プレフィルタ処理とプレフィルタ ポリシー

以下のトピックでは、プレフィルタを設定する方法について説明します。

プレフィルタの概要

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。管理対象デバイスに展開されたプレフィルタ ポリシーは、制限付きの外側のヘッダー基準を使ってトラフィックを迅速に処理します。

内側のヘッダーを使用し、より強力なインスペクション能力を備えた他のアクセス制御とは対照的で、プレフィルタはシンプルかつ迅速で、早い段階で機能します。

プレフィルタは、以下を行う場合に設定します。

- 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。

詳細は、プレフィルタリングとアクセス コントロール （2 ページ）を参照してください。

モデル制限のプレフィルタ

Firepower システムでプレフィルタがサポートされるのは Firepower Threat Defense デバイスのみです。

クラシック デバイス（7000 および 8000 シリーズ、NGIPSv、ASA FirePOWER）にプレフィルタ ポリシーを展開しても、何の影響もありません。代わりに、プレフィルタとほぼ同様の機能を持つ以前から用意されてる信頼およびブロック アクセス コントロール ルールを、機能の違いに留意しつつ使用してください。

以下の点にも注意してください。

- 8000 シリーズ デバイス：デバイス固有の FastPath ルールによってアクセス コントロールをバイパスできます（ただし、トラフィックをブロックすることはできません。高速パス ルールの設定（8000 シリーズ）を参照してください。
- クラシック デバイス：すべてのクラシック デバイスは、アクセス コントロール ルールを使用して GRE でカプセル化されたトンネル全体を照合しますが、いくつかの制約事項があります。ポートおよび ICMP コードの条件を参照してください。

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（カプセル化の条件を参照）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。	プレフィルタの概要 （1 ページ）

特性	プレフィルタリング	アクセス制御	詳細
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 ポリシーは、マスター構成です。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（6 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。	—	—
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（10 ページ） アクセス コントロール ルールのアクション

特性	プレフィルタリング	アクセス制御	詳細
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 （9 ページ） ルール条件タイプ

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 （5 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 （12 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。	設定可能な接続ロギング
サポートされるデバイス	Firepower Threat Defense のみ。	すべて。	モデル制限のプレフィルタ （2 ページ）

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、外側の 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。その一例は、（Firepower Threat Defense ではなく）Cisco ASA ソフトウェアを実行する Cisco ASA ファイアウォールです。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、Firepower 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 （12 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。

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。Firepower システムでは、アクセス コントロール ポリシーは、プレフィルタ ポリシーを含む、サブポリシーおよびその他の設定を呼び出すマスター設定です。

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 （9 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することができます。設定可能な接続ロギング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。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。デフォルトプレフィルタ ポリシーは、グローバル ドメインに属しています。

プレフィルタリングの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	該当なし	Firepower Threat Defense	任意（Any）	Admin/Access Admin/Network Admin

カスタム プレフィルタリングを実行するには、アクセス コントロールの一部として管理対象デバイスにプレフィルタ ポリシーを設定し、展開します。

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 コントロール（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。また、既存のポリシーをコピー（  ）したり編集（  ）したり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 アイコン（  ）をクリックします。ポリシーのデフォルト アクションによる接続のロギング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 （9 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 （12 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 （10 ページ）およびルール管理：共通の特性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、ルールのパフォーマンスに関するガイドライン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て、再ゾーン分割されたトンネルでの接続を照合します。インターフェイス条件の設定を参照してください。

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。

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高速パス化、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、カプセル化の条件 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。ポートおよび ICMP コード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。トンネル エンドポイント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。ネットワーク条件を参照してください。

特性	トンネル ルール	プレフィルタ ルール
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。
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 （12 ページ）を参照してください。	未サポート

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

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の対象から、一致するトラフィックを除外します。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。
- 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 （12 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 （13 ページ）を参照してください。

条件（Conditions）

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するには、次の外部ヘッダー制約を使用します。

- インターフェイス：インターフェイス条件
- ネットワーク：トンネル エンドポイント条件または ネットワーク条件
- ポート：カプセル化の条件または ポートおよび ICMP コードの条件
- VLAN：VLAN 条件

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。

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。詳細については、トンネル ルールおよびプレフィルタ ルールによる接続のロギング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

ルールのパフォーマンスに関するガイドライン

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 （5 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することができます。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。

トンネルを再ゾーン化すると、アクセス コントロール ルールなどの他の設定で、そのトンネルのすべてのカプセル化された接続をグループとして認識できます。トンネルの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ことで、インスペクションをそのカプセル化された接続に合わせて調整できます。

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。

トンネルゾーンの導入の簡潔なウォークスルー、および再ゾーン化されたトラフィックを明示的に処理せずに再ゾーン化することの影響の説明については、トンネル ゾーンの使用 （13 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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	任意（Any）	Firepower Threat Defense	任意（Any）	Admin/Access Admin/Network Admin

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 FirePOWER システムの展開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間における一連のセンシング 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。再ゾーン化が必要になるのは、FirePOWERシステムとアクセス コントロールが、カプセル化されたトラフィックを処理する方法によります。パススルー トンネルとアクセス制御 （5 ページ）およびトンネル ゾーンおよびプレフィルタリング （12 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 （7 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て、再ゾーン化されたトンネルを照合します。インターフェイス条件を参照してください。
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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス
任意（Any）	該当なし	Firepower Threat Defense	任意（Any）	Admin/Access Admin/Network Admin

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 （7 ページ）を参照してください。