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 ルールの概要

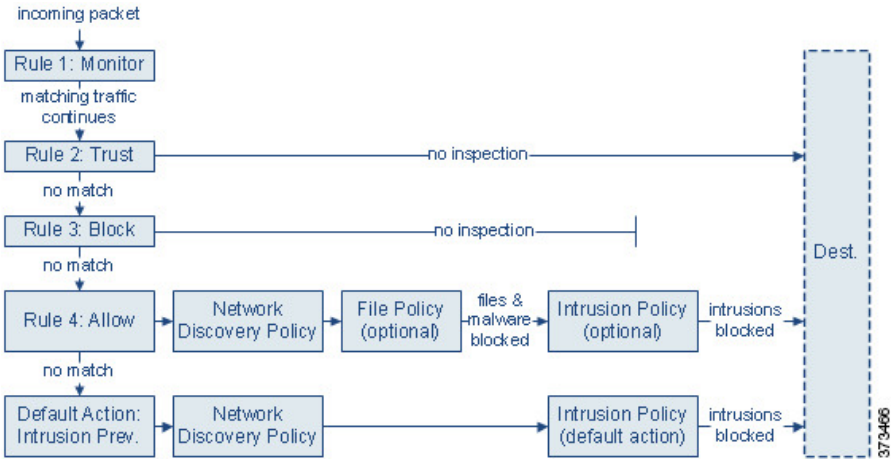
アクセス コントロール ポリシー内では、アクセス コントロール ルールによって複数の管理対象デバイスでネットワーク トラフィックを処理するきめ細かい制御方法が提供されます。

（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。



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 ルールのモニター 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。

- **時間範囲オプション**（[時間範囲（time range）] アイコン [時間範囲（time range）] アイコン）
- [侵入ポリシー（Intrusion policy）]（）
- [ファイルポリシー（File policy）]（）
- [ロギング（Logging）]（）
- [警告（Warning）]（）
- [エラー（Error）]（）
- [ルールの競合（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 エディタを使用します。

：次の操作を実行できます。

- ルール名を設定し、エディタの上部でその配置を選択します。
- エディターの上または下の行を選択して、別のルールの編集に切り替えます。
- 左側のリストを使用してルールアクションを選択し、侵入ポリシーと変数セット、ファイルポリシー、および時間範囲を適用し、ログオプションを設定します。
- ルール名の隣にあるオプションを使用してルールアクションを選択し、侵入ポリシーと変数セット、ファイルポリシー、および時間範囲を適用し、ログオプションを設定します。
- [ソース（Sources）] と [宛先とアプリケーション（Destinations and Applications）] 列を使用して、一致基準を追加します。[すべて（All）]リストからオプションを追加するか、別のタブに移動して、セキュリティゾーンやネットワークなど、必要なタイプのオプションをより簡単に見つけることができます。
- エディタの下部でルールにコメントを追加します。

関連トピック

アクセス コントロール ルールのコンポーネント （4 ページ）
アクセス制御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。モニタルールを除き、トラフィックが一致する最初のルールがそのトラフィックを処理するルールになります。

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

ルールを適用する日時を指定できます。

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

アクセス制御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 （14 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 （15 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
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。

関連トピック

順序付け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 ルールのモニター 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。

注意 ベストプラクティスとして、広範に定義されたモニタールールのレイヤ7の条件をルールの優先順位内で高く設定しないようにすることで、不注意でトラフィックがネットワークに流入することを防ぎます。さらに、ローカルでバインドされているトラフィックがレイヤ3展開のモニタールールに一致する場合、そのトラフィックは検査をバイパスすることがあります。トラフィックのインスペクションを確実に実行するには、トラフィックをルーティングしている管理対象デバイスの詳細設定で [Inspect Local Router Traffic] を有効にします。

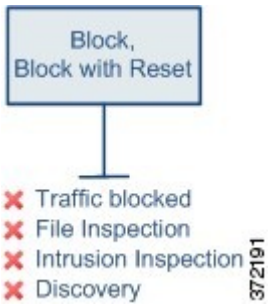
アクセス コントロール ルールの信頼アクション

[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。

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。

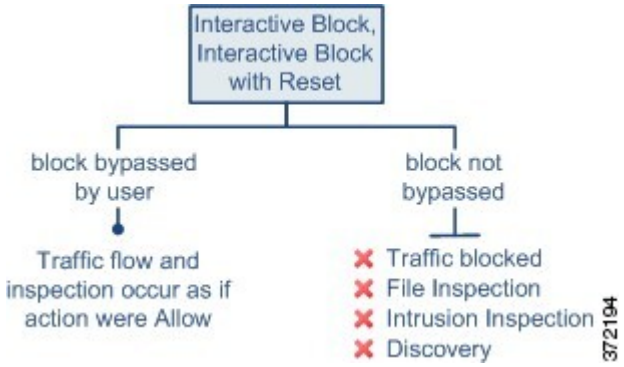
詳細については、HTTP 応答ページの設定を参照してください。

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 インタラクティブ ブロック 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

復号ルールのブロックアクション

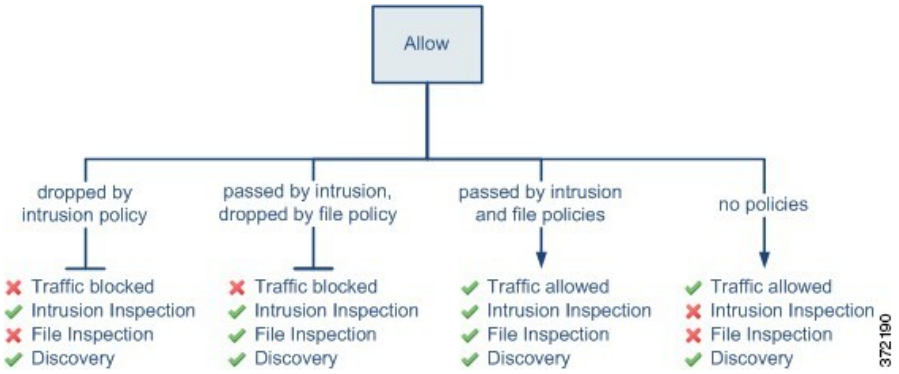
アクセス コントロール ルールの許可アクション

[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。

アクセスコントロールルールの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者
- ネットワーク管理者
- 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。
  - **[ポリシー（Policies）] > [アクセス制御（Access Control）] > [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を選択できます。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。

アクセス制御ルールのガイドラインと制限事項

- 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。

  Threat Defense の場合は、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。

  - DNS応答はスプーフィングされる可能性があるため、完全に信頼できる内部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サーバーが異なるセットのIPアドレスを返す場合があります。したがって、ユーザーが設定したものとは異なる DNS サーバー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。
- 16 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 16 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。

アクセス制御ルール 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、[新規カテゴリの挿入（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。

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、**[編集（Edit）]**（✎） をクリックします。
- 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（Select Action）] 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 [表示（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（Position）]：ルールの位置を指定します。アクセス コントロール ルールの順序（6 ページ）を参照してください。
- [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。
- [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。

- [時間範囲（Time Range）]：（オプション）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。
- [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。詳細については、『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Best Practices for Connection Logging」を参照してください。
- [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 （15 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、[投稿（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。

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

アクセス制御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、一致基準を空のままにします（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。
- アクセスコントロールルールは、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。アクセスコントロール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（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信されかつ宛先 IP アドレスに送信されるトラフィックの照合を行う必要があります。

この条件を追加する場合、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、大陸内のすべての国が選択されます。ルール内で地理的位置を直接選択する以外に、作成した地理位置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） 最新の地理的位置データを使用してトラフィックをフィルタ処理できるように、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強くお勧めします。

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
元のクライアントのネットワーク：なし 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
元のクライアントのネットワーク：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 サーバを使用する場合はブロックします。

送信元ネットワーク：any
元のクライアントのネットワーク：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 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 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

ユーザールール条件では、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。

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）。

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。

アプリケーションルール条件

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（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。

関連トピック

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、適応型プロファイルの設定で説明されているように、アダプティブプロファイルを有効（デフォルト状態）にする必要があります。
- コンテンツ制限を実装している場合は、この手順の代わりに アクセス コントロール ルールを使用したコンテンツ制限の実施 の手順に従ってください。
- 従来型デバイスモデルの場合、これらの条件を設定するには、制御ライセンスが必要です。

手順

ステップ 1 ルール エディタまたは設定エディタを起動します。

- アクセスコントロール、暗号解読、QoS ルール条件：ルールエディタで [アプリケーション（Applications）] をクリックします。
- アイデンティティルール条件：ルールエディタで [レルムおよび設定（Realms & Settings）] をクリックし、アクティブ認証を有効にします。アイデンティティ ルールの作成を参照してください。
- アプリケーション フィルタ：オブジェクト マネージャの [アプリケーション フィルタ（Application Filters）] ページで、アプリケーション フィルタを追加または編集します。フィルタの一意の**名前**を指定します。
- インテリジェント アプリケーション バイパス（IAB）：アクセス コントロール ポリシー エディタで [詳細（Advanced）] をクリックし、IAB の設定を編集して、[バイパス可能なアプリケーションおよびフィルタ（Bypassable Applications and Filters）] をクリックします。

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 [情報（Information）]（  ）をクリックします。**ロック解除**は、システムが復号されたトラフィックでのみ識別できるアプリケーションを示します。

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、[フィルタのクリア（Clear Filters）] 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、一致基準を空のままにします（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（FTD 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。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、URL フィルタリングを参照してください。

ダイナミック属性のルール条件

ダイナミック属性には次のものがあります。

- ダイナミックオブジェクト（Cisco Secure 動的属性コネクタ からのものなど）

  動的属性コネクタ 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 Firepower Management Center に送信して、アクセスコントロールルールで使用できるようにします。。

  動的属性コネクタ の詳細については、Cisco Secure 動的属性コネクタ コンフィギュレーション ガイドを参照してください。

- SGT オブジェクト
- ロケーション IP オブジェクト
- 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

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。

API で作成したダイナミックオブジェクトについて

ダイナミックオブジェクトは、REST API コールを使用するか、クラウドソースから IP アドレスを更新できる Cisco Secure 動的属性コネクタ を使用して取得した 1 つまたは複数の IP アドレスを指定するオブジェクトです。これらのダイナミックオブジェクトは、後でアクセス コントロール ポリシーを展開することなく、アクセス制御ルールで使用できます。

動的属性コネクタ の詳細については、『*Cisco Secure Dynamic Attributes Configuration Guide*』（ガイドへのリンク）を参照してください。https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/dynamic-attributes-connector/200/cisco-secure-dynamic-attributes-connector-v200.html

ダイナミックオブジェクトとネットワークオブジェクトの違いは次のとおりです。

- 動的属性コネクタを使用して作成したダイナミックオブジェクトは、作成されるとすぐに Management Center にプッシュされ、定期的に更新されます。
- API によって作成されたダイナミックオブジェクト：
  - Classless Inter-Domain Routing（CIDR）の有無にかかわらず、ネットワークオブジェクト同様にアクセスコントロールルールで使用できる IP アドレス。

- 完全修飾ドメイン名またはアドレス範囲をサポートしていません。
- API を使用して更新する必要があります。

関連トピック

API で作成したダイナミックオブジェクトの追加または編集

ダイナミック属性の条件の設定

アクセス制御ルールにダイナミック属性を設定すると、同じタイプのオブジェクトは OR 結合され、異なるタイプのオブジェクトは AND 結合されます。このトピックの最後に例を示します。

（注） この手順は、レガシー UI に基づいています。[新しいUIレイアウト（New UI Layout）] では、[送信元（Sources）]、[宛先とアプリケーション（Destinations and Applications）] フィールドの **Add** ( ) をクリックして、ダイナミック属性を追加できます。

始める前に

複数の動的オブジェクトを作成し、アクセス コントロール ポリシーでの動的オブジェクトの使用方法を理解します。

動的オブジェクトの詳細については、API で作成したダイナミックオブジェクトについてを参照してください。

アクセスコントロールポリシーでのダイナミックオブジェクトの詳しい使用方法については、ダイナミック属性のルール条件 （24 ページ）を参照してください。

手順

ステップ 1 ルールエディタで [Dynamic Attributes] をクリックします。

ステップ 2 [Available Attributes] セクションで、次のいずれかを実行します。

- フィールドに属性の名前の一部またはすべてを入力します。
- [Security Group Tag] または [Dynamic Objects] をクリックして、そのタイプのオブジェクトのみを表示します。

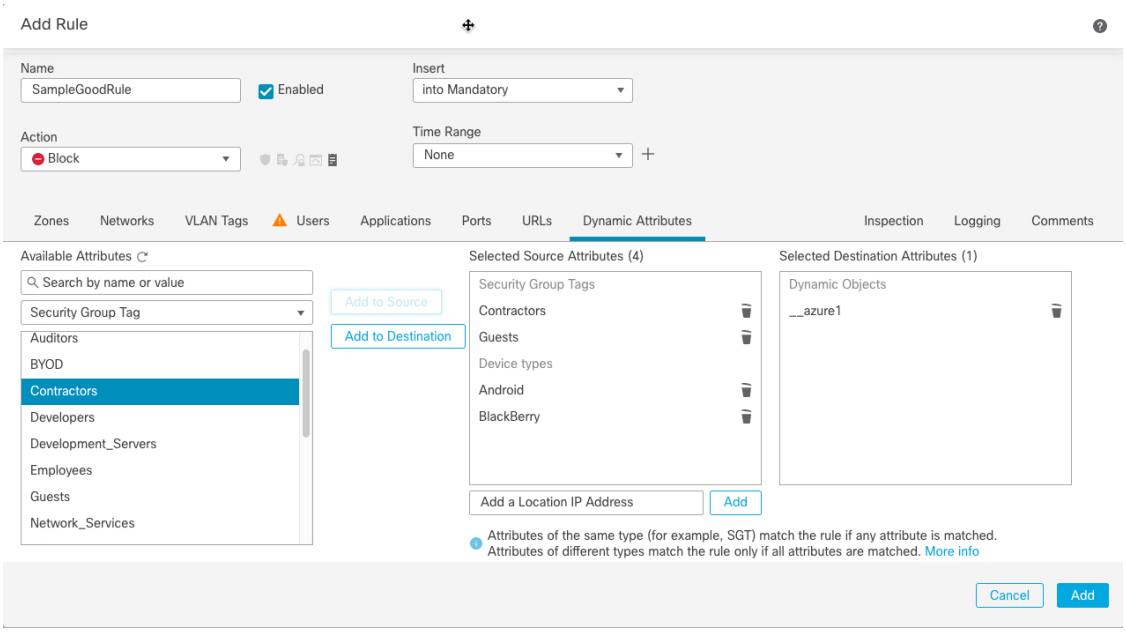
ステップ 3 選択したオブジェクトを送信元の一致基準に適用するには、[Add to Source] をクリックします。

ステップ 4 選択したオブジェクトを宛先の一致基準に適用するには、[Add to Destination] をクリックします。

ステップ 5 ルールの設定を終了したら、[Save] をクリックします。

例：ブロックルールでの複数の送信元条件の使用

次の例では、セキュリティグループタグの契約業者またはゲストからのトラフィックがブロックされ、デバイスタイプ Android または Blackberry が動的オブジェクト **__azure1** にアクセスできなくなります。



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。

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、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 [表示（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。

アクセス コントロール ポリシー間でのアクセス コントロール ルールのコピー

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、[別のポリシーにコピー（Copy 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 [別のポリシーにコピー（Copy 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）
リセットしてブロック（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）

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
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。
ブロック（Block）	• 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
リセットしてブロック（Block with reset）	• 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
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
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、[プレフィルタポリシーに移動（Move 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 [プレフィルタポリシーに移動（Move 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。

- ルールの最後のセットとして配置するには、[最下部に配置（At the bottom）] を選択します。
- ルールの最初のセットとして配置するには、[最上部に配置（At the top）] を選択します。

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 ルールの配置

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

アクセス制御ルールのベストプラクティス 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。
- 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 ルールを移動またはルールを挿入する場所を選択します。

- [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、[移動（Move）] または [確認（Confirm）] をクリックし、ルールを保存します。

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。

アクセス制御ルールへのコメントの追加

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 プラットフォームか、企業ネットワークの内部および外部で転送として Web プロトコルを使用するリッチ メディア アプリケーションかにかかわらず、Web は企業内でアプリケーションを配信するユビキタス プラットフォームになっています。

Threat Defense では、接続のインスペクションを実行して、使用するアプリケーションを決定します。これにより、特定の TCP/UDP ポートをターゲットにするのではなく、アプリケーションをターゲットとしたアクセス コントロール ルールを記述できるようになります。したがって、Web ベース アプリケーションが同じポートを使用していても、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許可またはブロックするよう選択できますが、タイプ、カテゴリ、タグ、リスク、またはビジネスとの関連性に基づいて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、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にアプリケーション ディテクタを更新し追加しています。そのため、手動でルールを更新することなく、高リスクのアプリケーションをブロックするルールを新しいアプリケーションに自動的に適用できます。

この使用例では、[アノニマイザー/プロキシ（anonymizer/proxy）] カテゴリに属するアプリケーションをブロックします。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス制御（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。

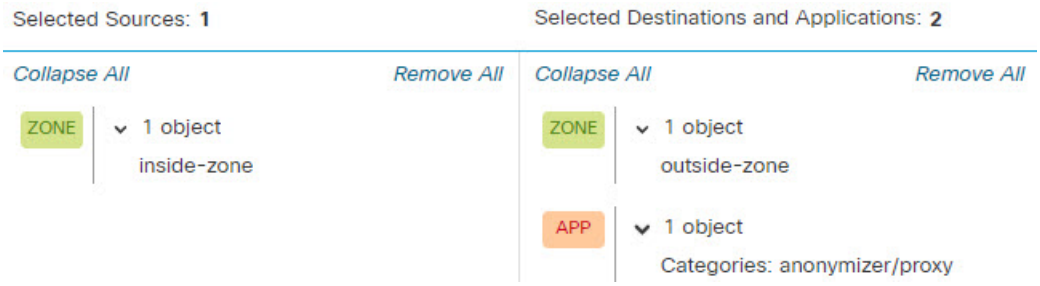
c) ゾーンが設定されており、このルールを内部から外部へのトラフィックに適用する場合は、[ゾーン（Zones）] タブを選択して、内部ゾーンを送信元ゾーンとして選択し、外部ゾーンを宛先ゾーンとして選択します。

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。記述したルールは、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 の更新で変更できることを覚えておいてください。

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なものになります。



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 コントロール ルールに追加することによって、次世代侵入防御システム（IPS）の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

分析して、トラフィックの内容を既知の脅威と比較します。接続がモニタリング中の脅威と一致した場合、システムはその接続をドロップして攻撃を阻止します。

その他すべてのトラフィックの処理は、ネットワーク トラフィックに侵入の形跡がないかどうかを調べる前に実行されます。侵入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 ポリシーを使用してトラフィックのインスペクションを実行するよう、システムに指示できます。

トラフィックのみを [許可（allow）] するルールに侵入ポリシーを設定できます。インスペクションは、トラフィックを [信頼（trust）] または [ブロック（block）] するよう設定されたルールでは実行されません。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。

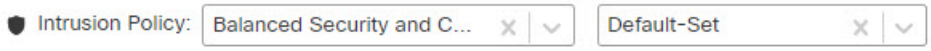
[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ポリシーは、ほとんどのネットワークに適しています。ドロップしたくないトラフィックをドロップする可能性がある、過度に強力な防御ではなく、侵入に対する適切な防御を実現しま

す。ドロップされるトラフィックが多すぎると判断した場合は、[セキュリティより接続を優先する（Connectivity over Security）] ポリシーを選択することによって侵入インスペクションを緩和できます。

セキュリティを強力にする必要がある場合は、[接続性よりもセキュリティを優先（Security over Connectivity）] ポリシーを試します。[最大検出（Maximum Detection）] ポリシーでは、ネットワークインフラストラクチャのセキュリティがよりいっそう重視され、動作にさらに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。

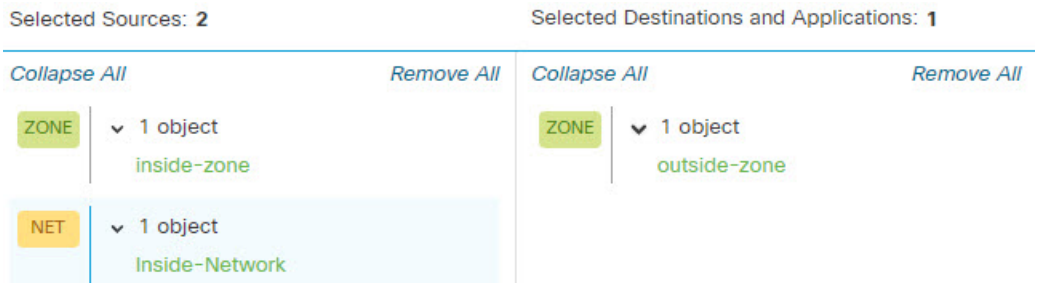
変数セットの説明は、この例の範囲外です。変数セットとカスタムポリシーの詳細については、侵入ポリシーに関する章をお読みください。



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 コントロール 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。

QUIC トラフィックのブロック方法

ベストプラクティスとして、QUIC トラフィックをブロックすることをお勧めします。Chrome ブラウザでは、QUIC プロトコルがデフォルトで有効になっています。Chrome ブラウザを使用して Google アプリケーションにアクセスしようとすると、TLS/SSL の代わりに QUIC プロトコルを使用して Google サーバーへのセッションが確立されます。QUIC は開発の初期段階にある実験的なプロトコルであり、独自の暗号化方式を使用します。

Hypertext Transfer Protocol Secure （HTTPS）は、Hypertext Transfer Protocol（HTTP）と同様に、Transmission Control Protocol（TCP）を使用します。Transmission Control Protocol は、コネクション型またはステートフルです。HTTPS は TCP ポート 443 を使用し、HTTP は TCP ポート 80 を

使用します。HTTP/3 は QUIC プロトコルで動作します。QUIC の場合、HTTP/3 は TCP ではなく User Datagram Protocol（UDP）に依存します。

QUIC は、意図せずネットワークセキュリティに悪影響を与える可能性があります。ファイアウォールやネットワークセンサーなどのセキュリティアプライアンスは、通常、レガシー TCP セッションでアクセスできる情報にアクセスできません。QUIC トラフィックがファイアウォールによってブロックされると、Chrome ブラウザは従来の TLS/SSL の使用にフォールバックします。これによってブラウザの機能が失われることはありません。SSL 復号が有効になっているかどうかにかかわらず、ファイアウォールによる Google アプリケーションの可視性と制御が向上します。したがって、QUIC トラフィックは適切に調査されず、ファイアウォールの Web 保護機能に転送されません。

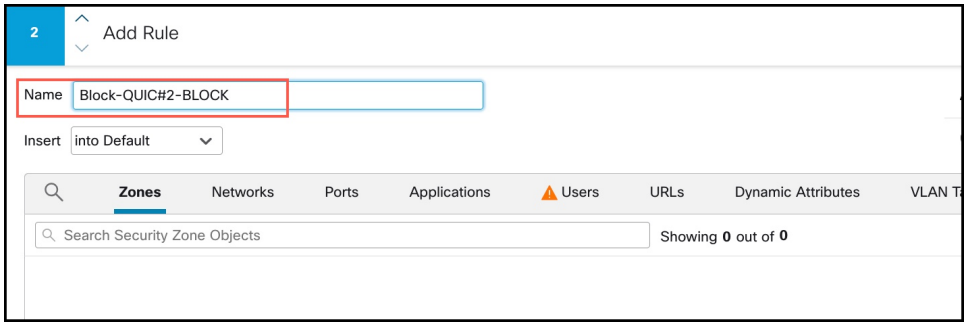
この使用例では、アクセス制御ルールを作成して QUIC および HTTP/3 トラフィックをブロックする方法を示します。

手順

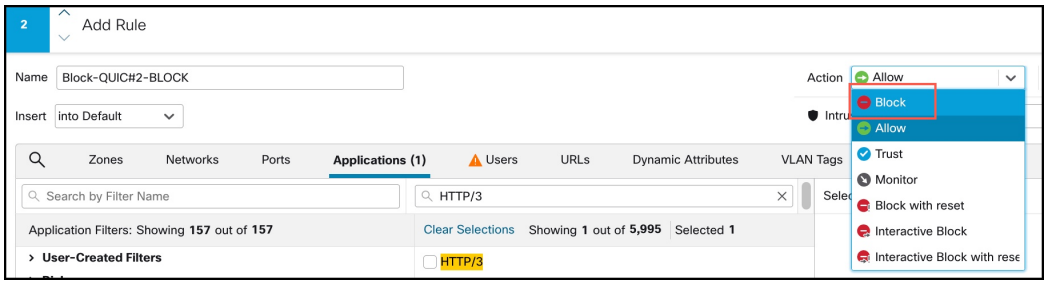
ステップ 1 **[ポリシー（Policies）] > [アクセス制御（Access Control）]** を選択し、アクセス コントロール ポリシーを編集します。

ステップ 2 [ルールの追加（Add Rule）] をクリックします。

ステップ 3 ルールにわかりやすい名前（Block-QUIC など）を入力します。

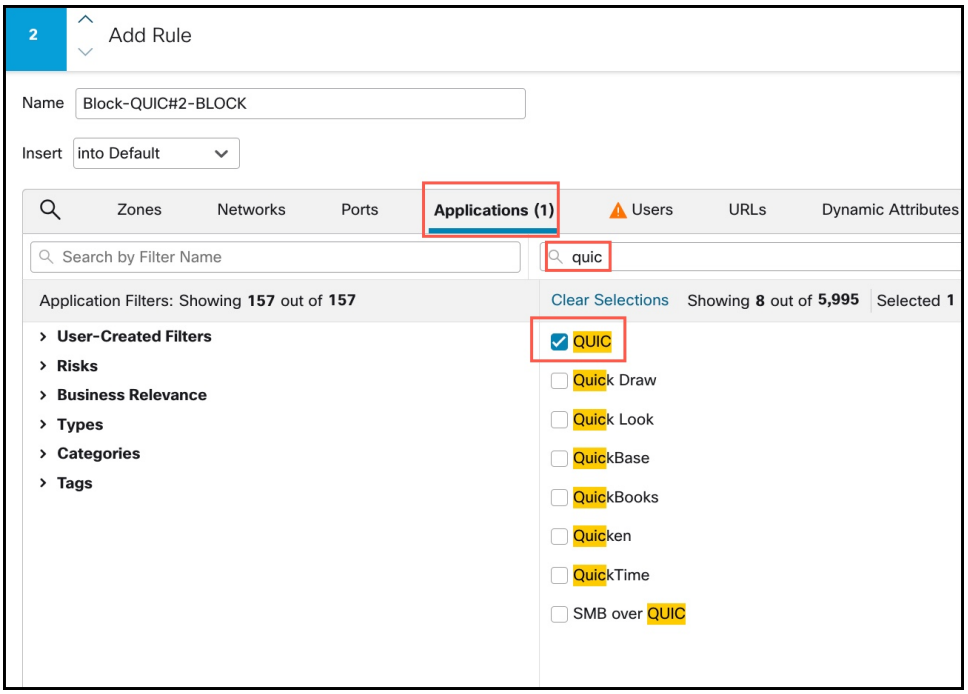


ステップ 4 [アクション（Actions）] ドロップダウンリストから、[ブロック（Block）] を選択します。

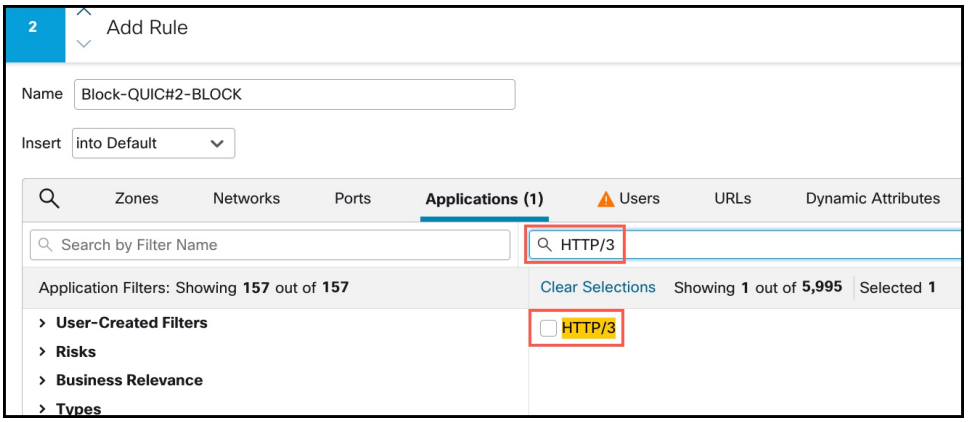


ステップ 5 [アプリケーション（Applications）] タブをクリックします。

ステップ 6 検索ボックスで「quic」を検索し、QUIC アプリケーションのチェックボックスをオンにします。



ステップ 7 検索ボックスで「HTTP/3」を検索し、HTTP/3 のチェックボックスをオンにします。



ステップ 8 [アプリケーションの追加（Add Application）] をクリックして、接続先とアプリケーションに追加します。

ステップ 9 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。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 10 [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。

ステップ 11 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 12 変更を展開します。

アクセス制御ルールの履歴

機能	最小 Management Center	最小 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： 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： Management Center
アクセス制御ルールの特定の設定の一括編集	6.6	任意（Any）	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： Management Center
設定されたルールの強化された検索	6.6	任意（Any）	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： Management Center

機能	最小 Management Center	最小 Threat Defense	詳細
ルール適用の時間範囲	6.6	任意（Any）	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：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： 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。