データセンターの最良のセキュリティポリシー

Version 10.0 (EoL)

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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

Last Revised

November 2, 2020

Table of Contents

データセンター セキュリティポリシーのベストプラクティスのチェックリスト

非公開のソースコード、知的財産、センシティブな企業・顧客のデータなど、企業の最も価値の高い資産はデータセンター内にあります。顧客や従業員は、自身のデータの機密性・整合性を維持すること、そのデータを常に利用できる状態にすることを管理者に求めているため、データセンターの最良のセキュリティポリシーを実装し、データを保護して攻撃を防止することが重要です。攻撃者はネットワーク内部から攻撃することができ、認証情報を盗まれた提携企業や契約者が攻撃の元になることがあり、またネットワーク内に足がかりを得た攻撃者はデバイスからデバイスへと横方向に移動してネットワーク内部から攻撃を行えるため、ネットワークの境界を強化するだけでは不十分です。

Palo Alto Networks のプラットフォームをよく知っている場合は、よく整理されたこのチェックリストを使ってデプロイ前、デプロイ時、デプロイ後のデータセンター セキュリティポリシーのベストプラクティスを実装することで、時間を短縮できます。ポリシールールおよびセキュリティ プロファイルの設定方法を含めて、各セクションには完全なデータセンターの最良のセキュリティポリシーのドキュメントや『PAN-OS 10.0管理者ガイド』の詳細な情報へのリンクが含まれています。

- データセンターの最良のデプロイメントを計画
- データセンターのベストプラクティスをデプロイ
- デプロイ後のデータセンターのベストプラクティスに従う

データセンターの最良のデプロイメントを計画

戦略を立ててロールアウト計画を作成し、ベストプラクティスをデータセンターに実装する準備を行います。セキュリティのポジティブ エンフォースメントを採用（許可したいユーザーおよびアプリケーション トラフィックを許可し、それ以外の全てを拒否するルールを作成）してゼロ トラストアーキテクチャを目指して作業を行います。

STEP 1 | ゴール設定。

- データセンター ネットワークの将来の理想的な形を定義し、明確な目標に向けて作業を行い、目標を達成できたかどうか分かるようにします。
- 接続を開始する各領域から来るトラフィック フローを保護します：
  1. データセンター内へと流れるローカルのユーザートラフィック。
  2. インターネットからデータセンターへと流れるトラフィック。
  3. データセンターからインターネットへと流れるトラフィック。
  4. データセンター内の VM あるいは サーバー間を流れるトラフィック（イントラ データセンター East-West トラフィック）。
- 未知のユーザー、アプリケーション、トラフィックをデータセンター内で許可しないでください。
- 各データセンター全体に対して複製· 適用できる、標準的なスケーリングできる設計を行います。

STEP 2 | IT/サポート、セキュリティ部門、エンジニアリング、法務、経理、人事などのデータセンターへのアクセスが必要なグループと協力し、アクセス戦略を立てます。

- アクセスが必要なユーザー、ユーザーがアクセスしなければならないアセットを判断します。これを把握することで、アクセス レベルの要件に基づいてユーザーグループを作成し、ユーザーグループ毎に効果的なセキュリティポリシールールを設計できるようになります。
- データセンター内で許可（sanction）したいアプリケーションを判断します。攻撃の入り口を減らすために、正当なビジネス上の目的を持つアプリケーションだけを許可してください。

STEP 3 | データセンターを評価して現在の状態を把握し、データセンターを将来の理想的な状態に変える計画を立てます。

- 次の項目を含めて、物理· 仮想環境およびアセットの一覧を作成します：
  - サーバー、ルーター、スイッチ、セキュリティデバイス、ロードバランサー、その他のネットワーク インフラストラクチャ。
  - 標準的および専有カスタム アプリケーション、およびそれらが通信するために使用するサービス アカウント。アプリケーションのリストと、許可したいアプリケーションのリストを照らし合わせてみてください。

    あなたの許可リストセキュリティポリシールールはそれらを許可し、デフォルトでは、それ以外のアプリケーションを拒否して攻撃の入り口を減らすことができますので、許可したいアプリケーションに焦点を当ててください。各アプリケーションをビジネス要件と照らし合わせます。アプリケーションに対応するビジネス要件がない場合、本当に許可すべきか検討してください。
  - 最初に保護すべき対象の優先順位を決めやすくなるよう、各アセットを評価します。「自社の特徴や強みを決定するものとは？」、「毎日の業務で利用できなくてはならないシステムとは？」、「このアセットを失ったらどうなるだろうか？」などを問いかけてみます。
- アプリケーション、ネットワーク、エンタープライズ設計者、ビジネスの代表者と協力してデータセンターのトラフィック フローの特徴をとらえ、典型的なベースラインのトラフィック負荷および

パターンを知ることで、通常時のネットワークの挙動を把握します。アプリケーション コマンドセンターウィジェットおよびトラフィック分析ツールを使用し、トラフィックのベースラインを把握してください。

STEP 4 | データセンターのセグメント化戦略を作成し、データセンター内に足がかりを得たマルウェアが横方向に移動して他のシステムを感染させるのを防ぎます。

- ファイアウォールをセグメント化ゲートウェイとして使用し、データセンター トラフィックおよびシステムに対する可視性を確保し、誰がどのアプリケーションを使ってどのデバイスにアクセスできるのか、細かく制御できるようにします。仮想的でないサーバーは物理的なファイアウォールを使用して、仮想的なネットワークは VM-Series ファイアウォールを使用してセグメント化および保護します。
- ゾーン、ダイナミック アドレス グループ、App-ID、User-IDなどのファイアウォールの柔軟なセグメント化ツールを使用し、センシティブなサーバーやデータを保護する細かなセグメント化戦略を立てます。
- 類似の機能を果たす各アセットをグループ化し、同じセグメント内で同じセキュリティ レベルを求めます。
- アプリケーションサーバー層（通常、サービス チェーンは Web サーバー層、アプリケーション サーバー層、データベースサーバー層で構成されます）をセグメント化し、ファイアウォールを構成するサーバー層使って各層間のトラフィックを制御・検査することで、データセンター アプリケーションをセグメント化します。
- データセンター内で SDN ソリューションを使用し、アジャイルなバーチャル インフラを構成してリソース使用率を最大化しつつ、自動化やスケーリングを容易にできるようにすることを検討してください。

STEP 5 | ベストプラクティスの方法論を採用し、すべてのデータセンター トラフィックを検査して完全な可視性を確保し、攻撃の入り口を減らし、既知および未知の脅威を防止する計画を立てます。

- すべてのデータセンターのネットワーク トラフィックが見える位置に物理あるいは仮想ファイアウォールを配置します。
- ファイアウォールの強力なツールセットを活用し、特定のユーザーグループに紐付いた、セキュリティ プロファイルによって保護されるアプリケーション ベースのセキュリティポリシールールを作成します。未知のファイルをWildFireに転送し、復号化をデプロイして暗号化されたトラフィックに潜む脅威がデータセンターに入らないようにします。
- GlobalProtectを内部モードでゲートウェイとして使用し、データセンターのアクセスを制御します。
- ユーザーを認証して不正なアクセスを防ぎ、特に契約者、提携企業、データセンターにアクセスする必要があるその他のサードパーティによるセンシティブなアプリケーション、サービス、サーバーへのアクセスに対して多要素認証を構成します。
- Panoramaを使ってファイアウォールを一元的に管理することで、物理・仮想環境全体でポリシーを一貫した形で適用し、確保した可視性を集約できます。
- データセンターが複数ある場合は、テンプレートおよびテンプレート スタックを再利用して複数の場所全体にかけて一貫した形でセキュリティポリシーを適用します。

STEP 6 | まずはビジネスやネットワークで発生する可能性の高い脅威に焦点を当て、最も価値の高い資産を最初に保護することで、ベストプラクティスのデプロイメントを段階的に導入していきます。

すべてのデータセンターのユーザー、アプリケーション、デバイス、トラフィック フローを考慮してからそれを対象にしたデータセンターの最良のセキュリティポリシーを作成するというのは、一度に行おうとすると大変な作業のように感じるかもしれません。しかし、最も価値の高い資産を最初に保護し、長期間にわたる段階的な実装を計画することで、スムーズかつ現実的な方法で「最善を祈る」

セキュリティポリシーからデータセンターの最良のセキュリティポリシーへと移行していき、アプリケーション、ユーザー、コンテンツを安全に使用できる状態にできます。

データセンターのベストプラクティスをデプロイ

セキュリティ プロファイル、復号化プロファイル、セキュリティポリシールール、認証ポリシールール、復号化ポリシー ルールを作成する際、データセンターのベストプラクティスを実装します。

セキュリティ、認証、および *DoS* ポリシールールについては、*Panorama* あるいは外部サービスへのログ転送を構成し、通知を使用しつつログを一元化し、閲覧や分析を行いやすくします。

- グローバルデータセンターのオブジェクト、ポリシー、およびアクション
- ユーザーデータセントラフィックポリシー
- インターネットからデータセンターへのトラフィックポリシー
- データセンターからインターネットへのトラフィックポリシー
- データセンター内トラフィックポリシー
- データセンター セキュリティポリシーのルールベースの順序

グローバルデータセンターのオブジェクト、ポリシー、およびアクション

カスタムアプリケーションを使用している場合は、それを保護できていることを確認してください。セキュリティプロファイルと復号化プロファイルを設定し、すべてのデータセンターエンドポイントにCortex XDRエージェントをインストールします。

- カスタム アプリケーション
- セキュリティ プロファイル
- 復号プロファイル
- トラフィックブロッキングルール
- エンドポイントへのCortex XDRエージェントのインストール

STEP 1 | データセンター アプリケーションのインベントリに専有のカスタム アプリケーションが含まれる場合、それらに使用するカスタム アプリケーションを作成し、セキュリティポリシーでそれらを指定できるようにします。

STEP 2 | 強固なデータセンターの最良のセキュリティ プロファイルを構成し、データセンターのネットワークを妨げる脅威を防止します。

- 事前定義済みのプロファイルをクローンして Action（アクション）および WildFire Action（アクション）列の imap、pop3、smtp デコーダーの値を **reset-both**に変更することで、最良のアンチウイルス プロファイルを構成します。
- 事前定義済みの厳格なプロファイルをクローンして最良のアンチスパイウェア プロファイルを構成します。**Rules**（ルール）タブで、ログを取る重大度 medium（中）、high（高）、critical（重要）のトラフィックに対する単一パケット キャプチャを有効化します。（ログを取らないトラフィックについては、パケット キャプチャを有効化せずに別のプロファイルを適用します。）

  DNS Signatures（DNS シグネチャ）タブで、ファイアウォールが DNS クエリの発信者を把握できない場合（通常、ファイアウォールが DNS サーバーの north にあたる場合）の DNS クエリに対する**Action**（アクション）を**sinkhole**（シンクホール）に変更し、感染したホストを特定できるようにします。DNS シンクホールは、疑わしいドメインにアクセスしようと試みる侵入された可能性

があるホストを特定・追跡し、それらが対象のドメインにアクセスできないようにします。シンクホール対象のトラフィックに対して拡張パケット キャプチャを有効化してください。

- 事前定義済みの厳格なプロファイルをクローンして各ルールの**simple-client-informational**および**simple-server-informational**以外のパケット キャプチャ設定を**single-packet**に変更することで、ベストプラクティスの脆弱性保護プロファイルを構成します。ファイアウォールが大量の脆弱性の脅威を特定し、それによってパフォーマンスが影響を受ける場合は、重大度の低いイベントのパケット キャプチャを無効化します。
- 事前定義済みの厳格なファイルブロッキングプロファイルは、最良のプロファイルです。重要なアプリケーションをサポートするために厳格なプロファイルがブロックするすべてのファイル形式をブロックできない場合（データセンター内で使用するファイル形式は**Monitor**（監視）> **Logs**（ログ）> **Data Filtering**（データ フィルタリング）にあるデータ フィルタリング ログで特定でき、厳格なプロファイルをクローンして必要に応じて変更を加えます。ファイルが双方向に進まなくて良い場合は**Direction**（方向）設定を使用し、そのファイル形式を一方向に制限します。
- 事前定義済みのWildFire 分析プロファイルがベストプラクティスのプロファイルになります。WildFire は未知の脅威および advanced persistent threats（APT）に対して最も優れた防御を提供します。

STEP 3 | 強固なデータセンターの最良の復号化プロファイルを構成し、未知のトラフィックがデータセンターに入るのを防ぎます。

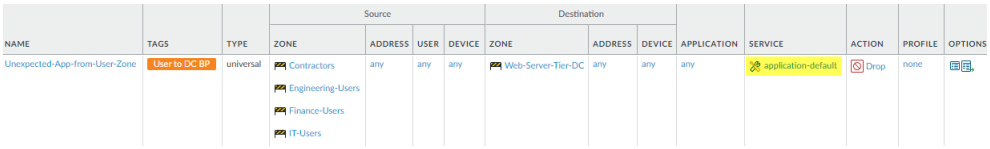
- CRL/OCSP チェックを行い、SSL 復号化の際に必ず証明書の有効性を検証するようにします。
- SSL プロトコル設定**Min Version**（最低バージョン）を**TLSv1.2**に、**Max Version**（最大バージョン）を**Max**（最大）に設定し、**SHA1**認証アルゴリズムのチェックを外します。（TLSv1.2 を選択すると、弱い 3DES および RC4 暗号化アルゴリズムのチェックが自動的に外れます。）TLSv1.3をサポートしているトラフィックには、TLSv1.3を使用してください（多くのモバイルアプリケーションが証明書のピンニング（ピン留め）を使用していますが、これはTLSv1.3の使用時に復号化を妨害します。そのため、このようなアプリケーションにはTLSv1.2を使用してください）。
- SSL 転送プロキシ：**Server Certificate Verification**（サーバー証明書検証）は、証明書が失効したセッション、信頼できない発行者、未知の証明書ステータスをブロックし、証明書の拡張を制限します。**Unsupported Mode Checks**（サポートされていないモード チェック）は、サポートされていないバージョン、Cipher Suite、クライアント認証を伴うセッションをブロックします。**Failure Checks**（失敗チェック）は、利用できないセッションがユーザーエクスペリエンス（ブロックすることでユーザーエクスペリエンスが低下するおそれがある）と危険な可能性がある接続のトレードオフになる場合、セッションをブロックします。このトレードオフを考慮しなければならない場合は、デプロイメントで利用できる復号化リソースを増やすことも検討してください。
- SSL インバウンド インスペクション：**Unsupported Mode Checks**（サポートされていないモード チェック）は、サポートされていないバージョンやアルゴリズムを持つセッションをブロックします。**Failure Checks**（失敗チェック）には SSL 転送プロキシと同様のトレードオフがあります。
- SSH プロキシ：**Unsupported Mode Checks**（サポートされていないモード チェック）は、サポートされていないバージョンやアルゴリズムを持つセッションをブロックします。**Failure Checks**（失敗チェック）には SSL 転送プロキシと同様のトレードオフがあります。
- TLSv1.3トラフィックを除いて、規制、コンプライアンスルール、またはビジネス上の理由から復号化を行わないトラフィックには、No Decryption（復号化なし）プロファイルを適用してください（TLSv1.3は証明書情報を暗号化するため、ファイアウォールは証明書情報に基づくトラフィックをブロックできません）。期限切れ証明書、信頼できない発行者を伴うセッションをブロックします。

STEP 4 | 悪意があることが分かっている、あるいはビジネスにとって不要なトラフィックを拒否するために、トラフィック ブロック ルールを設定します。

ブロック ルールのロギングおよび監視により、ネットワーク上に存在していることを知らなかったユーザーやアプリケーションを明らかにしたり、それらが正当なものか攻撃を示唆するのか把握したりできます。セキュリティポリシーのルールベース内のルールの順序は、シャドーイング（トラフィックをマッチさせたいルールにマッチする前に許可あるいはブロック ルールにマッチするトラ

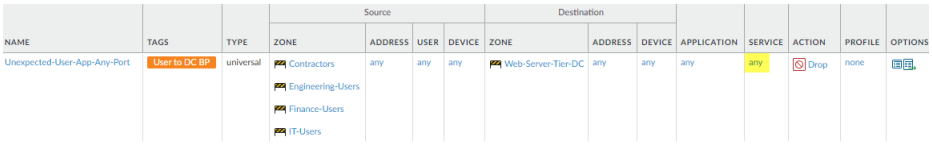
フィック）を防止するうえで重要です。一部のルールはほぼ同じですが、標準および標準的でないポートや、ユーザーアプリケーションおよび他のソースからのアプリケーション毎に個別のレポーティングが可能です。各ルールに対して、**Actions**（アクション）タブで**Log at Session End**（セッション終了時にログを記録）を設定し、Log Forwarding（ログ転送）をセットアップしてルールの違反を追跡・分析します。

- **application-default**ポート上でユーザーゾーンからのすべてのアプリケーションをブロックします。ユーザーゾーンからの正当なアプリケーションのトラフィックを許可するルールの後にこのルールを配置し、標準的なポート上の既知あるいは未知のユーザーアプリケーションを特定します。



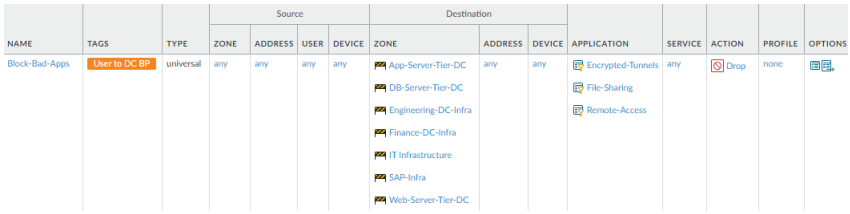
NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-User-Zone	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

- **any**（すべて）のポート上でユーザーゾーンからのすべてのアプリケーションをブロックし、標準的でないポートを使用しようとするユーザートラフィックを捕捉します。標準的でないポート上の既知あるいは未知のユーザーアプリケーションを特定するために、前述の**application-default**ブロック ルール（カスタム アプリケーションあるいは回避的なアプリケーションが可）の後にこのルールを配置してください。



NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-User-App-Any-Port	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

- 回避的および頻繁にエクスプロイトされるアプリケーションやビジネスにとって不要なアプリケーションなど、データセンターに決して入れたくないアプリケーションをブロックします。例えば、**Filesharing**アプリケーションフィルタが他のすべてのファイル共有アプリケーションをブロックする前に、制限付きのファイル共有アプリケーションを許可するために、このルールをアプリケーション許可ルールの後に配置してください。

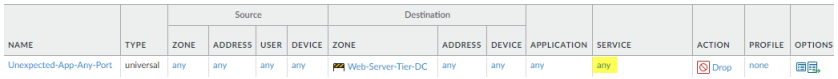


NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block-Bad-Apps	User to DC BP	universal	any	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	

- **application-default**ポート上で**any**（すべて）のゾーンから来るあらゆるアプリケーションをブロックし、標準的なポート上の予期せぬアプリケーションを特定します。ルールのマッチが発生すると、潜在的な脅威あるいは許可ルールの修正が必要なアプリケーションの変更を示している場合があります。このルールは、アプリケーション許可ルールおよび先行するブロックルールの後に配置します。

NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-Any-Zone	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

- **any**（すべて）のポート上であらゆるゾーンからのすべてのアプリケーションをブロックし、標準的でないポート上の予期せぬアプリケーションを特定します。unknown-tcp、unknown-udp、non-syn-tcp トラフィックは許可しないでください。このルールは、アプリケーション許可ルールおよび先行するブロックルールの後に配置します。

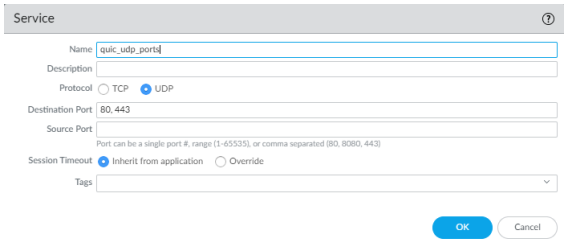


NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-Any-Port	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

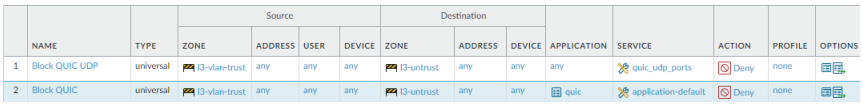
- あらゆるポート上でアプリケーションを実行しようとする未知のユーザーをブロックし、未知のユーザー（User-ID のカバー範囲外あるいは攻撃者）を発見して感染したデバイス（プリンター、

カードリーダー、カメラなどの組み込みデバイスを含む）を特定します。このルールは、アプリケーション許可ルールおよび先行するブロックルールの後に配置します。

- ビジネス上の理由で暗号化されたブラウザのトラフィックを許可する場合を除き、潜在的に悪意のある不要なトラフィックをブロックするだけでなく、クイックUDPインターネット接続（QUIC）プロトコルをブロックします。Chrome およびその他の一部のブラウザは TLS ではなく QUIC を使ってセッションを確立しますが、QUIC はファイアウォールが復号化できないプロプライエタリな暗号化を使用するため、危険があるトラフィックが暗号化されたトラフィックの状態でネットワークに侵入するおそれがあります。ブラウザにTLSの使用を強制するために、QUICアプリケーションとUDPポート80および443の両方をブロックしてください。まず、UDP ポート 80 および 443 を含むサービス（**Objects**（オブジェクト）> **Services**（サービス）を作成します。



サービスを使用して、QUIC をブロックする UDP ポートを指定します。2番目のルールで、ルールベース内の最初の2つのルールがQUICをブロックするように、QUICアプリケーションをブロックします:



STEP 5 | すべてのデータセンターのエンドポイントにCortex XDRエージェントをインストールし、マルウェアやエンドポイントに対するエクスプロイトを防止します。

Cortex XDRエージェントはすべてのエンドポイントを同じ方法で保護するため、データセンターのデプロイメントプロセスおよびマルウェア防止ポリシーのベストプラクティスは他のどのネットワーク領域でも同じになります。

ユーザーデータセンタートラフィックポリシー

データセンターへのアクセスが必要なユーザーの、セキュリティポリシー、認証ポリシー、および復号化ポリシーを設定します。

- ユーザーセキュリティポリシールール
- ユーザー認証ポリシールール
- ユーザー復号化ポリシールール

STEP 1 | ユーザートラフィック用のアプリケーション許可リストセキュリティポリシールールを作成し、適切なアクセスを許可します。

ユーザーアクセス用の許可ルールはルールベースの先頭、ブロック ルールよりも前に配置し、正当なトラフィックを誤ってブロックしないようにします。各ルールに対し、**Actions**（アクション）タブで**Log at Session End**（セッション終了時にログを記録）を設定し、ログ転送をセットアップしてルールの違反を追跡・分析します。

- 社内 DNS サーバーに対する従業員ユーザーアクセスを有効化します。ユーザーはログイン前にDNSにアクセスするため、このルールは任意のユーザーを許可します。このルールは送信元ゾー

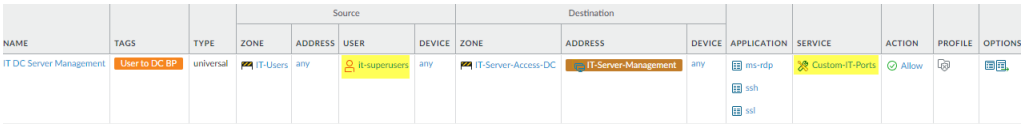
ン、宛先サーバー、アプリケーションを強固に制御し、セキュリティ プロファイルをトラフィックに適用します。

インターネット ゲートウェイにて外部 *DNS* サーバーへのアクセスをブロックし、*DNS* トラフィックが外部のインターネットを通じて公開サーバーに向かうのを防ぎます。

			Source				Destination						
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
DNS Services	User to DC BP	universal	any	any	any	any	IT Infrastructure	DNS-Servers	any	dns	application-default	Allow		

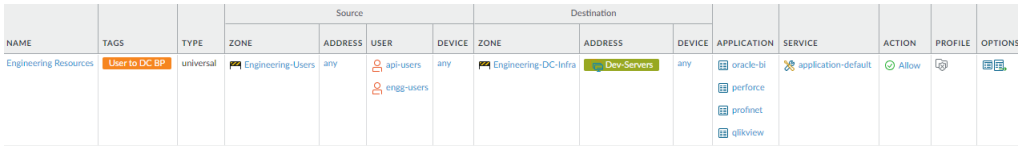
- 許可が必要な IT 部門の担当者のために、データセンターの管理インターフェイスに対する安全な権限付きアクセスを許可します。このルールは管理インターフェイス（この例ではアドレスグループを使用してデバイスを、カスタム サービスを使用して管理ポートを識別）および必要なアプリケーション（この例では RDP、SSH、SSL）に限定してください。専用 VLAN を使用して管理トラフィックを他のトラフィックと別け、同じサブネット上の管理インターフェイスを配置します。

同じ *IT* ユーザーグループがスイッチ、ルーター、その他のデータセンターのデバイスも管理する場合は、それらを宛先に追加し、そのポートをカスタム サービスに追加して管理インターフェイスに接続するためのトラフィックをルールが保護するようにします。別の *IT* グループが異なるデータセンターのリソースを管理する場合は、各グループ用に別々のセキュリティポリシールール、対応する復号化および認証ポリシールールを作成してください。



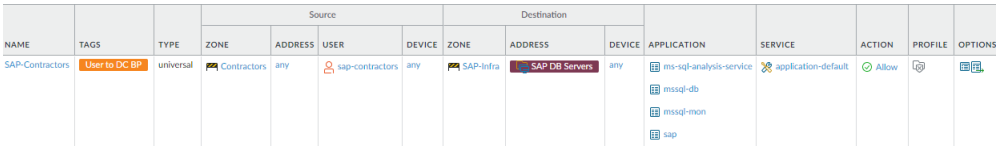
			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT DC Server Management	User to DC BP	universal	IT-Users	any	it-superusers	any	IT-Server-Access-DC	IT-Server-Management	any	ms-rdp ssh ssl	Custom-IT-Ports	Allow		

- 従業員ユーザーグループに必要なアクセスを許可します。これらのルールは、必要なアプリケーションやサーバーに対する各ユーザーグループ（あるいはユーザー）のアクセスを制限します。この例はエンジニアリング ユーザーグループのアクセスを開発用サーバーおよびアプリケーションに制限します。



			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Engineering Resources	User to DC BP	universal	Engineering-Users	any	api-users engg-users	any	Engineering-DC-Infra	Dev-Servers	any	oracle-bi perforce profinet qlikview	application-default	Allow		

- 契約者、提携企業、顧客、その他のサードパーティに対し、対象を絞った制限付きのアクセスを許可します。この例は、SAP 契約者グループのアクセスを、適切なアプリケーションを使用した適切な SAP データベースサーバーのみへのアクセスに制限します。



			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
SAP-Contractors	User to DC BP	universal	Contractors	any	sap-contractors	any	SAP-Infra	SAP DB Servers	any	ms-sql-analysis-service mssql-db mssql-mon sap	application-default	Allow		

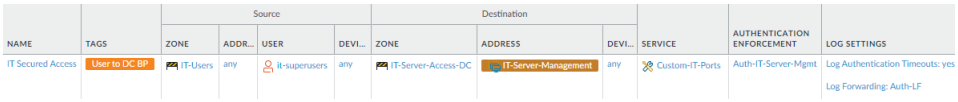
STEP 2 | ユーザートラフィック用の認証ポリシールールを作成し、データセンターのアクセスを認証します。

アプリケーション許可ルールを作成する対象である各ユーザーグループあるいはユーザーに対し、類似の認証ルール（DNS はユーザーがログイン用に認証を行う前に発生するため、DNS許可ルールを除く）を作成します。各ルールに対し、**Actions**（アクション）タブで**Log at Session End**（セッション終了時にログを記録）を設定し、ログ転送をセットアップしてルールの違反を追跡・分析します。

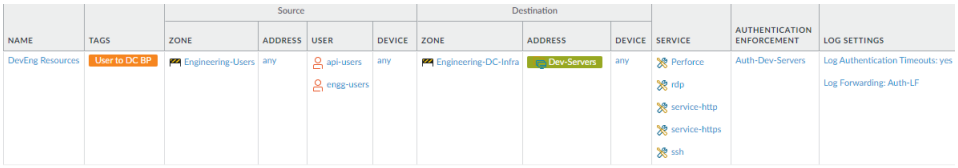
- 特別なアクセスが必要なユーザーを認証します。この例では前のステップの許可ルールの、データセンターサーバーを管理するために安全な権限付きアクセスを必要とするIT部門の担当者を認証し

ます。権限付きのユーザーの認証情報が奪われると攻撃者にデータセンターへの鍵を渡してしまうことになるため、多要素認証（MFA）を求めて認証情報の盗難による被害を回避してください。

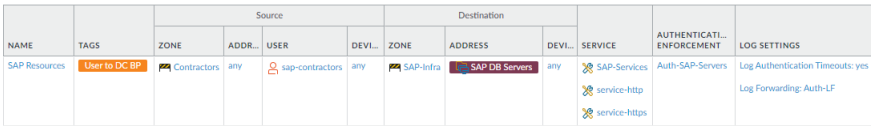
同じ *IT* ユーザーグループがスイッチ、ルーター、その他のデータセンターのデバイスも管理する場合は、それらを宛先に追加し、そのポートをカスタム サービスに追加して管理インターフェイスに接続するためのトラフィックをルールが認証するようにします。別の *IT* グループが異なるデータセンターのリソースを管理する場合は、各グループ用に別々のセキュリティポリシールール、対応する復号化および認証ポリシールールを作成してください。



- データセンターにアクセスする正当なビジネス上の理由を持つ従業員を認証します。この例では、前述のステップの許可ルールのエンジニアリング開発ユーザーグループを認証します。



- 契約者、提携企業、顧客、その他の非従業員グループを認証します。非従業員グループに対して MFA を求め、サードパーティの企業で認証情報が盗まれても被害を受けないようにしてください。この例では、前述のステップの許可ルールの SAP 開発者を認証します。



STEP 3 | ユーザートラフィック用に復号化ポリシー ルールを作成して許可するトラフィックを復号化し、ファイアウォールがトラフィックを把握・検査してセキュリティポリシーを適用できるようにします。

脆弱なプロトコルおよびアルゴリズムをブロックしてサーバー証明書を検証するために、各復号化ポリシー ルールに対し、適切な最良の復号化プロファイル（SSL インバウンド インスペクションおよび SSL 転送プロキシ ルール用のベストプラクティスの SSL プロトコル設定を含めて、SSL インバウンド インスペクション、SSL 転送プロキシ、SSH プロキシ、あるいは非複合化）を適用します。各 SSL インバウンド インスペクション ルールについては、復号化によって保護するデータセンター サーバーの証明書をインポートします。

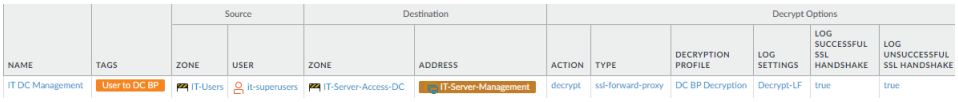
次の *2* つに対してのみ、トラフィックを復号化から除外します：

- 証明書のピンニングや相互認証などの技術的な理由で復号化を妨げるトラフィック。技術的な例外は*Device*（デバイス）> *Certificate Management*（証明書管理）> *SSL Decryption Exclusion*（*SSL* 復号化除外）リストに追加します。
- 金融、健康、軍事、政府関連のトラフィックなど、ビジネス、規制、コンプライアンスあるいは他の理由で復号化しないことにしたトラフィック。復号化しないことにしたトラフィック用のポリシー ベース復号化除外を作成します。

- 管理サーバーへの IT 部門の権限付きアクセスを許可する、以前に作成したセキュリティポリシー ルールからのトラフィックを復号化します。復号化ポリシー ルールおよびその関連する復号化プロファイルは、IT グループが SSL（SSL 転送プロキシの復号化プロファイル）と SSH（SSH プロキシ復号化プロファイル）のどちらを使用して管理ポートにアクセスするのかによって異なります。

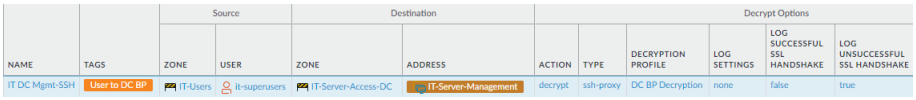
同じ *IT* ユーザーグループがデータセンターのスイッチ、ルーター、その他のデバイスも管理する場合は、それらを宛先に追加し、サーバー証明書を追加して管理インターフェイスに接続するためのトラフィックをルールが復号化するようにします。別の *IT* グループが一連の異なるデータセンターのリソースを管理する場合は、各グループ用に別々の強固なセキュリティポリシールール、対応する復号化および認証ポリシールールを作成してください。

SSL の権限付きアクセスの場合：



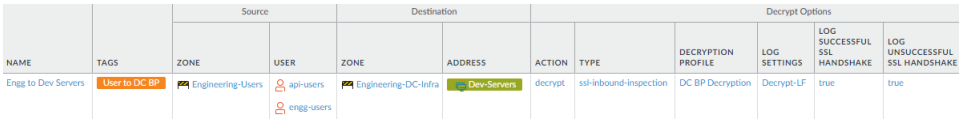
NAME	TAGS	Source ZONE	Source USER	Destination ZONE	Destination ADDRESS	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Management	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

SSH の権限付きアクセスの場合：



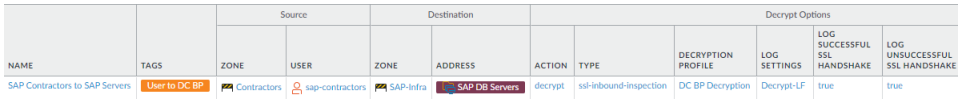
NAME	TAGS	Source ZONE	Source USER	Destination ZONE	Destination ADDRESS	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Mgmt-SSH	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssh-proxy	DC BP Decryption	none	false	true

- SSL インバウンド インスペクションを設定し、従業員ユーザーグループからの許可されたトラフィックを復号化します。この例では、類似のエンジニアリング開発ユーザーグループ許可ルールからのトラフィックを復号化します。



NAME	TAGS	Source ZONE	Source USER	Destination ZONE	Destination ADDRESS	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Engg to Dev Servers	User to DC BP	Engineering-Users	api-users engg-users	Engineering-DC-Infra	Dev-Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

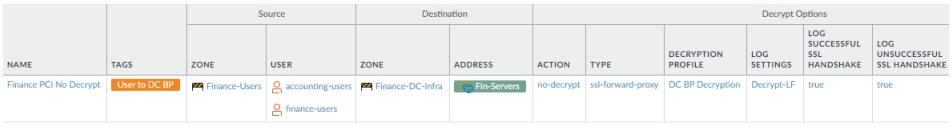
- SSL インバウンド インスペクションを設定し、契約者、提携企業、顧客、その他のサードパーティからの許可されたトラフィックを復号化します。この例では、類似の SAP 契約者ユーザーグループ許可ルールからのトラフィックを復号化します。



NAME	TAGS	Source ZONE	Source USER	Destination ZONE	Destination ADDRESS	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
SAP Contractors to SAP Servers	User to DC BP	Contractors	sap-contractors	SAP-Infra	SAP DB Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

- ビジネス、規制、コンプライアンスあるいは他の理由で復号化しないことにしたトラフィック。この例は、**Fin Servers**（財務サーバー）アドレスグループ内のサーバーにアクセスする際、2 つの財務部門のユーザーグループを復号化から除外する方法を示します。

No Decryption（復号化なし）プロファイルを*TLSv1.3*トラフィックには適用しないでください。証明書情報は暗号化されているため、ファイアウォールが証明書情報に基づいてセッションをブロックできなくなります。



NAME	TAGS	Source ZONE	Source USER	Destination ZONE	Destination ADDRESS	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Finance PCI No Decrypt	User to DC BP	Finance-Users	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	no-decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

インターネットからデータセンターへのトラフィックポリシー

インターネットからデータセンターへのトラフィックに対して、セキュリティポリシー、復号化ポリシー、およびサービス拒否攻撃（DoS）保護ポリシーを設定します。

- インターネットからデータセンターへのセキュリティポリシー
- インターネットからデータセンターへの復号化ポリシー
- インターネットからデータセンターへのDoS保護ポリシー

STEP 1 | インターネットからデータセンターへのトラフィック用にアプリケーションの許可リストセキュリティポリシールールを作成し、提携企業、契約者、顧客のアクセスを制御し、保護します。

感染した外部クライアントからマルウェアをダウンロードすることや、感染したデータセンター サーバーから外部サーバーにマルウェアを侵入させるのを防ぎます。ビジネス上の目的で必要なアプリケーションに対する許可ルールを作成し、外部動的リストEDL）を作成して不適切な IP アドレスをブロックします。各ルールに対し、**Actions**（アクション）タブで**Log at Session End**（セッション終了時にログを記録）を設定し、ログ転送をセットアップしてルールの違反を追跡・分析します。

この例はインターネットからデータセンターへのトラフィックのアプリケーションおよび宛先を制限し、**Negate**（拒否）オプションを使用して**Bad IPs List**（悪い **IP** リスト）EDL との通信を防止します。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Web Server Inbound	Internet to DC	universal	L3-External	Bad IPs List	any	any	Web-Server-Tier-DC	Web Servers	any	Acme	application-default	Allow		

インターネットから他のサーバーグループへのトラフィック（許可する場合）および他のアプリケーション用に同様のルールを作成します。必要なアプリケーションおよびサーバーへのアクセスを制御することに特化したルールを作成してください。

STEP 2 | インターネットからデータセンターへのトラフィック用に復号化ポリシー ルールを作成し、許可されたトラフィックを復号化します。

SSL インバウンド インスペクションを構成（および宛先サーバー証明書をファイアウォールにインポート）し、インターネットからデータセンターへのトラフィック用にセキュリティポリシールールが許可する提携企業、契約者、顧客のトラフィックを復号化します。この例は、前述のセキュリティポリシー ルール用の復号化ポリシーを示します。

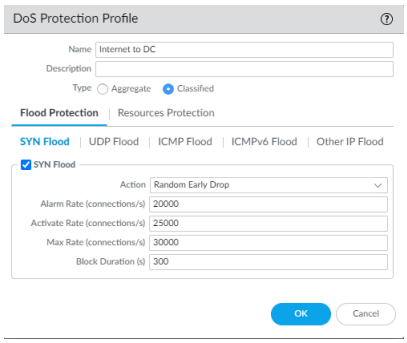
		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Internet to DC	Internet to DC BP	L3-External	any	Web-Server-Tier-DC	Web Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

インターネットからデータセンターへのセキュリティポリシールールが許可するトラフィックにマッチさせる復号化ルールを作成します。

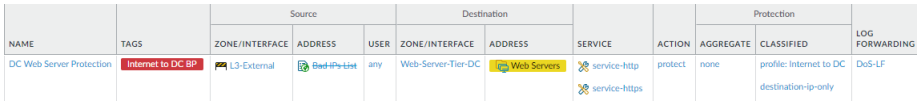
STEP 3 | インターネットからデータセンターへのDoS 保護ポリシールールを作成し、ファイアウォールが許可するサーバーへの 1 秒あたりの接続数（CPS）を制限してSYN フラッド攻撃を防ぐことで、センシティブなサーバーをサービス拒否（DoS）攻撃から保護します。

WEB サーバー層をダウンさせればデータセンターへのほとんどの正当なアクセスを妨害できるため、攻撃者は WEB サーバー層をターゲットにします。インバウンド CPS を制限するDoS 保護プロファイルを持つ分類化DoS 保護ポリシールールを適用し、サーバーのパフォーマンスや可用性に影響を与えるおそれのあるトラフィックの急激な増加を防いでください。

- 分類化 DoS 保護プロファイルを作成して WEB サーバー層を保護し、SYN フラッド攻撃を防ぎます。設定する CPS のしきい値は、ピーク時の CPS レートのベースラインによって異なります。



- 保護する WEB サーバーを指定する DoS 保護ポリシールールを作成し、それに分類化 DoS 保護プロファイルを適用します。



NAME	TAGS	Source ZONE/INTERFACE	Source ADDRESS	Source USER	Destination ZONE/INTERFACE	Destination ADDRESS	SERVICE	ACTION	Protection AGGREGATE	Protection CLASSIFIED	LOG FORWARDING
DC Web Server Protection	Internet to DC BP	L3-External	~~Bad-IPs-List~~	any	Web-Server-Tier-DC	Web Servers	service-http service-https	protect	none	profile: Internet to DC destination-ip-only	DoS-LF

  内部ソースからの SYN フラッド攻撃を防止するためには、DoS 保護ポリシールールを別途作成し、送信元ゾーンとして**L3-External**ではなく内部ゾーンを指定します。外部および内部の攻撃ソースに対して個別のルールを作成することで、別々にレポートを作成して攻撃の試みを調査しやすくなります。
- さらに、各データセンター ゾーン用のパケット バッファ保護を設定し、正当なトラフィックをドロップさせるおそれのある単一セッション DoS 攻撃からファイアウォールを保護します。

データセンターからインターネットへのトラフィックポリシー

データセンターからインターネットへのトラフィックに対して、セキュリティポリシーと復号化ポリシーを設定します。

- データセンターからインターネットへのセキュリティポリシー
- データセンターからインターネットへの復号化ポリシー

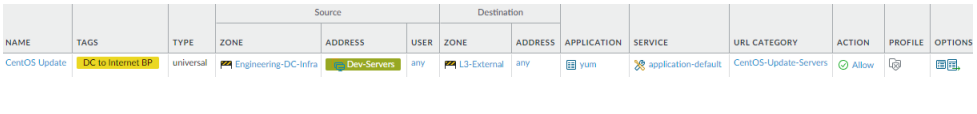
STEP 1 | データセンターからインターネットへの許可ルールを作成し、外部サーバーへの接続を保護します。

データセンター サーバーはインターネット上のサーバーからソフトウェア更新や証明書ステータスを取得する場合があります。誤ったサーバーに接続してしまうのが、最も大きなリスクになります。更新用に厳格な許可ルールを作成し、到達できる外部サーバーおよび許可するアプリケーションを制限してください（デフォルトのポートのみ）。これにより、感染したデータセンター サーバーが Phoning home を行ったり、標準的でないポート上で FTP、HTTP、DNS などの正当なアプリケーションを使用してデータを盗んだりすることを防止できます。さらに、ファイルブロッキングプロファイルの**Direction**（方向）制御を使用してアウトバウンドの更新ファイルをブロックし、ソフトウェア更新ファイルのダウンロードのみを許可するようにしてください。

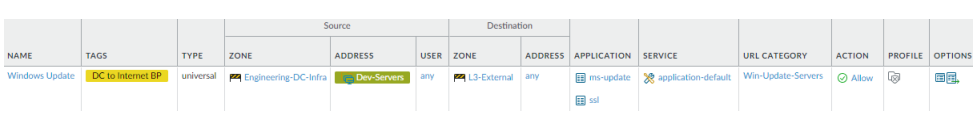
各ルールについて、最良のセキュリティ プロファイルを適用して**Actions**（アクション）タブで**Log at Session End**（セッション終了時にログを記録）を設定します。

ソフトウェアをアップデートするエンジニアリングおよびその他のグループと協力してウェブ ブラウジング セッションをログに記録して分析し、開発者がアップデートを行うために接続する *URL* を把握します。

- これらの例では、エンジニアリング サーバーが**yum**アプリケーションを使って CentOS 更新サーバー（**CentOS-Update-Servers**カスタム URL カテゴリ）と、**ms-update**を使って Microsoft 更新サーバー（**Win-Update-Servers**カスタム URL カテゴリ）と通信するのを許可します（**ms-update**は SSL に依存するため、**ssl**も許可する必要があります）。



NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
CentOS Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		



NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
Windows Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		

- DNS および NTP アップデートへのアクセスを許可します（**NTP DNS Update Servers**（**NTP DNS** 更新サーバー）カスタム URL カテゴリ）。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
NTP DNS Update	DC to Internet BP	universal	IT Infrastructure	DNS-NTP-Servers	any	L3-External	any	dns ntp	application-default	NTP-DNS-Update-Servers	Allow		

- 認証証明書の失効状態を確認してそれが有効であることを確かめるために、インターネットのオンライン証明書ステータス プロトコル（OCSP）レスポンダへの接続を許可します。ファイアウォール上で証明書プロファイルを設定する際、OCSP レスポンダに到達できない場合の OCSP に対するフォールバック方法として CRL ステータス検証をセットアップします。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Cert Update	DC to Internet BP	universal	IT Infrastructure	IT-Server-Management	any	L3-External	any	ocsp	application-default	Allow		

STEP 2 | データセンターからインターネットへの復号化ポリシー ルールを作成し、前述のセキュリティポリシールールで許可されるトラフィックを復号化します。

感染した更新サーバーがマルウェアをダウンロードし、ソフトウェア更新プロセスを通じてそれを拡散してしまうおそれがあるため、トラフィックを復号化して可視性を確保することが重要です。更新トラフィックを開始するのはサービス アカウントだけであり、更新トラフィックには個人情報やセンシティブな情報が含まれないため、プライバシー関連の問題はありません。

OCSP 証明書無効化サーバーへのトラフィックは通常 *HTTP* を使用し、暗号化されていないため、復号化しないでください。さらに、ファイアウォールがプロキシとして動作してクライアント証明書をプロキシ証明書と交換し、*OCSP* レスポンダがこれを有効なものとみなさない可能性があるため、*SSL* フォワード プロキシ復号化が更新プロセスを妨げるおそれがあります。

- データセンターおよび更新サーバー間のトラフィックを復号化します。これらの 2 つの例では、前述のステップの類似のセキュリティポリシールールが許可する CentOS および Windows 更新トラフィックを復号化します。

NAME	TAGS	Source ZONE	Source ADDRESS	Destination ZONE	Destination ADDRESS	URL CATEGORY	Decrypt Options ACTION	Decrypt Options TYPE	Decrypt Options DECRYPTION PROFILE	Decrypt Options LOG SETTINGS	Decrypt Options LOG SUCCESSFUL SSL HANDSHAKE	Decrypt Options LOG UNSUCCESSFUL SSL HANDSHAKE
CentOS Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	CentOS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

NAME	TAGS	Source ZONE	Source ADDRESS	Destination ZONE	Destination ADDRESS	URL CATEGORY	Decrypt Options ACTION	Decrypt Options TYPE	Decrypt Options DECRYPTION PROFILE	Decrypt Options LOG SETTINGS	Decrypt Options LOG SUCCESSFUL SSL HANDSHAKE	Decrypt Options LOG UNSUCCESSFUL SSL HANDSHAKE
Win Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	Win-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

- データセンター サーバーと NTP および DNS 更新サーバー間のトラフィックを復号化します。この例では、前述のステップの類似のセキュリティポリシールールが許可する更新トラフィックを復号化します。

NAME	TAGS	Source ZONE	Source ADDRESS	Destination ZONE	Destination ADDRESS	URL CATEGORY	Decrypt Options ACTION	Decrypt Options TYPE	Decrypt Options DECRYPTION PROFILE	Decrypt Options LOG SETTINGS	Decrypt Options LOG SUCCESSFUL SSL HANDSHAKE	Decrypt Options LOG UNSUCCESSFUL SSL HANDSHAKE
DNS-NTP Update Decrypt	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	L3-External	any	NTP-DNS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

データセンター内トラフィックポリシー

データセンターのサーバーとアプリケーション層間のトラフィックに対する、セキュリティポリシーと復号化ポリシーを設定します。

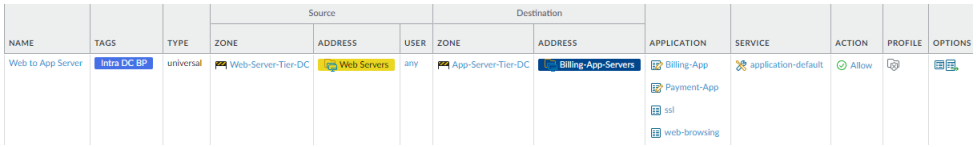
- データセンター内セキュリティポリシー
- データセンター内復号化ポリシー

STEP 1 | データセンター内アプリケーション許可ルールを作成し、感染した可能性がある他のデータセンター サーバーから、データセンター サーバーを保護します。

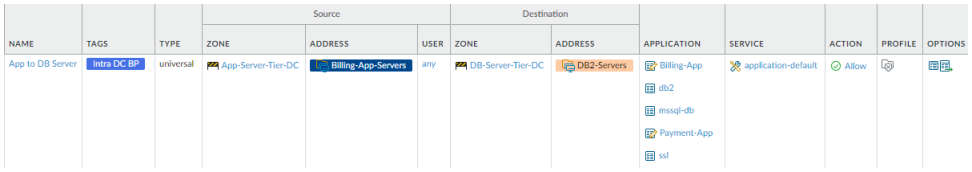
一般的なアプリケーション アーキテクチャは、WEB サーバー、アプリケーションサーバー、データベースサーバーという 3 つのサーバー層で構成されます。サーバー層間のほとんどのトラフィックに最良のセキュリティ プロファイルを適用し、脅威を防いでください。メールボックスのレプリケーションやバックアップ フローのような価値が低く大容量のトラフィックにはセキュリティ プロファイルを適用しません（ファイアウォールがすでに元のフローを検査しているため、それらに対して CPU サイクルを使用しても意味がありません）。これらのアプリケーションに対して許可ルールを作成し、誤った利用を防止してください。各ルールに対し、**Actions**（アクション）タブで**Log at Session End**（セッション終了時にログを記録）を設定し、ログ転送をセットアップしてルールの違反を追跡・分析します。

この例では、カスタム アプリケーション（**Billing-App**および**Payment-App**）の作成対象である 2 つの社内向けの財務アプリケーション用にアプリケーションサーバー間のトラフィックを許可するルールを構成します。

- WEB サーバー層およびアプリケーションサーバー層間で財務アプリケーションのトラフィックを許可します。



- アプリケーションサーバー層およびデータベースサーバー層間で財務アプリケーションのトラフィックを許可します。

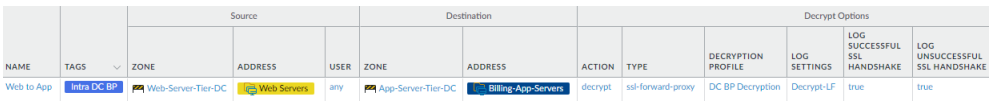


STEP 2 | データセンター内復号化ポリシー ルールを作成し、前述のセキュリティポリシールールで許可されるトラフィックを復号化します。

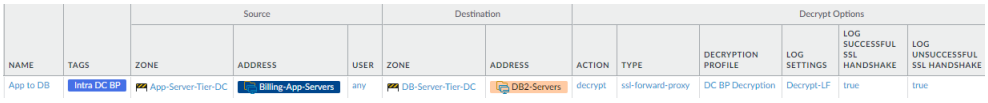
多くの人がデータセンターは安全だと考え、侵入者を探さないため、データセンターは攻撃者にとって格好の潜伏場所になります。しかし、ネットワークの他の場所と同じ原則、つまり、目に見えないものは防止できないという原則が、データセンターにも当てはまります。ファイアウォールがトラフィックを検査し、アクセスを制御し、脅威を明らかにし、重要なアセットを保護できるよう、データセンターのトラフィックを復号化してください。

すべてのデータセントートラフィックが暗号化されている訳ではありません。暗号化されていない（クリアテキスト）トラフィックの復号化にリソースを無駄にしないでください。

- このルールは、Finance（財務）部門の課金サーバーに対して、Webサーバー層とアプリケーションサーバー層間を移動するトラフィックを復号化します。



- このルールは、Finance（財務）部門の請求サーバーに対して、アプリケーションサーバー層とデータベースサーバー層間を移動するトラフィックを復号化します。



データセンター セキュリティポリシーのルールベースの順序

セキュリティポリシールールベースで、ルールの順序を適切に並べ替えて、目的の許可するアプリケーションとトラフィックのみを許可し、あるルールが他のルールを妨害しないようにしてください。

データセンター セキュリティポリシーのルールベースの順序を指定では、前の例（許可およびブロックルール）のルールベース全体を正しい順序で示し、各ルールの配置を説明します。

デプロイ後のデータセンターのベストプラクティスに従う

データセンターのベストプラクティスを導入し始めた後はネットワークを監視し、セキュリティとアクセスが想定通りに機能していることを確認してから、環境の変化に合わせてルールベースの保守を行ってください。

STEP 1 | 事前定義済みのアプリケーション レポート（**Monitor**（監視）> **Reports**（レポート）> **Application Reports**（アプリケーション レポート）> **Applications**（アプリケーション））をチェックし、セキュリティポリシールールで許可したアプリケーションだけが実行されていることを確認します。

予期せぬアプリケーションが見つかった場合はセキュリティポリシールールを確認して調整し、予期せぬアプリケーションを取り除くか、正当なアプリケーションを承諾してください。

STEP 2 | すべてのデータセンター トラフィックをログに記録します。

Palo Alto Networks の豊富な監視ツール、ロギングツール、事前定義済みのレポート、カスタム レポートを使用すれば、予期せぬアプリケーション、ユーザー、トラフィック、挙動などのアクティビティを捕捉・監視できます。

STEP 3 | ブロック ルールを監視するカスタム レポートを作成し、潜在的な攻撃を防ぎつつ、ポリシーのギャップや予期せぬ挙動を特定し、ルールベースを調整できるようにします。

STEP 4 | ルールベースの最下部にある事前定義済みのイントラゾーン デフォルト許可ルールにマッチするイントラ データセンター トラフィックをログに記録するカスタム レポートを作成し、同じゾーン内のすべてのトラフィックをデフォルトで許可します。

STEP 5 | ロギングを有効化し、ルールベースの最下部にある事前定義済みのインターゾーン デフォルト ルールにマッチするデータセンター トラフィック用のカスタム レポートを作成して、ゾーン間のすべてのトラフィックをデフォルトで拒否します。

STEP 6 | ユーザーからフィードバックを得て対応を行います。

アプリケーションにアクセスできなくなったというユーザの苦情があれば、ルールベースの漏れや、アプリケーションの許可リストによって使用が妨げられる前にネットワーク上で使用されていたリスクのあるアプリケーションを特定します。

STEP 7 | 計画段階で測定したベースラインと現在の測定値を定期的に比較し、進捗状況を評価し、変化を知り、改善が必要な部分を把握します。

同時に、目標にしたネットワークの将来の理想的な状態を再確認し、進捗状況を評価します。Panorama を使ってファイアウォールを管理する場合は、ファイアウォールの安全状態を監視し、各デバイス同士およびそのパフォーマンスのベースラインと比較し、通常の動作からの逸脱を把握します。

STEP 8 | アプリケーションは進化し、ユーザーの要件は変化し、コンテンツ更新によって既存の App-ID が新しい App-ID に変わるため、アプリケーション許可ルールを適宜調整してください。

データセンターの最良のルールベースを管理し、新しいコンテンツ リリースをインストールする前に新規および変更された App-ID の確認を行い、その変更によってポリシーが影響を受ける場合にルールベースを変更できるようにします。

STEP 9 | Palo Alto Networks の評価およびレビューツールを使用し、現在の保護方針やベストプラクティスの実装状況を評価してください。

STEP 10 | 計画、デプロイ、デプロイ後の各ステップやそのメリットに関する詳細については、データセンターの最良のセキュリティポリシー全体を参照してください。

データセンターの最良のセキュリティポリシー

非公開のソースコード、知的財産、センシティブな企業・顧客のデータなど、企業の最も価値の高い資産はデータセンター内にあります。顧客や従業員は、自身のデータの機密性・整合性を維持すること、そのデータを常に利用できる状態にすることを管理者に求めています。事業の完全性を保って成功を収めるためには、データを保護して攻撃を防止するデータセンターの最良のセキュリティポリシーを実装することが重要です。

データセンターの最良のセキュリティポリシーを優先順位に従って段階的な方法で計画・設計・実装するうえで、次に紹介する方法や推奨事項が基本になります。一度にネットワークのすべての場所であらゆる保護を実装しようとすると、データセンターの最良のセキュリティポリシーを作成するのが困難な作業になります。しかし、保護すべき最も重要なものが何であるのか評価し、データセンターの最良のセキュリティポリシーを実装する作業を最も価値の高い資産を保護することから始めれば、不要なリスクを負わずにアプリケーション、ユーザー、コンテンツを保護するセキュリティポリシーへと徐々に移行していくことができます。

データセンター セキュリティポリシーのベストプラクティスのチェックリストでは、デプロイ前、デプロイ時、デプロイ後のベストプラクティスの概要や、詳細な説明が不要である場合に素早くベストプラクティスを実装する方法を説明しています。

- データセンターの最良のセキュリティポリシーとは？
- データセンターの最良のセキュリティポリシーが必要な理由とは？
- データセンターの最良の方法論
- データセンターの最良のセキュリティポリシーをデプロイする方法とは？
- データセンターを評価する方法
- データセンターのトラフィックを復号化する方法
- データセンターのセグメント化戦略を作成
- データセンターの最良のセキュリティポリシーを作成する方法
- Cortex XDRエージェントを使用したデータセンターエンドポイントの保護
- データセンターのトラフィック ブロック ルールを作成
- 最初のユーザーからデータセンターへのトラフィックのセキュリティポリシーを定義
- 最初のインターネットからデータセンターへのトラフィックのセキュリティポリシーを定義
- 最初のデータセンターからインターネットへのトラフィックのセキュリティポリシーを定義
- 最初のイントラ データセンター トラフィックのセキュリティポリシーを定義
- データセンター セキュリティポリシーのルールベースの順序を指定
- データセンター トラフィックのログおよび監視
- データセンターの最良のルールベースを管理
- Palo Alto Networks の評価およびレビューツールを使用

データセンターの最良のセキュリティポリシーとは？

データセンターの最良のセキュリティポリシーは企業の貴重なデータを保護し、顧客、提携企業、ベンダーの機密情報を守り、ネットワークや事業運営全体の一貫性を確保し、ネットワークを常に利用できる状態にします。これは、ネットワーク内外で発生してあらゆる侵入経路を通る攻撃を防止します。

データセンターの最良のセキュリティポリシーは、4 つのトラフィック フロー（接続が開始される領域）を保護します。

1. データセンター内へと流れるローカルのユーザートラフィック。
2. インターネットからデータセンターへと流れるトラフィック。
3. データセンターからインターネットへと流れるトラフィック。
4. サーバーあるいは VM 間を流れるイントラ データセンター トラフィック（East-West トラフィックとも呼ばれます）。

データセンターの最良のセキュリティポリシーは、攻撃者がデータセンター内に足がかりを得るのを防止し、どうにかしてデータセンターのセキュリティを破った攻撃者がいれば、データの盗難やネットワーク内を横方向に移動して重要なサーバーに侵入するのを防ぎます。これは、セキュリティポリシールールを実装し、お客様のビジネス要件に合うベストプラクティスの目標を達成することで、既知および未知の脅威の両方を防止します。これは：

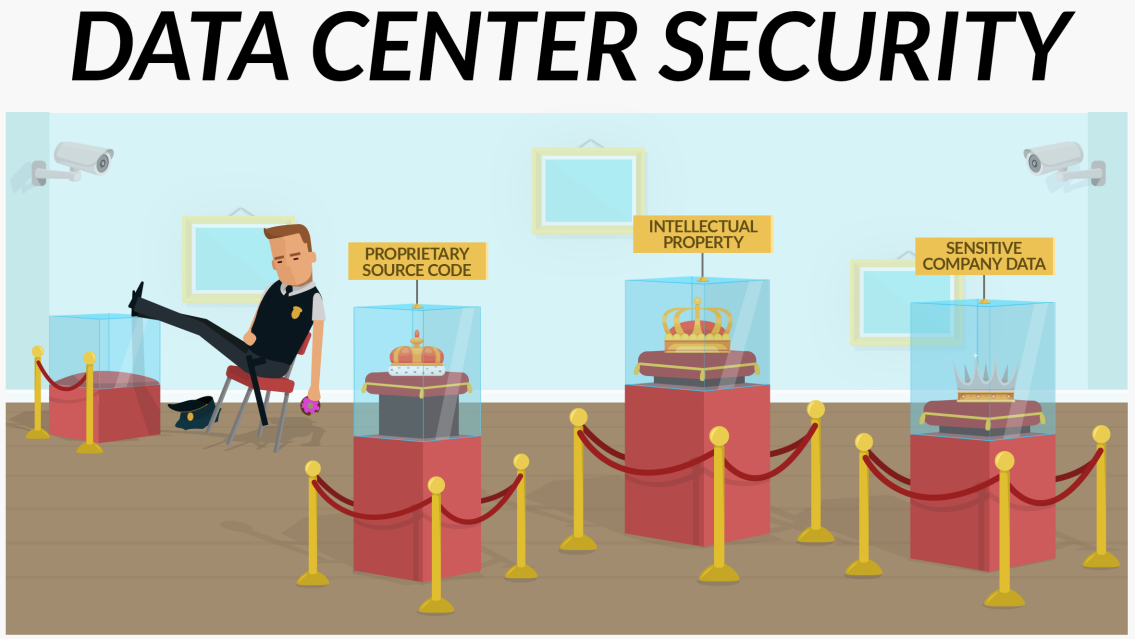
- 暗号化されたトラフィックを復号化するなどして、ポート、プロトコル、回避技術に関わらず、アプリケーションを特定します。
- IP アドレス、場所、デバイスに関わらず、ユーザーを特定して制御します。
- アプリケーションが媒介する既知および未知の脅威や脆弱性を防止します。
- 攻撃が進行中であることを示唆する異常な行動を検出します。

データセンターの最良のセキュリティポリシーはまた、ポリシールールに違反した際に侵入者を捕捉します。違反によって次世代ファイアウォールはアクセスを拒否し、問題を調査して適切な対応を行えるよう、違反をログに記録するため、ルールの違反によって攻撃が終了します。

データセンターの最良のセキュリティポリシーが必要な理由とは？

センシティブなデータを保護することも求める規制に則った形で中断することなく安全に業務を行うために、ネットワークの可用性、機密性、整合性を保護することが重要です。ネットワークの境界を強化し、ネットワーク内部は信頼できるため制限を緩いままにしても構わないというのは過去の話であり、ネットワークの内側から攻撃する機会を攻撃者に与えてしまいます。豊富なリソースを持つ粘り強い攻撃者が境界内に足がかりを得るというシナリオを考慮して計画を立てていません。エンタープライズ ネットワークの境界を保護するのと同じくらい強固にデータセンターの境界および内部を保護しなければならないのは、そのためです。

内部攻撃は、現在の従業員やオンサイトの契約者などが元になって発生する可能性があります。攻撃者が正当なユーザーやアプリケーション ソースに起因するのが、内部攻撃で良くある脅威です。外部攻撃はサイバー犯罪集団、ハクティビスト、国が後ろ盾になっている攻撃者だけでなく、感染した提携企業やベンダーのシステム、ネットワークをよく知る元従業員など、意外なところから発生する可能性があります。外部攻撃者の最初のステップは、ネットワーク内に足がかりを得て、攻撃を内部攻撃に変えることです。結局、ネットワークへのアクセスを掌握した攻撃者はネットワーク中を移動できるため、攻撃の元が外部にあったとしても、すべてのセキュリティ違反が内部攻撃になります。



提携企業が持つ正当なアクセス認証情報を盗んだ攻撃者は、正当なユーザーになりすましてデータセンターにアクセスできます。その後、攻撃者はセキュリティが緩いネットワーク内部から、内部サーバーおよびエンドポイントを使用してネットワーク内を横方向に移動し、重要なシステムに侵入するおそれがあります。攻撃が内部から始まる場合と同じく、外部の攻撃者にネットワークのセキュリティを破られたら、データを保護するために頼れるのはネットワーク内の複数の保護層およびネットワークとユーザーのセグメント化になります。

優先順位を伴う段階的な方法で最も価値の高い資産を始めに保護し、徐々に保護を追加していき、最良のセキュリティポリシーを作成することで、攻撃がどこから発生しようとデータセンターを守ることができます。「最善を祈る」セキュリティポリシーからデータセンターの最良のセキュリティポリシーへと徐々に移行していくことで、データの機密性、組織の一貫性、データセンターの可用性を現実的な方法で守ることができます。データセンターの最良のセキュリティポリシーを設計・実装するための次の推奨事項

は、エンドユーザーを妨げるのを最小限に抑えつつ、すべてのトラフィックを分類化することで常にアプリケーション、ユーザー、コンテンツを保護する方法を示します。

データセンターの最良の方法論

次の最良の方法論により、攻撃サイクルの複数の段階で確実に検知・防御を行うことができます。

最良の方法論	これが重要な理由
すべてのトラフィックを検査して完全な可視性を確保	ネットワーク トラフィックを把握することで、攻撃者の存在を明らかにできます。トラフィックを検査し、データセンターを出入りするユーザー、アプリケーション、コンテンツを把握してください。 ❑ すべてのネットワーク トラフィックを検査できる場所に次世代ファイアウォールをデプロイします。ファイアウォールがトラフィックを検査できない位置にある状態で、データセンターに入るトラフィックやネットワーク セグメント間を流れるトラフィックを許可しないでください。 ❑ 健康、金融、政治、軍事など、規制やコンプライアンス規則に従って除外しなければならないカテゴリーでない限り、データセンターを出入りするすべてのトラフィックに対して SSL復号化を有効化してください。ネットワークを脅威から保護するためには、脅威を把握できなければなりません。典型的なネットワークのトラフィックは 50% 以上が暗号化されており、その割合は増えてきているため、トラフィックを復号化しなければ、ネットワークを完全に保護することは不可能です。 ❑ App-IDを使用してアプリケーションを特定し、専有アプリケーション用にカスタム アプリケーションを作成し、ファイアウォールが識別を行ってアプリケーションを適切にカテゴリー分けし、正しいセキュリティポリシー ルールを適用できるようにします。誤って「web-browsing」あるいは「unknown-tcp」にカテゴリー分けされる古いアプリケーションにとって、特にこれが重要になります。 一連のポート用のカスタム セッション タイムアウトを定義するだけの目的で作成した既存のアプリケーション オーバーライド ポリシーがある場合、サービスベースのセッション タイムアウトを設定して各アプリケーションのカスタム タイムアウトを管理してからルールをアプリケーション ベースのルールに移行することで、既存のアプリケーション オーバーライド ポリシーをアプリケーション ベースのポリシーに変換します。アプリケーション オーバーライド ポリシーはポートベースです。アプリケーション オーバーライド ポリシーを使用して一連のポートのカスタム セッション タイムアウトを管理する際、それらのフローに対するアプリケーションの可視性が失われるため、どのアプリケーションがポートを使用するのか把握することも、管理することもできません。サービスベースのセッション タイムアウトはアプリケーションの可視性も維持しつつ、カスタム タイムアウトを利用できるようにします。 ❑ データセンターを出入りするすべてのトラフィックに対してUser-IDを有効化し、アプリケーション トラフィックおよびコンテンツ内の関連する脅威をユーザーおよびサービスにマッピングします。User-ID をネットワーク セグメント (ゾーン) 上で有効化するため、ネットワークをセグメント化して User-ID を有効化する必要があります。可視性を確保して攻撃の入り口を減らすうえで、ネットワークをセグメント化することがベストプラクティスになります。 ❑ GlobalProtectを内部モードでゲートウェイとしてデプロイし、データセンターへのアクセスを制御します。GlobalProtect はユーザー情報をチェックしてユーザーを検証し、ユーザーが定義するプロファイルおよび HIP オブジェクトとホスト情報を照らし合わせることで、ホストのセキュリティが最新の状態であることを確認します。これにより、ネットワークに接続するホストに、必要なレベルのセキュリティを求めることができます。 ❑ すべてのセキュリティポリシールールで「log at session end (セッション終了時に口グを記録) 」を有効化してください。

最良の方法論	これが重要な理由
	トラフィックに対する可視性を確保することで、ユーザーの位置、デバイス タイプ、ポート、暗号、回避技術に関わらず、ファイアウォールがネイティブの App-ID、コンテンツ ID、User-ID テクノロジーを使ってアプリケーション、脅威、コンテンツをユーザーに紐付けられるようになります。
攻撃面を低減	アプリケーション、コンテンツ、ユーザー、サーバー、スイッチ、ルーター、その他の物理・仮想装置を含むハードウェアおよびソフトウェアの両方で、ネットワークが通信を行うすべての場所が攻撃の入り口になります。攻撃の入り口を減らすことで、攻撃者が利用できる脆弱性を減らすことができます。攻撃の入り口が少ないほど、ネットワークのセキュリティを破るのが難しくなります。 ❑ データセンターを評価し、ネットワーク上のアプリケーション、コンテンツ、ユーザーを把握してください。 ❑ ポジティブ エンフォースメントを採用（正当なビジネス上の目的を持つアプリケーションのみをネットワーク上で許可するアプリケーション ベースのセキュリティポリシールール、および正当に使用できる場面がない高リスクのアプリケーションをすべてブロックするルールを作成）することで、セキュリティを確保します。 ❑ 環境を評価することで得た情報を使用し、ビジネス要件、基本的な機能、グローバルなポリシー要件に基づいてネットワークを各ゾーンにセグメント化する戦略を作成し、各ゾーン内のリソースに同じセキュリティ レベルが求められるようにします。データセンター内では、データベース、WEB サーバー、アプリケーションサーバー、開発用サーバー、本番用サーバーなどのアプリケーション層を各ゾーンにセグメント化します。トラフィックはゾーン間を移動する際にファイアウォールを経由しなければならないため、セグメント化を行うことで、アプリケーション層間のトラフィックを把握できるようになります。 細かくセグメント化を行うことで、各ゾーンのビジネス要件に特化したセキュリティポリシールールを作成し、各セグメントを適切に保護できるようになります。また、App-ID、Content-ID（脅威防止）、User-ID を組み合わせることで、アクセスを許可すべきトラフィックを識別してそれ以外を拒否できるため、セグメント化を行うことで、データセンターに存在/侵入するマルウェアが横方向に移動するのを防ぐこともできます。 ❑ GlobalProtect を内部モードでゲートウェイとしてデプロイし、データベースへのアクセスを制御します。 ❑ アプリケーション トラフィックを許可するセキュリティポリシールール上でファイル ブロッキング プロファイルを適用して悪意のあるリスクの高いファイル形式をブロックすれば、攻撃の入り口をさらに減らすことができます。ファイアウォールの認証ポリシーを使用して多要素認証を有効化することで、攻撃者が認証情報を盗んだ場合でもデータセンターのネットワークにアクセスできないようにして、認証情報の盗難によるセキュリティ侵害を防いでください。
既知の脅威を阻止	セキュリティポリシー許可ルールに付与されたセキュリティ プロファイルは、トラフィックをスキャンしてウイルス、スパイウェア、アプリケーション層の脆弱性を狙ったエクスプロイト、悪意のあるファイルのような既知の脅威を発見します。ファイアウォールはセキュリティ プロファイルの設定に基づき、許可、アラート、ドロップ、IP のブロック、接続のリセットなどのアクションをそれらの脅威に適用します。 コンテンツ更新のベストプラクティスに従い、コンテンツ更新をダウンロードしたらすぐにインストールしてセキュリティ プロファイルをアップデートし、最新の保護をデータセンターに適用してください。簡単にセキュリティポリシールールに適用できるセキュリティ プロファイルは、保護の土台を提供してくれます。 また、外部動的リスト（EDL）も既知の脅威を防止します。EDL は悪意のあるリスクの高い IP アドレス、URL、ドメインのリストをファイアウォールにインポートすることで既

最良の方法論	これが重要な理由
	知の脅威を防止します。信頼できるサードパーティが提供する EDL、ファイアウォール上で事前定義された EDL、ユーザー自身が作成するカスタム EDL が存在します。EDL はファイアウォール上で動的にアップデートされ、コミットは不要です。 復号化を有効にする重要な理由の一つが、既知の脅威を防止することです。脅威のことを知っていても脅威を把握できなければ意味がないため、被害に遭う可能性があります。
未知の脅威を阻止	これまで誰も遭遇したことがない脅威を検出する方法は、すべての未知のファイルをWildFireに転送して分析を行うことです。 WildFire は未知あるいはターゲットのマルウェアを特定します。ファイアウォールは初めて未知のマルウェアを検出すると、ファイルを内部の宛先だけでなく WildFire クラウドに転送して分析を行います。WildFire はファイル（あるいはメール内のリンク）を分析し、わずか 5 分以内に判定をファイアウォールに返します。また WildFire はファイルを特定するシグネチャも含み、未知のファイルを既知のファイルに変えます。ファイルに脅威が含まれていた場合、その脅威が既知のものになります。悪意のあるファイルだった場合、次回にそのファイルがファイアウォールに到達した際、ファイアウォールはそのファイルをブロックするようになります。 判定は WildFire 送信ログで確認できます（**Monitor**（監視）> **Logs**（ログ）> **WildFire Submissions**（**WildFire** 送信））。分毎に自動的にダウンロードおよびインストールを行うようWildFire アプライアンスのコンテンツ更新をセットアップし、常に最新のサポートを得られるようにします。例えば、Linux および SMB ファイルのサポートは、最初に WildFire アプライアンスのコンテンツ更新として配信されます。

さらに：

- Panorama を使ってファイアウォールを一元的に管理することで、物理・仮想環境全体でポリシーを一貫した形で適用し、確保した可視性を集約できます。
- セキュリティのポジティブ エンフォースメントを採用し、データセンターのネットワーク上で対象のトラフィックのみを許可し、それ以外をブロックします。
- 各データセンター全体に対して複製・適用できる、標準的なスケーリングできる設計を行います。
- 重役、IT 部門およびデータセンターの管理者、ユーザー、その他の関係者の協力を求めます。

自身のビジネスおよびネットワークで最も発生しそうな脅威にフォーカスして保護すべき最も重要なアセットを判断し、まずはそれを保護することで、次世代型のセキュリティを段階的に導入していきます。最初に保護すべきアセットの優先順位を決める際、次のことを考えてください：

1. 自社の特徴とは何か？企業の特徴を形成する要素は何で、その要素に関連するのはどのアセットでしょうか。企業の強みとなる専有アセットは、優先して保護する必要があります。例えばソフトウェア開発企業の場合はソースコードを、製薬会社の場合は医薬品の成分を優先するでしょう。
2. 事業運営に必要なものとは？企業が毎日の業務を行ううえで、どのシステムやアプリケーションが必要でしょうか。例えば、アクティブディレクトリ（AD）サービスは、従業員がアプリケーションやワークステーションにアクセスできるようにします。攻撃者が AD サービスを攻撃すると、企業のすべてのアカウントを使用してネットワークに自由にアクセスできるようになってしまいます。他にも、管理ツール、認証サーバー、事業を運営するうえで最も重要なデータをホストするサーバーなど、不可欠な IT インフラもこれに該当する例です。
3. このアセットを失ったらどうなるだろうか？失った時に被害が大きくなるアセットは、優先して保護します。例えば、ユーザーエクスペリエンスが強みであるサービス企業にとっては、そのユーザーエクスペリエンスを守ることが優先されます。独自工程や自社開発の装置が強みであるメーカーの場合は、知的財産や独自の設計を保護することが優先されます。優先順位のリストを作成し、何を優先して保護するのか決定してください。

将来のデータセンターのネットワークの理想的な形を考え、段階的に作業を行ってそれを実現していきます。事業、新しい規制や法的要件、新たなセキュリティ要件を加味しつつ、定期的にその計画を再確認してください。

データセンターの最良のセキュリティポリシーをデプロイする方法とは？

データセンターのネットワーク、そのアセット、ファイアウォールの脅威防止機能を理解してから、その情報に基づいて最初のセキュリティポリシールールを作成し、最も価値の高い資産を最初に保護するという流れで、データセンターの最良のセキュリティポリシーを実装できます。

- データセンターを評価する方法—保護すべきアセット、それに対する最も大きな脅威、アクセスが制限されるアプリケーションおよびユーザーを把握し、優先順位を決めます。
- データセンターのトラフィックを復号化する方法—ネットワークを目に見えない脅威から防止することはできません。復号化されたトラフィックは、攻撃者が脅威をもたらす際に頻繁に使用する手段になります。4
- データセンターのセグメント化戦略を作成—データセンターをセグメント化することで、データセンター内に足がかりを得た攻撃者が他の領域へと横方向に移動するのを防ぎます。
- データセンターの最良のセキュリティポリシーを作成する方法—正当なアプリケーションが、コマンドアンド コントロール、マルウェア、共通脆弱性識別子（CVE）、悪意のあるコンテンツのドライブバイダウンロード、フィッシング攻撃、および APT をもたらす可能性があります。ベストプラクティスのセキュリティ プロファイルは、4 つすべてのデータセンター トラフィック フローに関する既知および未知の脅威から、許可されたトラフィックを保護します。
- Cortex XDRエージェントを使用してデータセンターのエンドポイントを保護—ファイアウォールはネットワークを通る脅威を防止します。しかし、エンドポイント上で実行される脅威はネットワークを通過しないため、ファイアウォールを通ることもありません。すべてのエンドポイントにCortex XDRエージェントをインストールし、エンドポイントを脅威から保護してください。
- データセンターのトラフィック ブロック ルールを作成—悪意のある既知の IP アドレス、攻撃者が頻繁にエクスプロイトに利用するアプリケーション、セキュリティをかいくぐることを意図したアプリケーション、データセンター内でビジネス上の目的で使用することがないアプリケーションをブロックします。
- 最初のユーザーからデータセンターへのトラフィックのセキュリティポリシーを定義—不正なアクセスは、データセンター内の貴重な情報に対して大きなリスクをもたらします。社内ネットワーク上の従業員や他のユーザーは信頼されていることが多いため、セキュリティ対策が不十分であることがあります。ユーザーおよびデータセンターが単一のフラットなネットワークである場合もあります。データセンターにアクセスできるユーザー、個々のユーザーグループがアクセスできるアセット、個々のユーザーグループのアプリケーションに対するアクセス レベルを厳重に制御してください。
- 最初のインターネットからデータセンターへのトラフィックのセキュリティポリシーを定義—悪意のある インターネット トラフィックからデータセンター サーバーを保護します。サーバー側の脆弱性をエクスプロイトされると、データセンターが攻撃され、感染したデータセンター サーバーがサードパーティのクライアントをエクスプロイトするおそれがあるため、パートナーがリスクにさらされるかもしれません。
- 最初のデータセンターからインターネットへのトラフィックのセキュリティポリシーを定義—インターネットに接続する感染したサーバーに潜むコマンド アンド コントロールのマルウェアは、正当なアプリケーションを使用してマルウェアをさらにダウンロードできます。アプリケーションが標準的でないポートを使用するのを防ぎ、各アプリケーションが正当な目的で使用しなければならないファイル形式の転送のみを許可し、マルウェア、フィッシング、プロキシ アナライザ、ピアツーピア、その他の悪意のある可能性がある URL カテゴリをブロックします。
- 最初のイントラ データセンター トラフィックのセキュリティポリシーを定義（East-West トラフィック）—ユーザートラフィックはデータセンター内から発生せず、データセンターは信頼できるとみなされているため、データセンター内の脅威が見落とされることがよくあります。しかし、攻撃者がデータセンター サーバーのセキュリティを破った場合、サーバーおよび VM 間の通信によってマルウェアが繁殖する可能性があります。最良のセキュリティポリシーは、攻撃者がデータセンターを通じて横方向に移動し、他のシステムに侵入してデータを盗むのを防止します。

- データセンター トラフィックのログおよび監視– 許可・ブロックされたトラフィックをログに記録して監視することで、データセンターの最良のセキュリティポリシーの移行・保守の全段階に関する情報を得られます。これにより、存在を知らなかったものも含め、ネットワーク上の各アプリケーション、ユーザー、トラフィックのパターンが明らかになります。潜在的なセキュリティの問題を調査するうえで、この情報が役立ちます。
- データセンターのベストプラクティスのルールベースを管理–新しい制限付きのアプリケーションを承諾できるようにルールを調整し、新規あるいは変更された App-ID がポリシーに与える影響を判断できるよう、アプリケーション許可リストを継続的に監視します。

データセンター セキュリティポリシーのルールベースの順序を指定は、セキュリティポリシーのルールベースの情報を簡潔にまとめています。

データセンターを評価する方法

ゼロ トラストのセキュリティモデルを構築するためには、最初に保護すべき最も価値の高い資産を優先し、それらのアセットにアクセスできるユーザーやそれらのアセットに対する最も大きなリスクを判断できるよう、データセンター内のアセットを把握して評価する必要があります。アセットにアクセスするユーザー、許可されたアプリケーション、ネットワーク自体を知ることで、何が必要で何を信頼できるのか評価し、正当なビジネス上の目的を持つユーザーアクセスおよびアプリケーションだけをネットワーク上で許可するデータセンターの最良のセキュリティポリシーを作成できるようになります。

1. データセンター環境全体を把握—サーバー、ルーター、スイッチ、セキュリティデバイス、その他のネットワーク インフラストラクチャを含め、物理・仮想データセンター環境全体、およびデータセンター アプリケーション（社内開発のカスタム アプリケーションを含む）およびサービス アカウント全体を把握します。

   - ネットワーク内での役割とビジネスにとっての重要性に基づいて各システムを評価し、どの物理・仮想インフラを最初に保護すべきか、優先順位を決めます。例えばクレジットカードのトランザクションが関わるビジネスの場合、クレジットカードのトランザクション、およびクレジットカード情報を運ぶトラフィックの通信経路を扱うサーバーは極めて重要なアセットであり、優先的に保護する必要があります。
   - 少なくとも 90 日間分のトラフィックログを検査し、データセンター ネットワークのアプリケーションの一覧を作成します。データセンターのアプリケーション データベースに基づいてカスタム レポートを作成し、既存のデータセンター アプリケーションを把握しやすくします。このデータセンター アプリケーションの一覧を使用し、社内開発のカスタムアプリケーションを含め、制限を設けたい、あるいはデータセンターネットワークで許容できるアプリケーションの許可リストを作成します。

     データセンターの最良のセキュリティ ルールベースのために構成したブロック ルールを監視することで、特定していないアプリケーションを発見できるため、最初のアプリケーションの一覧では、すべてのアプリケーションを特定する必要はありません。許可したいアプリケーションおよびアプリケーション タイプの一覧を作ることを重視してください。アプリケーション許可リストを作成し終えたら、明示的に許可していないすべてのアプリケーションが拒否されるようになります。

     各アプリケーションとビジネス要件を照らし合わせます。ビジネス要件と一致しないアプリケーションがあれば、ネットワーク上でそれを許可すべきか評価してください。明確なビジネス上の必要性がないアプリケーションは攻撃の入り口を広げ、攻撃者に利用されるおそれがあります。不要なアプリケーションが無害なものであっても、それを取り除いて攻撃者がエクスプロイトできる攻撃の入り口を減らすことがベストプラクティスになります。例えばファイル共有やインスタントメッセージなど、同じ機能を持つアプリケーションが複数ある場合、1 つか 2 つのアプリケーションに統一して攻撃の入り口を減らしてください。

     アプリケーションのデフォルト ポートを使用しない社内のカスタム アプリケーションが存在する場合、カスタム アプリケーションをサポートするために必要なポートおよびサービスに注意します。アプリケーションのデフォルト ポートを使用するように社内のカスタム アプリケーションを書き換えることを検討してみてください。

     同様の扱いが必要なネットワーク上のアプリケーション グループを作成し、個々のアプリケーションではなくアプリケーション グループに対して効率良くセキュリティポリシーを適用できるようにします。一度にグループ内のすべてのアプリケーションにポリシーを適用し足り、グループ全体のポリシーを変更したり、グループに新しいアプリケーションを追加してグループのポリシーを新しいアプリケーションに適用し足り、複数のセキュリティポリシールールでアプリケーション グループを再利用したりできるため、アプリケーション グループによってセキュリティポリシーの設計や実装が簡単になります。例えば、データセンターのストレージ アプリケーション用のアプリケー

ション グループに、crashplan、ms-ds-smb、NFS などのアプリケーションを含めることができます。
- データセンター内のサーバー内およびサーバー間で通信するためにアプリケーションが使用するサービス アカウントの一覧を作成します。複数の機能に対してではなく、各機能に対してサービス アカウントを一つ使用することがベストプラクティスになります。これにより、アクセスをサービス アカウントに限定し、システムのセキュリティが破られた場合にサービス アカウントがどのように使用されたのかを把握しやすくなります。もう一つのベストプラクティスは、アプリケーションにハードコーティングされたサービス アカウントを特定し、それらに対して IPS シグネチャを書いてアカウントの使用状況を監視することです。

2. データセンター トラフィックのカスタマイズ–データセンター トラフィックの特徴を知って位置づけを行うことで、ネットワーク全体やユーザーおよびリソース間をどのようにデータが流れるのか把握します。アプリケーション設計者、ネットワーク設計者、エンタープライズ設計者、事業の代表者などから成る、部門をまたいだチームで作業を行います。トラフィック フローの特徴を明確にすることで、ネットワーク トラフィックの送信元および宛先、典型的なトラフィック パターンおよび負荷をよく知り、ネットワーク上のトラフィックを把握して保護すべき最も重要なトラフィックを優先できるようになります。アプリケーション コマンドセンターウィジェット、Panorama のファイアウォール ヘルス モニタリング機能、通常の（ベースライン）トラフィック パターンを把握するための他の手段により、攻撃を示唆する異常なトラフィック パターンを把握しやすくなります。
3. データセンターのセグメント化を評価–データセンター サーバー層をセグメント化し、異なるサーバー層間の通信が必ず次世代ファイアウォールを経由し、最良のセキュリティポリシーによって復号化、検査、保護され、またユーザーあるいはインターネットからの通信が次世代ファイアウォールを経由するようにします。データセンターの外部でどのゾーンがデータセンターの各ゾーンと通信できるのか把握してから、データセンターの各ゾーンと通信しなければならないゾーンを決定します。
4. 一連のユーザーのセグメント化を評価し、データセンターにアクセスできるユーザーを決定–ユーザーをグループにマッピングし、センシティブなシステムへのアクセスを簡単に制御できるよう、一連のユーザーをセグメント化します。例えば、Product Management グループのユーザーが財務や人事部のシステムにアクセスできてはなりません。アクティブディレクトリ（あるいは使用する任意のシステム）で、正当なビジネス上の理由でユーザーに与える必要があるアクセス レベルに基づいて細かくグループを作成し、システムやアプリケーションへのアクセスを制御できるようにします。これには、必要なアクセス レベルに基づいてグループ化された異なる従業員グループ、契約者、提携企業、顧客、ベンダーのグループが含まれます。

   役割だけではなくアクセス要件も考慮してユーザーグループを作成することで攻撃の入り口を減らし、各グループにアプリケーションに対する最小限のアクセス レベルを付与します。マーケティングや契約者のような機能領域内で、アプリケーションのアクセス要件に対応する複数のユーザーグループを作成してください。
5. データセンターのネットワークを継続的に監視–データセンター トラフィックのログおよび監視を行い、データセンターの最良のセキュリティポリシーの漏れ、攻撃を示唆する異常なトラフィック パターンや予期せぬアクセスの試みを明らかにし、アプリケーションの問題を診断します。

アセットを評価するうえで役立つのはアセットのグループ化です。最初に保護すべき最も価値の高い資産を判断し、それらのアセットを保護した後で保護すべきアセットを決定していきます。各カテゴリーでアセットを保護する優先順位を決定します。ビジネスにとって最適な形でアセットを整理してください。次の表は一例であり、包括的なものではありません。また、保護すべきアセットの優先順位を決める際は、パスワード、個人情報、財務情報など、データの保護を求める規則に対するコンプライアンス要件も考慮してください。

表 **1 :** アセット カテゴリーの例

最も価値の高い資産	その他の価値の高い資産	他の資産（反復）
• 特許 • ソース コード	• ルーターやファイアウォールのインターフェイスなど、重要な IT インフラ	• ネットワーク実験装置 • IT 管理システム • その他の資産

最も価値の高い資産	その他の価値の高い資産	他の資産（反復）
• 製品の設計、医薬品の成分、ユーザーデータなどの機密情報。 • 独自のアルゴリズム • コードサイニング証明書および PKI（組織の暗号を守る鍵） • AD ドメインサーバー（AD を失うと、無制限にネットワークにアクセスできる認証情報を攻撃者が作成できるようになります） • ビジネスの強みとなる、非常に価値の高い他の資産	• 認証サービス • 電子メール • VPN（特に高度に分散されたエンタープライズ） • 不可欠なビジネス アプリケーション • ファイル共有サーバー • データベース	

資産の優先順位はビジネス毎に異なります。ユーザーエクスペリエンスが強みであるサービス企業にとっては、最高のユーザーエクスペリエンスを提供するためのアセットメーカーの場合は独自工程や自社開発の装置が最も価値の高い資産になるかもしれません。対象の資産を失った時の結果を想像してみることで、どの資産を最初に保護すべきなのかを判断しやすくなります。

データセンターのトラフィックを復号化する方法

見えなくて、検査できない脅威からネットワークを保護することはできません。典型的なネットワークトラフィックの大半が暗号化されており、またその量は増加しているため、トラフィックを復号化してマルウェアを明らかにすることが重要です。ネットワークへの侵入の隠匿、コマンドアンドコントロールマルウェアのインストール、暗号化を使用してデータの漏洩を行うマルウェアキャンペーンが増えています。

暗号化されたアプリケーションおよび脅威を明らかにするために、物理・仮想の次世代ファイアウォールをすべてのデータセンター トラフィックが見える位置に配置してください。可能なトラフィック、特にリスクの高いトラフィックカテゴリ、ビジネス上重要なトラフィック、および重要なサーバーに向かうトラフィックをすべて復号化してください。トラフィックを復号化することでそのトラフィックを識別し、ファイアウォールがアンチウイルス、脆弱性保護、WildFire、およびその他の脅威保護を適切に適用できるようになります。

復号化をトラフィックに適用するには、TLSおよびSSHトラフィックおよび復号化しない、あるいはできないトラフィックを扱う方法を指定する復号化プロファイルを作成します。復号化プロファイルは、トラフィックに対して許可するプロトコル、アルゴリズム、モード、セッションの性質を設定できます。復号化プロファイルは、ファイアウォールが復号化プロファイルを適用する対象となるトラフィックを指定する復号化ポリシー ルールに適用します。

ファイアウォールは 2 種類の SSL/TLS 復号化および SSH 復号化をサポートしています：

- SSL転送プロキシ（アウトバウンドトラフィック）
- SSLインバウンド検査（インバウンドトラフィック）
- SSHプロキシ（一般的にネットワークデバイスを管理する管理者の安全なアクセス用）

データセンター内でできるだけ多くの East-West トラフィックを復号化してください。ファイアウォールのサイジングが不適切であるためにパフォーマンスの懸念が生じてすべてのトラフィックを復号化できない場合は、最も重要なサーバー、リスクが最も大きいトラフィックのカテゴリー、最も信頼できないセグメントおよび IP サブネットを優先し、許容できるパフォーマンスを維持しつつできるだけトラフィックを復号化します。尋ねるべき重要な質問:「このサーバーのセキュリティが破られたらどうなるか？」、「各カテゴリーのトラフィックのリスクはどの程度か？」、「データセンター内で目標のパフォーマンスを達成するためにどの程度のリスクを取れるだろうか？」

データセンターからインターネットへと流れるトラフィックについては、例外の対象にしなければならないトラフィック以外はすべて復号化してください。データセンター内のサーバーが悪質なサイトに接続したり、悪意のあるファイルを転送したり、マルウェアのダウンロードに対して脆弱になったりするのは避けたいため、復号化が提供する可視性が特に重要です。

復号化ポリシーを計画する際、企業のセキュリティに関するコンプライアンス要件と位置づけを考慮してください。ユーザーからデータセンターへのトラフィックの場合、厳格な復号化ポリシーに対して最初は少し不満があがるかもしれませんが、これらの不満が、弱いアルゴリズムを使用していたり証明書に問題があったりしてブロックしている制限付きあるいは不適切なサイトに注意を向ける機会になります。ネットワーク上のトラフィックに対する理解を深めるツールとして苦情を利用してください。

また、復号化ポリシーで復号化ロギングを有効にして、リソースが許す場合は成功したSSLハンドシェイクと失敗したSSLハンドシェイクの両方をログに記録してください。復号化のモニタリングおよびトラブルシューティングツールを有効活用し、デプロイ環境を調査して、ポリシーとプロファイルをきめ細かく調整します。

トラフィックを復号化するとファイアウォールのリソースを消費します。復号化するトラフィックの量はデータセンター毎に異なります。復号化をサポートしつつ許容できるパフォーマンスを維持するためにファイアウォールのデプロイメントをサイジングする際は、復号化する予定であるトラフィックの量（一部のアプリケーションは復号化が必須であり、

復号化しなくても良いアプリケーションもあります）、復号化の暗号（堅牢で複雑な暗号の復号化には多くの処理能力が求められます）、キーのサイズ（大きなキーは多くの復号化リソースを消費します）、キー交換のタイプ（例えば、*RSA* キー交換は *PFS* キーの場合よりも多くの処理リソースを消費します）、ファイアウォールのキャパシティを考慮に入れてください。*Palo Alto Networks* の営業チームや担当者と協力し、お客様のネットワークに合わせてファイアウォールのデプロイメントを適切にサイジングすることで、トラフィックを復号化して脅威を明らかにすることができます。

極めて強固な秘密鍵のセキュリティが求められる銀行業などの企業の場合、ファイアウォール上に秘密鍵を保存するのではなく、サードパーティのハードウェア セキュリティ モジュール（HSM）を使用して企業の秘密鍵を保護・管理することができます。

- データセンターの最良の復号化プロファイルを作成
- 不適切なトラフィックをデータセンターの復号化から除外

データセンターの最良の復号化プロファイルを作成

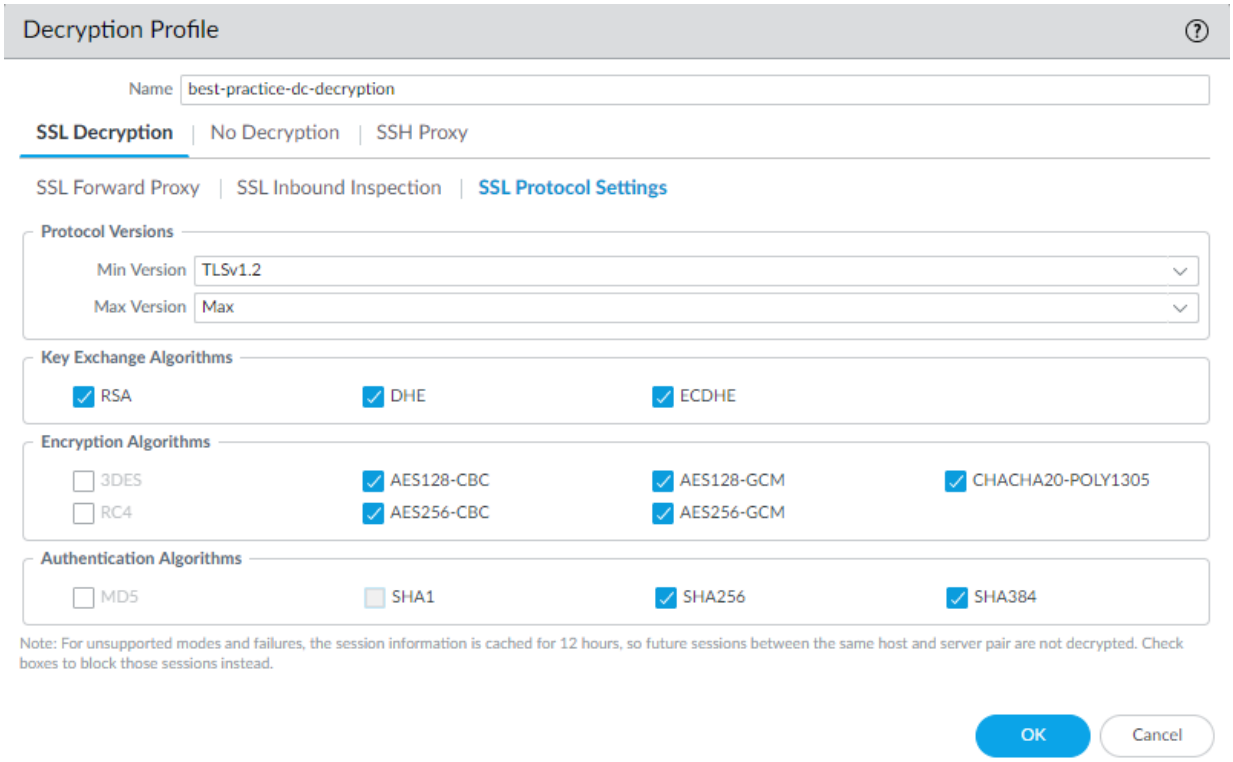
復号化プロファイルは、ファイアウォールが復号化されたトラフィックをチェックする方法、および復号化できない、あるいは復号化しないことにするトラフィックを指定します。ファイアウォールはプロトコル、サーバー証明書、セッションの特性、暗号（キー交換アルゴリズム、暗号化アルゴリズム、認証アルゴリズム）をチェックします。また、復号化プロファイル（**Objects**（オブジェクト）> **Decryption Profile**（復号化プロファイル））を復号化ポリシールール（**Policies**（ポリシー）> **Decryption**（復号化））に適用します。復号化ポリシー ルールは、送信元、宛先、サービス カテゴリ、URL カテゴリを一致条件として使用してチェックする対象のトラフィックを定義し、復号化プロファイルを適用するトラフィックを細かく制御できるようにします。ポリシールールに、復号化のロギングとログ転送も設定します。

アウトバウンド トラフィックを復号化するために、ファイアウォールは内部クライアントおよび外部サーバー間で転送プロキシデバイスとして機能します。ファイアウォールはインバウンドトラフィックを検査するためにインバウンドのセッション トラフィックのコピーを作成し、そのコピーを復号化して検査します。

STEP 1 | CRL/OCSP チェックを行うようにファイアウォールを設定し、復号化の際に必ず証明書の有効性を検証するようにします。

STEP 2 | TLSv1.0、TLSv1.1、SSLv3 などの脆弱な SSL/TLS バージョンをブロックし、RC4 や 3DES などの弱い暗号化アルゴリズムやMD5 ならびに SHA1 などの脆弱な認証アルゴリズムを拒否するために、**SSL Decryption**（**SSL** 復号化）> **SSL Protocol Settings**（**SSL** プロトコル設定）で設定を行います。

SSL プロトコル設定はすべての復号化されたトラフィックに適用されます。



弱いプロトコルをブロックするために、プロトコル**Min Version**（最小バージョン）を**TLSv1.2**に、また**Max Version**（最大バージョン）を**Max**（最大）に設定します。利用可能な最強の TLS プロトコルを使用します。個別の復号化ポリシーとプロファイルを作成して、最大限のセキュリティを確保します。たとえば、ビジネス目的で必要なレガシーサイトがそれより弱いプロトコルしかサポートしていない場合、別個の復号化プロファイルを作成してその弱いプロトコルを受け入れて、復号化プロファイル内で最低でもTLSv1.2 をサポートしていないサイトだけに適用します。これは、セキュリティとパフォーマンスをきめ細かく調整するために、強力なアルゴリズムおよび異なるURLカテゴリをサポートしていない、必要なビジネスサイトにも適用されます。

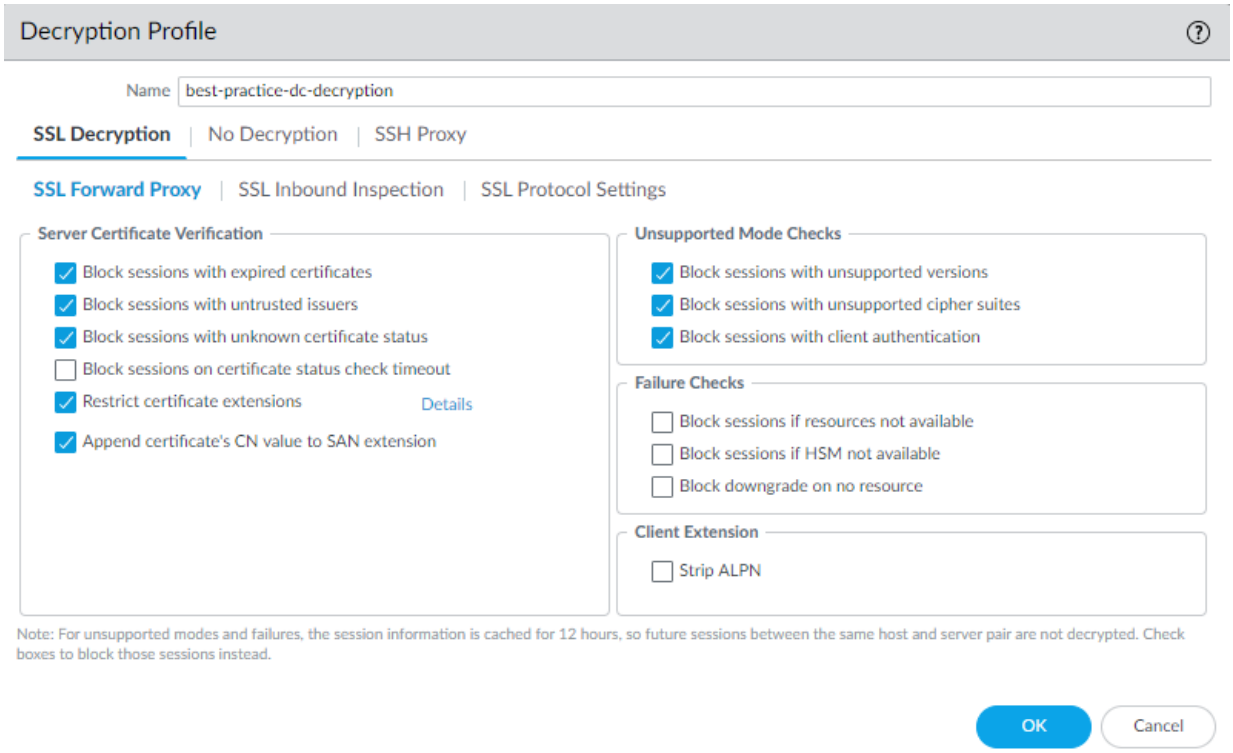
サイトが本当に必要なビジネス アプリケーションをホストしていない場合、そのサイトをサポートすることでセキュリティを低下させないでください。弱いプロトコルおよび暗号には、攻撃者がエクスプロイトできる既知の脆弱性が含まれています。そのサイトがビジネスにとって不要なサイト カテゴリーに属す場合、URL フィルタリングを使ってカテゴリー全体へのアクセスをブロックします。重要な古いサイトをサポートする必要性がない限り、弱いプロトコルや弱い暗号と認証アルゴリズムをサポートしないようにしてください。

Max Version (最大バージョン)は特定のバージョンではなく**Max** (最大)に設定し、プロトコルが改善される度に、ファイアウォールが自動的に最新かつ最高のプロトコルをサポートするようにしてください。インバウンド（SSL インバウンド インスペクション）あるいはアウトバウンド（SSL 転送プロキシ）トラフィックを制御する復号化ポリシー ルールに復号化プロファイルを付与する際、どちらの場合でも、弱いアルゴリズムを許可しないようにしてください。

多くのモバイルアプリケーションが*Pinning*された証明書(有効な証明書であっても見知らぬ証明書は受け入れない設定)を使用しています。*TLSv1.3*は証明書情報を暗号化するため、ファイアウォールはこれらのモバイルアプリケーションを*SSL Decryption Exclusion List*（*SSL*復号化除外リスト）に自動的に追加することはできません。これらのアプリケーションに対して、復号化プロファイルの*Max Version*（最大バージョン）が*TLSv1.2*に設定されていることを確認するか、またはトラフィックに対して*No Decryption*（復号化なし）ポリシーを適用します。

STEP 3 | アウトバウンド トラフィック用に**SSL Decryption**（**SSL** 復号化）> **SSL Forward Proxy**（**SSL** 転送プロキシ）の設定を行い、TLS ネゴシエートの際の例外、および復号化できないセッションをブロックします。

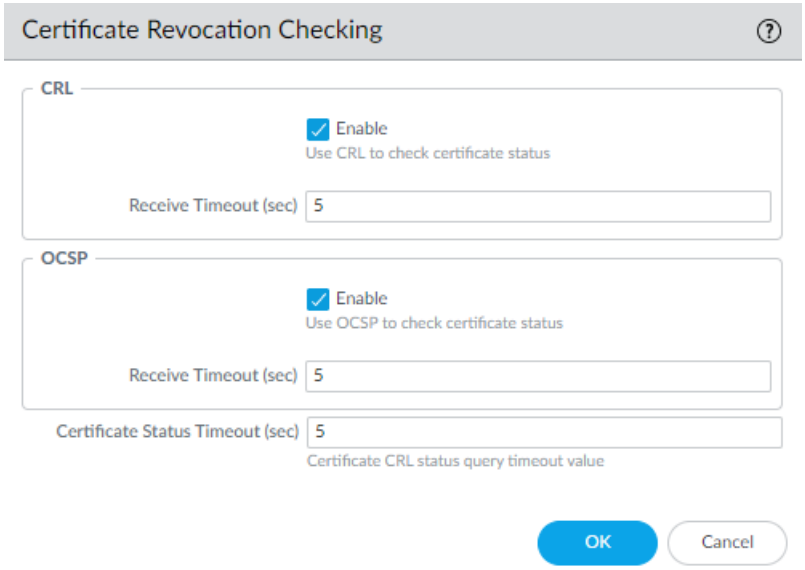
企業のセキュリティ コンプライアンス ルールによって最良の設定が異なるケースも一部あります。SSL 転送プロキシの復号化プロファイルを、アウトバウンド トラフィックを制御するセキュリティポリシールールに適用してください。



TLSネゴシエートの際の例外、および復号化できないセッションをブロックします。

- サーバー証明書の検証—強固なセキュリティと優れたユーザーエクスペリエンスの間にはトレードオフが存在するため、**Block sessions on certificate status check timeout**（証明書のステータスチェックのタイムアウト時にセッションをブロック）のボックスにチェックを入れるかどうかは、企業のセキュリティに関するコンプライアンス要件によって異なります。証明書ステータスの検証は、無効化サーバーの証明書無効リスト（CRL）を調べるか、あるいは発行者である CA が証明書

を取り消し、証明書を信頼できないかどうかをオンライン証明書ステータス プロトコル（OCSP）を使って判断します。しかし、証明書が有効な場合でも、無効化サーバーの応答が遅く、セッションのタイムアウトにつながり、ファイアウォールがセッションをブロックしてしまう可能性があります。**Block sessions on certificate status check timeout**（証明書のステータスチェックのタイムアウト時にセッションをブロック）し、かつ無効化サーバーの応答が遅い場合は、**Device**（デバイス）> **Setup**（セットアップ）> **Session**（セッション）> **Decryption Settings**（復号化設定）を使用して**Certificate Revocation Checking**（証明書無効化のチェック）をクリックし、デフォルトのタイムアウト値（5 秒）を別の値に変更できます。



サーバー証明書は CRL Distribution Point（CDP）拡張子内に CRL URL を、認証機関アクセス情報（AIA）証明書拡張子内に OCSP URL を含んでいる可能性があるため、CRL および OCSP 証明書の失効チェックの両方を有効化してください。

適切な証明書を使用することがベストプラクティスになりますが、サブジェクト代替名（SAN）フィールドが空になっている証明書が存在し、ファイアウォールが証明書を拒否する可能性があります。**Append certificate's CN value to SAN extension**（証明書の **CN** 値を **SAN** 拡張に付与）にチェックを入れ、SAN フィールドが空である場合に自動的に証明書番号を SAN フィールドにコピーさせることで、証明書の SAN フィールドを自動入力しないサイトを利用する際でも、証明書を許可できるようになります。そうしない場合、サイトが必要な流れに沿う証明書を再生成し、SAN フィールドを自動入力する必要があります。

他のサーバー証明書検証の例外はすべてブロックします。

- サポートされていないモード チェック—バージョンおよび Cipher Suite がサポートされていないセッションをブロックしない場合はユーザーに警告メッセージが送信され、それをクリックしていくことでリスクのあるウェブサイトにアクセスできるようになります。強固な SSL プロトコル設定を行う目的は、弱い（リスクのある）プロトコル バージョンおよびアルゴリズムを使用するサーバーをブロック· 防止することです。さらに、モード チェックがサポートされていないセッションをブロックすることで、悪意のあるバックドアや、カスタムおよび標準的でない暗号化を使用してアクティビティを隠蔽するその他の脅威を防止できます。

  クライアント認証を伴うセッションをブロックを使用すれば、クライアント認証を使用するセッションをブロックするか許可するかどうかを選択できます。セッションを確立するために使用できる認証はサーバー認証だけですが、セッションを確立するためにサーバーおよびクライアントの両方が認証を行う、相互認証を使用するサイトもあります。X.509 デジタル証明書を使用するクライアント認証とサーバー認証はどちらも信頼できる認証局が発行したデジタル証明書を使ってセッションを認証するため、その点で似ています。クライアント デバイス上にあるクライアント証明書はクライアントのデジタル識別子として機能し、他のデバイスにポートすることはできません。しかし、ファイアウォールが双方向の復号化を実行するためにはクライアントおよびサーバー証明書

の両方が必要ですが、ファイアウォールはサーバー証明書しか把握していないため、クライアント認証によってファイアウォールがセッションを復号化できなくなります。そのため、クライアント認証を伴うセッションの復号化が妨げられます。

クライアント認証を伴うセッションのブロックを有効化しない場合、クライアント認証を使用するセッションをファイアウォールが復号化しようとする際、ファイアウォールはセッションを許可し、サーバー URL/IP アドレス、アプリケーション、復号化プロファイルが含まれるローカルの除外キャッシュにエントリを追加します。このエントリは 12 時間キャッシュに残った後、失効します。同じユーザーあるいは別のユーザーが 12 時間以内にクライアント認証を使ってサーバーにアクセスすると、ファイアウォールはそのセッションを復号化除外キャッシュのエントリと照らし合わせ、トラフィックを復号化しようとせず、暗号化されたセッションを許可します。

除外キャッシュが一杯になると、新しいエントリが入る際にファイアウォールが最も古いエントリをパージします。復号化ポリシーあるいはプロファイルを変更する場合、ポリシーあるいはプロファイルを変更するとセッションの分類化の結果が変わることがあるため、ファイアウォールが除外キャッシュをフラッシュします。

クライアント認証を伴うセッションをブロックを有効にすると、ファイアウォールは SSL 復号化除外リスト（**Device**（デバイス）> **Certificate Management**（証明書管理）> **SSL Decryption Exclusion**（**SSL** 復号化除外））に含まれるサイトからのセッションを除き、クライアント認証を伴うすべてのセッションをブロックします。

SSL 復号化除外リストで事前定義済みのサイトに加え、クライアント認証を使用する他のサイトからネットワークに来るトラフィックを許可する必要があるかもしれません。クライアント認証を伴うセッションを許可する復号化プロファイルを作成してください。アプリケーションをホストするサーバーにのみ適用する復号化ポリシー ルールに、それを追加します。ログイン作業を完了するために多要素認証をユーザーに求めれば、セキュリティをさらに向上します。

他のすべてのトラフィックに対し、クライアント認証を伴うセッションをブロックする復号化プロファイルを適用します。

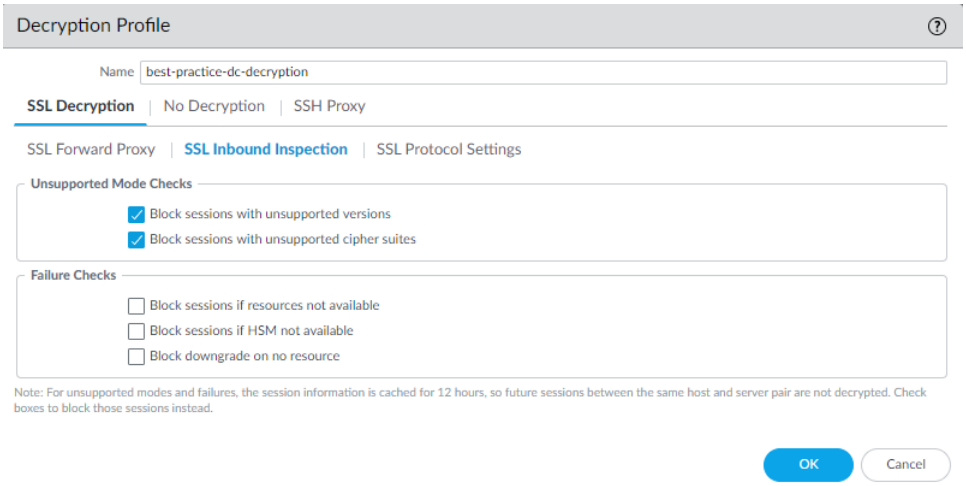
- 失敗のチェック–処理リソースの欠如により、危険な可能性のある接続を許可してしまうということが、**Block sessions if resources not available**（リソースが利用できない場合にセッションをブロック）しない場合のリスクです。リソースが利用できないセッションをブロックすると、ユーザーエクスペリエンスに影響を及ぼすおそれがあります。エラーチェックを実装するかどうかは、企業のセキュリティ コンプライアンスの内容や、強固なセキュリティと比べてユーザーエクスペリエンスがどの程度重要なビジネスなのかによって異なります。

  ハードウェア セキュリティ モジュール（HSM）を使って秘密鍵を保存する場合、**Block sessions if HSM not available**（**HSM** を利用できない場合にセッションをブロック）にチェックを入れるかどうかは、秘密鍵の取得元、および HSM を利用できない場合に暗号化されたトラフィックをどのように扱うのかという、企業のコンプライアンス ルールによって異なります。例えば、秘密鍵の署名に HSM を使うことを求める企業は、HSM が利用できない場合にセッションをブロックします。しかし、これに関してそこまで厳重でない企業は、HSM が利用できない場合でもセッションをブロックしないという選択もできます。（HSM がダウンしている場合、ファイアウォールは HSM からのレスポンスをキャッシュしているサイトの復号化は行えますが、それ以外は復号化できません）この場合のベストプラクティスは、企業のポリシーによって異なります。ビジネスにとって HSM が不可欠であれば、高可用性（HA）ペアで HSM を実行してください（PAN-OS 8.0 は単一の HSM HA ペアで 2 つのメンバーをサポートしています）。
- リソースなしへのダウングレードをブロック–ファイアウォールが利用できる TLSv1.3 処理リソースがない場合にファイアウォールによる TLSv1.3 から TLSv1.2 へのダウングレードを防ぎます。ダウングレードをブロックする場合、ファイアウォールでTLSv1.3リソースが不足すると、TLSv1.2にダウングレードする代わりに TLSv1.3を使用するトラフィックがドロップされます。ダウングレードをブロックしない場合、ファイアウォールが TLSv1.3リソースを使い果たすと、ファイアウォールは TLSv1.2にダウングレードします。しかし、ファイアウォールが処理するリソースを利用できない時にダウングレードをブロックすると、ユーザーが通常時にアクセスできるサイトが一時的にアクセス不可になるため、ユーザーエクスペリエンスが低下する可能性があります。このエラーチェックを実装するかどうかは、セキュリティコンプライアンスの立場や、強固なセキュリティと

ユーザー利便性のどちらを重要視するかによって異なります。TLS バージョンをダウングレードしたくない機密性の高いトラフィックの復号化を管理するために、個別の復号ポリシーとプロファイルを作成することを推奨します。

STEP 4 | **SSL Decryption**（**SSL** 復号化）> **SSL Inbound Inspection**（**SSL** インバウンド インスペクション）で設定を行い、外部クライアントから内部サーバーに向かうトラフィックを検査し、疑わしいセッションをブロックします。

インバウンドトラフィックを制御するセキュリティポリシールールに SSL インバウンド インスペクション復号化プロファイルを適用します。



- サポートされていないモード チェック—ファイアウォールは、自身がサポートしていないセッションのバージョンおよび暗号を復号化できません。攻撃者がサポートされていないバージョンおよび暗号を使ってネットワークに侵入するのを防ぐために、ファイアウォールがサポートしていないセッションのバージョンおよび Cipher Suite をブロックしてください。さらに、サポートされていないモード チェックを伴うセッションをブロックすることで、悪意のあるバックドアや、カスタムおよび標準的でない暗号を使ってアクティビティを隠蔽するその他の脅威を防ぐこともできます。

  サーバー上でファイアウォールがサポートしている暗号のみを有効化してください。この互換性を確保することで、クライアントおよびサーバー間のネゴシエーションがスムーズに行われるようになります。
- 失敗のチェック—処理リソースの欠如により、危険な可能性のある接続を許可してしまうということが、**Block sessions if resources not available**（リソースが利用できない場合にセッションをブロック）しない場合のリスクです。リソースが利用できないセッションをブロックすると、ユーザーエクスペリエンスに影響を及ぼすおそれがあります。エラーチェックを実装するかどうかは、企業のセキュリティ コンプライアンスの内容や、強固なセキュリティと比べてユーザーエクスペリエンスがどの程度重要なビジネスなのかによって異なります。

  ハードウェア セキュリティ モジュール（HSM）を使って秘密鍵を保存する場合、**Block sessions if HSM not available**（**HSM** を利用できない場合にセッションをブロック）にチェックを入れるかどうかは、秘密鍵の取得元、および HSM を利用できない場合に暗号化されたトラフィックをどのように扱うのかという、企業のコンプライアンス ルールによって異なります。例えば、秘密鍵の署名に HSM を使うことを求める企業は、HSM が利用できない場合にセッションをブロックします。しかし、これに関してそこまで厳重でない企業は、HSM が利用できない場合でもセッションをブロックしないという選択もできます。（HSM がダウンしている場合、ファイアウォールは HSM からのレスポンスをキャッシュしているサイトの復号化は行えますが、それ以外は復号化できません）この場合のベストプラクティスは、企業のポリシーによって異なります。ビジネスにとって HSM が不可欠であれば、高可用性（HA）ペアで HSM を実行してください（PAN-OS 8.0 は単一の HSM HA ペアで 2 つのメンバーをサポートしています）。

- リソースなしへのダウングレードをブロック–ファイアウォールが利用できる TLSv1.3 処理リソースがない場合にファイアウォールによる TLSv1.3 から TLSv1.2 へのダウングレードを防ぎます。ダウングレードをブロックする場合、ファイアウォールでTLSv1.3リソースが不足すると、TLSv1.2にダウングレードする代わりに TLSv1.3を使用するトラフィックがドロップされます。ダウングレードをブロックしない場合、ファイアウォールが TLSv1.3リソースを使い果たすと、ファイアウォールは TLSv1.2にダウングレードします。しかし、ファイアウォールが処理するリソースを利用できない時にダウングレードをブロックすると、ユーザーが通常時にアクセスできるサイトが一時的にアクセス不可になるため、ユーザーエクスペリエンスが低下する可能性があります。このエラーチェックを実装するかどうかは、セキュリティコンプライアンスの立場や、強固なセキュリティとユーザー利便性のどちらを重要視するかによって異なります。TLS バージョンをダウングレードしたくない機密性の高いトラフィックの復号化を管理するために、個別の復号ポリシーとプロファイルを作成することを推奨します。

STEP 5 | SSH トラフィックに対し、SSH プロキシ復号化プロファイル設定を構成します。

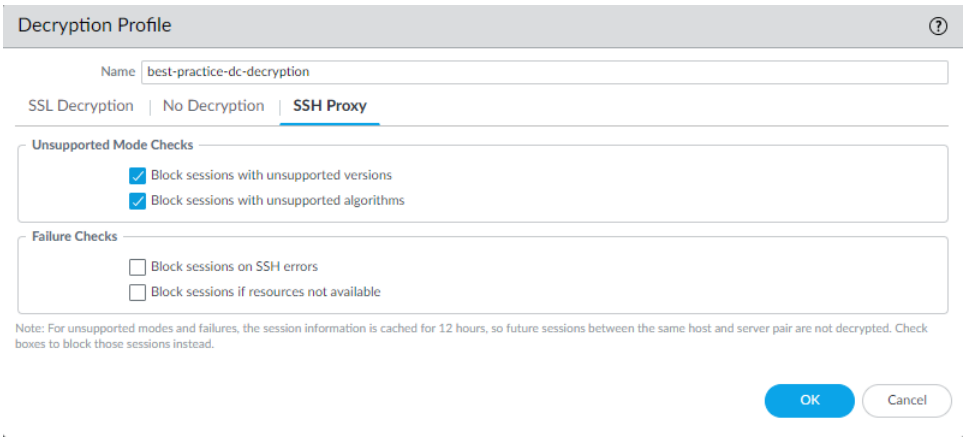
SSH 復号化は通常の方法でルーティングされた SSH トラフィックを許可し、SSH トンネル（SSH ポート転送）を拒否しますが、SSH トラフィックに対してコンテンツ検査や脅威検査を実行しません。SSH トンネル セッションは、X11 Windows パケットおよび TCP パケットをトンネル化できます。単一の SSH 接続に複数のチャネルが含まれている場合があります。SSH 復号化プロファイルをトラフィックに適用する際、接続に含まれる各チャネルについて、ファイアウォールがトラフィックの App-ID を検証し、チャネルのタイプを識別します。チャネルには次のタイプがあります：

- session
- X11
- forwarded-tcpip
- direct-tcpip

チャネル タイプが session である場合、ファイアウォールはトラフィックを、SFTP や SCP などの許可された SSH トラフィックとして識別します。チャネル タイプが X11、forwarded-tcpip、あるいは direct-tcpip である場合、ファイアウォールはトラフィックを SSH トンネル トラフィックとして識別し、それをブロックします。

ほとんどのユーザーグループに対しては、データセンター内で SSH トラフィックを許可しないでしょう。通常、SSH はサーバーへのリモート アクセスに使用し、Linux サーバー、ファイル転送に関して、データセンター サーバーを大きなリスクにさらすため、大抵のユーザーに対して使用する機能ではありません。SSH トラフィックは復号化できないため、データセンターのリソースに SSH でアクセスするユーザーをすべて信頼できなくてはなりません。さらにその場合でも、SSH アクセスを許可するすべてのルールにあらゆる脅威プロファイルを付与し、マルウェア、ウイルス、スパイウェアなどをスキャンする必要があります。

SSH を使用するユースケースの例は、データセンター サーバーの管理・保守を行い、SSH を使用してリモート アクセスを行う IT 部門の担当者です。

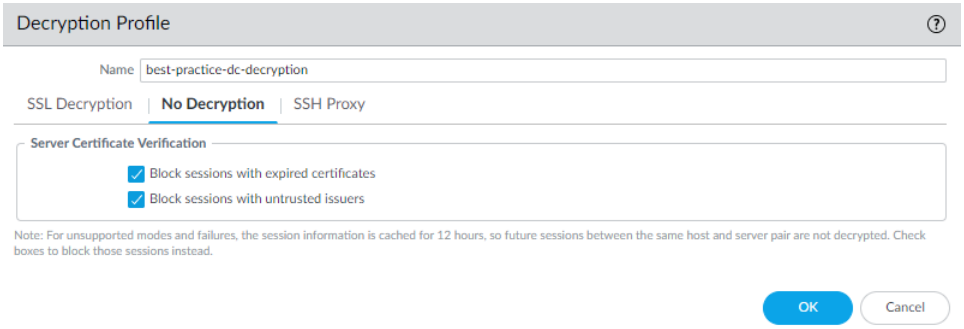


- サポートされていないモード チェック–ファイアウォールは、自身がサポートしていないセッションのバージョンおよび暗号を復号化できず、またサポートされていないバージョンや暗号に脆弱性がある場合があります。攻撃者がサポートされていないバージョンおよび暗号を使ってネットワークに侵入するのを防ぐために、ファイアウォールがサポートしていないセッションのバージョンおよび Cipher Suite をブロックしてください。さらに、サポートされていないモード チェックを伴うセッションをブロックすることで、悪意のあるバックドアや、カスタムおよび標準的でない暗号を使ってアクティビティを隠蔽するその他の脅威を防ぐこともできます。
- 失敗のチェック–処理リソースの欠如により、危険な可能性のある接続を許可してしまうということが、**Block sessions if resources not available**（リソースが利用できない場合にセッションをブロック）しない場合のリスクです。リソースが利用できないセッションをブロックすると、ユーザーエクスペリエンスに影響を及ぼすおそれがあります。エラーチェックを実装するかどうかは、企業のセキュリティ コンプライアンスの内容や、強固なセキュリティと比べてユーザーエクスペリエンスがどの程度重要なビジネスなのかによって異なります。

STEP 6 | 復号化しないことにしたトラフィックの場合は、**No Decryption**（復号化なし）の設定を行い、証明書の期限が切れている、あるいは発行者を信頼できない暗号化されたセッションがサイトに来るのをブロックします。

証明書のpinningなどの技術的な理由で復号化できないトラフィックではなく、規制やコンプライアンス規則の関係で復号化しないことにしたトラフィックにのみ非復号化プロファイルを適用します（そのトラフィックをSSL復号化除外リストに追加する）。データセンター トラフィックをできるだけ復号化することがベストプラクティスになります。

復号化しない *TLSv1.3* トラフィックの復号化ポリシーに復号化なしのプロファイルをアタッチしないでください。以前のバージョンとは異なり、*TLSv1.3* は証明書情報を暗号化するため、ファイアウォールは証明書データを可視化できません。そのため、期限切れの証明書や信頼できない発行者とのセッションをブロックできず、プロファイルは効果がありません。*(*これらのプロトコルは証明書情報を暗号化しないため、ファイアウォールは *TLSv1.2* 以前で証明書チェックを実行できますが、トラフィックに復号化なしのプロファイルを適用する必要があります。*)* ただし、復号化ポリシーがそのトラフィックを制御しない限り、ファイアウォールは復号化されていないトラフィックをログに記録しないため、復号化しない *TLSv1.3* トラフィックの復号化ポリシーを作成する必要があります。



不適切なトラフィックをデータセンターの復号化から除外

復号化が適さないトラフィックは次の 2 種類です：

- クライアント証明書認証の使用、証明書のピンニング、不完全な証明書チェーンなどの技術的な理由で復号化を妨げるトラフィック。
- 復号化しないことにしたトラフィック。

ファイアウォールは、技術的な理由で復号化を妨げる、頻繁に使用されるサイトを事前定義した SSL 復号化除外リスト（**Device**（デバイス）> **Certificate Management**（証明書管理）> **SSL Decryption Exclusion**（**SSL** 復号化除外））を提供します。サイトのホスト名の隣にあるチェックボックスをクリックしてから**Disable**（無効）をクリックすることで、事前定義済みのサイトをリストから削除したり、サイトをリストに追加したりできます。技術的な理由で復号化を妨げるサイトに対してのみ復号化除外リストを使用し、復号化しないことにしたサイトには使用しないでください。復号化によって重要なアプリケーションが妨げられる場合は、それを復号化除外リストに追加し、特定の IP アドレス、ドメイン、あるいはそのアプリケーションに関連する証明書内の共通名に対する例外を作成します。復号化によって妨げられる場合がある内部カスタム アプリケーションも存在します。

復号化プロファイルで**Unsupported Modes**（非サポートモード）（クライアント認証、非サポートのバージョン、または非サポートの暗号スイートとのセッション）が許可されている場合、ファイアウォールは、Local Decryption Exclusion Cache（ローカル復号化除外キャッシュ）（**Device**（デバイス）> **Certificate Management**（証明書管理）> **SSL Decryption Exclusion**（**SSL**復号化除外）> **Show Local Exclusion Cache**（ローカル除外キャッシュ表示））に、許可された非サポートモードを使用するサーバーとアプリケーションを自動追加します。サポートされていないモードをブロックすると、セキュリティが向上しますが、それらのモードを使用するアプリケーションとの通信もブロックされます。

復号化からサイトを除外する技術的な理由が、不完全な証明書チェーンの場合、復号化ログの情報を使って不完全な証明書チェーンを修復して、トラフィックを許可、復号化、および検査できるようにすることができます。

規制や法的要件などの理由でトラフィックを復号化しない場合もあります。例えば、欧州（EU）一般データ保護規則（GDPR）はあらゆる個人のすべての個人データを厳重に保護することを求めています。GDPR は海外企業を含めて、EU 内の居住者の個人データを収集あるいは処理するすべての企業に適用されます。異なる規制やコンプライアンスのルールが存在するため、同じデータの扱い方を国や地域毎に変えなければならないことがあります。通常、企業は情報を所有しているため、個人情報を社内のデータセンターで復号化できます。トラフィックをできるだけ復号化し、可視性を高めてセキュリティ保護を適用するのがベストプラクティスになります。

トラフィックを復号化しないことにした場合は、本当に復号化しなくて良いか確認してから、アプリケーション、ユーザーグループ、送信元および宛先、URL カテゴリおよび/またはサービスを指定するポリシーベースの例外を作成し、例外をできるだけ限定してください。復号化から除外しなくても良いトラフィックを意図せず除外してしまうことがなくなるため、復号化除外は詳細なほど優れたものになります。

データセンターのセグメント化戦略を作成

ネットワークへのアクセスを掌握した攻撃者が横方向に移動して重要なシステムを攻撃できるため、セグメント化していないフラットなネットワークを保護することは容易ではありません。企業が最も価値の高い資産を保存しているデータセンター内部の場合、特にこれが該当します。VLAN のような古いセグメント化手法は上手くスケーリングできず、自動化が難しく、またユーザー、コンテンツ、アプリケーションを加味しないため、トラフィックに対する制御や可視性をほとんど得られません。

データセンターのリソースに対するより細かなアクセス制御を可能にするセグメント化戦略を作成することで、トラフィックに対する可視性が向上します。トラフィックはセグメント間を移動する際にファイアウォール（セグメンテーション ゲートウェイ）を通過しなければならないため、より細かなセグメント化戦略により、トラフィックに対する優れた可視性を得られます。また、個人情報に対する必要なアクセス以外を防止し、データを保護しつつ監査の対象を減らせるため、セグメント化によりコンプライアンスの遵守やコンプライアンス監査も容易になります。

データセンターのセグメント化戦略は組織のアーキテクチャやビジネス ゴールによって異なるため、「万能な」実装方法はありません。しかし、一般的なガイドラインを学ぶことで、セグメント化戦略の設計·実装を通じてデータセンターのネットワークを保護できるようになります。

- データセンターをセグメント化する方法
- データセンター アプリケーションをセグメント化する方法

データセンターをセグメント化する方法

データセンターをセグメント化する方法は、セグメント化の方法を決定づける SDN ソリューションなどを含めて、ビジネス要件やデータセンターのネットワークのアーキテクチャによって異なります。例えば、vwire インターフェイスはNSX ホスト上のファイアウォールの接続性を制御します。各 vwire インターフェイスは NSX ホスト上でトラフィックをルーティングしたりスイッチングしたりせず、同じゾーンに属す必要があるため、特定のテナント（部門、顧客、アプリケーション層）用のすべてのリソースが単一のゾーン内に存在しなければならず、ファイアウォールがダイナミック アドレス グループを使ってそのゾーン内のアプリケーション トラフィックをセグメント化する必要があります。各テナントは、自身の vwire インターフェイスを持つ別々のゾーンを持っています。他の SDN ソリューションの場合、個別の仮想ファイアウォール インスタンスがトラフィックをセグメント化できます。

Palo Alto Networks の次世代ファイアウォールは、トラフィックをセグメント化するための柔軟なツールを提供します：

- ゾーン—複数のゾーンをまたがるトラフィックはファイアウォールを経由し、検査されます。許可されたすべてのデータセンター通信はファイアウォールを経由し、完全な脅威検査（アンチウイルス、アンチスパイウェア、脆弱性保護、ファイル ブロッキング、WildFire 分析、エンタープライズ外に出るデータセンター トラフィックおよび顧客のテナントがホストするアプリケーションに対する URL フィルタリング）の対象にする必要があります。デフォルトでは、ファイアウォールはゾーン間のすべてのトラフィック（イントラゾーン トラフィック）を拒否します。明示的に許可したトラフィックだけがゾーン間を移動できるようにするために、トラフィックを許可する具体的なセキュリティポリシールールを作成する必要があります。データセンターをセグメント化するためにゾーンを使用する方法は、どのようなアセットを他のアセットと区別しなければならないのかによって異なります。例えば、開発用サーバーと本番用サーバーでゾーンを分けるというのが良くあるアーキテクチャの一つです。支払いカード情報（PCI）や個人の ID 情報（PII）などの極めてセンシティブな情報を保管するサーバーをセグメント化したり、マーケティング、エンジニアリング、人事のような社内の各部門をセグメント化したり、顧客のリソースや顧客がホストするアプリケーションをセグメント化したりするためにゾーンを使用できます。

  ゾーン プロテクション プロファイルを使用し、各ゾーンをフラッド、偵察行為（ポートスキャンおよびホスト スイープ）、レイヤー 3 のパケット ベースの攻撃、非 IP プロトコル（レイヤー 2）のパケット ベースの攻撃から保護します。

- ダイナミック アドレス グループ—この目的の場合、ファイアウォールが静的ではなく動的にサーバーグループを定義するためにセキュリティポリシーにインポートして使用する IP アドレスのリストになるのがダイナミック アドレス グループです。IP アドレスをダイナミック アドレス グループに追加したり削除したりするとセキュリティポリシーが自動的に更新され、ファイアウォール上でコミット操作を行う必要はありません。ゾーン内でセキュリティポリシー許可ルール中のダイナミック アドレス グループを使用することで、指定したアプリケーションおよびサービスのためのサーバー同士のやり取りが可能になります。例えば NSX にて、ダイナミック アドレス グループを使用して単一のアプリケーション層内のサーバー層をセグメント化します。
- **User-ID**—ユーザーグループに基づいてアプリケーション許可ルールを作成するために User-ID を有効化し、アプリケーションおよびサーバーグループからのユーザーをセグメント化します。

データセンターのセグメント化を計画する際は、次の一般的なガイドラインを考慮してください：

- データセンターにアクセスする方法。段階的にセグメント化を行い、最も価値が高くセンシティブな資産を最初に保護するためです。
- データセンター内で SDN ソリューション（NSX、ACI、OpenStack など）を使用し、スケーラブルかつアジャイルな仮想インフラを実現します。データセンターのネットワークの管理を一元化し、計算処理リソースの使用量を最大化し、ネットワークのスケーリング・自動化を行い、仮想ネットワーク上のトラフィックを制御・保護するうえで、SDN が最適な方法になります。根本的に SDN と同じアーキテクチャを持つ非 SDN のアーキテクチャを構成することも可能ですが、それは難しく時間がかかり、エラーが発生して機能停止につながりやすく、ベストプラクティスとは言えません。SDN ソリューションはセキュリティを犠牲にする事なく、背後にあるデータセンターの計算処理リソースを最大限に使用できるようにします。
- 仮想的でない古いサーバーは物理的な次世代ファイアウォールを使用して、仮想的なデータセンターのネットワークは VM-Series ファイアウォールを使用してセグメント化および保護します。
- 類似の機能を果たす各アセットをグループ化し、同じデータセンターのセグメント内で同じセキュリティ レベルを求めます。例えば、インターネットに接続する各サーバーを同じセグメントに配置します。

複数の基準に基づいてセグメント化の計画を立て、お客様のビジネスを保護できる適切な計画を作成してください。

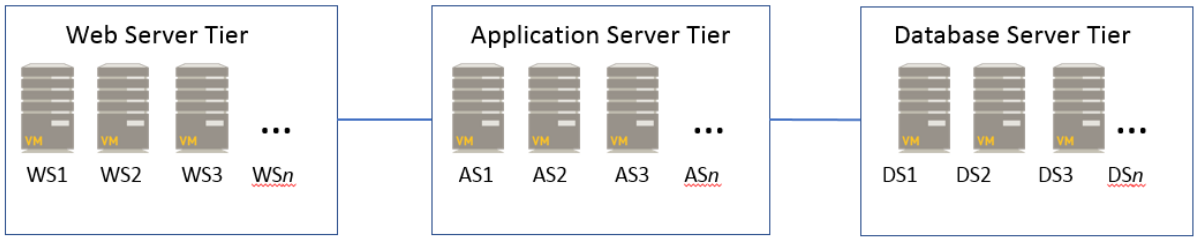
データセンター アプリケーションをセグメント化する方法

データセンター アプリケーションをセグメント化してマルウェアがアプリケーション間を移動するのを防ぎ、ユーザーがそれらのアプリケーションを安全に使用できる状態にします。データセンター アプリケーションに必要なリソースや機能を提供するのがアプリケーション層です。アプリケーション層は、特定のアプリケーションに関連するリクエストやコマンドに協力して対応する複数のサーバー層で構成されます。通常、アプリケーション層は次の 3 つのサーバー層で構成されます：

- *Web* サーバー層—ユーザーに対するアプリケーション インターフェイスです。
- アプリケーションサーバー層—Web サーバー層からリクエストを処理してアプリケーションの機能を実現します。
- データベースサーバー層—アプリケーションが機能するために必要なデータを持っています。

アプリケーション層がアプリケーションをユーザーに提供できるようにするために、各サーバー層には互いに協力する機能的に似たサーバーが複数含まれています。

Typical Application Tier



各アプリケーション層内のサーバー層は VM のサービス チェーンを構成します。サービス チェーンはトラフィックを仮想データセンター アプリケーションに誘導してアプリケーション サービスを提供します。アプリケーション層内で、Web サーバーはアプリケーションのコードをホストするアプリケーションサーバーと通信でき、そのアプリケーションサーバーはコンテンツをホストするデータベースサーバーと通信できます。これら 3 つのサーバー (単一のアプリケーション層内の異なるサーバー層内に存在) 間の通信がサービス チェーンになります。

データセンターには、特定の部門、顧客、契約者、その他のグループ専用のアプリケーション層が多く含まれています。データセンターのアプリケーション インフラストラクチャをセグメント化し、アプリケーション リソース間の不正・不要な通信を防ぎ、アプリケーション トラフィックを検査してください。

アプリケーションのセグメント化	アプリケーションをセグメント化する方法
アプリケーション層	各サーバー層に対して別々のファイアウォール ゾーンを構成することで各アプリケーション層内のサーバー層をセグメント化し、一連の各サーバーへのアクセスを制御し、各サーバー層間を流れる際にファイアウォールを通過するトラフィックを検査できるようにします。例えば、WEB サーバー、アプリケーションサーバー、データベースサーバーを別々のゾーンに配置し、サーバー層間のトラフィックが必ず次世代ファイアウォールを通過して完全に検査されるようにします。 ビジネス要件によっては、テナントを分けたり、負荷分散を行ったり、異なる目的毎にアプリケーション層を使ったり、複数のセキュリティ レベルを提供したり、異なる一連のサーバーに接続したりするために、複数のゾーンを作成しなければならない場合があります。同様の信頼度が必要であり、同様のアプリケーション層と通信しなければならない同じゾーン内のサーバーをグループ化することで、各アプリケーション層の攻撃の入り口を減らすために、データセンターをセグメント化してください。
Web サーバー層	管理目的でデータセンター サーバーに安全な方法で直接アクセスする IT 部門などの特別な場合を除き、通常、トラフィックは Web サーバーを通じてデータセンターに入ります。他のサーバー層と同様に、Web サーバー層用に別のゾーンを作成し、細かなセキュリティポリシーを適用できるようにします。 Web サーバー層はデータセンター外にあるデバイスと通信するため、攻撃者の格好の標的になります。例えば VLAN などを使用し、Web サーバー層を別のネットワークに配置します。VLAN を出入りするすべてのトラフィック (データセンターを出入りするすべてのトラフィック) は、次世代ファイアウォールを通過する必要があります。これは、次世代ファイアウォールをデフォルトゲートウェイとして構成するか、トラフィックを誘導する NSX などの SDN ソリューションを使用すれば実現できます。 Web サーバー層内のサーバーをセグメント化し、例えば、*NSX* が配布されたファイアウォール (*DFW*) のような伝統的なルールを使用してポートを開くか層内のトラフィックをブロックすることで、サーバーがお互いに通信するのを防ぎます。

アプリケーションのセグメント化	アプリケーションをセグメント化する方法
インフラストラクチャ サービス アプリケーション サーバー	DNS、DHCP、NTP などの重要なインフラストラクチャ サービスを提供するサーバーをセグメント化し、適切なアプリケーションを使用する特定の IP アドレスへのアクセスのみを許可します。
アプリケーション [applications]	App-IDを使用し、各アプリケーションにどのユーザーがどの一連のサーバーを使って（ダイナミック アドレス グループを使用）アクセスできるのかを制御することでアプリケーションをセグメント化するアプリケーションベースの許可リストセキュリティポリシールールを作成します。App-ID により、同じ計算処理リソース上にありながら異なるセキュリティ レベルやアクセス制御を要する各アプリケーションに細かなセキュリティポリシールールを適用できるようになります。 専有アプリケーションおよびセグメント アクセスを一意に識別するカスタム アプリケーションを作成します。一連のポート用のカスタム セッション タイムアウトを定義するだけの目的で作成した既存のアプリケーション オーバーライド ポリシーがある場合、サービスベースのセッション タイムアウトを設定して各アプリケーションのカスタム タイムアウトを管理してからルールをアプリケーション ベースのルールに移行することで、既存のアプリケーション オーバーライド ポリシーをアプリケーション ベースのポリシーに変換します。アプリケーション オーバーライド ポリシーはポートベースです。アプリケーション オーバーライド ポリシーを使用して一連のポートのカスタム セッション タイムアウトを管理する際、それらのフローに対するアプリケーションの可視性が失われるため、どのアプリケーションがポートを使用するのか把握することも、管理することもできません。サービスベースのセッション タイムアウトはアプリケーションの可視性も維持しつつ、カスタム タイムアウトを利用できるようにします。 カスタム アプリケーション タイムアウトを伴うポート ベースのセキュリティポリシーからアプリケーション ベースのポリシーに移行する場合は、アプリケーションに対する可視性が失われるため、アプリケーション オーバーライド ルールを使用してカスタム タイムアウトを管理しないでください。その代わりに、各アプリケーションのカスタム タイムアウトを管理するサービスベースのセッション タイムアウトを定義してから、ルールをアプリケーション ベースのルールに移行します。

次世代ファイアウォールを使って特定のサーバー層内のサーバーをセグメント化しないでください。単一のサーバー層内のサーバーが互いに通信するのを防止する必要がある場合は、NSX DFW などの伝統的なルールを使用し、ポートを開くか層内のトラフィックをブロックします。しかし、単一のサーバー層内の各サーバーが互いに通信しなければならないことも多くあります。例えばデータベースサーバー層が、互いに自由に通信できなければならないサーバー クラスタとして構成されている場合があります。

データセンターの最良のセキュリティポリシーを作成する方法

ネットワーク上で許可するトラフィックに潜む脅威をスキャンすることで、基盤となる保護を提供するのがセキュリティ プロファイルです。セキュリティ プロファイルは、ピアツーピアのコマンド アンド コントロール（C2）アプリケーション トラフィック、危険なファイル形式、脆弱性をエクスプロイトしようとする試み、アンチウイルス シグネチャをブロックし、新規および未知のマルウェアを特定する一連の連携する脅威防止ツール一式を提供します。

セキュリティポリシー許可ルールに追加するだけで良い事前定義済みのプロファイルを Palo Alto Networks が提供しているため、セキュリティ プロファイルは比較的簡単に適用できます。事前定義済みのプロファイルをクローンして編集すれば良いため、セキュリティ プロファイルは簡単にカスタマイズできます。当然、ファイアウォールあるいは Panorama 上で一からセキュリティ プロファイルを作成することもできます。

ネットワーク トラフィック内の既知および未知の脅威を検出するために、ネットワーク上のトラフィックを許可するすべてのセキュリティポリシールールにSecurity Profiles（セキュリティ プロファイル）を付与し、許可されたすべてのトラフィックをファイアウォールに検査させます。ファイアウォールはセキュリティポリシー許可ルールにマッチしたトラフィックにセキュリティ プロファイルを適用し、セキュリティ プロファイルの設定に基づいてトラフィックをスキャンしてから、適切なアクションを実行してネットワークを保護します。最良のセキュリティ プロファイルに関する推奨事項は、明記されているものを除き、4 つすべてのデータセンター トラフィックにも適用されます。

コンテンツ更新を自動的にダウンロードしてできるだけ早くインストールし、ファイアウォールの脅威防止シグネチャおよびコンテンツ（アンチウイルス、アンチスパイウェア、脆弱性、マルウェアなど）を最新に保ち、新しい脅威をブロックできるようにしてください。

- データセンターの最良のアンチウイルス プロファイルを作成
- データセンターの最良のアンチスパイウェア プロファイルを作成
- データセンターの最良の脆弱性保護プロファイルを作成
- データセンターの最良のファイルブロッキングプロファイルを作成
- データセンターの最良の WildFire 分析プロファイルを作成

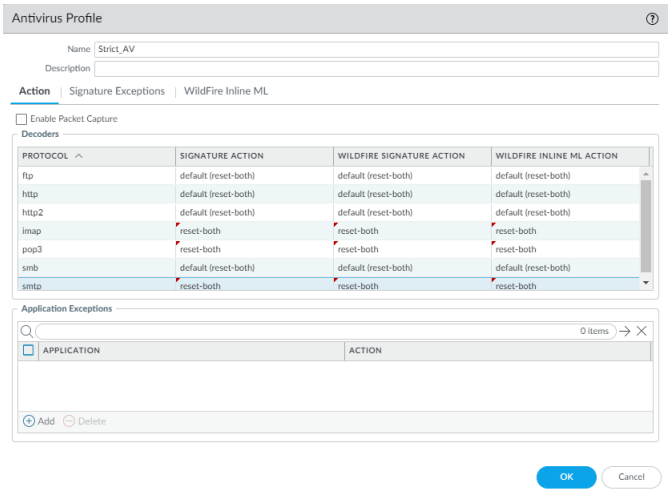
*1*つまたは複数のセキュリティプロファイルグループを作成し、プロファイルを個別に指定する代わりに、すべてのプロファイルをセキュリティポリシールールにまとめて適用できるようにします。

インターネットに直に接続するアウトバウンド接続がない場合、データセンター ファイアウォールのURL フィルタリングは不要です。PAN-DB URL フィルタリング ソリューションはプライベート データセンターの URL ではなくインターネット URL を識別し、PAN-DB データベースのインポートとそれに対する URL のチェックはデータセンター トラフィックに適用されないため、インターネットに直接接続しないファイアウォールは PAN-DB URL フィルタリング ソリューションを必要としません。ファイアウォールが URL トラフィックを持っているのか定かでない場合、試用版の URL フィルタリング サブスクリプションを入手し、すべての URL カテゴリに対してアラートするようプロファイルを設定し、URL トラフィックを識別してください。そうしない場合、データセンターの境界ではなく、ユーザートラフィックがネットワークを出入りするネットワークの境界に位置するファイアウォール上で URL フィルタリングを行う必要があります。カスタム URL カテゴリを作成（**Objects**（オブジェクト）> **Custom Objects**（カスタム オブジェクト）> **URL Category**（**URL** カテゴリ））し、内部のデータセンターのウェブサービスへのアクセスを識別・制御してください。

データセンターの最良のアンチウイルス プロファイルを作成

デフォルトのアンチウイルス プロファイルを複製し、編集します。ビジネス的に重要なアプリケーションを確実に利用できるように、現在の状況からベストプラクティスのプロファイルに移行する際には、安全な移行手順を実施してください。ベストプラクティスのプロファイルを実現するために、デフォルトのプロファイルをここで説明する方法で修正し、トラフィックを許可するすべてのセキュリティポリシールールにそれを適用します。アンチウイルスプロファイルには、次の7つのプロトコルを介して転送されるウイルスおよびマルウェアを検出して防止するプロトコルデコーダーが備わっています：FTP、HTTP、HTTP2、IMAP、POP3、SMB、および SMTP。アンチウイルスプロファイルはWildFireシグネチャとインライン機械学習モデルに基づいてアクションも適用するため、7つのプロトコルすべてに対してWildFireアクションを設定できます。

クローンした最良のアンチウイルスプロファイルを7つのすべてのプロトコルデコーダーおよびWildFireアクションをクライアントとサーバーの両方をリセット(reset-both)するよう設定した後、4つのデータセンタートラフィック フロー用の許可ルールにプロファイルを付与します。



セル左上の赤い三角はアクションが修正（デフォルトから変更）されたことを示し、修正されたプロファイルの名前は**Strict_AV**です。

トラフィックを許可するすべてのセキュリティポリシールールに最良のアンチウイルスプロファイルを付与して、ネットワークに侵入しようとする悪意のある既知のファイル（マルウェア、ランサム攻撃ボット、ウイルス）をブロックします。以下に例を示します。

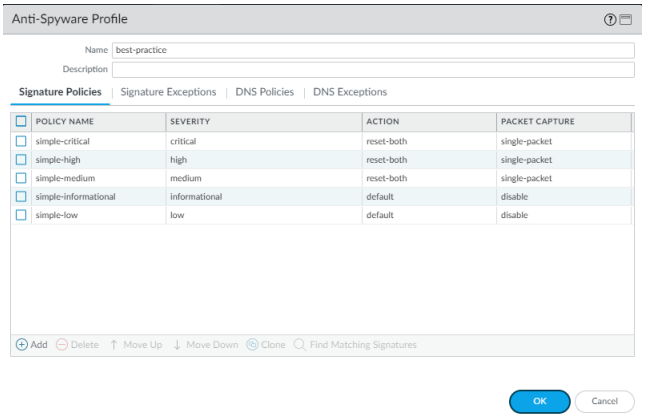
- イントラ データセンター トラフィック—攻撃者が脆弱性をエクスプロイトしてマルウェアやハッキング ツールをデータセンター ネットワーク内のサーバー間で横方向に蔓延させるのを防止するうえで、アンチウイルス プロファイルおよび脆弱性保護プロファイルが役立ちます。
- データセンターからインターネットへのトラフィックの場合—コマンド アンド コントロール トラフィック、マルウェアの最初のダウンロード、ハッキング ツールを特定およびブロックするうえで、アンチウイルス プロファイルおよびアンチスパイウェア プロファイルが役立ちます。

データセンターの最良のアンチスパイウェア プロファイルを作成

データセンター トラフィックを許可するすべてのセキュリティポリシールールにアンチスパイウェア プロファイルを付与します。アンチスパイウェア プロファイルは、アドウェア、バックドア、ブラウザ ハイジャック、データ盗難、キーロギングなどのカテゴリーを含めて、サーバーあるいはエンドポイントにインストールされたスパイウェアが開始するコマンド アンド コントロール（C2）トラフィックを検出し、侵入されたシステムがネットワークの外部と接続を確立するのを防ぎます。

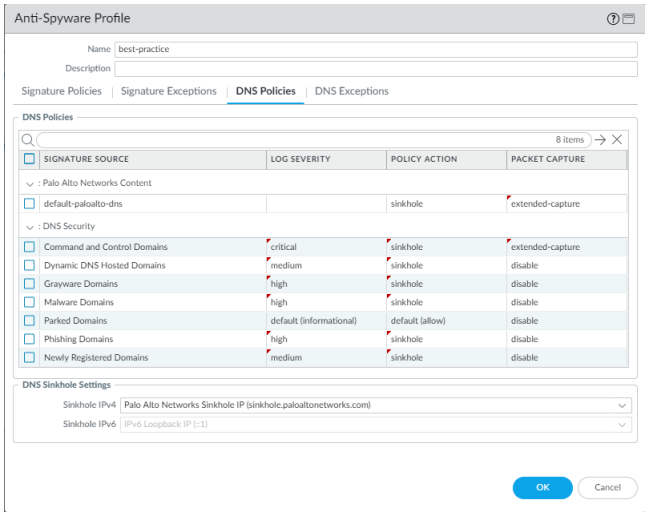
事前に設定された厳格なアンチスパイウェアプロファイルを複製し、編集します。ビジネス的に重要なアプリケーションを確実に利用できるように、現在の状況からベストプラクティスのプロファイルに移行す

る際には、安全な移行手順を実施してください。分析を行うためにトラフィックを送信できるシンクホールをセットアップしている場合、パケット キャプチャを伴う DNS シンクホールを有効化することで、悪意のあるドメインを解決しようと試みたエンドポイントを追跡しやすくなります。最良のアンチスパイウェア プロファイルではデフォルトの**Action**（アクション）をそのままにし、ファイアウォールが中、高、重要の重大度を持つ脅威を検出した際に接続をリセットするようにし、それらの脅威に対する単一のパケット キャプチャ（PCAP）を有効化します。



通知のアクティビティは比較的大量のトラフィックを生成し、かつ潜在的な脅威の場合よりも役立たないため、通知のアクティビティに対して PCAP を有効化しないでください。拡張 PCAP（単一 PCAP ではなく）を、**alert**（アラート）アクションを適用する高価値のトラフィックに適用します。ログに記録するトラフィックを指定するために使用するロジックと同じものを使用する PCAP を適用します（ログに記録するトラフィックの PCAP を取ります）。単一 PCAP をブロックするトラフィックに適用します。拡張 PCAP が記録して管理プレーンに送信するデフォルトのパケット数は 5 パケットであり、これが推奨される値になります。大抵の場合、5 つのパケットをキャプチャすれば脅威を分析するのに十分な情報を得られます。過剰な PCAP トラフィックが管理プレーンに送信される場合、5 つよりも多くパケットをキャプチャすると PCAP がドロップされるおそれがあります。

既知の悪意のあるドメインに対する DNS クエリをブロックあるいはシンクホールし、DNS クエリに対する可視性がない場合に PCAP を有効化するのが、ベストプラクティスの**Action on DNS Queries**（**DNS** クエリに対するアクション）になります。



DNS シンクホールを有効化すれば、ホストを追跡し、それらが疑わしいドメインにアクセスできないようにすることで、疑わしいドメインにアクセスしようと試みる侵入された可能性があるホストを特定できます。ファイアウォールが DNS クエリの送信者を把握できない場合（通常、ファイアウォールがローカル DNS サーバーの North にあたる場合）に DNS シンクホールを有効化することで、感染ホストを特定で

きるようにします。ファイアウォールが DNS クエリの送信者を把握できる場合（通常、ファイアウォールがローカル DNS サーバーの South にあたる場合。このケースでは、ファイアウォールのブロッキングルールおよびログにより、トラフィックに対する可視性が得られます）あるいはブロックするトラフィックの場合は DNS シンクホールを有効化しないでください。

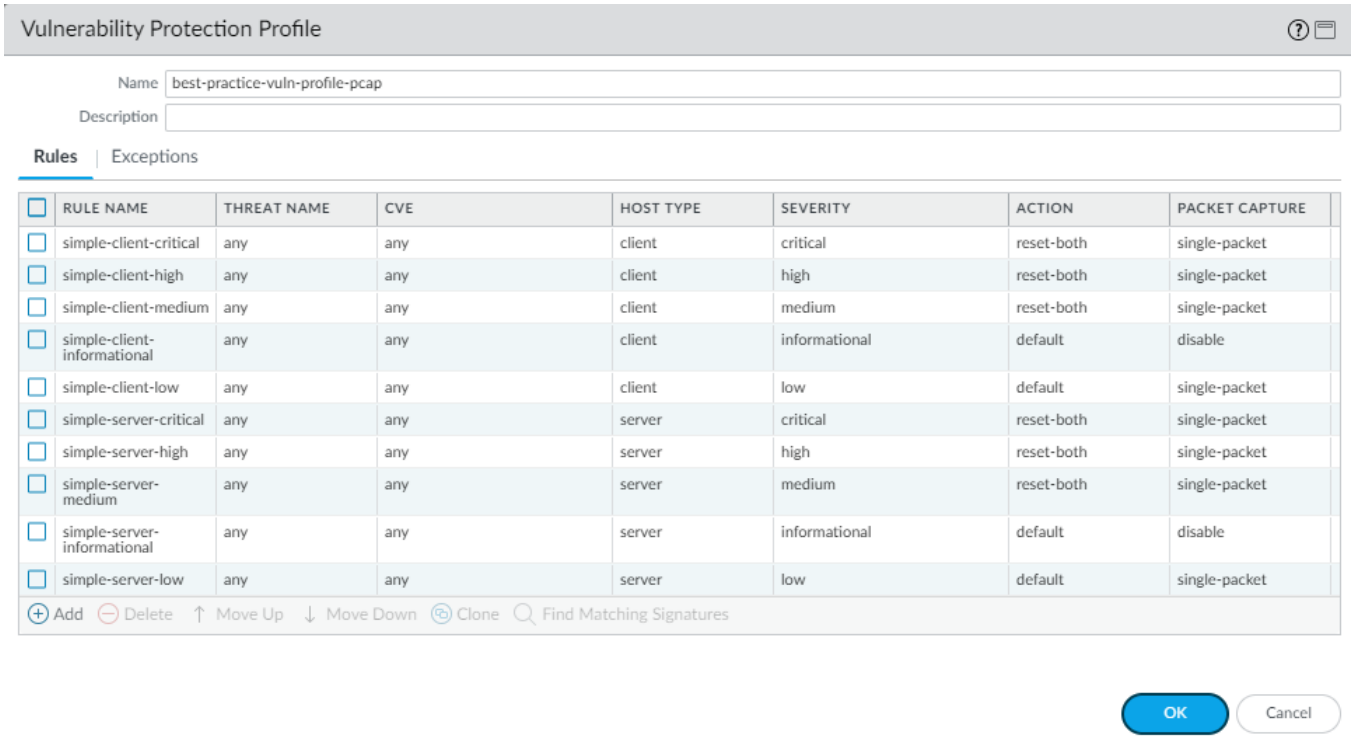
DNS シンクホールを伴うホストを保護することに加え、トラフィックを許可するすべてのセキュリティポリシールールに最良のアンチスパイウェア プロファイルを適用し、トラフィックがネットワークを出る際に感染ホストを特定し、感染したシステムが悪意のある C2 ネットワークと通信するのを防止して攻撃者を阻止できるようにします。システムがC2ネットワークと通信できない場合、C2ネットワークはシステムを制御できません。以下に例を示します。

- ユーザーからデータセンターへのトラフィック、イントラ データセンター トラフィック、インターネットからデータセンターへのトラフィックの場合—アンチスパイウェア プロファイルはピアツーピアの C2 トラフィックをブロックします。
- データセンターからインターネットへのトラフィックの場合—C2 トラフィック、マルウェアの最初のダウンロード、ハッキング ツールを特定およびブロックするのに、アンチスパイウェア プロファイルとアンチウイルス プロファイルが役立ちます。

データセンターの最良の脆弱性保護プロファイルを作成

トラフィックを許可するすべての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を付与します。脆弱性保護プロファイルは、バッファオーバーフロー、不正なコードの実行、クライアント側およびサーバー側の脆弱性を狙ったその他のエクスプロイトの試みにより、攻撃者がセキュリティを破ってデータセンターのネットワークを通して横方向に移動するのを防ぎます。

事前に設定された厳密な脆弱性保護プロファイルを複製します。ビジネス的に重要なアプリケーションを確実に利用できるように、現在の状況からベストプラクティスのプロファイルに移行する際には、安全な移行手順を実施してください。ベストプラクティスのプロファイルとして、潜在的な攻撃のソースを追跡できるように、**simple-client-informational**および**simple-server-informational**を除く各ルールについて、**Rule Name**（ルール名）をダブルクリックして**Packet Capture**（パケット キャプチャ）を**disable**（無効）から**single-packet**（単一パケット）に変更し、各ルールのパケット キャプチャ（PCAP）を有効化します。他の設定を変更してはなりません。シグネチャセットが常に最新に保たれるよう、content updates（コンテンツ更新）を自動的にダウンロードし直ちにインストールします。



通知のアクティビティは比較的大量のトラフィックを生成し、かつ潜在的な脅威の場合よりも役立たないため、通知のアクティビティに対して PCAP を有効化しないでください。拡張 PCAP（単一 PCAP ではなく）を、**alert**（アラート）アクションを適用する高価値のトラフィックに適用します。ログに記録するトラフィックを指定するために使用するロジックと同じものを使用する PCAP を適用します（ログに記録するトラフィックの PCAP を取ります）。単一 PCAP をブロックするトラフィックに適用します。拡張 PCAP が記録して管理プレーンに送信するデフォルトのパケット数は 5 パケットであり、これが推奨される値になります。大抵の場合、5 つのパケットをキャプチャすれば脅威を分析するのに十分な情報を得られます。過剰な PCAP トラフィックが管理プレーンに送信される場合、5 つよりも多くパケットをキャプチャすると PCAP がドロップされるおそれがあります。

トラフィックを許可するすべてのセキュリティポリシールールにベストプラクティスの脆弱性保護プロファイルを付与する理由は、厳格な脆弱性保護がない場合、攻撃者がクライアント側およびサーバー側の脆弱性を利用してデータセンターのセキュリティを破るおそれがあるためです。以下に例を示します。

- イントラ データセンター トラフィック—攻撃者が脆弱性をエクスプロイトしてマルウェアやハッキング ツールをデータセンター ネットワーク内のサーバー間で横方向に蔓延させるのを防止するうえで、厳格な脆弱性保護プロファイルおよびアンチウイルス プロファイルが役立ちます。
- データセンターからインターネットへのトラフィック—感染したデータセンター サーバーがインターネット サーバーを感染させるのを防ぐうえで、脆弱性保護が役立ちます。
- インターネットからデータセンターへのトラフィック—サーバー側の脆弱性を伴うデータセンター サーバーのセキュリティを破る試みを厳格な脆弱性保護プロファイルが防ぎます。サーバーが感染した場合、感染したサーバーによるクライアントに対するエクスプロイトを阻止し、感染を隔離して提携企業や顧客をウォーターホール攻撃から保護するうえで、脆弱性保護が役立ちます。また、脆弱性保護はブロック IP アクションを使用するブルートフォース攻撃も阻止します。ブルートフォース攻撃のシグネチャがアクションを開始すると、ファイアウォールは設定した期間中、攻撃者の IP アドレスをブロックします。この期間が修了した後にブルートフォース攻撃が再開した場合、シグネチャがブロック アクションを再び開始します。ブルートフォース攻撃が継続する可能性はありますが、成功することはありません。

データセンターの最良のファイルブロッキングプロファイルを作成

事前定義済みの厳格なファイルブロッキングプロファイルを使用し、頻繁にマルウェア攻撃に使用されるファイル、アップロード/ダウンロードする必要性がないファイルをブロックします。これらのファイルをブロックすることで攻撃の入り口を減らすことができます。事前定義済みの厳格なプロファイルは、バッチファイル、DLL、Java クラス ファイル、ヘルプ ファイル、Windows ショートカット（.lnk）、BitTorrent ファイル、.rar ファイル、.tar ファイル、encrypted-rar および encrypted-zip ファイル、マルチレベル エンコード ファイル（最大 4 回、暗号化あるいは圧縮されたファイル）、.hta ファイル、および .exe、.cpl、.dll、.ocx、.sys、.scr、.drv、.efi、.fon、.pif などを含む Windows Portable Executable（PE）ファイルをブロックします。事前定義済みの厳格なプロファイルは他のすべてのファイル タイプについてアラートを生成し、他のファイル転送について可視性を持たせ、ポリシーの変更を行う必要があるかどうか判断できるようにします。

重要なアプリケーションをサポートする必要があり、厳格なプロファイルのファイル形式をすべてブロックできないケースもあります。安全な移行へのアドバイスに従って、ネットワークの各所で例外事項を行うかどうかを判断してください。データ フィルタリング ログ（*Monitor*（監視）> *Logs*（ログ）> *Data Filtering*（データ フィルタリング））を確認し、データセンター内で使用されるファイル形式を把握し、関係者と相談してアプリケーションで必要なファイル形式を判断してください。その情報に基づき、必要に応じて厳格なプロファイルをクローンして編集し、重要なアプリケーションをサポートするために必要な他のファイル形式だけを許可します。また、*Direction*（方向）設定を使用し、対象のファイル形式が双方向に流れるのを制限したり、片方の方向にファイルが流れるのだけをブロックしたりできます。

NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
		Log all other file types	any	any	both	alert
strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
		Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
		Log all other file types	any	any	both	alert

トラフィックを許可するすべてのセキュリティポリシールールにベストプラクティスのファイルブロッキングプロファイルを適用する目的は、攻撃者がファイル共有アプリケーション、エクスプロイトキットを使用したり、データセンターにアクセスするユーザーを感染させたり、USB スティックを使ったりして悪意のあるファイルをデータセンターに入れるのを防ぐことです。

- ユーザーからデータセンターへのトラフィック–ファイル共有やコラボレーションが不要なアプリケーションについては、厳格なファイルブロッキングプロファイルをセキュリティポリシールールに付与し、エクスプロイトやマルウェアにつながるおそれがある危険なファイル形式をブロックします。
- イントラ データセンター トラフィック–厳格なファイルブロッキングプロファイルをセキュリティポリシールールに付与し、感染したサーバーが悪意のあるファイルをデータセンター内の他のサーバーと共有するのを防ぎます。これにより感染を隔離し、データセンターを通じてマルウェアが広がるのを防止できます。
- データセンターからインターネットへのトラフィック–ファイル転送を、使用するアプリケーションに欠かせないファイル形式に制限します。

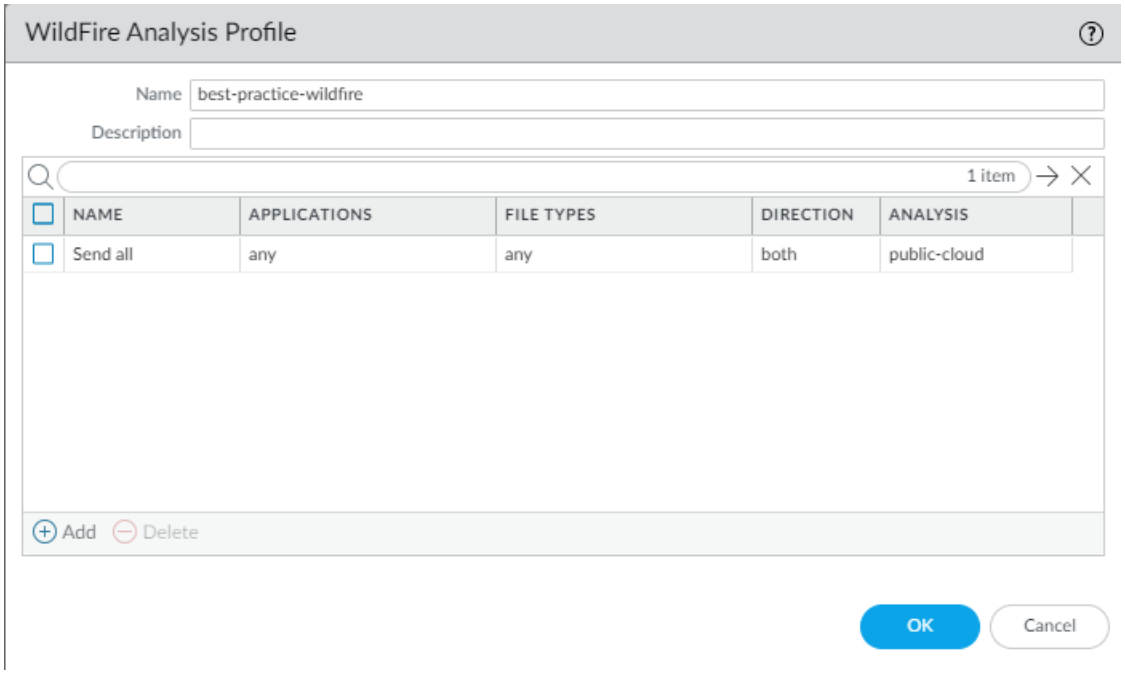
Windows PE ファイルを一部ブロックしない場合は、未知のファイルをすべて WildFire に送信して分析を行ってください。ユーザーアカウントについては**Action**（アクション）を**continue**（続行）に設定するこ

とで、悪意のあるウェブサイト、メール、ポップアップが意図せずユーザーに悪意のあるファイルをダウンロードさせるドライブバイダウンロード攻撃を防げるようになります。自身で開始しテイアにファイル転送の継続を求めるプロンプトは、悪意のあるダウンロードであり得るということを、ユーザーに伝えてください。

データセンターの最良の WildFire 分析プロファイルを作成

他のセキュリティ プロファイルは既知の脅威を検出してブロックします。WildFireは未知の脅威からデータセンターを保護します。事前定義済みのデフォルトのプロファイルを使用してファイアウォールがすべての未知のファイルを WildFire に転送して分析を行うように設定します。様々なファイル形式の中に未知の脅威が潜んでおり、被害を被ってからずっと後に攻撃が成功したことを知ることがあります。例えば、WildFire はステージング サーバーに読み込まれたマルウェアを攻撃者が攻撃を行う前に特定し、攻撃者が目的を達成する前に脆弱性スキャナーおよび横方向の移動アシスタント ツールを発見できます。過去数年間に発生したエンタープライズ システムに対する大規模な攻撃の多くを、WildFire が保護できたでしょう。現在・将来・過去にファイル転送アクティビティが生じるトラフィックを制御するすべてのセキュリティポリシー ルールに、有効な WildFire 分析プロファイルを含める必要があります。

分毎に自動的にダウンロードおよびインストールを行うようWildFire アプライアンスのコンテンツ更新をセットアップし、常に最新のサポートを得られるようにします。例えば、*Linux* ファイルおよび *SMB* ファイルのサポートは、最初に *WildFire* アプライアンスのコンテンツ更新として配信されます。



トラフィックを許可するすべてのセキュリティポリシールールにデフォルトの WildFire 分析プロファイルを付与する理由は、WildFire により、未知の脅威や advanced persistent threats (APT) に対する最も優れた防御が得られるためです。以下に例を示します。

- ユーザーからデータセンターへのトラフィック—WildFire が Confluence や Sharepoint など、データセンター内に侵入した未知のマルウェアを特定します。
- イントラ データセンター トラフィック—WildFire がデータセンター サーバー間で人ファル未知のマルウェアを特定し、被害が出る前にマルウェアを発見することで、データ流出を防ぎます。
- データセンターからインターネットへのトラフィック—このトラフィックはソフトウェアおよびオペレーティングシステムを更新する実行ファイルをダウンロードするため、すべてのアプリケーション上で WildFire を実行して不審な挙動を特定することが重要です。

潜在的な問題に遭遇した際にファイアウォールが通知できるように、電子メール、SNMPまたは syslog サーバーを通して、マルウェア検出時のアラートを設定します。危険にさらされたホストをより迅速に切り分けるほど、これまで知られていなかったマルウェアが他のデータセンターデバイスに拡散した可能性が低くなり、問題の修正が容易になります。

必要な場合はトラフィックの方向に基づいて、分析に送るアプリケーションおよびファイル形式を制限できます。

アンチウイルスプロファイルの*WildFire Action*設定は、リセットまたはドロップアクションにつながる*WildFire*シグネチャをトラフィックが生成する場合、トラフィックに影響を与える可能性があります。*WildFire*は独自に作成されたプログラムを悪意のあるプログラムと判断し、それらに対するシグネチャを生成する可能性があるため、独自のプログラムを安全に移行する、ソフトウェア配布アプリケーションなどの内部トラフィックを除外することができます。内部の独自に作成されたプログラムが*WildFire*シグネチャを引き起こすかどうかを調べるには、*Monitor*（モニター）> *Logs*（ログ）> *WildFire Submissions*（*WildFire* への送信）をチェックします。

Cortex XDRエージェントを使用したデータセンターエンドポイントの保護

次世代ファイアウォールがネットワークを横切ってエンドポイントに到達する脅威（つまり、ファイアウォールを通過しなければならない）を防止する一方、Cortex XDRエージェントは、サーバーや VM などのデータセンターのエンドポイントを、マルウェアやエンドポイント上で行われるエクスプロイトから保護します。マルウェアやエクスプロイトがすでにエンドポイント上に存在する、あるいはエンドポイントに侵入する際、エンドポイントが脅威を実行（例えば .exe や .dll ファイルを通じて）する際、エンドポイント上でアクションが発生し、トラフィックはファイアウォールを通過しないため、ファイアウォールには脅威の存在が分かりません。しかし、各エンドポイント上のCortex XDRエージェントは実行ファイル、ドキュメント内のマクロ、DLL ファイルなどに潜む脅威を発見できます。これらの脅威が実行されようとすると、Traps はエンドポイント上でアクションを実行してエンドポイントを保護します。

Cortex XDRエージェントおよび次世代ファイアウォールはデータセンターのエンドポイントを2重の層で保護し、ファイアウォールがエンドポイントをネットワーク上の脅威から保護しつつ、Cortex XDRエージェントがエンドポイント上の脅威を監視してエンドポイントを保護できるようにします。Endpoint Security Manager（ESM）上でエンドポイント用に構成するセキュリティポリシーおよび Panorama あるいはファイアウォール上で構成するセキュリティポリシーは、別の場所で別のイベントを制御するため、互いに衝突しません。Cortex XDRエージェントは個々のエンドポイント内のセキュリティを制御します。ファイアウォールは自身を通過するトラフィックのセキュリティを制御します。

Cortex XDRエージェントをすべてのデータセンターのエンドポイントにインストールしてください。コンテキストは常にエンドポイント自体であり、コンテキストが「データセンター内」であろうと「ユーザーグループ内」であろうと違いはないため、データセンター内のCortex XDRエージェントのベストプラクティスは各エンドポイント上のCortex XDRエージェントの場合と同じです。Cortex XDRエージェントはすべてのエンドポイントを同じ方法で保護します。デプロイメントプロセスおよびマルウェア防止ポリシーのベストプラクティスなどは他のどのネットワーク領域でも同じになります。

データセンターのトラフィック ブロック ルールを作成

4つのデータセントートラフィックフローに使用するアプリケーション許可ルールを作成する前に、データセンター内で使用しないアプリケーションや既知の不適切なアプリケーションをブロックし、ネットワーク上に存在することを知らない可能性があるアプリケーションを発見するために、ブロッキングおよびロギング ルールを作成します。ブロックしたトラフィックに関するログを取ることで、潜在的な攻撃についての情報が得られ、調査を行いやすくなります。

未知のアプリケーションを発見した際、それを許可するかどうか、それが潜在的な脅威を表すかどうかを指定します。これらのルールが許可すべきアプリケーションを発見した場合は、それに基づいてアプリケーション許可ルールを調整します。これらのルールが不当なアプリケーションを発見した場合は潜在的な脅威を示している可能性があり、ログ情報を使って調査を行えます。セキュリティ プロファイルが制御するトラフィックはネットワークに入らないため、セキュリティ プロファイルをブロック ルールに適用しないでください。

内部の専有アプリケーションあるいは他のタイプの正当なアプリケーションである未知のアプリケーションを発見した場合、それぞれの未知のアプリケーションに対してカスタム アプリケーションを作成し、識別を行ってセキュリティポリシーを適用できるようにしてください。

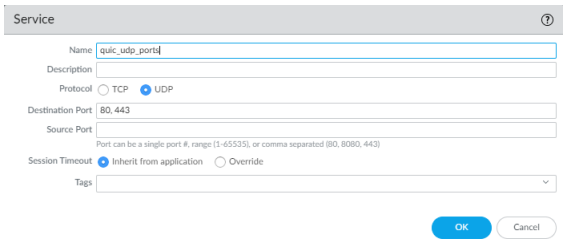
データセンター セキュリティポリシーのルールベースの順序を指定は、これらのルールと、4 つのデータセンター トラフィック フロー用に作成するその他すべてのルールの順序を決め、あるルールによって他のルールが遮られないようにする方法を説明します。

複数のデータセンター全体にかけて一貫した形でセキュリティポリシーを適用するために、テンプレートおよびテンプレート スタックを再利用し、同じポリシーをすべてのデータセンターに適用することができます。このテンプレートは、グローバル セキュリティポリシーを維持し、管理しなければならないテンプレートおよびテンプレート スタックの数を減らしつつ、*IP* アドレス、*FQDN* などのデバイス固有の値を適用するために変数を使用します。

STEP 1 | Quick UDP Internet Connections（QUIC）プロトコルをブロックします。

Chrome およびその他の一部のブラウザは TLS ではなく QUIC を使ってセッションを確立しますが、QUIC はファイアウォールが復号化できないプロプライエタリな暗号化を使用するため、危険があるトラフィックが暗号化されたトラフィックの状態でネットワークに侵入するおそれがあります。QUIC をブロックするとブラウザが TLS にフォールバックするため、ファイアウォールがトラフィックを復号化できるようになります。

UDP のサービスポート（80 および 443）で QUIC をブロックするセキュリティポリシールールを作成し、QUIC アプリケーションをブロックする別のルールを作成します。UDP ポート 80 および 443 をブロックするルールでは、UDP ポート 80 および 443 を含むサービス（**Objects**（オブジェクト）> **Services**（サービス））を作成します。



サービスを使用して、QUIC をブロックする UDP ポートを指定します。2番目のルールで、ルールベース内の最初の2つのルールがQUICをブロックするように、QUICアプリケーションをブロックします:

	NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block QUIC UDP	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	quic	application-default	Deny	none	

STEP 2 | ユーザーゾーンからのアプリケーションをそのデフォルトのポートですべてブロックし、予期しないアプリケーションを特定します。

このルールは、ユーザーが使用しようと試み、かつデータセンター上で実行されていることを知らなかったアプリケーションを発見します。このルールにマッチするトラフィックを監視し、それが潜在的な脅威であるのか、あるいは許可ルールを編集してアプリケーションへのアクセスを許可すべきなのかを判断します。このルールは必ず、トラフィックを許可するルールの後に配置してください。そうしない場合、許可したいトラフィックをこのルールがブロックしてしまいます。

このルールの後に表示されるルールは、ユーザーゾーンからのトラフィックだけでなく、あらゆるソースから来るトラフィックに適用されるという点を除き、このルールと同様です。別のルールを作成する理由は、*user-zone*ルールに対する違反が、一部のユーザーが業務を行うために必要とする正当なアプリケーションをブロックしていることを示している可能性があり、その特定のユーザーのためにルールを修正してアプリケーションを許可しなければならないことがあるためです。非ユーザー ゾーンからの違反は、アプリケーションの変更、あるいは潜在的な攻撃を示している可能性があります。他のトラフィック用のルールを別に作成することで、ユーザートラフィックおよびデータセンターに侵入しようと試みるその他のトラフィックに関するログを個別に確認できるようになり、潜在的な問題に対する調査や対応が容易になります。

ユーザーゾーンからの違反を最初にログに記録した後、送信元に関わらず、アプリケーションのデフォルトのポート上で予期せぬアプリケーションを使用しようとする試みをログに記録し、監視できるようにするために、このルールをすべてのトラフィックに適用される次のルールの前に配置する必要があります。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-User-Zone	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

このルールを作成するには：

- ソースゾーンには、すべてのユーザーゾーンおよびユーザーが含まれています（配置によっては、この例よりも多くのユーザーゾーンが存在することもあります）。
- Destination Zone（宛先ゾーン）は、データセンターの境界に位置するデータセンター Web サーバー層（**Web-Server-Tier-DC**）です。
- Application（アプリケーション）を**any**（すべて）に、Service（サービス）を**application-default**に設定し、標準的なポート上で実行されているすべてのアプリケーションにルールが適用されるようにします。
- Action（アクション）を**Drop**（ドロップ）に設定し、クライアントあるいはサーバーに信号を送ることなく密かにトラフィックをドロップします。

STEP 3 | すべてのポート上でユーザーゾーンからのアプリケーションをすべてブロックし、不適切な場所で実行されているアプリケーションを特定します。

このルールは、ユーザーが標準的でないポート上で実行しようとしている正当かつ既知のアプリケーション、およびカスタム アプリケーションを作成しなければならない可能性がある未知のアプリケーションを識別します。このルールにマッチするすべてのトラフィックの送信元を調査し、unknown-

tcp、unknown-udp、non-syn-tcp トラフィックを許可していないことを確認してください。このルールは必ず、トラフィックを許可するルールの後に配置してください。そうしない場合、許可したいトラフィックをこのルールがブロックしてしまいます。

ユーザーゾーンからのトラフィックだけでなく、あらゆるソースから来るトラフィックに適用されるという点を除き、このルール（*Unexpected-App-from-Any-Zone*）と同様の別のブロック ルールもこのセクションの後半で作成します。別のルールを作成する理由は、*user-zone* ルールに対する違反が、一部のユーザーが業務を行うために必要とする正当なアプリケーションが適切に指定されておらず、アプリケーションを修正しなければならないことを示す場合があるためです。他のトラフィック用のルールを別に作成することで、ユーザートラフィックおよびデータセンターに侵入しようと試みるその他のトラフィックに関するログを個別に確認できるようになり、潜在的な問題に対する調査や対応が容易になります。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-User-App-Any-Port	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

このルールを作成するには：

- ソースゾーンには、すべてのユーザーゾーンおよびユーザーが含まれています（配置によっては、この例よりも多くのユーザーゾーンが存在することもあります）。
- Destination Zone（宛先ゾーン）は、データセンターの境界に位置するデータセンター Web サーバー層（**Web-Server-Tier-DC**）です。
- Application（アプリケーション）を**any**（すべて）に、Service（サービス）を**any**（すべて）に設定し、あらゆるポート上で実行されているすべてのアプリケーションにルールが適用されるようにします。
- Action（アクション）を**Drop**（ドロップ）に設定し、クライアントあるいはサーバーに信号を送ることなく密かにトラフィックをドロップします。

STEP 4 | セキュリティをかいくぐることを目的とする攻撃者によるエクスプロイトやデータセンター内で不要なアプリケーションをブロックします。

このルールは、ネットワーク内に入れるべきでないことが分かっているアプリケーションからデータセンターを保護します。最良のセキュリティポリシーの目的はポジティブエンフォースメントですが、アプリケーションルールを使用して、許可されていないファイル共有アプリケーション、リモートアクセスアプリケーション、暗号化されたトンネルなどの危険な可能性があるアプリケーションのアクティビティを明示的にブロックし、ログに記録することで、潜在的な攻撃に関する情報を得て可視性を確保できます。違反の試みに関するログは潜在的な攻撃の調査に役立つため、強固なアプリケーション許可リストを作成した後でも、このアプリケーション ブロックルールをルールベース内で維持してください。

このルールを使用し、データセンターに入れたくないアプリケーションだけをブロックします。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block-Bad-Apps	User to DC BP	universal	any	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	

このルールを作成するには：

- データセンター内で誰も使用してはならないアプリケーションをブロックしようとしているため、Source Zone（送信元ゾーン）、Addresses（アドレス）、User（ユーザー）、およびDevice（デバイス）を**any**（すべて）に設定します。
- Destination Zone（宛先ゾーン）内のすべてのデータセンター ゾーンを指定し、すべてのデータセンター サーバーを不適切なアプリケーションから保護します。
- ブロックするアプリケーションの各タイプ（カテゴリ）用のアプリケーション フィルターを作成し、追加のアプリケーションがあればそれを指定します。この例には、暗号化されたトンネル、リモート アクセス、ファイル共有用のアプリケーション フィルターが含まれます。データセンターで使用しないアプリケーションをブロックして、不要なアプリケーションを排除し、攻撃面を減らすことでリスクも削減します。アプリケーショングループを使用する、あるいは個々のアプリケーションをリストアップする代わりにアプリケーション フィルターを使用するメリットは、フィルターが自動的にアップデートされるため、新しいアプリケーションがある場合に管理を行う必要がなくなることです。
- Service（サービス）を**any**（すべて）に設定し、標準的でないポートおよびデフォルトのポート上の不要なアプリケーションを捕捉します。
- Action（アクション）を**Drop**（ドロップ）に設定し、クライアントあるいはサーバーに信号を送ることなく密かにトラフィックをドロップします。

ルールの例にあるアプリケーション フィルターは、包括的なリストではありません。データセンターを評価する方法に基づいて作成するアプリケーション リストを評価し、許可しないアプリケーションをこのルールに追加してください。このブロッキング ルールは、ルールの例外を許可する許可ルールの後に配置します。例えば、IT 部門がリモートアクセス アプリケーションを使ってデータセンター デバイスを管理する必要がある場合、他のすべてのユーザーに対してリモートアクセス アプリケーションをブロックする前に、リモートアクセス アプリケーションの使用を許可しなければなりません。他の例としては、このブラックリスト ルールの前にある許可ルールで1つあるいは2つのファイル共有アプリケーションを許可した後、このルール内のアプリケーション フィルターが他のすべてのアプリケーションをブロックする場合です。例外なくネットワークに入れたくない一連のアプリケーションがある場合、それらのアプリケーションだけをブロックする具体的なブロックルールを作成し、ルールベースの一番上、アプリケーション許可リストルールよりも上に配置することができます。しかしその場合はユーザーがアクセスできなくなるため、ブラックリストに登録したすべてのアプリケーションがビジネス上の使用目的を持っていないことを確認してください。

STEP 5 | あらゆるゾーンからのアプリケーションをそのデフォルトのポートですべてブロックし、予期しないアプリケーションを特定します。

このルールは、データセンター上で実行されていることを知らなかった、あらゆるゾーンからのアプリケーションを発見します。このルールに対する違反は、アプリケーションが変更されたこと、あるいは潜在的な脅威がある可能性を示唆します。このルールにマッチしたトラフィックを監視し、それが潜在的な脅威であるのか、アプリケーション許可ルールを修正する必要があるのか判断してください。このルールは、トラフィックを許可するルールの後に配置してください。そうしない場合、許可したいトラフィックをこのルールがブロックしてしまいます。また、ユーザーゾーンからのトラフィックを捕捉しないよう、このルールはステップ 1 のルールの後に配置してください。

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-Any-Zone	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

このルールを作成するには：

- Source（送信元）を**any**（すべて）に設定し、データセンターに入ろうとする他のすべてのトラフィックを対象にします（ステップ 1 のルールは、このルールがトラフィックに適用される前に、予期せぬユーザー アプリケーションをブロックおよび特定します）。
- Destination Zone（宛先ゾーン）は、データセンターの境界に位置するデータセンター Web サーバー層（**Web-Server-Tier-DC**）です。

- Application（アプリケーション）を**any**（すべて）に、Service（サービス）を**application-default**に設定し、標準的なポート上で実行されているすべてのアプリケーションにルールが適用されるようにします。
- Action（アクション）を**Drop**（ドロップ）に設定し、クライアントあるいはサーバーに信号を送ることなく密かにトラフィックをドロップします。

STEP 6 | すべてのポート上であらゆるゾーンからのアプリケーションをすべてブロックし、不適切な場所で実行されているアプリケーションを特定します。

このルールは、標準的でないポート上で実行しようとしている正当かつ既知のアプリケーション、およびカスタム アプリケーションを作成しなければならない可能性がある未知のアプリケーションを識別します。このルールにマッチするすべてのトラフィックの送信元を調査し、unknown-tcp、unknown-udp、non-syn-tcp トラフィックを許可していないことを確認してください。このルールは必ず、トラフィックを許可するルールの後に配置してください。そうしない場合、許可したいトラフィックをこのルールがブロックしてしまいます。また、ユーザーゾーンからのトラフィックを捕捉しないよう、先行するルールの後に配置してください。

		Source				Destination						
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-Any-Port	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

このルールを作成するために、送信元でユーザーゾーンを指定する代わりに**any**（すべて）のゾーンを指定してデータセンターに入ろうとする他のすべてのトラフィックを対象にし、Service（サービス）を**any**（すべて）にして標準的でないポートを対象にすることを除き、**Unexpected-App-from-User-Zone**ルールと同じ設定を使用します。

STEP 7 | すべてのポート上であらゆるアプリケーションを実行しようとしている未知のユーザーを発見します。

このルールは、未知のユーザーを見つけることで、User-ID がカバーする範囲の漏れを特定します。また、これはデータセンターにアクセスしようとする、ユーザー コミュニティ内の侵入されたデバイスや組み込みデバイスも特定します。（プリンター、カード リーダー、カメラなどの組み込みデバイスにはユーザーインターフェイスがありませんが、攻撃者はこれらのデバイスに侵入し、攻撃を行うために使用できます。）

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Discover-Unknown-Users	universal	any	any	unknown	any	any	any	any	any	any	Deny	none	

このルールは、すべてのユーザーからのトラフィックをドロップするのではなく未知のユーザーからのトラフィックだけをドロップするという点を除き、ゾーン間の通信を防止する（他のルールがトラフィックを許可する場合を除く）interzone-default ルールと同じものです。これにより、ルールのマッチを個別にログに記録できるようになり、データセンターにアクセスしようとする未知のユーザーを非常に調査しやすくなります。

最初のユーザーからデータセンターへのトラフィックのセキュリティポリシーを定義

データセンターへと流れるユーザートラフィック用に最初のベストプラクティスのセキュリティポリシーを定義する作業は、データセンター アプリケーションの許可リストを作成することから始まります。最終目的は、誰がデータセンターにアクセスできるのか、どのデータセンター アプリケーションにアクセスできるのか、データセンター内のどのリソースにアクセスできるのかを明示的に制御することで、ゼロ トラスト アーキテクチャを持つデータセンターを保護できるポジティブ エンフォースメントのセキュリティを導入することです。最良のセキュリティポリシーを構築し終えたら、データセンターにアクセスできる未知のユーザーは存在せず、未知のアプリケーションやリソースがデータセンター内に存在しない状態になります。

- ユーザーからデータセンターへのトラフィックを保護するためのアプローチ
- ユーザーからデータセンターへのアプリケーション許可ルールを作成
- ユーザーからデータセンターへの認証ポリシールールを作成
- ユーザーからデータセンターへの復号化ポリシー ルールを作成

ユーザーからデータセンターへのトラフィックを保護するためのアプローチ

従来型の古いアプローチでデータセンターに向かうユーザートラフィックを保護すると、貴重なアセットがリスクにさらされたままになってしまいますが、ベストプラクティスのアプローチであれば貴重なアセットを保護できます。

従来型のアプローチ	リスク	ベストプラクティスのアプローチ
データセンターは信頼できるネットワーク内にあるため、ポートベースのルールで十分に保護できます。	悪意のあるアプリケーションは、ポート番号を偽装したり、トンネル内でポートを抜けたり、ポート ホッピングを使用して発見をまぬがれたりすることでネットワークにアクセスします。	アプリケーション 許可ルールは各アプリケーション、ユーザー、サーバーを紐付け、正当なユーザーだけが許可されたアプリケーションを使用して一連の適切なデータセンター サーバーにアクセスできるようにします。 ポートベースからアプリケーション ベースのルールに移行する際、ルールベース内で、入れ替えるポートベースのルールよりも上にアプリケーション ベースのルールを配置し両方のルールのポリシールール ヒット数をリセットします。トラフィックがポートベースのルールにヒットすると、そのポリシールールのヒット数が増加します。一定期間どのトラフィックもポートベースのルールにヒットしなくなるまでアプリケーション ベースのルールを調整してから、ポートベースのルールを削除します。

従来型のアプローチ	リスク	ベストプラクティスのアプローチ
内部ユーザーを信頼し、ユーザーがアクセスするアプリケーションを許可し、認証情報および可能な場合は IP アドレスルールに基づいてアクセスが許可されているかどうか判断します。	攻撃者はデータセンターのエンドポイントへのアクセスを掌握してから、横方向に任意の他のデータセンターのエンドポイントへと移動し、盗んだ認証情報やサーバー側の脆弱性をエクスプロイトします。未知のユーザーはデータセンターのエンドポイントにアクセスできるようになります。	User-ID を有効化し、未知のユーザーをブロックし、許可されたユーザーによるアクセスを許可します。従業員、提携企業、契約者に対して個別のID ドメインを作成してください。提携企業、契約者、センシティブなサーバーのアクセスの場合は多要素認証（MFA）を使用します。
データセンターは信頼できるネットワーク内にあるため、未知のファイルの分析は不要です。	ユーザーがファイル共有やその他のクラウド アプリケーションから誤ってマルウェアをダウンロードしてしまうおそれがあります。	すべての未知のファイルを WildFire 分析 に送信して分析を行い、新規および未知のマルウェアを特定してそれを防止するようにしてください。
複数のベンダーのものを混ぜ合わせた脅威防止プロファイル。	個々のツールをひとまとめにすると、攻撃者が利用できるセキュリティの穴が生じ、また上手く連携して動作しません。	Palo Alto Networks の一連のセキュリティツールは適切に連携し、セキュリティの穴をふさいで攻撃を防止します。

ユーザーからデータセンターへのアプリケーション許可ルールを作成

データセンターを評価する際、どの一連のサーバー上で実行されているどのアプリケーションに、誰がアクセスできるのかをしっかり決定するために情報を集め、それに基づいて一連のアプリケーション許可ルールを作成します。アプリケーションのセキュリティポリシー許可ルールを作成（**Policies**（ポリシー）> **Security**（セキュリティ））し、明示的に許可したユーザーだけが、適切な一連のサーバー上にある、業務に関係するアプリケーションだけを使用できるようにします。不要なアクセス、未知のユーザー、不明なアプリケーションは許可しないでください。

事前定義済みの*Sanctioned*（許可）タグを使ってすべての許可されたアプリケーションをタグ付けします。*Panorama* およびファイアウォールは、*Sanctioned* タグが付いていないアプリケーションを許可されていないアプリケーションとみなします。

データセンター セキュリティポリシーのルールベースの順序を指定は、これらのルールと、他の 3 つのデータセンター トラフィック フロー用に作成するその他すべてのルールおよびブロック ルールの順序を決め、あるルールによって他のルールが遮られないようにする方法を説明します。

複数のデータセンター全体にかけて一貫した形でセキュリティポリシーを適用するために、テンプレートおよびテンプレート スタックを再利用し、同じポリシーをすべてのデータセンターに適用することができます。このテンプレートは、グローバル セキュリティポリシーを維持し、管理しなければならないテンプレートおよびテンプレート スタックの数を減らしつつ、*IP* アドレス、*FQDN* などのデバイス固有の値を適用するために変数を使用します。

下記の各々の許可ルール:

- ベストプラクティスセキュリティプロファイルグループが添付されている、これはベストプラクティスセキュリティプロファイルから構成されている。セキュリティプロファイルグループを使用することで、それぞれのプロファイルを個別に指定するのではなく、すべてのベストプラクティスプロファイルをルールにまとめて適用することができます。セキュリティプロファイルグループにより、マルウェア、脆弱性、C2トラフィック、未知および既知の脅威に対する保護の設定を素早く簡単に行えます。
- ルール違反を追跡、解析できるようにトラフィックをログに記録、ログを転送（セッション終了時）します。該当する場合はログサーバーにログを転送、ログのメールを適切な管理者に転送します。

STEP 1 | 適切なユーザーが社内の DNS サーバーにアクセスできるようにします（外部の DNS サーバーにはアクセスできないようにしてください）。

このルールは企業の DNS サーバーへのアクセスを制限することで攻撃の入り口を減らし、内部ホストおよびサービスについての DNS エントリを保護します。パブリックな DNS クエリによるディスカバリーを防止するために、社内リソース用の DNS エントリは公に利用できる DNS サーバーに保存せず、攻撃者が企業の DNS サーバーを攻撃しなければこれらのエントリを知ることができない状態にします。そのため、DNS サーバーが格好のターゲットになります。

インターネット ゲートウェイ（ネットワークの境界）上で公開 *DNS* サーバーに向かうすべての *DNS* トラフィックをブロックします。インターネットに向かう *DNS* トラフィックを許可しないでください。

このルールは、ユーザーがログイン前に DNS サービスにアクセスする必要があるため、ポリシールール内で「any（あらゆる）」ユーザーを許可しないというベストプラクティスの例外になります。このルールは DNS サービスへのアクセスを保護します。このルールを作成するには：

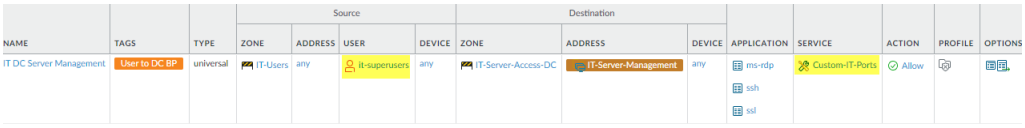
- データセンター**IT infrastructure**（**IT** インフラ）内の適切な Destination Zone（宛先ゾーン）へのアクセスを制限します。
- **DNS Servers**（**DNS** サーバー）のアドレスグループを設定し、アクセスをそのグループに限定します。
- **dns**を除くすべてのアプリケーションを使用するアクセスを防止します。
- 攻撃者がDNSサーバーを乗っ取ると、ユーザーがアクセスしようとした本物のWebサイトに似たフィッシングサイトにトラフィックをリダイレクトできるため、DNSトラフィックにベストプラクティスセキュリティグループを適用することが、特に重要になります。

STEP 2 | 必要な IT 担当者が管理･保守を行うためにデータセンター サーバーに保護された状態でアクセスできるよう、権限を付与します。

このルールは、権限付きのアカウントを持つユーザーによる重要なシステムへのアクセスを保護する方法を示します。権限付きのアカウントには高いレベルの信頼性が求められ、非常に重要な企業のデータが含まれる重要なシステムへの管理者アクセスを許可する必要があるため、権限付きのアカウントは厳重に制御･監視する必要があります。App-ID を活用し、IT 部門のユーザーがデータセンターデバイスを管理するために必要とするアプリケーションだけを指定し、ファイアウォールが他のすべてのアプリケーションに対するアクセスを拒否できるようにします。この例では、IT 部門のユーザーグループがデータセンター サーバーを管理するために管理者アクセスを必要とします。

データセンター サーバーを管理するための *IT* 部門の権限付きアクセスは管理インターフェイスおよび専用の *VLAN* に限定し、サーバーの管理トラフィックを他のトラフィックと別ける必要があります。管理インターフェイスは同じサブネット上になければなりません。データ インターフェイス上でこのタイプのアクセスを許可しないでください。*IT* グループが管理アクセス用に *SSH* あるいは *RDP* を使用する場合、他の目的による *SSH* や *RDP* アクセスを許可しないでください。

IT ネットワーク チームの編成により、誰に *IT* 権限付きアクセスを与えるのかが決まります。権限付きアクセスの各タイプについて、アクセス要件に応じてサーバーおよび他のデバイスをグループ化します。必要な *IT* ユーザーだけが、デバイス管理のために必要になるアプリケーションだけを使用して各サーバーのセットにアクセスできるようにしてください。



このルールを作成するには：

- IT ユーザーのサブセットだけにデータセンター サーバーの管理を許可するため、User-ID を活用し、そのレベルの権限付きアクセスを必要とする具体的な IT ユーザーのグループを作成します（この例では**it-superusers**）。
- **it-superusers**に管理させるサーバーの管理インターフェイスのアドレスを含む静的アドレスグループ（**IT-Server-Management**）を作成し、Destination（宛先）を**IT-server-access-DC**ゾーン内のアドレスグループに制限します。
- デフォルトのポート上で、IT スーパーユーザーが業務を行ううえで必要なアプリケーションだけを許可します。この例では、ルールが**ssl**、**ssh**、および**ms-rdp**アプリケーションを許可します。

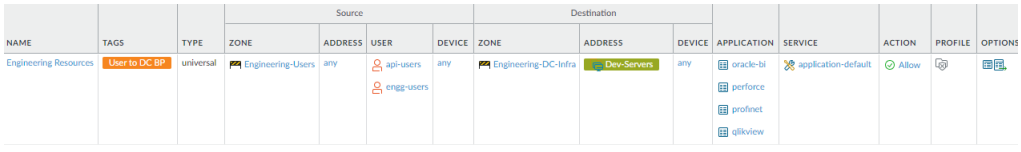
許可するアプリケーションは一例です。*IT* 部門がデータセンター サーバーを管理するために使用するアプリケーションを許可してください。*SSL* 経由のアプリケーションでは、*App-ID* で正しく識別を行うために、具体的なアプリケーションを追加しなければならない場合があります。

また、IT 担当者はスイッチ、ルーター、データセンター内のその他のデバイスも管理します。同じグループの IT ユーザーが同じアプリケーションを使ってそれらのリソースを管理する場合、宛先ゾーンおよびアドレスにそれらを追加すれば、IT スーパーユーザーによるそれらのデバイスの管理インターフェイスへのアクセスをルールが許可するようになります。別の IT ユーザーグループが一連の異なるデータセンター リソースを管理する、あるいは異なるアプリケーションを使用する場合は、各ユーザーグループおよび一連のアプリケーション毎に強固なセキュリティポリシールールを別途作成します。

権限付きのアカウントを持つユーザーグループは重要なシステムにアクセスできるため、ユーザーからデータセンターへの認証ポリシールールを作成する際、攻撃者に認証情報を奪われた場合にアクセスを防止するために MFA を強制します。各権限付きアクセスルールに対し、対応する認証ポリシーおよび復号化ポリシー ルールを作成してください。

STEP 3 | データセンター サーバーと通信を行う正当なビジネス上の理由を持つ従業員ユーザーグループによるアクセスを許可します。

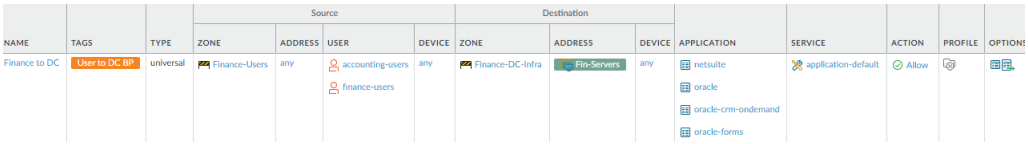
このルールは、各ユーザーグループ（場合によっては個々のユーザー）のアクセスを必要なアプリケーションおよびサーバーに限定する方法を示します。例えば、エンジニアはデータセンター内の開発用サーバーにアクセスできなくてはなりません。セキュリティポリシー ルールを作成するには、対象のグループが使用するデータセンター サーバーの開発用サーバーすべての IP アドレスを含むダイナミック アドレス グループを作成し、エンジニアがそれらのサーバー上で使用しなければならないアプリケーションを特定し、それらのグループに基づいてルールを構成します。



このルールを作成するには：

- データセンター内のエンジニアリング サーバーにアクセスする必要があるエンジニアリング ユーザーグループを指定します（この例では**api-users**および**engg-users**）。
- ダイナミック アドレス グループ（**Dev-Servers**）を作成して Destination Address（宛先アドレス）として設定し、データセンターの開発用サーバーへのアクセスを制限します。
- ビジネス上の目的で必要となる、デフォルトのポート上のアプリケーションにアクセスを限定します。

同じ方法で各ユーザーグループ用（必要な場合は個々のユーザーに対して作業することも可能）に詳細な許可ルールを作成し、各グループがデフォルトのポート上で実行されている正当なアプリケーションだけを使って、ビジネス上の理由でアクセスする必要がある一連のサーバーのみにアクセスできるようにします。例えば、PCI が含まれるサーバーにアクセスしなければならない会計部門のユーザーグループだけが、業務を行うために必要な制限付きの財務アプリケーションのみを使ってサーバーにアクセスできるようにします。



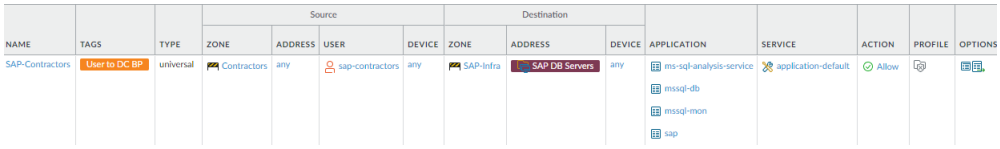
このルールはエンジニアリング ユーザーによるデータセンター サーバーへのアクセスを対象にしたホワイトリスト ルールの場合と同様に、指定したアプリケーションだけを使用して**finance-users**および**accounting-users**グループのユーザーが**Fin-Servers**ダイナミック アドレス グループ内のサーバーにのみアクセスすることを許可します。このルールは許可されたトラフィックおよびログ アクティビティに最良のセキュリティ プロファイルを適用します。

STEP 4 | 取引先、提携企業、顧客、その他のサードパーティに対し、データセンターへの限定的なアクセスを許可します。

このルールは、サードパーティのユーザーによるアクセスを厳格に制御し、それらのユーザーが必要とするサーバー上の必要なアプリケーションだけを使用できるようにする方法を示します。例えば、企業が SAP 開発者のグループを雇用するとします。開発の契約者はデータセンター内の SAP データベースにアクセスし、SQL クエリを発行する必要があります。しかし、SQL は SAP 開発者がアクセスできない本番用のデータベース上でも実行されます。企業は次の 3 つのアクセス ベクトルを制御する必要があります：

- ユーザーグループ—SAP 開発の契約者です。
- アプリケーション—MS-SQL および SAP です。
- サーバー—SAP データベースサーバーのみです。他のデータセンター サーバーのアクセスはすべて拒否します。

SAP 契約者のユーザーグループ、App-ID を隔離してグループが必要なアプリケーションだけを使用できるようにする User-ID、およびデータセンター内の SAP データベースサーバーのみにアクセスを限定するダイナミック アドレス グループを組み合わせることで、SAP 契約者が業務を行ううえで必要とするアクセスのみを企業が許可できるようになります。



このルールを作成するには：

- Source Zone（送信元ゾーン）および User（ユーザー）を指定し、アクセスを**Contractors**（契約者）ゾーンから来る**sap-contractors**グループのユーザーに限定します。
- Destination（宛先）を**SAP-Infra**ゾーン内の SAP データベースサーバー（**SAP DB Server**ダイナミック アドレス グループ）に制限します。

- デフォルトのポート上で、SAP 契約者が業務を行ううえで必要なアプリケーションだけを使用できるようにします。この例では、ルールが**ms-sql-analysis-service**、**mssql-db**、**mssql-mon**、および**sap**アプリケーションを許可します。

詳細なセキュリティポリシー許可ルールはビジネス上の目的で必要となるアクセス以外をすべて禁止し、攻撃の入り口を減らすことでリスクを少なくします。データセンターにアクセスする必要がある各サードパーティのグループに対し、同様の許可ルールを作成してください。

認証情報を保護するためにサードパーティのユーザーや企業を頼るのではなく、多要素認証（MFA、ユーザーからデータセンターへの認証ポリシールールを作成）を強制し、攻撃者が認証情報を盗んだ場合やサードパーティのシステムが感染した場合にアクセスを禁止できるようにします。過去数年間に発生したいくつかの大規模なデータ漏洩は、MFA 認証で防ぐことができたでしょう。

事前定義済みの Applications（アプリケーション）レポート（**Monitor**（監視）> **Reports**（レポート）> **Application Reports**（アプリケーション レポート）> **Applications**（アプリケーション））をチェックし、セキュリティポリシールールで明示的に許可されたアプリケーションのみが実行されていることを確認します。レポートに予期せぬアプリケーションが含まれている場合はアプリケーション許可ルールを確認してルールを調整し、予期せぬアプリケーションを許可しないようにしてください。

ユーザーからデータセンターへの認証ポリシールールを作成

認証ポリシールールは、ユーザーがデータセンター サービス、アプリケーション、その他のリソースにアクセスする前に、ユーザーが示す身元が正しいことを証明するよう求めます。攻撃者が認証情報を盗んでファイアウォールに認証すると、データセンター内の任意のアセットにアクセスしてデータを盗めるようになるおそれがあるため、特に最も価値の高い資産を保護するうえで、認証が重要になります。

センシティブなサーバーの場合やサードパーティのユーザーがサーバーにアクセスする場合（例えば、データセンター内の SAP サーバーにアクセスする SAP 開発の契約者）、多要素認証（MFA）を実装し、攻撃者が盗んだ認証情報を使ってシステムにアクセスするのを防止します。過去数年間に発生した大規模なセキュリティの侵害は、MFA を使用する認証ポリシーによって防げたはずです。

認証ポリシールールを作成（**Policies**（ポリシー）> **Authentication**（認証））する前に認証ポリシーの依存関係を構成し、認証方法、認証タイプ、認証サーバーにアクセスする方法、認証ポータルの利用を、どのサービスを使って誰がどのサーバーに認証できるのかを指定する認証ポリシールールと紐付ける必要があります。

STEP 1 | データセンター サーバーを使用するビジネス上の理由を持つ従業員ユーザーグループおよび各ユーザーを認証します。

このルールは、ユーザーが業務に必要なサーバー上のサービスにアクセスできるよう、ユーザーグループを認証する方法を示します。例えば、エンジニアは開発用サーバーおよびアプリケーションにアクセスする前に認証を行う必要があります。

		Source				Destination					
NAME	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
DevEng Resources	User to DC BP	Engineering-Users	any	api-users engg-users	any	Engineering-DC-infra	Dev-Servers	any	Perforce rdp service-http service-https ssh	Auth-Dev-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

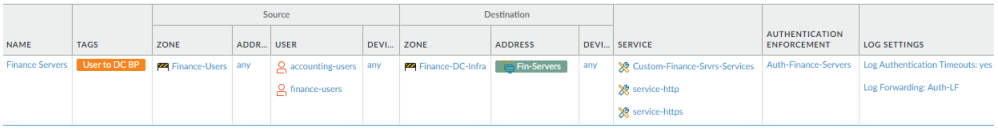
このルールを作成するには：

- データセンター内のエンジニアリング サーバーにアクセスする前に認証を行う必要があるエンジニアリング ユーザーグループを指定します（この例では**api-users**および**engg-users**）。
- ダイナミック アドレス グループ（**Dev-Servers**）を作成して Destination Address（宛先アドレス）として設定し、これらのユーザーグループによるデータセンターの開発用サーバーのアクセス リクエストに認証を適用します。
- ビジネス上の目的でエンジニアリング グループが使用する必要があるサービスに認証ルールを適用します。例えば、**Perforce**、**rdp**、**service-http**、**service-https**、および**ssh**（開発者は SSH および

RDP を使って Linux サーバーにアクセスしなければならない場合があり、それらのサーバーにアクセスする前に認証を行う必要があります）。認証ルール内のサービスは、グループが使用しなければならないサービスによって異なります。

- 認証方法を指定する認証適用オブジェクト（**Auth-Dev-Servers**）および認証プロファイルを設定し、ルールに追加します。
- 攻撃の試みを示唆する、ルールに対する違反を追跡・分析できるよう、アクティビティのログを取ってください。

認証のもう一つのユースケースは、グループが一連の特定のサーバーにアクセスしなければならない場合です。例えば、財務部門のユーザーが特定のサービスを使ってセンシティブな支払いカード情報（PCI）にアクセスする必要があり、アクセスする前に認証しなければならない場合があります。これらのサービスに対してユーザーを認証するために、このルールは、ファイアウォールが財務部門のユーザーを認証しなければならないサーバーだけを含むサービスグループを使用します（**Objects**（オブジェクト）> **Service Groups**（サービスグループ））。

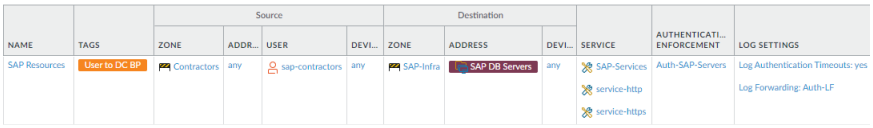


このルールを作成するには：

- データセンター内の財務サーバーにアクセスする前に認証を行う必要があるユーザーグループを指定します（この例では**accounting-users**および**finance-users**）。
- ダイナミック アドレス グループ（**Fin-Servers**）を作成して Destination Address（宛先アドレス）として設定し、これらのユーザーグループによるデータセンターの財務サーバーのアクセス リクエストに認証を適用します。
- 財務部門のユーザーがビジネス上の理由で使用する必要があるサービス（例えば**service-http**、**service-https**、およびカスタム サービス グループ**Custom-Finance-Srvrs-Services**で定義されている各サービス）に認証ルールを適用し、それらのサービスにアクセスする前にユーザーに認証を求めます。
- 認証方法を指定する認証適用オブジェクト（**Auth-Finance-Servers**）および認証プロファイルを設定し、ルールに追加します。
- 攻撃の試みを示唆する、ルールに対する違反を追跡・分析できるよう、アクティビティのログを取ってください。

STEP 2 | データセンターにアクセスしなければならない契約者、提携企業、顧客、その他の従業員以外のグループを認証します。

自社の従業員と比べて、契約者、提携企業、顧客などのサードパーティのユーザーグループのビジネスやセキュリティに関する行動は制御しづらいため、このルールではそのようなユーザーグループに対する MFA が求められます。2 つ以上の要素を使った認証をこれらのユーザーに求めることで、サードパーティの企業側で認証情報の盗難が生じてもデータセンターを保護できます。



このルールを作成するには：

- SAP 契約者がビジネス上の目的で必要とするサービスに認証ルールを適用します。カスタム サービス グループ（**Sap-Services**）を作成し、SAP 契約者が認証できるポートを定義して必要な他のサービスを追加します（この例では**service-http**および**service-https**）。
- 認証方法および認証プロファイルを指定する認証適用オブジェクト（**Auth-SAP-Servers**）を設定してルールに追加します。このケースでは、MFA をサポートしている認証タイプを使用し、MFA

サーバープロファイルを認証プロファイルに**Add**（追加）（**Factors**（要素）タブ）して、残りの作業を行ってMFA を構成する必要があります。

MFA を設定し、センシティブなシステムにアクセスするすべてのユーザーおよびユーザーグループを認証することで、認証情報を盗んだ攻撃者の攻撃を防止します。

- 攻撃の試みを示唆する、ルールに対する違反を追跡・分析できるよう、アクティビティのログを取ってください。

STEP 3 | 管理・保守を行うために安全な方法でデータセンター サーバーにアクセスしなければならない IT 担当者など、特別なアクセスが必要なユーザーを認証します。

このルールは、重要なシステムに対して管理者アクセスを行える権限付きのアカウントを持つユーザーを認証するための設定方法を示します。権限付きのユーザーの認証情報が盗まれると攻撃者がデータセンターやその貴重なアセットにアクセスできるようになってしまうため、2 つ以上の要素を使った認証を求め、必ず正当なユーザーだけにアクセスを許可するようにしてください。この例は、データセンター サーバーの管理インターフェイスにアクセスする適切な IT 部門のユーザーを認証する方法を示します。

		Source				Destination					
NAME	TAGS	ZONE	ADDR...	USER	DEVI...	ZONE	ADDRESS	DEVI...	SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
IT Secured Access	User to DC BP	IT-Users	any	it-superusers	any	IT-Server-Access-DC	IT-Server-Management	any	Custom-IT-Ports	Auth-IT-Server-Mgmt	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

このルールを作成するには：

- データセンター サーバーの管理インターフェイスにアクセスする前に認証しなければならない権限付きのアカウントを持つユーザーを指定します（この例では**it-superusers**グループ）。
- ダイナミック アドレス グループ（**IT-Server-Management**静的アドレスグループ）を作成して Destination Address（宛先アドレス）として設定し、ユーザーグループによるデータセンターの管理インターフェイスのアクセス リクエストに認証を適用します。
- 権限付きの IT 担当者がビジネス上の目的で使用しなければならないサービスに認証ルールを適用します（この例ではすべてのサーバーの管理用ポートを識別する**Custom-IT-Ports**カスタム サービス グループであり、同じサブネット上に配置する必要があります）。
- 認証で MFA（2 要素）を求める認証適用オブジェクト（この例では**Auth-IT-Server-Mgmt**）を設定・適用します。MFA サーバープロファイルを認証プロファイルに**Add**（追加）（**Factors**（要素）タブ）し、MFA を設定する残りの作業を行います。デバイス管理を行える、権限付きのアカウントを持つ IT 部門の各ユーザーの本人確認を必ず行わなければならないため、MFA を使用する必要があります。

  MFA を構成する際に認証要素の認証タイムスタンプを設定し、攻撃者が盗んだ認証情報を使って、あるいはワークステーションがロックされずに放置された隙をついてデータセンターに信任するリスクをさらに減らします。データセンターのアセットは重要であるため、サービスおよびアプリケーションのセキュリティを最優先してください。
- ルールに対する違反を追跡・分析できるよう、アクティビティのログを取ってください。

また、IT 担当者はスイッチ、ルーター、データセンター内のその他のデバイスも管理します。同じグループの IT ユーザーがそれらのリソースを管理する場合、宛先ゾーンおよびアドレスにそれらを追加すれば、IT スーパーユーザーがそれらのデバイスの管理インターフェイスにアクセスする前に、ルールが認証を行うようになります。別の IT ユーザーグループが一連の異なるデータセンター リソースを管理する場合は、強固なセキュリティポリシールール、対応する認証ポリシー、各ユーザーグループ用の復号化ポリシー ルールを別途作成します。

認証情報はクリアテキストで送信しないでください。例えば *RADIUS* を使う場合はサポートされている EAP 方式を使って TLS 内で安全に認証情報を転送します。

ユーザーからデータセンターへの復号化ポリシー ルールを作成

ユーザーの元からデータセンターに入るトラフィック用の復号化ポリシー ルールを作成して可視性を確保し、トラフィックを検査して最も価値の高い資産を保護します。一連のデータセンター サーバーに対するアクセスをユーザーグループ（あるいは特定のユーザー）に許可するセキュリティポリシー ルールを作成する際、トラフィックを復号化する復号化ポリシー ルールを作成します。

データセンターには最も価値の高い資産が保存されているため、復号化できるデータセンター トラフィックはすべて復号化してください。リスクの高いトラフィック カテゴリーの復号化、一番信頼できないネットワーク セグメントの復号化から開始（例えば、信頼できる内部セグメントからのトラフィックよりも提携企業、顧客、契約者からのサードパーティ トラフィックの復号化を優先）し、データセンターのあらゆるアセットに向かうトラフィックに復号化を適用するまで、作業範囲を広げていきます。許容できるパフォーマンスを維持しつつ、できるだけトラフィックを復号化するようにしてください。

不適切なトラフィックをデータセンターの復号化から除外。個人情報に関する規制やコンプライアンス強健は、国や地域毎に異なります。また、企業毎に個人情報に関するコンプライアンス規則が異なります。トラフィックをできるだけ復号化しますが、規制や企業の規則によって復号化から除外することが求められている情報がデータセンターにある場合、そのトラフィックは復号化しません。

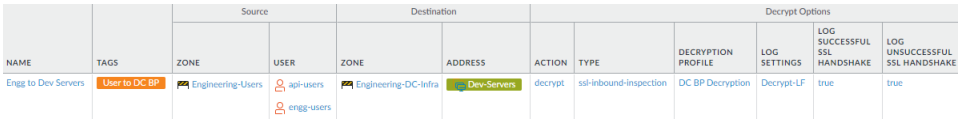
DNSアクセスを許可し、エンジニアリング部門のユーザーがエンジニアリング用の開発用サーバーにアクセスし、SAP開発の契約者が SAP 開発用サーバーにのみアクセスし、一連の特定のIT部門のユーザーが管理目的でデータセンターサーバーにアクセスするのを許可するセキュリティポリシールールを作成しました。ここでは、これらのルールが許可するトラフィックを復号化する復号化ポリシー ルールを作成（**Policies**（ポリシー）> **Decryption**（復号化））します。

復号化ポリシー ルールは、これらのトラフィック フローに関連する一部の共通要素を共有します：

- 復号化ポリシー ルールを作成する目的は、セキュリティポリシー ルールがトラフィックを検査し、ポリシーに基づいてそれを許可あるいはブロックできるように、トラフィックを復号化することです。そのためには、復号化ポリシー ルールが類似のセキュリティポリシー ルールと同じ送信元ゾーンおよびユーザーを使用し、同じ宛先ゾーンおよびアドレス（サーバーを追加･削除する際にコミット操作なしでファイアウォールをアップデートできるよう、ダイナミック アドレス グループで定義されていることが多い）を使用する必要があります。セキュリティポリシーおよび復号化ポリシーで同じ送信元および宛先を定義することで、同じトラフィックに両方のポリシーを適用します。
- ステップ 4に示されている通り、センシティブな個人情報の場合を除き、これらのルールのAction（アクション）はすべて復号化になります。
- 各ルールに対して、復号化のロギングとログ転送を設定します。ファイアウォールのリソースが許可する限り、できる限りの復号化トラフィックをログに記録します。
- SSL インバウンド インスペクションを使用してインバウンド トラフィックを検査する復号化ルールには、適切なサーバー証明書が求められます。
- これらすべての復号化ルールは、データセンターの最良の復号化プロファイルを作成で紹介するベストプラクティスのデータセンター復号化プロファイルを使用します。

STEP 1 | 従業員ユーザーグループからデータセンター サーバーに向かう、許可されたトラフィックを復号化します。

このルールは、ユーザーグループからグループがアクセスできるデータセンター サーバーに向かうトラフィックを復号化してトラフィックに対する可視性を確保する方法を示します。例えば、作成したアプリケーション許可ルールは、エンジニアリング部門のユーザーがデータセンター内の開発用サーバーにアクセスするのを許可するセキュリティポリシー ルールを含みます。開発用サーバーを保護するために、インバウンド トラフィックを復号化し、ファイアウォールが検査を行って脅威防止プロファイルを適用できるようにしてください。



NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Engg to Dev Servers	User to DC BP	Engineering-Users	api-users engg-users	Engineering-DC-Infra	Dev-Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

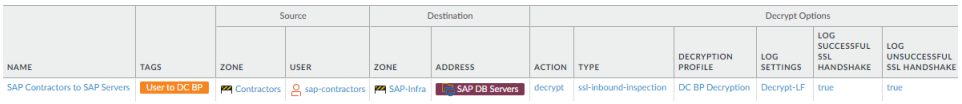
このルールを作成するには：

- 類似のセキュリティポリシールールと同じ送信元および宛先を指定します。このケースでは、Source（送信元）ユーザーが **Engineering-Users**ゾーン内の**api-users**および**engg-users**ユーザーグループ、Destination（宛先）が**Engineering-DC-Infra**ゾーン内の**Dev-Servers**ダイナミック アドレス グループで指定されているサーバーになります。
- Options（オプション）タブで Action（アクション）を**Decrypt**（復号化）に、復号化の Type（タイプ）を**SSL Inbound Inspection**（**SSL** インバウンド インスペクション）に設定します。開発用サーバーのサーバー証明書を指定してデータセンターの最良の復号化プロファイルを適用し、SSL 転送プロキシおよび SSL プロトコル設定をトラフィックに適用します。

送信元ゾーンおよびユーザーグループ（あるいはユーザー）、宛先ゾーンおよびサーバーグループ（ダイナミック アドレス グループのメンバーシップで定義）に基づき、各ユーザーグループ（あるいは適切な場合は個々のユーザー）の許可されたデータセンター トラフィックに使用する、同様の復号化ポリシー ルールを作成します。

STEP 2 | 契約者、提携企業、顧客、その他のサードパーティから来る許可されたトラフィックを復号化してください。

このルールは、サードパーティのグループから、グループがアクセスできるデータセンター サーバーへのトラフィックを復号化する方法を示します。例えば許可ルールには、SAP 開発の契約者によるデータセンター内の SAP データベースサーバーへ限定的なアクセスを許可するセキュリティポリシー ルールが含まれます。インバウンド トラフィックを復号化することで、ファイアウォールがトラフィックを検査して脅威防止プロファイルを適用し、SAP データセンター サーバーを保護できるようにしてください。



NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
SAP Contractors to SAP Servers	User to DC BP	Contractors	sap-contractors	SAP-Infra	SAP DB Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

このルールを作成するには：

- 類似のセキュリティポリシールールと同じ、復号化するトラフィックの送信元および宛先を指定します。このケースでは、Source（送信元）ユーザーが**Contractors**（契約者）ゾーン内の**sap-contractors**ユーザーグループ、Destination（宛先）が**SAP-Infra**ゾーン内の**SAP DB Servers**（**SAP DB** サーバー）ダイナミック アドレス グループで指定されているサーバーになります。
- Options（オプション）タブで Action（アクション）を**Decrypt**（復号化）に、復号化の Type（タイプ）を**SSL Inbound Inspection**（**SSL** インバウンド インスペクション）に設定します。開発用サーバーのサーバー証明書を指定してデータセンターの最良の復号化プロファイルを適用し、SSL 転送プロキシおよび SSL プロトコル設定をトラフィックに適用します。

送信元ゾーンおよびユーザーグループ、宛先ゾーンおよびサーバーグループ（ダイナミック アドレス グループのメンバーシップで定義）に基づき、各サードパーティ グループの許可されたデータセンター トラフィックに使用する、同様の復号化ポリシー ルールを作成します。

STEP 3 | データセンター サーバーに対する許可された権限付きのアクセスを復号化してください（規制やコンプライアンス規則によって復号化が禁止されている個人情報に関わるトラフィックを除く）。

ユーザーの信頼性の高さに関わらず、できるだけトラフィックを復号化して可視性を確保することでデータセンターを保護する必要があるため、このルールは、権限付きアクセスのトラフィックを復号化する方法を示します。許可されたトラフィックを復号化しなければ脅威防止プロファイルを適用できず、トラフィックにマルウェアやその他の脅威が潜んでいてもそれを把握できません。この例で

は、以前に作成したセキュリティポリシーの許可ルールを参照しつつ、IT スーパーユーザーがデータセンターサーバーの管理インターフェイスにアクセスできるようにします。

データセンター サーバーの管理・保守を行う *IT* グループが *SSH* を使用する場合、*SSH* トラフィックを復号化することはできません。SSH プロキシを構成して *SSH* トンネルをブロックすることで、*SSH* が悪意のある可能性があるコンテンツやアプリケーションをトンネル化するのを防止できます。*IT* グループが *SSL* を使用する場合は、*SSL* インバウンド インスペクションではなく *SSL* 転送プロキシを使用する復号化ポリシー ルールを作成してください。これは、*SSL* インバウンド インスペクションが復号化を行うためにはサーバー証明書が必要になるためです。*IT* 部門は多くのデータセンター サーバーを管理しますが、各サーバー用に *SSL* インバウンド インスペクション ルールを作成するのは手間がかかり、管理も難しくなります。このユースケースでは、*SSL* 転送プロキシによってより優れたスケーリングが可能になります。

次の例では、SSL 転送プロキシを使用する場合の復号化ポリシー ルールを示します。

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Management	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

このルールを作成するには：

- 類似のセキュリティポリシールールと同じ、復号化するトラフィックの送信元および宛先を指定します。このケースでは、Source（送信元）ユーザーが**IT-Users**ゾーン内の**it-superusers**ユーザーグループ、Destination（宛先）が**IT-server-access-DC**ゾーン内の**IT-Server-Management**静的アドレスグループで指定されているサーバーになります。
- Options（オプション）タブで Action（アクション）を**Decrypt**（復号化）に、復号化の Type（タイプ）を**SSL Forward Proxy**（**SSL** 転送プロキシ）に設定します。データセンターの最良の復号化プロファイルを適用し、SSL 転送プロキシおよび SSL プロトコル設定をトラフィックに適用します。

権限付きアクセスを必要とするグループが他にある場合は、各グループに対して同様のタイプの復号化ポリシー ルールを作成してください。

また、IT 担当者はスイッチ、ルーター、データセンター内のその他のデバイスも管理します。同じグループの IT ユーザーがそれらのリソースを管理する場合、宛先ゾーンおよびアドレスにそれらを追加すれば、それらのデバイスの管理インターフェイスに接続するトラフィックをルールが復号化できるようになります。別の IT ユーザーグループが一連の異なるデータセンター リソースを管理する場合は、強固なセキュリティポリシールール、各ユーザーグループ用の復号化および認証ポリシー ルールを別途作成します。

次の例では、SSH プロキシを使用する場合の復号化ポリシー ルールを示します。SSH プロキシ復号化を使用する代わりに、トラフィックを復号化しないことにするのも可能です。

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Mgmt-SSH	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssh-proxy	DC BP Decryption	none	false	true

このルールを作成するには：

- トラフィックの送信元および宛先は、前述の SSL 転送プロキシのルールの例のものと同じです。
- Options（オプション）タブで Action（アクション）を**Decrypt**（復号化）に、復号化の Type（タイプ）を**SSH Proxy**（**SSH** プロキシ）に設定します。データセンターの最良の復号化プロファイルを適用し、SSH プロキシおよび SSL プロトコル設定をトラフィックに適用します。

  また、IT 担当者はデータセンターのスイッチ、ルーター、その他のデバイスも管理します。同じグループの IT ユーザーがそれらのリソースを管理する場合、宛先ゾーンおよびアドレスにそれらを追加すれば、それらのデバイスの管理インターフェイスに接続するトラフィックをルールが復号化できるようになります。別の IT ユーザーグループが一連の異なるデータセンター リソースを管理

する場合は、強固なセキュリティポリシールール、各ユーザーグループ用の復号化および認証ポリシー ルールを別途作成します。

STEP 4 | 規制やコンプライアンス規則によって禁止されている場合は、センシティブな個人情報を復号化しないでください。

このルールは、規制やコンプライアンス関連の要件によってトラフィックを復号化から除外しなければならない場合に、ポリシー ベース復号化除外を作成する方法を示します。この例では、以前に作成したセキュリティポリシーの許可ルールを参照して、財務部門のユーザーに財務サーバーへのアクセスを与えます。規制やコンプライアンス関連の要件によってこのトラフィックを復号化することが許可されている場合は、ファイアウォールがトラフィックを把握して脅威を防止できるよう、復号化を行ってください。

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Finance PCI No Decrypt	User to DC BP	Finance-Users	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	no-decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

このルールを作成するには：

- 類似のセキュリティポリシールールと同じ、復号化するトラフィックの送信元および宛先を指定します。このケースでは、Source（送信元）ユーザーが **Finance-Users**ゾーン内の**accounting-users**および**finance-users**ユーザーグループ、Destination（宛先）が**Finance-DC-Infra**ゾーン内の**Fin-Servers**ダイナミック アドレス グループで指定されているサーバーになります。
- Options（オプション）タブで、Action（アクション）を**No Decrypt**（復号化なし）に設定します。証明書の問題から保護するために、データセンターのベストプラクティスNo Decryption（復号化なし）プロファイルを適用します。

No Decryption（復号化なし）プロファイルをTLSv1.3トラフィックには適用しないでください。証明書情報は暗号化されているため、ファイアウォールが証明書情報に基づいてセッションをブロックできません。

最初のインターネットからデータセンターへのトラフィックのセキュリティポリシーを定義

他のデータセンター トラフィックのフローの場合と同様に、アプリケーション許可セキュリティポリシールールを使ってインターネットからデータセンターに流れるトラフィックを強固に制御し、未知あるいは制限されていないアプリケーションがデータセンターに侵入するのを防ぎます。さらに、データセンターの WEB サーバー層に向かう外部トラフィックに（DoS 保護プロファイルと共に）DoS 保護ポリシールールを適用し、データセンターの WEB サーバーをサービス拒否（DoS）攻撃から保護します。

- インターネットからデータセンターへのトラフィックを保護するためのアプローチ
- インターネットからデータセンターへのアプリケーション許可ルールを作成
- インターネットからデータセンターへの DoS 保護ポリシー ルールを作成
- インターネットからデータセンターへの復号化ポリシー ルールを作成

インターネットからデータセンターへのトラフィックを保護するためのアプローチ

インターネットからデータセンターへと流れるデータセンター トラフィックを保護する従来型の古いアプローチの場合、貴重なアセットがリスクにさらされたままになりますが、ベストプラクティスのアプローチであれば、貴重なアセットを保護できます。データセンターに入るトラフィックによって生じる最も大きなリスクは、感染した外部サーバーから意図せずマルウェアをダウンロードしたり、セキュリティを破られたデータセンター サーバーから外部サーバーにマルウェアを移動させてしまったりすることです。

従来型のアプローチ	リスク	ベストプラクティスのアプローチ
ポート ベースのセキュリティポリシーを作成します。	悪意のあるアプリケーションは、ポート番号を偽装したり、トンネル内でポートを抜けたり、ポート ホッピングを使用して発見をまぬがれたりすることでネットワークにアクセスします。	アプリケーション許可ルールは、アプリケーションがh非標準ポート上で実行されるのを防ぎます。許可リスト違反を監視し、ログに記録します。 ポートベースからアプリケーション ベースのルールに移行する際、ルールベース内で、入れ替えるポートベースのルールよりも上にアプリケーション ベースのルールを配置し両方のルールのポリシー ルール ヒット数をリセットします。トラフィックがポートベースのルールにヒットすると、そのポリシールールのヒット数が増加します。一定期間どのトラフィックもポートベースのルールにヒットしなくなるまでアプリケーション ベースのルールを調整して

従来型のアプローチ	リスク	ベストプラクティスのアプローチ
		から、ポートベースのルールを削除します。
侵入防止システム（IPS）が侵入検知システム（IDS）としてデプロイされることも良くあります。	IPS はインバンドの検知および保護システムであり、IDS はアウトオブバンドの検知システムです。IPS を IDS としてデプロイすると、侵入検知が送信元および宛先間の直接通信パスの外で行われるため、リアルタイムに保護できず、脅威がデータセンターに入るおそれがあります。	ファイアウォールのインバンドでPalo Alto Networksの App-ID、User-ID、コンテンツIDを使用し、アクセスを強固に制御するアプリケーションの許可リストセキュリティポリシーを作成してください。セキュリティプロファイルを適用して既知および新しい脅威を防止します。
Web アプリケーション ファイアウォールはデータセンターを十分保護できます。	攻撃者はコマンド アンド コントロール（C2）ソフトウェアを感染したデータセンターのエンドポイント上に配置し、ネットワークに攻撃の入り口を作り、さらにウォータリングホール攻撃によってクライアント側をエクスプロイトする可能性もあります。	単純に厳格なアンチスパイウェア セキュリティ プロファイルをトラフィックを制御するセキュリティポリシー ルールに割り当てることで、攻撃者が C2 ソフトウェアをデータセンターのエンドポイント上に配置するのを阻止できます。このプロファイルはファイアウォールに含まれている機能の一つであるため、保護を適用してもコストが増えることはありません。

インターネットからデータセンターへのアプリケーション許可ルールを作成

インターネットからデータセンターに入るトラフィックに関する最も大きなリスクは、クライアントがデータセンター内の攻撃されたサーバーからデータを取得する場合に、感染した外部のクライアントから意図せずマルウェアをダウンロードしたり、外部サーバー上にマルウェアを不意に残してしまったりすることです。インターネットからデータセンターに向かうトラフィックを保護し、サーバーの脆弱性を狙うマルウェアを不意にダウンロードしたり、提携企業、顧客を感染させるおそれのあるマルウェアをクライアントがダウンロードしたり、業界で使用するウェブサイトを妨げたり（ウォータリングホール攻撃に加担）しないようにします。

データセンターに向かうトラフィックの送信元が悪意のある IP アドレスやその他の危険な送信元から来ないようにし、ビジネス上の目的で必要となるアプリケーションだけを許可するようにしてください。また、データセンター内で不要な（特に未知の）アプリケーションを許可しないようにしてください。そのためには：

- 外部デバイスがデータセンターと通信するために使用できる許可されたアプリケーションを制御する許可ルールを作成します。

  事前定義済みの*Sanctioned*（許可）タグを使ってすべての許可されたアプリケーションをタグ付けします。*Panorama* およびファイアウォールは、*Sanctioned* タグが付いていないアプリケーションを許可されていないアプリケーションとみなします。
- 不適切な IP アドレスを識別する外部動的リストを作成し、それを使って対象の IP アドレスがデータセンターにアクセスするのを防ぎます。
- すべての専有アプリケーションに対してカスタム アプリケーションを作成し、アプリケーションを識別して保護できるようにします。

  一連のポート用のカスタム セッション タイムアウトを定義するだけの目的で作成した既存のアプリケーション オーバーライド ポリシーがある場合、サービスベースのセッション タイムアウトを設定

して各アプリケーションのカスタム タイムアウトを管理してからルールをアプリケーション ベースのルールに移行することで、既存のアプリケーション オーバーライド ポリシーをアプリケーション ベースのポリシーに変換します。アプリケーション オーバーライド ポリシーはポートベースです。アプリケーション オーバーライド ポリシーを使用して一連のポートのカスタム セッション タイムアウトを管理する際、それらのフローに対するアプリケーションの可視性が失われるため、どのアプリケーションがポートを使用するのか把握することも、管理することもできません。サービスベースのセッション タイムアウトはアプリケーションの可視性も維持しつつ、カスタム タイムアウトを利用できるようにします。

- マルウェア、脆弱性、C2トラフィック、既知および未知の脅威を防ぐためのルールを許可する、ベストプラクティスセキュリティプロファイルで構成されるベストプラクティスセキュリティプロファイルグループを適用してください。
- セッション終了時に、許可したすべてのトラフィックをログに記録して、ルール違反を追跡、解析してください。該当する場合はログサーバーにログを転送、ログのメールを適切な管理者に転送します。

データセンター セキュリティポリシーのルールベースの順序を指定は、これらのルールと、他の 3 つのデータセンター トラフィック フロー用に作成するその他すべてのルールおよびブロック ルールの順序を決め、あるルールによって他のルールが遮られないようにする方法を説明します。

複数のデータセンター全体にかけて一貫した形でセキュリティポリシーを適用するために、テンプレートおよびテンプレート スタックを再利用し、同じポリシーをすべてのデータセンターに適用することができます。このテンプレートは、グローバル セキュリティポリシーを維持し、管理しなければならないテンプレートおよびテンプレート スタックの数を減らしつつ、*IP* アドレス、*FQDN* などのデバイス固有の値を適用するために変数を使用します。

ベンダー、取引先、顧客からの許可されたアプリケーション トラフィックの宛先を必要なアプリケーションに制限して許可します。

このルールは、許可するアプリケーションを強固に制御し、それらをデフォルトのポート上でのみ許可し、外部動的リストを使って既知の不適切な IP アドレスを特定することで既知の悪いソースをブロックすることで、外部のソースからデータセンターに至るアプリケーション トラフィックを保護する方法を示します。

このルールを作成するには：

- 既知の悪い送信元がデータセンターにアクセスしようとするのを防ぎます。セキュリティポリシールールの**Source Address**（送信元アドレス）内の**Negate**（移動）オプションを使って不適切な IP アドレスからの接続をブロックします。この例では、外部動的リスト（**Bad IPs List**（不適切な **IP** リスト））を使って既知の不適切な IP アドレスを識別してブロックします。（取り消し線のある送信元アドレスは、許可ではなく拒否されることを示します。）
- ビジネス上の目的で必要となるアプリケーションだけに制限し、デフォルトのポート（**application-default**）上でのみ実行を許可し、セキュリティをかいくぐるマルウェアを標準的でないポート上で実行しようとする試みを防ぎます。ベンダーが**Acme**という名前の専有アプリケーションを使用するこの例では、ファイアウォールがトラフィックを分類化して適切なセキュリティポリシーを適用できるよう、**Acme**専有アプリケーションを識別するカスタム アプリケーションを作成しました。
- **Acme**アプリケーション トラフィックの宛先を、**Web-Server-Tier-DC**ゾーン内の**Web-Servers**ダイナミック アドレス グループに制限します。宛先アドレスが WEB サーバー層内にない場合、ファイアウォールはトラフィックをドロップします。

事前定義済みの Applications（アプリケーション）レポート（**Monitor**（監視）> **Reports**（レポート）> **Application Reports**（アプリケーション レポート）> **Applications**（アプリケーション））を確認し、セキュリティポリシールールで明示的に許可したアプリケーションのみが実行されていることを確認しま

す。レポートに予期せぬアプリケーションが含まれている場合はアプリケーション許可ルールを確認してルールを調整し、予期せぬアプリケーションを許可しないようにしてください。

インターネットからデータセンターへの復号化ポリシー ルールを作成

復号化ポリシー ルールを作成してデータセンターからインターネットに向かうトラフィックに対する可視性を確保し、トラフィックにセキュリティポリシーを適用できるようにします。一連のデータセンターサーバーへのアクセスを許可するセキュリティポリシー ルールを作成する際、トラフィックを復号化する復号化ポリシー ルールを作成します。「インターネットからデータセンターへのアプリケーション許可ルールを作成」では、許可したアプリケーションだけを使ってインターネットからデータセンター内のWebサーバー群へのアクセスを許可するセキュリティポリシー ルールを作成しました。ここでは、ルールで許可するトラフィックを復号化する復号化ポリシー ルールを作成します（**Policies**（ポリシー）> **Decryption**（復号化））。

セキュリティポリシー ルールがトラフィックを検査し、ポリシーに基づいてそれを許可あるいはブロックできるよう、トラフィックを復号化するためには、復号化ポリシー ルールが類似のセキュリティポリシールールと同じ送信元ゾーンおよびユーザーを使用し、同じ宛先ゾーンおよびアドレス（サーバーを追加･削除する際にコミット操作なしでファイアウォールをアップデートできるよう、ダイナミック アドレス グループで定義されていることが多い）を使用する必要があります。セキュリティポリシーおよび復号化ポリシーで同じ送信元および宛先を定義することで、同じトラフィックに両方のポリシーを適用します。

復号化ルールは、データセンターの最良の復号化プロファイルを作成で紹介するベストプラクティスのデータセンター復号化プロファイルを使用します。

各ルールに対して、復号化のロギングとログ転送を設定します。ファイアウォールリソースが許可する限り、できる限りの復号化トラフィックをログに記録します。

STEP 1 | インターネットからデータセンターの WEB サーバーに向かう、許可されたトラフィックを復号化します。

このルールは、データセンターへの接続を外部から開始したトラフィックを復号化する方法を示します。例えば、作成したアプリケーション許可ルールは、特定のアプリケーションのみを使用して外部のトラフィックがデータセンターのWebサーバーにアクセスすることを許可します。データセンターの WEB サーバーを保護するために、ファイアウォールがトラフィックを検査して脅威防止プロファイルを適用できるよう、トラフィックを復号化します。

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Internet to DC	Internet to DC BP	L3-External	any	Web-Server-Tier-DC	Web Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

このルールを作成するには：

- 類似のセキュリティポリシールールと同じ送信元および宛先を指定します。このケースでは、**L3-External**ゾーンが Source（送信元）、**Web-Server-Tier-DC**ゾーン内の**Web-Servers**ダイナミック アドレス グループで指定されたサーバーが Destination（宛先）です。
- Options（オプション）タブで Action（アクション）を**Decrypt**（復号化）に、復号化の Type（タイプ）を**SSL Inbound Inspection**（**SSL** インバウンド インスペクション）に設定します。WEB サーバーのサーバー証明書を指定してデータセンターの最良の復号化プロファイルを適用し、SSL 転送プロキシおよび SSL プロトコル設定をトラフィックに適用します。

STEP 2 | アクセスを許可する場合は、インターネットから他のサーバーグループに向かうトラフィック、および許可する他のアプリケーション用に同様の復号化ポリシー ルールを作成してください。

インターネットからデータセンターへの DoS 保護ポリシー ルールを作成

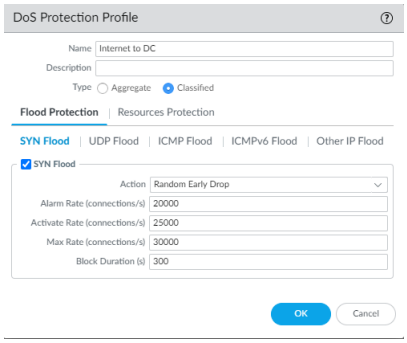
インターネットに接続されたターゲットのシステムを圧倒してダウンさせ、正当なあらゆるユーザーやサービスがシステムを利用できなくさせることを目的としたサービス拒否（DoS）攻撃が、攻撃者がネットワークを妨害する方法の一つです。データセンターの WEB サーバーをダウンさせれば、ほとんどのデータセンターへの正当なアクセスを妨害できるため、データセンターの WEB サーバーは格好のターゲットになります。

それらのサーバーに向かうインターネット トラフィックに分類化DoS 保護プロファイルを適用することで、データセンターの WEB サーバー層を保護します。分類化 DoS 保護ポリシーは、インバウンドの接続数を制御する分類化DoS 保護プロファイルをポリシーで定義されたトラフィックに適用します。

さらに、各ゾーンに対してパケット バッファ保護を設定し、ファイアウォールのパケット バッファを溢れさせ、特に重要なサービスを保護するファイアウォールに正当なトラフィックをドロップさせようとする単一セッション DoS 攻撃からファイアウォールを保護します。

STEP 1 | 1 秒あたりの接続数を制限してSYN フラッド攻撃を防止することでデータセンターの WEB サーバーを DoS 攻撃から保護する、分類化 DoS 保護プロファイルを作成します。

この DoS 保護プロファイルは、プロファイルに付与した DoS 保護ポリシールールで定義されたトラフィックの 1 秒あたりの接続数（CPS）を制限し、DoS 攻撃によって WEB サーバーがダウンするのを防ぎます。このプロファイルは、アラートを発生させたり、ランダム早期ドロップ（RED）パケット ドロップを有効化したり、新規接続をブロックしたりするためのプログレッシブ CPS しきい値、および新規接続をブロックする期間を指定します。データセンターの WEB サーバーを保護するための CPS しきい値の設定は、WEB サーバーの能力によって異なります。



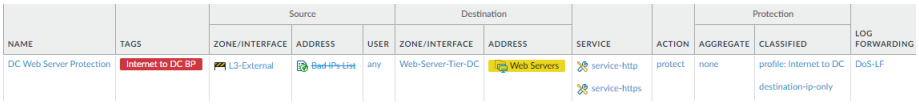
このプロファイルを作成するには：

- **Objects**（オブジェクト）> **Security Profiles**（セキュリティ プロファイル）> **DoS Protection**（**DoS** 保護）でClassifiedタイプのDoS プロテクションプロファイルを**Add**（追加）します。
- プロファイルに**Name**（名前）を付け、**Classified**（分類化）をプロファイルの**Type**（タイプ）として選択し、CPS レートが**Max Rate**（最大レート）のしきい値に達した際にアラートを発生（**Alarm Rate**（アラーム レート））させたり、RED を有効化（**Activate Rate**（アクティベート レート））したり、新規セッションのブロックを開始（**Max Rate**（最大レート））したり、新規セッションをブロックする期間を設定（**Block Duration**（ブロック期間））したりするための CPS 値を設定します。

UDP などのプロトコルやその他の *IP* プロトコルを使用しない場合、アプリケーションを許可するセキュリティポリシールールおよびゾーン プロテクション プロファイルを組み合わせて使用してそれらを制限し、ブロックするプロトコルのフラッド防御 *CPS* を *0* に設定することで使用しないプロトコルをブロックします。

STEP 2 | DoS 攻撃から保護したいサーバーを定義する分類化 DoS 保護ポリシールールを作成し、DoS 保護プロファイルをそれに付与します。

このルールは、SYN フラッド攻撃によってデータセンターの WEB サーバーがダウンするのを防ぎます。この例では、WEB サーバー層への接続を許可された外部のトラフィックに分類化 DoS 保護プロファイルを適用します。



このルールを作成するには：

- WEB サーバーに向かうトラフィックに DoS 保護を適用するためには、トラフィックを許可するセキュリティポリシー ルールと同じトラフィックに DoS 保護ポリシーを適用する必要があります。この例で、このDoSルールは「インターネットからデータセンターへのアプリケーション許可ルールを作成」で許可したトラフィックを保護します。
- Option/Protection（オプション/保護）タブでWEB サービスを指定（**service-http**および**service-https**）し、Action（アクション）を**protect**（保護）に設定して DoS 保護プロファイルの SYN フラッドのしきい値をトラフィックに適用し、Log Forwarding（ログ転送）方法を設定し（ログ転送の設定を行っていることが前提）、前のステップ（**Internet to DC**（インターネットから **DC**））でトラフィック用に構成したClassifiedタイプのDoSプロテクションプロファイルを選択します。

内部ソースからの SYN フラッド攻撃を防止するためには、DoSプロテクションポリシールールを別途作成し、送信元ゾーンとして**L3-External**ではなく内部ゾーンを指定します。外部および内部の攻撃ソースに対して個別のルールを作成することで別々にレポートを作成すれば、攻撃の試みを調査しやすくなります。

最初のデータセンターからインターネットへのトラフィックのセキュリティポリシーを定義

データセンターのアーキテクチャによっては、データセンター内のサーバーがインターネットを介してソフトウェア更新を取得したり、サーバー証明書の失効状態を確認したりする場合があります。ユーザーの通信に焦点を当ててセキュリティ計画が立てられ、インターネットと通信するサーバーが見落とされている場合もよくあるため、データセンターは攻撃者にとって格好の潜伏場所になります。データセンターサーバーがインターネットと直接通信し始める際、いくつかのセキュリティリスクを防止する必要があります：

- データ漏洩–攻撃者が FTP や HTTPなどの正当なアプリケーション、あるいは DNS トンネリングなどの他の方法を使ってデータを盗みます。サーバーの更新に必要なアプリケーションのみを許可するアプリケーションセキュリティポリシー ルール許可リストを作成し、他の状況では正当とみなされるアプリケーションも含め、他のすべてのアプリケーションをブロックします。アプリケーション ルールが強固でなければ、攻撃の機会を与えてしまいます。
- 正当なアプリケーションを使用するコマンド アンド コントロール（**C2**）–データセンター サーバーがソフトウェア更新用でない正当なアプリケーションを使ってインターネットと通信するのを許可する場合、他の場合は正当とみなされるそれらのアプリケーションを使って攻撃者が C2 アクティビティを行える可能性があります。例えば、標準的でないポート上でウェブブラウジングを許可すると、攻撃の機会を与えてしまいます。サーバーが他のアプリケーションではなくソフトウェア更新に必要な特定のアプリケーションだけを使ってデフォルトのポート上でのみインターネットと通信するのを許可してください。他の使用目的ではそのアプリケーションが正当であり、制限が加えられている場合もこれに該当します。
- さらなるマルウェアのダウンロード–攻撃者がデータセンター サーバーのセキュリティを破ると、サーバー上のマルウェアが phone-home やその他のメカニズムを通じてインターネットからマルウェアをさらにダウンロードするおそれがあります。必要な更新アプリケーションを使って適切な更新サーバーとのみ通信することを許可する厳格な許可ルールにより、攻撃者がマルウェアをホストするウェブサイトと通信してデータを盗むことを防止できます。さらに、Cortex XDRエージェントをデータセンターサーバー（およびすべてのエンドポイント）にインストールすることで、すでにサーバー上に存在するマルウェアが実行されるのを防止できます。

- データセンターからインターネットへのトラフィックを保護するためのアプローチ
- データセンターからインターネットへのアプリケーション許可ルールを作成
- データセンターからインターネットへの復号化ポリシー ルールを作成

データセンターからインターネットへのトラフィックを保護するためのアプローチ

従来型の古いアプローチでインターネットに向かうデータセンター トラフィックを保護すると、貴重なアセットがリスクにさらされたままになってしまいますが、ベストプラクティスのアプローチであれば貴重なアセットを保護できます。

従来型のアプローチ	リスク	ベストプラクティスのアプローチ
ポートベースのルールおよび/または IP ベースのルールを	ポートベースおよび IP ベースのルールは、インターネットへの接続をどのアプリケーション	更新コンテンツを取得するデータセンターサーバーだけが正当なアプリケーションのみを使って正当な更新サーバーとのみ通信することを許

従来型のアプローチ	リスク	ベストプラクティスのアプローチ
作成し、信頼できるネットワークに対して十分な保護を適用します。	に許可するのかを制御できません。ポートが開いていれば、すべてのアプリケーションがそのポートを利用できます。	可する、厳格なアプリケーションベースの許可ルールを作成します。許可ルールへの違反を監視し、ログに記録します。  ポートベースからアプリケーション ベースのルールに移行する際、ルールベース内で、入れ替えるポートベースのルールよりも上にアプリケーション ベースのルールを配置し両方のルールのポリシールール ヒット数をリセットします。トラフィックがポートベースのルールにヒットすると、そのポリシールールのヒット数が増加します。一定期間どのトラフィックもポートベースのルールにヒットしなくなるまでアプリケーション ベースのルールを調整してから、ポートベースのルールを削除します。
データセンター サーバーは更新サーバーなどの信頼できるサーバーとのみ通信するため、そのトラフィックを復号化する必要があります。	すでにデータセンター内に存在するマルウェアやコマンド アンド コントロール ソフトウェアは、外部サーバーと通信してさらにマルウェアをダウンロードしたり、データを盗んだりしようとする可能性があります。	データセンターからインターネットへのトラフィックをすべて復号化します。データセンター サーバーが接続できる URL を定義するカスタム URL カテゴリを作成し、それをセキュリティポリシーで使用して外部サーバーへのアクセスを制限します。同じカスタム URL を復号化ポリシーで使用し、それらの外部サーバーへのトラフィックを復号化します。
複数のベンダーからの脅威防止プロファイルに対するブロックおよびアラートを組み合わせます。	個々のツールをひとまとめにすると、攻撃者が利用できるセキュリティの穴が生じ、また上手く連携して動作しません。	Palo Alto Networks の一連のセキュリティツールは適切に連携し、セキュリティの穴をふさいで攻撃を防止します。

データセンターからインターネットへのアプリケーション許可ルールを作成

ソフトウェアをアップデートすることや、証明書ステータスを取得することが、インターネット上の外部サーバーへの接続を開始するデータセンター サーバーの主なユースケースです。特に Linux アップデートの場合、意図せずアクセスするおそれがあるサードパーティの URL が多く存在するため、間違ったサーバーに接続するとリスクが最も大きくなります。デフォルトのポートで必要なアプリケーションだけを使用し、データセンター サーバーに正当な更新サーバーから更新コンテンツを受信させるようにしてください。

そのためには、データセンター サーバーが接続する外部サーバー、およびデータセンター サーバーが外部サーバーに接続する際に使用するアプリケーションを限定する厳格なアプリケーション許可ルールを作成します。事前定義済みの*Sanctioned*（許可）タグを使ってすべての許可されたアプリケーションをタグ付けします。（Panorama およびファイアウォールは、Sanctioned タグがないアプリケーションを許可さ

れていないアプリケーションとして扱います。）厳格なアプリケーション許可ルールセットは、次のような方法で潜在的な攻撃を防ぎます：

- すでにデータセンター サーバー上に存在するマルウェアが、セキュリティが破られた外部サーバー（*phoning home*）に接続して、さらにデータをダウンロードするのを防ぎます。なぜなら、許可ルールはそれらのサーバーへの接続を許可しないからです。
- 攻撃者が FTP、HTTP、DNS トンネリングなどの正当なアプリケーションを使ってデータを盗んだり、コマンド アンド コントロール（C2）操作のために、ウェブブラウジングのような正当なアプリケーションを標準的でないポート上で使用したりするのを防ぎます。なぜなら、許可ルールは、データセンター サーバーがそれらのアプリケーションを使ってインターネットと通信するのを許可しないからです。データの盗難を防止するもう一つの方法は、ファイルブロッキングプロファイルの**Direction**（方向）制御を使用してアウトバウンドの更新ファイルをブロックし、ソフトウェア更新ファイルのダウンロードのみを許可することです。

異なる一連の外部サーバーからのソフトウェア更新を必要とする各アプリケーション用の厳格な許可ルールを作成します。多くの場合、App-ID だけではデータセンターのサーバーを十分に保護できません。例えば Linux サーバーの更新の場合、正当なサーバーへの接続を防止できないため、*yum*あるいは*apt-get*のような更新アプリケーションへのトラフィックを制限するのに十分ではありません。データセンター サーバーが接続する必要がある URL を見つけ、使用するウェブサイトを指定するカスタム URL カテゴリを作成（**Objects**（オブジェクト）> **Custom Objects**（カスタム オブジェクト）> **URL Category**（**URL** カテゴリ））し、それらをセキュリティポリシー ルール内の App-ID と組み合わせることがベストプラクティスになります。App-ID およびカスタム URL カテゴリを組み合わせ、不当なアプリケーションの使用およびカスタム URL カテゴリに含まれない更新サーバーへの接続を防ぐことで、データセンター サーバーが接続できる外部サーバーをロックダウンできます。例えば、データセンター サーバーが CentOS 更新サーバーに接続するのを許可するセキュリティポリシー ルール内で*CentOS-Update-Servers* という名前のカスタム URL カテゴリを作成し、サーバーが使用する CentOS 更新サイトをカスタム カテゴリに追加することもできます。

正当な *Linux* 更新サーバーおよびその他の更新サーバーの *URL* を見つけるために、ソフトウェア エンジニアリング、開発運用、ソフトウェアをアップデートするその他のグループと協力し、更新コンテンツを入手する場所を把握します。また、ウェブ ブラウジング セッションのログを取り、開発者が接続する *URL* を収集してから、その *URL* をエンジニアリング部門に持ち寄り、セキュリティポリシー用に適切な *URL* を取り除くこともできます。

すべての更新サーバーを許可することはないため、インターネットで通信を行うデータセンター サーバー用のセキュリティポリシールール内で *URL* フィルタリング プロファイル（*PAN-DB URL* フィルタリング）を使用しないでください。データセンター サーバーが更新コンテンツを取得する特定のサーバーにのみ到達できるよう、通信を制限します。

さらに、許可するすべての通信は各アプリケーションの標準的なポート上で行う必要があります。標準的でないポート上ではいかなるアプリケーションも実行してはなりません。すべてのデータセンター トラフィックの場合と同様に、許可ルールの違反を監視します。なぜなら、その違反は、セキュリティポリシーを更新して正当なトラフィックを許可する必要があるか、あるいは攻撃者がネットワーク内に侵入したか、侵入を試みているということのいずれかを示しているためです。

データセンター セキュリティポリシーのルールベースの順序を指定は、これらのルールと、他の 3 つのデータセンター トラフィック フロー用に作成するその他すべてのルールおよびブロック ルールの順序を決め、あるルールによって他のルールが遮られないようにする方法を説明します。

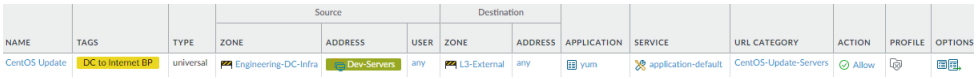
複数のデータセンター全体にかけて一貫した形でセキュリティポリシーを適用するために、テンプレートおよびテンプレート スタックを再利用し、同じポリシーをすべてのデータセンターに適用することができます。このテンプレートは、グローバル セキュリティポリシーを維持し、管理しなければならないテンプレートおよびテンプレート スタックの数を減らしつつ、*IP* アドレス、*FQDN* などのデバイス固有の値を適用するために変数を使用します。

次の各許可ルール:

- ベストプラクティスセキュリティプロファイルグループは、ベストプラクティスセキュリティプロファイルから構成されています。セキュリティプロファイルグループを使用することで、それぞれのプロファイルを個別に指定するのではなく、すべてのベストプラクティス プロファイルをルールにまとめて適用することができます。セキュリティプロファイルグループにより、マルウェア、脆弱性、C2トラフィック、未知および既知の脅威に対する保護の設定を素早く簡単に行えます。
- ルール違反とログ転送を追跡、解析できるようにトラフィックをログに記録（セッション終了時）します。ログサーバーにログを転送し、該当する場合は、ログのメールを適切な管理者に転送します。

STEP 1 | データセンター サーバーがソフトウェア更新サーバーにアクセスするのを許可します。

このルールは、データセンター サーバーが正当かつ既知のサーバーとのみ通信を行い、他の外部の更新サーバーとは通信を行わないようにするために、インターネット上のソフトウェア更新サーバーに対するアクセスを制限する方法を示します。この例では、エンジニアリング データセンター サーバーが CentOS 更新サーバーにアクセスできるようにし、必要なアプリケーションだけを使用して適切な一連の更新サーバーとのみ接続を確立するように通信を制限します。



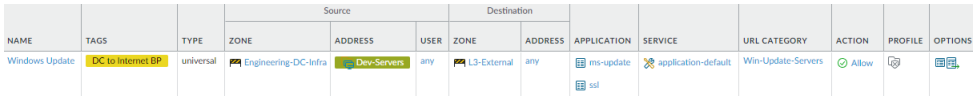
NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
CentOS Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		

このルールを作成するには：

- CentOS 更新リクエストのソースを、更新コンテンツを取得する必要があるデータセンター サーバーだけに制限します（この例では**Engineering-DC-Infra**ゾーン内の**Dev-Servers**ダイナミック アドレス グループ）。
- データセンター サーバーが外部の更新サーバーと通信するために使用できるアプリケーションを、必要なアプリケーション（この例では、CentOS の更新に使用する**yum**のみ）だけに限定します。アプリケーションの実行をデフォルトのポート上のみで許可し、マルウェアが標準的でないポートを使用しようとする試みを防いでください。
- カスタム URL カテゴリを作成し、データセンター サーバーが接続できる更新サーバーの URL を定義します。この例では、**CentOS-Update-Servers**カスタム URL カテゴリが、データセンター サーバーが到達できる更新サーバーの URL を定義します。

このように制限を組み合わせることで、すでにデータセンター サーバーに侵入している攻撃者が別の場所に到達し、他のアプリケーションを使ってデータを盗んだり、さらにマルウェアをダウンロードしたりするのを防ぐこともできます。

同様に、同じサーバーが Microsoft Windows 更新サーバーと通信するのを許可するルールは、同じ構造を使用します。

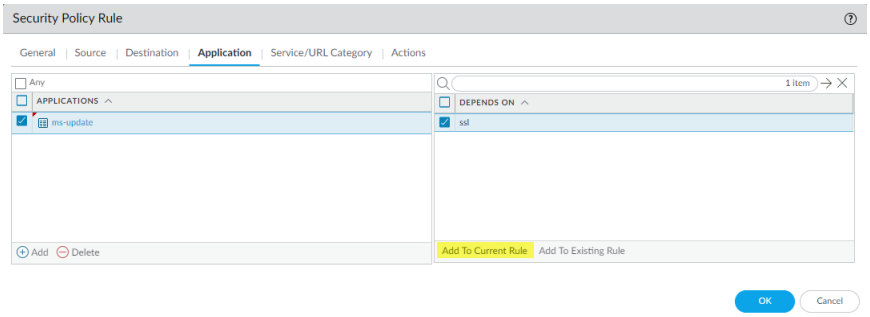


NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
Windows Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		

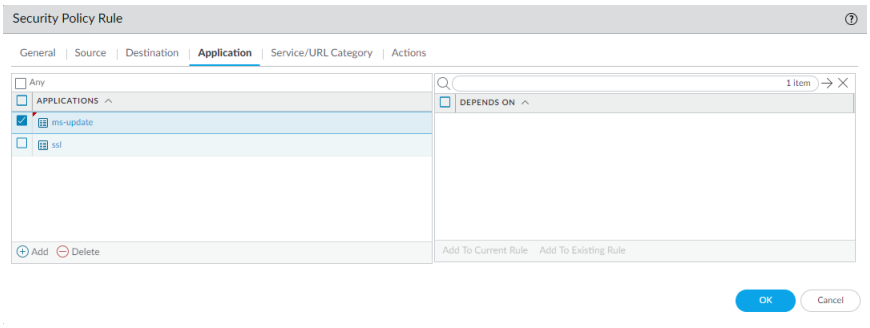
ソースゾーンとアドレスは、前出のCentOS 更新ルールと同じです。違いは次のとおりです：

- 他の URL へのアクセスを拒否するために、カスタム URL カテゴリ（**Win-Update-Servers**）には Windows アップデート用の URL が含まれています。
- アプリケーションは Microsoft アップデートに関連するものです。ms-update は SSL に依存するため、Microsoft アップデートでは**ms-update**アプリケーションに加え、**ssl**アプリケーションが必要になります。CentOS 更新ルールの場合と同様に、標準的なポートだけを使用できます。

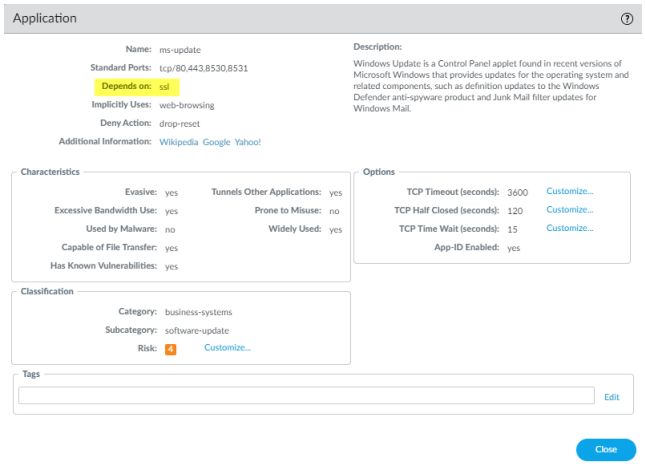
  他のアプリケーションに依存するアプリケーションもあります。任意のアプリケーションが依存するすべてのアプリケーションを許可しなければ、アプリケーションが動作しません。セキュリティポリシールールの作成時に、ユーザーインターフェイスにはアプリケーションの依存関係が表示されます。例えば、ルール内にms-updateアプリケーションを指定する場合、インターフェイスにはms-updateはSSLの許可にも依存することが表示されます:



選択したアプリケーションをルールに追加するには、**Add to Current Rule**（現在のルールに追加）をクリックします。



検索機能（*Objects*（オブジェクト）> *Applications*（アプリケーション））を使ってアプリケーションの依存関係を検索することもできます。たとえば、*ms-update*アプリケーションの依存関係を検索するには、*ms-update*を検索して、結果のアプリケーションリストから*ms-update*アプリケーションをクリックし、次に*Depends on:*（依存）フィールドを確認します。



STEP 2 | データセンター サーバーが DNS および NTP 更新サーバーにアクセスするのを許可します。

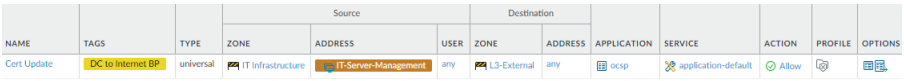
このルールは、データセンター サーバーが正当かつ既知のサーバーとのみ通信を行うようにするために、インターネット上の DNS および NTP 更新サーバーに対するアクセスを制限する方法を示します。この例では、IT データセンター サーバーが DNS および NTP 更新サーバーにアクセスできるようにし、必要なアプリケーションだけを使用して適切な一連の更新サーバーとのみ接続を確立するよう通信を制限します。

このルールを作成するには：

- DNS および NTP 更新リクエストのソースを、更新コンテンツを取得する必要があるデータセンター サーバーだけに制限します（この例では**Engineering-DC-Infra**ゾーン内の**DNS-NTP-Servers**ダイナミック アドレス グループ）。
- データセンター サーバーがこれらの外部の更新サーバーと通信するために使用できるアプリケーションを、必要なアプリケーション（この例では、**dns** および **ntp**のみ）だけに限定します。アプリケーションの実行をデフォルトのポート上のみで許可し、マルウェアが標準的でないポートを使用しようとする試みを防ぎます。
- カスタム URL カテゴリを作成し、データセンター サーバーが接続できる更新サーバーの URL を定義します。この例では、**NTP-DNS-Update-Servers**カスタム URL カテゴリが、データセンター サーバーが到達できる更新サーバーの URL を定義します。

STEP 3 | データセンター サーバーが認証局サーバーにアクセスし、デジタル証明書の失効状態を取得してその有効性を検証できるようにします。

このルールにより、データセンター サーバーがインターネット上のオンライン証明書ステータス プロトコル（OCSP）レスポンダ（サーバー）にアクセスし、認証用の証明書の失効状態をチェックできるようになります。OCSP レスポンダは、証明書無効リスト（CRL）アップデートと比べて新しい証明書ステータスを提供します。CRL は証明書の最新の失効状況を得るための CRL ブラウザ更新の頻度によるため、OCSP レスポンダよりも古いことが予想されます。OCSP レスポンダに到達できない場合に備え、ファイアウォール上で証明書プロファイルを設定する際、OCSP のフォールバック方法として CRL ステータス検証をセットアップできます。



このルールを作成するには：

- 証明書失効チェック リクエストのソースを、証明書の有効性をチェックする必要があるデータセンター サーバーだけに制限します（この例では**IT-Infrastructure**ゾーン内の**IT-Server-Management**ダイナミック アドレス グループ）。
- データセンター サーバーが外部の証明書無効化サーバーと通信するために使用できるアプリケーションを、必要なアプリケーションだけに限定します。この例ではデータセンター サーバーおよび OCSP レスポンダ間の接続を保護するため、指定するアプリケーションは**ocsp**だけです。アプリケーションの実行をデフォルトのポート上のみで許可し、マルウェアが標準的でないポートを使用しようとする試みを防いでください。

事前定義済みの アプリケーション レポート（**Monitor**（監視）> **Reports**（レポート）> **Application Reports**（アプリケーション レポート）> **Applications**（アプリケーション））をチェックし、セキュリティポリシールールで明示的に許可されたアプリケーションのみが実行されていることを確認します。レポートに予期せぬアプリケーションが含まれている場合は、アプリケーション許可ルールを確認してルールを調整し、予期せぬアプリケーションを許可しないようにしてください。

データセンターからインターネットへの復号化ポリシー ルールを作成

復号化ポリシー ルールを作成し、データセンター サーバーからインターネットに向かうトラフィックに対する可視性を確保します。データセンターからインターネットへのトラフィックをすべて復号化します。データセンター内部からインターネットへの接続を開始したアカウントだけがサービス アカウント

であり、このトラフィックのほとんどはソフトウェア更新に関連するものであるため、プライバシーの問題を考慮する必要はありません。更新サーバーが攻撃を受けた場合、データセンター サーバーがマルウェアをダウンロードしてソフトウェアの更新中にマルウェアが広がるおそれがあるため、このトラフィックを復号化して検査することが重要です。トラフィックを検査し、ベストプラクティスの脅威防止プロファイルを適用することで、データセンターをマルウェアから保護できます。そうしない場合、正当なアプリケーションを使って正当な更新サーバーからマルウェアをダウンロードしてしまうおそれがあります。

データセンターからインターネットへのアプリケーション許可ルールを作成で、データセンター サーバーがインターネット更新サーバーとの接続を開始してオペレーティングシステムのソフトウェア、DNS、NTP を更新したり、証明書をチェックしたりすることを許可するセキュリティポリシールールを作成しました。ここではそれと似た復号化ポリシー ルールを作成し、更新セキュリティポリシールールが許可するトラフィックを復号化します。

証明書無効化サーバー（オンライン レスポンダ）に向かうトラフィックは復号化しないでください。通常、オンライン証明書ステータス プロトコル（*OCSP*）トラフィックは *HTTP* を使用するため、トラフィックはクリアテキストであり、暗号化されていません。さらに、ファイアウォールが中間者のプロキシとして動作してクライアント証明書をプロキシ証明書と交換し、*OCSP* レスポンダがこれを有効なものとみなさない可能性があるため、*SSL* フォワード プロキシ復号化が更新プロセスを妨げるおそれがあります。

復号化ポリシー ルールは、これらのトラフィック フローに関連する一部の共通要素を共有します：

- 復号化ポリシー ルールを作成する目的は、セキュリティポリシー ルールがトラフィックを検査し、ポリシーに基づいてそれを許可あるいはブロックできるように、トラフィックを復号化することです。そのためには、復号化ポリシー ルールが類似のセキュリティポリシー ルールと同じ送信元ゾーンおよびユーザーを使用し、同じ宛先ゾーンおよびアドレス（サーバーを追加・削除する際にコミット操作なしでファイアウォールをアップデートできるよう、ダイナミック アドレス グループで定義されていることが多い）を使用する必要があります。セキュリティポリシーおよび復号化ポリシーで同じ送信元および宛先を定義することで、同じトラフィックに両方のポリシーを適用します。
- これらすべてのルールの Action（アクション）が復号化されます。
- 各ルールに対して、復号化のロギングと ログ転送を設定します。ファイアウォールリソースが許可する限り、できる限りの復号化トラフィックをログに記録します。
- これらすべての復号化ルールは、データセンターの最良の復号化プロファイルを作成で紹介するベストプラクティスのデータセンター復号化プロファイルを使用します。

URL復号化するトラフィックの範囲を絞るために、多くの場合、復号化ポリシー ルールの例にはカスタム URL カテゴリ（**Objects**（オブジェクト）> **Custom Objects**（カスタム オブジェクト）> **URL Category**（**URL** カテゴリ））が含まれています。各復号化ポリシー ルールは、復号化およびセキュリティポリシーを全く同じトラフィックに適用するために、類似のセキュリティポリシー ルールと同じカスタム URL カテゴリ（および送信元および宛先）を使用します。App-ID およびカスタム URL カテゴリを組み合わせることで、ルールで許可されているトラフィックだけをファイアウォールが復号化できるようになるため、ファイアウォールがブロックするトラフィックを復号化せずに処理プロセスを節約できます。（セキュリティポリシー ルールを評価する前に復号化を行います。）

STEP 1 | インターネット上のソフトウェア更新サーバーおよびデータセンター サーバー間のトラフィックを復号化します。

このルールは、データセンター サーバーのソフトウェア更新トラフィックを復号化し、インターネット更新サーバーに存在する可能性がある脅威に対する可視性を確保して、ファイアウォールがそれをブロックできるようにする方法を示します。この例では、「データセンターからインターネットへのアプリケーション許可ルールを作成」で作成した類似のアプリケーション許可ルールに基づき、インターネット上のCentOS更新サーバーとデータセンターサーバー間で許可されているトラフィックを復号化します。

NAME	TAGS	Source		Destination		URL CATEGORY	Decrypt Options					
		ZONE	ADDRESS	ZONE	ADDRESS		ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
CentOS Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	CentOS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

このルールを作成するには：

- 類似のセキュリティポリシールールと同じ送信元および宛先を指定します。このケースでは、送信元が**Engineering-DC-Infra**ゾーン内の**Dev-Servers**ダイナミック アドレス グループ、宛先がインターネット（**L3-External**ゾーン）になります。
- 類似のセキュリティポリシー ルールのものと同じカスタムURLカテゴリを指定（**CentOS-Update-Servers**）し、復号化する範囲をルールが許可するトラフィックだけに絞り、ファイアウォールがドロップするトラフィックを復号化することでサイクルを浪費しないようにします。
- Options（オプション）タブで Action（アクション）を**Decrypt**（復号化）に、復号化の Type（タイプ）を**SSL Forward Proxy**（**SSL** 転送プロキシ）に設定します。データセンターの最良の復号化プロファイルを適用し、SSL 転送プロキシおよび SSL プロトコル設定をトラフィックに適用します。

類似のセキュリティポリシーと同じ送信元および宛先、同じカスタム URL カテゴリに基づき、インターネット更新サーバーに接続する必要があるデータセンター サーバーの各グループの許可されたデータセンター トラフィックに使用する、同様の復号化ポリシー ルールを作成します。例えば、Microsoft Windows 更新サーバーと通信を行う必要がある、類似のセキュリティポリシー ルールに基づくデータセンター サーバー用の復号化ポリシー ルールは次のようになります：

NAME	TAGS	Source		Destination		URL CATEGORY	Decrypt Options					
		ZONE	ADDRESS	ZONE	ADDRESS		ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Win Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	Win-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

STEP 2 | インターネット上の NTP および DNS 更新サーバーとデータセンター サーバー間のトラフィックを復号化します。

このルールは、データセンター サーバーの NTP および DNS 更新トラフィックを復号化し、これらのインターネット サーバーに存在する可能性がある脅威に対する可視性を確保して、ファイアウォールがそれをブロックできるようにする方法を示します。この例では、「データセンターからインターネットへのアプリケーション許可ルールを作成」で作成した類似のアプリケーション許可リスト ルールに基づき、許可されているトラフィックを復号化します。

NAME	TAGS	Source		Destination		URL CATEGORY	Decrypt Options					
		ZONE	ADDRESS	ZONE	ADDRESS		ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
DNS-NTP Update Decrypt	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	L3-External	any	NTP-DNS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

このルールを作成するには：

- 類似のセキュリティポリシールールと同じ送信元および宛先を指定します。このケースでは、送信元が**IT Infrastructure**（**IT** インフラ）ゾーン内の**DNS-NTP-Servers**ダイナミック アドレス グループ、宛先がインターネット（**L3-External**ゾーン）になります。
- 類似のセキュリティポリシー ルールのものと同じカスタム URL カテゴリを指定（**NTP-DNS-Update-Servers**）し、復号化する範囲をルールが許可するトラフィックだけに絞ります。
- Options（オプション）タブで Action（アクション）を**Decrypt**（復号化）に、復号化の Type（タイプ）を**SSL Forward Proxy**（**SSL** 転送プロキシ）に設定します。データセンターの最良の復号化プロファイルを適用し、SSL 転送プロキシおよび SSL プロトコル設定をトラフィックに適用します。

最初のイントラ データセンター トラフィックのセキュリティポリシーを定義

イントラ データセンター トラフィックは、データセンター サーバーおよびアプリケーション層間を流れます。データセンターの境界内はすべて信頼できるため、それらのトラフィックを検査する必要はないという考え方もできるかもしれません。しかし、攻撃者がデータセンター サーバーに侵入し、アプリケーション層間のトラフィックがファイアウォールを経由しない場合、攻撃者がデータセンターを通じて横方向に重要なサーバーへと移動し、マルウェアをさらにダウンロードし、サーバーの用途を変え、データセンターでは不要な、正当なアプリケーションを使ってデータを盗むおそれがあります。これは、過去数年間に発生した大規模なセキュリティ侵害で実際に起きていることです。

データセンター内に侵入したマルウェアに対する最も優れた防御策は、厳格かつ特定のアプリケーション許可ルールを使ってトラフィックを保護し、アプリケーション層の間に配置した次世代ファイアウォールを使ってトラフィックを検査することです。

さらに、未知のアプリケーションはデータセンター内で許可しないでください。未知のアプリケーションは、攻撃者がデータセンターへのアクセスを掌握したことを示唆する場合があります。社内の専有アプリケーション用のカスタム アプリケーションを作成し、それらをApp-IDを使って識別してトラフィックにセキュリティを適用できるようにします。専有アプリケーション用にカスタム アプリケーションを作成しない場合、ファイアウォールはそれらを unknown-tcp あるいは unknown-udp トラフィックとみなします。この時、ファイアウォールは他の未知のアプリケーションの場合と同じ方法で専有アプリケーションを扱いますが、未知のアプリケーションは攻撃者のツールである可能性があるため、ブロックしなければならないという問題が生じます。データセンター内で未知のアプリケーションを許可するという行為は、重要なアセットの保管場所への鍵を攻撃者に与えるのと同じようなものです。

未知の商用アプリケーションの場合、*Palo Alto Networks* にリクエストを送信して *App-ID* を作成できます。

一連のポート用のカスタム セッション タイムアウトを定義するだけの目的で作成した既存のアプリケーション オーバーライド ポリシーがある場合、サービスベースのセッション タイムアウトを設定して各アプリケーションのカスタム タイムアウトを管理してからルールをアプリケーション ベースのルールに移行することで、既存のアプリケーション オーバーライド ポリシーをアプリケーション ベースのポリシーに変換します。アプリケーション オーバーライド ポリシーはポートベースです。アプリケーション オーバーライド ポリシーを使用して一連のポートのカスタム セッション タイムアウトを管理する際、それらのフローに対するアプリケーションの可視性が失われるため、どのアプリケーションがポートを使用するのか把握することも、管理することもできません。サービスベースのセッション タイムアウトはアプリケーションの可視性も維持しつつ、カスタム タイムアウトを利用できるようにします。

- イントラ データセンター トラフィックを保護するためのアプローチ
- データセンター内アプリケーション許可ルールを作成
- イントラ データセンターの復号化ポリシー ルールを作成

イントラ データセンター トラフィックを保護するためのアプローチ

従来型の古いアプローチでデータセンター サーバー間の East-West トラフィックを保護すると、貴重なアセットがリスクにさらされたままになってしまいますが、ベストプラクティスのアプローチであれば貴重なアセットを保護できます。

従来型のアプローチ	リスク	ベストプラクティスのアプローチ
データセンターの境界を通り抜けないトラフィックをセグメント化する必要はないため、アプリケーション層間のトラフィックがセキュリティ インフラを通過する必要はありません。	いずれかのデータセンター サーバーのセキュリティを破った攻撃者は、横方向に重要なデータセンター サーバーへと移動してそれを別の目的で使用できます。データセンター内の攻撃者は、発見される可能性を考えずに自由に移動することができます。	強固な許可ルールを使用してアプリケーション層間のトラフィックをセグメント化し、不要な通信を防止し、攻撃対象を減らし、攻撃者がデータセンター内を横方向に移動するのを防止します。許可リスト違反を監視し、ログに記録します。
信頼できるネットワーク内にあるデータセンターは安全であるため、データセンター サーバーに急いでパッチをあてる必要はありません。	脆弱性が長く放置されると、攻撃者に侵入経路を与えてしまいます。	適宜データセンター サーバーにパッチをインストールし、脆弱性を修復してください。許可リストのセキュリティポリシールールを作成することで、データセンター内で何が実行されており、パッチが適用されていないサービスがどこで実行されているのかを理解するのに役立ちます。
複数のベンダーからの脅威防止プロファイルに対するブロックおよびアラートを組み合わせます。	個々のツールをひとまとめにすると、攻撃者が利用できるセキュリティの穴が生じ、また上手く連携して動作しません。	Palo Alto Networks のセキュリティツール一式は互いに連携してセキュリティの穴を塞ぎ、攻撃を防ぎ、データセンター サーバー間で増殖しようとする未知のマルウェアを特定します。

さらに：

- 機能毎に独自のサービス アカウントを作成します。例えば、特定のサービス アカウントだけが Exchange のメールボックスの複製を、WEB サーバー上の特定のサービスアカウントだけが MySQL データベースにクエリを送信できるようにします。両方の機能に対して一つのサービス アカウントを使用しないでください。
- サービス アカウントの監視
- データセンター内で通常のユーザーアカウントを許可しないでください。

ポートベースからアプリケーション ベースのルールに移行する際、ルールベース内で、入れ替えるポートベースのルールよりも上にアプリケーション ベースのルールを配置し両方のルールのポリシールール ヒット数をリセットします。トラフィックがポートベースのルールにヒットすると、そのポリシールールのヒット数が増加します。一定期間どのトラフィックもポートベースのルールにヒットしなくなるまでアプリケーション ベースのルールを調整してから、ポートベースのルールを削除します。

データセンター内アプリケーション許可ルールを作成

データセンターのトラフィックはしばしば、SharePoint、WordPress、内部独自のアプリケーションなどの、サービスを提供するために複数の異なるサービスを使用するマルチティアアプリケーショントラフィックから成り立っています。代表的なマルチティアアプリケーションアーキテクチャは、Webサーバー（プレゼンテーション層）、アプリケーションサーバー（アプリケーション層）、およびデータベースサーバー（データ層）から成り立っています。データセンターのセグメント化戦略を作成で、アプリケーション層間にファイアウォールを配置する方法、データセンターをセグメント化する方法に関するガイドラインを紹介しています。

データセンター サーバー間のトラフィックを扱う方法は、トラフィックによって異なります。大抵のアプリケーション トラフィックの場合、脅威防止プロファイルをセキュリティポリシー許可ルールに追加し、トラフィックを検査します。例えば、常に最良のセキュリティ プロファイルを適用し、財務アプリケーションや技術開発アプリケーションなどのウェブ、アプリケーション、サーバー層間のトラフィックを保護します。メールボックスのレプリケーションやバックアップのフローのように、大容量かつ重要度の低いアプリケーションのトラフィックが、脅威防止プロファイルの適用に関する例外になります。これらのアプリケーションへのアクセスも許可しますが、レプリケーションを行う前にファイアウォールがすでにトラフィックを検査しているため、脅威防止プロファイルを適用することで不必要にファイアウォールのCPUサイクルを消費してしまいます。

WildFire セキュリティ プロファイルは、データセンター サーバー間で増殖しようとする未知のマルウェアを識別し、被害が出る前にマルウェアを発見することでデータ漏洩を防ぎます。WildFire グローバル クラウドを使用できない場合、WildFire プライベート クラウドあるいはWildFire ハイブリッド クラウドをデプロイできます。

このセクションのセキュリティポリシールールの例では、WEB サーバー、アプリケーションサーバー、データベースサーバー層を使ってアプリケーションを提供する必要があるマルチティアデータセンターの財務アプリケーションのトラフィックを許可する方法を示します。この例には、カスタム アプリケーション（**Billing-App**および**Payment-App**）の作成対象である 2 つの社内向けの財務アプリケーション用にアプリケーションサーバー間のトラフィックを許可するルールを構成します。これらのアプリケーション用にカスタム App-ID を作成することで、ファイアウォールがそれらを識別· 制御し、セキュリティポリシーを適用できるようになります。未知のアプリケーションを識別してセキュリティを適用することはできず、それらの存在がデータセンターに対する攻撃を示唆する場合があるため、未知のアプリケーションをデータセンター内で許可しないでください。各データセンター アプリケーションに必ず App-ID を付ける必要があります。

アプリケーションは標準的（*application-default*）なポート上でのみ許可してください。ビジネス要件によっては、例外を設けて特定のクライアントおよびサーバー間でアプリケーションが標準的でないポートを使用することを許可しなければならない場合もあります。その場合、標準的でないポートを通るアプリケーション トラフィック、および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のすべてのインスタンスを必ず把握しておくようにしてください。明示的に（既知の）例外を設けていないにも関わらず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がある場合、マルウェアがセキュリティをかいくぐろうとしている可能性があります。

事前定義済みの*Sanctioned*（許可）タグを使ってすべての許可されたアプリケーションをタグ付けします。*Panorama* およびファイアウォールは、*Sanctioned* タグが付いていないアプリケーションを許可されていないアプリケーションとみなします。

データセンター セキュリティポリシーのルールベースの順序を指定は、これらのルールと、他の 3 つのデータセンター トラフィック フロー用に作成するその他すべてのルールおよびブロック ルールの順序を決め、あるルールによって他のルールが遮られないようにする方法を説明します。

複数のデータセンター全体にかけて一貫した形でセキュリティポリシーを適用するために、テンプレートおよびテンプレート スタックを再利用し、同じポリシーをすべてのデータセンターに適用することができます。このテンプレートは、グローバル セキュリティポリシーを維持し、管理しなければならないテンプレートおよびテンプレート スタックの数を減らしつつ、*IP* アドレス、*FQDN* などのデバイス固有の値を適用するために変数を使用します。

下記の各々の許可ルール:

- ベストプラクティスセキュリティプロファイルから構成されるベストプラクティスセキュリティプロファイルグループが割り当てられている。セキュリティプロファイルグループを使用することで、それぞれのプロファイルを個別に指定するのではなく、すべてのベストプラクティスプロファイルを

ルールに一度にまとめて適用することができます。セキュリティプロファイルグループにより、マルウェア、脆弱性、C2トラフィック、未知および既知の脅威に対する保護の設定を素早く簡単に行えます。

- ルール違反を追跡、解析できるようにトラフィックをログに記録、ログを転送（セッション終了時）します。該当する場合はログサーバーにログを転送、ログのメールを適切な管理者に転送します。

STEP 1 | WEB サーバー層およびアプリケーションサーバー層間で財務アプリケーションのトラフィックを許可します。

このルールは、財務部門の請求用サーバーの WEB サーバー層およびアプリケーション サーバー層の間を通ることができるトラフィックを制限し、正当なアプリケーションを使うトラフィックだけが請求用サーバーにアクセスできるようにします。（また、ユーザーからデータセンターへのアプリケーション許可ルールを作成する際に、データセンターに対する財務部門のユーザーのアクセスを制限するルールを作成し、適切な財務部門のユーザーだけがデータセンターにアクセスできるようにします。）このルールはダイナミック アドレス グループを使用して各アプリケーション層内のサーバーを指定します（**Web-Servers**は WEB サーバー層内のサーバーのアドレスを指定し、**Billing-App-Servers**は財務部門の請求アプリケーション サーバー層内のサーバーのアドレスを指定します）。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Web to App Server	Intra DC BP	universal	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	Billing-App Payment-App ssl web-browsing	application-default	Allow		

このルールを作成するには：

- 財務アプリケーションのトラフィックの送信元を WEB サーバー（**Web-Server-Tier-DC**ゾーン内の**Web-Servers**）に制限します。
- 財務アプリケーションのトラフィックの宛先を請求用サーバー（**App-Server-Tier-DC**ゾーン内の**Billing-App-Servers**）に制限します。
- WEB サーバーが請求アプリケーション サーバーにアクセスするために使用できるアプリケーションを制限し、デフォルトのポート上のアプリケーションだけを許可します。この例では、2 つのカスタム アプリケーション、**Billing-App**および**Payment-App**がアプリケーションに含まれ、アプリケーションを作成する際にそれらのデフォルトのポートを指定します。請求および支払いサービスのために、財務部門はこれらの専有アプリケーションを使用します。

WEB サーバー層およびその他のアプリケーションサーバー層間のアプリケーションおよびトラフィックを制御する同様のルールを作成します。

STEP 2 | アプリケーションサーバー層およびデータベースサーバー層間で財務アプリケーションのトラフィックを許可します。

このルールは、財務部門の請求用サーバーのアプリケーションサーバー層およびデータベースサーバー層の間を通ることができるトラフィックを制限し、正当なアプリケーションを使うトラフィックだけが請求アプリケーションサーバーおよび請求データベースサーバー間を通ることができるようにします。このルールはダイナミック アドレス グループを使用して各アプリケーション層内のサーバーを指定します（**Billing-App-Servers**はアプリケーションサーバー層内のサーバーのアドレスを指定し、**DB2-Servers**は財務部門のデータベースサーバー層内のサーバーのアドレスを指定します）。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
App to DB Server	Intra DC BP	universal	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	Billing-App db2 mssql-db Payment-App ssl	application-default	Allow		

このルールを作成するには：

- 財務アプリケーションのトラフィックの送信元を請求アプリケーションサーバー（**App-Server-Tier-DC**ゾーン内の**Billing-App-Servers**）に制限します。
- 財務アプリケーションのトラフィックの宛先をデータベースサーバー（**DB-Server-Tier-DC**ゾーン内の**DB2-Servers**）に制限します。
- 請求アプリケーションサーバーがデータベースサーバーにアクセスするために使用できるアプリケーションを制限し、デフォルトのポートあるいは既知のデフォルトでないポート上のアプリケーションだけを許可します。

その他のアプリケーション用に、アプリケーションサーバー層およびデータベースサーバー層間のアプリケーションおよびトラフィックを制御する同様のルールを作成します。

事前定義済みの Applications（アプリケーション）レポート（**Monitor**（監視）> **Reports**（レポート）> **Application Reports**（アプリケーション レポート）> **Applications**（アプリケーション））をチェックし、セキュリティポリシールールで明示的に許可したアプリケーションのみが実行されていることを確認します。レポートに予期せぬアプリケーションが含まれている場合はアプリケーション許可ルールを確認してルールを調整し、予期せぬアプリケーションを許可しないようにしてください。

イントラ データセンターの復号化ポリシー ルールを作成

ユーザーが存在しないため、データセンターはセキュリティレベルの高いネットワークの内部にある安全な環境です。しかし、なぜデータセンター内のトラフィックを復号化するのでしょうか。多くの人がデータセンターは安全だと考え、それを顧みないため、データセンターは攻撃者にとって格好の潜伏場所になります。しかし、ネットワークの他の場所と同じ原則、つまり、目に見えないものは防止できないという原則が、データセンターにも当てはまります。ファイアウォールがトラフィックを検査し、アクセスを制御し、脅威を明らかにし、重要なアセットを保護できるよう、データセンターのトラフィックを復号化してください。

暗号化されていない（クリアテキストの）データセンター トラフィックも存在します。復号化する対象が存在しないため、クリアテキストのフローには復号化を適用しないでください。

「データセンター内アプリケーション許可ルールを作成」では、お互いに通信を行う財務部門の各アプリケーションとやり取りする異なるアプリケーション内にあるサーバーを許可するセキュリティポリシールールを作成しました。ここでは、類似の復号化ポリシー ルールを作成し、それらのルールが許可するトラフィックを復号化します。

各ルールに対して、復号化のロギングとログ転送を設定します。ファイアウォールリソースが許可する限り、できる限りの復号化トラフィックをログに記録します。

STEP 1 | WEB サーバー層およびアプリケーションサーバー層間で財務アプリケーションのトラフィックを復号化します。

このルールは、財務部門の請求用サーバーの WEB サーバー層およびアプリケーションサーバー層の間を流れるトラフィックを復号化し、ファイアウォールがトラフィックを把握して各層内のサーバーを潜在的な脅威から保護できるようにします。

		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Web to App	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

このルールを作成するには：

- 類似のセキュリティポリシールールと同じ送信元および宛先を指定します。この例では、送信元が**Web-Server-Tier-DC**ゾーン内の**Web-Servers**ダイナミック アドレス グループ、宛先が**App-Server-Tier-DC**ゾーン内の**Billing-App-Servers**になります。
- Options（オプション）タブで Action（アクション）を**Decrypt**（復号化）に、復号化の Type（タイプ）を**SSL Forward Proxy**（**SSL** 転送プロキシ）に設定します。データセンターの最良の復号化プロファイルを適用し、SSL 転送プロキシおよび SSL プロトコル設定をトラフィックに適用します。

STEP 2 | アプリケーションサーバー層およびデータベースサーバー層間で財務アプリケーションのトラフィックを復号化します。

このルールは、財務部門の請求用サーバーのアプリケーションサーバー層およびデータベースサーバー層の間を流れるトラフィックを復号化し、ファイアウォールがトラフィックを把握して各層内のサーバーを潜在的な脅威から保護できるようにします。

		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
App to DB	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

このルールを作成するには：

- 類似のセキュリティポリシールールと同じ送信元および宛先を指定します。。この例では、送信元が**App-Server-Tier-DC**ゾーン内の**Billing-App-Servers**ダイナミック アドレス グループ、宛先が**DB-Server-Tier-DC**ゾーン内の**DB2-Servers**になります。
- Options（オプション）タブで Action（アクション）を**Decrypt**（復号化）に、復号化の Type（タイプ）を**SSL Forward Proxy**（**SSL** 転送プロキシ）に設定します。データセンターの最良の復号化プロファイルを適用し、SSL 転送プロキシおよび SSL プロトコル設定をトラフィックに適用します。

データセンター セキュリティポリシーのルールベースの順序を指定

このトピックは、4つのデータセントラフィックフローすべてのルールの順序を示すセキュリティポリシールールベースの例のスナップショットを提供しています。前述の各セクションでは、各セキュリティポリシー ルール（および復号化ポリシー ルール、必要な場面では認証ポリシーおよびDoS 保護ポリシールール）を詳細に説明しています。

セキュリティポリシールールの順序はとても重要です。ルールが別のルールを妨げてはなりません。例えば、ブロック ルールが許可したいトラフィックをブロックしてはならないため、トラフィックをブロックするルールが機能する前の場所に、許可ルールを配置する必要があります。さらに、許可ルールがブロックしたいトラフィックを許可しないようにする必要があります。非常に限定した許可ルールを作成することで、許可するアプリケーションおよび誰がそれを使用できるか、誰が使用できないのかを厳密にコントロールすることができます。

ルール**1**～**7**:最初の2つのルールは、トラフィックのブロックや復号化の防止を回避するために、QUICアプリケーションをブロックします。次の5つのルールは、特定のユーザーグループに対して特定のアプリケーションとサーバーへのアクセスを許可します。これらのルールは、「ユーザーからデータセンターへのアプリケーション許可ルールを作成」で設定されたものです。

	NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block QUIC UDP	none	any	any	any	L3-External	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	none	any	any	any	L3-External	any	quic	application-default	Deny	none	
3	DNS Services	User to DC BP	any	any	any	IT Infrastructure	DNS-Servers	dns	application-default	Allow		
4	IT DC Server Management	User to DC BP	IT-Users	any	it-superusers	IT-Server-Access-DC	IT-Server-Management	ms-rdp ssh ssl	Custom-IT-Ports	Allow		
5	Engineering Resources	User to DC BP	Engineering-Users	any	api-users engg-users	Engineering-DC-Infra	Dev-Servers	oracle-bi perforce profinet qlikview	application-default	Allow		
6	Finance to DC	User to DC BP	Finance-Users	any	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	netsuite oracle oracle-crm-ondemand oracle-forms	application-default	Allow		
7	SAP-Contractors	User to DC BP	Contractors	any	sap-contractors	SAP-Infra	SAP DB Servers	ms-sql-analysis-service mssql-db mssql-mon sap	application-default	Allow		

図 **1**：データ センタールール**1**～**7**

指定されたユーザーだけが指定されたアプリケーションだけをそのデフォルトのポート上で使用し、指定されたデータセンターの宛先サーバー（アドレス）だけにアクセスできます。セキュリティ プロファイルはこれらすべての許可ルールを脅威から保護します。これらのルールは非常に具体的であり、許可されたユーザーやアプリケーションがルールベースの下の方にあるより一般的なルールにマッチしないようにするために、ネットワーク上の未知のユーザーやアプリケーションを発見するブロック ルールよりも前に配置します。

ルール**8**～**9**:先行のルールが認可されたアプリケーションを許可する一方、「データセントラフィックブロックルールの作成」で作成された次の2つのルールは、標準ポートのユーザーからの予期しないアプリケーションの検出とブロック、および非標準ポートのすべてのアプリケーションをブロックします。（ご利用のデプロイ環境に、この例よりも多くのユーザーゾーンが存在している場合もあります。）

	NAME	TAGS	Source			Destination		APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	ZONE	ADDRESS					
8	Unexpected-App-from-User-Zone	User to DC BP	Contractors Engineering-Users Finance-Users IT-Users	any	any	Web-Server-Tier-DC	any	any	application-default	Drop	none	
9	Unexpected-User-App-Any-Port	User to DC BP	Contractors Engineering-Users Finance-Users IT-Users	any	any	Web-Server-Tier-DC	any	any	any	Drop	none	

図 **2 :** データセンタールール**8 ~ 9**

非ユーザーゾーンからのトラフィックは、これらのルールに一致しません。これらのルールをアプリケーションブロッキングルール（ルール18および19）よりも上に配置しなければ、それらのルールによって妨げられてしまいます。（これら 2 つのルールにマッチするトラフィックは、より一般的なアプリケーション ブロッキング ルールにもマッチする可能性があります。アプリケーション ブロッキング ルールが最初に来てこれらのルールにもマッチするトラフィックにマッチする場合、トラフィックはこれらのルールに一致せず、個別にログに記録されないため、従業員のユーザーアクティビティの結果によるブロックと、非ユーザーゾーンからのアクティビティの結果によるブロックを区別するという、ルールが意図する役割を果たせません。）

ルール**10 ~ 16**:次の7つのルールは、データセンターとインターネットおよびデータセンター内（「インターネットからデータセンターへのアプリケーション許可ルールを作成」「データセンターからインターネットへのアプリケーション許可ルールを作成」および「データセンター内アプリケーション許可ルールを作成」で作成）の間のトラフィックを許可します。 セキュリティ プロファイルはこれらすべての許可ルールを脅威から保護します。

	NAME	TAGS	Source		USER	Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS		ZONE	ADDRESS						
10	Web Server Inbound	Internet to DC BP	L3-External	~~Bad IPs List~~	any	Web-Server-Tier-DC	Web Servers	Acme	application-default	any	Allow		
11	NTP DNS Update	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	any	L3-External	any	dns ntp	application-default	NTP-DNS-Update-Servers	Allow		
12	CentOS Update	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		
13	Windows Update	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		
14	Cert Update	DC to Internet BP	IT Infrastructure	IT-Server-Management	any	L3-External	any	ocsp	application-default	any	Allow		
15	App to DB Server	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	Billing-App db2 mssql-db Payment-App ssl	application-default	any	Allow		
16	Web to App Server	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	Billing-App Payment-App ssl web-browsing	application-default	any	Allow		

図 **3 :** データセンタールール**10 ~ 16**

ルール**17 ~ 20**:「データセンターのトラフィック ブロック ルールを作成」で構成した最後の4つのルールは、データセンターに不要なアプリケーションおよび予期せぬアプリケーションをブロックし、ネットワーク上の未知のユーザーを発見します。

	NAME	Source			Destination		APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
		ZO...	ADDRESS	USER	ZONE	ADDRESS					
17	Block-Bad-Apps	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	
18	Unexpected-App-from-Any-Zone	any	any	any	Web-Server-Tier-DC	any	any	application-default	Drop	none	
19	Unexpected-App-Any-Port	any	any	any	Web-Server-Tier-DC	any	any	any	Drop	none	
20	Discover-Unknown-Users	any	any	unknown	any	any	any	any	Deny	none	

ルール17はデータセンターで使用しないアプリケーションをブロックします。例外へのアクセスを有効にするために、このルールはアプリケーション許可ルールの後に配置されます。例えば、このブロックルー

ルの前にあるアプリケーション許可ルールで1つか2つのファイル共有アプリケーションを許可してから、このルールのアプリケーションフィルターが残りのアプリケーションタイプをブロックし、許可されていないファイル共有アプリケーションの使用を防止します。BitTorrent など、ネットワーク上で絶対に使用したくない一連のアプリケーションや個々のアプリケーションがある場合、それらのアプリケーションだけをブロックする具体的なブロックルールを作成し、ルールベースの最上位、アプリケーション許可ルールよりも上に配置することができます。しかしその場合はユーザーがアクセスできなくなるため、ブロックしたすべてのアプリケーションが正当なビジネス用途に使用されていないことを確認する必要があります。

ルール18および19は、ユーザーからの予期せぬアプリケーションを発見するルール8および9と同様のものです(これらのルールが適用されるトラフィックは、ユーザーゾーンからのみ発生します)。ルール18および19は、すべての他のゾーンからの予期せぬアプリケーションを発見します。ルールを分けることで、ブロッキング ルールのマッチを細かくログに記録できるようになります。

ルール20は未知のユーザーを発見し、アクセスの試みを個別にログに記録することで調査を容易にします。

すべてのセキュリティポリシーのルールベースと同様に、最後の 2 つのルールはイントラゾーン トラフィック（許可）およびインターゾーン トラフィック（拒否）用のPalo Alto Networksのデフォルトルールになります。

データセンター トラフィックのログおよび監視

ファイアウォールのロギングおよび監視ツールを使用すれば、存在することさえ知らなかったアプリケーションやユーザーを含め、ネットワーク上のアプリケーション、ユーザー、トラフィック パターンを把握できます。ロギングおよび監視を行うことで、セキュリティポリシー ルールが正しく厳格に作成されていないことを示唆する、未知のユーザー（User-ID で特定できない）、不明なアプリケーション、予期せぬポート上のトラフィックも明らかにできるため、データセンターの最良のセキュリティポリシーに移行する際やその管理を行う際のあらゆる段階で役立つ情報を得られます。ロギングおよび監視を行うことで、どのアプリケーションを許可し、どのユーザーにどのアプリケーションやデバイスへのアクセスを許可するか判断しやすくなり、セキュリティの潜在的な問題の調査がはかどります。

データセンターを評価する際はベースラインの測定値を取ってください。これらのベースラインの測定値を現在の測定値と定期的に比較し、データセンターの最良のセキュリティポリシーを実装する際に進行状況を評価し、変化を把握し、改善が必要な領域を特定します。

Panorama を使用してファイアウォールを管理する場合、ファイアウォールの安全状態を監視することで、デバイス同士やそのベースラインのパフォーマンスを比較して通常の動作からの逸脱を把握することができます。

ファイアウォールから SNMP トラップ サーバーや Syslog サーバーなどの外部サービスあるいは Panorama へのログ転送を設定し、複数のファイアウォールから得たログを一元化し、表示や分析（ファイアウォールが表示できるのはローカルのログおよびレポートだけであり、他のファイアウォールからのログおよびレポートは表示できません）を行いやすくします。ログ転送を設定する際に通知の送信を設定し、設定したログの宛先がファイアウォール ログを受信していることを確認してください。

次の項目がデータセンターのロギングおよび監視のベストプラクティスに含まれます：

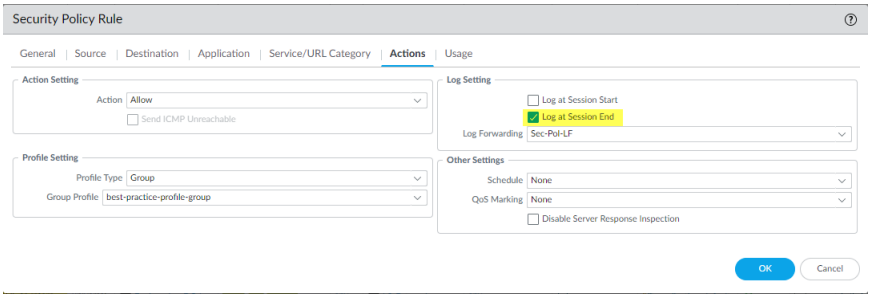
- ログ記録および監視の対象にするデータセンター トラフィック
- データセンター ブロック ルールを監視してルールベースを調整
- イントラゾーン ルールにマッチしないデータセンター トラフィックのロギング
- イントラゾーン許可ルールにマッチするイントラ データセンター トラフィックのロギング

ログ記録および監視の対象にするデータセンター トラフィック

Palo Alto Networks の次世代ファイアウォールはデフォルトでいくつかのログを作成しますが、他のトラフィックについてはログを設定する必要があります。すべてのデータセンター トラフィックをログに記録し、予期せぬアプリケーション、ユーザー、トラフィック、動作を発見するためにログを監視することがベストプラクティスになります。

デフォルト設定では、ファイアウォールは明示的に設定したセキュリティポリシールールにマッチするトラフィックをログに記録し、事前定義済みのイントラゾーン デフォルト（同じゾーン内の送信元および宛先を持つトラフィックを許可）、およびルールベースの一番下にあるインターゾーン デフォルト（先行するルールのいずれにもマッチしないトラフィックを拒否する、ルールベースの最後のルール）ルールにマッチするトラフィックはログに記録しません。

セキュリティポリシー ルールを作成する際、デフォルトでファイアウォールはセッションの最後にトラフィックをログに記録します。



ただし、デフォルトでファイアウォールはログを転送せず、またセキュリティプロファイルを適用しません。前の例では、適切なログサーバーと管理者にログを転送するためのベストプラクティスを表しており、ベストプラクティスセキュリティプロファイルを適用しています。

セッションの有効期間の途中でアプリケーションが変化する場合も良くあるため、**Log at Session End**（セッション終了時にログを記録）することが大抵の場合にベストプラクティスになります。例えば、あるセッションの最初の App-ID が web-browsing であっても、ファイアウォールがいくつかのパケットを処理した後にそのアプリケーションのより具体的な App-ID を知り、App-ID を変更する場合があります。DNS シンクホール、長期間継続するトンネル セッションの場合や、トラブルシューティングを行うためにセッション開始時に情報が必要な場合など、セッション開始時にトラフィックをログに記録するユースケースもいくつかあります。

トラフィックのログを取ることで、ルールが許可するトラフィックおよびルールが拒否あるいはドロップ（ルール違反）するトラフィックについての情報を記録し、ファイアウォールがトラフィックを扱う方法に関わらず、貴重な情報を提供できるようになります。ルールの違反は脅威の可能性、あるいは許可ルールを調整して正当なビジネスアプリケーションを許可しなければならないことを示唆します。

ブロックされたトラフィックをログで検証する際、許可されていないアプリケーションのブロックなど、システムに侵入される前に予防措置としてファイアウォールがブロックしたトラフィックと、すでにデータセンター サーバー上に存在したマルウェアによる、外部サーバーと通信してさらにマルウェアをダウンロードさせたりデータを盗んだりする試みなどのように、侵入後のイベントとしてファイアウォールがブロックしたトラフィックとを区別します。

ファイアウォールが提供する一連の役立つ監視ツール、ログ、ログ レポートを使用してネットワークを分析できます：

- **Monitor**（監視）> **Logs**（ログ）は、トラフィック、脅威、User-ID、および**Unified**（統一）ログを含む他の多くのログ タイプを表示します。これは、複数のログ タイプを単一の画面で表示するため、異なるタイプのログを個別に確認する必要がなくなります。拡大鏡のアイコンがサマリーに含まれる場合、それをクリックすればログ エントリの詳細を確認できます。
- **Monitor**（監視）> **PDF Reports**（PDF レポート）は、閲覧可能な事前定義済みのレポートと、事前定義済みのレポートおよびカスタム レポートから成るレポート グループを作成する機能を提供します。例えば、トラフィックのアクティビティを確認したり、ベースラインの測定値を取ったりして、ゾーンやインターフェイス毎に各データセンター内のトラフィック フローおよび帯域幅の使用率を把握できます。
- **Monitor**（監視）> **Manage Custom Reports**（カスタム レポートの監視）では、カスタマイズされたレポートを作成し、ブロック ルール、許可ルール、その他の関連する項目に関する情報を閲覧できます。
- **Monitor**（監視）> **Packet Capture**（パケット キャプチャ）では、ファイアウォールの管理インターフェイスおよびネットワークインターフェイスを通過するトラフィックのパケット キャプチャを取ることができます。
- アプリケーション コマンド センター（**ACC**）は、ネットワークを通過するアプリケーション、ユーザー、URL、脅威、およびコンテンツに関する詳細かつインタラクティブなサマリーを表示するウィジェットを提供します。例えば、ネットワーク上のアプリケーションを確認・評価（**ACC** > **Network Activity**（ネットワーク アクティビティ）> **Application Usage**（アプリケーション使用状況）>

Threats（脅威）)し、アプリケーションに何らかの変更があるか、あるいはアプリケーションが脅威を示唆する挙動を示すかどうかを確認できます。リストに予期せぬアプリケーションがある場合、それらのアプリケーションをどのように扱うべきか評価してください。

感染したユーザーアカウントやホスト システムを把握する際にも ACC 情報が役立ちます。**ACC** > **Network Activity**（ネットワーク アクティビティ）> **User Activity**（ユーザー アクティビティ）> **Threats**（脅威）ウィジェットを使用して脅威に関連するユーザー名とともに脅威を分析してから、脅威ログを使って正確に問題を隔離します。

- ダッシュボード（**Dashboard**）は、一般的なファイアウォールの情報と、脅威、設定、システム ログの最新のエントリを最大 10 件表示するウィジェットを提供します。
- パフォーマンス指標を比較するためや、コミット、ソフトウェア更新、コンテンツ更新、ルールの変更、新規アプリケーションの追加などのようなイベント後のファイアウォールのパフォーマンスを追跡するために、Panorama を使用してファイアウォールの安全状態を監視し、新規デバイスのベースラインを測ります。パフォーマンスがデバイスのベースラインから逸脱している場合は、閲覧して手動でトラブルシューティングを行ったり、調査用のチケットを自動で開いたりできます。
- Panorama あるいは個々のファイアウォール上でポリシールール ヒット カウンターを使用してルールベースに対する変更を分析します。例えば、新しいアプリケーションを追加する際、そのアプリケーションのトラフィックをネットワーク上で許可する前に、許可ルールをルールベースに追加します。トラフィックがルールにヒットしてカウント数が増えた場合、アプリケーションをアクティベートしていないにも関わらずルールにマッチしたトラフィックがすでにネットワーク上に存在するか、ルールを調整する必要があることを示唆します。別の例としては、アプリケーション ベースのルールをポートベースのルールの前に配置し、ポートベースのルールにヒットするトラフィックがあるかどうか確認することで、ポートベースのルールをアプリケーション ベースのルールと交換することが挙げられます。トラフィックがポートベースのルールにヒットした場合、そのトラフィックを捕捉するようにアプリケーション ベースのルールを調整する必要があります。

  ポリシールール ヒット カウンターとあわせて、**ACC** > **Threat Activity**（脅威アクティビティ）> **Applications Using Non Standard Ports**（標準的でないポートを使用しているアプリケーション）および**ACC** > **Threat Activity**（脅威アクティビティ）> **Rules Allowing Apps On Non Standard Ports**（標準的でないポート上のアプリを許可するルール）ウィジェットもチェックし、標準的でないポート上のトラフィックが予期せぬルールのヒットを生じさせていないか確認します。

ポリシールール ヒット カウンターを使用する際の鍵は、新しいアプリケーションを導入したりルールの意味合いを変えたりするなど、変更を行った際にカウンターをリセットすることです。ヒット カウンターをリセットすることで、変更の結果および変更前に生じたイベントの結果の両方ではなく、変更による結果だけを確認できるようになります。

データセンター ブロック ルールを監視してルールベースを調整

最良のセキュリティポリシーをデプロイするのは反復的な作業です。データセンターのトラフィック ブロック ルールを作成したらすぐ、ポリシーの漏れを特定するためのブロック ルールにマッチするトラフィック、予期せぬ挙動、攻撃の可能性を監視し始めます。ブロック ルールにマッチするが許可する必要があるトラフィックに合わせてアプリケーション許可ルールを調整して、攻撃を示す可能性があるトラフィックを調査します。

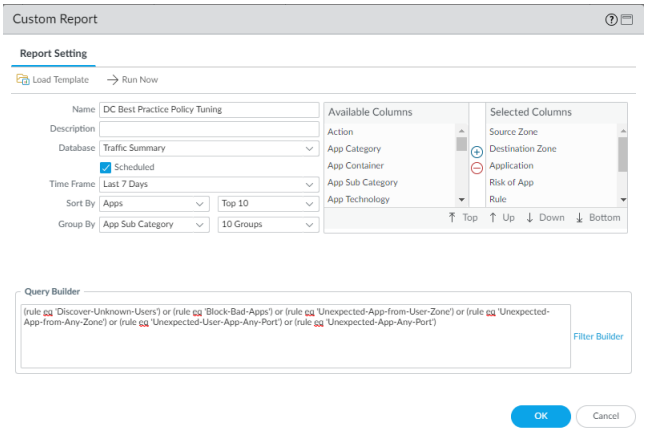
ブロックされたトラフィックについてのレポートには、潜在的な問題を調査するうえで役立つ情報が含まれています。ルールベース内のブロック ルールを維持すれば、貴重なデータセンターのアセットを保護しつつ、ブロック ルールにマッチしたトラフィックに関する情報を得られます。

コンテンツ更新のベストプラクティスに従ってファイアウォールの保護を最新の状態に保ってください。データセンターの最良のルールベースを管理には、データセンターのファイアウォールに関する具体的なベストプラクティスが記されています。

STEP 1 | ポリシーの漏れや潜在的な攻撃を特定するためのブロック ルールにマッチするトラフィックを監視するために、カスタム レポートを作成します。

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. レポートを**Add**（追加）し、レポートの目的が分かるような**Name**（名前）（この例では**DC Best Practice Policy Tuning**（DC ベストプラクティスのポリシーの調整））を付けます。
3. **Database**（データベース）を**Traffic Summary**（トラフィックサマリー）に設定します。これにより、**Available Columns**（利用可能な列）オプションも変化します。
4. **Available Columns**（利用可能な列）から、**Source Zone**（ソースゾーン）、**Destination Zone**（宛先ゾーン）、**Sessions**（セッション）、**Bytes**（バイト）、**Application**（アプリケーション）、**Risk of App**（アプリケーションのリスク）、**Rule**（ルール）、および**Threats**（脅威）を**Selected Columns**（選択した列）リストに追加します。監視したい他の種類の情報がある場合は、それも選択してください。
5. **Scheduled**（スケジュール設定）のボックスを選択します。
6. 任意の**Time Frame**（期間）、**Sort By**（並び替え基準）、**Group By**（グループ化基準）の値を設定します。この例では、**Time Frame**（期間）に**Last 7 Days**（過去7日間）、**Sort By**（ソート条件）を**Apps**（アプリケーション）、および**Group By**（グループ化条件）を**App Sub Category**（アプリケーションサブカテゴリ）に設定します。
7. ポリシーの漏れおよび潜在的な攻撃を特定するためのルールにヒットするトラフィックにマッチさせるクエリを定義します。**or**（または）演算子を使用してルールのいずれかにマッチするトラフィック用の単一のレポートを作成したり、個々のレポートを作成して各ルールを監視したりすることができます。**Query Builder**（クエリ ビルダー）では、レポートに含めたい各ルールの名前を指定します。この例では、6つのブロッキングルールを使用し、また**Or**（または）演算子を使用してそのルールのいずれかにマッチするトラフィックについての情報を含めます：

   - `(rule eq 'Discover-Unknown-Users')`
   - `(rule eq 'Block-Bad-Apps')`
   - `(rule eq 'Unexpected-App-from-User-Zone')`
   - `(rule eq 'Unexpected-App-from-Any-Zone')`
   - `(rule eq 'Unexpected-User-App-Any-Port')`
   - `(rule eq 'Unexpected-App-Any-Port')`



STEP 2 | 定期的にレポートを確認し、ブロック ルールそれぞれにトラフィックがマッチした理由を把握し、ポリシーを更新して正当なアプリケーションおよびユーザーを含めるか、その情報を利用してルールにマッチするトラフィックのリスクを評価します。

イントラゾーン許可ルールにマッチするイントラ データセンター トラフィックのロギング

デフォルト設定では、すべてのイントラゾーン トラフィック（送信元および宛先が同じゾーン内）が許可されます。ファイアウォールはセキュリティポリシーを評価した後、アプリケーションの許可リスト ルールによって制御されているトラフィックを許可するか、ブロックルールによって制御されているトラフィックを拒否するか、あるいはイントラゾーントラフィックがルールにマッチしない場合、デフォルトでトラフィックを許可します。（ファイアウォールはインターゾーン トラフィックをデフォルトでブロックします。）データセンターのアセットは貴重であるため、イントラゾーン デフォルト許可ルールによって許可されているトラフィックも含めて、データセンター内のデータセンター サーバー間ですべてのトラフィックを監視することがベストプラクティスになります。

このトラフィックに対する可視性を確保するために、イントラゾーン デフォルト ルールがデータセンターのゾーン内でトラフィックに適用される際の口ギングを有効化します。このトラフィックをログに記録することで、明示的に許可していないアクセスを検査したり、許可ルールを修正してトラフィックを許可したり、明示的にブロックしたりできるようになります。

最初のイントラ データセンター トラフィックのセキュリティポリシーを定義では、データセンター内で Web-Server-Tier-DC、App-Server-Tier-DC、DB-Server-Tier-DC という 3 つのゾーンの例を使用しました。この例ではカスタム レポートを作成し、これら 3 つの内部データセンター ゾーン内のデータセンター イントラゾーン トラフィックに関するログ情報を収集します。

STEP 1 | ルールベースのイントラゾーン デフォルトの行を選択し、**Override**（オーバーライド）をクリックしてルールを編集できるようにします。

STEP 2 | **intrazone-default**（イントラゾーン デフォルト）ルールの名前を選択し、ルールを編集します。

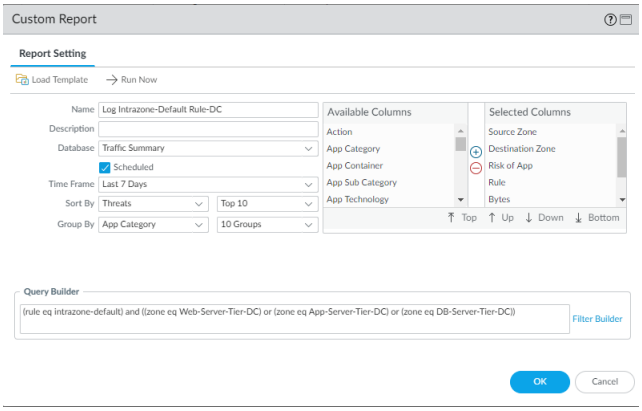
STEP 3 | Actions（アクション）タブで**Log at Session End**（セッション終了時にログを記録）を選択し、**OK**をクリックします。

STEP 4 | カスタム レポートを作成し、内部データセンター ゾーン用のこのルールにヒットしたトラフィックを監視します。

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. レポートを **Add**（追加）して分かりやすい **Name**（名前）を付けます。この例では、名前は**Log Intrazone-Default Rule-DC**になります。
3. **Database**（データベース）を**Traffic Summary**（トラフィックサマリー）に設定します。
4. **Available Columns**（利用可能な列）から、**Source Zone**（ソースゾーン）、**Destination Zone**（宛先ゾーン）、**Sessions**（セッション）、**Bytes**（バイト）、**Application**（アプリケーション）、**Risk of App**（アプリケーションのリスク）、**Rule**（ルール）、および**Threats**（脅威）を**Selected Columns**（選択した列）リストに追加します。監視したい他の種類の情報がある場合は、それも選択してください。
5. **Scheduled**（スケジュール設定）のボックスを選択します。
6. 任意の**Time Frame**（期間）、**Sort By**（並び替え基準）、**Group By**（グループ化基準）の値を設定します。この例では、値がそれぞれ**Threats**（脅威）、**App Category**（アプリ カテゴリー）になります。
7. データセンター ゾーン用のイントラゾーン デフォルト ルールにマッチするトラフィックにマッチさせるクエリを定義します：

```
(rule eq intrazone-default) and ((zone eq Web-Server-Tier-DC) or (zone eq
 App-Server-Tier-DC) or (zone eq DB-Server-Tier-DC))
```

そのクエリは、イントラゾーンのデフォルトルールにマッチするトラフィックと、定義した3つの内部データセンターゾーンのいずかにマッチするトラフィックをフィルタリングします。デフォルトのSelected Columns（選択中の列）にはゾーンが含まれるため、各セッションのゾーンがレポートに表示されます。実際のデータセンターではさらに多くのゾーンがあり、各ゾーンをクエリに追加することになるでしょう。最終的なカスタム レポートは次のようになります：



8. 変更を **Commit**（コミット）します。

イントラゾーン ルールにマッチしないデータセンター トラフィックのロギング

設定したどのセキュリティポリシールールにもマッチしないトラフィックは、ルールベースの一番下にある事前定義済みのインターゾーンデフォルトブロックルールにマッチして拒否されます。明示的に設定したルールにマッチしないトラフィックに対する可視性を確保するために、インターゾーン デフォルト ルールのロギングを有効化してください。このトラフィックをログに記録することで、明示的に許可していないアクセスの試みを検査し、攻撃の試みやトラフィックを識別して許可ルールを修正できるようになります。

STEP 1 | ルールベースのインターゾーン デフォルトの行を選択し、**Override**（オーバーライド）をクリックしてルールを編集できるようにします。

STEP 2 | **interzone-default**（インターゾーン デフォルト）ルールの名前を選択し、ルールを編集します。

STEP 3 | Actions（アクション）タブで**Log at Session End**（セッション終了時にログを記録）を選択し、**OK**をクリックします。

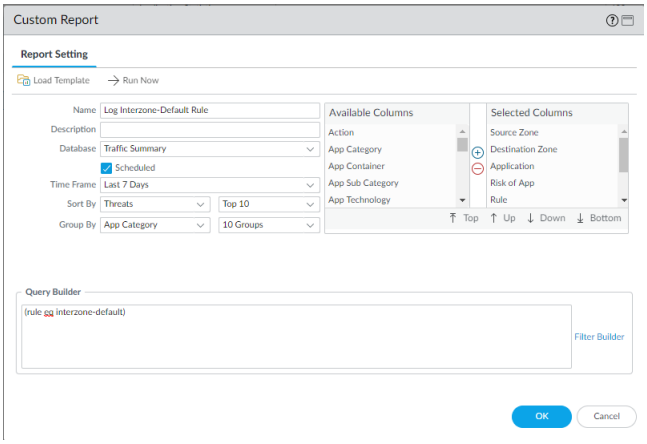
STEP 4 | このルールにヒットしたトラフィックを監視できるようにカスタム レポートを作成します。

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. レポートを **Add**（追加）して分かりやすい **Name**（名前）を付けます。この例では、名前は**Log Interzone-Default Rule**になります。
3. **Database**（データベース）を**Traffic Summary**（トラフィックサマリー）に設定します。
4. **Available Columns**（利用可能な列）から、**Source Zone**（ソースゾーン）、**Destination Zone**（宛先ゾーン）、**Sessions**（セッション）、**Bytes**（バイト）、**Application**（アプリケーション）、**Risk of App**（アプリケーションのリスク）、**Rule**（ルール）、および**Threat**（脅威）を**Selected Columns**（選択した列）リストに追加します。監視したい他の種類の情報がある場合は、それも選択してください。
5. **Scheduled**（スケジュール設定）のボックスを選択します。

6. 任意のTime Frame（期間）、Sort By（並び替え基準）、Group By（グループ化基準）の値を設定します。この例では、値がそれぞれLast 7 Days（過去7日間）、Threats（脅威）、App Category（アプリカテゴリ）になります。
7. そのインターゾーン デフォルト ルールにマッチするトラフィックにマッチさせるクエリを定義します：

```
(rule eq interzone-default)
```

最終的なカスタム レポートは次のようになります：



8. 変更を Commit（コミット）します。

データセンターの最良のルールベースを管理

アプリケーションは継続的に進化していくため、それに合わせてアプリケーション許可リストも修正していく必要があります。ベストプラクティスルールはポリシーオブジェクトを利用して管理を簡素化するため、新しいアプリケーションのサポートを追加したり、許可リストからアプリケーションを削除したりすることは、通常、対応するアプリケーショングループやアプリケーションフィルタを適宜変更することを意味します。

Palo Alto Networks が送信するコンテンツ更新を自動的にダウンロードしてファイアウォールにできるだけ早くインストールするように、スケジュールを設定してください。大抵のコンテンツ更新には脅威コンテンツ（アンチウイルス、脆弱性、アンチスパイウェアなど）に対する更新が含まれており、変更された App-ID が含まれている場合もあります。毎月第 3 火曜日のコンテンツ更新には、新しい App-ID も含まれます。ダウンロード後に指定した時間だけ通常のコンテンツ更新のインストールを遅らせたり、新しい App-ID が含まれる月一度の更新を遅らせたりするしきい値を、個別に設定できます。インストールを遅らせることで、新しい App-ID が含まれないコンテンツ更新をできるだけ早くインストールして最新の脅威シグネチャを入手しつつ、新しい App-ID をインストールする前に時間をかけて検証を行えるようになります。

新しい App-ID が含まれる毎月第 3 火曜日のコンテンツ更新によって、セキュリティポリシーの適用が変化する場合があります。新規あるいは変更された App-ID をインストールする前にポリシーによる影響を確認し、段階的に更新を行って影響をテストし、必要な場合は既存のセキュリティポリシールールを修正してください。Panorama を使用する場合、Panorama にコンテンツを読み込んで Panorama からプッシュするというのが、ファイアウォールにコンテンツ更新をダウンロードおよびインストールする際の最も効率の良い方法になります。

一般的なコンテンツ更新のベストプラクティスに従いつつも、基本的にデータセンターに高い可用性は不可欠であるため、データセンターではインターネットに接続されたファイアウォールほど素早くコンテンツ更新をロールアウトしないという選択肢があることも考慮してください。

- データセンターにインストールする前に、ネットワークの安全な領域で素早くコンテンツ更新をテストします。
- 新しい App-ID が含まれないコンテンツ更新の場合、自動ダウンロードからインストールを行うまでのしきい値を 8 時間以下に設定し、その期間中にテストを行ってください。
- 新しい App-ID が含まれるコンテンツ更新の場合、自動ダウンロードからインストールを行うまでのしきい値を 8 日以下に設定し、その期間中にテストを行ってください。
- すべてのコンテンツ更新に関するログ転送を設定します。

STEP 1 | 新しいコンテンツ更新をインストールする前に新規および変更された App-ID を確認し、ポリシーが影響を受けるかどうか判断します。

STEP 2 | 必要な場合は既存のセキュリティポリシールールを修正し、App-ID の変更を反映させてください。

さらにテストが必要な App-ID が一部ある場合は選択した App-ID を無効化し、他の新規 App-ID をインストールすることができます。オーバーラップを避けるため、新しい App-ID が含まれる翌月のコンテンツ リリースまでに、必要なポリシーの変更に対するテストを終わらせてください。

データセンター内で使用されるアプリケーションのリストは時間をかけて固まっていくため、新しい *App-ID* の数は徐々に少なくなっていきます。（大抵の *App-ID* はインターネットに接続するアプリケーションに関するものになります。）これにより、新しい *App-ID* がデータセンターの問題を発生させるリスクが減り、新しい *App-ID* を持つコンテンツ更新を素早くインストールできるようになるかもしれません。

STEP 3 | ポリシーを更新する準備を行い、コンテンツ リリースに含まれたApp-IDの変更に対応させるか、許可ルールに許可するアプリケーションを新しく追加したり、あるいは削除します。

最良のルールベースを維持する他の方法には次のようなものがあります：

- Palo Alto Networks の評価およびレビューツールを使用し、セキュリティのカバー範囲の漏れを特定します。
- アプリケーションにアクセスできなくなったというユーザーからのフィードバックがあれば、ルールベースの漏れや、ポジティブ エンフォースメントによって様ブロックされる前にネットワークで使用されていたリスクのあるアプリケーションを把握できます。
- データセンターを評価する際に作成したアセット インベントリのリストとアセット自体を比較し、対象のアセットが適切に保護されていることを確認します。
- アプリケーション コマンド センター（ACC）などの Palo Alto Networks のロギングおよび監視ツールを使用し、設定の誤りやルールの不足を示唆する予期せぬアクティビティを見つけて調査してください。定期的にレポートを実行し、適用したいレベルのセキュリティが適用されていることを確認します。

Panorama を使用してファイアウォールを管理する場合、ファイアウォールの安全状態を監視することで、デバイス同士やそのベースラインのパフォーマンスを比較して通常の動作からの逸脱を把握することができます。

Palo Alto Networks の評価およびレビューツールを使用

Palo Alto Networks のカスタマーサクセス チームは、ネットワークのセキュリティリスクや、ネットワークを保護するためにどの程度ファイアウォールやその他のツールの機能を活用できるのかを評価・確認するうえで役立つツールやリソースを使用する防止アーキテクチャを作成しています。Palo Alto Networks の担当者にお問い合わせいただければ、評価・レビュー（Palo Alto Networks のセールス エンジニアがレビューを行い、専門的な方法でお客様のネットワークのセキュリティの状態を評価いたします）を予定していただけます。執筆中の現時点で、利用できるセキュリティリスク防止ツールには次のものが含まれます：

- 保護状況評価（**PPA**）—ネットワークおよびセキュリティのアーキテクチャの全領域を対象にして、セキュリティリスクの防止対策が漏れている部分を見つけるのに役立つ一連のアンケートが PPA です。PPA はあらゆるセキュリティリスクを特定するうえで役立つだけでなく、リスクを防止して漏れをなくす方法も詳しく示してくれます。Palo Alto Networks の経験豊富なセールス エンジニアが主導する評価により、集中的に防止対策を行うべき、リスクの高い領域を把握しやすくなります。この PPA はファイアウォールおよび Panorama で実行できます。
- ベストプラクティス評価（**BPA**）ツール—次世代ファイアウォールおよび Panorama 用の BPA は、機能の導入状況を測定し、ポリシーがベストプラクティスに沿っているかどうか検証することでデバイスの設定を評価し、ベストプラクティスに対する違反を解決する方法を提案・指示してくれます。

  セキュリティポリシー アダプション ヒートマップ コンポーネントは、デバイス、シリアル番号、ゾーン、アーキテクチャの各エリア、その他のカテゴリー毎に情報をフィルタリングします。結果には、新機能を導入し、漏れを修正することでセキュリティを改善した率、ゼロトラスト ネットワークに向けた進捗状況などの傾向データが含まれています。

  BPA コンポーネント プラットフォームふぁ行うファイアウォールおよび Panorama 設定に対する 200 を超えるセキュリティ チェックでは、各チェックの通過/失敗スコアを得られます。各チェックは、Palo Alto Networks のセキュリティの専門家によるベストプラクティスに基づいています。チェックの結果が失敗スコアを返す場合、失敗スコアになった理由と問題の修正方法を提示してくれます。

Palo Alto Networks は継続的に新しいツールを作成して既存のツールを改善しています。Palo Alto Networks の担当者にお問い合わせいただければ、最新のツールを使用してデータセンターのネットワークのセキュリティを改善する方法をお伝えします。