アクセス コントロールの概要

アクセス制御の概要

アクセス制御は、（非高速パスを通る）ネットワーク トラフィックの指定、検査、ロギングが可能な階層型ポリシーベースの機能です。

各管理対象デバイスは 1 つのアクセス コントロール ポリシーのターゲットにすることができます。ポリシーのターゲット デバイスがネットワーク トラフィックについて収集したデータは、以下に基づいてそのトラフィックのフィルタや制御に使用できます。

- トランスポート層およびネットワーク層の特定しやすい単純な特性（送信元と宛先、ポート、プロトコルなど）
- レピュテーション、リスク、ビジネスとの関連性、使用されたアプリケーション、または訪問した URL などの特性を含む、トラフィックに関する最新のコンテキスト情報
- レルム、ユーザ、ユーザ グループ、または ISE の属性
- カスタム セキュリティ グループ タグ（SGT）
- 暗号化されたトラフィックの特性（このトラフィックを復号してさらに分析することもできます）
- 暗号化されていないトラフィックまたは復号されたトラフィックに、禁止されているファイル、検出されたマルウェア、または侵入の試みが存在するかどうか
- 時刻と日（サポートされているデバイス上）

各タイプのトラフィックのインスペクションと制御は、最大限の柔軟性とパフォーマンスを引き出すために最も意味がある局面で実行されます。たとえば、レピュテーションベースのブロッキングはシンプルな送信元と宛先のデータを使用しているため、禁止されているトラフィックを初期の段階でブロックできます。これに対し、侵入およびエクスプロイトの検知とブロックは最終防衛ラインです。

ルールの概要

さまざまなポリシータイプ（アクセス制御、SSL、アイデンティティなど）のルールで、ネットワークトラフィックをきめ細かく制御できます。システムは最初の一致のアルゴリズムを使用して、指定した順番でルールに照らし合わせてトラフィックを評価します。

これらのルールにはポリシー全体で一貫していない他の設定が含まれている場合もありますが、次のような基本的な特性や設定メカニズムの多くは共通です。

- 条件：ルールの条件は各ルールが処理するトラフィックを指定します。複数の条件により各ルールを設定できます。トラフィックは、ルールに一致するすべての条件に適合する必要があります。
- アクション：ルールのアクションによって、一致するトラフィックの処理方法が決まります。選択できる [アクション（Action）] リストがルールにない場合でも、ルールには関連付けられたアクションが 1 つある点に注意してください。たとえば、カスタム ネットワーク分析ルールはそのルールの「アクション」としてネットワーク分析ポリシーを使用します。 別の例としては、QoS ルールの場合、どの QoS ルールでもトラフィックのレート制限という同じ動作をするため、明示的なアクションはありません。
- 位置：ルールの位置は評価の順番を決定します。ポリシーを使ってトラフィックを評価すると、システムは指定した順序でトラフィックとルールを照合します。通常は、システムによるトラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初のルールに従って行われます（追跡とログ記録を行うように設計されたモニタールールは例外です）。適切なルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。
- カテゴリ：いくつかのルール タイプを整理するために、各親ポリシーでカスタムのルール カテゴリを作成できます。
- ロギング：多くのルールでは、ルールが処理する接続をシステムがロギングするかどうか、およびロギングの処理方法は、ロギングの設定によって制御されます。一部のルール（ID ルールやネットワーク分析ルールなど）にはロギング設定は含まれません。これは、ルールが接続の最終的な性質を決定するわけではなく、またそのルールが接続をロギングするために特別に設計されているわけではないためです。 別の例としては、QoS ルールにはロギングの設定は含まれていません。これは、レート制限されているというだけの理由で接続をロギングすることはできないためです。
- コメント：一部のルール タイプでは、変更を保存するたびにコメントを追加できます。たとえば、他のユーザーのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。

ヒント　多くのポリシーエディタでは、右クリック メニューで編集、削除、移動、有効化、無効化など、数多くのルール管理オプションへのショートカットを提供しています。

詳細については、関心のあるルール（アクセス制御ルールなど）について記載されている章を参照してください。

関連トピック

アプリケーション条件とフィルタの設定
アプリケーション制御のベストプラクティス （13 ページ）

デバイス別のフィルタリング ルール

一部のポリシーエディタでは、該当デバイスによってルールの表示をフィルタ処理することができます。

システムは、ルールがそのデバイスに影響するかどうかを判断するために、ルールのインターフェイス制約を使用します。インターフェイス（セキュリティゾーンまたはインターフェイス グループの条件）でルールを制約すると、インターフェイスが置かれている場所のデバイスがそのルールの影響を受けます。インターフェイス制約のないルールは、すべてのインターフェイスに適用されるので、すべてのデバイスに適用されることになります。

QoS ルールは、常にインターフェイスで制約されます。

（注）　次の手順は、アクセス コントロール ポリシーには適用されません。アクセス コントロール ポリシー内の特定のデバイスまたは一連のデバイスに適用されるルールを確認するには、[フィルタ（FIlter）] アイコンをクリックしてデバイスを選択します。

手順

ステップ 1　ポリシーエディタで、[ルール（Rules）] をクリックし、[デバイスでフィルタ処理（Filter by Device）] をクリックします。
ターゲット デバイスとデバイス グループのリストが表示されます。

ステップ 2　1 つまたは複数のチェック ボックスをオンにして、これらのデバイスまたはグループに適用されるルールだけを表示します。または、[すべて（All）] をオンにしてリセットし、すべてのルールを表示します。

ヒント　ポインタをルール基準に合わせると、その値が表示されます。基準がデバイス特有のオーバーライドを持つオブジェクトを表し、そのデバイスだけでルール リストをフィルタ処理する場合、システムはオーバーライド値を表示します。基準がドメイン特有のオーバーライドを持つオブジェクトを表し、そのドメインのデバイスでルール リストをフィルタ処理する場合、システムはオーバーライド値を表示します。

ステップ 3 [OK] をクリックします。

ルールとその他のポリシーの警告

ポリシーおよびルールエディタでは、トラフィックの分析やフローに悪影響を与える可能性のある設定をアイコンで示します。問題に応じて、システムはユーザがそのようなポリシーを展開しようとするときに警告するか、導入を完全に阻止します。

ヒント 警告、エラー、または情報のテキストを確認するには、マウスのポインタをアイコンの上に置きます。

表 *1*: ポリシーのエラー アイコン

アイコン	説明	例
[エラー（Error）] (✖)	ルールまたは設定にエラーがある場合、影響を受けるルールを無効にしても、問題を修正するまではポリシーを展開できません。	カテゴリおよびレピュテーション ベースの URL フィルタリングを実行するルールは、URL フィルタリング ライセンスのないデバイスをターゲットにする時点まで有効です。その時点で、ルールの横にエラー アイコンが表示され、ポリシーを展開できなくなります。ポリシーを展開するには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、URL フィルタリング ライセンスを有効にする必要があります。
[警告（Warning）] (⚠)	ルールに関する警告またはその他の警告が表示されていても、ポリシーを展開することはできます。しかし、警告でマークされている誤った設定は有効になりません。 警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。	プリエンプトされるルール、または誤った設定によりトラフィックを照合できないルールは有効になりません。誤った設定には、空のオブジェクト グループ、一致するアプリケーションがないアプリケーション フィルタ、除外された LDAP ユーザ、無効なポートなどを使用した条件が含まれます。 一方、警告アイコンがライセンス エラーまたはモデルの不一致を示している場合は、問題を修正するまでそのポリシーを展開することはできません。

アイコン	説明	例
[情報（Information）]（  ）	情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を表示します。これらの問題によってポリシーの展開が阻止されることはありません。	システムは接続でアプリケーショントラフィックまたは Web トラフィックを識別するまで、その接続の最初の数パケットと一部のルールとの照合をスキップすることがあります。これにより、アプリケーションと HTTP 要求が識別されるように接続が確立されます。
[ルールの競合（Rule Conflict）]（）	ルール競合分析を有効にすると、競合のあるルールのルールテーブルにこのアイコンが表示されます。	競合には、冗長なルール、冗長なオブジェクト、およびシャドウイングされたルールが含まれます。以前のルールがすでに基準に一致しているため、冗長なルールやシャドウイングされたルールはトラフィックと一致しません。冗長なオブジェクトは、ルールを不必要に複雑にします。

アクセス コントロール ポリシーのデフォルト アクション

新しく作成したアクセス コントロール ポリシーは、デフォルト アクションを使用して、すべてのトラフィックを処理するようにターゲット デバイスに指示します。

単純なアクセス コントロール ポリシーでは、デフォルト アクションは、ターゲット デバイスがすべてのトラフィックをどう処理するかを指定します。より複雑なポリシーでは、デフォルト アクションは次のトラフィックを処理します。

- インテリジェント アプリケーション バイパスで信頼されないトラフィック
- セキュリティ インテリジェンス ブロック リストにないトラフィック
- SSLインスペクションによってブロックされていないトラフィック（暗号化トラフィックのみ）
- ポリシー内のどのルールにも一致しないトラフィック（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）

アクセス コントロール ポリシーのデフォルト アクションにより、追加のインスペクションなしでトラフィックをブロックまたは信頼することができます。また、侵入およびディスカバリデータの有無についてトラフィックを検査することもできます。

（注） デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行**できません**。デフォルトアクションで処理される接続のロギングは、初期設定では無効ですが、有効にすることもできます。

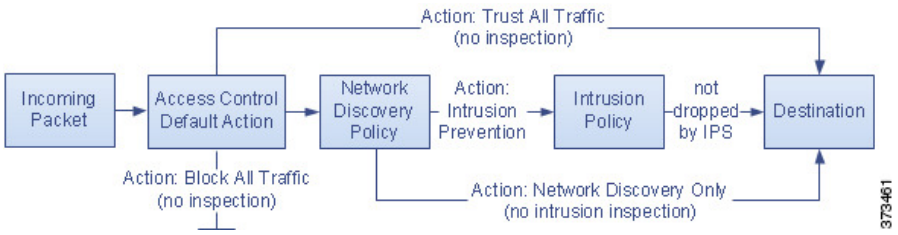
ポリシーを継承している場合、最下位の子孫のデフォルトアクションによってトラフィックの最終的な処理が決まります。アクセス コントロール ポリシーのデフォルト アクションは基本ポリシーから継承することもできますが、継承したデフォルトアクションを強制的に実施することはできません。

次の表に各デフォルトアクションが処理するトラフィックに対して実施可能なインスペクションの種類を示します。

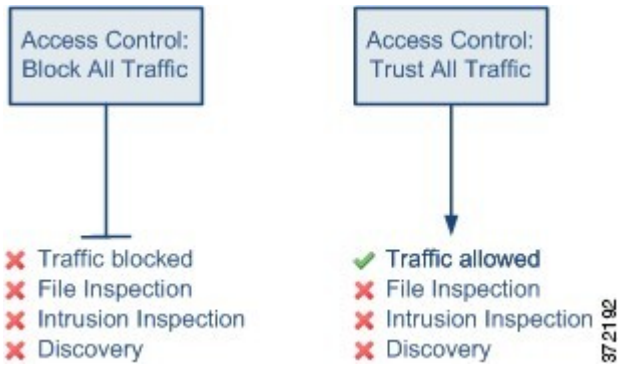
表 *2:* アクセス コントロール ポリシーのデフォルト アクション

デフォルト アクション	トラフィックに対して行う処理	インスペクション タイプとポリシー
アクセス コントロール：すべてのトラフィックをブロック	それ以上のインスペクションは行わずにブロックする	なし
アクセス コントロール：すべてのトラフィックを信頼	信頼（追加のインスペクションなしで最終宛先に許可）	なし
侵入防御（Intrusion Prevention）	ユーザが指定した侵入ポリシーに合格する限り、許可する	侵入、指定した侵入ポリシーおよび関連する変数セットを使用、および 検出（discovery）、ネットワーク検出ポリシーを使用
ネットワーク検出のみ（Network Discovery Only）	許可（allow）	検出のみ（discovery only）、ネットワーク検出ポリシーを使用
基本ポリシーから継承	基本ポリシーで定義	基本ポリシーで定義

次の図は、表を図で表したものです。



次の図は、[すべてのトラフィックをブロック（Block All Traffic）]および[すべてのトラフィックを信頼（Trust All Traffic）] のデフォルト アクションを示しています。



次の図は、[侵入防御（Intrusion Prevention）] および [ネットワーク検出のみ（Network Discovery Only）] のデフォルト アクションを説明しています。

ヒント [ネットワーク検出のみ（Network Discovery Only）] の目的は、検出のみの展開でパフォーマンスを向上させることです。侵入検知および防御のみを目的としている場合は、さまざまな設定でディスカバリを無効にできます。

ファイルポリシーと侵入ポリシーを使用したディープインスペクション

ディープインスペクションは、トラフィックが宛先に対して許可される前の最後のとりでとして、侵入ポリシーとファイルポリシーを使用します。

- 侵入ポリシーは、システムの侵入防御機能を制御します。

  詳細については、侵入検知と防御を参照してください。

- ファイル ポリシーは、システムのファイル制御と マルウェア防御 の機能を管理します。

  詳細については、ネットワークマルウェア防御とファイルポリシーを参照してください。

アクセス コントロールはディープ インスペクションの前に発生し、アクセス コントロール ルールおよびアクセス コントロールのデフォルト アクションによって、侵入ポリシーおよびファイル ポリシーで検査されるトラフィックが決まります。

侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセスコントロールルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイルポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。

アクセスコントロールポリシーでは、1つの侵入ポリシーを各許可ルール、インタラクティブブロック ルール、およびデフォルト アクションと関連付けることができます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。

アクセス制御ルールに侵入ポリシーとファイルポリシーを関連付けるには、次を参照してください。

- 侵入防御を実行するためのアクセスコントロールルール設定
- マルウェア保護のためのアクセス コントロール ルールの設定

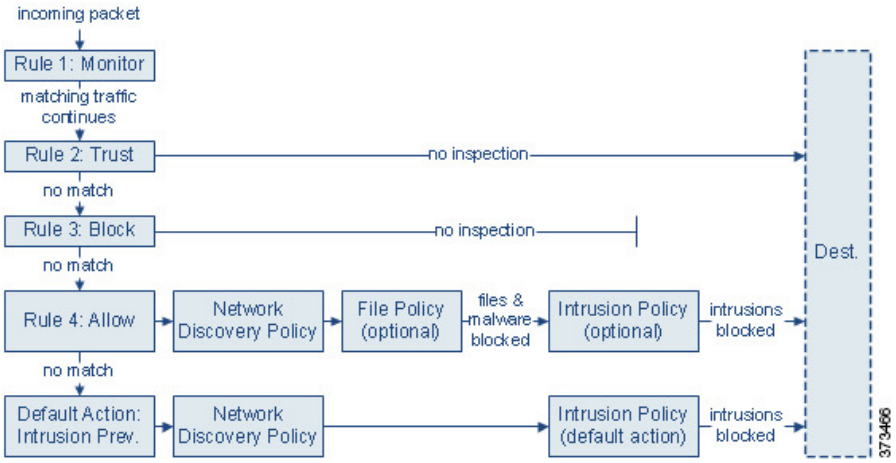
（注） デフォルトでは、暗号化されたペイロードの侵入インスペクションとファイルインスペクションは無効になっています。これにより、侵入およびファイルインスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。

関連トピック

ポリシーがトラフィックで侵入を検査する方法
ファイル ポリシー

侵入ポリシーとファイルポリシーを使用したアクセス制御トラフィック処理

次の図は、4 つの異なるタイプのアクセス コントロール ルールとデフォルト アクションを含むアクセスコントロールポリシーによって制御されている、インラインの侵入防御とマルウェア防御 の展開におけるトラフィックのフローを示します。



上記のシナリオでは、ポリシー内の最初の 3 つのアクセス コントロール ルール（モニター、信頼およびブロック）は一致するトラフィックを検査できません。モニター ルールはネットワーク トラフィックの追跡とロギングを行いますが検査はしないので、システムは引き続きトラフィックを追加のルールと照合し、許可または拒否を決定します。（ただし、重要な例外と注意事項をアクセス コントロール ルールのモニター アクションで確認してください）。信頼ルールおよびブロック ルールは、どのような種類のインスペクションも追加で行うことなく一致するトラフィックを処理しますが、一致しないトラフィックは引き続き次のアクセス コントロール ルールに照合されます。

ポリシー内の 4 番目と最後のルールである許可ルールは、次の順序で他のさまざまなポリシーを呼び出し、一致するトラフィックを検査および処理します。

- **ディスカバリ**：**ネットワーク検出ポリシー**：最初に、ネットワーク検出ポリシーがトラフィックのディスカバリ データの有無を検査します。ディスカバリはパッシブ分析で、トラフィックのフローに影響しません。明示的にディスカバリを有効にしなくても、それを拡張または無効にできます。ただし、トラフィックを許可しても、ディスカバリ データ収集が自動的に保証されるわけではありません。システムは、ネットワーク検出ポリシーによって明示的にモニターされる IP アドレスを含む接続に対してのみ、ディスカバリを実行します。

- **[マルウェア防御 とファイル制御**：**ファイル ポリシー（AMP for Networks and File Control: File Policy）]**：トラフィックが検出により調査された後、システムが禁止ファイルやマルウェアを調査します。マルウェア防御 は PDF や Microsoft Office ドキュメントなど、多くのタイプのファイルでマルウェアを検出し、必要に応じてブロックします。部門がマルウェア ファイル伝送のブロックに加えて、（ファイルにマルウェアが含まれるかどうかにかかわらず）特定のタイプのすべてのファイルをブロックする必要がある場合は、ファイル制御機能により、特定のファイル タイプの伝送についてネットワーク トラフィックをモニターし、ファイルをブロックまたは許可できます。

- **侵入防御**：**侵入ポリシー**：ファイルインスペクションの後、システムは侵入およびエクスプロイトについてトラフィックを検査できます。侵入ポリシーは、復号されたパケットの攻撃をパターンに基づいて調査し、悪意のあるトラフィックをブロックしたり、変更したりします。侵入ポリシーは変数セットとペアになり、それによって名前付き値を使用してネットワーク環境を正確に反映できます。

- **接続先**：前述のすべてのチェックを通過したトラフィックは、その接続先に渡されます。

インタラクティブ ブロック ルール（この図には表示されていません）には、許可ルールと同じインスペクション オプションがあります。これにより、あるユーザーが警告ページをクリック スルーすることによってブロックされた Web サイトをバイパスした場合に、悪意のあるコンテンツがないかトラフィックを検査できます。

モニター以外のアクションに関するポリシー内のアクセスコントロールルールのいずれにも一致しないトラフィックは、デフォルトアクションによって処理されます。このシナリオでは、デフォルトアクションは侵入防御アクションとなり、トラフィックは指定された侵入ポリシーを通過する限りその最終接続先に許可されます。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルトアクションが割り当てられている場合もあります。システムはデフォルトアクションによって許可されたトラフィックに対しディスカバリ データおよび侵入の有無を検査できますが、禁止されたファイルまたはマルウェアの有無は検査できないことに注意してください。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

（注） 場合によっては、接続がアクセス コントロール ポリシーによって分析される場合、システムはトラフィックを処理するアクセス コントロール ルール（存在する場合）を決定する前に、その接続の最初の数パケットを処理し**通過を許可する**必要があります。ただし、こうしたパケットが検査されていない宛先に到達しないように、こうしたパケットを検査して侵入イベントを生成する侵入ポリシーを（アクセスコントロールポリシーの詳細設定で）指定できます。

ファイル インスペクションおよび侵入インスペクションの順序

アクセス コントロール ポリシーで、複数の許可ルールとインタラクティブ ブロック ルールを異なる侵入ポリシーおよびファイル ポリシーに関連付けて、インスペクション プロファイルをさまざまなタイプのトラフィックに照合できます。

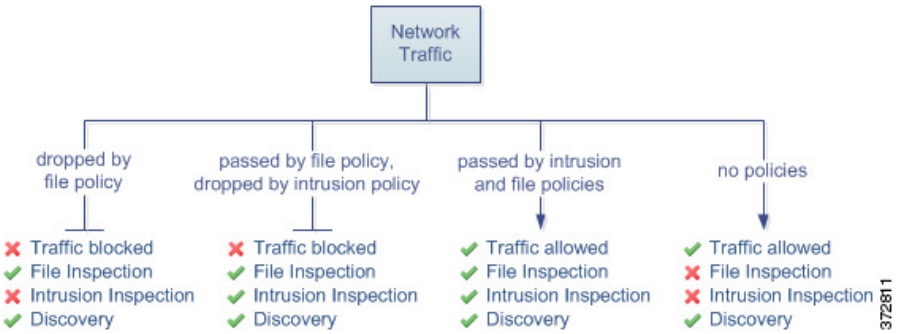
（注） 侵入防御またはネットワーク検出のみのデフォルトアクションによって許可されたトラフィックは、検出データおよび侵入の有無について検査されますが、禁止されたファイルまたはマルウェアの有無については検査されません。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

同じルールでファイルインスペクションと侵入インスペクションの両方を実行する必要はありません。許可ルールまたはインタラクティブ ブロック ルールに一致する接続の場合：

- ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーによって決まります
- 侵入ポリシーがない場合、トラフィック フローはファイル ポリシーによって決まります
- どちらもない場合、許可されたトラフィックはネットワーク検出のみで検査されます。

ヒント システムは、信頼されたトラフィックに対してはどんなインスペクションも実行しません。侵入ポリシーもファイルポリシーも含めずに許可ルールを設定すると、信頼ルールの場合と同様にトラフィックが通過しますが、許可ルールでは一致するトラフィックに対して検出を実行できます。

以下の図は、「許可」アクセス コントロール ルール、またはユーザによりバイパスされた「インタラクティブブロック」アクセス コントロール ルールのどちらかの条件を満たすトラフィックに対して実行できるインスペクションの種類を示しています。単純化のために、侵入/ファイル ポリシーの両方が 1 つのアクセス コントロール ルールに関連付けられている（またはどちらも関連付けられていない）状態でのトラフィック フローを図に示しています。



アクセス コントロール ルールによって処理される単一接続の場合、ファイル インスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入のためファイル ポリシーによってブロックされたファイルを検査しません。ファイルインスペクション内では、タイプによる単純なブロッキングの方が、マルウェア インスペクションおよびブロッキングよりも優先されます。

たとえば、アクセス コントロール ルールで定義された特定のネットワーク トラフィックを正常に許可するシナリオを考えてください。ただし、予防措置として、実行可能ファイルのダウンロードをブロックし、ダウンロードされた PDF のマルウェア インスペクションを行って検出された場合はブロックし、トラフィックに対して侵入インスペクションを実行する必要があるとします。

一時的に許可するトラフィックの特性に一致するルールを持つアクセス コントロール ポリシーを作成し、それを侵入ポリシーとファイル ポリシーの両方に関連付けます。ファイル ポリシーはすべての実行可能ファイルのダウンロードをブロックし、マルウェアを含む PDF も検査およびブロックします。

- まず、システムはファイル ポリシーで指定された単純なタイプ マッチングに基づいて、すべての実行可能ファイルのダウンロードをブロックします。これはすぐにブロックされるため、これらのファイルは、マルウェア インスペクションの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされた PDF に対するマルウェア クラウド ルックアップを実行します。マルウェアの性質を持つ PDF はすべてブロックされ、侵入インスペクションの対象にはなりません。

- 最後に、システムはアクセス コントロール ルールに関連付けられている侵入ポリシーを使用して、ファイルポリシーでブロックされなかったファイルを含む残りのトラフィック全体を検査します。

（注） ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

アクセス コントロール ポリシーの継承

アクセス コントロール ポリシーはネストすることができます。このポリシーでは各ポリシーが先祖（または基本）ポリシーからルールや設定を継承します。この継承を強制することもできますが、下位のポリシーによる先祖ポリシーの上書きを許可することもできます。

アクセス制御は階層型ポリシーベース実装となっています。ドメイン階層を作成するのと同様に、対応するアクセス コントロール ポリシーの階層を作成できます。子孫（あるいは子）アクセス コントロール ポリシーは、直接の親（あるいは基本）ポリシーからルールや設定を継承します。この基本ポリシーにもさらに親ポリシーがあり、その親ポリシーにもさらに、というようにルールや設定が継承されている場合もあります。

アクセス コントロール ポリシーのルールは、親ポリシーの [強制（Mandatory）] ルール セクションと [デフォルト（Default）] のルール セクションの間にネストされています。この実装により、先祖ポリシーの [強制（Mandatory）] ルールは実施される一方、先祖ポリシーの [デフォルト（Default）] ルールは現在のポリシーでプリエンプション処理することが可能です。

次の設定をロックすることで、すべての子孫ポリシーに設定を実行させることができます。ロック解除された設定については、子孫ポリシーによる上書きが可能です。

- セキュリティ インテリジェンス：IPアドレス、URL、ドメイン名の最新のレピュテーション インテリジェンスをもとに接続を許可またはブロックされた接続。
- HTTP 応答ページ：ユーザーの Web サイト リクエストをブロックした際、カスタム応答ページあるいはシステム提供の応答ページを表示します。
- 詳細設定：関連するサブポリシー、ネットワーク分析設定、パフォーマンス設定、その他の一般設定オプションを指定します。

ポリシーを継承している場合、最下位の子孫のデフォルトアクションによってトラフィックの最終的な処理が決まります。アクセス コントロール ポリシーのデフォルト アクションは先祖ポリシーから継承することもできますが、継承を強制的に実施することはできません。

ポリシーの継承とマルチテナンシー

アクセス制御の階層型ポリシーベース実装はマルチテナンシーを補完します。

通常のマルチドメイン導入環境では、アクセス コントロール ポリシーの階層がドメイン構造に対応しており、管理対象デバイスに最下位レベルのアクセス コントロール ポリシーを適用

します。この実装により、ドメインの上層レベルでは選択的にアクセス制御を実施しながらも、ドメインの下層レベルの管理者は展開ごとに設定を調整することが可能です（子孫ドメインの管理者を制限するには、ポリシー継承と適用だけでなく、ロールによる制限を行う必要があります）。

たとえば、所属している部門のグローバル ドメイン管理者は、グローバル レベルのアクセス コントロール ポリシーを作成できます。そして、そのグローバル レベルのポリシーを基本ポリシーとして、機能別にサブドメインに分けられたすべてのデバイスで使用するよう要求することがことが可能です。

サブドメインの管理者が Secure Firewall Management Center にログインしてアクセス制御を設定する際、グローバル レベルのポリシーはそのまま展開できます。あるいは、グローバル レベルのポリシーの範囲内の子孫アクセス コントロール ポリシーを作成、展開することも可能です。

（注） アクセス制御の継承および適用が最も有効に実装されるのは、マルチテナンシーを補完する場合ですが、1 つのドメイン内においてもアクセス制御ポリシーを階層化することが可能です。また、任意のレベルでアクセス コントロール ポリシーを割り当て、展開することもできます。

アプリケーション制御のベストプラクティス

次のトピックでは、アクセス制御ルールを使用してアプリケーションを制御するための推奨されるベストプラクティスについて説明します。

アプリケーション制御に関する推奨事項

アプリケーション制御に関する次の注意事項と制約事項に注意してください。

アダプティブ プロファイルが有効になっていることの確認

アダプティブ プロファイルが無効な場合（デフォルト状態）、アクセス制御ルールは、アプリケーション制御を実行できません。

アプリケーション ディテクタの自動有効化

ディテクタが検出対象のアプリケーションに対して有効でない場合、システムは、そのアプリケーションに対応するシステム提供のすべてのディテクタを自動的に有効にします。存在しない場合、システムはそのアプリケーション対応で最近変更されたユーザー定義のディテクタを有効にします。

アプリケーションを識別する前に通過する必要のあるパケットを調べるためのポリシーの設定

システムは、次の両方の条件が満たされるまで、インテリジェント アプリケーション バイパス（IAB）およびレート制限を含むアプリケーション制御を実行できません。

- モニター対象の接続がクライアントとサーバーの間で確立される。
- システムがセッションでアプリケーションを識別する

この識別は3～5パケット以内で、またはトラフィックが暗号化されている場合は、SSLハンドシェイクのサーバー証明書交換の後に行われる必要があります。

重要これらの初期パケットをシステムが確実に調べるようにするには、トラフィック識別の前に通過するパケットを処理するためのポリシーの指定を参照してください。

早期のトラフィックがその他のすべての基準に一致するが、アプリケーション識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、SSLハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッション トラフィックに適切なアクションを適用します。

（注） システムがアプリケーションを認識できるようにするため、サーバーはアプリケーションのプロトコル要件に準拠する必要があります。たとえば、ACKが期待されるときにACKではなくキープアライブパケットを送信するサーバーがある場合、そのアプリケーションは識別されない可能性があり、接続はアプリケーションベースのルールに一致しません。代わりに、接続は別の一致するルールまたはデフォルトアクションによって処理されます。これは、許可したい接続がむしろ拒否される可能性があることを意味します。この問題が発生し、プロトコルの標準規格に準拠するようにサーバーを修正できない場合は、たとえば、IPアドレスとポート番号を照合することで、そのサーバーのトラフィックをカバーする非アプリケーションベースのルールを作成する必要があります。

URLとアプリケーションのフィルタリング用の個別のルールの作成

アプリケーションとURLの基準を組み合わせることで、予期しない結果が生じることがある（特に暗号化されたトラフィックの場合）ため、可能な限り、URLとアプリケーションのフィルタリング用に個別のルールを作成します。

アプリケーションとURLの基準の両方を含むルールは、より一般的なアプリケーションのみまたはURLのみのルールの例外として機能している場合を除き、アプリケーションのみまたはURLのみのルールの後に来る必要があります。

アプリケーションや他のルールより前に配置されるURLルール

URLマッチングを最も効果的に行うには、URL条件を含むルールを他のルールより前に配置します。特に、URLルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。
- 検査対象のトラフィックが暗号化されている。

暗号化および復号トラフィックのアプリケーション制御

システムは暗号化トラフィックと復号トラフィックを識別し、フィルタ処理することができます。

- 暗号化トラフィック：システムは、SMTPS、POPS、FTPS、TelnetS、IMAPS を含む StartTLS で暗号化されたアプリケーション トラフィックを検出できます。さらに、TLS ClientHello メッセージの Server Name Indication、またはサーバー証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。これらのアプリケーションに `SSL Protocol` タグが付けられます。SSL ルールでは、これらのアプリケーションのみを選択できます。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。
- 復号トラフィック：システムは、復号されたトラフィック（暗号化されたまたは暗号化されていないトラフィックではなく）のみで検出を行うことができるアプリケーションに `decrypted traffic` タグを割り当てます。

TLS サーバーアイデンティティ検出とアプリケーション制御

RFC 8446 で定義されている最新バージョンの Transport Layer Security（TLS）プロトコル 1.3 は、セキュアな通信を提供するために多くの Web サーバーで採用されているプロトコルです。TLS 1.3 プロトコルが、セキュリティを強化するためにサーバーの証明書を暗号化する一方で、証明書が、アクセスコントロールルールのアプリケーションおよび URL フィルタリング基準に適合する必要があるため、Firepower システムは、パケット全体を復号せずにサーバー証明書を抽出する方法を提供します。

この機能は、アプリケーションまたは URL の基準に適合させたいトラフィックに関して、特にそのトラフィックの詳細な検査を実行する必要がある場合に、有効にすることを強くお勧めします。サーバー証明書を抽出するプロセスでトラフィックが復号されないため、復号ポリシー は必要ありません。

詳細については、アクセス コントロール ポリシーの詳細設定を参照してください。

アプリケーションのアクティブ認証の免除

アイデンティティ ポリシーでは、特定のアプリケーションのアクティブ認証を免除し、トラフィックにアクセス コントロールの続行を許可できます。これらのアプリケーションには、`User-Agent Exclusion` タグが付けられます。アイデンティティ ルールでは、これらのアプリケーションのみを選択できます。

ペイロードのないアプリケーション トラフィック パケットの処理

アクセスコントロールを実行している場合、システムは、アプリケーションが識別された接続内にペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。

参照されるアプリケーション トラフィックの処理

アドバタイズメント トラフィックなどの Web サーバーによって参照されるトラフィックを処理するには、参照しているアプリケーションではなく、参照されるアプリケーションを照合します。

複数のプロトコルを使用するアプリケーション トラフィックの制御（Skype、Zoho）

一部のアプリケーションは、複数のプロトコルを使用します。このようなアプリケーションのトラフィックを制御するには、関連するすべてのオプションがアクセス コントロール ポリシーの対象となっていることを確認します。次に例を示します。

- Skype：Skype のトラフィックを制御するには、個々のアプリケーションを選択するのではなく、[アプリケーション フィルタ（Application Filters）] リストから [Skype] タグを選択します。これにより、システムは同じ方法で Skype のすべてのトラフィックを検出して制御できるようになります。
- Zoho：Zoho メールを制御するには、[使用可能なアプリケーション（Available Application）] リストから [Zoho] と [Zohoメール（Zoho mail）] の両方を選択します。

コンテンツ制限機能用にサポートされる検索エンジン

システムは、特定の検索エンジンの場合のみ、セーフ サーチ フィルタリングをサポートします。システムは、これらの検索エンジンからのアプリケーション トラフィックに `safesearch supported` タグを割り当てます。

回避的アプリケーション トラフィックの制御

用途別の注意事項と制限事項 （19 ページ） を参照してください。

アプリケーション制御の設定のベストプラクティス

アプリケーションによるネットワークへのアクセスを次のように制御することをお勧めします。

- 安全性の低いネットワークからより安全なネットワークへのアプリケーション アクセスを許可またはブロックするには、アクセス コントロール ルールで**ポート**(選択された宛先ポート) 条件を使用します。

  たとえば、インターネット（安全性が低い）から内部ネットワーク（安全性が高い）への ICMP トラフィックを許可します。

- ユーザー グループによってアクセスされるアプリケーションを許可またはブロックするには、アクセス コントロール ルールで**アプリケーション**条件を使用します。

  たとえば、契約業者グループのメンバーによる Facebook へのアクセスをブロックします。

注意 アクセス コントロール ルールを適切に設定しないと、ブロックする必要があるトラフィックを含め、予期しない結果が発生する可能性があります。一般的に、アプリケーション制御ルールは、たとえば IP アドレスに基づくルールよりも照合に時間がかかるため、アクセス コントロール リスト内の順位を低くする必要があります。

特定の条件 (ネットワークや IP アドレスなど) を使用するアクセス コントロール ルールは、一般的な条件 (アプリケーションなど) を使用するルールの前にオーダーする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および 3 (物理、データリンク、およびネットワーク) の条件を持つルールは、アクセス コントロール ルールで最初に注文する必要があります。レイヤ5、6、および 7 (セッション、プレゼンテーション、およびアプリケーション) の条件は、アクセス コントロール ルールの後で順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

次の表に、アクセス コントロール ルールを設定する方法の例を示します。

コントロールの種類	操作	ゾーン、ネットワーク、VLAN タグ	ユーザ	アプリケーション	ポート	URL	SGT/ISE 属性	インスペクション、ロギング、コメント
アプリケーションがポート（SSH など）を使用する場合の、安全性の高いネットワークから安全性の低いネットワークへのアプリケーション	お客様の選択（この例では [許可（Allow）]）	外部インターフェイスを使用する宛先ゾーンまたはネットワーク	任意	設定しない	使用可能なポート：**SSH** [選択した宛先ポート（Selected Destination Port）] に追加	任意	ISE/ISE-PIC でのみ使用。	任意

コントロールの種類	操作	ゾーン、ネットワーク、VLANタグ	ユーザ	アプリケーション	ポート	URL	SGT/ISE 属性	インスペクション、ロギング、コメント
アプリケーションがポートを使用していない場合の（ICMP など）、安全性の高いネットワークから安全性の低いネットワークへのアプリケーション	お客様の選択（この例では [許可（Allow）]）	外部インターフェイスを使用する宛先ゾーンまたはネットワーク	任意	設定しない	選択された宛先ポート プロトコル：**ICMP** **タイプ**：**Any**	設定しない	ISE/ISE-PIC でのみ使用。	任意
ユーザー グループによるアプリケーション アクセス	お客様の選択（この例では [ブロック（Block）]）	お客様の選択	ユーザー グループ（この例では契約業者 グループ）を選択。	アプリケーションの名前（この例では [Facebook]）を選択。	設定しない	設定しない	ISE/ISE-PIC でのみ使用。	お客様の選択

アプリケーションの特性

システムは、次の表に示す基準を使用して、検出された各アプリケーションの特性を判別します。これらの特性をアプリケーション フィルタとして使用します。

表 *3:* アプリケーションの特性

特性	説明	例
タイプ	アプリケーションプロトコルは、ホスト間の通信を意味します。 クライアントは、ホスト上で動作しているソフトウェアを意味します。 Web アプリケーションは、HTTP トラフィックの内容または要求された URL を意味します。	HTTP と SSH はアプリケーション プロトコルです。 Web ブラウザと電子メール クライアントはクライアントです。 MPEG ビデオと Facebook は Web アプリケーションです。
リスク（Risk）	アプリケーションが組織のセキュリティ ポリシーに違反することがある目的で使用される可能性。	ピアツーピア アプリケーションはリスクが極めて高いと見なされます。
ビジネスとの関連性（Business Relevance）	アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。	ゲーム アプリケーションはビジネスとの関連性が極めて低いと見なされます。
カテゴリ（Category）	アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。	Facebook はソーシャル ネットワーキングのカテゴリに含まれます。
タグ（Tag）	アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。	ビデオ ストリーミング Web アプリケーションには、ほとんどの場合、`high bandwidth` と `displays ads` というタグが付けられます。

用途別の注意事項と制限事項

- Office 365 管理者用ポータル：

  制限：アクセス ポリシーのロギングが最初と最後で有効になっている場合、最初のパケットは Office 365 として検出され、接続の終了は Office 365 管理者用ポータルとして検出されます。これがブロッキングに影響を与えないようにする必要があります。

- Skype:

  アプリケーション制御に関する推奨事項 （13 ページ）を参照してください

- GoToMeeting

GoToMeeting を完全に検出するには、ルールに次のすべてのアプリケーションが含まれている必要があります。

- GoToMeeting
- Citrix Online
- Citrix GoToMeeting プラットフォーム
- LogMeIn
- STUN

- Zoho:

  アプリケーション制御に関する推奨事項 （13 ページ）を参照してください

- Bittorrent、Tor、Psiphon、および Ultrasurf などの回避的なアプリケーションの場合：

  回避的なアプリケーションの場合、デフォルトでは、信頼性の高いシナリオのみが検出されます。このトラフィックに対するアクション（ブロックや QoS の実装など）を実行する必要がある場合、より効果の高い、さらに積極的な検出の設定が必要なことがあります。これを実行する場合、設定の変更によって誤検出が発生する可能性がありますので、TAC に問い合わせて設定を確認してください。

- WeChat：

  WeChat を許可する場合、WeChat のメディアを選択的にブロックすることはできません。

- RDP（Remote Desktop Protocol）：

  RDP アプリケーションを許可してもファイル転送が許可されない場合は、RDP のルールに TCP と UDP の両方のポート 3389 が含まれていることを確認してください。RDP ファイル転送では UDP が使用されます。

アクセス制御ルールのベストプラクティス

ルールを適切に設定して順序付けることは、効果的な導入を確立する上で不可欠な要素です。次のトピックでは、ルールのパフォーマンスに関するガイドラインを要約します。

（注） 設定の変更を展開すると、システムはすべてのルールをまとめて評価し、ターゲットデバイスでネットワークトラフィックを評価するために使用する拡張基準セットを作成します。それらの基準がターゲット デバイスのリソース（物理メモリ、プロセッサなど）を上回っている場合、そのデバイスに展開することはできません。

アクセス制御の一般的なベストプラクティス

次の要件と一般的なベストプラクティスを確認してください。

- プレフィルタポリシーを使用して、不要なトラフィックを早期にブロックし、アクセス制御インスペクションの恩恵を受けないトラフィックを高速パスします。詳細については、「Fastpath プレフィルタリングのベストプラクティス」を参照してください。
- 展開のライセンスを取得せずにシステムを設定することはできますが、多くの機能では、展開する前に適切なライセンスを有効にする必要があります。
- アクセス制御ルールは、デバイスのアクセス制御リストとして展開されます。アクセス制御ルールごとに作成されるアクセス制御エントリの数を最小限に抑え、全体的なパフォーマンスを向上させるには、各デバイスのオブジェクトグループ検索を有効にします。オブジェクトグループ検索はデバイス設定であり、アクセス制御ポリシー設定ではないため、各デバイスを編集して機能を有効にする必要があります。詳細については、「オブジェクトグループ検索の構成」を参照してください。
- アクセス コントロール ポリシーを展開しても、そのルールは既存の接続に適用されません。既存の接続のトラフィックは、展開された新しいポリシーによってバインドされません。また、ポリシーヒットカウントは、ポリシーに一致する接続の最初のパケットに対してのみ増加します。したがって、ポリシーに一致する可能性がある既存の接続のトラフィックは、ヒットカウントから除外されます。ポリシールールを効果的に適用するには、既存の接続セッションをクリアしてからポリシーを展開します。
- 可能な限り、複数のネットワークオブジェクトを1つのオブジェクトグループに結合します。複数のオブジェクトを（送信元または宛先を個別に）選択すると、システムは（展開時に）オブジェクトグループを自動的に作成します。既存のグループを選択すると、オブジェクトグループの重複を回避し、多数の重複オブジェクトがある場合の CPU 使用率への潜在的な影響を軽減できます。
- システムがトラフィックに影響を与えるためには、ルーテッド、スイッチド、トランスペアレント インターフェイスまたはインライン インターフェイスのペアを使用して関連する設定を管理対象デバイスに展開する必要があります。

  場合によっては、タップ モードのインライン デバイスを含むパッシブに展開されたデバイスにインライン設定を展開することがシステムによって阻害されます。

  それ以外の場合、ポリシーは正常に展開されますが、パッシブに展開されたデバイスを使用してトラフィックのブロックや変更を試みると、予期しない結果になる可能性があります。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。
- URL フィルタリング、アプリケーション検出、レート制限、インテリジェントアプリケーションバイパスなどの特定の機能では、システムがトラフィックを識別するために、一部のパケットの通過を許可する必要があります。

  これらのパケットが検査されずに接続先に到達しないようにするには、トラフィック識別の前に通過するパケットを処理するためのベストプラクティスおよびトラフィック識別の前に通過するパケットを処理するためのポリシーの指定を参照してください。
- アクセス コントロール ポリシーのデフォルトアクション で処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません。

- 一部の機能は、特定のデバイスモデルでのみ使用できます。サポートされていない機能は、警告アイコンおよび確認ダイアログ ボックスに示されます。
- syslog またはストアイベントを外部で使用する場合は、ポリシー名やルール名などのオブジェクト名に特殊文字を使用しないでください。オブジェクト名には、カンマなどの特殊文字を含めることはできません。受信側アプリケーションで区切り文字として使用される可能性があります。
- デフォルトアクションで処理される接続のロギングは、初期設定では無効ですが、有効にすることもできます。
- アクセスコントロールルールを作成、順序付け、および実装するためのベストプラクティスについては、アクセス制御ルールのベストプラクティス （20 ページ） およびサブトピックを参照してください。

順序付けルールのベストプラクティス

一般的なガイドライン：

- 通常、すべてのトラフィックに適用する必要がある最優先順位のルールはポリシーの先頭近くに配置します。
- 固有のルールは一般的なルールの前に来る必要があります（特に特定のルールが一般的なルールの例外である場合）。

  そうしないと、トラフィックはまず一般ルールに一致し、適用する特定のルールにヒットしません。
- レイヤ 3/4 基準（IP アドレス、セキュリティゾーン、ポート番号など）のみに基づいてトラフィックをドロップするルールはできるだけ上に配置する必要があります。これらの基準に基づくルールでは、一致する接続を識別するための検査は必要ありません。
- 可能な限り、固有のドロップルールはポリシーの最上位近くに配置します。これにより、望ましくないトラフィックへの可能な限り早期の決定が保証されます。
- URL フィルタリング、アプリケーションベース、地理位置情報ベースのルール、および検査が必要なその他のルールは、レイヤ 3/4 基準（IP アドレス、セキュリティゾーン、ポート番号など）のみに基づいてトラフィックをドロップするルールの後（ただしファイルポリシーと侵入ポリシーを指定するルールの前）に配置する必要があります。
- URL フィルタリングルールをアプリケーションルールの上に配置し、アプリケーションルールの後にマイクロ アプリケーション ルールと Common Industrial Protocol（CIP）の下位分類アプリケーション フィルタリング ルールを続けます。
- ファイルポリシーと侵入ポリシーを指定するルールは、ルールの順序の最後に配置する必要があります。これらのルールに関しては、リソースを大量に消費する詳細な検査が必要です。パフォーマンス上の理由から、詳細な検査が必要とされる潜在的な脅威の数を最小限に抑えるために、最初はそれほどリソースを消費しない方法で可能な限り多くの脅威を排除する必要があります。

• 常に、ルールを組織のニーズに適した順序に配置する必要があります。

上記のガイドラインの例外と補足事項は、以下のセクションに記載されています。

ルールのプリエンプション

ルールのプリエンプションが発生するのは、評価する順番が前のルールがトラフィックと一致するために、その後のルールが全くトラフィックと一致しない場合です。ルールの条件により、そのルールが他のルールをプリエンプション処理するかどうかが決まります。次の例では、最初のルールが管理トラフィックを許可するため、2 番目のルールがそのトラフィックをブロックできません。

アクセス コントロール ルール 1：管理ユーザを許可
アクセス コントロール ルール 2：管理ユーザをブロック

どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。次の例では、最初の SSL ルールでの VLAN 範囲に 2 番目のルールでの VLAN が含まれるため、最初のルールが 2 番目のルールをプリエンプション処理します。

SSL ルール 1：VLAN 22 ～ 33 を復号しない
SSL ルール 2：VLAN 27 をブロック

次の例では、VLANが設定されていないルール1はあらゆるVLANと一致します。そのため、ルール 1 がルール 2 をプリエンプション処理し、ルール 2 での VLAN 2 の照合は行われません。

アクセス コントロール ルール 1：送信元ネットワーク 10.4.0.0/16 を許可
アクセス コントロール ルール 2：送信元ネットワーク 10.4.0.0/16、VLAN 2 を許可

あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールがプリエンプション処理されます。

QoS ルール 1: VLAN 1 URL www.netflix.com をレート制限
QoS ルール 2: VLAN 1 URL www.netflix.com をレート制限

条件が 1 つでも異なる場合は、後続のルールがプリエンプション処理されることはありません。

QoS ルール 1: VLAN 1 URL www.netflix.com をレート制限
QoS ルール 2: VLAN 2 URL www.netflix.com をレート制限

例：プリエンプションを避けるための SSL ルールの順序付け

ここで1つのシナリオとして、信頼できるCA（GoodCA）が悪意のあるエンティティ（Bad CA）に間違って CA 証明書を発行してしまい、その証明書を取り消していない状況を考えてみましょう。信頼できない CA によって発行された証明書で暗号化されたトラフィックは SSL ポリシーを使用してブロックしたいものの、信頼できる CA の信頼チェーン内にあるそれ以外のトラフィックは許可したいとします。CA証明書とすべての中間 CA 証明書をアップロードした後、ルールを以下の順序で設定した SSL ポリシーを構成します。

SSL ルール 1：発行元 CN=www.badca.com をブロック
SSL ルール 2：発行元 CN=www.goodca.com を復号しない

上記のルールを逆の順序にすると、不正な CA で信頼されたトラフィックを含め、正当な CA で信頼されたすべてのトラフィックが最初に一致することになります。どのトラフィックも後続の不正な CA ルールに一致しないため、悪意のあるトラフィックはブロックされずに許可される可能性があります。

ルールのアクションとルールの順序

ルールのアクションによって、一致したトラフィックの処理方法が決まります。パフォーマンスを向上させるには、リソースを集約的に使用するルールを実行する前に、トラフィックの追加処理を実行または保証しないルールを配置してください。これにより、システムはさらに検査する必要のあるトラフィックだけを転送できます。

以下の例は、一連のルールがすべて同等に重要であり、プリエンプションが問題にならない場合に、さまざまなポリシーでルールを順序付ける方法を示しています。

ルールにアプリケーション条件が含まれている場合は、アプリケーション制御の設定のベストプラクティス （16 ページ）も参照してください。

最適な順序：復号 ルール

復号にはリソースが必要になるだけでなく、復号後のトラフィックの分析も必要になります。トラフィックを復号するルールは最後に配置します。

（注） 特定の管理対象デバイスはハードウェアの TLS/SSL トラフィックの暗号化と復号をサポートしているため、パフォーマンスが大幅に向上します。詳細については、TLS 暗号化アクセラレーションを参照してください。

1. [モニター（Monitor）]：一致する接続をログに記録するだけで、トラフィックに対して他のアクションは実行しないルール。
2. [ブロック（Block）]、[リセットしてブロック（Block with reset）]：それ以上のインスペクションを行わずにトラフィックをブロックするルール。
3. [復号しない（Do not decrypt）]：暗号化トラフィックを復号しないまま、暗号化セッションをアクセス コントロール ルールに渡すルール。これらのセッションのペイロードにディープ インスペクションは適用されません。
4. [復号 - 既知のキー（Decrypt - Known Key）]：既知の秘密キーを使用して着信トラフィックを復号するルール。
5. [復号 - 再署名（Decrypt - Resign）]：サーバ証明書に再署名することによって発信トラフィックを復号するルール。

最適な順序：アクセス コントロール ルール

複数のカスタム侵入ポリシーと変数セットを使用している場合は特に、侵入、ファイル、マルウェアのインスペクションにリソースが必要です。したがって、ディープインスペクションを呼び出すアクセス コントロール ルールを最後に配置します。

1. [モニター（Monitor）]：一致する接続をログに記録するだけで、トラフィックに対して他のアクションは実行しないルール。ただし、重要な例外と注意事項をアクセス コントロール ルールのモニター アクションで確認してください。
2. [信頼（Trust）]、[ブロック（Block）]、[リセットしてブロック（Block with reset）]：それ以上のインスペクションを行わずにトラフィックを処理するルール。信頼できるトラフィックは、アイデンティティ ポリシーが課す認証要件、およびレート制限の対象となることに注意してください。
3. [許可（Allow）]、[インタラクティブ ブロック（ディープ インスペクションなし）（Interactive Block (no deep inspection)）]：それ以上のインスペクションを行わずにトラフィックのディスカバリを許可するルール。許可されるトラフィックは、アイデンティティ ポリシーが課す認証要件、およびレート制限の対象となることに注意してください。
4. [許可（Allow）]、[インタラクティブ ブロック（ディープ インスペクションあり）（Interactive Block (deep inspection)）]：禁止されているファイル、マルウェア、エクスプロイトのディープ インスペクションを実行するファイル ポリシーまたは侵入ポリシーに関連付けられているルール。

アプリケーション ルールの順序

アプリケーション条件を使用するルールは、ルールのリストでより低い順序に移動すると、トラフィックに一致する可能性が高くなります。

特定の条件 (ネットワークや IP アドレスなど) を使用するアクセス コントロール ルールは、一般的な条件 (アプリケーションなど) を使用するルールの前にオーダーする必要があります。オープン システム相互接続（OSI）モデルに精通している場合は、考え方として同様の順位付けを使用してください。レイヤ1、2、および 3 (物理、データリンク、およびネットワーク) の条件を持つルールは、アクセス コントロール ルールで最初に注文する必要があります。レイヤ5、6、および 7 (セッション、プレゼンテーション、およびアプリケーション) の条件は、アクセス コントロール ルールの後で順序付けする必要があります。OSI モデルの詳細については、こちらの Wikipedia の記事を参照してください。

詳細と例については、アプリケーション制御の設定のベストプラクティス （16 ページ）およびアプリケーション制御に関する推奨事項 （13 ページ）を参照してください。

URL ルールの順序

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。

- 検査対象のトラフィックが暗号化されている。

ルールに例外を設定する場合は、例外を他のルールの上に配置してください。

ルールの簡素化および絞り込みのベストプラクティス

簡素化：設定しすぎない

個々のルール条件を最小化します。できる限り少ない個々の要素をルールの条件に使用します。たとえば、ネットワーク条件では、個々の IP アドレスではなく IP アドレス ブロックを使用します。

処理するトラフィックの照合が 1 つの条件で十分な場合には、2 つの条件を使用しないでください。冗長な条件を使用すると、展開される設定が大幅に拡張される可能性があります。それにより、デバイスのパフォーマンスに関する問題が発生したり、クラスタおよび高可用性ユニットの再参加において予期しないデバイス動作が発生する場合があります。次に例を示します。

- 複数のインターフェイスを表すセキュリティゾーンは、慎重に使用してください。送信元ネットワークと宛先ネットワークを条件として指定し、これらが、ターゲットのトラフィックに十分に一致する場合は、セキュリティゾーンを指定する必要はありません。
- たとえば、一連の内部インターフェイスをインターネット上の「任意」の宛先と照合する場合は、単に、それらの内部インターフェイスを含む送信元セキュリティゾーンを使用します。ネットワークまたは宛先インターフェイスの基準は必要ありません。

要素をオブジェクトに組み合わせても、パフォーマンスは向上**しません**。たとえば、50 個の IP アドレスを 1 つのネットワーク オブジェクトに含めて使用することにパフォーマンス的なメリットはなく、条件にこれらの IP アドレスを個別に含めるよりも単に構成上のメリットがあるだけです。

アプリケーション検出の推奨事項については、アプリケーション制御の設定のベストプラクティス （16 ページ）を参照してください。

絞り込み：特にインターフェイスによってリソース消費ルールを絞り込んで制約する

できる限り、ルールの条件を使用してリソース消費ルールが処理するトラフィックを絞り込んで定義します。絞り込まれたルールは、広範な条件を持つルールが多様なタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンプション処理できるという理由からも重要です。以下は、リソース消費ルールの例です。

- トラフィックを復号する TLS/SSL ルール：復号だけでなく、復号されたトラフィックの更なる分析にもリソースが必要です。絞り込みを細かくし、また可能な場合は、暗号化トラフィックをブロックするか、復号しないようにします。

  Threat Defense モデルではハードウェアで TLS/SSL 暗号化および復号が実行されます。これによりパフォーマンスが大きく向上します。詳細については、TLS 暗号化アクセラレーションを参照してください。

- ディープ インスペクションを呼び出すアクセス コントロール ルール：特に複数のカスタム侵入ポリシーと変数セットを使用している場合、侵入ファイルやマルウェアのインスペクションにはリソースが必要です。ディープインスペクションは必要な場所でのみ呼び出されることを確認してください。

最大のパフォーマンスによるメリットを得るため、インターフェイスによってルールを制約します。ルールがデバイスのすべてのインターフェイスを除外する場合、そのルールはそのデバイスのパフォーマンスに影響しません。

アクセス制御ルールと侵入ポリシーの最大数

ターゲットデバイスでサポートされるアクセス制御ルールまたは侵入ポリシーの最大数は、ポリシーの複雑性、物理メモリ、デバイスのプロセッサ数などの、多くの要因によって異なります。

デバイスでサポートされる最大を超えるとアクセス コントロール ポリシーは展開できず、再評価する必要があります。

侵入ポリシーのガイドライン：

- アクセス コントロール ポリシーでは、1 つの侵入ポリシーを各許可ルール、インタラクティブ ブロック ルール、およびデフォルト アクションと関連付けることができます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーと見なされます。
- いくつかの侵入ポリシーまたは変数セットを統合すると、複数のアクセス コントロール ルールに1つの侵入ポリシーと変数セットのペアを関連付けることができます。一部のデバイスでは、すべての侵入ポリシーに関して1つの変数セットだけを使用できる場合や、デバイス全体でただ 1 つの侵入ポリシー/変数セット ペアだけを使用できる場合があります。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。