paloalto TECHDOCS

Advanced Threat Preventionの管理

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2022-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

May 18, 2023

Table of Contents

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

高度な脅威防御

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

Palo Alto Networks®の次世代ファイアウォール脅威侵入防御サブスクリプションは、多面的な検出メカニズムを使用して、脅威のランドスケープの全範囲に対抗するために、コモディティの脅威や高度な永続的な脅威(APT)からネットワークを保護し、防御します。Palo Alto Networksの脅威防御ソリューションは、以下のサブスクリプションで構成されています。

- **Advanced Threat Prevention**: Advanced Threat Preventionクラウド サービスは、インラインのディープ ラーニングと機械学習モデルを使用して、回避的でこれまでに見たことのない未知のC2脅威とゼロデイ脆弱性エクスプロイトをリアルタイムで検出します。超低レイテンシのネイティブクラウドサービスとして、この拡張可能で無限にスケーラブルなソリューションは、モデルトレーニングの改善により常に最新の状態に保たれます。また、ゼロデイ脅威やその他の回避脅威をローカル ディープ ラーニングベースで高速に解析するメカニズムを提供することで、Advanced Threat Preventionのクラウドベースのインライン クラウド解析コンポーネントを補完するローカル ディープ ラーニングもサポートしています。Advanced Threat Prevention（高度な脅威防御） ライセンスには、Threat Prevention（脅威防御） に含まれるすべての利点が含まれています。
- 脅威防御: ベースの脅威防御サブスクリプションは、さまざまなPalo Alto Networksサービスから収集された悪意のあるトラフィック データから生成されたシグネチャに基づいています。これらのシグネチャは、コマンド アンド コントロール (C2)、さまざまな種類の既知のマルウェア、脆弱性の悪用など、特定の脅威に基づいてセキュリティ ポリシーを適用するために ファイアウォール によって使用されます。また、ファイアウォール の App-ID およびユーザー ID 識別テクノロジと組み合わせることで、コンテキスト データを相互参照して、きめ細かいポリシーを生成できます。脅威軽減ポリシーの一環として、既知または危険なファイルの種類と IP アドレスを特定してブロックすることもできます。これらのファイルの種類と IP アドレスは、防弾サービス プロバイダーや既知の悪意のある IP を指定するリストなど、事前に作成されたいくつかのカテゴリを使用できます。特殊なツールやソフトウェアを使用する場合は、独自の脆弱性シグネチャを作成して、侵入防御機能をネットワーク固有の要件に合わせてカスタマイズできます。

Palo Alto Networksでは、脅威防御を最大限に高めるために、Advanced | Threat Preventionに加えて、以下のサブスクリプション サービスも推奨しています。

- **DNS** セキュリティ: 高度な DNS ベースの脅威から組織を保護するために設計されたDNS セキュリティ クラウド サービス。DNS Securityは、高度な機械学習と予測分析をさまざまな脅威インテリジェンスソースに適用することで、強化されたDNSシグネチャセットを生成し、DNSリクエストのリアルタイム分析を提供して、新しく生成された悪意のあるドメインからネットワークを保護します。DNS Securityは、DNSトンネリング、DNS再バインド攻撃、自動生成を使用して作成されたドメイン、マルウェアホストなど、さまざまなC2脅威を検出できます。DNS Security は、完全な DNS 脅威カバレッジのために、Advanced Threat Prevention（高度な脅威防御） または Threat Prevention （脅威防御）サブスクリプションを必要とし、連携します。

Palo Alto Networksの侵入防御サブスクリプションは連携して、攻撃プロセスのさまざまな段階でチェーンを傍受して切断し、ネットワークインフラストラクチャのセキュリティ侵害を防ぐための可視性を提供する包括的なソリューションを提供します。

©2025 Palo Alto Networks, Inc.

Advanced Threat Prevention検出サービス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

Advanced Threat Prevention(高度な脅威防御)は侵入防御システム(IPS)ソリューションで、ファイアウォールとクラウドで動作するコンポーネントを備えた多層防御システムを使用して、すべてのポートとプロトコルでマルウェア、脆弱性の悪用、およびコマンド アンド コントロール(C2)を検出してブロックできます。脅威防御クラウドは、Palo Alto Networksサービスからの脅威データを組み合わせて多数の検出サービスを実行し、それぞれが特定の識別可能なパターンを持つシグネチャを作成し、ファイアウォールによって、一致する脅威と悪意のある動作が検出されたときにセキュリティポリシーを適用するために使用されます。これらのシグネチャは、脅威の種類に基づいて分類され、一意の識別子番号が割り当てられます。これらのシグネチャに対応する脅威を検出するために、firewall は、異常な特性を示すネットワーク トラフィックを検査および分類する分析エンジンを操作します。

Advanced Threat Prevention（高度な脅威防御） クラウド のこれらのディープラーニング、MLベースの検出エンジンは、SQLインジェクションとコマンドインジェクションを利用する未知のC2 および脆弱性のトラフィックを分析し、ゼロデイ脅威からユーザーを保護します。Advanced Threat Preventionクラウドは、拡張可能なディープ ラーニング モデルを運用し、要求ごとにファイアウォールでインライン解析機能を有効にして、ゼロデイ脅威がネットワークに侵入するのを防ぐとともに、保護を分散させます。これにより、インライン検出器を使用したリアルタイムのトラフィック検査を使用して、未知の脅威を防ぐことができます。Advanced Threat Preventionクラウドのこれらのディープ ラーニング、MLベースの検出エンジンは、SQLインジェクションとコマンド インジェクションを利用する未知のC2および脆弱性のトラフィックを解析し、ゼロデイ脅威からユーザーを保護します。脅威のコンテキストと包括的な検出の詳細を提供するために、レポートが生成されます。レポートには、攻撃者が使用したツールや手法、検出の範囲、影響のほか、MITRE ATT&CK®フレームワークで定義された対応するサイバー攻撃の分類が含まれます。

*MITRE ATT&CK®*は、サイバー敵対行動のためのキュレーションされたナレッジベースおよびモデルです。本作品は、*MITRE Corporation*の許可を得て複製・配布しています。*MITRE Corporation* (以下*MITRE*)は、*ATT&CK®*を研究、開発、商業目的で使用するための非独占的かつロイヤリティフリーなライセンスをお客様に許諾します。そのような目的で作成されたコピーは、*MITRE*の著作権指定および本ライセンスをそのようなコピーに複製することを条件に許可されます。

©2025 Palo Alto Networks, Inc.

クラウドベースの検出エンジンを操作することで、ユーザーがコンテンツ パッケージをダウンロードしたり、リソースを消費する可能性のあるプロセス集約型のファイアウォールベースのアナライザーを操作したりすることなく、自動的に更新および展開される幅広い検出メカニズムにアクセスできます。クラウドベースの検出エンジン ロジックは、WildFireのC2トラフィック データセットを使用して継続的に監視および更新され、Palo Alto Networksの脅威研究者による追加のサポートにより、高度に高速化された検出機能強化のための人間の介入を提供します。Advanced Threat Preventionのディープ ラーニング エンジンは、HTTP、HTTP2、SSL、未知のUDP、および未知のTCPアプリケーション上のC2ベースの脅威の解析をサポートします。追加の解析モデルはコンテンツの更新によって提供されますが、既存のモデルに対する拡張機能はクラウド側の更新として実行され、ファイアウォールの更新は必要ありません。

Advanced Threat Preventionは、Advanced Threat Preventionのクラウドベースのインライン クラウド解析コンポーネントを補完する機能として、ゼロデイ脅威やその他の回避脅威をローカル ディープ ラーニングベースで高速に解析するメカニズムを提供するLocal Deep Learning (ローカル ディープ ラーニング)もサポートします。Palo Alto Networksが公開したシグニチャ セットと一致する既知の悪意のあるトラフィックはドロップされます(または、別のユーザー定義のアクションが適用されます)。ただし、疑わしいコンテンツの基準に一致する特定のトラフィックは、ディープ ラーニング解析検出モジュールを使用して解析用にルート変更されます。さらなる解析が必要な場合、トラフィックはAdvanced Threat Preventionクラウドに送られ、追加解析が行われます。また、必須の誤検知および偽陰性チェックも行われます。ディープ ラーニング検出モジュールは、Advanced Threat Preventionクラウドで動作する実証済みの検出モジュールをベースとしており、それと同様にゼロデイおよび高度な脅威検出機能を備えています。しかし、クラウド クエリに伴う遅延がなく、はるかに大量のトラフィックを処理できるという追加の利点もあります。これにより、より多くのトラフィックを検査し、より短いスパンで判定を受け取ることができます。これは、困難なネットワーク条件に直面したときに特に有益です。

*Palo Alto Networks*では、クラウドベースの*Advanced Threat Prevention*ライセンスに含まれる機能を含まない脅威防御サブスクリプションも提供しています。

ファイアウォールで使用される脅威シグネチャは、アンチウイルス、アンチスパイウェア、脆弱性の3種類に大別され、対応するセキュリティ プロファイルによってユーザー定義のポリシーを適用するために使用されます。

©2025 Palo Alto Networks, Inc.

Palo Alto Networks がクラウド提供するセキュリティサービスは、それぞれのサービスに対して*WildFire*および*DNS C2*シグネチャと、脅威シグネチャの代わりにファイルタイプを指定できるファイル形式シグネチャも生成します。たとえば、署名の例外などです。

- ウイルス対策シグネチャは、ワーム、トロイの木馬、スパイウェアのダウンロードなど、さまざまな種類のマルウェアやウイルスを検出します。
- アンチスパイウェア シグネチャは、侵害されたホスト上のC2スパイウェアが、オートコールまたはビーコンを外部のC2サーバーに送信しようとすることを検出します。
- 脆弱性シグネチャは、エクスプロイトシステムの脆弱性を検出します。

シグネチャには、デフォルトの重大度レベルと、関連するデフォルト アクションがあります。たとえば、非常に悪意のある脅威の場合、デフォルトのアクションは[Reset Both (両方をリセット)]になります。この設定は、Palo Alto Networks のセキュリティに関する推奨事項に基づいています。

特殊な内部アプリケーションが存在する展開や、オープンソースのSnortルールとSuricataルールが使用されているサードパーティのインテリジェンス フィードでは、専用の保護のためにカスタム シグネチャを作成できます。

Firewallsは、毎日のウイルス対策コンテンツと毎週のアプリケーションおよび脅威コンテンツの更新の2つのアップデートパッケージの形でシグネチャアップデートを受け取ります。アンチウイルス コンテンツの更新には、アンチウイルスおよびアンチスパイウェアのセキュリティ プロファイルがそれぞれ使用する、アンチウイルス シグネチャとDNS (C2)シグネチャが含まれます。アプリケーションおよび脅威のコンテンツ更新には、脆弱性およびアンチスパイウェアのセキュリティ プロファイルがそれぞれ使用する、脆弱性シグネチャとアンチスパイウェア シグネチャが含まれます。更新プログラム パッケージには、他のサービスやサブ機能によって活用される追加コンテンツも含まれています。詳細については、Dynamic Content Updates を参照してください。

©2025 Palo Alto Networks, Inc.

脅威シグネチャのカテゴリ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

Palo Alto Networksの脅威シグネチャには3つの種類があり、いずれもネットワーク トラフィックをスキャンする際に異なる脅威を検出するように設計されています。

- アンチウイルス シグネチャ–実行ファイル内のウイルスおよびマルウェア、ファイルの種類を検出します。
- アンチスパイウェア シグネチャ–感染したクライアント上のスパイウェアがユーザーの同意成しにデータを収集する、および/または離れた攻撃者と通信するコマンド アンド コントロール（C2）アクティビティを検出します。
- 脆弱性シグネチャ–攻撃者がエクスプロイトの対象にし得るシステムの欠陥を検出します。

シグネチャの重大度は検出されたイベントのリスクを示し、シグネチャのデフォルトのアクション（例：ブロックあるいはアラート）は、マッチするトラフィックに対して適用する Palo Alto Networks が推奨するアクションを示します。

アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップを行って、脅威を検出した際に行うアクションを定義する必要があります。また、デフォルトのセキュリティ プロファイルを使って、Palo Alto Networksの推奨事項に基づいて簡単に脅威のブロックを開始できます。各シグネチャ タイプ、カテゴリー、特定のシグネチャについて、新しいプロファイルを作成あるいは編集する作業を進め、潜在的な脅威に細かく対応できます。

次の表は、すべてのシグネチャ カテゴリーをタイプ毎（アンチウイルス、スパイウェア、脆弱性）に一覧表示しています。また、各カテゴリーのシグネチャを提供するコンテンツ更新（アプリケーションおよび脅威、アンチウイルス、WildFire）も含まれています。また、Palo Alto Networks Threat Vault にアクセスして脅威シグネチャの詳細を把握することもできます。

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	詳説
アンチウイルス シグネチャ		

©2025 Palo Alto Networks, Inc.

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	詳説
apk	Antivirus [アンチウイルス] WildFire	悪意のある Android Application（APK）ファイル。
MacOSX	Antivirus [アンチウイルス] WildFire	次のような悪意のある MacOSX ファイル: • Apple ディスク イメージ (DMG) ファイル • Machオブジェクトファイル(Mach-O)は、実行可能ファイル、ライブラリ、およびオブジェクトコード • Apple ソフトウェア インストーラー パッケージ (PKG)
Flash	Antivirus（アンチウイルス） WildFire または WildFire Private	Web ページに組み込まれている Adobe Flashアプレットおよびフラッシュコンテンツ
jar	Antivirus [アンチウイルス] WildFire	Java アプレット（JAR/クラス ファイル タイプ）。
ms-office	Antivirus [アンチウイルス] WildFire または WildFire Private	ドキュメント（DOC、DOCX、RTF）、ワークブック（XLS、XLSX）、PowerPoint プレゼンテーション（PPT、PPTX）を含む Microsoft Office ファイル。これには、Office Open XML (OOXML) 2007+ ドキュメントも含まれます。
pdf	Antivirus（アンチウイルス） WildFire または WildFire Private	ポータブルドキュメントフォーマット（PDF）ファイル。
pe	Antivirus（アンチウイルス） WildFire または WildFire Private	Portable executable（PE）ファイルは Microsoft Windows システムで自動的に実行され、身元が確認できる場合のみ許可できます。これには次のようなファイル形式があります： • オブジェクトコード。 • フォント（FON）。 • システムファイル（SYS）。

©2025 Palo Alto Networks, Inc.

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	詳説
		• ドライバーファイル（DRV）。 • Windows コントロールパネルのアイテム（CPL）。 • DLL（ダイナミック リンク ライブラリ）。 • OCX（OLE カスタムコントロール、あるいは ActiveX コントロール用ライブラリ）。 • Windows スクリーンセーバー ファイル (SCR)。 • デバイスの更新および起動操作をサポートする、OS およびファームウェアの間で実行される Extensible Firmware Interface（EFI）ファイル。 • プログラム情報ファイル（PIF）。
linux	Antivirus [アンチウイルス] WildFire	実行可能およびリンク可能な形式（ELF）ファイル。
アーカイブ	Antivirus [アンチウイルス] WildFire	Roshalアーカイブ（RAR）と7-Zip（7z）アーカイブファイル。
スパイウェア シグネチャ		
［Adware］	アプリケーションおよび脅威	好ましくない広告を表示するおそれのあるプログラムを検出します。一部のアドウェアはブラウザに変更を加え、頻繁に検索されるキーワードを Web ページ上でハイライト表示し、ハイパーリンクを付与します。これらのリンクは、ユーザーを広告サイトにリダイレクトさせます。また、アドウェアはコマンド アンド コントロール（C2）サーバーからアップデートを取得し、それをブラウザやクライアントシステムにインストールすることもできます。 このカテゴリーで新たにリリースされる保護はあまりありません。
autogen	Antivirus（アンチウイルス）	このペイロード ベースのシグネチャは、コマンド アンド コントロール（C2）トラフィックを検出し、自動生成されます。自動生成されたシグネチャは C2 ホストが未知である場合、あるいは急速に変化する場合でも C2 トラフィックを検出できるというのが重要です。

©2025 Palo Alto Networks, Inc.

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	詳説
backdoor	アプリケーションおよび脅威	攻撃者がシステムへの不正なリモートアクセスを得られるようにするプログラムを検出します。
［Botnet］	アプリケーションおよび脅威	ボットネット アクティビティを示します。ボットネットとは、攻撃者が制御する、マルウェアに感染したコンピューター（ボット）のネットワークのことです。攻撃者はボットネットの全コンピューターに一元的に命令を出し、同時に一斉にアクション（例えば DoS 攻撃などを行う）を実行させます。
browser-hijack	アプリケーションおよび脅威	ブラウザ設定を変更しているプラグインやソフトウェアを検出します。ブラウザを乗っ取った攻撃者は、自動検索をコントロールしたり、ユーザーのウェブ アクティビティを追跡したり、その情報を C2 サーバーに送信したりする可能性があります。 このカテゴリーで新たにリリースされる保護はあまりありません。
クリプトマイナー	アプリケーションおよび脅威	(クリプトジャッキングまたはマイナーと呼ばれることもあります) ユーザーの知らないうちにコンピューティング リソースを使用して暗号通貨をマイニングするように設計された悪意のあるプログラムから生成されたダウンロードの試行またはネットワーク トラフィックを検出します。クリプトマイナー バイナリは、システム アーキテクチャを決定し、システム上の他のマイナー プロセスを強制終了しようとするシェル スクリプト ダウンローダーによって頻繁に配信されます。一部のマイナーは、悪意のある Web ページをレンダリングする Web ブラウザなど、他のプロセス内で実行します。
data-theft	アプリケーションおよび脅威	情報を既知の C2 サーバーに送信しているシステムを検出します。 このカテゴリーで新たにリリースされる保護はあまりありません。
dns	Antivirus（アンチウイルス）	悪意のあるドメインに接続するための DNS リクエストを検出します。 dns および dns-wildfire シグネチャは、同じ悪意のあるドメインを検出しますが、dns シグネチャは日次のアンチウイルス コンテンツ更新に、dns-wildfire シグネ

©2025 Palo Alto Networks, Inc.

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	詳説
		チャは 5 分毎に保護をリリースする WildFire 更新に含まれます。
dns-security	Antivirus（アンチウイルス）	悪意のあるドメインに接続するための DNS リクエストを検出します。 dns-security には、DNS Security サービスによって生成された固有の署名に加えて、dns および dns-wildfire からの署名が含まれています。
dns-wildfire	WildFire または WildFire Private	悪意のあるドメインに接続するための DNS リクエストを検出します。 dns および dns-wildfire シグネチャは、同じ悪意のあるドメインを検出しますが、dns シグネチャは日次のアンチウイルス コンテンツ更新に、dns-wildfire シグネチャは 5 分毎に保護をリリースする WildFire 更新に含まれます。
ダウンローダー	アプリケーションおよび脅威	（ドロッパー、ステージャー、ローダーとも呼ばれる） インターネット接続を使用してリモート サーバーに接続し、侵入先のシステムにマルウェアをダウンロードして実行するプログラムを検出します。最も一般的な使用例は、ダウンローダーがサイバー攻撃のステージ*1*の集大成として展開されることであり、ダウンローダーのフェッチされたペイロードの実行は、ステージ*2*と見なされます。シェルスクリプト (Bash、PowerShell など)、トロイの木馬、および PDFや Word ファイルなどの悪意のあるルアー ドキュメント (maldocs とも呼ばれます) は、一般的なダウンローダータイプです。
詐欺行為	アプリケーションおよび脅威	(フォームジャック、フィッシング、詐欺を含む) ユーザーの機密情報を収集するため悪意のある JavaScript コードが挿入されていると判断された侵害された Web サイトへのアクセスを検出します。(例えば：名前、住所、メール アドレス、クレジットカード番号、CVV、有効期限等) eコマース Web サイトの決済ページにある支払いフォームから。
hacktool	アプリケーションおよび脅威	悪意のある攻撃者が偵察を行ったり、脆弱なシステムを攻撃またはアクセスしたり、データを盗み出したり、コマンドと制御チャネルを作成して許可なくコンピュー タシステムを密かに制御したりする目的でソ

©2025 Palo Alto Networks, Inc.

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	詳説
		フトウェア ツールを用いて生成したトラフィックを検出します。これらのプログラムは、マルウェアやサイバー攻撃との関連度が高いです。ハッキング ツールは、Red team および Blue team の運用、侵入テスト、ならびに R&D で使用される場合、良識ある方法で展開される可能性があります。これらのツールの使用または所持は、意図に関係なく、一部の国では違法である可能性があります。
Keylogger	アプリケーションおよび脅威	攻撃者がキー操作を記録し、スクリーンショットを撮影してユーザーアクティビティを密かに追跡できるようにするプログラムを検出します。 キーロガーは様々な C2 手法を使用し、定期的にログおよびレポートを事前定義済みのメールアドレスあるいは C2 サーバーに送信します。キーロガーによる監視を通じて、攻撃者がネットワーク アクセスを可能にする認証情報を入手する可能性もあります。
networm	アプリケーションおよび脅威	自己増殖し、システムからシステムへと広がるプログラムを検出します。ネットワームは、共有リソースを使用し、あるいはセキュリティの不備を利用して目標のシステムにアクセスする可能性があります。
phishing-kit	アプリケーションおよび脅威	ユーザーがフィッシング キットのランディングページに接続しようとしているのを検出します（悪意のあるサイトへのリンクが記載されたメールの受信後が多い）。フィッシング サイトは、ユーザーをだまして認証情報を送信させ、攻撃者がその情報を盗んでネットワークへのアクセスを得られるようにします。 フィッシング キットのランディングページへのアクセスをブロックするだけでなく、多要素認証および認証情報フィッシング防止を有効化することで、あらゆる段階でフィッシング攻撃を防ぐことができます。
post-exploitation	アプリケーションおよび脅威	攻撃者が侵入したシステムの価値を評価しようとするエクスプロイト後の段階を示唆するアクティビティを検出します。これには、システムに保存されているデータの重要性、さらにネットワークに侵入する上で

©2025 Palo Alto Networks, Inc.

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	詳説
		そのシステムがどの程度重要かを評価することが含まれます。
webshell	アプリケーションおよび脅威	インプラントの検出やコマンドと制御の相互通信など、Web シェルと Web シェル トラフィックを検出します。Web シェルは、最初に悪意のある攻撃者によって侵害されたホストに埋め込まれる必要があり、ほとんどの場合、Web サーバーまたはフレームワークを標的にします。その後のWebシェルファイルとの通信により、悪意のある攻撃者がシステムに足場を確立し、Webサーバーユーザーのコンテキストでサービスとネットワークの列挙、データの漏えい、およびリモートコード実行を行うことができます。最も一般的な Web シェル タイプは、PHP、.NET、および Perl マークアップ スクリプトです。また、攻撃者はウェブシェルに感染した Web サーバー（インターネットに接続されたサーバー、内部システムの両方）を利用し、その他の内部システムもターゲットにします。
spyware	アプリケーションおよび脅威	アウトバウンド C2 通信を検出します。これらのシグネチャは自動生成されるか、Palo Alto Networks の調査員が手作業で作成します。 スパイウェアおよび自動生成シグネチャの両方がアウトバウンド *C2* 通信を検出しますが、自動生成シグネチャはペイロード ベースであり、未知、あるいは急速に変化する *C2* ホストとの *C2* 通信を一意に検出できます。
脆弱性シグネチャ		
brute force	アプリケーションおよび脅威	ブルート フォース シグネチャは、一定期間に繰り返し生じる事象を検出します。正当なアクティビティが隔離される可能性もありますが、ブルート フォース シグネチャはアクティビティの正当性が疑わしくなるような頻度を示唆します。例えば、FTP ログインが一度失敗しても、悪意のあるアクティビティにはなりません。しかし、短期間に FTP ログインが多く失敗した場合、攻撃者が FTP サーバーへのアクセスを求めて組み合わせを変えながらパスワードを試していることが示唆されます。

©2025 Palo Alto Networks, Inc.

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	詳説
		ブルート フォース シグネチャのアクションおよび発動条件を調整できます。
code execution	アプリケーションおよび脅威	攻撃者が悪用し、ログイン済みのユーザーの権限でシステム上でコードを実行できるようにする、コード実行時の脆弱性を検出します。
code-obfuscation	アプリケーションおよび脅威	機能を維持したまま特定のデータを隠蔽するよう変更されたコードを検出します。難読化されたコードは読みづらい、あるいは判読不可能であるため、どのようなコマンドをコードが実行しているのか、どのプログラムとやり取りするよう設計されているのかをすぐに把握できません。最も多いのは、攻撃者がコードを難読化してマルウェアを隠蔽することです。それより頻度は落ちますが、プライバシー、知的財産を保護する、あるいはユーザーエクスペリエンスを向上させるために、正当な開発者がコードを難読化することもあります。例えば、ファイル サイズを減らしてウェブサイトの読み込み時間と帯域幅の消費量を減らす特定の難読化（ミニマイズ）があります。
dos	アプリケーションおよび脅威	攻撃者が目標のシステムを利用不可能にし、一時的にシステムおよびそれに従属するアプリケーションおよびサービスを中断させる、サービス拒否（DoS）攻撃を検出します。DoS 攻撃を行うために、攻撃者は目標のシステムに大量のトラフィックを送ったり、エラーを発生させる情報を送信したりします。DoS 攻撃は、サービスの正当なユーザー（従業員、会員、アカウント所有者など）やユーザーがアクセスできるリソースなどを奪います。
exploit-kit	アプリケーションおよび脅威	エクスプロイトキットのランディングページを検出します。エクスプロイトキットのランディングページには、複数のブラウザおよびプラグインに関して、一つあるいは多くの共通脆弱性識別子（CVE）をターゲットにする複数のエクスプロイトが含まれていることが多くあります。目標の CVE はすぐに変化するため、エクスプロイトキット シグネチャは CVE ではなくエクスプロイトキットのランディングページに基づいて発動します。 エクスプロイトキットを含むウェブサイトにユーザーがアクセスする際、エクスプロイトキットは目標の

©2025 Palo Alto Networks, Inc.

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	詳説
		CVE をスキャンし、被害者のコンピューターに悪意のあるペイロードを密かに送り込もうとします。
info-leak	アプリケーションおよび脅威	攻撃者がエクスプロイトしてセンシティブあるいは占有情報を盗む可能性があるソフトウェアの脆弱性を検出します。通常、データを保護する包括的なチェックは存在しないため、情報流出が発生する可能性があり、攻撃者は巧妙なリクエストを送信して情報流出をエクスプロイトできます。
insecure-credentials	アプリケーションおよび脅威	ソフトウェア、ネットワークアプライアンス、および IoT デバイスの脆弱な、侵害された、製造元のデフォルトのパスワードの使用を検出します。
オーバーフロー	アプリケーションおよび脅威	リクエストのチェックが不適切であり、攻撃者がエクスプロイトする可能性があるオーバーフローの脆弱性を検出します。攻撃が成功すると、アプリケーション、サーバー、あるいはオペレーティングシステムの権限でリモートからコードを実行できる可能性があります。
phishing	アプリケーションおよび脅威	ユーザーがフィッシング キットのランディングページに接続しようとしているのを検出します（悪意のあるサイトへのリンクが記載されたメールの受信後が多い）。フィッシング サイトは、ユーザーをだまして認証情報を送信させ、攻撃者がその情報を盗んでネットワークへのアクセスを得られるようにします。 フィッシング キットのランディングページへのアクセスをブロックするだけでなく、多要素認証および認証情報フィッシング防止を有効化することで、あらゆる段階でフィッシング攻撃を防ぐことができます。
protocol-anomaly	アプリケーションおよび脅威	プロトコルの挙動が通常の適切な用途から外れる、プロトコルの異常を検出します。例えば、不正な形式のパケット、プログラムが不適切なアプリケーション、標準的でないポート上で実行されているアプリケーションはすべて、異常なプロトコルとみなされ、回避ツールとして使用される可能性があります。あらゆる

©2025 Palo Alto Networks, Inc.

脅威カテゴリ	これらのシグネチャを提供するコンテンツ更新	詳説
		重大度の異例のプロトコルをブロックすることがベストプラクティスになります。
SQLインジェクション	アプリケーションおよび脅威	攻撃者が SQL クエリをアプリケーションのリクエストに含め、データベースからデータを読み取る、あるいはデータを変更する、よくあるハッキング技術を検出します。このタイプのテクニックは、ユーザーの入力情報のサニタイズが不十分なウェブサイトに対してよく利用されます。

©2025 Palo Alto Networks, Inc.

ネットワークをレイヤー 4 およびレイヤー 7 回避から保護するためのベスト プラクティス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

以下に、ほとんどのレイヤー 4 攻撃およびレイヤー 7 攻撃をモニタリングし、ネットワークを保護するための推奨事項を示します。

- ❑ 最新の PAN-OS ソフトウェア バージョンおよびコンテンツ リリース バージョンにアップグレードして、最新のセキュリティ更新を使用してください。コンテンツとソフトウェア更新のインストールを参照してください。
- ❑ DNSセキュリティを有効にして(脅威防御サブスクリプションおよびDNS セキュリティ サブスクリプションのライセンスが必要)、悪意のあるDNS要求をシンクホールするPalo Alto Networks では、ご利用のアンチスパイウェア プロファイル内で、以下の DNS セキュリティ カテゴリ設定を使用するようお勧めします:

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
: Palo Alto Networks Content			
default-paloalto-dns		sinkhole	extended-capture
: DNS Security			
Command and Control Domains	default (high)	sinkhole	extended-capture
Dynamic DNS Hosted Domains	default (informational)	sinkhole	disable
Grayware Domains	default (low)	sinkhole	disable
Malware Domains	default (medium)	sinkhole	disable
Parked Domains	default (informational)	sinkhole	disable
Phishing Domains	default (low)	sinkhole	disable
Proxy Avoidance and Anonymizers	default (low)	sinkhole	disable
Newly Registered Domains	default (informational)	sinkhole	disable

  - ログの重大度設定の場合は、デフォルト設定を使用します。
  - ポリシーのアクションについては、すべてのシグネチャ送信元を **sinkhole (**シンクホール**)** に設定します。
  - packet capture (パケット キャプチャ - pcap) については、Command and Control Domains (コマンド アンド コントロール ドメイン) を **extended-capture (**拡張キャプチャ**)** に設定します。その他のすべてのカテゴリはデフォルト設定のままにします。

  関連するアンチスパイウェアの設定詳細については、インターネット ゲートウェイのアンチスパイウェア プロファイルのベストプラクティスを参照してください。
- ❑ 高度な脅威防御サブスクリプションが有効な場合は、インライン クラウド解析とローカル ディープ ラーニング(利用可能な場合)を有効にして、高度なC2およびスパイウェアの脅威を

©2025 Palo Alto Networks, Inc.

リアルタイムでブロックします。各分析エンジンの既定のアクションは **alert** で、対応する脅威が検出されると脅威ログを生成しますが、Palo Alto Networks では、すべての分析モデルアクションを **Reset-Both** に設定することをお勧めします。これにより、一致するパケットがドロップされ、RST がクライアントとサーバーに送信し、接続が切断され、脅威ログエントリが生成されます。

- ファイアウォールがDNSプロキシとして振る舞うように設定し、回避シグネチャを有効にします。

  DNS プロキシはファイアウォール セキュリティ ポリシー エンジンの一部ではありません。代わりに、ドメインから *IP* へのマッピングを管理しながら、 *DNS* ホスト名を解決するようファイアウォールに指示します。この指示は、*TLS/HTTP* 回避を防ぐのに不可欠です。

  - DNS プロキシ オブジェクトの設定を行います。

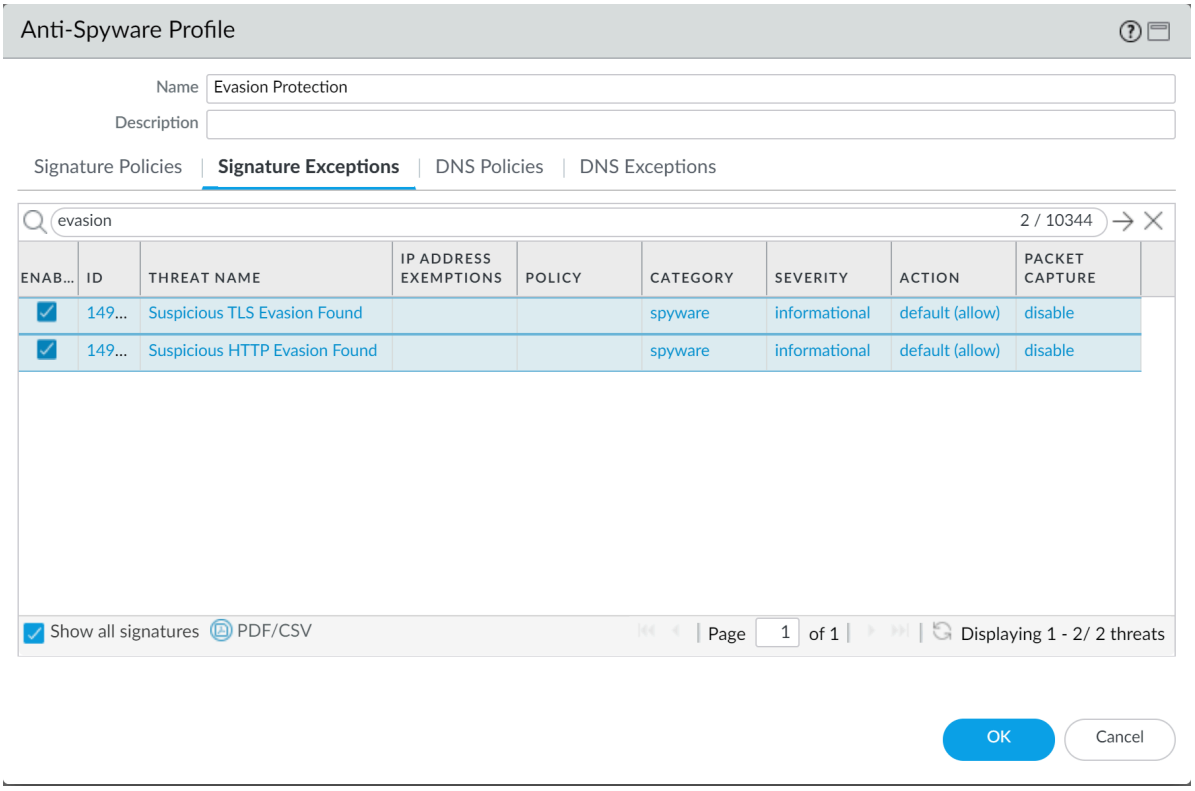
    DNS プロキシとして振る舞う際、ファイアウォールは DNS リクエストを解決し、今後の DNS クエリを効率よく迅速に解決するためにホスト名から IP アドレスへのマッピングをキャッシュします。

  - 回避シグネチャの有効化

    偽装された HTTP あるいは TLS リクエストを検知する回避シグネチャは、元の DNS リクエストで指定されているもの以外のドメインにクライアントが接続する際にアラートを送信できます。回避シグネチャを有効化する前に必ず DNS プロキシを設定するようにしてください。DNS プロキシがなくても、DNS 負荷分散構成における DNS サーバーが同じ DNS リクエストへの応答としてファイアウォールおよびクライアントに異なる IP アドレ

 ©2025 Palo Alto Networks, Inc.

ス（同じリソースをホストするサーバーについて）を返す際にアラートをトリガーできます。



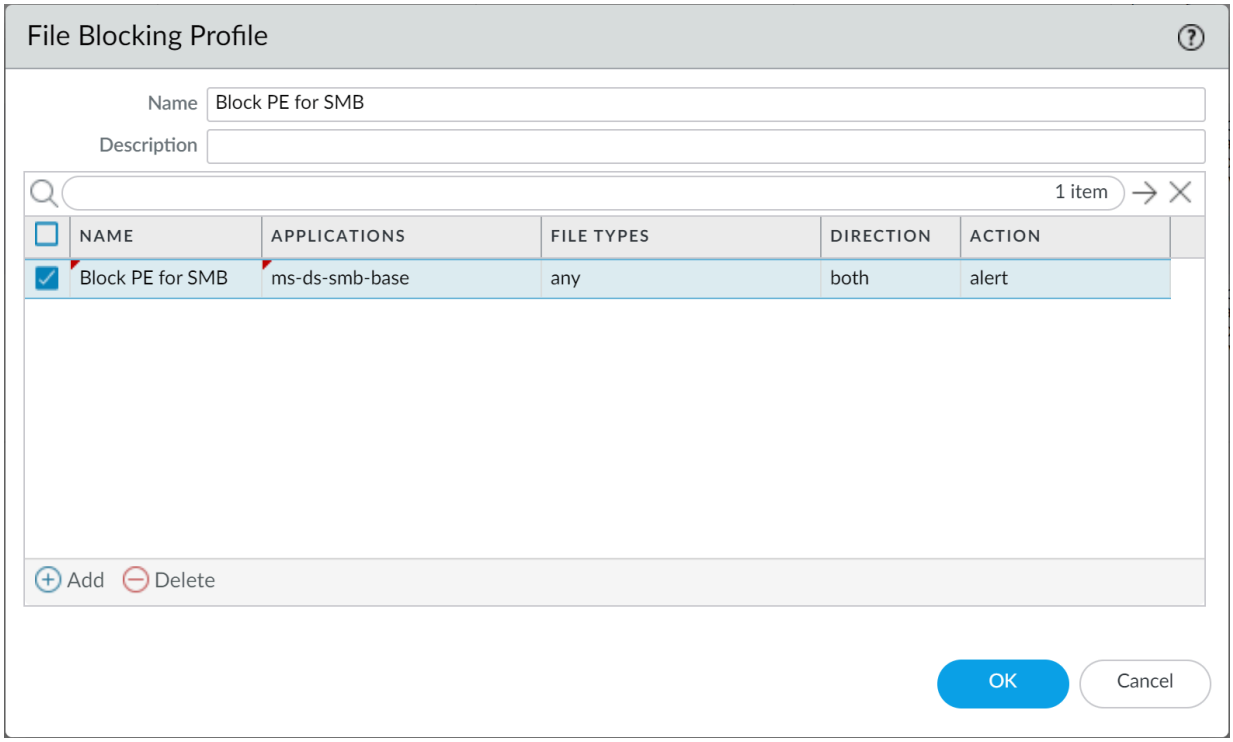
- Prisma Accessを運用している展開、または内部DNSサーバーのないネットワークの場合は、既定のシンクホールFQDN (sinkhole.paloaltonetworks.com)の代わりにPalo Alto NetworksシンクホールIPアドレス(72.5.65.111)を使用するようにDNSポリシーを構成します。

  Anti-Spyware Profile によって使用される DNS シンクホールを使用すると、firewall は、指定されたシンクホール サーバーに対してシンクホール アクション用に構成されたカテゴリに一致するドメインの DNS クエリに対する応答を偽造し、侵害されたホストの識別を支援します。デフォルトのシンクホール FQDN が使用される場合、firewall は、内部 DNS サーバーが CNAME レコードを解決することを期待して、CNAME レコードを応答としてクライアントに送信し、クライアントから構成済みのシンクホール・サーバーへの悪意のある通信をログに記録し、容易に識別できるようにします。ただし、クライアントがPrisma Accessを運用している場合、内部DNSサーバーのないネットワークにいる場合、またはCNAMEをAレコード応答に適切に解決できない他のソフトウェアやツールを使用している場合、DNS要求はドロップされ、脅威解析に不可欠な不完全なトラフィック ログの詳細が生成されます。
- サーバーについては、各サーバーで制限が加えられたアプリケーションのみを許可するセキュリティポリシー ルールを作成します。アプリケーションの標準的なポートがサーバーの

©2025 Palo Alto Networks, Inc.

リッスン ポートにマッチしていることを確認してください。例えば、SMTPトラフィックだけがメール サーバーへのアクセスを許可されるように、Application (アプリケーション) を **smtp** に設定し、Service (サービス) を **application-default** に設定します。サーバーが標準的なポートのサブネットだけを使用する場合（例えば、SMTP アプリケーションが 25 および 587 と定義された標準的なポートを持っていながら SMTP サーバーがポート 587 のみを使用する場合）、ポート 587 のみを含んだ新しいカスタム サービスを作成し、application-default の代わりにその新しいサービスをセキュリティ ポリシー ルールで使用してください。さらに、特定の送信元および宛先ゾーンや IP アドレス群にアクセスを制限するようにしてください。

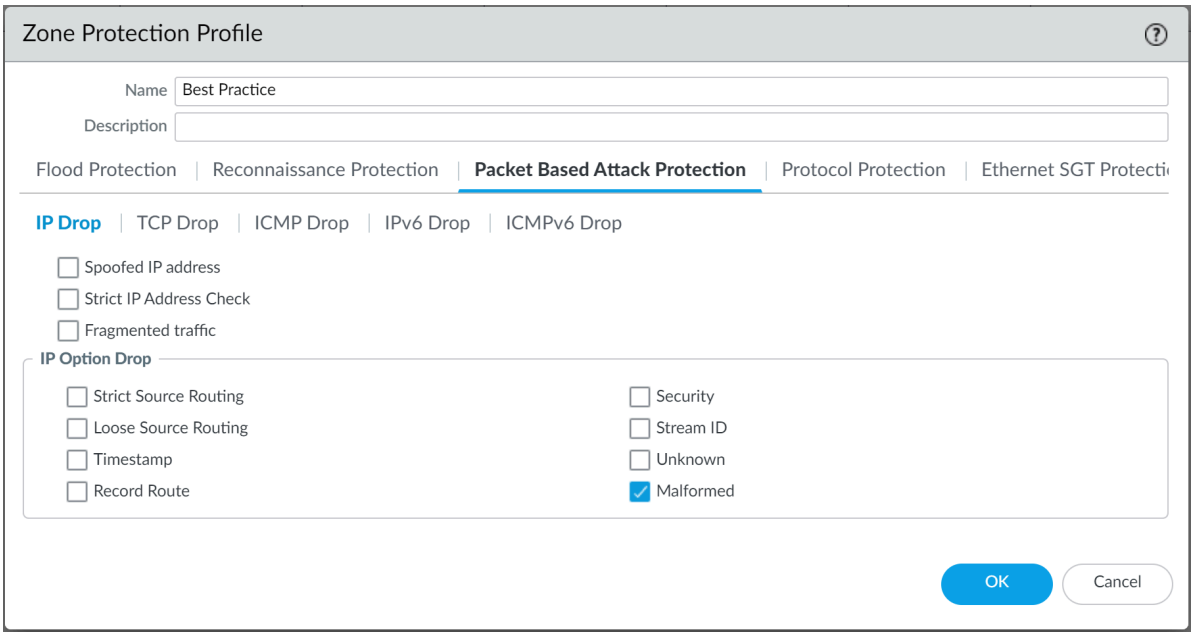
- セキュリティ ポリシーを使用してすべての不明なアプリケーションおよびトラフィックをブロックします。通常、不明なトラフィックに分類されるのは、ネットワーク上の内部アプリケーションまたはカスタム アプリケーションおよび潜在的な脅威です。不明なトラフィックは、変則的で異常な非準拠のアプリケーションまたはプロトコルであるか、または非標準ポートを使用する既知のアプリケーションの可能性があり、どちらの場合でもブロックする必要があります。「カスタム アプリケーションや不明なアプリケーションの管理」を参照してください。
- ファイル ブロッキングのセットアップを行い、インターネットベースの SMB （Server Message Block）トラフィックの Portable Executable （PE）ファイル タイプが Trust ゾーンから Untrust ゾーンに通過するのをブロックします（ms-ds-smb アプリケーション）。



- PE (Portable Executable)、ELFおよびMS Officeファイル、PowerShellおよびシェル スクリプトの悪意のある亜種をリアルタイムでブロックします。WildFire Inline MLを有効にすると、ファイアウォールで機械学習を使用してファイルを動的に解析できます。このアンチウィルス保護の追加レイヤーは、WildFire ベースのシグネチャを補完し、シグネチャがまだ存在しないファイルのカバー範囲を拡大します。

 ©2025 Palo Alto Networks, Inc.

- パケットベースの攻撃を防御するように設定されたゾーン プロテクション プロファイルを作成します（**Network** (ネットワーク) > **Network Profiles** (ネットワーク プロファイル) > **Zone Protection** (ゾーン プロテクション)）。
  - **Malformed** (不正な形式の) IPパケットをドロップするオプションを選択します（**Packet Based Attack Protection** (パケット ベースの攻撃防御) > **IP Drop** (IPドロップ)）。



  - **Mismatched overlapping TCP segment** (重複する **TCP** セグメントの不一致) をドロップするオプションを有効化します（**Packet Based Attack Protection** (パケット ベースの攻撃防御) > **TCP Drop** (TCP ドロップ)）。

    重複するけれども異なるデータを故意に使用して接続を構築することにより、攻撃者は接続の意図を誤解させ、誤検出を故意に発生させようとすることができます。また、攻撃者は IP スプーフィングとシーケンス番号予測を利用してユーザーの接続をインターセプトし、接続を介して攻撃者のデータを挿入します。**Mismatched overlapping TCP segment** (重複する **TCP** セグメントの不一致) オプションを選択すると、不一致かつ重複したデータを持つフレームを PAN-OS に破棄させることができます。受信したセグメントは、別のセグメントに含まれている場合、別のセグメントの一部とオーバーラップしている場合、あるいは別のセグメントの全体を含んでいる場合に破棄されます。
  - **TCP SYN with Data** (データを伴う **TCP SYN**) および **TCP SYNACK with Data** (データを伴う **TCP SYNACK**) をドロップするオプションを有効化します（**Packet Based Attack Protection** (パケット ベースの攻撃防御) > **TCP Drop** (TCP ドロップ)）。

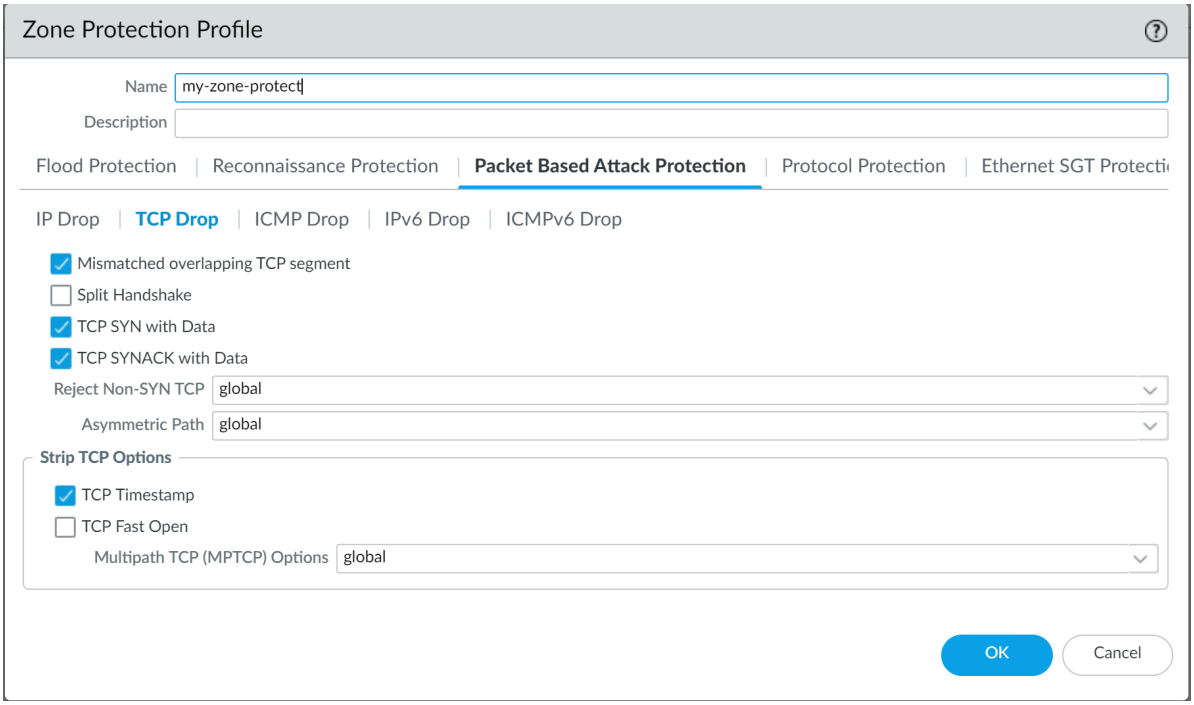
    3 方向ハンドシェイクの際にペイロードにデータを含む SYN および SYN-ACK パケットをドロップすることで、ペイロードに含まれるマルウェアをブロックし、TCP ハンドシェイ

©2025 Palo Alto Networks, Inc.

クが完了する前に不正なデータの抽出を回避できるようになり、セキュリティが向上します。

- ファイアウォールがパケットを転送する前に SYN パケットから TCP タイムスタンプを除去します（**Packet Based Attack Protection (**パケット ベースの攻撃防御**) > TCP Drop (TCP** ドロップ**)**）。

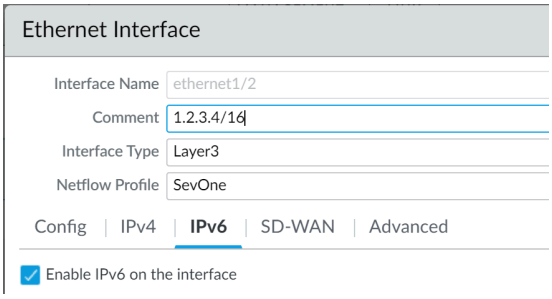
  SYN パケットの **Strip TCP Options - TCP Timestamp (TCP** ストリップのオプション**—TCP** タイムスタンプ**)** オプションを有効化すると、TCP 接続の両端の TCP スタックで TCP タイムスタンプがサポートされなくなります。これにより、同じシーケンス番号について複数のパケット上で異なるタイムスタンプを使用する攻撃を回避できます。



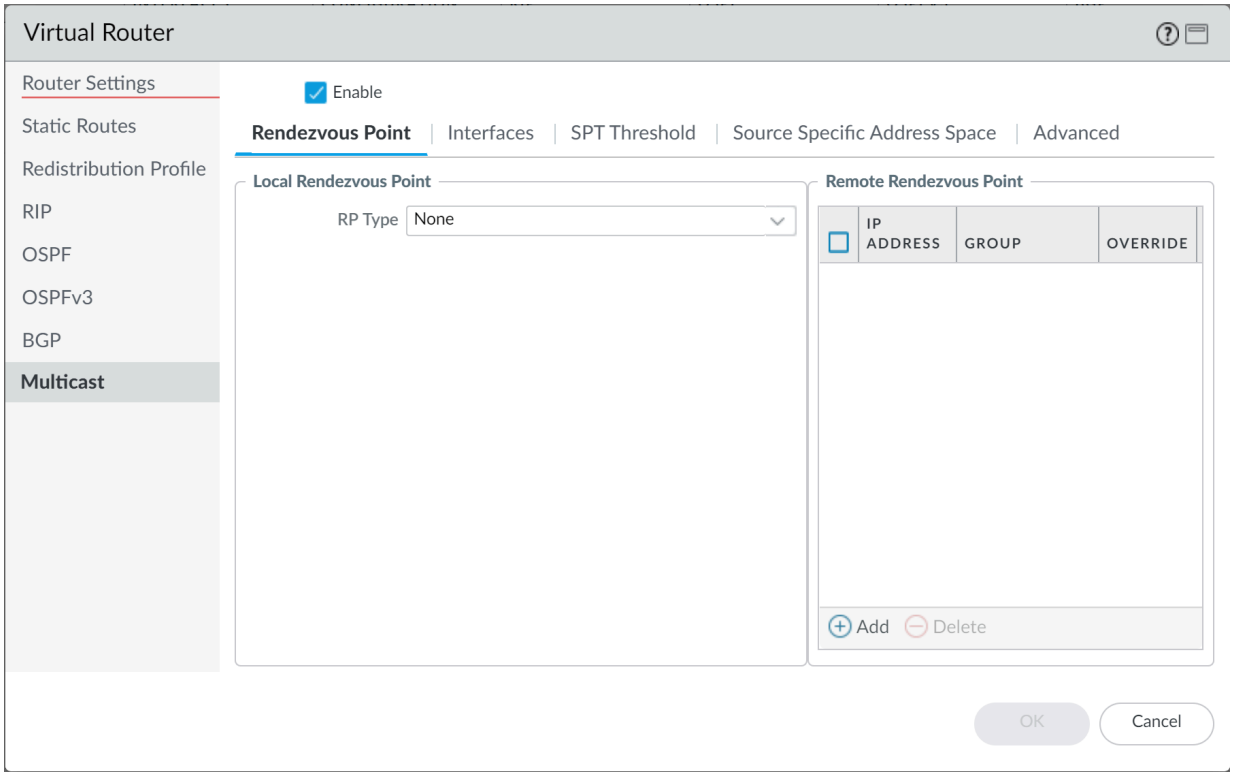
©2025 Palo Alto Networks, Inc.

- ネットワークホスト上で IPv6 アドレスを設定する場合、IPv6 のサポートをまだ有効にしていないのであれば、必ず有効にしてください（**Network (ネットワーク) > Interfaces (インターフェイス) > Ethernet (イーサネット) > IPv6**）。

  IPv6 のサポートを有効化することで、IPv6 ホストへのアクセスを許可し、さらに IPv4 パケットにカプセル化された IPv4 パケットをフィルタリングし、IPv6 over IPv4 のマルチキャスト アドレスがネットワークの偵察行為に悪用されるのを防ぐことができます。



- マルチキャスト トラフィックのサポートを有効にして、ファイアウォールがマルチキャスト トラフィックにポリシーを適用できるようにします（**Network (ネットワーク) > Virtual Router (仮想ルーター) > Multicast (マルチキャスト)**）。



©2025 Palo Alto Networks, Inc.

- **Forward datagrams exceeding UDP content inspection queue (UDP** コンテンツ検査キューを超過するデータグラムを転送) および **Forward segments exceeding TCP content inspection queue (TCP** コンテンツ検査キューを超過するセグメントを転送) を無効化します (**Device (**デバイス) > **Setup (**セットアップ) > **Content-ID** > **Content-ID Settings (Content-ID** 設定)。

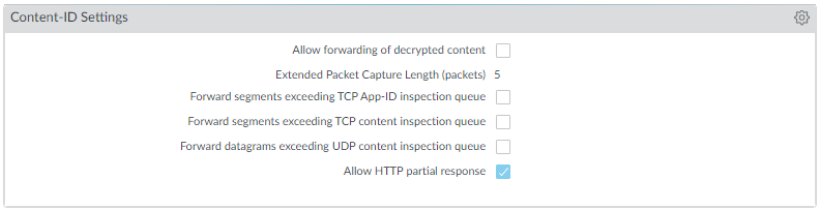
  デフォルト設定では、TCP または UDP コンテンツ検査キューが一杯になると、ファイアウォールはキュー制限 64 を超過した UDP データグラムあるいは TCP セグメントに対するコンテンツ検査をスキップします。このオプションを無効にすると、ファイアウォールが許可するすべての TCP および UDP データグラムに対して必ずコンテンツ検査が行われるようになります。例えば、ユースケースに合わせてファイアウォール プラットフォームが適切にサイジングされていないなどの特定の状況下でのみ、この設定を無効化するとパフォーマンスが影響を受ける場合があります。

- **Allow HTTP partial response (HTTP** 部分レスポンスの許可) を無効化します（**Device (**デバイス) > **Setup (**セットアップ) > **Content-ID** > **Content-ID Settings (Content-ID** 設定)）。

  HTTP 部分レスポンス オプションにより、クライアントはファイルの一部のみを取得することができるようになります。転送の途中経路にある次世代ファイアウォールが悪意のあるファイルの検知と破棄を行った場合、RSTパケットにてTCPセッションを強制終了します。ウェブ ブラウザが HTTP ヘッダー レンジ オプションを実装している場合、新しいセッションを開始してファイルの残りの部分だけを取得することで、最初のセッションのコンテクストが欠如しているためにファイアウォールが同一のシグネチャを再びトリガーするのを防ぐと同時に、ウェブ ブラウザがファイルを再構築して悪意のあるコンテンツを配信することができます。このオプションを無効にすると、これが発生しなくなります。

  HTTP部分応答の許可は、デフォルトでfirewallで有効になっています。これにより、最大限の可用性が提供されますが、サイバー攻撃が成功するリスクが高まります。最大限のセキュリティのために、このオプションを無効にして、悪意のあるアクティビティのためにファイアウォールが元のセッションを終了した後に、Webブラウザが新しいセッションを開始してファイルの残りの部分を取得するのを防ぎます。HTTP 部分応答を無効にすると、RANGE ヘッダーを使用する HTTP-based データ転送に影響し、特定のアプリケーションでサービス異常が発生する可能性があります。HTTP 部分応答を無効にした後、ビジネス クリティカルなアプリケーションの動作を検証します。

  ビジネスクリティカルなアプリケーションでHTTPデータ転送の中断が発生した場合は、その特定のアプリケーションに対してApplication Overrideポリシーを作成できます。Application Override は App-ID (脅威とコンテンツの検査を含む) をバイパスするため、特定のビジネスクリティカルなアプリケーションに対してのみ Application Override ポリシーを作成し、ソースと宛先を指定してルールを制限します (最小特権アクセスの原則)。必要な場合を除き、Application Override ポリシーを作成しないでください。Application Override ポリシーの詳細については、「https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVLCA0 を参照してください。



 ©2025 Palo Alto Networks, Inc.

- プロトコルの異常と、重大度が「低」および「高」のすべての脆弱性をブロックする脆弱性防御プロファイルを作成します。

  プロトコルの挙動が通常の適切な用途から外れたとき、プロトコルの異常が発生します。例えば、不正な形式のパケット、プログラムが不適切なアプリケーション、標準的でないポート上で実行されているアプリケーションはすべて、異常なプロトコルとみなされ、回避ツールとして使用される可能性があります。

  ビジネスにおいてアプリケーションの可用性を最優先するミッション クリティカルなネットワークの場合、一定期間、特異なプロトコルに対するアラートを通知することから始め、重要な内部アプリケーションが標準的でない方法で確立されたプロトコルを決して使用しないようにします。特定の重要なアプリケーションが特異なプロトコルのシグネチャをトリガーすることが判明した場合、それらのアプリケーションを異例のプロトコルの適用から除外することができます。これを行うには、特異なプロトコルを許可する別のルールを脆弱性防御プロファイルに追加し、そのプロファイルを、重要なアプリケーションを出入りするトラフィックを実行するセキュリティ ポリシー ルールに付与します。

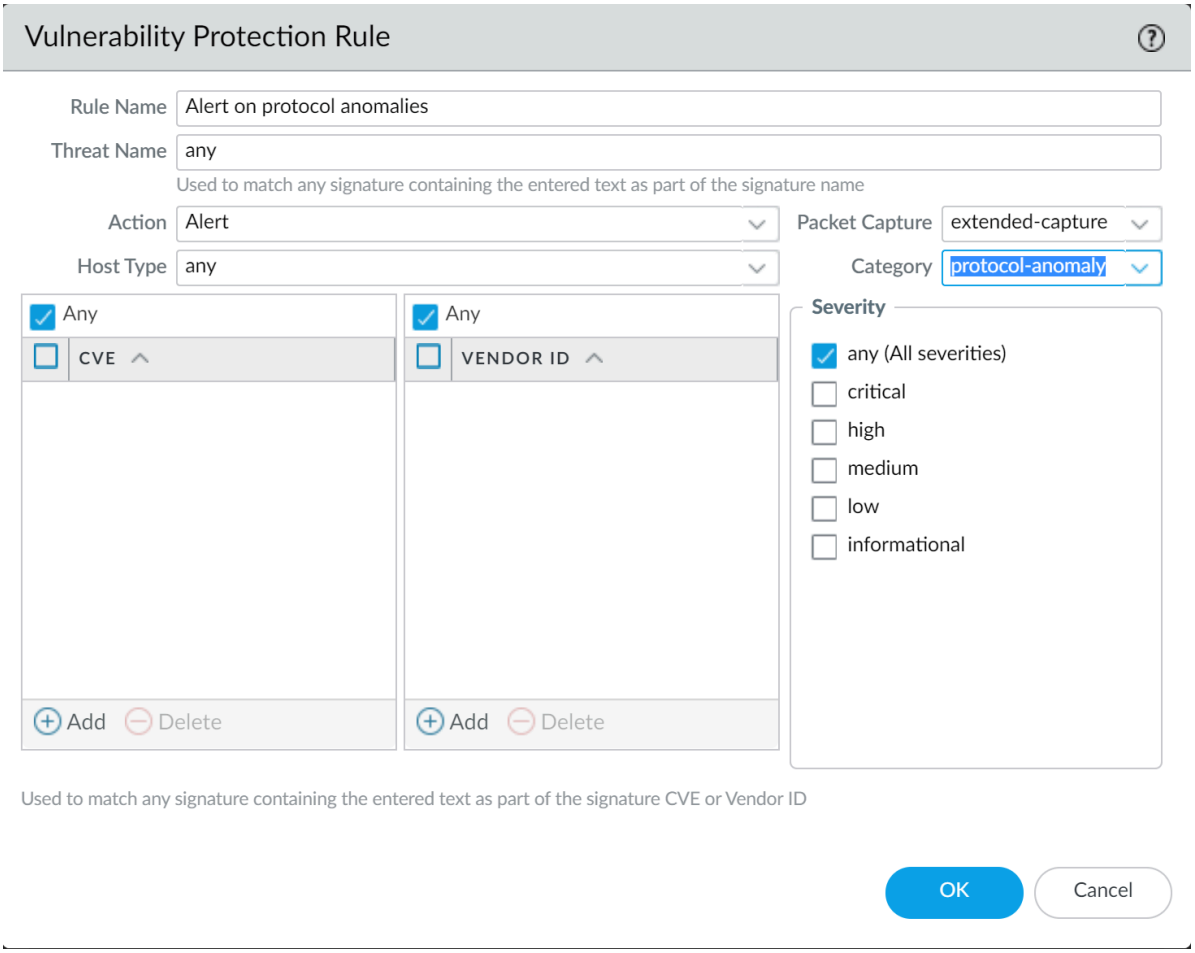
  重要な内部アプリケーションについて特異なプロトコルを許可する、脆弱性防御プロファイル ルール、およびセキュリティ ポリシー ルールが、上記、特異なプロトコルをブロックするルールにリストされていることを確認します。トラフィックはセキュリティポリシールールおよび関連する脆弱性保護プロファイル ルールに対して上から順に評価され、最初にマッチしたルールが適用されます。

  - 異例のプロトコルについてアラートを通知することから始めます。

    Vulnerability Protection Profile (脆弱性保護プロファイル) ルールを作成し、**Action (**アクション**)** を Alert (アラート)に、**Category (**カテゴリ**)** を protocol-anomaly に、**Severity (**重大度**)** を Any (すべて) に設定します。トラフィックを監視し、標準的でない方法で確立されたプロトコルを使用している重要な内部アプリケーションがあるかどうか判断します。そうであることが分かった場合、該当するアプリケーションで特異なプロトコルの許可を

©2025 Palo Alto Networks, Inc.

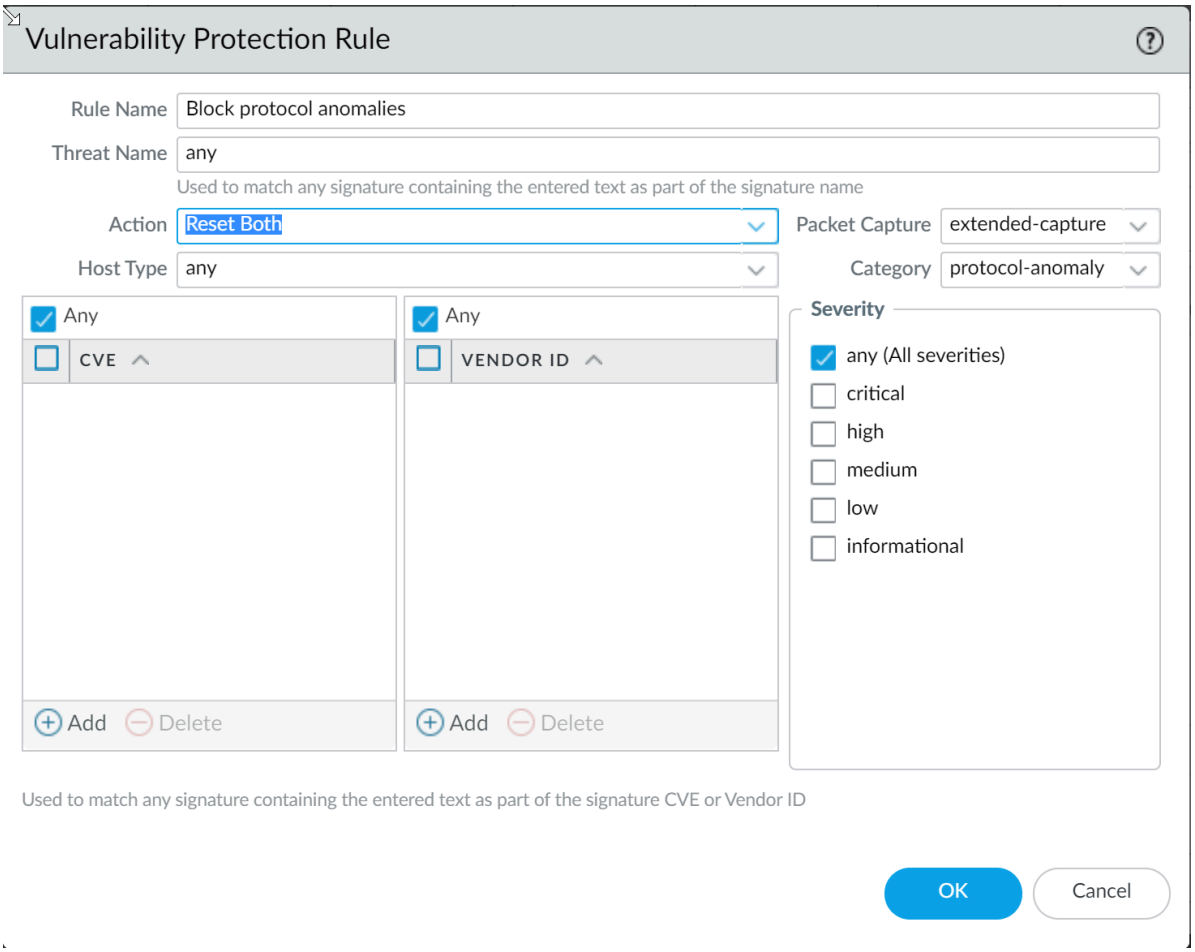
continue (続行) してから、その他すべてのアプリケーションについて、特異なプロトコルをブロックします。



©2025 Palo Alto Networks, Inc.

- 特異なプロトコルをブロックします。

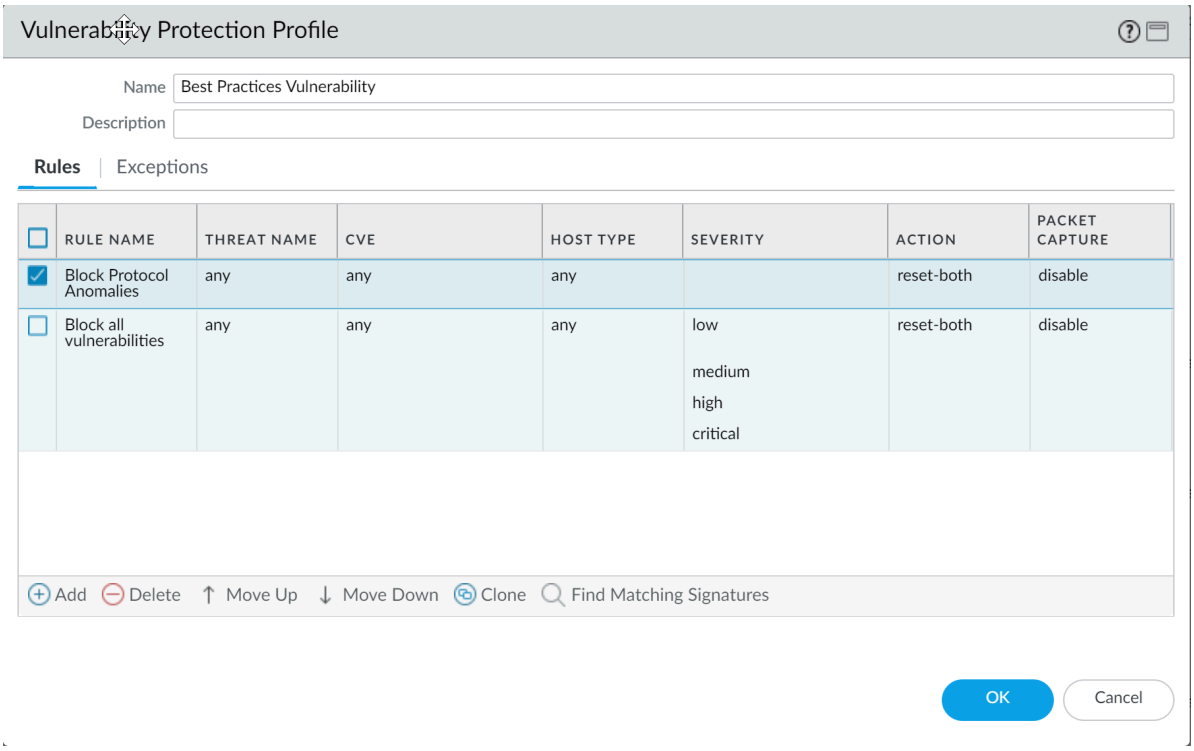
  Vulnerability Protection Profile (脆弱性保護プロファイル) ルールを作成し、**Category (**カテゴリ**)** を protocol-anomaly に、**Action (**アクション**)** を Reset Both (どちらもリセット) に、**Severity (**重大度**)** を Any (すべて) に設定します。



- 必要に応じて、非標準的な方法で確立されたプロトコルを使用する重要なアプリケーションについて、特異なプロトコルを許可します。そうするには、特異なプロトコルを許可する Vulnerability Protection Profile (脆弱性保護プロファイル) ルールを作成します（**Action (**アクション**)** を Allow (許可) に、**Category (**カテゴリ**)** を protocol-anomaly に、**Severity (**重大度**)** を any (すべて) に設定）。重要なアプリケーションを出入りするトラフィックに適用されるセキュリティポリシー ルールに脆弱性保護プロファイル ルールを付与します。

©2025 Palo Alto Networks, Inc.

- 重大度が「low」以上の脆弱性をすべてブロックする脆弱性防御プロファイルに別のルールを追加します。このルールは、特異なプロトコルをブロックするルールの後にリストアップする必要があります。



- 作業を続行し、以下のセキュリティ プロファイルをセキュリティ ポリシールールに関連付けて、シグネチャベースの防御を提供します：
  - 重大度が「low」以上のスパイウェアをすべてブロックするアンチスパイウェア プロファイル。
  - アンチウイルス シグネチャに一致するコンテンツをすべてブロックするアンチウイルス プロファイル。

©2025 Palo Alto Networks, Inc.

脅威インテリジェンスを Palo Alto Networks と共有

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

テレメトリーは、分析用のデータの収集と送信を行うプロセスです。ファイアウォールでテレメトリーを有効にすると、ファイアウォールは、アプリケーション、脅威、デバイスの安全状態に関する情報を含むデータを定期的に収集し、Palo Alto Networks に送信します。脅威インテリジェンスを共有することには、次のようなメリットがあります。

- ご自身や世界中のお客様に、強化された脆弱性およびスパイウェア シグネチャを提供。例えば、脅威イベントが脆弱性あるいはスパイウェア シグネチャをトリガーする際、ファイアウォールがその脅威に関連する URL を Palo Alto Networks 脅威リサーチ チームと共有し、その URL を悪意があるものとして適切に分類できるようになります。
- ネットワークに一切影響を与えることなく試験的な脅威シグネチャを素早くテスト・評価することで、すべての Palo Alto Networks のお客様に不可欠な脅威防止を素早く提供可能。
- PAN-DB URL フィルタリング、DNS ベースのコマンドアンドコントロール （C2）シグネチャ、および WildFire 内の精度とマルウェア検出機能が向上。

Palo Alto Networks は、テレメトリーから抽出された脅威インテリジェンスを使用して、これらのメリットをご自身や他の Palo Alto Networks のお客様に提供します。各ユーザーが共有するテレメトリーデータにより、すべての Palo Alto Networks ユーザーがメリットを得ます。テレメトリーはコミュニティ駆動の、脅威を阻止するためのアプローチです。Palo Alto Networks はユーザーのデータを他のお客様またはサードパーティ組織と共有しません。

テレメトリの利点、使用法、構成など、テレメトリの詳細については、「デバイス テレメトリ」を参照してください。

©2025 Palo Alto Networks, Inc.

Advanced Threat Preventionのリソース

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

脅威防御のベストプラクティスに関する詳細は、以下の資料を参照してください：

- Creating Custom Threat Signatures（英語）
- ネットワークをレイヤー 4 およびレイヤー 7 回避から保護するためのベスト プラクティス
- URL フィルタリングのベストプラクティス
- ゼロトラストのベストプラクティス
- DoS およびゾーン プロテクションのベストプラクティス

Palo Alto Networks 製品で識別可能な脅威およびアプリケーションのリストを参照するには、以下のリンクを使用してください。

- Applipedia — Palo Alto Networks で識別できるアプリケーションについて詳細に説明しています。
- Threat Vault — Palo Alto Networks 製品で識別可能な脅威の一覧が掲載されています。脆弱性、スパイウェア、またはウイルスを条件にして検索できます。脅威についての詳細は、ID 番号の横にある詳細アイコンをクリックしてください。

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

脅威防御の設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

インライン クラウド解析を有効にして構成する前に、運用元のプラットフォーム ライセンスに加えて、Threat PreventionまたはAdvanced Threat Preventionを取得してインストールする必要があります(クラウドベースのインライン クラウド解析機能にアクセスするため)。ライセンスはPalo Alto Networksカスタマー サポート ポータルかアクティベートされ、脅威防御機能を有効にする前にアクティブ化されている必要があります。さらに、(他のPalo Alto Networksセキュリティ サービスと同様に) Threat Preventionはセキュリティ プロファイルを通じて管理されますが、セキュリティ プロファイルはセキュリティ ポリシー ルールを通じて定義されたネットワーク適用ポリシーの構成に依存します。Threat Preventionを有効にする前に、セキュリティ サブスクリプションが有効になっているセキュリティ プラットフォームのコア コンポーネントを理解しておくことをお勧めします。詳細については、製品のドキュメントを参照してください。

脅威防御サブスクリプションを有効にして、ネットワーク セキュリティのデプロイメント内で最適に機能するように構成するには、以下のタスクを参照してください。ここに示すすべてのプロセスを実装する必要はありませんが、デプロイメントを成功させるために、すべてのタスクを見直して利用可能なオプションに慣れることをお勧めします。最適な操作性とセキュリティを実現するためには、Palo Alto Networksが提供するベストプラクティスに従うことがさらに推奨されます。

アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

すべての Palo Alto Networks の次世代ファイアウォールには、セキュリティ ポリシーに適用できる事前定義されたアンチウイルス、アンチスパイウェア、および脆弱性防御プロファイルが付属します。事前定義されたアンチウイルス プロファイルは 1 つで、**default** と呼ばれ、プロトコルごとにデフォルトのアクション（HTTP、FTP、および SMB トラフィックのブロック、および SMTP、IMAP、POP3 トラフィックでアラート生成）を使用します。アンチスパイウェアおよび脆弱性保護用の事前定義されたプロファイルは以下の 2 つです。

- **default** – デフォルトのアクションがクライアントおよびサーバーのすべてのスパイウェア/脆弱性防御イベント（重大度 critical、high、および medium）に適用されます。low および informational イベントは検出しません。
- **strict** – ブロック応答がクライアントおよびサーバーのすべてのスパイウェア/脆弱性防御イベント（重大度 critical、high、medium）に適用され、low および informational イベントではデフォルトのアクションを使用します。

ネットワークに流れ込むトラフィックに脅威が含まれることのないようにするため、事前定義されたプロファイルを基本 Web アクセス ポリシーに関連付けます。ネットワーク上のトラフィックをモニターしてポリシー ルールベースを拡張し、その後、特定のセキュリティ ニーズに対応する詳細なプロファイルを設計できます。

次の流れに従ってデフォルトのアンチウイルス、アンチスパイウェア、および脆弱性保護セキュリティ プロファイルをセットアップします。

- Strata Cloud Manager
- PAN-OS & Panorama

アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップ(Cloud Management)

©2025 Palo Alto Networks, Inc.

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerにログインします。

脅威防御サブスクリプションでは、1つのライセンスに、アンチウイルス、アンチスパイウェア、および脆弱性防御の機能をバンドルしたもので、Prisma Accessサブスクリプションの一部です。Prisma Accessで提供されるアプリケーションとサービスに関する詳細については、「利用可能なすべてのアプリケーションとサービス」を参照してください。現在アクティブなライセンスがあるサブスクリプションを確認するには、ライセンスでサポートされている内容を確認してください。

STEP 2 | （任意）アンチウイルス、アンチスパイウェア、および脆弱性保護用のカスタム セキュリティ プロファイルを作成します。

または、事前定義済みのベストプラクティス プロファイルを使用することもできます。

安全に ベストプラクティスとしてのセキュリティプロファイル へ移行し、最高のセキュリティ体制を整えます。

- カスタムのWildFireおよびアンチウイルス プロファイルを作成するには、**[Manage (管理)] > [Configuration (設定)] > [NGFW and Prisma Access (NGFWとPrisma Access)] > [Security Services (セキュリティ サービス)] > [WildFire and Antivirus (WildFireとアンチウイルス)]**を選択して、**[Add Profile (プロファイルを追加)]**を選択します。安全に目標を達成するために、アンチウイルス プロファイル移行ステップを利用してください。
- カスタムのアンチスパイウェア プロファイルを作成するには、**[Manage (管理)] > [Configuration (設定)] > [NGFW and Prisma Access (NGFWとPrisma Access)] > [Security Services (セキュリティ サービス)] > [Anti-Spyware (アンチスパイウェア)]**を選択して、**[Add Profile (プロファイルを追加)]**を選択します。安全に目標を達成するために、アンチスパイウェア プロファイル移行ステップ を利用してください。
- カスタムの脆弱性防御プロファイルを作成するには、**[Manage (管理)] > [Configuration (設定)] > [NGFW and Prisma Access (NGFWとPrisma Access)] > [Security Services (セキュリティ サービス)] > [Vulnerability Protection (脆弱性防御)]**を選択して、**[Add Profile (プロファイルを追加)]**を選択します。安全に目標を達成するために、脆弱性プロテクション プロファイル移行ステップ を利用してください。

STEP 3 | セキュリティ プロファイルをセキュリティ ポリシー ルールにアタッチします。Prisma Accessは、デフォルトでベストプラクティスのセキュリティ ポリシー ルールを適用します。

脆弱性防御プロファイルを使用して、エクスプロイトまたは不正アクセスの取得の試みが検出されたときに接続をブロックするセキュリティ ポリシー ルールを設定すると、*Prisma Access*はそのトラフィックを自動的にブロックし、それらのインシデントをログに記録します(「ブロックされたIPアドレスの監視」を参照)。

1. **[Manage (管理)] > [Configuration (設定)] > [NGFW and Prisma Access (NGFWとPrisma Access)] > [Security Services (セキュリティ サービス)] > [Security Policy(セキュリティ**

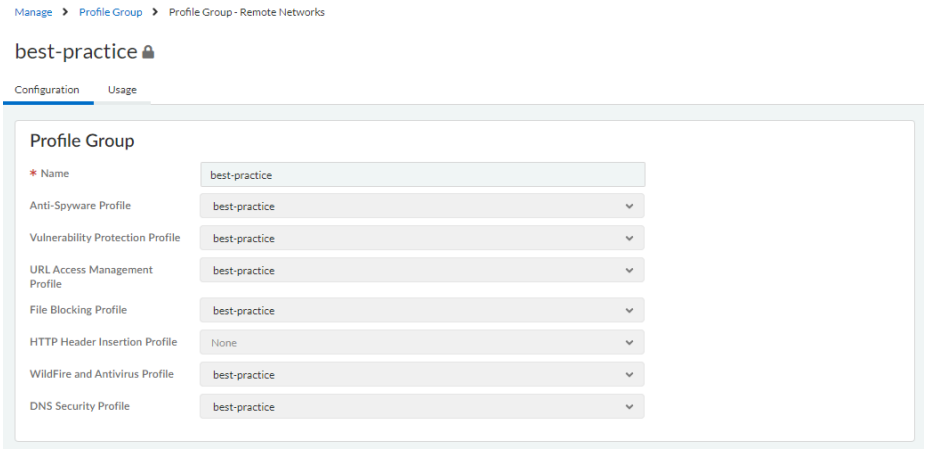
©2025 Palo Alto Networks, Inc.

ポリシー)]を選択し、変更するルールを選択するか[Add Rule (ツールの追加)]を選択します。

2. [Action and Advanced Inspection (アクションと詳細検査)]で、[Profile Group (プロファイル グループ)]を選択します。このグループには、次のセキュリティ プロファイルが含まれます。WildFireとアンチウイルス、アンチスパイウェア、および脆弱性防御。

   新しいプロファイル グループを作成するには、*[Manage (管理)]* > *[Configuration (設定)]* > *[NGFW and Prisma Access (NGFWとPrisma Access)]* > *[Security Services (セキュリティ サービス)]* > *[Profile Groups (プロファイル グループ)]*を選択します。詳細は、「セキュリティ プロファイルの有効化」を参照してください。

   デフォルトでは、ベストプラクティスのプロファイル グループが使用可能なすべてのセキュリティ プロファイルのベストプラクティス構成で有効になります。



STEP 4 | 変更をコミットします。

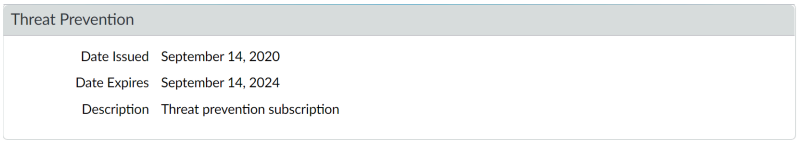
アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップ(NGFW (Managed by PAN-OS or Panorama))

Palo Alto Networks は、すべてのアンチスパイウェアおよび脆弱性保護シグネチャに対するデフォルトのアクションを定義しています。デフォルトのアクションを表示するには、***Objects** (オブジェクト)* > ***Security Profiles** (セキュリティ プロファイル)* > ***Anti-Spyware** (アンチスパイウェア)* あるいは ***Objects** (オブジェクト)* > ***Security Profiles** (セキュリティ プロファイル)* > ***Vulnerability Protection** (脆弱性保護)* を選択してから、プロファイルを選択します。*Exceptions (例外)* タブをクリックし、*Show all signatures (すべてのシグネチャを表示)* をクリックしてシグネチャのリストおよび対応するデフォルトの ***Action** (アクション)* を表示します。デフォルト アクションを変更するには、新しいプロファイルを作成し、***Action** (アクション)* を指定し、かつ/または個々のシグネチャ例外をプロファイルの ***Exceptions** (例外)* に追加します。

©2025 Palo Alto Networks, Inc.

STEP 1 | 脅威防止サブスクリプションがあることを確認します。

脅威防止サブスクリプションでは、1 つのライセンスに、アンチウイルス、アンチスパイウェア、および脆弱性防御の全機能をバンドルしています。アクティブな脅威防止サブスクリプションを持っていることを確認するには、**Device (デバイス) > Licenses (ライセンス)** を選択し、**Threat Prevention (脅威防止)** の有効期限が未来の日付になっていることをチェックします。



STEP 2 | 最新のコンテンツをダウンロードします。

1. **Device (デバイス) > Dynamic Updates (動的更新)** の順に選択し、ページの下部にある **Check Now (今すぐチェック)** をクリックして最新のシグネチャを取得します。
2. **Actions** （アクション） 列で **Download (ダウンロード)** をクリックして最新のアンチウイルス アップデートをインストールしてから、最新のアプリケーションおよび脅威更新を **Install (インストール)** します。

STEP 3 | コンテンツ更新のスケジュールを設定します。

更新プログラムの展開に関する重要な情報については、アプリケーションと脅威コンテンツ更新のベストプラクティスを参照してください。

1. **Device (デバイス) > Dynamic Updates (動的更新)** を選択して **Schedule (スケジュール)** をクリックし、**Antivirus (アンチウイルス)** および **Applications and Threats (アプリケーションおよび脅威)** のシグネチャ更新を自動的に取得します。
2. 更新の頻度およびタイミングを指定します。
   - **download-only**–ファイアウォールは、定義したスケジュールに従って最新の更新を自動的にダウンロードしますが、**Install (インストール)** は手動で行う必要があります。
   - **download-and-install**–ファイアウォールは、定義したスケジュールに従って更新コンテンツを自動的にダウンロードしてインストールします。
3. **OK** をクリックしてスケジュール更新を保存します。コミットは不要です。
4. （任意）更新コンテンツを利用できるようになってからファイアウォールがダウンロードを行うまでの最低時間を示す **Threshold (しきい値)** を定義します。例えば、**Threshold (しきい値)** を **10** に設定すると、スケジュールに関係なく、更新コンテンツを利用できるようになってから少なくとも 10 時間経過するまでの間、ファイアウォールが更新コンテンツをダウンロードしなくなります。
5. （HA のみ）ダウンロードおよびインストール後にピアがコンテンツ更新を同期できるようにする稼働かを、**Sync To Peer (ピアと同期)** で決定します（更新スケジュールはピ

 ©2025 Palo Alto Networks, Inc.

ア間で同期されません。両方のピアに対して手動でスケジュールを設定する必要があります）。

次のように、**Sync To Peer (**ピアと同期**)** を行うかどうか、またその方法を判断するために HA デプロイメント環境に応じて考慮すべき事項が他にもあります。

- アクティブ/パッシブ**HA**–ファイアウォールがコンテンツ更新のために MGT ポートを使用している場合、両方のファイアウォールが独立して更新コンテンツをダウンロードおよびインストールするようスケジュールを設定します。しかし、ファイアウォールがコンテンツ更新用にデータポートを使用している場合は、パッシブ ファイアウォールがアクティブになるまでの間、ファイアウォールは更新コンテンツのダウンロードもインストールも行いません。更新のためにデータポートを使用する際、両方のファイアウォールがスケジュールを同期した状態を保つためには、両方のファイアウォールで更新のスケジュール設定を行った後、**Sync To Peer (**ピアと同期**)** を有効化し、どちらかアクティブな方のファイアウォールが更新コンテンツをダウンロードおよびインストールしたら、それをパッシブ ファイアウォールにもプッシュさせるようにします。
- アクティブ/アクティブ**HA**–ファイアウォールがコンテンツ更新用に MGT インターフェイスを使用している場合は、両方のファイアウォールで **download-and-install** を選択しますが、**Sync To Peer (**ピアと同期**)** は有効化しません。ただし、ファイアウォールがデータポートを使用している場合は、両方のファイアウォールで **download-and-install** を選択し、**Sync To Peer (**ピアと同期**)** を有効化して、いずれかのファイアウォールがアクティブ-セカンダリ状態になった場合に、アクティブ-プライマリ ファイアウォールが更新コンテンツをダウンロードおよびインストールして、それをアクティブ-セカンダリ ファイアウォールにプッシュさせるようにします。

STEP 4 | （任意）アンチウイルス、アンチスパイウェア、および脆弱性保護用のカスタム セキュリティ プロファイルを作成します。

あるいは、事前定義済みのデフォルトあるいは厳格なプロファイルを使用することもできます。

安全に ベストプラクティスとしてのセキュリティプロファイル へ移行し、最高のセキュリティ体制を整えます。

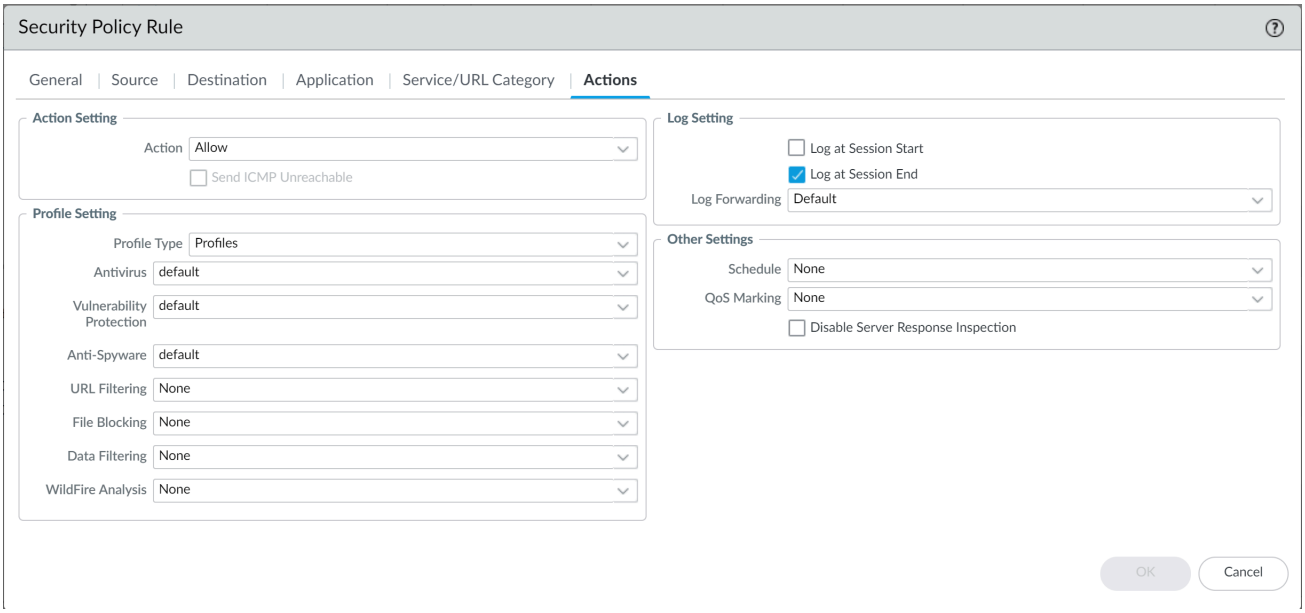
- カスタムのアンチウイルス プロファイルを作成するには、**[Objects (**オブジェクト**)]** > **[Security Profiles (**セキュリティ プロファイル**)]** > **[Antivirus (**アンチウイルス**)]**を選択して、新しいプロファイルを**[Add (**追加**)]**します。安全に目標を達成するために、アンチウイルス プロファイル移行ステップを利用してください。
- カスタムのアンチスパイウェア プロファイルを作成するには、**[Objects (**オブジェクト**)]** > **[Security Profiles (**セキュリティ プロファイル**)]** > **[Anti-Spyware (**アンチスパイウェア**)]**を選択して、新しいプロファイルを**[Add (**追加**)]**します。安全に目標を達成するために、アンチスパイウェア プロファイル移行ステップ を利用してください。
- カスタムの脆弱性防御プロファイルを作成するには、**[Objects (**オブジェクト**)]** > **[Security Profiles (**セキュリティ プロファイル**)]** > **[Vulnerability Protection (**脆弱性防御**)]**を選択して、新しいプロファイルを**[Add (**追加**)]**します。安全に目標を達成するために、脆弱性プロテクション プロファイル移行ステップ を利用してください。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | セキュリティ プロファイルをセキュリティポリシールールにアタッチします。

脆弱性保護プロファイルを使用して接続をブロックするセキュリティポリシールールを持つファイアウォールを設定すると、ファイアウォールは自動的にそのハードウェア内のトラフィックをブロックします（ブロックされた IP アドレスの監視を参照）。

1. **Policies (ポリシー) > Security (セキュリティ)** を選択し、さらに変更したいルールを選択します。
2. **Actions** （アクション） タブで **Profiles (プロファイル)** を **Profile Type (プロファイルタイプ)** として選択します。
3. **Antivirus (アンチウイルス)**、**Anti-Spyware (アンチスパイウェア)**、および **Vulnerability Protection (脆弱性保護)** 用に作成したセキュリティ プロファイルを選択します。



STEP 6 | 変更をコミットします。

Commit（コミット）をクリックします。

©2025 Palo Alto Networks, Inc.

インラインクラウド解析の設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 高度な脅威防御機能(拡張機能のサポート用)

インライン クラウド解析は、Advanced Threat Preventionクラウド サービスにクエリを実行することで、高度で回避性の高いゼロデイ コマンドアンドコントロール(C2)の脅威やコマンド インジェクション、SQLインジェクションの脆弱性をリアルタイムで検出できるAdvanced Threat Preventionの機能です。インライン クラウド解析による保護は、アンチスパイウェアと脆弱性防御のセキュリティ プロファイルを通じて提供され、前者は高度なC2 (コマンドアンドコントロール)とスパイウェアの脅威、後者はコマンド インジェクションとSQLインジェクションの脆弱性に対処します。

PAN-OS 11.2以降の展開を運用しているサポートされているファイアウォールは、Advanced Threat Preventionのローカル ディープ ラーニングにアクセスすることもできます。ローカル ディープ ラーニングは、ゼロデイ脅威やその他の回避脅威をローカル ディープ ラーニングベースで高速に解析するメカニズムを提供することで、Advanced Threat Preventionのクラウドベースのインライン クラウド解析コンポーネントを補完します。ローカル ディープ ラーニング モデルの更新は、コンテンツ更新を通じて提供されます。ローカル ディープ ラーニング検出モジュールの実行には追加のシステム リソースが必要なため、ローカル ディープ ラーニングは、次のプラットフォームでのみ利用できます。

- PA-5400シリーズ(PA-5450アプライアンスを除く)。
- VMシリーズ(合計メモリ16GB以上を割り当てる必要あり)
- VMシリーズ パブリック クラウド
- VMシリーズ プライベート クラウド

インライン クラウド解析、およびローカル ディープ ラーニングを有効化および設定するには、Advanced Threat Preventionライセンスを有効化し、アンチスパイウェアと脆弱性防御のセキュリティ プロファイルを作成(または変更)する必要があります。次に、各カテゴリ解析エンジンのポリシー設定を構成し、プロファイルをセキュリティ ポリシー ルールに関連付けます。

セキュリティ ポリシー ルールの作成の詳細については、『PAN-OS®管理者ガイド』の「ポリシー」の章を参照してください。

- Strata Cloud Manager
- PAN-OS & Panorama

©2025 Palo Alto Networks, Inc.

インライン クラウド解析の設定(PAN-OS & Panorama)

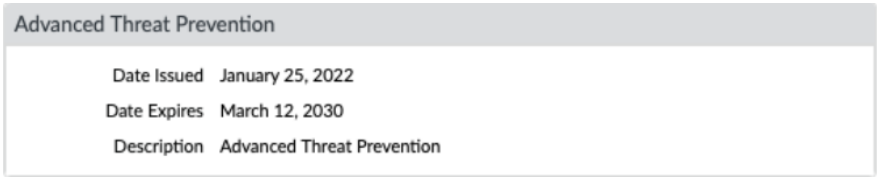
*Advanced Threat Prevention*のインライン クラウド解析は、複数の検出エンジンをサポートしています。これらのエンジンでは、次の機能を実現するために、さまざまな最小*PAN-OS*リリースが必要です。

- 高度な*C2* (コマンドアンドコントロール)およびスパイウェアの脅威の検出には、*PAN-OS 10.2*以降が必要です。
- ゼロデイ エクスプロイト脅威の検出には、*PAN-OS 11.0*以降が必要です。
- *LDL* (ローカル ディープ ラーニング)のサポートには、*PAN-OS 11.2*以降が必要です。

STEP 1 | PAN-OS Web インターフェイスにログインします。

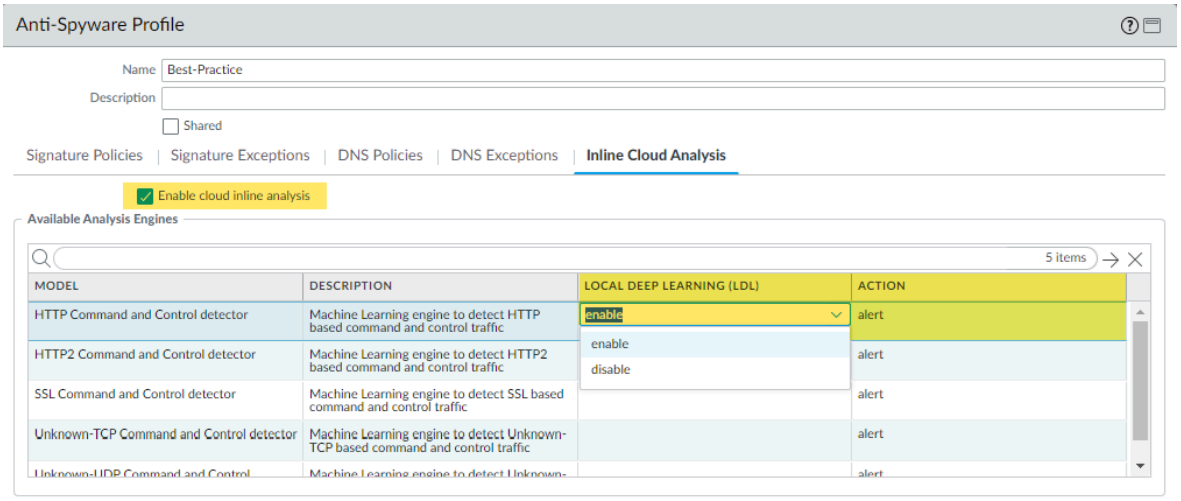
STEP 2 | インラインクラウド分析を利用するには、Advanced Threat Preventionのサブスクリプションが有効である必要があります。

現在アクティブなライセンスがあるサブスクリプションを確認するには、**Device > Licenses**を選択し、適切なライセンスが使用可能で有効期限が切れていないことを確認します。



©2025 Palo Alto Networks, Inc.

STEP 3 | インライン クラウド解析(高度なC2 (コマンドアンドコントロール)とスパイウェアの脅威についてトラフィックをリアルタイムで解析)を有効にするために、アンチスパイウェア セキュリティ プロファイルを更新または新規作成します。



1. 既存の **Anti-Spyware Profile** または **Add** を新しいもの (**Objects** > **Security Profiles** > **Anti-Spyware**) を選択します。
2. アンチスパイウェア プロファイルを選択し、**[Inline Cloud Analysis (**インライン クラウド解析**)]**および**[Enable inline cloud analysis (**インライン クラウド解析を有効にする**)]**に進みます。
3. (ローカル ディープ ラーニング[PAN-OS 11.2以降でサポート]) **[Local Deep Learning (LDL) (**ローカル ディープ ラーニング**(LDL))]**オプションで、利用可能な解析エンジンごとに**[enable (**有効にする**)]**を選択します。現在、オプションのLDLモードで利用可能な解析エンジンは2種類あります。**HTTP**コマンド アンド コントロール検出器と**HTTP2**コマンド アンド コントロール検出器です。
4. 対応する分析エンジンを使用して脅威が検出されたときに取る **Action** を指定します。

   各解析エンジンのデフォルトのアクションは***alert***ですが、*Palo Alto Networks*では、セキュリティ体制を最適にするために、すべてのアクションを***Reset-Both***に設定することをお勧めします。

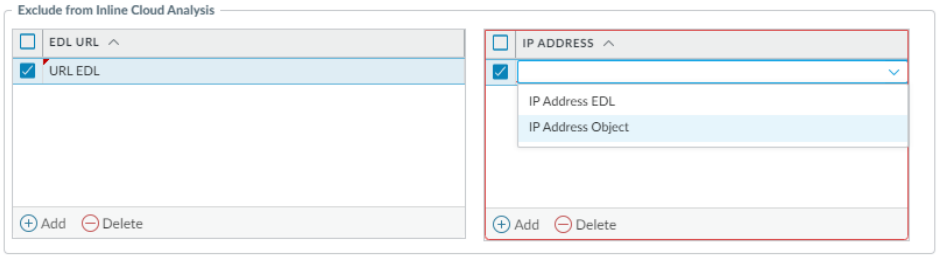
   - **Allow** - 要求は許可され、ログ エントリは生成されません。
   - **Alert** - 要求が許可され、Threat ログ エントリが生成されます。
   - **Drop** - 要求を削除します。リセットアクションはホスト/アプリケーションに送信されません。
   - **Reset-Client** - クライアント側の接続をリセットします。
   - **Reset-Server** - サーバー側の接続をリセットします。
   - **Reset-Both** - クライアント側とサーバー側の両方で接続をリセットします。
5. **OK** をクリックして Anti-Spyware Profile 構成ダイアログを終了し、**Commit** をクリックして変更を行います。

©2025 Palo Alto Networks, Inc.

STEP 4 | (Optional)Inline Cloud Analysis で誤検知が発生した場合は、Anti-Spyware プロファイルに URL や IP アドレスの例外を追加します。例外を追加するには、外部動的リスト (URL または IP アドレス一覧の種類) または **Addresses** オブジェクトを指定します。

1. **External Dynamic Lists** または [IP] **Addresses** オブジェクト例外を追加します。
2. **Objects > Security Profiles > Anti-Spyware** を選択します。
3. 特定の URL や IP アドレスを除外する Anti-Spyware プロファイルを選択し、**Inline Cloud Analysis** を選択します。
4. **Add** を追加する例外の種類に応じて、**EDL URL** または **IP** アドレス を選択し、既存の URL または IP アドレスの外部動的リストを選択します。使用可能なものがない場合は、新しい external dynamic list を作成します。IP アドレスの例外については、オプションで **Addresses** オブジェクト リストを選択できます。

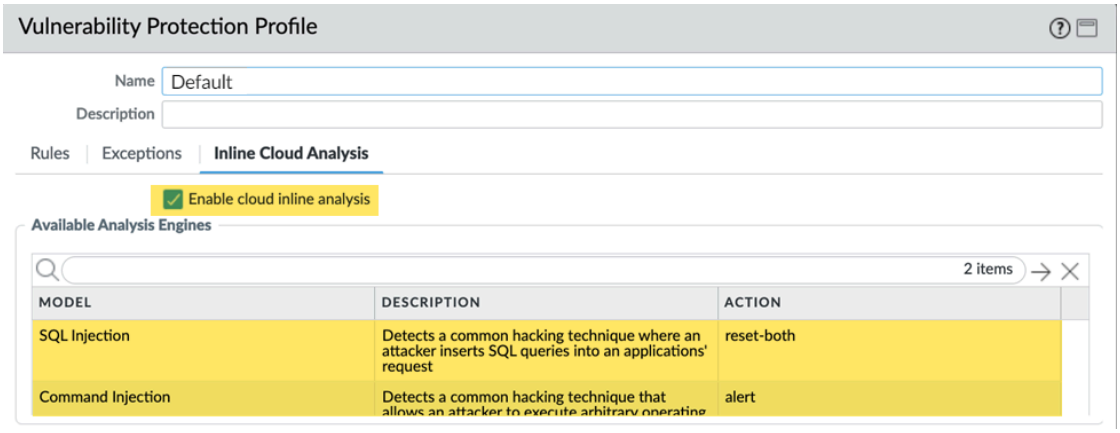
   *Panorama*管理対象ファイアウォールで***[Shared (共有)]***として構成されているアンチスパイウェア プロファイルは、インライン クラウド解析の例外リストに*IP*アドレス オブジェクトを追加できません。



5. **OK** をクリックしてスパイウェア対策プロファイルを保存し、**Commit** に変更を保存します。

©2025 Palo Alto Networks, Inc.

STEP 5 | (PAN-OS 11.0以降でサポート)インライン クラウド解析(コマンド インジェクションやSQLインジェクションの脆弱性についてトラフィックをリアルタイムで解析する)を有効にするために、脆弱性防御セキュリティ プロファイルを更新または新規作成します。



1. 既存の脆弱性防御セキュリティ プロファイルを選択するか、新しいプロファイルを追加します(**[Objects (オブジェクト)]** > **[Security Profiles (セキュリティ プロファイル)]** > **[Vulnerability Protection (脆弱性防御)]**)。
2. 脆弱性防御プロファイルを選択し、**[Inline Cloud Analysis (インライン クラウド解析)]**と**[Enable cloud inline analysis (クラウド インライン解析を有効にする)]**に進みます。
3. 対応する解析エンジンを使用して脆弱性の悪用が検出されたときに取るアクションを指定します。現在、次の2つの解析エンジンを利用できます。**SQL**インジェクションとコマンド インジェクションです。
   - **Allow** - 要求は許可され、ログ エントリは生成されません。
   - **Alert** - 要求が許可され、Threat ログ エントリが生成されます。
   - **Reset-Client** - クライアント側の接続をリセットします。
   - **Reset-Server** - サーバー側の接続をリセットします。
   - **Reset-Both** - クライアント側とサーバー側の両方で接続をリセットします。
4. **[OK]**をクリックして脆弱性防御プロファイル構成ダイアログを終了し、**[Commit (コミットする)]**をクリックして変更を行います。

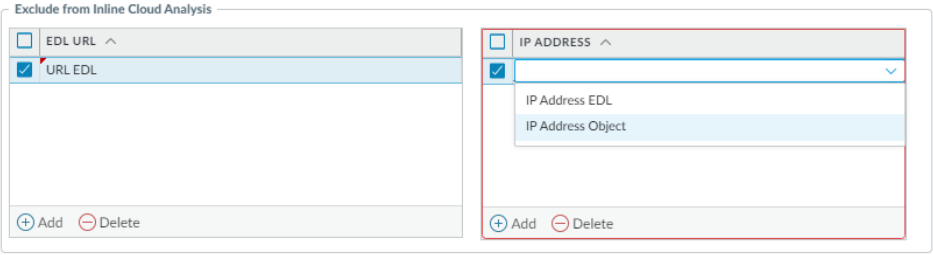
STEP 6 | (オプション)インライン クラウド解析で誤検知が発生した場合は、脆弱性防御プロファイルにURLやIPアドレスの例外を追加します。例外を追加するには、外部動的リスト (URL または IP アドレス一覧の種類) または **Addresses** オブジェクトを指定します。

1. **External Dynamic Lists** または [IP] **Addresses** オブジェクト例外を追加します。
2. **[Objects (オブジェクト)]** > **[Security Profiles (セキュリティ プロファイル)]** > **[Vulnerability (脆弱性)]**を選択し、脆弱性防御プロファイルに戻ります。
3. 特定のURLやIPアドレスを除外する脆弱性プロファイルを選択し、**[Inline Cloud Analysis (インライン クラウド解析)]**を選択します。
4. **Add** を追加する例外の種類に応じて、**EDL URL** または **IP** アドレス を選択し、既存の URL または IP アドレスの外部動的リストを選択します。使用可能なものがない場合は、新

©2025 Palo Alto Networks, Inc.

しい external dynamic list を作成します。IP アドレスの例外については、オプションで **Addresses** オブジェクト リストを選択できます。

*Panorama*管理対象ファイアウォールで*[Shared (*共有*)]*として構成されている脆弱性プロファイルは、インライン クラウド解析の例外リストに*IP*アドレス オブジェクトを追加できません。



5. **[OK]**をクリックして脆弱性防御プロファイルを保存し、**[Commit (**コミットする**)]**をクリックして変更を行います。

STEP 7 | タイムアウト遅延と、要求が最大遅延を超えた場合に実行するアクションを設定します。

1. **[Device (**デバイス**)]** > **[Setup (**セットアップ**)]** > **[Content-ID (**コンテンツID**)]** > **[Threat Prevention Inline Cloud Analysis (Threat Prevention**インライン クラウド解析**)]**を選択します。
2. インライン クラウド解析リクエストのタイムアウト値と、遅延制限に達したときに実行する関連アクションを指定します。
   - Max Latency (ms) (最大遅延(ms)): 結果を返すインライン クラウド解析の最大許容処理時間を秒単位で指定します。
   - Allow on Max Latency (最大遅延時に許可): 最大遅延に達したときに、ファイアウォールが許可のアクションを実行できるようにします。このオプションの選択を解除すると、ファイアウォール アクションがブロックに設定されます。
   - Log Traffic Not Scanned (スキャンされていないトラフィックをログに記録): 高度で回避的なコマンドアンドコントロール(C2)の脅威の存在を示す異常な特性を示すが、Threat Preventionのインライン クラウド アナライザーによって処理されていないトラフィック要求をファイアウォールがログに記録できるようにします。
3. **OK** をクリックして変更を確定します。

STEP 8 | デバイス証明書をインストールするインライン クラウド解析が有効になっているすべてのファイアウォールについて繰り返します。

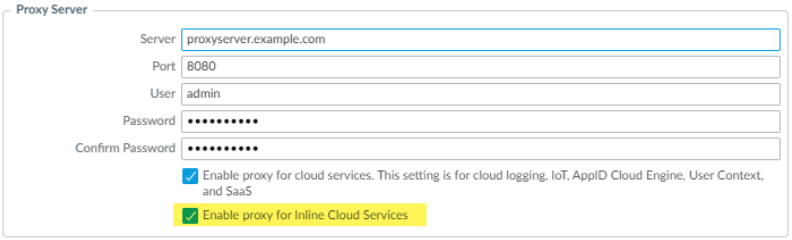
STEP 9 | (ファイアウォールが明示的なプロキシ サーバーを使用してデプロイされている場合に必要)設定されたすべてのインライン クラウド解析機能によって生成される要求を促進するサーバーへのアクセスに使用するプロキシ サーバーを構成します。単一のプロキシ サー

©2025 Palo Alto Networks, Inc.

バーを指定することができ、構成済みのすべてのインライン クラウドおよびロギング サービスを含む、すべてのPalo Alto Networksの更新サービスに適用されます。

1. (PAN-OS 11.2.3以降）PAN-OSを介してプロキシ サーバーを構成します。
   1. **[Device (デバイス)]** > **[Setup (セットアップ)]** > **[Services (サービス)]**の順に選択し、**[Services (サービス)]**セクションを編集します。
   2. **[Proxy Server (プロキシ サーバー)]**設定を指定し、**[Enable proxy for Inline Cloud Services (インライン クラウド サービスのプロキシを有効にする)]**を選択します。**[Server (サーバー)]**フィールドにIPアドレスまたはFQDNのいずれかを指定できます。

      プロキシ サーバーのパスワードには、6文字以上を含める必要があります。

   3. **OK** をクリックします。
2. (次のリリースのみ:PAN-OS 10.2.11以降およびPAN-OS 11.1.5以降)ファイアウォールCLIを使用してプロキシ サーバーを構成します。
   1. ファイアウォール CLI にアクセスします。
   2. 次のCLIコマンドを使用して、基本プロキシ サーバーの設定を行います。

```
set deviceconfig system secure-proxy-server <FQDN_or_IP>
 set deviceconfig system secure-proxy-port <1-65535>
```


©2025 Palo Alto Networks, Inc.

```
set deviceconfig system secure-proxy-user <value> set
deviceconfig system secure-proxy-password <value>
```

プロキシ サーバーのパスワードには、6文字以上を含める必要があります。

3. 次のCLIコマンドを使用して、プロキシ サーバーがインライン クラウド サービス サーバーに要求を送信できるようにします。

```
debug dataplane mica set inline-cloud-proxy enable
```

4. 次のCLIコマンドを使用して、インライン クラウド サービスのプロキシ サポートの現在の動作ステータスを表示します。

```
debug dataplane mica show inline-cloud-proxy
```

以下に例を示します。

```
debug dataplane mica show inline-cloud-proxy Proxy for
 Advanced Services is Disabled
```

STEP 10 | (Optional)インラインクラウド分析サービス要求を処理するために firewall によって使用される Cloud Content Fully Qualified Domain Name (FQDN) を設定します。既定の FQDN は hawkeye.services-edge.paloaltonetworks.com に接続し、最も近い cloud サービス サー

©2025 Palo Alto Networks, Inc.

バーに解決されます。自動サーバー選択をオーバーライドするには、データの常駐性とパフォーマンスの要件に最も適した地域の cloud コンテンツサーバーを指定します。

Cloud Content FQDN はグローバルに使用されるリソースであり、この接続に依存する他のサービスがトラフィックペイロードを送信する方法に影響します。

firewall がお住まいのリージョンに対して正しい Content Cloud FQDN (**Device** > **Setup** > **Content-ID** > **Content Cloud Setting**) を使用していることを確認し、必要に応じて FQDN を変更します。

*NGFW*が*SaaS Security*の導入を容易にするためにインラインで設定されている場合、フランスと日本にある*FQDN*は、現在*SaaS Security*の機能をサポートしていないことに注意してください。

- 米国中部(米国アイオワ州): **us.hawkeye.services-edge.paloaltonetworks.com**
- ヨーロッパ(ドイツ、フランクフルト): **eu.hawkeye.services-edge.paloaltonetworks.com**
- アジア太平洋(シンガポール): **apac.hawkeye.services-edge.paloaltonetworks.com**
- インド(ムンバイ): **in.hawkeye.services-edge.paloaltonetworks.com**
- 英国(イギリス、ロンドン）: **uk.hawkeye.services-edge.paloaltonetworks.com**
- フランス(フランス、パリ）: **fr.hawkeye.services-edge.paloaltonetworks.com**
- 日本(東京）: **jp.hawkeye.services-edge.paloaltonetworks.com**
- オーストラリア(オーストラリア、シドニー）: **au.hawkeye.services-edge.paloaltonetworks.com**
- カナダ(モントリオール、カナダ）: **ca.hawkeye.services-edge.paloaltonetworks.com**
- スイス(チューリッヒ、スイス）: **ch.hawkeye.services-edge.paloaltonetworks.com**

©2025 Palo Alto Networks, Inc.

STEP 11 | (Optional)Advanced Threat Prevention cloud サービスへの firewall 接続の状態を確認します。

接続ステータスを表示するには、ファイアウォール上で次のCLIコマンドを実行します。

```
show ctd-agent status security-client
```

以下に例を示します。

```
show ctd-agent status security-client ...Security Client AceMlc2(1)
 Current cloud server: hawkeye.services-edge.paloaltonetworks.com
 Cloud connection: connected ...
```

*CLI*出力は簡潔にするために短縮されています。

Advanced Threat Prevention クラウドサービスに接続できない場合、次のドメインがブロックされていないことを確認します。: hawkeye.services-edge.paloaltonetworks.com。

STEP 12 | （任意） Advanced Threat Preventionの監視

インライン クラウド解析の設定(Strata Cloud Manager)

STEP 1 | インライン クラウド解析を利用するには、Advanced Threat Prevention 機能にアクセスできるアクティブなPrisma Accessサブスクリプションが必要です。Prisma Accessで提供されるアプリケーションとサービスに関する詳細については、「利用可能なすべてのアプリケーションとサービス」を参照してください。

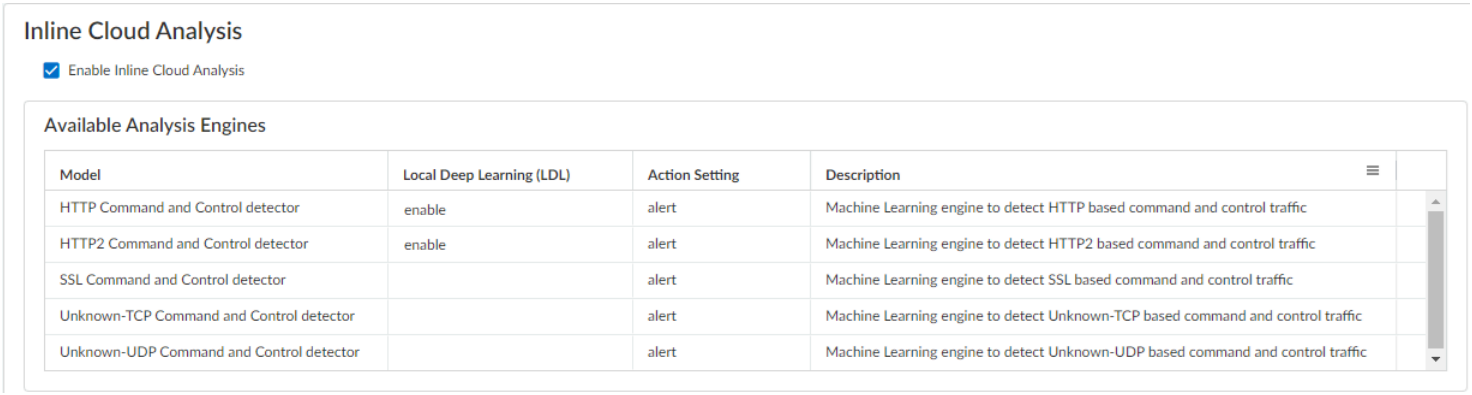
現在アクティブなライセンスがあるサブスクリプションを確認するには、ライセンスでサポートされている内容を確認してください。

STEP 2 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerにログインします。

©2025 Palo Alto Networks, Inc.

STEP 3 | インライン クラウド解析(高度なC2 (コマンドアンドコントロール)とスパイウェアの脅威についてトラフィックをリアルタイムで解析)を有効にするために、アンチスパイウェア セキュリティ プロファイルを更新または新規作成します。

1. **[Manage (管理)] > [Configuration (設定)] > [NGFW and Prisma Access (NGFWとPrisma Access)] > [Security Services (セキュリティ サービス)] > [Anti-Spyware (アンチスパイウェア)]**を選択します。
2. アンチスパイウェア セキュリティ プロファイルを選択し、**[Inline Cloud Analysis (インライン クラウド解析)]**パネルおよび**[Enable Inline Cloud Analysis (インライン クラウド解析を有効にする)]**に進みます。



3. **[Local Deep Learning (LDL) (ローカル ディープ ラーニング(LDL))]**オプションで、利用可能な解析エンジンごとに**[enable (有効にする)]**を選択します。現在、オプションのLDLモードで利用可能な解析エンジンは2種類あります。**HTTP**コマンド アンド コントロール検出器と**HTTP2**コマンド アンド コントロール検出器です。
4. 対応する分析エンジンを使用して脅威が検出されたときに取る **Action** を指定します。

   各解析エンジンのデフォルトのアクションは***alert***ですが、*Palo Alto Networks*では、セキュリティ体制を最適にするために、すべてのアクションを***Reset-Both***に設定することをお勧めします。

   - **Allow** - 要求は許可され、ログ エントリは生成されません。
   - **Alert** - 要求が許可され、Threat ログ エントリが生成されます。
   - **Drop** - 要求を削除します。リセットアクションはホスト/アプリケーションに送信されません。
   - **Reset-Client** - クライアント側の接続をリセットします。
   - **Reset-Server** - サーバー側の接続をリセットします。
   - **Reset-Both** - クライアント側とサーバー側の両方で接続をリセットします。
5. **[OK]** をクリックしてアンチスパイウェア セキュリティ プロファイル設定ダイアログを終了し、**[Commit (コミット)]**をクリックして変更を行います。

©2025 Palo Alto Networks, Inc.

STEP 4 | (Optional)Inline Cloud Analysis で誤検知が発生した場合は、Anti-Spyware プロファイルに URL や IP アドレスの例外を追加します。例外を追加するには、外部動的リスト(URLまたはIPアドレス一覧の種類)または**Addresses**ポリシー オブジェクトを指定します。

1. **External Dynamic Lists** または [IP] **Addresses** オブジェクト例外を追加します。
2. **[Manage (管理)]** > **[Configuration (設定)]** > **[Anti-Spyware (アンチスパイウェア)]**の順に選択します。
3. 特定のURLやIPアドレスを除外するアンチスパイウェア プロファイルを選択し、**[Inline Cloud Analysis (インライン クラウド解析)]**ペインに移動します。
4. 追加する例外の種類に応じて、**[Add EDL/URL (DL/URLの追加)]**または**[Add IP Address (IPアドレスの追加)]**を選択し、既存のURLまたはIPアドレスの外部動的リストを選択します。使用可能なものがない場合は、新しい外部動的リスト ポリシー オブジェクトを作成します。IP アドレスの例外については、オプションで **Addresses** オブジェクト リストを選択できます。

5. **OK** をクリックしてスパイウェア対策プロファイルを保存し、**Commit** に変更を保存します。

STEP 5 | （任意） Advanced Threat Preventionの監視

©2025 Palo Alto Networks, Inc.

ブルート フォース攻撃の防御

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

ブルート フォース攻撃は、同じ送信元または宛先 IP アドレスで大量の要求/応答を使用してシステムに侵入します。攻撃者は試行錯誤を繰り返す方法によって、チャレンジまたは要求に対する応答を推測します。

脆弱性防御プロファイルにはブルートフォース攻撃から保護するシグネチャも含まれています。各シグネチャには ID、脅威名、および重大度が設定されており、パターンが記録されるとトリガーされます。パターンは、トラフィックがブルート フォース攻撃として識別される条件と間隔を指定します。一部のシグネチャは、重大度がより低く、一致パターンを指定する別の子シグネチャと関連付けられています。パターンがシグネチャや子シグネチャと一致すると、シグネチャのデフォルト アクションがトリガーされます。

防御を適用するには、以下の手順を実行します。

- 脆弱性保護プロファイルをセキュリティポリシー ルールに適用します。アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップを参照してください。
- 新しいシグネチャを含むコンテンツ更新をインストールし、ファイアウォールに対する新たに出現した脅威から防御します。コンテンツとソフトウェア更新のインストールを参照してください。

©2025 Palo Alto Networks, Inc.

ブルート フォース シグネチャのアクションとトリガー条件のカスタマイズ

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

ファイアウォールには、2 種類の事前定義されたブルート フォース シグネチャが含まれています。親シグネチャと子シグネチャです。子シグネチャはシグネチャに一致するトラフィック パターンの 1 回の発生です。親シグネチャは子シグネチャに関連付けられ、子シグネチャで定義されたトラフィック パターンに一致するイベントが指定された時間内に複数回発生した場合にトリガーされます。

通常、子シグネチャのデフォルト アクションは許可です。1 回のイベントだけで攻撃されたことにはならないためです。これにより、正当なトラフィックがブロックされず、また重要性の低いイベントについての脅威ログが生成されなくなります。Palo Alto Networks は、デフォルト アクションを変更する場合は必ず慎重に検討することをお勧めします。

多くの場合、ブルート フォース シグネチャが注目に値するイベントであるのは、その繰り返しパターンのためです。必要な場合は次のいずれかの作業を行って、ブルート フォース シグネチャ用のアクションをカスタマイズできます。

- ブルート フォース カテゴリ内のすべてのシグネチャのデフォルト アクションを変更するルールを作成します。トラフィックの許可、アラート、ブロック、リセット、または破棄のいずれかを選択できます。
- 特定のシグネチャに例外を定義します。例えば、CVE を検索したり、CVE 用の例外を定義したりできます。

親シグネチャの場合、トリガー条件およびアクションの両方を変更できます。子シグネチャの場合は、アクションのみを変更できます。

効果的に攻撃を軽減するために、ほとんどのブルート フォース シグネチャで *drop* アクションや *reset* アクションよりも *block-ip address* アクションを指定します。

©2025 Palo Alto Networks, Inc.

STEP 1 | 新しい脆弱性防御プロファイルを作成します。

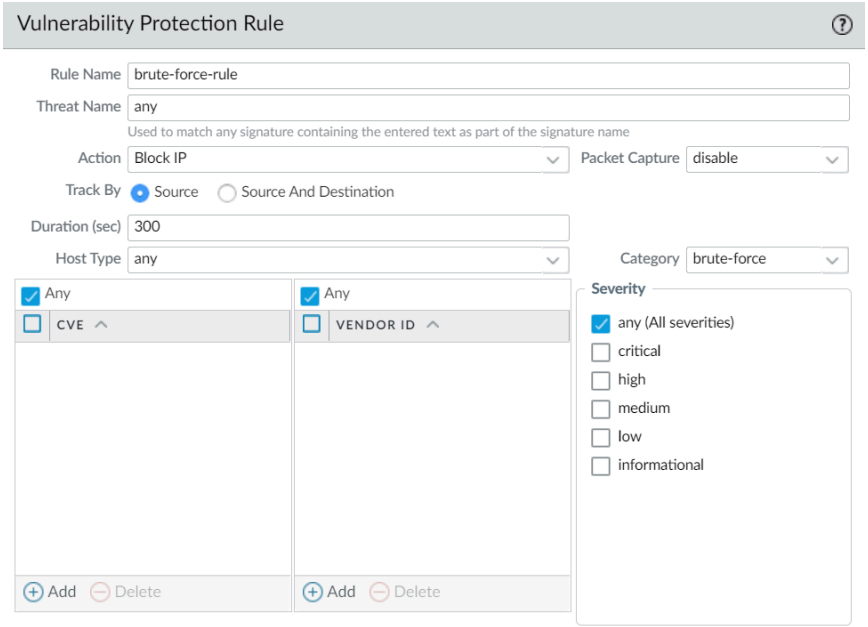
1. **Objects (**オブジェクト**) > Security Profiles (**セキュリティ プロファイル**) > Vulnerability Protection (**脆弱性保護**)** を選択してプロファイルを **Add (**追加**)** します。
2. 脆弱性保護プロファイルの **Name (**名前**)** を入力します。
3. （任意）**Description (**内容**)** を入力します。
4. （任意）プロファイルを次のものと **Shared (**共有**)** することを指定します。
   - マルチ **vsys** ファイアウォール上のすべての仮想システム（**vsys**）–クリア（無効化）すると、**Objects (**オブジェクト**)** タブで選択された仮想システムでのみプロファイルを利用できます。
   - **Panorama** 上のすべてのデバイスグループ–クリア（無効化）すると、**Objects (**オブジェクト**)** タブで選択されたデバイスグループでのみプロファイルを利用できます。
5. （任意—Panorama only） **Disable (**無効化**) override** to prevent administrators from overriding the settings of this Vulnerability Protection (脆弱性保護) profile in device groups that inherit the profileデフォルトでこのオプションはオフになっており、管理者は、このプロファイルを継承するデバイス グループの設定をオーバーライドできます。

©2025 Palo Alto Networks, Inc.

STEP 2 | カテゴリ内のすべてのシグネチャのアクションを定義するルールを作成します。

1. **Rules (**ルール**)** タブで新しいルールを **Add (**追加**)** し、**Rule Name (**ルール名**)** を入力します。
2. （任意）具体的な脅威名を指定します（デフォルトは **any (**すべて**)**）。
3. **[**アクション**]** を設定します。この例では、**Block IP[**ブロックIP**]** に設定されています。

   脆弱性保護プロファイルで *IP* をブロックするように設定した場合、ファイアウォールはまずハードウェアを使用して *IP* アドレスをブロックします。攻撃トラフィックがハードウェアのブロック容量を超えた場合、次にファイアウォールはソフトウェア ブロック メカニズムを使用して残りの *IP* アドレスをブロックします。
4. **[**カテゴリ**]** を **[brute-force]** に設定します。
5. （任意）ブロック中の場合はブロックする **Host Type (**ホスト タイプ**)** を指定します。**server** あるいは **r client** (default is **any**).
6. 特定の署名のアクションをカスタマイズするには、「手順 3」を参照してください。
7. 親署名のトリガーしきい値をカスタマイズするには、ステップ 4 を参照してください。



8. **[OK]** をクリックしてルールおよびプロファイルを保存します。

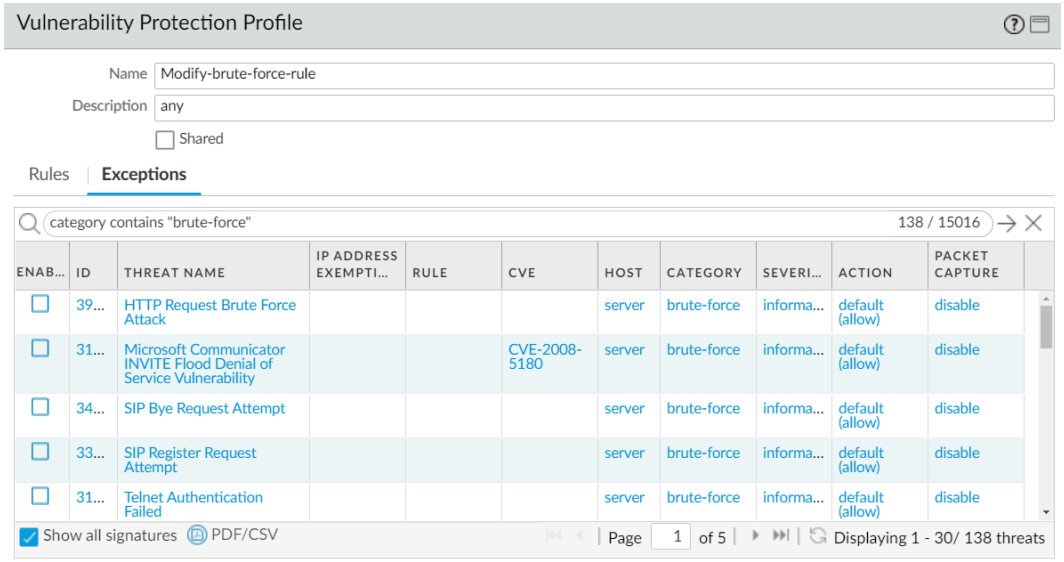
©2025 Palo Alto Networks, Inc.

STEP 3 | （任意）特定のシグネチャのアクションをカスタマイズします。

1. **Exceptions (**例外**)** タブで **Show all signatures (**すべてのシグネチャを表示**)** し、修正したいシグネチャを探します。

   ブルート フォース カテゴリのすべてのシグネチャを表示するには、`category contains 'brute-force'`と検索します。

2. 特定のシグネチャを編集するには、Actions（操作）列の事前定義されたデフォルト アクションをクリックします。



3. アクションを設定します。**Allow (**許可**)**、**Alert (**アラート**)**、**Block Ip (**ブロック **IP)**、あるいは **Drop (**ドロップ**)**。**Block Ip (**ブロック **IP)** を選択した場合、以下の追加タスクを実行します。

   1. **[**日時**]** にアクションをトリガーするまでの時間を秒数で指定します。
   2. **Track By (**追跡区分**)** を指定するかどうか、**IP source (IP** 送信元**)** あるいは **IP source and destination (IP** 送信元および宛先**)** のどちらを使用して IP アドレスをブロックするかを指定します。

4. **OK** をクリックします。
5. 変更したシグネチャのそれぞれに対して、**[**有効化**]** 列のチェックボックスをオンにします。
6. **OK** をクリックします。

©2025 Palo Alto Networks, Inc.

STEP 4 | 親シグネチャのトリガー条件をカスタマイズします。

編集可能な親シグネチャにはこのアイコンがついています。 .

この例では、検索条件はブルート フォース カテゴリおよび CVE-2008-1447 です。

1. シグネチャの時間属性および集約条件を編集（ ）します。
2. トリガーしきい値を変更するには、**seconds (秒)** あたりの **Number of Hits (ヒット数)** を指定します。
3. ヒット数（**Aggregation Criteria (集約条件)**）を **source (送信元)**、**destination (宛先)**、または**source-and-destination (送信元および宛先)** のいずれで集約するかを指定します。
4. **OK** をクリックします。

STEP 5 | この新しいプロファイルをセキュリティポリシー ルールに関連付けます。

1. **Policies (ポリシー)** > **Security (セキュリティ)**を選択し、セキュリティポリシールールを**Add**（追加）または変更します。
2. **Actions** （アクション） タブで、プロファイル設定の **Profile Type (プロファイル タイプ)** として **Profiles (プロファイル)** を選択します。
3. **Vulnerability Protection (脆弱性保護)** プロファイルを選択します。
4. **OK** をクリックします。

STEP 6 | 変更をコミットします。

1. **Commit**（コミット）をクリックします。

©2025 Palo Alto Networks, Inc.

回避シグネチャの有効化

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

偽装された HTTP あるいは TLS リクエストを検知する Palo Alto Networks の回避シグネチャが、DNS リクエストで指定されているもの以外のドメインにクライアントが接続する際にアラートを生成できます。回避シグネチャは、ファイアウォールがさらに DNS プロキシとして動作してドメイン名のクエリを解決できるように設定されている場合のみ機能します。ベストプラクティスとして、次の各ステップを実施して回避シグネチャを有効化してください。

STEP 1 | ファイアウォールをクライアントおよびサーバー間で DNS プロキシとして動作できるようにします。

次の作業を含馬手、DNS プロキシ オブジェクトの設定を行います。

- ファイアウォールに DNS クエリをリッスンさせるインターフェイスを指定します。
- DNS リクエストを解決するためにファイアウォールが通信を行う DNS サーバーを定義します。
- 静的 FQDN から IP アドレスへのエントリーをセットアップし、ファイアウォールが DNS サーバーにアクセスすることなくローカルで解決できるようにします。
- 解決したホスト名から IP アドレスへのマッピングをキャッシュできるようにします。

STEP 2 | 最新のアプリケーションおよび脅威コンテンツ バージョン（コンテンツ バージョン 579 以降のもの）を入手します。

1. **Device**（デバイス） > **Dynamic Updates**（動的更新）を選択します。
2. 最新のアプリケーションおよび脅威コンテンツ更新を**Check Now**[今すぐチェック]して入手します。
3. アプリケーションおよび脅威コンテンツ バージョン 579（あるいはそれ以降）をダウンロードし、インストールします。

©2025 Palo Alto Networks, Inc.

STEP 3 | 回避シグネチャにマッチしたトラフィックをファイアウォールがどのように扱うか定義します。

1. **Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > Anti-Spyware (アンチスパイウェア)** を選択し、アンチスパイウェア プロファイル を **Add (追加)** あるいは変更します。
2. **Exceptions (例外)** を選択し、さらに**Show all signatures (すべてのシグネチャを表示)** を選択します。
3. キーワード`evasion`に基づいてシグネチャをフィルタリングします。
4. すべての回避シグネチャの**Action** [アクション]を、許可あるいはデフォルトのアクション以外のものに設定します（デフォルトのアクションは回避シグネチャが許可されるものです）。例えば、シグネチャ ID 14978 および 14984 の **Action (アクション)** を **alert (アラート)** あるいは **drop (ドロップ)** に設定します。
5. **OK** をクリックし、更新したアンチスパイウェア プロファイルを保存します。
6. アンチスパイウェア プロファイルをセキュリティポリシールールに適用します。**Policies (ポリシー) > Security (セキュリティ)** の順に選択し、適切なポリシーを選択して変更し、**Actions** （アクション） タブをクリックします。Profile Settings (プロファイル設定) で **Anti-Spyware (アンチスパイウェア)** の隣りにあるドロップダウンリストをクリックし、先ほど変更したアンチスパイウェア プロファイルを選択して回避シグネチャを強制します。

STEP 4 | 変更をコミットします。

Commit（コミット）をクリックします。

©2025 Palo Alto Networks, Inc.

脅威例外の作成

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

Palo Alto Networks は、脅威シグネチャの推奨されるデフォルトのアクション（ブロックやアラートなど）を定義しています。脅威IDを使用することで、脅威シグネチャを適用対象から除外したり、脅威シグネチャに適用するアクションを変更したりできます。例えば、ネットワーク上で誤検出を引き起こす脅威シグネチャに対するアクションを変更することができます。

アンチウイルス、脆弱性、スパイウェア、およびDNSシグネチャ用の脅威例外を設定し、脅威に対する対応方法を変更します。ただし、開始する前に、最適なセキュリティ体制を実現するために、デフォルトまたはベストプラクティスのシグニチャ設定に基づいて脅威が適切に検出され、実施されていることを確認してください。

- アンチウイルス、脅威およびアプリケーション、WildFireシグネチャの最新の更新プログラムを取得します(ファイアウォール用)。
- アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップし、これらのセキュリティ プロファイルをセキュリティポリシーに適用します。
- Strata Cloud Manager
- PAN-OS & Panorama

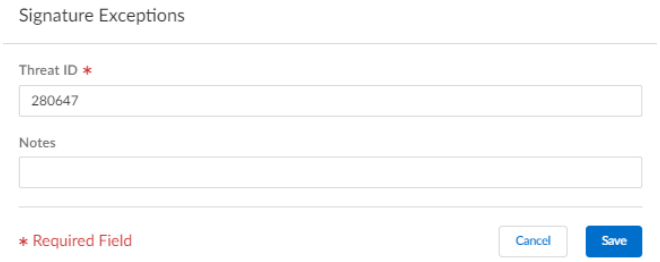
©2025 Palo Alto Networks, Inc.

脅威例外の作成(Strata Cloud Manager)

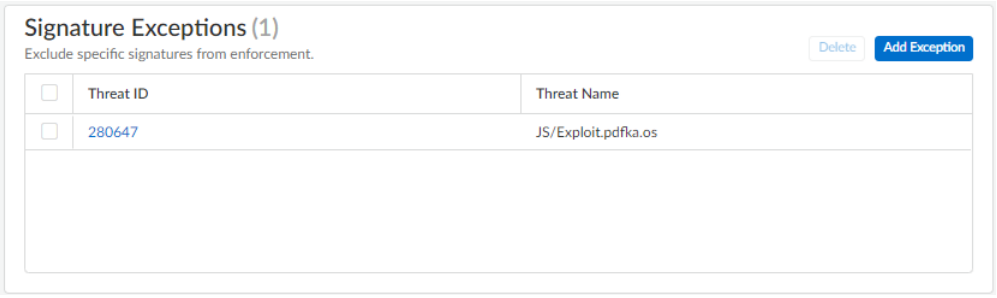
STEP 1 | アンチウイルス シグネチャを適用対象から除外します。

*WildFire*およびアンチウイルス プロファイルを使用してアンチウイルス シグネチャを適用対象から除外できますが、特定のアンチウイルス シグネチャに対するアクションを変更することはできません。ただし、セキュリティ プロファイルの***[Enforcement Actions (**強制アクション**)]***を編集することで、さまざまな種類のトラフィックでウイルスが検出された場合の強制アクションを定義することができます。

1. **[Manage (管理)] > [Configuration (設定)] > [NGFW and Prisma Access (NGFW**と**Prisma Access)] > [Security Services (**セキュリティ サービス**)] > [WildFire and Antivirus (WildFire**とアンチスパイウェア**)]**を選択します。
2. プロファイルを追加するか、脅威シグネチャを除外する既存のWildFireおよびアンチウイルス プロファイルを選択し、**[Advanced Settings (**詳細設定**)]**タブに移動します。
3. **[Signature Exceptions (**シグネチャ例外**)]** メニューから、**[Add Exception (**例外を追加**)]**を選択し、適用から除外する脅威シグニチャの脅威**ID**を指定します。オプションで、シグニチャ例外に注記を追加できます。



4. 終了したら、シグニチャ例外を保存します。
5. 有効な脅威シグニチャIDによって、脅威名のフィールドにデータが自動入力されます。アクティブなシグニチャ例外の完全なリストを表示するだけでなく、不要になったエントリを削除することもできます。



6. 繰り返して追加の例外を追加するか、すべての脅威例外を追加したら**[Save (**保存**)]**をクリックします。

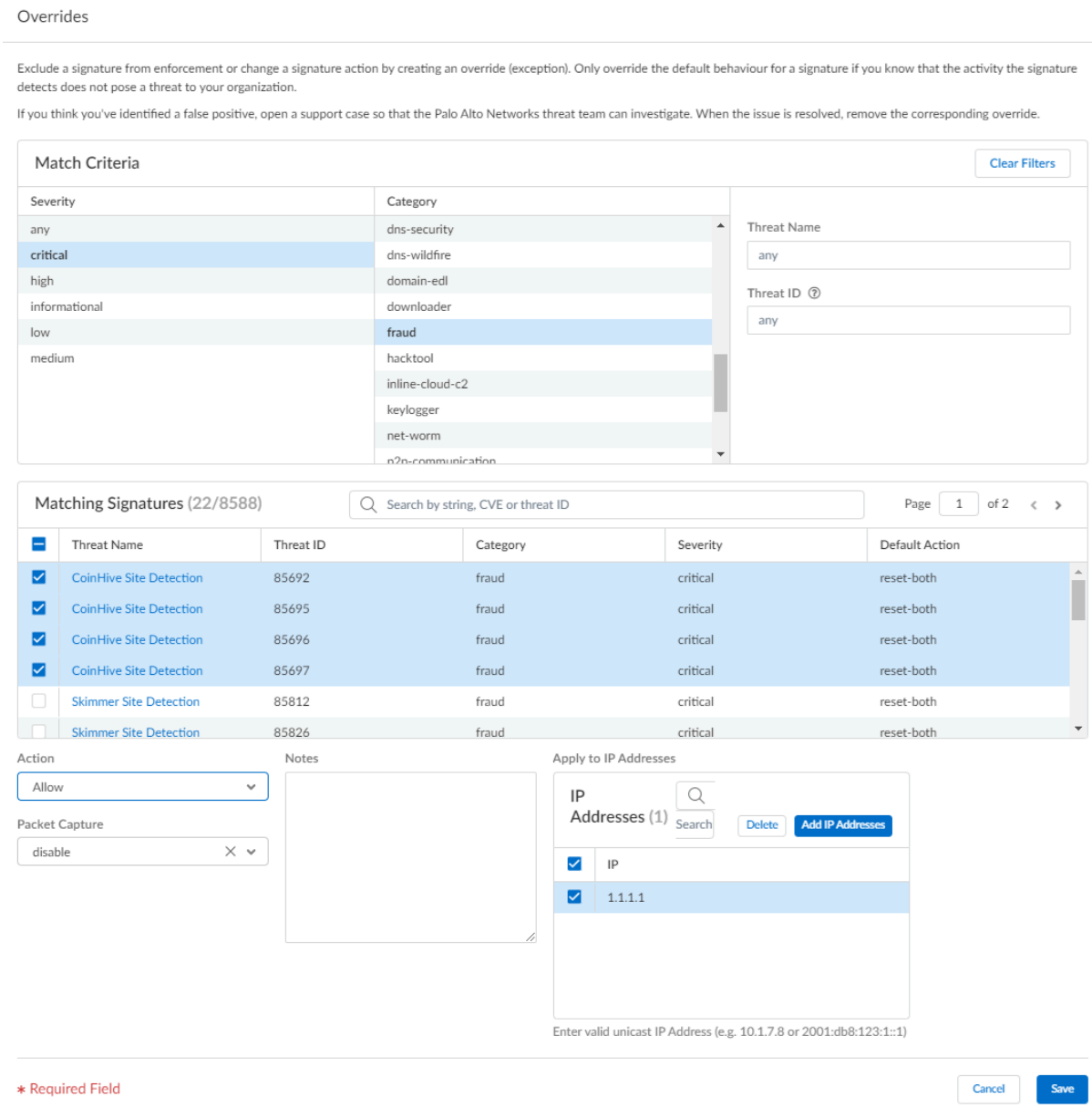
©2025 Palo Alto Networks, Inc.

STEP 2 | 脆弱性とスパイウェアのシグネチャに対する適用を変更します（DNSシグネチャは除く。スパイウェア シグネチャの一種ですが、DNSシグネチャはPrisma AccessのDNS セキュリティ サブスクリプションを通じて処理されます）。

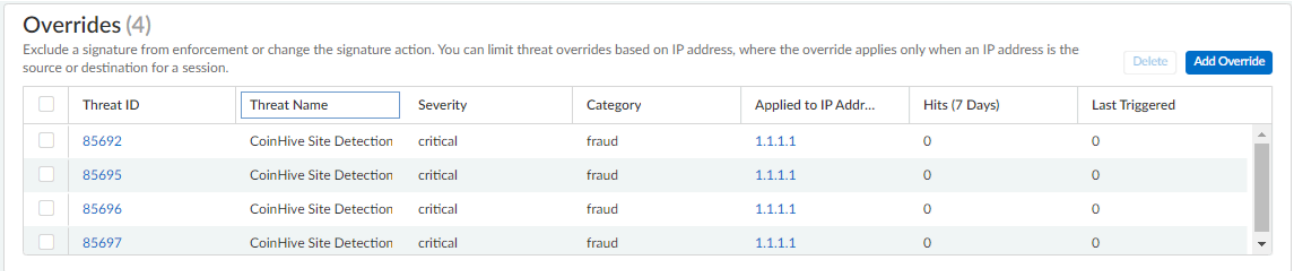
1. シグニチャのタイプに応じて、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW and Prisma Access (NGFWとPrisma Access)]** > **[Security Services (セキュリティ サービス)]** > **[Anti-Spyware (アンチスパイウェア)]**を選択するか、または**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW and Prisma Access (NGFWとPrisma Access)]** > **[Security Services (セキュリティ サービス)]** > **[Vulnerability Protection (脆弱性防御)]**を選択します。
2. プロファイルを追加するか、シグネチャ適用を変更する既存のアンチスパイウェア プロファイルまたは脆弱性防御プロファイルを選択し、**[Add Override (オーバーライドを追加)]**を選択します。
3. 関連する一致条件を指定して、スパイウェアまたは脆弱性シグネチャを検索します。これにより、使用可能なシグニチャが自動的にフィルタリングされ、その結果が**[Matching Signatures (一致するシグネチャ)]**セクションに表示されます。
4. 適用を変更するシグニチャのチェックボックスをオンにします。

©2025 Palo Alto Networks, Inc.

5. 選択したシグニチャに対して、変更した強制ルールを適用する更新後のアクション、パケット キャプチャ、および**IP**アドレスを指定します。



6. 更新したシグネチャ適用設定を保存します。
7. 各種統計を含むオーバーライドの完全なリストを表示するだけでなく、不要になったエントリを削除することもできます。



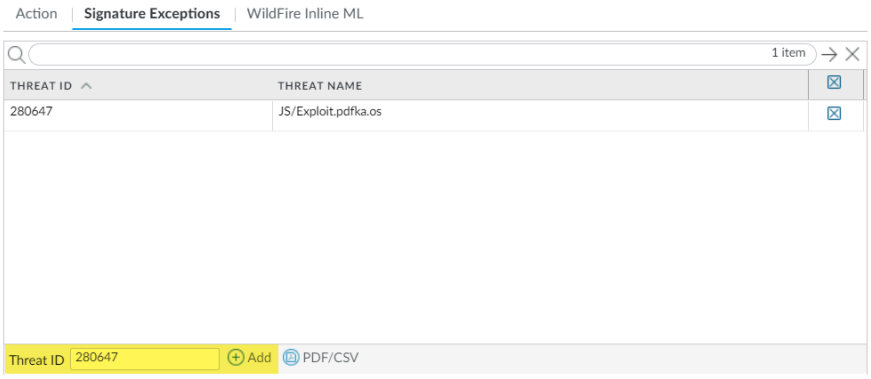
©2025 Palo Alto Networks, Inc.

脅威例外の作成(NGFW (Managed by PAN-OS or Panorama))

STEP 1 | アンチウイルス シグネチャを適用対象から除外します。

アンチウイルス プロファイルを使用してアンチウイルス シグネチャを適用対象から除外できますが、特定のアンチウイルス シグネチャに対するファイアウォールのアクションを変更することはできません。ただし、*Decoders* (***Objects** > **Security Profiles** > **Antivirus** > **<antivirus-profile>** > **Antivirus***) を編集することで、*firewall* がさまざまな種類のトラフィックで見つかったウイルスを強制するアクションを定義できます。

1. **Objects** (オブジェクト) **>** > **Security Profiles** (セキュリティ プロファイル) **>** > **Antivirus** (アンチウイルス) を選択します。
2. 脅威シグネチャを除外したいアンチウイルス プロファイルを **Add** (追加) するか、既存のものを変更し、**Signature Exception** (シグネチャ例外) を選択します。
3. 適用対象から除外したい脅威シグネチャの **Threat ID** (脅威 ID) を **Add** (追加) します。



4. **OK** をクリックしてアンチウイルス プロファイルを保存します。

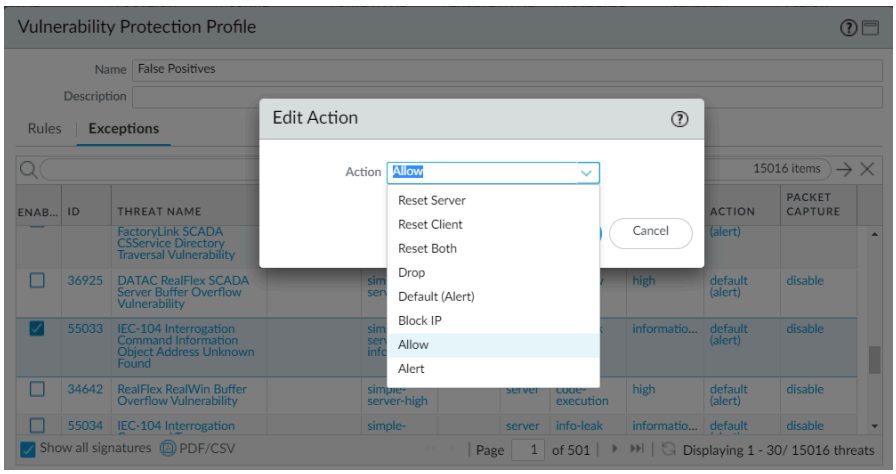
STEP 2 | 脆弱性およびスパイウェア シグネチャに対する対処方法を変更します（DNS シグネチャを除きます。スパイウェア シグネチャの一種である DNS シグネチャに対する対処方法を変更する場合は、次のオプションまでスキップしてください）。

1. **Objects** (オブジェクト) **>** > **Security Profiles** (セキュリティ プロファイル) **>** > **Anti-Spyware** (アンチスパイウェア) あるいは **Objects** (オブジェクト) **>** > **Security Profiles** (セキュリティ プロファイル) **>** > **Vulnerability Protection** (脆弱性保護) を選択します。
2. 脅威シグネチャを除外したい既存のアンチスパイウェアまたは脆弱性防御プロファイルを **Add** (追加) するか変更してから、アンチスパイウェア保護プロファイルの **Signature**

©2025 Palo Alto Networks, Inc.

Exceptions (シグネチャ例外**)** または脆弱性防御プロファイルの **Exceptions (**例外**)** のいずれかを選択します。

3. **Show all signatures (**すべてのシグネチャを表示**)** してフィルタリングし、適用ルールを変更したいシグネチャを選択します。
4. 適用の仕方を変更したいシグネチャの **Enable (**有効**)**列にあるボックスにチェックを入れます。
5. この脅威シグネチャについて、ファイアウォールに適用させたい **Action (**アクション**)** を選択します。



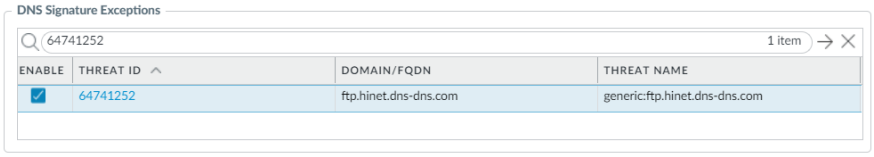
誤検出を引き起こすため、シグネチャを適用から除外したい場合は、**Action (**アクション**)** を **Allow (**許可**)** に設定します。

6. **OK** をクリックし、新しい、あるいは変更したアンチスパイウェアまたは脆弱性保護プロファイルを保存します。

STEP 3 | DNS シグネチャに対する対処方法を変更します。

デフォルト設定では、DNS シグネチャにシンクホールがあると検知された悪意のあるホスト名を DNS が検索します。

1. **Objects (**オブジェクト**) > > Security Profiles (**セキュリティ プロファイル**) > > Anti-Spyware (**アンチスパイウェア**)** を選択します。
2. 脅威シグネチャを除外したいアンチスパイウェア プロファイルを **Add (**追加**)** するか、既存のものを変更し、**DNS Exceptions (DNS** 例外**)** を選択します。
3. 施行から除外する DNS シグネチャの DNS 脅威 ID を検索し、該当するシグネチャのボックスを選択します:



4. **OK** をクリックし、新しい、あるいは変更したアンチスパイウェア プロファイルを保存します。

©2025 Palo Alto Networks, Inc.

DNS クエリを使用してネットワーク上の感染ホストを特定する

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

アンチスパイウェア プロファイルの DNS シンクホール アクションにより、既知の悪意あるドメインの DNS クエリあるいはカスタムドメインに対する応答をファイアウォールが偽装し、ネットワーク上のマルウェアに感染したホストを特定することができます。侵入されたホストは、コマンド アンド コントロール (C2) サーバーとの通信を開始する可能性があります。接続が確立されると、攻撃者は感染したホストをリモートから制御し、ネットワークにさらに侵入したりデータを漏洩させることができます。

Palo Alto Networks の DNS シグネチャ リストに含まれているあらゆるドメインにクエリするDNSは、Palo Alto Networks のサーバー IP アドレスにシンクホールされます。

ファイアウォールには、悪意のあるドメインおよび C2 ドメインを識別するために使用できる DNS シグネチャの送信元が 2 つあります。

- (高度/脅威防御サブスクリプションが必要)ローカルDNSシグネチャ: これはファイアウォールが悪意のあるドメインを識別するために使用できるDNSシグネチャの限定された内蔵セットです。ファイアウォールは、日々のウイルス対策アップデートの一環として新規の DNS シグネチャを取得します。
- (DNS セキュリティ サブスクリプションが必要) DNS セキュリティ シグネチャ: ファイアウォールは、Palo Alto NetworksのDNS セキュリティ クラウド サービスにアクセスして、DNSシグネチャの完全なデータベースに対して悪意のあるドメインをチェックします。DNS セキュリティのみが提供する特定のシグネチャは、ドメイン生成アルゴリズム (DGA) や DNS トンネリングなどの機械学習技術を使用した C2 攻撃を一意に検出することができます。DNS セキュリティ サブスクリプションの詳細については、DNSセキュリティ ガイドを参照してください。

  DNSセキュリティ シグネチャのシンクホール アクションを指定する場合は、それらの設定をDNSセキュリティ プロファイルの一部として構成できます。

ローカル DNS シグネチャセットまたは DNS セキュリティシグネチャセット内のドメインへの DNS クエリは、Palo Alto Networks サーバーにリダイレクトされ、ホストは悪意のあるドメインにはアクセスできません。次のトピックでは、DNS シンクホールを有効にして、感染ホストを特定する方法について詳細にご説明します。

- DNS シンクホールの動作原理
- DNS シンクホールの設定
- カスタムドメインのリスト用にDNS シンクホールを設定

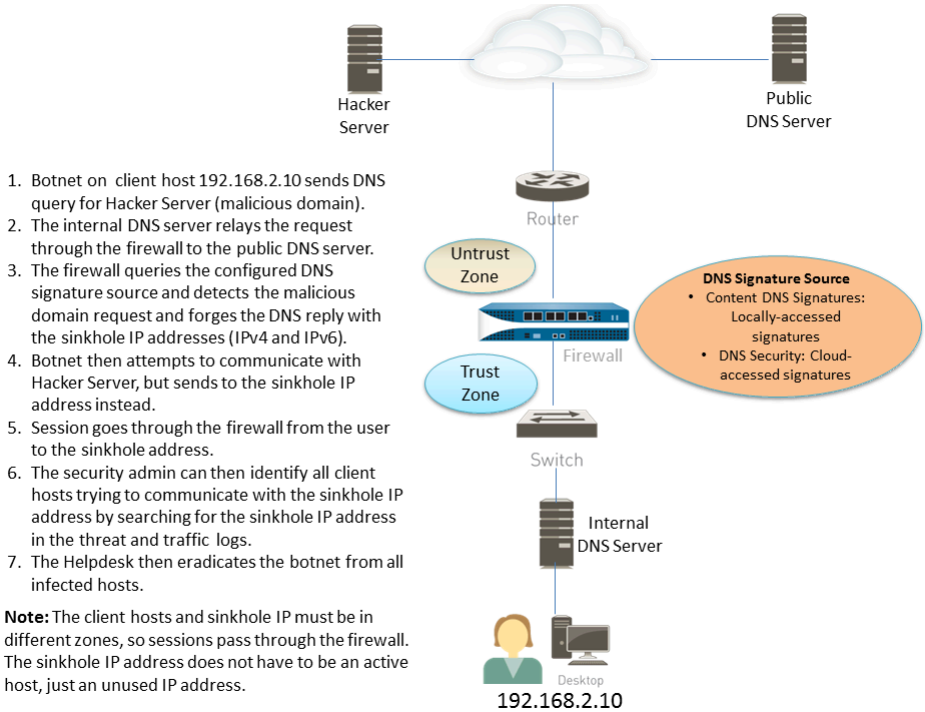
©2025 Palo Alto Networks, Inc.

- ネットワーク上のローカル サーバーにシンクホールIPアドレスを設定
- 悪意のあるドメインへの接続を試みた感染ホストを確認

DNS シンクホールの動作原理

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

DNS シンクホール機能を使用すると、ファイアウォールが感染クライアントの DNS クエリを見ることができない状況（つまり、ファイアウォールが DNS クエリの発信元を確認できない状況）で、DNS トラフィックを使用して保護されたネットワーク上の感染ホストを特定できます。ファイアウォールがローカル DNS サーバーよりもインターネット側にある通常のデプロイメントでは、脅威ログは、実際の感染ホストではなくローカル DNS リゾルバをトラフィックの送信元として識別します。マルウェア DNS クエリのシンクホール処理では、この可視性の問題を以下のようにして解決します。すなわち、クライアント ホストによる悪意あるドメインへのクエリに対する応答を偽装することで、悪意あるドメイン (たとえば、コマンド アンド コントロールなど) への接続を試みるクライアントが、デフォルトの Palo Alto Networks シンクホール IP アドレス (あるいはカスタムドメインのリスト用に DNS シンクホールを設定する場合は定義済みの IP アドレス) に接続を試みるように仕向けます。その後、感染ホストを簡単にトラフィックログで特定することができます。



 ©2025 Palo Alto Networks, Inc.

DNS シンクホールの設定

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

DNSシンクホールを有効にするには、ファイアウォール セキュリティ ポリシー ルールにデフォルトのアンチスパイウェア プロファイルをアタッチします(アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップを参照)。ユーザーが指定する Palo Alto Networks の DNS シグネチャ ソースに含まれているあらゆるドメインに対する DNS クエリは、Palo Alto Networks のシンクホール IP アドレスに解決されます。現在、この IP アドレスは IPv4—sinkhole.paloaltonetworks.com、およびループバック アドレス IPv6 address—::1 です。このアドレスは変更される場合があり、コンテンツ更新で更新される可能性があります。

STEP 1 | 外部動的リスト内のドメインのカスタム リスト用にDNS シンクホールを有効化します。

1. **Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > Anti-Spyware (アンチスパイウェア)** を選択します。
2. 既存のプロファイルを変更するか、既存のデフォルト プロファイルの 1 つを選択してコピーします。
3. プロファイルの **Name**（名前） を入力し、**DNS Policies**（**DNS**ポリシー）タブを選択します。
4. **default-paloalto-dns** が **Signature Source (シグネチャ送信元)**にあることを確認します。
5. （任意）**Packet Capture (パケット キャプチャ)** ドロップダウンリストにて、セッションの最初のパケットをキャプチャする場合は**single-packet**を、1～50の間で設定を行うには**extended-capture**を選択します。その後、パケット キャプチャを使用してさらに分析できます。

STEP 2 | アンチスパイウェア プロファイルのシンクホール設定を確認します。

1. **DNS Policies (DNS ポリシー)** タブで、DNSクエリの**Policy Action**が **sinkhole(シンクホール)** になっていることを確認します。
2. DNS Sinkhole Settings (DNSシンクホールの設定) セクションで **Sinkhole (シンクホール)** が有効になっていることを確認します。便宜を図るため、デフォルトのシンクホールのIPアドレスはPalo Alto Networksサーバーにアクセスするよう設定されています。Palo Alto Networksはコンテンツ更新によりこのIPアドレスを自動的に更新する場合があります。

   Sinkhole IPv4 または**Sinkhole IPv6**アドレスをネットワーク上のローカルサーバーまたはループバックアドレスに変更する場合は、ネットワーク上のローカル サーバーにシンクホールIPアドレスを設定を参照してください。
3. **OK** をクリックし、アンチスパイウェア プロファイルを保存します。

©2025 Palo Alto Networks, Inc.

STEP 3 | アンチスパイウェア プロファイルをセキュリティポリシールールに適用します。

1. **Policies (**ポリシー**) > Security (**セキュリティ**)** を選択し、セキュリティポリシー ルールを選択します。
2. **Actions** [アクション] タブで、**Log at Session Start** [セッション開始時にログ]チェックボックスをオンにして、ログを有効にします。
3. Profile Setting [プロファイル設定]セクションで**Profile Type**[プロファイルタイプ]ドロップダウンリストをクリックし、すべての**Profiles**[プロファイル]を表示します。**Anti-Spyware** [アンチスパイウェア]ドロップダウンリストで、新しいプロファイルを選択します。
4. **[OK]** をクリックしてポリシー ルールを保存します。

STEP 4 | ファイアウォール上のアクティビティを監視することで、ポリシーアクションが適用されていることをテストします。

1. **ACC**を選択し、URL Domain [URLドメイン]をグローバルフィルターとして追加し、アクセスしたドメインのThreat Activity [脅威アクティビティ]およびBlocked Activity [ブロックされたアクティビティ]を確認します。
2. **Monitor (**監視**) > Logs (**ログ**) > Threat (**脅威**)** を選択し、`(action eq sinkhole)` でフィルタリングしてシンクホールされたドメインのログを確認します。

カスタムドメインのリスト用にDNS シンクホールを設定

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

ドメインのカスタム リスト用のDNS シンクホールを有効にするには、そのドメインを含む外部動的リストを作成し、アンチスパイウェア プロファイルでシンクホール アクションを有効にし、そのプロファイルをセキュリティポリシー ルールに付与する必要があります。クライアントがリストに挙がっている悪意のあるドメインにアクセスしようとすると、ファイアウォールがパケット中の宛先IPアドレスをシンクホール用にデフォルトのPalo Alto Networksサーバーあるいはユーザー定義のIPアドレスに偽装します。

外部動的リストに含まれたカスタムドメインごとに、ファイアウォールはDNSベースのスパイウェア シグネチャを生成します。このシグネチャは Custom Malicious DNS Query <domain name> という名前で、重大度が中程度のスパイウェアです。各シグネチャは、 24 バイトのドメイン名のハッシュです。

ドメイン リストのエントリ制限については、「外部動的リスト」を参照してください。

©2025 Palo Alto Networks, Inc.

STEP 1 | 外部動的リスト内のドメインのカスタム リスト用にDNS シンクホールを有効化します。

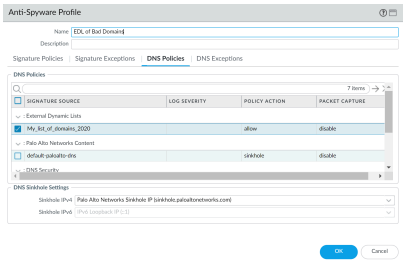
1. **Objects (**オブジェクト**) > Security Profiles (**セキュリティ プロファイル**) > Anti-Spyware (**アンチスパイウェア**)** を選択します。
2. 既存のプロファイルを変更するか、既存のデフォルト プロファイルの 1 つを選択してコピーします。
3. プロファイルの **Name** [名前]を入力し、**DNS Policies** [DNS ポリシー]タブを選択します。
4. **External Dynamic Lists (**外部動的リスト**)** シグネチャ送信元から EDL を選択します。

   次のタイプの外部動的リストをすでに作成済みの場合：ドメイン リストはここで選択できます。*URL*あるいは*IP*アドレスのタイプの外部動的リストを作成していても、このリストには表示されません。
5. アンチスパイウェア プロファイルの外部動的リストを設定します（外部動的リストにアクセスするためにファイアウォールを設定を参照）。**Type (**タイプ**)** のデフォルトの値は **Domain List (**ドメイン リスト**)** です。
6. （任意）**Packet Capture (**パケット キャプチャ**)** ドロップダウンリストにて、セッションの最初のパケットをキャプチャする場合は**single-packet**を、1～50の間で設定を行うには**extended-capture**を選択します。その後、パケット キャプチャを使用してさらに分析できます。

STEP 2 | アンチスパイウェア プロファイルのシンクホール設定を確認します。

1. **DNS Policies (DNS** ポリシー**)** タブで、DNSクエリの**Policy Action**が **sinkhole(**シンクホール**)** になっていることを確認します。
2. DNS Sinkhole Settings (DNSシンクホールの設定) セクションで **Sinkhole (**シンクホール**)** が有効になっていることを確認します。便宜を図るため、デフォルトのシンクホールのIPアドレスはPalo Alto Networksサーバーにアクセスするよう設定されています。Palo Alto Networksはコンテンツ更新によりこのIPアドレスを自動的に更新する場合があります。

   Sinkhole IPv4 (シンクホール **IPv4)** あるいは**Sinkhole IPv6 (**シンクホール **IPv6)** アドレスをネットワーク上のローカル サーバーあるいはループバック アドレスに変更する場合はネットワーク上のローカル サーバーにシンクホールIPアドレスを設定をご覧ください。



3. **OK** をクリックし、アンチスパイウェア プロファイルを保存します。

©2025 Palo Alto Networks, Inc.

STEP 3 | アンチスパイウェア プロファイルをセキュリティポリシールールに適用します。

1. **Policies (**ポリシー**) > Security (**セキュリティ**)** を選択し、セキュリティポリシー ルールを選択します。
2. **Actions** [アクション] タブで、**Log at Session Start** [セッション開始時にログ]チェックボックスをオンにして、ログを有効にします。
3. Profile Setting [プロファイル設定]セクションで**Profile Type**[プロファイルタイプ]ドロップダウンリストをクリックし、すべての**Profiles**[プロファイル]を表示します。**Anti-Spyware** [アンチスパイウェア]ドロップダウンリストで、新しいプロファイルを選択します。
4. **[OK]** をクリックしてポリシー ルールを保存します。

STEP 4 | ポリシー アクションが適用されているかどうかテストします。

1. ドメイン リストに属する外部動的リスト エントリを表示し、リストに含まれるドメインにアクセスします。
2. ファイアウォール上のアクティビティを監視するには：
   1. **ACC**を選択し、URL Domain [URLドメイン]をグローバルフィルターとして追加し、アクセスしたドメインのThreat Activity [脅威アクティビティ]およびBlocked Activity [ブロックされたアクティビティ]を確認します。
   2. **Monitor (**監視**) > Logs (**ログ**) > Threat (**脅威**)** を選択し、(`action eq sinkhole`) でフィルタリングしてシンクホールされたドメインのログを確認します。

STEP 5 | 外部動的リストのエントリーが無視されるかスキップされるかを検証します。

ファイアウォール上で次のCLIコマンドを実行し、リストの詳細情報を表示します。

```
request system external-list show type domain name <list_name>
```

以下に例を示します。

```
request system external-list show type domain name
 My_List_of_Domains_2015 vsys1/EBLDomain:Next update
 at :Thu May 21 10:15:39 2015 Source : https://1.2.3.4/
My_List_of_Domains_2015 Referenced :Yes Valid :Yes Number of
 entries :3 domains:www.example.com baddomain.com qqq.abcedfg.com
```

STEP 6 | （任意）外部動的リストを必要な時に取得します。

更新されたリストを次の更新のタイミング（その外部動的リスト用に定義した**Repeat** [繰り返し]頻度）ではなくオンデマンドでファイアウォールに取得させるには、次のCLIコマンドを実行します。

```
request system external-list refresh type domain name  <list_name>
```

代わりに、ファイアウォールのインターフェイスを使用して Web　サーバーから外部動的リストを取得することもできます。

©2025 Palo Alto Networks, Inc.

ネットワーク上のローカル サーバーにシンクホールIPアドレスを設定

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

デフォルト設定では、すべてのPalo Alto Networks DNSシグネチャに対してシンクホールが有効になっており、シンクホールIPアドレスはPalo Alto Networksサーバーにアクセスするよう設定されています。シンクホールIPアドレスをネットワーク上のローカル サーバーに設定したい場合はこのセクションの説明に従ってください。

悪意あるソフトウェアがIPv4 と IPv6 のどちらか一方または両方のプロトコルを使用して DNS クエリを実行する可能性があるため、IPv4およびIPv6アドレスの両方を取得してシンクホールIPアドレスとして使用する必要があります。シンクホール IP アドレスとセッションの開始を試みた感染ホストがファイアウォール経由でルーティングされるように、DNS シンクホール アドレスは、クライアント ホストと異なるゾーンに属している必要があります。

このシンクホール アドレスは、この目的のために予約する必要があります。このアドレスを物理ホストに割り当てる必要はありません。また、ハニーポット サーバーを物理ホストとして使用することで、悪意あるトラフィックをさらに詳しく分析することもできます。

以下に示す設定手順では、以下の *DNS* シンクホール アドレスを使用します。

IPv4 DNS シンクホール アドレス – *10.15.0.20*

IPv6 DNS シンクホール アドレス – *fd97:3dec:4d27:e37c:5:5:5:5*

STEP 1 | シンクホール インターフェイスとゾーンを設定します。

クライアント ホストが存在するゾーンからのトラフィックはシンクホール IP アドレスが定義されているゾーンにルーティングする必要があります。これにより、トラフィックがログに記録されます。

シンクホール トラフィックには専用のゾーンを使用します。このゾーンに、感染ホストからのトラフィックが送信されます。

1. **Network (**ネットワーク**) > Interfaces (**インターフェイス**)** の順に選択し、シンクホール インターフェイスとして設定するインターフェイスを選択します。
2. **Interface Type**（インターフェイス タイプ） ドロップダウン リストで、**Layer3**（レイヤー **3**） を選択します。

©2025 Palo Alto Networks, Inc.

3. IPv4 アドレスを追加するには、**[IPv4]** タブで [スタティック] を選択して、[追加] をクリックします。この例では、10.15.0.20 を IPv4 DNS シンクホール アドレスとして追加します。
4. **[IPv6]** タブで [スタティック] を選択し、[追加] をクリックして、IPv6 アドレスとサブネット マスクを入力します。この例では、fd97:3dec:4d27:e37c::/64 を IPv6 シンクホール アドレスとして入力します。
5. **OK** をクリックして保存します。
6. シンクホール用のゾーンを追加するには、**Network (ネットワーク) > Zones (ゾーン)** を選択して **Add (追加)** をクリックします。
7. ゾーンの [名前] を入力します。
8. [タイプ] ドロップダウン リストで、[レイヤー **3**] を選択します。
9. [インターフェイス] セクションで、[追加] をクリックして、先ほど設定したインターフェイスを追加します。
10. **OK** をクリックします。

STEP 2 | DNS シンクホールを有効化します。

デフォルト設定では、すべてのPalo Alto Networks DNSシグネチャに対してシンクホールが有効になっています。シンクホール アドレスをローカル サーバーに変更するには、「カスタム ドメインの一覧に対するDNSシンクホールの設定」の手順2を参照してください。

STEP 3 | Trust ゾーンのクライアント ホストから Untrust ゾーンへのトラフィックを許可するセキュリティ ポリシー ルールを編集して、シンクホール ゾーンを宛先に含め、アンチスパイウェア プロファイルを添付します。

Trustゾーン内のクライアント ホストからUnTrustゾーンに向かうトラフィックを許可するセキュリティポリシールールを編集することで、感染ホストからのトラフィックを確実に識別できるようになります。シンクホール ゾーンをルールに宛先として追加することで、感染クライアントが偽の DNS クエリを DNS シンクホールに送信するようになります。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. クライアント ホスト ゾーンから Untrust ゾーンへのトラフィックを許可する既存のルールを選択します。
3. [宛先] タブで、シンクホール ゾーンを [追加] します。これにより、クライアント ホスト トラフィックがシンクホール ゾーンに流れるようになります。
4. **Actions** [アクション] タブで、**Log at Session Start** [セッション開始時にログ]チェックボックスをオンにして、ログを有効にします。これにより、Trust ゾーンのクライアント ホストからのトラフィックが、Untrust ゾーンまたはシンクホール ゾーンへのアクセス時にログに記録されるようになります。
5. [プロファイル設定] セクションで、DNS シンクホールを有効にした [アンチスパイウェア] プロファイルを選択します。
6. **OK** をクリックして Security (セキュリティ) ポリシールールを保存し、**Commit (コミット)** を実行します。

©2025 Palo Alto Networks, Inc.

STEP 4 | 感染ホストを確実に特定できるようにするために、Trust ゾーンのクライアント ホストから新しいシンクホール ゾーンへのトラフィックがログに記録されていることを確認します。

この例では、感染したクライアント ホストは 192.168.2.10、シンクホールの IPv4 アドレスは 10.15.0.20 です。

1. Trust ゾーンのクライアント ホストでコマンド プロンプトを開き、以下のコマンドを実行します。

```
C:\>ping <sinkhole address>
```

以下の出力例は、DNS シンクホール アドレス 10.15.0.2 に対して Ping 要求を送信したときの結果です。この例では、シンクホール IP アドレスが物理ホストに割り当てられていないため、結果は、`Request timed out` になっています。

```
C:\>ping 10.15.0.20 Pinging 10.15.0.20 with 32 bytes of
 data:Request timed out.Request timed out.Ping statistics for
 10.15.0.20:Packets:Sent = 4, Received = 0, Lost = 4 (100%
 loss)
```

2. ファイアウォール上で、**Monitor (監視) > Logs (ログ) > Traffic (トラフィック)** の順に選択して、送信元が 192.168.2.10、宛先が 10.15.0.20 のログ エントリを探します。これにより、シンクホール IP アドレスへのトラフィックがファイアウォール ゾーンを通過していることを確認できます。

ログを検索またはフィルタリングして、宛先が *10.15.0.20* のログのみ表示することもできます。それには、*[宛先]* 列で *IP* アドレス（*10.15.0.20*）をクリックします。すると、検索フィールドにフィルタ（*addr.dst in 10.15.0.20*）が追加されます。検索フィールドの右側の *Apply Filter*（フィルタの適用）アイコンをクリックして、フィルタを適用します。

STEP 5 | DNS シンクホールの設定が適切であることを検証します。

悪意のあるアプリケーションがホームを呼び出そうとする際に感染したクライアント ホストが実行するアクションを模擬的に行います。

1. ファイアウォールの現行のアンチウイルス シグネチャ データベースに含まれている悪意のあるドメインを探し、シンクホールのテストを行います。
    1. **Device (デバイス) > Dynamic (動的) Updates (アップデート)** を選択し、**Antivirus** セクションで現在インストールしているアンチウイルス データベースの **Release Notes (リリースノート)** リンクをクリックします。追加分のシグネチャ更新をリストアップしたアンチウイルス リリース ノートは、Palo Alto Networksサポート サイトのDynamic Update [動的更新]以下にもあります。
    2. リリース ノートの 2 列目で、特定のドメイン拡張子（たとえば、.com、.edu、.net など）を持つ行項目を探します。左側の列にドメイン名が表示されます。たとえ

 ©2025 Palo Alto Networks, Inc.

ば、アンチウイルス リリース 1117-1560 には、左側の列が "tbsbana" で、右側の列が "net" になっている項目が含まれます。

以下に、リリース ノートのこの行項目の内容を示します。

```
conficker:tbsbana 1 variants: net
```

2. クライアント ホストでコマンド プロンプトを開きます。
3. 既知の悪意あるドメインとして特定した URL に対して、NSLOOKUP を実行します。

   以下の例では、`track.bidtrk.com` という URL を使用しています。

```
C:\>nslookup track.bidtrk.com Server: my-local-
dns.local Address:10.0.0.222 Non-authoritative
 answer:Name: track.bidtrk.com.org Addresses:
 fd97:3dec:4d27:e37c:5:5:5:510.15.0.20
```

   悪意あるドメインに対する NSLOOKUP が、設定したシンクホール IP アドレス（10.15.0.20）を使用して偽造されている点に注目してください。このドメインは悪意ある DNS シグネチャと一致したため、シンクホール アクションが実行されています。
4. **Monitor (監視) > Logs (ログ) > Threat (脅威)** の順に選択して、対応する脅威ログ エントリを探し、NSLOOKUP 要求に対して正しいアクションが実行されたことを確認します。
5. **`track.bidtrk.com`** に対して Ping を実行します。シンクホール アドレスに対するネットワーク トラフィックが生成されます。

悪意のあるドメインへの接続を試みた感染ホストを確認

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

DNS シンクホールを設定して、悪意あるドメインへのトラフィックがシンクホール アドレスに向けて送信されることを確認したら、シンクホール アドレスへのトラフィックを定期的にモニターして、感染ホストを突き止め、脅威を排除する必要があります。

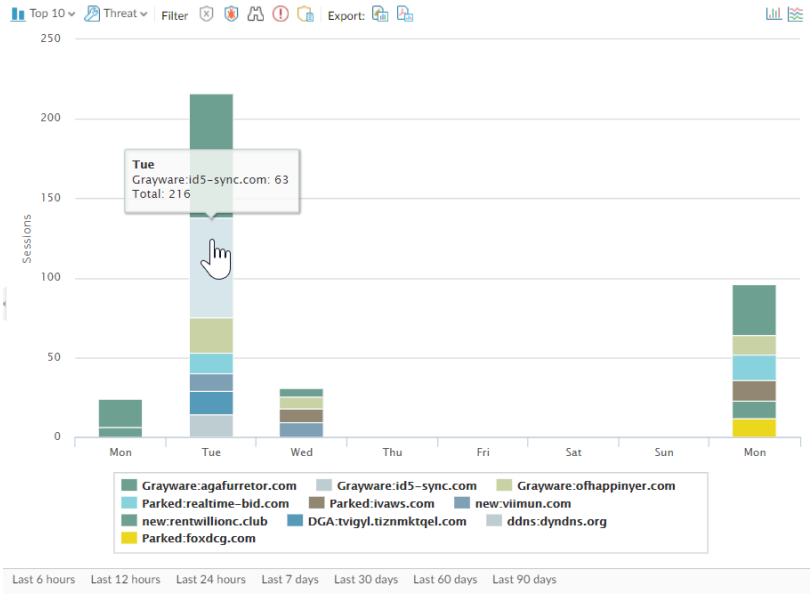
アプリケーション スコープを使用して感染したクライアント ホストを特定します。

1. **Monitor (監視) > App Scope (アプリケーション スコープ)** を選択し、さらに **Threat Monitor (脅威モニター)** を選択します。
2. 表示ページの上部にある [スパイウェアの表示] ボタンをクリックします。
3. 時間範囲を選択します。

   以下のスクリーンショットでは、疑わしい 3 つの DNS クエリのインスタンスが表示されています。これらは、テスト クライアント ホストが既知の悪意あるドメインに対し

 ©2025 Palo Alto Networks, Inc.

て NSLOOKUP を実行したときに生成されたクエリです。グラフをクリックして、イベントの詳細情報を表示します。



シンクホール IP アドレス（この例では 10.15.0.20）に対してトラフィックを送信したすべてのクライアント ホストを明示するカスタム レポートを設定します。

SNMP マネージャ、*Syslog* サーバー、および（または）*Panorama* に転送して、これらのイベントのアラートを有効にしてください。

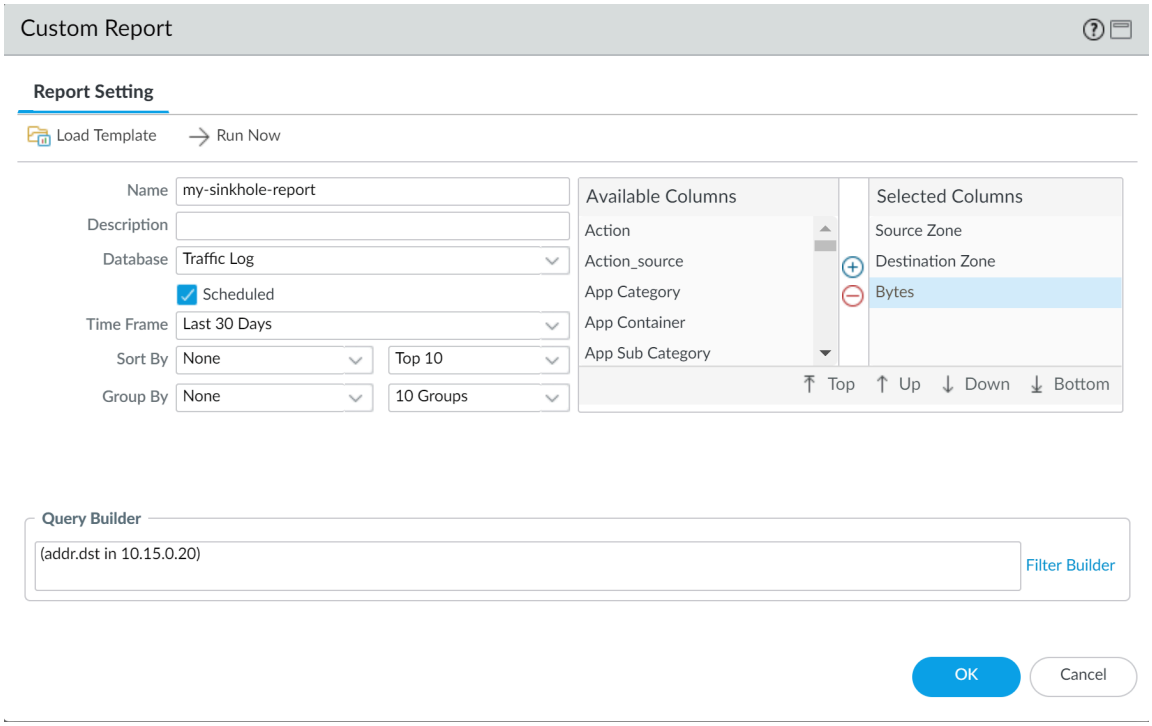
この例では、感染したクライアント ホストが、Palo Alto Networks DNS シグネチャ データベースに登録されている既知の悪意あるドメインに対して NSLOOKUP を実行します。すると、ローカルの DNS サーバーにクエリが送信され、その要求がファイアウォール経由で外部の DNS サーバーに転送されます。アンチスパイウェア プロファイルが設定されたファイアウォール セキュリティ ポリシーによって、このクエリが DNS シグネチャ データベースと照合され、シンクホール アドレス 10.15.0.20 および fd97:3dec:4d27:e37c:5:5:5:5 を使用して応答が偽造されます。クライアントがセッションを開始すると、アクティビティが送信元ホストおよび宛先アドレスと一緒にトラフィック ログに記録されます。この時点で、宛先アドレスは偽造されたシンクホール アドレスに置き換わっています。

ファイアウォール上のトラフィック ログを確認することによって、シンクホール アドレスにトラフィックを送信しているクライアント ホストをすべて特定できます。この例では、送信元アドレス 192.168.2.10 から悪意ある DNS クエリが送信されたことがログから分かります。これで、感染ホストを見つけて排除できます。DNS シンクホール オプションがなければ、管理者には、クエリを実行したシステムとしてローカルの DNS サーバーしか見えず、感染したクライアント ホストは分かりません。仮にシンクホール アクションを使用して脅威ログに対するレポートを実行したとしたら、ログには、感染ホストではなく、ローカルの DNS サーバーが表示されます。

1. **Monitor (監視) > Manage Custom Reports (カスタム レポートの管理)**の順に選択します。
2. **Add**（追加） をクリックして、レポートに **Name**（名前） をつけます。

©2025 Palo Alto Networks, Inc.

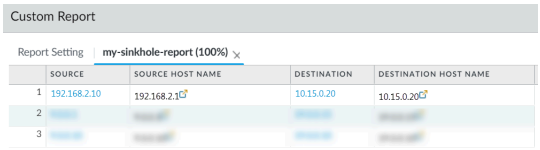
3. 以下のとおり、シンクホール アドレスへのトラフィックをキャプチャするカスタム レポートを定義します。
   - データベース – [トラフィック ログ] を選択します。
   - スケジュール設定 – [スケジュール設定] をオンにすると、レポートが毎晩実行されます。
   - 期間 – 30 日
   - 選択した列 – [送信元アドレス] または [送信元ユーザー]（User-ID を設定している場合）、および [宛先アドレス] を選択します。前者はレポート内の感染したクライアント ホストを識別します。後者はシンクホール アドレスです。
   - 画面下部のセクションで、シンクホール アドレス（この例では、10.15.0.20）へのトラフィックに対するカスタム クエリを作成します。**Query Builder**（クエリ ビルダー）ウィンドウに宛先アドレスを入力するか（**addr.dst in 10.15.0.20**）、各列で次の項目を選択して、**Add**（追加）をクリックします。結合子 = and、属性 = 宛先アドレス、演算子 = in、値 = 10.15.0.20。**Add**（追加） をクリックしてクエリを追加します。



4. [今すぐ実行] をクリックしてレポートを生成します。シンクホール アドレスに対してトラフィックを送信したすべてのクライアント ホストがレポートに表示されます。こ

©2025 Palo Alto Networks, Inc.

れらは、感染している可能性が極めて高いホストです。これで、ホストを突き止めて、スパイウェアに感染していないかチェックできます。



5. スケジュール設定された実行済みレポートを表示するには、**Monitor (監視)** > **Reports (レポート)** を選択します。

©2025 Palo Alto Networks, Inc.

カスタム シグネチャ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

特定のトラフィックを検出してブロックするカスタム脅威シグネチャを作成できます。ファイアウォールが Panorama管理サーバーによって管理されている場合、ThreatID はファイアウォール上の対応するカスタム脅威にマップされ、ファイアウォールが設定済みのカスタム ThreatID を入力した脅威ログを生成できるようにします。詳細については、カスタム アプリケーションと脅威シグネチャのガイドをご覧ください。

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Advanced Threat Preventionの監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

Palo Alto Networksでは、Advanced Threat Preventionとそれに関連するデータに依存するさまざまな製品のインテリジェンス検索に対応するため、Advanced Threat Preventionで処理されたアクティビティを監視するオプションをいくつか提供しています。製品プラットフォームによっては、ネットワーク アクティビティのコンテキストや特定ユーザーからのDNSリクエストの詳細など、DNSリクエストの統計や利用傾向も確認できる高レベルのダッシュボードにアクセスできます。

また、Advanced Threat PreventionがPalo Alto Networksの他のアプリケーションやセキュリティ サービスとどのように統合され、脅威から組織を保護するかを確認できるほか、Strata Cloud Managerコマンド センターを通じて、デプロイメント環境の運用の全体的な健全性を大まかに把握できます。コマンド センターはNetSecのホームページとして機能し、ネットワークの健全性、セキュリティ、および効率性の包括的なサマリーを、複数のデータ ファセットを備えたインタラクティブなビジュアル ダッシュボードで提供します。これにより、一目で簡単に評価できます。

ネットワーク アクティビティの大まかなビューについては、ネットワーク全体の脅威管理データだけでなく、さまざまなDNSトレンドを可視化するダッシュボードを表示できます。各ダッシュボードカードでは、脅威のネットワークへの影響をグラフィカルなレポート形式で独自のビューで確認できます。これにより、アプリケーションやユーザー、組織のポリシーを適用しているセキュリティ ルールに基づいて、脅威の影響を最も受けているエンティティを一目で把握できます。

Palo Alto Networksは、脅威アクティビティを監視するいくつかの方法を提供しています。

- Strata Cloud Managerコマンド センター
- 脅威ログの表示
- Advanced Threat Preventionレポートの表示
- Monitor Blocked IP Addresses（ブロックされた IP アドレスのモニター）
- 脅威シグネチャの詳細を把握

- 脅威カテゴリに基づくカスタム レポートの作成

©2025 Palo Alto Networks, Inc.

脅威ログの表示

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

脅威カテゴリは異なる種類の脅威シグネチャを分類化し、理解しやすくすると共に、脅威シグネチャが検出した各イベントを関連付けます。脅威カテゴリは、より広汎な脅威シグネチャ タイプ(スパイウェア、脆弱性、アンチウイルス)のサブセットです。脅威ログの各エントリは、記録された各イベントの **Threat Category (脅威カテゴリ)** を表示します。

脅威が検出されたときに自動的に生成される高度な脅威防御ログを参照、検索、および表示できます。通常、これには、ログの重大度レベルが特別に「なし」に設定していなければ、インラインMLを含む脅威防御機能が解析する適格な脅威シグニチャの一致が含まれます。ログ エントリは、脅威レベルや該当する場合は脅威の性質など、イベントに関する多数の詳細を提供します。

- Strata Cloud Manager
- PAN-OS & Panorama

脅威ログの確認(Cloud Management)

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerにログインします。

> [Activity (アクティビティ)]ダッシュボードの使用方法の詳細については、「ログ ビューアー」を参照してください。

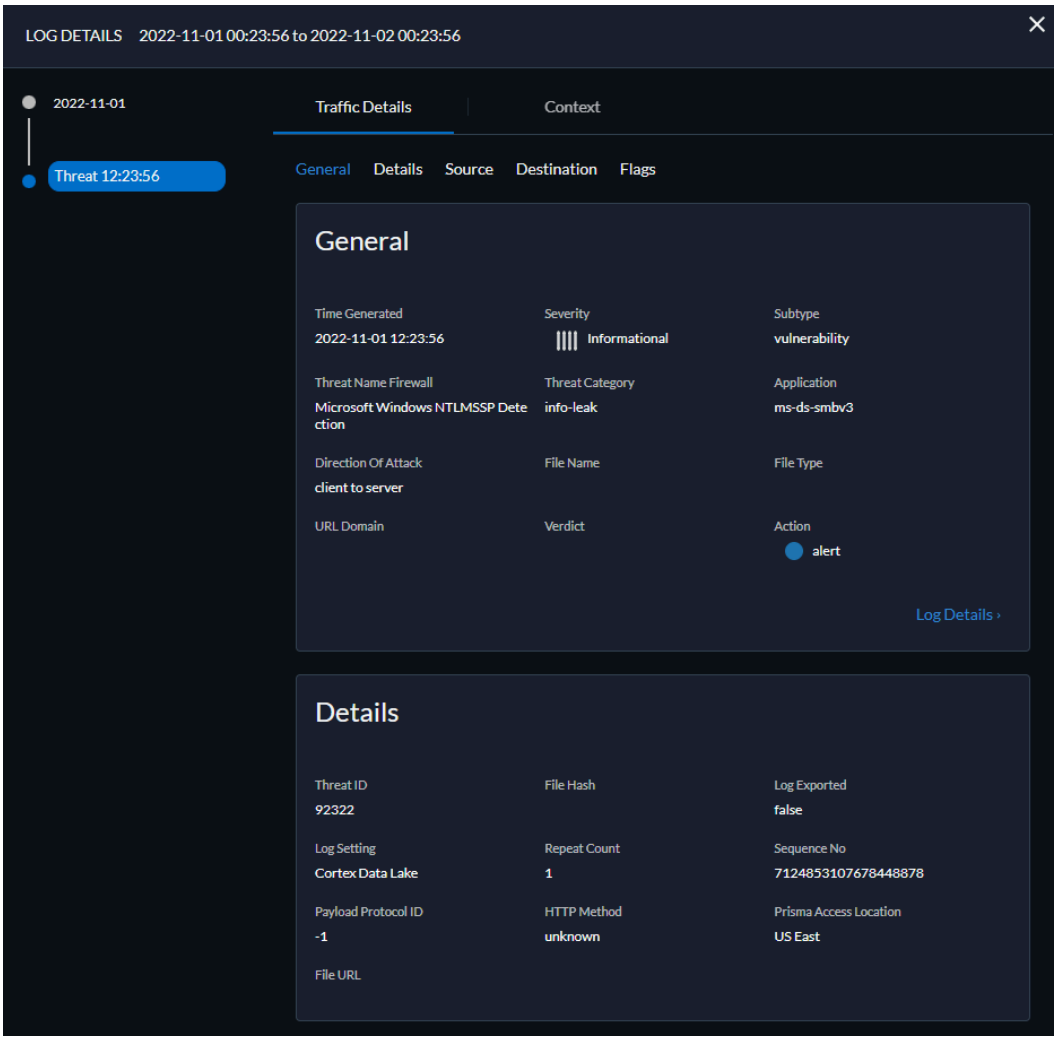
STEP 2 | Prisma Accessの**[Threat Category (脅威カテゴリ)]**または**[Subtype (サブタイプ)]**に基づいて脅威ログをフィルタリングします。

1. **[Incidents & Alerts (インシデントとアラート)]** > **[Log Viewer (ログ ビューアー)]**を選択します。
2. 検索するログの種類を **Threat(脅威)**に変更します。
3. アンチウイルス、アンチスパイウェア、または脆弱性防御プロファイル(それぞれ**antivirus**、**spyware**、**vulnerability**)で使用される脅威シグニチャのサブタイプのいずれかを使用するか、クエリ ビルダーを使用して脅威カテゴリに基づいて検索フィルターを作成します。たとえば、`sub_type.value = 'spyware'`を使用すると、スパイウェアと判断された脅威のログを表示できます。他のサブタイプを検索するには、上

©2025 Palo Alto Networks, Inc.

記の例のspywareをサポートされている別のサブタイプ(**vulnerability**または**spyware**)に置き換えます。`threat_category.value = 'info-leak'`というクエリを使うことで、情報漏えいの脆弱性など特定の脅威カテゴリに基づいて検索することもできます。使用できる有効なカテゴリの一覧については、脅威シグネチャのカテゴリを参照してください。必要に応じて、追加のクエリ パラメータ (重大度レベルやアクションなど) や日付範囲など、検索条件を調整します。

4. フィルターの組み立てが完了したら、クエリを実行します。
5. 結果からログ エントリを選択すると、ログの詳細が表示されます。



©2025 Palo Alto Networks, Inc.

6. 脅威カテゴリは、詳細ログ ビューの**[Details (詳細)]**ペインに表示されます。脅威に関するその他の関連詳細は、対応するウィンドウに表示されます。

STEP 3 | インライン クラウド解析(スパイウェア)により検知された脅威[カテゴリ]で脅威ログをフィルタリングします。

*Inline Cloud Analyzed HTTP Command and Control Traffic Detection*という脅威名で分類され、複数の脅威*ID*に関連付けられていた*HTTP*ベースの*C2*トラフィックが、固有の脅威*ID*に対応し、*Advanced Threat Prevention*による検出をより正確に説明するために、*3*つの固有の脅威名に分割されました。***Evasive HTTP C2 Traffic Detection** (脅威ID:89950)*、***Evasive Cobalt Strike C2 Traffic Detection** (脅威ID:89955*、*89956*、および*89957)*、***Evasive Empire C2 Traffic Detection** (脅威ID:89958)*。

*2023*年*12*月*11*日以前に生成された*HTTP*ベースの*C2*トラフィックログは、引き続き脅威名「*Inline Cloud Analyzed HTTP Command and Control Traffic Detection*」で分類されます。

1. **[Incidents & Alerts (インシデントとアラート)]** > **[Log Viewer (ログ ビューアー)]**を選択します。
2. 検索するログの種類を **Threat(脅威)**に変更します。
3. インライン クラウド解析(スパイウェア)専用に使用される脅威カテゴリ`threat_category.value = 'inline-cloud-c2'`を使用して、検索フィルターを作成します。特定のC2タイプに対応するThreat-IDの値を相互参照することで、検索をさらに制限できます。例えば、`threat_category.value = 'inline-cloud-c2' AND Threat ID = 89958`があり、この場合、89958はEvasive Empire C2トラフィックの脅威IDを示します。
4. ログ エントリを選択して、検出された C2 脅威の詳細を表示します。
5. 脅威カテゴリは、ログ詳細の**[General (全般)]**ペインに表示されます。インラインクラウド解析を用いて検知されたC2脅威は、脅威カテゴリがinline-cloud-c2となっています。**[Details (詳細)]**ペインの[Threat **ID** (脅威ID]の値を相互参照して、検出された特定のタイプのC2を判別できます。

STEP 4 | インライン クラウド解析(脆弱性)により検知された脅威[カテゴリ]で脅威ログをフィルタリングします。

1. **[Incidents & Alerts (インシデントとアラート)]** > **[Log Viewer (ログ ビューアー)]**を選択します。
2. 検索するログの種類を **Threat(脅威)**に変更します。
3. インライン クラウド解析(脆弱性)専用に使用される脅威カテゴリ`threat_category.value = 'inline-cloud-exploit'`を使用して、検索フィルターを作成します。
4. ログ エントリを選択すると、検出されたコマンド インジェクションおよびSQLインジェクションの脆弱性の詳細が表示されます。インライン エクスプロイト(SQLイン

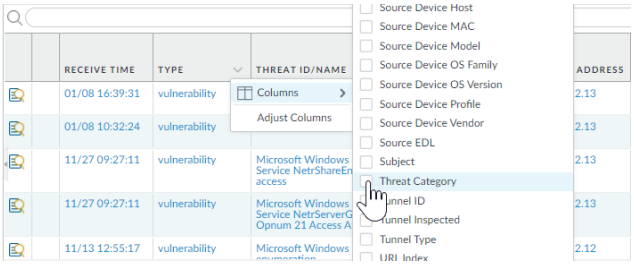
 ©2025 Palo Alto Networks, Inc.

ジェクション)脅威のIDは99950ですが、インライン エクスプロイト(コマンドインジェクション)脅威のIDは99951です。

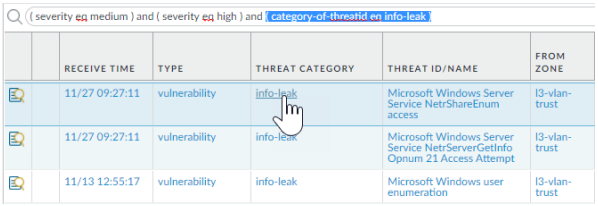
脅威ログの確認(NGFW (Managed by PAN-OS or Panorama))

脅威カテゴリで脅威ログをフィルタリングします。

1. **Monitor (監視) > Logs (ログ) >** 選択します。
2. Threat Category (脅威カテゴリ) 列を追加し、ログ エントリ毎に脅威カテゴリを閲覧できるようにします。



3. 脅威カテゴリに基づいてフィルタリングする方法：
   - ログ クエリ ビルダーを使用して Threat Category (脅威カテゴリ) の **Attribute (属性)** を持つフィルタを追加し、**Value (値)** フィールドに Threat Category (脅威カテゴリ) を入力します。
   - いずれかのログ エントリの Threat Category (脅威カテゴリ) を選択し、そのカテゴリをフィルターに追加します。



脅威シグネチャの種類で脅威ログをフィルタリングします。

1. **Monitor (監視) > Logs (ログ) >** を選択します
2. 各ログ エントリの脅威シグニチャ カテゴリを表示できるように、**[Type (タイプ)]**列が存在しない場合は追加します。
3. シグニチャの種類に基づいてフィルタリングするには、次の手順を実行します。
   - ログ クエリ ビルダーを使用して、脅威シグニチャ カテゴリの**[Attribute (属性)]**を持つフィルターを追加し、**[Value (値)]**フィールドに脅威シグニチャのタイプを入力します。脆弱性、ウイルス、およびスパイウェアから選択できます。これらは、脆弱性防御、アンチウイルス、およびアンチスパイウェアのセキュリティ プロファイルで処理されるシグニチャに対応します。
   - フィルターにその脅威シグニチャ タイプを追加するには、任意のログ エントリの**[Type (タイプ)]**を選択します。フィルターと脅威シグネチャ タイプを使用して、クエリを手動で作成することもできます。

©2025 Palo Alto Networks, Inc.

インライン クラウド解析(スパイウェア)により検知された脅威[カテゴリ]で脅威ログをフィルタリングします。

*Inline Cloud Analyzed HTTP Command and Control Traffic Detection*という脅威名で分類され、複数の脅威*ID*に関連付けられていた*HTTP*ベースの*C2*トラフィックが、固有の脅威*ID*に対応し、*Advanced Threat Prevention*による検出をより正確に説明するために、*3*つの固有の脅威名に分割されました。***Evasive HTTP C2 Traffic Detection** (脅威ID:89950)*、***Evasive Cobalt Strike C2 Traffic Detection** (脅威ID:89955、89956、および89957)*、***Evasive Empire C2 Traffic Detection** (脅威ID:89958)*。

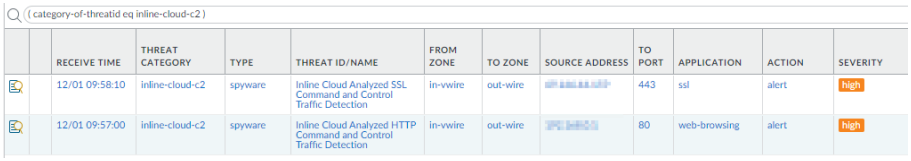
更新コンテンツをインストールしない場合や、*2023*年*12*月*11*日(コンテンツ更新のリリース日)以前に生成された*HTTP*ベースの*C2*トラフィックログを確認している場合は、すべての*HTTP*ベースの*C2*トラフィックは引き続き脅威名「*Inline Cloud Analyzed HTTP Command and Control Traffic Detection*」で分類されます。

1. **[Monitor (監視)]** > **[Logs (ログ)]** > **[Threat (脅威)]**を選択します。脅威の特定の特性に基づいてログをフィルタリングできます。次の例を考えてみてください。
   - `(category-of-threatid eq inline-cloud-c2)`でフィルタリングすると、Advanced Threat Preventionのインライン クラウド解析メカニズムを使用して解析されたC2脅威に関するログが表示されます。
   - 特定のC2タイプに対応するThreat-IDの値を相互参照することで、検索をさらに制限できます。例えば、`(category-of-threatid eq inline-`

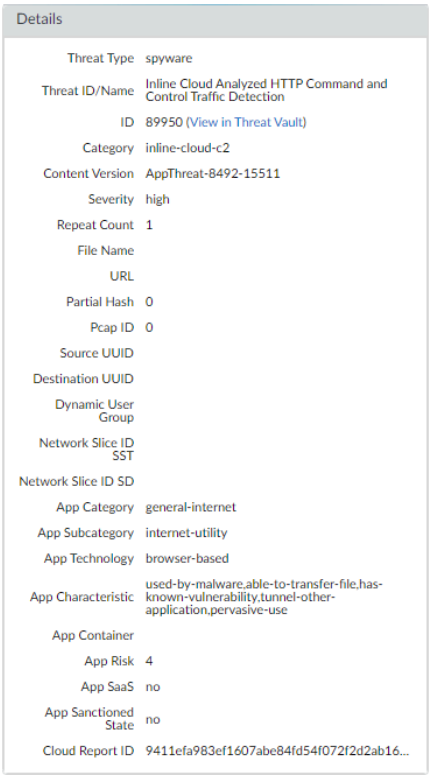
©2025 Palo Alto Networks, Inc.

`cloud-c2 )`や`(name-of-threatid eq 89958)`があります。この場合、89958はEvasive Empire C2トラフィックの脅威IDを示します。

- `(local_deep_learning eq yes)`でフィルタリングすると、Advanced Threat Preventionのローカル ディープ解析メカニズムを使用して解析された脅威のログが表示されます。

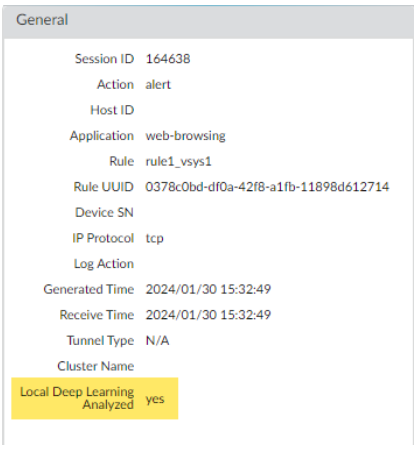


2. ログ エントリを選択して、検出された C2 脅威の詳細を表示します。
3. 脅威 **Category** は、詳細ログ ビューの **Details** ペインの下に表示されます。インライン クラウド解析を用いて検知されたC2脅威は、脅威カテゴリがinline-cloud-c2となっています。脅威**ID**の値を相互参照して、検出された特定のタイプのC2を判別できます。



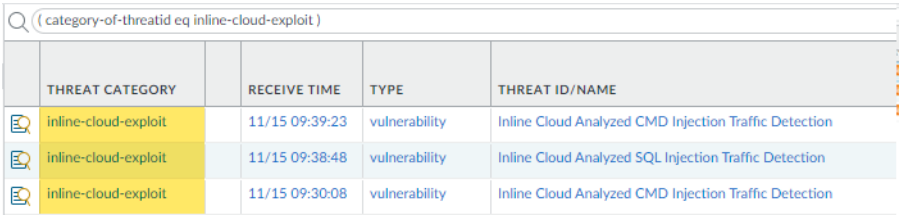
4. ローカル ディープ ラーニングを使用して脅威が解析された場合は、**[Local Deep Learning Analyzed (**ローカル ディープ ラーニングによる解析済み**)]**フィールドに「はい」と表示されます。

 ©2025 Palo Alto Networks, Inc.

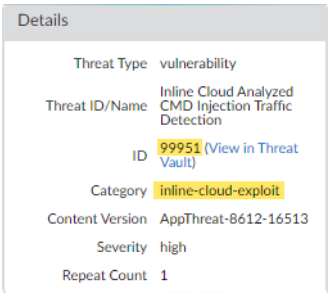


インライン クラウド解析を使用して検出された脆弱性の悪用(脆弱性)について、ファイアウォール上のアクティビティを監視します。

1. **[Monitor (監視)] > [Logs (ログ)] > [Threat (脅威)]**を選択し、`(category-of-threatid eq inline-cloud-exploit)`でフィルタリングすると、Advanced Threat Preventionのインライン クラウド解析メカニズムを使用して解析されたログが表示されます。インライン エクスプロイト(SQLインジェクション)脅威のIDは99950ですが、インライン エクスプロイト(コマンドインジェクション)脅威のIDは99951です。



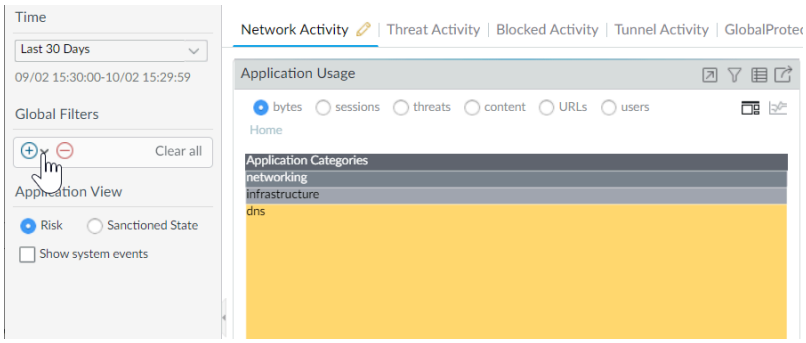
2. ログ エントリを選択すると、脆弱性の悪用の詳細が表示されます。
3. 脅威 **Category** は、詳細ログ ビューの **Details** ペインの下に表示されます。インライン クラウド解析を用いて検知された脆弱性の悪用は、脅威カテゴリがinline-cloud-exploitとなっています。



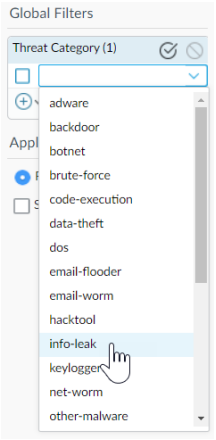
 ©2025 Palo Alto Networks, Inc.

脅威カテゴリに基づいて ACC アクティビティをフィルタリングします。

1. **ACC** を選択し、脅威カテゴリをグローバルフィルターとして追加します。



2. 脅威カテゴリを選択し、すべての ACC タブをフィルタリングします。



©2025 Palo Alto Networks, Inc.

Advanced Threat Preventionレポートの表示

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

Advanced Threat PreventionレポートはThreat Vault APIを通じて利用可能で、詳細な解析と検出情報のほか、トランザクション、セッション、その他の関連プロセスに関する情報も提供します。レポートには、ファイルを処理したファイアウォールで構成されたセッション情報と、JSON形式のファイルの解析詳細に基づいて、次の表に示す情報の一部またはすべてが含まれます。

*NGFW*は*PAN-OS*を通じてレポートに直接アクセスすることはしません。そのため、脅威ログに関連付けられた*cloud_reportid*を参照し、*Threat Vault API*を使用してレポートを検索および取得する必要があります。

*Prisma Access*の場合(Strata Cloud Manager経由)、レポートはログ ビューアーで表示できます(脅威ログの表示)。生成された*Advanced Threat Prevention*レポートを含むログ エントリには、***[Cloud ReportID (*クラウドレポート*ID)]***列の下のレポート*ID*値の横にダウンロード リンクがあります。

レポートの見出し	詳説
General Information	脅威を処理したファイアウォール/セキュリティ プラットフォームに関する情報が含まれます。 • 高度な脅威レポート データを含むクラウド レポートID番号。 • レポートの作成中に生成された可能性のあるエラー メッセージ。
PAN-OS情報	脅威を処理したファイアウォール/セキュリティ プラットフォームに関する情報が含まれます。 • ファイアウォール インターフェース(IPv4/IPv6)

©2025 Palo Alto Networks, Inc.

レポートの見出し	詳説
	• コンテンツ パッケージ バージョン • ファイアウォールのホスト名 • ファイアウォール モデル • シリアル番号 • PAN-OS バージョン
Session information [セッション情報]	脅威を転送したファイアウォール/セキュリティ プラットフォームを通過したトラフィックに基づくセッション情報が含まれます。 以下のオプションを使用できます。 • ソースIP • 送信元ポート • 宛先IP • Destination port • セッション ID • セッション タイムスタンプ • ペイロード タイプ
トランザクション データ	トランザクション データはペイロードの詳細の概要を提供し、検出サービス レポートを含みます。 以下のオプションを使用できます。 • トランザクションID • ペイロードのSHA256ハッシュ
検出サービスの結果	Advanced Threat Preventionクラウドによって脅威解析が実行されると、このセクションには解析結果を示すエントリが含まれます。これには、使用されたMITRE ATT&CK®分類手法とペイロードの詳細も提供する検出サービス レポートが含まれます。 Empire C2フレームワークのコマンド アンド コントロール検出では、追加のコンテキスト情報が表示されます。これには、別々のセッションで発生する攻撃のステージング フェーズとコマンド フェーズ(エクスプロイト後)の両方から生成されたレポートが含まれます。 以下の情報エントリが利用可能です。 • 攻撃の説明 - C2攻撃の性質を説明します。

©2025 Palo Alto Networks, Inc.

レポートの見出し	詳説
	• 攻撃の詳細 - Empire C2攻撃のフェーズを示し、サーバーとクライアント間のやり取りについて説明します。 • 攻撃の証拠 - 既知のEmpire C2と一致する動作とアクションを一覧表示します。 *Empire*ベースの*C2*は、固有の脅威*ID 89958*を持つ、***Inline Cloud Analyzed HTTP Command and Control Traffic Detection***解析エンジンに含まれるサブモジュール検出器を使用して検出されます。

©2025 Palo Alto Networks, Inc.

Monitor Blocked IP Addresses（ブロックされた IP アドレスのモニター）

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

ファイアウォールは、自身がブロックしている送信元 IP アドレスのブロックリストを維持します。ファイアウォールが送信元 IP アドレスをブロックする際（次のいずれかのポリシールールを設定する際など）、パケットが CPU あるいは次のパケット バッファ リソースを使用する前に、ファイアウォールがハードウェア内のそのトラフィックをブロックします。

- アクションが **Protect (保護)** である分類化 DoS 保護ポリシールール（新規セッションのフラッド攻撃に対する DoS プロテクションの設定に示されている通り、分類化 DoS 保護プロファイルに関連する分類化 DoS 保護ポリシーは、そのインバウンド接続が送信元 IP アドレス、宛先 IP アドレス、あるいは送信元および宛先 IP アドレスのペアにマッチすることを指定します）
- 脆弱性保護プロファイルを使用するセキュリティポリシー

ハードウェアIPアドレスブロッキングは、PA-3200 Series、PA-5200 Series、PA-5400 Series(PA-5450を除く)、およびPA-7000 Series firewallsでサポートされています。

ブロックリストを表示したり、ブロックリスト上の IP アドレスについての詳細な情報を取得したり、ハードウェアおよびソフトウェアがブロックしているアドレスの数を確認したりできます。ブロックすべきだと判断した場合は、リストの IP アドレスを削除可能です。リストにあるアドレスについての詳細情報のソースは変更できます。また、ハードウェアが IP アドレスをブロックする期間も変更できます。

ブロックリストのエントリを表示します。

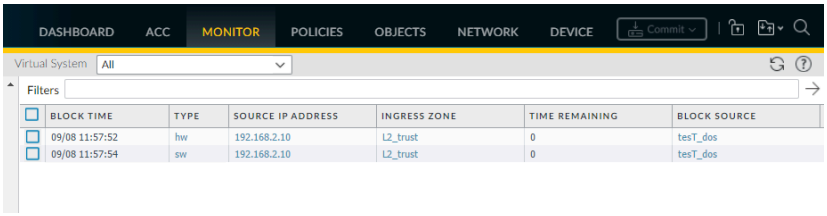
1. **Monitor (監視) > Block IP List (ブロック IP リスト)** を選択します。

   ブロックリストの各エントリの Type (タイプ) 列は、ハードウェア（hw）とソフトウェア（sw）のどちらによってブロックされたのかを示します。
2. 画面下部の表示を確認します：
   - ファイアウォールがサポートする、ブロックされた IP アドレスの数のうち **Total Blocked IPs (ブロックされた IP の合計)** カウント。
   - ファイアウォールが使用したブロックリストの割合。
3. 表示されたエントリをフィルタリングするには、列の値を選択(**[Filters (フィルター)]** フィールドにフィルターが作成されます)し、[Apply Filter (フィルターを適用)]しま

©2025 Palo Alto Networks, Inc.

す(→)。そうしない場合、ファイアウォールは最初の 1,000 件のエントリを表示します。

4. **Page (**ページ**)** 番号を入力するか、画面下部にある矢印をクリックして項目のページを進めます。
5. ブロックリストのアドレスの詳細情報を確認するには、ソース IP アドレスにカーソルを合わせて下向きの矢印リンクをクリックします。**[Who Is]**リンクをクリックすると、そのアドレスについてのNetwork Solutions Who Is情報が表示されます。



ブロックリストのエントリを削除します。

ブロックすべきでないと判断した *IP* アドレスがある場合は、エントリを削除します。その後、ファイアウォールにそのアドレスをブロックさせているポリシールールを修正します。

1. **Monitor (**監視**) > Block IP List (**ブロック **IP** リスト**)** を選択します。
2. 単一あるいは複数の項目を選択して **Delete (**削除**)** をクリックします。
3. （任意）**Clear All (**すべてクリア**)** を選択し、リストの全項目を削除します。

トラブルシューティングを行うために、ハードウェア IP アドレス ブロッキングを無効あるいは再度有効にします。

ハードウェア *IP* アドレス ブロッキングが無効になっていても、ファイアウォールは設定済みのソフトウェア *IP* アドレス ブロッキングをすべて実行できます。

```
> set system setting hardware-acl-blocking [enable | disable]
```

CPU およびパケット バッファのリソースを節約するために、ハードウェア *IP* アドレス ブロッキングは、*Palo Alto Networks* の技術サポートから無効にするよう求められない限り (トラフィック フローのデバッグを行っている際など)、有効な状態を保てるようにしてください。

©2025 Palo Alto Networks, Inc.

ハードウェアによってブロックされた IP アドレスがブロックリストを残す秒数を調整します（範囲は 1～3,600、デフォルトは 1）。

```
> set system setting hardware-acl-blocking duration <seconds>
```

ハードウェアのブロック能力を超過するリスクを減らすには、ソフトウェア ブロックリストの各エントリよりもハードウェア ブロックリストの期間を短く保ちます。

IP アドレスの詳細情報を探すデフォルトのウェブサイトを、Network Solutions Who Is から別のウェブサイトに変更します。

```
# set deviceconfig system ip-address-lookup-url <url>
```

ハードウェアおよびソフトウェアによってブロックされた 送信元 IP アドレスのカウントを確認します（例えば、攻撃の頻度を見るなど）。

ハードウェア ブロック表およびブロックリストの IP アドレス エントリの合計数を確認します（ハードウェアおよびソフトウェアによってブロック）。

```
> show counter global name flow_dos_blk_num_entries
```

ハードウェアによってブロックされたハードウェア ブロック表の IP アドレス エントリの数を確認します。

```
> show counter global name flow_dos_blk_hw_entries
```

ソフトウェアによってブロックされたブロックリスト上の IP アドレス エントリの数を確認します。

```
> show counter global name flow_dos_blk_sw_entries
```

PA-7000 Series ファイアウォールのスロット毎のブロックリスト情報を表示します。

```
> show dos-block-table software filter slot <slot-number>
```


©2025 Palo Alto Networks, Inc.

脅威シグネチャの詳細を把握

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

ファイアウォールの脅威ログは、脅威シグネチャ(アンチウイルス、アンチスパイウェア、および脆弱性防御のセットアップ)に基づいてファイアウォールが検知した脅威をすべて記録し、ACCがネットワークの上位の脅威についての概要を表示します。ファイアウォールが記録する各イベントには、関連する脅威シグネチャを特定する ID が含まれています。

脅威ログあるいは ACC エントリと共に見つかった脅威 ID を使用すれば、次のことが可能になります。

- 脅威シグネチャがセキュリティ ポリシーの例外として設定されているかどうか簡単に確認する(脅威例外の作成)。
- 特定の脅威に関する最新の Threat Vault の情報を見つける。Threat Vault はファイアウォールと統合されているため、ファイアウォール コンテキストで直に脅威に関する詳細を確認したり、新しいブラウザ ウィンドウで Threat Vault 検索を起動して、ファイアウォールがログに記録した脅威を確認したりすることができます。

シグネチャが無効化されている場合、新しいシグネチャに対してシグネチャ *UTID* が再利用される場合があります。

コンテンツ更新のリリースノートを読み、新規および無効化されたシグネチャに関する通知をご確認ください。対象のシグネチャが検出する行為を攻撃者が利用しなくなっている場合、対象のシグネチャが誤って許可するケースが多い場合、あるいは対象のシグネチャが他の類似のシグネチャと統合された（シグネチャの最適化）場合に、シグネチャが無効化されることがあります。

STEP 1 | ファイアウォールが Threat Vault に接続されていることを確認します。

Device（デバイス） > **Setup**（設定） > **Management**（管理）を選択し、**Logging and Reporting** （ロギングとレポート） 設定を編集して **Enable Threat Vault Access** （**Threat Vault** アクセスの有効化） を行います。Threat Vault へのアクセスはデフォルトで有効になっています。

STEP 2 | ファイアウォールが検出した脅威の脅威 ID を探します。

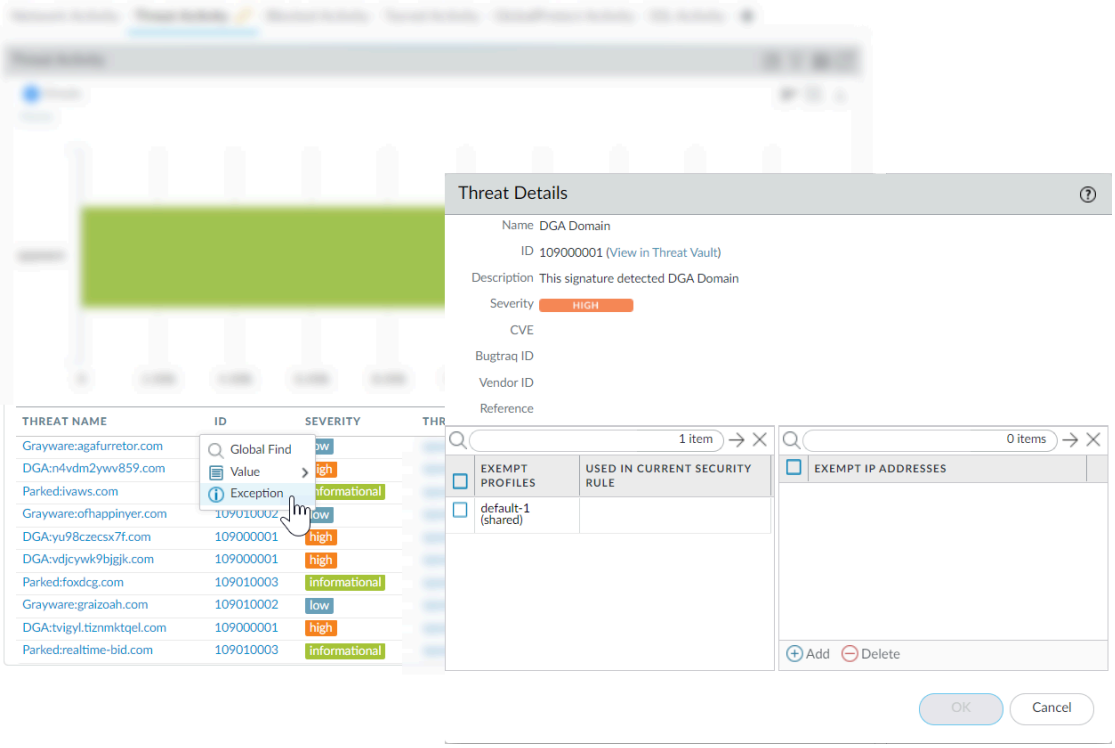
- 脅威シグネチャに基づいてファイアウォールが検知する各脅威イベントを表示するには、**Monitor (**監視**) > Logs (**ログ**) > Threat (**脅威**)**を選択します。脅威エントリの ID は ID 列の一覧で確認したり、ログ エントリを選択し、脅威 ID を含むログの詳細を表示して確認したりできます。

©2025 Palo Alto Networks, Inc.

- ネットワーク上の上位の脅威の概要を確認するには、**ACC** > **Threat Activity** (脅威アクティビティ) を選択し、Threat Activity (脅威アクティビティ) ウィジェットをチェックします。表示されている各脅威の脅威 IDが ID 列に表示されます。
- 脅威例外（つまり、その脅威シグネチャに対して定義されているデフォルトのアクションとは異なる方法でファイアウォールが脅威に対応）として設定できる脅威の詳細を表示するには、**Objects** (オブジェクト) > **Security Profiles** (セキュリティ プロファイル) > **Anti-Spyware/Vulnerability Protection** (アンチスパイウェア/脆弱性保護)を選択します。プロファイルを **Add** (追加) あるいは変更し、**Exceptions** (例外) タブをクリックして設定済みの例外を表示します。例外が設定されていない場合、脅威シグネチャに基づいてフィルタリングしたり、**Show all signatures** (すべてのシグネチャを表示) を選択したりできます。

STEP 3 | **Threat Name** (脅威名) あるいは脅威 **ID** にカーソルを合わせてドロップダウンリストを開き、**Exception** (例外) をクリックし、脅威の詳細と、ファイアウォールがその脅威にどのように対処するよう設定されているのかを確認します。

例えば、ACC のチャートで上位の脅威に関する詳細を確認できます。



STEP 4 | その脅威に関する最新の **Threat Details** (脅威の詳細) を確認し、脅威 ID に基づいて Threat Vault 検索を起動します。

- 脅威の詳細表示には、脅威の最新の Threat Vault 情報、脅威を詳細に理解するために使用できるリソース、その脅威に関連する CVE が含まれています。
- Threat Vault 検索を新しいウィンドウで開き、Palo Alto Networks の脅威データベースに含まれている、この脅威シグネチャの最新情報を検索するには、**View in Threat Vault** (**Threat Vault** で表示) を選択します。

©2025 Palo Alto Networks, Inc.

STEP 5 | 脅威シグネチャがセキュリティポリシーの例外として設定されているかどうか確認します。

- **Used in current security rule (**現在のセキュリティルールで使用中**)** 列が空である場合、ファイアウォールは推奨されるデフォルトのシグネチャ アクション（ブロックやアラートなど）に基づいて脅威に対処しています。
- **Used in current security rule (**現在のセキュリティルールで使用中**)** 列のどこかにチェックマークがある場合、セキュリティポリシー ルールが **Exempt Profiles (**除外プロファイル**)** 設定に基づき、その脅威用のデフォルト以外のアクション（許可など）を適用するように設定されていることが分かります。

> ***Used in security rule column (***セキュリティルール列で使用中**)** では、セキュリティポリシー ルールが有効かどうかは判断できません。分かるのはセキュリティポリシー ルールに脅威例外が設定されているかどうかのみです。指摘されたセキュリティポリシー ルールが有効になっているかどうか確認するには、***Policies (***ポリシー**) > Security (***セキュリティ**)** を選択します。

STEP 6 | 脅威例外をフィルタリングする IP アドレスを **Add (**追加**)** するか、既存の **Exempt IP Addresses** （除外 **IP** アドレス） を表示します。

関連するセッションがマッチする送信元あるいは宛先 IP アドレスを持っている場合のみ脅威例外を適用するには、除外する IP アドレスを設定します。その他のあらゆるセッションについては、デフォルトのシグネチャ アクションが脅威に適用されます。

©2025 Palo Alto Networks, Inc.

脅威カテゴリに基づくカスタム レポートの作成

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced Threat Prevention (拡張機能サポート用)またはThreat Preventionライセンス

ファイアウォール上にカスタム レポートを作成して、取得および解析する属性または主要な情報に基づいてレポートを(オンデマンドで)生成したり、スケジュール設定(毎晩)したりできます。

脅威カテゴリに基づいてカスタム レポートを作成し、ファイアウォールが検出した特定のタイプの脅威についての情報を取得します。

1. **[Monitor (監視)]** > **[Manage Custom reports (カスタム レポートの管理)]**を選択し、新しいカスタム レポートを追加、あるいは既存のレポートを変更します。
2. カスタム レポートのソースとして使用する **Database (データベース)** を選択します。このケースでは、2 種類のデータベース ソース（サマリーデータベースおよび詳細ログ）のいずれかから **Threat (脅威)** を選択します。応答時間を短縮できるよう、サマリーデータベースのデータはレポート生成時に集約されます。詳細ログは生成により時間がかかりますが、各ログ エントリに関するすべてのデータを項目別に提供できます。
3. Query Builder (クエリ ビルダー) で、**Threat Category (脅威カテゴリ)** の属性を持つレポート フィルタを追加し、Value (値) フィールドで、レポートの基準にする脅威カテゴリを選択します。
4. 新しいレポート設定をテストするために **Run Now (今すぐ実行)** をクリックします。
5. **OK** をクリックしてレポートを保存します。

©2025 Palo Alto Networks, Inc.