アクセス コントロール ルール

次の各トピックでは、アクセス コントロール ルールの設定方法について説明します。

アクセス コントロール ルール

アクセス コントロール ポリシー内では、アクセス コントロール ルールによって複数の管理対象デバイスでネットワーク トラフィックを処理するきめ細かい制御方法が提供されます。

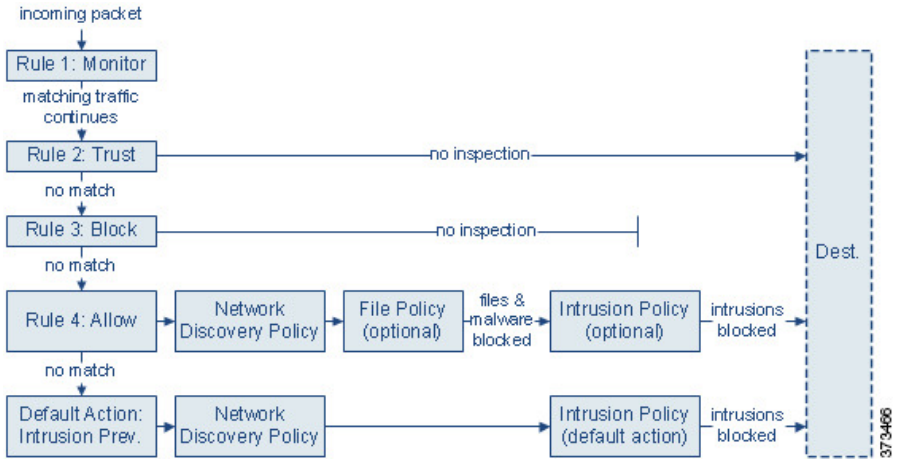
（注） アクセス制御ルールがネットワークトラフィックを評価する前に、セキュリティインテリジェンスのフィルタ処理、暗号解読、ユーザーの識別、および一部の復号と前処理が行われます。

システムは、指定した順にアクセス コントロール ルールをトラフィックと照合します。ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。

また、各ルールにはアクションがあり、これによって一致するトラフィックをモニター、信頼、ブロック、または許可するかを決定します。トラフィックを許可するときは、システムが侵入ポリシーまたはファイルポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

次のシナリオでは、インラインの侵入防御展開環境で、アクセス コントロール ルールによってトラフィックを評価できる方法を要約しています。

アクセス コントロール ルール



このシナリオでは、トラフィックは次のように評価されます。

- **ルール 1**：**モニタ**はトラフィックを最初に評価します。モニタールールはネットワークトラフィックを追跡してログに記録します。システムはトラフィックと追加ルールの照合を継続して、許可するか拒否するかを決定します（ただし、重要な例外と注意事項をアクセス コントロール ルールの監視アクション （7 ページ）で確認してください）。
- **ルール 2**：**信頼**はトラフィックを 2 番目に評価します。一致するトラフィックは追加のインスペクションなしで宛先まで通過することが許可されますが、引き続きアイデンティティの要件とレート制限の対象となります。一致しないトラフィックは、引き続き次のルールと照合されます。
- **ルール 3**：**ブロック**はトラフィックを 3 番目に評価します。一致するトラフィックは、追加のインスペクションなしでブロックされます。一致しないトラフィックは、引き続き最後のルールと照合されます。
- **ルール 4**：**許可**は最後のルールです。このルールの場合、一致したトラフィックは許可されますが、トラフィック内の禁止ファイル、マルウェア、侵入、エクスプロイトは検出されてブロックされます。残りの禁止されていない悪意のないトラフィックは宛先まで通過することが許可されますが、引き続きアイデンティティの要件とレート制限の対象となります。ファイルインスペクションのみを実行する、または侵入インスペクションのみを実行する、もしくは両方とも実行しない許可ルールを設定できます。
- **デフォルト アクション**は、いずれのルールにも一致しないすべてのトラフィックを処理します。このシナリオでは、デフォルトアクションは、悪意のないトラフィックの通過を許可する前に侵入防御を実行します。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を割り当てることもあります。（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。）

アクセス コントロール ルールまたはデフォルト アクションによって許可したトラフィックは、自動的にホスト、アプリケーション、およびユーザ データについてネットワーク検出ポリシーによるインスペクションの対象になります。検出は明示的には有効にしませんが、拡張したり無効にしたりすることができます。ただし、トラフィックを許可することで、検出データの収

集が自動的に保証されるものではありません。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。また、アプリケーション検出は、暗号化されたセッションに限定されます。

暗号化されたトラフィックの通過が暗号解読設定で許可される場合、または暗号解読が設定されていない場合は、そのトラフィックがアクセスコントロールルールによって処理されることに注意してください。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、暗号化ペイロードの侵入およびファイル検査を、システムは無効化します。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。

アクセス コントロール ルールの管理

アクセス コントロール ポリシー エディタの [ルール（Rules）] タブでは、現在のポリシー内のアクセスコントロールルールの追加、編集、分類、検索、フィルタ処理、移動、有効化、無効化、削除、その他の管理が行えます。

アクセス コントロール ルールの適切な作成と順序付けは複雑なタスクですが、効果的な展開を構築するためには不可欠です。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、追加のライセンスが必要となったり、ルールに無効な設定が含まれる場合があります。システムが想定どおりにトラフィックを確実に処理できるように、アクセス コントロール ポリシー インターフェイスにはルールに対する強力な警告およびエラーのフィードバック システムがあります。

検索バーを使用して、アクセス コントロール ポリシー ルールのリストをフィルタ処理します。[一致するルールのみを表示（Show Only Matching Rules）] オプションの選択を解除して、すべてのルールを表示できます。一致したルールが強調表示されます。

ポリシー エディタでは、各アクセス コントロール ルールに対してルールの名前、条件の概要、ルール アクションが表示され、さらにルールのインスペクション オプションや状態を示すアイコンが表示されます。各アイコンの意味は次のとおりです。

- **Time Range Option** ( )
- **Intrusion policy** ( )
- **File policy** ( )
- **Logging** ( )
- **Warning** ( )
- **Errors** ( )
- **Rule Conflict** ( )

無効なルールはグレー表示され、ルール名の後に [無効（disabled）] というマークが付きます。

ルールを作成または編集するには、アクセス コントロール ルールの作成および編集 （28 ページ） を参照してください。

ヒント　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。

関連トピック

アクセス制御ルールのコンポーネント （4 ページ）
アクセス コントロール ルールのベストプラクティス （21 ページ）

アクセス制御ルールのコンポーネント

一意の名前に加え、各アクセス コントロール ルールには次の基本コンポーネントがあります。

状態（State）

デフォルトでは、ルールは有効になっています。ルールを無効にすると、システムはそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置（Position）

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。ポリシー継承を使用する場合、ルール 1 は再外部ポリシーの 1 番目のルールです。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

また、ルールはセクションおよびカテゴリに属していることがあります。これは、単に整理のためであり、ルールの位置に影響しません。ルールの位置は、すべてのセクションとカテゴリにまたがって設定されます。

セクションおよびカテゴリ

アクセス コントロール ルールの整理に役立つように、アクセス コントロール ポリシーには、システムで用意されている 2 つのルール セクションとして「必須（Mandatory）」と「デフォルト（Default）」があります。アクセス コントロール ルールをさらに細かく整理するため、「必須（Mandatory）」セクション内と「デフォルト（Default）」セクション内にカスタム ルール カテゴリを作成することができます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須（Mandatory）」セクションと「デフォルト（Default）」セクションの間にネストされます。

条件

条件は、ルールが処理する特定のトラフィックを指定します。条件には単純なものと複雑なものがあり、ライセンスによって用途が異なります。

トラフィックは、ルールで指定されたすべての条件を満たす必要があります。たとえば、アプリケーション条件で HTTP が指定されていて、HTTPS は指定されていない場合、URL カテゴリとレピュテーションの条件は、HTTPS トラフィックには適用されません。

適用時間

ルールの運用中の日数と時間を指定できます。

操作（Action）

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。一致したトラフィックをモニター、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。信頼できるトラフィック、ブロックされたトラフィック、または暗号化されたトラフィックに対しては、詳細な検査は実行されません。

インスペクション（Inspection）

詳細検査オプションは、悪意のあるトラフィックをどのように検査してブロックし、それ以外のものは許可するかを決定します。ルールを使用してトラフィックを許可するときは、システムが侵入ポリシーまたはファイルポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出たりする前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

ログ

ルールのロギング設定によって、システムが記録する処理済みトラフィックのレコードを管理します。1 つのルールに一致するトラフィックのレコードを 1 つ保持できます。一般的に、接続の開始時または終了時（あるいは、その両方）にセッションをログに記録できます。接続のログは、データベースの他に、システム ログ（Syslog）または SNMP トラップ サーバに記録できます。

説明

アクセス コントロール ルールで変更を保存するたびに、コメントを追加できます。

関連トピック

アクセス コントロール ルールのベストプラクティス （21 ページ）
アクセス コントロール ルールの管理 （3 ページ）
アクセス コントロール ルールの作成および編集 （28 ページ）
アクセス コントロール ルールのアクション （7 ページ）
アクセス コントロール ルール条件 （30 ページ）
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 （10 ページ）
アクセス コントロール ルールのコメント

アクセス コントロール ルールの順序

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で先頭から順にアクセス コントロール ルールをトラフィックと照合します。

ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセスコントロールルールに従ってネットワーク トラフィックを処理します。モニタールールを除いて、トラフィックがルールに一致した後、システムは優先度の低い追加のルールに対してトラフィックの評価は続行しません。

アクセス コントロール ルールの整理に役立つように、アクセス コントロール ポリシーには、システムで用意されている 2 つのルール セクションとして「必須（Mandatory）」と「デフォルト（Default）」があります。さらに細かく整理するため、「必須（Mandatory）」セクション内や「デフォルト（Default）」セクション内にカスタム ルール カテゴリを作成することができます。カテゴリは、作成した後に移動することはできません。ただし、カテゴリを削除または名前変更したり、ルールをカテゴリ内またはカテゴリ間で移動したりすることはできます。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

ポリシーの継承を使用する場合、現在のポリシーのルールは、その親ポリシーの「必須（Mandatory）」ルール セクションと「デフォルト（Default）」ルール セクションの間にネストされます。ルール 1 は、現在のポリシーではなく、最外部ポリシーの 1 番目のルールです。ルールの番号は、すべてのポリシー、セクション、カテゴリにまたがって割り当てられます。

アクセス コントロール ポリシーの変更を許可する定義済みユーザ ロールによって、ルールのカテゴリ内またはカテゴリ間でアクセス コントロール ルールを移動および変更することもできます。しかし、ユーザがルールを移動および変更することを制限するには、カスタム ロールを作成できます。アクセスコントロールポリシーの変更権限が割り当てられているユーザは、制限なく、カスタム カテゴリにルールを追加することや、カテゴリ内のルールを変更することができます。

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。

ヒント　アクセス コントロール ルールの順序を適切に設定することで、ネットワーク トラフィック処理に必要なリソースを削減して、ルールのプリエンプションを回避できます。ユーザーが作成するルールはすべての組織と展開に固有のものですが、ユーザーのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。具体的なヒントについては、順序付けルールのベスト プラクティス を参照してください。

アクセス コントロール ルールのアクション

アクセス コントロール ルールには、システムが一致するトラフィックをどのように処理し、ロギングするのかを指定するアクションがあります。モニター、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。

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、モニター以外のアクションをもつどのアクセスコントロールルールの条件にも一致しないトラフィックを処理します。

アクセス コントロール ルールの監視アクション

[Monitor] アクションは、トラフィックを許可または拒否するように設計されていません。むしろ、その主な目的は、一致するトラフィックが最終的にどのように処理されるかに関係なく、接続ロギングを強制することです。

接続がモニタールールに一致する場合、接続が一致する次の非モニタールールがトラフィック処理とそれ以降のインスペクションを決定する必要があります。さらに一致するルールがない場合、システムはデフォルトアクションを使用する必要があります。

ただし、例外があります。モニタールールにレイヤ7の条件（アプリケーション条件など）が含まれている場合、そのシステムでは早期パケットを通過させ、接続を確立（またはSSLハンドシェイクの完了）することができます。これは、接続が後続のルールによってブロックされる必要がある場合でも発生します。これらの早期パケットが後続のルールに対して評価されないためです。こうしたパケットが完全に検査されていない宛先に到達しないように、アクセスコントロールポリシーの詳細設定で、このための侵入ポリシーを指定できます。トラフィック識別の前に通過するパケットのインスペクションを参照してください。システムはレイヤ7の識別を完了した後、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。

アクセス コントロール ルールの信頼アクション

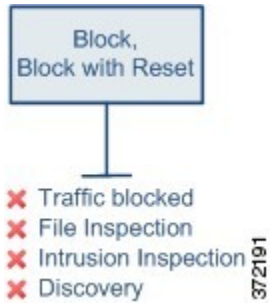
[信頼（Trust）] アクションは、ディープ インスペクションやネットワーク検出をせずにトラフィックを通過させます。信頼処理されたトラフィックも、ID 条件およびレート制限の対象です。

（注）

- FTP や SIP などの一部のプロトコルは、検査プロセスを通じてシステムが開くセカンダリチャネルを使用します。場合によっては、信頼できるトラフィックがすべての検査をバイパスでき、これらのセカンダリチャネルを適切に開くことができません。この問題が発生した場合は、信頼ルールを [許可（Allow）] に変更します。
- ロギング オプションが無効になっている信頼ルールの場合、フロー終了イベントは引き続きシステムで生成されます。ただし、イベントはイベントページには表示されません。
- アクセス コントロール ルールは復号などの他のポリシーの後に評価されるため、接続が信頼されていてもインスペクションなしで高速パスされるとは限りません。たとえば、接続が、復号を必要とする復号ルールと信頼できるアクセス制御ルールの両方に一致する場合、その接続は、信頼ルールによって許可される前に、必要に応じて復号化および検査されます。信頼とは、侵入インスペクションなどの追加のインスペクションが適用されないことを意味します。インスペクションのない接続を許可する場合は、プレフィルタ ポリシーを使用して接続を高速パス処理するか、他のポリシーが接続にインスペクション サービスを適用しないようにします。

アクセス コントロール ルールのブロック アクション

ブロック アクションおよび**リセットしてブロック** アクションはトラフィックを拒否し、いかなる追加のインスペクションも行われません。



[HTTP 応答（HTTP response）] ページに一致する Web 要求を除き、リセット ルールを持つブロックが接続をリセットします。これは、システムが Web 要求をブロックするときに表示されるように設定した応答ページは、接続がすぐにリセットされた場合は表示できないためです。

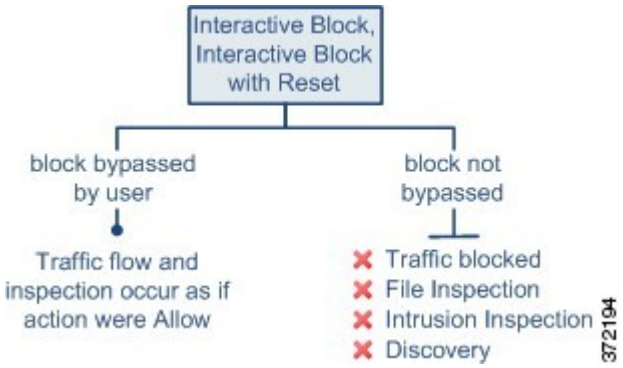
詳細については、「HTTP 応答ページの設定」を参照してください。

関連トピック

HTTP 応答ページの設定

アクセス コントロール ルールのインタラクティブ ブロッキング アクション

[インタラクティブブロック（Interactive Block）] と [リセット付きインタラクティブブロック（Interactive Block with reset）] アクションにより、Web ユーザーは目的の宛先に進む選択肢が与えられます。



ユーザーがブロックをバイパスしている場合、ルールは許可ルールを模倣します。したがって、インタラクティブ ブロック ルールをファイル ポリシーと侵入ポリシーに関連付けることができるため、一致するトラフィックもネットワーク検出の対象となります。

ユーザーがブロックをバイパスしない（できない）場合は、ルールはブロック ルールを模倣します。一致するトラフィックは、追加のインスペクションなしで拒否されます。

インタラクティブブロックを有効にした場合は、ブロックされているすべての接続をリセットできません。これは、接続がすぐにリセットされた場合は応答ページを表示できないためです。[リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションを（非インタラクティブに）Web 以外のすべてのトラフィックをリセットしてブロックしても、Web 要求についてはインタラクティブ ブロックは有効になっています。

詳細については、「HTTP 応答ページの設定」を参照してください。

関連トピック

Decryption ruleのブロック アクション

アクセス コントロール ルールの許可アクション

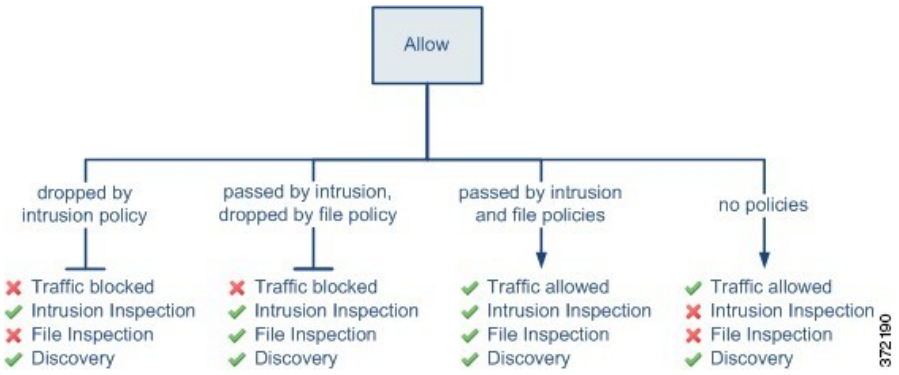
[許可（Allow）] アクションは、一致するトラフィックを通過させます。ただし、引き続き ID 条件およびレート制限の対象となります。

任意で、ディープインスペクションを行い、トラフィックが接続先に到達する前に暗号化されていないトラフィックや復号されたトラフィックを検査、ブロックすることも可能です。

- 侵入ポリシーでは、侵入検知と防御設定に応じてネットワーク トラフィックを分析し、設定内容に応じて違反パケットをドロップすることが可能です。

- ファイルポリシーでは、ファイルの制御ができます。ファイル制御により、ユーザーが特定のアプリケーション プロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。
- ネットワークベースの高度なマルウェア保護（AMP）もファイル ポリシーを使用して実行できます。マルウェア防御はファイルのマルウェアを調べ、検出したマルウェアを設定に応じてブロックします。

下の図は、許可ルールの条件（またはユーザーによりバイパスされるインタラクティブブロック ルール）を満たすトラフィックに対して実行されるインスペクションの種類を示しています。侵入インスペクションの前にファイルインスペクションが行われることに注意してください。そこでブロックされたファイルに対しては、侵入関連のエクスプロイトについては検査されません。



シンプルにするために、この図では、侵入ポリシーとファイル ポリシーの両方がアクセス コントロール ルールに関連付けられている状態（またはどちらも関連付けられていない状態）のトラフィック フローを示しています。ただし、どちらか1つだけを設定することも可能です。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が決定します。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 ポリシーが決定します。

トラフィックが侵入ポリシーとファイルポリシーのどちらかによって検査またはドロップされるかどうかに関わらず、システムはネットワーク検出を使ってトラフィックを検査できます。ただし、トラフィックを許可しても、ディスカバリ検査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。また、アプリケーション検出は、暗号化されたセッションに限定されます。

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、「侵入防御について」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 マルウェア防御のためのファイル 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。

（注） デフォルトでシステムは、暗号化ペイロードの侵入検査とファイル検査を無効化します。これにより、暗号化された接続が、侵入検査とファイル検査が設定されたアクセス制御ルールに一致した際の誤検出を減らすため、パフォーマンスが向上されます。

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。

- アクセス コントロール ルール：侵入ポリシーの選択
- 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

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

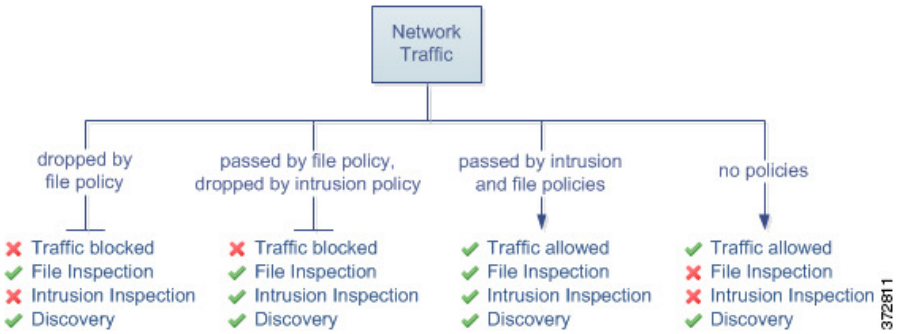
アクセス コントロール ポリシーで、複数の許可ルールとインタラクティブ ブロック ルールを異なる侵入ポリシーおよびファイル ポリシーに関連付けて、インスペクション プロファイルをさまざまなタイプのトラフィックに照合できます。

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。



アクセス制御ルールで処理されるすべての単一接続において、侵入検査の前にファイル検査が行われます。つまり、侵入のファイル ポリシーによってブロックされたファイルに対してシステムは検査を行いません。ファイル 検査では、ファイル タイプによるブロックが、マルウェア インスペクションおよびブロック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。

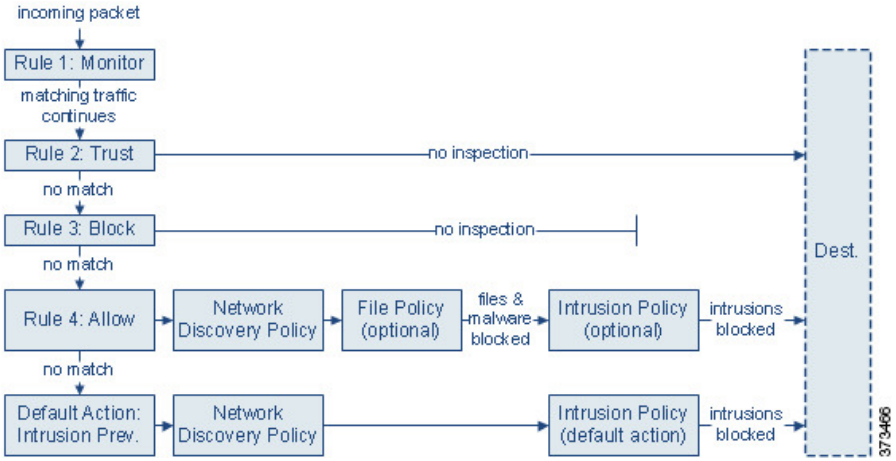
- まず、システムはファイル ポリシーで指定された単純なタイプ マッチングに基づいて、すべての実行可能ファイルのダウンロードをブロックします。これはすぐにブロックされるため、これらのファイルは、マルウェア インスペクションの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされた PDF に対するマルウェア クラウド ルックアップを実行します。マルウェアの性質を持つ PDF はすべてブロックされ、侵入インスペクションの対象にはなりません。

- 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） セッションでファイルが検出されブロックされるまで、そのパケットは侵入検査の対象となります。

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 ルールの監視アクション （7 ページ）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。

アクセス コントロール ルールの要件と前提条件

Model support

任意

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin
- カスタムユーザーロールを定義して、アクセス コントロール ポリシーおよびルールの侵入設定と、その他のアクセス コントロール ポリシーおよびルールを区別できます。これらのアクセス許可を使用すると、ネットワーク管理チームと侵入管理チームの責任を分離できます。アクセス コントロール ポリシーの変更権限を含む既存の事前定義されたユーザーロールは、すべてのサブ権限をサポートします。詳細な権限を適用する場合は、独自のカスタムロールを作成する必要があります。詳細な権限は次のとおりです。
  - **Policies** > **Access Control heading** > **Access Control** そして **[アクセスコントロールポリシー（Access Control Policy）]** > **[アクセスコントロールポリシーの変更（Modify Access Control Policy）]** > **[脅威設定の変更（Modify Threat Configuration）]**では、侵入ポリシー、変数セット、およびルール内のファイルポリシー、ネットワーク分析および侵入ポリシーの詳細オプションの設定、アクセス コントロール ポリシーのセキュリティ インテリジェンス ポリシーの構成、およびポリシーのデフォルト アクションの侵入アクションの選択を行えます。これ以外のオプションが表示されない場合、ユーザーはポリシーまたはルールの他の部分を変更できません。
  - [残りのアクセスコントロールポリシー設定の変更（Modify Remaining Access Control Policy Configuration）] は、ポリシーの他のすべての側面を編集する機能を制御します。

アクセスコントロールルールに関する注意事項と制限事項

- 現在のページに一度に表示できるルールは1000個までに制限されています。したがって、1つのカテゴリ内に3000のルールがあるなど、非常に多くのルールがある場合、カテゴリ内のすべてのルールを選択して削除するなどのアクションを実行しても、すべてのルール

は削除されません。対象のすべてのルールを削除するには、ルールを再度選択/削除することが必要な場合があります。

- 実際に使用されているアクセスコントロールルールを編集する場合、その変更は、展開時に確立されている接続には適用されません。更新されたルールは、将来の接続に対する照合に使用されます。ただし、システムが実際に接続を検査している場合（たとえば、侵入ポリシーを使用して）、変更された一致基準またはアクション基準が既存の接続に適用されます。

  Firewall Threat Defense の場合は、Firewall Threat Defense **clear conn** CLI コマンドを使用して確立されている接続を終了させることにより、現在のすべての接続に確実に変更を適用できます。後で接続の送信元が接続の再確立を試み、そのために新しいルールに対して適切に照合されることを前提として、これらの接続を終了しても問題がない場合にのみ、このような処理を行う必要があることに注意してください。

- アクセスルールのVLANタグは、インラインセットにのみに適用されます。このタグは、ファイアウォール インターフェイスに適用されるアクセスルールでは使用できません。

- 完全修飾ドメイン名（FQDN）ネットワークオブジェクトを送信元または宛先の基準として使用するには、プラットフォーム設定ポリシーでデータインターフェイスの DNS も設定する必要があります。システムは、アクセス制御ルールで使用されている FQDN オブジェクトのルックアップを実行するために管理 DNS サーバ設定を使用しません。

  FQDNによるアクセスの制御はベストエフォート型のメカニズムであることに注意してください。次の点を考慮してください。

  - 可能な限り、FQDNルールの代わりにセキュリティインテリジェンスまたはURLフィルタリングを使用します。
  - DNS応答はスプーフィングされる可能性があるため、完全に信頼できるDNSサーバーのみを使用します。
  - 一部のFQDNは、特に非常に人気の高いサーバーの場合、数千とはいかなくても、数百の IP アドレスを持つことがあり、それらが頻繁に変更されることがあります。システムはキャッシュされている DNS ルックアップの結果を使用するため、ユーザーはキャッシュに存在しないアドレスを取得する可能性があり、その接続はFQDNルールに合致しません。FQDN ネットワークオブジェクトを使用するルールは、100 未満のアドレスに解決される名前に対してのみ効果的に機能します。

    100 を超えるアドレスに解決される FQDN のネットワーク オブジェクト ルールを作成しないことを推奨します。接続のアドレスが解決され、デバイスのDNSキャッシュで使用可能である可能性は低いからです。このような場合は、FQDNネットワーク オブジェクト ルールの代わりに URL ベースのルールを使用します。

  - 人気のある FQDN では、異なる DNS サーバが異なるセットの IP アドレスを返す場合があります。したがって、ユーザが設定したものとは異なる DNS サーバを使用している場合、FQDNベースのアクセス制御ルールがクライアントで使用されているサイトのすべての IP アドレスに適用されないことがあり、ルールで意図した結果が得られません。

- 一部の FQDN DNS エントリには、非常に短い存続可能時間（TTL）値が設定されています。この結果、ルックアップテーブルで頻繁に再コンパイルが発生し、全体的なシステムパフォーマンスに影響を与える場合があります。
- 8 を超える FQDN が同じ IP アドレスに解決される場合、システムはそれらの FQDN のルールにトラフィックを確実に一致させることができません。IP アドレスごとに最大 8 の FQDN を処理できます。

- アクセス制御ルールごとの一致基準の最大オブジェクト数は 200 です。たとえば、1 つのアクセス制御ルールに最大 200 のネットワークオブジェクトを含めることができます。

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 コントロール 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、以下の両方の動作の前にアプリケーション制御を実行することはできません。

- 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。

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。

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、アクセス コントロール ポリシーの詳細設定で、**[アクセス制御ルールが決定される前に使用される侵入ポリシー（Intrusion Policy used before Access Control rule is determined）]** オプションで侵入ポリシーを選択します。

アプリケーションの特定に関する制限事項の理解

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 URL ルール を配置する

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。

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

Web サーバによって参照されるトラフィック（アドバタイズメント トラフィックなど）を処理するには、参照元アプリケーションではなく、参照先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

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。通常、これらのアプリケーションには、制御できる各側面のアプリケーション名が含まれています。アプリケーション固有のガイドラインと制限事項 （20 ページ）も参照してください。

回避的アプリケーション トラフィックの制御

「アプリケーション固有のガイドラインと制限事項 （20 ページ）」を参照してください。

アプリケーション マッチングとポート マッチングの選択

従来のファイアウォールでは、 IP や TCP /80 などの OSI レイヤ 3（プロトコル）および 4（トランスポート）に基づいてトラフィックを照合できます。特定のポート（またはプロトコル全体）のすべてのトラフィックは、そのルールのアクションに基づいて許可またはブロックされます。

一方、アプリケーションの基準は OSI レイヤ 7 です。異なるアプリケーションが同じ TCP/UDP ポートを使用できます。アプリケーション基準を使用することで、同じポート上のすべてのアプリケーションを許可またはブロックするのではなく、同じポート上の異なるアプリケーションを選択的に許可またはブロックできます。

ルールでポートベースの基準とアプリケーション ベースの基準のどちらを使用するかによって、ルールのパフォーマンスに影響を与える可能性があります。TCP/UDP ポートはパケット内で迅速に識別できるため、システムは最初のパケットで正しいルールと一致させることができます。アプリケーション レイヤ基準を使用すると、特定のアプリケーションを識別するのに 3 ～ 5 パケットを使用できます（ポートも指定しなかった場合）。

次の推奨事項を考慮してください。

- 特定の TCP/UDP ポート上のすべてのトラフィックを、指定したインターフェイスとネットワーク上で同じ方法で処理する場合は、ポートベースの照合を使用します。たとえば、すべての SSH トラフィックを同じ方法で処理するには、ポート タブで SSH ポート（TCP/22）を選択します。
- 他のアプリケーションと同じポートを使用する特定のアプリケーションを絞り込む場合は、アプリケーション タブでそのアプリケーションを選択します。これは、すべてが TCP/80 または 443 を使用する Web アプリケーションを処理する方法です。これにより、すべての Web アプリケーションをブロックまたは許可することなく、特定の Web アプリケーションを選択的にブロックまたは許可できます。
- ユーザー グループによるアプリケーションの使用を制御する場合は、[ユーザー（Users）] タブでユーザー グループを選択し、[アプリケーション（Application）] タブでアプリケーションを選択します。たとえば、請負業者のユーザー グループのメンバーに対してゲーム アプリケーションのカテゴリをブロックできます。

ルールをプロトコル/ポートのすべての接続に適用する必要がある場合は、ユーザーグループ単位でプロトコル/ポートを許可またはブロックすることもできます。

- 安全性の低いネットワーク（インターネットなど）から安全性の高いネットワーク（内部で保護されたネットワークなど）に移行するルールの場合は、可能な限りポートタブを使用します。たとえば、インターネットから内部ネットワークへのICMPトラフィックを許可/ブロックできます。
- ポートベースのルールとアプリケーションベースのルールが混在している場合は、ルールリスト内でポートベースのルールを上位に配置して、接続をそれらのルールに最初に一致させることができます。プロトコルとポートは、アプリケーションよりも迅速に識別できます。

アプリケーション固有のガイドラインと制限事項

- Office 365 管理ポータル：アクセス ポリシーのロギングが接続の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：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。
- 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：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。
- Bittorrent、Tor、Psiphon、およびUltrasurfなどの回避的なアプリケーション：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（リモートデスクトップ プロトコル）：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 コントロール ルールのベストプラクティス

アクセス コントロール ルールを適切に構成して順序付けることは、ネットワークを保護するうえで不可欠です。次のトピックでは、ルールのパフォーマンスと有効性を最大化するためのベスト プラクティスを要約します。

（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、割り当てられた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、そのデバイスにデプロイ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（ACL）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。ポリシー規則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。
- 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。
- 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 コントロール ルールのベストプラクティス （21 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よりも優先する必要があります（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、トラフィックが先に一般ルールに一致し、適用対象であ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 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。
- 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。
- 一般に、アプリケーション条件のルールは、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。詳細については、アプリケーション マッチングとポート マッチングの選択 （19 ページ）およびアプリケーション制御に関する推奨事項 （17 ページ）を参照してください。
- 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、次のセクションに記載されています。

アプリケーション ルールの順序

一般に、アプリケーション条件のルールは、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。

詳細については、「アプリケーション マッチングとポート マッチングの選択 （19 ページ）」および「アプリケーション制御に関する推奨事項 （17 ページ）」を参照してください。

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

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。VLAN 27 をブロックするには、 VLAN 22-33 を許可するルールの上にそのルールを移動する必要があります。

アクセス コントロール ルール 1：送信元ネットワーク VLAN 22-33 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 VLAN 27、VLAN 2 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。

アクセス コントロール ルール 1：送信元ネットワーク 10.10.10.0/24 をURL www.netflix.com に許可
アクセス コントロール ルール 2：送信元ネットワーク 10.10.10.0/24 をURL www.netflix.com に許可

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。

アクセス コントロール ルール 1：送信元ネットワーク 10.10.10.0/24 をURL www.netflix.com に許可
アクセス コントロール ルール 2：送信元ネットワーク 10.10.11.0/24 をURL www.netflix.com に許可

ルール アクションとルール順序

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、アプリケーションマッチングとポートマッチングの選択 （19 ページ）も参照してください。

アクセス コントロール ルールの最適な順序

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 ルールの監視アクション （7 ページ）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。
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。
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。

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：設定し過ぎない

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 マッチングとポート マッチングの選択 （19 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。

  Firewall 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。

- ルールでセキュリティゾーンを指定すると、ルールは、指定したゾーンにインターフェイスを持つデバイスにのみ展開されます。そのため、ポリシーに割り当てられた一部のデバイスのみにルールを適用する場合は、セキュリティゾーンが適切なデバイスのサブセットに適用されるよう選択します。これにより、不要なルールがデバイスに展開されないようになります。

アクセス制御ルールと侵入ポリシーの最大数

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。

アクセス コントロール ルールの管理

ここでは、アクセス コントロール ルールの管理方法について説明します。

アクセス コントロール ルールのカテゴリの追加

アクセス コントロール ポリシーの必須ルールセクションとデフォルトルールセクションをカスタムカテゴリに分割できます。カテゴリは、作成した後に移動することはできません。ただし、カテゴリを削除または名前変更したり、ルールをカテゴリ内またはカテゴリ間で移動したりすることはできます。システムはセクションとカテゴリに横断的にルール番号を割り当てます。

手順

ステップ1 アクセス コントロール ポリシー エディタで、[カテゴリの追加（Add Category）] をクリックします。

ヒント
ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[Insert new category] を選択することもできます。

ステップ2 名前を入力します。

ステップ3 [挿入（Insert）] ドロップダウン リストから、カテゴリを追加する先を選択します。

- カテゴリをセクションのすべての既存カテゴリの下に挿入するには、[必須ルール内（Into Mandatory）] または [デフォルトルール内（into Default）] を選択します。
- 既存のカテゴリの上に挿入するには、[カテゴリの上（above category）] を選択した後、カテゴリを選択します。
- アクセス制御ルールの上または下に挿入するには、[ルールの上（above rule）] または [ルールの下（below rule）] を選択した後、既存のルール番号を入力します。

ステップ4 **[適用（Apply）]** をクリックします。

ステップ5 [保存（Save）] をクリックしてポリシーを保存します。

次のタスク

次の作業に進んでください。

- カテゴリ内またはカテゴリからルールをドラッグ アンド ドロップします。
- ルールの作成時に、そのルールを含める必要があるカテゴリを選択します。
- ルールを編集する場合、ルールをカテゴリ内に再配置するか、カテゴリ外に移動します。

アクセス コントロール ルールの作成および編集

アクセスコントロールルールを使用して、特定のトラフィッククラスにアクションを適用します。ルールを使用すると、望ましいトラフィックを選択的に許可し、望ましくないトラフィックをドロップできます。

手順

ステップ 1 アクセス コントロール ポリシー エディタには、以下のオプションがあります。

- 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。
- 既存のルールを編集するには、**Edit** (✎) をクリックします。
- 既存のルールのコピーから開始するには、[**More** (⋮)] メニューから次のコマンドのいずれかを選択します。
  - **[ルールをコピー（Copy Rule）]**：ルールをクリップボードにコピーします。これにより、**Paste Above/Below** コマンドを使用して、同じポリシーの任意の場所にルールを配置できます。
  - **[ルールを別のポリシーにコピー Rule to Different Policy）]**：ルールを別のアクセス コントロール ポリシーにコピーします。ダイアログボックスが開き、ポリシーを選択してルール配置を選択できます。
  - **[ルールをクローン（Clone Rule）]** は、重複しているルールに即座にコピーを作成します。
- 複数のルールを編集するには、チェックボックスを使用して複数のルールを選択してから、検索ボックスの横にある **[アクションの選択/バルク ルール アクション（Select Action/Bulk Rule Actions）]** リストで **[編集（Edit）]** または別のアクションを選択します。
- インライン編集を行うには、つまりルール条件のオブジェクトの構成を変更するには、値を右クリックして [編集（Edit）] を選択します。右クリックメニューを使用して、項目を削除したり、フィルタに追加したり、テキストや値をコピーしたりすることもできます。

代わりに **View** (👁) がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 2 これが新しいルールである場合は、[名前（Name）] を入力します。

ステップ 3 （）ルールコンポーネントを設定します。

複数のルールを一括編集する場合は、オプションのサブセットのみを使用できます。

- 位置：ルールの位置を指定します（新しいルールの場合は**[挿入（Insert）]**、既存のルールの場合はルール名の横にある**[再配置（Reposition）]**アイコン）。アクセス コントロール ルールの順序 （6 ページ） を参照します。
- [アクション（Action）]：ルールの [アクション（Action）] を選択します。アクセス コントロール ルールのアクション （7 ページ）を参照してください。
- [ロギング（Logging）]：[ロギング（Logging）] をクリックし、接続ロギングと SNMP トラップのオプションを指定します。同じロギング設定は、**[デフォルトアクションの構成（Default Action Configuration）]** ダイアログ（ナビゲーションパス：アクセス コントロール ポリシーを編集する）で構成できます。**[デフォルトアクション（Default Action）]** 領域で、**[デフォルトロギングおよび調査（Default logging and inspection）]** アイコン（**Cog** ()）をクリックします。

  詳細については、「*Cisco Secure Firewall Management Center Administration Guide*」の「接続ロギングのベストプラクティス」を参照してください。
- [時間範囲（Time Range）]：（オプション）Firewall Threat Defense デバイスの場合、ルールが適用される曜日と時間を選択します。オプションを選択しない場合、ルールは常にアクティブになります。詳細は、時間範囲オブジェクトの作成を参照してください。
- **[ルールの有効化（Enable Rule）]**：ルールがアクティブであるかどうか。無効化されたルールは接続に適用されません。ルールを無効にして、トラブルシューティング中など、一時的にオフにすることができます。
- [ディープインスペクション（Deep Inspection）]：（オプション）許可ルールおよびインタラクティブ ブロック ルールの場合は、[侵入ポリシー（Intrusion Policy）]、[変数セット（Variable Set）]、および [ファイルポリシー（File Policy）] のオプションを選択します。侵入ポリシーとファイルポリシーを個別に適用できます。両方を設定する必要はありません。
- [条件（Conditions）]：追加するオブジェクト、または送信元か接続先を選択し、[送信元に追加（Add to Sources）] または [宛先とアプリケーションに追加（Add to Destinations and Applications）] をクリックして、接続の一致条件を追加します。タブをクリックして、使用可能なオブジェクトのリストをネットワーク、セキュリティゾーン、アプリケーションなどに限定できます。ただし、送信元と接続先の列には、現在表示しているタブに関係なく、選択したすべてのオブジェクトが常に表示されます。詳細については、アクセス コントロール ルール条件 （30 ページ）を参照してください。
- [コメント（Comments）]：ダイアログボックスの下部にあるコメントリストを開いてコメントを入力し、**[コメント/投稿を追加（Add Comment/Post）]** をクリックしてコメントを追加します。

ステップ 4 [追加（Add）] または [適用（Apply）] をクリックして、ルールを保存します。[新しいルールの適用および追加（Apply and Add New Rule）] をクリックしてダイアログボックスを開いたままにし、新しいルールを作成できるようにします。

ステップ 5 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

時間ベースのルールを展開する場合は、ポリシーが割り当てられるデバイスのタイムゾーンを指定します。「タイムゾーン」を参照してください。

設定変更を展開します設定変更の展開を参照してください。

関連トピック

アクセス コントロール ルールのベストプラクティス （21 ページ）

アクセス コントロール ルール条件

ルール条件は、各ルールで対象とする接続の特性を定義します。条件を正確に使用してルールを微調整し、該当するルールで処理する必要があるトラフィックのすべてに、またそのトラフィックのみに適用されるようにします。次のトピックでは、使用できる一致条件について説明します。

セキュリティ/トンネル ゾーンのルール条件

セキュリティゾーンとトンネルゾーンを使用して、ルールのトラフィックを選択できます。

セキュリティ ゾーンを利用すると、ネットワークをセグメント化し、複数のデバイスでインターフェイスをグループ化して、トラフィック フローを管理および分類する上で助けになります。トンネルゾーンでは、トンネル内のカプセル化された接続にアクセスコントロールルールを適用するのではなく、トンネルとして処理する必要があるトンネルトラフィック（GRE など）を識別することができます。

セキュリティゾーンを使用して、送信元および宛先インターフェイスごとにトラフィックを制御できます。送信元ゾーンと宛先ゾーンの両方をゾーン条件に追加する場合、トラフィックがルールに一致するには、一致するトラフィックが送信元ゾーンのいずれかにあるインターフェイスから発信され、宛先ゾーンのいずれかにあるインターフェイスを通過する必要があります。セキュリティゾーン内のすべてのインターフェイスは同じタイプ（すべてインライン、パッシブ、スイッチド、またはルーテッド）である必要がるのと同じく、ゾーン条件で使用するすべてのゾーンも同じタイプである必要があります。パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブインターフェイスのあるゾーンを宛先ゾーンとして使用することはできません。

トンネルゾーンを使用する場合は、プレフィルタポリシーに一致するルールがあることを確認して、トンネル化トラフィックをゾーンに関連付けます。次に、ルールの送信元ゾーンとしてトンネルゾーンを選択できます。トンネルゾーンを宛先にすることはできません。トンネルをトンネルゾーンに再ゾーン化するためのプレフィルタルールがない場合、トンネルのアクセスコントロールルールはどの接続にも適用されません。宛先セキュリティゾーンを、特定のインターフェイスを介してデバイスを離れるターゲットトンネルに指定することができます。

セキュリティ ゾーンに関する注意事項

セキュリティゾーンの基準を決定するときは、次の点を考慮してください。

- 可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。
- アクセス制御ルールは、デバイス設定で ACL エントリ（ACE）を生成して、可能な限り早期の処理およびドロップを提供します。ルールでセキュリティゾーンを指定すると、ゾーン内のインターフェイスごとに ACE が作成されるため、ACL のサイズが非常に大きくなる可能性があります。アクセス制御ルールから生成された ACL が大きすぎると、システムパフォーマンスに影響を与える可能性があります。

ネットワークルールの条件

ネットワークルール条件とは、トラフィックのネットワークアドレスまたは場所を定義するネットワークオブジェクトまたは地理的位置です。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[送信元（Source）] リストに条件を追加します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[宛先（Destinations）] リストに条件を追加します。
- 送信元と送信先ネットワークの両方の条件をルールに追加すると、一致するトラフィックは指定した IP アドレスのいずれかから送信され、送信先 IP アドレスのいずれかを通って出力されなければなりません。

この条件を追加するには、次のタブから選択します。

- [ネットワーク（Network）]：制御するトラフィックの送信元または宛先 IP アドレスを定義するネットワーク オブジェクトまたはグループを選択します。

  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。

  完全修飾ドメイン名（FQDN）を使用してアドレスを定義するオブジェクトを使用できます。このアドレスは DNS ルックアップによって判別されます。ただし、アクセス コントロール ポリシー内の次のセクションでは、FQDN オブジェクトはサポートされていません：元のクライアントネットワーク、SGT/ISE 属性、ネットワーク分析および侵入ポリシー、セキュリティインテリジェンス、Threat Detection、エレファント フロー設定。

- [地理位置情報（Geolocation）]：位置情報機能を選択して、その送信元または宛先の国や大陸に基づいてトラフィックを制御できます。大陸を選択すると、その大陸内のすべての国が選択されます。地理的位置を直接ルールで選択するほかに、作成した位置情報オブジェクトを選択して場所を定義することもできます。地理的位置を使用すると、特定の国

で使用されているすべての潜在的な IP アドレスを知る必要なく、その国へのアクセスを簡単に制限できます。

（注） 地理的位置の最新データを常にトラフィック フィルタリングで使用できるよう、地理位置情報データベース（GeoDB）を定期的に更新することを推奨します。

ネットワーク条件での元のクライアント（プロキシ トラフィックのフィルタリング）

一部のルールでは、発信元クライアントに基づいてプロキシトラフィックを処理できます。送信元ネットワーク条件を使用してプロキシサーバーを指定し、次に元のクライアント制約を追加して元のクライアント IP アドレスを指定します。システムはパケットの X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義 HTTP ヘッダー フィールドを使用して、元のクライアント IP を判別します。

プロキシの IP アドレスがルールの送信元ネットワークの制約と一致する場合、トラフィックはルールに一致し、さらに元のクライアントの IP アドレスは、ルールの元のクライアント制約に一致します。たとえば、特定の元のクライアントアドレスからのトラフィックを許可するものの、それが特定のプロキシを使用している場合のみに限定するには、以下の 3 つのアクセス コントロール ルールを作成します。

アクセスコントロールルール 1：特定の IP アドレス（209.165.201.1）からのプロキシトラフィックをブロックします。

送信元ネットワーク：209.165.201.1
元のネットワーク クライアント：none または any
アクション：ブロック

アクセス コントロール ルール 2：同じ IP アドレスからのプロキシ トラフィックを許可します。ただし、そのトラフィックのプロキシサーバーが、選択したもの（209.165.200.225 または 209.165.200.238）である場合に限ります。

送信元ネットワーク：209.165.200.225 および 209.165.200.238
元のクライアント ネットワーク：209.165.201.1
アクション：許可

アクセス コントロール ルール 3：同じ IP アドレスからのプロキシ トラフィックを、それが他のプロキシ サーバーを使用する場合はブロックします。

[Source Networks]：any
元のクライアント ネットワーク：209.165.201.1
アクション：ブロック

VLAN タグ ルールの条件

（注） アクセス ルールの VLAN タグは、インラインセットにのみ適用されます。VLAN タグを持つアクセスルールは、ファイアウォール インターフェイス上のトラフィックを照合しません。

VLAN ルール条件によって、Q-in-Q（スタック VLAN）など、VLAN タグ付きトラフィックが制御されます。システムでは、プレフィルタ ポリシー（そのルールで最も外側の VLAN タグを使用する）を除き、最も内側の VLAN タグを使用して VLAN トラフィックをフィルタ処理します。

次の Q-in-Q サポートに注意してください。

- Firepower 4100/9300 上の Firewall Threat Defense：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。
- 他のすべてのモデルの Firewall Threat Defense
  - インラインセットおよびパッシブインターフェイス：Q-in-Q をサポートします（最大 2 つの VLAN タグをサポート）。
  - ファイアウォール インターフェイス：Q-in-Q をサポートしません（1 つの VLAN タグのみをサポート）。

事前定義のオブジェクトを使用して VLAN 条件を作成でき、また 1 ～ 4094 の VLAN タグを手動で入力することもできます。VLAN タグの範囲を指定するには、ハイフンを使用します。

クラスタで VLAN マッチングに問題が発生した場合は、アクセス コントロール ポリシーの詳細オプションである [トランスポート/ネットワークリプロセッサ設定（Transport/Network Preprocessor Settings）] を編集し、[接続の追跡時にVLAN ヘッダーを無視する（Ignore the VLAN header when tracking connections）] オプションを選択します。

ユーザー ルール条件

接続を開始したユーザー、またはユーザーが属するグループに基づいてトラフィックが照合されます。たとえば、財務グループの全員がネットワークリソースにアクセスすることを禁止するブロックルールを設定できます。

Microsoft Active Directory レルムのユーザーに対してのみユーザー ルール条件を設定できます。

設定されたレルムのユーザーとグループの設定に加えて、次の特殊なアイデンティティユーザーのポリシーを設定できます。

- [失敗した認証（Failed Authentication）]：キャプティブポータルでの認証に失敗したユーザー。
- [ゲスト（Guest）]：キャプティブポータルでゲストユーザーとして設定されたユーザー。
- [認証不要（No Authentication Required）]：アイデンティティの [認証不要（No Authentication Required）] ルールアクションに一致するユーザー。

- [不明（Unknown）]：識別できないユーザー。たとえば、設定されたレルムによってダウンロードされていないユーザー。

アクセス制御ルールのみの場合、ID ポリシーをアクセス コントロール ポリシーに最初に関連付ける必要があります（アクセス制御への他のポリシーの関連付けを参照）。

アプリケーションルールの条件

システムはIP トラフィックを分析する際、ネットワークで一般的に使用されているアプリケーションを識別および分類できます。このディスカバリベースのアプリケーション認識は、アプリケーション制御、つまりアプリケーション トラフィック制御機能の基本です。

システム提供のアプリケーション フィルタは、アプリケーションの基本特性（タイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグ）にしたがってアプリケーションを整理することで、アプリケーション制御に役立ちます。システム提供のフィルタの組み合わせやアプリケーションの任意の組み合わせをもとに、ユーザー定義の再利用可能フィルタを作成できます。

ポリシーのアプリケーション ルール条件ごとに、少なくとも 1 つのディテクタが有効にされている必要があります。有効になっているディテクタがないアプリケーションについては、システム提供のすべてのディテクタが自動的に有効になります。ディテクタが存在しない場合は、そのアプリケーションについて最後に変更されたユーザー定義ディテクタが有効になります。アプリケーション ディテクタの詳細については、アプリケーション ディテクタの基本を参照してください。

アプリケーション フィルタと個別に指定されたアプリケーションの両方を使用することで、完全なカバレッジを確保できます。ただし、アクセス コントロール ルールの順序を指定する前に、次の注意事項を確認してください。

アプリケーションフィルタの利点

アプリケーション フィルタにより、迅速にアプリケーション制御を設定できます。たとえば、システム提供のフィルタを使って、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを簡単に作成できます。ユーザーがそれらのアプリケーションの 1 つを使用しようとすると、システムがセッションをブロックします。

アプリケーション フィルタを使用することで、ポリシーの作成と管理は簡単になります。この方法によりアプリケーション トラフィックが期待どおりに制御されます。シスコは、システムと脆弱性データベース（VDB）の更新を通して、頻繁にアプリケーション ディテクタを更新しています。このため、アプリケーション トラフィックは常に最新のディテクタによってモニターされます。また、独自のディテクタを作成し、どのような特性のアプリケーションを検出するかを割り当て、既存のフィルタを自動的に追加することもできます。

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 *1*: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	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	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。

アプリケーション条件とフィルタの設定

アプリケーションの条件またはフィルタを作成するには、使用可能なアプリケーションのリストから、トラフィックを制御するアプリケーションを選択します。オプションとして（推奨）、フィルタを使用して使用可能なアプリケーションを抑制します。フィルタと個別に指定されたアプリケーションを同じ条件で使用できます。

始める前に

- アクセス コントロール ルールでアプリケーション制御を実行するためには、アクセス コントロール ポリシーの詳細設定で、アダプティブ プロファイルを有効にする必要があります（これがデフォルト状態）。

手順

ステップ 1 アクセス ポリシー ルール エディタで、**[アプリケーション（Applications）]** タブを選択します。

ステップ 2 [使用可能なアプリケーション（Available Applications）] リストから追加するアプリケーションを見つけて選択します。

[使用可能なアプリケーション（Available Applications）] に表示されるアプリケーションを抑制するには、1つ以上の**アプリケーション フィルタ**を選択するか、個別のアプリケーションを検索します。

ヒント
サマリー情報とインターネットの検索リンクを表示するには、アプリケーションの横の **Information**( ) をクリックします。**ロック**アイコン（）は、システムが、そのアプリケーションを、復号されたトラフィックでのみ識別できることを示します。

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション（Available Applications）] リストが更新され、条件を満たすアプリケーションのみが表示されます。システムによって提供されるフィルタは組み合わせて選択できますが、ユーザー定義フィルタはできません。

- 同じ特性（リスク、ビジネス関連性など）の複数のフィルタ：アプリケーショントラフィックは1つのフィルタのみに一致する必要があります。たとえば、中リスク フィルタと高リスク フィルタの両方を選択すると、[使用可能なアプリケーション（Available Applications）] リストにすべての中リスク アプリケーションと高リスク アプリケーションが表示されます。
- 異なるアプリケーション特性のフィルタ：アプリケーショントラフィックは、両方のフィルタ タイプに一致する必要があります。たとえば、高リスク フィルタとビジネスとの関連性が低いフィルタの両方を選択すると、[使用可能なアプリケーション（Available Applications）] リストに両方の条件を満たすアプリケーションのみが表示されます。

ステップ 3 [アプリケーションの追加（Add Application）] または [ルールに追加（Add to Rule）] をクリックするか、ドラッグアンドドロップします。

ヒント
フィルタとアプリケーションをさらに追加する前に、**[フィルタ/選択項目のクリア（Clear Filters/Selection）]** をクリックして現在の選択をクリアします。

ステップ 4 ルールまたは設定を保存するか、編集を続けます。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

ポート、プロトコル、および ICMP コード ルールの条件

ポート条件により、送信元ポートと宛先ポートに基づいてトラフィックが照合されます。ルールのタイプによって、「ポート」は次のいずれかを表します。

- TCP と UDP：TCP と UDP のトラフィックは、ポートに基づいて制御できます。システムは、カッコ内に記載されたプロトコル番号+オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- ICMP：ICMP および ICMPv6（IPv6 ICMP）トラフィックは、そのインターネット層プロトコルと、オプションでタイプおよびコードに基づいて制御できます。例：ICMP(1):3:3
- プロトコル：ポートを使用しないその他のプロトコルを使用してトラフィックを制御できます。

可能な場合は常に、一致基準の数を最小限にします（特にセキュリティゾーン、ネットワークオブジェクト、およびポートオブジェクトの場合）。基準を複数指定すると、指定した条件の内容について「すべて」の組み合わせと照合する必要があります。

ポートベースのルールのベスト プラクティス

ポートの指定は、アプリケーションをターゲット指定するための従来の方法です。ただし、アプリケーションは、固有のポートを使用してアクセス コントロール ブロックをバイパスするように設定することが可能です。そのため、可能な場合は常に、ポート基準ではなくアプリケーションフィルタリング基準を使用してトラフィックをターゲット指定します。なお、プレフィルタルールではアプリケーション フィルタリングを使用できません。

アプリケーションフィルタリングは、制御フローとデータフローのために個別のチャネルを動的に開くアプリケーション（FTP など）にも推奨されます。ポートベースのアクセス コントロール ルールを使用すると、これらの種類のアプリケーションが正しく動作しなくなり、望ましい接続がブロックされる可能性があります。

送信元と宛先ポートの制約の使用

送信元ポートと宛先ポートの両方を制約に追加する場合、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat（UDP）は追加できません。

送信元ポートのみ、あるいは宛先ポートのみを追加する場合は、異なるトランスポートプロトコルを使用するポートを追加できます。たとえば、DNS over TCP と DNS over UDP の両方を 1 つのアクセスコントロールルールの宛先ポート条件として追加できます。

ポート条件を使用した非 TCP トラフィックの照合

ポートベースではないプロトコルを照合できます。デフォルトでは、ポート条件を指定しない場合は IP トラフィックを照合します。非 TCP トラフィックを照合するためのポート条件を設定することはできますが、いくつかの制約事項があります。

- アクセス コントロール ルール：クラシック デバイスの場合、GRE でカプセル化されたトラフィックをアクセス コントロール ルールに照合するには、宛先ポート条件として GRE（47）プロトコルを使用します。GRE 制約ルールには、ネットワーク ベースの条件（ゾーン、IP アドレス、ポート、VLAN タグ）のみを追加できます。また、GRE 制約ルールが設定されたアクセス コントロール ポリシーでは、システムが外側のヘッダーを使用して

すべてのトラフィックを照合します。Firewall Threat Defense デバイスの場合、GRE でカプセル化されたトラフィックを制御するには、プレフィルタ ポリシーでトンネル ルールを使用します。

- 復号ルール：これらのルールは TCP ポート条件のみをサポートします。
- IMCP エコー：タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートは、要求されていないエコー応答だけと照合されます。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。

URL ルール条件

URL 条件を使用してネットワークのユーザーがアクセスできる Web サイトを制御します。

詳細については、カテゴリおよびレピュテーションによる URL のフィルタリングについてを参照してください。

ダイナミック属性ルールの条件

ダイナミック属性には次のものがあります。

- （送信元または宛先）。ダイナミックオブジェクト（dynamic attributes connector からのものなど）

  dynamic attributes connector では、クラウドプロバイダーからデータ（ネットワークや IP アドレスなど）を収集し、それを Secure Firewall Management Center に送信して、アクセス制御ルールで使用できるようにします。

  dynamic attributes connector の詳細については、「Dynamic Attributes Connector について」を参照してください。

- （送信元のみ）。SGT オブジェクトは、手動で定義したタグ、または ISE が定義したタグを含みます。詳細については、送信元および宛先セキュリティグループタグ（SGT）の照合 および セキュリティグループタグを参照してください。
- （送信元のみ）。Cisco ISE が定義したロケーション IP オブジェクト
- （送信元のみ）。Cisco ISE が定義したデバイスタイプオブジェクト（エンドポイント プロファイル オブジェクトとも呼ばれます）

ダイナミック属性は、アクセスコントロールルールの送信元基準および接続先基準として使用できます。次の注意事項に従ってください。

- 異なるタイプのオブジェクトは AND 結合される
- 同様のタイプのオブジェクトは OR 結合される

たとえば、送信元と宛先の基準 SGT 1、SGT 2、およびデバイスタイプ 1 を選択した場合、デバイスタイプ 1 が SGT 1 または SGT 2 で検出された場合、ルールが一致します。別の例として、セキュリティグループタグと、IP アドレスをリストするダイナミックオブジェクトの両方

を選択した場合、タグを持つトラフィックがそれらの IP アドレスのいずれかを発信元（または宛先）とする場合にルールが一致します。

時間と日のルール条件

連続する時間範囲または定期的な期間を指定できます。

たとえば、平日の勤務時間、週末、または休日のシャットダウン期間中にのみルールを適用できます。

時間ベースのルールは、トラフィックを処理するデバイスの現地時間に基づいて適用されます。

時間ベースのルールは、Firewall Threat Defense デバイスでのみサポートされます。時間ベースのルールを含むポリシーを別のタイプのデバイスに割り当てると、ルールに関連付けられた時間制限はそのデバイスでは無視されます。この場合、警告が表示されます。

アクセス コントロール ルールの有効化と無効化

アクセスコントロールルールを作成すると、そのルールはデフォルトで有効になります。ルールを無効にすると、システムはネットワークトラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。アクセス コントロール ポリシーのルール リストを表示したときに、無効なルールはグレー表示されますが、変更は可能です。

また、ルール エディタを使用してアクセス コントロール ルールを有効化または無効化することもできます。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、ルールを右クリックし、ルールの状態を選択します。

代わりに **View** ( ) がルールの横に表示される場合、ルールは先祖ポリシーに属しており、ルールを変更する権限がありません。

ステップ 2 **[保存（Save）]** をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

あるアクセス コントロール ポリシーから別のアクセス コントロール ポリシーにアクセス制御ルールをコピー。

あるアクセス コントロール ポリシーから別のアクセス コントロール ポリシーにアクセス制御ルールをコピーできます。ルールは、アクセス コントロール ポリシーの[デフォルト（Default）] セクションまたは [必須（Mandatory）] セクションにコピーできます。

コメントを除く、コピーしたルールのすべての設定は、貼り付けたバージョンに保持されます。

手順

ステップ 1 次のいずれかを実行します。

- 単一のルールをコピーするには、ルールを右クリックし、**[別のポリシーにルールをコピー（Copy Rule to Different Policy）]** を選択します。
- 複数のルールをコピーするには、それらのチェックボックスをオンにして、**[一括アクションの選択（Select Bulk Action）]** メニューから **[別のポリシーにルールをコピー（Copy Rule to Different Policy）]** を選択します。

ステップ 2 [アクセスポリシー（Access Policy）] ドロップダウンリストから宛先アクセス コントロール ポリシーを選択します。

ステップ 3 [ルールの配置（Place Rules）] ドロップダウンリストから、コピーしたルールを配置する場所を選択します。それらは、[必須（Mandatory）] セクションまたは [デフォルト（Default）] セクションのいずれかの上部または下部に配置できます。

ステップ 4 **[コピー（Copy）]** をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

アクセス コントロール ルールのプレフィルタ ポリシーへの移動

アクセス コントロール ポリシーから関連するデフォルト以外のプレフィルタポリシーにアクセス制御ルールを移動できます。

まず、ユーザー定義のプレフィルタポリシーをアクセス コントロール ポリシーに適用する必要があります。デフォルトのプレフィルタポリシーにはルールを設定できないため、デフォルトのプレフィルタポリシーにはアクセス制御ルールを移動できません。

始める前に

続行する前に、次の条件に注意してください。

- アクセスコントロールルールをプレフィルタポリシーに移動する場合、アクセスコントロールルールのレイヤ 7（L7）パラメータ（アプリケーションや URL のフィルタイン）は移動できません。L7 パラメータは、操作中に削除されます。
- ルールを移動すると、アクセス コントロール ルール構成のコメントが失われます。ただし、ソースアクセスコントロールポリシーに言及する新しいコメントがコピーされたルールに追加されます。
- [アクション（Action）]パラメータとして[モニター（Monitor）]セットを使用してアクセスコントロールルールを移動することはできません。
- アクセスコントロールルールの[アクション（Action）]パラメータは、移動時にプレフィルタルールの適切なアクションに変更されます。アクセスコントロールルールの各アクションが何にマップされるかを知るには、次の表を参照してください。

アクセスコントロールルールのアクション	プレフィルタルールのアクション
許可（Allow）	分析（Analyze）
ブロック（Block）	ブロック（Block）
Block with reset	ブロック（Block）
インタラクティブブロック（Interactive Block）	ブロック（Block）
リセット付きインタラクティブ ブロック（Interactive Block with reset）	ブロック（Block）
信頼（Trust）	高速パス（Fastpath）

- 同様に、次の表に示すように、アクセスコントロールルールで構成されたアクションに基づいて、ルールの移動後にロギング構成が適切な設定になります。

アクセスコントロールルールのアクション	プレフィルタルールの有効なロギング構成
許可（Allow）	どのチェックボックスもチェックされていません。
Block Block with reset インタラクティブブロック リセット付きインタラクティブブロック	• 接続開始時にロギング（Log at Beginning of Connection） • イベント ビューア • Syslog サーバ • SNMP トラップ

アクセスコントロールルールのアクション	プレフィルタルールの有効なロギング構成
[信頼（Trust）]	• 接続開始時にロギング（Log at Beginning of Connection） • 接続終了時にロギング（Log at End of Connection） • イベント ビューア • Syslog サーバ • SNMP トラップ

- ソースポリシーからルールを移動しているときに、別のユーザーがそれらのルールを変更すると、メッセージが表示されます。ページを更新した後、プロセスを続行できます。

手順

ステップ 1 次のいずれかを実行します。

- 単一のルールを移動するには、ルールを右クリックし、**[ルールをプレフィルタ ポリシーに移動（Move Rule to Prefilter Policy）]** を選択します。
- 複数のルールを移動するには、各ルールのチェックボックスをオンにし、**[一括アクションの選択（Select Bulk Action）]** メニューから **[ルールをプレフィルタ ポリシーに移動（Move Rule to Prefilter Policy）]** を選択します。

ステップ 2 **[ルールの配置（Place Rules）]** ドロップダウン リストから、移動したルールを配置する場所を選択します。**[末尾（At the bottom）]** または **[先頭（At the top）]** です。

ステップ 3 [移動（Move）] をクリックします。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

アクセス コントロール ルールの位置指定

既存のルールをアクセス コントロール ポリシー内で移動したり、新しいルールを目的の場所に挿入することができます。カテゴリにルールを追加または移動すると、そのルールはシステムによってカテゴリの最後に配置されます。

始める前に

アクセス コントロール ルールのベストプラクティス （21 ページ） でルールの順序のガイドラインを確認してください。

手順

ステップ 1 次のいずれかを実行します。

- 新しいルール：既存のルール間の線にマウスのカーソルを合わせ、[ルールの追加（Add Rule）]をクリックして、新しいルールを挿入します。場所は、[ルールの追加（Add Rule）] ダイアログボックスの [挿入（Insert）] ボックスで選択されています。別のルールを選択して位置を調整することができます。右クリックメニューから [上にルールを追加（Add Rule Above）] または [下にルールを追加（Add Rule Below）] を選択することもできます。
- ルールテーブルを表示する場合の既存のルール：ルールをクリックして、新しい位置にドラッグします。このアクションは最終的なものであり、確認は求められません。
- ルールテーブルを表示している場合の既存のルール：1 つのルールを右クリックし、[ルールの再配置（Reposition Rule）] を選択します。複数のルールを 1 つのグループとして移動するには、各ルールのチェックボックスをオンにし、[一括アクションの選択（Select Bulk Action）] メニューから [ルールの再配置（Reposition Rules）] を選択します。ルールをどこに移動するかを尋ねるプロンプトが表示されます。
- ルールを編集している場合の既存のルール：ルール名の横にある [ルールの再配置（Reposition Rule）] アイコンをクリックします。

ステップ 2 ルールを編集または再配置するときは、ルールを移動または挿入する場所を選択してから、**[移動（Move）]**、**[確認（Confirm）]**、または **[再配置（Reposition）]**（操作の内容に応じて）をクリックします。

- [必須に挿入（into Mandatory）] または [デフォルトに挿入（into Default）] を選択します。
- [カテゴリに挿入（into Category）] を選択して、カテゴリを選択します。
- [ルールの上（above rule）] または [ルールの下（below rule）] を選択し、ルールを選択します。

ステップ 3 ルールを編集している場合は、保存します。

ステップ 4 [保存（Save）] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します設定変更の展開を参照してください。

アクセス コントロール ルールにコメントを追加する

アクセス コントロール ルールを作成または編集するときは、コメントを追加できます。たとえば、他のユーザ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。あるルールの全コメントのリストを表示し、各コメントを追加したユーザやコメント追加日を確認することができます。

ルールを保存すると、最後に保存してから追加されたすべてのコメントは読み取り専用になります。

アクセス コントロール ルールのコメントを検索するには、ルール一覧表示ページの [ルールの検索（Search Rules）] バーを使用します。

手順

ステップ 1 アクセス コントロール ルール エディタで、[コメント（Comments）] をクリックします。

ステップ 2 コメントを入力し、[コメントの追加（Add Comment）] をクリックします。ルールを保存するまでこのコメントを編集または削除できます。

ステップ 3 ルールを保存します。

アクセスコントロールルールの例

次のトピックで、アクセスコントロールルールの例を示します。

セキュリティ ゾーンを使用したアクセスの制御方法

たとえば、ホストがインターネットに無制限でアクセスできるような導入にする一方、着信トラフィックで侵入およびマルウェアの有無を検査することでホストを保護したいとします。

それにはまず、内部ゾーンと外部ゾーンという 2 つのセキュリティ ゾーンを作成します。次に、これらのゾーンに 1 つ以上のデバイス上のインターフェイス ペアを割り当て、各ペアの一方のインターフェイスを内部ゾーンに割り当て、もう一方のインターフェイスを外部ゾーンに割り当てます。内部側のネットワークに接続されたホストは、保護されている資産を表します。

（注） 内部（または外部）のすべてのインターフェイスを 1 つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。

次に、宛先ゾーン条件を内部に設定したアクセス コントロール ルールを構成します。この単純なルールでは、内部ゾーンのいずれかのインターフェイスでデバイスから出力されるトラフィックが照合されます。一致するトラフィックを侵入やマルウェアについて検査するには、

ルール アクションとして [許可（Allow）] を選択し、そのルールを侵入ポリシーとファイル ポリシーに関連付けます。

アプリケーションの使用を制御する方法

ブラウザ ベースのアプリケーション プラットフォームの場合も、あるいは企業ネットワーク内外の伝送として Web プロトコルを使用するリッチ メディア アプリケーションの場合も、Web は企業内でアプリケーションを配信するユビキタス プラットフォームとなりました。

Firewall Threat Defense は接続を検査し、使用されているアプリケーションを判別します。これにより、特定の TCP/UDP ポートを対象とするだけではなく、アプリケーションを対象としたアクセス制御ルールを記述することが可能になります。したがって、複数の Web ベース アプリケーションが同じポートを使用する場合でも、それらを選択的にブロックまたは許可できます。

特定のアプリケーションを選択して許可またはブロックできることに加えて、種類、カテゴリ、タグ、リスク、ビジネスとの関連性などに基づきルールを記述することもできます。たとえば、リスクが高くビジネス関連性が低いすべてのアプリケーションを識別してブロックするアクセス制御ルールを作成できます。ユーザがこのようなアプリケーションのいずれかを使用しようとすると、セッションがブロックされます。

シスコは、システムや脆弱性データベース（VDB）の更新プログラムにより、追加のアプリケーション検出機能を頻繁に更新および追加しています。これにより、リスクの高いアプリケーションをブロックするルールが新しいアプリケーションに自動的に適用され、手動でルールを更新する必要がなくなります。

この事例では、[アノニマイザー/プロキシ（anonymizer/proxy）] カテゴリに属するすべてのアプリケーションをブロックします。

手順

ステップ 1 **Policies** > **Access Control heading** > **Access Control** を選択し、アクセス コントロール ポリシーを編集します。

ステップ 2 [ルールの追加（Add Rule）] をクリックし、アプリケーション制御のルールを設定します。

a) ルールに意味のある名前を付けます（Block_Anonymizers など）。

b) [アクション（Action）] で [ブロック（Block）] を選択します。

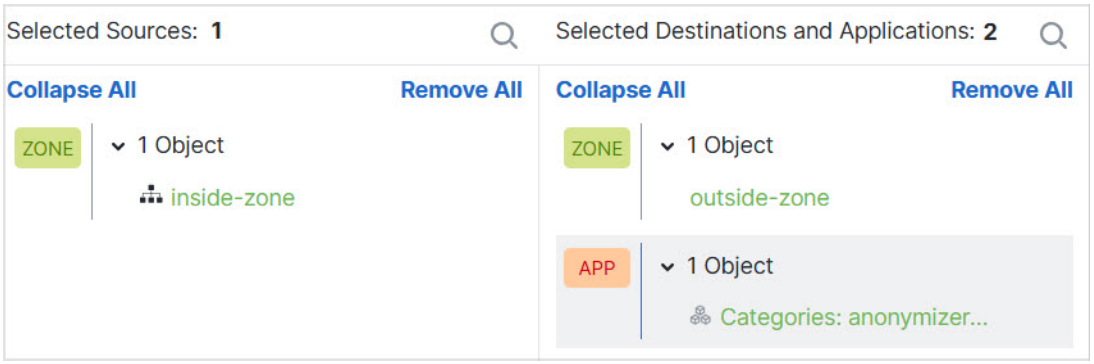
c) ゾーンが設定されており、このルールを内部から外部へのトラフィックに適用する場合は、[ゾーン（Zones）] タブを選択して、内部ゾーンを送信元ゾーンとして選択し、外部ゾーンを宛先ゾーンとして選択します。

d) [アプリケーション（Applications）] タブをクリックし、照合するアプリケーションを選択して、[アプリケーションの追加（Add Application）] をクリックします。

カテゴリやリスクレベルなどの基準を選択すると、基準の右側にあるリストが更新され、基準に一致するアプリケーションが正確に表示されます。作成しようとしているルールは、これらのアプリケーションに適用されます。

このリストをよく見てください。たとえば、リスクが非常に高いすべてのアプリケーションをブロックしようとする場合があります。ただし、本書を作成している時点で、TFPTは非常に高リスクに分類されています。ほとんどの組織は、このアプリケーションをブロックすることを希望しません。さまざまなフィルタ条件を試して、選択に一致するアプリケーションを確認するには時間がかかります。これらのリストはVDB更新のたびに変更される可能性があることに注意してください。

この例では、[カテゴリ（Categories）] リストからアノニマイザー/プロキシを選択し、[宛先とアプリケーション（Destinations and Applications）] に追加します。一致基準は次の図のようになるはずです。



e) ルールアクションの横にある [ロギング（Logging）] をクリックし、接続開始時のロギングを有効にします。syslogサーバーを使用している場合は、そのサーバーを選択できます。

このルールによってブロックされる接続の情報を取得するには、ロギングを有効化する必要があります。

ステップ3 このルールを、プロトコルとポートの基準のみを使用するルール（ただし、アプリケーションルールによってブロックされる必要があるトラフィックを許可しないルール）の後に移動します。

アプリケーションの照合にはSnort検査が必要です。プロトコルとポートのみを使用するルールではSnort検査が必要ないため、これらの単純なルールをアクセス コントロール ポリシーの最上位にグループ化することで、システムパフォーマンスを向上させることができます。

ステップ4 変更を展開します。

アプリケーションルールのヒット数および分析ダッシュボードを使用して、このルールのパフォーマンスと、ユーザーがこれらのアプリケーションを試用する頻度を確認できます。

脅威をブロックする方法

侵入ポリシーをアクセス制御ルールに追加することにより、次世代の侵入防御システム（IPS）フィルタリングを実装できます。侵入ポリシーはネットワーク トラフィックを分析し、トラフィック コンテンツを既知の脅威と比較します。いずれかの接続が監視対象の脅威と一致する場合、システムはその接続をドロップし、こうして攻撃を防止できます。

ネットワーク トラフィックに対して侵入検査を行う前に、他のすべてのトラフィック処理が行われます。侵入ポリシーをアクセス制御ルールに関連付けると、アクセス制御ルールの条件に一致するトラフィックをシステムが通過させる前に、侵入ポリシーを使ってまずトラフィックを検査するようシステムに指示できます。

単にトラフィックを許可するルール上で侵入ポリシーを設定できます。トラフィックを信頼またはブロックするように設定したルールにインスペクションは実行されません。さらに、単純なブロックを使用しない場合は、デフォルトアクションとして侵入ポリシーを設定できます。

潜在的な侵入を許可するトラフィックの検査に加え、セキュリティ インテリジェンス ポリシーを使用することで、既知の不正IPアドレスとのすべてのトラフィック、または既知の不正URLへのすべてのトラフィックを先制的にブロックできます。

この例では、内部の 192.168.1.0/24 ネットワークの外部への侵入を許可する侵入ポリシーを追加し、プリエンプティブブロックを実行するセキュリティ インテリジェンス ポリシーを追加しながら、不要な接続を選択的に排除するブロックルールがすでにあることを前提としています。

始める前に

このルールを使用するすべての管理対象デバイスに IPS ライセンスを適用する必要があります。

この例では、内部および外部インターフェイスのセキュリティゾーン、および内部ネットワークのネットワークオブジェクトがすでに作成されていることを前提としています。

手順

ステップ 1 侵入ポリシーを適用するアクセス制御ルールを作成します。

a) アクセス コントロール ポリシーの編集時に、[ルールの追加（Add Rule）] をクリックします。

b) ルールに Inside_Outside などのわかりやすい名前を付け、ルールアクションが [許可（Allow）] であることを確認します。

c) [侵入ポリシー（Intrusion policy）] で、[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] を選択します。デフォルトの変数セットを受け入れるか、独自の変数セットを選択してカスタマイズできます。

ほとんどのネットワークでは、[バランスのとれたセキュリティと接続（Balanced Security and Connectivity）]ポリシーが適しています。このポリシーは適度な侵入保護を提供し、過剰にアグレッシブ（ドロップすべきでないトラフィックがドロップされる可能性がある）でもありません。ドロップされるトラフィックが多すぎる場合は、[セキュリティを上回る接続性（Connectivity over Security）]ポリシーを選択することにより、侵入検査を緩和できます。

アグレッシブなセキュリティが必要な場合は、[接続性を上回るセキュリティ（Security over Connectivity）]ポリシーを試してください。[最大検出（Maximum Detection）]ポリシーは、ネットワーク インフラストラクチャ セキュリティをさらに重視したポリシーであり、運用上より大きな影響を及ぼす可能性があります。

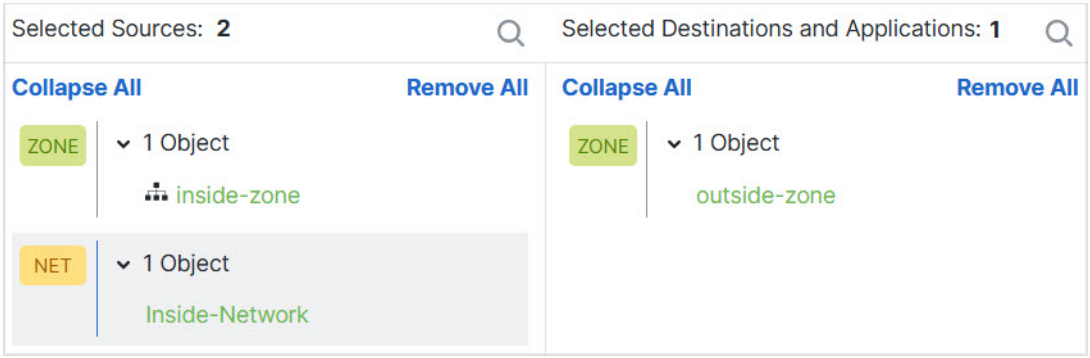
独自のカスタムポリシーを作成する場合は、代わりにそのカスタムポリシーを選択できます。

変数セットの説明は、この例の範囲外です。変数セットとカスタムポリシーの詳細については、侵入ポリシーに関する章をお読みください。

d) [ゾーン（Zones）]タブを選択し、内部セキュリティゾーンを送信元基準に追加し、外部ゾーンを宛先基準に追加します。

e) [ネットワーク（Networks）]タブを選択し、内部ネットワークを定義するネットワークオブジェクトを送信元基準に追加します。

一致基準は次のようになります。



f) [ロギング（Logging）]をクリックし、必要に応じて、接続の開始時または終了時、またはその両方でロギングを有効にします。

g) [適用（Apply）]をクリックしてルールを保存し、[保存（Save）]をクリックして更新されたポリシーを保存します。

h) ルールをアクセス コントロール ポリシーの適切な場所に移動します。

ステップ 2 既知の不正ホストやサイトとの接続を先制的にドロップするためのセキュリティ インテリジェンス ポリシーを設定します。

セキュリティ インテリジェンスを使用して、脅威だとわかっているホストやサイトとの接続をブロックすることで、接続ごとに脅威を特定するためのディープ パケット インスペクション

に必要な時間を節約できます。セキュリティインテリジェンスにより、不必要なトラフィックを早期にブロックして、実際に関心があるトラフィックの処理により多くのシステム時間を残すことができます。

a) アクセス コントロール ポリシーの編集時に、パケットパスで [セキュリティインテリジェンス（Security Intelligence）] リンクをクリックします。

リンクには、上部の DNS ポリシーと下部のセキュリティ インテリジェンス（ネットワークとURL）の2つのポリシーが含まれています。この例では、ネットワークリストとURLリストを設定しています。デフォルトでは、これらのリストにはすでにグローバルブロックリストとブロックしないリストが含まれています。各リストは、項目を追加するまでデフォルトでは空です。

b) **[ネットワーク（Networks）]** を選択し、セキュリティゾーンの **[任意（Any）]** を選択した状態で、グローバルリストと最初のセキュリティ インテリジェンス カテゴリ（おそらく [攻撃者（Attackers）]）が表示されるまで、リストを下にスクロールします。[攻撃者（Attackers）] をクリックし、カテゴリ（おそらく Tor_exit_node）の最後までスクロールし、Shift キーを押した状態でクリックしてすべてのカテゴリを選択します。[ブロックリストに追加（Add to Block List）] をクリックします。

c) [URL] タブとセキュリティゾーンの [任意（Any）] を選択し、Shift キーを押した状態でクリックして同じカテゴリの URL バージョンを選択します。[ブロックリストに追加（Add to Block List）] をクリックします。

d) [保存（Save）] をクリックしてポリシーを保存します。

e) 必要に応じて、ネットワークおよび URL オブジェクトをブロックリストまたはブロックしないリストに追加できます。

[ブロックしない（Do Not Block）] リストは、ホワイトリストではなく、例外リストです。例外リストにあるアドレスや URL がブロックリストにも表示されている場合、そのアドレスや URL の接続はアクセス制御ポリシーの通過を許可されます。

フィードはこのようにしてブロックできますが、後で必要なアドレスやサイトがブロックされていることに気付いた場合は、例外リストを使用して、フィードを完全に削除することなく、そのブロックをオーバーライドできます。

その後、それらの接続はアクセス制御、および侵入ポリシー（設定されている場合）によって評価される点に注意してください。したがって、接続に脅威が含まれている場合は、侵入検査中に特定されてブロックされます。

イベントおよびダッシュボードを使用して、ポリシーによって実際にドロップされているトラフィックを特定し、[ブロックしない（Do Not Block）] リストにアドレスや URL を追加する必要があるかどうかを決めます。

ステップ 3 変更を展開します。

アクセス制御ルールの履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
アクセス制御ルールごとの一致基準の最大オブジェクト数は 200 です。	7.3	任意（Any）	以前は、1 つのアクセス制御ルールの一致基準ごとに最大 50 個のオブジェクトを含めることができました。たとえば、1 つのアクセス制御ルールに最大 50 のネットワークオブジェクトを含めることができます。制限数は、1 つのルールの一致基準ごとに 200 オブジェクトになりました。 増加したオブジェクト制限を許可するようにアクセス コントロール ポリシーを更新しました。
アクセス制御ルールのコメントの検索	6.7	任意（Any）	[検索ルール（Search Rules）]バーに、コメントを検索するオプションが追加されました。 新規/変更されたページ：アクセス制御ルールのページ、[検索ルール（Search Rules）] テキスト入力フィールド。 サポートされているプラットフォーム： Firewall Management Center
アクセスコントロールポリシーとプレフィルタポリシー間のルールのコピーまたは移動	6.7	任意（Any）	あるアクセス コントロール ポリシーから別のアクセス コントロール ポリシーにアクセス制御ルールをコピーできます。また、アクセス制御ルールをアクセス コントロール ポリシーから関連するプレフィルタポリシーに移動できます。 新規/変更されたページ：アクセス コントロール ポリシーのページ。選択したルールの右クリックメニューに、コピーおよび移動するための追加オプションがあります。 サポートされているプラットフォーム： Firewall Management Center
アクセス制御ルールの特定の設定の一括編集	6.6	すべて	ポリシー内のルールのリストで、Shift キーまたは Ctrl キーを押したままクリックして複数のルールを選択し、右クリックしてオプションを選択します。一括操作の例：ルールを有効または無効にしたり、ルールアクションを選択したり、ほとんどの検査とロギングの設定を編集したりできます。 新規/変更されたページ：アクセス制御ルールのページ。 サポートされているプラットフォーム： Firewall Management Center
設定されたルールの強化された検索	6.6	すべて	設定されたルールの強化された検索。 新規/変更されたページ：アクセス制御ルールのページ。 サポートされているプラットフォーム： Firewall Management Center

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
ルール適用の時間範囲	6.6	すべて	適用するルールの絶対時間または反復時間、あるいは時間範囲を指定する機能。このルールは、トラフィックを処理するデバイスのタイムゾーンに基づいて適用されます。 新規/変更されたページ： • アクセス制御の [ルールの追加（Add Rule）] ページの新しいオプション。 • **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [Threat Defense]** ページにある管理対象デバイスのタイムゾーンの指定に関連する新しいオプション。 サポートされているプラットフォーム：Firewall Threat Defense デバイスのみ
アクセス制御ルールページからのオブジェクトの詳細の表示	6.6 以前	任意（Any）	ルールのリストまたはルール設定ダイアログからオブジェクトに関する情報を表示するには、オブジェクトを右クリックします。 新規/変更されたページ：**[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access control）]**、および **[ルールの追加（Add Rule）]** ページ。 サポートされているプラットフォーム： Firewall Management Center

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。