paloalto
TECHDOCS

インターネット ゲートウェイの最良のセキュリティポリシー

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

July 24, 2023

Table of Contents

最良のインターネット ゲートウェイのセキュリティポリシー

攻撃者がネットワークにアクセスするための最も安価かつ簡単な方法は、インターネットにアクセスするユーザーを利用することです。エンドポイントの悪用に成功すると、攻撃者はネットワークに侵入し、ソースコードの盗用、顧客データの流出、インフラストラクチャの停止などの最終目標に向かって横方向に移動することができます。ネットワークをサイバー攻撃から守り、セキュリティを全体的に向上させるために、最良のインターネット ゲートウェイのセキュリティ ポリシーを導入します。この最良のポリシーを使用してすべてのトラフィックをあらゆるポートで常に制御することにより、アプリケーション、ユーザー、コンテンツを安全に有効することができます。

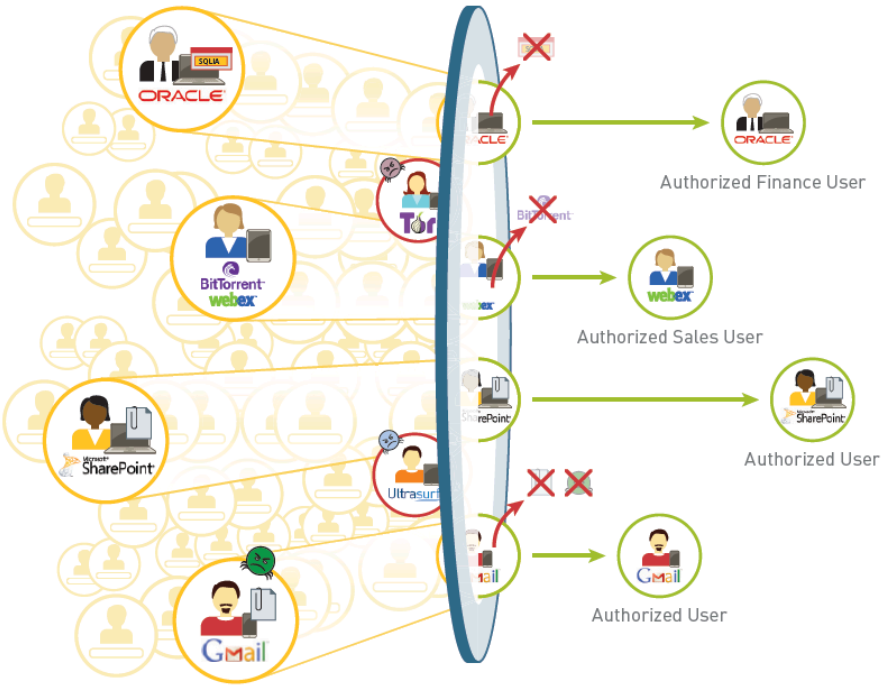
復号化、DoS、ゾーン保護（パケット バッファ保護を含む）などのテーマに関する最良のアドバイスについては、Palo Alto Networks のベストプラクティス ブック シリーズを参照してください。

最良のインターネット ゲートウェイのセキュリティポリシーとは

最良のインターネット ゲートウェイのセキュリティポリシーには、セキュリティ上の目標が 2 つあります。

- **Minimize the chance of a successful intrusion**（進入が成功する確率を最小化）–従来型のポート ベースのセキュリティ ポリシーはネットワーク セキュリティのためにすべてをブロックする、あるいはビジネスのためにすべてを許可します。最良のセキュリティポリシーはこれとは違い、App-ID、User-ID、Content-ID およびデバイス ID（IoTセキュリティのため、本書の範囲外） を最大限利用し、未知および既知の脅威両方のトラフィックをすべてスキャンしつつ、すべてのポートであらゆるユーザーが常にアプリケーションを安全に使用できるようにします。
- 攻撃者の存在を検知–最良のインターネット ゲートウェイのセキュリティポリシーには、ルールベースのずれを認識し、ネットワーク上の危険な活動や潜在的な脅威を検知するのに役立つビルトイン式のメカニズムが備わっています。

これらの目標を達成するために、最良のインターネットゲートウェイのセキュリティ ポリシーはアプリケーションベースのルールを使用し、特定のアプリケーションにユーザーがアクセスするのを許可しつつ、すべてのトラフィックをスキャンしてあらゆる既知の脅威を検知し、未知のファイルを WildFire に送信して新しい脅威を特定し、それらをブロックするためにシグネチャを生成します。



ベストプラクティス ポリシーは、攻撃ライフ サイクルの複数の段階での検出と防止を保証する次の方法論に基づいています。

最良の方法論	これが重要な理由
可視化のためにすべてのトラフィックを検査	把握できない脅威は防御することができないため、すべてのトラフィック、あらゆるユーザーやアプリケーションに対して常に完全な可視性を維持する必要があります。 • GlobalProtectを導入し、あらゆる場所のユーザーやデバイスに次世代セキュリティ プラットフォームを拡張します。 • ファイアウォールが暗号化されたトラフィックを検査できるように、復号化を有効にします（毎年多くの企業Webトラフィックが暗号化され、マルウェアキャンペーンの多くが暗号化を使用しています）。 • User-ID を有効にして、アプリケーション トラフィックおよび関連する脅威をユーザー/デバイスにマッピングし、ユーザーがどこにいても追跡するポリシーを有効にします。 • 会社のポリシーでネットワーク上のユーザーのデバイス (GlobalProtect やその他のセキュリティ管理アプリケーションがインストールされていない BYOD または企業デバイス) が許可されている場合、SaaS Security API の管理対象外デバイスのアクセス制御により、ユーザーは個人のデバイスや場所を問わずクラウド SaaS アプリケーションにアクセスできるようになります。データや組織を誤って危険にさらすことはありません。ポリシーの適用と脅威防御のために、トラフィックはファイアウォール経由でリダイレクトされます。 完全な視認性により、場所やデバイスの種類、ポート、暗号化の有無、回避テクニックに関わらず、App-ID、コンテンツID、User-IDテクノロジーによってファイアウォールがすべてのトラフィック（アプリケーション、脅威、コンテンツを含む）を検査することができます。 ネットワーク上のアプリケーション、コンテンツおよびユーザーの完全な可視化を実現することが、データに基づいたポリシー制御を行うための最初のステップになります。
攻撃面を低減	ネットワーク上のアプリケーション、コンテンツ、およびユーザーのコンテキストを取得したら、アプリケーション ベースのセキュリティ ポリシー ルールを作成して、重要なビジネス アプリケーションを許可し、正当なビジネス ユースケースを持たない高リスクのアプリケーションをブロックします。 攻撃の入り口をさらに減らすため、アプリケーション トラフィックを許可するすべてのルールに対して行うファイル ブロッキングおよび URLフィルタリング プロファイルの付与をし、脅威のあるウェブサイトにユーザーがアクセスしたり、危険なファイル タイプ（未知、既知を問わず）をユーザーがアップロードあるいはダウンロードしたりしないようにします。攻撃者がフィッシング攻

最良の方法論	これが重要な理由
	撃を実行できないように、資格情報フィッシング防止を構成します。
既知の脅威を阻止	すべての許可ルールにセキュリティ プロファイルを添付すると、ファイアウォールがネットワークおよびアプリケーション層の脆弱性エクスプロイト、バッファ オーバーフロー、DoS 攻撃、ポート スキャン、および既知のマルウェアの亜種 (圧縮ファイルまたは圧縮 HTTP/HTTPS トラフィック内に隠されたものを含む) を検出してブロックできるようになります。復号化を有効化し、暗号化されたトラフィックに対する検査を行えるようにします。 アプリケーション ベースのセキュリティポリシールールに加え、Palo Alto Networks および信頼できるサードパーティのフィードが提供する脅威インテリジェンスに基づき悪意のある既知の IP アドレスをブロックするルールを作成します。
未知の脅威を検出	未知のファイルをすべてWildFireに送信して分析を行います。WildFire は、クラウドあるいは WildFireアプライアンス上の仮想化環境で未知のファイルを直接観察・実行し、ファイルに隠された未知のマルウェアや対象のマルウェア（持続的標的型攻撃あるいは*APT*とも呼ばれる）を特定します。WildFire がマルウェアを検出すると、シグネチャが自動的に作成され、リアルタイムまたは選択した時間間隔でシグネチャを配信できます。

最良のインターネット ゲートウェイのセキュリティポリシーが必要な理由

ベスト プラクティスのセキュリティ ポリシーを使用すると、暗号化されたトラフィックを含む、すべてのポートにわたるすべてのトラフィックを常に分類することで、アプリケーションを安全に有効にすることができます。各アプリケーションのビジネス ユース ケースを決定して、関連するアプリケーションへのアクセスを許可および保護するセキュリティ ポリシー ルールを作成します。ベスト プラクティスのセキュリティ ポリシーでは、パロアルトネットワークスのエンタープライズ セキュリティ プラットフォームで次世代テクノロジーである App-ID、Content-ID、User-ID、および Device-ID (IoT セキュリティについては、本書の範囲外です) を活用します。

- ポート、プロトコル、回避策、暗号化に関係なくアプリケーションを識別します。
- IPアドレス、場所、デバイスに関係なくユーザーを識別し、制御します。
- アプリケーションが媒介する既知および未知の脅威から保護します。
- アプリケーションのアクセスと機能に対するきめ細かい可視性とポリシー制御を提供します。
- IoT を導入している場合は、IoT セキュリティのベスト プラクティス に従います。

ベストプラクティスのセキュリティ ポリシーでは、階層化されたアプローチを使用して、正当なユースケースのないアプリケーションをブロックしながら、認可されたアプリケーションを安全に有効にします。ポートベースの適用からアプリケーションベースの適用に移行するときにアプリケーションが破損するリスクを軽減するために、ベスト プラクティスのルールベースには、ルールベース内のギャップを特定し、憂慮すべきアクティビティと潜在的な脅威を検出し、アプリケーションが不正なアクセスを行わないようにする一時的なセキュリティ ポリシー ルールが含まれています。移行中に中断し、アプリケーションの使用状況を監視して、適切なルールを作成できるようにします。従来のポートベースのポリシーで許可されていた一部のアプリケーションは、許可したくないアプリケーション、またはより詳細なユーザー セットに制限したいアプリケーションである可能性があります。

ベスト プラクティスのセキュリティ ポリシーは、各ルールが特定のビジネス目標を満たし、特定のユーザー グループにアプリケーションまたはアプリケーションのグループへのアクセスを許可するため、管理と保守が容易になります。各ルールのアプリケーションとユーザーの一致条件により、ルールが適用するトラフィックを理解しやすくなります。ベスト プラクティスのセキュリティ ポリシー ルールベースでは、タグとオブジェクトも活用して、ルールベースのスキャンを容易にし、変化する環境との同期を維持しやすくします。

最良のインターネット ゲートウェイのセキュリティポリシーをデプロイする方法

目標は、ビジネス目標と許容利用ポリシーに適合し、管理を簡素化し、エラーの可能性を減らし、ネットワーク アクセスに ゼロ トラスト 原則を適用する、アプリケーション ベースのベスト プラクティス セキュリティ ポリシーを構築することです。

他のテクノロジーと同様に、完全な実装には通常、段階的なアプローチが必要です。エンドユーザーへの影響を最小限に抑えながら、移行をできるだけスムーズに行うために、導入フェーズを慎重に計画してください。最良のインターネット ゲートウェイのセキュリティポリシーを導入する一般的な流れは次のようになります。

- ビジネスを評価し、保護する必要があるものを特定する- セキュリティ アーキテクチャを導入する最初のステップは、ビジネスを評価することです。最も価値のある資産と、それらの資産に対する最大の脅威を特定します。例えばテクノロジー企業の場合、最も価値の高い資産は知的財産です。この場合、最大の脅威の 1 つはソース コードの盗難です。
- インターフェイスとゾーンを使用してネットワークをセグメント化する- セキュリティ ポリシー ルールで許可されている場合にのみ、トラフィックがゾーン間を流れることができます。ネットワークにアクセスした攻撃者がネットワーク内を横方向に移動するのを防ぐ強力な防御策は、詳細なゾーンを定義し、各ゾーン内のアプリケーションまたはリソースにアクセスする必要がある特定のユーザー グループのみにアクセスを許可することです。ネットワークを細かなゾーンに分けることで、攻撃者が（正当なアプリケーションに対するエクスプロイト、あるいはマルウェアによって）ネットワーク内で通信チャネルを確立するのを防ぎ、攻撃が成功する可能性を抑えることができます。
- アプリケーション許可リストの特定- インターネット ゲートウェイのベストプラクティス セキュリティ ポリシーを作成する前に、ネットワーク上で許可するアプリケーションのインベントリを作成します。自分が管理するアプリケーション、ビジネスとして正式に認可されているアプリケーション、および従業員の使用を許可しているアプリケーションを個別にリストします。許可するアプリケーションを特定した後、ポートベースのルールベースから移行する場合は、アプリケーションをポートベースのルールにマッピングします。ポートベースのルールにアプリケーションがマッピングされていない場合、そのルールは必要ない可能性があります。
- 許可したアプリケーションにアクセスするためのユーザーグループの作成–許可するアプリケーションを決定した後、そのそれぞれにアクセスする必要があるユーザーグループを決定します。エンド ユーザーのシステムを侵害することは、攻撃者がネットワークにアクセスする最も安価で簡単な方法の 1 つです。攻撃対象領域を大幅に減らすには、正当なビジネス ニーズを持つユーザー グループにのみアプリケーション アクセスを許可します。
- 完全な可視化および脅威検査のためにトラフィックの復号化–表示および検査できない脅威からネットワークを保護することはできません。暗号化されたトラフィックは、攻撃者が脅威をもたらす一般的な方法です。例えば、攻撃者はTLS暗号化を用いるGmailといったWebアプリケーションを使い、企業ネットワーク上でそのアプリケーションにアクセスしている社員に対してエクスプロイトやマルウェアを付与したメールを送信するかもしれません。あるいは、攻撃者はTLS暗号化を使用するウェブサイトを攻撃し、サイト訪問者が知らない内にエクスプロイトやマルウェアをダウンロードさせるかもしれません。

- インターネット ゲートウェイの最良のセキュリティ プロファイルの作成–コマンド アンド コントロール トラフィック、CVE、悪意のあるコンテンツのドライブバイダウンロード攻撃、フィッシング攻撃はすべて、正当なアプリケーションを介して侵入します。既知および未知の脅威から保護するには、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 ルールに厳格なセキュリティ プロファイルを添付します。
- 初期インターネット ゲートウェイ セキュリティ ポリシーの定義- 作成したアプリケーションおよびユーザー グループ インベントリを使用して、ユーザーまたはユーザー グループによるアプリケーションへのアクセスを許可する初期ポリシーを定義します。初期のポリシー ルールベースには、既知の悪意のある IPアドレスをブロックするためのルールや、未知のアプリケーションの破壊を防ぎ、既存の設計内のポリシー ギャップやセキュリティ ホールを特定するための一時的なルールも含まれています。
- ポリシー ルールベースの監視と調整–一時ルールを配置した後でそれにマッチするトラフィックを監視し始め、ポリシーを微調整することができます。この一時ルールは、デフォルト以外のポートを移動するトラフィックや未知のユーザーによるトラフィックといったネットワーク上の予期せぬトラフィックを発見することが目的であるため、このルールにマッチしたトラフィックを査定し、それに合わせてアプリケーション許可ルールを調整する必要があります。
- 一時ルールの削除–数か月の監視期間が過ぎれば、一時ルールにヒットするトラフィックの数が徐々に少なくなっていくはずです。トラフィックが一時ルールにヒットしなくなった時点でそれを取り除き、最良のインターネット ゲートウェイのセキュリティ ポリシーを完成させます。
- ルールベースの維持- アプリケーションの動的な性質により、アプリケーションの許可リストを継続的に監視し、新しいアプリケーションに合わせてルールを調整し、新規または変更された App-ID がポリシーにどのような影響を与えるかを判断する必要があります。ベストプラクティス ルールベースのルールはビジネス目標に合わせて管理を簡素化するためにポリシー オブジェクトを利用するため、多くの場合、新しいアプリケーションや新しいまたは変更された App-ID のサポートの追加は、アプリケーション グループまたは アプリケーション グループ からアプリケーションを追加または削除するのと同じくらい簡単です。 アプリケーションフィルターの変更。

アプリケーション許可リストの識別

アプリケーション許可リストには、ビジネス、インフラストラクチャ、およびユーザーの作業目的でプロビジョニングおよび管理する認可されたアプリケーションと、個人使用を許可するために選択した許容アプリケーションが含まれます。インターネット ゲートウェイ セキュリティ ポリシーを作成する前に、許可するアプリケーションのインベントリを作成します。

- ルールベースをシンプルにするためにアプリケーションをビジネス ゴールにマッピング
- 一時ルールを使用した許可リストの調整
- アプリケーション許可リストの例

ルールベースをシンプルにするためにアプリケーションをビジネス ゴールにマッピング

ネットワーク内のアプリケーションのリストを作成する際、ビジネス ゴールや利用規約を考慮し、それぞれに対応するアプリケーションを決定します。これにより、目標主導型のルールベースを作成できます。例えば、営業担当者やサポート担当者が顧客データベースにアクセスできるようにするというビジネス上の目的があるかもしれません。各ゴールに対応する許可ルールを作成し、そのゴールに関連するすべてのアプリケーションを単一のルールにグループ化します。このアプローチにより、より少数の個別ルールを含むルールベースを作成でき、各ルールには明確な目的があります。

個々のルールはビジネス ゴールに合わせて作成しているため、アプリケーション オブジェクトを使用して許可したアプリケーションをグループ化し、ルールベースの管理をさらにシンプルにすることができます。

- 認可されたアプリケーションのセットごとにアプリケーション グループを作成する - 認可されたアプリケーションのセットのみを明示的に含むアプリケーション グループを作成します。アプリケーション グループを使用すると、個々のセキュリティ ポリシー ルールを変更せずに、認可されたアプリケーションを追加および削除できるため、ポリシーの管理が簡素化されます。一般的に、同じゴールにマップされるアプリケーションが同じアクセス要件を持っている場合（例えば、すべてインターネットを指す宛先アドレスを持っている、すべて既知のユーザーからのアクセスを許可している、デフォルトのポートでのみ有効にしたいなど）、同じアプリケーショングループに追加します。

  事前定義済みの*Sanctioned*（許可）タグを使ってすべての許可されたアプリケーションをタグ付けします。*Panorama* とファイアウォールは、*Sanctioned* タグのないアプリケーションを未承認のアプリケーションとみなします。

- 各種の一般アプリケーションを許可するアプリケーション フィルタを作成する - 公式に認可したアプリケーションに加えて、ユーザーにアクセスを許可する追加アプリケーションを決定する必要があります。アプリケーション フィルターを使用すると、タグ、カテゴリ、サブカテゴリ、テクノロジー、リスク要因、または特性に基づいて、アプリケーションの特定のカテゴリを安全に有効にすることができます。ビジネス ユースおよび個人ユース用の異なるタイプのアプリケーションを区別します。各タイプのアプリケーション用のフィルターを作成すれば、各ポリシー ルールを理解しやすくなります。

一時ルールを使用した許可リストの調整

アプリケーションベースのセキュリティ ポリシーの最終目標は、許可したいアプリケーション トラフィックを明示的に許可し、不要なトラフィックを暗黙的に拒否することです。ただし、最初のルールベースにはいくつかの一時的なルールが必要です。これにより、ネットワーク上のすべてのアプリケーションを完全に可視化し、ポリシーを適切に調整できるようになります。初期ルールベースには次のタイプのルールが必要です。

- ビジネス目的で正式に認可および展開するアプリケーションのルールを許可します。
- 利用規約によって許可を与える、許容されるアプリケーションに安全にアクセスできるようにする許可ルール。
- 正当に使用できる場面がないアプリケーションをブロックするブロックルール。これらのルールは、悪意のあるトラフィックがネットワークに侵入するのを防ぎ、一時ルールはポリシー ルールベースでまだ考慮されていないアプリケーションを検出します。
- ネットワーク上のすべてのアプリケーションに対する可視性を一時的にルールに提供させることで、ルールベースを調整できるようになります。

一時的なルール:

- ネットワーク上に存在することを知らなかったアプリケーションを可視化します。
- 把握されていない正規のアプリケーションがブロックされるのを防ぎます。
- 不明なユーザー、不明なアプリケーション、および非標準ポートで実行されているアプリケーションを特定します (攻撃者は通常、悪意のあるアクティビティの回避手法として非標準ポートで標準アプリケーションを使用します)。

非標準ポートで実行されている正規のアプリケーション (たとえば、内部開発されたアプリケーション) を特定して、アプリケーションが使用するポートを変更したり、ポリシーで使用する カスタム アプリケーションを作成 したりできるようにします。

一連のポートのカスタム セッション タイムアウトを定義するために作成した アプリケーション オーバーライド ポリシー ルールが ある場合は、各アプリケーションのカスタム タイムアウトを維持するように サービス ベースのセッション タイムアウト を構成することによって、アプリケーション オーバーライド ポリシーをアプリケーション ベースのポリシーに変換します。次に、各ルールをアプリケーション ベースのルールに移行します。アプリケーション オーバーライド ポリシーはポートベースであり、トラフィックに対するアプリケーションの可視性を提供しないため、どのアプリケーションがポートを使用するかを把握したり制御したりすることはできません。サービスベースのセッション タイムアウトはアプリケーションの可視性も維持しつつ、カスタム タイムアウトを利用できるようにします。

アプリケーション許可リストの例

ネットワーク上で使用される可能性があるアプリケーションを最初のリストにすべて含める必要はありません。代わりに、許可するアプリケーションに焦点を当ててください。一時的なルールはネットワーク上に存在する可能性のある他のアプリケーションを検出するため、アプリケーション ベースのポリシーへの移行中に壊れたアプリケーションに関する苦情が殺到することは

ありません。以下は、エンタープライズ ゲートウェイを導入するためのアプリケーション許可リストの例です。

アプリケーション タイプ	セキュリティのためのベスト プラクティス
SaaS アプリケーション	SaaS アプリケーションのサービスプロバイダはソフトウェアおよびインフラストラクチャを所有・管理しますが、誰がデータを作成、アクセス、共有、転送できるのかということも含め、データを制御するのはすべてユーザーです。SaaS アプリケーションを制御するには、SaaS Security を使用します (サブスクリプションが必要です)。SaaS セキュリティを使用する場合は、SaaS ポリシー推奨 を使用してファイアウォール上の SaaS アプリケーションを制御します。 SaaS セキュリティのサブスクリプションがない場合は、SaaS アプリケーションの利用状況レポートを生成し、過去にデータ流出があった、適切な証明書が欠けているなど、現在使用している SaaS アプリケーションのホスティングが不適切かどうかチェックします。ビジネスニーズおよび許容できるリスクの大きさに基づき、この情報を使用して： • ホスティングが不適切な既存のアプリケーションをすぐにブロックします。 • ホスティングが不適切なアプリケーションをブロックする細かなポリシーを作成し、将来のセキュリティ違反を防止します。 • ホスティングが不適切な上位のアプリケーションのネットワーク トラフィックの傾向を把握し、それに合わせてポリシーを調整できるようにします。 多くの SaaS アプリケーションにはエンタープライズ バージョンとコンシューマー (個人) バージョンがありますが、無制限に使用すると、機密データがネットワークから流出するリスクが高まります。HTTP ヘッダーの挿入により、ネットワーク上で許可する SaaS アプリケーションのバージョンを制御できます。たとえば、Box または Office 365 のエンタープライズ バージョンを許可し、コンシューマ バージョンをブロックすることができます。HTTP ヘッダーを挿入すると、ユーザーの個人的な使用を許可または許容したい各 SaaS アプリケーションのバージョンのみが許可されるため、アタックサーフェスが減少します。
許可されたアプリケーション	特に組織内でのビジネス ユースのために、あるいはネットワークおよびアプリケーションのインフラストラクチャを提供するためにIT部門が管理するアプリケーションというものが存在します。例えば、インターネット ゲートウェイのデプロイでは、これらのアプリケーションは次のカテゴリーに分類されます。 • **Infrastructure Applications**（インフラストラクチャ アプリケーション）—ping、NTP、SMTP、およびDNSといったネットワークおよ

アプリケーション タイプ	セキュリティのためのベスト プラクティス

	びセキュリティを有効化することを許可する必要があるアプリケーションです。
	• **IT Sanctioned Applications**（IT制限付きアプリケーション）–ユーザーのために提供・管理されるアプリケーションです。これは2つのカテゴリーに分かれます。
	  • **IT Sanctioned On-Premise Applications**（IT制限付き業務用アプリケーション）–ビジネス ユースのためにデータセンターにインストール・ホストするアプリケーションです。IT制限付き業務用アプリケーションを使用し、アプリケーション インフラストラクチャおよびデータが社内設備で保持されます。例えば、Microsoft ExchangeやActiveSync、KerberosやLDAPといった認証ツールがあります。
	  • **IT Sanctioned SaaS Applications**（IT 部門に対して許可された SaaS アプリケーション）–Salesforce、Box、GitHub など、IT 部門がビジネス上の目的で使用することが許可された SaaS アプリケーションです。
	• **Administrative Applications**（管理アプリケーション）–アプリケーションの管理を行ったりユーザーをサポートしたりするために特定の管理ユーザーのグループのみがアクセスできるアプリケーションです（例えば、リモート デスクトップ アプリケーション）。
	事前定義済みの*Sanctioned*（許可）タグを使ってすべての許可されたアプリケーションをタグ付けします。Panorama およびファイアウォールは、Sanctioned タグが付いていないアプリケーションを許可されていないアプリケーションとみなします。

許容されるアプリケーションの種類	公式に認可したアプリケーションに加えて、ユーザーが他の種類の許容アプリケーションに安全にアクセスできるようにする必要もあります。 • **General Business Applications**（一般的なビジネス アプリケーション）–例えば許容されているアプリケーションのソフトウェア更新や、WebEx、Adobeオンラインサービス、Evernoteといったウェブ サービスへのアクセスを許可します。 • **Personal Applications**（個人アプリケーション）–例えば、一部のコンシューマー用の SaaS アプリケーションを含め、ユーザーがWebブラウジングを行ったり、Webベースのメール、インスタント メッセージ、ソーシャルネットワーク アプリケーションを安全に使用することを許可する場合があります。 ネットワーク上にどのアプリケーションがあるかを理解するには、広範なアプリケーション フィルターから始めます。その後、どの程度のリスクを予期するのかを決定し、アプリケーション許可リストを絞り始めることができます。たとえば、複数のメッセージングアプリケーション

アプリケーション タイプ	セキュリティのためのベスト プラクティス
	が使用中で、それぞれにデータ損失やマルウェアに感染したファイルの転送などの、固有リスクが存在している場合を考えてみましょう。 最善のアプローチは、単一のメッセージング アプリケーションを許可し、許可ポリシーから警告ポリシーに徐々に移行し、ユーザーに十分な警告を与えた後、ブロック ポリシーに移行して他のメッセージング アプリケーションを段階的に廃止することです。一部の小さなユーザー グループがパートナーと協働するために必要に応じて他のメッセージ アプリケーションを使用し続けられるようにすることもできます。
環境に合わせたカスタム アプリケーション	独自のアプリケーションまたは非標準ポートで実行するアプリケーション用のカスタム アプリケーションを作成します。これにより、アプリケーションを許可されたアプリケーションにして（そして事前定義済みの Sanctioned タグを適用）、デフォルトのポートに固定することができます。そうしなければ、別のポートを開く（標準的でないポート上で実行されているアプリケーション用）か、未知のトラフィックを許可（専有アプリケーション用）することになりますが、どちらもベストプラクティスのセキュリティポリシーでは推奨されません。 一連のポート用のカスタム セッション タイムアウトを定義するだけの目的で作成した既存のアプリケーション オーバーライド ポリシーがある場合、サービスベースのセッション タイムアウトを設定して各アプリケーションのカスタム タイムアウトを管理することで、既存のアプリケーション オーバーライド ポリシーをアプリケーション ベースのポリシーに変換します。次に、各ルールをアプリケーションベースのルールに移行します。アプリケーション オーバーライド ポリシーはポートベースであり、トラフィックに対するアプリケーションの可視性を提供しないため、どのアプリケーションがポートを使用するかを把握したり制御したりすることはできません。サービスベースのセッション タイムアウトはアプリケーションの可視性も維持しつつ、カスタム タイムアウトを利用できるようにします。

許可したアプリケーションにアクセスするためのユーザーグループを作成

アプリケーションを安全に有効にするということは、許可するアプリケーションのリストを定義し、正当なビジネス ニーズを持つユーザーのみにアクセスを有効にすることを意味します。例えば、人材サービス（WorkdayやService Nowなど）にアクセスし得るSaaSアプリケーションなど、一部のアプリケーションはネットワーク上の既知のユーザーがすべて利用できなくてはなりません。ただし、機密性の高いアプリケーションの場合は、ビジネス目的でアプリケーションを必要とするユーザーのみにアクセスを許可することで、攻撃対象領域を減らします。たとえば、IT サポート担当者は正当にリモート デスクトップ アプリケーションにアクセスする必要があるかもしれませんが、ほとんどのユーザーは必要ありません。アプリケーションへのユーザーアクセスを制限すると、攻撃者がネットワーク内のシステムにアクセスして制御するために利用する可能性がある潜在的なセキュリティ ギャップを防ぐことができます。

アプリケーションへのアクセスをユーザーベースで行うには：

- ユーザーがトラフィックを発生させるゾーン内のUser-ID を有効化します。
- 定義する各アプリケーション許可ルールについて、アプリケーションにアクセスする正当なビジネス上の理由があるユーザーグループを決定します。アプリケーション許可ルールをビジネス目標にマッピングすると (どのユーザーが特定の種類のアプリケーションに対するビジネス ニーズを持っているかを考慮することも含まれます)、ポートベースのルールをユーザーにマッピングする場合と比較して、管理するルールの数が少なくなります。
- Active Directory (アクティブディレクトリ AD) サーバー上に既存のユーザー グループがない場合は、代わりに、特定のアプリケーションにアクセスする必要があるユーザーのグループに一致する カスタム LDAP グループを作成します。
- エンドユーザーがフィッシング リンクをクリックして認証情報を入力するだけで、攻撃者がネットワークにアクセスできるようになってしまいます。このシンプルかつ効果的な攻撃テクニックを防止するために、ユーザーがインターネットにアクセスするのを許可するセキュリティポリシー ルールのすべてに対し、認証情報フィッシング防止のセットアップを行います。Windows ベースの User-IDエージェントと共に認証情報検知を設定し、不当なカテゴリに含まれるサイトにユーザーが企業の認証情報を送信しようとしているのを必ず検知します。

完全な可視化および脅威検査のためにトラフィックを復号化

機密カテゴリを除くすべてのトラフィックを復号化します。これには、金融サービス、健康および医療、政府などの URL カテゴリや、ビジネス、法律、または規制上の理由で復号化しないその他のトラフィックが含まれます。URL カテゴリ、 カスタム URL カテゴリ、および 外部ダイナミック リスト (EDL) を使用して、復号化しないトラフィックを指定します。

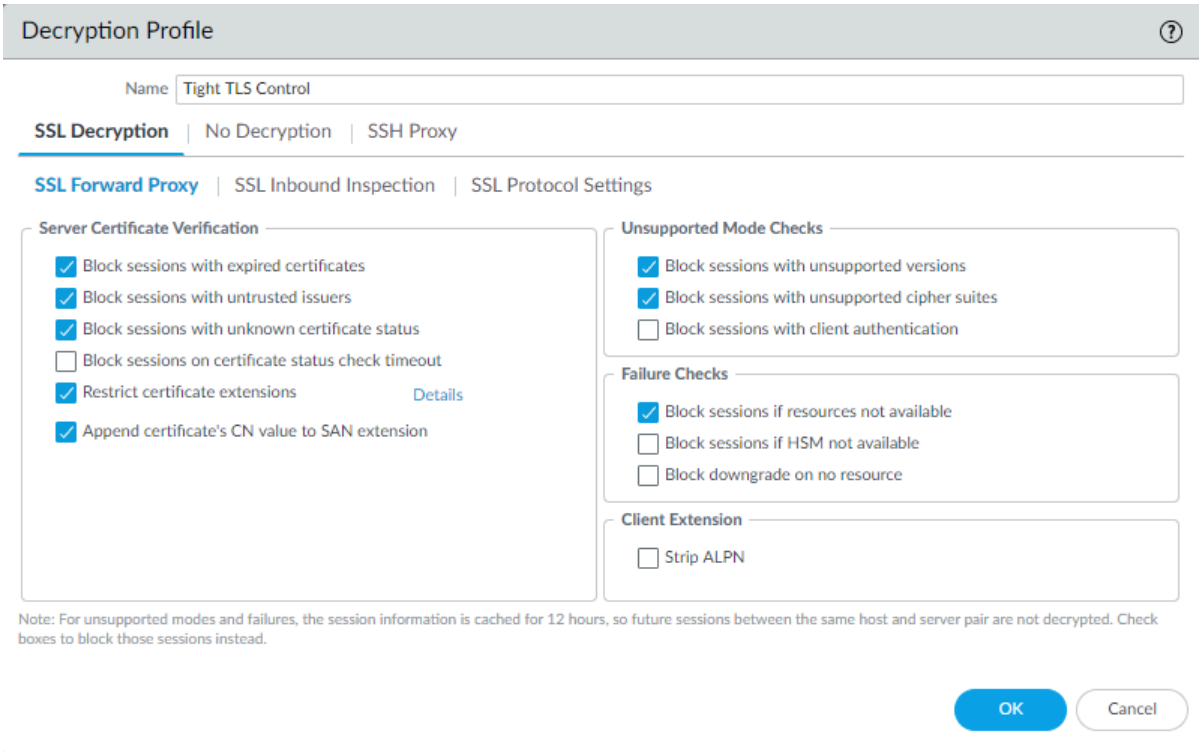
復号化例外は必要な場合にのみ使用してください。必要に応じて例外を特定のアプリケーションまたはユーザーに制限するように正確に行ってください。

- 復号化によりアプリケーションが壊れる場合は、そのアプリケーションに紐付けられた証明書内の特定の IP アドレス、ドメイン、あるいは共通名に対して例外を作成します。
- 規則、ビジネス、法的な理由で特定のユーザーを除外する場合は、そのユーザーだけに適用される例外を作成します。

復号化中に提示された証明書が有効であることを確認するには、CRL/OCSP チェックを実行します。

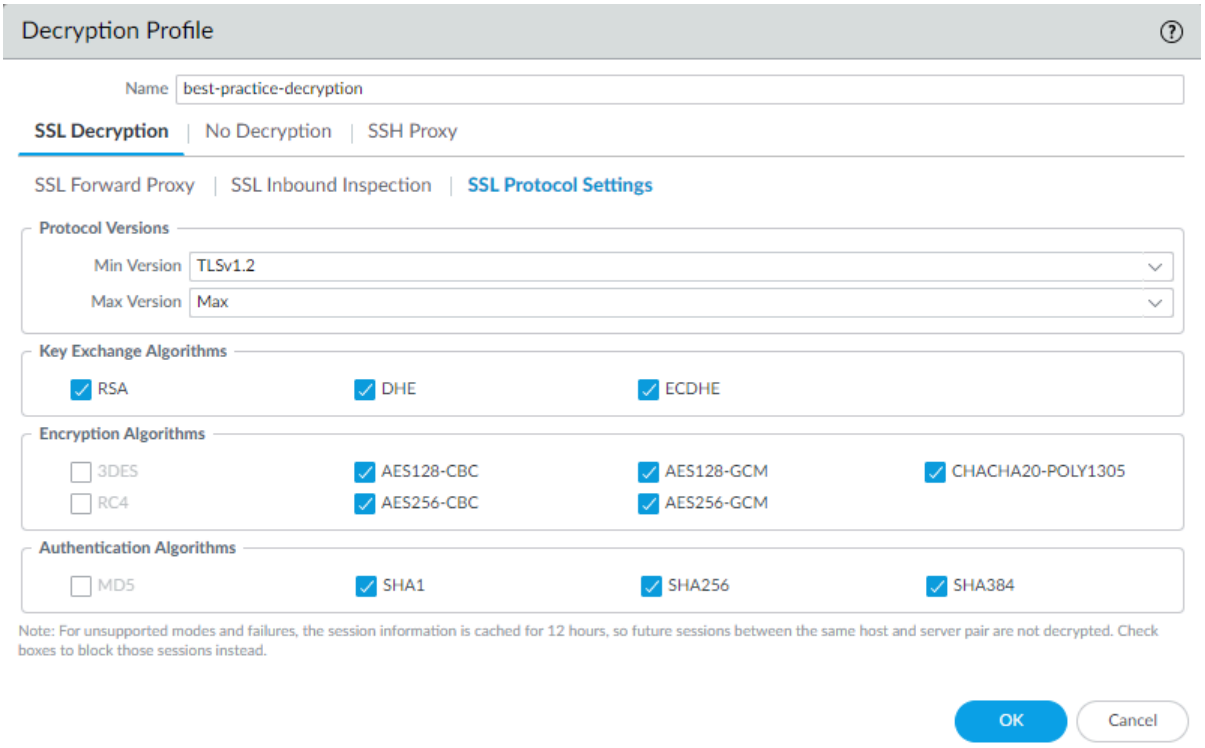
厳密な復号プロファイルを復号化ポリシー ルールに追加します。SSLフォワードプロキシを設定する前に、最良の復号化プロファイルを作成（**Objects**（オブジェクト）**> Decryption Profile**（復号化プロファイル））して復号化ポリシー ルールに付与し、一般的な復号化のベストプラクティスに従います。

STEP 1 | **SSL Decryption**（**SSL** 復号化）**> SSL Forward Proxy**（**SSL** 転送プロキシ） の設定を行い、TLSネゴシエートの際の例外、および復号化できないセッションをブロックします。



リソースが使用できない場合はセッションをブロックすること で、ファイアウォールに復号化を実行するリソースがない場合に潜在的に危険な接続が許可されるのを防ぎますが、この理由で復号化できないトラフィックをブロックすると、ユーザー エクスペリエンスに影響を与える可能性があります。

STEP 2 | **SSL**復号化 > **SSL** プロトコル設定 を構成して、脆弱な SSL/TLS バージョン (TLSv1.0、TLSv1.1、および SSLv3) の使用をブロックし、弱いアルゴリズム (MD5、RC4、および 3DES) を回避します。

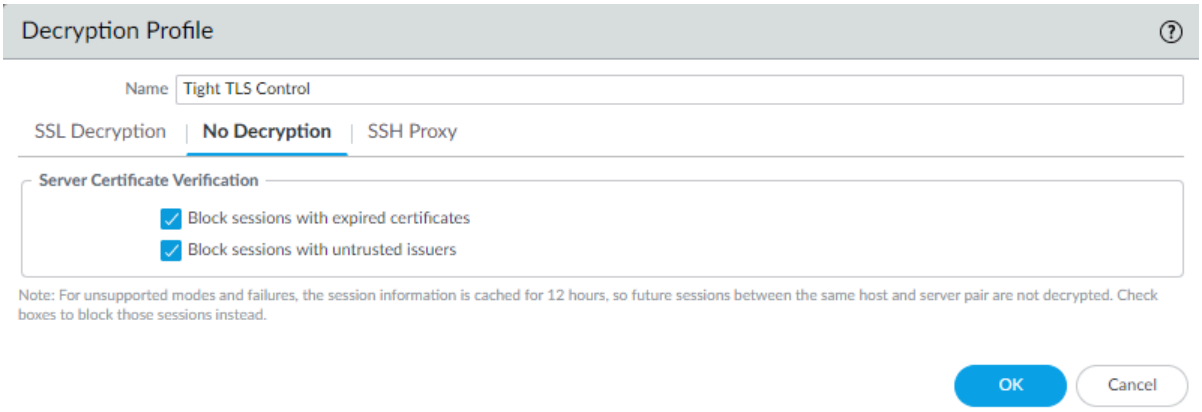


可能な場合は、TLSv1.3（もっとも安全なプロトコル）を使用してください。多くのモバイルアプリケーションでは、証明書のピン留めが使用されているため、復号化が妨げられ、ファイアウォールによるトラフィックのドロップが発生します。そのトラフィックには、TLSv1.2 を使用します。

ビジネス上の目的でアクセスする必要があるサイトを確認してください。いずれかがTLSv1.1を使用している場合は、そのようなサイト個別の復号ポリシーとプロファイルを作成し、ビジネス上の目的でアクセスが必要とされるサイトのみが、安全性に劣るプロトコルを使用するようにしてください。

必要がない限り、SHA1 認証アルゴリズムを許可しないでください。ビジネス目的でアクセスする必要がある SHA1 を使用するサイトに対して、別の復号ポリシー ルールとプロファイルを作成します。

STEP 3 | 自分で復号化しないトラフィックの場合は、**No Decryption**（復号化なし） の設定を行い、証明書の期限が切れている、あるいは発行者を信頼されていない暗号化されたセッションがサイトに来るのをブロックします。



No Decryption（復号化なし）プロファイルは、*TLSv1.2*またはそれ以前のバージョンにのみ使用してください。復号化しない*TLSv1.3*トラフィックに、復号化なしのプロファイルをアタッチしないでください。*TLSv1.3*は、前のバージョンで暗号化されていない証明書情報を暗号化します。そのため、ファイアウォールは証明書情報に基づいてセッションをブロックできなくなります。

ベスト プラクティス セキュリティ プロファイルに安全に移行

セキュリティ プロファイルを使用すると、脆弱性の悪用、マルウェア、コマンド アンド コントロール (C2) 通信、未知の脅威などの脅威についてネットワーク トラフィックを検査し、さまざまな種類の脅威シグネチャ、機械学習、AI を使用してネットワークへの侵害を防ぐことができます。 (一部の保護には サブスクリプションが必要です)。

最終目標は、すべてのセキュリティ プロファイルがベスト プラクティス状態に到達することです。しかしながら、ビジネスに重要なアプリケーションの利用可能性を確保するためには、最初から完全なベストプラクティス セキュリティ プロファイルを導入することは現実的ではありません。多くの場合、いくつかのシグネチャ、ファイルタイプ、あるいはプロトコルを、それ以外のものに注意しながら安全にブロックすることができます。これは、可用性を損なうことなく、ベストプラクティス セキュリティ プロファイルに安全に移行が完了することができたと確証が得られるまで行います。

ベストプラクティス セキュリティ プロファイルへの道筋：

1. AIOps を使用して、セキュリティ体制に関する オンデマンドのベストプラクティス評価 (BPA) レポートを生成します 。導入のベストプラクティスを確認し、導入におけるギャップを特定し、セキュリティ プロファイルの構成を確認します。
2. セキュリティ プロファイル用の ベストプラクティス状態に進むために、下記の安全移行ステップを使用します。

次のように自問して、与えられたネットワーク セグメントあるいはセキュリティ ポリシー ルール用のセキュリティ プロファイルを有効化する正しいアプローチを決定します：

1. 同様のアプリケーションあるいはネットワーク セグメントを保護するルールでセキュリティ プロファイルを既に有効にしていますか？答えが「はい」の場合、既に有効化しても安全であるとしたブロック アクションを含め、これらのプロファイル設定を複製しても構いません。
2. 保護しようとしているネットワーク セグメントはビジネスにとって重要だろうか？答えが「はい」で、同様のセグメントで有効になっている実証済みのプロファイルがない場合は、まずアラートを出し、アラートの原因となっているトラフィックを調べてプロファイルが重要なアプリケーションをブロックしていないことを確認し、必要なときにブロックすることをお勧めします。快適。
3. 喫緊の脅威に対向するためセキュリティプロファイルを今展開しているのだろうか？答えが「はい」の場合、初期のアクションとして、アラートよりもブロックを望んでいるかもしれません。

4. タイムリーにフォルスポジティブの調査と修復を可能にするファイアウォールの変更プロセスはありますか？答えが「はい」の場合、初期のアクションとしてあなたは、警告の代りにブロックできるかもしれません。

   「フォルスポジティブ」の大多数はネットワーク上に実在しない脆弱性に対しての攻撃の試みです。攻撃は事実ですが、危険はありません。なぜなら脆弱性は現存しないからです。従って攻撃はしばしばフォルスポジティブとして見られます。*Brute Force*（力ずく）攻撃シグネチャは、攻撃の閾値の設定が低すぎる場合、フォルスポジティブを起こすことがあります。

現在のセキュリティ体制を各タイプのセキュリティ プロファイルのガイダンスと組み合わせて検討し、最初にプロファイルを展開する方法を決定し、次にベストプラクティス ガイダンスに移行します。

- 脆弱性防御プロファイルを安全にベスト プラクティスに移行
- アンチスパイウェア プロファイルを安全にベストプラクティスに移行
- アンチウイルスプロファイルを安全にベストプラクティスに移行する
- WildFireプロファイルを安全にベスト プラクティスに移行
- URLフィルタリング プロファイルを安全にベスト プラクティスに移行
- ファイル ブロッキング プロファイルを安全にベスト プラクティスに移行

脆弱性防御プロファイルを安全にベスト プラクティスに移行

ブロックか警告を行う決定は、現在のセキュリティ体制とセキュリティ対可用性に関するビジネス要求項目に基づく脆弱性防御プロファイルの最初の適用に左右されます。次のガイダンスは、ベストプラクティスの脆弱性防御プロファイルへの移行を開始するときに、ブロック アクションとアラート アクションのどちらから開始するかを決定するのに役立ちます。

脆弱性防御には、高度な脅威対策またはアクティブなレガシー脅威防御サブスクリプションが必要です。

脅威を特定して防ぐには、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。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。

- ビジネス クリティカルなアプリケーション- 通常、アプリケーションの可用性を確保するために、最初のルール [アクション] を [アラート] に設定 することをお勧めします。しかしながら、ある状況では、最初からブロックアクションを使用することができます。例えば、既に脆弱性シグネチャをブロックする脆弱性防護プロファイルで同様なアプリケーションを保護している時、そして、プロファイルはビジネスとセキュリティのニーズに適合していると把握している場合、同様なプロファイルを使用して脆弱性をブロックし、同様のアプリケーションを保護できます。

アラートを使用すると、トラフィックのブロックを開始する前に、脅威ログを分析し、必要に応じて例外を作成できます。ブロッキングに移行する前に警告と監視を行うことで、次のことを確実に実行できます。

- 初期プロファイルは、デプロイ時にビジネス クリティカルなアプリケーションをブロックしません。
- ブロッキング状態に移行するときに、アプリケーションの可用性を維持するために必要な例外を作成します。

初期のアラートアクションを維持する時間長を、セキュリティ侵害の機会を低減するため最小に維持します。作成する必要がある例外を特定し、それに応じてプロファイルを構成したことに満足したらすぐに、ブロック状態に移行します。

- 極めて危険度の高いシグネチャ–重大で危険性の高いシグネチャのフォルスポジティブの割合は一般的には低く、通常はネットワーク上に存在しない脆弱性に対する攻撃を示します。インターネットアクセスなど、ビジネスにとって重要ではないアプリケーションの場合は、最初から重要なシグネチャと重大度の高いシグネチャをブロック (リセット)します。
- 中程度に危険なシグネチャ–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。中程度の重大度のシグネチャについてアラートすることから始め、脅威ログを監視して（**Monitor**（モニター） > **Logs**（ログ） > **Threat**（脅威））、アラートを受信したアプリケーションをブロックするか、またはそれらを許可する必要があるかを判断します。
- ブロックに移行する前に警告するプロファイル ルールを微調整します (特にインターネットに接続するトラフィックとデータセンターのトラフィックの場合)。できるだけ早くブロックに移行してください。
- ブルートフォース カテゴリのシグネチャをアラートに設定し、できるだけ早くブロックに移行します。ブルートフォースイベントは、アクションが短期間に複数回発生したときにトリガーされる集約イベントです。たとえば、1 回の SSH ログイン試行は情報イベントですが、10 秒間に 100 回のログイン試行でブルートフォース シグネチャがトリガーされます。通常のネットワークトラフィックがブルートフォース シグネチャをトリガーしないようにプ

ロファイルを調整するには時間がかかる場合がありますが、快適さのレベルに基づいて、できるだけ早くこれらのシグネチャをブロックするように移行してください。

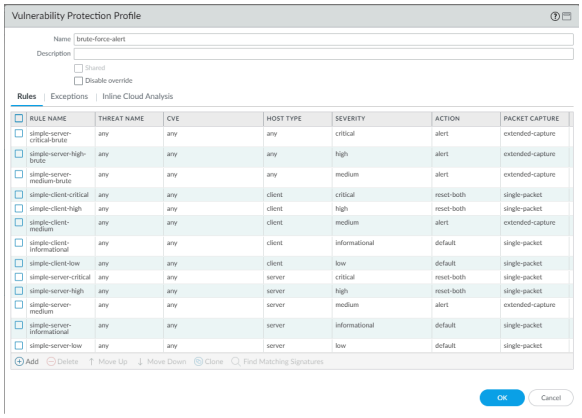


図 **1 :** ブルートフォースアラート脆弱性防御プロファイル

- ほとんどのlow(低)やinformational(通知)の重要度シグネチャのデフォルトアクションは**alert**または**allow**です。すべての低シグネチャと情報シグネチャについて警告する必要が特にない限り、アクション を デフォルトとして構成します。
- リソースが使用可能な場合は、アラートの重大度、重大度が高、および中程度のシグネチャの拡張 パケット キャプチャ を有効にします。ブロックされたシグネチャと、低重大度および情報重大度のシグネチャに対して、単一パケット キャプチャを有効にします。パケットキャプチャーを有効にすると、必要に応じてイベントを非常に詳細に調査することができます。ベストプラクティスプロファイルに移動すると、Informational イベントが膨大なパケットキャプチャーアクティビティ（トラフィックの非常に巨大なボリューム）を生成し、情報が特に有益でない場合、情報イベントに対するパケットキャプチャーの無効化に移ります。

  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。
- インラインクラウド分析では、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。既存のコントロールがある場合は、それらをレプリケートしてトラフィックをブロックできます。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。

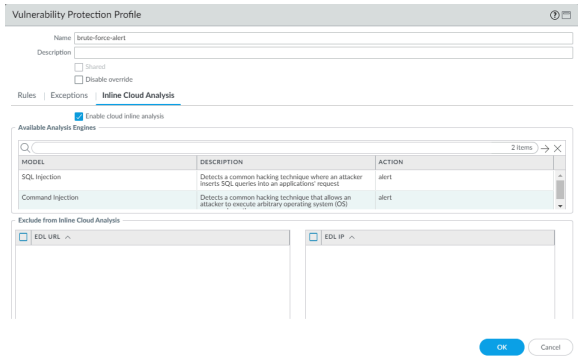


図 **2 :** インライン クラウド分析アラートの脆弱性防御プロファイル

初期プロファイルの導入時、ビジネスに重要なアプリケーションがアラートやブロックを生じさせていないかを把握するのに充分な期間脅威ログを監視します。完全な ベストプラクティスの脆弱性防御プロファイル に移行する前に、必要に応じて各プロファイルで例外を作成し(必要に応じてサポートチケットを開いて)、確認された誤検知を修正します。ベストプラクティス プロファイルへの移行をどれだけ早く完了するかは、ビジネス、アプリケーション、および快適性レベルによって異なります。一部のアプリケーションは、監査、定期的なイベントや会議などのために毎週、毎月、四半期ごと、または毎年のみ使用されることに注意してください。

アンチスパイウェア プロファイルを安全にベストプラクティスに移行

以下のガイダンスは、初期アンチスパイウェア プロファイルを定義し、ベストプラクティスのプロファイルへの移行を開始する際に、ブロックまたはアラートアクションのどちらから開始するかを決定するのに役立ちます。

アンチスパイウェアを利用するには、高度な脅威防御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。

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。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。

- ビジネスクリティカルなアプリケーション–アプリケーションの可用性を確保するために、初期アクションをアラートに設定します。しかしながら、ある状況では、最初からブロックアクションを使用することができます。例えば、重大で、高いおよび/または中程度のシグネチャをブロックするアンチスパイウェアプロファイル付きのアプリケーションで既に保護されており、プロファイルがビジネスとセキュリティのニーズに適合しているのであれば、ス

パイウェアをブロックし、アプリケーションを保護するために同様のプロファイルを使用することができます。

警告アクションは脅威ログを分析し、ブロックアクションに移る前に必要であれば例外を作成することが可能です。ブロッキングに移行する前にアラートとモニタリングを行うことで、次のことを確信できます。

- プロファイルはデプロイ時にビジネスクリティカルなアプリケーションをブロックしません。
- ブロッキング状態に移行するときに、アプリケーションの可用性を維持するために必要な例外を作成します。

決めなければならない全ての例外とプロファイルをそれに従って構成することを把握し、特に問題がなければすぐにベストプラクティス状態に移行します。

- 重大で危険度の高いシグネチャーフォルスポジティブの割合は、一般的に低いです。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。
- 中程度に危険なシグネチャー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。まず、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送信し、外部向け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することから始めます。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すべきか、許可する必要があるかを確認します。
- 重要度の低いシグネチャーこれらのシグニチャのほとんどに対するデフォルトアクションは、アラートまたは許可です。すべての低く情報的なシグネチャに警告しなければならない特定の必要性がない限り、デフォルトアクションで始めます。
- リソースに余裕がある場合は、移行中に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ます。パケットキャプチャーを有効にすると、必要に応じてイベントを非常に詳細に調査することができます。ベストプラクティスプロファイルに移行するにつれて、情報量が少ないイベントによってパケットキャプチャアクティビティが多すぎる（トラフィック量が多すぎる）ため、情報が役に立たない場合は、これらの重大度ではパケットキャプチャを無効にする方法に移行してください。

  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。
- 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。

- **DNS**ポリシー:
  - DNSシグネチャのポリシーアクションを**Sinkhole**に設定して、疑わしいドメインにアクセスしようとする侵害の可能性があるホストを特定します。DNSシンクホールを使用すると、ホストを追跡し、それらのドメインにアクセスできないようにすることができます。(DNSシンクホールをすぐに有効にするのがベストプラクティスです)。 **packet capture** (パケット キャプチャ)を拡張キャプチャに設定します。
  - **DNS**セキュリティドメインタイプをすべてシンクホールし、図1 (PAN-OS 10.0以降) に示すように**Packet Capture**(パケットキャプチャ)を設定します。
  - さらに、すべての DNS レコードタイプは暗号化された DNS クエリで使用されるため、すべてブロックしてください。これにより、DNS 解決プロセス中にクライアントが client hello を暗号化して、キー情報の交換がブロックされるのを防ぐことができます。

制裁対象の *DNS* サーバーへのトラフィックのみを許可します。DNS セキュリティ サービス を使用して、悪意のある *DNS* サーバーへの接続を防ぎます。

PAN-OS ベースのシステムでは、*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。

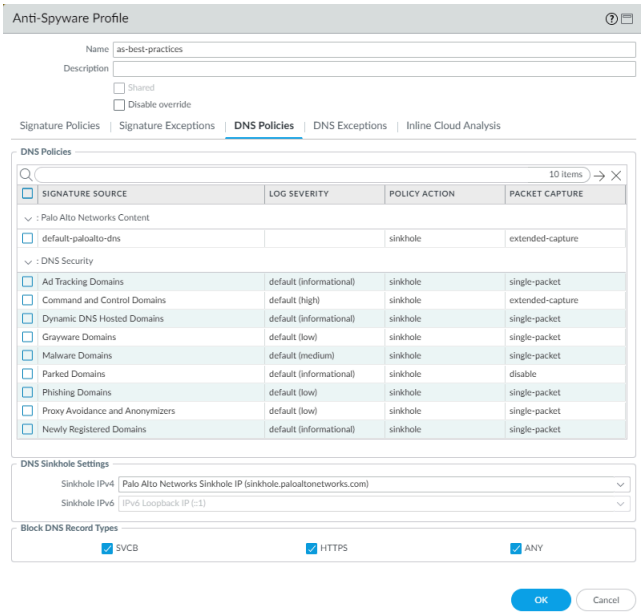


図 **3 :** アンチスパイウェア プロファイルの **DNS**ポリシー

- インラインクラウド分析 (高度な脅威防御サブスクリプションとPAN-OS 10.2以降が必要) – 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。

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。

初期プロファイルの導入時、ビジネスに重要なアプリケーションがアラートやブロックを生じさせていないかを把握するのに充分な期間脅威ログを監視します。慣れたらすぐに、ベストプラクティスのアンチスパイウェア プロファイルに移行してください。完全なベストプラクティス アンチスパイウェア プロファイルを導入する前に確認されたフォルスポジティブを修復するに、必要な個々のプロファイルに必要に応じて例外を作成します（必要であればサポートチケットを開く）。

アンチウイルスプロファイルを安全にベストプラクティスに移行する

次のガイダンスは、デフォルトのアンチウイルスプロファイルのクローンを作成し、初期プロファイルを定義してベストプラクティスプロファイルへの移行を開始するときに、ブロックアクションとアラートアクションのどちらから始めるかを決定するのに役立ちます。

ウイルス対策には、高度な脅威防止またはアクティブなレガシー脅威防御サブスクリプションが必要です。

脅威を特定して防ぐには、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。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。

- ビジネスクリティカルなアプリケーション–アプリケーションの可用性を確保するために、初期アクションをアラートに設定します。しかしながら、ある状況では、最初からアンチウィルスシグネチャをブロックすることができます。例えば、同様のアプリケーションをアンチウイルスプロファイルで既に防護しており、プロファイルがビジネスとセキュリティのニーズに合致していると確信している時は、既に何をブロックしれいるのか把握していることから、同様のアプリケーションを保護するために同様のプロファイルを使用できます。

アラートアクションは、ブロックアクションに移行する前に脅威ログ（***Monitor***（モニター） > ***Logs***（ログ） > ***Threat***（脅威））を分析し、必要であれば例外を作成することができます。ブロッキングに移行する前に警告と監視を行うことで、次のことを確実に実行できます。

- プロファイルはデプロイ時にビジネスクリティカルなアプリケーションをブロックしません。
- ブロッキング状態に移行するときに、アプリケーションの可用性を維持するために必要な例外を作成します。

初期のアラートアクションを維持する時間長を、セキュリティ インシデントの機会を低減するため最小に維持します。決めなければならない全ての例外とプロファイルをそれに従って構成することを把握し、特に問題がなければすぐにベストプラクティス状態に移行します。

- 重要かつ高重大度のシグネチャ–ベストプラクティスのアンチウイルスプロファイルを導入して、ビジネスに重要でないアプリケーションの悪意のあるトラフィックをすぐにブロックしても安全です。誤検出率が低いため、不要なブロックはほとんど発生しません。
- 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、インターネットに接続するトラフィックにはアンチウイルスプロファイル、内部トラフィックには別のアンチウイルスプロファイルが必要になることがあります。
- 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。
- アンチウイルス プロファイルの WildFire Action 設定は、トラフィックが WildFire シグニチャを生成し、その結果としてリセットまたは廃棄アクションが発生する場合、トラフィックに影響を与える可能性があります。

初期プロファイルの導入時、ビジネスに重要なアプリケーションがアラートやブロックを生じさせていないかを把握するのに充分な期間脅威ログを監視します。また、ビジネスに重要なア

プリケーションがアンチウイルスプロファイル WildFireアクションにより警告やブロックを起こすかどうかを把握するのに充分な時間、WildFire送信ログをモニターします（**Monitor**（モニター） > **Logs**（ログ） > **WildFire Submissions**（**WildFire**サブミッション））。 あるいはデータセンター用の完全なベストプラクティスアンチウイルスプロファイルを導入する前に確認されたフォルスポジティブを修復するに必要な個々のプロファイルに必要に応じ例外を作成（必要であればサポートチケットを開く）します。ベストプラクティスプロファイルへの移行速度は、ビジネス、アプリケーション、および快適さのレベルによって異なります。アプリケーションによっては、監査、定期的なイベントや会議などに毎週、毎月、四半期、または毎年しか使用されないことに注意してください。

WildFireプロファイルを安全にベスト プラクティスに移行

次のガイダンスは、WildFire分析プロファイルの初期構成を定義するのに役立ちます。

パロアルトネットワークスの次世代ファイアウォールには、基本的な WildFire サービスが含まれており、高度な WildFire (またはアクティブな従来の WildFire) サブスクリプションは必要ありません。基本サービスでは、ファイアウォールが分析のために PE ファイルを転送し、24 ～ 48 時間ごとにウイルス対策および/または脅威防御のアップデートを使用してのみ高度な WildFire シグネチャを取得できるようにします。高度な WildFireサブスクリプション (PAN-OS 10.0 以降) または従来の WildFire サブスクリプションには、リアルタイムでのアップデートの受信、より多くのファイル タイプのサポート、API など、さらに多くの機能が含まれています。

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。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。

WildFireシグネチャの生成は非常に正確で誤判定は稀です。デフォルトの WildFire分析プロファイル (ベスト プラクティス プロファイル) を展開しても、ネットワーク トラフィックには影響しません。(しかしながら、アンチウイルス プロファイル へのWildFire 設定は、もしトラフィックがリセットあるいはドロップアクションの結果となる WildFire シグネチャを生成する場合、トラフィックにインパクトを与えるかもしれません。)

初期プロファイルを用意したら、WildFire送信ログ (**Monitor** > **Logs** > **WildFire Submissions**) を十分な時間監視して、ウイルス対策プロファイル WildFire アクションが原因でビジネス クリティカルなアプリケーションがアラートまたはブロックを引き起こしているかどうかを確実に理解できるようにします。確認されたフォルスポジティブを修復するため必要に応じてアンチウイルス内に例外を生成します（必要であればサポートチケットを開きます）。

URLフィルタリング プロファイルを安全にベスト プラクティスに移行

初期のURLフィルタリング プロファイルを定義するようにブロックあるいは警告アクションでスタートするかどうかの決定を助けるため下記のガイドラインを使用します。そしてベストプラクティス プロファイルへの移行を始めます。URLフィルタリング ファイルをインターネット トラフィックに適用します。（URLフィルタリング プロファイルを内部トラフィックには適用ないでください）

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、トラフィックを復号化して正確な *URL* を明らかにする必要があるため、*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。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。

高度な URLフィルタリングに はサブスクリプションが必要です。

- 事前定義済みの URL カテゴリは非常に正確であるため、さまざまなタイプの Web サイトへのアクセスを許可または拒否するには企業のポリシーに従って構成されたカテゴリ アクションでURLフィルタリング プロファイルを実装するのが安全です。
- マルウェア、コマンド・アンド・コントロール、著作権侵害、過激思想、フィッシング、ランサムウェア、ダイナミック DNS、ハッキング（ただし、社内 PEN テスターは例外）、プロキシ回避・匿名化など、既知の悪質な URL カテゴリのサイトアクセスとユーザークレデンシャルの送信を最初からブロックします。
- URL カテゴリが不明 (サイト PAN-DB がまだ識別していない)、パーク (資格情報フィッシングによく使用される)、グレーウェア (悪意のあるまたは疑わしい)、および新規登録ドメイン (悪意のあるアクティビティによく使用される) については、最初にアラートを発します。これらのカテゴリをブロックするベストプラクティスに移行する前に、正規の Web サイトがアラートをトリガーした場合に備えて、URLフィルタリング ログを監視できます (ログ > 監視 > **URL** フィルタリング)。
- 他のすべての URL カテゴリを アラート に設定し、トラフィックのログを生成します。アクセスが 許可に設定されている場合、ファイアウォールはトラフィックを記録しません。URL フィルタリング ログを監視して、他のカテゴリをブロックするかどうかを確認します。

  高リスク、中リスク、低リスクのカテゴリを他のカテゴリと組み合わせて、どのトラフィックを許可、ブロック、復号化するかを決定できます。たとえば、高リスクの *Web* サイトと金融サービスの両方の *Web* サイトへのアクセスをすべてブロックできます。または、ファイアウォールでリソースを節約する必要がある場合は、一部のカテゴリの高リスクおよび中リスクのトラフィックをすべて復号化し、それらのカテゴリの低リスクのトラフィックを復号化しないこともできます。

初期プロファイルの導入時、ビジネスに重要なサイトが、もし警告からブロッキングへ、そしてベストプラクティスURL フィルタリング プロファイルへ移行した場合、ブロックされるかどうかを把握するのに充分な時間URLフィルタリング プロファイルをモニターします。与えられたURLが正しくカテゴライズされていないと考える場合、URLが正しいカテゴリに含まれるようにURL 再カテゴリ化 します。ベストプラクティス プロファイルへの移行速度は、ビジネス、アプリケーション、快適さのレベルによって異なります。

ファイル ブロッキング プロファイルを安全にベスト プラクティスに移行

以下のガイダンスは、初期ファイル ブロック プロファイルを定義し、ベストプラクティスのプロファイルへの移行を開始する際に、ブロックまたはアラートアクションのどちらから開始す

るかを決定するのに役立ちます。ファイル タイプによるログの生成を許可するのではなく、アラートを発行してトラフィックを可視化します。

- ベストプラクティス ファイル ブロック プロファイルはアプリケーションの種類によって異なることが多く、インバウンド トラフィック、アウトバウンド トラフィック、および内部トラフィックでも異なる場合があります。以下に例を示します。
  - 内部アプリケーションがファイルの種類の転送に依存していて、ベストプラクティスのファイル ブロック プロファイルでブロックが推奨されている場合は、それらファイルの種類を内部アプリケーションに許可します(dllファイルなど)。これらのファイル転送タイプは、すべてのアプリケーションではなく、必要な内部アプリケーションに対してのみ許可します。
  - インターネット ベースのトラフィックに関しては、攻撃者が悪意のあるファイルを配信したり、攻撃面を低減するために、非常に厳格なアプローチをとります。
  - データセンターのトラフィックに関しては、攻撃可能な箇所を縮小し、価値ある財産を守るためより厳格なアプローチ（他のファイル転送タイプはブロックする内部アプリケーションは例外）を採ります。
  - 例外を設定する場合は、最小特権の原則に従い、ビジネス目的でそのファイル タイプにアクセスする必要があるアプリケーションとユーザーにのみ例外を適用します。
- ビジネス クリティカルなアプリケーション–すべてのファイル タイプに対するアラート アクションから開始し、できるだけ早く ベストプラクティスのファイル ブロック プロファイル に移行します。すでにブロック制御を導入している場合は、それを複製し、ブロックする必要がある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ます。
- ビジネスクリティカルではないアプリケーションの場合は、ベストプラクティスのファイル ブロック 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 トラフィックとアウトバウンド トラフィック-
    7z、bat、chm、class、cpl、dll、dlp、hta、jar、ocx、pif、scr、torrent、vbe、および wsf ファイルを ブロック する アクション を設定します。他のすべてのファイルについて アラート を発するように アクションを 設定します。
  - 内部トラフィック-
    7z、bat、chm、class、cpl、dlp、hta、jar、ocx、pif、scr、torrent、vbe、および wsf ファイルをブロックします (これは、.dll で警告を発する点を除き、インバウンド/アウトバウンド プロファイルと同じです)ファイルをブロックするのではなく)。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。

プロファイル ルールを微調整して、特にインターネットに接続されたトラフィックやデータセンターのトラフィックに対して、できるだけ早く警告を発してブロックに移行します。特定のファイル タイプにブロック アクションを設定する前にファイル タイプの使用法を理解するため、データ フィルタリング ログ（**Monitor**（モニター） > **Logs**（ログ） > **Data Filtering**（データフィルタリング））をモニターします。ビジネス クリティカルなアプリケーションや社内のカスタム アプリケーションに必要なファイルの種類を学習したら、ビジネス ニーズをサポートするために必要に応じて変更されたベストプラクティスのファイル ブロック構成に移行してください。

インターネット ゲートウェイの最良のセキュリティ プロファイルを作成

大抵のマルウェアは、正当なアプリケーションやサービスからネットワーク内に潜入します。アプリケーションを安全に有効にするには、許可されているすべてのトラフィックをスキャンして脅威を検出する必要があります。トラフィックを許可するすべてのセキュリティポリシー ルールにセキュリティ プロファイルを付与し、ネットワーク トラフィック内の脅威（未知および既知）を検出できるようにしなければなりません。次のベスト プラクティスの推奨事項は、最も厳格なセキュリティに焦点を当てています。URL フィルタリング プロファイルをインターネット経由のトラフィックを許可するすべてのルールに添付し、他のプロファイルをすべての許可ルールに添付します。

Web トラフィックの 90% 以上が暗号化されています。復号化 を有効にしてトラフィックを可視化し、セキュリティ プロファイルを使用してペイロードを検査し、悪意のあるイベントを防止します。

ベストプラクティスのセキュリティ プロファイルを デフォルトのセキュリティ プロファイル グループに追加することを検討してください。セキュリティ プロファイル グループに「**default**」という名前を付けると、ファイアウォールは、作成するすべての新しいセキュリティ ポリシー ルールにそのグループを自動的に付加し、トラフィックに悪意のあるアクティビティがないか検査するようにします。

また、さまざまな種類のトラフィック用に専用のセキュリティ プロファイル グループを作成することも検討してください。セキュリティ プロファイル グループを使用すると、必要なすべてのプロファイルをセキュリティ ポリシー ルールに簡単に適用できるようになり、重要なプロファイルが忘れられることがなくなります。

- インターネット ゲートウェイのファイルブロッキングプロファイルのベストプラクティス
- インターネット ゲートウェイのアンチウイルス プロファイルのベストプラクティス
- インターネット ゲートウェイの脆弱性保護プロファイルのベストプラクティス
- インターネット ゲートウェイのアンチスパイウェア プロファイルのベストプラクティス
- インターネット ゲートウェイの URL フィルタリング プロファイルのベストプラクティス
- インターネット ゲートウェイの WildFire 分析プロファイルのベストプラクティス

インターネット ゲートウェイのファイルブロッキングプロファイルのベストプラクティス

マルウェア攻撃に頻繁に使用され、かつアップロード/ダウンロードを行う意味がないファイルタイプをブロックする、事前定義済みの厳格なファイルブロッキングプロファイルを作成します。これらのファイル タイプをブロックすると、攻撃対象領域が減少します。事前定義済みの厳格なプロファイルは、バッチファイル、DLL、Java クラス ファイル、ヘルプ ファイル、Windows ショートカット（.lnk）、BitTorrent ファイル、.rar ファ

イル、.tar ファイル、encrypted-rar および encrypted-zip ファイル、マルチレベル エンコード ファイル（最大 4 回、暗号化あるいは圧縮されたファイル）、.hta ファイル、および .exe、.cpl、.dll、.ocx、.sys、.scr、.drv、.efi、.fon、.pif などを含む Windows Portable Executable（PE）ファイルをブロックします。事前定義済みの厳格なプロファイルは他のすべてのファイル タイプについてアラートを生成し、他のファイル転送について可視性を持たせ、ポリシーの変更を行う必要があるかどうか判断できるようにします。

重要なアプリケーションをサポートする必要があり、厳格なプロファイルのファイル形式をすべてブロックできないケースもあります。ファイル ブロッキング プロファイルを安全にベスト プラクティスに移行アドバイスに従って、ネットワークの異なるエリアで例外を作る必要があるかどうかを決定します。データフィルタリング ログ（***Monitor***（モニター） > ***Logs***（ログ） > ***Data Filtering***（データフィルタリング）を確認してファイル形式を把握し、関係者と相談してアプリケーションで必要なファイル形式を決定してください。その情報に基づき、厳格なプロファイルをクローンして編集し、重要なアプリケーションをサポートするために必要な他のファイル形式だけを許可します。また、***Direction***（方向）設定を使用し、対象のファイル形式が双方向に流れるのを制限したり、片方の方向にファイルが流れるのだけをブロックしたりできます。

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

Windows アップデートなどのアクティビティで悪意のある目的でよく使用されるプロトコルがいくつか必要になる場合もあります。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に対してプロトコルを許可する例外を作成するには、次の手順を実行します。

1. 他のトラフィックに対してブロックしたいプロトコルを使用する必要なユーザーとビジネス 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. 厳密なファイル ブロック プロファイルを複製し、必要なプロトコルを許可するように変更して、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。

このプロファイルが必要な理由

攻撃者はさまざまな方法で悪意のあるファイルを配布する可能性があります。

- 企業または個人の電子メール内の添付ファイルまたはリンク。
- ソーシャルメディアやその他のソースのリンクまたは IM。
- エクスプロイトキット。

- ファイル共有アプリケーション (FTP、Google ドライブ、Dropbox など)。
- USB ドライブ。
-

厳密なファイル ブロック プロファイルをアタッチすると、この種の攻撃が防止され、攻撃対象領域が減少します。

すべての PE ファイルをブロックしないことを選択した場合は、すべての不明なファイルを分析のために WildFire に送信します。Java アプレットや実行ファイルといった悪意のあるファイルをインストールさせるコンテンツをエンドユーザーがダウンロードする時に知らない間に発生する、ドライブバイダウンロード攻撃を継続的に防止できるよう、アクションを設定します。また、ドライブバイダウンロード攻撃はユーザーがウェブサイトを訪問する際、電子メールを閲覧する際、偽装されたポップアップ ウィンドウを表示する際に発生することがあります。よく分かっていないファイル転送を続行してもよいか尋ねられた場合、危険なダウンロードを行おうとしている可能性があるということを各ユーザーに周知させてください。さらに、脅威を運ぶ可能性のあるファイル タイプを許可する必要がある場合は、URL フィルタリングによるファイル ブロックを使用して、ユーザーがファイルを転送できるカテゴリを制限し、攻撃対象領域を減らします。

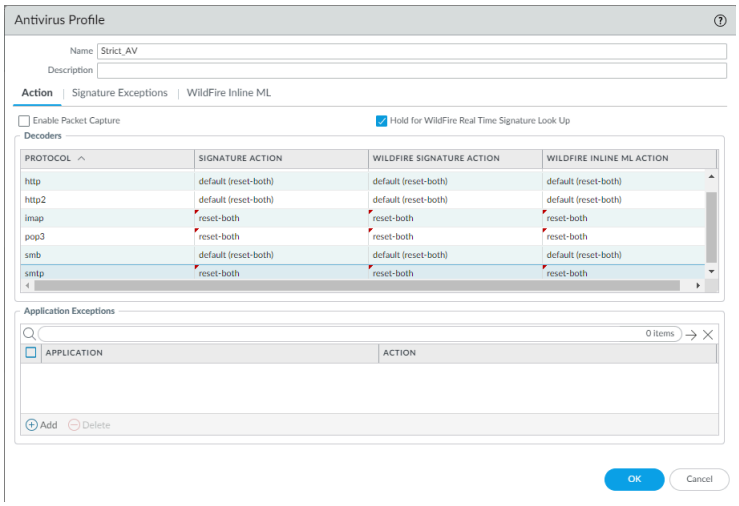
インターネット ゲートウェイのアンチウイルス プロファイルのベストプラクティス

業務に必須のアプリケーションを常に使えるようにするには、現在の状態からベストプラクティス プロファイルに移行する際、アンチウイルスプロファイルを安全にベストプラクティスに移行するのアドバイスに従います。目標は、ここに示すようにプロファイルに移行し、それをトラフィックを許可するすべてのセキュリティ ポリシー ルールにアタッチすることです。アンチウイルスプロファイルには、次の7つのプロトコルを介して転送されるウイルスおよびマルウェアを検出して防止するプロトコルデコーダーが備わっています：FTP、HTTP、HTTP2、IMAP、POP3、SMB、および SMTP。

7 つすべてのプロトコルに対して WildFire シグネチャと WildFire インライン ML アクションを設定し (ウイルス対策プロファイルは、WildFire シグネチャに基づくアクションも強制します)、まだ実行していない場合は、次に示すようにリアルタイム シグネチャ検索を有効にします。 アンチウイルスプロファイルを安全にベストプラクティスに移行する。

7つのすべてのプロトコルデコーダーおよびWildFireアクションを両方ともリセットするよう、クローンしたアンチウイルスプロファイルを設定した後、セキュリティポリシー許可ルールにプロファイルを付与します。

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。



リアルタイム シグネチャ検索をグローバルおよびウイルス対策プロファイルで有効にして、ファイアウォールがクラウドから最新のリアルタイム ウイルス対策シグネチャを受信するまでファイルを保持します。

- グローバルに有効にする:[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 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。ウイルス対策プロファイルでリアルタイム シグネチャ検索を有効にするには、グローバルで有効にする必要があります。
- ウイルス対策プロファイルで **WildFire** リアルタイムシグネチャ検索の保留を 有効にします。ファイルを保持して WildFire が最新のウイルス対策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 マルウェアや古いウイルス対策シグネチャから保護します。

このプロファイルが必要な理由

アンチウイルス プロファイルをすべてのセキュリティルールに付与することで、ネットワークに侵入しようとする悪意のある既知のファイル（マルウェア、ランサムウェア ボット、ウイルス）をブロックします。ユーザーに悪意のあるファイルを受信させる方法としてよくあるのが悪意のある電子メール添付、悪意のあるファイルをダウンロードさせるリンク、そして脆弱性をエクスプロイトして自動的に悪意のあるペイロードをエンドユーザーのデバイスにダウンロードするエクスプロイトキットを利用した密かなセキュリティ攻撃などがあります。

インターネット ゲートウェイの脆弱性保護プロファイルのベストプラクティス

脆弱性保護プロファイルを許可されたすべてのトラフィックに付与し、バッファオーバーフロー、不正なコードの実行、およびクライアント側およびサーバー側の脆弱性を狙ったその他の攻撃から保護します。業務に必須のアプリケーションを常に使えるようにするには、現在の状態からベストプラクティス プロファイルに移行する際、脆弱性防御プロファイルを安全にベストプラクティスに移行のアドバイスに従います。事前定義された厳密な脆弱性保護プロファイルのクローンを作成し、それを編集してベスト プラクティス プロファイルを作成します。

- 3 つのブルート フォース ルールの アクションを両方リセットに変更し、パケット キャプチャを単一パケット に変更して、ブルート フォース攻撃イベントのアラートからブロックに移行します。
- サーバーとクライアントの重要度、高度、中度のイベントを 1 つのルールに統合します。**[Action]** を **[reset-both]** に設定し、**[Packet Capture]** を **[single-packet]**に設定します。これにより、プロファイルはこれらの重大度に対して同じアクションと同じパケット キャプチャ設定を使用するため、プロファイルが簡素化され、機能します。

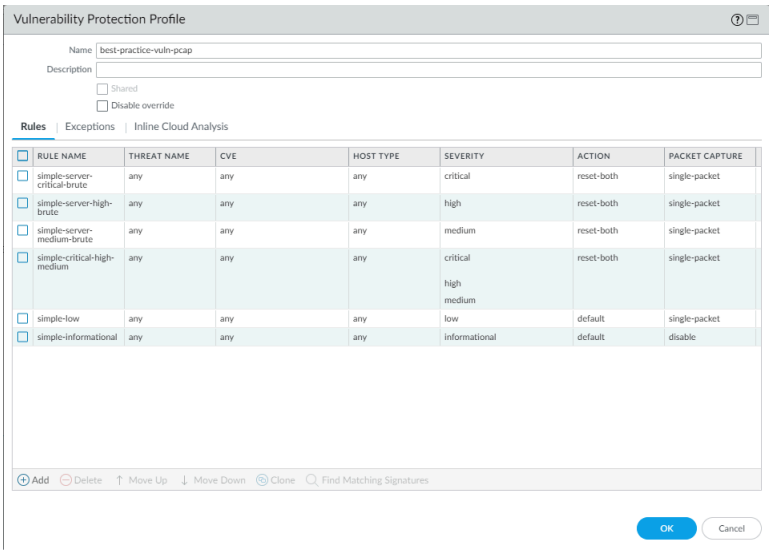
  内部 (東西) トラフィックを制御するプロファイルの場合、中程度の重大度のイベントをブロックすると、ビジネス アプリケーションに影響を与える可能性があります。ブロックがビジネス アプリケーションに影響を与える場合は、*[アクション]* を ***[alert]***に設定して、中程度の重大度のイベント用の別のルールをプロファイルに作成します。プロファイルを内部トラフィックにのみ適用します。
- プロファイルを簡素化するには、サーバーとクライアントの重大度の低いイベントを 1 つのルールに統合します。[アクション] を [デフォルト] に設定し、[パケット キャプチャ] を **[single-packet]**に設定します。
- サーバーとクライアントの情報イベントを 1 つのルールに統合します。[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]に設定します。

  情報イベントの PCAP は比較的大量のトラフィックを生成しますが、これは通常、潜在的な脅威に関するキャプチャと比較して役に立ちません。
- 単一 PCAP の代わりに拡張 PCAPを、**alert**（アラート）アクションを適用する高価値のトラフィックに適用します。ログに記録するトラフィックを指定するために使用するロジックと同じものを使用する PCAP を適用し、ログに記録するトラフィックの PCAP を取ります。単一 PCAP をブロックするトラフィックに適用します。拡張 PCAP が記録して管理プレーンに送信するデフォルトのパケット数は 5 パケットであり、これが推奨される値になります。大抵の場合、5 つのパケットをキャプチャすれば脅威を分析するのに十分な情報を得られます。過剰な PCAP トラフィックが管理プレーンにいく場合、5 つよりも多くパケットをキャプチャすると PCAP がドロップされるおそれがあります。

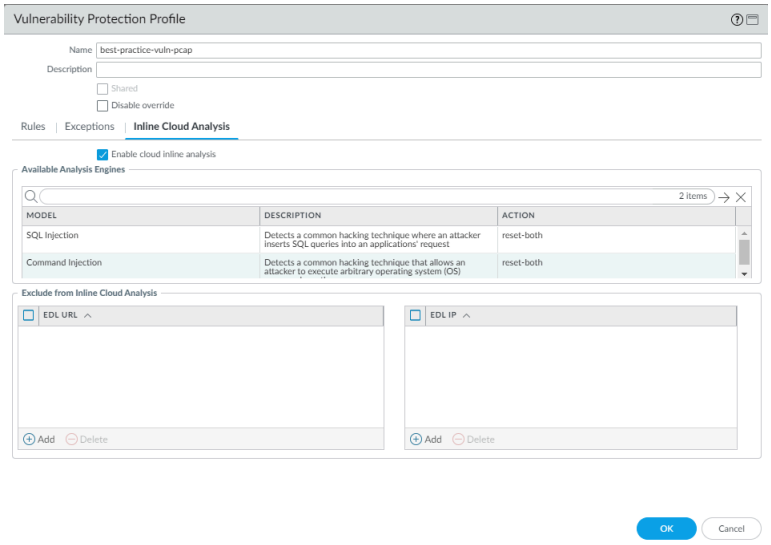
プロファイルをさらに細かく微調整したい場合は、説明に従って アクション と パケット キャプチャの 設定を使用して別のルールを作成します。たとえば、サーバーに対して重大度、高、中程度の重大度のルールを作成し、クライアントに対して別の同様のルールを作成するか、クライアントとサーバーの重大度ごとに個別のルールを作成して、必要な粒度および制御のレベルを実現します。

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。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) をチェックして、パケット キャプチャを実装する前後の使用状況を把握し、必要なパケット キャプチャを取得するのに十分なリソースがシステムにあることを確認します。

潜在的な攻撃の送信元を追跡できるように、ルールごとに パケット キャプチャ (PCAP) を有効にします。シグネチャセットが常に最新に保たれるよう、content updates（コンテンツ更新）を自動的にダウンロードし直ちにインストールします。



インライン クラウド分析の場合、 アクションを両方リセットに設定し、 一般的なハッキング手法をブロックします。



このプロファイルが必要な理由

厳格に脆弱性を保護しなければ、攻撃者がクライアント側およびサーバー側の脆弱性を利用してエンドユーザーを危険にさらすリスクが生じます。例えば、攻撃者は脆弱性を利用して悪意のあるコードをクライアントシステムにインストールしたり、エクスプロイトキットを使用して自動的に悪意のあるペイロードをエンドユーザーに送ったりします。脆弱性保護プロファイルは攻撃者が内部ホストの脆弱性を利用してネットワーク内で横方向に移動するのを防ぎます。

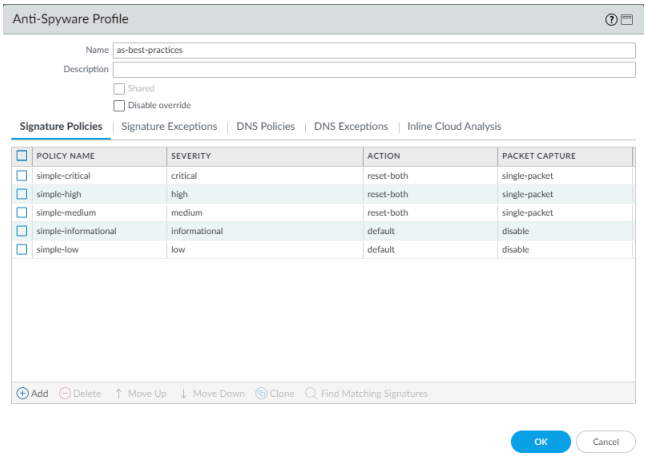
インターネット ゲートウェイのアンチスパイウェア プロファイルのベストプラクティス

アンチスパイウェア プロファイルを許可されたすべてのトラフィックに付与し、サーバーあるいはエンドポイント上で実行された悪意のあるコードが開始したコマンド アンド コントロール

トラフィック（C2）を検知し、攻撃されたシステムがネットワークからアウトバウンドの接続を確立するのを防ぎます。事前に設定された厳格なアンチスパイウェアプロファイルを複製し、編集します。ビジネス 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、 スパイウェア対策プロファイルをベスト プラクティスに安全に移行します。プロファイルを編集し、必ず DNS シンクホールおよびパケット キャプチャを有効化して悪意のあるドメインを解決しようとしたエンドポイントの追跡に役立てるようにします。ファイアウォールが中、高、または重大度の脅威を検出したときに接続をリセットするデフォルトの アクション を保持し、それらの脅威に対して単一の PCAP を有効にします。

認可された *DNS* サーバーへのトラフィックのみを許可します。DNS セキュリティ サービス を使用して、悪意のある *DNS* サーバーへの接続を防ぎます。

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するトラフィック用のアンチスパイウェア プロファイルと、内部トラフィック用の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。



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

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。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) をチェックして、パケット キャプチャを実装する前後の使用状況を把握し、必要なすべてのパケット キャプチャを取得するのに十分なリソースがシステムにあることを確認します。

ネットワークを、悪意のあるドメインへのDNSクエリから保護するように、DNSポリシーを設定します。最高のセキュリティを実現するには 、DNS セキュリティ サービス を使用して DNS トラフィックを保護します。それ以外の場合は、ローカルで利用可能でダウンロード可能な DNS シグネチャ セット (ウイルス対策および WildFire アップデートにパッケージされている) を使用します。

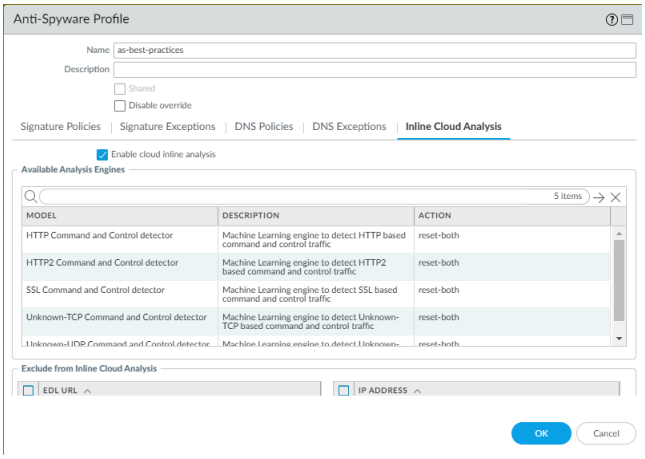
悪意のあるトラフィックをブロックするのではなくシンクホールして、ホストを追跡し、それらのドメインへのアクセスを阻止することで、疑わしいドメインにアクセスしようとする侵害された可能性のあるホストを特定します。より大きな脅威をもたらすドメイン カテゴリの場合は、より高いログ重大度レベルやパケット キャプチャ設定を構成して、攻撃が成功したかどうかを判断し、攻撃方法を特定し、より適切な全体的なコンテキストを提供できるようにします。

デフォルトの Palo Alto Networks DNS と個々の DNS シグネチャ ソース カテゴリ (PAN-OS 10.0 以降) を構成します。

DNS シグネチャ ソース	ログ重大度	Policy Action（ポリシーアクション）	パケット キャプチャ
Palo Alto Networksコンテンツ			
default-paloalto-dns	default（デフォルト）	シンクホール	extended-capture
DNS セキュリティ			
コマンドアンドコントロールドメイン	高 (デフォルト)	シンクホール	extended-capture
ダイナミックDNS主催ドメイン	情報 (デフォルト)	シンクホール	単一パケット
グレイウェアドメイン	低 (デフォルト)	シンクホール	単一パケット
マルウェアドメイン	中 (デフォルト)	シンクホール	単一パケット
パークドメイン	情報 (デフォルト)	シンクホール	無効（デフォルト）
フィッシングドメイン	低 (デフォルト)	シンクホール	単一パケット
プロキシ回避とアノニマイザ	低 (デフォルト)	シンクホール	単一パケット
新しく登録されたドメイン	情報 (デフォルト)	シンクホール	単一パケット
広告追跡ドメイン	情報 (デフォルト)	シンクホール	単一パケット

インライン クラウド分析 (Advanced Threat Prevention サブスクリプションが必要) の場合は、すべての送信トラフィックで クラウド インライン分析を有効にします 。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。

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



インターネット ゲートウェイの URL フィルタリング プロファイルのベストプラクティス

高度な URL フィルタリング を使用して、悪意のあるアクティビティのリスクが高い Web コンテンツへのアクセスを防ぎます。ウェブベースのアプリケーションへのアクセスを許可するすべてのルールにURLフィルタリング プロファイルをアタッチ（付与）し、マルウェアや、潜在的なマルウェア、責任リスク、悪意のあるコンテンツをホストしていることをPalo Alto Networksが確認しているURLから保護します。

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、トラフィックを復号化して正確な *URL* を明らかにする必要があるため、*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。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。

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、 URLフィルタリング プロファイルを安全にベスト プラクティスに移行。ベスト プラクティス URL フィルタリング プロファイルは、既知の危険な URL カテゴリと認証情報の送信をすべてブロックするように設定します。目標は、次のカテゴリをブロックすることです。

- 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資格情報の送信の両方をブロックします。必要に応じて、PEN テスト、脅威調査、情報セキュリティに対して適切な例外を作成します。
  - コマンドアンドコントロール：マルウェアまたは侵害されたシステムが攻撃者のリモートサーバーと通信するために使用する URL とドメイン。
  - グレイウェアーこれらのサイトは、ウイルスの定義や直接的なセキュリティ上の脅威をもたらすものではないが、ユーザーにリモート・アクセスを許可したり、その他の不正な行

動を実行するよう影響を与えます。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「タイポスクワッティング」ドメインを含むその他の迷惑アプリケーションが含まれます。

- マルウェア–[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 アクティビティ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、標的型攻撃を実行したりするサイト。

- 一部の URL カテゴリは悪意がある可能性が高いですが、確実に悪意があるわけではありません。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。必要に応じて、PEN テスト、脅威調査、情報セキュリティに対して適切な例外を作成します。

- **Dynamic-dns**—動的に割り当てられた IP アドレスを持つシステム。マルウェア 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ます。

  ダイナミック*DNS*ドメインの業務目的がある場合は、これらの*URL*が*URL*フィルタリングプロファイルで許可されていることを確認しましょう。

- 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または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。
- **new-registered-domains**—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。
- **not-resolved**- 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。
- **proxy-avoidance-and-anonymizers (**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。

- 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。

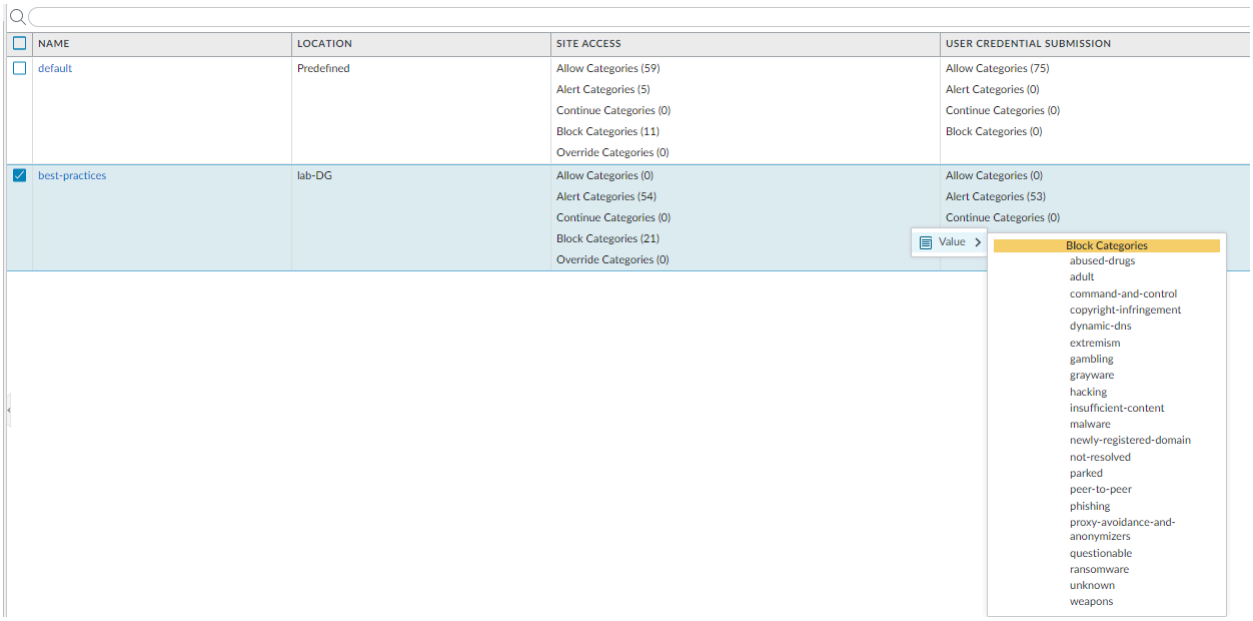
これらのサイトをブロックしない場合は、トラフィックに警告を発し、厳格なセキュリティ プロファイルを適用します。

- 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 -法的責任のリスクを引き起こす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、児童搾取などを奨励する Web サイト。
- ギャンブル- 宝くじおよびギャンブルのサイト。
- ピアツーピアー 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。)
- 疑わしい- 悪趣味なユーモアや、特定の層をターゲットにした不快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。

- 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。)

既知の好ましくないカテゴリをブロックすることに加え、他のすべてのカテゴリについてアラートを発することで、ユーザーが訪問しているサイトに対する可視性を確保することができます。ブロック ポリシーを段階的に導入する必要がある場合は、カテゴリをcontinue（継続）に設定し、カスタム応答ページを生成します。これにより、ユーザーに利用規約を周知し、脅威をもたらす可能性があるサイトを閲覧しているという事実に注意を喚起することになります。これにより、モニタリング期間後にそのカテゴリを完全にブロックできるようになります。



プロファイル内で ログ コンテナ ページのみ を無効にします。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。

PAN-OS 9.0.4以降を実行している場合は、クライアント要求を保持するオプションを有効にして（**config**を入力し、**set deviceconfig setting ctd hold-client-request yes**と入力）、ファイアウォールがユーザーのWeb要求を可能な限り安全に処理するようにします。デフォルトで、ファイアウォールはPAN-DBのキャッシュされていないURLカテゴリをルックアップしている間、リクエストを許可し、サーバーが応答すると適切なポリシーを適用します。セキュリティを最大化するために、この検索中にリクエストを保留します (これにより待ち時間が長くなる可能性がありますが、最も安全なオプションです)。詳細は、「URLフィルタリングの設定」を参照してください。

推奨されるすべてのカテゴリをブロックできない場合

ビジネス目的でユーザーがブロックされたカテゴリのサイトにアクセスする必要がある場合、リスクが正当であると思われる場合は、必要なユーザーとアプリケーションのみを許可するルールで特定のサイトのみの許可リストを作成します。ブロックできる、ブロックできない、またはブロックしなければならないサイトのタイプを規定している地域ごとの法規制について把握しておく必要があります。アクセスを許可することにした危険なカテゴリでは、 認証情報フィッシング保護を設定して 、フィッシング攻撃をホストする可能性のあるサイトにユーザーが企業認証情報を送信しないようにします。

悪意のある URL カテゴリ、または潜在的に責任問題を引き起こす Web サイトへのトラフィックを許可すると、次のようなリスクが生じます。

- 悪意のある URL カテゴリ:
  - **command-and-control** (コマンド アンド コントロール)–マルウェアや感染したホストが、密かに攻撃者のリモートサーバーと通信を行って悪意のあるコマンドを受信したりデータを盗んだりするために使用する、コマンド アンド コントロール URL およびドメイン。
  - **grayware** (グレイウェア)–ウイルスの定義には適合していませんが、悪意があるか疑わしく、デバイスのパフォーマンスを低下させ、セキュリティリスクを引き起こす可能性のある Web サイトおよびサービスです。コンテンツ リリース バージョン 8206 より前は、ファイアウォールはグレイウェアをマルウェアまたは疑わしい URL カテゴリのいずれかに分類していました。グレイウェアをブロックするかどうかわからない場合は、まずグレイウェアでアラートを生成し、アラートを調査してから、グレイウェアをブロックするか、グレイウェアでアラートを続行するかを決定します。
  - マルウェア：マルウェアをホストすることが知られているサイト、またはコマンド アンド コントロール (C2) トラフィックに使用され、エクスプロイト キットが存在する可能性があるサイト。
  - **phishing** [フィッシング]–認証ページを偽装、あるいはフィッシングにより個人のID情報を盗むことが分かっている。
  - 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、標的型攻撃を実行したりするサイト。

- 悪意のある可能性のある URL カテゴリ:
  - **dynamic-dns** [動的DNS]–動的にIPアドレスが割り当てられ、しばしばマルウェアのペイロードやC2トラフィックを送るシステムのホストおよびドメイン名。また、動的DNSドメインは、信頼できるドメイン登録業者が登録したドメインとは違う検査プロセスを経ているため、信頼度が低くなります。
  - 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または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。
  - **newly-registered-domain (**新規登録ドメイン**)**–新規登録ドメインは、故意またはドメイン生成アルゴリズムによって生成されることが多く、悪意のある活動に使用されます。
  - **not-resolved**- 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** [パークド]–個人によって登録されたドメインであり、後に認証情報を盗むフィッシングに使用されていることが分かることがあります。フィッシングにより認証情報や個人のID情報を盗むために用意されたこれらのドメインは、正当なドメインに似通っている場合があります（例：pal0alto0netw0rks.com）。あるいはpanw.netなど、いつか価値が出ると期待させて不当な個人購入を行わせるドメインもあります。
  - **proxy-avoidance-and-anonymizers (**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。
  - **unknown (**未知**)**–PAN-DB によってまだ識別されていないサイトです。可用性がビジネスにとって重要であり、トラフィックを許可し、未知のサイトに警告し、トラフィックにベストプラクティスセキュリティプロファイルを適用し、アラートを調査する必要がある場合。

    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を行うため、未知の *URL* は迅速に識別され、ファイアウォールが実際の *URL* カテゴリに基づいて処理できる既知の *URL* となります。

- 潜在的な責任リスクのある URL カテゴリ:
  - 乱用薬物–合法および違法の薬物の乱用、薬物関連器具の販売と使用、薬物の製造または販売を促進する Web サイト。
  - アダルト– 職場にはふさわしくない可能性のある Web サイト。
  - **copyright-infringement (**著作権侵害**)**–ソフトウェアまたはその他の知的財産の違法ダウンロードを許可するコンテンツなど、違法なコンテンツがあるドメインであり、潜在的な責任のリスクをもたらします。教育業界で求められる児童保護法や、ユーザーがサービスを介して著作権で保護されたコンテンツを共有することをインターネットプロバイダーが防止しなければならない国の法律に準拠するために、このカテゴリーが導入されました。
  - **extremism (**過激な思想**)**–テロ、人種差別、ファシズムや、民族的な出自や宗教、その他の考え方が異なる人や集団を差別するその他の過激な思想を喧伝するウェブサイト。このカテゴリーは、教育業界で求められる児童保護法に準拠するために導入されました。地域によっては、法規制により過激派サイトへのアクセスが禁止されている場合があり、アクセスを許可すると責任を問われる可能性があります。
  - ギャンブル–リアルマネーおよび/またはバーチャルマネーの交換を容易にする宝くじまたはギャンブルのウェブサイト。また、ギャンブルに関するチュートリアル、アドバイス、または賭けのオッズやプールなどのその他の情報を提供する Web サイト。
  - ピアツーピア ：主に bitTorrent ダウンロード機能から保護するために、クライアントがトレント、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 アプリケーションをピアツーピアで共有するため、またはそれらにアクセスする Web サイト。シェアウェアまたはフリーウェアのサイトは含まれません。
  - 疑わしい- 個人またはグループの特定の層をターゲットにした不快なコンテンツ、犯罪行為、違法行為、一攫千金スキームを含む可能性のある Web サイト。
  - 武器- 職場では不適切である可能性のある武器およびその使用方法に関する販売、レビュー、説明、または指示を提供する Web サイト。

デフォルトの*URL*フィルタリング プロファイルは、マルウェア、フィッシング、コマンド アンド コントロールの*URL*カテゴリをブロックしますが、ブロックすることを推奨される他のカテゴリをブロックしてはいません。デフォルトの *URL* フィルタリングプロファイルは、薬物乱用、アダルト、ギャンブル、疑わしい、そして武器の *URL* カテゴリもブロックします。これらの *URL* カテゴリをブロックするかどうかは、ビジネス要件によって異なります。たとえば、可用性が重要であるため、大学が学生に対しこれらほとんどのサイトへアクセスを制限することはしないでしょうが、セキュリティを最重要視する企業では、すべてをブロックするかもしれません。

URLフィルタリングの例

URLフィルタリングは、ファイル ブロッキング、複号化、外部ダイナミックリスト (EDL)、ロギング等のセキュリティ機能と連携し、URLカテゴリを単にブロックしたり許可したりすることを超えた粒度の高い ポリシーを生成します。URL Filtering safe transition steps（URLフィルタリング安全移行ステップ）を使ってどのサイトを許可しどのサイトをブロックしたいかを検討し、その後、業務要求に見合うポリシーを実現します。以下に例を示します。

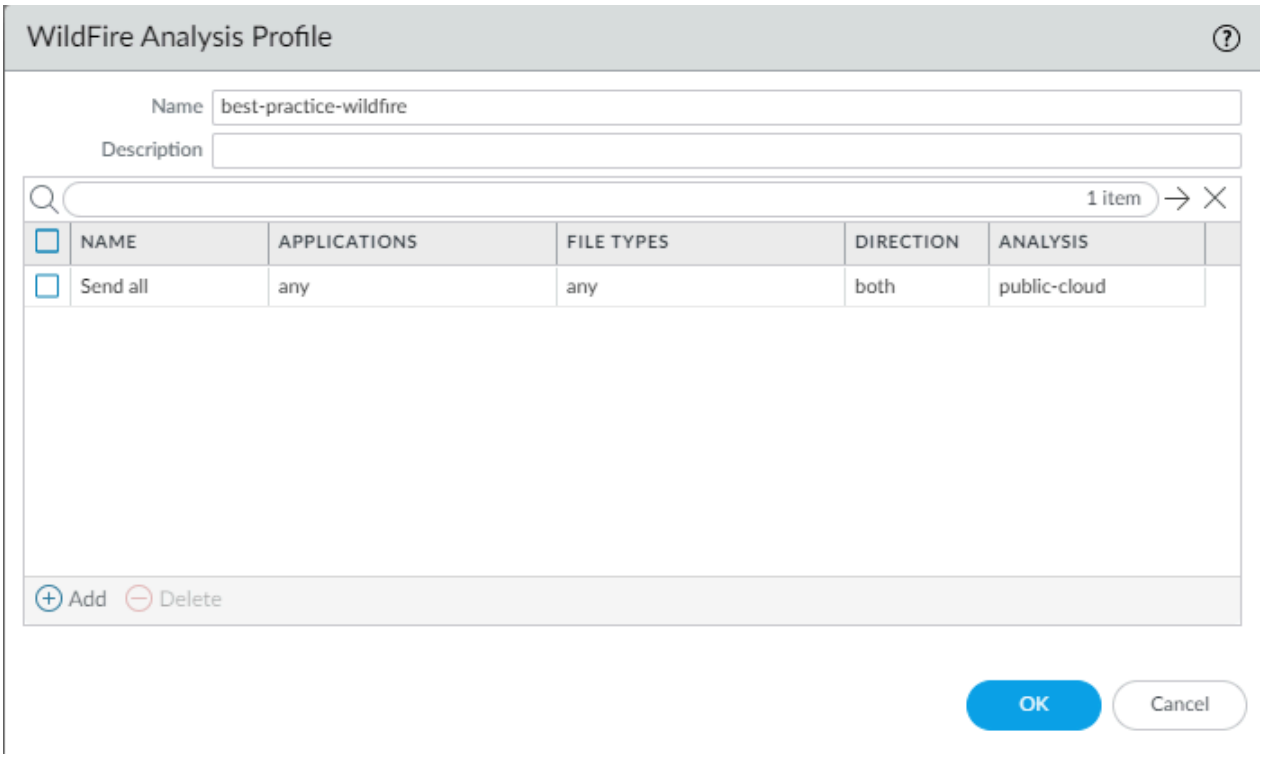
- リスクベースの URL カテゴリ (高リスク、中リスク、および低リスク) を他の URL カテゴリと組み合わせて使用し、復号化をターゲットにしたりトラフィックのブロックをターゲットにします。例えば以下のことが可能です：
  - 金融サービス カテゴリの高リスク Web サイトへのトラフィックをブロックします。
  - 高リスクおよび中リスクの Web トラフィックをすべて復号化します。
  - ファイアウォールに、復号化するすべてのトラフィックを復号化するための十分なリソースがない場合は、特定の URL カテゴリへの高リスクおよび中リスクのトラフィックを復号化します。
- 可視性を高めるために、高リスクや中リスクのカテゴリドメインについて、すべてのユーザーエージェントおよびリファラー、すべてのURL、および すべてのファイル ダウンロードをログに記録します。
- .exe、.scr その他潜在的に悪意あるファイルのような危険性をはらむコンテンツのダウンロードを防止すべくファイル ブロッキング プロファイルをトラフィックに適用しながら、personal-sites-and-blogs のような カテゴリへのアクセスを許可します。
- 特に高リスクまたは中リスクの金融サイトへのアクセスを許可している場合は、定義済みの **Palo Alto Networks - Bulletproof IP addresses** EDL を使用して、防弾 ISP でホストされているサイトへのアクセスを防止します。
- ポリシーを簡単化するには、複数のURLカテゴリを組合せます。

インターネット ゲートウェイの WildFire 分析プロファイルのベストプラクティス

ファイルを WildFire に転送して分析し、未知の脅威からネットワークを保護します。この保護がなければ、攻撃者がネットワークに侵入し、ユーザーが日常的に使用するアプリケーションの脆弱性を狙ったエクスプロイトを行えるようになってしまいます。WildFireは未知の脅威を防止するため、APT（advanced persistent threat）に対する保護が最大限に高まります。

リアルタイムに自動的にダウンロードおよびインストールを行うようWildFire アプライアンスのコンテンツ更新をセットアップし、常に最新のサポートを得られるようにします。

最良のWildFire分析により、分析のためにすべてのファイルが双方向（アップロードおよびダウンロード）で WildFire に送られます。具体的には、PEファイル（ファイル ブロッキングの推奨事項に従ってブロックしていない場合）、Adobe FlashおよびReaderファイル（PDF、SWF）、Microsoft Officeファイル（PowerPoint、Excel、Word、RTF）、Javaファイル（Java、.CLASS）、Androidファイル（.APK）を必ずすべて送信するようにしてください。



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

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

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

インターネット ゲートウェイのセキュリティポリシーの初回定義

インターネット ゲートウェイのセキュリティ ポリシーの推奨設定の目的は、許可されたアプリケーションを確実に安全に使用できるようにすることです。ただし、ネットワーク上で実行されている正確なアプリケーション、ビジネスにとって重要なアプリケーション、および各アプリケーションに誰がアクセスする必要があるかを特定するには時間がかかります。アプリケーション許可ルールに基づいてセキュリティ ポリシーを作成するには、ユーザーに対して公式に認可したアプリケーションと、一般的なビジネス アプリケーションおよび個人用アプリケーション (ビジネスに適している場合) を寛大に許可するルールベースから始めます。

初期ポリシーには、既知の悪意のある IPアドレスとアプリケーションを明示的にブロックするルールと、ポリシーを改良し、ベスト プラクティス ポリシーへの移行中にアプリケーションの可用性を維持するのに役立つ一時的な許可ルールが含まれています。

テンプレートおよびテンプレート スタックを再利用し、同じポリシーがすべての場所のあらゆるインターネット ゲートウェイのファイアウォールに適用されるようにすることで、複数の場所全体にかけて一貫した形でセキュリティ ポリシーを適用できます。テンプレートは、グローバル セキュリティポリシーを維持し、管理しなければならないテンプレートおよびテンプレート スタックの数を減らしつつ、*IP*アドレス、*FQDN* などのデバイス固有の値を適用するために変数を使用します。

次のトピックでは、初期ルールベースの作成方法、各ルールが必要な理由を説明し、ベスト プラクティスの推奨事項を無視するリスクを明らかにします。

- ステップ1:信頼できる脅威インテリジェンスのソースに基づいてルールを作成
- ステップ 2:アプリケーション許可ルールの作成
- ステップ3:アプリケーション ブロック ルールの作成
- ステップ4:一時的調整ルールの作成
- ステップ 5:どのルールにもマッチしないトラフィックのロギングを有効化

ステップ1:信頼できる脅威インテリジェンスのソースに基づいてルールを作成

Palo Alto Networks および信頼できるサードパーティのソースが悪意があると証明したホストからのトラフィックをブロックします。Advanced Threat Prevention (高度な脅威防御) ライセンス（またはアクティブなレガシーThreat Prevention (脅威防御) ライセンス）には、既知の悪意のあるIPアドレスを含む組み込み外部動的リスト（EDL）が含まれています。ポリシーでEDLを使用して悪意のあるトラフィックをブロックします。Palo Alto Networks は、最新の脅威インテリジェンスに基づいてリストをコンパイルし、動的に更新します。ファイアウォールは、再起動することなくダイナミック更新を受信して実装します。

STEP 1 | Palo Alto Networks が悪意を確認した IPアドレスを出入りするトラフィックをブロックします。

これらのルールが必要な理由	ルールのハイライト
❑ ほぼ独占的にマルウェアの配信、コマンド アンド コントロール活動、攻撃を行うために使用されていることを Palo Alto Networks が確認した IP アドレスから、このルールによって保護されます。	• ルールの一つは悪意のある既知の IPアドレスへのアウトバウンド トラフィックをブロックし、もう一つのルールはそれらのアドレスへのインバウンドトラフィックをブロックします。 • 外部動的リスト **Palo Alto Networks - Known malicious IP addresses**（**Palo Alto Networks -** 悪意のある既知の **IP** アドレス）を、アウトバウンド トラフィック ルール用の宛先アドレス、インバウンドトラフィック ルール用の送信元アドレスとして設定します。 • これらのルールに一致するトラフィックを拒否します。 • これらのルールにマッチしたトラフィックのログ機能を有効化し、ネットワーク上の潜在的な脅威を調査できるようにします。 • これらのルールは悪意のあるトラフィックを阻止するため、任意のポートで実行されている任意のユーザーからトラフィックを保護します。

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Drop Outbound Malicious IP	universal	any	any	any	any	any	Palo Alto Networks - Known malicio...	any	any	any	Deny	none	
Drop Inbound Malicious IP	universal	any	Palo Alto Networks - Known malic...	any	any	any	any	any	any	any	Deny	none	

STEP 2 | Bulletproof ホスティングプロバイダからのトラフィックの送受信をブロックします。

これらのルールが必要な理由	ルールのハイライト
❑ このルールは、PaloAlto ネットワークが Bulletproof ホスティングプロバイダに属していることを示した IP アドレスからあなたを保護します。 Bulletproof ホスティングプロバイダはコンテンツに対する制約が全くないか、限定されており、イベントログもありません。Bulletproof サイトは、コマンドアンドコントロール (C2) 攻撃や非合法活動を	• ルールの一つはBulletproof ホストの既知の IP アドレスへのアウトバウンド トラフィックをブロックし、もう一つのルールはそれらのアドレスへのインバウンドトラフィックをブロックします。 • 外部動的リスト **Palo Alto Networks - Bulletproof addresses (Palo Alto Networks - Bulletproof IP** アドレス) を、アウトバウンド トラフィック ルール用の宛先アドレ

これらのルールが必要な理由	ルールのハイライト
発動するのに最適な場所となります。なぜなら、何でもできて、追跡されることがないからです。	ス、インバウンドトラフィック ルール用の送信元アドレスとして設定します。 • これらのルールに一致するトラフィックを拒否します。 • これらのルールにマッチしたトラフィックのログ機能を有効化し、ネットワーク上の潜在的な脅威を調査できるようにします。 • これらのルールは悪意のあるトラフィックを阻止するため、任意のポートで実行されている任意のユーザーからトラフィックを保護します。

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Drop Outbound Bulletproof IP	universal	any	any	any	any	any	Palo Alto Networks - Bulletproof IP ...	any	any	any	Deny	none	
Drop Inbound Bulletproof IP	universal	any	Palo Alto Networks - Bulletproof I...	any	any	any	any	any	any	any	Deny	none	

STEP 3 | 信頼できる脅威アドバイザリーから得られる高リスク IPアドレスを出入りするトラフィックをブロックしログに記録します。

これらのルールが必要な理由	ルールのハイライト
Palo Alto Networks は高リスク IPアドレス フィードに含まれる IP アドレスの悪意を直接確認したわけではありませんが、脅威アドバイザリーはこれらを悪意のある挙動と紐付けています。 ❑ この例のようにトラフィックをブロックしてログに記録します。 ❑ ビジネス上の理由で高リスクのIPアドレスを許可する必要がある場合は、そのIPアドレスのみを許可する厳格なセキュリティプロファイルを持つセキュリティ ポリシー ルールを作成し、ルールベースの高リスクIPアドレスブロックルールの前に配置します。許可するように選択した高リスクIPアドレスを詳細に監視し、ログに記録します。	• ログの一つは高リスク IPアドレスへのアウトバウンド トラフィックをブロックし、もう一つのログはそれらのアドレスへのインバウンドトラフィックをブロックします。 • 外部動的リスト **Palo Alto Networks - High risk IP addresses**（**Palo Alto Networks - 高リスク IPアドレス**）を、アウトバウンド トラフィック ルール用の宛先アドレス、インバウンドトラフィック ルール用の送信元アドレスとして設定します。 • トラフィックを許可する場合は、ベストプラクティスのセキュリティ プロファイルを適用します。 • これらの規則は悪意のあるトラフィックを阻止するため、任意のポートで実行されている任意のユーザ、任意のアプリケーショ

これらのルールが必要な理由	ルールのハイライト
	ンから任意のアプリケーションのためにトラフィックを保護します。

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block Outbound High Risk IPs	universal	any	any	any	any	any	Palo Alto Networks - High risk IP addresses	any	any	any	Deny	none	
Block Inbound High Risk IPs	universal	any	Palo Alto Networks - Known malicious IP addresses	any	any	any	any	any	any	any	Deny	none	

STEP 4 | 同様に、「**Palo Alto Networks - Tor exit IP addresses** external dynamic list」を使用して、Tor出口ノードを出入りするトラフィックをブロックし、ログに記録する2つのルールを作成します。これらのトラフィックは、特にエンタープライズ環境で、悪意のあるアクティビティとよく関連付けられます（常にそうとは限りません）。

ステップ 2:アプリケーション許可ルールの作成

アプリケーション許可ルールを作成する前に、アプリケーション許可リストを特定 します。ポートではなくアプリケーションに基づいて許可ルールを作成します。ファイアウォールがユーザーを識別する前にユーザー アクセスを必要とする特定のインフラストラクチャ アプリケーションを除き、既知のユーザーにのみアクセスを許可します。許可されたアプリケーションにアクセスするためのユーザー グループを作成し 、ビジネス上各アプリケーションにアクセスする必要がある特定のユーザーまたはユーザー グループのみにユーザー アクセスを制限します。

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か、ポートベースのファイアウォールから移行するには、Policy Optimizerを活用する 「アプリケーションベースのポリシーへの移行のベストプラクティス」のアドバイスに従ってください。*Policy Optimizer* は、ポートベースのルールを分析し、それらのルールに一致する正確なアプリケーションを表示するのに役立ちます。また、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 (オーバープロビジョニングされたルール)、および既存のポートベースのルールを見つけるのにも役立ちます。

セキュリティ ポリシー ルールベースの一般ルールの上に特定のルールを配置します。そうしないと、一般ルールが特定のルールに影を落とす可能性があります。(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により、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が一般的なルールに一致するようにすることです。)

ルールベースの部分には、次のようなアプリケーション許可リストに含めることにしたアプリケーション用の許可ルールが含まれます。

- ビジネスやインフラストラクチャのために提供・管理する制限付きのアプリケーション
- 一般的なビジネス アプリケーション ユーザーは、仕事を完了する必要がある場合があります。
- 個人使用を許可することを選択した許容アプリケーション。

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

ベストプラクティス セキュリティ プロファイルを添付して、許可されているすべてのトラフィックをスキャンして既知および未知の脅威を検出します。これらのプロファイルをまだ作成していない場合は、インターネット ゲートウェイの最良のセキュリティ プロファイルを作成を参照してください。目に見えないものは検査できないため、 完全な可視性と脅威の検査のためにトラフィックを復号化するようにファイアウォールを構成します。

STEP 1 | 企業DNSサーバーへのアクセスを許可します。

認可された *DNS* サーバーへのトラフィックのみを許可します。DNS セキュリティ サービス を使用して、悪意のある *DNS* サーバーへの接続を防ぎます。

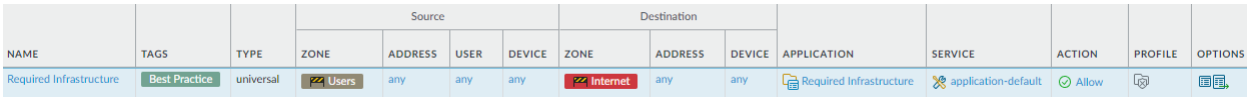
このルールが必要な理由	ルールのハイライト
❑ DNS へのアクセスはネットワーク インフラストラクチャ サービスを提供し、通常は攻撃者によって悪用されます。 ❑ 内部DNSサーバー上にのみアクセスを許可することで、攻撃の入り口を減らせます。	• これは非常に具体的なルールであるため、ルールベースのトップ近くに配置します。 • 宛先アドレス用に使用するアドレス オブジェクトを作成し、必ずデータセンター内のDNSサーバーにのみユーザーがアクセスするようにします。 • ユーザーはログインする前にこれらのサービスにアクセスする必要があるため、すべてのユーザーにアクセスを許可します。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT DNS Services	Best Practice	universal	Users	any	any	any	IT Infrastructure	DNS Servers	any	dns	application-default	Allow		

STEP 2 | 他の必要なITインフラのリソースへのアクセスを許可します。

このルールが必要な理由	ルールのハイライト
❑ NTP、OCSP、STUN、およびpingといったネットワーク インフラストラクチャおよび管理機能を提供するアプリケーションを有効化します。 ❑ 前述のルールは、許可される DNS トラフィックをデータ センター内の宛先アドレスに制限します。これらのアプリケーションはデータセンターに存在しない可能性があるため、別のルールが必要です。	• これらのアプリケーションはデフォルトのポートで実行されるため、任意のユーザーにアクセスが許可され (これらのサービスが必要なときにユーザーがまだログインしておらず、認識されていない可能性があります)、宛先アドレスが 任意であるため、それらを 1 つのアプリケーション グループに追加して、1 つのアプリケーション グ

このルールが必要な理由	ルールのハイライト
	ループを作成します。すべてへのアクセスを有効にするルール。



NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Required Infrastructure	Best Practice	universal	Users	any	any	any	Internet	any	any	Required Infrastructure	application-default	Allow		

STEP 3 | IT制限付きSaaSアプリケーションへのアクセスを許可します。

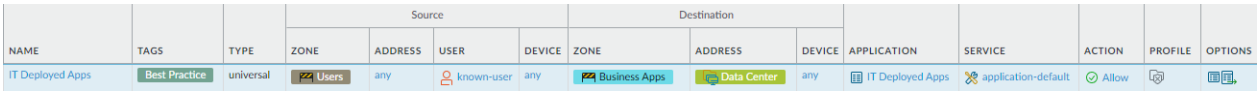
このルールが必要な理由	ルールのハイライト
❑ SaaS アプリケーションでは、独自のデータがクラウドに存在します。このルールにより、既知のユーザーだけがこれらのアプリケーション（さらにその中のデータ）にアクセスできるようになります。 ❑ 許可されたSaaSトラフィック内の脅威をスキャンします。	• アプリケーション グループを作成し、すべての許可された SaaS アプリケーションを制御します。 • SaaS アプリケーションは常にアプリケーションのデフォルト ポートで実行する必要があります。 • アクセスを既知のユーザーに制限します。「許可したアプリケーションにアクセスするためのユーザーグループの作成」を参照してください。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT Sanctioned SaaS Apps	Best Practice	universal	Users	any	known-user	any	Internet	any	any	IT Sanctioned SaaS Applica...	application-default	Allow		

STEP 4 | ITが整った業務用アプリケーションへのアクセスを許可します。

このルールが必要な理由	ルールのハイライト
❑ 攻撃は、抽出段階で FTP などのビジネス クリティカルなデータセンター アプリケーションを使用したり、横方向に移動するためにアプリケーションの脆弱性を悪用したりすることがよくあります。 ❑ 多くのデータセンター アプリケーションは複数のポートを使用します。サービスをアプリケーションのデフォルトに設定すると、 アプリケーションが標準ポートで安全に有効になります。非標準ポートでのアプリケーションを許可しないでください。	• アプリケーション グループを作成し、すべてのデータセンター アプリケーションをグループ化します。 • データセンター サーバーのアドレス用のアドレスグループを作成します。 • アクセスを既知のユーザーに制限します。「許可したアプリケーションにアクセスするためのユーザーグループの作成」を参照してください。

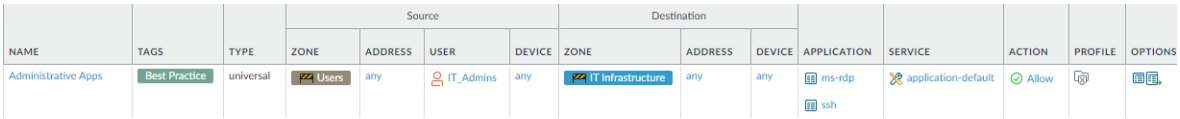
このルールが必要な理由	ルールのハイライト
これは回避動作に関連することがよくあります。	



NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT Deployed Apps	Best Practice	universal	Users	any	known-user	any	Business Apps	Data Center	any	IT Deployed Apps	application-default	Allow		

STEP 5 | 管理ユーザーに必要なアプリケーションへのアクセスを許可します。

このルールが必要な理由	ルールのハイライト
❑ 攻撃の入り口を減らすために、許可したアプリケーションにアクセスするためのユーザーグループを作成します。 ❑ 管理者は多くの場合、機密アカウント データへのアクセスや他のシステム (RDP など) へのリモート アクセスを必要とするため、アタックサーフェスを減らすために、ビジネス ニーズがある管理者のみにアクセスを許可します。	• このルールはIT_adminsグループのユーザーにだけアクセスを許可します。 • 各内部アプリケーションや非標準ポート上で実行されるアプリケーション用のカスタム アプリケーションを作成し、ネットワーク上で他のポートを開けるのではなく、必ずデフォルトのポート上で実行されるようにします。 • 異なるアプリケーションごとに別のユーザーグループが存在する場合は、細かな管理を行えるように個別のルールを作成します。

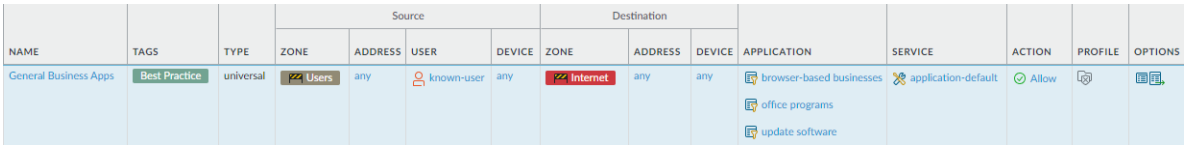


NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Administrative Apps	Best Practice	universal	Users	any	IT_Admins	any	IT Infrastructure	any	any	ms-rdp ssh	application-default	Allow		

STEP 6 | 一般的な業務用アプリケーションへのアクセスを有効にします。

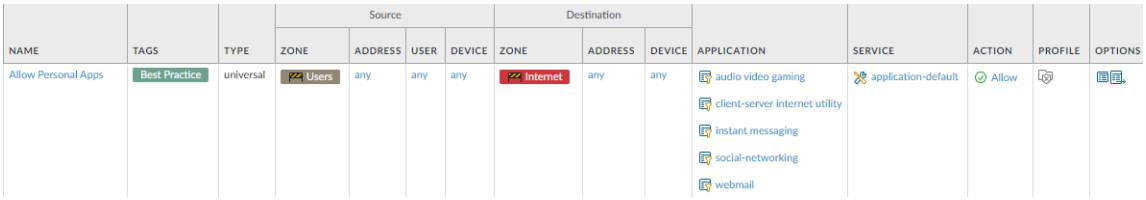
このルールが必要な理由	ルールのハイライト
❑ 多くの場合、ユーザーは、ユーザーに認可および管理するアプリケーションに加えて、Zoom、Adobe オンライン サービス、G Suite などの他のビジネス アプリケーションにアクセスする必要があります。 ❑ このルールにより、脅威のスキャン中にWebブラウジングを安全に許可できます。インターネット ゲートウェイの最良のセキュリティ プロファイルを作成を参照してください。	• アクセスを既知のユーザーのみに制限します。「許可したアプリケーションにアクセスするためのユーザーグループの作成」を参照してください。 • 可視性を保つため、許可する各タイプのアプリケーションごとにアプリケーション フィルターを作成します。 • すべてのトラフィックにおける既知および未知の脅威を防ぐための ベスト プラク

このルールが必要な理由	ルールのハイライト
	ティス セキュリティ プロファイル を添付します。



STEP 7 | （任意）個人アプリケーションへのアクセスを許可します。

このルールが必要な理由	ルールのハイライト
❑ 仕事用デバイスと個人用デバイスの境界線が曖昧になる中、ユーザーがアクセスするすべてのアプリケーションが安全に有効化され、脅威から解放されます。 ❑ この初期ルールベースを作成するときに、アプリケーション フィルターを使用して、個人用アプリケーションへのアクセスを安全に有効にします。使用中のアプリケーションを評価した後、その情報を使用して、フィルターを削除し、許容される使用ポリシーに適した個人用アプリケーションのより小さなサブセットを許可するかどうかを決定します。	• アクセスを既知のユーザーのみに制限します。「許可したアプリケーションにアクセスするためのユーザーグループの作成」を参照してください。 • 可視性を保つため、許可する各タイプのアプリケーションごとにアプリケーションフィルターを作成します。 • すべてのトラフィックにおける既知および未知の脅威を防ぐための ベスト プラクティス セキュリティ プロファイル を添付します。



STEP 8 | ウェブ ブラウジング全般を許可します。

このルールが必要な理由	ルールのハイライト
❑ 以前のルールでは、個人アプリケーション(その多くはブラウザベース) へのアクセスが許可されていました。このルールにより、一般的な Webブラウジングが許可されます。 ❑ ウェブ ブラウジングは一般的に、他の種類のアプリケーション トラフィックより	• 他のルールと同じベスト プラクティス セキュリティ プロファイルを使用し、URL フィルタリング プロファイルを可能な限り強化します。 • マルウェアが組み込まれたデバイスや組み込みデバイスがインターネットにアクセス

このルールが必要な理由	ルールのハイライト
もリスクが高くなります。Webブラウジングを安全に有効にするために、ベスト プラクティス セキュリティ プロファイル を作成し、このルールに添付します。 ❑ 脅威が暗号化されたトラフィックに隠されていることがあるため、Webブラウジングを安全に有効化するために完全な可視性および脅威検査のためにトラフィックを復号化します。	するのを防ぐには、既知のユーザーのみを許可します。 • アプリケーション フィルターを使用して一般的なアプリケーションへのアクセスを許可します。 • アプリケーションとして SSL を明示的に許可し、復号化から除外するように選択した HTTPS サイトをユーザーが参照できるようにします。 • サービスを **application-default**に設定します。

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
General Web Browsing	Best Practice	universal	Users	any	known-user	any	Internet	any	any	general browsing ssl yahoo-web-analytics	application-default	Allow		

ステップ3:アプリケーション ブロック ルールの作成

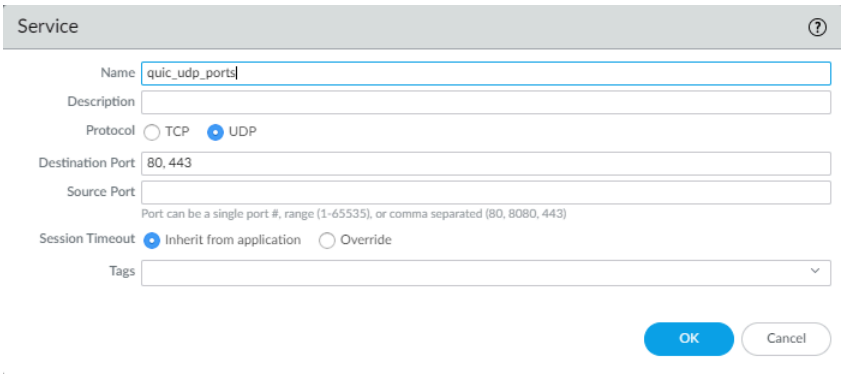
アプリケーション ブロック ルールは、セキュリティ ポリシー ルールベースを開発および調整する際に、回避的で一般的に悪用されるアプリケーションからユーザーを保護します。一時的な調整ルールは、 ポリシーのギャップを見つけて、潜在的な攻撃を特定するのに役立ちます。ネットワーク上で実行されていることを知らなかったアプリケーション トラフィックを捕捉するため、セキュリティ リスクを引き起こす可能性のあるトラフィックが許可されます。次のブロック ルールは、パブリック DNS や SMTP、暗号化されたトンネル、リモート アクセス、認可されていないファイル共有アプリケーションなど、攻撃者が一般的に使用する潜在的に悪意のあるアプリケーションとプロトコルを明示的にブロックします。

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

このルールが必要な理由	ルールのハイライト
❑ Chrome および他の一部のブラウザは、TLS の代わりに QUIC を使用してセッションを確立します。QUIC はファイアウォールが復号できない独自の暗号化を使用するため、潜在的に危険な暗号化トラフィックがネットワークに侵入する可能性があります。 ❑ QUIC をブロックするとブラウザが TLS にフォールバックするため、ファイアウォー	• UDP ポート 80 と 443 を指定するサービス (**Objects > Services**) を作成します。 • 最初のルールは、UDPサービスポート（80と443）のQUICをブロックし、作成したサービスを使用してそれらのポートを指定します。 • 2 番目のルールは、QUIC アプリケーションをブロックします。

このルールが必要な理由	ルールのハイライト
ルがトラフィックを復号化できるようになります。	

このサービスは、QUIC に対してブロックする UDP ポートを指定します。



最初のルールは QUIC 用に構成したサービスを指定し、2 番目のルールは QUIC アプリケーションをブロックします。

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

STEP 2 | 正当に使用する場面がないアプリケーションをブロックします。

このルールが必要な理由	ルールのハイライト
❑ IT 部門が承認していない暗号化トンネル、ピアツーピア ファイル共有、Webベースのファイル共有アプリケーションなど、悪意のある可能性のあるアプリケーションをブロックします。 ❑ 一時的な調整ルール では、予想どおりポリシー ルールに一致しない正規のトラフィックだけでなく、悪意のあるトラフィックも許可される可能性があるため、危険なトラフィックや悪意のあるトラフィックが許可される可能性があります。このルールは、正当な使用例がなく、攻撃	• **Drop**（ドロップ）アクションを使用し、クライアントあるいはサーバーに信号を送ることなく密かにトラフィックをドロップします。 • このルールに一致するトラフィックのロギングを有効にして、ネットワーク上の潜在的な脅威やアプリケーションの悪用を調査できるようにします。 • このルールは悪意のあるトラフィックを捉えるようにできているため、すべてのユーザーが発生させたあらゆるポート上のトラフィックにマッチします。

このルールが必要な理由	ルールのハイライト
者または不注意なユーザーが使用する可能性のあるトラフィックをブロックします。	

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block Bad Apps	Best Practice	universal	Users	any	any	any	Internet	any	any	encrypted tunnels file sharing remote access	any	Drop	none	

STEP 3 | 公開DNSおよびSMTPアプリケーションをブロックします。

認可された *DNS* サーバーへのトラフィックのみを許可します。DNS セキュリティ サービス を使用して、悪意のある *DNS* サーバーへの接続を防ぎます。

このルールが必要な理由	ルールのハイライト
❑ 公開DNS/SMTPアプリケーションをブロックし、DNSトンネル、コマンド アンド コントロール トラフィック、リモート管理アプリケーションを行えなくします。	• **Reset both client and server**（クライアントおよびサーバーを両方リセット）するアクションを利用し、クライアント側とサーバー側の両方のデバイスに TCP リセット メッセージを送信します。 • 潜在的な脅威を調査できるように、このルールに一致するトラフィックのログを有効にします。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block Public DNS and SMTP	Best Practice	universal	Users	any	any	any	Internet	any	any	dns smtp	any	Reset Both	none	

ステップ4:一時的調整ルールの作成

一時的なチューニング ルールは、初期のベストプラクティス ルールベースのギャップを監視し、警戒すべき動作を警告するのに役立ちます。

たとえば、一時ルールは、未知のユーザーからのトラフィックや、予期しないポートで実行されているアプリケーションからのトラフィックを識別します。一時的なルールに一致するトラフィックを監視して、ネットワーク上で使用されているすべてのアプリケーションを完全に理解します (そして、ベストプラクティスのルールベースに移行する際にアプリケーションの可用性を確保します)。この情報を使用して、必要と認識していなかったアプリケーションに新しい許可ルールを追加したり、許可ルールを絞り込んでアプリケーション フィルターをアプリケーション グループまたは特定のアプリケーションに置き換えたりすることで、許可リストを微調整することができます。トラフィックがもうこのルールにヒットしなくなった時点で、一時ルールの削除を行えます。

一時的なチューニング ルールの中には、不正なアプリケーションをブロックするルールよりも優先されるものと、不正なトラフィックがネットワークに侵入しないようにしながら、対象のトラフィックが適切なルールに一致することを確認するために適用されるものがあります。

STEP 1 | 既知のユーザーに対して標準的でないポート上におけるウェブ ブラウジングおよびSSLを許可し、標準的でないポート上で実行されている正当なアプリケーションがあるかどうか確認します。

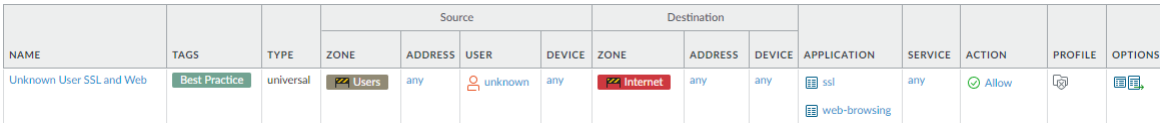
このルールが必要な理由	ルールのハイライト
❑ このルールは、正規のアプリケーションが非標準ポートで実行されるためにユーザーがアクセスできないというポリシーのギャップがあるかどうかを判断するのに役立ちます。 ❑ このルールに一致するすべてのトラフィックを監視します。正当なトラフィックの場合は、適切なアプリケーションを適切な許可ルールに追加します。必要に応じてカスタム アプリケーションを作成 します。	• デフォルト ポートでのみアプリケーションを許可する許可ルールとは異なり、このルールでは、任意のポートでの Webブラウジングと SSL トラフィックが許可リスト内のギャップを見つけることができます。 • このルールはポリシーのギャップを検出するため、ネットワーク上の既知のユーザーに限定してください。 • ユーザーが復号化されていない HTTPS サイト (金融サービスやヘルスケア サイトなど) を閲覧できるようにする場合は、このルールでアプリケーションとして SSL を明示的に許可します。 • 脅威をスキャンするためのベストプラクティス セキュリティ プロファイルを添付します。 • このルールをアプリケーション ブロック ルールの上に追加しないと、このルールに一致するトラフィックが存在しません。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected Port SSL and Web	Best Practice	universal	Users	any	known-user	any	Internet	any	any	ssl web-browsing	any	Allow		

STEP 2 | 標準的でないポート上の未知のユーザーからのウェブ ブラウジング トラフィックおよびSSLトラフィックを許可し、ポートに関係なくすべての未知のユーザーがよく分かるようにします。

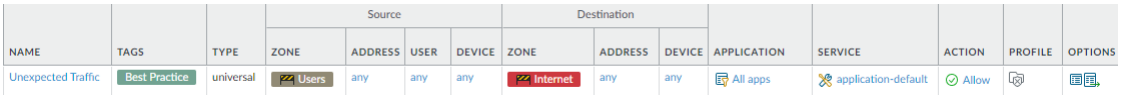
このルールが必要な理由	ルールのハイライト
❑ User-IDの範囲にギャップがないか確認する際にこのルールが役立ちます。	• 大抵のアプリケーション許可ルールが既知のユーザーあるいは特定のユーザーグループに適用されますが、このルールは未知の

このルールが必要な理由	ルールのハイライト
❑ このルールは、インターネットにアクセスしようとする侵害されたデバイスや埋め込まれたデバイスを特定するのに役立ちます。 ❑ これは回避手法であるため、Webブラウジング トラフィックであっても、標準以外のポートの使用をブロックすることが重要です。	ユーザーからのトラフィックに明示的にマッチします。 • このルールをアプリケーション ブロック ルールより上に配置しなければトラフィックが一切これにヒットしなくなります。 • 脅威をスキャンするためのベストプラクティス セキュリティ プロファイルを添付します。



STEP 3 | アプリケーションをそのデフォルトのポートですべて許可し、予期しないアプリケーションを特定します。

このルールが必要な理由	ルールのハイライト
❑ このルールによりネットワーク上で実行されていることを知らなかったアプリケーションに対する可視性を得られるため、アプリケーション許可リストを微調整できるようになります。 ❑ このルールにマッチするすべてのトラフィックを監視し、それが潜在的な脅威を示すかどうかや、その他のアプリケーションへのアクセスを有効にする許可ルールを修正する必要があるかどうかを判断します。	• すべてのアプリケーションを許可するこのルールをアプリケーション ブロック ルールの後に配置し、好ましくないアプリケーションがネットワーク上で実行されないようにする必要があります。 • PAN-OS 7.0.x 以降を実行している場合は、予期せぬアプリケーションを正しく特定するために、ルールが**any**（すべて）のアプリケーションを許可するよう設定する代わりに、すべてのアプリケーションを含んだアプリケーション フィルターを作成する必要があります。



STEP 4 | 任意のポート上の任意のアプリケーションが、非標準ポートで実行されているアプリケーションを識別できるようにします。

このルールが必要な理由	ルールのハイライト
❑ このルールは、未知のポートで実行されている正規の既知のアプリケーションを識別するのに役立ちます。	• これは、任意のポート上の任意のユーザーの任意のアプリケーションを許可する非常

このルールが必要な理由	ルールのハイライト
❑ またこのルールは、カスタム アプリケーションを作成してアプリケーション許可ルールに追加すべき未知のアプリケーションを特定する際にも役立ちます。 ❑ このルールに一致するトラフィックはアクション可能です。トラフィックの送信元を追跡し、不明な tcp、udp、または非 syn-tcp トラフィックを許可しないようにしてください。	に一般的なルールであるため、ルールベースの一番下に配置します。 • このルールに一致するトラフィックのログを有効にすると、アプリケーションの悪用や潜在的な脅威を調査したり、カスタム アプリケーションを必要とする正当なアプリケーションを特定したりできます。

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Unexpected Port Usage	Best Practice	universal	Users	any	any	any	Internet	any	any	any	any	Allow		

ステップ 5:どのルールにもマッチしないトラフィックのロギングを有効化

定義したルールに一致しないインターネット ゲートウェイ トラフィックは、ルールベースの下部にある事前定義されたインターゾーン間デフォルトルールと一致し、拒否されます。作成したルールに一致しないトラフィックを可視化するには、インターゾーン間デフォルトルールのロギングを有効にします。

STEP 1 | ルールベースでインターゾーン間デフォルトルールの行を選択し、ルールを 上書き して編集します。

STEP 2 | **interzone-default**（インターゾーン デフォルト）ルールの名前を選択し、編集できるようにそのルールを開きます。

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

STEP 4 | ルールに一致するトラフィックをモニタするカスタム レポートを作成します。

1. **Monitor (モニター) > Manage Custom Reports (**カスタム レポートの管理**)**の順に選択します。
2. レポートを **Add**（追加）して分かりやすい **Name**（名前）を付けます。
3. **Database**（データベース）を**Traffic Summary**（トラフィックサマリー）に設定します。
4. **[**スケジュール設定**]** チェック ボックスをオンにします。
5. **[Rule (**ルール**)]** 、**[Application (**アプリケーション**)]** 、**[byte (**バイト**)]**、**[Sessions (**セッション**)]** を [選択した列] リストに追加します。
6. 目標の**[Time Frame**（期間）**]**、**[Sort By**（ソート基準）**]**および**[Group By**（グループ化基準）**]**を設定します。
7. そのインターゾーン デフォルト ルールにマッチするトラフィックにマッチさせるクエリを定義します：

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

STEP 5 | **Commit**（コミット）をクリックして変更内容をルールベースにコミットします。

ポリシー ルールベースの監視と調整

最良のセキュリティ ポリシーを作成するのは反復的な作業です。最初のインターネット ゲートウェイ セキュリティ ポリシーを定義した後、ポリシーのギャップや警戒すべき動作を特定する一時的なルールに一致するトラフィックを監視し、それに応じてポリシーを調整します。これらのルールに一致するトラフィックを監視すると、永続ルールを適切に調整して、すべてのトラフィックがアプリケーションの許可ルールに一致することを確認したり、ルールに一致しないアプリケーションを許可するかどうかを評価したりできます。

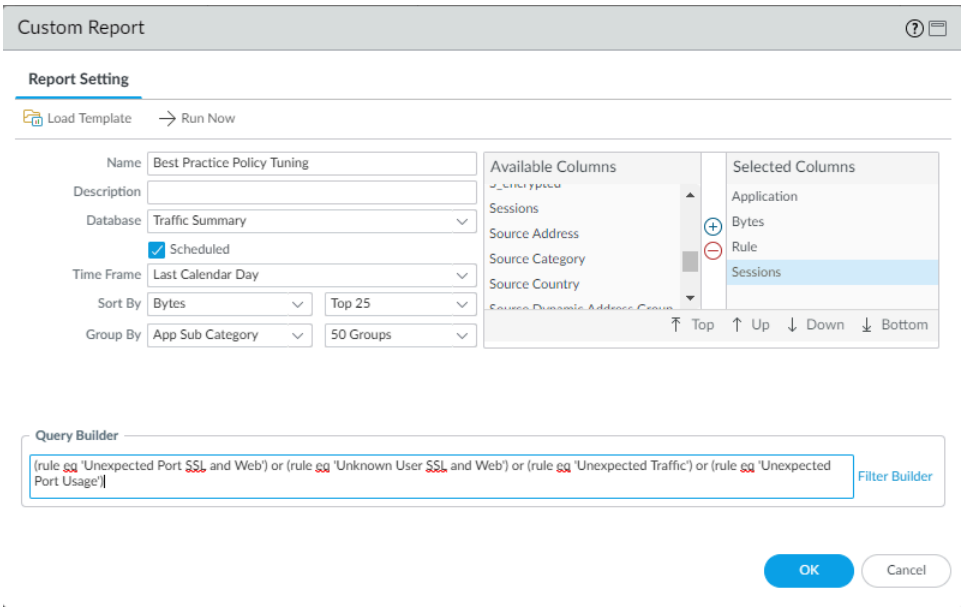
ルールベースを調整すると、一時ルールとの一致を許可するトラフィックが減少するはずです。これらのルールに一致する許可したいトラフィックが表示されなくなったら、ポジティブ強制許可ルールは完了し、一時ルールを削除できます (インターゾーン間デフォルトの拒否ルールは、どのルールも明示的に許可しないトラフィックを自動的に拒否します)。

毎月のコンテンツ リリースでは新しい *App-ID* が追加されるため、App-ID の変更がセキュリティ ポリシーに与える影響を確認してください。

STEP 1 | カスタム レポートを作成して、ポリシー ギャップを特定するルールに一致するトラフィックを監視します。

1. **Monitor (監視) > Manage Custom Reports (カスタム レポートの管理)**の順に選択します。
2. レポートを追加 し、調査しているポリシーのギャップを示す分かりやすい 名前 を付けます。
3. **Database**（データベース）を**Traffic Summary**（トラフィックサマリー）に設定します。
4. **Scheduled**（スケジュール済み）を選択します。
5. **Rule (ルール)**、**Application (アプリケーション)**、**byte (バイト)**、**Sessions (セッション)**を[選択された列] リストに追加します。
6. 目標の**Time Frame**（期間）、**Sort By**（ソート基準）および**Group By**（グループ化基準）を設定します。
7. ポリシーのギャップや警告動作を検出するルールに一致するトラフィックを照合するクエリを定義します。**or**（または）演算子を使用してルールのいずれかにマッチするトラフィックの詳細に関する単一のレポートを作成したり、個々のレポートを作成して各ルールを監視したりすることができます。次のクエリの例では、ポリシー例で定義されたルール名を使用します。
   - `(rule eq 'Unexpected Port SSL and Web')`
   - `(rule eq 'Unknown User SSL and Web')`
   - `(rule eq 'Unexpected Traffic')`

- `(rule eq 'Unexpected Port Usage')`



STEP 2 | レポートを定期的に確認して、トラフィックが各調整ルールに一致する理由を理解してください。正規のアプリケーションとユーザーを含めるようにルールを更新するか、レポートの情報を使用してアプリケーションのリスクを評価し、ポリシー改革を実施します。

一時ルールの削除

最初のインターネット ゲートウェイのベストプラクティス セキュリティ ポリシーを数か月監視し、ルールベースを調整すると、一時的なルールに一致する許可したいトラフィックが減少するはずです。許可するトラフィックがこれらのルールに一致しなくなれば、完全にアプリケーション ベースのセキュリティポリシーのルールベースへの移行を達成できたことになります。正当なユースケースを持たないアプリケーションやパブリック DNS および SMTP アプリケーションの アプリケーション ブロック ルール を含む一時ルールを削除できるようになりました。これは、デフォルトのインターゾーン間デフォルト拒否ルールが明示的な許可ルールに一致しないため、そのトラフィックが自動的にブロックされるためです。（QUICというルールを守ってください。）

STEP 1 | **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。

STEP 2 | ルールを選択して**Delete**（削除）をクリックします。

あるいは、削除する前に一定期間そのルールを**Disable**（無効化）します。これにより、許可したいトラフィックがインターゾーン間デフォルトの拒否ルールに一致することがトラフィック ログで確認された場合、それらを再度 有効にする ことができます。

STEP 3 | 変更を **Commit**（コミット）します。

ルールベースの管理

ビジネスとアプリケーションは進化するため、セキュリティ ポリシーのルールベースも進化する必要があります。認可されたアプリケーションが変更された場合は、新しいルールを追加するのではなく、可能な限り、アプリケーションのビジネスユースケースに合わせて既存のポリシールールに対応する変更を加えます。多くの場合、変更は、アプリケーション グループに新しいアプリケーションを追加したり、アプリケーション グループから非推奨のアプリケーションを削除したりするのと同じくらい簡単です。

Panorama あるいはスタンドアロンのファイアウォール上でポリシー ルール ヒット カウンターを使用してルールベースに対する変更を分析します。例えば、新しいアプリケーションを追加する際、そのアプリケーションのトラフィックをネットワーク上で許可する前に、許可ルールをルールベースに追加します。トラフィックがルールにヒットしてカウンタがインクリメントされた場合は、アプリケーションをアクティブ化していないにもかかわらず、ルールに一致するトラフィックがすでにネットワーク上にあるか、ルールを調整する必要がある場合があります。続けて、***ACC > Threat Activity***（脅威アクティビティ）***> Applications Using Non Standard Ports***（非標準ポートを使用するアプリケーション）および***ACC > Threat Activity***（脅威アクティビティ）***> Rules Allowing Apps On Non Standard Ports***（標準的でないポート上のアプリを許可するルール）ウィジェットをチェックし、標準的でないポート上のトラフィックが予期せぬルールのヒットを生じさせていないか確認します。

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

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

Palo Alto Networks のコンテンツアップデートを自動的にダウンロードするように設定し、できるだけ早くファイアウォールへのインストールをスケジュールします。アプリケーションと脅威のコンテンツの更新は、セキュリティ プロファイルの署名の更新 が必要になるたびに行われます。毎月第 3 火曜日に送信されるコンテンツの更新には、新しい App-ID と変更された App-ID も含まれています (アプリケーションの更新、まれにアプリケーションの更新が 1 日または 2 日遅れることがあります)。新規および変更された App-ID が非実稼働環境でセキュリティ ポリシーのルールベースにどのように影響するかを評価し、必要に応じてルールを変更します。

コンテンツ更新のベストプラクティス に従い 、インターネットゲートウェイを保護するためにできるだけ早く更新をインストールし、すべてのコンテンツ更新に対してログ転送 を設定します 。

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

STEP 2 | 必要な場合は既存のセキュリティポリシールールを修正し、App-ID の変更を反映させてください。さらにテストが必要な App-ID が一部ある場合は選択した App-ID を無効化し、他の新規および変更された App-ID をインストールすることができます。オーバーラップを避けるため、新しい App-ID が含まれる翌月のコンテンツがリリースされるまでに、必要なポリシーの修正およびテストを終わらせてください。

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