プレフィルタリングおよびプレフィルタポリシー

- プレフィルタリングについて （1 ページ）
- Fastpath プレフィルタリングのベストプラクティス （7 ページ）
- カプセル化されたトラフィックの処理のベストプラクティス （8 ページ）
- プレフィルタポリシーの要件と前提条件 （9 ページ）
- プレフィルタリングの設定 （10 ページ）
- トンネル ゾーンおよびプレフィルタリング （17 ページ）
- プレフィルタルールのアクセス コントロール ポリシーへの移動 （21 ページ）
- プレフィルタ ポリシーのヒット カウント （23 ページ）
- 大規模フローのオフロード （23 ページ）
- プレフィルタリングの履歴 （27 ページ）

プレフィルタリングについて

プレフィルタはアクセス制御の最初のフェーズで、システムがより大きいリソース消費の評価を実行する前に行われます。プレフィルタリングはシンプルかつ高速で、初期に実行されます。プレフィルタリングでは、限定された外部ヘッダーを基準にしてトラフィックを迅速に処理します。内部ヘッダーを使用し、より堅牢なインスペクション機能を備えた後続の評価とこのプレフィルタリングを比較します。

次の目的でプレフィルタリングを設定します。

- パフォーマンスの向上：インスペクションを必要としないトラフィックの除外は、早ければ早いほど適切です。特定のタイプのプレーン テキストをファストパスまたはブロックし、カプセル化された接続を検査することなく外側のカプセル化ヘッダーに基づいてトンネルをパススルーします。早期処理のメリットがあるその他の接続についても、ファストパスやブロックをすることができます。
- カプセル化トラフィックに合わせたディープインスペクションの調整：同じ検査基準を使用してカプセル化接続を後で処理できるように、特定のタイプのトンネルを再区分できま

す。アクセス制御はプレフィルタ後に内側のヘッダーを使用するため、再区分は必須です。

プレフィルタ ポリシーについて

プレフィルタリングは、ポリシーベースの機能です。デバイスに割り当てるには、そのデバイスに割り当てられているアクセス コントロール ポリシーに割り当てます。

ポリシー コンポーネント：ルールとデフォルト アクション

プレフィルタ ポリシーでは、トンネル ルール、プレフィルタ ルール、デフォルト アクションに基づいてネットワーク トラフィックを処理します。

- トンネル ルールとプレフィルタ ルール：最初にプレフィルタ ポリシーのルールが、指定した順序でトラフィックを処理します。トンネル ルールは指定のトンネルのみを照合するもので、再ゾーニングをサポートします。プレフィルタ ルールはより広範囲の制約を設けるもので、再ゾーニングをサポートしていません。詳細については、トンネルとプレフィルタのルール （3 ページ）を参照してください。
- デフォルト アクション（トンネルのみ）：トンネルがどのルールとも一致しない場合は、デフォルト アクションによって処理されます。デフォルト アクションは、そのトンネルをブロックするか、あるいは個々のカプセル化された接続のアクセス制御を継続します。デフォルト アクションでトンネルの再ゾーニングを行うことはできません。

  カプセル化されていないトラフィックに対するデフォルト アクションはありません。カプセル化されていない接続がどのプレフィルタ ルールにも一致しない場合、システムはアクセス制御を継続します。

接続ロギング

プレフィルタポリシーで FastPath された接続およびブロックされた接続のログを記録できます。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「*Other Connections You Can Log*」を参照してください。

接続イベントには、すべてのトンネルを含め、ロギングされる接続がプレフィルタ処理されるのかどうか、また、どのようなプレフィルタ処理を行うのかに関する情報が含まれています。この情報は、イベント表示（ワークフロー）、ダッシュボード、およびレポートで表示することができ、相関基準として使用できます。FastPath された接続やブロックされた接続は、ディープインスペクションの対象外であるため、これらの接続に関連する接続イベントに含まれる情報は限定的となります。

デフォルト プレフィルタ ポリシー

すべてのアクセス コントロール ポリシーにプレフィルタ ポリシーが関連付けられています。

カスタム プレフィルタリングを設定しなければ、システムはデフォルト ポリシーを使用します。このシステム提供のポリシーの初期設定では、すべてのトラフィックをアクセス制御の次

のフェーズに渡します。デフォルト ポリシーのデフォルト アクションを変更し、ロギングのオプションを設定することはできますが、ルールの追加や削除はできません。

プレフィルタ ポリシーの継承とマルチテナンシー

アクセス制御は、マルチテナンシーを補完する階層型実装となっています。プレフィルタ ポリシーの関連付けは、その他の詳細設定と同様にロックすることが可能で、これによりすべての子孫アクセス コントロール ポリシーでこの関連付けが強制的に継承されます。詳細については、アクセス コントロール ポリシーの継承を参照してください。

トンネルとプレフィルタのルール

トンネルとプレフィルタのどちらのルールを設定するかは、照合するトラフィックのタイプと、実行するアクションや詳細な分析によって異なります。

特性	トンネル ルール	プレフィルタ ルール
主な機能	プレーンテキストのパススルートンネルをすばやく fastpath、ブロック、または再ゾーニングします。	初期段階の操作の影響を受ける他の接続をすばやく高速パス化またはブロックします。
カプセル化とポート/プロトコル条件	カプセル化の条件は、カプセル化ルールの条件 （17 ページ） にリストされる選択済みプロトコルについて、プレーンテキスト トンネルのみと照合されます。	ポート条件では、トンネル ルールより広範囲のポートおよびプロトコル制約を使用できます。ポート、プロトコル、および ICMP コードルールの条件を参照してください。
ネットワーク条件	トンネル エンドポイント条件は、処理対象にするトンネルのエンドポイントを制約します。ネットワークルール条件を参照してください。	ネットワーク条件は、各接続の送信元ホストと宛先ホストを制約します。ネットワークルール条件を参照してください。
方向（Direction）	双方向または単方向（構成可）。 トンネル ルールはデフォルトで双方向であるため、トンネル エンドポイント間のすべてのトラフィックを処理できます。	単方向のみ（構成不可）。 プレフィルタ ルールは、送信元から宛先へ送信されるトラフィックのみと照合されます。許可された接続のリターントラフィックも許可されます。
詳細分析のためのセッションの再ゾーニング	トンネル ゾーンを使用する場合にサポートされます。トンネル ゾーンおよびプレフィルタリング （17 ページ）を参照してください。	サポート対象外。

プレフィルタリングとアクセス コントロール

プレフィルタとアクセスコントロールポリシーのどちらを使用しても、トラフィックをブロックしたり信頼したりできますが、プレフィルタリングの「信頼」機能の方がより多くのインスペクションをスキップするため、「高速パス」と呼ばれます。次の表ではこれについて説明し、プレフィルタリングとアクセスコントロールのその他の違いを示します。これは、カスタム プレフィルタリングを設定するかどうかの決定に役立ちます。

カスタム プレフィルタリングを設定しない場合は、アクセス コントロール ポリシーに初期に配置されたブロックおよび信頼ルールにより、プレフィルタ機能に近づけることのみ可能です（複製するのではなく）。

特性	プレフィルタリング	アクセス制御	詳細
主な機能	特定のタイプのプレーンテキストのパススルートンネル（カプセル化ルールの条件 （17 ページ）を参照）を迅速に高速パス処理またはブロックしたり、後続のインスペクションをそのカプセル化されたトラフィックに適合させたりします。 早期処理による利点が得られる他の接続を高速パス処理またはブロックします。	コンテキスト情報やディープインスペクションの結果など、単純または複雑な基準を使用して、すべてのネットワーク トラフィックを検査および制御します。	プレフィルタリングについて （1 ページ）
実装	プレフィルタ ポリシー プレフィルタ ポリシーは、アクセス コントロール ポリシーによって呼び出されます。	アクセス コントロール ポリシー アクセス コントロール ポリシーがメインの構成です。サブポリシーの呼び出しに加えて、アクセス コントロール ポリシーの独自のルールがあります。	プレフィルタ ポリシーについて （2 ページ） アクセス制御への他のポリシーの関連付け
アクセス コントロール内のシーケンス	最初。 トラフィックは、他のすべてのアクセスコントロール構成の前にプレフィルタ基準と照合されます。	—	—

特性	プレフィルタリング	アクセス制御	詳細
ルール アクション	少ない。 追加のインスペクションを停止したり（高速パス処理とブロック）、他のアクセス コントロールによる追加の分析を許可したり（分析）できます。	多い。 アクセス コントロール ルールには、モニタリング、ディープ インスペクション、リセットしてブロック、インタラクティブ ブロッキングなどのさまざまなアクションがあります。	トンネルとプレフィルタ ルールのコンポーネント （12 ページ） アクセス コントロール ルールのアクション
バイパス機能	高速パス ルール アクション。 プレフィルタ段階のトラフィックの高速パス処理では、その後のすべてのインスペクションと次のような処理をバイパスします。 • セキュリティ インテリジェンス • アイデンティティ ポリシーによって課される認証要件 • SSL 復号 • アクセス コントロール ルール • パケット ペイロードのディープ インスペクション • 検出 • レート制限	信頼ルール アクション。 アクセス コントロール ルールによって信頼されるトラフィックのみがディープ インスペクションとディスカバリを免除されます。	アクセス コントロール ルールの概要
ルール基準	制限。 プレフィルタ ポリシーのルールでは、単純なネットワーク基準、つまり IP アドレス、VLAN タグ、ポート、およびプロトコルを使用します。 トンネルについては、トンネル エンドポイント条件によって、トンネルの両側にあるネットワーク デバイスのルーテッド インターフェイスの IP アドレスを指定します。	堅牢。 アクセス コントロール ルールでは、ネットワーク基準を使用しますが、パケット ペイロードで使用できるユーザ、アプリケーション、要求された URL、およびその他のコンテキスト情報も使用します。 ネットワーク条件によって、送信元と宛先ホストの IP アドレスが指定されます。	トンネルとプレフィルタのルール （3 ページ） プレフィルタルール条件 （14 ページ） トンネルルール条件 （16 ページ）

特性	プレフィルタリング	アクセス制御	詳細
IP ヘッダーの使用（トンネル処理）	最も外側。 外部ヘッダーを使用して、プレーンテキストのパススルー トンネル全体を処理できます。 カプセル化されていないトラフィックについては、プレフィルタリングで引き続き「外部」ヘッダーが使用され、この場合は唯一のヘッダーになります。	可能な限り内側。 カプセル化されていないトンネルについては、アクセス コントロールは、トンネル全体ではなく、個々のカプセル化された接続に適用されます。	パススルー トンネルとアクセス制御 （6 ページ）
さらに分析するためのカプセル化された接続の再ゾーン化	トンネルされたトラフィックを再ゾーン化します。 トンネルゾーンにより、後続のインスペクションをプレフィルタされたカプセル化トラフィックに適合させることができます。	トンネル ゾーンを使用。 アクセス コントロールでは、プレフィルタリング中に割り当てたトンネル ゾーンを使用します。	トンネル ゾーンおよびプレフィルタリング （17 ページ）
接続のロギング	高速パス処理およびブロックされたトラフィックのみ。許可された接続は、他の構成によってログに記録されることがあります。	任意の接続。	Cisco Secure Firewall Management Center アドミニストレーション ガイドの「ログ可能なその他の接続」
サポートされるデバイス	Secure Firewall Threat Defense のみ。	すべて。	—

パススルー トンネルとアクセス制御

プレーンテキスト（暗号化されていない）トンネルでは、複数の接続をカプセル化できます。これらのトンネルは、多くの場合、連続していないネットワーク間をつなぎます。したがって、IP ネットワークでカスタム プロトコルをルーティングする場合や、IPv4 ネットワークで IPv6 トラフィックをルーティングする場合などには特に役立ちます。

外側のカプセル化ヘッダーには、トンネル エンドポイント（トンネルのいずれかの側にあるネットワーク デバイスのルーテッド インターフェイス）の送信元と宛先の IP アドレスが指定されます。内側のペイロードヘッダーには、カプセル化された接続の実際のエンドポイントの送信元と宛先の IP アドレスが指定されます。

通常、ネットワーク セキュリティ デバイスは、プレーンテキスト トンネルをパススルー トラフィックとして扱います。つまり、ネットワーク セキュリティ デバイスはトンネル エンドポイントのうちの 1 つではないということです。代わりに、ネットワーク セキュリティ デバイ

スはトンネルエンドポイントの間に展開されて、それらのエンドポイント間を流れるトラフィックをモニタします。

一部のネットワーク セキュリティ デバイスは、外部 IP ヘッダーを使用してセキュリティポリシーを適用します。プレーン テキスト トンネルの場合でも、これらのデバイスはカプセル化された個々の接続とそのペイロードを制御したりその内容を把握したりすることはできません。

それとは対照的に、システムは以下のようにアクセス制御を活用します。

- 外側のヘッダーの評価：まず、プレフィルタで外側のヘッダーを使用してトラフィックを処理します。この段階で、プレーン テキストのパススルー トンネル全体をブロックすることも、FastPath を適用することもできます。
- 内側のヘッダーの評価：次に、アクセス制御の残り（および QoS などのその他の機能）では、最も内側にあるヘッダーの検出可能レベルを使用して、可能な限り詳細なレベルでインスペクションと処理が行われるようにします。

  パススルー トンネルが暗号化されていなければ、システムはこの段階で、カプセル化された個々の接続に対処します。カプセル化されたすべての接続に対処するには、トンネルの再ゾーン分割（トンネル ゾーンおよびプレフィルタリング （17 ページ）を参照）を行う必要があります。

アクセス制御では、暗号化されたパススルー トンネルの内容を把握しません。たとえば、アクセス制御ルールは、パススルー VPN トンネルを 1 つの接続と見なします。システムは外側のカプセル化ヘッダーに含まれる情報だけを使用して、トンネル全体を処理します。

Fastpath プレフィルタリングのベストプラクティス

プレフィルタルールで fastpath アクションを使用すると、一致するトラフィックは検査をバイパスし、単にデバイスを介して送信されます。このアクションは、信頼できるトラフィックと、利用可能などのセキュリティ機能でもメリットを得られないトラフィックに使用してください。

次のタイプのトラフィックは、fastpath アクションに最適です。たとえば、エンドポイントまたはサーバーの IP アドレスに対して送受信されるトラフィックの fastpath のルールを設定できます。使用するポートに基づいてルールをさらに制限できます。

- デバイスを通過する VPN トラフィック。つまり、このデバイスは VPN トポロジのエンドポイントではありません。
- スキャナのトラフィック。スキャナプローブにより、侵入ポリシーから多くの誤検知応答が発生する可能性があります。
- 音声/ビデオ。
- バックアップ。
- Threat Defense デバイスを通過する管理トラフィック（sftunnel）。（アクセス コントロール ポリシーを使用して）管理トラフィックでディープインスペクションを実行すると、問

題が発生する可能性があります。管理センターと管理対象デバイス間のポート TCP/8305 に基づいてプレフィルタリングできます。

カプセル化されたトラフィックの処理のベストプラクティス

このトピックでは、カプセル化されたトラフィックの次のタイプについてガイドラインを説明します。

- Generic Routing Encapsulation (GRE)
- Point-to-Point Tunneling Protocol（PPTP）
- IPinIP
- IPv6inIP
- Teredo

GRE トンネルの制限事項

GRE トンネル処理は、IPv4 および IPv6 のパッセンジャーフローに限定されます。PPTP や WCCP などの他のプロトコルは、GRE トンネル内ではサポートされません。

管理対象デバイスの Snort バージョンサポートについて

管理対象デバイスで使用されるインスペクションエンジンは、Snort と呼ばれます。Snort 3 は Snort 2 よりも多くの機能をサポートしています。これらがネットワーク上の管理対象デバイスにどのように影響するかを理解するには、次のことを知っておく必要があります。

- デバイスがサポートする Snort のバージョン

  Snort のバージョンサポートは、『*Cisco Firepower Compatibility Guide*』のバンドルされたコンポーネントに関するセクションで確認することができます。

- Management Center および Threat Defense ソフトウェアが Snort 2 および Snort 3 をサポートする方法

  Snort 2 および Snort 3 の制約事項については、『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』の「Management Center の Snort 3 機能の制約事項 - Managed Threat Defense 」トピックを参照してください。

GRE v1 および PPTP による外部フロー処理のバイパス

GRE v1（ステートフル GRE とも呼ばれる）および PPTP トラフィックは、外部フロー処理をバイパスします。

パッセンジャフロー処理は IPv6inIP および Teredo でサポートされていますが、次の制限が適用されます。

- セッションは、ロードバランシングされていない単一のトンネルを経由する
- HA またはクラスタリング レプリケーションがない
- プライマリフローとセカンダリフローの関係は維持されない
- プレフィルタポリシーのホワイトリストとブラックリストはサポートされない

GRE v0 シーケンス番号フィールドはオプションである必要がある

ネットワーク上でトラフィックを送信するすべてのエンドポイントは、オプションとしてシーケンス番号フィールドを使用して GREv0 トラフィックを送信する必要があります。それ以外の場合、シーケンス番号フィールドは削除されます。RFC 1701 と RFC 2784 はどちらも、シーケンスフィールドをオプションとして指定しています。

トンネルがインターフェイスで機能する方法

プレフィルタおよびアクセスコントロールポリシールールは、ルーテッドインターフェイス、トランスペアレントインターフェイス、インラインセットインターフェイス、インラインタップインターフェイス、およびパッシブインターフェイスのすべてのトンネルタイプに適用されます。

参考資料

GRE および PPTP プロトコルの詳細については、以下を参照してください。

- RFC 1701、RFC 2784、および RFC 2890（GRE プロトコル v0）
- RFC 2637（PPTP および GRE プロトコル v1）

プレフィルタポリシーの要件と前提条件

モデルのサポート

Threat Defense

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

プレフィルタリングの設定

カスタムプレフィルタリングを実行するには、プレフィルタポリシーを設定し、そのポリシーをアクセス コントロール ポリシーに割り当てます。管理対象デバイスへのプレフィルタポリシーの割り当ては、アクセス コントロール ポリシーを介して行われます。

ポリシーの編集は、1 つのブラウザウィンドウを使用して、一度に 1 人のみで行う必要があります。複数のユーザが同じポリシーを保存した場合は、最後に保存された変更が保持されます。ユーザにとっての便宜性を考慮して、各ポリシーを現在編集している人（いる場合）の情報が表示されます。セッションのプライバシーを保護するために、ポリシーエディタが非アクティブになってから 30 分後に警告が表示されます。60 分後には、システムにより変更が破棄されます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[プレフィルタ（Prefilter）]**を選択します。

ステップ 2 [新しいポリシー（New Policy）] をクリックして、カスタム プレフィルタ ポリシーを作成します。

新しいプレフィルタ ポリシーには、ルールや、すべてのトンネル トラフィックを分析するデフォルト アクションはありません。新しいプレフィルタ ポリシーでは、ロギングやトンネルの再ゾーン分割は実行されません。既存のポリシーを [コピー（Copy）]（  ） または **[編集（Edit）]**（） することもできます。

ステップ 3 プレフィルタ ポリシーのデフォルト アクションとそのロギング オプションを設定します。

- デフォルトアクション：サポートされるプレーンテキスト、パススルー トンネルのデフォルト アクションを選択します。[すべてのトンネル トラフィックを分析（Analyze all tunnel traffic）]（アクセス コントロールあり）または [すべてのトンネル トラフィックをブロック（Block all tunnel traffic）]。
- デフォルトアクションのロギング：デフォルトアクションの横にある [ロギング（Logging）]（  ）をクリックします。『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「Logging Connections with a Policy Default Action」を参照してください。デフォルトアクションのロギングは、ブロックされたトンネルに対してのみ設定できます。

ステップ 4 トンネルおよびプレフィルタ ルールを設定します。

カスタム プレフィルタ ポリシーでは、両方の種類のルールを任意の順序で使用できます。照合する特定のタイプのトラフィックおよび実行するアクションまたは追加の分析に応じてルールを作成します。トンネルとプレフィルタのルール （3 ページ）を参照してください。

注意 トンネル ルールを使用してトンネル ゾーンを割り当てる場合は、注意してください。再ゾーン分割されたトンネルでの接続は、後の評価でセキュリティ ゾーンの制約に一致しない可能性があります。詳細については、トンネル ゾーンおよびプレフィルタリング（17 ページ）を参照してください。

ルールコンポーネントの設定の詳細については、「トンネルとプレフィルタ ルールのコンポーネント （12 ページ）」を参照してください。

ステップ 5 ルールの順序を評価します。ルールを移動するには、クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。

ルールを適切に作成して順序付けることは複雑な作業ですが、効果的な展開を構築する上で不可欠な作業です。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、ルールに無効な設定が含まれてしまう可能性があります。詳細については、アクセス制御ルールのベストプラクティスを参照してください。

ステップ 6 プレフィルタ ポリシーを保存します。

ステップ 7 トンネル ゾーンの制約をサポートする設定では、再ゾーン分割されたトンネルを適切に処理します。

トンネルゾーンを送信元ゾーンの制約として使用し、再ゾーン分割されたトンネルでの接続を照合します。

ステップ 8 プレフィルタ ポリシーを管理対象デバイスに展開されたアクセス コントロール ポリシーに関連付けます。

アクセス制御への他のポリシーの関連付けを参照してください。

ステップ 9 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。

（注） プレフィルタポリシーを展開しても、そのルールは既存のトンネルセッションに適用されません。したがって、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でバインドされません。また、ポリシーヒットカウントは、ポリシーに一致する接続の最初のパケットに対してのみ増加します。したがって、ポリシーに一致する可能性がある既存の接続のトラフィックは、ヒットカウントから除外されます。ポリシールールを効果的に適用するには、既存のトンネルセッションをクリアしてからポリシーを展開します。

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。

トンネルとプレフィルタ ルールのコンポーネント

状態（有効/無効）

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）

ルールの番号は1から始まります。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。トラフィックが一致する最初のルールは、ルール タイプ（トンネルまたはプレフィルタ）に関係なく、そのトラフィックを処理するルールです。

操作

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とログ記録の方法が決まります。

- [高速パス（Fastpath）]：アクセス制御、ID 要件、レート制限を含む、すべての詳細な検査および制御から一致するトラフィックを免除します。トンネルを高速パス化すると、すべてのカプセル化された接続が高速パス化されます。
- [ブロック（Block）]：どのような種類の検査も行わずにトラフィックを照合します。トンネルをブロックすると、カプセル化されたすべての接続がブロックされます。
- [分析（Analyze）]：残りのアクセス制御で内部ヘッダーを使用して引き続きトラフィックを分析できるようにします。アクセス制御および関連するディープ インスペクションによって渡された場合、このトラフィックはレート制限も行われる場合があります。トンネル ルールの場合は、[トンネル ゾーンの割り当て（Assign Tunnel Zone）] オプションを指定して、再ゾーニングを有効にします。

方向（トンネル ルールのみ）

トンネル ルールの方向によって、システムの送信元と宛先の条件に従った処理方法が決まります。

- 送信元からのトンネルのみを照合します（単方向）。送信元から宛先へ送信されるトラフィックのみを照合します。一致するトラフィックは、指定された送信元インターフェイスまたはトンネル エンドポイントから発信され、宛先インターフェイスまたはトンネル エンドポイントを通過する必要があります。許可された接続のリターントラフィックも許可されます。
- 送信元と宛先からのトンネルを照合します（双方向）。送信元から宛先へ送信されるトラフィックと宛先から送信元へ送信されるトラフィックの両方を照合します。この効果は、単方向のルールを2つ作成した場合と同じで、一方のルールがもう一方のルールのミラーとなります。

プレフィルタ ルールは常に単方向です。

トンネル ゾーンの割り当て（トンネル ルールのみ）

トンネル ルールで、トンネル ゾーン（既存のゾーンまたはオンザフライで作成したゾーン）を割り当てると、一致するゾーンが再ゾーニングされます。再ゾーニングするには、分析アクションが必要です。

トンネルを再ゾーニングすると、アクセス制御ルールなどの他の構成で、すべてのトンネルのカプセル化された接続の所属先が同じであると認識させることができます。トンネルに割り当てられたトンネルゾーンをインターフェイスの制約として使用すると、カプセル化された接続に合わせた検査を実行することができます。詳細については、トンネルゾーンおよびプレフィルタリング （17 ページ）を参照してください。

注意 トンネル ゾーンを割り当てるときには注意が必要です。再ゾーニングされたトンネルの接続は、後から実行される評価でセキュリティ ゾーンの制約と一致しないことが検出される可能性があります。トンネルゾーン実装の簡単なウォークスルーと、再ゾーニングするトラフィックを明示的に処理せずに再ゾーニングする理由については、トンネル ゾーンの使用 （18 ページ）を参照してください。

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。トラフィックは、ルールのすべての条件と一致し、ルールと一致する必要があります。各条件の種類には、ルール エディタ内に独自のタブがあります。

トラフィックをプレフィルタリングするには、次の外部ヘッダー制約を使用します。トンネルルールは、カプセル化プロトコルで制約する必要があります。

- インターフェイス：インターフェイスルール条件
- ネットワーク（プレフィルタルール）/トンネルエンドポイント（トンネルルール）：ネットワークルール条件
- VLAN：VLAN タグルール条件
- ポート（プレフィルタルール）/カプセル化およびポート（トンネルルール）：プレフィルタルールのポートルール条件 （15 ページ）またはカプセル化ルールの条件 （17 ページ）
- 時間範囲—時間と日のルール条件

ログ

システムが記録する処理済みトラフィックのレコードは、ルールのロギング設定によって管理します。

トンネルとプレフィルタのルールでは、高速パスが適用されたトラフィックとブロックされたトラフィック（[高速パス（Fastpach）] と [ブロック（Block）] のアクション）をログに記録することができます。詳細分析（[分析（Analyze）] アクション）の対象となるトラフィックで

は、一致する接続が他の構成で記録されている可能性がありますが、プレフィルタ ポリシーでのログ記録は無効になります。ロギングは、カプセル化フローではなく、内部フローで実行されます。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「Logging Connections with Tunnel and Prefilter Rules」を参照してください。

説明

ルールで変更を保存するたびに、コメントを追加することができます。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。

ルールを保存した後で、これらのコメントを編集または削除することはできません。

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

プレフィルタルール条件

ルール条件を使用すると、プレフィルタポリシーを微調整して、制御するネットワークをターゲットにすることができます。詳細については、次の項を参照してください。

インターフェイスルール条件

インターフェイス ルールの条件は送信元インターフェイスと宛先インターフェイスによってトラフィックを制御します。

ルールタイプと導入環境でのデバイスにより、セキュリティゾーンやインターフェイスグループと呼ばれる定義済みのインターフェイス オブジェクトを使用してインターフェイス条件を構築できます。インターフェイス オブジェクトはネットワークをセグメント化して複数のデバイス間でインターフェイスをグループ化することによってトラフィック フローを制御し、分類しやすくします。インターフェイス（Interface）を参照してください。

ヒント インターフェイスによってルールを制約するのは、システムパフォーマンスを改善するための最適な方法の1つです。ルールがデバイスのすべてのインターフェイスを除外する場合、そのルールはそのデバイスのパフォーマンスに影響しません。

インターフェイス オブジェクト内のすべてのインターフェイスが同じタイプ（すべてインライン、パッシブ、スイッチド、ルーテッド、または ASA FirePOWER）である必要があるのと同様に、インターフェイス条件で使用されているすべてのインターフェイス オブジェクトは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、パッシブ展開では宛先インターフェイスでルールを制約することはできません。

ネットワークルール条件

ネットワーク ルールの条件では、内部ヘッダーを使用して、送信元と宛先の IP アドレスを基準にトラフィックを制御します。外部ヘッダーを使用するトンネルルールでは、ネットワーク条件の代わりにトンネル エンドポイント条件を使用します。

事前定義されたオブジェクトを使用してネットワーク条件を作成することも、個々の IP アドレスまたはアドレス ブロックを手動で指定することもできます。

（注） アイデンティティルールで FDQN ネットワークオブジェクトを使用することはできません。

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。

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。

プレフィルタルールのポートルール条件

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。

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。プレフィルタルールで他のプロトコルと一致するようにポート条件を設定できますが、GRE、IP 内の IP、IP 内の IPv6、および Toredo ポート 3544 を一致させる場合は、代わりにトンネルルールを使用する必要があります。

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、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。

トンネルルール条件

ルール条件を使用すると、トンネルポリシーを微調整して、制御するネットワークをターゲットにすることができます。トンネルルールでは、次の条件を使用できます。

- [インターフェイスオブジェクト（Interface Objects）]：接続が通過するデバイスインターフェイスを定義するセキュリティゾーンまたはインターフェイスグループ。インターフェイスルール条件 を参照してください。
- [トンネルエンドポイント（Tunnel Endpoints）]：トンネルの送信元 IP アドレスと宛先 IP アドレスを定義するネットワークオブジェクト。
- [VLANタグ（VLAN Tags）]：トンネルの最も外側の VLAN タグ。VLAN タグルール条件 を参照してください。
- [カプセル化とポート（Encapsulation and Ports）]：トンネルのカプセル化プロトコル。カプセル化ルールの条件 （17 ページ） を参照してください。
- [時間範囲（Time Range）]：ルールがアクティブな日時。時間範囲を指定しない場合、ルールは常にアクティブです。時間と日のルール条件 を参照してください。

カプセル化ルールの条件

カプセル化の条件は、トンネル ルールに固有です。

この条件では、カプセル化プロトコルによって特定のタイプのプレーンテキスト、パススルートンネルを制御します。ルールを保存する前に、一致するプロトコルを 1 つ以上選択する必要があります。次のオプションを選択できます。

- GRE（47）
- IP-in-IP（4）
- IPv6-in-IP（41）
- Teredo（UDP（17）/3455）

トンネル ゾーンおよびプレフィルタリング

トンネルゾーンを使用すれば、プレフィルタリングを使って後続のトラフィック処理をカプセル化された接続に合わせることができます。

システムは通常最も内側の検出可能なレベルのヘッダーを使用してトラフィックを処理するため、特殊なメカニズムが必要になります。これにより、可能な限りきめ細かなインスペクションが保証されます。ただし、これは、パススルートンネルが暗号化されていない場合、システムは個々のカプセル化された接続に対して処理を行うことも意味しています。パススルートンネルとアクセス制御 （6 ページ）を参照してください。

トンネルゾーンはこの問題を解決します。アクセス制御の最初のフェーズ（プレフィルタリング）で、特定のタイプのプレーンテキスト、パススルートンネルを識別するために外側のヘッダーを使用できます。次に、それらのトンネルは、カスタム トンネル ゾーンを割り当てることで再ゾーン化できます。

トンネルを再ゾーニングすると、アクセス制御ルールなどの他の構成で、すべてのトンネルのカプセル化された接続の所属先が同じであると認識させることができます。トンネルに割り当

てられたトンネルゾーンをインターフェイスの制約として使用すると、カプセル化された接続に合わせた検査を実行することができます。

トンネル ゾーンは、その名称にもかかわらず、セキュリティ ゾーンではありません。トンネル ゾーンは、インターフェイスの一式を表すわけではありません。トンネル ゾーンは、場合によっては、カプセル化された接続に関連付けられているセキュリティゾーンに置き換わるタグとして考える方がより正確です。

⚠

注意 トンネルゾーンの制約をサポートする設定の場合、再ゾーン化されたトンネル内の各接続はセキュリティゾーンの制約とは一致**しません**。たとえば、トンネルを再ゾーン化した後、アクセス コントロール ルールでは、そのカプセル化された各接続を、それらの新しく割り当てられたトンネル ゾーンと突き合わせることができますが、元のセキュリティ ゾーンと突き合わせることはできません。

トンネルゾーン実装の簡単なウォークスルーと、再ゾーニングするトラフィックを明示的に処理せずに再ゾーニングする理由については、トンネル ゾーンの使用 （18 ページ）を参照してください。

トンネル ゾーンの制約をサポートする設定

トンネル ゾーンの制約をサポートするのは、アクセス コントロール ルールだけです。

他のどの設定もトンネルゾーンの制約をサポートしません。たとえば、QoS を使用してプレーン テキスト トンネル全体をレート制限することはできず、個々のカプセル化されたセッションをレート制限できるだけです。

トンネル ゾーンの使用

この例の手順は、トンネル ゾーンを使用してさらに分析するために GRE トンネルを再ゾーン化する方法をまとめたものです。この例で説明されている概念は、プレーンテキストのパススルー トンネルにカプセル化された接続に合わせてトラフィック インスペクションを調整する必要があるシナリオにも適応できます。

組織の内部トラフィックが信頼済みセキュリティゾーンを通過する状況について考えてみましょう。信頼済みセキュリティゾーンは、さまざまな場所に展開された複数の管理対象デバイスにわたる一連のインターフェイスを表します。組織のセキュリティポリシーでは、エクスプロイトとマルウェアのディープインスペクション後の内部トラフィックを許可する必要があります。

内部トラフィックには、特定のエンドポイント間のプレーンテキストのパススルー GRE トンネルが含まれている場合があります。このカプセル化されたトラフィックのトラフィック プロファイルは、「通常」の局間アクティビティとは異なるため（おそらく既知かつ無害）、セキュリティポリシーに従いながら、特定のカプセル化された接続のインスペクションを制限できます。

この例では、構成の変更を展開した後、次のようになります。

- 信頼済みゾーンで検出されたプレーンテキストのパススルーGREカプセル化トンネルは、個別のカプセル化接続が1セットの侵入およびファイル ポリシーによって評価されます。
- 信頼済みゾーンの他のすべてのトラフィックは、侵入およびファイル ポリシーの別のセットで評価されます。

このタスクは、GREトンネルの再ゾーン化によって実行します。再ゾーン化を実行すると、アクセス コントロールによって、GRE カプセル化接続が元の信頼済みセキュリティ ゾーンではなくカスタム トンネル ゾーンに関連付けられます。再ゾーン化は、アクセス制御によるカプセル化されたトラフィックの処理方法に起因して必要になります。「パススルー トンネルとアクセス制御 （6 ページ）」と「トンネル ゾーンおよびプレフィルタリング （17 ページ）」を参照してください

手順

ステップ 1 カプセル化されたトラフィック向けのディープインスペクションを実行するカスタムの侵入およびファイル ポリシーを設定し、カプセル化されていないトラフィックには別の侵入およびファイル ポリシーのセットを設定します。

ステップ 2 信頼済みセキュリティ ゾーンを通過するGREトンネルを再ゾーン化するようにカスタム プレフィルタリングを設定します。

カスタム プレフィルタ ポリシーを作成し、アクセス コントロールに関連付けます。そのカスタム プレフィルタ ポリシーで、トンネル ルール（この例では**GRE_tunnel_rezone**）と対応するトンネル ゾーン（**GRE_tunnel**）を作成します。詳細については、プレフィルタリングの設定 （10 ページ）を参照してください。

表 *1 : GRE_tunnel_rezone* トンネル ルール

ルールコンポーネント	説明
インターフェイス オブジェクト条件	信頼済みセキュリティ ゾーンを送信元インターフェイス オブジェクトと宛先インターフェイス オブジェクトの両方の制約として使用して、内部のみのトンネルを照合します。
トンネルエンドポイント条件	組織で使用されている GRE トンネルの送信元と宛先のエンドポイントを指定します。 トンネル ルールは、デフォルトでは双方向です。[トンネルの照合（Match tunnels from）] オプションを変更しない場合は、どのエンドポイントを送信元として指定し、どのエンドポイントを宛先として指定するかは重要ではありません。
カプセル化条件	GRE トラフィックを照合します。
トンネルゾーンの割り当て	**GRE_tunnel** トンネル ゾーンを作成し、ルールに一致するトンネルに割り当てます。
操作	（残りのアクセス コントロールで）分析します。

ステップ 3 再ゾーン化されたトンネルの接続を処理するようにアクセス コントロールを設定します。

管理対象デバイスに展開されたアクセス コントロール ポリシーでは、再ゾーン化したトラフィックを処理するルール（この例では**GRE_inspection**）を設定します。詳細については、アクセスコントロールルールの作成および編集を参照してください。

表 *2 : GRE_inspection* アクセス コントロール ルール

ルールコンポーネント	説明
セキュリティゾーン条件	GRE_tunnel セキュリティゾーンを送信元ゾーン制約として使用し、再ゾーン化されたトンネルを照合します。
操作	ディープ インスペクションを有効にして許可します。 カプセル化された内部トラフィックのインスペクションを実行するように調整されたファイルおよび侵入ポリシーを選択します。

注意 この手順をスキップすると、再ゾーン化された接続は、セキュリティゾーンによって制約されていない**任意の**アクセス コントロール ルールに一致する場合があります。再ゾーン化された接続がどのアクセス コントロール ルールにも一致しない場合は、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。意図してそのようにしていることを確認してください。

ステップ 4 信頼済みセキュリティ ゾーンを通過するカプセル化されていない接続を処理するようにアクセス コントロールを設定します。

同じアクセス コントロール ポリシーで、信頼済みセキュリティ ゾーン内の再ゾーン化されていないトラフィックを処理するルール（この例では **internal_default_inspection**）を設定します。

表 *3 : internal_default_inspection* アクセス コントロール ルール

ルールコンポーネント	説明
セキュリティゾーン条件	信頼済みセキュリティ ゾーンを送信元ゾーンと宛先ゾーンの両方の制約として使用して、再ゾーン化されていない内部のみのトラフィックを照合します。
操作	ディープ インスペクションを有効にして許可します。 カプセル化されていない内部トラフィックのインスペクションを実行するように適合されたファイルおよび侵入ポリシーを選択します。

ステップ 5 既存のルールに対して相対的な新しいアクセス コントロール ルールの位置を評価します。ルールの順序を必要に応じて変更します。

2つの新しいアクセス コントロール ルールを隣同士に配置した場合は、最初にどちらを配置するかは重要ではありません。GRE トンネルを再ゾーン化したため、2つのルールは互いをプリエンプション処理することはできません。

ステップ 6 すべての変更された構成を保存します。

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。

トンネル ゾーンの作成

次の手順では、オブジェクトマネージャでトンネルゾーンを作成する方法について説明します。トンネルルールの編集時にゾーンを作成することもできます。

手順

ステップ 1 **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）]**を選択します。
ステップ 2 オブジェクト タイプのリストから [トンネル ゾーン（Tunnel Zone）] を選択します。
ステップ 3 [トンネル ゾーンの追加（Add Tunnel Zone）] をクリックします。
ステップ 4 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。
ステップ 5 [保存（Save）] をクリックします。

次のタスク

- カスタム事前フィルタリングの一部として、トンネル ゾーンをプレーン テキストのパススルー トンネルに割り当てます。プレフィルタリングの設定 （10 ページ）を参照してください。

プレフィルタルールのアクセス コントロール ポリシーへの移動

プレフィルタルールをプレフィルタポリシーから関連するアクセス コントロール ポリシーに移動できます。

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 ポリシーに移動できるのは、プレフィルタルールだけです。トンネルルールは移動できません。
- プレフィルタルールは、関連付けられたアクセス コントロール ポリシーにのみ移動できます。

- インターフェイスグループが設定されているプレフィルタルールは移動できません。
- プレフィルタルールの [アクション（Action）] パラメータは、移動時にアクセスコントロールルールの適切なアクションに変更されます。プレフィルタ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。

プレフィルタルールのアクション	アクセスコントロールルールのアクション
分析（Analyze）	許可（Allow）
ブロック（Block）	ブロック（Block）
高速パス（Fastpath）	[信頼（Trust）]

- 同様に、次の表に示すように、プレフィルタ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。

プレフィルタルールのアクション	アクセスコントロールルールの有効なロギング構成
分析（Analyze）	どのログ設定も有効ではありません。
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
高速パス（Fastpath）	• 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

- ルールを移動すると、プレフィルタルール構成のコメントが失われます。ただし、ソースのプレフィルタポリシーに言及する新しいコメントが、移動後のルールに追加されます。
- 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、Management Center に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 プレフィルタ ポリシー エディタで、マウスを左クリックして移動するルールを選択します。

ヒント 複数のルールを選択するには、キーボードの Ctrl（Control）キーを使用します。

ステップ 2 選択したルールを右クリックし、[別のポリシーに移動（Move to another policy）] を選択します。

ステップ 3 [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 4 [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。

- [デフォルト（Default）] セクションの最後のルールセットとして配置するには、[一番下（[デフォルト]セクション内）（At the bottom (within the Default section)）] を選択します。
- [必須（Mandatory）] セクションの最初のルールセットとして配置するには、[一番上（[必須]セクション内）（At the top (within the Mandatory section)）] を選択します。

ステップ 5 [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。

プレフィルタ ポリシーのヒット カウント

ヒットカウントは、一致する接続に対してポリシールールがトリガーされた回数を示します。

プレフィルタ ポリシー ヒット カウントの表示に関する詳細詳細については、ルールヒットカウントの表示を参照してください。

大規模フローのオフロード

Cisco Secure Firewall 3100、Cisco Secure Firewall 4200、Firepower 4100/9300 シャーシ では、プレフィルタポリシーによってファストパスされるように設定した特定のトラフィックは、Threat Defense ソフトウェアではなくハードウェア（具体的には NIC 内）で処理されます。これらの接続フローをオフロードすると、特に大規模なファイル転送などのデータ集約型アプリケーションの場合、スループットが向上し、遅延が減少します。この機能は、データセンターで特に役立ちます。これは、静的フロー オフロードと呼ばれます。

さらに、デフォルトでは、Threat Defense デバイスは信頼を含む他の基準に基づいてフローをオフロードします。これは、動的フロー オフロードと呼ばれます。

オフロードされたフローは、引き続き制限付きステートフルインスペクション（基本的なTCPフラグおよびオプションのチェックなど）を受信します。システムは必要に応じてさらなる処理のためにファイアウォール システムへのパケットを選択的に増やすことができます。

大規模フローをオフロードすることでメリットが得られるアプリケーションの例は次のとおりです。

- ハイパフォーマンス コンピューティング（HPC）調査サイト。ここでは、Threat Defense デバイスがストレージと高コンピューティング ステーション間で展開されます。1つの調査サイトが NFS 経由の FTP ファイル転送またはファイル同期を使用してバックアップを行うと、大量のデータ トラフィックがすべての接続に影響を与えます。NFS を介する FTP ファイル転送およびファイル同期のオフロードによって、他のトラフィックへの影響が軽減されます。
- 主にコンプライアンス目的で使用される High Frequency Trading（HFT）。ここでは、Threat Defense デバイスがワークステーションと Exchange 間で展開されます。セキュリティは通常は問題にはなりませんが、遅延は大きな問題です。

次のフローをオフロードできます。

- （静的フロー オフロードのみ）プレフィルタポリシーにより FastPath される接続。
- 標準または 802.1Q タグ付きイーサネット フレームのみ。
- （動的フローオフロードのみ）：
  - インスペクションエンジンが検査の必要がなくなったと判断した検査済みのフロー。これらのフローには次が含まれます。
    - 信頼アクションを適用し、セキュリティゾーン、送信元と宛先のネットワーク、およびポートの一致のみに基づくアクセスコントロールルールによって処理されるフロー。
    - 復号ポリシー を使用した復号に選択されていない TLS/SSL フロー。
    - インテリジェントアプリケーションバイパス（IAB）ポリシーで、明示的か、またはフロー バイパスのしきい値を超えているために信頼されているフロー。
    - ファイルポリシーまたは信頼ポリシーに一致し、そのフローが信頼できると判断されたフロー。
    - 検査する必要がなくなった許可されたフロー。
  - 次の IPS プリプロセッサが検査したフロー：
    - SSH および SMTP。
    - FTP プリプロセッサのセカンダリ接続。
    - Session Initiation Protocol（SIP）プリプロセッサのセカンダリ接続。
  - キーワードを使用する侵入ルール（オプションとも呼ばれる）。

- Cisco Secure Firewall 3100 では、動的フローオフロードはサポートされていません。

重要 上記の詳細、例外、および制限については、フロー オフロードの制限事項 （25 ページ）を参照してください。

静的フロー オフロードの使い方

ハードウェアに適格なトラフィックをオフロードするには、**FastPath** アクションを適用するプレフィルタポリシールールを作成します。TCP/UDP にはプレフィルタ ルールを使用し、GRE にはトンネル ルールを使用します。

（推奨されていません。）静的フローオフロードを無効にし、副産物として動的フローオフロードを無効にするには、FlexConfig を使用して **no flow-offload enable** コマンドを実行します。このコマンドの詳細については、https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-command-reference-list.html から入手可能な『*Cisco ASA Series Command Reference*』を参照してください。

動的フロー オフロードの使い方

動的フローオフロードは、サポートしていない Cisco Secure Firewall 3100 などのデバイスを除き、デフォルトで有効になっています。

動的オフロードを無効にするには：

```
> configure flow-offload dynamic whitelist disable
```

動的オフロードを再度有効にするには：

```
> configure flow-offload dynamic whitelist enable
```

動的オフロードは、事前フィルタリングが構成されているかどうかに関係なく、静的フローオフロードが有効になっている場合にのみ発生することに注意してください。

フロー オフロードの制限事項

すべてのフローをオフロードできるわけではありません。オフロードの後でも、フローを特定の条件下でのオフロードから除外することができます。次に、制限事項の一部を示します。

デバイスによる制限

この機能は、以下のデバイスでサポートされています。

- FXOS 1.1.3 以降を実行している Firepower 4100/9300。
- Cisco Secure Firewall 4200
- Cisco Secure Firewall 3100

オフロードできないフロー

次のタイプのフローはオフロードできません。

- IPv6 アドレッシングなど、IPv4 アドレッシングを使用しないフロー。
- TCP、UDP、GRE 以外のプロトコルに対するフロー。

（注） PPTP GRE 接続はオフロードできません。

- パッシブ、インラインまたはインライン タップ モードで設定されたインターフェイス上のフロー。ルーテッドインターフェイスおよびスイッチドインターフェイスがサポートされている唯一のタイプです。
- （Cisco Secure Firewall 3100）。トンネリングされたフローの内部ヘッダーに基づくオフロード。
- （Cisco Secure Firewall 3100）。マルチインスタンス オフロード。
- Snort またはその他のインスペクション エンジンによるインスペクションが必要なフロー。FTP など場合によっては、コントロール チャネルはオフロードできませんがセカンダリ データ チャネルはオフロードできます。
- デバイスで終端する IPsec および TLS/DTLS VPN 接続。
- 暗号化または復号を必要とするフロー。たとえば、復号ポリシーによって復号される接続です。
- ルーテッド モードのマルチキャスト フロー。ブリッジグループにメンバーインターフェイスが 2 つしかない場合、トランスペアレントモードでサポートされます。
- TCP インターセプト フロー。
- TCP ステートバイパスフロー。同じトラフィックにフローオフロードと TCP ステートバイパスを設定することはできません。
- セキュリティ グループでタグ付けされたフロー。
- クラスタで非対称フローが発生した場合に備えて、別のクラスタ ノードから転送されるリバース フロー。
- クラスタ内の一元化されたフロー（フローのオーナーが制御ユニットでない場合）。
- IP オプションを含むフローは動的にオフロードできません。

その他の制限事項

- フローオフロードとデッド接続検出（DCD）は互換性がありません。オフロードできる接続に DCD を設定しないでください。
- フローオフロード条件に一致する複数のフローがキューイングされて、ハードウェア上の同じ場所に同時にオフロードされる場合、最初のフローのみがオフロードされます。他のフローは通常どおりに処理されます。これをコリジョン（衝突）といいます。この状況の統計を表示するには、CLI で **show flow-offload flow** コマンドを使用します。

- ダイナミック フローのオフロードによってすべての TCP ノーマライザのチェックが無効になります。
- オフロードされたフローはFXOSインターフェイスを通過しますが、それらのフローの統計は論理デバイスインターフェイスには表示されません。したがって、論理デバイスインターフェイスのカウンタとパケットレートには、オフロードされたフローは反映されません。

特定のデバイスでサポートされていない動的フローオフロード

Cisco Secure Firewall 3100では、動的フローオフロードはサポートされていません。

オフロードを無効にする条件

フローがオフロードされた後、フロー内のパケットは次の条件を満たす場合にThreat Defenseに返され、さらに処理されます。

- タイムスタンプ以外の TCP オプションが含まれている。
- フラグメント化されている。
- これらは等コストマルチパス（ECMP）ルーティングの対象であり、入力パケットは 1 つのインターフェイスから別のインターフェイスに移動する。

プレフィルタリングの履歴

機能	最小 Management Center	最小 Threat Defense	詳細
プレフィルタルールのアクセスコントロールポリシーへの移動	6.7	任意（Any）	プレフィルタルールをプレフィルタポリシーから関連するアクセス コントロール ポリシーに移動できます。 新規/変更されたページ：プレフィルタポリシーページで、選択したルールの右クリックメニューに、新しい [別のポリシーに移動（Move to another policy）] オプションが表示されます。 サポートされているプラットフォーム： Management Center
時間ベースのルール	6.6	任意（Any）	Threat Defense デバイスのタイムゾーンによって決定される日時に応じて、プレフィルタおよびトンネルルールを適用する機能。 アクセス制御ルールの履歴の説明を参照してください。

機能	最小 Management Center	最小 Threat Defense	詳細
プレフィルタルールページからのオブジェクトの詳細の表示	6.6	任意（Any）	導入された機能：プレフィルタルールを表示するときに、オブジェクトまたはオブジェクトグループの詳細を表示するオプション。 新しいオプション：プレフィルタルールリストの次のいずれかの列の値を右クリックすると、オブジェクトの詳細を表示するオプションが提供されます：[送信元ネットワーク（Source Networks）]、[接続先ネットワーク（Destination Networks）]、[送信元ポート（Source Port）]、[接続先ポート（Destination Port）]、および[VLANタグ（VLAN Tag）]。 サポートされているプラットフォーム： Secure 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。