が見られる場合は、Webペイロードデータもクラウド上のアドバンストURLフィルタリングに送信してリアルタイムに解析し、追加の解析データを生成しています。その結果生じるリスク カテゴリはファイアウォールによって取得され、ポリシー構成に基づいて Web アクセス ルールを適用するために使用されます。さらに、ファイアウォールは新しいエントリのサイトのカテゴリ情報をキャッシュして、以降の要求に対して高速に取得できるようにしますが、ユーザーが最近アクセスしていない URL を削除して、ネットワーク内のトラフィックを正確に反映します。また、PAN-DB クラウド クエリに組み込まれているチェック機能により、ファイアウォールが最新の URL 分類情報を確実に受信するようにします。インターネットに接続されていない場合、またはURLフィルタリングライセンスが有効でない場合、PAN-DBへの問い合わせは行われません。

firewall は、Web サイトの URL カテゴリを、1) カスタム URL カテゴリ、2) 外部動的リスト (EDL)、および 3) 定義済みURLカテゴリのエントリと比較し、優先順位をつけてウェブサイトのURLカテゴリを決定します。

データプレーンで機械学習を使用して URL をリアルタイムで分析するように設定されたファイアウォールは、フィッシング Web サイトや JavaScript のエクスプロイトに対するセキュリティの追加レイヤーを提供します。ローカルインライン分類で使用される ML モデルは、Palo Alto Networks が悪意のあるものとして識別した特性に一致する URL ベースの脅威の現在未知および将来の亜種を識別します。最新の脅威の変化に対応するため、ローカルのインライン分類MLモデルは、コンテンツリリースによって追加・更新されます。

ファイアウォールが PAN-DB の URL をチェックするとき、以前は無害であると認定されていたが現在は悪意のある URL などの重要な更新も検索します。

PAN-DB がサイトを誤って分類したと思われる場合は、Test A Site を介して、またはファイアウォール ログから直接、ブラウザで URL カテゴリ変更要求を送信できます。

補足

技術的には、ファイアウォールは管理プレーンとデータプレーンの両方で *URL* をキャッシュします。

- *PAN-OS 9.0* 以降のリリースでは、*PAN-DB* シードデータベースはダウンロードされません。代わりに、*URL* フィルタリング ライセンスがアクティベーションされると、ファイアウォールは *URL* クエリが行われるときにキャッシュを読み込みます。
- 管理プレーンはより多くの *URL* を保持し、*PAN-DB* と直接通信します。ファイアウォールは、キャッシュ内で *URL* のカテゴリを見つけることができず、*PAN-DB* で検索を実行すると、取得したカテゴリ情報を*management plane (* 管理プレーン *- MP)*にキャッシュします。*management plane (* 管理プレーン *- MP)*はその情報をデータプレーンに渡します。データプレーンもそれをキャッシュし、それを使用してポリシーを適用します。
- データプレーンは保持する *URL* が少なく、管理プレーンから情報を受信します。ファイアウォールが の URL カテゴリの例外リスト *(*カスタム *URL* カテゴリと外部動的リスト*)* を *URL* に対してチェックした後、次に表示される場所はデータプレーンです。ファイアウォールは、データ プレーンに分類された *URL* を見つけることができない場合にのみ*management plane (* 管理プレーン *- MP)*をチェックし、カテゴリ情報がそこにない場合は、*PAN-DB* をチェックします。

ローカルインライン分類

URL Filtering ローカル インライン分類 (以前はインライン ML と呼ばれていました) を使用すると、firewall データプレーンは Web ページに機械学習を適用して、フィッシングの亜種が検出されたときにユーザーに警告し、JavaScript エクスプロイトの悪意のある亜種がネットワークに侵入するのを防ぐことができます。ローカル インライン分類は、一連の ML モデルを使用してさまざまな Web ページの詳細を評価することにより、悪意のあるコンテンツを動的に分析および検出します。各 ML モデルは、デコーダー フィールドやパターンなどのファイルの詳細を評価して、高確率の分類と判定を定式化することによって悪意のあるコンテンツを検出し、より大きな Web セキュリティ ポリシーの一部として使用されます。悪意のある URL は、追加の分析と検証のために PAN-DB に転送されます。URL 例外を指定して、検出される可能性のある誤検知を除外できます。これにより、特定のセキュリティニーズをサポートするために、プロファイルに対してより詳細なルールを作成できます。脅威の状況の最新の変更に追いつくために、インライン ML モデルは定期的に更新され、コンテンツ リリースを通じて追加されます。アクティブな Advanced URL Filtering サブスクリプションは、インライン分類 を構成するために必要です。

インライン ML ベースの保護を有効にして、Antivirus プロファイル構成の一部として、悪意のある PE (ポータブル実行可能ファイル)、ELF および MS Office ファイル、PowerShell およびシェルスクリプトをリアルタイムで検出することもできます。詳細については、以下を参照してくださいWildFire インライン ML

ローカルのインライン分類は、*VM-50* または *VM50L* 仮想アプライアンスではサポートされていません。

URL フィルタリングのユース ケース

Webページへのアクセスを強制するには、特定のサイトをブロックして許可するだけでなく、多くの方法があります。たとえば、URL ごとに複数のカテゴリを使用して、ユーザーがサイトにアクセスできるようにしますが、企業の認証情報の送信やファイルのダウンロードなどの特定の機能をブロックできます。URL カテゴリを使用して、認証、復号化、QoS、セキュリティなどのさまざまなtypes of policy（ポリシータイプ）を適用することもできます。

URL フィルタリングを展開するさまざまな方法の詳細については、以下をお読みください。

URL カテゴリに基づいた Web アクセスの制御

URL カテゴリのアクションを指定し、プロファイルをポリシー ルールに関連付ける URL フィルタリング プロファイルの作成を行うことができます。ファイアウォールは、プロファイルの設定に基づいて、トラフィックに対してポリシーを適用します。たとえば、すべてのゲーム Web サイトをブロックするには、URL フィルタリング プロファイルの URL カテゴリ *games* にブロック アクションを設定し、Web アクセスを許可するセキュリティ ポリシー ルールにアタッチします。

マルチカテゴリ URL フィルタリング

すべての URL には最大 4 つのカテゴリを含めることができます。これには、サイトが脅威にさらされる可能性を示すリスクカテゴリが含まれます。よりきめ細かい URL 分類により、ウェブ アクセスへの基本的な「ブロックまたは許可」アプローチ以上のことができます。代わりに、ビジネスには必要ですが、サイバー攻撃の一部として使用される可能性が高いオンライン コンテンツとユーザーがどのようにinteract(相互作用)するかを制御できます。

たとえば、特定の URL カテゴリは組織にとって危険であると考えるかもしれませんが、貴重なリソースまたはサービス（クラウド ストレージ サービスやブログなど）も提供するため、完全にブロックすることを躊躇します。これで、ユーザーがこれらの種類の URL カテゴリに分類されるサイトにアクセスできるようにしながら、トラフィックを復号化して検査し、コンテンツへの読み取り専用アクセスを強制することでネットワークを保護します。

厳密に制御する URL カテゴリの場合は、構成 URL フィルター に手順の一部として警告する URL フィルター プロファイル アクションを設定します。次に、URL フィルタリングのベスト プラクティス に従い続けます: URL カテゴリを復号化し、危険なファイルのダウンロードをブロックし、資格情報フィッシング防止を有効にします。

また、**Category Match** を選択し、新しいカテゴリで構成される 2 つ以上の PAN-DB カテゴリを指定することで、カスタム URL カテゴリを定義することもできます。複数のカテゴリからカスタムカテゴリを作成すると、カスタム URL カテゴリオブジェクトで指定されたすべてのカテゴリに一致する Web サイトまたはページの適用をターゲットにできます。

URL カテゴリに基づいて企業の認証情報の送信をブロックまたは許可する

資格情報フィッシングを防止する を有効にして、サイトへの企業資格情報の送信をファイアウォールで検出し、URL カテゴリに基づいて送信を制御します。ユーザーが悪意のあるサイトや信頼されていないサイトに認証情報を送信するのをブロックし、ユーザーが未知のサイトで企業の認証情報を入力する際に警告を発し、企業外のサイトで企業の認証情報を再利用する際は警

告し、ユーザーが企業のサイトや確認済みのサイトに認証情報を送信するのを明示的に許可します。

セーフサーチ設定の適用

多くの検索エンジンには、検索結果からアダルト画像やアダルト動画を除外するセーフ サーチ設定が備わっています。エンドユーザーが厳格なセーフ サーチ設定を使用していない場合にファイアウォールに検索結果をブロックさせたり、ユーザーのセーフ サーチを透過的に有効化したりできます。ファイアウォールは次の各プロバイダーのセーフ サーチをサポートしています。Google、Yahoo、Bing、Yandex、YouTube。セーフ サーチの適用の使用を開始する方法をご覧ください。

特定のサイトへのパスワード アクセスを実施

特定のユーザーがサイトにアクセスすることを許可しながら、ほとんどのユーザーに対してサイトへのアクセスをブロックできます。特定のサイトへのパスワードアクセスを許可する方法を参照してください。

特定の **URL** カテゴリからのリスクの高いファイルのダウンロードをブロック

ファイルブロックプロファイルがアタッチされたセキュリティポリシーを作成することで、特定のURLカテゴリからのファイルダウンロードをブロックできます。

URL カテゴリに基づいたセキュリティ、復号化、認証、**QoS**ポリシーの適用

URL カテゴリに基づいて、さまざまなタイプのファイアウォール ポリシーを適用できます。たとえば、復号を有効にしたが、特定の個人情報を復号化から除外するとします。この場合、URL カテゴリ *financial-services* および *health-and-medicine* に一致する Web サイトを復号化から除外する Decryption ポリシー ルールを作成できます。他の例では、QoS ポリシーで *streaming-media* という URL カテゴリを使用して、このカテゴリに分類される Web サイトに対して帯域幅の制御を適用できます。

以下の表では、URL カテゴリを一致条件として受け入れるポリシーについて説明します。

ポリシーのタイプ	説明
復号	URL カテゴリを使用して復号化を段階的に導入し、機密情報や個人情報を含む可能性のある URL カテゴリを復号化から除外することもできます（金融サービスや健康と医療など）。 最も危険なトラフィックを最初に復号化する計画 (ゲームや危険度の高いなどの悪意のあるトラフィックを収容する可能性が最も高い URL カテゴリ) し、経験を積むにつれてさらに復号化を行います。あるいは、ビジネスに影響を与えない URL カテゴリを最初に復号化します (問題が発生してもビジネスに影響を与えない) などのニュース フィード。どちらの場合も、いくつかの URL カテゴリの暗号化を解除し、ユーザーからのフィードバックを聞き、レポートを実行して、復号化が期待どおりに機能していることを確認し、さらにいくつかの URL カテゴリを徐々に復号化します。技術的な理由で復号化できない、または復

ポリシーのタイプ	説明
	号化しないことを決めた多売に、復号化から除外するために復号化除外 の作成を計画します。 ***URL*** カテゴリに基づくトラフィックの復号化は、***URL***フィルタリングとDecryption（復号化）の両方のベストプラクティスです。
認証	特定のカテゴリへのアクセスが許可される前に、ユーザーが確実に認証されるようにするために、URL カテゴリを認証ポリシールールの一致条件として 関連付けることができます。
QoS	URL カテゴリを使用して、特定の Web サイトのカテゴリのスループット レベルを割り当てることができます。たとえば、***streaming-media*** カテゴリを許可するが、QoS ポリシー ルールに URL カテゴリを追加することでスループットを制限できます。
セキュリティ	Security ポリシー規則では、URL カテゴリを次の 2 つの方法で使用できます。 • URL カテゴリを一致条件として選択して、URL カテゴリに基づいてポリシーを適用します。 • Attach a URL Filtering profile that specify policy action for each category. たとえば、社内の IT セキュリティ グループが ***hacking*** カテゴリへのアクセスを必要としているが、他のすべてのユーザーがそのカテゴリへのアクセスを拒否されている場合は、次のルールを作成する必要があります。 • IT-Security グループが ***hacking*** に分類されるコンテンツにアクセスできるようにする Security ポリシー ルール。Security ポリシー ルールは、**Services/URL Category** タブの ***hacking*** カテゴリと **Users** タブの IT-Security グループを参照します • すべてのユーザーに一般的な Web アクセスを許可するもう 1 つの Security ポリシー規則。このルールには、 ***hacking*** カテゴリをブロックする URL Filtering プロファイルをアタッチします。 ***hacking*** をブロックするポリシーの前に、***hacking*** へのアクセスを許可するポリシーを一覧表示する必要があります。これは、ファイアウォールがセキュリティ ポリシールールを上から評価するため、セキュリティ グループに属するユーザーが ***hacking*** サイトにアクセスしようとすると、ファイアウォールはアクセスを許可するポリシールールを評価し、ユーザーにアクセスを許可するためです。ファイアウォールは、ハッキングサイトへのアクセスをブロックする一般的な Web アクセス ルールに対してその他すべてのグループのユーザーを評価します。

URL カテゴリ

PAN-DB は、サイトのコンテンツ、特徴、安全性に基づいてウェブサイトを分類します。1 つの URL には、サイトが脅威となる可能性がどれほど高いかを示すリスクカテゴリ (高、中、低) などの最大 4 つのカテゴリを含めることができます。定義済み URL カテゴリの完全なリストについては、PAN-DB URL フィルタリング カテゴリ を参照してください。

Test A Siteにアクセスして、PAN-DB が URL をどのように分類するかを確認し、利用可能なすべての URL カテゴリについて学習します。また、テスト A サイトを使用して URL カテゴリの変更要求を送信するか、ファイアウォールで直接要求を送信することもできます。[URL] カテゴリの下に、変更リクエストを送信するオプションが表示されます。

URL カテゴリについての詳細を学習するため読んでください：

- URL フィルタリングのユース ケース
- セキュリティ重視の URL カテゴリ
- 不正な URL カテゴリ
- 検証済の URL カテゴリ
- URL カテゴリに基づいて実行できるポリシーアクション

セキュリティ重視の URL カテゴリ

セキュリティを重視した URL カテゴリでは、さまざまなレベルのリスクをもたらすが悪意があるとは確認されていないサイトに対して、対象となる復号化および適用を提供することで、攻撃の入り口を減らすことができます。ウェブサイトがセキュリティ関連のカテゴリに分類されるのは、そのカテゴリの基準を満たしている場合だけです。サイトのコンテンツが変わると、ポリシーの適用は動的に行われます。セキュリティに重点を置いた URL カテゴリの変更要求を送信することはできません。

セキュリティ重視の **URL** カテゴリ	
高リスク	高リスクのサイトには次のものがあります。 • 以前にマルウェア、フィッシング、または C2サイトであることが確認されたサイト。これらのサイトは、少なくとも30日間はこのカテゴリのままになります。 • PAN-DB がサイト分析と分類を完了するまで、未知のドメインは高リスクとして分類されます。 • 確認された悪意のある活動に関連するサイト。たとえば、ページ自体に悪意のあるコンテンツが含まれていなくても、同じドメインに悪意のあるホストが存在する場合、そのページは危険性が高い可能性があります。 • 防弾 ISP によってホストされているサイト。

セキュリティ重視の **URL** カテゴリ	
	• アクティブな動的 DNS 設定が存在するため、DDNS として分類されたドメイン。 • 悪意のあるコンテンツを許可することが知られている ASN から IP でホストされているサイト。 デフォルトおよび推奨ポリシーアクション:アラート
中リスク	中リスクのサイトには以下が含まれます。 • すべてのクラウドストレージサイト (URL カテゴリが **online-storage-and-backup** であるもの)。 • マルウェア、フィッシング、または C2 サイトであることが以前に確認されたサイトで、少なくとも 30 日間は良性の活動しか示されていないもの。これらのサイトは、さらに60日間このカテゴリのままになります。 • PAN-DB がサイト分析と分類を完了するまでは、未知の IP アドレスは中リスクとして分類されます。 デフォルトおよび推奨ポリシーアクション:アラート
低リスク	中リスクまたは高リスクではないサイトは、低リスクと見なされます。これらのサイトは最低 90 日間良性の活動を見せています。 デフォルトおよび推奨ポリシーアクション:**Allow** [許可]
新しく登録されたドメイン	過去 32 日以内に登録されたサイトを識別します。新しいドメインは、悪意のあるキャンペーンツールとして頻繁に使用されます。 デフォルトのポリシーアクション:アラート 推奨されるポリシー アクション:ブロック 新しく登録されたドメインは、意図的にまたはドメイン生成アルゴリズムによってしばしば生成され、悪意のある活動に使用されます。この ***URL*** カテゴリをブロックするのがベストプラクティスです。

不正な URL カテゴリ

悪意のあるコンテンツまたは悪用されるコンテンツを識別する URL カテゴリをブロックすることを強くお勧めします。はじめに、デフォルトのマルウェア、フィッシング、およびコマンドアンドコントロールの URL カテゴリをブロックする、デフォルトの URL フィルタリングプロファイルをコピーします。デフォルトの URL フィルタリングプロファイルは、薬物乱用、アダルト、ギャンブル、ハッキング、疑わしい、そして武器の URL カテゴリもブロックします。

これらの URL カテゴリをブロックするかどうかは、ビジネス要件によって異なります。たとえば、大学では可用性が重要であるため、これらサイトのほとんどに対する学生によるアクセスを制限したくないと思うかもしれませんが、セキュリティを第一に重視する企業ではそれらの一部またはすべてをブロックすることがあります。

- **command-and-control (コマンド アンド コントロール)**—マルウェアや感染したホストが、密かに攻撃者のリモートサーバーと通信を行って悪意のあるコマンドを受信したりデータを盗んだりするために使用する、コマンド アンド コントロール URL およびドメイン。
- **malware** [マルウェア]—マルウェアをホストしていることが分かっている、あるいはコマンド アンド コントロール（C2）トラフィックに使用されているサイト。エクスプロイトキットを使用する場合もあります。
- **phishing** [フィッシング]—認証ページを偽装、あるいはフィッシングにより個人のID情報を盗むことが分かっている。これには、ログイン資格情報、クレジットカード情報(自発的または不本意な情報)、アカウント番号、PIN、およびソーシャルエンジニアリング技術を介して被害者から個人を特定できる情報(PII)と見なされる情報を含む、情報を収集するためにユーザーをだまそうとするWebコンテンツが含まれます。テクニカルサポート詐欺やスケアウェアもフィッシングとして含まれています。
- **grayware (グレイウェア)**—ウイルスの定義を満たさないもの、もしくはセキュリティに直接的な脅威をもたらさないものだが、目ざわりな挙動をし、ユーザーに影響を与えて、リモート アクセスを許可したり、その他の不正なアクションを実行したりする、Web サイトおよびサービス。グレイウェアには、詐欺、違法行為、犯罪行為、一攫千金を謳うサイト、アドウェア、その他の不要または未承諾のアプリケーション、例えば組み込み暗号マイナーや、ブラウザの要素を変更するハイジャッカーなどが含まれます。悪意を示すものではなく、ターゲットドメインが所有していないタイポスクワッティング ドメインは、グレイウェアとして分類されます。コンテンツ リリース バージョン 8206 より前は、ファイアウォールはグレイウェアをマルウェアまたは疑わしい URL カテゴリのいずれかに分類していました。グレイウェアをブロックするかどうかわからない場合は、まずグレイウェアでアラートを生成し、アラートを調査してから、グレイウェアをブロックするか、グレイウェアでアラートを続行するかを決定します。
- **dynamic-dns** [動的DNS]—動的にIPアドレスが割り当てられ、しばしばマルウェアのペイロードやC2トラフィックを送るシステムのホストおよびドメイン名。また、動的DNSドメインは、信頼できるドメイン登録業者が登録したドメインとは違う検査プロセスを経ているため、信頼度が低くなります。
- **unknown (未知)**—PAN-DB によってまだ識別されていないサイトです。可用性がビジネスにとって重要であり、トラフィックを許可し、未知のサイトに警告し、トラフィックにベストプラクティスセキュリティプロファイルを適用し、アラートを調査する必要がある場合。

  PAN-DB リアルタイム更新は、未知のサイトへの最初のアクセス試行後に未知のサイトを学習を行うため、未知の *URL* は迅速に識別され、ファイアウォールが実際の *URL* カテゴリに基づいて処理できる既知の *URL* となります。
- **newly-registered-domain (新規登録ドメイン)**—新規登録ドメインは、故意またはドメイン生成アルゴリズムによって生成されることが多く、悪意のある活動に使用されます。
- **copyright-infringement (著作権侵害)**—ソフトウェアまたはその他の知的財産の違法ダウンロードを許可するコンテンツなど、違法なコンテンツがあるドメインであり、潜在的な責任のリスクをもたらします。教育業界で求められる児童保護法や、ユーザーがサービスを介し

て著作権で保護されたコンテンツを共有することをインターネットプロバイダーが防止しなければならない国の法律に準拠するために、このカテゴリーが導入されました。

- **extremism (過激な思想)**—テロ、人種差別、ファシズムや、民族的な出自や宗教、その他の考え方が異なる人や集団を差別するその他の過激な思想を喧伝するウェブサイト。このカテゴリーは、教育業界で求められる児童保護法に準拠するために導入されました。地域によっては、法規制により過激派サイトへのアクセスが禁止されている場合があり、アクセスを許可すると責任を問われる可能性があります。
- **proxy-avoidance-and-anonymizers (プロキシ回避およびアノニマイザー)**—しばしばコンテンツのフィルタリングを回避するのに使用されるURLおよびサービス。
- **questionable (疑わしい)**— 個人やグループの特定の層を標的とした、悪趣味なユーモアや不快なコンテンツを含む Web サイト。
- **parked** [パークド]—個人によって登録されたドメインであり、後に認証情報を盗むフィッシングに使用されていることが分かることがあります。フィッシングにより認証情報や個人のID情報を盗むために用意されたこれらのドメインは、正当なドメインに似通っている場合があります（例：paloaltoonetworks.com）。あるいはpanw.netなど、いつか価値が出ると期待させて不当な個人購入を行わせるドメインもあります。

ブロックする代わりにアラートを出すカテゴリでは、ユーザーがサイトコンテンツと対話する方法を非常に厳格に制御できます。例えば、研究目的の開発者ブログやクラウドストレージサービスなど、必要なリソースへのアクセスをユーザーに許可しますが、ウェブベースでの脅威にさらされる可能性を減らすために次の予防策を講じます。

- アンチスパイウェア、脆弱性対策、ファイル遮断の ベストプラクティスに従ってください。危険なファイルタイプのダウンロードをブロックし、警告を出しているサイトの難読化された JavaScript をブロックすることが保護手段となります。
- URL カテゴリに基づく ターゲット復号化 です。高リスクと中リスクのサイトを復号化することから始めることを推奨します。
- 応答ページを表示して、ユーザーに高リスクおよび中リスクのサイトにアクセスしたことを知らせます。ユーザーにアクセスしようとしているサイトが悪意のある可能性があることを警告し、そのサイトにアクセスする場合の予防策についてアドバイスします。
- 高リスクおよび中リスクのサイトを含むサイトにユーザーが企業の認証情報を送信するのをブロックすることにより、認証情報の盗難を防止します。

検証済の URL カテゴリ

Palo Alto Networksは、要求されたサイトが属する URL カテゴリを検証します。URL が 悪意のある URL カテゴリ に属していると PAN-DB が判断した場合、サイトに セキュリティに重点を置いた URL カテゴリ (高リスク、中リスク、低リスク) は割り当てられません。ほとんどの環境において許容できないレベルのリスクをもたらすため、ファイアウォールはこれらのカテゴリのサイトを自動的にブロックします。リスク レベルは、悪意のある ***URL*** として分類されていないか、証拠がないためにもはや悪意のある ***URL*** として分類されていない URL に対してのみ予約されています。

次の表に プライベート `IP` アドレス を除き、PAN-DB が悪意のあるカテゴリと見なし、デフォルトでブロックするカテゴリを示します。プライベート IP アドレス (およびホスト) はホスト環境

に固有であり、PAN-DB からは見えません。その結果、Palo Alto Networksはこのカテゴリのサイトにリスク評価を割り当てません。

カテゴリ	デフォルト アクション
Malware	ブロック
フィッシング	
コマンドアンドコントロール	
グレイウェア	
プライベート **IP** アドレス	許可済み (デフォルトのアクションなし)

現在の ***URL*** カテゴリの詳細情報については、以下を参照してください:PAN-DB URLフィルタリングカテゴリ全一覧

URL カテゴリに基づいて実行できるポリシーアクション

ファイアウォールでは、URL フィルタリング プロファイルを使用して、URL カテゴリを適用する方法を指定できます。デフォルト設定では、新しい URL フィルタリング プロファイルの作成を行う際、すべての URL カテゴリに対してサイト アクセスが許可されるように設定されています。これは、ユーザーはすべてのサイトを自由に閲覧でき、トラフィックがログに記録されないことを意味しています。各カテゴリに適用する**Site Access**（サイトアクセス）のタイプを決定して、URL フィルタリング プロファイルをカスタマイズします。資格情報フィッシングを防止する には、URL カテゴリに基づいて **User** 資格情報の送信 を許可または禁止することもできます (たとえば、中程度およびリスクの高いサイトへのユーザー資格情報の送信をブロックできます)。ユーザーは引き続きこれらのサイトにアクセスできますが、企業の認証情報を入力することはできません。

URL フィルタリングで定義したアクションの適用を開始するには、プロファイルをセキュリティ ポリシー ルールにアタッチする必要があります。firewall は、Security ポリシー・ルールに一致するトラフィックにプロファイル・アクションを適用します (詳しくは、URL フィルタリングの設定 を参照してください)。

最良の URL フィルタリング プロファイルを設定する詳細な方法を学び、マルウェアあるいは悪意のあるコンテンツをホストしていることが分かっている ***URL*** から確実に保護されるようにします。

操作	説明
サイト アクセス	
Alert [アラート]	Web サイトが許可され、URL フィルタリング ログにログ エントリが生成されます。

操作	説明
	ブロックしないトラフィックのカテゴリーに対するアクションとして***alert*** **(**アラート**)**を設定し、トラフィックをログに記録して可視性を確保します。
allow [許可]	Web サイトが許可され、ログ エントリは生成されません。 ログに記録しないトラフィックに対する可視性が失われるため、ブロックしないトラフィックのカテゴリーに対するアクションとして***allow*** **(**許可**)**を設定しないでください。その代わりに、ブロックしないトラフィックのカテゴリーに対するアクションとして***alert*** **(**アラート**)**を設定し、トラフィックをログに記録して可視性を確保します。
block	Web サイトがブロックされ、応答ページが表示されます。Web サイトへのアクセスを続行することはできません。URL フィルタリング ログでログ エントリが生成されます。 ある URL カテゴリについてサイト アクセスをブロックすると、その URL カテゴリの User Credential Submissions (ユーザーの認証情報送信) もブロックに設定されます。
続行	会社のポリシーによりサイトがブロックされたことを示す応答ページが表示され、Web サイトへのアクセスを続行するオプションが表示されます。**[continue]** アクションは、通常、無害とみなされるカテゴリで使用され、ユーザーがサイトが正しく分類されていないと感じる場合に、操作を続行するためのオプションを提供することで、ユーザーの操作性を向上させるために使用されます。応答ページのメッセージをカスタマイズして、自社専用の詳細情報を含めることができます。URL フィルタリング ログでログ エントリが生成されます。 プロキシ サーバーを使用するように設定されているクライアントシステムでは、*Continue* (続行) ページは正しく表示されません。
override [オーバーライド]	特定のカテゴリの Web サイトへのアクセスを許可するためにパスワードが必要であることを示す応答ページが表示されます。このオプションを使用して、セキュリティ管理者またはヘルプデスク担当者は、特定のカテゴリのすべての Web サイトに一時的なアクセスを付与するパスワードを提供します。URL フィルタリング ログでログ エントリが生成されます。特定のサイトへのパスワード アクセスを許可するを参照してください。 以前のバージョンでは、URL フィルタリングカテゴリのオーバーライドがカスタム URL カテゴリより優先されていました。PAN-OS 9.0 へ

操作	説明
	のアップグレードの一環として、URL カテゴリのオーバーライドはカスタム URL カテゴリに変換され、他のカスタム URL カテゴリに優先されることはなくなりました。以前のバージョンでカテゴリのオーバーライドに対して定義したアクションの代わりに、最も厳格な URL フィルタプロファイルアクションを使用する新しいカスタム URL カテゴリがセキュリティポリシールールによって適用されます。最も厳格なものから最も緩やかなものまで、可能な URL フィルタリングプロファイルアクションは、ブロック、上書き、続行、警告、および許可となります。 つまり、アクション allow で URL カテゴリのオーバーライドを行った場合、PAN-OS 9.0 でカスタム URL カテゴリに変換された後にオーバーライドがブロックされる可能性があります。 プロキシ サーバーを使用するように設定されているクライアントシステムでは、*Override* (オーバーライド) ページは正しく表示されません。
none [なし]	**none** アクションはカスタム URL カテゴリにのみ適用されます。**none** を選択して、複数の URL フィルタリング プロファイルが存在する場合、カスタム カテゴリが他のプロファイルに影響を与えないようにします。たとえば、2 つの URL フィルタリング プロファイルがあり、一方のプロファイルでカスタム URL カテゴリが **block** に設定されている場合、ブロック アクションをもう一方のプロファイルに適用しない場合は、アクションを **none** に設定する必要があります。 また、カスタム URL カテゴリを削除するには、使用されるプロファイルで **[none]** に設定されている必要があります。
ユーザーの認証情報の権限 これらの設定では、最初の 設定された資格情報フィッシング防止 を設定する必要があります。	
Alert [アラート]	この URL カテゴリに属すサイトにユーザーが企業の認証情報を送信することを許可しますが、毎回 URL フィルタリング アラート ログを生成します。
allow（デフォルト）	この URL カテゴリに属すサイトにユーザーが企業の認証情報を送信することを許可します。
block	この URL カテゴリに属すサイトにユーザーが企業の認証情報を送信することをブロックします。デフォルトのアンチフィッシング応答ページは、ユーザーが企業の認証情報を送信することがブロックされてい

操作	説明
	るサイトにアクセスする際に表示されます。カスタム ブロック ページを作成して表示することもできます。
続行	応答ページを表示し、サイトにアクセスするためにユーザーが Continue（続行）を選択することを要求します。デフォルト設定では、認証情報を送信することが推奨されないサイトにユーザーがアクセスする際にアンチフィッシング続行ページが表示されます。また、カスタム ブロック ページを作成して表示することもできます（フィッシングの試みや、他のウェブサイトで認証情報を再利用することについてユーザーに警告を促したい場合など）。

URL フィルタリングデプロイメントの計画

ネットワークに URL フィルタリングを展開するには、確認された悪意のあるコンテンツをブロックしながら、Web アクティビティ パターンを可視化する基本的な設定から始めることをお勧めします。

- 大抵のカテゴリについて警告を出す (おおよそ) パッシブな URL フィルタリング プロファイルから始めます。これにより、ユーザーがアクセスするサイトに対する可視性を得て、何を許可、制限、ブロックするべきか判断できるようになります。
- 好ましくないことが分かっている URL カテゴリ (マルウェア、C2、フィッシング) をブロックします。

すべてのウェブ アクティビティに対してアラートを出すとログ ファイルの量が増えるため、初めて URL フィルタリングをデプロイするなら、上記のみを有効にする方法も妥当かもしれません。

現時点では、*URL* フィルタリング プロファイルで ***Log container page only*** **(**コンテナ ページのみロギング**)** オプションを有効にすると、カテゴリに一致するメイン ページのみがログに記録され、コンテナ ページ内にロードされる可能性のある後続のページ/カテゴリは記録されないため、*URL* フィルタリング ログを削減できます。

STEP 1 | いつでも、Test A Site を使用して、PAN-DB（URLフィルタリング クラウド データベース）が特定の URL を分類する方法を確認し、考えられるすべての URL カテゴリについて学習します。

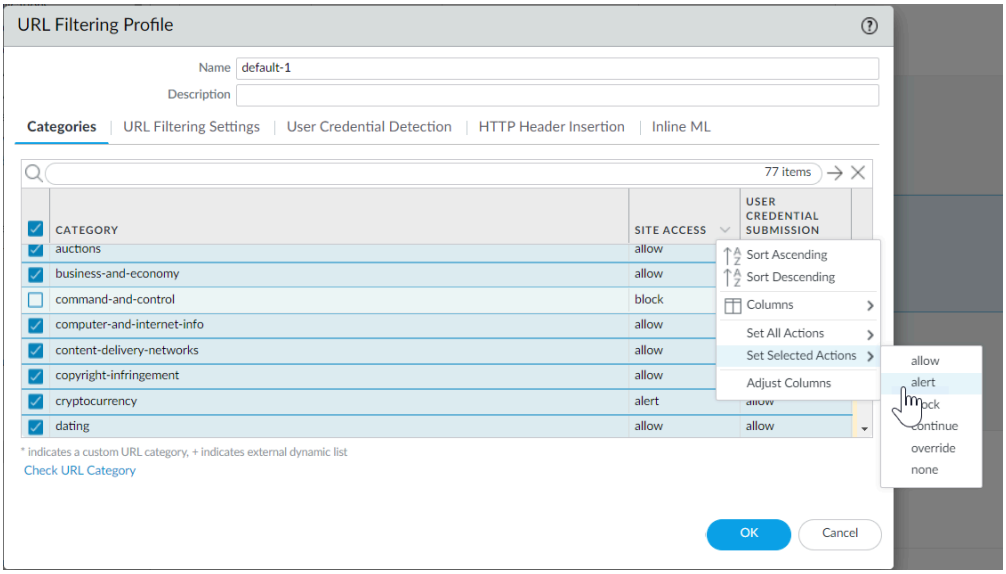
特定の URL の分類方法に同意できない場合は、Test A Site を使用して、change request（変更要求）を送信することもできます。

STEP 2 | すべてのカテゴリで警告を送信するパッシブ URL フィルタリング プロファイルを作成して、Web トラフィックを可視化します。

1. **Objects (**オブジェクト**)** > **Security Profiles (**セキュリティ プロファイル**) URL Filtering (URL**フィルタリング**)** の順に選択します。
2. デフォルト プロファイルを選択し、**Clone**[コピー] をクリックします。新しいプロファイルには **default-1** という名前が付けられます。
3. **default-1** プロファイルを選択して、名前を変更します。たとえば、URL-Monitoring と名前を変更します。

STEP 3 | ブロック状態を維持しなければならないマルウェア、コマンド アンド コントロール、フィッシングを除き、すべてのカテゴリのアクションを **alert (アラート)** に設定します。

1. すべての URL カテゴリをリストするセクションでは、すべてのカテゴリを選択して、マルウェア、command-and-control およびフィッシングを解除します。
2. *[アクション]* 列のヘッダーの右にマウスを重ね、下向き矢印を選択して、**[選択したアクションの設定]** を選択し、**[alert]** を選択します。



3. 既知の危険な URL カテゴリへのアクセスを **Block**（ブロック）します。

   マルウェア、フィッシング、ダイナミック *DNS*、未知、コマンド&コントロール、過激思想、著作権侵害、プロキシ回避・アノニマイザー、新しく登録されたドメイン、グレイウェアおよびドメインパーキングに使用された *URL* カテゴリへのアクセスをブロックします。

4. **OK** をクリックしてプロファイルを保存します。

STEP 4 | URL フィルタリング プロファイルを、ユーザーの Web トラフィックを許可するセキュリティ ポリシー ルールに適用します。

1. [ポリシー > セキュリティ] を選択し、適切なセキュリティ ポリシーを選択して変更します。
2. **[アクション]** タブを選択して、**[プロファイル設定]** セクションで、**[URL フィルタリング]** のドロップダウンをクリックし、新しいプロファイルを選択します。
3. **OK** をクリックして保存します。

STEP 5 | 設定を保存します。

Commit（コミット）をクリックします。

STEP 6 | URL フィルタリング ログを表示して、ユーザーがアクセスしているすべての Web サイトのカテゴリを確認します。また、ブロックすることにしたカテゴリはログに記録されます。

ログの表示およびレポートの生成の詳細は、Web アクティビティのモニターを参照してください。

Monitor (監視) > **Logs (ログ)** > **URL Filtering (URL フィルタリング)** を選択します。アクションが **allow (許可)** 以外に設定されているカテゴリに含まれる URL フィルタリング データベースに存在するすべてのウェブサイトでログ エントリが作成されます。URL フィルタリング レポートでは、24 時間の Web アクティビティを表示できます。（**Monitor**（モニター） > **Reports**（レポート））。

STEP 7 | 次のステップ：

- PAN-DB はすべての URL を最大 4 つのカテゴリに分類し、すべての URL にはリスク カテゴリ（高、中、低）があります。高および中リスクのあるサイトは悪意があると確定されているわけではありませんが、悪意のあるサイトと密接に関連しています。例えば、悪意のあるサイトと同じドメインであったり、つい最近まで悪意のあるコンテンツをホストしていたりする可能性があります。許可またはブロックしていないものすべてについて、リスクカテゴリを使用して、Webサイトの安全性に基づいた簡単なポリシーを作成します。

  安全上の懸念があるサイトであっても、ユーザーアクセスを許可したい場合があるため、リスクの高いサイトでのユーザーの操作を制限する予防策を講じることができます。（例えば開発者のブログを調査目的で使用することを許可しようとしますが、ブログは一般的にマルウェアをホストしていることが知られているカテゴリです）。
- URL フィルタリングを User-ID とペアにして、組織または部門に基づいて Web アクセスを制御し、認可されていないサイトへの企業の認証情報の送信をブロックします。
  - URL フィルタリングは、サイトカテゴリに基づいてサイトへの企業の認証情報の送信を検出することにより、認証情報の盗難を防ぎます。ユーザーが悪意のあるサイトや信頼されていないサイトに認証情報を送信するのをブロックし、ユーザーが未知のサイトで企業の認証情報を入力する際、および企業外のサイトで企業の認証情報を再利用する際に警告し、ユーザーが企業のサイトに認証情報を送信するのを明示的に許可します。
  - パッシブ URL フィルタリング プロファイルを使用してセキュリティ ポリシー ルールを追加または更新し、部門のユーザー グループ (たとえば、マーケティングまたはエンジニアリング (ポリシー > セキュリティ > ユーザー) に適用されるようにします。部門の活動を監視し、部門のメンバーからフィードバックを得て、部門のメンバーが行う作業に不可欠な Web リソースを理解します。
- URL フィルタリングを使用するすべての方法を検討して、攻撃対象を減らし、Web の使用を制御してください。たとえば、学校の場合は、URL フィルタリングを使用して、検索エンジンがアダルト画像や動画を検索結果から除外する厳密なセーフサーチ設定を適用できます。または、セキュリティ オペレーション センターがある場合は、侵害されたサイトや危険なサイトへのパスワード アクセスを脅威アナリストに与え、それ以外の場合は、組織やチーム全体に公開したくない場合があります。
- URL フィルタリングのベスト プラクティス に従います。

URL フィルタリングのベストプラクティス

Palo Alto Networks URLフィルタリングソリューションは、Webベースの脅威からお客様を保護し、Webアクティビティを監視および制御する簡単な方法を提供します。URL フィルターの展開を最大限に活用するには、まず、ビジネスを行うために依存しているアプリケーションの許可ルールを作成する必要があります。次に、悪意のあるコンテンツおよび悪用されるコンテンツを分類する URL カテゴリを確認します。これらを完全にブロックすることをお勧めします。次に、他のすべてについて、これらのベストプラクティスは、ユーザーが必要とする Web コンテンツへのユーザーのアクセスを制限することなく、Web ベースの脅威にさらされるリスクを減らす方法を案内します。

- 開始する前に、ベスト プラクティスのインターネット ゲートウェイ セキュリティ ポリシーの構築の一環として、許可するアプリケーションを特定し および アプリケーション許可ルールの作成 を実行します。

  許可するアプリケーションには、ビジネスとインフラストラクチャの目的でプロビジョニングまた管理するアプリケーションだけでなく、ユーザーが業務を行うために必要なアプリケーションや、個人的利用のために使用を許可する一部のアプリケーションも含まれます。

  これらの承認済みアプリケーションを特定したら、URL フィルターを使用して、許可リストにないすべての Web アクティビティを制御および保護できます。
- ユーザーの Web アクティビティを可視化して、組織にとって最も効果的な URL フィルタリング ポリシーを 計画し、スムーズにロールアウトできるようにします 。これには次のものが含まれます。
  - Test A Site を使用して、PAN-DB (Palo Alto Networks URL フィルタリング クラウド データベース) が特定の URL を分類する方法を確認し、考えられるすべての URL カテゴリについて学習します。
  - URL カテゴリについてアラートを出す (おおよそ) パッシブな URL フィルタリング プロファイルから始めます。これにより、ユーザーがアクセスするサイトに対する可視性を得て、何を許可、制限、ブロックするべきか判断できるようになります。
  - Web アクティビティを監視して、ユーザーがアクセスしているサイトを評価し、ビジネスニーズにどのように対応しているかを確認します。
- 悪質で悪用される Web コンテンツを分類する URL カテゴリをブロックします。これらのカテゴリは危険であることがわかっていますが、ブロックすることを決定した URL カテゴリはビジネスニーズに依存する可能性があることに常に注意してください。
- URL カテゴリを使用して復号化を段階的に導入し、機密情報または個人情報（金融サービスや健康と医療など）を復号化から除外します。

  最も危険なトラフィックを最初に復号化する計画 (ゲームや危険度の高いなどの悪意のあるトラフィックを収容する可能性が最も高い URL カテゴリ) し、経験を積むにつれてさらに復号化を行います。あるいは、ビジネスに影響を与えない URL カテゴリを最初に復号化します (問題が発生してもビジネスに影響を与えない) などのニュース フィード。どちらの場合も、いくつかの URL カテゴリの暗号化を解除し、ユーザーからのフィードバックを聞き、レポートを実行して、復号化が期待どおりに機能していることを確認し、さらにいくつかの URL カ

テゴリを徐々に復号化します。技術的な理由で復号化できない、または復号化しないことを決めた多売に、復号化から除外するために復号化除外 の作成を計画します。

URL カテゴリに基づいて復号化をターゲットにすることも、Decryption（復号化）のベストプラクティスです。

- ファイアウォールを有効にすることにより認証情報の盗難を防止して、サイトへの企業の認証情報の送信を検出し、URL カテゴリに基づいてそれらの送信を制御します。ユーザーが悪意のあるサイトや信頼されていないサイトに認証情報を送信するのをブロックし、ユーザーが未知のサイトで企業の認証情報を入力する際に警告を発し、企業外のサイトで企業の認証情報を再利用する際は警告し、ユーザーが企業のサイトや確認済みのサイトに認証情報を送信するのを明示的に許可します。
- JavaScript エクスプロイトの悪意がある亜種やフィッシング攻撃を、リアルタイムでブロックします。ローカルインライン分類を有効にすると、firewall で機械学習を使用して Web ページを動的に分析できます。
- Advanced URL Filtering インライン クラウド分類 を有効にして、インライン ディープ ラーニング、ML ベースの検出エンジンを使用して、疑わしい Web ページ コンテンツを分析し、ゼロデイ Web 攻撃からユーザーを保護します。クラウドのインライン分類は、高度な標的型フィッシング攻撃や、クローキング、マルチステップ攻撃、CAPTCHAチャレンジ、以前は見られなかったワンタイム使用URLなどの高度な回避技術を使用するその他のWebベースの攻撃を検出して防止することができます。
- の高リスクおよび中リスクのコンテンツ とのユーザーの対話方法を解読し、検査し、厳密に制限します (ビジネス上の理由から、の悪質な URL カテゴリ をブロックしないことにした場合は、ユーザーがそれらのカテゴリと対話する方法も厳密に制限する必要があります)。

  認可する Web コンテンツと完全にブロックする悪意のある URL カテゴリは、Web トラフィック全体の一部にすぎません。ユーザーがアクセスしている残りのコンテンツは、良性（低リスク）と危険なコンテンツ（高リスクと中リスク）の組み合わせです。高および中リスクのコンテンツは悪意があると確定されているわけではありませんが、悪意のあるサイトと密接に関連しています。たとえば、リスクの高い URL が悪意のあるサイトと同じドメインにある場合や、過去に悪意のあるコンテンツをホストしていた場合などです。

  ただし、組織にリスクをもたらす多くのサイトは、ユーザーに貴重なリソースとサービスも提供しています（クラウドストレージサービスは良い例です）。これらのリソースとサービスはビジネスに必要ですが、サイバー攻撃の一部として使用される可能性も高くなります。ユーザーに優れたユーザーエクスペリエンスを提供しながら、この潜在的に危険なコンテンツを操作する方法を制御する方法は次のとおりです。

  - URL フィルタリング プロファイルで、高リスクと中リスクのカテゴリを**continue(続行)**に設定し、応答ページを表示して、ユーザーに危険性のあるサイトにアクセスしていることを警告します。ユーザーがサイトにcontinue (続行)することを決定した場合に予防策をとる方法をアドバイスします。ユーザーに応答ページを表示したくない場合は、リスクの高いカテゴリとリスクが中程度のカテゴリで警告します。
  - 高リスクおよび中リスクのサイトを復号します。
  - 高リスクおよび中リスクのサイトのためのアンチスパイウェア、脆弱性対策、ファイル遮断の ベストプラクティスに従ってください。危険なファイルタイプのダウンロードをブロックし、難読化された JavaScript をブロックすることが保護手段となります。

  - 高リスクおよび中リスクのサイトにユーザーが企業の認証情報を送信するのをブロックすることにより、認証情報の盗難を防止します。
- 学校や教育機関は、セーフ サーチを適用して、検索エンジンが検索結果からアダルト画像や動画を確実に除外するようにする必要があります。ユーザーに対して透過的にセーフ サーチを有効にすることができます。
- ファイアウォールが PAN-DB を使用して Web サイトの URL カテゴリを検索するときに、初期 Web 要求を保持できるようにします。

  ユーザーが Web サイトにアクセスすると、Advanced URL Filtering が有効になっている firewall は、URL カテゴリのローカルキャッシュをチェックしてサイトを分類します。ファイアウォールが URL カテゴリをキャッシュで見つけられない場合、ファイアウォールはPalo Alto Networks URL データベースである PAN-DB で検索を実行します。デフォルトでは、ファイアウォールはこのクラウド検索中にユーザーの Web 要求を許可し、サーバーが応答したときにポリシーを適用します。

  ただし、Web 要求を保持することを選択した場合、ファイアウォールは、URL カテゴリが見つかるか、タイムアウトになるまで要求をブロックします。検索がタイムアウトした場合、ファイアウォールは解決されていない URL カテゴリと見なします。

  1. In **Device** > **Setup** > **Content-ID**, チェックボックスをオンにします

     カテゴリ検索のクライアント要求を保持する.

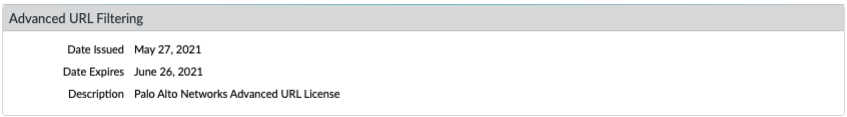
Advanced URL Filtering サブスクリプションを有効にする

Palo Alto NetworksのURLフィルタリングソリューションであるAdvanced URL Filteringサブスクリプションは、リアルタイムのURL分析とマルウェア防止を提供します。Palo Alto Networksが開発した高性能URLルックアップ用のURLフィルタリングデータベースであるPAN-DBアクセスに加えて、悪意のあるURLやIPアドレスに対するカバレッジも提供します。この多層保護ソリューションは、URL フィルタリングプロファイルを使用して構成されます。

STEP 1 | Advanced URL Filtering ライセンスを取得してインストールし、インストールされていることを確認します。

詳細な *URL* フィルタリング ライセンスには、*PAN-DB* へのアクセスが含まれます。ライセンスの有効期限が切れると、ファイアウォールは *URL* フィルタリング機能、*URL* カテゴリの適用、および *URL* クラウドルックアップの実行を停止します。また、有効なライセンスをインストールするまで、他のすべてのクラウド ベースの更新プログラムは機能しません。

1. **Device (デバイス)** > **Licenses (ライセンス)** の順に選択し、License Management (ライセンス管理) セクションで、ライセンスのインストール方法を選択します。
   - ライセンス サーバーからライセンス キーを取得
   - 認証コードを使用した機能のアクティベーション
2. ライセンスをインストールした後、[詳細な URL フィルタリング] セクション [日の有効期限] フィールドに有効な日付が表示されていることを確認します。



Advanced URL Filtering ライセンスをアクティベートすると、*PAN-DB* および *Advanced URL Filtering* のライセンス資格がファイアウォールに正しく表示されないことがあります – これは表示の異常であり、ライセンスの問題ではなく、サービスへのアクセスには影響しません。次の *CLI* コマンドを使用して、ファイアウォールのライセンスを更新して表示の問題を修正できます。ライセンス取得を要求します。

STEP 2 | 最新の PAN-OS コンテンツ リリース をダウンロードしてインストールします。PAN-OS アプリケーションと脅威コンテンツリリース 8390-6607 以降では、PAN-OS 9.x 以降を動作するファイアウォールが、新しいリアルタイム検出カテゴリを使用して分類された URL を識別し、高度な URL フィルタリングによって分類される URL を識別することができます。この更新プログラムの詳細については、「アプリケーション」および「脅威コンテンツのリリース ノート」を参照してください。Palo Alto Networksサポートポータルで、またはファイアウォールのWebインターフェイスで直接デバイスと脅威のコンテンツリリー

スノートを確認することもできます。デバイス > 動的更新を選択し、特定のコンテンツリリースバージョンのリリースノートを開きます。

最新のコンテンツ リリース バージョンに更新する場合は、 のベスト プラクティスに従ってアプリケーションと脅威のコンテンツ更新 を更新します。

STEP 3 | アプリケーションおよび脅威のダイナミック更新をダウンロードするようにファイアウォールをスケジュールします。

アンチウイルス、アプリケーションおよび脅威を含むコンテンツの更新を受信するには、脅威防御ライセンスが必要です。

1. **Device**（デバイス） > **Dynamic Updates**（動的更新）を選択します。
2. Applications and Threats [アプリケーションおよび脅威]セクションの Schedule [スケジュール]フィールドで、**None** [なし]リンクをクリックし、定期的な更新をスケジュールします。

   ファイアウォールからインターネットに直接アクセスできる場合、ダイナミック更新のみをスケジュールできます。セクションで更新がすでにスケジュールされている場合、リンク テキストにスケジュール設定が表示されます。

   アプリケーションおよび脅威更新には、セーフ サーチを適用に関連する URL フィルタリングの更新が含まれていることがあります。

次のステップ：

1. URL フィルタリング プロファイル を設定して、組織の Web 利用ポリシーを定義します。
2. 詳細な URL フィルタリングを確認する

URL フィルタリングの設定

URL フィルタリング ポリシーの要件 を決定したら、ユーザーがアクセスしている Web サイトの種類と Web サイトのカテゴリについて基本的な理解が得られたはずです。この情報を使用して、カスタム URL フィルタリング プロファイルを作成し、Web アクセスを許可するセキュリティ ポリシー ルールに関連付けます。URL フィルタリング プロファイルで Web アクセスを管理できるだけでなく、User-ID™ を設定している場合、ユーザーが企業の認証情報を送信できる各サイトを管理することができます。

STEP 1 | URL フィルタリング プロファイルを作成します。

まだ行っていない場合は、最良の URL フィルタリング プロファイルを設定し、マルウェアあるいは悪意のあるコンテンツをホストしている *URL* から確実に保護されるようにします。

Objects（オブジェクト） > **Security Profiles**（セキュリティプロフィール） > **URL Filtering**（**URL**フィルタリング）を選択し、URL フィルタリングプロファイルを **Add**（追加）または変更します。

STEP 2 | URL カテゴリ毎にサイト アクセスを定義します。

Categories (カテゴリ**)** を選択し、各 URL カテゴリ毎に Site Access (サイト アクセス) を設定します。

- その URL カテゴリ宛てのトラフィックを**allow**（許可）します。許可されたトラフィックは記録されません。
- ユーザーがアクセスしているサイトに可視性をもたらすには、**alert (**アラート**)** を選択します。そのカテゴリに一致するトラフィックは許可されますが、ユーザーがそのカテゴリのサイトにいつアクセスしたかを記録する URL フィルタリング ログが生成されます。
- そのカテゴリに一致するトラフィックへのアクセスを拒否し、ブロックされたトラフィックのロギングを有効にするには、**block (**ブロック**)** を選択します。
- **continue (**続行**)** を選択し、ユーザーに警告付きのページを表示し、サイトにアクセスするためにカテゴリーの中から **Continue(**続行**)** をクリックするよう求めます。
- ユーザーが設定されたパスワードを入力した場合にのみアクセスを許可するには、**override** を選択します。詳細については、特定のサイトへのパスワード アクセスを許可するを参照してください。

STEP 3 | 許可する URL カテゴリに属すウェブサイトに対して行う、企業の認証情報の送信を検知する URL フィルタリング プロファイルを設定します。

最高のパフォーマンスを維持して誤検出の頻度を下げるために、マルウェアあるいはフィッシングのコンテンツをホストしていることが一度も判明していないサイトに関連付けられた *App-ID*™ について、ファイアウォールは自動的に認証情報の送信のチェックをスキップします（対応するカテゴリでチェックを有効にしている場合でも）。ファイアウォールが認証情報のチェックをスキップするサイトのリストは、アプリケーションおよび脅威コンテンツ更新を通じて自動的に更新されます。

1. **User Credential Detection (**ユーザーの認証情報検出**)** を選択します。
2. ユーザー資格情報検出 ドロップダウンから、Web ページの企業資格情報の送信 を確認する方法のいずれかを選択します。
   - **Use IP User Mapping**（**IP** ユーザー マッピングの使用）—企業のユーザー名送信が正当なものであり、セッションの送信元 IP アドレスにログインしたユーザーにユーザー名が一致することが確認されます。ファイアウォールは、送信されたユーザー名を IP アドレスからユーザー名へのマッピング テーブルと照合します。Map IP アドレスからユーザー に説明されているユーザー マッピングメソッドを使用できます。
   - **Use Domain Credential Filter**（ドメイン認証情報フィルタを使用）—有効な企業ユーザー名とパスワード送信をチェックし、ユーザー名が、ログイン ユーザーの IP アドレスに対応することを確認します。User-ID をセットアップしてこの方式を有効にする方法については、Windows User-ID エージェントを使用したユーザー マッピングの設定を参照してください。
   - グループ マッピングを使用する] - ユーザーをグループにマップする場合に設定されたユーザーからグループへのマッピング テーブルに基づいて有効なユーザー名の送信をチェックします

     グループ マッピングの場合、最も重要なアプリケーションにアクセスできる IT のようなグループなど、特定のグループ、あるいはディレクトリの **any (**いずれか**)** の部分に認証情報検知を割り当てることができます。

     この方法は、一意に構造化されたユーザー名を持たない環境では誤検知が発生しやすいため、価値の高いユーザー アカウントを保護するためにのみこの方法を使用する必要があります。
3. ファイアウォールが企業の認証情報送信の検知をロギングするために使用する **Valid Username Detected Log Severity (**有効なユーザー名が検知されたログの重大度**)** を設定します（デフォルトは中）。

STEP 4 | URL フィルタリングプロファイルを構成して、ローカルインライン分類を使用してフィッシングや悪意のある JavaScript をリアルタイムで検出します。

STEP 5 | フィッシング認証を防止する資格情報 への URL カテゴリに基づいて、ユーザーがサイトに企業資格情報を送信できないようにすることを許可または禁止します。

マルウェアあるいはフィッシングのコンテンツをホストしていることが一度も判明していないサイトに関連付けられた *App-ID* については、そのカテゴリでチェックを有効にしている場合でも、ファイアウォールは自動的に認証情報の送信のチェックをスキップし、最高のパフォーマンスを維持して誤検出の頻度を下げます。ファイアウォールが認証情報のチェックをスキップするサイトのリストは、アプリケーションおよび脅威コンテンツ更新を通じて自動的に更新されます。

1. **Site Access (**サイト アクセス**)** を許可する各 URL カテゴリについて、**User Credential Submissions (**ユーザー証明書送信**)** をどのように扱いたいか選択します。
   - **alert** – ユーザーが Web サイトに資格情報を送信できるようにしますが、ユーザーがこの URL カテゴリのサイトに資格情報を送信するたびに URL フィルタリング アラート ログを生成します。
   - **allow (**許可**)**（デフォルト）–ユーザーが認証情報を Web サイトに送信することを許可します。
   - **block (**ブロック**)**–アンチフィッシング ブロックページを表示し、ユーザーが認証情報をウェブサイトに送信するのをブロックします。
   - **continue (**続行**)**–Anti Phishing Continue Page（アンチ フィッシング続行ページ）を表示し、サイトにアクセスするユーザーに **Continue**（継続）をクリックするよう求めます。
2. 許可する URL カテゴリに属すウェブサイトに対して行う、企業の認証情報の送信を検知する URL フィルタリング プロファイルを設定します。

STEP 6 | URL カテゴリ例外リスト を定義して、URL カテゴリに関係なく、常にブロックまたは許可される Web サイトを指定します。

たとえば、URL フィルタリング ログを減らすには、企業の Web サイトを許可リストに追加して、それらのサイトのログが生成されないようにしたり、過度に使用されている Web サイトがあり、作業に関連していない場合は、そのサイトをブロック リストに追加できます。

カスタム URL カテゴリ用に構成されたポリシー アクションは、外部動的リスト内の一致する URL よりも優先的に適用されます。

ブロックリストの Web サイトへのトラフィックは、関連付けられたカテゴリのアクションにかかわらず、常にブロックされ、許可リストの URL へのトラフィックは常に許可されます。

適切な形式とワイルドカードの使用方法の詳細については、URL カテゴリ例外リスト のガイドラインを参照してください。

STEP 7 | セーフ サーチの適用を有効化します。

STEP 8 | URL フィルタリング イベントについては、コンテナ ページのみログに記録します。

1. **URL Filtering Settings (URL** フィルタリング設定**)** を選択します。**Log container page only (**コンテナ ページのみロギング**)**（デフォルト）が有効になっており、ファイア

ウォールはコンテナ ページ内にロードされた後続のページまたはカテゴリではなく、カテゴリに一致するメイン ページのみをログに記録します。

2. すべてのページおよびカテゴリのロギングを有効にするには、**Log container page only**（コンテナ ページのみロギング）オプションを無効にします。

STEP 9 | サポートされている 1 つ以上の HTTP ヘッダー フィールドで HTTP ヘッダーのロギングを有効にします。

URL Filtering Settings (URL フィルタリング設定**)** を選択し、ログに記録する以下のフィールドを 1 つ以上選択します。

- ユーザーエージェント
- リファラー
- **X-Forwarded-For (XFF)**

STEP 10 | URL フィルタリング プロファイルを保存し、変更をコミットします。

1. **OK** をクリックします。
2. **Commit**（コミット）をクリックします。

STEP 11 | URL フィルタリングポリシー構成をテストします。

1. 目的の URL カテゴリの Web サイトにアクセスし、ファイアウォールの動作を確認します。

   サイトに直接アクセスしないようにするには、Palo Alto Networks URL Filtering Test Pages (urlfiltering.paloaltonetworks.com/test-***<url-category>***) を使用します。Palo Alto Networksには、良性および悪意のある URL カテゴリの URL をテストしています。たとえば、ブロック ポリシーでマルウェアをテストするには、「https://urlfiltering.paloaltonetworks.com/test-malware」を参照してください。

2. トラフィックおよび URL フィルタリング ログ (**Monitor** > **Logs**) を確認して、正しいポリシー ルールがログに記録されていることを確認します。

STEP 12 | ファイアウォールが URL カテゴリ検索を実行している間、クライアント要求をブロックするには、**Hold client request for category lookup**（カテゴリ検索のクライアント要求を保持）を有効にします。

1. **Device (** デバイス**)** > **Setup (**設定**)** > **Content-ID**の順に選択します。
2. **Hold client request for category lookup**（カテゴリ検索のクライアント要求を保持）を選択します。
3. 変更を Commit (コミット) します。

この機能を URL Filtering best practice（URL フィルタリングのベストプラクティス）として有効にします。

STEP 13 | URL カテゴリ検索がタイムアウトするまでの時間を秒単位でセットします。

1. **Device**（デバイス） > **Setup**（セットアップ） > **Content-ID** > **gear icon**（ギアアイコン）の順に選択します。
2. **Category lookup timeout**（**sec**）（カテゴリ検索タイムアウト（秒））に数値を入力します。
3. <239>OK</239> をクリックします。
4. 変更を Commit (コミット)します。

テスト URL フィルタリング構成

URL Filtering および Advanced URL Filtering ポリシー構成をテストするには、Palo Alto Networks URL Filtering Test Pages を使用します。テスト ページは、Advanced URL Filtering を実行しているファイアウォールにのみ適用されるリアルタイム検出カテゴリを含む、すべての 定義済み URL カテゴリ の安全なテストのために作成されました。

テスト ページが *HTTPS* 接続で動作するようにするには、*SSL* 復号化を有効にする必要があります。

Advanced URL フィルタリング テスト ページには、*URL* に "リアルタイム検出" が含まれており、ファイアウォールが悪意のある *URL* をリアルタイムで正しく分類および分析していることを確認します。他のカテゴリのファイアウォールの動作は検証されません。

特定の *Web* サイトの分類は、*Palo Alto Networks* の *URL* カテゴリ検索ツール Test A Site を使用して確認できます。

URL フィルタリング サブスクリプションに対応する手順に従います。

- URL フィルタリングの確認
- 詳細な URL フィルタリングを確認する

URL フィルタリングの確認

従来の URL Filtering サブスクリプションがある場合は、ファイアウォールがアクセスするカテゴリの URL を正しく分類、適用、およびログに記録することをテストおよび検証します。

STEP 1 | 目的の URL カテゴリの Web サイトにアクセスします。

ブロックされた URL カテゴリのサイトをテストすることを検討してください。test page (urlfiltering.paloaltonetworks.com/test-***<url-category>***) を使用すると、サイトに直接アクセスしないようにすることができます。たとえば、ブロック ポリシーでマルウェアをテストするには、「https://urlfiltering.paloaltonetworks.com/test-malware」を参照してください。

STEP 2 | Traffic ログと URL Filtering ログ (**Monitor** > **Logs**) を確認して、ファイアウォールがサイトを正しく処理していることを確認します。

たとえば、組織のポリシーに違反するサイトにアクセスしたときに表示されるブロック ページを構成した場合は、テスト サイトにアクセスしたときにブロック ページが表示されることを確認します。

詳細な URL フィルタリングを確認する

Advanced URL Filtering サブスクリプションをお持ちの場合は、リアルタイム URL 分析が行われていることをテストして確認します。

*Palo Alto Networks*では、リアルタイム検出アクション設定を設定して、アクティブな*URL*フィルタリングプロファイルに対してアラートを表示することをお勧めします。これにより、リアルタイムで分析された *URL* の可視性が提供され、特定の *Web* 脅威に対して構成されたカテゴリ設定に基づいてブロック (またはポリシー設定に応じて許可) されます。

ファイアウォールは、特定の *URL* の検出された *URL* カテゴリに対して構成されたアクションの最も重大なアクションを実行します。たとえば、*example.com* が、それぞれアラート、ブロック、許可アクションが設定されたカテゴリであるリアルタイム検出、コマンドアンドコントロール、ショッピングに分類されるとします。ブロックは検出されたカテゴリからの最も重大なアクションであるため、ファイアウォールは *URL* をブロックします。

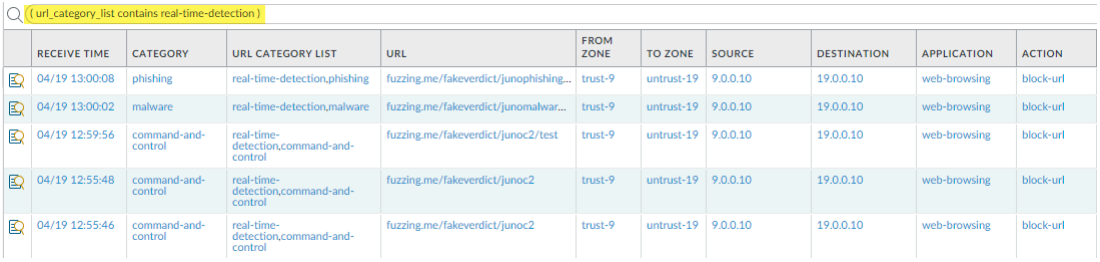
STEP 1 | 次の各テスト URL にアクセスして、Advanced URL Filtering サービスが URL を正しく分類していることを確認します。

- マルウェア-urlfiltering.paloaltonetworks.com/test-real-time-detection-malware
- フィッシング-urlfiltering.paloaltonetworks.com/test-real-time-detection-phishing
- **C2**-urlfiltering.paloaltonetworks.com/test-real-time-detection-command-and-control
- グレーウェア-urlfiltering.paloaltonetworks.com/test-real-time-detection-grayware
- 良性 (不明)-urlfiltering.paloaltonetworks.com/test-real-time-detection

STEP 2 | ファイアウォールのアクティビティをモニターして、テストされたURLがリアルタイム検出として正しく分類されていることを確認します。

1. **Monitor** > **Logs** > **URL** フィルタリング を選択し、(`url_category_list`には `real-time-detection` が含まれています) でフィルタリングして、Advanced URL Filtering を使用して分析されたログを表示します。

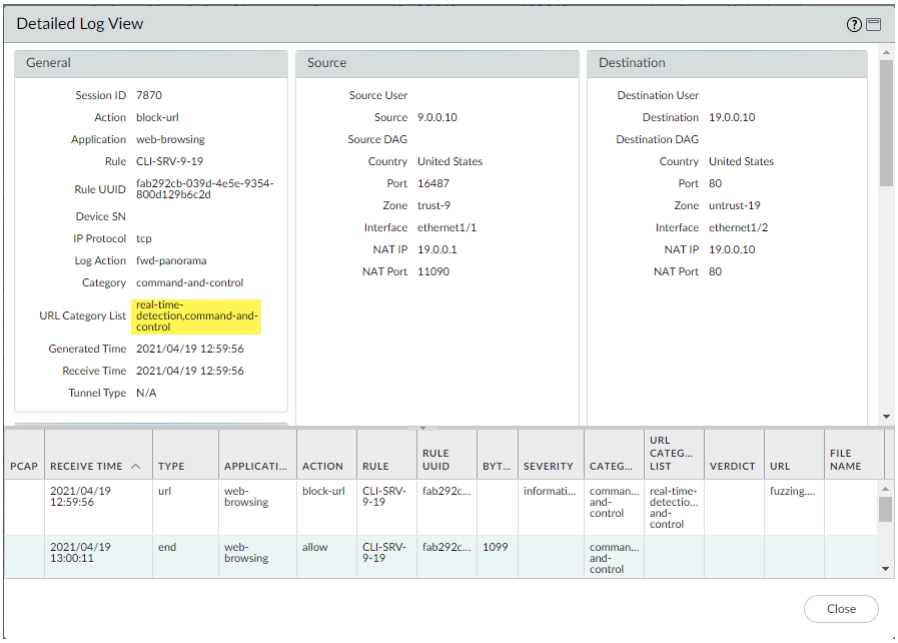
   追加の Web ページカテゴリの一致も表示され、PAN-DB で定義されているカテゴリに対応します。

2. ログを詳しく見て、各種類の Web の脅威が正しく分析され、分類されていることを確認します。

   次の例では、URL は real-time で分析され、コマンド・アンド・コントロール (C2) として定義する特徴を持っているものとして分類されます。C2 カテゴリにはリアルタイ

ム検出よりも厳しいアクションが関連付けられているため (アラートではなくブロック)、URL はコマンド アンド コントロールに分類され、ブロックされます。



インライン分類の設定

URL フィルタリングのインライン分類設定を有効にするには、インライン分類設定で構成された URL フィルタリングプロファイルをセキュリティポリシールールにアタッチします (基本的なセキュリティ ポリシーのセットアップ を参照)。

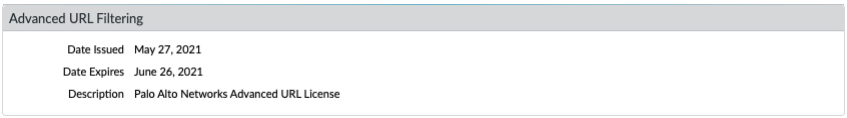
URL フィルタリングのローカル インライン分類は、*VM-50* または *VM50L* 仮想アプライアンスでは現在サポートされていません。

STEP 1 | PAN-OS Web インターフェイスにログインします。

STEP 2 | インライン分類を利用するには、アクティブな Advanced URL Filtering が必要です。

ローカルのインライン分類は、従来の *URL Filtering* サブスクリプションの既存の所有者である場合に有効にできます。

高度な URL フィルタリング サブスクリプションがあることを確認します。現在アクティブなライセンスがあるサブスクリプションを確認するには、**Device** > **Licenses** を選択し、適切なライセンスが使用可能で有効期限が切れていないことを確認します。

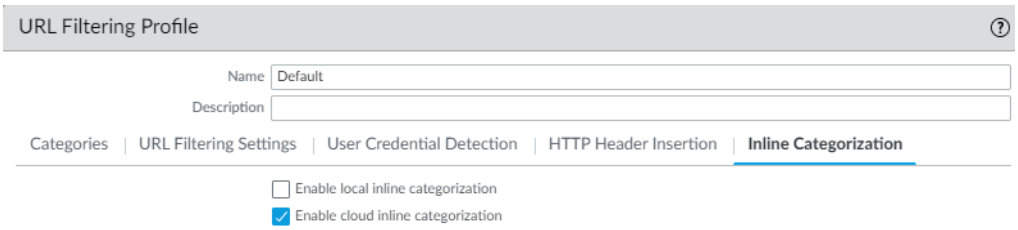


STEP 3 | 新しい URL Filtering Security プロファイルを更新または作成して、クラウドのインライン分類を有効にします。

ローカルおよびクラウドのインライン分類で使用されるポリシーアクションは、***Categories*** タブで構成されている設定によって異なります。

1. 既存の **URL** フィルタリング プロファイル または を選択して 新しいものを追加します (オブジェクト > セキュリティ プロファイル > **URL** フィルタリング)。
2. URL Filtering プロファイルを選択し、**Inline Categorization** に移動し、デプロイするインライン分類メソッドを有効にします。
   - クラウド インライン分類を有効にする — 疑わしい Web ページのコンテンツをリアルタイムで分析し、標的型フィッシング攻撃や高度な回避手法を使用するその他の Web ベースの攻撃など、ゼロデイ Web 攻撃からユーザーを保護するクラウドベースのインライン ディープ ラーニング エンジン。

- ローカルのインライン分類を有効にする – 機械学習技術を使用して、Web ページに埋め込まれた JavaScript エクスプロイトやフィッシング攻撃の悪意のある亜種を防止する firewall ベースの検出エンジン。

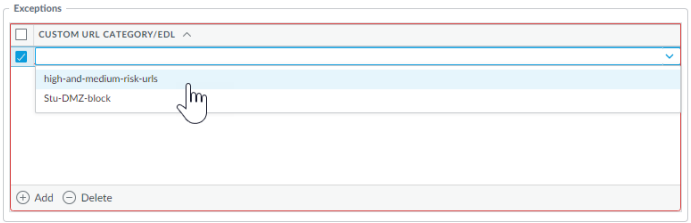


3. **OK** をクリックして URL フィルタリング プロファイルの設定ダイアログを終了し、変更内容を **Commit (コミット)** します。

STEP 4 | (オプション) 誤検知が発生した場合は、URL フィルタリング セキュリティ プロファイルに URL の例外を追加します。URL Filtering プロファイルで外部動的リストまたはカスタム URL カテゴリ リストを指定することで、例外を追加できます。指定された例外は、クラウドとローカルのインライン分類の両方に適用されます。

カスタム *URL* カテゴリ *(**Objects** > **Custom Objects** > **URL** カテゴリ)* にエントリを追加する他のメカニズムによって作成された *URL* 例外も、インライン分類の例外として機能します。

1. **[Objects] > [セキュリティ プロファイル] > [URL フィルタリング]** の順に選択します。
2. 特定の URL を除外する URL Filtering プロファイルを選択し、**Inline Categorization** を選択します。
3. **Add** をクリックして、既存の URL ベースの外部動的リストまたはカスタム URL カテゴリを選択します。使用可能なものがない場合は、それぞれ新しい external dynamic list または Custom URL Category を作成します。



4. **OK** をクリックして URL フィルタリング プロファイルを保存し、変更を **Commit (コミット)** コミットします。

STEP 5 | (Optional)インライン分類サービス要求を処理するために firewall によって使用される Cloud Content Fully Qualified Domain Name (FQDN) を設定します。既定の FQDN は hawkeye.services-edge.paloaltonetworks.com に接続し、最も近い cloud サービス サーバーに

解決されます。自動サーバー選択をオーバーライドするには、データの常駐性とパフォーマンスの要件に最も適した地域の cloud コンテンツサーバーを指定します。

Cloud Content FQDN はグローバルに使用されるリソースであり、この接続に依存する他のサービスがトラフィックペイロードを送信する方法に影響します。

ファイアウォールがお住まいのリージョンに対して正しい Content Cloud FQDN (**Device** > **Setup** > **Content-ID** > **Content Cloud Setting**) を使用していることを確認し、必要に応じて FQDN を変更します。

- US—**us.hawkeye.services-edge.paloaltonetworks.com**
- EU—**eu.hawkeye.services-edge.paloaltonetworks.com**
- UK — **uk.hawkeye.services-edge.paloaltonetworks.com**

  英国ベースのクラウド コンテンツ *FQDN* は、*EU (eu.hawkeye.services-edge.paloaltonetworks.com)* にあるバックエンド サービスに接続することにより、高度な *URL* フィルタリングのインライン分類サービス サポートを提供します。
- APAC—**apac.hawkeye.services-edge.paloaltonetworks.com**

STEP 6 | (Optional)インライン分類サーバーへの firewall の接続状況を確認します。

1. ml.service.paloaltonetworks.com サーバーは、クラウドおよびローカルのインライン分類の操作に関連する firewall ベースのコンポーネントの定期的な更新を提供します。

   接続ステータスを表示するには、ファイアウォール上で次のCLIコマンドを実行します。

   ```
   mlav クラウドの状態を表示する
   ```

   以下に例を示します。

   ```
   sow mlav cloud-status MLAV cloud Current cloud server:
    ml.service.paloaltonetworks.com Cloud connection: connected
   ```

   インライン ML クラウド サービスに接続できない場合は、次のドメインがブロックされていないことを確認してください: ml.service.paloaltonetworks.com.

2. hawkeye.services-edge.paloaltonetworks.com サーバーは、クラウドのインライン分類によってサービス要求を処理するために使用されます。

   接続ステータスを表示するには、ファイアウォール上で次のCLIコマンドを実行します。

   ```
   show ctd-agent status security-client
   ```

   以下に例を示します。

   ```
   show ctd-agent status security-client ...Security
    Client AceMlc2(1) 現在の cloud サーバ: hawkeye.services-
   edge.paloaltonetworks.com Cloud 接続: 接続 ...
   ```

   CLI 出力は簡潔にするために短縮されました。

   Advanced URL Filtering クラウド サービスに接続できない場合は、次のドメインがブロックされていないことを確認します: hawkeye.services-edge.paloaltonetworks.com。

STEP 7 | 高度な URL Filtering クラウド サービスへの認証に使用される更新された firewall デバイス証明書をインストールします。クラウドのインライン分類が有効になっているすべての firewall について、この手順を繰り返します。

STEP 8 | (Optional—Cloud 分類のみ)次のテスト URL にアクセスして、Advanced URL Filtering サービスがクラウド インライン分類によって検出された URL を適切に分類していることを確認します。

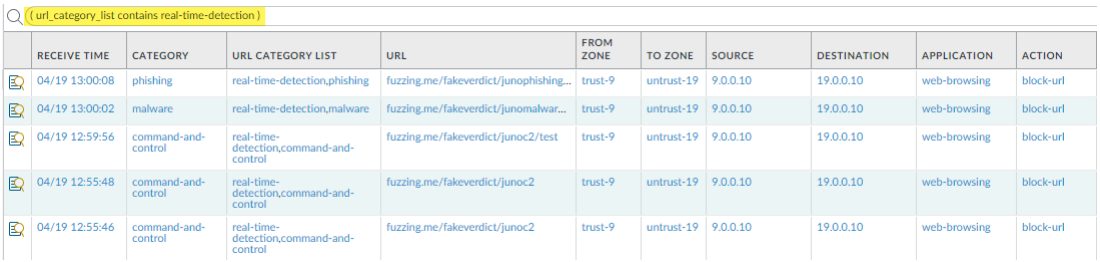
- **Malware**—urlfiltering.paloaltonetworks.com/query-real-time-content-detection-malware
- **Phishing**—urlfiltering.paloaltonetworks.com/query-real-time-content-detection-phishing
- **C2**—urlfiltering.paloaltonetworks.com/query-real-time-content-detection-command-and-control
- **Grayware**—urlfiltering.paloaltonetworks.com/query-real-time-content-detection-grayware

STEP 9 | (Optional)firewall のアクティビティーをモニターして、テスト済みの URL がリアルタイム検出として正しく分類されていることを確認します。

real-time-detection として分類される *URL* には、ローカルのインライン分類 *(URL Filtering* インライン *ML)* とクラウドのインライン分類の両方によって分析されたコンテンツが含まれます。

1. **Monitor** > **Logs** > **URL** フィルタリング を選択し、`(url_category_list`には `real-time-detection` が含まれています`)` でフィルタリングして、Advanced URL Filtering を使用して分析されたログを表示します。

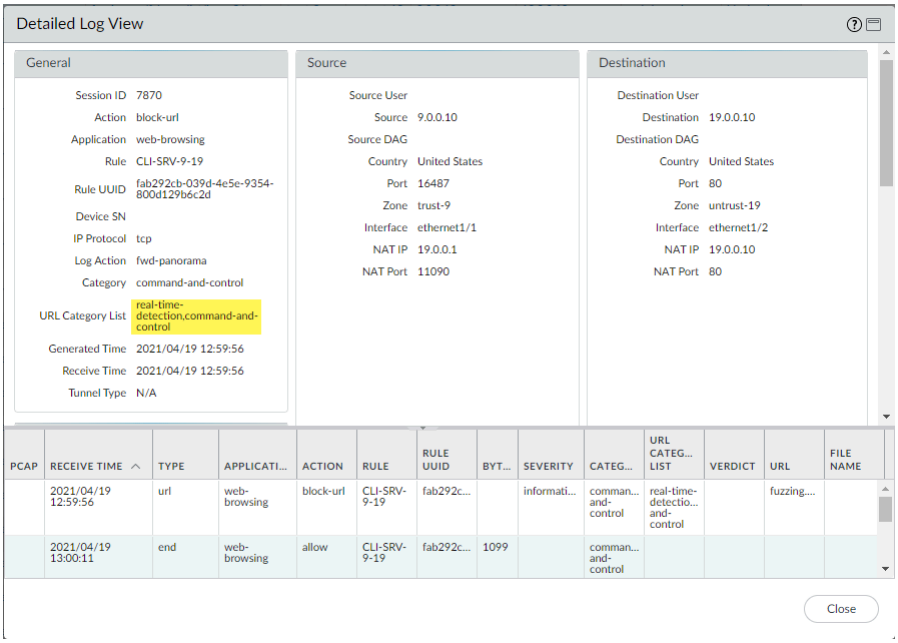
   追加の Web ページカテゴリの一致も表示され、PAN-DB で定義されているカテゴリに対応します。



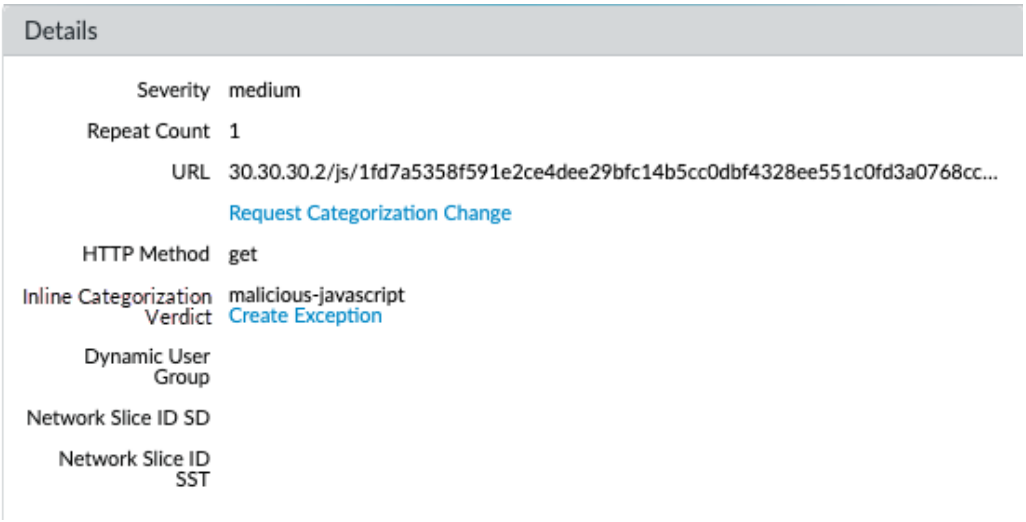
2. ログを詳しく見て、各種類の Web の脅威が正しく分析され、分類されていることを確認します。

   次の例では、URL は real-time で分析され、コマンド・アンド・コントロール (C2) として定義する品質を持っているものとして分類されます。C2 カテゴリにはリアルタイ

ム検出よりも厳しいアクションが関連付けられているため (アラートではなくブロック)、URL はコマンド アンド コントロールに分類され、ブロックされます。



3. **Inline Categorization Verdict** は、詳細ログ ビューの **Details** ペインの下に表示されます。ローカルのインライン分類によって脅威が含まれていると判断された Web ページは、**phishing** または **malicious-javascript** の判定で分類されます。クラウドのインライン分類された評決は、**cloud** と表示されます。



Web アクティビティのモニター

ACC と URL フィルタリング ログおよびレポートには、**alert** [アラート]、**block** [ブロック]、**continue** [続行]、**override** [オーバーライド]に設定されている URL カテゴリのすべてのユーザーの Web アクティビティが表示されます。ログをモニターすることにより、Web アクセス ポリシーを特定するためのユーザー ベースの Web アクティビティをより詳しく理解することができます。

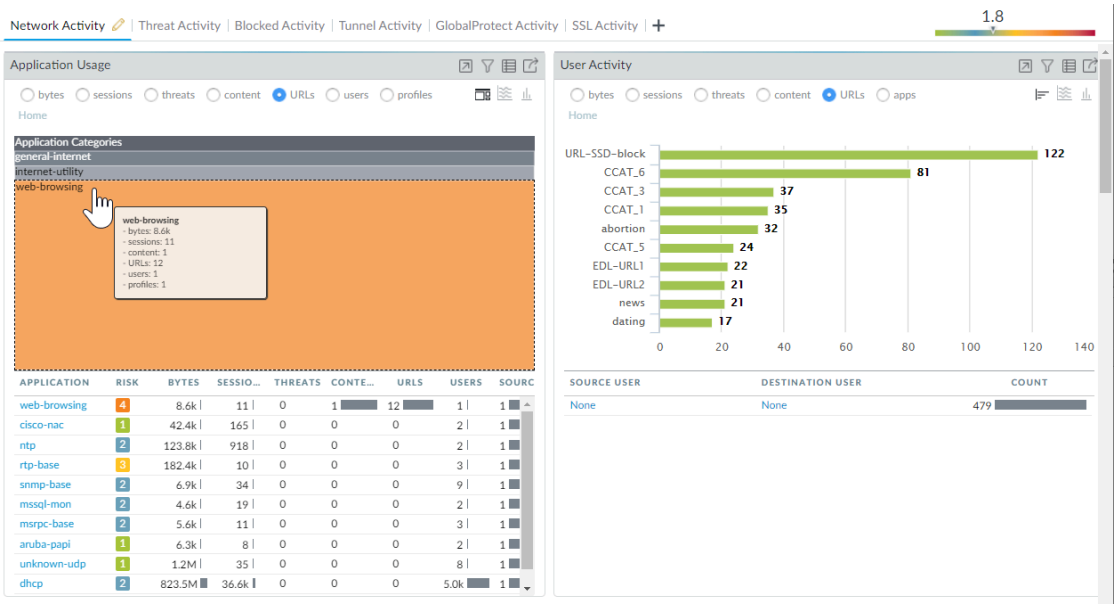
以下のトピックでは、Web アクティビティをモニターする方法を説明します。

- ネットワーク ユーザーの Web アクティビティのモニター
- ユーザー アクティビティ レポートの表示
- カスタム URL フィルタリング レポートの設定

ネットワーク ユーザーの Web アクティビティのモニター

アプリケーション コマンド センター (ACC)、URL フィルタリング レポート、およびファイアウォールで生成されたログを使用して、ユーザーのアクティビティを追跡できます。

使用する環境でユーザーが最もよくアクセスしているカテゴリをすばやく把握するには、**ACC** ウィジットを確認します。大抵の **Network Activity (**ネットワーク アクティビティ**)** ウィジェットは、URL で並び替えられるようになっています。たとえば、Application Usage （アプリケーション使用率）ウィジットの場合、最もアクセスされているカテゴリは networking カテゴリで、その次に encrypted tunnel と ssl が続きます。**Threat Activity** [脅威アクティビティ]と **Blocked Activity** [ブロックされたアクティビティ]のリストも URL でソートして表示できます。



ログを表示してログ オプションを設定します：

ACC から直にログ（）にジャンプするか、**Monitor (監視)** > **Logs (ログ)** > **URL Filtering (URL フィルタリング)** を選択できます。

各エントリのログ アクションは、該当するカテゴリ用に定義したサイト アクセス設定によって異なります。

- アラート ログ—この例では、computer-and-internet-info カテゴリがアラートに設定されています。

	RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
	2020/04/16 14:10:53	computer-and-internet-info	outlook.office36...	pm wifi	UNTRUST				outlook-web-online	alert

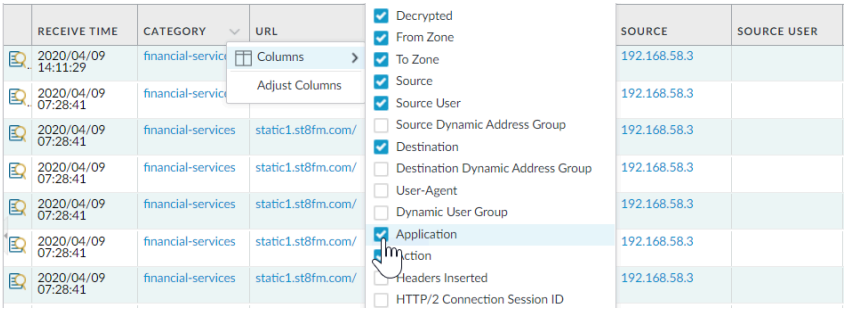
- ブロック ログ—この例では、insufficient-content カテゴリが続行するよう設定されています。そうではなくブロックするようにカテゴリが設定されていた場合、ログの Action (アクション) は block-url になります。

	RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
	2020/04/08 18:47:49	insufficient-content	munchkin.mark...	pm wifi	UNTRUST				ssl	block-continue

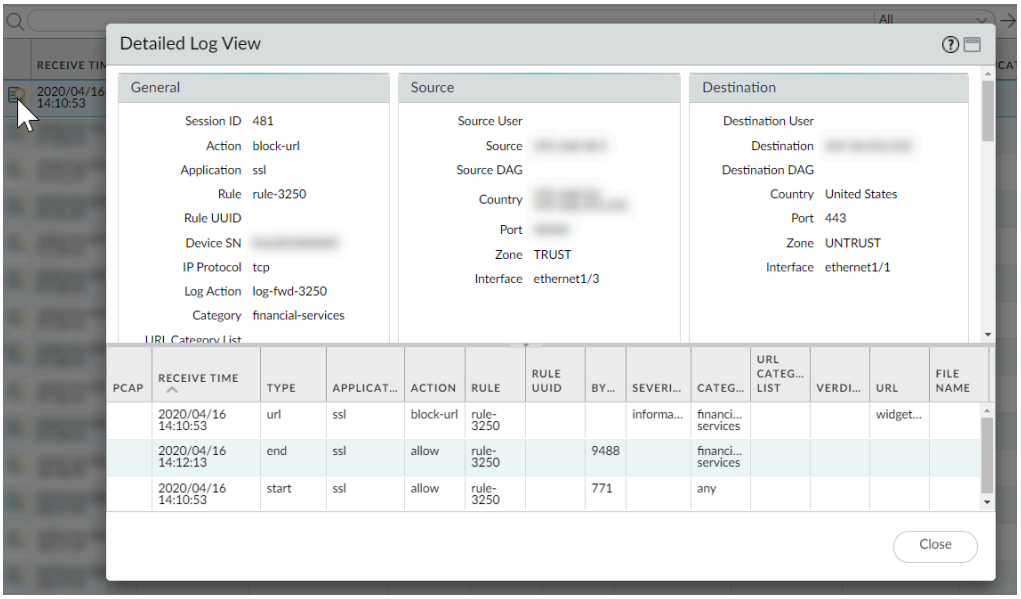
- 暗号化されたウェブサイトでアラート ログ—この例では、カテゴリは private-ip-addresses であり、アプリケーションは web-browsing です。このログは、ファイアウォールがトラフィックを復号化したことも示します。

	RECEIVE TIME	CATEGORY	URL	DECRYPTED	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
	2020/04/09 14:11:29	private-ip-addresses	/Updates/Updat...	yes	TRUST	UNTRUST	192.168.58.3			web-browsing	alert

また、送信元ゾーンと宛先ゾーン、コンテンツ タイプ、およびパケット キャプチャを実行するかどうかなどの複数の列を URL フィルタリングのログ ビューに追加することもできます。表示する列を変更するには、任意の列の下向き矢印をクリックし、表示する属性を選択します。

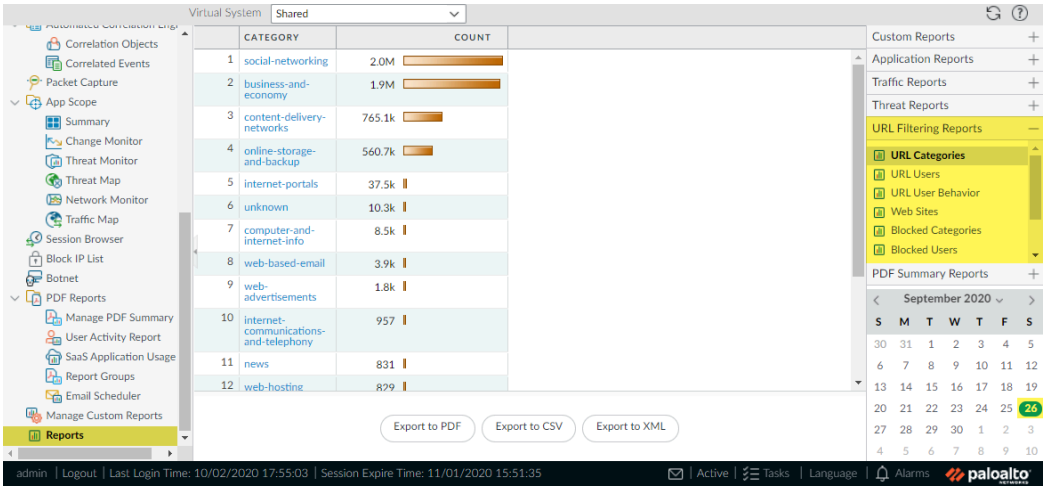


アクセスした特定の URL の完全なログの詳細またはカテゴリの変更要求、あるいはその両方を表示するには、ログの最初の列のログ詳細アイコンをクリックします。



URL カテゴリ、URL ユーザー、アクセスされたウェブサイト、ブロックするカテゴリなどに関する事前定義済みの URL フィルタリング レポートを生成します。

Monitor (監視) > **Reports (レポート)** を選択し、**URL Filtering Reports (URL フィルタリング レポート)** セクションでいずれかのレポートを選択します。レポートには、カレンダーで選択した日付の 24 時間分のデータが含まれます。レポートを PDF、CSV、または XML にエクスポートすることもできます。



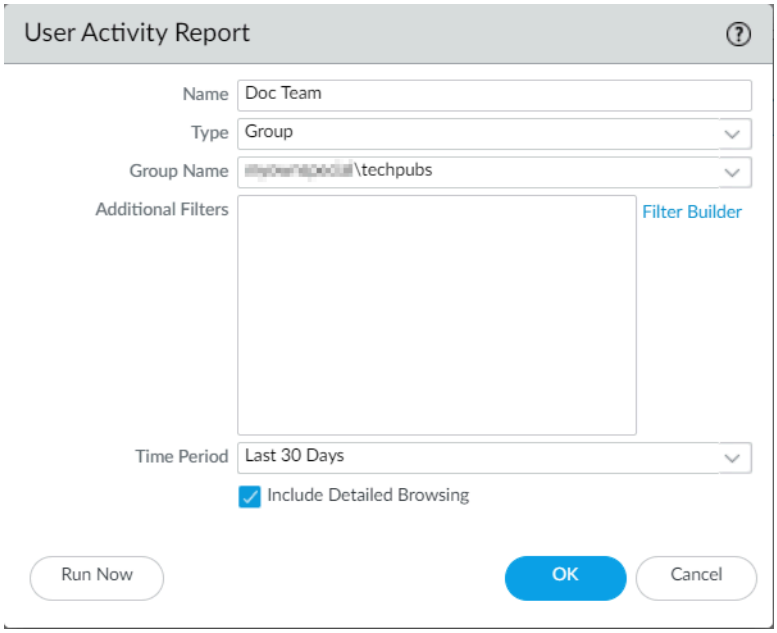
ユーザー アクティビティ レポートの表示

このレポートでは、ユーザー アクティビティ、グループ アクティビティを迅速に表示し、閲覧時のアクティビティを表示するオプションを提供します。

STEP 1 | ユーザー アクティビティ レポートを設定します。

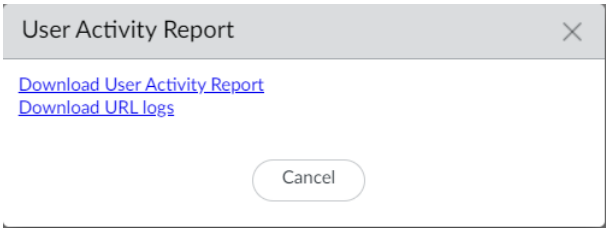
1. **Monitor (監視)** > **PDF Reports (PDF レポート)** > **User Activity Report (ユーザー アクティビティ レポート)** の順に選択します。
2. レポートを **Add (追加)** してその **Name (名前)** を入力します。
3. 次の中からレポートの **Type (タイプ)** を選択します。
   - 一人分のレポートを生成するには、**User (ユーザー)** を選択します。
   - 複数のユーザーを対象にする場合は **Group (グループ)** を選択します。

   ユーザー名またはグループ名を選択するには、*User-ID* を にする必要があります。*User-ID* が設定されていない場合は、*[ユーザー]* タイプを選択して、ユーザーのコンピュータの *IP* アドレスを入力します。
4. ユーザー レポートの**Username/IP Address (ユーザー名/IP アドレス)**を入力するか、ユーザー グループ レポートのグループ名を入力します。
5. 期間を選択します。既存の期間または、**[カスタム]** を選択できます。
6. 閲覧情報をレポートに表示できるように **[Include Detailed Browsing]** チェックボックスをオンにします。



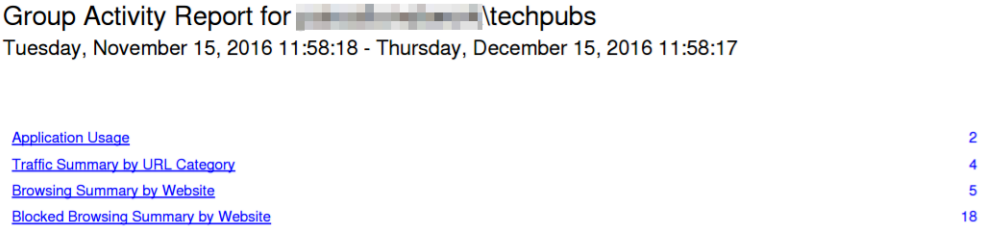
STEP 2 | レポートを実行します。

1. **[今すぐ実行]** をクリックします。
2. ファイアウォールがレポートの生成を完了させたら、いずれかのリンクをクリックしてそれをダウンロードします。
   - **Download User Activity Report (**ユーザー アクティビティ レポートをダウンロード**)** をクリックすると、PDF 版のレポートをダウンロードできます。
   - 対応するログ エントリの CSV ファイルをダウンロードするには、**Download URL Logs (URL** ログをダウンロード**)** をクリックします。

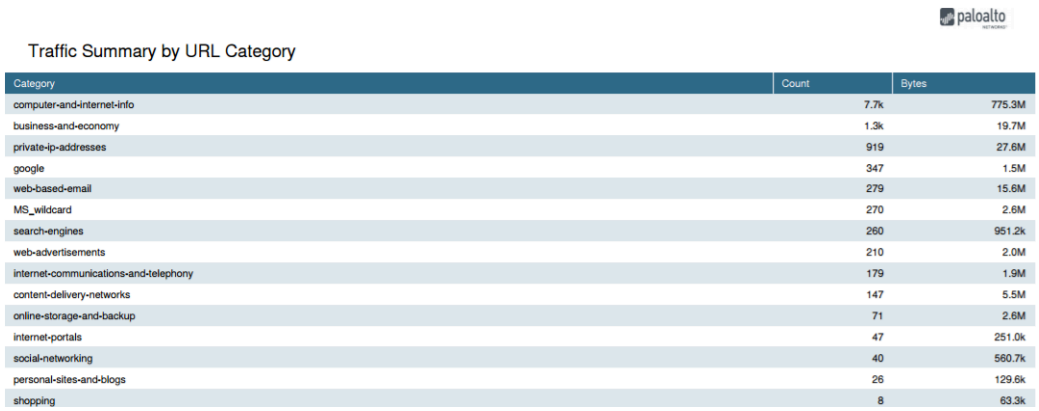


3. レポートをダウンロードした後、**Cancel (**キャンセル**)** をクリックします。
4. ユーザー アクティビティ レポートの設定を保存し、同じレポートを後で実行できるようにしたい場合は **OK** をクリックします。そうでない場合は **Cancel (**キャンセル**)** をクリックします。

STEP 3 | ダウンロードしたファイルを開いて、ユーザー アクティビティ レポートを確認します。PDF 版のレポートには、レポートの基準にしたユーザーあるいはグループ、レポート期間、目次が記載されています。


Group Activity Report for [redacted]\techpubs
Tuesday, November 15, 2016 11:58:18 - Thursday, December 15, 2016 11:58:17

STEP 4 | 目次の項目をクリックして、レポートの詳細を表示します。たとえば、Traffic Summary by URL Category （URL カテゴリ別トラフィックサマリー）をクリックして、選択されたユーザーまたはグループの統計情報を表示します。


paloalto

Traffic Summary by URL Category

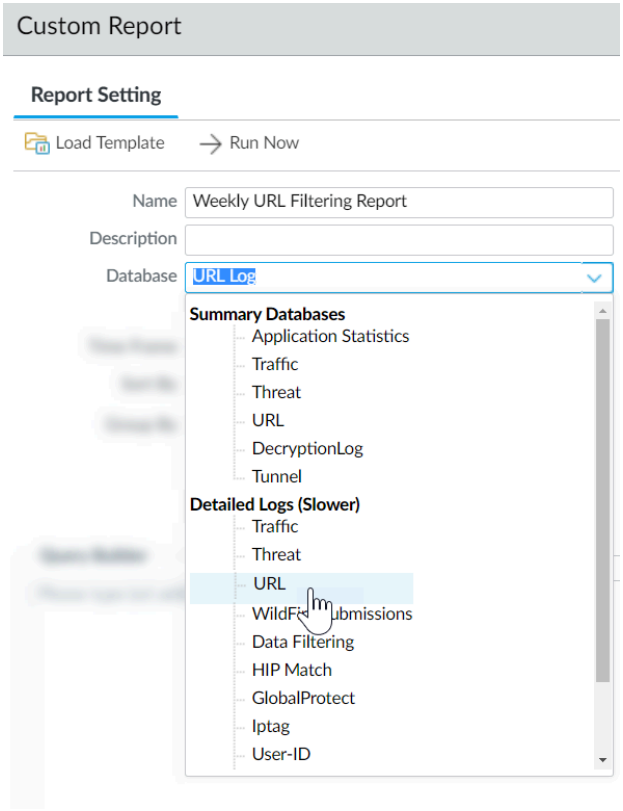
Category	Count	Bytes
computer-and-internet-info	7.7k	775.3M
business-and-economy	1.3k	19.7M
private-ip-addresses	919	27.6M
google	347	1.5M
web-based-email	279	15.6M
MS_wildcard	270	2.6M
search-engines	260	951.2k
web-advertisements	210	2.0M
internet-communications-and-telephony	179	1.9M
content-delivery-networks	147	5.5M
online-storage-and-backup	71	2.6M
internet-portals	47	251.0k
social-networking	40	560.7k
personal-sites-and-blogs	26	129.6k
shopping	8	63.3k

カスタム URL フィルタリング レポートの設定

スケジュールを指定して定期的に実行できる詳細なレポートを生成するためには、カスタム URL フィルタリング レポートを設定します。レポートの基準にする URL フィルタリング ログの各フィールドは、自由に選択して組み合わせることができます。

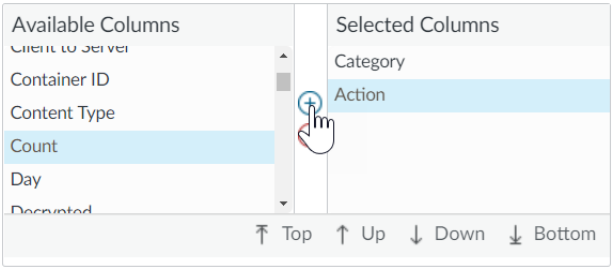
STEP 1 | 新しいカスタム レポートを追加します。

1. **Monitor (監視)** > **Manage Custom Reports (カスタム レポートの管理)** を選択してレポートを **Add (追加)** します。
2. レポートに一意の **Name (名前)** を付け、任意で **Description (説明)** を加えます。
3. レポートを生成するために使用する **Database (データベース)** を選択します。詳細な URL フィルタリング レポートを生成するためには、Detailed Logs (詳細ログ) セクションで **URL** を選択します。

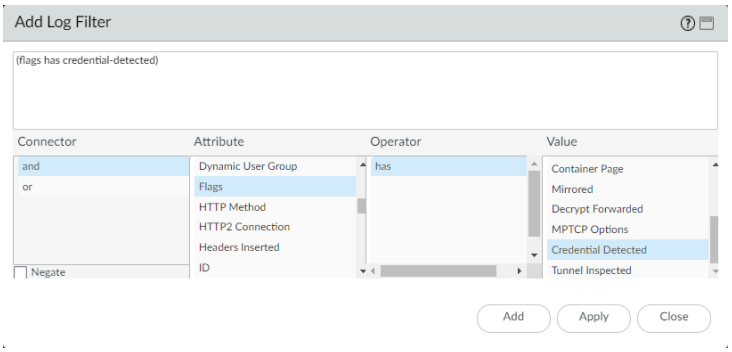


STEP 2 | レポート オプションを設定します。

1. 定義済みの **Time Frame (期間)** あるいは **Custom (カスタム)** を選択します。
2. Available Columns (利用可能な列) リストから、レポートに含めるログの列を選択し、それらを Selected Columns (選択済みの列) に追加します（⊕）。例えば、URL Filtering (URL フィルタリング) レポートについては、次のような選択を行う可能性があります。
   - Action（アクション）
   - アプリケーション カテゴリ
   - カテゴリ
   - 宛先国
   - Source User （送信元ユーザー）
   - URL

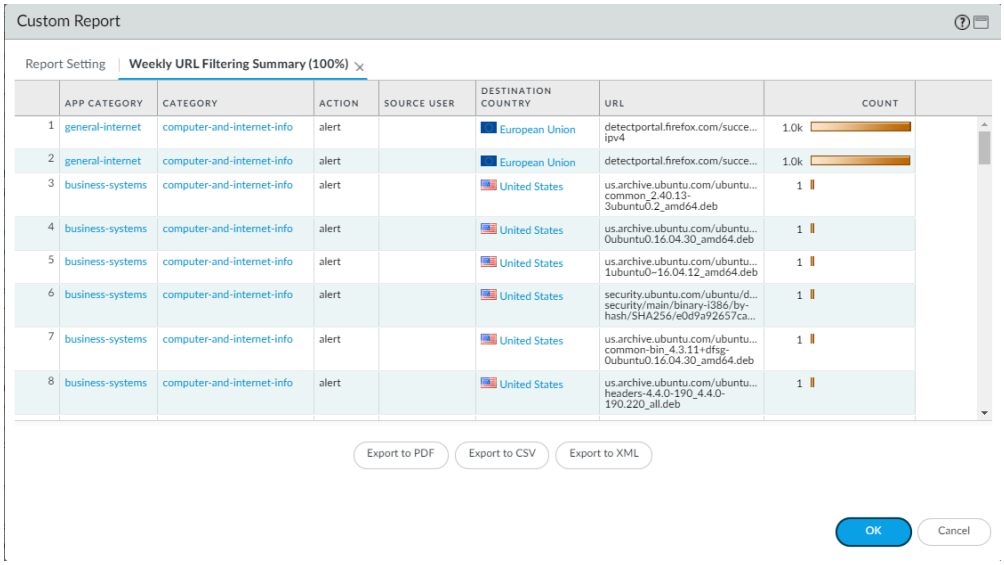


3. ファイアウォールが に対して に設定されている場合は、属性 フラグ 、オペレーター が 、値 の資格情報が検出された を選択して、ユーザーが有効な企業資格情報をサイトに送信したときに記録されるイベントをレポートに含めます。



4. （任意）**Sort By (ソート基準)** オプションを選択し、レポートの詳細を集約するために使用する属性を設定します。ソート基準にする属性を選択しないと、レポートには集約情報なしで最初の N 件の結果が返されます。データのグループ化時にアンカーとして使用する **Group By (グループ化基準)** 属性を選択します。次の例は、**Group By (グルー**

プ化基準) を **App Category** (アプリ カテゴリ) に、**Sort By** (ソート基準) を **Top 5** (トップ 5) の **Count** (カウント) に設定したレポートの例です。



STEP 3 | レポートを実行します。

1. 新しいタブに表示されるレポートをすぐに生成するには、**Run Now** (今すぐ実行) アイコンをクリックします。
2. レポートのレビューが完了したら **Report Setting** (レポート設定) タブに戻り、設定を調整するか、再びレポートを実行するか、次のステップに進んでレポートのスケジュール設定を行います。
3. **Schedule** (スケジュール) チェックボックスを選択し、1 日に一度レポートを実行します。直近の 24 時間の Web アクティビティの詳細に関する日次レポートが作成されます。

STEP 4 | 設定を **Commit**（コミット）します。

STEP 5 | カスタム レポートを表示します。

1. **Monitor** (監視) > **Logs** (ログ)を選択します。
2. 右の列にある **Custom Reports** (カスタム レポート) ペインを開き、表示したいレポートを選択します。最新のレポートが自動的に表示されます。
3. 以前の日付のレポートを表示するためには、カレンダーからその日付を選択します。レポートを PDF、CSV、または XML にエクスポートすることもできます。

ユーザーがアクセスしたページのみを記録

コンテナ ページは、Web サイトを訪れるときにユーザーがアクセスするメインのページです。ただし、メインのページと共に追加のページがロードされる場合があります。URL フィルタリング プロファイルで の [ログ コンテナー ページのみ] オプションが有効になっている場合 (オブジェクト > セキュリティ プロファイル > **URL** フィルタリング)、メイン コンテナ ページのみがログに記録され、コンテナ ページ内に読み込まれる後続のページはログに記録されません。URL フィルタリングではログ エントリが多数生成される可能性があるため、要求されたページ ファイル名が特定の MIME タイプに一致する URI のみがログ エントリに格納されるように、このオプションを有効にすることをお勧めします。デフォルトのセットには、以下の MIME タイプが含まれています。

- application/pdf
- application/soap+xml
- application/xhtml+xml
- text/html
- text/plain
- text/xml

> ***Log*** コンテナ ページのみ オプションを有効にすると、ウイルス対策または脆弱性の保護によって検出された脅威に対して、関連する ***URL*** ログ エントリが常に存在するとは限りません。

カスタム URL カテゴリの作成

カスタム URL フィルタリングオブジェクトを作成して、URL カテゴリの適用に対する例外を指定し、複数の URL カテゴリに基づいてカスタム URL カテゴリを作成できます。

- **URL** カテゴリの強制に対する例外を定義する - セキュリティ ポリシー ルールで一致条件として使用する URL のカスタム リストを作成します。これは、特定の URL をそれが属す URL カテゴリとは別に適用したい場合に、URL カテゴリに対する例外を指定する際に良い方法になります。たとえば、`social-networking` カテゴリをブロックし、LinkedIn へのアクセスを許可したい場合があります。
- 複数の **PAN-DB** に基づいてカスタム **URL** カテゴリを定義—一連のカテゴリにマッチするウェブサイトに絞って適用させることができます。ウェブサイトあるいはページは、カスタム カテゴリの一部として定義されたすべてのカテゴリにマッチしなければなりません。

  たとえば、PAN-DB では、エンジニアが調査に使用する開発者ブログを `personal-sites-and-blogs`、`computer-and-internet-info`、および `high-risk` に分類できます。エンジニアがブログや類似の Web サイト ***and*** にアクセスしてこれらの Web サイトを表示できるようにするには、3 つのカテゴリに基づいてカスタム URL カテゴリを作成し、URL Filtering プロファイルで警告するカテゴリに サイト アクセス を設定します。

次の手順に従ってカスタム URL カテゴリを作成し、firewall でカスタム URL カテゴリを適用する方法を定義します。

STEP 1 | **Objects (**オブジェクト**)** > **Custom Objects (**カスタム オブジェクト**)** > **URL Category (URL** カテゴリ**)**を選択します。

STEP 2 | **Add** またはカスタム URL カテゴリを変更し、カテゴリに説明的な **Name** を指定します。

STEP 3 | カテゴリの **Type (**タイプ**)** を **Category Match (**カテゴリ一致**)** あるいは **URL List (URL** リスト**)** のいずれかに設定します：

- **URL List (URL** リスト**)**—属する対象の URL カテゴリとは別に適用したい URL を追加します。このリスト・タイプを使用して、URL カテゴリーの適用に対する例外を定義したり、URL のリストをカスタム・カテゴリーに属するものとして定義したりします。URL

リスト エントリの作成に関するガイドラインについては、URL Category Exceptions を参照してください。

デフォルトでは、*firewall* は、末尾のスラッシュまたはアスタリスク (*) で終わらないドメイン・エントリー (***example.com***) に、末尾のスラッシュ (/) を自動的に追加します。末尾のスラッシュは、*firewall* がドメインの右側に暗黙のアスタリスクを仮定するのを防ぎます。ワイルドカード以外のドメインエントリでは、末尾のスラッシュ制限は、指定されたドメインとそのサブディレクトリと一致します。たとえば、***example.com*** (処理後の ***example.com/***) は、それ自体と ***example.com/search*** と一致します。

ワイルドカード・ドメイン項目 (アスタリスクまたはキャレットを使用する項目) では、末尾のスラッシュ制限は、指定されたパターンに準拠する *URL* と一致します。たとえば、エントリ ****.example.com*** に一致させるには、*URL* は厳密に *begin* を *1* つ以上のサブドメインで、ルート ドメイン ***example.com*** で終わる必要があります。***news.example.com*** は一致しますが、***example.com*** はサブドメインがないためではありません。

末尾にスラッシュを手動で追加して、*URL* リストを調べるすべてのユーザーに対して、エントリの意図された一致動作を明確にすることをお勧めします。末尾のスラッシュは、*firewall*によって追加されると見えなくなります。URL Category Exceptions では、末尾のスラッシュと一致の動作についてさらに詳しく説明します。

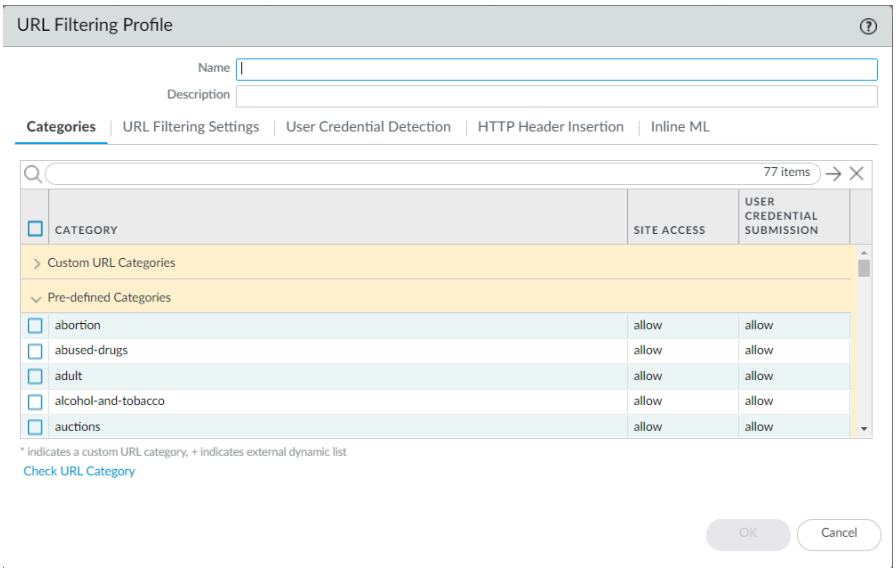
この機能を無効にするには、***Device*** > ***Setup*** > ***Content-ID*** > ***URL*** フィルタリング に進みます。次に、***Append Ending Token*** の選択を解除します。この機能を無効にすると、意図したよりも多くの *URL* へのアクセスをブロックまたは許可する可能性があります。URL Category Exceptions*(PAN-OS 10.1* 以前*)* では、この機能が無効になっている場合の *firewall* の動作について説明します。

- **Category Match (**カテゴリ一致**)**—一連のカテゴリにマッチするウェブサイトに絞って適用します。Web サイトまたはページは、カスタム カテゴリで定義されているカテゴリ *all* と一致する必要があります。

STEP 4 | **OK** をクリックしてカスタム URL カテゴリを保存します。

STEP 5 | Select **Objects (オブジェクト)** > **Security Profiles (セキュリティプロフィール)** > **URL Filtering (URLフィルタリング)**を選択し、URLフィルタリングプロファイルを**Add**（追加）または変更します。

新しいカスタム カテゴリが **Custom URL Categories** の下に表示されます。



STEP 6 | カスタム URL カテゴリに サイト アクセス と のユーザー資格情報送信 を適用する方法を決定します。(ユーザーが会社の資格情報を送信できるサイトを制御するには、Prevent Credential Phishing を参照してください。

STEP 7 | URL Filtering プロファイルを Security ポリシールールにアタッチして、そのルールに一致するトラフィックを適用します。

[ポリシー > セキュリティ > アクション] を選択し、更新した URL フィルタリング プロファイルに基づいてトラフィックを適用するセキュリティ ポリシー ルールを指定します。変更を忘れずに **Commit (コミット)** してください。

カスタム *URL* カテゴリを *Security* ポリシールールの一致条件として使用することもできます。この場合、*URL Filtering* プロファイルで *URL* カテゴリのサイトアクセスを定義しません。カスタム カテゴリを作成したら、カスタム *URL* カテゴリを追加する *Security* ポリシー ルールに移動します (***Policies* > *Security***)。次に、***Service/URL Category*** を選択して、カスタム *URL* カテゴリをルールの一致条件として使用します。

URL カテゴリの例外

URL カテゴリの適用から特定の Web サイトを除外して、URL カテゴリに関連付けられたポリシー アクションに関係なく、これらの Web サイトがブロックまたは許可されるようにすることができます。たとえば、ソーシャル ネットワーキング URL カテゴリをブロックし、LinkedIn へのアクセスを許可する場合があります。URL カテゴリ ポリシーの適用に対する例外を作成するには、次の手順を実行します。

- ブロックまたは許可するサイトの IP アドレスまたは URL を、タイプ **URL リスト** (**Objects** > **Custom Objects** > **URL Category**) のカスタム URL カテゴリ に追加します。次に、URL フィルタリング プロファイルでカテゴリのサイト アクセスを定義します。最後に、プロファイルをセキュリティ ポリシー ルールにアタッチします。

  また、カスタム ***URL*** カテゴリを *Security* ポリシー規則 (***Policies*** > ***Security*** の一致条件として使用し、***Service/URL Category*** を選択することもできます。例外ルールは、***URL*** 例外が属するカテゴリをブロックまたは許可するルールの上に必ず配置してください。

- ブロックまたは許可するサイトのURLを、**URL**リスト（オブジェクト > の外部ダイナミックリスト）のタイプの外部ダイナミックリストに追加します https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/external-dynamic-list.html。次に、https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/url-filtering/use-an-external-dynamic-list-in-a-url-filtering-profile.htmlhttps://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/enforce-policy-on-an-external-dynamic-list.htmlURLフィルタリングプロファイル、またはセキュリティポリシールールの一致基準として、外部ダイナミックリストを使用します。外部動的リストを使用する利点は、ファイアウォールで構成変更やコミットを実行せずにリストを更新できることです。

  タイプ ***URL List*** の外部動的リストは、タイプ Domain List または IP アドレス の外部動的リストと混同しないでください。***URL*** の外部動的リストはドメインと ***IP*** アドレスを許可しますが、その逆は当てはまらず、無効なエントリになります。

次のガイドラインでは、URL カテゴリの例外リスト (カスタム URL カテゴリまたは URL の外部動的リスト) を設定する方法について説明します。

- URL カテゴリ例外リストの基本的なガイドライン
- URL カテゴリ例外リストのワイルドカードのガイドライン
- URL カテゴリ除外リスト - 例

URL カテゴリ例外リストの基本的なガイドライン

エントリを URL カテゴリの例外リストに追加する前に、エントリが一致する可能性があるかどうかを検討してください。次のガイドラインでは、意図した Web サイトやページをブロックまたは許可するエントリを作成する方法を指定します。

デフォルトでは、*firewall* は、末尾のスラッシュ *(/)* またはアスタリスク *(*)* で終わらないドメインエントリに、末尾のスラッシュ *(/)* を自動的に追加します。末尾にスラッシュを追加すると、*firewall* が一致と見なし、ポリシーを適用する *URL* が変更されます。ワイルドカードでないドメインエントリでは、末尾のスラッシュは、指定されたドメインとそのサブディレクトリにマッチを限定します。たとえば、***example.com*** *(*処理後の ***example.com/*** *)* は、自分自体と ***example.com/search*** とマッチします。

ワイルドカードドメインのエントリ（アスタリスクまたはキャレットが付いたエントリ）では、最後のスラッシュが、指定されたパターンに一致する*URL*へのマッチングを限定します。たとえば、エントリ ****.example.com*** と一致するには、*URL* に少なくとも *1* つのサブドメインが含まれ、ルート ドメイン ***example.com*** で終わる必要があります。パターンは ***<subdomain>.example.com***; ***news.example.com*** はマッチしますが、***example.com*** はサブドメインがないためマッチしません。

末尾にスラッシュを手動で追加して、エントリを検査するすべてのユーザーに対して、エントリの意図されたマッチ動作を明確にすることをお勧めします。末尾のスラッシュは、*firewall* によって追加されると見えなくなります。

PAN-OS® 10.2 を実行している *Panorama™* 管理サーバーは、同じソフトウェアバージョンのファイアウォールに対してのみこの機能を有効にすることができます。*PAN-OS 10.1* 以前を実行している *firewall* に対してこの機能を有効にするには、各 *firewall* で次の *CLI* コマンドを使用します:

```
admin@PA-850> debug device-server append-end-token on
```

```
admin@PA-850> configure
```

```
admin@PA-850# commit
```

この機能を無効にするには、***Device > Setup > Content-ID > URL Filtering*** を選択します。次に、***Append Ending Token*** の選択を解除します。ただし、この機能を無効にすると、予想よりも多くの *URL* へのアクセスをブロックまたは許可されます。*firewall* は、*/* または *** で終わらないドメインエントリの末尾に 暗黙のアスタリスク を追加します。たとえば、許可された *Web* サイトの *URL* リストに ***example.com*** を追加すると、*firewall* はそのエントリを ***example.com.**** と解釈します。その結果、*firewall* は ***example.com.domain.xyz*** などのサイトへのアクセスを許可します。URL Category Exceptions*(PAN-OS 10.1* 以前*)* では、この機能を無効にした場合の *firewall* の動作について説明します。

- リストエントリは大文字と小文字を区別しません。
- URL エントリから **http** と **https** を省略します。
- 各 URL エントリの長さは最大255文字です。
- ブロックまたは許可するIPアドレスまたはURLと完全に一致するものを入力するか、ワイルドカードを使用してパターンマッチを作成します。

  エントリが異なると、完全一致も異なります。特定の *Web* ページ (***example.com/contact***) の *URL* を入力すると、*firewall* は、そのページのみに一致を限定します。ドメインの完全一致は、ドメイン自体とそのサブディレクトリに一致を限定します。
- 元のエントリが URL 以外のエントリからアクセスできる場合は、Web サイトまたはページへのアクセスに最も一般的に使用される URL を例外リストに追加することを検討してください (たとえば、**blog.paloaltonetworks.com** や **paloaltonetworks.com/blog**)。
- エントリ **example.com** は **www.example.com** とは異なります。ドメイン名は同じですが、2 番目のエントリには *www* サブドメインが含まれています。

Palo Alto Networks は、カスタム *URL* カテゴリまたは外部動的リストエントリでの正規表現の使用をサポートしていません。特定の *URL* を知っているか、ワイルドカードと次の文字を使用して照合する *URL* パターンを作成する必要があります: **.** **/** **?** **&** **=** **;** **+**。

URL カテゴリ例外リストのワイルドカードのガイドライン

URL カテゴリの例外リストでアスタリスク (*) とキャレット (^) を使用すると、正確な URL を指定せずに、複数のサブドメイン、ドメイン、トップレベルドメイン (TLD)、またはページに一致するように 1 つのエントリを設定できます。

アスタリスク（*）およびキャレット（^）ワイルドカードの使用方法

次の文字はトークン区切り文字です: **.** **/** **?** **&** **=** **;** **+**。これらの文字の 1 つまたは 2 つで区切られたすべての文字列はトークンです。ワイルドカード文字をトークン プレースホルダとして使用すると、特定のトークンに任意の値を含めることができます。エントリ **docs.paloaltonetworks.com** では、トークンは "docs"、"paloaltonetworks"、および "com" です。

次の表は、アスタリスクとキャレットの仕組みとその例です。

*	^
1 つ以上の可変サブドメイン、ドメイン、TLD、またはサブディレクトリーを示します。 末尾のスラッシュの後にアスタリスクを使用できます (**example.com/*** など)。	1 つの可変サブドメイン、ルート・ドメイン、または TLD を示します。 末尾のスラッシュの後にキャレットを使用することはできません。次のエントリは無効です: **example.com/^**。

*	^
例: ***.domain.com** は **docs.domain.com** と **abc.xyz.domain.com** に一致します。	例: **^.domain.com** は **docs.domain.com** と **blog.domain.com** に一致します。

Key Point:アスタリスクは、キャレットよりも広い範囲の URL に一致します。アスタリスクは任意の数の連続するトークンに対応し、キャレットは 1 つのトークンのみに対応します。

xyz.*.com のようなエントリは、**xyz.^.^.com** よりも多くのサイトに一致します。**xyz.*.com** は、文字列間の任意の数のトークンを持つサイトに一致し、**xyz.^.^.com** は、正確に 2 つのトークンを持つサイトに一致します。

- ワイルドカード文字はトークン内の唯一の文字でなければなりません。たとえば、**example*.com** は、example と * が同じトークン内にあるため 、無効なエントリです。ただし、1 つのエントリに複数のトークンにワイルドカードを含めることができます。
- 同じエントリ内でアスタリスクとキャレットを使用できます (***.example.^** など)。

連続するアスタリスク ***(*)*** または ***9*** つ以上の連続するキャレット ***(^)*** を含むエントリを作成しないでください。このようなエントリは、***firewall*** のパフォーマンスに影響を与える可能性があります。

たとえば、***mail.*.*.com*** のようなエントリを追加しないでください。代わりに、アクセスを制御する *Web* サイトの範囲に応じて、***mail.*.com*** または ***mail.^.^.com*** と入力します。

URL カテゴリ除外リスト - 例

次の表は、URLリストエントリーの例、マッチングサイト、およびファイアウォールが自動的に末尾のスラッシュを追加する場合のマッチング動作の説明を示しています。

*The entries in this table do not contain a trailing slash to reflect that the firewall appends one to applicable entries in the background.*さらに、例外リストには、末尾のスラッシュのガイダンスの前に追加された項目が含まれることがあります。URL カテゴリ例外リスト:例 *(PAN-OS 10.1)*は、ファイアウォールがデフォルトで末尾のスラッシュを追加しない場合に一致する動作を示しています。

末尾にスラッシュを手動で追加して、エントリを検査するすべてのユーザーに対して、エントリの意図されたマッチ動作を明確にすることをお勧めします。末尾のスラッシュは、ファイアウォールによって追加された場合は見えません。

URL 例外リストのエントリ	サイト一致	説明
セット **1** の例		

URL 例外リストのエントリ	サイト一致	説明
paloaltonetworks.com	paloaltonetworks.com paloaltonetworks.com/network-security/security-subscriptions	firewall はエントリの末尾にスラッシュを追加し、正確なドメインとそのサブディレクトリへの一致を限定します。
paloaltonetworks.com/example	paloaltonetworks.com/example	firewall は、サブディレクトリー **example** がドメインの後に続くため、このエントリーに末尾のスラッシュを追加しません。特定の Web ページの URL を入力すると、firewall は指定された Web ページに例外アクションを適用します。
Example Set 2— アスタリスク		
*.example.com	www.example.com docs.example.com support.tools.example.com	アスタリスクは、すべての **example.com** サブドメインに一致を拡張します。 firewall は、ルートドメインである **example.com** の右側に一致するものを除き、エントリに末尾のスラッシュを追加します。
mail.example.* このエントリは、末尾のスラッシュ機能を有効にしてもしなくても、同じマッチを生成します。	mail.example.com mail.example.co.uk mail.example.com/#inbox	アスタリスクは、**mail.example.*<TLD>**パターンに続くすべてのURLにマッチするように拡張します。
example.*.com	example.yoursite.com example.es.domain.com example.abc.xyz.com	アスタリスクは、左端のサブドメインが **example** で、最上位ドメインが **com** の URL に一致を拡張します。末尾のスラッシュは、TLD の右側にある一致を除外します。

URL 例外リストのエントリ	サイト一致	説明
example.com/*	example.com/photos example.com/blog/latest 任意の example.com サブディレクトリ	ドメインの後には、/ と、サブディレクトリーが存在しなければならないことを示すアスタリスクが続きます。アスタリスクは、任意の **example.com** サブディレクトリーのトークン・プレースホルダーとして機能します。 firewall は、エントリーがアスタリスクで終わるため、末尾にスラッシュを追加しません。
Example Set 3— キャレット		
google.^ *example.co.^* などのパターンは、通常、***example.co.jp*** などの国固有のドメインを照合するために使用されます。ただし、汎用トップレベルドメイン *(gTLD)* では、*example.co.^* マッチング *example.co.info* や *example.co.amzn* などのパターンが発生し、同じ組織に属していない可能性があります。	google.com google.info google.com/search?q=paloaltonetworks	キャレットは、**google** で始まり、単一の TLD で終わる URL に一致を拡張します。末尾のスラッシュは、最後のトークンの右側にある一致を除外します。
^.google.com	www.google.com news.google.com	キャレットは、一致を **google.com** の単一レベル サブドメインに展開します。firewall は、ルートドメインの右側にある一致を除

URL 例外リストのエントリ	サイト一致	説明
		き、エントリの末尾にスラッシュを追加します。
^.^.google.com	www.maps.google.com support.tools.google.com	2 つのキャレットは、**google.com** の前に 2 つの連続するサブドメインを含む URL に一致を拡張します。firewall は、ルートドメインの右側にある一致を除き、エントリの末尾にスラッシュを追加します。
google.^.com	google.example.com google.company.com	キャレットは、**google**が一番左のサブドメインで、その後に1つのトークンと**.com**が続くURLにマッチするように展開されます。 firewall は、TLD の右側にある一致を除き、エントリの末尾にスラッシュを追加します。

URLフィルタリング プロファイルで外部動的リストを使用

新たに検出された脅威やマルウェアからネットワークを保護するために、URL フィルタリング プロファイルで の外部動的リスト を使用できます。外部ダイナミック リストを使用すると、設定を変更せずにリストを更新したり、ファイアウォールでコミットしたりできます。外部ダイナミック リストは外部の Web サーバーでホストされているテキストファイルです。このリストを使用してURLをインポートし、それらのURLにポリシーを適用することができます。WEBサーバー上でリストが更新されるとファイアウォールが変更内容を取得し、ファイアウォール上でコミットすることなくポリシーを変更されたリストに適用できます。

ファイアウォールは設定済みの間隔で動的にリストをインポートし、リスト内の URL（IPアドレスやドメインは無視されます）に対してポリシーを適用します。URL フォーマットのガイドラインについては、「URL カテゴリの例外」を参照してください。

詳細については外部ダイナミック リストを参照してください。

STEP 1 | 外部動的リストにアクセスするようにファイアウォールを設定する 。

- リストにIPアドレスやドメイン名を含めないでください。ファイアウォールはURL以外のエントリーをスキップします。
- リストの書式を確認するには、 カスタム URL リストのガイドライン を使用します。
- Type (タイプ) ドロップダウンリストから **URL List (URL リスト)** を選択します。

STEP 2 | URLフィルタリング プロファイル内で外部動的リストを使用します。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **URL Filtering (URL フィルタリング)** の順に選択します。
2. **Add** [追加]、あるいは既存のURLフィルタリング プロファイルを変更します。
3. このプロファイルに**Name** [名前]を付け、**Categories** [カテゴリ]タブのCategory [カテゴリ]リストから外部動的リストを選択します。
4. Action [アクション]を選択し、外部動的リスト内のURLに対する細かなアクションを選択します。

   外部動的リストに含まれる *URL* がカスタム *URL* カテゴリにも含まれている場合、または ブロックと許可リスト に含まれる場合、カスタム カテゴリまたはブロックリストと許可リストで指定されたアクションが外部動的リストよりも優先されます。
5. **OK** をクリックします。
6. URL フィルタリング プロファイルをセキュリティポリシー ルールに適用します。
   1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
   2. **Actions** [アクション]タブを選択し、Profile Setting [プロファイル設定]セクションの**URL Filtering** [URLフィルタリング]ドロップダウンリストで新しいプロファイルを選択します。
   3. **OK**、**Commit (コミット)** の順にクリックします。

STEP 3 | ポリシー アクションが適用されているかどうかテストします。

1. 外部動的リストエントリ を表示し、リストから URL にアクセスします。
2. 定義したアクションがブラウザに適用されることを確認します。
3. ファイアウォール上のアクティビティを監視するには：
   1. **ACC**を選択し、URL Domain [URLドメイン]をグローバルフィルターとして追加し、アクセスしたURLのNetwork Activity [ネットワーク アクティビティ]およびBlocked Activity [ブロックされたアクティビティ]を確認します。
   2. 詳細ログ ビューにアクセスするには、**Monitor (監視)** > **Logs (ログ)** > **URL Filtering (URL フィルタリング)** を選択します。

STEP 4 | 外部動的リストのエントリーが無視されたかスキップされたかを検証します。

タイプがURLのリストでは、ファイアウォールはURL以外のエントリーを無効なものとしてスキップし、ファイアウォール モデルの限度を超えるエントリーは無視します。

外部動的リストの種類について制限に達しているかどうか確認するためには、***Objects (オブジェクト)*** > ***External Dynamic Lists (外部動的リスト)*** を選択し、***List Capacities (キャパシティをリストアップ)*** をクリックします。

ファイアウォール上で次のCLIコマンドを実行し、リストの詳細情報を表示します。

```
request system show type url name <list_name>
```

以下に例を示します。

```
request system external-list show type url name My_URL_List
 vsys5/My_URL_List:次の更新:Tue Jan 3 14:00:00 2017 Source: http://
example.com/My_URL_List.txt  Referenced:はい 有効:はい認証有効:Yes 有
効なエントリの合計数:3 無効なエントリの合計数:0 有効な URL: www.URL1.com
 www.URL2.com www.URL3.com
```


特定のサイトへのパスワード アクセスを許可する

場合によっては、URL カテゴリをブロックするが、特定のユーザーがアクセスを許可する場合があります。この場合、カテゴリ アクションを **[override]**\ に設定し、ファイアウォールの [コンテンツ ID] 設定で URL 管理オーバーライド パスワードを定義します。これらのカテゴリのサイトにアクセスする前に、ユーザーは上書きパスワードを入力する必要があります。URL 管理オーバーライドを設定するには、以下の手順を実行します。

STEP 1 | URL 管理オーバーライド パスワードを設定します。

1. **Device (デバイス)** > **Setup (設定)** > **Content-ID**の順に選択します。
2. **[URL** 管理オーバーライド] セクションで、**[追加]** をクリックします。
3. **[場所]**フィールドで、このパスワードを適用する仮想システムを選択します。
4. **[パスワード]** と **[パスワードの確認]** を入力します。
5. **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）を選択します。このプロファイルでは、オーバーライドが設定されたサイトが HTTPS サイトの場合にファイアウォールからユーザーに提供される証明書を指定します。詳細は、「SSL/TLS サービス プロファイルの設定」を参照してください。
6. ユーザーにパスワードを要求する **[モード]**を選択します。
   - **Transparent (メッセージを表示しない)** – ファイアウォールは、オーバーライドするように設定した URL カテゴリのサイト宛てのブラウザのトラフィックをインターセプトし、元の宛先 URL を偽装して HTTP 302 を発行し、パスワードを要求します。これは vsys 単位で適用されます。

     証明書が信頼されていない場合、クライアント ブラウザに証明書エラーが表示されます。

   - リダイレクト– ファイアウォールは、オーバーライドするように設定した URL カテゴリへの HTTP または HTTPS トラフィックをインターセプトし、オーバーライド パスワードを要求するために HTTP 302 リダイレクトを使用してファイアウォールのレイヤー 3 インターフェイスに要求をリダイレクトします。このオプションを選択する場合、トラフィックをリダイレクトする <91></91>**[アドレス]**（IP アドレスまたは DNS ホスト名）を入力する必要があります。
7. **OK** をクリックします。

STEP 2 | （任意）カスタム オーバーライド期間を設定します。

1. URL Filtering （URL フィルタリング）セクションを編集します。
2. ユーザーがオーバーライド パスワードを正しく入力したカテゴリのサイトを閲覧できる時間を変更するには、 **URL Admin Override Timeout**（URL 管理オーバーライド タイムアウト）フィールドに新しい値を入力します。デフォルトでは、ユーザーがカテゴリのサイトにアクセスできる時間は 15 分間です。この時間を経過すると、パスワードを再入力する必要があります。
3. ユーザーがオーバーライド パスワードの入力に 3 回失敗した場合に、オーバーライドするように設定されたサイトにアクセスできなくなる時間を変更するには、**[URL** 管理

ロックアウト タイムアウト] フィールドに新しい値を入力します。デフォルトでは、ユーザーは 30 分間ブロックされます。

4. **OK** をクリックします。

STEP 3 | （リダイレクト モードのみ）オーバーライド用に設定したカテゴリのサイトに Web 要求をリダイレクトするレイヤー 3 インターフェイスを作成します。

1. 管理プロファイルを作成して、インターフェイスに URL Filtering Continue and Override Page （URL フィルタリングの続行とオーバーライド ページ）の応答ページを表示できるようにします。
   1. **Network**（ネットワーク） > **Interface Mgmt**（インターフェイス **Mgmt**）を選択し、**Add**（追加）をクリックします。
   2. **Name** [名前]フィールドにプロファイル名を入力し、**Response Pages** [応答ページ]を選択してから **OK** をクリックします。
2. レイヤー 3 インターフェイスを作成します。作成した管理プロファイルが関連付けられていることを確認します（イーサネット インターフェイス ダイアログの**Advanced**（詳細） > **Other Info**（その他の情報） タブ）。

STEP 4 | (リダイレクト モードのみ) 証明書エラーを表示せずにユーザーを透過的にリダイレクトするには、オーバーライド用にURLカテゴリで設定されたサイトにWebリクエストをリダイレクトする IP アドレスに一致する証明書をインストールします。自己署名証明書を生成するか、外部 CA によって証明された証明書をインポートできます。

自己署名証明書を使用するには、以下のとおり、まずルート CA の証明書を作成してから、その CA を使用して URL 管理オーバーライドに使用する証明書に署名する必要があります。

1. ルート CA 証明書を作成するには、**Device** > **Certificate Management** > **Certificates** > **Device Certificates**(デバイス > 証明書の管理 > 証明書 > デバイス証明書) の順に選択し、**Generate**(生成) をクリックします。**Certificate Name** [証明書名]に「RootCA」などの名前を入力します。**Signed By** [署名者]フィールドの値は選択しないでください（その証明書が自己署名証明書であることを示すものであるため）。**[認証局]** チェックボックスがオンになっていることを確認してから **[生成]** をクリックすると、証明書が生成されます。
2. URL 管理オーバーライドに使用する証明書を作成するには、**[生成]** をクリックします。**[証明書名]** に名前を入力し、インターフェイスの DNS ホスト名または IP アドレスを **[共通名]** として入力します。**Signed By** [署名者]フィールドで、前の手順で作成した CA を選択します。IP アドレスの属性を追加し、override アクションが設定されている URL カテゴリに Web 要求をリダイレクトするレイヤー 3 インターフェイスの IP アドレスを指定します。
3. 証明書を **Generate**[生成] します。
4. クライアントが証明書を信頼するように設定するには、**[デバイス証明書]** タブで CA 証明書を選択し、**[エクスポート]** をクリックします。次に、証明書を信頼されたルート CA としてすべてのクライアント ブラウザにインポートする必要があります。インポートはブラウザから手動で設定するか、または証明書を Active Directory のグループ ポリシー オブジェクト（GPO）の信頼されたルートに追加します。

STEP 5 | アクセスを有効にするためにオーバーライド パスワードが必要な URL カテゴリを指定します。

1. オブジェクト > **URL** フィルタリング を選択し、既存の URL フィルタリング プロファイルを選択するか、または新しい URL フィルタリング プロファイルを 追加 を選択します。
2. **[カテゴリ]** タブで、パスワードを必要とする各カテゴリの [アクション] を **[override]** に設定します。
3. URL フィルタリング プロファイルの残りのセクションをすべて完了し、[**OK**] をクリックしてプロファイルを保存します。

STEP 6 | URL フィルタリング プロファイルをセキュリティ ポリシー ルールに適用し、アクセスのためにパスワードの上書きを要求するサイトにアクセスできるようにします。

1. [ポリシー > セキュリティ] を選択し、適切なセキュリティ ポリシーを選択して変更します。
2. **[アクション]** タブを選択して、**[プロファイル設定]** セクションで、**[URL** フィルタリング**]** のドロップダウンをクリックし、プロファイルを選択します。
3. **OK** をクリックして保存します。

STEP 7 | 設定を保存します。

Commit（コミット）をクリックします。

認証情報フィッシングの阻止

フィッシング サイトとは、攻撃者がユーザー情報、特にネットワークへのアクセスを提供する資格情報を盗もうとする正当な Web サイトを偽装するサイトです。フィッシングのメールがネットワークに侵入すると、いずれかのユーザーがリンクをクリックして認証情報を提供するだけで、セキュリティの穴が顕在化してしまいます。サイトの URL カテゴリに基づき、ユーザーが企業の認証情報を送信できるサイトを制御することで、進行中のフィッシング攻撃を検知・阻止できるので、証明書の盗難を防止します。これにより、信頼されていないサイトに資格情報を送信できないようにし、企業サイトや認可されたサイトへの資格情報の送信を許可することができます。

ウェブサイトに送信されるユーザー名およびパスワードをスキャンし、それらの送信を正当な企業の認証情報と比較することで、認証情報フィッシング防止が行われます。ウェブサイトの URL カテゴリに基づき、企業の認証情報を送信するのを許可あるいはブロックするウェブサイトを選択できます。ファイアウォールは、制限を受けたカテゴリのサイトに資格情報を送信しようとするユーザーを検出すると、ユーザーが資格情報を送信できないようにするブロック応答ページを表示するか、特定の URL カテゴリのサイトに資格情報を送信しないように警告する続行ページを表示します。 は、正当なフィッシング以外のサイトであっても、企業の資格情報を再利用できないようにユーザーを教育するために、これらのブロック ページ をカスタマイズできます。

認証情報フィッシング防止を有効化するためには、ユーザーが正当な企業の認証情報（個人の認証情報ではなく）をサイトに送信するのを検知する User-ID と、ユーザーが企業の認証情報を入力するのを防止する URL カテゴリを指定する URL フィルタリングの両方を設定する必要があります。次のトピックでは、認証情報の送信を検知するために使用できる各種の方法、および認証情報フィッシング防止を設定する方法を説明します。

- 企業の認証情報送信をチェックする方式
- Windows ベースの User-ID エージェントを使用する認証情報検知の設定
- 認証情報フィッシング防御のセットアップ

企業の認証情報送信をチェックする方式

を設定する前に、認証情報フィッシング防止 を設定する前に、有効な企業資格情報が Web ページに送信されているかどうかを確認するためにファイアウォールを使用する方法を決定します。

送信された認証情報をチェックする方式	**User-ID** 設定の要件	この方法では、ユーザーが **Web** サイトに送信する企業のユーザー名および/またはパスワードをどのように検出しますか？
Group Mapping（グループ マッピング）	ファイアウォール上の グループ マッピング設定	ファイアウォールは、制限されているサイトにユーザーが送信するユーザー名が有効な企業ユーザー名と一致するかどうかを判断することを確認します。 これを行うため、ファイアウォールは、送信されるユーザー名をユーザーとグループのマッピング テーブルのユーザー名のリストと照合し、ユーザーが制限

送信された認証情報をチェックする方式	User-ID 設定の要件	この方法では、ユーザーが Web サイトに送信する企業のユーザー名および/またはパスワードをどのように検出しますか？
		されているカテゴリのサイトに企業ユーザー名を送信する時に検出します。 この方法では、LDAP グループ メンバーシップに基づいて企業ユーザー名の送信のみがチェックされるため、設定は簡単ですが、誤検出が多くなる傾向があります。
IP ユーザー マッピング	IPユーザマッピングは、認証ポリシーや認証ポータル、GlobalProtectを通じてユーザーマッピングの識別が行われます。	ファイアウォールは、ユーザーが制限されているサイトに送信するユーザー名がログインユーザー名の IP アドレスにマッピングされているかどうかを確認します。 これを行うため、ファイアウォールは、ログイン中のユーザー名およびウェブサイトに送信されたユーザー名を自身の IP アドレス対ユーザーのマッピング テーブルと一致させ、ユーザーが制限されているカテゴリのサイトに企業ユーザー名を送信していればそれを検出します。 この方式は、セッションに関連するログイン済みのユーザー名の IP アドレスを IP アドレス対ユーザー名のマッピング テーブルと照合するため、企業のユーザー名の送信を検出するのに適した方式ですが、企業のパスワードの送信を検出することはできません。企業のユーザー名およびパスワードの送信を検出したい場合は、ドメイン認証情報フィルタ方式を使用する必要があります。
ドメイン認証情報フィルタ	User-ID 認証情報サービス アドオンと共に設定された Windows の User-ID エージェント - および - IPユーザマッピングは、認証ポリシーや認証ポータル、GlobalProtectを通じてユーザーマッピングの	ファイアウォールは、ユーザーが送信するユーザー名とパスワードが、同じユーザーの企業ユーザー名とパスワードと一致するかどうかを判断することを確認します。 これを行うため、ファイアウォールは次のように、送信される認証情報を有効な企業ユーザー名とパスワードと照合し、送信されるユーザー名が、ログインユーザー名の IP アドレスに対応することを確認できる必要があります。 • 企業のユーザー名およびパスワードを検出する—ファイアウォールは User-ID 認証情報サービス アドオンを備えた Windows の User-ID エージェントから、ブルーム フィルタと呼ばれる安全なビットマスクを取得します。このアドオン サービスはディレクトリをスキャンしてユーザー名およ

送信された認証情報をチェックする方式	User-ID 設定の要件	この方法では、ユーザーが Web サイトに送信する企業のユーザー名および/またはパスワードをどのように検出しますか？
	識別が行われます。	びパスワードのハッシュを見つけ、それを安全なビットマスク（ブルーム フィルタ）の形に解体して Windows User-ID エージェントに送付します。ファイアウォールは、Windows User-ID エージェントから定期的にブルームフィルターを取得します。制限されたカテゴリに認証情報を送信しているユーザーを検知した場合は必ず、ブルーム フィルタを再構築し、マッチするユーザー名およびパスワードのハッシュを探します。ファイアウォールは、User-ID 認証情報サービスのアドオンを実行している単体の Windows の User-ID エージェントにのみ接続できます。 • 認証情報がログイン中のユーザー名のものであることを検証する—ファイアウォールは、ログイン中のユーザー名の IP アドレスと、自身の IP アドレス対ユーザー名のマッピング テーブルに含まれる検出されたユーザー名との間のマッピングを探します。 ドメイン認証方式がどのように動作するか、またこのタイプの検知を有効化するための要件の詳細については、Windows ベースの User-ID エージェントを使用する認証情報検知を設定を参照してください。

Windows の User-ID エージェントを使用する認証情報検知の設定

ドメイン認証情報フィルタ検知により、Web ページに送信されたパスワードをファイアウォールが検出できるようになります。この認証情報検知方式には Windows の User-ID エージェントおよび、読み取り専用ドメイン コントローラ（*RODC*） にインストールする User-ID エージェントのアドオンである User-ID 認証情報サービスが必要になります。

ドメイン認証情報フィルタの検出方式は、*Windows* の *User-ID* エージェントでのみサポートされています。*PAN-OS* 統合 *User-ID* エージェントを使用してこの方式の認証情報検知を設定することはできません。

RODC は、ドメイン コントローラがホストするアクティブディレクトリ データベースの読み取り専用のコピーを保持する Microsoft Windows サーバーです。例えば、ドメイン コントローラが企業本部に位置している場合、RODC をリモートネットワークのロケーションにデプロイし、ローカル認証サービスを利用可能にできます。ドメイン コントローラのディレクトリにアクセスするために認証情報検知を有効化する必要がないこと、一部のユーザーを対象にして認証情報検知をサポートできることなど、、User-ID エージェントを RODC 上にインストールすることが役立つ理由はいくつかあります。RODC がホストするディレクトリは読み取り専用であるため、ドメイン コントローラ上でディレクトリ内のコンテンツの安全が確保されます。

証明書の検出のために *RODC* に *Windows* の *User-ID* エージェントをインストールする必要があるため、ベストプラクティスとして別のエージェントを展開してください。*RODC* にインストールされている *User-ID* エージェントを使用して *IP* アドレスをユーザーにマップしないでください。

RODC 上に User-ID エージェントをインストールした後、User-ID 認証情報サービスがバックグラウンドで実行され、ディレクトリをスキャンし、RODC パスワード複製ポリシー（PRP）（このリストに載せるユーザーを定義可能）にリストアップされているグループ メンバーのユーザー名およびパスワードのハッシュを探します。その後、収集されたユーザー名およびパスワードのハッシュを User-ID 認証情報サービスが引き受け、データを解体してブルーム フィルタと呼ばれるビットマスクの携帯にします。コンパクトなデータ構造を持つブルーム フィルタは、エレメント（ユーザー名あるいはパスワードのハッシュ）が一連のエレメント（RODC に対して複製を許可した一連の認証情報）のメンバーであるかどうかを確認する上で、セキュアな方法を提供します。User-ID 認証情報サービスはブルーム フィルタを Windows の User-ID エージェントに転送します。ファイアウォールは定期的に最新のブルーム フィルタを User-ID エージェントから受け取り、送信されたユーザー名およびパスワードのハッシュを検知するためにそれを使用します。設定に応じて、その後ファイアウォールは Web ページに対する有効なパスワード送信をブロック、通知、あるいは許可するか、フィッシングの危険についてユーザーに警告を伝える応答ページを表示しつつ、送信を続行することを許可します。

このプロセス全体を通じて、User-ID エージェントは一切パスワードのハッシュを保存・表示したりせず、またそれをファイアウォールに転送することもありません。ブルーム フィルタの形に解体されたパスワードのハッシュを復元する方法はありません。

STEP 1 | Windows ユーザー ID エージェント を使用してユーザー マッピングを構成します。

> 資格情報の検出を有効にするには、*RODC* に *Windows* の *User-ID* エージェントをインストールする必要があります。サポートされているサーバーのリストについては、Compatibility Matrix（互換性マトリックス）を参照してください。この目的のために別個の *User-ID* エージェントをインストールしてください。

User-ID をセットアップしてドメイン認証情報フィルタ検知を有効化する際に、頭にとどめておくべき重要事項：

- 認証情報フィッシング詐欺検出の効果は RODC の設定に左右されるため、必ず RODC 管理のベストプラクティスおよび推奨事項も確認するようにしてください。
- User-ID ソフトウェア更新のダウンロード：
  - User-ID エージェント Windows インストーラ—UaInstall-x.x.x-x.msi。
  - User-ID エージェント認証情報サービス Windows インストーラ—UaCredInstall64-x.x.x-x.msi。
- LDAP を介してアクティブディレクトリを読み取る権限を持つアカウントを使用して RODC に User-ID エージェントおよびユーザーエージェント認証情報サービスをインストールします。
  - User-ID エージェント認証情報サービスでは、ローカルシステムのアカウントを使ってログを記録する権限が必要になります。詳細については、User-ID エージェント専用のサービスアカウントを作成を参照してください。
  - サービス アカウントが RODC 上のローカル管理者グループのメンバーでなければなりません。詳細は、次のリンクを参照してください。

STEP 2 | （バックグラウンドで稼働して許可された認証情報をスキャンする）User-ID エージェントおよびユーザーエージェント認証情報サービスを有効化し、情報を共有します。

1. RODC サーバーで User-ID エージェントを起動します。
2. **Setup (セットアップ)** を選択し、Setup (セットアップ) セクションを編集します。
3. **Credentials (認証情報)** タブを選択します。このタブは、User-ID エージェント認証情報サービスをインスール済みである場合のみ表示されます。
4. **Import from User-ID Credential Agent (User-ID** 認証情報エージェントからインポート**)** を選択します。これにより、ユーザーおよび対応するパスワードのハッシュを提供するために User-ID 認証情報エージェントが作成するブルーム フィルタを User-ID エージェントがインポートできるようになります。
5. **OK** をクリックして設定を **Save (保存)** し、**Commit (コミット)** します。

STEP 3 | RODC ディレクトリにて、認証情報送信検知の対象にしたいユーザーグループを定義します。

- 認証情報送信を適用するグループが Allowed RODC Password Replication Group (許可された RODC パスワード複製グループ) に追加されていることを確認します。
- Allowed RODC Password Replication Group (許可された RODC パスワード複製グループ) に含まれるどのグループも、デフォルトで Denied RODC Password Replication Group 拒否さ

れた RODC パスワード複製グループ) に含まれないことを確認します。両方にリストアップされたグループは、認証情報フィッシング防止の適用対象にはなりません。

STEP 4 | 次のタスクに進みます。

ファイアウォールで資格情報フィッシング防止 を設定します。

認証情報フィッシング防御のセットアップ

使用する企業資格情報の送信 を検出する メソッドを決定したら、次の手順を実行して、ユーザーが Web ページに企業資格情報を送信するタイミングを検出し、このアクションで警告を表示するか、資格情報の送信をブロックするか、またはユーザーにフィッシングの危険性を確認してもらってから送信を続行します。

クレデンシャルフィッシング防止を有効にする前に、ファイアウォールで構成するプライマリユーザー名が *samAccountName* 属性を使用していることを確認します。資格情報フィッシング防止機能は代替属性をサポートしていません。

STEP 1 | まだ有効にしていない場合は、ユーザー ID を有効にします。

メソッドで企業資格情報の送信を確認する方法 には、次の異なる User-ID 構成が必要です。

- ユーザーが有効な企業ユーザー名を送信しているかどうかを検出するグループ マッピング方法を使用する場合は、ユーザーを group にマップします。
- ユーザーが有効な企業ユーザー名を送信しているかどうか、そのユーザー名がログイン ユーザー名と同じであることを検出する IP ユーザー マッピング方法を使用する場合は、ユーザー名をユーザーにマップ 。
- ドメイン資格情報フィルターメソッドを使用する場合、ユーザーが有効なユーザー名とパスワードを送信しているかどうか、およびそれらの資格情報がログインユーザーに属しているかどうかを検出する場合>Windows ベースのユーザー ID エージェント と map IP アドレスを使用してユーザーに IP アドレスを設定します.

STEP 2 | すでに実施済みの場合は、最良のURLフィルタリング プロファイルを設定し、マルウェアあるいは悪意のあるコンテンツをホストしていることが分かっている URL から確実に保護されるようにします。

1. Select **Objects (オブジェクト)** > **Security Profiles (セキュリティプロフィール)** > **URL Filtering (URL**フィルタリング**)**を選択し、URLフィルタリングプロファイルを**Add**（追加）または変更します。
2. すべての既知の危険なURLカテゴリであるマルウェア、フィッシング、ダイナミック DNS、未知、コマンド& コントロール、エクストリミズム、著作権侵害、プロキシ回避・アノニマイザー、新しく登録されたドメイン、グレイウェアおよびパークドへのアクセスをブロックします。

STEP 3 | Add ユーザー資格情報の送信を監視するトラフィックを復号化するための復号化ポリシールール。

STEP 4 | 許可する URL カテゴリに属すウェブサイトに対して行う、企業の認証情報の送信を検知する URL フィルタリング プロファイルを設定します。

ファイアウォールは、サイトの *URL* カテゴリのチェックを有効にしても、信頼済みサイトへの認証情報の送信はチェックせず、最高のパフォーマンスが得られます。信頼済みサイトは、*Palo Alto Networks* が悪意のある攻撃やフィッシング攻撃を確認していないサイトを表しています。この信頼済みサイトリストの更新は、アプリケーションおよび脅威コンテンツ更新を通じて配信されます。認証情報の検出が免除される *App-ID* のリストについては、live.paloaltonetworks.com の認証情報送信検出をスキップする信頼された App-ID を参照してください。

1. **User Credential Detection (**ユーザーの認証情報検出**)** を選択します。
2. ユーザー資格情報検出 ドロップダウンから、ユーザーの資格情報検出方法 から Web ページに対して 1 つを選択します。

   プライマリ ユーザー名の形式が、*User-ID* ソースが提供するユーザー名の形式と同一であることを確認します。

   - **Use IP User Mapping (IP** ユーザー マッピングの使用**)**—企業のユーザー名送信が正当なものであり、セッションの送信元 IP アドレスにログイン ユーザー名がマッピングすることが確認されます。そうするために、ファイアウォールは送信されるユーザー名およびセッションの送信元 IP アドレスを IP アドレス対ユーザー名のマッピング テーブルと照合します。この方法を使用するには、「ユーザーに IP アドレスをユーザーにマップする」で説明されているユーザー マッピング方法 を使用できます。
   - **Use Domain Credential Filter (**ドメイン認証情報フィルタを使用**)**—送信される企業ユーザー名とパスワードが正当なものであるか確認し、ユーザー名が、ログイン中のユーザーの IP アドレスに対応することを確認します。User-ID をセットアップしてこの方式を有効にする方法については、Windows ベースの User-ID エージェントを使用する認証情報検知を設定を参照してください。
   - グループ マッピングを使用する] - ユーザーをグループにマップする場合に設定されたユーザーからグループへのマッピング テーブルに基づいて有効なユーザー名の送信をチェックします

     グループ マッピングの場合、 IT のような最も重要なアプリケーションにアクセスできる特定のグループのため、あるいはディレクトリのいずれかの部分に認証情報検知を割り当てられます。

     この方法は、ユーザー名が一意な構造でない環境では誤検出が多くなりがちです。そのため、この方法は高価値なユーザーアカウントを保護する用途でのみ使用するようにしてください。
3. ファイアウォールが企業の認証情報送信の検知をロギングするために使用する **Valid Username Detected Log Severity (**有効なユーザー名が検知されたログの重大度**)** を設定します。デフォルト設定では、ファイアウォールはこれらのイベントの重大度を中としてログに記録します。

STEP 5 | 許可されたサイトへの認証情報の送信をブロック（あるいは警告）します。

1. **Categories (**カテゴリ**)** を選択します。
2. **Site Access (**サイト アクセス**)** を許可する各 Category (カテゴリ) について、**User Credential Submissions (**ユーザー証明書送信**)** を扱う方法を選択します。
   - **alert** （アラート） – 認証情報を Web サイトに送信することをユーザーに許可しますが、ユーザーがこのカテゴリのサイトに認証情報を送信するたびに、URL フィルタリング ログを生成します。
   - **allow (**許可**)**–（デフォルト）ユーザーが認証情報を Web サイトに送信することを許可します。
   - **block**（ブロック） – ユーザーが認証情報を Web サイトに送信することをブロックします。ユーザーが認証情報を送信しようとする際、ファイアウォールはAnti-Phishing Block Page（アンチフィッシング ブロックページ）を表示し、認証情報の送信を阻止します。
   - **continue** （続行）–ユーザーが認証情報を送信しようとした際、Anti-Phishing Continue Page（アンチフィッシング 続行ページ）応答ページをユーザーに表示します。ユーザーが送信を続行するためには、応答ページで Continue (続行) を選択する必要があります。
3. **OK** を選択して URL フィルタリング プロファイルを保存します。

STEP 6 | 認証情報検知が設定されたURL フィルタリング プロファイルをセキュリティポリシールールに適用します。

1. **Policies (**ポリシー**)** > **Security (**セキュリティ**)**を選択し、セキュリティポリシールールを**Add**（追加）または変更します。
2. **Actions** （アクション） タブで **Profile Type (**プロファイル タイプ**)** を **Profiles (**プロファイル**)** に設定します。
3. 新規あるいは更新された **URL Filtering (URL** フィルタリング**)** プロファイルを選択し、セキュリティポリシー ルールに割り当てます。
4. **OK** をクリックし、セキュリティポリシー ルールを保存します。

STEP 7 | 設定を **Commit**（コミット）します。

STEP 8 | ファイアウォールが検知した認証情報の送信を監視します。

マルウェアおよびフィッシング サイトを訪問したユーザーの数を確認するには、***ACC*** **>** ***Hosts Visiting Malicious URLs (***有害な ***URL*** にアクセスしているホスト***)*** を選択します。

Monitor (監視**)** > **Logs (**ログ**)** > **URL Filtering (URL** フィルタリング**)** を選択します。

新たに **Credential Detected (**検出された認証情報**)** 列には、正当な認証情報を含む HTTP POST リクエストをファイアウォールが検知したイベントが表示されます。

この列を表示するためには、いずれかの列の見出しにカーソルを合わせ、矢印をクリックして表示したい列を選択します。

ログ エントリの詳細は、認証情報の送信も示唆します。

STEP 9 | 認証情報送信の検知を検証し、トラブルシューティングを行います。

- 次の CLI コマンドを使って認証情報検知の統計情報を表示します。

```
> show user credential-filter statistics
```

このコマンドの出力は、ファイアウォールが認証情報の送信を検知するために設定した方式によって異なります。例えば、Domain Credential Filter (ドメイン認証情報フィルタ) 方法が URL フィルタリング プロファイルで設定されている場合、ブルーム フィルタをファイアウォールに転送した User-ID エージェントのリストが、ブルーム フィルタに含まれている認証情報の数と共に表示されます。

- (Group Mapping メソッドのみ) 次の CLI コマンドを使用して、Group Mapping 資格情報検出が有効になっている URL Filtering プロファイルの数や、制限付きサイトに資格情報を送信しようとしたグループ メンバーのユーザー名など、グループ マッピング情報を表示します。

```
> show user group-mapping statistics
```

- (Domain Credential Filter method only) 次の CLI コマンドを使用して、firewall にマッピングを送信しているすべての Windows ベースの User-ID エージェントを表示します:

```
> show user user-id-agent state all
```

コマンド出力には、ファイアウォールが各エージェントから受信したブルーム フィルター更新の数、ブルーム フィルターの更新が処理に失敗した場合、および最後のブルーム フィルターの更新から経過した秒数を含むブルーム フィルター数が表示されるようになりました

- （ドメイン認証情報フィルタ方式のみ）Windows ベースの User-ID エージェントが、ファイアウォールへの BF（ブルーム フィルタ）プッシュを参照するログ メッセージを表示します。User-ID エージェント インターフェイスにて、**Monitoring (**モニタリング**)** > **Logs (**ログ**)** を選択します。

セーフ サーチの適用

多くの検索エンジンには、検索クエリ リターン トラフィックでアダルト画像やアダルト動画を除外するセーフ サーチ設定が備わっています。エンドユーザーが厳格なセーフ サーチ設定を使用していない場合にファイアウォールに検索結果をブロックさせたり、またユーザーのセーフ サーチを透過的に有効化したりできます。ファイアウォールは次の各プロバイダーのセーフ サーチをサポートしています。Google、Yahoo、Bing、Yandex、YouTube。セーフ サーチはベスト エフォート設定であり、サービスプロバイダはすべてのウェブサイトでこれが機能するという保証はしておらず、検索プロバイダはサイトを安全なものとそうでないものに分類しているということを考慮してください（Palo Alto Networks ではない）。

この機能を使用するには、URL フィルタリング プロファイルで [セーフ サーチの強制] オプションを有効にして、セキュリティ ポリシー ルールにアタッチする必要があります。ファイアウォールは、最も厳しい安全な検索設定を使用していない一致する検索クエリリターン トラフィックをブロックします。セーフ サーチを適用する方法には次の 2 つがあります。

- 厳密なセーフ サーチが有効でない場合の検索結果のブロック – エンド ユーザーが最も厳密なセーフ サーチ設定を有効にする前に検索を実行しようとすると、ファイアウォールで検索クエリ結果がブロックされ、URL フィルタリング セーフ サーチのブロック ページが表示されます。デフォルトでは、セーフ サーチを設定できるように、このページに検索プロバイダ設定への URL が表示されます。
- ユーザーに対して透過的にセーフ サーチの有効化 – エンド ユーザーが厳密なセーフ サーチ設定を有効にする前に検索を実行しようとすると、ファイアウォールで検索結果がブロックされて HTTP 503 ステータス コードが表示され、セーフ サーチ パラメータがある URL に検索クエリがリダイレクトされます。この機能を有効にするには、厳密なセーフ サーチ パラメータが含まれるように検索 URL を書き換える Javascript を備える新しい URL フィルタリング セーフ サーチのブロック ページをインポートします。この設定では、ユーザーにブロック ページは表示されませんが、代わりに、最も厳密なセーフ サーチ オプションを適用する検索クエリに自動的にリダイレクトされます。この安全な検索の実施方法は、Google、Yahoo、および Bing の検索でサポートされています。

検索プロバイダ毎にセーフ サーチ設定が異なるため、まずは各セーフ サーチの実装方法を確認してください。次に、セーフ検索を無効にした場合に検索結果をブロックする方法、またはユーザーの安全な検索を透過的に有効にする方法の 2 つのうちのいずれかで、安全な検索を強制します。

- 検索プロバイダのセーフ サーチ設定
- 厳密なセーフ サーチが有効でない場合の検索結果のブロック
- ユーザーに対して透過的にセーフ サーチの有効化

検索プロバイダのセーフ サーチ設定

検索プロバイダ毎にセーフ サーチ設定が異なるため、次の設定を確認して理解を深めてください。

検索プロバイダ	セーフ サーチ設定の説明
Google/YouTube	個々のコンピュータまたはネットワーク全体（Google のセーフ サーチ仮想 IP アドレスを使用）でセーフ サーチを提供します。 個々のコンピュータでの **Google** 検索のセーフ サーチの適用 Google の検索の設定 の **Filter explicit results**（不適切な検索結果を除外する） 設定で、セーフ サーチ機能を有効にします。有効にした設定はブラウザの Cookie に **FF=** として保存され、ユーザーが Google の検索を実行するたびにサーバーに渡されます。 **safe=active** を Google の検索クエリ URL に追加して、最も厳密なセーフ サーチ設定を有効にすることもできます。 仮想 **IP** アドレスを使用した **Google** および **YouTube** 検索のセーフ サーチの適用 Google が提供するサーバー（forcesafesearch.google.com）では、すべての Google および YouTube 検索で、Lock SafeSearch(セーフサーチをロック)するように設定できます。**forcesafesearch.google.com** を指し示す CNAME レコードを含む、**www.google.com** と **www.youtube.com**（および Google や YouTube に関連するその他の国別サブドメイン）の DNS エントリを DNS サーバー設定に追加すると、ネットワーク上のすべてのユーザーが Google または YouTube 検索を実行するときに必ず厳密なセーフ サーチ設定を使用するようになります。ただし、このソリューションには、ファイアウォールの Safe Search Enforcement（セーフ サーチを適用）との互換性はありません。したがって、このオプションを使用して Google で安全な検索を強制する場合、カスタム URL カテゴリを作成して URL フィルタリング プロファイルのブロック リストに追加することで、ファイアウォール上の他の検索エンジンへのアクセスをブロックすることをお勧めします。

検索プロバイダ	セーフ サーチ設定の説明
	 • *PAN-OS* は、*HTTP*ヘッダー挿入による *YouTube* のセーフサーチ適用をサポートします。*HTTP* ヘッダー挿入は現在 *HTTP/2* をサポートしていません。*YouTube* の安全な検索を強制するには、適切な復号化プロファイルの ***Strip ALPN***機能を使用して、*HTTP/2* 接続を *HTTP/1.1* にダウングレードする<があります。 • *Google* のセーフ サーチ ロック ソリューションの使用を計画している場合、*DNS* プロキシ（***Network (ネットワーク) > DNS Proxy (DNS プロキシ)***）を設定し、*DHCP* を介してサービス プロバイダからファイアウォールに *DNS* 設定を送信するときに使用するレイヤー *3* インターフェイスとして継承ソースを設定することを検討してください。*forcesafesearch.google.com* サーバーのローカル *IP* アドレスを使用して、*www.google.com* と *www.youtube.com* の *[*スタティック エントリ*]* で *DNS* プロキシを設定します。
Yahoo	個々のコンピュータでのみセーフ サーチを提供します。Yahoo の 検索設定 には3つのセーフサーチ設定があります。**Strict** [強]、**Moderate** [中]、**Off** [オフ]。有効にした設定はブラウザの Cookie に `vm=` として保存され、ユーザーが Yahoo の検索を実行するたびにサーバーに渡されます。 `vm=r` を Yahoo の検索クエリ URL に追加して、最も厳密なセーフ サーチ設定を有効にすることもできます。

検索プロバイダ	セーフ サーチ設定の説明
	Yahoo アカウントでログイン中に *Yahoo Japan*（*yahoo.co.jp*）で検索を実行する場合、エンド ユーザーは *[*チャイルド ロック*]* オプションも有効にする必要があります。
Bing	個々のコンピュータまたは Bing in the Classroom プログラムでセーフ サーチを提供します。Bing の 検索設定 には3つのセーフサーチ設定があります。**Strict** [強]、**Moderate** [中]、**Off** [オフ]。有効にした設定はブラウザの Cookie に **adtl=** として保存され、ユーザーが Bing の検索を実行するたびにサーバーに渡されます。 **adlt=strict** を Bing の検索クエリ URL に追加して、最も厳密なセーフ サーチ設定を有効にすることもできます。 Bing SSL 検索エンジンでは、セーフ サーチ URL パラメータが適用されないため、完全なセーフ サーチを適用するために SSL 経由の Bing をブロックすることを検討してください。

厳密なセーフ サーチが有効でない場合の検索結果のブロック

デフォルトでは、セーフサーチの適用を有効にし、ユーザーが最も厳密な設定なしで検索した場合、firewallは検索結果をブロックし、URLフィルタリング セーフサーチ ブロックページ をブラウザに表示します。応答ページには、エンド ユーザーが設定を調整できるように、対応する検索プロバイダーの検索設定ページへのリンクが表示されます。URL フィルタリング 応答ページ をカスタマイズして、組織の特定のニーズを満たすことができます。この既定の方法を使用してセーフ サーチを適用する場合は、ポリシーを実装する前にエンド ユーザーに通知する必要があります。または、透過的にユーザーのセーフサーチを有効に して、ユーザーが手動で設定を構成する必要がないようにすることもできます。

検索プロバイダのセーフ サーチ設定各検索事業者がどのようにセーフサーチを実装しているかをまとめたものです。

STEP 1 | URL フィルタリング プロファイルでセーフ サーチの適用を有効にします。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **URL Filtering (URL フィルタリング)** の順に選択します。
2. 既存のプロファイルを選択して変更するか、デフォルト プロファイルをコピーして新しいプロファイルを作成します。
3. **Settings** タブで、**Safe Search Enforcement** オプションを選択します。
4. （任意）ユーザーが特定の検索エンジンにしかアクセスできないようにします。
   1. **[カテゴリ]** タブで、**[search-engines]** カテゴリを **[block]** に設定します。
   2. ユーザーにアクセスを許可する各検索エンジンの Web アドレスを **[許可リスト]** テキスト ボックスに入力します。たとえば、Google および Bing 検索へのアクセスのみをユーザーに許可する場合、以下のように入力します。

      ```
      www.google.com
      ```

      ```
      www.bing.com
      ```
5. 必要に応じて、その他の設定を指定します。
   - 2
   - URL カテゴリに関係なく、ブロックまたは許可される Web サイトを指定するブロックリストと許可リストを定義します。
6. **OK** をクリックしてプロファイルを保存します。

STEP 2 | 信頼ゾーン内のクライアントからインターネットへのトラフィックを許可するセキュリティ ポリシー ルールに URL フィルタリング プロファイルを追加します。

1. **Policies** > セキュリティ を選択し、検索の安全な強制を有効にしたばかりの URL フィルタリング プロファイルを適用するルールを選択します。
2. **Actions**（操作） タブで、**URL Filtering**（**URL** フィルタリング） プロファイルを選択します。
3. [**OK**] をクリックして、セキュリティ ポリシー ルールを保存します。

STEP 3 | SSL フォワード プロキシ復号化を有効にします。

ほとんどの検索エンジンは検索結果を暗号化するため、ファイアウォールが検索トラフィックを検査し、安全な検索設定を検出できるように、SSL Forward Proxy 復号化を有効にする必要があります。

1. 検索サイトのカスタム URL カテゴリを追加します。
   1. **Objects (オブジェクト)** > **Custom Objects (カスタム オブジェクト)** > **URL Category (URL カテゴリ)** を選択してカスタム カテゴリを **Add (追加)** します。
   2. カテゴリの **Name** [名前]（SearchEngineDecryption など）を入力します。
   3. 以下を [サイト] リストに **[追加]** します。

      www.bing.*

      www.google.*

      search.yahoo.*
   4. **[OK]** をクリックしてカスタム URL カテゴリ オブジェクトを保存します。
2. SSL フォワード プロキシ を構成する手順に従います。
3. 復号化ポリシー規則の **Service/URL Category** タブで、作成したカスタム URL カテゴリを **Add** し、[**OK** をクリックします。

STEP 4 | （任意）SSL 経由で実行される Bing 検索トラフィックをブロックします。

Bing SSL 検索エンジンは、セーフ サーチ設定に従わないため、完全なセーフ サーチを適用するために、SSL 経由で実行されるすべての Bing セッションを拒否する必要があります。

1. Bing のカスタム URL カテゴリを追加します。
   1. **Objects (オブジェクト)** > **Custom Objects (カスタム オブジェクト)** > **URL Category (URL カテゴリ)** を選択してカスタム カテゴリを **Add (追加)** します。
   2. カテゴリの **[名前]**（EnableBingSafeSearch など）を入力します。
   3. 以下を [サイト] リストに **[追加]** します。

      `www.bing.com/images/*`

      `www.bing.com/videos/*`
   4. **[OK]** をクリックしてカスタム URL カテゴリ オブジェクトを保存します。
2. 作成したカスタム カテゴリをブロックする別の URL フィルタリング プロファイルを作成します。
   1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **URL Filtering (URL フィルタリング)** の順に選択します。
   2. 新しいプロファイルを **[追加]** し、分かりやすい **[名前]** をつけます。
   3. [カテゴリ] リストでカスタム カテゴリを見つけて、**[block]** に設定します。
   4. **OK**をクリックして、URL フィルタリング プロファイルを保存します。
3. SSL トラフィックをブロックするセキュリティ ポリシー ルールBing追加します。
   1. **Policies (ポリシー)** > **Security (セキュリティ)** の順に選択し、Trust ゾーンからインターネットへのトラフィックを許可するポリシー ルールを **Add (追加)** します。
   2. **Actions** タブで、カスタム Bing カテゴリをブロックするために作成した URL フィルタリング プロファイルを添付します。
   3. **[サービス/URL カテゴリ]** タブで、新しいサービスを **[追加]** し、分かりやすい **[名前]**（bingssl など）をつけます。
   4. **[プロトコル]** として **[TCP]** を選択し、**[宛先ポート]** を 443 に設定します。
   5. **OK** をクリックしてルールを保存します。
   6. **[移動]** オプションを使用して、セーフ サーチの強制が有効になっている URL フィルタリング プロファイルが設定されたルールの下にこのルールがくるようにします。

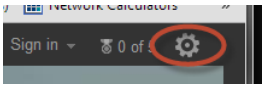
STEP 5 | 設定を保存します。

Commit（コミット）をクリックします。

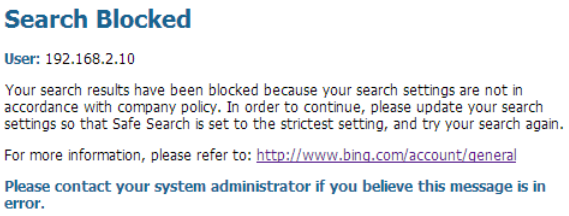
STEP 6 | Safe Search Enforcement （セーフ サーチを適用）設定を確認します。

この確認手順は、ブロック ページを使用してセーフ サーチを適用している場合にのみ機能します。透過的なセーフ サーチの適用を使用している場合、ファイアウォールのブロック ページでは、クエリ文字列のセーフ サーチ パラメータで URL が書き換えられます。

1. ファイアウォールの背後にあるコンピュータから、サポートされているいずれかの検索プロバイダの厳密な検索設定を無効にします。たとえば、bing.com で、Bing メニューバーの設定アイコンをクリックします。



2. **[セーフサーチ]** オプションを **[標準]** または **[オフ]** に設定し、**[保存]** をクリックします。
3. Bing 検索を実行し、検索結果ではなく、URL Filtering Safe Search Block page （URL フィルタリング セーフ サーチのブロック ページ）が表示されることを確認します。



4. ブロック ページのリンクを使用して、検索プロバイダの検索設定に移動し、セーフ サーチ設定を最も厳密な設定（Bing の場合は **[高レベル]**）に戻し、**[保存]** をクリックします。
5. Bing から再度検索を実行し、ブロック ページではなく、フィルタリングされた検索結果が表示されることを確認します。

ユーザーに対して透過的にセーフ サーチの有効化

最も厳密なセーフ サーチ フィルタで検索クエリ結果をフィルタリングするが、エンド ユーザーが手動で設定する必要がないようにする場合、以下のように透過的なセーフ サーチの適用を有効にできます。この機能は、Google、Yahoo、および Bing 検索エンジンでのみサポートされており、コンテンツ リリース バージョン 475 以降が必要です。

STEP 1 | ファイアウォールでコンテンツ リリース バージョン 475 以降が実行されていることを確認します。

1. Select **Device (デバイス)** > **Dynamic Updates (動的アップデート)**を選択します:
2. **[アプリケーションおよび脅威]** セクションを確認し、現在どの更新が実行されているのかを特定します。
3. ファイアウォールで必要なバージョン（またはそれ以降）の更新が実行されていない場合、**Check Now**（今すぐチェック）をクリックし、使用可能な更新のリストを取得します。
4. 必要な更新を見つけて **[ダウンロード]** をクリックします。
5. ダウンロードが完了したら、**Install**（インストール）をクリックします。

STEP 2 | URL フィルタリング プロファイルでセーフ サーチの適用を有効にします。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **URL Filtering (URL フィルタリング)** の順に選択します。
2. 既存のプロファイルを選択して変更するか、デフォルト プロファイルをコピーして新しいプロファイルを作成します。
3. **Settings**（設定） タブで、**Safe Search Enforcement**（セーフ サーチを適用） チェックボックスをオンにして有効にします。
4. （任意）特定の検索エンジンへのアクセスのみを許可します。
   1. **[カテゴリ]** タブで、**[search-engines]** カテゴリを **[block]** に設定します。
   2. ユーザーにアクセスを許可する各検索エンジンの Web アドレスを **[許可リスト]** テキスト ボックスに入力します。たとえば、Google および Bing 検索へのアクセスのみをユーザーに許可する場合、以下のように入力します。

      ```
      www.google.com
      ```

      ```
      www.bing.com
      ```
5. 必要に応じて、その他の設定を指定します。
   - URL カテゴリ毎にサイト アクセスを定義します。
   - URL カテゴリに関係なく、ブロックまたは許可される Web サイトを指定するブロックリストと許可リストを定義します。
6. **OK** をクリックしてプロファイルを保存します。

STEP 3 | 信頼ゾーン内のクライアントからインターネットへのトラフィックを許可するセキュリティ ポリシー ルールに URL フィルタリング プロファイルを追加します。

1. **Policies** > セキュリティ を選択し、検索の安全な強制を有効にしたばかりの URL フィルタリング プロファイルを適用するルールを選択します。
2. **Actions**（操作） タブで、**URL Filtering**（**URL** フィルタリング） プロファイルを選択します。
3. **OK** をクリックして、セキュリティ ポリシー ルールを保存します。

STEP 4 | （任意）SSL 経由で実行される Bing 検索トラフィックをブロックします。

Bing SSL 検索エンジンは、セーフ サーチ設定に従わないため、完全なセーフ サーチを適用するために、SSL 経由で実行されるすべての Bing セッションを拒否する必要があります。

1. Bing のカスタム URL カテゴリを追加します。
   1. **Objects (オブジェクト)** > **Custom Objects (カスタム オブジェクト)** > **URL Category (URL カテゴリ)** を選択してカスタム カテゴリを **Add (追加)** します。
   2. カテゴリの **[名前]**（EnableBingSafeSearch など）を入力します。
   3. 以下を [サイト] リストに **[追加]** します。

      `www.bing.com/images/*`

      `www.bing.com/videos/*`
   4. **[OK]** をクリックしてカスタム URL カテゴリ オブジェクトを保存します。
2. 作成したカスタム カテゴリをブロックする別の URL フィルタリング プロファイルを作成します。
   1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **URL Filtering (URL フィルタリング)** の順に選択します。
   2. 新しいプロファイルを **[追加]** し、分かりやすい **[名前]** をつけます。
   3. [カテゴリ] リストで、作成したカスタム カテゴリを見つけ、**[block]** に設定します。
   4. **OK** をクリックして、URL フィルタリング プロファイルを保存します。
3. **add** SSL トラフィックをブロックするセキュリティ ポリシー ルールBingします。
   1. **Policies (ポリシー)** > **Security (セキュリティ)** の順に選択し、Trust ゾーンからインターネットへのトラフィックを許可するポリシー ルールを **Add (追加)** します。
   2. **Actions** タブで、カスタム Bing カテゴリをブロックするために作成した URL フィルタリング プロファイルを添付します。
   3. **[サービス/URL カテゴリ]** タブで、新しいサービスを **[追加]** し、分かりやすい **[名前]**（bingssl など）をつけます。
   4. **[プロトコル]** として **[TCP]** を選択し、**[宛先ポート]** を **443** に設定します。
   5. **OK** をクリックしてルールを保存します。
   6. **Move** オプションを使用して、このルールが、安全な検索の強制が有効になっている URL フィルタリング プロファイルを持つルールの下にあることを確認します。

STEP 5 | URL フィルタリング セーフ サーチのブロック ページを編集し、既存のコードを、検索クエリ URL を書き換えて透過的にセーフ サーチを適用する Javascript に置き換えます。

1. **Device (デバイス)** > **Response Pages (応答ページ)** > **URL Filtering Safe Search Block Page (URL フィルタリング セーフ サーチのブロック ページ)** を選択します。
2. **[事前定義済み]** を選択し、**[エクスポート]** をクリックして、ファイルをローカルに保存します。
3. HTML エディタを使用して、既存のすべてのブロック ページ テキストを以下のテキストに置き換えて、ファイルを保存します。

```
<html> <head> <title>検索ブロック</title> <meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
 <meta http-equiv="pragma" content="no-cache"> <meta
 name="viewport" content="initial-scale=1.0"> <style> #content
 { border:3px solid#aaa; background-color:#fff; margin:1.5em;
 padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-serif;
 font-size:1em; } h1 { font-size:1.3em; font-weight:bold;
 color:#196390; } b { font-weight:normal; color:#196390; }</
style> </head> <body bgcolor="#e7e8e9"> <div id="content">
 <h1>検索がブロックされた</h1> <p> <b>ユーザー:</b><user/> </
p> <p>検索設定が会社のポリシーに従っていないため、検索結果がブロックされました。続行するには、Safe Searchが最も厳しい設定に設定されるように検索設定を更新してください。現在アカウントにログインしている場合は、Safe Searchもロックして検索を再試行してください。</p><p> 詳細については、<a href="<ssurl/>"を参照してください> <ssurl/> </
a> </p> <p id="java_off">お使いのブラウザでJavaScriptを有効にしてください。<br></p><p><b>このメッセージに誤りがあると思われる場合は、システム管理者に問い合わせてください。</b></p> </div> </
body> <script> // ブラウザにある URL を取得します。var s_u =
 location.href;bing // 先頭のスラッシュ、何でも、次に ".bing." 、次に何かに一致し、その後に非貪欲なスラッシュが続きます。うまくいけば、最初のスラッシュ。var b_a = /^.*//(.+.bing..+?)//.exec(s_u);if (b_a)
 { s_u = s_u + "&adlt=strict"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 'あなたはより安全な検索にリダイレクトされています!'; } //
google // 冒頭のスラッシュと一致し、次に ".google." 、その後に非貪欲なスラッシュが続きます。うまくいけば、最初のスラッシュ。var g_a = /^.*//(.+.google..+?)//.exec(s_u);if
 (g_a) { s_u = s_u.replace(/&safe=off/ig,""); s_u =
 s_u + "&safe=active"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML = 'あなたはより安全な検索にリダイレクトされています!'; } //yahoo // 先頭のスラッシュと一致し、次に ".yahoo."" の後に ".yahoo."" が続きます。うまくいけば、最初のスラッシュ。var y_a = /^.*//(.+.yahoo..
+?)//.exec(s_u);if (y_a) { s_u = s_u.replace(/&vm=p/
ig,""); s_u = s_u + "&vm=r"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML
 = 'You are redirected to a safer search!'; }
 document.getElementById("java_off").innerHTML = ' ';</script>
 </html>
```

STEP 6 | 編集した URL フィルタリング セーフ サーチのブロック ページをファイアウォールにインポートします。

1. 編集したブロック ページをインポートするには、**Device (デバイス)** > **Response Pages (応答ページ)** > **URL Filtering Safe Search Block Page (URL フィルタリング セーフ サーチのブロック ページ)** の順に選択します。
2. **Import**（インポート）をクリックし、**Import File**（インポート ファイル）フィールドにパスとファイル名を入力するか、**Browse**（参照）をクリックしてファイルを指定します。
3. （任意）**Destination** [宛先]ドロップダウンリストから、このログイン ページが使用される仮想システムを選択するか、すべての仮想システムから利用できるように **Shared** [共有]を選択します。
4. **OK** をクリックしてファイルをインポートします。

STEP 7 | SSL フォワード プロキシ復号化を有効にします。

大部分の検索エンジンでは検索結果が暗号化されるため、ファイアウォールで検索トラフィックを調べてセーフ サーチ設定を検出できるように、SSL フォワード プロキシ復号化を有効にする必要があります。

1. 検索サイトのカスタム URL カテゴリを追加します。
   1. **Objects (オブジェクト)** > **Custom Objects (カスタム オブジェクト)** > **URL Category (URL カテゴリ)** を選択してカスタム カテゴリを **Add (追加)** します。
   2. カテゴリの **Name** [名前]（SearchEngineDecryption など）を入力します。
   3. 以下を [サイト] リストに **[追加]** します。

      www.bing.*

      www.google.*

      search.yahoo.*
   4. **[OK]** をクリックしてカスタム URL カテゴリ オブジェクトを保存します。
2. SSL フォワード プロキシ を構成する手順に従います。
3. 復号ポリシー ルールの **Service/URL Category** [サービス/URL カテゴリ]タブで、作成したカスタム URL カテゴリを **Add** [追加]し、**OK** をクリックします。

STEP 8 | 設定を保存します。

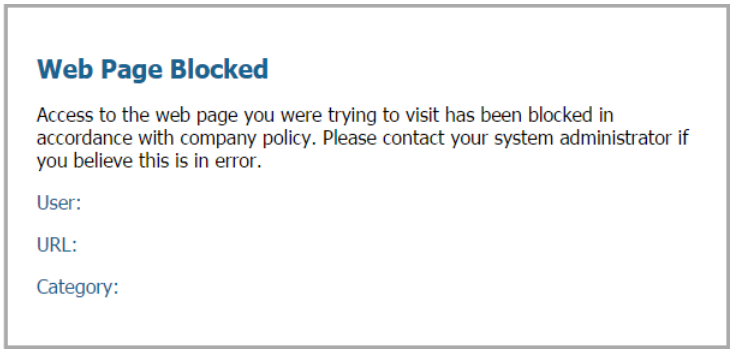
Commit（コミット）をクリックします。

URL フィルタリング応答ページ

ファイアウォールには、URL フィルタリング プロファイルのいずれかのブロック アクション（block、continue、または override）で設定されたカテゴリのサイトをユーザーが閲覧しようとしたとき、またはコンテナ ページが有効になっているときに、デフォルトで表示される事前定義済みの 3 つの応答ページが用意されています。

- **URL** フィルタリングおよびカテゴリ一致ブロック ページ

  URL フィルタリング プロファイルによってブロックされたアクセス、または URL カテゴリがセキュリティ ポリシー ルールによってブロックされているため。



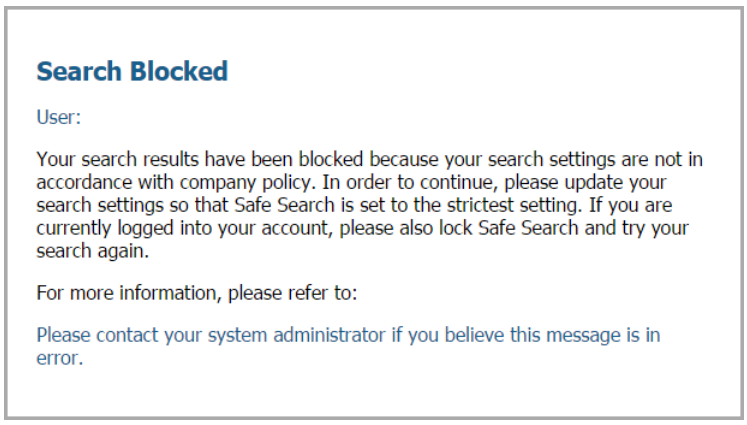
- **URL** フィルタリングの続行とオーバーライド ページ

  Continue (続行) をクリックすることでユーザーがブロックをバイパスできる、最初のブロック ポリシーを持つページです。URL 管理の上書きを有効にした (特定のサイトへのパスワードアクセスを許可する)、**Continue** をクリックした後、ユーザーは URL をブロックするポリシーを上書きするためにパスワードを入力する必要があります。

- **URL** フィルタリング セーフ サーチのブロック ページ

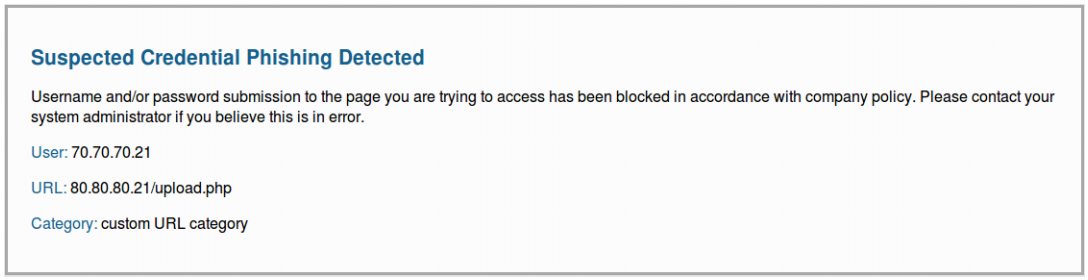
  Safe Search Enforcement (セーフ サーチを適用) オプションが有効になっている URL フィルタリング プロファイルを使用したセキュリティ ポリシー ルールによって、アクセスがブロックされたことを示します（セーフ サーチの適用を参照）。Google、Bing、Yahoo、または

Yandex を使用して検索が実行され、ブラウザまたは検索エンジン アカウント設定でセーフサーチが厳密に設定されていない場合、このページが表示されます。



- アンチフィッシング ブロックページ

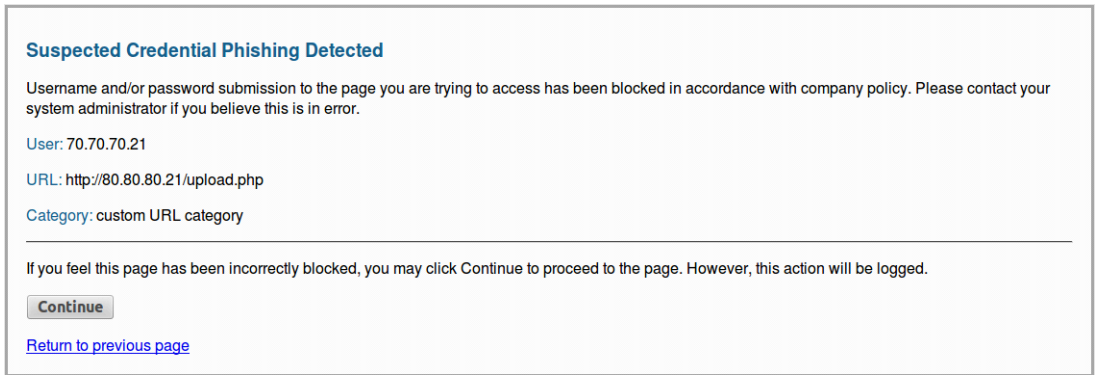
  このページは、認証情報の送信がブロックされているカテゴリーに属する Web ページで、ユーザーが企業の認証情報（ユーザー名あるいはパスワード）を入力しようとしたときに表示されます。ユーザーは引き続きサイトにアクセスできますが、関連する Web フォームに企業の有効な認証情報を送信することはできません。ユーザーが企業の資格情報を送信できるサイトを制御するには、ファイアウォールにユーザー ID を構成し、URL カテゴリに基づいて フィッシング詐欺を防止する に設定する必要があります。



- アンチフィッシング 続行ページ

  このページは、認証情報（ユーザー名とパスワード）を Web サイトに送信することに対してユーザーに警告を表示します。認証情報の送信に対してユーザーに警告を表示することで、企業の認証情報をユーザーが再利用することを阻止できるほか、フィッシングの可能性についてユーザーを教育することができます。サイトで認証を続行するには、ユーザーが Continue (続行) を選択する必要があります。ユーザーが企業の資格情報を送信できるサ

イトを制御するには、ファイアウォールにユーザー ID を構成し、URL カテゴリに基づいて フィッシング詐欺を防止する に設定する必要があります。



事前定義済みのページを使用することも、特定の利用規定やコーポレート ブランディングに合わせてURL フィルタリング応答ページのカスタマイズを行うこともできます。さらに、URL フィルタリング応答ページ変数 をブロック イベント時の置換に使用したり、サポートされている 応答ページ参照 のいずれかを外部イメージ、サウンド、またはスタイル シートに追加したりできます。

検査 SSL/TLS ハンドシェイク を有効にしている場合、ブラウザは応答ページを表示しません。

表 **2 : URL** フィルタリング応答ページの変数

変数	使用率
<user/>	ファイアウォールは、応答ページを表示するときにこの変数をユーザー名（ユーザー ID を介して使用可能な場合）またはユーザーの IP アドレスに置き換えます。
<url/>	ファイアウォールは、応答ページを表示するときにこの変数を、要求された URL に置き換えます。
<category/>	ファイアウォールは、この変数を、ブロックされた要求の URL フィルタリング カテゴリに置き換えます。
<pan_form/>	URL Filtering Continue and Override page [URL フィルタリングの続行とオーバーライド ページ]に **Continue** [続行]ボタンを表示する HTML コード。

ユーザーがアクセスしようとしている URL カテゴリに基づいて異なるメッセージを表示するようにファイアウォールをトリガーするコードを追加することもできます。たとえば、応答ページから以下のコード スニペットを使用して、URL カテゴリが games の場合は Message 1、カテゴリが travel の場合は Message 2、カテゴリが kids の場合は Message 3 を表示するように指定します。


```
var cat = "<category/>"; switch(cat) { case 'games':
 document.getElementById("warningText").innerHTML = "Message 1";
 break; case 'travel':
 document.getElementById("warningText").innerHTML = "Message 2";
 break; case 'kids': document.getElementById("warningText").innerHTML
 = "Message 3"; break; }
```

各仮想システムにロードできるのは、ブロック ページのタイプごとに 1 つの HTML ページのみです。ただし、イメージ、サウンド、カスケード スタイル シート（CSS ファイル）などの他のリソースは、ブラウザに応答ページが表示されるときに他のサーバーからロードできます。すべてのリファレンスに完全修飾 URL が含まれている必要があります。

表 **3 :** 応答ページのリファレンス

リファレンス タイプ	**HTML** コードの例
Image （イメージ）	`<img src="http://virginiadot.org/images/Stop-Sign-gif.gif">`
サウンド	`<embed src="http://simplythebest.net/sounds/WAV/WAV_files/ movie_WAV_files/ do_not_go.wav" volume="100" hidden="true" autostart="true">`
スタイル シート	`<link href="http://example.com/style.css" rel="stylesheet" type="text/css" />`
ハイパーリンク	`<a href="http://en.wikipedia.org/wiki/Acceptable_use_policy">企業ポリシーを表示</a>`

URL フィルタリング応答ページのカスタマイズ

ファイアウォールは、次の場合に既定で表示される定義済みの URL フィルタリング応答ページを提供します。

- アクセスが制限されているカテゴリに属すサイトをユーザーが閲覧しようと試みる際。
- ユーザーは、資格情報の検出が有効になっているサイトに有効な企業資格情報を送信します (URL カテゴリに基づいて認証情報フィッシングの阻止)。
- ユーザーがアクセスしたページのみを記録検索の試行をブロックします。

ただし、コーポレート ブランディング、利用規定、内部リソースへのリンクを使用して独自のカスタム応答ページを作成できます。

サポートされている最大サイズを超えるカスタム応答ページは復号化されないか、ユーザーに対して表示されません。*PAN-OS 8.1.2* および古い *PAN-OS 8.1* リリースでは、復号化されているサイトのカスタム応答ページは *8,191* バイトを超えられません。*PAN-OS 8.1.3* 以降のリリースでこの最大サイズが *17,999* バイトに増加しました。

STEP 1 | デフォルト応答ページをエクスポートします。

1. **Device(デバイス) > Response Pages(応答ページ)** の順に選択します。
2. 変更する URL フィルタリング応答ページのリンクを選択します。
3. 応答ページ（[事前定義済み] または [共有]）をクリックして、**[エクスポート]** リンクをクリックし、そのファイルをデスクトップに保存します。

STEP 2 | エクスポートしたページを編集します。

1. 任意の HTML テキスト エディタを使用して、ページを編集します。
   - ブロックされた特定のユーザー、URL、またはカテゴリに関するカスタム情報を応答ページに表示する場合は、サポートされている 応答ページ変数 を 1 つ以上追加します。
   - カスタムイメージ (企業ロゴなど)、サウンドシート、スタイルシート、または別の URL へのリンク (Web 使用ポリシーの詳細を示すドキュメントなど) を含める場合は、サポートされている 応答ページ参照 を 1 つ以上含めます。
2. 編集したページを新しいファイル名で保存します。ページが UTF-8 エンコーディングのままであることを確認してください。たとえば、メモ帳の [名前を付けて保存] ダイアログで、**[文字コード]** ドロップダウンから **[UTF-8]** を選択すします。

STEP 3 | カスタマイズした応答ページをインポートします。

1. **Device(デバイス) > Response Pages(応答ページ)** の順に選択します。
2. 編集した URL フィルタリング応答ページに対応するリンクを選択します。
3. **Import**（インポート）をクリックし、**Import File**（インポート ファイル）フィールドにパスとファイル名を入力するか、**Browse**（参照）をクリックしてファイルを指定します。
4. （任意）**Destination** [宛先]ドロップダウンリストから、このログイン ページが使用される仮想システムを選択するか、すべての仮想システムから利用できるように **Shared** [共有]を選択します。
5. **OK** をクリックしてファイルをインポートします。

STEP 4 | 新しい応答ページを保存します。

変更を **Commit**（コミット）します。

STEP 5 | 新しい応答ページが表示されることを確認します。

ブラウザから、応答ページをトリガーする URL に移動します。たとえば、変更された URL フィルタリングとカテゴリ一致の応答ページを表示するには、URL フィルタリング ポリシーがブロックするように設定されている URL を参照します。

ファイアウォールは、次のポートを使用して URL フィルタリング応答ページを表示します。

- **HTTP**—6080
- **Default TLS with firewall certificate (**ファイアウォール証明書を含む デフォルト**TLS)** —6081
- **Custom SSL/TLS profile (**カスタム **SSL/TLS** プロファイル**)** —6082

HTTP ヘッダのロギング

URL フィルタリングでは、ネットワーク上の Web トラフィックを可視化および制御できます。Web コンテンツの可視化を向上させるために、Web 要求に含まれる HTTP ヘッダー属性をログに記録するように URL フィルタリング プロファイルを設定できます。クライアントが Web ページを要求すると、ユーザー エージェント、Referer、x-forwarded-for フィールドが属性-値ペアとして HTTP ヘッダーに格納され、Web サーバーに転送されます。ファイアウォールで HTTP ヘッダーのロギングが有効になっている場合、以下の属性-値ペアが URL フィルタリング ログに記録されます。

HTTP ヘッダーを使用して、*SaaS* アプリケーションへのアクセスを管理することもできます。これを行うために *URL* フィルタリング ライセンスは必要ありませんが、この機能をオンにするには *URL* フィルタリング プロファイルを使用する必要があります。

属性	説明
ユーザーエージェント	ユーザーが URL へのアクセスに使用した Web ブラウザ（Internet Explorer など）。この情報は、HTTP 要求でサーバーに送信されます。 HTTP ヘッダーには、ユーザー エージェントの完全な文字列が含まれていません。ヘッダー・エンドを含むパケットより前のパケットからの最大ログ・バイト数は 36 バイトです。
リファラー	ユーザーを別の Web ページにリンクした Web ページの URL。要求された Web ページにユーザーをリダイレクト（参照）した送信元です。
X-Forwarded-For （XFF）	Web ページを要求したユーザーの IP アドレスを保持する HTTP 要求のヘッダー フィールドのオプション。ネットワークにプロキシ サーバーがある場合、XFF により、Web ページを要求した送信元 IP アドレスとしてプロキシ サーバーの IP アドレスを記録するだけではなく、コンテンツを要求したユーザーの IP アドレスを識別できます。
挿入されたヘッダー	ファイアウォールが挿入するヘッダーのタイプとヘッダーのテキスト。

URL のカテゴリを変更するためのリクエスト

URL が正確に分類されていないと思われる場合は、別の分類を要求することができます。ファイアウォールで直接変更要求を送信するか、Test A Site を使用します。変更要求により、PAN-DB（URL フィルタリング クラウド）がトリガーされ、カテゴリの変更を提案している URL を即座に分析します。PAN-DB が新しいカテゴリの提案が正しいことを検証すると、変更要求が承認されます。PAN-DB が新しいカテゴリの提案が正確であると判断しない場合、変更要求は Palo Alto Networks の脅威調査チームとデータサイエンスチームの編集者によってレビューされます。

変更要求を送信すると、要求を受信したことを確認する電子メールが届きます。調査が完了すると、結果を確認する 2 回目の電子メールが届きます。

URL が受け取るリスクカテゴリ（**high risk (高リスク)**、**medium risk (中リスク)**、または**low risk (低リスク)**）、または**insufficient content (不十分なコンテンツ)**または**newly-registered domains (新しく登録されたドメイン)**として分類された URL への変更を要求することはできません。

- Make a Change Request Online（オンラインで変更要求を行う）
- Make a Bulk Change Request（一括変更要求を行う）
- Make a Change Request From the Firewall（ファイアウォールから変更要求を行う）

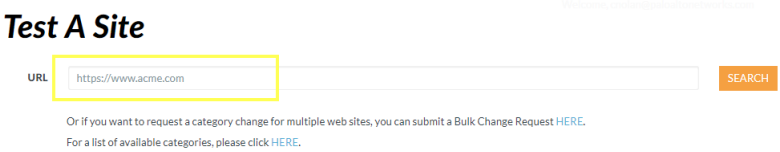
Make a Change Request Online（オンラインで変更要求を行う）

Palo Alto Networks URL Filtering Test A Site(サイトのテスト) にアクセスして、オンラインで変更要求を行ってください。

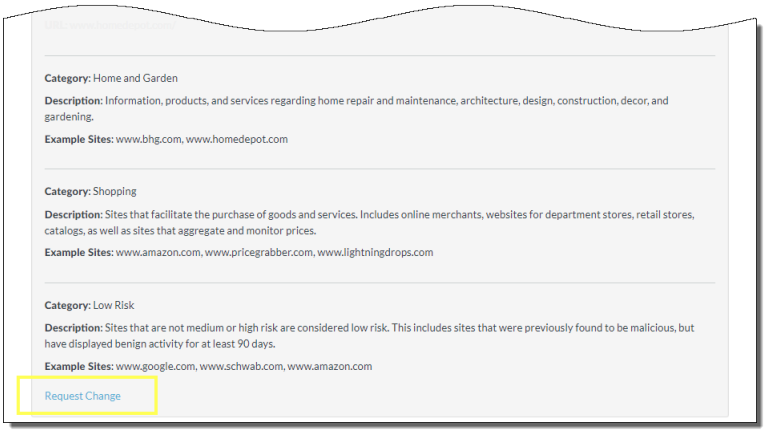
STEP 1 | Test A Site(サイトのテスト)に移動します。

変更要求を送信するためにログインする必要はありませんが、変更要求フォームの一部として電子メールを提供する必要があります。ログインしないことにした場合は、CAPTCHA テストを受けて、自分が人間であることを確認する必要があります（CAPTCHA テストを回避するにはログインしてください）。

STEP 2 | URL を入力して、カテゴリを確認します。

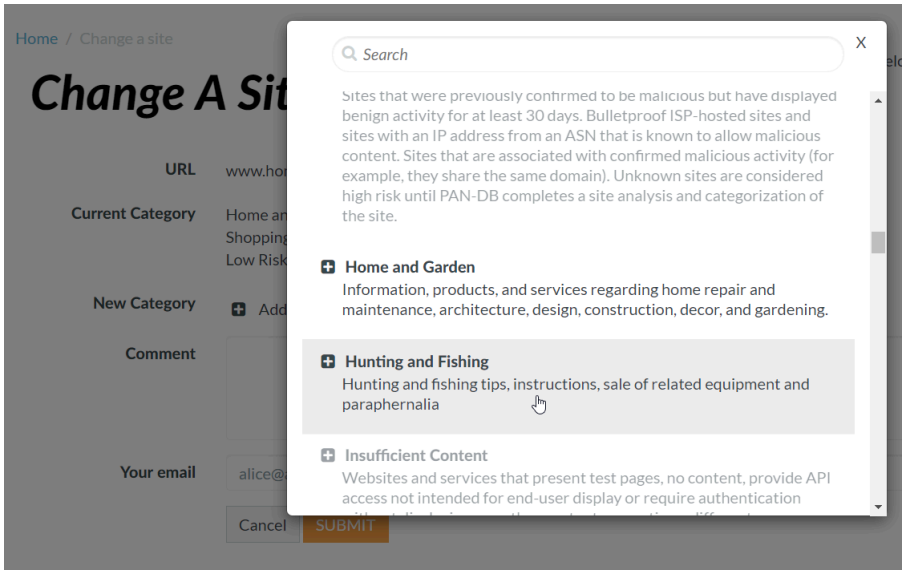


STEP 3 | URL カテゴリを確認し、正確ではないと思われる場合は、**Request Change (変更を要求)**を選択してください。



STEP 4 | 変更要求フォームの入力と送信を続けます。

少なくとも1つ（最大 2 つ）の新しいカテゴリの提案を含め、コメントを残して（任意）提案について詳しく教えてください。



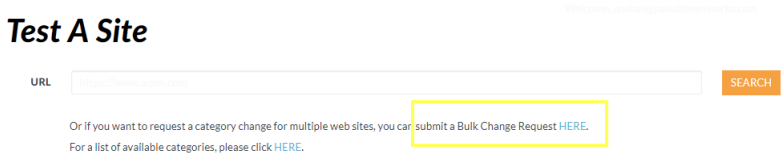
Make a Bulk Change Request（一括変更要求を行う）

また、Test A Site(サイトのテスト) を使用して一括変更要求を作成し、一度に複数の URL の変更要求を送信することもできます。

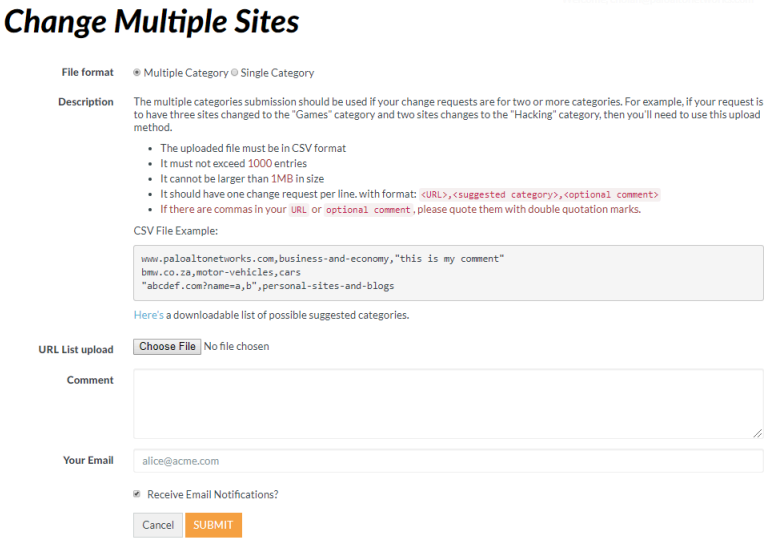
STEP 1 | Test A Site(サイトのテスト)に移動します。

変更要求を行うためにログインする必要はありません。 ただし、変更要求フォームの記入の一環として、電子メールアドレスを提供する必要があります。ログインしないことにした場合は、CAPTCHA テストを受けて、自分が人間であることを確認する必要があります（CAPTCHA テストを回避するにはログインしてください）。

STEP 2 | 一括変更要求を送信するオプションを選択します。

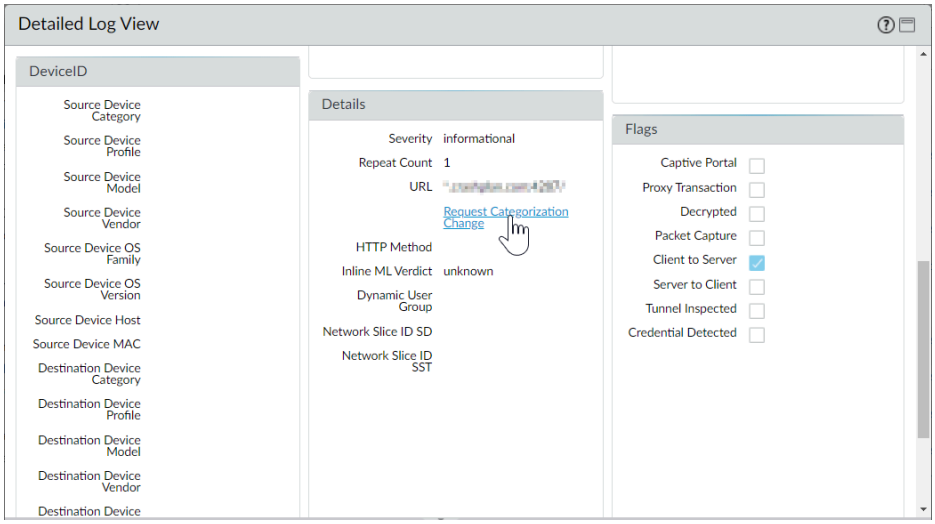


STEP 3 | 一括変更要求フォームに記入して送信します。

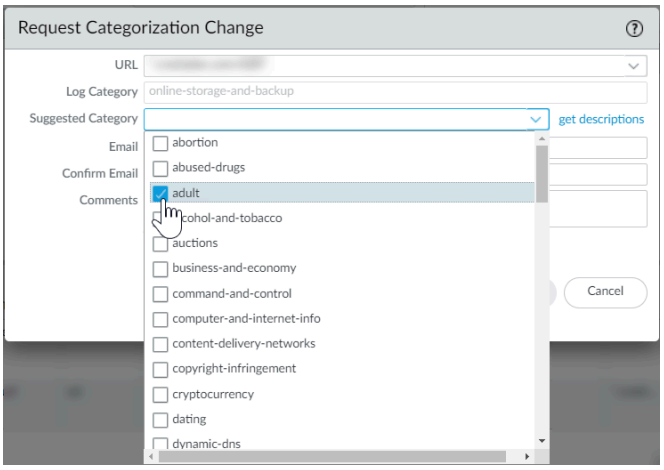


Make a Change Request from the Firewall（ファイアウォールから変更要求を行う）

ファイアウォールから直接 URL カテゴリ変更要求を送信することもできます。URL フィルタリング ログでは、各ログ エントリの詳細は、**Request Categorization Change**（分類変更の要求）（**Monitor**（監視） > **Logs**（ログ） > （**URL Filtering**）**URL** フィルタリング）へのオプションを含みます。



ここから、要求フォームに記入して送信できます。



URL フィルタリングのトラブルシューティング

以下のトピックでは、一般的な URL フィルタリングの問題を診断および解決するためのトラブルシューティングのガイドラインを説明します。

- 高度なURLフィルタリングのアクティブ化に関する問題
- PAN-DB クラウド接続の問題
- Not-Resolved に分類された URL
- 誤った分類

高度なURLフィルタリングのアクティブ化に関する問題

次のワークフローを使用して、高度なURLフィルタリングのアクティブ化の問題をトラブルシューティングします。

STEP 1 | PAN-OS CLI にアクセスします。

STEP 2 | 次のコマンドを実行して、高度なURLフィルタリングがアクティブ化されているかどうかを確認します。

```
show system setting url-database
```

応答が **paloaltonetworks**の場合、PAN-DB（Palo Alto Networks URLフィルタリングデータベース）がアクティブなベンダーです。

STEP 3 | 次のコマンドを実行して、ファイアウォールに有効なAdvancedURLFilteringライセンスがあることを確認します。

```
request license info
```

次のライセンス エントリ機能を確認してください。高度な URL フィルタリングライセンスがインストールされていない場合は、ライセンスを取得しインストールする必要があります。URL フィルタリングの設定を参照してください。

STEP 4 | PAN-DB クラウド接続ステータスを確認してください。

PAN-DB クラウド接続の問題

PAN-DB クラウドへの接続を確実にするために、専用の セキュリティポリシー ルール を作成し、すべての *Palo Alto Management Service* トラフィックを許可します。これにより、管理トラフィックが ***not-resolveed*** として分類されるのを防ぎ、データプレーンを経由する際にトラフィックがブロックされることを防ぐことができます。

firewall と PAN-DB クラウド間の接続を確認するには:

```
show url-cloud status
```

クラウドにアクセスできる場合は、以下のような応答が予測されます。

```
show url-cloud status PAN-DB URL Filtering License : valid Current
 cloud server : serverlist.urlcloud.paloaltonetworks.com Cloud
 connection : connected Cloud mode : public URL database version -
 device :20200624.20296 URL database version - cloud :20200624.20296
 ( last update time 2020/06/24 12:39:19 ) URL database status : good
 URL protocol version - device : pan/2.0.0 URL protocol version -
 cloud : pan/2.0.0 Protocol compatibility status : compatible
```

クラウドにアクセスできない場合は、以下のような応答が予測されます。

```
show url-cloud status PAN-DB URL Filtering License : valid
 Cloud connection : not connected URL database version -
 device :0000.00.00.000 URL protocol version - device : pan/0.0.2
```

次のチェックリストを使用し、接続の問題を特定して解決します。

- PAN-DB URL フィルタリング ライセンスのフィールドに invalid と表示されていますか？有効な PAN-DB ライセンスを取得してインストールします。
- URL プロトコルのバージョンが not compatible と表示されていますか？PAN-OS を最新バージョンにアップグレードします。
- ファイアウォールから PAN-DB クラウド サーバーに ping を行えますか？次のコマンドを実行してチェックします。

  ```
  ping source <ip-address> host
   serverlist.urlcloud.paloaltonetworks.com <
  ```

  たとえば、管理インターフェイス IP アドレスが 10.1.1.5 の場合、以下のコマンドを実行します。

  ```
  ping source 10.1.1.5 host serverlist.urlcloud.paloaltonetworks.com
  ```

- ファイアウォールは HA 構成ですか？ファイアウォールの HA 状態が active、active-primary、あるいは active-secondary 状態であることを確認します。ファイアウォールが他の状態である場合、PAN-DB クラウドへのアクセスがブロックされます。ペアになっている各ファイアウォールに対して次のコマンドを実行し、状態を確認します。

  ```
  show high-availability state
  ```

ファイアウォールおよび PAN-DB クラウド間の接続にまだ問題がある場合は、Palo Alto Networks のサポートにお問い合わせください。

Not-Resolved に分類された URL

URL は、PAN-DB URL フィルタリング クラウド サービスへの接続が中断され、URL 参照が失敗した場合に解決されないと分類されます。クラウド接続の状態と URL の分類は、有効期限が切れたサブスクリプション ライセンスまたはライセンスのないユーザーには適用されません。

次の流れで、PAN-DB で識別される一部またはすべての URL が Not-resolved に分類される問題を解決します。

STEP 1 | 以下のコマンドを実行して、PAN-DB のクラウド接続を確認します。

```
show url-cloud status
```

Cloud connection: フィールドに `connected` と表示されます。`connected` 以外が表示されている場合、管理プレーン キャッシュに存在しないすべての URL は、`not-resolved` に分類されます。この問題を解決する方法は、PAN-DB クラウド接続の問題を参照してください。

STEP 2 | クラウド接続の状態が `connected` と表示されている場合、ファイアウォールの現在の使用率を確認します。ファイアウォールの使用状況がスパイク状態である場合、URL 要求はドロップ（管理プレーンに到達することができない）され、`not-resolved` として分類されます。

システム リソースを表示するには、以下のコマンドを実行し、`%CPU` および `%MEM` 列を表示します。

```
show system resources
```

また、Web インターフェイスの**Dashboard (**ダッシュボード**)** にある System Resources (システム リソース) ウィジェットでシステム リソースを表示することもできます。

STEP 3 | 問題が解決しない場合は、Palo Alto Networks サポートにお問い合わせください。

誤った分類

時々、カテゴリ分けが間違っていると思われる URL に遭遇することもあるでしょう。次の作業を行うことで、サイトの URL カテゴリを判断し、必要に応じてカテゴリの変更をリクエストできます。

STEP 1 | 以下のコマンドを実行して、データプレーンのカテゴリを確認します。

```
show running url <URL>
```

たとえば、Palo Alto Networks Web サイトのカテゴリを表示するには、以下のコマンドを実行します。

```
show running url paloaltonetworks.com
```

データプレーン キャッシュに保存されている URL のカテゴリが正しい場合（この例では、computer-and-internet-info）、分類は正しく、さらに対策を実行する必要はありません。カテゴリが正しくない場合は、以下の手順に進みます。

STEP 2 | 以下のコマンドを実行して、管理プレーンのカテゴリを確認します

```
test url-info-host <URL>
```

以下に例を示します。

```
test url-info-host paloaltonetworks.com
```

管理プレーン キャッシュに保存されている URL のカテゴリが正しい場合、以下のコマンドを実行して、データプレーン キャッシュから URL を削除します。

```
clear url-cache url <URL>
```

次回、この URL のカテゴリをファイアウォールが要求すると、要求は管理プレーンに転送されます。この処理により問題は解決し、さらに対策を実行する必要はありません。この処理で問題が解決しない場合は、以下の手順に進み、クラウド システムの URL カテゴリを確認します。

STEP 3 | 以下のコマンドを実行して、クラウドのカテゴリを確認します。

```
test url-info-cloud <URL>
```

STEP 4 | クラウドに保存されている URL のカテゴリが正しい場合、データプレーンおよび管理プレーン キャッシュから URL を削除します。

データプレーン キャッシュから URL を削除するには、以下のコマンドを実行します。

```
clear url-cache url <URL>
```

管理プレーン キャッシュから URL を削除するには、以下のコマンドを実行します。

```
delete url-database url <URL>
```

次回、所定の URL のカテゴリをファイアウォールがクエリすると、要求は管理プレーンに転送され、さらに、クラウドに転送されます。これで、カテゴリ検索に関する問題は解決します。問題が解決しない場合は、以下の手順を参照して、分類の変更要求を提出します。

STEP 5 | Web インターフェイスから変更要求を提出するには、URL ログに移動して、変更する URL のログ エントリを選択します。

STEP 6 | [分類の変更要求] リンクをクリックして、以下の手順を実行します。URL を検索し、変更要求アイコンをクリックして、Palo Alto Networks の Test A Site Web サイトからカテゴリ変更を要求することもできます。すべての使用可能なカテゴリのリストと各カテゴリの説

明を表示する方法については、https://urlfiltering.paloaltonetworks.com/CategoryList.aspx を参照してください。

変更要求が承認されると、電子メール通知が送信されます。その後、2 つの方法で、ファイアウォールで URL カテゴリが更新されたことを確認できます。

- キャッシュ内の URL の有効期限が切れるまで待機します。次回ユーザーが URL にアクセスするときに、新しい分類の更新がキャッシュに配置されます。
- 以下のコマンドを実行して、キャッシュの更新を強制的に行います。

```
request url-filtering update url <URL>
```

PAN-DB プライベート クラウド

PAN-DB プライベート クラウドは、クラウド サービスの使用を制限する組織向けのオンプレミス ソリューションです。このオンプレミス ソリューションを使用すると、ネットワークまたはデータセンター内に 1 台以上の M-600 アプライアンスを PAN-DB サーバーとして展開できます。ファイアウォールはURL 検索を実行するときに PAN-DB パブリック クラウドにアクセスせず、PAN-DB プライベート クラウドにクエリを発行します。

ネットワーク上のファイアウォールが URL 検索を実行するプロセスは、プライベート クラウドでもパブリック クラウドでも同じです。デフォルトでは、ファイアウォールは PAN-DB パブリック クラウドにアクセスするように設定されています。PAN-DB プライベート クラウドをデプロイする場合は、プライベート クラウドのサーバーにアクセスするための IP アドレスまたは FQDN のリストを使用してファイアウォールを設定する必要があります。

PAN-OS 5.0 以降のバージョンを実行するファイアウォールは *PAN-DB* プライベート クラウドと通信できます。

を設定すると、PAN-DB プライベート クラウド 、M-600 アプライアンスを直接インターネット アクセスを持つように設定するか、完全にオフラインに保つことができます。M-600 アプライアンスが URL 検索を実行するにはデータベースとコンテンツ更新が必要になるため、アプライアンスにアクティブなインターネット接続がない場合は、ネットワーク上のサーバーに手動で更新をダウンロードし、SCP を使用して、これらの更新を PAN-DB プライベート クラウド内の各 M-600 アプライアンスにインポートする必要があります。またアプライアンスはシード データベースと、サービスを提供するファイアウォール用のその他の定期更新コンテンツ更新または重要なコンテンツ更新を入手できる状態でなければなりません。

PAN-DB プライベート クラウドに接続するファイアウォールを認証するため、アプライアンスにはデフォルトのサーバー証明書のセットがパッケージされており、ユーザーが別のサーバー証明書をインポートまたは使用してファイアウォールを認証することはできません。M-600 アプライアンスのホスト名を変更する場合、アプライアンスはファイアウォールを認証するための新しい証明書のセットを自動的に生成します。

- PAN-DB プライベート クラウド用の M-600 アプライアンス
- PAN-DB プライベート クラウドのセットアップ

PAN-DB プライベート クラウド用の M-600 アプライアンス

PAN-DB プライベート クラウドをデプロイするには、1 台以上の M-600 アプライアンスが必要です。M-600 アプライアンスは Panorama モードで出荷され、PAN-DB プライベート クラウドとしてデプロイするには、PAN-URL-DB モードで動作するようにセットアップする必要があります。PAN-URL-DB モードでは、このアプライアンスは PAN-DB パブリック クラウドを使用しない企業向けに URL 分類サービスを提供します。

PAN-DB プライベート クラウドとしてデプロイされた M-600 アプライアンスは、MGT（Eth0）と Eth1 の 2 つのポートを使用します。Eth2 は使用できません。管理ポートは、アプライアンスへの管理アクセスや、最新のコンテンツ更新を PAN-DB パブリック クラウドまたはネットワーク上のサーバーから入手するときに使用します。PAN-DB プライベート クラウドとネットワーク上のファイアウォール間の通信には、MGT ポートまたは Eth1 を使用できます。

M-200 アプライアンスは *PAN-DB* プライベート クラウドとしてデプロイできません。

PAN-URL-DB モードの M-600 アプライアンスには、以下の留意事項があります。

- Web インターフェイスを持たない場合は、コマンド ライン インターフェイス(CLI)のみをサポートします。
- Panorama による管理はできません。
- 高可用性ペアでのデプロイはできません。
- URL フィルタリング ライセンスは必要ありません。ファイアウォールが PAN-DB プライベート クラウドに接続してクエリするには、有効なPAN-DB URL Filtering ライセンスが必要です。
- 出荷時に、PAN-DB プライベート クラウドに接続するファイアウォールを認証するために使用するデフォルトのサーバー証明書のセットが付属します。ファイアウォールの認証に別のサーバー証明書をインポートまたは使用することができません。M-600 アプライアンスのホスト名を変更すると、アプライアンスは、サービス提供先のファイアウォールを認証するための新しい証明書のセットを自動的に生成します。
- Panorama モードへのリセットしかできません。アプライアンスを専用ログ・コレクターとしてデプロイする場合は、Panorama モードに切り替えてから、Log Collector モードに設定します。

表 **4 : PAN-DB** パブリック クラウドと **PAN-DB** プライベート クラウドの差異

差異	**PAN-DB** パブリック クラウド	**PAN-DB** プライベート クラウド
コンテンツ更新およびデータベース更新	コンテンツ（定期および重要）更新と完全なデータベース更新は、1 日の間に複数回公開されます。PAN-DB パブリック クラウドは、マルウェアおよびフィッシングの URL カテゴリを 5 分毎に更新します。ファイアウォールは、URL 検索のためにクラウド サーバーをクエリするたびに、重要な更新がないかチェックします。	コンテンツ更新と完全な URL データベース更新は、営業日に 1 日に 1 回提供されます。
URL 分類の要求	URL 分類の変更要求は、以下のオプションを使用して送信できます。 • Palo Alto Networks Test A Site Web サイト。 • ファイアウォールの [URL フィルタリング プロファイルのセットアップ] ページ。	URL 分類の変更要求は、Palo Alto Networks Test A Site Web サイトのみを使用して送信できます。

差異	PAN-DB パブリック クラウド	PAN-DB プライベート クラウド
	• ファイアウォールの URL フィルタリング ログ。	
未解決の **URL** クエリ	ファイアウォールが URL クエリを解決できない場合、要求はパブリック クラウドのサーバーに送信されます。	ファイアウォールがクエリを解決できない場合、要求は PAN-DB プライベート クラウドの M-600 アプライアンスに送信されます。URL の一致がない場合、PAN-DB プライベート クラウドはカテゴリ「未知」応答をファイアウォールに送信します。M-600 アプライアンスに PAN-DB パブリック クラウドへのアクセスを設定していない限り、要求がパブリック クラウドに送信されることはありません。 PAN-DB プライベート クラウドを構成する M-600 アプライアンスが完全にオフラインになるように設定されている場合、データや分析がパブリック クラウドに送信されることはありません。

PAN-DB プライベート クラウドのセットアップ

ネットワークまたはデータセンター内に 1 台以上の M-600 アプライアンスを PAN-DB プライベート クラウドとしてデプロイするためには、次のタスクを完了させる必要があります。

- PAN-DB プライベート クラウドの設定
- ファイアウォールに PAN-DB プライベート クラウドへのアクセスを設定します。
- PAN-DB プライベート クラウド上のカスタム証明書による認証の設定

PAN-DB プライベート クラウドの設定

STEP 1 | M-600 アプライアンスをラックマウントします。

手順は、M-600 ハードウェア リファレンス ガイドを参照してください。

STEP 2 | M-600 アプライアンスを登録します。

M-600 アプライアンスを登録する方法については、ファイアウォールの登録を参照してください。

STEP 3 | M-600アプライアンスの初期設定を実行します。

PAN-DB モードの *M-600* アプライアンスは、*MGT*（*Eth0*）と *Eth1* の *2* つのポートを使用します。*Eth2* は *PAN-DB* モードでは使用しません。管理ポートは、アプライアンスへの管理アクセスと、*PAN-DB* パブリック クラウドから最新のコンテンツ更新を取得するために使用します。アプライアンス（*PAN-DB* サーバー）とネットワーク上のファイアウォール間の通信には、*MGT* ポートまたは *Eth1* を使用できます。

1. 以下のいずれかの方法で M-600 アプライアンスに接続します。
   - コンピュータから M-600 アプライアンスのコンソール ポートにシリアル ケーブルを接続し、ターミナル エミュレーション ソフトウェア（9600-8-N-1）を使用して接続します。
   - コンピュータから M-600 アプライアンスの MGT ポートに RJ-45 イーサネット ケーブルを接続します。ブラウザで、https://192.168.1.1 に移動します。この URL にアクセスできるようにするには、コンピュータの IP アドレスを、192.168.1.0 ネットワークでのアドレス（192.168.1.2 など）に変更しなければならない場合があります。
2. ログインを促されたら、アプライアンスにログインします。デフォルトのユーザー名とパスワード（admin/admin）を使用してログインします。アプライアンスの初期化が開始されます。
3. IP アドレスなど、MGT インターフェイスのネットワーク アクセス設定を行います。

```
set deviceconfig system ip-address  <server-IP>
 netmask <netmask> default-gateway <gateway-IP> dns-setting
 servers primary <DNS-IP>
```

   ここで、*<server-IP>* はサーバーの管理インターフェイスに割り当てる IP アドレス、*<netmask>* はサブネット マスク、*<gateway-IP>* はネットワーク ゲートウェイの IP アドレス、*<DNS-IP>* はプライマリ DNS サーバーの IP アドレスです。
4. IP アドレスなど、Eth1 インターフェイスのネットワーク アクセス設定を行います。

```
set deviceconfig system eth1 ip-address  <server-IP>
 netmask <netmask> default-gateway <gateway-IP> dns-setting
 servers primary <DNS-IP>
```

   ここで、*<server-IP>* はサーバーのデータ インターフェイスに割り当てる IP アドレス、*<netmask>* はサブネット マスク、*<gateway-IP>* はネットワーク ゲートウェイの IP アドレス、*<DNS-IP>* は DNS サーバーの IP アドレスです。
5. 変更を PAN-DB サーバーに保存します。

   コミットする

STEP 4 | PAN-DB プライベート クラウド モードに切り替えます。

1. PAN-DB モードに切り替えるには、以下の CLI コマンドを使用します。

```
request system system-mode pan-url-db
```

> *Panorama* モードから *PAN-DB* モード（およびその逆）、Panorama モードからログ コレクタ モード（およびその逆）に切り替えることができます。*PAN-DB* モードからログ コレクタ モード（またはその逆）への直接の切り替えはサポートされていません。操作モードを切り替えると、データのリセットがトリガーされます。管理アクセス設定を除き、すべての既存の設定とログが再起動時に削除されます。

2. モードが変更されたことを確認するには、以下のコマンドを使用します。

```
show pan-url-cloud-status hostname:M-600 ip-address:1.2.3.4
 netmask:255.255.255.0 default-gateway:1.2.3.1 ipv6-address:
 unknown ipv6-link-local-address: fe80:00/64 ipv6-default-
gateway: mac-address:00:56:90:e7:f6:8e time:Mon Apr 27
 13:43:59 2015 uptime:10 days, 1:51:28 family: m model:M-600
 serial:0073010000xxx sw-version:7.0.0 app-version:492-2638
 app-release-date:2015/03/19 20:05:33 av-version:0 av-release-
date: unknown wf-private-version:0 wf-private-release-date:
 unknown logdb-version:7.0.9 platform-family: m pan-url-
db:20150417-220 system-mode:Pan-URL-DB operational-mode:
 normal
```

3. アプライアンス上のクラウド データベースのバージョンを確認するには、以下のコマンドを使用します。

```
show pan-url-cloud-status Cloud status:Up URL database
 version:20150417-220
```

STEP 5 | コンテンツおよびデータベース更新をインストールします。

アプライアンスには、コンテンツの現在実行中のバージョンと *1* つ前のバージョンのみが保存されます。

以下のコンテンツ更新とデータベース更新のインストール方法からいずれかを選択します。

- PAN-DB サーバーがインターネットに直接アクセスできる場合は、以下のコマンドを使用します。
  1. 新しいバージョンが公開されているかどうかを確認するには、以下のコマンドを使用します。

     request pan-url-db upgrade check
  2. サーバーに現在インストールされているバージョンを確認するには、以下のコマンドを使用します。

     request pan-url-db upgrade info
  3. 最新のバージョンをダウンロードしてインストールするには、以下のコマンドを使用します。
     - **request pan-url-db upgrade download latest**
     - **request pan-url-db upgrade install** *<version latest | file>*
  4. M-600 アプライアンスが自動的に更新を確認するようにスケジュールするには、以下のコマンドを使用します。

     ```
     set deviceconfig system update-schedule pan-url-db recurring
      weekly action download-and-install day-of-week  <day of week>
      at <hr:min>
     ```
- PAN-DB サーバーがオフラインの場合は、Palo Alto Networksカスタマーサポート ウェブサイトにアクセスして、コンテンツ更新をダウンロードし、ネットワークの SCP サーバーに保存します。その後で、以下のコマンドを使用して更新をインポートおよびインストールできます。
  - **scp import pan-url-db remote-port** *<port-number>* from username@host:path
  - **request pan-url-db upgrade install file** *<filename>*

STEP 6 | PAN-DB プライベート クラウドへの管理アクセスをセットアップします。

アプライアンスにはデフォルトの ***admin*** アカウントがあります。追加の管理ユーザーを作成して、フル アクセス権または読み取り専用アクセス権を持つスーパーユーザーにすることができます。

PAN-DB プライベート クラウドは、RADIUS VSA の使用をサポートしていません。VSA がファイアウォールまたは Panorama で PAN-DB プライベート クラウドへのアクセスを有効にするために使用されると、認証エラーが発生します。

- PAN-DB サーバー上にローカル管理ユーザーをセットアップするには、以下のコマンドを実行します。
  1. **configure**
  2. ```
     set mgt-config users  <username> permissions role-based
      <superreader | superuser> yes
     ```
  3. ```
     set mgt-config users <username> password
     ```
  4. **Enter password:xxxxx**
  5. **Confirm password:xxxxx**
  6. **commit**
- RADIUS 認証を使用して管理ユーザーをセットアップするには、以下の手順を実行します。
  1. RADIUS サーバー プロファイルを作成します。

     ```
     set shared server-profile radius  <server_profile_name>
      server <server_name> ip-address <ip_address> port <port_no>
      secret <shared_password>
     ```
  2. 認証プロファイルを作成します。

     ```
     set shared authentication-profile  <auth_profile_name> user-
     domain <domain_name_for_authentication> allow-list <all> method
      radius server-profile <server_profile_name>
     ```
  3. 認証プロファイルをユーザーに適用します。

     ```
     set mgt-config users  <username> authentication-
     profile <auth_profile_name>
     ```
  4. 変更を [コミット] します。

     コミットする
- ユーザーのリストを表示するには、以下のコマンドを実行します。

```
show mgt-config users users { admin { phash fnRL/G5lXVMug;
 permissions { role-based { superuser yes; } } } admin_user_2
```

```
{ permissions { role-based { superreader yes; } }
authentication-profile RADIUS; } }
```

STEP 7 | PAN-DB プライベート クラウド にアクセスするようにファイアウォールを設定します。

ファイアウォールに PAN-DB プライベート クラウドへのアクセスを設定します。

PAN-DB パブリック クラウドを使用するとき、各ファイアウォールは AWS クラウドの PAN-DB サーバーにアクセスし、URL 検索のために接続可能な適格なサーバーのリストをダウンロードします。PAN-DB プライベート クラウドでは、URL 検索に使用する PAN-DB プライベート クラウド サーバーの（スタティック）リストを使用してファイアウォールを設定する必要があります。リストには最大 20 個のエントリを含めることができます。IPv4 アドレス、IPv6 アドレス、および FQDN がサポートされています。リストの各エントリ（IP アドレスまたは FQDN）は、PAN-DB サーバーの管理ポートまたは eth1 （またはその両方）に割り当てる必要があります。

STEP 1 | PAN-OS CLI から、URL ルックアップに使用される静的 PAN-DB プライベート クラウド サーバのリストを追加します。

- 次の CLI コマンドを使用して、PAN-DB サーバーのプライベート IP アドレスを追加します。

```
> configure
```

```
# set deviceconfig setting pan-url-db cloud-static-list <IP
 addresses>
```

あるいは、各ファイアウォールの Web インターフェイスで **Device (デバイス)** > **Setup (セットアップ)** > **Content-ID** を選択し、URL Filtering (URL フィルタリング) セクションを編集し、**PAN-DB Server (サーバー)** の IP アドレスあるいは FQDN を入力します。リストはカンマで区切る必要があります。

- プライベート PAN-DB サーバのエントリを削除するには、次のコマンドを使用します。

```
# delete deviceconfig setting pan-url-db cloud-static-list <IP
 addresses>
```

プライベート PAN-DB サーバーのリストを削除すると、ファイアウォール上で再選択プロセスがトリガーされます。ファイアウォールは最初に PAN-DB プライベート クラウド サーバーのリストがあるかチェックし、リストがない場合は、AWS クラウドの PAN-DB サーバーにアクセスして接続可能な適格なサーバーのリストをダウンロードします。

STEP 2 | **#** コミット を入力して、変更を保存します。

STEP 3 | 変更が有効になっていることを確認するには、ファイアウォールで以下の CLI コマンドを使用します。

```
> show url-cloud status Cloud status:Up URL database
 version:20150417-220
```

PAN-DB プライベート クラウド上のカスタム証明書による認証の設定

デフォルトでは、PAN-DB サーバーは管理アクセスおよびデバイス間通信に使用される SSL 接続を確立するための相互認証に事前定義済みの証明書を使用します。ただし、代わりにカスタム証明書を使用して認証を設定することもできます。カスタム証明書を使用すると、PAN-DB サーバーとファイアウォール間の相互認証を確実にするための信頼関係を確立することができます。PAN-DB プライベート クラウドの場合、ファイアウォールはクライアントとして動作し、PAN-DB サーバーは該当のサーバーとして動作します。

STEP 1 | PAN-DB サーバーとファイアウォールのキーペアと認証局（CA）証明書を取得します。

STEP 2 | CA 証明書をインポートして、ファイアウォールの証明書を検証します。

1. PAN-DB サーバー上で CLI にログインし、設定モードを開始します。

   ```
   admin@M-600> configure
   ```

2. TFTP または SCP を使用して CA 証明書をインポートします。

   ```
   admin@M-600# {tftp | scp} import certificate from <value>
    file <value> remote-port <1-65535> source-ip <ip/netmask>
    certificate-name <value> passphrase <value> format {pkcs12 |
    pem}
   ```

STEP 3 | TFTP または SCP を使用して、PAN-DB M-600 アプライアンスのサーバー証明書と秘密鍵を含むキーペアをインポートします。

```
admin@M-600# {tftp | scp} import keypair from <value> file <value>
 remote-port <1-65535> source-ip <ip/netmask> certificate-
name <value> passphrase <value> format {pkcs12 | pem}
```


STEP 4 | ルート CA および中間 CA が含まれる証明書プロファイルを設定します。この証明書プロファイルは、PAN-DB サーバーとファイアウォール間のデバイス認証を定義します。

1. PAN-DB サーバーの CLI で、設定モードを開始します。

```
admin@M-600> configure
```

2. 証明書プロファイルに名前を付けます。

```
admin@M-600# set shared certificate-profile <name>
```

3. （省略可能）ユーザー ドメインを設定します。

```
admin@M-600# set shared certificate-profile <name>
 domain <value>
```

4. CA を設定します。

   Default-ocsp-url と ***ocsp-verify-cert*** は任意のパラメータです。

admin@M-600# **set shared certificate-profile <*name*> CA <*name*>**

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [default-ocsp-url <value>]
```

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [ocsp-verify-cert <value>]
```

STEP 5 | PAN-DB M-600 アプライアンスの SSL/TLS プロファイルを設定します。このプロファイルは、PAN-DB およびクライアント デバイスが SSL/TLS サービスに使用する証明書およびプロトコルの範囲を定義します。

1. SSL/TLS プロファイルを識別します。

```
admin@M-600# set shared ssl-tls-service-profile <name>
```

2. 証明書を選択します。

```
admin@M-600# set shared ssl-tls-service-profile <name>
 certificate <value>
```

3. SSL/TLS 範囲を定義します。

PAN-OS 8.0 以降のリリースでは、*TLS 1.2* 以降の *TLS* バージョンのみがサポートされています。最大バージョンを ***TLS 1.2*** または ***max***（最大）に設定する必要があります。

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings min-version {tls1-0 | tls1-1 | tls1-2
```

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings max-version {tls1-0 | tls1-1 | tls1-2 | max
```

STEP 6 | PAN-DB 上の安全なサーバー通信を設定します。

1. SSL/TLS プロファイルを設定します。この SSL/TLS サービス プロファイルは、PAN-DB とファイアウォール間のすべての SSL 接続に適用されます。

```
admin@M-600# set deviceconfig setting management secure-conn-
server ssl-tls-service-profile <ssltls-profile>
```

2. 証明書プロファイルを設定します。

```
admin@M-600# set deviceconfig setting management secure-conn-
server certificate-profile <certificate-profile>
```

3. PAN-DB がファイアウォールとの接続を切断して再確立するまでに待機する必要のある切断待ち時間を分単位で設定します（範囲は 0～44,640）。

```
admin@M-600# set deviceconfig setting management secure-conn-
server disconnect-wait-time <0-44640
```

STEP 7 | CA 証明書をインポートして、PAN-DB M-600 アプライアンスの証明書を検証します。

1. ファイアウォール インターフェイスにログインします。
2. 証明書をインポートします。

STEP 8 | ファイアウォールのローカル証明書または SCEP 証明書を設定します。

1. ローカル証明書の場合、 ファイアウォールのキーペアのインポート。
2. 、ファイアウォールの SCEP 証明書、SCEP プロファイルを設定します。

STEP 9 | ファイアウォールの証明書プロファイルを設定します。これを各ファイアウォールで個別に設定することも、Panorama の設定をテンプレートの一部としてファイアウォールにプッシュすることもできます。

1. ファイアウォールの場合は **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificate Profile**（証明書プロファイル）を選択し、また、Panorama の場合は **Panorama** > **Certificate Management**（証明書の管理） > **Certificate Profile**（証明書プロファイル）を選択します。
2. 証明書プロファイルの設定を行います。

STEP 10 | 各ファイアウォールにカスタム証明書をデプロイします。Panorama から一元的に証明書をデプロイすることも、各ファイアウォールに手動で証明書を設定することもできます。

1. ファイアウォール インターフェイスにログインします。
2. ファイアウォールの場合は **Device**（デバイス） > **Setup**（セットアップ） > **Management**（管理）を、Panorama の場合は **Panorama** > **Setup**（セットアップ） > **Management**（管理）を選択し、セキュア通信を **Edit**（編集）します
3. **Certificate Type**（証明書タイプ）、**Certificate**（証明書）、および **Certificate Profile**（証明書プロファイル）をそれぞれのドロップダウンリストから選択します。
4. 通信のカスタマイズ設定内で、**PAN-DB Communication**（**PAN-DB** 通信）を選択します。
5. **OK** をクリックします。
6. 変更をコミットします。

変更をコミットした後、ファイアウォールは、 **Disconnect Wait Time**（切断待ち時間）の経過後まで PAN-DB サーバーとの現在のセッションを終了しません。次のステップでカスタム証明書の使用を強制すると、切断待機時間がカウントダウンを開始します。

STEP 11 | すべてのファイアウォールにカスタム証明書のデプロイ後に、カスタム証明書認証を適用します。

1. PAN-DB サーバー上で CLI にログインし、設定モードを開始します。

```
admin@M-600> configure
```

2. カスタム証明書の使用を適用します。

```
admin@M-600# set deviceconfig setting management secure-conn-
server disable-pre-defined-cert yes
```

この変更のコミット後は、切断待機時間のカウントダウンが開始します（PAN-DB の 設定で構成した場合）。待機時間が終了すると、PAN-DB とそのファイアウォールは、設定された証明書だけを使用して接続します。

STEP 12 | 新しいファイアウォールまたは Panorama を PAN-DB プライベート クラウドのでプロイに追加する場合は、2 つの選択肢があります。

- **Custom Certificate Only**（カスタム証明書のみ）を有効にしていない場合は、新しいファイアウォールを PAN-DB プライベート クラウドに追加し、上記のようにカスタム証明書をデプロイできます。
- PAN-DB プライベート クラウドで **Custom Certificate Only**（カスタム証明書のみ）を有効にした場合、カスタム証明書を PAN-DB プライベート クラウドに接続する前に、ファイアウォールにカスタム証明書をデプロイする必要があります。

SSL/TLS ハンドシェイク検査を有効にする

SSL / TLSハンドシェイク検査は、復号化のマークが付けられたSSL / TLSWebトラフィックの脅威検出のギャップを埋めます。有効にすると、ファイアウォールのコンテンツおよび脅威検出(CTD) エンジンは、SSL/TLS ハンドシェイク中に潜在的な脅威について HTTPS トラフィックを検査します。ファイアウォールはハンドシェイクのデータを使用してトラフィックを識別し、適用可能なセキュリティ ポリシー ルールを適用します。ハンドシェイクを調べると、ネットワークセキュリティが向上し、脅威を防ぎ、できるだけ早くWebトラフィックにセキュリティポリシーアクションを適用することで、URLフィルタリングソリューションを最適化します。

具体的には、ファイアウォールはクライアント Hello メッセージをスキャンして、要求された Web サイトのホスト名を含む SSL/TLS プロトコルの拡張である サーバー名表示 *(SNI)* フィールドを探します。ファイアウォールは、ホスト名から、トラフィックの URL カテゴリとサーバー宛先を取得できます。次に、URL カテゴリを、セキュリティ ポリシールールに一致する URL フィルタリング プロファイルに照らして評価し、どのアクションを強制するかを決定します。ファイアウォールが SNI フィールドの悪意のある Web サーバーなどの脅威を検出した場合、またはポリシーによって Web サイトがブロックされると指示された場合、ファイアウォールはハンドシェイクを終了し、Web セッションを直ちに終了します。脅威が検出されず、ポリシーごとにトラフィックが許可されている場合、クライアントとサーバーは SSL/TLS ハンドシェイクを完了し、セキュア接続を介してアプリケーション データを交換できます。

> *SSL / TLS*ハンドシェイク検査中に*firewall*によってブロックされたサイトについては、*URL Filtering*応答ページは表示されません。ブロックされたカテゴリからのトラフィックを検出した後、ファイアウォールは *HTTPS* 接続をリセットし、ハンドシェイクを終了し、応答ページによるユーザー通知を防ぎます。代わりに、ブラウザーは標準の接続エラー メッセージを表示します。

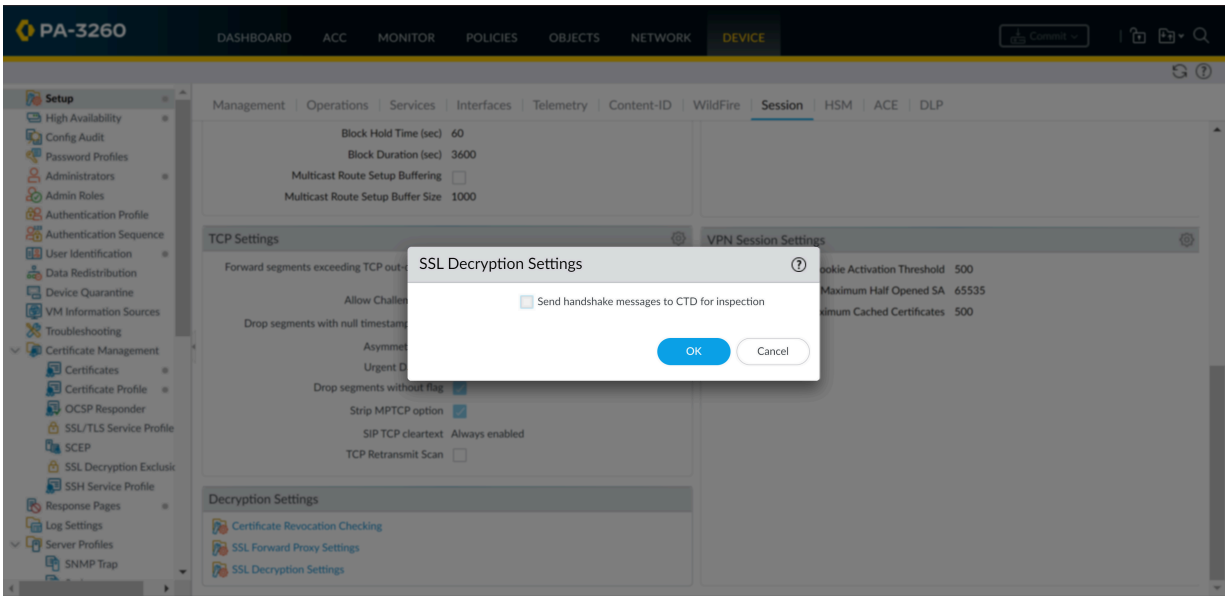
> 成功した *SSL/TLS* ハンドシェイクとセッションの詳細は、*Traffic* および *Decryption* ログに記載されています。*SSL/TLS* ハンドシェイク中にファイアウォールが *Web* セッションをブロックした場合、復号化ログは生成されません。ただし、失敗したセッションの詳細は、*URL Filtering* ログで確認できます。

SSL/TLS ハンドシェイクインスペクションを有効にするために必要な要件と手順を次に示します。

STEP 1 | デバイス>ライセンス を選択して、アクティブな Advanced URL Filtering ライセンスまたはレガシ URL Filtering ライセンスがあることを確認します。

STEP 2 | SSL フォワード プロキシ または SSL インバウンドインスペクション を介して SSL/TLS トラフィックを復号化することを確認します。

STEP 3 | CTD による SSL/TLS ハンドシェイクのインスペクションを有効にします。既定では、このオプションは無効になっています。



1. デバイス > **Setup** > セッション > 復号化設定 > **SSL** 復号化設定 を選択します。
2. [検査のために **CTD** にハンドシェイク メッセージを送信 を選択します。

   あるいは、**set deviceconfig setting ssl-decrypt scan-handshake *<yes|no>*** CLI コマンドを使用することもできます。
3. **OK** をクリックします。

STEP 4 | 設定の変更を **Commit** (コミット) します。

Quality of Service (QoS)

Quality of Service （QoS）とは、限りあるネットワーク容量で優先順位の高いアプリケーションおよびトラフィックを処理するときの信頼性を保証するため、ネットワーク上で機能する一式のテクノロジです。QoS テクノロジでは、ネットワーク トラフィックの特定のフローごとに異なる処理方法と容量を割り当てることによって、QoS を実現します。これによりネットワーク管理者は、トラフィックの処理順位およびトラフィックに振り分ける帯域幅を割り当てることができます。

Palo Alto Networks のアプリケーション Quality of Service （QoS）により、基本的な QoS をネットワークに適用し、それを拡張してアプリケーションとユーザーに QoS を適用することができます。

以下のトピックを読んで Palo Alto Networks のアプリケーション ベースの QoS について理解し、設定を行ってください。

- QoS の概要
- QoS の概念
- QoS の設定
- 仮想システムの QoS の設定
- DSCP 分類に基づく QoS の適用
- QoS のユース ケース

Palo Alto Networks の製品比較ツールを使用して、お使いのファイアウォール モデルでサポートされている QoS 機能を確認します。2 つ以上の製品モデルを選択して、**Compare Now (**今すぐ比較する**)** をクリックすると、各モデルでサポートされている QoS 機能が表示されます（たとえば、お使いのファイアウォール モデルでサブインターフェイスの QoS がサポートされているかどうか、サポートされている場合は、QoS を有効にできるサブインターフェイスの最大数をチェックできます）。

Aggregate Ethernet(AE)インターフェイスの QoS は、PA-7000 Series、PA-5400 Series、PA-5200 Series、PA-3400 Series、PA-3200 Series、および PA-400 Series firewall でサポートされています。

QoS の概要

QoS を使用し、ネットワーク トラフィックの品質に優先順位を設定して調整を図ります。パケットを処理する順序と帯域幅を割り当て、選択したトラフィック、アプリケーション、およびユーザーにとって望ましい処理方法と最適レベルのパフォーマンスが確保されるようにします。

QoS の実装に関係するサービス品質の測定量は、帯域幅（最大転送速度）、スループット（実転送速度）、遅延（待ち時間）、およびジッター（遅延の変動）です。これらのサービス品質測定量を形成および制御する QoS の能力は、VoIP （Voice over IP）、ビデオ会議、および遅延やジッターの影響を受けやすいビデオオンデマンドなど、高帯域幅のリアルタイム トラフィックの場合に特に重要です。また、QoS を使用して、以下を実現できます。

- ネットワークおよびアプリケーション トラフィックの優先順位を指定して、重要なトラフィックに高い優先順位が指定されるよう保証したり、重要度の低いトラフィックを制限したりします。
- 同じネットワーク内のさまざまなサブネット、クラス、またはユーザー間で、帯域幅を均等に共有します。
- 外部、内部、またはその両方で帯域幅を割り当て、アップロードとダウンロードの両方のトラフィックに QoS を適用するか、または一方のトラフィックにのみ適用します。
- 企業環境における顧客および収益に関係するトラフィックで低遅延が確保されるようにします。
- アプリケーションのトラフィック プロファイリングを実行して帯域幅の使用量を確保します。

Palo Alto Networks ファイアウォールで QoS を実装するには、完全な QoS ソリューションをサポートする 3 つの主要なコンポーネント、QoS プロファイル、QoS ポリシー、および QoS 出力インターフェイスの設定から始めます。QoS 設定タスクにおけるこれらの各オプションによって広範なプロセスを円滑に処理し、これによりトラフィック フローの最適化と優先順位付けを行い、設定可能なパラメータに応じた帯域幅を割り当てて確保します。

QoS トラフィック フローは、送信元から送信され、QoS が有効なファイアウォールによってシェーピングされ、最終的に優先順位付けされて宛先に配信されるトラフィック フローを示しています。

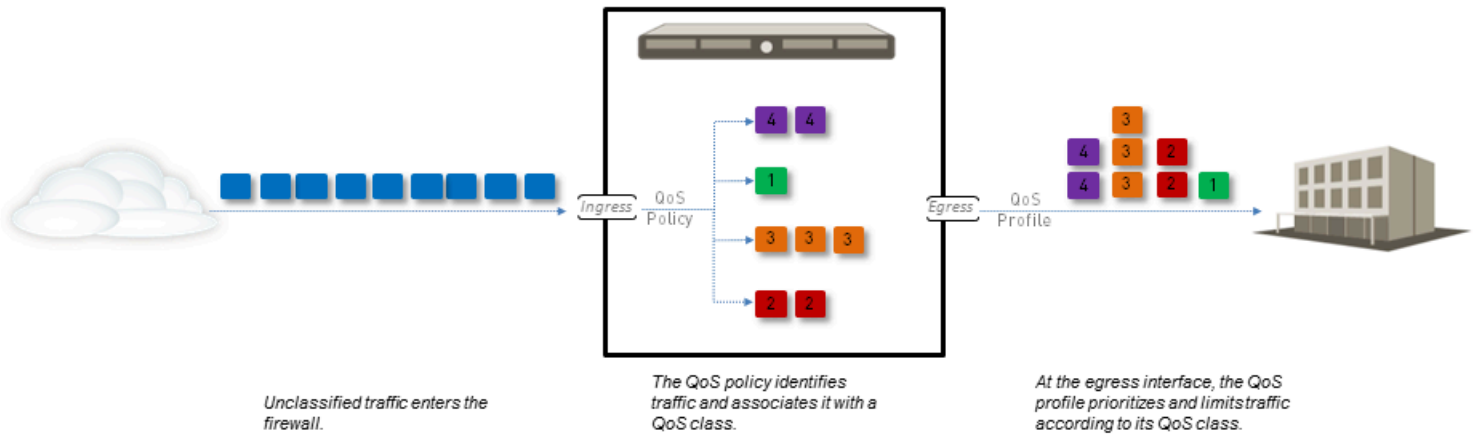


図 **6 : QoS** トラフィック フロー

QoS 設定オプションにより、トラフィック フローを制御し、フローのさまざまな位置で定義することができます。QoS トラフィック フローの図は、設定可能なオプションによってトラフィック フローを定義できる場所を示しています。QoS ポリシールールを使用すれば、QoS 処理を受けるトラフィックを定義したり、そのトラフィックをQoSクラスに割り当てたりすることができます。次に、マッチしたトラフィックは物理インターフェイスを出る際にQoSプロファイル クラス設定に基づいて形成されます。

お互いに影響を与えるコンポーネントがQoS 設定に含まれており、QoS 設定の各オプションは、全体的で詳細な QoS を実装するために使用するか、最小限の管理者アクションで限定的に使用することができます。

各ファイアウォール モデルは、QoS で設定可能な最大ポート数をサポートしています。お使いのファイアウォール モデルの仕様シートをご覧ください。または、製品比較ツールを使用すれば、2 つ以上のファイアウォールでサポートされている QoS 機能を単一ページで確認できます。

QoS の概念

以下のトピックを読み、Palo Alto Networks ファイアウォールにおける QoS 設定のさまざまなコンポーネントおよびメカニズムについて学習してください。

- アプリケーションおよびユーザーの QoS
- QoS ポリシー
- QoS プロファイル
- QoS クラス
- QoS優先キューイング
- QoS帯域幅管理
- QoS 出力インターフェイス
- クリア テキスト トラフィックおよびトンネル トラフィック用のQoS

アプリケーションおよびユーザーの QoS

Palo Alto Networks ファイアウォールには、ネットワークまたはサブネットに応じてファイアウォールから送出されるトラフィックを制御する基本的な QoS 機能があり、QoS の機能を拡張して、アプリケーションおよびユーザーに応じてトラフィックの分類とシェーピングも実行します。Palo Alto Networks ファイアウォールは、App-IDとUser-IDの機能を QoS 設定と統合することによってこの機能を実現します。ネットワーク内の特定のアプリケーションとユーザーを識別するための App-ID およびユーザー ID エントリは QoS 設定に含まれているため、帯域幅を管理かつ/または保証したいアプリケーションとユーザーを容易に指定することができます。

QoS ポリシー

QoS ポリシー ルールを使用して、QoS 処理（優先処理または帯域幅制限）を受けるトラフィックを定義し、そのトラフィックを QoS サービス クラスに割り当てます。

以下に基づいてトラフィックを照合する QoS ポリシー ルールを定義します。

- アプリケーションとアプリケーション グループ。
- 送信元ゾーン、送信元アドレス、および送信元ユーザー。
- 宛先ゾーンと宛先アドレス。
- 特定の TCP や UDP のポート番号に制限されるサービスまたはサービス グループ。
- カスタム URL カテゴリを含む URL カテゴリ。
- Differentiated Services Code Point （DSCP）値および Type of Service （ToS）値。これらの値は、トラフィックに求められるサービス レベル（高い優先順位、ベスト エフォート配信など）を示すために使用されます。

DSCP コード ポイントまたは *QoS* を *SSL* フォワード プロキシ、*SSL* インバウンド インスペクション、および *SSH* プロキシ トラフィックに適用することはできません。

各種のトラフィックをサービスのさまざまなQoS クラス に関連付ける場合は、複数の QoS ポリシー ルールをセットアップします（**Policies (ポリシー)** > **QoS**）。

ファイアウォールを通過するトラフィックに QoS が適用されるため、ファイアウォールがネットワークアドレス変換（NAT）ルールを含む他のすべてのセキュリティ ポリシー ルールを適用した後、QoS ポリシー ルールがトラフィックに適用されます。ソースに基づいてトラフィックに QoS 処理を適用する場合は、QoS ポリシー ルールでポスト NAT 送信元アドレスを指定していることを確認してください（NAT 前の送信元アドレスは使用しないでください）。

QoS プロファイル

QoS プロファイル ルールを使用し、その単一のプロファイル ルールに含まれる QoS クラスの値を最大 8 つまで定義します。

QoS プロファイル ルールを使用して、QoS クラス用の QoS 優先キューイングおよび QoS 帯域幅管理を定義できます。各QoSプロファイル ルールにより、最大8つのQoSクラスに対して個々の帯域幅および優先度を設定し、8つのクラス全体に割り当てる帯域幅の合計を指定することができます。単一のQoSプロファイル ルール（あるいは複数のQoSプロファイル ルール）を物理インターフェイスに付与し、定義済みの優先度および帯域幅設定をそのインターフェイスから出るトラフィックに適用します。

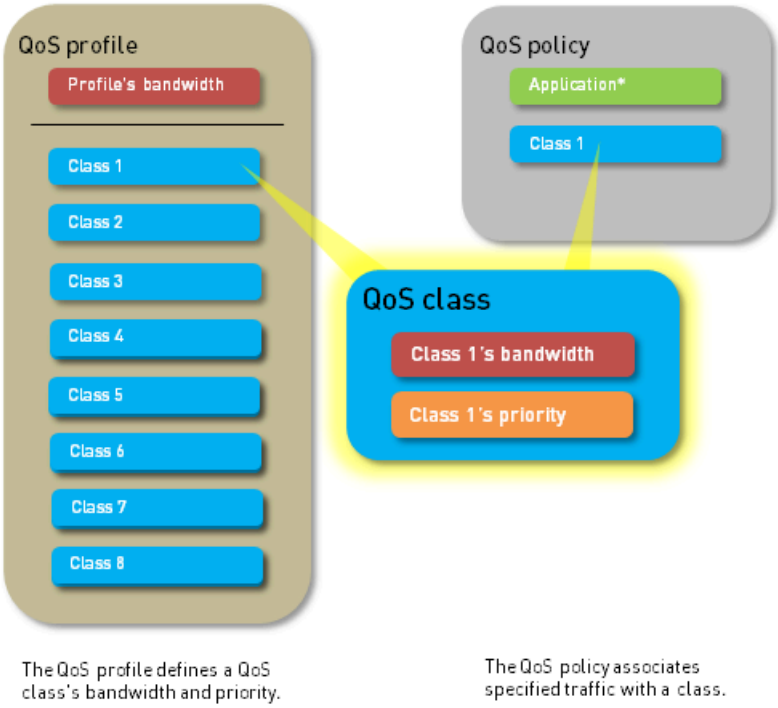
ファイアウォールでは、デフォルトのQoSプロファイル ルールを使用できます。プロファイルで定義されているデフォルトのプロファイル ルールおよびクラスには、最大帯域幅または保証帯域幅の制限が事前定義されていません。

QoS クラス用に優先順位および帯域幅設定を定義するには、QoS プロファイル ルールを追加のステップを参照してください。

QoS クラス

QoS クラスにより、QoS ポリシールールにマッチしたトラフィックの優先度と帯域幅が決まります。QoS プロファイル ルールを使用して QoS クラスを定義できます。単一の QoS プロファイルには、定義可能な QoS クラスが 8 つあります。特に設定しない限り、QoS クラスに一致しないトラフィックには class 4 が割り当てられます。

QoS プライオリティ キュー および QoS 帯域幅管理 は、QoS クラス定義内で設定されます(手順 4を参照)。各QoSクラスについて、マッチするトラフィックの優先度（リアルタイム、高、中、低）および最大帯域幅と保証された帯域幅を設定することができます。QoS優先キューイングおよび帯域幅管理により、トラフィックの順序と、ネットワークを出入りするときのトラフィックの処理方法が決まります。



QoS優先キューイング

QoS クラスでは、4 つの優先順位（real-time、high、medium、および low）のいずれかを適用できます。QoS ポリシールールにマッチしたトラフィックはそのルールに関連するQoSクラスが割り当てられ、ファイアウォールはそのマッチしたトラフィックをQoSクラスの優先順位に基づいて処理します。その後、アウトバウンドのトラフィック フローのパケットは、ネットワーク側でパケットを処理する準備ができるまで、それぞれの優先順位に従ってキューに格納されます。この優先キューイングにより、重要なトラフィック、アプリケーション、およびユーザーが確実に優先されるようにすることができます。リアルタイム優先順位は、通常、音声およびビデオアプリケーションなど、遅延の影響を受けやすいアプリケーションで使用されます。

QoS帯域幅管理

QoS帯域幅管理により、ネットワーク上のトラフィック フローを制御してトラフィックがネットワークの限界を超えないようにし（ネットワークの混雑につながる）、特定の種類のトラフィック、アプリケーション、ユーザーに帯域幅を割り当てることができます。QoSでは、トラフィック用の帯域幅を広げたり、狭めたりできます。QoSプロファイル ルールを使用すれば、個々のQoSクラス用の帯域幅や、8つすべてのQoSクラスの合計帯域幅を制限できます。QoS の設定 を行う作業の一環として、QoSプロファイル ルールを物理インターフェイスに付与し、そのインターフェイスを出るトラフィックに帯域幅設定を適用できます。そのQoSクラス（QoSクラスはQoS ポリシー ルールにマッチしたトラフィックに割り当てられます）にマッチしたトラフィックに個々のQoSクラス設定が適用され、そのプロファイルの合計帯域幅に関する制限をすべてのクリア テキスト トラフィック、ソース インターフェイスで発生した特定のクリア テキスト トラフィック、ソース サブネット、すべてのトンネル トラフィック、および個々のトンネル

インターフェイスに割り当てられます。複数のプロファイル ルールを単一のQoSインターフェイスに追加し、可変の帯域幅設定をそのインターフェイスを出るトラフィックに適用できます。

次のフィールドはQoS帯域幅設定をサポートしています。

- **Egress Guaranteed** [最低保証帯域 出力側]—マッチしたトラフィックに対して保証されている帯域幅の量。出力側の最大保証帯域を超過した場合、ファイアウォールはベストエフォート制でトラフィックを通過させます。保証されているが未使用の帯域幅は、すべてのトラフィックが利用できる状態のままになります。QoS 設定に応じて、単一のQoSクラス、すべてあるいは一部のクリア テキスト トラフィック、すべてあるいは一部のトンネル トラフィックに対して帯域幅を保証できます。

  例：

  Class 1トラフィックは出力側で5 Gbpsの最低帯域幅を保証されています。つまり、5 Gbpsを利用できますがそれはClass 1トラフィックのために確保されているわけではありません。Class 1トラフィックがその保証された帯域幅を使用しない、あるいは一部しか使用しない場合、他のトラフィックのクラスが残りの帯域幅を使用できます。しかし、トラフィックが多い時間帯では、Class 1トラフィックが5 Gbpsすべての帯域幅を使用できます。この混雑時、5 Gbpsを超えたClass 1トラフィックはベスト エフォート型として扱われます。

- **Egress Max** [最大保証帯域　出力側]—マッチしたトラフィックに対して割り当てられる帯域幅の合計。設定した最大保証帯域幅の限界を超えるトラフィックはファイアウォールによってドロップされます。QoS 設定に応じて、単一のQoSクラス、すべてあるいは一部のクリア テキスト トラフィック、すべてあるいは一部のトンネル トラフィック、およびQoSインターフェイスを出るすべてのトラフィックに対する最大帯域幅の制限を設定することができます。

  そのインターフェイスに付与された*QoS*プロファイル ルール用に保証された帯域幅の累積値が、そのインターフェイスに割り当てられている合計帯域幅を上回ってはなりません。

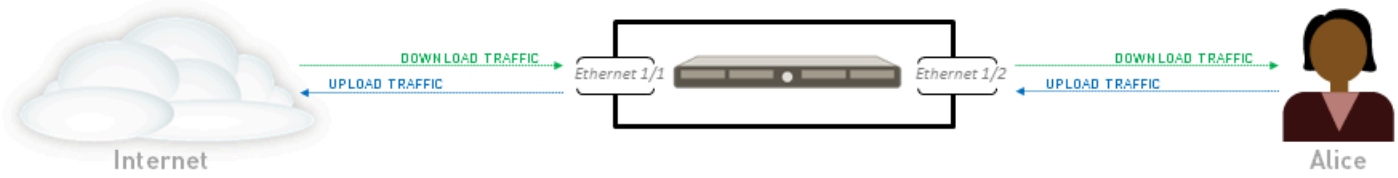
QoS クラス用に帯域幅設定を定義するには、QoS プロファイル ルールを追加のステップを参照してください。後でクリア テキスト トラフィックおよびトンネル トラフィックにこれらの帯域幅設定を適用する方法、QoS インターフェイス用に合計帯域幅の制限を設定する方法については、物理インターフェイスで QoS を有効化のステップを参照してください。

QoS 出力インターフェイス

QoS 処理対象として識別されたトラフィックの出力インターフェイスで QoS プロファイル ルールを有効にすれば、QoS 設定が完了します。QoS トラフィックの入力インターフェイスは、トラフィックがファイアウォールに入るときのインターフェイスです。QoS トラフィックの出力インターフェイスは、トラフィックがファイアウォールから出るときのインターフェイスです。QoS は常時有効で、トラフィック フローの出力インターフェイスで適用されます。QoS 設定の出力インターフェイスは、ファイアウォールの外向きまたは内向きのインターフェイスであり、QoS 処理の対象となるトラフィックのフローに応じて決まります。

たとえば、企業ネットワークで特定の Web サイトからの従業員のダウンロード トラフィックを制限する場合、QoS 設定での出力インターフェイスはファイアウォールの内部インターフェイスとなります。これは、インターネット側から出発してファイアウォールを通過し、企業ネットワークに送信されるトラフィック フローだからです。一方、同じ Web サイトに向かう従業員

のアップロード トラフィックを制限する場合、QoS 設定での出力インターフェイスはファイアウォールの外部インターフェイスです。これは、制限対象のトラフィックが、企業ネットワークから出発してファイアウォールを通過し、インターネット側に送信されるフローだからです。



- The egress interface for Alice's download traffic is Ethernet 1/2. To prioritize or limit her download traffic, Alice enables QoS on Ethernet 1/2.
- The egress interface for Alice's upload traffic is Ethernet 1/1. To prioritize or limit her upload traffic, Alice enables QoS on Ethernet 1/1.

ファイアウォールを通過するトラフィックに QoS が適用されるため、ファイアウォールがネットワークアドレス変換（NAT）ルールを含む他のすべてのセキュリティ ポリシー ルールを適用した後、QoS ポリシー ルールがトラフィックに適用されます。ソースに基づいてトラフィックに QoS 処理を適用する場合は、QoS ポリシー ルールでNAT後の送信元アドレスを指定する必要があります（NAT前の送信元アドレスは使用しないでください）。

QoS 処理を受信するアプリケーションの出口インターフェースを識別する方法の詳細をご覧ください。

クリア テキスト トラフィックおよびトンネル トラフィック用のQoS

QoS インターフェイスを有効にする場合は、最低でも、インターフェイスから送出されるクリア テキスト トラフィックの優先度および帯域幅を定義するQoS プロファイルを選択する必要があります。ただし、QoS インターフェイスをセットアップまたは変更するときに、発信されるクリア テキスト トラフィックおよびトンネル対象トラフィックに詳細な QoS 設定を適用することができます。QoS の優先処理および帯域幅制限は、トンネル トラフィック、個別のトンネル インターフェイスや、さまざまな送信元インターフェイスおよび送信元サブネットから発信されるクリア テキスト トラフィックに適用できます。Palo Alto Networks ファイアウォールで「トンネル対象トラフィック」とは、トンネル インターフェイスのトラフィックで、特にトンネル モードの IPSec トラフィックのことをいいます。

QoS の設定

以下の手順に従って、Quality of Service （QoS）を設定します。この手順には、QoS プロファイルの作成、QoS ポリシーの作成、インターフェイスでの QoS の有効化を伴います。

STEP 1 | QoSで管理するトラフィックを決定します。

この例では、QoS を使用して Web 閲覧を制限する方法を示します。

ACC を選択して **Application Command Center**（アプリケーション コマンド センター）ページを表示します。**ACC** ページの設定項目およびグラフを使用して、アプリケーション、URL フィルタリング、脅威防御、データ フィルタリング、および HIP マッチに関連した傾向およびトラフィックを表示します。

任意のアプリケーション名をクリックして、詳細なアプリケーション情報を表示します。

STEP 2 | QoS を受け取りたいアプリケーションの出力インターフェイスを特定します。

トラフィックの出力インターフェイスは、トラフィック フローによって決まります。受信トラフィックをシェーピングする場合、出力インターフェイスは内向きインターフェイスです。送信トラフィックをシェーピングする場合、出力インターフェイスは外向きインターフェイスです。

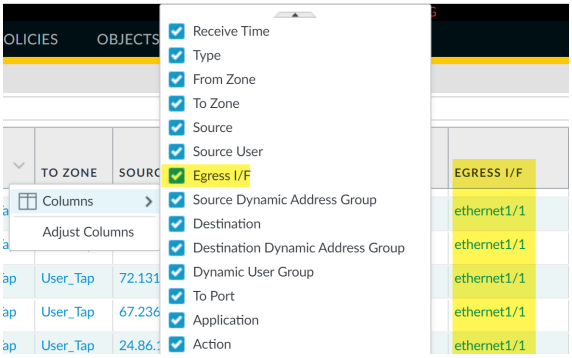
Traffic (トラフィック) ログを表示するには、**Monitor (監視)** > **Logs (ログ)** > **Traffic (トラフィック)** を選択します。

フィルタリングして特定のアプリケーションのログのみを表示するには、以下の手順を実行します。

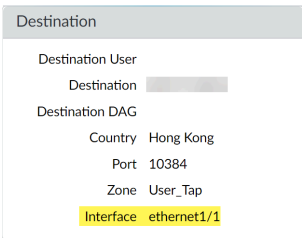
- アプリケーションのエントリが表示された場合は、Application （アプリケーション）列の下線の付いたリンクをクリックし、Submit （サブミット）アイコンをクリックします。
- アプリケーションのエントリが表示されない場合は、ログの追加アイコンをクリックして、アプリケーションを検索します。

トラフィック ログの **[出力インターフェイス]** には、各アプリケーションの出力インターフェイスが表示されます。デフォルトで表示されていない場合に **Egress I/F**（出力 **I/F**） 列を表示するには、以下の手順を実行します。

- 任意の列ヘッダーをクリックして、ログに列を追加します。



- 任意のエントリの左側にある拡大鏡アイコンをクリックして、詳細ログを表示します。Destination （宛先）セクションのリストにアプリケーションの出力インターフェイスが表示されます。



STEP 3 | QoS ポリシー ルールを追加します。

QoS ポリシールールはQoS処理の対象となるトラフィックを定義します。ファイアウォールはサービスのQoSクラスをポリシールールにマッチしたトラフィックに割り当てます。

ファイアウォールを通過するトラフィックに *QoS* が適用されるため、ファイアウォールがネットワークアドレス変換（*NAT*）ルールを含む他のすべてのセキュリティ ポリシー ルールを適用した後、*QoS* ポリシー ルールがトラフィックに適用されます。ソースに基づいてトラフィックに *QoS* 処理を適用する場合は、*QoS* ポリシー ルールで*NAT*後の送信元アドレスを指定する必要があります（*NAT*前の送信元アドレスは使用しないでください）。

1. **Policies (ポリシー)** > **QoS** を選択して新しいポリシールールを **Add (追加)** します。
2. **General**（全般） タブで、QoS ポリシー ルールに分かりやすい **Name**（名前） を付けます。
3. **Source (送信元)**、**Destination (宛先)**、**Application (アプリケーション)**、**Service/URL Category (サービス/URL カテゴリ)**、および **DSCP/ToS** の値に基づき QoS 処理を受けるトラフィックを指定します（**DSCP/ToS** 設定によりDSCP 分類に基づく QoS の適用を行えます）。

   たとえば、**Application** [アプリケーション]を選択して**Add** [追加]をクリックし、web-browsingを選択してQoSをWebブラウジング トラフィックに割り当てます。
4. （任意）追加のパラメータを定義します。例えば **Source (送信元)** を選択し、特定のユーザーの Web トラフィック用の QoS を提供する **Source User (送信元ユーザー)** を **Add (追加)** します。
5. **Other Settings (その他の設定)** を選択し、ポリシールールにマッチしたトラフィックに **QoS Class (QoS** クラス) を割り当てます。たとえば、user1 の Webトラフィックトラフィックを class 2 に割り当てます。
6. **OK** をクリックします。

STEP 4 | QoS プロファイル ルールを追加します。

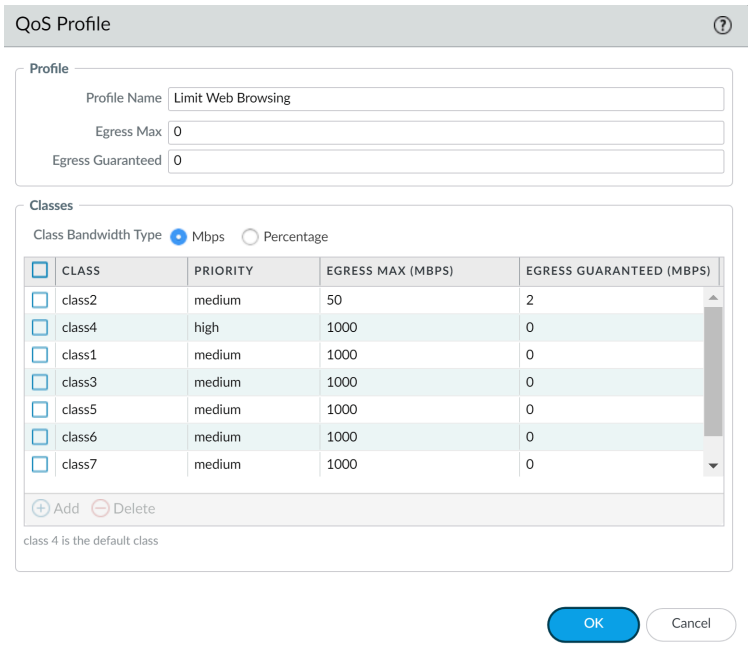
QoS プロファイル ルールにより、トラフィックが受けられる 8 つのサービス クラス（優先度を含む）を定義でき、QoS 帯域幅管理を行えます。

QoS プロファイル名をクリックすることにより、デフォルトを含む任意の既存 QoS プロファイルを編集できます。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **QoS Profile (QoS プロファイル)** を選択して新しいプロファイルを **Add (追加)** します。
2. 分かりやすい **[プロファイル名]** を入力します。
3. そのQoSプロファイル ルール用の合計帯域幅の制限を設定します。
   - **Egress Max**[最大保証帯域 出力側] の値を入力して、QoS プロファイル ルールの全体的な帯域幅割り当てを設定します。
   - **Egress Guaranteed (最低保証帯域 出力側)** の値を入力して、QoS プロファイルの保証帯域幅を設定します。

   *Egress Guaranteed [最低保証帯域 出力側]*の値を超えるトラフィックは、ベスト エフォートで、保証されません。保証されているが未使用の帯域幅は、すべてのトラフィックが利用できる状態のままになります。
4. Classes （クラス）セクションで、最大で 8 つの個々の QoS クラスの処理方法を指定します。
   1. クラスを QoS プロファイルに**Add**（追加）します。
   2. クラスの **Priority (優先順位)** を選択します（リアルタイム、高、中、低）。
   3. 各QoSクラスに割り当てられたトラフィックの **Egress Max (最大保証帯域 出力側)** および **Egress Guaranteed (最低保証帯域 出力側)** を入力します。
5. **OK** をクリックします。

以下の例では、Limit Web Browsing という名前の QoS プロファイル ルールが、class 2 トラフィックの最大帯域幅を 50 Mbps に、保証帯域幅を 2 Mbps に制限しています。



STEP 5 | 物理インターフェイスで QoS を有効にします。

このステップの一部には、特殊なQoS処理用にクリア テキスト トラフィックおよびトンネル トラフィックを選択するオプションが含まれます。

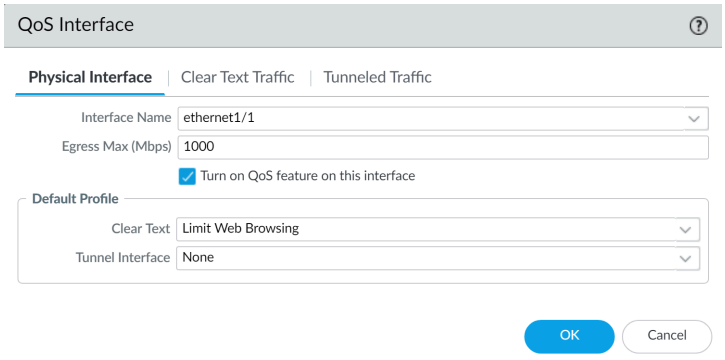
製品仕様のサマリーを参照して、ご使用のファイアウォール モデルがサブインターフェイスの *QoS* の有効化をサポートしているかどうか確認してください。

1. **Network (ネットワーク)** > **QoS** を選択して QoS インターフェイスを **Add (追加)** します。
2. **Physical Interface (物理インターフェイス)** を選択し、QoS を有効にするインターフェイスの **Interface Name (インターフェイス名)** を選択します。

   この例の場合、web-browsing トラフィックの出力インターフェイスは ethernet 1/1 です（ステップ 2 を参照）。
3. このインターフェイスを出るすべてのトラフィック用の**Egress Max** [最大保証帯域 出力側]を設定します。

   QoS インターフェイスの *Egress Max*（最大保証帯域 出力側）値は、常に定義しておくことをお勧めします。必ず、そのインターフェイスに付与された*QoS*プロファイル ルール用に保証された帯域幅の累積値が、そのインターフェイスに割り当てられている合計帯域幅を上回わらないようにしてください。
4. **[このインターフェイスの QoS 機能をオンにする]** を選択します。
5. Default Profile (デフォルト プロファイル) セクションで、物理インターフェイスを出るすべての**Clear Text (クリア テキスト)** トラフィックに割り当てるQoSプロファイル ルールを選択します。
6. （任意）インターフェイスを出るすべてのトンネル トラフィックに割り当てるデフォルトのQoSプロファイル ルールを選択します。

例えば、ethernet 1/1でQoSを有効化し、QoSプロファイル ルール「Limit Web Browsing (ステップ 4)」用に定義した帯域幅および優先度設定を適用し、出力側のクリア テキスト トラフィック用のデフォルト設定として使用します。



1. （任意）より詳細な設定を定義し、クリア テキスト トラフィックおよびトンネル トラフィック用の QoS を提供します。**Clear Text Traffic** [クリア テキスト トラフィック]タブおよび**Tunneled Traffic** [トンネル トラフィック]タブで行った設定は自動的にPhysical

Interface [物理インターフェイス]タブのクリア テキスト トラフィックおよびトンネル トラフィックの設定をオーバーライドします。

- **Clear Text Traffic** [クリア テキスト トラフィック]を選択し：
  - クリアテキスト トラフィックの **Egress Guaranteed**（最低保証帯域 出力側） および **Egress Max**（最大保証帯域 出力側） の帯域幅を設定します。
  - **Add** [追加] をクリックしてQoSプロファイル ルールを適用し、送信元インターフェイスおよび送信元サブネットに基づいてクリア テキスト トラフィックを強制します。

    *(PA-3200 Series, PA-5200 Series, PA-5400 Series, PA-7000 Series のみ)*また、特定のサブインターフェイスにルールが適用される場合は、*QoS* ポリシー ルールを設定するときに宛先インターフェイスを選択する必要があります。
- **Tunneled Traffic (**トンネル トラフィック**)** を選択し：
  - トンネル対象トラフィックの **Egress Guaranteed**（最低保証帯域 出力側） および **Egress Max**（最大保証帯域 出力側） の帯域幅を設定します。
  - **Add** [追加] をクリックして、QoS プロファイル ルールを 1 つのトンネル インターフェイスに関連付けます。

2. **OK** をクリックします。

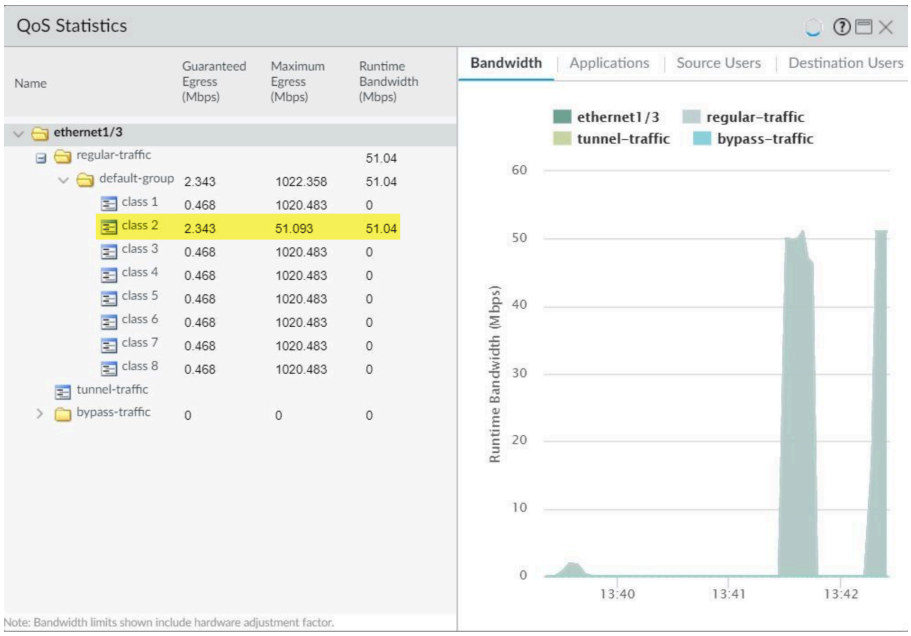
STEP 6 | 変更をコミットします。

Commit（コミット）をクリックします。

STEP 7 | QoS 設定を確認します。

Network (ネットワーク) > **QoS**、**Statistics (統計)** の順に選択して、QoS 帯域幅、選択した QoS クラスのアクティブなセッション、および選択した QoS クラスのアクティブなアプリケーションを表示します。

たとえば、QoS が有効化されたイーサネット 1/3 の統計を表示します。



クラス 2のトラフィックの保証帯域幅は 2.343 Mbps に、最大帯域幅は 51.093 Mbps に制限されています。

続けて該当するタブをクリックし、アプリケーション、送信元ユーザー、宛先ユーザー、セキュリティ ルール、および QoS ルールに関する詳細を表示します。

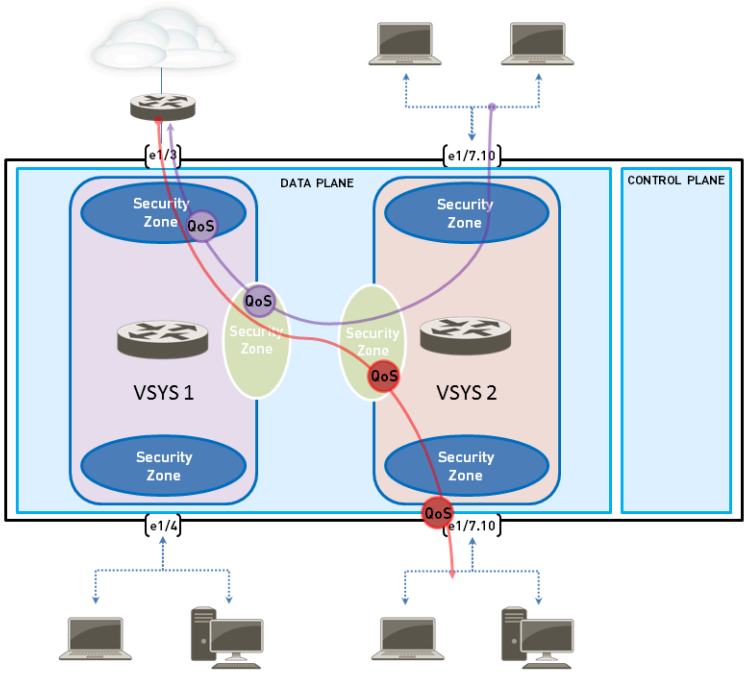
***[QoS** 統計情報]* ウィンドウに表示される帯域幅制限には、ハードウェアの調整ファクタが含まれます。

仮想システムの QoS の設定

QoS は、Palo Alto Networks ファイアウォールの 1 つの仮想システムにも、複数の仮想システムにも設定できます。仮想システムは独立したファイアウォールであるため、1 つの仮想システムに QoS を個別に設定する必要があります。

仮想システムに QoS を設定する方法は、物理ファイアウォールに QoS を設定する方法と似ています。異なる点は、仮想システムに QoS を設定する場合は、トラフィックの送信元と宛先を指定する必要があることです。仮想システムは物理的境界を設定されることなく存在するため、そして、仮想環境ではトラフィックが複数の仮想システムにまたがるため、1 つの仮想のトラフィックを制御およびシェーピングするためには、トラフィックの送信元ゾーンと宛先ゾーンおよびインターフェイスを指定する必要があります。

以下の例は、ファイアウォールに設定された 2 つの仮想システムを示しています。VSYS （紫）および VSYS （赤）のそれぞれに、2 つの明確なトラフィック フローの優先順位を設定するか制限する目的で QoS が設定されており、それぞれの対応する紫（VSYS 1）および赤（VSYS 2）の線で表示されています。QoS ノードは、トラフィックが QoS ポリシーに適合し、QoS サービス クラスに割り当てられる時点を示し、その後トラフィックがファイアウォールから送出されるときにシェーピングされる時点を示します。



仮想システムとその設定方法は仮想システムを参照してください。

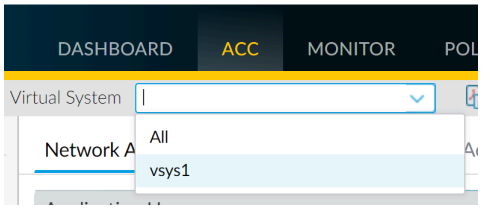
STEP 1 | 各仮想システムに、適切なインターフェイス、仮想ルーター、およびセキュリティ ゾーンが関連付けられていることを確認します。

- 設定されているインターフェイスを表示するには、**Network (ネットワーク)** > **Interface (インターフェイス)** の順に選択します。
- 設定されているゾーンを表示するには、**Network (ネットワーク)** > **Zones (ゾーン)** の順に選択します。
- 定義されている仮想ルーターの情報を表示するには、**Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択します。

STEP 2 | QoS を適用するトラフィックを指定します。

ACC を選択して **Application Command Center**（アプリケーション コマンド センター）ページを表示します。**ACC** ページの設定項目およびグラフを使用して、アプリケーション、URL フィルタリング、脅威防御、データ フィルタリング、および HIP マッチに関連した傾向およびトラフィックを表示します。

特定の仮想システムの情報を表示するには、**[仮想システム]** ドロップダウンから仮想システムを選択します。



任意のアプリケーション名をクリックして、詳細なアプリケーション情報を表示します。

STEP 3 | QoS 処理が必要なアプリケーションの出力インターフェイスを特定します。

仮想システム環境では、仮想システム上のトラフィックの出力点で、トラフィックに QoS が適用されます。仮想システムの設定および QoS ポリシーに応じて、QoS トラフィックの出力点が、物理インターフェイスに関連付けられていることや、ゾーンであることがあります。

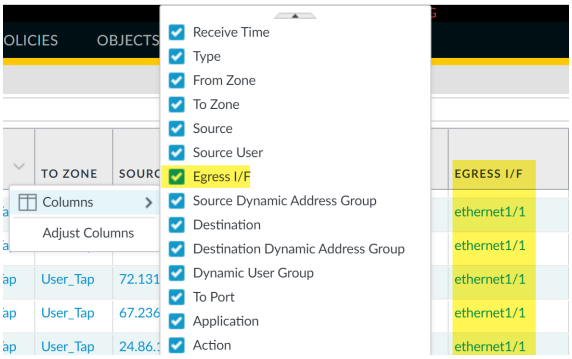
この例は、vsys 1 での web-browsing トラフィックの制限方法を示しています。

トラフィックログを表示するには、**Monitor (監視)** > **Logs (ログ)** > **Traffic (トラフィック)** を選択します。各エントリには、仮想システム環境で QoS を設定するために必要な情報を含む列を表示するオプションがあります。

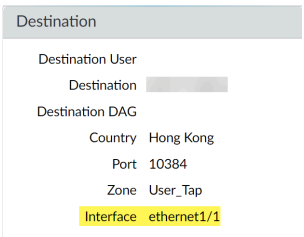
- 仮想システム(vsys)
- 出口インターフェイス
- 入口インターフェイス
- 送信元ゾーン
- 宛先ゾーン

デフォルトで表示されていない場合にその列を表示するには、以下の手順を実行します。

- 任意の列ヘッダーをクリックして、ログに列を追加します。



- 任意のエントリの左側にある拡大鏡アイコンをクリックしてアプリケーションの出力インターフェイスを含む詳細ログを表示します。同時に **[送信元]** と **[宛先]** のセクションには、送信元ゾーンと宛先ゾーンが表示されます。



たとえば、VSYS 1 からの web-browsing トラフィックの場合は、入力インターフェイスが ethernet 1/2、出力インターフェイスが ethernet 1/1、送信元ゾーンが trust、および宛先ゾーンが untrust です。

STEP 4 | QoS プロファイルを作成します。

プロファイル名をクリックすることにより、デフォルトを含む任意の既存 QoS プロファイルを編集できます。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **QoS Profile** の順に選択し、**Add (追加)** をクリックして QoS Profile (QoS プロファイル) ダイアログを開きます。
2. 分かりやすい **[プロファイル名]** を入力します。
3. **[最大保証帯域 出力側]** を入力して、QoS プロファイルの全体的な帯域幅割り当てを設定します。
4. **Egress Guaranteed (最低保証帯域 出力側)** を入力して、QoS プロファイルの保証帯域幅を設定します。

   QoS プロファイルの出力保証制限を超えるトラフィックは、ベスト エフォートであり、保証されません。
5. **[QoS プロファイル]** の [クラス] セクションで、最大で 8 つの個々の QoS クラスの処理方法を指定します。
   1. **Add**（追加） をクリックして、クラスを QoS プロファイルに追加します。
   2. クラスの **Priority**（優先順位）を選択します。
   3. クラスの **Egress Max** （最大保証帯域 出力側）を入力して、その個別のクラス全体の帯域幅制限を設定します。
   4. クラスの **Egress Guaranteed**（最低保証帯域 出力側） を入力して、個々のクラスの保証帯域幅を設定します。
6. **[OK]** をクリックして QoS プロファイルを閉じます。

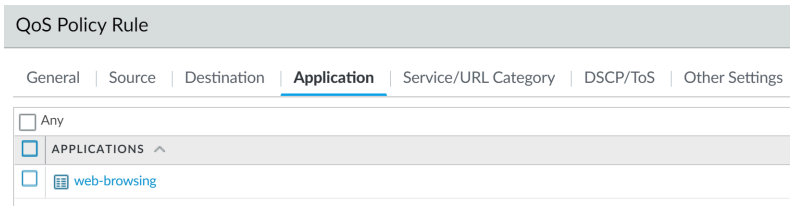
STEP 5 | QoS ポリシーを作成します。

仮想システムが複数ある環境では、トラフィックが複数の仮想システムにまたがります。このため、仮想システムの QoS を有効にするときに、送信元ゾーンと宛先ゾーンに基づいて QoS 処理を受けるトラフィックを定義する必要があります。この定義により、その仮想システムのトラフィックのみに優先順位が付けられ、シェーピングされます（このトラフィックが通過する可能性のある他の仮想システムのトラフィックは対象外です）。

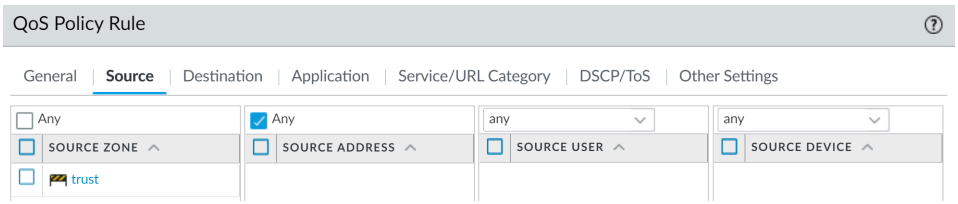
1. **Policies (ポリシー)** > **QoS**を選択して QoS ポリシー ルールを **Add (追加)** します。
2. **General** （全般） を選択して、QoS ポリシー ルールに分かりやすい **Name (名前)** を付けます。

3. QoS ポリシー ルールを適用するトラフィックを指定します。[送信元]、[宛先]、[アプリケーション]、および [サービス/**URL** カテゴリ] タブを使用して、トラフィックを識別するための照合パラメータを定義します。

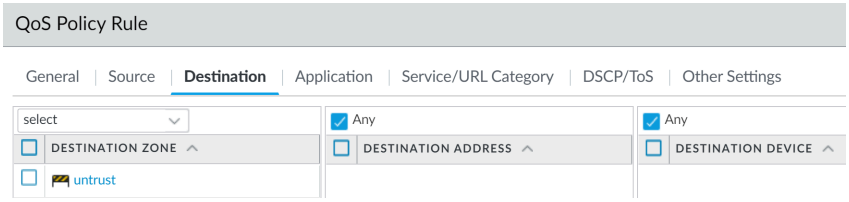
   たとえば、**Application** [アプリケーション]を選択して、web-browsing を **Add** [追加]し、QoS ポリシー ルールをそのアプリケーションに適用します。



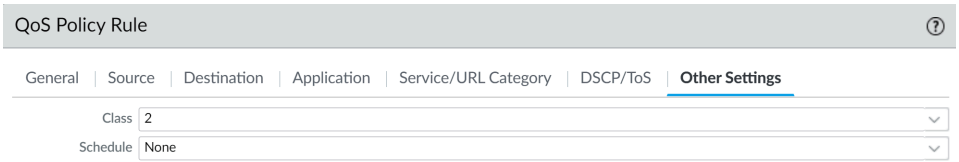
4. **Source (**送信元**)** を選択して、vsys 1 の web-browsing トラフィックの送信元ゾーンを **Add (**追加**)** します。



5. **Destination** [宛先]を選択して、vsys 1 の web-browsing トラフィックの宛先ゾーンを **Add** [追加]します。



6. **Other Settings** [その他の設定]を選択して、QoS ポリシー ルールに割り当てる **QoS Class** [QoS クラス]を選択します。たとえば、vsys 1 の web-browsing トラフィックにクラス 2 を割り当てます。



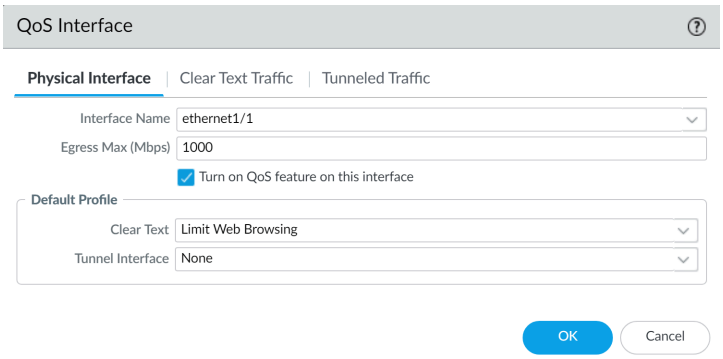
7. **OK** をクリックして QoS ポリシー ルールを保存します。

STEP 6 | 物理インターフェイスで QoS プロファイルを有効にします。

QoS インターフェイスの ***Egress Max***（最大保証帯域 出力側）値は、常に定義しておくことをお勧めします。

1. **Network (ネットワーク)** > **QoS** の順に選択し、**Add (追加)** をクリックして QoS Interface (QoS インターフェイス) ダイアログを開きます。
2. 物理インターフェイスで QoS を有効にします。
   1. **Physical Interface**（物理インターフェイス） タブで、QoS プロファイルを適用するインターフェイスの **Interface Name**（インターフェイス名） を選択します。

      この例の場合、vsys 1 での web-browsing トラフィックの出力インターフェイスは ethernet 1/1 です（ステップ 2 を参照）。

   2. **[このインターフェイスの QoS 機能をオンにする]** を選択します。
3. **[物理インターフェイス]** タブで、すべての **[クリア テキスト]** トラフィックに適用するデフォルトの QoS プロファイルを選択します。

   （任意）**Tunnel Interface**（トンネル インターフェイス） フィールドを使用して、デフォルトの QoS プロファイルをすべてのトンネル対象トラフィックに適用します。
4. （任意）**Clear Text Traffic**（クリア テキスト トラフィック） タブで、クリア テキスト トラフィックの追加の QoS 設定を行います。
   - クリアテキスト トラフィックの **Egress Guaranteed**（最低保証帯域 出力側） および **Egress Max**（最大保証帯域 出力側） の帯域幅を設定します。
   - **Add**[追加] をクリックして、選択したクリア テキスト トラフィックに QoS プロファイルを適用し、さらに、送信元インターフェイスと送信元サブネット（QoS ノードを作成）に従って QoS 処理を行うトラフィックを選択します。
5. （任意）**Tunneled Traffic**（トンネル対象トラフィック） タブで、トンネル インターフェイスの追加の QoS 設定を行います。
   - トンネル対象トラフィックの **Egress Guaranteed**（最低保証帯域 出力側） および **Egress Max**（最大保証帯域 出力側） の帯域幅を設定します。
   - **Add**[追加] をクリックし、選択したトンネル インターフェイスに QoS プロファイルを関連付けます。
6. **OK** をクリックして変更を保存します。

7. 変更を **Commit**（コミット）します。

STEP 7 | QoS 設定を確認します。

- **Network (**ネットワーク**)** > **QoS** の順に選択して、QoS Policies (QoS ポリシー) ページを表示します。**QoS Policies**（**QoS** ポリシー） ページで、QoS が有効になっており、**Statistics**（統計） リンクが含まれることを確認します。Statistics （統計）リンクをクリックして、QoS 帯域幅、選択した QoS ノードまたはクラスのアクティブなセッション、および選択した QoS ノードまたはクラスのアクティブなアプリケーションを表示します。
- マルチ VSYS 環境では、セッションが複数のシステムをまたぐことはできません。トラフィックが複数の仮想システムを通過する場合は、1 つのトラフィック フローについて複数のセッションが作成されます。ファイアウォール上で実行されているセッションを参照し、適用されている QoS ルールと QoS クラスを表示するには、**Monitor (**監視**)** > **Session Browser (**セッション ブラウザ**)** の順に選択します。

DSCP 分類に基づく QoS の適用

Differentiated Services Code Point （DSCP）とは、トラフィックの（例えば）高い優先順位、ベスト エフォート配信などを求めるのに使用できるパケット ヘッダー値です。セッションベースのDSCP分類を使用すると、インバウンド トラフィックのDSCP値を優先するとともに、セッション トラフィックがファイアウォールを出る際にDSCP値でセッションをマークすることができます。これにより、セッションのすべてのインバウンドおよびアウトバウンド トラフィックが、ネットワークを通過するときに、継続的に QoS/DSCP 処理を受けることができます。たとえば、外部サーバーからのインバウンド リターン トラフィックを、セッション開始時にファイアウォールが検知したDSCP値に基づいてファイアウォールが最初にアウトバウンド フローに適用したものと同じ QoS 優先順位で処理することができるようになりました。次に、ファイアウォールとエンド ユーザー間にあるネットワーク デバイスも、リターン トラフィック（およびそのセッションの他のアウトバウンドまたはインバウンド トラフィック）に同じ優先順位を適用します。

DSCP コード ポイントまたは *QoS* を *SSL* フォワード プロキシ、*SSL* インバウンド インスペクション、および *SSH* プロキシ トラフィックに適用することはできません。

DSCPマークの種類が異なれば、サービスのレベルが違うということが分かります。

この手順を完了すると、ファイアウォールが、セッションの開始時に検出されたものと同じ DSCP 値をトラフィックにマークできます（この例では、ファイアウォールがリターン トラフィックに DSCP の AF11 値をマークします）。QoS を設定すると、ファイアウォールから送出されるトラフィックをシェーピングできる一方で、セキュリティ ルールでこのオプションを有効にすると、他のネットワーク デバイスがファイアウォールとクライアントを仲介して、継続的に DSCP マークの付いたトラフィックに優先順位を適用できます。

- **Expedited Forwarding (EF)** [完全優先転送 (EF)]：トラフィックに低損失、低レイテンシの保証帯域幅を求める場合に使用します。コードポイント値が EF のパケットは、通常、優先順位が最も高く、保証された配信です。
- **Assured Forwarding (AF)** [相対的優先転送 (AF)]：アプリケーションに信頼できる配信を提供する場合に使用します。コードポイントが AF のパケットは、トラフィックにベスト エフォート サービスよりも高い優先順位の処理を求めることを示します（ただし、コードポイントが EF のパケットが引き続いて、コードポイントが AF のパケットよりも優先されます）。
- **Class Selector (CS)** [クラス セレクタ (CS)]：IP Precedence （IP 優先）フィールドを使用して優先トラフィックをマークするネットワーク デバイスに下位互換性をもたせる場合に使用します。
- **IP Precedence (ToS)** [IP 優先 (TOS)]：レガシー ネットワーク デバイスが優先トラフィックをマークするために使用します（DSCP 分類が導入されるまでは、パケットの優先順位を示すために IP Precedence （IP 優先）ヘッダー フィールドが使用されていました）。
- **Custom Codepoint** [カスタム コードポイント]：**Codepoint Name** [コードポイント名]と **Binary Value** [バイナリ値]を入力して、トラフィックと照合するカスタム コードポイントを作成します。

たとえば、**Assured Forwarding** （**AF**）[相対的優先転送（AF）]を選択して、コードポイント値が AF とマークされたトラフィックは、マークされた優先順位が低いアプリケーションよりも、信頼できる配信の優先順位が高いことを確認します。セッションベースの DSCP 分類を有効にするには、以下の手順を実行します。最初に、セッションの開始時に検出された DSCP マーキングに基づいて QoS を設定します。そうすると、ファイアウォールがセッションのリターン フローにも引き続き、最初のアウトバウンド フローへの QoS の適用に使用したものと同じ DSCP 値をマークできます。

STEP 1 | QoS の設定を行うための準備として各作業を行います。

STEP 2 | DSCP 値に基づいて QoS 処理を受けるトラフィックを定義します。

1. **Policies (ポリシー)** > **QoS** を選択し、既存の QoS ルールを **Add (追加)** あるいは変更し、各フィールドを自動入力します。
2. DSCP/ToSおよびコードポイントを選択します。
3. QoSを強制したいDSCP/ToSコードポイントを **Add (追加)** します。
4. トラフィックに照合する QoS ルールの DSCP/ToS マーキングの **Type** [タイプ]を選択します。

   ネットワーク トラフィックの管理および優先順位付けに *1* つの *DSCP* タイプを使用することをお勧めします。
5. **Codepoint (コードポイント)** の値を指定すると、トラフィックがより詳細に QoS ポリシーと照合されます。たとえば、照合するポリシーの DSCP 値の **Type (タイプ)** に相対的優先転送（AF）が選択されている場合、AF の **Codepoint (コードポイント)** の値を「AF11」のようにさらに指定します。

   DSCP マーキングの ***Type** [タイプ]*に完全優先転送（*EF*）が選択されている場合は、詳細な ***Codepoint** [コードポイント]*の値を指定することはできません。*QoS* ポリシールールは、*EF* コードポイント値がマークされているトラフィックを照合します。
6. **Other Settings** [その他の設定]を選択し、QoS ルールと照合するトラフィックに**QoS Class** [QoS クラス]を割り当てます。この例では、セッションの最初のパケットに AF11 という DSCP マーキングが検出されたセッションに Class 1 を割り当てます。
7. **OK** をクリックして、QoS ルールを保存します。

STEP 3 | セッションの開始時に検出された DSCP マーキングに基づいて QoS ルールに適合したトラフィックに設定する QoS の優先順位を定義します。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **QoS Profile (QoS プロファイル)** を選択して既存の QoS プロファイルを **Add (追加)** あるいは変更します。トラフィックの優先順位と帯域幅を設定するプロファイルのオプションの詳細は、「QoS の概念」および「QoS の設定」を参照してください。
2. プロファイル クラスを **Add (追加)** または変更します。たとえば、ステップ 2 では AF11 トラフィックをクラス 1 トラフィックとして分類する手順を示したため、**class1** エントリを追加または変更できます。
3. トラフィックのクラスの **Priority (優先順位)**（**high** など）を入力します。
4. **[OK]** をクリックして QoS プロファイルを閉じます。

STEP 4 | インターフェイスで QoS を有効にします。

Network (ネットワーク) > **QoS** を選択し、既存のインターフェイスを **Add (追加)** あるいは変更し、**Turn on QoS feature on this interface (**このインターフェイスの **QoS** 機能をオン**)** にします。

この例では、DSCP マーキングが AF11 であるトラフィックが QoS ルールに適合し、Class 1 に割り当てられています。インターフェイスで有効になっている QoS プロファイルが、ファイアウォールから送出される Class 1 トラフィック（セッションのアウトバウンド トラフィック）に、高い優先順位の処理を適用します。

STEP 5 | DSCP マーキングを有効にします。

リターン トラフィックに DSCP 値をマークして、セッションのインバウンド フローに、アウトバウンド フローで検出されたものと同じ DSCP 値がマークされるようにします。

1. **Policies (ポリシー)** > **Security (セキュリティ)** の順に選択し、セキュリティ ポリシーを **Add (追加)** または変更します。
2. **Actions (操作)** を選択し、**QoS Marking (QoS** マーキング**)** ドロップダウンで、**Follow-Client-to-Server-Flow (**クライアントからサーバーへのフローに従う**)** を選択します。
3. **OK** をクリックして変更内容を保存します。

この手順を完了すると、ファイアウォールが、セッションの開始時に検出されたものと同じ DSCP 値をトラフィックにマークできます（この例では、ファイアウォールがリターン トラフィックに DSCP の AF11 値をマークします）。QoS を設定すると、ファイアウォールから送出されるトラフィックをシェーピングできる一方で、セキュリティ ルールでこのオプションを有効にすると、他のネットワーク デバイスがファイアウォールとクライアントを仲介して、継続的に DSCP マークの付いたトラフィックに優先順位を適用できます。

STEP 6 | 設定を Commit（コミット）します。

変更を **Commit (コミット)**します。

QoS のユース ケース

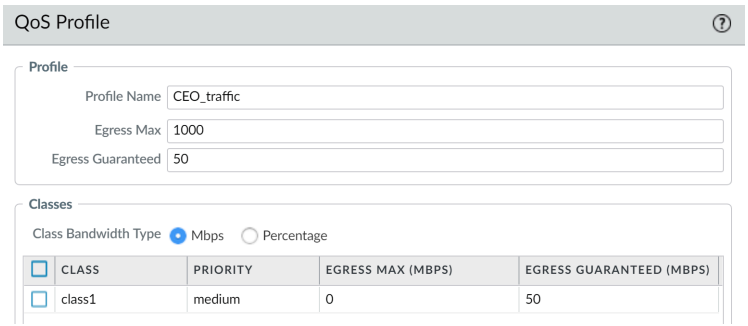
以下のユース ケースは、一般的なシナリオでの QoS の使用方法を示しています。

- 「ユース ケース：単一ユーザーの場合の QoS
- 「ユース ケース：音声およびビデオ アプリケーションの QoS

「ユース ケース：単一ユーザーの場合の QoS

ある企業の CEO が、ネットワーク使用量が多い時間帯になると、アプリケーションにアクセスできなくなり、重要な業務連絡に十分に応答できないことに気付きました。IT 管理者は、CEO が送受信するすべてのトラフィックが他の従業員のトラフィックよりも優先的に処理されるようにして、CEO が重要なネットワーク リソースにアクセスできることはもとより、アクセス時のパフォーマンスも十分に得られることを保証する必要があります。

STEP 1 | 管理者は、QoS プロファイル ***CEO_traffic*** を作成して、CEO が送信するトラフィックが企業ネットワークから出るときに、どのように処理され形成されるかを定義します。



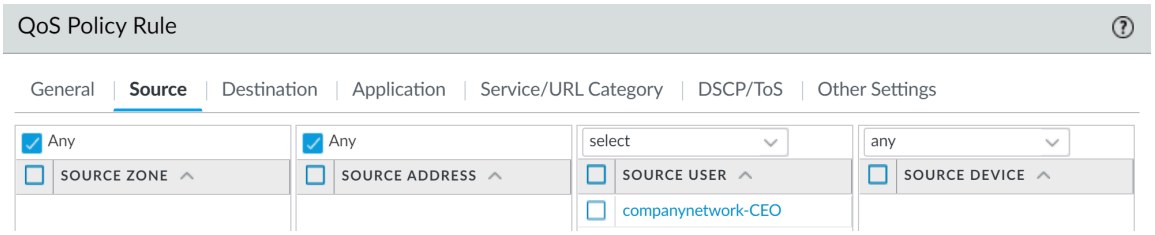
管理者は、50 Mbps を保証帯域（**[最低保証帯域 出力側]**）として割り当て、ネットワークの輻輳状態に関係なく常にその帯域幅（CEO の必要量を超える）が CEO に割り当てられるように保証します。

管理者は、次に class1 トラフィックの優先順位を high に指定し、プロファイルの最大帯域幅使用量（**[最大保証帯域 出力側]**）を、管理者が QoS を有効にするインターフェイスの最大帯域幅と同じ 1000 Mbps に設定します。管理者は、いかなる場合でも CEO の帯域幅使用量が制約されないような設定を選択しています。

ベスト プラクティスでは、プロファイルの最大帯域幅がインターフェイスの最大帯域幅と一致する場合でも、***QoS*** プロファイルの ***[最大保証帯域 出力側]*** フィールドに値を入力します。***QoS*** プロファイルの最大帯域幅は、***QoS*** を有効にする予定のインターフェイスの最大帯域幅を決して超えないようにする必要があります。

STEP 2 | 管理者は、CEO のトラフィックを識別する QoS ポリシーを作成し（**Policies (ポリシー)** > **QoS**）、QoS プロファイルで定義したクラスに割り当てます（前のステップを参照）。ユーザー ID が設定されていることから、管理者は QoS ポリシーの **Source** （送信元）タブを使用して、CEO のトラフィックを企業ネットワークのユーザー名で個別に識別します

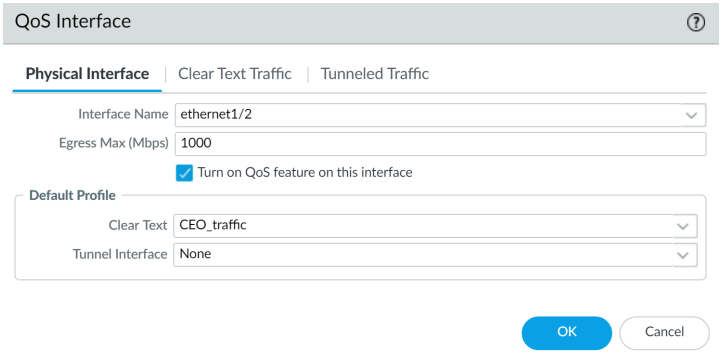
（User-ID が設定されていない場合、管理者は **[送信元アドレス]** の下に CEO の IP アドレスを **[追加]** できます。User-IDを参照）：



管理者は、CEO のトラフィックを class1 と関連付け（**[その他の設定]** タブ）、続けて残りの必須フィールドに値を入力します。つまり管理者は、ポリシーに分かりやすい **[名前]**（**[全般]** タブ）を付け、**[送信元ゾーン]**（**[送信元]** タブ）と**[宛先ゾーン]**（**[宛先]** タブ）で **[いずれか]** を選択します。

	NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	DSCP/TOS	CLASS
1	HTTPS	none	trust	any	any	any	untrust	any	any	web-browsing	any	any	2
2	Voice-Video	none	any	any	any	any	any	any	any	voip-video-l...	any	any	1
3	Guarantee CEO bandwidth	none	any	any	companynet...	any	any	any	any	any	any	any	1

STEP 3 | これで CEO のトラフィックに class1 が関連付けられ、管理者は、**[このインターフェイスの QoS 機能をオンにする]** をオンにし、トラフィック フローの出力インターフェイスを選択して、QoS を有効にします。CEO のトラフィック フローの出力インターフェイスは外向きインターフェイスで、この場合は ethernet 1/2 です。

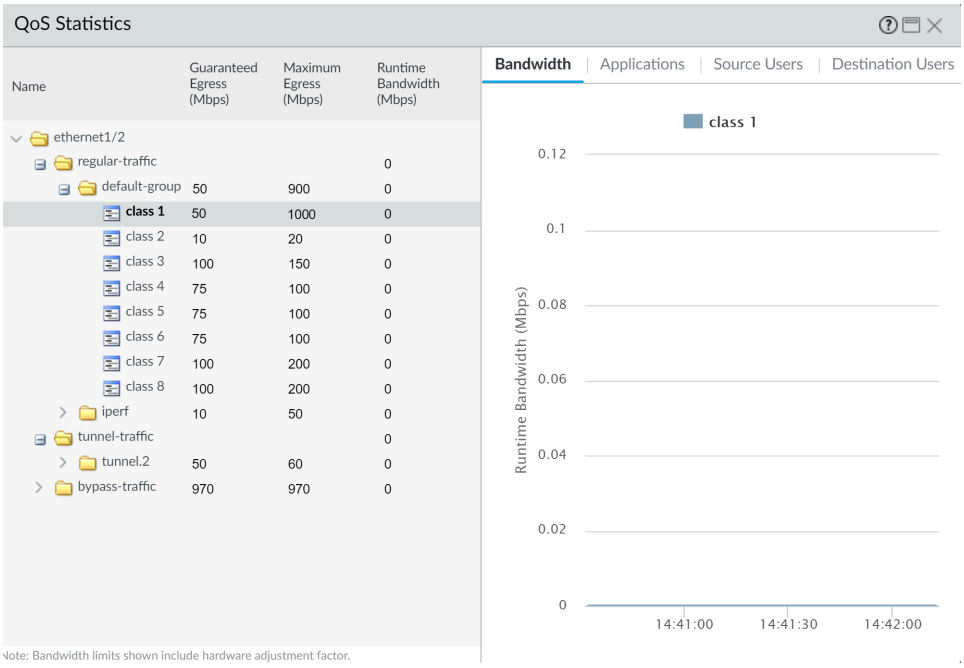


管理者は、作成した QoS プロファイルと関連 QoS ポリシーによって CEO が送信するすべてのトラフィックが保証されるようにするため、*CEO_traffic* を選択して ethernet 1/2 からの **[クリア テキスト]** トラフィックに適用します。

STEP 4 | QoS 設定のコミット後、管理者は **Network (ネットワーク)** > **QoS** ページに移動して、外向きインターフェイス ethernet 1/2 で QoS プロファイル CEO_traffic が有効になっていることを確認します。

NAME	GUARANTEED EGRESS (MBPS)	MAXIMUM EGRESS (MBPS)	PROFILE	ENABLED	
ethernet1/2		1,000.000		☑	Statistics
Tunneled Traffic					
Clear Text Traffic	50.000		CEO_traffic		

STEP 5 | [統計] をクリックして、CEO が発信するトラフィック（class 1）が ethernet 1/2 から出て行くときにどのようにシェーピングされているかを確認します。



このケースでは、単一の送信元ユーザーからのトラフィックに *QoS* を適用する方法を示します。ただし、宛先ユーザーへのトラフィックの保証およびシェーピングも行う場合は、同様の *QoS* セットアップを設定できます。このワークフローの代わりに、またはこのワークフローに加えて、（ユーザーの送信元情報を指定する代わりに）***Policies* (ポリシー) > *QoS*** ページで ***Destination Address* (宛先アドレス)**としてユーザーの *IP*アドレスを指定する*QoS*ポリシーを作成し、***Network* (ネットワーク) > *QoS*** ページで、（外向きインターフェースの代わりに）ネットワークの内向きインターフェースで *QoS* を有効にします。

「ユース ケース：音声およびビデオ アプリケーションの QoS

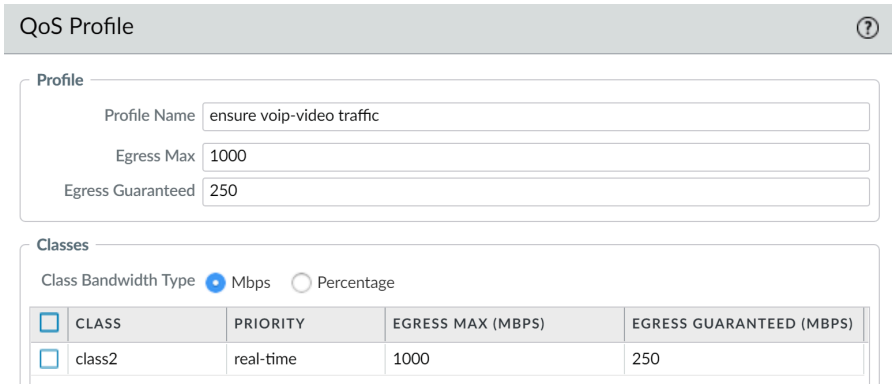
音声およびビデオ トラフィックは、QoS 機能でシェーピングおよび制御する測定量（特に遅延およびジッター）の影響を大きく受けます。音声およびビデオ送信情報が聞き取り可能で明瞭であるためには、音声およびビデオ パケットがドロップされたり、遅れたり、または不均一に配信されたりしないようにする必要があります。音声およびビデオ アプリケーションの場合のベスト プラクティスは、帯域幅を保証することのほかに、音声およびビデオ トラフィックが優先されるように保証することです。

この例では、企業の支社の従業員が、ビデオ会議や Voice over IP （VoIP）テクノロジを利用して行われる他の支社、パートナー企業、および顧客との間のビジネス通信で困難を経験しており、信頼性を確立することができていません。IT 管理者は、これらの問題に対処するために QoS を実装し、支社の従業員のビジネス通信の効果性と信頼性を高めようとしています。管理者は、送受信両方のネットワーク トラフィックに対して QoS を保証するため、ファイアウォールの内向きと外向きの両方のインターフェイスで QoS を有効にします。

STEP 1 | 管理者は QoS プロファイルを作成して Class 2 を定義します。これにより、Class 2 トラフィックに優先順位 real-time が設定され、最大帯域幅が 1000 Mbps のインターフェイスでは、ネットワーク使用量のピーク期間を含め、250 Mbps の帯域幅が常時保証されます。

real-time 優先順位は、通常、遅延の影響を受けやすいアプリケーションの場合に推奨され、特に音声およびビデオ アプリケーションのパフォーマンスおよび品質を保証する場合に役立ちます。

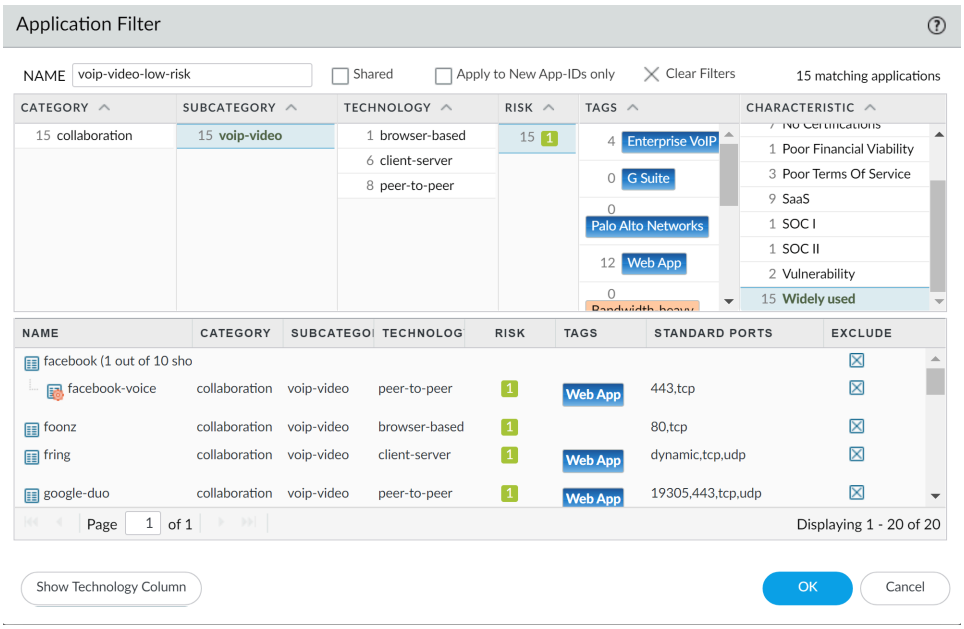
ファイアウォールの Web インターフェイス上で管理者が **Network** (ネットワーク) > **Network Profiles** (ネットワーク プロファイル) > **Qos Profile** (Qos プロファイル) ページを選択し、**Add** (追加) をクリックし、**Profile Name** (プロファイル名) 「ensure voip-video traffic」を入力し、Class 2 トラフィックを定義します。



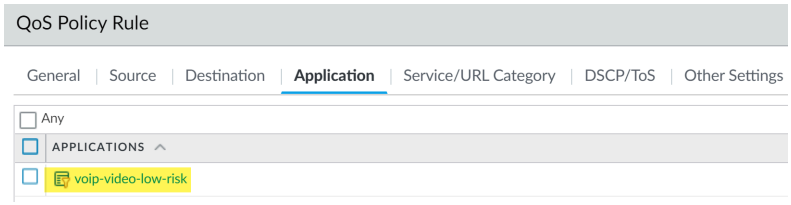
STEP 2 | 管理者は、QoS ポリシーを作成して、音声およびビデオ トラフィックを識別します。この企業には音声およびビデオ用の 1 つの標準アプリケーションがないため、管理者は、他の支社、パートナー企業、および顧客との通信で一般的に従業員が通常使用するいくつかのアプリケーションに、確実に QoS が適用されるようにします。管理者は、**Policies** (ポリシー) > **QoS** > **QoS Policy Rule** (QoS ポリシー ルール) > **Applications** (アプリケーション) タブで **Add** (追加) をクリックして、**Application Filter** (アプリケーション フィルタ) ウィンドウを開きます。次に管理者は、QoS を適用するアプリケーションをフィルタするための基

準を選択し、サブカテゴリとして voip-video を選択し、low-risk と widely-used の両方が当てはまる viop-video アプリケーションのみを指定することによって対象を絞り込みます。

アプリケーション フィルタは動的なツールであり、QoS ポリシーでアプリケーションのフィルタリングに使用すると、任意の時点で voip-video、low risk、および widely used の基準を満たすすべてのアプリケーションに QoS が適用されるようにできます。



管理者は、この **[アプリケーション フィルタ]** に「voip-video-low-risk」という名前を付け、QoS ポリシーに含めます。

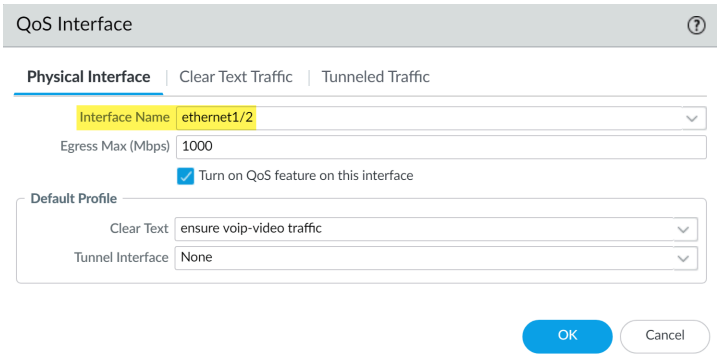


管理者はQoSポリシーにVoice-Video という名前を付け、Other Settings [その他の設定]を選択し、ポリシーClass 2にマッチしたすべてのトラフィックを割り当てます。管理者は、送受信両方の QoS トラフィックに Voice-Video QoS ポリシーを使用するため、**Source** （送信元）と **Destination** （宛先）の両方の情報を **Any** （いずれか）に設定します。

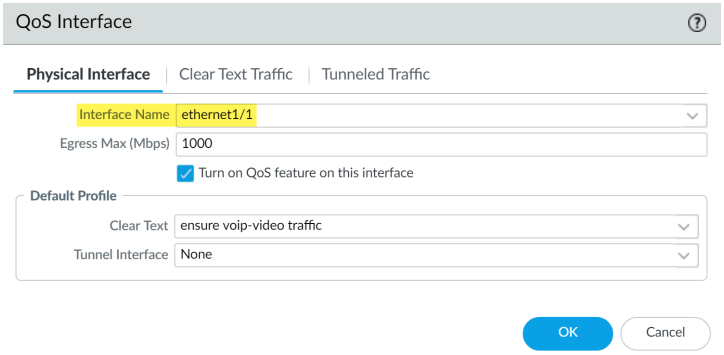
			Source				Destination						
	NAME	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	DSCP/TOS	CLASS
1	HTTPS	none	trust	any	any	any	untrust	any	any	web-browsing	any	any	2
2	Voice-Video	none	any	any	any	any	any	any	any	voip-video-l...	any	any	1

STEP 3 | 管理者は、音声およびビデオ通信の送受信の両方で QoS を確保するため、ネットワークの外向きインターフェイス（QoS を送信の通信に適用する）と内向きインターフェイス（QoS を受信の通信に適用する）で QoS を有効にします。

管理者はまず、外向きインターフェイス（この場合は ethernet 1/2）について作成した QoS プロファイル ensure voice-video traffic（このプロファイルで、Class 2 は作成したポリシー Voice-Video と関連付けられます）を有効にします。



次に、2番目のインターフェイス、内向きインターフェイス（この場合は ethernet 1/1）で同じ QoS プロファイル ensure voip-video traffic を有効にします。



STEP 4 | 管理者は **Network (ネットワーク)** > **QoS** を選択し、送受信両方の音声およびビデオ トラフィックで QoS が有効になっていることを確認します。

NAME	GUARANTEED EGRESS (MBPS)	MAXIMUM EGRESS (MBPS)	PROFILE	ENABLED	
ethernet1/1		1,000.000		☑	Statistics
Tunneled Traffic					
Clear Text Traffic	250.000		ensure voip-video traffic		
ethernet1/2		1,000.000		☑	Statistics
Tunneled Traffic					
Clear Text Traffic	250.000		ensure voip-video traffic		

管理者は、ネットワークの内向きと外向きの両方のインターフェイスで QoS を有効にすることができました。これで、ネットワークを出入りする両方向で音声およびビデオ アプリケーション トラフィックに対して real-time 優先順位が保証され、特に遅延およびジッターの影響を受けやすいそれらの通信を使用して企業内外のビジネス上の通信を行うときの信頼性と効果性が確保されます。

VPN

仮想プライベート ネットワーク（VPN）は、ユーザー/システムをローカル エリア ネットワーク（LAN）で接続している場合と同様に、パブリック ネットワークでも安全に接続することができるトンネルを作成します。VPN トンネルをセットアップするには、互いに認証し、両者間の情報の流れを暗号化できるデバイスのペアが必要です。デバイスとして使用できるのは、Palo Alto Networks ファイアウォールのペア、または Palo Alto Networks ファイアウォールと他ベンダーの VPN 対応デバイスです。

- VPN デプロイメント
- サイト間 VPN の概要
- サイト間 VPN の概念
- サイト間 VPN のセットアップ
- サイト間 VPN のクイック設定

VPN デプロイメント

Palo Alto Networks ファイアウォールでは、以下の VPN デプロイメントをサポートしています。

- サイト間 **VPN** – 中央サイトとリモート サイトを接続する簡易 VPN、または中央サイトと複数のリモート サイトを接続するハブ アンド スポーク VPN。ファイアウォールはプロトコルの IP Security （IPSec）セットを使用して、2 つのサイト間のトラフィックの安全なトンネルをセットアップします。サイト間 VPN の概要を参照してください。
- リモート ユーザーからサイトへの **VPN** – GlobalProtect エージェントを使用してリモート ユーザーがファイアウォール経由で安全な接続を確立できるようにするソリューション。このソリューションは、SSL および IPSec を使用してユーザーとサイト間の安全な接続を確立します。『GlobalProtect 管理者ガイド』を参照してください。
- 大規模 **VPN** – Palo Alto Networks の GlobalProtect 大規模 VPN （LSVPN）は、最大 1,024 のサテライト オフィスまで拡張可能なハブ アンド スポーク VPN を展開するための簡略化されたメカニズムを提供します。このソリューションを使用するには、Palo Alto Networks ファイアウォールをハブおよびすべてのスポークでデプロイする必要があります。デバイスの認証に証明書を、すべてのコンポーネント間の安全な通信のために SSL を、データの保護のために IPSec を使用します。大規模 VPN （LSVPN）を参照してください。

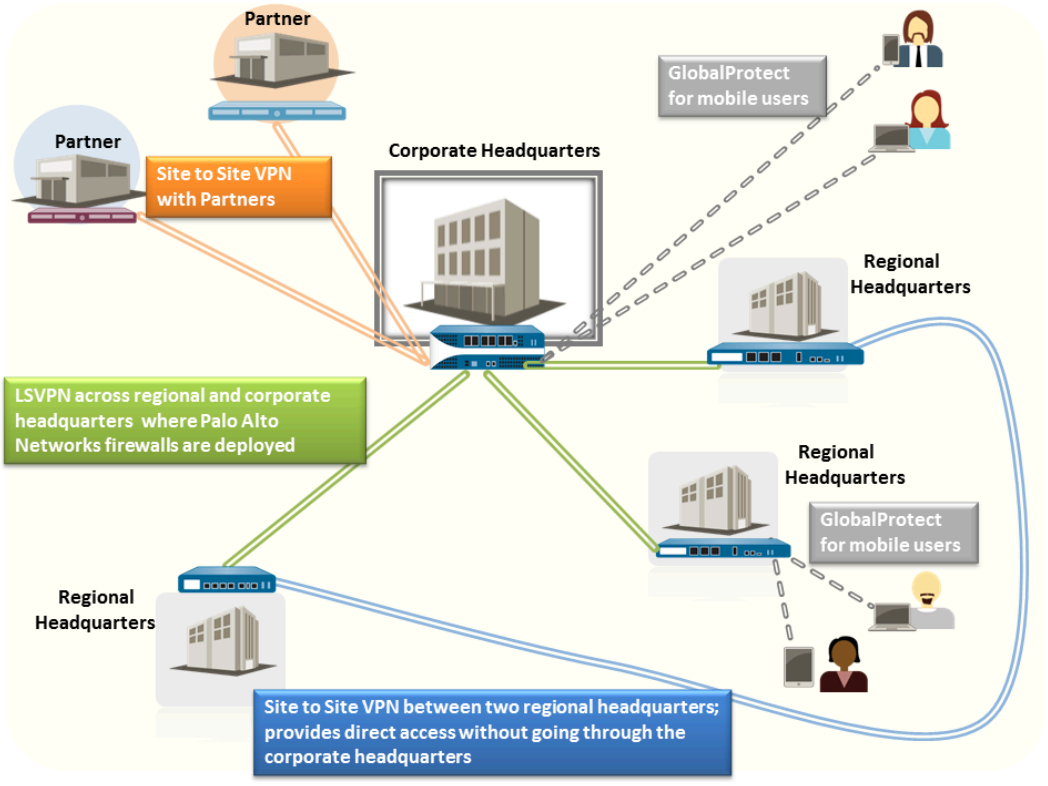


図 **7 : VPN** デプロイメント

サイト間 VPN の概要

2 つのローカル エリア ネットワーク（LAN）を接続できるようにする VPN 接続はサイト間 VPN と呼ばれます。ルートベースの VPN を設定すると、2 つのサイトに設置された Palo Alto Networks ファイアウォール間、または Palo Alto Networks ファイアウォールと別の場所に設置されたサードパーティのセキュリティ デバイスを接続できます。ファイアウォールは、サードパーティのポリシーベースの VPN デバイスとの相互運用性も確保しています。Palo Alto Networks ファイアウォールはルートベースの VPN をサポートしています。

Palo Alto Networks ファイアウォールはルートベースの VPN をセットアップし、ファイアウォールは宛先 IP アドレスに基づいてルーティングの判断を行います。トラフィックが VPN トンネル経由で特定の宛先にルーティングされた場合は、VPN トラフィックとして処理されます。

プロトコルの IP Security （IPSec）セットを使用して VPN トラフィックに安全なトンネルをセットアップすると、TCP/IP パケットの情報の安全が確保されます（トンネル タイプが ESP の場合は暗号化されます）。IP パケット（ヘッダーおよびペイロード）は別の IP ペイロードに埋め込まれ、新しいヘッダーが適用され、IPSec トンネルを経由して送信されます。新しいヘッダーの送信元 IP アドレスはローカル VPN ピアのアドレスであり、宛先 IP アドレスはトンネルの反対側の VPN ピアのアドレスです。パケットがリモート VPN ピア（トンネルの反対側のファイアウォール）に達すると、外部ヘッダーが削除され、元のパケットがその宛先に送信されます。

VPN トンネルをセットアップするには、最初にピアを認証する必要があります。認証に成功したら、ピアは暗号化メカニズムおよびアルゴリズムをネゴシエートして、通信を安全にします。Internet Key Exchange （IKE）プロセスが VPN ピアの認証に使用され、VPN 通信を保護するために IPSec Security Associations （SA）がトンネルの両端で定義されます。IKE はデジタル証明書または事前共有鍵、および Diffie Hellman 鍵を使用して IPSec トンネル用の SA をセットアップします。SA は、セキュリティパラメータインデックス (SPI)、セキュリティプロトコル、暗号化キー、および宛先 IP アドレス (暗号化、データ認証、データ整合性、エンドポイント認証) を含む、安全な伝送に必要なすべてのパラメータを指定します。

以下の図は、2 つのサイト間の VPN トンネルを示しています。VPN ピア A によって保護されたクライアントが他のサイトに設置されたサーバーのコンテンツを必要とする場合、VPN ピア A は VPN ピア B への接続要求を開始します。セキュリティ ポリシーによって接続が許可される場合、VPN ピア A は IKE 暗号のプロファイル パラメータ（IKE フェーズ 1）を使用して安全な接続を確立し、VPN ピア B を認証します。次に、VPN ピア A は IPSec 暗号のプロファイルを使用して VPN トンネルを確立し、これによって IKE フェーズ 2 パラメータを定義して、2 つのサイト間の安全なデータ転送を可能にします。

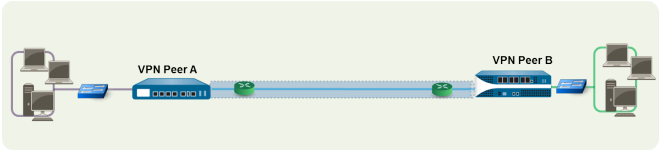


図 **8 :** サイト間**VPN**

サイト間 VPN の概念

VPN 接続により、2 つ以上のサイト間で安全に情報にアクセスできるようになります。リソースへの安全なアクセスを可能にして接続の信頼性を高めるために、VPN 接続には以下のコンポーネントが必要です。

- IKE ゲートウェイ
- トンネルインターフェイス
- トンネル モニタ
- VPN 用の Internet Key Exchange（IKE）
- IKEv2

IKE ゲートウェイ

Palo Alto Networks ファイアウォール同士、またはファイアウォールと別のセキュリティ デバイスが 2 つのネットワーク間で VPN 接続を開始して終了する場合、これらは IKE ゲートウェイと呼ばれます。VPN トンネルをセットアップして IKE ゲートウェイ間でトラフィックを送信するには、各ピアにスタティックまたはダイナミックな IP アドレスまたは FQDN が必要です。VPN ピアは事前共有鍵または証明書を使用して相互に認証します。

ピアは、VPN トンネルをセットアップするためのモード（main または aggressive）と IKE フェーズ 1 における SA のライフタイムをネゴシエートする必要があります。main モードはピアの ID を保護し、トンネルをセットアップするときにより多くのパケットが交換されるため安全性が高いモードです。両方のピアでサポートされている場合、IKE ネゴシエーションのための推奨モードは main モードです。aggressive モードは VPN トンネルをセットアップするために使用するパケットが少ないため、高速ですが VPN トンネルをセットアップする場合に安全性が劣る選択肢です。

構成の詳細については、IKE ゲートウェイのセットアップを参照してください。

トンネルインターフェイス

VPN トンネルをセットアップするには、両端のレイヤー 3 インターフェイスに VPN トンネルを接続して確立するためのファイアウォール用の論理トンネル インターフェイスが必要です。トンネル インターフェイスとは、2 つのエンドポイント間でトラフィックを配信するために使用される論理（仮想）インターフェイスです。設定済みのプロキシ ID がある場合、IPSec トンネルの容量にプロキシ ID が加味されます。

トンネル インターフェイスはポリシーを適用するセキュリティ ゾーンに属する必要があり、既存のルーティング インフラストラクチャを使用するには仮想ルーターに割り当てる必要があります。ファイアウォールがルート検索を実行して、使用する適切なトンネルを判断できるように、トンネル インターフェイスと物理インターフェイスが同じ仮想ルーターに割り当てられるようにします。

一般に、トンネル インターフェイスが接続されたレイヤー 3 インターフェイスは、たとえば Untrust ゾーンなどの外部ゾーンに属します。トンネル インターフェイスは物理インターフェイスと同じセキュリティ ゾーンに配置できますが、安全性と可視性を高めるため、トンネル イン

ターフェイス用に別個のゾーンを作成することができます。トンネル インターフェイス用に、たとえば VPN ゾーンなどの別個のゾーンを作成する場合、VPN ゾーンと Trust ゾーン間でトラフィックが流れるようにセキュリティ ポリシーを作成する必要があります。

サイト間のトラフィックのルーティングでは、トンネル インターフェイスに IP アドレスは必要ありません。IP アドレスが必要になるのは、トンネル モニタリングを有効にする場合か、トンネル間のトラフィックをルーティングするためにダイナミック ルーティング プロトコルを使用している場合のみです。ダイナミック ルーティングでは、トンネル IP アドレスは VPN トンネルへのトラフィックをルーティングするためのネクスト ホップ IP アドレスとして機能します。

ポリシーベースの VPN を実行する VPN ピアで Palo Alto Networks ファイアウォールを設定している場合、IPSec トンネルをセットアップするときにローカルおよびリモートのプロキシ ID を設定する必要があります。各ピアは、IKE フェーズ 2 ネゴシエーションを成功させるために、ここで設定したプロキシ ID をパケットで実際に受信する ID と比較します。複数のトンネルが必要な場合、各トンネル インターフェイスに一意のプロキシ ID を設定します。1 つのトンネル インターフェイスに最大 250 個のプロキシ ID を設定できます。各プロキシ ID はファイアウォールの IPSec VPN トンネル容量にカウントされます。トンネル容量はファイアウォールのモデルごとに異なります。

構成の詳細については、IPSec トンネルのセットアップを参照してください。

トンネル モニタ

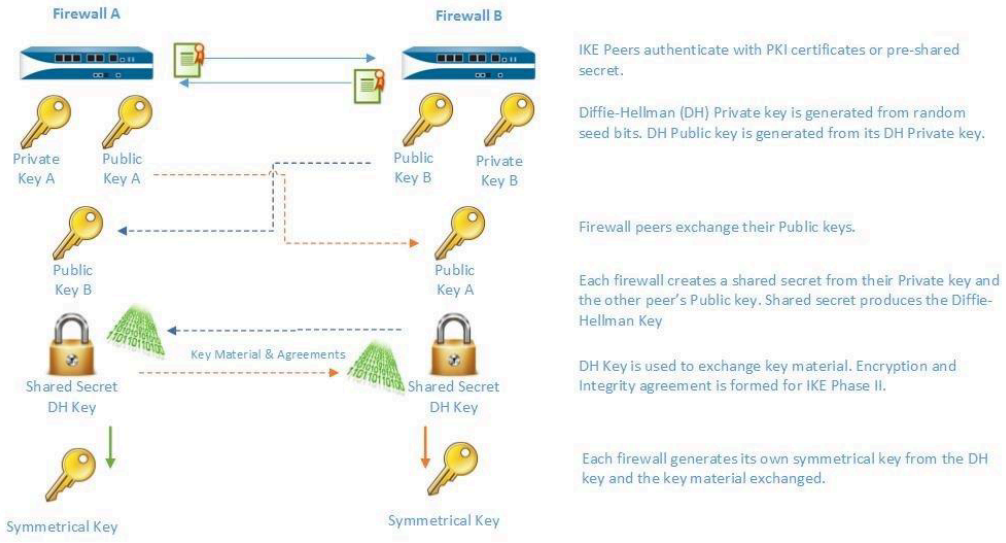
VPN トンネルでは、トンネルを経由して宛先 IP アドレスへの接続を確認できます。ファイアウォールでネットワーク モニタリング プロファイルを使用することで、宛先 IP アドレスへの接続（ICMP を使用）または指定したポーリング間隔でネクスト ホップを確認し、モニタリング対象 IP アドレスへのアクセスで障害が発生した場合のアクションを指定できます。

宛先 IP にアクセスできない場合、トンネルが回復するのを待機するようにファイアウォールを設定するか、別のトンネルへの自動フェイルオーバーを設定できます。どちらの場合も、ファイアウォールはトンネル障害を警告するシステム ログを生成し、IPSec 鍵を再ネゴシエートして回復を加速させます。

構成の詳細については、トンネル モニタリングのセットアップを参照してください。

VPN 用の Internet Key Exchange（IKE）

IKE プロセスにより、トンネル両端の VPN ピアは、相互に合意したキーまたは証明書、および暗号化方法を使用して、パケットを暗号化および復号化することができます。IKE プロセスは、2 つのフェーズで行われます。IKE フェーズ 1 および IKE フェーズ 2。各フェーズは、暗号プロファイル（IKE 暗号プロファイルおよび IPSec 暗号プロファイル）を使用して定義されたキーと暗号化アルゴリズムを使用し、IKE ネゴシエーションの結果が Security Association （SA）です。SA は相互に合意されたキーとアルゴリズムのセットで、VPN トンネルでのデータのフローを許可するため両方の VPN ピアによって使用されます。以下の図は、VPN トンネルをセットアップするための鍵交換プロセスを示しています。



IKE フェーズ 1

このフェーズでは、ファイアウォールは IKE ゲートウェイ設定で定義されたパラメータおよび IKE 暗号プロファイルを使用して相互に認証し、安全な制御チャネルをセットアップします。IKE フェーズは、VPN ピアの相互認証に事前共有鍵またはデジタル証明書（公開鍵インフラストラクチャ（PKI）を使用）の使用をサポートしています。事前共有鍵は PKI インフラストラクチャのサポートを必要としないため、小規模なネットワークを保護するための単純なソリューションです。大規模なネットワーク、またはより堅牢な認証セキュリティが必要な実装では、デジタル証明書の方が適しています。

証明書を使用する場合、証明書を発行する CA が両方のゲートウェイ ピアによって信頼されており、証明書チェーン内の証明書の最大長が 5 以下であることを確認します。IKE フラグメンテーションを有効にすると、ファイアウォールは証明書チェーン内の最大 5 個の証明書で IKE メッセージを再アセンブルし、正常に VPN トンネルを確立できます。

IKE 暗号プロファイルは、IKE SA ネゴシエーションで使用される以下のオプションを定義します。

- IKE 用の対象鍵を生成するための Diffie-Hellman（DH）グループ。

  Diffie-Hellman アルゴリズムは、一方の秘密鍵ともう一方の公開鍵を使用して共有のシークレットを作成します。これは、両方の VPN トンネル ピアによって共有される暗号化鍵です。ファイアウォールでサポートされている DH グループ：

グループ番号	ビット数
グループ1	768 ビット
グループ2	1024 ビット (デフォルト)
グループ 5	1536 ビット
グループ 14	2048 ビット

グループ番号	ビット数
グループ 15	3072ビットモジュラー指数群
グループ 16	4096ビットモジュラー指数群
グループ 19	256 ビット楕円曲線グループ
グループ 20	384 ビット楕円曲線グループ
グループ 21	512 ビットのランダム楕円曲線グループ

- 認証アルゴリズム – sha1、sha 256、sha 384、sha 512、または md5
- Encryption algorithms—aes-256-gcm, aes-128-gcm, 3des, aes-128-cbc, aes-192-cbc, or aes-256-cbc

IKE フェーズ 2

トンネルが保護されて認証されると、フェーズ 2 では、ネットワーク間でのデータ送受信のためにチャネルがさらに保護されます。IKE フェーズ 2 では、プロセスのフェーズ 1 で確立されたキーと、IKE フェーズ 2 の SA で使用する IPSec プロトコルとキーを定義する IPSec 暗号プロファイルを使用します。

IPSEC は、以下のプロトコルを使用して安全な通信を可能にします。

- Encapsulating Security Payload （ESP） – IP パケット全体を暗号化し、送信元を認証してデータの整合性を確認できます。ESP ではパケットを暗号化して認証する必要がありますが、暗号化オプションを Null （ヌル）に設定することで暗号化のみまたは認証のみを行うように設定できます。認証をせずに暗号化を使用するのは推奨されません。
- Authentication Header （AH） – パケットの送信元を認証し、データの整合性を確認します。AH はデータ ペイロードを暗号化しないため、データ保護が重要なデプロイメントには適していません。AH は、データ保護が必要でなく、主な懸念がピアの正当性を確認することである場合によく使用されます。

表 **5 : IPSEC** 認証および暗号化でサポートされるアルゴリズム

エスケープ	**AH**
サポートされる Diffie Hellman （DH）交換オプション	

- グループ 1 – 768 ビット
- グループ 2 - 1024 ビット(デフォルト)
- グループ 5 – 1536 ビット
- グループ 14:2048 ビット
- グループ 15:3072 ビットのモジュラー指数グループ
- グループ 16:4096 ビットのモジュラー指数グループ

エスケープ	AH
• グループ 19 - 256 ビット楕円曲線グループ • グループ 20 – 384 ビット楕円曲線グループ • グループ 21:512 ビットのランダム楕円曲線グループ • no-pfs – デフォルトでは、Perfect Forward Secrecy （PFS）が有効化され、上記いずれかのグループを使用して IKE フェーズ 2 で新しい DH キーが生成されます。このキーは IKE フェーズ 1 で交換されるキーとは関係なく、より堅牢なデータ転送セキュリティが提供されます。no-pfs を選択すると、フェーズ 1 で作成された DH キーが更新されず、1 つのキーが IPSec SA ネゴシエーションに使用されます。両方の VPN ピアを PFS について有効化または無効化する必要があります。	
サポートされる暗号化アルゴリズム	
• 3desIPv6	セキュリティ強度が 112 ビットの Triple Data Encryption Standard （トリプル DES 暗号化）
• aes-128-cbc	セキュリティ強度が 128 ビットの暗号ブロック チェーン（CBC）を使用した Advanced Encryption Standard （AES）
• aes-192-cbc	セキュリティ強度が 192 ビットの CBC を使用した AES
• aes-256-cbc	セキュリティ強度が 256 ビットの CBC を使用した AES
• aes-128-ccm	セキュリティ強度が 128 ビットの CBC-MAC （CCM）を使用した AES
• aes-128-gcm	セキュリティ強度が 128 ビットの Galois/Counter Mode （GCM）を使用した AES
• aes-256-gcm	セキュリティ強度が 256 ビットの GCM を使用した AES
サポートされる認証アルゴリズム	
• md5	• md5
• sha 1	• sha 1
• sha 1	• sha 1
• sha 1	• sha 1
• SHA512	• sha 512

IPSec VPN トンネルを保護するための方法（IKE フェーズ 2）

IPSec VPN トンネルは、手動キーまたは自動キーを使用して保護できます。さらに、IPSec の設定オプションには、Diffie-Hellman グループによる鍵共有、暗号化アルゴリズム、およびメッセージ認証のためのハッシュなどがあります。

- 手動キー — 手動キーは一般に、Palo Alto Networks ファイアウォールがレガシー デバイスとの VPN トンネルを確立しているか、セッション キーを生成するオーバーヘッドを軽減する場合に使用されます。手動キーを使用する場合、同じキーを両方のピアで設定する必要があります。

  ピア間でキー情報をリレーする際にセッション キーが解読されるおそれがあるため、VPN トンネルを確立する場合、手動キーは推奨されません。キーが解読されると、データの送受信が保護されなくなります。
- 自動キー — 自動キーを使用すると、IPSec 暗号プロファイルで定義されたアルゴリズムに基づいて IPSec トンネルをセットアップしてメンテナンスするためにキーを自動的に生成できます。

IKEv2

IPSec VPN ゲートウェイは、IKEv1 または IKEv2 を使用して IKE Security Association （SA）および IPSec トンネルをネゴシエートします。IKEv2 は RFC 5996 で定義されています。

フェーズ 1 SA とフェーズ 2 SA を使用する IKEv1 とは異なり、IKEv2 は IKE SA で設定された Encapsulating Security Payload （ESP）または Authentication Header （AH）の子 SA を使用します。

2 つのゲートウェイ間に配置されたデバイスで発生する NAT がある場合は、両方のゲートウェイで NAT トラバーサル（NAT-T）を有効にする必要があります。ゲートウェイは、NAT デバイスの（グローバルにルーティング可能な）パブリック IP アドレスのみを確認できます。

IKEv2 には、IKEv1 に比べて以下の利点があります。

- トンネル確立時にエンドポイント間で交わされるメッセージ数が少なくなります。IKEv2 は 4 個のメッセージを使用し、IKEv1 は 9 個（main モードの場合）または 6 個のメッセージ（aggressive モードの場合）を使用します。
- 組み込み NAT-T 機能により、ベンダー間の互換性が向上します。
- トンネルがダウンした場合でも、組み込みのヘルスチェックが自動的にトンネルを再確立します。IKEv1 で使用されていた Dead Peer Detection の代替として、存続性チェックを使用できます。
- トラフィック セレクターがサポートされます (1 交換につき 1 つ)。IKE ネゴシエーションではトラフィック セレクターを使用して、トンネルへのアクセスを許可するトラフィックを決定します。
- フラグメンテーションを軽減するためのハッシュおよび URL 証明書の交換がサポートされています。
- 向上したピア検証による DoS 攻撃に対する耐障害性。ハーフオープン SA が過剰に検出されると、cookie 検証が実行されます。

IKEv2 を設定する前に、以下の概念を把握する必要があります。

- ライブネス チェック
- Cookie アクティベーションのしきい値と Cookie の厳密な検証
- トラフィック セレクタ
- ハッシュおよび URL 証明書の交換
- SA キーの有効期間と再認証間隔

IKE ゲートウェイのセットアップ後、IKEv2 を選択した場合は、ご使用の環境で要求されているように、IKEv2 に関連する以下のオプション・タスクを実行します。

- ハッシュおよび URL を使用してアクセスするピアの証明書のエクスポート
- IKEv2 ゲートウェイ認証の証明書のインポート
- IKEv2 のキーの有効期間または認証間隔の変更
- IKEv2 の Cookie アクティベーションのしきい値の変更
- IKEv2 トラフィック セレクタの設定

ライブネス チェック

IKEv2 のライブネス チェックは、IKEv1 でピアがまだ使用可能かどうかを判断するために使用されるデッド ピア検出（DPD）と似ています。

IKEv2 では、ライブネス チェックはすべての IKEv2 パケット送信、または設定可能な間隔（デフォルトは 5 秒）でゲートウェイがピアに送信する空の情報メッセージで実行されます。必要に応じて、送信側が最大 10 回まで再送信を試行できます。応答が得られない場合、送信側は IKE_SA および対応する CHILD_SA を閉じて削除します。送信側は、別の IKE_SA_INIT メッセージを送信して、もう一度やり直します。

Cookie アクティベーションのしきい値と Cookie の厳密な検証

Cookie の検証は IKEv2 では常に有効化され、ハーフオープン SA DoS 攻撃に対する保護に役立ちます。Cookie の検証をトリガーするハーフオープン SA のグローバルしきい値を設定できます。新しい IKEv2 SA ごとに Cookie の検証を適用するように、個々の IKE ゲートウェイを設定することもできます。

- **Cookie Activation Threshold (Cookie** アクティベーションのしきい値**)** は、同時に発生するハーフオープン IKE SA の数（デフォルトは 500）を制限するグローバル VPN セッション設定です。ハーフオープン IKE SA の数が **Cookie Activation Threshold** [Cookie アクティベーションのしきい値]を超えると、レスポンダが Cookie を要求し、イニシエータは接続を検証する Cookie が含まれる IKE_SA_INIT で応答する必要があります。Cookie の検証に成功すると、別の SA を開始できます。値を 0 にすると、Cookie の検証が常にオンになります。

  レスポンダはイニシエータが Cookie を返すまで、イニシエータの状態を管理せず、Diffie-Hellman キーの交換も実行しません。IKEv2 の Cookie の検証は、多数の接続をハーフオープンのままにしようとする DoS 攻撃を軽減します。

  Cookie Activation Threshold[Cookie アクティベーションのしきい値] は、**Maximum Half Opened SA** [ハーフ オープン SA の最大数]設定を超えないようにする必要があります。非常に高い数値 (65534 など) にIKEv2 の Cookie アクティベーションのしきい値の変

更し、**Maximum Half Open SA** 設定がデフォルト値の 65535 のままの場合、Cookie の検証は基本的に無効になります。

- グローバルしきい値に関係なく、ゲートウェイが受信するすべての新しい IKEv2 SA に対して Cookie の検証を実行するには、**Strict Cookie Validation** [Cookie の厳密な検証]を有効にします。**Strict Cookie Validation** [Cookie の厳密な検証]は設定されいる IKE ゲートウェイにのみ影響し、デフォルトでは無効になっています。**Strict Cookie Validation (Cookie** の厳密な検証**)** が無効な場合、システムは **Cookie Activation Threshold (Cookie** アクティベーションのしきい値**)** を使用して Cookie が必要かどうかを判断します。

トラフィック セレクタ

IKEv1 では、ルートベースの VPN があるファイアウォールで IPSec トンネルをセットアップするには、ローカルおよびリモート プロキシ ID を使用する必要があります。各ピアは、IKE フェーズ 2 を正常にネゴシエートするために、プロキシ ID をパケットで受信する ID と比較します。IKE フェーズ 2 は、SA をネゴシエートして IPSec トンネルをセットアップします(Proxy ID について詳しくは、トンネルインターフェイスを参照してください。

IKEv2 では、IKE ネゴシエーション時に使用されるネットワーク・トラフィックのコンポーネントであるIKEv2 トラフィック セレクタの設定できます。トラフィック セレクタは、トンネルをセットアップし、トンネルの通過が許可されるトラフィックを判断するために、CHILD_SA （トンネル作成）フェーズ 2 で使用されます。2 つの IKE ゲートウェイ ピアがネゴシートしてトラフィック セレクタについて合意する必要があります。合意しなかった場合、一方がアドレス範囲を絞り込んで合意に達します。1 つの IKE 接続で複数のトンネルを使用できます。たとえば、各部門に異なるトンネルを割り当ててトラフィックを分離することができます。トラフィックの分離によって、QoS などの機能も実装できます。

IPv4 および IPv6 トラフィック セレクタは以下のとおりです。

- 送信元 **IP** アドレス – ネットワーク プレフィックス、アドレス範囲、特定のホスト、またはワイルドカード。
- 宛先 **IP** アドレス – ネットワーク プレフィックス、アドレス範囲、特定のホスト、またはワイルドカード。
- プロトコル – 転送プロトコル（TCP または UDP など）。
- 送信元ポート – パケットの送信元ポート。
- 宛先ポート – パケットの宛先ポート。

IKE ネゴシエーション中、異なるネットワークとプロトコル用に複数のトラフィック セレクタを使用できます。たとえば、イニシエータがトンネルを介して 172.168.0.0/16 からそのピアの宛先 198.5.0.0/16 に TCP パケットを送信するとします。さらに、同じトンネルを介して 172.17.0.0/16 から同じゲートウェイの宛先 0.0.0.0 に UDP パケットを送信します。ピア ゲートウェイは、この送信を承諾するためにこれらのトラフィック セレクタに同意する必要があります。

ゲートウェイは、他のゲートウェイの IP アドレスよりも具体的な IP アドレスのトラフィック セレクタを使用してネゴシエーションを開始できます。

- たとえば、ゲートウェイ A は 172.16.0.0/16 の送信元 IP アドレスと 192.16.0.0/16 の宛先 IP アドレスを提供します。一方、ゲートウェイ B は送信元 IP アドレスとして 0.0.0. （任意の送信元）、宛先 IP アドレスとして 0.0.0. （任意の宛先）が設定されています。したがっ

て、ゲートウェイ B は送信元 IP アドレスを 192.16.0.0/16、宛先アドレスを 172.16.0.0/16 に絞り込みます。この絞り込みによって、ゲートウェイ A のアドレスに対応し、2 つのゲートウェイのトラフィック セレクタが同意に達します。

- （送信元 IP アドレスとして 0.0.0.0 が設定された）ゲートウェイ B はレスポンダではなくイニシエータになり、ゲートウェイ A はより具体的な IP アドレスで応答し、ゲートウェイ B がアドレスを絞り込んで合意に達します。

ハッシュおよび URL 証明書の交換

IKEv2 では、ハッシュおよび URL 証明書の交換がサポートされています。この交換は、SA の IKEv2 ネゴシエーション中に使用されます。証明書は、URL で指定された HTTP サーバーに保存します。ピアはサーバーへの URL の受信に基づいて、サーバーから証明書をフェッチします。ハッシュは、証明書のコンテンツが有効であるかどうかの確認に使用されます。したがって、2 つのピアは証明書を相互に交換する代わりに、HTTP CA を使用して交換します。

ハッシュおよび URL のハッシュ部分によってメッセージ サイズが削減されるため、IKE ネゴシエーション中のパケット フラグメンテーションの発生確率が低くなります。ピアは期待される証明書とハッシュを受信するため、IKE フェーズ 1 でピアが検証されます。フラグメンテーションの発生の削減は、DoS 攻撃に対する保護に役立ちます。

ハッシュおよび URL 証明書の交換は、IKE ゲートウェイの設定時に **HTTP Certificate Exchange** [HTTP 証明書の交換]を選択し、**Certificate URL** [証明書 URL]を入力することで有効にできます。交換が正常に行われるには、ピアもハッシュおよび URL 証明書の交換を使用する必要があります。ピアがハッシュおよび URL を使用できない場合、X.509 証明書が IKEv1 での交換方法と同様に交換されます。

ハッシュおよび URL 証明書の交換を有効にする場合、独自の証明書を証明書サーバーにエクスポートする必要があります（サーバーにまだ存在しない場合）。証明書をエクスポートするときに、ファイル フォーマットを **Binary Encoded Certificate (DER)** [バイナリ エンコード済み証明書 (DER)]にする必要があります。ハッシュおよび URL を使用してアクセスするピアの証明書のエクスポートを参照してください。

SA キーの有効期間と再認証間隔

IKEv2 では、**Key Lifetime** [キーの有効期間]と **IKEv2 Authentication Multiple** [IKEv2 多重認証]の 2 つの IKE 暗号プロファイル値を使用して、IKEv2 IKE SA の確立を制御します。キーの有効期間は、ネゴシエートされた IKE SA キーが有効な期間です。キーの有効期間が切れる前に、SA のキーを再生成する必要があります。そうしないと、有効期限が切れたときに、SA は新しい IKEv2 IKE SA キーの再生成を開始する必要があります。デフォルト値は 8 時間です。

再認証間隔は、**Key Lifetime (**キーの有効期間**)** に **IKEv2 Authentication Multiple (IKEv2** 多重認証**)** を乗算して求められます。多重認証のデフォルトは、再認証機能が無効になる 0 に設定されています。

多重認証の範囲は 0 ～ 50 です。たとえば、多重認証を 20 に設定すると、システムは 20 回のキーの再生成（160 時間）ごとに再認証を実行します。この場合、ゲートウェイが IKE を再認証して IKE SA を最初から作り直す前に、160 時間、子 SA の作成を実行できます。

IKEv2 では、イニシエータ ゲートウェイとレスポンダ ゲートウェイに独自のキーの有効期間値が設定され、キーの有効期間が短い方のゲートウェイが SA キーの再生成を要求します。

サイト間 VPN のセットアップ

サイト間 VPN をセットアップするには、以下の手順を実行します。

- Ethernet インターフェイス、仮想ルーター、およびゾーンが正しく設定されていることを確認してください。詳細は、「インターフェイスとゾーンの設定」を参照してください。
- トンネル インターフェイスを作成します。トンネル インターフェイスを別のゾーンに置き、トンネル対象トラフィックで異なるポリシーを使用できるようにするのが理想的です。
- スタティック ルートをセットアップするか、またはルーティング プロトコルを割り当て、VPN トンネルにトラフィックを転送します。ダイナミック ルーティング（OSPF、BGP、RIP がサポートされます）をサポートするには、IP アドレスをトンネル インターフェイスに割り当てる必要があります。
- VPN トンネルの両端にあるピア間の通信を確立するために IKE ゲートウェイを定義します。また、IKEv1 フェーズ 1 で VPN トンネルをセットアップするために使用する ID、認証、暗号化のプロトコルおよびアルゴリズムを指定する暗号プロファイルも定義します。IKE ゲートウェイのセットアップおよびIKE 暗号プロファイルの定義を参照してください。
- VPN を経由してデータを転送する IPSec 接続を確立するために必要なパラメータを設定します。IPSec トンネルのセットアップを参照してください。IKEv1 Phase-2 についてはIPSec 暗号プロファイルの定義を参照してください。
- （任意）ファイアウォールによる IPSec トンネルのモニター方法を指定します。トンネル モニタリングのセットアップを参照してください。
- セキュリティ ポリシーを定義し、トラフィックのフィルタリングおよび検証を行います。

  セキュリティ ルールベースの最後に拒否ルールがある場合、許可されていない限りゾーン内のトラフィックはブロックされます。*IKE* および *IPsec* アプリケーションを許可するルールは、上記の拒否ルールに明示的に含まれている必要があります。

  VPN トラフィックが *PA-7000 Series* あるいは *PA-5200 Series* ファイアウォールを通過（送信元でも宛先でもなく）する場合、*ESP* あるいは *AH* トラフィックを双方向で許可する双方向セキュリティポリシールールを設定します。

以上の作業を実行すると、トンネルを使用できるようになります。ポリシーで定義されるゾーン/アドレスを宛先とするトラフィックは、ルーティング テーブルの宛先ルートに基づいて自動的に適切にルーティングされ、VPN トラフィックとして処理されます。サイト間 VPN の例は、サイト間 VPN のクイック設定を参照してください。

トラブルシューティングのために、IKE ゲートウェイまたは IPSec トンネルの有効化/無効化、更新、または再起動を行えます。

IKE ゲートウェイのセットアップ

VPN トンネルをセットアップするには、VPN ピアまたはゲートウェイが事前共有鍵またはデジタル証明書を使用して相互に認証し、安全なチャネルを確立して、両側のホスト間でトラフィックを保護するために使用される IPSec Security Association （SA）をネゴシエートします。

STEP 1 | IKE ゲートウェイを定義します。

1. **Network**（ネットワーク） > **Network Profiles**（ネットワークのプロファイル） > **IKE Gateways**（**IKE** ゲートウェイ）を選択して、ゲートウェイを **Add**（追加）し、そのゲートウェイの **Name**（名前）を入力します（**General**（全般）タブ）。
2. **Version**（バージョン）を、**IKEv1 only mode**（**IKEv1** 専用モード）、**IKEv2 only mode**（**IKEv2** 専用モード）、または **IKEv2 preferred mode**（**IKEv2** 優先モード） を選択します。ここで指定したモードで、IKE ゲートウェイがピアとのネゴシエーションを開始します。**IKEv2 preferred mode** [IKEv2 優先モード]を選択すると、リモート ピアで IKEv2 がサポートされている場合は 2 つのピアで IKEv2 が使用され、サポートされていない場合は IKEv1 が使用されます。

   Version (バージョン**)** の選択に応じて、**Advanced Options (**詳細オプション**)** タブの設定で使用可能なオプションも決定されます。

STEP 2 | トンネルのローカル エンドポイント（ゲートウェイ）を確立します。

1. **Addres Type**（アドレス タイプ）を選択します。**IPv4**または**IPv6**
2. ローカル ゲートウェイが存在するファイアウォールで物理的な発信 **Interface (**インターフェイス**)** を選択します。
3. **Local IP Address (**ローカル **IP** アドレス**)** リストから、VPN 接続がエンドポイントとして使用する IP アドレスを選択します。これは、ファイアウォール上の公的にルーティング可能な IP アドレスを持つ外部向きのインターフェイスです。

STEP 3 | トンネルの反対側のピア（ゲートウェイ）を確立します。

Peer IP Address Type（ピア **IP** アドレス タイプ）の場合、次のいずれかを選択し、ピアの対応する情報を入力します：

- **IP** — IPv4 または IPv6 アドレスのいずれかである **Peer Address** を入力するか、IPv4 または IPv6 アドレスであるアドレス オブジェクトを入力します。
- **FQDN** — FQDN 文字列または FQDN 文字列を使用するアドレス オブジェクトである **Peer Address** を入力します。FQDN または FQDN アドレス オブジェクトが複数の IP アドレスに解決される場合、ファイアウォールは、IKE ゲートウェイの Address Type (IPv4 または IPv6) に一致するアドレスのセットから、次のように優先アドレスを選択します。
  - IKE セキュリティ アソシエーション (SA) がネゴシエートされていない場合、優先アドレスは最小値を持つ IP アドレスです。
  - IKE ゲートウェイが返されたアドレスのセット内のアドレスを使用する場合、ファイアウォールはそのアドレスを (セット内の最小のアドレスであるかどうかにかかわらず) 選択します。

- IKE ゲートウェイが返されたアドレスのセットに含まれていないアドレスを使用する場合、ファイアウォールは新しいアドレスを選択し、それがセット内の最小のアドレスになります。

- **Dynamic** — ピア IP アドレスまたは FQDN 値が不明な場合、ピアがネゴシエーションを開始する際**Dynamic** を選択します。

FQDN または *FQDN* アドレス オブジェクトを使用すると、ピアが動的 *IP* アドレスの変更を受ける *(*それ以外の場合はこの *IKE* ゲートウェイ ピア アドレスを再構成する必要がある*)* 環境での問題が軽減されます。

STEP 4 | ピアの認証方法を指定します。

Authentication [認証]の方法を選択します。**Pre-Shared Key** [事前共有鍵]あるいは**Certificate** [認証]です。事前共有鍵を選択した場合は、次のステップに進みます。証明書を選択した場合は、ステップ 6 の証明書ベースの認証を設定までスキップします。

STEP 5 | 事前共有鍵を設定します。

1. **Pre-shared Key**（事前共有鍵）に、トンネル間の認証用のセキュリティ キーを入力します。**Confirm Pre-shared Key** [再入力 事前共有鍵]に値を再入力します。最大 255 文字の ASCII 文字または非 ASCII 文字を使用してください。

   辞書攻撃で解読されにくいキーを生成します。必要に応じて、事前共有鍵生成プログラムを使用します。

2. **Local Identification** [ローカル ID]で次のタイプの中から選択を行い、決定した値を入力します。**FQDN (hostname)**（**FQDN**（ホスト名））、**IP address**（**IP** アドレス）、**KEYID (binary format ID string in HEX)**（**HEX** のバイナリフォーマット **ID** 文字列）、**User FQDN (email address)**（ユーザー **FQDN**（電子メール アドレス））。ローカル ID は、ローカル ゲートウェイのフォーマットと ID を定義します。値を指定しないと、ローカル IP アドレスがローカル ID の値として使用されます。

3. **Peer Identification**（ピア **ID**）で次のタイプの中から選択を行い、決定した値を入力します。**FQDN (hostname)**（**FQDN**（ホスト名））、**IP address**（**IP** アドレス）、**KEYID (binary format ID string in HEX)**（**HEX** のバイナリフォーマット **ID** 文字列）、**User FQDN (email address)**（ユーザー **FQDN**（電子メール アドレス））。ピア ID は、ピア ゲートウェイのフォーマットと ID を定義します。値を指定しない場合は、ピア IP アドレスがピア ID 値として使用されます。

4. ステップ 7 (ゲートウェイの詳細オプションを設定) に進みます。

STEP 6 | 証明書ベースの認証を設定します。

トンネルの反対側にあるピア ゲートウェイの認証方式として **Certificate** [証明書]を選択した場合、この手順の残りのステップを実行します。

1. すでにファイアウォールにある **Local Certificate (**ローカル証明書**)** を選択するか、証明書を **Import (**インポート**)** するか、新しい証明書を **Generate (**生成**)** します。
   - 証明書を **Import (**インポート**)** する必要がある場合は、はじめに IKEv2 ゲートウェイ認証の証明書のインポート を行ってから、このタスクに戻ってください。
   - 新しい証明書を **Generate**（生成）する場合は、はじめにファイアウォールでの証明書の生成を行ってから、このタスクに戻ります。
2. (任意) **HTTP Certificate Exchange (HTTP** 証明書の交換**)** を有効化 (選択) して、ハッシュと URL (IKEv2 限定) を設定します。HTTP 証明書の交換を行う **Certificate URL** [証明書 URL]を入力します。詳細についてはハッシュおよび URL 証明書の交換を参照してください。
3. **Local Identification**（ローカル **ID**）タイプを **Distinguished Name** （**Subject**）（識別名（サブジェクト）、FQDN （ホスト名）、**IP address** （**IP** アドレス）、または **User FQDN** （**email address**）（ユーザー **FQDN** （電子メール アドレス））から選択してから、値を入力します。ローカル ID は、ローカル ゲートウェイのフォーマットと ID を定義します。
4. **Peer Identification**（ピア **ID**） タイプを **Distinguished Name** （**Subject**）（識別名（サブジェクト）、FQDN （ホスト名）、**IP address** （**IP** アドレス）、または **User FQDN**（**email address**）（ユーザー **FQDN** （電子メール アドレス））から選択してから、値を入力します。ピア ID は、ピア ゲートウェイのフォーマットと ID を定義します。
5. **Peer ID Check**（ピア **ID** チェック）で以下のいずれかのタイプを指定します。
   - **Exact**（完全） – ローカル設定とピア IKE ID ペイロードが完全に一致するピア ID のみを許可します。
   - **Wildcard**（ワイルドカード） – （*）より前のすべての文字に一致するピア ID を許可します。ワイルドカードより後の文字が一致する必要はありません。
6. （任意）ピア ID が証明書のピア ID に一致しなくても IKE SA を正常に確立できるようにするには、**Permit peer identification and certificate payload identification mismatch**（ピア **ID** と証明書ペイロード **ID** の不一致を許可する）をクリックします。
7. **Certificate Profile (**証明書プロファイル**)** を選択します。証明書プロファイルには、ピア ゲートウェイの認証方法に関する情報が含まれています。
8. （任意）鍵の使用方法を厳密に制御する場合は、**Enable strict validation of peer's extended key use**（ピアの拡張鍵使用の厳密な検証を有効にする）をクリックします。

STEP 7 | ゲートウェイの詳細オプションを設定します。

1. ファイアウォールが IKE 接続リクエストにのみ応答し、それらを開始させないように指定するには、（任意）共通オプション（**Advanced Options**（詳細オプション））で **Enable Passive Mode**（パッシブ モードを有効にする）を行います。
2. ゲートウェイ間で NAT を実行しているデバイスがあり、IKE および UDP プロトコルで UDP カプセル化が使用され、中間 NAT デバイスを通過できるようにするには、**Enable NAT Traversal**（**NAT** トラバーサルを有効にする） を使用します。
3. ステップ 1 で **IKEv1 only mode (IKEv1** 専用モード**)** を設定した場合は、IKEv1 タブで以下の設定を指定します：

   - **Exchange Mode**（交換モード）を選択します： **auto**（自動）、**aggressive**（アグレッシブ）、または **main**（メイン）。ファイアウォールが **auto (**自動**)** の交換モードを使用するように設定されている場合、**main (**メイン**)** モードと **aggressive (**アグレッシブ**)** モードの両方のネゴシエーション要求を受け入れることができますが、可能な場合は常にネゴシエーションを開始して **main (**メイン**)** モードで交換ができるようにします。

     交換モードを ***auto***（自動） に設定しない場合、各ピアがネゴシエーション要求を受け入れることができるように、両方のピアを同じ交換モードで設定する必要があります。

   - **IKE Crypto Profile (IKE** 暗号プロファイル**)** リストから既存のプロファイルを選択するか、デフォルト プロファイルのままにします。必要に応じて、 IKE 暗号プロファイルを定義することができます。
   - （証明書ベースの認証を使用していて交換モードが aggressive モードに設定されていない場合のみ）ファイアウォールが IKE フラグメンテーションで動作するようにするには、**Enable Fragmentation (**フラグメンテーションを有効にする**)** をクリックします。
   - **Dead Peer Detection**（デッド ピア検出）をクリックして **Interval**（間隔）（範囲は 2 ～ 100 秒）を入力します。**Retry (**再試行**)** で、可用性の再確認を試行するまでの遅延時間（範囲は 2 ～ 100 秒）を定義します。デッド ピア検出は、IKE フェーズ 1 通知ペイロードをピアに送信して確認を待機することで、無効または使用できない IKE ピアを識別します。

4. ステップ 1 で **IKEv2 only mode (IKEv2** 専用モード**)** あるいは **IKEv2 preferred mode (IKEv2** 優先モード**)** を設定した場合は、IKEv2 タブで：

   - **IKE Crypto Profile (IKE** 暗号プロファイル**)** を選択します。このプロファイルは、DH グループ、ハッシュ アルゴリズム、ESP 認証などの IKE フェーズ 1 オプションを設定します。IKE 暗号化プロファイルの詳細は、IKE フェーズ 1を参照してください。
   - （任意） **Strict Cookie Validation(Cookie** アクティベーションのしきい値**)** Cookie アクティベーションのしきい値と Cookie の厳密な検証を有効にします。
   - （任意）ゲートウェイからそのゲートウェイ ピアに応答を要求するメッセージ要求を送信する場合は、**Enable Liveness Check (**ライブネス チェックを有効化**)** して **Interval**（**sec**）**(**間隔（秒）**)**（デフォルトは 5）を入力します。必要に応じて、イニシエータが最大 10 回までライブネス チェックを試行できます。応答が得られない

場合、イニシエータは IKE_SA および CHILD_SA を閉じて削除します。イニシエータは、別の IKE_SA_INIT を送信して、もう一度やり直します。

STEP 8 | **OK** をクリックし、変更を **Commit (コミット)** します。

ハッシュおよび URL を使用してアクセスするピアの証明書のエクスポート

IKEv2 は、トンネルのリモート エンドのピアが証明書をエクスポートしたサーバーから証明書をフェッチする方法として、ハッシュおよび URL 証明書の交換をサポートしています。このタスクを実行して、証明書をそのサーバーにエクスポートします。**Device (デバイス)** > **Certificate Management (証明書管理)** を使用して、すでに証明書を作成済みである必要があります。

STEP 1 | **Device (デバイス)** > **Certificates (証明書)** を選択し、プラットフォームで複数の仮想システムがサポートされている場合は、**Location (場所)** で適切な仮想システムを選択します。

STEP 2 | **Device Certificates**[デバイス証明書] タブで、サーバーに **Export**[エクスポート] する証明書を選択します。

証明書の状態は失効ではなく有効である必要があります。ファイアウォールは無効な証明書のエクスポートを禁止していません。

STEP 3 | **File Format** [ファイル フォーマット]で、**Binary Encoded Certificate （DER）** [バイナリ エンコード済み証明書（DER）]を選択します。

STEP 4 | **Export private key** [秘密鍵のエクスポート]はオフのままにします。秘密鍵のエクスポートは、ハッシュおよび URL には不要です。

STEP 5 | **OK** をクリックします。

IKEv2 ゲートウェイ認証の証明書のインポート

IKEv2 ゲートウェイのピアを認証するときに、ファイアウォールにすでに存在するローカル証明書を使用せずに他の場所から証明書をインポートする場合は、このタスクを実行します。

このタスクは、**Network (ネットワーク)** > **IKE Gateways (IKE ゲートウェイ)** の順に選択してゲートウェイを追加し、**Local Certificate (ローカル証明書)** で **Import (インポート)** をクリックしていることを前提としています。

STEP 1 | 証明書をインポートします。

1. **Network (ネットワーク)** > **IKE Gateways (IKE ゲートウェイ)** の順に選択してゲートウェイを **Add (追加)** し、**General （全般）** タブの **Authentication (認証)** で **Certificate (証明書)** を選択します。**Local Certificate** [ローカル証明書]で、**Import** [インポート]をクリックします。
2. Import Certificate [証明書のインポート]ウィンドウで、インポートする証明書の **Certificate Name** [証明書名]を入力します。
3. この証明書を複数の仮想システムで共有する場合は、**Shared** [共有]を選択します。
4. **Certificate File** [証明書ファイル]で、証明書ファイルを **Browse** [参照]します。ファイル名をクリックして **Open** [開く]をクリックすると、**Certificate File** [証明書ファイル]フィールドに証明書ファイルが設定されます。

5. **File Format** [ファイル フォーマット]で、以下のいずれかを選択します。
   - **Base64 Encoded Certificate (PEM)**（**Base64** エンコード済み証明書 **(PEM)**） – 鍵ではなく、証明書が含まれます。これはクリアテキストです。
   - **Encrypted Private Key and Certificate (PKCS12)**（暗号化された秘密鍵と証明書 **(PKCS12)**） – 証明書と鍵の両方が含まれます。
6. 証明書ファイルとは別のファイル内に秘密鍵がある場合は、**Import private key** [秘密鍵のインポート]を選択します。秘密鍵は任意ですが、以下の例外があります。
   - **File Format** [ファイル フォーマット]を **PEM** に設定した場合は、秘密鍵をインポートする必要があります。**Browse** [参照]をクリックしてインポートするキー ファイルに移動し、**Key file** [キー ファイル]を入力します。
   - **Passphrase** [パスフレーズ]と **Confirm Passphrase** [パスフレーズの確認]を入力します。
7. **OK** をクリックします。

STEP 2 | 次のタスクに進みます。

証明書ベースの認証の設定ステップ。

IKEv2 のキーの有効期間または認証間隔の変更

このタスクは任意です。IKEv2 IKE SA キー再生成の有効期間のデフォルト設定は 8 時間です。IKEv2 多重認証のデフォルト設定は、再認証機能が無効になる 0 です。詳細については、SA キーの有効期間と再認証間隔を参照してください。

デフォルト値を変更するには、以下のタスクを実行します。前提条件として、IKE 暗号プロファイルがすでに存在する必要があります。

STEP 1 | IKE 暗号プロファイルの SA キーの有効期間または認証間隔を変更します。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **IKE Crypto (IKE 暗号)** の順に選択し、ローカル ゲートウェイに適用する IKE 暗号プロファイルを選択します。
2. **Key Lifetime** [キーの有効期間]で、単位（**Seconds** [秒]、**Minutes** （分）、**Hours** [時間]、または **Days** [日]）を選択して値を入力します。最小値は 3 分です。
3. **IKE Authentication Multiple** [IKE 多重認証]に値を入力します。この値は、再認証間隔を決定するために有効期間で乗算されます。

STEP 2 | 変更をコミットします。

OK、**Commit (コミット)** の順にクリックします。

IKEv2 の Cookie アクティベーションのしきい値の変更

Cookie の検証が必要になる前に、ファイアウォールに 500 ハーフオープン SA セッションのデフォルト設定とは異なるしきい値を設定する場合は、以下のタスクを実行します。Cookie 検証の詳細については、Cookie アクティベーションのしきい値と Cookie の厳密な検証を参照してください。

STEP 1 | Cookie アクティベーションのしきい値を変更します。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** を選択して VPN Session Settings (VPN セッション設定) を編集します。**Cookie Activation Threshold (Cookie** アクティベーションのしきい値**)** で、レスポンダがイニシエータから Cookie を要求する前に許可される、ハーフオープン SA の最大数を入力します（範囲は 0 ～ 65535、デフォルトは 500）。
2. **OK** をクリックします。

STEP 2 | 変更をコミットします。

OK、**Commit (コミット)** の順にクリックします。

IKEv2 トラフィック セレクタの設定

IKEv2 では、IKE ネゴシエーション中に使用されるネットワーク トラフィックのコンポーネントであるトラフィック セレクタを設定することができます。トラフィック セレクタは、トンネルをセットアップし、トンネルの通過が許可されるトラフィックを判断するために、CHILD_SA（トンネル作成）フェーズ 2 で使用されます。2 つの IKE ゲートウェイ ピアがネゴシートしてトラフィック セレクタについて合意する必要があります。合意しなかった場合、一方がアドレス範囲を絞り込んで合意に達します。1 つの IKE 接続で複数のトンネルを使用できます。たとえば、各部門に異なるトンネルを割り当ててトラフィックを分離することができます。トラフィックの分離によって、QoS などの機能も実装できます。以下の流れでトラフィック セレクタを設定します。

STEP 1 | **Network (ネットワーク)** > **IPSec Tunnels (IPSec** トンネル**)** > **Proxy IDs (プロキシ ID)** を選択します。

STEP 2 | **IPv4** または **IPv6** タブを選択します。

STEP 3 | **Add** [追加]をクリックし、**Proxy ID** [プロキシ ID]フィールドの **Name** [名前]に入力します。

STEP 4 | **Local** [ローカル]フィールドで、**Source IP Address** [送信元 IP アドレス]を入力します。

STEP 5 | **Remote** [リモート]フィールドで、**Destination IP Address** [宛先 IP アドレス]を入力します。

STEP 6 | **Protocol (プロトコル)** フィールドで、トランスポート プロトコル (**TCP** または **UDP**) を選択します。

STEP 7 | **OK** をクリックします。

暗号プロファイルの定義

暗号プロファイルは、2 つの IKE ピア間の認証や暗号化に使用される暗号と、キーのライフタイムを指定します。各再ネゴシエーション間の期間はライフタイムとして知られます。指定した時間が経過すると、ファイアウォールは新しいキーのセットを再ネゴシエートします。

VPN トンネルを経由した通信を保護するため、ファイアウォールでは、IKE フェーズ 1 とフェース 2 のネゴシエーションの完了に、それぞれ IKE と IPSec 暗号プロファイルが必要です。ファイアウォールにはデフォルトの IKE 暗号プロファイルとデフォルトの IPSec 暗号プロファイルが含まれており、すぐに使用できます。

- IKE 暗号プロファイルの定義
- IPSec 暗号プロファイルの定義

IKE 暗号プロファイルの定義

IKE 暗号プロファイルは、IKE フェーズ 1 の鍵交換プロセスに使用される暗号化および認証アルゴリズムと、キーが有効な期間を指定するキーのライフタイムをセットアップするために使用されます。プロファイルを呼び出すには、IKE ゲートウェイ設定に関連付ける必要があります。

IKE ゲートウェイの ***Peer IP Address Type*** **(**ピア ***IP***アドレス タイプ**)**が***Dynamic*** **(**ダイナミック**)** として設定され、*IKEv1*メイン モードまたは *IKEv2*が適用されている場合、同じインターフェースまたはローカル *IP*アドレスで設定されたすべての *IKE* ゲートウェイは同じ暗号プロファイルを使用する必要があります。

STEP 1 | 新しい IKE プロファイルを作成します。

1. **Network (**ネットワーク**) >** > **Network Profiles (**ネットワーク プロファイル**)** > **IKE Crypto (IKE** 暗号**)** の順に選択し、**Add (**追加**)** をクリックします。
2. 新しいプロファイルの **Name (**名前**)** を入力します。

STEP 2 | キー交換用の DH（Diffie –Hellman）グループ、認証および暗号化アルゴリズムを指定します。

対応するセクション (DH Group (DH グループ)、Authentication (認証)、および Encryption (暗号化)) で **Add (追加)** をクリックしメニューから選択します。

VPN ピアが何をサポートしているか不明確な場合は、安全性の高い順に複数のグループまたはアルゴリズムを追加します。ピアはサポートされている最も堅牢なグループまたはアルゴリズムをネゴシエートしてトンネルを確立します。

- DH Group—
  - **group21**
  - **group20**
  - **group16**
  - **group15**
  - **group19**
  - **group14**
  - **group5**
  - **group2**
  - **group1**
- Authentication—
  - **sha512**
  - **sha384**
  - **sha25**
  - **<sha1**
  - **md5**
  - **none**

  暗号化に *AES-GCM* アルゴリズムを選択した場合は、*Authentication* 設定***none***を選択しないとコミットは失敗し<。ハッシュは、選択した *DH* グループに基づいて自動的に選択されます。*DH Group 19* 以下では ***sha256*** を使用します。*DH Group 20* では ***sha384*** を使用します。
- 暗号化—
  - **aes-256-gcm** (IKEv2 が必要; DH Group は **group20** に設定する必要があります)
  - **aes-128-gcm** (IKEv2 および DH Group を **group19** に設定する必要があります)
  - **aes-256-cbc**
  - **aes-192-cbc**
  - **aes-128-cbc**
  - **3des**

ピアがサポートできる最も強力な認証アルゴリズムと暗号化アルゴリズムを選択します。認証アルゴリズムでは、*SHA-256* 以上（*SHA-384* 以上が長寿命トランザクションに適しています）を使用します。*SHA-1* または *MD5* は使用しないでください。暗号化アルゴリズムには、*AES* を使用します。*DES* と *3DES* は弱く脆弱です。*Galois / Counter Mode (AES-GCM)* を備えた *AES* は、最も強力なセキュリティを提供し、認証が組み込まれているため、***aes-256-gcm*** または ***aes-128-gcm***暗号化を選択する場合は、認証を ***none*** に設定する必要があります。

STEP 3 | キーが有効な期間と再認証間隔を指定します。

詳細については、SA キーの有効期間と再認証間隔を参照してください。

1. **Key Lifetime (**キーの有効期間**)** フィールドで、キーが有効な期間（秒、分、時間、または日）を指定します（範囲は 3 分～365 日、デフォルトは 8 時間）。キーの有効期限が切れると、ファイアウォールは新しいキーを再ネゴシエートします。有効期間は、各ネゴシエーション間の期間です。
2. **IKEv2 Authentication Multiple (IKEv2** 多重認証**)** で、認証カウントを決定するために、**Key Lifetime (**キーの有効期間**)** で乗算される値を指定します（範囲は 0 ～ 50、デフォルトは 0）。デフォルト値の 0 は、再認証機能が無効になります。

STEP 4 | IKE 暗号プロファイルをコミットします。

[OK] をクリックし、**[Commit]** をクリックします。

STEP 5 | IKE 暗号プロファイルを IKE ゲートウェイ設定に関連付けます。

ゲートウェイの詳細オプションを設定を参照してください。

IPSec 暗号プロファイルの定義

IPSec 暗号プロファイルは IKE フェーズ 2 で呼び出されます。IKE SA のキーを自動的に生成するために自動キー IKE を使用する場合にトンネル内でデータを保護する方法を指定します。

STEP 1 | 新しい IPSec プロファイルを作成します。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **IPSec Crypto (IPSec 暗号)** の順に選択し、**Add (追加)** をクリックします。
2. 新しいプロファイルの **Name (名前)** を入力します。
3. トンネルを通過するデータを保護するために適用する **[IPSec プロトコル]** を ESP と AH から選択します。

   ESP は、*AH* が認証のみを提供する接続に対して機密性と認証の両方を提供するため、*AH (認証ヘッダー)* で *ESP (Encapsulating Security* ペイロード*)* を選択することをお勧めします。
4. **[追加]** をクリックし、ESP の **[認証]** および **[暗号化]** アルゴリズム、AH の **[認証]** アルゴリズムを選択し、トンネルを経由するデータの転送を保護するために IKE ピアがキーをネゴシエートできるようにします。

   IKE ピアが何をサポートしているか不明確な場合は、以下のように安全性の高い順に複数のアルゴリズムを追加します。ピアはサポートされている最も堅牢なアルゴリズムをネゴシエートしてトンネルを確立します。

   - Encryption—**aes-256-gcm**, **aes-256-cbc**, **aes-192-cbc**, **aes-128-gcm**, **aes-128-ccm** (VM-Series firewall はこのオプションをサポートしていません), **aes-128-cbc**, **3des**.

     ベストプラクティスとして、ピアがサポートできる最も強力な認証アルゴリズムと暗号化アルゴリズムを選択します。認証アルゴリズムでは、*SHA-256* 以上（*SHA-384* 以上が長寿命トランザクションに適しています）を使用します。*SHA-1*、*MD5* 、または「なし」を使用しないでください。暗号化アルゴリズムには、*AES* を使用します。*3DES* は弱く、脆弱です。
   - Authentication [認証] — **sha512**、**sha384**、**sha256**、**sha1**、**md5**。

STEP 2 | IKE フェーズ 2 で IPSec SA に使用する DH グループを選択します。

DH Group から、使用するキーの強度を選択します: **group1**、**group2**、**group5**、**group14**、**group15**、**group16**、**group19**、**group20**、または **group21** を選択します。セキュリティを最も強化するには、数値が最も大きいグループを選択します。

IKE フェーズ 1 でファイアウォールが作成する鍵を更新しない場合は、**no-pfs** (Perfect Forward Secrecy なし) を選択します。ファイアウォールは、IPSec セキュリティ アソシエーション (SA) ネゴシエーションで現在の鍵を再利用します。

STEP 3 | キーの期間、つまり時間とトラフィックの量を指定します。

時間とトラフィック量の組み合わせを使用すると、データの安全性を確保できます。

Lifetime [ライフタイム]またはキーが有効な秒、分、時間、または日単位の期間（範囲は 3 分～ 365 日）を選択します。指定した時間が経過すると、ファイアウォールは新しいキーのセットを再ネゴシエートします。

[ライフサイズ]、つまりそれを過ぎるとキーを再ネゴシエートする必要のあるデータの量を選択します。

STEP 4 | IPSec プロファイルをコミットします。

[OK] をクリックし、**[Commit]** をクリックします。

STEP 5 | IPSec プロファイルを IPSec トンネル設定に関連付けます。

キー交換のセットアップを参照してください。

IPSec トンネルのセットアップ

IPSec トンネル設定により、データ (IP パケット) がトンネルを通過するときに、データの認証や暗号化を行うことができます。

ポリシーベースの VPN をサポートするピアと連携するようにファイアウォールを設定している場合は、プロキシ ID を定義する必要があります。ポリシーベースの VPN をサポートするデバイスは、関連するトラフィックが IPSec トンネルを通過するのを許可するために特定のセキュリティ ルール/ポリシーまたはアクセスリスト（送信元アドレス、宛先アドレス、およびポート）を使用します。これらのルールはクイック モード/IKE フェーズ 2 ネゴシエーション中に参照され、プロセスの最初または 2 番目のメッセージのプロキシ ID として交換されます。したがって、ポリシーベースの VPN ピアと連携するようにファイアウォールを設定している場合は、フェーズ 2 ネゴシエーションを成功させるために、両方のピアの設定が同じになるように Proxy-ID を定義する必要があります。ファイアウォールがルートベースの VPN をサポートしているために Proxy-ID が設定されていない場合、Proxy-ID として使用されるデフォルト値は source ip です。0.0.0.0/0、宛先 IP が0.0.0.0/0およびアプリケーションが「任意」になります。これらの値がピアと交換されると、VPN 接続のセットアップに失敗します。

STEP 1 | **Network (**ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)** を選択した後、新しいトンネル設定を **Add (**追加**)** します。

STEP 2 | **General** （全般） タブでトンネルの **Name (**名前**)** を入力します。

STEP 3 | IPSec トンネルをセットアップする**Tunnel interface (**トンネル インターフェイス**)** を選択します。

新しいトンネル インターフェイスを作成するには、以下の手順を実行します。

1. **Tunnel Interface (**トンネル インターフェイス**)** > **New Tunnel Interface (**新規トンネル インターフェイス**)** を選択します。（また、**Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** > **Tunnel (**トンネル**)** を選択して**Add (**追加**)** をクリックすることもできます）
2. **Interface Name**（インターフェイス名）フィールドで、**.2**などの数値のサフィックスを指定します。
3. **Config (**設定**)** タブで、**Security Zone (**セキュリティ ゾーン**)** リストを選択して次のようにゾーンを定義します。

信頼ゾーンをトンネルの終端点として使用する—ゾーンを選択します。トンネル インターフェイスをパケットがファイアウォールに入る外向きのインターフェイスとして同じゾーン

（および仮想ルーター）に関連付けると、ゾーン間ルーティングを作成する必要性が低くなります。

または：

VPN トンネルの終端のゾーンを別に作成する (推奨) —**New Zone (新規ゾーン)** を選択し、その新しいゾーンの **Name (名前)** を定義 (vpn-corp など) して **OK** をクリックします。

1. **Virtual Router (仮想ルータ)** の場合、**default (デフォルト)** を選択します。
2. (任意) IPv4 アドレスをトンネル インターフェイスに割り当てるには、**IPv4** タブを選択し、IPv4 アドレスおよびネットワーク マスクを **Add (追加)** します (10.31.32.1/32 など)。
3. **OK** をクリックします。

STEP 4 | （任意）トンネル インターフェイスで IPv6 を有効化します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Tunnel (トンネル)** > **IPv6** 上でIPv6 タブを選択します。
2. **Enable IPv6 on the interface (インターフェイスでの IPv6 の有効化)** を選択します。

   このオプションを使用すると、IPv6 トラフィックを IPv4 IPSec トンネル経由でルーティングでき、IPv6 ネットワーク間の機密性が確保されます。IPv6 トラフィックは、IPv4 でカプセル化された後で ESP でカプセル化されます。IPv6 トラフィックをトンネルにルーティングするには、トンネルへのスタティック ルートを使用するか、OSPFv3 を使用するか、ポリシー ベース フォワーディング (PBF) ルールを使用します。
3. 64 ビット拡張一意 **[インターフェイス ID]** を 16 進数形式で入力します（たとえば、00:26:08:FF:FE:DE:4E:29）。デフォルトでは、物理インターフェイスの MAC アドレスから生成された EUI-64 がファイアウォールで使用されます。
4. トンネル インターフェイスに IPv6 **Address (アドレス)** を割り当てるには、IPv6 アドレスおよびプレフィックス長を **Add (追加)** します（2001:400:f00::1/64 など）。Prefix（プレフィックス）が選択されていない場合、インターフェイスに割り当てる IPv6 アドレスをアドレス テキスト ボックスですべて指定します。

   1. インターフェイス ID をアドレスのホスト部分に使用するインターフェイスに IPv6 アドレスを割り当てるには、**[ホスト部分にインターフェイス ID を使用]** を選択します。
   2. 最も近いノードを経由するルーティングを含めるには **[エニーキャスト]** を選択します。

STEP 5 | キー交換をセットアップします。

General (一般) タブで、次のいずれかのタイプのキー交換を設定します。

自動キー交換のセットアップ

1. IKE ゲートウェイを選択します。IKE ゲートウェイをセットアップするには、IKE ゲートウェイのセットアップを参照してください。
2. （任意）デフォルトの IPSec 暗号プロファイルを選択します。新しい IPSec プロファイルを作成する方法については、IPSec 暗号プロファイルの定義を参照してください。

手動キー交換のセットアップ

1. ローカル ファイアウォールの **Local SPI (ローカル SPI)** を指定します。SPI とは、IPSec トラフィック フロー間の差をアシストするためにトンネルする IPSec のヘッダーに追加される 32 ビット 16 進数です。VPN トンネルを確立するために必要な SA を作成するために使用されます。
2. トンネル エンドポイントとなる **Interface** [インターフェイス]を選択し、任意でトンネルのエンドポイントであるローカル インターフェイスの IP アドレスを選択します。
3. 使用するプロトコルを **[AH]** または **[ESP]** から選択します。
4. AH については、**Authentication (認証)** 方式を選択し、**Key (鍵)** に続いて **Confirm Key (鍵の確認)** を入力します。
5. ESP については、**Authentication (認証)** 方式を選択し、**Key (鍵)** に続いて **Confirm Key (鍵の確認)** を入力します。次に、**Encryption** [暗号化]方式を選択して必要に応じて **Key** [キー]に続いて **Confirm Key** [再入力 キー]を入力します。
6. リモート ピアの **Remote SPI (リモート SPI)** を指定します。
7. **[リモート アドレス]**、つまりリモート ピアの IP アドレスを入力します。

STEP 6 | リプレイ攻撃に対して保護します。

リプレイ防止は IPSec のサブプロトコルであり、インターネット技術標準化委員会 (IETF) コメントの要求 (RFC) 6479 の一部です。アンチリプレイ プロトコルは、ハッカーが送信元から宛先に移動するパケットを挿入または変更するのを防ぐために使用され、ネットワーク内の 2 つのノード間の安全な接続を確立するために、単方向セキュリティ アソシエーションを使用します。

セキュリティで保護された接続が確立されると、アンチリプレイ プロトコルはパケット シーケンス番号を使用してリプレイ攻撃を打ち破ります。送信元がメッセージを送信すると、パケットにシーケンス番号が追加されます。シーケンス番号は 0 から始まり、後続のパケットごとに 1 ずつ増分されます。宛先は、 スライディング ウィンドウ 形式の番号のシーケンスを保持し、検証された受信パケットのシーケンス番号のレコードを保持し、スライディング ウィンドウの最下位 (古すぎるパケット) または既にスライディング ウィンドウに表示されているパケット (複製または再生パケット) よりも低いシーケンス番号を持つすべてのパケットを拒否します。受け入れられたパケットは、検証後にスライディング ウィンドウを更新し、ウィンドウの中で最も低いシーケンス番号が既に満杯の場合は、その番号を置き換えます。

1. 一般タブで、**Show Advanced Options (詳細オプションの表示)** を選択し、**Enable Replay Protection (リプレイ プロテクションを有効にする)** を選択してリプレイ攻撃を検出して無力化します。

2. 使用する アンチリプレイウィンドウ を選択します。64、128、256、512、1024、2048、または4096のアンチリプレイウィンドウサイズを選択できます。デフォルトは 1024 です。

STEP 7 | （任意）IP パケットの優先順位または処置について Type of Service ヘッダーを保持します。

詳細オプションの表示セクションで、**Copy TOS Header**（**TOS** ヘッダーのコピー） を選択します。これにより、元の TOS （Type of Service）情報を保持するため、カプセル化されたパケットの内部 IP ヘッダーから外部 IP ヘッダーに TOS ヘッダーをコピーします。

トンネル内に複数のセッション（それぞれ*TOS*値が異なる）ある場合、*TOS*をコピーすると*IPSec*パケットが誤った順序で届くおそれがあります。

STEP 8 | (任意) **Add GRE Encapsulation (GRE Encapsulation** の追加**)** を選択して、GRE over IPSec を有効にします。

IPSec がトラフィックを暗号化する前に、リモートエンドポイントでトラフィックを GRE トンネル内にカプセル化する必要がある場合は、GRE カプセル化を追加します。例えば、一部の実装では、IPSec が暗号化する前にマルチキャストトラフィックをカプセル化する必要があります。IPSec でカプセル化された GRE パケットが、カプセル化された IPSec トンネルと同じ送信元 IP アドレスと宛先 IP アドレスを持つ場合は、GRE カプセル化を追加します。

STEP 9 | トンネル モニタリングを有効化します。

モニタニングする場合は、トンネル インターフェイスに *IP* アドレスを割り当てる必要があります。

デバイス管理者にトンネルの障害についてアラートを送信し、別のトンネル インターフェイスへの自動フェイルオーバーを実行するには、このオプションを選択します。

1. **Tunnel Monitor (**トンネル モニター**)**を選択します。
2. トンネルが正常に動作しているかどうかを判別するために、トンネルの反対側の **[**宛先 **IP]** アドレスを指定します。
3. **Profile (**プロファイル**)** を選択して、トンネル障害時のアクションを決定します。新しいプロファイルを作成する方法については、トンネル モニタリング プロファイルの定義を参照してください。

STEP 10 | VPN ピアを識別するためのプロキシ ID を作成します。

VPN ピアがポリシーベースの VPN を使用する場合のみ、このステップが必要です。

1. **Network (ネットワーク)** > **IPSec Tunnels (IPSec トンネル)** の順に選択して **Add (追加)** をクリックします。
2. **Proxy IDs** （プロキシ ID）タブを選択します。
3. **IPv4** または **IPv6** タブを選択します。
4. **Add** [追加]をクリックし、**Proxy ID** [プロキシ ID]の名前を入力します。
5. VPN ゲートウェイの **Local** [ローカル] IP アドレスまたはサブネットを入力します。
6. VPN ゲートウェイの **Remote** [リモート]アドレスを入力します。
7. **Protocol (プロトコル)** を選択します：
   - **Number**（番号） – プロトコル番号 (サードパーティ デバイスとの相互運用性を実現するために使用) を指定します。
   - **Any** – TCP や UDP トラフィックを許可します。
   - **TCP** – ローカル ポートとリモート ポートの番号を指定します。
   - **UDP** – ローカル ポートとリモート ポートの番号を指定します。
8. **OK** をクリックします。

STEP 11 | 変更をコミットします。

OK、**Commit (コミット)** の順にクリックします。

トンネル モニタリングのセットアップ

VPN サービスが中断されないようにするために、ファイアウォールでトンネル モニタリング機能と一緒にデッド ピア検出機能を使用できます。トンネルの状態をモニタリングすることもできます。これらのモニタリング タスクについては、以下のセクションで説明します。

- トンネル モニタリング プロファイルの定義
- トンネルの状態の表示

トンネル モニタリング プロファイルの定義

トンネル モニタリング プロファイルにより、VPN ピア間の接続を確認できます。トンネル インターフェイスが指定した間隔で宛先 IP アドレスに ping を送信するように設定し、トンネル間の通信が切断された場合のアクションを指定できます。

STEP 1 | **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **Monitor (監視)** を選択します。デフォルトのトンネル モニタリング プロファイルが使用できます。

STEP 2 | [追加] をクリックし、プロファイルの [名前] を入力します。

STEP 3 | 宛先 IP アドレスに到達できない場合に実行する **Action (**アクション**)** を選択します。

- 回復を待機 – ファイアウォールはトンネルが回復するのを待機します。ファイアウォールでは、トンネルがまだアクティブであるかのようにして、そのトンネル インターフェイスをルート決定で使用し続けます。
- フェイル オーバー – バックアップ パスが使用できる場合、強制的にトラフィックをバックアップ パスに誘導します。ファイアウォールはトンネル インターフェイスを無効化し、それによってそのインターフェイスを使用するルーティング テーブルのルートが無効になります。

いずれの場合でも、ファイアウォールは新しい IPSec キーをネゴシエートすることで回復を早めようとします。

STEP 4 | 指定したアクションをトリガーする**Interval (sec) (**間隔（秒）**)** と **Threshold (**しきい値**)** を指定します。

- **Threshold (**しきい値**)** は、指定したアクションがファイアウォールによって実行されまでに待機するハートビートの数（範囲は 2～100、デフォルトは 5）を指定します。
- **Interval (sec) (**間隔（秒）**)** は、ハートビート間隔（範囲は2～ 10、デフォルトは3）を指定します。

STEP 5 | モニタリング プロファイルを IPsec トンネル設定に関連付けます。トンネル モニタリングの有効化を参照してください。

トンネルの状態の表示

トンネルの状態から、有効な IKE フェーズ 1 およびフェーズ 2 SA が確立されているかどうか、トンネル インターフェイスが起動していてトラフィックを通過させることができるかどうかが分かります。

トンネル インターフェイスは論理インターフェイスであるため、物理リンクの状態を示すことはできません。したがって、トンネル モニタリングを有効にして、トンネル インターフェイスで IP アドレスへの接続を確認し、パスが使用できるかどうかを判断できるようにする必要があります。IP アドレスに到達できない場合、ファイアウォールはトンネルが回復するのを待機するか、フェイルオーバーします。フェイルオーバーが行われると、既存のトンネルはダウンして、ルーティング変更がトリガーされ、新しいトンネルがセットアップされてトラフィックが転送されます。

STEP 1 | **Network (**ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)**の順に選択します。

STEP 2 | トンネルの **[**状態**]** を確認します。

- 緑は、有効な IPSec SA トンネルがあることを表します。
- 赤は、IPSec SA が使用できないか、有効期限が切れていることを表します。

STEP 3 | IKE ゲートウェイの **[**状態**]** を確認します。

- 緑は、有効な IKE フェーズ 1 SA があることを表します。
- 赤は、IKE フェーズ 1 SA が使用できないか、有効期限が切れていることを表します。

STEP 4 | **Tunnel Interface Status**（トンネル インターフェイスの状態）を確認します。

- 緑は、トンネル インターフェイスが起動していることを表します。
- 赤は、トンネル インターフェイスがダウンしている（トンネル モニタリングが有効になっていて状態がダウンであるため）ことを表します。

まだ稼働していない VPN トンネルのトラブルシューティングを行うには、VPN エラー メッセージの解釈を参照してください。

IKE ゲートウェイまたは IPSec トンネルの有効化/無効化、更新、または再起動

IKE ゲートウェイまたは VPN トンネルを有効化、無効化、更新、または再起動できます。

- IKE ゲートウェイまたは IPSec トンネルの有効化または無効化
- 更新および再起動の挙動
- IKE ゲートウェイまたは IPSec トンネルの更新または再起動

IKE ゲートウェイまたは IPSec トンネルの有効化または無効化

IKE ゲートウェイあるいは IPSec トンネルを有効化/無効化してトラブルシューティングを行いやすくします。

IKE ゲートウェイを有効または無効にします。

1. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IKE Gateways (IKE** ゲートウェイ**)** の順に選択し、有効または無効にするゲートウェイを選択します。
2. 画面の下部で **Enable** [有効化]または **Disable** [無効化]をクリックします。

IPSec トンネルを有効または無効にします。

1. **Network (**ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)** の順に選択し、有効または無効にするトンネルを選択します。
2. 画面の下部で **Enable** [有効化]または **Disable** [無効化]をクリックします。

更新および再起動の挙動

IKE ゲートウェイまたは IPSec トンネルの更新、または再起動を行えます。IKE ゲートウェイと IPSec トンネルの更新および再起動の動作は以下のようになります。

フェーズ	**Refresh**（更新）	再起動
IKE ゲートウェイ（IKE フェーズ 1）	選択した IKE ゲートウェイの画面上の統計を更新します。	選択した IKE ゲートウェイを再起動します。 **IKEv2**：関連付けられた子 IPSec Security Associations （SA）も再起動されます。

フェーズ	Refresh（更新）	再起動
	CLI で 2 番目の **show** コマンド（最初の **show** コマンドの後）を発行することと同じです。	**IKEv1**:関連付けられた IPSec SA は再起動されません。 再起動は既存のすべてのセッションに影響します。 CLI で **clear**、**test**、**show** コマンドを連続して発行することと同じです。
IPSec トンネル（IKE フェーズ 2）	選択した IPSec トンネルの画面上の統計を更新します。 CLI で 2 番目の **show** コマンド（最初の **show** コマンドの後）を発行することと同じです。	IPSec トンネルを再起動します。 再起動は既存のすべてのセッションに影響します。 CLI で **clear**、**test**、**show** コマンドを連続して発行することと同じです。

IKE ゲートウェイまたは IPSec トンネルの更新または再起動

IKE ゲートウェイを再起動した結果は、それが IKEv1 か IKEv2 かによって異なりますので、ご注意ください。IKE ゲートウェイ（IKEv1 および IKEv2）および IPSec トンネルの更新および再起動時の挙動を参照してください。

IKE ゲートウェイを更新または再起動します。

1. **Network (ネットワーク)** > **IPSec Tunnels (IPSec トンネル)** の順に選択し、更新または再起動するゲートウェイのトンネルを選択します。
2. そのトンネルの行の Status [状態]列で、**IKE Info** [IKE 情報]をクリックします。
3. IKE Info （IKE 情報）画面の下部で、以下のいずれかのアクションをクリックします。
   - **Refresh** [更新] — 画面上の統計を更新します。
   - **Restart** [再起動] — SA をクリアします。これにより、IKE ネゴシエーションをやり直してトンネルが再作成されるまでトラフィックはドロップされます。

IPSec トンネルを更新または再起動します。

トンネル モニターを使用したトンネル状態のモニタリング、または外部ネットワーク モニターを使用した IPSec トンネル経由のネットワーク接続のモニタリングを行うときに、トンネルを更新するか再起動するかの判断が必要な場合があります。

1. **Network (ネットワーク)** > **IPSec Tunnels (IPSec トンネル)** の順に選択し、更新または再起動するトンネルを選択します。
2. そのトンネルの行の Status [状態]列で、**Tunnel Info** [トンネル情報]をクリックします。
3. Tunnel Info （トンネル情報）画面の下部で、以下のいずれかのアクションをクリックします。
   - **Refresh** [更新] — 画面上の統計を更新します。
   - **Restart** [再起動] — SA をクリアします。これにより、IKE ネゴシエーションをやり直してトンネルが再作成されるまでトラフィックはドロップされます。

VPN 接続のテスト

このタスクを実行して VPN 接続をテストします。

STEP 1 | トンネルを経由してホストに ping 送信するか、以下の CLI コマンドを使用して IKE フェーズ 1 を開始します。

```
test vpn ike-sa gateway <gateway_name>
```

STEP 2 | 以下のコマンドを入力して IKE フェーズ 1 がセットアップされているかどうかをテストします。

```
show vpn ike-sa gateway <gateway_name>
```

出力で、Security Association が表示されているかどうかを確認します。表示されていない場合、システム ログ メッセージを確認して失敗の理由を見直します。

STEP 3 | トンネルを経由してホストに ping 送信するか、以下の CLI コマンドを使用して IKE フェーズ 2 を開始します。

```
test vpn ipsec-sa tunnel <tunnel_name>
```

STEP 4 | 以下のコマンドを入力して IKE フェーズ 2 がセットアップされているかどうかをテストします。

```
show vpn ipsec-sa tunnel <tunnel_name>
```

出力で、Security Association が表示されているかどうかを確認します。表示されていない場合、システム ログ メッセージを確認して失敗の理由を見直します。

STEP 5 | VPN トラフィック フロー情報を表示するには、以下のコマンドを使用します。

```
show vpn flow total tunnels configured:              1 filter - type
 IPSec, state any total IPSec tunnel configured:       1 total
 IPSec tunnel shown:                1 name                      id
      state      local-ip       peer-ip       tunnel-i/f
 ------------------------------------------------------------------------------
 vpn-to-siteB       5       active
    100.1.1.1     200.1.1.1     tunnel.41
```

VPN エラー メッセージの解釈

以下の表に、システム ログに記録される一般的な VPN エラー メッセージの一部を示します。

表 **6 : VPN** に問題がある場合の **Syslog** エラー メッセージ

エラーの内容	対処法
IKE フェーズ 1 ネゴシエーションは、イニシエーター、メイン・モードとして失敗します。失敗した SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9:0000000000000000 タイムアウトのため。 もしくは IKE フェーズ 1 ネゴシエーションが失敗しました。ピア IP x.x.x.x に対する IKE フェーズ 1 要求の構成が見つかりませんでした[1929]	• IKE ゲートウェイ設定で各 VPN ピアのパブリック IP アドレスが正しいことを確認します。 • IP アドレスに ping を送信可能であり、接続の失敗の原因がルーティングの問題ではないことを確認します。
Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x[500] to y.y.y.y[500], ignored... もしくは IKE フェーズ 1 ネゴシエーションが失敗しました。ピアの SA ペイロードを処理できません。	IKE 暗号プロファイル設定で、両側のプロポーザルに共通の暗号化、認証、および DH グループ プロポーザルがあることを確認します。
pfs グループが一致しない:my:2ピア:0 もしくは SA ペイロードの処理中に IKE フェーズ 2 ネゴシエーションが失敗しました。ピアの SA ペイロードに適切な提案が見つかりません。	IPSec 暗号プロファイル設定で、以下を確認します。 • pfs が両方の VPN ピアで有効または無効のいずれかであること • 各ピアによって提案される DH グループに少なくとも 1 つ共通の DH グループがあること

エラーの内容	対処法
Proxy ID の処理中に IKE フェーズ 2 ネゴシエーションが失敗しました。受信したローカル ID x.x.x.x/x タイプ IPv4 アドレス プロトコル 0 ポート 0、リモート ID y.y.y.y/y タイプ IPv4 アドレス プロトコル 0 ポート 0 を受信しました。	一方の VPN ピアがポリシーベースの VPN を使用しています。Palo Alto Networks ファイアウォールでプロキシ ID を設定する必要があります。VPN ピアを識別するためのプロキシ ID の作成を参照してください。

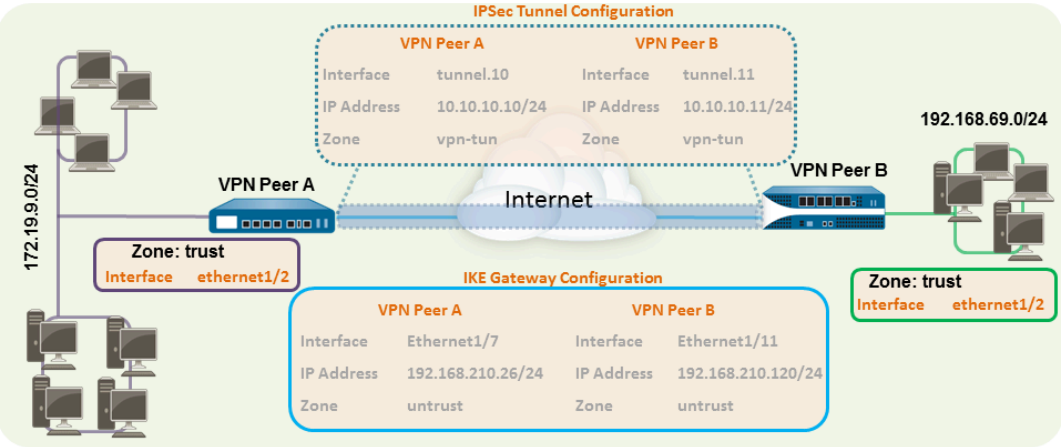
サイト間 VPN のクイック設定

以下のセクションでは、一般的な VPN デプロイメントのための手順を説明します。

- スタティック ルーティングを使用したサイト間 VPN
- OSPF を使用したサイト間 VPN
- スタティック ルーティングおよびダイナミック ルーティングを使用したサイト間 VPN

スタティック ルーティングを使用したサイト間 VPN

以下の例は、スタティック ルートを使用する 2 つのサイト間の VPN 接続を示しています。ダイナミック ルーティングを使用しない場合、VPN ピア A および VPN ピア B のトンネル インターフェイスに IP アドレスは必要ありません。これは、ファイアウォールが、サイト間のトラフィックのルーティングのために自動的にトンネル インターフェイスをネクスト ホップとして使用するためです。ただし、トンネル モニタリングを有効化するために、スタティック IP アドレスが各トンネル インターフェイスに割り当てられています。



STEP 1 | レイヤー 3 インターフェイスを設定します。

このインターフェイスが IKE フェーズ 1 トンネルに使用されます。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** の順に選択し、VPN について設定するインターフェイスを選択します。
2. **Interface Type (インターフェイス タイプ)** で **Layer3 (レイヤー 3)** を選択します。
3. **Config (設定)** タブでインターフェイスが属する **Security Zone (セキュリティ ゾーン)** を選択します。
   - インターフェイスは、信頼されるネットワークの外部のゾーンからアクセスできる必要があります。VPN トラフィックを可視化して制御するために、専用の VPN ゾーンを作成することを検討してください。
   - まだゾーンを作成していない場合は、**Security Zone (セキュリティ ゾーン)** から **New Zone (新規ゾーン)** を選択し、新規ゾーンの **Name (名前)** を定義してから **OK** をクリックします。
4. 使用する **Virtual Router (仮想ルーター)** を選択します。
5. IP アドレスをインターフェイスに割り当てるには、**IPv4** タブを選択してから IP セクションで **Add**（追加）をクリックし、インターフェイスに割り当てる IP アドレスとネットマスク（例: 192.168.210.26/24）を入力します。
6. インターフェイス設定を保存するには、**OK** をクリックします。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Interface(インターフェイス)**—ethernet1/7
   - セキュリティ ゾーン — Untrust
   - 仮想ルーター — デフォルト
   - **IPv4** — 192.168.210.26/24

   VPN ピア B の設定は以下のようになります。

   - **Interface(インターフェイス)**—ethernet1/11
   - セキュリティ ゾーン — Untrust
   - 仮想ルーター — デフォルト
   - **IPv4** — 192.168.210.120/24

STEP 2 | トンネル インターフェイスを作成し、仮想ルーターおよびセキュリティ ゾーンに関連付けます。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Tunnel (トンネル)** の順に選択し、**Add(追加)** をクリックします。
2. **Interface Name**（インターフェイス名）フィールドで、**.1**などの数値のサフィックスを指定します。
3. **Config (設定)** タブで、**Security Zone (セキュリティ ゾーン)** を展開して以下のようにゾーンを定義します。
   - トンネルの終端点として信頼されたゾーンを使用するには、そのゾーンを選択します。
   - （推奨）VPN トンネルの終端のゾーンを別に作成するには、**New Zone**（新規ゾーン）をクリックします。[ゾーン] ダイアログの **[名前]** で「*vpn-tun*」などの名前を付けて新しいゾーンを定義し、**[OK]** をクリックします。
4. **Virtual Router**[仮想ルーター] を選択します。
5. （任意）トンネル インターフェイスに IP アドレスを割り当て、**IPv4** タブまたは **IPv6** タブを選択してから IP セクションで **Add** [追加]をクリックし、インターフェイスに割り当てる IP アドレスとネットマスクを入力します。

   スタティック ルートでは、トンネル インターフェイスに IP アドレスは必要ありません。指定したサブネット/IP アドレスを宛先とするトラフィックでは、トンネル インターフェイスが自動的にネクスト ホップになります。トンネル モニタリングを有効化する場合、IP アドレスの追加を検討してください。
6. インターフェイス設定を保存するには、**OK** をクリックします。

   この例では、VPN ピア A の設定は以下のようになります。
   - インターフェイス – tunnel.10
   - セキュリティ ゾーン – vpn_tun
   - 仮想ルーター – デフォルト
   - **IPv4** – 172.19.9.2/24

   VPN ピア B の設定は以下のようになります。
   - インターフェイス – tunnel.11
   - セキュリティ ゾーン – vpn_tun
   - 仮想ルーター – デフォルト
   - **IPv4** – 192.168.69.2/24

STEP 3 | 仮想ルーターで宛先サブネットへのスタティック ルートを設定します。

1. **Network (**ネットワーク**)** > **Virtual Router (**仮想ルーター**)** の順に選択し、前のステップで定義したルーターをクリックします。
2. **[**スタティック ルート**]** を選択し、追加 をクリックして、トンネルの反対側にあるサブネットにアクセスする新しいルートを入力します。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Destination**（宛先） — 192.168.69.0/24
   - インターフェイス — tunnel.10

   VPN ピア B の設定は以下のようになります。

   - 宛先 — 172.19.9.0/24
   - インターフェイス — tunnel.11

STEP 4 | 暗号プロファイル（フェーズ 1 では IKE 暗号プロファイル、フェーズ 2 では IPSec 暗号プロファイル）をセットアップします。

両方のピアでこのタスクを実行し、必ず同じ値を設定します。

1. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IKE Crypto (IKE** 暗号**)** を選択します。この例では、デフォルトのプロファイルを使用します。
2. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IPSec Crypto (IPSec** 暗号**)** を選択します。この例では、デフォルトのプロファイルを使用します。

STEP 5 | IKE ゲートウェイをセットアップします。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **IKE Gateway (IKE ゲートウェイ)** を選択します。
2. **Add**（追加） をクリックして、**General**（全般） タブでオプションを設定します。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Interface(インターフェイス)**—ethernet1/7
   - ローカル **IP** アドレス – 192.168.210.26/24
   - ピア **IP** タイプ/アドレス – スタティック/192.168.210.120
   - 事前共有鍵 – 値を入力
   - ローカル **ID** – なし。ローカル ID 値としてローカル IP アドレスが使用されます。
   - VPN ピア B の設定は以下のようになります。
   - **Interface(インターフェイス)**—ethernet1/11
   - ローカル **IP** アドレス – 192.168.210.120/24
   - ピア **IP** タイプ/アドレス – スタティック/192.168.210.26
   - 事前共有鍵 – ピア A と同じ値を入力
   - ローカル **ID** – なし
3. **[詳細フェーズ 1 のオプション]** を選択し、IKE フェーズ 1　で使用するために以前に作成した IKE 暗号プロファイルを選択します。

STEP 6 | IPSec トンネルをセットアップします。

1. **Network (ネットワーク)** > **IPSec Tunnels (IPSec トンネル)**の順に選択します。
2. **Add**（追加） をクリックして、**General**（全般） タブでオプションを設定します。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Tunnel Interface**(トンネル インターフェイス)—tunnel.10
   - タイプ – 自動キー
   - **IKE** ゲートウェイ – 上で定義した IKE ゲートウェイを選択します。
   - **IPSec Crypto Profile**—ステップ 4 で定義した IPSec Crypto プロファイルを選択して下さい。

   VPN ピア B の設定は以下のようになります。

   - **Tunnel Interface**(トンネル インターフェイス)—tunnel.11
   - タイプ – 自動キー
   - **IKE** ゲートウェイ – 上で定義した IKE ゲートウェイを選択します。
   - **IPSec Crypto Profile** - 手順 4 で定義した IPSec Crypto を選択します。
3. （任意）**Show Advanced Options**（詳細オプションの表示）をオンにし、**Tunnel Monitor**（トンネル監視）をオンにして、接続を確認するために ping を送信する宛先

IP アドレスを指定します。一般に、VPN ピアのトンネル インターフェイス IP アドレスが使用されます。

4. （任意）接続の確立に失敗した場合のアクションを定義する方法については、トンネル モニタリング プロファイルの定義を参照してください。

STEP 7 | トラフィックをサイト（サブネット）間で許可するためのポリシーを作成します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. 指定した送信元および宛先 IP アドレスから発信されるトラフィックについて、トラフィックを Uuntrust ゾーンと vpn-tun ゾーン間および vpn-tun ゾーンと Untrust ゾーン間で許可するためのルールを作成します。

STEP 8 | 保留中の設定の変更をすべてコミットします。

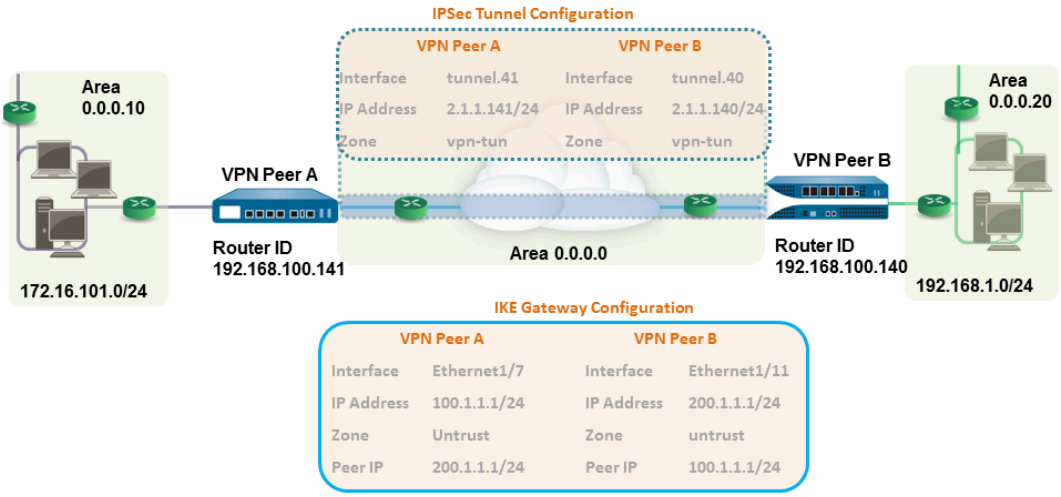
Commit（コミット）をクリックします。

STEP 9 | 「VPN 接続のテスト」を行います。

トンネルの状態の表示も参照してください。

OSPF を使用したサイト間 VPN

この例では、各サイトはトラフィックのダイナミック ルーティングに OSPF を使用します。各 VPN ピアのトンネル IP アドレスは静的に割り当てられ、2 つのサイト間でトラフィックをルーティングするためのネクスト ホップとして機能します。



STEP 1 | 各ファイアウォールでレイヤー 3 インターフェイスを設定します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** の順に選択し、VPN について設定するインターフェイスを選択します。
2. **Interface Type (インターフェイス タイプ)** リストから **Layer3 (レイヤー 3)** を選択します。
3. **Config (設定)** タブでインターフェイスが属する **Security Zone (セキュリティ ゾーン)** を選択します。
   - インターフェイスは、信頼されるネットワークの外部のゾーンからアクセスできる必要があります。VPN トラフィックを可視化して制御するために、専用の VPN ゾーンを作成することを検討してください。
   - まだゾーンを作成していない場合は、**Security Zone (セキュリティ ゾーン)** リストから **New Zone (新規ゾーン)** を選択し、新規ゾーンの **Name (名前)** を定義してから **OK** をクリックします。
4. 使用する **Virtual Router (仮想ルーター)** を選択します。
5. IP アドレスをインターフェイスに割り当てるには、**IPv4** タブを選択してから IP セクションで **Add**（追加）をクリックし、インターフェイスに割り当てる IP アドレスとネットマスク（例: 192.168.210.26/24）を入力します。
6. インターフェイス設定を保存するには、**OK** をクリックします。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Interface(インターフェイス)**—ethernet1/7
   - セキュリティ ゾーン — Untrust
   - 仮想ルーター — デフォルト
   - **IPv4** — 100.1.1.1/24

   VPN ピア B の設定は以下のようになります。

   - **Interface(インターフェイス)**—ethernet1/11
   - セキュリティ ゾーン — Untrust
   - 仮想ルーター — デフォルト
   - **IPv4** — 200.1.1.1/24

STEP 2 | トンネル インターフェイスを作成し、仮想ルーターおよびセキュリティ ゾーンに関連付けます。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Tunnel (トンネル)** の順に選択し、**Add(追加)** をクリックします。
2. **Interface Name (インターフェイス名)** フィールドで、**.11** などの数値のサフィックスを指定します。
3. **Config (設定)** タブで、**Security Zone (セキュリティ ゾーン)** を展開して以下のようにゾーンを定義します。
   - トンネルの終端点として信頼されたゾーンを使用するには、そのゾーンを選択します。
   - （推奨）VPN トンネルの終端のゾーンを別に作成するには、**New Zone**（新規ゾーン）をクリックします。Zone (ゾーン) ダイアログの **Name (名前)** で「vpn-tun」などの名前を付けて新しいゾーンを定義し、**OK** をクリックします。
4. **Virtual Router**[仮想ルーター] を選択します。
5. IP アドレスをトンネル インターフェイスに割り当て、**[IPv4]** または **[IPv6]** タブを選択します。[IP] セクションで **[追加]** をクリックし、インターフェイスに割り当てる IP アドレスとネットワーク マスク/プレフィックス（例: 172.19.9.2/24）を入力します。

   この IP アドレスは、トンネルにトラフィックをルーティングするためにネクスト ホップ IP アドレスとして使用され、トンネルの状態をモニタリングするために使用することもできます。
6. インターフェイス設定を保存するには、**OK** をクリックします。

   この例では、VPN ピア A の設定は以下のようになります。
   - **Interface**[インターフェイス] – tunnel.41
   - セキュリティ ゾーン – vpn_tun
   - 仮想ルーター – デフォルト
   - **IPv4** – 2.1.1.141/24

   VPN ピア B の設定は以下のようになります。
   - **Interface**[インターフェイス] – tunnel.40
   - セキュリティ ゾーン – vpn_tun
   - 仮想ルーター – デフォルト
   - **IPv4** – 2.1.1.140/24

STEP 3 | 暗号プロファイル（フェーズ 1 では IKE 暗号プロファイル、フェーズ 2 では IPSec 暗号プロファイル）をセットアップします。

両方のピアでこのタスクを実行し、必ず同じ値を設定します。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **IKE Crypto (IKE 暗号)** を選択します。この例では、デフォルトのプロファイルを使用します。
2. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **IPSec Crypto (IPSec 暗号)** を選択します。この例では、デフォルトのプロファイルを使用します。

STEP 4 | 仮想ルーターで OSPF 設定をセットアップし、OSPF エリアをファイアウォール上の適切なインターフェイスに関連付けます。

ファイアウォールで使用可能な OSPF オプションの詳細は、「OSPF の設定」を参照してください。

ルーティング情報を交換する必要がある OSPF ルートが 2 つ以上ある場合、リンク タイプとして Broadcast （ブロードキャスト）を使用します。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、デフォルトのルーターを選択するか新しいルーターを追加します。
2. **OSPF**（IPv4 の場合）または **OSPFv3** （IPv6 の場合）を選択し、**Enable**（有効）をオンにします。
3. この例では、VPN ピア A の OSPF 設定は以下のようになります。
   - ルーター**ID**：192.168.100.141
   - エリア **ID**：0.0.0.0 – リンク タイプ「p2p」で、インターフェイス tunnel.1 に割り当てられている
   - エリア **ID**：インターフェイス Ethernet1/1およびリンク タイプに0.0.0.10 が割り当てられているブロードキャスト

   VPN ピア B の OSPF 設定は以下のようになります。
   - ルーター**ID**：192.168.100.140
   - エリア **ID**：0.0.0.0 – リンク タイプ「p2p」で、インターフェイス tunnel.1 に割り当てられている
   - エリア **ID**：インターフェイス Ethernet1/15およびリンク タイプに0.0.0.20 が割り当てられているブロードキャスト

STEP 5 | IKE ゲートウェイをセットアップします。

この例では、両方の VPN ピアについてスタティック IP アドレスを使用します。一般に、企業オフィスでは静的に設定された IP アドレスを使用し、支社側をダイナミック IP アドレス

にできます。ダイナミック IP アドレスは、VPN などの安定したサービスの設定には適しません。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **IKE Gateway (IKE ゲートウェイ)** を選択します。
2. **Add**（追加） をクリックして、**General**（全般） タブでオプションを設定します。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Interface(インターフェイス)**—ethernet1/7
   - ローカル **IP** アドレス – 100.1.1.1/24
   - ピア **IP** アドレス – 200.1.1.1/24
   - 事前共有鍵 – 値を入力

   VPN ピア B の設定は以下のようになります。

   - **Interface(インターフェイス)**—ethernet1/11
   - ローカル **IP** アドレス – 200.1.1.1/24
   - ピア **IP** アドレス – 100.1.1.1/24
   - 事前共有鍵 – ピア A と同じ値を入力
3. IKE フェーズ 1 で使用するために以前に作成した IKE 暗号プロファイルを選択します。

STEP 6 | IPSec トンネルをセットアップします。

1. **Network (ネットワーク)** > **IPSec Tunnels (IPSec トンネル)**の順に選択します。
2. **Add**（追加） をクリックして、**General**（全般） タブでオプションを設定します。

   この例では、VPN ピア A の設定は以下のようになります。

   - トンネル インターフェイス – tunnel.41
   - タイプ – 自動キー
   - **IKE** ゲートウェイ – 上で定義した IKE ゲートウェイを選択します。
   - **IPSec** 暗号プロファイル – 上で定義した IKE ゲートウエィを選択します。

   VPN ピア B の設定は以下のようになります。

   - **Tunnel Interface**(トンネル インターフェイス)—tunnel.40
   - タイプ – 自動キー
   - **IKE** ゲートウェイ – 上で定義した IKE ゲートウェイを選択します。
   - **IPSec** 暗号プロファイル – 上で定義した IKE ゲートウエィを選択します。
3. **Show Advanced Options** [詳細オプションの表示]をオンにし、**Tunnel Monitor** [トンネル モニター]をオンにして、接続を確認するために ping を送信する宛先 IP アドレスを指定します。
4. 接続の確立に失敗した場合のアクションを定義する方法については、トンネル モニタリング プロファイルの定義を参照してください。

STEP 7 | トラフィックをサイト（サブネット）間で許可するためのポリシーを作成します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. 指定した送信元および宛先 IP アドレスから発信されるトラフィックについて、トラフィックを Uuntrust ゾーンと vpn-tun ゾーン間および vpn-tun ゾーンと Untrust ゾーン間で許可するためのルールを作成します。

STEP 8 | OSPF 隣接および CLI からのルートを確認します。

両方のファイアウォールが互いにネイバーとして完全な状態で表示できることを確認します。また、VPN ピアのトンネル インターフェイスの IP アドレスおよび OSPF ルーター ID も確認します。各 VPN ピアで以下の CLI コマンドを使用します。

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route type ospf**

```
admin@FW-A> show routing route type ospf

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface          next-AS
2.1.1.0/24              0.0.0.0                 10   Oi       6760  tunnel.41
172.16.101.0/24         0.0.0.0                 10   Oi       6854  ethernet1/1
192.168.1.0/24          2.1.1.140               20 A Oo       6754  tunnel.40
total routes shown: 3
```

```
admin@FW-B> show routing route type ospf

flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface
2.1.1.0/24              0.0.0.0                 10   Oi       20033 tunnel.40
172.16.101.0/24         2.1.1.141               20   AOo      6896  tunnel.40
192.168.1.0/24          0.0.0.0                 10   Oi       8058  ethernet1/15
total routes shown: 3
```

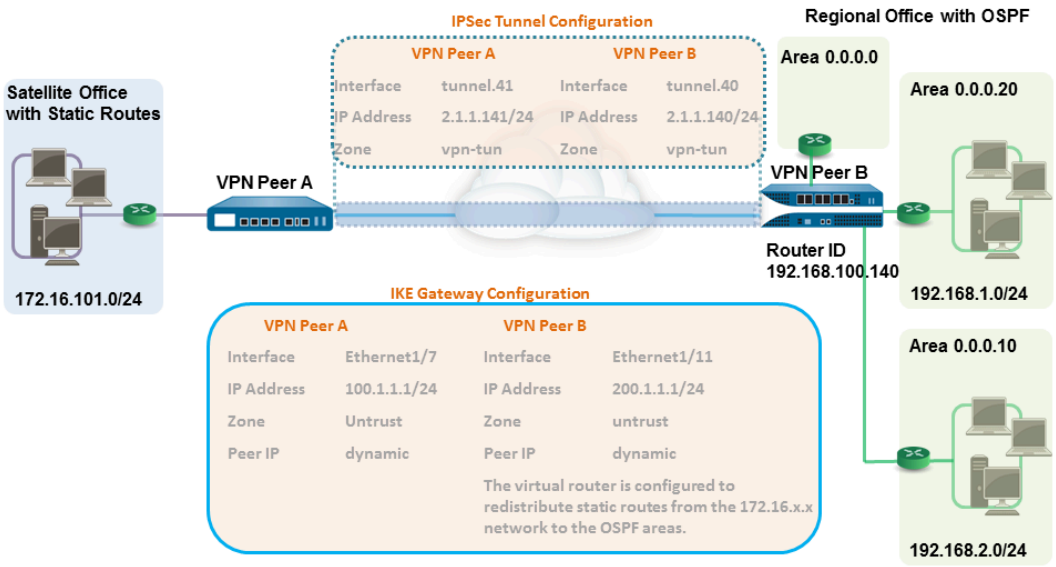
STEP 9 | 「VPN 接続のテスト」を行います。

トンネル モニタリングのセットアップおよびトンネルの状態の表示を参照してください。

スタティック ルーティングおよびダイナミック ルーティングを使用したサイト間 VPN

この例では、一方のサイトでスタティック ルートを使用し、もう一方のサイトで OSPF を使用しています。ルーティング プロトコルが場所間で同じでない場合、各ファイアウォールのトンネル インターフェイスはスタティック IP アドレスで設定する必要があります。次に、ルーティング情報の交換を可能にするために、スタティック ルーティングとダイナミック ルーティングの両方のプロセスに参加するファイアウォールを再配信プロファイルで設定する必要があります。再配信プロファイルを設定すると、仮想ルーターはプロトコル間のルート（スタティック ルート、接続済みルート、ホスト）をスタティック Autonomous System から OSPF Autonomous System に再配信してフィルタリングできます。この再配信プロファイルがない場合、各プロトコルは独自に機能し、同じ仮想ルーターを実行している他のプロトコルとルート情報を交換しません。

この例では、サテライト オフィスはスタティック ルートを持ち、192.168.x.x ネットワークを宛先とするすべてのトラフィックは tunnel.41 にルーティングされます。VPN ピア B の仮想ルーターはスタティック ルーティングとダイナミック ルーティングの両方のプロセスに参加し、スタティック ルートを OSPF Autonomous System に配信（エクスポート）するために再配信プロファイルで設定されます。



STEP 1 | 各ファイアウォールでレイヤー 3 インターフェイスを設定します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** の順に選択し、VPN について設定するインターフェイスを選択します。
2. **Interface Type (インターフェイス タイプ)** で **Layer3 (レイヤー 3)** を選択します。
3. **Config (設定)** タブでインターフェイスが属する **Security Zone (セキュリティ ゾーン)** を選択します。
   - インターフェイスは、信頼されるネットワークの外部のゾーンからアクセスできる必要があります。VPN トラフィックを可視化して制御するために、専用の VPN ゾーンを作成することを検討してください。
   - まだゾーンを作成していない場合は、**Security Zone (セキュリティ ゾーン)** から **New Zone (新規ゾーン)** を選択し、新規ゾーンの **Name (名前)** を定義してから **OK** をクリックします。
4. 使用する **Virtual Router (仮想ルーター)** を選択します。
5. IP アドレスをインターフェイスに割り当てるには、**IPv4** タブを選択してから IP セクションで **Add**（追加）をクリックし、インターフェイスに割り当てる IP アドレスとネットマスク（例: 192.168.210.26/24）を入力します。
6. インターフェイス設定を保存するには、**OK** をクリックします。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Interface(インターフェイス)**—ethernet1/7
   - セキュリティ ゾーン — Untrust
   - 仮想ルーター — デフォルト
   - **IPv4** — 100.1.1.1/24

   VPN ピア B の設定は以下のようになります。

   - **Interface(インターフェイス)**—ethernet1/11
   - セキュリティ ゾーン — Untrust
   - 仮想ルーター — デフォルト
   - **IPv4** — 200.1.1.1/24

STEP 2 | 暗号プロファイル（フェーズ 1 では IKE 暗号プロファイル、フェーズ 2 では IPSec 暗号プロファイル）をセットアップします。

両方のピアでこのタスクを実行し、必ず同じ値を設定します。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **IKE Crypto (IKE 暗号)** を選択します。この例では、デフォルトのプロファイルを使用します。
2. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **IPSec Crypto (IPSec 暗号)** を選択します。この例では、デフォルトのプロファイルを使用します。

STEP 3 | IKE ゲートウェイをセットアップします。

IKE フェーズ 1 トンネルをセットアップするときに認証の精度を高めるために事前共有鍵を使用すると、ローカルおよびピア ID 属性、および IKE ネゴシエーション プロセスで照合される対応する値をセットアップできます。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **IKE Gateway (IKE ゲートウェイ)** を選択します。
2. **Add**（追加） をクリックして、**General**（全般） タブでオプションを設定します。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Interface(インターフェイス)**—ethernet1/7
   - ローカル **IP** アドレス — 100.1.1.1/24
   - ピア **IP** タイプ — ダイナミック
   - 事前共有鍵 — 値を入力
   - ローカル **ID** — **[FQDN (hostname)]** を選択し、VPN ピア A の値を入力します。
   - ピア **ID** — **[FQDN (hostname)]** を選択し、VPN ピア B の値を入力します。

   VPN ピア B の設定は以下のようになります。

   - **Interface(インターフェイス)**—ethernet1/11
   - ローカル **IP** アドレス — 200.1.1.1/24
   - ピア **IP** アドレス — ダイナミック
   - 事前共有鍵 — ピア A と同じ値を入力
   - ローカル **ID** — **[FQDN (hostname)]** を選択し、VPN ピア B の値を入力します。
   - ピア **ID** — **[FQDN (hostname)]** を選択し、VPN ピア A の値を入力します。
3. IKE フェーズ 1 で使用するために以前に作成した IKE 暗号プロファイルを選択します。

STEP 4 | トンネル インターフェイスを作成し、仮想ルーターおよびセキュリティ ゾーンに関連付けます。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Tunnel (トンネル)** の順に選択し、**Add(追加)** をクリックします。
2. **[インターフェイス名]** フィールドで、**.41** などの数値のサフィックスを指定します。
3. **Config (設定)** タブで、**Security Zone (セキュリティ ゾーン)** を展開して以下のようにゾーンを定義します。
   - トンネルの終端点として信頼されたゾーンを使用するには、そのゾーンを選択します。
   - （推奨）VPN トンネルの終端のゾーンを別に作成するには、**New Zone**（新規ゾーン）をクリックします。[ゾーン] ダイアログの **[名前]** で「*vpn-tun*」などの名前を付けて新しいゾーンを定義し、**[OK]** をクリックします。
4. **Virtual Router**[仮想ルーター] を選択します。
5. IP アドレスをトンネル インターフェイスに割り当て、**[IPv4]** または **[IPv6]** タブを選択します。[IP] セクションで **[追加]** をクリックし、インターフェイスに割り当てる IP アドレスとネットワーク マスク/プレフィックス（例: 172.19.9.2/24）を入力します。

   この IP アドレスは、トンネルにトラフィックをルーティングするため、およびトンネルの状態をモニタリングするために使用されます。
6. インターフェイス設定を保存するには、**OK** をクリックします。

   この例では、VPN ピア A の設定は以下のようになります。
   - **Interface**[インターフェイス] – tunnel.41
   - セキュリティ ゾーン – vpn_tun
   - 仮想ルーター – デフォルト
   - **IPv4** – 2.1.1.141/24

   VPN ピア B の設定は以下のようになります。
   - インターフェイス – tunnel.42
   - セキュリティ ゾーン – vpn_tun
   - 仮想ルーター – デフォルト
   - **IPv4** – 2.1.1.140/24

STEP 5 | 192.168.x.x ネットワーク上の宛先にトラフィックをルーティングするインターフェイスを指定します。

1. VPN ピア A で、仮想ルーターを選択します。
2. **[スタティック ルート]** を選択し、192.168.x.x ネットワークを**[宛先]** とするトラフィックをルーティングするために **[インターフェイス]** として tunnel.41 を **[追加]** します。

STEP 6 | 仮想ルーターでスタティック ルートと OSPF 設定をセットアップし、OSPF エリアをファイアウォール上の適切なインターフェイスに関連付けます。

1. VPN ピア B で **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、デフォルトのルーターを選択するか新しいルーターを追加します。
2. **Static Routes**（静的ルート） を選択し、172.168.x.x. ネットワークでトラフィックのネクスト ホップとしてトンネル IP アドレスを **Add**（追加） します。

   目的のルート メトリックを割り当てます。低い値を使用すると、テーブルの転送におけるルート選択で優先順位が高くなります。
3. **OSPF**（IPv4 の場合）または **OSPFv3** （IPv6 の場合）を選択し、**Enable**（有効）をオンにします。
4. この例では、VPN ピア B の OSPF 設定は以下のようになります。
   - ルーターID：192.168.100.140
   - エリア ID：インターフェイス Ethernet 1/12およびリンク タイプに0.0.0.0 が割り当てられているブロードキャスト
   - エリア ID：インターフェイス Ethernet1/1およびリンク タイプに0.0.0.10 が割り当てられているブロードキャスト
   - エリア ID：インターフェイス Ethernet1/15およびリンク タイプに0.0.0.20 が割り当てられているブロードキャスト

STEP 7 | スタティック ルートを OSPF Autonomous System に注入するための再配信プロファイルを作成します。

1. VPN ピア B で再配信プロファイルを作成します。
   1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、上で使用したルーターを選択します。
   2. **Redistribution Profiles**（再配信プロファイル）を選択し、**Add**（追加）をクリックします。
   3. [名前] フィールドにプロファイル名を入力し、**[再配信あり]** を選択して **[優先順位]** の値を割り当てます。複数のプロファイルを設定している場合、優先順位の最も低い値を持つプロファイルが最初に一致されます。
   4. **Source Type (送信元タイプ)** を **static**（静的） に設定し、**OK** をクリックします。ステップ 6 で定義した静的ルートが再配信に使用されます。
2. スタティック ルートを OSPF システムに注入します。
   1. **OSPF** > **Export Rules (ルールのエクスポート)**（IPv4 の場合）または **OSPFv3** > **Export Rules (ルールのエクスポート)**（IPv6 の場合）の順に選択します。
   2. **[追加]** をクリックし、作成した再配信プロファイルを選択します。
   3. 外部ルートを OSPF システムに誘導する方法を選択します。デフォルト オプションである **Ext2** は、外部メトリックのみを使用したルートの総コストを計算します。内部と外部の両方の OSPF メトリックを使用するには、**Ext1** を使用します。
   4. OSPF システムに注入されるルートについて、**Metric**（メトリック） コスト値）を割り当てます。このオプションを使用すると、注入されたルートが OSPF システムに到達したときにそのメトリックを変更できます。
   5. **OK** をクリックします。

STEP 8 | IPSec トンネルをセットアップします。

1. **Network (ネットワーク)** > **IPSec Tunnels (IPSec トンネル)**の順に選択します。
2. **Add**（追加） をクリックして、**General**（全般） タブでオプションを設定します。

   この例では、VPN ピア A の設定は以下のようになります。

   - トンネル インターフェイス – tunnel.41
   - タイプ – 自動キー
   - **IKE** ゲートウェイ – 上で定義した IKE ゲートウェイを選択します。
   - **IPSec** 暗号プロファイル – 上で定義した IKE ゲートウエィを選択します。

   VPN ピア B の設定は以下のようになります。

   - **Tunnel Interface**(トンネル インターフェイス)–tunnel.40
   - タイプ – 自動キー
   - **IKE** ゲートウェイ – 上で定義した IKE ゲートウェイを選択します。
   - **IPSec** 暗号プロファイル – 上で定義した IKE ゲートウエィを選択します。
3. **Show Advanced Options** [詳細オプションの表示]をオンにし、**Tunnel Monitor** [トンネル モニター]をオンにして、接続を確認するために ping を送信する宛先 IP アドレスを指定します。
4. 接続の確立に失敗した場合のアクションを定義する方法については、トンネル モニタリング プロファイルの定義を参照してください。

STEP 9 | トラフィックをサイト（サブネット）間で許可するためのポリシーを作成します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. 指定した送信元および宛先 IP アドレスから発信されるトラフィックについて、トラフィックを Uuntrust ゾーンと vpn-tun ゾーン間および vpn-tun ゾーンと Untrust ゾーン間で許可するためのルールを作成します。

STEP 10 | OSPF 隣接および CLI からのルートを確認します。

両方のファイアウォールが互いにネイバーとして完全な状態で表示できることを確認します。また、VPN ピアのトンネル インターフェイスの IP アドレスおよび OSPF ルーター ID も確認します。各 VPN ピアで以下の CLI コマンドを使用します。

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route**

以下は、各 VPN ピアの出力例です。

```
VPN PeerA

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          2.1.1.141       20      A S             tunnel.41
192.168.2.0/24          2.1.1.141       20      A S             tunnel.41
172.16.101.0/24         0.0.0.0         1       A H             ethernet1/1
2.1.1.140/24            2.1.1.141       20      A S             tunnel.41

VPN PeerB

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          0.0.0.0         10      A Oo            ethernet1/1
192.168.2.0/24          0.0.0.0         10      A Oo            ethernet1/15
172.16.101.0/24         2.1.1.140       20      A H             tunnel.40
2.1.1.141/24            2.1.1.140       10      A C             tunnel.40
```

STEP 11 | 「VPN 接続のテスト」を行います。

トンネル モニタリングのセットアップおよびトンネルの状態の表示を参照してください。

大規模 VPN（LSVPN）

Palo Alto Networks 次世代ファイアウォールに搭載された GlobalProtect 大規模 VPN （LSVPN）機能により、従来のハブ アンド スポーク VPN のデプロイメントが簡略化され、リモートサテライトでの設定を最小限に抑えて複数の支社がある企業ネットワークを素早くデプロイできます。このソリューションでは、データの安全性を高めるため、ファイアウォール認証と IPSec に証明書を使用します。

LSVPN により、Palo Alto Networks ファイアウォール同士のサイト間 VPN が実現されます。Palo Alto Networks ファイアウォールと別のデバイスとのサイト間 VPN をセットアップする方法については、「VPNs」を参照してください。

以下のトピックでは、LSVPN コンポーネントと、Palo Alto Networks ファイアウォール同士のサイト間 VPN サービスを実現するためのセットアップ方法について説明します。

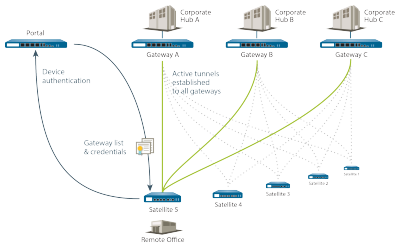
- LSVPN の概要
- LSVPN のインターフェイスおよびゾーンの作成
- GlobalProtect LSVPN コンポーネント間の SSL の有効化
- サテライトを認証するためのポータルの設定
- LSVPN の GlobalProtect ゲートウェイの設定
- LSVPN の GlobalProtect ポータルの設定
- LSVPN に参加するためのサテライトの準備
- LSVPN 設定の確認
- LSVPN のクイック設定

LSVPN の概要

GlobalProtect には、リモート サイトから企業リソースへの安全なアクセスを管理するための十分なインフラストラクチャが用意されています。このインフラストラクチャには、以下のコンポーネントが含まれています。

- **GlobalProtect** ポータル — GlobalProtect LSVPN インフラストラクチャの管理機能を提供します。GlobalProtect LSVPN に参加するすべてのサテライトは、サテライト（スポーク）をゲートウェイ（ハブ）に接続するための設定情報など、設定情報をポータルから受信します。ポータルは、Palo Alto Networks 次世代ファイアウォールのインターフェイスで設定します。
- **GlobalProtect** ゲートウェイ — サテライト接続のトンネル エンド ポイントを提供する Palo Alto Networks ファイアウォール。サテライトがアクセスするリソースはゲートウェイのセキュリティ ポリシーによって保護されます。個別のポータルとゲートウェイは必要ありません。1 つのファイアウォールがポータルおよびゲートウェイの両方として機能できます。
- **GlobalProtect** サテライト — リモート サイトにある Palo Alto Networks ファイアウォールで、企業オフィスにあるゲートウェイとの IPSec トンネルを確立し、中央管理されたリソースに安全にアクセスできるようにします。サテライト ファイアウォールでの設定は最小限で済み、新しいサイトを追加したときに素早く容易に VPN の規模を拡大できます。

以下の図は、GlobalProtect LSVPN コンポーネントの連携を示しています。



LSVPN のインターフェイスおよびゾーンの作成

LSVPN インフラストラクチャでは、以下のインターフェイスおよびゾーンを作成する必要があります。

- **GlobalProtect portal**[GlobalProtect ポータル] — GlobalProtect サテライトが接続するためにはレイヤー 3 インターフェイスが必要です。ポータルおよびゲートウェイが同じファイアウォールにある場合、同一のインターフェイスを使用することができます。ポータルは、支社からアクセスできるゾーンにある必要があります。
- **GlobalProtect gateways**[GlobalProtect ゲートウェイ] — リモート サテライトからアクセスできるゾーンのレイヤー 3 インターフェイス、保護されたリソースに接続する トラスト ゾーンの内部インターフェイス、サテライトから VPN トンネルを終端するための論理トンネル インターフェイスの 3 つのインターフェイスが必要です。他のサイト間 VPN ソリューションとは異なり、GlobalProtect ゲートウェイで必要なのは 1 つのトンネル インターフェイスのみです。すべてのリモート サテライトとのトンネル接続に使用します（ポイントツーマルチポイント）。ダイナミック ルーティングを使用する予定の場合、IP アドレスをトンネル インターフェイスに割り当てる必要があります。GlobalProtect はトンネル インターフェイスの IPv4 および IPv6 アドレシングの両方をサポートしています。
- **GlobalProtect satellites**[GlobalProtect サテライト] — リモート ゲートウェイとの VPN を確立するために単一のトンネル インターフェイスが必要です（最大 25 個のゲートウェイ）。ダイナミック ルーティングを使用する予定の場合、IP アドレスをトンネル インターフェイスに割り当てる必要があります。GlobalProtect はトンネル インターフェイスの IPv4 および IPv6 アドレシングの両方をサポートしています。

ポータル、ゲートウェイ、サテライトの詳細は、LSVPN の概要を参照してください。

STEP 1 | レイヤー 3 インターフェイスを設定します。

ポータル、各ゲートウェイ、およびサテライトは、いずれもトラフィックがサイト間をルーティングされるようにレイヤー 3 インターフェイスが必要です。

ゲートウェイとポータルが同じファイアウォールにある場合、1 つのインターフェイスを両方のコンポーネントに使用できます。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** の順に選択し、GlobalProtect LSVPN について設定するインターフェイスを選択します。
2. **Interface Type (インターフェイス タイプ)**ドロップダウン リストから **Layer3 (レイヤー 3)**を選択します。
3. **Config (設定)** タブでインターフェイスが属する **Security Zone (セキュリティ ゾーン)** を選択します。
   - インターフェイスは、信頼されるネットワークの外部のゾーンからアクセスできる必要があります。VPN トラフィックを可視化して制御するために、専用の VPN ゾーンを作成することを検討してください。
   - まだゾーンを作成していない場合は、**Security Zone (セキュリティ ゾーン)** ドロップダウン リストから **New Zone (新規ゾーン)** を選択し、新しいゾーンの **Name (名前)** を定義してから **OK** をクリックします。
4. 使用する **Virtual Router (仮想ルーター)** を選択します。
5. IP アドレスをインターフェイスに割り当てます。
   - IPv4 アドレスの場合、**IPv4** を選択して、インターフェイスに割り当てる IP アドレスとネットワーク マスクを **Add**（追加）します（例: 203.0.11.100/24）。
   - IPv6 アドレスの場合、**IPv6** を選択して、**Enable IPv6 on the interface**（インターフェースでの **IPv6** の有効化）を行い、インターフェイスに割り当てる IP アドレスとネットワーク マスクを **Add**（追加）します（例：2001:1890:12f2:11::10.1.8.160/80）。
6. インターフェイス設定を保存するには、**OK** をクリックします。

STEP 2 | GlobalProtect ゲートウェイをホストするファイアウォールで、GlobalProtect サテライトによって確立される VPN トンネルを終端する論理トンネル インターフェイスを設定します。

ダイナミック ルーティングを使用する予定がなければ、トンネル インターフェイスに *IP* アドレスは必要ありません。ただし、*IP* アドレスをトンネル インターフェイスに割り当てると、接続の問題をトラブルシューティングするときに役立つ場合があります。

VPN トンネルの終端となるゾーンで必ず ユーザー *ID* を有効にしてください。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Tunnel (トンネル)** の順に選択し、**Add(追加)** をクリックします。
2. **Interface Name**（インターフェイス名）フィールドで、**.2**などの数値のサフィックスを指定します。
3. **Config**（設定）タブで、**Security Zone**（セキュリティ ゾーン）ドロップダウン リストを展開して以下のようにゾーンを定義します。
   - トンネルの終端点として信頼されたゾーンを使用するには、ドロップダウン リストからそのゾーンを選択します。
   - （推奨）VPN トンネルの終端のゾーンを別に作成するには、**New Zone**（新規ゾーン）をクリックします。Zone [ゾーン] ダイアログの **Name**[名前] で新しいゾーンを定義し（たとえば、*lsvpn-tun*）、**Enable User Identification**[ユーザー ID の有効化] チェックボックスをオンにしてから **OK** をクリックします。
4. **Virtual Router**[仮想ルーター] を選択します。
5. （任意）トンネル インターフェイスに IP アドレスを割り当てるには：
   - IPv4 アドレスの場合、**IPv4** を選択して、インターフェイスに割り当てる IP アドレスとネットワーク マスクを **Add**（追加）します（例: 203.0.11.100/24）。
   - IPv6 アドレスの場合、**IPv6** を選択して、**Enable IPv6 on the interface**（インターフェースでの **IPv6** の有効化）を行い、インターフェイスに割り当てる IP アドレスとネットワーク マスクを **Add**（追加）します（例：2001:1890:12f2:11::10.1.8.160/80）。
6. インターフェイス設定を保存するには、**OK** をクリックします。

STEP 3 | VPN 接続のトンネルの終端のために別のゾーンを作成した場合、VPN ゾーンと Trust ゾーンの間をトラフィックが通過できるセキュリティ ポリシーを作成します。

例えば、ポリシー ルールにより*lsvpn-tun* ゾーンと *L3-Trust* ゾーン間のトラフィックを有効にできます。

STEP 4 | 変更をコミットします。

Commit（コミット）をクリックします。

GlobalProtect LSVPN コンポーネント間の SSL の有効化

GlobalProtect コンポーネント間のすべての相互作用は SSL/TLS 接続を介して行われます。したがって、各コンポーネントの設定する際に適切な証明書や証明書プロファイルを参照できるよう、各コンポーネントを設定する前に必要な証明書を生成してインストールしておく必要があります。以下のセクションでは、サポートされる証明書のデプロイ方法、説明、さまざまな GlobalProtect 証明書のベスト プラクティス ガイドラインについて説明し、必要な証明書を生成してデプロイする手順を紹介します。

- 証明書のデプロイメントについて
- GlobalProtect LSVPN コンポーネントへのサーバー証明書のデプロイ
- SCEPを使用してクライアント証明書をGlobalProtectサテライトにデプロイ

証明書のデプロイメントについて

GlobalProtect LSVPN の証明書をデプロイする基本的な方法は 2 つあります。

- **Enterprise Certificate Authority**[企業認証局] – すでに自分の企業認証局がある場合、この内部 CA を使用して GlobalProtect ポータルの中間 CA 証明書を発行し、証明書を GlobalProtect ゲートウェイおよびサテライトに発行できるようにします。また、GlobalProtectポータルを設定し、GlobalProtectサテライトにクライアント証明書を発行するSCEP（Simple Certificate Enrollment Protocol）クライアントとして動作させることもできます。
- **Self-Signed Certificates**[自己署名証明書] – ファイアウォールで自己署名ルート CA 証明書を生成し、それを使用してポータル、ゲートウェイ、サテライトのサーバー証明書を発行できます。自己署名ルート CA 証明書を使用する際、ポータルで自己署名ルート CA 証明書を作成し、それを使用してゲートウェイおよびサテライトのサーバー証明書を発行することをお勧めします。この方法では、証明書の署名に使用される秘密鍵はポータルにとどまります。

GlobalProtect LSVPN コンポーネントへのサーバー証明書のデプロイ

GlobalProtect LSVPN コンポーネントは相互認証に SSL/TLS を使用します。LSVPN をデプロイする前に、各ポータルおよびゲートウェイに SSL/TLS サービス プロファイルを割り当てる必要があります。このプロファイルは、サテライトと通信するためのサーバー証明書および許可された TLS バージョンを指定します。ポータルは最初の接続の際にサテライト登録プロセスの一部として各サテライトへサーバー証明書を発行するため、サテライトの SSL/TLS サービス プロファイルを作成する必要はありません。

さらに、ゲートウェイまたはサテライトとしてホストする予定の各ファイアウォールにサーバー証明書を発行するために使用されるルート認証局（CA）証明書をインポートする必要があります。最後に、LSVPN に参加する各ゲートウェイおよびサテライトで、相互認証を使用して SSL/TLS 接続を確立できるようにする証明書プロファイルを設定する必要があります。

以下のワークフローは、GlobalProtect LSVPN コンポーネントに SSL 証明書をデプロイするためのベスト プラクティスの手順を示しています。

STEP 1 | GlobalProtect ポータルをホストするファイアウォールで、GlobalProtect コンポーネントの証明書に署名するためにルート CA 証明書を作成する必要があります。

自己署名ルート CA 証明書の作成を行います。

1. **Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificates (証明書)** > **Device Certificates (デバイス証明書)** を選択して **Generate (生成)** をクリックします。
2. **Certificate Name** [証明書名]に「**LSVPN_CA**」などの名前を入力します。
3. **Signed By** [署名者]フィールドの値は選択しないでください（その証明書が自己署名証明書であることを示すものであるため）。
4. **Certificate Authority**(認証局) チェックボックスをオンにしてから **OK** をクリックし、証明書を生成します。

STEP 2 | GlobalProtect ポータルおよびゲートウェイの SSL/TLS サービス プロファイルを作成します。

ポータルおよび各ゲートウェイに対して、一意の自己署名サーバー証明書を参照する SSL/TLS サービス プロファイルを割り当てる必要があります。

ベスト プラクティスとして、ポータルで必要なすべての証明書を発行し、署名付き証明書（秘密鍵を含む）をエクスポートする必要がないようにします。

GlobalProtect ポータルとゲートウェイが同じファイアウォール インターフェイスにある場合、両方のコンポーネントについて同じサーバー証明書を使用できます。

1. ポータルでルート CA を使用し、デプロイする各ゲートウェイに対して証明書の生成を行います。
   1. **Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificates (証明書)** > **Device Certificates (デバイス証明書)** を選択して **Generate (生成)** をクリックします。
   2. **Certificate Name**（証明書名）を入力します。
   3. **Common Name**（共通名）フィールドに、ゲートウェイを設定するインターフェイスの FQDN （推奨）または IP アドレスを入力します。
   4. **Signed By** [署名者]フィールドで、作成した「**LSVPN_CA**」を選択します。
   5. Certificate Attributes [証明書の属性] セクションで、**Add**[追加] をクリックしてゲートウェイを一意に識別する属性を定義します。**Host Name** [ホスト名]属性（証明書

の SAN フィールドに入力される）を追加する場合、この値は **Common Name** [共通名]に定義した値と完全に一致する必要があります。

6. 証明書を **Generate**[生成] します。

2. ポータルおよび各ゲートウェイに対してSSL/TLS サービス プロファイルの設定を行います。

1. **Device** > **Certificate Management** > **SSL/TLS Service Profile**(デバイス > 証明書の管理 > SSL/TLS サービス プロファイル) の順に選択し、**Add**(追加) をクリックします。
2. **Name** [名前]にプロファイルを識別する名前を入力し、ポータルまたはゲートウェイについて作成したサーバーの **Certificate** [証明書]を選択します。
3. サテライトとの通信を許可する TLS バージョンの範囲（**Min Version** [最小バージョン] ～ **Max Version** [最大バージョン]）を定義し、**OK** をクリックします。

STEP 3 | 自己署名サーバー証明書をゲートウェイにデプロイします。

ベスト プラクティス:

- ルート CA によって発行された自己署名サーバー証明書をポータルからエクスポートし、ゲートウェイにインポートします。
- 各ゲートウェイに対して一意のサーバー証明書を発行します。
- 証明書の Common Name [共通名]（CN）フィールドと、該当する場合は、Subject Alternative Name [サブジェクト代替名]（SAN）フィールドが、ゲートウェイを設定するイ

ンターフェイスの IP アドレスまたは完全修飾ドメイン名（FQDN）と完全に一致する必要があります。

1. ポータルで **Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificates (証明書)** > **Device Certificates (デバイス証明書)** の順に選択し、デプロイするゲートウェイ証明書を選択して **Export (エクスポート)** をクリックします。
2. **File Format** [ファイル フォーマット]ドロップダウン リストから **Encrypted Private Key and Certificate (PKCS12)** [暗号化された秘密鍵と証明書（PKCS12）]を選択します。
3. **Passphrase**[パスフレーズ] を入力（および再入力）して証明書に関連付けられた秘密鍵を暗号化し、**OK** をクリックして PKCS12 ファイルをコンピュータにダウンロードします。
4. ゲートウェイで **Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificates (証明書)** > **Device Certificates (デバイス証明書)** の順に選択し、**Import (インポート)** をクリックします。
5. **Certificate Name**（証明書名）を入力します。
6. **Certificate File** [証明書ファイル]にポータルからダウンロードしたファイルのパスと名前を入力するか、**Browse** [参照]をクリックしてファイルを探します。
7. **File Format**（ファイル フォーマット）に **Encrypted Private Key and Certificate (PKCS12)**（暗号化された秘密鍵と証明書（**PKCS12**））を選択します。
8. **Key File** [キー ファイル]に PKCS12 ファイルのパスと名前を入力するか、**Browse** [参照]でファイルを見つけます。
9. ポータルからエクスポートしたときに秘密鍵の暗号化に使用した **Passphrase** [パスフレーズ]を 2 回入力した後に、**OK** をクリックして証明書と秘密鍵をインポートします。

STEP 4 | LSVPN コンポーネントのサーバー証明書を発行するために使用するルート CA 証明書をインポートします。

ルート CA 証明書をすべてのゲートウェイおよびサテライトにインポートする必要があります。セキュリティ上の理由により、必ず証明書のみをエクスポートし、関連付けられた秘密鍵はエクスポートしないでください。

1. ルート CA 証明書をポータルからダウンロードします。
   1. **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択します。
   2. LSVPN コンポーネントの証明書を発行するために使用するルート CA 証明書を選択し、**[エクスポート]** をクリックします。
   3. **File Format** [ファイル フォーマット]ドロップダウン リストから **Base64 Encoded Certificate (PEM)** [Base64 エンコード済み証明書（PEM）]を選択し、**OK** をクリックして証明書をダウンロードします（秘密鍵はエクスポートしないでください）。
2. ゲートウェイおよびサテライトをホストするファイアウォールで、ルート CA 証明書をインポートします。
   1. **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択し、**Import**（インポート）をクリックします。
   2. **Certificate Name**（証明書名）フィールドに、クライアント CA 証明書であることを識別できる名前を入力します。
   3. **Browse**（参照）をクリックして、CA からダウンロードした **Certificate File**（証明書ファイル）を選択します。
   4. **Base64 Encoded Certificate (PEM)**（**Base64** エンコード済み証明書（**PEM**））を **File Format**（ファイル フォーマット）フィールドで選択し、**OK** をクリックします。
   5. **Device Certificates**（デバイス証明書）タブで、先ほどインポートした証明書を選択して開きます。
   6. **Trusted Root CA**（信頼されたルート **CA**）を選択して **OK** をクリックします。
   7. 変更を **Commit**（コミット）します。

STEP 5 | 証明書プロファイルを作成します。

GlobalProtect LSVPN ポータルおよび各ゲートウェイには、サテライトの認証に使用する証明書を指定する証明書プロファイルが必要です。

1. **Device** > **Certificate Management** > **Certificate Profile**(デバイス > 証明書の管理 > 証明書プロファイル) の順に選択し、**Add**(追加) をクリックして **Name**(名前) フィールドにプロファイル名を入力します。
2. **Username Field**[ユーザー名フィールド] が **None**[なし] に設定されていることを確認します。
3. **CA Certificates (**証明書**)** フィールドで **Add (**追加**)** をクリックし、前のステップでインポートした信頼できるルート CA 証明書を選択します。
4. （推奨）CRL や OCSP の使用を有効にして、証明書の状態を検証できるようにします。
5. **OK** をクリックしてプロファイルを保存します。

STEP 6 | 変更をコミットします。

Commit（コミット）をクリックします。

SCEPを使用してクライアント証明書をGlobalProtectサテライトにデプロイ

クライアント証明書をサテライトにデプロイする別の方法として、GlobalProtectポータルをお客様のエンタープライズPKI内のSCEPサーバーへのSCEP（Simple Certificate Enrollment Protocol）クライアントとして動作させることができます。エンタープライズPKIはポータルからリクエストを受けた際に証明書を生成し、その証明書をポータルに送信します。つまり、SCEPのオペレーションは動的なものになります。

サテライト デバイスはポータルあるいはゲートウェイへの接続をリクエストする際、接続リクエストに自身のシリアル番号も含めます。ポータルはSCEPプロファイルの設定を使用してCSRをSCEPサーバーに送信しますが、その際、クライアント証明書のサブジェクトにデバイスのシリアル番号を自動的に含めます。エンタープライズPKIからクライアント証明書を受信した後、ポータルはバックグラウンドでそのクライアント証明書をサテライト デバイスにデプロイします。次にサテライト デバイスは認証のためにクライアント証明書をポータルあるいはゲートウェイに提示します。

STEP 1 | SCEP プロファイルを作成します。

1. **Device** > **Certificate Management** > **SCEP**(デバイス > 証明書管理 > SCEP) の順に選択し、**Add**(追加) をクリックして新しいプロファイルを追加します。
2. SCEP プロファイルを識別する **Name**（名前）を入力します。
3. このプロファイルが複数の仮想システム容量のあるファイアウォール用であれば、仮想システムを選択するか、そのプロファイルを利用できる **Location**（場所）として **Shared**（共有）を選択します。

STEP 2 | （任意）SCEP ベースの証明書発行をより安全に行いたい場合は、各回の証明書要求について PKI およびポータルとの間に SCEP チャレンジレスポンス機能を設定します。

この機能の設定後はバックグラウンドで動作するため、追加の入力が必要になることはありません。

連邦情報処理標準（FIPS）に準拠するため、連邦情報処理標準 (FIPS) では、**Dynamic** SCEP チャレンジを使用し、HTTPS を使用する **Server URL** を指定します (手順 7 を参照)。

以下のいずれかのオプションを選択します。

- **None**(なし) - （デフォルト）SCEPサーバーは証明書の発行前にポータルとのチャレンジを行いません。
- **Fixed**（固定）–PKIインフラストラクチャ内のSCEPサーバー（**`http://10.200.101.1/CertSrv/mscep_admin/`**）から必須の登録パスワードを取得し、そのパスワードをPassword[パスワード]欄に入力します。
- **Dynamic**[動的]–ポータルのクライアントがこれらの認証情報を送信するSCEP **Server URL**[サーバーURL]（例：**`http://10.200.101.1/CertSrv/mscep_admin/`**）、ユーザー名、および任意のOTPを入力します。このユーザー名およびパスワードには、PKI管理者の認証情報を使用できます。

STEP 3 | SCEP サーバーとポータル間の接続設定を指定し、ポータルがクライアント証明書をリクエスト・受信できるようにします。

サテライトを識別するために、ポータルは自動的にSCEPサーバーへのCSRリクエストにデバイスのシリアル番号を含めます。SCEPプロファイルには**Subject**[サブジェクト]フィールドの値が必要なため、LSVPN用のクライアント証明書で値を使用しない場合でもデフォルトの**$USERNAME**トークンはそのままにしておくことができます。

1. PKI 内の SCEP サーバーにアクセスするためにポータルが使用する**Server URL**（サーバー **URL**）を設定します（例：**`http://10.200.101.1/certsrv/mscep/`**）。
2. SCEP サーバーを識別するための文字列（255 文字まで）を **CA-IDENT Name**（**CA-IDENT** 名）に入力します。
3. **Subject Alternative Name Type**（サブジェクトの別名タイプ）を選択します。
   - **RFC 822 Name**（**RFC822** 名）– 証明書のサブジェクトまたはサブジェクト代替名拡張子に電子メールアドレス名を入力します。
   - **DNS Name**（**DNS** 名）– 証明書の検証に使用する DNS 名を入力します。
   - **Uniform Resource Identifier**（ユニフォームリソース識別子）– クライアントが証明書を取得する URI リソース名を入力します。
   - **None**（なし）– 証明書の属性を指定しません。

STEP 4 | （任意）証明書の暗号設定を行います。

- 証明書の鍵長（**Number of Bits**（ビット数））を選択します。ファイアウォールが FIPS-CC モードで鍵生成アルゴリズムが RSA の場合。RSA キーは 2,048 ビット以上でなければなりません。
- 証明書署名要求（CSR）用のダイジェストアルゴリズムを示す **Digest for CSR (CSR** 用ダイジェスト**)** を選択します。（SHA1、SHA256、SHA384、またはSHA512）。

STEP 5 | （任意）許可される証明書の用途を設定します（署名用または暗号化用）。

- この証明書を署名のために使用する場合、**Use as digital signature**（デジタル署名として使用）のチェックボックスを選択します。これにより、デジタル署名の検証を行う際にエンドポイントが証明書に含まれる秘密鍵を使用するようになります。
- この証明書を暗号化のために使用する場合、**Use for key encipherment**（鍵の暗号化のために使用）のチェックボックスを選択します。これにより、SCEP サーバーが発行する証明書を通して確立された HTTPS 接続を経由して交換されたデータをクライアントのエンドポイントで暗号化する際に、証明書に含まれる秘密鍵を使用するようになります。

STEP 6 | （任意）ポータルが正しい SCEP サーバーに確実に接続されるようにするために、**CA Certificate Fingerprint**（**CA** 証明書フィンガープリント）を入力します。SCEP サーバーインターフェイスの Thumbprint（指紋）のフィールドからフィンガープリントを入手してください。

1. SCEP サーバーの管理 UI の URL を入力します (たとえば、**`http://<hostname or IP>/CertSrv/mscep_admin/`** など)。
2. Thumbprint（指紋）をコピーし、**CA Certificate Fingerprint**（**CA** 証明書フィンガープリント）に入力します。

STEP 7 | SCEP サーバーと GlobalProtect ポータルの間の相互 SSL 認証を有効にします。米国の連邦情報処理標準（FIPS）に準拠するためにこれが必須になります。Federal Information Processing Standard (連邦情報処理標準 - FIPS)

FIPS-CC の実施についてはファイアウォールのログインページおよびそのステータスバーに表示されます。

SCEP サーバーのルート**CA Certificate**（**CA** 証明書）を選択します。また、必要に応じて**Client Certificate**（クライアント証明書）を選択し、SCEP サーバーと GlobalProtect ポータルの間の相互 SSL 認証を有効にすることも可能です。

STEP 8 | 設定を保存・コミットします。

1. **OK** をクリックして設定を保存し、SCEP 設定を閉じます。
2. 設定を **Commit**（コミット）します。

ポータルが SCEP プロファイルの設定を使用して CA 証明書をリクエストしようと試み、それをファイアウォールがホストするポータルに保存します。正しく実行されると、CA証明書が**Device** > **Certificate Management** > **Certificates**(デバイス > 証明書管理 > 証明書)に表示されます。

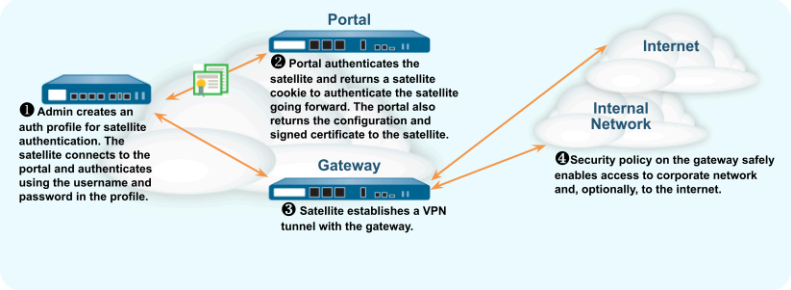
STEP 9 | （任意）SCEP プロファイルの保存後にポータルが証明書の取得に失敗する場合、ポータルから手動で CSR を生成することができます。

1. **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択してから **Generate**（生成）をクリックします。
2. **Certificate Name**（証明書名）を入力します。この名前にはスペースを含められません。
3. お客様のエンタープライズ PKI に CSR を送信する際に使用する **SCEP Profile**（**SCEP** プロファイル）を選択します。
4. **OK** をクリックしてリクエストを送信し、証明書を生成します。

サテライトを認証するためのポータルの設定

LSVPN に登録するには、各サテライトとポータルとの SSL/TLS 接続を確立する必要があります。接続の確立後、ポータルはサテライトを認証し、LSVPN に参加する権限があることを確認します。サテライトの認証に成功すると、ポータルはそのサテライトのサーバー証明書を発行し、サテライトが接続できるゲートウェイと、ゲートウェイとの SSL 接続を確立するために必要なルート CA 証明書を指定する LSVPN 設定をプッシュします。

サテライトが最初の接続時にポータルに対して認証を受けるには、ポータル LSVPN 構成の認証プロファイルを作成する必要があります。サテライト管理者は、最初の接続を確立するために、ポータルに対してサテライトを手動で認証する必要があります。認証に成功すると、ポータルはサテライト Cookie を返し、後続の接続でサテライトを認証します。ポータルが発行するサテライト Cookie の有効期間は 180 日です。Cookie の有効期限が切れると、サテライト管理者は手動で再度認証する必要があり、その時点でポータルは新しい Cookie を発行します。



以下のワークフローは、既存の認証サービスに対してサテライトを認証するためにポータルをセットアップする方法を示しています。ポータルへのサテライトの認証のために、GlobalProtect LSVPN はローカル データベース認証のみをサポートします。

STEP 1 | ローカル データベース認証を設定 して、サテライト管理者がポータルに対してサテライトを認証できるようにします。

1. **Device** > ローカルユーザーデータベース > ユーザー を選択し、 ユーザー アカウントをローカル データベースに追加します。
2. ユーザー アカウントをローカル データベースへ追加します。

STEP 2 | 認証プロファイルを設定します。

1. **Device** > 認証プロファイル > 追加 を選択します。
2. プロファイルに 名前 を入力し、タイプ を ローカル データベース に設定します。
3. **OK** をクリックし、変更を **Commit (コミット)** します。

STEP 3 | サテライトを認証します。

ポータルに対してサテライトを認証するには、サテライト管理者がローカル データベースで構成されたユーザー名とパスワードを提供する必要があります。

1. **Network (**ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)** の順に選択し、LSVPN 用に作成したトンネル設定の Status (ステータス) 列で **Gateway Info (**ゲートウェイ情報**)** リンクをクリックします。
2. **Portal Status** [ポータル状態]フィールドで **enter credentials** [資格情報の入力]リンクをクリックし、サテライトがポータルの認証を受けられるようにするために必要なユーザー名とパスワードを入力します。

   ポータルが初めてポータルに対して正常に認証されると、ポータルはサテライト Cookie を生成し、それを使用して後続のセッションでサテライトを認証します。

LSVPN の GlobalProtect ゲートウェイの設定

ポータルがサテライトに配信する GlobalProtect 設定にはサテライトが接続できるゲートウェイのリストが含まれているため、ポータルを設定する前にゲートウェイを設定すると良いでしょう。

GlobalProtect ゲートウェイを設定する前に、以下のタスクを完了する必要があります。

- LSVPN のインターフェイスおよびゾーンの作成各ゲートウェイを設定するインターフェースに、物理インターフェイスと仮想トンネル インターフェイスの両方を設定する必要があります。
- GlobalProtect LSVPN コンポーネント間の SSL の有効化 GlobalProtectサテライトからゲートウェイへの相互SSL/TLS接続を確立するために必要なゲートウェイサーバー証明書、SSL/TLSサービスプロファイル、証明書プロファイルを構成することによって。

以下のように LSVPN に参加する各 GlobalProtect ゲートウェイを設定します。

STEP 1 | ゲートウェイを追加します。

1. **Network** > **GlobalProtect** > **Gateways**(ネットワーク > GlobalProtect > ゲートウェイ) の順に選択し、**Add(追加)** をクリックします。
2. **General**（全般）画面で、**Name**（名前）フィールドにゲートウェイ名を入力します。ゲートウェイ名にスペースを含めることはできません。ベスト プラクティスとして、ユーザーや管理者がゲートウェイを識別できるように、場所や説明的情報を含めます。
3. （任意）**Location**（場所）フィールドから、このゲートウェイが属する仮想システムを選択します。

STEP 2 | サテライト デバイスがゲートウェイに接続できるようにするネットワーク情報を指定します。

ゲートウェイのネットワーク インターフェイスを作成していない場合は、LSVPN のインターフェイスおよびゾーンの作成を参照してください。

1. サテライトがゲートウェイへの入力アクセスに使用する **Interface**[インターフェイス] を選択します。
2. ゲートウェイ アクセス用の **IP Address Type (アドレス タイプ)** および **IP address (IP アドレス)** を指定します。
   - IP アドレス タイプは、**IPv4**（のみ）、**IPv6**（のみ）、あるいは **IPv4 and IPv6 (IPv4 および IPv6)** にできます。ネットワークがデュアル スタック構成をサポートしているときは、**IPv4 and IPv6**（**IPv4** および **IPv6**）を使用します。これにより IPv4 と IPv6 が同時に動作します。
   - IP アドレスは IP アドレス タイプに対応するものでなければなりません。たとえば、IPv4 の場合は **172.16.1/0**、IPv6 の場合は **21DA:D3:0:2F3B** のように指定します。デュアル スタック構成の場合は、IPv4 アドレスと IPv6 アドレスの両方を入力します。
3. **OK** をクリックして変更を保存します。

STEP 3 | トンネルを確立しようとしているサテライトをゲートウェイが認証する方法を指定します。ゲートウェイの SSL/TLS サービス プロファイルをまだ作成していない場合は、GlobalProtect LSVPN コンポーネントへのサーバー証明書のデプロイを参照してください。

認証プロファイルまたは証明書プロファイルを設定していない場合は、サテライトを認証するためのポータルの設定で手順を参照してください。

証明書プロファイルをまだ設定していない場合は、GlobalProtect LSVPN コンポーネント間の SSL の有効化で手順を参照してください。

GlobalProtect Gateway Configuration [GlobalProtectゲートウェイ設定]ダイアログでAuthentication [認証]を選択し、次のいずれかを設定します。

- ゲートウェイとサテライト間でセキュアな通信を行うために、ゲートウェイ用の**SSL/TLS Service Profile**[SSL/TLSサービス プロファイル]を選択します。
- サテライトを認証するために使用する認証プロファイルを指定するには、Client Authentication [クライアント認証]を**Add**[追加]します。次に、設定を識別できる **Name** [名前]を入力し、**OS**を選択します。**Satellite**[サテライト]で設定をサテライトに適用し、サテライトを認証するために使用する**Authentication Profile**[認証プロファイル]を指定します。トンネルを確立しようとしているサテライト デバイスの認証に使用するゲートウェイの**Certificate Profile**[証明書プロファイル]を選択することもできます。

STEP 4 | トンネル パラメータを設定してトンネルを有効にします。

1. GlobalProtect Gateway Configuration (GlobalProtect ゲートウェイ設定) ダイアログで、**Satellite (サテライト)** > **Tunnel Settings (トンネル設定)** の順に選択します。
2. **Tunnel Configuration**[トンネル設定] チェック ボックスをオンにして、トンネルを有効にします。
3. LSVPN のインターフェイスおよびゾーンの作成 へのタスクを実行したときに GlobalProtect サテライトによって確立された VPN トンネルを終了するために定義した **Tunnel Interface**を選択します。
4. （任意）カプセル化されたパケットで ToS （Type of Service）情報を保持する場合、**Copy TOS** [TOS のコピー]を選択します。

   トンネル内に複数のセッション（それぞれ*TOS*値が異なる）ある場合、*TOS*をコピーすると*IPSec*パケットが誤った順序で届くおそれがあります。

STEP 5 | （任意）トンネル モニタリングを有効化します。

トンネル モニタリングによって、サテライトはそのゲートウェイ トンネル接続を監視でき、接続に失敗した場合にバックアップ ゲートウェイにフェイルオーバーできるようになります。別のゲートウェイへのフェイルオーバーは、LSVPN でサポートされている唯一のトンネル モニタリング プロファイルのタイプです。

1. **Tunnel Monitoring**[トンネル監視] チェック ボックスをオンにします。
2. **Destination IP (宛先 IP) Address (アドレス)** フィールドで、ゲートウェイがアクティブかどうかをサテライトが判断するために使用するアドレスを指定します。**IPv4** アドレス、**IPv6** アドレス、あるいはその両方を指定できます。または、トンネル インター

フェイスに IP アドレスを設定した場合はこのフィールドを空白のままにでき、トンネル モニターは代わりにトンネル インターフェイスを使用して接続がアクティブかどうかを判断します。

3. **Tunnel Monitor Profile**[トンネル監視プロファイル] ドロップダウン リストから **Failover**[フェイルオーバー] を選択します（これは、サポートされる唯一の LSVPN のトンネル モニターのプロファイルです）。

STEP 6 | トンネル接続を確立するときに使用する IPSec Crypto profile [IPSec 暗号プロファイル]を選択します。

このプロファイルは、トンネルを通過するデータを安全にするための IPSec 暗号化や認証方法のタイプを指定します。LSVPN の両方のトンネル エンドポイントが組織内の信頼されるファイアウォールであるため、一般に、IPSec プロトコルとして ESP、DH グループに group2、暗号化に AES-128-CBC、認証に SHA-1 を使用するデフォルトの（事前定義済み）プロファイルを使用できます。

IPSec Crypto Profile [IPSec 暗号プロファイル]ドロップダウン リストから **default** を選択して事前定義済みプロファイルを使用するか、**New IPSec Crypto Profile** [新規 - IPSec 暗号プロファイル]を選択して新しいプロファイルを定義します。認証と暗号化のオプションの詳細については、IPSec 暗号プロファイルの定義を参照してください。

STEP 7 | IPSec トンネルの確立中に、ネットワークを設定しサテライトを割り当てます。

サテライトをホストするファイアウォールに *DHCP* サーバーを設定することで、*DNS* 設定をそのローカル クライアントにプッシュするようにサテライトを設定することもできます。この設定では、サテライトはゲートウェイから収集する *DNS* 設定を *DHCP* クライアントにプッシュします。

1. GlobalProtect Configuration Gateway (GlobalProtect 設定ゲートウェイ) ダイアログで、**Satellite (サテライト)** > **Network Settings (ネットワーク設定)** の順に選択します。
2. （任意）サテライトにローカルなクライアントが企業ネットワーク上の FQDN を解決する必要がある場合、以下のいずれかの方法で、ゲートウェイが DNS 設定をサテライトにプッシュするように設定します。
   - ゲートウェイに DHCP クライアントとして設定されたインターフェイスがある場合、そのインターフェイスへの **Inheritance Source**[継承ソース] を設定し、DHCP クライアントから受信したのと同じ設定をGlobalProtect サテライトに割り当てられます。また、同じソースからDNSサフィックスを継承することもできます。

- **Primary DNS**[プライマリ DNS]、**Secondary DNS**[セカンダリ DNS]、**DNS Suffix**[DNS サフィックス] 設定を、サテライトにプッシュするように手動で定義します。

3. VPN を確立するときに、アドレスの **IP Pool**[IP プール] を指定して、サテライトのトンネル インターフェイスに割り当てるには、**Add**[追加] をクリックして使用する IP アドレス範囲を指定します。
4. トンネルを経由してルーティングする宛先サブネットを定義するには、**Access Route**（アクセス ルート）エリアで **Add**（追加）をクリックして、以下のようにルートを入力します。

   - サテライトからのすべてのトラフィックをトンネルを経由してルーティングする場合、このフィールドは空白のままにします。

     その場合、ローカル サブネット宛てのトラフィックを除くすべてのトラフィックはゲートウェイにトンネリングされます。

   - ゲートウェイを経由する一部のトラフィックのみをルーティングするには（スプリット トンネルと呼ばれます）、トンネルする必要のある宛先サブネットを指定します。この場合、サテライトは独自のルーティング テーブルを使用して、指定したアクセス ルートの宛先になっていないトラフィックをルーティングします。たとえば、企業ネットワークの宛先になっているトラフィックのみをトンネルし、ローカル サテライトを使用して安全にインターネット アクセスを有効にすることができます。
   - サテライト間のルーティングを有効にするには、各サテライトによって保護されたネットワークのサマリー ルートを入力します。

STEP 8 | （任意）ゲートウェイがサテライトから受け入れるルート（ある場合）を定義します。

デフォルトでは、ゲートウェイはサテライトが通知したルートをルーティング テーブルに追加しません。ゲートウェイがサテライトからのルートを受け入れないようにする場合、この手順を実行する必要はありません。

1. ゲートウェイがサテライトによって通知されたルートを受け入れるようにするには、**Satellite (サテライト)** > **Route Filter** の順に選択します。
2. **Accept published routes**[公開されたルートの受け入れ] チェック ボックスをオンにします。
3. サテライトによって通知されたルートのうちゲートウェイ ルーティング テーブルに追加するものをフィルタリングするには、**Add**[追加] をクリックして含めるサブネットを定義します。たとえば、すべてのサテライトが LAN 側のサブネット 192.168.x.0/24 で設定されている場合、許可されたルートとして 192.168.0.0/16 を設定すると、ゲートウェイはサテライトが 192.168.0.0/16 サブネットにある場合のみサテライトからのルートを受け入れます。

STEP 9 | ゲートウェイの設定を保存します。

1. **OK** をクリックして設定を保存し、GlobalProtect Gateway Configuration（GlobalProtect ゲートウェイ設定）ダイアログを閉じます。
2. 設定を **Commit**（コミット）します。

LSVPN の GlobalProtect ポータルの設定

GlobalProtect ポータルでは、GlobalProtect LSVPN の管理機能を提供します。LSVPN に参加するすべてのサテライト システムは、ポータルから設定情報を受信します。これには、使用可能なゲートウェイ、ゲートウェイへの接続に必要な証明書などの情報が含まれます。

以下のセクションでは、ポータルのセットアップの手順について説明します。

- LSVPN 用の GlobalProtect ポータルの前提条件となるタスク
- ポータルの設定
- サテライト設定の定義

LSVPN 用の GlobalProtect ポータルの前提条件となるタスク

GlobalProtect ポータルを設定する前に、以下のタスクを完了する必要があります。

- ポータルを構成するインターフェイスでLSVPN のインターフェイスおよびゾーンの作成します。
- GlobalProtect LSVPN コンポーネント間の SSL の有効化ポータル・サーバー証明書の SSL/TLS サービス・プロファイルの作成、ゲートウェイ・サーバー証明書の発行、および GlobalProtect サテライト用のサーバー証明書を発行するようにポータルを構成することによって行われます。
- サテライトを認証するためのポータルの設定は、ローカル・データベース認証をセットアップし、ポータルがサテライトの認証に使用する認証プロファイルを定義します。
- 「LSVPN の GlobalProtect ゲートウェイの設定」を行います。

ポータルの設定

LSVPN 用 GlobalProtect ポータルの前提条件となるタスクを完了した後に、以下のように GlobalProtect ポータルを設定します。

STEP 1 | ポータルを追加します。

1. **Network** > **GlobalProtect** > **Portals**(ネットワーク > GlobalProtect > ポータル) の順に選択し、**Add**(追加) をクリックします。
2. **General** （全般） タブで、**Name (**名前**)** フィールドにポータル名を入力します。ポータル名にスペースを含めることはできません。
3. （任意）**Location**（場所）フィールドから、このポータルが属する仮想システムを選択します。

STEP 2 | サテライトがポータルに接続できるようにネットワーク情報を指定します。

ポータル用のネットワーク インターフェイスをまだ作成していない場合は、LSVPN のインターフェイスおよびゾーンの作成の手順を参照してください。

1. サテライトがポータルへの入力アクセスに使用する **Interface**[インターフェイス] を選択します。
2. ポータへのサテライト アクセスを行うための **IP Address Type (IP** アドレス タイプ**)** および **IP address (IP** アドレス**)** を指定します。
   - IP アドレス タイプは、**IPv4**（IPv4 トラフィックの場合のみ）、**IPv6**（IPv6 トラフィックの場合のみ、または **IPv4 and IPv6**（**IPv4** および **IPv6**）です。ネットワークがデュアル スタック構成をサポートしているときは、**IPv4 and IPv6**（**IPv4** および **IPv6**）を使用します。これにより IPv4 と IPv6 が同時に動作します。
   - IP アドレスは IP アドレス タイプに対応するものでなければなりません。たとえば、IPv4 の場合は **172.16.1/0**、IPv6 の場合は **21DA:D3:0:2F3B** のように指定します。デュアル スタック構成の場合は、IPv4 アドレスと IPv6 アドレスの両方を入力します。
3. **OK** をクリックして変更を保存します。

STEP 3 | サテライトがポータルとの SSL/TLS 接続を確立できるようにするために使用するSSL/TLS Service Profile [SSL/TLS サービス プロファイル]を指定します。

ポータルおよび発行済みゲートウェイ証明書用のSSL/TLSサービス プロファイルをまだ作成していない場合は、GlobalProtect LSVPN コンポーネントへのサーバー証明書のデプロイを参照してください。

1. GlobalProtect Portal Configuration [GlobalProtectポータル設定]ダイアログで**Authentication**[認証]を選択します。
2. **SSL/TLS Service Profile**（**SSL/TLS** サービスプロファイル）を選択します。

STEP 4 | サテライトを認証するための認証プロファイルおよび任意で証明書プロファイルを指定します。

サテライトがポータルに初めて接続するときは、ローカルデータベース認証を使用して認証する必要があります *(*後続のセッションでは、ポータルによって発行されたサテライト *Cookie* が使用されます*)*。そのため、ポータル設定を保存（***OK***をクリック）する前に 認証プロファイルを設定する必要があります。

Client Authentication [クライアント認証]を**Add**[追加]し、設定を識別するための**Name**[名前]を入力して**OS**を選択します。**Satellite**[サテライト]で設定をサテライトに適用し、サテライト デバイスを認証するために使用する**Authentication Profile**[認証プロファイル]を指定します。サテライト デバイスの認証に使用するポータルの**Certificate Profile**[証明書プロファイル]を指定することもできます。

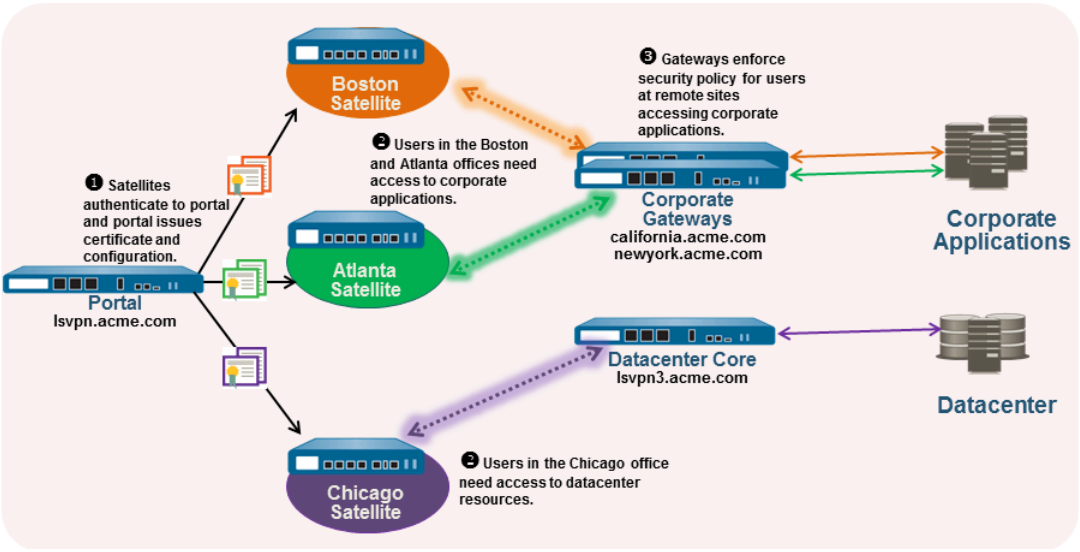
STEP 5 | サテライトにプッシュするための設定の定義を続行するか、すでにサテライト設定を作成している場合は、ポータル設定を保存します。

OK をクリックしてポータル設定を保存するか、サテライト設定の定義を続行します。

サテライト設定の定義

GlobalProtect サテライトが GlobalProtect ポータルに接続して認証に成功すると、ポータルはサテライト設定を配信し、これによってサテライトが接続できるゲートウェイが指定されます。すべてのサテライトで同じゲートウェイおよび証明書設定を使用する場合、1 つのサテライト設定を作成しておき、認証が成功したときにすべてのサテライトにそれを配信することができます。ただし、たとえばサテライトの 1 つのグループを 1 つのゲートウェイに接続し、サテライトの別のグループを別のゲートウェイに接続するなど、異なるサテライト設定が必要な場合、それぞれについて個別のサテライト設定を作成できます。ポータルは、ユーザー名/グループ名の登録またはサテライトのシリアル番号を使用して、デプロイするサテライト設定を決定します。セキュリティ ルール評価によって、ポータルはリストの先頭から一致を検索します。一致が見つかると、ポータルは対応する設定をサテライトに配信します。

例えば、以下の図は、一部の支社ではペリメータ ファイアウォールによって保護された企業アプリケーションへの VPN アクセスが必要で、別の支社ではデータセンターへの VPN アクセスが必要なネットワークを示しています。



以下の手順に従って、1 つ以上のサテライト設定を作成します。

STEP 1 | サテライト設定を追加します。

サテライト設定は、接続元サテライトにデプロイする GlobalProtect LSVPN 設定を指定します。少なくとも 1 つのサテライト設定を定義する必要があります。

1. **Network (ネットワーク)** > **GlobalProtect** > **Portals (ポータル)** の順に選択し、サテライト設定を追加するポータル設定を選択してから **Satellite (サテライト)** タブを選択します。
2. Satellite (サテライト) セクションで **Add (追加)** をクリックします。
3. **Name**（名前）に設定名を入力します。

   複数の設定を作成する予定の場合、分かりやすい名前をそれぞれの設定に定義して、区別できるようにしてください。
4. ポータルに設定の更新があるかどうかをサテライトがチェックする間隔を変更するには、**Configuration Refresh Interval (hours)**[設定の更新間隔（時間）]で値を指定します（範囲は1～48、デフォルト設定は24）。

STEP 2 | この設定をデプロイするサテライトを指定します。

ポータルは **Enrollment User/User Group** [登録ユーザー/登録ユーザー グループ]設定および **Devices** [デバイス]シリアル番号を使用してサテライトと設定を照合します。したがって、複数の設定がある場合、適切に順序付けする必要があります。ポータルが一致を認めるとすぐに、設定が配信されます。そのため、より具体的な設定が、一般的な設定よりも優先される必要があります。サテライト構成のリストを注文する手順については、ステップ 5 を参照してください。

以下のようにサテライト設定の一致基準を指定します。

- この設定を特定のシリアル番号を持つサテライトに制限するには、 **Devices** [デバイス]タブを選択して **Add** [追加]をクリックし、シリアル番号を入力します（サテライト ホスト名はサテライトが接続したときに自動的に追加されるため、入力する必要はありません）。この設定を受信するサテライトごとにこの手順を繰り返します。
- **Enrollment User/User Group** [登録ユーザー/登録ユーザー グループ]タブを選択して **Add** [追加]をクリックし、この設定を受信するユーザーまたはグループを選択します。シリアル番号に一致しないサテライトは、ここで指定したユーザー（個人ユーザーまたはグループ メンバー）として認証する必要があります。

設定を特定のグループに制限するには、ユーザー対グループのマッピングを行う必要があります。

STEP 3 | この設定を持つサテライトが VPN トンネルを確立できるゲートウェイを指定します。

ゲートウェイによって公開されたルートはスタティック ルートとしてサテライトにインストールされます。スタティック ルートのメトリックは、ルーティングの優先順位の *10* 倍です。複数のゲートウェイがある場合、必ずルーティングの優先順位も設定して、バックアップ ゲートウェイによって通知されるルートがプライマリ ゲートウェイによって通知される同じルートよりも高いメトリックになるようにしてください。たとえば、プライマリ ゲートウェイとバックアップ ゲートウェイのルーターの優先順位をそれぞれ *1* と *10* に設定した場合、サテライトは *10* をプライマリ ゲートウェイのメトリックとして使用し、*100* をバックアップ ゲートウェイのメトリックとして使用します。

1. **Gateways**[ゲートウェイ] タブで **Add**[追加] をクリックします。
2. **Name**（名前）フィールドに分かりやすいゲートウェイ名を入力します。ここで入力する名前は、ゲートウェイを設定したときに定義した名前と一致し、ゲートウェイの場所を識別できるように分かりやすい名前にする必要があります。
3. ゲートウェイを設定するインターフェイスの FQDN または IP アドレスを **Gateways**（ゲートウェイ）フィールドに入力します。指定するアドレスは、ゲートウェイ サーバー証明書のコモンネーム（CN）に完全に一致する必要があります。
4. (任意) 設定に 2 つ以上のゲートウェイを追加している場合、**Routing Priority**[ルーターの優先順位] を使用するとサテライトが優先するゲートウェイを選択できます。1 ～ 25 の範囲で値を入力します。小さい数値の方が優先順位が高くなります（つまり、すべてのゲートウェイが使用できる場合、サテライトが接続するゲートウェイとなります）。サテライトは、ルーティング メトリックを算出するためにルーティングの優先順位を 10 倍します。

STEP 4 | サテライトの設定を保存します。

1. **OK** をクリックして、サテライト設定を保存します。
2. 別のサテライト設定を追加する場合、前の各ステップを繰り返します。

STEP 5 | 適切な設定が各サテライトにデプロイされるように、サテライト設定を並べ替えます。

- サテライト設定を設定のリストの上に移動するには、設定を選択して **Move Up**[上へ] をクリックします。
- サテライト設定を設定のリストの下に移動するには、設定を選択して **Move Down**[下へ] をクリックします。

STEP 6 | サテライトが LSVPN に参加するために必要な証明書を指定します。

1. **Trusted Root CA**[信頼されたルート CA] フィールドで、**Add**[追加] をクリックしてからゲートウェイ サーバー証明書を発行するために使用する CA 証明書を選択します。ポータルは、ここで追加したルート CA 証明書を設定の一部としてすべてのサテライトにデプロイするため、サテライトはゲートウェイとの SSL 接続を確立できます。ベスト プラクティスとして、すべてのゲートウェイに同じ発行者を使用します。

2. **Client Certificate**[クライアント証明書]の配布方法を選択します。
   - **To store the client certificates on the portal**[クライアント証明書をポータルに保存]—**Issuing Certificate**[証明書の発行] ドロップダウン リストから**Local**[ローカル]を選択し、認証に成功したときにポータルがクライアント証明書をサテライトに発行するために使用するルート CA 証明書を選択します。

     ゲートウェイ サーバー証明書を発行するために使用するルート *CA* 証明書がポータルにない場合、ここで***Import****[インポート]*できます。ルート *CA* 証明書のインポート方法の詳細は、GlobalProtect LSVPN コンポーネント間の SSL の有効化 を参照してください。

   - **To enable the portal to act as a SCEP client to dynamically request and issue client certificates**[クライアント証明書を直接リクエスト・発行するSCEPクライアントとしてポータルが振る舞うようにする]—**SCEP**を選択し、SCEPサーバーにCSRを生成するために使用した**SCEP**プロファイルを選択します。

     ポータルが*SCEP*クライアントとして振る舞うようセットアップを行っていない場合は、ここで***New*** *[新規] SCEP*プロファイルを追加することができます。詳細についてはSCEPを使用してクライアント証明書をGlobalProtectサテライトにデプロイを参照してください。

STEP 7 | ポータルの設定を保存します。

1. **OK** をクリックして設定を保存し、GlobalProtect Portal Configuration（GlobalProtect ポータル設定）ダイアログを閉じます。
2. 変更を **Commit (コミット)**します。

LSVPN に参加するためのサテライトの準備

サテライトが LSVPN に参加するためには最小限の設定が必要です。必要な設定は最小限であるため、インストールのために支社に配送する前にサテライトを事前設定できます。

STEP 1 | レイヤ 3 インターフェイスの設定

これは、サテライトがポータルおよびゲートウェイに接続するために使用する物理インターフェイスです。このインターフェイスは、ローカルの信頼されるネットワークの外部からのアクセスが可能なゾーンにある必要があります。企業ゲートウェイを宛先とするトラフィックを可視化して制御するために、VPN 接続専用のゾーンを作成することをお勧めします。

STEP 2 | GlobalProtect ゲートウェイとの VPN トンネルを確立するために使用するトンネルの論理トンネル インターフェイスを設定します。

ダイナミック ルーティングを使用する予定がなければ、トンネル インターフェイスに *IP* アドレスは必要ありません。ただし、*IP* アドレスをトンネル インターフェイスに割り当てると、接続の問題をトラブルシューティングするときに役立つ場合があります。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Tunnel (トンネル)** の順に選択し、**Add(追加)** をクリックします。
2. **Interface Name**（インターフェイス名）フィールドで、**.2**などの数値のサフィックスを指定します。
3. **Config** [設定]タブで **Security Zone** [セキュリティ ゾーン]ドロップダウン リストを展開し、既存のゾーンを選択するか、**New Zone** [新規ゾーン]をクリックして **Name** [名前]フィールドで新しいゾーンの名前（「*lsvpnsat*」など）を定義して VPN トンネル トラフィック用の個別のゾーンを作成します。
4. **Virtual Router**（仮想ルーター）ドロップダウン リストで、**defaul**（デフォルト）を選択します。
5. （任意）トンネル インターフェイスに IP アドレスを割り当てるには：
   - IPv4 アドレスの場合、**IPv4** を選択して、インターフェイスに割り当てる IP アドレスとネットワーク マスクを **Add**（追加）します（例: 203.0.11.100/24）。
   - IPv6 アドレスの場合、**IPv6** を選択して、**Enable IPv6 on the interface**（インターフェースでの **IPv6** の有効化）を行い、インターフェイスに割り当てる IP アドレスとネットワーク マスクを **Add**（追加）します（例：2001:1890:12f2:11::10.1.8.160/80）。
6. インターフェイス設定を保存するには、**OK** をクリックします。

STEP 3 | サテライトによって信頼されないルート CA を使用してポータル サーバー証明書を生成した場合（たとえば、自己署名証明書を使用した場合）、ポータル サーバー証明書を発行するために使用するルート CA 証明書をインポートします。

ルート CA 証明書は、サテライトがポータルとの最初の接続を確立して LSVPN 設定を取得できるようにするために必要です。

1. ポータル サーバー証明書を生成するために使用された CA 証明書をダウンロードします。自己署名証明書を使用している場合、以下のようにルート CA 証明書をポータルからエクスポートします。
   1. **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択します。
   2. CA certificate [CA 証明書]を選択して **Export** [エクスポート]をクリックします。
   3. **File Format** [ファイル フォーマット]ドロップダウン リストから **Base64 Encoded Certificate (PEM)** [Base64 エンコード済み証明書（PEM）]を選択し、**OK** をクリックして証明書をダウンロードします（秘密鍵をエクスポートする必要はありません）
2. 以下のように、エクスポートしたルート CA 証明書を各サテライトにインポートします。
   1. **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択し、**Import**（インポート）をクリックします。
   2. **Certificate Name**（証明書名）フィールドに、クライアント CA 証明書であることを識別できる名前を入力します。
   3. **Browse**（参照）をクリックして、CA からダウンロードした **Certificate File**（証明書ファイル）を選択します。
   4. **Base64 Encoded Certificate (PEM)**（**Base64** エンコード済み証明書（**PEM**））を **File Format**（ファイル フォーマット）フィールドで選択し、**OK** をクリックします。
   5. **Device Certificates**（デバイス証明書）タブで、先ほどインポートした証明書を選択して開きます。
   6. **Trusted Root CA**（信頼されたルート **CA**）を選択して **OK** をクリックします。

STEP 4 | IPSec トンネル設定を設定します。

1. **Network (ネットワーク)** > **IPSec Tunnels (IPSec トンネル)** の順に選択して **Add (追加)** をクリックします。
2. **General**[全般] タブの **Name**[名前] フィールドに IPSec 設定の分かりやすい名前を入力します。
3. サテライトについて作成した **Tunnel Interface**[トンネル インターフェイス] を選択します。
4. **Type**[タイプ] として **GlobalProtect Satellite**[GlobalProtect サテライト] を選択します。
5. ポータルの IP アドレスまたは FQDN を **Portal Address**[ポータル アドレス] として入力します。
6. サテライト用に設定したレイヤー 3 の **Interface**[インターフェイス] を選択します。
7. 選択したインターフェイスで使用する **IP Address (IP アドレス)** を選択します。**IPv4** アドレス、**IPv6** アドレス、あるいはその両方を選択できます。**IPv6 preferred for portal registration (ポータル登録で IPv6 を優先)** したい場合に指定します。

STEP 5 | （任意）ゲートウェイにローカル ルートを公開するようにサテライトを設定します。

ルートをゲートウェイにプッシュすると、サテライトにローカルなサブネットへのトラフィックがゲートウェイを経由できるようになります。ただし、LSVPN の GlobalProtect ゲートウェイの設定の説明に従ってルートを受け入れるようにゲートウェイを設定する必要もあります。

1. サテライトがルートをゲートウェイにプッシュできるようにするには、**Advanced**[詳細] タブで **Publish all static and connected routes to Gateway**[静的なすべての接続済みルートをゲートウェイに公開] をオンにします。

   このチェック ボックスをオンにすると、ファイアウォールは静的なすべての接続済みルートをサテライトからゲートウェイに転送します。ただし、ルーティング ループの発生を回避するため、以下のようないくつかのルート フィルタが適用されます。

   - デフォルト ルート
   - トンネル インターフェイスに関連付けられた仮想ルーター以外の仮想ルーター内のルート
   - トンネル インターフェイスを使用するルート
   - トンネル インターフェイスに関連付けらえた物理インターフェイスを使用するルート
2. （任意）すべてのルートではなく特定のサブネットのルートのみをプッシュするには、Subnet [サブネット] セクションで **Add**[追加] をクリックして公開するサブネット ルートを指定します。

STEP 6 | サテライトの設定を保存します。

1. **OK** をクリックして、IPSec トンネル設定を保存します。
2. **Commit**（コミット）をクリックします。

STEP 7 | 必要に応じて、認証情報を入力し、サテライトがポータルの認証を受けられるようにします。

ポータルに対して初めて, 認証を行うには 、サテライト管理者がローカル・データベース内のサテライト管理者アカウントに関連付けられたユーザー名とパスワードを提供する必要があります。

1. **Network (**ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)** の順に選択し、LSVPN 用に作成したトンネル設定の Status (ステータス) 列で **Gateway Info (**ゲートウェイ情報**)** リンクをクリックします。
2. **Portal Status** [ポータル状態]フィールドで **enter credentials** [資格情報の入力]リンクをクリックし、サテライトがポータルの認証を受けられるようにするために必要なユーザー名とパスワードを入力します。

   サテライトがポータルの認証を受けると、その署名付き証明書と設定を受信し、それを使用してゲートウェイに接続します。トンネルが確立され **Status**[状態] が **Active**[アクティブ] に変更されます。

LSVPN 設定の確認

ポータル、ゲートウェイ、サテライトを設定したら、サテライトがポータルおよびゲートウェイに接続して、ゲートウェイとの VPN トンネルを確立できることを確認します。

STEP 1 | サテライトとポータルの接続を確認します。

ポータルをホストするファイアウォールから、**Network (ネットワーク)** > **GlobalProtect** > **Portal (ポータル)** の順に選択してポータル設定エントリの Info (情報) 列で **Satellite Info (サテライト情報)** をクリックして、サテライトが接続に成功したことを確認します。

STEP 2 | サテライトとゲートウェイの接続を確認します。

ゲートウェイをホストするファイアウォールから、**Network (ネットワーク)** > **GlobalProtect** > **Gateways (ゲートウェイ)** の順に選択してゲートウェイ設定エントリの Info (情報) 列で **Satellite Info (サテライト情報)** をクリックして、サテライトが VPN トンネルを確立できることを確認します。ゲートウェイとのトンネルを正常に確立したサテライトが **Active Satellites**[アクティブ サテライト] タブに表示されます。

STEP 3 | サテライトでの LSVPN トンネルの状態を確認します。

サテライトをホストする各ファイアウォールで、**Network (ネットワーク)** > **IPSec Tunnels (IPSec トンネル)** の順に選択することによってトンネルの状態を確認し、緑色のアイコンでアクティブな状態が示されていることを確認します。

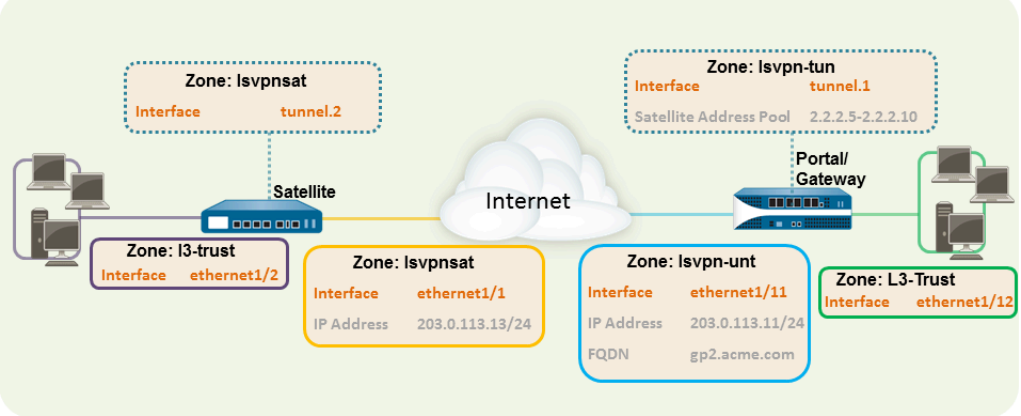
LSVPN のクイック設定

以下のセクションでは、一般的な GlobalProtect LSVPN のデプロイメント設定のための手順を説明します。

- スタティック ルーティングを使用した基本的な LSVPN 設定
- ダイナミック ルーティングを使用した高度な LSVPN 設定
- iBGP を使用した高度な LSVPN 設定

スタティック ルーティングを使用した基本的な LSVPN 設定

このクイック設定では、最短時間で LSVPN を起動して実行する方法を示します。この例では、企業の本社側で 1 つのファイアウォールをポータルおよびゲートウェイの両方として設定します。サテライトは、最小限の設定で素早く簡単にデプロイすることができ、最適な拡張性が得られます。



以下のワークフローは、この基本的な設定をセットアップするための手順を示しています。

STEP 1 | レイヤー 3 インターフェイスを設定します。

この例では、ポータル/ゲートウェイのレイヤー 3 インターフェイスで以下の設定が必要です。

- **Interface(インターフェイス)**—ethernet1/11
- **Security Zone**[セキュリティ ゾーン] — lsvpn-tun
- **IPv4** — 203.0.113.11/24

STEP 2 | GlobalProtect ゲートウェイをホストするファイアウォールで、GlobalProtect サテライトによって確立される VPN トンネルを終端する論理トンネル インターフェイスを設定します。

VPN を経由して接続するユーザーおよびグループを可視化するために、*VPN* トンネルを終端するゾーンで ユーザー *ID* を有効にします。

この例では、ポータル/ゲートウェイのトンネル インターフェイスで以下の設定が必要です。

- **Interface**[インターフェイス] — tunnel.1
- **Security Zone**[セキュリティ ゾーン] — lsvpn-tun

STEP 3 | セキュリティ ポリシー ルールを作成して、トンネルが終端する VPN ゾーン（lsvpn-tun）と企業アプリケーションが存在する Trust ゾーン（L3-Trust）間でトラフィックをやり取りできるようにします。

セキュリティ ポリシー ルールの作成を参照してください。

STEP 4 | ポータル/ゲートウェイに SSL/TLS Service profile [SSL/TLS サービス プロファイル]を割り当てます。プロファイルは自己署名サーバー証明書を参照する必要があります。

証明書のサブジェクト名は、ポータル/ゲートウェイについて作成したレイヤー 3 インターフェイスの FQDN または IP アドレスに一致する必要があります。

1. GlobalProtect ポータルをホストするファイアウォールで、GlobalProtect コンポーネントの証明書に署名するためにルート CA 証明書を作成する必要があります。この例では、ルート CA 証明書「**lsvpn-CA**」がポータル/ゲートウェイのサーバー証明書を発行するために使用されます。さらに、ポータルはこのルート CA 証明書を使用してサテライトからの CSR に署名します。
2. GlobalProtect ポータルおよびゲートウェイの SSL/TLS サービス プロファイルを作成します。

   この例ではポータルとゲートウェイが同じインターフェイス上にあるため、同じサーバー証明書を使用する SSL/TLS サービス プロファイルを共有できます。この例でのプロファイル名は「**lsvpnserver**」です。

STEP 5 | 証明書プロファイルを作成します。

この例では、証明書プロファイル「**lsvpn-profile**」がルート CA 証明書「**lsvpn-CA**」を参照します。ゲートウェイはこの証明書プロファイルを使用して、VPN トンネルの確立を試みるサテライトを認証します。

STEP 6 | ローカルデータベース認証を使用してサテライトを認証するようにポータルを設定します。

STEP 7 | LSVPN の GlobalProtect ゲートウェイを設定します。

Network（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ）を選択し、設定を**Add**（追加）します。この例では、以下のゲートウェイ設定が必要です。

- **Interface(インターフェイス)**—ethernet1/11
- **IP Address**[IP アドレス] — 203.0.113.11/24
- **SSL/TLS Server Profile** [SSL/TLS サーバー プロファイル] — lsvpnserver
- **Certificate Profile**[証明書プロファイル] — lsvpn-profile
- **Tunnel Interface**(トンネル インターフェイス)—tunnel.1
- **Primary DNS**[プライマリ DNS]/**Secondary DNS**[セカンダリ DNS] — 4.2.2.1/4.2.2.2
- **IP Pool**[IP プール] — 2.2.2.111-2.2.2.120
- **Access Route**[アクセス ルート] — 10.2.10.0/24

STEP 8 | ポータルの設定を行います。

Network（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）を選択し、設定を**Add**（追加）します。この例では、以下のポータル設定が必要です。

- **Interface(インターフェイス)**—ethernet1/11
- **IP Address**[IP アドレス] — 203.0.113.11/24
- **SSL/TLS Server Profile** [SSL/TLS サーバー プロファイル] — lsvpnserver
- **Authentication Profile**[認証プロファイル設定] — lsvpn-sat

STEP 9 | サテライト設定の定義を行います。

ポータル設定の **Satellite**（サテライト）タブで、Satellite（サテライト）設定およびTrusted Root CA（信頼されたルート CA）を **Add**（追加）し、ポータルがサテライトの証明書の発行に使用する CA を指定します。この例では、必要な設定は以下のようになります。

- **Gateway**[ゲートウェイ] — 203.0.113.11
- **Issuing Certificate**[証明書の発行] — lsvpn-CA
- **Trusted Root CA**[信頼されたルート CA] — lsvpn-CA

STEP 10 | LSVPN に参加するためのサテライトを準備します。

この例のサテライト設定では、以下の設定が必要です。

インターフェイス設定

- レイヤー 3 インターフェイス – ethernet1/1、203.0.113.13/24
- トンネル インターフェイス – tunnel.2
- ゾーン – lsvpnsat

ポータルからのルート CA 証明書

- lsvpn-CA

IPSec トンネル設定

- **Tunnel Interface**(トンネル インターフェイス)–tunnel.2
- **Portal Address**[ポータル アドレス] – 203.0.113.11
- インターフェイス –ethernet1/1
- **Local IP Address**[ローカル IP アドレス] – 203.0.113.13/24
- **Publish all static and connected routes to Gateway**[静的なすべての接続済みルートをゲートウェイに公開] – オン

ダイナミック ルーティングを使用した高度な LSVPN 設定

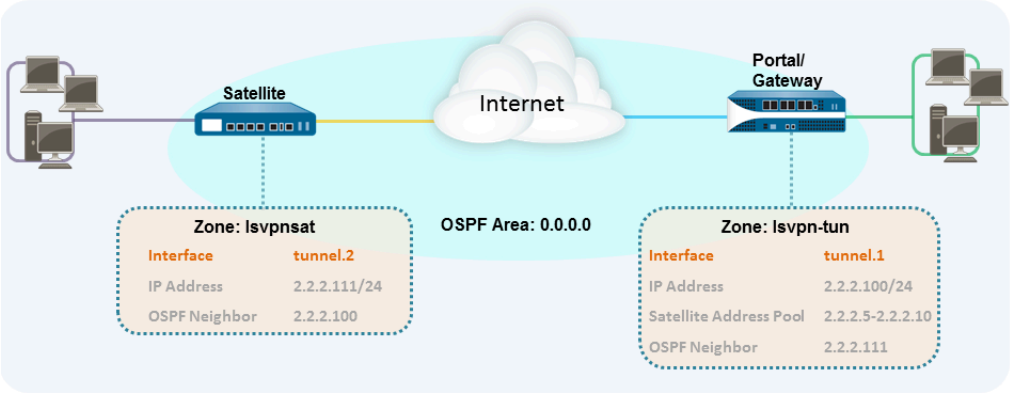
複数のゲートウェイと多数のサテライトを持つ大規模な LSVPN のデプロイメントでは、初期設定に少し時間をかけてダイナミック ルーティングをセットアップすることで、アクセス ルートが動的に更新されるようになるため、ゲートウェイ設定のメンテナンスが簡略化されます。以下の設定例では、基本的な LSVPN 設定を拡張して OSPF をダイナミック ルーティング プロトコルとして設定する方法を示しています。

ダイナミック ルーティングに OSPF を使用するように LSVPN をセットアップするには、ゲートウェイおよびサテライトで以下の追加手順が必要です。

- すべてのゲートウェイおよびサテライトで、トンネル インターフェイスに IP アドレスを手動で割り当てる。
- すべてのゲートウェイおよびサテライトで仮想ルーターの OSPF ポイントツーマルチポイント（P2MP）を設定する。さらに、各ゲートウェイでの OSPF 設定の一環として、各サテライトのトンネル IP アドレスを OSPF ネイバーとして手動で定義する必要があります。同様に、各サテライトで、各ゲートウェイのトンネル IP アドレスを OSPF ネイバーとして手動で定義する必要があります。

ダイナミック ルーティングでは LSVPN の初期設定中に追加のセットアップが必要ですが、これにより、ネットワークでトポロジが変更されたときにルートを最新の状態に保つためのメンテナンス タスクが軽減されます。

以下の図は、LSVPN ダイナミック ルーティング設定を示しています。この例は、OSPF を VPN のダイナミック ルーティング プロトコルとして設定する方法を示しています。



LSVPN の基本設定については、「静的ルーティングを使用した基本的な LSVPN 設定」の手順に従ってください。基本的なセットアップを行った後で、以下のワークフローの手順を実行して、スタティック ルーティングではなくダイナミック ルーティングを使用するように設定を拡張できます。

STEP 1 | IP アドレスを各ゲートウェイおよび各サテライトのトンネル インターフェイス設定に追加します。

各ゲートウェイおよび各サテライトで以下の手順を実行します。

1. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Tunnel**（トンネル）を選択し、LSVPN 用に作成したトンネル設定を選択して、トンネル インターフェイス ダイアログを開きます。

   トンネル インターフェイスをまだ作成していない場合は、LSVPNのインターフェイスと Zones を作成するの 2 のステップを参照してください。
2. **IPv4** タブで **Add**[追加] をクリックして、IP アドレスとサブネット マスクを入力します。たとえば、ゲートウェイ トンネル インターフェイスの IP アドレスを追加するには「2.2.2.100/24」と入力します。
3. **OK** をクリックして設定を保存します。

STEP 2 | ゲートウェイでダイナミック ルーティング プロトコルを設定します。

ゲートウェイで OSPF を設定するには、以下の手順を実行します。

1. **Network**（ネットワーク） > **Virtual Routers**（仮想ルーター） を選択し、VPN インターフェイスに関連付けられた仮想ルーターを選択します。
2. **Areas**[エリア] タブで **Add**[追加] をクリックしてバックボーン エリアを作成するか、すでに設定している場合は、エリア ID をクリックして編集します。
3. 新しいエリアを作成している場合、**Area ID**[エリア ID] を **Type**[タイプ] タブに入力します。
4. **Interface**[インターフェイス] タブで **Add**[追加] をクリックし、LSVPN について作成したトンネルの **Interface**[インターフェイス] を選択します。
5. **Link Type**[リンク タイプ] として **p2mp** を選択します。
6. Neighbors （ネイバー）セクションで **Add** （追加）をクリックし、各サテライトのトンネル インターフェイスの IP アドレスを「2.2.2.111」のように入力します。
7. **OK** を 2 回クリックして仮想ルーター設定を保存してから、**Commit** [コミット]をクリックして変更内容をゲートウェイにコミットします。
8. この手順を、新しいサテライトを LSVPN に追加するごとに繰り返します。

STEP 3 | サテライトでダイナミック ルーティング プロトコルを設定します。

サテライトで OSPF を設定するには、以下の手順を実行します。

1. **Network**（ネットワーク） > **Virtual Routers**（仮想ルーター） を選択し、VPN インターフェイスに関連付けられた仮想ルーターを選択します。
2. **Areas**[エリア] タブで **Add**[追加] をクリックしてバックボーン エリアを作成するか、すでに設定している場合は、エリア ID をクリックして編集します。
3. 新しいエリアを作成している場合、**Area ID**[エリア ID] を **Type**[タイプ] タブに入力します。
4. **Interface**[インターフェイス] タブで **Add**[追加] をクリックし、LSVPN について作成したトンネルの **Interface**[インターフェイス] を選択します。
5. **Link Type**[リンク タイプ] として **p2mp** を選択します。
6. Neighbors [ネイバー] セクションで **Add**[追加] をクリックし、各 GlobalProtect ゲートウェイのトンネル インターフェイスの IP アドレスを「2.2.2.100」のように入力します。
7. **OK** を 2 回クリックして仮想ルーター設定を保存してから、**Commit** [コミット]をクリックして変更内容をゲートウェイにコミットします。
8. この手順を、新しいゲートウェイを追加するごとに繰り返します。

STEP 4 | ゲートウェイとサテライトがルーターに隣接できることを確認します。

- 各サテライトおよび各ゲートウェイで、ピア隣接が形成され、ルーティング テーブル エントリがピアについて作成されていることを確認します（つまり、サテライトにゲートウェイへのルートがあり、ゲートウェイにサテライトへのルートがある）。**Network**（ネットワーク） > **Virtual Router**（仮想ルーター） を選択し、LSVPN について使用している仮想ルーターの **More Runtime Stats**（詳細ランタイム状態）リンクを

クリックします。Routing [ルーティング] タブで、LSVPN ピアにルートがあることを確認します。

- **OSPF** > **Interface**（インターフェイス） タブで、**Type**（タイプ）が **p2mp** であることを確認します。
- **OSPF** > **Neighbor**（ネイバー） タブで、ゲートウェイをホストするファイアウォールがサテライトをホストするファイアウォールとルーター隣接を確立し、その逆の隣接も確立していることを確認します。また、**Status**[状態] が **Full**[フル] であり、フル隣接が確立されていることも確認します。

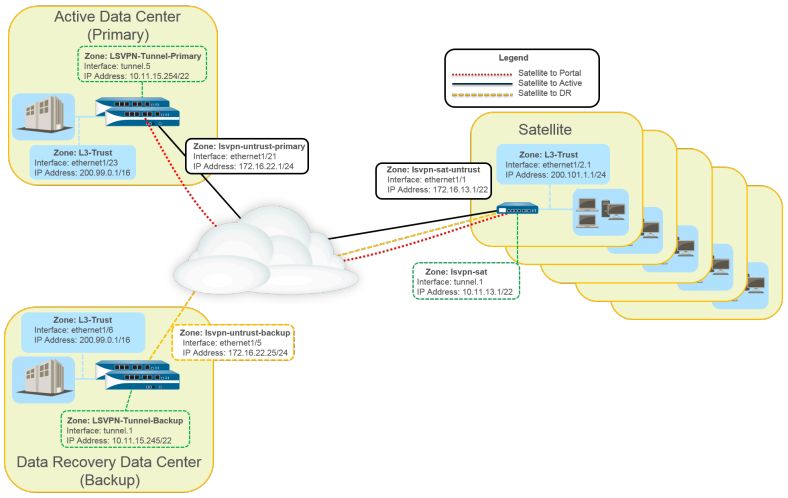
iBGP を使用した高度な LSVPN 設定

このユース ケースは、GlobalProtect LSVPN が分散オフィスの場所を、重要なアプリケーションを格納するプライマリおよび災害復旧データセンターと、内部ボーダゲートウェイ プロトコル（iBGP）がデプロイおよび維持を容易にする方法を安全に接続する方法を示しています。この方法を使用すると、1 つのゲートウェイに接続する最大 500 のサテライト オフィスを拡張できます。

BGP はスケーラビリティの高い動的ルーティング プロトコルで、LSVPN などのハブアンドスポーク デプロイメントに最適です。追加のサテライト ファイアウォールを、動的ルーティング プロトコルとして、デプロイしやすくすることで、アクセス ルート（静的ルート）に関連する諸経費を大幅に削減します。BGP は、複数の調整可能なタイマー、ルート ダンプニング、およびルート更新などのルート フィルタリング機能により、RIP や OSPF などの他のルーティング プロトコルよりも高いルーティング プレフィクスに拡張されます。iBGP の場合、LSVPN デプロイメントのすべてのサテライトとゲートウェイを含むピア グループは、トンネル エンドポイント上で隣接関係を確立します。プロトコルは、ルート広告、更新、およびコンバージェンスを暗黙的に制御します。

この設定例では、PA-5200ァイアウォールのアクティブ/パッシブ HA ペアがプライマリ（アクティブ）データセンターにデプロイされ、ポータルおよびプライマリ ゲートウェイとして機能します。災害復旧データセンターには、バックアップ LSVPN ゲートウェイとして機能するアクティブ/パッシブ HA ペアに 2 つの PA-5200 もあります。このポータルとゲートウェイは、ブランチ オフィスに LSVPN サテライトとしてデプロイされた 500 台の PA-220 を提供します。

どちらのデータセンター サイトでも、ルートは宣伝されていますが、指標は異なります。その結果、サテライトはアクティブなデータセンターのルートを優先してインストールします。ただし、バックアップ ルートはローカル ルーティング情報ベース（RIB）にも存在します。アクティブなデータセンターに障害が発生すると、そのデータセンターによってアドバタイズされたルートが削除され、災害復旧データセンターのルートからのルートに置き換えられます。フェイルオーバー時間は、iBGP 時間の選択と iBGP に関連するルーティング収束に依存します。



次のワークフローは、このデプロイメントを設定するためのステップを示しています。

STEP 1 | LSVPN のインターフェイスおよびゾーンを作成します。

ポータルおよびプライマリ ゲートウェイ：

- ゾーン：LSVPN-Untrust-Primary
- インターフェイス: ethernet1/21
- IPv4：172.16.22.1/24
- ゾーン：l3-trust
- インターフェイス: ethernet1/23
- **IPv4**：200.99.0.1/16

バックアップ ゲートウェイ：

- ゾーン：LSVPN-Untrust-Primary
- インターフェイス: ethernet1/5
- **IPv4**：172.16.22.25/24
- ゾーン：l3-trust
- インターフェイス: ethernet1/6
- **IPv4**：200.99.0.1/16

サテライト：

- ゾーン：LSVPN-Sat-Untrust
- インターフェイス: ethernet1/1
- **IPv4**：172.16.13.1/22
- ゾーン：l3-trust
- インターフェイス: ethernet1/2.1
- **IPv4**：200.101.1.1/24

各サテライトのゾーン、インターフェイス、および *IP* アドレスを設定します。インターフェースとローカル *IP* アドレスは、各サテライトごとに異なります。このインターフェイスは、ポータルとゲートウェイへの *VPN* 接続に使用されます。

STEP 2 | GlobalProtect ゲートウェイをホストするファイアウォールで、GlobalProtect サテライトによって確立される VPN トンネルを終端する論理トンネル インターフェイスを設定します。

プライマリ ゲートウェイ ：

- インターフェイス：tunnel.5
- **IPv4**：10.11.15.254/22
- ゾーン：LSVPN-Tunnel-Primary

バックアップ ゲートウェイ：

- インターフェイス：tunnel.1
- **IPv4**：10.11.15.245/22
- ゾーン：LSVPN-Tunnel-Backup

STEP 3 | GlobalProtect LSVPN コンポーネント間の SSL を有効化します。

ゲートウェイは、自己署名付きルート認証局（CA）を使用して、GlobalProtect LSVPN 内のサテライトの証明書を発行します。1 つのファイアウォールにはポータルとプライマリ ゲートウェイが格納されているため、1 つの証明書がサテライトの認証に使用されます。同じ CA を使用して、バックアップ ゲートウェイ用の証明書を生成します。CA は、ポータルからサテライトにプッシュされた証明書を生成し、サテライトがゲートウェイに対して認証するために使用します。

また、バックアップ ゲートウェイ用の同じ CA から証明書を生成し、サテライトで認証できるようにする必要があります。

1. GlobalProtect ポータルをホストするファイアウォールで、GlobalProtect コンポーネントの証明書に署名するためにルート CA 証明書を作成する必要があります。この例では、ルート CA 証明書は CA-cert と呼ばれています。
2. GlobalProtect ポータルおよびゲートウェイの SSL/TLS サービス プロファイルを作成します。GlobalProtect ポータルとプライマリ ゲートウェイが同じファイアウォール インターフェイスにあるため、両方のコンポーネントについて同じサーバー証明書を使用できます。
   - ルート **CA** 証明書：CA 証明書
   - 証明書名：LSVPN-Scale
3. 自己署名サーバー証明書をゲートウェイにデプロイします。
4. LSVPN コンポーネントのサーバー証明書を発行するために使用するルート CA 証明書をインポートします。
5. 証明書プロファイルを作成します。
6. 次の設定を使用して、バックアップ ゲートウェイでステップ 2～5 を繰り返します。
   - ルート **CA** 証明書：CA 証明書
   - 証明書名：LSVPN-back-GW-cert

STEP 4 | LSVPN の GlobalProtect ゲートウェイを設定します。

1. **Network** > **GlobalProtect** > **Gateways**(ネットワーク > GlobalProtect > ゲートウェイ) の順に選択し、**Add(追加)** をクリックします。
2. **General**（全般）タブで、プライマリ ゲートウェイの **LSVPN-Scale** の名前を付けます。
3. **Network Settings**（ネットワーク設定）で、**ethernet1/21**をプライマリ ゲートウェイのインターフェイスとして選択して、**172.16.22.1/24** を IP アドレスとして入力します。
4. **Authentication**タブで、3 で作成した LSVPN-Scale 証明書を選択します。
5. **Satellite**（サテライト） > **Tunnel Settings**（トンネル設定）を選択してから **Tunnel Configuration**（トンネル構成）を選択します。**Tunnel Interface**（トンネル インターフェイス）を tunnel.5 に設定します。このユース ケースのすべてのサテライトは 1 つのゲートウェイに接続するため、1 つのサテライト設定が必要です。サテライトはシリアル番号に基づいて照合されるため、サテライトはユーザーとして認証する必要はありません。
6. **Satellite**（サテライト） > **Network Settings**（ネットワーク設定）で、VPN 接続が確立されたら、サテライトのトンネル インターフェイスに割り当てる IP アドレスのプールを定義します。このユース ケースでは動的ルーティングが使用されるため、アクセス ルートの設定は空白のままです。
7. 次の設定を使用して、バックアップ ゲートウェイでステップ 1～5 を繰り返します:
   - **Name**(名前)：LSVPN-backup
   - ゲートウェイ インターフェイス：ethernet1/5
   - ゲートウェイ **IP**：172.16.22.25/24
   - サーバー証明書：LSVPN-backup-GW-cert
   - トンネル インターフェイス：tunnel.1

STEP 5 | iBGP をプライマリー ゲートウェイとバックアップ ゲートウェイで設定し、再配信プロファイルを追加して、サテライトがローカル ルートをゲートウェイに戻すことができるようにします。

各サテライト オフィスは独自のネットワークとファイアウォールを管理しているため、ToAllSat という再配信プロファイルはローカル ルートを GlobalProtect ゲートウェイに再配信するように設定されています。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、さらに仮想ルーターを **Add**（追加）します。
2. **Router Settings**（ルーター設定）で、仮想ルーターの **Name**（名前） と **Interface**（インターフェイス）を追加します。
3. **Redistribution Profile**（再配信プロファイル）で、**Add**（追加）を選択します。
   1. 再配信プロファイルに **ToAllSat** という名前を付け、 **Priority**（優先度）を 1 に設定します。
   2. 再配信を **Redist** に設定します。
   3. インターフェイスのドロップダウン リストで**ethernet1/23** を **Add**（追加）します。
   4. **OK** をクリックします。
4. BGP を設定するには、仮想ルーターで **BGP** を選択します。
   1. **BGP** > **General**（全般）で、**Enable**（有効）を選択します。
   2. ゲートウェイ IP アドレスを **Router ID**（ルーター ID）を（**172.16.22.1**）、**1000** を **AS Number**（**AS** 番号） で入力します。
   3. オプション セクションで、**Install Route**（ルートのインストール）を選択します。
   4. **BGP** > **Peer Group**（ピア グループ）で、ゲートウェイに接続するすべてのサテライトを含むピア グループの **Add**（追加）をクリックします。
   5. **BGP** > **Redist Rules**（**Redist Rules**（**Redist** ルール）で、以前に作成した **ToAllSat** 再配信プロファイルを **Add**（追加）します。
5. **OK** をクリックします。
6. 再配信プロファイルに対して **ethernet1/6** を使用するバックアップ ゲートウェイで、ステップ 1～5 を繰り返します。

STEP 6 | LSVPN に参加するためのサテライトを準備します。

表示中の設定は、サテライトのサンプルです。

この設定を、新しいサテライトを LSVPN デプロイメントに追加するごとに繰り返します。

1. ゲートウェイへの VPN 接続のトンネル エンドポイントとしてトンネル インターフェイスを設定します。
2. IPSec トンネル タイプを GlobalProtect サテライトに設定し、GlobalProtect Portal の IP アドレスを入力します。
3. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、さらに仮想ルーターを **Add**（追加）します。
4. **Router Settings**（ルーター設定）で、仮想ルーターの **Name**（名前） と **Interface**（インターフェイス）を追加します。
5. **Virtual Router**（仮想ルーター） > **Redistribution Profile**（再配信プロファイル）を選択して、次の設定を含むプロファイルを **Add**（追加）します。
   1. 再配信プロファイルに **ToLSVPNGW** という名前を付け、**Priority**（優先度）を 1 に設定します。
   2. **Interfaces**（インターフェイス） **ethernet1/2.1** を **Add**（追加）します。
   3. **OK** をクリックします。
6. Select **BGP** > **General**（全般）を選択し、BGP を **Enable**（有効化）にて、プロトコルを次のように設定します：
   1. ゲートウェイ IP アドレスを **Router ID**（ルーター ID）を（**172.16.22.1**）、**1000** を **AS Number**（**AS** 番号） で入力します。
   2. オプション セクションで、**Install Route**（ルートのインストール）を選択します。
   3. **BGP** > **Peer Group**（ピア グループ）で、ゲートウェイに接続するすべてのサテライトを含むピア グループを **Add**（追加）します。
   4. **BGP** > **Redist Rules**（**Redist Rules**（**Redist** ルール）で、以前に作成した **ToLSVPNGW** 再配信プロファイルを **Add**（追加）します。
7. **OK** をクリックします。

STEP 7 | LSVPN の GlobalProtect ポータルを設定します。

どちらのデータセンターも、アクティブなデータ センターが優先ゲートウェイであることを確認するために、ルーティング優先度を変えてルートを宣言します。

1. **Network** > **GlobalProtect** > **Portals**(ネットワーク > GlobalProtect > ポータル) の順に選択し、**Add**(追加) をクリックします。
2. **General**（全般）で、**LSVPN-Portal** をポータル名として入力します。
3. **Network Settings**（ネットワーク設定）で、**Interface**（インターフェイス）として **ethernet1/21** を選択して、**IP Address**（IP アドレス）として **172.16.22.1/24** を選択します。
4. **Authentication**（認証）タブで、**SSL/TLS service Profile**（**SSL/TLS** サービス プロファイル）ドロップダウン リストから以前作成したプライマリ ゲートウェイ SSL/TLS プロファイル **LSVPN-Scale** を選択します。
5. **Satellite**（サテライト）タブで、サテライトを **Add**（追加）して、**sat-config-1** という **Name**（名前）を付けます。
6. **Configuration Refresh Interval**（設定の更新間隔）を **12** に設定します。
7. **GlobalProtect Satellite**（**GlobalProtect** サテライト） > **Devices**（デバイス）で、LSVPN 内の各サテライト デバイスのシリアル番号とホスト名を追加します。
8. **GlobalProtect Satellite**（**GlobalProtect** サテライト） > **Gateways**（ゲートウェイ）で、各ゲートウェイの名前と IP アドレスを追加します。プライマリ ゲートウェイのルーティング優先度を 1 に設定し、バックアップ ゲートウェイを 10 に設定して、アクティブなデータセンターが優先ゲートウェイであることを確認します。

STEP 8 | LSVPN 設定を検証します。

STEP 9 | （任意）新しいサイトを LSVPN デプロイメントに追加します。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > **GlobalProtect Portal**（**GlobalProtect** ポータル） > **Satellite Configuration**（サテライト設定） > **GlobalProtect Satellite**（**GlobalProtect** サテライト） > **Devices**（デバイス）を選択して、新しいサテライトのシリアル番号を GlobalProtect ポータルに追加します。
2. サテライト上の IPSec トンネルを GlobalProtect ポータルの IP アドレスで設定します。
3. 各ゲートウェイの BGP ピア グループ設定にサテライトを追加するには、**Network**（ネットワーク） > **Virtual Router**（仮想ルーター） > **BGP** > **Peer Group**（ピア グループ）を選択します。
4. **Network**（ネットワーク） > **Virtual Router**（仮想ルーター） > **BGP** > **Peer Group**（ピア グループ）を選択して、新しいサテライト上でゲートウェイを BGP ピア グループ設定に追加します。

Policy（ポリシー）

ポリシーにより、ルールを適用してアクションを実行できます。ファイアウォール上に作成できる様々なタイプのポリシー：具体的には、セキュリティ、NAT、QoS（Quality of Service）、ポリシー ベース フォワーディング（PBF）、復号、アプリケーション オーバーライド、認証、サービス拒否（DoS）、ゾーン プロテクションなどです。これらのさまざまなポリシーが連携することにより、許可、拒否、優先度の設定、転送、暗号化、復号、例外の作成、アクセスの認証、接続のリセットなど、必要に応じてネットワークを保護できます。以下のトピックでは、ポリシーの使用方法を説明します。

- ポリシーのタイプ
- セキュリティ ポリシー
- ポリシー オブジェクト
- セキュリティ プロファイル
- ルールベース内のルールの追跡
- ポリシールールの説明、タグ、監査コメントを適用
- ポリシー ルールまたはオブジェクトの異なる仮想システムへの移動またはコピー
- アドレス オブジェクトを使用して IP アドレスを表す
- タグを使用したオブジェクトのグループ化および視覚的な区別
- ポリシーで外部動的リストを使用
- IP アドレスとタグの動的登録
- ポリシー内でのダイナミック ユーザー グループの使用
- 自動タグ付けを使用してセキュリティアクションを自動化する
- 仮想環境における変更のモニタリング
- ダイナミック IP アドレスおよびタグを確認する CLI コマンド
- プロキシ サーバーを介して接続されたユーザーの識別
- ポリシー ベース フォワーディング
- ポリシールールのテスト

ポリシーのタイプ

Palo Alto Networks の次世代ファイウォールでサポートされているさまざまなタイプのポリシーを組み合わせることで、ネットワーク上でアプリケーションを安全に有効化できます。

すべてのポリシータイプについて、ポリシールールの説明、タグ、監査コメントを適用を行う場合、監査コメントアーカイブを使用して、ポリシールールが時間の経過とともにどのように変化したかを表示できます。監査コメント履歴と設定ログを含むアーカイブを使用すると、設定バージョンを比較して、誰が作成または変更したのか、またその理由を確認することができます。

ポリシーのタイプ	説明
セキュリティ	送信元および宛先のセキュリティ ゾーン、送信元および宛先の IP アドレス、アプリケーション、ユーザー、サービスなどのトラフィック属性に基づいて、セッションをブロックするか許可するかが決定されます。詳細についてはセキュリティポリシーを参照してください。
NAT	変換が必要なパケットおよび変換方法についてファイアウォールに指示します。ファイアウォールでは、送信元アドレスとポートの変換、宛先アドレスとポートの変換のどちらにも対応します。詳細については、 NATを参照してください。
QoS	1 つの定義済みパラメータまたは複数のパラメータを使用して QoS 処理（優先処理または帯域幅制限）を必要とするトラフィックを識別し、クラスに分類します。詳細についてはサービスの品質を参照してください。
ポリシー ベース フォワーディング	ルーティング テーブルに基づいて、通常とは異なる出力インターフェイスを使用する必要があるトラフィックを識別します。詳細については ポリシーベース フォワーディングを参照してください。
復号	可視化、管理、および詳細なセキュリティを調べる必要がある暗号化トラフィックを識別します。詳細については復号化を参照してください。
アプリケーション オーバーライド	レイヤー 7 検査である App-ID エンジンによる処理が不要なセッションを識別します。アプリケーション オーバーライド ポリシーに一致するトラフィックによって、ファイアウォールは、通常のステートフル インスペクション ファイアウォールとしてレイヤー 4 でセッションを処理するようになります。詳細についてはカスタム アプリケーションや不明なアプリケーションの管理を参照してください。
認証	ユーザーに認証を求めるトラフィックを識別します。詳細については認証ポリシーを参照してください。

ポリシーのタイプ	説明
DoS プロテクション	サービス拒否（DoS）攻撃を特定し、一致したルールに対応する保護アクションを実行します。詳細については DoS プロテクション プロファイルを参照してください。

Security Policy（セキュリティ ポリシー）

セキュリティ ポリシーにより、ネットワーク資産を脅威や障害から保護し、ネットワーク リソースの最適な割り当てを補助することで、ビジネス プロセスでの生産性や効率性を向上させます。Palo Alto Networks のファイアウォールでは、セキュリティ ポリシー ルールにより、送信元および宛先のセキュリティ ゾーン、送信元および宛先の IP アドレス、アプリケーション、ユーザー、サービスなどのトラフィック属性に基づいて、セッションをブロックするか許可するかが決定されます。

ネットワーク リソースへのアクセス試行時にエンド ユーザーの認証を確実に行うために、ファイアウォールは認証ポリシーを評価してから、セキュリティ ポリシーを評価します。

ファイアウォールを通過するすべてのトラフィックはセッションと照合され、各セッションはセキュリティ ポリシールールと照合されます。セッションが一致すると、ファイアウォールは一致するセキュリティ ポリシー ルールをそのセッション（クライアントからサーバー、およびサーバーからクライアント）の双方向トラフィックに適用します。定義されたルールのいずれとも一致しないトラフィックには、デフォルト ルールが適用されます。セキュリティ ルールベースの下部に表示されるデフォルト ルールは、すべてのイントラゾーン (ゾーン内) トラフィックを許可し、すべてのインターゾーン (ゾーン間) トラフィックを拒否するよう事前定義されています。これらのルールは、事前定義済み設定に含まれ、デフォルトで読み取り専用になっていますが、オーバーライドして、タグ、アクション (許可またはブロック)、ログ設定、セキュリティ プロファイルなど、一部の設定項目は変更することができます。

セキュリティ ポリシー ルールは、左から右に、および上から下の順に評価されます。定義済みの基準を満たす最初のルールとパケットが一致すると、それが引き金となり、それ以降のルールは評価されません。そのため、ベストマッチする基準を適用するには、個別のルールを一般的なルールよりも優先的に評価する必要があります。トラフィックがルールと一致すると、そのルールでログが有効になっていれば、セッションの最後にログのエントリがトラフィック ログに記録されます。ログのオプションはルールごとに設定可能で、セッションの最後ではなく最初にログを記録するように設定したり、セッションの最初と最後の両方でログを記録するように設定することも可能です。

管理者がルールを構成したら、ポリシールールの使用状況を表示して、セキュリティ ポリシー ルールと一致するトラフィックの時期と回数を決定し、その有効性を判断できます。ルールベースが進化するにつれて、ルールの作成時点や変更時点にこの情報をアーカイブしない限り、変更情報および監査情報は時間の経過とともに失われます。監査コメント・アーカイブを表示したり、コメントと構成ログの履歴を確認したり、選択したルールのルール構成バージョンを比較できるように、すべての管理者が監査コメントを入力するようにポリシールールの説明、タグ、監査コメントを適用することができます。こうすることで、ルールベースに対する可視性と制御性が向上します。

- セキュリティ ポリシー ルールのコンポーネント
- セキュリティポリシーのアクション
- セキュリティ ポリシー ルールを作成する

セキュリティ ポリシー ルールのコンポーネント

セキュリティ ポリシールールの構文では、次の表に示すように、必須フィールドとオプションフィールドを組み合わせて使用することができます。送信元アドレスまたは宛先アドレスにワイルドカードアドレスオブジェクトを使用する場合の詳細は表のとおりです。

必須/任意	項目	説明
必須	名前	ルールを識別するラベル (最大 63 文字)。
	UUID	UUID は、ルールの名前などを変更してもルールを追跡できるよう、ルールを永続的に識別する、固有の 32 文字の文字列です。
	ルールの種類	ルールがゾーン内、ゾーン間、その両方のどれに適用されるかを指定します。 • **universal**[ユニバーサル] （デフォルト） – 指定された送信元ゾーンおよび宛先ゾーン内の一致するすべてのインターゾーン トラフィックとイントラゾーン トラフィックにルールを適用します。たとえば、送信元ゾーンが A と B で、宛先ゾーンが A と B のユニバーサル ルールを作成するとします。ルールは、ゾーン A 内のすべてのトラフィック、ゾーン B 内のすべてのトラフィック、ゾーン A からゾーン B へのすべてのトラフィック、ゾーン B からゾーン A へのすべてのトラフィックに適用されます。 • **intrazone**[イントラゾーン] – 指定された送信元ゾーン内の一致するすべてのトラフィックにルールを適用します（イントラゾーン ルールには宛先ゾーンを指定できません）。たとえば、送信元ゾーンを A と B に設定するとします。ルールは、ゾーン A 内のすべてのトラフィック、ゾーン B 内のすべてのトラフィックに適用されますが、ゾーン A とゾーン B 間のトラフィックには適用されません。 • **interzone**[インターゾーン] – 指定された送信元ゾーンおよび宛先ゾーン間の一致するすべてのトラフィックにルールを適用します。たとえば、送信元ゾーンを A、B、C、宛先ゾーンを A、B に設定したとします。ルールは、ゾーン A からゾーン B、ゾーン B から ゾーン A、ゾーン C からゾーン A、ゾーン C からゾーン B へのトラフィックには適用されますが、ゾーン A、B、または C 内のトラフィックには適用されません。
	Source Zone	トラフィックの送信元となるゾーン。
	Destination Zone	トラフィックの宛先となるゾーン。NAT を使用している場合、常に NAT 後のゾーンを参照するようにしてください。

必須/任意	項目	説明
	Application [アプリケーション]	制御するアプリケーション。ファイアウォールでは、トラフィックの分類テクノロジーである App-ID を使用して、ネットワーク上のトラフィックを識別します。App-ID により、作成されたセキュリティ ポリシーの中でアプリケーションを制御および可視化し、不明なアプリケーションをブロックすると同時に、許可されるアプリケーションを有効化、検査、およびシェーピングできます。
	Action（アクション）	ルールで定義する基準に基づいて、トラフィックのアクションを許可または拒否に指定します。トラフィックを拒否するようにファイアウォールを設定すると、ファイアウォールは接続をリセットするか、確認なしでパケットをドロップします。ユーザーの操作性を向上させるため、確認なしでパケットをドロップする代わりに、トラフィックを拒否する詳細なオプションを設定できます。確認なしでドロップすると、一部のアプリケーションが破損してユーザーには応答なしのように見える可能性があります。詳細については、セキュリティポリシーのアクションを参照してください。
(任意)	タグ	セキュリティ ルールをフィルタリングできるようにするための、キーワードまたはフレーズ。多数のルールを定義していて、*IT* 制限付きのアプリケーション や 高リスクのアプリケーションなど、特定のキーワードによりタグ付けされているルールをレビューする場合には、これらのタグが便利です。
	説明	1024文字以下のテキスト フィールドで、ルールの説明に使用します。
	送信元アドレス	ホストの IP アドレス、サブネット、アドレス オブジェクト (IP ネットマスク、IP 範囲、FQDN、あるいは IP ワイルドカード マスク型)、アドレスグループ、国単位の適用を定義します。NAT を使用している場合、常にパケットの元の IP アドレス (NAT 前の IP アドレスなど) を参照するようにしてください。IP ワイルドカードマスクの詳細については、次の表を参照してください。
	宛先アドレス	パケットの場所または宛先。IP アドレス、サブネット、アドレス オブジェクト (IP ネットマスク、IP 範囲、FQDN、あるいは IP ワイルドカード マスク型)、アドレスグループ、国単位の適用を定義します。NAT を使用している場合、常にパケットの元の IP アドレス (NAT 前の IP アドレスなど) を参照するようにしてください。IP ワイルドカードマスクの詳細については、次の表を参照してください。

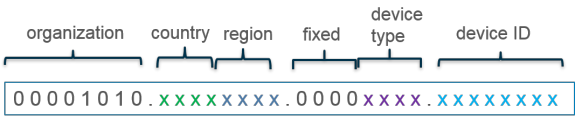
必須/任意	項目	説明
	ユーザー	ポリシーの適用対象となるユーザーまたはユーザー グループ。ゾーンで ユーザー ID を有効にする必要があります。User-IDを有効にするには、User-ID の概要を参照してください。
	URL カテゴリ	一致条件として URL Category （URL カテゴリ）を使用すると、URL カテゴリ単位にセキュリティ プロファイル（アンチウイルス、アンチスパイウェア、脆弱性、ファイル ブロッキング、データ フィルタリング、DoS）をカスタマイズできます。たとえば、危険度が高いことを示す URL カテゴリの .exe ファイルをダウンロード/アップロードできないようにし、それ以外のカテゴリのファイルを許可することが可能です。この機能では、特定の URL カテゴリにスケジュールを関連付けること（昼休み中または勤務時間外のソーシャル メディア Web サイトを許可する）や、特定の URL カテゴリを QoS でマークすること（金融、医療、ビジネス）、URL カテゴリ単位に異なるログ転送プロファイルを選択することもできます。 URL カテゴリはファイアウォールで手動設定できますが、Palo Alto Networks ファイアウォールで提供される URL カテゴリの動的更新を利用するには、URL フィルタリング ライセンスを購入する必要があります。 *URL* カテゴリに基づいてトラフィックをブロックまたは許可するには、セキュリティ ポリシー ルールに *URL* フィルタリング プロファイルを適用する必要があります。*URL Category [URL* カテゴリ*]*を *Any [*いずれか*]*として定義し、セキュリティ ポリシーに *URL* フィルタリング プロファイルを関連付けます。デフォルトのプロファイルをセキュリティ ポリシーで使用する方法の詳細は、基本的なセキュリティ ポリシーのセットアップを参照してください。
	Service	レイヤー 4 (TCP または UDP) のポートをアプリケーション用に選択することもできます。*any* を選択するか、ポートを指定するか、または *application-default*を使用して、アプリケーションの標準ベースのポートの使用を許可できます。たとえば DNS など、既知のポート番号を持つアプリケーションの場合、*application-default* オプションを選択すると、TCP ポート 53 でのみ DNS トラフィックと一致します。カスタム アプリケーションを追加して、そのアプリケーションで使用可能なポートを定義することもできます。

必須/任意	項目	説明
		インバウンド許可ルールの場合（たとえば *Untrust* から *Trust* など）、*application-default* を使用すると、アプリケーションを標準以外のポートやプロトコルで実行できなくなります。*application-default* はデフォルトのオプションです。ファイアウォールは引き続きすべてのポートのすべてのアプリケーションをチェックしますが、この設定にすることで、アプリケーションは標準のポート/プロトコルでのみ許可されます。
	セキュリティ プロファイル	脅威、脆弱性、データの漏洩などから、システムを保護します。セキュリティ プロファイルは、許可のアクションを含むルールに対してのみ評価されます。
	HIP プロファイル（GlobalProtect の場合）	ホスト情報プロファイル（HIP）を持つクライアントを識別してから、アクセス権を適用できます。
	オプション	セッションのログの定義、ログの転送設定、ルールに一致するパケットの Quality of Service （QoS）マーキングの変更、およびセキュリティ ルールを有効にするタイミング（日時）のスケジュールなどの設定が可能です。

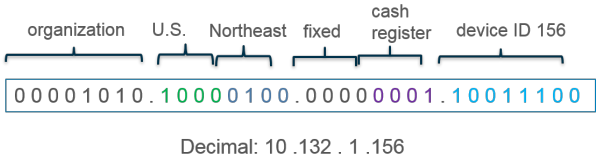
このセクションでは、セキュリティ ポリシールールの 送信元アドレス または 宛先アドレス でのワイルドカードアドレスオブジェクトの使用について説明します。内部デバイスにプライベート IPv4 アドレスを割り当てる場合、アドレス内の特定のビットに意味を割り当てる IP アドレス構造を使用できます。たとえば、IP アドレスの 第 3 オクテットの最初の 3 ビットは、デバイスの種類を示します。この構造により、デバイスの IP アドレスに基づいて、デバイスの種類や場所など、デバイスに関する詳細を簡単に識別できます。セキュリティ ポリシールールでこの同じ IP アドレス構造を使用すると、展開が容易になります。ワイルドカード アドレス (IP アドレスとワイルドカード マスクをスラッシュで区切ったもの、 10.1.2.3/0.127.248.0 など) を使用した アドレスオブジェクト を作成します。ワイルドカードアドレスは、単一の セキュリティ ポリシールール内で多くの送信元アドレスまたは宛先アドレスを識別できるため、特に多くのデバイスにサービスを提供するデータセンターの ファイアウォール に有用です。一致するすべての IP アドレスをカバーするために不必要に多数のアドレス オブジェクトを管理したり、IP アドレスの容量の制約のために必要以上に制限の緩い セキュリティ ポリシー ルールを使用したりする必要がなくなります。

たとえば、次の図に示す IPv4 アドレス体系を使用して、第 1 オクテットが組織を表すとします (ビット00001010は固定されています)。第2オクテットでは、最初の 4 ビットはネットワーク デバイスが配置されている国 (1000 は米国を示します) を示し、最後の 4 ビットは地域を示します (0100 は北東部を示します)。第 3 オクテットでは、最初の 4 ビットはゼロで、最後の 4 ビッ

トはデバイスタイプを示します (0001 はキャッシュ・レジスター、0011 はプリンターを示します)。最後のオクテットは、ネットワーク 機器の ID 番号を示します。



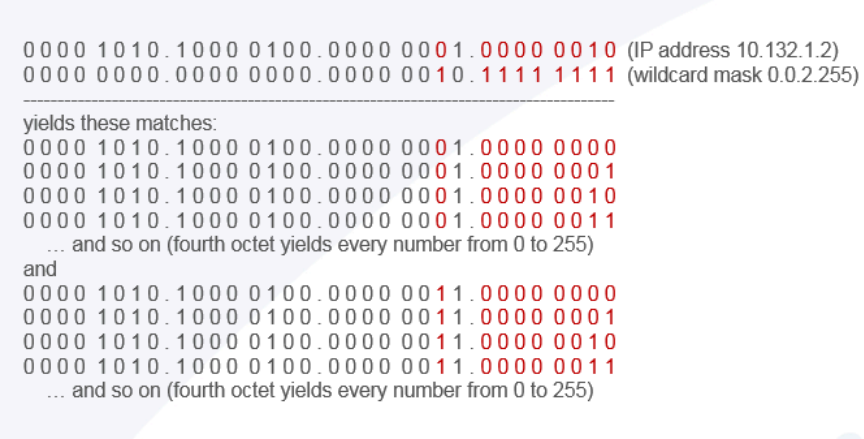
この構造に基づくと、米国北東部にあるキャッシュレジスター番号 156 の IP アドレスは 10.132.1.156 になります。



IP ワイルドカードマスク タイプのアドレス オブジェクトを使用して、セキュリティ ポリシー ルールでこのようなアドレス構造をサポートすることができます。IPv4 の送信元アドレスまたは宛先アドレスにワイルドカードマスクを適用して、どのアドレスがルールの対象になるかを指定します。Palo Alto Networks のワイルドカード マスクでは、ゼロ ビットは、比較対象のビットが、ゼロでカバーされる IP アドレスのビットと一致する必要があることを示します。マスク内の 1 ビットはワイルドカードまたは「無視」ビットであり、比較対象のビットが IP アドレスのビットと一致する必要はないことを意味します。たとえば、次のIP アドレスとワイルドカードマスクのスニペットは、4 つの一致を生成する方法を示しています。

すべてのベンダーがワイルドカードビットとして*1*を使用し、一致するビットとしてゼロを使用するわけではありません。

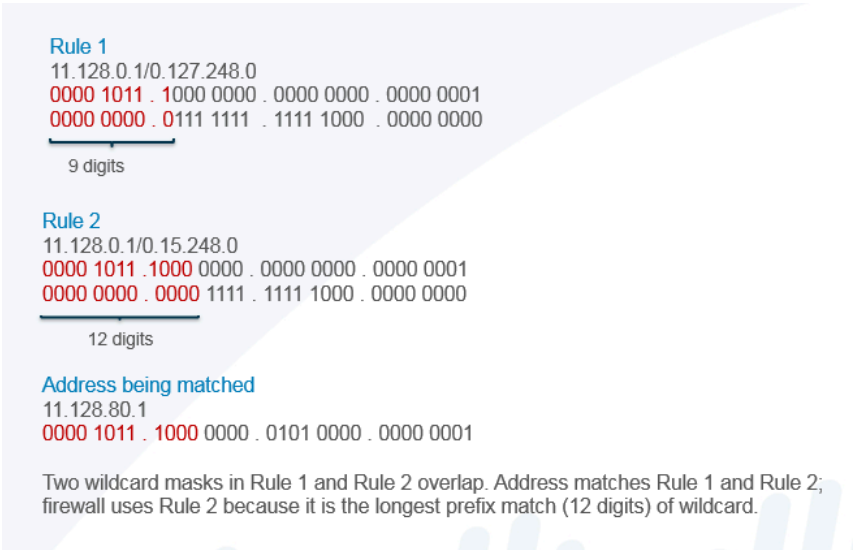
この例では、キャッシュ レジスターは 第３オクテット 00000001を持つ IPv4 アドレスを持ち、プリンターは 第３オクテット 00000011を持つ IPv4 アドレスを持ちます。0 から 255 までの任意の ID 番号を持つすべてのキャッシュレジスターおよびプリンターに セキュリティ ポリシー ルールを適用するとします。その結果を得るためには、ワイルドカードマスクが必要です。ワイルドカードマスクの 第３オクテットは 2 でなければならず、デバイス ID (第４オクテット) は 255 でなければなりません。米国北東部のすべてのキャッシュレジスタとプリンタを指定するアドレスオブジェクトは、ワイルドカードアドレス10.132.1.2/0.0.2.255を使用することになります。



このように、ワイルドカードアドレス 10.132.1.2/0.0.2.255 を宛先アドレスとするアドレスオブジェクトを使用する単一の セキュリティ ポリシールールは、512 台のデバイス (256 個のキャッシュレジスター + 256 台のプリンター) のアドレスと一致するため、多くのデバイスにルールを適用する効率的な方法となります。ワイルドカード・マスクは、0.0.2.255 のように、少なくとも 1 つのゼロ (0) で始める必要があります。

セキュリティ ポリシー ルールで IP ワイルドカードマスク タイプのアドレス オブジェクトを使用する場合、次のことを考慮してください。

- **IP** ワイルドカード マスク のアドレス オブジェクトを使用する送信元アドレスまたは宛先アドレスは、**Negate** オプションをサポートしていません。
- ファイアウォール はシャドウマッチングを行うときにワイルドカードアドレスを考慮しないため、**IP** ワイルドカード マスクタイプ のアドレスオブジェクトを使用する セキュリティ ポリシールールが後続のルールと重複していたり、リストの上位のルールと重複していたりしても警告は表示されません。
- ワイルドカードマスクが重複するルールにアドレスが一致する場合、ファイアウォール は、次の図に示すように、ワイルドカードマスク内の最も長いプレフィックスに一致するものを選択します。



前出の箇条書きは、デフォルトの動作を説明したものです。ただし、一部の送信元が汎用アプリケーション (Ping、Traceroute、Web ブラウジングなど) にアクセスできるようにする広範なルールを使用し、これらの送信元のサブセットが汎用アプリケーションに加えてさまざまなアプリケーション (SSH、SCP など) にアクセスできるようにする、より狭いルールが必要な場合があります。以前のリリースでは、ワイルドカード マスク内のプレフィックスが最も長いルールに一致するもののみが処理され、他のルールは考慮されなかったため、このような展開は機能しませんでした。

PAN-OS 10.2.1 以降では、ワイルドカード トップ ダウン マッチ モード を有効にすると、あるIP アドレスを持つパケットがワイルドカード マスクが重複する セキュリティ ポリシー ルールのプレフィックスと一致する場合、ファイアウォール は ワイルドカード マスクで最長のプレフィックスを持つ一致ルールを選択するのではなく、トップダウン順で最初の完全一致ルールを選択するようにできます。パケットは、重複するワイルドカードマスクを使用するルールでプレフィックスに一致することがわかります。次に、ファイアウォール は、マスク内のルールがワイルドカードまたは「無視」ビットを示すことを念頭に置いて、マスキングに基づいてすべてのアドレスビットに完全に一致するルールを選択します。次に、アプリケーションやゾーンなどの他のルール条件が調べられます。他のルール基準の検査中に、ファイアウォール はその基準に一致するルールを（上から順に）最初に選択します。他のルールは評価されません。

ワイルドカード トップ ダウン マッチ モード は、複数のルールが異なるパケット に適用される可能性があることを意味します。(最も長く一致するプレフィックスを持つルールだけではありません) より具体的なルールをリストの一番上に配置します。たとえば、一致するアドレスの範囲を狭くして (ワイルドカード マスクを長くする) 特定のアプリケーションへのアクセスを許可したり、後続のルールで、より広い範囲の IP アドレス (より短いワイルドカード マスク) が別の (より汎用的な) アプリケーション セットにアクセスすることを許可したりできます。ワイルドカード トップ ダウン マッチ モード を有効にするには、**Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択し、Policy Rulebase Settings (ポリシールールベース設定) を編集します。

次の例では、ワイルドカード トップ ダウン マッチ モード が有効で、3 つの セキュリティ ポリシールールがあり、それぞれがワイルドカードマスクアドレスオブジェクトで送信元 IP アドレスを指定し、ワイルドカードマスクが重複しています。

Rule 1: 10.128.0.1/0.127.248.0

0000 1010 1000 0000 0000 0000 0000 0001 IP address
0000 0000 0111 1111 1111 1000 0000 0000 Wildcard Mask
Resulting prefix that matches Rule 1: 10.128.0.1/9

Rule 2: 10.128.0.1/0.15.248.0

0000 1010 1000 0000 0000 0000 0000 0001 IP address
0000 0000 0000 1111 1111 1000 0000 0000 Wildcard Mask
Resulting prefix that matches Rule 2: 10.128.0.1/12

Rule 3: 10.128.0.1/0.127.255.0

0000 1010 1000 0000 0000 0000 0000 0001 IP address
0000 0000 0111 1111 1111 1111 0000 0000 Wildcard Mask
Resulting prefix that matches Rule 3: 10.128.0.1/9

この例では、送信元 IP アドレスが 10.143.8.1 (0000 1010 1000 1111 0000 1000 0000 0001) のクライアント A は、ルール 1、ルール 2、およびルール 3 に完全に一致します。最初の一致はルール 1 です (トップダウン順)。他のルール条件が一致すると仮定すると、クライアント A からのパケットはルール 1 のアクションの対象となります。

送信元 IP アドレスが 10.160 2.1 (0000 1010 1010 0000 0000 0010 0000 0001) のクライアント B は、ルール 1 のアドレスと完全には一致せず、ルール 2 のプレフィックスとも一致しません。クライアント B のアドレスは、トップダウン順で最初に一致するルールであるルール 3 に完全に一致します。他のルール条件が一致すると仮定すると、クライアント B からのパケットはルール 3 のアクションの対象となります。したがって、ワイルドカード トップ ダウン マッチ モード の利点は、ルール 1 とルール 3 の両方が異なるパケットに対して有効になり得ることだとわかります。

セキュリティポリシーのアクション

セキュリティ ポリシーに定義された属性に一致するトラフィックに対して、以下のアクションを適用できます。

Action（アクション）	の意味
Allow (許可)（デフォルト）	トラフィックを許可します。
拒否	トラフィックをブロックし、拒否されるアプリケーションについて定義されたデフォルトの拒否アクションを実行します。アプリ

Action（アクション）	の意味
	ケーションについてデフォルトで定義されている拒否アクションを表示するには、**Objects (オブジェクト)** > **Applications (アプリケーション)** でアプリケーションの詳細を表示するか、Applipedia でアプリケーションの詳細を確認します。
Drop（ドロップ）	確認なしでトラフィックをドロップします。アプリケーションの場合、デフォルトの拒否アクションはオーバーライドされます。TCP リセットはホスト/アプリケーションに送信されません。 レイヤー3 インターフェイスで必要に応じて ICMP 送信到達不能応答をクライアントに送信するには、Action [アクション]を：**Drop** [ドロップ]に設定し、**Send ICMP Unreachable**[ICMP 送信到達不能]チェック ボックスをオンにします。有効にすると、ファイアウォールは通信が管理上禁止されている宛先の ICMP コードを送信します—ICMPv4：Type 3、Code 13、ICMPv6：Type 1、Code 1。
クライアントのリセット	クライアント側デバイスに TCP リセットを送信します。
サーバーのリセット	サーバー側デバイスに TCP リセットを送信します。
両方のリセット	クライアント側とサーバー側の両方のデバイスに TCP リセットを送信します。

リセットは、セッションが確立された後にのみ送信されます。*3* ウェイ ハンドシェークが完了する前にセッションがブロックされた場合、ファイアウォールはリセットを送信しません。

リセット アクションの TCP セッションでは、ファイアウォールは ICMP 到達不能応答を送信しません。

ドロップまたはリセット アクションの UDP セッションでは、**ICMP Unreachable** [ICMP 到達不能]チェック ボックスがオンの場合、ファイアウォールは ICMP メッセージをクライアントに送信します。

セキュリティ ポリシー ルールを作成する

STEP 1 | （任意）デフォルトのセキュリティポリシー ルールを削除します。

デフォルトでは、「*rule1*」という名前のセキュリティ ルールがファイアウォールに含まれています。このルールでは、Trust ゾーンから Untrust ゾーンへのトラフィックがすべて許可されています。このルールを削除する、またはゾーンの命名規則を反映するようにルールを変更することもできます。

STEP 2 | ルールを追加します。

1. **Policies** > **Security**(ポリシー > セキュリティ) の順に選択し、新しいルールを**Add**(追加)します。
2. **General**（全般）タブで、ルールの分かりやすい **Name**（名前）を入力します。
3. **Rule Type (**ルール タイプ**)** を選択します。

STEP 3 | パケットの送信元フィールド用の一致条件を定義します。

1. **Source (**送信元**)** タブで **Source Zone (**送信元ゾーン**)** を選択します。
2. **Source (**送信元**) IP Address (IP** アドレス**)** を指定するか、値を **any (**すべて**)** のままにします。

   リージョンを ***Source Address (***送信元アドレス***)*** として***Negate(***除外***)*** する場合は、プライベート*IP*アドレス間の接続が失われないように、プライベート *IP* を含むすべてのリージョンが***Source Address (***送信元アドレス***)*** に追加されていることを確認してください。
3. Source (送信元) **User (**ユーザー**)** を指定するか、値を **any (**すべて**)** のままにします。

STEP 4 | パケットの宛先フィールド用の一致条件を定義します。

1. **Destination (**宛先**)** タブで **Destination Zone (**宛先ゾーン**)** を設定します。
2. **Destination IP Address (**宛先 **IP** アドレス**)** を指定するか、値を **any (**すべて**)** のままにします。

   リージョンを ***Destination Address (***宛先アドレス***)*** として ***Negate(***除外***)*** する場合は、プライベート *IP*アドレスを含むすべてのリージョンが ***Destination Address (***宛先アドレス***)*** に追加されていることを確認して、それらのプライベート *IP*アドレス間の接続が失われないようにします。

   ベストプラクティスとしては、アドレス オブジェクトを ***Destination Address (***宛先アドレス***)*** として使用して、特に *DNS* や *SMTP* などの一般的に悪用されるサービスの特定のサーバーまたは特定のサーバー グループのみにアクセスできるようにします。特定の宛先サーバーのアドレスにユーザーを制限することで、データの盗難を防止し、*DNS* トンネリングといった手法を用いてコマンド アンド コントロールトラフィックが接続を確立するのを防ぐことができます。

STEP 5 | ルールが許可あるいはブロックするアプリケーションを指定します。

常にポート ベースのルールではなくアプリケーション ベースのセキュリティポリシー ルールを使用し、標準的なポートよりもアプリケーションに対する制限が厳しいポートのリストを使用しているのでない限り、*Service [サービス]*を常に*application-default*に設定しておくことが推奨されます。

1. **Applications (アプリケーション)** タブで **Application (アプリケーション)** を **Add (追加)** し、安全に有効化します。複数のアプリケーションを選択する、あるいはアプリケーション グループやアプリケーション フィルターを使用することができます。
2. **Service/URL Category (サービス/URL カテゴリ)** タブで Service (サービス) を **application-default** のままにし、ルールが許可するすべてのアプリケーションがその標準的なポート上でのみ許可されるようにします。

STEP 6 | （任意）そのルールの一致条件としてURLカテゴリを指定します。

Service/URL Category (サービス/URL カテゴリ) タブで **URL Category (URL カテゴリ)** を選択します。

URLカテゴリを選択した場合、指定されたカテゴリにトラフィックに向かう Web トラフィックのみにルールがマッチします。

STEP 7 | ルールにマッチしたトラフィックに対してファイアウォールが取るべきアクションを定義します。

Actions [アクション]タブで**Action** [アクション]を選択します。各アクションの説明については、セキュリティポリシーのアクションを参照してください。

STEP 8 | ログ設定を行います。

- デフォルトでは、ルールは**Log at Session End** [セッション終了時にログ]に設定されています。トラフィックがこのルールにマッチした際にログを生成したくない場合はこの設定を無効化するか、**Log at Session Start**（セッション開始時にログ） を選択して詳細なロギングを設定することができます。
- **Log Forwarding** [ログ転送]プロファイルを設定します。

ベストプラクティスとしては、 ***Disable Server Response Inspection***サーバー レスポンス検査の無効化） （*DSRI*）チェックボックスを選択しないでください。このオプションを選択すると、ファイアウォールがサーバーからクライアントへのパケットを検査できなくなります。セキュリティを最適にするために、ファイアウォールは、クライアントからサーバーへのフローとサーバーからクライアントへのフローの両方を調べて、脅威を検出して防御する必要があります。

STEP 9 | セキュリティ プロファイルを付与し、その脅威に関して許可されているすべてのトラフィックをファイアウォールがスキャンできるようにします。

既知の脅威と未知の脅威の両方からネットワークを保護するためのベストプラクティスのセキュリティ プロファイルを作成してください。

Actions [アクション]タブの**Profile Type** [プロファイル タイプ]ドロップダウンリストで**Profiles** [プロファイル]を選択し、そのルールに付与する個々のセキュリティ プロファイルを選択します。

あるいは、 **Profile Type** [プロファイル タイプ]ドロップダウンリストで**Group** [グループ]を選択し、付与する**Group Profile** [グループ プロファイル]を選択します。

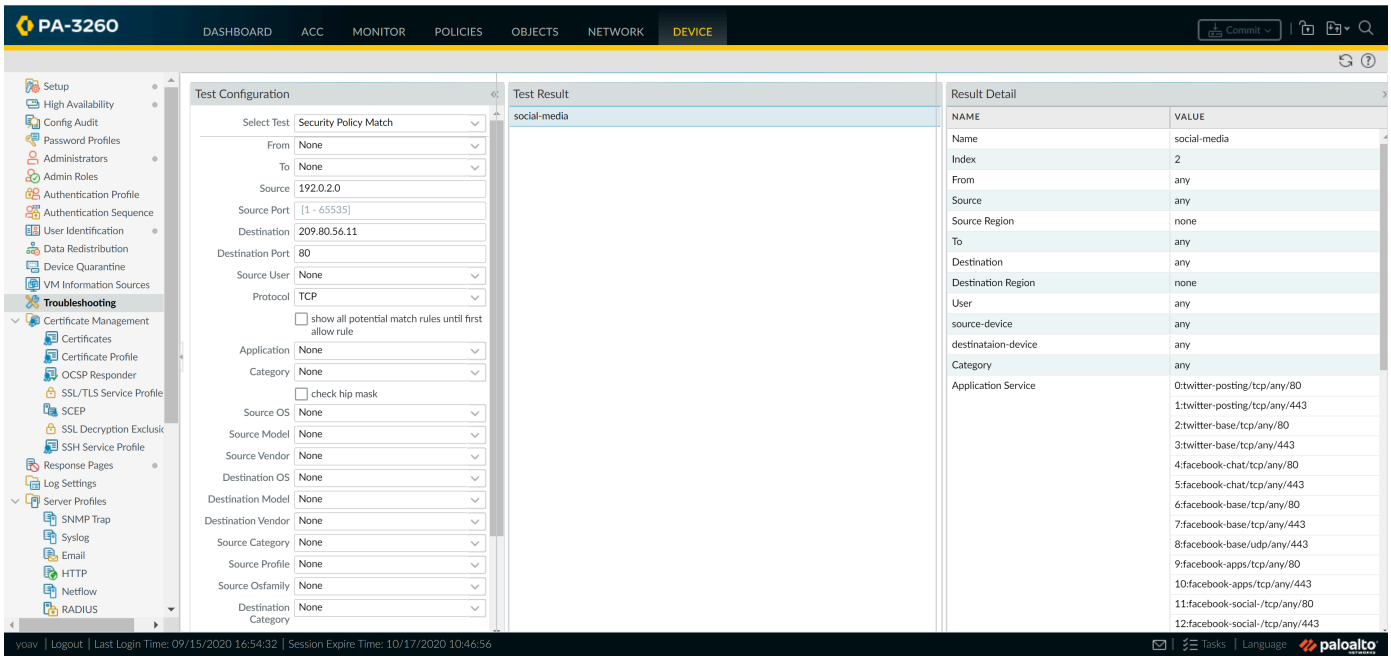
STEP 10 | **Commit(コミット)** をクリックして、ファイアウォールの実行中の設定にポリシー ルールを保存します。

STEP 11 | 基本的なセキュリティ ポリシーを効果的に設定できていることを確認するために、セキュリティポリシー ルールが評価されているかどうかテストし、どのセキュリティポリシー ルールがトラフィック フローに適用されているかを判断します。

この CLI コマンドで指定する送信元と宛先の IP アドレスに最も一致するルールが出力されます。

たとえば、IP アドレスが 208.90.56.11 のデータセンター内のサーバーから Microsoft Update サーバーにアクセスする場合、このサーバーに適用されるポリシー ルールを確認するには：

1. **Device (デバイス)** > **Troubleshooting (トラブルシューティング)** を選択し、Select Test (テストの選択) ドロップダウンから **Security Policy Match (セキュリティポリシー マッチ)** を選択します。
2. Source (送信元) および Destination (宛先) IP アドレスを入力します。
3. Protocol (プロトコル) を入力します。
4. セキュリティポリシー マッチ テストを **Execute (実行)** します。



STEP 12 | トラフィックがファイアウォールを通過するまで十分に待機してから、 ポリシー ルールの使用状況を監視してポリシー ルールの使用状況を監視し、ポリシー ルールの有効性を判断します。

ポリシー オブジェクト

ポリシー オブジェクトは、単一のオブジェクトまたは集合単位で、IP アドレス、URL、アプリケーション、ユーザーなどの個別の ID をグループ化するものです。ポリシー オブジェクトが集合単位の場合、複数のオブジェクトを手動で 1 つずつ選択しなくても、セキュリティ ポリシーでそのオブジェクトを参照できます。一般的にポリシー オブジェクトを作成する場合、ポリシーで同様のアクセス権限を必要とするオブジェクトをグループ化します。たとえば、組織が一連のサーバーの IP アドレスを使用してユーザーを認証する場合、それらのサーバーの IP アドレスをアドレス グループのポリシー オブジェクトとしてグループ化し、そのアドレス グループをセキュリティ ポリシーで参照します。オブジェクトをグループ化することにより、ポリシー作成時の管理者の負担が大幅に軽減されます。

内部レビューまたは監査のために設定の特定の部分をエクスポートする必要がある場合は、 *PDF* または *CSV* ファイルで設定テーブルデータをエクスポートできます。

以下のポリシー オブジェクトをファイアウォールで作成できます。

ポリシー オブジェクト	説明
アドレス/アドレス グループ、地域	同じポリシーを実施する必要のある特定の送信元アドレスまたは宛先アドレスをグループ化できます。アドレス オブジェクトには、IPv4 または IPv6 のアドレス (単一 IP、範囲、サブネット)、IP ワイルドカードアドレス (IPv4 アドレス/ワイルドカードマスク)、または FQDN を含めることができます。または、緯度と経度の座標で地域を定義したり、国を選択して IP アドレスまたは IP の範囲を定義したりできます。こうすることで、アドレス オブジェクトのコレクションをグループ化し、アドレス グループ オブジェクトを作成できます。 また、ダイナミック アドレス グループの使用も可能です。このグループは、ホスト IP アドレスが頻繁に変わる環境で動的に IP アドレスを更新します。 ファイアウォール上で事前定義された外部動的リスト *(EDL)* は、ファイアウォールモデルがサポートするアドレスオブジェクトの最大数にカウントされます。
ユーザー/ユーザー グループ	ローカル データベース、外部データベースまたは一致条件からユーザーのリストを作成し、それらをグループ化できます。
アプリケーション グループおよびアプリケーション フィルタ	アプリケーション フィルタにより、アプリケーションを動的にフィルタリングでき、ファイアウォールのアプリケーション データベースで定義した属性を使用して、一連のアプリケーションをフィルタリングおよび保存できます。たとえば、カテゴリ、サブカテゴリ、テクノロジー、リスク、特性など、1 つ以上の属性ごとのアプリケー

ポリシー オブジェクト	説明
	ション フィルタの作成が可能です。アプリケーション フィルタがあれば、コンテンツの更新が発生した場合に、フィルタ基準を満たす新規アプリケーションが自動的に保存されているアプリケーション フィルタに追加されます。 アプリケーション グループにより、あるユーザー グループまたは特定のサービスに対してグループ化したり、特定のポリシー目標を達成したりするために特定のアプリケーションの静的グループを作成できます。「アプリケーション グループの作成」を参照してください。
サービス/サービス グループ	送信元ポートと宛先ポート、およびサービスで使用できるプロトコルを指定できます。ファイアウォールには、service-http と service-https という 2 つの事前定義サービスが含まれています。これらのサービスでは、TCP ポート 80 および 8080 を HTTP に、TCP ポート 443 を HTTPS に使用します。ただし、カスタム サービスを任意の TCP/UDP ポートで自由に作成して、アプリケーションの使用をネットワーク上の特定のポートに制限できます (つまり、アプリケーションのデフォルト ポートを定義できます)。 アプリケーションで使用する標準ポートを表示するには、***Objects (オブジェクト) > Applications (アプリケーション)*** の順に選択してアプリケーションを検索し、リンクをクリックします。簡単な説明が表示されます。

セキュリティ プロファイル

セキュリティ ポリシールールにより、ネットワーク上のトラフィックを許可またはブロックできますが、セキュリティ プロファイルを使用すると、許可するがスキャンを実施するルールを定義できます。このルールでは、許可されたアプリケーションに、ウイルス、マルウェア、スパイウェア、DDOS 攻撃などの脅威が潜んでいないかスキャンされます。トラフィックがセキュリティ ポリシーで定義した許可ルールと一致する場合、そのルールに添付されたセキュリティ プロファイルが、アンチウイルス チェックやデータ フィルタリングなどのコンテンツ検査ルールに追加適用されます。

セキュリティ プロファイルは、トラフィック フローの一致基準には使用されません。セキュリティ プロファイルは、セキュリティ ポリシーでアプリケーションまたはカテゴリが許可された後に適用され、トラフィックをスキャンします。

ファイアウォールでは、デフォルトのセキュリティ プロファイルをそのまま使用して、すぐにネットワークを脅威から保護できます。デフォルトのプロファイルをセキュリティ ポリシーで使用する方法の詳細は、基本的なセキュリティ ポリシーのセットアップを参照してください。ネットワーク上のセキュリティのニーズをよりよく理解するには、カスタム プロファイルを作成する方法については、「インターネット ゲートウェイのベストプラクティスのセキュリティ プロファイルを作成する」を参照してください。

セキュリティ プロファイルの推奨設定についてはインターネット ゲートウェイ用の最良のセキュリティ プロファイルを作成をご覧ください。

セキュリティ プロファイル グループの作成を行うことで、一緒に適用することが多いセキュリティ プロファイルをまとめておくことができます。セキュリティ プロファイル グループは 1 つの単位として扱うことができるプロファイルのセットであり、セキュリティ ポリシーに 1 ステップで追加できます（デフォルトのセキュリティ プロファイル グループを設定した場合は、デフォルトでセキュリティ ポリシーに追加されます）。

プロファイル タイプ	の意味
アンチウイルス プロファイル	アンチウイルス プロファイルは、ウイルス、ワーム、トロイの木馬、およびスパイウェア ダウンロードからの保護を実現します。Palo Alto Networks アンチウイルス ソリューションでは、パケットを最初に受信する瞬間にトラフィックを検査するストリームベースのマルウェア防御エンジンを使用して、ファイアウォールのパフォーマンスに大きな影響を与えることなくクライアントを保護することができます。このプロファイルは、実行ファイル、PDF ファイル、HTML、および JavaScript ウイルスに含まれるさまざまなマルウェアをスキャンします。また、圧縮ファイルとデータ エンコード スキームの内部スキャンもサポートしています。ファイアウォールで復号化を有効にしている場合は、復号化されたコンテンツのスキャンも可能です。 デフォルト プロファイルでは、ウイルスが含まれていないかどうかについてリストにあるプロトコル デコーダすべてを検査

プロファイル タイプ	の意味
	し、FTP、HTTP、および SMB プロトコルの場合にはブロックし、SMTP、IMAP、および POP3 プロトコルの場合にはアラートを生成します。デコーダまたはアンチウイルス シグネチャのアクションを設定し、脅威イベントに対するファイアウォールの応答方法を指定できます。 • **Default (デフォルト)** — Palo Alto Networks によって定義された各脅威シグネチャとアンチウイルス シグネチャの場合、デフォルト アクションが内部で指定されます。通常、デフォルト アクションは「alert」または「reset-both」です。デフォルト アクションはかっこに囲まれて表示されます。たとえば、脅威またはアンチウイルス シグネチャでは「default（alert）」になります。 • **Allow** — アプリケーション トラフィックが許可されます。 ***Allow (許可)*** アクションは、シグネチャまたはプロファイルに関連するログを生成しません。 • **Alert** — 各アプリケーション トラフィック フローのアラートが生成されます。アラートは脅威ログに保存されます。 • **Drop** — アプリケーション トラフィックが廃棄されます。 • **Reset Client** [クライアントのリセット] — TCP の場合、クライアント側の接続がリセットされます。UDP の場合、接続がドロップされます。 • **Reset Server** [サーバーのリセット] — TCP の場合、サーバー側の接続がリセットされます。UDP の場合、接続がドロップされます。 • **Reset Both** [両方のリセット] — TCP の場合、クライアント側とサーバー側の両方の接続がリセットされます。UDP の場合、接続がドロップされます。 カスタマイズしたプロファイルを使用して、信頼されたセキュリティ ゾーン間のトラフィックに対するウイルス対策の検査を最小限に抑え、インターネットなどの信頼されていないゾーンから受信したトラフィックや、サーバー ファームなどの機密性の高い宛先に送信されるトラフィックの検査を最大化できます。 Palo Alto Networks WildFire システムは、より回避的で、他のアンチウイルス ソリューションによってまだ検出されていない脅威のシグネチャも生成できます。WildFire によって脅威が検出されると、シグネチャが素早く作成され、脅威防御ライセンスの加入者は毎日（WildFire ライセンスの加入者の場合は 1 時間以内の間隔で）ダウンロードされる標準のアンチウイルス シグネチャに組み込まれます。
アンチスパイウェア プロファイル	アンチスパイウェア プロファイルは、ホストに侵入したスパイウェアが、外部指揮統制（C2）サーバーに対して phone-home 通信また

プロファイル タイプ	の意味
	はビーコン通信を試行するのをブロックします。これにより、感染クライアントからネットワーク外に送出される悪意あるトラフィックを検出できます。ゾーン間では、さまざまなレベルで保護機能を適用できます。たとえば、信頼されたゾーン間での検査を最小限に抑えるカスタム アンチスパイウェア プロファイルを作成する一方で、インターネット側ゾーンなどの信頼されないゾーンから受信するトラフィックでの検査を最大化することができます。ファイアウォールが Panorama 管理サーバーによって管理されている場合、ThreatID はファイアウォール上の対応するカスタム脅威にマップされ、ファイアウォールが設定済みのカスタム ThreatID を入力した脅威ログを生成できるようにします。 アンチスパイウェアをセキュリティ ポリシールールに適用するには、独自のカスタム アンチスパイウェア プロファイルを定義する方法と、以下のどちらかの事前定義プロファイルを選択する方法があります。 • **default** – 各シグネチャのデフォルトのアクションを使用します。デフォルトのアクションは、シグネチャの作成時に Palo Alto Networks によって指定されます。 • **strict** – シグネチャ ファイルで定義されているアクションに関係なく、重大度が「critical」、「high」、および「medium」の脅威のデフォルトのアクションがすべてブロック アクションでオーバーライドされます。重大度が「low」および「informational」のシグネチャの場合にはデフォルト アクションが実行されます。 ファイアウォールが脅威イベントを検出したときに、アンチスパイウェア プロファイルで以下のアクションを設定できます。 • **Default** [デフォルト] – Palo Alto Networks によって定義された各脅威シグネチャとアンチスパイウェア シグネチャの場合、デフォルト アクションが内部で指定されます。通常、デフォルト アクションは「alert」または「reset-both」です。デフォルト アクションはかっこに囲まれて表示されます。たとえば、脅威またはアンチウイルス シグネチャでは「default（alert）」になります。 • **Allow** [許可] – アプリケーション トラフィックが許可されます。 ***Allow (許可)*** アクションは、シグネチャまたはプロファイルに関連するログを生成しません。 • **Alert** – 各アプリケーション トラフィック フローのアラートが生成されます。アラートは脅威ログに保存されます。 • **Drop** – アプリケーション トラフィックが廃棄されます。 • **Reset Client** [クライアントのリセット] – TCP の場合、クライアント側の接続がリセットされます。UDP の場合、接続がドロップされます。

プロファイル タイプ	の意味
	• **Reset Server** [サーバーのリセット] – TCP の場合、サーバー側の接続がリセットされます。UDP の場合、接続がドロップされます。 • **Reset Both** [両方のリセット] – TCP の場合、クライアント側とサーバー側の両方の接続がリセットされます。UDP の場合、接続がドロップされます。  プロファイルのアクションが***reset-both*** **(**両方をリセット**)**に設定されている場合、一部のケースで、関連する脅威ログ中でアクションが***reset-server*** **(**サーバーリセット**)**として表示されることがあります。これは、セッション開始時にファイアウォールが脅威を検出し、クライアントに *503* ブロック ページを提示する際に発生します。ブロック ページは接続を許可しないため、クライアント側でリセットを行う必要はなく、サーバー側でのみ接続がリセットされます。 • **Block IP** [ブロック IP] – このアクションでは、送信元または送信元と宛先のペアからのトラフィックがブロックされます。ブロックする期間を指定できます。 また、アンチスパイウェア プロファイル内では、DNS シンクホール アクションを有効にすることができます。これにより、ファイアウォールが、既知の悪意あるドメインに問い合わせる DNS クエリに対する応答を偽装して、悪意あるドメイン名を、管理者が定義した IP アドレスに解決できます。この機能により、DNS トラフィックを使用して保護されているネットワーク上で感染したホストを特定しやすくなります。こうすることで、感染ホストをトラフィック ログおよび脅威ログ内で容易に特定できます。シンクホール IP アドレスへの接続を試みるホストはすべて、マルウェアに感染している可能性が高いためです。 アンチスパイウェア プロファイルと脆弱性防御プロファイルは同様の方法で設定されます。
脆弱性防御プロファイル	脆弱性防御プロファイルは、システムの脆弱性の悪用やシステムへの不正アクセスを防止します。アンチスパイウェア プロファイルでは、ネットワークから流出するトラフィックにより感染したホストを検出するのに役立ちますが、脆弱性防御プロファイルではネットワークに入ってくる脅威から保護します。この機能は、たとえば、バッファ オーバーフロー、不正なコード実行、およびシステムの脆弱性を悪用するその他の試みからシステムを防御します。デフォルトの脆弱性防御プロファイルでは、重大度が「critical」、「high」、および「medium」のすべての既知の脅威からクライアントとサーバーを保護します。また、特定のシグネチャに対する応答の変更を可能にする

プロファイル タイプ	の意味
	例外を作成することもできます。ファイアウォールが Panorama 管理サーバーによって管理されている場合、ThreatID はファイアウォール上の対応するカスタム脅威にマップされ、ファイアウォールが設定済みのカスタム ThreatID を入力した脅威ログを生成できるようにします。 ファイアウォールが脅威イベントを検出したときに、アンチスパイウェア プロファイルで以下のアクションを設定できます。 • **Default** [デフォルト] – Palo Alto Networks によって定義された各脅威シグネチャとアンチスパイウェア シグネチャの場合、デフォルト アクションが内部で指定されます。通常、デフォルト アクションは「alert」または「reset-both」です。デフォルト アクションはかっこに囲まれて表示されます。たとえば、脅威またはアンチウイルス シグネチャでは「default（alert）」になります。 • **Allow** [許可] – アプリケーション トラフィックが許可されます。 ***Allow (***許可***)*** アクションは、シグネチャまたはプロファイルに関連するログを生成しません。 • **Alert** – 各アプリケーション トラフィック フローのアラートが生成されます。アラートは脅威ログに保存されます。 • **Drop** – アプリケーション トラフィックが廃棄されます。 • **Reset Client** [クライアントのリセット] – TCP の場合、クライアント側の接続がリセットされます。UDP の場合、接続がドロップされます。 • **Reset Server** [サーバーのリセット] – TCP の場合、サーバー側の接続がリセットされます。UDP の場合、接続がドロップされます。 • **Reset Both** [両方のリセット] – TCP の場合、クライアント側とサーバー側の両方の接続がリセットされます。UDP の場合、接続がドロップされます。 プロファイルのアクションが***reset-both (***両方をリセット***)***に設定されている場合、一部のケースで、関連する脅威ログ中でアクションが***reset-server (***サーバーリセット***)***として表示されることがあります。これは、セッション開始時にファイアウォールが脅威を検出し、クライアントに *503* ブロック ページを提示する際に発生します。ブロック ページは接続を許可しないため、クライアント側でリセットを行う必要はなく、サーバー側でのみ接続がリセットされます。

プロファイル タイプ	の意味
	• **Block IP** [ブロック IP] – このアクションでは、送信元または送信元と宛先のペアからのトラフィックがブロックされます。ブロックする期間を指定できます。
URL フィルタリング プロファイル	URL フィルタリング プロファイルでは、ユーザーが HTTP または HTTPS で Web にどのようにアクセスしているかを監視および制御できます。ファイアウォールには、既知のマルウェア サイト、フィッシング サイト、アダルト コンテンツ サイトなどの Web サイトをブロックするように設定されているデフォルト プロファイルが付属しています。このデフォルト プロファイルは、セキュリティ ポリシーで使用したり、コピーして新しい URL フィルタリング プロファイルを作成するときに利用したりできます。また、ネットワーク上のトラフィックを可視化できるように、すべてのカテゴリを許可に設定する新しい URL プロファイルを追加することもできます。新しく追加されたこの URL プロファイルをカスタマイズして、常にブロックまたは許可する必要のある特定の Web サイトのリストを追加できます。これにより、URL カテゴリをより細かく制御することができます。
データ フィルタリング プロファイル	データ フィルタリング プロファイルを使用すると、クレジット カード番号や社会保障番号などの機密情報が、保護されたネットワークから出て行かないよう防御できます。また、重要なプロジェクト名や秘密の言葉などのキーワードに基づいてフィルタリングすることもできます。プロファイルの焦点を適切なファイル タイプに合わせ、誤検知を削減することが重要です。たとえば、Word ドキュメントまたは Excel スプレッドシートのみを検索することができます。また、web-browsing トラフィック、または FTP のみをスキャンすることも可能です。 カスタム データパターン オブジェクトを作成してデータ フィルタリング プロファイルにアタッチし、フィルタリングしたい情報の種類を定義することができます。次の項目に基づいてデータパターン オブジェクトを作成します。 • **Predefined Pattern (定義済みのパターン)**–定義済みのパターンを使用して、クレジットカードおよび社会保障番号（ダッシュは付けても付けなくても良い）をフィルタリングします。 • **Regular Expressions (正規表現)**–文字列をフィルタリングします。 • **File Properties (ファイル プロパティ)**–ファイルの種類に応じて、ファイル プロパティおよび値に基づいてフィルタリングします。  センシティブなコンテンツを示すファイル プロパティを、サードパーティのエンドポイント データ損失防止（*DLP*）製品を使用して自動生成している場合、このオプションによってファイアウォールが *DLP* ポリシーを適用できるようになります。

プロファイル タイプ	の意味
	はじめに、データ フィルタリングのセットアップを行います。
ファイル ブロッキング プロファイル	ファイアウォールはファイル ブロッキング プロファイルを使用して、指定したファイル タイプの指定したアプリケーションおよび指定したセッション フロー方向（インバウンド、アウトバウンド、両方）のトラフィックをブロックします。アップロードまたはダウンロードでアラート送信またはブロックするプロファイルを設定し、ファイル ブロッキング プロファイルの適用対象となるアプリケーションを指定できます。また、指定したファイル タイプのダウンロードをユーザーが試みるときに表示される、カスタム ブロック ページを設定することもできます。これによりユーザーは、ファイルをダウンロードするかどうか考える時間を持つことができます。 ファイル ブロッキングをセキュリティ ポリシールールに適用するには、独自のファイルブロッキングプロファイルを定義する方法と、以下のどちらかの事前定義プロファイルを選択する方法があります。コンテンツ リリース バージョン 653 以降で利用できる事前定義済みのプロファイルにより、ベストプラクティスのファイル ブロッキング設定を素早く有効化できるようになります。 • **basic file blocking (**基本的なファイル ブロッキング**)**—比較的センシティブでないアプリケーションをトラフィックが出入りするのを許可するセキュリティポリシールールにこのプロファイルをアタッチし、頻繁にマルウェア攻撃キャンペーンに含まれる、あるいはアップロード/ダウンロードする意味がないファイルをブロックします。このプロファイルは PE ファイル（.scr、.cpl、.dll、.ocx、.pif、.exe）、Java ファイル（.class、.jar）、ヘルプファイル（.chm、.hlp）および .vbe、.hta、.wsf、.torrent、.7z、.rar、.bat などの悪意のある可能性があるファイル タイプをアップロードおよびダウンロードするのをブロックします。さらにこれは、ユーザーが encrypted-rar や encrypted-zip ファイルのダウンロードを試みた際にユーザーに確認を求めます。このルールは、他のすべてのファイル タイプに対してアラートを通知することで、ネットワークを出入りするすべてのファイル タイプに完全な可視性をもたらします。 • **strict file blocking (**厳格なファイル ブロッキング**)**—極めて重要なアプリケーションへのアクセスを許可するセキュリティポリシールールでは、この厳格なプロファイルを使用します。このプロファイルは他のプロファイルと同じファイル タイプをブロックするだけでなく、さらに flash、.tar、multi-level encoding、.cab、.msi、encrypted-rar、および encrypted-zip ファイルもブロックします。 ファイル ブロッキング プロファイルに以下のアクションを設定します。

プロファイル タイプ	の意味
	• **alert** - 指定したファイル タイプが検出されると、データ フィルタリング ログでログが生成されます。 • **Block** [ブロック] - 指定したファイル タイプが検出されると、そのファイルはブロックされ、ユーザーに対してカスタマイズ可能なブロック ページが表示されます。データ フィルタリング ログでログも生成されます。 • **continue** - 指定したファイル タイプが検出されると、ユーザーに対して応答ページが表示されます（この応答ページはカスタマイズ可能です）。ユーザーはページをクリックスルーしてファイルをダウンロードすることができます。データ フィルタリング ログでログも生成されます。このタイプの転送アクションは、ユーザーとのやり取りが必要になるため、Web トラフィックにのみ使用可能です。 はじめに、ファイル ブロッキングのセットアップを行います。
WildFire 分析プロファイル	ファイアウォールが 不明なファイルまたは電子メール リンクを転送して WildFire 分析を実行できるようにするには、WildFire 分析プロファイルを使用します。アプリケーション、ファイル タイプ、および送信方向（アップロードまたはダウンロード）に基づいて、転送して分析を行うファイルを指定します。プロファイル ルールに一致するファイルまたは電子メール リンクは、ルールで定義された分析場所に応じて、WildFire パブリック クラウドまたは WildFire プライベート クラウド（WF-500 アプライアンスでホスト）のいずれかに転送されます。ファイルを WildFire パブリック クラウドに転送するようにプロファイル ルールが設定されている場合、ファイアウォールは未知のファイルに加え、既存のアンチウイルス シグネチャにマッチするファイルも転送します。 WildFire 分析プロファイルを使用して、 WildFire ハイブリッド クラウド デプロイメントをセットアップすることもできます。WildFire アプライアンスを使用して機密性の高いファイル（PDF など）をローカルで分析している場合、機密性の低いファイル タイプ（PE ファイルなど）または WildFire アプライアンス分析ではサポートされていないファイル タイプ（APK など）を WildFire パブリック クラウドで分析するように指定できます。WildFire アプライアンスと WildFire クラウドの両方を分析に使用することで、クラウドですでに処理されているファイルとアプライアンスではサポートされていないファイルを即座に判定し、機密性の高いコンテンツ用にアプライアンスの容量を確保できます。
DoS 防御プロファイル	DOS プロテクション プロファイルでは、サービス拒否（DoS）防御ポリシーの詳細を制御できます。DoS ポリシーでは、インターフェイス、ゾーン、アドレス、国に対するセッション数を、セッション総数、送信元 IP アドレスおよび宛先 IP アドレス毎に基いて制御できま

プロファイル タイプ	の意味
	す。Palo Alto Networks のファイアウォールでサポートされる DoS プロテクション メカニズムは以下の 2 つです。 • フラッド防御 - ネットワークがパケットでフラッドされたために、ハーフオープン セッションの数が非常に多くなったり、サービスが各要求に応答できなくなる攻撃を検出および防御します。この場合、攻撃の送信元アドレスは通常偽装されています。新規セッションのフラッド攻撃に対する DoS プロテクションの設定を参照してください。 • リソース保護 - セッション消耗攻撃を検出および防御します。このタイプの攻撃では、大量数のホスト（ボット）を使用して完全に確立されたセッションを可能な限り多く確立し、システム リソースのすべてを消費します。 1 つの DOS プロテクション プロファイルで、これら両方の防御メカニズムを有効にできます。 DoS プロファイルを使用して、実行するアクションのタイプと DoS ポリシーの照合基準の詳細を指定します。DoS プロファイルでは、SYN、UDP、および ICMP フラッドの設定項目を定義し、リソースの保護を有効にし、最大同時接続数を定義します。DoS プロテクション プロファイルを設定したら、DoS ポリシーに適用します。 DoS プロテクションの設定時には、適正なしきい値を設定するため、使用環境を分析することが重要です。また、DoS プロテクション ポリシーの定義にはいくつかの複雑な設定が関係しているため、このガイドでは詳細な例は示しません。
ゾーン保護プロファイル	ゾーン プロテクション プロファイルでは、ゾーンを攻撃から保護するため、特定のネットワーク ゾーン間の保護を強化します。プロファイルはゾーン全体に適用する必要があるため、各ゾーンを通過する通常のトラフィックによって問題が発生しないようにするため、慎重にプロファイルをテストすることが重要です。ゾーン プロテクション プロファイルにパケット/秒 (pps) のしきい値制限を定義する場合、しきい値は以前に確立したセッションと一致しないパケット/秒を基にしています。
セキュリティ プロファイル グループ	セキュリティ プロファイル グループは、セキュリティ プロファイルのセットとして、1 つの単位として処理でき、セキュリティ ポリシーに追加できます。同時に割り当てられることが多いプロファイルをプロファイル グループにまとめることで、セキュリティ ポリシーの作成を簡略化できます。また、デフォルトのセキュリティ プロファイル グループをセットアップすることもできます。新規のセキュリティ ポリシーは、デフォルトのプロファイル グループに定義されている設定を使用して、セキュリティ ポリシーに一致するトラフィックをチェックおよび制御できます。セキュリティ プロファイル グループに「default」という名前を付けると、そのグループに属する

プロファイル タイプ	の意味
	プロファイルをデフォルトで新規のセキュリティ ポリシーに追加できます。これにより、組織の優先プロファイル設定が新規のポリシーにいつでも自動的に追加されるようになるため、新規ルールを作成するたびにセキュリティ プロファイルを手動で追加する手間が省けます。 セキュリティ プロファイル グループの作成およびデフォルトのセキュリティ プロファイル グループの設定またはオーバーライドを参照してください。 セキュリティ プロファイルの推奨設定についてはインターネット ゲートウェイ用の最良のセキュリティ プロファイルを作成をご覧ください。

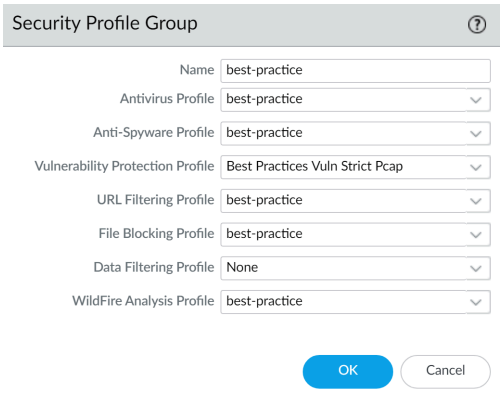
セキュリティ プロファイル グループの作成

セキュリティ プロファイル グループを作成して、セキュリティ ポリシーに追加するには、以下の手順を実行します。

STEP 1 | セキュリティ プロファイル グループを作成する。

*default*という名前にしたグループは、作成したあらゆる新しいルールにファイアウォールによって自動的に付与されます。すべての新しいルールに必ず付与する一連のセキュリティ プロファイルがある場合、これを使って作業時間を短縮できます。

1. **Objects (オブジェクト)** > **Security Profile Groups (セキュリティ プロファイル グループ)** の順に選択し、新規のセキュリティ プロファイル グループを **Add (追加)** します。
2. プロファイル グループに分かりやすい [名前]（たとえば、「脅威」）をつけます。
3. ファイアウォールがマルチ仮想システム モードになっている場合は、プロファイルをすべての仮想システムで [共有] 可能にします。
4. 既存のプロファイルをグループに追加します。



5. **[OK]** をクリックしてプロファイル グループを保存します。

STEP 2 | セキュリティ プロファイル グループをセキュリティ ポリシーに追加します。

1. **Policies (**ポリシー**)** > **Security (**セキュリティ**)**を選択し、セキュリティポリシールールを**Add**（追加）または変更します。
2. **[**アクション**]** タブを選択します。
3. Profile Setting (プロファイル設定) セクションで、**Profile Type (**プロファイル タイプ**)** として **Group (**グループ**)** を選択します。
4. **Group Profile (**グループ プロファイル**)** ドロップダウン リストで、作成したグループ（たとえば、ベストプラクティス グループ）を選択します。

5. **OK** をクリックしてポリシーを保存し、変更を **Commit (**コミット**)** します。

STEP 3 | 変更を保存します。

Commit（コミット）をクリックします。

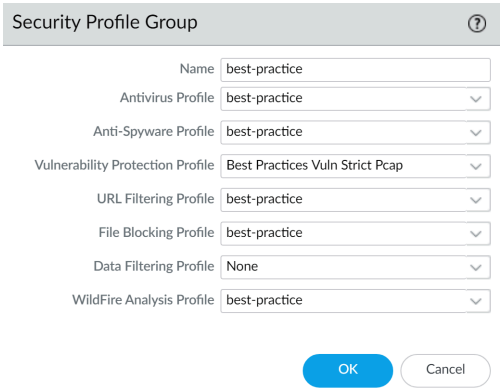
デフォルトのセキュリティ プロファイル グループの設定またはオーバーライド

新規のセキュリティ ポリシーで使用するデフォルトのセキュリティ プロファイル グループの設定、または既存のデフォルト グループのオーバーライドを実行するには、以下の手順を実行します。新規のセキュリティ ポリシーを作成する際には、デフォルトのプロファイル グループが自動的に新規ポリシーのプロファイル設定として選択され、そのポリシーに一致するトラフィックが、プロファイル グループに定義された設定に従ってチェックされます（必要に応じて、デフォルトとは異なるプロファイル設定を手動で選択することもできます）。デフォルトのセキュリティ プロファイル グループの設定、またはデフォルトの設定のオーバーライドを実行するには、以下の手順を実行します。

デフォルトのセキュリティ プロファイルが存在しない場合、新規のセキュリティ ポリシーのプロファイル設定は、デフォルトで *[*なし*]* に設定されます。

セキュリティ プロファイル グループを作成する。

1. **Objects (**オブジェクト**)** > **Security Profile Groups (**セキュリティ プロファイル グループ**)** の順に選択し、新規のセキュリティ プロファイル グループを Add (追加) します。
2. プロファイル グループに分かりやすい **[**名前**]**（たとえば、「脅威」）をつけます。
3. ファイアウォールがマルチ仮想システム モードになっている場合は、プロファイルをすべての仮想システムで **[**共有**]** 可能にします。
4. 既存のプロファイルをグループに追加します。プロファイル作成の詳細についてはセキュリティ プロファイルを参照してください。

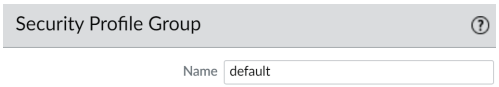


5. **[OK]** をクリックしてプロファイル グループを保存します。
6. セキュリティ プロファイル グループをセキュリティ ポリシーに追加します。
7. セキュリティ ポリシー ルールを **[**追加**]** または変更して、**[**アクション**]** タブを選択します。
8. **Profile Type (**プロファイル タイプ**)** として **Group (**グループ**)** を選択します。
9. **Group Profile (**グループ プロファイル**)** ドロップダウン リストで、作成したグループ（たとえば、脅威グループ）を選択します。

10. **OK** をクリックしてポリシーを保存し、変更を **Commit (**コミット**)** します。

デフォルトのセキュリティ プロファイル グループを設定します。

1. **Objects (オブジェクト)** > **Security Profile (セキュリティ プロファイル) Groups** を選択して、新規のセキュリティ プロファイル グループを追加するか、既存のセキュリティ プロファイル グループを変更します。
2. セキュリティ プロファイル グループに「**default**」という [名前] を付けます。



3. **OK**、**Commit (コミット)** の順にクリックします。
4. default というセキュリティ プロファイル グループが新規のセキュリティ ポリシーにデフォルトで含まれていることを確認します。
   1. **Policies (ポリシー)** > **Security (セキュリティ)** を選択して新しいセキュリティポリシーを **Add (追加)** します。
   2. [アクション] タブを選択して、[プロファイル設定] フィールドを表示します。

   デフォルトでは、新規のセキュリティ ポリシーの **Profile Type** （プロファイル タイプ）が Group（グループ）に設定されており、**Group Profile**（グループ プロファイル）として default が選択されています。

デフォルトのセキュリティ プロファイル グループをオーバーライドします。

既存のデフォルト セキュリティ プロファイル グループのプロファイル セットを新規のセキュリティ ポリシーに適用しない場合は、自分の好みに合わせてプロファイル設定を変更してください。その場合は、まずポリシーのプロファイル タイプを選択するところから始めます（**Policies (ポリシー)** > **Security (セキュリティ)** > **Security Policy Rule (セキュリティ ポリシー ルール)** > **Actions** （アクション））。

ルールベース内のルールの追跡

ルールベース内のルールを追跡するために、ルールベースにおけるルールの順序によって変化するルール番号を参照することができます。ルール番号は、ファイアウォールがルールを適用する順序を決定します。

ルール名を変更するなどしてルールを変更しても、ルールの *universally unique identifier (UUID)* は変化しません。UUID により、ルールを削除した後でも、複数のルールベースにかけてルールを追跡できるようになります。

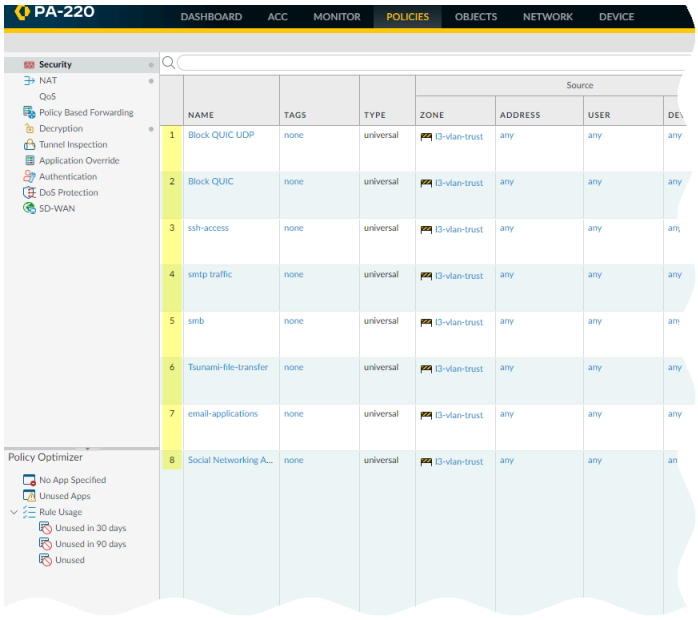
ルール番号

ファイアウォールは自動的にルールベース内の各ルールに番号を振ります。ルールを移動させたり順序を変えたりすると、新しい順序に基づいて番号が変化します。ルールのリストをフィルタリングして特定の条件にマッチするルールを検索する際、ファイアウォール上で各ルールはルールベース内の全ルールのコンテキストで番号が振られ、評価順に従って並べられます。

Panorama はプレルール、ポストルール、デフォルトルールに独自の番号を付けます。Panorama がルールをファイアウォールにプッシュするときに、ルールの付番は共有ルール、デバイス グループのプレ ルール、ファイアウォール ルール、デバイス グループのポスト ルールおよびデフォルト ルールの階層と評価順を反映します。Panorama で **Preview Rules**（ルールのプレビュー）を行い、ファイアウォールの全ルールの順序付きリストが表示されます。

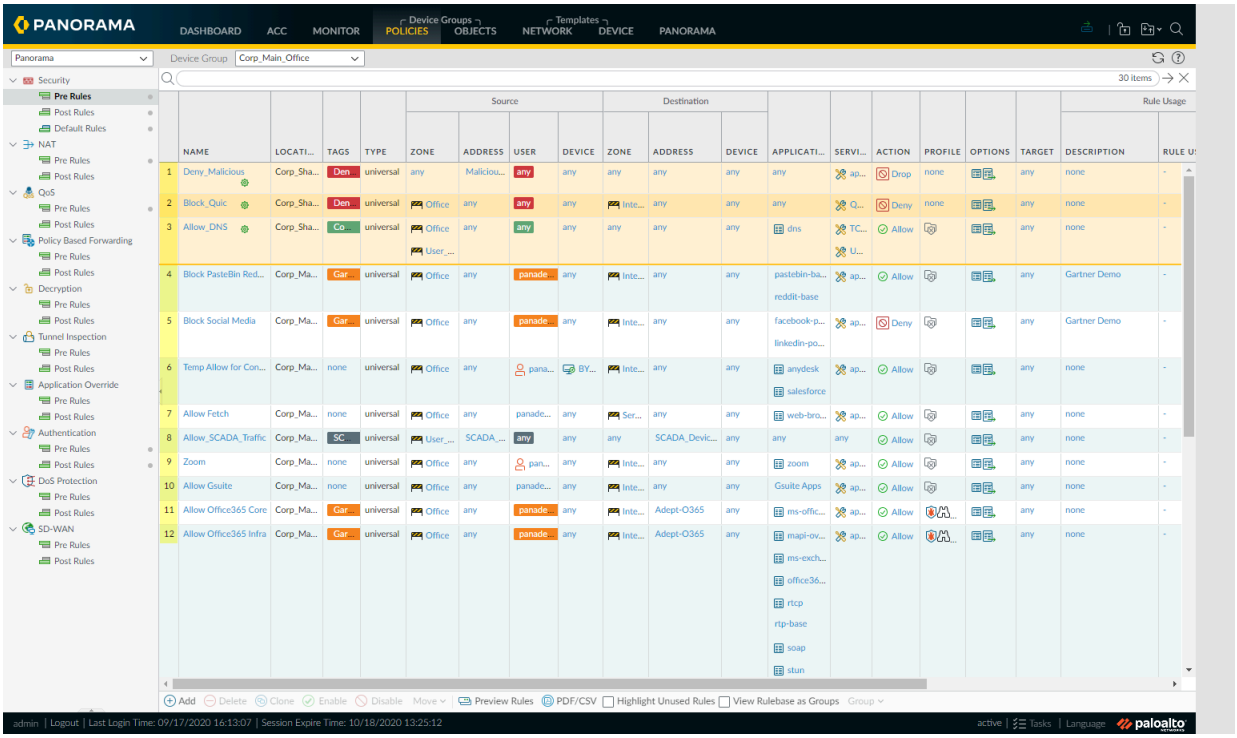
ファイアウォール上のルールの番号付きリストを表示します。

[Policies] を選択し、その配下のルールベースを選択します。例えば、 **Policies (ポリシー)** > **Security (セキュリティ)**。表の最左端の列にルール番号が表示されます。



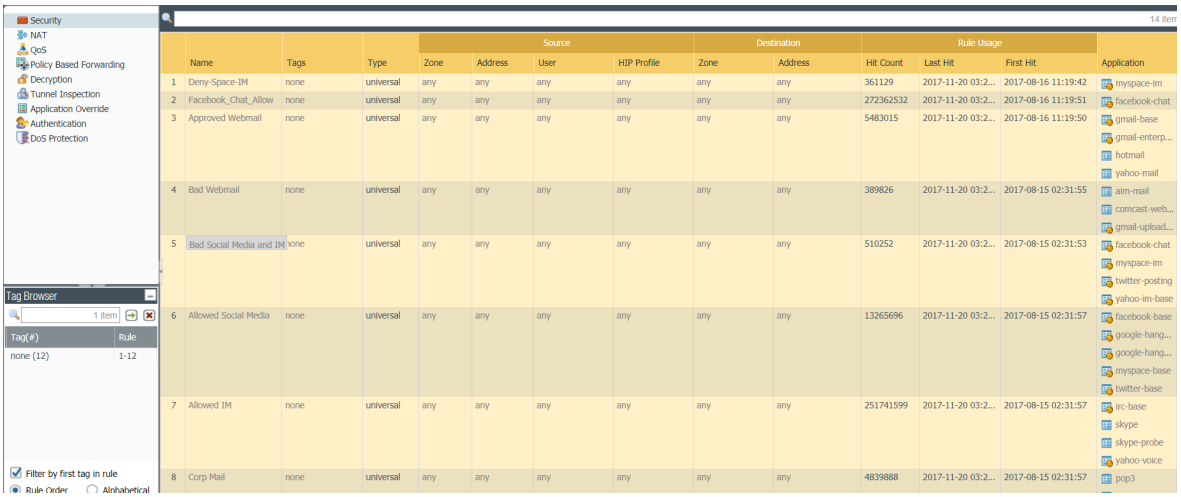
Panorama 上のルールの番号付きリストを表示します。

[Policies] を選択し、その配下のルールベースを選択します。例えば、**Policies (ポリシー)** > **Security (セキュリティ** > **Pre-rules**。



Panorama からルールをプッシュすると、ファイアウォール上の番号の付いたルールの全リストが表示されます。

ファイアウォールの Web インターフェイスで **Policies**（ポリシー）を選択して、その配下の任意のルールベースを選択します。たとえば、 **Policies (ポリシー)** > **Security (セキュリティ)** の順に選択すると、ファイアウォールで評価されるすべての番号付きルールが表示されます。



ルールの UUID

ルールの universally unique identifier (UUID) は、ファイアウォールあるいは Panorama がルールに付与する 32 文字の文字列です (ネットワーク アドレスや作成時のタイムスタンプなどのデータに基づきます)。UUID は 8-4-4-4-12 の書式を使用します (8、4、12 が一意の文字を表し、ハイフンでそれらを区切ります)。UUID はすべてのポリシー ルールベースを識別します。また、UUID を使って次のログ タイプで対象のルールを識別することもできます：Traffic、Threat、URL Filtering、WildFire Submission、Data Filtering、GTP、SCTP、Tunnel Inspection、Configuration、および Unified。

UUID を使ってルールを検索することで、同じような、あるいは同じ名前を持つかもしれない数千のルールの中から特定のルールを探せるようになります。また、UUID は名前をサポートしていないサードパーティ システム (チケット発行やオーケストレーションなど) でルールを自動化・統合する作業を簡単にします。

一部のケースでは、既存のルールベースに対して新しい UUID を生成しなければならない場合があります。例えば、別のファイアウォールに設定をエクスポートしたい場合、UUID の重複を回避するために、設定をインポートする際にルールの ***UUID*** を生成する必要があります。UUID を再生成すると、以前の UUID を使用して対象のルールを追跡できなくなり、ルールのヒットデータおよびアプリ使用状況データがリセットされます。

ファイアウォールあるいは Panorama は次の場合に UUID を割り当てます：

- ルールを新規作成
- 既存のルールをコピー
- デフォルトのセキュリティルールをオーバーライド
- 名前を付けた設定を読み込んで UUID を再生成
- 現在アクティブな設定にはない新しいルールを含む、名前を付けた設定を読み込む
- ファイアウォールあるいは Panorama を PAN-OS 9.0 リリースにアップグレード

UUID を持つルールを含む設定を読み込む際、ファイアウォールはルール名、ルールベース、仮想システムがすべて一致する場合、ルールを同一のものとみなします。Panorama は、ルール名、ルールベース、デバイスグループがすべて一致する場合、ルールを同一のものとみなします。

UUID に関する次の重要な内容にご注意ください：

- Panorama からファイアウォール ポリシーを管理する場合、UUID は Panorama 上で生成されるため、Panorama からプッシュする必要があります。ファイアウォールを PAN-OS 9.0 にアップグレードする前に Panorama から設定をプッシュしないと、ファイアウォールが UUID を持たなくなるため、ファイアウォールのアップグレードが成功しません。
- さらに HA ペアをアップグレードする場合、PAN-OS 9.0 にアップグレードする際に各ピアが独立して各ポリシールールの UUID を割り当てます。そのため、設定を同期 (**Dashboard (ダッシュボード)** > **Widgets (ウィジェット)** > **System (システム)** > **High Availability (高可用性)** > **Sync to peer (ピアと同期)**) するまで、ピアが同期されていないと表示されます。
- PAN-OS 9.0 にアップグレードしてから既存の高可用性 (HA) 構成を削除する場合、いずれかのピアで UUID を再生成 (**Device (デバイス)** > **Setup (セットアップ)** > **Operations (操作)** > **Load named configuration snapshot (名前付きのスナップショットを読み込み)** > **Regenerate**

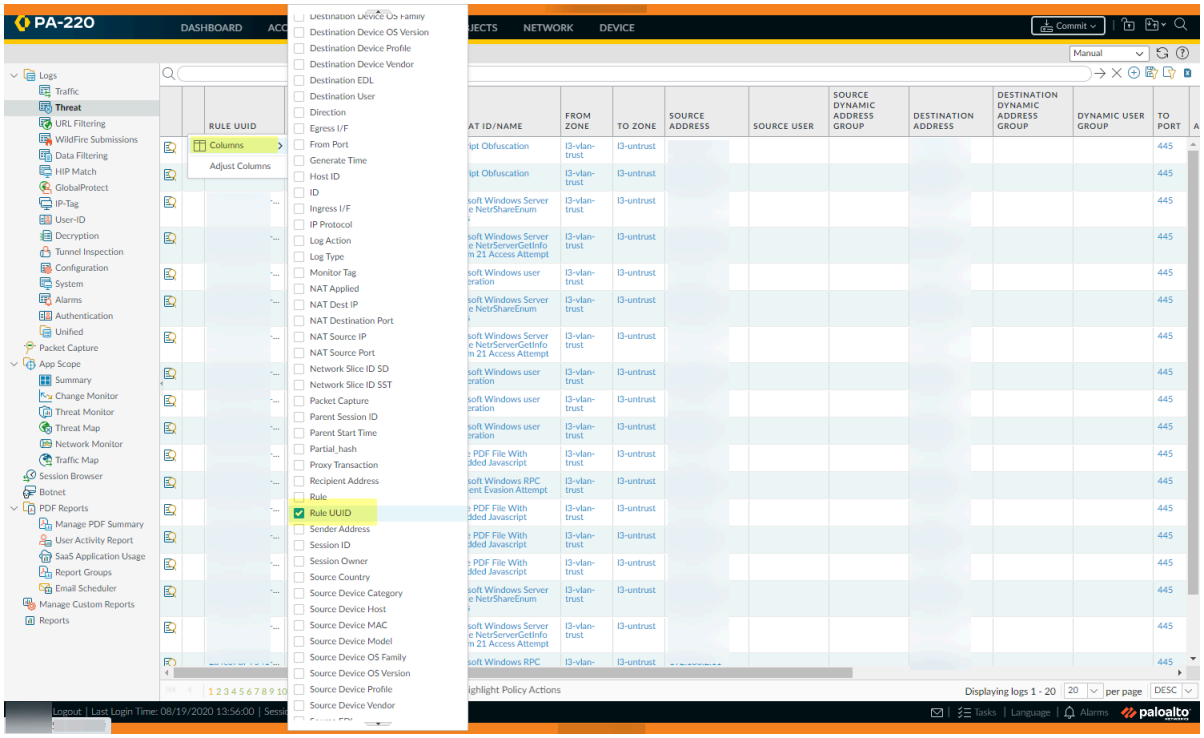
UUIDs for the selected named configuration (選択した名前付きの設定のために **UUID** を再生成**)**) して変更をコミットし、UUID の重複を回避する必要があります。

- Panorama からプッシュされたすべてのルールは同じ UUID を共有します。ファイアウォールのローカルにあるすべてのルールは別の UUID を持ちます。Panorama からファイアウォールにルールをプッシュしてからファイアウォールのローカルでルールを作成する場合、ローカルで作成したルールは独自の UUID を持ちます。
- RMA Panorama を置き換える場合、名前付きの Panorama 設定スナップショットを読み込む際に必ず **Retain Rule UUIDs (**ルールの **UUID** を維持**)** してください。このオプションを選択しない場合、Panorama は以前のルールの UUID をすべて設定スナップショットから削除し、新しい UUID を Panorama 上のルールに割り当てます。つまり、ポリシールール ヒット数など、以前の UUID に紐付いていた情報は保持されません。

ログではルールの UUID 列を、ポリシールールでは UUID 列を表示します。

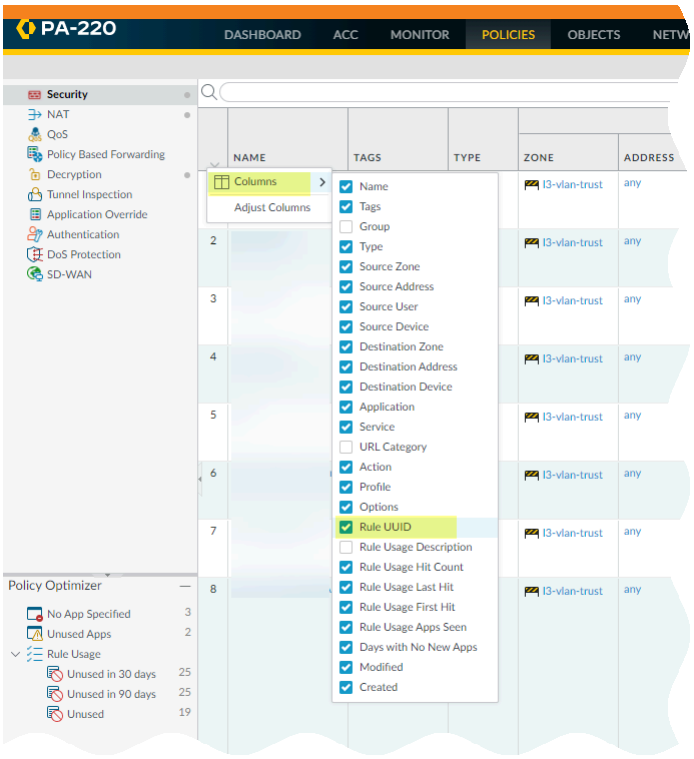
UUID を表示するには、デフォルトでは非表示に設定されている列を表示する必要があります。

- ログで UUID を表示する方法：
  1. [モニター] を選択し、列ヘッダー (▾) を展開します。
  2. 選択 列.
  3. Enable **Rule UUID**.



- ポリシー ルールベースで UUID を表示する方法：
  1. **Policies** を選択し、列ヘッダー (▾) を展開します。
  2. 選択 列.
  3. ルール **UUID** を有効にします。

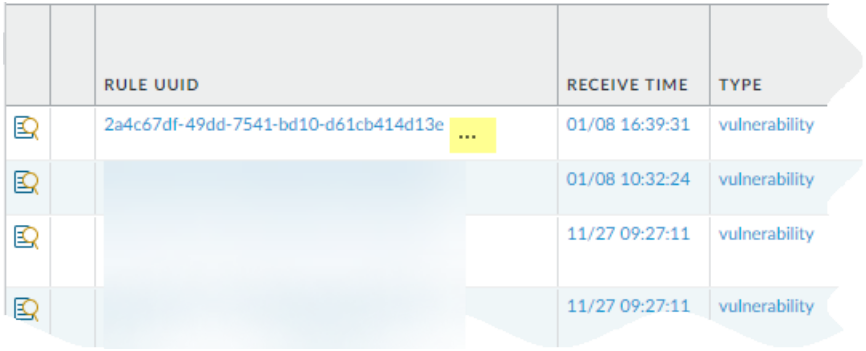
     UUID はすべてのポリシールールベースで使用できます。



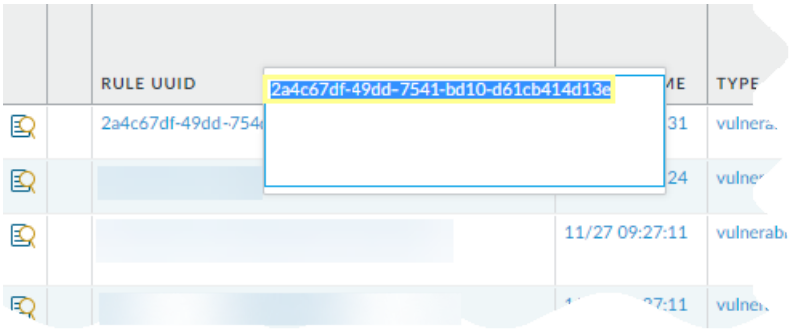
ログあるいはポリシールールの UUID をコピーします。

UUID をコピーすれば、検索、ACC、カスタム レポート、フィルタや、UUID を使ってルールを識別できる場所ならどこでも、UUID をペーストできるようになります。

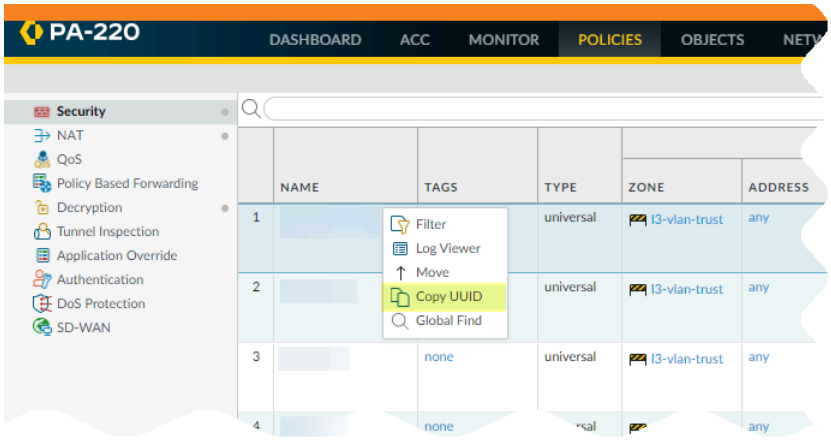
1. ルールの UUID 列にある項目にカーソルを合わせると表示される楕円を選択します。



2. ポップアップから UUID をコピーします。



また、**Policies (**ポリシー**)** タブに移動してルール名の右にある矢印をクリックして **Copy UUID (UUID** をコピー**)** することもできます。



設定ログをチェックして削除されたルールの UUID を表示します。

削除されたルールの UUID を表示するには、**Monitor (**監視**)** > **Logs (**ログ**)** > **Configuration (**設定**)** を選択します。

ポリシールールの説明、タグ、監査コメントを適用

ルールを作成あるいは変更する際、ルールの説明、タグ、監査コメントを必須にして、ポリシールールベースを確実に正しく整理・グループ化することで、重要なルールの履歴を監査目的で維持することができるようになります。ルールを作成あるいは変更する際にルールの説明、タグ、監査コメントを必須にし、確実にルールを適切にグループ化してルールの変更履歴を残すことで、ポリシー ルールベースのレビューを簡略化できます。統一性を確保するため、監査コメントに含められる項目について、特定の要件を設定することができます。

デフォルト設定では、説明、タグ、監査コメントの強制は有効になっていません。ルールを追加したり変更したりするために説明、タグ、監査コメント、あるいはそれらの任意の組み合わせが必要かどうかを指定することができます。監査コメント アーカイブを使用すれば、選択したルールで入力された監査コメントを閲覧し、設定ログの履歴を確認し、ルールの構成バージョンを比較することができます。

STEP 1 | 「Web インターフェイスの起動」を行います。

STEP 2 | **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択し、Policy Rulebase Settings (ポリシー ルールベース設定) を編集します。

STEP 3 | 適用したい設定を構成します。この例では、タグおよび監査コメントがすべてのポリシーで必要になります。

ポリシールールの監査コメントを強制し、管理者がルールを作成あるいは修正した理由を記録します。ポリシールールで監査コメントを強制することで、監査目的でルールの履歴を正確に確保することができます。

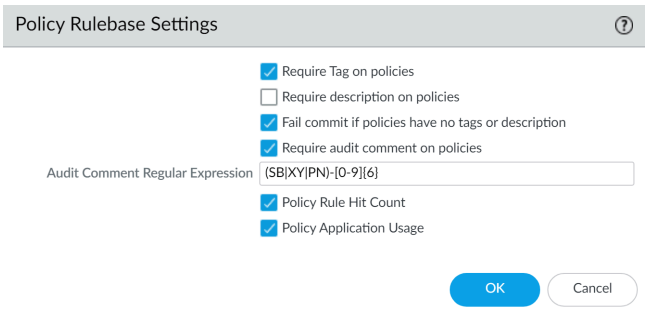
STEP 4 | 監査コメント正規表現を設定し、監査コメントの書式を指定します。

管理者がルールを作成あるいは変更する際、文字と数字の表現を指定することで、ビジネスニーズや監査ニーズに即した特定の書式で監査コメントを入力するよう求めることができます。例えば、この設定を使用し、チケット番号の書式と一致する正規表現を指定することができます：

- **[0-9]{<Number of digits>}** - 監査コメントに 0 ~ 9 の範囲の最小桁数を含める必要があります。例えば**[0-9]**は、0〜9 の数字から成る 6 桁以上の表現を求めます。
- <文字表現>—文字表現が含まれる監査コメントを求めます。例えば **Reason for Change-** は、監査コメントをこの文字表現で始めることを管理者に求めます。
- <**Letter Expression**>-**[0-9]{<Number of digits>}** - 監査コメントに、あらかじめ定義された文字の後に 0 ~ 9 の範囲の最小桁数を含める必要があります。例えば**SB-[0-9]** は、 **SB-**で始まり、0〜9 の数字から成る 6 桁以上の表現が続く監査コメントの書式を求めます。以下に例を示します。**SB-012345**.
- **(**<**Letter Expression**>**)|(**<**Letter Expression**>**)|(**<**Letter Expression**>**)|-[0-9]{<Number of digits>}** - 監査コメントに、0 ~ 9 の範囲の最小桁数を持つ事前定義された文字式のいずれかを使用するプレフィックスを含める必要があります。例えば **(SB|XY|PN)-[0-9]** は、**SB-**、**XY-**、あるいは **PN-** で始ま

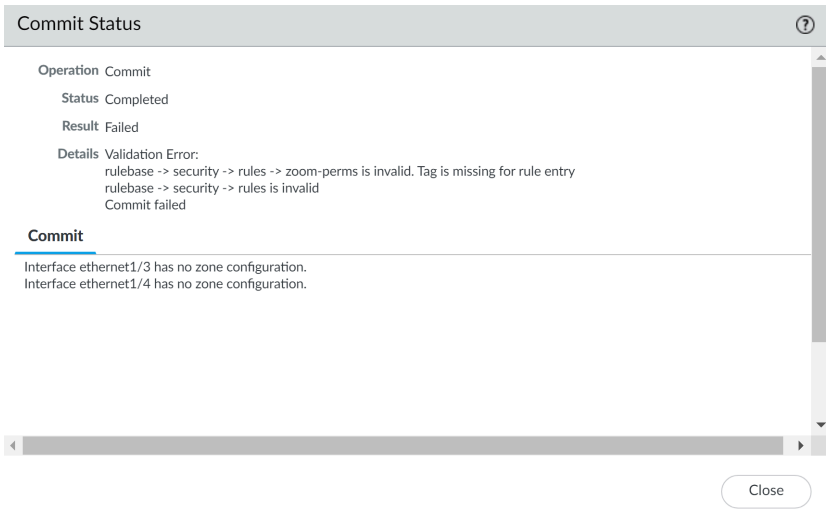
り、0～9 の数字から成る 6 桁以上の表現が続く監査コメントの書式を求めます。例えば、**SB-012345**、**XY-654321**、**PN-012543** などです。

STEP 5 | **OK** をクリックして新しいポリシー ルールベースの設定を適用します。



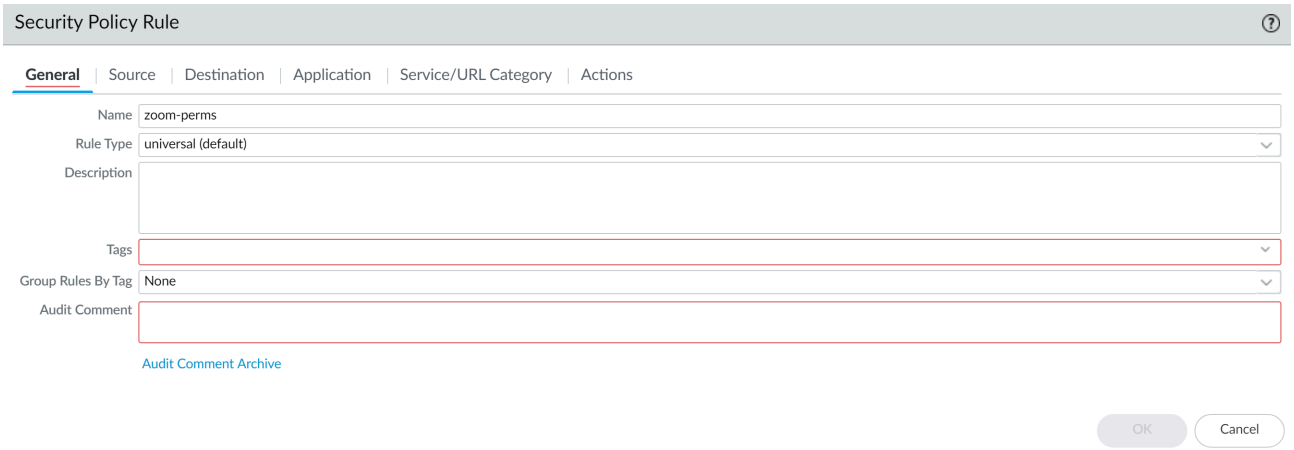
STEP 6 | 変更を **Commit**（コミット）します。

ポリシー ルールベース設定の変更をコミットしたら、ルールベース設定で適用する既存のポリシールールベースを変更します。



STEP 7 | ファイアウォールが新しいポリシー ルールベース設定を適用していることを確認します。

1. **Policies (ポリシー)** を選択し、新しいルールを **Add(追加)** します。
2. タグを追加して監査コメントを入力しなければならないことを確認し、**OK** をクリックします。



ポリシー ルールまたはオブジェクトの異なる仮想システムへの移動またはコピー

複数の仮想システム（vsys）があるファイアウォールでは、ポリシー ルールとオブジェクトを異なる vsys または共有場所に移動またはコピーできます。移動とコピーにより、ルールとオブジェクトの削除、再作成、または名前変更を行う手間を省くことができます。vsys から移動またはコピーするポリシー ルールやオブジェクトがその vsys 内のオブジェクトを参照している場合、参照されているオブジェクトも移動またはコピーします。共有オブジェクトを参照している場合は、移動またはコピー時にそれらのオブジェクトを含める必要はありません。グローバル検索を使用してファイアウォールあるいは Panorama の管理サーバーを検索することができます。

複数のポリシー ルールをコピーするとき、ルールを選択する順序により、ルールがデバイス グループにコピーされる順序が決まります。たとえば、ルール *1* ～ *4* があり、選択順序が、*2*、*1*、*4*、*3* である場合、このルールがコピーされるデバイス グループでは、この選択順序でルールが表示されます。ただし、正常にコピーされた後で、ルールの順序を適切に変更できます。

STEP 1 | ポリシータイプ（例：**Policy (ポリシー)** > **Security (セキュリティ)**）あるいはオブジェクトタイプ（例：**Objects (オブジェクト)** > **Addresses (アドレス)**）を選択します。

STEP 2 | **Virtual System (仮想システム)** を選択し、1 つ以上のポリシー ルールまたはオブジェクトを選択します。

STEP 3 | 以下のいずれかの手順を実行します。

- **Move (移動)** > **Move to other vsys (他の vsys に移動)** の順に選択します（ポリシー ルールの場合）。
- **Move** [移動]をクリックします（オブジェクトの場合）。
- **Clone** [コピー]をクリックします（ポリシー ルールまたはオブジェクトの場合）。

STEP 4 | **Destination** [宛先]ドロップダウン リストで、新しい仮想システムまたは **Shared** [共有]を選択します。

STEP 5 | （ポリシー ルールのみ）**Rule order** [ルール順序]を選択します。

- **Move top**（最上部へ） — （デフォルト）他のすべてのルールの前の位置を選択します。
- **Move bottom**（最下部へ） — 他のすべてのルールの後の位置を選択します。
- **Before rule**（事前ルール） — 隣接するドロップダウン リストで、選択されたルールの直後のルールを選択します。
- **After rule**（事後ルール） — 隣接するドロップダウン リストで、選択されたルールの直前のルールを選択します。

STEP 6 | **Error out on first detected error in validation** [検証で最初に検出されたエラーに対するエラーを出す]チェック ボックスはデフォルトでオンになっています。ファイアウォールが最初のエラーを検出すると、移動またはコピー アクションの確認が停止され、このエラー

のみが表示されます。たとえば、移動するポリシー ルールで参照されるオブジェクトが **Destination** [宛先] vsys に存在しない場合、ファイアウォールでこのエラーが表示され、その後の検証は停止します。同時に複数の項目を移動またはコピーするときにこのチェック ボックスをオンにしていると、一度に 1 つのエラーを検出してトラブルシューティングを行うことができます。チェック ボックスをオフにすると、ファイアウォールはエラーのリストを収集して表示します。検証でエラーが発生した場合、すべてのエラーを修正するまでオブジェクトは移動またはコピーされません。

STEP 7 | **OK** をクリックしてエラーの検証を開始します。ファイアウォールにエラーが表示される場合は、エラーを修正して移動またはコピー操作を再試行します。ファイアウォールでエラーが検出されない場合、オブジェクトは正常に移動またはコピーされます。操作が完了したら、**Commit** [コミット]をクリックします。

アドレス オブジェクトを使用して IP アドレスを表す

ファイアウォール上にアドレスオブジェクトを作成して IP アドレスをグループ化するか、または FQDN を指定してから、そのルール、フィルタ、またはその他の機能内で複数の IP アドレスを個別に指定しなくても済むようにファイアウォールポリシールール、フィルタ、またはその他の機能でアドレスオブジェクトを参照します。

さらに、各用途で同じ個別のアドレスを指定することなく、複数のポリシールール、フィルタ、または他の機能で同じアドレスオブジェクトを参照することができます。例えば、IPv4 アドレス範囲を指定するアドレスオブジェクトを作成してから、セキュリティポリシールール、NAT ポリシールール、およびカスタムレポートログフィルタでそのアドレスオブジェクトを参照できます。

- アドレス オブジェクト
- アドレス オブジェクトの作成

アドレス オブジェクト

アドレス オブジェクトは、一か所で管理して、その後複数のファイアウォール ポリシールール、フィルタ、他の機能で使用できる一連の IP アドレスです。アドレス オブジェクトには、次の 4 種類があります。**IP Netmask (IP** ネットマスク**)**、**IP Range (IP** 範囲**)**、**IP Wildcard Mask (IP** ワイルドカード マスク**)**、および **FQDN**。

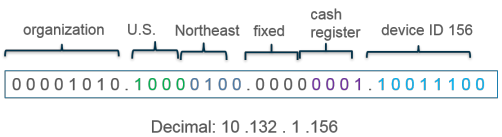
IP Netmask (IP ネットマスク**)**、**IP Range (IP** 範囲**)**、**FQDN** タイプのアドレス オブジェクトは IPv4 あるいは IPv6 アドレスを指定できます。タイプ の **IP** ワイルドカード マスク のアドレス オブジェクトは、IPv4 アドレスのみを指定できます。

タイプ の **IP Netmask** のアドレス・オブジェクトでは、IPv4 ネットワークまたは IPv6 接頭部長を示すためにスラッシュ表記を使用して IP アドレスまたはネットワークを入力する必要があります。例えば、192.168.18.0/24 または 2001:db8:123:1::/64。

タイプ の **IP** 範囲 のアドレス オブジェクトでは、ハイフンで区切られた IPv4 または IPv6 アドレスの範囲を入力する必要があります。

ユーザーが IP アドレスを知り、FQDN が新しい IP アドレスに解決される度に手動で更新することなく、DNS が IP アドレスへの FQDN 解決を提供するため、使いやすいのが **FQDN** 型のアドレス オブジェクト (例えば paloaltoneworks.com) です。

内部デバイスへのプライベート IPv4 アドレスを定義し、アドレス内の特定のビットに意味を持たせるアドレス構造である場合、便利なのが **IP Wildcard Mask (IP** ワイルドカード マスク**)** 型のアドレス オブジェクトです。例えば、アメリカ合衆国北東部のキャッシュレジスタ 156 の IP アドレスは、これらのビット割り当てに基づくと 10.132.1.156 になるでしょう：



タイプ の **IP** ワイルドカード マスク のアドレス オブジェクトは、セキュリティ ポリシー規則に従う送信元または宛先アドレスを指定します。たとえば、10.132.1.1/0.0.2.255 です。マスクの

0bit (ビット- bit) は、比較対象のbit (ビット- bit)が、0 がカバーする IP アドレスのbit (ビット- bit)と一致しなければならないことを示します。マスク内の 1 ビット (**1**) (ワイルドカードビット) は、比較対象のビットが IP アドレスのビットと一致する必要がないことを示します。次の IP アドレスおよびワイルドカード マスクのスニペットは、これらがどのようにマッチを得るのか示しています：

```
0 0 1 1    binary snippet
1 0 1 0    wildcard mask
---------
0 0 0 1    yields four matches
0 0 1 1
1 0 0 1
1 0 1 1
```

アドレス オブジェクトの作成を行った後:

- セキュリティ、認証、NAT、NAT64、復号化、DoS 保護、ポリシーベース フォワーディング (PBF)、QoS、アプリケーション オーバーライド、トンネル検査のポリシールール、あるいは NAT アドレス プール、VPN トンネル、パス モニタリング、外部動的リスト、偵察行為防御、ACC グローバルフィルタ、ログ フィルタ、カスタム レポート ログ フィルタで **IP Netmask (IP** ネットマスク)、**IP Range (IP** 範囲)、あるいは **FQDN** 型のアドレス オブジェクトを参照できます。
- タイプ の **IP** ワイルドカード マスク のアドレス オブジェクトは、セキュリティ ポリシー ルールでのみ参照できます。

アドレス オブジェクトの作成

1 つ以上の IP アドレスを表すアドレス オブジェクトを作成し、1 つ以上のポリシー規則、フィルター、またはその他の firewall 関数でアドレス・オブジェクトを参照します。アドレスのセットを変更する場合は、複数のポリシールールまたはフィルタを変更するのではなく、アドレスオブジェクトを 1 回変更するだけで、運用上のオーバーヘッドを削減できます。

STEP 1 | アドレスオブジェクトを作成します。

1. **Objects (**オブジェクト**)** > **Addresses (**アドレス**)** を選択して、**Name (**名前**)** でアドレスオブジェクトを **Add (**追加**)** します。名前は大文字と小文字を区別し、一意の名前を最大 63 文字 (文字、数字、スペース、ハイフン、アンダースコア) で入力する必要があります。
2. アドレスオブジェクトの **Type (**タイプ**)** を選択します。
   - **IP Netmask (IP** ネットマスク**)**—単一の IPv4 または IPv6 アドレス、スラッシュ表記の IPv4 ネットワーク、または IPv6 アドレスとプレフィックスを指定します。例えば、192.168.18.0/24 または 2001:db8:123:1::/64。必要に応じて、(ファイアウォールまたはパノラマの DNS 構成に基づいて) 関連する FQDN を表示するには、**Resolve (**解決**)** をクリックします。アドレスオブジェクトの種類 **IP Netmask (IP** ネットマスク**)** から **FQDN** に変更するには、FQDN を選択して、**Use this FQDN (**この **FQDN** を使用**)** をクリックします。**Type (**タイプ**)** が **FQDN** に代わり、選択した FQDN がテキストフィールドに表示されます。

- **IP Range (IP 範囲)**—ハイフンで区切られた IPv4 アドレスまたは IPv6 アドレスの範囲を指定します。例えば、192.168.40.1-192.168.40.255 または 2001:db8:123:1::1-2001:db8:123:1::22 です。
- **IP Wildcard Mask (IP** ワイルドカード マスク**)**—IP ワイルドカードアドレスを指定します (IPv4 アドレスの後にスラッシュとマスクが続き、0 から始める必要があります)。例：10.5.1.1/0.127.248.2マスクのゼロ（**0**）は、比較されるビットが、0 でカバーされる IP アドレスのビットと一致しなければならないことを示します。マスク内の 1（**1**）（ワイルドカードbit (ビット- bit)）は、比較対象のビットが、1 がカバーする IP アドレスのbit (ビット- bit)と一致する必要がないことを示します。
- **FQDN**—ドメイン名を指定します。FQDN はコミット時に最初に解決されます。その後、ファイアウォールは、TTL が構成した**Minimum FQDN Refresh Time**（最小 **FQDN** 更新時間）(またはデフォルト設定の 30 秒) 以上である限り、DNS の FQDN のtime-to-live (Time-To-Live - TTL)に基づいて FQDN を更新します。FQDN は、プロキシが構成されている場合、システム DNS サーバーまたは DNS プロキシオブジェクトによって解決されます。**Resolve (解決)** をクリックして、関連付けられた IP アドレスを確認します (ファイアウォールまたはパノラマの DNS 構成に基づきます)。アドレスオブジェクトの種類を FQDN から IP ネットマスクに変更するには、IP ネットマスクを選択して、**Use this address (**このアドレスを使用**)** をクリックします。**Type (**タイプ**)** が **IP Netmask (IP** ネットマスク**)** に変更され、選択した IP アドレスがテキスト フィールドに表示されます。

3. (Optional)アドレスオブジェクトに適用する 1 つ以上のタグを使用したオブジェクトのグループ化および視覚的な区別を入力します。
4. **OK** をクリックします。

STEP 2 | 変更をコミットします。

STEP 3 | アドレスオブジェクト、アドレスグループ、またはワイルドカードアドレスでフィルタリングされたログを表示します。

1. たとえば、トラフィックログを表示するには、**Monitor (**監視**)** > **Logs (**ログ**)** > **Traffic (**トラフィック**)** を選択します。
2. **+**を選択して、フィルタを追加します。
3. **Address (**アドレス**)** 属性、**in** 演算子を選択し、ログを表示するアドレスオブジェクト名を入力します。または、10.155.3.4/0.0.240.255 などのアドレスグループ名またはワイルドカードアドレスを入力します。
4. **Apply**（適用）をクリックします。

STEP 4 | アドレスオブジェクトに基づいてカスタムレポートを表示します。

1. **Monitor (**モニター**)** > **Manage Custom Reports (**カスタムレポートの管理**)** を選択して、トラフィックログなどのデータベースを利用するレポートを選択します。
2. **Filter Builder (**フィルタ ビルダー**)** を選択します。
3. **Address (**アドレス**)**、**Destination Address (**宛先アドレス**)** または **Source Address (**送信元アドレス**)** などの属性を選択し、演算子を選択して、レポートを表示するアドレスオブジェクトの名前を入力します。

STEP 5 | アドレスオブジェクトを使用する送信元 IP アドレスまたは宛先 IP アドレスに基づいてネットワークアクティビティを表示するには、ACC のフィルタを使用します。

1. **ACC** > **Network Activity (**ネットワークアクティビティ**)** を選択します。
2. **Source IP Activity—For Global Filters**（送信元 **IP** アクティビティの表示—グローバルフィルタ）の場合、 **+**をクリックしてフィルタを追加し、次のいずれかを選択します。**Address (**アドレス**)** またはSource (送信元)**Source Address (**送信元アドレス**)** または Destination (宛先)**Destination Address (**宛先アドレス**)**。それからアドレスオブジェクトを選択します。
3. **Destination IP Activity—For Global Filters**（宛先 **IP** アクティビティの表示—グローバルフィルタ）の場合、 **+**をクリックしてフィルタを追加し、以下のいずれかを選択します。**Address (**アドレス**)** またはSource (送信元)**Source Address (**送信元アドレス**)** または Destination (宛先)**Destination Address (**宛先アドレス**)**。それからアドレスオブジェクトを選択します。

タグを使用したオブジェクトのグループ化および視覚的な区別

オブジェクトにタグ付けして関連項目をグループ化し、タグに色を追加すれば、それらを視覚的に区別してスキャンを分かりやすくできます。タグを作成できるオブジェクトは、アドレス オブジェクト、アドレス グループ、ユーザー グループ、ゾーン、サービス グループ、ポリシー ルールです。

ファイアウォールおよび Panorama はスタティック タグとダイナミック タグの両方をサポートしています。ダイナミック タグはさまざまな送信元から登録され、スタティック タグとは別に表示されます。これは、ダイナミック タグがファイアウォールまたは Panorama 上の設定の一部ではないためです。タグを動的に登録する方法については、IP アドレスとタグの動的登録を参照してください。このセクションで説明するタグは、静的に追加され、設定に含まれます。

単体あるいは複数のタグをオブジェクトおよびポリシールールに追加できます（オブジェクトごとにタグは64個まで）。Panorama はPanorama 全体（共有およびデバイス グループ）と管理対象デバイス（複数の仮想システムを持つデバイスを含む）に分配できる最大 10,000 個のタグをサポートしています。

- タグの作成および適用
- タグの変更
- タグ グループ毎にルールを表示

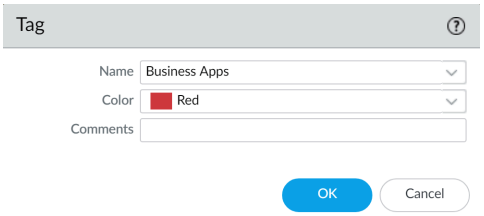
タグの作成および適用

ルールまたは構成オブジェクトの目的を識別し、ルールベースをより適切に整理するためにタグを使用します。ポリシー規則に適切にタグ付けされるようにするには、「ポリシールールの説明、タグ、監査コメントを適用方法」を参照してください。さらに、最初にタグを作成してから Group タグとして設定することで、タグ グループ毎にルールを表示できます。

STEP 1 | タグを作成します。

ゾーンにタグを付けるには、ゾーンと同じ名前のタグを作成する必要があります。ゾーンがポリシー ルールに関連付けられている場合は、タグの色がゾーン名の背景色として自動的に表示されます。

1. **Objects (オブジェクト)** > **Tags (タグ)** を選択して Add (追加) します。
2. Panorama またはマルチvirtual system (仮想システム - vsys)ファイアウォールで、**Device Group (デバイス グループ)**あるいは **virtual system (仮想システム - vsys)** を選択し、タグを利用できるようにします。
3. タグを**Add**（追加）し、タグを識別できる**Name**（名前）を入力するか、ゾーン**Name**（名前）を選択してゾーン用のタグを作成します。最大長は 127 文字です。
4. （任意）**Shared**（共有）を選択すると、共有場所にオブジェクトを作成して、Panorama の共有オブジェクトとしてアクセスしたり、マルチ仮想システム ファイアウォールのすべての仮想システムで使用可能にしたりすることができます。
5. （任意）事前定義済み 17 色から色を割り当てます。デフォルトでは**Color** [色]は**None** [なし]になっています。



6. **OK** および **Commit (コミット)** をクリックして変更を保存します。

STEP 2 | タグをポリシーに適用します。

1. **[Policies]** を選択し、その配下のルールベースを選択します。
2. ポリシー ルールを**Add**（追加）し、ステップ 1 で作成したタグ付きオブジェクトを使用します。
3. タグが使用されていることを確認します。

				Source				Destination	
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS
1	General Business Apps	Business Apps	universal	any	any	known-user	any	any	any

STEP 3 | アドレス オブジェクト、アドレス グループ、サービス、またはサービス グループにタグを適用します。

1. オブジェクトを作成します。

   例えば、サービスグループを作成するためには、**Objects (オブジェクト)** > **Service Groups (サービスグループ)** > **Add (追加)** を選択します。
2. タグ（**Tags**）選択するか、フィールドに名前を入力して新規タグを作成します。

   タグを編集したり、タグに色を追加したりするには、Modify Tags を参照してください。

タグの変更

Objects (オブジェクト) > **Tags (タグ)** の順に選択し、タグに対して以下のいずれかの操作を実行します。

- **Name**（名前）をクリックして、タグのプロパティを編集します。
- 表からタグを選択し、ファイアウォールからタグを**Delete**（削除）します。
- タグを**Clone**（複製）して、同じプロパティでコピーします。タグ名には数字のサフィックスが追加されます（例: FTP-1）。

タグの作成の詳細については、「タグの作成および適用」を参照してください。タグの操作については、「タグ グループ毎にルールを表示」を参照してください。

タグ グループ毎にルールを表示

ポリシールールベースをタググループとして表示し、作成したタグ付け構造に基づいてルールを視覚的にグループ化します。このビューでは、選択したタググループ内のルールの追加、削除、移動などの操作手順をより簡単に実行できます。ルールベースをタググループとして表示すると、ルールの評価順序が維持され、ルール階層を視覚的に維持するために 1 つのタグがルールベース全体に複数回表示される場合があります。

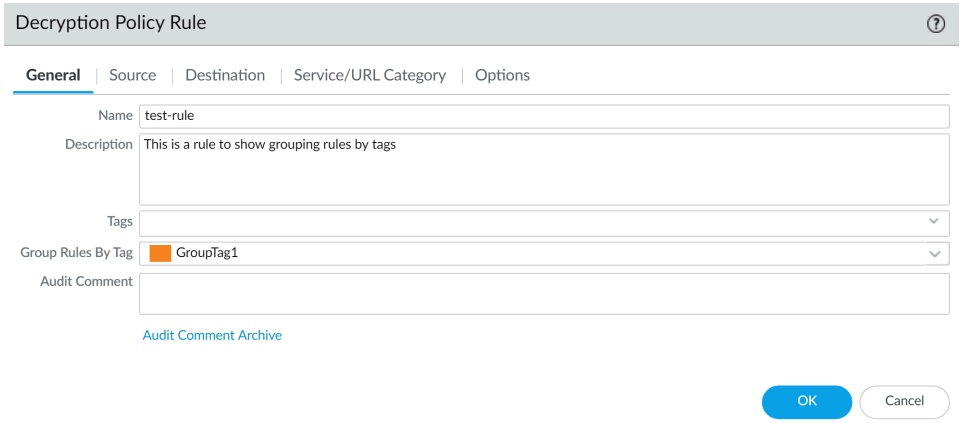
ルールのグループタグとして割り当てる前に、タグを作成する必要があります。PAN-OS 9.0 へのアップグレード時にすでにタグ付けされているポリシールールには、最初のタグが自動的にグループタグとして割り当てられます。PAN-OS 9.0 にアップグレードする前に、ルールベース内のタグ付きルールを確認して、ルールが正しくグループ化されていることを確認してください。PAN-OS 9.0 へのアップグレード後にルールが誤ってグループ化されている場合は、各タグルールを手動で編集して正しいグループタグを設定する必要があります。

STEP 1 | 「Web インターフェイスの起動」を行います。

STEP 2 | タグの作成および適用を行い、ルールのグループ化に使用します。

STEP 3 | タググループにポリシールールを割り当てます。

1. ポリシールールを作成します。ポリシールールの作成の詳細については、Policy（ポリシー）を参照してください。
2. **Group Rules by Tag (**タグによるグループルール**)** フィールドで、ドロップダウンからタグを選択して **OK** をクリックします。

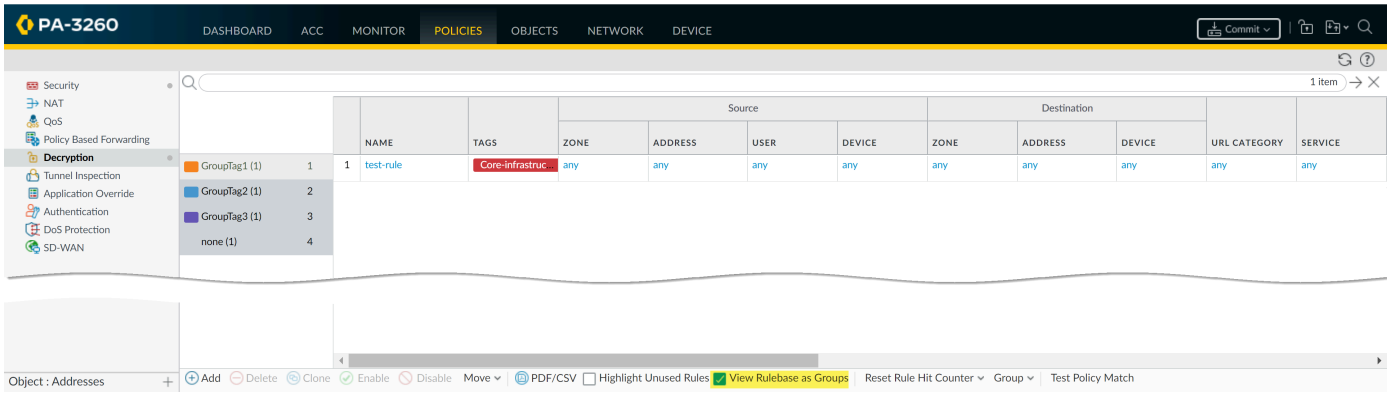


3. 変更を **Commit (**コミット**)** します。

STEP 4 | ポリシールールベースをグループとして表示します。

1. (Panorama のみ) **Device Group (**デバイスグループ**)** から、表示するデバイスグループルールベースを選択するか、すべての共有ルールを表示します。
2. **Policies (**ポリシー**)** をクリックして、手順 2 でルールを作成したルールベースを選択します。
3. 下部にある **View Rulebase as Groups (**ルールベースをグループとして表示**)** オプションを選択します。

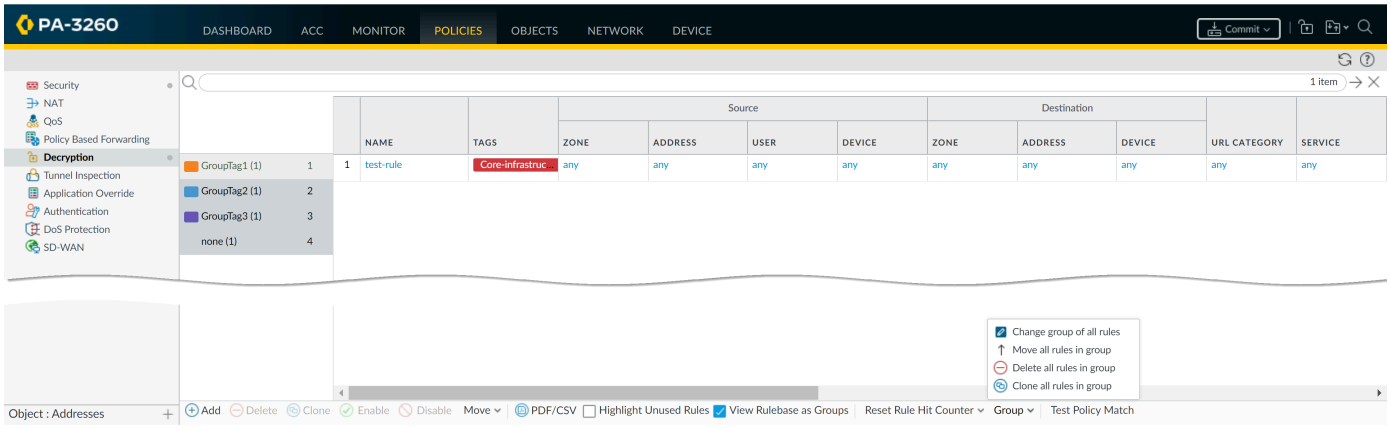
タググループを割り当てられていないルールは、***None (***なし**)*** と表示されます。



STEP 5 | 必要に応じてグループ操作を実行してください。

1. **Group (グループ)** をクリックして、選択したタググループ内のルールに対してグループ操作を実行します。

   - (Panorama のみ) **Move rules in group to a different rulebase or device group (グループ内のルールを別のルールベースまたはデバイスグループに移動する)**—選択したタググループ内のすべてのポリシールールを Pre-Rulebase または Post-Rulebase、あるいは別のデバイスグループに移動します。
   - **Change group of all rules (すべてのルールのグループを変更)**—選択したタグ グループ内のすべてのルールを別のタグ グループに移動させます。
   - **Move all rules in group (グループ内のすべてのルールを移動)**—ルールの優先順位を変更するために、選択したタググループ内のすべてのルールを移動します。
   - **Delete all rules in group (グループ内のすべてのルールを削除)**—選択したタググループ内のすべてのルールを削除します。
   - **Clone all rules in group (グループ内のすべてのルールをコピー)**—選択したタググループ内のすべてのルールをコピーします。



2. 変更を **Commit (コミット)** します。

ポリシーで外部動的リストを使用

外部動的リスト（公式名はダイナミック ブロック リスト）は、自分自身あるいは他のソースが外部の Web サーバーにホストするテキストファイルであり、これによってファイアウォールがオブジェクト（IP アドレス、URL、ドメイン）をインポートしてリストに挙がっているエントリーに対してポリシーを適用できるようになります。リストが更新される際、ファイアウォールが指定された間隔でリストを動的にインポートするため、ファイアウォール上で設定変更を行ったりコミットしたりすることなくポリシーを適用できます。

- 外部ダイナミック リスト
- 外部動的リストのフォーマットに関するガイドライン
- ビルトイン外部動的リスト
- ファイアウォールを設定して外部ダイナミックリストにアクセス
- EDL ホスティング サービスから外部動的リストにアクセスするようにファイアウォールを構成する
- Web　サーバーから外部動的リストを取得
- 外部動的リスト エントリの表示
- 外部動的リストからエントリを除外
- 外部ダイナミック リストでポリシーを適用
- 認証に失敗した外部動的リストを探す
- 外部動的リストの認証を無効化

外部ダイナミック リスト

外部ダイナミック リストは、外部のWebサーバーにホストするテキストファイルであり、これによってファイアウォールがリストに含まれるオブジェクト（IPアドレス、URL、ドメイン、International Mobile Equipment Identities (IMEIs)、International Mobile Subscriber Identities (IMSIs)）をインポートしてポリシーを適用できるようになります。外部ダイナミック リストに含まれるエントリーに対してセキュリティ ポリシーを適用するには、サポートされているポリシー ルールあるいはプロファイル内のリストを参照する必要があります。複数のリストが参照されている場合、評価順序を設定し、キャパシティの上限に達する前に EDL で最も重要な項目が確実にコミットされるようにします。リストを変更する際、ファイアウォールが指定された間隔でリストを動的にインポートするため、ファイアウォール上で設定変更を行ったりコミットしたりすることなくポリシーを適用できます。Webサーバが到達不能な場合、ファイアウォールは、Webサーバとの接続が回復するまで、最後に正常に受信したリストを使用してポリシーを適用します。EDL への認証が失敗した場合、セキュリティ ポリシーは EDL の適用を停止します。外部ダイナミック リストを取得するために、ファイアウォールは **Palo Alto Networks Services** サービスルートで設定されたインターフェイスを使用します。

ファイアウォールは、最後に正常に取得された EDL を保持し、次の場合に EDL をホストするサーバーとの接続が復元されるまで、最新の EDL 情報で動作を続けます。

- ファイアウォールをアップグレードまたはダウングレードする
- ファイアウォール、管理プレーン、またはデータ プレーンを再起動します。

- EDL をホストしているサーバーに到達不能になる

次の警告は、firewall がサーバーから最新の EDL 情報を接続できないか、フェッチできない場合に表示されます。

外部リストを取得できません。更新に古いコピーを使用する。

ファイアウォールは次のタイプの外部ダイナミック リストをサポートしています。

- 事前定義済みの **IP** アドレス—事前定義済みの IP アドレス リストは、不変あるいは「事前定義済み」のコンテンツを持つ、組み込み型の動的 IP リストを参照する IP アドレス リストの一種です。アクティブな脅威防御ライセンスをお持ちの場合、これらのBuilt-In External Dynamic Lists (組み込みの外部ダイナミック リスト) (堅牢なホスティング プロバイダー、悪意のある既知のファイル、高リスク IP アドレス向け) は自動的にファイアウォールに追加されます。また、事前定義済みの IP アドレス リストは、組み込み型のリストのいずれかをソースとして使用する EDL を参照することもできます。事前定義済みのリストの内容は変更できないため、リストの項目を追加・削除したい場合、事前定義済みのリストを別の EDLの送信元として使用できます。
- **Predefined URL List (**事前定義済みの **URL** リスト**)**—このタイプの外部ダイナミック リストには、ファイアウォールが認証ポリシーから安全に除外できる、更新やCertificate Revocation List (証明書失効リスト- CRL)チェックなどのバックグラウンド サービスにアプリケーションが使用する事前入力された URL が含まれています。Palo Alto Networks は、コンテンツ更新を通じて、このタイプの外部ダイナミック リスト (認証ポータル除外リストとも呼ばれる) を改訂および管理します。
- **IP** アドレス—ファイアウォールは通常、ファイアウォール上で静的オブジェクトとして定義された送信元あるいは宛先 IP アドレス用のポリシーを適用します（Enforce Policy on an External Dynamic List（外部ダイナミック リストにポリシーを適用）を参照）。その都度出現する送信元あるいは宛先IPアドレスのリスト用のポリシーを敏速に適用する必要がある場合、タイプがIPアドレスである外部ダイナミック リストをポリシールール内の送信元あるいは宛先アドレス オブジェクトとして使用し、ファイアウォールがリストに含まれているそのIPアドレス（IPv4およびIPv6アドレス、IP範囲およびIPサブネット）へのアクセスを拒否/許可するように設定できます。SD-WAN ポリシー ルールの送信元または宛先で IP アドレス EDL を使用することもできます。ファイアウォールはタイプがIPアドレスの外部ダイナミック リストをアドレス オブジェクトとして扱います。リストに含まれているすべてのIPアドレスは一つのアドレス オブジェクトとして使用されます。
- **Domain (**ドメイン**)**—このタイプの外部ダイナミック リストを使用すると、カスタム ドメイン名をファイアウォールにインポートして、アンチスパイウェア プロファイルまたは SD-WAN ポリシー ルールを使用してポリシーを適用できます。サードパーティ製の脅威インテリジェンス フィードを購入しており、さらに悪意のあるドメインが分かったらできるだけ早く脅威やマルウェアの新しい出元からネットワークを保護したい場合に、アンチスパイウェア プロファイルの EDL が役立ちます。外部ダイナミック リストに含めるドメインごとにファイアウォールがDNSベースのスパイウェア シグネチャを作成するため、DNS シンクホールが可能になります。DNS ベースのスパイウェア署名は、重大度が中程度のスパイウェアの種類で、各署名の名前は **`Custom Malicious DNS Query <domain name>`** です。また、ファイアウォールが特定のドメインのサブドメインを含めるように指定することもできます。例えば、ドメインリストに paloaltonetworks.com が含まれている場合、ドメイン名の下位レベルのコンポーネント (*.paloaltonetworks.com など) もすべてリストの一部として含まれます。こ

の設定が有効な場合、リストの各ドメインは追加のエントリを必要とするため、リストが使用するエントリの数は 2 倍になります。ドメイン リストの設定に関する詳細についてはカスタムドメインのリスト用に DNS シンクホールを設定を参照してください。

- **URL**—このタイプの外部ダイナミック リストにより、脅威やマルウェアの送信元からネットワークをアジャイルに保護することができます。ファイアウォールはURLを伴う外部ダイナミック リストをカスタムURLカテゴリとして扱い、これは次の2つの方法で使用できます。
  - セキュリティポリシー ルール、復号ポリシールール、およびQoS ポリシールールの一致条件として、カスタム カテゴリ内のURL用の帯域幅を許可、拒否、復号化、復号化しない、あるいは割り当てます。
  - プロファイルをセキュリティポリシー ルールに付与する前に、続行、アラート、オーバーライドといった細かなアクションを定義できる URL フィルタリング プロファイルで使用（URL フィルタリング プロファイルで外部ダイナミック リストを使用を参照）。
- **Equipment Identity (**設備 の識別情報**)**—5G または4G ネットワークに接続された機器のトラフィックを制御するセキュリティ ポリシー ルール内で、International Mobile Equipment Identities (IMEI) によって定義された IoT デバイスの外部ダイナミック リストを参照できます。サポートされているファイアウォール モデルで機器 ID セキュリティを設定する方法については、モバイル ネットワーク インフラストラクチャスタートガイドを参照してください。
- **Subscriber Identity (**サブスクライバ識別情報**)**—5G または4G ネットワークに接続されているサブスクライバのトラフィックを制御するセキュリティ ポリシー ルール内で、International Mobile Subscriber Identity (IMSI) の外部ダイナミック リストを参照できます。サポートされているファイアウォール モデルでサブスクライバ ID セキュリティを設定する方法については、モバイル ネットワーク インフラストラクチャスタートガイドを参照してください。

各ファイアウォールモデルで、ポリシーを強制するために ファイアウォールを設定して外部ダイナミックリストにアクセス を使用できる一意のソースを持つカスタム EDL を最大 30 個まで追加でき<す。この外部ダイナミック リストの制限は Panorama にはありません。複数仮想システムが有効にされたファイアウォールをPanoramaを使用して管理する際、そのファイアウォールの制限を超過すると、Panoramaにコミット エラーが表示されます。送信元とは、IPアドレスまたはホスト名、パス、そして外部ダイナミック リストのファイル名を含むURLを指します。ファイアウォールはURL（完全な文字列）を照合し、送信元が一意のものであるかどうかを判断します。

ファイアウォールは特定のタイプのリストの数を制限しませんが、一方で、以下の制限が課せられます。

- IP アドレス — PA-5200 Series、および PA-7000 Series のファイアウォールは合計で最大 150,000 個の IP アドレスをサポートしています。その他のモデルでは最大で合計 50,000 個の IP アドレスをサポートしています。リストあたりのIPアドレス数に制限はありません。ファイアウォールでIPアドレスがサポートされている最大数に達すると、そのファイアウォールがsyslogメッセージを生成します。事前定義済みの IP アドレス リスト内の IP アドレスは、この数には含まれません。

- URL およびドメイン—サポートされている URL およびドメインの最大数はモデルによって異なります。リストあたりの URL やドメインのエントリの数に制限はありません。次の表で、お使いのモデルの数字を確認できます：

model	URL リスト項目の制限	ドメイン リスト項目の制限
PA-5200 Series、PA-5400 Series、PA-7000 Series(PA-7000 20GXM NPC、PA-7000 20GQXM NPC、またはPA-7000 100G NPCでアップグレード)。 *NPC* が混在する *PA-7000* アプライアンスは、標準容量のみをサポートします。	250,000	4,000,000
VM-500, VM-700	100,000	2,000,000
PA-400 Series (PA-410を除く), PA-850, PA-820, PA-3200 Series, PA-3400 Series	100,000	1,000,000
PA-7000 Series (および PA-7000 20GQ NPC あるいは PA-7000 20G NPC でアップグレードしたアプライアンス)、VM-300	100,000	500,000
PA-220, PA-410, VM-50, VM-50 (Lite), VM-100, VM-1000-HV	50,000	50,000

リストのエントリがポリシー内で参照されている外部ダイナミック リストに属す場合、エントリの数はファイアウォールの制限に対してのみ考慮されます。

- リストをパースする際、ファイアウォールはリスト タイプにマッチしないエントリーをスキップし、そのモデルでサポートされている上限を超えたエントリーを無視します。エントリがこの上限数を超過することがないよう、現在ポリシーで使用しているエントリの数を確認します。***Objects (***オブジェクト***) > External Dynamic Lists (***外部ダイナミック リスト***)*** を選択して ***List Capacities (***キャパシティをリストアップ***)*** をクリックします。
- 外部ダイナミック リストはエントリを含む必要があります。リストの使用を停止する場合は、リストを空欄のままにする代わりに、ポリシー ルールまたはプロファイルから参照を削除します。リストにエントリが含まれていない場合、ファイアウォールはリストの更新に失敗し、最後に取得した情報を引き続き使用します。
- ベストプラクティスとして、複数の仮想システムを使用する場合は、共有 *EDL* を使用することを推奨します。各仮想システムのエントリが重複する個別の *EDL* を使用すると、より多くのメモリが使用され、ファイアウォールのリソースが過剰に使用される可能性があります。
- 複数仮想システムを実行するファイアウォールの *EDL* の項目数は、他の要素 *(DAG*、*virtual system (* 仮想システム - *vsys)*の数、ルールベースなど*)* も考慮してより正確なキャパシティ消費リストを生成します。これにより、*PAN-OS 8.x* リリースからアップグレードした後、キャパシティ消費が一致しないようになるかもしれません。
- メモリ割り当ての更新により、*EDL* キャパシティ制限を満たす前に、ファイアウォールで有効化している機能に応じてメモリ消費の制限を超過する可能性があります。ベストプラクティスとして、*Palo Alto Networks* は *EDL* キャパシティを確認し、必要な場合は *EDL* を削除するか共有リストに統合してメモリ使用量を最小化することを推奨しています。

外部動的リストのフォーマットに関するガイドライン

各タイプ（IPアドレス、URLあるいはドメイン）の外部動的リストには、そのタイプのエントリーのみを含める必要があります。事前定義済みの IP アドレス リストの各エントリは、IP アドレス リストのフォーマット ガイドラインに準拠しています。

- IPアドレス リスト
- ドメイン リスト
- URL リスト

IPアドレス リスト

外部動的リストには、個々の IP アドレス、サブネット アドレス（アドレス/マスク）、または IP アドレスの範囲を指定できます。また、コメントや特殊文字も指定できます。例：*****, **:**, **;**, **#**, or **/**.リスト内の各行の構文は次のとおりです。**[IP address, IP/Mask, or IP start range-IP end range] [space] [comment]**

1 行に 1 つの IP アドレス、IP 範囲、または IP サブネットを指定します。URL あるいはドメインは指定できません。「92.168.20.0/24」、「192.168.20.40-192.168.20.50」など、サブネットや IP アドレス範囲は 1 つの IP アドレス エントリとしてカウントされ、複数の IP アドレスとしてはカウントされません。コメントを追加する場合は、IP アドレス、IP 範囲、または IP サブネットと同じ行に指定する必要があります。IP アドレスの末尾のスペースは、IP アドレスとコメントを分ける区切り文字です。

IPアドレス リストの例：

```
192.168.20.10/32 2001:db8:123:1::1 #test IPv6アドレス
 192.168.20.0/24 ;テスト内部サブネット 2001:db8:123:1::/64 内部 IPv6 範囲
 192.168.20.40-192.168.20.50 をテストする
```

IP アドレスをブロックする場合は、プロトコルが *HTTP* の場合のみ、通知ページを表示できます。

ドメイン リスト

ドメイン リストでプレースホルダー文字を使用し、複数のウェブサイトのサブドメイン、トップレベル ドメイン全体を含む各ページ、特定の Web ページにマッチする単一のエントリを設定できます。

ドメイン リストのエントリを作成するときは、次のガイドラインに従ってください：

- 1 行に 1 つの ドメイン名を指定します。URL あるいはIPアドレスは指定できません。
- http://やhttps://のプロトコルをドメイン名の頭に付けないでください。
- アスタリスク (*) を使用してワイルドカードの値を示すことができます。
- キャレット (^) を使用して完全一致の値を示すことができます。
- 以下の文字はトークン区切り文字とみなされます： . / ? & = ; +

  これらの文字の 1 つまたは 2 つで区切られたすべての文字列はトークンです。ワイルドカード文字をトークン プレースホルダとして使用すると、特定のトークンに任意の値を含めることができます。
- ワイルドカード文字はトークン内の唯一の文字でなければなりません。ただし、エントリには複数のワイルドカードを含めることができます。
- 各ドメイン エントリの長さは最大255文字です。

アスタリスク（*）ワイルドカードを使用する場合：

1 つまたは複数の変数サブドメインを示すには、アスタリスク（*）ワイルドカードを使用します。たとえば、使用しているドメインの拡張子（場所によっては 1 つまたは 2 つのサブドメイン）にかかわらず、Palo Alto Network の Web サイトに強制を指定するには、次のエントリを追加します。 ***.paloaltonetworks.com**.このエントリは docs.paloaltonetworks.com と support.paloaltonetworks.com の両方に一致します。

また、このワイルドカードを使用してトップレベル ドメイン全体を示すこともできます。例えば、.work という名前の TLD に適用することを指定するには、エントリ ***.work** を追加します。これは .work で終わるあらゆるウェブサイトに一致します。

ワイルドカード (*) はドメイン項目の前でしか使用できません。

Asterisk (*) examples（アスタリスク （*）の例）

EDL ドメイン リストのエントリ	サイト一致
***.company.com**	eng.tools.company.com support.tools.company.com tools.company.com docs.company.com
***.click**	.click というトップレベル ドメインで終わるすべてのウェブサイト。

キャレット **(^)** を使用する場合：

キャレット (^) を使用してサブドメインの完全一致を示すことができます。たとえば、**^paloaltonetworks.com** は paloaltonetworks.com にのみ一致します。このエントリは他のサイトにはマッチしません。

Caret (^) examples（キャレット（^）の例）

EDL ドメイン リストのエントリ	サイト一致
^company.com	company.com
^eng.company.com	eng.company.com

URL リスト

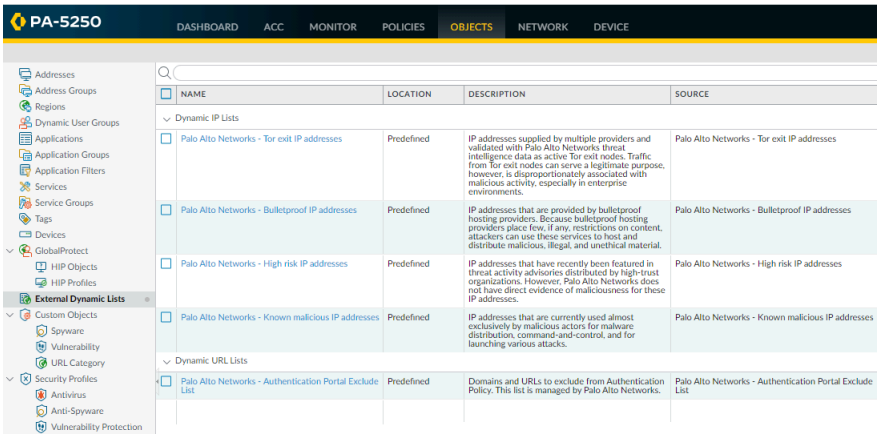
URL カテゴリの例外を参照してください。

ビルトイン外部動的リスト

Palo Alto Networks はアクティブな脅威防止ライセンスを持つユーザーに、組み込み型の悪意のあるホストを防止するために使用できる IP アドレス EDL を提供しています。

- **Palo Alto Networks** バレットプルーフ **IP** アドレス—バレットプルーフ ホスティング プロバイダーが提供する IP アドレスが含まれます。バレットプルーフ ホスティング プロバイダーはコンテンツにほとんど (あるいは全く) 制約を設けないため、攻撃者は頻繁にこれらのサービスを使用して悪意のある、違法な、非倫理的なものをホストして配信します。
- **Palo Alto Networks** 高リスク **IP** アドレス—信頼できるサードパーティの組織が発行した脅威アドバイザリーから得られる悪意のある IP アドレスを含みます。Palo Alto Networks は脅威アドバイザリーのリストに従いますが、それらの IP アドレスに悪意があるという証拠を直接持っているわけではありません。
- **Palo Alto Networks** 悪意のある既知の **IP** アドレス—WildFire 分析、Unit 42 リサーチ、テレメトリーから収集されたデータに基づいて悪意があることが検証された IP アドレスを含みます（脅威インテリジェンスを Palo Alto Networks と共有）。攻撃者はこれらの IP アドレスをほぼ独占的に使用してマルウェアを配布し、コマンド アンド コントロール アクティビティを開始し、攻撃を行います。
- **Palo Alto Networks Tor Exit IP** アドレス — 複数のプロバイダから提供され、Palo Alto Networks の脅威インテリジェンス データをアクティブな Tor 出口ノードとして検証した IP アドレスが含まれます。Tor 出口ノードからのトラフィックは正当な目的を果たすことができますが、特に企業環境では、悪意のあるアクティビティに不釣り合いに関連付けられます。

ファイアウォールはコンテンツ更新でこれらのフィードの更新コンテンツを取得します。これにより、Palo Alto Networks の最新の脅威インテリジェンスに基づいてファイアウォールが自動的にポリシーを適用できるようになります。ビルトイン リストのコンテンツを変更することはできません。(「外部動的リストのポリシーを適用する」を参照)、いずれかのリストをソースとして使用するカスタム外部ダイナミックリストを作成して (「ファイアウォールを設定して外部ダイナミックリストにアクセス」を参照)、必要に応じてリストからエントリを除外します。



ファイアウォールを設定して外部ダイナミックリストにアクセス

外部ダイナミック リスト上でポリシーを適用する前に、外部動的リストをホストするソースおよびファイアウォール間の接続を確立する必要があります。

STEP 1 | （任意）外部動的リストを取得するためにファイアウォールが使用するサービスルートをカスタマイズします。

Device (デバイス) > **Setup (セットアップ)** > **Services (サービス)** > **Service Route Configuration (サービスルート設定)** > **Customize (カスタマイズ)** を選択して **External Dynamic Lists (外部動的リスト)** のサービスルートを変更します。

ファイアウォール は、ビルトイン外部動的リストを取得するために *External Dynamic Lists* サービスルートを使用しません。コンテンツの更新は、これらのリストの内容を変更または更新します *(*有効な *Threat Prevention* ライセンスが必要です*)*。

STEP 2 | ファイアウォールで使用する外部動的リストを探します。

- 外部動的リストを作成し、WEB サーバー上でホストします。IP アドレス、ドメイン、あるいは URL を空のテキストファイルに入力します。各リスト項目は、1 行ずつ指定する必要があります。以下に例を示します。

  ```
  financialtimes.co.in

  www.wallaby.au/joey

  www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx
  ```

  外部動的リストのフォーマットに関するガイドラインを参照し、必ずファイアウォールがリスト項目をスキップしないようにしてください。コミット エラーやエントリーが無効になるのを避けるため、そのエントリーの頭にもhttp://あるいはhttps://を付けないでください。
- 別のソースにホストされている外部動的リストを使用し、それが外部動的リストのフォーマットに関するガイドラインに従っていることを確認します。

STEP 3 | **Objects (オブジェクト)** > **External Dynamic Lists (外部動的リスト)** を選択します。

STEP 4 | **[追加]** をクリックして、リストの分かりやすい **[名前]** を入力します。

STEP 5 | （任意）マルチ仮想システムとして有効化されているデバイス上のすべての仮想システムとリストを共有するには、**Shared (共有)** を選択します。デフォルトでは、**[仮想システム]** ドロップダウン リストで現在選択されている仮想システム上にオブジェクトが作成されます。

ベストプラクティスとして、複数の仮想システムを使用する場合は、共有 *EDL* を使用することを推奨します。各 *vsys* のエントリが重複する個別の *EDL* を使用すると、より多くのメモリが使用され、ファイアウォールのリソースが過剰に使用される可能性があります。

STEP 6 | （Panoramaのみ）**Disable override** [オーバーライドを無効化]を選択し、Panoramaからのデバイスグループのコミットによってこの設定を継承するファイアウォールの設定をファイアウォール管理者がローカルでオーバーライドすることがないようにします。

STEP 7 | リストの **Type (タイプ)** を選択します（例：**URL List (URL リスト)**）。

リストにはそのリスト タイプのエントリーのみを含めるようにしてください。外部動的リストのエントリーが無視されたかスキップされたかを検証を参照してください。

ドメインリストを使用している場合、オプションで **Automatically expand to include subdomains (自動展開してサブドメインを含める)** を有効にして、指定したドメインのサブドメインも含めることができます。例えば、ドメインリストに paloaltonetworks.com が含まれている場合、ドメイン名の下位レベルのコンポーネント (*.paloaltonetworks.com など) もすべてリストの一部として含まれます。この設定を有効にすると、特定のリスト内の各ドメインに追加のエントリが必要になり、消費されるエントリの数が事実上 2 倍になることに注意してください。

STEP 8 | Web サーバー上に作成したリストの **Source** （送信元） URLを入力します。送信元には、リストにアクセスできる完全パスを含める必要があります。例：https://1.2.3.4/EDL_IP_2015。

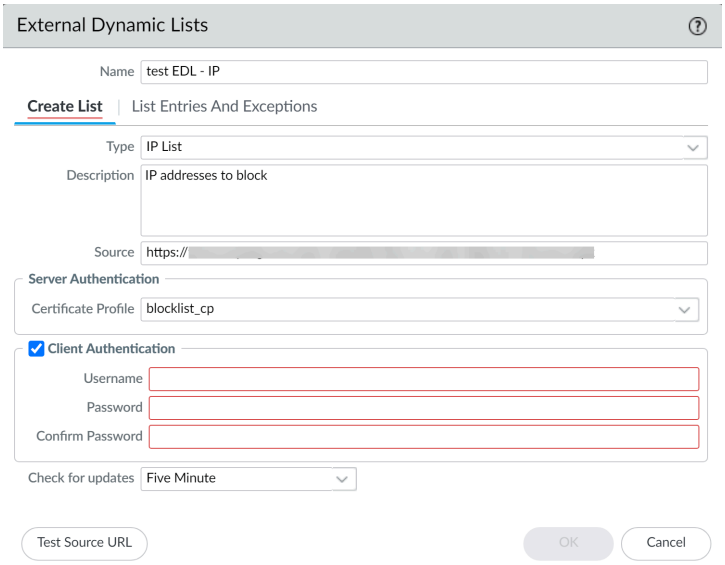
- Predefined IP (事前定義済み IP) 外部動的リストを作成している場合は、Palo Alto Networks の悪意のある IPアドレス フィードを選択し、送信元として使用します。
- Predefined URL (事前定義済み URL) 外部動的リストを作成している場合は、**panw-auth-portal-exclude-list** を送信元として選択します。

STEP 9 | リストのソースが SSL で保護されている場合（つまり、HTTPS の URL を持つリスト）、認証サーバーを有効化します。リストをホストしているサーバーの認証に使用する **Certificate Profile (証明書プロファイル)** を選択するか、**New Certificate Profile (新しい証明書プロファイル)** を作成します。認証中のサーバーにインストールされている証明書と一致する、ルート Certificate Authority (認証局 - CA)、および中間 CA 証明書を持つ、証明書プロファイルを選択する必要があります。

ポリシーを適用するために使用できる外部動的リストの数を最大化します。同じ証明書プロファイルを使用し、同じソース *URL* の外部動的リストを認証します。同じソース *URL* の外部動的リストに異なる証明書プロファイルを割り当てる場合、ファイアウォールは各リストを固有の外部動的リストとしてカウントします。

STEP 10 | リストのソースが HTTPS の URL であり、リストにアクセスするために HTTP 基本認証が必要な場合は、クライアント認証を有効化します。

1. **Client Authentication (**クライアント認証**)** を選択します。
2. リストにアクセスするための有効な **Username**（ユーザー名） を入力します。
3. **[**パスワード**]** と **[**パスワードの確認**]** を入力します。



STEP 11 | （Panorama または事前定義済み URL EDL では利用不可） **Test Source URL** 送信元 **URL** のテスト**)** をクリックして、ファイアウォールが Web サーバに接続できることを確認します。

Test Source URL (送信元 ***URL*** のテスト***)*** 機能は、*EDL* アクセスに認証が使用されている場合は利用できません。

STEP 12 | (任意) ファイアウォールがリストの **Check for updates (**更新確認**)** する頻度を指定します。デフォルト設定では、ファイアウォールは1時間ごとに1回リストを取得して更新をコミットします。

この間隔は前回のコミットの時間からの相対値です。そのため、間隔が*5*分の場合、前回のコミットが*1*時間前であれば*5*分後にコミットが行われることになります。リストを直ちに取得するには、Web　サーバーから外部動的リストを取得を参照してください。

STEP 13 | **OK** をクリックし、変更を **Commit (**コミット**)** します。

STEP 14 | (任意) EDL は評価順に上から下に表示されます。方向ボタン (ページ下部) を使ってリストの順序を変更することができます。そうすることで、キャパシティの上限に達する前に EDL で最も重要な項目を確実にコミットできるようにリストを並べることができます。

Group By Type (タイプでグループ化***)*** が選択解除されている場合のみ、*EDL* の順序を変更することができます。

STEP 15 | 外部ダイナミック リスト上でポリシーを適用します。

サーバーあるいはクライアント認証が失敗すると、最後に取得に成功した外部動的リストに基づき、ファイアウォールはポリシーを適用しなくなります。認証に失敗した外部動的リストを探し、認証に失敗した原因を確認します。

EDL ホスティング サービスから外部動的リストにアクセスするようにファイアウォールを構成する

EDL サービスとしてのソフトウェア (SaaS) アプリケーションの外部動的リスト (EDL) にアクセスするようにファイアウォールを構成する

- EDL ホスティング サービスを使用して外部動的リストを作成する
- グローバルサイン ルート R1 証明書を PEM 形式に変換する

EDL ホスティング サービスを使用して外部動的リストを作成する

サービスとしてのソフトウェア (SaaS) プロバイダーの中には、IP アドレスと URL の一覧を SaaS アプリケーションの宛先エンドポイントとして公開するものがあります。SaaS プロバイダーは、サポートが拡大し、サービスが拡大するにつれて、SaaS アプリケーションの宛先エンドポイントリストを頻繁に更新します。このため、SaaS アプリケーションのエンドポイントの変更を手動で監視し、ポリシー構成を手動で更新して、これらの重要な SaaS アプリケーションへの接続を確保するか、EDL を監視および更新するための外部ツールをセットアップする必要があります。

SaaS アプリケーションの EDL を維持する運用上の負担を軽減するために、Palo Alto Networks によって管理される EDL ホスティング サービス を使用して EDL を構成します。EDL ホスティング サービスは、SaaS アプリケーション プロバイダーによって公開された SaaS アプリケーション エンドポイントに対して、一般に公開されているフィード URL を提供します。フィード URL を EDL のソースとして利用することで、独自の EDL ソースをホストおよび維持する必要なく、SaaS アプリケーション トラフィックを動的に適用できます。

Palo Alto Networksは、SaaSプロバイダによって発行されたアプリケーションフィードURLを毎日チェックします。IP ベースのフィードの場合、Palo Alto Networks は、連続的なネットマスクからのエントリを結合する最適化を実行し、エンドポイントが複数の領域にわたってオーバーラップする場合は重複除去が実行されます。さらに、Microsoft 365 共通および Office オンライン SaaS アプリケーションのエンドポイントは、EDL ホスティング サービスのすべてのフィード URL に常に追加されます。

マイクロソフトでは、各暦月の終わりに Microsoft 365 フィード URL をすべて更新し、更新前に 30 日前に事前通知を提供します。詳細については、公式マイクロソフト 365 Web サービスページ を参照してください。EDL ホスティング サービスの可用性の状態と更新は Palo Alto Networks クラウド サービスの状態 ページに投稿されます。

STEP 1 | EDL ホスティング サービス にアクセスし、SaaS アプリケーションのフィード URL を確認します。

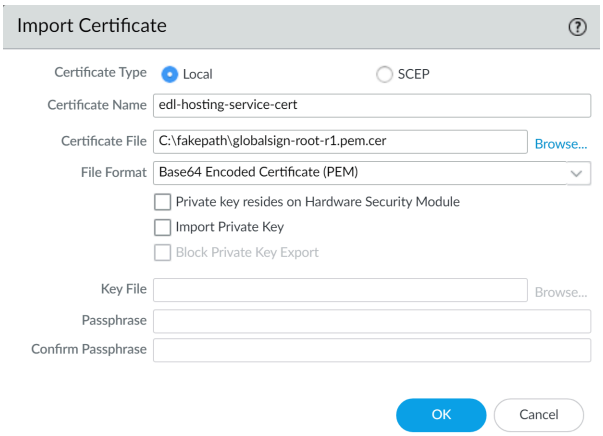
使用事例に最適なフィード URL の詳細については、Microsoft 365 のドキュメント を参照してください。さらに、フィード URL を識別する際に、SaaS アプリケーションと、SaaS アプリケーションにアクセスするユーザーの場所を検討してください。たとえば、Exchange

Online にアクセスする必要がある支店がドイツにある場合は、サービス エリアからフィード **URL** を選択します。ドイツ のオンライン交換。

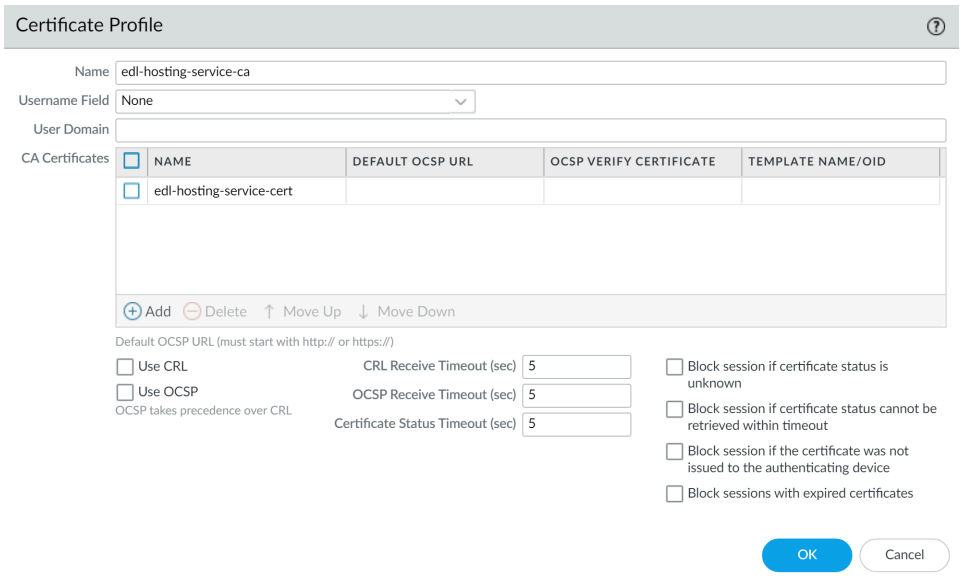
ポリシーベースの転送 ポリシールールの場合は、*IP* ベースのフィード *URL* を使用します。

STEP 2 | (ベスト プラクティス)EDL ホスティング サービスを認証するための証明書プロファイルを作成します。

1. グローバルサイン ルート R1 証明書 をダウンロードします。
2. 「グローバルサイン ルート R1 証明書を PEM 形式に変換する」を行います。
3. ファイアウォール Web インターフェースを起動します。
4. グローバルサイン ルート R1 証明書をインポートします。
   1. デバイス > 証明書管理 > 証明書 と **import** を選択します。
   2. 証明書タイプの場合は、[ローカルを選択します。
   3. 分かりやすい名前を **Certificate Name**（証明書名）に入力します。
   4. 証明書ファイルの場合は、**Browse**を選択し、前の手順で変換した証明書を選択します。
   5. ファイル形式 で、**Base64** エンコード証明書 **(PEM)** を選択します。
   6. **OK** をクリックします。



5. 認証局 (CA) 証明書プロファイルを作成します。
   1. デバイス > 証明書管理 > 証明書プロファイル と 追加 を選択します。
   2. 分かりやすい **Name**（名前）を入力します。
   3. **CA** 証明書の場合、追加 前の手順でインポートした証明書を指定します。
   4. **OK** をクリックします。



6. **[コミット]** します。

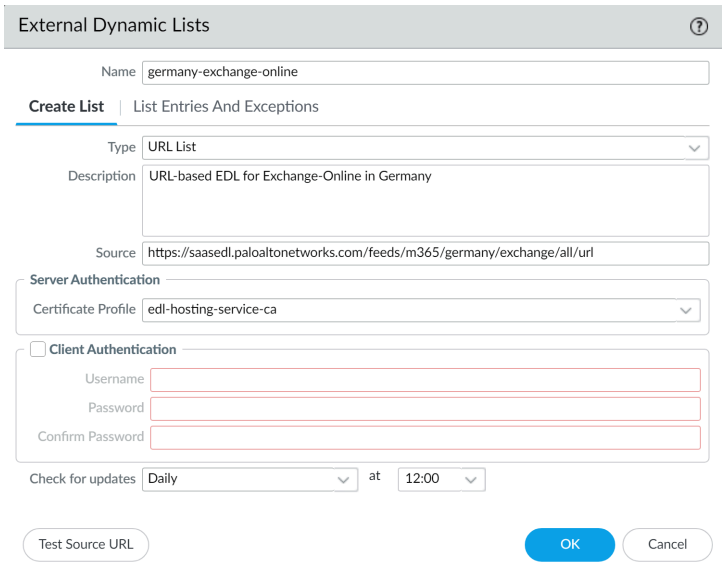
STEP 3 | EDL ホスティング サービスのフィード URL を使用して EDL を作成します。

1. オブジェクト > 外部動的リスト と 追加 を選択します。
2. EDL の説明的な 名前 を入力します。
3. EDL タイプ を選択します。
   - IP ベースの EDL の場合は、**IP** リスト を選択します。
   - URL ベースの EDL の場合は、[**URL** リスト を選択します。
4. (オプション) EDL の 説明を入力します。
5. フィード URL を EDL ソース として入力します。

   特定のフィード ***URL*** 内のすべてのエンドポイントを強制します。フィード ***URL*** から特定のエンドポイントを除外すると、***SaaS*** アプリケーションへの接続の問題が発生する可能性があります。
6. (ベスト プラクティス) 前の手順で作成した 証明書プロファイル を選択します。
7. フィード URL の更新頻度と一致するようにファイアウォールが 更新プログラムを確認する の頻度を指定します。

   たとえば、フィード URL が Palo Alto Networks によって毎日更新される場合、更新 日を確認するように EDL を構成します。

   Palo Alto Networks は、EDL ホスティング サービス の各フィード URL の更新頻度を表示します。フィード URL は、新しいエンドポイントで自動的に更新されます。
8. **Test** ソース **URL** をクリックして、ファイアウォールが EDL ホスティング サービスからフィード URL にアクセスできることを確認します。
9. **OK** をクリックします。



STEP 4 | 「外部ダイナミック リストでポリシーを適用」を行います。

EDL ホスティング サービスから EDL にポリシーを適用する場合、EDL がソースである場合、アプリケーションへの過剰プロビジョニングアクセスを回避するために、SaaS アプリケーションにアクセスできるユーザーを構成する際に特定の方法を指定します。

SaaS アプリケーション トラフィックの厳密な適用を追加するために、ポリシー ルールで *EDLs* と共に App-ID を活用します。

グローバルサイン ルート **R1** 証明書を **PEM** 形式に変換する

EDL ホスティング サービスを認証するための証明書プロファイルを作成するには、GlobalSign ルート R1 証明書を **PEM** 形式に変換する必要があります。EDL ホスティング サービスを認証するための証明書プロファイルの作成は、EDL ホスティング サービスから外部動的リストにアクセスするように .

GlobalSign ルート R1 証明書をダウンロードしたデバイスのオペレーティング システムに基づく適切な手順を参照してください。

STEP 1 | 証明書をまだダウンロードしていない場合は、GlobalSign ルート R1 証明書 をダウンロードします。

STEP 2 | 証明書を変換します。

- **Mac** および **Linux** オペレーティング システム

1. ターミナルを開き、ダウンロードした GlobalSign ルート R1 証明書を変換します。

```
admin: openssl x509 -in <certificate-path>.crt -inform DER -out
 <target-export-path>.pem -outform PEM
```

```
admin-1@admin-1:~$ openssl x509 -in /home/admin-1/Downloads/Root-R1.crt -inform
DER -out /home/admin-1/Downloads/globalsign-root-r1.pem -outform PEM
```

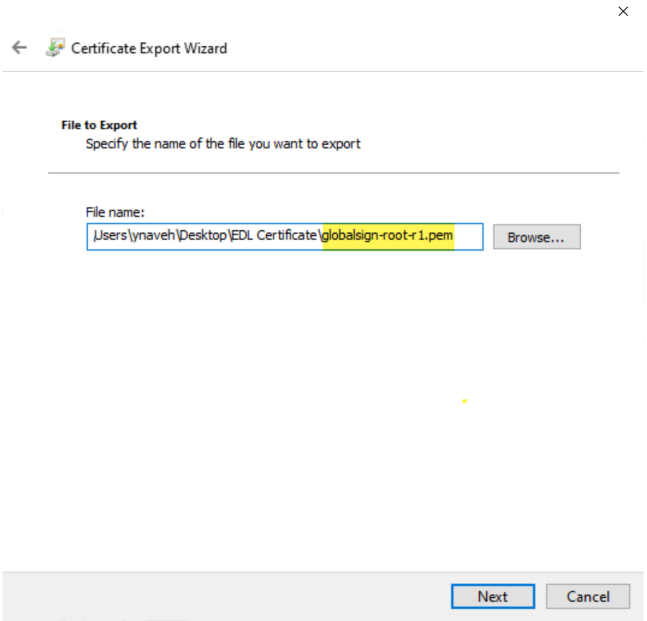
ターゲット のエクスポート パスが指定されていない場合、変換された証明書はデバイス デスクトップに作成されます。

- **Windows** オペレーティング システム

1. GlobalSign Root1 証明書をダウンロードした場所に移動します。
2. ダブルクリックして 開く 証明書。
3. 詳細 と コピーをファイル にします。

   続行するように求められたら、[次へ をクリックします。
4. **Base-64** エンコード **x.509 (.CER)** をクリックし、[次へ をクリックします。
5. **Browse** をクリックして、証明書をコピーする場所に移動し、ファイル名の末尾に **.pem** を含む証明書の名前を入力します。たとえば、グローバルサインルート**r1.pem**

   保存 証明書。表示される ファイル名 には、ターゲットのエクスポート パスと、.cer を追加して入力した証明書名が表示されます。追加された.cerを削除します。



6. 次へ をクリックし、完了 をクリックして証明書をエクスポートします。

Web サーバーから外部動的リストを取得

ファイアウォールを設定して外部動的リストにアクセスする際、ファイアウォールが WEB サーバーからリストを毎時（デフォルト）、5 分毎、毎日、毎週、あるいは毎月取得するよう設定できます。リストの IP アドレスを追加または削除したため、即座にリストの更新処理を起動する必要がある場合は、次の作業を行って更新されたリストを取得します。

STEP 1 | その都度リストを取得するには、**Objects (オブジェクト)** > **External Dynamic Lists (外部動的リスト)** を選択します。

STEP 2 | 更新するリストを選択し、**Import Now**[今すぐインポート] をクリックします。リストをインポートするジョブがキューに追加されます。

STEP 3 | タスク マネージャでジョブの状態を確認するには、管理タスクの管理・監視をご覧ください。

STEP 4 | （任意）ファイアウォールがリストを取得した後、外部動的リスト エントリを表示します。

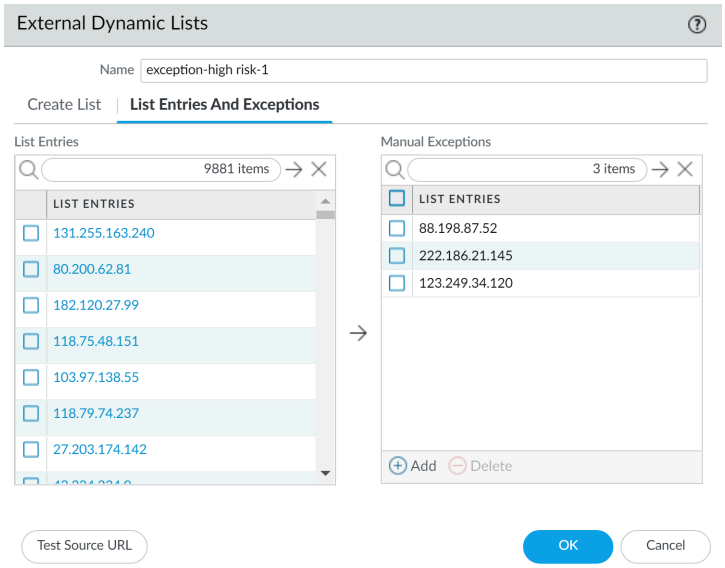
外部動的リスト エントリの表示

外部動的リストでポリシーを適用する前に、ファイアウォール上で直に外部動的リストのコンテンツを表示し、特定の IP アドレス、ドメイン、あるいは URL が含まれているかどうか確認できます。表示されるエントリは、ファイアウォールがごく最近受信した外部動的リストのバージョンに基づくものです。

STEP 1 | **Objects (オブジェクト)** > **External Dynamic Lists (外部動的リスト)** を選択します。

STEP 2 | 表示したい外部動的リストをクリックします。

STEP 3 | **List Entries and Exceptions (**リスト項目および例外**)** をクリックし、ファイアウォールがりストから取得したオブジェクトを表示します。



次の場合、リストが空になる場合があります。

- EDL は、セキュリティ ポリシー ルールにまだ適用されていません。EDL をセキュリティ ポリシー ルールに適用し、EDL を設定するには、外部ダイナミック リストでポリシーを適用を参照してください。
- ファイアウォールがまだ外部動的リストを取得していない。ファイアウォールにリストを直ちに取得させるために、Web　サーバーから外部動的リストを取得します。
- ファイアウォールが外部動的リストをホストしているサーバーにアクセスできない。**Test Source URL (**ソース **URL** のテスト**)** をクリックすれば、ファイアウォールがサーバーに接続できることを確認できます。

STEP 4 | フィルタ フィールドに（リストのタイプに応じて）IP アドレス、ドメイン、あるいは URL を入力し、Apply Filter (フィルタを適用)（→）して、リストにそれが含まれているかどうか確認します。どの IP アドレス、ドメイン、 URL をブロックあるいは許可するのかに基づき、外部動的リストからエントリを除外します。

STEP 5 | （任意）リスト エントリの AutoFocus インテリジェンス サマリーを表示します。項目にカーソルを合わせてドロップダウンリストを開き **AutoFocus** をクリックします。

外部動的リストからエントリを除外

外部動的リストの各エントリを表示している間、リストから最大 100 件のエントリを除外することができます。外部動的リストからエントリを除外することで、リストの一部（全部ではなく）のエントリに対してポリシーを適用できるようになります。これはサードパーティのソースから取得されているため、外部動的リスト（Palo Alto Networks High-Risk IP アドレス フィードなど）のコンテンツを編集できない場合に役立ちます。

STEP 1 | 外部動的リスト エントリを表示します。

STEP 2 | リストから除外する項目を最高 100 件まで選択して Submit (送信) （→）をクリックするか、リストの例外を手作業で **Add (追加)** します。

- 手動例外リストに重複エントリがある場合、外部ダイナミックリストへの変更を保存することはできません。赤い下線が付いたエントリを探すことで、重複したエントリを特定できます。
- マニュアル除外は、リストのエントリと完全に一致しなければなりません。また、IP アドレスの範囲内から特定の IP アドレスを除外することはできません。IP アドレス範囲から特定の IP アドレスを除外するには、範囲内の各 IP アドレスをリストエントリとして追加し、目的の IP アドレスを除外する必要があります。

  ファイアウォールは、IP アドレス範囲から個々の IP アドレスを除外することはできません。

STEP 3 | **OK** および **Commit (コミット)** をクリックして変更を保存します。

STEP 4 | （任意）外部ダイナミック リスト上でポリシーを適用します。

外部ダイナミック リストでポリシーを適用

外部ダイナミック リスト内の IP アドレスあるいは URL に基づいてトラフィックをブロックあるいは許可するか、DNS シンクホールと共に動的ドメイン リストを使って悪意のあるドメインにアクセスするのを防ぎます。

外部ダイナミック リストを使ってファイアウォール上でポリシーを適用するためのヒント：

- ファイアウォール上で外部ダイナミック リストを閲覧する際（***Objects (***オブジェクト***)*** > ***External Dynamic Lists (***外部ダイナミック リスト***)***）に ***List Capacities (***キャパシティをリストアップ***)*** をクリックすれば、現在ポリシーで使用している *IP* アドレス、ドメイン、*URL* の数と、ファイアウォールがサポートしている合計のエントリー数をリストタイプ毎に比較できます。
- グローバル検索を使用してファイアウォールあるいはPanoramaの管理サーバーを検索し、ポリシーで使用されている一つあるいは複数の外部ダイナミック リストに属すドメイン、*IP* アドレス、*URL* を探します。これは、ファイアウォールが特定のドメイン、*IP* アドレス、あるいは *URL* をブロックあるいは許可している原因がどの外部ダイナミック リスト（セキュリティポリシー ルールで参照されているもの）なのかを判断する際に役立ちます。
- ページ下部にある方向ボタンを使って *EDL* の評価順序を変更できます。そうすることでリストの順序を変更し、キャパシティの上限に達する前に *EDL* で最も重要な項目を確実にコミットできるようになります。

  Group By Type (タイプでグループ化***)*** が選択解除されている場合のみ、*EDL* の順序を変更することができます。

カスタムドメインのリスト用にDNS シンクホールを設定します。

URLフィルタリング プロファイルで外部動的リストを使用します。

セキュリティポリシールール内でタイプが**URL**の外部ダイナミック リストを一致条件として使用

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. **Add**[追加] をクリックし、分かりやすいルールの**Name**[名前] を入力します。
3. **Source** [送信元]タブで、**Source Zone** [送信元ゾーン]を選択します。
4. **Destination**[宛先] タブで宛先ゾーンを選択します。
5. **Service/URL Category** [サービス/URL カテゴリ]タブで**Add** [追加]をクリックし、URL Category [URLカテゴリ]リストから適切な外部ダイナミック リストを選択します。
6. **Actions** （アクション）タブで、**Action Setting** （アクション設定）を **Allow**（許可）または**Deny**（拒否）に設定します。
7. **OK**、**Commit (**コミット**)** の順にクリックします。
8. 外部ダイナミック リストのエントリーが無視されたかスキップされたかを検証します。

ファイアウォール上で次のCLIコマンドを実行し、リストの詳細情報を表示します。

```
request system external-list show type <domain | ip | url>
 name_of_list
```

以下に例を示します。

```
request system external-list show type url EBL_ISAC_Alert_List
```

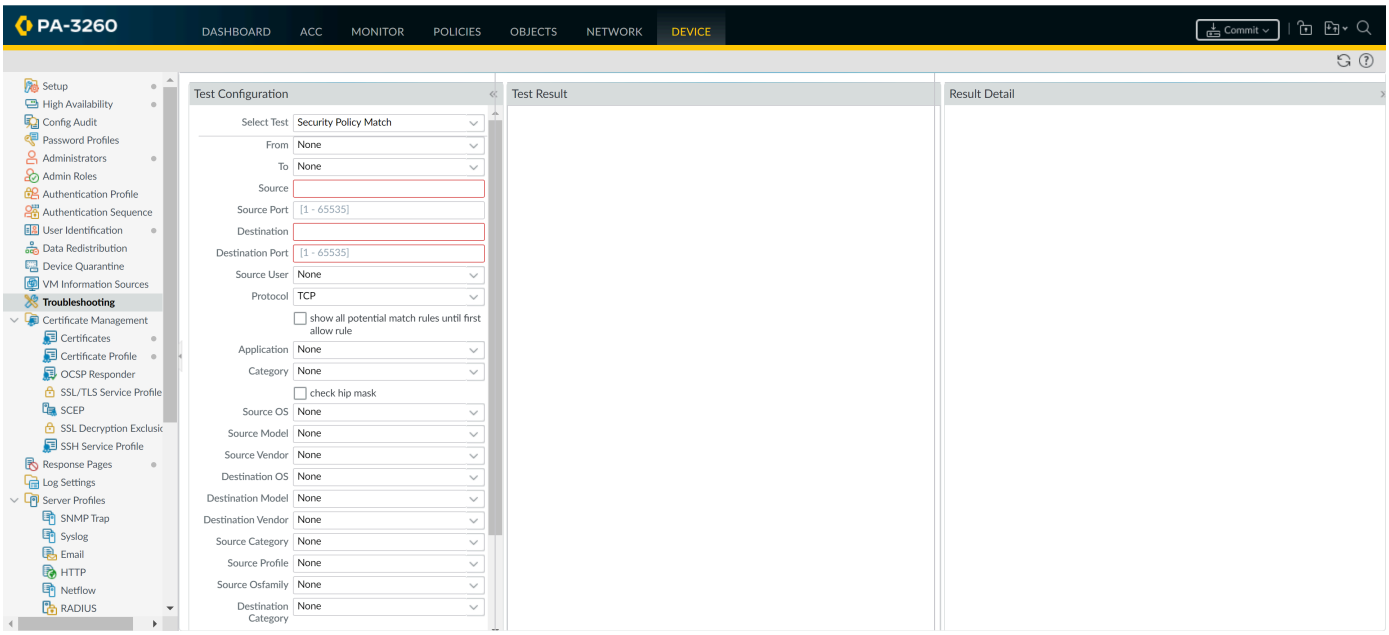
9. ポリシー アクションが適用されているかどうかテストします。
   1. URL リストについて外部ダイナミック リストのエントリを表示し、リストの URL にアクセスを試みます。
   2. 定義したアクションが適用されることを確認します。
   3. ファイアウォール上のアクティビティを監視するには：
      - **ACC**を選択し、URL Domain [URLドメイン]をグローバルフィルターとして追加し、アクセスしたURLのNetwork Activity [ネットワーク アクティビティ]およびBlocked Activity [ブロックされたアクティビティ]を確認します。
      - 詳細ログ ビューにアクセスするには、**Monitor (**監視**)** > **Logs (**ログ**)** > **URL Filtering (URL** フィルタリング**)** を選択します。

セキュリティ ポリシー ルール内で、**IP** 外部ダイナミック リスト、または 事前定義済みの **IP** 外部ダイナミック リストを、送信元、または宛先アドレス オブジェクトとして使用します。

新しいサーバーを導入し、ファイアウォールのコミットを行わずにそのサーバーへのアクセスを許可する場合にこの機能が役立ちます。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. **Add (追加)** をクリックして、ルールに分かりやすい **Name (名前)** を付けます。
3. **Source/Destination (送信元/宛先)**タブで、**Source/Destination Address (送信元/宛先アドレス)**として使用する外部ダイナミック リストを設定します。
4. Service/ URL Category (サービス/URL カテゴリ) タブで、**Service (サービス)** が **application-default** に設定されていることを確認します。
5. Actions （アクション）タブで、Action Setting （アクション設定）を **Allow**（許可）または **Deny**（拒否）に設定します。

   特定の *IP* アドレスについて、許可または拒否アクションを指定する必要がある場合は、別の外部ダイナミック リストを作成してください。
6. それ以外のオプションは、すべてデフォルト値にしておきます。
7. **OK**をクリックして変更を保存します。
8. 変更を **Commit**（コミット）します。
9. ポリシー アクションが適用されているかどうかテストします。
   1. 外部ダイナミック リストについて外部ダイナミック リストのエントリを表示し、リストの IP アドレス にアクセスを試みます。
   2. 定義したアクションが適用されることを確認します。
   3. **Monitor (監視)** > **Logs (ログ)** > **Traffic (トラフィック)** を選択し、そのセッションのログ項目を表示します。
   4. フローにマッチするポリシールールを検証するには、**Device (デバイス)** > **Troubleshooting (トラブルシューティング)**を選択し、セキュリティポリシー マッチ テストを実行します：



事前定義済み **URL** 外部ダイナミック リストを使用して、アプリケーションがバックグラウンド トラフィックに使用する安全なドメインを、認証ポリシーから除外します。

panw-auth-portal-exclude-list EDL タイプを選択すると、多くのアプリケーションが更新やその他信頼できるサービスなどのバックグラウンド トラフィックに使用するドメインを、認証ポリシーの適用から簡単に除外できます。これにより、ファイアウォールがこれらのサービスに必要なトラフィックをブロックせず、アプリケーションのメンテナンスが中断されないようになります。

1. **Policies** > **Authentication** (ポリシー認証) を選択します。
2. **Service/URL Category (サービス/URL カテゴリ)** タブで事前定義済みの URL EDL を **URL Category (URL カテゴリ)** として選択します。
3. **Actions (アクション)** タブで、**`default-no-captive-portal`** を **Authentication Enforcement (認証の実施)** として選択します。
4. **OK** をクリックします。
5. ルールを一番上に **Move (移動)** して、ポリシー内の第一ルールにします。
6. 変更を **Commit (コミット)**します。

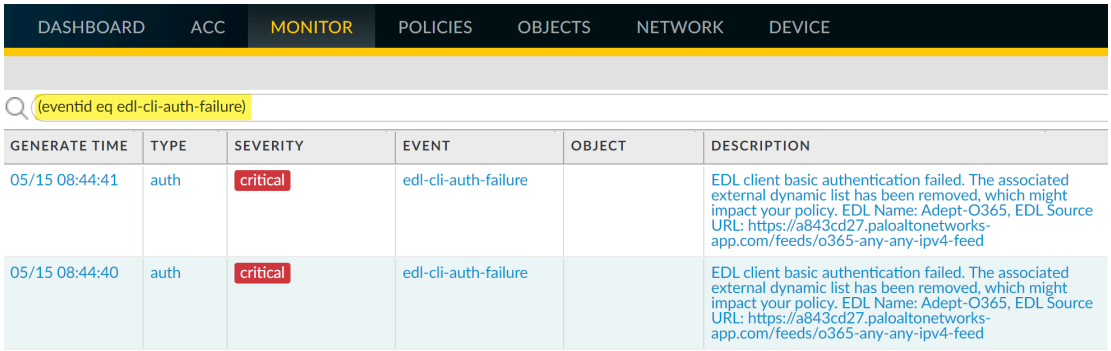
認証に失敗した外部動的リストを探す

SSL が必要な外部動的リストがクライアントあるいはサーバー認証に失敗すると、ファイアウォールは重大度が critical (重要) であるシステム ログを生成します。ファイアウォールは、認証に失敗した後も、最新バージョンを使用するのではなく、最後に成功した外部動的リストに基づいてポリシーを適用し続けるため、ログは重要です。次の各作業を行い、外部動的リストに関する認証の失敗を伝える重要なシステム ログを表示します。

STEP 1 | **Monitor (監視)** > **Logs (ログ)** > を選択します。

STEP 2 | 認証の失敗に関するメッセージをすべて表示する次のフィルタを作成し、フィルタを適用します。詳細については、ログのフィルターに記載されている全体の作業をご確認ください。

- サーバー認証失敗–**(eventid eq tls-edl-auth-failure)**
- クライアント認証失敗–**(eventid eq edl-cli-auth-failure)**



STEP 3 | システム ログのメッセージを確認します。メッセージの説明には、外部動的リストの名前、リストのソース URL、認証が失敗した理由が含まれています。

証明書の期限が切れていると、外部動的リストをホストしているサーバーが認証に失敗します。証明書無効リスト（CRL）あるいはオンライン証明書ステータス プロトコル（OCSP）を介して証明書の失効状態を確認するよう証明書プロファイルを設定している場合、次の状況でサーバーが認証に失敗する可能性もあります。

- 証明書が無効になっている。
- 証明書の失効状態が不明である。
- ファイアウォールが CRL/OCS サービスへの接続を試行している間に接続がタイムアウトした。

証明書プロファイル設定の詳細については、証明書プロファイルの設定を行う各ステップを参照してください。

外部動的リストが設定されている証明書プロファイルにサーバーのルート *CA* および中間 *CA* を追加したことを確認します。そうしないと、ファイアウォールがリストを正しく認証しません。

外部動的リスト用のユーザー名およびパスワードを誤った組み合わせで入力すると、クライアント認証が失敗します。

STEP 4 | （任意）リストをホストしているサーバーの証明書をリストのオーナーが更新するまでの間、応急処置として、認証に失敗した外部動的リストの認証を無効化します。

外部動的リストの認証を無効化

Palo Alto Networks は、ファイアウォール上で設定されている外部動的リストをホストするサーバーの認証を有効化することを推奨しています。ただし、認証に失敗した外部動的リストを発見し、そのリストのサーバー認証を無効化したい場合は、CLI を通して操作を行えます。次の作

業の流れは、SSL で保護されている外部動的リスト（つまり、HTTPS の URL を持つリスト）にしか当てはまりません。ファイアウォールは HTTP の URL を持つリストに対してはサーバー認証を適用しません。

また、外部動的リストのサーバー認証を無効化すると、クライアント認証も無効化されます。クライアント認証が無効な場合、アクセスにユーザー名およびパスワードが必要となる外部動的リストにファイアウォールが接続できなくなります。

STEP 1 | CLI を起動し、次のようにして設定モードに切り替えます。

```
username@hostname> configure Entering configuration mode [edit]
 username@hostname#
```

> が # の記号に変われば、設定モードになったことが分かります。

STEP 2 | そのリスト タイプに対して適切な CLI コマンドを入力します。

- IP アドレス

```
set external-list <external dynamic list name> type ip
 certificate-profile None
```

- ドメイン

```
set external-list <external dynamic list name> type domain
 certificate-profile None
```

- URL

```
set external-list <external dynamic list name> type url
 certificate-profile None
```

STEP 3 | 外部動的リスト用の認証が無効になっていることを確認します。

リストの更新を開始します（Web　サーバーから外部動的リストを取得を参照）。ファイアウォールがリストの取得に成功した場合、サーバー認証が無効になっています。

IP アドレスとタグの動的登録

スケール、および柔軟性とパフォーマンスの低下に関する問題を軽減するため、最近のネットワーク アーキテクチャでは、仮想マシン（VM）、およびアプリケーションをオンデマンドでプロビジョニング、変更、削除できます。ただし、こうした敏捷性と引き替えに、ダイナミックにプロビジョニングされた VM、およびこれらの仮想リソース上で有効化できる大量のアプリケーションの IP アドレスを完全に把握することが難しくなるため、セキュリティ管理者は難題を突きつけられています。

弊社のファイアウォール（ハードウェア ベースおよび VM-Series モデル）では、IPアドレス、IP セット (IP 範囲およびサブネット)、ならびにタグを動的に登録する機能をサポートしています。IP アドレスとタグは、ファイアウォールに直接登録するか、Panorama からファイアウォールに登録できます。また、ファイアウォール ログに含まれる送信元および宛先 IP アドレスのタグを自動的に取り除くこともできます。

PAN-OS は、*IPv4 IP* サブネットと、*Dynamic Address Group (*ダイナミック アドレス グループ*)* の範囲のみをサポートします。

このダイナミック登録プロセスは、以下のいずれかのオプションを使用して有効にできます。

- **User-ID agent for Windows** （Windows の User-ID エージェント） — User-ID エージェントがデプロイされている環境では、User-ID エージェントを使用して、VMware ESXi サーバー、vCenter Server、または 2 つの組み合わせを 100 台までモニターできます。これらの VMware サーバー上の仮想マシンをプロビジョニングまたは変更すると、エージェントが、IP アドレスの変更を取得し、その情報をファイアウォールと共有します。
- **VM Information Sources** （VM 情報ソース） — ファイアウォール上でVMware ESXi、vCenter サーバー、AWS-VPC、および Google Compute Engines（ネイティブではファイアウォール上）をネイティブにモニターして、ユーザーがこれらのソース上の仮想マシンをプロビジョニングまたは変更したとき、IP アドレスの変更を取得できます。VM 情報ソース オプションでは、事前定義済みの属性のセットをポーリングするため、XML API を介して IP アドレスを登録する外部スクリプトは必要ありません。仮想環境における変更のモニタリングを参照してください。
- **Panorama Plugin**—Panorama™ M-Series またはバーチャルアプライアンスを Azure または AWS パブリッククラウド環境に接続し、サブスクリプションまたは VPC 内に展開されているVirtual Machine (仮想マシン - VM)の情報を取得できるようにします。次に Panorama は、通知用に設定した管理対象の Palo Alto Networks ファイアウォールに VM 情報を登録し、ユーザーが属性を使用してDynamic Address Group (ダイナミック アドレス グループ)を定義し、それらをセキュリティポリシールールに付与して対象の VM を行き来するトラフィックを許可/除外できるようになります。
- **VMware Service Manager** (統合化 NSX ソリューションのみ) — 統合化 NSX ソリューションは、Palo Alto Networks Next-Generation Security Operating Platform® の自動プロビジョニングと配信の自動化、および Panorama によるダイナミックなコンテキスト ベースのセキュリティ ポリシーの適用を実現するよう設計されています。NSX Manager は、この統合化ソリューションでデプロイされたVirtual Machine (仮想マシン - VM) に関連付けられた、IPアドレス、IP セット、およびタグに関する最新情報で、Panorama を更新します。このソリュー

ションについての詳細は、「VM-Series NSX エディションのファイアウォールの設定」.を参照してください。

- **XML API** – ファイアウォールと Panorama では、標準の HTTP 要求を使用してデータの送受信を行う XML API をサポートしています。XML API を使用して、IP アドレスとタグをファイアウォールまたは Panorama に登録できます。API 呼び出しは、cURL などのコマンドラインユーティリティから直接実行できます。また、REST ベースのサービスをサポートする任意のスクリプトやアプリケーション フレームワークを使用することにより実行することもできます。詳細は、『PAN-OS XML API Usage Guide』（英語）を参照してください。
- 自動タグ– ログがファイアウォール上で生成される際に自動的に送信元あるいは宛先 IP アドレスにタグ付けし、HTTP サーバープロファイルを使用してファイアウォールあるいは Panorama 上の User-ID エージェント、あるいはリモート User-ID エージェントに IP アドレスとタグのマッピングを登録します。例えば、脅威ログを生成する際、常にファイアウォールが脅威ログ内のソース IP アドレスを特定のタグ名を使ってタグ付けするよう、設定することができます。詳細については、「自動タグ付けを使用してセキュリティアクションを自動化する」を参照してください。

  さらに、タイムアウトを使用して設定した時間後にタグを動的に登録解除するようにファイアウォールを設定できます。たとえば、タイムアウトを IP アドレスの DHCP リース タイムアウトと同じ期間に設定できます。これにより、IP アドレス-タグ間のマッピングが DHCP リースと同じ時に失効するようになり、IP アドレスが割り当て直される際にポリシーが誤って適用されなくなります。

  ログを HTTP(S) 宛先に転送を参照してください。

Dynamic Address Groups の作成と使用については、ポリシー内でのダイナミック アドレス グループの使用を参照してください。

タグを動的に登録するための CLI コマンドについては、ダイナミック IP アドレスおよびタグを確認する CLI コマンドを参照してください。

ポリシー内でのダイナミック ユーザー グループの使用

ダイナミック ユーザー グループは、ユーザーの可視性を維持しながら、異常なユーザーの動作や悪意のあるアクティビティの自動修復を提供するポリシーの作成に役立ちます。グループを作成して変更をコミットすると、ファイアウォールはユーザーと関連するタグを登録し、ダイナミック ユーザー グループのメンバーシップを自動的に更新します。ダイナミック ユーザー グループ メンバーシップの更新は自動的に行われるため、スタティック グループ オブジェクトの代わりにダイナミック ユーザー グループを使用すると、手動でポリシーを変更することなく、ユーザーの行動の変化や潜在的な脅威に対応できます。

メンバーとして含めるユーザーを決定するために、ダイナミック ユーザー グループはタグをフィルタリング基準として使用します。ユーザーがフィルター条件に一致するとすぐに、そのユーザーはダイナミック ユーザー グループのメンバーになります。タグベースのフィルタでは、論理演算子 *and* および *or* を使用します。各タグは、ソースにスタティックまたはダイナミックに登録するメタデータ要素または属性と値のペアです。スタティック タグはファイアウォール設定の一部ですが、ダイナミック タグはランタイム設定の一部です。その結果、ダイナミック タグがファイアウォールでコミットしたポリシーにすでに関連付けられている場合は、ダイナミック タグの更新をコミットする必要はありません。

タグを動的に登録するには、

- XML API
- User-ID エージェント
- Panorama
- ファイアウォールの Web インターフェース

を使用できます。

ファイアウォールは、ダイナミック ユーザー グループのタグをリッスンしている再配信エージェントに再配信します。これには、他のファイアウォール、Panorama、専用ログコレクター、および Cortex アプリケーションが含まれます。

動的ユーザー グループ タグの再配布をサポートするには、すべてのファイアウォールが *PAN-OS 9.1* を使用して登録ソースからタグを受信する必要があります。

ファイアウォールは動的ユーザー グループのタグをネクストホップに再配布し、ログ転送 を構成して、ログを特定のサーバーに送信することができます。ログ転送では、自動タグ設定を使用して、ログのイベントに基づいてダイナミック ユーザー グループのメンバーを自動的に追加または削除することもできます。

STEP 1 | **Objects**（オブジェクト） > **Dynamic User Groups**（ダイナミック ユーザー グループ）を選択し、新しいダイナミック ユーザー グループを**Add**（追加）します。

STEP 2 | ダイナミック ユーザー グループのメンバーシップを定義します。

1. グループの **Name**（名前） を入力します。
2. （任意）グループの**Description**（説明）入力します。
3. 動的基準を使用して**Add Match Criteria**（一致基準を追加）し、ダイナミック ユーザー グループのメンバーを定義します。
4. （任意）**And** または **Or** 演算子を、フィルタリングまたは照合に使用するタグで使用します。
5. **OK** をクリックします。
6. （任意）グループ自体に割り当てる**Tags**（タグ）を選択します。

   このタグは、***Dynamic User Group***（ダイナミック ユーザー グループ）リストの***Tags***（タグ）列に表示され、グループのメンバーではなく、ダイナミック グループ オブジェクトを定義します。
7. **OK** をクリックし、変更を **Commit (コミット)** します。

   ユーザー グループ オブジェクト フィルターを更新する場合は、変更をコミットして設定を更新する必要があります。

STEP 3 | 一致基準として使用するログ情報に応じて、ログ転送プロファイルを作成するか、ログ設定を行い、自動タグ付けを設定します。

- 認証、データ、脅威、トラフィック、トンネル検査、URL、および WildFire ログの場合、ログ転送プロファイルを作成します。
- ユーザ ID、グローバル保護、および IP タグ ログの場合は、 ログ設定 を設定します。

STEP 4 | （任意）一定時間後にダイナミック ユーザー グループ メンバーを元のグループに戻すには、**Timeout**（タイムアウト）値を分単位で入力します（デフォルトは 0、範囲は 0 ～ 43200 です）。

STEP 5 | ポリシー でダイナミック ユーザー グループを使用して、グループのメンバーのトラフィックを規制します。

少なくとも 2 つのルールを作成する必要があります。1 つはダイナミック トラフィック グループへの初期トラフィックの入力を許可するルール、もう 1 つは防止するアクティビティのトラフィックを拒否するルールです。ユーザーにタグを付けるには、トラフィックを許可するルールのルールベースで、トラフィックを拒否するルールよりも大きなルール番号が必要です。

1. ステップ 1 のダイナミック ユーザー グループを **Source User**（送信元ユーザー）として選択します。
2. **Action**（アクション）がダイナミック ユーザー グループ メンバーへのトラフィックを拒否するルールを作成します。
3. トラフィックがダイナミック ユーザー グループ メンバーに入力できるようにするルールを作成します。
4. ステップ 3 で**Log Forwarding**（ログ転送）プロファイルを設定した場合は、それを選択してポリシーに追加します。

5. 変更を **Commit (コミット)** します。

STEP 6 | （任意）グループのメンバーシップを絞り込み、ユーザーからタグへのマッピング更新の登録ソースを定義します。

最初のユーザーとタグのマッピングで、メンバーにすべきでないユーザーを取得する場合、またはメンバーにすべきでないユーザーを含める場合は、グループのメンバーを変更して、ポリシーを適用するユーザーを含め、マッピングの送信元を指定します。

1. **Users**（ユーザー）列で、**more**を選択します。
2. **Register Users**（ユーザーの登録）してユーザーをグループに追加し、タグとユーザーからタグへのマッピングに**Registration Source**（登録送信元）を選択します。
   - **Local**（ローカル）（デフォルト）—ダイナミック ユーザー グループ メンバーのタグとマッピングをファイアウォールのローカルに登録します。
   - **Panorama User-ID Agent**（**Panorama User-ID** エージェント）—Panoramaに接続されている User-ID エージェントで、ダイナミック ユーザー グループ メンバーのタグとマッピングを登録します。ダイナミック ユーザー グループが Panorama からのものである場合、行は黄色で表示され、グループ名、説明、一致基準、およびタグは読み取り専用です。ただし、ユーザーをグループに登録または登録解除することはできます。
   - **Remote device User-ID Agent**（リモートデバイス **User-ID** エージェント）—リモート User-ID エージェントで、ダイナミック ユーザー グループ メンバーのタグとマッピングを登録します。このオプションを選択するために、HTTP サーバー プロファイルを設定する必要があります。
3. グループの設定に使用したタグを使用して、送信元に登録する**Tags**（タグ）を選択します。
4. （任意）一定時間後にダイナミック ユーザー グループ メンバーを元のグループに戻すには、**Timeout**（タイムアウト）値を分単位で入力します（デフォルトは 0、範囲は 0 ～ 43200 です）。
5. 必要に応じて、ユーザーを**Add**（追加）または**Delete**（削除）します。
6. （任意）**Unregister Users**（ユーザーの登録解除）を行い、タグとユーザーからタグへのマッピングを削除します。

STEP 7 | ファイアウォールがダイナミック ユーザー グループのユーザーを正しく設定していることを確認します。

1. トラフィック、脅威、URL フィルタリング、WildFire 送信、データ フィルタリング、トンネル検査ログの**Dynamic User Group**（ダイナミック ユーザー グループ）列にダイナミック ユーザー グループが正しく表示されていることを確認します。
2. **show user group list dynamic**（ダイナミック ユーザー グループ リストを表示）コマンドを使用して、すべてのダイナミック ユーザー グループのリストとダイナミック ユーザー グループの総数を表示します。
3. **show object registered-user all**（オブジェクト登録ユーザーすべてを表示）コマンドを使用して、動的ユーザーグループの登録メンバーであるユーザーのリストを表示します。
4. **show user group name**（ユーザー グループ名を表示）***group-name***（グループ名）コマンドを使用して、送信元タイプなどのダイナミック ユーザー グループに関する情報を表示します。

自動タグ付けを使用してセキュリティアクションを自動化する

自動タグ付けにより、ファイアウォールまたは Panorama は、特定の基準に一致するログを受信したときにポリシー オブジェクトにタグを付け、IP アドレスからタグまたはユーザーからタグへのマッピングを確立できます。例えば、脅威ログを生成する際、常にファイアウォールが脅威ログ内のソース IP アドレスを特定のタグ名を使ってタグ付けするよう、設定することができます。次に、これらのタグを使用して、ダイナミック ユーザー グループやDynamic Address Group (ダイナミック アドレス グループ)などのポリシー オブジェクトを自動的に設定できます。これを使用して、セキュリティ、認証、または復号化ポリシーのセキュリティ アクションを自動化できます。たとえば、**Credential Detected**（検出された認証情報）列で**yes**（はい）の URL ログのフィルターを作成する場合、ユーザーに認証を要求する認証ポリシーを適用するタグをユーザーに適用できます 。多要素認証（MFA）を使用します。

動的ユーザーグループは、***HIP*** マッチログからの自動タグ付けをサポートしていません。

IP アドレスからタグへのマッピングとユーザーからタグへのマッピングを、ファイアウォールまたは Panorama 上の PAN-OS 統合User-IDエージェント、または HTTP サーバ プロファイルを使用したリモートUser-IDエージェント に登録することにより、ネットワーク全体にマッピングを再配信します 。ログ転送プロファイルの組み込みアクションの一部として、またはログ転送設定の一部としてタイムアウトを設定すると、ファイアウォールは IP アドレスまたはユーザーに関連付けられたタグを自動的に削除（登録解除）できます。たとえば、ユーザーが認証情報を危険にさらしている可能性があることをファイアウォールが検出した場合、そのユーザーに対して MFA 認証を一定期間要求するようにファイアウォールを設定し、タイムアウトを設定してユーザーを MFA 要件グループから削除できます。

STEP 1 | タグ付けに使用するログのタイプに応じて、ログ転送プロファイルを作成するか、ログ設定を行い、ファイアウォールまたは Panorama でログを処理する方法を定義します。

- 認証、データ、脅威、トラフィック、トンネル検査、URL、および WildFire ログの場合、ログ転送プロファイルを作成します。
- ユーザー ID、グローバル保護、および IP タグログのログ設定を構成します。

STEP 2 | ファイアウォールまたは Panorama がタグをポリシー オブジェクトに追加するタイミングを決定する一致リスト基準を定義します。

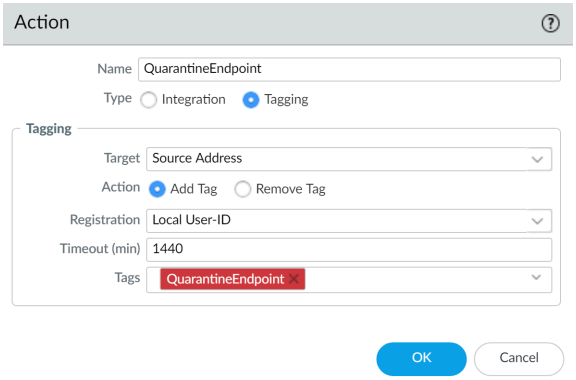
たとえば、フィルターを使用してしきい値を設定したり、値を定義したりできます（**user eq“ unknown”**などで、ファイアウォールがまだマッピングしていないユーザーを識別できます）。 ファイアウォールがそのしきい値に達するか、その値を見つけると、ファイアウォールはタグを追加します。

- ログ転送プロファイルを作成するには、**Add**（追加）して、一致リストの条件を監視する**Log Type**（ログタイプ）を選択します（**Objects**（オブジェクト） > **Log Forwarding**（ログ転送））。
- ログ設定を行うには、一致リストの条件（**Device**（デバイス） > **Log Settings**（ログ設定）)を監視するログタイプのログ設定を**Add**（追加）します 。

STEP 3 | **Filter**（フィルター）値をコピーして貼り付けるか、**Filter Builder**（フィルタービルダー）を使用してタグの一致基準を定義します。

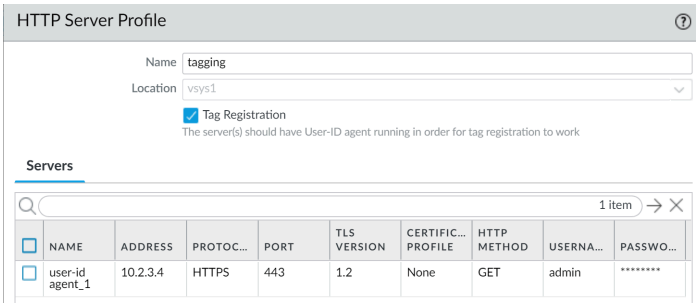
STEP 4 | 組み込みアクションを追加して、ポリシー オブジェクトにタグを付けます。

1. ログに一致リストの条件を満たすエントリが含まれている場合にファイアウォールまたは Panorama で実行する**Built-in Actions**（組み込みアクション）を**Add**（追加）します。
2. アクションの**Name**（名前）を付けます。
3. タグを付ける**Target**（ターゲット）のタイプ（**Destination Address**（宛先アドレス）、**Source Address**（送信元アドレス）、**User**（ユーザー）、または**X-Forwarded-For Address**）を選択します。
4. **Add Tag**（追加タグ）が**Action**（アクション）であることを確認します。
5. タグの**Registration**（登録）送信元を選択して、ファイアウォールまたは Panorama が IP アドレスとタグのマッピングを再配信する方法を決定します。
   - **Local User-ID**（ローカル **User-ID**）—ファイアウォールまたは Panorama の User-ID エージェントで、IP アドレスとタグのマッピングを再配信します。
   - **Panorama User-ID**—Panorama で IP アドレスとタグのマッピングを再配信します。
   - **Remote User-ID**（リモート **User-ID**）—HTTP サーバー プロファイルを使用して、IP アドレスとタグのマッピングを別のUser-ID エージェントに再配信します。このオプションを選択する場合は、HTTP サーバー プロファイルを設定する必要があります（ステップ 5 を参照）。
6. ポリシーオブジェクトに追加する**Tags**（タグ）を入力または選択します。
   フィールドの外側をクリックするか、Enter キーを押して **OK** ボタンを有効にする必要がある場合があります。
7. **OK** をクリックします。



STEP 5 | （リモート User-ID のみ）ログをリモート User-ID エージェントに転送するように HTTP サーバー プロファイルを設定します。

1. **Device**（デバイス） > **Server Profiles**（サーバープロファイル） > **HTTP** を選択します。
2. プロファイルを**Add**（追加）し、サーバープロファイルの**Name**（名前）を指定します。
3. （仮想システムのみ）**Location**（場所）を選択します。プロファイルは、すべての仮想システムで **Shared (**共有**)** することも、特定の仮想システムに所属させることもできます。
4. **Tag Registration (**タグ登録**)** を選択し、リモート ファイアウォール上の User-ID エージェントとのタグ マッピングおよび IP アドレスをファイアウォールが登録できるようにします。タグ登録が有効な場合、ペイロード フォーマットを指定することはできません。
5. リモート User-ID エージェントにアクセスするために、サーバー接続の詳細を**Add**（追加）し、**OK** をクリックします。



6. 作成したログ転送プロファイルを選択し、このサーバー プロファイルを**Remote User-ID**（リモート **User-ID**）タグ**Registration**（登録）の HTTP サーバー プロファイルとして選択します。

STEP 6 | タグを適用するポリシー オブジェクトを定義します。

1. 動的アドレスグループ、ポリシー内でのダイナミック ユーザー グループの使用、addresses、アドレスグループ、ゾーン、ポリシールール、サービス、またはサービスグループのいずれかのポリシーオブジェクトを作成または選択します。
2. オブジェクトに適用するタグを**Match**（一致）条件として入力します。

   タグがステップ 4 のタグと同一であることを確認します。

STEP 7 | タグ付けされたポリシー オブジェクトをポリシーに追加します。

このワークフローでは、例としてセキュリティ ポリシーを使用していますが、認証ポリシーでタグ付きポリシー オブジェクトを使用することもできます。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. **Add**（追加） をクリックし、ポリシーの **Name**（名前）および任意で**Description**（説明）を入力します。
3. トラフィックが発生する**Source Zone**（送信元ゾーン）を追加します。
4. トラフィックが発生する**Destination Zone**（宛先ゾーン）を追加します。
5. ステップ 5.1 で作成した **Source**（送信元）オブジェクトを選択します。
6. ルールがトラフィックを**Allow**（許可）するか**Deny**（拒否）するかを選択します。

STEP 8 | ログ転送プロファイルを設定した場合は、それをセキュリティ ポリシーに割り当てます。

ポリシーごとに 1 つのログ転送プロファイルを割り当てることができますが、プロファイルごとに複数の方法とアクションを割り当てることができます。例については、ポリシー内でのダイナミック アドレス グループの使用を参照してください。

STEP 9 | 変更を **Commit (コミット)** します。

STEP 10 | （任意）指定した時間が経過した後にポリシー オブジェクトからタグを削除するタイムアウトを設定します。

ファイアウォールがポリシー オブジェクトからタグを削除するまでの時間（分単位）を指定します。範囲は 0 ～ 43,200です。タイムアウトをゼロに設定すると、IP アドレスとタグのマッピングはタイムアウトせず、明示的なアクションで削除する必要があります。タイムアウトを最大 43,200 分に設定すると、ファイアウォールは 30 日後にタグを削除します。

Timeout を ***Remove Tag*** アクションで構成することはできません。

1. Log Forwarding（ログ転送）プロファイルを設定します。
2. **Add**（追加）するか、**Built-in Actions**（組み込みアクション）のいずれかを編集します。
3. **Timeout**（タイムアウト）（分単位）を指定します。指定した時間が経過すると、ファイアウォールまたは Panorama がタグを削除します。

   IP-タグのタイムアウトの値は、その IP アドレスのDHCP リースのタイムアウトの値と同じに設定する必要があります。これにより、IP 対タグのマッピングが DHCP リースと同じ時に失効するようになり、IP アドレスが割り当て直される際にポリシーが誤って適用されなくなります。
4. **OK** をクリックし、変更を **Commit (コミット)** します。

仮想環境における変更のモニタリング

新しいユーザーとサーバーが次々に現れる環境でアプリケーションのセキュリティを保護し脅威を防ぐには、セキュリティ ポリシーの敏捷性を高める必要あがります。敏捷性を高めるには、ファイアウォールが新規の IP アドレスまたは変更された IP アドレスを学習して、常に確実にポリシーを適用できなければなりません。しかも、こうした操作をファイアウォールの設定を変更することなく実行できる必要があります。

これは、ファイアウォールの **[VM** 情報ソース**]** 機能と **[**ダイナミック アドレス グループ**]** 機能を組み合わせることによって実現できます。弊社のファイアウォールと Panorama では、モニター対象の各ソース上の仮想マシン（またはゲスト）インベントリに関する情報の自動収集機能を用意しており、ネットワーク上の動的な変更と同期されたポリシー オブジェクトを作成します。

- VM をモニタリングして仮想ネットワーク上の変更を追跡する
- クラウド プラットフォームの仮想マシンで監視される属性
- ポリシー内でのダイナミック アドレス グループの使用

VM をモニタリングして仮想ネットワーク上の変更を追跡する

VM 情報ソースを使用すると、モニター対象の各ソース（ホスト）上の仮想マシン（VM）インベントリに関する情報を自動的に収集できます。これにより、ファイアウォールは、VMware ESXi、vCenter Server、および AWS-VPC をモニターできます。仮想マシン（ゲスト）がデプロイまたは移行されると、ファイアウォールはタグとして事前定義済みの属性（またはメタデータ要素）のセットを収集します。これらのタグを使用してダイナミック アドレス グループ（ポリシー内でのダイナミック アドレス グループの使用を参照）を定義し、ポリシー内の情報と照合できます。

ファイアウォールを直接構成したり、Panorama テンプレートを使って最大 10 VM の情報ソースを監視したりできます。**VM** 情報ソース は設定が容易で、事前定義済みの 16 のメタデータ要素または属性のセットをモニターできます。リストについては、クラウド プラットフォームの仮想マシンで監視される属性を参照してください。デフォルトでは、ファイアウォールとモニター対象ソース間のトラフィックに、ファイアウォール上の管理（MGT）ポートを使用します。

- VM-Series NSXエディション製品の一部となっているESXiホストをモニターしており、仮想環境内の変更点を調べる場合は、VM情報ソースの代わりにダイナミック アドレス グループを使用してください。VM-Series NSXエディション製品の場合、NSXマネージャーはIPアドレスの所属するNSXセキュリティグループの情報をPanoramaに提供します。NSXマネージャーはサービスプロファイルIDを使用して識別を行うので、NSXマネージャーからの情報にはダイナミック アドレス グループにおける一致条件を定義するために必要な情報がすべて含まれています。このため、複数のNSXセキュリティグループにまたがってIPアドレスが重複している場合にも適切なポリシーを適用することができます。1つのIPアドレスに対し、（vCenterサーバーおよびNSXマネージャーから）最大32個のタグを付与することができます。
- Azure のデプロイメント内の仮想マシンを監視するには、VM 監視ソースではなく、Azure パブリック クラウド内の仮想マシン上で実行されるVM 監視スクリプトをデプロイする必要があります。このスクリプトは Azure アセットの IP アドレスとタグのマッピング情報を収集し、ファイアウォールとそれに対応するスクリプトで指定した仮想システムに公開します。
- また、Panorama のバージョン 8.1.3 以降では、AWS あるいは Azure 用の Panorama プラグインを使用して VM 情報を取得し、それを管理対象のファイアウォールに登録することもできます。詳細については、クラウド プラットフォームの仮想マシンで監視される属性を参照してください。

STEP 1 | VM 監視を有効化します。

各ファイアウォール、またはマルチ仮想システム対応ファイアウォールの各仮想システムについて、最大10 VMの情報ソースをセットアップすることができます。

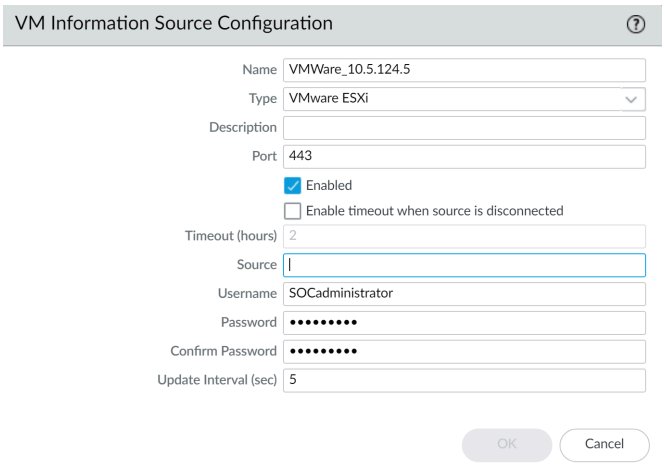
高可用性設定でファイアウォールが設定されている場合、以下が適用されます。

- アクティブ/パッシブ セットアップでは、アクティブなファイアウォールのみが VM 情報ソースをモニターします。
- アクティブ/アクティブ セットアップでは、優先度の値が「プライマリ」のファイアウォールのみが VM 情報ソースをモニターします。

1. **Device (デバイス)** > **VM Information Sources (VM 情報ソース)** を選択します。この例では、VMware ESX（i）または vCenter Server を追加する方法を示します。
2. **Add**（追加）をクリックして、以下の情報を入力します。
   - **Name**（名前）に、モニターする送信元を識別する名前を入力します。
   - ソースが **AWS VPC**、**Google Compute Engine** インスタンス、**VMware ESX(i)** サーバー、または **VMware vCenter** サーバーかどうかを示すには、**Type**（タイプ）を選択します。

     選択したタイプにより、表示されるフィールドが決まります。
   - 送信元がリッスンしている **Port (ポート)** を入力します。

- デフォルト値を変更するには、[送信元切断時のタイムアウトを有効にする] チェック ボックスをオンにして値を指定します。指定した時間に達した場合、またはホストがアクセス不能か応答しない場合、ファイアウォールによって送信元への接続が閉じられます。
- 上記のサーバーの認証を受けるため、認証情報（[ユーザー名] と [パスワード]）を追加します。
- **Source (送信元)** を定義する—ホスト名または IPアドレス。
- （任意）**Update interval**（更新間隔）を 5 ～ 600 秒の値に変更します。デフォルトでは、ファイアウォールは 5 秒ごとにポーリングします。API 呼び出しは毎回 60 秒以内にキューに登録され取得されるため、更新の最大所要時間は 60 秒に設定ポーリング間隔を加えた値となります。



- **OK** をクリックし、変更を**Commit**（コミット）します。
- 接続 **Status (ステータス)** が connected (接続済み) と表示されていることを確認します。

STEP 2 | 接続状態を確認します。

接続 **Status (ステータス)** が connected (接続済み) と表示されていることを確認します。

接続状態が保留または切断の場合は、送信元が動作しており、ファイアウォールが送信元にアクセスできることを確認します。モニター対象送信元ソースとの通信に MGT ポート以外のポートを使用する場合は、サービス ルートを変更する必要があります（**Device (デバイス)** > **Setup (セットアップ)** > **Services (サービス)** の順に選択し、**Service Route Configuration (サービスルート設定)** リンクをクリックして、**VM Monitor (VM 監視)** サービスの **Source Interface (ソース インターフェイス)** を変更します）。

クラウド プラットフォームの仮想マシンで監視される属性

プライベートあるいはパブリック クラウドで仮想マシンのプロビジョニングあるいは削除を行う際、Panorama プラグイン、VM 監視スクリプト、あるいは次世代ファイアウォール上の VM 情報ソースを使用し、仮想環境にデプロイされた仮想マシン（VM）の変更を監視できます。

VM 情報ソース—ハードウェアあるいは VM-Series ファイアウォール上で仮想マシンのインスタンスを監視し、監視対象のソース（AWS、ESXi あるいは vCenter サーバー、あるいは AWS）上で構成されたゲストをプロビジョニングあるいは変更する際に、変更を取得できます。firewall (および/または firewall に複数の仮想システム機能がある場合は仮想システム) ごとに、最大 10 個のソースを構成できます。VM 情報 ソース と Dynamic Address Group が同期して動作し、仮想環境内の変更を監視できるようにする方法については、VM-Series Deployment ガイド を参照してください。firewall が高可用性構成で構成されている場合:

- アクティブ/パッシブ 構成では、アクティブな firewall のみが VM 情報ソースを監視します。
- アクティブ/アクティブ・セットアップでは、プライマリー firewall のみが VM 情報ソースをモニターします。

Panorama プラグイン—Microsoft Azure および AWS 用のプラグインを Panorama（バージョン 8.1.3 を実行するハードウェア アプライアンスあるいはバーチャル アプライアンス）にインストールできます。プラグインを使用することで、Panorama を Azure パブリック クラウド サブスクリプションあるいは AWS VPC に接続し、仮想マシンの IP アドレス対タグのマッピングを取得できます。次に Panorama は、通知用に設定した管理対象の Palo Alto Networks® ファイアウォールに VM 情報を登録します。

各クラウドベンダーでサポートされているオプション、およびダイナミック アドレス グループを作成するために監視できる仮想マシンの属性を、次のセクションでご紹介します。

- VMware ESXi
- Amazon Web Services (AWS)
- Microsoft Azure
- Google

VMware ESXi

モニター対象の ESXi または vCenter Server の各 VM に VMware Tools がインストールされていて実行中である必要があります。VMware Tools を使用して、各 VM に割り当てられた IP アドレスとその他の値を収集できます。

*VM-Series NSX*エディション製品の一部となっている*ESXi*ホストをモニターしており、仮想環境内の変更点を調べる場合は、*VM*情報ソースの代わりにダイナミック アドレス グループを使用してください。*VM-Series NSX*エディション製品の場合、*NSX*マネージャーは*IP*アドレスの所属する*NSX*セキュリティグループの情報を*Panorama*に提供します。*NSX*マネージャーはサービスプロファイル*ID*を使用して識別を行うので、*NSX*マネージャーからの情報にはダイナミック アドレス グループにおける一致条件を定義するために必要な情報がすべて含まれています。このため、複数の*NSX*セキュリティグループにまたがって*IP*アドレスが重複している場合にも適切なポリシーを適用することができます。

1 つの *IP* アドレスに対し、（*vCenter* サーバーおよび *NSX* マネージャーから）最大 *32* 個のタグを付与することができます。

モニター対象の VM に割り当てられた値を収集するには、ファイアウォール上の VM 情報ソースを使用して以下の事前定義済み ESXi 属性のセットを監視します：

VMware ソースでモニターされる属性
UUID
氏名
Guest OS
VM State — 電源状態は「poweredOff」、「poweredOn」、「standBy」、「unknown」のいずれかです。
Annotation
Version（バージョン）
Network — Virtual Switch Name、Port Group Name, and VLAN ID
Container Name —vCenter Name、Data Center Object Name、Resource Pool Name、Cluster Name、Host、Host IP address

Amazon Web Services (AWS)

AWS VPC 内で仮想マシンのプロビジョニングあるいは変更を行う際、これらのインスタンスを監視し、ダイナミック アドレス グループで一致条件として使用するタグを取得する方法が 2 つあります。

- **VM** 情報ソース–次世代ファイアウォール上で最大で合計 32 件のタグ（事前定義済みのものが 14、ユーザー定義のキーおよび値のペア（タグ）が 18）を監視できます。以下の属性（またはタグ名）は、ダイナミック アドレス グループの一致条件として使用できます。
- **AWS Plugin on Panorama**–AWS 用の Panorama プラグインを使用することで、Panorama を AWS VPC に接続し、AWS Virtual Machine (仮想マシン - VM) の IP アドレスtoタグのマッピングを取得できます。次に Panorama は、通知用に設定した管理対象の Palo Alto Networks®

ファイアウォールに VM 情報を登録します。プラグインを使用すれば、各仮想マシンにつき合計 32 件のタグ（事前定義済みのタグが 11、ユーザー定義のタグが最大 21）を取得できます。

AWS-VPC でモニターされる属性	ファイアウォール上の VM 情報ソース	AWS Plugin on Panorama
Architecture	あり。	無し
Guest OS	あり。	無し
AMI ID	あり。	あり。
IAM Instance Profile	無し	あり。
インスタンスID	あり。	無し
Instance State	あり。	無し
Instance Type	あり。	無し
Key Name	あり。	あり。
Owner ID	無し	あり。
Placement—Tenancy	あり。	あり。
Placement—Group Name	あり。	あり。
Placement—Availability Zone	あり。	あり。
Private DNS Name	あり。	無し
Public DNS Name	あり。	あり。
Subnet ID	あり。	あり。
セキュリティグループ ID	無し	あり。
セキュリティグループ名	無し	あり。
VPC ID	あり。	あり。
タグ（キー、値）	あり。	あり。

AWS-VPC でモニターされる属性	ファイアウォール上の VM 情報ソース	AWS Plugin on Panorama
	最大 18個 のユーザー定義のタグがサポートされています。ユーザー定義のタグはアルファベット順に並べられ、最初の 18個 のタグがファイアウォールで使用できます。	最大 21個 のユーザー定義のタグがサポートされています。ユーザー定義のタグはアルファベット順に並べられ、最初の 21個のタグが Panorama およびファイアウォールで使用できます。

Microsoft Azure

Azure での VM 監視については、Azure VM の IP アドレスtoタグのマッピングを取得し、ダイナミック アドレス グループの一致条件として使用できるようにする必要があります。Microsoft Azure 用のPanorama プラグインを使用することで、Panorama を Azure パブリック クラウド サブスクリプションに接続し、Azure Virtual Machine (仮想マシン - VM) の IP アドレスtoタグのマッピングを取得できます。Panorama は、Virtual Machine (仮想マシン - VM) ごとに合計26個のタグ、11個の事前定義済みタグ、最大15個のユーザー定義タグを取得し、通知用に構成した管理対象の Palo Alto Networks® ファイアウォールに VM 情報を登録できます。

Azure 用の Panorama プラグインを使用すると、Microsoft Azure デプロイメント内の次のVirtual Machine (仮想マシン - VM) 属性のセットを監視できます。

Microsoft Azure 上で監視される属性	Azure Plugin on Panorama
VM 名	あり。
VM サイズ	無し
Network Security Group Name（ネットワーク セキュリティ グループ名）	あり。
OS タイプ	あり。
OS パブリッシャー	あり。
OS オファー	あり。
OS SKU	あり。
サブネット	あり。
VNet	あり。
Azure リージョン	あり。
リソース グループ名	あり。

Microsoft Azure 上で監視される属性	Azure Plugin on Panorama
サブスクリプション ID	あり。
ユーザー定義のタグ	はい 最大 15 個のユーザー定義タグがサポートされます。ユーザー定義のタグはアルファベット順に並べられ、最初の 15 個のタグは Panorama と firewall で使用できる。

Google

次世代ファイアウォール上の VM 情報ソースを使用することで、以下の定義済みの Google Compute Engine (GCE) 属性セットを監視できます。

ファイアウォールでは高可用性がサポートされていません。

Google Compute Engine (GCE) 上で監視する属性
VM のホスト名
マシン タイプ
プロジェクト ID
プラットフォーム（OS タイプ）
ステータス
サブネットワーク
VPC ネットワーク

ポリシー内でのダイナミック アドレス グループの使用

ダイナミック アドレス グループは、ポリシー内で使用します。ダイナミック アドレス グループを使用すると、サーバーの追加、移動、削除といった変更に自動的に適応するポリシーを作成できます。また、ネットワーク、オペレーティング システム、またはオペレーティング システムが処理するさまざまな種類のトラフィックのロールを定義するタグに基づいて異なるルールを同じサーバーに適用する柔軟性も実現できます。

ダイナミック アドレス グループは、グループのメンバーを決定するためのフィルタリング基準としてタグを使用します。フィルタでは、論理演算子 *and* および *or* を使用します。フィルタリング基準に一致するすべての IP アドレスまたはアドレス グループがダイナミック アドレス グ

ループのメンバーになります。タグはファイアウォール上に静的に定義することも、ファイアウォールに動的に登録することもできます。スタティック タグとダイナミック タグの違いは、スタティック タグがデバイス設定の一部であるのに対して、ダイナミック タグはランタイム設定の一部である点です。したがって、ダイナミック タグを更新するためにコミットは必要ありません。ただし、ダイナミック アドレス グループによって使用されるタグはポリシーによって参照されるため、ポリシーをファイアウォールにコミットする必要があります。

タグを動的に登録するには、ファイアウォール上または ユーザー ID エージェント上で XML API または VM モニタリングを使用します。各タグは、ファイアウォールまたは Panorama に登録されるメタデータ要素または属性値のペアです。たとえば、IP1 {tag1, tag2,.....tag32} では、IP アドレスと関連タグがリストとして保持されています。登録済みの各 IP アドレスには、オペレーティング システム、データセンター、またはその所属先仮想スイッチなど最大 32 個のタグを付けることができます。ファイアウォールは、API 呼び出しを受けると、IP アドレスと関連タグを登録し、ダイナミック アドレス グループのメンバー情報を自動的に更新します。

登録可能な IP アドレスの最大個数はモデルによって異なります。以下の表で、お使いのモデルの数字を確認してください。

model	動的に登録可能な IP アドレスの最大個数
M Series および Panorama バーチャル アプライアンス	500,000
PA-5400 シリーズ (PA-5450 を除く), PA-5200 シリーズ, PA-7000 SMC-B シリーズ	500,000
VM-500, VM-700	300,000
PA-3430、PA-3440、PA-3200シリーズ、VM-300	200,000
PA-3410、PA-3420	150,000
PA-7000シリーズ、PA-5450、PA-450、PA-460	100,000
PA-440	50,000
PA-850, VM-100	2,500
PA-820、PA-410、PA-220、VM-50	1,000

*IP*レンジやサブネットなどの*IP*設定は、各ファイアウォールモデルでサポートされている登録*IP*アドレスの最大数にカウントする際、*1*つの登録*IP*アドレスとみなされます。

以下の例に、ダイナミック アドレス グループによってネットワーク セキュリティの実施を簡素化する方法を示します。この例のワークフローは、以下の操作を実行する方法を示しています。

- ファイアウォール上で VM モニタリング エージェントを有効にして、VMware ESX(i) ホストまたは vCenter Server をモニターし、VM IP アドレスと関連タグを登録します。
- ダイナミック アドレス グループを作成し、フィルタリング用のタグを定義します。この例では、2 つのアドレス グループを作成します。1 つはダイナミック タグのみを使用してグループのメンバーを決定するアドレス グループ、もう 1 つは、スタティック タグとダイナミック タグの両方を使用してグループのメンバーを決定するアドレス グループです。
- ファイアウォール上で、ダイナミック アドレス グループのメンバーが決定されていることを確認します。
- ポリシー内でダイナミック アドレス グループを使用します。この例では、以下の 2 つの異なるセキュリティ ポリシーを使用します。
  - FTP サーバーとしてデプロイされたすべての Linux サーバーのセキュリティ ポリシー。このルールは、動的に登録されたタグに基づいてマッチングを行います。
  - Web サーバーとしてデプロイされたすべての Linux サーバーのセキュリティ ポリシー。このルールは、スタティック タグとダイナミック タグを使用しているダイナミック アドレス グループに基づいてマッチングを行います。
- 新規の FTP サーバーまたは Web サーバーをデプロイすると、ダイナミック アドレス グループのメンバーが更新されることを確認します。これにより、セキュリティ ルールが、これらの新しい仮想マシンにも適用されます。

STEP 1 | VM 送信元モニタリングを有効化します。

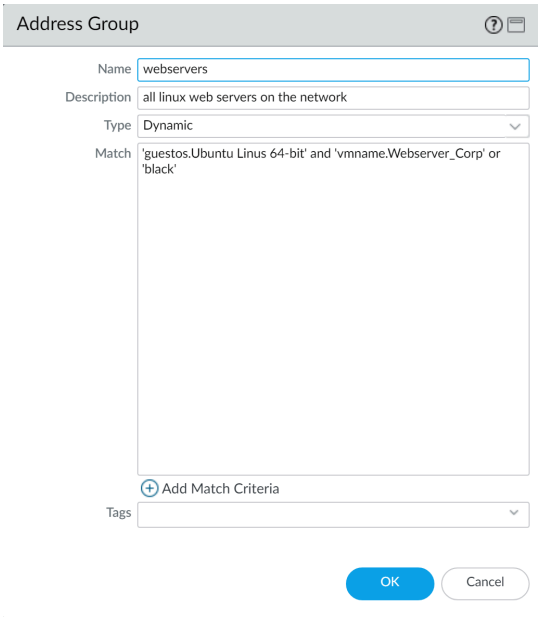
VM をモニタリングして仮想ネットワーク上の変更を追跡するを参照してください。

STEP 2 | ファイアウォール上にダイナミック アドレス グループを作成します。

この機能の概略を把握するために、チュートリアルを参照してください。

1. ファイアウォールの Web インターフェイスにログインします。
2. **Object (オブジェクト)** > **Address Groups (アドレス グループ)** を選択します。
3. **Add**（追加）をクリックし、**Name**（名前）にアドレス グループの名前を、**Description**（内容）にアドレス グループの内容を入力します。
4. **Type**（タイプ）で **Dynamic**（ダイナミック）を選択します。
5. 一致条件を指定します。グループのメンバーを決定する一致条件として、スタティック タグとダイナミック タグを選択できます。**Add Match Criteria**（条件の追加） をクリッ

クして、**AND** または **OR** 演算子を選択し、フィルタリングまたは照合に使用する属性を選択して **OK** をクリックします。



6. **Commit**（コミット）をクリックします。

STEP 3 | この例の各ダイナミック アドレス グループの一致条件は以下のとおりです。

ftp_server: ゲスト オペレーティング システム「Linux 64-bit」に一致し、「ftp」という注釈が付いている（'guestos.Ubuntu Linux 64-bit' and 'annotation.ftp'）

web-servers: 次の 2 つの条件に一致する。すなわち、タグが黒色か、またはゲスト オペレーティング システムが Linux 64 ビットでなおかつサーバー名が Web_server_Corp

STEP 4 | ポリシー内でダイナミック アドレス グループを使用します。

チュートリアルを参照してください。

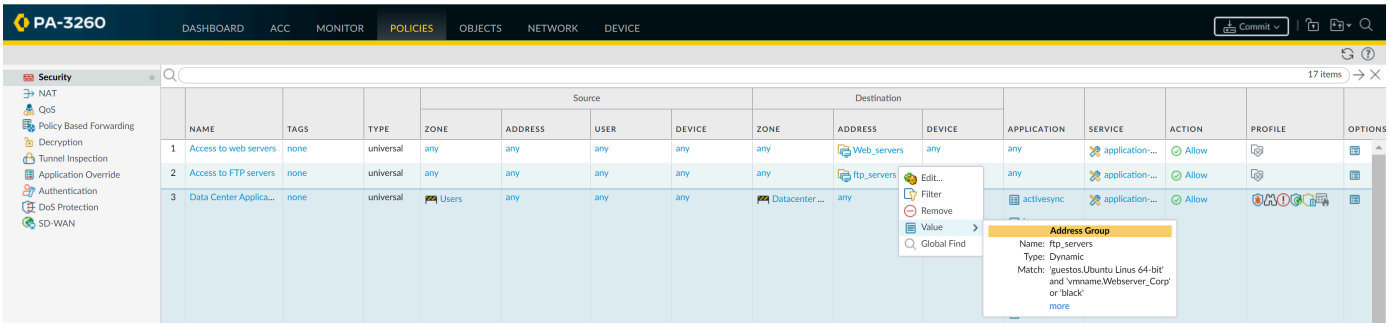
1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. [追加] をクリックし、ポリシーの [名前] および [説明] を入力します。
3. **Source Zone** (送信元ゾーン) を追加して、トラフィックの送信元となるゾーンを指定します。
4. トラフィックが終端する **Destination Zone** (宛先ゾーン) を追加します。
5. **Destination Address** (宛先アドレス) については、先ほど作成したダイナミック アドレス グループを選択します。
6. トラフィックに対するアクション（[許可] または [拒否]）を指定し、必要に応じてデフォルト セキュリティ プロファイルをルールに関連付けます。
7. 手順 1～6 を繰り返し、もう 1 つポリシー ルールを作成します。
8. **Commit**（コミット）をクリックします。

STEP 5 | この例では、2 つのポリシー、すなわち、FTP サーバーにアクセスするためのポリシーと Web サーバーにアクセスするためのポリシーを作成する方法を示します。

				Source				Destination							
	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTI
1	Access to web servers	none	universal	any	any	any	any	any	Web_servers	any	any	application-...	Allow		
2	Access to FTP servers	none	universal	any	any	any	any	any	ftp_servers	any	any	application-...	Allow		

STEP 6 | ファイアウォール上で、ダイナミック アドレス グループのメンバーが決定されていることを確認します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択し、ルールを選択します。
2. アドレス グループリンクの隣にあるドロップダウンの矢印を選択し、**Value**（値）を選択します。一致条件が正確であるか確認することもできます。



3. **more**（詳細）リンクをクリックし、登録された IP アドレスのリストが表示されることを確認します。

   このアドレス グループに属し、ここに表示されるすべての IP アドレスについてポリシーが適用されます。

登録済みのすべての *IP* アドレスを削除する場合は、*CLI* コマンド***debug object registered-ip clear all(***デバッグ オブジェクト登録済み ***IP*** すべてクリア***)***を使用し、タグをクリアした後にファイアウォールを再起動します。

ダイナミック IP アドレスおよびタグを確認する CLI コマンド

弊社ファイアウォールおよび Panorama の コマンドライン インターフェイスを使用すると、タグおよび IP アドレスの動的登録元となるさまざまなソースの詳細を確認できます。また、タグの登録と登録解除を監査することもできます。以下に、CLI の機能を例を挙げて説明します。

例	CLIコマンド
すべての登録済み IP アドレスのうち、state.poweredOn タグに一致するか、vSwitch0 というタグの付いていないものを表示します。	**show log iptag tag_name equal state.poweredOn** **show log iptag tag_name not-equal switch.vSwitch0**
VM 情報ソースによって取得された動的に登録された IP アドレスのうち、vmware1 という名前で、poweredOn というタグの付いているものを表示します。	**show vm-monitor source source-name vmware1 tag state.poweredOn registered-ip all**registered IP Tags ---------- ---------- -------- ------- fe80::20c:29ff:fe69:2f76 "state.poweredOn" 10.1.22.100 "state.poweredOn" 2001:1890:12f2:11:20c:29ff:fe69:2f76"state.poweredOn" fe80::20c:29ff:fe69:2f80 "state.poweredOn" 192.168.1.102 "state.poweredOn" 10.1.22.105 "state.poweredOn" 2001:1890:12f2:11:2cf8:77a9:5435:c0d "state.poweredOn " fe80::2cf8:77a9:5435:c0d "state.poweredOn"
特定の VM モニタリング送信元から学習したすべての IP アドレスとタグを、同送信元から切断せずにクリアします。	**debug vm-monitor clear source-name <*name*>**
すべての送信元から登録された IP アドレスを表示します。	**show object registered-ip all**
すべての送信元から登録された IP アドレスの数を表示します。	**show object registered-ip all option count**
すべての送信元から登録された IP アドレスをクリアします。	**debug object registered-ip clear all**

例	CLIコマンド
XML API を使用して登録された特定の IP アドレスのタグを追加または削除します。	**debug object registered-ip test [<register/unregister>] <ip/netmask><tag>**
特定の情報ソースから登録されたすべてのタグを表示します。	**show vm-monitor source source-name vmware1 tag all** vlanId.4095 vswitch.vSwitch1 host-ip.10.1.5.22 portgroup.TOBEUSED hostname.panserver22 portgroup.VM Network 2 datacenter.ha-datacenter vlanId.0 state.poweredOn vswitch.vSwitch0 vmname.Ubuntu22-100 vmname.win2k8-22-105 resource-pool.Resources vswitch.vSwitch2 guestos.Ubuntu Linux 32-bit guestos.Microsoft Windows Server 2008 32-bit annotation. version.vmx-08 portgroup.VM Network vm-info-source.vmware1 uuid.564d362c-11cd-b27f-271f-c361604dfad7 uuid.564dd337-677a-eb8d-47db-293bd6692f76 Total:22
ファイアウォール上の VM モニタリング エージェント、XML API、Windows ユーザー ID エージェント、CLI など、特定のデータ送信元から登録されたすべてのタグを表示します。	• CLI から登録されたタグを表示するには、以下のコマンドを実行します。 **show log iptag datasource_type equal unknown** • XML API から登録されたタグを表示するには、以下のコマンドを実行します。 **show log iptag datasource_type equal xml-api** • VM 情報ソースから登録されたタグを表示するには、以下のコマンドを実行します。 **show log iptag datasource_type equal vm-monitor** • Windows ユーザー ID エージェントから登録されたタグを表示するには、以下のコマンドを実行します。 **show log iptag datasource_type equal xml-api datasource_subtype equal user-id-agent**

例	CLIコマンド
（すべての送信元について）特定の IP アドレスから登録されたすべてのタグを表示します。	`debug object registered-ip show tag-source ip ip_address tag all`

アップストリーム デバイスの背後にあるエンドポイントとユーザーにポリシーを適用する

ネットワーク上のユーザーとファイアウォールの間に明示的プロキシ サーバーまたはロード バランスなどのアップストリーム デバイスを有する場合、ファイアウォールは、アップストリーム デバイスの IPアドレスを、コンテンツを要求したクライアントの IPアドレスではなく、プロキシが転送する HTTP/HTTPS トラフィックの送信元 IPアドレスと見なすことがあります。多くの場合、アップストリーム デバイスは、コンテンツを要求したクライアントまたは要求の送信元クライアントの実際の IPv4 または IPv6 アドレスが含まれている HTTP リクエストに、X-Forwarded-For (X-Forwarded-For - XFF)ヘッダーを追加します。

このような場合、XFF フィールドから IPアドレスを抽出し、それを User-ID を持つユーザーにマップするか、IPアドレスに基づいてセキュリティ ポリシーを適用するようにファイアウォールを設定できます。

- **User-ID** で**X-Forwarded-For (X-Forwarded-For - XFF)** ヘッダーを使用する—これにより、ユーザーベースのポリシーを適用して、プロキシ サーバーの背後にあるユーザーの Webベースのアプリケーションに安全にアクセスできるようになります。さらに、User-ID が XFF IP アドレスをユーザー名にマッピング可能な場合、ファイアウォールはトラフィック、脅威、WildFire の送信、および URL フィルタリングのログにそのユーザー名を送信元ユーザーとして表示し、プロキシの背後のユーザの Web アクティビティを表示します。
- セキュリティ ポリシー内で**X-Forwarded-For (X-Forwarded-For - XFF)** ヘッダーを使用する—これにより、HTTP ヘッダーの XFF フィールドの IPアドレスを使用して、送信元 IPアドレスに基づいてセキュリティ ポリシーを適用できます。さらに、XFF フィールドに IPアドレスを含むトラフィックにポリシーが適用される場合、トラブルシューティングと修復を支援するために、トラフィック、脅威、データ フィルタリング、および Wildfire 送信ログを設定できます。

ファイアウォールから送信されて外部サーバーからコンテンツを取得する Web 要求パケットの XFF 値を攻撃者が読み取って悪用できないようにするため、送信パケットから XFF 値を除去するようにファイアウォールを設定することもできます。User-ID 用に、またはポリシー内で XFF IPアドレスを使用することと XFF 値をストリップすることは相互に排他的ではありません。両方のオプションを設定した場合、ファイアウォールはポリシー適用とロギングに使用した後でのみ XFF 値をゼロに設定します。

*User-ID*とセキュリティ ポリシーの *XFF* フィールドの *IP*アドレスを同時に使用するようにファイアウォールを設定することはできません。

- ポリシーおよび送信元ユーザーのロギングでの XFF 値の使用
- セキュリティ ポリシーとロギングの XFF IPアドレス値
- イベントのトラブル シューティングに XFF ヘッダーの IP アドレスを使用する

送信元ユーザーに基づいたポリシーに XFF 値を使用する

ファイアウォールのマップは、XFF ヘッダーの IP アドレスを User-ID を使用するユーザー名に設定することで、他の方法では識別できないプロキシ サーバーの背後にあるユーザーの Web ト

ラフィックをユーザーが制御できるようにします。XFF ヘッダーの IP アドレスをユーザー名にマップするには、はじめに User-ID を有効にする必要があります。

このオプションを有効にすると、ファイアウォールはユーザー マッピングの目的でのみ XFF ヘッダーの IP アドレスを使用します。ファイアウォールが記録する送信元 IP アドレスは、依然としてプロキシ サーバーのものであり、送信元ユーザーのものではありません。ファイアウォールが XFF ヘッダーから抽出した IP アドレスを使用してマッピングされたユーザーに帰属するログ イベントが表示された場合、そのイベントに関連付けられている特定のデバイスを追跡することは困難です。プロキシサーバーの背後にあるユーザーに起因するイベントのデバッグとトラブルシューティングを簡素化するには、 URL フィルタリングのログ エントリと相関関係があるログ イベントに関連付けられた特定のユーザーおよびデバイスを追跡するために、URL フィルタリング ログの X-Forwarded-For 列に XFF ヘッダーの IP アドレスを入力するようにファイアウォールを設定する必要があります。

プロキシ サーバーが追加する XFF ヘッダーには、リクエストを送信したエンド ユーザーの送信元 IP アドレスが含まれている必要があります。ヘッダーに複数の IP アドレスが含まれている場合、ファイアウォールは最初の IP アドレスのみを使用します。ヘッダーに IP アドレス以外の情報が含まれている場合、ファイアウォールはユーザー マッピングを実行できません。

X-Forwarded-For ヘッダーを使用してユーザー マッピングを実行するようにファイアウォールを有効にしても、ファイアウォールは *XFF* ヘッダーのクライアント *IP* アドレスをログの送信元アドレスとして使用できません。ログには依然としてプロキシ サーバーの *IP* アドレスが送信元アドレスのままで表示されます。ただし、デバッグおよびトラブルシューティング プロセスを簡素化するために、XFF 値を URL フィルタリング ログに追加して、*XFF* ヘッダーからのクライアント *IP* アドレスを *URL* フィルタリング ログに表示するようにファイアウォールを設定することができます。

STEP 1 | ファイアウォールがポリシー、およびログの送信元ユーザー フィールドで XFF 値を使用できるようにします。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Content-ID** の順に選択し、X-Forwarded-For Headers (X-Forwarded-For ヘッダー) 設定を編集します。
2. **Use X-Forwarded-For Header in User-ID (User-ID** 内の **X-Forwarded-For** ヘッダ**)** を選択します。

STEP 2 | 送信 Web 要求から XFF 値を削除します。

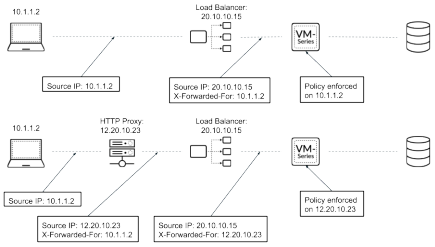
1. **Strip X-Forwarded-For Header (X-Forwarded-For** ヘッダの除去**)** を選択します。
2. **OK**、**Commit (コミット)** の順にクリックします。

STEP 3 | ファイアウォールがログの送信元ユーザー フィールドを入力していることを確認します。

1. 送信元ユーザー フィールドがあるログ タイプ（**Monitor (監視)** > **Logs (ログ)** > **Traffic (トラフィック)** など）を選択します。
2. Source User （送信元ユーザー）列に、Web アプリケーションにアクセスするユーザーのユーザー名が表示されていることを確認します。

セキュリティ ポリシーとロギングの XFF IPアドレス値

X-Forwarded-For (XFF) HTTP ヘッダー・フィールド 内のソース IP アドレスを使用するようにファイアウォールを構成して、セキュリティー ポリシーを適用できます。パケットがファイアウォールに到達する前に単一のプロキシ サーバーを通過する場合、XFF フィールドには発信元エンドポイントの IP アドレスが入ります。ただし、パケットが複数のアップストリーム デバイスを通過する場合、ファイアウォールは最後に追加された IP アドレスを使用してポリシーを適用したり、IP 情報に依存する他の機能を使用することができます。



- XFF 値をポリシー内で使用する
- ログ内の XFF 値を表示する
- レポート内の XFF値を表示する

XFF 値をポリシー内で使用する

XFF ヘッダー内のクライアント IP アドレスを使用してセキュリティー ポリシーを適用するには、以下の手順を実行します。

Microsoft Azure では、デフォルトで、アプリケーション ゲートウェイが元の送信元 *IP*アドレスとポートを *XFF* ヘッダーに挿入します。ファイアウォールのポリシーで *XFF* ヘッダーを使用するには、*XFF* ヘッダーからポートを省略するようにアプリケーション ゲートウェイを設定する必要があります。詳細は、Azure マニュアルを参照してください。

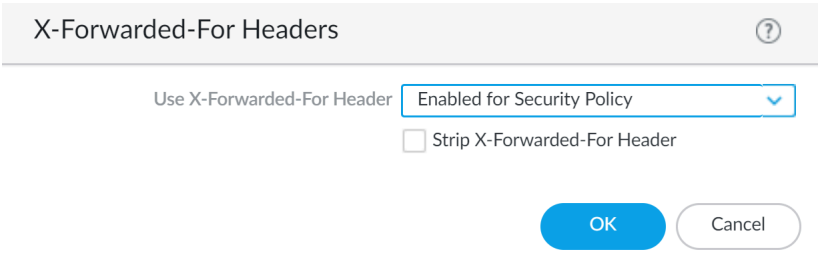
STEP 1 | 利用中のファイアウォールにログインします。

STEP 2 | **Device** > **Setup (デバイスのセットアップ)** > **Content-ID** > **X-Forwarded-For (XFF)**ヘッダーを選択します。

STEP 3 | 編集アイコンをクリックします。

STEP 4 | **Use X-Forwarded-For (XFF)** ヘッダードロップダウンから、**Enabled for Security Policy** (セキュリティ ポリシーに対して有効化) を選択します。

X-Forwarded-For Header for security policy と *User-ID* を同時に有効にすることはできません。



STEP 5 | (Optional) **Strip X-Forwarded-For Header** を選択して、発信 HTTP 要求から XFF フィールドを削除します。

このオプションを選択しても、XFF ヘッダーの使用は無効になりません。ファイアウォールは、XFF フィールドをポリシーの適用と IP アドレスのログ記録 をした後に クライアント要求から XFF フィールドを除去します。

STEP 6 | **OK** をクリックします。

STEP 7 | 変更を **Commit** (コミット) します。

ログ内の XFF 値を表示する

セキュリティー ポリシーでの XFF ヘッダーの使用に加えて、さまざまなログ、レポート、およびアプリケーションコマンドセンター (ACC) で XFF IP アドレスを表示して、モニターおよびトラブルシューティングに役立てることができます。[X-Forwarded-For] 列を Traffic、Threat、Data Filtering、および Wildfire Submissions の各ログに追加できます。

URL フィルタリング以外のログでは、*XFF IP* ロギングはパケット キャプチャーが使用可能になっていない場合にのみサポートされます。

リセット アクションを必要とする脅威 (***reset-client***、***reset-server***、または ***reset-both***) をファイアウォールが検出し、最後に検査されたパケットに *XFF* ヘッダーが含まれていない場合、*X-Forwarded-For IP* 列は値を表示しません。

ログに XFF IPアドレスを表示するには、以下の手順を実行します。

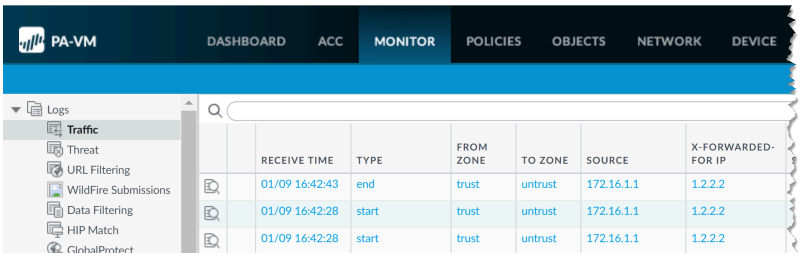
STEP 1 | 利用中のファイアウォールにログインします。

STEP 2 | **Monitoring** > **Log** (ログのモニタリング) を選択します。

STEP 3 | **Traffic** (トラフィック)、**Threat** (脅威)、**Data Filtering** (データ フィルタリング)、または **WildFire Submissions** (WildFire 送信) を選択します。

STEP 4 | 列ヘッダーの右側にある矢印をクリックし、**Columns**(列) を選択します。

STEP 5 | **X-Forwarded-For (XFF) IP** を選択して、ログ内の XFF IP を表示します。



レポート内の XFF値を表示する

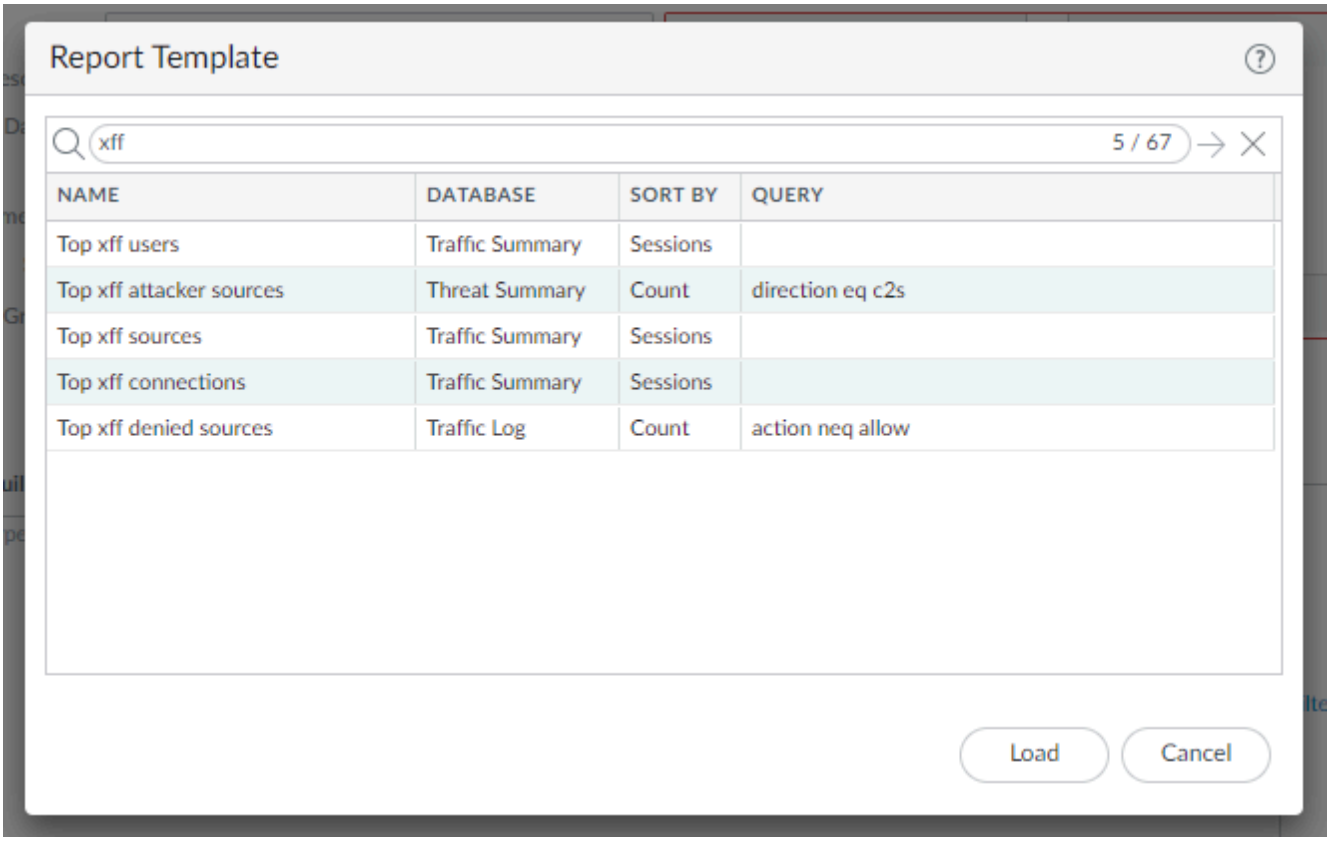
ファイアウォールによって生成される 定義済みレポート には、XFF 値が含まれていません。ただし、ファイアウォールには、XFF 情報を含む組み込みのレポート テンプレートがあります。XFF IP アドレスをレポートで表示するには、ビルトイン テンプレートを使用してレポートを生成する手順に従います。

STEP 1 | 利用中のファイアウォールにログインします。

STEP 2 | **Monitor (監視)** > **Manage Custom Reports (カスタム レポートの管理)** > **Add (追加)** の順に選択します。

STEP 3 | **Load Template (テンプレートのロード)** をクリックします。

STEP 4 | 検索バーに「XFF」と入力し、検索ボタンをクリックして、組み込みの XFF レポート テンプレートを見つけます。



STEP 5 | **Load (ロード)** をクリックします。

STEP 6 | カスタム レポートを構成します。**Time Frame**、**Sort By**、および **Group By** をクリックして、ニーズに最も適した方法で XFF 情報を表示します。

STEP 7 | (オプション) 今すぐ実行 をクリックして、スケジュールされた時間 の代わりに、またはそれに加えて、オンデマンドでレポートを生成します。

イベントのトラブル シューティングに XFF ヘッダーの IP アドレスを使用する

デフォルトでは、ユーザー マッピングに X-Forwarded-For（XFF）ヘッダーからこのアドレスを使用している場合でも、ファイアウォールはプロキシ サーバーの背後にあるクライアントの送信元アドレスを記録しません。したがって、ログイベントに関連付けられた特定のユーザーを識別することはできますが、ログイベントを発信したソースデバイスを簡単に識別することはできません。プロキシー・サーバーの背後にあるユーザーのイベントのデバッグとトラブルシューティングを単純化するには、Web ベース・アプリケーションへのアクセスを許可するセキュリティー・ポリシー・ルールにアタッチする URL フィルタリング・プロファイルで X-Forwarded-For オプションを有効にします。このオプションを有効にすると、ファイアウォールは XFF ヘッダーの IP アドレスをルールに一致するすべてのトラフィックの送信元アドレスとして記録します。

URL Filtering ログに *X-Forwarded For IP* フィールドは表示されません。*X-Forwarded-For IP* ログ イベントを表示するには、ログを *CSV* 形式にエクスポートする必要があります。

XFF ヘッダーを *URL* フィルタリング ログの送信元アドレスとして使用するようにファイアウォールを有効にしても、送信元アドレスのユーザー マッピングは有効になりません。送信元ユーザーのフィールドを生成するには、「ポリシーおよび送信元ユーザーのロギングでの XFF 値の使用」を参照してください。

STEP 1 | URL フィルタリングプロファイルで X-Forwarded-For オプションを有効にします。

1. **Objects** > セキュリティプロファイル > **URL** フィルタリング を選択し、構成する URL フィルタリング プロファイルを選択するか、 新しいプロファイルを追加します。

   デフォルトの *URL* フィルタリング プロファイルで *XFF* ロギングを有効にすることはできません。

2. **URL** フィルタリング設定 タブを選択し、**X-Forwarded-For** を有効にします。
3. **OK** をクリックしてプロファイルを保存します。

STEP 2 | URL フィルタリング プロファイルを、Web アプリケーションへのアクセスを可能にするセキュリティ ポリシー ルールに適用します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）を選択してルールをクリックします。
2. **Actions**（操作）タブを選択して、**Profile Type**（プロファイル タイプ）を **Profiles**（プロファイル）に設定し、X-Forwarded-For HTTP ヘッダーのロギング用に設定した **URL Filtering**（**URL** フィルタリング）プロファイルを選択します。
3. **OK**、**Commit (コミット)** の順にクリックします。

STEP 3 | ファイアウォールが XFF 値をログに記録していることを確認します。

XFF 列は、ファイアウォールの *URL* フィルタリング ログには表示されません。

1. **Monitor (監視)** > **Logs (ログ)** > **URL Filtering (URL** フィルタリング**)** を選択します。
2. 以下のいずれかの方法で XFF 値を表示します。
   - 「Export to CSV ( )」をクリックして、URL Filtering ログをコンマ区切り値ファイルにエクスポートします。ダウンロードが完了したら、**Download file** をクリックして、ファイルのコピーをローカル デバイスに保存します。
   - **`show log url csv-output equal yes`** CLI コマンドを使用します。

STEP 4 | 別のログ タイプのログ イベントのトラブルシューティングを行うには、URL フィルタリング ログの XFF フィールドを使用します。

HTTP/HTTPS トラフィックに関連付けられたイベントに気付いたが、プロキシ サーバーのイベントであるために送信元 IP アドレスを識別できない場合は、相関 URL Filtering ログの X-Forwarded-For 値を使用して、ログ イベントに関連付けられた送信元アドレスを識別できます。このために、次の作業を行います：

1. Traffic、Threat、または WildFire Submissions ログで、プロキシサーバーの IP アドレスを送信元アドレスとして示すイベントを見つけます。
2. ログの詳細を表示するには、拡大鏡アイコンをクリックし、詳細ログ ビューア ウィンドウの下部にある関連 URL フィルタリング ログを探します。
3. 関連付けられた URL フィルタリング ログを CSV ファイルにエクスポートし、X-Forwarded For IP 列を探します。この列の IP アドレスは、プロキシー・サーバーの背後にあるソース・ユーザーの IP アドレスを表します。この IP アドレスを使用して、調査中のイベントをトリガしたデバイスを追跡します。

ポリシー ベース フォワーディング

ファイアウォールは通常、パケットの宛先 IP アドレスを使用して発信インターフェイスを決定します。具体的には、インターフェイスに接続されている仮想ルーターに関連付けられたルーティング テーブルを使用してルート検索を実行します。ポリシー ベース フォワーディング（PBF）では、ルーティング テーブルをオーバーライドして、送信元と宛先の IP アドレスやトラフィック タイプなどの個々のパラメータに基づいて、発信または *egress*（出力）インターフェイスを指定できます。

- PBF
- ポリシー ベース フォワーディング ルールの作成
- 「ユース ケース：デュアル ISP でのアウトバウンド アクセス用 PBF

PBF

PBF ルールを使用すると、ルーティング テーブルに指定されたネクスト ホップからの代替経路を選択させることができます。これは通常、セキュリティまたはパフォーマンス上の理由で出力インターフェイスを指定するときに使用します。たとえば、本社と支店が、安価なインターネットと高価な専用線の 2 つのリンクで接続されているとします。専用線は帯域幅が広く、低レイテンシーの（遅延の少ない）リンクです。セキュリティを高める場合は、PBF を使用して、FTP などのアプリケーションによって生成される非暗号化トラフィックは専用線を介して送信し、その他のトラフィックはインターネット経由で送信します。また、パフォーマンスを高める場合は、基幹業務アプリケーションのトラフィックは専用線を通すようにルーティングし、Web ブラウジングなど、その他のすべてのトラフィックは安価なリンクを介して送信します。

- 出力パスと対称リターン
- PBF のためのパス モニタリング
- PBF におけるサービスとアプリケーション

出力パスと対称リターン

PBF を使用すると、トラフィックを特定のインターフェイスに向ける、トラフィックをドロップする、（マルチ仮想システムが有効になっているシステムで）トラフィックを別の仮想システムに向けるといった操作を実行できます。

デュアル ISP 環境など、非対称ルートのあるネットワークでは、ファイアウォール上のトラフィック着信インターフェイスと発信インターフェイスが異なっていると接続の問題が発生します。ルートが非対称の場合、すなわち、フォワード（SYN パケット）パスとリターン（SYN/ACK）パスが異なる場合、ファイアウォールはセッション全体の状態を追跡できないため、接続エラーが発生します。トラフィックが対称パスを通過するようにするには、つまり、トラフィックの発信および着信インターフェイスと、セッションが作成されたインターフェイスを一致させるには、対称リターンオプションを有効にします。

対称リターンでは、仮想ルーターがリターン トラフィックのルーティング検索をオーバーライドして、自分が SYN パケット（または最初のパケット）を受信した MAC アドレスに向けてトラフィックを戻します。ただし、宛先 IP アドレスが入力/出力インターフェイスの IP アドレス

と同じサブネット上に存在する場合は、ルート検索が実行され、対称リターンは実施されません。この動作により、トラフィックがサイレントに破棄されるのを防ぎます。

対称リターンのネクスト ホップを決定するために、ファイアウォールはアドレス解決プロトコル（*ARP*）テーブルを使用します。*ARP* テーブルの最大エントリ数は、ファイアウォールのモデルによって制限されており、ユーザーが設定することはできません。お使いのモデルの制限値を確認するには、次の*CLI* コマンドを使用します。***show pbf return-mac all***。

PBF のためのパス モニタリング

パス モニタリングでは、IP アドレスへの接続を確認し、必要に応じてファイアウォールが代替ルート経由でトラフィックを送信できるようにします。ファイアウォールでは、ICMP ping をハートビートとして使用して、指定された IP アドレスが到達可能かどうかを確認します。

モニタリング プロファイルを使用すると、ハートビートのしきい値を指定して、IP アドレスが到達可能かどうかを確認できます。モニター対象の IP アドレスが到達不可能な場合は、PBF ルールを無効化するか、フェイル オーバーまたは回復を待機アクションを指定します。PBF ルールを無効化すると、仮想ルーターがルーティング決定を引き受けます。フェイル オーバーまたは回復を待機アクションが実行されると、モニタリング プロファイルはターゲット IP アドレスが到達可能かどうかを引き続きモニターし、回復するときにファイアウォールは元のルートを使用して元に戻します。

以下の表に、新規セッションと確立済みセッションとで、パス モニタリング エラーが発生したときの動作の違いを示します。

モニタリング エラー発生時のセッションの動作	モニター対象 **IP** アドレスが到達不能な場合もルールを有効なままにする	モニター対象 **IP** アドレスが到達不能な場合はルールを無効にする
確立済みセッションの場合	回復を待機 – PBF ルールに指定された出力インターフェイスを引き続き使用します	回復を待機 – PBF ルールに指定された出力インターフェイスを引き続き使用します
	フェイル オーバー – ルーティング テーブルによって決定したパスを使用します（PBF なし）	フェイル オーバー – ルーティング テーブルによって決定したパスを使用します（PBF なし）
新規セッションの場合	回復を待機 – ルーティング テーブルによって決定したパスを使用します（PBF なし）	回復を待機 – 残りの PBF ルールを確認します。一致するルールがなければ、ルーティング テーブルを使用します。
	フェイル オーバー – ルーティング テーブルによって決定し	フェイル オーバー – 残りの PBF ルールを確認します。一致する

モニタリング エラー発生時のセッションの動作	モニター対象 IP アドレスが到達不能な場合もルールを有効なままにする	モニター対象 IP アドレスが到達不能な場合はルールを無効にする
	たパスを使用します（PBF なし）	ルールがなければ、ルーティング テーブルを使用します。

PBF におけるサービスとアプリケーション

PBF ルールは、最初のパケット（SYN）または最初のパケットに対する応答（SYN/ACK）に適用されます。つまり、アプリケーションを確認できる十分な情報をファイアウォールが取得する前に、PBF ルールが適用される可能性があります。このため、アプリケーション固有のルールを PBF で使用することはお勧めできません。できるかぎり、サービス オブジェクト（プロトコルまたはアプリケーションによって使用されるレイヤー 4 ポート（TCP または UDP））を使用してください。

PBF ルールにアプリケーションを指定すると、ファイアウォールは *App-ID* キャッシングを実行します。アプリケーションが初めてファイアウォールを通過するとき、ファイアウォールにはそのアプリケーションを識別するだけの十分な情報がないため、PBF ルールを適用できません。さらに多くのパケットが到達するにつれ、ファイアウォールがアプリケーションを決定し、App-IDキャッシュにエントリーを作成し、そのセッション用にこのApp-IDを保持します。同じ宛先 IP アドレス、宛先ポート、およびプロトコル ID で新規のセッションが作成されると、ファイアウォールは、そのアプリケーションを（App-ID キャッシュに基づいて）最初のセッションと同じアプリケーションとして識別し、PBF ルールを適用します。したがって、完全一致ではない、同じアプリケーションではないセッションは、PBF ルールに基づいて転送できます。

また、アプリケーションには依存性があり、アプリケーションの識別情報は、ファイアウォールが受信するパケット数が増えてくると変化する可能性があります。PBF はセッションの開始時にルーティングを決定するため、ファイアウォールは、アプリケーションの識別情報の変化に対応できません。たとえば、YouTube は、Web ブラウジングとして開始されますが、その後、ページに含まれているさまざまなリンクや動画に応じて、Flash、RTSP、YouTube などに変化します。ところが、PBF を使用すると、ファイアウォールはセッションの開始時に YouTube アプリケーションを Web ブラウジングとして識別するため、その後アプリケーションの識別情報が変化しても認識されません。

カスタム アプリケーション、アプリケーション フィルタ、アプリケーション グループは *PBF* ルールで使用できません。

ポリシー ベース フォワーディング ルールの作成

PBF ルールを使用して、firewall 上の特定の出力インターフェイスにトラフィックを転送し、トラフィックのデフォルト パスをオーバーライドします。

STEP 1 | Policy-Based Forwarding (ポリシー ベース フォワーディング - PBF)ルールの作成

PBF ルールを作成する際には、ルールの名前、送信元ゾーンまたはインターフェイス、および出力インターフェイスを指定する必要があります。その他のコンポーネントはすべて、オプション指定になっているか、デフォルト値が設定されています。

IP アドレス、アドレス オブジェクト、あるいは *FQDN* を使用して送信元および宛先アドレスを指定できます。

1. **Policies (**ポリシー**)** > **Policy Based Forwarding (**ポリシーベース フォワーディング**)** を選択して、PBF ポリシー ルールを **Add (**追加**)** します。
2. ルールの名前を入力します（**General**（全般））。
3. **Source**（送信元）を選択して、以下を設定します。
   1. 転送 ポリシーを適用する **Type (**タイプ**)**（**Zone (**ゾーン**)** または **Interface (**インターフェース**)**）を選択し、該当するゾーンまたはインターフェースを指定します。対

称リターンを適用したい場合は、送信元インターフェイスを選択する必要があります。

レイヤー *3* インターフェイスだけが *PBF* をサポートしています。ループバック インターフェイスは *PBF* をサポートしていません。

2. (任意) PBF ルールが適用される **Source Address (**送信元アドレス**)** を指定します。たとえば、このルールで指定したインターフェイスまたはゾーンへのトラフィックの送信元となる IP アドレスまたはサブネット IP アドレスなどです。

   Negate (反転***)*** をクリックし、*1* つまたは複数の ***Source Addresses (***送信元アドレス***)*** を *PBF* ルールから除外します。たとえば、特定のゾーンからのすべてのトラフィックをインターネットに向ける *PBF* ルールを記述している場合、***Negate*** を使用して *PBF* ルールから内部 *IP* アドレスを除外できます。

   ルールは上から順に評価されます。定義済みの基準を満たす最初のルールとパケットが一致すると、それが引き金となり、それ以降のルールは評価されません。

3. （任意）**[**追加**]** をクリックして、**[**送信元ユーザー**]** またはポリシーが適用されるユーザーのグループを選択します。

4. **Destination/Application/Service (**宛先**/**アプリケーション**/**サービス**)** を選択し、以下を設定します。

   1. **Destination Address**（宛先アドレス）—デフォルトでは、ルールは **Any(**任意の） IP アドレスに適用します。**Negate (**反転**)** をクリックし、1 つまたは複数の宛先 IP アドレスを PBF ルールから除外します。
   2. PBF を使用して制御する必要がある任意の**Application (**アプリケーション**)** および **Service (**サービス**)** を **Add (**追加**)** します。

      PBF ルールはアプリケーションを判断できるだけの十分な情報をファイアウォールが得る前に適用される場合があるため、*PBF* と共にアプリケーション固有のルールを使用することは推奨しません。できるかぎり、サービス オブジェクト（プロトコルまたはアプリケーションによって使用されるレイヤー *4* ポート（*TCP* または *UDP*））を使用してください。詳細については、「PBF におけるサービスとアプリケーション」を参照してください。

STEP 2 | ルールにマッチするパケットを転送する方法を指定します。

マルチ VSYS 環境で PBF の設定を行っている場合、仮想システム毎に別の *PBF* ルールを作成（そして適切なセキュリティポリシールールを作成してトラフィックを有効化）する必要があります。

1. **Forwarding**（転送）を選択します。
2. パケットが一致するとき、取るべき**Action (**アクション**)** を設定します。
   - **Forward (**転送**)**—パケットを特定の **Egress Interface (**出力インターフェイス**)** に向けます。
   - **Forward To VSYS**（**VSYS** に転送）（マルチvirtual system (仮想システム - vsys)が有効化されているファイアウォールで）—パケットの転送先仮想システムを選択します。
   - **Discard (**破棄**)** —パケットを廃棄します。
   - **No PBF (PBF** なし**)**—ルールに定義された送信元、宛先、アプリケーション、またはサービスの条件に一致するパケットを除外します。パケットの照合には、PBF の代わりにルーティング テーブルを使用します。ファイアウォールは、ルーティング テーブルを使用して、一致したトラフィックをリダイレクト ポートから除外します。
3. 指定した **Action (**アクション**)** を毎日、毎週、または 1 回限りの頻度でトリガーするには、**Schedule (**スケジュール**)** を作成して関連付けます。
4. **Next Hop (**ネクストホップ**)** については次のいずれかを選択します。
   - **IP Address (IP** アドレス**)**—ファイアウォールが一致するパケットを転送する IP アドレスを入力するか、IP ネットマスク タイプのアドレス オブジェクトを選択します。IPv4 アドレス オブジェクトには /32 ネットマスクが必要で、IPv6 アドレス オブジェクトには /128 ネットマスクが必要です。
   - **FQDN**—ファイアウォールがマッチするパケットを転送する FQDN を入力します (あるいは、タイプ FQDN のアドレス オブジェクトを選択するか作成します)。FQDN は IPv4 アドレス、IPv6 アドレス、あるいはその両方に解決されます。FQDN が IPv4 および IPv6 アドレスの両方に解決される場合、PBF ルールは IPv4 アドレスおよび IPv6 アドレスという 2 つのネクストホップを持ちます。IPv4 および IPv6 トラフィックの両方で同じ PBF ルールを使用できます。IPv4 トラフィックは IPv4 ネク

ストホップに転送されます。IPv6 トラフィックは IPv6 ネクストホップに転送されます。

この *FQDN* は、*PBF* 用に構成したインターフェイスと同じサブネットに属する *IP* アドレスに解決する必要があります。解決しない場合、*firewall* は解決を拒否し、*FQDN* は未解決のままになります。

firewall は、*FQDN* の *DNS* 解決から *(*各 *IPv4* または *IPv6* ファミリ・タイプの*) IP* アドレスを *1* つだけ使用します。*DNS* 解決が複数のアドレスを返すと、ファイアウォールはネクストホップ用に設定された *IP* 系統 *(IPv4* あるいは *IPv6)* にマッチする、優先される *IP* アドレスを使用します。優先される *IP* アドレスは、*DNS* サーバーが初回の応答で返す最初のアドレスです。*firewall* は、順序に関係なく、アドレスが後続の応答に表示される限り、このアドレスを優先的に保持します。

- **None (**なし**)**—ネクストホップがないということは、パケットの宛先 IP アドレスがネクストホップとして使用されていることを意味します。宛先 IP アドレスが出力インターフェイスと同じサブネットに存在しない場合、転送はエラーになります。

5. (任意) モニタリングを有効にして、IP アドレスが指定されていない場合にターゲット IP アドレスまたは **Next Hop (**ネクストホップ**)** IP アドレスとの接続を確認します。**Monitor (**監視**)** を選択して、監視対象のアドレスが到達不能な場合のアクションを指定した (デフォルトまたはカスタムの) モニタリング **Profile (**プロファイル**)** を関連付けます。

   - **Disable this rule if nexthop/monitor ip is unreachable (**ネクストホップ**/**監視 **IP** に到達できない場合にこのルールを無効化**)**を行うことができます。
   - 監視対象の **IP Address (IP** アドレス**)** を入力します。

   Egress Interface (出口インターフェース**)** は IPv4 および IPv6 アドレスの両方を持つことができ、**Next Hop (**ネクストホップ**)** FQDN は IPv4 および IPv6 アドレスの両方に解決される場合があります。この場合：

   1. 出力インターフェイスが IPv4 および IPv6 アドレスの両方を持っており、ネクストホップ FQDN が単一のアドレス系統にのみ解決される場合、ファイアウォールは解決済みの IP アドレスを監視します。FQDN が IPv4 および IPv6 アドレスの両方に解決されるものの、出口インターフェースが単一のアドレス系統しか持っていない場合、ファイアウォールは出口インターフェースのアドレス系統に一致する解決済みのネクストホップ アドレスを監視します。
   2. 出力インターフェイスおよびネクストホップ FQDN の両方が IPv4 および IPv6 アドレスの両方を持っている場合、ファイアウォールは IPv4 ネクストホップ アドレスを監視します。
   3. 出口インターフェースが単一のアドレス系統を持っており、ネクストホップ FQDN が別のアドレス系統に解決される場合、ファイアウォールは何も監視しません。

6. (非対称ルーティング環境では必須。それ以外の場合はオプション) **Enforce Symmetric Return (**対称リターンの適用**)**を行い、**Next Hop Address List (**ネクスト ホップ アドレス リスト**)** に 1 つ以上の IP アドレスを **Add (**追加**)** します。ネクストホップ IP アドレスは

最大 8 つ追加できます。トンネルおよび PPoE インターフェイスはネクストホップ IP アドレスとして利用できません。

対称リターンを有効にすると、リターン トラフィック（たとえば、LAN 上の信頼されたゾーンからインターネットへのトラフィック）が、インターネットからトラフィックが入るときと同じインターフェースを介して外向きに転送されます。

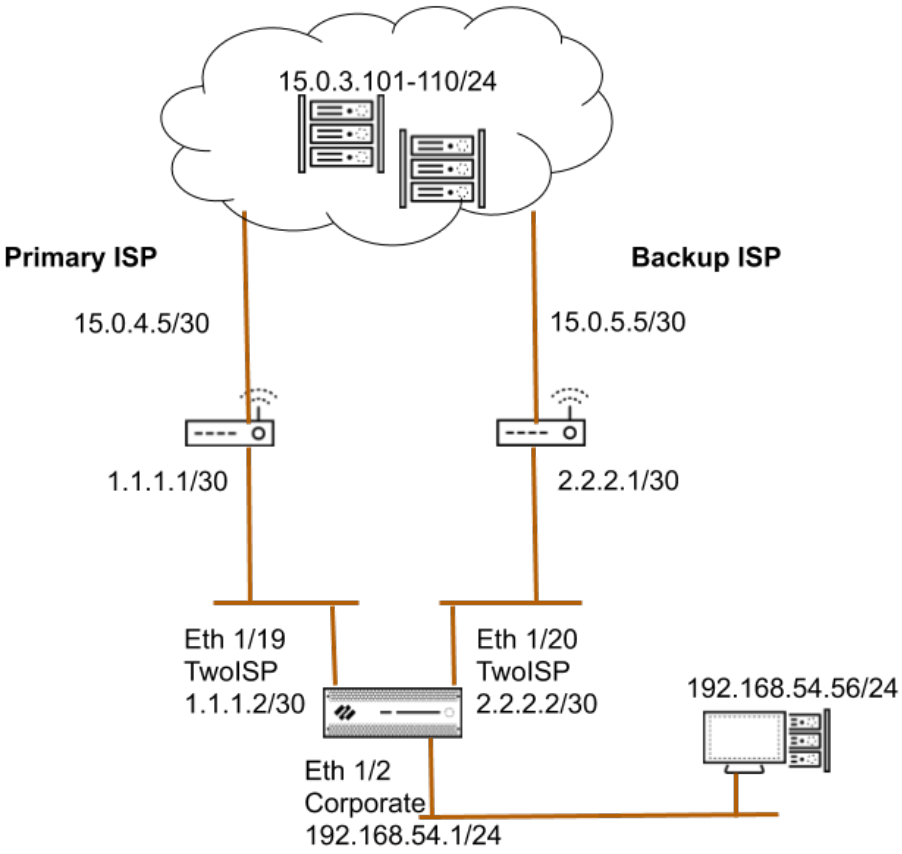
STEP 3 | 変更をコミットします。PBF ルールが有効になります。

	Source			Destination			Forwarding			Monitoring	
NAME	ZONE/INTERFACE	ADDRESS	USER	ADDRESS	SERVICE	ACTION	EGRESS I/F	NEXT HOP	ENFORCE SYMMETRIC RETURN	PROFILE	DISABLE IF UNREACHABL
pdf2	ethernet1/3	any	any	HQ-subnet	service-http	forward	ethernet1/1.100	192.168.100.2	false	none	false

「ユース ケース：デュアル ISP でのアウトバウンド アクセス用 PBF

このユース ケースでは、支店にデュアル ISP が構成されており、PBF による冗長なインターネット アクセスを実装しています。バックアップ用の ISP は、クライアントから Web サーバーへのトラフィックのデフォルト ルートになっています。BGP などのネットワーク間プロトコルを使用せずに冗長なインターネット アクセスを実現するために、ここでは、宛先インターフェイス ベースの送信元 NAT とスタティック ルートに PBF を使用して、以下のようにファイアウォールを設定します。

- プライマリ ISP 経由でトラフィックをルーティングする PBF ルールを有効化し、そのルールにモニタリング プロファイルを関連付けます。プライマリ ISP が使用できない場合は、モニタリング プロファイルによって、バックアップ ISP 経由のデフォルト ルートを使用するよう指示するトリガーがファイアウォールに対して起動されます。
- プライマリ ISP とバックアップ ISP の両方について、対応する ISP の出力インターフェイスに関連付けられた送信元 IP アドレスを使用するようファイアウォールに指示する送信元 NAT ルールを定義します。これにより、アウトバウンド トラフィックに正しい送信元 IP アドレスが設定されるようになります。
- バックアップ ISP にスタティック ルートを追加します。これにより、プライマリ ISP が使用不可になった場合に、デフォルト ルートが有効になり、トラフィックがバックアップ ISP 経由でルーティングされるようになります。



STEP 1 | ファイアウォール上で入力および出力インターフェイスを設定します。

出力インターフェイスは同じゾーン内に存在していてもかまいません。

1. **Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** の順に選択し、設定するインターフェイスを選択します。

   この例で使用するファイアウォール上のインターフェイス設定を以下に示します。

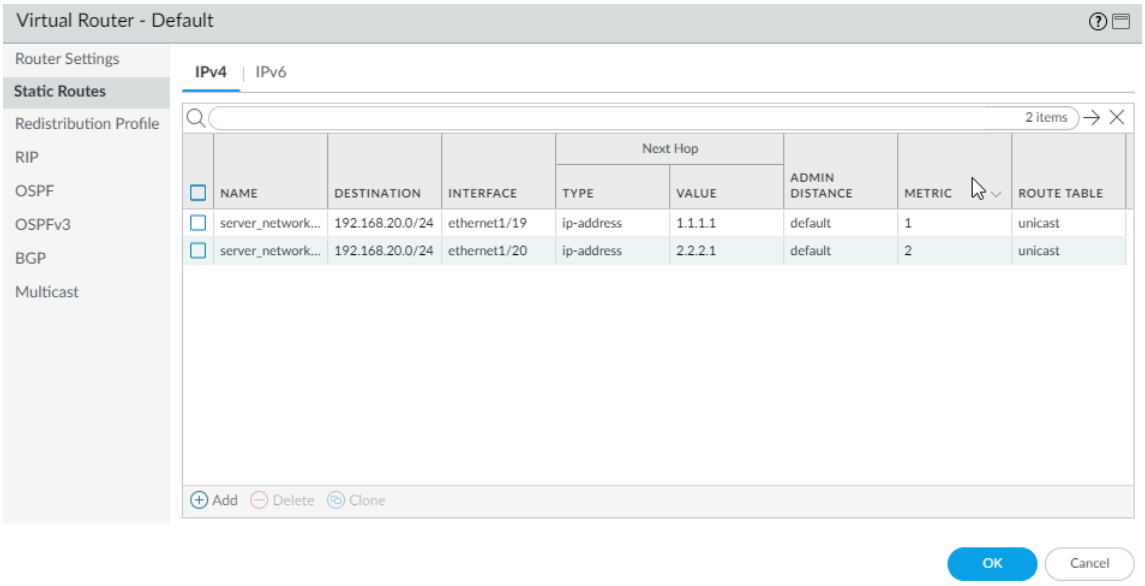
   - イーサネット 1/19 をプライマリ ISP に接続:
     - ゾーン:TwoISP
     - IPアドレス:1.1.1.2/30
     - 仮想ルーター：Default（デフォルト）
   - イーサネット1/20 をバックアップ ISP に接続:
     - ゾーン:TwoISP
     - IPアドレス:2.2.2.2/30
     - 仮想ルーター：Default（デフォルト）
   - Ethernet 1/2 は、ネットワーク クライアントがインターネットに接続するために使用する入力インターフェイスです。
     - ゾーン:企業
     - IPアドレス:192.168. 54.1/24
     - 仮想ルーター：Default（デフォルト）
2. インターフェイス設定を保存するには、**OK** をクリックします。

STEP 2 | 仮想ルーター上で、バックアップ ISP に対するスタティック ルートを追加します。

1. **Network (**ネットワーク**)** > **Virtual Router (**仮想ルーター**)** を選択し、**default (**デフォルト**)** リンクを選択して Virtual Router (仮想ルーター - VR) ダイアログを開きます。
2. **Static Routes**（スタティック ルート） を選択して **Add**（追加）をクリックします。**[**名前**]** フィールドにルート名を入力し、**[**宛先**]** フィールドにスタティック ルートを定義する IP アドレスの宛先を入力します。この例では、すべてのトラフィックに 0.0.0.0/0 を使用しています。
3. **IP Address (IP** アドレス**)** ラジオ ボタンを選択し、バックアップ インターネット ゲートウェイに接続するルーターの **Next Hop (**ネクスト ホップ**)** IP アドレスを設定しま

す（ネクストホップに対してドメイン名を使用することはできません）。この例では、2.2.2.1 です。

4. ルートのコスト メトリックを指定します。



5. **OK** を 2 回クリックして仮想ルーターの設定を保存します。

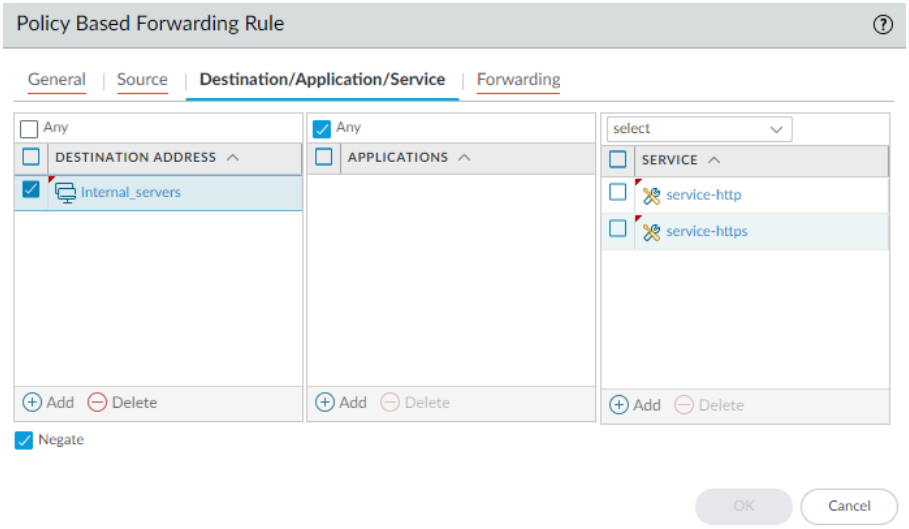
STEP 3 | プライマリ ISP に接続されたインターフェイスにトラフィックを向ける PBF ルールを作成します。

PBF から内部サーバー/IP アドレス宛てのトラフィックを除外します。Negate ルールを定義して、内部 IP アドレスを宛先とするトラフィックが、PBF ルールに定義された出力インターフェイス経由でルーティングされないようにします。

1. **Policies (ポリシー)** > **Policy Based Forwarding (ポリシーベース フォワーディング)** を選択して **Add (追加)** をクリックします。
2. **[全般]** タブで、ルールの分かりやすい **[名前]** を入力します。
3. **Source (送信元)** タブで、**Source Zone (送信元ゾーン)** を設定します。この例では、ゾーンは Corporate (企業) です。
4. **[宛先/アプリケーション/サービス]** タブで、以下を設定します。
   1. [宛先アドレス] セクションで、内部ネットワークのサーバーの IP アドレスまたはアドレス範囲を **[追加]** するか、内部サーバーのアドレス オブジェクトを作成します。**[Negate]** を選択して、上記の IP アドレスまたはアドレス オブジェクトをこのルールから除外します。
   2. [サービス] セクションで、**service-http** および **service-https** サービスを **[追加]** して、HTTP および HTTPS トラフィックがデフォルト ポートを使用するのを許可しま

す。セキュリティ ポリシーで許可されているその他のすべてのトラフィックについては、デフォルト ルートが使用されます。

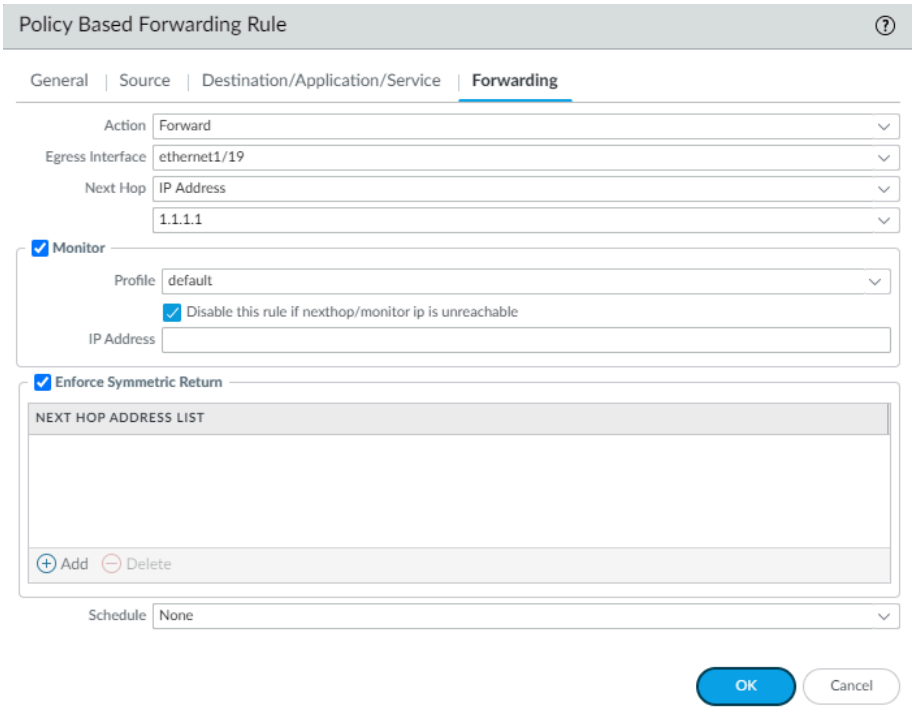
PBF を使用してすべてのトラフィックを転送するには、*[サービス]* を ***[any]*** に設定します。



STEP 4 | トラフィックの転送先を指定します。

1. **[転送]** タブで、トラフィックの転送先インターフェイスを指定して、パス モニタリングを有効にします。
2. トラフィックを転送するには、**Action (アクション)** を **Forward (転送)** に設定し、**Egress Interface (出力インターフェイス)** を選択して、**Next Hop (ネクストホップ)** を指定しま

す。この例では、出口インターフェースは ethernet1/19、ネクスト ホップ IPアドレスは 1.1.1.1 です（ネクスト ホップに FQDN は使用できません）。



3. **Monitor**（モニター）を有効にして、デフォルトのモニタリング プロファイルを関連付け、バックアップ ISP へのフェイルオーバーをトリガーします。この例では、モニターするターゲット IP アドレスを指定していません。ファイアウォールはネクスト ホップ IP アドレスをモニターします。ネクスト ホップ IP アドレスが到達不能な場合、ファイアウォールは、仮想ルーターに指定されたデフォルト ルートに向けてトラフィックを送信します。
4. （非対称ルートがある場合は必須）**Enforce Symmetric Return (**対称リターンの適用**)** を選択して、Trust ゾーンからインターネットへのリターン トラフィックが、インターネットからの入力トラフィックを受信したのと同じインターフェイスを介して外向きに転送されるようにします。
5. NAT を使用すると、インターネットからのトラフィックがファイアウォール上の正しいインターフェイス/IP アドレスに返されます。
6. **OK**をクリックして変更を保存します。

		Source			Destination				Forwarding			Monitoring		
	NAME	ZONE/INTERFACE	ADDRESS	USER	ADDRESS	APPLICATION	SERVICE	ACTION	EGRESS I/F	NEXT HOP	ENFORCE SYMMETRIC RETURN	PROFILE	TARGET	DISABLE IF UNR
1	pbf_rule_source_zone	Corporate	192.168.10.2	any	any	any	service-http service-https	forward	ethernet1/19	1.1.1.1	true	default	none	true

STEP 5 | 出力インターフェイスと ISP に基づいて NAT ルールを作成します。NAT ルールを使用すると、アウトバウンド接続時に正しい送信元 IP アドレスが使用されます。

1. **Policies (ポリシー)** > **NAT** の順に選択して **Add (追加)** をクリックします。
2. この例では、各 ISP について、以下の NAT ルールを作成します。

   プライマリ **ISP** の **NAT**

   [元のパケット] タブで、以下を選択します。

   Source Zone [送信元ゾーン]：企業

   Destination Zone [宛先ゾーン]：TwoISP

   [変換済みパケット] タブの [送信元アドレスの変換] で、以下を選択します。

   Translation Type [変換タイプ] :ダイナミック IP およびポート

   Address Type [アドレスタイプ] :インターフェイス アドレス

   Interface（インターフェース）: ethernet1/19

   IP Address [IPアドレス]：1.1.1.2/30

   バックアップ **ISP** の **NAT**

   [元のパケット] タブで、以下を選択します。

   Source Zone [送信元ゾーン]：企業

   Destination Zone [宛先ゾーン]：TwoISP

   [変換済みパケット] タブの [送信元アドレスの変換] で、以下を選択します。

   Translation Type [変換タイプ] :ダイナミック IP およびポート

   Address Type [アドレスタイプ] :インターフェイス アドレス

   Interface（インターフェース）: ethernet1/20

   IP Address [IPアドレス]：2.2.2.2/30

			Original Packet						Translated Packet	
	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSL
1	NAT for Primary ISP	none	Corporate	TwoISP	any	any	any	any	dynamic-ip-and-port ethernet1/19 1.1.1.2/30	none
2	NAT for Backup ISP	none	Corporate	TwoISP	any	any	any	any	dynamic-ip-and-port ethernet1/20 2.2.2.2/30	none

STEP 6 | インターネットへのアウトバウンド アクセスを許可するセキュリティ ポリシーを作成します。

アプリケーションを安全に有効化するには、インターネットへのアクセスを許可する簡単なルールを作成し、ファイアウォール上で利用可能なセキュリティ プロファイルを関連付けます。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択し、**Add**（追加）をクリックします。
2. **[全般]** タブで、ルールの分かりやすい **[名前]** を入力します。
3. **Source** (送信元) タブで**Source Zone** (送信元ゾーン) を Corporate に設定します。
4. **Destination**（宛先） タブで **Destination Zone**（宛先ゾーン） を TwoISP に設定します。
5. **[サービス/URL カテゴリ]** タブで、デフォルト値 **application-default** をそのまま使用します。
6. **Actions**（アクション）タブで以下の手順を実行します。
   1. **Action Setting**（アクション設定）を **Allow**（許可）に設定します。
   2. **Profile Setting** [プロファイル設定]で、Antiviru [アンチウイルス]、Anti-Spyware [アンチスパイウェア]、Vulnerability Protection [脆弱性防御]、URL Filtering [URL フィルタリング]のデフォルト プロファイルを関連付けます。
7. **[オプション]** で、セッション終了時のログが有効になっていることを確認します。セキュリティ ルールに一致するトラフィックのみログに記録されます。

	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1	Copr2ISP	none	universal	Corporate	any	any	any	TwoISP	any	any	any	any	Allow

STEP 7 | ファイアウォールで現在アクティブな設定に対するポリシーを保存します。

Commit（コミット）をクリックします。

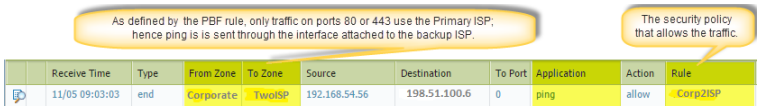
STEP 8 | PBF ルールがアクティブで、プライマリ ISP がインターネット アクセスに使用されていることを確認します。

1. Web ブラウザを起動して、Web サーバーにアクセスします。ファイアウォール上で、Web ブラウジング アクティビティのトラフィック ログをチェックします。
2. ネットワーク上のクライアントから、ping ユーティリティを使用して、インターネット上の Web サーバーとの接続を確認し、ファイアウォール上のトラフィック ログをチェックします。

```
C:\Users\pm-user1>ping 198.51.100.6 Pinging 198.51.100.6 with
 32 bytes of data:Reply from 198.51.100.6: bytes=32 time=34ms
 TTL=117 Reply from 198.51.100.6: bytes=32 time=13ms TTL=117
 Reply from 198.51.100.6: bytes=32 time=25ms TTL=117 Reply
 from 198.51.100.6: bytes=32 time=3ms TTL=117 Ping statistics
 for 198.51.100.6:Packets:Sent = 4, Received = 4, Lost = 0 (0%
```



```
loss), Approximate round trip times in milliseconds:Minimum =
3ms, Maximum = 34ms, Average = 18ms
```



3. 次の CLI コマンドを使用し、PBF ルールがアクティブであることを確認します。

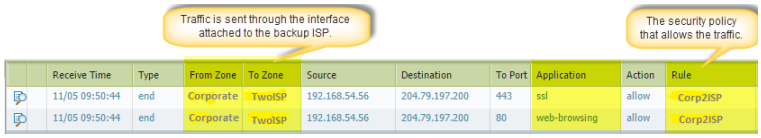
```
admin@PA-NGFW> show pbf rule all Rule ID Rule State Action Egress
 IF/VSYS NextHop ========== === ========== ====== ==============
 Use ISP-Pr 1 Active Forward ethernet1/1 1.1.1.1
```

STEP 9 | バックアップ ISP へのフェイルオーバーが発生すること、および送信元 NAT が正しく適用されていることを確認します。

1. プライマリ ISP との接続を切断します。
2. 次の CLI コマンドを使用し、PBF ルールがアクティブでないことを確認します。

```
admin@PA-NGFW> show pbf rule all Rule ID Rule State Action
 Egress IF/VSYS NextHop ========== ========== ======
 ============ ============ === Use ISP-Pr 1 Disabled Forward
 ethernet1/19 1.1.1.1
```

3. Web サーバーにアクセスし、トラフィック ログをチェックして、トラフィックがバックアップ ISP 経由で転送されていることを確認します。



4. セッションの詳細を表示して、NAT ルールが正しく機能していることを確認します。

```
admin@PA-NGFW> show session all
 ---------------------------------------------------------- ID
 Application State Type Flag Src[Sport]/Zone/Proto (translated
 IP[Port]) Vsys Dst[Dport]/Zone (translated IP[Port])
 ------------------------------------------------------------
 87212 ssl ACTIVE FLOW NS 192.168.54.56[53236]/Corporate/6
 (2.2.2.2[12896]) vsys1 204.79.197.200[443]/TwoISP
 (204.79.197.200[443])
```

5. 出力からセッション識別番号を取得して、セッションの詳細を表示します。

PBF ルールは使用されていないため、出力に表示されません。

```
admin@PA-NGFW> show session id 87212 Session 87212 c2s flow:
 source:192.168.54.56 [Corporate] dst:204.79.197.200 proto:6
 sport:53236 dport:443 state:ACTIVE type:FLOW src user:
 unknown dst user: unknown s2c flow: source:204.79.197.200
 [TwoISP] dst:2.2.2.2 proto:6 sport:443 dport:12896
```



```
 state:ACTIVE type:FKLOW src user: unknown dst user: unknown
 start time :Wed Nov5 11:16:10 2014 timeout :1800 sec time
 to live:1757 sec total byte count(c2s):1918 total byte
 count(s2c) :4333 layer7 packet count(c2s):10 layer7 packet
 count(s2c) :7 vsys : vsys1 application : ssl rule :Corp2ISP
 session to be logged at end:True session in session ager:True
 session synced from HA peer:False address/port translation :
 source nat-rule :NAT-Backup ISP(vsys1) layer 7 processing :
 enabled URL filtering enabled :True URL category : search-
engine session via syn-cookies :False session terminated on
 host :False session traverses tunnel :False authentication
 portal session :False ingress interface: ethernet1/2  egress:
 ethernet1/20 session QoS rule:N/A (class 4)
```

ポリシールールのテスト

実行中の設定でポリシールールをテストして、ビジネスニーズや要件に合わせて、ポリシーがトラフィックやアプリケーションやウェブサイトへのアクセスを適切に許可および拒否していることを確認します。ウェブインターフェイスから直接ファイアウォールのポリシーマッチテストを実行することで、ポリシールールが正しいトラフィックを許可および拒否していることをテストして確認できます。

STEP 1 | 「Web インターフェイスの起動」を行います。

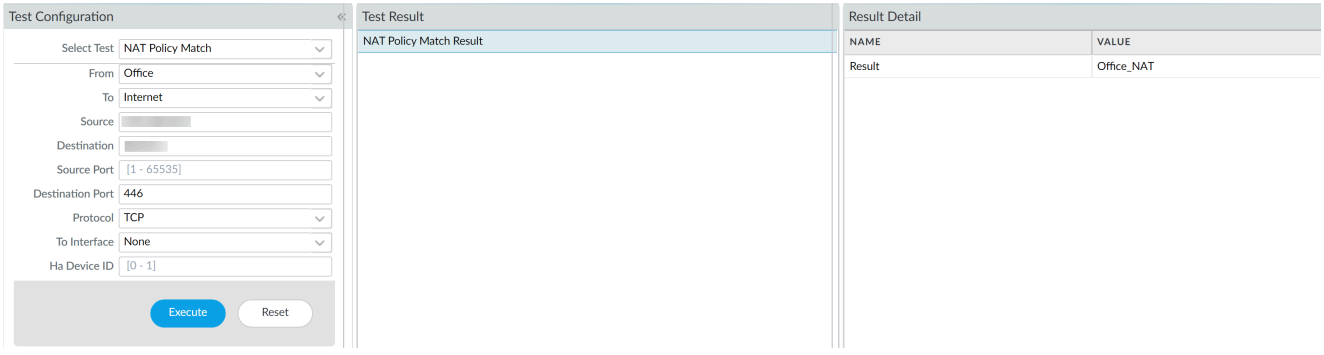
STEP 2 | ポリシーマッチまたは接続性テストを実行するには、**Device** > **Troubleshooting (デバイストラブルシューティング)** を選択します。

STEP 3 | ポリシーマッチテストを実行するために必要な情報を入力します。この例では、NAT ポリシーマッチテストを実行します。

1. **Select Test (テストの選択)**—**NAT** ポリシーマッチ を選択します。
2. **From (送信元)**—トラフィックが発信されているゾーンを選択します。
3. **To (送信先)**—トラフィックの宛先ゾーンを選択します。
4. **Source (送信元)**—トラフィックの送信元の IP アドレスを入力します。
5. **Destination (宛先)**—トラフィックの送信先デバイスの IP アドレスを入力します。
6. **Destination Port (宛先ポート)**—トラフィックに使用されるポートを入力します。このポートは、次の手順で使用される IP プロトコルによって異なります。
7. **Protocol (プロトコル)**—トラフィックに使用される IP プロトコルを入力します。
8. 必要に応じて、NAT ポリシールールのテストに関連する追加情報を入力してください。

STEP 4 | NAT ポリシーマッチテストを **Execute (実行)** します。

STEP 5 | テストポリシーと一致するポリシールールを確認するには、**NAT Policy Match Result (NAT ポリシーマッチ結果)** を確認してください。



仮想システム

このトピックでは、仮想システムとその利点、一般的なユース ケース、および仮想システムの設定方法について説明します。また、仮想システムを他の機能と併用する場合の説明が記載された、他のトピックへのリンクも含まれています。

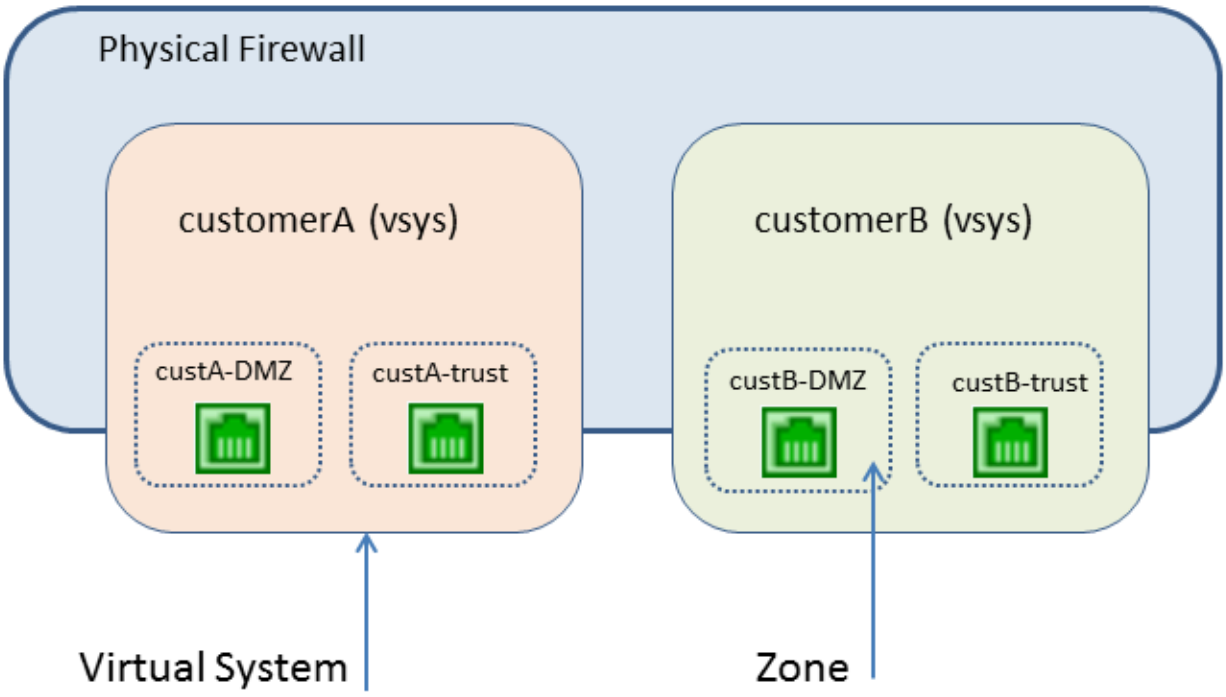
仮想システムの概要

仮想システムは、単一の物理 Palo Alto Networks ファイアウォール内に存在する別個の論理ファイアウォール インスタンスです。管理サービス プロバイダやエンタープライズは、複数のファイアウォールを使用するのではなく、（可用性を高めるために）ファイアウォールの 1 組のペアを使用し、それらのファイアウォールで仮想システムを有効にすることができます。各仮想システム（vsys）は、個別に管理される独立したファイアウォールで、そのトラフィックは他の仮想システムのトラフィックから分離された状態で維持されます。

- 仮想システムのコンポーネントとセグメンテーション
- 仮想システムの利点
- 仮想システムのユース ケース
- 仮想システムのプラットフォーム サポートおよびライセンス
- 仮想システムの管理ロール
- 仮想システムの共有オブジェクト

仮想システムのコンポーネントとセグメンテーション

仮想システムは、以下の図に示すように、管理上の境界を作成する 1 つのオブジェクトです。



仮想システムは、物理的および論理的な一連のインターフェイスとサブインターフェイス（VLAN やバーチャル ワイヤーなど）、仮想ルーター、およびセキュリティ ゾーンで構成されます。仮想システムごとに、デプロイメント モード（バーチャル ワイヤー、レイヤー 2、またはレイヤー 3 の任意の組み合わせ）を選択します。仮想システムを使用することにより、以下の処理をセグメント化することができます。

- 管理アクセス
- すべてのポリシーの管理 (セキュリティ、NAT、QoS、ポリシーベース フォワーディング、復号化、アプリケーション オーバーライド、トンネル検査、認証、および DoS プロテクション)
- すべてのオブジェクト (アドレス オブジェクト、アプリケーション グループとフィルタ、外部ダイナミック リスト、セキュリティ プロファイル、復号化プロファイル、カスタム オブジェクトなど)
- User-ID
- 証明書の管理
- サーバー プロファイル
- ロギング、レポート作成、および可視化機能

仮想システムはファイアウォールのセキュリティ機能に影響しますが、仮想システム単独で、スタティックおよびダイナミック ルーティングなどのネットワーク機能に影響を与えることはありません。以下のユース ケースのように、仮想システムごとに 1 つ以上の仮想ルーターを作成することにより、仮想システムごとにルーティングをセグメント化することができます。

- 1 つの組織の各部門に複数の仮想システムを設定しており、すべての部門のネットワーク トラフィックが共通のネットワーク内を通過する場合は、複数の仮想システム用に 1 つの仮想ルーターを作成することができます。
- ルーティング セグメンテーションを行い、各仮想システムのトラフィックを他の仮想システムから隔離する必要がある場合は、仮想システムごとに 1 つ以上の仮想ルーターを作成できます。
- すべてのマッピングが仮想システム間で共有されないようにユーザーマッピングをセグメント化したい場合は、User-ID ハブではない仮想システム上で User-ID ソースを構成できます。仮想システム間でのユーザー ID マッピングの共有を参照してください。

仮想システムの利点

仮想システムには、物理ファイアウォールと同じ基本的な機能を提供することのほかに、以下のような利点があります。

- セグメント化された管理 – さまざまな組織（または顧客や事業単位）が別個のファイアウォール インスタンスを制御（およびモニタリング）することができるため、同じ物理ファイアウォール上の別のファイアウォール インスタンスのトラフィックまたはポリシーと干渉することなく、その組織自体のトラフィックを制御することができます。
- 拡張性 – 物理ファイアウォールの設定後は、顧客または業務単位を効率よく追加または削除することができます。ISP、セキュリティ管理サービス プロバイダ、またはエンタープライズは、各顧客に異なるセキュリティ サービスを提供することができます。
- 設備投資と運用費の削減 – 仮想システムは 1 つのファイアウォール上に共存できるため、1 か所に複数のファイアウォールを設置する必要がありません。ファイアウォールを複数購入する必要がないため、組織では、ハードウェアの経費、電気代、およびラック スペースを節約することができ、メンテナンスと管理の費用を削減できます。
- **IP** アドレス対ユーザー名のマッピングを共有する機能–仮想システムを User-ID ハブとして割り当てることで、IP アドレス対ユーザー名のマッピングを複数の仮想システムで共有し、

ファイアウォールの User-ID 機能をフル活用してオペレーションの複雑さを軽減することができます。

仮想システムのユース ケース

仮想システムは、ネットワークにおいてさまざまな方法で使用できます。一般的なユース ケースの 1 つは ISP やセキュリティ管理サービス プロバイダ（MSSP）によるもので、1 つのファイアウォールで複数の顧客にサービスを提供します。顧客は、簡単に無効または有効にすることが可能な数多くのサービスの中から、サービスを選択することができます。ファイアウォールのロールベース管理により、ISP や MSSP では、ロギングやレポート作成などの機能への各顧客のアクセスを制御しつつ、他の機能を非表示、あるいは読み取り専用にできます。

別の一般的なユース ケースは、技術的な要件や機密保持の要件が異なるために複数の部門間で別々のファイアウォール インスタンスが必要とされる、大規模なエンタープライズの場合です。上のケース同様、さまざまなグループに異なるレベルのアクセス権を付与しつつ、IT 部門ではファイアウォール自体を管理します。サービスを部門まで遡って追跡または請求することができるため、1 つの組織内で別々に財務処理を行うことができます。

仮想システムのプラットフォーム サポートおよびライセンス

仮想システムは、PA-3200 Series、PA-3400 Series、PA-5200 Series、PA-5400 Series、およびPA-7000 Series ファイアウォールでサポートされています。ファイアウォールのそれぞれのシリーズは基本数の仮想システムをサポートしており、その数はプラットフォームによって異なります。PA-3200 Series および PA-3400 Series ファイアウォールで複数の仮想システムをサポートし、プラットフォームでサポートされる仮想システムの基本数を超えるものを作成するには、Virtual Systems ライセンスが必要です。

ライセンス情報については、「サブスクリプション」を参照してください。サポートされる仮想システムの基本数と最大数の詳細は、Compare Firewalls（英語）ツールを参照してください。

複数の仮想システムは、PA-220、PA-400 Series、PA-800 Series、またはVM-Series ファイアウォールではサポートされていません。

デフォルトは ***vsys1*** です。*vsys1* はファイアウォールの内部階層に関連しているため、削除できません。*vsys1* は、複数の*virtual system* (仮想システム - *vsys*)をサポートしていないファイアウォール モデルでも表示されます。

仮想システムで許可されているセッション、ルール、および VPN トンネルへの リソース割り当てを制限 して、ファイアウォールリソースを制御できます。各リソース設定には、ファイアウォールモデルごとに異なる値の有効範囲が表示されます。デフォルト設定は 0 です。これは、仮想システムの制限がファイアウォールモデルの制限であることを意味します。ただし、特定の設定に関する制限は各仮想システムには反映されません。例えば、ファイアウォールに 4 つの仮想システムがある場合、各仮想システムには、ファイアウォールごとに許可されている復号化ルールの総数を設定することはできません。すべての仮想システムの復号化ルールの総数がファイアウォールの制限に達すると、それ以上追加することはできません。

仮想システムの管理ロール

Superuser (スーパーユーザー) 管理者は、仮想システムを作成し、**Device administrator (デバイスの管理者)**、**vsysadmin**、または **vsysreader** を追加することができます。**Device administrator (デバイスの管理者)** は、すべての仮想システムにアクセスできますが、管理者を追加することはできません。管理者ロール プロファイルを作成して **Virtual System (仮想システム)** にするロールを選択する際、ロールはファイアウォール上の特定の仮想システムに適用されます。**Command Line (コマンドライン)** タブの 2 つの仮想システム管理者ロールは：

- **vsysadmin**—選択されたファイアウォールの仮想システムにアクセスでき、仮想システムの特定の要素を作成・管理します。vsysadmin はネットワークインターフェイス、VLAN、バーチャル ワイヤ、仮想ルーター、IPSec トンネル、GRE トンネル、DHCP、DNS プロキシ、QoS、LLDP やネットワーク プロファイルにアクセスできません。vsysadmin 権限を持つユーザーは、自分に割り当てられている仮想システムについてのみ、その設定をコミットすることができます。
- **vsysreader**—選択されたファイアウォールの仮想システムおよび仮想システムの特定の要素に対する読み取り専用のアクセスが可能です。vsysreader はネットワークインターフェイス、VLAN、バーチャル ワイヤ、仮想ルーター、IPSec トンネル、GRE トンネル、DHCP、DNS プロキシ、QoS、LLDP やネットワーク プロファイルにアクセスできません。

仮想システム管理者は、管理者に割り当てられている仮想システムについてのみ、そのログを表示できます。**Superuser (スーパーユーザー)** あるいは **Device administrator (デバイス管理者)** は、すべてのログを閲覧したり、仮想システムを選択して表示したり、仮想システムを User-ID ハブとして設定したりすることができます。

仮想システムの共有オブジェクト

管理者アカウントが複数の仮想システムを包含する場合は、特定の仮想システムのオブジェクト（アドレス オブジェクトなど）およびポリシーを共有オブジェクトとして設定することを選択できます。共有オブジェクトは、ファイアウォール上の仮想システムすべてに適用されます。仮想システムで、既存のオブジェクトと同じ名前およびタイプの共有オブジェクトを作成しようとすると、その仮想システム オブジェクトが使用されます。

仮想システム間の通信

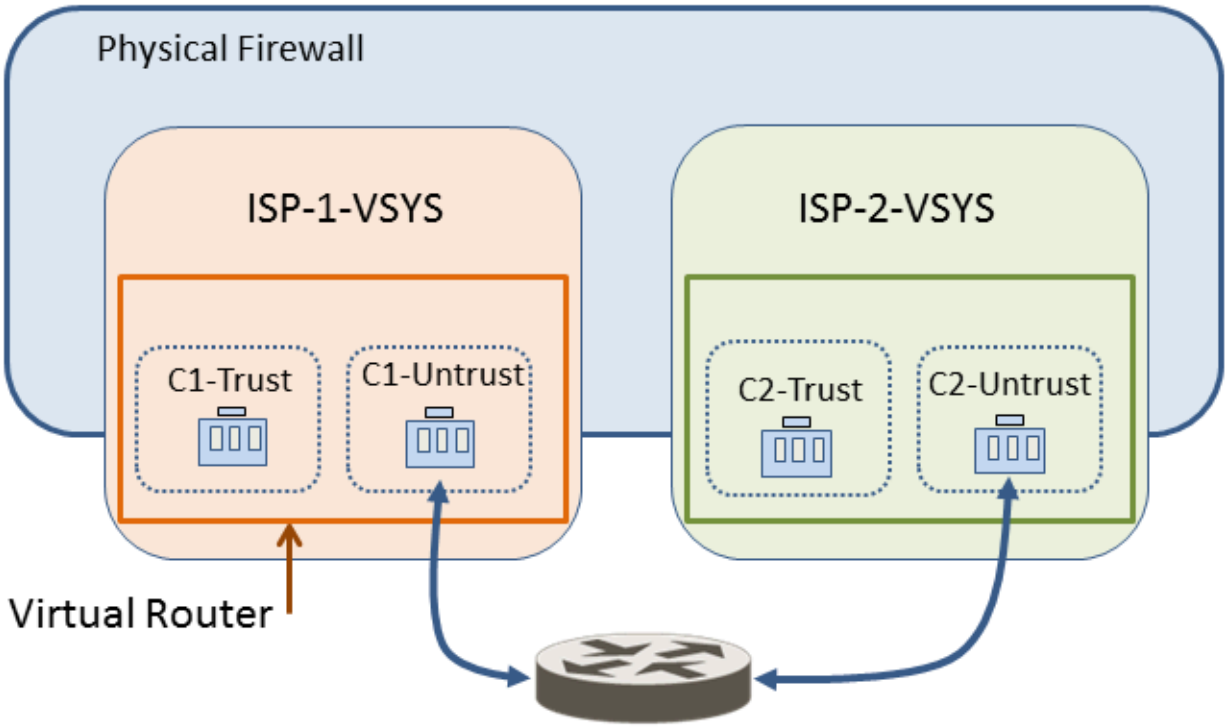
仮想システム間の通信（vsys 間トラフィック）が望ましいとされる一般的なシナリオは 2 つあります。まずマルチテナンシー環境では、トラフィックがファイアウォールから離れ、インターネットを通過し、再びファイアウォールに戻ってくることによって、仮想システム間の通信が発生します。単一組織の環境では、ファイアウォール内で仮想システム間の通信が行われます。このセクションでは、両方のシナリオについて説明します。

- ファイアウォールから離れる必要がある vsys 間トラフィック
- ファイアウォール内に残る vsys 間トラフィック
- vsys 間通信で使用する 2 つのセッション

ファイアウォールから離れる必要がある vsys 間トラフィック

1 つのファイアウォール上で複数の顧客にサービスを提供する（マルチテナンシー） ISP は、顧客ごとに 1 つの仮想システムを使用し、それにより各顧客がその仮想システム設定を制御できるようにすることができます。この場合 ISP は、**vsysadmin** 権限を顧客に付与します。各顧客のトラフィックおよび管理は、他の顧客から分離されます。各仮想システムは、トラフィックおよびシステム専用のインターネット接続を管理するため、固有の IP アドレスと 1 つ以上の仮想ルーターを指定して設定する必要があります。

仮想システムが相互に通信する必要がある場合、そのトラフィックは、仮想システムが以下の図のように同じ物理ファイアウォール上に存在するとしても、ファイアウォールから出て別のレイヤー 3 ルーティング デバイスに向かい、再びファイアウォールに戻ります。



ファイアウォール内に残る vsys 間トラフィック

上記のマルチテナンシーのシナリオとは異なり、1 つのファイアウォール上に設定されているすべての仮想システムは、1 つの組織の制御下に置くことができます。組織では、仮想システム間のトラフィックを隔離すると同時に、仮想システム間の通信を許可する必要があります。このような一般的なユース ケースは、組織において、部門間を分離しつつ、各部門が相互に通信したり、同じネットワークに接続したりできるようにする場合に当てはまります。このシナリオでは、以下のトピックで説明するように、vsys 間通信がファイアウォール内で行われます。

- 外部ゾーン
- ファイアウォール内のトラフィック用の外部ゾーンとセキュリティ ポリシー

外部ゾーン

上記のユース ケースにおいて適切な通信は、外部ゾーンを指し示すか、または外部ゾーンから指し示されるセキュリティ ポリシーを設定することによって実現できます。外部ゾーンは、到達可能な特定の仮想システムに関連付けられるセキュリティ オブジェクトで、その仮想システムの外部に存在します。1 つの仮想システムには、その仮想システム内に存在するセキュリティ ゾーンの数に関係なく、外部ゾーンを 1 つだけ関連付けることができます。外部ゾーンは、別々の仮想システム内のゾーン間におけるトラフィックを許可し、トラフィックがファイアウォールを離れないようにするために必要です。

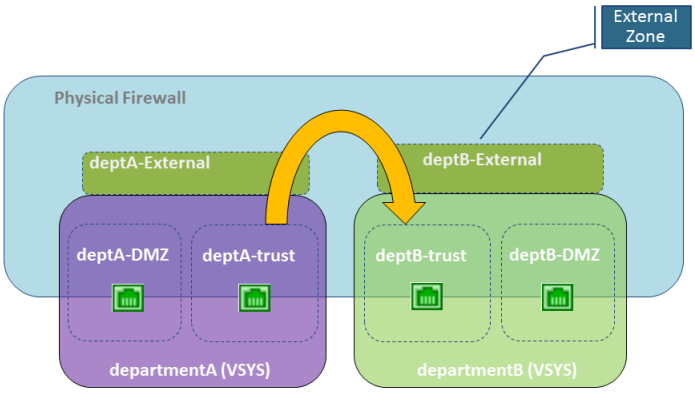
仮想システム管理者は、2 つの仮想システム間のトラフィックを許可するために必要なセキュリティ ポリシーを設定します。セキュリティ ゾーンとは異なり、外部ゾーンはインターフェイスとは関連付けられず、仮想システムと関連付けられます。セキュリティ ポリシーにより、セキュリティ（内部）ゾーンと外部ゾーンの間のトラフィックを許可または拒否します。

外部ゾーンでは、それに関連付けられているインターフェイスまたは IP アドレスが存在しないため、一部のゾーン プロテクション プロファイルがサポートされません。

各仮想システムは 1 つのファイアウォールの別々のインスタンスであるため、仮想システム間を移動する各パケットは、セキュリティ ポリシーと App-ID 評価に基づいて検査されます。

ファイアウォール内のトラフィック用の外部ゾーンとセキュリティ ポリシー

以下の例において、エンタープライズには、departmentA および departmentB 仮想システムという 2 つの別個の管理グループがあります。以下の図は、各仮想システムに関連付けられている外部ゾーンを示しています。図では、1 つの Trust ゾーンからのトラフィック フローが外部ゾーンから出て、別の仮想システムの外部ゾーンに入り、さらにその仮想システムの Trust ゾーンに入っています。



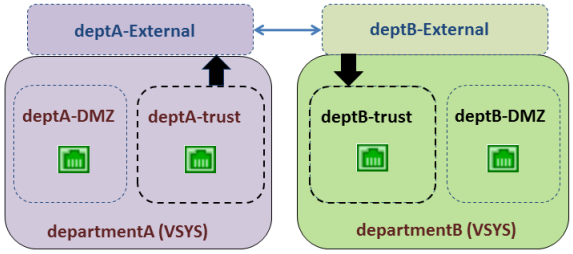
外部ゾーンを作成するため、ファイアウォール管理者は、相互に認識できるように仮想システムを設定する必要があります。外部ゾーンの仮想システムは相互に存在を認識することができるため、外部ゾーン間のセキュリティ ポリシーはありません。

仮想システム間の通信のため、ファイアウォール上の入力および出力インターフェイスは、単一の仮想ルーターに割り当てられるか、または仮想ルーター間スタティック ルートを使用して接続されます。これら 2 つのアプローチのうちで簡単なのは、相互に通信する必要があるすべての仮想システムを 1 つの仮想ルーターに割り当てるアプローチのほうです。

仮想システムにそれ専用の仮想ルーターを指定する必要があるのは、たとえば、仮想システムで使用する IP アドレス範囲が重複していることがあるためです。トラフィックは仮想システム間でルーティング可能ですが、各仮想ルーターには、ネクスト ホップとして他の仮想ルーターを指し示すスタティック ルートを指定しておく必要があります。

上の図のシナリオの場合であれば、エンタープライズには、departmentA および departmentB という 2 つの管理グループがあります。departmentA グループは、ローカル ネットワークと DMZ リソースを管理します。departmentB グループは、ネットワークの営業セグメントを出入りするトラフィックを管理します。すべてのトラフィックが 1 つのローカル ネットワーク上に存在するため、1 つの仮想ルーターを使用しています。2 つの仮想システム間の通信のために、2 つの外部ゾーンが設定されています。departmentA 仮想システムには、セキュリティ ポリシーで使用される、deptA-DMZ、deptA-trust、および deptA-External の 3 つのゾーンがあります。departmentB の仮想システムにも、deptB-DMZ、deptB-trust、および deptB-External の 3 つのゾーンがあります。両方のグループが、それぞれの仮想システムを通過するトラフィックを制御できます。

deptA-trust から deptB-trust へのトラフィックを許可するため、2 つのセキュリティ ポリシーが必要です。以下の図において、2 つの垂直矢印は、セキュリティ ポリシー（図の下で説明）によってトラフィックを制御している場所を示しています。



- セキュリティ ポリシー 1:上の図において、トラフィックが向かう先は deptB-trust ゾーンです。トラフィックは deptA-trust ゾーンを離れ、deptA-External ゾーンに入ります。セキュリティ ポリシーでは、送信元ゾーン（deptA-trust）から宛先ゾーン（deptA-External）へのトラフィックを許可する必要があります。仮想システムでは、このトラフィックの場合に、NAT を含むすべてのポリシー タイプを使用できます。

  外部ゾーンに送信されるトラフィックは、元の外部ゾーンで認識可能な他の外部ゾーンで認識され、自動的にアクセスできるため、外部ゾーン間にポリシーは必要ありません。
- Security Policy（セキュリティ ポリシー）2：上の図において、deptB-External からのトラフィックはさらに deptB-trust ゾーンに向かいます。セキュリティ ポリシーは、それを許可するように設定する必要があります。そのポリシーでは、送信元ゾーン（deptB-External）から宛先ゾーン（deptB-trust）へのトラフィックを許可する必要があります。

departmentB 仮想システムを departmentA 仮想システムからのトラフィックをブロックするように設定したり、その逆の設定をしたりすることが可能です。他のゾーンから出力されるトラフィックの場合と同様、外部ゾーンから出力されるトラフィックが仮想システム内の他のゾーンに到達するには、ポリシーで明示的に許可されている必要があります。

ファイアウォールから離れない仮想システム間のトラフィックで必要とされる外部ゾーンに加えて、トラフィックがファイアウォールを離れることになる共通ゲートウェイを設定する場合にも、外部ゾーンが必要とされます。

vsys 間通信で使用する 2 つのセッション

1 つの仮想システムの場合にセッションが 1 つ使用されるのとは異なり、2 つの仮想システム間の通信では、2 つのセッションが使用されることを理解しておく必要があります。シナリオを比較してみましょう。

シナリオ 1 – vsys1 には、trust1 と untrust1 の 2 つのゾーンがあります。trust1 ゾーンのホストは、untrust1 ゾーンのデバイスとの通信が必要になると、トラフィックを開始します。ホストはファイアウォールにトラフィックを送信し、そのファイアウォールは、送信元ゾーン trust1 から宛先ゾーン untrust1 への新しいセッションを作成します。このトラフィックに必要なセッションは 1 つだけです。

シナリオ 2 – vsys1 からのホストが vsys2 上のサーバーにアクセスする必要があります。trust1 ゾーンのホストはファイアウォールへのトラフィックを開始し、そのファイアウォールは、送信元ゾーン trust1 から宛先ゾーン untrust1 への最初のセッションを作成します。トラフィックは、内部で、または外部を介して、vsys2 にルーティングされます。次にファイアウォールは、送信元ゾーン untrust2 から宛先ゾーン trust2 への 2 番目のセッションを作成します。この vsys 間トラフィックでは、2 つのセッションが必要です。

共有ゲートウェイ

このトピックには、共有ゲートウェイに関する以下の情報が含まれています。

- 外部ゾーンと共有ゲートウェイ
- 共有ゲートウェイでのネットワーキングに関する考慮事項

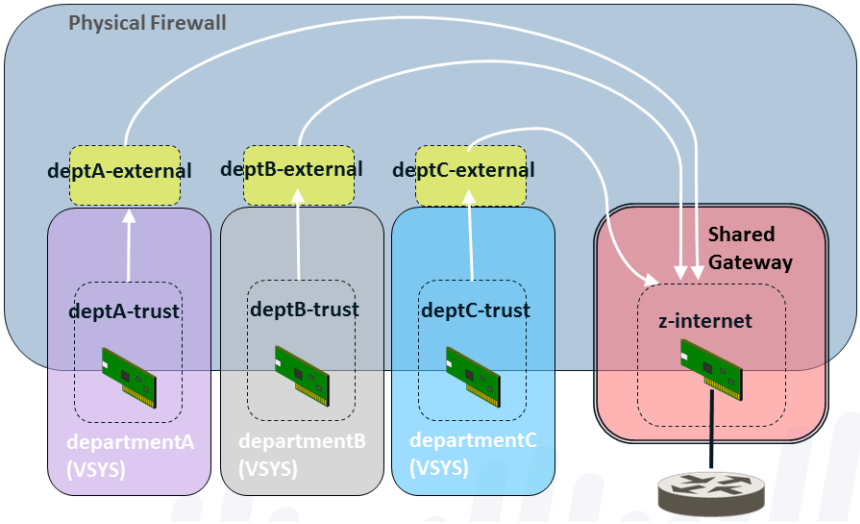
外部ゾーンと共有ゲートウェイ

共有ゲートウェイは、インターネットを介して通信するために複数の仮想システムが共有するインターフェイスです。各仮想システムには、仮想システムの内部ゾーンから共有ゲートウェイへのトラフィックを許可または拒否するセキュリティー・ポリシーを構成するための仲介者として機能する外部ゾーンーが必要です。

共有ゲートウェイは、1 つの仮想ルーターを使用してすべての仮想システムのトラフィックをルーティングします。共有ゲートウェイは、インターフェイスがその周辺で完全な管理の境界を必要としない場合、または複数の仮想システムで 1 つのインターネット接続を共有する必要がある場合に使用されます。この 2 番目のケースは、ISP から組織に提供された IP アドレス（インターフェイス）が 1 つしかないときに、複数の仮想システムが外部通信を必要とする場合に発生します。

仮想システム間での動作とは異なり、セキュリティ ポリシーと App-ID の評価は、仮想システムと共有ゲートウェイの間では実行されません。そのため、共有ゲートウェイを使用してインターネットにアクセスする場合は、別の仮想システムを作成してアクセスする場合よりも負担が少なくて済みます。

以下の図では 3 件の顧客がファイアウォールを共有していますが、インターネットにアクセス可能なインターフェイスは 1 つしかありません。別の仮想システムを作成すると、追加した仮想システム経由でインターネットに送信されるトラフィックについて、App-ID およびセキュリティ ポリシーの評価の負担が増加します。別の仮想システムを追加しないで済ませるには、以下の図に示すように、共有ゲートウェイを設定します。



共有ゲートウェイには、外部との通信に使用されるグローバルにルーティング可能な IP アドレスが 1 つ割り当てられています。仮想システム内のインターフェイスにも IP アドレスが割り当てられていますが、それらはプライベート IP アドレスであり、ルーティング可能ではありません。

管理者は、任意の仮想システムが、他の仮想システムによって認識されるかどうかを指定する必要があります。仮想システムとは異なり、共有ゲートウェイは、ファイアウォール上のすべての仮想システムによって常に認識されます。

共有ゲートウェイ ID 番号は、Web インターフェイスに **sg<ID>** と表示されます。共有ゲートウェイには、その ID 番号を含めた名前を付けることをお勧めします。

共有ゲートウェイにゾーンやインターフェイスなどのオブジェクトを追加すると、その共有ゲートウェイは、選択可能な仮想システムとして vsys メニューに表示されます。

共有ゲートウェイは、仮想システムの限定バージョンです。NAT およびポリシーベース フォワーディング（PBF）をサポートしますが、セキュリティ、DoS ポリシー、QoS、復号、アプリケーション オーバーライド、または認証ポリシーはサポートしません。

共有ゲートウェイでのネットワーキングに関する考慮事項

共有ゲートウェイの設定時には、以下の点を考慮してください。

- 共有ゲートウェイのシナリオにおける仮想システムは、1 つの IP アドレスを使用して、共有ゲートウェイの物理インターフェイスを介してインターネットにアクセスします。仮想システムの IP アドレスをグローバルにルーティングできない場合は、送信元 NAT を設定して、それらのアドレスをグローバルにルーティング可能な IP アドレスに変換します。
- 仮想ルーターは、すべての仮想システムのトラフィックを、共有ゲートウェイを介してルーティングします。
- 仮想システムのデフォルト ルートは、共有ゲートウェイを指し示すようにする必要があります。
- 内部ゾーンと外部ゾーンの間のトラフィックを許可するには、共有ゲートウェイで認識可能な仮想システムごとにセキュリティ ポリシーを設定する必要があります。
- ファイアウォール管理者が仮想ルーターを制御し、仮想システムのメンバーが他の仮想システムのトラフィックに影響を与えることのないようにします。
- Palo Alto Networks のファイアウォール内では、仮想システムから別の仮想システム、または共有ゲートウェイに、パケットがホップする可能性があります。3 つ以上の仮想システムまたは共有ゲートウェイにかけてパケットが横断することはありません。例えば、パケットは、vsys1 から vsys2、vsys3、または同様に vsys1 から vsys2、共有ゲートウェイ 1 には送信できません。どちらの例も 2 つ以上の仮想システムを含みますが、許可されていません。

設定の時間と手間を省くため、共通ゲートウェイの以下の利点を考慮してください。

- 1 つの共有ゲートウェイに関連付けられている複数の仮想システムで NAT を設定するのではなく、その共有ゲートウェイで NAT を設定することができます。
- 1 つの共有ゲートウェイに関連付けられている複数の仮想システムでポリシーベース ルーティング（PBR）を設定するのではなく、その共有ゲートウェイで PBR を設定することができます。

仮想システムの設定

仮想システムを作成するには、以下が必要です。

- スーパーユーザー 管理ロール。
- インターフェイスが設定されている。
- 仮想システム ライセンス（プラットフォームでサポートされている基本数より多くの仮想システムを作成する場合）。仮想システムのプラットフォーム サポートおよびライセンスを参照してください。

STEP 1 | 仮想システムを有効にします。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Management (管理)** を選択して **General Settings (一般設定)** を編集します。
2. **[マルチ仮想システム機能]** チェックボックスをオンにして、**[OK]** をクリックします。承認すると、このアクションによってコミットがトリガーされます。

   仮想システムを有効にした場合のみ、**Device (デバイス)** タブに **Virtual Systems (仮想システム)** オプションと **Shared Gateways (共有ゲートウェイ)** オプションが表示されます。

STEP 2 | 仮想システムを作成します。

1. **Device (デバイス)** > **Virtual Systems (仮想システム)** の順に選択して、**Add (追加)** をクリックし、「vsys」に付加される仮想システムの **ID**（範囲は 1 ～ 255）を入力します。

   デフォルトは ***vsys1*** です。*vsys1* はファイアウォールの内部階層に関連しているため、削除できません。*vsys1* は、複数の*virtual system (* 仮想システム - *vsys)*をサポートしていないファイアウォール モデルでも表示されます。
2. 復号化されたコンテンツをファイアウォールから外部のサービスに転送できるようにする場合は、**Allow forwarding of decrypted content (復号化されたコンテンツの転送を許可)** を選択します。たとえば、ファイアウォールから WildFire に復号化されたコンテンツを送信して分析できるようにするには、このオプションを有効にする必要があります。
3. 仮想システムの分かりやすい **[名前]** を入力します。合計で最大 31 文字の英数字、スペース、アンダースコアを使用できます。

STEP 3 | 仮想システムにインターフェイスを割り当てます。

仮想ルーター、バーチャル ワイヤ、または VLAN は、すでに設定されているか、または後で設定するかのどちらかです。後で設定する場合は、その時点で、それぞれに関連付ける仮想システムを指定します。

1. DNS プロキシ ルールをインターフェイスに適用する場合は、**General** （全般） タブで **DNS Proxy (DNS プロキシ)** オブジェクトを選択します。
2. **[インターフェイス]** フィールドで **[追加]** をクリックし、仮想システムに割り当てるインターフェイスまたはサブインターフェイスを入力します。インターフェイスは、1 つの仮想ルーターにのみ属することができます。
3. その仮想システムで必要なデプロイメント タイプに基づいて、以下のいずれかの操作を行います。
   - **Add** に **VLAN** を vsys に割り当てます。
   - **Add** を **Virtual Wires** から vsys に割り当てる。
   - **Add** を **Virtual Routers** に vsys に割り当てます。
   - ファイアウォールで **Advanced Routing** が有効になっている場合、**Add** は **Logical Routers** を vsys に割り当てます。
4. **Visible Virtual System (認識可能な仮想システム)** フィールドで、設定中の仮想システムで認識できるようにする仮想システムをすべて選択します。これは、相互に通信する必要がある仮想システムにおいて必要な操作です。

   管理境界を厳密に設定する必要があるマルチテナンシー シナリオの場合、選択する仮想システムはありません。
5. **OK** をクリックします。

STEP 4 | (パノラマ管理の firewalls に必須) パノラマ Web インターフェイスにログイン を選択し、**Commit** > **Push to Devices** を選択し、パノラマ管理された設定全体をマルチ vsys firewall の各 vsys にプッシュします。

これは、Panorama によって管理される複数 vsys firewalls の共有構成オブジェクトを利用するために必要です。

STEP 5 | （任意）仮想システムで許可される、セッション、ルール、および VPN トンネルのリソース割り当てを制限します。仮想システムあたりの割り当てを柔軟に制限できるため、ファイアウォールのリソースを効率よく制御することができます。

1. **[リソース]** タブで、仮想システムの制限を必要に応じて設定します。各フィールドには、ファイアウォールモデルごとに異なる有効な範囲の値が表示されます。デフォルト設定は 0 です。これは、仮想システムの制限がファイアウォールモデルの制限であることを意味します。ただし、特定の設定に関する制限は各仮想システムには反映されません。例えば、ファイアウォールに 4 つの仮想システムがある場合、各仮想システムには、ファイアウォールごとに許可されている復号化ルールの総数を設定することはで

きません。すべての仮想システムの復号化ルールの総数がファイアウォールの制限に達すると、それ以上追加することはできません。

- セッション制限

  show session meter CLI コマンドを使用すると、データ プレーンごとに許可される最大セッション数、仮想システムで使用されている現在のセッション数、および仮想システムあたりのセッション数が表示されます。*PA-5200* あるいは *PA-7000 Series* ファイアウォールでは、仮想システム毎に複数のデータプレーンがあるため、使用中のセッションの現在の数が、セッションの制限値として設定されている数よりも大きくなる場合があります。*PA-5200* シリーズまたは *PA-7000* シリーズのファイアウォールで設定する セッション制限は、データプレーンあたりであり、仮想システムごとに最大値が高くなります。

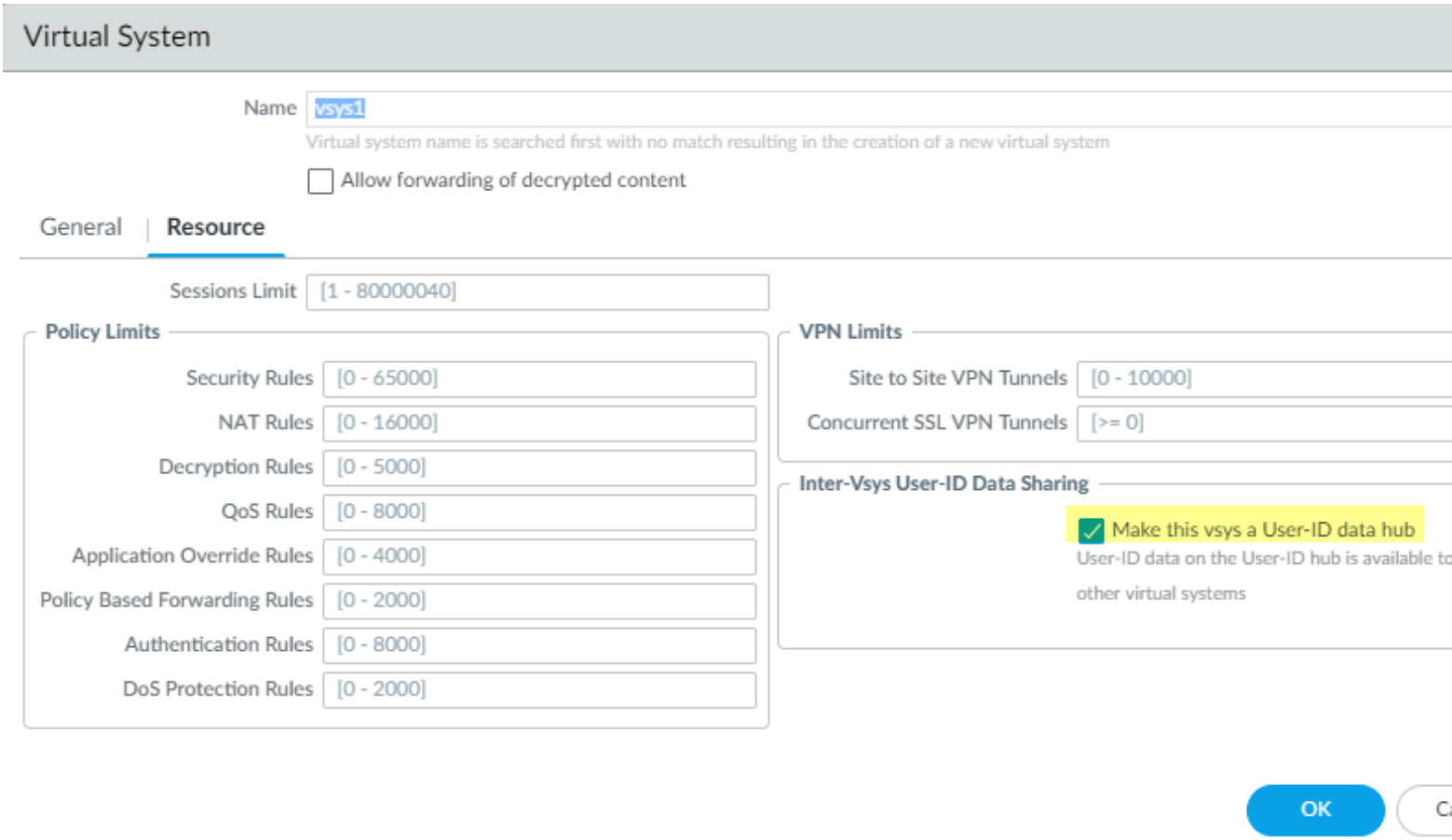
- セキュリティルール数
- **NAT**ルール
- 復号ルール
- **QoS** ルール
- アプリケーション オーバーライド ルール
- ポリシー ベース フォワーディング ルール
- 認証ルール
- **DoS** プロテクション ルール
- サイト間 **VPN** トンネル
- 同時 **SSL VPN** トンネル

2. **OK** をクリックします。

STEP 6 | (Optional)仮想システムを User-ID ハブとして構成し、仮想システム間でのユーザー ID マッピングの共有します。

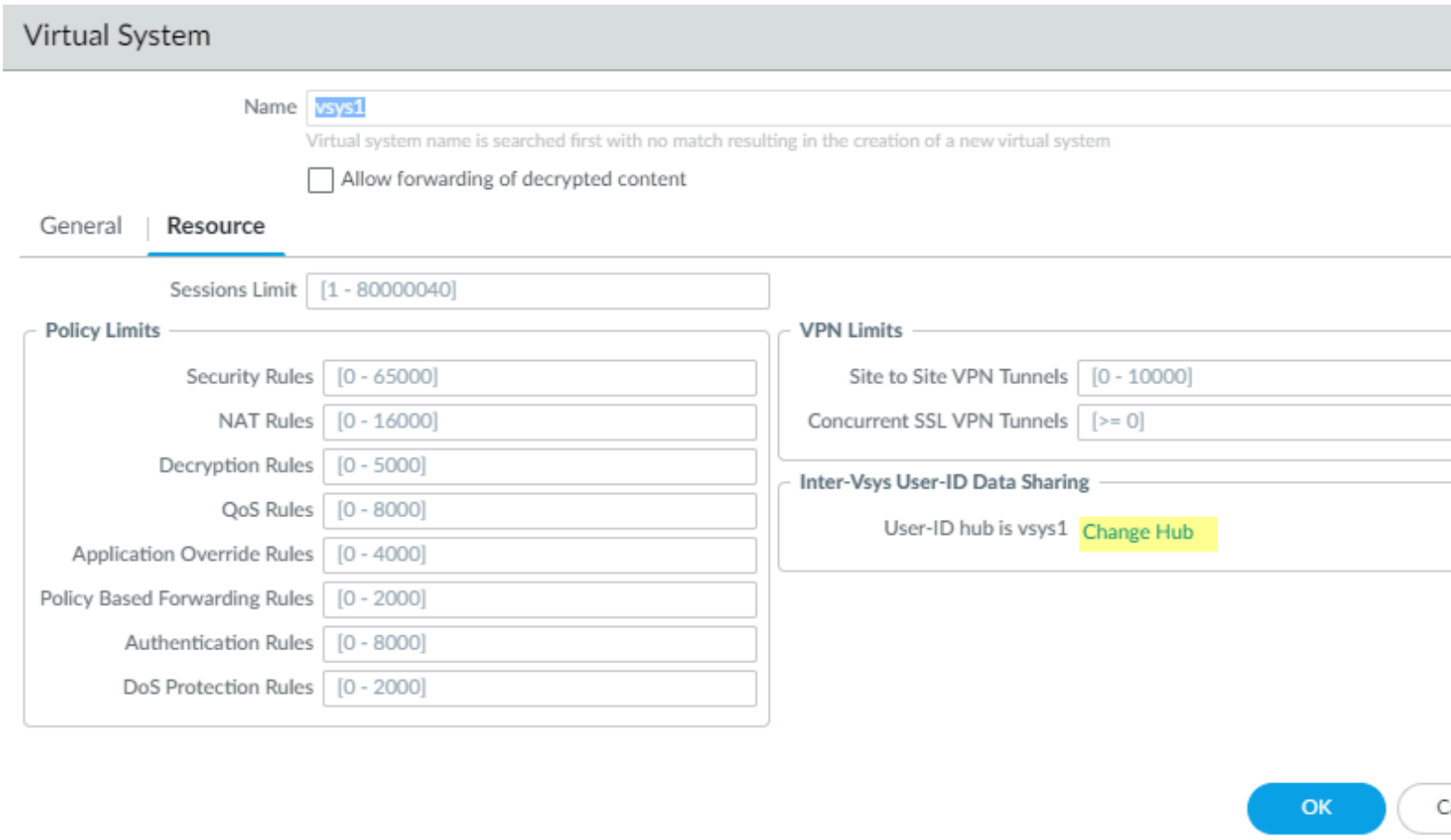
Terminal Server エージェントからの *Ip-address-and-port-to-username* マッピング情報とグループマッピングデータは、仮想システムハブと接続された仮想システム間で共有されません。

1. 既存の仮想システムの場合、共有するユーザー ID ソース (監視対象サーバーやユーザー ID エージェントなど) の構成を、ハブとして使用する仮想システムに転送します。
2. **Resource (リソース)** タブで、**Make this vsys a User-ID data hub (この vsys をユーザー ID データハブにする)** を選択します。

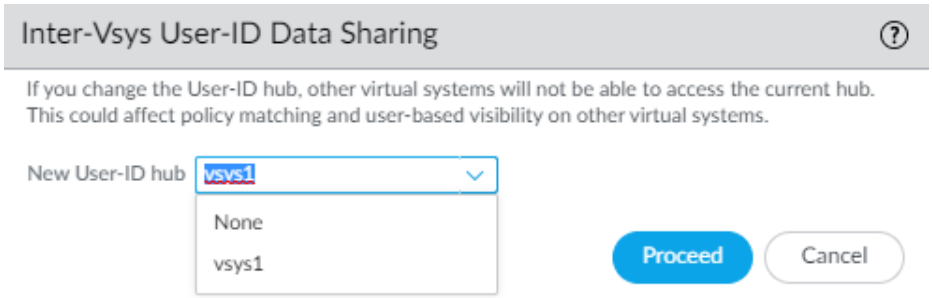


3. **Yes (はい)** をクリックして確認してから、**OK** をクリックします。

   User-ID ハブを別の仮想システムに変更するか無効にする場合は、現在 User-ID ハブとして構成されている仮想システムを選択してから、**Resource (リソース)** > **Change Hub (ハブの変更)** を選択します。



リストから **New User-ID** ハブ を選択するか、**none** を選択して User-ID ハブを無効にし、仮想システム間でのマッピングの共有を停止します。



Proceed をクリックして、変更を確認してコミットします。

STEP 7 | 設定をコミットします。

Commit（コミット）をクリックします。これで仮想システムは、**[Objects]** タブからアクセス可能なオブジェクトになります。

STEP 8 | 仮想システムでスタティックおよびダイナミック ルーティングなどのネットワーク機能を使用できるようにするため、その仮想システム用に少なくとも 1 つの仮想ルーターを作成します。

あるいは、デプロイメントに応じて、仮想システムで VLAN またはバーチャル ワイヤーを使用することもできます。

1. **Network (ネットワーク)** > **Virtual Routers (仮想ルーター)** の順に選択し、**Name (名前)** を入力して仮想ルーターを **Add (追加)** します。
2. **Interfaces (インターフェイス)** で、**Add (追加)** をクリックし、仮想ルーターに属するインターフェイスを選択します。
3. **OK** をクリックします。

STEP 9 | 仮想システムのインターフェイスごとにセキュリティ ゾーンを設定します。

少なくとも 1 つのインターフェイスについて、1 つのレイヤー 3 セキュリティ ゾーンを作成します。「インターフェイスとゾーンの設定」を参照してください。

STEP 10 | 仮想システムの各ゾーンとの間のトラフィックを許可または拒否するセキュリティ ポリシールールを設定します。

セキュリティ ポリシー ルールの作成を参照してください。

STEP 11 | 設定をコミットします。

Commit（コミット）をクリックします。

仮想システムを作成した後、*CLI* を使用して特定の仮想システムについてのみ設定をコミットすることができます。

部分的な **vsys *<vsys-id>*** をコミットする

STEP 12 | （任意）仮想システムに設定されているセキュリティ ポリシーを表示します。

CLI を使用する SSH セッションを開きます。仮想システムのセキュリティ ポリシーを表示するには、操作モードで以下のコマンドを使用します。

```
set system setting target-vsys <vsys-id>
show running security-policy
```


ファイアウォール内での仮想システム間通信の設定

このタスクを行うのは、たとえば単一の企業内において、ファイアウォール内の各仮想システムが相互に通信できるようにするユース ケースの場合です。そのようなケースはファイアウォール内に残る vsys 間トラフィックに記載されています。このタスクでは、以下を想定しています。

- 仮想システムの設定を行うタスクが完了しました。
- 仮想システムの設定時に、**Visible Virtual System (**認識可能な仮想システム**)** フィールドで、相互通信のために相互に認識可能にする必要があるすべての仮想システムのチェック ボックスをオンにしている。

STEP 1 | 仮想システムごとに外部ゾーンを設定します。

1. **Network (**ネットワーク**)** > **Zones (**ゾーン**)** を選択し、**Name (**名前**)** で新しいゾーンを **Add (**追加**)** します。
2. **[**場所**]** として、作成する外部ゾーンの対象仮想システムを選択します。
3. **[**タイプ**]** として、**[**外部**]** を選択します。
4. **Virtual Systems** [仮想システム]で **Add** [追加]をクリックし、外部ゾーンが到達可能な仮想システムを入力します。
5. （任意）フラッド、偵察行為、パケット ベースの攻撃防御を提供する **Zone Protection Profile (**ゾーン プロテクション プロファイル**)**を選択（あるいは後で設定）します。
6. （任意）必要に応じて、**Log Setting (**ログ設定**)** でゾーン プロテクション ログを外部システムに転送するためのログ転送プロファイルを選択します。
7. （任意）**Enable User Identification (**ユーザー **ID** の有効化**)** を選択し、外部ゾーン用の User-ID を有効にします。
8. **OK** をクリックします。

STEP 2 | 仮想システムの内部ゾーンから外部ゾーンへのトラフィック、およびその逆方向のトラフィックを許可または拒否するためのセキュリティポリシールールを設定します。

- セキュリティ ポリシー ルールの作成を参照してください。
- ファイアウォール内に残る vsys 間トラフィックを参照してください。

STEP 3 | 変更をコミットします。

Commit（コミット）をクリックします。

共有ゲートウェイの設定

このタスクを行うのは、複数の仮想システムでインターネットへの接続のために 1 つのインターフェイス（共通ゲートウェイ）を共有する必要がある場合です。このタスクでは、以下を想定しています。

- グローバルにルーティング可能な IP アドレスを使用して、共有ゲートウェイとなるインターフェイスを設定している。
- 仮想システムの設定を行うタスクが完了しました。インターフェイスとして、グローバルにルーティング可能な IP アドレスが設定されている外向きのインターフェイスが選択されている。
- 仮想システムの設定時に、**Visible Virtual System (**認識可能な仮想システム**)** フィールドで、通信のために相互に認識可能にする必要があるすべての仮想システムのチェック ボックスをオンにしている。

STEP 1 | 共有ゲートウェイを設定します。

1. **Device (**デバイス**)** > **Shared Gateway (**共通ゲートウェイ**)** を選択し、**Add (**追加**)** をクリックして **ID** を入力します。
2. できるならゲートウェイの **[ID]** を含めて分かりやすい [名前] を入力します。
3. DNS プロキシ ルールをインターフェイスに適用する場合は、**DNS Proxy (DNS** プロキシ**)** フィールドで DNS プロキシ オブジェクトを選択します。
4. 外部に接続する [インターフェイス] を　[追加] します。
5. **OK** をクリックします。

STEP 2 | 共有ゲートウェイのゾーンを設定します。

> 共有ゲートウェイにゾーンやインターフェイスなどのオブジェクトを追加すると、その共有ゲートウェイ自体が、***VSYS*** メニューに選択可能な *vsys* として表示されます。

1. **Network (**ネットワーク**)** > **Zones (**ゾーン**)** を選択し、**Name (**名前**)** で新しいゾーンを **Add (**追加**)** します。
2. **[**場所**]** として、作成するゾーンの対象共有ゲートウェイを選択します。
3. **[**タイプ**]** として、**[**レイヤー **3]** を選択します。
4. （任意）フラッド、偵察行為、パケット ベースの攻撃防御を提供する **Zone Protection Profile (**ゾーン プロテクション プロファイル**)**を選択（あるいは後で設定）します。
5. （任意）必要に応じて、**Log Setting (**ログ設定**)** でゾーン プロテクション ログを外部システムに転送するためのログ転送プロファイルを選択します。
6. （任意）**Enable User Identification (**ユーザー **ID** の有効化**)** を選択し、共通ゲートウェイ用の User-ID を有効にします。
7. **OK** をクリックします。

STEP 3 | 変更をコミットします。

Commit（コミット）をクリックします。

仮想システムのサービス ルートのカスタマイズ

単一のファイアウォールが複数の仮想システムで有効になっている場合、仮想システムがグローバル サービスおよびサービスルート設定を継承します。たとえば、ファイアウォールが共有電子メール サーバーを使用して、すべての仮想システムに電子メール アラートを発信できます。仮想システム毎に異なるサービスルートを作成したいケースもあります。

仮想システム レベルでサービス ルートを設定する 1 つのユース ケースが、1 つの Palo Alto Networks ファイアウォールで複数の個別のテナントをサポートする必要がある ISP の場合です。DNS、Kerberos、LDAP、NetFlow、RADIUS、TACACS+、マルチ ファクター認証、email、SNMP trap、syslog、HTTP、User-ID エージェント、VM モニター、および Panorama などのサービスにアクセスするためのカスタム サービス ルートがテナント毎に必要になります（コンテンツ更新およびソフトウェア更新のデプロイ）。もう 1 つのユース ケースは、サービス用のサーバーを設定するグループに完全な自律性をもたせようとする IT 組織です。グループごとに仮想システムを設定して、独自のサービス ルートを定義できるようにします。

仮想システムのサービス ルートに使用する仮想ルーターを選択できますが、出力インターフェイスを選択することはできません。管理者が仮想ルーターを選択し、ファイアウォールが仮想ルーターからパケットを送信した後、ファイアウォールは宛先 *IP* アドレスに基づいて出力インターフェイスを選択します。そのため、仮想システムに複数の仮想ルーターが設定されている場合、サービスのすべてのサーバーへのパケットは、*1* つの仮想ルーターのみを通過する必要があります。インターフェイス送信元アドレスが設定されたパケットが別のインターフェイスを通過する可能性がありますが、リターン トラフィックは送信元 *IP* アドレスが設定されたインターフェイスに戻るため、非対称トラフィックが作成されることがあります。

- 仮想システムのサービスへのサービス ルートのカスタマイズ
- PA-7000 シリーズ ファイアウォールでの仮想システム別のロギングの設定
- 仮想システムまたはファイアウォール別の管理アクセスの設定

仮想システムのサービスへのサービス ルートのカスタマイズ

マルチ仮想システム機能を有効にする際、特定のサービス ルートが設定されていない仮想システムは、ファイアウォールに対するグローバルのサービスおよびサービス ルート設定を継承します。代わりに、次に記載している通り、仮想システムを設定して異なるサービスルートを使用することができます。

ファイアウォールに仮想システムが複数ある場合は、IP アドレスが重複していないインターフェイスとサブインターフェイスが必要です。SNMP トラップまたは Kerberos に対して仮想システム別のサービス ルートを使用できるのは、IPv4 のみです。

サービスのサービス ルートは、サービスのサーバー プロファイルを設定した方法に厳密に従います。

- 共有ロケーションのサーバープロファイル（ **Device**（デバイス） > **Server Profiles**（サーバープロファイル） ）を定義すると、ファイアウォールはそのサービスのグローバル サービス ルートを使用します。

- 特定の仮想システム用のサーバー プロファイルを定義する場合、ファイアウォールはそのサービスに仮想システム固有のサービス ルートを使用します。
- 特定の仮想システムのサーバー プロファイルを定義しても、そのサービスの仮想システム固有のサービス ルートが設定されていない場合、ファイアウォールはそのサービスのグローバル サービス ルートを使用します。

ファイアウォールは、仮想システム単位の *syslog* の転送をサポートします。ファイアウォールの複数の仮想システムが *SSL* トランスポートを使用して *syslog* サーバーに接続している場合、ファイアウォールは安全な通信の証明書を *1* つのみ生成できます。仮想システムごとに独自の証明書を発行することはサポートされません。

STEP 1 | 仮想システムのサービス ルートをカスタマイズします。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Services (サービス)** > **Virtual Systems (仮想システム)** を選択し、さらに設定したい仮想システムを選択します。
2. **Service Route Configuration**（サービス ルートの設定）リンクをクリックします。
3. 以下のうち1つを選択します。
   - **Inherit Global Service Route Configuration** [グローバル サービス ルート設定の継承] – 仮想システムが、仮想システムに関連するグローバル サービス ルート設定を継承します。このオプションを選択する場合は、カスタマイズを行うステップをスキップしてください。
   - **Customize (カスタマイズ)**–サービスごとに送信元アドレスを指定できます。
4. **Customize** [カスタマイズ]を選択した場合は、サービスが使用するサーバー製品のアドレス タイプに応じて、**IPv4** タブまたは **IPv6** タブを選択します。サービスに IPv4 と IPv6 の両方のアドレスを指定できます。サービスをクリックします。（選択できるのは、仮想システムに関連するサービスのみです）。

   複数のサービスで同じ送信元アドレスを使用しやすくするためには、***Set Selected Routes (選択したルートを設定)*** をクリックして続行します。

   - 送信元アドレスのリストを制限するためには、**Source Interface (ソース インターフェイス)** を選択し、(そのインターフェイスから) 送信元アドレスをサービスルートとして選択します。**Any (すべての)** Source Interface (ソース インターフェイス) を選択すると、アドレスを選択する Source Address (送信元アドレス) リストで、その仮想システムのあらゆるインターフェイスのすべての IP アドレスを利用できるようになります。**Inherit Global Setting (グローバル設定の継承)** を選択できます。
   - **Source Interface (送信元インターフェイス)** で **Inherit Global Setting (グローバル設定を継承)** を選択した場合は **Source Address (送信元アドレス)** が **Inherited (継承済み)** と表示され、それ以外の場合は選択した送信元インターフェイスが示されます。**Source Interface (送信元インターフェイス)**に **Any (すべて)**を選択した場合は、IP アドレスを選択するか、(選択したタブと一致する IPv4 または IPv6 形式で) IP アドレスを入力して、外部サービスに送信されるパケットで使用される送信元アドレスを指定します。

- アドレス オブジェクトを変更し、IP のファミリ タイプ（IPv4/IPv6）が変更された場合は、**Commit** [コミット]をクリックして使用するサービス ルート ファミリを更新する必要があります。

5. **OK** をクリックします。
6. 前の各ステップを繰り返して、他の外部サービスの送信元アドレスも設定します。
7. **OK** をクリックします。

STEP 2 | 変更をコミットします。

[コミット] をクリックし、**[OK]** をクリックします。

PA-7000 シリーズ ファイアウォールのロギング サービスに仮想システムごとのサービス ルートを設定している場合は、PA-7000 シリーズ ファイアウォールでの仮想システム別のロギングの設定を行うタスクに進みます。

PA-7000 シリーズ ファイアウォールでの仮想システム別のロギングの設定

ログ タイプがトラフィック、HIP マッチ、脅威、WildFire の場合、PA-7000 Series ファイアウォールは SNMP トラップ、Syslog、電子メール サービスにサービス ルートを使用しません。その代わりに、PA-7000 Series ファイアウォールはロギング カードの使用をサポートしています。

ファイアウォールの設定によっては、次のいずれかのタイプのカードがあるかもしれません：

- **Log Processing Card (LPC) (ログ処理カード (LPC))**—LPC サブインターフェイスからサーバー上の各サービスに対するオンプレミス スイッチへの仮想システム固有のパスをサポートします。システム ログおよび設定ログについては、PA-7000 シリーズ ファイアウォールは、LPC ではなく、グローバル サービス ルートを使用します。ファイアウォールに LPC をインストールしている場合、ログカード ポートを設定する必要があります。
- ログ転送カード **(LFC)**—すべてのデータプレーンの、外部のログコレクタ (例えば、Panorama および Syslog サーバー) への高速ログ転送をサポートします。ファイアウォールに LFC をインストールしている場合、ログカード ポートを設定する必要はありません。

PAN-OS 10.1 以降を実行している *PA-7000 Series* ファイアウォール からシステム ログを転送する唯一の方法は、*LFC* を設定することです。

外部サーバーへのログ転送は、*LFC* サブインターフェイスではまだサポートされていません。

他の Palo Alto Networks モデルでは、データプレーンがロギング サービスのルート トラフィックを管理プレーンに送信し、このプレーンがトラフィックをロギング サーバーに送信します。PA-7000 Series ファイアウォールでは、LPC あるいは LFC にインターフェイスが 1 つしかなく、複数の仮想システムのデータプレーンが (上記のタイプの) ロギング サーバー トラフィックを PA-7000 Series ファイアウォールのロギング カードに送信します。ロギング カードには複数のサブインターフェイスが設定され、プラットフォームがロギング サービス トラフィックをこれらのサブインターフェイス経由で顧客のスイッチに送信します。このスイッチは複数のロギング サーバーに接続できます。

サブインターフェイスはそれぞれ、設定時にサブインターフェイス名とドット区切りのサブインターフェイス番号を付けることができます。このサブインターフェイスは、ロギング サービス用に設定されている仮想ルーターに割り当てられます。PA-7000 シリーズ ファイアウォールの他のサービス ルートは、その他の Palo Alto Networks プラットフォームのサービス ルートと同じように機能します。LPC や LFC 自体の詳細は、『PA-7000 Series Hardware Reference Guide』(英語) を参照してください。

- PA-7000 Series LPC での仮想システム別のロギングの設定
- PA-7000 Series LFC での仮想システム別のロギングの設定

PA-7000 Series LPC での仮想システム別のロギングの設定

ログ処理カード (LPC)をインストールした PA-7000 Series ファイアウォール上でマルチ vsys 機能を有効化している場合、次の流れに従い、異なる仮想システムに対してロギングを設定することができます。

STEP 1 | ログ カード サブインターフェイスを作成します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** の順に選択し、ログ カード インターフェイスにするインターフェイスを選択します。
2. **Interface Name** [インターフェイス名]を入力します。
3. **Interface Type (インターフェイス タイプ)** については **Log Card (ログカード)** を選択します。
4. **OK** をクリックします。

STEP 2 | LPC 物理インターフェイスのテナントごとにサブインターフェイスを追加します。

1. インターフェイス タイプがログ カードである Ethernet インターフェイスを強調表示して、**Add Subinterface** [サブインターフェイスの追加]をクリックします。
2. **Interface Name** [インターフェイス名]には、ピリオドの後に、テナントの仮想システムに割り当てるサブインターフェイスを入力します。
3. **Tag** [タグ]には、VLAN タグの値を入力します。

   このタグをサブインターフェイス番号と同じにすると便利ですが、異なる番号も設定できます。
4. （任意）**Comment** [コメント]を入力します。
5. **Config (設定)**タブの **Assign Interface to Virtual System (仮想システムへのインターフェイスの割り当て)** フィールドで、LPC サブインターフェイスを割り当てる仮想システムを選択します。または、**Virtual Systems** [仮想システム]をクリックして、新しい仮想システムを追加します。
6. **OK** をクリックします。

STEP 3 | サブインターフェイスに割り当てるアドレスを入力し、デフォルト ゲートウェイを設定します。

1. **Log Card Forwarding** [ログ カード転送]タブを選択し、以下のいずれかまたは両方を実行します。
   - IPv4 セクションに、サブインターフェイスに割り当てる **IP Address (IP アドレス)** および **Netmask (ネットマスク)** を入力します。**Default Gateway** [デフォルト ゲートウェイ]（Routing Information Base （RIB）に既知のネクスト ホップ アドレスがないパケットが送信されるネクスト ホップ）を入力します。
   - IPv6 セクションに、サブインターフェイスに割り当てる **IPv6 Address** [IPv6 アドレス]を入力します。**IPv6 Default Gateway** [IPv6 デフォルト ゲートウェイ]を入力します。
2. **OK** をクリックします。

STEP 4 | 変更をコミットします。

OK、**Commit (コミット)** の順にクリックします。

STEP 5 | 仮想システムの残りのサービス ルートをまだ設定していない場合は実行します。

仮想システムのサービス ルートのカスタマイズを行います。

PA-7000 Series LFC での仮想システム別のロギングの設定

ログ転送カード(LFC)がインストールされているPA-7000シリーズファイアウォールで複数の仮想システム(マルチvsys)機能を有効にしている場合は、異なる仮想システムのロギングを設定できます。LFC はログを Panorama ログコレクタ または syslog サーバに転送できます。

物理インターフェイスのみを設定できます。サブインターフェイスを介した *syslog* 転送は *LFC* ではまだサポートされていないため、各仮想システムは単一のタグなし物理インターフェイスを使用します。

ログを外部に転送するように *LFC* サブインターフェイスを設定すると、インターフェイスは期待どおりに動作しなくなります。

各仮想システムに対して個別のサブインターフェイスを設定するには、物理インターフェイスにサブインターフェイスを追加し、必要なタグを割り当ててサブインターフェイス トラフィックをセグメント化します。

Panorama 管理サーバーによって管理される *PA-7000 Series* ファイアウォールの場合、*LFC* 設定が *Panorama* からプッシュされた場合、ファイアウォール上で *LFC* 設定をローカルで上書きまたは元に戻すことはできません。*Panorama* からプッシュされた *LFC* 設定をオーバーライドするには、 でファイアウォール CLI にログインし、*Panorama* プッシュ設定を削除する必要があります。

```
admin> configure
```

```
admin# delete deviceconfig log-fwd-card
```

```
admin# commit
```

仮想システムまたはファイアウォール別の管理アクセスの設定

スーパーユーザー管理アカウントがある場合に、vsysadmin またはデバイス管理者ロールの詳細な権限を作成および設定できるようになりました。

STEP 1 | Web インターフェイスのさまざまな領域の設定権限または読み取り専用権限を管理者に付与する、または無効にする管理者ロール プロファイルを作成します。

1. **Device (デバイス)** > **Admin Roles (管理者ロール)** の順に選択し、**Admin Role Profile (管理者ロール プロファイル)** を **Add (追加)** します。
2. プロファイルの **Name** [名前]と **Description** [内容]（任意）を入力します。
3. **Role** [ロール]では、プロファイルによる制御のレベルを指定します。
   - **Device** [デバイス] – プロファイルで、グローバル設定およびすべての仮想システムを管理できます。
   - **Virtual System** [仮想システム] – プロファイルで、このプロファイルのある管理者に割り当てられている仮想システムのみを管理できます（管理者は **Device (デバイス)** > **Setup (セットアップ)** > **Services (サービス)** > **Virtual Systems (仮想システム)** にアクセスできますが、**Global (グローバル)** タブにはアクセスできません）
4. 管理者ロール プロファイルの **Web UI** タブで、**Device** [デバイス]までスクロール ダウンし、緑色のチェック マークをそのまま（有効）にします。
   - **Device** [デバイス]で、**Setup** [セットアップ]を有効にします。**Setup** [セットアップ]で、以下に示すように、このプロファイルで管理者に設定権限を付与する領域を有効にします（この設定で Read Only （読み取り専用）を許可した場合は、Enable/Disable （有効化/無効化）ローテーションに読み取り専用ロック アイコンが表示されます）。
     - **Management** [管理] – 管理者がこのプロファイルを使用して、**Management** [管理]タブの設定を行うことができます。
     - **Operations** [操作] – 管理者がこのプロファイルを使用して、**Operations** [操作]タブの設定を行うことができます。

- **Services** [サービス] – 管理者がこのプロファイルを使用して、**Services** [サービス]タブの設定を行うことができます。管理者が **Device (デバイス)** > **Setup Services** > **Virtual Systems (仮想システム)** タブにアクセスするためには **Services (サービス)** が有効になっている必要があります。前の手順で **Role (ロール)** を **Virtual System (仮想システム)** に指定した場合、**Device (デバイス)** > **Setup (セットアップ)** で有効にできる設定は**Services (サービス)** のみです。
- **Content-ID** [コンテンツ ID] – 管理者がこのプロファイルを使用して、**Content-ID** [コンテンツ ID]タブの設定を行うことができます。
- **WildFire** – 管理者がこのプロファイルを使用して、**WildFire** タブの設定を行うことができます。
- **Session** [セッション] – 管理者がこのプロファイルを使用して、**Session** [セッション]タブの設定を行うことができます。
- **HSM** – 管理者がこのプロファイルを使用して、**HSM** タブの設定を行うことができます。

5. **OK** をクリックします。
6. （任意）必要に応じて、権限が異なる別の管理者ロールを作成する場合は、すべての手順を繰り返します。

STEP 2 | 管理者ロール プロファイルを管理者に適用します。

1. **Device (デバイス)** > **Administrators (管理者)** の順に選択して、**Add (追加)** をクリックし、**Name (名前)**を入力して管理者を追加します。
2. （任意）**Authentication Profile**（認証プロファイル） を選択します。
3. （任意）**Use only client certificate authentication (Web) (**クライアント証明書認証のみを使用（**Web**）**)** を選択して、双方向認証を設定し、サーバーがクライアントを認証するようにします。
4. **Password** [パスワード]と **Confirm Password** [パスワードの確認]を入力します。
5. （任意）パスワードのみではなく、SSH 公開鍵を使ったより強固な認証方式を使用する場合は、**Use Public Key Authentication (SSH) (**公開鍵認証（**SSH**）の使用**)** を選択します。
6. **Administrator Type** [管理者タイプ]に、**Role Based** [ロール ベース]を選択します。
7. **Profile** [プロファイル]には、作成したプロファイルを選択します。
8. （任意）**Password Profile**（パスワード プロファイル）を選択します。
9. **OK** をクリックします。

STEP 3 | 設定をコミットします。

Commit（コミット）をクリックします。

仮想システムのその他の機能

ファイアウォールの機能の多くでは、仮想システムごとに、設定、表示、ロギング、またはレポート作成することができます。したがって、ドキュメントの他の関連するセクションでも仮想システムについて説明しているため、ここではそれらの情報は割愛します。関連する章のいくつかを以下に示します。

- アクティブ/パッシブ HA を設定する場合、2 つのファイアウォールの仮想システム機能は等しくする必要があります（単一または複数の仮想システム機能）。高可用性（HA）を参照してください。
- 仮想システムの QoS を構成するには、仮想システムの QoS の設定を参照してください。
- サブインターフェイス(および VLAN タグ)を使用する仮想ワイヤ展開で仮想システムを使用するファイアウォールの設定については、仮想ワイヤ インターフェイス を参照してください。
- ユーザー ID と複数の仮想システムを構成している場合は、仮想システム間でユーザーマッピングを共有することができます。仮想システム間でのユーザー ID マッピングの共有を参照してください。

ゾーン プロテクションおよび DoS 保護

ネットワークを機能ゾーンと組織ゾーンに分割すれば、ネットワークの攻撃の入り口（攻撃者にさらされるネットワークの領域）が小さくなります。ゾーン プロテクションは、フラッド攻撃、偵察行為の試み、パケット ベースの攻撃、非 IP プロトコルを使用する攻撃からネットワーク ゾーンを保護します。ゾーン プロテクション プロファイルをカスタマイズし、各ゾーンを保護してください（類似のゾーンには同じプロファイルを適用できます）。サービス拒否（DoS）保護は、特定の重要なシステム、特に WEB サーバーやデータベースサーバーのようなユーザーがインターネットからアクセスするデバイスをフラッド攻撃から保護し、リソースをセッション フラッドから保護します。DoS 保護プロファイルおよびポリシールールをカスタマイズし、重要な一連のデバイス保護してください。ベストプラクティス ドキュメント ポータルにアクセスすれば、ゾーン プロテクションおよび DoS 保護のベストプラクティスに関するチェックリストを入手できます。

ファイアウォールのデータプレーン *CPU* 使用量をチェック・監視し、復号化などの *CPU* サイクルを消費する各機能と共に、*DoS*、ゾーン プロテクションをサポートできるよう、各ファイアウォールが適切にサイジングされていることを確認します。*Panorama* を使ってファイアウォールを管理する場合は、デバイス モニター（***Panorama*** **>** ***Managed Devices*** **(**管理対象デバイス**)** **>** ***Health*** **(**ヘルス**)**）を使用し、すべての管理対象ファイアウォールの *CPU* 消費を一度にチェック・監視できます。

- ゾーンを使用してネットワークをセグメント化
- ゾーンがネットワークを保護する方法とは？
- ゾーン保護
- ゾーン保護を設定してネットワーク セキュリティを向上
- 新規セッションのフラッド攻撃に対する Dos プロテクション

ゾーンを使用してネットワークをセグメント化

大規模なネットワークは、保護するのが容易ではありません。大規模でセグメント化されていないネットワークは攻撃の入り口が大きくなり、管理や保護が難しくなります。トラフィックおよびアプリケーションはネットワーク全体にアクセスできるため、ネットワークに侵入した攻撃者は、ネットワーク内を横方向に移動して重要なデータにアクセスできます。また、大規模なネットワークでは監視や制御も難しくなります。ネットワークをセグメント化することで、攻撃者がゾーン間を横方向に動くのを防いでネットワーク内を移動できなくします。

セキュリティ ゾーンは、物理的あるいは仮想的な一つあるいは複数のファイアウォール インターフェイス、およびゾーンのインターフェイスに接続されたネットワーク セグメントから成るグループです。各ゾーンが必要とする特定の保護を利用できるよう、各ゾーンの保護を個別に管理します。例えば、財務部門用のゾーンでは、IT 部門のゾーンで許可されるアプリケーションがすべて必要というわけではない場合があります。

ネットワークを完全に保護するためには、すべてのトラフィックがファイアウォールを通るようにする必要があります。インターフェイスとゾーンの設定を行い、インターネット ゲートウェイ、重要なデータ ストレージ、ビジネス アプリケーションなどの機能領域毎に別のゾーンを、さらに財務、IT、マーケティング、エンジニアリングなどの組織ユニット毎に別のゾーンを作成します。機能、アプリケーションの使用、ユーザーのアクセス権限に論理的なビジョンがある場合は常に、個別のゾーンを作成してその領域を隔離・保護し、適切なセキュリティポリシールールを適用して、一部のグループだけがアクセスを必要とするデータやアプリケーションに対する不要なアクセスを阻止します。ゾーンが小さければ、ネットワーク トラフィックに対する可視性や制御能力が増します。ネットワークを複数のゾーンに別けることで、ユーザー、デバイス、アプリケーション、パケットを一切信頼せず、あらゆるものに対して検証を行うというセキュリティの考え方、ゼロ トラスト アーキテクチャを実装しやすくなります。正当なビジネス上の理由があるユーザー、デバイス、アプリケーションに対してのみアクセスを許可し、他のトラフィックはすべて拒否するネットワークを作成することが、最終的な目標になります。

ゾーンへのアクセスを適切な形で制限・許可する方法は、ネットワーク環境によって異なります。例えば、重要な製造装置や出入りが厳重に管理されている領域をワークステーションが制御する、セミコンダクター製造フロアやロボット組み立て工場のような環境では、外部のデバイスからアクセスできない（モバイル デバイスでアクセスできない）、物理的に隔離された空間が必要になる場合があります。

ユーザーがモバイル デバイスからネットワークにアクセスできる環境では、ネットワークを複数のゾーンにセグメント化するとともに、User-ID および App-ID を有効化することで、ユーザーがどこからネットワークにアクセスしていても、必ず適切なアクセス権限を得られるようにすることができます。これは、アクセス権限が特定のゾーンにあるデバイスではなくユーザーあるいはユーザーグループに結びつけられるためです。

機能領域やグループが異なると、保護要件も異なる可能性があります。例えば、大量のトラフィックを扱うゾーンの場合、通常少ないトラフィックを扱うゾーンとは異なるフラッド防御のしきい値が必要になるかもしれません。各ゾーンに対して適切な保護を定義できるということも、ネットワークをセグメント化する理由になります。適切な保護方法は、ネットワーク アーキテクチャ、保護対象、拒否・許可したいトラフィックの性質によって決まります。

ゾーンがネットワークを保護する方法とは？

ゾーンへのアクセスやゾーン間のトラフィックの動きを制御できるため、ゾーンはネットワークを小さく管理しやすいエリアにセグメント化して保護するだけでなく、ネットワークも保護します。

ファイアウォールのインターフェイスはゾーンに割り当てられるまでの間、トラフィックを処理できないため、ゾーンは制御不能なトラフィックがファイアウォールのインターフェイスを通じてネットワークに流入するのを防ぎます。ファイアウォールは入力インターフェイスにゾーンプロテクションを適用します。そこでは、トラフィックがゾーンに入る前にトラフィックをフィルタリングするために、元のクライアントから応答するサーバー（c2s）に向かう方向で、トラフィックがファイアウォールに入ります。

ファイアウォールのインターフェイス タイプおよびゾーン タイプ（タップ、バーチャル ワイヤ、L2、L3、トンネル、あるいは外部）が一致しなければなりません。それにより、ゾーンに属さないトラフィックを許可せずにネットワークを保護しやすくなります。例えば、L2 インターフェイス を L2 ゾーンに、あるいは L3 インターフェイスを L3 ゾーンに割り当てることができますが、L2 インターフェイスを L3 ゾーンに割り当てることはできません。

さらに、ファイアウォールのインターフェイスは単一のゾーンにのみ所属できます。別のゾーンに向かうトラフィックは同じインターフェイスを使えません。これにより、不適切なトラフィックがゾーンに入らないようにしつつ、各ゾーン毎に適切な保護を設定できるようになります。ゾーンの入り口となる複数のインターフェイスに接続して帯域幅を増やすことができますが、各インターフェイスは単一のゾーンにしか接続できません。

ゾーンに入るトラフィックをファイアウォールが許可した後は、トラフィックは自由にゾーン内を流れることが可能になり、ログに記録されることもありません。各ゾーンを細分化することで、各ゾーンにアクセスするトラフィックを制御しやすくなり、マルウェアがゾーン間でネットワーク内を横方向に動くのが難しくなります。セキュリティポリシー ルールによって許可され、かつゾーン タイプ（タップ、バーチャル ワイヤ、L2、L3、トンネル、あるいは外部）が同じでない場合、トラフィックはゾーン間を流れることができません。例えば、セキュリティポリシー ルールは 2 つの L3 ゾーン間のトラフィックを許可できますが、 L3 ゾーンおよび L2 ゾーン間のトラフィックは許可できません。ポリシールールによってゾーン間トラフィックが許可されている場合、ファイアウォールはゾーン間を流れるトラフィックをログに記録します。

デフォルト設定では、セキュリティポリシールールはトラフィックがゾーン間を横方向に流れるのを拒否し、あるゾーンのアクセスを掌握したマルウェアが自由にネットワーク内を移動して他の目標に向かうのを防ぐようになっています。

トンネル ゾーンは暗号化されないトンネル用です。トンネル コンテンツ検査の概要に記載されているとおり、トンネル コンテンツ、および外側のトンネルのゾーンに対して異なるセキュリティポリシールールを適用することができます。

ゾーン保護

ゾーン プロテクション プロファイルはフラッド、偵察行為、パケット ベース、および非 IP プロトコル ベースの攻撃からゾーンを保護します。DoS 保護ポリシールールで使用される DoS 保護プロファイルは、特定の重要なデバイスを、ターゲットを定めたフラッドおよびリソース ベースの攻撃から保護します。DoS 攻撃は、大量の望ましくないトラフィックでネットワークあるいはターゲットのクライアント システムに負荷をかけ、ネットワークサービスを中断させようとする行為です。

各種の DoS 攻撃からネットワークを保護する計画を立ててください：

- アプリケーション ベースの攻撃—特定のアプリケーションの脆弱性を狙い、正当なユーザーが利用できないよう、リソースを消耗させようと試みます。Slowloris攻撃がこの例です。
- プロトコル ベースの攻撃—state-exhaustion攻撃とも呼ばれ、プロトコルの脆弱性を狙って攻撃します。SYN フラッド攻撃が良くある例です。
- 大ボリューム攻撃—利用できるネットワークリソース、特に帯域幅を消耗させることでターゲットをダウンさせ、正当なユーザーがリソースにアクセスできないようにしようと試みる大容量の攻撃です。UDP フラッド攻撃がこの例です。

デフォルトのゾーン保護プロファイルまたは DoS 保護プロファイルと DoS 保護ポリシー ルールはありません。各ゾーンのトラフィックの性質に基づいてゾーン プロテクションを設定・適用し、各ゾーンで保護したい個々の重要なシステムに基づいて DoS 保護を設定してください。

- ゾーン保護ツール
- ゾーン保護ツールはどのように機能しますか？
- DoS 保護のためのファイアウォールの配置
- ゾーン保護プロファイル
- パケット バッファ保護
- DoS プロテクション プロファイルおよびポリシールール

ゾーン保護ツール

DoS 攻撃を効果的に防ぐには、レイヤーアプローチが必要になります。インターネットに接続されたネットワークの境界および周辺ルーター、スイッチ、あるいは適切なアクセス制御リスト（ACL）を持つその他のハードウェアベースのパケット ドロップ デバイスのところにある専用の大容量 DDoS 保護デバイスを使い、セッションベースのファイアウォールが対応できない大容量の攻撃を防ぐことが、最初の防御層になります。ファイアウォールは、専用の DDoS デバイスでは得られない、DoS 攻撃を細かく防ぐ層を追加してくれます。

Palo Alto Networks のファイアウォールは、4 つの補完的なツールを提供し、ネットワーク ゾーンおよび重要なデバイスを守る DoS 保護をレイヤー化します。

- ゾーン プロテクション プロファイルは、IP フラッド攻撃、偵察行為のポートスキャン、ホスト スイープ、IP パケット ベースの攻撃、非 IP プロトコルの攻撃から入力ゾーンの先端を保護します。入力ゾーンは、トラフィックがファイアウォールのクライアントからサーバー（c2s）へのフロー方向に入る場所です。クライアントはフローの発信元であり、サーバーはレスポンダです。ゾーン プロテクション プロファイルは、ゾーンに向かう 1 秒あたりの新規

接続数（CPS）を制限することで、ゾーンに入る集約トラフィックに基づき、DoS 攻撃を防止する全般的な保護を提供する 2 つ目の層を提供します。ゾーンに入る集約トラフィックに対してプロファイルが適用されるため、ゾーン プロテクション プロファイルは個々のデバイス（IP アドレス）を考慮しません。

ゾーン保護プロファイルは、ファイアウォールが DoS 保護ポリシーおよびセキュリティ ポリシー ルックアップを実行する前にセッションが形成されるときにネットワークを防御し、DoS 保護ポリシーまたはセキュリティ ポリシー ルールのルックアップよりも少ない CPU サイクルを消費します。ゾーン保護プロファイルがトラフィックを拒否した場合、ファイアウォールはポリシー ルールのルックアップで CPU サイクルを消費しません。

ゾーン プロテクション プロファイルをすべてのゾーン、インターネットに接続されたゾーンと内部のゾーンの両方に適用します。

- **DoS 保護プロファイルおよびポリシールール**は、個々の具体的なエンドポイントおよびリソース、特にユーザーがインターネットからアクセスする重要なターゲットをフラッド攻撃から保護します。ゾーン プロテクション プロファイルがゾーンをフラッド攻撃から保護するのに対し、適切な DoS 保護プロファイルを持つ DoS 保護ポリシールールはゾーン内の個々の重要なシステムを、ターゲットを定めたフラッド攻撃から保護し、DoS 攻撃に対する 3 つ目の防御層を提供します。

  DoS 保護の目的は重要なデバイスを保護することであり、またそれによってリソースが消費されるため、*DoS* 保護は *DoS* 保護ポリシールールで指定したデバイスのみを保護します。他のデバイスは保護されません。

  DoS 保護プロファイルは、フラッド攻撃に対する保護のしきい値（新規 CPS 制限）、リソース保護のしきい値（指定されたエンドポイントとリソースのセッション制限）、およびプロファイルが集約トラフィックまたは分類トラフィックに適用されるかどうかを個々のデバイスあるいはデバイス グループに設定します。DoS 保護ポリシールールは、一致条件（送信元、宛先、サービス ポート）、トラフィックがルールにマッチした際に行うアクション、各ルールに関連する集約および分類化 DoS 保護プロファイルを指定します。

  Aggregate (集約) DoS 保護ポリシールールは、集約 DoS 保護プロファイルで定義された CPS のしきい値を、DoS 保護ポリシールールの一致条件を満たすすべてのデバイスの全トラフィックに適用します。例えば、集約 DoS 保護プロファイルで CPS レートを 20,000 に制限する場合、その 20,000 CPS の制限は、グループ全体で集約された接続数に対して適用されます。この場合、許可された接続数の大部分を単一のデバイスが受信する可能性もあります。

  Classified (分類化) DoS 保護ポリシールールは、分類化 DoS 保護プロファイルで定義された CPS のしきい値を、ポリシールールにマッチする個々のデバイスに適用します。例えば、分類化 DoS 保護プロファイルで CPS レート を 4,000 に設定する場合、グループ内のどのデバ

イスも 4,000 CPS までしか許容できなくなります。DoS 保護ポリシーは、集約プロファイルおよび分類化プロファイルを一つずつ持つことができます。

分類化プロファイルは送信元 *IP*、宛先 *IP*、あるいはその両方に基づいて接続を分類化できます。ファイアウォールはインターネット ルーティングテーブルを保持するだけのスケーリングを行えないため、インターネットに接続されたゾーンでは、宛先 *IP* のみで分類化します。

DoS 保護は、WEB サーバーやデータベースサーバーなど、ユーザーがインターネットからアクセスする特に攻撃対象になりやすい重要なデバイスのみに適用します。

- 既存のセッションに対し、パケット バッファ保護は、しきい値とタイマーを使って悪用されているセッションを回避することで、ファイアウォールのパケット バッファを溢れさせようと試みる単一セッション DoS 攻撃からファイアウォールを（つまり、同時にゾーンを）保護します。パケット バッファ保護はグローバルな範囲で設定し、ゾーン毎に適用します。
- セキュリティポリシールールは、セッションの入力フローと出力フローの両方に影響します。セッションを確立するには、受信トラフィックが既存のセキュリティ ポリシー ルールと一致する必要があります。一致するものがなければ、ファイアウォールはパケットを破棄します。セキュリティポリシーは、ゾーン、IP アドレス、ユーザー、アプリケーション、サービス、および URL カテゴリを含む基準を使用して、ゾーン間（インターゾーン）およびゾーン内（イントラゾーン）間のトラフィックを許可あるいは拒否します。

  各セキュリティポリシールールに対してベストプラクティスの脆弱性保護プロファイルを適用し、*DoS* 攻撃を防止します。

  デフォルトのセキュリティ ポリシー ルールでは、ゾーン間でトラフィックの移動が許可されないため、インターゾーン トラフィックを許可する場合はセキュリティポリシー ルールを設定する必要があります。すべてのイントラゾーン トラフィックはデフォルトで許可されます。セキュリティ ポリシー ルールを設定して、イントラゾーン、ゾーン間、またはユニバーサル（イントラゾーンおよびインターゾーン）トラフィックを照合および制御できます。

  ゾーン保護プロファイル、*DoS* 保護プロファイルとポリシー ルール、およびセキュリティ ポリシー ルールは、ファイアウォール上のデータプレーン トラフィックにのみ影響します。ファイアウォール管理インターフェイスから発信されるトラフィックはデータプレーンを通過しないため、ファイアウォールはこれらのプロファイルまたはポリシー ルールに対する管理トラフィックと一致しません。
- また、ハッシュ、CVE、シグネチャ ID、ドメイン名、URL、IP アドレスを基準にしてPalo Alto Networks Threat Vault（有効なサポートアカウントとログインが必要）で脅威を検索できます。

ゾーン保護ツールはどのように機能しますか？

パケットがファイアウォールに到達する際、ファイアウォールはパケット ヘッダから得られる入力ゾーン、出力ゾーン、送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびアプリケーションに基づき、パケットを既存のセッションとマッチさせようと試みます。ファイアウォールがマッチを見つければ、パケットはそのセッションをすでに制御しているセキュリ

ティポリシールールを使用します。パケットが既存のセッションとマッチしない場合、ファイアウォールはゾーン プロテクション プロファイル、DoS 保護プロファイルおよびポリシールール、セキュリティポリシールールを使用し、セッションを確立するかパケットを破棄するか判断し、パケットが受け取るアクセス レベルを決定します。

インターネットに接続されたネットワークの先端にある専用の DDoS デバイスをトラフィックが通過する際にファイアウォールが最初に適用する保護は、ゾーン プロテクション プロファイルがゾーンに付与されている場合、それによる全般的な防御です。ファイアウォールは、パケットが到達するインターフェイスからゾーンを決定します（各インターフェイスは単一のゾーンにのみ割り当てられており、トラフィックを運ぶすべてのインターフェイスは単一のゾーンに属す必要があります）。ゾーン プロテクション プロファイルがパケットを拒否すると、ファイアウォールはそのパケットを破棄してリソースを保存するため、DoS 保護ポリシーやセキュリティポリシーに対してルックアップを行う必要がありません。ファイアウォールは、新規セッション（既存のセッションにマッチしないパケット）に対してのみゾーン プロテクション プロファイルを適用します。ファイアウォールがセッションを確立した後、そのセッション中の後続のパケットに対しては、ファイアウォールはゾーン プロテクション プロファイルのルックアップをスキップします。

ゾーン プロテクション プロファイルがパケットをドロップしない場合、ファイアウォールは 2 つ目の保護として DoS 保護ポリシールールを適用します。ゾーンにやって来るトラフィックの集約された合計量に基づいてゾーン プロテクション プロファイルがパケットを許可する場合、ルールの DoS 保護プロファイルにあるフラッド防御あるいはリソース保護設定を超過する特定のソースからパケットが来る、あるいは特定の宛先に向かう場合、DoS 保護ポリシールールはパケットを拒否する可能性があります。パケットが DoS 保護ポリシールールにマッチする場合、ファイアウォールはルールをパケットに適用します。ルールがアクセスを拒否する場合、ファイアウォールはパケットを破棄し、セキュリティポリシーのルックアップを行いません。ルールがアクセスを許可する場合、ファイアウォールはセキュリティポリシーのルックアップを実行します。ゾーン プロテクション プロファイルと同様に、ファイアウォールは新規セッションに対してのみ DoS 保護ポリシーを適用します。

ファイアウォールが適用する 3 つ目の保護はセキュリティポリシーのルックアップであり、これはゾーン プロテクション プロファイルおよび DoS 保護ポリシールールがパケットを許可する場合にのみ発生します。ファイアウォールがそのパケットについてマッチするセキュリティポリシー ルールを見つけられない場合、ファイアウォールはパケットを破棄します。ファイアウォールがマッチするセキュリティポリシー ルールを見つけた場合、ファイアウォールはルールをパケットに適用します。セッションの有効期間全体を通して、ファイアウォールはセキュリティポリシー ルールをトラフィックに対して双方向（c2s および s2c）に適用します。すべてのセキュリティポリシールールに対してベストプラクティスの脆弱性保護プロファイルを適用し、DoS 攻撃を防止します。

ファイアウォールが適用する 4 つ目の保護がパケット バッファ保護です。これは、グローバルに適用してデバイスを保護することも、個々にゾーンに適用することもでき、ファイアウォールのパケット バッファを溢れさせようと試みる単一セッション DoS 攻撃を防止します。グローバルな保護の場合、トラフィックのレベルが保護のしきい値を超える際にファイアウォールはランダム早期ドロップ（RED）を使用してパケット（セッションではなく）をドロップします。ゾーン単位の保護の場合、ファイアウォールはパケット バッファのしきい値を超える送信元 IP アドレスをブロックします。ゾーンおよび DoS 保護の場合と異なり、パケット バッファ保護は既存のセッションに適用されます。

DoS 保護のためのファイアウォールの配置

ファイアウォールはセッションベースのデバイスであり、大ボリュームの DoS 攻撃を防止するために何百万もの 1 秒あたりの接続数（CPS）に合わせてスケーリングするようには設計されていません。ファイアウォールはそれぞれの固有のフローをセッションとして扱い（入力および出力ゾーン、送信元および宛先 IP、プロトコル、およびアプリケーションに基づいて）、CPU サイクルを消費してポートおよび IP 単位でパケット検査を行います。フラッドのしきい値カウンターのために各セッションをカウントする必要があるため、ファイアウォールのフラッドを回避するためには、ファイアウォールの配置が重要になります。

最適な DoS 保護を得るために、保護するリソースのできるだけ近くにファイアウォールを配置してください。これにより、ファイアウォールが処理しなければならないセッション数が減るため、DoS 保護を提供するために必要になるファイアウォール リソースの量も減ります。

インターネットに面した境界では、専用の DDoS デバイス、境界ルーター、スイッチの前に、DoS 保護あるいはゾーン プロテクションに使うファイアウォールを配置しないでください。それらの大容量のデバイスを DoS 保護の最初のラインにすることで、大ボリュームのフラッド攻撃を抑えることができます。境界にあるゾーンおよび DoS 保護では大容量のファイアウォールを使用し、大容量のデバイスの後ろに配置してください。原則として、境界に近いファイアウォールは、トラフィックに対処するために高い能力を必要とします。

ネットワークをゾーンに分ける方法によって、内部 DoS 攻撃を緩和できます。ゾーンが小さいと、多くのトラフィックがゾーン間を通過しなければならないため、トラフィックに対する可視性が増し、マルウェアの横方向の動きを阻止しやすくなります。ゾーン間のトラフィックを許可するためには、特定のセキュリティポリシー ルールを作成する必要があります（すべてのゾーン内トラフィックはデフォルトで許可されています）。ネットワークのセグメント分けをあまり行っていない場合は、セグメント化を再び検討してみてください。

フラッドのしきい値を設定するためのベースライン CPS 測定

フラッド防御のしきい値は、ゾーン（ゾーン プロテクション プロファイル）、ゾーン内のデバイスのグループ（集約 DoS 保護ポリシー）、あるいはゾーン内の個々のデバイス（分類化 DoS 保護ポリシー）に対して許可する 1 秒あたりの新規接続数（CPS）、新規接続をスロットリングして可能性のあるフラッド攻撃を抑えるタイミング、すべての新規接続をドロップするタイミングを決定します。各ファイアウォールは異なるため、デフォルトのゾーン プロテクション プロファイルおよびDoS 保護プロファイル フラッド防御のしきい値は、大抵のネットワークにとって適切ではありません。各ゾーンの通常およびピーク時の集約された CPS を把握して効果的なゾーン プロテクション プロファイルのしきい値を設定し、保護したい個々の重要なシステムに対し、過度に大きすぎるしきい値を設定してフラッド攻撃を許すことなく、あるいは小さすぎるしきい値を設定してトラフィックをスロットリングすることなく効果的な DoS 保護プロファイルのしきい値を設定する必要があります。

- 行うべき CPS 測定
- CPS を測る方法

行うべき **CPS** 測定

最低 5 営業日の期間を通して、あるいは測定値がネットワークの典型的なトラフィック パターンを反映していると確信できるまで、平均およびピーク時の CPS トラフィックを計測します。

計測期間が長いほど、より精確な計測結果を得られます。サポート対象の CPS 数が大きく増加するような特別なイベント、四半期のイベント、年に 1 度のイベントを考慮してください。ファイアウォールがさらなるトラフィックに対応できる能力を持っている場合、DoS 保護ポリシールールで調整するスケジュールおよびゾーン プロテクション プロファイルを調整し、これらのタイプのイベントに対処できるようにする必要があるかもしれません。次のベースラインを計測してください：

- ゾーン プロテクション プロファイルの場合、各ゾーンから侵入する平均およびピーク時の CPS を計測します。
- 集約 DoS 保護プロファイルの場合、保護したい各グループのデバイスを合わせた平均およびピーク時の CPS を計測します。
- 分類化 DoS 保護プロファイルの場合、保護したい個々のデバイスの平均およびピーク時の CPS を計測します。

また、ファイアウォールの能力、そして復号化などのようにリソースを消費する他の機能が、各ファイアウォールが制御できる接続数にどのように影響するのか把握してください。原則として、境界に近いファイアウォールは多くのトラフィックに対処するため、高い能力が必要になります。各ファイアウォール モデルのデータシートには、ファイアウォールがサポートできる 1 秒あたりの合計新規セッション数（CPS）が記載されており、ファイアウォール比較ツールを使用すれば、各ファイアウォール モデルの CPS（およびその他のメトリック）を比較できます。

CPS を測る方法

CPS は様々な方法で計測できます：

- Panorama を使ってファイアウォールを管理する場合、デバイス監視を使ってファイアウォールに向かう CPS を計測します（**Panorama** > **Managed Devices (管理対象デバイス)** > **Health (ヘルス)** > **All Devices (すべてのデバイス)**）。また、各ファイアウォールで典型的に利用できるキャパシティを把握する際に役立つ、90 日間の平均およびピーク時の CPU 使用状況の傾向をデバイス監視で確認することもできます。
- 操作 CLIコマンド **`show session info`** を実行します。

  操作 *CLI*コマンド ***`show counter interface`*** を実行すると、実際の *CPS* 値の*2*倍を表示します。このコマンドを使用する場合は、*CPS* 値を*2*で割って、実際の *CPS* 値を導き出します。
- 適切な DoSプロテクション プロファイルのしきい値を設定するために、アプリケーション チームと協力し、通常およびピーク時のサーバーへの CPS、そのサーバーがサポートできる最大 CPS を把握します。

  さらに、保護したい重要なデバイスの宛先 IP アドレスに基づいてファイアウォールのトラフィックログおよび脅威ログをフィルタリングし、通常およびピーク時のセッション アクティビティ情報を得ることができます。
- Wireshark、NetFlow などのサードパーティ制のツールを使用し、ネットワーク トラフィックを収集・分析します。
- CPS 情報の収集、継続的な監視、ログ情報のマイニングを自動化するスクリプトを使用します。

- ファイアウォール上のすべてのセキュリティポリシー ルールが**Log at Session End** (セッション終了時にログを記録)するよう設定します。NetFlow や Wireshark などの監視ツールがなく、自動化スクリプトを入手・作成できない場合は、**Log at Session End** (セッション終了時にログを記録)でセッション終了時の接続数をキャプチャできます。CPS 情報は提供されませんが、選択した期間に終了するセッションの数を示し、その情報から1秒あたりのセッションの概算を計算できます。

ファイアウォールはリソースを節約するために、*10* 秒間隔で集約 *CPS* を計測します。このため、ファイアウォールで表示される測定値は、*10*秒間隔内にバーストをキャッチしない場合があります。平均 *CPS* 測定値は影響を受けませんが、ピーク *CPS* 測定値は正確でない場合があります。例えば、ファイアウォール ログが *10* 秒間の平均を *5,000 CPS* と報告する場合、*1* 秒間で *4,000 CPS* が一気に入り、あとの *1,000 CPS* は残りの *9* 秒間に分散されている可能性もあります。

時間の経過に伴う CPS 履歴データを収集するには、SNMP サーバーを使用している場合は、ユーザー所有の管理ツールを使用して SNMP MIB をポーリングできます。ただし、MIB の CPS 測定値は実際の CPS 値の2倍を示すことを理解することが重要です (たとえば、実際のCPS 測定値が10,000の場合、MIB は値として20,000を示します)。MIB から傾向を確認することは可能で、CPS 値を2で割って、真の値を導き出すことができます。SNMP MIB OIDs は以下の通りです:PanZoneActiveTcpCps、PanZoneActiveUdpCps、および PanZoneOtherIpCps。ファイアウォールは測定を行い、SNMP サーバーを10秒ごとに更新するだけなので、10秒ごとにポーリングします。

加えて、フラッド イベント用のログ転送プロファイルを別途作成し、適切な管理者がフラッド（DoS 攻撃の可能性を示す）イベントだけを含むメールを受け取るようにします。ゾーン プロテクションおよび DoS 保護のしきい値イベントの両方に対し、ログ転送を設定します。

ゾーンおよび *DoS* 保護を実装した後、これらの方式を使ってデプロイメントを監視し、ネットワークの拡大やトラフィック パターンの変化に合わせて、フラッド防御のしきい値を調整できるようにしてください。

ゾーン保護プロファイル

ゾーン保護プロファイルを各ゾーンに適用して、入力ゾーンに入る集約トラフィックに基づいてゾーンを防御します。

ゾーン プロテクションおよび *DoS* 保護を構成することに加え、各セキュリティポリシールールに対してベストプラクティスの脆弱性保護プロファイルを適用し、*DoS* 攻撃を防止します。

- フラッド防御
- 偵察行為防御
- パケットベース攻撃防御パケットベースコウゲキボウギョ
- プロトコル保護
- イーサネット SGT 保護

フラッド防御

フラッド防御を設定したゾーン プロテクション プロファイルは、入力ゾーン全体を SYN、ICMP、ICMPv6、UDP、およびその他の IP フラッド攻撃から保護します。ファイアウォールはゾーンに入る各フラッド タイプの合計数を1 秒あたりの接続数（CPS）に基づき測定し、ゾーン プロテクション プロファイルで設定ですしきい値とその合計を比較します。（DoS プロテクション プロファイルおよびポリシールールを使ってゾーン内の個々の重要なデバイスを保護します）

ファイアウォールのデータプレーン *CPU* 使用量を測定・監視し、*DoS*、ゾーン プロテクション、そして復号化などの *CPU* サイクルを消費するその他の機能をサポートできるよう、各ファイアウォールが適切にサイジングされていることを確認します。*Panorama* を使ってファイアウォールを管理する場合、デバイス監視（***Panorama*** **>** ***Managed Devices*** *(*管理対象デバイス*)* **>** ***Health*** *(*ヘルス*)* **>** ***All Devices*** *(*すべてのデバイス*)*）に管理対象の各ファイアウォールの *CPU* およびメモリ使用量が表示されます。また、各ファイアウォールで典型的に利用できるキャパシティを把握する際に役立つ、*90* 日間の平均およびピーク時の *CPU* 使用状況の傾向を確認することもできます。

各フラッド タイプについて、ゾーンに入る新しい CPS のしきい値を 3 つ設定します。また、SYN フラッド用にドロップ**Action (**アクション**)**を設定できます。ゾーンのベースライン CPS レートが分かっている場合、これらのガイドラインを使用して初期しきい値を設定してから、監視を行って必要に応じてしきい値を調整します。

- アラーム レート—アラームを発動する新しい CPS のしきい値。通常の変動でアラームを発生させないよう、ゾーンの平均 CPS レートよりも 15～20% 高い**Alarm Rate (**アラーム レート**)**を設定することを目指してください。
- アクティベート—フラッド保護メカニズムをアクティベートし、新規接続をドロップし始める新しい CPS のしきい値。ICMP、ICMPv6、UDP、およびその他の IP フラッドの場合、保護メカニズムはランダム早期ドロップ（RED、ランダム初期検知とも呼ばれる）です。SYN フラッドについてのみ、ドロップ**Action (**アクション**)**を SYN Cookies あるいは RED に設定できます。潜在的なフラッドを抑制し始められるよう、ゾーンのピーク CPS レートよりもわずかに高い**Activate (**アクティベート**)**レートを設定することを目指してください。
- 最大—RED が保護メカニズムである間にインバウンド パケットをドロップする 1 秒あたりの接続数。ファイアウォール リソースを消費する他の機能を加味しつつ、ファイアウォールの能力のおよそ 80～90% の**Maximum (**最大**)**レートを設定することを目指してください。

ゾーンのベースライン CPS レートが分からない場合、まずは**Maximum (**最大**)** CPS レートをファイアウォールの能力のおよそ 80～90% に設定し、それを使って合理的なフラッド抑制アラームおよびアクティベーション レートを割り出してください。Maximum (最大) レートに基づいて**Alarm Rate (**アラーム レート**)**および**Activate (**アクティベート**)**レートを設定します。例えば、**Alarm Rate (**アラーム レート**)**を**Maximum (**最大**)**レートの半分に設定し、受信するアラームの数、消費されるファイアウォール リソースの量に基づいて調整することもできます。**Activate Rate (**アクティベート レート**)**によって接続がドロップされ始めるため、慎重に設定してください。通常時のトラフィック負荷はある程度上下するため、あまり積極的に接続をドロップしようとしないのがベストです。ファイアウォール リソースが影響を受けている場合は、十分慎重にレートを調整してください。

SYN フラッド防御は、ドロップ**Action (**アクション**)**を設定できる唯一のタイプです。まずは**Action (**アクション**)**を**SYN Cookies**に設定します。*SYN Cookies* は正当なトラフィックを公正に扱い、*SYN* ハンドシェイクに失敗したトラフィックにみをドロップします。それに対し、ランダム早期ドロップを使用するとトラフィックがランダムにドロップされるため、*RED* は正当なトラフィックに影響を与えることがあります。しかし、*SYN Cookies* の場合、ファイアウォールがターゲット サーバーのプロキシとして動作し、そのサーバーの *3* 方向ハンドシェイクを制御するため、リソース消費量が大きくなります。正当なトラフィック（*SYN Cookies*）をドロップさせず、ファイアウォール リソースを保つ（*RED*）というバランスを取ることになります。ファイアウォールを監視し、*SYN Cookies* がリソースを消費し過ぎている場合は、*RED* に切り替えます。ファイアウォールの前面に専用の *DDoS* 保護デバイスがない場合、ドロップ メカニズムとして必ず *RED* を使用してください。

SYN クッキー がアクティブ化されると、ファイアウォールは *SYN/ACK* をプロキシする時点でこれらの値を認識しないため、サーバが送信する *TCP* オプションを受け入れなくなります。したがって、*TCP* サーバーのウィンドウ サイズや *MSS* 値などの値は、*TCP* ハンドシェイク中にネゴシエートできず、ファイアウォールは独自の既定値を使用します。サーバーへのパスの *MSS* がファイアウォールの既定の *MSS* 値よりも小さい場合、パケットをフラグメント化する必要があります。

ゾーン プロテクション プロファイルが有効になることで正当なトラフィックが意図せずドロップされることがないよう、デフォルトのしきい値は高く設定されています。このしきい値を、ネットワークのトラフィックに対して適切な値に調整してください。合理的なフラッドのしきい値を判断する最適な方法は、各フラッド タイプについて平均およびピーク時 CPS のベースラインを計測し、各ゾーンの通常のトラフィック状態を把握し、復号化などのリソースを消費する他の機能の影響を加味しつつファイアウォールの能力を知ることです。ネットワークの拡大に合わせ、必要に応じてフラッドのしきい値を監視・調整してください。

複数のデータプレーン プロセッサ（*DP*）を持つファイアウォールは、*DP* 全体に接続を分配します。通常、ファイアウォールは *CPS* のしきい値設定を *DP* 全体に対して均等に割ります。例えば、ファイアウォールに *5* つの *DP* があり、**Alarm Rate (**アラーム レート**)**を *20,000 CPS* に設定する場合、各 *DP* の**Alarm Rate (**アラーム レート**)**が *4,000 CPS*（*20,000 / 5 = 4,000*）になるため、*DP* の新規セッションが *4,000* を超えると、その *DP* の**Alarm Rate (**アラーム レート**)**のしきい値が発動します。

偵察行為防御

軍における定義と同様に、ネットワーク セキュリティにおける偵察行為の定義は、攻撃者が秘密裏にネットワークを調査して弱点を探り、ネットワークの脆弱性についての情報を得ようと試みることです。偵察行為はしばしば、ネットワークへの攻撃の前触れになります。すべてのゾーンで偵察行為防御を有効化し、ポートスキャンおよびホスト スイープを防ぎます：

- ポートスキャンは、ネットワーク上の開いたポートを探します。攻撃時にエクスプロイトするアクティブなポートを探り当てることを目的として、ポートスキャン ツールがホスト上のポート番号の範囲をクライアントにリクエストします。ゾーン プロテクション プロファイルは TCP および UDP ポート スキャンを防ぎます。

- ホスト スイープは複数のホストを調査し、特定のポートが開かれており、脆弱であるかどうかを判断します。

ネットワーク セキュリティあるいはファイアウォールの効力を検査するペンテストなど、正当な目的のために偵察行為ツールを使うことができます。社内の IT 部門がペンテストを実施してネットワークの脆弱性を発見して修復できるよう、偵察行為防御から除外する IPアドレスあるいはネットマスク アドレス オブジェクトを最大 20 件まで指定できます。

偵察行為防御の設定時に、偵察トラフィック (ペン テスト トラフィックを除く) が設定済みのしきい値を超えたときに実行するアクションを設定できます。偵察行為をブロックする前に分析目的でいくつかのパケットをログに記録するためのデフォルトの**Interval (**間隔**)**および**Threshold (**しきい値**)**を保持します。

パケットベース攻撃防御パケットベースコウゲキボウギョ

パケット ベースの攻撃には様々な形態があります。ゾーン プロテクション プロファイルは IP、TCP、ICMP、IPv6 および ICMPv6 パケット ヘッダをチェックし、次の方法でゾーンを保護します。

- 好ましくない特性を持つパケットをドロップします。
- ゾーンへの侵入を許可する前に、好ましくないオプションをパケットから取り除きます。

パケット ベースの攻撃保護の設定の場合、パケットタイプごとにドロップ特性を選択します。各 IP プロトコルのベストプラクティス：

- **IP Drop (IP** ドロップ**)**—**Unknown (**未知**)**および**Malformed (**不正な形式**)**のパケットをドロップします。また、**Strict Source Routing (**ストリクト ソース ルーティング**)**および**Loose Source Routing (**ルーズ ソース ルーティング**)**もドロップします。これは、これらのオプションにより、宛先 IP アドレスを一致条件として使用するセキュリティポリシールールを攻撃者がバイパスできるようになるためです。内部ゾーンについてのみ**Spoofed IP Address (**なりすまし **IP** アドレス**)**をチェックし、ファイアウォールのルーティングテーブルにマッチする送信元アドレスを持つトラフィックだけがゾーンにアクセスできるようにします。
- **TCP Drop (TCP** ドロップ**)**—デフォルトの**TCP SYN with Data (**データを伴う **TCP SYN)**および**TCP SYNACK with Data (**データを伴う **CP SYNACK)**ドロップを維持し、**Mismatched overlapping TCP segment (**一致しない **TCP** 重複セグメント**)**および**Split Handshake (**スプリット ハンドシェイク**)**パケットをドロップし、パケットから**TCP Timestamp (TCP** タイムスタンプ**)**をはぎ取ります。

> ***Rematch Sessions (***セッションの再マッチ***)***を有効化（***Device (***デバイス***) > Setup (***セットアップ***) > Session (***セッション***) > Session Settings (***セッション設定***)***）することが、コミット済みの新たな設定あるいは編集済みのセキュリティポリシールールを既存のセッションに適用する際のベストプラクティスになります。しかし、ゾーンでトンネル コンテンツ検査の設定を行い、***Rematch Sessions (***セッションに再マッチ***)***が有効な場合、***Reject Non-SYN TCP (***非 ***SYN TCP*** を拒否**)**を無効化（選択内容を***Global (***グローバル**)***から***No (***いいえ**)***に変更）する必要もあります。そうしなければ、トンネル コンテンツ検査ポリシーを有効化あるいは編集する際、ファイアウォールがすべての既存のトンネル セッションをドロップします。ゾーン プロテクション プロファイルを別途作成し、トンネル コンテンツ検査ポリシーを持つゾーンでのみ、***Rematch Sessions (***セッションに再マッチ***)***が有効な場合のみ***Reject Non-SYN TCP (***非 ***SYN TCP*** を拒否**)**を無効化します。

- **ICMP Drop (ICMP** ドロップ**)**—ICMP パケットのドロップは ICMP の使用方法（あるいは ICMP を使用するかどうか）によって左右されるため、標準的なベストプラクティスはありません。例えば、ping アクティビティをブロックする場合、**ICMP Ping ID 0**をブロックできます。
- **IPv6 Drop (IPv6** ドロップ**)**—コンプライアンスが関わる場合、コンプライアンスを満たしていないルーティング ヘッダー、拡張子などを持つパケットをファイアウォールに必ずドロップさせます。
- **ICMPv6 Drop (ICMPv6** ドロップ**)**—コンプライアンスが関わる場合、パケットがセキュリティ ポリシー ルールにマッチしない際にファイアウォールに必ず特定のパケットをドロップさせます。

プロトコル保護

プロトコル保護はゾーン プロテクション プロファイル内で、非 IP プロトコルベースの攻撃を防止します。プロトコル保護を有効化すれば、レイヤー 2 VLAN あるいはバーチャル ワイヤ上のセキュリティ ゾーン間、あるいはレイヤー 2 VLAN 上の単一のゾーン内のインターフェイス間で非 IP プロトコルをブロックあるいは許可できます（レイヤー 3 インターフェイスおよびゾーンは非 IP プロトコルをドロップするため、非 IP プロトコル保護は適用されません）。 プロトコル保護の設定あまり安全でないプロトコルがゾーン内のインターフェイスあるいはゾーンに侵入するのを防ぐことで、セキュリティリスクを減らし、コンプライアンス要件を満たします。

デフォルトのイントラゾーンはセキュリティポリシー ルールを許可するため、同じゾーン内の非 *IP* プロトコルが任意のレイヤー *2* インターフェイスから別のところに移動するのを防ぐゾーン プロテクション プロファイルを設定しない場合、ファイアウォールはトラフィックを許可します。ゾーン内でLLDP などのプロトコルをブロックするゾーン プロテクション プロファイルを作成し、他のゾーンのインターフェイス経由で到達できるネットワークの探査を防ぎます。

ネットワーク上でどの非 IP プロトコルが実行されているのか調査する必要がある場合、NetFlow、Wireshark、あるいはその他のサードパーティ製の監視ツールなどを使ってネットワーク上の非 IP プロトコルを探します。ブロックあるいは許可できる IP 以外のプロトコルの一部の例として、LLDP、NetBEUI、Spanning Tree や、Generic Object Oriented Substation Event（GOOSE）などの Supervisory Control and Data Acquisition（SCADA）システムが挙げられます。

Exclude List (除外リスト**)**あるいは**Include List (**許可リスト**)**を作成してゾーンのプロトコル保護を構成します。**Exclude List (**除外リスト**)**はブロックリストです。ファイアウォールは **Exclude List (**除外リスト**)** に追加されたすべてのプロトコルをブロックし、他のプロトコルはすべて許可します。**Include List (**許可リスト**)**は許可リストです。ファイアウォールはリストで指定されたプロトコルのみを許可し、他のプロトコルはすべてブロックします。

プロトコル保護では、除外リストではなく許可リストを使用してください。許可リストは許可したい具体的なプロトコルだけを許可し、必要でない、あるいはネットワーク上に存在することを知らなかったプロトコルをブロックするため、攻撃の入り口を狭めつつ未知のトラフィックをブロックできます。

リストは最大 64 の Ethertype 項目をサポートでき、そのそれぞれが IEEE の 16 進数 Ethertype コードで識別されます。他にも、Ethertype コードのソースは standards.ieee.org/develop/

regauth/ethertype/eth.txt および http://www.cavebear.com/archive/cavebear/Ethernet/type.html があります。集約イーサネット（AE）インターフェイスを持つゾーン上の非 IP プロトコル用にゾーン プロテクションを設定する際、各 AE インターフェイスのメンバーはグループとして扱われるため、いずれか一つの AE インターフェイスのメンバー上の非 IP プロトコルのみをブロックしたり許可したりすることはできません。

プロトコル保護では、*IPv4*（*Ethertype 0x0800*）、*IPv6*（*0x86DD*）、*ARP*（*0x0806*）、あるいは *VLAN* タグが付いたフレーム（*0x8100*）をブロックできません。ユーザーが明示的にリストに追加せずとも、ファイアウォールは***Include List (***許可リスト**)**に含まれるそれら *4* つの *Ethertype* を常に暗黙的に許可し、それらを***Exclude List (***除外リスト**)**に追加できなくします。

イーサネット SGT 保護

Cisco TrustSec ネットワークでは、Cisco Identity Services Engine (アイデンティティ サービス エンジン: ISE) が、16 bit (ビット- bit) のレイヤー2 Security Group Tag (セキュリティ グループ タグ; SGT) を、ユーザーまたはエンドポイントのセッションに割り当てます。ファイアウォールが Cisco TrustSec ネットワークの一部である場合、イーサネット SGT 保護を使用してゾーン プロテクション プロファイルを作成できます。ファイアウォールは、802.1Q (Ethertype 0x8909) のヘッダーで、特定のレイヤー2 Security Group Tag (セキュリティ グループ タグ; SGT) 値を検査し、SGT がインターフェースに適用されたゾーン プロテクション プロファイル用に設定したリストと一致する場合に、パケットをドロップできます。ゾーンへのアクセスを拒否したい SGT 値を決定します。

パケット バッファ保護

パケット バッファ保護は、ファイアウォールのパケット バッファを上回って正当なトラフィックをドロップさせることができる単一セッション DoS 攻撃から、ファイアウォールおよびネットワークを保護します。ゾーン プロテクション プロファイルや DoS 保護プロファイルあるいはポリシールール内でパケット バッファ保護を設定しませんが、パケット バッファ保護は入力ゾーンを保護します。より細かなゾーンおよび DoS 保護は新規セッション（接続）に、グローバルなパケット バッファ保護は既存のセッションに適用されます。

firewall全体を保護するためにグローバルにパケット バッファ保護の設定し、各ゾーンでPacket Buffer Protectionを有効にしてゾーンを保護します。

- グローバル パケット バッファ保護—ファイアウォールはすべてのゾーン（ゾーンでパケット バッファ保護が有効になっているかによらず）からのセッション、およびそれらのセッションによるパケット バッファの利用方法を監視します。パケット バッファ保護をグローバルに設定（**Device (**デバイス**)** > **Setup (**セットアップ**)** > **Session Settings**セッション設定）してファイアウォールを保護し、個々のゾーンで有効化する必要があります。パケット バッファの消費量が設定済みの**Activate (**アクティベート**)**パーセントに達すると、ファイアウォールはランダム早期ドロップ（RED）を使用して問題のセッションから来るパケットをドロップします（ファイアウォールがグローバル レベルでセッション全体をドロップすることはありません）。
- ゾーン単位のパケット バッファ保護—各ゾーンでパケット バッファ保護を有効化（**Network (**ネットワーク**)** > **Zones (**ゾーン**)**）し、2 つ目の保護の層を形成します。パケット バッファの

消費量が**Activate (**アクティベート**)**のしきい値を超え、グローバルな保護が RED をセッション トラフィックに適用し始めると、**Block Hold Time (**ブロック ホールド タイム**)**のタイマーが起動します。**Block Hold Time (**ブロック ホールド タイム**)**は、ファイアウォールがセッション全体をブロックするまで、問題のセッションが継続できる時間を秒単位で示します。問題のセッションは**Block Duration (**ブロック期間**)**が終了するまでブロックされたままになります。

パケットバッファ保護をゾーンでアクティブにするには、グローバルに有効にする必要があります。

パケット バッファ保護は2種類あります：

- バッファ使用率基準のパケット バッファ保護
- レイテンシ基準のパケット バッファ保護

バッファ使用率基準のパケット バッファ保護

バッファ使用率基準のパケット バッファ保護は、デフォルトで有効になっています。一定期間（少なくとも 7 営業日ですが、測定期間が長いほどベースラインの精度が向上します）ファイアウォールのパケット バッファの使用率のベースラインを測定し、典型的な使用状況を把握してください。

指定した期間のパケットバッファ使用率を確認するには (またはパケット バッファの 2% 以上を使用する上位 5 つのセッションを確認するには)、操作可能な CLI コマンドを使用します:

```
admin1138@thxvm
```

show running resource-monitor [ing resource-monitor [ing backlog | day | hour | ingress-backlog | minute| < second week]1}CLIコマンドは、特定の期間のバッファ使用率のスナップショットを提供しますが、自動的または継続的ではありません。継続的なパケット バッファ使用率の測定を自動化して、動作の変化や異常なイベントを監視できるようにするには、スクリプトを使用します。Palo Alto Networks アカウント チームは、独自のスクリプトを開発するために変更できるサンプル スクリプトを提供できます。ただし、スクリプトは公式にはサポートされておらず、スクリプトの使用または変更に利用できる技術サポートはありません。

ベースラインの測定値が継続して異常に高いパケット バッファの使用率を示す場合、通常のトラフィック負荷に対してファイアウォールのキャパシティが小さ過ぎることになります。この場合、ファイアウォールのデプロイメントのサイズ変更をご検討ください。あるいは、パケット バッファ保護のしきい値を慎重に調整し、影響を受けたバッファがオーバーフローしないようにする（また、正当なトラフィックがドロップされないようにする）必要があります。ファイアウォールがデプロイ環境に適したサイズであれば、バッファの使用量を急激に増やせるのは攻撃者だけ、ということになります。

ファイアウォールのパケット バッファをオーバーランさせると、ファイアウォールのパケット転送能力が悪影響を受けます。バッファが一杯である時、攻撃を受けているインターフェイスだけでなく、すべてのインターフェイス上のファイアウォールにパケットが侵入できなくなります。

しきい値の設定のベストプラクティス：

- **Alert (アラート)**および**Activate (アクティベート)**—デフォルトのしきい値から始め、パケット バッファの使用率を監視し、しきい値を必要に応じて調整します。**Alert (アラート)** しきい値のデフォルトは 50% です。パケットバッファの使用率がしきい値を 10 秒以上超えた場合、ファイアウォールは 1 分ごとにシステム ログにアラート エントリを作成します。**Activate (アクティベート)** しきい値のデフォルトは80%です。このしきい値に到達すると、ファイアウォールは最も危険性の高いセッションの軽減を開始します。ファイアウォールのサイズが正しい場合、バッファの使用率は 50% を大きく下回るはずです。
- **Block Hold Time (ブロック ホールド タイム)**—パケット バッファの使用率が**Activate (アクティベート)**のしきい値を発動する際、ファイアウォールがセッション全体をブロックするまでに、問題のセッションが存続できる時間を設定するのが**Block Hold Time (ブロック ホールド タイム)**です。**Block Hold Time (ブロック ホールド タイム)**の間、ファイアウォールは問題のセッションのパケットに RED を適用し続けます。デフォルトの**Block Hold Time (ブロック ホールド タイム)**のしきい値（60 秒）から始め、パケット バッファの使用率を監視し、必要に応じてしきい値を調整してください。**Block Hold Time (ブロック ホールド タイム)**が終了する前にパケット バッファの使用率が**Activate (アクティベート)**のしきい値を下回ると、タイマーがリセットされ、**Activate (アクティベート)**のしきい値を再び超えるまで停止したままになります。**Block Hold Time (ブロック ホールド タイム)**を増やすと問題のセッションに対するペナルティが大きくなり、これを減らすと問題のセッションに対するペナルティが小さくなります。
- **Block Duration (ブロック期間)**—**Block Hold Time (ブロック ホールド タイム)**が終了する際、ファイアウォールは**Block Duration (ブロック期間)**で定義された期間、問題のセッションをブロックします。デフォルトのしきい値（3600 秒）から始め、パケット バッファの使用率を監視し、必要に応じてしきい値を調整してください。ゾーンでパケット バッファ保護を有効化すると、ある IP アドレスから発生したいずれか一つのセッションのパケット バッファ使用率が高すぎる場合でも、その IP アドレスから来るすべてのセッションが**Block Duration (ブロック期間)**の影響を受けます。IP アドレスを 1 時間（3600 秒）ブロックするのはペナルティが大きすぎると思う場合は、**Block Duration (ブロック期間)**を許容できる値まで減らしてください。

パケット バッファ保護は各セッションのバッファの使用率を監視するだけでなく、特定の基準を満たした場合に IP アドレスをブロックすることもできます。ファイアウォールがパケット バッファを監視している間に、単体では攻撃とはみなされない複数のセッションを急激な速度で作成する送信元 IP アドレスを検出すると、ファイアウォールは設定済みの**Block Duration (ブロック期間)**の間、その IP アドレスをブロックします。

ネットワーク アドレス変換（NAT）（インターネットに向かうトラフィックを送信元 *NAT* を使って変換した外部ソース）は *IP* アドレス変換のおかげで、パケット バッファの使用率をより大きく見せることができます。これが生じる場合、個々のセッションにペナルティを課すものの、その背後にある *IP* アドレスにはペナルティを課さない形でしきい値を調整します（そのため、同じ *IP* アドレスから来る他のセッションは影響を受けなくなります）。そうするには、***Block Hold Time (ブロック ホールド タイム)***を減らしてバッファを高速に使用し過ぎる個々のセッションをファイアウォールにブロックさせ、***Block Duration (ブロック期間)***を減らして背後にある *IP* アドレスが不当にペナルティを課されないようにします。

レイテンシ基準のパケット バッファ保護

使用率に基づくパケット バッファ保護の代わりに、ファイアウォールの輻輳を示すデータプレーン パケット バッファリングによって引き起こされるパケット レイテンシを基準とするパケット バッファ保護をトリガできます。このようなパケット バッファ保護は、輻輳を警告し、パケットに対してランダム早期ドロップ (RED) を実行することにより、ヘッドオブライン ブロッキングを軽減します。レイテンシ基準のパケット バッファ保護は、レイテンシの影響を受けやすいプロトコルまたはアプリケーションが影響を受ける前に保護をトリガーできます。

トラフィックに遅延の影響を受けやすいプロトコルまたはアプリケーションが含まれている場合、レイテンシに基づくパケット バッファ保護は、バッファ使用率に基づくパケット バッファ保護よりも有用です。

レイテンシ基準のパケット バッファ保護には、**Latency Alert (**レイテンシ アラート**)** しきい値 (ミリ秒単位) の設定が含まれます。このしきい値を超えると、ファイアウォールはアラート ログ イベントの生成を開始します。**Latency Activate (**レイテンシ アクティベート**)** しきい値は、ファイアウォールが着信パケットで RED をアクティブ化し、アクティブ化ログの生成を開始するタイミングを示します。**Latency Max Tolerate (**レイテンシ最大許容**)** しきい値は、ファイアウォールがほぼ 100% のドロップ確率で RED を使用する場合を示します。

Block Hold Time (ブロック保留時間**)** および **Block Duration (**ブロック期間**)** の設定は、使用率に基づくパケット バッファ保護の場合と同じように、レイテンシ基準パケット バッファ保護のために機能します。

DoS プロテクション プロファイルおよびポリシールール

DoS 保護プロファイルおよび DoS 保護ポリシールールは協力して、重要な特定のリソースのグループおよび個々の重要なリソースをセッション フラッドから守ります。DoS 保護は特定のシステム、特に WEB サーバーやデータベースサーバーなど、ユーザーがインターネットからアクセスする、攻撃対象になりやすい重要なシステムに対して、ゾーン全体をフラッド攻撃から守るゾーン プロテクション プロファイルよりも細かな防御を提供します。ゾーン プロテクション プロファイルだけを適用すると、1 秒あたりの合計接続数（CPS）がゾーンの**Activate (**アクティベート**)**および**Maximum (**最大**)**レートを超過しない場合に、ゾーン内の特定のシステムに対する DoS 攻撃が成功するため、両方のタイプの保護を適用してください。

DoS 保護はリソースを多く消費するため、重要なシステムでのみ使用してください。ゾーン プロテクション プロファイルと同様に、DoS 保護プロファイルもフラッドのしきい値を指定します。DoS 保護ポリシールールは、DoS 保護を適用するデバイス、ユーザー、ゾーン、サービスを決定します。

DoS 保護およびゾーン プロテクションを構成することに加え、各セキュリティポリシールールに対してベストプラクティスの脆弱性制御プロファイルを適用し、*DoS* 攻撃を防止します。

- 分類化および集約 DoS 保護
- DoS 防御プロファイル
- Dos プロテクション ポリシー ルール

分類化および集約 DoS 保護

DoS 保護を設定するときには、集約と分類を設定し、1 つのプロファイルまたは各タイプのプロファイルを 1 つずつ適用できます。

- <41>Aggregate (集約)</41>—個々のデバイスではなく、DoS 保護ポリシールールで指定されているデバイスのグループ全体に適用されるしきい値を設定し、許容される接続トラフィックの大部分を単一のデバイスが受信できるようにします。例えば、**Max Rate (最大レート)**が 20,000 CPS である場合、グループ用の合計 CPS は 20,000 であり、他のデバイスが接続されていなければ、個々のデバイスが最大 20,000 CPS を受信できます。特定のサブネット、ユーザー、サービスに対してさらに制限を加えたい場合、集約 DoS 保護ポリシーにより、重要な特定のデバイス グループを全般的に保護する層を追加できます（インターネットの境界にある DDoS デバイスおよびゾーン プロテクション プロファイルの後）。
- **Classified (分類化)**—DoS 保護ポリシールールで指定された個々のデバイスに対して適用されるフラッドのしきい値を設定します。例えば、<48>Max Rate (最大レート)</48>を 5,000 CPS に設定すると、ルールで指定されている各デバイスは、新しい接続をドロップする前に最大 5,000 CPS を許容できます。分類化のしきい値は個々のデバイスに適用されるため、分類化 DoS 保護ポリシールールを複数のデバイスに適用する場合、ルールが対象とする各デバイスのキャパシティ、CPS レートの制御方法が同様のものでなければなりません。分類化プロファイルは、個々の重要なリソースを保護します。

  分類化 DoS 保護プロファイルと共に DoS 保護ポリシールールを構成する際（**Option/Protection (オプション/保護)** > **Classified (分類化)** > **Address (アドレス)**）、**source-ip-only**、**destination-ip-only**、あるいは**scr-dest-ip-both**とのマッチに基づき、インバウンドの接続数がプロファイルのしきい値に加味されるかどうかを**Address (アドレス)**フィールドを使って指定します。カウンターはリソースを消費するため、アドレスのマッチ数をカウントする方法によって、ファイアウォール リソースの消費量が左右されます。分類化 DoS 保護を使えば次のことが可能です：

  - 重要な個々のデバイス、特に WEB サーバー、データベースサーバー、DNS サーバーなど、ユーザーがインターネット経由でアクセスし、攻撃の対象になりやすいサーバーを保護します。適切なフラッドおよびリソース保護のしきい値を分類化 DoS 保護プロファイルで設定します。IP アドレスをルールの宛先条件として追加し、**Address (アドレス)**を**destination-ip-only**に設定することで、各サーバーの IP アドレスにプロファイルを適用する DoS 保護ポリシールールを作成します。

    ファイアウォールはインターネット上のすべての *IP* アドレスの候補を対象としてカウンターを保存できる容量を持っていないため、インターネットに接続されたゾーンについては、分類化 *DoS* 保護ポリシールールで***source-IP-only***や***src-dest-ip-both***を使用しないでください。内部ゾーンあるいは同じゾーン ルールの場合のみ、ソース *IP* のしきい値カウンターをインクリメントします。境界ゾーンでは*<70>destination-ip-only</70>*を使用します。
  - 候補のホストあるいはホスト グループの CPS レートを監視します（ホストを含むゾーンをインターネットに接続することはできません）。分類化 DoS 保護プロファイルで適切なアラームのしきい値を設定し、ホストが異常に大量の接続を開始した場合に通知させます。プロファイルを個々の送信元あるいは送信元アドレス グループに適用する DoS 保護ポリシールールを作成し、**Address (アドレス)**を**source-ip-only**に設定します。大量の新しい接続を開始したホストを調査してアラームを切ります。

分類化プロファイル用に**Address (アドレス)**（**source-ip-only**、**destination-ip-only**、あるいは**src-dest-ip-both**）を設定する方法は、DoS 保護の目的、保護する対象、保護対象のデバイスがインターネットに接続されたゾーン内にあるかどうかで異なります。

カウンターは送信元および宛先 *IP* アドレスのいずれかではなく両方のリソースを消費するため、***Address (アドレス)***が***src-dest-ip-both***である場合、ファイアウォールは***source-IP-only***や***destination-ip-only***の場合よりも多くのリソースを使います。

集約および分類化 DoS 保護プロファイルの両方を同じ DoS 保護ポリシールールに適用する場合、ファイアウォールは最初に集約プロファイルを、次に必要に応じて分類化プロファイルを適用します。例えば、DoS 保護ポリシールール内で両方のタイプのプロファイルを使って 5 つの WEB サーバーのグループを保護します。グループを対象にした合計値が 25,000 CPS の**Max Rate (最大レート)**に達すると、集約プロファイル構成は新しい接続をドロップします。分類化プロファイル構成は 6,000 CPS の**Max Rate (最大レート)**に達すると、グループ内のいずれかの WEB サーバーへの新しい接続をドロップします。新しい接続トラフィックが**Max Rate (最大レート)**のしきい値を超えるケースは 3 つあります：

- 新しい CPS レートが集約**Max Rate (最大レート)**を超え、分類化**Max Rate (最大レート)**を超過しない場合。この場合、ファイアウォールは集約プロファイルを適用し、設定済みのブロック期間中、すべての新しい接続をブロックします。
- 新しい CPS レートが集約 **Max Rate (最大レート)** を超えず、いずれかのウェブサーバーへの CPS が分類化 **Max Rate (最大レート)** を超過する場合。この場合、ファイアウォールは集約プロファイルをチェックし、グループのレートが 25,000 CPS 未満であることを確認するため、それに従ってファイアウォールは新しい接続をブロックしません。次に、ファイアウォールは分類化プロファイルをチェックし、特定のサーバーのレートが 6,000 CPS を超えていることを確認します。ファイアウォールは分類化プロファイルを適用し、設定済みのブロック期間中、そのサーバーへの新しい接続をブロックします。グループ内の他のサーバーは分類化プロファイルの**Max Rate (最大レート)**の範囲内であるため、それらを対象にしたトラフィックは影響を受けません。
- 新しい CPS レートが集約**Max Rate (最大レート)**を超え、さらにいずれかの WEB サーバーの分類化**Max Rate (最大レート)**を超過する場合。この場合、ファイアウォールは集約プロファイルをチェックし、グループのレートが 25,000 CPS を超過していることを確認するため、それに従ってファイアウォールは新しい接続をブロックしてグループの合計 CPS を制限します。それからファイアウォールは分類化プロファイルをチェックし、特定のサーバーのレートが 6,000 CPS を超過していることを確認します（そのため、集約プロファイルがグループの合計上限を適用していますが、それでも対象のサーバーを保護するのに十分ではありませんでした）。ファイアウォールは分類化プロファイルを適用し、設定済みのブロック期間中、そのサーバーへの新しい接続をブロックします。グループ内の他のサーバーは分類化プロファイルの**Max Rate (最大レート)**の範囲内であるため、それらを対象にしたトラフィックは影響を受けません。

集約および分類化 *DoS* 保護プロファイルの両方を同じトラフィックに適用する場合、両方のプロファイルを同じ *DoS* 保護ポリシールールに適用する必要があります。集約プロファイルをいずれかのルールに、分類化プロファイルを別のルールに適用する場合、トラフィックが最初の *DoS* 保護ポリシールールにマッチした時点で、ファイアウォールはそのルールで指定されている***Action* (アクション)**を実行し、後続のルールとトラフィックを照らし合わせることはないため、つまり、トラフィックが *2* つ目のルールにマッチしてファイアウォールがそのアクションを適用することは決してないため、両方のプロファイルが全く同じトラフィックを指定している場合でも、ファイアウォールはいずれか一方のプロファイルだけを適用します。（これは、セキュリティポリシールールと同じ動作になります）

DoS 防御プロファイル

DoS 保護プロファイルは新規セッション IP フラッド攻撃を防止するしきい値を設定し、リソース保護（特定のエンドポイントおよびリソースの最大同時セッション数の制限）を提供します。DoS 保護プロファイルは特定のグループ（分類化プロファイル）およびデバイスのグループ（集約プロファイル）を SYN、UDP、ICMP、ICMPv6、およびその他の IP フラッド攻撃から保護します。DoS 保護プロファイル内のフラッド防御のしきい値は、ゾーン プロテクション プロファイル内のhttps://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/dos-protection-against-flooding-of-new-sessionsと同様に設定しますが、ゾーン プロテクション プロファイルが入力ゾーン全体を保護する一方、DoS 保護プロファイルおよびポリシールールはより細かく対象を指定でき、単一のデバイス（IP アドレス）に分類化することさえ可能です。ファイアウォールはデバイスのグループ（集約プロファイル）への集約された 1 秒あたりの接続数（CPS）を計測したり、個々のデバイスへ（分類化プロファイル）の CPS を計測したりします。

ファイアウォールのデータプレーン *CPU* 使用量を測定・監視し、*DoS*、ゾーン プロテクション、そして復号化などの *CPU* サイクルを消費するその他の機能をサポートできるよう、各ファイアウォールが適切にサイジングされていることを確認します。*Panorama* を使ってファイアウォールを管理する場合、デバイス監視（***Panorama* > *Managed Devices* (管理対象デバイス) > *Health* (ヘルス) > *All Devices* (すべてのデバイス)**）に管理対象の各ファイアウォールの *CPU* およびメモリ使用量が表示されます。また、各ファイアウォールで典型的に利用できるキャパシティを把握する際に役立つ、*90* 日間の平均およびピーク時の *CPU* 使用状況の傾向を確認することもできます。

各フラッド タイプについて、デバイスのグループ（集約）あるいは個々のデバイス（分類化）への新しい CPS のしきい値を 3 つ、および**Block Duration (ブロック期間)**を設定し、また SYN フラッドの場合はドロップ**Action (アクション)**を設定できます：

- **Alarm Rate (アラーム レート)**—新しい CPS がこのしきい値を超過すると、ファイアウォールが DoS アラームを生成します。分類化プロファイルの場合、レートをデバイスの平均 CPS レートよりも 15～20% 高く設定し、通常の変動でアラームが発生しないようにします。集約プロファイルの場合、レートをグループの平均 CPS レートよりも 15～20% 高く設定します。
- **Activate Rate (アクティベート レート)**—新しい CPS がこのしきい値を超過すると、CPS レートがしきい値を下回るまでフラッドを抑えるために、ファイアウォールが新しい接続をドロップし始めます。分類化プロファイルの場合、**Max Rate (最大レート)**は保護中のデバイス

が許容できる cps 速度にする必要があります（**Max Rate (最大レート)**が重要なデバイスにフラッドを生じさせることはありません）。トラフィックが**Max Rate (最大レート)**に達する前にファイアウォールがトラフィックをドロップし始めるために RED あるいは SYN を使用しないよう、**Activate Rate (アクティベート レート)**は**Max Rate (最大レート)**と同じしきい値に設定できます。**Max Rate (最大レート)**に達する前にトラフィックをドロップしたい場合のみ、**Activate Rate (アクティベート レート)**を**Max Rate (最大レート)**よりも低く設定します。集約プロファイルの場合、グループが RED を使ってフラッドを抑え始める平均ピーク時 CPS レートよりもわずかに高いしきい値を設定します。

- **Max Rate (最大レート)**—新しい CPS がこのしきい値を超過すると、ファイアウォールは指定された**Block Duration (ブロック期間)**の間、問題の IP アドレスからの新規接続をすべてブロック（ドロップ）します。分類化プロファイルの場合、保護中のデバイスの能力に基づいて**Max Rate (最大レート)**のしきい値を設定し、CPS レートがフラッドを発生させないようにしてください。集約プロファイルの場合、グループの能力の 80〜90% に設定します。
- **Block Duration (ブロック期間)**—新しい CPS が**Max Rate (最大レート)**を超過すると、ファイアウォールは問題の IP アドレスからの新規接続をブロックします。**Block Duration (ブロック期間)**は、対象の IP アドレスの新規接続をファイアウォールがブロックし続ける時間を指定します。ファイアウォールは新規接続をブロックしますが、インバウンド接続は加味せず、しきい値のカウンターをインクリメントすることはありません。分類化および集約プロファイルについて、デフォルトの値（300 秒）を使って、送信元からの正当なセッションに長くペナルティを課すことなく、攻撃中のセッションをブロックします。

SYN フラッド防御は、ドロップ***Action (アクション)***を設定できる唯一のタイプです。まずは***Action (アクション)***を***SYN Cookies***に設定します。*SYN Cookies* は正当なトラフィックを公正に扱い、*SYN* ハンドシェイクに失敗したトラフィックにみをドロップします。それに対し、ランダム早期ドロップを使用するとトラフィックがランダムにドロップされるため、*RED* は正当なトラフィックに影響を与えることがあります。しかし、*SYN Cookies* の場合、ファイアウォールがターゲット サーバーのプロキシとして動作し、そのサーバーの *3* 方向ハンドシェイクを制御するため、リソース消費量が大きくなります。正当なトラフィック（*SYN Cookies*）をドロップさせず、ファイアウォール リソースを保つ（*RED*）というバランスを取ることになります。ファイアウォールを監視し、*SYN Cookies* がリソースを消費し過ぎている場合は、*RED* に切り替えます。ファイアウォールの前面に専用の *DDoS* 保護デバイスがない場合、ドロップ メカニズムとして必ず *RED* を使用してください。

DoS 保護プロファイルが正当なトラフィックを意図せずドロップすることがないよう、デフォルトのしきい値は高く設定されています。接続トラフィックを監視し、しきい値をネットワークに適した値に調整します。まずは各フラッド タイプの平均およびピーク時の CPS のベースラインを計測し、保護したい重要なデバイスの通常のトラフィックの状態を把握します。通常時のトラフィック負荷はある程度上下するため、あまり積極的に接続をドロップしようとしないのがベストです。ネットワークの拡大に合わせ、必要に応じてフラッドのしきい値を監視・調整してください。

フラッドのしきい値を設定する別の方法は、ベースラインの測定値を使って許可したい最大 CPS を設定し、そこから遡って合理的なフラッド抑制アラームおよびアクティベーション レートを割り出すことです。

複数のデータプレーン プロセッサ（*DP*）を持つファイアウォールは、*DP* 全体に接続を分配します。通常、ファイアウォールは *CPS* のしきい値設定を *DP* 全体に対して均等に割ります。例えば、ファイアウォールに *5* つの *DP* があり、***Alarm Rate (***アラーム レート*)***を *20,000 CPS* に設定する場合、各 *DP* の***Alarm Rate (***アラーム レート*)***が *4,000 CPS*（*20,000 / 5 = 4,000*）になるため、*DP* の新規セッションが *4,000* を超えると、その *DP* の***Alarm Rate (***アラーム レート*)***のしきい値が発動します。

IP フラッドのしきい値を設定することに加え、DoS 保護プロファイルを使って、大量のホスト（ボット）ができるだけ多くのセッションを確立してターゲットのリソースを消費するセッション枯渇攻撃を検出・防止します。プロファイルの**Resources Protection (**リソース保護**)**タブで、プロファイルを割り当てる DoS 保護ポリシールールで定義されたデバイスが受信できる最大同時セッション数を設定できます。同時セッションの数が上限数に達すると、新規セッションがドロップされるようになります。

設定する最大同時セッション数は、ネットワークの状況によって異なります。保護中のリソース（プロファイルを付与する DoS 保護ポリシールールで定義）が対応できる同時セッション数を把握してください。しきい値をリソースの能力のおよそ 80% に設定してから、監視して必要に応じてしきい値を調整します。

集約プロファイルの場合、**Resources Protection (**リソース保護**)**のしきい値はポリシールールで定義されたすべてのデバイスのトラフィックに適用されます（送信元および宛先）。分類化プロファイルの場合、**Resources Protection (**リソース保護**)**のしきい値は、分類化ポリシールールが送信元 IP のみ、宛先 IP のみ、あるいは送信元および宛先 IP の両方に適用されるのかに応じて、トラフィックに適用されます。

Dos プロテクション ポリシー ルール

DoS 保護ポリシールールは、ファイアウォールが DoS 保護を適用するシステム（DoS 保護ポリシールールに付与する DoS 保護プロファイルで設定されたフラッドのしきい値）、ルールで定義された条件にトラフィックが一致する際に行うアクション、DoS トラフィックをログに記録する方法を制御します。DoS 保護はファイアウォールのリソースを消費するため、重要な特定のリソース、特に WEB サーバーやデータベースサーバーなど、ユーザーがインターネットからアクセスする攻撃対象になりやすいリソースをセッション フラッドから保護する目的でのみ使用してください。ゾーン プロテクション プロファイルを使用してゾーン全体をフラッドやその他の攻撃から保護します。保護対象を厳密かつ柔軟に定義できるよう、DoS 保護ポリシールールが細かな一致条件を提供します：

- 送信元ゾーン、インターフェイス、IP アドレス（リージョン全体を含む）、およびユーザー。
- 宛先ゾーン、インターフェイス、および IP アドレス（リージョン全体を含む）。
- サービス（ポートおよびプロトコル別）。DoS 保護は指定したサービスにのみ適用されます。しかし、サービスを指定してもサービスが許可されるわけではなく、他のすべてのサー

ビスが暗黙的にブロックされます。サービスを指定すると DoS 保護がそれらのサービスに制限されますが、他のサービスはブロックされません。

重要なサーバーで使用しているサービス ポートを保護することに加え、重要なサーバーの未使用のサービス ポートを *DoS* 攻撃から守ることもできます。これは、重要なシステムに対し、サービスを実行しているポートを保護する単一の *DoS* 保護ポリシールールおよびプロファイルを作成し、サービスを実行していないポートを保護する別の *DoS* 保護ポリシールールおよびプロファイルを作成することで実現できます。例えば、*80* や *443* など、*WEB* サーバーの通常のサービス ポートを単一のポリシー/プロファイルで保護し、その他すべてのサービス ポートを別のポリシー/プロファイルで保護することができます。*DoS* カウンターを実行することでパフォーマンスに影響を及ばさないよう、ファイアウォールのキャパシティにご注意ください。

トラフィックが DoS 保護ポリシールールにマッチすると、ファイアウォールは次の 3 つのうちいずれかのアクションを実行します。

- 拒否—ファイアウォールはアクセスを拒否し、DoS 保護プロファイルを適用しません。該当のルールと一致するトラフィックはブロックされます。
- 許可—ファイアウォールはアクセスを許可し、DoS 保護プロファイルを適用しません。該当のルールと一致するトラフィックは許可されます。
- 保護—特定の DoS 保護プロファイルあるいはプロファイルのしきい値をルールにマッチするトラフィックに適用することで、ファイアウォールは DoS 保護ポリシールールで定義されているデバイスを保護します。分類化および集約 DoS 保護に記載されているように、ルールには単一の集約 DoS 保護プロファイルおよび単一の分類化 DoS 保護プロファイルを持たせることができ、分類化プロファイルの場合、送信元 IP、宛先 IP、あるいは両方を使用してフラッドのしきい値をインクリメントすることができます。ルールにマッチする場合、インバウンド パケットは両方の DoS 保護プロファイルのしきい値に対してカウントされます。

ファイアウォールは、**Action (**アクション**)** が **Protect (**保護**)** である場合のみ、DoS 保護プロファイルを適用します。DoS 保護ポリシールールの **Action (**アクション**)** が **Protect (**保護**)** である場合は、ルール内で適切な集約および/または分類済み DoS 保護プロファイルを指定し、ルールにマッチするトラフィックにファイアウォールが DoS 保護プロファイルのしきい値を適用するようにします。大抵のルールは**Protect (**保護**)**ルールです。

Allow (許可**)**および**Deny (**拒否**)**アクションにより大規模なグループに例外を設けられますが、DoS 保護をトラフィックに適用しないでください。例えば、大抵のグループのトラフィックを拒否しつつ、そのトラフィックのサブセットを許可することができます。逆に、大抵のグループのトラフィックを許可しつつ、そのトラフィックのサブセットを拒否することもできます。

DoS 保護ポリシールールを有効にする**Schedule (**スケジュール**)**を設定できます（開始および終了時間、反復期間）。スケジュール設定のユースケースの一つとして、日あるいは週単位の異なる時間に別のフラッドのしきい値を適用することができます。例えば、日中と比べて夜間のトラフィックが極端に減るようなビジネスの場合、夜間よりも日中のフラッドのしきい値を高くするのが良いでしょう。また、別のユースケースとして、ファイアウォールが CPS レートをサポートしている場合、特別なイベント用に特別なしきい値をスケジュール設定することができます。

Log Forwarding (ログ転送**)**を設定して DoS 保護のログと他の脅威ログを別ければ、管理が容易になり、細かなレポートを行えるようになります。SNMP や Syslog サーバーなどのサーバーにロ

グを転送するだけでなく、DoS しきい値の違反イベントを管理者にメールで直接転送してください。ファイアウォールが適切にサイジングされているとすれば、しきい値の違反が頻繁に発生することはないため、攻撃の試みである可能性が高くなります。

ゾーン保護を設定してネットワーク セキュリティを向上

次の各トピックは、ゾーン プロテクション設定の例を示しています。

- 偵察行為防御の設定
- パケット ベースの攻撃保護の設定
- プロトコル保護の設定
- パケット バッファ保護の設定
- レイテンシ基準のパケット バッファ保護の設定
- イーサネット SGT 保護の設定

偵察行為防御の設定

firewall が対応する偵察の試行に応答して実行する次の偵察行為防御アクションのいずれかを構成します。

- 許可–ファイアウォールがホストスイープ偵察行為またはポートスキャンの続行を許可します。
- アラート–指定した時間間隔内でポートスキャンまたはホストスイープが設定済みのしきい値に達するたびにファイアウォールがアラートを生成します。アラートはデフォルトのアクションです。
- ブロック–指定した時間間隔が終わるまで、送信元から宛先へ向けた後続のパケットをファイアウォールがすべて廃棄します。
- ブロック**IP**–指定した **Duration**（持続時間） にわたり、ファイアウォールが後続のパケットをすべて廃棄します（範囲は1～ 3600、単位は秒数）。**Track By** （追跡区分）により、ファイアウォールが送信元をブロックするか、あるいは送信元-宛先間トラフィックをブロックするかを選択できます。

STEP 1 | 偵察行為防御を設定します。

1. **Network**（ネットワーク） > **Network Profiles**（ネットワーク プロファイル） > **Zone Protection**（ゾーン プロテクション）を選択します。
2. ゾーン プロテクション プロファイルを選択するか、新しいプロファイルを **Add** (追加) してその **Name** (名前) を入力します。
3. Reconnaissance Protection (偵察行為防御) タブで、防御対象のスキャンタイプを選択します。
4. 各スキャンについて **Action** (アクション) を選択します。Block IP (ブロック IP) を選択する場合、**Track By**（追跡区分）（source あるいは source-and-destination) および **Duration** (継続期間) も設定する必要があります。
5. **Interval** (間隔)（秒）を設定します。このオプションは、ポート スキャンおよびホスト スイープ検出の時間間隔を定義します。
6. **Threshold** (しきい値) を設定します。このしきい値は、上記で設定した、アクションをトリガーする時間間隔内に発生するポートスキャン イベント あるいはホスト スイープの数を定義します。

STEP 2 | （任意）送信元アドレス例外を設定します。

1. Reconnaissance Protection (偵察行為防御) タブで、宛先アドレス除外を **Add** (追加) します。
   1. 除外するアドレスの分かりやすい**Name** (名前) を入力します。
   2. Address Type (アドレス タイプ) を **IPv4** あるいは **IPv6** に設定し、アドレス オブジェクトを選択するか、IP アドレスを入力します。
   3. **OK** をクリックします。
2. **OK** をクリックしてゾーン プロテクション プロファイルを保存します。
3. 変更を **Commit** (コミット)します。

パケット ベースの攻撃保護の設定

ゾーンのセキュリティを強化するために、パケットベース攻撃防御パケットベースコウゲキボウギョ では、特定の特性を持つ IP、IPv6、TCP、ICMP、または ICMPv6 パケットをドロップするか、パケットから特定のオプションを削除するかを firewall がドロップするかを指定できます。

例えば、TCP 3 方向ハンドシェイクの間に、ペイロードにデータを含む TCP SYN および SYN-ACK パケットをドロップすることができます。デフォルト設定では、ゾーン プロテクション プロファイルはデータと共に SYN および SYN-ACK パケットをドロップするように設定されています（プロファイルをゾーンに割り当てる必要があります）。

TCP Fast Open オプション（RFC 7413）は、データを SYN および SYN-ACK パケットのペイロードに含めることで、接続のセットアップ速度を維持します。ゾーン プロテクション プロファイルは、TCP Fast Open オプションを使用するハンドシェイクを他の SYN および SYN-ACK パケットとは別に扱います。デフォルト設定では、ハンドシェイク パケットに有効な Fast Open の Cookie が含まれる場合、プロファイルがハンドシェイク パケットを許可するように設定されています。

PAN-OS 8.0 にアップグレードする際にすでに既存のゾーン プロテクション プロファイルがある場合、各プロファイルに *3* つのデフォルト設定が適用され、ファイアウォールがそれに従って動作するようになります。

PAN-OS 8.1.2 以降のリリースから、CLI コマンド（このタスクのステップ 4）を使用して、ファイアウォールが次のタイプのパケットを受信してドロップする際に脅威ログを生成できるようにすることで、これらの発生を容易に分析し、監査やコンプライアンスの要件を満たしやすくなります：

- Teardrop 攻撃
- Ping of Death を使用する DoS 攻撃

さらに、対応するパケット ベースの攻撃防御を有効化すれば、同じ CLI コマンドを使用して、ファイアウォールが次のタイプの脅威ログを生成できるようにすることもできます。

- フラグメント化された IP パケット
- IP アドレスの偽装
- 1024 バイトを超える ICMPパケット
- ICMP フラグメントを含むパケット
- エラーメッセージが組み込まれている ICMP パケット
- SYN パケットではない最初の TCP セッション用パケット

STEP 1 | ゾーン プロテクション プロファイルを作成し、パケット ベースの攻撃防止設定を行います。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **Zone Protection (ゾーン プロテクション)** を選択して新しいプロファイルを **Add (追加)** します。
2. プロファイルの **Name (名前)** を入力し、任意で **Description (説明)** を入力します。
3. **Packet Based Attack Protection (パケット ベースの攻撃防御)** を選択します。
4. 各タブ（**IP Drop (IP ドロップ)**、**TCP Drop (TCP ドロップ)**、**ICMP Drop (ICMP ドロップ)**、**IPv6 Drop (IPv6 ドロップ)**、and **ICMPv6 Drop (ICMPv6 ドロップ)**）で、ゾーンを保護するために適用したいパケット ベースの攻撃に対する保護設定を選択します。
5. **OK** をクリックします。

STEP 2 | 保護したいインターフェイスに割り当てられているセキュリティ ゾーンにゾーン プロテクション プロファイルを適用します。

1. **Network (ネットワーク)** > **Zones (ゾーン)** の順に選択し、ゾーン プロテクション プロファイルを割り当てるゾーンを選択します。
2. このゾーンに属す **Interfaces (インターフェイス)** を **Add (追加)** します。
3. **Zone Protection Profile (ゾーン プロテクション プロファイル)** については、先ほど作成したプロファイルを選択します。
4. **OK** をクリックします。

STEP 3 | 変更を **Commit (コミット)**します。

STEP 4 | （PAN-OS 8.1.2 以降のリリース）ファイアウォールが Teardrop 攻撃および Ping of Death を使用する DoS 攻撃についての脅威ログを生成し、また対応するパケット ベースの攻撃防止を有効化している場合に、先にリストアップしたタイプのパケットについての脅威ログを生成できるようにします（ステップ 1）。例えば、**Spoofed IP address (**なりすまし **IP** アドレス**)**用にパケット ベースの攻撃防止を有効化する場合、次の CLI を使用することで、ファイアウォールがなりすまし IP アドレスを持つパケットを受信およびドロップする際に脅威ログを生成できるようになります。

1. CLI へのアクセスを行います。
2. 運用 CLI コマンド **set** システム設定追加脅威ログ を使用します。デフォルトは**off (**オフ**)**です。

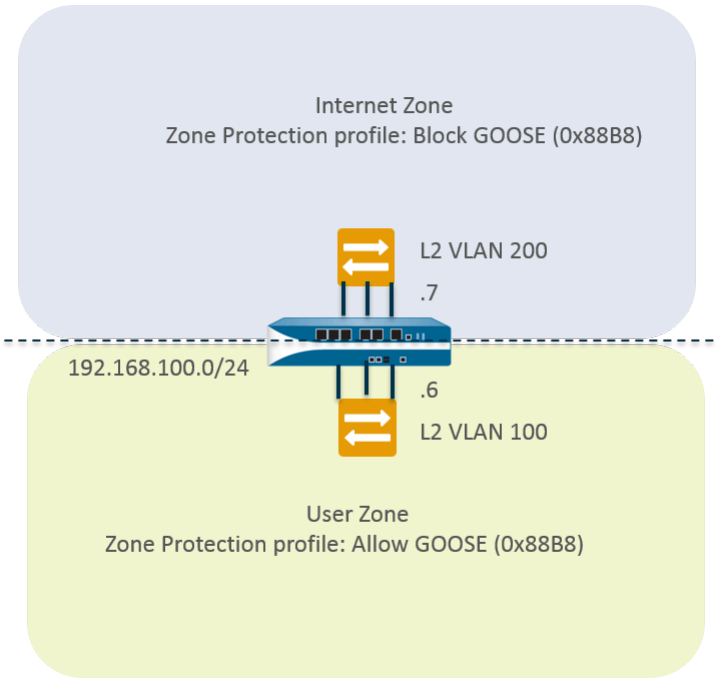
プロトコル保護の設定

プロトコル保護を使用して、非 IP プロトコル パケットからバーチャル ワイヤまたはレイヤ 2 セキュリティ ゾーンを保護します。

- 「ユース ケース：レイヤー 2 インターフェイス上のセキュリティ ゾーン間の非 IP プロトコル保護
- 「ユース ケース：レイヤー 2 インターフェイス上のセキュリティ ゾーン内の非 IP プロトコル保護

「ユース ケース：レイヤー **2** インターフェイス上のセキュリティ ゾーン間の非 **IP** プロトコル保護

このユースケースのファイアウォールは、2 つのサブインターフェイスに分けられた単一のレイヤー 2 VLAN 内にあります。VLAN 100 は 192.168.100.1/24、サブインターフェイス .6 です。VLAN 200 は 192.168.100.1/24、サブインターフェイス .7 です。非 IP プロトコル保護は入力ゾーンに適用されます。このユースケースでは、Internet ゾーンが入力ゾーンである場合、ファイアウォールは Generic Object Oriented Substation Event（GOOSE）プロトコルをブロックします。User ゾーンが入力ゾーンである場合、ファイアウォールは GOOSE プロトコルを許可します。ファイアウォールは IPv4、IPv6、ARP、および VLAN タグを持つフレームを両方のゾーンで暗黙的に許可します。



STEP 1 | 2 つの VLAN サブインターフェイスを設定します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **VLAN** を選択してインターフェイスを**Add (追加)** します。
2. vlan が **Interface Name (インターフェイス名)** のデフォルト設定です。ピリオドの後に「7」を入力します。
3. **Config (設定)** タブで、**Assign Interface To (インターフェイスの割り当て対象)** を **VLAN** 200 にします。
4. **OK** をクリックします。
5. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **VLAN** を選択してインターフェイスを**Add (追加)** します。
6. vlan が **Interface Name (インターフェイス名)** のデフォルト設定です。ピリオドの後に「6」を入力します。
7. **Config (設定)** タブで、**Assign Interface To (インターフェイスの割り当て対象)** を **VLAN** 100 にします。
8. **OK** をクリックします。

STEP 2 | ゾーン プロテクション プロファイルでプロトコル保護を設定し、GOOSE プロトコル パケットをブロックします。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **Zone Protection (ゾーン プロテクション)** を選択してプロファイルを **Add (追加)** します。
2. Block GOOSE という **Name (名前)** を入力します。
3. **Protocol Protection (プロトコル保護)** を選択します。
4. **Exclude List (除外リスト)** の **Rule Type (ルール タイプ)** を選択します。
5. リストにあるイーサネットを識別しやすくするために、GOOSE という **Protocol Name (プロトコル名)** を入力します。ファイアウォールは、入力した名前が Ethertype コード

にマッチするかどうかを検証しません。Ethertype コードはフィルタリングでのみ使用されます。

6. **Ethertype** コード 0x88B8 を入力します。16 進数の値であることを示すために、Ethertype は 0x で始める必要があります。範囲は 0x0000～0xFFFF です。
7. **Enable (有効)** を選択してプロトコル保護を適用します。例えばテストを行う目的で、リストのプロトコルを無効化できます。
8. **OK** をクリックします。

STEP 3 | ゾーン プロテクション プロファイルを Internet ゾーンに適用します。

1. **Network (ネットワーク)** > **Zones (ゾーン)** を選択してゾーンを **Add (追加)** します。
2. ゾーンの **Name (名前)** として Internet を入力します。
3. **Location (場所)** については、ゾーンを適用する仮想システムを選択します。
4. **Type（タイプ）** には、**Layer2（レイヤー 2）** を選択します。
5. vlan.7 ゾーンに属する **Interface (インターフェイス)** を **Add (追加)** します。
6. **Zone Protection Profile (ゾーン プロテクション プロファイル)** については Block GOOSE プロファイルを選択します。
7. **OK** をクリックします。

STEP 4 | プロトコル保護を設定し、GOOSE プロトコル パケットを許可します。

Allow GOOSE という名前のゾーン プロテクション プロファイルを別に作成し、**Rule Type (ルール タイプ)** で **Include List（許可リスト）** を選択します。

含有リストを設定する際は、必要な 非 *IP* プロトコルをすべて含めてください。リストが不完全な場合、正当な非 *IP* トラフィックがブロックされてしまうおそれがあります。

STEP 5 | ゾーン プロテクション プロファイルを User ゾーンに適用します。

1. **Network (ネットワーク)** > **Zones (ゾーン)** を選択してゾーンを **Add (追加)** します。
2. ゾーンの **Name (名前)** として User を入力します。
3. **Location (場所)** については、ゾーンを適用する仮想システムを選択します。
4. **Type（タイプ）** には、**Layer2（レイヤー 2）** を選択します。
5. vlan.6 ゾーンに属する **Interface (インターフェイス)** を **Add (追加)** します。
6. **Zone Protection Profile (ゾーン プロテクション プロファイル)** については Allow GOOSE プロファイルを選択します。
7. **OK** をクリックします。

STEP 6 | コミットします。

Commit（コミット） をクリックします。

STEP 7 | プロトコル保護に基づいてファイアウォールがドロップした非 IP パケットの数を表示します。

CLI へのアクセスを行います。

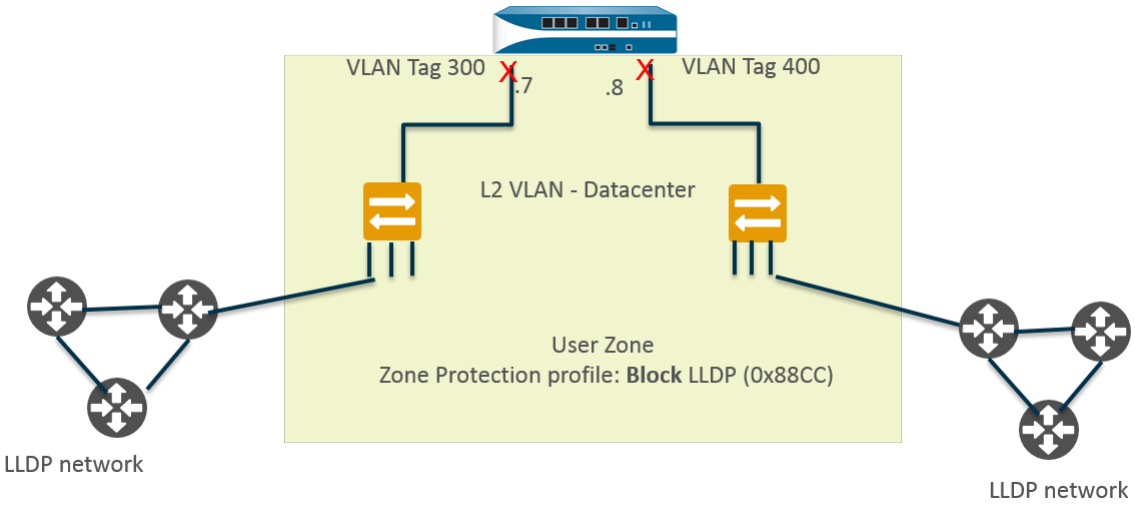
```
> show counter global name pkt_nonip_pkt_drop > show counter global
 name pkt_nonip_pkt_drop delta yes
```

「ユース ケース：レイヤー 2 インターフェイス上のセキュリティ ゾーン内の非 IP プロトコル保護

ゾーン プロテクション プロファイルを非 IP プロトコル保護と共に実装しない場合、ファイアウォールは単一のゾーン内の非 IP プロトコルが、あるレイヤー 2 インターフェイスから別のインターフェイスに進むのを許可します。このユースケースでは、LLDP パケットをブロックすることで、一つのネットワークの LLDP がゾーン内の別のインターフェイスを介して到達可能なネットワークを検出しないようにします。

次の図では、Datacenter という名前のレイヤー 2 VLAN が 2 つのサブインターフェイスに分けられています。192.168.1.1/24、サブインターフェイス .7 および 192.168.1.2/24、サブインターフェイス .8。VLAN は User ゾーンに属しています。LLDP をブロックするゾーン プロテクション プロファイルを User ゾーンに適用することで：

- サブインターフェイス .7 が、自身のスイッチから左側の赤い X のところにあるファイアウォールに向かう LLDP をブロックし、そのトラフィックがサブインターフェイス .8 に到達できないようにします。
- サブインターフェイス .8 が、自身のスイッチから右側の赤い X のところにあるファイアウォールに向かう LLDP をブロックし、そのトラフィックがサブインターフェイス .7 に到達できないようにします。



STEP 1 | Ethernet インターフェイスのサブインターフェイスを作成します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** を選択し、レイヤー 2 インターフェイスを選択します（この例では ethernet1/1）。
2. **Add Subinterfaces (サブインターフェイスの追加)** を選択します。
3. **Interface Name (インターフェイス名)** のデフォルト設定は interface（ethernet 1/1）です。ピリオドの後に「7」を入力します。
4. **Tag (タグ)** については 300 を入力します。
5. **Security Zone (セキュリティ ゾーン)** については User (ユーザー) を選択します。
6. **OK** をクリックします。

STEP 2 | Ethernet インターフェイスの 2 つ目のサブインターフェイスを作成します。

1. **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** を選択し、レイヤー 2 インターフェイス（ethernet1/1）を選択します。
2. **Add Subinterfaces (サブインターフェイスの追加)** を選択します。
3. **Interface Name (インターフェイス名)** のデフォルト設定は interface（ethernet 1/1）です。ピリオドの後に「8」を入力します。
4. **Tag (タグ)** については400 を入力します。
5. **Security Zone (セキュリティ ゾーン)** については User (ユーザー) を選択します。
6. **OK** をクリックします。

STEP 3 | レイヤー 2 インターフェイス用の VLAN および 2 つのサブインターフェイスを作成します。

1. **Network (ネットワーク)** > **VLANs** を選択して VLAN を **Add (追加)** します。
2. VLAN の **Name (名前)**（この例では Datacenter）を入力します。
3. **VLAN Interface (インターフェイス)** については **None (なし)** を選択します。
4. **Interfaces (インターフェイス)** については、**Add (追加)** をクリックしてレイヤー 2 インターフェイスを選択します（ethernet1/1、および ethernet1/1.7 と ethernet1/1.8 という 2 つのサブインターフェイス）。
5. **OK** をクリックします。

STEP 4 | ゾーン プロテクション プロファイルで非 IP プロトコル パケットをブロックします。

1. **Network (ネットワーク)** > **Network Profiles (ネットワーク プロファイル)** > **Zone Protection (ゾーン プロテクション)** を選択してプロファイルを **Add (追加)** します。
2. **Name (名前)** を入力します（この例では Block LLDP）。
3. プロファイルの **Description (復号化)** を入力します（LLDP からゾーン内の他のインターフェイスに向かう（ゾーン内）LLDP パケットをブロック）。
4. **Protocol Protection (プロトコル保護)** を選択します。
5. **Exclude List (除外リスト)** の **Rule Type (ルール タイプ)** を選択します。
6. **Protocol Name (プロトコル名)** として LLDP を入力します。
7. **Ethertype** コード 0x88cc を入力します。16 進数の値であることを示すために、Ethertype は 0x で始める必要があります。
8. **Enable**[有効] を選択します。
9. **OK** をクリックします。

STEP 5 | レイヤー 2 VLAN が属すセキュリティ ゾーンにゾーン プロテクション プロファイルを適用します。

1. **Network (ネットワーク)** > **Zones(ゾーン)**の順に選択します。
2. ゾーンを **Add (追加)** します。
3. ゾーンの **Name (名前)** として User を入力します。
4. **Location (場所)** については、ゾーンを適用する仮想システムを選択します。
5. **Type（タイプ）** には、**Layer2（レイヤー 2）** を選択します。
6. ethernet1/1.7 ゾーンに属する **Interface (インターフェイス)** を **Add (追加)** します。
7. ethernet1/1.8 ゾーンに属する **Interface (インターフェイス)** を **Add (追加)** します。
8. **Zone Protection Profile (ゾーン プロテクション プロファイル)** については Block LLDP プロファイルを選択します。
9. **OK** をクリックします。

STEP 6 | コミットします。

Commit（コミット）をクリックします。

STEP 7 | プロトコル保護に基づいてファイアウォールがドロップした非 IP パケットの数を表示します。

CLI へのアクセスを行います。

```
> show counter global name pkt_nonip_pkt_drop > show counter global
 name pkt_nonip_pkt_drop delta yes
```

パケット バッファ保護の設定

Packet Buffer Protection（パケット バッファ保護）を 2 つのレベルで設定できます。デバイス レベル（グローバル）と、グローバルに有効化されている場合は、ゾーンレベルでも有効化で

きます。グローバルレベルの パケット バッファ保護（**Device**（デバイス） > **Setup**（セットアップ） > **Session**（セッション））は、ファイアウォール リソースを保護し、悪意のあるトラフィックが原因でファイアウォールが応答しなくなることがないことを保証します。

入力ゾーンごとのパケット バッファ保護（**Network**（ネットワーク） > **Zones**（ゾーン））は、問題のある IP アドレスがパケット バッファ保護のしきい値を超え続けている場合、問題のあるIPアドレスのブロックを開始する第 2 の保護レイヤーです。ファイアウォールは、問題のある送信元 IP アドレスからのすべてのトラフィックをブロックできます。送信元 IP アドレスが変換された NAT IP アドレスである場合、多くのユーザーが同じ IP アドレスを使用している可能性があることに注意してください。1 人の悪意のあるユーザーがパケット バッファ保護を引き起こし、入口ゾーンでパケット バッファ保護が有効になっている場合、ファイアウォールがそのブロックリストに IP アドレスを置くと、その悪意のある送信元 IP アドレスからのすべてのトラフィックが（悪意のないユーザーからでも）ブロックされます。

ファイアウォールの背後にあるサービスに対する DoS 攻撃をブロックする最も効果的な方法は、パケット バッファ保護をグローバルと、および入力ゾーンごとに設定することです。

ゾーンの**Enable Packet Buffer Protection**（パケット バッファ保護の有効化）をすることができますが、パケット バッファ保護をグローバルに有効にして設定を指定するまで、ゾーンではアクティブになりません。

STEP 1 | パケット バッファ保護をグローバルに有効にする。

1. **Device (デバイス)** > **Setup (セットアップ)** > **Session (セッション)** を選択して Session Settings (セッション設定) を編集します。
2. **Packet Buffer Protection**（パケット バッファ保護）を選択します。
3. パケットバッファ保護動作を定義します。
   - **Alert (%)**（アラート（%））– このしきい値をパケット バッファの使用率が 10 秒より長い時間超えている場合、ファイアウォールはログ イベントを毎分作成します。範囲は 0% ～ 99%、デフォルトは 50% です。値が 0% の場合、ファイアウォールはログ イベントを作成しません。
   - **Activate**（%）（アクティベート（%））–パケット バッファの使用率がこのしきい値に達すると、ファイアウォールはランダムアーリードロップ（RED）を適用することにより、最も悪質なセッションの緩和を開始します。範囲は 0% ～ 99%、デフォルトは 50% です。値が 0% の場合、ファイアウォールは RED を適用しません。不正行為者がパケット バッファ保護が有効になっているゾーンにパケットを送信している場合、ファイアウォールは不正なセッションを破棄したり、問題の送信元 IP アドレスをブロックしたりすることもできます。デフォルトのしきい値から始め、必要に応じて値を調整します。

     ファイアウォールは、システム ログのアラート イベントを記録し、トラフィックのドロップ、破棄されたセッション、ブロックされた *IP* アドレスの各イベントを脅威ログに記録します。
   - **Block Hold Time (sec)**（ブロック ホールド タイム（秒））–ファイアウォールが破棄するまでの間、RED で軽減されたセッションが継続するのを許可する期間。範囲は 0 ～ 65,535、デフォルトは 60 です。値が 0 の場合、ファイアウォールは、パケット バッファ保護に基づくセッション廃棄を実施しません。

- **Block Duration (sec)**（ブロック期間（秒））—セッションが破棄されたままになる時間、あるいは IP アドレスがブロックされたままになる時間。範囲は 1 ～ 15,999,999、デフォルトは 3,600 です。

4. **OK** をクリックします。
5. 変更を **Commit (コミット)**します。

STEP 2 | 入力うゾーン上に追加のパケット バッファ保護を有効にします。

1. **Network**（ネットワーク） > **Zones**（ゾーン）を選択します。
2. 入力ゾーンを選択してその名前をクリックします。
3. ゾーン プロテクション セクションで **Enable Packet Buffer Protection**（パケット バッファ保護の有効化）にチェックを入れます。
4. **OK** をクリックします。
5. 変更を **Commit (コミット)**します。

レイテンシ基準のパケット バッファ保護の設定

レイテンシに基づくパケット バッファ保護を設定し、レイテンシの影響を受けやすいプロトコルとアプリケーションで構成されるトラフィックのあるゾーンに適用します。

STEP 1 | **Device**（デバイス） > **Setup**（セットアップ） > **Services**（サービス）を選択します。

STEP 2 | Session Settings (セッション設定) セクションを編集して、**Packet Buffer Protection (パケット バッファ保護)** を有効化します。

STEP 3 | **Buffering Latency Based (レイテンシ ベースのバファリング)** を有効化します。

STEP 4 | **Latency Alert (milliseconds) (レイテンシ アラート (ミリ秒))** しきい値を入力します。これを超えると、ファイアウォールが毎分アラート ログ イベントの生成を開始します。範囲は 1～20,000、デフォルトは 50 です。

STEP 5 | **Latency Activate (milliseconds) (レイテンシ アクティブ化 (ミリ秒))** しきい値を入力します。これを超えると、ファイアウォールが受信パケットの random early drop (ランダム早期ドロップ; RED) をアクティベートし、10 秒毎にアクティベート ログの生成を開始します。範囲は 1～20,000ms、デフォルトは 200ms です。

STEP 6 | **Latency Max Tolerate (milliseconds) (レイテンシ最大許容値 (ミリ秒))** のしきい値を入力します。これを超えると、ファイアウォールがほぼ100%のドロップ確率で RED を使用します。範囲は 1～20,000ms、デフォルトは500msです。

現在のレイテンシが、**Latency Activate (レイテンシ アクティベート)** しきい値と、**Latency Max Tolerate (レイテンシ最大許容)** しきい値の間の値である場合、ファイアウォールは RED ドロップ確率を以下のように計算します: (現在のレイテンシ - **Latency Activate (レイテンシ アクティベート)** しきい値) / (**Latency Max Tolerate (レイテンシ最大許容)** しきい値 - **Latency Activate (レイテンシ アクティベート)** しきい値)。例えば、現在のレイテンシが 300 である場合、**Latency Activate (レイテンシ アクティベート)** は 200、**Latency Max Tolerate (レイテンシ 最大許容値)** は 500であり、したがって (300-200)/(500-200) = 1/3となり、ファイアウォールは約 33%の RED ドロップ確率を使用することになります。

STEP 7 | 使用状況に基づいて、 Packet Buffer Protection (パケット バッファ保護) に関する、**Block Hold Time (**ブロック ホールド タイム**)** と **Block Duration (**ブロック期間**)** を設定します。

STEP 8 | **OK** をクリックします。

STEP 9 | レイテンシに基づいてパケット バッファ保護したい各ゾーンで、保護の第 2 レイヤーを有効にします。

1. **Network (**ネットワーク**)** > **Zones (**ゾーン**)** を選択して、ゾーンを 選択 します。
2. **Packet Buffer Protection (**パケット バッファ保護**)** を有効化します。

STEP 10 | **[**コミット**]** します。

イーサネット SGT 保護の設定

以下のタスクを使用して、イーサネット SGT 保護 プロファイルを設定します。

STEP 1 | イーサネット SGT 保護を提供するために、ゾーン プロテクション プロファイルを作成します。

1. **Network**（ネットワーク） > **Network Profiles**（ネットワーク プロファイル） > **Zone Protection**（ゾーン プロテクション）を選択します。
2. ゾーン プロテクション プロファイル を**Name (**名前**)** ごとに **Add (**追加**)** します。
3. **Ethernet SGT Protection (**イーサネット **SGT** 保護**)** を選択します。
4. **Layer 2 SGT Exclude List (**レイヤー**2 SGT** 除外リスト**)** を名前ごとに**Add (**追加**)** します。
5. リストに対して1つ以上の **Tag (**タグ**)** 値を入力します。値の範囲は 0 ～ 65,535 です。タグ値の連続した範囲 (100～500等) である個々のエントリを入力できます。除外リストには、最大100個 (個別または範囲) のタグ エントリを追加できます。
6. レイヤー2 SGT 除外リストを**Enable (**有効化**)** します。リストはいつでも無効化可能です。
7. **OK** をクリックします。

STEP 2 | レイヤー2、 バーチャル ワイヤ、タップインターフェースが属するセキュリティ ゾーンにゾーン プロテクション プロファイルを適用します。

1. **[Network]** > **[**ゾーン**]** の順に選択します。
2. ゾーンを **Add (**追加**)** します。
3. ゾーンの **Name (**名前**)** を入力します。
4. **Location (**場所**)** については、ゾーンを適用する仮想システムを選択します。
5. **Type (**種類**)** に対して、**Layer2 (**レイヤー**2)** 、**Virtual Wire (**バーチャル ワイヤ**)** 、または**Tap (**タップ**)** を選択します。
6. このゾーンに属する **Interface (**インターフェース**)** を **Add (**追加**)** します。
7. **Zone Protection Profile (**ゾーン プロテクション プロファイル**)** については、作成したプロファイルを選択します。
8. **OK** をクリックします。

STEP 3 | **Commit (**コミット**)** します。

STEP 4 | イーサネット SGT 保護を採用しているすべてのゾーン プロテクション プロファイルの結果としてファイアウォールがドロップしたパケットのグローバル カウンターを表示します。

1. CLI へのアクセスを行います。
2. **> show counter global name pan_flow_dos_l2_sec_tag_drop**

新規セッションのフラッド攻撃に対する Dos プロテクション

新規セッションのフラッド攻撃に対する DoS プロテクションは、大量の単一セッション攻撃と複数セッション攻撃に対して効果的です。単一セッション攻撃では、攻撃者が単一セッションを使用してファイアウォールの背後にあるデバイスをターゲットにします。セキュリティ ルールでトラフィックが許可されている場合、セッションが確立され、攻撃者が同じ送信元 IP アドレスとポート番号、宛先 IP アドレスとポート番号、およびプロトコルを使用して非常に高いレートでパケットを送信することで攻撃を開始し、ターゲットを圧倒しようとします。複数セッション攻撃では、攻撃者が単一ホストから複数のセッション（または 1 秒あたりの接続数（cps））を使用して DoS 攻撃を開始します。

この機能は、新規セッション（ハードウェアにオフロードされていないトラフィック）の *DoS* 攻撃のみを防御します。オフロード攻撃はこの機能では保護されません。ただし、このトピックではクライアントをリセットするセキュリティ ポリシー ルールの作成方法について説明しています。*1* 秒間に多数の接続で攻撃を再開する攻撃者は、このトピックに示された防御によってブロックされます。

DoS プロテクション プロファイルおよびポリシールール連携して、多数の着信 SYN、UDP、ICMP、および ICMPv6 パケット、およびその他のタイプの IP パケットのフラッディングに対する保護を提供します。フラッド攻撃とみなすしきい値を決定します。通常、ファイアウォールが DoS アラームを生成し、ランダム早期ドロップなどのアクションを実行し、さらなるインバウンド接続をドロップするようになるしきい値を DoS 保護プロファイルで設定します。保護用（パケットの許可あるいは拒否ではなく）に設定された DoS プロテクションポリシールールが、しきい値に向かってカウントされるように、一致するパケットの基準 (ソースアドレスなど) を決定します。この柔軟性により、特定のトラフィックをあるいはブロックするか、他のトラフィックを DoS トラフィックとして扱うことを許可できるようになります。受信速度がしきい値を超過すると、ファイアウォールは送信元アドレスから来るインバウンド トラフィックをブロックします。

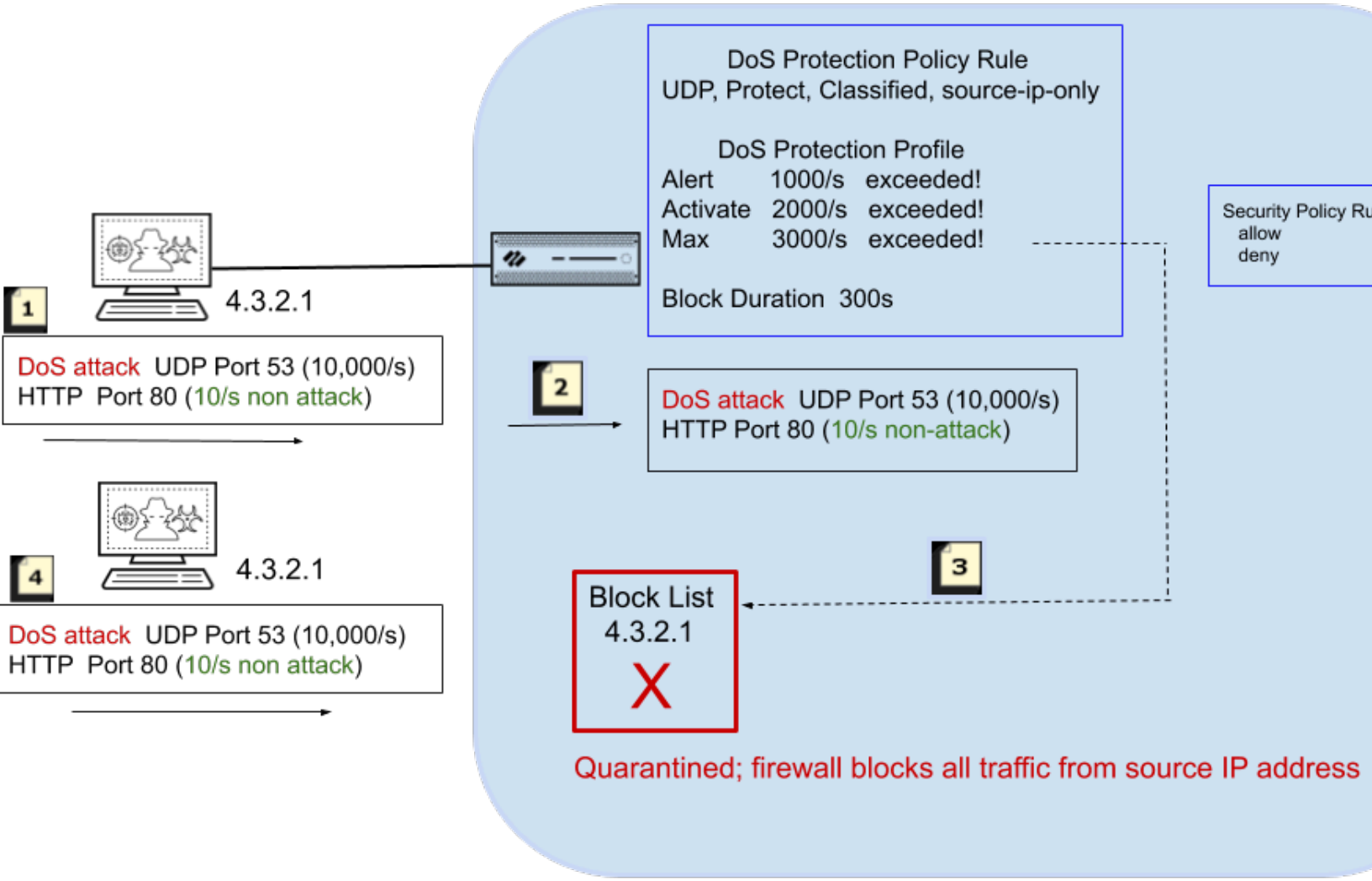
- 複数セッション DoS 攻撃
- 単一セッション DoS 攻撃
- 新規セッションのフラッド攻撃に対する DoS プロテクションの設定
- 単一セッション DoS 攻撃の終了
- オンチップ パケット記述子の使用が多すぎるセッションの識別
- コミットせずにセッションを破棄

複数セッション DoS 攻撃

DoS プロテクション ポリシー ルールを設定し、新規セッションのフラッド攻撃に対する DoS プロテクションの設定を行います。このルールは条件を判断し、受信パケットがこの条件に一致すると、**Protect (保護)** アクションがトリガーされます。DoS プロテクション プロファイルでは、Alert Rate （アラート レート）、Activate Rate （アクティベーション レート）、および Max Rate （最大レート）しきい値に対して各新規接続がカウントされます。1 秒あたりの新規

受信接続数がアクティベート レートを超えると、ファイアウォールは DoS プロテクション プロファイルで指定されたアクションを実行します。

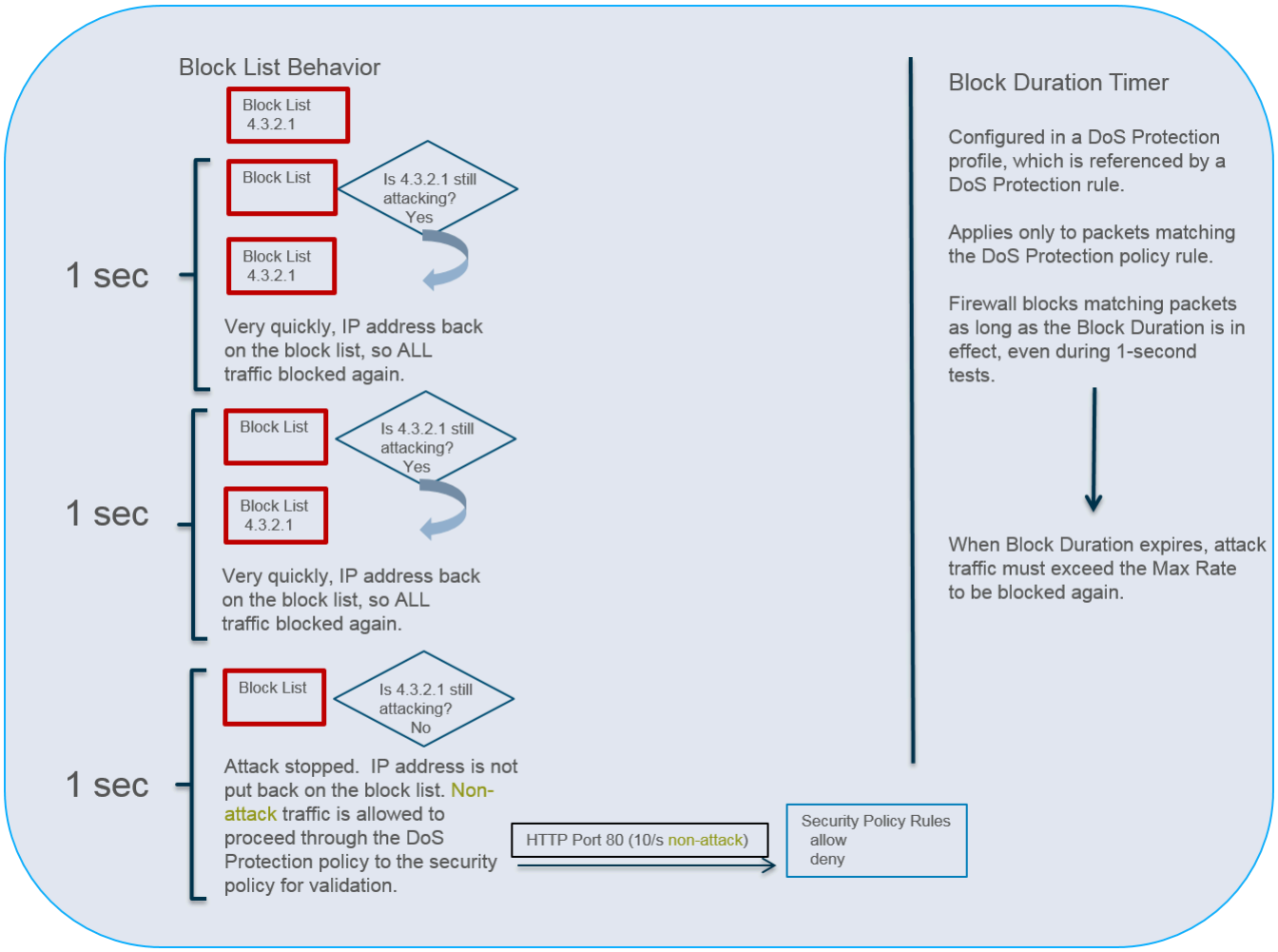
以下の図と表は、セキュリティ ポリシー ルール、DoS プロテクション ポリシー ルール、およびプロファイルの連携例を示しています。



ファイアウォールが IP アドレスを隔離するイベントの順序	
1	この例では、攻撃者が UDP ポート 53 に対して 1 秒あたり 10,000 件の新規接続のレートで DoS 攻撃を開始します。さらに、HTTP ポート 80 に対して 1 秒あたり 10 件の新規接続も送信します。
2	新規接続が設定内の DoS プロテクション ポリシー ルールの条件（送信元ゾーンまたはインターフェイス、送信元 IP アドレス、宛先ゾーンまたはインターフェイス、宛先 IP アドレス、サービ

ファイアウォールが IP アドレスを隔離するイベントの順序	
	スなど）に一致します。この例では、ポリシー ルールで UDP が指定されています。 DoS 保護ポリシールールでは、DoS Protection Profile （DoS プロテクション プロファイル）設定を動的に適用する **Protect** （保護） アクションと **Classified (分類化)** の 2 つの設定も指定します。DoS Protection Profile （DoS プロテクション プロファイル）では、1 秒あたり 3000 パケットの Max Rate （最大レート）が許可されることを指定します。入力パケットが DoS 保護ポリシールールに一致すると、1 秒あたりの新規接続数が **Alert** （アラート）、**Activate** （アクティベーション）、および **Max Rate (最大速度)** しきい値に対してカウントされます。 送信元 *IP* アドレスが常に有害であると判断した場合は、セキュリティ ポリシー ルールを使用してそのアドレスからのすべてのトラフィックをブロックすることもできます。
3	1 秒あたり 10,000 件の新規接続は Max Rate （最大レート）しきい値を超えます。以下のすべての条件に一致するとします。 • しきい値を超過する • Block Duration [ブロック期間]が指定されている • **Classified** が送信元 IP アドレスを含むように設定されている この場合、ファイアウォールは有害な送信元 IP アドレスをブロック リストに追加します。
4	ブロック リストにある IP アドレスは隔離され、その IP アドレスからのすべてのトラフィックはブロックされます。ファイアウォールはその後の攻撃パケットがセキュリティ ポリシーに到達する前に、有害な送信元 IP アドレスをブロックします。

以下の図は、DoS プロテクション ポリシー ルールに一致する IP アドレスがブロック リストに追加された後の動作を詳細に示しています。また、ブロック期間タイマーについても説明されています。



ファイアウォールは 1 秒ごとに IP アドレスのブロック リストからの除外を許可するため、トラフィックのパターンをテストし、攻撃が継続中かどうかを判断できます。ファイアウォールでは以下のアクションが実行されます。

- この 1 秒のテスト期間中に、DoS プロテクション ポリシー条件（この例では HTTP トラフィック）に一致しないパケットは DoS プロテクション ポリシー ルールを通過し、セキュリティ ポリシーで検証されます。IP アドレスがブロック リストから除外された後にファイアウォールが受信する最初の攻撃パケットは DoS プロテクション ポリシー条件に一致し、すぐに 1 秒後のブロック リストに再追加されるため、通過するパケットがあるとしてもごくわずかです。ファイアウォールは攻撃が停止するまでこのテストを 1 秒ごとに繰り返します。
- ブロック期間が終了するまですべての攻撃トラフィックはブロックされ、DoS プロテクション ポリシー ルール（アドレスがブロックリストに残ります）を通過できません。

前述の図にある *1* 秒間のチェックは、複数のデータプレーン *CPU* とハードウェア ネットワーク プロセッサを持つファイアウォール モデルで発生します。単一データプレーン システムやハードウェア ネットワーク プロセッサを持たないシステムはすべて、ソフトウェア上でこの移行を実行し、*5* 秒間の間隔を採用します。

攻撃が停止した場合、ファイアウォールはその IP アドレスをブロック リストに再追加しません。非攻撃トラフィックは DoS プロテクション ポリシー ルールを通過してセキュリティ ポリ

シーで評価されます。セキュリティ ポリシー ルールがないと暗黙的な拒否ルールによってすべてのトラフィックが拒否されてしまうため、セキュリティ ポリシー ルールを設定してトラフィックを許可あるいは拒否する必要があります。

ブロック リストは、送信元ゾーンと送信元アドレスの組み合わせに基づいています。この動作によって、別々の仮想ルーターに属する別のゾーンに存在する重複 IP アドレスが許可されます。

DoS プロテクション プロファイルの Block Duration （ブロック期間）設定では、DoS プロテクション ポリシー ルールに一致する「有害な」パケットをファイアウォールがブロックする期間を指定します。攻撃トラフィックはブロック期間が終了するまでブロックされたままになり、期間終了後にその攻撃トラフィックが再度ブロックされるには、Max Rate （最大レート）しきい値を再度超える必要があります。

攻撃者が複数の攻撃セッションを開始する複数セッションまたはボットを使用している場合、セッションはセキュリティ ポリシーの拒否あるいはドロップ ルールが適用されずに *DoS* プロテクション プロファイルのしきい値に対してカウントされます。つまり、単一セッション攻撃では、各パケットがしきい値に対してカウントされるにはセキュリティ ポリシーの拒否あるいはドロップ ルールが必要ですが、複数セッション攻撃では不要です。

したがって、新規セッションのフラッド攻撃に対する DoS プロテクションでは、攻撃トラフィックが進行中の送信元 IP アドレスを効率的に防御し、攻撃が停止したらすぐに非攻撃トラフィックを許可できます。有害な IP アドレスをブロック リストに追加することで、DoS プロテクション機能がブロック リストを利用して、異なるアプリケーションのパケットなど、送信元 IP アドレスからのすべてのアクティビティを隔離できます。IP アドレスのすべてのアクティビティを隔離することで、単にアプリケーションを変更して新しい攻撃を開始したり、ハイブリッド DoS 攻撃でさまざまな攻撃の組み合わせを使用したりする新手の攻撃者に対して保護できます。ブロック中の IP アドレスの監視を行ってブロックリストを表示したり、エントリを削除したり、ブロックリストに含まれる IP アドレスの詳細情報を取得したりできます。

PAN-OS 7.0.2 以降、ファイアウォールが送信元 *IP* アドレスをブロック リストに追加する動作が変更されます。攻撃が停止すると、非攻撃トラフィックはセキュリティ ポリシーの適用に進むことができます。*DoS* プロテクション プロファイルと *DoS* プロテクション ポリシー ルールに一致する攻撃トラフィックは、ブロック期間が終了するまでブロックされたままになります。

単一セッション DoS 攻撃

単一セッション DoS 攻撃はセッションが作成された後に実行される攻撃であるため、通常はゾーン プロファイルや DoS プロテクション プロファイルをトリガーしません。セッションの作成は可能であり、攻撃はセッションの作成後にパケット量を増加させてターゲット デバイスを不能状態にするため、これらの攻撃はセキュリティ ポリシーでは許可されます。

新しいセッションのフラッディング (単一セッションおよび複数セッションのフラッディング) から保護するための新規セッションのフラッド攻撃に対する DoS プロテクションの設定。進行中の単一セッション攻撃が発生した場合は、さらに単一セッション DoS 攻撃の終了します。

新規セッションのフラッド攻撃に対する DoS プロテクションの設定

STEP 1 | 攻撃者の IP アドレスからのトラフィックを拒否し、ネットワークのニーズに基づいてその他のトラフィックを許可するようにセキュリティ ポリシー ルールを設定します。セキュリティ ポリシー ルールでは、任意の一致条件（送信元 IP アドレスなど）を指定できます。（単一セッション攻撃を軽減する場合または DoS プロテクション ポリシーしきい値をトリガーしない攻撃の場合は必須。複数セッションの攻撃を軽減する場合は任意）。

この手順は、既存の攻撃を停止するために一般的に実行される手順の *1* つです。単一セッション DoS 攻撃の終了を参照してください。

- セキュリティ ポリシー ルールを作成する

STEP 2 | フラッド防御を行うように DoS プロテクション プロファイルを設定します。

フラッド攻撃は複数のプロトコル上で発生する可能性があるため、ベスト プラクティスとして、*DoS* プロテクション プロファイルですべてのフラッド タイプに対する保護をアクティベーションします。

1. **Objects (オブジェクト)** > **Security Profiles (セキュリティ プロファイル)** > **DoS Protect (保護)ion** を選択してプロファイルの **Name (名前)** を **Add (追加)** します。
2. **Type (タイプ)** として **Classified (分類済み)** を選択します。
3. **Flood Protection** [フラッド防御]についてはすべてのタイプのフラッド防御を選択します。
   - **SYN**フラッド
   - **UDP** フラッド
   - **ICMP** フラッド
   - **ICMPv6** フラッド
   - その他の **IP** フラッド
4. **SYN Flood (SYN** フラッド) を有効化する際、1 秒あたりの接続数（cps）が **Activate Rate (アクティベーション レート)** のしきい値を超えた際に起こす **Action (アクション)** を選択します。
   1. **Random Early Drop (ランダム早期ドロップ)**—ファイアウォールが、そのタイプのパケットのドロップを漸進的に開始するアルゴリズムを使用します。攻撃が続くと、インバウンドの cps 速度が大きくなり（**Activate Rate (アクティベーション レート)** を超える）、ファイアウォールがドロップするパケットも多くなります。インバウンドの cps 速度が **Max Rate (最大速度)**（この時点でファイアウォールがすべてのインバウンド接続をドロップ）に達するまで、ファイアウォールがパケットをドロップします。**Random Early Drop (ランダム早期ドロップ)**（RED）は **SYN Flood (SYN** フラッド) のデフォルトのアクションであり、**UDP Flood (UDP** フラッド)、**ICMP Flood (ICMP** フラッド)、**ICMPv6 Flood (ICMPv6** フラッド)、および **Other IP Flood (その他の IP** フラッド) における唯一のアクションです。RED は SYN Cookie より

も効率が良く、より多くの攻撃に対処できますが、良いトラフィックと悪いトラフィックを判別しません。

2. **SYN Cookies**—ファイアウォールが SYN をサーバーに速やかに送信するのではなく、Cookie を生成（サーバーの代わりに）し、SYN-ACK に含めてクライアントに送信します。クライアントは ACK および Cookie によって応答します。この検証の後、ファイアウォールが SYN をサーバーに送信します。**Random Early Drop (**ランダム早期ドロップ**)** の場合よりも多くのファイアウォール リソースを必要とする **SYN Cookies (SYN Cookie)** アクションは、好ましくないトラフィックに影響を与えるため、より正確性が高くなっています。

5. （任意）各フラッド タブで、環境に合わせて以下のしきい値を変更します。

   - **Activate Rate （connections/s） (**アクティベーション レート（接続数/秒）**)**—DoS アラームが生成されるしきい値レート（cps）を指定します。（範囲は 0 ～ 2000000、デフォルトは 10,000）。
   - **Activate Rate（packets/s） (**アクティベーション レート（接続数/秒）**)**— DoS 応答がアクティベーションされるしきい値レート（cps）を指定します。**Activate Rate** [アクティベーション レート]しきい値に達すると、**Random Early Drop** が発生します。範囲は 0 ～ 2000000、デフォルトは 10,000。（SYN フラッドについては、発生するアクションを選択できます）
   - **Max Rate （packets/s） (**最大レート（接続数/秒）**)**— ファイアウォールが許可する 1 秒あたりの受信接続数のしきい値レートを指定します。しきい値を超過すると、受信した新しい接続をドロップします。範囲は 2 ～ 2,000,000、デフォルトは40,000。

   このステップのデフォルトしきい値はほんの開始点であり、ネットワークによっては適切でない場合があります。ネットワークの動作を分析し、しきい値の初期値を適切に設定する必要があります。

6. 各フラッド タブの **Block Duration** [ブロック期間]で、このプロファイルを参照する DoS プロテクション ポリシー ルールに一致するパケットをファイアウォールがブロックする時間（秒）を指定します。0 よりも大きい値を指定します（範囲は 1 ～ 21600、デフォルトは 300）。

   誤って攻撃トラフィックと見なされたパケットのブロックを回避することを重視する場合は、***Block Duration (***ブロック期間**)**に低い値を設定します。

   攻撃の一部ではないパケットを誤ってブロックしてしまうことよりも、帯域幅消費型攻撃のブロックを重視する場合は、**Block Duration (**ブロック期間**)**に高い値を設定します。

7. **OK** をクリックします。

STEP 3 | 受信トラフィックの一致条件を指定する DoS プロテクション ポリシー ルールを設定します。

ファイアウォール リソースは有限であり、*DoS* 保護ポリシールールにマッチするユニーク *IP* アドレスの数が膨大になり得るため、インターネットに接続されたゾーン上で送信元アドレスを使用して分類化を行うのは好ましくありません。これには多くのカウンターが必要になり、ファイアウォールがトラッキング リソースを消費しきってしまうおそれがあります。その代わりに、（保護中のサーバーの）宛先アドレスを使用して分類化を行う *DoS* 保護ポリシールールを定義します。

1. **Policies (ポリシー)** > **DoS Protection (Dos プロテクション)** を選択し、**General** （全般）タブで **Name (名前)** を **Add (追加)** します。名前の大文字と小文字は区別され、文字、数字、スペース、ハイフン、およびアンダースコアを含む最大 31 文字を指定できます。
2. **Source** [送信元]タブで、**Type** [タイプ]に **Zone** [ゾーン]または **Interface** [インターフェイス]を選択し、ゾーンまたはインターフェイスを **Add** [追加]します。デプロイ環境と保護対象を考慮しつつ、ゾーンあるいはインターフェイスを選択します。例えば、ファイアウォールの入り口となるインターフェイスが一つしかない場合、インターフェイスを選択します。
3. （任意）**Source Address** [送信元アドレス]で、**Any** [いずれか]を選択してすべての受信 IP アドレスをルールに一致させるか、地域などのアドレス オブジェクトを **Add** [追加]します。
4. （任意）**Source User** [送信元ユーザー]で、**any** [任意]を選択するか、ユーザーを指定します。
5. （任意）**Negate** [無効]を選択して、指定した送信元以外のすべての送信元に一致させます。
6. （任意）**Destination** [宛先]タブで、**Type** [タイプ]に **Zone** [ゾーン]または **Interface** [インターフェイス]を選択し、宛先ゾーンまたはインターフェイスを **Add** [追加]します。たとえば、保護するセキュリティ ゾーンを入力します。
7. （任意）**Destination Address** [宛先アドレス]で、**Any** [いずれか]を選択するか、保護するデバイスの IP アドレスを入力します。
8. （任意）**Option/Protection (オプション/保護)** タブで、**Service (サービス)** を **Add (追加)** します。サービスを選択するか、**Service** [サービス]をクリックして **Name** [名前]を入力します。**TCP** または **UDP** を選択します。**Destination Port** [宛先ポート]を入力します。特定のサービスを指定しない場合、アプリケーション固有のポートに関係なく、すべてのプロトコル タイプのフラッドをルールに一致させることができます。
9. **Option/Protection (オプション/保護)** タブの **Action (アクション)** で、**Protect (保護)** を選択します。
10. **Classified** [分類済み]を選択します。
11. **Profile** [プロファイル]で、作成した **DoS Protection** [DoS プロテクション]プロファイルの名前を選択します。

12. **Address** [アドレス]で、**source-ip-only** または **src-dest-ip-both** を選択します。この選択によって、ルールが適用される IP アドレスのタイプを決定します。ファイアウォールで有害なトラフィックを識別する方法に基づいて、設定を選択します：
    - ファイアウォールが送信元 IP アドレスでのみ分類を行うようにする場合は、**source-ip-only** を指定します。攻撃者は多くの場合ホストのネットワーク全体をテストして攻撃するため、**source-ip-only** は広範囲の調査で一般的な設定です。
    - 特定の宛先アドレスがあるサーバーへの DoS 攻撃に対して保護し、さらにそのサーバーに固有の cps をすべての送信元 IP アドレスが超えないようにする場合は、**src-dest-ip-both** を指定します。
13. **OK** をクリックします。

STEP 4 | コミットします。

Commit（コミット）をクリックします。

単一セッション DoS 攻撃の終了

単一セッション DoS 攻撃を減らすために、事前に新規セッションのフラッド攻撃に対する DoS プロテクションの設定をさらに行います。この機能を設定した後のある時点で、特定のセッションが確立され、そのセッションの IP アドレスからの DoS 攻撃が進行中であることにしばらく気付かない可能性があります。単一セッション DoS 攻撃に気付いた場合は、以下のタスクを実行してそのセッションを終了し、その IP アドレスからの後続の接続試行で新規セッションのフラッド攻撃に対する DoS プロテクションがトリガーされるようにします。

STEP 1 | 攻撃を実行している送信元 IP アドレスを識別します。

たとえば、ファイアウォールのパケット キャプチャ機能で宛先フィルタを使用し、宛先 IP アドレスへのトラフィックのサンプルを収集します。または、ACC を使用して宛先アドレスをフィルタリングし、攻撃されているターゲット ホストに対するアクティビティを表示します。

STEP 2 | 攻撃しきい値を超えたら攻撃者の IP アドレスをブロックする DoS プロテクション ポリシー ルールを作成します。

STEP 3 | 送信元 IP アドレスとその攻撃トラフィックを拒否するセキュリティ ポリシー ルールを作成します。

STEP 4 | **clear session all filter source <*ip-address*>** 操作コマンドを実行して、攻撃元 IP アドレスからの既存の攻撃をすべて終了します。

または、セッション ID がわかっている場合は、**clear session id <*value*>** コマンドを実行して、そのセッションのみを終了することもできます。

> ***clear session all filter source <ip-address>*** コマンドを使用すると、ソース *IP* アドレスに一致するすべてのセッションが破棄され、これには正常なセッションと無効なセッションの両方が含まれる可能性があります。

既存の攻撃セッションを終了したら、攻撃セッションからの後続の試行はセキュリティ ポリシーによってブロックされます。DoS プロテクション ポリシーは、しきい値に対してすべての接続試行数をカウントします。Max Rate (最大速度)（最大レート）しきい値を超えると、複数セッション DoS 攻撃で説明されているように、送信元 IP アドレスはブロック期間が終了するまでブロックされます。

オンチップ パケット記述子の使用が多すぎるセッションの識別

リソース枯渇の兆候をファイアウォールが示した場合、膨大な数のパケットを送信する攻撃にさらされている可能性があります。この場合、ファイアウォールはインバウンド パケットのバッファリングを開始します。オンチップパケット記述子の過剰な割合を使用しているセッションをすばやく識別し、それらを破棄することによって影響を軽減できます。

ハードウェア ベースのファイアウォール モデル (VM シリーズ ファイアウォールではない) で次のタスクを実行して、各スロットとデータプレーン、使用されるオンチップ パケット記述子の割合、上位 5 つのセッションで、オンチップ パケット記述子の 2% 以上を使用し、それらのセッションに関連付けられた送信元 IP アドレスを識別します。この情報を得ることで適切なアクションを実行できるようになります。

STEP 1 | ファイアウォールのリソース使用状況、上位のセッション、セッションの詳細を表示します。CLIで次の操作コマンドを実行します（コマンド画面の出力例）。

```
admin@PA-7050> show running resource-monitor ingress-backlogs --
 SLOT:s1, DP:dp1 -- USAGE - ATOMIC: 合計92%:93% トップセッション:セス-
ID PCT GRP-ID カウント 6 92% 1 156 7 1732 セッション詳細 セス-ID プロ
```



```
ト SZONESRC スポーツ DST DTA IGR-if EGR-IFアプリ 6 信頼 192.168.2.35
 55653 10.1.8.89 80 イーサネット1/21 イーサネット1/22 未定
```

このコマンドは、各セッションが 2% 以上のオンチップパケット記述子を使用する上位 5 つのセッションの最大値を表示します。

上記の出力例は、セッション 6 が、発信元 IP アドレス 192.168.2.35 から送信される TCP パケット(プロトコル 6)を持つオンチップ パケット記述子の 92% を使用していることを示しています。

- **SESS-ID**—他のすべての **show session** コマンドで使用されているグローバル セッションIDを示します。ファイアウォール内のグローバル セッションIDは一意です。
- **GRP-ID**—パケット処理の内部段階を示します。
- **COUNT**—そのセッションでいくつのパケットがそのGRP-IDにあるのかを示します。
- **APP**—セッション情報から抽出されたApp-IDを示し、これはトラフィックが正当であるかどうかを判断するのに役立ちます。例えば、パケットがTCP または UDPポートを使用し、しかしCLIの出力が**undecided**（不定）を示す場合、悪意のあるトラフィックのパケットである可能性があります。Application IP Decoder [アプリケーションIPデコーダ]がアプリケーションを判断するのに十分な情報を得られない場合、APPは**undecided** [不定]になります。APP が 未知 の場合は、アプリケーション IP デコーダがアプリケーションを判別できないことを示します。オンチップパケット記述子の高い割合を使用する未知の APPのセッションも疑わしいです。

画面出力を制限するには：

PA-7000 Series モデルのみ、出力をスロット、データプレーン、あるいは両方に絞ることができます。以下に例を示します。

```
admin@PA-7050> show running resource-monitor ingress-backlogs slot
 s1 admin@PA-7050> show running resource-monitor ingress-backlogs
 slot s1 dp dp1
```

PA-5200 Series および PA-7000 Series モデルのみ、出力をデータプレーンに絞ることができます。以下に例を示します。

```
admin@PA-5260> show running resource-monitor ingress-backlogs dp
 dp1
```


STEP 2 | コマンド出力を使用して、オンチップパケット記述子の高い割合を使用して送信元 IP アドレスの送信元が正当なトラフィックまたは攻撃トラフィックを送信しているかどうかを確認します。

上記の出力サンプルでは、おそらく単一のセッション攻撃が発生しています。単一のセッション（セッションID 6）がSlot 1、DP 1用のパケット バッファの92%を使用しており、そのポイントでアプリケーションが`undecided` になっています。

- 単一のユーザーが悪意のあるトラフィックを送っており、トラフィックがオフロードされていない場合は、単一セッション DoS 攻撃の終了を行うことができます。最低でも、新規セッションのフラッド攻撃に対する DoS プロテクションの設定を行えます。
- FPGA（field-programmable gate array）があるハードウェア モデルでは、パフォーマンスを向上できそうな場合はファイアウォールがFPGAにトラフィックをオフロードします。トラフィックがハードウェアにオフロードされる場合、後で大量のパケットを処理するのはソフトウェアであるため、セッションをクリアしても何も変わりません。代わりに、コミットせずにセッションを破棄する必要があります。

セッションがオフロードされているかどうかを確認するには、次の例に示すように、CLI で **`show session id <session-id>`** 操作コマンドを使用します。`layer7processing`

の値は、セッションがオフロードされている場合は completed、されていない場合は enabled になります。

```
admin@PA-5060> show session id 68088184

Session        68088184

        c2s flow:
                source:      1.1.42.15 [trust]
                dst:         1.2.27.99
                proto:       6
                sport:       55993           dport:      6881
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        s2c flow:
                source:      1.2.27.99 [untrust]
                dst:         1.1.42.15
                proto:       6
                sport:       6881            dport:      55993
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        DP                                   : 2
        index(local):                        : 979320
        start time                           : Tue Oct 27 14:20:09 2015
        timeout                              : 1200 sec
        time to live                         : 1167 sec
        total byte count(c2s)                : 270
        total byte count(s2c)                : 270
        layer7 packet count(c2s)             : 3
        layer7 packet count(s2c)             : 3
        vsys                                 : vsys1
        application                          : bittorrent
        rule                                 : rule1
        session to be logged at end          : True
        session in session ager              : True
        session updated by HA peer           : False
        layer7 processing                    : completed
        URL filtering enabled                : False
        session via syn-cookies              : False
        session terminated on host           : False
        session traverses tunnel             : False
        captive portal session               : False
        ingress interface                    : ethernet1/21
        egress interface                     : ethernet1/22
        session QoS rule                     : N/A (class 4)
        tracker stage l7proc                 : ctd decoder bypass
        end-reason                           : unknown
```

show セッション **ID** ***<session-id>*** コマンドの出力に次のような情報が表示されている場合、その出力は、セッションがまだ PAN-OS firewall にインストールされていないことを意味します。これが発生する理由の 1 つは、セキュリティ ポリシー ルールが構成されているためにトラフィックが拒否されるためです。

> show session id *xxxxxxxxxx*

Session *xxxxxxxxxx*

Bad Key: c2s: ‘c2s’

Bad Key: s2c: ‘s2c’

index(local): : *yyyyyyy*

コミットせずにセッションを破棄

このタスクを実行して、のセッションがパケット バッファやオンチップ パケット記述子 をオーバーロードしているセッションなど、セッションを永続的に破棄します。コマンド実行後にセッションが即座に破棄されるため、コミットは不要です。このコマンドはオフロードされているセッション、されていないセッションの両方に適用されます。

STEP 1 | 任意のハードウェア モデルの CLI で次の操作コマンドを実行します。

```
admin@PA-7050> request session-discard [timeout <seconds>]
 [reason <reason-string>] id <session-id>
```

デフォルトのタイムアウト値は 3,600 秒です。

STEP 2 | セッションが破棄されたことを確認します。

```
admin@PA-7050> show session all filter state discard
```

証明書

以下のトピックでは、標準のセキュリティ保証と機能の確保に対するセキュリティ認証である、情報セキュリティ国際評価基準（CC）と連邦情報処理標準 140-2 （FIPS 140-2）をサポートするように Palo Alto Networks® のファイアウォールおよびアプライアンスを設定する方法を説明します。これらの認証は、多くの場合米国の政府機関や政府請負業者によって取得されます。

製品証明書およびサードパーティの検証に関する詳細については、証明書ページを参照してください。

- FIPS および情報セキュリティ国際評価基準のサポートの有効化
- FIPS-CCセキュリティ機能
- FIPS-CC モードのファイアウォールあるいはアプライアンスにおけるスワップメモリのスクラブ

FIPS および情報セキュリティ国際評価基準のサポートの有効化

情報セキュリティ国際評価基準および連邦情報処理標準 140-2 （FIPS 140-2）をサポートしているソフトウェア バージョンで FIPS-CC モードを有効にするには、以下の手順を実行します。FIPS-CCモードを有効にする際、すべてのFIPSおよびCCの機能がインクルードされます。

Palo Alto Networks 次世代ファイアウォールおよびアプライアンス（VM-Series ファイアウォールを含む）はすべて FIPS-CC モードをサポートしています。FIPS-CC モードを有効化するには、まずファイアウォールを Maintenance Recovery Tool（MRT）として立ち上げ、操作モードを通常モードから FIPS-CC モードに変更します。操作モードを変更する流れはすべてのファイアウォールおよびアプライアンスで同じですが、MRT にアクセスする流れが異なります。

FIPS-CC モードを有効にすると、ファイアウォールが工場出荷時のデフォルト設定にリセットされ、すべての設定が削除されます。

- Maintenance Recovery Tool (MRT)にアクセス
- 操作モードを FIPS-CC モードに変更

Maintenance Recovery Tool (MRT)にアクセス

Maintenance Recovery Tool（MRT）を使用すると、Palo Alto Networks のファイアウォールやアプライアンスでいくつかのタスクを実行できます。たとえば、ファイアウォールやアプライアンスを出荷時のデフォルト設定に戻したり、PAN-OS またはコンテンツのアップデートを以前のバージョンに戻したり、ファイル システムの診断を実行したり、システム情報を収集したり、ログを抽出することができます。さらに、MRT を使用して 操作モードを FIPS-CC モードに変更するか FIPS-CC モードを通常モードに変更できます。

以下の手順では、さまざまな Palo Alto Networks 製品の Maintenance Recovery Tool（MRT）にアクセスする方法について説明します。

ハードウェアのファイアウォールやアプライアンス（PA-220 ファイアウォール、PA-7000 シリーズ ファイアウォール、M-Series アプライアンスなど）で MRT にアクセスします。

1. ファイアウォールまたはアプライアンスへのシリアル コンソール セッションを確立します。
   1. シリアル ケーブルをコンピュータのシリアル ポートからファイアウォールまたはアプライアンスのコンソール ポートに接続します。

      コンピュータに *9 pin* シリアル ポートがなく *USB* ポートがある場合は、シリアル/ *USB* コンバータを使用して接続を確立します。ファイアウォールには micro USB コンソール ポートがある場合は、*Type-A USB* を *micro USB* ケーブルに接続します。
   2. お使いのコンピュータのターミナル エミュレーション ソフトウェアを開き、9600-8-N-1 に設定してから、適切な COM ポートに接続します。

      Windows システムでは、コントロールパネルにアクセスして、デバイスとプリンタの *COM* ポート設定を表示して、どの *COM* ポートがコンソールに割り当てられているかを判断できます。
   3. 管理者アカウントを使用してログインします。デフォルトのユーザー名/パスワードは admin/admin です。
2. 次の CLI コマンドを入力し、 **y** を押して確定します。

   ```
   debug system maintenance-mode
   ```
3. ファイアウォールまたはアプライアンスを MRT 開始画面で起動してから（約 2～3 分後）、**Continue**で Enter を押して MRT メインメニューにアクセスします。

   また、*MRT* にアクセスするには、ファイアウォールまたはアプライアンスを再起動し、メンテナンス モード プロンプトで ***maint*** を入力します。シリアル コンソール直接接続が必要です。

ファイアウォールまたはアプライアンスが MRT にブートした後、管理（MGT）インターフェイスの IP アドレスへの SSH 接続を確立することによって、リモートから MRT にアクセスできます。ログイン プロンプトで、ユーザー名として **maint** を、パスワードとしてファイアウォールまたはアプライアンスのシリアル番号を入力します。

プライベート クラウドにデプロイされた VM-Series ファイアウォール（VMware ESXi または KVM ハイパーバイザ等）上の MRT にアクセスします。

1. ファイアウォールの管理 IP アドレスへの SSH セッションを確立し、管理者アカウントを使用してログインします。
2. 次の CLI コマンドを入力し、 **y** を押して確定します。

```
debug system maintenance-mode
```

ファイアウォールが *MRT* を起動するまでに約 *2*～*3* 分かかります。この間、*SSH* セッションは切断されます。

3. ファイアウォールが起動して MRT の開始画面が表示されたら、操作モードを基準にログインします。
   - 通常モード—ファイアウォールの管理 IP アドレスへの SSH セッションを確立し、**maint** をユーザー名、ファイアウォールまたはアプライアンスのシリアル番号をパスワードとして使用してログインします。
   - **FIPS-CC** モード—仮想マシン管理ユーティリティ（vSphere クライアントなど）にアクセスし、仮想マシン コンソールに接続します。
4. MRT の開始画面で、Enter を押して**Continue** をクリックし、MRT メインメニューにアクセスします。

パブリック クラウドにデプロイされた VM-Series ファイアウォール（AWS や Azure など）で MRT にアクセスします。

1. ファイアウォールの管理 IP アドレスへの SSH セッションを確立し、管理者アカウントを使用してログインします。
2. 次の CLI コマンドを入力し、 **y** を押して確定します。

```
debug system maintenance-mode
```

ファイアウォールが *MRT* を起動するまでに約 *2*～*3* 分かかります。この間、*SSH* セッションは切断されます。

3. ファイアウォールが起動して MRT の開始画面が表示されたら、仮想マシンのタイプを基準にログインします。
   - **AWS**—**ec2-user** でログインし、仮想マシンをデプロイしたときに SSH パブリック キーを選択します。
   - **Azure** —VM-Series ファイアウォールをデプロイしたときに作成した証明書を入力します。
   - **GCP**—**gcp-user** でログインし、仮想マシンをデプロイしたときに SSH パブリック キーを選択します。
4. MRT の開始画面で、Enter を押して**Continue** をクリックし、MRT メインメニューにアクセスします。

操作モードを FIPS-CC モードに変更

次の作業の流れは、Palo Alto Networks 製品の操作モードを通常モードから FIPS-CC モードに変更する方法を示しています。

アプライアンスが *FIPS-CC* モードの場合、管理インターフェイス設定を含むコンソールを介して設定を行うことはできなくなります。*FIPS-CC* モードを有効にする前に、*SSH* または *Web* インターフェイスを介して管理インターフェイスにアクセスできるようにネットワークが設定されていることを確認してください。管理インターフェイスは、*PA* シリーズ ファイアウォールを使用する場合は *192.168.1.1* の静的アドレスにデフォルト設定され、*VM-Series* ファイアウォールの場合は *DHCP* 経由で取得されたアドレスにデフォルトで *192.168.1.1* が設定されます。*WildFire*、仮想 *Panorama*、および *M-series Panorama* アプライアンスは、デフォルトで *192.168.1.1* の静的アドレスになります。

FIPS-CC モードが有効になると、すべての設定と設定が消去されます。管理者が *FIPS-CC* モードを有効にした後で再利用したい構成または設定を持っている場合、管理者は *FIPS-CC* モードに変更する前に、構成を保存してエクスポートできます。操作モードの変更が完了したら、構成をインポートできます。インポートされた構成は FIPS-CCセキュリティ機能 ごとに編集する必要があります。編集しないと、インポート処理が失敗します。

キー、パスワード、およびその他の重要なセキュリティ パラメータは、モード間で共有できません。

Panorama 管理サーバーによって管理されるファイアウォールまたは専用 *Log Collector* の動作モードを *FIPS-CC* モードに変更する場合は、*Panorama* の動作モードを *FIPS-CC* モードに変更する必要があります。*Panorama* からプッシュされたローカル管理者パスワードのパスワードのセキュリティを確保するために必要です。

STEP 1 | (Existing HA Configuration only) 高可用性 (HA) 構成を無効にします。

これは、すでに HA 構成になっている firewall の動作モードを FIPS-CC モードに正常に変更するために必要です。

1. プライマリ HA ピアの firewall Web インターフェイス にログインします。
2. **Device** > **High Availability** > **General** を選択し、HA Pair Settings Setup を編集します。
3. [**HA** を有効にする] をオフ (無効) にし、 [**OK**] をクリックします。
4. **[コミット]** します。

STEP 2 | (パブリッククラウドVM-SeriesファイアウォールまたはパブリッククラウドPanorama仮想アプライアンスのみ)SSH キーを作成し、ファイアウォールまたは Panorama にログインします。

Microsoft Azure などの一部のパブリック クラウド プラットフォーム上では、FIPS-CC モードに変更した後の認証の失敗を防ぐために、SSH キーが必要です。SSH キーを使用して、認証にファイアウォールをデプロイしたことを確認します。Azure 上で VM-Series ファイアウォールまたは Panorama をデプロイし、ユーザー名とパスワードを使用してログインすることは可能ですが、操作モードを FIPS-CC に変更すると、そのユーザー名とパスワードを使

用して認証できなくなります。FIPS-CCモード へのリセット後、SSH キーを使用してログインする必要があります。その後、ファイアウォール Webインターフェースに後でログインするために使用できるユーザー名とパスワードを設定できます。

STEP 3 | firewallまたはアプライアンスに接続して、Maintenance Recovery Tool (MRT)にアクセスします。

STEP 4 | メニューから **Set FIPS-CC Mode** [FIPS-C Cモードを設定]を選択します。

STEP 5 | **Enable FIPS-CC Mode (FIPS-CC** モードの有効化**)** を選択します。モード変更操作は完全な工場出荷時のリセットを開始し、ステータス インジケータが進行状況を示します。モード変更が完了したら、ステータスが Success (成功) になります。

すべての設定と設定は消去され、モードの変更が完了すると取得できません。

STEP 6 | プロンプトが表示されたら、**Reboot**[再起動]を選択します。

パブリック クラウドでデプロイした *VM-Series* ファイアウォール上で操作モードを変更し、***Reboot* (**再起動**)** を行う前に *MRT* との *SSH* 接続が解除された場合、モード変更が完了し、*MRT* に再度ログインし、ファイアウォールを再起動して操作を完了させるまで、*10*～*15* 分待つ必要があります。*FIPS-CC* モードへのリセット後、一部の仮想フォームファクタ *(Panorama* または *VM-Series)*では、*SSH* キーを使用してのみログインでき、*SSH* キーを使用して認証をセットアップしていない場合は、再起動時にファイアウォールにログインできなくなります。

FIPS-CC モードに切り替えると、次のステータスが表示されます。`FIPS-CC mode enabled successfully`.

さらに、次のような変化もあります。

- Web インターフェイスの下部にあるステータス バーに常に FIPS-CC と表示されます。
- デフォルトの管理者ログイン認証情報が admin/paloalto に変更されます。

FIPS-CC モードで適用されるセキュリティー機能について詳しくは、FIPS-CCセキュリティ機能を参照してください。

STEP 7 | (Existing HA のみ)HA を再度有効にします。

このステップは、FIPS-CC モードに変更する前に HA で構成された firewall に必要です。

HA を初めてセットアップする方法の詳細については、High Availability を参照してください。

1. プライマリ HA ピアの firewall Web インターフェイス にログインします。
2. **Device** > **High Availability** > **General** を選択し、HA Pair Settings Setup を編集します。
3. **HA** を有効にする にチェックを入れ、**OK** をクリックします。
4. **[コミット]** します。

STEP 8 | HA1 制御リンク の暗号化を有効にします。

これは、HA 構成の FIPS-CC モードのすべての firewall に必要です。

FIPS-CC モードで firewall に HA を正常に活用するには、自動キー更新パラメーターを設定し、データ・パラメーターを 1000 MB 以下の値に設定する必要があります。キーをデフォルトのままにすることはできず、時間間隔を設定する必要があります (無効のままにすることはできません)。

FIPS-CCセキュリティ機能

FIPS-CC モードが有効になると、以下のセキュリティ機能がすべてのファイアウォールおよびアプライアンスに適用されます。

- ログインするには、ブラウザがTLS 1.2(またはそれ以降)と互換性がなければなりません。WF-500 アプライアンスでは、CLI を介してのみアプライアンスを管理し、SSHv2 互換のクライアント アプリケーションを使用して接続する必要があります。
- すべてのパスワードは 8 文字以上でなければなりません。
- 認証設定の **Failed Attempts (**試行失敗回数**)** および **Lockout Time (min) (**ロックアウト時間（分）**)** が必ず 0 より大きくなければなりません。**Failed Attempts (**試行回数**)** に達した管理者は、**Lockout Time (min) (**ロックアウト時間（分）**)** フィールドで指定した期間、アクセスを拒否されます。
- 認証設定の **Idle Timeout (**アイドル タイムアウト**)** が必ず 0 より大きくなければなりません。ログイン セッションのアイドル状態が指定された期間を超えると、管理者が自動的にログアウトします。
- **Absolute Session Length (**絶対セッション長**)** を設定して、ユーザーがログインできる最大時間を分単位で設定できます。設定できる最小長は60分間です。タイムアウトの5分前にセッション終了の警告を受信します。この機能は FIPS-CC モードでは無効にできず、デフォルトでは30日間のセッションです。
- **Max No. of Session (**最大セッション数**)** を設定して、同じ管理者アカウントに同時にログインできるユーザー数を設定できます。
- ファイアウォールあるいはアプライアンスは適切な自己テストレベルを自動的に判断し、暗号化アルゴリズムと暗号スイートに適切なレベルの強度を適用します。
- 未承認の FIPS-CC アルゴリズムは復号化されません。復号化の際は無視されます。
- MS-CHAPv2 は FIPS-CC モードと互換性がありません。TLS で RADIUS を使用することをお勧めします。
- IPSec VPN を設定する場合、管理者は IPSec のセットアップ時に表示された暗号スイート オプションを選択する必要があります。
- (Panorama および WildFire のみ) 管理インターフェースで IPSec を有効にして、NTP、RADIUS、TACACS、DNS などのプロトコルを保護できます。
- 自己生成証明書およびインポート証明書には、RSA 2,048 ビット (またはそれ以上) または ECDSA 256 ビット (またはそれ以上) の公開鍵が含まれている必要があります。また、SHA256 以上のダイジェストを使用する必要があります。
- Telnet、TFTP、および HTTP 管理接続は使用できません。
- (New HA Deployments) FIPS-CC モードで firewall に対して high availability (HA) をセットアップするときに、HA1 制御リンク の暗号化を有効にする必要があります。自動鍵変更のパラメーターを設定する必要があります。データ パラメーターを 1000 MB 以下の値に設定し (デフォルトにはできません)、時間間隔を設定する必要があります (無効にすることはできません)。

- (既存のHA展開) 高可用性 (HA) 構成の firewall に対して 操作モードを FIPS-CC モード に変更する前に、操作モードを FIPS-CC モードに変更する前に、まず HA (デバイス > **High Availability** > 一般) を無効にする必要があります。

  両方の HA ピアで操作モードを FIPS-CC モードに変更した後、上記のように HA を再度有効にし、HA1 control link の暗号化を有効にします。
- FIPS-CC モードのシリアルコンソール ポートは制限付きのステータス出力ポートとしてのみ機能します。CLI でアクセスすることはできません。
- MRT として起動したプライベート クラウド VM-Series ファイアウォールおよびハードウェアのシリアルコンソール ポートは、MRT へのインタラクティブなアクセスを提供します。
- インタラクティブなコンソールへのアクセスは、MRT として起動したハイパーバイザー環境のプライベート クラウド VM-Series ファイアウォールではサポートされていないため、SSH を使わなければ MRT にアクセスできません。
- 古いマスターキーの有効期限が切れる前に、新しい マスターキー を手動で設定する必要があります。**FIPS-CC** モードでは、マスター鍵 の自動更新はサポートされていません。

  マスター キーが失効すると、ファイアウォールまたは Panorama は自動的にメンテナンス モードで再起動されます。次にファイアウォールの工場出荷時設定へのリセットを行う必要があります。
- FIPS-CC モードが有効になっている場合、Zero Touch Provisioning (ZTP) モードは Palo Alto Networks ファイアウォールで無効になります。
- (Panorama管理対象デバイス)FIPS-CC が有効になっている場合、firewall および Log Collectors の Panorama サポートを確認します。

Panorama	ファイアウォール		ログ コレクタ	
FIPS-CC が有効	FIPS-CC が有効	FIPS-CC が無効	FIPS-CC が有効	FIPS-CC が無効
	サポート	サポート	サポート	サポート
FIPS-CC が無効	サポートされていません	サポート	サポートされていません	サポート

- (Panorama管理対処湯デバイス) FIPS-CC モードの Panorama および管理対象デバイスを PAN-OS 10.2 以降のリリースにアップグレードするには、PAN-OS 10.2 リリースの実行中に Panorama 管理に追加した場合、FIPS-CC モードのデバイスのセキュア接続ステータスをリセットする必要があります。

  詳細については、「Upgrade Panorama and Managed Devices in FIPS-CC モードを参照してください。
- (PA-7000シリーズ ファイアウォールのみ) Palo Alto Networks Hardware End of Life Dates および Compatibility Matrix を確認して、サポートされているラインカードがあることを確認します。サポート終了に達したラインカード、またはサポートされていない PAN-OS リリースを実行しているラインカードは、PA-7000シリーズファイアウォールがメンテナンス モードに入る原因となることがあります。

FIPS-CC モードで実行中のファイアウォールあるいはアプライアンスにおけるスワップメモリのスクラブ

firewallまたはアプライアンスを(FIPS-CCモードで)使用停止にするか、修理のために送付する前に、機密情報がスワップメモリから削除されていることを確認する必要があります。この作業を行い、すべての暗号セキュリティ パラメーター（CSP）情報をスワップ領域から削除します。

Panorama によって管理されている *firewall* を修理のために送付する場合は、Before Starting RMA Firewall Replacement.

を参照してください。

STEP 1 | ファイアウォールあるいはアプライアンスへの SSH 管理セッションを開きます。

STEP 2 | 次の操作コマンドを実行します：

```
request [restart | shutdown] system with-swap-scrub [dod | nnsa]
```

例えば、ファイアウォールあるいはアプライアンスをシャットダウンして Department of Defense（DoD）スクラブを実行する場合、次のコマンドを実行します：

```
request shutdown system with-swap-scrub dod
```

STEP 3 | 警告プロンプトが表示されたら**Y**を押してスクラブを開始します。

STEP 4 | スクラブが正常に完了したことを確認します。swapという語のところで**System (**システム**)**ログおよびフィルターを表示します。**System (**システム**)**ログは、各スワップ領域（パーティションはモデルによって 1 つあるいは 2 つ）のスクラブ ステータス、およびスクラブ全体のステータスを示すログ エントリを示します。すべてのスワップ領域に対してス

クラブが正常に完了している場合、**System (**システム**)**ログに`Swap space scrub was successful`と表示されます。

いずれかのスワップ領域でスクラブが失敗した場合、**System (**システム**)**ログに`Swap space scrub was unsuccessful`と表示されます。次のスクリーンショットは、2 つのパーティションを持つファイアウォールのログ結果を示しています。

06/08 10:24:02	general	medium	general		Swap space scrub was successful
06/08 10:24:02	general	medium	general		Scrub performed on swap space /opt/panlogs/.secondary_swapfile
06/08 10:24:02	general	medium	general		Scrub performed on swap space /dev/sda7

CLI を使ってスクラブ ログを表示する場合は、***show log system | match swap***コマンドを実行します。

シャットダウン コマンドを使ってスクラブを開始する場合、スクラブが完了した後にファイアウォールあるいはアプライアンスの電源がオフになります。まずは電源を外し、接続し直してからファイアウォールあるいはアプライアンスの電源を入れてください。