paloalto TECHDOCS

セキュリティ ポリシーのベストプラクティス

Contact Information

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

About the Documentation

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

Copyright

Last Revised

July 5, 2023

Table of Contents

セキュリティ ポリシーのベストプラクティス

セキュリティ ポリシーは、ネットワーク上で許可するトラフィックと、そのトラフィックの処理方法を決定します。セキュリティ ポリシーのベストプラクティスでは、許可するトラフィックを、ビジネスに必要なトラフィックと従業員に許容されるトラフィックだけに制限します。これにより、攻撃対象領域が減少し、ネットワークとビジネス資産の保護に役立ちます。このドキュメントの視点は、ビジネスがセキュリティ優先かミッションクリティカルな可用性優先かにかかわらず、最適なネットワークセキュリティのために何をすべきかということです。

セキュリティ ポリシーのベストプラクティスは、最小権限の原則に従います。最小権限の原則とは、特定のアプリケーション、データ、およびインフラストラクチャへのアクセスを必要とする人だけにアクセスを許可し、トラフィックを適切に復号化、検査、およびログ記録して、資産、知的財産、およびビジネスにとって重要なその他のものを保護します。他のすべてのアクセスは、ビジネス目標を達成せずにリスクを増大させます。

本書には、次のことを行うための合理化されたステップバイステップのベストプラクティスが含まれています。

- セキュリティ ポリシーの計画
- セキュリティ ポリシーの導入
- セキュリティ ポリシーの維持

設定が必要な手順、または詳細な概念情報が記載されている手順には、該当するマニュアルへのリンクが含まれています。Palo Alto Networks 製品の特長、機能、および動作については、製品管理者ガイド、リリースノート、アップグレードガイド、インターコネクトガイドなどを参照してください。これらのガイドは、技術文書のホームページ（

- PAN-OS
- Panorama
- Panorama Managed Prisma Access（GlobalProtect アプリケーションのドキュメントを含む）
- クラウドマネージドPrisma Access
- Prisma SD-WAN
- クラウドで提供されるセキュリティサービス
- Cloud Identity Engine
- グローバルプロテクト
- VM-Series
- CN-Series
- Cortex Help Center

- ファイアウォールとアプライアンスのハードウェアガイド

復号化、DoS、ゾーン プロテクション（パケット バッファ保護を含む）などのテーマに関する最良のアドバイスについては、Palo Alto Networks のベストプラクティス ブック シリーズを参照してください。

セキュリティ ポリシーのベストプラクティスを計画する

ベストプラクティスのセキュリティ ポリシー ルールを作成する前に、安全なネットワークを計画するためのベストプラクティス、特に ゼロ トラスト ネットワーク アクセス (ZTNA) の原則を必ず理解してください。セキュリティ ポリシーは、許可およびブロックするトラフィックを定義します。ただし、ネットワークを完全に保護するには、次のようなツールやサービスの包括的なセットが必要です。

- 復号化、App-ID、User-ID、Device-ID などの可視性。
- 脆弱性防御、ウイルス対策、アンチスパイウェア、ファイル ブロック、サンドボックス、データ損失防止 (DLP)、DNS セキュリティなどの高度な脅威防御。
- 管理対象外のデバイスを制御するIoTセキュリティと、SaaSアプリケーションを制御するSaaSセキュリティ（次世代CASB）。

ネットワークを保護し、セキュリティ ポリシー内で使用するための適切なツールセットがあることを確認してください。

STEP 1 | 目に見えない脅威から身を守ることはできません。法的コンプライアンス、地域の規制、プライバシー規制、ビジネス上の考慮事項に従って、可能な限りすべてのトラフィックを復号化 して、トラフィックを可視化し、トラフィックを検査して脅威を防止できるようにします。SSLフォワード プロキシ (アウトバウンド) 復号化の場合、最初にユーザー ID と URLフィルタリングを実装して、効果的に復号化をターゲットにできるようにします。ピン留めされた証明書、クライアント認証、IoT デバイスの埋め込み証明書などの技術的な理由により、一部のトラフィックは復号化できません。

トラフィックを復号化しないと、ファイアウォールはアプリケーションを詳細に識別できません。たとえば、ファイアウォールは、コンテナ アプリケーションが Facebook であることを認識できますが、機能アプリケーションは認識できないため、ユーザーが Facebook 上でアップロード、ダウンロード、投稿などを行っているかどうかがわからず、制御できません。また、ファイアウォールはペイロードを確認して検査することができないため、悪意のあるコンテンツを防御するための可視性がありません。他のサブスクリプションを最大限に活用し、最適な保護を実現するには、トラフィックを復号してそのトラフィックを可視化する必要があります。

復号化にはライセンスは必要ありませんが、アウトバウンド トラフィックを復号化する場合は、Advanced URL Filtering ライセンスを追加すると、復号化に対するきめ細かなアプローチが可能になり、復号化するトラフィックの種類と復号化しないトラフィックの種類を簡単に選択できるようになります。URLフィルタリングを使用すると、法的、個人情報、規制、ま

たはその他の理由で復号化すべきではないカテゴリを除外できます。URLフィルタリングを使用すると、悪意のある Web サイトへのユーザー アクセスをブロックすることもできます。

さらに、インバウンド トラフィックを復号化して重要なサーバーを保護し、SSHプロキシ トラフィックを復号化して悪意のある管理トラフィックを防止します。

復号化の準備、展開、保守を行うには、復号化のベストプラクティス に従ってください。

STEP 2 | 最小特権アクセスと ゼロトラスト ネットワーク アクセスのレンズを通して、計画と展開のプロセスを表示します。

誰がどのデータとどのインフラストラクチャにアクセスするためにどのアプリケーションを使用する必要があるかを理解します。これにより、ビジネス目的でアクセスが必要なユーザーのみに必要なデータとインフラストラクチャへのアクセスを許可し、その他のアクセスはすべてブロックするセキュリティ ポリシー ルールを構築できます。

セキュリティ ポリシーで使用可能な属性を使用して、最小限の特権アクセスを定義します: ユーザー、デバイス、アプリケーション、送信元と宛先、サービス、および URL (アウトバウンド トラフィックの場合、復号化が有効になっているため、ファイアウォールはコンテナだけでなく各機能アプリケーションを可視化できます)応用）。

STEP 3 | ビジネスに適切な サブスクリプション を取得して、最良の脅威防御とセキュリティ体制を実現します。

- 高度な URLフィルタリング：Web サイトへの安全なアクセスを可能にし、ユーザーを危険なサイトから保護し、資格情報フィッシング攻撃の防止に役立つクラウド提供のサービスです。
- Advanced Threat Prevention (高度な脅威防御) またはアクティブなレガシー脅威保護 - クラウドで提供される Advanced Threat Prevention は、インライン ディープ ラーニングおよび機械学習モデルを使用して、回避型およびデイワン コマンド アンド コントロール (C2) 脅威をリアルタイムで適用します。また、標準のすべての機能が含まれています。脅威の防止。標準の脅威防御は、C2、マルウェア、および脆弱性の悪用から保護します。

  *Advanced Threat Prevention (*高度な脅威防御)はクラウドサービスであり、クラウド接続が必要なため、エアギャップ環境では使用できません。

  脅威コンテンツ更新のベストプラクティス に従って、最新の保護を確保してください。
- DNS セキュリティ—Advanced Threat Prevention (高度な脅威防御)を購入するか、アクティブな従来の脅威防御ライセンスとアクティブ化する DNS セキュリティ ライセンスが必要です。DNS トラフィック内の脅威を特定してブロックし、悪意のある DNS サイトへの

接続を防止するクラウド配信サービスであり、常に更新されます。新しいタイプの DNS ベースの攻撃を防ぎます。

- Enterprise Data Loss Prevention (データ損失防止 - DLP) ：すべての企業ネットワーク、クラウド、ユーザー全体でデータを保護し、データ安全規制への準拠を可能にするクラウド提供サービス。
- Cortex Data Lake (CDL)- ログ量に合わせて拡張し、次世代ファイアウォール、Panorama、Prisma Access、Cortex XDR からログを取り込むクラウドベースのログ ストレージ。ほとんどの Cortex アプリケーションは CDL を使用して、ログに記録されたネットワーク データにアクセスし、分析し、レポートします。
- WildFire—既知および未知の (新しい) マルウェアを識別し、ファイアウォールが悪意のあるトラフィックを識別してブロックするために使用するシグネチャを生成する、クラウドベースまたはプライベートの分析環境。
- SaaS セキュリティ—スタンドアロンまたはバンドルできるライセンスを使用して、認可された SaaS アプリケーションを保護するクラウド配信サービス:
  - データ セキュリティ ライセンスには、SaaS Security API と Enterprise DLP が含まれます。
  - SaaS Security Inline アドオン ライセンスは CDL と連携して、シャドウ IT アプリケーションを含むネットワーク上のすべての SaaS アプリケーションを検出して制御し、ファイアウォール管理者への SaaS ポリシーの推奨 を有効にします。
  - SaaS アプリケーションでのデータ損失を防ぐエンタープライズ DLP。
- IoT セキュリティ: ネットワーク上の IoT デバイスを検出して保護し、ファイアウォール管理者に対する IoT ポリシー ルールの自動推奨 を有効にします。計画、導入、監視については、IoT セキュリティのベストプラクティス に従ってください。
- GlobalProtect ： GlobalProtect モバイル アプリ、HIP チェック、 クライアントレス VPNなど、無料の VPN 機能を超える機能を提供します。

STEP 4 | ネットワークのセグメント化 計画を見直してください。

Panorama 管理の Prisma アクセスの場合、実質的にゾーンは trust と untrust の 2 つだけであり、 すべての Panorama ゾーンを Prisma trust ゾーンまたは Prisma untrust ゾーンにマッピングします。

Panorama とファイアウォール上で、ゾーンの粒度が十分でなく、異なるセキュリティ処理を必要とするデバイス、ユーザー、アプリケーションが含まれている場合は、ゾーンを再設計して、より粒度の高い方法でネットワークをセグメント化することを検討してください。同

様の処理が必要なユーザー、アプリケーション、デバイスを同じゾーンに配置します。小さなゾーンは大きなゾーンよりも防御が簡単です。

一部のクラウド環境では、構成できるゾーンの数がアーキテクチャによって制限される場合があります。

DoS およびゾーン プロテクションのベストプラクティス に従って、フラッド攻撃を防止し、各ゾーン内のデバイスとファイアウォール バッファを保護します。

クラウドマネージド Prisma アクセスの場合、 アイデンティティに基づいてマイクロセグメンテーションを行います。

STEP 5 | ビジネス目的で許可する必要があるアプリケーション (許可されたアプリケーション) と、その他の目的で許可したアプリケーション (許可されたアプリケーション) を定義します。

セキュリティ ポリシーの App-ID を使用して (サブスクリプションは必要ありません)、コンテナ アプリケーションとその機能アプリケーション (たとえば、「facebook」だけでなく「facebook-post」、「facebook-download」など) の両方を識別します。SaaS Security を使用する場合は、App-ID Cloud Engine (ACE) を使用してクラウド アプリケーションを識別します (SaaS Security サブスクリプションが必要です)。

ファイアウォールは、 アクション が許可であるセキュリティ ポリシー ルールで指定されたアプリケーションを許可し、ルールの条件に基づいて、 アクションがトラフィック を拒否、ドロップ、またはリセットするルールで指定されたアプリケーションを ブロック します。ルールに一致するには、トラフィックがルールの基準をすべて満たしている必要があります。アプリケーションがルールに一致しない場合は、セキュリティ ポリシー ルールベースの下部にある 2 つのデフォルト ルールによってトラフィックが制御されます。ゾーン間 (送信元と宛先が異なるゾーンにある) トラフィックは、デフォルトで拒否されます。ゾーン内 (送信元と宛先が同じゾーン内にある) トラフィックはデフォルトで許可されます。

アクセス ポリシーを伝達し、従業員が特定のアプリケーションにアクセスできない理由を理解できるようにします。

STEP 6 | すべてのユーザーを特定します。セキュリティ ポリシーで誰がどのアプリケーションやデバイスにアクセスできるかを制御し、ネットワーク内のどこにいても各ユーザーに一貫したポリシーが適用されるようにします。

User-ID(サブスクリプションは必要ありません) は、複数のソースからのユーザー情報を組み合わせて、ネットワーク上のすべてのユーザーを識別します。ユーザー ID の一貫性を確保し、ネットワーク全体に拡張するには、User-ID の集約された単一ソースとして Cloud Identity Engine (CIE)(サブスクリプションは必要ありません) を使用します。CIE は、ネットワーク上のソースからユーザー データを収集し、同期します。すべてのファイアウォールは、キャンパス上にあるかクラウド上にあるかに関係なく、CIE からまったく同じユーザー情報を取得

します。CIE は、Okta、Azure AD、PingID などのほとんどの主要な ID プロバイダー (IdP) と連携した認証も提供します。

PAN-OS 10.2 以前では、*CIE* はディレクトリ同期 *(DSS)* サービスとクラウド認証 *(CAS)* サービスを提供します。*PAN-OS 11.0* 以降では、*CIE* を再配布ポイントとして使用することもできます。

ユーザー グループを構成するときは、同じビジネス目的で誰が同じ方法で同じリソースにアクセスする必要があるかを考慮し、ユーザー グループ マッピングのベストプラクティス とダイナミック ユーザー グループ (DUG) のベストプラクティスに従ってください。

可能であれば、最高のセキュリティと信頼性の高いユーザー識別を実現するために、Always On モードで GlobalProtectVPN を使用してください。リモート アクセスおよび内部ゲートウェイに GlobalProtect を使用して、ユーザーがどこにいてもユーザー ID 情報を収集します。

STEP 7 | 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、適切なセキュリティ プロファイルまたはセキュリティ プロファイル グループ を添付することを計画します。(ルールによってトラフィックがブロックされる場合、ファイアウォールはブロックされたトラフィックを検査しません。)

セキュリティ プロファイル グループは、各プロファイルを個別に適用するのではなく、セキュリティ ポリシー ルールに適用する特定の目的に合わせて調整されたプロファイルのグループです。これにより時間を節約し、誤った構成を防ぐことができます。

STEP 8 | ログを保存する方法 (CDL、ログ コレクターなど) と、さまざまな種類と重大度のログ イベントについてどの管理者に通知するかを計画します。イベント発生後に調査できるように、十分なログ ストレージ容量を計画します。

STEP 9 | パノラマ や クラウド マネージド Prisma アクセス などの単一の管理ペインを使用して展開を管理し、より簡単で一貫性のあるセキュリティを実現します。

STEP 10 | 管理アクセスのベストプラクティス に従って、Panorama 管理者とファイアウォール管理者に最小限の権限でアクセスできるようにします。

STEP 11 | Day 1 構成は、カスタマー サポート ポータル **([Tools (ツール)] > [Run Day 1 Configuration (Day 1 構成)]** の実行) で利用でき、サポート ログインが必要です。これは、最小特権アクセスへのパスを開始するためのユースケースに依存しない構成モデルを提供するテンプレートです。Day 1 構成は、ダイナミック更新、セキュリティ プロファイル、ログなどの重要な要素を含む、基本的なネットワーク セキュリティのベストプラクティスをすぐに実装するのに役立ちます。

セキュリティ ポリシーのベストプラクティスを導入する

セキュリティ ポリシーの導入のベストプラクティスには次のものが含まれます。

- セキュリティ ポリシー ルールのベストプラクティス：誰がどのアプリケーションやリソースにどのようにアクセスできるか、マルウェアからトラフィックを保護する脅威プロファイルの適用まで、セキュリティ ポリシー ルール構築のあらゆる側面に焦点を当てます。
- セキュリティ ポリシー ルールベースのベストプラクティス：ルールベース内のセキュリティ ポリシー ルールのシーケンスと、それが許可およびブロックするトラフィックにどのような影響を与えるかに焦点を当てます。
- ポリシー オプティマイザーのベストプラクティス—ポリシー オプティマイザーを使用してルールベースを強化し、管理することに重点を置いています。
- App-ID Cloud Engine のベストプラクティス：セキュリティ ポリシーでクラウド App-ID を使用する方法と、ルールベースへの新しいクラウド App-ID の追加を自動化する方法に焦点を当てます。(App-ID Cloud Engine には SaaS Security Inline サブスクリプションが必要です。)
- ポリシーの推奨事項のベストプラクティス—SaaS ポリシーの推奨と IoT ポリシーの推奨に焦点を当てます。(SaaS Policy Recommendation には SaaS Security Inline サブスクリプションが必要で、IoT Policy Recommendation には IoT Security サブスクリプションが必要です。)

計画と導入を行う際には、次の原則に留意してください。

- 最小特権アクセスの原則。適切なソースから適切な宛先へ、適切なアプリケーションのみを使用して、適切なユーザーのみにアクセスを制限します。
- 復号化のベストプラクティスに従ってください。ビジネス上の考慮事項、地域のプライバシー規制、法的コンプライアンスを考慮して、トラフィックを最大限に可視化して検査および制御できる限りのトラフィックを復号化します。SSLフォワード プロキシ (アウトバウンド) 復号化の場合、最初にユーザー ID と URL フィルタリングを実装して、効果的に復号化をターゲットにできるようにします。

  

  アウトバウンド復号化の場合は、高度な *URL* フィルタリング ライセンスを取得して、復号化によって悪意のある *Web* サイトが公開された場合に、*URL* フィルタリングでその *Web* サイトへのアクセスをブロックできるようにします。

  

  ピン留めされた証明書、クライアント認証、*IoT* デバイスの埋め込み証明書などにより、一部のトラフィックは技術的な理由で復号化できません。
- 脅威がないか両方向のすべてのトラフィックを検査します。暗黙のうちに何も信頼しないでください。

- ダイナミック アドレス グループ (DAG)、 外部動的リスト (EDL)、および VM 監視 機能を使用して、セキュリティ ポリシーを最新の状態に保つために、可能な限り自動化します。

  自動タグ付けを使用して、ログ イベントに基づいてユーザーとデバイスのセキュリティ アクションを自動化します。自動タグ付けを使用すると、感染した可能性のあるデバイスを隔離したり、ユーザーに MFA 認証の使用を強制したりするなど、ログ イベントの発生時に実行するアクションを自動化できます。

- 構成の肥大化を回避します：

  - セキュリティ プロファイルとプロファイル グループ、タグ、アプリケーション グループ、アプリケーション フィルタ、ユーザー グループ、アドレス グループなどのオブジェクトを再利用します。Panorama では、 共有オブジェクト を使用して、複数のデバイス グループに同じオブジェクトを設定しないようにします。
  - 新しいポリシー ルールをルールベースに追加する前に、既存のルールをチェックして、複数の同様のルールを作成する代わりに、既存のルールに新しいアプリケーション、ユーザー、またはデバイスを追加できるかどうかを確認してください。

    既存のルールが、送信元ゾーン、宛先ゾーン、送信元 IP アドレス、宛先 IPアドレス、アプリケーション、サービス ポート、またはユーザーのオブジェクトのいずれかを除いて同じかどうかを確認します。これらのオブジェクトのうち 1 つだけが異なる場合は、新しいルールを作成する代わりに、新しいオブジェクトを既存のルールに追加します。

    たとえば、新しい会計アプリケーションを許可するとします。既存のルールベースを見ると、アプリケーションのデフォルト ポートを使用して、同じユーザー グループに対して、同じ送信元から同じ宛先へのアクセスを許可する、別の会計アプリケーションのルールが見つかります。新しいアプリケーション用に新しいルールを作成する代わりに、新しいアプリケーションを既存のルールに追加するだけです。

    この方法は、既存のルールを統合する場合にも有効です。

  - アウトバウンド トラフィックの場合は、同じセキュリティ処理を必要とする複数のアプリケーションの URL カテゴリに基づいて 1 つのルールを作成します。たとえば、すべての低リスク金融サービス トラフィックを許可するには (同じ方法でトラフィックを検査してログに記録したいと仮定して)、 金融サービス URL カテゴリと 低リスク URL カテゴリの両方を指定する許可ルールを作成します。
  - Policy Optimizer を使用して、 未使用のルールを削除 します。

- Panorama または Cloud Managed Prisma Access を使用してファイアウォール展開を管理し、デバイス グループを使用して単一またはファイアウォールのグループに一貫したセキュリティ ポリシーを適用できるようにします。

  プレ ルールとポスト ルールを 適切に使用します。

  - プレ ルール - ファイアウォールは、ローカルに定義されたルールおよびポスト ルールの前にプレ ルールを評価します。(個々のファイアウォールでローカルに定義されたルールは、それらのファイアウォールにのみ適用されます。) DNS やその他の重要なサービスを

許可したり、事前定義された脅威 EDL を使用して既知の悪意のある高リスク IP アドレスをブロックしたりするなど、すべてのファイアウォール展開に適用されるポリシーをプレ ルールに配置します。

- ポスト ルール - ファイアウォールは、プレ ルールおよびローカルに定義されたルールの後にこれらのルールを評価します。

> *Panorama Security* ポリシー ルールで、*[*ターゲット*]* タブを使用して、特定のファイアウォールまたはデバイス グループのサブセットをルールから除外します *(*これらの指定されたデバイスを除くすべてのデバイスをターゲットにします*)*。これにより、例外を作成するために階層の下位に複数の同様のルールを作成する代わりに、階層の上位に *1* つの広範なルールを作成できます。

- アプリケーション オーバーライド ポリシーは、レイヤー7 セキュリティ ポリシーと同じではありません。アプリケーション オーバーライドは、Palo Alto Networks プラットフォームに固有の多くのセキュリティ制御を削除するため、必要な場合を除き、これを使用しないでください。アプリケーション オーバーライドでは、レイヤー7 トラフィックの検査、セキュリティ プロファイルを使用した脅威からのトラフィックの保護、または App-ID の使用ができないため、リスクが増大します。ほとんどの場合、アプリケーション オーバーライドを使用するよりも、カスタム アプリケーションを 作成するか、 カスタム サービス タイムアウト を使用する方が適切です。

  既存のルールベースを確認します。SMB または SIP 以外のトラフィックに対するアプリケーション オーバーライド ルールがある場合は、ルールを App-ID ベースのルールに変換して、レイヤー7 でトラフィックを復号化して検査し、脅威を防止できるようにします。ルールが SMB または SIP トラフィック用の場合は、最小特権アクセスの原則に従い、可能な限り制限的なものであることを確認してください。

セキュリティ ポリシー ルールのベストプラクティス

このセクションでは、誰がどのアプリケーションやリソースにどの方法でアクセスできるかから、トラフィックをマルウェアから保護するのに役立つ脅威プロファイルを適用することまで、セキュリティ ポリシー ルールの構築について説明します。

セキュリティ ポリシー ルールは、アプリケーション、ユーザ、デバイス、送信元と宛先、URL、サービス (ポート) などのトラフィック一致条件を定義します。一致条件を組み合わせると、ルールにさらに詳細なコンテキストが追加され、ルールの範囲が狭まり、攻撃対象領域が減少します。一致条件により、ルールで制御したいトラフィックを正確に定義し、ゼロトラストネットワークアクセス (ZTNA) の原則に従うことができます。

セキュリティ ポリシー ルールは、トラフィックを許可または拒否するかどうか、ロギングとログ転送、脅威検査、スケジューリングなど、ルールの基準に一致するトラフィックに対して実行するアクションも定義します。

最小権限アクセスの原則を適用し、ネットワークをセグメント化するために、できるだけ具体的なセキュリティ ポリシー ルールを作成します。

- セキュリティ ポリシーの重要な概念セキュリティ ポリシー ルール:
- ルール名、説明、監査コメント、タグ—セキュリティ ポリシー ルールを管理するためのベストプラクティス
- ソースと宛先—最小権限アクセスの原則を適用してトラフィックの送信元と宛先をロックダウンするためのベストプラクティス。
- アプリケーションとサービス—ルールにアプリケーションを追加するためのベストプラクティス。
- Web サイトへのアクセス (URL フィルタリング)—外部 Web サイトへのユーザアクセスを許可する方法のベストプラクティス。
- ポリシーアクションとその他の設定—トラフィックを許可または拒否する方法、および QoS を適用する方法に関するベストプラクティス
- ロギングとログ転送—トラフィックを記録し、長期保存と分析のためにログを転送するためのベストプラクティス。
- セキュリティ プロファイル—セキュリティ プロファイルをセキュリティ ポリシー ルールに適用するためのベストプラクティス

セキュリティ ポリシーの重要な概念

効果的なセキュリティ ポリシーを作成するには、セキュリティ ポリシー ルールの機能、セキュリティ ポリシー ルールベースでの仕組み、トラフィックがルールと一致する方法、ルール構築のベストプラクティスに関する重要な概念を理解することが役立ちます。

- 地域の規制、コンプライアンス、ビジネス要件、プライバシーに関する考慮事項で許可されているすべてのトラフィックを復号化します。SSLフォワード プロキシ (アウトバウンド) 復号化の場合、最初にユーザー ID と URLフィルタリングを実装して、効果的に復号化をターゲットにできるようにします。トラフィックを復号化することで可視性が得られるため、ファイアウォールは機能しているアプリケーション（Facebookだけでなく、Facebookの投稿、Facebookのダウンロード、Facebookのファイル共有など）を特定し、Webサイトを特定し、脅威プロファイルを適用してトラフィック内の脅威を検査して防止できます。トラフィックを復号化することで、脅威対策を最大限に活用し、防御することができます。
- 許可ルールとブロックルール：Palo Alto Networksファイアウォールのセキュリティ ポリシーは、ポリシー ルールでトラフィックを明示的に許可し、明示的に許可しないトラフィック（許可リスト）はすべて拒否することに基づいています。明示的に許可しないトラフィックは暗黙的に拒否されます。目標は、ネットワーク上で必要なアプリケーション、ユーザー、デバイスのみを許可し、不要なものはファイアウォールで自動的にブロックすることです。

  許可リストベースのセキュリティ ポリシーに移行したら、ブロックルールを使用して危険な IP アドレス、Web サイト、アプリケーションへのアクセスを防止してください。定義済みの外部ダイナミックリスト (EDL) に基づいてブロックルールを作成してテストすることで、安全性が低いアプリケーションカテゴリに潜む防弾IPアドレス、高リスクIPアドレス、既知の悪意のある IP アドレスをブロックし、悪意のある URL やドメインへの認証を防止できま

す。高度な URLフィルタリングを使用して、危険な Web サイトへのアクセスをブロックします。

> ファイル共有アプリケーションには特に注意してください。悪意のある人物がそれらを利用してデータを盗み出す可能性があるためです。ほとんどのファイル共有アプリケーションをブロックします。ビジネス目的で必要なファイル共有アプリケーションについては、ビジネス目的でそれらのアプリケーションを必要とするユーザーにのみアクセスを許可してください。

セキュリティを最も厳しくするために、ビジネス目的で使用されるアプリケーションのみを許可してください。ただし、ほとんどの企業では、一部の非業務アプリケーション（許容アプリケーション）を従業員に許可する必要があります。許容範囲内のどのアプリケーションを許可するかを検討し、それらのアプリケーションがデータのアップロードやダウンロードなど、組織に何らかの脅威をもたらすかどうかを自問してください。できるだけ多くのトラフィックを復号化して検査し、脅威がないか調べます。

- セキュリティ ポリシー ルールは具体的です。トラフィックがセキュリティ ポリシー ルールで指定されたすべての条件に一致しない場合、トラフィックはルールと一致しません。たとえば、ルールで特定のユーザ、アプリケーション、送信元と宛先が指定されている場合、トラフィックがルールに一致するにはこれらの条件をすべて満たす必要があります。ユーザ、ソース、宛先が一致してもアプリケーションが一致しない場合、トラフィックはルールに一致しません。
- セキュリティ ポリシー ルールは、誰がどのアプリケーションとインフラストラクチャにアクセスできるかを定義することにより、ネットワークをセグメント化します。ルールは、ソース、宛先、ユーザ、デバイス、サービス、URL を定義することによってネットワークをセグメント化します。
- セキュリティ ポリシー ルールは、添付されているすべての脅威対策プロファイルを、ルールに一致するトラフィックに適用します。
- セキュリティ ポリシー ルールは順序付けられたルールベースにあります (ルールの順序はユーザーが選択します)。ファイアウォールは、セキュリティ ポリシー ルールベースの最初のルールから始まり、ルールベースの最後のルールまでトラフィックをセキュリティ ポリシー ルールと比較します。トラフィックがルールの条件に一致すると、ファイアウォールはトラフィックに対してルールのアクションを実行し、トラフィックを他のルールと比較しません。トラフィックに一致するルールがない場合、ファイアウォールはトラフィックをドロップします (暗黙的な拒否)。
- ルールがシャドーイングされないように、ルールベースの一般的なルールの上に、より具体的で詳細なセキュリティ ポリシー ルールを配置します。シャドウイングとは、より具体的なルールと同じ一致条件を含む広範なルールが、特定のルールよりもルールベースの上位に配置されることです。その場合、特定のルールに一致することを意図したトラフィックは、代わりに一般的なルールに最初に一致します。
- トラフィックが他のルールと一致しない場合、ルールベースの一番下にある **2** つのデフォルトのセキュリティ ポリシー ルールは、異なるゾーン間のすべてのトラフィックを自動的に

ドロップし（**interzone-default**）、同じゾーン間のすべてのトラフィックを自動的に許可します（**intrazone-default**）。インターゾーン間のデフォルトルールとゾーン内のデフォルトルールを変更して、トラフィックをログに記録したり、脅威検査を適用したりできます。ルールベースの早い段階ですべてのトラフィックを拒否するルール（ローカル ファイアウォール ルールまたはパノラマプレルールとポスト ルール）を追加すると、デフォルトルールに一致するトラフィックはありません。

- 最小権限アクセスの原則をセキュリティ ポリシーのルール構築に適用します (詳細かつ正確に)。
  - どの管理者がどのファイアウォールや Panorama デバイスのどの部分を管理できるかを制御します。管理アクセスを保護するためのベストプラクティスに従ってください。
  - すべてのユーザー (ネットワーク上に未知のユーザーがいないこと)、ネットワーク上で許可するアプリケーション、インフラストラクチャ (ユーザーとアプリケーションがアクセスするリソース) を特定します。セキュリティ ポリシー ルールで不要なアクセスを許可しないように、ビジネス目的でどのアプリケーションやリソースにアクセスする必要があるかをマッピングします。ビジネスリソースと認可対象アプリケーションへのアクセスは、ビジネス目的でアクセスする必要があるユーザーにのみ許可し、必要最小限のアクセス権限のみを許可します。
  - 従業員の利益のために許容される業務以外のアプリケーションへのアクセスを許可してください。
  - ほとんどの場合、ブロックルールの代わりに許可ルールを使用してください。増え続けるネットワーク上で許可したくないアプリケーションを明示的にブロックするよりも、ネットワーク上で許可したいものを定義し、残りを暗黙的に拒否する方が正確で簡単です。
  - ルールベースを最適化して、未使用のアプリケーションを含むルールを編集し、使用されていないルールを削除または無効にします。

ルール名、説明、監査コメント、タグ

[名前]、[説明]、[監査コメント]、および [タグ] フィールドを使用すると、セキュリティ ポリシー ルールベースの管理と操作が容易になり、各ルールの内容を理解しやすくなります。また、経験の浅い管理者も、新しいアプリケーション、ユーザー、またはユーザーグループを既存のルールに追加するタイミングと、新しいルールを作成するタイミングを理解するのにも役立ちます。

STEP 1 | 名前 — 各ルールが何をするのかを識別します。

ルールベースの検索を容易にする用語を使用する標準的な命名規則を開発してください。各ルールの機能を管理者にわかりやすく示す名前を使用すると、各ルールが制御するトラフィックを理解しやすくなり、特定のルールをより簡単かつ直感的に検索できます。

STEP 2 | 説明 — ルールベースを調べる人なら誰でも、ルールが作成された理由と意図した結果を理解できるように、ルールの目的を説明します。

PAN-OS と Panorama Managed Prisma Access にすべてのポリシーの説明が表示されるようにするには、[パノラマ > セットアップ > 管理 > ポリシー ルールベース設定(デバイス > セットアップ > 管理 > ポリシー ルールベース設定) の **[ポリシーの説明が必要]** を有効にします。説明のない既存のルールについては、次にルールを編集するときに追加してください。

クラウド・マネージド・プリズマ・アクセスでは、管理者が説明を入力するようにしてください。

STEP 3 | タグ — フローベースのコンポーネント、アプリケーションベースのポリシー、内部サービス、特定のユーザーグループなど、ビジネスにとって意味のあるものをすべて説明する高レベルの記述子。

タグはポリシーをグループにまとめ、タグに基づいてポリシーをフィルタリングおよび検索できます。

たとえば、**`disabled`** というタグを作成し、無効になっているすべてのルールに適用すると、ルールベースをフィルタリングして、そのタグに基づいて無効になっているすべてのルールを表示できます。同じタグを使用して、無効とラベル付けされているが、無効タグと無効化された**`eq no`**をフィルタリングして再有効化されたルールをルールベースで検索できます。

PAN-OS と Panorama Managed Prisma Access にすべてのポリシーのタグが表示されるようにするには、[パノラマ > セットアップ > 管理 > ポリシー ルールベース設定(デバイス > セットアップ > 管理 > ポリシー ルールベース設定) の **[ポリシーのタグが必要]** を有効にします。タグのない既存のルールについては、次にルールを編集するときにタグを追加します。

STEP 4 | タグや説明がない場合は、管理者がポリシーをコミットできないようにします。

PAN-OS と Panorama Managed Prisma Access で、[パノラマ > セットアップ > 管理 > ポリシー ルールベース設定(デバイス > セットアップ > 管理 > ポリシー ルールベース設定) の **[Fail commit if policies have no tags or description (**ポリシーにタグや説明がない場合、コミットを失敗**)]** を有効にします。既存のルールでは、次にルールを編集するときにタグと説明を追加しないと、コミットは失敗します。

STEP 5 | 監査コメント — ルールへの変更と変更の理由を追跡して、ルール変更の履歴と変更の根拠を把握できます。これは、災害復旧時のみに使用されるルールや、限定的に使用されるルールを文書化する場合に特に役立ちます。

PAN-OS と Panorama Managed Prisma Access では、すべてのポリシーに監査コメントが含まれていることを確認し、[パノラマ > セットアップ > 管理 > ポリシー ルールベース設定] (デバイス > セットアップ > 管理 > ポリシー ルールベース設定) で [ポリシーに監査コメントが必

要] を有効にし、監査コメント形式を指定します。監査コメントのない既存のルールについては、次にルールを編集するときに追加する必要があります。

監査コメントはルールに永久に残ります。ルールの [監査コメントアーカイブ] をクリックすると、削除できない履歴が表示されます。

ソースと宛先

トラフィックの送信元と送信先を制御するには、最小権限アクセスの原則に従う必要があります。ルールと一致させたいアプリケーショントラフィックの正確な送信元と宛先を指定するセキュリティ ポリシー ルールを作成します。アプリケーションがビジネス目的で必要としない送信元や宛先からのトラフィックをルールで許可すると、攻撃対象領域が増え、リスクが高まります。送信元と宛先をビジネス目的に必要なものに厳密に制限することで、攻撃対象領域が減り、リスクが軽減されます。

ソースとデスティネーションをきめ細かく制御することで、最小限の権限アクセスを実現できます。

- ソース — ゾーン、アドレス、ユーザ、デバイス、5G セキュリティ、加入者、機器、ネットワークスライス。
- 宛先-ゾーン、アドレス、デバイス。

ソースオブジェクトと宛先オブジェクトの数を減らすには、個々のアドレスとユーザーの代わりにアドレス グループオブジェクトとユーザーグループオブジェクトをできるだけ使用してください。これにより、ポリシーが簡略化され、理解しやすくなります。ルールベースを明確にするために、ソースオブジェクトとターゲットオブジェクトの合計数を制限します。

STEP 1 | PAN-OSでは、データやアプリケーションへの不要なアクセスを防ぐために、ソースゾーンとターゲットゾーンをできるだけ狭く指定してください。

すべてのウェブサーバー用のゾーンなど、特定の目的にゾーンを割り当てると、通常、ゾーン内のすべてのサーバーが同じセキュリティ ポリシーを必要とするため、きめ細かなポリシーを簡単に作成できます。

パノラママネージドプリズマアクセスは、信頼ゾーンと非信頼ゾーンという2つのゾーンを使用します。Panorama　ゾーンを Prisma トラスト ゾーンまたはプリズマ非トラスト ゾーンにマッピングします。

Cloud Managed Prisma Access は、信頼、非信頼、クライアントレス *VPN* の 3 つのゾーンを使用します。これらのゾーンは、デフォルトでトラスト ゾーンにマッピングされます。多くのサードパーティ *SD-WAN* 統合では、ログビューアーのソースゾーンはリモートネットワークの名前を使用します。

STEP 2 | データやアプリケーションへの不要なアクセスを防ぐため、送信元アドレスと宛先アドレスはできるだけ狭く指定してください。ポリシーを簡略化するために、個々のアドレスで

はなくアドレス グループをできるだけ使用してください。ルールがゾーン内のすべてのデバイスに適用される場合、インバウンド トラフィックでは宛先アドレスを **any** として指定し、アウトバウンド トラフィックでは送信元アドレスを **any** として指定します。

- FQDN アドレスオブジェクトを使用して内部システムを参照し、システム IP アドレスが変更されてもその変更がポリシーに影響しないようにします。
- ポリシーで動的アドレス グループ (DAG) を使用すると、ログイベントと自動タグ付けに基づいて、サーバーの役割やセキュリティ体制の変更に自動的に適応できます。サーバーをグループ化し、ビジネスに適したタグ付け戦略を立てる方法を考えてください。

  指定されたログイベントが発生すると、ファイアウォールは自動タグ付けに基づいて IP アドレスをある DAG から別の DAG に移動します。DAG は自動的に更新され、コミット アクションは必要ありません。これにより、感染の可能性があるサーバーまたはエンドポイントを、重要なリソースへのアクセスを許可するポリシー ルール内の DAG から、そのアクセスをブロックするポリシー ルール内の DAG に移動する（デバイスを隔離する）などのセキュリティアクションを自動化できます。
- 自動化が進んだデータセンター環境では、データセンターが仮想サーバーをスピンアップおよびスピンダウンするときに、DAG を使用して VM へのアクセスを制御します。ネイティブ XML API またはファイアウォール上の VM 監視エージェントを使用してタグを動的に登録します。
- データセンター環境では、セグメンテーションと自動化を組み合わせると、個々の IP アドレスの管理が困難になる場合があります。環境の管理が難しすぎる場合の最後の手段として、サブネットを使用しますが、これは安全性の低い方法です。
- パロアルトネットワークスの定義済み外部ダイナミックリスト (EDL) を送信元または宛先として使用して、高リスクで防弾性のあるその他の悪意のある IP アドレスとの間のトラフィックをブロックします。
- コンプライアンス、ビジネスポリシー、またはその他の理由により、地域をブロックする必要がある場合は、その地域を住所として指定してください。（インバウンド トラフィックの場合は、送信元として地理的地域を指定し、宛先として任意の地域を指定します。アウトバウンド トラフィックの場合は、送信元として **any** を指定し、宛先として地理的リージョンを指定します。）

STEP 3 | セキュリティ ポリシーがオンプレミスとリモートアクセスの両方で有効になるように、User-IDを使用してソースユーザーを指定します。ユーザーの場所や接続方法に関係なく、一貫したポリシーを確保するには、一貫したユーザー識別が不可欠です。

- コンテキストに基づいてユーザーグループを作成します。ユーザーはビジネス目的で何をする必要があるか、一般的なアクセス要件は何か。このビューポイントでは、アクセスす

る必要のあるリソースと使用する必要のあるアプリケーションごとにユーザーをグループ化できるため、論理グループを作成してポリシーを適用できます。

ネットワークセキュリティチームに、ユーザーグループを管理するチームと協力してもらい、グループ分けがセキュリティコントロールにとって意味のあるものになるようにします。

グループを使用できない場合にのみ、ポリシーで個々のユーザーを指定してください。たとえば、CEO をはじめとする少数の経営幹部が、他のユーザーやグループに付与すべきではないさまざまなアクセス権を必要とする場合があります。

- 導入環境で許可されている場合は、クラウド・アイデンティティ・エンジン (CIE) を使用して次のことを行います。
  - クラウドとオンプレミスの両方のネットワーク全体のすべてのUser-IDソースを集約します。
  - ディレクトリソースを同期します。
  - ネットワーク全体で一貫したユーザ ID 情報を提供します。

  Consistent User-ID を使用すると、ポリシーによってネットワーク上のあらゆる場所のユーザーを追跡できます。

  *CIE*は、*Okta*、*Azure AD*、その他多くのアイデンティティプロバイダーとの統合を通じて認証を提供します。
- GlobalProtectは、最も正確で包括的なユーザー情報と最高の精度を備えたユーザーIDマッピングソースです（他にも多くの可能なユーザーIDマッピングソースがあります）。
- ポリシーで動的ユーザーグループ（DUG）を使用すると、ログイベントと自動タグ付けに基づいて、ユーザーの異常な行動や悪意のあるアクティビティを自動的に修正できま

す。DUG は DAG と同様に機能します。隔離やアクセス制限が必要なアクティビティは何かを考え、ビジネスに適したタグ付け戦略を立ててください。

また、DUG を使用してユーザーグループへの定期的なアクセスを許可します。たとえば、DUG は、監査中は四半期ごとの監査人（監査人のユーザーグループで定義されているとおり）にアクセスを許可し、それ以外の時間にはアクセスをブロックできます。

- セキュリティ ポリシー ルールの設定では、特定のユーザーとグループを指定することに加えて、ルールをすべてのユーザー、ログオン前のユーザー、既知のユーザー (認証済み)、または未知 (認証されていない) ユーザーのいずれに適用するかを指定できます。
  - DNS、NTP、OCSP などの基本サービスへのアクセスなど、すべてのネットワークユーザーに適用されるルールには **any** を使用してください。
  - ネットワーク上で未知のユーザーを許可しないでください。未知のユーザーをブロックするルールを作成します。または、社内ネットワークへのアクセスを許可しないという条件で、ゲストアクセスには**unknown**を使用してください。
  - 事前ログオン機能付きリモートアクセス VPN は、GlobalProtect ユーザー専用です。ユーザーがデバイスにログインする前にVPNトンネルを確立してエンドポイントを認証し、DHCP、DNSなどの特定のサービスへのアクセスを可能にします。また、各エンドポイントにマシン証明書をインストールする必要があります。ログオン前のユーザーアクセスを許可するポリシー ルールは、マシン認証と必要なネットワークサービスへのアクセスのみを許可する必要があります。ログオン前のユーザーのその他のアクセスをすべて拒否します。

  最も重要な原則は、最小限の権限アクセスです。ビジネス目的でアプリケーションやリソースへのアクセスを必要とするユーザーとグループにのみアクセスを許可します。

- User-IDのベストプラクティスに従ってください。

STEP 4 | IoT デバイスを管理するセキュリティ ポリシー ルール (IoT セキュリティにはサブスクリプションが必要) で、デバイス ID (PAN-OS 10.0 以降) を使用して IoT デバイスを指定します。

デバイスオブジェクトは、User-IDがソースユーザーを識別するのと同じ方法で、IoTデバイスのデバイスIDを定義し、ソースデバイスを識別します。デバイスオブジェクトには、一致条件として使用する 6 つのメトリックがあります。デバイス ID と一致するには、デバイスが設定されたすべてのメトリックと一致する必要があります。ほとんどの場合、1 つか 2 つのメトリックを定義すれば十分です。定義する指標が多いほど、フィルターが限定的すぎて、一致させたいデバイスと一致しない可能性が高くなります。デバイスがファイアウォールに送信する情報を把握して、デバイスオブジェクトを定義するためにどのメトリックを設定すればよいかを判断します (すべてのデバイスがすべてのメトリックを送信するわけではありません)。以下の操作コマンドは、IoT デバイスがファイアウォールに送信する情報を表示します。

- **`> show iot ip-device-mapping-mp all`**—ファイアウォール上のすべての IP アドレスとデバイスのマッピングを表示します。

- **> show iot ip-device-mapping-mp ip<ip-address>**—指定した IP アドレスの IP アドレスからデバイスへのマッピングを表示します。

IoT セキュリティのベストプラクティスに従ってください。

アプリケーションとサービス

デフォルトでは、セキュリティ ポリシー ルールベースの一番下にある暗黙の拒否ルールは、セキュリティ ポリシー ルールで明示的に許可していないアプリケーションをブロックします。最小権限アクセスを強制するには、ビジネス目的（制裁対象アプリケーション）と従業員（許容されるアプリケーション）で許可したいアプリケーション（許容されるアプリケーション）のみを指定するように、セキュリティ ポリシー ルールを調整します。アプリケーションベースのルールでは、各機能アプリケーションを使用するユーザーとその使用方法をきめ細かく制御できるため、ゼロトラストネットワークアクセス環境に移行する際に正確なセキュリティ ポリシー ルールを作成できます。ポートベースのルールは、開いているポート上のすべてのアプリケーションを許可しますが、避けてください。

ファイアウォールが「*-base*」アプリケーションだけでなく、機能しているアプリケーションを表示するには、復号化を有効にする必要があります。機能しているアプリケーションを確認することで、アプリケーションをきめ細かく制御できます。たとえば、ファイアウォールには、コンテナアプリケーション「*facebook*」だけが表示されるのではなく、「*facebook*への投稿」、「*facebook*のダウンロード」、「*facebook*のファイル共有」などが表示されます。これにより、最小権限アクセスに基づいてセキュリティ ポリシーを設定できます。すべての従業員にすべての*Facebook*機能アプリケーションへのアクセスを許可する代わりに、特定の機能アプリケーションへのアクセスを適切なユーザーに対して制限またはブロックできます。

コンテナアプリケーションをルールに追加すると、その機能アプリケーションすべてが暗黙的にルールに追加されます。許可するアプリケーションとその使用を許可するユーザーをよりきめ細かく制御できるように、許可するアプリケーションの機能を正確に指定してください。

アプリケーションにベストプラクティスのアドバイスをどのように適用するかは、環境が新規、既存、移行のいずれであるかによって異なります。推奨事項の多くは、最終的なベストプラクティスの状態を反映しています。場合によっては、移行に関するアドバイスやさまざまな環境に関するアドバイスを提供します。ただし、環境はそれぞれ異なります。目標は、どのアプリケーションがネットワークを通過し、どのアプリケーションが許可され許容されるかを把握し、その情報を利用して、ビジネス目的で制裁対象とするアプリケーションのみを許可し、従業員のアクセスは許可するアプリケーションのみを許可するセキュリティ ポリシー ルールベースに安全に移行することです。

セキュリティ ポリシー ルールベースのベストプラクティス セキュリティ ポリシー ルール ベースのどこにルールを配置するかについて説明します。

1. セキュリティ ポリシー ルールの作成を簡素化および強化し、ルールベースのサイズを縮小するには、できるだけアプリケーショングループを使用してください。

   アプリケーショングループは、同様のセキュリティ処理を必要とするユーザー定義のアプリケーションセットです。セキュリティ ポリシー ルールにアプリケーショングループを追加すると、アプリケーションごとに個別のルールを作成する代わりに、1つのルールで複数のアプリケーションを制御できます。アプリケーションをグループに追加したり、その他の変更を加える必要がある場合は、すべてのルールを変更するのではなく、一度変更するだけで済みます。アプリケーショングループを更新すると、それを参照するルールが自動的に更新されるからです。
2. アプリケーションをアプリケーショングループに追加する場合でも、個々のセキュリティ ポリシー ルールに追加する場合でも、グループを使用してコンテナアプリケーションをブロックする（これにより、機能しているアプリケーションがすべてブロックされる）場合や、コンテナアプリケーションの機能アプリケーションすべてへのアクセスを許可する場合を除き、必要な機能アプリケーションを正確に指定してください。
3. アプリケーションの依存関係は、アプリケーションが正常に動作するために他のアプリケーション (依存アプリケーション) を必要とする場合に発生します。アプリケーションの依存関係は、許可するアプリケーションにのみ関係し、ブロックするアプリケーションには関係ありません。依存アプリケーションには次の 2 種類があります。

   - 明示的なアプリケーション。ルールにアプリケーションを追加するとファイアウォールに表示され、アプリケーションが正しく動作するように手動で追加します。たとえば、facebook-chat アプリケーションは facebook-base アプリケーションと mqtt ベースアプリケーションを手動で追加することに依存しています。
   - 暗黙的なアプリケーション。指定したアプリケーションのサポートをファイアウォールが自動的に許可し、ルールに明示的に追加する必要はありません。たとえば、facebook-chatが正常に動作するために必要な明示的なアプリケーションに加えて、facebook-chatをルールに追加すると、ファイアウォールは自動的にアプリケーションのジャバーとWebブラウジングを許可します。（ルールに明示的に追加しない限り、JabberとWebブラウジングはすべてのトラフィックで許可されるわけではなく、facebook-chatトラフィックでのみ許可されます。）

     アプリケーションを許可するときは、どのアプリケーションを暗黙的に許可するかに注意してください。

   アプリケーションの依存関係はいくつかの方法で確認できます。

   - **Applications** オブジェクトは、アプリケーションの検索可能なデータベースを提供します。アプリケーションを選択すると、その明示的なアプリケーション依存関係 (依存) と暗黙的なアプリケーション依存関係 (暗黙的に使用) が表示されます。
   - Palo Alto Networks の applipedia は、コンテンツ配信アプリIDの検索可能なデータベースです。アプリケーションを検索して選択すると、その明示的なアプリケーション依存関係

(アプリケーションによって異なります) と暗黙的なアプリケーション依存関係 (暗黙的な使用アプリケーション) が表示されます。

- セキュリティ ポリシー ルールにアプリケーションを追加すると、ファイアウォールは明示的な依存アプリケーションを表示しますが、暗黙的な依存アプリケーションは表示しません。
- **Validate** をコミットすると、1 つのルールだけでなく、セキュリティ ポリシー ルールベース全体に基づいてアプリケーションの依存関係を確認できます。

ネットワーク環境とビジネスはそれぞれ異なるため、アプリケーションの依存関係をどのように処理するかは万能な推奨事項ではありません。ビジネス要件とセキュリティ要件に応じて、アプリケーションの依存関係に対処する方法は2つあります。

- 可用性を重視-セキュリティ ポリシー ルールに表示されているすべての依存アプリケーションをルールに追加して、アプリケーションが正しく機能するようにします。たとえば、フェイスブックチャットを制御するルールでは、facebook-base と mqtt-base をルールに追加します。

  ただし、その結果、SSL などの一般的な依存アプリケーションが 1 つのルールだけでなく多くのルールに追加され、ルールベースが乱雑になることがあります。(ルールベースで既に SSL が許可されている場合でも、SSL は他の多くのアプリケーションの依存アプリケーションとして表示されます)。 これを軽減する良い方法は、Policy Optimizerを使用して依存アプリケーションの重複を削除することです。
- セキュリティに重点を置く — 許可するアプリケーションをできるだけ少なくするには、**Commit Validate** を実行して、セキュリティ ポリシー ルールベース内のすべてのアプリケーション依存関係を確認します。Commit Validate の出力に基づいて必要な依存関係を追加します。ユーザーに基づいてアクセスを制御できるように、許可したいすべての依存アプリケーションを含むさまざまなアプリケーションの依存関係（VMwareの依存関係、ソフトウェア更新の依存関係など）用のアプリケーショングループを作成することを検討してください。

4. 新規および既存の導入では、既知の悪質で危険なトラフィックを直ちにブロックします。

   - Advanced Threat PreventionまたはThreat Preventionのサブスクリプションを必要とするパロアルトネットワークスの組み込み外部ダイナミックリスト（EDL）など、信頼できる脅威インテリジェンスソースに基づいて、潜在的に悪意のあるトラフィックをブロックし、防弾IPアドレス、高リスクIPアドレス、既知の悪意のあるIPアドレス、およびTor出口ノードと呼ばれるIPアドレスをブロックします。
   - 暗号化された DNS をブロックしてトラフィックの可視性を維持し、脅威プロファイルを使用してトラフィックに脅威がないか検査します。攻撃者はさまざまな種類の攻撃にDNSを使用するため、DNSトラフィックを検査する必要があります。DNS-over-HTTPS (DoH) とDNS-over-TLS (DoT) の両方をブロックし、パロアルトネットワークスのDNSサービスを

使用してください。暗号化されたDNSをすぐにブロックできない場合は、トラフィックを可視化し、DoHトラフィックと (DoT) トラフィックのブロックに移行してください。

> *App-ID*は細分性があるため、あるルールでは通常の*DNS*トラフィックを許可し、別のルールでは*DoT*トラフィックと*DoH*トラフィックをブロックできます。これは、セキュリティ ポリシー ルールで指定できるアプリ*ID*がそれぞれ異なるためです。

- 悪意のある攻撃者は、ファイル共有アプリケーションを使用してデータを盗み出すことがよくあります。ほとんどのファイル共有アプリケーションをブロックし、ビジネス目的でそれらのアプリケーションを必要とするユーザーのみにビジネスファイル共有アプリケーションへのアクセスを許可します。これを実現する簡単な方法は、ユーザーを指定し、サブカテゴリのファイル共有やタグ「アップロード」を含むアプリケーションフィルタを設定するルールを作成することです。

許可リストベースのセキュリティ ポリシーを作成すると、ほとんどの不要なアプリケーションが暗黙的にブロックされるため、多くのブロックルールは必要ありません。ネットワーク上で必要なアプリケーショントラフィックのみを許可し、各アプリケーションを誰が使用する必要があるかを検討することで、ブロックする対象をビジネス要件に基づいて決定します。

5. ほとんどの場合、サービスをアプリケーションデフォルトに設定します。App-IDはポートやプロトコル（スプーフィング可能）ではなく署名に基づいているため、App-IDは非常に正確であるため、ポートを指定する必要はありません。アプリケーションのデフォルトを使用すると、正規のアプリケーション以外のアプリケーションがポートを使用できなくなり、回避的なアプリケーションが非標準ポートを使用できなくなります。将来、アプリケーションのデフォルトポートが変更されても、application-default は新しいポートを自動的に適用するため、サービスポート設定を再構成する必要はありません。

   カスタムアプリケーション、特別なアーキテクチャ要件、または会社のセキュリティ要件で要求される場合にのみ、サービスポートを指定してください。

6. 内部アプリケーションやApp-IDのないアプリケーションについては、カスタムアプリケーションを作成して、トラフィックをレイヤ7で可視化します。アプリケーションオーバーライドポリシーは、レイヤー 7 の処理と脅威検査をバイパスするため、使用しないでください。アプリケーションオーバーライドのユースケースは、SMB または SIP トラフィックでは珍しい状況です。

7. アプリケーションフィルタを使用して、ネットワーク上のトラフィックを検出し、新しいアプリケーションを処理します。

   アプリケーションフィルターは動的なアプリケーションセットです。アプリケーションは、カテゴリ、サブカテゴリ、リスク、タグ (定義済みのタグまたはカスタムタグ)、特性など、定義した属性に基づいてアプリケーション フィルタを照合します。ファイアウォールは、フィルター条件に一致すると、新しいアプリケーションをフィルターに自動的に追加しま

す。アプリケーションフィルタを含むセキュリティ ポリシー ルールは、フィルタに一致する新しいアプリケーションを自動的に制御します。

アプリケーションフィルタは、アプリケーショングループよりも制御が緩いです。どのアプリケーションをアプリケーション グループに入れるかを正確に制御できます。定義する属性によって、どのアプリケーションがアプリケーションフィルタに含まれるかが制御されるため、メンバーシップの幅が広がり、必要以上に多くのアプリケーションが許可される可能性があります。そのため、トラフィックを検出して制御するのに最適です。

ユースケースには以下が含まれます。

- トラフィックにまだ慣れていない新しい導入環境では、アプリケーションフィルターを使用してトラフィックのさまざまなカテゴリやサブカテゴリを分析し、それらのタイプのアプリケーションのうちどれがネットワーク上にあるかを確認できます。

  アプリケーションフィルターを作成して、成熟したデプロイメントでさまざまなタイプのトラフィックを検出することもできます。
- 新しいアプリケーション用にルールベースをフィルタリングします。新しいアプリケーションに一致するフィルターを作成し、ルールベースの上部付近にルールを配置します。ポリシーオプティマイザーを使用すると、アプリケーションを可視化して制御できます。

  コンテンツの更新により新しいアプリケーションが制御されます。アプリケーションコンテンツアップデートがリリースされると、次のアプリケーションコンテンツアップデートがリリースされるまで、新しいアプリケーションとして認識されます。リリースは通常、毎月第3火曜日またはその前後に行われます。次の新しいアプリケーションセットがリリースされると、以前の新しいアプリケーションセットは新しいものとして認識されなくなり、アプリケーションフィルタはそれらと一致しなくなります。アプリケーションと脅威に関するコンテンツアップデートのベストプラクティスに従い、次回のアプリケーションコンテンツアップデートの前に新しいアプリケーションの処理方法を決定してください。
- 移行シナリオでは、アプリケーションフィルタを使用して特定の種類のアプリケーションを幅広くブロックまたは許可し、次にポリシーオプティマイザを使用してネットワーク上で必要なアプリケーションのみに絞り込みます。アプリケーションフィルターを使用すると、特定のタイプの新しいアプリケーションがフィルターに一致したときに自動的に許可されるようにすることもできます。

- 新しいアプリケーションがフィルターに一致すると自動的に処理されるため、将来性のあるルールを作成できます。これは、移行や新規デプロイのアプリケーション発見フェーズでも、成熟した環境でも役立ちます。

  たとえば、**Palo Alto Networks** タグに基づくアプリケーションフィルターを使用して許可ルールを作成します。これにより、現在のすべての Palo Alto Networks のアプリケーションと今後のすべての Palo Alto Networks のアプリケーションを許可することが保証されます。

  もう 1 つの例として、コンテンツ配信の新しいアプリ ID をフィルタリングするルールを作成して、より綿密に調査できるようになるまで安全に処理します。

8. アプリケーション定義は静的ではありません。アプリケーションのコンテンツを更新すると、アプリケーションの定義が変更され、したがってルールによるアプリケーションの処理方法が変わる可能性があります。アプリケーションコンテンツ更新のベストプラクティスに従い、更新に伴って必要な変更を行う時間を確保してください。

Web サイトへのアクセス (URL フィルタリング)

高度な URL フィルタリングにはライセンスが必要です。PAN-OS、Prisma Access (通常はPrisma Accessライセンスに含まれています)、およびクラウドNGFW for AWSで高度なURLフィルタリングを使用してください。

Web サイトのカテゴリに基づく URL フィルタリングは、送信セキュリティ ポリシーを簡素化し、悪意のある Web サイトからユーザーを保護します。各 URL カテゴリは、同じ種類のコンテンツを含むサイトのグループを定義します。たとえば、医療・医療サイト、ゲームサイト、ハッキングサイトなどです。また、特定のカテゴリ内のサイトの相対リスクレベルを定義するカテゴリには、低リスク、中リスク、高リスクの3つのカテゴリがあります。カテゴリとリスクレベルを組み合わせると、URL カテゴリ内のリスクに基づいてトラフィックをブロックまたは許可するセキュリティ ポリシー ルールを作成できます。

URL フィルタリングを利用するには、復号化を有効にする必要があります。トラフィックを復号化して正確な *URL* を表示し、ファイアウォールが適切なアクションを実行できるようにする必要があるためです。少なくとも、高リスクおよび中リスクのトラフィックを復号化します。

STEP 1 | URL カテゴリでは危険なトラフィックを簡単に識別できるため、URL カテゴリに基づいて復号するトラフィックをターゲットにします。

最もリスクの高いURLカテゴリを最初に復号化し、経験を積むにつれてより多くのトラフィックを復号化します。

STEP 2 | アウトバウンドインターネットトラフィックを制御するセキュリティ ポリシー ルールでは、

- URL フィルタリングプロファイルを添付して、セキュリティ ポリシーを簡素化します。悪意のある Web サイトのすべてのカテゴリ（サイトアクセスとユーザー認証情報の送信の両方）をブロックし、その他すべてのカテゴリのアラートをブロックするベストプラク

ティスの URL フィルタリングプロファイルを設定し、Web アクセスを許可するすべてのルールに添付します。

- 法律、コンプライアンス、ビジネス、プライバシー、規制、その他の理由で復号できないトラフィックを URL カテゴリで制御します。たとえば、適切なユーザーとアプリケーションを使用して、適切なカテゴリを一致条件として指定し、ルールに一致するトラフィックを復号化しないセキュリティ ポリシー ルールを作成します。
- URL フィルタリングベースのセキュリティ ポリシー ルールに例外を作成できるように、カスタム URL カテゴリを設定します。カスタム URL カテゴリを URL フィルタリングプロファイルに追加して適切なセキュリティ ポリシー ルールに添付するか、カスタムカテゴリをセキュリティ ポリシーの一致条件として使用します。例外を設定すると、ほとんどのユーザーの URL カテゴリへのアクセスをブロックし、PEN テスターや infosec などの特定のユーザーには許可したり、ソーシャルネットワーキングなどのカテゴリ全体をブロックして LinkedIn へのアクセスを許可したり、復号化する対象を制御したりできます。以下に例を示します。
  - URL カテゴリとリスクベースのカテゴリを一致条件として組み合わせて、URL カテゴリのトラフィックをリスクに基づいてブロックまたは許可します。たとえば、危険な金融サイトへのアクセスをブロックするには、金融サービス URL カテゴリと 高リスクカテゴリの両方を一致条件として指定するセキュリティ ポリシー ルールを作成し、ルール **[アクション]** を **[拒否]** に設定します。このルールは、金融サービス URL カテゴリへのアクセスを許可するルールの上に配置して、ファイアウォールが中リスクおよび低リスクのサイトへのアクセスを許可する前にリスクの高いサイトをブロックするようにします。
  - ファイアウォールリソースの可用性により、合法的に復号化できるトラフィックやビジネス目的で復号化できるすべてのトラフィックを復号化できない場合は、カスタム URL カテゴリを使用して、復号化してもほとんど価値のない低リスクのトラフィックに一致するセキュリティ ポリシー ルールを作成します。たとえば、低リスクのストリーミングサービスの復号化をバイパスするには、ストリーミングメディア URL カテゴリと低リスクカテゴリの両方を一致条件として指定するセキュリティ ポリシー ルールを作成し、ルール **[アクション]** を **[許可]** に設定します。トラフィックが TLSv1.2 以前を使用している場合は、トラフィックの復号化なしポリシーとプロファイルを作成して、不正なセッションをブロックします。トラフィックが TLSv1.3 以降を使用している場合は、トラフィックの復号化禁止ポリシーとプロファイルを作成しないでください。
- セキュリティ ポリシー ルールのソースゾーンを保護された内部ネットワーク (トラストゾーン) に設定します。URL フィルタリングはアウトバウンド トラフィックにのみ適用するため、外部ゾーンや任意のゾーンをソースとして指定しないでください。（インバウンド トラフィックにURLフィルタリングを適用すると、DoS攻撃につながる可能性さえあります）。

STEP 3 | URL フィルタリングプロファイルをベストプラクティス設定に安全に移行し、ベストプラクティスの URL フィルタリングプロファイル:を作成するには

1. デフォルトの URL フィルタリングプロファイル (**default** という名前) を複製して編集します。
2. プロファイルの名前を適切に変更します (例:ベストプラクティス URL フィルタリングプロファイル)。
3. URL カテゴリのすべてのアクションを、サイトアクセスとユーザー認証情報の送信の両方でアラートするように設定します。(デフォルトの許可アクションではログは生成されません)。 ログを生成してトラフィックを可視化するには、アラートを生成する URL カテゴリを手動で設定する必要があります。

   URL フィルタリングに新しいカテゴリが追加されると、デフォルトでは、そのカテゴリはサイトアクセスとユーザー認証情報の送信を許可するように設定されます。サイトアクセスとユーザー認証情報の送信時にアラートを送信するように新しいカテゴリを手動で設定し、*URL*フィルタリングログを取得します。また、カスタム *URL* カテゴリも適宜更新してください。

4. 悪意のある URL カテゴリに対するすべてのアクションを設定して、サイトアクセスとユーザー認証情報の送信の両方をブロックします。PENテスト、脅威調査、情報セキュリティについては、必要に応じて適切な例外を設けてください。
   - コマンドアンドコントロール — マルウェアや侵害されたシステムが攻撃者のリモートサーバーとの通信に使用する URL とドメイン。
   - グレーウェア — これらのサイトは、ウイルスの定義を満たしておらず、直接的なセキュリティ上の脅威にもなりませんが、ユーザーに影響を与えてリモートアクセスを許可したり、その他の不正な操作を実行したりします。グレーウェアサイトには、詐欺、違法行為、犯罪行為、アドウェア、およびその他の望ましくないアプリケーションや一方的なアプリケーション（「タイポスクワッティング」ドメインを含む）が含まれます。
   - マルウェア — マルウェアをホストしていることが分かっている、あるいはコマンド アンド コントロール（C2）トラフィックに使用されているサイト。
   - フィッシング — テクニカルサポート詐欺やスケアウェアなど、資格情報や個人情報のフィッシングページをホストすることが知られているサイト。
   - ランサムウェア — ランサムウェアを配布することが知られているサイト。
   - スキャンアクティビティ — 既存の脆弱性を調査したり、標的を絞った攻撃を行ったりします。
5. URL カテゴリの中には、悪質である可能性が非常に高いものの、必ずしも悪質ではないものもあります。これらの URL カテゴリのすべてのアクションを、サイト アクセスとユー

ザー資格情報の送信の両方をブロックするように設定します。PENテスト、脅威調査、情報セキュリティについては、必要に応じて適切な例外を設けてください。

- ダイナミック-DNS — マルウェアのペイロードやコマンドアンドコントロールマルウェアの配信によく使用される、IP アドレスが動的に割り当てられたシステム。
- ハッキング — 機器やソフトウェアへの違法または疑わしいアクセスや使用に関連するサイト。ライセンスとデジタル著作権システムのバイパスを容易にするサイトも含まれます。

  適切な *PEN* テストおよび脅威研究ユーザーについては、このカテゴリに例外を設けてください。
- 不十分なコンテンツ — テストページを表示したり、コンテンツを表示しなかったり、エンドユーザが表示することを意図していない API アクセスを提供したり、他のコンテンツを表示せずに認証を要求したりするウェブサイトやサービス。
- 新規登録ドメイン — ドメイン生成アルゴリズムが頻繁に生成するドメイン、または悪意のある活動のために悪意のある者が生成するドメイン。
- 未解決 - PAN-DB クラウドに到達できず、URL がファイアウォールの URL フィルタリング キャッシュにない場合、ファイアウォールは URL カテゴリを解決して識別できません。

  最高のセキュリティを実現するには、 カテゴリ検索のクライアント要求を保留する を有効にして、ファイアウォールが *URL* カテゴリを解決するまでの時間を長くします。これにより、ファイアウォールがクラウドからカテゴリ タイプをクエリする時間が延長され、セキュリティは向上しますが、遅延が増加する可能性があります。
- parked — クレデンシャルフィッシングや個人情報の盗難によく使用されるドメイン。
- プロキシ回避およびアノニマイザー — しばしばコンテンツのフィルタリングを回避するのに使用されるURLおよびサービス。
- 不明 - Palo Alto Networks(PAN-DB)で未確認のサイト。

  PAN-DB リアルタイム更新は、未知のサイトへの最初のアクセス試行後に未知のサイトを学習するため、ファイアウォールは未知の *URL* を迅速に識別し、サイトの実際の *URL* カテゴリに基づいてそれらを処理します。

  可用性がビジネスにとって重要であり、未知のサイトからのトラフィックを許可しなければならない場合は、トラフィックに最も厳格なセキュリティ・プロファイルを適用し、そのトラフィックに関するすべてのアラートを調査してください。

6. 法的またはビジネス上の要件および潜在的な責任リスクに基づいて、次の URL カテゴリをブロックするように、サイト アクセスとユーザー認証情報の送信のアクションを設定します。これらのサイトをブロックしない場合は、トラフィックに警告を発し、厳格なセキュリティ プロファイルを適用します。

   - 乱用薬物 - 違法および合法の薬物乱用を助長するサイト。
   - アダルト - ゲームやコミックのほか、性的に露骨な素材、メディア、アート、フォーラム、サービスなど、あらゆる種類のアダルト コンテンツを含むすべてのサイト。
   - 著作権侵害 — 賠償責任のリスクがある違法なコンテンツを含むドメイン。
   - 過激主義 — テロ、人種差別、児童搾取などを助長するウェブサイト
   - ギャンブル — 宝くじやギャンブルのサイト。
   - ピアツーピア — トレント、ダウンロードプログラム、メディアファイル、またはその他のソフトウェアアプリケーションのピアツーピア共有。(シェアウェアやフリーウェアのサイトは含まれません。)
   - いかがわしい — 特定のユーザー層をターゲットにした、趣味の悪いユーモアや攻撃的なコンテンツを宣伝するサイト。
   - 武器 — 武器およびその使用に関する販売、レビュー、説明または指示。

   また、暗号通貨とアルコールとタバコの URL カテゴリをどのように処理するかについても検討してください。ビジネス ニーズに応じて、トラフィックに警告を発して厳格なセキュリティ プロファイルを適用するか、トラフィックをブロックします。
7. 高リスクカテゴリのユーザー認証情報の送信をブロックします。(高リスクカテゴリのサイトアクセスをブロックしないでください。)
8. URL フィルタリングプロファイルの URL フィルタリング設定の場合:

   - ログコンテナページのみを無効にする。これはデフォルトで有効になっています。コンテナ ページのみをログに記録すると、投稿、アップロード、ダウンロードなどの機能的なアプリケーションが見えなくなります。完全なログを表示するには、ログ コンテナ ページのみを無効にして、実際に機能するアプリケーションを確認します。
   - ご使用の環境が連邦政府の資金を受け取っている学校の場合は、 セーフ サーチの強制 (法的要件) を有効にします。
9. ユーザー認証情報の検出を有効にします (User-ID の設定と有効化が必要です)。

STEP 4 | スパイウェア対策セキュリティ プロファイルで DNS シンクホールが設定されているセキュリティ ポリシー ルールに URL フィルタリングを適用して (クラウドベースの DNS セキュリティを使用するには、Advanced Threat Protection またはアクティブなレガシー Threat Protection サブスクリプション、および DNS セキュリティサブスクリプションが必要)、どのマシンが感染しているか、どこで DNS に接続しようとしていたかを確認します。

ポリシーアクションとその他の設定

セキュリティ ポリシーアクションでは、トラフィックを許可するかブロックするか、許可しないトラフィックをどのようにブロックするかを指定します。Quality of Service（QoS）は必要に応じて帯域幅を制御し、ルールで許可されるトラフィックが適切な帯域幅を受け取るようにします。

STEP 1 | セキュリティ ポリシー ルールごとにアクションを定義します。

- 許可され許容されるトラフィックのみを許可してください。ビジネスに関係のないトラフィックを許可すればするほど、リスクは大きくなります。ファイアウォールは、セキュリティ ポリシー ルールで明示的に許可されていないトラフィックをブロックします。
- セキュリティ ポリシー ルールが最小権限アクセスの原則に従えば従うほど、必要なブロックルールは少なくなります。トラフィックをブロックする方法は、ブロックするアプリケーションへの対応方法によって異なります。
  - クライアント、サーバー、あるいはその両方をリセットしたり、トラフィックをサイレントドロップしたりして、ファイアウォールが特定の方法でアプリケーションに応答するようにしたい場合を除いて、アプリケーションのデフォルトアクションを使用する [拒否] を使用してください。
  - リセットレスポンスを送信せずにサイレントにサービスを拒否したい場合は **Drop** を使用してください。定義済みのPalo Alto Networks EDLに基づいてブロックするなど、明らかに悪意のあるトラフィックをブロックする場合、ドロップアクションにより、通信の悪意のある側がブロックされた理由を知ることができなくなります。
  - クライアントのみまたはサーバーのみをリセットするユースケースがある場合は、ルールの送信元と宛先の設定に基づくクライアントとサーバーの方向性 (通信のどちら側が接続を開始するか) を理解していることを確認してください。

STEP 2 | 必要に応じて、QoS を適用して特定のアプリケーションの帯域幅を制御します。

QoS はオプションです。帯域幅に関して優先順位を付けたいアプリケーションと、ポリシーにQoSを適用する場合に帯域幅を制限したいアプリケーションを理解してください。たとえば、特定のストリーミングアプリケーションを使用するワールドカップなどの人気のイベントでは、従業員がそれらのアプリケーションを使用してイベントを視聴できるようにし、帯域幅を制限してビジネス活動に適した帯域幅を確保できます。もう 1 つの例として、一般的なアプリケーションのアップデートがリリースされると、大量ダウンロードによって帯域幅の可用性が影響を受けることがあります。これを防ぐには、QoS を適用して、そのアプリケーションのダウンロードトラフィックに使用できる帯域幅を制限します。

ロギングとログ転送

インシデントを調査するには、ログを記録して保存することが重要です。コミュニケーション:

- セキュリティオペレーションセンター (SOC) は、必要に応じてイベントを調査するための適切な情報を収集できるようにします。

- 監査コンプライアンスチームが、監査とコンプライアンスのための適切な情報を確実に収集できるようにします。
- 法務チームは、現地の規制、コンプライアンス、ビジネス要件、プライバシーなどに違反する平文やその他のデータを保存しないようにします。

STEP 1 | 現在および将来必要となるログストレージ容量を検討し、それに応じてログストレージ容量を決定してください。

- 脅威を調査するのに十分な期間ログを保持できるように、ストレージ容量を計画してください。所要時間は調査手順によって異なります。
- SOC が保存されている場所を問わずログを取り込めるようにしてください。Cortex Data Lake (CDL) は、ログの保存と分析を一元化し、ログの量に合わせて拡張できるソリューションを提供します。
- 同じログを複数の場所に複製して保存しないでください。CDL またはログコレクターなどの別のストレージスペースを使用してください。ログをあるストレージスペースから別のストレージスペースに移動するときは、複製を使用しないでください。代わりに、ハードカットオーバーに備えて実行してください。

  ファイアウォールまたは *Panorama* で重複ログ転送を有効にすると、システムログと構成ログは *CDL* に送信されないため、*CDL* ログは不完全になります。このため、ログバックアップでは重複ログ転送を有効にしないでください。

  ログストレージを分割する必要がある場合は、ログ転送を一貫性のある方法で分離してください。たとえば、すべての*Prisma*アクセスログを*CDL*に送信し、すべてのファイアウォールログをログコレクターに送信します。

STEP 2 | 何を記録したいのか、どのように記録したいのか、コンプライアンスやストレージ容量上の理由で記録したくないものや記録できないものを考えてください。

ほとんどのアプリケーションでは、セキュリティオペレーションセンター (SOC) の調査に役立つ情報をすべて記録してください。ただし、包括的なログを取得できないアプリケーションや状況もあります。

- コンプライアンス、ビジネス要件、ISO などの監査要件、プライバシーに関する考慮事項 (PII、GDPR など)、および SOC 要件に基づいて、ルールにロギングが必要かどうかを評価します。SSN、認証情報、PII などをアプリケーションで暗号化しない場合は、SSN、認証情報、PII などをクリアテキストで記録しないように注意してください。
- DNS、NTP、Syslogなどの基本的なサービスでは、何千もの小さなセッションが作成され、その結果、不要なログが多数生成されます。これはログストレージに影響を与え、インシデントの調査をより困難にします。これらのサービスでは、他のログを取得するストレージ容量がない限り、脅威ログの転送のみを設定します。

STEP 3 | セキュリティ ポリシー ルールでは、一時的なアプリケーションをログに記録しないように、セッションの開始時ではなく終了時にトラフィックを記録します。

Log At Session Start (セッション開始時にログに記録**)** は、セッション終了時にのみログを記録するよりも多くのリソースを消費します。ほとんどの場合、**Log At Session End** のみになります。**Log At Session Start** と **Log At Session End** の両方を有効にするのは、アプリケーションがセキュリティ ポリシー ルールに一致しない理由のトラブルシューティング、GRE トンネルなどのアクティブで長期間有効なトンネルセッションの表示（セッションの開始時にログインしない限り ACC ではこれらのセッションは表示されない）、および同じく長期間有効なセッションであるオペレーショナルテクノロジー/産業用制御システム（OT/ICS）セッションを可視化する場合に限ります。

ポリシーオプティマイザと *Cloud App-ID Engine (ACE)* は、セッション開始時にログを記録するルールを統計にカウントしません。

STEP 4 | ゾーン内のすべてのトラフィックをデフォルトで許可するゾーン内デフォルトルールと、セキュリティ ポリシー ルールがデフォルトで明示的に許可していないゾーン間のすべてのトラフィックをブロックするインターゾーン間拒否ルールに一致するトラフィックをログに記録します。

STEP 5 | ログ転送プロファイルを設定してセキュリティ ポリシー ルールに割り当てて、CDL やログコレクターなどの適切なストレージにログを送信し、イベント、特に重大、高、中程度の脅威イベントについて適切な管理者に警告します。

クラウドマネージド *Prisma Access* は、すべてのログを *CDL* に転送します。

- すべてのセキュリティ ポリシー ルールにログ転送プロファイルが添付されていることを確認してください。

  すべての新しいセキュリティ ポリシー ルール用の基本的なデフォルトログ転送プロファイルを作成し、デフォルトという名前を付けて脅威を記録するようにします。プロファイルに **`default`** という名前を付けると、ファイアウォールはそのプロファイルをすべての新しいセキュリティ ポリシー ルールに自動的に適用するため、すべての新しいルールにログ転送プロファイルが割り当てられます。

  コンプライアンス、個人情報、地域の規制、ビジネス要件などに関連するトラフィックのログや、DNS や NTP などの一般的なサービスのログなど、異なるログ処理を必要とする

いくつかのルールのプロファイルを置き換えたり変更したりする方が、新しいルールごとに個別にログ転送プロファイルを添付するよりも簡単です。

> *IoT Security* を管理するセキュリティ ポリシー ルールには、***IoT Security*** のデフォルトプロファイル-***EAL*** 対応の事前定義済みログ転送プロファイルを使用してください。これにより、拡張アプリケーションログを含め、必要なすべてのログタイプが *IoT Security* に提供されます。

- ポリシーオプティマイザーのセキュリティサービスのログ転送を使用して、ログ転送プロファイルがアタッチされていないセキュリティ ポリシー ルールを特定します (フィルタで [なし] を選択します)。ログ転送プロファイルがない各ルールに、適切なログ転送プロファイルを追加します。

STEP 6 | 調査の目的で、トラフィックの真の送信元と宛先がわかっていることを確認してください。ロードバランサー、NAT デバイス、または実際の送信元とファイアウォールの間にある悪意のある DNS サーバーなどのプロキシデバイスの IP アドレスだけではありません。ファイアウォールと実際のソースの間にプロキシデバイスがある場合は、ネットワークアーキテクチャとアプリケーションによって異なります。

- ロードバランサーの前にファイアウォールを配置して、実際の送信元 IP アドレスを確認します。
- パケットキャプチャ設定で受信ステージを設定して、NAT 以前のパケットキャプチャを行います。
- X-Forwarded-For (XFF) フィールドを記録できるようにする URL フィルタリングプロファイルをセキュリティ ポリシー ルール (オブジェクト > プロファイル > **URL** フィルタリング > **URL** フィルタリング設定) に適用します。XFF フィールドには、元の送信元 IP アドレスが表示されます。XFF ログは URL フィルタリングログにあります。

セキュリティ プロファイル

セキュリティ プロファイルは、許可されたトラフィックをスキャンして、ウイルス、マルウェア、スパイウェア、悪意のあるファイルタイプ、その他の既知および未知の脅威などの脅威を検出し、それらの脅威を防止します。セキュリティ プロファイルをセキュリティ ポリシー ルールにアタッチして、トラフィックがルールに一致するトラフィックに脅威防止を適用できるようにします。

Day 1 Configurationsは、ユースケースにとらわれないベストプラクティスを提供するテンプレートで、許可されたトラフィックを正しく設定するためのセキュリティ プロファイルを作成してください。Day 1 構成はカスタマーサポートポータル (**Tools** > **Run Day 1 Configuration**) で利用可能で、サポートへのログインが必要です。そこから、ここで説明する脅威ブロッキングのベストプラクティスに移行してください。

脅威を特定して防止するには、ファイアウォールがアプリケーショントラフィックを可視化する必要があります。地域の規制、ビジネス上の考慮事項、プライバシー上の考慮事項、および技術的能力が許す限り、トラフィックを復号化します。SSLフォワード プロキシ *(*アウトバウンド*)* 復号化の場合、最初にユーザー *ID* と *URL*フィルタリングを実装して、効果的に復号化をターゲットにできるようにします。トラフィックを復号化しないと、ファイアウォールは暗号化されたヘッダーとペイロード情報を分析できません。

さらに、脅威コンテンツアップデートのベストプラクティスに従って、セキュリティ プロファイルのシグネチャが最新のものであることを確認してください。

Advanced Threat Prevention (高度な脅威防御)クラウドサービスのサブスクリプションを利用すると、未知のコマンドアンドコントロールやゼロデイ脆弱性の脅威などの脅威をリアルタイムで防止できます。高度な脅威防止機能は、PAN-OS、Prisma Access 3.2イノベーション、およびそれ以降のイノベーション導入で利用できます。Prisma Accessの以前のバージョンを実行している場合は、通常の脅威防止サブスクリプションを使用してください。

*Advanced Threat Prevention*はクラウドサービスであり、クラウド接続が必要なため、エアギャップ環境では使用できません。

クラウドマネージドPrisma Accessのベストプラクティス セキュリティ プロファイルの推奨事項は、*PAN-OS*および*Panorama Managed Prisma Access*の推奨事項とは若干異なります。さらに、*Cloud Managed Prisma Access*では、個々のセキュリティ プロファイルをセキュリティ ポリシー ルールに適用することはできません。適用できるのはプロファイルグループのみです。プロファイルグループには、グループに含めるセキュリティ プロファイルが含まれます。

ベストプラクティスのアドバイスは、最も安全を確保するために何をすべきかに焦点を当てており、それがセキュリティ プロファイルの究極の目標です。ただし、ビジネスクリティカルなアプリケーションの可用性を確保するには、既知の悪意のあるトラフィックをブロックし、他のほとんどのトラフィックについて警告することから始めます。ベストプラクティスのセキュリティ プロファイル移行アドバイスに従って、トラフィックをブロックするセキュリティ プロファイルに安全にアラートからベストプラクティスに移行してください。アラートからブロッキングに移行するときは、ビジネスクリティカルなアプリケーションに影響を与えないように注意してください。

セキュリティ プロファイル設定をアラートからブロックに移行するタイミングは、プロファイルが適切に調整され、必要な例外をすべて設定し、ビジネスに不可欠なアプリケーションをブロックするシグネチャを誤ってトリガーすることがないことを確認するときです。

この簡略化されたセクションでは、ベストプラクティスの設定について説明します。「ベスト・プラクティス・セキュリティ・プロファイルの作成」では、設定の理由に関するより詳細な情報が提供されています。

- アンチウイルスプロファイル (WildFire シグネチャとインライン機械学習アクションを含む)
- アンチスパイウェア プロファイル (DNS ポリシー/シンクホールとインラインクラウド分析を含む)

  広範囲をカバーするには、*Advanced URL Filtering*サブスクリプションと*DNS*セキュリティサブスクリプションを購入して、悪意のある*URL*、ドメイン、*DNS*プロトコルの悪用を可視化して保護してください。
- 脆弱性保護プロファイル (インラインクラウド分析を含む)
- ファイル ブロッキング プロファイル
- WildFire 分析プロファイル

STEP 1 | アンチウイルスプロファイルをベストプラクティス設定に安全に移行したら、定義済みのデフォルトのアンチウイルスプロファイルを複製して名前を変更し、編集します。

アンチウイルスプロファイルをベストプラクティスプロファイルに安全に移行するには:

1. 誤検知はまれです。ビジネスにとって重要ではないアプリケーションには、ベストプラクティスのウイルス対策プロファイルをすぐに導入できます。
2. ビジネスクリティカルなアプリケーションについては、重要なアプリケーションの可用性に影響を与えないようにアラートを出すことから始めてください。アンチウイルスプロファイルがこれらのアプリケーションをブロックしないことに不安を感じたら、ブロッキングに移行してください。
3. 既存のデプロイメントがある場合や移行中であり、既存のブロックが存在する場合は、トラフィックとそれをブロックする理由をすでに理解しているため、それを複製してください。
4. 内部アプリケーションを外部アプリケーションとは異なる方法で扱う場合は、インターネットに接続されたトラフィック用のウイルス対策プロファイルと、内部トラフィック用の別のウイルス対策プロファイルが必要になる場合があります。

脅威ログを監視して、ビジネスに不可欠なアプリケーションがアラートやブロックの原因となっているかどうかを確認します。Advanced WildFire またはレガシー WildFire サブスクリプションをお持ちの場合は、WildFire 送信ログを監視し、WildFire アクション設定を使用してください。

ベストプラクティスのウイルス対策プロファイルは、既知のマルウェア、ウイルス、ランサムウェアボットをブロックします。

- リアルタイム シグネチャ検索をデバイスおよびウイルス対策プロファイルでグローバルに有効にして、ファイアウォールがクラウドから最新のリアルタイム アンチウイルス シグネチャを受信するまでファイルを保持します。
  - **[デバイス > セットアップ >] [コンテンツ ID] [> コンテンツ ID 設定] > [リアルタイムシグネチャ検索]、[WildFire** リアルタイムシグネチャ検索**]** の [保留] を グローバルに有効にし、**[**リアルタイムシグネチャタイムアウト時のアクション**]** を **[**両方をリセット**]**に設

定します。アンチウイルスプロファイルで有効にするには、リアルタイムシグネチャ検索をグローバルに有効にする必要があります。

- [アンチウイルスプロファイルで有効にする]:[オブジェクト > セキュリティプロ ファイル > アンチウイルス]を選択し、[**Hold for WildFire Real Time Signature Look Up**]を有効にします。

ファイルを保持して WildFire が最新のアンチウイルス シグネチャを取得できるようにすることで、最新のシグネチャを保持せずにファイルを転送した場合に危険にさらされる可能性があるゼロデイ マルウェアや古いアンチウイルス シグネチャから保護します。

- ファイアウォールが特定のプロトコルでウイルスを検出したときに実行するアクションを設定します。最も安全な方法は、クライアントとサーバーの両方をリセットして、セッションを確実に終了させることです。
  - デフォルトのアクションがアラートであるsmtp、pop3、imapプロトコルのシグネチャアクションを**reset-both (**両方リセット**)**に変更します。他のプロトコルのシグネチャ アクションは **reset-both (**両方リセット**)** のままにしておきます。
  - デフォルトのアクションがアラートであるsmtp、pop3、imapプロトコルの**WildFire** シグネチャ アクションを**reset-both (**両方リセット**)**に変更します。他のプロトコルの **WildFire** シグニチャアクションは **reset-both** のままにしておきます。
  - デフォルトのアクションがアラートであるsmtp、pop3、imapプロトコルの**WildFire** インライン **ML**を**reset-both (**両方リセット**)**に変更します。他のプロトコルの **WildFire** インライン **ML** は**reset-both (**両方リセット**)** のままにしておきます。

すべての許可ルールにベストプラクティスプロファイルを添付します。

WildFire シグネチャアクションと *WildFire* インライン *ML* アクションを設定するには、*WildFire* サブスクリプションが必要です。

クラウドマネージド*Prisma Access*では、アンチウイルスと*WildFire*が別々のプロファイルではなく、*1*つのプロファイルにまとめられます。

STEP 2 | アンチスパイウェアプロファイルをベストプラクティス設定に安全に移行したら、定義済みのデフォルトのアンチスパイウェアプロファイルを複製して名前を変更し、編集します。アンチスパイウェア署名ポリシーに加えて、プロファイルは DNS シンクホールポリシーも制御します。

アンチスパイウェアプロファイルをシグネチャポリシーのベストプラクティスプロファイルに安全に移行するには：

1. 誤検知は比較的まれです。ビジネスにとって重要ではないアプリケーションでは、critical(重要)とhigh(高)のシグネチャを最初からブロックします。
2. 中程度に危険なシグネチャはフォルスポジティブを生じさせる可能性があり、初期のモニタリングが必要です。内部トラフィックでは重大度が中程度のシグネチャではアラートを出し、外部に向いているトラフィックでは重大度が中程度のシグネチャをブロックしま

す。脅威ログ（**Monitor Logs > Threat**）を監視して、アラートを受信したアプリケーションをブロックできるかどうか、または許可する必要があるかどうかを確認します。

3. ビジネスクリティカルなアプリケーションの場合は、アクションをアラートに設定して、アプリケーションの可用性を確保します。ただし、クリティカル、ハイ、ミディアムのシグネチャをブロックするスパイウェア対策プロファイルですでにアプリケーションを保護していて、そのプロファイルがビジネスやセキュリティのニーズを満たしていると確信できる場合は、同様のプロファイルを使用してスパイウェアをブロックし、それらのアプリケーションを保護してください。
4. 移行中は、すべての重要度シグネチャの単一パケットキャプチャを有効にして、リソースに余裕があれば必要に応じてイベントをより詳細に調査できるようにします。ベストプラクティスプロファイルに移行する際、low(低)やinformational(情報)のイベントが（トラフィック量が多すぎて）膨大なパケットキャプチャーアクティビティを生成し、有効な情報が十分でない場合、重大度でパケットキャプチャを無効にすることができます。

   パケットキャプチャは管理プレーンのリソースを消費します。パケットキャプチャを実装する前後にシステムリソース *(*ダッシュボード > システムリソースなど*)* を確認して使用状況を把握し、システムにすべてのパケットキャプチャを実行するのに十分なリソースがあることを確認します。
5. ベストプラクティスの完全なスパイウェア対策プロファイルを実装する前に、必要に応じて例外を作成して誤検出が確認された場合は修正します。

内部アプリケーションを外部アプリケーションと異なる方法で扱う場合は、インターネットに直接接続するトラフィックにはスパイウェア対策プロファイルを、内部トラフィックには別のアンチスパイウェアプロファイルが必要になる場合があります。

ブロックしているトラフィックについて確信が持てたらすぐに、プロファイルの **DNS** ポリシーをベストプラクティスに移行してください。

- DNS シグネチャのポリシーアクションをシンクホールに設定し、疑わしいドメインへのアクセスを試みる可能性のあるホストを追跡してそれらのドメインへのアクセスを阻止することで、疑わしいドメインへのアクセスを試みる可能性のあるホストを特定します。パケットキャプチャを拡張キャプチャに設定します。

  PAN-OS システムでは、*DNS* シンクホールアドレスを *FQDN*（*sinkhole.paloaltonetworks.com* など）として設定します。これにより、*IP* アドレスが変更されても設定は引き続き有効になります。*Prisma* アクセスには、シンクホール *IP* アドレスを使用してください。
- すべての **DNS** セキュリティドメインタイプをシンクホールし、コマンドアンドコントロールドメインでは **Packet Capture (** パケット キャプチャ**)** を **extended-capture (**拡張キャプチャ**)** に、パークドメイン (PAN-OS 10.0 以降) を除く他のすべてのドメインタイプでは [シングルパケット] に設定します。

- DNS 解決プロセス中にクライアントが client hello を暗号化できないように、暗号化された DNS クエリで使用されるすべての DNS レコードタイプをブロックします。

プロファイルのインラインクラウド分析（Advanced Threat Preventionサブスクリプションとの PAN-OS 10.2以降が必要）を、すべてのアウトバウンド トラフィックのクラウドインライン分析を有効にするに設定します。すべてのモデルで アクション を リセット **(**両方**)** に設定します。

Transition Anti-Spyware プロファイルで、トラフィックをブロックし、ビジネスニーズを満たす既存のスパイウェア対策コントロールがある場合は、トラフィックとブロックする理由をすでに理解しているので、それらのコントロールをすぐに実装してください。

ベストプラクティスのスパイウェア対策プロファイルは、コマンドアンドコントロール (C2) トラフィックを検出し、侵害されたシステムがアウトバウンド接続を確立するのを防ぎ、DNS シンクホールによって感染したホストを特定できるようにします。GlobalProtectを使用すると、PAN-OSとパノラママネージドプリズマアクセスで侵害されたデバイスを自動的に隔離できます。また、クラウドマネージドプリズマアクセスで侵害されたデバイスを隔離することもできます。

署名ポリシーの場合:

1. Critical、High、Mediumの深刻度の**Action (**アクション**)**を**reset-both (**両方リセット**)**に設定し、**packet-capture (**パケットキャプチャ**)**を**single-packet (**単一パケット**)**に設定する。
2. 低重度と情報重要度の**Action (**アクション**)**をデフォルトに設定し、**packet-capture (**パケットキャプチャ**)**を無効にする。

DNS ポリシーについては、移行期間に推奨されているものと同じ設定を使用してください。すべてのシグネチャソースのポリシーアクションをシンクホールに設定し、**Palo Alto Networks**のコンテンツドメインとコマンドアンドコントロールドメインのパケットキャプチャを拡張キャプチャに設定し、パークドメインを除く他のすべてのDNSセキュリティドメインのパケットキャプチャを単一のパケットに設定します。

インラインクラウド分析のベストプラクティス設定は、移行設定と同じです。すべてのアウトバウンド トラフィックでこの機能を有効にし、アクションを **reset-both (**両方リセット**)** に設定します。

DNS セキュリティサービスを使用して、高度な DNS ベースの脅威からユーザーを保護してください (DNS セキュリティライセンスと高度な脅威対策、または有効な従来の脅威防止サブスクリプションが必要です)。

すべての許可ルールにベストプラクティスプロファイルを添付します。

STEP 3 | 脆弱性保護プロファイルをベストプラクティス設定に安全に移行したら、定義済みの厳格な脆弱性保護プロファイルを複製して名前を変更し、編集します。

脆弱性保護プロファイルは、バッファオーバーフロー、不正なコード実行、およびクライアント側とサーバー側の脆弱性を悪用するその他の試みを防ぎます。脆弱性保護プロファイルをベストプラクティスプロファイルに安全に移行するには：

1. 誤検知は低いです。ビジネスにとって重要ではないアプリケーションのルールを設定して、すぐにブロック（両方リセット）できます。
2. ビジネスクリティカルなアプリケーションについては、重要なアプリケーションの可用性に影響を与えないようにアラートを出すことから始めてください。脆弱性保護プロファイルがこれらのアプリケーションをブロックしないことに不安を感じたら、ブロッキングに移行してください。
3. 既存のデプロイメントがある場合や移行中であり、既存のブロックが存在する場合は、トラフィックとそれをブロックする理由をすでに理解しているため、それを複製してください。
4. 重大度（クリティカル、高、中）のブルートフォースカテゴリにシグネチャを設定してアラートを発信し、ブロッキングに問題なく移行できるようになるまで微調整します。パケットキャプチャを拡張キャプチャに設定します。
5. クリティカルなルールと重要度の高いルールのシグネチャを設定して両方リセットし、パケットキャプチャを単一パケットに設定します。
6. 重大度が中程度のルールにはアラートを設定し、パケットキャプチャを拡張キャプチャに設定します。
7. 重要度が低いルールや情報レベルのルールのシグニチャをデフォルトに設定し、パケットキャプチャを単一パケットに設定します。
8. インラインクラウド分析では、初期の脆弱性防御ルールに使用するのと同じ基準をアラートとビジネスアプリケーションのブロックに使用します。既存の統制がある場合は、それらを複製してトラフィックをブロックします。新しいコントロールの場合は、ブロックに

移行する前に少なくとも 1 週間アラートを行います。できるだけ早くブロックに移行します。

パケットキャプチャは管理プレーンのリソースを消費します。パケットキャプチャを実装する前後にシステムリソース *(*ダッシュボード > システムリソースなど*)* を確認して使用状況を把握し、十分なリソースがあることを確認します。

脅威ログを監視して、ビジネスに不可欠なアプリケーションがアラートやブロックの原因となっているかどうかを確認します。WildFire サブスクリプションをお持ちの場合は、WildFire 送信ログを監視し、WildFire アクションを使用してください。

ベストプラクティスの脆弱性保護プロファイルは、クリティカル、高、中、低、および情報イベントにおけるクライアント側およびサーバー側の脆弱性の処理方法を制御します。プロファイルで、次の 6 つのルールを設定します。

1. 移行プロファイルでブルートフォース攻撃を防ぐ同じ3つのルールを作成し、アクションを**reset-both (**両方リセット**)** に、パケットキャプチャをシングルパケットに設定します。
2. simple-client-critical、simple-client-high、simple-client-medium、simple-server-critical、simple-server-high、simple-server-lowの重大度を1つのルールにまとめます。**[Action]** を **[reset-both]** に設定し、**[Packet Capture]** を **[single-packet]**に設定します。

   内部 *(*東西*)* トラフィックを制御するプロファイルの場合、中程度の重大度のイベントをブロックすると、ビジネス アプリケーションに影響を与える可能性があります。ブロックがビジネス アプリケーションに影響を与える場合は、***[***アクション***]*** を ***[alert]***に設定して、中程度の重大度のイベント用の別のルールをプロファイルに作成します。このプロファイルは内部トラフィックにのみ適用してください。
3. simple-client-lowおよびsimple-server-lowの深刻度では、アクションをデフォルトに設定し、パケットキャプチャを単一キャプチャに設定します。
4. simple-client-informationalとsimple-server-informationalの深刻度では、アクションをデフォルトに設定し、パケットキャプチャを無効にします。（情報アクティビティによって比較的大量のパケットキャプチャトラフィックが生成される場合がありますが、これは潜在的な脅威となるパケットキャプチャと比較して特に有用ではありません。）
5. インライン・クラウド分析のアクションを**reset-both (**両方リセット**)**に設定する。

脆弱性保護プロファイルをより詳細に制御し、特定のユースケースに合わせて脆弱性保護を微調整するには、クライアント側とサーバー側の両方の検出について、重要度ごとに個別のルールをプロファイル内に作成します。アクションとパケットキャプチャの設定が同じ場合は、設定を簡略化するためにこれらを 1 つのルールにまとめるのが理にかなっています。

すべての許可ルールにベストプラクティスプロファイルを添付します。

STEP 4 | ファイルブロックプロファイルを、警告から、潜在的に悪意のあるすべてのファイルタイプをブロックするように移行します。

*Cloud Managed Prisma Access*は、セキュリティ ポリシー ルールのファイルブロックプロファイルをサポートしていません。

ファイルブロックプロファイルは、サイバー攻撃に使用される潜在的に悪意のあるファイルタイプをブロックします。ファイルブロッキングプロファイルをベストプラクティス設定からベストプラクティスプロファイルに安全に移行するには：

- ビジネスに不可欠なアプリケーションについては、すべてのファイルタイプについて警告し、できるだけ早く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に移行してください。ブロック制御をすでに導入している場合は、それらを複製して、ブロックしたいことがすでにわかっているトラフィックを引き続きブロックしてください。
- ビジネスクリティカルではないアプリケーションについては、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への移行を開始してください。
  - インバウンドおよびアウトバウンド トラフィック—7z、bat、chm、クラス、cpl、dll、dlp、hta、jar、ocx、pif、scr、トレント、vbe、および wsf ファイルをブロックします。他のすべてのファイルについて警告します。
  - 内部トラフィック — 7z、bat、chm、クラス、cpl、dlp、hta、jar、ocx、pif、scr、トレント、vbe、および wsf ファイルをブロックします (.dll ファイルをブロックする代わりに警告する点を除いて、インバウンド/アウトバウンドプロファイルと同じです)。他のすべてのファイルについて警告します。
  - ビジネス目的でファイルを必要としないユーザーに対して、できる限りすべてのファイル タイプをブロックします: cab、exe、flash、msi、Multi-Level-Encoding、PE、rar、tar、encrypted-rar、および encrypted-zip。

必要に応じて、これらのファイル タイプのいずれかへの正当なビジネス アクセスが必要な *IT* グループやその他のユーザーに対して例外を作成します。他のファイル タイプをすでにブロックしている場合は、引き続きブロックします。

慣れればできるだけ早く、ベストプラクティスのファイル ブロック プロファイルに移行してください。

定義済みの厳格なファイルブロックプロファイルは、サイバー攻撃でよく使用され、アップロードやダウンロードには実際に使用されないファイルタイプをブロックします。ただし、悪意のある目的で使用されるいくつかのプロトコルは、Windows の更新などのアクティビティにも必要になる場合があります。厳密なファイルブロックプロファイル

は、.exe、.dll、.pe、および.cab ファイルをブロックします。Windows アップデートなどの特定のアクティビティのプロトコルを許可する例外を設けるには:

1. ビジネス目的でアクセスする必要があるユーザーと、他のトラフィックでブロックしたいプロトコルを使用するビジネスアプリケーションのみを許可する特定のセキュリティ ポリシー ルールを作成します。
2. 必要なプロトコルを許可するファイルブロックプロファイルをルールに添付します。
3. 他のすべてのトラフィックのプロトコルをブロックするファイル ブロック プロファイルを含むセキュリティ ポリシー ルールの上にルールを配置します。

この方法を使用すると、悪意のある可能性のあるファイルの種類を安全な方法で使用できるようになり、悪意のあるトラフィックをブロックしながらビジネス アプリケーションを有効にすることができます。プロファイルとルールベースを微調整して、必要な例外を許可します。

すべての許可ルールにベストプラクティスプロファイルを添付します。

STEP 5 | ゼロデイマルウェアを検出して防止するためのすべての許可ルールにデフォルトの WildFire Analysis プロファイルを添付します。

リアルタイムのアップデートやその他の高度な機能を入手するには、Advanced WildFireサブスクリプション（PAN-OS 10.0以降）またはWildFireサブスクリプションを入手してください。

ベストプラクティスプロファイルであるデフォルトの WildFire プロファイルを展開します。WildFire はネットワークトラフィックに影響を与えないため、移行期間は必要ありません。（ただし、アンチウイルスプロファイルのベストプラクティスの WildFire Action 設定は、シグニチャを生成するトラフィックに影響し、その結果、リセットやドロップアクションが実行されたり、最新のアンチウイルスシグニチャを検索するために保留になったりします）。 WildFire 分析プロファイルをすべての許可ルールに添付して、すべてのファイルを WildFire に送信して分析します。

クラウドマネージドプリズマアクセスでは、*WildFire*と*Antivirus*が*1*つのプロファイルにまとめられ、*Prisma Access*プロファイルグループに追加されます。

STEP 6 | セキュリティ プロファイルグループは、名前付きのグループにまとめられた個々のセキュリティ プロファイルで構成されます。これにより、セキュリティ プロファイルをセキュリティ ポリシー ルールに簡単かつ一貫して適用できます。

ルールベースのロジックに基づいて、さまざまな条件のセキュリティ プロファイルグループを作成します。

- 各プロファイルグループには、トラフィックの流れに固有のプロファイルグループを作成するなど、異なる目的が必要です。たとえば、インバウンド トラフィックのプロファイル

グループには URL フィルタリングプロファイルは必要ありませんが、アウトバウンド トラフィックのプロファイルグループには必要です。

トラフィックの流れに固有のプロファイルグループを使用すると、内部向けのトラフィックと外部向けのトラフィックを異なる方法で処理したい場合に例外を設けやすくなります。たとえば、使用する内部トラフィックについてはブロックし、外部トラフィックは許可したい場合があります。その場合は、内部トラフィックと外部トラフィックに異なるプロファイルを使用します。個別のプロファイルが必要かどうかは、トラフィックをどのように処理するかによって異なります。

- アラートからブロックへのプロファイルの移行を簡単にするには、初期アラート用のプロファイルグループと、ベストプラクティスブロッキング用のプロファイルグループを作成します。これにより、すべての許可ルールで脅威を簡単に警告できます。アラートからブロックへの移行に慣れてきたら、プロファイルグループを使用すると変更が簡単になります。個々のプロファイルではなく 1 つのオブジェクトを交換するだけで済むからです。
- グループに **default** という名前を付けて、デフォルトのプロファイルグループを作成することを検討してください。たとえば、セキュリティ プロファイル移行に関するベストプラクティスのアドバイスに基づいて、アラートを出すがほとんどのトラフィックをブロックしないプロファイルを含むグループを作成します。ファイアウォールは、トラフィックを許可するすべての新しいセキュリティ ポリシー ルールにデフォルトのプロファイルグループを自動的に適用します。(ファイアウォールは既存のルールにデフォルトプロファイルを適用しません。) これにより、すべての新しい許可ルールにある程度の脅威防止が保証されます。必要に応じてデフォルトのプロファイルを編集または置き換えます。

セキュリティ ポリシー ルールベースのベストプラクティス

セキュリティ ポリシー ルールベースは、セキュリティ ポリシー ルールの順序付きリストです。ルールの順序によって、ファイアウォールがトラフィックを処理する方法が決まります。

ファイアウォールは、セキュリティ ポリシー ルールベースの先頭にある最初のルールから始めて、トラフィックをセキュリティ ポリシー ルールと比較します。トラフィックがルールの条件に一致すると、ファイアウォールはトラフィックに対してルールのアクションを実行し、トラフィックを他のルールと比較しません。トラフィックに一致するルールがない場合、ファイアウォールはトラフィックをドロップします (暗黙的な拒否)。ファイアウォールは最初のルール一致時にトラフィックに対してアクションを実行し、その後トラフィックとルールベースの比較を停止するため、ルールベース内でルールを順序付ける方法は重要です。

別のベンダーのファイアウォールからセキュリティ ポリシーを移行した場合、以前のファイアウォールはルールベースに対してトラフィックを異なる方法で評価していた可能性があります。たとえば、ルールの順序は古いファイアウォールでは違いがなかったかもしれませんが、*Palo Alto Networks* ファイアウォールでは重要です。

さまざまな種類のトラフィックをどのように処理するかを理解し、 #unique_18 ルールベース内でルールを順序付ける方法を評価するのに役立ちます。このセクションで説明するように、論理的な方法でセキュリティ ポリシー ルールベースを設計および最適化します。既存のルールベー

スの場合、ルールベースが可能な限り最適化されていない場合は、このセクションのアドバイスに従って変更を計画し、テストしてください。変更を段階的にロールアウトする予定がある場合は、適切なタイミングで変更を加えてください。

このセクションでは以下について説明します。

- ルールベース内のセキュリティ ポリシー ルールの順序付け
- ルールベースの肥大化を回避する
- ルールに例外を設けるための位置付け
- ルールのシャドウイングの防止と修復
- Panorama でデバイス グループ階層を使用してルールベースを簡素化する

STEP 1 | セキュリティ ポリシー ルールをルールベースで論理的に順序付けします。

トラフィックがルールの基準に一致すると、ファイアウォールはトラフィックに対してポリシー ルールのアクションを実行するため、ルールの順序が重要であり、どのルールのトラフィックが一致するか、つまりファイアウォールがトラフィックに対してどのアクションを実行するか、およびファイアウォールがトラフィックを検査する方法が決まります。:

1. 悪意のあるトラフィックをブロックするルールをルールベースの先頭に配置して、ルールベースの後半で不正なトラフィックが誤って許可されることを防ぎます。アクティブな Advanced Threat Prevention またはアクティブなレガシー Threat Prevention ライセンスをお持ちの場合は、 事前定義された外部動的リスト (EDL) に基づいてブロック ルールを作成し 、それらが許可するトラフィックをブロックしないことを確認するためにテストします。Panorama では、これらのルールをプレ ルールに配置して、ファイアウォール固有のルールより前に実行されるようにします。
2. 基本的なインフラストラクチャ アプリケーションと、DNS や NTP などの共通サービスをルールベースの先頭近くで許可し、誤ってブロックすることを防ぎます。これらのルールは通常、任意の送信元ゾーンから任意の宛先ゾーンへのトラフィックを許可し、すべてのすべての人に適用されます。

   Panorama では、これらのルールをプレルールに配置して、ファイアウォール上でローカルに定義されたルールよりも前に実行されるようにします。
3. 他のすべてのルールのロジックは、最も具体的なルールをルールベースの上部近くに配置し、最も一般的なルールをルールベースの下部近くに配置することです。ルールベース内の特定のルールの前に一般ルールを配置すると、特定のルールに一致するつもりのトラフィックが、代わりに一般ルールに一致する可能性があり、その結果、トラフィックに必要とは異なるアクションや異なる検査が適用される可能性があります。これは シャドウイングと呼ばれます。トラフィックが一致するように意図したルールを、別のルールが「シャドウイング」します。
4. ポートベースおよびサービスベースのセキュリティ ポリシー ルールのすべてを App-ID ベースのルールにまだ変換していない場合、または変換できない場合は、App-ID ベースのルールをポートベースおよびサービスベースのルールよりも前に配置します。

STEP 2 | 管理を容易にし、ルールベースの肥大化を避けるために、ルールベースをできるだけ小さくしてください。

1. 次の 6 つのオブジェクトのうち 5 つが複数のルールで同じである場合は、それらのルールを 1 つのルールに結合します。

   - ソースゾーン
   - 宛先ゾーン
   - 送信元 IP アドレス
   - 宛先 IP アドレス
   - サービスポート
   - アプリケーション

   たとえば、3 つのルールで異なるアプリケーションが指定されているが、送信元ゾーンと宛先ゾーン、送信元 IP アドレスと宛先 IP アドレス、およびサービス ポートが同じである場合、元の各ルールのアプリケーションを指定する 1 つのルールにルールを結合できます。

2. グループ オブジェクトを使用すると、ポリシーの作成が簡素化され、ルールベースのサイズが削減されます。

   アプリケーション グループ と アドレス グループ を使用すると、グループ メンバー全員に適用されるルールを統合できます。

   ポリシーで個別のオブジェクトとグループ オブジェクトの両方を使用する場合、オブジェクトがルールで個別に指定されており、ルールでもオブジェクト グループの一部として指定されている場合、グループ内のオブジェクトのメンバーシップによってルール シャドウイング が発生する可能性があることに注意してください。この場合、トラフィックが最初に間違ったルールに一致する可能性があるため、ファイアウォールは意図したアクションを実行しない可能性があります。変更管理プロセスでアクセスを追跡するために特定のポリシーが必要な場合を除き、可能であればルールを組み合わせてください。オブジェクトをグループ内の他のオブジェクトとは異なる方法で扱いたい場合は、そのオブジェクトをグループから削除します。

3. ルールが必要なくなったら、セキュリティ ポリシー ルールベースからルールを無効にするか削除します。

   組織がアプリケーションやインフラストラクチャを変更したり、一時的なテスト ルールが必要なくなったりした場合、セキュリティ ポリシー ルールが不要になる可能性があります。これらのルールを無効にするか削除しないと、トラフィックに対して予期しないアクションが発生する可能性があります。ルールを無効にすることで問題が発生した場合に再度有効にできるように、最初にルールを無効にするのが最も安全です。ルールを無効にする場合は、ルールを無効にした日付を含むタグを適用します。Policy Optimizer の ルール使

用状況 機能を定期的に使用して、各ルールが使用されていない期間を確認します。一定期間が経過して、そのルールが本当に必要ないと確信できたら、ルールを削除します。

四半期会議や年次会議などの定期的なイベントにのみ使用するアプリケーションのルールに注意してください。イベント期間中のみルールを有効にする スケジュール を構成することが適切な場合があります。

4. Policy Optimizer を使用してルールベースを最適化します。Policy Optimizer は、未使用のルール、未使用のアプリケーションを含むルール、長期間使用されていないルール、およびログ転送プロファイルを持たないルールを検出します。また、SaaS をお持ちの場合は、セキュリティ ポリシーで新しい SaaS アプリケーションを管理できるようにします。セキュリティサブスクリプション。
5. Panorama では、組織全体の複数の VSYS およびファイアウォールに適用される共通のグローバル デバイス グループを使用して、共通のグローバル セキュリティ ポリシー ルール（共通の基本サービスや、広範なデバイス グループに適用するその他のサービスやアプリケーションを制御するルールなど）を実現します。デバイス グループ階層を作成すると、グループ間でルールを繰り返す必要がなくなります。階層を使用してルールを 1 回作成し、それを適切なすべてのファイアウォール グループに適用します。
6. 定期的なメンテナンスの一環として、セキュリティ ポリシー ルールベースを定期的に確認します。

STEP 3 | ルールに例外を作成するには、より一般的なルールの前に、より具体的なルールを配置します。

たとえば、従業員が悪意のある Web サイトにアクセスできないようにしたい場合は、すべての従業員のすべての悪意のある Web サイトへのアクセスをブロックする一般的なセキュリティ ポリシー ルールを作成します。ただし、InfoSec チームと PEN テスターはテスト目的でアクセスする必要があります。この場合、必要な悪意のある Web サイトへのアクセスをそれらのユーザーのみに許可するルールを作成し (トラフィックを復号化し、最も厳格な脅威プロファイルをルールに適用し、テストに使用するアプリケーションのみを指定します)、そのルールを一般的なルールの上に配置します。ルールベース内のルール。

InfoSec および侵入テスターがテストのために悪意のあるサイトにアクセスしようとすると、それらは許可されますが、他のユーザーがルールの基準に一致しないため、一般ルールによってブロックされます。InfoSec およびペン テスト チームのアクセス ルールを一般的なブロック ルールの後に配置すると、一般的なルールは特定のルール のシャドウイングを実行し、InfoSec/ペン テスターのトラフィックは一般的なルールと一致してブロックされます。

STEP 4 | 一般的なルールがより具体的なルールに影を落とすことを防ぎます。

シャドウイングとは、より具体的なルールと同じ一致基準を含む広範なルールを、ルールベース内で特定のルールよりも上位に配置することです。そのため、特定のルールに一致することを目的としたトラフィックは、代わりに最初に一般的なルールに一致し、特定のルールとは決して比較されません。その結果、ファイアウォールは、特定のルールでアクション

とインスペクションを実行することが意図されている場合に、一般ルールで構成されたアクションとインスペクションを実行します。一般的なルールは特定のルールを覆い隠します。

シャドウ ルールは、ルールベース内の他の 2 つ以上のルールをシャドウする場合があります。

シャドウイングを防ぐ最も簡単な方法は、ルールベースを最初から正しく構築することです。ただし、既存のルールベースと移行されたルールベースにはシャドウ ルールが存在する可能性があります。シャドウイングを防止および修正するには:

1. トラフィックに対して実行するアクションとトラフィックを検査する方法を理解します。

   特定のルールのアクションとインスペクションによってトラフィックを処理したい場合は、ルールベース内の一般ルールの上に特定のルールを移動します。一般ルールのアクションとインスペクションによってトラフィックを処理する方法であれば、特定のルールは必要ありません。
2. ルールベースの一般的なルールの上に、より具体的なセキュリティ ポリシー ルールを配置します。一般ルールを最初に配置すると、次のように特定のルールが影になります。
   1. Facebook へのすべてのアクセスをブロックする一般ルールを作成します。
   2. マーケティングおよび PR グループが Facebook にアクセスできるようにする特定のルールを作成しますが、そのルールをルールベース内の一般的な Facebook ルールの下に配置します。
   3. 一般ルールは、ユーザー グループに関係なくすべての Facebook アクセスをブロックするため、トラフィックが、許可する特定のグループへのアクセスを許可する特定のルールに一致することはありません。

   修正するには、ルールベース内の一般ルールの上に特定のルールを移動します。
3. シャドウ ルールを確認して解決し、ファイアウォールが必要なアクションを実行し、必要な方法でトラフィックを検査していることを確認します。

   新しいセキュリティ ポリシー ルールを作成する場合:
   1. コミット オプションを選択し、ファイアウォールで コミット を実行するか、Panorama で コミットを検証 して構成の問題を確認します。構成をコミットしないでください。続行する前に、検証チェックで検出された問題を解決してください。
   2. 設定を **Commit and Push**（コミットしてプッシュ）します。
   3. コミットが完了したら、右下のリボンから **[Tasks (タスク)]** を選択してタスク マネージャーを開きます。
   4. タイプ 列で **[Commit All (すべてコミット)]** をクリックして **[Job Status (ジョブのステータス)]**を表示します。(コミットとプッシュではシャドウイング情報は提供されません。)
   5. ステータス 列のメッセージをクリックして **[Last Push State Details (最終プッシュ状態の詳細)]** を開き、**[Rule Shadow (ルール・シャドウ)]** タブを選択します。**[Rule Shadow**

(ルール シャドウ)] タブがない場合、ファイアウォールにはシャドウ ルールがありません。

6. **[Last Push State Details (最後のプッシュ状態の詳細)]** の左側には、他のルールをシャドウするルールが表示されます。各シャドウ ルールの名前は、ルールへのリンクです。各シャドウ ルールについて、**[Count (数)]** 列の数値をクリックして、シャドウ ルールがシャドウするルールを表示します。シャドウ ルール名がリストされますが、シャドウ ルールへのリンクではありません。
7. シャドウ ルールのリストはコミット操作全体では永続的ではないため、シャドウ ルールごとにシャドウ ルールのリストを取得することが重要です。たとえば、スクリプトを使用して API 経由でステータスを取得したり、リストをコピーしてテキスト エディターに貼り付けたり、スクリーン キャプチャや写真を撮ったり、シャドウイング ルールとシャドウイングされたルールの名前を書き留めたりします。

   PAN-OS 構成の ***Commit (コミット)*** 操作では、シャドウ ルールが検証されます。ルールのシャドウイングが検出された場合、影響を受けるルールを特定する警告メッセージが生成されます。シャドウ リストをキャプチャする前に別のコミット操作を実行すると、シャドウ情報が失われます。この情報はすぐに取得してください。
8. セキュリティ ポリシー ルールベースで各シャドウイングおよびシャドウイングされたルールを検索し、各ルールの設定をキャプチャします。
9. 各シャドウ ルールとそのシャドウ ルールを並べて比較し、各ルールの目的を理解します。これにより、関連するルールをまとめて評価し、ルールによって制御されるアプリケーションをどのように処理するかを理解できるようになります。
10. シャドウ ルール内のアプリケーションとそのシャドウ ルールをどのように処理するかを理解したら、ルールを結合してルールベースを簡素化し、重複ルールを無効化または削除し、特定のルールを一般ルールの上に移動してシャドウイングを解決します。
11. 繰り返して、残っているシャドウイングを修正します。
12. シャドウ ルールごとにこのプロセスを繰り返します。

非実稼働テスト システムでは、新しいポリシー ルールやその他のテスト目的をテストするために、シャドウイングとシャドウイングされたルールを保持しておきたい場合があります。

STEP 5 | Panorama では、セキュリティ ポリシー ルールをデバイス グループ階層内に適切に配置します。

複数のデバイス グループで同じルールを不必要に繰り返す必要がないようにルールを配置します。複数のデバイス グループに共通のルールは、階層内のそれらのグループの上に属するため、1 つのルールがすべてのグループに適用されます。

- アクセスする予定のファイアウォール グループにのみアクセスを許可するように、慎重に階層を構築します。デバイス グループを構築するときに各ファイアウォールに必要なアクセスを考慮し、デバイス グループ階層を作成するときに各デバイス グループに必要なア

クセスを考慮します。構築の鍵となるのは共通性です。つまり、どのファイアウォールが同様のアクセスを必要とするか、どのファイアウォールのグループが同様のアクセスを必要とするか、また、階層の上位のグループにその下のレベルに適用されるルールを含めて重複の必要性を排除できる階層を構築する方法です。ルール。

- ルールの重複を避けるために、すべてのファイアウォールに適用されるルールを階層内の最上位のグループに配置します。
- ルールを重複させる必要がないように、ファイアウォール グループのセットに適用するルールを階層内の十分な上位に配置します。

『Panorama 管理者ガイド』 には、デバイス グループ階層の図例など、デバイス グループ に関する詳細な情報が記載されています。

ポリシー オプティマイザーのベストプラクティス

Policy Optimizerは、ポートベースのセキュリティ ポリシー ルールをアプリケーションベースのルールに変換し、最小権限アクセスポリシールールに移行するのに役立ちます。

- ポートベースのルール（アプリケーションは特定のアプリケーションではなく任意のアプリケーション）を検出し、最小権限アクセスの原則に従うアプリケーションベースのルール（ポリシー > セキュリティ > ポリシー オプティマイザー > 、アプリケーションコントロールなしのルール）に変換します。
- 過剰にプロビジョニングされたルール (ポリシー、セキュリティ ポリシー オプティマイザー、未使用アプリ) から未使用のアプリケーションを検出して削除します。
- 使用しないルールを見つけて削除し、ポリシー ルールの使用状況（ポリシー > セキュリティ > ポリシーオプティマイザー > ルールの使用状況）を把握します。
- セキュリティ ポリシールールで使用されているアプリケーション フィルタとアプリケーション グループと一致する新しいアプリケーションを検出します。新しいアプリケーションを評価し、それらを許可するかブロックするかを評価します (ポリシー > セキュリティ > ポリシーオプティマイザー > 新しいアプリケーションビューア)。

> *SaaS Security Inline* サブスクリプションをお持ちで、App-ID Cloud Engine (ACE) を使用している場合は、ポリシーオプティマイザーを使用して ACE アプリ ID をセキュリティ ポリシールールベースに統合してください。

- ログ転送プロファイルが添付されていないセキュリティ ポリシー ルールを見つけて、それらのルールにログ転送プロファイルを追加します (ポリシー > セキュリティ > ポリシー オプティマイザー > セキュリティサービス用ログ転送)。

ポリシーオプティマイザーは、パノラマおよび*PAN-OS*ファイアウォール用の*PAN-OS 9.0*以降で使用できます（パノラマが*PAN-OS 9.0*以降を実行している場合、ファイアウォールは*PAN-OS 8.1*でも使用できます）。*Prisma Access*はポリシーオプティマイザーをサポートしていません。

Cortex Data Lake (CDL) との互換性には、*PAN-OS 10.0.3* 以降を実行し、クラウドサービスプラグイン *2.0 Innovation* 以降を実行しているパノラマが必要です。

ポリシーオプティマイザーのベストプラクティスには以下が含まれます。

- ポリシーオプティマイザーの使用方法—主な使用例、セキュリティ ポリシー ルールにアプリケーションを追加する方法、ルールをソートおよびフィルタリングする方法、アプリケーション フィルタとアプリケーション グループの使用方法。
- ポリシーオプティマイザルールベースワークフロー—アプリケーションベースのルールへの移行を計画する方法、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に変換する方法、未使用のルールを排除する方法、未使用のアプリケーションを削除してルールベースを強化する方法。

より正確なアプリケーション情報を提供し、*Policy Optimizer* を使用して制御しているアプリケーションを可視化するために、地域の規制、コンプライアンス、ビジネス要件、プライバシーの考慮事項によって許可されるすべてのトラフィックをできるだけ早く復号化します。復号化を行わないと、ファイアウォールは親アプリケーションを識別できますが、通常は機能しているアプリケーションを識別できません。たとえば、ファイアウォールは「*facebook*」を認識しますが、*Facebook*投稿、*Facebook*ダウンロード、*facebook*ファイル共有などは認識しません。機能するアプリケーションを可視化し、制御するには、トラフィックを復号化する必要があります。SSLフォワード プロキシ *(*アウトバウンド*)* 復号化の場合、最初にユーザー *ID* と *URL*フィルタリングを実装して、効果的に復号化をターゲットにできるようにします。

ポリシーオプティマイザーの使用方法

このセクションでは、ポリシーオプティマイザの主な使用例とツールの使用方法について説明します。ポリシーオプティマイザルールベースワークフローではワークフローについて説明します。

ポリシーオプティマイザーのユースケースには以下が含まれます。

- ポートベースのアプリケーションベースのルールからの移行 — 各ポートベースのルールに一致するレイヤー 7 アプリケーションを表示し、許可するアプリケーションを選択して、各ルールを 1 つ以上のアプリケーションベースのルールに変換します。
- 新規導入—ネットワーク上のアプリケーションを検出し、時間をかけてアプリケーションベースのポリシーに移行します。

- 成熟した導入—ルールベースを精査し、アプリケーション フィルタに基づく広範なルールを、制裁対象アプリケーションのみを許可するアプリケーション グループに基づく厳しいルールに変換し、未使用のルールやアプリケーションを排除します。
- **DevOps**—テスト環境内の新規または変更されたアプリケーションを理解します。実稼働環境に変更を加える前に、セキュリティ ポリシー ルールでそれらをどのように処理するかを検討してください。新しいルールや変更されたルールは、実稼働環境に適用する前にテストしてください。

STEP 1 | 適切な担当者と協力して、ビジネス目的でネットワーク上で許可したい制裁対象アプリケーションと、従業員に許可したい許容されるアプリケーションを理解してください。

どのアプリケーションがビジネスクリティカルであるかを把握しておいてください。どのアプリケーションが四半期ごと、年次、またはその他のイベントでのみ定期的に使用されるかを確認し、それらのアプリケーションの動作を確認できる期間にわたって関連するルールを検討してください。アプリケーションを許可するためのビジネスロジックを知ることは、セキュリティ ポリシーを構築する方法を理解するのに役立ちます。アプリケーションをよりよく理解するには、Applipediaまたはファイアウォールまたはパノラマ上のオブジェクト > アプリケーションでコンテンツ配信アプリIDを調べてください。

STEP 2 | さまざまな目的でさまざまなメトリックを使用して、ポリシーオプティマイザーの情報と統計をソート、フィルタリング、および調べる方法を学びます。

ポリシーオプティマイザの統計情報はリアルタイムでは報告されません。アプリケーションリストの更新には、アプリケーションのトラフィック量とルールベースのサイズにもよりますが、約 1 時間以上かかります。ルールにアプリケーションを追加したら、少なくとも 1 時間待ってから、トラフィック ログでアプリケーションの情報を確認します。情報が表示されない場合は、しばらく待ってからもう一度確認してください。

ポリシーオプティマイザーは、一時的なアプリケーションをカウントしないように、セッション開始時にのみログを記録するルールからのトラフィックを無視します。（セッション終了時にもログを記録するルールの場合、ポリシーオプティマイザはルールの統計情報を取得します。）

STEP 3 | セキュリティ ポリシーでアプリケーション フィルタとアプリケーション グループを使用する方法を理解してください。

セキュリティ ポリシールールのアプリケーション フィルタを使用して、ネットワーク上のアプリケーションを検出します。次に、それらのルールをアプリケーション フィルタからアプリケーション グループに変換して、許可するアプリケーションを正確に指定できるようにします。

- セキュリティ ポリシールールを簡素化および強化し、ルールベースのサイズを縮小するには、できるだけアプリケーション グループを使用してください。

  アプリケーショングループは、ユーザー定義の特定のアプリケーションのセットで、同様のセキュリティ処理を施した1つのルールで制御したいものです。アプリケーションごと

に個別のルールを作成するのではなく、アプリケーション グループを使用してルールにアプリケーションを追加します（リンク先のトピックはACEアプリケーションに焦点を当てていますが、すべてのアプリケーションに適用されます）。これにより、1つのルールで複数のアプリケーションを制御できます。さまざまなルールでアプリケーション グループを再利用して、さまざまなユーザー、ソース、宛先に異なるアプリケーションへのアクセスを許可します。グループを再利用すると、複数のルールにアプリケーションを自動的に追加できます (アプリケーション グループに変更を加えると、その変更はアプリケーション グループを含むすべてのルールに反映されます)。

- アプリケーション フィルタを使用して次のことを行います。
  - ネットワーク上のアプリケーションを検出します。
  - 新しいアプリケーションがフィルターに一致すると自動的に処理されるため、将来性のあるルールを作成できます。これは、移行や新規デプロイのアプリケーション発見フェーズでも、成熟した環境でも役立ちます。

    たとえば、**Palo Alto Networks** タグに基づくアプリケーション フィルタを使用して許可ルールを作成します。これにより、現在のすべての Palo Alto Networks のアプリケーションと今後のすべての Palo Alto Networks のアプリケーションを許可することが保証されます。

    もう 1 つの例として、コンテンツ配信の新しいアプリ ID をフィルタリングするルールを作成して、より綿密に調査できるようになるまで安全に処理します。
  - 成熟したルールベースでは、アプリケーション フィルタを使用してルールにアプリケーションを追加し、望ましくないタイプ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 グループを使用してトラフィックを意図的に許可します（リンク先のトピックは ACE アプリケーションに焦点を当てていますが、すべてのアプリケーションに適用されます）。

  アプリケーション フィルタは動的なアプリケーションセットです。アプリケーションは、カテゴリ、サブカテゴリ、リスク、タグ (定義済みのタグまたはカスタムタグ)、特性など、定義した属性に基づいてアプリケーション フィルタを照合します。ファイアウォールは、フィルター条件に一致すると、新しいアプリケーションをフィルターに自動的に追加します。アプリケーション フィルタを含むセキュリティ ポリシー ルールは、フィルタに一致する新しいアプリケーションを自動的に制御します。

  アプリケーション フィルタは、アプリケーション グループよりも制御が緩いです。どのアプリケーションをアプリケーション グループに入れるかを正確に制御できます。定義する属性は、アプリケーション フィルター内のアプリケーションを制御します。これにより、必要以上に多くのアプリケーションが許可される可能性があります。そのため、トラフィックを検出したり、トラフィックのアプリケーション サブカテゴリをブロックしたりするには、フィルタが最適です。さまざまなルールでアプリケーション フィルタを再利用

して、さまざまなユーザー、ソース、宛先にさまざまなアプリケーションへのアクセスを許可します。

個々のアプリケーションをルールに追加する代わりに、できる限りアプリケーション グループとアプリケーション フィルタを使用してください。PAN-OS 10.1以降、Policy Optimizerから直接アプリケーションをアプリケーション グループやフィルタに追加できるようになりました。これは、ルールが認識するすべてのアプリケーションを可視化できるため、ベストプラクティスです。

PAN-OS 10.1より前のバージョンでは、オブジェクト > アプリケーション グループ、オブジェクト > アプリケーション フィルタを使用してアプリケーションをグループとフィルタに追加していました。

STEP 4 | ルールの目的に基づいて、ルールに追加するアプリケーションを決定します。ルールの目的は、アプリケーションへのアクセスを必要とするユーザーと、アクセスを許可する方法（ソース、ターゲット、インスペクション、ロギング）を決定するのに役立ちます。

STEP 5 | ポリシー内のアプリケーション フィルタオブジェクトとアプリケーション グループ オブジェクトを再利用して、異なるユーザーグループにそれらのアプリケーションへの異なるアクセスレベルを与えたり、異なる送信元と宛先の組み合わせを異なる方法で処理したりします。

ユーザーIDは、最小権限アクセスの原則に基づくベストプラクティスのセキュリティ ポリシーを作成するために不可欠です。User-ID がないと、アプリケーションを使用できるユーザーを指定できません。

アプリケーション グループとアプリケーション フィルタオブジェクトを再利用すると、ルールベースが簡略化され、ルールベースの肥大化が軽減されます。

ポリシーオプティマイザルールベースワークフロー

このセクションでは、Policy Optimizer ツールのポートベースのルールからアプリケーションベースのルールとワークフローへの移行について説明します。ポリシーオプティマイザーの使用方法では、主な使用例とツールの使用方法について説明します。

最終的な目標は、制裁対象のアプリケーションと従業員の使用を許容するアプリケーションのみを許可するようにルールをロックダウンすることです。それと同時に、ビジネス上の正当な理由があるユーザーをロックダウンして、さまざまなアプリケーションにアクセスするようにしてください。トラフィックログと ACC を使用すると、ルールの範囲を特定のユーザーに絞り込み、ユーザーアクセスを過剰にプロビジョニングすることを回避できます。アプリケーション所有者や他のグループと協力して、アプリケーションにアクセスするビジネス上の理由がある人を把握します。

STEP 1 | ポートベースのルールからアプリケーションベースのルールへの段階的な移行を計画し、移行の主要な概念と方法を理解してください。

移行と新規導入の計画と方法論:

- ポートベースのルールからアプリケーションベースのルールへの移行については、ポートベースのセキュリティ ポリシールールベースから始めてください。新しいデプロイや移行では、アプリケーション フィルタに基づいてルールを作成してさまざまなタイプのアプリケーションを可視化し、ルールベースの最下部にキャッチオールルールを追加して、ミッションクリティカルなアプリケーションを誤ってブロックしないようにします。これらのルールには、ベストプラクティスの脅威防御プロファイル (両方向) と URL フィルタリング プロファイル (アウトバウンドトラフィック) を適用します。アプリケーションがキャッチオールルールに一致したら、ステップ 2 のアドバイスに従って、最初に変換と調整を開始するルールに優先順位を付け、アプリケーションベースのルールに移行する前に、さまざまなタイプのアプリケーションのルールをどのくらいの期間遵守するかを決めます。

  ポリシーオプティマイザーは、各ポートベースのルールに一致する特定のレイヤー7 アプリケーション (アプリ ID) を表示します。

- ベストプラクティス評価レポートをAIOpsで直接実行してベースラインを設定し、現在のベストプラクティスの状態を理解できるようにします。定期的にレポートを作成して、進捗状況を測定します。進歩するということは、時間の経過とともに、ポートベースのルール、未使用のルール、および未使用のアプリケーションに関するルールが減少することを意味します。

既存の導入計画と方法:

- デプロイメントがポートベースのルールで構成されている場合、またはほとんどがポートベースのルールで構成されている場合は、アプリケーションベースのポリシーへの移行に関する前述のアドバイスに従ってください。
- デプロイメントが主にアプリケーションベースのルールで構成されている場合は、セキュリティ ポリシールールベースの一番下にキャッチオールルールを配置して、他のルールと一致しないアプリケーションを検出して可視化し、厳格なセキュリティプロファイルで悪意のあるトラフィックを阻止します。ステップ 2 の優先順位付けに関するアドバイスに従って、ルールを厳しくします。

アプリケーションをポートベースのルールからアプリケーションベースのルールに移動したら、ポリシーオプティマイザとルールヒットカウンタのリセットでポートベースのルールを選択します。これにより、**Days with no new apps** カウンターがリセットされ、元のポートベースのルールに一致する新しいアプリケーションがいつ増えるかを確認し、それらを許可するかブロックするかを評価できます。

ルールを絞り込んだら、「新しいアプリがない日数」が 7 日以上になるのを待ってから、ルールを再確認して調整を続行します。キャッチオールルールとポートベースのルールに、許可したいアプリケーションが表示されなくなったら、それらを無効にするか削除します。ルールを無効化または削除する前に、企業が定期的なイベントにのみ使用するアプリケーションに注意してください。

STEP 2 | ポートベースのセキュリティ ポリシールール (アプリケーションが「任意」に設定されているルール) に優先順位を付け、レイヤー 7 のアプリケーションベースのルールに変換します。

移行のどの段階で、どのルールをポートベースのルールからアプリケーションベースのルールに変換するかを優先順位付けします。これらの手法は、移行や新規デプロイのほか、ルールベースを強化する必要がある既存のアプリケーションベースのデプロイメントに有効です。

1. 新規および既存の導入環境では、既知の悪質なトラフィックや危険なトラフィックを直ちにブロックします。
2. アプリケーション フィルタに基づいてキャッチオールルールを実装します。
3. 1週間後、簡単なルールを有名なアプリケーションに変換します。たとえば、ポート 21 (FTP)、ポート 53 (DNS)、ポート 22 (SSH) を制御するルールは、迅速な変換に適しています。ポートベースのルールに含まれるアプリケーションが少なく、よく知られているほど、そのアプリケーションをアプリケーションベースのルールに変換する自信が高まります。
4. 30 日が経過したら、最も安定したルールを変換します。30 日間にわたって新しいアプリケーションが見つからず、制御するアプリケーションが比較的少ないルールが適しています。
5. 30 日以上経過したら、インターネットアクセスルール (SSL、Web ブラウジング) とトラフィックが最も多いルールの変換を開始します。
6. ルールに表示されているアプリケーションに適した期間が経過したら、表示されるアプリの数が少ないルールを変換します。
7. ルールを変換するときは、新しいアプリがない日数が少なくとも7日（複雑なルールや多数のアプリケーションを含むルールの場合はそれ以上）に達したら各ルールを確認し、必要に応じて新しいアプリケーションを処理します。

ルールを複製することは、ポートベースのルールからアプリケーションベースのルールに移行する最も安全な方法です。クローニングでは元のポートベースのルールが保持され、クローンされたルールは元のルールのすぐ上に配置されます。これにより、Webブラウジングとsslトラフィックをアプリケーションベースのルールに移行するこのクローニングのユースケースに示すように、アプリケーションの可用性を損なうことなく、元のルールから特定のアプリケーションベースのルールを作成できます。複製されたルールに一致しないアプリケーションは、元のポートベースのルールに引き続き一致します。元のルールで、ネットワーク上で必要なアプリケーションが一定期間表示されなくなった場合は、元のルールを安全に無効化または削除できます。

ルールを変換するときは、アプリケーション グループとアプリケーション フィルタを適切に使用してください。

移行シナリオについては、「アプリケーション ベースのポリシーへの移行に関するベストプラクティス」に従ってください。

STEP 3 | ルールを調べるときは、アプリケーション フィルタを使用して、ネットワークに含めないとわかっている種類のアプリケーションをブロックします。サブカテゴリ、タグ、特性に基づいてトラフィックをブロックします。アプリケーション フィルタを使用して、ブロックルールに例外を設けます。ブロックフィルター条件としてリスクを使用しないでください。リスクを使用してトラフィックを適切に検査、記録、制御する方法を決定してください。

既知の悪質なトラフィックを阻止するための推奨ブロックルールに加えて、ルールを定期的に見直して、望ましくないことがわかっている他のトラフィックをブロックしてください。

1. ネットワークで使用したくないアプリケーションタイプを特定し、それらに一致するアプリケーション フィルタを作成します。これらのアプリケーション フィルタに基づいてブロックルールを作成し、キャッチオールルールの前に配置します (または、既存のルールからルールを複製し、複製されたルールをルールベースの元のルールのすぐ上に配置します)。
2. ブロックされているアプリケーションの種類の中で、ネットワーク上で許可したい特定のアプリケーションがあるかどうかを確認します。ブロックルールを複製し、アクションを許可に変更し、許可するアプリケーション以外のすべてのアプリケーションを削除します。許可ルールをブロックルールのすぐ上に配置して、ブロックルールに例外を作成します。
3. ブロックルールを監視して、ブロックされた他のアプリケーションを許可するかどうかを確認します。例外の許可ルールを作成した場合は、許可するアプリケーションをそのルールに追加します。それ以外の場合は、アプリケーション用の新しい許可ルールを作成し、ルールベースのブロックルールのすぐ上に配置します。

たとえば、ファイル共有アプリケーションは特に危険な場合があります。トラフィックを復号化し、セキュリティ ポリシールールで、ビジネス目的で使用する特定のファイル共有アプリケーションのみを必要なユーザーのみに許可し、トラフィックを検査して記録します。ルールベースの次のルールでは、ファイル共有サブカテゴリに基づくアプリケーション フィルタを使用して、明示的に意図的に許可していないすべてのファイル共有アプリケーションをブロックします。

STEP 4 | 過剰にプロビジョニングされたルールから未使用のアプリケーションを削除します。

ルールからアプリケーションを削除する前に、アプリケーションの目的を理解してください。

- 使用済みのアプリと許可されているアプリを比較します。ルールで許可されているアプリケーションの数よりも多くのアプリケーションが許可されている場合は、未使用のアプリケーションを調べて、それらを削除できるかどうかを判断します。
- 四半期ごと、毎年、またはその他の定期的なイベントにのみ使用されるアプリケーションに注意してください。これらのアプリケーションを確認するのに十分な長さのルールの履歴をキャプチャしてください。また、テスト環境でアクティブなアプリケーションや、アプリケーションの制裁措置を見越して本番環境に追加されたアプリケーションも考慮に入れてください。

STEP 5 | セキュリティ ポリシールールベースから未使用のルールを削除します。

未使用のルールは乱雑になり、ルールベースが複雑になります。「ルール使用状況」には、さまざまな期間の未使用のルールに関する情報が表示されます。ルール内のアプリケーションを評価して、まだ使用されていないにもかかわらず必要かどうかを確認してください。未使用のルールを削除する前に、次の点を考慮してください。

- ヒットしないブロックルール-これらのルールを無効にしたり、削除したりしないでください。たとえば、脅威 EDL を使用するブロックルールはヒットしません。それは良いことですが、悪意のあるトラフィックがネットワークにアクセスしようとした場合に備えて、引き続きブロックする必要があります。
- 臨時規則 — たとえば、請負業者または監査人に関する規則。これらのルールを削除する代わりに、定期的にアクセスする時間がある場合は、ルールがいつ有効になるかを制御するスケジュールを設定します。アクセスが断続的な場合は、ルールを無効にし、必要に応じて有効にしてください。
- 無効化されたポリシールール — ルールが無効になった日付のタグを適用します。ルールが特定の期間（たとえば 1 年以上）内に使用されない場合、そのルールは削除の対象となります。説明を追加して、ルールを無効にする理由と、監査人や請負業者のアクセスなどのためにルールを有効にする場合や、いつ有効にする必要があるかを示します。
- 定期的に使用されるアプリケーション — 一部のアプリケーションは、四半期ごと、年ごと、またはその他の定期的なイベントにのみ使用されます。これらのタイプのアプリケーションを制御するルールの履歴を十分に長く記録して、アプリケーションが使用されなくなったことを確認します。

STEP 6 | 各ルールに適切なログ転送プロファイルが添付されていることを確認します。

ログ転送プロファイルがないルールを特定し、プロファイルを追加します (ポリシー > セキュリティ > ポリシーオプティマイザー > セキュリティサービスのログ転送)。

STEP 7 | アプリケーション フィルタに基づく広範なルールを、アプリケーション グループに基づく狭いルールに変換します。

ルール使用状況の統計を使用してルールの使用方法を把握し、ポリシーオプティマイザーを使用してアプリケーションをアプリケーション グループに追加し（PAN-OS 10.1以降、PAN-OS 10.0以前の場合は、オブジェクト > アプリケーション グループ）、より厳密なルールを作成します。

最終的な目標は、アプリケーション フィルターに一致する幅広いアプリケーションを許可するのではなく、承認したアプリケーションのみを許可することです。アプリケーション フィルタを使用してネットワーク上のアプリケーションを検出し、アプリケーションの幅広いサブカテゴリをブロックしたり、アプリケーション グループを使用して許可したいアプリケーションを正確に指定したりできます。Policy Optimizer を使用してアプリケーション フィルタベースのルールをアプリケーション グループベースのルールに変換するには：

- アプリケーション フィルタに基づいてルールに一致するアプリケーションを調べ、許可するアプリケーションを決定します。

- アプリケーション フィルターに基づくルールごとに、許可するアプリケーションを選択し、 複製されたルールまたは既存のルールのアプリケーション グループにアプリケーションを追加します。
- アプリケーションをアプリケーション フィルタに基づくルールからアプリケーション グループに基づくルールに移動したら、ポリシーオプティマイザとルールヒットカウンタのリセットでそれらのルールを選択します。これにより、**Days with no new apps** カウンターがリセットされ、新しいアプリケーションがアプリケーション フィルタ ベースのルールと一致するタイミングを確認できます。
- アプリケーション フィルターに基づいてルールを監視し、 新しいアプリのない日数 カウンターが、ルールで新しいアプリケーションが検出されなくなったことを示すしきい値に達するまで確認します。しきい値は、環境とアプリケーション フィルターが一致するアプリケーションの種類によって異なります。四半期や年次イベントなど、特定の期間にのみ使用されるアプリケーションを考慮し、それらのアプリケーションが表示されるまでフィルタをそのままにして、適切なアプリケーション グループに追加できるようにします。アプリケーション フィルター ルールがネットワーク上に必要なアプリケーションに一致しない場合は、企業のポリシーに応じてルールを無効にするか削除します。

STEP 8 | 新しいアプリケーションが環境に導入されたら、セキュリティ ポリシールールを確認して更新してください。

新しいアプリビューアーで新しいアプリ ID を定期的に確認してください。既存および新規のアプリケーション グループにアプリケーションを追加するか、既存のセキュリティ ポリシールールにアプリケーションを直接追加します。アプリケーション フィルタをアプリケーション グループに変換し続けます。

App-ID Cloud Engine のベストプラクティス

App-ID Cloud Engine (ACE) は、ファイアウォールが特定のアプリケーションではなく、SSL または Webブラウジング トラフィックとして以前に識別していた数千の SaaS アプリケーションを識別します。ACE は、これらの SaaS アプリケーションに固有の App-ID を与えるため、それらを可視化し、制御し、セキュリティ ポリシーで明示的に使用できるようになります。

ACE には、*PAN-OS 10.1* 以降と *SaaS Security Inline* サブスクリプションが必要です。*ACE* は、*Prisma Access*Cloud Services 3.0 Innovation*for Panorama Managed Prisma Access* で使用でき、また Cloud Managed Prisma Accessでも使用できます。

ACE アプリ *ID* は、セキュリティ ポリシーでのみサポートされます。*ACE* アプリ *ID* は、他の種類のポリシー ルールでは使用できません。

ファイアウォールは *ACE* アプリ *ID* のカタログ全体をダウンロードしますが、環境内で見られるアプリケーションの *ACE* アプリ *ID* シグネチャのみをダウンロードします。

ACE は、アウトバウンド フローで SaaS アプリケーションを制御し、クラウド アクセス セキュリティ ブローカー (CASB) のように機能します。新しい展開では、ACE はネットワーク上の SaaS アプリケーションを識別して、レイヤー7 アプリケーション ベースのポリシーへの移行を簡素化します。

既存の展開では、ACE は、これまでに SSL または Webブラウジング トラフィックとして識別されていた潜在的に多くの SaaS アプリケーションを安全に理解して管理し、セキュリティ ポリシーで明示的に制御するためのツールを提供します。

より正確なアプリケーション情報を提供し、*ACE* アプリケーションを可視化するために、地域の規制、コンプライアンス、ビジネス要件、プライバシーの考慮事項によって許可されるすべてのトラフィックをできるだけ早く復号化します。復号化を解除しないと、ファイアウォールは親アプリケーションを識別できる場合がありますが、通常は機能するアプリケーションを識別できません。たとえば、ファイアウォールは「*facebook*」を認識しますが、*facebook-post*、*facebook-download*、*facebook-file-sharing* などは認識しません。機能するアプリケーションを可視化し、制御するには、トラフィックを復号化する必要があります。SSL フォワード プロキシ *(*アウトバウンド*)* 復号化の場合、最初にユーザー *ID* と *URL* フィルタリングを実装して、効果的に復号化をターゲットにできるようにします。

STEP 1 | ACE を有効にする前に、ファイアウォール上で ACE アプリ ID がどのように機能するかを理解してください。

ACE の処理とポリシーの使用法 を読んで、ファイアウォールが次のような ACE アプリ ID を処理する方法を学習します。

- ファイアウォールが ACE アプリ ID をダウンロードする方法とタイミング。
- ACE アプリ ID とコンテンツ配信 アプリ ID の違い。
- ファイアウォールが、ACE アプリ ID、コンテンツ配信 App-ID、およびコンテナ アプリケーション (facebook など) とその機能アプリケーション (facebook-post、facebook-download など) を含むカスタム App-ID の間の競合を解決する方法。
- HA の動作。
- コミットまたはプッシュ時の Panorama の動作。

ACE は、ファイアウォールが以前に SSL または Webブラウジング トラフィックとして識別していた特定の SaaS アプリケーションを識別します。ACE を有効にすると、次のようになります。

- SSL および Webブラウジング トラフィックを許可するセキュリティ ポリシー ルールがある場合、ダウンロードされた ACE アプリ ID は、ルールで使用されているアプリケーション フィルタに一致しない限り、そのルールに一致します。ACE アプリ ID は、コンテンツ配信される ACE アプリ ID と同様に、タグを含むフィルターの基準に基づいてアプリケーション フィルターと一致します。ACE アプリ ID がルール内のアプリケーション フィルタと一致する場合、アプリケーションは暗黙的にルールに追加されます。このルールは、SSL/Webブラウジング ルールの代わりに ACE アプリケーションを制御します。これには、ルールのアクション (許可または拒否)、アプリケーションにアクセスできるユーザー、ソースと宛先、アプリケーションの検査とログの方法が含まれます。
- ACE アプリ ID を明示的にルールに追加するか、ACE アプリ ID が暗黙的にルールに追加するアプリケーション フィルタに一致するまで、ACE アプリケーションは、ACE を有効にする前と同様に、引き続き ssl/Web 閲覧許可ルールに一致します。 。
- SSL および Webブラウジング トラフィックを許可するルールがない場合は、 ステップ 3 のアドバイスに従って、ACE アプリ ID を検出して制御します。

ポリシーで ACE アプリ ID を明示的に使用すると、ファイアウォールはコンテンツ配信アプリケーションを処理するのと同じ方法でアプリケーションを処理します。

STEP 2 | ACE を有効にする前に、セキュリティ ポリシー ルールベースを確認して、アプリケーション フィルタを使用するルールを見つけてください。

アプリケーション フィルターでは、タグなどの一致フィルター条件に基づいてアプリケーションが許可されるため、アプリケーションがルールに自動的に追加されます。これらのルールを調べて、各フィルターがどの特定のアプリケーションを許可するか、およびそれらのアプリケーションに誰がアクセスできるかを確認する必要があります。ACE アプリ ID がルール内のアプリケーション フィルタと一致する場合、そのルールでは、SSL および Webブ

ラウジング ルールと同じユーザーが許可されない場合があります。ssl および Webブラウジング ルールでアプリケーションにアクセスしていたユーザーは、そのルールに一致しなくなり、それらのユーザーが明示的なルールで指定されていないため、アプリケーションにアクセスできなくなる可能性があります。

特に多くのルール、アプリケーション、ユーザー グループがある環境では、ビジネス目的で誰がどのアプリケーションを使用する必要があるかを理解することが重要です。たとえば、ルール内のアプリケーション グループで ***Web Apps*** タグを使用すると、タグによって、一致する *ACE* アプリケーションが暗黙的にルールに追加されます。これらの *ACE* アプリケーションは、*SSL* および *Web*ブラウジング ルールに一致しないため、***Web Apps*** ルールで指定されたユーザーのみがアクセスできます。

ルールにアプリケーション フィルタが含まれていない場合は、ACE アプリケーションをルールに明示的に追加していないため、ACE を有効にした後に ACE アプリケーションが既存のルールと自動的に一致する危険はありません。

セキュリティ ポリシー ルールでアプリケーション フィルターを使用する場合、ACE を有効にすると次のようになります。

- 拒否ルールの場合、ルールに一致する ACE アプリケーションはブロックされます。これはまさに、拒否ルールに一致するアプリケーションに対して行うことです。ファイアウォールが ACE なしでは識別できなかった未承認の SaaS アプリケーションをブロックできるようになるため、このルールはより効果的です。
- 許可ルールの場合は、そのルールが許可するアプリケーションを注意深く監視してください。フィルタを使用したアプリケーションの暗黙的な追加は、管理者が特定のアプリケーションを意図的に追加するのではなく、条件に基づいて行われます。最も影響を受けるルールは、**Web App**などの広範なタグに基づくフィルタを含むルールで、ACE とコンテンツ配信される App-ID の両方の大部分に適用されます。

  既存の展開では、*SSL* および *Web*ブラウジング トラフィックを許可するルールがある場合、*ACE* が現在識別しているすべてのアプリケーションを許可していることに注意してください。アプリケーション フィルターを使用して、望ましくないことがわかっている種類のトラフィックをブロックし 、承認するものとブロックするものを評価しながら、残りのアプリケーションを許可し続けます。

ステップ 3、 ステップ 4、および ステップ 5 では、アプリケーション フィルタを使用して ACE アプリ ID をルールに安全に追加する方法を示します。

STEP 3 | アプリケーション フィルタを使用して ACE アプリケーションを明示的に許可すると、制御された方法でアプリケーションを評価できるようになります。

ネットワーク上で必要なアプリケーション タイプを許可するアプリケーション フィルタを作成することは、すべての新しい ACE アプリケーションを定期的に確認してどの特定のアプリ

ケーションを許可するかを決定するよりも簡単です。アプリケーション フィルターを使用すると、同じ種類のアプリケーションを並べて検査し、どのアプリケーションをビジネス目的で許可するかを決定できます。

1. **App-ID Cloud Engine** タグに基づいてアプリケーション フィルタを作成します。これは、すべての ACE アプリ ID (ACE より前に ssl または Webブラウジングとして識別されていたアプリケーション) に一致します。適切なセキュリティ プロファイルとログを含むセキュリティ ポリシー ルールにフィルタをアタッチし、そのルールをセキュリティ ポリシー ルールベースの最後に配置します。これにより、以前のルールで指定されていない限り、ルールがすべての新規および既存の ACE アプリ ID に一致し、許可されることが保証されます。また、ファイアウォールがトラフィックを ACE 許可ルールと比較する前に、ファイアウォールのブロック ルールが確実に有効になります。
2. ACE アプリケーションに慣れてくると、サブカテゴリ、タグ、リスク、特性に基づいてより具体的なアプリケーション フィルタ ルールを作成し、より小さなアプリケーション グループに一致させることができます。これらの許可ルールは 、**App-ID Cloud Engine** タグに基づいて一般的な ACE 許可ルールのすぐ上に配置します。フィルターに一致するアプリケーションを絞り込むと、より類似したアプリケーションを並べて調べて、どのアプリケーションをビジネス目的に許可するかを決定できます。
3. Policy Optimizer の 新しいアプリ ビューアを 頻繁に確認して、ダウンロードされた ACE アプリ ID がセキュリティ ポリシー ルールに一致することを確認し、それらのアプリケーションの可視性を高めます。アプリケーションを評価し、許可するかブロックするかを決定します。

> アプリケーション フィルターを含むルールにユーザーを追加してルールを拡張しないでください。これにより、アプリケーションへの必要以上のアクセスが許可されるためです。ユーザー アクセスを過剰にプロビジョニングするとリスクが増大し、ゼロトラスト ネットワーク アクセスの原則に反します。ビジネス目的でアクセスが必要なユーザーのみを許可します。

STEP 4 | アプリケーション フィルターを使用して、サブカテゴリ、タグ、特性に基づいて、ネットワーク上で望ましくないアプリケーション タイプをブロックします。リスクをブロック フィルター基準として使用しないでください (リスクは、カテゴリまたはサブカテゴリ内の相対的なリスクの評価であり、必ずしも悪意のある使用の評価ではありません)。リスクを考慮して、トラフィックを適切に検査、記録、制御する方法を決定します。

アプリケーション フィルタに基づいてブロックすることは、すべての新しい ACE アプリケーションを定期的に確認して、ネットワーク上で何を行い、何を望まないかを判断するよりも簡単です。アプリケーション フィルターを使用すると、不要とわかっている新しいアプリケーションがファイアウォールによって即座にブロックされます。

1. ネットワーク上で使用したくない ACE アプリケーションのタイプを決定します。これらのアプリケーション タイプに基づいてブロック ルールを作成し、キャッチオール ルールの上に配置します。

2. これらの種類の中に、ネットワーク上で許可する特定のアプリケーションがあるかどうかを確認します。一部のアプリケーションを許可したい場合:
   1. ブロック ルールのクローンを作成します。
   2. **[**アクション**]** を **[**許可**]**に変更します。
   3. 許可するアプリケーションを除くすべてのアプリケーションをルールから削除します。
   4. 許可されたアプリケーションにアクセスする必要があるユーザーを指定し、適切なセキュリティ プロファイルを追加して、ログを構成します。
   5. 新しい許可ルールをブロック ルールのすぐ上に配置して、ブロック ルールに対する例外を作成します。
3. ブロック ルールを監視して、許可する特定のアプリケーションが他にあるかどうかを確認し、それらを既存の許可ルールに追加するか、新しい許可ルールを作成して例外を作成します。

たとえば、ファイル共有アプリケーションは特に危険な場合があります。ビジネス目的で使用するファイル共有アプリケーションを必要なユーザーのみに許可し、トラフィックを検査してログに記録します。セキュリティ ポリシー ルールベースの次のルールでは、 ファイル共有 サブカテゴリに基づくアプリケーション フィルターを使用して、明示的または意図的に許可していないすべてのファイル共有アプリケーションをブロックします。ブロック ルールを監視して、許可するファイル共有アプリケーションがブロックされていないことを確認します。

STEP 5 | アプリケーション フィルターに基づく広範なルールを、アプリケーション グループに基づく狭いルールに変換します。

ルール使用統計 は、環境内でルールがどのように使用されているかを示します。Policy Optimizer を使用してアプリケーション グループ (PAN-OS 10.1 以降) にアプリケーションを追加するか、アプリケーション グループにアプリケーションを手動で追加してより厳格なルールを作成します。

最終的な目標は、アプリケーション フィルターに一致する幅広いアプリケーションを許可するのではなく、承認したアプリケーションのみを許可することです。アプリケーション フィルターを使用してネットワーク上のアプリケーションを検出し、アプリケーション グループを使用して許可するアプリケーションを正確に指定します。Policy Optimizer を使用して、アプリケーション フィルター ベースのルールをアプリケーション グループ ベースのルールに変換するには、次の手順を実行します。

- アプリケーション フィルターに基づいてルールに一致するアプリケーションを調べ、どのアプリケーションを許可するかを決定します。
- アプリケーション フィルターに基づくルールごとに、許可するアプリケーションを選択し、 複製されたルールまたは既存のルールのアプリケーション グループにアプリケーションを追加します。
- アプリケーションをアプリケーション グループに基づいたルールに移動した後、Policy Optimizer と **Reset Rule Hit Counter (**ルール ヒット カウンターのリセット**)**で元のアプリ

ケーション フィルタ ベースのルールを選択します。これ により、新しいアプリケーションのない日数 カウンターがリセットされ、新しいアプリケーションがアプリケーション フィルター ベースのルールに一致する時期を確認できるようになります。

- アプリケーション フィルターに基づいてルールを監視し、 新しいアプリのない日数 カウンターが、ルールで新しいアプリケーションが検出されなくなったことを示すしきい値に達する時期を確認します。しきい値は、環境とアプリケーション フィルターが一致するアプリケーションの種類によって異なります。四半期ごとや年次イベントなど、特定の期間にのみ使用されるアプリケーションを考慮し、それらのアプリケーションが表示されるまで十分な期間フィルタをそのままにしておきます。アプリケーション フィルター ルールがネットワーク上に必要なアプリケーションに一致しない場合は、企業のポリシーに応じてルールを無効にするか削除します。

新しい *ACE* アプリケーションを許可するための包括的なルールとして、ルール ベースの下部にある ***App-ID Cloud Engine*** タグに基づくルールを保持します。アプリケーション フィルタ ベースのルールからアプリケーション グループ ベースのルールに移行すると、すべての新しい *ACE* アプリ *ID* がキャッチオール ルールに一致します。ルールを定期的に調べて、既存のルールおよびアプリケーション グループに追加するアプリケーション、新しいルールが必要なアプリケーション、およびブロックするアプリケーションを決定します。

STEP 6 | **New App Viewer** を頻繁にチェックして、SSL または Webブラウジング アプリケーションとして以前に識別されていた新しい ACE アプリ ID を可視化し、明示的に制御できるようにします。新しい ACE アプリ ID を、SSL または Webブラウジング アプリケーションとしてではなく、ポリシー内で明示的に使用します。

Policy Optimizer の New App Viewerで、ファイアウォールが定期的にダウンロードする新しい ACE アプリ ID を確認します。Policy Optimizer を使用して、既存および新規のアプリケーション グループにアプリケーションを追加したり、既存のセキュリティ ポリシー ルールにアプリケーションを直接追加したりできます 。引き続き Policy Optimizer を使用して、アプリケーション フィルターをアプリケーション グループに変換します。

ポリシーの推奨事項のベストプラクティス

SaaS ポリシー推奨事項 と IoT ポリシー推奨事項 を使用すると、SaaS セキュリティ管理者と IoT セキュリティ管理者はセキュリティ ポリシー推奨事項を作成し、以下に送信できます。

- PAN-OS ファイアウォールと Panorama (SaaS および IoT ポリシーの推奨事項)。
- Panorama マネージド Prisma アクセス (SaaS および IoT ポリシーの推奨事項)。
- クラウド管理型 Prisma アクセス (SaaS ポリシー推奨のみ)。

IoT や *SaaS* ポリシー推奨などのクラウドベースのサービスは、クラウド接続が必要なため、エアギャップ環境では使用できません。

エアギャップ環境では、*IoT* セキュリティのために、クラウド サービスと対話し、ポリシーの推奨事項を受け取るための管理エンジンとして *Panorama* を使用することを検討してください。次に、クラウド接続を持たない管理対象ファイアウォールに推奨事項をプッシュします。このソリューションは、ポリシー推奨自体にのみ適用されます。デバイスから *IP* へのマッピングなどの機能では、管理対象デバイスのクラウド接続が依然として必要です。

SaaS ポリシー推奨事項は、PAN-OS および Prisma Access での未承認の SaaS アプリケーションを制御します。IoT ポリシー推奨事項は、PAN-OS および Panorama マネージド Prisma アクセスのアンマネージド ネットワーク デバイスを制御します。彼らのワークフローには多くの類似点があります。

要件:

- SaaS ポリシーの推奨事項:
  - SaaS セキュリティ インライン ライセンス

    SaaS Security Inline ライセンスには、ポリシー推奨用に数千の SaaS App-ID を提供する App-ID Cloud Engine (ACE)が含まれています。SaaS ポリシー推奨には ACE の展開が必要です。
  - PAN-OS および Panorama Managed Prisma Access の場合は PAN-OS 10.1 以降。
  - エンタープライズデータ損失防止 (DLP) は、 データ損失防止のベストプラクティスを実装し、データを可視化します。
  - User-ID 用に Azure AD を設定して、ポリシー ルールの推奨事項でユーザーを指定します (User-ID がないとユーザーベースのポリシー ルールを作成できません)。
- IoT ポリシーの推奨事項:
  - IoT セキュリティ ライセンス。
  - IoT セキュリティの前提条件。
  - PAN-OS の適切なサポート および/または Panorama Managed Prisma Access のサポートを確認します。
  - IoT デバイスを制御する各ゾーンで Device-ID を 有効にします。(IoT セキュリティにとっての Device-ID は、SaaS セキュリティにとっての User-ID と同じです。Device-ID は、IoT セキュリティの「誰」に相当します。)

Panorama は、適切なライセンスを持つファイアウォールにのみ *SaaS* および *IoT* ポリシーの推奨事項をプッシュできるため、*IoT* および *SaaS* ポリシーの推奨事項を使用するファイアウォールにこれらをインストールする必要があります。管理対象デバイスに適切なライセンスがない場合、プッシュは失敗します。

ライセンスに加えて、ベストプラクティスに従って適切に機能するには、IoT と SaaS の両方のポリシー推奨事項に次のものが必要です。

- SaaS または IoT ポリシーの推奨事項を使用する各アプライアンス上の有効なデバイス証明書。
- トラフィックを可視化するための Cortex Data Lake (CDL) への接続。
- 各セキュリティ ポリシー ルールの推奨事項で設定された CDL へのログ転送。SaaS セキュリティの場合は、少なくともトラフィック ログ、URLフィルタリング ログ、および脅威ログを転送します。

SaaS ポリシーの推奨事項は、未承認のアプリケーションを制御するのに役立ちます。

認可された SaaS アプリケーションを保護するには、SaaS Security APIを使用します。*SaaS* セキュリティ *API* は、 サポートされている一般的に認可された SaaS アプリケーション にセキュリティを提供し、 それらの SaaS アプリケーションのポリシーを管理できるようにします。

- Policy Recommendation 推奨ポリシー—政策を推奨する前に理解しておくべき重要な考え方。
- ポリシー推奨ワークフロー—SaaS および IoT のワークフローとワークフローのベストプラクティス。

Policy Recommendation 推奨ポリシー

SaaS と IoT のポリシー推奨には、ワークフローと目標において多くの類似点があります。PAN-OS と Prisma Access におけるポリシー推奨のワークフローと思考プロセスにも多くの類似点があります。ルールのコンポーネントのベストプラクティスをより深く理解するためセキュリティ ポリシー ルールのベストプラクティスをレビューします。

クラウドマネージド *Prisma Access* は、*IoT* ポリシー推奨をサポートしていません。

SaaS セキュリティと IoT セキュリティの管理者は、ポリシーの推奨事項を PAN-OS と Prisma Access に送信します。PAN-OS 管理者は、SaaS ポリシーの推奨事項 と IoT ポリシーの推奨事項を PAN-OS および Panorama Managed Prisma Access にインポートします。クラウド管理 Prisma Access 管理者は、SaaS ポリシーの推奨事項を クラウド プラットフォームにインポートします。多くの場合、さまざまな管理者が協力してポリシー ルールを推奨および実装する必要があるため、管理者間の良好なコミュニケーションが重要です。

IoT ポリシー推奨事項の一般的なベストプラクティスには次のものが含まれます。

- 検出されたデバイスが ネットワーク上に属しているかどうかを確認します。
- デバイスに対して表示 される検出されたアプリケーションが それらのデバイスに適切であることを確認してください。

- 検出された デバイスの脆弱性を理解します。
- IoT セキュリティがデバイスに関する十分なデータを収集し、高い信頼性でデバイスを識別できるよう十分な時間を確保します。

SaaS ポリシー推奨事項の一般的なベストプラクティスは次のとおりです。

- ネットワーク上に含めるべきアプリケーションとアプリケーションの種類を理解してください。認可されたアプリケーション、許容されたアプリケーション、および認可されていないアプリケーションとアプリケーションの種類の正式なリストを作成し、アプリケーションを可視化するときにアプリケーションに適切にタグを付けます。承認されていないアプリケーションの使用状況データを表示し、フィルターを使用してアプリケーションを誰がどのように使用しているかを確認します。可視化 ツールを使用して、検出されたアプリケーションを表示し、検出されたアプリケーションにタグ付けを行います。
- ファイル内で探したいデータを理解して、ポリシー ルールの推奨事項に適した DLP プロファイルを作成できるようにします。
- ほとんどの SaaS ポリシー ルールの推奨事項は、トラフィックをブロックするためのものです。最小特権アクセスの原則を SaaS アプリケーションに適用することは、制御する必要がある SaaS アプリケーションが数万あるため、コンテンツ配信アプリケーションのみに適用する場合よりも複雑になります。SaaS ポリシーの推奨事項が厳しすぎる場合、ビジネス アプリケーションに影響を与える可能性があります。ブロックする前に、ブロックするアプリケーションとアプリケーションの種類を必ず理解してください。

  フィルターを使用して、ファイル転送や CMS アプリケーションなどの高リスクのカテゴリに焦点を当て、どのアプリケーションの使用率が最も高いかを確認します。まず、これらのカテゴリとサブカテゴリに焦点を当てます。
- 可能な限り多くのコンテキストベースのコンポーネントを使用して、最小特権アクセス ポリシーの推奨事項を作成します。Cloud Identity Engine (CIE) を使用して User-ID を実装し (Azure AD が必要)、ユーザーとグループに必要なアクセス例外を作成します。Enterprise DLP を使用して、機密データの損失を防ぎます。
- クラウド管理 Prisma アクセスの場合、組織の管理ポリシーで許可されている場合は、SaaS Security アプリをクラウド管理コンソールに追加します。スタンドアロン アプリを使用する代わりに、クラウド管理コンソールを使用して SaaS ポリシーの推奨事項 (および SaaS セキュリティやその他のクラウド アプリ) を管理すると、次の利点が得られます。
  - すべてのクラウド セキュリティ要素を、さまざまなアプリ インターフェースからではなく、単一のインターフェースから管理します。
  - 1 人の管理者が、Prisma Access ルールベースへのルールの追加を含む、すべての SaaS ポリシー推奨アクションを実行できます。スタンドアロン アプリで管理する場合は、ポリシー

の推奨事項を作成できますが、ルールを Prisma Access に追加するには、別のアプリに切り替えるか、別の管理者に引き継ぐ必要があります。

クラウド管理コンソールで *SaaS* セキュリティとエンタープライズ *DLP* を使用するには、コンソールで Web セキュリティを 有効にする必要があります。*(*これは無料の機能であり、サブスクリプションではありません。*)*

事前定義されたポリシー推奨事項 を使用したり、ユーザー作成のポリシー推奨事項を作成したりすることによって、SaaS ポリシー推奨事項を作成できます。

ポリシー推奨ワークフロー

このワークフローは、IoT セキュリティ、SaaS セキュリティ アプリ (PAN-OS、Panorama マネージド Prisma アクセス) とクラウド管理コンソール (クラウド マネージド Prisma アクセス) の両方に有効です。各ステップには、どの管理者が関与しているかが示されています。各管理者にとって、ポリシーの推奨事項に関与する他の管理者の責任を理解すると役立ちます。

STEP 1 | (すべての管理者) ポリシー推奨のさまざまな部分を管理する管理者間でオープンなコミュニケーションを確立します。

ポリシーの推奨では、多くの場合、さまざまな管理者が協力して、新しい SaaS セキュリティおよび IoT セキュリティ ポリシー ルールを推奨、インポート、PAN-OS または Prisma Access ルールベースに統合する必要があります。IoT セキュリティまたは SaaS セキュリティの管理者がポリシーの推奨事項を Panorama、ファイアウォール、または Prisma Access の管理者に引き渡すときに、良好な通信を確保するプロセスを考案します。ハンドオフは、IoT セキュリティまたは SaaS セキュリティの管理者が新しいルールを作成するか、既存のルールを変更するか、ルールを削除して、ルールを有効にする (SaaS セキュリティで送信する) かアクティブにする (IoT セキュリティ) 後に発生します。

管理ワークフローは次のとおりです。

1. **SaaS** セキュリティ管理者は、 新しいルールの推奨事項を作成し、アプリケーション、ユーザー/ユーザー グループ、および DLP プロファイルを追加して、アクションを設定します。ルールの推奨事項を確認し、PAN-OS、Panorama Managed Prisma Access、または Cloud Managed Prisma Access に送信します。SaaS Security 管理者のコラボレーションとオーサリングに関するガイドラインを確認してください。

   IoT セキュリティ管理者は 、自動生成されたルール推奨事項を評価し、必要に応じて修正し、ポリシー セット (同じデバイス プロファイル内の IoT デバイスからのトラフィックに基づくルール推奨事項のグループ) を作成し、PAN-OS および Panorama Managed Prisma Access に送信します。

2. **PAN-OS** および **Prisma Access** 管理者は、SaaS および IoT ポリシーの推奨事項をインポートします。ルールの推奨事項を評価してインポートし、セキュリティ プロファイル グループやその他のオブジェクトをルールに追加します。また、セキュリティ ポリシー ルールベース内のルールも順序付けします。Panorama がポリシーの推奨事項をファイア

ウォールと Prisma Access にプッシュすると、ファイアウォールと Prisma 管理者は推奨ルールをインポートします。

管理者は、適切なオブジェクトを推奨ルールに追加し、それらのルールの目的を理解するために連絡を取る必要があります。

クラウド管理 *Prisma Access* の場合、特に管理者がクラウド管理コンソールで両方のアプリを管理する場合、同じ管理者が *SaaS* ポリシーの推奨事項と *Prisma Access* の業務の両方を処理する場合があります。

3. **SaaS** および **IoT** セキュリティ管理者は、ルールの推奨事項を更新または削除し、変更を PAN-OS または Prisma Access に送信します。

   PAN-OS および **Prisma Access** 管理者は、ルールの更新または削除を確認し、更新されたルールをインポートするか、PAN-OS または Prisma Access からルールを削除します。

推奨ルールの目的、ルール更新の目的、ルールが削除される理由をすべての関係者が理解するには、管理者間のコミュニケーションが非常に重要です。管理者間のコミュニケーションにより、SaaS および IoT ポリシーの推奨事項が、管理者がその存在に気づいてルールベースにインポートするのを待って PAN-OS または Prisma Access に残らないようにすることができます。

STEP 2 | (*SaaS* セキュリティおよび *IoT* セキュリティ管理者) SaaS セキュリティ管理者は、未承認の SaaS アプリケーションのリスクを評価する必要があり、IoT セキュリティ管理者は、ネットワーク上の管理対象外デバイスの種類とその動作を説明するデバイス プロファイルを理解する必要があります。

IoT セキュリティは、ネットワーク上の管理対象外のデバイスを自動的に学習し、同様のデバイスのセットごとにデバイス プロファイルを作成します。プロファイルはデバイスの特性を説明します。

ネットワーク上の SaaS アプリケーションと IoT デバイスについてよく理解してください。

- SaaS - ポリシー推奨のためにアプリケーションを分析する前に、少なくとも 7 営業日のデータを待ちます。アプリケーションとそのビジネス用途を理解するために十分なデータを収集します。

  IoT - デバイス プロファイルのリストを監視して、どのプロファイルがポリシー推奨の対象となるかを確認します。デバイス プロファイルの信頼度評価が 90% に達すると、ポリシーの推奨事項を作成できます。これは、デバイスの動作について高い信頼性があることを示します。一部のデバイスでは生成されるトラフィックが少なく、高い信頼性評価を達成するまでに時間がかかる場合があります。IoT セキュリティが 90% の信頼性評価を達成するのに十分なデータを収集する時間を確保します。

- SaaS - ユーザーが特定の SaaS アプリケーションを使用する方法と理由、およびそれらのアプリケーションを許可するビジネス上の理由があるかどうかを理解します。

  IoT - 検出されたデバイスがネットワーク上に属しているかどうかを理解します。ビジネスが銀行業の場合、ネットワーク上に医療機器が表示されると、問題が発生している可能性があります。

- SaaS - リスク許容度に基づいて、SaaS アプリケーションの セキュリティとプライバシー、ID アクセス管理、およびコンプライアンスの属性 を評価します。

  IoT - 医療環境において、医療 IoT デバイスの コンプライアンス リスク を評価します。

- SaaS - 認可されたアプリケーション、許容されたアプリケーション、および認可されていないアプリケーションにタグ を付けて分類します。

STEP 3 | (*SaaS* セキュリティ管理者) 事前定義された SaaS ポリシーの推奨事項を構成します。(IoT セキュリティ管理者は ステップ 5に進みます)

事前定義された SaaS ポリシー ルールの推奨事項により、 アプリケーション アクセス、個人アカウント アクセス、コンテンツの共有とアクセスがブロックされ、適切なユーザーに読み取り専用アクセスが強制されます。事前定義された推奨事項にアプリケーションを追加すると、SaaS アプリケーションのロックダウンを開始する簡単な方法です。

クラウド管理コンソールで *SaaS* セキュリティとエンタープライズ *DLP* を使用するには、コンソールで Web セキュリティを 有効にする必要があります。*(*これは無料の機能です*)*

クラウド管理コンソールでは、同じ管理者が *SaaS* ポリシーの推奨事項を作成し、 それを Prisma Access にインポートできる場合があります。

1. 事前定義されたルールを選択します。(クラウド管理コンソールの検出されたアプリ > ポリシーの推奨事項 、または SaaS セキュリティ コンソールの 可視性 > セキュリティ ルール 。)
2. アプリケーションを選択してルールに追加します。ルールがすべてのユーザーに適用されない場合は、ユーザーとユーザー グループを追加します。ブロックする前に、ブロックする予定のアプリケーションとアプリケーションの種類を必ず理解し、特定のアプリケーションをビジネス目的で誰が使用する必要があるかを理解してください。

   ファイル共有、コンテンツ管理、コラボレーションおよび生産性アプリケーションなど、最初にリスクの高いアプリケーションの種類に焦点を当てます。ファイル共有サイトへのアップロードを減らし、ビジネス目的でアップロードする必要があるユーザーのみが、ビ

ジネス目的で使用されるファイル共有アプリケーションのみにアクセスできるようにします。

3. Enterprise DLP ライセンス (ベストプラクティス) をお持ちの場合は、 サポートされている DLP アプリケーションの事前定義プロファイルなど、DLP プロファイルを追加してトラフィックの機密情報を検査し、不正アクセスから保護します。
4. ルールが希望どおりの動作を行うことを確認します。
5. デフォルトのルールを保存します 。
6. ルールを有効にして PAN-OS または Prisma Access に送信します。PAN-OS または Prisma Access 管理者がルールをインポートするには、ルール を有効にする 必要があります。

   有効なルールについては、SaaS ポリシーの推奨事項の確認、評価、インポートを担当する管理者と連絡してください。

STEP 4 | (*SaaS* セキュリティ管理者) ユーザー定義の SaaS ポリシーの推奨事項を構成します。(IoT セキュリティ管理者は ステップ 5に進みます)

[検出されたアプリケーション] ビュー のフィルターを使用すると、アプリケーションとその使用状況メトリックを検索し、アプリケーションをブロックするか許可するかを理解するのに役立ちます。ファイル転送、コンテンツ管理、コラボレーションおよび生産性アプリケーションなど、最もリスクの高いアプリケーション カテゴリに焦点を当てます。使用率 も高い 高 リスクの アプリケーションは、潜在的なリスクが最も高くなる傾向があります。アプリ

ケーションを選択して、そのアプリケーションを使用するユーザーとその使用方法を確認します。

ポリシーの推奨事項を構成して送信すると、*PAN-OS* と *Prisma Access* は、添付された *HIP* プロファイル、タグ、および アプリケーション グループ を自動的に作成します。ターゲット ファイアウォールで *Enterprise DLP* ライセンスを持っている場合は、*DLP* プロファイルも作成されます *(*そうでない場合、送信は失敗します*)*。*SaaS Security* 管理者が他のタイプのプロファイルをルール推奨に追加し、それらのプロファイルがファイアウォールにまだ存在していない場合、送信は失敗します。添付されたプロファイル オブジェクトがファイアウォール上に存在する場合、送信は成功します。*(PAN-OS* または *Prisma Access* 管理者は、インポートされたルールの推奨事項にプロファイルを追加できます。*Cloud Managed Prisma Access* では、プロファイル グループのみを追加できます。個々のプロファイルは追加できません。*)*

プロファイルに適切なライセンスは、*SaaS* ポリシーの推奨事項をインポートするすべてのファイアウォールに存在する必要があります。

CIE のユーザー グループは組織全体で一貫しています。*CIE* を使用しない場合、または *CIE* から同期できない場合は、*SaaS* セキュリティで ユーザーとグループの 構成を使用できず、ユーザーに基づいて *SaaS* ポリシーの推奨事項を設定することはできません。ベストプラクティスは、*CIE* を使用し、ビジネス目的でアプリケーションにアクセスする必要があるユーザーに基づいてアプリケーション ポリシーを作成することです。

SaaS セキュリティとエンタープライズ *DLP* を強制するには、クラウド管理コンソールで Web セキュリティ を有効にする必要があります。*(*これは無料の機能です*)*

クラウド管理コンソールでは、同じ管理者が *SaaS* ポリシーの推奨事項を作成し、 それを Prisma Access にインポートできる場合があります。

ベストプラクティス SaaS ポリシーの推奨事項を構成するには、次の手順を実行します。

1. 新しい SaaS セキュリティ ポリシーの推奨事項を作成します。
   - SaaS セキュリティ コンソール:可視性 > セキュリティ ルール > 新しいルールの作成
   - クラウド管理コンソール:検出されたアプリ > ポリシーの推奨事項 > ポリシーの追加
2. ルールの Name(名前) と description(説明)を指定する際のベストプラクティスに従ってください。
3. アプリケーションをルールに追加します。

カテゴリ、リスク、機能のフィルターを使用して、SaaS アプリケーションを検索します。フィルター結果から直接アプリケーションをルールに追加します。最初に、最もリスクが高く、使用量が最も多いアプリケーションに焦点を当てます。

4. 検出する ユーザー アクティビティ を選択します。ルールに対して選択されたすべてのアプリケーションは、選択されたユーザー アクティビティをサポートする必要があります。アプリケーションがアクティビティをサポートしていない場合、インターフェースはエラーを返します。
5. ルールの残りのパラメーターを構成します。
   - ユーザーとグループ - SaaS ポリシー推奨事項でユーザーとグループを指定するには、CIE を使用して同期する必要があります。
   - デバイス ポスチャ — ルールのアプリケーションにアクセスできるデバイスのタイプを指定します。ルールが PAN-OS または Prisma Access にインポートされると、デバイス ポスチャはモバイル デバイス用のホスト情報プロファイル (HIP) オブジェクトを自動的に作成します。
   - データ プロファイル- この機能を使用するには、SaaS セキュリティと対象のファイアウォールで Enterprise DLP ライセンスが必要です。Enterprise DLP サブスクリプションを使用すると、 特定の DLP プロファイル のルールを作成し、プロファイルに一致するデータが含まれる場合にのみアプリケーションをブロックできます。
   - 応答— ルールに一致するトラフィックを許可 または ブロックします 。ほとんどの推奨事項は、オーバープロビジョニング アクセスを防ぐためのブロック ルールです。
6. ルールが希望どおりの動作を行うことを確認します。
7. ルールを保存します。
8. ルールを有効にして PAN-OS または Prisma Access に送信します。PAN-OS または Prisma Access 管理者がルールをインポートするには、ルール を有効にする 必要があります。

   有効なルールについては、SaaS ポリシー推奨事項の確認、評価、インポートを担当する PAN-OS または Prisma Access 管理者と連絡してください。

   SaaS ポリシー ルールの作成に関する推奨事項では、ワークフローの詳細が説明されています。

STEP 5 | (*IoT* セキュリティ管理者) IoT セキュリティ アプリで IoT ポリシーの推奨事項 (PAN-OS および Panorama Managed Prisma Access のみ) を構成します。

IoT セキュリティは、IoT セキュリティがプロファイルの信頼スコア (デバイスの識別において IoT セキュリティが持つ信頼レベル) が 90% 以上に達すると 、デバイス プロファイルに属するデバイスの動作に基づいて IoT ポリシーの推奨事項を 自動的に生成します。IoT セキュリティがデバイスに関するより多くの情報を収集するにつれて、信頼度スコアは時間の

経過とともに上昇します。自動生成されたルールは、Panorama、ファイアウォール、または Prisma Access に送信する前に編集できます。

IoT セキュリティは、*PC*、スマートフォン、タブレットなどの *IT* デバイスに対するポリシーの推奨事項を提供しませんが、*IoT* セキュリティはそれらのデバイスを識別します。

自動ポリシー推奨を使用して、複数の IoT セキュリティ テナントにわたる同じデバイス プロファイル内の IoT デバイスの動作に基づいてポリシー ルール セットを作成します。ポリシー ルール セットには、デバイス プロファイル内のデバイスを制御するために選択したポリシー ルールの推奨事項が含まれています。

1. 次の 2 つの方法のいずれかで、新しい IoT セキュリティ ポリシーの推奨事項を作成します。
   - 「プロファイル」ページに移動し、プロファイル名の上にカーソルを置き、ポップアップで 「ポリシー セットの作成」 をクリックします。
   - プロフィール > **<profile-name>** > **[**動作**]**、**[**アウトバウンド動作**]**、**[**ポリシーの作成**]**の順に選択して、**[**次へ**]**をクリックします。
2. **[**ポリシーの選択**]**には、デバイスが使用するアプリケーションを含む、選択したデバイス プロファイルに対して自動的に生成されたポリシーの推奨事項が表示されます。
   1. リストに表示されるアプリケーションがデバイスに適切であることを確認してください。たとえば、プリンターやカメラを見ているときに iTunes アプリケーションが表示されるべきではありません。リストに予期しないアプリケーションが含まれている場合は、デバイスが危険にさらされている可能性があります。

      デバイスとデバイス プロファイルを把握して、それらを管理するための適切な推奨事項を作成できるようにします。
   2. 発生したアラートを確認します。特にアラートの重大度が高いかクリティカルである場合は、ポリシー セットに追加する前に、アラートの数が多いアプリケーションを調査してください。
   3. デバイスに適用するポリシーを選択します。これらのポリシーは、デバイス プロファイルのポリシー セットに含まれています。

      ポリシー セットに含めたいアプリケーションが表示されない場合は、 ルールを追加して アプリケーションと宛先タイプを手動で選択し、ルールを 作成します 。
   4. デフォルトでは、ルールはデバイス プロファイルのトラフィックで検出されたすべての **(Any(**任意**))** 宛先に適用されます。アプリケーションの宛先を制限する場合は、任意

の > 宛先]をクリックし、**[Allow any destination (すべての宛先を許可)]** を オフに切り替え、リストで許可したくない宛先のチェックを外します。

5. ポリシー セットに必要なルールが含まれていることを確認したら、**[次へ]**を選択します。

3. ファイアウォール構成 > ポリシーの構成で、必要に応じて自動生成された推奨事項を変更します。ポリシー構成には、 選択したアプリケーションが表示されます。
   - ベストプラクティスに従って、ポリシー セットの Name(名前) と description(説明)を指定します。名前がルールの動作を識別し、説明がルールの目的を示していることを確認してください。
   - アプリケーションが非標準ポートを使用しないようにするには、 サービス をアプリケーションの デフォルト のままにしておきます。これは、回避的で潜在的に悪意のある動作の兆候です。
   - セキュリティ プロファイルとセキュリティ プロファイル グループ、ログ転送プロファイル、およびその他のオブジェクトを、IoT セキュリティ アプリではなく Panorama またはファイアウォールに追加します。
4. ポリシーセットを確認します。希望どおりに構成されていることを確認したら、ポリシーセットを作成します。これにより、ポリシー セットも保存されます。
5. ポリシー セットをアクティブ化して、ポリシー ルールの推奨事項を Panorama および個々のファイアウォールにインポートできるようにします。

   有効なルールについては、IoT ポリシー推奨事項の確認、評価、インポートを担当する PAN-OS または Prisma Access 管理者と連絡してください。

ワークフローの詳細については、「IoT ポリシー セットの作成」を参照してください。

STEP 6 | (Panorama およびファイアウォール管理者) (SaaS セキュリティの Cloud Managed Prisma Access 管理者のみ) ポリシー ルールの推奨事項を評価、インポートし、必要に応じて変更します。

クラウド管理コンソールを使用すると、すべてのクラウド アプリを *1* か所で管理できるため、*Cloud Managed Prisma Access* 管理者は、*SaaS* セキュリティ ポリシーの推奨事項を作成した管理者と同じである可能性があります。

ルールをインポートする前にすること。

- Panorama、ファイアウォール、クラウド管理コンソール上に セキュリティ プロファイル グループ を作成し、インポートされた SaaS セキュリティおよび IoT セキュリティ ポリシーの推奨事項に適用できるようにします。少なくとも、ほとんどのトラフィックに対して警告を発し、可用性を維持するために既知の悪意のあるトラフィックをブロックするプロファイル グループを作成します。時間が経つにつれ、ポリシーの推奨事項をよりよく理解できるようになり、 セキュリティ プロファイルのベストプラクティス に従って、重要

なアクセス機能を危険にさらすことなく、プロファイル グループを可能な限り厳格にしてください。ビジネス アプリケーションとデバイス。

SaaS プロファイル グループの場合は、アプリケーションの種類を理解し、アプリケーションのユーザーを理解して、どのプロファイルを使用するか、最初にどの程度厳密にする必要があるかを決定します。

IoT プロファイル グループの場合、デバイスとデバイス プロファイルを把握して、それらを管理する適切なセキュリティ プロファイル グループを作成できるようにします。ルール内のアプリケーションの意味を理解して、適切なセキュリティ プロファイルをグループに適用できるようにします。

セキュリティ プロファイル グループを作成するときは、IoT セキュリティ管理者や SaaS セキュリティ管理者に相談して、セキュリティ プロファイル グループが IoT および SaaS ポリシーの推奨事項に適していることを確認してください。

- IoT セキュリティの展開では、IoT デバイスを制御する各ゾーンで Device-ID を有効にします。Device-ID は IoT デバイスにとって、User-ID はユーザーにとって、App-ID はアプリケーションにとってのようなものであり、一意の識別子です。Device-ID が有効になっていないゾーンでは、IoT デバイスにセキュリティ ポリシーを適用できません。
- SaaS ポリシーの推奨には、数万の SaaS アプリケーションを識別する App-ID Cloud Engine (ACE) が必要です。これにより、それらを制御するセキュリティ ポリシーを作成できます。ACE では、Cortex Data Lake へのログ転送が必要です。CDL プロファイルを作成するときは、 ログ転送のベストプラクティス に従ってください。

  セキュリティ ポリシー ルールで *ACE App-ID* を使用する場合、ルールが *1* 人のユーザーまたはユーザー グループにのみ適用される場合でも、ファイアウォールはすべてのユーザーに *ACE App-ID* を強制します。*(*ポリシーで *ACE App-ID* を使用すると、ファイアウォールはコンテンツ提供の *App-ID* を適用するのと同じ方法で *App-ID* を適用します。*)*

SaaS および IoT ポリシーの推奨事項をインポートするには:

1. インポートされたルールを定期的に確認します。IoT または SaaS ポリシーの推奨事項ページを更新して、最新のポリシー推奨事項が表示されていることを確認します。
   - Panorama：**Panorama** > ポリシー推奨 > **SaaS** または **Panorama** > ポリシー推奨 > **IoT**。
   - ファイアウォールデバイス > ポリシー推奨 > **SaaS** または デバイス > ポリシー推奨 > **IoT**。
   - クラウド管理型 Prisma アクセス (SaaS ポリシー推奨のみ):**[**ポリシーの推奨事項**] [** > **Web** セキュリティ > **Web** アクセス ポリシー > の管理を選択し、**[**ポリシーの推奨事項**]** タブを選択して、 新しい **SaaS** ルールの推奨事項を表示します。
2. 新しいルールを選択して評価します。インポートされたルール内のすべてのオブジェクト、アドレスなどが意味をなすものであることを確認してください。推奨事項に不明な点

がある場合は、IoT セキュリティ管理者または SaaS セキュリティ管理者に相談して、ルールとそのコンポーネントの目的を確実に理解してください。

SaaS ポリシー ルールの推奨事項については、アプリケーションへのユーザー アクセスが広すぎないことを確認してください。

3. ルールのインポート プロセスでは、ルールを変更したり、セキュリティ ポリシー ルールベースに配置したりできます。インポートするルールを 1 つまたは複数選択し、次の操作を行います。

   - Panorama および PAN-OS ファイアウォール:インポート ポリシー ルール。

     一度に最大 *10* 個の *IoT* ポリシー ルールをインポートできます。

   - クラウド管理型 Prisma アクセス (SaaS ポリシー推奨のみ):アクション > インポート。

     セキュリティおよびログ転送プロファイルを追加し、ルールを評価し、セキュリティ ポリシー ルールベースでの順序を選択する次の手順を完了するまで、ルールのインポートを終了しないでください。

   ルールをインポートすると、PAN-OS と Prisma Access はポリシー ルール内にルールのオブジェクトの一部を自動的に作成します。

   - IoT ポリシーの推奨事項をインポートすると、IoT デバイス プロファイルに基づいて、デバイスから IP へのマッピングを含むデバイス オブジェクトが自動的に作成されます。

     Panorama がデバイス オブジェクトをインポートし、管理対象ファイアウォールにプッシュした後、ファイアウォールはデバイスから *IP* へのマッピングをクラウドから直接プルダウンします。*Panorama* は、デバイスから *IP* へのマッピングの更新には関与しません。

   - SaaS ポリシーの推奨事項をインポートすると、必要な HIP プロファイル、タグ、アプリケーション グループが自動的に作成されます。Enterprise DLP プロファイルの場合、ターゲット デバイスには Enterprise DLP ライセンスが必要です。他のプロファイルは、ターゲット デバイスにすでに存在する場合にのみインポートできます。

4. 各ルールにセキュリティ プロファイル グループを追加します。

   個々のプロファイルの代わりにプロファイル グループを使用すると、より速く簡単になり、ルールからプロファイルを誤って省略することを防ぎます。また、主にアラートを生

成するプロファイル グループから始めて、SaaS アプリケーションや IoT デバイスの経験を積むにつれて、より厳格なプロファイル グループに簡単に置き換えることもできます。

SaaS アプリケーションと IoT デバイス ルールへのプロファイルの適用は次のように異なります。

- **SaaS** セキュリティ ポリシー ルールの推奨事項:
  - PAN-OS および Panorama マネージド Prisma アクセス- 高度な脅威防御 と 高度な URL フィルタリングの ベストプラクティス プロファイルを SaaS アプリケーション トラフィックに適用します。
  - クラウド管理 Prisma アクセス - セキュリティ プロファイル グループをポリシーの推奨事項に適用できますが、個々のセキュリティ プロファイルは適用できません。セキュリティ プロファイルをプロファイル グループに追加し、そのグループをルールに適用します。

    クラウド マネージド Prisma アクセスのベストプラクティス セキュリティ プロファイルの推奨事項は、*PAN-OS* および*Panorama* マネージド *Prisma* アクセスの推奨事項とは若干異なります。
- **IoT** セキュリティ ポリシー ルールの推奨事項— 悪意のある動作を防ぐために、セキュリティ プロファイルがデバイスに適切であることを確認します。IoT セキュリティ管理者と協力して、 デバイス プロファイルに表示されるさまざまなデバイスの動作とアラートを理解します。動作とアラートに基づいてプロファイルを IoT ポリシーの推奨事項に適用します。脆弱なメーカー認証情報、危険な URL への接続、古いウイルス対策、不正なデバイスへのアクセスの許可、安全でないプロトコル、EOL オペレーティング システムなど、IoT デバイスに共通する弱点を探します。また、パッチが適用されていないデバイスやパッチが適用できないデバイスも探します。パッチが当てられる。
  - 脆弱性保護プロファイルとスパイウェア対策プロファイル (コマンド アンド コントロール マルウェアを防ぐため) をすべてのデバイスに適用します。
  - デバイスにインターネットへの送信トラフィック、特に不明な宛先への送信トラフィックがある場合は、高度な URL フィルタリングと高度な脅威防御を適用します。デバイスがファイルを送信できる場合は、高度な WildFire プロファイルとファイル ブロック プロファイルを追加します。
  - デバイスにサーバー ポートがあり、受信接続を受け入れる場合は、ファイル ブロック、高度な WildFire、および高度な脅威防御プロファイルに加えて、DoS 保護を適用します。

5. 各ルールにログ転送プロファイルを追加します。
   - IoT ポリシーの推奨事項については、**IoT** セキュリティのデフォルト プロファイル - **EAL** 有効の 事前定義ログ転送プロファイルを追加します。これにより、 拡張アプリケーション ログなど、IoT セキュリティに必要なすべてのログ タイプが提供されます。

- SaaS ポリシーの推奨では、ACE が SaaS アプリケーションを識別する必要があります。ACE では CDL へのログ転送が必要なため、SaaS アプリケーションに基づくセキュリティ ポリシー ルールでも CDL へのログ転送が必要です。

  ルールをインポートした後、Policy Optimizer の セキュリティ サービスのログ転送を 使用して、ログ転送プロファイルを複数のルールに一度に適用し、ログ転送プロファイルが添付されていないセキュリティ ポリシー ルールを特定できます *(*フィルタで ***[None(***なし***)]*** を選択します*)*。

6. Panorama および Cloud Managed Prisma Access で、ルールが事前ルールであるか事後ルールであるかを選択します。(スタンドアロン ファイアウォールには適用されません。)

   ルールを評価する優先順位は、事前ルール、次に展開固有のルール、次に事後ルールです。Cloud Managed Prisma Access の事前ルールと事後ルールは、共有設定フォルダーに存在します。Panoramaの事前ルールと事後ルールは、 「**Policies(**ポリシー**)** > **Security (**セキュリティ**)**」にあります。Panorama では、ルールのデバイス グループを指定できます。

7. インポートされたルールがセキュリティ ポリシー ルールベースで適用するルールを選択します。ルールベースのベストプラクティスに従ってください。

   [ルールの選択なし***]***を選択しないでください。これにより、ルールがセキュリティ ポリシー ルールベースの先頭に配置されます。多くの場合、ルールベースの先頭に新しいルールを置くのは間違った場所です。たとえば、新しい許可ルールは、既知の悪意のあるトラフィックをブロックする重要なルールの対象になりません。新しいブロック ルールは、アプリケーションの正当なユーザーに対する許可ルールの後に配置されない場合、正当なユーザーのアクセスをブロックする可能性があります。ルールベース内で各ルールを適切に順序付けします。

8. ルールを確認し、問題がなければインポートします。

   - クラウド管理型 **Prisma** アクセス—インポート。
   - **Panorama** ファイアウォールとスタンドアロン ファイアウォール—**OK**。

     ルールをインポートした後、Panorama 管理者はルールを管理対象ファイアウォールにプッシュし、ルールがファイアウォールでアクティブになる前にファイアウォール管理者はルールをインポートする必要があります。最新の推奨事項を確認するには、デバイス > ポリシー推奨事項 > **IoT** または デバイス > ポリシー推奨事項 > **SaaS** を更新します。

     ファイアウォール管理者は、ルールをインポートした後に変更する必要がある場合があります。ファイアウォール管理者は、ルールの目的がわからない場合

は、Panorama、SaaS セキュリティ、または IoT セキュリティの管理者に確認する必要があります。

セキュリティ ポリシー ルールベースをチェックして、ルールが正しい順序になっていることを確認してください。

9. (IoT セキュリティのみ) ルールをインポートした後、 デバイス オブジェクト を表示して、デバイスの属性フィルターを確認します。

   セキュリティ ポリシーで IoT デバイス属性を使用して、デバイスをより適切に識別します。IoT ポリシー ルールをインポートすると、デバイスに関連付けられた属性が自動的にインポートされ、 デバイス IDが作成されます。IoT デバイスにとっての Device-ID は、人間にとっての User-ID と同じです。デバイス属性は 6 つありますが、多くの場合、ファイアウォールはデバイスから属性を 1 つだけ受け取ります。デバイス オブジェクト (**Objects** > **Devices**) が、デバイスがファイアウォールに送信しない属性を指定している場合、トラフィックはデバイスと一致せず、ルールはデバイスを制御しないため、デバイスがファイアウォールに送信する属性のみを指定します。 。

   

   ルール内の デバイス ***ID*** をクリックして、関連付けられたデバイス オブジェクトをポップアップ表示します。

   CLI コマンド **`show iot ip-device-mapping-mp all`** または **`show iot ip-device-mapping-mp ip`** を実行します。 <IP-address>ファイアウォールがルールとともにインポートされた属性を受信していることを検証します。ファイアウォールがデバイス オブジェクトで構成されている属性を受け取らない場合は、デバイス オブジェクトから属性を削除します。

詳しい構成手順については、該当する管理者ガイドを参照してください。

- **IoT**セキュリティ:
  - 輸入手続き
  - ポリシー セットを Panorama にインポートする
  - Device-IDの設定
- **SaaS** セキュリティ:
  - PAN-OS および Panorama 管理対象 Prisma アクセス -SaaS ポリシー推奨事項のインポート (スタンドアロン ファイアウォールの場合。Panorama では、インポートされたルールが事前ルールか事後ルールかを指定し、Panorama にルールをインポートした後にファイアウォールにプッシュします。)
  - クラウド管理 Prisma アクセス-SaaS ポリシーの推奨事項を表示し、 新しい SaaS ポリシーの推奨事項をインポートします。

STEP 7 | (すべての管理者) セキュリティ ポリシー ルールベースを最新の状態に保つために、必要に応じてポリシーの推奨事項を更新および削除します。

ポリシー推奨事項のインポートは継続的なプロセスです。管理者は、新しいルールを推奨し、ルールを変更し、古いルールを削除します。IoT デバイスの数は増加し、デバイスの状態は時間の経過とともに変化します。SaaS アプリケーションの数は増加し、企業が承認済み、許容済み、および非承認としてタグ付けするアプリケーションは時間の経過とともに変化します。日次、週次、月次項目のチェックリストを作成して、IoT デバイスと SaaS アプリケーションの可視性を監視および維持します。

更新されたポリシー推奨事項をインポートする手順:

- IoTセキュリティ:IoT ポリシー ルールの推奨事項の変更と更新には、IoT セキュリティと PAN-OS の両方の手順が含まれます。
- SaaS セキュリティ:
  - SaaS セキュリティ インライン- アクティブな SaaS ポリシー ルールの推奨事項の変更では、SaaS セキュリティの既存のルールを変更する方法を示します。
  - クラウド管理 Prisma アクセス- クラウド管理 Prisma アクセスに関するインポートされた SaaS ポリシー ルールの推奨事項を更新します。

    同じ管理者が SaaS ポリシー推奨と Prisma Access 管理者の両方である場合、 自動更新を有効にして 、ルール推奨の変更を自動的に適用できます。
  - 「Panorama Managed Prisma Access および PAN-OS -更新された SaaS ポリシー推奨事項のインポート」では、 更新された SaaS セキュリティ ポリシー推奨事項を確認してインポートする方法を示します。

削除されたポリシー推奨事項を削除する手順:

- IoT:ポリシー ルールの削除に関する推奨事項には、IoT セキュリティと PAN-OS の両方の手順が含まれます。
- SaaS セキュリティ:
  - SaaS セキュリティ インライン-SaaS ポリシー ルールの削除に関する推奨事項では、SaaS セキュリティの既存のルールを削除する方法を示します。
  - クラウド管理 Prisma アクセス- クラウド管理 Prisma アクセスに関する削除された SaaS ポリシー ルールの推奨事項を削除します。
  - Panorama 管理の Prisma アクセスと PAN-OS -削除された SaaS ポリシーの推奨事項の削除。

セキュリティ ポリシーのベストプラクティスを維持する

セキュリティ ポリシーのベストプラクティスを 計画 して 展開 した後、ネットワークとそのアプリケーション、ユーザー、デバイス、インフラストラクチャの変化に応じてベスト プラクティスの展開を維持します。

STEP 1 | 適用範囲のギャップを避けるために、すべてのセキュリティ サブスクリプションを最新の状態に保ちます。

STEP 2 | アプリケーションと脅威のコンテンツの更新を常に把握し、アプリケーションと脅威のコンテンツの更新に関するベストプラクティスに従ってください。

STEP 3 | 最新の機能、デフォルトの動作の変更、問題などについては、リリース ノート を確認してください。

STEP 4 | 毎日、毎週、毎月（およびその他の必要な期間）のメンテナンス チェックリストを作成します。

時間の経過とともに状況が変化するにつれて、新しいアプリケーション、ユーザー、IoT デバイスが継続的に環境に追加されたり、環境から削除されたりするため、セキュリティ ポリシーの展開のメンテナンスは再帰的なタスクです。たとえば、チェックリストには次のものが含まれます。

- アプリケーションの評価と脅威コンテンツの更新
- Policy Optimizer を使用してアプリケーションを管理します。
- IoT および SaaS ポリシーの推奨事項と更新を確認します。IoT デバイスの状態は時間の経過とともに変化する可能性があり、使用される SaaS アプリケーションも時間の経過とともに変化するか、別の方法で処理して更新する必要がある場合があります。アプリケーションの認可/許容/非認可タグを常に最新の状態に保ちます。
- セキュリティ体制分析ツールを実行する時間を設定します。
- リリース ノートに記載されている動作の変更点と問題点を確認します。
- セキュリティ ポリシー ルールを確認して、ルールを強化できるかどうか、または不要になったかどうかを確認します。

STEP 5 | セキュリティ ポリシーで App-ID を維持します。

- 新規および変更されたコンテンツ配信 App-ID を確認し、必要に応じてルールを調整します。
- 新しいアプリケーションをネットワークに追加するときは、それらを具体的で詳細なポリシー ルールに含めます。タグとアプリケーション フィルタを使用して、新しい App-ID

Cloud Engine アプリケーションなどの認可されたアプリケーションのルールへの追加を自動化します。

- 会社でアプリケーションの使用を停止した場合は、不正使用を防ぐために許可ルールからそのアプリケーションを削除します。
- セキュリティ ポリシー ルールで許可されているアプリケーションを定期的に確認してください。

STEP 6 | セキュリティ ポリシーでユーザー ID を維持します。

- 新しいユーザーをネットワークに追加するときは、そのユーザーを適切なユーザー グループに追加してアクセスを制御し、ポリシーに含めるか、グループに属していない場合はルールに直接追加します。
- ユーザーが退職したり、契約が終了したりした場合は、ユーザー グループからユーザーを削除してアクセスを禁止します。グループの一部として追加されていない個人をルールから削除します。
- グループおよびポリシー ルールに対してユーザーを追加および削除するときは、引き続き ユーザー グループ マッピングの ベストプラクティス と ダイナミック ユーザー グループ (DUG) のベストプラクティス に従ってください。

STEP 7 | ネットワークと目標の進化に合わせて、セキュリティ プロファイルとプロファイル グループを維持および更新します。新しい許可ルールを追加するときは、適切なセキュリティ プロファイルがアタッチされていることを確認してください。

STEP 8 | 新しいルールやアプリケーションの場合と同様に、必要に応じてログ転送を更新します。

- すべての新しいセキュリティ ポリシー ルールに適切なログ転送プロファイルを適用するか、デフォルトのログ転送プロファイルを使用して新しいルールにログ転送プロファイルを自動的に適用します。デフォルトのプロファイルを使用する場合は、ルールをチェックしてデフォルトのプロファイルが適切であることを確認し、適切でない場合は適切なプロファイルに置き換えます。
- 何を記録し、何を記録していないのか、またどのように記録しているのかを定期的に確認してください。ログに記録したいトラフィックをログに記録し、セキュリティ オペレーティング センター (SOC) の操作に関してログに記録したいすべての情報をログに記録していることを確認してください。
- 管理者が会社に入社したり退職したりしたときに、ログ転送プロファイルを更新します。
- 新しいアプリケーションがネットワークに導入されると、それらに対応できるようにログ転送を更新します。

STEP 9 | セキュリティ体制分析ツールを使用して、ベストプラクティスの展開を確認します。

- PAN-OS および Prisma Access では、Strata Cloud Manager を使用してセキュリティ ポリシーを作成時に確認します。
- Strata Cloud Manager オンデマンドのベストプラクティス評価 (BPA) を定期的に実行して、ベスト プラクティスの導入に向けた進捗状況を測定します。
- セキュリティ ライフサイクル レビュー (SLR) を四半期ごとに実行して、ネットワークをよりよく把握します。

STEP 10 | ファイアウォール ツールを使用してアクティビティを確認し、必要に応じてセキュリティ ポリシーを調整します。

- PAN-OS(Panorama Managed Prisma Access にも適用) および Cloud Managed Prisma Accessのログ情報を使用して、トラフィックを調査および監視します。
- Application Command Center を使用すると、ネットワークを通過するアプリケーション、ユーザー、脅威、URL、コンテンツの概要をグラフィカルに表示できます。
- アプリケーション スコープ レポート を使用すると、アプリケーションの使用状況とユーザー アクティビティ、帯域幅の使用状況、ネットワークの脅威の変化を理解できます。
- カスタム レポート を作成して、調査したい正確なデータを表示します。

STEP 11 | Policy Optimizer を定期的にチェックしてルールベースを調べ、未使用のルール、過剰にプロビジョニングされたルール、未使用のアプリケーションを含むルールを見つけて修正します。Policy Optimizer のチェックを定期的にスケジュールされたメンテナンスに追加します。

STEP 12 | SecOps ツールとサービスを使用して、セキュリティ体制全体をプロアクティブに監視し、脅威を防止し、問題を調査します。

- Cortex XSIAM は、 プロアクティブな監視のための SOC 分析と SIEM 機能を組み合わせています。
- Cortex XSOAR は、包括的な脅威インテリジェンス管理とリアルタイム コラボレーションのために、包括的なセキュリティ オーケストレーション、自動化、および応答プレイブックを含む応答を提供します。
- Cortex XDR は、クラウド、ネットワーク、エンドポイントのイベントとデータを監視および管理する拡張検出および応答プラットフォームを提供します。
- SecOps 予防体制の評価、最適化、学習ワークショップなどのSOC サービス。

STEP 13 | 次のリソースでは、Palo Alto Networks のプラットフォーム、機能、サポートに関する詳細情報を提供します。

- セキュリティ ベスト プラクティス ドキュメント ポータルには、「IoT セキュリティ ベスト プラクティス」、「管理アクセスのベスト プラクティス」、「復号化のベストプラクティス」などの独立した書籍と、さまざまな管理者ガイドのベスト プラクティスのトピックへのリンクが含まれています。

- 管理者ガイド:
  - PAN-OS 管理者ガイド
  - Prisma Access 管理者ガイド (Panorama Managed および Cloud Managed Prisma Access用)
  - SaaS セキュリティ管理者ガイド
  - IoT セキュリティ管理者ガイド
- ドキュメントポータル:
  - Cloud Delivered Security Services (CDSS) ドキュメント ポータル
  - Cloud Identity Engine (CIE) ドキュメント ポータル
  - GlobalProtect ドキュメント ポータル
  - Palo Alto Networks カスタマー サポート ポータル
- ベストプラクティスを使用して IoT セキュリティの導入を監視する
- IoT セキュリティ ソリューションの構造 (IoT セキュリティ ソリューションの仕組みの概要)
- Prisma Access の SaaS セキュリティ (Panorama 管理およびクラウド管理)
- SaaS Security Inline に関する問題のトラブルシューティング