セキュリティ コンフィギュレーション ガイド：ゾーンベース ポリシー ファイアウォール、Cisco IOS XE Release 3S（ASR 1000）

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

ゾーンベース ポリシー ファイアウォール

このモジュールでは、ゾーンと呼ばれるインターフェイス グループの間の Cisco 単方向ファイアウォール ポリシーについて説明します。 Cisco 単方向ファイアウォール ポリシーがリリースされるまでは、Cisco ファイアウォールはインターフェイス上の検査ルールとしてのみ設定されていました。 設定されたインターフェイスを出入りするトラフィックは、検査ルールが適用される方向に基づいて検査されました。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ゾーンベース ポリシー ファイアウォールの前提条件

- ゾーンを作成する前に、ゾーンの構成について検討する必要があります。 一般的なガイドラインは、セキュリティの観点から同様の性質をもつインターフェイスをグループにすることです。
- ご使用のリリースによっては、Wide Area Application Services（WAAS）および Cisco ファイアウォールの相互運用性機能を使用できます。

ゾーンベース ポリシー ファイアウォールの前提条件

- コンフィギュレーションにセキュリティ ゾーンとインターフェイス上の検査ルール（以前の手法）の両方を含めても機能する可能性はありますが、そのようなコンフィギュレーションは推奨されません。
- ご使用のリリースによっては、ネストされたクラスマップ コンフィギュレーション内の **match** ステートメントについて、**show policy-map type inspect zone-pair** コマンド出力の累積カウンタは増加しません。 このカウンタに関する問題は、トップレベル クラス マップで **match-any** と **match-all** のいずれのキーワードが使用されているかに関係なく存在します。 詳細については、「例：クラス マップのプロトコル一致データが増加しない」の項を参照してください。
- ご使用のリリースによっては、クラス マップでのインスペクション用にシンプル メール転送プロトコル（SMTP）が設定されている場合、インスペクション用の拡張SMTP（ESMTP）を設定する必要があるとき、**match protocol smtp extended** コマンドを追加する前に **no match protocol smtp** コマンドを入力する必要があります。 通常の SMTP インスペクションに戻すには、**no match protocol smtp extended** コマンドを使用してから **match protocol smtp** コマンドを入力します。 これらのコマンドが適切な順序で設定されていない場合は、次のエラーが表示されます。

```
%Cannot add this filter. Remove match protocol smtp filter and then add this filter.
```

- WAAS および Cisco ファイアウォール コンフィギュレーションでは、Web Cache Coordination Protocol（WCCP）をサポートするために、Wide Area Application Engine（WAE）デバイスによって処理されるすべてのパケットは両方向で Cisco ファイアウォールを通過する必要があります。 ご使用のリリースによっては、レイヤ 2 リダイレクトが使用できないためにこの状況が発生します。 レイヤ 2 リダイレクトが WAE で設定されている場合、システムはデフォルトで、総称ルーティング カプセル化（GRE）リダイレクトを続行させます。
- 内部から外部へのゾーンベース ポリシーが、Windows システムでのインターネット制御メッセージプロトコル（ICMP）と一致するよう設定されている場合は、**traceroute** コマンドが機能します。 ただし、Apple システムでは、UDP ベースの traceroute を使用しているため、この同じ設定は機能しません。 この問題を解決するには、**icmp time-exceeded** コマンドと **icmp host unreachable** コマンドを **pass** コマンド（**inspect** コマンドではなく）とともに使用して外部から内部へのゾーンベース ポリシーを設定します。

- WAAS および Cisco ファイアウォール コンフィギュレーションでは、WCCP はポリシーベース ルーティング（PBR）を使用したトラフィック リダイレクトをサポートしません。
- マルチキャスト トラフィックのステートフル インスペクション サポートは、セルフ ゾーンを含むいずれのゾーン間でもサポートされません。 マルチキャスト トラフィックに対するコントロール プレーンの保護には、コントロール プレーン ポリシングを使用します。
- UDP ベースの traceroute は、ICMP インスペクションではサポートされません。
- GRE およびカプセル化セキュリティ ペイロード（ESP）プロトコル トラフィックがゾーンベース ポリシー ファイアウォールを通過することを許可するには、**pass** コマンドを使用する必要があります。 GRE および ESP プロトコルはステートフル インスペクションをサポートしておらず、**inspect** コマンドを使用する場合、これらのプロトコルのトラフィックはドロップされます。

ゾーンベース ポリシー ファイアウォールについて

トップレベルのクラス マップとポリシー マップ

トップレベル クラス マップでは、高レベルでトラフィック ストリームを識別できます。 トラフィック ストリームの識別は、**match access-group** コマンドと **match protocol** コマンドによって実現されます。 トップレベル クラス マップは、レイヤ 3 およびレイヤ 4 クラス マップとも呼ばれます。

トップレベル ポリシー マップでは、**inspect**、**drop**、**pass**、および **urlfilter** キーワードを使用して高レベルのアクションを定義できます。 マップをターゲット（ゾーン ペア）に付加できます。

（注） ゾーン ペアで設定できるのは、検査タイプのポリシーだけです。

CSCto44113 修正に伴い、**access-group match** コマンドを設定する場合は、レイヤ 4 ポリシー マップのみがファイアウォールによって検査されます。 この修正の前は、**access-group match** コマンドが設定されている場合、レイヤ 4 およびレイヤ 7 ポリシー マップの両方が検査されていました。

アプリケーション固有のクラス マップとポリシー マップ

アプリケーション固有クラスマップを使用すると、特定のプロトコルの属性に基づいてトラフィックを識別できます。 これらのクラス マップの一致基準はすべて、ある特定のアプリケーション（HTTP や SMTP など）のみに適用されます。 アプリケーション固有クラス マップは追加のサブタイプ（通常はタイプ **inspect** にプロトコル名（HTTP や SMTP）を加えたもの）によって識別されます。

アプリケーション固有ポリシーマップは、アプリケーションプロトコルのポリシーを指定するために使用します。 たとえば、Unique Resource Identifier（URI）の長さが 256 バイトを超える HTTP トラフィックをドロップする場合は、HTTP ポリシー マップを設定する必要があります。 アプリケーション固有ポリシーマップはターゲット（ゾーンペア）に直接付加できません。 これらは、トップレベルのレイヤ 3 またはレイヤ 4 ポリシー マップの「子」ポリシーとして設定する必要があります。

ゾーンの概要

ゾーンとは、同様の機能を果たすインターフェイスのグループです。 ゾーンによって、Cisco ファイアウォールを適用する場所を指定する方法が提供されます。

たとえば、デバイスで、ギガビット イーサネット インターフェイス 0/0/0 とギガビット イーサネット インターフェイス 0/0/1 をローカル LAN に接続できるとします。 これら 2 つのインターフェイスは、内部ネットワークを表している点で同類です。したがって、ファイアウォール設定でゾーンとしてグループ化できます。

デフォルトでは、同じゾーン内のインターフェイス間のトラフィックはポリシーには従わず、自由に通過します。 ファイアウォール ゾーンはセキュリティ機能に使用されます。

（注） ゾーンは、異なる VPN ルーティングおよび転送（VRF）インスタンスのインターフェイスまでは拡大できません。

ゾーン ベース ポリシー ファイアウォールが TCP キープアライブ トラフィックでイネーブルになっており、ファイアウォールの背後にあるホストが異常切断された場合、TCP キープアライブは、設定された TCP タイムアウトが終了したときにのみ機能します。 ウィンドウ外リセット（RST）パケットを受信すると、ファイアウォールは空の確認応答（ACK）パケットを RST パケットの発信側に送信します。 この ACK には、ファイアウォール セッションからの現在のシーケンス（SEQ）および ACK 番号が含まれています。 この ACK を受信すると、クライアントは ACK パケットの ACK 番号に等しい SEQ 番号が含まれた RST パケットを送信します。 ファイアウォールは、この RST パケットを処理し、ファイアウォール セッションをクリアし、RST パケットを渡します。

セキュリティ ゾーン

セキュリティ ゾーンとは、ポリシーを適用できるインターフェイスのグループです。

インターフェイスをゾーンにグループ化するには、次の 2 つの手順を実行します。

- インターフェイスを付加できるようにゾーンを作成します。
- インターフェイスを特定のゾーンのメンバーとなるように設定します。

デフォルトでは、トラフィックは、同じゾーンのメンバーであるインターフェイス間を通ります。

インターフェイスがセキュリティ ゾーンのメンバーである場合、そのインターフェイスと、別のゾーン内のインターフェイスとの間のすべてのトラフィック（デバイス宛またはデバイス発信のトラフィックを除く）はデフォルトでドロップされます。ゾーンメンバーインターフェイスと別のインターフェイスとの間の両方向のトラフィックを許可するには、そのゾーンをゾーン ペアの一部にして、そのゾーン ペアにポリシーを適用する必要があります。 ポリシーで、**inspect** または **pass** アクションを通してトラフィックが許可されると、トラフィックはインターフェイスを通過します。

ゾーンを設定する際に検討する基本ルールは次のとおりです。

- ゾーン インターフェイスからゾーン外のインターフェイスへのトラフィックまたはゾーン外のインターフェイスからゾーン インターフェイスへのトラフィックは常にドロップされます。ただし、デフォルト ゾーンがイネーブルになっている場合を除きます（デフォルト ゾーンはゾーン外のインターフェイスです）。
- 2 つのゾーン インターフェイス間のトラフィックは、各ゾーンにゾーン ペアの関係があるかどうか、およびそのゾーン ペアにポリシーが設定されているかどうかが検査されます。
- デフォルトでは、同じゾーン内の 2 つのインターフェイス間のすべてのトラフィックは、常に許可されます。
- ゾーン ペアは、ゾーンを送信元ゾーンおよび宛先ゾーンの両方として設定できます。 このゾーン ペアで検査ポリシーを設定して、同じゾーン内の 2 つのインターフェイス間のトラフィックを検査またはドロップできます。
- インターフェイスをゾーンとレガシー検査ポリシーの両方に同時に所属させることはできません。
- インターフェイスがメンバーになれるのは、1 つのセキュリティ ゾーンだけです。
- インターフェイスがセキュリティ ゾーンのメンバーの場合、そのゾーンを含むゾーン ペアで明示的なゾーン間ポリシーを設定しない限り、方向に関係なくそのインターフェイスを通過するすべてのトラフィックがブロックされます。
- トラフィックは、セキュリティ ゾーンのメンバーであるインターフェイスとセキュリティ ゾーンのメンバーではないインターフェイスの間では通過できません。これは、ポリシーは 2 つのゾーンだけで適用できるからです。
- トラフィックがデバイスのすべてのインターフェイスを通過するようにするには、すべてのインターフェイスは 1 つのセキュリティ ゾーンまたは別のゾーンのメンバーでなければなりません。 インターフェイスをセキュリティ ゾーンのメンバーにした後、**inspect** や **pass** などのポリシーアクションによってパケットを明示的に許可する必要があるため、このことは特に重要です。 それ以外の場合、パケットはドロップされます。
- デバイスのインターフェイスをセキュリティ ゾーンまたはファイアウォール ポリシーに所属させることができない場合、そのインターフェイスをセキュリティ ゾーンに追加し、そのゾーンとトラフィック フローの対象となる他のゾーンとの間に、「すべて通過」ポリシー（つまり、「ダミー」ポリシー）を設定する必要がある場合があります。
- セキュリティ ゾーン間またはゾーン ペアに対してアクセス コントロール リスト（ACL）を適用することはできません。

- セキュリティ ゾーンとゾーン ペアの間で ACL は適用できません。 トラフィックをドロップするには、ACL 設定をクラス マップに含め、ポリシー マップを使用します。
- ゾーン メンバーのインターフェイス上の ACL を制約的（厳密）にしないでください。
- 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 VPN ルーティングおよび転送（VRF）インスタンスに属している必要があります。
- メンバ インターフェイスが個別の VRF にあるセキュリティ ゾーン間でポリシーを設定できます。 ただし、設定で許可されていない場合、これらの VRF 間をトラフィックは流れません。
- トラフィックが VRF 間を流れない場合（VRF 間のルートリークが設定されていないため）、VRF 間のポリシーは実行されません。 これは、ポリシー側ではなく、ルーティング側の設定の誤りです。
- 同じセキュリティ ゾーン内のインターフェイス間のトラフィックはポリシーには従わず、自由に通過します。
- ゾーン ペアの送信元ゾーンおよび宛先ゾーンは、タイプ セキュリティのゾーンである必要があります。
- 同じゾーンを送信元ゾーンと宛先ゾーンの両方として定義することはできません。

ポリシーは、トラフィック フローの最初のパケットに適用されます。最初のパケットが分類および許可されると、トラフィックは、それ以上のパケット再分類なしでピア間を通過します（これは、最初の分類後に双方向トラフィック フローが許可されたことを意味します）。 ゾーン Z1 とゾーン Z2 間のゾーン ペアがあり、ゾーン Z2 とゾーン Z1 間のゾーン ペアはない場合、ゾーン Z2 から開始されたすべてのトラフィックはブロックされます。 ゾーン Z1 からゾーン Z2 へのトラフィックは、ゾーン ペアのポリシーに基づいて許可または拒否されます。

トラフィックがデバイスのすべてのインターフェイスを通過するようにするには、すべてのインターフェイスはセキュリティ ゾーンまたはデフォルト ゾーンのメンバーでなければなりません。

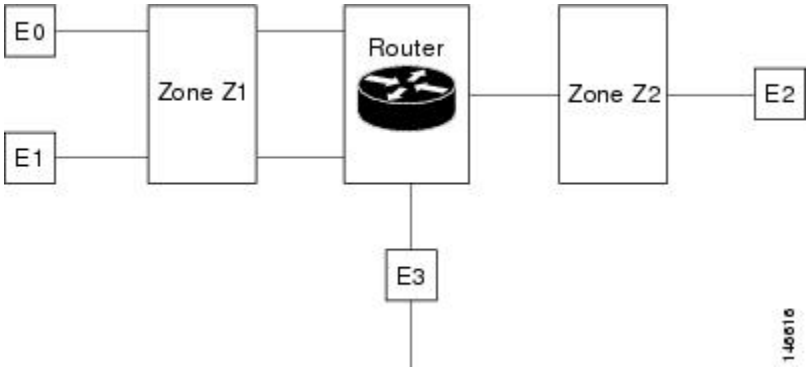
すべてのデバイス インターフェイスがセキュリティ ゾーンのメンバーである必要はありません。

下の図は、次のことを示しています。

- インターフェイス E0 と E1 はセキュリティ ゾーン Z1 のメンバーです。
- インターフェイス E2 は、セキュリティ ゾーン Z2 のメンバーです。

- インターフェイス E3 は、どのセキュリティ ゾーンのメンバーでもありません。

図 *1*：セキュリティ ゾーンの制約



次の状況が存在します。

- ゾーン ペアとポリシーは、同じゾーンで設定されます。Z1 と Z2 用のポリシーが設定されていない場合、トラフィックは E0 と E1 間を自由に通過しますが、E0 または E1 と E2 間は通過しません。 このトラフィックを検査するためのゾーン ペアとポリシーを作成できます。
- ポリシーが設定されていない場合、他のインターフェイス間（E0 と E2、E1 と E2、E3 と E1、および E3 と E2）でトラフィックは流れません。
- トラフィックを許可する明示的なポリシーがゾーン Z1 とゾーン Z2 間で設定されている場合だけ、E0 または E1 と E2 間でトラフィックが流れます。
- デフォルト ゾーンがイネーブルで、ゾーン ペアがデフォルト ゾーンと他のゾーンとの間に作成されている場合を除き、E3 と E0、E1、または E2 間をトラフィックが流れることはまったくありません。

セキュリティ ゾーンのメンバーとしての仮想インターフェイス

仮想テンプレート インターフェイスは、特定の目的のため、または特定のユーザに共通のコンフィギュレーションを定義するための汎用的なコンフィギュレーション情報と、デバイスに依存した情報を組み合わせて設定された論理インターフェイスです。 このテンプレートには、仮想アクセス インターフェイスに適用される Cisco ソフトウェア インターフェイス コマンドが含まれます。 仮想テンプレート インターフェイスを設定するには、**interface virtual-template** コマンドを使用します。

ゾーン メンバー情報は、RADIUS サーバから取得され、ダイナミックに作成されたインターフェイスがそのゾーンのメンバーになります。

zone-member security コマンドにより、ダイナミック インターフェイスを対応するゾーンに追加します。

ゾーン ペア

ゾーン ペアにより、2 つのセキュリティ ゾーン間で単方向のファイアウォール ポリシーを指定できます。

ゾーン ペアを定義するには、**zone-pair security** コマンドを使用します。 トラフィックの方向は、送信元ゾーンと宛先ゾーンによって指定します。 ゾーン ペアの送信元ゾーンと宛先ゾーンはセキュリティ ゾーンである必要があります。

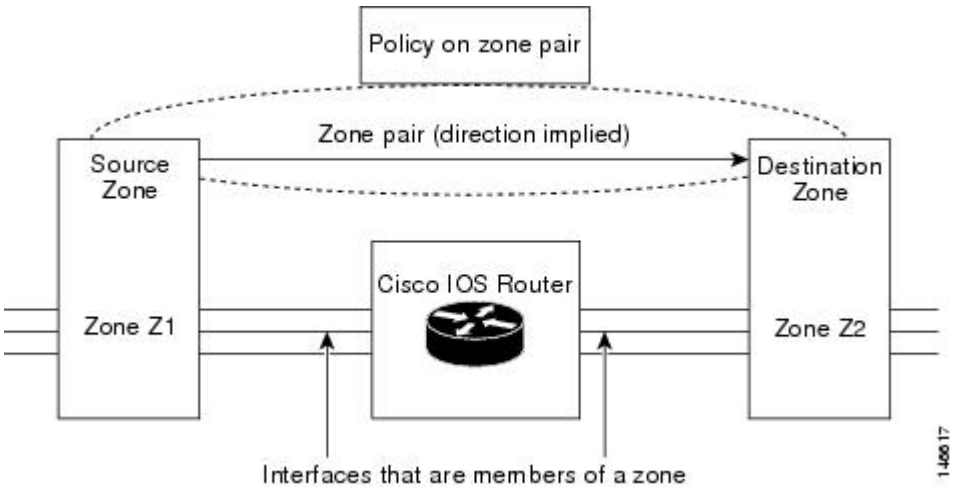
デフォルトまたはセルフ ゾーンを送信元ゾーンまたは宛先ゾーンとして選択できます。 セルフ ゾーンは、メンバーとしてインターフェイスを持たないシステム定義のゾーンです。セルフゾーンを含むゾーン ペアは、関連付けられたポリシーとともに、デバイス宛のトラフィックまたはデバイスによって生成されたトラフィックに適用されます。 デバイスを経由するトラフィックには適用されません。

ファイアウォールの最も一般的な用途は、デバイス経由のトラフィックに適用することです。したがって、少なくとも 2 つのゾーンが必要です（つまり、セルフ ゾーンは使用できません）。

ゾーン メンバー インターフェイス間のトラフィックを許可するには、そのゾーンと別のゾーン間のトラフィックを許可（または検査）するポリシーを設定する必要があります。 ターゲットのゾーン ペアにファイアウォール ポリシー マップを付加するには、**service-policy type inspect** コマンドを使用します。

下の図に、ゾーン Z1 からゾーン Z2 への方向に流れるトラフィック（つまり、入口インターフェイスがゾーン Z1 のメンバーで、出口インターフェイスがゾーン Z2 のメンバーであるトラフィック）にファイアウォール ポリシーを適用する例を示します。

図 *2*：ゾーン ペア



2 つのゾーンがあり、両方向（Z1 から Z2 への方向と Z2 から Z1 への方向）のトラフィックに対するポリシーが必要な場合は、2 つのゾーン ペア（各方向について 1 つずつ）を設定する必要があります。

ポリシーがゾーンペア間で設定されていない場合、トラフィックはドロップされます。ただし、リターン トラフィックのためだけにゾーン ペアとサービス ポリシーを設定する必要はありません。 デフォルトでは、リターン トラフィックは許可されません。 サービス ポリシーがフォワード方向のトラフィックを検査し、リターン トラフィックのゾーン ペアとサービス ポリシーがない場合、リターン トラフィックは検査されます。 サービス ポリシーがフォワード方向のトラフィックを渡し、リターン トラフィックのゾーン ペアとサービス ポリシーがない場合、リターントラフィックはドロップされます。いずれの場合も、リターン トラフィックを許可するには、ゾーン ペアとサービス ポリシーを設定する必要があります。 上の図では、Z2 から Z1 へのリターン トラフィックを許可するために送信元 Z2、宛先 Z1 のゾーン ペアを設定することは必須ではありません。 Z1 から Z2 ゾーンへのペアのサービス ポリシーが適用されます。

レガシー ファイアウォールは、デフォルトでルールまたはポリシーによって明示的に定義されていないパケットを許可するのに対し、ゾーンベース ファイアウォールは、ルールまたはポリシーによって明示的に許可されていないパケットをドロップします。

ゾーンベースのファイアウォールは、ゾーン内部とゾーン外部の間を流れるトラフィックにより、ゾーン内部で生成された断続的なインターネット制御メッセージプロトコル（ICMP）を処理する場合、異なる動作をします。

セルフ ゾーンを送信元とするゾーンペア、およびゾーン内部とゾーン外部の間を流れるトラフィックについて明示的なポリシーが設定されたコンフィギュレーションでは、断続的な ICMP 応答が生成された場合、ゾーンベース ファイアウォールはセルフ ゾーンを送信元とするゾーン ペアで ICMP の明示的な許可ルールを探します。 セルフ ゾーンを送信元とするゾーン ペアに対する ICMP の明示的な検査ルールは、断続的な ICMP 応答に関連するセッションが存在しないという理由で役に立たない場合があります。

ゾーンと検査

ゾーンベースポリシーファイアウォールでは、入力および出力インターフェイスから送信元ゾーンと宛先ゾーンでファイアウォールポリシーを調べます。インターフェイスを通過するすべてのトラフィックを検査する必要はありません。ゾーンペア全体で適用されるポリシーマップを通して、ゾーン ペアの個々のフローを検査するように指定できます。 ポリシー マップには、個々のフローを指定するクラス マップが含まれます。

また、フロー ベースで TCP しきい値やタイムアウトなどの**検査**パラメータを設定できます。

ゾーンと ACL

ゾーンのメンバーであるインターフェイスに適用されるアクセス コントロール リスト（ACL）は、ポリシーがゾーンペアに適用される前に処理されます。ゾーン間にポリシーがある場合、インターフェイス ACL がポリシー ファイアウォール トラフィックを阻害しないようにする必要があります。

ピンホール（保護されたネットワークへのアプリケーション コントロール アクセスを可能にする、ファイアウォールに開かれたポート）は、インターフェイス ACL のリターン トラフィック用にパンチされません。

ゾーンと VRF 認識ファイアウォール

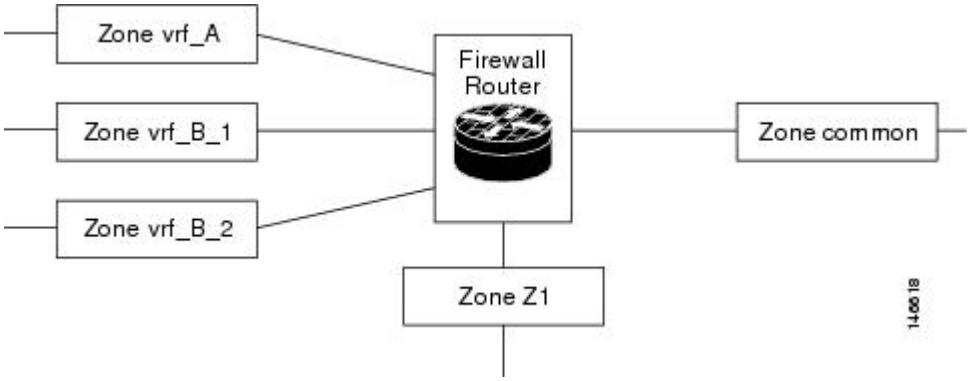
Cisco ファイアウォールは VPN ルーティングおよび転送（VRF）を認識し、 異なる VRF 間での IP アドレスの重複や各 VRF の異なるしきい値とタイムアウトを処理します。 ゾーンのすべてのインターフェイスは、同じ VRF に属している必要があります。

ただし、異なるエンティティに属する VRF は、通常、独自のポリシーを持っているため、異なる VRF のインターフェイスを同じゾーンにグループ化しないでください。

下の図に示しているように、異なる VRF が含まれる 2 つのゾーンのゾーン ペアを設定できます。

1 つのデバイス上に複数の VRF が設定されており、かつ、1 つのインターフェイスによってすべての VRF に共通のサービス（インターネット サービスなど）が提供されている場合は、そのインターフェイスを別のゾーンに配置します。 その後、共通ゾーンと他のゾーンとの間のポリシーを定義できます （VRF あたり 1 つ以上のゾーンを設定できます）。

図 *3*：ゾーンと *VRF*



上の図では、共通サービスを提供するインターフェイスは、ゾーン「共通」のメンバーです。VRF A はすべて、単一のゾーン vrf_A にあります。 VRF B には複数のインターフェイスが含まれており、vrf_B_1 と vrf_B_2 の複数のゾーンに分割されています。 ゾーン Z1 には VRF インターフェイスがありません。 これらの各ゾーンと common ゾーンの間にポリシーを指定できます。 また、VRF ルートエクスポートが設定されており、トラフィック パターンが道理にかなっている場合、ゾーン vrf_A、vrf_B_n、および Z1 間でポリシーを指定できます。 ゾーン vrf_A と vrf_B_1 の間にポリシーを設定できますが、トラフィックがこれらのゾーン間を流れることができることを確認します。

VRF ごとにグローバルなしきい値とタイマーを指定する必要はありません。 その代わりに、パラメータ マップによって **inspect** アクションにパラメータが提供されます。

ゾーンとトランスペアレント ファイアウォール

Cisco ファイアウォールは、インターフェイスがブリッジ モードで、ファイアウォールがブリッジド トラフィックを検査するトランスペアレント ファイアウォールをサポートします。

トランスペアレント ファイアウォールを設定するには、**bridge** コマンドを使用して指定したブリッジで指定したプロトコルのブリッジングをイネーブルにし、**zone-member security** コマンドを使用してインターフェイスをゾーンに付加します。インターフェイス上の **bridge** コマンドは、そのインターフェイスがブリッジ モードであることを示します。

ブリッジ インターフェイスはゾーン メンバーになることができます。 典型的な例では、レイヤ 2 ドメインを複数のゾーンに分割し、レイヤ 3 インターフェイスと同じようにポリシーを適用します。

P2P インスペクションに関するトランスペアレント ファイアウォールの制約

Cisco ファイアウォールは、ピアツーピア（P2P）プロトコルの分類とポリシーの施行に Network-Based Application Recognition（NBAR）を使用します。 NBAR はブリッジされたパケットには使用できません。そのため、トランスペアレント ブリッジングをイネーブルにしたファイアウォールでは P2P パケット インスペクションはサポートされません。

セキュリティ ゾーンのファイアウォール ポリシーの概要

クラスとは、内容に基づいてパケットのセットを識別する方法です。 通常は、識別されたトラフィックでポリシーを反映するアクションを適用できるように、クラスを定義します。 クラスは、クラス マップを介して指定されます。

アクションとは、通常、トラフィック クラスに関連付けられる、特定の機能のことです。 たとえば、**inspect**、**drop**、**pass** はアクションです。

セキュリティ ゾーンのファイアウォール ポリシーを作成するには、次の作業を実行する必要があります。

- 一致基準を定義する（クラス マップ）。
- アクションと一致基準の関連付け（ポリシー マップ）。
- ゾーン ペアへのポリシー マップの付加（サービス ポリシー）。

class-map コマンドは、パケットを指定されたクラスに一致させるためのクラス マップを作成します。 ターゲット（入力インターフェイス、出力インターフェイス、またはゾーン ペアなど）に到達したパケットは、**service-policy** コマンドの設定方法に従って、クラス マップ用に設定された一致基準に基づいてチェックされ、パケットがそのクラスに属しているかどうかが判断されます。

policy-map は、1 つ以上のターゲットに付加できるポリシー マップを作成または変更し、サービス ポリシーを指定します。 **policy-map** コマンドを使用して、作成、追加または変更するポリシー マップの名前を指定してから、クラス マップで一致基準を定義するクラスにポリシーを設定します。

ファイアウォール ドロップ メッセージをログに記録するには、ポリシー マップの class-default クラスの下で **drop-log** コマンドをイネーブルにします。 たとえば、次のポリシー マップを検討します。

```
policy-map type inspect in-out-pol
 class type inspect in-out
```

```
  inspect
 class class-default
  drop-log
policy-map type inspect out-in-pol
 class type inspect out-in
  inspect
 class class-default
  drop-log
```

検査パラメータ マップのドロップされたパケットをログに記録するには、**log dropped-packets enable** コマンドを使用します。 次に、検査ポリシーによりドロップされたパケットのロギングを設定する例を示します。

```
parameter-map type inspect global
 log dropped-packets enable
```

ゾーンベース ポリシー ファイアウォールのクラス マップとポリシー マップ

Quality of Service（QoS）クラス マップには多数の一致基準があります。ファイアウォールの一致基準はそれより少なくなっています。 ファイアウォール クラス マップにはタイプの検査があります。この情報により、ファイアウォール クラス マップの下に表示される内容が決まります。

ポリシーとは、トラフィック クラスとアクションの関連付けです。 定義されたトラフィック クラスで実行するアクションを指定します。アクションは特定の機能で、通常、トラフィック クラスに関連付けられます。 たとえば、**inspect** と **drop** はアクションです。

レイヤ 3 およびレイヤ 4 クラス マップとポリシー マップ

レイヤ 3 およびレイヤ 4 クラス マップは、異なるアクションを実行する必要のあるトラフィック ストリームを識別します。

トラフィックの基本的な検査には、レイヤ 3 またはレイヤ 4 ポリシー マップで十分です。

次の例は、ACL 101 と HTTP プロトコルの一致基準を含むクラス マップ c1 を設定し、さらに p1 という名前の検査ポリシーマップを作成して c1 に一致するトラフィックのパケットをドロップするよう指定する方法を示します。

```
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match access-group 101
Device(config-cmap)# match protocol http
Device(config)# policy-map type inspect p1
Device(config-pmap)# class type inspect c1
Device(config-pmap-c)# drop
```

レイヤ 3 またはレイヤ 4 ポリシーを作成するには、「レイヤ 7 プロトコル固有ファイアウォール ポリシーの設定」の項を参照してください。

クラスマップ設定の制約

トラフィックが複数の一致基準を満たす場合、個別性の高い基準から低い基準の順序で適用する必要があります。 たとえば、次のクラス マップを考えてみましょう。

```
class-map type inspect match-any my-test-cmap
```

```
match protocol http
match protocol tcp
```

この例では、HTTP トラフィックが HTTP インスペクションのサービス固有機能によって確実に処理されるようにするため、トラフィックがまず **match protocol http** コマンドに遭遇するようにする必要があります。「match」の行が逆で、**match protocol http** コマンドと比較される前にトラフィックが **match protocol tcp** コマンドに遭遇した場合、トラフィックは、TCP トラフィックとして分類され、ファイアウォールの TCP インスペクション コンポーネントの機能に従って検査されます。 match protocol TCP が最初に設定されている場合、FTP や TFTP などのサービス、および H.323、リアルタイム ストリーミング プロトコル（RTSP）、Session Initiation Protocol（SIP）、Skinny などのマルチメディアと音声シグナリング サービスで問題を引き起こします。 これらのサービスには、より複雑なアクティビティを認識するために追加のインスペクション機能が必要です。

レイヤ 3 およびレイヤ 4 ポリシー マップ内のレート制限（ポリシング）トラフィック

ご使用のリリースによっては、検査ポリシーで **police** コマンドを使用して、インスタント メッセンジャ（IM）やピアツーピア（P2P）などのアプリケーションに許可する同時接続の数を制限できます。

police コマンドを使用するには、検査ポリシー マップ内の Cisco ステートフル パケット インスペクションをイネーブルにする必要があります。 **inspect** コマンドを設定しないで **police** コマンドを設定すると、エラー メッセージが表示され、**police** コマンドが拒否されます。

既存のポリシング アクションとの互換性

モジュラ QoS CLI（MQC）ポリシーマップでプロビジョニングされたポリシング アクションは、インターフェイスの入力および出力ポリシーとして適用されます。検査ポリシーマップはゾーンペアにのみ適用できます。インターフェイスには適用できません。 このポリシング アクションは、ゾーンペアを通過するトラフィックに対して施行されます。（トラフィックの方向はゾーンペアの仕様に固有のものです）。したがって、ポリシング アクションを含む Quality of Service（QoS）ポリシーは、ゾーン ペアを構成するインターフェイス、およびゾーン ペア全体に適用される検査ポリシー マップに存在します。 両方のポリシング アクションを設定した場合、ゾーンペアのポリシングアクションは、入力インターフェイスのポリシングアクションの後、かつ出力インターフェイスのポリシングアクションの前に実行されます。QoS と検査ポリシングアクションは連携しません。

ポリシングの制約

- ポリシング アクションは、「セルフ」ゾーンを含むゾーン ペアに付加されたポリシーでは許可されません。 このタスクを実行するには、コントロール プレーン ポリシングを使用します。
- ポリシングはレイヤ 3 およびレイヤ 4 ポリシー マップでのみ指定できます。レイヤ 7 ポリシー マップでは指定できません。

レイヤ 7 のクラス マップとポリシー マップ

レイヤ 7 クラス マップは、ディープ パケット インスペクション（DPI）のためにのみ検査ポリシー マップで使用できます。 DPI 機能は、レイヤ 7 クラス マップおよびポリシー マップを通じて提供されます。

レイヤ 7 クラス マップを作成するには、目的のプロトコルに対して **class-map type inspect** コマンドを使用します。 たとえば、HTTP プロトコルの場合は、**class-map type inspect http** コマンドを入力します。

クラス マップのタイプ（HTTP など）によって、使用できる一致基準が決まります。 Java アプレットを含む HTTP トラフィックを指定する場合は、「inspect HTTP」クラス マップのコンテキストで「match response body java」ステートメントを指定する必要があります。

レイヤ 7 ポリシー マップは、アプリケーション レベルでのトラフィックのインスペクションを実現します。 このポリシー マップには、同じタイプのクラス マップを含めることができます。

レイヤ 7 ポリシー マップを作成するには、**policy-map type inspect** コマンドでプロトコルを指定します。 たとえば、レイヤ 7 HTTP ポリシー マップを作成するには、**policy-map type inspect http** *policy-map-name* コマンドを使用します。 *policy-map-name* 引数に HTTP ポリシー マップの名前を入力します。

プロトコル名を指定しない場合（たとえば、**policy-map type inspect** コマンドを使用する場合）は、レイヤ 3 またはレイヤ 4 ポリシー マップを作成します。これは常に検査タイプ ポリシー マップになります。

レイヤ 7 ポリシー マップはレイヤ 3 またはレイヤ 4 ポリシー マップに含める必要があります。ターゲットに直接付加することはできません。 レイヤ 7 ポリシー マップをトップレベル ポリシー マップに付加し、**service-policy** コマンドを使用して、アプリケーション名（つまり、HTTP、Internet Message Access Protocol（IMAP）、Post Office Protocol バージョン 3（POP3）、シンプル メール転送プロトコル（SMTP）、または Sun リモート プロシージャ コール（SUNRPC））を指定します。レイヤ 7 ポリシーを付加する前に、その親クラスに 1 つのレイヤ 7 プロトコルのみに一致する明示的な一致基準を設定しておく必要があります。

レイヤ 7 ポリシー マップが下位のレベルにある場合は、レイヤ 7 ポリシー マップの親レベルで **inspect** アクションを指定する必要があります。

レイヤ 7 のサポート対象プロトコル

次のプロトコルのレイヤ 7 クラス マップおよびポリシー マップを作成できます。

- America Online（AOL）インスタント メッセンジャ（IM）プロトコル。
- eDonkey ピアツーピア（P2P）プロトコル。
- FastTrack トラフィック P2P プロトコル。
- Gnutella バージョン 2 トラフィック P2P プロトコル。
- H.323 VoIP プロトコル バージョン 4。

- HTTP：Web ブラウザと Web サーバがファイル（テキスト ファイルやグラフィック ファイルなど）の転送に使用するプロトコル。
- Internet Message Access Protocol（IMAP）：共有されるメール サーバに保管された電子メールや掲示板メッセージにアクセスする方法。
- I Seek You（ICQ）IM プロトコル。
- Kazaa バージョン 2 P2P プロトコル。
- MSN Messenger IM プロトコル。
- Post Office Protocol, Version 3（POP3）：クライアント電子メール アプリケーションがメール サーバからメールを取得するために使用するプロトコル。
- SIP：Session Initiation Protocol（SIP）。
- SMTP：簡易ネットワーク管理プロトコル。
- SUNRPC：Sun RPC（リモート プロシージャ コール）。
- Windows Messenger IM プロトコル。
- Yahoo IM プロトコル。

レイヤ 7 クラス マップおよびポリシー マップ（ポリシー）の設定の詳細については、「レイヤ 7 プロトコル固有ファイアウォール ポリシーの設定，（36 ページ）」の項を参照してください。

class-default クラス マップ

ユーザ定義クラスに加えて、class-default という名前のシステム定義クラス マップは、ポリシーのユーザ定義クラスのどれとも一致しないすべてのパケットを表します。 class-default クラスは、常にポリシー マップの最後のクラスです。

いずれのユーザ定義クラスとも一致しないパケットのグループに対して明示的にアクションを定義できます。 検査ポリシーで class-default クラスに対してアクションを設定しない場合、デフォルトのアクションは **drop** です。

（注） 検査ポリシーの class-default では、**drop** アクションまたは **pass** アクションのみを設定できます。

次の例は、ポリシー マップで class-default を使用する方法を示します。 この例では、HTTP トラフィックはドロップされ、残りのトラフィックが検査されます。 HTTP トラフィックに対してクラス マップ c1 が定義されており、ポリシー マップ p1 で class-default が使用されています。

```
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match protocol http
Device(config)# policy-map type inspect p1
Device(config-pmap)# class type inspect c1
Device(config-pmap-c)# drop
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
```

階層ポリシー マップ

あるポリシーの中でポリシーをネストできます。 ネストされたポリシーを含むポリシーのことを「階層ポリシー」と呼びます。

階層ポリシーを作成するには、ポリシーをトラフィックのクラスに直接付加します。 階層ポリシーには子ポリシーと親ポリシーが含まれます。 子ポリシーは、**service-policy** コマンドの使用によって新しいポリシーに関連付けられている、事前定義済みのポリシーです。 既存のポリシーを使用する新しいポリシーが親ポリシーです。

（注） 階層検査サービス ポリシーに作成できる階層レベルは 2 レベルまでです。

パラメータ マップ

パラメータ マップを使用すると、ポリシー マップで指定したアクションとクラス マップで指定した一致基準の動作を制御するパラメータを指定できます。

パラメータ マップには次の 3 種類があります。

- 検査パラメータ マップ

  検査パラメータ マップは任意です。 パラメータ マップを使用しない場合、デフォルトのパラメータが使用されます。 inspectアクションに関連付けられたパラメータは、ネストされたすべてのアクション（ある場合）に適用されます。 トップ レベルと下位レベルの両方でパラメータを指定すると、下位レベルのパラメータがトップ レベルのパラメータよりも優先されます。

- URL フィルタ パラメータ マップ

  パラメータ マップは、（レイヤ 3 またはレイヤ 4 ポリシー マップと URL フィルタ パラメータ マップの URL フィルタ アクションによる）URL フィルタリングに必要です。

- プロトコル固有パラメータ マップ

  インスタントメッセンジャ（IM）アプリケーション（レイヤ7）のポリシーマップにはパラメータ マップが必要です。

ファイアウォールとネットワーク アドレス変換

ネットワークアドレス変換（NAT）は、登録されていないIPアドレスを使用してインターネットへ接続するプライベート IP インターネットワークをイネーブルにします。 NAT はデバイス上で動作し、通常は 2 つのネットワークを接続して、内部ネットワークのプライベート（グローバルに一意ではない）アドレスを正規のアドレスに変換してから、パケットを次のネットワークに転送します。 NAT は、ネットワーク全体の 1 つだけのアドレスを外部にアドバタイズするように設

定できます。 NAT が設定されたデバイスには、少なくとも内部ネットワークに対して 1 つ、外部ネットワークに対して 1 つのインターフェイスがあります。

標準的な環境では、NAT はスタブ ドメインとバックボーンの間の出口デバイスに設定されます。パケットがドメインから出て行くとき、NAT はローカルで意味のある送信元アドレスをグローバル固有アドレスに変換します。パケットがドメインに入ってくるときは、NAT はグローバルで一意の宛先アドレスをローカル アドレスに変換します。 出力点が複数存在する場合、個々の NAT は同一の変換テーブルを持っていなければなりません。 アドレスが足りなくなってアドレスを割り当てられなくなった場合、ソフトウェアはそのパケットをドロップし、インターネット制御メッセージ プロトコル（ICMP）ホスト到達不能パケットを送信します。

NAT については、「内部」という用語は組織により所有され、変換を必要とするネットワークを意味します。 このドメイン内では、ホストは 1 つのアドレス空間に複数のアドレスを持ちます。NAT が設定されている場合、ホストが外部にあると、そのホストには別のアドレス空間にアドレスがあるように見えます。内部アドレス空間はローカルアドレス空間として参照され、外部アドレス空間はグローバル アドレス空間として参照されます。

NAT が送信元と宛先の両方の IP アドレスを変換するシナリオについて考えてみます。 パケットは、送信元アドレス 192.168.1.1 および宛先アドレス 10.1.1.1 を使用して NAT の内側からデバイスに送信されます。 NAT は、これらのアドレスを変換し、送信元アドレス 209.165.200.225 および宛先アドレス 209.165.200.224 を使用して外部ネットワークにパケットを送信します。

同様に、応答が外部 NAT から返されると、送信元アドレスは 209.165.200.225 になり、宛先アドレスは 209.165.200.224 になります。 したがって、NAT 内部では、パケットの送信元アドレスは 10.1.1.1、宛先アドレスは 192.168.1.1 となります。

このシナリオでは、ファイアウォール ポリシーで使用されるアプリケーション コントロール エンジン（ACE）を作成する場合は、NAT 前の IP アドレス（別名、内部ローカルおよび外部グローバル アドレス）192.168.1.1 と 209.165.200.224 を使用する必要があります。

Cisco ファイアウォールに関する WAAS のサポート

ご使用のリリースによっては、Wide Area Application Services（WAAS）ファイアウォール ソフトウェアでは、セキュリティ準拠 WAN とアプリケーション アクセラレーション ソリューションを最適化する統合ファイアウォールを提供します。これには、次の利点があります。

- WAAS ネットワークのトランスペアレントな統合。
- トランスペアレントな WAN 加速化トラフィックの保護。
- フル ステートフル インスペクション機能を通して WAN を最適化。
- Payment Card Industry（PCI）コンプライアンスの簡略化。
- ネットワーク管理機器（NME）-Wide Area Application Engine（WAE）モジュールまたはスタンドアロンの WAAS デバイスの導入のサポート。

WAAS には、初期の 3 方向ハンドシェイク中に WAE デバイスをトランスペアレントに識別するための TCP オプションを使用する自動検出メカニズムがあります。 自動検出後、最適化されたト

ラフィック フロー（パス）ではTCP シーケンス番号が変化し、エンドポイントは最適化されたトラフィック フローと最適化されてないトラフィック フローを区別できます。

（注） パスは接続と同じ意味で使用されています。

WAAS により、Cisco ファイアウォールは、内部ファイアウォール TCP ステート変数を含む TCP トラフィック フローのステートフルなレイヤ 4 インスペクションを損なうことなく、シーケンス番号を変更できるようにすることで、最適化されたトラフィックを自動的に検出できます。 これらの変数は、WAE デバイスの存在に応じて調整されます。

Cisco ファイアウォールは、トラフィック フローが正常に WAAS 自動検出を完了したことを認識すると、トラフィック フロー用の初期シーケンス番号のシフトを許可し、最適化されたトラフィック フローのレイヤ 4 の状態を維持します。

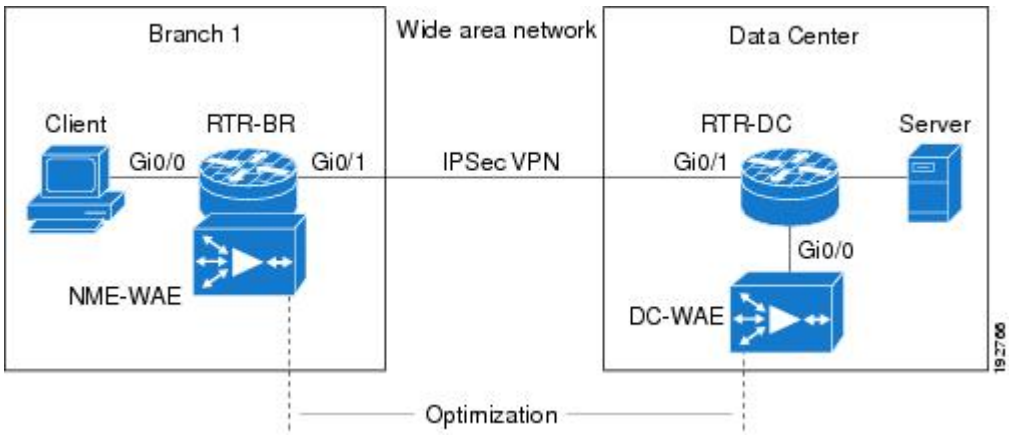
（注） クライアント側のステートフルなレイヤ7インスペクションは、最適化されてないトラフィックでも実行できます。

WAAS トラフィック フロー最適化展開シナリオ

次の各項では、支店オフィス展開における 2 種類の WAAS トラフィック フロー最適化シナリオについて説明します。 WAAS トラフィック フローの最適化は、シスコ サービス統合型ルータ（ISR）の Cisco ファイアウォール機能と連動します。

下の図は、Cisco ファイアウォールを使用したエンドツーエンドの WAAS トラフィック フロー最適化の例を示しています。 この特別な展開では、ネットワーク管理機器（NME）-WAE デバイスは、Cisco ファイアウォールと同じデバイス上にあります。 Web Cache Communication Protocol（WCCP）を使用して、代行受信するためにトラフィックをリダイレクトします。

図 *4*：エンドツーエンドの *WAAS* 最適化パス

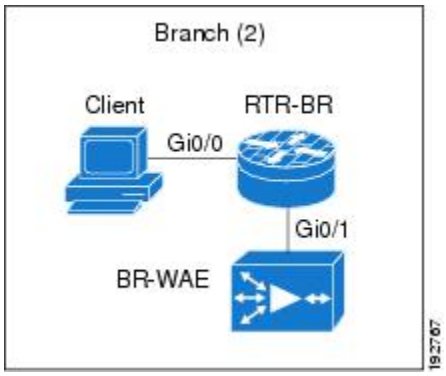


Off-Path デバイスによる WAAS 支店の展開

Wide Area Application Engine（WAE）デバイスは、（Wide Area Application Services（WAAS）支店の展開の図に示すように）統合サービス エンジンとしてサービス統合型ルータ（ISR）にインストールされたスタンドアロン WAE デバイスまたは NME-WAE です。

下の図は、トラフィック代行受信のために、Web Cache Communication Protocol（WCCP）を使用して、トラフィックを Off-Path スタンドアロン WAE デバイスにリダイレクトする WAAS 支店の展開を示します。 このオプションの設定は、NME-WAE を使用した WAAS 支店の展開と同じです。

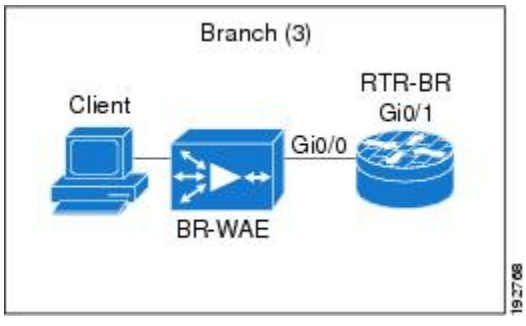
図 *5*：*WAAS Off-Path* 支店の展開



インライン デバイスを使用した WAAS 支店の展開

下の図は、物理的にサービス統合型ルータ（ISR）の前にあるインライン Wide Area Application Engine（WAE）デバイスが含まれた Wide Area Application Services（WAAS）支店の展開を示します。 WAE デバイスがデバイスの前にあるため、Cisco ファイアウォールは WAAS 最適化パケットを受信し、その結果、クライアント側のレイヤ 7 インスペクションはサポートされません。

図 *6*：*WAAS* インライン パス支店の展開



ブランチ オフィス サイトで WAN 接続へのトラフィック、および WAN 接続からのトラフィックを検査する場合は、そのサイトで Cisco ファイアウォールを備えたエッジ WAAS デバイスを使用します。 Cisco ファイアウォールは、最適化インジケータ（TCP オプションおよび後続 TCP シー

ケンス番号の変更）のためにトラフィックをモニタし、すべてのトラフィックにレイヤ4のステートフル インスペクションとディープ パケット インスペクションを提供しながら、最適化されたトラフィックが通過できるようにすることで、WAAS 最適化の利点に対応すると同時にセキュリティを維持します。

（注） WAE デバイスがインライン ロケーションにある場合、デバイスは自動検出プロセス後にバイパス モードになります。 デバイスは WAAS 最適化に直接関係しませんが、Cisco ファイアウォール インスペクションをネットワーク トラフィックに適用し、最適化インジケータが存在する場合は最適化アクティビティに対応できるようにするには、WAAS 最適化がトラフィックに適用されていることをデバイスが認識できる必要があります。

ゾーンベース ファイアウォール アプリケーションでの Out-of-Order パケット処理のサポート

Common Classification Engine（CCE）ファイアウォール アプリケーションで Out-of-Order（OoO）パケット処理がサポートされ、侵入防御システム（IPS）で CCE が採用されていることにより、誤った順序で到着したパケットを正しい順序でコピーして再構築できます。 OoO パケット処理は、ドロップされたパケットの再送信の必要性を減らし、ネットワークでのトラフィックの送信に必要な帯域幅を削減します。 OoO サポートを設定するには、**parameter-map type ooo global** コマンドを使用します。

（注） IPS セッションは、**parameter-map type ooo global** コマンドを使用して設定された OoO パラメータを使用します。

OoO 処理は、シンプル メール転送プロトコル（SMTP）ではサポートされていません。これは、SMTP がパケットの変更を必要とするマスキング アクションをサポートしているためです。

OoO パケット処理のサポートは、レイヤ7ポリシーを次のプロトコルでディープ パケット インスペクション（DPI）用に設定している場合はデフォルトでイネーブルになります。

- AOL IM プロトコル。
- eDonkey P2P プロトコル。
- FastTrack トラフィック P2P プロトコル。
- Gnutella バージョン 2 トラフィック P2P プロトコル。
- H.323 VoIP プロトコル バージョン 4。
- HTTP：Web ブラウザと Web サーバがファイル（テキスト ファイルやグラフィック ファイルなど）の転送に使用するプロトコル。
- IMAP：共有されるメール サーバに保管された電子メールや掲示板メッセージにアクセスする方法。

- ICQ IM プロトコル。
- Kazaa バージョン 2 P2P プロトコル。
- 一致プロトコル SIP：一致プロトコル SIP。
- MSN Messenger IM プロトコル。
- POP3：クライアント電子メール アプリケーションがメール サーバからメールを取得するために使用するプロトコル。
- SUNRPC：Sun RPC。
- Windows Messenger IM プロトコル。
- Yahoo IM プロトコル。

レイヤ 7 クラス マップおよびポリシー マップ（ポリシー）の設定の詳細については、「レイヤ 7 プロトコル固有ファイアウォール ポリシーの設定」の項を参照してください。

（注） OoOパケットは、レイヤ4インスペクションを使用するIPSおよびゾーンベースポリシーファイアウォールがイネーブルな場合、ドロップされます。

ゾーンベース ファイアウォール アプリケーションでのイントラゾーンのサポート

イントラゾーンがサポートされていることで、ネットワーク内部のユーザとネットワーク外部のユーザの両方をゾーン構成に含めることができます。イントラゾーンのサポートにより、異なるネットワーク上の同じゾーンに属するユーザ間のトラフィック インスペクションが可能となります。 ご使用のリリースによっては、デフォルトで、ゾーン内のトラフィックが検査なしの通過を許可されていました。 送信元ゾーンと宛先ゾーンが同じであるゾーンペア定義を設定するには、**zone-pair security** コマンドを使用します。 これにより、ポリシー マップを付加し、同じゾーン内のトラフィックを検査することができます。

ゾーンベース ポリシー ファイアウォールの設定方法

レイヤ 3 およびレイヤ 4 ファイアウォール ポリシーの設定

レイヤ 3 およびレイヤ 4 のポリシーは、ターゲット（ゾーン ペア）に付加される「トップ レベル」のポリシーです。 レイヤ 3 およびレイヤ 4 のファイアウォール ポリシーを設定するには、次の作業を実行します。

レイヤ 3 およびレイヤ 4 のファイアウォール ポリシーのクラス マップの設定

ネットワーク トラフィックを分類するためのクラスマップを設定するには、次の作業を実行します。

（注） ステップ 4、5、6 のうち、少なくとも 1 つの一致手順を実行する必要があります。

パケットがアクセスグループ、プロトコル、クラスマップのいずれかにマッチングされると、それらのパケットのトラフィック レートが生成されます。 ゾーンベースのファイアウォール ポリシーでは、セッションを作成する最初のパケットのみがポリシーに一致します。 このフローの後続のパケットは、設定されているポリシーのフィルタに一致しませんが、セッションに直接一致します。 後続のパケットに関連する統計情報が検査アクションの一部として表示されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** [**match-any** | **match-all**] *class-map-name*
4. **match access-group** {*access-group* | **name** *access-group-name*}
5. **match protocol** *protocol-name* [**signature**]
6. **match class-map** *class-map-name*
7. **end**
8. **show policy-map type inspect zone-pair session**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect** [**match-any** | **match-all**] *class-map-name* 例： `Device(config)# class-map type inspect match-all c1`	レイヤ 3 またはレイヤ 4 の検査タイプ クラスマップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**match access-group** {*access-group* | **name** *access-group-name*} 例： `Device(config-cmap)# match access-group 101`	アクセス コントロール リスト（ACL）の名前または番号に基づいて、クラス マップの一致基準を設定します。
ステップ 5	**match protocol** *protocol-name* [**signature**] 例： `Device(config-cmap)# match protocol http`	指定したプロトコルに基づいてクラス マップの一致基準を設定します。 • 検査タイプ クラス マップの一致基準には、Cisco ステートフル パケット インスペクションでサポートされているプロトコルのみを使用できます。 • **signature**：ピアツーピア（P2P）パケットのシグニチャ ベースの分類がイネーブルになります。
ステップ 6	**match class-map** *class-map-name* 例： `Device(config-cmap)# match class-map c1`	前に定義したクラスをクラス マップの一致基準として指定します。
ステップ 7	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 8	**show policy-map type inspect zone-pair session** 例： `Device(config-cmap)# show policy-map type inspect zone-pair session`	（任意）ポリシー マップが指定したゾーン ペアに適用されているため、作成された Cisco ステートフル パケット インスペクション セッションを表示します。 （注） クラスマップ フィールドの下に表示される情報は、接続開始トラフィックのみに属するトラフィックのトラフィック レート（ビット/秒）です。 接続セットアップ レートが非常に高く、レートが計算される複数のインターバルにわたって高い接続セットアップ レートが持続する場合を除き、接続に関する意味のあるデータは表示されません。

レイヤ 3 およびレイヤ 4 のファイアウォール ポリシーのポリシー マップの作成

後でゾーン ペアに付加するレイヤ 3 およびレイヤ 4 ファイアウォール ポリシーのポリシー マップを作成するには、次の作業を実行します。

（注） 検査タイプのポリシーマップを作成している場合、作成できるのはdrop、inspect、pass、police、service-policy、および urlfilter アクションだけなので注意してください。

（注） ステップ 5、8、9、10 のうち、少なくとも 1 つの手順を実行する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class type inspect** *class-name*
5. **inspect** [*parameter-map-name*]
6. **police rate** *units* **bps burst** *burst-in-bytes* **bytes**
7. **drop** [**log**]
8. **pass**
9. **service-policy type inspect** *policy-map-name*
10. **urlfilter** *parameter-map-name*
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p1`	レイヤ 3 およびレイヤ 4 の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**class type inspect** *class-name* 例： `Device(config-pmap)# class type inspect c1`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect inspect-params`	Cisco ステートフル パケット インスペクションをイネーブルにします。
ステップ 6	**police rate** *units* **bps burst** *burst-in-bytes* **bytes** 例： `Device(config-pmap-c)# police rate 2000 bps burst 3000 bytes`	（任意）ファイアウォール（検査）ポリシー内で一致するトラフィックを制限します。
ステップ 7	**drop** [**log**] 例： `Device(config-pmap-c)# drop`	（任意）定義されたクラスと一致するパケットをドロップします。 （注） アクションの **drop** と **pass** は排他的です。また、アクションの **inspect** と **drop** も排他的です。つまり、両方を同時に指定することはできません。
ステップ 8	**pass** 例： `Device(config-pmap-c)# pass`	（任意）定義されたクラスと一致するパケットを許可します。
ステップ 9	**service-policy type inspect** *policy-map-name* 例： `Device(config-pmap-c)# service-policy type inspect p1`	ファイアウォール ポリシー マップをゾーン ペアに付加します。
ステップ 10	**urlfilter** *parameter-map-name* 例： `Device(config-pmap-c)# urlfilter param1`	（任意）Cisco ファイアウォール URL フィルタリングをイネーブルにします。
ステップ 11	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

パラメータ マップの設定

作成するポリシーによっては、検査、URL フィルタ、プロトコル固有のいずれかのパラメータ マップを設定できます。URL フィルタ タイプまたはプロトコル固有ポリシーを設定する場合は、パラメータ マップを設定する必要があります。ただし、検査タイプのポリシーを使用する場合には、パラメータ マップは任意です。

（注） パラメータ マップへの変更は、ファイアウォールを通してすでに確立している接続には反映されません。 変更は、ファイアウォールに許可された新しい接続だけに適用されます。 ファイアウォールでポリシーが厳格に適用されるようにするには、パラメータ マップの変更後に、ファイアウォールで許可されたすべての接続をクリアしてください。 既存の接続をクリアするには、**clear zone-pair inspect sessions** コマンドを使用します。

パラメータ マップを設定するには、次のいずれかの作業を実行します。

検査パラメータ マップの作成

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** {*parameter-map-name* | **global** | **default**}
4. **log** {**dropped-packets** {**disable** | **enable**} | **summary** [**flows** *number*] [**time-interval** *seconds*]}
5. **alert** {**on** | **off**}
6. **audit-trail** {**on** | **off**}
7. **dns-timeout** *seconds*
8. **icmp idle-timeout** *seconds*
9. **max-incomplete** {**low** | **high**} *number-of-connections*
10. **one-minute** {**low** | **high**} *number-of-connections*
11. **sessions maximum** *sessions*
12. **tcp finwait-time** *seconds*
13. **tcp idle-time** *seconds*
14. **tcp max-incomplete host** *threshold* [**block-time** *minutes*]
15. **tcp synwait-time** *seconds*
16. **tcp window-scale-enforcement loose**
17. **udp idle-time** *seconds*
18. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect** {*parameter-map-name* | **global** | **default**} 例： `Device(config)# parameter-map type inspect eng-network-profile`	接続しきい値、タイムアウト、およびその他の **inspect** アクションに関連するパラメータの検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**log** {**dropped-packets** {**disable** | **enable**} | **summary** [**flows** *number*] [**time-interval** *seconds*]} 例： `Device(config-profile)# log summary flows 15 time-interval 30`	（任意）ファイアウォール アクティビティの実行時のパケット ロギングを設定します。 （注） このコマンドが見えるのは、パラメータ マップ タイプ検査コンフィギュレーション モードの場合のみです。
ステップ 5	**alert** {**on** | **off**} 例： `Device(config-profile)# alert on`	（任意）コンソールに表示される Cisco ステートフル パケット インスペクション アラート メッセージをイネーブルにします。
ステップ 6	**audit-trail** {**on** | **off**} 例： `Device(config-profile)# audit-trail on`	（任意）監査証跡メッセージをイネーブルにします。
ステップ 7	**dns-timeout** *seconds* 例： `Device(config-profile)# dns-timeout 60`	（任意）ドメイン ネーム システム（DNS）のアイドル タイムアウト（アクティビティのない間、DNS ルックアップ セッションが管理される時間の長さ）を指定します。
ステップ 8	**icmp idle-timeout** *seconds* 例： `Device(config-profile)# icmp idle-timeout 90`	（任意）Internet Control Message Protocol（ICMP）セッションのタイムアウトを設定します。

	コマンドまたはアクション	目的
ステップ 9	**max-incomplete** {**low** | **high**} *number-of-connections* 例： `Device(config-profile)# max-incomplete low 800`	（任意）Cisco ファイアウォールによるハーフオープン セッションの削除の開始および停止を起動する既存のハーフオープン セッションの数を定義します。
ステップ 10	**one-minute** {**low** | **high**} *number-of-connections* 例： `Device(config-profile)# one-minute low 300`	（任意）システムによるハーフオープン セッションの削除の開始と停止を起動する新規の未確立セッションの数を定義します。
ステップ 11	**sessions maximum** *sessions* 例： `Device(config-profile)# sessions maximum 200`	（任意）1 つのゾーン ペアに存在できる許可されたセッションの最大数を設定します。 • このコマンドを使用して、セッションで使用される帯域幅を制限します。
ステップ 12	**tcp finwait-time** *seconds* 例： `Device(config-profile)# tcp finwait-time 5`	（任意）Cisco ファイアウォールが finish（FIN）-exchange を検出した後、TCP セッションが管理される時間の長さを指定します。
ステップ 13	**tcp idle-time** *seconds* 例： `Device(config-profile)# tcp idle-time 90`	（任意）TCP セッションのタイムアウトを設定します。
ステップ 14	**tcp max-incomplete host** *threshold* [**block-time** *minutes*] 例： `Device(config-profile)# tcp max-incomplete host 500 block-time 10`	（任意）TCP ホスト固有のサービス拒否（DoS）の検出および回避のために、しきい値とブロックする時間値を指定します。
ステップ 15	**tcp synwait-time** *seconds* 例： `Device(config-profile)# tcp synwait-time 3`	（任意）セッションをドロップする前に、TCP セッションが設定された状態に達するまで待機する時間を指定します。
ステップ 16	**tcp window-scale-enforcement loose** 例： `Device(config-profile)# tcp window-scale-enforcement loose`	（任意）ゾーンベース ポリシー ファイアウォールにおいて無効なウィンドウ スケール オプションを持つ TCP パケットのウィンドウ スケール オプションのチェックをパラメータ マップでディセーブルにします。

	コマンドまたはアクション	目的
ステップ 17	**udp idle-time** *seconds* 例： `Device(config-profile)# udp idle-time 75`	（任意）ファイアウォールを通る UDP セッションのアイドル タイムアウトを設定します。
ステップ 18	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権EXECコンフィギュレーション モードを開始します。

URL フィルタ パラメータ マップの作成

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type urlfilter** *parameter-map-name*
4. **alert** {**on** | **off**}
5. **allow-mode** {**on** | **off**}
6. **audit-trail** {**on** | **off**}
7. **cache** *number*
8. **exclusive-domain** {**deny** | **permit**} *domain-name*
9. **max-request** *number-of-requests*
10. **max-resp-pak** *number-of-requests*
11. **server vendor** {**n2h2** | **websense**} {*ip-address* | *hostname* [**port** *port-number*]} [**outside**] [**log**] [**retrans** *retransmission-count*] [**timeout** *seconds*]
12. **source-interface** *interface-name*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type urlfilter** *parameter-map-name* 例： `Device(config)# parameter-map type urlfilter eng-network-profile`	URL フィルタリング パラメータのパラメータ マップを作成または変更し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。 （注） ご使用のリリースによっては、このコマンドは非表示になりますが、引き続き機能します。**parameter-map type urlfpolicy** コマンドは、ローカル、トレンド、Websense インターネット フィルタリング、および N2H2 インターネット ブロッキング プログラムの URL フィルタリング パラメータの作成に使用することもできます。ご使用のリリースによっては、URL フィルタ アクションではなく URL フィルタ ポリシーを使用してください。URL フィルタによってアクションとしてサポートされている使用例はすべて、URL フィルタ ポリシーでもサポートされています。詳細については、「URL フィルタ ポリシーの設定」の項を参照してください。
ステップ 4	**alert** {**on** | **off**} 例： `Device(config-profile)# alert on`	（任意）コンソールに表示される Cisco ステートフル パケット インスペクション アラート メッセージをイネーブルにします。
ステップ 5	**allow-mode** {**on** | **off**} 例： `Device(config-profile)# allow-mode on`	（任意）フィルタリング アルゴリズムのデフォルト モードをイネーブルにします。
ステップ 6	**audit-trail** {**on** | **off**} 例： `Device(config-profile)# audit-trail on`	（任意）監査証跡メッセージをイネーブルにします。
ステップ 7	**cache** *number* 例： `Device(config-profile)# cache 5`	（任意）URL フィルタが維持する HTTP サーバのキャッシュを URL フィルタがどのように扱うかを制御します。

	コマンドまたはアクション	目的
ステップ 8	**exclusive-domain** {**deny** | **permit**} *domain-name* 例： `Device(config-profile)# exclusive-domain permit cisco.com`	（任意）Cisco ファイアウォールがベンダー サーバにルックアップ要求を送信しなくて済むように、専用ドメイン リストにドメイン名を追加します。
ステップ 9	**max-request** *number-of-requests* 例： `Device(config-profile)# max-request 80`	（任意）同時に存在できる未処理要求の最大数を指定します。
ステップ 10	**max-resp-pak** *number-of-requests* 例： `Device(config-profile)# max-resp-pak 200`	（任意）Cisco ファイアウォールがパケット バッファに保持できる HTTP 応答の最大数を指定します。
ステップ 11	**server vendor** {**n2h2** | **websense**} {*ip-address* | *hostname* [**port** *port-number*]} [**outside**] [**log**] [**retrans** *retransmission-count*] [**timeout** *seconds*] 例： `Device(config-profile)# server vendor n2h2 10.193.64.22 port 3128 outside retrans 9 timeout 8`	URL フィルタリング サーバを指定します。
ステップ 12	**source-interface** *interface-name* 例： `Device(config-profile)# source-interface ethernet0`	（任意）URL フィルタ サーバ（N2H2 または Websense）への TCP 接続を確立するときに送信元 IP アドレスとして使用する IP アドレスを持つインターフェイスを指定します。
ステップ 13	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC コンフィギュレーション モードを開始します。

レイヤ 7 プロトコル固有パラメータ マップの設定

（注） プロトコル固有パラメータ マップは、インスタント メッセンジャ アプリケーション（AOL、ICQ、MSN Messenger、Yahoo Messenger、Windows Messenger）のためにのみ作成されます。

はじめる前に

名前解決をイネーブルにするには、**ip domain name** コマンドと **ip name-server** コマンドをイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type protocol-info** *parameter-map-name*
4. **server** {**name** *string* [**snoop**] | **ip** {*ip-address* | **range** *ip-address-start ip-address-end*}}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type protocol-info** *parameter-map-name* 例： `Device(config)# parameter-map type protocol-info ymsgr`	アプリケーション固有のパラメータ マップを定義し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**server** {**name** *string* [**snoop**]	**ip** {*ip-address*	**range** *ip-address-start ip-address-end*}} 例： `Device(config-profile)# server name example1.example.com`	特定のインスタント メッセンジャ アプリケーションが相互通信するドメイン ネーム システム（DNS）サーバ セットを設定します。 （注） 少なくとも 1 つのサーバ インスタンスが設定されていない場合、パラメータ マップには適用する定義がありません。つまり、設定されたインスタント メッセンジャ ポリシーは適用できません。 （注） 複数のサーバ セットを設定するには、インスタント メッセンジャのパラメータ マップ内で **server** コマンドを複数回発行します。 複数のエントリは、累積的に処理されます。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC コンフィギュレーション モードを開始します。

トラブルシューティングのヒント

インスタント メッセンジャ（IM）プロトコル固有のパラメータ マップの詳細を表示するには、**show parameter-map type protocol-info** コマンドを使用します。

ゾーンベース ファイアウォール アプリケーションでの OoO パケット処理のサポートの設定

（注） ディープ パケット インスペクション（DPI）のために TCP ベースのレイヤ 7 ポリシーを設定した場合、Out-of-Order（OoO）パケット処理はデフォルトでイネーブルになります。 OoO パケット サポート パラメータを設定する場合や OoO 処理をディセーブルにする場合は **parameter-map type ooo global** コマンドを使用します。 ご使用のリリースによっては、ゾーンベース ファイアウォールおよび侵入防御システム（IPS）の、レイヤ 4 一致（**match protocol tcp**、**match protocol http**）、および任意の TCP ベース レイヤ 7 パケット配列が使用された共有セッションで、OoO 処理がイネーブルになっていました。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type ooo global**
4. **tcp reassembly alarm** {**on** | **off**}
5. **tcp reassembly memory limit** *memory-limit*
6. **tcp reassembly queue length** *queue-length*
7. **tcp reassembly timeout** *time-limit*
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type ooo global** 例： `Device(config)# parameter-map type ooo global`	OoO 処理を設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**tcp reassembly alarm** {**on** | **off**} 例： `Device(config-profile)# tcp reassembly alarm on`	アラート メッセージ コンフィギュレーションを指定します。
ステップ 5	**tcp reassembly memory limit** *memory-limit* 例： `Device(config-profile)# tcp reassembly memory limit 2048`	OoO ボックスワイド バッファ サイズを指定します。
ステップ 6	**tcp reassembly queue length** *queue-length* 例： `Device(config-profile)# tcp reassembly queue length 45`	TCP フローごとの OoO キュー長を指定します。
ステップ 7	**tcp reassembly timeout** *time-limit* 例： `Device(config-profile)# tcp reassembly timeout 34`	OoO キュー再構築タイムアウト値を指定します。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC コンフィギュレーション モードを開始します。

ゾーンベースファイアウォールアプリケーションでのイントラゾーンのサポートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **zone-pair security** *zone-pair-name* [**source** *source-zone-name* **destination** *destination-zone-name*]
4. **exit**
5. **policy-map type inspect** *policy-map-name*
6. **class-map type inspect** *protocol-name* {**match-any** | **match-all**}*class-map-name*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone-pair security** *zone-pair-name* [**source** *source-zone-name* **destination** *destination-zone-name*] 例： `Device(config)# zone-pair security zonepair17 source zone8 destination zone8`	インターフェイスに付加するゾーン ペアの名前と、このゾーン ペアを通過する情報の送信元ゾーンおよび宛先ゾーンを指定します。 • セキュリティ ゾーンペア コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
		（注） イントラゾーンのサポートを設定するには、送信元ゾーンと宛先ゾーンを同じにする必要があります。
ステップ 4	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect my-pmap`	ポリシー マップ名を指定し、Quality of Service（QoS）ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 6	**class-map type inspect** *protocol-name* {**match-any** | **match-all**}*class-map-name* 例： `Device(config-pmap)# class-map type inspect aol match-any cmap1`	ファイアウォールのクラス マップ プロトコルとクラス マップ名を指定します。
ステップ 7	**end** 例： `Device(config-pmap)# end`	QoS ポリシー マップ コンフィギュレーション モードを終了し、特権 EXEC コンフィギュレーション モードを開始します。

レイヤ 7 プロトコル固有ファイアウォール ポリシーの設定

レイヤ 7 インスペクション モジュールの追加プロビジョニングが必要な場合は、レイヤ 7 ポリシー マップを設定します。 必ずしもこの項で指定されているすべてのレイヤ 7 ポリシー マップを設定する必要はありません。

レイヤ 7 プロトコル固有ファイアウォール ポリシーを設定するには、次のいずれかの作業を実行します。

レイヤ 7 のクラス マップとポリシー マップの制約

- レイヤ 7 のディープ パケット インスペクション（DPI）クラス マップは、該当するタイプの検査ポリシー マップで使用できます。 たとえば、**class-map type inspect http** は、**policy-map type inspect http** でのみ使用できます。
- DPI ポリシーでは、親レベルに **inspect** アクションが必要です。

- レイヤ 3 またはレイヤ 4 検査ポリシーは第 1 レベルで付加できますが、レイヤ 7（DPI）ポリシー マップはレイヤ 3 またはレイヤ 4 検査ポリシー マップ内の第 2 レベルにネストする必要があります。したがって、レイヤ 7 ポリシーマップはゾーンペアに直接付加できません。
- 検査サービス ポリシーの階層パスでアクションが指定されていない場合、パケットはドロップされます。トップレベル ポリシーの class-default に一致するトラフィックは、class-default で明示的にアクションが設定されていない場合、ドロップされます。レイヤ 7 ポリシーのどのクラスとも一致しないトラフィックはドロップされません。制御が親ポリシーに戻り、親ポリシーに後続のアクションがあれば、そのアクションがパケットに対して実行されます。
- レイヤ 7 ポリシー マップには、同じタイプのクラス マップのみが含まれます。
- **reset** アクションは TCP トラフィックに対してのみ指定できます。このアクションは TCP 接続をリセットします。
- ご使用のリリースによっては、正規表現によるヘッダーがあるクラスをレイヤ 7 ポリシー マップから削除すると、アクティブな HTTP セッションがリセットされます。この変更が行われる前は、クラスがレイヤ 7 ポリシーマップから削除されたときに、デバイスがリロードされます。

HTTP ファイアウォール ポリシーの設定

パラメータ マップ内の要素に基づいて一致基準を設定する場合は、「検査パラメータ マップの作成」に従ってパラメータ マップを設定する必要があります。

少なくとも 1 つの一致基準を指定する必要があります。一致基準を指定しなければ、ファイアウォール ポリシーは有効になりません。

HTTP ファイアウォール クラス マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect http** [**match-any** | **match-all**] *class-map-name*
4. **match response body java-applet**
5. **match req-resp protocol violation**
6. **match req-resp body length** {**lt** | **gt**} *bytes*
7. **match req-resp header content-type** {**violation** | **mismatch** | **unknown**}
8. **match** {**request** | **response** | **req-resp**} **header** [*header-name*] **count gt** *number*
9. **match** {**request** | **response** | **req-resp**} **header** [*header-name*] **length gt** *bytes*
10. **match request** {**uri** | **arg**} **length gt** *bytes*
11. **match request method** {**connect** | **copy** | **delete** | **edit** | **get** | **getattribute** | **getattributenames** | **getproperties**| **head** | **index** | **lock** | **mkdir** | **move** | **options** | **post** | **put** | **revadd** | **revlabel** | **revlog** | **revnum** | **save** | **setattribute** | **startrev** | **stoprev** | **trace** | **unedit** | **unlock**}
12. **match request port-misuse** {**im** | **p2p** | **tunneling** | **any**}
13. **match req-resp header transfer-encoding** {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **all**}
14. **match** {**request** | **response** | **req-resp**} **header** [*header-name*] **regex** *parameter-map-name*
15. **match request uri regex** *parameter-map-name*
16. **match** {**request** | **response** | **req-resp**} **body regex** *parameter-map-name*
17. **match response status-line regex** *parameter-map-name*
18. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**class-map type inspect http** [**match-any** | **match-all**] *class-map-name* 例： `Device(config)# class-map type inspect http http-class`	一致基準を入力するために HTTP プロトコルのクラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match response body java-applet** 例： `Device(config-cmap)# match response body java-applet`	（任意）HTTP 接続で Java アプレットを識別します。
ステップ 5	**match req-resp protocol violation** 例： `Device(config-cmap)# match req-resp protocol violation`	（任意）HTTP 非準拠トラフィックが検出されたされたときにHTTP メッセージがファイアウォールを通過、またはTCP 接続をリセットできるように HTTP クラス マップを設定します。
ステップ 6	**match req-resp body length** {**lt** | **gt**} *bytes* 例： `Device(config-cmap)# match req-resp body length gt 35000`	（任意）HTTP トラフィックのファイアウォールの通過を許可または拒否するための一致基準としてメッセージの最小サイズまたは最大サイズ（バイト単位）を使用できるように HTTP クラス マップを設定します。
ステップ 7	**match req-resp header content-type** {**violation** | **mismatch** | **unknown**} 例： `Device(config-cmap)# match req-resp header content-type mismatch`	（任意）HTTP トラフィックのコンテンツ タイプに基づいて HTTP クラス マップを設定します。
ステップ 8	**match** {**request** | **response** | **req-resp**} **header** [*header-name*] **count gt** *number* 例： `Device(config-cmap)# match req-resp header count gt 16`	（任意）要求と応答の両方のメッセージのヘッダー カウントが指定されたフィールドの最大数を超えているかどうかに基づいて HTTP トラフィックを許可または拒否する HTTP ファイアウォール ポリシーを設定します。
ステップ 9	**match** {**request** | **response** | **req-resp**} **header** [*header-name*] **length gt** *bytes* 例： `Device(config-cmap)# match response header length gt 50000`	（任意）HTTP 要求ヘッダーの長さに基づいて HTTP トラフィックを許可または拒否します。

	コマンドまたはアクション	目的
ステップ 10	**match request** {**uri** | **arg**} **length gt** *bytes* 例： `Device(config-cmap)# match request uri length gt 500`	（任意）HTTP トラフィックを許可または拒否するための一致基準として要求メッセージ内の Uniform Resource Identifier（URI）または引数の長さを使用する HTTP ファイアウォール ポリシーを設定します。
ステップ 11	**match request method** {**connect** | **copy** | **delete** | **edit** | **get** | **getattribute** | **getattributenames** | **getproperties**| **head** | **index** | **lock** | **mkdir** | **move** | **options** | **post** | **put** | **revadd** | **revlabel** | **revlog** | **revnum** | **save** | **setattribute** | **startrev** | **stoprev** | **trace** | **unedit** | **unlock**} 例： `Device(config-cmap)# match request method connect`	（任意）HTTP トラフィックを許可または拒否するための一致基準として要求メソッドまたは拡張メソッドを使用する HTTP ファイアウォール ポリシーを設定します。
ステップ 12	**match request port-misuse** {**im** | **p2p** | **tunneling** | **any**} 例： `Device(config-cmap)# match request port-misuse any`	（任意）HTTP ポートを誤用しているアプリケーションを特定します。
ステップ 13	**match req-resp header transfer-encoding** {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **all**} 例： `Device(config-cmap)# match req-resp header transfer-encoding compress`	（任意）メッセージの指定した転送エンコーディングに従って HTTP トラフィックを許可または拒否します。
ステップ 14	**match** {**request** | **response** | **req-resp**} **header** [*header-name*] **regex** *parameter-map-name* 例： `Device(config-cmap)# match req-resp header regex non_ascii_regex`	（任意）ヘッダーがパラメータ マップで定義された正規表現と一致するかどうかに基づいて HTTP ファイアウォール ポリシーの一致基準を設定します。 • HTTP には 2 つの正規表現（regex）オプションがあります。 1 つは **header** キーワード、**content-type** ヘッダー名、および **regex** キーワードと *parameter-map-name* 引数を組み合わせたもので、 もう 1 つは **header** キーワードと **regex** キーワードを *parameter-map-name* 引数と組み合わせたものです。 • **header** および **regex** キーワードを *parameter-map-name* 引数と組み合わせる場合には、*parameter-map-name* 引数の前にピリオドとアスタリスクは必要ありません。 たとえば、*parameter-map-name* 引数として「html」と「.*html」のいずれを設定してもかまいません。

	コマンドまたはアクション	目的
		• **header** キーワードを content-type ヘッダー名および **regex** キーワードと組み合わせる場合には、*parameter-map-name* 引数の前にピリオドとアスタリスク（.*）が必要です。 たとえば、*parameter-map-name* 引数の「html」は「.*html」と表現します。 （注） 「html」の前にピリオドとアスタリスクを追加した場合（.*html）、その *parameter-map-name* 引数は両方の HTTP regex オプションに対して機能します。 • **mismatch** キーワードは、**match response header content-type regex** コマンド構文で、content-type ヘッダー名の不一致があるメッセージと一致させる場合にのみ有効です。 ヒント **regex** *parameter-map-name* 引数がテキスト文字列の先頭にない場合、「.*」を追加するのは良い方法です。
ステップ 15	**match request uri regex** *parameter-map-name* 例： `Device(config-cmap)# match request uri regex uri-regex-cm`	（任意）要求メッセージの URI または引数（パラメータ）が定義された正規表現と一致しているかどうかに基づいて HTTP トラフィックを許可または拒否する HTTP ファイアウォール ポリシーを設定します。
ステップ 16	**match** {**request** | **response** | **req-resp**} **body regex** *parameter-map-name* 例： `Device(config-cmap)# match response body regex body-regex`	（任意）要求メッセージ、応答メッセージ、または要求メッセージと応答メッセージの両方の本体と照合する正規表現のリストを設定します。
ステップ 17	**match response status-line regex** *parameter-map-name* 例： `Device(config-cmap)# match response status-line regex status-line-regex`	（任意）応答メッセージのステータス ラインと照合する正規表現のリストを指定します。
ステップ 18	**end** 例： `Device(config-cmap)# end`	（任意）QoS クラス マップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

HTTP ファイアウォール ポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect http** *policy-map-name*
4. **class-type inspect http** *http-class-name*
5. **allow**
6. **log**
7. **reset**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect http** *policy-map-name* 例： `Device(config)# policy-map type inspect http myhttp-policy`	レイヤ 7 HTTP ポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class-type inspect http** *http-class-name* 例： `Device(config-pmap)# class-type inspect http http-class`	HTTP プロトコルのクラス マップを作成します。
ステップ 5	**allow** 例： `Device(config-pmap)# allow`	（任意）このクラスに一致するトラフィック クラスを許可します。

	コマンドまたはアクション	目的
ステップ 6	**log** 例： `Device(config-pmap)# log`	ログ メッセージが生成されます。
ステップ 7	**reset** 例： `Device(config-pmap)# reset`	（任意）シンプル メール転送プロトコル（SMTP）本体のデータ長が **class-map type inspect smtp** コマンドで設定された値を超えている場合、TCP 接続をリセットします。
ステップ 8	**end** 例： `Device(config-pmap)# end`	QoS ポリシーマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

URL フィルタ ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type urlfpolicy** {**local** | **n2h2** | **websense**} *parameter-map-name*
4. **exit**
5. **class-map type urlfilter** {*class-map-name* | **match-any** *class-map-name* | **n2h2** {*class-map-name* | **match-any** *class-map-name*} | **websense** {*class-map-name* | **match-any** *class-map-name*}}
6. **exit**
7. **policy-map type inspect urlfilter** *policy-map-name*
8. **service-policy urlfilter** *policy-map-name*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type urlfpolicy** {**local** | **n2h2** | **websense**} *parameter-map-name* 例： `Device(config)# parameter-map type urlfpolicy websense websense-param-map`	パラメータ マップ（これにはローカル、Websense、または N2H2 のパラメータを含めることができます）に関連付ける URL フィルタ名を設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**class-map type urlfilter** {*class-map-name* | **match-any** *class-map-name* | **n2h2** {*class-map-name* | **match-any** *class-map-name*} | **websense** {*class-map-name* | **match-any** *class-map-name*}} 例： `Device(config)# class-map type urlfilter websense websense-param-map`	URL フィルタのクラス マップを設定し、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**policy-map type inspect urlfilter** *policy-map-name* 例： `Device(config)# policy-map type inspect urlfilter websense-policy`	URL フィルタ ポリシーを設定し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 8	**service-policy urlfilter** *policy-map-name* 例： `Device(config-pmap)# service-policy urlfilter websense-policy`	検査クラスの URL フィルタ ポリシーをサービス ポリシーとして適用します。
ステップ 9	**end** 例： `Device(config-pmap)# end`	QoS ポリシーマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

IMAP ファイアウォール ポリシーの設定

IMAP クラス マップの設定

Integrated Messaging Access Protocol（IMAP）クラス マップを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**reset**] [**secure-login**] [**timeout** *seconds*]
4. **class-map type inspect imap** [**match-any**] *class-map-name*
5. **log**
6. **match invalid-command**
7. **match login clear-text**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip inspect name** *inspection-name protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**reset**] [**secure-login**] [**timeout** *seconds*] 例： `Device(config)# ip inspect name mail-guard imap`	検査ルール セットを定義します。

	コマンドまたはアクション	目的
ステップ 4	**class-map type inspect imap** [**match-any**] *class-map-name* 例： `Device(config)# class-map type inspect imap imap-class`	一致基準を入力するために IMAP のクラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 5	**log** 例： `Device(config-cmap)# log`	ログ メッセージが生成されます。
ステップ 6	**match invalid-command** 例： `Device(config-cmap)# match invalid-command`	（任意）IMAP 接続上の無効なコマンドを特定します。
ステップ 7	**match login clear-text** 例： `Device(config-cmap)# match login clear-text`	（任意）IMAP サーバが使用されるときにセキュアでないログインを特定します。
ステップ 8	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC コンフィギュレーション モードを開始します。

IMAP ポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect imap** *policy-map-name*
4. **class-type inspect imap** *imap-class-name*
5. **log**
6. **reset**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect imap** *policy-map-name* 例： `Device(config)# policy-map type inspect imap myimap-policy`	レイヤ 3 の Integrated Messaging Access Protocol（IMAP）ポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class-type inspect imap** *imap-class-name* 例： `Device(config-pmap)# class-type inspect imap pimap`	IMAP プロトコルのクラス マップを作成します。
ステップ 5	**log** 例： `Device(config-pmap)# log`	ログ メッセージが生成されます。
ステップ 6	**reset** 例： `Device(config-pmap)# reset`	（任意）シンプル メール転送プロトコル（SMTP）本体のデータ長が **class-map type inspect smtp** コマンドで設定された値を超えている場合、TCP 接続をリセットします。
ステップ 7	**end** 例： `Device(config-pmap)# end`	QoS ポリシーマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

インスタント メッセンジャ ポリシーの設定

IM クラス マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class map type inspect** {**aol** | **msnmsgr** | **ymsgr** | **icg** | **winmsgr**} [**match-any**] *class-map-name*
4. **match service** {**any** | **text-chat**}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class map type inspect** {**aol** | **msnmsgr** | **ymsgr** | **icg** | **winmsgr**} [**match-any**] *class-map-name* 例： `Device(config)# class map type inspect aol myaolclassmap`	一致基準を追加するためにインスタント メッセンジャ（IM）タイプのクラス マップを作成し、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match service** {**any** | **text-chat**} 例： `Device(config-cmap)# match service text-chat`	（任意）テキスト チャット メッセージに基づいて一致条件を作成します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

IM ポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy map type inspect** *protocol-name policy-map-name*
4. **class type inspect** {**aol** | **msnmsgr** | **ymsgr** | **icq** | **winmsgr**} *class-map-name*
5. **reset**
6. **log**
7. **allow**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy map type inspect** *protocol-name policy-map-name* 例： `Device(config)# policy map type inspect aol myaolpolicymap`	インスタントメッセンジャ（IM）ポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class type inspect** {**aol** | **msnmsgr** | **ymsgr** | **icq** | **winmsgr**} *class-map-name* 例： `Device(config-pmap)# class type inspect aol myaolclassmap`	アクションを実行する対象のトラフィック クラスを指定します。 • *class-map-name*：このクラスマップ名は、**class-map type inspect** コマンドを使用して指定したクラスマップと一致する必要があります。
ステップ 5	**reset** 例： `Device(config-pmap)# reset`	（任意）接続をリセットします。

	コマンドまたはアクション	目的
ステップ 6	**log** 例： `Device(config-pmap)# log`	（任意）パラメータの一致に関するログ メッセージを生成します。
ステップ 7	**allow** 例： `Device(config-pmap)# allow`	（任意）接続を許可します。
ステップ 8	**end** 例： `Device(config-pmap)# end`	QoS ポリシーマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

次の作業

まだ実行していない場合は、「レイヤ 7 プロトコル固有パラメータ マップの設定」に従って IM 固有のパラメータ マップを設定する必要があります。

ピアツーピア ポリシーの設定

ピアツーピア（P2P）ポリシーは、eDonkey、FastTrack、Gnutella、Kazaa バージョン 2 の各 P2P アプリケーションのために作成できます。

P2P クラス マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class map type inspect** {**edonkey** | **fasttrack** | **gnutella** | **kazaa2**} [**match-any**] *class-map-name*
4. **match file-transfer** [*regular-expression*]
5. **match search-file-name** [*regular-expression*]
6. **match text-chat** [*regular-expression*]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class map type inspect** {**edonkey** | **fasttrack** | **gnutella** | **kazaa2**} [**match-any**] *class-map-name* 例： `Device(config)# class map type inspect edonkey myclassmap`	一致基準を追加するためにピアツーピア（P2P）タイプのクラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match file-transfer** [*regular-expression*] 例： `Device(config-cmap)# match file-transfer *`	（任意）サポートされている任意の P2P プロトコル内のファイル転送接続に一致します。 （注） すべてのファイル転送接続がこのトラフィック クラスによって識別されるよう指定するには、正規表現として「*」を使用します。
ステップ 5	**match search-file-name** [*regular-expression*] 例： `Device(config-cmap)# match search-file-name`	（任意）eDonkey P2P アプリケーションを使用したクライアントの検索要求に含まれるファイル名をブロックします。 （注） このコマンドは、eDonkey P2P アプリケーションに対してのみ使用できます。
ステップ 6	**match text-chat** [*regular-expression*] 例： `Device(config-cmap)# match text-chat`	（任意）eDonkey P2P アプリケーションを使用したクライアント間のテキスト チャット メッセージをブロックします。 （注） このコマンドは、eDonkey P2P アプリケーションに対してのみ使用できます。
ステップ 7	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ピアツーピア ポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy map type inspect p2p** *policy-map-name*
4. **class type inspect** {**edonkey** | **fasttrack** | **gnutella** | **kazaa2**} *class-map-name*
5. **reset**
6. **log**
7. **allow**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy map type inspect p2p** *policy-map-name* 例： `Device(config)# policy map type inspect p2p mypolicymap`	ピアツーピア（P2P）ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class type inspect** {**edonkey**	**fasttrack**	**gnutella**	**kazaa2**} *class-map-name* 例： `Device(config-pmap)# class type inspect edonkey myclassmap`	アクションを実行する対象のトラフィック クラスを指定し、ポリシーマップ コンフィギュレーション モードを開始します。 • *class-map-name*：このクラス マップ名は、**class-map type inspect** コマンドで指定したクラス マップと一致する必要があります。
ステップ 5	**reset** 例： `Device(config-pmap)# reset`	（任意）接続をリセットします。

	コマンドまたはアクション	目的
ステップ 6	**log** 例： `Device(config-pmap)# log`	（任意）パラメータの一致に関するログ メッセージを生成します。
ステップ 7	**allow** 例： `Device(config-pmap)# allow`	（任意）接続を許可します。
ステップ 8	**end** 例： `Device(config-pmap)# end`	QoS ポリシーマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

POP3 ファイアウォール ポリシーの設定

POP3 ファイアウォール クラス マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-name protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**reset**] [**secure-login**] [**timeout** *seconds*]
4. **class-map type inspect pop3** [**match-any**] *class-map-name*
5. **match invalid-command**
6. **match login clear-text**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip inspect name** *inspection-name protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**reset**] [**secure-login**] [**timeout** *seconds*] 例： `Device(config)# ip inspect name mail-guard pop3`	検査ルール セットを定義します。
ステップ 4	**class-map type inspect pop3** [**match-any**] *class-map-name* 例： `Device(config)# class-map type inspect pop3 pop3-class`	一致基準を入力するために Post Office Protocol, Version 3（POP3）プロトコルのクラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 5	**match invalid-command** 例： `Device(config-cmap)# match invalid-command`	（任意）POP3 サーバ上の無効なコマンドを特定します。
ステップ 6	**match login clear-text** 例： `Device(config-cmap)# match login clear-text`	（任意）POP3 サーバを使用するときにセキュアでないログインを特定します。
ステップ 7	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

POP3 ファイアウォール ポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect pop3** *policy-map-name*
4. **class-type inspect pop3** *pop3-class-name*
5. **log**
6. **reset**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect pop3** *policy-map-name* 例： `Device(config)# policy-map type inspect pop3 mypop3-policy`	レイヤ 7 Post Office Protocol, Version 3（POP3）ポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class-type inspect pop3** *pop3-class-name* 例： `Device(config-pmap)# class-type inspect pop3 pcl`	POP3 プロトコルのクラス マップを作成します。
ステップ 5	**log** 例： `Device(config-pmap)# log`	ログ メッセージが生成されます。
ステップ 6	**reset** 例： `Device(config-pmap)# reset`	（任意）シンプル メール転送プロトコル（SMTP）本体のデータ長が **class-map type inspect smtp** コマンドで設定された値を超えている場合、TCP 接続をリセットします。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-pmap)# end`	QoS ポリシーマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

SMTP ファイアウォール ポリシーの設定

SMTP ファイアウォール クラス マップの設定

（注） クラス マップで拡張 SMTP（ESMTP）のインスペクションをイネーブルにするには、**match protocol smtp extended** コマンドを使用します。 このコマンドの使用の詳細については、「ゾーンベース ポリシー ファイアウォールの前提条件」の項を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect smtp** [**match-all** | **match-any**] *class-map-name*
4. **match data-length gt** *max-data-value*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**class-map type inspect smtp** [**match-all** | **match-any**] *class-map-name* 例： `Device(config)# class-map type inspect smtp smtp-class`	一致基準を入力するためにシンプル メール転送プロトコル（SMTP）プロトコルのクラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match data-length gt** *max-data-value* 例： `Device(config-cmap)# match data-length gt 200000`	SMTP 接続で転送されたデータ量が設定した制限を超えているかどうかを判断します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

SMTP ファイアウォール ポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect smtp** *policy-map-name*
4. **class-type inspect smtp** *smtp-class-name*
5. **reset**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**policy-map type inspect smtp** *policy-map-name* 例： `Device(config)# policy-map type inspect smtp mysymtp-policy`	レイヤ 7 のシンプル メール転送プロトコル（SMTP）ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class-type inspect smtp** *smtp-class-name* 例： `Device(config-pmap)# class-type inspect smtp sc`	SMTP プロトコルのインスペクション パラメータを設定します。
ステップ 5	**reset** 例： `Device(config-pmap)# reset`	（任意）SMTP 本体のデータ長が **class-map type inspect smtp** コマンドで設定された値を超えている場合、TCP 接続をリセットします。
ステップ 6	**end** 例： `Device(config-pmap)# end`	QoS ポリシーマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

SUNRPC ファイアウォール ポリシーの設定

（注） リモート プロシージャ コール（RPC）プロトコルを検査する場合（つまり、レイヤ 4 クラスマップで **match protocol sunrpc** コマンドを指定した場合）は、レイヤ 7 SUNRPC ポリシーマップが必要です。

SUNRPC ファイアウォール クラス マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect sunrpc** [**match-any**] *class-map-name*
4. **match program-number** *program-number*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect sunrpc** [**match-any**] *class-map-name* 例： `Device(config)# class-map type inspect sunrpc long-urls`	一致基準を入力するために SUNRPC プロトコルのクラスマップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match program-number** *program-number* 例： `Device(config-cmap)# match program-number 2345`	（任意）許可するリモート プロシージャ コール（RPC）プロトコル プログラム番号を一致基準として指定します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	QoS ポリシーマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

SUNRPC ファイアウォール ポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect sunrpc** *policy-map-name*
4. **class-type inspect sunrpc** *sunrpc-class-name*
5. **allow** [**wait-time** *minutes*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect sunrpc** *policy-map-name* 例： `Device(config)# policy-map type inspect sunrpc my-rpc-policy`	レイヤ 7 SUNRPC ポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class-type inspect sunrpc** *sunrpc-class-name* 例： `Device(config-pmap)# class-type inspect sunrpc cs1`	SUNRPC プロトコルのインスペクション パラメータを設定します。
ステップ 5	**allow** [**wait-time** *minutes*] 例： `Device(config-pmap)# allow wait-time 10`	（任意）設定したプログラム番号を許可します。 • 後続の同じ送信元アドレスからの接続と同じ宛先アドレスおよびポートへの接続を許可するためにファイアウォールに小さい穴を開けておく分数を指定します。デフォルトの待機時間は 0 分です。 このキーワードはリモート プロシージャ コール（RPC）プロトコルに対してのみ使用できます。
ステップ 6	**end** 例： `Device(config-pmap)# end`	QoS ポリシーマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

MSRPC ファイアウォール ポリシーの設定

（注） リモート プロシージャ コール（RPC）プロトコルを検査する場合（つまり、レイヤ 4 クラスマップで **match protocol msrpc** コマンドを指定した場合）は、レイヤ 7 Microsoft リモート プロシージャ コール（MSRPC）ポリシー マップが必要です。

MSRPC ファイアウォール ポリシーを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type protocol-info msrpc** *parameter-map-name*
4. **timeout** *seconds*
5. **exit**
6. **class-map type inspect match-any** *class-map-name*
7. **match protocol msrpc**
8. **match protocol msrpc-smb-netbios**
9. **exit**
10. **policy-map type inspect** *policy-map-name*
11. **class type inspect** *class-map-name*
12. **inspect**
13. **exit**
14. **class class-default**
15. **drop**
16. **exit**
17. **exit**
18. **zone security** *security-zone-name*
19. **exit**
20. **zone security** *security-zone-name*
21. **exit**
22. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
23. **service-policy type inspect** *policy-map-name*
24. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type protocol-info msrpc** *parameter-map-name* 例： `Device(config)# parameter-map type protocol-info msrpc para-map`	アプリケーション固有のパラメータ マップを定義し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**timeout** *seconds* 例： `Device(config-profile)# timeout 60`	MSRPCエンドポイントマッパー（EPM）のタイムアウトを設定します。
ステップ 5	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any c-map`	トラフィック クラスの検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 7	**match protocol msrpc** 例： `Device(config-cmap)# match protocol msrpc`	指定されたプロトコルに基づくクラス マップの一致基準を設定します。 • 検査タイプ クラスマップの一致基準には、Cisco ステートフル パケット インスペクションでサポートされているプロトコルのみを使用できます。
ステップ 8	**match protocol msrpc-smb-netbios** 例： `Device(config-cmap)# match protocol msrpc-smb-netbios`	指定されたプロトコルに基づくクラス マップの一致基準を設定します。 • 検査タイプ クラスマップの一致基準には、Cisco ステートフル パケット インスペクションでサポートされているプロトコルのみを使用できます。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p-map`	レイヤ 3 およびレイヤ 4 の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 11	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect c-map`	アクションを実行する対象のトラフィック（クラス）を指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 12	**inspect** 例： `Device(config-pmap-c)# inspect`	Cisco ステートフル パケット インスペクションをイネーブルにします。
ステップ 13	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 14	**class class-default** 例： `Device(config-pmap)# class class-default`	システム デフォルト クラスの照合を指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。 • システム デフォルト クラスを指定しない場合、未分類のパケットが照合されます。
ステップ 15	**drop** 例： `Device(config-pmap-c)# drop`	定義されたクラスに一致するパケットをドロップします。
ステップ 16	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 17	**exit** 例： `Device(config-pmap)# exit`	QoS ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 18	**zone security** *security-zone-name* 例： `Device(config)# zone security in-zone`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 19	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 20	**zone security** *security-zone-name* 例： `Device(config)# zone security out-zone`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 21	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 22	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security in-out source in-zone destination out-zone`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 23	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect p-map`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 24	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

セキュリティ ゾーンとゾーン ペアの作成、およびゾーン ペアへのポリシー マップの付加

ゾーン ペアを作成するには、2つのセキュリティ ゾーンが必要です。ただし、セキュリティ ゾーンを 1 つだけ作成し、「セルフ」と呼ばれるシステム定義のセキュリティ ゾーンを使用できます。セルフ ゾーンを選択する場合、検査ポリシングは設定できません。

このプロセスを使用して、次の作業を実行します。

- セキュリティ ゾーンにインターフェイスを割り当てます。
- ポリシー マップをゾーン ペアに付加します。
- セキュリティ ゾーンを少なくとも 1 つ作成します。
- ゾーン ペアを定義します。

ヒント　ゾーンを作成する前に、ゾーンの構成要素をよく検討する必要があります。 一般的なガイドラインは、セキュリティの観点から同様の性質をもつインターフェイスをグループにすることです。

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **description** *line-of-description*
5. **exit**
6. **zone-pair security** *zone-pair name* [**source** *source-zone-name* | **self**] **destination** [**self** | *destination-zone-name*]
7. **description** *line-of-description*
8. **exit**
9. **interface** *type number*
10. **zone-member security** *zone-name*
11. **exit**
12. **zone-pair security** *zone-pair-name* [**source** *source-zone-name* | **self**] **destination** [**self** | *destination-zone-name*]
13. **service-policy type inspect** *policy-map-name*
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *zone-name* 例： `Device(config)# zone security zone1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**description** *line-of-description* 例： `Device(config-sec-zone)# description Internet Traffic`	（任意）ゾーンの説明を入力します。
ステップ 5	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**zone-pair security** *zone-pair name* [**source** *source-zone-name* | **self**] **destination** [**self** | *destination-zone-name*] 例： `Device(config)# zone-pair security zp source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 7	**description** *line-of-description* 例： `Device(config-sec-zone-pair)# description accounting network`	（任意）ゾーン ペアの説明を入力します。
ステップ 8	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	**interface** *type number* 例： `Device(config)# interface ethernet 0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 （注） インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 11	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 12	**zone-pair security** *zone-pair-name* [**source** *source-zone-name* | **self**] **destination** [**self** | *destination-zone-name*] 例： `Device(config)# zone-pair security zp source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 13	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect p2`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 14	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

WAAS による Cisco ファイアウォールの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip wccp** *service-id*
4. **ip inspect waas enable**
5. **class-map type inspect** *class-name*
6. **match protocol** *protocol-name* [**signature**]
7. **exit**
8. **policy-map type inspect** *policy-map-name*
9. **class class-default**
10. **class-map type inspect** *class-name*
11. **inspect**
12. **exit**
13. **exit**
14. **zone security** *zone-name*
15. **description** *line-of-description*
16. **exit**
17. **zone-pair security** *zone-pair name* [**source** *source-zone-name* | **self**] **destination** [**self** | *destination-zone-name*]
18. **description** *line-of-description*
19. **exit**
20. **interface** *type number*
21. **description** *line-of-description*
22. **zone-member security** *zone-name*
23. **ip address** *ip-address*
24. **ip wccp** *service-id* {**group-listen** | **redirect** {**in** | **out**}} | **redirect exclude in** | **web-cache** {**group-listen** | **redirect** {**in** | **out**}}
25. **exit**
26. **zone-pair security** *zone-pair-name* {**source** *source-zone-name* | **self**} **destination** [**self** | *destination-zone-name*]
27. **service-policy type inspect** *policy-map-name*
28. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip wccp** *service-id* 例： `Device(config)# ip wccp 61`	Web Cache Communication Protocol（WCCP）の動的に定義されたサービス識別番号を入力します。
ステップ 4	**ip inspect waas enable** 例： `Device(config)# ip inspect waas enable`	Cisco Wide Area Application Services（WAAS）最適化を検出できるように、Cisco ファイアウォール インスペクションをイネーブルにします。 （注） サービス統合型ルータ（ISR）が Cisco ファイアウォールとともに WAAS 最適化パス内の中間デバイスとして展開されている場合は、**ip inspect waas enable** コマンドを使用して、WAAS 対応と相互運用性をイネーブルにする必要があります。 このデバイスが最適化を認識するよう設定されていない場合、最適化されたトラフィックは想定されている TCP アクティビティに違反し、ファイアウォールによってドロップされます。
ステップ 5	**class-map type inspect** *class-name* 例： `Device(config)# class-map type inspect most-traffic`	トラフィック クラスの検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。 （注） **class-map type inspect most-traffic** コマンドは非表示です。
ステップ 6	**match protocol** *protocol-name* [**signature**] 例： `Device(config-cmap)# match protocol http`	指定されたプロトコルに基づくクラス マップの一致基準を設定します。 • 検査タイプ クラスマップの一致基準には、Cisco ステートフル パケット インスペクションでサポートされているプロトコルのみを使用できます。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p1`	レイヤ 3 およびレイヤ 4 の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 9	**class class-default** 例： `Device(config-pmap)# class class-default`	システム デフォルト クラスの照合を指定します。 • システム デフォルト クラスを指定しない場合、未分類のパケットが照合されます。
ステップ 10	**class-map type inspect** *class-name* 例： `Device(config-pmap)# class-map type inspect most-traffic`	アクションを実行する対象のファイアウォール トラフィック（クラス）マップを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 11	**inspect** 例： `Device(config-pmap-c)# inspect`	Cisco ステートフル パケット インスペクションをイネーブルにします。
ステップ 12	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 13	**exit** 例： `Device(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 14	**zone security** *zone-name* 例： `Device(config)# zone security zone1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 15	**description** *line-of-description* 例： `Device(config-sec-zone)# description Internet Traffic`	（任意）ゾーンの説明を入力します。

	コマンドまたはアクション	目的
ステップ 16	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 17	**zone-pair security** *zone-pair name* [**source** *source-zone-name* | **self**] **destination** [**self** | *destination-zone-name*] 例： `Device(config)# zone-pair security zp source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 18	**description** *line-of-description* 例： `Device(config-sec-zone)# description accounting network`	（任意）ゾーン ペアの説明を入力します。
ステップ 19	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 20	**interface** *type number* 例： `Device(config)# interface ethernet 0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 21	**description** *line-of-description* 例： `Device(config-if)# description zone interface`	（任意）インターフェイスについて説明します。
ステップ 22	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 （注） インターフェイスをセキュリティゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。

	コマンドまたはアクション	目的
ステップ 23	**ip address** *ip-address* 例： `Device(config-if)# ip address 10.70.0.1 255.255.255.0`	セキュリティ ゾーンのインターフェイス IP アドレスを割り当てます。
ステップ 24	**ip wccp** *service-id* {**group-listen** | **redirect** {**in** | **out**}} | **redirect exclude in** | **web-cache** {**group-listen** | **redirect** {**in** | **out**}} 例： `Device(config-if)# ip wccp 61 redirect in`	インターフェイスでの WCCP パラメータを指定します。
ステップ 25	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 26	**zone-pair security** *zone-pair-name* {**source** *source-zone-name* | **self**} **destination** [**self** | *destination-zone-name*] 例： `Device(config)# zone-pair security zp source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 27	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect p2`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 28	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンベース ポリシー ファイアウォールの設定例

例：レイヤ 3 およびレイヤ 4 ファイアウォール ポリシーの設定

次の例は、レイヤ 3 またはレイヤ 4 トップレベル ポリシーを示します。 トラフィックはアクセス コントロール リスト（ACL）199 と照合され、ディープ パケット HTTP インスペクションが設定されています。 **match access-group** 101 を設定すると、レイヤ 4 インスペクションがイネーブルになります。 結果として、クラスマップのタイプが **match-all** である場合を除き、レイヤ 7 インスペクションは省略されます。

```
class-map type inspect match-all http-traffic
 match protocol http
 match access-group 101
policy-map type inspect mypolicy
 class type inspect http-traffic
  inspect
  service-policy http http-policy
```

例：レイヤ 7 プロトコル固有ファイアウォール ポリシーの設定

次の例は、URL の長さが 500 を超える HTTP セッションと一致させる方法を示します。 レイヤ 7 ポリシー アクション **reset** が設定されます。

```
class-map type inspect http long-urls
 match request uri length gt 500
policy-map type inspect http http-policy
 class type inspect http long-urls
  reset
```

次に、**extended** キーワードを指定して拡張 SMTP（ESMTP）のインスペクションをイネーブルにする例を示します。

```
class-map type inspect c1
 match protocol smtp extended
policy-map type inspect p1
 class type inspect c1
  inspect
```

service-policy type inspect smtp コマンドは任意であり、**inspect** コマンドの後に入力できます。

例：セキュリティ ゾーンとゾーン ペアの作成、およびゾーン ペアへのポリシー マップの付加

例：セキュリティ ゾーンの作成

次の例は、財務部門ネットワークと呼ばれるセキュリティ ゾーン z1、およびエンジニアリング サービス ネットワークと呼ばれるセキュリティ ゾーン z2 を作成する方法を示します。

```
zone security z1
 description finance department networks
```

```
!
zone security z2
 description engineering services network
```

例：ゾーン ペアの作成

次の例は、ゾーン z1 と z2 を作成し、両ゾーン間を流れるトラフィックについてゾーン z2 でファイアウォール ポリシー マップを適用するよう指定する方法を示します。

```
zone-pair security zp source z1 destination z2
service-policy type inspect p1
```

例：セキュリティ ゾーンへのインターフェイスの割り当て

次の例は、イーサネット インターフェイス 0 をゾーン z1 に、およびイーサネット インターフェイス 1 をゾーン z2 に付加する方法を示します。

```
interface ethernet0
 zone-member security z1
!
interface ethernet1
 zone-member security z2
```

例：Websense の URL フィルタ ポリシーの設定

例：Websense サーバの設定

```
parameter-map type urlfpolicy websense websense-param-map
 server fw21-ss1-bldr.example.com timeout 30
 source-interface Loopback0
 truncate script-parameters
 cache-size maximum-entries 100
 cache-entry-lifetime 1
 block-page redirect-url http://abc.example.com
```

例：Websense クラス マップの設定

```
class-map type urlfilter websense match-any websense-class
 match server-response any
```

例：Websense URL フィルタ ポリシーの設定

```
policy-map type inspect urlfilter websense-policy
 parameter type urlfpolicy websense websense-param-map
 class type urlfilter websense websense-class
  server-specified-action
  log
```

例：URL フィルタ ポリシーの設定

```
parameter-map type urlfpolicy websense-param-map
class-map type urlfilter websense websense-param-map
```

```
policy-map type inspect urlfilter websense-policy
service-policy urlfilter websense-policy
```

例：WAAS による Cisco ファイアウォールの設定

次に、Web Cache Communication Protocol（WCCP）を使用してトラフィックの代行受信のために Wide Area Application Engine（WAE）デバイスにトラフィックをリダイレクトする Cisco ファイアウォールのエンドツーエンド Wide Area Application Services（WAAS）トラフィック フロー最適化の設定例を示します。

次の設定例では、integrated-service-engine インターフェイスが異なるゾーンで設定され、各セキュリティ ゾーン メンバーにインターフェイスが割り当てられているため、セキュリティ ゾーン メンバー間でトラフィックがドロップされないようになっています。 ご使用のリリースによっては、異なる入力インターフェイスに対処するために Cisco ファイアウォール コンフィギュレーションに変更が加えられています。

```
ip wccp 61
ip wccp 62
ip inspect waas enable
class-map type inspect most-traffic
 match protocol icmp
 match protocol ftp
 match protocol tcp
 match protocol udp
!
policy-map type inspect p1
 class-type inspect most-traffic
  inspect
!
class class-default
zone security zone-hr
!
zone security zone-outside
!
zone security z-waas
!
zone-pair security hr-out source zone-hr destination zone-outside
 service-policy type inspect p1
!
zone-pair security out--hr source zone-outside destination zone-hr
 service-policy type inspect p1
!
zone-pair security eng--out source zone-eng destination zone-outside
service-policy type inspect p1
interface GigabitEthernet 0/0
 description Trusted interface
 ip address 10.70.0.1 255.255.255.0
 ip wccp 61 redirect in!
 zone-member security zone-hr
interface GigabitEthernet 0/0
 description Trusted interface
 ip address 10.71.0.2 255.255.255.0
 ip wccp 61 redirect in
 zone-member security zone-eng
!
interface GigabitEthernet 0/1
 description Untrusted interface
 ip address 10.72.2.3 255.255.255.0
 ip wccp 62 redirect in
 zone-member security zone-outside
```

（注） 新しいコンフィギュレーションでは、ご使用のリリースによって、統合サービス エンジンを独自のゾーンに配置し、いずれのゾーン ペアにも含まれる必要がないようにしています。zone-hr（zone-out）と zone-eng（zone-output）の間にゾーン ペアが設定されます。

```
interface Integrated-Service-Engine 1/0
 ip address 10.70.100.1 255.255.255.252
 ip wccp redirect exclude in
 zone-member security z-waas
```

例：クラス マップのプロトコル一致データが増加しない

次のコンフィギュレーション例では、**show policy-map type inspect zone-pair** コマンドの出力で一致カウンタの問題が発生します。

```
class-map type inspect match-any y
 match protocol tcp
 match protocol icmp
class-map type inspect match-all x
 match class y
```

ただし、クラスマップが任意のクラスマップに一致する場合、このコンフィギュレーションの累積カウンタは **show policy-map type inspect zone-pair** コマンドの出力に表示されます。

```
Device# show policy-map type inspect zone session

policy exists on zp zp
 Zone-pair: zp
  Service-policy inspect : fw
    Class-map: x (match-any)
      Match: class-map match-any y
        2 packets, 48 bytes   <======= Cumulative class map counters are incrementing.
        30 second rate 0 bps
        Match: protocol tcp
          0 packets, 0 bytes     <==== The match for the protocol is not incrementing.
          30 second rate 0 bps
        Match: protocol icmp
          0 packets, 0 bytes
          30 second rate 0 bps
   Inspect
      Number of Established Sessions = 1
      Established Sessions
        Session 53105C0 (10.1.1.2:19180)=>(172.16.1.2:23) telnet:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:02
          Bytes sent (initiator:responder) [30:69]
    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

SMTP のアプリケーション インスペクションと制御の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
ファイアウォール コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
ESMTP ファイアウォール情報。	『ESMTP Support for Cisco IOS Firewall』
SMTP ポリシーの設定の情報。	『Zone-Based Policy Firewall』

標準および RFC

標準/RFC	タイトル
RFC 821 とは別の、RFC 1869 およびその他の SMTP RFC 拡張	『*SMTP Service Extensions*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ゾーンベース ポリシー ファイアウォールの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *1*：ゾーンベース ポリシー ファイアウォールの機能情報

機能名	リリース	機能情報
HTTP のアプリケーション インスペクションと制御：フェーズ 2	12.4(9)T	HTTP のアプリケーション インスペクションと制御：フェーズ 2 機能は、現在のサポート機能を HTTP アプリケーション ファイアウォール ポリシーに対応するように拡張します。 次のコマンドが、この機能によって導入または変更されました。**regexmatch body regex**、**match header count**、**match header length**、**match header regex**、**match request length**、**match request**、**match response status-line regex**。

機能名	リリース	機能情報
電子メール インスペクション エンジン	15.1(1)S	電子メール インスペクション エンジン機能を使用すると、シスコ デバイスを通過する SSL VPN トンネル接続に含まれる POP3、IMAP、および E/SMTP 電子メール トラフィックを検査できます。
P2P アプリケーション インスペクションと制御：フェーズ 1	12.4(9)T 12.4(20)T	P2P アプリケーション インスペクションと制御：フェーズ 1 機能には、eDonkey、FastTrack、Gnutella バージョン 2、および Kazaa バージョン 2 のピアツーピア アプリケーションに対して設定されたポリシーを識別および施行するためのサポートが導入されています。 また、AOL、MSN Messenger、Yahoo Messenger の各インスタント メッセンジャ（IM）アプリケーションに対して設定されたポリシーを識別および施行するためのサポートも導入されます。 Release 12.4(20)T で、H.323、VoIP、および SIP アプリケーションのサポートが追加されました。 Release 12.4(20)T で、ICQ、Windows Messenger の各 IM アプリケーションのサポートも追加されました。 次のコマンドが、この機能によって導入または変更されました。**class-map type inspect**、**class type inspect**、**clear parameter-map type protocol-info**、**debug policy-firewall**、**match file-transfer**、**match protocol (zone)**、**match search-file-name**、**match service**、**match text-chat**、**parameter-map type**、**policy-map type inspect**、**server (parameter-map)**、**show parameter-map type protocol-info**。
検査トラフィックのレート制限	12.4(9)T	検査トラフィックのレート制限機能を使用すると、ユーザは Cisco ファイアウォール（検査）ポリシー内でトラフィックをレート制限できます。また、1 つのゾーン ペアに存在できるセッションの絶対数を制限することもできます。 次のコマンドが、この機能によって導入されました。**police (zone policy)**、**sessions maximum**。

機能名	リリース	機能情報
ゾーンベース ポリシー ファイアウォール	12.4(6)T	ゾーンベースポリシーファイアウォール機能は、ゾーンと呼ばれるインターフェイス グループ間の Cisco 単方向ファイアウォール ポリシーを提供します。 この機能により、次のコマンドが導入または変更されました。 **class-map type inspect**、**class type inspect**、**clear parameter-map type protocol-info**、**debug policy-firewall**、**match body regex**、**match file-transfer**、**match header count**、**match header length**、**match header regex**、**match protocol (zone)**、**match request length**、**match request regex**、**match response status-line regex**、**match search-file-name**、**match service**、**match text-chat**、**parameter-map type**、**policy-map type inspect**、**server (parameter-map)**、**service-policy (policy-map)**、**service-policy type inspect**、**show parameter-map type protocol-info**。
Microsoft リモート プロシージャ コール（MSRPC）のゾーンベース ファイアウォール サポート	15.1(4)M	MSRPC のゾーンベース ファイアウォール サポート機能により、MSRPC に対するゾーンベース ポリシー ファイアウォール サポートが追加されます。

機能名	リリース	機能情報
ゾーンベース ファイアウォール（ZBFW）操作性および管理性	15.0(1)M 15.1(1)T	このマニュアルで扱うゾーン ベース ファイアウォール操作性および管理性機能は、ゾーンベース ファイアウォールでの Out-of-Order（OoO）パケット処理のサポート、ゾーンベース ファイアウォールでのイントラゾーンのサポート、および拡張デバッグ機能です。 次のコマンドが、この機能によって導入または変更されました。**clear ip ips statistics**、**debug cce dp named-db inspect**、**debug policy-firewall**、**debug ip virtual-reassembly list**、**parameter-map type ooo global**、**show parameter-map type ooo global**、**zone-pair security**。 ご使用のリリースによっては、次のコマンドが導入または変更されました。**class-map type inspect**、**clear policy-firewall**、**log (parameter-map type)**、**match request regex**、**parameter-map type inspect**、**show parameter-map type inspect**、**show policy-firewall config**、**show policy-firewall mib**、**show policy-firewall sessions**、**show policy-firewall stats**、**show policy-firewall summary-log**。

第 2 章

ゾーンベース ポリシー ファイアウォール IPv6 サポート

ゾーンベース ポリシー ファイアウォールでは、IPv4 パケットの高度なトラフィック フィルタリングまたはインスペクションを提供します。 IPv6 サポートによって、ゾーンベース ポリシー ファイアウォールは、IPv6 パケットのインスペクションをサポートします。 IPv6 サポートの前は、ファイアウォールがサポートしているのは IPv4 パケット インスペクションだけでした。 レイヤ 4 プロトコル、インターネット制御メッセージ プロトコル（ICMP）、TCP、および UDP パケットだけが、IPv6 パケット インスペクションの対象となります。

このモジュールでは、サポートされるファイアウォール機能、および IPv6 パケット インスペクション用にファイアウォールを設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ゾーンベース ポリシー ファイアウォール IPv6 サポートの制約事項

次の機能はサポートされていません。

- アプリケーション レベル ゲートウェイ（ALG）
- ボックスツーボックス ハイ アベイラビリティ（HA）
- 分散型サービス拒否攻撃
- ファイアウォール リソース管理
- レイヤ 7 インスペクション
- マルチキャスト パケット
- 加入者単位のファイアウォールまたはブロードバンド ベースのファイアウォール
- ステートレス ネットワーク アドレス変換 64（NAT64）
- VRF-Aware Software インフラストラクチャ（VASI）
- Wide Area Application Services（WAAS）と Web Cache Communication Protocol（WCCP）

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートについて

ファイアウォール機能の IPv6 サポート

次の表で説明するファイアウォール機能は、IPv6 パケット インスペクションでサポートされます。

表 *2*：*IPv6* でサポートされるファイアウォール機能

機能	設定情報
クラス マップ	「ゾーンベース ポリシー ファイアウォール」モジュール。

機能	設定情報
インターネット制御メッセージ プロトコル バージョン 6（ICMPv6）、TCP、および UDP プロトコル	• 「*ICMP* のファイアウォール ステートフル インスペクション」モジュール。 • 「ゾーンベース ポリシー ファイアウォール」モジュール。
IP フラグメンテーション	「仮想フラグメンテーション再構成」モジュール。
シャーシ内 HA	—
エラー メッセージのロギング	「ゾーンベース ポリシー ファイアウォール」モジュール。
ネストされたクラス マップ	「ゾーンベース ポリシー ファイアウォールのネストされたクラス マップ サポート」モジュール。
Out-of-Order パケット処理	「ゾーンベース ポリシー ファイアウォール」モジュールの「Out-of-Order パケット処理」の項。
パラメータ マップ：検査タイプ パラメータ マップの場合、パラメータ マップで定義されたセッション数は、IPv4 と IPv6 セッションで累積されます	「ゾーンベース ポリシー ファイアウォール」モジュール。
ポリシー マップ	「ゾーンベース ポリシー ファイアウォール」モジュール。
ポートツーアプリケーション マッピング	—
ステートフル ネットワーク アドレス変換 64（NAT64）	『*IP Addressing: NAT Configuration Guide*』の「*Stateful Network Address Translation 64*」モジュール。
TCP SYN Cookie	「ファイアウォール *TCP SYN Cookie* の設定」モジュール。
VPN ルーティングおよび転送（VRF）認識ファイアウォール	「*VRF-Aware Cisco IOS XE* ファイアウォール」モジュール。
仮想フラグメンテーション再構成（VFR）	「仮想フラグメンテーション再構成」モジュール。
ゾーン、デフォルト ゾーン、およびゾーン ペア	「ゾーンベース ポリシー ファイアウォール」モジュール。

デュアル スタック ファイアウォール

デュアル スタック ファイアウォールは、IPv4 および IPv6 トラフィックを同時に実行するファイアウォールです。 デュアル スタック ファイアウォールは、次のシナリオで設定できます。

- IPv4 トラフィックを実行する 1 つのファイアウォール ゾーン、および IPv6 トラフィックを実行する別のファイアウォール ゾーン。
- IPv4 と IPv6 は、ステートフル ネットワーク アドレス変換 64（NAT64）を使用して展開している場合に共存します。 このシナリオでは、トラフィックは IPv6 から IPv4 へ、およびその逆に流れます。
- 同じゾーン ペアは、IPv4 および IPv6 トラフィックの両方を許可します。

IPv6 ヘッダー フィールドのファイアウォール アクション

IPv6 ヘッダー フィールドのファイアウォール アクションについては、（IPv6 ヘッダーで使用可能な順に）次の表で説明します。

表 *3*：*IPv6* ヘッダー フィールド

IPv6 ヘッダー フィールド	IPv6 ヘッダー フィールドの説明	ファイアウォール アクション
バージョン	IPv4 パケット ヘッダーのバージョン フィールドと同様ですが、IPv4 を意味する数字 4 の代わりに IPv6 を意味する数字 6 が示されます。	IPv6 である必要があります。
トラフィック クラス	IPv4 パケット ヘッダーのタイプ オブ サービス（ToS）フィールドと同様です。 トラフィック クラス フィールドは、差別化されたサービスで使用されるトラフィック クラスのタグをパケットに付けます。	検査されません。
フロー ラベル	IPv6 パケット ヘッダーの新しいフィールドです。 フロー ラベル フィールドは、ネットワーク層でパケットを差別化する特定のフローのタグをパケットに付けます。	検査されません。

IPv6 ヘッダー フィールド	IPv6 ヘッダー フィールドの説明	ファイアウォール アクション
ペイロード長	IPv4 パケット ヘッダーの合計長フィールドと同様です。 ペイロード長フィールドは、パケットのデータ部分の合計長を示します。	ファイアウォールはこのフィールドを限定的に使用して、ICMP、TCP などのレイヤ 4 プロトコルの一部の長さを計算します。
次ヘッダー長	IPv4 パケット ヘッダーのプロトコル フィールドと同様です。 次ヘッダー長フィールドの値により、基本 IPv6 ヘッダーに続く情報のタイプが決まります。 基本 IPv6 ヘッダーに続く情報のタイプは、TCP パケット、UDP パケット、または拡張ヘッダーなどのトランスポート層パケットです。	ファイアウォールは、セッションを作成するためにこのフィールドを認識する必要があります。
ホップ リミット	IPv4 パケット ヘッダーの存続可能時間（TTL）フィールドと同様です。 ホップ リミット フィールドの値は、IPv6 パケットが無効と見なされる前に通過できるデバイスの最大数です。 各デバイスでは、ホップ リミット値は 1 ずつ減少します。 IPv6 ヘッダーにはチェックサムがないため、デバイスはチェックサムを計算し直すことなく、値を減少できます。	検査されません。

IPv6 ファイアウォール セッション

トラフィックのステートフル インスペクションを実行するために、ファイアウォールは各トラフィック フローの内部セッションを作成します。 セッション情報には、IP 送信元アドレスと宛先アドレス、UDP または TCP の送信元ポートと宛先ポートまたは ICMP タイプ、レイヤ 4 プロトコル タイプ（ICMP、TCP、または UDP）、および VPN ルーティングおよび転送（VRF）ID が含まれます。 IPv6 ファイアウォールでは、送信元アドレスと宛先アドレスには IPv6 アドレスの 128 ビットが含まれます。

ファイアウォールは、パケットが設定済みのポリシーと一致した場合、最初のパケットの受信後に TCP セッションを作成します。 ファイアウォールは、TCP シーケンス番号を追跡し、TCP パケットのシーケンス番号が設定された範囲内にない場合、その TCP パケットをドロップします。セッションが削除されるのは、TCP アイドル タイマーが期限切れになった場合、またはリセット（RST）や終了確認応答（FIN-ACK）パケットを適切なシーケンス番号で受信した場合です。

ファイアウォールは、設定されたポリシーに一致する最初のUDPパケットが到着したときにUDPセッションを作成し、UDP アイドル タイマーが期限切れになった場合にセッションを削除します。 ファイアウォールは、マルチキャスト IPv6 アドレスまたは未知の IPv6 アドレスが含まれた IPv6 パケットの TCP または UDP セッションを作成しません。

フラグメント化されたパケットのファイアウォールインスペクション

ファイアウォールは、フラグメント化された IPv6 パケットのインスペクションをサポートします。 IP フラグメンテーションは、単一の IP データグラムを小さなサイズの複数のパケットに分割するプロセスです。 IPv6 では、エンド ノードはパス最大伝送単位（MTU）探索を実行して、送信されるパケットの最大サイズを判別し、MTUサイズよりも大きいパケットについて、フラグメント拡張ヘッダーが含まれる IPv6 パケットを生成します。

ファイアウォールは、仮想フラグメンテーション再構成（VFR）を使用して、フラグメント化されたパケットを検査します。 VFRは、シーケンス外のフラグメントのフラグメント拡張ヘッダーを調べ、インスペクションのためにそれらを正しい順序に配置します。 インターフェイスをゾーンに追加してインターフェイス上のファイアウォールをイネーブルにすると、VFRは同じインターフェイス上で自動的に設定されます。 明示的にVFRをディセーブルにした場合、ファイアウォールはレイヤ 4 ヘッダーを持つ最初のフラグメントだけを検査し、残りのフラグメントは検査なしで渡します。

フラグメント拡張ヘッダーは、次のヘッダー順で表示されます。

- IPv6 ヘッダー
- ホップバイホップ オプション ヘッダー
- 宛先オプション ヘッダー
- ルーティング ヘッダー
- フラグメント拡張ヘッダー

シスコ エクスプレス フォワーディングは、フラグメント拡張ヘッダーが含まれた IPv6 パケットを検査することで、ファイアウォールがパケットを処理する前にさらに検査する必要がないようにします。

ICMPv6 メッセージ

IPv6 は ICMPv6 を使用して、診断機能、エラー レポーティング、およびネイバー探索を実行します。 ICMPv6 メッセージは、情報およびエラー メッセージにグループ化されます。

ファイアウォールは、次の ICMPv6 メッセージのみを検査します。

- ECHO REQUEST
- ECHO REPLY
- DESTINATION UNREACHABLE
- PACKET TOO BIG

- PARAMETER PROBLEM
- TIME EXCEEDED

（注） ネイバー探索パケットが渡され、ファイアウォールによって検査されません。

ステートフル NAT64 のファイアウォール サポート

ゾーンベース ポリシー ファイアウォールは、ステートフル NAT64 をサポートします。 ステートフル NAT64 は、IPv6 パケットを IPv4 パケットに変換したり、その逆に変換したりします。 ファイアウォールおよびステートフル NAT64 の両方がルータで設定されている場合、そのファイアウォールはアクセス コントロール リスト（ACL）内の IP アドレスを使用して、パケットをフィルタリングします。 ただし、ACL は IPv4 アドレスと IPv6 アドレスの混在をサポートしません。ファイアウォールとステートフル NAT64 が連携して動作するには、IPv6 ACL を使用する必要があり、IPv4 アドレスは IPv6 ACL に組み込まれている必要があります。

（注） ステートフル NAT64 は VRF を認識しないため、VRF をファイアウォールおよびステートフル NAT64 設定とともに使用することはできません。

ファイアウォール クラス マップが ACL を使用する場合、ACL はホスト上で実際の IP アドレスを使用して、パケットフローを設定する必要があります。 送信元または宛先アドレスだけが必要な場合は、IPv4 アドレスまたは IPv6 アドレスがクラス マップ ACL で使用されます。 パケット フローが送信元アドレスと宛先アドレスの両方に基づいてフィルタリングできるようにするには、IPv6 アドレスが使用され、IPv4 アドレスが ACL に組み込まれている必要があります。 ACL は、IPv6 アドレスを使用して、ステートフル NAT64 パケットをフィルタリングする必要があります。

（注） ファイアウォールでのステートレス NAT64 はサポートされません。

ポートツーアプリケーション マッピング

ポートツーアプリケーション マッピング（PAM）を使用して、ネットワーク サービスやアプリケーション用の TCP または UDP ポート番号をカスタマイズできます。 ファイアウォールは PAM を使用して、TCP または UDP ポート番号を特定のネットワーク サービスやアプリケーションに関連付けます。 ポート番号をネットワーク サービスやアプリケーションにマッピングすることで、管理者は既知のポートを使用して定義されていないカスタム設定に対してファイアウォール インスペクションを強制適用できます。 **ip port-map** コマンドを使用して、PAM を設定します。

ハイ アベイラビリティおよび ISSU

IPv6 ファイアウォールはボックス内 HA をサポートします。 ファイアウォール セッションは、スイッチオーバーのためにスタンバイ組み込みサービス プロセッサ（ESP）に同期されます。 IPv6 ファイアウォールでは In Service Software Upgrade（ISSU）もサポートされます。

トラフィック クラスの pass アクション

ファイアウォールでは、トラフィック クラスはパケットの内容に基づいてパケットセットを識別します。 クラスを定義し、ポリシーを反映するアクションを識別されたトラフィックに適用できます。 アクションとは、トラフィック クラスに関連付けられる、特定の機能のことです。 クラスの inspect アクション、drop アクション、および pass アクションを設定できます。

pass アクションは、あるゾーンから別のゾーンにトラフィックを渡します。 pass アクションが設定されている場合、ファイアウォールはトラフィックを検査しません。つまり、トラフィックを渡します。IPv6 ファイアウォールでは、ゾーンペアおよび pass アクションに関するポリシーマップを定義して、リターン トラフィックの pass アクションを明示的に設定する必要があります。

次に、ポリシー マップの pass アクション、外部から内部へのポリシーと内部から外部へのポリシーを IPv6 トラフィックに設定する例を示します。

```
policy-map type inspect outside-to-inside-policy
 class type inspect ipv6-class
  pass (Defines pass action for the ipv6-class from the outside to the inside)
!
 class class-default
!
policy-map type inspect inside-to-outside-policy
 class type inspect ipv4-class
  inspect (Defines inspect action for ipv4-class)
 class type inspect v6_class
  pass (Defines pass action for ipv6-class from the inside to the outside)
 class class-default
!
!
zone security inside
!
zone security outside
!
zone-pair security in-out source inside destination outside
 service-policy type inspect inside-to-outside-policy
!
zone-pair security out-in source outside destination inside
 service-policy type inspect outside-to-inside-policy
```

ゾーンベース ポリシー ファイアウォール IPv6 サポートの設定方法

IPv6 ファイアウォールの設定

IPv4 ファイアウォールと IPv6 ファイアウォールを設定する手順は同じです。 IPv6 ファイアウォールを設定するには、IPv6 アドレスファミリだけが一致するようにクラスマップを設定する必要があります。

match protocol コマンドは、IPv4 トラフィックと IPv6 トラフィックの両方に適用され、IPv4 ポリシーまたは IPv6 ポリシーに含めることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf-definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **sessions maximum** *sessions*
9. **exit**
10. **ipv6 unicast-routing**
11. **ip port-map** *appl-name* **port** *port-num* **list** *list-name*
12. **ipv6 access-list** *access-list-name*
13. **permit ipv6 any any**
14. **exit**
15. **class-map type inspect match-all** *class-map-name*
16. **match access-group name** *access-group-name*
17. **match protocol** *protocol-name*
18. **exit**
19. **policy-map type inspect** *policy-map-name*
20. **class type inspect** *class-map-name*
21. **inspect** [*parameter-map-name*]
22. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vrf-definition** *vrf-name* 例： `Device(config)# vrf-definition VRF1`	仮想ルーティングおよび転送（VRF）ルーティング テーブル インスタンスを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、標準IPv6アドレスプレフィックスを伝送するセッションを設定します。
ステップ 5	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect ipv6-param-map`	ファイアウォールのグローバル検査タイプ パラメータ マップを、検査アクションに関連するしきい値、タイムアウト、およびその他のパラメータに関連付けることができるようにし、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**sessions maximum** *sessions* 例： `Device(config-profile)# sessions maximum 10000`	ゾーン ペア上に存在可能な最大許容セッション数を設定します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 11	**ip port-map** *appl-name* **port** *port-num* **list** *list-name* 例： `Device(config)# ip port-map ftp port 8090 list ipv6-acl`	IPv6 アクセス コントロール リスト（ACL）を使用してポートツーアプリケーション マッピング（PAM）を確立します。
ステップ 12	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list ipv6-acl`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 13	**permit ipv6 any any** 例： `Device(config-ipv6-acl)# permit ipv6 any any`	IPv6 アクセス リストに許可条件を設定します。
ステップ 14	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**class-map type inspect match-all** *class-map-name* 例： `Device(config)# class-map type inspect match-all ipv6-class`	アプリケーション固有検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 16	**match access-group name** *access-group-name* 例： `Device(config-cmap)# match access-group name ipv6-acl`	指定した ACL をベースにクラスマップに対して一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 17	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルに基づくクラス マップの一致基準を設定します。
ステップ 18	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 19	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ipv6-policy`	プロトコル固有検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 20	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ipv6-class`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 21	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect ipv6-param-map`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 22	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンの設定およびインターフェイスへのゾーンの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ipv6 address** *ipv6-address*/*prefix-length*
12. **encapsulation dot1q** *vlan-id*
13. **zone-member security** *zone-name*
14. **end**
15. **show policy-map type inspect zone-pair sessions**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *zone-name* 例： `Device(config)# zone security z1`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**zone security** *zone-name* 例： `Device(config)# zone security z2`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*] 例： `Device(config)# zone-pair security in-2-out source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy`	ポリシー マップをトップレベル ポリシー マップに付加します。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードを開始します。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0.1`	サブインターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ipv6 address** *ipv6-address*/*prefix-length* 例： `Device(config-subif)# ipv6 address 2001:DB8:2222:7272::72/64`	IPv6の一般的なプレフィックスに基づいてIPv6アドレスを設定し、インターフェイスまたはサブインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 12	**encapsulation dot1q** *vlan-id* 例： `Device(config-subif)# encapsulation dot1q 2`	インターフェイスで使用するカプセル化方式を設定します。

	コマンドまたはアクション	目的
ステップ 13	**zone-member security** *zone-name* 例： `Device(config-subif)# zone member security z1`	ゾーン メンバーとしてインターフェイスを設定します。 • *zone-name* 引数では、**zone security** コマンドを使用して設定したゾーンのいずれかを設定する必要があります。 • インターフェイスがセキュリティ ゾーンにある場合、そのインターフェイスを通るトラフィックはどちらの方向でもすべて（デバイス宛またはデバイス発信のトラフィックを除く）デフォルトでドロップされます。 ゾーン メンバーであるインターフェイスをトラフィックが通過することを許可するには、そのゾーンをゾーン ペアの一部にして、そのゾーンペアにポリシーを適用する必要があります。 ポリシーで、inspect または pass アクションを通してトラフィックが許可されると、トラフィックはインターフェイスを通過します。
ステップ 14	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 15	**show policy-map type inspect zone-pair sessions** 例： `Device# show policy-map type inspect zone-pair sessions`	ポリシー マップが指定したゾーン ペアに適用されているため、作成されたステートフル パケット インスペクション セッションを表示します。 • このコマンドの出力は、IPv4 と IPv6 の両方のファイアウォール セッションを表示します。

例

show policy-map type inspect zone-pair sessions コマンドからの次のサンプル出力には、IPv6 アドレスと IPv4 アドレスの双方向のパケット変換が表示されます。

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:32847=>(209.165.201.2:21) ftp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [37:84]

        Half-open Sessions
```

```
        Session 110D930C [2001:DB8:1::104]:32848=>(209.165.201.2:21) ftp SIS_OPENING
         Created 00:00:00, Last heard 00:00:00
         Bytes sent (initiator:responder) [0:0]
```

show policy-map type inspect zone-pair sessions コマンドからの次のサンプル出力には、IPv6 アドレスから IPv6 アドレスへのパケットの変換が表示されます。

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:63=>[2001:DB8:2::102]:63 udp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [162:0]
```

IPv6 ファイアウォールおよびステートフル NAT64 ポート アドレス変換の設定

次の作業では、ステートフル NAT64 のダイナミック ポート アドレス変換（PAT）を使用した IPv6 ファイアウォールを設定します。

PAT 設定では、複数の IPv6 ホストを、使用可能な IPv4 アドレス プールに先着順でマッピングします。 ダイナミック PAT 設定は、IPv4 インターネットへの接続を提供しながら、不足している IPv4 アドレス空間の節約に直接役立ちます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **no ip address**
6. **zone-member security** *zone-name*
7. **negotiation auto**
8. **ipv6 address** *ipv6-address*/*prefix-length*
9. **ipv6 enable**
10. **nat64 enable**
11. **exit**
12. **interface** *type number*
13. **ip address** *ip-address mask*
14. **zone member security** *zone-name*
15. **negotiation auto**
16. **nat64 enable**
17. **exit**
18. **ipv6 access-list** *access-list-name*
19. **permit ipv6 host** *source-ipv6-address* **host** *destination-ipv6-address*
20. **exit**
21. **ipv6 route** *ipv6-prefix*/*length interface-type interface-number*
22. **ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address*
23. **nat64 v4 pool** *pool-name start-ip-address end-ip-address*
24. **nat64 v6v4 list** *access-list-name* **pool** *pool-name* **overload**
25. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**no ip address** 例： `Device(config-if)# no ip address`	IP アドレスを削除するか、IP 処理をディセーブルにします。
ステップ 6	**zone-member security** *zone-name* 例： `Device(config-if)# zone member security z1`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 7	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 8	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:1::2/96`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 9	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 10	**nat64 enable** 例： `Device(config-if)# nat64 enable`	インターフェイスで NAT64 をイネーブルにします。
ステップ 11	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 12	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 13	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 209.165.201.25 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 14	**zone member security** *zone-name* 例： `Device(config-if)# zone member security z2`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 15	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 16	**nat64 enable** 例： `Device(config-if)# nat64 enable`	インターフェイスで NAT64 をイネーブルにします。
ステップ 17	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 18	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list ipv6-ipv4-pair`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 19	**permit ipv6 host** *source-ipv6-address* **host** *destination-ipv6-address* 例： `Device(config-ipv6-acl)# permit ipv6 host 2001:DB8:1::2 host 209.165:201.25`	IPv6 アクセス リスト、送信元 IPv6 ホスト アドレス、および宛先 IPv6 ホスト アドレスの許可条件を設定します。
ステップ 20	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 21	**ipv6 route** *ipv6-prefix/length interface-type interface-number* 例： `Device(config)# ipv6 route 2001:DB8:1::2/96 gigabitethernet 0/0/0`	スタティック IPv6 ルートを確立します。
ステップ 22	**ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address* 例： `Device(config)# ipv6 neighbor 2001:DB8:1::2/96 gigabitethernet 0/0/0 0000.29f1.4841`	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。
ステップ 23	**nat64 v4 pool** *pool-name start-ip-address end-ip-address* 例： `Device(config)# nat64 v4 pool pool1 209.165.201.25 209.165.201.125`	ステートフル NAT64 IPv4 アドレス プールを定義します。
ステップ 24	**nat64 v6v4 list** *access-list-name* **pool** *pool-name* **overload** 例： `Device(config)# nat64 v6v4 list nat64-ipv6-any pool pool1 overload`	NAT64 PAT または過負荷アドレス変換をイネーブルにします。
ステップ 25	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンベース ポリシー ファイアウォール IPv6 サポートの設定例

例：IPv6 ファイアウォールの設定

```
Device# configure terminal
Device(config)# vrf-definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
```

```
Device(config-vrf)# exit
Device(config)# parameter-map type inspect ipv6-param-map
Device(config-profile)# sessions maximum 10000
Device(config-profile)# exit
Device(config)# ipv6 unicast-routing
Device(config)# ip port-map ftp port 8090 list ipv6-acl
Device(config)# ipv6 access-list ipv6-acl
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# class-map type inspect match-all ipv6-class
Device(config-cmap)# match access-group name ipv6-acl
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect ipv6-policy
Device(config-pmap)# class type inspect ipv6-class
Device(config-pmap-c)# inspect ipv6-param-map
Device(config-pmap-c)# end
```

例：ゾーンの設定およびインターフェイスへのゾーンの適用

```
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security in-to-out source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0.1
Device(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
Device(config-if)# encapsulation dot1q 2
Device(config-if)# zone member security z1
Device(config-if)# end
```

例：IPv6 ファイアウォールおよびステートフル NAT64 ポートアドレス変換の設定

```
configure terminal
 ipv6 unicast-routing
 interface gigabitethernet 0/0/0
  no ip address
  zone member security z1
  negotiation auto
  ipv6 address 2001:DB8:1::2/96
  ipv6 enable
  nat64 enable
!
 interface gigabitethernet 0/0/1
  ip address 209.165.201.25 255.255.255.0
  zone member security z2
  negotiation auto
  nat64 enable
!
 ipv6 access-list ipv6-ipv4-pair
  permit ipv6 host 2001:DB8:1::2 host 209.165:201.25
!
 ipv6 route 2001:DB8:1::2/96 gigabitethernet 0/0/0
 ipv6 neighbor 2001:DB8:1::2/96 gigabitethernet 0/0/0 0000.29f1.4841
 nat64 v4 pool pool1 209.165.201.25 209.165.201.125
 nat64 v6v4 list nat64-ipv6-any pool pool1 overload
```

ゾーンベース ポリシー ファイアウォール IPv6 サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Commands List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
ステートフル NAT64	『Stateful Network Address Translation 64』

標準および RFC

標準/RFC	タイトル
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2473	『*Generic Packet Tunneling in IPv6 Specification*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ゾーンベース ポリシー ファイアウォール IPv6 サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *4*：ゾーンベース ポリシー ファイアウォール *IPv6* サポートの機能情報

機能名	リリース	機能情報
ゾーンベース ポリシー ファイアウォール IPv6 サポート	Cisco IOS XE Release 3.6S	ゾーンベース ポリシー ファイアウォール サポートは、IPv6 パケットのインスペクションをサポートします。 次のコマンドが導入または変更されました。**ip port-map** および **show policy-map type inspect zone-pair**。

第 3 章

VRF-Aware Cisco IOS XE ファイアウォール

VRF-Aware Cisco IOS XE ファイアウォールは、ファイアウォールがサービス プロバイダー（SP）または大企業のエッジ ルータに設定されている場合、VPN ルーティングおよび転送（VRF）インターフェイスに Cisco IOS XE ファイアウォール機能を適用します。 SP は中小企業の市場向けにマネージド サービスを提供します。

VRF-Aware Cisco IOS XE ファイアウォールは、VRF-lite（Multi-VRF CE とも呼ばれる）および各種プロトコルでのアプリケーション インスペクションと制御（AIC）をサポートします。

VRF 認識ファイアウォールは、VRF-lite（Multi-VRF CE とも呼ばれる）および各種プロトコルでのアプリケーション インスペクションと制御（AIC）をサポートします。

（注） Cisco IOS XE リリースは、コンテキストベース アクセス コントロール（CBAC）ファイアウォールをサポートしません。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

VRF-Aware Cisco IOS XE ファイアウォールの前提条件

- Cisco IOS XE ファイアウォールについて理解します。
- VRF を設定します。

VRF-Aware Cisco IOS XE ファイアウォールの制約事項

- 2 つの VPN ネットワークに重複するアドレスがある場合、VRF 認識ファイアウォールをサポートするには、VRF 対応ネットワーク アドレス変換（NAT）が必要です。 NAT は、Inter-VRF ルーティングをサポートしません。 VRF-Aware Software インフラストラクチャ（VASI）を Inter-VRF ルーティング機能に使用できます。
- クリプト トンネルが、単一のインターフェイスで終端する複数の VPN に属する場合、VRF 別のファイアウォール ポリシーを適用できません。
- 同じゾーンを、異なる VRF に設定されたインターフェイスに適用することはできません。

VRF-Aware Cisco IOS XE ファイアウォールについて

VRF-Aware Cisco IOS XE ファイアウォール

VRF 認識ファイアウォールは、VRF で送信または受信された IP パケットを検査します。 VRF により、ルーティング テーブルの複数のインスタンスが単一ルータ内に共存できます。 これにより、VPN 分離が可能になり、独立した重複 IP アドレス空間を持つことができます。 VRF により、あるサービス プロバイダーの顧客からのトラフィックを別のトラフィックから隔離できます。 Cisco IOS XE VRF サポートは、ルータを複数のルーティング ドメインに分割し、各ルーティング ドメインは、インターフェイスおよびルーティング/転送テーブルの独自のセットで構成されま

す。 各ルーティング ドメインは、テーブル ID と呼ばれる固有識別子で参照されます。 グローバルルーティング ドメインおよび（いずれの VRF にも関連付けられていない）デフォルト ルーティング ドメインは、テーブル ID、ゼロにアドレス指定されます。 VRF は、重複する IP アドレス空間をサポートするため、交差しない VRF のトラフィックが同じ IP アドレスを持つことができます。

VRF-Aware Cisco IOS XE ファイアウォールには、次の利点があります。

- スケーラブルな展開：あらゆるネットワークの帯域幅およびパフォーマンスの要件に合わせて調整できます。
- VPN のサポート：Cisco IOS XE IPsec や他のソフトウェアベースのテクノロジー（レイヤ 2 トンネリング プロトコル（L2TP）トンネリングや Quality of Service（QoS）など）に基づいて、統合的な VPN ソリューションを提供します。
- AIC サポート：Internet Message Access Protocol（IMAP）、Post Office Protocol 3（POP3）、シンプル メール転送プロトコル（SMTP）、および Sun リモート プロシージャ コール（SUN RPC）のポリシー マップを提供します。
- ユーザは VRF ファイアウォールごとに設定できます。 ファイアウォールは、VRF 内で送受信した IP パケットを検査します。 ファイアウォールは、2 つの異なる VRF（交差する VRF）間のトラフィックも検査します。
- SP は、プロバイダー エッジ（PE）ルータにファイアウォールを展開できます。
- 重複する IP アドレス空間をサポートするため、交差しない VRF のトラフィックが同じ IP アドレスを持つことができます。
- （グローバルではない）VRF のファイアウォール コマンド パラメータおよびサービス拒否（DoS）パラメータをサポートして、VRF 認識ファイアウォールが多様な VPN カスタマーに割り当てられた（VRF インスタンスを含む）複数インスタンスとして実行できるようにします。
- VRF ID を含む高速ロギング（HSL）を生成します。ただし、これらのメッセージは単一のコレクタによって収集されます。

VRF 認識ファイアウォールにより、ファイアウォール セッション数を制限できます。 ファイアウォール セッションが制限されていない場合、VRF はルータ リソースを共有することが困難になります。これは、1 つの VRF がリソースの最大量を消費し、他の VRF にリソースがほとんど残らず、このため他の VRF に対するサービス拒否が発生する可能性があるためです。

アドレス空間の重複

VRF は、デバイスを複数のルーティング ドメインに分割します。 これらの各ルーティング ドメインには、インターフェイスとルーティング テーブルの独自のセットが含まれます。 ルーティング テーブルは、VRF ごとに一意のテーブル ID を使用して参照されます。 ゼロは、VPN ルーティングおよび転送（VRF）に関連付けられていないデフォルトのグローバル ルーティング テーブル ID です。

交差しない VRF は、重複するアドレス空間を持つことができます（つまり、ある VRF の IP アドレスが他の VRF に含まれている場合があります）。

VRF

VPN ルーティングおよび転送（VRF）により、ルーティング テーブルの複数のインスタンスが単一デバイス内に共存できます。 VRF には、プロバイダー エッジ（PE）デバイス内の VRF テーブルのテンプレートが含まれます。

通常、アドレスの重複は、カスタマーネットワークでプライベート IP アドレスを使用していることから発生します。アドレスの重複は、ピアツーピア（P2P）VPN の実装を展開するうえで主要な障害物の 1 つです。 マルチ プロトコル ラベル スイッチング（MPLS）VPN テクノロジーを使用して、重複するアドレスの問題を解決できます。

各 VPN は、デバイスに独自のルーティング/転送テーブルがあるため、VPN に属するすべてのカスタマーまたはサイトには、そのテーブルに含まれるルート セットに対してのみアクセス権があります。 そのため、MPLS VPN ネットワークの PE デバイスには、多数の VPN 別のルーティング テーブルと、サービス プロバイダー（SP）ネットワーク内の他のデバイスに到達するために使用される 1 つのグローバル ルーティング テーブルが含まれます。 事実上、数多くの仮想デバイスが単一の物理デバイスに作成されます。

VRF-Lite

MPLS 対応ファイアウォールなしの VRF とも呼ばれる VRF-Lite Aware ファイアウォール機能により、ファイアウォール ゾーンを MPLS 非対応の VPN ルーティングおよび転送（VRF）インターフェイスに適用できます。

VRF-Lite Aware ファイアウォール機能により、サービス プロバイダー（SP）は 2 つ以上の VPN をサポートでき、VPN 間での IP アドレスの重複が可能になります。 VRF-lite では、1 つまたは複数のレイヤ 3 インターフェイスを各 VRF に関連付けることで、入力インターフェイスを使用して異なる VPN のルートを区別し、仮想パケット転送テーブルを構成します。 VRF には、イーサネット ポートなどの物理インターフェイス、または VLAN スイッチ仮想インターフェイス（SVI）などの論理インターフェイスを使用できます。 ただし、1 つのレイヤ 3 インターフェイスは同時に複数の VRF に所属できません。

（注） すべての VRF-lite インターフェイスはレイヤ 3 インターフェイスにする必要があります。

VRF-lite には、次のデバイスが含まれています。

- カスタマー エッジ（CE）デバイスは、データ リンク上の SP ネットワークへのアクセスをカスタマーに提供します。 CE デバイスは、サイトのローカル ルートをプロバイダー エッジ（PE）デバイスにアドバタイズし、PE デバイスからリモート VPN ルートについて学習します。

- PE デバイスは、スタティック ルーティングまたはルーティング プロトコル（ボーダー ゲートウェイ プロトコル（BGP）、ルーティング情報プロトコル バージョン 1（RIPv1）や RIPv2 など）を使用して、ルーティング情報を CE デバイスと交換します。
- PE デバイス（またはコア デバイス）は、CE デバイスに接続されていない、SP ネットワーク内の任意のデバイスです。
- PE デバイスでは、直接接続された VPN の VPN ルートを維持することだけが必要とされます。すべての SP VPN ルートを PE デバイスが維持する必要はありません。 各 PE デバイスは、直接接続しているサイトごとに VRF を維持します。 すべてのサイトが同じ VPN に含まれている場合は、PE デバイスの複数のインターフェイスを 1 つの VRF に関連付けることができます。 各 VPN は、指定された VRF にマッピングされます。 PE デバイスは、ローカル VPN ルートを CE デバイスから学習した後で、内部 BGP（iBGP）を使用して別の PE デバイスと VPN ルーティング情報を交換します。

VRF-lite を使用すると、複数のカスタマーが 1 つの CE デバイスを共有できます。また、1 つの物理リンクのみが CE デバイスと PE デバイス間に使用されます。 共有の CE デバイスは、カスタマーごとに個別の VRF テーブルを保守し、その独自のルーティング テーブルに基づいてカスタマーごとにパケットのスイッチングとルーティングを行います。 VRF-lite は限定された PE デバイスの機能を CE デバイスに拡張して、個別の VRF テーブルを保守する機能を付与し、VPN のプライバシーおよびセキュリティをブランチ オフィスまで拡張します。

図 *7*：*VRF* 間シナリオでのファイアウォール

MPLS VPN

マルチ プロトコル ラベル スイッチング（MPLS）VPN 機能により、複数のサイトが、サービス プロバイダー（SP）ネットワークを通じて透過的に相互接続できます。 1 つの SP ネットワークで、複数の IP VPN をサポートできます。 VPN ユーザから見ると、各 VPN はその他すべてのネットワークとは隔離されたプライベート ネットワークです。 1 つの VPN 内では、各拠点は同一 VPN 内のいずれの拠点にも IP パケットを送信できます。

各 VPN は、1 つ以上の VPN ルーティングおよび転送（VRF）インスタンスに関連付けられています。 VRF は、1 つの IP ルーティング テーブル、派生した 1 つのシスコ エクスプレス フォワーディング テーブル、次のテーブルを使用する複数のインターフェイスで構成されます。

デバイスは、各 VRF に対し別々のルーティングおよびシスコ エクスプレス フォワーディング テーブルを保持します。 これにより、情報が VPN 外に送信されることが回避でき、重複 IP アドレスの問題を起こすことなく同一のサブネットが複数の VPN で使用可能になります。

マルチプロトコル BGP（MP-BGP）を使用しているデバイスは、BGP 拡張コミュニティを使用して VPN のルーティング情報を配布します。

VRF-Aware NAT

ネットワーク アドレス変換（NAT）を使用すると、デバイスなどの単一のデバイスが、インターネット（またはパブリック ネットワーク）とローカル（またはプライベート）ネットワーク間でエージェントとして動作できます。 NAT システムは多様なレベルのセキュリティ機能を提供できますが、主な目的は、アドレス空間を節約することです。

組織が NAT を使用すると、既存のネットワークを持っていてインターネットにアクセスする必要がある場合に、IP アドレスが枯渇する問題を解決できます。 まだ Network Information Center（NIC）-registered IP アドレスを所有していないサイトは、取得する必要があります。 NAT は、何千もの非表示内部アドレスを、取得が容易なアドレス範囲に動的にマッピングすることで、NIC-registered IP アドレスの問題を排除します。

NAT システムがあると、攻撃者は次の情報を特定するのが困難になります。

- ネットワーク上で実行されているシステム数。
- ネットワーク上で実行されているマシンとオペレーティング システムのタイプ。
- ネットワークのトポロジおよび配置。

NAT とマルチプロトコル ラベル スイッチング（MPLS）の統合によって、単一のデバイスに複数の MPLS VPN を設定して、連携させることができます。 NAT は、すべての MPLS VPN が同じ IP アドレッシング スキームを使用している場合でも、IP トラフィックを受信した MPLS VPN を区別できます。 そのため、複数の MPLS VPN ユーザでサービスを共有しながら、各 MPLS VPN を相互に隔離できます。

インターネット接続、ドメイン ネーム サーバ（DNS）、VoIP サービスなどの付加価値サービスをカスタマーに提供するには、MPLS サービス プロバイダーは NAT を使用する必要があります。 NAT により、MPLS VPN カスタマーは、それぞれのネットワーク内で重複した IP アドレスを使用できます。

NAT は、カスタマー エッジ（CE）デバイスまたはプロバイダー エッジ（PE）デバイスに実装できます。 NAT と MPLS VPN の統合機能によって、MPLS クラウド内の PE デバイス上に NAT を実装できます。

VRF-Aware ALG

アプリケーション層ゲートウェイ（ALG）は、アプリケーション パケットのペイロード内の IP アドレス情報を変換するアプリケーションです。 ALG は、NAT によって上書きが必要な、パケット ペイロード内のアドレス情報を識別し、このアドレス情報を NAT およびファイアウォールに提供して従属フローやドアを作成し、データが適切に流れるようにします（データ フローの例は、FTP データ フローです）。 ドアは、特定の基準に一致する着信トラフィックを許可する一時的な構造です。 ドアは、完全な NAT セッション エントリを作成するための十分な情報がないときに作成されます。 ドアには、送信元と宛先 IP アドレスおよび宛先ポートに関する情報が含まれます。 ただし、送信元ポートに関する情報は含まれません。 メディア データが到達すると、その送信元ポート情報は既知であり、ドアは実際の NAT セッションにプロモートされます。

VRF 認識 IPSec

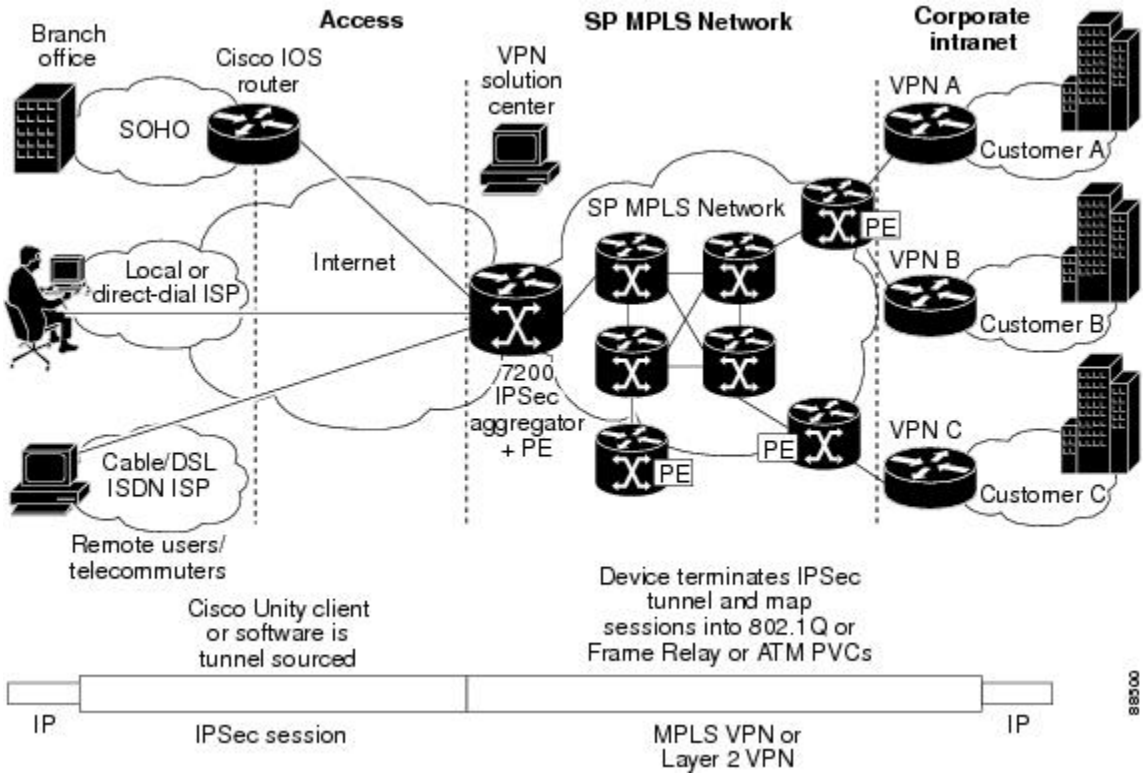
VRF 認識 IPsec 機能を使用すれば、IPsec トンネルをマルチ プロトコル ラベル スイッチング（MPLS）VPN にマッピングできます。 VRF 認識 IPsec 機能を使用すれば、シングル パブリック方向 IP アドレスによって、IPsec トンネルを VPN ルーティングおよび転送（VRF）インスタンスにマッピングできます。

各 IPsec トンネルは、2 つの VRF ドメインに関連付けられます。 外部のカプセル化されたパケットは Front Door VRF（FVRF）という VRF ドメインに属します。 内部の保護された IP パケットは、Inside VRF（IVRF）というドメインに属します。 言い換えると、IPsec トンネルのローカル エンドポイントはFVRFに属し、内部パケットの送信元および宛先アドレスはIVRFに属します。

1つ以上のIPsecトンネルを、単一のインターフェイス上で終了できます。 これらのトンネルのすべての FVRF は同じものであり、そのインターフェイス上で設定されている VRF に設定されます。 これらのトンネルの IVRF は異なる可能性があり、クリプト マップ エントリに付加された Security Association and Key Management Protocol（ISAKMP）プロファイル内で定義されている VRF に依存します。

次の図に、MPLS およびレイヤ 2 VPN に対する IPsec のシナリオを示します。

図 *8*：*MPLS* およびレイヤ *2 VPN* に対する *IPsec*



VRF-Aware Software インフラストラクチャ

VRF-Aware Software インフラストラクチャ（VASI）を使用すると、アクセス コントロール リスト（ACL）、NAT、ポリシング、ゾーンベース ファイアウォールなどのサービスを、2 つの異なる VRF インスタンス上を流れるトラフィックに適用できます。 VASI インターフェイスは、ルートプロセッサ（RP）および転送プロセッサ（FP）の冗長性をサポートします。 この機能は、VASI インターフェイスでの IPv4 および IPv6 ユニキャスト トラフィックをサポートします。

VASI の主な用途は、より効率的に VRF を分離できるようにすることです。 VASI では、VRF ごとに固有の機能を、共通のインターフェイスを共有する（たとえば、すべての VRF がインターネットへの同じインターフェイスを共有している場合があります）他の VRF に影響を与えることなく VASI インターフェイスに適用できます。 ファイアウォールでは、この機能により、ゾーンを VASI に適用できます。

VASI は、仮想インターフェイスのペアを使用して実装され、ペアの各インターフェイスは異なる VRF に関連付けられます。 VASI 仮想インターフェイスは、これら 2 つの VRF 間で交換される必要があるパケットのネクスト ホップ インターフェイスです。 VASI インターフェイスは、2 つの VRF 間の NAT をサポートするために必要なフレームワークを提供します。

各インターフェイス ペアは、異なる 2 つの VRF インスタンスに関連付けられています。 2 つの仮想インターフェイスのペア（vasileft と vasiright）は、論理的にバックツーバックで接続されており、完全な対称性を有しています。 各インターフェイスにはインデックスがあります。 ペアリングの関連付けは、vasileft が自動的に vasiright へのペアを取得するという方法で、2 つのインターフェイスのインデックスに基づいて自動的に行われます。 BGP、Enhanced Interior Gateway Routing Protocol（EIGRP）、または Open Shortest Path First（OSPF）によるスタティック ルーティングまたはダイナミック ルーティングを設定できます。 BGP ダイナミック ルーティング プロトコルの制約事項とコンフィギュレーションは、VASI インターフェイス間の BGP ルーティング コンフィギュレーションに有効です。 VASI の詳細については、「VRF-Aware Software インフラストラクチャの設定」機能を参照してください。

セキュリティ ゾーン

セキュリティ ゾーンとは、ポリシーを適用できるインターフェイスのグループです。

インターフェイスをゾーンにグループ化するには、次の 2 つの手順を実行します。

- インターフェイスを付加できるようにゾーンを作成します。
- インターフェイスを特定のゾーンのメンバーとなるように設定します。

デフォルトでは、トラフィックは、同じゾーンのメンバーであるインターフェイス間を通ります。

インターフェイスがセキュリティ ゾーンのメンバーである場合、そのインターフェイスと、別のゾーン内のインターフェイスとの間のすべてのトラフィック（デバイス宛またはデバイス発信のトラフィックを除く）はデフォルトでドロップされます。 ゾーンメンバーインターフェイスと別のインターフェイスとの間の両方向のトラフィックを許可するには、そのゾーンをゾーン ペアの一部にして、そのゾーン ペアにポリシーを適用する必要があります。 ポリシーで、**inspect** また

は **pass** アクションを通してトラフィックが許可されると、トラフィックはインターフェイスを通過します。

ゾーンを設定する際に検討する基本ルールは次のとおりです。

- ゾーン インターフェイスからゾーン外のインターフェイスへのトラフィックまたはゾーン外のインターフェイスからゾーン インターフェイスへのトラフィックは常にドロップされます。ただし、デフォルト ゾーンがイネーブルになっている場合を除きます（デフォルト ゾーンはゾーン外のインターフェイスです）。
- 2 つのゾーン インターフェイス間のトラフィックは、各ゾーンにゾーン ペアの関係があるかどうか、およびそのゾーン ペアにポリシーが設定されているかどうかが検査されます。
- デフォルトでは、同じゾーン内の 2 つのインターフェイス間のすべてのトラフィックは、常に許可されます。
- ゾーン ペアは、ゾーンを送信元ゾーンおよび宛先ゾーンの両方として設定できます。 このゾーン ペアで検査ポリシーを設定して、同じゾーン内の 2 つのインターフェイス間のトラフィックを検査またはドロップできます。
- インターフェイスをゾーンとレガシー検査ポリシーの両方に同時に所属させることはできません。
- インターフェイスがメンバーになれるのは、1 つのセキュリティ ゾーンだけです。
- インターフェイスがセキュリティ ゾーンのメンバーの場合、そのゾーンを含むゾーン ペアで明示的なゾーン間ポリシーを設定しない限り、方向に関係なくそのインターフェイスを通過するすべてのトラフィックがブロックされます。
- トラフィックは、セキュリティ ゾーンのメンバーであるインターフェイスとセキュリティ ゾーンのメンバーではないインターフェイスの間では通過できません。これは、ポリシーは 2 つのゾーンだけで適用できるからです。
- トラフィックがデバイスのすべてのインターフェイスを通過するようにするには、すべてのインターフェイスは 1 つのセキュリティ ゾーンまたは別のゾーンのメンバーでなければなりません。 インターフェイスをセキュリティ ゾーンのメンバーにした後、**inspect** や **pass** などのポリシー アクションによってパケットを明示的に許可する必要があるため、このことは特に重要です。 それ以外の場合、パケットはドロップされます。
- デバイスのインターフェイスをセキュリティ ゾーンまたはファイアウォール ポリシーに所属させることができない場合、そのインターフェイスをセキュリティ ゾーンに追加し、そのゾーンとトラフィック フローの対象となる他のゾーンとの間に、「すべて通過」ポリシー（つまり、「ダミー」ポリシー）を設定する必要がある場合があります。
- セキュリティ ゾーン間またはゾーン ペアに対してアクセス コントロール リスト（ACL）を適用することはできません。
- セキュリティ ゾーンとゾーン ペアの間で ACL は適用できません。 トラフィックをドロップするには、ACL 設定をクラス マップに含め、ポリシー マップを使用します。
- ゾーン メンバーのインターフェイス上の ACL を制約的（厳密）にしないでください。

- 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 VPN ルーティングおよび転送（VRF）インスタンスに属している必要があります。
- メンバ インターフェイスが個別の VRF にあるセキュリティ ゾーン間でポリシーを設定できます。 ただし、設定で許可されていない場合、これらの VRF 間をトラフィックは流れません。
- トラフィックが VRF 間を流れない場合（VRF 間のルートリークが設定されていないため）、VRF 間のポリシーは実行されません。 これは、ポリシー側ではなく、ルーティング側の設定の誤りです。
- 同じセキュリティ ゾーン内のインターフェイス間のトラフィックはポリシーには従わず、自由に通過します。
- ゾーン ペアの送信元ゾーンおよび宛先ゾーンは、タイプ セキュリティのゾーンである必要があります。
- 同じゾーンを送信元ゾーンと宛先ゾーンの両方として定義することはできません。

ポリシーは、トラフィック フローの最初のパケットに適用されます。最初のパケットが分類および許可されると、トラフィックは、それ以上のパケット再分類なしでピア間を通過します（これは、最初の分類後に双方向トラフィック フローが許可されたことを意味します）。 ゾーン Z1 とゾーン Z2 間のゾーン ペアがあり、ゾーン Z2 とゾーン Z1 間のゾーン ペアはない場合、ゾーン Z2 から開始されたすべてのトラフィックはブロックされます。 ゾーン Z1 からゾーン Z2 へのトラフィックは、ゾーン ペアのポリシーに基づいて許可または拒否されます。

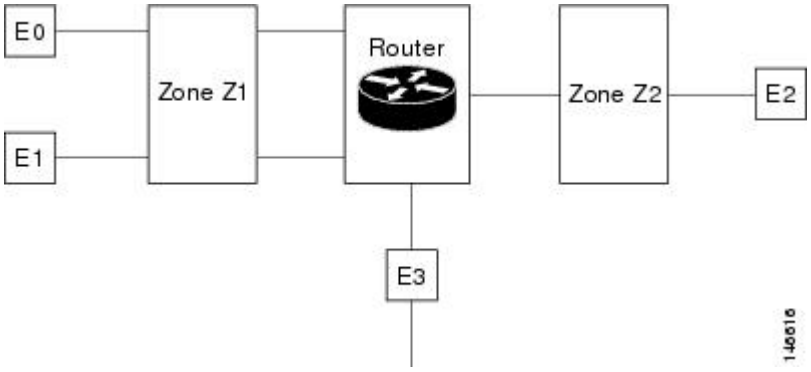
トラフィックがデバイスのすべてのインターフェイスを通過するようにするには、すべてのインターフェイスはセキュリティ ゾーンまたはデフォルト ゾーンのメンバーでなければなりません。

すべてのデバイス インターフェイスがセキュリティ ゾーンのメンバーである必要はありません。

下の図は、次のことを示しています。

- インターフェイス E0 と E1 はセキュリティ ゾーン Z1 のメンバーです。
- インターフェイス E2 は、セキュリティ ゾーン Z2 のメンバーです。
- インターフェイス E3 は、どのセキュリティ ゾーンのメンバーでもありません。

図 *9*：セキュリティ ゾーンの制約



次の状況が存在します。

- ゾーン ペアとポリシーは、同じゾーンで設定されます。 Z1 と Z2 用のポリシーが設定されていない場合、トラフィックは E0 と E1 間を自由に通過しますが、E0 または E1 と E2 間は通過しません。 このトラフィックを検査するためのゾーン ペアとポリシーを作成できます。
- ポリシーが設定されていない場合、他のインターフェイス間（E0 と E2、E1 と E2、E3 と E1、および E3 と E2）でトラフィックは流れません。
- トラフィックを許可する明示的なポリシーがゾーン Z1 とゾーン Z2 間で設定されている場合だけ、E0 または E1 と E2 間でトラフィックが流れます。
- デフォルト ゾーンがイネーブルで、ゾーン ペアがデフォルト ゾーンと他のゾーンとの間に作成されている場合を除き、E3 と E0、E1、または E2 間をトラフィックが流れることはまったくありません。

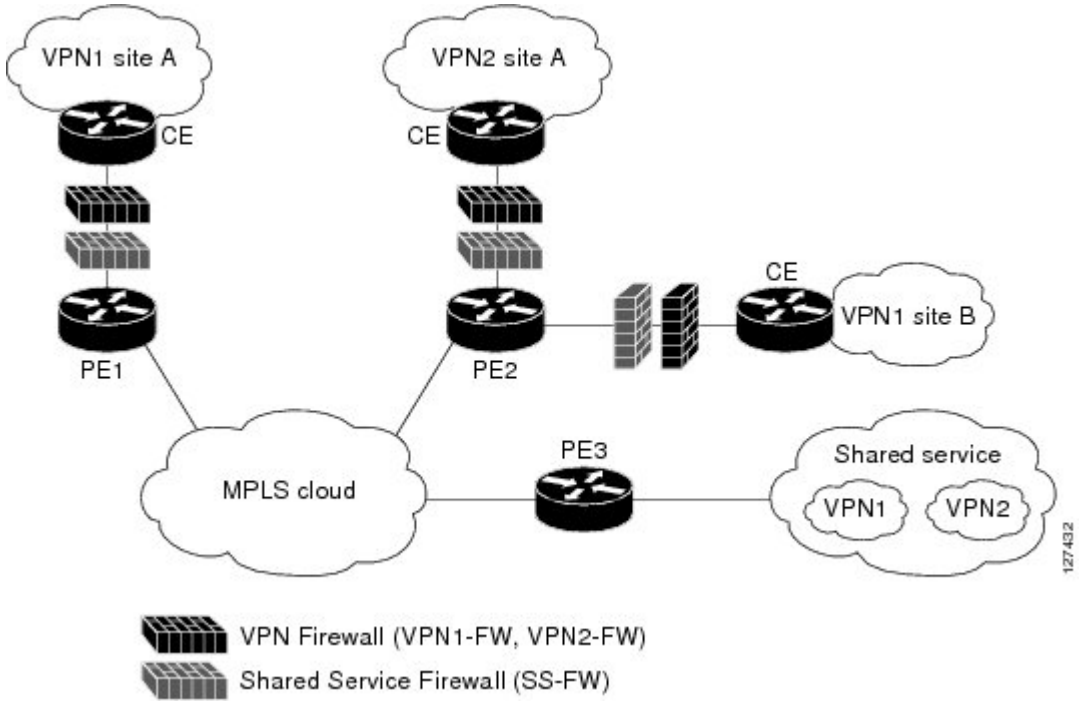
VRF-Aware Cisco ファイアウォールの展開

ファイアウォールをネットワーク内の多数のポイントに展開することで、VPN サイトと共有サービス（またはインターネット）を双方向で保護できます。 ここでは、次のファイアウォール展開シナリオについて説明します。

VRF-Aware Cisco ファイアウォールを擁する分散型ネットワーク

次の図では、サービス プロバイダー（SP）がファイアウォール サービスを VPN カスタマーの VPN1 および VPN2 に提供し、VPN サイトと外部ネットワーク（共有サービスやインターネットなど）を双方向で保護するという一般的な状況について示します。

図 *10*：分散型ネットワーク



この例では、VPN1 には、マルチ プロトコル ラベル スイッチング（MPLS）コア全体を対象とする Site A と Site B という 2 つのサイトがあります。 Site A は PE1 に接続され、Site B は PE2 に接続されています。 VPN2 には、PE2 に接続している 1 つのサイトのみがあります。 各 VPN には、PE3 上の対応する VLAN サブインターフェイスに接続されている共有サービス内の VLAN セグメントがあります。

各 VPN（VPN1 および VPN2）には 2 つのファイアウォール ルールがあります。1 つは、VPN サイトを共有サービスから保護するためのもので、もう 1 つは共有サービスを VPN サイトから保護するためのものです。 VPN サイトを共有サービスから保護するファイアウォールは VPN ファイアウォールと呼ばれ、共有サービスを VPN サイトから保護するファイアウォールは共有サービス ファイアウォールと呼ばれます。 両方のファイアウォール ルールが、VPN サイトに接続された各入力プロバイダーエッジ（PE）デバイスの VPN ルーティングおよび転送（VRF）インターフェイスに適用されます。 VPN ファイアウォール ルールは、VRF インターフェイスが VPN サイトへの入力であるため、入力方向に適用されます。共有サービス ファイアウォール ルールは、VRF インターフェイスが共有サービスへの出力であるため、出力方向に適用されます。

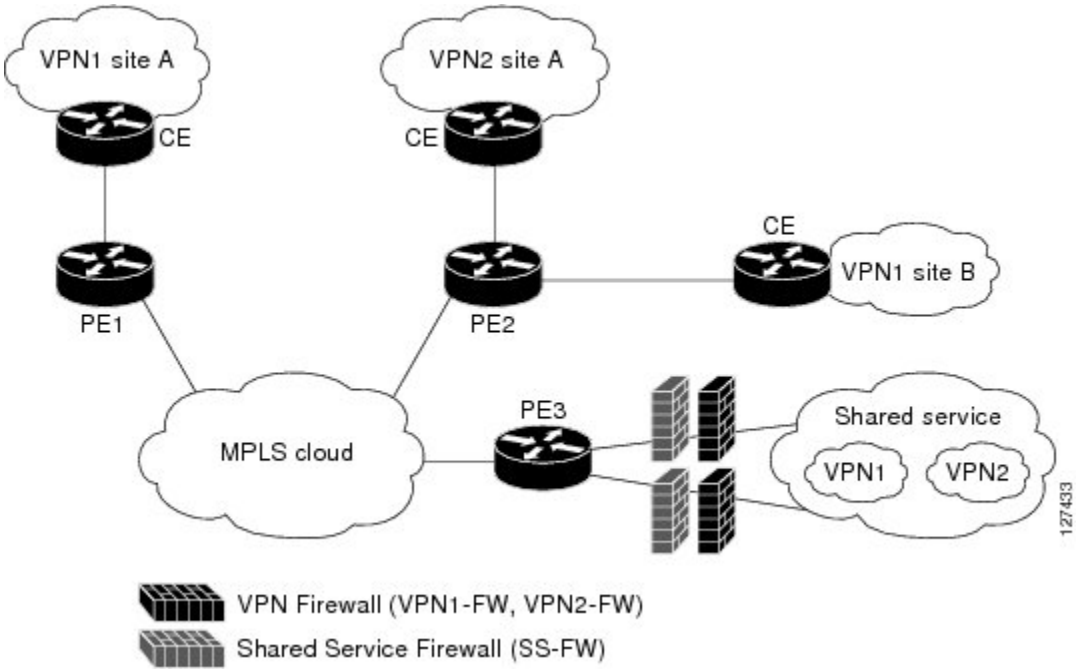
分散型ネットワークを使用する利点は次のとおりです。

- ファイアウォールの展開はマルチプロトコル ラベル スイッチング（MPLS）クラウドで分散されるため、ファイアウォールの処理負荷はすべての入力 PE デバイスに分散されます。
- 共有サービスは、入力 PE デバイスの VPN サイトから保護されるため、VPN サイトから送信された悪意のあるパケットは、MPLS クラウドに入る前に、入力 PE デバイスでフィルタリングされます。
- VPN ファイアウォール機能は入力方向に展開できます。

VRF-Aware Cisco ファイアウォールを擁するハブアンドスポーク ネットワーク

次の図に、すべての VPN サイトのファイアウォールが、共有サービスに接続されている出力 PE デバイス、PE3 に適用されるハブアンドスポーク ネットワークを示します。

図 *11*：ハブアンドスポーク ネットワーク



通常、各 VPN には、共有サービスに接続された VLAN および/または VPN ルーティングおよび転送（VRF）サブインターフェイスがあります。 パケットがマルチ プロトコル ラベル スイッチング（MPLS）インターフェイスに到達すると、MPLS は、共有サービスに接続されている対応するサブインターフェイスにパケットをルーティングします。 各 VPN のファイアウォール ポリシーは、上記の図に示すように対応するサブインターフェイス（VRF インターフェイス）に適用されます。 VPN ファイアウォール ルールは、サブインターフェイスが VPN サイトへの出力であるため、出力方向に適用されます。 共有サービス ファイアウォール ルールは、サブインターフェイスが共有サービスへの入力であるため、入力方向に適用されます。

ハブアンドスポーク ネットワークの利点は次のとおりです。

- ファイアウォール展開はプロバイダーエッジ（PE）デバイス（PE3）に集中化されるため、ファイアウォールを簡単に展開および管理できます。
- 共有サービス ファイアウォール機能は、入力方向に適用できます。
- VPN サイトは出力 PE デバイスの共有サービスから保護されるため、共有サービスからの悪意のあるパケットは MPLS クラウドに入る前に PE デバイスでフィルタリングされます。

VRF-Aware Cisco IOS XE ファイアウォールの設定方法

VRF、クラス マップ、およびポリシー マップの定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*
7. **exit**
8. **class-map type inspect match-any** *class-map-name*
9. **match protocol tcp**
10. **match protocol h323**
11. **exit**
12. **policy-map type inspect** *policy-map-name*
13. **class type inspect** *class-map-name*
14. **inspect** [*parameter-map-name*]
15. **exit**
16. **class class-default**
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： `Router(config)# ip vrf vrf1`	VRF インスタンスを定義し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Router(config-vrf)# rd 10:1`	VRF インスタンスのルート識別子（RD）を指定します。
ステップ 5	**route-target export** *route-target-ext-community* 例： `Router(config-vrf)# route-target export 10:1`	VRF インスタンスのルートターゲット拡張コミュニティを作成し、ルーティング情報をターゲット VPN 拡張コミュニティにエクスポートします。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Router(config-vrf)# route-target import 10:1`	VRF インスタンスのルートターゲット拡張コミュニティを作成し、ルーティング情報をターゲット VPN 拡張コミュニティにインポートします。
ステップ 7	**exit** 例： `Router(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**class-map type inspect match-any** *class-map-name* 例： `Router(config)# class-map type inspect match-any class-map1`	レイヤ 3 およびレイヤ 4（アプリケーション固有）検査タイプ クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。
ステップ 9	**match protocol tcp** 例： `Router(config-cmap)# match protocol tcp`	指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 10	**match protocol h323** 例： `Router(config-cmap)# match protocol h323`	指定されたプロトコルに基づいて、クラスマップの一致基準を設定します。
ステップ 11	**exit** 例： `Router(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 12	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect global-vpn1-pmap`	レイヤ3とレイヤ4（プロトコル固有）検査タイプポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 13	**class type inspect** *class-map-name* 例： `Router(config-pmap)# class type inspect class-map1`	アクションを実行する対象のトラフィック（クラス）を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 14	**inspect** [*parameter-map-name*] 例： `Router(config-pmap-c)# inspect class-map1`	Cisco IOS XE ステートフル パケット インスペクションをイネーブルにします。
ステップ 15	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 16	**class class-default** 例： `Router(config-pmap)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。 • class-default クラスはデフォルトで定義されています。class-default に関連付けられているデフォルトのドロップ属性を変更するように **class class-default** コマンドを設定します。
ステップ 17	**end** 例： `Router(config-pmap)# end`	ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

ゾーンとゾーン ペアの定義

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *security-zone-name*
4. **exit**
5. **zone security** *security-zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *security-zone-name* 例： `Router(config)# zone security vpn1-zone`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**zone security** *security-zone-name* 例： `Router(config)# zone security global-zone`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Router(config)# zone-pair security vpn1-global-zone-pair source vpn1-zone destination global-zone`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 • *zone-pair-name*：インターフェイスに付加されているゾーンの名前。 • **source** *source-zone*：トラフィックが発信されるルータの名前を指定します。 • **destination** *destination-zone*：トラフィックがバインドされているルータの名前を指定します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect global-vpn1-pmap`	レイヤ 7 ポリシー マップをトップレベル ポリシー マップに付加します。
ステップ 9	**end** 例： `Router(config-sec-zone-pair)# end`	ゾーンペア コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

インターフェイスへのゾーンの適用およびルートの定義

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *name*
5. **ip address** *ip-address mask*
6. **zone-member security** *zone-name*
7. **negotiation auto**
8. **exit**
9. **interface** *type number*
10. **ip address** *ip-address mask*
11. **zone-member security** *zone-name*
12. **negotiation auto**
13. **exit**
14. **ip route vrf** *vrf-name destination-ip-address destination-prefix interface-type number* [**global**]
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip vrf forwarding** *name* 例： `Router(config-if)# ip vrf forwarding vrf1`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。

	コマンドまたはアクション	目的
ステップ 5	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 6	**zone-member security** *zone-name* 例： `Router(config-if)# zone-member security vpn1-zone`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 7	**negotiation auto** 例： `Router(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 8	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 9	**interface** *type number* 例： `Router(config)# interface gigabitethernet 1/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.111.111.111 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 11	**zone-member security** *zone-name* 例： `Router(config-if)# zone-member security global-zone`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 12	**negotiation auto** 例： `Router(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 13	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 14	**ip route vrf** *vrf-name destination-ip-address destination-prefix interface-type number* [**global**] 例： `Router(config)# ip route vrf vpn1 10.111.111.0 255.255.255.0 gigabitethernet 1/1/1 global`	VRF インスタンスのスタティック ルートを確立します。
ステップ 15	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

VRF-Aware Cisco IOS XE ファイアウォールの設定例

例：VRF、クラス マップ、およびポリシー マップの定義

```
Router# configure terminal
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 10:1
Router(config-vrf)# route-target export 10:1
Router(config-vrf)# route-target import 10:1
Router(config-vrf)# exit
Router(config)# class-map type inspect match-any class-map1
Router(config-cmap)# match protocol tcp
Router(config-cmap)# match protocol h323
Router(config-cmap)# exit
Router(config)# policy-map type inspect global-vpn1-pmap
Router(config-pmap)# class type inspect match-acl-111
Router(config-pmap-c)# inspect match-acl-111
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap)# end
```

例：ポリシー マップ、ゾーン、およびゾーン ペアの定義

```
Router# configure terminal
Router(config)# zone security vpn1-zone
Router(config-sec-zone)# exit
Router(config)# zone security global-zone
Router(config-sec-zone)# exit
Router(config)# zone-pair security vpn1-global-zone-pair source vpn1-zone destination
global-zone
Router(config-sec-zone-pair)# service-policy type inspect vpn1-global-pmap
Router(config-sec-zone-pair)# end
```

例：インターフェイスへのゾーンの適用およびルートの定義

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip vrf forwarding vrf1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# zone-member security vpn1-zone
Router(config-if)# negotiation auto
Router(config-if)# exit
Router(config)# interface gigabitethernet 1/1/1
Router(config-if)# ip address 10.111.111.111 255.255.255.0
Router(config-if)# zone-member security global-zone
Router(config-if)# negotiation auto
Router(config-if)# exit
Router(config)# ip route vrf vpn1 10.111.111.0 255.255.255.0 gigabitethernet 1/1/1 global
Router(config)# end
```

VRF-Aware Cisco IOS XE ファイアウォールの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
NAT	『Configuring Network Address Translation: Getting Started』
MPLS VPN	『*Configuring a Basic MPLS VPN*』
ゾーンベース ポリシー ファイアウォール	『*Zone-based Policy Firewall*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VRF-Aware Cisco IOS XE ファイアウォールの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *5*：*VRF-Aware Cisco IOS XE* ファイアウォールの機能情報

機能名	リリース	機能情報
VRF-Aware Cisco IOS XE ファイアウォール	Cisco IOS XE Release 2.5	SP または大企業のエッジ ルータに VRF-Aware Cisco IOS XE ファイアウォールが設定されている場合、Cisco IOS XE ファイアウォール機能が VRF インターフェイスに適用されます。
Firewall--VRF-Aware ALG サポート	Cisco IOS XE Release 2.5	Firewall--VRF-Aware ALG のサポート機能によって、正しい IP アドレスの VRF ID ペアが必要な ALG トークンを作成するときに、ALG はキャッシュ済みの情報から適切な IP アドレスと VRF ID を抽出できます。

用語集

C3PL：Cisco Common Classification Policy Language。 イベント、条件、およびアクションに基づいてトラフィック ポリシーを作成するためにポリシー マップおよびクラス マップを使用する、構造化された機能固有のコンフィギュレーション コマンドです。

EHLO：機能ネゴシエーションを開始するための Extended HELO 置換コマンド。 このコマンドは、ESMTPプロトコルを使用してリモートSMTPサーバに接続する送信元（クライアント）を識別します。

ESMTP：拡張 SMTP。 シンプル メール転送プロトコル（SMTP）の拡張バージョン。配信通知やセッションの配信などの追加機能が含まれています。 ESMTP は、RFC 1869「SMTP Service Extensions」で定義されています。

HELO：SMTP 機能ネゴシエーションを開始するコマンド。 このコマンドは、完全修飾 DNS ホスト名でリモート SMTP サーバに接続する送信元（クライアント）を識別します。

MAIL FROM：メッセージの From: フィールドに表示される、送信者の電子メール アドレスおよび名前（使用する場合）を識別する電子メール メッセージの開始部分です。

MIME：Multipurpose Internet Mail Extension。 電子メールで、テキスト以外のデータ（つまり、プレーン ASCII コードでは表現できないデータ）を転送するための規格。たとえば、バイナリ、外国語テキスト（ロシア語や中国語など）、オーディオ、ビデオなどのデータです。 MIME は RFC 2045 で定義されています。

RCPT TO：単一のメッセージを複数の受信者に配信するために、類似のメッセージで複数回繰り返すことができる受信者の電子メール アドレスおよび名前（使用する場合）。

SMTP：シンプル メール転送プロトコル。 電子メール サービスを提供するインターネット プロトコル。

第 4 章

ゾーンベース ポリシー ファイアウォールのネストされたクラス マップ サポート

ゾーンベース ポリシー ファイアウォールのネストされたクラス マップ サポート機能では、複数のトラフィック クラス（ネストされたクラス マップまたは階層型クラス マップとも呼ばれます）を単一のトラフィック クラスとして設定する機能を Cisco IOS XE ファイアウォールに提供します。 パケットが複数の一致条件を満たす場合、単一のトラフィック ポリシーに関連付けることができる複数のクラス マップを設定できます。 Cisco IOS XE ファイアウォールは、クラス マップ階層を 3 つのレベルまでサポートします。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用の

プラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ゾーンベースポリシーファイアウォールのネストされたクラス マップ サポートの前提条件

ネストされたクラス マップを設定する前に、モジュラ Quality of Service（QoS）CLI（MQC）を十分に理解している必要があります。

ゾーンベースポリシーファイアウォールのネストされたクラス マップ サポートについて

ネストされたクラス マップ

Cisco IOS XE Release 3.5S 以降のリリースでは、複数のトラフィック クラス（ネストされたクラス マップまたは階層型クラスマップとも呼ばれます）を単一のトラフィック クラスとして設定できます。 パケットが複数の一致条件を満たす場合、単一のトラフィック ポリシーに関連付けることができる複数のクラス マップを設定できます。 クラス マップのネストを **match class-map** コマンドにより実現できます。 1 つのトラフィック クラスで match-any 特性と match-all 特性を組み合わせる唯一の方法は、**class-map** コマンドを使用することです。

class-map コマンドの match-all キーワードと match-any キーワード

トラフィック クラスを作成するには、**class-map** コマンドを **match-all** キーワードと **match-any** キーワードを使用して設定する必要があります。 トラフィック クラスで複数の一致条件が設定されている場合にのみ、**match-all** キーワードと **match-any** キーワードを指定する必要があります。 次のルールは、**match-all** キーワードおよび **match-any** キーワードに適用されます。

- 指定したトラフィック クラスにパケットを配置するために、トラフィック クラスのすべての一致条件が満たされる必要がある場合は、**match-all** キーワードを使用します。
- 指定したトラフィック クラスにパケットを配置するために、トラフィック クラスの一致条件の 1 つだけが満たされる必要がある場合は、**match-any** キーワードを使用します。
- **match-all** キーワードまたは **match-any** キーワードを指定しない場合、トラフィック クラスは **match-all** キーワードと一致する方法で動作します。

ゾーンベース ポリシー ファイアウォール コンフィギュレーションでは、次の条件が満たされた場合にネストされたクラス マップをサポートします。

- 階層の個々のクラス マップには複数の **match class-map** コマンド リファレンスが含まれます。
- 階層の個々のクラスマップには、**match class-map** コマンド以外の一致ルールが含まれます。

ゾーンベースポリシーファイアウォールのネストされたクラス マップ サポートの設定方法

ネストされた Two-Layer クラス マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **class-map match-any** *class-map-name*
7. **match protocol** *protocol-name*
8. **exit**
9. **class-map match-any** *class-map-name*
10. **match class-map** *class-map-name*
11. **match class-map** *class-map-name*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**class-map match-any** *class-map-name* 例： `Router(config)# class-map match-any child1`	レイヤ 3 またはレイヤ 4 のクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Router(config-cmap)# match protocol tcp`	指定されたプロトコルを基づくクラス マップの一致基準を設定します。
ステップ 5	**exit** 例： `Router(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**class-map match-any** *class-map-name* 例： `Router(config)# class-map match-any child2`	レイヤ 3 またはレイヤ 4 のクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。
ステップ 7	**match protocol** *protocol-name* 例： `Router(config-cmap)# match protocol udp`	指定されたプロトコルを基づくクラス マップの一致基準を設定します。
ステップ 8	**exit** 例： `Router(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 9	**class-map match-any** *class-map-name* 例： `Router(config)# class-map match-any parent`	レイヤ 3 またはレイヤ 4 のクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。
ステップ 10	**match class-map** *class-map-name* 例： `Router(config-cmap)# match class-map child1`	トラフィック クラスを分類ポリシーとして設定します。
ステップ 11	**match class-map** *class-map-name* 例： `Router(config-cmap)# match class-map child2`	トラフィック クラスを分類ポリシーとして設定します。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Router(config-cmap)# end`	クラス マップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ネストされたクラス マップのポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class-type inspect** *class-map-name*
5. **inspect**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect pmap`	レイヤ 3 またはレイヤ 4 の検査タイプ ポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class-type inspect** *class-map-name* 例： `Router(config-pmap)# class-type inspect parent`	アクションを実行する対象のトラフィック（クラス）を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**inspect** 例： `Router(config-pmap-c)# inspect`	Cisco IOS XE ステートフル パケット インスペクションをイネーブルにします。
ステップ 6	**end** 例： `Router(config-pmap-c)# end`	ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーン ペアへのポリシー マップの付加

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *zone-name* **destination** [*zone-name*]]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**zone security** *zone-name* 例： `Router(config)# zone security source-zone`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**zone security** *zone-name* 例： `Router(config)# zone security destination-zone`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** *zone-name* **destination** [*zone-name*]] 例： `Router(config)# zone-pair security secure-zone source source-zone destination destination-zone`	ゾーン ペアを作成し、セキュリティ ゾーン ペア コンフィギュレーション モードを開始します。 • ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect pmap`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Router(config-sec-zone-pair)# exit`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**zone-member security** *zone-name* 例： `Router(config-if)# zone-member security source-zone`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンベースポリシーファイアウォールのネストされたクラス マップ サポートの設定例

例：ネストされた Two-Layer クラス マップの設定

```
Router# configure terminal
Router(config)# class-map match-any child1
Router(config-cmap)# match protocol tcp
Router(config-cmap)# exit
Router(config)# class-map match-any child2
Router(config-cmap)# match protocol udp
Router(config-cmap)# exit
Router(config)# class-map match-any parent
Router(config-cmap)# match class-map child1
Router(config-cmap)# match class-map child2
Router(config-cmap)# end
```

例：ネストされたクラス マップのポリシー マップの設定

```
Router# configure terminal
Router(config)# policy-map type inspect pmap
Router(config-pmap)# class-type inspect parent
Router(config-pmap-c)# inspect
```

```
Router(config-pmap-c)# end
```

例：ゾーン ペアへのポリシー マップの付加

```
Router# configure terminal
Router(config)# zone security source-zone
Router(config-sec-zone)# exit
Router(config)# zone security destination-zone
Router(config-sec-zone)# exit
Router(config)# zone-pair security secure-zone source source-zone destination destination-zone
Router(config-sec-zone-pair)# service-policy type inspect pmap
Router(config-sec-zone-pair)# exit
Router(config)# interface gigabitethernet 0/0/1
Router(config-if)# zone-member security source-zone
Router(config-if)# end
```

ゾーンベースポリシーファイアウォールのネストされたクラス マップ サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
ゾーンベース ポリシー ファイアウォール	『*Zone-Based Policy Firewall*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ゾーンベースポリシーファイアウォールのネストされたクラス マップ サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *6*：ゾーンベース ポリシー ファイアウォールのネストされたクラス マップ サポートの機能情報

機能名	リリース	機能情報
ゾーンベース ポリシー ファイアウォールのネストされたクラス マップ サポート	Cisco IOS XE Release 3.5S	ゾーンベース ポリシー ファイアウォールのネストされたクラス マップ サポート機能では、複数のトラフィック クラス（ネストされたクラス マップまたは階層型クラス マップとも呼ばれます）を単一のトラフィック クラスとして設定する機能を Cisco IOS XE ファイアウォールに提供します。 パケットが複数の一致条件を満たす場合、単一のトラフィック ポリシーに関連付けることができる複数のクラス マップを設定できます。

第 5 章

ファイアウォール ステートフル シャーシ間冗長性の設定

ファイアウォール ステートフル シャーシ間冗長性機能を使用すると、相互にバックアップとして動作するルータのペアを設定できます。 この機能を設定し、複数のフェールオーバー条件に基づいてアクティブ ルータを判断できます。 フェールオーバーが発生すると、中断なくスタンバイ ルータが引き継ぎ、トラフィック フォワーディング サービスの実行とダイナミック ルーティング テーブルのメンテナンスを開始します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ファイアウォールステートフルシャーシ間冗長性の前提条件

- ファイアウォールに接続しているインターフェイスは、同じ冗長インターフェイス識別子（RII）を持つ必要があります。
- アクティブ デバイスおよびスタンバイ デバイスは、Cisco IOS XE ゾーンベース ファイアウォールの設定を同じにする必要があります。
- アクティブ デバイスとスタンバイ デバイスは、同じバージョンの Cisco IOS XE ソフトウェアで実行する必要があります。 アクティブ デバイスとスタンバイは、スイッチを介して接続する必要があります。
- 組み込みサービス プロセッサ（ESP）は、アクティブデバイスとスタンバイ デバイスの両方で一致する必要があります。

ファイアウォールステートフルシャーシ間冗長性の制約事項

- マルチプロトコル ラベル スイッチング（MPLS）および仮想ルーティングおよび転送（VRF）はサポートされません。
- LAN および WAN シナリオはサポートされません。
- LAN および MESH シナリオはサポートされません。
- デュアル組み込みサービス プロセッサ（ESP）またはデュアル ルート プロセッサ（RP）がシャーシに含まれている Cisco ASR 1006 および Cisco ASR 1013 プラットフォームは、ボックス間ハイ アベイラビリティ（HA）およびボックス内 HA がサポートされていないため、サポートされていません。
  単一の ESP および単一の RP がシャーシに含まれている Cisco ASR 1006 および Cisco ASR 1013 プラットフォームは、シャーシ間冗長をサポートします。
- デュアル IOS デーモン（IOSd）が設定されている場合、デバイスはファイアウォール ステートフル シャーシ間冗長構成をサポートしません。

ファイアウォールステートフルシャーシ間冗長性について

ファイアウォール ステートフル シャーシ間冗長性の機能

相互にホットスタンバイとして動作するようにルータのペアを設定できます。 この冗長性は、インターフェイスベースで設定します。冗長インターフェイスのペアは、冗長グループと呼ばれます。 下の図は、アクティブ-スタンバイ デバイス シナリオを示しています。 また、1 つの発信インターフェイスを持つルータのペアについて、冗長グループを設定する方法を示します。 冗長グループの設定：*2*つの発信インターフェイスの図は、アクティブ-アクティブ デバイス シナリオを表し、2つの冗長グループが、2つの発信インターフェイスを持つルータのペアに設定される方法を示しています。

いずれの場合でも、設定可能なコントロール リンクおよびデータ同期リンクによって冗長ルータは参加します。 コントロール リンクは、ルータのステータスを通信するために使用されます。 データ同期リンクは、ネットワーク アドレス変換（NAT）およびファイアウォールからステートフル情報を転送し、これらのアプリケーションについてステートフル データベースを同期するために使用されます。

また、いずれの場合でも、冗長インターフェイスのペアは、同じ固有ID番号（RIIと呼ばれます）で設定されます。

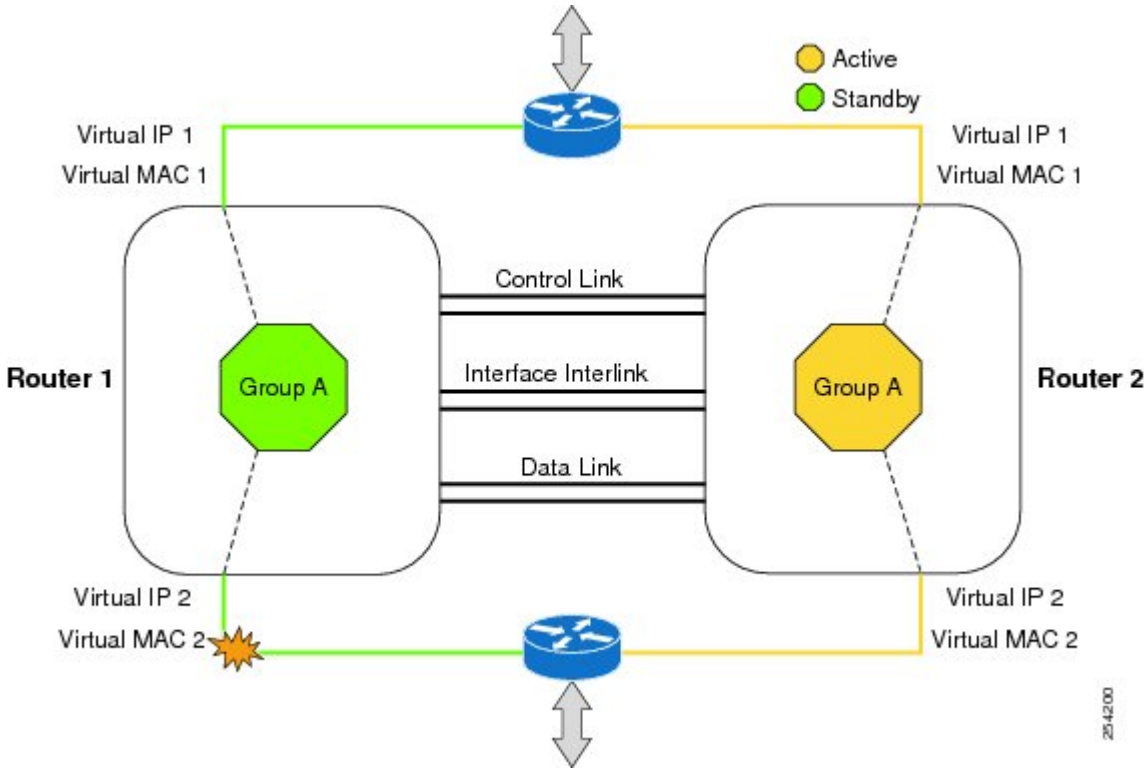
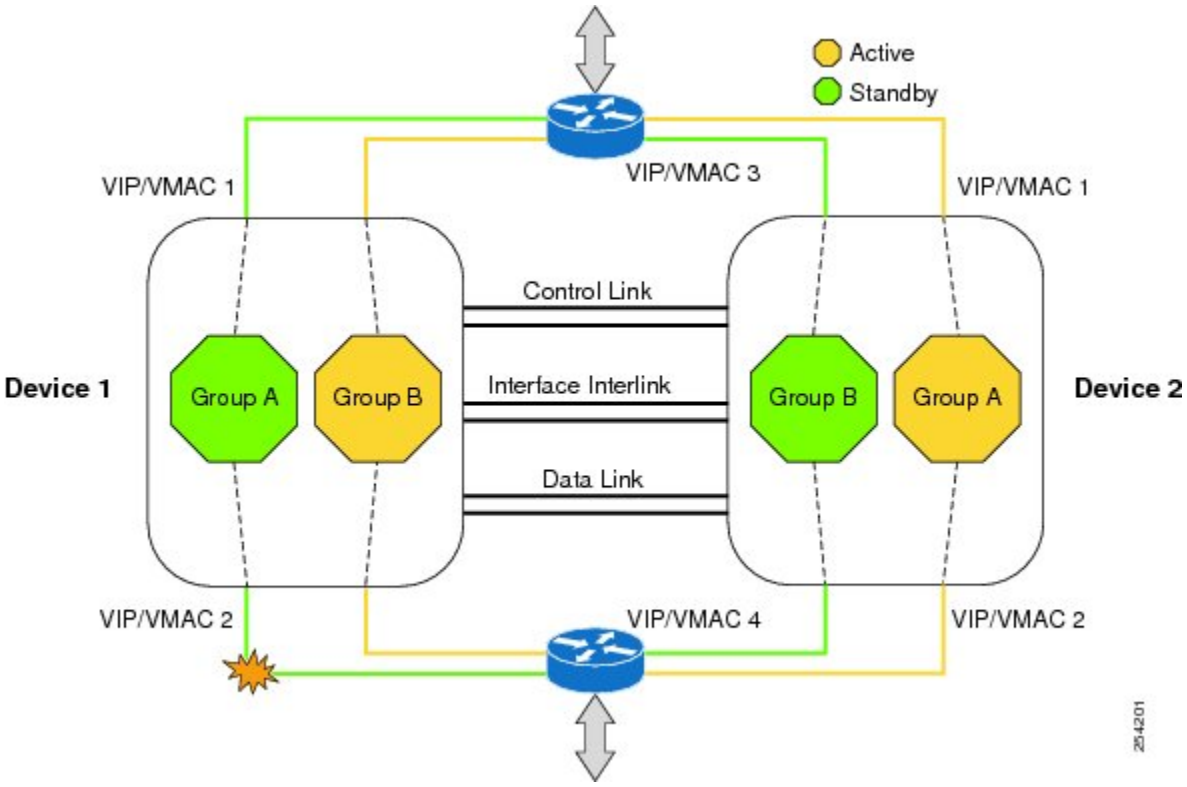


図 *12*：冗長グループの設定：*2* つの発信インターフェイス



冗長グループ メンバーのステータスは、コントロール リンクで送信される hello メッセージを使用することで判断できます。 設定可能な時間内に、いずれかのルータが hello メッセージに応答しない場合、エラーが発生したと見なされ、スイッチオーバーが開始されます。 ミリ秒単位でエラーを検出するには、双方向フォワーディング検出（BFD）プロトコルと統合されたフェールオーバー プロトコルをコントロール リンクで実行します。 hello メッセージについて次のパラメータを設定できます。

- Active timer
- Standby timer
- Hellotime：hello メッセージが送信される間隔
- Holdtime：アクティブまたはスタンバイ ルータがダウン状態と宣言されるまでの時間

hellotime のデフォルトは、ホットスタンバイ ルータ プロトコル（HSRP）に合わせるために 3 秒です。また、holdtime のデフォルトは 10 秒です。 また、**timers hellotime msec** コマンドを使用して、これらのタイマーをミリ秒単位で設定することもできます。

スイッチオーバーの影響を受けるインターフェイスのペアを判断するには、冗長インターフェイスの各ペアについて、固有の ID 番号を設定する必要があります。 この ID 番号は RII と呼ばれ、インターフェイスに関連付けられています。

また、スタンバイ ルータに対するスイッチオーバーは、他の条件でも発生する可能性があります。 スイッチオーバーが発生する別の要因として、各ルータで設定可能な優先順位設定があります。 最も優先度が高いルータがアクティブ ルータになります。 アクティブ ルータまたはスタン

バイ ルータで障害が発生した場合、重みと呼ばれる設定可能な数値分、ルータの優先度が減らされます。 アクティブ ルータの優先度が、スタンバイ ルータの優先度を下回る場合、スイッチオーバーが発生し、スタンバイ ルータがアクティブ ルータになります。 このデフォルトの動作を無効にするには、冗長グループについて preemption 属性をディセーブルにします。 また、インターフェイスのL1状態がダウン状態になった場合、各インターフェイスを設定して優先度を減らします。 この数は、冗長グループに設定されているデフォルトの値よりも優先されます。

冗長グループの優先度が変更されるエラーイベントごとに、タイムスタンプ、影響を受けた冗長グループ、以前の優先度、新しい優先度、およびエラー イベントの原因の説明を含む syslog エントリが生成されます。

スイッチオーバーが発生する原因となるもう 1 つの状況は、ルータまたはインターフェイスの優先度が、設定可能なしきい値レベルを下回る場合です。

一般的に、スタンバイ ルータへのスイッチオーバーは次の条件で発生します。

- アクティブ ルータで停電またはリロードが発生した場合（クラッシュも含まれます）。
- アクティブ ルータのランタイム優先度が、スタンバイ ルータの優先度を下回った場合。
- アクティブ ルータのランタイム優先度が、設定したしきい値を下回った場合。
- 、**redundancy application reload group** *rg-number* コマンドを使用して、アクティブ ルータの冗長グループを手動でリロードした場合。
- 任意のモニタ対象インターフェイスで 2 つの連続する hello メッセージに失敗し、インターフェイスが強制的にテスト モードになった場合。 この問題が発生すると、いずれのユニットもまずインターフェイス上のリンク ステータスを確認してから、次のテストを実行します。
  - ネットワーク アクティビティ テスト
  - ARP テスト
  - ブロードキャスト ping テスト

ファイアウォール ステートフル シャーシ間冗長性機能では、冗長グループのトラフィックは、冗長グループの入力インターフェイスに関連付けられた仮想 IP アドレスによりルーティングされます。 仮想IPアドレスに送信されるトラフィックは、アクティブ状態の冗長グループを持つルータによって受信されます。 冗長グループのフェールオーバー中に、仮想IPアドレスへのトラフィックは新しいアクティブ冗長グループに自動的にルーティングされます。

ファイアウォールは、冗長グループのトラフィックがスタンバイ ルータの物理IPアドレスにルーティングされ、トラフィックがスタンバイ冗長グループに到達した場合は、スタンバイ冗長グループに到達したトラフィックをドロップします。 ただし、トラフィックがアクティブな冗長グループに到達した場合、確立された TCP セッションまたは UDP セッションはスタンバイ冗長グループに同期されます。

排他的仮想 IP アドレスと排他的仮想 MAC アドレス

仮想IP（VIP）アドレスと仮想MAC（VMAC）アドレスは、セキュリティ アプリケーションが、トラフィックを受信するインターフェイスを制御するために使用します。 インターフェイスは、別のインターフェイスとペアになり、これらのインターフェイスは同じ冗長グループ（RG）に関連付けられます。 アクティブ RG に関連付けられたインターフェイスは、VIP と VMAC を排他的に所有します。 アクティブ デバイスのアドレス解決プロトコル（ARP）プロセスによって、VIP への ARP 要求に対する ARP 応答が送信されます。また、インターフェイスのイーサネット コントローラは、VMACを宛先とするパケットを受信するようにプログラミングされます。RGフェールオーバーが発生した場合、VIP と VMACの所有権が変更されます。 新しくアクティブになった RG に関連付けられたインターフェイスは、Gratuitous ARP を送信し、インターフェイスのイーサネット コントローラを、VMAC を宛先とするパケットを受け入れるようにプログラミングします。

IPv6 サポート

各冗長グループ（RG）を、IPv4 と IPv6の両方の仮想IP（VIP）アドレスのトラフィック インターフェイスに同じ冗長インターフェイス識別子（RII）で割り当てることができます。 各 RG は RII ごとに一意の仮想MAC（VMAC）アドレスを使用します。 RG では、IPv6 リンクローカル VIP とグローバル VIP がインターフェイス上に共存します。

トラフィック インターフェイス上の各 RG に対して IPv4 VIP、リンクローカル IPv6 VIP、および/またはグローバル IPv6 VIP を設定できます。 IPv6 リンクローカル VIP は、スタティック ルートまたはデフォルト ルートを設定する場合に主に使用され、一方、IPv6 グローバル VIP は、LAN トポロジと WAN トポロジの両方で広く使用されています。

IPv4 VIP を設定する前に、物理 IP アドレスを設定する必要があります。

サポートされるトポロジ

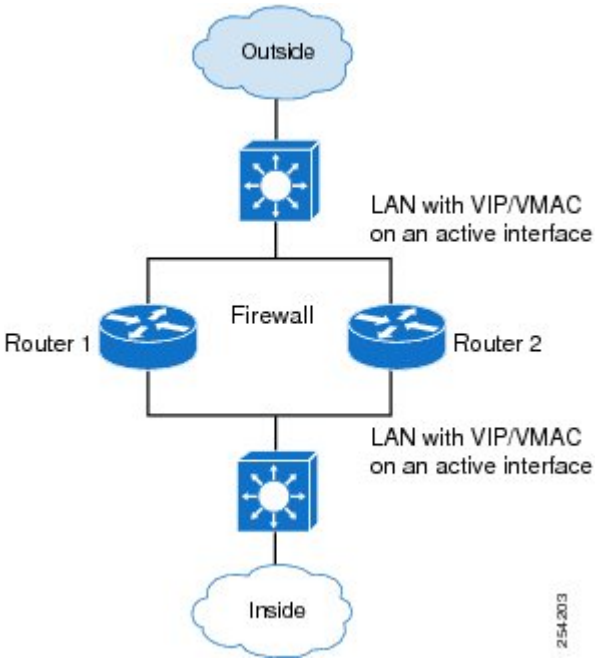
LAN-LANトポロジは、ファイアウォール ステートフル シャーシ間冗長性アーキテクチャでサポートされます。

（注） 非対称ルーティングはサポートされません。

LAN/LAN

下の図は、LAN-LANトポロジを示しています。 専用のアプリケーションベースのファイアウォール ソリューションを使用するときに、アップストリームまたはダウンストリームルータから適切な仮想IPアドレスへのスタティック ルーティングを設定することで、多くの場合、トラフィックは適切なファイアウォールに送信されます。 さらに、アグリゲーション サービス ルータ（ASR）は、アップストリームまたはダウンストリームルータとのダイナミック ルーティングに参加します。 LAN 方向のインターフェイスでサポートされるダイナミック ルーティング構成では、ルー

ティング プロトコルのコンバージェンスへの依存が生じないようにしてください。依存があると、高速フェールオーバー要件に適合しなくなります。



LAN-LAN コンフィギュレーションの詳細については、「LAN-LAN の設定例」の項を参照してください。

ファイアウォールステートフルシャーシ間冗長性の設定方法

冗長アプリケーション グループの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*
7. **shutdown**
8. **priority** *value* [**failover threshold** *value*]
9. **preempt**
10. **track** *object-number* {**decrement** *value* | **shutdown**}
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-grp)# name group1`	（任意）プロトコル インスタンスに任意のエイリアスを指定します。
ステップ 7	**shutdown** 例： `Device(config-red-app-grp)# shutdown`	（任意）冗長グループを手動でシャットダウンします。
ステップ 8	**priority** *value* [**failover threshold** *value*] 例： `Device(config-red-app-grp)# priority 100 failover threshold 50`	（任意）冗長グループの初期優先度とフェールオーバーしきい値を指定します。
ステップ 9	**preempt** 例： `Device(config-red-app-grp)# preempt`	グループでプリエンプションをイネーブルにし、優先度に関係なく、スタンバイ デバイスがアクティブ デバイスをプリエンプション処理できるようにします。
ステップ 10	**track** *object-number* {**decrement** *value* | **shutdown**} 例： `Device(config-red-app-grp)# track 200 decrement 200`	冗長グループの優先度を指定します。この値は、イベントが発生した場合に減らされます。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

冗長グループ プロトコルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **protocol** *id*
6. **name** *group-name*
7. **timers hellotime** {*seconds* | **msec** *milliseconds*} **holdtime** {*seconds* | **msec** *milliseconds*}
8. **authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key-string* **timeout** *seconds* | **key-chain** *key-chain-name*}
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーションモードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**protocol** *id* 例： `Device(config-red-app)# protocol 1`	コントロール インターフェイスに接続されるプロトコル インスタンスを指定し、冗長アプリケーション プロトコル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**name** *group-name* 例： `Device(config-red-app-prtcl)# name prot1`	（任意）名前を使用して冗長グループ（RG）を設定します。
ステップ 7	**timers hellotime** {*seconds* | **msec** *milliseconds*} **holdtime** {*seconds* | **msec** *milliseconds*} 例： `Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9`	helloメッセージが送信される間隔と、デバイスがダウン状態と宣言されるまでの時間を指定します。
ステップ 8	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key-string* **timeout** *seconds* | **key-chain** *key-chain-name*} 例： `Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100`	認証情報を指定します。
ステップ 9	**end** 例： `Device(config-red-app-prtcl)# end`	冗長アプリケーションプロトコルコンフィギュレーションモードを終了し、特権EXECモードを開始します。

仮想 IP アドレスと冗長インターフェイス識別子の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **redundancy rii** *id*
5. **redundancy group** *id* **ip** *address* **exclusive** [**decrement** *value*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface GigabitEthernet 0/1/1`	インターフェイスの名前と番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**redundancy rii** *id* 例： `Router(config-if)# redundancy rii 600`	冗長グループ用に冗長インターフェイス識別子を設定します。 • 有効な範囲は 1 ～ 65535 です。
ステップ 5	**redundancy group** *id* **ip** *address* **exclusive** [**decrement** *value*] 例： `Router(config-if)# redundancy group 1 ip 10.10.1.1 exclusive decrement 20`	グループの *id* 引数によって識別される冗長グループにインターフェイスを関連付けます。
ステップ 6	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

コントロール インターフェイスおよびデータ インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **data** *interface-type interface-number*
7. **control** *interface-type interface-number* **protocol** *id*
8. **timers delay** *seconds* [**reload** *seconds*]
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長アプリケーション グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**data** *interface-type interface-number* 例： `Device(config-red-app-grp)# data GigabitEthernet 0/0/0`	冗長グループに使用されるデータ インターフェイスを指定します。
ステップ 7	**control** *interface-type interface-number* **protocol** *id* 例： `Device(config-red-app-grp)# control gigabitethernet 0/0/2 protocol 1`	冗長グループに使用されるコントロール インターフェイスを指定します。 • このインターフェイスは、コントロール インターフェイス プロトコルのインスタンスにも関連付けられます。
ステップ 8	**timers delay** *seconds* [**reload** *seconds*] 例： `Device(config-red-app-grp)# timers delay 100 reload 400`	障害の発生後、またはシステムのリロード後に起動するロールのネゴシエートを遅らせるために、冗長グループが待機する時間を指定します。
ステップ 9	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォール ステートフル シャーシ間冗長性の管理とモニタリング

ファイアウォール ステートフル シャーシ間冗長性機能を管理およびモニタするには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **debug redundancy application group config** {**all**| **error** | **event** | **func**}
3. **debug redundancy application group faults** {**all** | **error** | **event** | **fault** | **func**}
4. **debug redundancy application group media** {**all** | **error** | **event** | **nbr** | **packet**{**rx** | **tx**} | **timer**}
5. **debug redundancy application group protocol** {**all** | **detail** | **error** | **event** | **media** | **peer**}
6. **debug redundancy application group rii** {**error** | **event**}
7. **debug redundancy application group transport** {**db** | **error** | **event** | **packet** | **timer** | **trace**}
8. **debug redundancy application group vp** {**error** | **event**}
9. **show redundancy application group** [*group-id* | **all**]
10. **show redundancy application transport** {**client** | **group** [*group-id*]}
11. **show redundancy application control-interface group** [*group-id*]
12. **show redundancy application faults group** [*group-id*]
13. **show redundancy application protocol** {*protocol-id* | **group** [*group-id*]
14. **show redundancy application if-mgr group** [*group-id*]
15. **show redundancy application data-interface group** [*group-id*]
16. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug redundancy application group config** {**all**	**error**	**event**	**func**} 例： `Router# debug redundancy application group config all`	冗長グループ アプリケーションの設定を表示します。
ステップ 3	**debug redundancy application group faults** {**all**	**error**	**event**	**fault**	**func**} 例： `Router# debug redundancy application group faults error`	冗長グループ アプリケーションの障害を表示します。

	コマンドまたはアクション	目的
ステップ 4	**debug redundancy application group media** {**all** | **error** | **event** | **nbr** | **packet**{**rx** | **tx**} | **timer**} 例： `Router# debug redundancy application group media timer`	冗長グループ アプリケーションのグループ メディア情報を表示します。
ステップ 5	**debug redundancy application group protocol** {**all** | **detail** | **error** | **event** | **media** | **peer**} 例： `Router# debug redundancy application group protocol peer`	冗長グループ アプリケーションのグループ プロトコル情報を表示します。
ステップ 6	**debug redundancy application group rii** {**error** | **event**} 例： `Router# debug redundancy application group rii event`	冗長グループ アプリケーションのグループ RII 情報を表示します。
ステップ 7	**debug redundancy application group transport** {**db** | **error** | **event** | **packet** | **timer** | **trace**} 例： `Router# debug redundancy application group transport trace`	冗長グループ アプリケーションのグループ トランスポート情報を表示します。
ステップ 8	**debug redundancy application group vp** {**error** | **event**} 例： `Router# debug redundancy application group vp event`	冗長グループ アプリケーションのグループ VP 情報を表示します。
ステップ 9	**show redundancy application group** [*group-id* | **all**] 例： `Router# show redundancy application group all`	冗長グループ情報を表示します。
ステップ 10	**show redundancy application transport** {**client** | **group** [*group-id*]} 例： `Router# show redundancy application transport group 1`	冗長グループのトランスポート固有の情報を表示します。

	コマンドまたはアクション	目的
ステップ 11	**show redundancy application control-interface group** [*group-id*] 例： `Router# show redundancy application control-interface group 2`	冗長グループのコントロール インターフェイス情報を表示します。
ステップ 12	**show redundancy application faults group** [*group-id*] 例： `Router# show redundancy application faults group 2`	冗長グループの障害固有の情報を表示します。
ステップ 13	**show redundancy application protocol** {*protocol-id* | **group** [*group-id*] 例： `Router# show redundancy application protocol 3`	冗長グループのプロトコル固有の情報を表示します。
ステップ 14	**show redundancy application if-mgr group** [*group-id*] 例： `Router# show redundancy application if-mgr group 2`	冗長グループのインターフェイスマネージャ情報を表示します。
ステップ 15	**show redundancy application data-interface group** [*group-id*] 例： `Router# show redundancy application data-interface group 1`	データ インターフェイス固有の情報を表示します。
ステップ 16	**end** 例： `Router# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ファイアウォールステートフルシャーシ間冗長性の設定例

例：冗長アプリケーション グループの設定

次に、優先度とプリエンプション属性を使用する group1 という冗長グループを設定する例を示します。

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name group1
Device(config-red-app-grp)# priority 100 failover-threshold 50
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# track 200 decrement 200
Device(config-red-app-grp)# end
```

例：冗長グループ プロトコルの設定

次に、helloタイムおよびホールドタイムメッセージ用にタイマーが設定されている冗長グループを設定する例を示します。

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9
Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100
Device(config-red-app-prtcl)# bfd
Device(config-red-app-prtcl)# end
```

仮想 IP アドレスと冗長インターフェイス識別子の設定例

次に、ギガビット イーサネット インターフェイス 0/0/0 の冗長グループ仮想 IP アドレスを設定する例を示します。

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1/1
Router(conf-if)# redundancy rii 600
Router(config-if)# redundancy group 2 ip 10.2.3.4 exclusive decrement 200
Router(config)# redundancy
Router(config-red-app-grp)# data GigabitEthernet0/0/0
Router(config-red-app-grp)# control GigabitEthernet0/0/2 protocol 1
```

例：コントロール インターフェイスおよびデータ インターフェイスの設定

```
Device# configure terminal
Device(config-red)# application redundancy
Device(config-red-app-grp)# group 1
Device(config-red-app-grp)# data GigabitEthernet 0/0/0
Device(config-red-app-grp)# control GigabitEthernet 0/0/2 protocol 1
Device(config-red-app-grp)# timers delay 100 reload 400
Device(config-red-app-grp)# end
```

LAN-LAN の設定例

次のサンプル LAN-LAN コンフィギュレーションでは、2 つの発信インターフェイスを持つ ASR ルータのペアが設定される方法を示します。 この例では、GigabitEthernet0/1 は入力インターフェイスであり、GigabitEthernet0/2 は出力インターフェイスです。 両方のインターフェイスがゾーンに割り当てられ、ゾーン間のトラフィックを記述するためにクラスマップが定義されます。 インターフェイスは、冗長性用としても設定されます。「inspect」アクションにより、アプリケーション レベル ゲートウェイ（ALG）が起動され、他のポートのトラフィックを許可するためのピンホールが開きます。 ALG ピンホールは、保護されたネットワークに対する制御アクセスを特定のアプリケーションが取得できるようにするために、ALG に開かれたポートです。

```
! Identifies and defines network zones
  zone security zone1
  zone security zone2
!
! Assigns interfaces to zones
  interface GigabitEthernet0/1
  zone-member security zone1
interface GigabitEthernet0/2
zone-member security zone2
!
! Defines class-maps to describes traffic between zones
  class-map type inspect match-any inter-zone-class-map
  match access-group 1
  access-list 1 permit 10.1.1.1
!
! Associates class-maps with policy-maps to define actions to be applied
  policy-map type inspect inter-zone-policy-map
  class type inspect inter-zone-class-map
  inspect
!
! Sets zone pairs for any policy other than deny all and assign policy-maps to zone-pairs
by defining service-policy
  zone-pair inter-zone source zone1 destination zone2
  service-policy type inspect inter-zone-policy-map
!
```

ファイアウォールステートフルシャーシ間冗長性の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールステートフルシャーシ間冗長性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 7：ファイアウォール ステートフル シャーシ間冗長性の機能情報

機能名	リリース	機能情報
ファイアウォール ステートフル シャーシ間冗長性	Cisco IOS XE Release 3.1(S)	ファイアウォール ステートフル シャーシ間冗長性機能を使用すると、相互にバックアップとして動作するルータのペアを設定できます。 次のコマンドが導入または変更されました。**application redundancy**、**authentication**、**control**、**data**、**debug redundancy application group config**、**debug redundancy application group faults**、**debug redundancy application group media**、**debug redundancy application group protocol**、**debug redundancy application group rii**、**debug redundancy application group transport**、**debug redundancy application group vp**、**group**、**name**、**preempt**、**priority**、**protocol**、**redundancy rii**、**redundancy group**、**track**、**timers delay**、**timers hellotime**、**show redundancy application group**、**show redundancy application transport**、**show redundancy application control-interface**、**show redundancy application faults**、**show redundancy application protocol**、**show redundancy application if-mgr**、**show redundancy application data-interface**。

第 6 章

IPv6 ゾーンベース ファイアウォールのボックスツーボックスハイアベイラビリティサポート

IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポート機能は、IPv6 ファイアウォールでの冗長グループ（RG）に基づいたハイ アベイラビリティ（HA）をサポートします。 この機能により、デバイスのペアが互いのバックアップとして動作するように設定できます。 この機能を設定し、複数のフェールオーバー条件に基づいてアクティブ デバイスを判断できます。 この機能は、IPv6 パケット インスペクションの FTP66 アプリケーション層ゲートウェイ（ALG）をサポートしています。

このモジュールでは、ボックスツーボックス（B2B）HA サポートに関する情報を提供し、この機能を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポートの前提条件

- ファイアウォールに接続しているインターフェイスは、同じ冗長インターフェイス識別子（RII）を持つ必要があります。
- アクティブ デバイスとスタンバイ デバイスは、同じゾーンベース ポリシー ファイアウォール コンフィギュレーションである必要があります。
- アクティブ デバイスとスタンバイ デバイスは、同じバージョンの Cisco ソフトウェアで実行する必要があります。 アクティブ デバイスとスタンバイ デバイスは、スイッチを介して接続する必要があります。
- アクティブ デバイスとスタンバイ デバイス間のコンフィギュレーションは自動同期されないため、これらの両方のデバイス上のボックスツーボックス（B2B）コンフィギュレーションは同じである必要があります。
- 非対称ルーティング トラフィックを渡すには、class-default クラスの pass アクションを設定する必要があります。 class-default クラスは、ポリシーのいずれのユーザ定義クラスとも一致しないすべてのパケットを表すシステム定義クラス マップです。
- 2 つの LAN インターフェイス間にゾーン ペアを設定する場合は、両方のインターフェイスに同じ冗長グループ（RG）を必ず設定してください。 ゾーン ペア コンフィギュレーションは、LAN インターフェイスが異なる RG に属している場合はサポートされません。

IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポートの制約事項

- ボックスツーボックス（B2B）インターリンク インターフェイスでは、IPv4 だけがサポートされています。

- マルチプロトコル ラベル スイッチング（MPLS）と、仮想ルーティングおよび転送（VRF）はサポートされません。
- デュアル組み込みサービス プロセッサ（ESP）またはデュアル ルート プロセッサ（RP）がシャーシに含まれている Cisco ASR 1006 および 1013 アグリゲーション サービス ルータは、ボックス間ハイ アベイラビリティ（HA）およびボックス内 HA がサポートされていないため、サポートされていません。

  単一の ESP および単一の RP がシャーシに含まれている Cisco ASR 1006 および Cisco ASR 1013 アグリゲーション サービス ルータは、シャーシ間冗長をサポートします。
- デュアル IOS デーモン（IOSd）が設定されている場合、デバイスはファイアウォール ステートフル シャーシ間冗長構成をサポートしません。
- IPv6 ファイアウォールでのステートレスなネットワーク アドレス変換 64（NAT64）はサポートされません。

IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポートについて

ゾーンベース ポリシー ファイアウォール ハイ アベイラビリティの概要

ハイ アベイラビリティ（HA）により、ネットワークのいかなる部分で発生した障害からも高速回復でき、ネットワーク規模での保護が可能になります。 HA により、ユーザやネットワーク アプリケーションに対する中断からの迅速なリカバリが可能になります。

ゾーンベース ポリシー ファイアウォールは、アクティブ/アクティブとアクティブ/スタンバイの HA フェールオーバーおよび非対称ルーティングをサポートします。

アクティブ/アクティブ フェールオーバーにより、フェールオーバーに関連する両方のデバイスが、トラフィックを同時に転送できます。

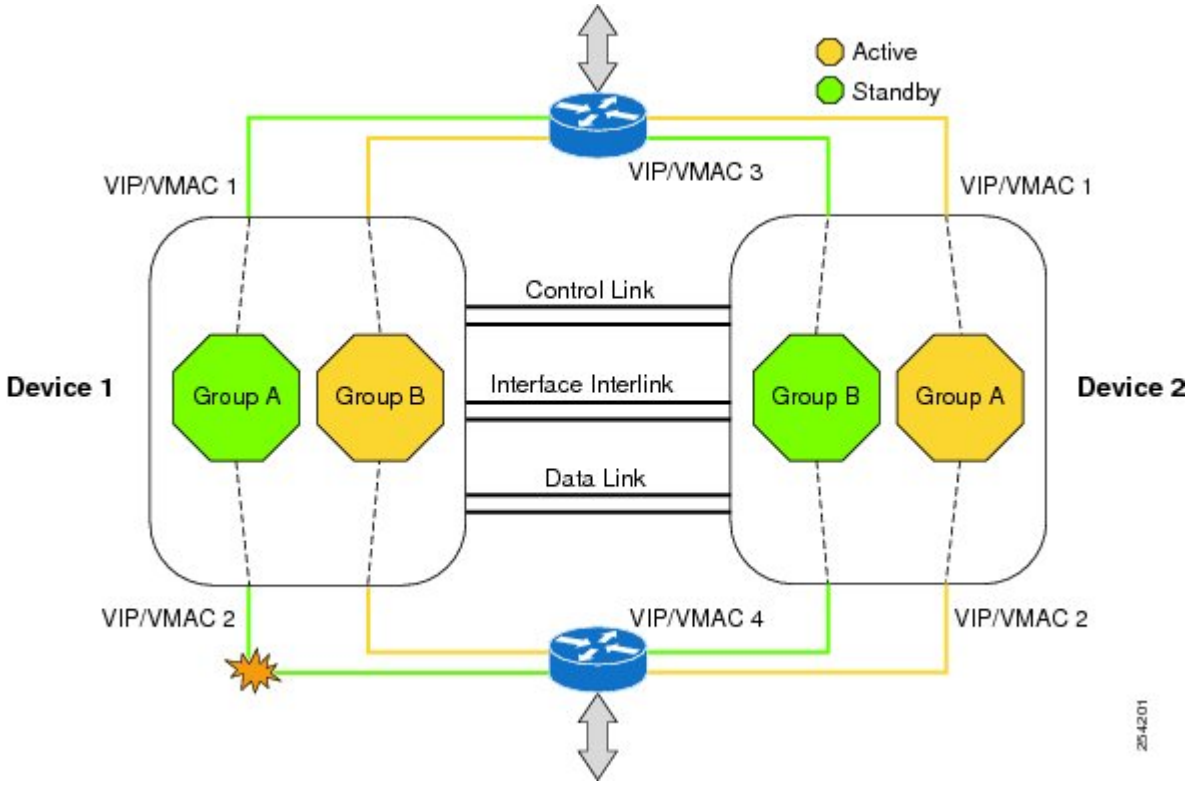
アクティブ/スタンバイ HA フェールオーバーが設定されている場合、フェールオーバーに関連する 1 つのデバイスのみがトラフィックを一度処理し、他のデバイスがスタンバイ モードになり、定期的にアクティブ デバイスからのセッション情報を同期します。

非対称ルーティングは、パケット処理のために、スタンバイ冗長グループからのパケットをアクティブな冗長グループに転送することをサポートします。 この機能がイネーブルでない場合、初期同期（SYN）メッセージを受信しなかったデバイスに転送されたリターン TCP パケットは、既存で既知のいずれのセッションにも属していないため、ドロップされます。

ボックスツーボックス ハイ アベイラビリティの動作

相互にホット スタンバイとして動作するようにデバイスのペアを設定できます。 冗長性はインターフェイスごとに設定します。 冗長インターフェイスのペアは、冗長グループ（RG）と呼ばれます。 図 1 は、アクティブ/アクティブ フェールオーバー シナリオを示しています。 2 つの発信インターフェイスを持つデバイス ペアに対して 2 つの冗長グループがどのように設定されているかを示します。

図 *13*： 冗長グループの設定：*2* つの発信インターフェイス



冗長デバイスは、設定可能なコントロール リンク、データ同期リンク、およびインターリンク インターフェイスによって参加します。 コントロール リンクは、デバイスのステータスを通信するために使用されます。 データ同期リンクは、ステートフル情報をファイアウォールから転送し、ステートフルデータベースを同期するために使用されます。 冗長インターフェイスのペアは、同じ固有 ID 番号（冗長インターフェイス識別子（RII）と呼ばれます）で設定されます。 ルーティング テーブルは、アクティブからスタンバイに同期されません。

非対称ルーティングはファイアウォールHAの一部としてサポートされます。 リターントラフィックがスタンバイ デバイスに入る LAN-WAN シナリオでは、非対称ルーティングがサポートされます。 非対称ルーティング機能を実装するには、非対称トラフィックの専用インターフェイス（インターリンク インターフェイス）で両方の冗長デバイスを設定します。 この専用インターフェイ

スは、スタンバイ WAN インターフェイスに着信するトラフィックを、アクティブ デバイスにリダイレクトします。

冗長グループ メンバーのステータスは、コントロール リンクで送信される hello メッセージを使用することで判断できます。 いずれかのデバイスが、設定された時間内に hello メッセージに応答しないと、ソフトウェアは障害が発生したと見なし、スイッチオーバーが開始されます。 ミリ秒単位で障害を検出するには、コントロール リンクでフェールオーバー プロトコルを実行します。 hello メッセージについて次のパラメータを設定できます。

- Active timer。
- Standby timer。
- Hello time：hello メッセージが送信される間隔。
- Hold time：アクティブ デバイスまたはスタンバイ デバイスがダウン状態と宣言されるまでの時間。

hello タイムのデフォルトは、ホットスタンバイ ルータ プロトコル（HSRP）に合わせるために 3 秒です。また、ホールドタイムのデフォルトは 10 秒です。 また、**timers hellotime msec** コマンドを使用して、これらのタイマーをミリ秒単位で設定することもできます。

スイッチオーバーの影響を受けるインターフェイスのペアを判断するには、冗長インターフェイスの各ペアについて、固有の ID を設定する必要があります。 この ID は、インターフェイスに関連付けられた RII です。

スイッチオーバーの理由

スイッチオーバーが発生する別の要因として、各デバイスで設定可能な優先順位設定があります。最も優先度が高いデバイスがアクティブ デバイスになります。 アクティブ デバイスまたはスタンバイ デバイスで障害が発生した場合、重みと呼ばれる設定可能な数値分、デバイスの優先度が減らされます。 アクティブ デバイスの優先度が、スタンバイ デバイスの優先度を下回る場合、スイッチオーバーが発生し、スタンバイ デバイスがアクティブデバイスになります。 このデフォルトの動作を無効にするには、冗長グループについて preemption 属性をディセーブルにします。また、各インターフェイスについて、インターフェイスのレイヤ 1 状態がダウン状態になった場合に優先度が低下するように設定できます。 設定された優先度が、冗長グループのデフォルトの優先度を上書きします。

冗長グループの優先度が変更されるエラーイベントごとに、タイムスタンプ、影響を受けた冗長グループ、以前の優先度、新しい優先度、およびエラー イベントの原因の説明を含む syslog エントリが生成されます。

スイッチオーバーが発生する原因となるもう 1 つの状況は、デバイスまたはインターフェイスの優先度が、設定可能なしきい値レベルを下回る場合です。

スタンバイ デバイスへのスイッチオーバーは、次の状況で発生します。

- アクティブ デバイスで停電またはリロードが発生した場合（クラッシュも含まれます）。
- アクティブデバイスのランタイム優先度が、スタンバイデバイスの優先度を下回った場合。
- アクティブ デバイスのランタイム優先度が、設定したしきい値を下回った場合。

- アクティブ デバイスの冗長グループを手動でリロードするには、**redundancy application reload group** *rg-number* コマンドを使用します。
- 任意のモニタ対象インターフェイスで 2 つの連続する hello メッセージに失敗した場合、インターフェイスは強制的にテスト モードになります。 両方のデバイスが、インターフェイス上のリンク ステータスを確認してから、次のテストを実行します。
  - ネットワーク アクティビティ テスト
  - アドレス解決プロトコル（ARP）テスト
  - ブロードキャスト ping テスト

アクティブ/アクティブ フェールオーバー

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方のデバイスがネットワーク トラフィックを処理できます。 アクティブ/アクティブ フェールオーバーでは、各冗長グループ（RG）のインターフェイスに仮想 MAC（VMAC）アドレスを生成します。

アクティブ/アクティブ フェールオーバー ペアの 1 台のデバイスがプライマリ（アクティブ）デバイスとして指定され、もう一方はセカンダリ（スタンバイ）デバイスとして指定されます。 アクティブ/スタンバイ フェールオーバーとは異なり、この割り当ては、両方のデバイスが同時に起動した場合にどちらのデバイスがアクティブになるかということを示しているわけではありません。 代わりに、プライマリ/セカンダリの割り当てでは、次のことが決定されます。

- フェールオーバー ペアが同時に起動した場合、フェールオーバー ペアに実行コンフィギュレーションを提供するデバイス。
- デバイスが同時に起動した場合、フェールオーバー RG がアクティブ状態で表示されるデバイス。 コンフィギュレーション内の各フェールオーバー RG がプライマリかセカンダリのデバイス プリファレンスに設定されます。 両方のフェールオーバー RG を単一デバイス上でアクティブ状態に設定し、スタンバイ フェールオーバー RG を他のデバイス上に設定できます。 単一デバイス上で、1 つのフェールオーバー RG をアクティブ状態に設定し、他の RG をスタンバイ状態に設定できます。

Active/Standby フェールオーバー

アクティブ/スタンバイ フェールオーバーでは、スタンバイ デバイスを使用して、障害の発生したデバイスの機能を引き継ぐことができます。障害が発生したアクティブデバイスはスタンバイ状態になり、スタンバイデバイスがアクティブ状態になります。アクティブ状態になったデバイスは、障害が発生したデバイスの IP アドレスと MAC アドレスを引き継いで、トラフィックの処理を開始します。 スタンバイ状態になったデバイスは、スタンバイ IP アドレスと MAC アドレスを受け継ぎます。ネットワークデバイスはMAC-to-IPアドレスペアでの変更を確認しないため、アドレス解決プロトコル（ARP）エントリはネットワーク上のいずれの場所でも変更されず、タイムアウトしません。

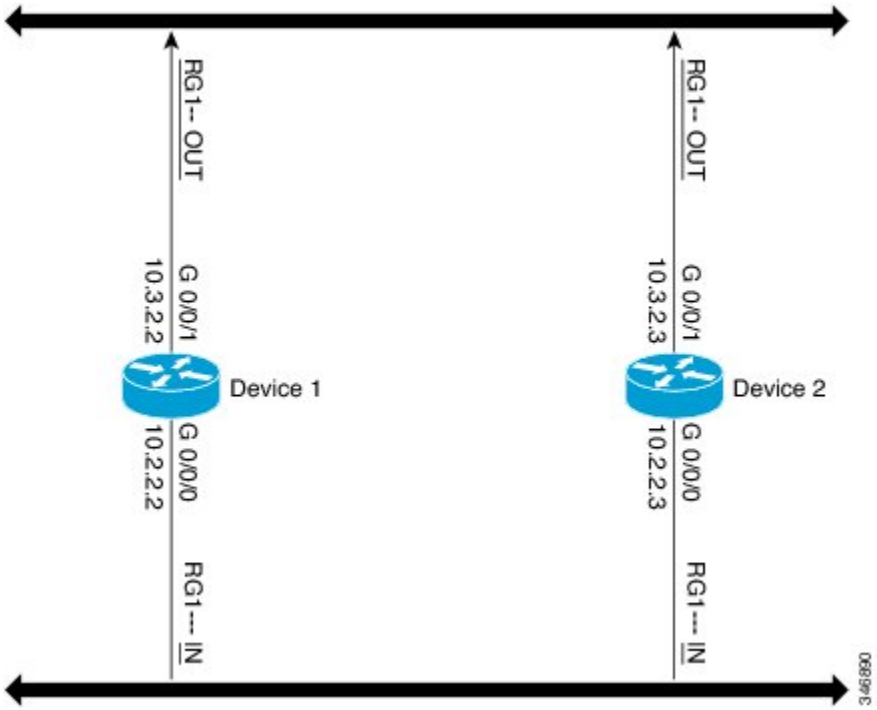
アクティブ/スタンバイ シナリオの場合、フェールオーバー ペアの 2 台のデバイス間の主な違いは、どのデバイスがアクティブで、どのデバイスがスタンバイであるか、つまり、どの IP アドレスを使用し、どのデバイスがアクティブにトラフィックを渡すかということに関連します。 両方のデバイスが同時に起動した場合（さらに動作ヘルスが等しい場合）、アクティブ デバイスが常にアクティブ デバイスになります。 アクティブ デバイスの MAC アドレスは、アクティブな IP アドレスと常に組み合わされます。

NAT ボックスツーボックス ハイ アベイラビリティ LAN-LAN トポロジ

LAN-LAN トポロジでは、参加するすべてのデバイスが、内部と外部両方の LAN インターフェイスを介して相互に接続されます。 下の図は、NAT ボックスツーボックス LAN-LAN トポロジを示しています。 ネットワーク アドレス変換（NAT）は、アクティブ/スタンバイ モードであり、ピアは1つの冗長グループ（RG）にあります。すべてのトラフィックまたはこのトラフィックのサブセットは、NAT 変換を実行します。

（注） フェールオーバーは、RG インフラストラクチャがリッスンするこれらの障害のみが原因で発生します。

図 *14*： *NAT* ボックスツーボックス ハイ アベイラビリティ *LAN-LAN* トポロジ



WAN-LAN トポロジ

WAN-LAN トポロジでは、2 台のデバイスが内部の LAN インターフェイスおよび外部の WAN インターフェイスを介して接続されます。 WAN リンク経由で受信したリターン トラフィックのルーティングに対する制御は行われません。

WAN リンクは、同じサービス プロバイダーまたは異なるサービス プロバイダーから提供されます。 ほとんどの場合、WAN リンクは異なるサービス プロバイダーから提供されます。 WAN リンクを最大限利用するには、フェールオーバーを提供するように外部デバイスを設定します。

排他的仮想 IP アドレスと排他的仮想 MAC アドレス

仮想IP（VIP）アドレスと仮想MAC（VMAC）アドレスは、セキュリティアプリケーションが、トラフィックを受信するインターフェイスを制御するために使用します。 インターフェイスは、別のインターフェイスとペアになり、これらのインターフェイスは同じ冗長グループ（RG）に関連付けられます。 アクティブ RG に関連付けられたインターフェイスは、VIP と VMAC を排他的に所有します。 アクティブ デバイスのアドレス解決プロトコル（ARP）プロセスによって、VIP への ARP 要求に対する ARP 応答が送信されます。また、インターフェイスのイーサネット コントローラは、VMACを宛先とするパケットを受信するようにプログラミングされます。RGフェールオーバーが発生した場合、VIP と VMAC の所有権が変更されます。 新しくアクティブになった RG に関連付けられたインターフェイスは、Gratuitous ARP を送信し、インターフェイスのイーサネット コントローラを、VMAC を宛先とするパケットを受け入れるようにプログラミングします。

IPv6 サポート

各冗長グループ（RG）を、IPv4 と IPv6 の両方の仮想IP（VIP）アドレスのトラフィック インターフェイスに同じ冗長インターフェイス識別子（RII）で割り当てることができます。 各 RG は RII ごとに一意の仮想MAC（VMAC）アドレスを使用します。 RG では、IPv6 リンクローカル VIP とグローバル VIP がインターフェイス上に共存します。

トラフィック インターフェイス上の各 RG に対して IPv4 VIP、リンクローカル IPv6 VIP、および/またはグローバル IPv6 VIP を設定できます。 IPv6 リンクローカル VIP は、スタティック ルートまたはデフォルト ルートを設定する場合に主に使用され、一方、IPv6 グローバル VIP は、LAN トポロジと WAN トポロジの両方で広く使用されています。

IPv4 VIP を設定する前に、物理 IP アドレスを設定する必要があります。

FTP66 ALG サポートの概要

ファイアウォールは、IPv6パケットおよびステートフル ネットワーク アドレス変換64（NAT64）のインスペクションをサポートします。 IPv6 パケット インスペクションにおいて FTP が機能するには、アプリケーション層ゲートウェイ（ALG）（アプリケーション レベル ゲートウェイ（ALG）とも呼ばれます）、FTP66 が必要となります。 FTP66 ALG は、オールインワン FTP ALG および 1 つの FTP ALG とも呼ばれます。

FTP66 ALG は次のことをサポートします。

- ファイアウォール IPv4 パケット インスペクション
- ファイアウォール IPv6 パケット インスペクション
- NAT 設定
- NAT64 設定（FTP64 サポートとともに）
- NAT およびファイアウォール設定
- NAT64 およびファイアウォール設定

FTP66 ALG には次のセキュリティ脆弱性があります。

- パケットセグメンテーション攻撃：FTP ALG ステートマシンは、セグメント化されたパケットを検出でき、ステート マシンの処理は、完全なパケットを受信するまで停止します。
- バウンス攻撃：FTP ALG は、1024 より少ないデータ ポート番号を使用して（NAT 用の）ドアまたは（ファイアウォール用の）ピンホールを作成しません。 バウンス攻撃の防止は、ファイアウォールがイネーブルな場合にのみアクティブです。

IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポートの設定方法

冗長グループ プロトコルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **protocol** *id*
6. **name** *group-name*
7. **timers hellotime** {*seconds* | **msec** *milliseconds*} **holdtime** {*seconds* | **msec** *milliseconds*}
8. **authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key-string* **timeout** *seconds* | **key-chain** *key-chain-name*}
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**protocol** *id* 例： `Device(config-red-app)# protocol 1`	コントロール インターフェイスに接続されるプロトコル インスタンスを指定し、冗長アプリケーション プロトコル コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-prtcl)# name prot1`	（任意）名前を使用して冗長グループ（RG）を設定します。
ステップ 7	**timers hellotime** {*seconds* | **msec** *milliseconds*} **holdtime** {*seconds* | **msec** *milliseconds*} 例： `Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9`	hello メッセージが送信される間隔と、デバイスがダウン状態と宣言されるまでの時間を指定します。
ステップ 8	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key-string* **timeout** *seconds* | **key-chain** *key-chain-name*} 例： `Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100`	認証情報を指定します。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-red-app-prtcl)# end`	冗長アプリケーションプロトコル コンフィギュレーション モードを終了し、特権EXECモードを開始します。

冗長アプリケーション グループの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*
7. **shutdown**
8. **priority** *value* [**failover threshold** *value*]
9. **preempt**
10. **track** *object-number* {**decrement** *value* | **shutdown**}
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-grp)# name group1`	（任意）プロトコル インスタンスに任意のエイリアスを指定します。
ステップ 7	**shutdown** 例： `Device(config-red-app-grp)# shutdown`	（任意）冗長グループを手動でシャットダウンします。
ステップ 8	**priority** *value* [**failover threshold** *value*] 例： `Device(config-red-app-grp)# priority 100 failover threshold 50`	（任意）冗長グループの初期優先度とフェールオーバーしきい値を指定します。
ステップ 9	**preempt** 例： `Device(config-red-app-grp)# preempt`	グループでプリエンプションをイネーブルにし、優先度に関係なく、スタンバイ デバイスがアクティブ デバイスをプリエンプション処理できるようにします。
ステップ 10	**track** *object-number* {**decrement** *value* | **shutdown**} 例： `Device(config-red-app-grp)# track 200 decrement 200`	冗長グループの優先度を指定します。この値は、イベントが発生した場合に減らされます。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

コントロール インターフェイスおよびデータ インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **data** *interface-type interface-number*
7. **control** *interface-type interface-number* **protocol** *id*
8. **timers delay** *seconds* [**reload** *seconds*]
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長アプリケーション グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**data** *interface-type interface-number* 例： `Device(config-red-app-grp)# data GigabitEthernet 0/0/0`	冗長グループに使用されるデータ インターフェイスを指定します。
ステップ 7	**control** *interface-type interface-number* **protocol** *id* 例： `Device(config-red-app-grp)# control gigabitethernet 0/0/2 protocol 1`	冗長グループに使用されるコントロール インターフェイスを指定します。 • このインターフェイスは、コントロール インターフェイス プロトコルのインスタンスにも関連付けられます。
ステップ 8	**timers delay** *seconds* [**reload** *seconds*] 例： `Device(config-red-app-grp)# timers delay 100 reload 400`	障害の発生後、またはシステムのリロード後に起動するロールのネゴシエートを遅らせるために、冗長グループが待機する時間を指定します。
ステップ 9	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

LAN トラフィック インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **encapsulation dot1q** *vlan-id*
6. **ip vrf forwarding** *name*
7. **ipv6 address** {*ipv6-prefix*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
8. **zone-member security** *zone-name*
9. **redundancy rii** *RII-identifier*
10. **redundancy group** *id* {**ip** *virtual-ip* | **ipv6** {*link-local-address* | *ipv6-address/prefix-length*} | **autoconfig**} [**exclusive**] [**decrement** *value*]
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/0/2`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**description** *string* 例： `Device(config-if)# description lan interface`	（任意）インターフェイス設定に説明を追加します。
ステップ 5	**encapsulation dot1q** *vlan-id* 例： `Device(config-if)# encapsulation dot1q 18`	インターフェイスで使用するカプセル化方式を設定します。
ステップ 6	**ip vrf forwarding** *name* 例： `Device(config-if)# ip vrf forwarding trust`	VPN ルーティングおよび転送（VRF）インスタンスをインターフェイスまたはサブインターフェイスに関連付けます。 • このコマンドは、指定された VRF を設定しない場合は設定されません。
ステップ 7	**ipv6 address** {*ipv6-prefix*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} 例： `Device(config-if)# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 8	**zone-member security** *zone-name* 例： `Device(config-if)# zone member security z1`	ゾーン メンバーとしてインターフェイスを設定します。 • *zone-name* 引数では、ファイアウォールの設定時に **zone security** コマンドを使用して設定したゾーンのいずれかを設定する必要があります。

	コマンドまたはアクション	目的
		• インターフェイスがセキュリティ ゾーンにある場合、そのインターフェイスを通るトラフィックはどちらの方向でもすべて（ルータ宛またはルータ発信のトラフィックを除く）デフォルトでドロップされます。ゾーン メンバーであるインターフェイスをトラフィックが通過することを許可するには、そのゾーンをゾーン ペアの一部にして、そのゾーン ペアにポリシーを適用する必要があります。 ポリシーで、inspect または pass アクションを通してトラフィックが許可されると、トラフィックはインターフェイスを通過します。
ステップ 9	**redundancy rii** *RII-identifier* 例： `Device(config-if)# redundancy rii 100`	冗長グループによって保護されるトラフィック インターフェイスの RII を設定します。
ステップ 10	**redundancy group** *id* {**ip** *virtual-ip* | **ipv6** {*link-local-address* | *ipv6-address/prefix-length*} | **autoconfig**} [**exclusive**] [**decrement** *value*] 例： `Device(config-if)# redundancy group 1 ipv6 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 exclusive decrement 50`	冗長グループの（RG）トラフィック インターフェイス コンフィギュレーションをイネーブルにします。
ステップ 11	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

WAN トラフィック インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **ipv6 address** {*ipv6-prefix*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
6. **zone-member security** *zone-name*
7. **ip tcp adjust-mss** *max-segment-size*
8. **redundancy rii** *RII-identifier*
9. **redundancy asymmetric-routing enable**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/1/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**description** *string* 例： `Device(config-if)# description wan interface`	（任意）インターフェイス設定に説明を追加します。
ステップ 5	**ipv6 address** {*ipv6-prefix*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} 例： `Device(config-if)# ipv6 address 2001:DB8:2222::/48`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z2`	ファイアウォールの設定中にゾーン メンバーとしてインターフェイスを設定します。 • *zone-name* 引数では、**zone security** コマンドを使用して設定したゾーンのいずれかを設定する必要があります。 • インターフェイスがセキュリティ ゾーンにある場合、そのインターフェイスを通るトラフィックはどちらの方向でもすべて（ルータ宛またはルータ発信のトラフィックを除く）デフォルトでドロップされます。 ゾーン メンバーであるインターフェイスをトラフィックが通過することを許可するには、そのゾーンをゾーン ペアの一部にして、そのゾーン ペアにポリシーを適用する必要があります。 ポリシーで、inspect または pass アクションを通してトラフィックが許可されると、トラフィックはインターフェイスを通過します。
ステップ 7	**ip tcp adjust-mss** *max-segment-size* 例： `Device(config-if)# ip tcp adjust-mss 1360`	ルータを通過する TCP SYN パケットの最大セグメント サイズ（MSS）の値を調整します。
ステップ 8	**redundancy rii** *RII-identifier* 例： `Device(config-if)# redundancy rii 360`	冗長グループによって保護されるトラフィック インターフェイスの RII を設定します。
ステップ 9	**redundancy asymmetric-routing enable** 例： `Device(config-if)# redundancy asymmetric-routing enable`	非対称ルーティングで使用されるインターフェイスに冗長グループを関連付けます。
ステップ 10	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

IPv6 ファイアウォールの設定

IPv4ファイアウォールとIPv6ファイアウォールを設定する手順は同じです。IPv6ファイアウォールを設定するには、IPv6アドレスファミリだけが一致するようにクラスマップを設定する必要があります。

match protocol コマンドは、IPv4 トラフィックと IPv6 トラフィックの両方に適用され、IPv4 ポリシーまたは IPv6 ポリシーに含めることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf-definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **sessions maximum** *sessions*
9. **exit**
10. **ipv6 unicast-routing**
11. **ip port-map** *appl-name* **port** *port-num* **list** *list-name*
12. **ipv6 access-list** *access-list-name*
13. **permit ipv6 any any**
14. **exit**
15. **class-map type inspect match-all** *class-map-name*
16. **match access-group name** *access-group-name*
17. **match protocol** *protocol-name*
18. **exit**
19. **policy-map type inspect** *policy-map-name*
20. **class type inspect** *class-map-name*
21. **inspect** [*parameter-map-name*]
22. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vrf-definition** *vrf-name* 例： `Device(config)# vrf-definition VRF1`	仮想ルーティングおよび転送（VRF）ルーティング テーブル インスタンスを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、標準IPv6アドレスプレフィックスを伝送するセッションを設定します。
ステップ 5	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect ipv6-param-map`	ファイアウォールのグローバル検査タイプ パラメータ マップを、検査アクションに関連するしきい値、タイムアウト、およびその他のパラメータに関連付けることができるようにし、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**sessions maximum** *sessions* 例： `Device(config-profile)# sessions maximum 10000`	ゾーン ペア上に存在可能な最大許容セッション数を設定します。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**ip port-map** *appl-name* **port** *port-num* **list** *list-name* 例： `Device(config)# ip port-map ftp port 8090 list ipv6-acl`	IPv6 アクセス コントロール リスト（ACL）を使用してポートツーアプリケーション マッピング（PAM）を確立します。
ステップ 12	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list ipv6-acl`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 13	**permit ipv6 any any** 例： `Device(config-ipv6-acl)# permit ipv6 any any`	IPv6 アクセス リストに許可条件を設定します。
ステップ 14	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**class-map type inspect match-all** *class-map-name* 例： `Device(config)# class-map type inspect match-all ipv6-class`	アプリケーション固有検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 16	**match access-group name** *access-group-name* 例： `Device(config-cmap)# match access-group name ipv6-acl`	指定した ACL をベースにクラスマップに対して一致基準を設定します。
ステップ 17	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルに基づくクラス マップの一致基準を設定します。
ステップ 18	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 19	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ipv6-policy`	プロトコル固有検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 20	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ipv6-class`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 21	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect ipv6-param-map`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 22	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンの設定およびインターフェイスへのゾーンの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ipv6 address** *ipv6-address*/*prefix-length*
12. **encapsulation dot1q** *vlan-id*
13. **zone-member security** *zone-name*
14. **end**
15. **show policy-map type inspect zone-pair sessions**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *zone-name* 例： `Device(config)# zone security z1`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**zone security** *zone-name* 例： `Device(config)# zone security z2`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*] 例： `Device(config)# zone-pair security in-2-out source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy`	ポリシー マップをトップレベル ポリシー マップに付加します。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードを開始します。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0.1`	サブインターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ipv6 address** *ipv6-address*/*prefix-length* 例： `Device(config-subif)# ipv6 address 2001:DB8:2222:7272::72/64`	IPv6の一般的なプレフィックスに基づいてIPv6アドレスを設定し、インターフェイスまたはサブインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 12	**encapsulation dot1q** *vlan-id* 例： `Device(config-subif)# encapsulation dot1q 2`	インターフェイスで使用するカプセル化方式を設定します。

	コマンドまたはアクション	目的
ステップ 13	**zone-member security** *zone-name* 例： `Device(config-subif)# zone member security z1`	ゾーン メンバーとしてインターフェイスを設定します。 • *zone-name* 引数では、**zone security** コマンドを使用して設定したゾーンのいずれかを設定する必要があります。 • インターフェイスがセキュリティ ゾーンにある場合、そのインターフェイスを通るトラフィックはどちらの方向でもすべて（デバイス宛またはデバイス発信のトラフィックを除く）デフォルトでドロップされます。 ゾーン メンバーであるインターフェイスをトラフィックが通過することを許可するには、そのゾーンをゾーン ペアの一部にして、そのゾーンペアにポリシーを適用する必要があります。 ポリシーで、inspect または pass アクションを通してトラフィックが許可されると、トラフィックはインターフェイスを通過します。
ステップ 14	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 15	**show policy-map type inspect zone-pair sessions** 例： `Device# show policy-map type inspect zone-pair sessions`	ポリシー マップが指定したゾーン ペアに適用されているため、作成されたステートフル パケット インスペクション セッションを表示します。 • このコマンドの出力は、IPv4 と IPv6 の両方のファイアウォール セッションを表示します。

例

show policy-map type inspect zone-pair sessions コマンドからの次のサンプル出力には、IPv6 アドレスと IPv4 アドレスの双方向のパケット変換が表示されます。

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:32847=>(209.165.201.2:21) ftp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [37:84]

        Half-open Sessions
```

```
        Session 110D930C [2001:DB8:1::104]:32848=>(209.165.201.2:21) ftp SIS_OPENING
         Created 00:00:00, Last heard 00:00:00
         Bytes sent (initiator:responder) [0:0]
```

show policy-map type inspect zone-pair sessions コマンドからの次のサンプル出力には、IPv6 アドレスから IPv6 アドレスへのパケットの変換が表示されます。

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:63=>[2001:DB8:2::102]:63 udp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [162:0]
```

IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポートの設定例

例：冗長グループ プロトコルの設定

次に、helloタイムおよびホールドタイムメッセージ用にタイマーが設定されている冗長グループを設定する例を示します。

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9
Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100
Device(config-red-app-prtcl)# bfd
Device(config-red-app-prtcl)# end
```

例：冗長アプリケーション グループの設定

次に、優先度とプリエンプション属性を使用する group1 という冗長グループを設定する例を示します。

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name group1
Device(config-red-app-grp)# priority 100 failover-threshold 50
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# track 200 decrement 200
Device(config-red-app-grp)# end
```

例：コントロール インターフェイスおよびデータ インターフェイスの設定

```
Device# configure terminal
Device(config-red)# application redundancy
Device(config-red-app-grp)# group 1
Device(config-red-app-grp)# data GigabitEthernet 0/0/0
Device(config-red-app-grp)# control GigabitEthernet 0/0/2 protocol 1
Device(config-red-app-grp)# timers delay 100 reload 400
Device(config-red-app-grp)# end
```

例：LAN トラフィック インターフェイスの設定

```
Device# configure terminal
Device(config-if)# interface gigabitethernet 2/0/2
Device(config-if)# description lan interface
Device(config-if)# encapsulation dot1q 18
Device(config-if)# ip vrf forwarding trust
Device(config-if)# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64
Device(config-if)# zone member security z1
Device(config-if)# redundancy rii 100
Device(config-if)# redundancy group 1 ipv6 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE exclusive
decrement 50
Device(config-if)# end
```

例：WAN トラフィック インターフェイスの設定

次に、WAN-LAN シナリオの冗長グループを設定する例を示します。

```
Device# configure terminal
Device(config-if)# interface gigabitethernet 2/1/0
Device(config-if)# description wan interface
Device(config-if)# ipv6 address 2001:DB8:2222::/48
Device(config-if)# zone-member security z2
Device(config-if)# ip tcp adjust-mss 1360
Device(config-if)# redundancy rii 360
Device(config-if)# redundancy asymmetric-routing enable
Device(config-if)# end
```

例：IPv6 ファイアウォールの設定

```
Device# configure terminal
Device(config)# vrf-definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
Device(config)# parameter-map type inspect ipv6-param-map
Device(config-profile)# sessions maximum 10000
Device(config-profile)# exit
Device(config)# ipv6 unicast-routing
Device(config)# ip port-map ftp port 8090 list ipv6-acl
Device(config)# ipv6 access-list ipv6-acl
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# class-map type inspect match-all ipv6-class
Device(config-cmap)# match access-group name ipv6-acl
```

```
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect ipv6-policy
Device(config-pmap)# class type inspect ipv6-class
Device(config-pmap-c)# inspect ipv6-param-map
Device(config-pmap-c)# end
```

例：ゾーンの設定およびインターフェイスへのゾーンの適用

```
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security in-to-out source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0.1
Device(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
Device(config-if)# encapsulation dot1q 2
Device(config-if)# zone member security z1
Device(config-if)# end
```

IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *8*：*IPv6* ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポートの機能情報

機能名	リリース	機能情報
IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポート	Cisco IOS XE Release 3.8S	IPv6 ゾーンベース ファイアウォールのボックスツーボックス ハイ アベイラビリティ サポート機能は、IPv6 ファイアウォールでの冗長グループ（RG）に基づいたハイ アベイラビリティ（HA）をサポートします。 この機能により、デバイスのペアが互いのバックアップとして動作するように設定できます。 この機能を設定し、複数のフェールオーバー条件に基づいてアクティブ デバイスを判断できます。 追加または変更されたコマンドはありません。

第 7 章

ゾーンベース ファイアウォールおよび NAT のシャーシ間非対称ルーティング サポート

ゾーンベース ファイアウォールおよびNAT のシャーシ間非対称ルーティング サポート機能は、パケット処理のための、スタンバイ冗長グループからアクティブ冗長グループへのパケットの転送をサポートします。 この機能がイネーブルでない場合、初期同期（SYN）メッセージを受信しなかったルータに転送されたリターン TCP パケットは、既存で既知のいずれのセッションにも属していないため、ドロップされます。

このモジュールでは、非対称ルーティングの概要、および非対称ルーティングの設定方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ゾーンベース ファイアウォールおよびNATのシャーシ間非対称ルーティング サポートの制約事項

- マルチプロトコル ラベル スイッチング（MPLS）および VPN を介した非対称ルーティングはサポートされません。
- 仮想IPアドレスおよび仮想MAC（VMAC）アドレスを使用するLANは、非対称ルーティングをサポートしません。
- VPN ルーティングおよび転送（VRF）はサポートされません。

ゾーンベース ファイアウォールおよびNATのシャーシ間非対称ルーティング サポートについて

非対称ルーティングの概要

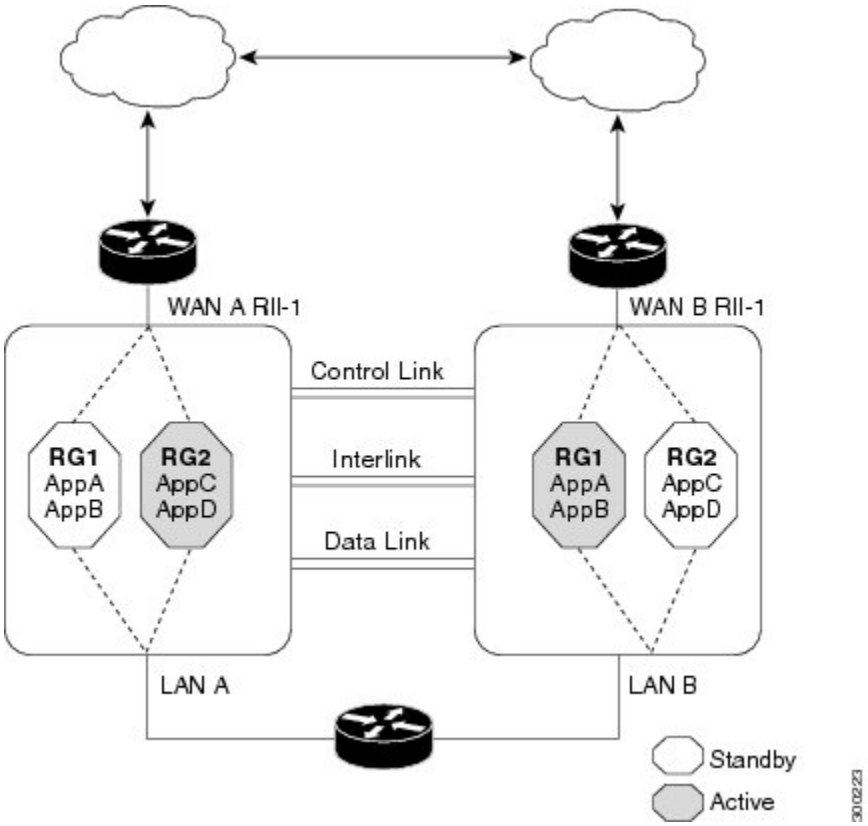
非対称ルーティングは、TCPまたはUDP接続のパケットが異なるルートを介して異なる方向に流れる場合に発生します。 非対称ルーティングでは、1 つの TCP または UDP 接続に属しているパケットは、冗長グループ（RG）の 1 つのインターフェイスを介して転送されますが、同じ RG の別のインターフェイスを介して戻されます。 非対称ルーティングでは、パケット フローは同じ RG に残ります。 非対称ルーティングを設定する場合、スタンバイ RG で受信したパケットは、処理のためにアクティブな RG にリダイレクトされます。 非対称ルーティングが設定されていない場合、スタンバイ RG で受信したパケットはドロップされる可能性があります。

非対称ルーティングは、特定のトラフィック フローの RG を決定します。 RG の状態は、パケット処理の決定において重要です。 RG がアクティブの場合は、通常のパケットの処理が実行されます。 RG がスタンバイ状態で、非対称ルーティングおよび **asymmetric-routing always-divert enable** コマンドを設定している場合、パケットはアクティブRGに転送されます。 スタンバイ RG

で受信したパケットをアクティブ RG に常に転送するには、**asymmetric-routing always-divert enable** コマンドを使用します。

下の図は、別の非対称ルーティング インターリンク インターフェイスを使用して、パケットをアクティブ RG に転送する非対称ルーティング シナリオを示しています。

図 *15*：非対称ルーティングのシナリオ



次のルールが非対称ルーティングに適用されます。

- 1:1 マッピングは、冗長インターフェイス識別子（RII）とインターフェイス間です。
- 1:*n* マッピングは、インターフェイスと RG 間です。（1 つのインターフェイスが複数の RG を持つことができます）。
- 1:*n* マッピングは、RG およびその RG を使用するアプリケーション間です。（複数のアプリケーションが同じ RG を使用できます）。
- 1:1 マッピングは、RG とトラフィック フロー間です。トラフィック フローは、単一 RG だけにマッピングされる必要があります。トラフィック フローが複数の RG にマッピングされると、エラーが発生します。
- 1:1 または 1:*n* マッピングは、非対称ルーティング インターリンクがすべての RG インターリンク トラフィックをサポートできる十分な帯域幅がある限り、RG と非対称ルーティング インターリンク間に存在します。

非対称ルーティングは、転送されるすべてのトラフィックを処理するインターリンク インターフェイスで構成されます。 非対称ルーティング インターリンク インターフェイスの帯域幅は、転送が予期されるすべてのトラフィックを処理できるだけの十分な大きさが必要です。 IPv4 アドレスは、非対称ルーティングインターリンクインターフェイスで設定され、非対称ルーティングインターフェイスの IP アドレスは、このインターフェイスから到達可能である必要があります。

（注） 非対称ルーティング インターリンク インターフェイスは、インターリンク トラフィックのみに使用し、ハイ アベイラビリティ（HA）制御インターフェイスまたはデータ インターフェイスと共有しないことを推奨します。これは、非対称ルーティングインターリンクインターフェイス上のトラフィック量が非常に高くなる可能性があるためです。

ファイアウォールでの非対称ルーティング サポート

ボックス内非対称ルーティング サポートでは、ファイアウォールは、インターネット制御メッセージ プロトコル（ICMP）、TCP、および UDP パケットのステートフル レイヤ 3 およびレイヤ 4 インスペクションを行います。 ファイアウォールは、パケット ウィンドウ サイズおよびパケットの順序を確認して、TCP パケットのステートフル インスペクションを実行します。 ファイアウォールでは、ステートフル インスペクションのために両方向のトラフィックからのステート情報も必要です。 ファイアウォールは、ICMP 情報フローの限定的なインスペクションを行います。ICMP エコー要求および応答に関連付けられているシーケンス番号を確認します。 ファイアウォールは、そのパケットに対するセッションが確立されるまで、スタンバイ冗長グループ（RG）へのパケット フローを同期しません。 確立されたセッションは、TCP、UDP の 2 番目のパケット、および ICMP の情報メッセージのスリーウェイ ハンドシェイクです。 すべての ICMP フローがアクティブな RG に送信されます。

ファイアウォールは、ICMP、TCP、および UDP プロトコルに属さないパケットのポリシーのステートレスな検証を実行します。

ファイアウォールは、双方向トラフィックを使用して、パケット フローがエージングアウトする時期を決定し、すべての検査対象パケット フローをアクティブ RG に転送します。 パス ポリシーを持ち、ポリシーなしまたはドロップ ポリシーと同じゾーンが含まれるパケット フローは、転送されません。

（注） ファイアウォールは、スタンバイ RG で受信したパケットをアクティブ RG に転送する **asymmetric-routing always-divert enable** コマンドをサポートしません。 デフォルトでは、ファイアウォールはすべてのパケット フローをアクティブ RG に強制的に転送します。

NAT での非対称ルーティング

デフォルトでは、非対称ルーティングが設定されている場合、ネットワーク アドレス変換（NAT）はスタンバイ RG の非 ALG パケットをアクティブ RG に転送するのはなく、処理します。 NAT

だけの設定（つまり、ファイアウォールが設定されていない場合）では、パケット処理のためにアクティブ RG とスタンバイ RG の両方を使用できます。 NAT のみの設定で、非対称ルーティングを設定している場合、デフォルトの非対称ルーティング ルールでは、NAT はスタンバイ RG でパケットを選択的に処理します。 スタンバイ RG で受信したパケットをアクティブ RG に転送するために、**asymmetric-routing always-divert enable** コマンドを設定できます。 また、NAT とともにファイアウォールを設定した場合、デフォルトの非対称ルーティング ルールでは、パケットをアクティブ RG に常に転送します。

NAT がスタンバイ RG でパケットを受信した場合、パケット転送を設定していないと、NAT は、セッションがそのパケットに存在するかどうかを確認するために検索を実行します。 セッションが存在し、そのセッションに関連付けられた ALG がない場合、NAT はそのパケットをスタンバイ RG で処理します。 セッションが存在している場合、スタンバイ RG のパケットの処理は、NAT トラフィックの帯域幅を大幅に増加させます。

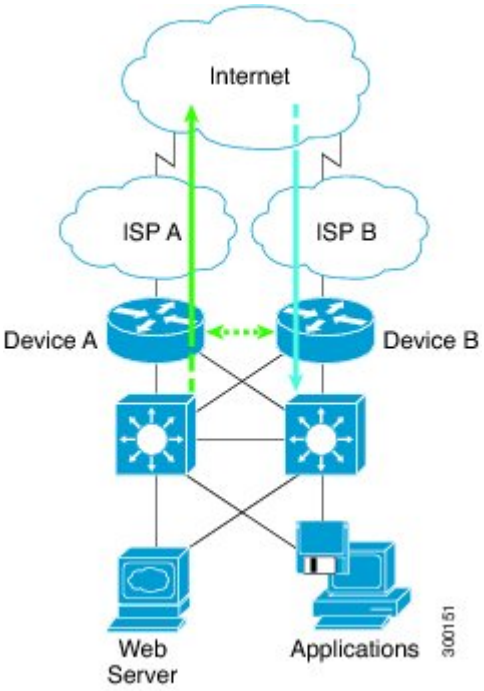
NAT は ALG を使用して、ペイロードを特定および変換し、子フローを作成します。 ALG では、双方向トラフィックが正しく機能する必要があります。 NAT は、ALG に関連付けられたパケット フローに関して、すべてのトラフィックをアクティブ RG に転送する必要があります。 これは、セッションに関連付けられている ALG データがスタンバイ RG にあるかどうかをチェックすることで実現されます。 ALG データが存在する場合、パケットは非対称ルーティングのために転送されます。

WAN-LAN トポロジでの非対称ルーティング

非対称ルーティングは、WAN-LAN トポロジだけをサポートします。 WAN-LAN トポロジでは、デバイスが内部の LAN インターフェイスおよび外部の WAN インターフェイスを介して接続されます。 WAN リンク経由で受信したリターン トラフィックのルーティングに対する制御は行われ

ません。 非対称ルーティングは、WAN-LAN トポロジの WAN リンク経由で受信したリターン トラフィックのルーティングを制御します。 下の図は、WAN-LAN トポロジを示しています。

図 *16*：*WAN-LAN* トポロジでの非対称ルーティング



ゾーンベース ファイアウォールおよびNATのシャーシ間非対称ルーティング サポートの設定方法

冗長アプリケーション グループおよび冗長グループ プロトコルの設定

冗長グループは、次の設定要素で構成されています。

- オブジェクトごとに優先度を減らす量。
- 優先度を減らす障害（オブジェクト）
- フェールオーバー優先度
- フェールオーバーしきい値
- グループ インスタンス
- グループ名

- 初期化遅延タイマー

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*
7. **priority** *value* [**failover threshold** *value*]
8. **preempt**
9. **track** *object-number* **decrement** *number*
10. **exit**
11. **protocol** *id*
12. **timers hellotime** {*seconds* | **msec** *msec*} **holdtime** {*seconds* | **msec** *msec*}
13. **authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] | **key-chain** *key-chain-name*}
14. **bfd**
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーションの冗長性を設定し、冗長アプリケーション コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長グループを設定し、冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-grp)# name group1`	プロトコル インスタンスに任意のエイリアスを指定します。
ステップ 7	**priority** *value* [**failover threshold** *value*] 例： `Device(config-red-app-grp)# priority 100 failover threshold 50`	冗長グループの初期優先度とフェールオーバーしきい値を指定します。
ステップ 8	**preempt** 例： `Device(config-red-app-grp)# preempt`	冗長グループでプリエンプションをイネーブルにし、スタンバイ デバイスがアクティブ デバイスをプリエンプション処理できるようにします。 • スタンバイ デバイスは、その優先度がアクティブ デバイスの優先度よりも高い場合にだけプリエンプトします。
ステップ 9	**track** *object-number* **decrement** *number* 例： `Device(config-red-app-grp)# track 50 decrement 50`	冗長グループの優先度を指定します。この値は、トラッキング対象のオブジェクトでイベントが発生した場合に減らされます。
ステップ 10	**exit** 例： `Device(config-red-app-grp)# exit`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 11	**protocol** *id* 例： `Device(config-red-app)# protocol 1`	コントロール インターフェイスに接続されるプロトコル インスタンスを指定し、冗長アプリケーション プロトコル コンフィギュレーション モードを開始します。
ステップ 12	**timers hellotime** {*seconds* | **msec** *msec*} **holdtime** {*seconds* | **msec** *msec*} 例： `Device(config-red-app-prtcl)# timers hellotime 3 holdtime 10`	hello メッセージが送信される間隔と、デバイスがダウン状態と宣言されるまでの時間を指定します。 • holdtime は、hellotime の少なくとも 3 倍以上にする必要があります。

	コマンドまたはアクション	目的
ステップ 13	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] | **key-chain** *key-chain-name*} 例： `Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100`	認証情報を指定します。
ステップ 14	**bfd** 例： `Device(config-red-app-prtcl)# bfd`	双方向フォワーディング検出（BFD）を使用してコントロール インターフェイスで実行されているフェールオーバー プロトコルを統合し、ミリ秒単位での障害検出を達成できるようにします。 • BFD はデフォルトでイネーブルになっています。
ステップ 15	**end** 例： `Device(config-red-app-prtcl)# end`	冗長アプリケーション プロトコル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

データ、コントロール、および非対称ルーティングのインターフェイスの設定

この作業では、次の冗長グループ（RG）要素を設定します。

- コントロール インターフェイスとして使用されるインターフェイス。
- データ インターフェイスとして使用されるインターフェイス。
- 非対称ルーティングに使用されるインターフェイス。 これはオプションのタスクです。 この作業は、ネットワーク アドレス変換（NAT）に非対称ルーティングを設定する場合にのみ実行します。

（注） 非対称ルーティング、データ、およびコントロールは、ゾーンベース ファイアウォールの個別のインターフェイスで設定する必要があります。ただし、ネットワーク アドレス変換（NAT）では、非対称ルーティング、データ、およびコントロールを同じインターフェイス上に設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **data** *interface-type interface-number*
7. **control** *interface-type interface-number* **protocol** *id*
8. **timers delay** *seconds* [**reload** *seconds*]
9. **asymmetric-routing interface** *type number*
10. **asymmetric-routing always-divert enable**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーションの冗長性を設定し、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長グループ（RG）を設定し、冗長アプリケーション グループ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**data** *interface-type interface-number* 例： `Device(config-red-app-grp)# data GigabitEthernet 0/0/1`	RG で使用されるデータ インターフェイスを指定します。
ステップ 7	**control** *interface-type interface-number* **protocol** *id* 例： `Device(config-red-app-grp)# control GigabitEthernet 1/0/0 protocol 1`	RG で使用されるコントロール インターフェイスを指定します。 • コントロールインターフェイスは、コントロール インターフェイスプロトコルのインスタンスにも関連付けられます。
ステップ 8	**timers delay** *seconds* [**reload** *seconds*] 例： `Device(config-red-app-grp)# timers delay 100 reload 400`	障害の発生後、またはシステムのリロード後に起動するロールのネゴシエートを遅らせるために、RG が待機する時間を指定します。
ステップ 9	**asymmetric-routing interface** *type number* 例： `Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 0/1/1`	RG で使用される非対称ルーティング インターフェイスを指定します。
ステップ 10	**asymmetric-routing always-divert enable** 例： `Device(config-red-app-grp)# asymmetric-routing always-divert enable`	スタンバイ RG から受信したパケットを常にアクティブ RG に転送します。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

インターフェイスでの冗長インターフェイス識別子および非対称ルーティングの設定

（注）
- データ インターフェイスまたはコントロール インターフェイスとして設定されたインターフェイス上に冗長インターフェイス識別子（RII）を設定する必要はありません。
- アクティブ デバイスとスタンバイ デバイスの両方で RII および非対称ルーティングを設定する必要があります。
- 仮想 IP アドレスが設定されているインターフェイス上では非対称ルーティングをイネーブルにできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **redundancy rii** *id*
5. **redundancy group** *id* [**decrement** *number*]
6. **redundancy asymmetric-routing enable**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/1/3`	冗長グループ（RG）に関連付けるインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**redundancy rii** *id* 例： `Device(config-if)# redundancy rii 600`	冗長インターフェイス識別子（RII）を設定します。
ステップ 5	**redundancy group** *id* [**decrement** *number*] 例： `Device(config-if)# redundancy group 1 decrement 20`	インターフェイスがダウンした場合、RG 冗長トラフィック インターフェイス コンフィギュレーションをイネーブルにし、優先度から減らす量を指定します。 （注） 非対称ルーティングがイネーブルになっているトラフィック インターフェイス上で RG を設定する必要はありません。
ステップ 6	**redundancy asymmetric-routing enable** 例： `Device(config-if)# redundancy asymmetric-routing enable`	各 RG に非同期フロー転送トンネルを確立します。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

非対称ルーティングによる動的な内部送信元変換の設定

次の設定は、非対称ルーティングを使用した動的な内部送信元変換の例です。 非対称ルーティングは、NAT 設定のタイプ（動的な内部送信元変換、静的な内部および外部送信元変換、ポートアドレス変換（PAT）の内部および外部送信元変換）を使用して設定できます。 NAT 設定のさまざまなタイプの詳細については、「Configuring NAT for IP Address Conservation」の章を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip nat outside**
6. **exit**
7. **redundancy**
8. **application redundancy**
9. **group** *id*
10. **asymmetric-routing always-divert enable**
11. **end**
12. **configure terminal**
13. **ip nat pool** *name start-ip end-ip* {*mask* | **prefix-length** *prefix-length*}
14. **exit**
15. **ip nat inside source list** *acl-number* **pool** *name* **redundancy** *redundancy-id* **mapping-id** *map-id*
16. **access-list** *standard-acl-number* **permit** *source-address wildcard-bits*
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/3`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**ip nat outside** 例： `Device(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 7	**redundancy** 例： `Device(config)# redundancy`	冗長性を設定し、冗長コンフィギュレーションモードを開始します。
ステップ 8	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーションの冗長性を設定し、冗長アプリケーション コンフィギュレーションモードを開始します。
ステップ 9	**group** *id* 例： `Device(config-red-app)# group 1`	冗長グループを設定し、冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 10	**asymmetric-routing always-divert enable** 例： `Device(config-red-app-grp)# asymmetric-routing always-divert enable`	アクティブ デバイスにトラフィックを転送します。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 12	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 13	**ip nat pool** *name start-ip end-ip* {*mask* | **prefix-length** *prefix-length*} 例： `Device(config)# ip nat pool pool1 prefix-length 24`	グローバル アドレスのプールを定義します。 • IP NAT プール コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 14	**exit** 例： `Device(config-ipnat-pool)# exit`	IP NAT プール コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**ip nat inside source list** *acl-number* **pool** *name* **redundancy** *redundancy-id* **mapping-id** *map-id* 例： `Device(config)# ip nat inside source list pool pool1 redundancy 1 mapping-id 100`	内部送信元アドレスの NAT をイネーブルにし、マッピング ID を使用して NAT を冗長グループに関連付けます。
ステップ 16	**access-list** *standard-acl-number* **permit** *source-address wildcard-bits* 例： `Device(config)# access-list 10 permit 10.1.1.1 255.255.255.0`	変換する内部アドレスの標準アクセス リストを定義します。
ステップ 17	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンベース ファイアウォールおよびNATのシャーシ間非対称ルーティング サポートの設定例

例：冗長アプリケーション グループおよび冗長グループ プロトコルの設定

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name group1
Device(config-red-app-grp)# priority 100 failover threshold 50
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# track 50 decrement 50
Device(config-red-app-grp)# exit
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# timers hellotime 3 holdtime 10
Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100
Device(config-red-app-prtcl)# bfd
Device(config-red-app-prtcl)# end
```

例：データ、コントロール、および非対称ルーティングのインターフェイスの設定

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# data GigabitEthernet 0/0/1
Device(config-red-app-grp)# control GigabitEthernet 1/0/0 protocol 1
Device(config-red-app-grp)# timers delay 100 reload 400
Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 0/1/1
Device(config-red-app-grp)# asymmetric-routing always-divert enable
Device(config-red-app-grp)# end
```

例：インターフェイスでの冗長インターフェイス識別子および非対称ルーティングの設定

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/3
Device(config-if)# redundancy rii 600
Device(config-if)# redundancy group 1 decrement 20
Device(config-if)# redundancy asymmetric-routing enable
Device(config-if)# end
```

例：非対称ルーティングによる動的な内部送信元変換の設定

```
Device(config)# interface gigabitethernet 0/1/3
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip nat outside
Device(config-if)# exit
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# asymmetric-routing always-divert enable
Device(config-red-app-grp)# end
Device# configure terminal
Device(config)# ip nat pool pool1 prefix-length 24
Device(config-ipnat-pool)# exit
Device(config)# ip nat inside source list pool pool1 redundancy 1 mapping-id 100
Device(config)# access-list 10 permit 10.1.1.1 255.255.255.0
```

ゾーンベース ファイアウォールおよびNATのシャーシ間非対称ルーティング サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
ファイアウォール シャーシ間冗長性	「Configuring Firewall Stateful Inter-Chassis Redundancy」モジュール
NAT シャーシ間冗長性	「Configuring Stateful Inter-Chassis Redundancy」モジュール

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ゾーンベース ファイアウォールおよびNATのシャーシ間非対称ルーティング サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *9*：ゾーンベース ファイアウォールおよび *NAT* のシャーシ間非対称ルーティング サポートの機能情報

機能名	リリース	機能情報
ゾーンベース ファイアウォールおよびNAT のシャーシ間非対称ルーティング サポート	Cisco IOS XE Release 3.5S	ゾーンベース ファイアウォールおよびNAT のシャーシ間非対称ルーティング サポート機能は、パケット処理のための、スタンバイ冗長グループからアクティブ冗長グループへのパケットの転送をサポートします。 次のコマンドが導入または変更されました。**asymmetric-routing**, **redundancy asymmetric-routing enable**。

第 8 章

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポート

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポート機能は、IPv4 トラフィックと IPv6 トラフィックを同時に実行するファイアウォールでの非対称ルーティングをサポートします。 非対称ルーティングは、パケット処理のために、スタンバイ冗長グループからのパケットをアクティブな冗長グループに転送することをサポートします。 この機能がイネーブルでない場合、初期同期（SYN）メッセージを受信しなかったデバイスに転送されたリターン TCP パケットは、既存で既知のいずれのセッションにも属していないため、ドロップされます。

このモジュールでは、非対称ルーティングの概要、およびIPv6ファイアウォールでの非対称ルーティングの設定方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポートの制約事項

- IPv4 のみが、非対称ルーティング インターリンク インターフェイスでサポートされています。
- FTP64 アプリケーション レベル ゲートウェイ（ALG）はサポートされません。
- 仮想 IP アドレスおよび仮想 MAC（VMAC）アドレスを使用する LAN は、非対称ルーティングをサポートしません。
- マルチプロトコル ラベル スイッチング（MPLS）および仮想ルーティングおよび転送（VRF）インスタンスは、VRF ID マッピングが、アクティブおよびスタンバイの Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ間にないためサポートされていません。

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポートについて

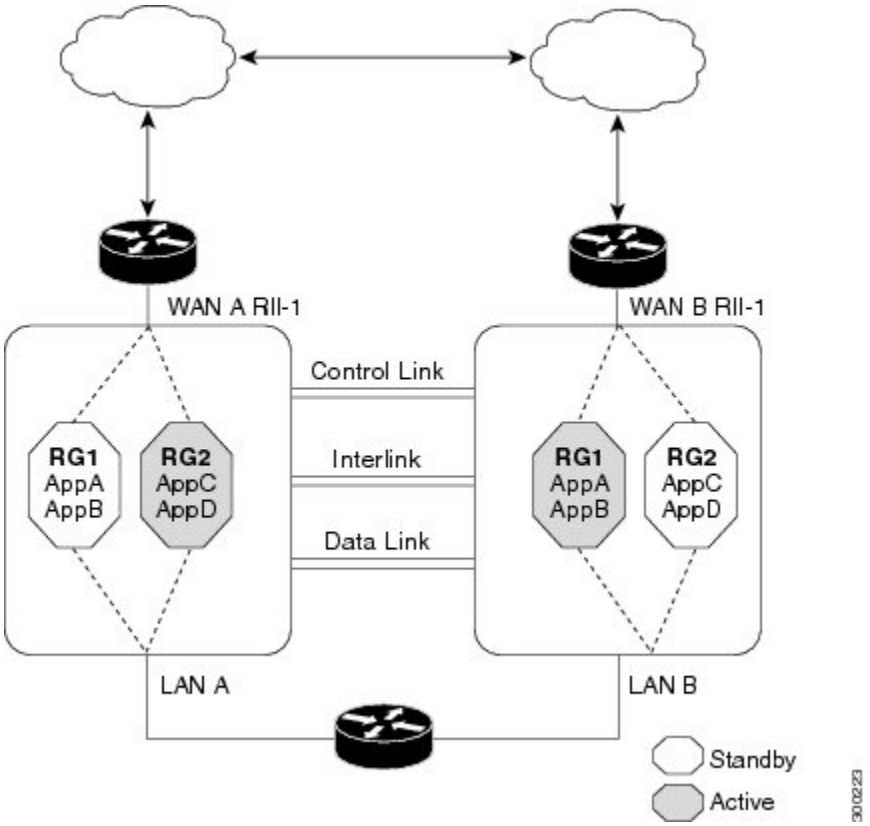
非対称ルーティングの概要

非対称ルーティングは、TCP または UDP 接続のパケットが異なるルートを介して異なる方向に流れる場合に発生します。 非対称ルーティングでは、1 つの TCP または UDP 接続に属しているパケットは、冗長グループ（RG）の 1 つのインターフェイスを介して転送されますが、同じ RG の別のインターフェイスを介して戻されます。 非対称ルーティングでは、パケット フローは同じ RG に残ります。 非対称ルーティングを設定する場合、スタンバイ RG で受信したパケットは、処理のためにアクティブな RG にリダイレクトされます。 非対称ルーティングが設定されていない場合、スタンバイ RG で受信したパケットはドロップされる可能性があります。

非対称ルーティングは、特定のトラフィック フローの RG を決定します。 RG の状態は、パケット処理の決定において重要です。 RG がアクティブの場合は、通常のパケットの処理が実行されます。 RG がスタンバイ状態で、非対称ルーティングおよび **asymmetric-routing always-divert enable** コマンドを設定している場合、パケットはアクティブ RG に転送されます。 スタンバイ RG で受信したパケットをアクティブ RG に常に転送するには、**asymmetric-routing always-divert enable** コマンドを使用します。

下の図は、別の非対称ルーティング インターリンク インターフェイスを使用して、パケットをアクティブ RG に転送する非対称ルーティング シナリオを示しています。

図 *17*：非対称ルーティングのシナリオ



次のルールが非対称ルーティングに適用されます。

- 1:1 マッピングは、冗長インターフェイス識別子（RII）とインターフェイス間です。
- 1: *n* マッピングは、インターフェイスと RG 間です。 （1 つのインターフェイスが複数の RG を持つことができます）。
- 1: *n* マッピングは、RG およびその RG を使用するアプリケーション間です。 （複数のアプリケーションが同じ RG を使用できます）。

- 1:1 マッピングは、RG とトラフィック フロー間です。 トラフィック フローは、単一 RG だけにマッピングされる必要があります。 トラフィック フローが複数の RG にマッピングされると、エラーが発生します。
- 1:1 または 1:*n* マッピングは、非対称ルーティング インターリンクがすべての RG インターリンク トラフィックをサポートできる十分な帯域幅がある限り、RG と非対称ルーティング インターリンク間に存在します。

非対称ルーティングは、転送されるすべてのトラフィックを処理するインターリンク インターフェイスで構成されます。 非対称ルーティング インターリンク インターフェイスの帯域幅は、転送が予期されるすべてのトラフィックを処理できるだけの十分な大きさが必要です。 IPv4 アドレスは、非対称ルーティング インターリンク インターフェイスで設定され、非対称ルーティング インターフェイスの IP アドレスは、このインターフェイスから到達可能である必要があります。

（注） 非対称ルーティング インターリンク インターフェイスは、インターリンク トラフィックのみに使用し、ハイ アベイラビリティ（HA）制御インターフェイスまたはデータ インターフェイスと共有しないことを推奨します。これは、非対称ルーティング インターリンク インターフェイス上のトラフィック量が非常に高くなる可能性があるためです。

デュアル スタック ファイアウォール

デュアル スタック ファイアウォールは、IPv4 および IPv6 トラフィックを同時に実行するファイアウォールです。 デュアル スタック ファイアウォールは、次のシナリオで設定できます。

- IPv4 トラフィックを実行する 1 つのファイアウォール ゾーン、および IPv6 トラフィックを実行する別のファイアウォール ゾーン。
- IPv4 と IPv6 は、ステートフル ネットワーク アドレス変換 64（NAT64）を使用して展開している場合に共存します。 このシナリオでは、トラフィックは IPv6 から IPv4 へ、およびその逆に流れます。
- 同じゾーン ペアは、IPv4 および IPv6 トラフィックの両方を許可します。

ファイアウォールでの非対称ルーティング サポート

ボックス内非対称ルーティング サポートでは、ファイアウォールは、インターネット制御メッセージ プロトコル（ICMP）、TCP、および UDP パケットのステートフル レイヤ 3 およびレイヤ 4 インスペクションを行います。 ファイアウォールは、パケット ウィンドウ サイズおよびパケットの順序を確認して、TCP パケットのステートフル インスペクションを実行します。 ファイアウォールでは、ステートフル インスペクションのために両方向のトラフィックからのステート情報も必要です。 ファイアウォールは、ICMP 情報フローの限定的なインスペクションを行います。ICMP エコー要求および応答に関連付けられているシーケンス番号を確認します。ファイアウォールは、そのパケットに対するセッションが確立されるまで、スタンバイ冗長グループ（RG）への

パケット フローを同期しません。 確立されたセッションは、TCP、UDP の 2 番目のパケット、および ICMP の情報メッセージのスリーウェイ ハンドシェイクです。 すべての ICMP フローがアクティブな RG に送信されます。

ファイアウォールは、ICMP、TCP、および UDP プロトコルに属さないパケットのポリシーのステートレスな検証を実行します。

ファイアウォールは、双方向トラフィックを使用して、パケットフローがエージングアウトする時期を決定し、すべての検査対象パケット フローをアクティブ RG に転送します。 パス ポリシーを持ち、ポリシーなしまたはドロップポリシーと同じゾーンが含まれるパケットフローは、転送されません。

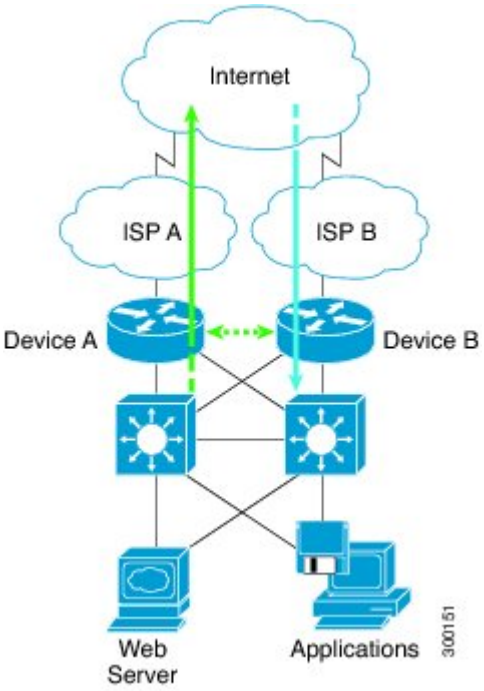
（注） ファイアウォールは、スタンバイ RG で受信したパケットをアクティブ RG に転送する **asymmetric-routing always-divert enable** コマンドをサポートしません。 デフォルトでは、ファイアウォールはすべてのパケット フローをアクティブ RG に強制的に転送します。

WAN-LAN トポロジでの非対称ルーティング

非対称ルーティングは、WAN-LAN トポロジだけをサポートします。 WAN-LAN トポロジでは、デバイスが内部の LAN インターフェイスおよび外部の WAN インターフェイスを介して接続されます。 WAN リンク経由で受信したリターン トラフィックのルーティングに対する制御は行われ

ません。 非対称ルーティングは、WAN-LAN トポロジの WAN リンク経由で受信したリターン トラフィックのルーティングを制御します。 下の図は、WAN-LAN トポロジを示しています。

図 *18*：*WAN-LAN* トポロジでの非対称ルーティング



アプリケーション冗長性のチェックポイント機能サポート

チェックポインティングは、デバイスの現在の状態を保持し、デバイスでの障害発生時にその情報を使用して再起動するプロセスです。チェックポイント機能（CF）は、プロセス間通信（IPC）プロトコル、および IP ベースの Stream Control Transmission Protocol（SCTP）を使用して、ピア間の通信をサポートします。 CF では、クライアントまたはデバイスにインフラストラクチャを提供して、複数ドメイン内のそれらのピアと通信できるようにします。デバイスは、アクティブデバイスからスタンバイ デバイスにチェックポイント メッセージを送信できます。

アプリケーションの冗長性は、同じシャーシ内およびシャーシ間に存在する複数のドメイン（グループとも呼ばれます）をサポートします。 複数のグループに登録されているデバイスは、1 つのグループからそれらのピア グループにチェックポイント メッセージを送信できます。 アプリケーションの冗長性は、シャーシ間ドメイン通信をサポートします。 チェックポインティングは、アクティブ デバイスからスタンバイ グループに対して発生します。 グループの任意の組み合わせがシャーシ間に存在する場合もあります。 シャーシ間の通信は、アプリケーションの冗長性専用のデータ リンク インターフェイス上の SCTP トランスポートによって行われます。

（注） 同じシャーシ内のドメインは相互に通信できません。

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポートの設定方法

冗長アプリケーション グループおよび冗長グループ プロトコルの設定

冗長グループは、次の設定要素で構成されています。

- オブジェクトごとに優先度を減らす量。
- 優先度を減らす障害（オブジェクト）
- フェールオーバー優先度
- フェールオーバーしきい値
- グループ インスタンス
- グループ名
- 初期化遅延タイマー

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*
7. **priority** *value* [**failover threshold** *value*]
8. **preempt**
9. **track** *object-number* **decrement** *number*
10. **exit**
11. **protocol** *id*
12. **timers hellotime** {*seconds* | **msec** *msec*} **holdtime** {*seconds* | **msec** *msec*}
13. **authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] | **key-chain** *key-chain-name*}
14. **bfd**
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーションの冗長性を設定し、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長グループを設定し、冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-grp)# name group1`	プロトコル インスタンスに任意のエイリアスを指定します。
ステップ 7	**priority** *value* [**failover threshold** *value*] 例： `Device(config-red-app-grp)# priority 100 failover threshold 50`	冗長グループの初期優先度とフェールオーバーしきい値を指定します。
ステップ 8	**preempt** 例： `Device(config-red-app-grp)# preempt`	冗長グループでプリエンプションをイネーブルにし、スタンバイ デバイスがアクティブ デバイスをプリエンプション処理できるようにします。 • スタンバイ デバイスは、その優先度がアクティブ デバイスの優先度よりも高い場合にだけプリエンプトします。

	コマンドまたはアクション	目的
ステップ 9	**track** *object-number* **decrement** *number* 例： `Device(config-red-app-grp)# track 50 decrement 50`	冗長グループの優先度を指定します。この値は、トラッキング対象のオブジェクトでイベントが発生した場合に減らされます。
ステップ 10	**exit** 例： `Device(config-red-app-grp)# exit`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 11	**protocol** *id* 例： `Device(config-red-app)# protocol 1`	コントロール インターフェイスに接続されるプロトコル インスタンスを指定し、冗長アプリケーション プロトコル コンフィギュレーション モードを開始します。
ステップ 12	**timers hellotime** {*seconds* | **msec** *msec*} **holdtime** {*seconds* | **msec** *msec*} 例： `Device(config-red-app-prtcl)# timers hellotime 3 holdtime 10`	hello メッセージが送信される間隔と、デバイスがダウン状態と宣言されるまでの時間を指定します。 • holdtime は、hellotime の少なくとも 3 倍以上にする必要があります。
ステップ 13	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] | **key-chain** *key-chain-name*} 例： `Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100`	認証情報を指定します。
ステップ 14	**bfd** 例： `Device(config-red-app-prtcl)# bfd`	双方向フォワーディング検出（BFD）を使用してコントロール インターフェイスで実行されているフェールオーバー プロトコルを統合し、ミリ秒単位での障害検出を達成できるようにします。 • BFD はデフォルトでイネーブルになっています。
ステップ 15	**end** 例： `Device(config-red-app-prtcl)# end`	冗長アプリケーション プロトコル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

データ、コントロール、および非対称ルーティングのインターフェイスの設定

この作業では、次の冗長グループ（RG）要素を設定します。

- コントロール インターフェイスとして使用されるインターフェイス。
- データ インターフェイスとして使用されるインターフェイス。
- 非対称ルーティングに使用されるインターフェイス。 これはオプションのタスクです。 この作業は、ネットワーク アドレス変換（NAT）に非対称ルーティングを設定する場合にのみ実行します。

（注） 非対称ルーティング、データ、およびコントロールは、ゾーンベース ファイアウォールの個別のインターフェイスで設定する必要があります。ただし、ネットワークアドレス変換（NAT）では、非対称ルーティング、データ、およびコントロールを同じインターフェイス上に設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **data** *interface-type interface-number*
7. **control** *interface-type interface-number* **protocol** *id*
8. **timers delay** *seconds* [**reload** *seconds*]
9. **asymmetric-routing interface** *type number*
10. **asymmetric-routing always-divert enable**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーション モードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーションの冗長性を設定し、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長グループ（RG）を設定し、冗長アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**data** *interface-type interface-number* 例： `Device(config-red-app-grp)# data GigabitEthernet 0/0/1`	RG で使用されるデータ インターフェイスを指定します。
ステップ 7	**control** *interface-type interface-number* **protocol** *id* 例： `Device(config-red-app-grp)# control GigabitEthernet 1/0/0 protocol 1`	RG で使用されるコントロール インターフェイスを指定します。 • コントロール インターフェイスは、コントロール インターフェイス プロトコルのインスタンスにも関連付けられます。
ステップ 8	**timers delay** *seconds* [**reload** *seconds*] 例： `Device(config-red-app-grp)# timers delay 100 reload 400`	障害の発生後、またはシステムのリロード後に起動するロールのネゴシエートを遅らせるために、RG が待機する時間を指定します。
ステップ 9	**asymmetric-routing interface** *type number* 例： `Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 0/1/1`	RG で使用される非対称ルーティング インターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 10	**asymmetric-routing always-divert enable** 例： `Device(config-red-app-grp)# asymmetric-routing always-divert enable`	スタンバイ RG から受信したパケットを常にアクティブ RG に転送します。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

インターフェイスでの冗長インターフェイス識別子および非対称ルーティングの設定

（注）
- データ インターフェイスまたはコントロール インターフェイスとして設定されたインターフェイス上に冗長インターフェイス識別子（RII）を設定する必要はありません。
- アクティブ デバイスとスタンバイ デバイスの両方で RII および非対称ルーティングを設定する必要があります。
- 仮想 IP アドレスが設定されているインターフェイス上では非対称ルーティングをイネーブルにできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **redundancy rii** *id*
5. **redundancy group** *id* [**decrement** *number*]
6. **redundancy asymmetric-routing enable**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/1/3`	冗長グループ（RG）に関連付けるインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**redundancy rii** *id* 例： `Device(config-if)# redundancy rii 600`	冗長インターフェイス識別子（RII）を設定します。
ステップ 5	**redundancy group** *id* [**decrement** *number*] 例： `Device(config-if)# redundancy group 1 decrement 20`	インターフェイスがダウンした場合、RG 冗長トラフィック インターフェイス コンフィギュレーションをイネーブルにし、優先度から減らす量を指定します。 （注） 非対称ルーティングがイネーブルになっているトラフィック インターフェイス上で RG を設定する必要はありません。
ステップ 6	**redundancy asymmetric-routing enable** 例： `Device(config-if)# redundancy asymmetric-routing enable`	各 RG に非同期フロー転送トンネルを確立します。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

IPv6 ファイアウォールの設定

IPv4 ファイアウォールと IPv6 ファイアウォールを設定する手順は同じです。IPv6 ファイアウォールを設定するには、IPv6 アドレス ファミリだけが一致するようにクラスマップを設定する必要があります。

match protocol コマンドは、IPv4 トラフィックと IPv6 トラフィックの両方に適用され、IPv4 ポリシーまたは IPv6 ポリシーに含めることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf-definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **sessions maximum** *sessions*
9. **exit**
10. **ipv6 unicast-routing**
11. **ip port-map** *appl-name* **port** *port-num* **list** *list-name*
12. **ipv6 access-list** *access-list-name*
13. **permit ipv6 any any**
14. **exit**
15. **class-map type inspect match-all** *class-map-name*
16. **match access-group name** *access-group-name*
17. **match protocol** *protocol-name*
18. **exit**
19. **policy-map type inspect** *policy-map-name*
20. **class type inspect** *class-map-name*
21. **inspect** [*parameter-map-name*]
22. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vrf-definition** *vrf-name* 例： `Device(config)# vrf-definition VRF1`	仮想ルーティングおよび転送（VRF）ルーティング テーブル インスタンスを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、標準 IPv6 アドレス プレフィックスを伝送するセッションを設定します。
ステップ 5	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect ipv6-param-map`	ファイアウォールのグローバル検査タイプ パラメータ マップを、検査アクションに関連するしきい値、タイムアウト、およびその他のパラメータに関連付けることができるようにし、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**sessions maximum** *sessions* 例： `Device(config-profile)# sessions maximum 10000`	ゾーン ペア上に存在可能な最大許容セッション数を設定します。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**ip port-map** *appl-name* **port** *port-num* **list** *list-name* 例： `Device(config)# ip port-map ftp port 8090 list ipv6-acl`	IPv6 アクセス コントロール リスト（ACL）を使用してポートツーアプリケーション マッピング（PAM）を確立します。
ステップ 12	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list ipv6-acl`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 13	**permit ipv6 any any** 例： `Device(config-ipv6-acl)# permit ipv6 any any`	IPv6 アクセス リストに許可条件を設定します。
ステップ 14	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**class-map type inspect match-all** *class-map-name* 例： `Device(config)# class-map type inspect match-all ipv6-class`	アプリケーション固有検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 16	**match access-group name** *access-group-name* 例： `Device(config-cmap)# match access-group name ipv6-acl`	指定した ACL をベースにクラス マップに対して一致基準を設定します。
ステップ 17	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルに基づくクラス マップの一致基準を設定します。
ステップ 18	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 19	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ipv6-policy`	プロトコル固有検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 20	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ipv6-class`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 21	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect ipv6-param-map`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 22	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

非対称ルーティングのゾーンおよびゾーン ペアの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ipv6 address** *ipv6-address*/*prefix-length*
12. **encapsulation dot1q** *vlan-id*
13. **zone-member security** *zone-name*
14. **end**
15. **show policy-map type inspect zone-pair sessions**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *zone-name* 例： `Device(config)# zone security z1`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**zone security** *zone-name* 例： `Device(config)# zone security z2`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*] 例： `Device(config)# zone-pair security in-2-out source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy`	ポリシー マップをトップレベル ポリシー マップに付加します。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0.1`	サブインターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-subif)# ipv6 address 2001:DB8:2222:7272::72/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスまたはサブインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 12	**encapsulation dot1q** *vlan-id* 例： `Device(config-subif)# encapsulation dot1q 2`	インターフェイスで使用するカプセル化方式を設定します。

	コマンドまたはアクション	目的
ステップ 13	**zone-member security** *zone-name* 例： `Device(config-subif)# zone-member security z1`	ゾーン メンバーとしてインターフェイスを設定します。 • *zone-name* 引数では、**zone security** コマンドを使用して設定したゾーンのいずれかを設定する必要があります。 • インターフェイスがセキュリティ ゾーンにある場合、そのインターフェイスを通るトラフィックはどちらの方向でもすべて（デバイス宛またはデバイス発信のトラフィックを除く）デフォルトでドロップされます。 ゾーン メンバーであるインターフェイスをトラフィックが通過することを許可するには、そのゾーンをゾーンペアの一部にして、そのゾーンペアにポリシーを適用する必要があります。 ポリシーで、inspect または pass アクションを通してトラフィックが許可されると、トラフィックはインターフェイスを通過します。
ステップ 14	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 15	**show policy-map type inspect zone-pair sessions** 例： `Device# show policy-map type inspect zone-pair sessions`	ポリシー マップが指定したゾーン ペアに適用されているため、作成されたステートフル パケット インスペクション セッションを表示します。 • このコマンドの出力は、IPv4 と IPv6 の両方のファイアウォール セッションを表示します。

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポートの設定例

例：冗長アプリケーション グループおよび冗長グループ プロトコルの設定

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name group1
Device(config-red-app-grp)# priority 100 failover threshold 50
```

```
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# track 50 decrement 50
Device(config-red-app-grp)# exit
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# timers hellotime 3 holdtime 10
Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100
Device(config-red-app-prtcl)# bfd
Device(config-red-app-prtcl)# end
```

例：データ、コントロール、および非対称ルーティングのインターフェイスの設定

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# data GigabitEthernet 0/0/1
Device(config-red-app-grp)# control GigabitEthernet 1/0/0 protocol 1
Device(config-red-app-grp)# timers delay 100 reload 400
Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 0/1/1
Device(config-red-app-grp)# asymmetric-routing always-divert enable
Device(config-red-app-grp)# end
```

例：インターフェイスでの冗長インターフェイス識別子および非対称ルーティングの設定

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/3
Device(config-if)# redundancy rii 600
Device(config-if)# redundancy group 1 decrement 20
Device(config-if)# redundancy asymmetric-routing enable
Device(config-if)# end
```

例：IPv6 ファイアウォールの設定

```
Device# configure terminal
Device(config)# vrf-definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
Device(config)# parameter-map type inspect ipv6-param-map
Device(config-profile)# sessions maximum 10000
Device(config-profile)# exit
Device(config)# ipv6 unicast-routing
Device(config)# ip port-map ftp port 8090 list ipv6-acl
Device(config)# ipv6 access-list ipv6-acl
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# class-map type inspect match-all ipv6-class
Device(config-cmap)# match access-group name ipv6-acl
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect ipv6-policy
Device(config-pmap)# class type inspect ipv6-class
Device(config-pmap-c)# inspect ipv6-param-map
Device(config-pmap-c)# end
```

例：非対称ルーティングのゾーンおよびゾーン ペアの設定

```
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security in-to-out source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0.1
Device(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
Device(config-if)# encapsulation dot1q 2
Device(config-if)# zone member security z1
Device(config-if)# end
```

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *10*：*IPv6* ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポートの機能情報

機能名	リリース	機能情報
IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポート	Cisco IOS XE Release 3.8S	IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポート機能は、IPv4 トラフィックと IPv6 トラフィックを同時に実行するファイアウォールでの非対称ルーティングをサポートします。 非対称ルーティングは、パケット処理のために、スタンバイ冗長グループからのパケットをアクティブな冗長グループに転送することをサポートします。 この機能がイネーブルでない場合、初期同期（SYN）メッセージを受信しなかったデバイスに転送されたリターン TCP パケットは、既存で既知のいずれのセッションにも属していないため、ドロップされます。 この機能によって導入または変更されたコマンドはありません。

第 9 章

ICMP のファイアウォール ステートフル インスペクション

ICMP のファイアウォール ステートフルインスペクション機能は、インターネット制御メッセージ プロトコル バージョン 4（ICMPv4）メッセージを悪意があるメッセージまたは良性メッセージとして分類します。 ファイアウォールは、ステートフル インスペクションを使用して、プライベート ネットワーク内で生成された良性 ICMPv4 メッセージを信頼し、関連する ICMP 応答のエントリがネットワークに入るのを許可します。 ICMP のファイアウォール ステートフル インスペクション機能を使用すると、ネットワーク管理者は ICMP を使用してネットワークの問題をデバッグすることができ、侵入者はネットワークに入れなくなります。

このモジュールでは、ICMPv4 メッセージのファイアウォール ステートフルインスペクションの概要、および ICMPv4 メッセージを検査するようにファイアウォールを設定する方法について説明します。

ICMP のファイアウォール ステートフル インスペクションの前提条件

- ICMP のファイアウォール ステートフル インスペクション機能を設定する前に、Cisco ファイアウォールを設定する必要があります。

- ネットワークで、すべての ICMP トラフィックがセキュリティ アプライアンス インターフェイスを通過できるようにする必要があります。
- セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックのアクセス ルールを設定する必要があります。

ICMP のファイアウォール ステートフル インスペクションの制約事項

この機能は、ICMP パケットの代わりに UDP データグラムが送信される UDP traceroute ユーティリティでは機能しません。 UDP traceroute は、UNIX システムのデフォルトです。 ファイアウォールで検査される ICMP traceroute パケットを生成する UNIX ホストでは、**traceroute** コマンドで「-I」オプションを使用します。

ICMP のファイアウォール ステートフル インスペクションについて

ICMP のファイアウォール ステートフル インスペクションの概要

インターネット制御メッセージ プロトコル（ICMP）は、ネットワークに関する情報を提供し、ネットワークでのエラーを報告するネットワーク プロトコルです。 ネットワーク管理者は、ICMP を使用して、ネットワーク接続の問題をデバッグします。プライベート ネットワークのトポロジの検出に ICMP を使用する潜在的な侵入者から保護するために、ICMPv4 メッセージをブロックしてプライベート ネットワークに入れないようにすることができます。ただし、ネットワーク管理者はネットワークをデバッグできなくなる可能性があります。

アクセス コントロール リスト（ACL）を使用して ICMPv4 メッセージを完全に許可するか拒否するように Cisco ルータを設定できます。 ICMPv4 メッセージに ACL を使用すると、メッセージ インスペクションは、設定済みの許可または拒否のアクションよりも優先されます。

IP プロトコルを使用する ICMPv4 メッセージは、次の 2 種類に分類できます。

- 単純な要求/応答メカニズムを利用する情報メッセージ。
- IP パケットの配信中に何らかのエラーが発生したことを示すエラー メッセージ。

（注） ICMP攻撃が宛先到達不能エラー メッセージを使用できないようにするには、セッションあたり1つの宛先到達不能エラー メッセージのみがファイアウォールで許可されるようにします。
ファイアウォールを通過する UDP セッションを処理しているホストは、宛先到達不能メッセージを使用して ICMP エラー パケットを生成する場合があります。 このような場合、そのセッションに対して1つの宛先到達不能メッセージのみがファイアウォールを通過できます。

次の ICMPv4 パケット タイプがサポートされます。

表 *11*：*ICMPv4* パケット タイプ

パケット タイプ	名前	説明
0	Echo Reply	エコー要求への応答（タイプ 8）。
3	Unreachable	任意の要求への考えられる応答。
8	Echo Request	ping または traceroute 要求。
11	Time Exceeded	パケットの存続可能時間（TTL）のサイズがゼロである場合の応答。
13	Timestamp Request	要求。
14	Timestamp Reply	タイムスタンプ要求への応答（タイプ13）。

ICMPv4 パケット タイプ 0 と 8 を使用して、宛先への ping を実行します。送信元は、エコー要求パケットを送信し、宛先はエコー応答パケットで応答します。 パケット タイプ 0、8、および 11 を ICMPv4 traceroute に使用し（つまり、送信されたエコー要求パケットは TTL サイズが 1 で始まります）、TTL のサイズはホップごとに増加します。 中間ホップでは時間超過パケットのエコー要求パケットに応答し、最終宛先がエコー応答パケットで応答します。

ICMPv4 エラー パケットが組み込みパケットの場合、組み込みパケットは、パケットに設定されたプロトコルとポリシーに基づいて処理されます。たとえば、組み込みパケットが TCP パケットで、パケットに drop アクションが設定されている場合、ICMPv4 に pass アクションが設定されている場合でも、パケットはドロップされます。

次のシナリオは、ICMPv4 パケットがファイアウォールを通過する方法を説明しています。

1 ICMPv4パケットは送信元インターフェイスに到着します。ファイアウォールは、パケットインスペクションを変更せずに、パケットの送信元および宛先アドレスを使用します。ファイアウォールは、セッション キーの作成および参照用に IP アドレス（送信元と宛先）、ICMP タイプ、およびプロトコルを使用します。

2 パケットは、ファイアウォール インスペクションに合格します。

3 リターン トラフィックは宛先インターフェイスで生じ、ICMPv4 メッセージ タイプに基づいて、ファイアウォールはセッション ルックアップ キーを作成します。

4 1 応答メッセージが情報メッセージの場合、ファイアウォールはパケット インスペクションのためにパケットの送信元および宛先アドレスを変更なしで使用します。 ここで、宛先ポートは ICMPv4 メッセージ要求タイプです。

2 応答メッセージが ICMPv4 エラー メッセージの場合、ファイアウォールは ICMP エラー パケットに存在するペイロード パケットを使用して、セッション ルックアップのセッション キーを作成します。

5 ファイアウォール セッション ルックアップが成功した場合、パケットは、ファイアウォール インスペクションに合格します。

ICMP インスペクションの確認

ICMP 戻りパケットは、アクセス コントロール リスト（ACL）ではなく、検査コードによって検査されます。 検査コードは、各発信パケットからの宛先アドレスを追跡し、各戻りパケットをチェックします。エコー応答パケットおよびタイムスタンプ応答パケットでは、リターンアドレスが検査されます。 到達不能パケットおよび時間超過パケットの場合、意図した宛先アドレスが、パケット データから抽出され、検査されます。

ICMP のファイアウォール ステートフル インスペクションの設定方法

ICMP のファイアウォール ステートフル インスペクションの設定

この作業を実行して、次を含む、ICMP のファイアウォール ステートフル インスペクションを設定します。

- ICMP トラフィックと一致するクラス マップ。
- 検査アクションを含むポリシー マップ。
- セキュリティ ゾーンとゾーン ペア（ファイアウォール ポリシー マップをゾーン ペアに付加するため）。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard*
4. **class-map type inspect** *class-map-name*
5. **match protocol** *protocol-name*
6. **exit**
7. **policy-map type inspect** *policy-map-name*
8. **class** *class-map-name*
9. **inspect**
10. **exit**
11. **exit**
12. **zone security** *zone-name*
13. **exit**
14. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
15. **service-policy type inspect** *policy-map-name*
16. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* 例： `Device(config)# access-list 102 permit icmp 192.168.0.1 255.255.255.0 192.168.2.22 255.255.255.0`	拡張 IP アクセス リストを定義します。

	コマンドまたはアクション	目的
ステップ 4	**class-map type inspect** *class-map-name* 例： `Device(config)# class-map type inspect c1`	アクションを実行する対象のクラスを定義し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 5	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol icmp`	指定されたプロトコルに基づくクラス マップの一致基準を設定します。
ステップ 6	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p1`	プロトコル固有検査タイプポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 8	**class** *class-map-name* 例： `Device(config-pmap)# class c1`	アクションを実行する対象のクラスを定義し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 10	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 11	**exit** 例： `Device(config-pmap)# exit`	QoS ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 12	**zone security** *zone-name* 例： `Device(config)# zone security z1`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定には、ゾーンペアを作成するために2つのセキュリティ ゾーン、送信元ゾーンと宛先ゾーンが含まれている必要があります。

	コマンドまたはアクション	目的
		• ゾーン ペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。
ステップ 13	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 14	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security inout source z1 destination z2`	インターフェイスを割り当てることができるゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 15	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect p1`	ファイアウォール ポリシー マップをゾーン ペアに付加します。
ステップ 16	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ICMP のファイアウォール ステートフル インスペクションの確認

次の **show** コマンドを任意の順序で使用できます。

手順の概要

1. **enable**
2. **show ip access-lists**
3. **show policy-map type inspect** *policy-map-name*
4. **show policy-map type inspect zone-pair** *zone-pair-name*
5. **show zone security** *zone-name*
6. **show zone-pair security** [**source** *source-zone* **destination** *destination-zone*]

手順の詳細

ステップ 1 **enable**

例：
```
Device> enable
```
特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **show ip access-lists**

例：
```
Device# show ip access-lists
```
指定したポリシー マップ情報を表示します。

ステップ 3 **show policy-map type inspect** *policy-map-name*

例：
```
Device# show policy-map type inspect p1
```
指定したポリシー マップ情報を表示します。

ステップ 4 **show policy-map type inspect zone-pair** *zone-pair-name*

例：
```
Device# show policy-map type inspect zone-pair inout
```
ゾーン ペアのランタイム検査タイプ ポリシーマップ統計情報を表示します。

ステップ 5 **show zone security** *zone-name*

例：
```
Device# show zone security z1
```
ゾーン セキュリティ情報を表示します。

ステップ 6 **show zone-pair security** [**source** *source-zone* **destination** *destination-zone*]

例：
```
Device# show zone-pair security source z1 destination z2
```
送信元ゾーンと宛先ゾーン、およびゾーン ペアに付加されたポリシーを表示します。

例：

show ip access-lists コマンドからの次のサンプル出力は、ping パケットだけがホストから発行された ICMP セッションに対して ACL がどのように作成されたかを示します。

```
Device# show ip access-lists

 Extended IP access list 102
     permit icmp any host 192.168.133.3 time-exceeded
     permit icmp any host 192.168.133.3 unreachable
     permit icmp any host 192.168.133.3 timestamp-reply
```

```
    permit icmp any host 192.168.133.3 echo-reply (4 matches)
```

次に、**show policy-map type inspect p1** コマンドの出力例を示します。

```
Device# show policy-map type inspect p1

 Policy Map type inspect p1
  Class c1
   Inspect
```

次に、**show policy-map type inspect zone-pair inout** コマンドの出力例を示します。

```
Device# show policy-map type inspect zone-pair inout

 Zone-pair: inout
  Service-policy : p1
   Class-map: c1 (match-all)
    Match: protocol icmp
    Inspect
     Session creations since subsystem startup or last reset 0
     Current session counts (estab/half-open/terminating) [0:0:0]
     Maxever session counts (estab/half-open/terminating) [0:0:0]
     Last session created never
     Last statistic reset never
     Last session creation rate 0
     half-open session total 0
   Class-map: class-default (match-any)
    Match: any
    Drop
     0 packets, 0 bytes
```

次に、**show zone security** コマンドの出力例を示します。

```
Device# show zone security

zone self
Description: System defined zone
```

次に、**show zone-pair security** コマンドの出力例を示します。

```
Device# show zone-pair security source z1 destination z2

zone-pair name inout
  Source-Zone z1  Destination-Zone z2
  service-policy p1
```

ICMP のファイアウォール ステートフル インスペクションの設定例

例：ICMP のファイアウォール ステートフル インスペクションの設定

```
Device# configure terminal
Device(config)# access-list 102 permit icmp 192.168.0.1 255.255.255.0 192.168.2.22
255.255.255.0
Device(config)# class-map type inspect c1
Device(config-cmap)# match protocol icmp
Device(config-cmap)# exit
Device(config)# policy-map type inspect p1
Device(config-pmap)# class c1
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# zone security z1
Device(config-sec-zone)# exit
```

```
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security inout source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect p1
Device(config-sec-zone-pair)# end
```

ICMP のファイアウォール ステートフル インスペクションの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 792	『*Internet Control Message Protocol*』
RFC 950	『*Internet Standard Subnetting Procedure*』
RFC 1700	『*Assigned Numbers*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ICMP のファイアウォール ステートフル インスペクションの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *12*：*ICMP* のファイアウォール ステートフル インスペクションの機能情報

機能名	リリース	機能情報
ICMP のファイアウォール ステートフル インスペクション	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.2S	ICMP のファイアウォール ステートフル インスペクション機能は、ICMPv4 メッセージを悪意があるメッセージまたは良性メッセージとして分類します。ファイアウォールは、ステートフル インスペクションを使用して、プライベート ネットワーク内で生成された良性 ICMP メッセージを信頼し、関連する ICMP 応答のエントリを許可します。

第 10 章

Skinny Client Control Protocol のファイアウォール サポート

Skinny Client Control Protocol のファイアウォール サポート機能により、Cisco IOS XE ファイアウォールは、VoIP および Skinny Client Control Protocol（SCCP）をサポートできます。 Cisco IP Phone は SCCP を使用して、Cisco Unified Communications Manager に接続および登録します。 スケーラブルな環境で IP フォンと Cisco Unified Communications Manager 間に Cisco IOS XE ファイアウォールを設定するには、ファイアウォールは SCCP を検出し、メッセージ内で渡される情報を理解する必要があります。 Skinny Client Control Protocol のファイアウォール サポート機能では、ファイアウォールは、Skinny クライアント（IP フォンなど）と Cisco Unified Communications Manager 間で交換される Skinny 制御パケットを検査し、Skinny データ チャネルがルータを経由できるようにルータを設定します。 この機能はビデオ チャネルに対応するために SCCP のサポートを拡張します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 こ

のモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

Skinny Client Control Protocol のファイアウォール サポートの前提条件

- Cisco IOS XE Release 2.1 以降のリリースをシステムで実行している必要があります。
- SCCP アプリケーション レベル ゲートウェイ（ALG）のファイアウォールが動作できるようにする必要があります。
- SCCP の TFTP ALG が動作できるようにする必要があります。これは、Skinny を使用する IP フォンが Cisco Unified Communications Manager の TFTP コンフィギュレーション ファイルを必要とするためです。

Skinny Client Control Protocol のファイアウォール サポートの制約事項

- IPv6 のアドレス検査およびアドレス変換はサポートされません。
- TCP セグメンテーションはサポートされません。

Skinny Client Control Protocol のファイアウォール サポートについて

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。 ALG は、アプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワークアドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。

- アプリケーション固有のコマンドを認識し、それらに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールはピンホールを開き、NATは、アプリケーション層データ ストリームの送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを実行します。IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションにはALGのサポートが必要です。

SCCP インスペクションの概要

SCCP インスペクションにより、Cisco Unified Communications Manager を使用して 2 つの SCCP クライアント間での音声通信が可能になります。 Cisco Unified Communications Managerは、TCP ポート2000（デフォルトのSCCPポート）を使用して、SCCPクライアントにサービスを提供します。最初に、SCCP クライアントは、TCP 接続を確立してプライマリ Cisco Unified Communications Manager に接続し、可能な場合は、セカンダリ Cisco Unified Communications Manager に接続します。 TCP 接続が確立されると、SCCP クライアントは、リブートまたはキープアライブ障害が発生するまでCisco Unified Communications Managerの制御として使用されるプライマリ Cisco Unified Communications Manager に登録します。 このため、SCCP クライアントと Cisco Unified Communications Manager 間の TCP 接続は永続し、クライアントへのコールやクライアントからのコールを確立するために使用されます。 TCP 接続が失敗すると、セカンダリ Cisco Unified Communications Manager が使用されます。 最初の Cisco Unified Communications Manager で確立されたすべてのデータ チャネルはアクティブなままとなり、コールが終了すると閉じられます。

SCCP プロトコルは、ローカルで生成または終了された SCCP 制御チャネルを検査し、ファイアウォールから発信された、またはファイアウォールを宛先とするメディア チャネルのピンホールを開くかまたは閉じます。ピンホールは、保護されたネットワークへのアプリケーション コントロール アクセスを可能にするために、ファイアウォールに開かれたポートです。

下の表に、データ セッションが開くまたは閉じるために必要なメッセージセットを一覧表示します。 SCCPインスペクションは、アクセス リスト ピンホールを開いたり閉じたりするために使用されるデータ セッションを検査します。

表 *13*：*SCCP* データ セッション メッセージ

Skinny インスペクション メッセージ	説明
CloseReceiveChannel	コールを中断する必要があることを示します。このメッセージを受信した場合、ファイアウォールおよびNATにより作成されたすべての中間セッションがクリーンアップされる必要があります。

Skinny インスペクション メッセージ	説明
OpenReceiveChannelACK	電話が、Cisco Unified Communications Manager から受信した OpenReceiveChannel メッセージを確認することを示します。
StartMediaTransmission	コールの送信元または宛先である電話のリアルタイム転送プロトコル（RTP）情報が含まれます。 メッセージには、IP アドレス、他の電話がリッスンしている RTP ポート、およびコールを一意に識別するコール ID が含まれます。
StopMediaTransmission	コールが終了したことを示します。セッションは、このメッセージの受信後にクリーンアップできます。
StationCloseReceiveChannel	Skinny クライアントに対して（このメッセージ内の情報に基づいて）受信チャネルを閉じるように指示します。
StationOpenMultiMediaReceiveChannelAck	このメッセージを送信する Skinny クライアントの IP アドレスとポート情報が含まれます。 クライアントがビデオおよびデータ チャネルを受信するかどうかのステータスが含まれます。
StationOpenReceiveChannelAck	このメッセージを送信する Skinny クライアントの IP アドレスとポート情報が含まれます。 このメッセージには、クライアントが音声トラフィックを受信するかどうかのステータスも含まれます。
StationStartMediaTransmission	リモート Skinny クライアントの IP アドレスとポート情報が含まれます。
StationStartMultiMediaTransmit	Cisco Unified Communications Manager がビデオまたはデータ チャネルの OpenLogicalChannelAck メッセージを受信したことを示します。
StationStopMediaTransmission	Skinny クライアントに対して（このメッセージ内の情報に基づいて）音声トラフィックの送信を停止するように指示します。
StationStopSessionTransmission	Skinny クライアントに対して（このメッセージ内の情報に基づいて）特定のセッションを終了するように指示します。

ALG--SCCP バージョン 17 のサポート

ALG—SCCP バージョン 17 サポート機能により、SCCP ALG は SCCP バージョン 17 パケットを解析できます。 Cisco Unified Communications Manager 7.0 および Cisco Unified Communications Manager 7.0 を使用する IP フォンは、SCCP バージョン 17 メッセージだけをサポートします。 SCCP の形式は、IPv6 をサポートするために、バージョン 17 から変更されました。 SCCP ALG は、メッセージのプレフィックス内の SCCP バージョンをチェックしてから、バージョンに応じて解析します。 SCCP メッセージバージョンは、メッセージヘッダーから抽出され、バージョン 17 よりも大きい場合、そのメッセージは、バージョン 17 形式を使用して解析され、IPv4 アドレスおよびポート情報が抽出されます。 SCCP ALG は、SCCP メッセージの IPv4 アドレス情報の検査および変換をサポートします。

（注） IPv6 のアドレス検査およびアドレス変換はサポートされません。

次の SCCP ALG 処理メッセージの IP アドレス形式は、バージョン 17 で変更されました。

- StationOpenMultiMediaReceiveChannelAck
- StationOpenReceiveChannelAckMessage
- StationRegisterMessage
- StationStartMediaTransmissionAckMessage
- StationStartMultiMediaTransmissionAckMessage
- StationStartMediaTransmissionMessage
- StationStartMultiMediaTransmissionMessage

Skinny Client Control Protocol のファイアウォール サポートの設定方法

Skinny クラス マップおよびポリシー マップの設定

ファイアウォールの設定で（**match protocol** コマンドを使用して）SCCP をイネーブルにしている場合、（**match protocol** コマンドを使用して）TFTP をイネーブルにする必要があります。そうしないと、SCCP を使用する IP フォンは Cisco Unified Communications Manager と通信できません。SCCP では、Cisco Unified Communications Manager を使用して、2 つの Skinny クライアント間での音声通信が可能です。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **match protocol** *protocol-name*
6. **exit**
7. **policy-map type inspect** *policy-map-name*
8. **class type inspect** *class-map-name*
9. **inspect**
10. **exit**
11. **class class-default**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Router(config)# class-map type inspect match-any cmap1`	検査タイプ クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Router(config-cmap)# match protocol skinny`	Skinny クラス マップの一致基準を設定します。
ステップ 5	**match protocol** *protocol-name* 例： `Router(config-cmap)# match protocol tftp`	TFTP クラス マップの一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Router(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了します。
ステップ 7	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect pmap1`	検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 8	**class type inspect** *class-map-name* 例： `Router(config-pmap)# class type inspect cmap1`	アクションを実行するクラスを指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**inspect** 例： `Router(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 10	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 11	**class class-default** 例： `Router(config-pmap)# class class-default`	これらのポリシーマップ設定が事前に定義したデフォルト クラスに適用されることを指定します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 12	**end** 例： `Router(config-pmap)# end`	ポリシー マップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーン ペアの設定および SCCP ポリシー マップの付加

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *zone-name*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name*	**default**} 例： `Router(config)# zone security zone1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Router(config)# zone security zone2`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]] 例： `Router(config)# zone-pair security in-out source zone1 destination zone2`	ゾーン ペアを作成し、セキュリティ ゾーン ペア コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect pmap1`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Router(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *zone-name* 例： `Router(config-if)# zone-member security zone1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。

	コマンドまたはアクション	目的
		（注） インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 13	**interface** *type number* 例： `Router(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**zone-member security** *zone-name* 例： `Router(config-if)# zone-member security zone2`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。
ステップ 15	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

Skinny Control Protocol のファイアウォール サポートの設定例

例：SCCP クラス マップおよびポリシー マップの設定

```
Router# configure terminal
Router(config)# class-map type inspect match-any cmap1
Router(config-cmap)# match protocol skinny
Router(config-cmap)# match protocol tftp
```

```
Router(config-cmap)# exit
Router(config)# policy-map type inspect pmap1
Router(config-pmap)# class type inspect cmap1
Router(config-pmap-c)# inspect
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap)# end
```

例：ゾーン ペアの設定および SCCP ポリシー マップの付加

```
Router# configure terminal
Router(config)# zone security zone1
Router(config-sec-zone)# exit
Router(config)# zone security zone2
Router(config-sec-zone)# exit
Router(config)# zone-pair security in-out source zone1 destination zone2
Router(config-sec-zone-pair)# service-policy type inspect pmap1
Router(config-sec-zone-pair)# exit
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# zone-member security zone1
Router(config-if)# exit
Router(config)# interface gigabitethernet 0/1/1
Router(config-if)# zone-member security zone2
Router(config-if)# end
```

Skinny Client Control Protocol のファイアウォール サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Skinny Client Control Protocol のファイアウォール サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *14*：*Skinny Client Control Protocol* のファイアウォール サポートの機能情報

機能名	リリース	機能情報
ALG—SCCP V17 サポート	Cisco IOS XE Release 3.5S	ALG—SCCP バージョン 17 サポート機能により、SCCP ALG は SCCP バージョン 17 パケットを解析できます。 SCCP 形式は、IPv6 をサポートするために、バージョン 17 から変更されました。

機能名	リリース	機能情報
ファイアウォール：SCCP ビデオ ALG サポート	Cisco IOS XE Release 2.4	SCCP では、Cisco Unified Communications Manager を使用して、2 つの Skinny クライアント間での音声通信が可能です。この機能により、Cisco ファイアウォールは Skinny クライアントと Cisco Unified Communications Manager の間で交換される Skinny 制御パケットを検査できます。 次のコマンドが変更されました。**match protocol**。
Skinny Client Control Protocol のファイアウォール サポート	Cisco IOS XE Release 2.1	Skinny Client Control Protocol のファイアウォール サポート機能により、Cisco IOS XE ファイアウォールは、VoIP および SCCP をサポートできます。Cisco IP Phone は SCCP を使用して、Cisco Unified Communications Manager に接続および登録します。 スケーラブルな環境で IP フォンと Cisco Unified Communications Manager 間に Cisco IOS XE ファイアウォールを設定するには、ファイアウォールは SCCP を検出し、メッセージ内で渡される情報を理解する必要があります。Skinny Client Control Protocol のファイアウォール サポート機能では、ファイアウォールは、Skinny クライアント（IP フォンなど）と Cisco Unified Communications Manager 間で交換される Skinny 制御パケットを検査し、Skinny データ チャネルがルータを経由できるようにルータを設定します。 この機能はビデオ チャネルに対応するために SCCP のサポートを拡張します。

第 11 章

VRF-Aware Software インフラストラクチャの設定

VRF-Aware Software インフラストラクチャ（VASI）機能を使用すると、アクセス コントロール リスト（ACL）、ネットワーク アドレス変換（NAT）、ポリシング、ゾーンベース ファイアウォールなどのサービスを、2 つの異なる仮想ルーティングおよび転送（VRF）インスタンスを通過するトラフィックに適用できます。 VASI インターフェイスは、ルート プロセッサ（RP）と転送プロセッサ（FP）の冗長性をサポートします。 VASI インターフェイスは、IPv4 および IPv6 ユニキャスト トラフィックをサポートします。

このモジュールでは、VASI インターフェイスを設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

VRF-Aware Software インフラストラクチャの設定の制約事項

- VASI インターフェイス上のマルチプロトコル ラベル スイッチング（MPLS）トラフィックはサポートされません。
- IPv4 および IPv6 マルチキャスト トラフィックはサポートされません。
- VASI インターフェイスは、キュー ベースの機能の付加をサポートしません。 次のコマンドは、VASI インターフェイスに接続されたモジュラ QoS CLI（MQC）ポリシーではサポートされません。
  - **bandwidth**（**policy-map クラス**）
  - **fair-queue**
  - **priority**
  - **queue-limit**
  - **random-detect**
  - **shape**
- 外部ボーダー ゲートウェイ プロトコル（eBGP）はサポートされません。

VRF-Aware Software インフラストラクチャの設定について

VASI の概要

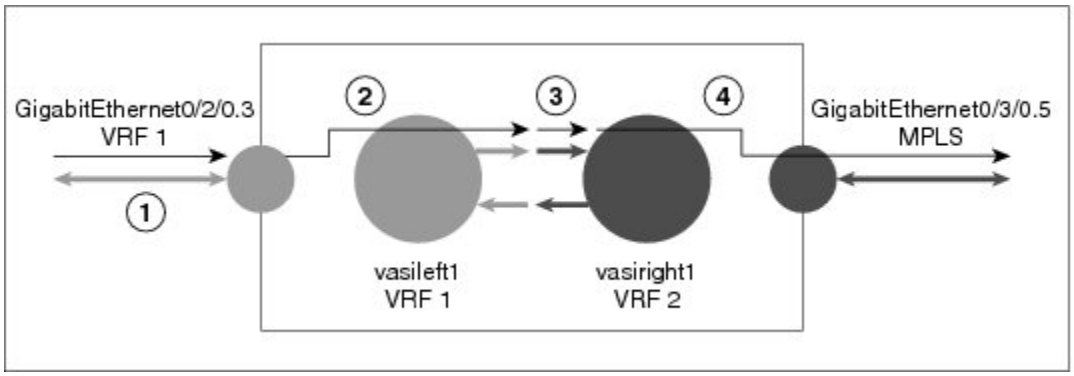
VRF-Aware Software インフラストラクチャ（VASI）を使用すると、ファイアウォール、IPsec、ネットワーク アドレス変換（NAT）などのサービスを、異なる仮想ルーティングおよび転送（VRF）インスタンスを通過するトラフィックに適用できます。 VASI は、仮想インターフェイスのペアを使用して実装され、ペアの各インターフェイスは異なる VRF インスタンスに関連付けられます。 VASI 仮想インターフェイスは、これら 2 つの VRF インスタンス間で交換される必要があるパケットのネクスト ホップ インターフェイスです。 VASI インターフェイスは、VRF インスタンス間のファイアウォールまたは NAT を設定するためのフレームワークを提供します。

各インターフェイス ペアは、異なる 2 つの VRF インスタンスに関連付けられています。 ペアリングの関連付けは、vasileft x が自動的に vasiright x へのペアを取得するという方法で、2 つのインターフェイスのインデックスに基づいて自動的に行われます。 たとえば、vasileft1 および vasiright1 は自動的にペアとなり、vasileft1 に入るパケットは、vasiright1 に内部的に渡されます。

VASI インターフェイス上で内部ボーダー ゲートウェイ プロトコル（iBGP）、Enhanced Interior Gateway Routing Protocol（EIGRP）、または Open Shortest Path First（OSPF）によるスタティック ルーティングまたはダイナミック ルーティングを設定できます。 iBGP ダイナミック ルーティング プロトコルの制約事項とコンフィギュレーションは、VASI インターフェイス間の iBGP ルーティング コンフィギュレーションに有効です。

次の図は、同じデバイス上の Inter-VRF VASI 設定を示します。

図 *19*：*Inter-VRF VASI* の設定



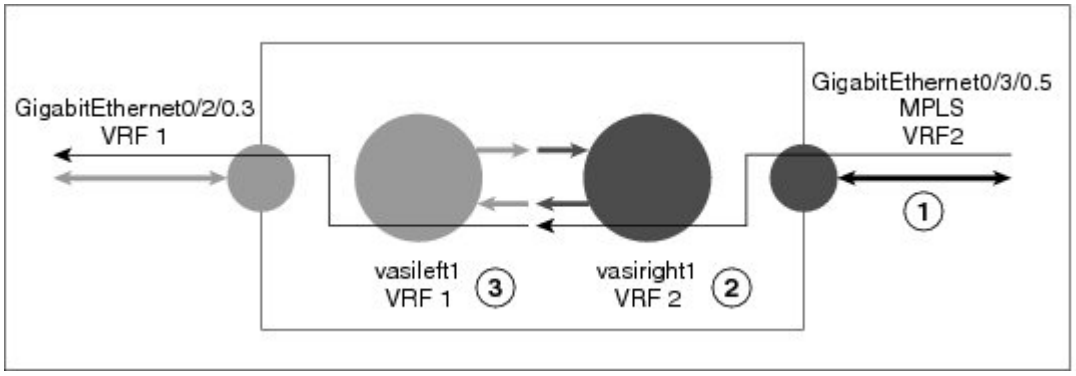
Inter-VRF VASI が同じデバイス上で設定されている場合、パケット フローは次の順序で発生します。

1. パケットは、VRF1（ギガビット イーサネット 0/2/0.3）に属する物理インターフェイスに入ります。
2. パケットを転送する前に、VRF1 ルーティング テーブルでのフォワーディング ルックアップが実行されます。 Vasileft1 は、ネクスト ホップとして選択され、存続可能時間（TTL）値がパケットから減らされます。 通常、転送アドレスは、VRF のデフォルト ルートに基づいて選択されます。 ただし、転送アドレスがスタティック ルートまたは学習されたルートになる場合もあります。 パケットは vasileft1 の出力パスに送信され、次に vasiright1 入力パスに自動的に送信されます。
3. パケットが vasiright1 に入ると、フォワーディング ルックアップが VRF2 ルーティング テーブルで行われ、TTL が再び減らされます（このパケットでは 2 回目）。
4. VRF2 は、パケットを物理インターフェイス、ギガビット イーサネット 0/3/0.5 に転送します。

次の図は、VASI がマルチ プロトコル ラベル スイッチング（MPLS）VPN 設定で動作する仕組みを示しています。

（注） 次の図で、MPLS はギガビット イーサネット インターフェイスでイネーブルですが、MPLS トラフィックは、VASI ペア間ではサポートされていません。

図 *20*：*MPLS VPN* 設定での *VASI*



VASI がマルチ プロトコル ラベル スイッチング（MPLS）VPN に設定されている場合、パケット フローは次の順序で発生します。

1. パケットは、VPN ラベルが付けられて MPLS インターフェイスに到着します。
2. VPN ラベルはパケットから取り除かれ、フォワーディング ルックアップが VRF2 内で実行され、パケットは vasiright1 に転送されます。 TTL 値はパケットから減らされます。
3. パケットが入力パスの vasileft1 に入ると、別のフォワーディング ルックアップが VRF1 で行われます。 パケットは、VRF1（ギガビット イーサネット 0/2/0.3）の出力物理インターフェイスに送信されます。 TTL 値はパケットから再び減らされます。

VRF-Aware Software インフラストラクチャの設定方法

VASI インターフェイス ペアの設定

VASI インターフェイス ペアを設定するには、1 つのインターフェイスで **interface vasileft** コマンドを設定し、2 つ目のインターフェイスで **interface vasiright** コマンドを設定する必要があります。 任意の VASI インターフェイスで VRF インスタンスを設定できます。 VASI インターフェイス ペアを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *table-name*
5. **ip address** {*ip-address mask* [**secondary**] | **pool** *pool-name*}
6. **exit**
7. **interface** *type number*
8. **vrf forwarding** *table-name*
9. **ip address** {*ip-address mask* [**secondary**] | **pool** *pool-name*}
10. **exit**
11. **ip route** [**vrf** *vrf-name*] *destination-prefix destination-prefix-mask interface-type interface-number*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface vasileft 200`	VASIインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • この例では、vasileft インターフェイスが設定されます。
ステップ 4	**vrf forwarding** *table-name* 例： `Device(config-if)# vrf forwarding table1`	VRF テーブルを設定します。 （注） VRF 転送は、任意の VASI インターフェイス上で設定できます。 両方の VASI インターフェイスで VRF インスタンスを設定する必要はありません。

	コマンドまたはアクション	目的
ステップ 5	**ip address** {*ip-address mask* [**secondary**] | **pool** *pool-name*} 例： `Device(config-if)# ip address 192.168.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 7	**interface** *type number* 例： `Device(config)# interface vasiright 200`	VASIインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 • この例では、vasiright インターフェイスが設定されます。
ステップ 8	**vrf forwarding** *table-name* 例： `Device(config-if)# vrf forwarding table1`	VRF テーブルを設定します。
ステップ 9	**ip address** {*ip-address mask* [**secondary**] | **pool** *pool-name*} 例： `Device(config-if)# ip address 192.168.1.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 10	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 11	**ip route** [**vrf** *vrf-name*] *destination-prefix destination-prefix-mask interface-type interface-number* 例： `Device(config)# ip route vrf vrf1 10.0.0.1 255.255.0.0 vasileft 200`	VRF インスタンスおよび VASI インターフェイスのスタティック ルートを確立します。 （注） VRF インスタンスの IP ルートを追加するには、**vrf** キーワードを指定する必要があります。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

VRF-Aware Software インフラストラクチャの設定例

例：VASI インターフェイスの設定

VRF インスタンスは、VASI ペア（vasileft と vasiright）の各インターフェイスでイネーブルになっている必要があります。

```
Device(config)# interface vasileft 200
Device(config-if)# vrf forwarding table1
Device(config-if)# ip address 192.168.0.1 255.255.255.0
Device(config-if)# exit
Device(config)# ip route vrf vrf1 10.0.0.1 255.255.0.0 vasileft 200
Device(config)# interface vasiright 200
Device(config-if)# vrf forwarding table2
Device(config-if)# ip address 192.168.1.1 255.255.255.0
Device(config-if)# exit
Device(config)# ip route 10.0.0.2 255.255.255.0 vasiright 200
```

VRF-Aware Software インフラストラクチャの設定の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VRF-Aware Software インフラストラクチャの設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *15*：*VRF-Aware Software* インフラストラクチャの設定の機能情報

機能名	リリース	機能情報
VRF-Aware Softwareインフラストラクチャ	Cisco IOS XE Release 2.6	VRF-Aware Software インフラストラクチャ機能を使用すると、ACL、NAT、ポリシング、ゾーンベース ファイアウォールなどのサービスを、2つの異なるVRFインスタンス上を流れるトラフィックに適用できます。 VASI インターフェイスは、RP および FP の冗長性をサポートします。 この機能は、VASIインターフェイスでの IPv4 および IPv6 ユニキャスト トラフィックをサポートします。
VASI（VRF-Aware Software インフラストラクチャ）拡張機能 フェーズ I	Cisco IOS XE Release 3.1S	VASI 機能拡張のフェーズ II 機能は、VASI に次の拡張機能を提供します。 • 500 VASIインターフェイスのサポート。 • VASI インターフェイス間の iBGP ダイナミック ルーティングのサポート。
VASI（VRF-Aware Software インフラストラクチャ）拡張機能 フェーズ II	Cisco IOS XE Release 3.2S	VASI 機能拡張のフェーズ II 機能は、VASI に次の拡張機能を提供します。 • VASI インターフェイス上の IPv6 ユニキャスト トラフィックのサポート。 • VASI インターフェイス間の OSPF および EIGRP ダイナミック ルーティングのサポート。
VASI（VRF-Aware Software インフラストラクチャ）スケール	Cisco IOS XE Release 3.3S	VASI スケール機能は 1000 VASI インターフェイスをサポートします。 次のコマンドが、新たに導入または変更されました。**interface (VASI)**。

第 12 章

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポート

この機能は、IPv6 ファイアウォールを介した VRF-Aware サービス インフラストラクチャ（VASI）のインターフェイスをサポートします。 この機能を使用すると、アクセス コントロール リスト（ACL）、ネットワーク アドレス変換（NAT）、ポリシング、ゾーンベース ファイアウォールなどのサービスを、2 つの異なる仮想ルーティングおよび転送（VRF）インスタンスを通過するトラフィックに適用できます。 VASI インターフェイスは、ルート プロセッサ（RP）と転送プロセッサ（FP）の冗長性をサポートします。 VASI インターフェイスは、IPv4 および IPv6 ユニキャスト トラフィックをサポートします。

このモジュールでは、VASI インターフェイスに関する情報を提供し、VASI インターフェイスを設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートの制約事項

- VRF-Aware Software インフラストラクチャ（VASI）インターフェイス上のマルチプロトコル ラベル スイッチング（MPLS）トラフィックはサポートされません。
- IPv4 および IPv6 マルチキャスト トラフィックはサポートされません。
- VASI インターフェイスは、キュー ベースの機能の付加をサポートしません。 次のコマンドは、VASI インターフェイスに接続されたモジュラ QoS CLI（MQC）ポリシーではサポートされません。
  - **bandwidth**（**policy-map クラス**）
  - **fair-queue**
  - **priority**
  - **queue-limit**
  - **random-detect**
  - **shape**

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートについて

VASI の概要

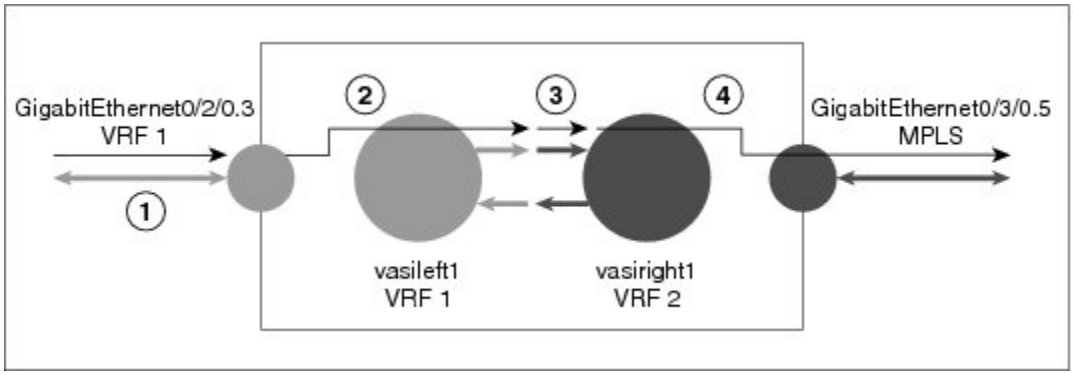
VRF-Aware Software インフラストラクチャ（VASI）を使用すると、ファイアウォール、IPsec、ネットワーク アドレス変換（NAT）などのサービスを、異なる仮想ルーティングおよび転送（VRF）インスタンスを通過するトラフィックに適用できます。 VASI は、仮想インターフェイスのペアを使用して実装され、ペアの各インターフェイスは異なる VRF インスタンスに関連付けられます。 VASI 仮想インターフェイスは、これら 2 つの VRF インスタンス間で交換される必要があるパケットのネクスト ホップ インターフェイスです。 VASI インターフェイスは、VRF インスタンス間のファイアウォールまたは NAT を設定するためのフレームワークを提供します。

各インターフェイス ペアは、異なる 2 つの VRF インスタンスに関連付けられています。 ペアリングの関連付けは、vasileft x が自動的に vasiright x へのペアを取得するという方法で、2 つのインターフェイスのインデックスに基づいて自動的に行われます。 たとえば、vasileft1 および vasiright1 は自動的にペアとなり、vasileft1 に入るパケットは、vasiright1 に内部的に渡されます。

VASI インターフェイス上で内部ボーダー ゲートウェイ プロトコル（iBGP）、Enhanced Interior Gateway Routing Protocol（EIGRP）、または Open Shortest Path First（OSPF）によるスタティック ルーティングまたはダイナミック ルーティングを設定できます。 iBGP ダイナミック ルーティング プロトコルの制約事項とコンフィギュレーションは、VASI インターフェイス間の iBGP ルーティング コンフィギュレーションに有効です。

次の図は、同じデバイス上の Inter-VRF VASI 設定を示します。

図 *21*：*Inter-VRF VASI* の設定



Inter-VRF VASI が同じデバイス上で設定されている場合、パケット フローは次の順序で発生します。

1 パケットは、VRF1（ギガビット イーサネット 0/2/0.3）に属する物理インターフェイスに入ります。

2 パケットを転送する前に、VRF1ルーティングテーブルでのフォワーディングルックアップが実行されます。 Vasileft1 は、ネクスト ホップとして選択され、存続可能時間（TTL）値がパケットから減らされます。 通常、転送アドレスは、VRF のデフォルト ルートに基づいて選択されます。 ただし、転送アドレスがスタティック ルートまたは学習されたルートになる場合もあります。 パケットは vasileft1 の出力パスに送信され、次に vasiright1 入力パスに自動的に送信されます。

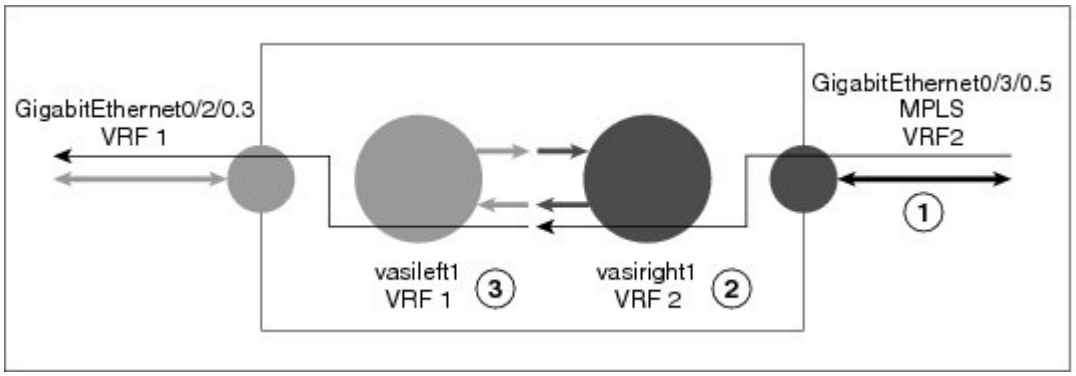
3 パケットが vasiright1 に入ると、フォワーディング ルックアップが VRF2 ルーティング テーブルで行われ、TTL が再び減らされます（このパケットでは 2 回目）。

4 VRF2 は、パケットを物理インターフェイス、ギガビット イーサネット 0/3/0.5 に転送します。

次の図は、VASI がマルチ プロトコル ラベル スイッチング（MPLS）VPN 設定で動作する仕組みを示しています。

（注） 次の図で、MPLS はギガビット イーサネット インターフェイスでイネーブルですが、MPLS トラフィックは、VASI ペア間ではサポートされていません。

図 *22*：*MPLS VPN* 設定での *VASI*



VASI がマルチ プロトコル ラベル スイッチング（MPLS）VPN に設定されている場合、パケットフローは次の順序で発生します。

1 パケットは、VPN ラベルが付けられて MPLS インターフェイスに到着します。

2 VPN ラベルはパケットから取り除かれ、フォワーディング ルックアップが VRF2 内で実行され、パケットは vasiright1 に転送されます。 TTL 値はパケットから減らされます。

3 パケットが入力パスの vasileft1 に入ると、別のフォワーディング ルックアップが VRF1 で行われます。 パケットは、VRF1（ギガビット イーサネット 0/2/0.3）の出力物理インターフェイスに送信されます。 TTL 値はパケットから再び減らされます。

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートの設定方法

VRF およびアドレス ファミリ セッションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition VRF1`	仮想ルーティングおよび転送（VRF）ルーティング テーブル インスタンスを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	アドレス ファミリ コンフィギュレーション モードを開始して、標準 IPv6 アドレス プレフィックスを伝送するセッションを設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了し、VRF コンフィギュレーション モードを開始します。
ステップ 6	**end** 例： `Device(config-vrf)# end`	VRF コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

VASI サポートのクラス マップとポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **class-map type inspect match-any** *class-map-name*
5. **match protocol** *name*
6. **match protocol** *name*
7. **exit**
8. **policy-map type inspect** *policy-map-name*
9. **class type inspect** *class-map-name*
10. **inspect**
11. **exit**
12. **class class-default**
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6-unicast routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any c-map`	検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 5	**match protocol** *name* 例： `Device(config-cmap)# match protocol icmp`	指定されたプロトコルに基づくクラスマップの一致基準を設定します。
ステップ 6	**match protocol** *name* 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルに基づくクラスマップの一致基準を設定します。
ステップ 7	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p-map`	プロトコル固有検査タイプ ポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 9	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect c-map`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 10	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoSポリシーマップ コンフィギュレーション モードを開始します。
ステップ 12	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシーマップ設定を定義済みのデフォルト クラスに適用して、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 13	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

VASI のサポートのゾーンおよびゾーン ペアの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
6. **service-policy type inspect** *policy-map-name*
7. **exit**
8. **interface** *type number*
9. **vrf forwarding** *vrf-name*
10. **no ip address**
11. **zone member security** *zone-name*
12. **ipv6 address** *ipv6-address*/*prefix-length*
13. **ipv6 enable**
14. **negotiation auto**
15. **exit**
16. **interface** *type number*
17. **no ip address**
18. **ipv6 address** *ipv6-address*/*prefix-length*
19. **ipv6 enable**
20. **negotiation auto**
21. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**zone security** *zone-name* 例： `Device(config)# zone security in`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定には、ゾーンペアを作成するために、2つのセキュリティゾーン（送信元ゾーンと宛先ゾーン）が含まれている必要があります。 • ゾーンペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティゾーン コンフィギュレーションモードを終了し、グローバル コンフィギュレーションモードを開始します。
ステップ 5	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security in-out source in destination out`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 • ポリシーを適用するには、ゾーンペアを設定する必要があります。
ステップ 6	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect p-map`	ポリシーマップをトップレベル ポリシーマップに付加します。 • ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 7	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティゾーンペア コンフィギュレーションモードを終了し、グローバル コンフィギュレーションモードを開始します。
ステップ 8	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding VRF1`	インターフェイスまたはサブインターフェイスに仮想ルーティングおよび転送（VRF）インスタンスまたは仮想ネットワークを関連付けます。

	コマンドまたはアクション	目的
ステップ 10	**no ip address** 例： `Device(config-if)# no ip address`	IP アドレスを削除するか、IP 処理をディセーブルにします。
ステップ 11	**zone member security** *zone-name* 例： `Device(config-if)# zone member security in`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 12	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:2:1234/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 13	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 14	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイス上で速度、デュプレックス モード、およびフロー制御のアドバタイズをイネーブルにします。
ステップ 15	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 16	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 17	**no ip address** 例： `Device(config-if)# no ip address`	IP アドレスを削除するか、IP 処理をディセーブルにします。
ステップ 18	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:3:1234/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 19	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 20	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイス上で速度、デュプレックス モード、およびフロー制御のアドバタイズをイネーブルにします。
ステップ 21	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

VASI インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **ipv6 address** *ipv6-address*/*prefix-length* **link-local**
6. **ipv6 address** *ipv6-address*/*prefix-length*
7. **ipv6 enable**
8. **no keepalive**
9. **zone member security** *zone-name*
10. **exit**
11. **interface** *type number*
12. **ipv6 address** *ipv6-address*/*prefix-length* **link-local**
13. **ipv6 address** *ipv6-address*/*prefix-length*
14. **ipv6 enable**
15. **no keepalive**
16. **exit**
17. **ipv6 route** *ipv6-prefix*/*prefix-length interface-type interface-number ipv6-address*
18. **ipv6 route vrf** *vrf-name ipv6-prefix*/*prefix-length interface-type interface-number ipv6-address*
19. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface vasileft 1`	VASI インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding VRF1`	インターフェイスまたはサブインターフェイスに仮想ルーティングおよび転送（VRF）インスタンスまたは仮想ネットワークを関連付けます。
ステップ 5	**ipv6 address** *ipv6-address*/*prefix-length* **link-local** 例： `Device(config-if)# ipv6 address FE80::8EB6:4FFF:FE6C:E701 link-local`	インターフェイスの IPv6 リンクローカルアドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ステップ 6	**ipv6 address** *ipv6-address*/*prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:4:1234/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 7	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 8	**no keepalive** 例： `Device(config-if)# no keepalive`	キープアライブ パケットをディセーブルにします。
ステップ 9	**zone member security** *zone-name* 例： `Device(config-if)# zone member security out`	インターフェイスをセキュリティ ゾーンにアタッチします。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 11	**interface** *type number* 例： `Device(config)# interface vasiright 1`	VASI インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**ipv6 address** *ipv6-address*/*prefix-length* **link-local** 例： `Device(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local`	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ステップ 13	**ipv6 address** *ipv6-address*/*prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:4:1234/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 14	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 15	**no keepalive** 例： `Device(config-if)# no keepalive`	キープアライブ パケットをディセーブルにします。
ステップ 16	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 17	**ipv6 route** *ipv6-prefix*/*prefix-length* *interface-type interface-number ipv6-address* 例： `Device(config)# ipv6 route 2001::/64 vasileft 1 2001::/64`	スタティック IPv6 ルートを確立します。
ステップ 18	**ipv6 route vrf** *vrf-name* *ipv6-prefix*/*prefix-length interface-type interface-number ipv6-address*	IPv6 アドレスのすべての VRF テーブルまたは特定の VRF テーブルを指定します。

	コマンドまたはアクション	目的
	例： `Device(config)# ipv6 route vrf vrf1 2001::/64 vasiright 1 2001::/64`	
ステップ 19	**end** 例： `Device(config# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートの設定例

例：VRF およびアドレス ファミリ セッションの設定

```
Device# configure terminal
Device(config)# vrf definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# end
```

例：VASI サポートのクラス マップとポリシー マップの設定

```
Device# configure terminal
Device(config)# ipv6-unicast routing
Device(config)# class-map type inspect match-any c-map
Device(config-cmap)# match protocol icmp
Device(config-cmap)# match protocol tcp
Device(config-cmap)# match protocol udp
Device(config-cmap)# exit
Device(config)# policy-map type inspect p-map
Device(config-pmap)# class type inspect c-map
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# end
```

例：VASI のサポートのゾーンおよびゾーン ペアの設定

```
Device# configure terminal
Device(config)# zone security in
Device(config)# exit
Device(config)# zone security out
Device(config)# exit
Device(config)# zone-pair security in-out source in destination out
```

```
Device(config-sec-zone-pair)# service-policy type inspect p-map
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# vrf forwarding VRF1
Device(config-if)# no ip address
Device(config-if)# zone member security in
Device(config-if)# ipv6 address 2001:DB8:2:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# negotiation auto
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:DB8:3:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# negotiation auto
Device(config-if)# end
```

例：VASI インターフェイスの設定

```
Device# configure terminal
Device(config)# interface vasileft 1
Device(config-if)# vrf forwarding VRF1
Device(config-if)# ipv6 address FE80::8EB6:4FFF:FE6C:E701 link-local
Device(config-if)# ipv6 address 2001:DB8:4:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# no keepalive
Device(config-if)# zone-member security out
Device(config-if)# exit
Device(config)# interface vasiright 1
Device(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
Device(config-if)# ipv6 address 2001:DB8:4:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# no keepalive
Device(config-if)# exit
Device(config)# ipv6 route 2001::/64 vasileft 1 2001::/64
Device(config)# ipv6 route vrf vrf1 2001::/64 vasiright 1 2001::/64
Device(config)# end
```

ファイアウォールステートフルシャーシ間冗長性の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *16*：*VASI* インターフェイス経由の *IPv6* ゾーンベース ファイアウォール サポートの機能情報

機能名	リリース	機能情報
VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポート	Cisco IOS XE Release 3.7S	この機能は、IPv6 ファイアウォール経由の VASI インターフェイスをサポートします。 この機能を使用すると、アクセス コントロール リスト（ACL）、ネットワーク アドレス変換（NAT）、ポリシング、ゾーンベース ファイアウォールなどのサービスを、2 つの異なる仮想ルーティングおよび転送（VRF）インスタンスを通過するトラフィックに適用できます。 VASI インターフェイスは、ルートプロセッサ（RP）と転送プロセッサ（FP）の冗長性をサポートします。 VASI インターフェイスは、IPv4 および IPv6 ユニキャスト トラフィックをサポートします。 この機能について導入または変更されたコマンドはありません。

第 13 章

分散型サービス拒否攻撃に対する保護

分散型サービス拒否攻撃に対する保護機能は、グローバル レベルで（すべてのファイアウォール セッションに対して）および VPN ルーティングおよび転送（VRF）レベルで、サービス拒否（DoS）攻撃から保護します。 Cisco IOS XE Release 3.4S 以降のリリースでは、分散型 DoS 攻撃を防ぐために、ファイアウォール セッションのアグレッシブ エージング、ファイアウォール セッションのイベント レート モニタリング、ハーフ オープン接続制限、およびグローバル TCP SYN Cookie 保護を設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

分散型サービス拒否攻撃に対する保護について

ファイアウォール セッションのアグレッシブ エージング

アグレッシブエージング機能により、ファイアウォールは、セッションを積極的にエージングアウトして、新しいセッションのためのスペースを確保することで、ファイアウォール セッション データベースがいっぱいになるのを防ぐことができます。 ファイアウォールは、アイドル セッションを削除して、そのリソースを保護します。アグレッシブエージング機能により、ファイアウォール セッションが存在できる時間は、エージングアウト時間と呼ばれる、タイマーで定義された時間よりも短くなります。

アグレッシブエージング機能には、アグレッシブエージング期間の開始と終了を定義するしきい値（高ウォーターマークと低ウォーターマーク）が含まれます。 アグレッシブ エージング期間は、セッション テーブルが高ウォーターマークを超えると開始され、低ウォーターマーク以下になると終了します。アグレッシブエージング期間中、セッションは、エージングアウト時間を使用して設定された期間よりも短い期間存在します。 攻撃者が、ファイアウォールがセッションを終了するレートよりも短い時間でセッションを開始する場合、セッションを作成するために割り当てられているすべてのリソースが使用され、新しいすべての接続が拒否されます。 このような攻撃を防ぐには、セッションを積極的にエージングアウトするようにアグレッシブエージング機能を設定できます。 この機能はデフォルトで無効に設定されています。

ボックス レベル（ボックスはファイアウォール セッション テーブル全体を示します）および仮想ルーティングおよび転送（VRF）レベルでハーフ オープン セッションおよび総セッションにアグレッシブエージングを設定できます。この機能を総セッションに設定している場合、ファイアウォールセッション リソースを消費するすべてのセッションが考慮されます。 総セッションは、確立されているセッション、ハーフ オープン セッション、および明確でないセッション データベース内のセッションで構成されます。（確立状態にまだ到達していないTCPセッションはハーフ オープン セッションと呼ばれます）。

ファイアウォールには、2 つのセッション データベース（セッション データベースおよび明確でないセッション データベース）があります。 セッション データベースには、5 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）のセッションが含まれます。 タプルは、要素の順序付きリストです。 明確でないセッション データベースには、5 タプルよりも少ない（IP アドレスやポート番号などが欠落している）セッションが含まれます。ハーフ オープン セッションのアグレッシブ エージングの場合、ハーフ オープン セッションだけが考慮されます。

インターネット制御メッセージ プロトコル（ICMP）、TCP、および UDP のファイアウォール セッションにアグレッシブ エージング アウト時間を設定できます。 エージング アウト時間は、デフォルトでアイドル時間に設定されます。

イベント レート モニタリング機能

イベント レート モニタリング機能は、ゾーンの定義済みイベントのレートをモニタします。 イベント レート モニタリング機能には基本脅威検出が含まれます。これにより、セキュリティ デバイスは、ファイアウォールの内側にあるリソースへの考えられる脅威、異常や攻撃を検出し、それに対するアクションを実行できます。イベントの基本脅威検出レートを設定できます。 特定のタイプのイベントの着信レートが、設定された脅威検出レートを超えると、イベント レート モニタリングはこのイベントを脅威と見なし、脅威を停止するアクションを実行します。 脅威検出は、入力のゾーンだけでイベントを検査します（イベント レート モニタリング機能が入力ゾーンでイネーブルの場合）。

ネットワーク管理者は、アラート メッセージ（syslog または高速ロガー（HSL））を介して潜在的な脅威について通知され、攻撃ベクトルの検出、攻撃の発生元のゾーンの検出、特定の動作やトラフィックをブロックするようネットワークのデバイスを設定するなどのアクションを実行できます。

イベント レート モニタリング機能では、次のタイプのイベントをモニタします。

- 基本的なファイアウォール チェック エラーが原因でファイアウォールがドロップする：これには、ゾーンまたはゾーン ペアのチェック エラー、または drop アクションを使用して設定されたファイアウォール ポリシーなどが含まれる場合があります。
- レイヤ 4 インスペクション エラーが原因でファイアウォールがドロップする：これには、最初の TCP パケットが同期（SYN）パケットではないため失敗した TCP インスペクションが含まれる場合があります。
- TCP SYN Cookie 攻撃：これには、ドロップされた SYN パケット数、およびスプーフィング攻撃として送信された SYN Cookie の数の集計が含まれる場合があります。

イベント レート モニタリング機能では、異なるイベントの平均レートとバースト レートをモニタします。 各イベント タイプには、設定可能なパラメータ セット（平均しきい値、バーストしきい値、および期間）が含まれる関連レートによって制御されるレート オブジェクトがあります。 期間はタイム スロットに分割されています。各タイム スロットは、期間の 1/30 です。

平均レートは、イベント タイプごとに計算されます。 各レート オブジェクトは、30 の完了済みサンプリング値に加えて、現在稼働中のサンプリング期間を保持するための 1 つの値を保持します。 現在のサンプリング値によって計算済みの最も古い値が置き換えられ、平均が計算されます。 平均レートは、各期間で計算されます。 平均レートが平均しきい値を超えると、イベント レート モニタリング機能は、これを潜在的な脅威と見なし、統計情報を更新し、ネットワーク管理者に通知します。

バースト レートは、トークン バケット アルゴリズムを使用して実装されます。 各タイム スロットでは、トークン バケットがトークンで埋められます。 発生する（特定のイベント タイプの）イベントごとに、トークンがバケットから削除されます。 空のバケットは、バーストしきい値に到達したことを意味し、管理者は syslog または HSL を介してアラームを受信します。 脅威検出統計情報の確認、およびゾーンのさまざまなイベントに対する潜在的脅威についての学習は、**show policy-firewall stats zone** コマンドの出力から行うことができます。

threat-detection basic-threat コマンドを使用して、最初に基本脅威検出をイネーブルにする必要があります。 基本脅威検出を設定すると、脅威検出レートを設定できます。 脅威検出レートを設定するには、**threat-detection rate** コマンドを使用します。

次の表に、イベント レート モニタリング機能がイネーブルの場合に適用可能な基本脅威検出のデフォルト設定を示します。

表 *17*：基本脅威検出のデフォルト設定

パケット ドロップの理由	脅威検出の設定
基本的なファイアウォール ドロップ	平均レート 400 パケット/秒（pps） バースト レート 1600 pps レート間隔 600 秒
インスペクション ベースのファイアウォール ドロップ	平均レート 400 pps バースト レート 1600 pps レート間隔 600 秒
SYN 攻撃ファイアウォール ドロップ	平均レート 100 pps バースト レート 200 pps レート間隔 600 秒

ハーフ オープン接続制限

ファイアウォール セッション テーブルは、ハーフ オープン ファイアウォール接続の制限をサポートします。 ハーフ オープン セッションの数を制限すると、ボックス単位レベルまたは仮想ルーティングおよび転送（VRF）レベルでハーフ オープン セッションを使用してファイアウォール セッション テーブルを満たす可能性がある攻撃からファイアウォールを守り、セッションが確立されるのを防ぎます。 ハーフ オープン接続制限は、レイヤ 4 プロトコル、インターネット制御メッセージ プロトコル（ICMP）、TCP、および UDP に設定できます。 UDP ハーフ オープン セッションの数に設定された制限は、TCP または ICMP のハーフ オープン セッションには影響しません。 設定されたハーフ オープン セッション制限を超えた場合、すべての新しいセッションは拒否され、ログ メッセージが syslog または高速ロガー（HSL）のいずれかに生成されます。

次のセッションは、ハーフ オープン セッションと見なされます。

- スリーウェイ ハンドシェイクが完了していない TCP セッション。
- UDP フローで 1 パケットだけが検出されている UDP セッション。
- ICMP エコー要求または ICMP タイムスタンプの要求に対する応答を受信しない ICMP セッション。

TCP SYN フラッド攻撃

SYN フラッド攻撃を制限するようにグローバル TCP SYN フラッド制限を設定できます。 TCP SYN フラッディング攻撃は、サービス拒否（DoS）攻撃の一種です。 設定された TCP SYN フラッド制限に到達すると、ファイアウォールは追加のセッションを作成する前にセッションの送信元を確認します。 通常、TCP SYN パケットは、ファイアウォールの背後にある対象のエンド ホストまたはサブネット アドレスの範囲に送信されます。 これらの TCP SYN パケットによって、送信元 IP アドレスがスプーフィングされます。 スプーフィング攻撃は、個人またはプログラムが不正なデータを使用してネットワークのリソースにアクセスしようとすることです。 TCP SYN フラッディングでは、ファイアウォールまたはエンド ホスト上のすべてのリソースを占有し、そのために正当なトラフィックに対するサービス拒否が発生します。 VRF レベルおよびゾーン レベルで TCP SYN フラッド保護を設定できます。

SYN フラッド攻撃は次の 2 つのタイプに分かれています。

- ホストのフラッディング：SYN フラッド パケットは、単一ホスト上のすべてのリソースを利用することを目的として、そのホストに送信されます。
- ファイアウォール セッション テーブルのフラッディング：SYN フラッド パケットが、ファイアウォール上のセッション テーブル リソースを使い果たすことで、そのファイアウォールを通過する正当なトラフィックに対してリソースが拒否されることを目的として、ファイアウォール背後のアドレス範囲に送られます。

分散型サービス拒否攻撃に対する保護の設定方法

ファイアウォールの設定

この作業では、次のことを実行します。

- ファイアウォールを設定します。
- セキュリティ送信元ゾーンを作成します。
- セキュリティ宛先ゾーンを作成します。
- 設定された送信元ゾーンと宛先ゾーンを使用して、セキュリティ ゾーン ペアを作成します。
- ゾーン メンバーとしてインターフェイスを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** {**icmp** | **tcp** | **udp**}
5. **exit**
6. **parameter-map type inspect global**
7. **redundancy**
8. **exit**
9. **policy-map type inspect** *policy-map-name*
10. **class type inspect** *class-map-name*
11. **inspect**
12. **exit**
13. **class class-default**
14. **drop**
15. **exit**
16. **exit**
17. **zone security** *security-zone-name*
18. **exit**
19. **zone security** *security-zone-name*
20. **exit**
21. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
22. **service-policy type inspect** *policy-map-name*
23. **exit**
24. **interface** *type number*
25. **ip address** *ip-address mask*
26. **encapsulation dot1q** *vlan-id*
27. **zone-member security** *security-zone-name*
28. **end**
29. ゾーンを別のインターフェイスに付加するには、ステップ 21 ～ 25 を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any ddos-class`	アプリケーション固有検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** {**icmp** | **tcp** | **udp**} 例： `Device(config-cmap)# match protocol tcp`	指定したプロトコルに基づいてクラス マップの一致基準を設定します。
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**parameter-map type inspect global** 例： `Device(config)# parameter-map type inspect global`	グローバル検査パラメータ マップを定義し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 7	**redundancy** 例： `Device(config-profile)# redundancy`	ファイアウォール ハイ アベイラビリティをイネーブルにします。
ステップ 8	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 9	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 10	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ddos-class`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 12	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 13	**class class-default** 例： `Device(config-pmap)# class class-default`	アクションを実行する対象のデフォルト クラスを設定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 14	**drop** 例： `Device(config-pmap-c)# drop`	同じゾーンの 2 つのインターフェイス間をトラフィックが通過できるようにします。
ステップ 15	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 16	**exit** 例： `Device(config-pmap)# exit`	QoS ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 17	**zone security** *security-zone-name* 例： `Device(config)# zone security private`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • ゾーン ペア（送信元ゾーンと宛先ゾーン）を作成するために 2 つのセキュリティ ゾーンが必要です。
ステップ 18	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 19	**zone security** *security-zone-name* 例： `Device(config)# zone security public`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • ゾーン ペア（送信元ゾーンと宛先ゾーン）を作成するために 2 つのセキュリティ ゾーンが必要です。

	コマンドまたはアクション	目的
ステップ 20	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 21	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security private2public source private destination public`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 22	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect ddos-fw`	ポリシー マップをトップレベル ポリシー マップに付加します。
ステップ 23	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 24	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/0.1`	インターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 25	**ip address** *ip-address mask* 例： `Device(config-subif)# ip address 10.1.1.1 255.255.255.0`	サブインターフェイスの IP アドレスを設定します。
ステップ 26	**encapsulation dot1q** *vlan-id* 例： `Device(config-subif)# encapsulation dot1q 2`	インターフェイスで使用するカプセル化方式を設定します。
ステップ 27	**zone-member security** *security-zone-name* 例： `Device(config-subif)# zone-member security private`	ゾーン メンバーとしてインターフェイスを設定します。 • *security-zone-name* 引数では、**zone security** コマンドを使用して設定したゾーンのいずれかを設定する必要があります。 • インターフェイスがセキュリティ ゾーンにある場合、そのインターフェイスを通るトラフィックはどちらの

	コマンドまたはアクション	目的
		方向でもすべて（デバイス宛またはデバイス発信のトラフィックを除く）デフォルトでドロップされます。ゾーン メンバーであるインターフェイスをトラフィックが通過することを許可するには、そのゾーンをゾーンペアの一部にして、そのゾーンペアにポリシーを適用する必要があります。 ポリシーで、**inspect** または **pass** アクションを通してトラフィックが許可されると、トラフィックはインターフェイスを通過します。
ステップ **28**	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ **29**	ゾーンを別のインターフェイスに付加するには、ステップ 21 ～ 25 を繰り返します。	—

ファイアウォール セッションのアグレッシブ エージングの設定

アグレッシブエージング機能をボックス単位（ボックス単位とは、ファイアウォールセッションテーブル全体を意味します）、デフォルト VRF、および VRF 単位のファイアウォール セッションに設定できます。 アグレッシブ エージング機能が動作するには、ファイアウォール セッションのアグレッシブ エージングおよびエージング アウト時間を設定する必要があります。

ファイアウォール セッションのアグレッシブ エージングを設定するには、次の作業を実行します。

ボックス単位のアグレッシブ エージングの設定

ボックス単位とは、ファイアウォール セッション テーブル全体を意味します。 **parameter-map type inspect-global** コマンドに従ったすべての設定がボックスに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **per-box max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
5. **per-box aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **end**
10. **show policy-firewall stats global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		しきい値とタイムアウトを関連付けるグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。 これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 4 と 5 をスキップしてください。

	コマンドまたはアクション	目的
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。
ステップ 4	**per-box max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# per-box max-incomplete 2000 aggressive-aging high 1500 low 1200`	ファイアウォール セッション テーブルのハーフ オープン セッションの上限およびアグレッシブ エージング レートを設定します。
ステップ 5	**per-box aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# per-box aggressive-aging high 1700 low 1300`	総セッションのアグレッシブ エージング制限を設定します。
ステップ 6	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、および **inspect** アクションに関連するその他のパラメータの検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCPセッションが確立状態に達するまでソフトウェアが待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古いTCP接続のSYN待機タイマーがデフォルトから設定済みエージアウト時間にリセットされます。 この例では、接続がタイムアウトするまで30秒待機する代わりに、最も古いTCP接続のタイムアウトが10秒に設定されます。接続が低ウォーターマークを下回ると、アグレッシブエージングはディセーブルになります。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 10	**show policy-firewall stats global** 例： `Device# show policy-firewall stats global`	グローバルなファイアウォール統計情報を表示します。

デフォルト VRF のアグレッシブ エージングの設定

max-incomplete aggressive-aging コマンドを設定する場合、デフォルト VRF に適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
5. **session total** *number* [**aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}]
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **end**
10. **show policy-firewall stats vrf global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		しきい値とタイムアウトを関連付けるグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。 これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 5 をスキップしてください。
		
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。

ステップ 4	**max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# max-incomplete 3455 aggressive-aging high 2345 low 2255`	ハーフ オープン ファイアウォール セッションの上限およびアグレッシブ エージング制限を設定します。
ステップ 5	**session total** *number* [**aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}] 例： `Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60`	総ファイアウォール セッションの合計制限およびアグレッシブ エージング制限を設定します。
ステップ 6	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、および **inspect** アクションに関連するその他のパラメータの検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態に達するまでソフトウェアが待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古いTCP接続のSYN待機タイマーがデフォルトから設定済みエージアウト時間にリセットされます。 この例では、接続がタイムアウトするまで30秒待機する代わりに、最も古いTCP接続のタイムアウトが10秒に設定されます。接続が低ウォーターマークを下回ると、アグレッシブエージングはディセーブルになります。
ステップ 9	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 10	**show policy-firewall stats vrf global** 例： `Device# show policy-firewall stats vrf global`	グローバル VRF ファイアウォール ポリシーの統計情報を表示します。

ファイアウォール セッションのエージング アウトの設定

ICMP、TCP、またはUDPのファイアウォール セッションのエージング アウトを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
5. **exit**
6. **parameter-map type inspect** *parameter-map-name*
7. **tcp idle-time** *seconds* [**ageout-time** *seconds*]
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **exit**
10. **policy-map type inspect** *policy-map-name*
11. **class type inspect match-any** *class-map-name*
12. **inspect** *parameter-map-name*
13. **end**
14. **show policy-firewall stats vrf** *vrf-pmap-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかのコマンドを入力します。 • **parameter-map type inspect-global** • **parameter-map type inspect global**	グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。 • ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。 • **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 4 をスキップしてください。

	コマンドまたはアクション	目的

	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspectglobal`
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。

ステップ 4	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	パラメータ マップで VRF をバインドします。
ステップ 5	**exit** 例： `Device(config-profile)# exit`	パラメータマップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、および **inspect** アクションに関連するその他のパラメータの検査タイプ パラメータ マップを設定し、パラメータマップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 7	**tcp idle-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp idle-time 3000 ageout-time 100`	アイドル状態の TCP セッションのタイムアウト、および TCP セッションのアグレッシブ エージング アウト時間を設定します。 • **tcp finwait-time** コマンドを設定して、ファイアウォールが finish（FIN）-exchange を検出した後に TCP セッションが管理される時間の長さを指定することもできます。または、**tcp synwait-time** コマンドを設定して、セッションをドロップする前に、TCP セッションが確立状態に達するまでソフトウェアが待機する時間を指定します。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態に達するまでソフトウェアが待機する時間を指定します。 • アグレッシブエージングがイネーブルになると、最も古い TCP 接続の SYN 待機タイマーがデフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。 接続が低ウォーターマークを下回ると、アグレッシブエージングはイネーブルになります。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 11	**class type inspect match-any** *class-map-name* 例： `Device(config-pmap)# class type inspect match-any ddos-class`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 12	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect pmap1`	パラメータ マップのステートフル パケット インスペクションをイネーブルにします。
ステップ 13	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 14	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォールの統計情報を表示します。

例

次に、**show policy-firewall stats vrf vrf1-pmap** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf vrf1-pmap

 VRF: vrf1, Parameter-Map: vrf1-pmap
  Interface reference count: 2
       Total Session Count(estab + half-open): 270, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- -----------     ------
```

```
All      0               0
UDP      0               0
ICMP     0               0
TCP      0               0

TCP Syn Flood Half Open Count: 0, Exceed: 12
Half Open Aggressive Aging Period Off, Event Count: 0
```

VRF 単位のアグレッシブ エージングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*
7. **exit**
8. **parameter-map type inspect-vrf** *vrf-pmap-name*
9. **max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
10. **session total** *number* [**aggressive-aging** {**high** *value* **low** *value* | **percent** *percent* **low percent** *percent*}]
11. **alert on**
12. **exit**
13. 次のいずれかのコマンドを入力します。
    - **parameter-map type inspect-global**
    - **parameter-map type inspect global**
14. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
15. **exit**
16. **parameter-map type inspect** *parameter-map-name*
17. **tcp idle-time** *seconds* [**ageout-time** *seconds*]
18. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
19. **exit**
20. **policy-map type inspect** *policy-map-name*
21. **class type inspect match-any** *class-map-name*
22. **inspect** *parameter-map-name*
23. **end**
24. **show policy-firewall stats vrf** *vrf-pmap-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf ddos-vrf1`	VRF インスタンスを定義し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:2`	VRF インスタンスのルート識別子（RD）を指定します。
ステップ 5	**route-target export** *route-target-ext-community* 例： `Device(config-vrf)# route-target export 100:2`	ルートターゲット拡張コミュニティを作成し、ルーティング情報をターゲット VPN 拡張コミュニティにエクスポートします。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Device(config-vrf)# route-target import 100:2`	ルートターゲット拡張コミュニティを作成し、ルーティング情報をターゲット VPN 拡張コミュニティからインポートします。
ステップ 7	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	**max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# max-incomplete 2000 aggressive-aging high 1500 low 1200`	ハーフ オープン セッションの上限およびアグレッシブ エージング制限を設定します。
ステップ 10	**session total** *number* [**aggressive-aging** {**high** *value* **low** *value* | **percent** *percent* **low percent** *percent*}] 例： `Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60`	総セッションの総セッション制限およびアグレッシブ エージング制限を設定します。 • 総セッション制限を絶対値またはパーセンテージとして設定できます。
ステップ 11	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 12	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

ステップ 13	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。 これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 14 をスキップしてください。
		
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。

	コマンドまたはアクション	目的
ステップ 14	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	パラメータ マップで VRF をバインドします。
ステップ 15	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 16	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、および **inspect** アクションに関連するその他のパラメータの検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 17	**tcp idle-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp idle-time 3000 ageout-time 100`	アイドル状態の TCP セッションのタイムアウト、および TCP セッションのアグレッシブ エージング アウト時間を設定します。
ステップ 18	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態に達するまでソフトウェアが待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古い TCP 接続の SYN 待機タイマーがデフォルトから設定済みエージアウト時間にリセットされます。 この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。 接続が低ウォーターマークを下回ると、アグレッシブ エージングはディセーブルになります。
ステップ 19	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 20	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 21	**class type inspect match-any** *class-map-name* 例： `Device(config-pmap)# class type inspect match-any ddos-class`	アクションを実行する対象のトラフィック（クラス）を指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 22	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect pmap1`	パラメータ マップのステートフル パケット インスペクションをイネーブルにします。
ステップ 23	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 24	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォールの統計情報を表示します。

例

次に、**show policy-firewall stats vrf vrf1-pmap** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf vrf1-pmap

VRF: vrf1, Parameter-Map: vrf1-pmap
  Interface reference count: 2
       Total Session Count(estab + half-open): 80, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- ------------    ------
       All      0               0
       UDP      0               0
       ICMP     0               0
       TCP      0               0

       TCP Syn Flood Half Open Count: 0, Exceed: 116
       Half Open Aggressive Aging Period Off, Event Count: 0
```

ファイアウォール イベント レート モニタリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-zone** *zone-pmap-name*
4. **alert on**
5. **threat-detection basic-threat**
6. **threat-detection rate fw-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
7. **threat-detection rate inspect-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
8. **threat-detection rate syn-attack average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
9. **exit**
10. **zone security** *security-zone-name*
11. **protection** *parameter-map-name*
12. **exit**
13. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
14. **end**
15. **show policy-firewall stats zone**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-zone** *zone-pmap-name* 例： `Device(config)# parameter-map type inspect-zone zone-pmap1`	ゾーン検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ゾーンのステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。 • **log** コマンドを使用して、アラートのロギングを syslog または高速ロガー（HSL）のいずれかに設定できます。
ステップ 5	**threat-detection basic-threat** 例： `Device(config-profile)# threat-detection basic-threat`	ゾーンの基本脅威検出を設定します。
ステップ 6	**threat-detection rate fw-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate fw-drop average-time-frame 600 average-threshold 100 burst-threshold 100`	ファイアウォールのドロップ イベントの脅威検出レートを設定します。 • **threat-detection rate** コマンドを設定する前に、**threat-detection basic-threat** コマンドを設定する必要があります。
ステップ 7	**threat-detection rate inspect-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate inspect-drop average-time-frame 600 average-threshold 100 burst-threshold 100`	ファイアウォール インスペクション ベースのドロップ イベントの脅威検出レートを設定します。
ステップ 8	**threat-detection rate syn-attack average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate syn-attack average-time-frame 600 average-threshold 100 burst-threshold 100`	TCP SYN 攻撃イベントの脅威検出レートを設定します。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**zone security** *security-zone-name* 例： `Device(config)# zone security public`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 11	**protection** *parameter-map-name* 例： `Device(config-sec-zone)# protection zone-pmap1`	ゾーン検査パラメータ マップをゾーンに付加し、ゾーン検査パラメータ マップで設定されている機能をゾーンに適用します。
ステップ 12	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 13	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security private2public source private destination public`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 14	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 15	**show policy-firewall stats zone** 例： `Device# show policy-firewall stats zone`	ゾーン レベルでファイアウォール ポリシーの統計情報を表示します。

ボックス単位のハーフ オープン セッション制限の設定

ボックス単位とは、ファイアウォール セッション テーブル全体を意味します。 **parameter-map type inspect-global** コマンドに従ったすべての設定がボックスに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **alert on**
5. **per-box max-incomplete** *number*
6. **session total** *number*
7. **end**
8. **show policy-firewall stats global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		しきい値とタイムアウトを関連付けるグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。 これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 5 と 6 をスキップしてください。
		
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。

	コマンドまたはアクション	目的
ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフルパケットインスペクションのアラートメッセージのコンソール表示をイネーブルにします。
ステップ 5	**per-box max-incomplete** *number* 例： `Device(config-profile)# per-box max-incomplete 12345`	ファイアウォールセッションテーブルのハーフオープン接続の最大数を設定します。
ステップ 6	**session total** *number* 例： `Device(config-profile)# session total 34500`	ファイアウォールセッションテーブルの総セッション制限を設定します。
ステップ 7	**end** 例： `Device(config-profile)# end`	パラメータマップタイプ検査コンフィギュレーションモードを終了し、特権 EXEC モードを開始します。
ステップ 8	**show policy-firewall stats global** 例： `Device# show policy-firewall stats global`	グローバルなファイアウォール統計情報を表示します。

VRF 検査パラメータ マップのハーフ オープン セッション制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-name*
4. **alert on**
5. **max-incomplete** *number*
6. **session total** *number*
7. **exit**
8. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
9. **alert on**
10. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
11. **end**
12. **show policy-firewall stats vrf** *vrf-pmap-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-vrf** *vrf-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**max-incomplete** *number* 例： `Device(config-profile)# max-incomplete 2000`	VRF 単位のハーフ オープン接続の最大数を設定します。
ステップ 6	**session total** *number* 例： `Device(config-profile)# session total 34500`	VRF の総セッション制限を設定します。
ステップ 7	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

ステップ 8	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		しきい値とタイムアウトを関連付けるグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドまたは **parameter-map type inspect global** コマンドを使用できます。 これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 10 をスキップしてください。
		
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。

ステップ 9	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 10	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	グローバル パラメータ マップに VRF をバインドします。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 12	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォールの統計情報を表示します。

グローバル TCP SYN フラッド制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **alert on**
5. **per-box tcp syn-flood limit** *number*
6. **end**
7. **show policy-firewall stats vrf global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドまたは **parameter-map type inspect global** コマンドを設定できます。 これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 5 をスキップしてください。
		
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。

ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 5	**per-box tcp syn-flood limit** *number* 例： `Device(config-profile)# per-box tcp syn-flood limit 500`	新しい SYN パケットの SYN Cookie 処理をトリガーする TCP ハーフ オープン セッション数を制限します。
ステップ 6	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**show policy-firewall stats vrf global** 例： `Device# show policy-firewall stats vrf global`	（任意）グローバル VRF ファイアウォール ポリシーのステータスを表示します。 • コマンド出力には、存在する TCP ハーフ オープン セッションの数も表示されます。

例

次に、**show policy-firewall stats vrf global** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf global

Global table statistics
       total_session_cnt: 0
```

```
exceed_cnt:        0
tcp_half_open_cnt: 0
syn_exceed_cnt:    0
```

分散型サービス拒否攻撃に対する保護の設定例

例：ファイアウォールの設定

```
Router# configure terminal
Router(config)# class-map type inspect match-any ddos-class
Router(config-cmap)# match protocol tcp
Router(config-cmap-c)# exit
Router(config)# parameter-map type inspect global
Router(config-profile)# redundancy
Router(config-profile)# exit
Router(config)# policy-map type inspect ddos-fw
Router(config-pmap)# class type inspect ddos-class
Router(config-pmap-c)# inspect
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# zone security private
Router(config-sec-zone)# exit
Router(config)# zone security public
Router(config-sec-zone)# exit
Router(config)# zone-pair security private2public source private destination public
Router((config-sec-zone-pair)# service-policy type inspect ddos-fw
Router((config-sec-zone-pair)# exit
Router(config)# interface gigabitethernet 0/1/0.1
Router(config-subif)# ip address 10.1.1.1 255.255.255.0
Router(config-subif)# encapsulation dot1q 2
Router(config-subif)# zone-member security private
Router(config-subif)# exit
Router(config)# interface gigabitethernet 1/1/0.1
Router(config-subif)# ip address 10.2.2.2 255.255.255.0
Router(config-subif)# encapsulation dot1q 2
Router(config-subif)# zone-member security public
Router(config-subif)# end
```

例：ファイアウォール セッションのアグレッシブ エージングの設定

例：ボックス単位のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# per-box max-incomplete 2000 aggressive-aging 1500 low 1200
Device(config-profile)# per-box aggressive-aging high 1700 low 1300
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# end
```

例：デフォルト VRF のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# max-incomplete 2000 aggressive-aging high 1500 low 1200
Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# end
```

例：ファイアウォール セッションのエージング アウトの設定

```
Device# configure terminal
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp idle-time 3000 ageout-time 100
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# exit
Device(config)# policy-map type inspect ddos-fw
Device(config-profile)# class type inspect match-any ddos-class
Device(config-profile)# inspect pmap1
Device(config-profile)# end
```

例：VRF 単位のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# ip vrf ddos-vrf1
Device(config-vrf)# rd 100:2
Device(config-vrf)# route-target export 100:2
Device(config-vrf)# route-target import 100:2
Device(config-vrf)# exit
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# max-incomplete 3455 aggressive-aging high 2345 low 2255
Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60
Device(config-profile)# alert on
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp idle-time 3000 ageout-time 100
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# exit
Device(config)# policy-map type inspect ddos-fw
Device(config-pmap)# class type inspect match-any ddos-class
Device(config-pmap-c)# inspect pmap1
Device(config-profile)# end
```

例：ファイアウォール イベント レート モニタリングの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect zone zone-pmap1
Device(config-profile)# alert on
Device(config-profile)# threat-detection basic-threat
Device(config-profile)# threat-detection rate fw-drop average-time-frame 600 average-threshold
```

```
 100 burst-threshold 100
Device(config-profile)# threat-detection rate inspect-drop average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# threat-detection rate syn-attack average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# exit
Device(config)# zone security public
Device(config-sec-zone)# protection zone-pmap1
Device(config-sec-zone)# exit
Device(config)# zone-pair security private2public source private destination public
Device(config-sec-zone-pair)# end
```

例：ボックス単位のハーフ オープン セッション制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# per-box max-incomplete 12345
Device(config-profile)# session total 34500
Device(config-profile)# end
```

例：VRF 検査パラメータ マップのハーフ オープン セッション制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect vrf vrf1-pmap
Device(config-profile)# alert on
Device(config-profile)# max-incomplete 3500
Device(config-profile)# session total 34500
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# end
```

例：グローバル TCP SYN フラッド制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# per-box tcp syn-flood limit 500
Device(config-profile)# end
```

分散型サービス拒否攻撃に対する保護の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	『Cisco IOS Security Command Reference』
ファイアウォール リソース管理	『*Configuring Firewall Resource Management feature*』
ファイアウォール TCP SYN Cookie	『*Configuring Firewall TCP SYN Cookie feature*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

分散型サービス拒否攻撃に対する保護の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *18*：分散型サービス拒否攻撃に対する保護の機能情報

機能名	リリース	機能情報
分散型サービス拒否攻撃に対する保護	Cisco IOS XE Release 3.4S	分散型サービス拒否攻撃に対する保護機能は、ボックス単位レベル（すべてのファイアウォール セッションに対して）および VRF レベルで DoS 攻撃から保護します。DDoS 攻撃を防ぐために、ファイアウォールセッションのアグレッシブエージング、ファイアウォール セッションのイベントレートモニタリング、ハーフ オープン接続制限、およびグローバル TCP SYN Cookie 保護を設定できます。 次のコマンドが導入または変更されました。**clear policy-firewall stats global**、**max-incomplete**、**max-incomplete aggressive-aging**、**per-box aggressive-aging**、**per-box max-incomplete**、**per-box max-incomplete aggressive-aging**、**per-box tcp syn-flood limit**、**session total**、**show policy-firewall stats global**、**show policy-firewall stats zone**、**threat-detection basic-threat**、**threat-detection rate**、および **udp half-open**。

第 14 章

ファイアウォール リソース管理の設定

ファイアウォール リソース管理機能は、ルータで設定される VPN ルーティングおよび転送（VRF）セッションとグローバル ファイアウォール セッションの数を制限します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ファイアウォール リソース管理の設定の制約事項

- グローバル レベルまたは VRF レベルのセッション制限を設定し、セッション制限を再設定すると、グローバル レベルまたはVRF レベルのセッション制限が最初に設定されたセッショ

ン数よりも低い場合、新しいセッションは追加されません。ただし、既存のセッションはドロップされません。

ファイアウォール リソース管理の設定について

ファイアウォール リソース管理

リソース管理は、デバイス上の共有リソースの利用レベルを制限します。 デバイス上の共有リソースは次のとおりです。

- 帯域幅
- 接続状態
- メモリ使用率（テーブル単位）
- セッションまたはコール数
- 1 秒あたりのパケット数
- Ternary Content Addressable Memory（TCAM）エントリ

ファイアウォール リソース管理機能は、ゾーンベースのファイアウォール リソース管理をクラス レベルから VRF レベルおよびグローバル レベルに拡張します。 クラス レベルのリソース管理は、クラス レベルでファイアウォール セッションのリソースを保護します。 たとえば、最大セッション制限、セッション レート制限、不完全セッション制限などのパラメータは、ファイアウォール リソース（チャンク メモリなど）を保護し、これらのリソースが単一クラスによって使い果たされないようにします。

複数の仮想ルーティングおよび転送（VRF）インスタンスが同じポリシーを共有する場合、1 つの VRF インスタンスからのファイアウォール セッション設定要求によって総セッション数が最大制限に達する可能性があります。 1 つの VRF がデバイス上のリソースの最大量を消費すると、他の VRF インスタンスがデバイス リソースを共有することが難しくなります。 VRF ファイアウォール セッションの数を制限するために、ファイアウォール リソース管理機能を使用できます。

グローバル レベルでは、ファイアウォール リソース管理機能により、グローバル ルーティング ドメインでのファイアウォール セッションによるリソースの使用を制限できます。

VRF-Aware Cisco IOS XE ファイアウォール

VRF-Aware Cisco IOS XE ファイアウォールは、ファイアウォールがサービス プロバイダー（SP）または大企業のエッジ ルータに設定されている場合、VPN ルーティングおよび転送（VRF）インターフェイスに Cisco IOS XE ファイアウォール機能を適用します。 SP は中小企業の市場向けにマネージド サービスを提供します。

VRF-Aware Cisco IOS XE ファイアウォールは、VRF-lite（Multi-VRF CE とも呼ばれる）および各種プロトコルでのアプリケーション インスペクションと制御（AIC）をサポートします。

VRF 認識ファイアウォールは、VRF-lite（Multi-VRF CE とも呼ばれる）および各種プロトコルでのアプリケーション インスペクションと制御（AIC）をサポートします。

（注） Cisco IOS XE リリースは、コンテキストベース アクセス コントロール（CBAC）ファイアウォールをサポートしません。

ファイアウォール セッション

セッション定義

仮想ルーティングおよび転送（VRF）レベルで、ファイアウォール リソース管理機能は、各 VRF インスタンスのファイアウォール セッションの数を追跡します。 グローバル レベルでは、ファイアウォール リソース管理は、デバイス レベルではなくグローバル ルーティング ドメインで総ファイアウォール セッション数を追跡します。 VRF レベルとグローバル レベルの両方で、セッション数は、開かれたセッション、ハーフ オープン セッション、および明確でないファイアウォール セッション データベース内のセッションの合計です。 確立状態にまだ到達していない TCP セッションはハーフ オープン セッションと呼ばれます。

ファイアウォールには、2 つのセッション データベース（セッション データベースおよび明確でないセッション データベース）があります。 セッション データベースには、5 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）のセッションが含まれます。 タプルは、要素の順序付きリストです。 明確でないセッション データベースには、5 タプルよりも少ない（IP アドレスやポート番号などが欠落している）セッションが含まれます。

次のルールが、セッション制限の設定に適用されます:

- クラス レベルのセッション制限は、グローバル制限を超えることができます。
- クラス レベルのセッション制限は、関連付けられた VRF セッションの最大値を超えることができます。
- グローバル コンテキストを含む VRF 制限の合計は、ハードコーディングされたセッション制限を超えることができます。

セッション レート

セッション レートは、特定の時間間隔でセッションが確立されるレートです。 最大および最小のセッション レート制限を定義できます。 セッション レートが指定された最大レートを超えると、ファイアウォールは新しいセッション設定要求を拒否するようになります。

リソース管理の観点から、最大および最小のセッション レート制限を設定すると、Cisco Packet Processor が多数のファイアウォール セッション設定要求を受信して過負荷状態になるのを防ぐことができます。

不完全なセッションまたはハーフ オープン セッション

不完全なセッションは、ハーフ オープン セッションです。 最大セッション制限を設定することで、不完全なセッションが使用するリソースがカウントされ、不完全なセッション数の増加が制限されます。

ファイアウォール リソース管理セッション

次のルールが、ファイアウォール リソース管理セッションに適用されます。

- デフォルトでは、開かれたセッションまたはハーフ オープン セッションのセッション制限は無制限です。
- 開かれたセッションまたはハーフ オープン セッションは、パラメータで制限され、個別にカウントされます。
- 開かれたセッション数またはハーフ オープン セッション数には、インターネット制御メッセージ プロトコル（ICMP）、TCP、または UDP セッションが含まれます。
- 開かれたセッションの数とレートを制限できます。
- ハーフ オープン セッションの数のみを制限できます。

ファイアウォール リソース管理の設定方法

ファイアウォール リソース管理の設定

（注） グローバル パラメータ マップは、ルータ レベルではなく、グローバル ルーティング ドメインで有効になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-pmap-name*
4. **session total** *number*
5. **tcp syn-flood limit** *number*
6. **exit**
7. **parameter-map type inspect-global**
8. **vrf** *vrf-name* **inspect** *parameter-map-name*
9. **exit**
10. **parameter-map type inspect-vrf vrf-default**
11. **session total** *number*
12. **tcp syn-flood limit** *number*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**session total** *number* 例： `Device(config-profile)# session total 1000`	セッションの総数を設定します。
ステップ 5	**tcp syn-flood limit** *number* 例： `Device(config-profile)# tcp syn-flood limit 2000`	新しいSYNパケットの同期（SYN）Cookie処理をトリガーする TCP ハーフ オープン セッション数を制限します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect-global** 例： `Device(config)# parameter-map type inspect-global`	グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**vrf** *vrf-name* **inspect** *parameter-map-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	パラメータ マップに VRF をバインドします。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**parameter-map type inspect-vrf vrf-default** 例： `Device(config)# parameter-map type inspect-vrf vrf-default`	デフォルトの VRF 検査タイプ パラメータ マップを設定します。
ステップ 11	**session total** *number* 例： `Device(config-profile)# session total 6000`	セッションの総数を設定します。 • **session total** コマンドを VRF 検査タイプ パラメータ マップおよびグローバル パラメータ マップに設定できます。 VRF 検査タイプ パラメータ マップに **session total** コマンドを設定した場合、セッションは VRF 検査タイプ パラメータ マップに関連付けられます。 **session total** コマンドがグローバル パラメータ マップに設定された場合、このコマンドはグローバル ルーティング ドメインに適用されます。
ステップ 12	**tcp syn-flood limit** *number* 例： `Device(config-profile)# tcp syn-flood limit 7000`	新しい SYN パケットの SYN Cookie 処理をトリガーする TCP ハーフ オープン セッション数を制限します。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォール リソース管理の設定例

例：ファイアウォール リソース管理の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# session total 1000
Device(config-profile)# tcp syn-flood limit 2000
Device(config-profile)# exit
Device(config)# parameter-map type inspect-global
Device(config-profile)# vrf vrf1 inspect pmap1
Device(config-profile)# exit
Device(config)# parameter-map type inspect-vrf vrf-default
Device(config-profile)# session total 6000
Device(config-profile)# tcp syn-flood limit 7000
Device(config-profile)# end
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

関連項目	マニュアル タイトル
VRF 認識ファイアウォール	「VRF-Aware Cisco IOS XE Firewall」モジュール
ゾーンベース ポリシー ファイアウォール	「Zone-Based Policy Firewall」モジュール

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォール リソース管理の設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *19*：ファイアウォール リソース管理の設定の機能情報

機能名	リリース	機能情報
ファイアウォール リソース管理	Cisco IOS XE Release 3.3S	ファイアウォール リソース管理機能は、ルータで設定される VPN ルーティングおよび転送（VRF）セッションとグローバル ファイアウォール セッションの数を制限します。 次のコマンドが導入または変更されました。**parameter-map type inspect-vrf**。

第 15 章

分散型サービス拒否攻撃の防止およびリソース管理のための IPv6 ファイアウォール サポート

IPv6 ゾーンベース ファイアウォールは、分散型サービス拒否攻撃への保護およびファイアウォール リソース管理機能をサポートします。

分散型サービス拒否攻撃に対する保護機能は、グローバル レベルで（すべてのファイアウォール セッションに対して）および VPN ルーティングおよび転送（VRF）レベルで、サービス拒否（DoS）攻撃から保護します。 分散型サービス拒否攻撃に対する保護機能を使用すると、分散型 DoS 攻撃を防ぐために、ファイアウォール セッションのアグレッシブ エージング、ファイアウォール セッションのイベント レート モニタリング、ハーフオープン接続制限、およびグローバル TCP 同期（SYN）Cookie 保護を設定できます。

ファイアウォール リソース管理機能は、デバイス上に設定される VPN ルーティングおよび転送（VRF）セッションとグローバル ファイアウォール セッションの数を制限します。

このモジュールでは、分散型サービス拒否攻撃への保護およびファイアウォール リソース管理機能を設定する方法について説明します。

- 分散型サービス拒否攻撃の防止およびリソース管理のための IPv6 ファイアウォール サポートの機能情報，380 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

分散型サービス拒否攻撃に対する保護およびリソース管理のための IPv6 ファイアウォール サポートの制約事項

次の制約事項がファイアウォール リソース管理機能に適用されます。

- グローバル レベルまたは仮想ルーティングおよび転送（VRF）レベルのセッション制限を設定し、セッション制限を再設定した後、グローバル レベルまたは VRF レベルのセッション制限が最初に設定されたセッション数よりも低い場合、新しいセッションは追加されません。ただし、既存のセッションはドロップされません。

分散型サービス拒否攻撃の防止およびリソース管理のための IPv6 ファイアウォール サポートについて

ファイアウォール セッションのアグレッシブ エージング

アグレッシブエージング機能により、ファイアウォールは、セッションを積極的にエージングアウトして、新しいセッションのためのスペースを確保することで、ファイアウォール セッション データベースがいっぱいになるのを防ぐことができます。 ファイアウォールは、アイドル セッションを削除して、そのリソースを保護します。アグレッシブエージング機能により、ファイアウォール セッションが存在できる時間は、エージングアウト時間と呼ばれる、タイマーで定義された時間よりも短くなります。

アグレッシブエージング機能には、アグレッシブエージング期間の開始と終了を定義するしきい値（高ウォーターマークと低ウォーターマーク）が含まれます。 アグレッシブ エージング期間

は、セッション テーブルが高ウォーターマークを超えると開始され、低ウォーターマーク以下になると終了します。アグレッシブエージング期間中、セッションは、エージングアウト時間を使用して設定された期間よりも短い期間存在します。 攻撃者が、ファイアウォールがセッションを終了するレートよりも短い時間でセッションを開始する場合、セッションを作成するために割り当てられているすべてのリソースが使用され、新しいすべての接続が拒否されます。 このような攻撃を防ぐには、セッションを積極的にエージングアウトするようにアグレッシブエージング機能を設定できます。 この機能はデフォルトで無効に設定されています。

ボックス レベル（ボックスはファイアウォール セッション テーブル全体を示します）および仮想ルーティングおよび転送（VRF）レベルでハーフ オープン セッションおよび総セッションにアグレッシブエージングを設定できます。この機能を総セッションに設定している場合、ファイアウォールセッションリソースを消費するすべてのセッションが考慮されます。総セッションは、確立されているセッション、ハーフ オープン セッション、および明確でないセッション データベース内のセッションで構成されます。（確立状態にまだ到達していないTCPセッションはハーフ オープン セッションと呼ばれます）。

ファイアウォールには、2 つのセッション データベース（セッション データベースおよび明確でないセッションデータベース）があります。 セッションデータベースには、5 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）のセッションが含まれます。 タプルは、要素の順序付きリストです。 明確でないセッション データベースには、5 タプルよりも少ない（IP アドレスやポート番号などが欠落している）セッションが含まれます。ハーフ オープン セッションのアグレッシブ エージングの場合、ハーフ オープン セッションだけが考慮されます。

インターネット制御メッセージ プロトコル（ICMP）、TCP、および UDP のファイアウォール セッションにアグレッシブ エージング アウト時間を設定できます。 エージング アウト時間は、デフォルトでアイドル時間に設定されます。

イベント レート モニタリング機能

イベント レート モニタリング機能は、ゾーンの定義済みイベントのレートをモニタします。 イベント レート モニタリング機能には基本脅威検出が含まれます。これにより、セキュリティ デバイスは、ファイアウォールの内側にあるリソースへの考えられる脅威、異常や攻撃を検出し、それに対するアクションを実行できます。イベントの基本脅威検出レートを設定できます。 特定のタイプのイベントの着信レートが、設定された脅威検出レートを超えると、イベント レート モニタリングはこのイベントを脅威と見なし、脅威を停止するアクションを実行します。 脅威検出は、入力のゾーンだけでイベントを検査します（イベント レート モニタリング機能が入力ゾーンでイネーブルの場合）。

ネットワーク管理者は、アラート メッセージ（syslog または高速ロガー（HSL））を介して潜在的な脅威について通知され、攻撃ベクトルの検出、攻撃の発生元のゾーンの検出、特定の動作やトラフィックをブロックするようネットワークのデバイスを設定するなどのアクションを実行できます。

イベント レート モニタリング機能では、次のタイプのイベントをモニタします。

- 基本的なファイアウォール チェック エラーが原因でファイアウォールがドロップする：これには、ゾーンまたはゾーン ペアのチェック エラー、または drop アクションを使用して設定されたファイアウォール ポリシーなどが含まれる場合があります。
- レイヤ4インスペクション エラーが原因でファイアウォールがドロップする：これには、最初の TCP パケットが同期（SYN）パケットではないため失敗した TCP インスペクションが含まれる場合があります。
- TCP SYN Cookie 攻撃：これには、ドロップされた SYN パケット数、およびスプーフィング攻撃として送信された SYN Cookie の数の集計が含まれる場合があります。

イベント レート モニタリング機能では、異なるイベントの平均レートとバースト レートをモニタします。 各イベント タイプには、設定可能なパラメータ セット（平均しきい値、バーストしきい値、および期間）が含まれる関連レートによって制御されるレート オブジェクトがあります。 期間はタイム スロットに分割されています。各タイム スロットは、期間の 1/30 です。

平均レートは、イベント タイプごとに計算されます。 各レート オブジェクトは、30 の完了済みサンプリング値に加えて、現在稼働中のサンプリング期間を保持するための 1 つの値を保持します。 現在のサンプリング値によって計算済みの最も古い値が置き換えられ、平均が計算されます。 平均レートは、各期間で計算されます。 平均レートが平均しきい値を超えると、イベント レート モニタリング機能は、これを潜在的な脅威と見なし、統計情報を更新し、ネットワーク管理者に通知します。

バースト レートは、トークン バケット アルゴリズムを使用して実装されます。 各タイム スロットでは、トークン バケットがトークンで埋められます。 発生する（特定のイベント タイプの）イベントごとに、トークンがバケットから削除されます。 空のバケットは、バーストしきい値に到達したことを意味し、管理者は syslog または HSL を介してアラームを受信します。 脅威検出統計情報の確認、およびゾーンのさまざまなイベントに対する潜在的脅威についての学習は、**show policy-firewall stats zone**コマンドの出力から行うことができます。

threat-detection basic-threat コマンドを使用して、最初に基本脅威検出をイネーブルにする必要があります。 基本脅威検出を設定すると、脅威検出レートを設定できます。 脅威検出レートを設定するには、**threat-detection rate** コマンドを使用します。

次の表に、イベント レート モニタリング機能がイネーブルの場合に適用可能な基本脅威検出のデフォルト設定を示します。

表 *20*：基本脅威検出のデフォルト設定

パケット ドロップの理由	脅威検出の設定
基本的なファイアウォール ドロップ	平均レート 400 パケット/秒（pps） バースト レート 1600 pps レート間隔 600 秒
インスペクション ベースのファイアウォール ドロップ	平均レート 400 pps バースト レート 1600 pps レート間隔 600 秒

パケット ドロップの理由	脅威検出の設定
SYN 攻撃ファイアウォール ドロップ	平均レート 100 pps バースト レート 200 pps レート間隔 600 秒

ハーフ オープン接続制限

ファイアウォールセッションテーブルは、ハーフ オープン ファイアウォール接続の制限をサポートします。 ハーフ オープン セッションの数を制限すると、ボックス単位レベルまたは仮想ルーティングおよび転送（VRF）レベルでハーフ オープン セッションを使用してファイアウォール セッション テーブルを満たす可能性がある攻撃からファイアウォールを守り、セッションが確立されるのを防ぎます。 ハーフ オープン接続制限は、レイヤ 4 プロトコル、インターネット制御メッセージプロトコル（ICMP）、TCP、およびUDPに設定できます。 UDPハーフ オープン セッションの数に設定された制限は、TCP またはICMP のハーフ オープン セッションには影響しません。 設定されたハーフ オープン セッション制限を超えた場合、すべての新しいセッションは拒否され、ログ メッセージが syslog または高速ロガー（HSL）のいずれかに生成されます。

次のセッションは、ハーフ オープン セッションと見なされます。

- スリーウェイ ハンドシェイクが完了していない TCP セッション。
- UDP フローで 1 パケットだけが検出されている UDP セッション。
- ICMP エコー要求または ICMP タイムスタンプの要求に対する応答を受信しない ICMP セッション。

TCP SYN フラッド攻撃

SYNフラッド攻撃を制限するようにグローバルTCP SYNフラッド制限を設定できます。 TCP SYN フラッディング攻撃は、サービス拒否（DoS）攻撃の一種です。 設定されたTCP SYNフラッド制限に到達すると、ファイアウォールは追加のセッションを作成する前にセッションの送信元を確認します。 通常、TCP SYN パケットは、ファイアウォールの背後にある対象のエンド ホストまたはサブネット アドレスの範囲に送信されます。 これらの TCP SYN パケットによって、送信元IPアドレスがスプーフィングされます。 スプーフィング攻撃は、個人またはプログラムが不正なデータを使用してネットワークのリソースにアクセスしようとすることです。 TCP SYN フラッディングでは、ファイアウォールまたはエンド ホスト上のすべてのリソースを占有し、そのために正当なトラフィックに対するサービス拒否が発生します。 VRF レベルおよびゾーン レベルで TCP SYN フラッド保護を設定できます。

SYN フラッド攻撃は次の 2 つのタイプに分かれています。

- ホストのフラッディング：SYN フラッド パケットは、単一ホスト上のすべてのリソースを利用することを目的として、そのホストに送信されます。

- ファイアウォール セッション テーブルのフラッディング：SYN フラッド パケットが、ファイアウォール上のセッション テーブル リソースを使い果たすことで、そのファイアウォールを通過する正当なトラフィックに対してリソースが拒否されることを目的として、ファイアウォール背後のアドレス範囲に送られます。

ファイアウォール リソース管理

リソース管理は、デバイス上の共有リソースの利用レベルを制限します。 デバイス上の共有リソースは次のとおりです。

- 帯域幅
- 接続状態
- メモリ使用率（テーブル単位）
- セッションまたはコール数
- 1 秒あたりのパケット数
- Ternary Content Addressable Memory（TCAM）エントリ

ファイアウォール リソース管理機能は、ゾーンベースのファイアウォール リソース管理をクラス レベルから VRF レベルおよびグローバル レベルに拡張します。 クラス レベルのリソース管理は、クラス レベルでファイアウォール セッションのリソースを保護します。 たとえば、最大セッション制限、セッション レート制限、不完全セッション制限などのパラメータは、ファイアウォール リソース（チャンク メモリなど）を保護し、これらのリソースが単一クラスによって使い果たされないようにします。

複数の仮想ルーティングおよび転送（VRF）インスタンスが同じポリシーを共有する場合、1 つの VRF インスタンスからのファイアウォール セッション設定要求によって総セッション数が最大制限に達する可能性があります。 1 つの VRF がデバイス上のリソースの最大量を消費すると、他の VRF インスタンスがデバイス リソースを共有することが難しくなります。 VRF ファイアウォール セッションの数を制限するために、ファイアウォール リソース管理機能を使用できます。

グローバル レベルでは、ファイアウォール リソース管理機能により、グローバル ルーティング ドメインでのファイアウォール セッションによるリソースの使用を制限できます。

ファイアウォール セッション

セッション定義

仮想ルーティングおよび転送（VRF）レベルで、ファイアウォール リソース管理機能は、各 VRF インスタンスのファイアウォール セッションの数を追跡します。 グローバル レベルでは、ファイアウォール リソース管理は、デバイス レベルではなくグローバル ルーティング ドメインで総ファイアウォール セッション数を追跡します。 VRF レベルとグローバル レベルの両方で、セッション数は、開かれたセッション、ハーフ オープン セッション、および明確でないファイアウォー

ルセッションデータベース内のセッションの合計です。 確立状態にまだ到達していない TCP セッションはハーフ オープン セッションと呼ばれます。

ファイアウォールには、2 つのセッション データベース（セッション データベースおよび明確でないセッションデータベース）があります。 セッションデータベースには、5 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）のセッションが含まれます。 タプルは、要素の順序付きリストです。 明確でないセッション データベースには、5 タプルよりも少ない（IP アドレスやポート番号などが欠落している）セッションが含まれます。

次のルールが、セッション制限の設定に適用されます:

- クラス レベルのセッション制限は、グローバル制限を超えることができます。
- クラス レベルのセッション制限は、関連付けられた VRF セッションの最大値を超えることができます。
- グローバル コンテキストを含む VRF 制限の合計は、ハードコーディングされたセッション制限を超えることができます。

セッション レート

セッション レートは、特定の時間間隔でセッションが確立されるレートです。 最大および最小のセッション レート制限を定義できます。 セッション レートが指定された最大レートを超えると、ファイアウォールは新しいセッション設定要求を拒否するようになります。

リソース管理の観点から、最大および最小のセッション レート制限を設定すると、Cisco Packet Processor が多数のファイアウォール セッション設定要求を受信して過負荷状態になるのを防ぐことができます。

不完全なセッションまたはハーフ オープン セッション

不完全なセッションは、ハーフ オープン セッションです。 最大セッション制限を設定することで、不完全なセッションが使用するリソースがカウントされ、不完全なセッション数の増加が制限されます。

ファイアウォール リソース管理セッション

次のルールが、ファイアウォール リソース管理セッションに適用されます。

- デフォルトでは、開かれたセッションまたはハーフ オープン セッションのセッション制限は無制限です。
- 開かれたセッションまたはハーフ オープン セッションは、パラメータで制限され、個別にカウントされます。
- 開かれたセッション数またはハーフ オープン セッション数には、インターネット制御メッセージ プロトコル（ICMP）、TCP、または UDP セッションが含まれます。
- 開かれたセッションの数とレートを制限できます。

• ハーフ オープン セッションの数のみを制限できます。

分散型サービス拒否攻撃の防止およびリソース管理のための IPv6 ファイアウォール サポートの設定方法

IPv6 ファイアウォールの設定

IPv4 ファイアウォールと IPv6 ファイアウォールを設定する手順は同じです。IPv6 ファイアウォールを設定するには、IPv6 アドレス ファミリだけが一致するようにクラスマップを設定する必要があります。

match protocol コマンドは、IPv4 トラフィックと IPv6 トラフィックの両方に適用され、IPv4 ポリシーまたは IPv6 ポリシーに含めることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf-definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **sessions maximum** *sessions*
9. **exit**
10. **ipv6 unicast-routing**
11. **ip port-map** *appl-name* **port** *port-num* **list** *list-name*
12. **ipv6 access-list** *access-list-name*
13. **permit ipv6 any any**
14. **exit**
15. **class-map type inspect match-all** *class-map-name*
16. **match access-group name** *access-group-name*
17. **match protocol** *protocol-name*
18. **exit**
19. **policy-map type inspect** *policy-map-name*
20. **class type inspect** *class-map-name*
21. **inspect** [*parameter-map-name*]
22. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vrf-definition** *vrf-name* 例： `Device(config)# vrf-definition VRF1`	仮想ルーティングおよび転送（VRF）ルーティング テーブル インスタンスを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、標準 IPv6 アドレス プレフィックスを伝送するセッションを設定します。
ステップ 5	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect ipv6-param-map`	ファイアウォールのグローバル検査タイプ パラメータ マップを、検査アクションに関連するしきい値、タイムアウト、およびその他のパラメータに関連付けることができるようにし、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**sessions maximum** *sessions* 例： `Device(config-profile)# sessions maximum 10000`	ゾーン ペア上に存在可能な最大許容セッション数を設定します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 11	**ip port-map** *appl-name* **port** *port-num* **list** *list-name* 例： `Device(config)# ip port-map ftp port 8090 list ipv6-acl`	IPv6 アクセス コントロール リスト（ACL）を使用してポートツーアプリケーション マッピング（PAM）を確立します。
ステップ 12	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list ipv6-acl`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 13	**permit ipv6 any any** 例： `Device(config-ipv6-acl)# permit ipv6 any any`	IPv6 アクセス リストに許可条件を設定します。
ステップ 14	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**class-map type inspect match-all** *class-map-name* 例： `Device(config)# class-map type inspect match-all ipv6-class`	アプリケーション固有検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 16	**match access-group name** *access-group-name* 例： `Device(config-cmap)# match access-group name ipv6-acl`	指定した ACL をベースにクラス マップに対して一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 17	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルに基づくクラス マップの一致基準を設定します。
ステップ 18	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 19	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ipv6-policy`	プロトコル固有検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 20	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ipv6-class`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 21	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect ipv6-param-map`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 22	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォール セッションのアグレッシブ エージングの設定

アグレッシブ エージング機能をボックス単位（ボックス単位とは、ファイアウォール セッション テーブル全体を意味します）、デフォルト VRF、および VRF 単位のファイアウォール セッションに設定できます。 アグレッシブ エージング機能が動作するには、ファイアウォール セッションのアグレッシブ エージングおよびエージング アウト時間を設定する必要があります。

ファイアウォール セッションのアグレッシブ エージングを設定するには、次の作業を実行します。

ボックス単位のアグレッシブ エージングの設定

ボックス単位とは、ファイアウォール セッション テーブル全体を意味します。 **parameter-map type inspect-global** コマンドに従ったすべての設定がボックスに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **per-box max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
5. **per-box aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **end**
10. **show policy-firewall stats global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかのコマンドを入力します。 • **parameter-map type inspect-global** • **parameter-map type inspect global**	しきい値とタイムアウトを関連付けるグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。 • ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global**

	コマンドまたはアクション	目的

	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		コマンドがサポートされます。 これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 4 と 5 をスキップしてください。
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。

ステップ 4	**per-box max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# per-box max-incomplete 2000 aggressive-aging high 1500 low 1200`	ファイアウォール セッション テーブルのハーフ オープン セッションの上限およびアグレッシブ エージング レートを設定します。
ステップ 5	**per-box aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# per-box aggressive-aging high 1700 low 1300`	総セッションのアグレッシブ エージング制限を設定します。
ステップ 6	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、および **inspect** アクションに関連するその他のパラメータの検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態に達するまでソフトウェアが待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古い TCP 接続の SYN 待機タイマーがデフォルトから設定済みエージアウト時間にリセットされます。 この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。

	コマンドまたはアクション	目的
		接続が低ウォーターマークを下回ると、アグレッシブエージングはディセーブルになります。
ステップ 9	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 10	**show policy-firewall stats global** 例： `Device# show policy-firewall stats global`	グローバルなファイアウォール統計情報を表示します。

デフォルト VRF のアグレッシブ エージングの設定

max-incomplete aggressive-aging コマンドを設定する場合、デフォルト VRF に適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
5. **session total** *number* [**aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}]
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **end**
10. **show policy-firewall stats vrf global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		しきい値とタイムアウトを関連付けるグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。 これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 5 をスキップしてください。
		
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。

ステップ 4	**max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# max-incomplete 3455 aggressive-aging high 2345 low 2255`	ハーフ オープン ファイアウォール セッションの上限およびアグレッシブ エージング制限を設定します。
ステップ 5	**session total** *number* [**aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}] 例： `Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60`	総ファイアウォール セッションの合計制限およびアグレッシブ エージング制限を設定します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、および **inspect** アクションに関連するその他のパラメータの検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態に達するまでソフトウェアが待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古い TCP 接続の SYN 待機タイマーがデフォルトから設定済みエージアウト時間にリセットされます。 この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。接続が低ウォーターマークを下回ると、アグレッシブエージングはディセーブルになります。
ステップ 9	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 10	**show policy-firewall stats vrf global** 例： `Device# show policy-firewall stats vrf global`	グローバル VRF ファイアウォール ポリシーの統計情報を表示します。

VRF 単位のアグレッシブ エージングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*
7. **exit**
8. **parameter-map type inspect-vrf** *vrf-pmap-name*
9. **max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*}
10. **session total** *number* [**aggressive-aging** {**high** *value* **low** *value* | **percent** *percent* **low percent** *percent*}]
11. **alert on**
12. **exit**
13. 次のいずれかのコマンドを入力します。
    - **parameter-map type inspect-global**
    - **parameter-map type inspect global**
14. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
15. **exit**
16. **parameter-map type inspect** *parameter-map-name*
17. **tcp idle-time** *seconds* [**ageout-time** *seconds*]
18. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
19. **exit**
20. **policy-map type inspect** *policy-map-name*
21. **class type inspect match-any** *class-map-name*
22. **inspect** *parameter-map-name*
23. **end**
24. **show policy-firewall stats vrf** *vrf-pmap-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf ddos-vrf1`	VRF インスタンスを定義し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:2`	VRF インスタンスのルート識別子（RD）を指定します。
ステップ 5	**route-target export** *route-target-ext-community* 例： `Device(config-vrf)# route-target export 100:2`	ルートターゲット拡張コミュニティを作成し、ルーティング情報をターゲット VPN 拡張コミュニティにエクスポートします。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Device(config-vrf)# route-target import 100:2`	ルートターゲット拡張コミュニティを作成し、ルーティング情報をターゲット VPN 拡張コミュニティからインポートします。
ステップ 7	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 8	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 9	**max-incomplete** *number* **aggressive-aging high** {*value* **low** *value* | **percent** *percent* **low percent** *percent*} 例： `Device(config-profile)# max-incomplete 2000 aggressive-aging high 1500 low 1200`	ハーフ オープン セッションの上限およびアグレッシブ エージング制限を設定します。

	コマンドまたはアクション	目的
ステップ 10	**session total** *number* [**aggressive-aging** {**high** *value* **low** *value* | **percent** *percent* **low percent** *percent*}] 例： `Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60`	総セッションの総セッション制限およびアグレッシブ エージング制限を設定します。 • 総セッション制限を絶対値またはパーセンテージとして設定できます。
ステップ 11	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 12	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

ステップ 13	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。 これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 14 をスキップしてください。
		
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。

ステップ 14	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	パラメータ マップで VRF をバインドします。
ステップ 15	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 16	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、および **inspect** アクションに関連するその他のパラメータの検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 17	**tcp idle-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp idle-time 3000 ageout-time 100`	アイドル状態の TCP セッションのタイムアウト、および TCP セッションのアグレッシブ エージング アウト時間を設定します。
ステップ 18	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態に達するまでソフトウェアが待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古い TCP 接続の SYN 待機タイマーがデフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。 接続が低ウォーターマークを下回ると、アグレッシブ エージングはディセーブルになります。
ステップ 19	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 20	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 21	**class type inspect match-any** *class-map-name* 例： `Device(config-pmap)# class type inspect match-any ddos-class`	アクションを実行する対象のトラフィック（クラス）を指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 22	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect pmap1`	パラメータ マップのステートフル パケット インスペクションをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 23	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 24	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォールの統計情報を表示します。

例

次に、**show policy-firewall stats vrf vrf1-pmap** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf vrf1-pmap

VRF: vrf1, Parameter-Map: vrf1-pmap
  Interface reference count: 2
       Total Session Count(estab + half-open): 80, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- ------------    ------
       All      0               0
       UDP      0               0
       ICMP     0               0
       TCP      0               0

       TCP Syn Flood Half Open Count: 0, Exceed: 116
       Half Open Aggressive Aging Period Off, Event Count: 0
```

ファイアウォール セッションのエージング アウトの設定

ICMP、TCP、または UDP のファイアウォール セッションのエージング アウトを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
5. **exit**
6. **parameter-map type inspect** *parameter-map-name*
7. **tcp idle-time** *seconds* [**ageout-time** *seconds*]
8. **tcp synwait-time** *seconds* [**ageout-time** *seconds*]
9. **exit**
10. **policy-map type inspect** *policy-map-name*
11. **class type inspect match-any** *class-map-name*
12. **inspect** *parameter-map-name*
13. **end**
14. **show policy-firewall stats vrf** *vrf-pmap-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかのコマンドを入力します。 • **parameter-map type inspect-global** • **parameter-map type inspect global**	グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。 • ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。これら両方のコマンドを一緒に設定することはできません。 • **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 4 をスキップしてください。

	コマンドまたはアクション	目的

	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspectglobal`
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。

ステップ 4	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	パラメータ マップで VRF をバインドします。
ステップ 5	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap1`	接続しきい値、タイムアウト、および **inspect** アクションに関連するその他のパラメータの検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 7	**tcp idle-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp idle-time 3000 ageout-time 100`	アイドル状態の TCP セッションのタイムアウト、および TCP セッションのアグレッシブ エージング アウト時間を設定します。 • **tcp finwait-time** コマンドを設定して、ファイアウォールが finish（FIN）-exchange を検出した後に TCP セッションが管理される時間の長さを指定することもできます。または、**tcp synwait-time** コマンドを設定して、セッションをドロップする前に、TCP セッションが確立状態に達するまでソフトウェアが待機する時間を指定します。
ステップ 8	**tcp synwait-time** *seconds* [**ageout-time** *seconds*] 例： `Device(config-profile)# tcp synwait-time 30 ageout-time 10`	セッションをドロップする前に、TCP セッションが確立状態に達するまでソフトウェアが待機する時間を指定します。 • アグレッシブ エージングがイネーブルになると、最も古い TCP 接続の SYN 待機タイマーがデフォルトから設定済みエージアウト時間にリセットされます。この例では、接続がタイムアウトするまで 30 秒待機する代わりに、最も古い TCP 接続のタイムアウトが 10 秒に設定されます。 接続が低ウォーターマークを下回ると、アグレッシブ エージングはイネーブルになります。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ddos-fw`	プロトコル固有検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 11	**class type inspect match-any** *class-map-name* 例： `Device(config-pmap)# class type inspect match-any ddos-class`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 12	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect pmap1`	パラメータ マップのステートフル パケット インスペクションをイネーブルにします。
ステップ 13	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 14	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォールの統計情報を表示します。

例

次に、**show policy-firewall stats vrf vrf1-pmap** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf vrf1-pmap

 VRF: vrf1, Parameter-Map: vrf1-pmap
  Interface reference count: 2
       Total Session Count(estab + half-open): 270, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- -----------     ------
```

```
All      0               0
UDP      0               0
ICMP     0               0
TCP      0               0

TCP Syn Flood Half Open Count: 0, Exceed: 12
Half Open Aggressive Aging Period Off, Event Count: 0
```

ファイアウォール イベント レート モニタリングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-zone** *zone-pmap-name*
4. **alert on**
5. **threat-detection basic-threat**
6. **threat-detection rate fw-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
7. **threat-detection rate inspect-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
8. **threat-detection rate syn-attack average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
9. **exit**
10. **zone security** *security-zone-name*
11. **protection** *parameter-map-name*
12. **exit**
13. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
14. **end**
15. **show policy-firewall stats zone**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**parameter-map type inspect-zone** *zone-pmap-name* 例： `Device(config)# parameter-map type inspect-zone zone-pmap1`	ゾーン検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ゾーンのステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。 • **log** コマンドを使用して、アラートのロギングを syslog または高速ロガー（HSL）のいずれかに設定できます。
ステップ 5	**threat-detection basic-threat** 例： `Device(config-profile)# threat-detection basic-threat`	ゾーンの基本脅威検出を設定します。
ステップ 6	**threat-detection rate fw-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate fw-drop average-time-frame 600 average-threshold 100 burst-threshold 100`	ファイアウォールのドロップ イベントの脅威検出レートを設定します。 • **threat-detection rate** コマンドを設定する前に、**threat-detection basic-threat** コマンドを設定する必要があります。
ステップ 7	**threat-detection rate inspect-drop average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate inspect-drop average-time-frame 600 average-threshold 100 burst-threshold 100`	ファイアウォール インスペクション ベースのドロップ イベントの脅威検出レートを設定します。
ステップ 8	**threat-detection rate syn-attack average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second* 例： `Device(config-profile)# threat-detection rate syn-attack average-time-frame 600 average-threshold 100 burst-threshold 100`	TCP SYN 攻撃イベントの脅威検出レートを設定します。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**zone security** *security-zone-name* 例： `Device(config)# zone security public`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 11	**protection** *parameter-map-name* 例： `Device(config-sec-zone)# protection zone-pmap1`	ゾーン検査パラメータ マップをゾーンに付加し、ゾーン検査パラメータ マップで設定されている機能をゾーンに適用します。
ステップ 12	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 13	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security private2public source private destination public`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 14	**end** 例： `Device(config-sec-zone-pair)# end`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 15	**show policy-firewall stats zone** 例： `Device# show policy-firewall stats zone`	ゾーン レベルでファイアウォール ポリシーの統計情報を表示します。

ボックス単位のハーフ オープン セッション制限の設定

ボックス単位とは、ファイアウォール セッション テーブル全体を意味します。 **parameter-map type inspect-global** コマンドに従ったすべての設定がボックスに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **alert on**
5. **per-box max-incomplete** *number*
6. **session total** *number*
7. **end**
8. **show policy-firewall stats global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		しきい値とタイムアウトを関連付けるグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドと **parameter-map type inspect global** コマンドがサポートされます。 これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 5 と 6 をスキップしてください。
		
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。

	コマンドまたはアクション	目的
ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 5	**per-box max-incomplete** *number* 例： `Device(config-profile)# per-box max-incomplete 12345`	ファイアウォール セッション テーブルのハーフ オープン接続の最大数を設定します。
ステップ 6	**session total** *number* 例： `Device(config-profile)# session total 34500`	ファイアウォール セッション テーブルの総セッション制限を設定します。
ステップ 7	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 8	**show policy-firewall stats global** 例： `Device# show policy-firewall stats global`	グローバルなファイアウォール統計情報を表示します。

VRF 検査パラメータ マップのハーフ オープン セッション制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-name*
4. **alert on**
5. **max-incomplete** *number*
6. **session total** *number*
7. **exit**
8. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
9. **alert on**
10. **vrf** *vrf-name* **inspect** *vrf-pmap-name*
11. **end**
12. **show policy-firewall stats vrf** *vrf-pmap-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-vrf** *vrf-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**max-incomplete** *number* 例： `Device(config-profile)# max-incomplete 2000`	VRF 単位のハーフ オープン接続の最大数を設定します。
ステップ 6	**session total** *number* 例： `Device(config-profile)# session total 34500`	VRF の総セッション制限を設定します。
ステップ 7	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

ステップ 8	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		しきい値とタイムアウトを関連付けるグローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドまたは **parameter-map type inspect global** コマンドを使用できます。 これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 10 をスキップしてください。
		
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォールセッションに適用されるためです。

ステップ 9	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 10	**vrf** *vrf-name* **inspect** *vrf-pmap-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	グローバル パラメータ マップに VRF をバインドします。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 12	**show policy-firewall stats vrf** *vrf-pmap-name* 例： `Device# show policy-firewall stats vrf vrf1-pmap`	VRF レベル ポリシー ファイアウォールの統計情報を表示します。

グローバル TCP SYN フラッド制限の設定

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **parameter-map type inspect-global**
   - **parameter-map type inspect global**
4. **alert on**
5. **per-box tcp syn-flood limit** *number*
6. **end**
7. **show policy-firewall stats vrf global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	次のいずれかのコマンドを入力します。
	• **parameter-map type inspect-global**
	• **parameter-map type inspect global**
	
	例：
	`Device(config)# parameter-map type inspect-global`
	`Device(config)# parameter-map type inspect global`
		グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
		• ご使用のリリースに基づいて、**parameter-map type inspect-global** コマンドまたは **parameter-map type inspect global** コマンドを設定できます。 これら両方のコマンドを一緒に設定することはできません。
		• **parameter-map type inspect-global** コマンドを設定する場合は、ステップ 5 をスキップしてください。
		
		（注） **parameter-map type inspect-global** コマンドを設定する場合は、**per-box** コンフィギュレーションはサポートされません。これは、デフォルトで、すべての **per-box** コンフィギュレーションがすべてのファイアウォール セッションに適用されるためです。

ステップ 4	**alert on** 例： `Device(config-profile)# alert on`	ステートフル パケット インスペクションのアラート メッセージのコンソール表示をイネーブルにします。
ステップ 5	**per-box tcp syn-flood limit** *number* 例： `Device(config-profile)# per-box tcp syn-flood limit 500`	新しい SYN パケットの SYN Cookie 処理をトリガーする TCP ハーフ オープン セッション数を制限します。
ステップ 6	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**show policy-firewall stats vrf global** 例： `Device# show policy-firewall stats vrf global`	（任意）グローバル VRF ファイアウォール ポリシーのステータスを表示します。 • コマンド出力には、存在する TCP ハーフ オープン セッションの数も表示されます。

例

次に、**show policy-firewall stats vrf global** コマンドの出力例を示します。

```
Device# show policy-firewall stats vrf global

Global table statistics
       total_session_cnt: 0
```

```
exceed_cnt:         0
tcp_half_open_cnt: 0
syn_exceed_cnt:     0
```

ファイアウォール リソース管理の設定

（注） グローバル パラメータ マップは、ルータ レベルではなく、グローバル ルーティング ドメインで有効になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-pmap-name*
4. **session total** *number*
5. **tcp syn-flood limit** *number*
6. **exit**
7. **parameter-map type inspect-global**
8. **vrf** *vrf-name* **inspect** *parameter-map-name*
9. **exit**
10. **parameter-map type inspect-vrf vrf-default**
11. **session total** *number*
12. **tcp syn-flood limit** *number*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Device(config)# parameter-map type inspect-vrf vrf1-pmap`	VRF 検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**session total** *number* 例： `Device(config-profile)# session total 1000`	セッションの総数を設定します。
ステップ 5	**tcp syn-flood limit** *number* 例： `Device(config-profile)# tcp syn-flood limit 2000`	新しいSYNパケットの同期（SYN）Cookie処理をトリガーする TCP ハーフ オープン セッション数を制限します。
ステップ 6	**exit** 例： `Device(config-profile)# exit`	パラメータマップタイプ検査コンフィギュレーションモードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**parameter-map type inspect-global** 例： `Device(config)# parameter-map type inspect-global`	グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 8	**vrf** *vrf-name* **inspect** *parameter-map-name* 例： `Device(config-profile)# vrf vrf1 inspect vrf1-pmap`	パラメータ マップに VRF をバインドします。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータマップタイプ検査コンフィギュレーションモードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**parameter-map type inspect-vrf vrf-default** 例： `Device(config)# parameter-map type inspect-vrf vrf-default`	デフォルトの VRF 検査タイプ パラメータ マップを設定します。

	コマンドまたはアクション	目的
ステップ 11	**session total** *number* 例： `Device(config-profile)# session total 6000`	セッションの総数を設定します。 • **session total** コマンドを VRF 検査タイプ パラメータ マップおよびグローバル パラメータ マップに設定できます。 VRF 検査タイプ パラメータ マップに **session total** コマンドを設定した場合、セッションは VRF 検査タイプ パラメータ マップに関連付けられます。 **session total** コマンドがグローバル パラメータ マップに設定された場合、このコマンドはグローバル ルーティング ドメインに適用されます。
ステップ 12	**tcp syn-flood limit** *number* 例： `Device(config-profile)# tcp syn-flood limit 7000`	新しい SYN パケットの SYN Cookie 処理をトリガーする TCP ハーフ オープン セッション数を制限します。
ステップ 13	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

分散型サービス拒否攻撃の防止およびリソース管理のための IPv6 ファイアウォール サポートの設定例

例：IPv6 ファイアウォールの設定

```
Device# configure terminal
Device(config)# vrf-definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
Device(config)# parameter-map type inspect ipv6-param-map
Device(config-profile)# sessions maximum 10000
Device(config-profile)# exit
Device(config)# ipv6 unicast-routing
Device(config)# ip port-map ftp port 8090 list ipv6-acl
Device(config)# ipv6 access-list ipv6-acl
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# class-map type inspect match-all ipv6-class
Device(config-cmap)# match access-group name ipv6-acl
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
```

```
Device(config)# policy-map type inspect ipv6-policy
Device(config-pmap)# class type inspect ipv6-class
Device(config-pmap-c)# inspect ipv6-param-map
Device(config-pmap-c)# end
```

例：ファイアウォール セッションのアグレッシブ エージングの設定

例：ボックス単位のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# per-box max-incomplete 2000 aggressive-aging 1500 low 1200
Device(config-profile)# per-box aggressive-aging high 1700 low 1300
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# end
```

例：デフォルト VRF のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# max-incomplete 2000 aggressive-aging high 1500 low 1200
Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# end
```

例：VRF 単位のアグレッシブ エージングの設定

```
Device# configure terminal
Device(config)# ip vrf ddos-vrf1
Device(config-vrf)# rd 100:2
Device(config-vrf)# route-target export 100:2
Device(config-vrf)# route-target import 100:2
Device(config-vrf)# exit
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# max-incomplete 3455 aggressive-aging high 2345 low 2255
Device(config-profile)# session total 1000 aggressive-aging high percent 80 low percent 60
Device(config-profile)# alert on
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp idle-time 3000 ageout-time 100
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# exit
Device(config)# policy-map type inspect ddos-fw
Device(config-pmap)# class type inspect match-any ddos-class
Device(config-pmap-c)# inspect pmap1
Device(config-profile)# end
```

例：ファイアウォール セッションのエージング アウトの設定

```
Device# configure terminal
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
```

```
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# exit
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp idle-time 3000 ageout-time 100
Device(config-profile)# tcp synwait-time 30 ageout-time 10
Device(config-profile)# exit
Device(config)# policy-map type inspect ddos-fw
Device(config-profile)# class type inspect match-any ddos-class
Device(config-profile)# inspect pmap1
Device(config-profile)# end
```

例：ファイアウォール イベント レート モニタリングの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect zone zone-pmap1
Device(config-profile)# alert on
Device(config-profile)# threat-detection basic-threat
Device(config-profile)# threat-detection rate fw-drop average-time-frame 600 average-threshold
 100 burst-threshold 100
Device(config-profile)# threat-detection rate inspect-drop average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# threat-detection rate syn-attack average-time-frame 600
average-threshold 100 burst-threshold 100
Device(config-profile)# exit
Device(config)# zone security public
Device(config-sec-zone)# protection zone-pmap1
Device(config-sec-zone)# exit
Device(config)# zone-pair security private2public source private destination public
Device(config-sec-zone-pair)# end
```

例：ボックス単位のハーフ オープン セッション制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# per-box max-incomplete 12345
Device(config-profile)# session total 34500
Device(config-profile)# end
```

例：VRF 検査パラメータ マップのハーフ オープン セッション制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect vrf vrf1-pmap
Device(config-profile)# alert on
Device(config-profile)# max-incomplete 3500
Device(config-profile)# session total 34500
Device(config-profile)# exit
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# vrf vrf1 inspect vrf1-pmap
Device(config-profile)# end
```

例：グローバル TCP SYN フラッド制限の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# alert on
Device(config-profile)# per-box tcp syn-flood limit 500
Device(config-profile)# end
```

例：ファイアウォール リソース管理の設定

```
Device# configure terminal
Device(config)# parameter-map type inspect-vrf vrf1-pmap
Device(config-profile)# session total 1000
Device(config-profile)# tcp syn-flood limit 2000
Device(config-profile)# exit
Device(config)# parameter-map type inspect-global
Device(config-profile)# vrf vrf1 inspect pmap1
Device(config-profile)# exit
Device(config)# parameter-map type inspect-vrf vrf-default
Device(config-profile)# session total 6000
Device(config-profile)# tcp syn-flood limit 7000
Device(config-profile)# end
```

分散型サービス拒否攻撃の防止およびリソース管理のための IPv6 ファイアウォール サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

分散型サービス拒否攻撃の防止およびリソース管理のための IPv6 ファイアウォール サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *21*：分散型サービス拒否攻撃の防止およびリソース管理のための *IPv6* ファイアウォール サポートの機能情報

機能名	リリース	機能情報
分散型サービス拒否攻撃の防止およびリソース管理のための IPv6 ファイアウォール サポート	Cisco IOS XE Release 3.7S	IPv6 ゾーンベース ファイアウォールは、分散型サービス拒否攻撃への保護およびファイアウォール リソース管理機能をサポートします。 分散型サービス拒否攻撃に対する保護機能は、グローバル レベルで（すべてのファイアウォール セッションに対して）および VPN ルーティングおよび転送（VRF）レベルで、サービス拒否（DoS）攻撃から保護します。 分散型 DoS 攻撃を防ぐために、ファイアウォール セッションのアグレッシブ エージング、ファイアウォール セッションのイベント レート モニタリング、ハーフオープン接続制限、およびグローバル TCP SYN Cookie 保護を設定できます。 ファイアウォール リソース管理機能は、デバイス上に設定される VPN ルーティングおよび転送（VRF）インスタンスとグローバル ファイアウォール セッションの数を制限します。

第 16 章

ファイアウォール TCP SYN Cookie の設定

ファイアウォール TCP SYN Cookie 機能は、TCP SYN フラッディング攻撃からファイアウォールを保護します。 TCP SYN フラッディング攻撃は、サービス拒否（DoS）攻撃の一種です。 通常、TCP 同期（SYN）パケットは、ファイアウォールの背後にある対象のエンド ホストまたはサブネット アドレスの範囲に送信されます。 これらの TCP SYN パケットによって、送信元 IP アドレスがスプーフィングされます。 スプーフィング攻撃は、個人またはプログラムが、データを改ざんして不正な優位性を獲得し、別のものになりすますことです。 TCP SYN フラッディングでは、ファイアウォールまたはエンド ホスト上のすべてのリソースを占有し、そのために正当なトラフィックに対する DoS が発生します。 ファイアウォールおよびファイアウォール背後のエンド ホストでの TCP SYN フラッディングを防ぐには、ファイアウォール TCP SYN Cookie 機能を設定する必要があります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ファイアウォール TCP SYN Cookie の設定の制約事項

- デフォルト ゾーンは、ゾーン タイプ パラメータ マップをサポートしていないため、デフォルト ゾーンにファイアウォール TCP SYN Cookie 機能を設定できません。
- ファイアウォール TCP SYN Cookie 機能は、加入者単位のファイアウォールをサポートしません。

ファイアウォール TCP SYN Cookie の設定について

TCP SYN フラッド攻撃

ファイアウォール TCP SYN Cookie 機能は、DoS 攻撃タイプである TCP SYN フラッディング攻撃からファイアウォールを保護するソフトウェアを実装します。

SYN フラッド攻撃は、ハッカーが集中的な接続要求でサーバをフラッディングさせると発生します。 このようなメッセージには到達不可の返信アドレスが含まれているため、接続を確立することができません。 結果としての未解決オープン接続の量が最終的にサーバを過負荷にし、有効な要求に対するサービス拒否を招く可能性があるため、正規ユーザが Web サイトへの接続、電子メールへのアクセス、FTP サービスの使用などを実行できなくなります。

SYN フラッド攻撃は次の 2 つのタイプに分かれています。

- ホストのフラッディング：SYN フラッド パケットは、単一ホスト上のすべてのリソースを利用することを目的として、そのホストに送信されます。
- ファイアウォール セッション テーブルのフラッディング：SYN フラッド パケットが、ファイアウォール上のセッション テーブル リソースを使い果たすことでそのファイアウォールを通過する正当なトラフィックに対してリソースが拒否されることを目的として、ファイアウォール背後のアドレス範囲に送られます。

ファイアウォール TCP SYN Cookie 機能により、TCP 接続要求を代行受信して検証して、SYN フラッディング攻撃を防止することができます。 ファイアウォールは、クライアントからサーバに送信される TCP SYN パケットを代行受信します。 TCP SYN Cookie は、トリガーされると、設定された VPN ルーティングおよび転送（VRF）またはゾーンに向かうすべての SYN パケットで機能します。 TCP SYN Cookie は、宛先サーバの代わりにクライアントとの接続を確立し、クライアントの代わりにサーバとの別の接続を確立して、2 つの半接続をトランスペアレントにバインドします。 したがって、到達不能なホストからの接続試行がサーバに到達することはありません。 TCP SYN Cookie は、接続されている間、パケットを代行受信して転送します。

ファイアウォール TCP SYN Cookie 機能は、グローバル ルーティング ドメインおよび VRF ドメインにセッション テーブル SYN フラッド保護を提供します。 ファイアウォールはグローバル テーブルのセッションを保存するため、TCP ハーフ オープン セッション数に対する制限を設定できます。 TCP ハーフ オープン セッションは、確立状態に達していないセッションです。 VRF 認識ファイアウォールでは、各 VRF の TCP ハーフ オープン セッション数に対する制限を設定できます。 グローバル レベルと VRF レベルの両方で、設定されている制限に達すると、TCP SYN Cookie は、追加のセッションを作成する前に、ハーフ オープン セッションの送信元を確認します。

ファイアウォール TCP SYN Cookie の設定方法

ファイアウォールによるホスト保護の設定

TCP SYN パケットが、単一ホスト上のすべてのリソースを占有することを目的として、そのホストに送信されます。ホストの保護は、送信元ゾーンに対してのみ設定できます。宛先ゾーンに対する保護を設定しても、TCP SYN 攻撃から宛先ゾーンは保護されません。

ファイアウォールによるホスト保護を設定するには、次の作業を実行します。

（注） **show** コマンドを任意の順序で指定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-zone** *zone-pmap-name*
4. **tcp syn-flood rate per-destination** *maximum-rate*
5. **max-destination** *limit*
6. **exit**
7. **zone security** *zone-name*
8. **protection** *parameter-map-name*
9. **exit**
10. **show parameter-map type inspect-zone** *zone-pmap-name*
11. **show zone security**
12. **show policy-firewall stats zone** *zone-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-zone** *zone-pmap-name* 例： `Router(config)# parameter-map type inspect-zone zone-pmap`	ゾーン検査タイプ パラメータ マップを設定し、プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**tcp syn-flood rate per-destination** *maximum-rate* 例： `Router(config-profile)# tcp syn-flood rate per-destination 400`	各宛先アドレスの 1 秒あたりの SYN フラッド パケット数を設定します。 • 特定の宛先アドレスに送信される SYN パケットのレートが、宛先ごとの制限を超えた場合、ファイアウォールは宛先アドレスにルーティングされる SYN パケットの SYN Cookie の処理を開始します。
ステップ 5	**max-destination** *limit* 例： `Router(config-profile)# max-destination 10000`	ファイアウォールがゾーンで追跡可能な宛先の最大数を設定します。 • ファイアウォールは、最大宛先が、*limit* 引数を使用して設定された制限を超えた場合に SYN パケットをドロップします。
ステップ 6	**exit** 例： `Router(config-profile)# exit`	プロファイル コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone security** *zone-name* 例： `Router(config)# zone security secure-zone`	セキュリティ ゾーンを設定し、セキュリティ ゾーン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 8	**protection** *parameter-map-name* 例： `Router(config-sec-zone)# protection zone-pmap`	パラメータ マップを使用して指定のゾーンに対する保護を設定します。
ステップ 9	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーションを終了し、特権 EXEC モードを開始します。
ステップ 10	**show parameter-map type inspect-zone** *zone-pmap-name* 例： `Router# show parameter-map type inspect-zone zone-pmap`	（任意）ゾーン検査タイプ パラメータ マップの詳細を表示します。
ステップ 11	**show zone security** 例： `Router# show zone security`	（任意）ゾーン セキュリティ情報を表示します。
ステップ 12	**show policy-firewall stats zone** *zone-name* 例： `Router# show policy-firewall stats zone secure-zone`	（任意）パケット制限を超え、SYN Cookie によって処理された SYN パケットの数を表示します。

ファイアウォール セッション テーブル保護の設定

ファイアウォール上のセッションテーブルリソースを使い果たすことでそのファイアウォールを通過する正当なトラフィックに対するサービスを拒否することを目的として、TCP SYN パケットがファイアウォール背後のアドレス範囲に送信されます。 グローバル ルーティング ドメインまたは VRF ドメインにファイアウォール セッション テーブル保護を設定できます。

グローバル ルーティング ドメインのファイアウォール セッション テーブル保護の設定

グローバル ルーティング ドメインにファイアウォール セッション テーブル保護を設定するには、次の作業を実行します。

（注） グローバル パラメータ マップは、ルータ レベルではなく、グローバル ルーティング ドメインで有効になります。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**
4. **tcp syn-flood limit** *number*
5. **end**
6. **show policy-firewall stats vrf global**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect global** 例： `Router(config)# parameter-map type inspect global`	グローバル パラメータ マップを設定し、プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**tcp syn-flood limit** *number* 例： `Router(config-profile)# tcp syn-flood limit 500`	新しい SYN パケットの SYN Cookie 処理をトリガーする TCP ハーフ オープン セッション数を制限します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Router(config-profile)# end`	プロファイル コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 6	**show policy-firewall stats vrf global** 例： `Router# show policy-firewall stats vrf global`	（任意）グローバル VRF ファイアウォール ポリシーのステータスを表示します。 • コマンド出力には、存在する TCP ハーフ オープン セッションの数も表示されます。

VRF ドメインのファイアウォール セッション テーブル保護の設定

VRF ドメインにファイアウォール セッション テーブル保護を設定するには、次の作業を実行します。

（注） **show** コマンドを任意の順序で指定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect-vrf** *vrf-pmap-name*
4. **tcp syn-flood limit** *number*
5. **exit**
6. **parameter-map type inspect global**
7. **vrf** *vrf-name* **inspect** *parameter-map-name*
8. **end**
9. **show parameter-map type inspect-vrf**
10. **show policy-firewall stats vrf** *vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect-vrf** *vrf-pmap-name* 例： `Router(config)# parameter-map type inspect-vrf vrf-pmap`	VRF 検査タイプ パラメータ マップを設定し、プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**tcp syn-flood limit** *number* 例： `Router(config-profile)# tcp syn-flood limit 200`	新しい SYN パケットの SYN Cookie 処理をトリガーする TCP ハーフ オープン セッション数を制限します。
ステップ 5	**exit** 例： `Router(config-profile)# exit`	プロファイル コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**parameter-map type inspect global** 例： `Router(config)# parameter-map type inspect global`	VRF 検査タイプ パラメータ マップを VRF にバインドし、プロファイル コンフィギュレーション モードを開始します。
ステップ 7	**vrf** *vrf-name* **inspect** *parameter-map-name* 例： `Router(config-profile)# vrf vrf1 inspect vrf-pmap`	VRF にパラメータ マップをバインドします。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Router(config-profile)# end`	プロファイル コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 9	**show parameter-map type inspect-vrf** 例： `Router# show parameter-map type inspect-vrf`	（任意）VRF 検査タイプ パラメータ マップに関する情報を表示します。
ステップ 10	**show policy-firewall stats vrf** *vrf-name* 例： `Router# show policy-firewall stats vrf vrf-pmap`	（任意）VRF ファイアウォール ポリシーのステータスを表示します。 • コマンド出力には、存在する TCP ハーフ オープン セッションの数も表示されます。

ファイアウォール TCP SYN Cookie の設定例

ファイアウォールによるホスト保護の設定例

次に、ファイアウォールによるホスト保護を設定する例を示します。

```
Router(config)# parameter-map type inspect-zone zone-pmap
Router(config-profile)# tcp syn-flood rate per-destination 400
Router(config-profile)# max-destination 10000
Router(config-profile)# exit
Router(config)# zone security secure-zone
Router(config-sec-zone)# protection zone-pmap
```

ファイアウォール セッション テーブル保護の設定例

グローバル パラメータ マップ

次に、グローバル ルーティング ドメインにファイアウォール セッション テーブル保護を設定する例を示します。

```
Router# configure terminal
Router(config)# parameter-map type inspect global
Router(config-profile)# tcp syn-flood limit 500
Router(config-profile)# end
```

VRF 検査タイプ パラメータ マップ

次に、VRF ドメインにファイアウォール セッション テーブル保護を設定する例を示します。

```
Router# configure terminal
Router(config)# parameter-map type inspect-vrf vrf-pmap
Router(config-profile)# tcp syn-flood limit 200
Router(config-profile)# exit
Router(config)# parameter-map type inspect global
Router(config-profile)# vrf vrf1 inspect vrf-pmap
Router(config-profile)# end
```

ファイアウォール TCP SYN Cookie の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォール TCP SYN Cookie の設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *22*：ファイアウォール *TCP SYN Cookie* の設定の機能情報

機能名	リリース	機能情報
ファイアウォール TCP SYN Cookie	Cisco IOS XE Release 3.3S	ファイアウォール TCP SYN Cookie 機能は、TCP SYN フラッディング攻撃からファイアウォールを保護します。 TCP SYN フラッディング攻撃は、DoS 攻撃の一種です。 通常、TCP SYN パケットは、ファイアウォールの背後にある対象のエンド ホストまたはサブネット アドレスの範囲に送信されます。 これらの TCP SYN パケットによって、送信元 IP アドレスがスプーフィングされます。 スプーフィング攻撃は、個人またはプログラムが、データを改ざんして不正な優位性を獲得し、別のものになりすますことです。 TCP SYN フラッディングでは、ファイアウォールまたはエンド ホスト上のすべてのリソースを占有することで正当なトラフィックに対する DoS が発生します。 ファイアウォールおよびファイアウォール背後のエンドホストでの TCP SYN フラッディングを防ぐには、ファイアウォール TCP SYN Cookie 機能を設定する必要があります。 次のコマンドが導入または変更されました。**parameter-map type inspect-vrf**、**parameter-map type inspect-zone**、**parameter-map type inspect global**、**show policy-firewall stats**、**tcp syn-flood rate per-destination**、**tcp syn-flood limit**。

第 17 章

GPRS トンネリング プロトコル サポートの設定

GPRS トンネリング プロトコル サポート機能は、General Packet Radio Switching（GPRS）トンネリングプロトコル（GTP）にファイアウォールサポートを提供します。GPRSは、既存のGlobal System for Mobile Communication（GSM）ネットワークと統合し、企業ネットワークおよびインターネットへの常時接続パケット交換データ サービスを提供するデータ ネットワーク アーキテクチャです。 欧州通信規格協会（ETSI）の第 3 世代パートナーシップ プロジェクト（3GPP）は、GPRS トンネリング プロトコル（GTP）を作成しました。これにより、ゲートウェイ GPRS サポート ノード（GGSN）、サービング GPRS サポート ノード（SGSN）、および UMTS Terrestrial Radio Access Network（UTRAN）間の UMTS（Universal Mobile Telecommunications System）または GPRS バックボーンでマルチプロトコル パケットをトンネリングできます。

GSM への GPRS の統合により、加入ユーザに携帯電話、モバイル インターネット、および VPN サービスを提供します。 これにより、新たなセキュリティ リスクがネットワークにもたらされます。 GTP は本質的にユーザ データのセキュリティや暗号化を提供しないため、ルータ ファイアウォールは、GTPに対するセキュリティをサポートする必要があります。GPRSトンネリングプロトコルのサポート機能では、GTP に対してファイアウォール サポートを設定します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

GPRS トンネリング サポートの設定の制約事項

- レイヤ 7 クラス マップの match ステートメントの数の制限は 64 です。
- レイヤ 7 ポリシー マップのクラス（デフォルト クラスを含む）の数の制限は 255 です。
- 正規表現パラメータ マップのパターン ストリングの文字数の制限は 245 です。
- データ パスは、最大 512 の正規表現（regex）をサポートします。
- 統計情報は、クラスのパケットおよびバイトでだけ使用可能です。 **match** コマンドで統計情報は使用できません。

GPRS トンネリング プロトコル サポートの設定について

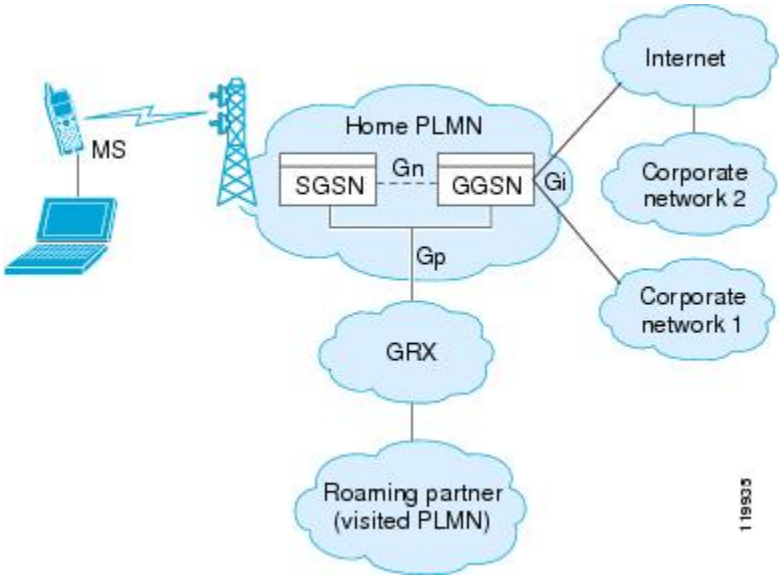
GPRS の概要

General Packet Radio Service（GPRS）は、モバイル通信用グローバル システム（GSM）ネットワークと企業ネットワークやインターネットとの間の中断のない接続をモバイル加入者に提供します。ゲートウェイ GPRS サポート ノード（GGSN）は、GPRS 無線データ ネットワークと他のネットワーク間のインターフェイスです。 サービング GPRS サポート ノード（SGSN）は、モビリティ、データ セッション管理、およびデータ圧縮を実行します。

GPRS コア ネットワーク アーキテクチャには、SGSN に論理的に接続されたモバイル ステーション（MS）が含まれます。 SGSN の主な機能は、MS にデータ サポート サービスを提供することです。 SGSN は、GTP を使用して GGSN に論理的に接続されます。 接続が同じオペレータのパブリック ランド モバイル ネットワーク（PLMN）内にある場合、その接続は Gn インターフェイスと呼ばれます。 接続が 2 つの異なる PLMN 間である場合、その接続は Gp インターフェイスと呼ばれます。 GGSN は、Gi インターフェイスと呼ばれるインターフェイスを介して、インターネットや企業ネットワークなどの外部ネットワークにデータ ゲートウェイを提供します。 GTP は、

MS のデータをカプセル化するために使用されます。 GTP には、ローミング シナリオで SGSN と GGSN 間のトンネルを確立、移動、および削除する機能が含まれます。

図 *23*：*GPRS* コア ネットワーク コア



Universal Mobile Telecommunications System（UMTS）は、固定回線テレフォニー、モバイル、インターネット、コンピュータ テクノロジーの商用コンバージェンスです。 UMTS Terrestrial Radio Access Network（UTRAN）は、システムにワイヤレス ネットワークを実装するために使用されるネットワーキング プロトコルです。 GTP を使用すると、GGSN、SGSN、および UTRAN 間の UMTS/GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。

Gp インターフェイスと Gi インターフェイスは、オペレータのネットワークと信頼できない外部ネットワークとの間の相互接続のプライマリ ポイントです。オペレータは、これらの外部ネットワークから発信された攻撃から自分のネットワークを保護するために注力する必要があります。

Gp インターフェイスは、PLMN 間のモバイル（ローミング）データ ユーザをサポートする論理接続です。 GTP は、ローカル SGSN とユーザのホーム GGSN との間の接続を確立します。

MS から発信されたデータは、Gi インターフェイスに送信されます。 これは、公衆データ網および企業顧客のネットワークに公開されるインターフェイスでもあります。

GGSN から送信される、または Gi インターフェイスで MS に到達するトラフィックは、MS で使用されるアプリケーションが未知であるため、実質的にあらゆる種類のインターフェイスになる可能性があります。

GTP を使用すると、GPRS サポート ノード（GSN）間の GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。 GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによって、SGSN は、トンネルの作成、変更、および削除を行い、MS に GPRS ネットワーク アクセスを提供できます。 GTP は、トンネリング メカニズムを使用して、ユーザ データ パケットを伝送するためのサービスを提供します。

（注） GTP をフェールオーバーと同時に使用しているとき、GTP 接続が確立され、データがトンネルを超えて伝送される前にアクティブ装置に障害が発生した場合、GTP データ接続（「j」フラグが設定されています）は、スタンバイ装置に複製されません。 これは、アクティブ装置が初期接続をスタンバイ装置に複製しないためです。

GTP の概要

General Packet Radio Service（GPRS）トンネリング プロトコル（GTP）を使用すると、GPRS サポート ノード（GSN）間の GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。 3 つの GTP バージョンを使用できます。 GPRS トンネリング サポート機能は、GTP バージョン 0（GTPv0）および GTP バージョン 1（GTPv1）という 2 つの GTP バージョンをサポートします。

GTPv0 では、GPRS モバイル ステーション（MS）は、プロトコルを認識せずにサービング GPRS サポート ノード（SGSN）に接続されます。 パケット データ プロトコル（PDP）コンテキストは、International Mobile Subscriber Identity（IMSI）およびネットワーク サービス アクセス ポイント識別子（NSAPI）との組み合わせであるトンネル識別子（TID）によって識別されます。 各 MS には最大 15 の NSAPI を設定できます。 これにより、MS は、さまざまな Quality of Service（QoS）レベルのアプリケーション要件に基づいて、異なる NSAPI を使用して複数の PDP コンテキストを作成できます。 TID は GTPv0 ヘッダーで伝送されます。

IMSI には次の 3 つの部分があります。

- 3 桁の数字で構成されるモバイル国番号（MCC）。 MCC は、モバイル加入者の居住地の国を一意に識別します。
- GSM アプリケーション用の 2 桁または 3 桁の数字で構成されるモバイル ネットワーク コード（MNC）。 MNC はモバイル加入者のホーム GSM パブリック ランド モバイル ネットワーク（PLMN）を識別します。 MNC の長さは、MCC の値によって異なります。

  （注） 単一 MCC エリア内での 2 桁と 3 桁の MNC コードの組み合わせは推奨されません。

- GSM PLMN 内のモバイル加入者を識別する Mobile Subscriber Identification Number（MSIN）。 National Mobile Subscriber Identity（NMSI）は、MNC と MSIN で構成されます。

GTPv1 は、MS のプライマリ コンテキストとセカンダリ コンテキストの概念を導入します。 プライマリ コンテキストは、IP アドレスに関連付けられ、受信 GSN に付加されるアクセス ポイント名（APN）などの他のパラメータを示します。 このプライマリ PDP コンテキスト用に作成されたセカンダリ コンテキストは、プライマリ コンテキストにすでに関連付けられている IP アドレスやその他のパラメータを共有します。 これにより、MS は、異なる Quality of Service（QoS）要件の別のコンテキストを開始することができ、プライマリ コンテキストですでに取得されている IP アドレスを共有することもできます。 プライマリ コンテキストとセカンダリ コンテキストは、

コントロール プレーンでトンネル エンドポイント ID（TEID）を共有し、データ プレーンでは異なる TEID 値を持ちます。 すべてのプライマリ コンテキストとセカンダリ コンテキストが IP アドレスを共有しているため、MS へのダウンリンク方向のトラフィックを分類するために、トラフィック フローテンプレート（TFT）が使用されます。 TFT は、コンテキストの作成中に交換されます。

プライマリ PDP への PDP コンテキスト作成要求だけに IMSI が含まれます。 IMSI および NSAPI は連携して PDP コンテキストを一意に識別します。 セカンダリ PDP コンテキストのアクティブ化には、この PDP アドレスおよび APN ですでにアクティブ化されている PDP コンテキストのいずれかに割り当てられた NSAPI を示す、Linked NSAPI（LNSAPI）が含まれます。

（注） UDP は、GTPv0 および GTPv1 のシグナリング メッセージ用の唯一サポートされた定義済みのパス プロトコルです。

ファイアウォールを通過する GTP トラフィック

デバイスが検査するメイン General Packet Radio Service（GPRS）トンネリング プロトコル（GTP）トラフィックは、ローミング トラフィックです。 ローミング トラフィックは、モバイル ステーション（MS）がそのホーム パブリック ランド モバイル ネットワーク（HPLMN）から Visited PLMN（VPLMN）に移動すると発生します。

ファイアウォールを通過する GTP トラフィックには次のメッセージが含まれます。

- サービング GPRS サポート ノード（SGSN）からゲートウェイ GPRS サポート ノード（GGSN）への GTP メッセージ
- GGSN-to-SGSN GTP メッセージ
- SGSN-to-SGSN GTP メッセージ

GPRS トンネリング プロトコル サポートの設定方法

General Packet Radio Service（GPRS）トンネリング プロトコル（GTP）コマンドは、レイヤ 7 ポリシー マップで生成される必要なアクションが含まれたフィルタを含む Cisco Common Classification Policy Language（C3PL）レイヤ 7 クラス マップを使用して設定されます。 レイヤ 7 ポリシー マップは、GTP プロトコルと一致するレイヤ 4 クラスで **service-policy (policy-map)** コマンドを使用して、レイヤ 4 ポリシー マップの子ポリシーとして検査アクションで設定されます。 レイヤ 4 ポリシーは、複数のプロトコルに対して複数のクラスを持つことができ、ファイアウォール ゾーン ペアに付加されます。

GPRS トンネリング プロトコル サポートの設定

GPRS トンネリング プロトコル（GTP）サポートを設定するには、次を実行します。

GPRS トンネリング プロトコル サポートの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type regex** *parameter-map-name*
4. **pattern** *expression*
5. **exit**
6. **parameter-map type inspect** {*parameter-map-name* | **global**}
7. **gtp** {**request-queue** *elements* | **timeout** {{**gsn** | **pdp-context** | **signaling** | **tunnel**} *minutes* | **request-queue** *seconds*} | **tunnel-limit** *number*}
8. **exit**
9. **class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name*
10. **match** {**apn regex** *parameter-name* | **mcc** *country-code* **mnc** *network-code* | **message-id** *id* | **message-length min** *min-length* **max** *max-length* | **version** *number*}
11. **exit**
12. **policy-map type inspect** *protocol-name policy-map-name*
13. **class type inspect** *protocol-name class-map-name*
14. **log**
15. **exit**
16. **exit**
17. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
18. **match protocol** *protocol-name* [*parameter-map*] **[signature]**
19. **exit**
20. **policy-map type inspect** *policy-map-name*
21. **class type inspect** *class-map-name*
22. **inspect** [*parameter-map-name*]
23. **service-policy** *protocol-name policy-map*
24. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**parameter-map type regex** *parameter-map-name* 例： `Router# parameter-map type regex PARAM_REG`	特定のトラフィック パターンに一致させるためのパラメータ マップ タイプを設定し、パラメータ マップ コンフィギュレーション モードを開始します。
ステップ 4	**pattern** *expression* 例： `Router(config-profile)# pattern apn.cisco.com`	ローカル URL フィルタリングで許可またはブロックされるドメイン、URL キーワード、または URL メタ文字のリストを指定する一致パターンを設定します。
ステップ 5	**exit** 例： `Router(config-profile)# exit`	パラメータ マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**parameter-map type inspect** {*parameter-map-name* | **global**} 例： `Router(config)# parameter-map type inspect global`	接続しきい値、タイムアウト、および inspect アクションに関連するその他のパラメータの検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ検査モードを開始します。
ステップ 7	**gtp** {**request-queue** *elements* | **timeout** {{**gsn** | **pdp-context** | **signaling** | **tunnel**} *minutes* | **request-queue** *seconds*} | **tunnel-limit** *number*} 例： `Router(config-profile)# gtp tunnel-limit 100`	GTP のインスペクション パラメータを設定します。
ステップ 8	**exit** 例： `Router(config-profile)# exit`	パラメータ マップ タイプ検査モードを終了し、グローバル コンフィギュレーション モードに戻ります。

GPRS トンネリング プロトコル サポートの設定

	コマンドまたはアクション	目的
ステップ 9	**class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name* 例： `Router(config)# class-map type inspect gtpv0 LAYER7_CLASS_MAP`	レイヤ 7（アプリケーション固有）検査タイプ クラスマップを作成し、クラスマップ コンフィギュレーション モードを開始します。
ステップ 10	**match** {**apn regex** *parameter-name* | **mcc** *country-code* **mnc** *network-code* | **message-id** *id* | **message-length min** *min-length* **max** *max-length* | **version** *number*} 例： `Router(config-cmap)# match mcc 100 mnc 91`	GTP の検査タイプ クラス マップ用の分類基準を設定します。
ステップ 11	**exit** 例： `Router(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**policy-map type inspect** *protocol-name policy-map-name* 例： `Router(config)# policy-map type inspect gtpv0 LAYER7_POLICY_MAP`	レイヤ 7（プロトコル固有）検査タイプ ポリシーマップを作成し、ポリシーマップ コンフィギュレーションを開始します。
ステップ 13	**class type inspect** *protocol-name class-map-name* 例： `Router(config-pmap)# class type inspect gtpv0 LAYER7_CLASS_MAP`	アクションを実行する対象のトラフィック（クラス）を指定し、ポリシー マップ クラス コンフィギュレーションを開始します。
ステップ 14	**log** 例： `Router(config-pmap-c)# log`	メッセージのログを生成します。

	コマンドまたはアクション	目的
ステップ 15	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーションを終了し、ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 16	**exit** 例： `Router(config-pmap)# exit`	ポリシー マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 17	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* 例： `Router(config)# class-map type inspect LAYER4_CLASS_MAP`	レイヤ 3 およびレイヤ 4 検査タイプ クラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。
ステップ 18	**match protocol** *protocol-name* [*parameter-map*] **[signature]** 例： `Router(config-cmap)# match protocol gtpv0`	指定したプロトコルに基づいてクラスマップの一致基準を設定します。
ステップ 19	**exit** 例： `Router(config-cmap)# exit`	クラスマップ コンフィギュレーションを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 20	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect LAYER4_POLICY_MAP`	レイヤ 3 とレイヤ 4 の検査タイプ ポリシー マップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 21	**class type inspect** *class-map-name* 例： `Router(config-pmap)# class type inspect LAYER4_CLASS_MAP`	アクションを実行する対象のトラフィック（クラス）を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 22	**inspect** [*parameter-map-name*] 例： `Router(config-pmap-c)# inspect`	Cisco IOS ステートフル パケット インスペクションをイネーブルにします。
ステップ 23	**service-policy** *protocol-name policy-map* 例： `Router(config-pmap-c)# service-policy gtpv0 LAYER7_POLICY_MAP`	レイヤ 7 ポリシー マップをトップレベルのレイヤ 3 またはレイヤ 4 ポリシー マップに付加します。
ステップ 24	**end** 例： `Router(config-pmap-c)# end`	ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GPRS トンネリング プロトコル サポートの設定例

例：GPRS トンネリング プロトコル サポートの設定

次に、GTP トンネリング プロトコル サポートを設定する例を示します。

```
Router> enable
Router# configure terminal
Router# parameter-map type regex PARAM_REG
Router(config-profile)# pattern apn.cisco.com
Router(config-profile)# exit
Router(config)# parameter-map type inspect global
Router(config-profile)# gtp tunnel-limit 100
Router(config-profile)# exit
Router(config)# class-map type inspect gtpv0 LAYER7_CLASS_MAP
Router(config-cmap)# match mcc 100 mnc 91
Router(config-cmap)# exit
Router(config)# policy-map type inspect gtpv0 LAYER7_POLICY_MAP
Router(config-pmap)# class type inspect gtpv0 LAYER7_CLASS_MAP
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# class-map type inspect LAYER4_CLASS_MAP
Router(config-cmap)# match protocol gtpv0
Router(config-cmap)# exit
Router(config)# policy-map type inspect LAYER4_POLICY_MAP
Router(config-pmap)# class type inspect LAYER4_CLASS_MAP
Router(config-pmap-c)# inspect
```

```
Router(config-pmap-c)# service-policy gtpv0 LAYER7_POLICY_MAP
Router(config-pmap-c)# end
```

GPRS トンネリング プロトコル サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GPRS トンネリング プロトコル サポートの設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *23*：*GPRS* トンネリング サポートの設定の機能情報

機能名	リリース	機能情報
GPRS トンネリング プロトコル サポートの設定	Cisco IOS XE Release 3.4S	GPRS トンネリング プロトコル サポート機能は、General Packet Radio Switching（GPRS）トンネリング プロトコル（GTP）にファイアウォール サポートを提供します。 次のコマンドが導入または変更されました。 **class type inspect**、 **class-map type inspect**、 **gtp**、 **match (gtp)**、 **match protocol(zone)**、 **inspect**、 **parameter-map type inspect**、 **parameter-map type regex**、 **policy-map type inspect** **service-policy (policy-map)**、 **show parameter-map type inspect**、 **show parameter-map type regex**、 **show policy-map type inspect zone-pair**。

第 18 章

GPRS トンネリング プロトコル サポート

General Packet Radio Service（GPRS）トンネリング プロトコル バージョン 2（GTPv2）は、2G および 3G モバイル ネットワークで使用される GPRS トンネリング プロトコルを変更して拡張する、第 3 世代パートナーシップ プロジェクト（3GPP）の技術仕様（TS）29.274 で導入されました。 GTPv2 は、GTP アプリケーション インスペクションと制御（AIC）ポリシーを拡張して、加入者データにセキュリティを提供します。

このモジュールでは、ゾーンベースのポリシー ファイアウォール上に GTPv2 を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

GPRS トンネリング プロトコル サポートの制約事項

- レイヤ 7 クラス マップの match ステートメントの数の制限は 64 です。
- レイヤ 7 ポリシー マップのクラス（デフォルト クラスを含む）の数の制限は 255 です。
- 正規表現（regex）パラメータ マップのパターン ストリングの文字数の制限は 245 です。
- データ パスは、最大 512 の正規表現をサポートします。
- **match** コマンドで統計情報は使用できません。 統計情報は、クラスのパケットおよびバイトでだけ使用可能です。
- 3GPP 技術仕様 29.274 リリース 8 および 9 は、GPRS トンネリング プロトコル バージョン 2（GTPv2）と互換性がありません。

GPRS トンネリング プロトコル サポートについて

GTPv2 の概要

進化したパケット サービス（GTP または eGTP）とも呼ばれる General Packet Radio Service（GPRS）トンネリング プロトコル バージョン 2（GTPv2）は、2G および 3G モバイル ネットワークで使用される GPRS トンネリング プロトコルから変更および拡張されました。 GTPv2 には、コントロール プレーン プロトコル（GTPv2-C）とユーザ プレーン プロトコル（GTPv2-U）という 2 つの種類があります。 GTPv2 は、Evolved Packet Core（EPC）ネットワークでの Serving Gateway（SGW）と Packet Data Network（PDN）ゲートウェイ（PGW）間の制御シグナリングに主に使用されます。

第 3 世代パートナーシップ プロジェクト（3GPP）は、第 3 世代（3G）モバイル システム用のグローバルに受け入れ可能な仕様を開発しました。 GPRS は、既存の Global System for Mobile Communication（GSM）ネットワークに統合され、企業ネットワークおよびインターネットへの常時接続パケット交換データ サービスを提供します。

GTPv0 および GTPv1 の詳細については、『セキュリティ コンフィギュレーション ガイド：ゾーンベース ポリシー ファイアウォール』の「GPRS トンネリング プロトコル サポートの設定」の章を参照してください。

図 *24*： *GTPv2-C* ヘッダーの一般的な形式

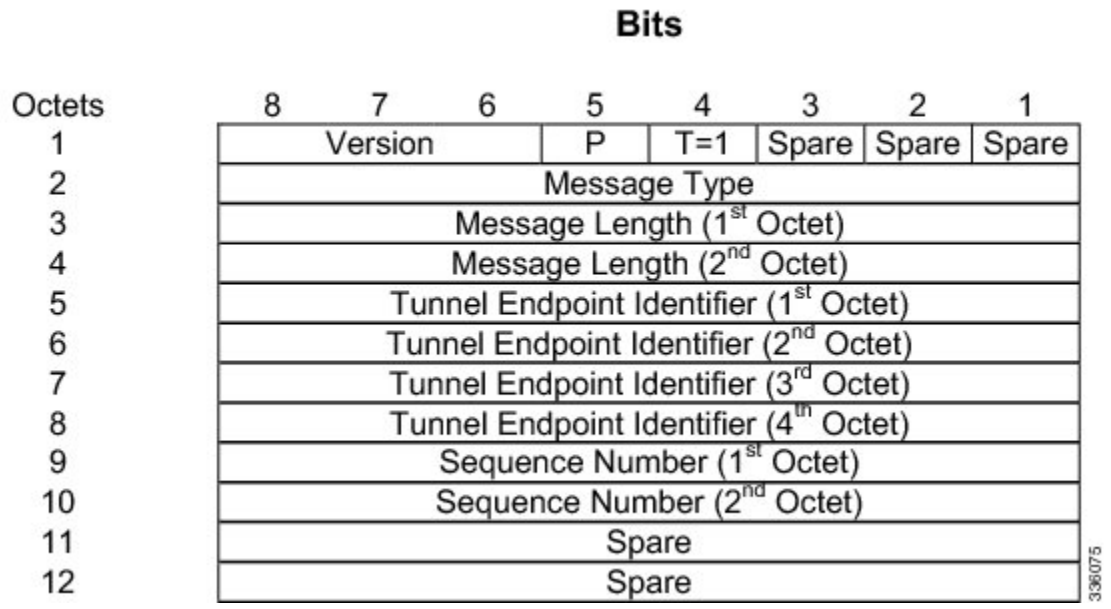
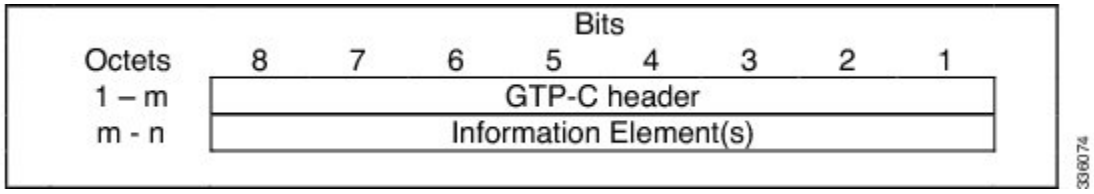


図 *25*：エコーおよびサポートされないバージョンのメッセージの *GTPv2-C* ヘッダー形式



EPC 固有のインターフェイスの GTPv2-C ヘッダーの使用は、下のように定義されています。

オクテット 1：

- オクテット 1 は、10 進数の 2（「010」）に設定されているバージョン（ビット 8 ～ 6）を表します。
- 「T」フラグ（ビット 4）が 1 に設定されている場合、トンネルエンドポイント識別子（TEID）フィールドは、オクテット 5 ～ 8 の Length フィールドのすぐ後に続きます。
- 「P」フラグ（ピギーバック サポート）はサポートされません。

オクテット 2：

- オクテット 2 は、Message Type フィールドを表します。 このフィールドは GTPv2-C メッセージ タイプ値をサポートします。

オクテット 3 ～ 4：

- オクテット 3 および 4 は Length フィールドを表します。 これは、GTPv2-C ヘッダーの必須部分（最初の 4 オクテット）を除くオクテットのメッセージの長さです。

オクテット 5 ～ 8：

- オクテット 5 ～ 8 は、「T」フラグが最初のオクテットに設定されている場合は、Tunnel Identifier フィールドを表します。

オクテット 9 ～ 10：

- オクテット 9 および 10 は、TEID が存在する場合、Sequence Number フィールドを表します。TEID フィールドが存在しない場合、Sequence Number フィールドはオクテット 5 と 6 に含まれます。

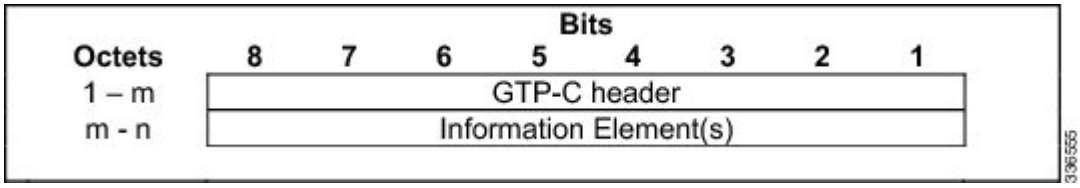
オクテット 11 ～ 12：

- オクテット 11 および 12 は、Sequence Number フィールドの後に続く 2 つのスペア オクテットです。

（注） 次のメッセージを除き、他のすべての GTPv2-C メッセージには、そのヘッダーに TEID が含まれます。

- Echo Request
- エコー応答
- サポートされないバージョンを示す

図 *26*：コントロール プレーンの *GTPv2* メッセージの一般的な形式



ステートフル インスペクション

ダイナミック パケット フィルタリングとも呼ばれるステートフル インスペクションは、パケットのヘッダー内の情報に基づいてそのパケットを検査し、ファイアウォールが接続されている各接続を追跡および検証します。 ステートフルインスペクション中、ファイアウォールは、特定のポートへの接続要求を受信するまでポートを閉じます。

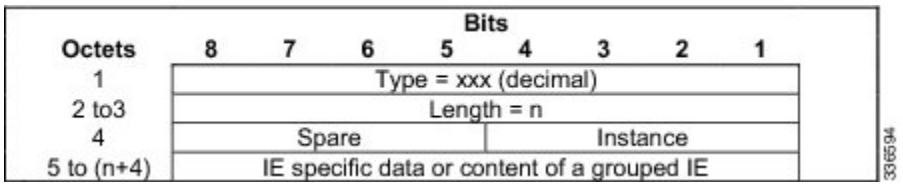
グローバルデータベースは、GTPv2 トラフィックのステートフルインスペクションのためにGTP アプリケーション インスペクションと制御（AIC）ポリシーに構築されます。 GTPv2 メッセージがゾーンベース ファイアウォールを通過する場合、GTP AIC ポリシーはパケット データ プロトコル（PDP）コンテキスト データベースに基づいてメッセージを検査します。 レイヤ 7 インスペクションが必要なパケット（パケットのペイロードの検査または変更が必要）は、コントロール プレーンに渡されます。

情報要素

GTP ヘッダーには、情報要素（IE）と呼ばれるいくつかのオプション フィールドが含まれます。 IE は、GTP プロトコル データ ユニット（PDU）に存在する場合があります。 IE は、メッセージ ヘッダーに含まれる場合があります。

IE は、IE のタイプおよびインスタンスの値で識別されます。 IE のタイプおよびインスタンス値の組み合わせが、メッセージ内の IE を一意に識別します。 グループ化された IE には複数の IE が含まれ、4 オクテットの IE ヘッダーがあります。 グループ化された IE 内の各 IE にも 4 オクテットの IE ヘッダーがあります。 GTPv2 の IE の形式は、TLIV（タイプ、長さ、インスタンス、値）符号化です。 グループ化された IE の長さの値は、組み込まれた IE の合計の長さです。

図 *27*：*GTPv2-C* メッセージ内の情報要素（*IE*）の一般的な形式



オクテット 1：

オクテット 1 は、IE Type フィールドを表します。 IE Type フィールドは、GTPv2-C IE タイプの値をサポートします。

オクテット 2 ～ 3：

オクテット 2 および 3 は、Type および Length フィールドを除く IE の長さを表します。

オクテット 4：

オクテット 4 は、IE のインスタンス番号（ビット 4 ～ 1）を表します。

オクテット 5 ～ n：

オクテット 5 ～ n は、IE に含まれている実際のデータを表します。

GPRS トンネリング プロトコル サポートの設定方法

GPRS トンネリング プロトコル サポートの設定

GPRS トンネリング プロトコル バージョン 2（GTPv2）は、ポリシーおよびクラス マップのゾーンベース ファイアウォール構造を使用して設定されます。 GTPv2 および GTPv1 プロトコルは同じ宛先ポートを共有するため、レイヤ 4 クラス マップは、GTPv2 および GTPv1 を分類できません。レイヤ 7 クラス マップで分類されます。

GPRS トンネリング プロトコル サポートのパラメータ マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type regex** *parameter-map-name*
4. **pattern** *expression*
5. **exit**
6. **parameter-map type inspect-global gtp**
7. **gtpv2** {**request-queue** *elements* | **tunnel-limit** *tunnels*}
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type regex** *parameter-map-name* 例： `Device(config)# parameter-map type regex PARAM-REG`	特定のトラフィック パターンに一致させるための正規表現パラメータ マップ タイプを設定し、パラメータ マップ タイプ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**pattern** *expression* 例： `Device(config-profile)# pattern apn.cisco.com`	ローカル URL フィルタリングで許可またはブロックされるドメイン、URL キーワード、または URL メタ文字のリストを指定する一致パターンを設定します。
ステップ 5	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**parameter-map type inspect-global gtp** 例： `Device(config)# parameter-map type inspect-global gtp`	接続しきい値、タイムアウト、および **inspect** アクションに関連するその他のパラメータの検査タイプ パラメータ マップを設定し、パラメータ マップ タイプ コンフィギュレーション モードを開始します。
ステップ 7	**gtpv2** {**request-queue** *elements* | **tunnel-limit** *tunnels*} 例： `Device(config-profile)# gtpv2 request-queue 429496`	GTP のインスペクション パラメータを設定します。
ステップ 8	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査モードを終了し、特権 EXEC モードに戻ります。

例：GPRS トンネリング プロトコル サポートのパラメータ マップ

次に、**show parameter-map type** コマンドの出力例を示します。

```
Device# show parameter-map type inspect-global gtp

parameter-map type inspect-global gtp
  gtp request-queue 40000 (default)
  gtp tunnel-limit 40000 (default)
  gtp pdp-context timeout 300 (default)
  gtp request-queue timeout 60 (default)
  permit-error Disable (default)
  gtpv2 request-queue 429496729
  gtpv2 tunnel-limit 42949672
```

GPRS トンネリング プロトコル サポートのクラス マップおよびポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name*
4. **match** {**apn regex** *parameter-name* | {**mcc** *country-code* **mnc** *network-code* | **message-length msisdn regex** *parameter-name* | **version** *number*}
5. **exit**
6. **policy-map type inspect** *protocol-name policy-map-name*
7. **class type inspect** *protocol-name class-map-name*
8. **inspect**
9. **service-policy** *protocol-name* **policy-map**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect** *protocol-name* {**match-any**	**match-all**} *class-map-name* 例： `Device(config)# class-map type inspect gtpv1 match-any gtpv2-cl7-1`	レイヤ 7（アプリケーション固有）検査タイプ クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match** {**apn regex** *parameter-name*	{**mcc** *country-code* **mnc** *network-code*	**message-length msisdn regex** *parameter-name*	**version** *number*} 例： `Device(config-cmap)# match version 2`	GTP の検査タイプ クラス マップ用の分類基準を設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**policy-map type inspect** *protocol-name policy-map-name* 例： `Device(config)# policy-map type inspect gtpv1 gtpv2-POLICY-MAP`	レイヤ7（プロトコル固有）検査タイプ ポリシーマップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *protocol-name class-map-name* 例： `Device(config-pmap)# class type inspect gtpv1 gtpv2-cl7-1`	アクションを実行する対象のトラフィック（クラス）を指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**service-policy** *protocol-name* **policy-map** 例： `Device(config-pmap-c)# service-policy gtpv1 gtpv2-POLICY-MAP`	レイヤ 7 ポリシー マップをトップレベルのレイヤ 3 またはレイヤ 4 ポリシー マップに付加します。
ステップ 10	**end** 例： `Device(config-pmap-c)# end`	ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GPRS トンネリング プロトコル サポートのゾーンおよびゾーン ペアの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone-pair security***zone-pair-name***source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}
6. **service-policy type inspect** *policy-map-name*
7. **exit**
8. **interface type** *number*
9. **zone-member security** *zone-name*
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**zone security** {*zone-name*	**default**}
		
		例：
		`Device(config)# zone security z1`
		`Device(config)# zone security z2`
			インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
			（注） セキュリティ ゾーン ペアを作成するには、インターフェイスを割り当てる 2 つのセキュリティ ゾーン（z1 と z2）を設定する必要があります。

ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**zone-pair security***zone-pair-name***source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**} 例： `Device(config)# zone-pair security clt2srv1 source z1 destination z2`	セキュリティ ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 6	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect gtpv2-POLICY-MAP`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） セキュリティ ゾーンのペア間でポリシーが設定されていない場合、トラフィックはデフォルトでドロップされます。
ステップ 7	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface type** *number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 9	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 （注） インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 10	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GPRS トンネリング プロトコル サポートの設定例

例：GPRS トンネリング プロトコル サポートの設定

次に、GTPv2 サポートを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type regex PARAM-REG
Device(config-profile)# pattern apn.cisco.com
Device(config-profile)# exit
Device(config)# parameter-map type inspect-global
Device(config-profile)# gtpv2 tunnel-limit 100
Device(config-profile)# exit
Device(config)# class-map type inspect gtpv1 match-any gtpv2-cl7-1
Device(config-cmap)# match version 2
Device(config-cmap)# exit
Device(config)# policy-map type inspect gtpv1 gtpv2-POLICY-MAP
Device(config-pmap)# class type inspect gtpv1 gtpv2-cl7-1
Device(config-pmap-c)# inspect
Device(config-pmap-c)# service-policy gtpv1 gtpv2-POLICY-MAP
Device(config-pmap)# end
```

例：GPRS トンネリング プロトコル サポートのゾーンおよびゾーン ペアの設定

次に、GTPv2 にゾーンおよびゾーン ペアを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone-pair security clt2srv1 source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect gtpv2-POLICY-MAP
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# ip address 5.0.0.1 255.255.255.0
Device(config-if)# zone-member security z1
Device(config-if)# exit
Device(config)# interface gigabitethernet0/0/2
Device(config-if)# ip address 4.0.0.1 255.255.255.0
Device(config-if)# zone-member security z2
Device(config)# end
```

GPRS トンネリング プロトコル サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	『Security Command Reference: Commands A to C』 『Security Command Reference: Commands D to L』 『Security Command Reference: Commands M to R』 『Security Command Reference: Commands S to Z』
セキュリティ設定	『Security Configuration Guide: Zone-Based Policy Firewall』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

GPRS トンネリング プロトコル バージョン 2 サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *24*：***GPRS*** トンネリング プロトコル バージョン *2* サポートの機能情報

機能名	リリース	機能情報
GTPv2 Support	Cisco IOS XE Release 3.9S	GTPv2 サポート機能は、第 3 世代パートナーシップ プロジェクト（3GPP）TS 29.274 によって導入され、2G および 3G モバイル ネットワークで使用される GPRS トンネリング プロトコルを変更および拡張します。 GTPv2 は、GTP アプリケーション インスペクションと制御（AIC）ポリシーを拡張して、加入者データにセキュリティを提供します。 このモジュールでは、ゾーンベースのポリシー ファイアウォール上に GTPv2 を設定する方法について説明します。 次のコマンドが、新たに導入または変更されました。**show parameter-map type inspect-global**、**zone-pair security**。

第 19 章

ファイアウォールのGGSNプーリングサポート

ファイアウォールの GGSN プーリング サポート機能は、ロード バランシング サポートを追加することで、General Packet Radio Switching（GPRS）トンネリング プロトコル（GTP）機能を拡張します。 GTP は、単一のゲートウェイ GPRS サポート ノード（GGSN）に指定された制御トラフィックのインスペクションをサポートします。 Global System for Mobile Communication（GSM）ネットワークに効率性と拡張性を提供するために、ロード バランシングがトポロジに追加されます。 ロード バランサは、サービング GPRS サポート ノード（SGSN）からプール内のさまざまな GGSN に要求を送信します。

このモジュールでは、ファイアウォールの GGSN プーリング サポート機能を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

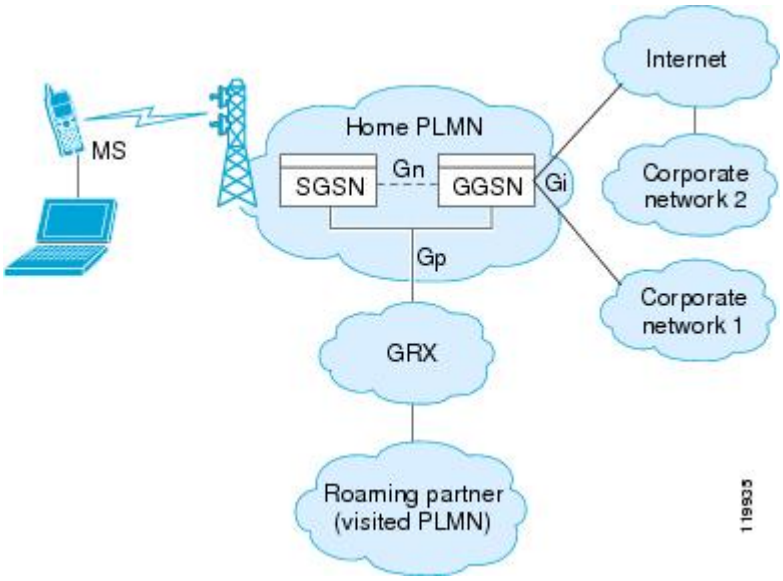
ファイアウォールの GGSN プーリング サポートについて

GPRS の概要

General Packet Radio Service（GPRS）は、モバイル通信用グローバル システム（GSM）ネットワークと企業ネットワークやインターネットとの間の中断のない接続をモバイル加入者に提供します。ゲートウェイ GPRS サポート ノード（GGSN）は、GPRS 無線データ ネットワークと他のネットワーク間のインターフェイスです。サービング GPRS サポート ノード（SGSN）は、モビリティ、データ セッション管理、およびデータ圧縮を実行します。

GPRS コア ネットワーク アーキテクチャには、SGSN に論理的に接続されたモバイル ステーション（MS）が含まれます。 SGSN の主な機能は、MS にデータ サポート サービスを提供することです。 SGSN は、GTP を使用して GGSN に論理的に接続されます。 接続が同じオペレータのパブリック ランド モバイル ネットワーク（PLMN）内にある場合、その接続は Gn インターフェイスと呼ばれます。 接続が 2 つの異なる PLMN 間である場合、その接続は Gp インターフェイスと呼ばれます。 GGSN は、Gi インターフェイスと呼ばれるインターフェイスを介して、インターネットや企業ネットワークなどの外部ネットワークにデータ ゲートウェイを提供します。 GTP は、MS のデータをカプセル化するために使用されます。 GTP には、ローミング シナリオで SGSN と GGSN 間のトンネルを確立、移動、および削除する機能が含まれます。

図 *28*：*GPRS* コア ネットワーク コア



Universal Mobile Telecommunications System（UMTS）は、固定回線テレフォニー、モバイル、インターネット、コンピュータ テクノロジーの商用コンバージェンスです。 UMTS Terrestrial Radio Access Network（UTRAN）は、システムにワイヤレス ネットワークを実装するために使用されるネットワーキング プロトコルです。 GTP を使用すると、GGSN、SGSN、および UTRAN 間の UMTS/GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。

Gp インターフェイスと Gi インターフェイスは、オペレータのネットワークと信頼できない外部ネットワークとの間の相互接続のプライマリ ポイントです。オペレータは、これらの外部ネットワークから発信された攻撃から自分のネットワークを保護するために注力する必要があります。

Gp インターフェイスは、PLMN 間のモバイル（ローミング）データ ユーザをサポートする論理接続です。 GTP は、ローカル SGSN とユーザのホーム GGSN との間の接続を確立します。

MS から発信されたデータは、Gi インターフェイスに送信されます。 これは、公衆データ網および企業顧客のネットワークに公開されるインターフェイスでもあります。

GGSN から送信される、または Gi インターフェイスで MS に到達するトラフィックは、MS で使用されるアプリケーションが未知であるため、実質的にあらゆる種類のインターフェイスになる可能性があります。

GTP を使用すると、GPRS サポート ノード（GSN）間の GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。 GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによって、SGSN は、トンネルの作成、変更、および削除を行い、MS に GPRS ネットワーク アクセスを提供できます。 GTP は、トンネリング メカニズムを使用して、ユーザ データ パケットを伝送するためのサービスを提供します。

（注） GTP をフェールオーバーと同時に使用しているとき、GTP 接続が確立され、データがトンネルを超えて伝送される前にアクティブ装置に障害が発生した場合、GTP データ接続（「j」フラグが設定されています）は、スタンバイ装置に複製されません。 これは、アクティブ装置が初期接続をスタンバイ装置に複製しないためです。

GTP の概要

General Packet Radio Service（GPRS）トンネリング プロトコル（GTP）を使用すると、GPRS サポート ノード（GSN）間の GPRS バックボーンで、マルチプロトコル パケットをトンネリングできます。 3 つの GTP バージョンを使用できます。 GPRS トンネリング サポート機能は、GTP バージョン 0（GTPv0）および GTP バージョン 1（GTPv1）という 2 つの GTP バージョンをサポートします。

GTPv0 では、GPRS モバイル ステーション（MS）は、プロトコルを認識せずにサービング GPRS サポート ノード（SGSN）に接続されます。 パケット データ プロトコル（PDP）コンテキストは、International Mobile Subscriber Identity（IMSI）およびネットワーク サービス アクセス ポイント識別子（NSAPI）との組み合わせであるトンネル識別子（TID）によって識別されます。 各 MS には最大 15 の NSAPI を設定できます。 これにより、MS は、さまざまな Quality of Service（QoS）レベルのアプリケーション要件に基づいて、異なる NSAPI を使用して複数の PDP コンテキストを作成できます。 TID は GTPv0 ヘッダーで伝送されます。

IMSI には次の 3 つの部分があります。

- 3 桁の数字で構成されるモバイル国番号（MCC）。 MCC は、モバイル加入者の居住地の国を一意に識別します。
- GSM アプリケーション用の 2 桁または 3 桁の数字で構成されるモバイル ネットワーク コード（MNC）。 MNC はモバイル加入者のホーム GSM パブリック ランド モバイル ネットワーク（PLMN）を識別します。 MNC の長さは、MCC の値によって異なります。

（注） 単一 MCC エリア内での 2 桁と 3 桁の MNC コードの組み合わせは推奨されません。

- GSM PLMN 内のモバイル加入者を識別する Mobile Subscriber Identification Number（MSIN）。 National Mobile Subscriber Identity（NMSI）は、MNC と MSIN で構成されます。

GTPv1 は、MS のプライマリ コンテキストとセカンダリ コンテキストの概念を導入します。 プライマリ コンテキストは、IP アドレスに関連付けられ、受信 GSN に付加されるアクセス ポイント名（APN）などの他のパラメータを示します。 このプライマリ PDP コンテキスト用に作成されたセカンダリ コンテキストは、プライマリ コンテキストにすでに関連付けられている IP アドレスやその他のパラメータを共有します。 これにより、MS は、異なる Quality of Service（QoS）要件の別のコンテキストを開始することができ、プライマリ コンテキストですでに取得されている IP アドレスを共有することもできます。 プライマリ コンテキストとセカンダリ コンテキストは、コントロール プレーンでトンネル エンドポイント ID（TEID）を共有し、データ プレーンでは異なる TEID 値を持ちます。 すべてのプライマリ コンテキストとセカンダリ コンテキストが IP アドレスを共有しているため、MS へのダウンリンク方向のトラフィックを分類するために、トラフィック フローテンプレート（TFT）が使用されます。 TFT は、コンテキストの作成中に交換されます。

プライマリ PDP への PDP コンテキスト作成要求だけに IMSI が含まれます。 IMSI および NSAPI は連携して PDP コンテキストを一意に識別します。 セカンダリ PDP コンテキストのアクティブ化には、この PDP アドレスおよび APN ですでにアクティブ化されている PDP コンテキストのいずれかに割り当てられた NSAPI を示す、Linked NSAPI（LNSAPI）が含まれます。

（注） UDP は、GTPv0 および GTPv1 のシグナリング メッセージ用の唯一サポートされた定義済みのパス プロトコルです。

GGSN プーリング サポート

ゲートウェイ GPRS サポート ノード（GGSN）は、サーバ ロード バランシング（SLB）機能を使用して、ファイアウォール ロード バランシングをサポートします。 SLB は、ファイアウォール ファームと呼ばれるファイアウォールのグループ間でトラフィック フローを分散させます。 このクラスタまたはプールで、クライアントは仮想サーバの IP アドレスに接続できます。 クライアン

トが仮想サーバへの接続を開始すると、SLBは、設定されているロードバランシングアルゴリズムに基づいて、接続する実サーバを選択します。

GTP ロード バランシングを設定する場合、GGSN のプールは SLB での GGSN ファームとして設定されます。 これらの GGSN を使用して、GPRS トンネリング プロトコル（GTP）セッションをロード バランシングすることができます。 GGSN ファーム全体で GTP セッションをロード バランシングするために、SLB で仮想サーバ インスタンスが設定されます。

GGSN プーリングをサポートするには、デバイスは、GSN が GTP SLB パケット内の IP アドレスとして指定されたものとは異なる場合でも、GSNのロードバランシングを許可し、パケットデータ プロトコル（PDP）要求に応答する必要があります。

GGSN プーリングでは、ローミング接続を使用する加入者が、サービング GPRS サポート ノード（SGSN）から、SLB の背後に存在する GGSN に PDP 要求を送信すると、ファイアウォールは PDP 要求を受け入れる必要があります。 ピンホールは未知の GGSN に作成されないため、ファイアウォールは PDP 応答をドロップします。 ファイアウォールによって PDP 応答がドロップされないようにするには、アクセス コントロール リスト（ACL）を設定する必要があります。 ファイアウォール ピンホールは、保護されたネットワークへの制御アクセスをアプリケーションが取得できるようにするために、ファイアウォールに開かれたポートです。

グローバル セッション データベースは、PDP 要求が SGSN から受信されると、保留中のすべての PDP 要求コンテキストを記録します。 PDP 要求が SGSN から受信されると、コンテキストを照合するためのセッション ルックアップが実行され、一致が見つからない場合は応答がドロップされます。 パケット データは、実質的にデータ セッションである PDP コンテキストの確立によって転送されます。

ファイアウォールを通過する GTP トラフィック

デバイスが検査するメイン General Packet Radio Service（GPRS）トンネリング プロトコル（GTP）トラフィックは、ローミング トラフィックです。 ローミング トラフィックは、モバイル ステーション（MS）がそのホーム パブリック ランド モバイル ネットワーク（HPLMN）から Visited PLMN（VPLMN）に移動すると発生します。

ファイアウォールを通過する GTP トラフィックには次のメッセージが含まれます。

- サービング GPRS サポート ノード（SGSN）からゲートウェイ GPRS サポート ノード（GGSN）への GTP メッセージ
- GGSN-to-SGSN GTP メッセージ
- SGSN-to-SGSN GTP メッセージ

ファイアウォールの GGSN プーリング サポートの設定方法

GGSN プーリングのアクセス コントロール リストおよびクラス マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **permit** *protocol source source-wildcard* **any**
4. **access-list** *access-list-number* **permit** *protocol* **any** *destination destination-wildcard*
5. **access-list** *access-list-number* **permit** *protocol source source-wildcard* **any**
6. **class-map type inspect gtpv1 match-any** *class-map-name*
7. **match mcc** *country-code* **mnc** *network-code*
8. **match mcc** *country-code* **mnc** *network-code*
9. **exit**
10. **class-map type inspect gtpv1 match-any** *class-map-name*
11. **match mcc** *country-code* **mnc** *network-code*
12. **match mcc** *country-code* **mnc** *network-code*
13. **exit**
14. **class-map type inspect gtpv1 match-all** *class-map-name*
15. **match protocol** *protocol-name*
16. **match access-group** *access-list-number*
17. **exit**
18. **class-map type inspect gtpv1 match-all** *class-map-name*
19. **match protocol** *protocol-name*
20. **match access-group** *access-list-number*
21. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* **permit** *protocol source source-wildcard* **any** 例： `Device(config)# access-list 101 permit ip 10.2.2.0 255.255.255.0 any`	拡張 IP アクセス リストを定義します。 • この例で設定されるアクセス リスト 101 は、GGSN または SGSN から任意の宛先へのトラフィックを許可します。
ステップ 4	**access-list** *access-list-number* **permit** *protocol* **any** *destination destination-wildcard* 例： `Device(config)# access-list 102 permit ip any 10.2.2.0 255.255.255.0`	拡張 IP アクセス リストを定義します。 • この例で設定されるアクセス リスト 102 は、任意の送信元から GGSN または SGSN へのトラフィックを許可します。
ステップ 5	**access-list** *access-list-number* **permit** *protocol source source-wildcard* **any** 例： `Device(config)# access-list 103 permit ip 10.2.2.0 255.255.255.0 any`	拡張 IP アクセス リストを定義します。 • この例で設定されるアクセス リスト 103 は、GGSN または SGSN から任意の宛先へのトラフィックを許可します。
ステップ 6	**class-map type inspect gtpv1 match-any** *class-map-name* 例： `Device(config)# class-map type inspect gtpv1 match-any gtp-cl7-rev`	アプリケーション固有検査タイプ クラスマップを作成し、クラスのメンバーと見なされるためには指定した一致条件のいずれかをパケットが満たす必要があることを指定して、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 7	**match mcc** *country-code* **mnc** *network-code* 例： `Device(config-cmap)# match mcc 1 mnc 1`	有効なモバイル国番号（MCC）およびモバイル ネットワーク コード（MNC）のフィルタリングを設定します。 • この例では、外国の MCC および MNC へのローミング接続のフィルタリングを設定します。
ステップ 8	**match mcc** *country-code* **mnc** *network-code* 例： `Device(config-cmap)# match mcc 2 mnc 1`	有効な MCC と MNC のフィルタリングを設定します。 • この例では、ローカルの MCC および MNC へのローミング接続のフィルタリングを設定します。
ステップ 9	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**class-map type inspect gtpv1 match-any** *class-map-name* 例： `Device(config)# class-map type inspect gtpv1 match-any gtp-cl7`	アプリケーション固有検査タイプ クラスマップを作成し、クラスのメンバーと見なされるためには指定した一致条件のいずれかをパケットが満たす必要があることを指定して、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 11	**match mcc** *country-code* **mnc** *network-code* 例： `Device(config-cmap)# match mcc 2 mnc 1`	有効な MCC と MNC のフィルタリングを設定します。
ステップ 12	**match mcc** *country-code* **mnc** *network-code* 例： `Device(config-cmap)# match mcc 1 mnc 1`	有効な MCC と MNC のフィルタリングを設定します。
ステップ 13	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 14	**class-map type inspect gtpv1 match-all** *class-map-name* 例： `Device(config)# class-map type inspect gtpv1 match-all gtp-l4c`	アプリケーション固有検査タイプ クラスマップを作成し、クラスのメンバーと見なされるためには指定した一致条件のすべてをパケットが満たす必要があることを指定して、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 15	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol gtpv1`	指定されたプロトコルに基づくクラス マップの一致基準を設定します。
ステップ 16	**match access-group** *access-list-number* 例： `Device(config-cmap)# match access-group 101`	指定された ACL に基づくクラス マップの一致基準を設定します。
ステップ 17	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 18	**class-map type inspect gtpv1 match-all** *class-map-name* 例： `Device(config)# class-map type inspect gtpv1 match-all gtp-l4c-rev`	アプリケーション固有検査タイプクラスマップを作成し、クラスのメンバーと見なされるためには指定した一致条件のすべてをパケットが満たす必要があることを指定して、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 19	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol gtpv1`	指定されたプロトコルに基づくクラス マップの一致基準を設定します。
ステップ 20	**match access-group** *access-list-number* 例： `Device(config-cmap)# match access-group 102`	指定された ACL に基づくクラス マップの一致基準を設定します。
ステップ 21	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

GGSN プーリングのポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect gtpv1** *gtpv1-policy*
4. **class type inspect gtpv1** *class-map-name*
5. **log**
6. **exit**
7. **class class-default**
8. **exit**
9. **policy-map type inspect gtpv1** *gtpv1-policy*
10. **class type inspect gtpv1** *class-map-name*
11. **log**
12. **exit**
13. **class class-default**
14. **exit**
15. **policy-map type inspect gtpv1** *gtpv1-policy*
16. **class type inspect gtpv1** *class-map-name*
17. **inspect**
18. **service-policy** *policy-map-name*
19. **exit**
20. **class class-default**
21. **exit**
22. **policy-map type inspect gtpv1** *gtpv1-policy*
23. **class type inspect gtpv1** *class-map-name*
24. **inspect**
25. **service-policy** *policy-map-name*
26. **exit**
27. **class class-default**
28. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect gtpv1** *gtpv1-policy* 例： `Device(config)# policy-map type inspect gtpv1 gtp-l7p-rev`	プロトコル固有検査タイプ ポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class type inspect gtpv1** *class-map-name* 例： `Device(config-pmap)# class type inspect gtpv1 gtp-cl7-rev`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**log** 例： `Device(config-pmap-c)# log`	メッセージのログを生成します。
ステップ 6	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 7	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 8	**exit** 例： `Device(config-pmap)# exit`	QoS ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 9	**policy-map type inspect gtpv1** *gtpv1-policy* 例： `Device(config)# policy-map type inspect gtpv1 gtp-l7p`	プロトコル固有検査タイプ ポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 10	**class type inspect gtpv1** *class-map-name* 例： `Device(config-pmap)# class type inspect gtpv1 gtp-cl7`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**log** 例： `Device(config-pmap-c)# log`	メッセージのログを生成します。
ステップ 12	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 13	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 14	**exit** 例： `Device(config-pmap)# exit`	QoS ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**policy-map type inspect gtpv1** *gtpv1-policy* 例： `Device(config)# policy-map type inspect gtpv1 gtp-l4p-rev`	プロトコル固有検査タイプ ポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 16	**class type inspect gtpv1** *class-map-name* 例： `Device(config-pmap)# class type inspect gtpv1 gtp-l4c-rev`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 17	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 18	**service-policy** *policy-map-name* 例： `Device(config-pmap-c)# service-policy gtp-l7p-rev`	ポリシー マップ内の QoS ポリシー（階層サービス ポリシーと呼ばれる）としてサービス ポリシーを使用します。
ステップ 19	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 20	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 21	**exit** 例： `Device(config-pmap)# exit`	QoS ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 22	**policy-map type inspect gtpv1** *gtpv1-policy* 例： `Device(config)# policy-map type inspect gtpv1 gtp-l4p`	プロトコル固有検査タイプ ポリシーマップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 23	**class type inspect gtpv1** *class-map-name* 例： `Device(config-pmap)# class type inspect gtpv1 gtp-l4c`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 24	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 25	**service-policy** *policy-map-name* 例： `Device(config-pmap-c)# service-policy gtp-l7p`	ポリシー マップ内の QoS ポリシー（階層サービス ポリシーと呼ばれる）としてサービス ポリシーを使用します。
ステップ 26	**exit** 例： `Device(config-pmap)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 27	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 28	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

GGSN プーリング サポートのゾーンおよびゾーン ペアの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *security-zone*
4. **exit**
5. **zone security** *security-zone*
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
11. **service-policy type inspect** *policy-map-name*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device(config)# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *security-zone* 例： `Device(config)# zone security roam-in`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定には、ゾーン ペアを作成するために、2 つのセキュリティ ゾーン（送信元ゾーンと宛先ゾーン）が含まれている必要があります。 • ゾーン ペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**zone security** *security-zone* 例： `Device(config-sec-zone)# zone security roam-out`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security in2out source roam-in destination roam-out`	セキュリティ ゾーンのペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。 • ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect gtp-l4p`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security out2in source roam-out destination roam-in`	セキュリティ ゾーンのペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 11	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect gtp-l4p-rev`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Device(config-sec-zone)# end`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォールの GGSN プーリング サポートの設定例

例：GGSN プーリングのアクセス コントロール リストおよびクラス マップの設定

```
Device# configure terminal
Device(config)# access-list 101 permit ip 10.2.2.0 255.255.255.0 any
Device(config)# access-list 102 permit ip any 10.2.2.0 255.255.255.0
Device(config)# access-list 103 permit ip 10.2.2.0 255.255.255.0 any
Device(config)# class-map type inspect gtpv1 match-any gtp-cl7-rev
Device(config-cmap)# match mcc 1 mnc 1
Device(config-cmap)# match mcc 2 mnc 1
Device(config-cmap)# exit
Device(config)# class-map type inspect gtpv1 match-any gtp-cl7
Device(config-cmap)# match mcc 2 mnc 1
Device(config-cmap)# match mcc 1 mnc 1
Device(config-cmap)# exit
Device(config)# class-map type inspect gtpv1 match-all gtp-l4c
Device(config-cmap)# match protocol gtpv1
Device(config-cmap)# match access-group 101
Device(config-cmap)# exit
Device(config)# class-map type inspect gtpv1 match-all gtp-l4c-rev
Device(config-cmap)# match protocol gtpv1
Device(config-cmap)# match access-group 102
Device(config-cmap)# end
```

例：GGSN プーリングのポリシー マップの設定

```
Device# configure terminal
Device(config)# policy-map type inspect gtpv1 gtp-l7p-rev
Device(config-pmap)# class type inspect gtpv1 gtp-cl7-rev
Device(config-pmap-c)# log
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap)# exit
Device(config)# policy-map type inspect gtpv1 gtp-l7p
Device(config-pmap)# class type inspect gtpv1 gtp-cl7
Device(config-pmap-c)# log
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap)# exit
Device(config)# policy-map type inspect gtpv1 gtp-l4p-rev
Device(config-pmap)# class type inspect gtpv1 gtp-l4c-rev
Device(config-pmap-c)# inspect
Device(config-pmap-c)# service-policy gtp-l7p-rev
```

```
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap)# exit
Device(config)# policy-map type inspect gtpv1 gtp-l4p
Device(config-pmap)# class type inspect gtpv1 gtp-l4c
Device(config-pmap-c)# inspect
Device(config-pmap-c)# service-policy gtp-l7p
Device(config-pmap)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# end
```

例：GGSN プーリングのゾーンおよびゾーン ペアの設定

```
Device(config)# configure terminal
Device(config)# zone security roam-in
Device(config-sec-zone)# exit
Device(config-sec-zone)# zone security roam-out
Device(config-sec-zone)# exit
Device(config)# zone-pair security in2out source roam-in destination roam-out
Device(config-sec-zone-pair)# service-policy type inspect gtp-l4p
Device(config-sec-zone-pair)# exit
Device(config)# zone-pair security out2in source roam-out destination roam-in
Device(config-sec-zone-pair)# service-policy type inspect gtp-l4p-rev
Device(config)# end
```

ファイアウォールステートフルシャーシ間冗長性の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールの GGSN プーリング サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *25*：ファイアウォールの *GGSN* プーリング サポートの機能情報

機能名	リリース	機能情報
ファイアウォールの GGSN プーリング サポート	Cisco IOS XE Release 3.7S	ファイアウォールの GGSN プーリング サポート機能は、ロード バランシング サポートを追加することで、GPRS トンネリング プロトコル（GTP）機能を拡張します。 GTP は、単一の GGSN に指定された制御トラフィックのインスペクションをサポートします。GSM ネットワークに効率性と拡張性を提供するために、ロード バランシングがトポロジに追加されています。ロード バランサは、SGSN からプール内のさまざまな GGSN に要求を送信します。

第 20 章

Cisco Firewall-SIP の機能拡張 ALG

Cisco XE ファイアウォールの強化された Session Initiation Protocol（SIP）検査には、基本的な SIP 検査機能（SIP パケットインスペクションとピンホール開口部）に加え、プロトコル準拠機能とアプリケーションセキュリティ機能があります。 これらの拡張機能により、SIP トラフィックに適用するポリシーおよびセキュリティ チェックを制御し、不要なメッセージやユーザをフィルタリングすることができます。

Cisco IOS XE ソフトウェアで追加の SIP 機能を開発することで、Cisco Call Manager、Cisco Call Manager Express、および Cisco IP-IP Gateway ベースの音声/ビデオ システムのサポートが改善されます。 また、アプリケーション層ゲートウェイ（ALG）SIP の強化は、RFC 3261 とその拡張もサポートしています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

Cisco Firewall-SIP の機能拡張 ALG の前提条件

Cisco IOS XE Release 2.4 以降のリリースをシステムで実行している必要があります。

Cisco Firewall-SIP の機能拡張 ALG の制約事項

DNS 名前解決

SIP メソッドでは、IP アドレスを直接指定する代わりにドメイン ネーム システム（DNS）名を使用できますが、この機能は現在 DNS 名をサポートしていません。

Cisco ASR 1000 シリーズ ルータ

この機能は、Cisco ASR 1000 シリーズ ルータ上のアプリケーション インスペクションと制御（AIC）に対するサポートなしに実装されました。 Cisco IOS XE Release 2.4 は次のコマンドだけをサポートします。**class-map type inspect**、**class type inspect**、**match protocol**、および **policy-map type inspect**。

Cisco Firewall-SIP の機能拡張 ALG について

SIP の概要

Session Initiation Protocol（SIP）は、1 人または複数の参加者とのセッションを作成、変更、および終了するためのアプリケーション層コントロール（シグナリング）プロトコルです。 SIP セッションには、インターネット電話の通話、マルチメディアの配布、マルチメディア会議などがあります。 SIP は HTTP のような要求/応答トランザクション モデルに基づいています。 各トランザクションは、サーバで特定のメソッドまたは関数を呼び出す 1 つの要求と 1 つ以上の応答で構成されます。

セッションの作成に使用される SIP の招待は、互換性のあるメディア タイプのセットに参加者が同意できるセッション記述を伝送しています。 SIP は、プロキシ サーバと呼ばれる要素を利用して、ユーザの所在地への要求のルーティング、サービスのためのユーザ認証および認可、プロバイダーのコールルーティング ポリシーの実装、およびユーザへの機能提供を行っています。 また、SIP には、プロキシ サーバから使用できるように、ユーザの所在地をアップロードできる登録機能があります。 SIP は複数のトランスポート プロトコルを基礎として実行されます。

SIP 用ファイアウォールの機能の説明

SIP 用ファイアウォールのサポート機能を使用すると、SIP シグナリング要求は、ゲートウェイ間の直接伝送によって、または複数のプロキシを介して、宛先ゲートウェイまたは電話に送信できます。 最初の要求後に、Record-Route ヘッダー フィールドを使用しない場合、後続の要求は、Contact ヘッダー フィールドに指定されている宛先ゲートウェイ アドレスに直接伝送できます。そのため、ファイアウォールは、周囲のすべてのプロキシとゲートウェイを認識し、次の機能を使用できます。

- SIP シグナリング応答は、SIP シグナリング要求と同じパスを伝送できます。
- 後続のシグナリング要求は、エンドポイント（宛先ゲートウェイ）に直接伝送できます。
- メディア エンドポイントは、相互にデータを交換できます。

SIP UDP および TCP のサポート

RFC 3261 は最新の SIP の RFC であり、RFC 2543 の置き換えです。 この機能は、シグナリングに SIP UDP と TCP 形式をサポートします。

SIP インスペクション

ここでは、Cisco Firewall--SIP ALG 拡張機能でサポートされる展開シナリオについて説明します。

SIP 電話と CCM 間の Cisco IOS XE ファイアウォール

Cisco IOS XE ファイアウォールは、Cisco Call Manager または Cisco Call Manager Express と SIP 電話との間にあります。 SIP 電話は、ファイアウォールを介して Cisco Call Manager または Cisco Call Manager Express に登録され、SIP 電話との間の SIP コールはファイアウォールを通過します。

SIP ゲートウェイ間の Cisco IOS XE ファイアウォール

Cisco IOS XE ファイアウォールは、2 つの SIP ゲートウェイ（Cisco Call Manager、Cisco Call Manager Express、または SIP プロキシ）間にあります。 電話は SIP ゲートウェイに直接登録されます。ファイアウォールから SIP セッションまたはトラフィックを認識するのは、異なる SIP ゲートウェイに登録された電話間で SIP コールが存在する場合のみです。 シナリオによっては、IP-IP ゲートウェイをファイアウォールと同じデバイスに設定することもできます。 このシナリオでは、SIP ゲートウェイ間のすべてのコールは IP-IP ゲートウェイで終端します。

Cisco IOS XE ファイアウォールおよびローカル Cisco Call Manager Express とリモート Cisco Call Manager Express/Cisco Call Manager

Cisco IOS XE ファイアウォールは、2 つの SIP ゲートウェイ（Cisco Call Manager、Cisco Call Manager Express、または SIP プロキシ）間にあります。 ゲートウェイの 1 つは、ファイアウォールと同じデバイスで設定されます。 このゲートウェイに登録されているすべての電話は、ファイアウォールによってローカルで検査されます。 また、2 つのゲートウェイ間に SIP コールがある場合、ファ

イアウォールによってその SIP セッションも検査されます。 このシナリオでは、ファイアウォールの一方では SIP 電話がローカルで検査され、もう一方では SIP ゲートウェイが検査されます。

Cisco IOS XE ファイアウォールとローカル Cisco Call Manager Express

Cisco IOS XE ファイアウォールと Cisco Call Manager Express は、同じデバイスで設定されます。 Cisco Call Manager Express に登録されているすべての電話は、ファイアウォールによってローカルで検査されます。 また、登録されている任意の電話間で行われる SIP コールも、Cisco IOS XE ファイアウォールによって検査されます。

ALG--SIP Over TCP の機能拡張

SIP が UDP を介して転送されると、すべての SIP メッセージが単一の UDP データグラムで伝送されます。 ただし、SIP が TCP を介して転送されると、1 つの TCP セグメントには複数の SIP メッセージが含まれることがあります。 また、いずれかの TCP セグメント内の最後の SIP メッセージが部分的メッセージである可能性があります。 Cisco IOS XE Release 3.5S 以前では、受信された 1 つの TCP セグメント内に複数の SIP メッセージがある場合、SIP ALG は最初のメッセージだけを解析します。 解析されないデータは、1 つの不完全な SIP メッセージと見なされ、vTCP に戻されます。 次の TCP セグメントを受信すると、vTCP は未処理データをそのセグメントの前に置き、それらを SIP ALG に渡すため、vTCP でバッファする必要があるデータが増えていきます。

Cisco IOS XE Release 3.5S では、ALG--SIP over TCP の拡張機能により、SIP ALG は 1 つの TCP セグメント内の複数の SIP メッセージを処理できます。 TCP セグメントを受信すると、このセグメント内のすべての完全な SIP メッセージは、1 つずつ解析されます。 最終的に不完全なメッセージがある場合、その部分だけが vTCP に戻されます。

Cisco Firewall-SIP の機能拡張 ALG の設定方法

SIP インスペクションのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any sip-class1`	検査タイプ クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol sip`	指定されたプロトコルに基づいてクラス マップの一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了します。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect sip-policy`	検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect sip-class1`	アクションを実行するクラスを指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーションモードに戻ります。
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	これらのポリシー マップ設定が事前に定義したデフォルト クラスに適用されることを指定します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 11	**end** 例： `Device(config-pmap)# end`	ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

SIP 対応のファイアウォール設定の問題を解決するには、次のコマンドを使用できます。

- **clear zone-pair**
- **debug cce**

- **debug policy-map type inspect**
- **show policy-map type inspect zone-pair**
- **show zone-pair security**

ゾーン ペアの設定および SIP ポリシー マップの付加

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *zone-name*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name*	**default**} 例： `Device(config)# zone security zone1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security zone2`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]] 例： `Device(config)# zone-pair security in-out source zone1 destination zone2`	ゾーン ペアを作成し、セキュリティ ゾーン ペア コンフィギュレーション モードに戻ります。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect sip-policy`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。

	コマンドまたはアクション	目的
		（注） インターフェイスをセキュリティゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone2`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。
ステップ 15	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Cisco Firewall-SIP 機能拡張 ALG の設定例

例：SIP インスペクションのイネーブル化

```
class-map type inspect match-any sip-class1
 match protocol sip
!
policy-map type inspect sip-policy
 class type inspect sip-class1
  inspect
!
class class-default
```

例：ゾーン ペアの設定および SIP ポリシー マップの付加

```
zone security zone1
!
zone security zone2
!
zone-pair security in-out source zone1 destination zone2
 service-policy type inspect sip-policy
!
interface gigabitethernet 0/0/0
 zone security zone1
!
interface gigabitethernet 0/1/1
 zone security zone2
```

Cisco Firewall-SIP の機能拡張 ALG の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
追加の SIP 情報	『Guide to Cisco Systems VoIP Infrastructure Solution for SIP』
vTCP のサポート	『*vTCP for ALG Support*』

標準および RFC

標準/RFC	タイトル
RFC 3261	『SIP: Session Initiation Protocol』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco Firewall-SIP の機能拡張 ALG の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *26*：*Cisco Firewall-SIP* の機能拡張：*ALG* の機能情報

機能名	リリース	機能情報
ALG--SIP Over TCP の機能拡張	Cisco IOS XE Release 3.5S	ALG--SIP Over TCP の拡張機能を使用すると、SIP ALG は 1 つの TCP セグメント内の複数の SIP メッセージを処理できます。 TCP セグメントを受信すると、このセグメント内のすべての完全な SIP メッセージは、1 つずつ解析されます。 最終的に不完全なメッセージがある場合、その部分だけが vTCP に戻されます。

機能名	リリース	機能情報
Cisco Firewall--SIP ALG 機能拡張	Cisco IOS XE Release 2.4	Cisco Firewall--SIP ALG 拡張機能により、Cisco ASR 1000 シリーズ ルータ上の Cisco IOS XE ソフトウェアに設定されたファイアウォール機能内で音声セキュリティを強化できます。 次のコマンドは、Cisco ASR 1000 シリーズ ルータ上のレイヤ 7（アプリケーション固有）構文に対するサポートなしに実装されました。**class type inspect**、**class-map type inspect**、**match protocol**、**policy-map type inspect**。
T.38 Fax Relay のための Firewall--SIP ALG 機能拡張	Cisco IOS XE Release 2.4.1	T.38 Fax Relay のための Firewall--SIP ALG 拡張機能は、Cisco ASR 1000 シリーズ ルータ上の Cisco IOS XE ソフトウェアに設定されたファイアウォール機能を拡張します。 この機能により、SIP ALG は T.38 Fax Relay over IP をサポートできるため、Cisco ASR 1000 シリーズ ルータ上のファイアウォールを通過できます。

第 21 章

ファイアウォールおよびNAT対応のMSRPC ALGサポート

ファイアウォールおよびNAT対応のMSRPC ALGサポート機能は、ファイアウォールおよびネットワーク アドレス変換（NAT）でのMicrosoft（MS）リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）をサポートします。 MSRPC ALGはMSRPCプロトコルのディープ パケット インスペクション（DPI）を提供します。 MSRPC ALGがプロビジョニング システムと連携して機能することにより、ネットワーク管理者は、MSRPCパケットで検索できる一致基準を定義するように一致フィルタを設定できます。

ファイアウォールおよびNAT対応のMSRPC ALGサポートの前提条件

- MSRPC ALGをパケットに適用する前に、Cisco IOS XEファイアウォールとNATをイネーブルにする必要があります。

ファイアウォールおよび NAT 対応の MSRPC AIC サポートの制約事項

- TCP-based MSRPC のみがサポートされます。
- **allow** コマンドと **reset** コマンドを一緒に設定することはできません。
- DPI に **match protocol msrpc** コマンドを設定する必要があります。

ファイアウォールおよび NAT 対応の MSRPC ALG サポートについて

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。 ALG は、アプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワークアドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバアプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、それらに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールはピンホールを開き、NATは、アプリケーション層データ ストリームの送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを実行します。 IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションにはALGのサポートが必要です。

MSRPC

MSRPCは、開発者が、サーバおよび企業向けの一連のアプリケーションとサービスを公開するために使用するフレームワークです。 RPCはプロセス間通信技術であり、これにより、クライアントおよびサーバ ソフトウェアはネットワークを越えて通信できます。 MSRPCは、多様なMicrosoft

アプリケーションで使用されるアプリケーション層プロトコルです。 MSRPC は、さまざまなトランスポート プロトコルを介したコネクション型（CO）およびコネクションレス型（CL）の両方の分散コンピューティング環境（DCE）RPC モードをサポートします。 MSRPC のすべてのサービスは、プライマリ接続と呼ばれる最初のセッションを確立します。 宛先ポートとしての 1024 ～ 65535 のポート範囲上のセカンダリ セッションは、MSRPC の一部のサービスによって確立されます。

ファイアウォールおよび NAT がイネーブルな場合に MSRPC が機能するには、MSRPC パケットの検査に加えて、ALG は、ダイナミック ファイアウォール セッションの確立、NAT 後のパケット コンテンツの修正など、MSRPC 固有の問題を処理する必要もあります。

MSRPC プロトコル インスペクションを適用すると、ほとんどの MSRPC サービスがサポートされ、レイヤ 7 ポリシー フィルタの必要がなくなります。

ファイアウォールでの MSRPC ALG

MSRPC プロトコルを検査するようにファイアウォールを設定すると、MSRPC ALG は MSRPC メッセージの解析を開始します。 次の表に、ファイアウォールおよび NAT での MSRPC ALG サポート機能でサポートされるプロトコル データ ユニット（PDU）のタイプを示します。

表 *27*：サポートされる *PDU* タイプ

PDU	番号	タイプ	説明
REQUEST	0	コール	コール要求を開始します。
RESPONSE	2	コール	コール要求に応答します。
FAULT	3	コール	RPC ランタイム、RPC スタブ、または RPC 固有の例外を示します。
BIND	11	アソシエーション	本文データのプレゼンテーション ネゴシエーションを開始します。
BIND_ACK	12	アソシエーション	バインド要求を受け入れます。
BIND_NAK	13	アソシエーション	アソシエーション要求を拒否します。
ALTER_CONTEXT	14	アソシエーション	別のインターフェイスやバージョンの追加のプレゼンテーション ネゴシエーションを要求するか、新しいセキュリティ コンテキストをネゴシエーションするよう要求するか、または両方を要求します。

PDU	番号	タイプ	説明
ALTER_CONTEXT_RESP	15	アソシエーション	ALTER_CONTEXT PDU に応答します。 有効な値は、許可または拒否です。
SHUTDOWN	17	コール	接続を終了するようクライアントに要求し、関連するリソースを解放します。
CO_CANCEL	18	コール	接続をキャンセルするか、孤立させます。 このメッセージは、クライアントがキャンセル エラーに遭遇した場合に送信されます。
ORPHANED	19	コール	進行中で、まだ完全に送信されていない要求を中止するか、または進行中の（時間がかかっていると思われる）応答を中止します。

NAT での MSRPC ALG

NAT は、MSRPC パケットを受信すると、パケット ペイロードを解析し、埋め込み IP アドレスを変換するトークンを形成する MSRPC ALG を呼び出します。 このトークンは NAT に渡され、NAT は NAT 設定に従ってアドレスまたはポートを変換します。 次に、変換されたアドレスは、MSRPC ALG によってパケット ペイロードに再び書き込まれます。

ファイアウォールと NAT の両方を設定している場合、NAT は、ALG を最初にコールします。

MSRPC ステートフル パーサー

MSRPC ステート マシンまたはパーサーは、MSRPC ALG の頭脳です。 MSRPC ステートフル パーサーは、ファイアウォールと NAT のいずれの機能が最初にパーサーを起動したかに応じて、ファイアウォールまたは NAT 内のすべてのステートフル情報を保持します。 パーサーは、MSRPC プロトコル パケットの DPI を提供します。 プロトコル準拠を確認し、シーケンス外のコマンドや不正な形式のパケットを検出します。パケットの解析時、ステートマシンはさまざまなデータを記録し、NAT およびファイアウォール インスペクションのために正しいトークン情報を入力します。

ファイアウォールおよび NAT 対応の MSRPC ALG サポートの設定方法

（注） デフォルトでは、NAT をイネーブルにすると、MSRPC ALG は自動的にイネーブルになります。 NAT のみの設定では MSRPC ALG を明示的にイネーブルにする必要はありません。 NAT において MSRPC ALG をディセーブルにするには、**no ip nat service msrpc** コマンドを使用します。

レイヤ 4 MSRPC クラス マップおよびポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Router(config)# class-map type inspect match-any msrpc-cmap`	トラフィック クラスの検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Router(config-cmap)# match protocol msrpc`	指定されたプロトコルを基づくクラス マップの一致基準を設定します。 • 検査タイプ クラス マップでは Cisco IOS XE ステートフル パケット インスペクションがサポートするプロトコルだけを一致基準として使用できます。
ステップ 5	**exit** 例： `Router(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect msrpc-pmap`	レイヤ 3 またはレイヤ 4 の検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Router(config-pmap)# class type inspect msrpc-class-map`	アクションを実行する対象のトラフィック（クラス）を指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Router(config-pmap-c)# inspect`	Cisco IOS XE ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**end** 例： `Router(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーン ペアの設定および MSRPC ポリシー マップの付加

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *security-zone-name*
4. **exit**
5. **zone security** *security-zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** [*destination-zone*]]
8. **service-policy type inspect** *policy-map-name*
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Rotuer# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** *security-zone-name* 例： `Router(config)# zone security in-zone`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 5	**zone security** *security-zone-name* 例： `Router(config)# zone security out-zone`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Router(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** [*destination-zone*]] 例： `Router(config)# zone-pair security in-out source in-zone destination out-zone`	ゾーン ペアを作成し、セキュリティ ゾーン ペア コンフィギュレーション モードを開始します。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect msrpc-pmap`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**end** 例： `Router(config-sec-zone-pair)# end`	セキュリティ ゾーン ペア コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォールおよび NAT 対応の MSRPC ALG サポートの設定例

例：レイヤ 4 MSRPC クラス マップおよびポリシー マップの設定

```
Router# configure terminal
Router(config)# class-map type inspect match-any msrpc-cmap
Router(config-cmap)# match protocol msrpc
Router(config-cmap)# exit
Router(config)# policy-map type inspect msrpc-pmap
Router(config-pmap)# class type inspect msrpc-cmap
Router(config-pmap-c)# inspect
Router(config-pmap-c)# end
```

例：ゾーン ペアの設定および MSRPC ポリシー マップの付加

```
Router# configure terminal
Router(config)# zone security in-zone
Router(config-sec-zone)# exit
Router(config)# zone security out-zone
Router(config-sec-zone)# exit
Router(config)# zone-pair security in-out source in-zone destination out-zone
Router(config-sec-zone-pair)# service-policy type inspect msrpc-pmap
Router(config-sec-zone-pair)# end
```

ファイアウォールおよび NAT 対応の MSRPC ALG サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
NAT ALG	「Using Application Level Gateways with NAT」モジュール
ALG サポート	『*NAT and Firewall ALG Support on Cisco ASR 1000 Series Routers*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールおよび NAT 対応の MSRPC ALG サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *28*：ファイアウォールおよび *NAT* 対応の *MSRPC ALG* サポートの機能情報

機能名	リリース	機能情報
ファイアウォールおよび NAT 対応の MSRPC ALG サポート	Cisco IOS XE Release 3.5S	ファイアウォールおよび NAT 対応の MSRPC ALG サポート機能は、ファイアウォールおよび NAT における MSRPC ALG のサポートを提供します。MSRPC ALG は MSRPC プロトコルのディープ パケット インスペクションを提供します。MSRPC ALG がプロビジョニング システムと連携して機能することにより、ネットワーク管理者は、MSRPC パケットで検索できる一致基準を定義する一致フィルタを設定できます。 次のコマンドが導入または変更されました。**ip nat service msrpc**、**match protocol msrpc**。

第 22 章

ファイアウォールおよびNAT対応のSun RPC ALG サポート

ファイアウォールおよびNAT 対応の Sun RPC ALG サポート機能により、ファイアウォールおよびネットワーク アドレス変換（NAT）における Sun Microsystems リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）のサポートが追加されます。 Sun RPC は、リモート サーバ プログラム内の関数をクライアント プログラムが呼び出すことができるようにするアプリケーション層プロトコルです。 このモジュールでは、Sun RPC ALG を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの制約事項

- ご使用のリリースによって、次の設定は、Cisco ASR 1000 アグリゲーション サービス ルータでは動作しません。 レイヤ 4 またはレイヤ 7 のクラス マップに検査アクションを設定した場合、ポート マッパー プロトコルの well-known ポート（111）に一致したパケットは、レイヤ 7 インスペクションなしでファイアウォールを通過します。 レイヤ 7 インスペクションなしの場合、ファイアウォール ピンホールはトラフィック フローに対して開かれず、Sun リモート プロシージャ コール（RPC）はファイアウォールによってブロックされます。 回避策として、Sun RPC プログラム番号に **match program-number** コマンドを設定します。
- ポート マッパー プロトコル バージョン 2 のみがサポートされます。他のバージョンはいずれもサポートされません。
- RPC バージョン 2 のみがサポートされます。

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートについて

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内の IP アドレス情報を変換するアプリケーションです。 ALG は、アプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワークアドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、それらに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールはピンホールを開き、NAT は、アプリケーション層データ ストリームの送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを実行します。 IP アドレス情報を埋め込む特定のプロトコルまたはアプリケーションには ALG のサポートが必要です。

Sun RPC

Sun リモート プロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）は、Sun RPC プロトコルのディープ パケット インスペクションを実行します。 Sun RPC ALG がプロビジョニング システムと連携して機能することにより、ネットワーク管理者は一致フィルタを設定できます。 各一致フィルタでは、Sun RPC パケットで検索される一致基準を定義し、これにより、基準に一致するパケットだけを許可します。

RPC では、クライアント プログラムは、サーバ プログラム内のプロシージャを呼び出します。RPC ライブラリは、プロシージャ引数をネットワーク メッセージ内にパッケージ化し、そのメッセージをサーバに送信します。 次にサーバは、RPC ライブラリを使用して、ネットワーク メッセージからプロシージャ引数を取り出し、指定されたサーバプロシージャを呼び出します。サーバ プロシージャが RPC に戻ると、戻り値はネットワーク メッセージ内にパッケージ化され、クライアントに送り返されます。

Sun RPC プロトコルの詳細については、RFC 1057、『*RPC: Remote Procedure Call Protocol Specification Version 2*』を参照してください。

ファイアウォールでの Sun RPC ALG サポート

ポリシーとクラス マップを使用して作成されたゾーンベース ファイアウォールを使用して、Sun RPC ALG を設定できます。 レイヤ 7 クラス マップにより、ネットワーク管理者は一致フィルタを設定できます。 このフィルタでは、Sun RPC パケット内で検索するプログラム番号を指定します。 Sun RPC レイヤ 7 ポリシー マップは、**service-policy** コマンドを使用するレイヤ 4 ポリシー マップの子ポリシーとして設定されます。

レイヤ 7 ファイアウォール ポリシーを設定しないで Sun RPC レイヤ 4 クラス マップを設定すると、Sun RPC によって返されたトラフィックは、ファイアウォールを通過しますが、セッションはレイヤ 7. で検査されません。 セッションが検査されないため、後続の RPC コールはファイアウォールによってブロックされます。 Sun RPC レイヤ 4 クラス マップおよびレイヤ 7 ポリシーを設定すると、レイヤ 7 インスペクションが使用できるようになります。 空のレイヤ 7 ファイアウォール ポリシー、つまり一致フィルタがないポリシーを設定できます。

NAT での Sun RPC ALG サポート

デフォルトで、ネットワーク アドレス変換（NAT）がイネーブルな場合、Sun RPC ALG は自動的にイネーブルになります。 NAT での Sun RPC ALG をディセーブルにするには、**no ip nat service alg** コマンドを使用します。

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの設定方法

ファイアウォールおよびNATがイネーブルの場合にSun RPCを動作させるには、ALGでSun RPCパケットを検査する必要があります。 ALG では、ダイナミック ファイアウォール セッションの

確立、NAT 変換後のパケット コンテンツの修正など、Sun RPC 固有の問題を処理する必要もあります。

Sun RPC ALG 対応のファイアウォールの設定

Sun RPC プロトコルの検査アクションを設定している場合（つまり、レイヤ 4 クラス マップで **match protocol sunrpc** コマンドを指定している場合）は、レイヤ 7 Sun リモート プロシージャ コール（RPC）ポリシー マップを設定する必要があります。

同じインターフェイス上にセキュリティ ゾーンと検査ルールの両方を設定しないことを推奨します。これは、この設定が機能しない場合があるためです。

Sun RPC ALG 対応のファイアウォールを設定するには、次の作業を実行します。

ファイアウォール ポリシーのレイヤ 4 クラス マップの設定

ネットワーク トラフィックを分類するためのレイヤ 4 クラス マップを設定するには、この作業を実行します。 **class-map type inspect** コマンドで **match-all** キーワードを指定した場合、Sun RPC トラフィックは、クラス マップ内の（プログラム番号として指定した）すべての Sun リモート プロシージャ コール（RPC）レイヤ 7 フィルタに一致します。 **class-map type inspect** で **match-any** キーワードを指定した場合、Sun RPC トラフィックは、クラス マップ内の（プログラム番号として指定した）少なくとも 1 つの Sun RPC レイヤ 7 フィルタに一致する必要があります。

レイヤ 4 クラス マップを設定するには、**class-map type inspect {match-any | match-all}** *classm-map-name* コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
4. **match protocol** *protocol-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* 例： `Device(config)# class-map type inspect match-any sunrpc-l4-cmap`	レイヤ 4 検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol sunrpc`	指定されたプロトコルに基づくクラスマップの一致基準を設定します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォール ポリシーのレイヤ 7 クラス マップの設定

ネットワーク トラフィックを分類するためのレイヤ 7 クラス マップを設定するには、この作業を実行します。 この設定により、Sun RPC を使用する mount（100005）、ネットワーク ファイル システム（NFS）（100003）などのプログラムが使用できるようになります。 100005 および 100003 は Sun RPC プログラムの番号です。 デフォルトでは、Sun RPC ALG はすべてのプログラムをブロックします。

Sun RPC プログラムおよびプログラム番号の詳細については、RFC 1057、『*RPC: Remote Procedure Call Protocol Specification Version 2*』を参照してください。

class-map type inspect *protocol-name* コマンドを使用して、レイヤ 7 クラス マップを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name*
4. **match program-number** *program-number*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect** *protocol-name* {**match-any** | **match-all**} *class-map-name* 例： `Device(config)# class-map type inspect sunrpc match-any sunrpc-l7-cmap`	レイヤ7（アプリケーション固有）検査タイプクラスマップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match program-number** *program-number* 例： `Device(config-cmap)# match program-number 100005`	許可する RPC プロトコル プログラム番号を一致基準として指定します。
ステップ 5	**end** 例： `Device(config-cmap)# end`	QoS クラスマップ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

Sun RPC ファイアウォール ポリシー マップの設定

Sun リモート プロシージャ コール（RPC）ファイアウォール ポリシー マップを設定するには、この作業を実行します。 ポリシー マップを使用して、レイヤ 7 ファイアウォール ポリシーのクラス マップで定義する Sun RPC レイヤ 7 クラスごとにパケット転送を許可します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *protocol-name policy-map-name*
4. **class type inspect** *protocol-name class-map-name*
5. **allow**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *protocol-name policy-map-name* 例： `Device(config)# policy-map type inspect sunrpc sunrpc-l7-pmap`	レイヤ 7（プロトコル固有）検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class type inspect** *protocol-name class-map-name* 例： `Device(config-pmap)# class type inspect sunrpc sunrpc-l7-cmap`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**allow** 例： `Device(config-pmap-c)# allow`	パケット転送を許可します。
ステップ 6	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

レイヤ 4 ポリシー マップへのレイヤ 7 ポリシー マップの付加

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class** {*class-map-name* | **class-default**}
5. **inspect** [*parameter-map-name*]
6. **service-policy** *protocol-name policy-map-name*
7. **exit**
8. **class class-default**
9. **drop**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect sunrpc-l4-pmap`	レイヤ 4 検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 4	**class** {*class-map-name*	**class-default**} 例： `Device(config-pmap)# class sunrpc-l4-cmap`	アクションを実行する対象のクラスを関連付け、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 5	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	**service-policy** *protocol-name policy-map-name* 例： `Device(config-pmap-c)# service-policy sunrpc sunrpc-l7-pmap`	レイヤ 7 ポリシー マップをトップレベル レイヤ 4 ポリシー マップに付加します。
ステップ 7	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードに戻ります。
ステップ 8	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシーを設定する前にデフォルト クラス（一般的にクラスデフォルト クラスと呼ばれます）を指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**drop** 例： `Device(config-pmap-c)# drop`	特定のクラスに属するパケットを廃棄するトラフィック クラスを設定します。
ステップ 10	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

セキュリティ ゾーンとゾーン ペアの作成、およびゾーン ペアへのポリシー マップの付加

ゾーン ペアを作成するには、2 つのセキュリティ ゾーンが必要です。 ただし、1 つのセキュリティ ゾーンのみ作成でき、もう 1 つのセキュリティ ゾーンはシステム定義のセキュリティ ゾーンにすることができます。 システム定義のセキュリティ ゾーンまたはセルフ ゾーンを作成するには、**self** キーワードを指定した **zone-pair security** コマンドを設定します。

（注） セルフ ゾーンを選択する場合、検査アクションは設定できません。

この作業では、次のことを実行します。

- セキュリティ ゾーンを作成します。
- ゾーン ペアを定義します。

- セキュリティ ゾーンにインターフェイスを割り当てます。
- ポリシー マップをゾーン ペアに付加します。

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}
6. **exit**
7. **zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name*
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
12. **zone-member security** *zone-name*
13. **exit**
14. **interface** *type number*
15. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
16. **zone-member security** *zone-name*
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name*	**default**} 例： `Device(config)# zone security z-client`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定には、ゾーン ペアを作成するために2つのセキュリティ ゾーン、送信元ゾーンと宛先ゾーンが含まれている必要があります。

	コマンドまたはアクション	目的
		• ゾーン ペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンまたはセルフ ゾーンを使用できます。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security z-server`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定には、ゾーン ペアを作成するために2つのセキュリティ ゾーン、送信元ゾーンと宛先ゾーンが含まれている必要があります。 • ゾーン ペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair-name* **source** *source-zone-name* **destination** *destination-zone-name* 例： `Device(config)# zone-pair security clt2srv source z-client destination z-server`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードを開始します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect sunrpc-l4-pmap`	ファイアウォール ポリシー マップをゾーン ペアに付加します。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/0/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] 例： `Device(config-if)# ip address 192.168.6.5 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 12	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z-client`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 13	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/1/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 15	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] 例： `Device(config-if)# ip address 192.168.6.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 16	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z-server`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 17	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの設定例

例：ファイアウォール ポリシーのレイヤ 4 クラス マップの設定

```
Device# configure terminal
Device(config)# class-map type inspect match-any sunrpc-l4-cmap
Device(config-cmap)# match protocol sunrpc
Device(config-cmap)# end
```

例：ファイアウォール ポリシーのレイヤ 7 クラス マップの設定

```
Device# configure terminal
Device(config)# class-map type inspect sunrpc match-any sunrpc-l7-cmap
Device(config-cmap)# match program-number 100005
Device(config-cmap)# end
```

例：Sun RPC ファイアウォール ポリシー マップの設定

```
Device# configure terminal
Device(config)# policy-map type inspect sunrpc sunrpc-l7-pmap
Device(config-pmap)# class type inspect sunrpc sunrpc-l7-cmap
Device(config-pmap-c)# allow
Device(config-pmap-c)# end
```

例：レイヤ 4 ポリシー マップへのレイヤ 7 ポリシー マップの付加

```
Device# configure terminal
Device(config)# policy-map type inspect sunrpcl4-pmap
Device(config-pmap)# class sunrpcl4-cmap
Device(config-pmap-c)# inspect
Device(config-pmap-c)# service-policy sunrpc sunrpc-l7-pmap
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
Device(config-pmap-c)# end
```

例：セキュリティ ゾーンとゾーン ペアの作成、およびゾーン ペアへのポリシー マップの付加

```
Device# configure terminal
Device(config)# zone security z-client
Device(config-sec-zone)# exit
Device(config)# zone security z-server
Device(config-sec-zone)# exit
Device(config)# zone-pair security clt2srv source z-client destination z-server
Device(config-sec-zone-pair)# service-policy type inspect sunrpc-l4-pmap
```

```
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 2/0/0
Device(config-if)# ip address 192.168.6.5 255.255.255.0
Device(config-if)# zone-member security z-client
Device(config-if)# exit
Device(config)# interface gigabitethernet 2/1/1
Device(config-if)# ip address 192.168.6.1 255.255.255.0
Device(config-if)# zone-member security z-server
Device(config-if)# end
```

例：Sun RPC ALG 対応のファイアウォールの設定

次に、Sun リモートプロシージャ コール（RPC）アプリケーション レベル ゲートウェイ（ALG）サポート対応のファイアウォールの設定例を示します。

```
class-map type inspect sunrpc match-any sunrpc-l7-cmap
 match program-number 100005
!
class-map type inspect match-any sunrpc-l4-cmap
 match protocol sunrpc
!
!
policy-map type inspect sunrpc sunrpc-l7-pmap
 class type inspect sunrpc sunrpc-l7-cmap
  allow
!
!
policy-map type inspect sunrpc-l4-pmap
 class type inspect sunrpc-l4-cmap
  inspect
  service-policy sunrpc sunrpc-l7-pmap
!
 class class-default
  drop
!
!
zone security z-client
!
zone security z-server
!
zone-pair security clt2srv source z-client destination z-server
 service-policy type inspect sunrpc-l4-pmap
!
interface GigabitEthernet 2/0/0
 ip address 192.168.10.1 255.255.255.0
 zone-member security z-client
!
interface GigabitEthernet 2/1/1
 ip address 192.168.23.1 255.255.255.0
 zone-member security z-server
!
```

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
IP アドレッシング コマンド	『IP Addressing Services Command Reference』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 1057	『*RPC: Remote Procedure Call Protocol Specification Version 2*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールおよび NAT 対応の Sun RPC ALG サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *29*：ファイアウォールおよび *NAT* 対応の *Sun RPC ALG* サポートの機能情報

機能名	リリース	機能情報
ファイアウォールおよび NAT 対応の Sun RPC ALG サポート	Cisco IOS XE Release 3.2S	ファイアウォールおよび NAT 対応の Sun RPC ALG サポート機能は、ファイアウォールおよび NAT における Sun RPC ALG のサポートを追加します。 次のコマンドが導入または変更されました。**match protocol**。

第 23 章

ファイアウォールおよびNAT対応のハイ アベイラビリティサポート付きALG-H.323vTCP

ファイアウォールおよびNAT対応のハイ アベイラビリティ サポート付きALG-H.323 vTCPの機能により、H.323アプリケーション レベル ゲートウェイ（ALG）が拡張され、単一H.323メッセージではないTCPセグメントがサポートされます。 仮想TCP（vTCP）は、TCPセグメント再構成をサポートします。 この機能の導入前、H.323 ALGは、TCPセグメントが完全なH.323メッセージである場合にだけTCPセグメントを処理していました。 TCPセグメントが複数のメッセージである場合、H.323 ALGはその TCP セグメントを無視し、パケットは処理せずに渡されていました。

このモジュールでは、ファイアウォール対応のハイ アベイラビリティ（HA）サポート付きALG-H.323 vTCP を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポート付き ALG-H.323 vTCP の制約事項

- 着信 TCP セグメントが完全な H.323 メッセージでない場合、H.323 ALG は、残りのメッセージを待機している間、TCP セグメントをバッファします。 バッファされたデータは、ハイアベイラビリティ（HA）用のスタンバイ デバイスに同期されません。
- vTCP がデータのバッファを開始すると、H.323 ALG のパフォーマンスが影響を受ける場合があります。

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポート付き ALG—H.323 vTCP について

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内の IP アドレス情報を変換するアプリケーションです。 ALG は、アプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワークアドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、それらに対するきめ細かいセキュリティ制御を提供します。

- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールはピンホールを開き、NATは、アプリケーション層データ ストリームの送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを実行します。IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションにはALGのサポートが必要です。

基本的な H.323 ALG サポート

H.323 は、パケットベース ネットワーク経由のマルチメディア伝送用の一連のネットワーク要素やプロトコルを定義した、ITU-T により公開された推奨技術です。 H.323 は、マルチメディア伝送で使用されるネットワーク要素の数を定義します。

今日のほとんどの H.323 実装がシグナリング用の転送メカニズムとして TCP を利用しますが、H.323 バージョン 2 では基本的な UDP トランスポートがイネーブルになります。

- H.323 端末：この要素は、別の H.323 端末またはゲートウェイとの双方向通信を提供する、ネットワークのエンドポイントです。
- H.323 ゲートウェイ：この要素は、H.323 端末と、H.323 をサポートしない他の端末との間のプロトコル変換を提供します。
- H.323 ゲートキーパー：この要素は、アドレス変換、ネットワーク アクセス コントロール、帯域幅管理とアカウントなどのサービスを H.323 端末およびゲートウェイに提供します。

次のコア プロトコルが、H.323 仕様で規定されています。

- H.225：このプロトコルは、通信を確立するために任意の2つのH.323エンティティ間で使用されるコール シグナリング方式を説明します。
- H.225 登録、アドミッション、およびステータス（RAS）：このプロトコルは、アドレス解決およびアドミッション制御サービスのために H.323 エンドポイントとゲートウェイによって使用されます。
- H.245：このプロトコルは、マルチメディア通信機能の交換のため、および音声、ビデオ、およびデータに論理チャネルを開いたり閉じたりするために使用されます。

一覧したプロトコルに加えて、H.323仕様では、リアルタイム転送（RTP）プロトコルとオーディオ（G.711、G.729 など）およびビデオ（H.261、H.263、および H.264）コーデックなどのさまざまな IETF プロトコルの使用を説明しています。

NAT では、パケット ペイロード内の埋め込み IP アドレスやポート番号の変換、制御チャネルからの新しい接続/セッション情報の抽出などのレイヤ 7 プロトコル固有サービスを処理するために、さまざまな ALG が必要となります。 H.323 ALG は、これらの H.323 メッセージ固有のサービスを実行します。

vTCP for ALG のサポートの概要

レイヤ 7 プロトコルが TCP を転送に使用する場合、TCP ペイロードは、アプリケーション設計、最大セグメントサイズ（MSS）、TCP ウィンドウサイズなどのさまざまな理由でセグメント化される場合があります。 ファイアウォールおよび NAT がサポートする ALG には、パケット インスペクションで TCP フラグメントを認識する機能がありません。 vTCP は、ALG が TCP セグメントを認識し、TCP ペイロードを解析するために使用する汎用フレームワークです。

vTCP は、NAT や Session Initiation Protocol（SIP）など、埋め込みデータを書き直すために TCP ペイロード全体を必要とするアプリケーションに役立ちます。 ファイアウォールは vTCP を使用して、ALG がパケット間のデータ分割をサポートするのを支援します。

ファイアウォールおよび NAT ALG を設定すると、vTCP 機能がアクティブ化されます。

TCP 確認応答と確実な送信

vTCP は 2 つの TCP ホストに存在するため、TCP セグメントを他のホストに送信するまで一時的に保存するためのバッファ スペースが必要です。 vTCP により、データ伝送がホスト間で適切に行われます。 vTCP は、多くのデータをデータ伝送する必要がある場合、TCP 確認応答（ACK）を送信します。 vTCP は、受信ホストから送信される ACK を TCP フローの始めから追跡し、確認応答されたデータを注意深くモニタします。

vTCP は、TCP セグメントを再構成します。 着信セグメントの IP ヘッダーおよび TCP ヘッダー情報は、確実な送信のために vTCP バッファに保存されます。

vTCP は、NAT 対応アプリケーションの発信セグメントの長さに軽微な変更を行うことができます。 vTCP は最後のセグメントのデータ長を長くするか、新しいセグメントを作成して、追加のデータを伝送することができます。 新しく作成されたセグメントの IP ヘッダーまたは TCP ヘッダーは、オリジナルの着信セグメントから派生したものです。 IP ヘッダーの合計の長さと TCP ヘッダーのシーケンス番号は、必要に応じて調整されます。

vTCP と NAT およびファイアウォール ALG

ALG は、NAT およびファイアウォールのサブコンポーネントです。 NAT とファイアウォールのいずれにも、ダイナミックに ALG を連結させるためのフレームワークがあります。 ファイアウォールがレイヤ 7 インスペクションを実行すると、または NAT がレイヤ 7 フィックスアップを実行すると、ALG によって登録された解析機能が呼び出され、ALG がパケット インスペクションを引き継ぎます。 vTCP は、NAT およびファイアウォールと、これらのアプリケーションを使用する ALG との間に介入します。 言い換えると、パケットはまず vTCP によって処理されてから、ALG に渡されます。 vTCP は、TCP 接続内で両方向の TCP セグメントを再構成します。

ハイ アベイラビリティ サポート付き ALG-H.323 vTCP の概要

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポート付き ALG-H.323 vTCP の機能により、H.323 アプリケーション レベル ゲートウェイ（ALG-H）が拡張され、単一 H.323 メッ

セージではない TCP セグメントがサポートされます。 H.323 ALG を vTCP と組み合わせると、ファイアウォールおよび NAT は vTCP を介して H.323 ALG と対話します。 vTCP がデータのバッファを開始すると、ハイ アベイラビリティ（HA）機能が影響を受けます。これは、vTCP がバッファされたデータをスタンバイ デバイスに同期できないためです。 vTCP がデータをバッファしているときにスタンバイ デバイスへのスイッチオーバーが発生した場合、バッファされたデータがスタンバイ デバイスに同期されていないと、接続がリセットされる可能性があります。 バッファされたデータが vTCP によって確認された後、データは失われ、接続はリセットされます。ファイアウォールおよび NAT は、HA のためにデータを同期します。 vTCP は、スタンバイ デバイスへの現在の接続ステータスのみを同期し、エラーの場合、接続はリセットされます。

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポート付き ALG-H.323 vTCP の設定方法

ファイアウォール対応のハイアベイラビリティサポート付きALG-H.323 vTCP の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **match protocol** *protocol-name*
6. **exit**
7. **policy-map type inspect** *policy-map-name*
8. **class type inspect** *class-map-name*
9. **inspect**
10. **exit**
11. **class class-default**
12. **exit**
13. **zone security** *zone-name*
14. **exit**
15. **zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
16. **service-policy type inspect** *policy-map-name*
17. **exit**
18. **interface** *type number*
19. **zone member security** *zone-name*
20. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any h.323-class`	検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol h323`	指定されたプロトコルを基づいて、クラス マップの一致基準を設定します。
ステップ 5	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol h323ras`	指定されたプロトコルを基づいて、クラス マップの一致基準を設定します。
ステップ 6	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 7	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect h.323-policy`	検査タイプポリシーマップを作成し、QoSポリシーマップ コンフィギュレーション モードを開始します。
ステップ 8	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect h.323-class`	アクションを実行するクラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 10	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 11	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシー マップ設定を定義済みのデフォルト クラスに適用します。 • 設定済みクラスマップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 12	**exit** 例： `Device(config)# exit`	QoS ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 13	**zone security** *zone-name* 例： `Device(config)# zone security inside`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定には、ゾーン ペアを作成するために、2 つのセキュリティ ゾーン（送信元ゾーンと宛先ゾーン）が含まれている必要があります。 • ゾーン ペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。
ステップ 14	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**zone-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security inside-outside source inside destination outside`	セキュリティ ゾーンのペアを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • ポリシーを適用するには、ゾーン ペアを設定する必要があります。

	コマンドまたはアクション	目的
ステップ 16	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect h.323-policy`	ファイアウォール ポリシーマップを宛先ゾーンペアに付加します。 • ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 17	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 18	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 19	**zone member security** *zone-name* 例： `Device(config-if)# zone member security inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）は、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーンペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 20	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポート付き ALG-H.323 vTCP の設定例

例：ファイアウォール対応のハイ アベイラビリティ サポート付き ALG-H.323 vTCP の設定

```
Device# configure terminal
Device(config)# class-map type inspect h.323-class
Device(config-cmap)# match protocol h323
Device(config-cmap)# match protocol h323ras
Device(config-cmap)# exit
Device(config)# policy-map type inspect h323-policy
Device(config-pmap)# class type inspect h323
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap)# exit
Device(config)# zone security inside
Device(config-sec-zone)# exit
Device(config)# zone security outside
Device(config-sec-zone)# exit
Device(config)# zone-pair security inside-outside source inside destination outside
Device(config-sec-zone-pair)# service-policy type inspect h.323-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# zone-member security inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# zone-member security outside
Device(config-if)# end
```

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポート付き ALG-H.323 vTCP の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Commands List, All Releases』
ファイアウォール コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』

関連項目	マニュアル タイトル
NAT コマンド	『IP Addressing Services Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポート付き ALG-H.323 vTCP の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *30*：ファイアウォールおよび *NAT* 対応のハイ アベイラビリティ サポート付き *ALG-H.323 vTCP* の機能情報

機能名	リリース	機能情報
ファイアウォールおよび NAT 対応のハイ アベイラビリティ サポート付き ALG-H.323 vTCP	Cisco IOS XE Release 3.7S	ファイアウォールおよびNAT対応のハイ アベイラビリティ サポート付き ALG-H.323 vTCP の機能により、H.323 ALG が拡張され、単一 H.323 メッセージではない TCP セグメントがサポートされます。 vTCPは、セグメント再構成をサポートします。 この機能の導入前は、H.323 ALGは、TCP セグメントが完全な H.323 メッセージである場合だけTCPセグメントを処理していました。TCPセグメントが複数のメッセージである場合、H.323 ALG はその TCP セグメントを無視し、パケットは処理せずに渡されていました。

第 24 章

IPv6 ファイアウォールの FTP66 ALG サポート

IPv6 ファイアウォールの FTP66 ALG サポート機能を使用すると、FTP は IPv6 ファイアウォールとともに機能することができます。 このモジュールでは、ファイアウォール、ネットワーク アドレス変換（NAT）、およびステートフル NAT64 が、FTP66 アプリケーション レベル ゲートウェイ（ALG）とともに機能するように設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IPv6 ファイアウォールの FTP66 ALG サポートの制約事項

FTP66 ALG は次をサポートしていません。

- ボックスツーボックス ハイ アベイラビリティ。
- 加入者単位のファイアウォール。
- ステートレス ネットワーク アドレス変換 64（NAT64）。
- ステートフル NAT64 が設定されている場合の仮想ルーティングおよび転送（VRF）。
- 仮想 TCP（vTCP）、または変換後の小さいパケットへのパケット分割。

IPv6 ファイアウォールの FTP66 ALG サポートについて

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。 ALG は、アプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワークアドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバアプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、それらに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールはピンホールを開き、NATは、アプリケーション層データ ストリームの送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを実行します。 IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションにはALGのサポートが必要です。

FTP66 ALG サポートの概要

ファイアウォールは、IPv6パケットおよびステートフル ネットワーク アドレス変換64（NAT64）のインスペクションをサポートします。 IPv6 パケット インスペクションにおいて FTP が機能するには、アプリケーション層ゲートウェイ（ALG）（アプリケーション レベル ゲートウェイ

（ALG）とも呼ばれます）、FTP66が必要となります。 FTP66 ALGは、オールインワンFTP ALGおよび1つの FTP ALG とも呼ばれます。

FTP66 ALG は次のことをサポートします。

- ファイアウォール IPv4 パケット インスペクション
- ファイアウォール IPv6 パケット インスペクション
- NAT 設定
- NAT64 設定（FTP64 サポートとともに）
- NAT およびファイアウォール設定
- NAT64 およびファイアウォール設定

FTP66 ALG には次のセキュリティ脆弱性があります。

- パケットセグメンテーション攻撃：FTP ALG ステートマシンは、セグメント化されたパケットを検出でき、ステート マシンの処理は、完全なパケットを受信するまで停止します。
- バウンス攻撃：FTP ALG は、1024 より少ないデータ ポート番号を使用して（NAT 用の）ドアまたは（ファイアウォール用の）ピンホールを作成しません。 バウンス攻撃の防止は、ファイアウォールがイネーブルな場合にのみアクティブです。

FTP66 ALG でサポートされる FTP コマンド

FTP66 アプリケーション レベル ゲートウェイ（ALG）は、RFC 959 に基づいています。 ここでは、FTP66 ALG が処理する主要な RFC 959 と RFC 2428 の FTP コマンドおよび応答について説明します。

PORT コマンド

PORT コマンドは、アクティブ FTP モードで使用されます。 PORT コマンドでは、サーバが接続するアドレスとポート番号を指定します。 このコマンドを使用する場合、引数は、32ビットのインターネット ホスト アドレスと 16 ビットの TCP ポートのアドレスを連結したものになります。 アドレス情報は8ビットのフィールドに分割され、各フィールドの値は10進数（文字列表記）として送信されます。 フィールドは、カンマで区切られます。

次に、*h1* がインターネット ホスト アドレスの最上位の 8 ビットである PORT コマンドの例を示します。

```
PORT h1,h2,h3,h4,p1,p2
```

PASV コマンド

PASV コマンドは、TRANSFER コマンドを受信した場合、サーバのデフォルト データ ポートではないデータ ポートをリッスンし、別の接続を開始するのではなく、接続を待機するようサーバに要求します。 PASV コマンドに対する応答には、サーバがリッスンするホストとポート アドレスが含まれます。

拡張 FTP コマンド

拡張 FTP コマンドは、FTP が IPv4 以外のネットワーク プロトコルのデータ接続エンドポイント情報をやり取りできる方法を提供します。 拡張FTP コマンドは、RFC 2428 で規定されています。 RFC 2428 では、拡張 FTP コマンドの EPRT および EPSV は、FTP コマンドの PORT および PASV をそれぞれ置き換えます。

EPRT コマンド

EPRT コマンドを使用すると、データ接続に拡張アドレスを指定できます。 拡張アドレスは、ネットワーク プロトコル、ネットワーク アドレス、および転送アドレスで構成されている必要があります。 EPRT のコマンドの形式は次のとおりです。

```
EPRT<space><d><net-prt><d><net-addr><d><tcp-port><d>
```

- <net-prt>引数は、アドレス ファミリ番号である必要があり、次の表で説明するように定義される必要があります。

表 *31*：*<net-prt>* 引数の定義

アドレス ファミリ番号	プロトコル
1	IPv4（Pos81a）
2	IPv6（DH96）

- <net-addr>引数は、ネットワーク アドレスのプロトコル固有文字列表記です。 上記の表で指定された 2 つのアドレス ファミリ番号（アドレス ファミリ番号 1 と 2）の場合、次の表に示すアドレス形式である必要があります。

アドレス ファミリ番号	アドレス フォーマット	例
1	ドット付き 10 進数	10.135.1.2
2	DH96 で定義された IPv6 文字列表記	2001:DB8:1::1

- <tcp-port> 引数は、ホストがデータ接続をリッスンする TCP ポートの番号の文字列表記である必要があります。
- 次のコマンドは、TCP ポート 6275 でホスト 10.235.1.2 へのデータ接続を開くために IPv4 アドレスを使用するようにサーバに指定する方法を示します。
  ```
  EPRT |1|10.235.1.2|6275|
  ```
- 次のコマンドは、ポート 5282 で TCP データ接続を開くために IPv6 ネットワーク プロトコルおよびネットワーク アドレスを使用するようにサーバに指定する方法を示します。
  ```
  EPRT |2|2001:DB8:2::2:417A|5282|
  ```
- <d> 引数は、デリミタ文字であり、33 ～ 126 の範囲の ASCII 形式である必要があります。

EPSV コマンド

EPSV コマンドは、サーバがデータ ポートでリッスンし、接続を待機するよう要求します。 このコマンドへの応答には、接続をリッスンするTCPポート番号のみが含まれます。 拡張アドレスを使用してパッシブ モードを開始するための応答コードは、229 である必要があります。

EPSV コマンドへの応答で返されるテキストは、次の形式である必要があります。
`(<d><d><d><tcp-port><d>)`

- カッコで囲まれた文字列の一部は、データ接続を開くために EPRT コマンドで必要とされる正確な文字列である必要があります。

  カッコ内の最初の 2 つのフィールドは空白である必要があります。 3 番目のフィールドは、サーバがデータ接続のためにリッスンするTCPポート番号の文字列表記である必要があります。 データ接続で使用されるネットワーク プロトコルは、制御接続で使用されるのと同じネットワーク プロトコルです。 データ接続を確立するために使用されるネットワーク アドレスは、制御接続で使用されるのと同じネットワーク アドレスです。

- 次に、応答文字列の例を示します。
  ```
  Entering Extended Passive Mode (|||6446|)
  ```

次のFTP応答とコマンドもFTP66 ALGによって処理されます。 これらのコマンドの処理結果は、ステート マシンの状態遷移を駆動するために使用されます。

- 230 応答
- AUTH
- USER
- PASS

IPv6 ファイアウォールの FTP66 ALG サポートの設定方法

FTP66 ALG サポート用ファイアウォールの設定

match protocol ftp コマンドを使用して、FTP66 ALG を明示的にイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **exit**
12. **exit**
13. **zone security** *zone-name*
14. **exit**
15. **zone-pair security** *zone-pair* **source** *source-zone* **destination** *destination-zone*
16. **service-policy type inspect** *policy-map-name*
17. **exit**
18. **interface** *type number*
19. **no ip address**
20. **ip virtual-reassembly**
21. **zone-member security** *zone-name*
22. **negotiation auto**
23. **ipv6 address** *ipv6-address*/*prefix-length*
24. **cdp enable**
25. **exit**
26. **ipv6 route** *ipv6-prefix*/*prefix-length interface-type interface-number*
27. **ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address*
28. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any in2out-class`	検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol ftp`	指定されたプロトコルに基づくクラスマップの一致基準を設定します。
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect in-to-out`	検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect in2out-class`	アクションを実行するクラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシー マップ設定を定義済みのデフォルト クラスに適用して、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 11	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 12	**exit** 例： `Device(config-pmap)# exit`	QoS ポリシーマップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 13	**zone security** *zone-name* 例： `Device(config)# zone security inside`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。 • 設定には、ゾーン ペアを作成するために、2 つのセキュリティ ゾーン（送信元ゾーンと宛先ゾーン）が含まれている必要があります。 • ゾーン ペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。
ステップ 14	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**zone-pair security** *zone-pair* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security in2out source inside destination outside`	セキュリティ ゾーンのペアを作成し、セキュリティ ゾーン ペア コンフィギュレーション モードを開始します。 • ポリシーを適用するには、ゾーン ペアを設定する必要があります。

	コマンドまたはアクション	目的
ステップ 16	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect in-to-out`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 • ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 17	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 18	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 19	**no ip address** 例： `Device(config-if)# no ip address`	IPアドレスを削除するか、IP処理をディセーブルにします。
ステップ 20	**ip virtual-reassembly** 例： `Device(config-if)# ip virtual-reassembly`	インターフェイスでの仮想フラグメンテーション再構成（VFR）をイネーブルにします。
ステップ 21	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 22	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。

	コマンドまたはアクション	目的
ステップ 23	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:1::1/96`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 24	**cdp enable** 例： `Device(config-if)# cdp enable`	インターフェイス上で Cisco Discovery Protocol をイネーブルにします。
ステップ 25	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 26	**ipv6 route** *ipv6-prefix/prefix-length interface-type interface-number* 例： `Device(config)# ipv6 route 2001::/96 gigabitethernet 0/0/1`	スタティック IPv6 ルートを確立します。
ステップ 27	**ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address* 例： `Device(config)# ipv6 neighbor 2001:DB8:1::1 gigabitethernet 0/0/1 0000.29f1.4841`	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。
ステップ 28	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

FTP66 ALG サポート用 NAT の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip nat inside**
6. **zone-member security** *zone-name*
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask*
10. **ip nat outside**
11. **zone-member security** *zone-name*
12. **exit**
13. **ip nat inside source static** *local-ip global-ip*
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/2`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**ip nat inside** 例： `Device(config-if)# ip nat inside`	インターフェイスが内部ネットワーク（NAT 変換の対象になるネットワーク）に接続されていることを示します。
ステップ 6	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 7	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 8	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.2.1.1 255.255.255.0`	インターフェイスが内部ネットワーク（NAT 変換の対象になるネットワーク）に接続されていることを示します。
ステップ 10	**ip nat outside** 例： `Device(config-if)# ip nat outside`	インターフェイスが外部ネットワークに接続されていることを示します。
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security outside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するに

	コマンドまたはアクション	目的
		は、ゾーンをポリシーの適用先のゾーンペアの一部にする必要があります。ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 13	**ip nat inside source static** *local-ip global-ip* 例： `Device(config)# ip nat inside source static 10.1.1.10 10.1.1.80`	内部送信元アドレスの NAT をイネーブルにします。
ステップ 14	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

FTP66 ALG サポート用 NAT64 の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **no ip address**
6. **ipv6 virtual-reassembly**
7. **zone-member security** *zone-name*
8. **negotiation auto**
9. **ipv6 address** *ipv6-address*
10. **ipv6 enable**
11. **nat64 enable**
12. **cdp enable**
13. **exit**
14. **interface** *type number*
15. **ip address** *type number*
16. **ip virtual-reassembly**
17. **zone member security** *zone-name*
18. **negotiation auto**
19. **nat64 enable**
20. **exit**
21. **ipv6 route** *ipv6-address interface-type interface-number*
22. **ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address*
23. **nat64 v6v4 static** *ipv6-address ipv4-address*
24. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。
ステップ 4	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**no ip address** 例： `Device(config-if)# no ip address`	IP アドレスを削除するか、IP 処理をディセーブルにします。
ステップ 6	**ipv6 virtual-reassembly** 例： `Device(config-if)# ipv6 virtual-reassembly`	インターフェイスでの仮想フラグメンテーション再構成（VFR）をイネーブルにします。
ステップ 7	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security inside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 8	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 9	**ipv6 address** *ipv6-address* 例： `Device(config-if)# ipv6 address 2001:DB8:1::2/96`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 10	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 11	**nat64 enable** 例： `Device(config-if)# nat64 enable`	インターフェイスで NAT64 をイネーブルにします。
ステップ 12	**cdp enable** 例： `Device(config-if)# cdp enable`	インターフェイス上で Cisco Discovery Protocol をイネーブルにします。
ステップ 13	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 14	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 15	**ip address** *type number* 例： `Device(config-if)# ip address 209.165.201.25 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 16	**ip virtual-reassembly** 例： `Device(config-if)# ip virtual-reassembly`	インターフェイス上で VFR をイネーブルにします。
ステップ 17	**zone member security** *zone-name* 例： `Device(config-if)# zone member security outside`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。 • インターフェイスをセキュリティ ゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（ルータ宛のトラフィックまたはルータ発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラ

	コマンドまたはアクション	目的
		フィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 18	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 19	**nat64 enable** 例： `Device(config-if)# nat64 enable`	インターフェイスで NAT64 をイネーブルにします。
ステップ 20	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 21	**ipv6 route** *ipv6-address interface-type interface-number* 例： `Device(config)# ipv6 route 2001:DB8:1::2/96 gigabitethernet 0/0/0`	スタティック IPv6 ルートを確立し、指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレスを指定します。
ステップ 22	**ipv6 neighbor** *ipv6-address interface-type interface-number hardware-address* 例： `Device(config)# ipv6 neighbor 2001:DB8:1::103 gigabitethernet 0/0/0 0000.29f1.4841`	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。
ステップ 23	**nat64 v6v4 static** *ipv6-address ipv4-address* 例： `Device(config)# nat64 v6v4 static 2001:DB8:1::103 209.165.201.32`	NAT64 の IPv6 送信元アドレスを IPv4 送信元アドレスに、および IPv4 宛先アドレスを IPv6 宛先アドレスに変換します。
ステップ 24	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

IPv6 ファイアウォールの FTP66 ALG サポートの設定例

例：FTP66 ALG サポート用 IPv6 ファイアウォールの設定

```
Device# configure terminal
Device(config)# class-map type inspect match-any in2out-class
Device(config-cmap)# match protocol ftp
Device(config-cmap)# exit
Device(config)# policy-map type inspect in-to-out
Device(config-pmap)# class type inspect in2out-class
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# zone security inside
Device(config-sec-zone)# exit
Device(config)# zone security outside
Device(config-sec-zone)# exit
Device(config)# zone-pair security in2out source inside destination outside
Device(config-sec-zone-pair)# service-policy type inspect in-to-out
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# ip virtual-reassembly
Device(config-if)# zone-member security inside
Device(config-if)# negotiation auto
Device(config-if)# ipv6 address 2001:DB8:1::1/96
Device(config-if)# cdp enable
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# no ip address
Device(config-if)# ip virtual-reassembly
Device(config-if)# zone-member security outside
Device(config-if)# negotiation auto
Device(config-if)# ipv6 address 2001:DB8:2::2/96
Device(config-if)# exit
Device(config)# ipv6 route 2001::/96 gigabitethernet 0/0/1
Device(config)# ipv6 route 2001::/96 gigabitethernet 0/1/1
Device(config)# ipv6 neighbor 2001:DB8:1::1 gigabitethernet 0/0/1 0000.29f1.4841
Device(config)# ipv6 neighbor 2001:DB8:2::2 gigabitethernet 0/1/1 0000.29f1.4842
Device(config)# end
```

例：FTP66 ALG サポート用 NAT の設定

```
Device# configure terminal
Device(config)# interface gigabitethernet 0/1/2
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip nat inside
Device(config-if)# zone-member security inside
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# ip address 10.2.1.1 255.255.255.0
Device(config-if)# ip nat outside
Device(config-if)# zone-member security outside
Device(config-if)# exit
Device(config-if)# ip nat inside source static 10.1.1.10 10.1.1.80
```

例：FTP66 ALG サポート用 NAT64 の設定

```
Device# configure terminal
Device(config)# ipv6 unicast-routing
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# no ip address
Device(config-if)# ipv6 virtual-reassembly
Device(config-if)# zone-member security inside
Device(config-if)# negotiation auto
Device(config-if)# ipv6 address 2001:DB8:1::2/96
Device(config-if)# ipv6 enable
Device(config-if)# nat64 enable
Device(config-if)# cdp enable
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/1/1
Device(config-if)# ip address 209.165.201.25 255.255.255.0
Device(config-if)# ip virtual-reassembly
Device(config-if)# zone member security outside
Device(config-if)# negotiation auto
Device(config-if)# nat64 enable
Device(config-if)# exit
Device(config)# ipv6 route 2001:DB8:1::2/96 gigabitethernet 0/0/0
Device(config)# 2001:DB8:1::103 gigabitethernet 0/0/0 0000.29f1.4841
Device(config)# nat64 v6v4 static 2001:DB8:1::103 209.165.201.32
```

IPv6 ファイアウォールの FTP66 ALG サポートの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
NAT コマンド	『IP Addressing Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 959	『*File Transfer Protocol*』
RFC 2428	『*FTP Extensions for IPv6 and NATs*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 ファイアウォールの FTP66 ALG サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *32*：*IPv6* ファイアウォールの *FTP66 ALG* サポートの機能情報

機能名	リリース	機能情報
IPv6 ファイアウォールの FTP66 ALG サポート	Cisco IOS XE Release 3.7S	IPv6 ファイアウォールの FTP66 ALG サポート機能を使用すると、FTP は IPv6 ファイアウォールとともに機能することができます。 このモジュールでは、ファイアウォール、ネットワークアドレス変換（NAT）、および NAT64 が、FTP66 アプリケーション レベル ゲートウェイ（ALG）とともに機能するように設定する方法について説明します。

第 25 章

NAT およびファイアウォールの SIP ALG の強化

NAT およびファイアウォールの SIP ALG の強化機能は、ネットワーク アドレス変換（NAT）およびファイアウォールの既存の Session Initiation Protocol（SIP）アプリケーション レベル ゲートウェイ（ALG）サポートを介してより適切なメモリ管理と RFC 準拠を提供します。 この機能は、次の拡張機能を提供します。

- すべての SIP レイヤ 7 データのローカル データベースの管理
- Via ヘッダーの処理
- 追加の SIP メソッドのロギングのサポート
- Provisional Response ACKnowledgment（PRACK）コール フローのサポート
- Record-Route ヘッダーのサポート

上記の拡張機能は、デフォルトで利用可能です。NAT またはファイアウォールに対する追加の設定は必要ありません。

このモジュールでは、SIP ALG 拡張機能について説明し、SIP 用の NAT およびファイアウォール サポートを有効にする方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

NAT およびファイアウォールの SIP ALG の強化の制約事項

- Session Initiation Protocol（SIP）アプリケーション レベル ゲートウェイ（ALG）は、セキュリティ機能を提供しません。
- SIP ALG は、コール ID に基づいてローカル データベースを管理します。 2 つのコールが同じコール ID で 2 つの異なるクライアントから発信され、結果としてコール ID が重複するというまれで厄介なケースが発生する場合があります。

NAT およびファイアウォールの SIP ALG の強化について

SIP の概要

Session Initiation Protocol（SIP）は、1 人または複数の参加者とのセッションを作成、変更、および終了するためのアプリケーション層コントロール（シグナリング）プロトコルです。 SIP セッションには、インターネット電話の通話、マルチメディアの配布、マルチメディア会議などがあります。 SIP は HTTP のような要求/応答トランザクション モデルに基づいています。 各トランザクションは、サーバで特定のメソッドまたは関数を呼び出す 1 つの要求と 1 つ以上の応答で構成されます。

セッションの作成に使用される SIP の招待は、互換性のあるメディア タイプのセットに参加者が同意できるセッション記述を伝送しています。 SIP は、プロキシ サーバと呼ばれる要素を利用して、ユーザの所在地への要求のルーティング、サービスのためのユーザ認証および認可、プロバイダーのコールルーティング ポリシーの実装、およびユーザへの機能提供を行っています。 また、SIP には、プロキシ サーバから使用できるように、ユーザの所在地をアップロードできる登録機能があります。 SIP は複数のトランスポート プロトコルを基礎として実行されます。

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。 ALG は、アプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、それらに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用できるネットワーク層アドレス情報を変換します。

ファイアウォールはピンホールを開き、NATは、アプリケーション層データ ストリームの送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換サービスを実行します。IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションにはALGのサポートが必要です。

SIP ALG ローカル データベース管理

Session Initiation Protocol（SIP）トランクは、SIP を使用した IP ネットワーク上のサービス プロバイダーへの IP PBX の直接接続です。 SIP トランクには多数の同時コールが存在する可能性があります。 コール設定プロセス中、すべてのコールが、コールの確立に同じ制御チャネルを使用します。 複数のコールが、コール設定に同じ制御チャネルを使用します。 同じ制御チャネルが複数のコールで使用されると、制御チャネル セッションに保存されたステートフル情報は、信頼できないものになります。 SIP ステートフル情報は、メディア データを送信するためにクライアントおよびサーバ エンドポイントが使用する IP アドレスやポート番号などのメディア チャネル情報で構成されます。 メディア チャネル情報を使用して、ファイアウォール ピンホールおよびネットワーク アドレス変換（NAT）ドアが、ファイアウォールおよび NAT のデータ チャネルにそれぞれ作成されます。 複数のコールがコース設定に同じ制御チャネルを使用するため、複数のメディア データ セットが存在することになります。

SIP トランクで、複数のコールが、同じファイアウォールおよび NAT セッションを共有します。NAT およびファイアウォールは、SIP パケットの 5 タプル（送信元アドレス、宛先アドレス、送信元ポート、宛先ポート、およびプロトコル）を使用して SIP セッションを識別および管理します。 コールの識別および照合に 5 タプルを使用する従来の方式は、SIP トランキングを完全にサポートしているわけではなく、多くの場合、レイヤ 7 データ メモリ リークやコール照合の問題を招きます。

他のアプリケーション レベル ゲートウェイ（ALG）とは対照的に、SIP ALG は、ローカル データベースを使用して通常の SIP コールおよび SIP トランクに埋め込まれた SIP コールに含まれる

すべてのメディア関連情報を保存することで、SIP レイヤ 7 データを管理します。 SIP ALG は、SIP メッセージに含まれる Call-ID ヘッダー フィールドを使用して、コール照合に関してローカル データベースを検索し、コールを管理および終了します。 Call-ID ヘッダー フィールドは、同じ SIP ダイアログに属するメッセージを識別するダイアログ識別子です。

SIP ALG は、コール ID を使用して、ローカル データベースで検索を実行し、メモリ リソースを管理します。 SIP ALG がレイヤ 7 データ レコードをデータベースから解放できない特定のシナリオでは、セッション タイマーを使用してリソースの管理および解放が行われ、データベース内に停止状態のコール レコードが残らないようにします。

（注） すべてのレイヤ 7 データは、ローカル データベースを使用して SIP ALG によって管理されるため、SIP ALG は、SIP レイヤ 7 データの解放をファイアウォールおよび NAT には依存せず、自分でデータを解放します。 **clear** コマンドを使用して、すべての NAT 変換およびファイアウォール セッションをクリアしている場合、ローカル データベース内の SIP レイヤ 7 データは解放されません。

SIP ALG Via ヘッダー サポート

Session Initiation Protocol（SIP）INVITE 要求には、Via ヘッダー フィールドが含まれます。 Via ヘッダー フィールドは、SIP 要求が通過する転送パスを示します。 Via ヘッダーには、後続の SIP 応答のリターン パスに関する情報も含まれます。これには、応答メッセージが送信される IP アドレスおよびポートが含まれます。

SIP ALG では、確認応答（ACK）メッセージを除き、受信した各 SIP 要求の Via ヘッダー フィールドの最初の値に基づいてファイアウォール ピンホールまたはネットワーク アドレス変換（NAT）ドアを作成します。 ポート番号情報が、最初の Via ヘッダーで欠落している場合、ポート番号は 5060 と見なされます。

SIP ALG メソッド ロギングのサポート

NAT およびファイアウォールの SIP ALG の強化機能は、Session Initiation Protocol（SIP）アプリケーション レベル ゲートウェイ（ALG）統計情報の次のメソッドの詳細なロギングをサポートします。

- PUBLISH
- OPTIONS
- 1XX（100、180、183 を除く）
- 2XX（200 を除く）

SIP ALG 統計情報に記録された既存の SIP メソッドには、ACK、BYE、CANCEL、INFO、INVITE、MESSAGE、NOTIFY、REFER、REGISTER、SUBSCRIBE、および 1XX-6XX が含まれます。

SIP ALG PRACK コール フローのサポート

Session Initiation Protocol（SIP）では、最終応答と暫定応答の 2 種類の応答が定義されています。最終応答は、要求の処理結果を伝え、信頼性のある方法で送信されます。 一方、暫定応答は、要求処理の進捗状況に関する情報を提供しますが、信頼性のある方法では送信されません。

Provisional Response ACKnowledgment（PRACK）は、確認応答（ACK）システムを暫定応答に提供する SIP メソッドです。 PRACK を使用すると、SIP エンドポイント間の SIP の暫定応答を確実に交換できます。 SIP の信頼性の高い暫定応答によってメディア情報の交換が保証され、コールの接続前にリソース予約を実行できます。

SIP は、接続ネゴシエーション中、セッション記述プロトコル（SDP）の接続、メディア、および属性のフィールドを使用します。 SIP アプリケーション レベル ゲートウェイ（ALG）は、PRACK メッセージ内の SDP 情報をサポートします。 メディア情報が PRACK メッセージに存在する場合、SIP ALG はメディア情報を取得して処理します。 SIP ALG は、以降のメディア ストリームのメディア チャネルの作成も処理します。 SIP ALG は、PRACK メッセージの SDP 情報に基づいて、ファイアウォール ピンホールおよび NAT ドアを作成します。

SIP ALG Record-Route ヘッダー サポート

Record-Route ヘッダー フィールドは、SIP ダイアログの今後の要求がプロキシ経由でルーティングされるよう強制するために、Session Initiation Protocol（SIP）プロキシによって SIP 要求に追加されました。 これで、ダイアログ内で送信されるメッセージはすべての SIP プロキシを通過し、これにより、Record-Route ヘッダー フィールドが SIP 要求に追加されます。 Record-Route ヘッダー フィールドには、プロキシを識別する、グローバルに到達可能な Uniform Resource Identifier（URI）が含まれます。

SIP アプリケーション レベル ゲートウェイ（ALG）は、Contact ヘッダーを解析し、Contact ヘッダーの IP アドレスとポートの値を使用して、ファイアウォール ピンホールおよびネットワーク アドレス変換（NAT）ドアを作成します。 さらに、SIP ALG は、プロキシ経由でルーティングされる今後のメッセージ用のファイアウォール ピンホールおよび NAT ドアを作成するための Record-Route ヘッダーの解析をサポートします。

Record-Route ヘッダーの解析では、SIP ALG は次のシナリオをサポートします。

- Cisco ASR 1000 アグリゲーション サービス ルータが、2 つのプロキシの間に配置されます。
- Cisco ASR 1000 アグリゲーション サービス ルータが、ユーザ エージェント クライアント（UAC）とプロキシの間に配置されます。
- Cisco ASR 1000 アグリゲーション サービス ルータが、プロキシとユーザ エージェント サーバ（UAS）の間に配置されます。
- クライアントとサーバ間にプロキシは存在しません。 このシナリオではレコード ルーティングは発生しません。

NAT およびファイアウォールの SIP ALG の強化の設定方法

SIP の NAT サポートのイネーブル化

SIP の NAT サポートは、ポート 5060 でデフォルトでイネーブルになっています。この機能がディセーブルになっている場合、SIP の NAT サポートを再びイネーブルにするには、この作業を実行します。SIP の NAT サポートをディセーブルにするには、**no ip nat service sip** コマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat service sip** {**tcp** | **udp**} **port** *port-number*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip nat service sip** {**tcp** | **udp**} **port** *port-number* 例： `Device(config)# ip nat service sip tcp port 5060`	SIP の NAT サポートをイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SIP インスペクションのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any sip-class1`	検査タイプ クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol sip`	指定されたプロトコルに基づいてクラス マップの一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了します。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect sip-policy`	検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect sip-class1`	アクションを実行するクラスを指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーションモードに戻ります。
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	これらのポリシー マップ設定が事前に定義したデフォルト クラスに適用されることを指定します。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 11	**end** 例： `Device(config-pmap)# end`	ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ゾーン ペアの設定および SIP ポリシー マップの付加

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** {*zone-name* | **default**}
4. **exit**
5. **zone security** {*zone-name* | **default**}
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *zone-name*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *zone-name*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**zone security** {*zone-name*	**default**} 例： `Device(config)# zone security zone1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security zone2`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]] 例： `Device(config)# zone-pair security in-out source zone1 destination zone2`	ゾーン ペアを作成し、セキュリティ ゾーンペア コンフィギュレーション モードに戻ります。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect sip-policy`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。

	コマンドまたはアクション	目的
		（注） インターフェイスをセキュリティゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone2`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。
ステップ 15	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

NAT およびファイアウォールの SIP ALG の強化の設定例

例：SIP の NAT サポートのイネーブル化

```
Device> enable
Device# configure terminal
Device(config)# ip nat service sip tcp port 5060
Device(config)# end
```

例：SIP インスペクションのイネーブル化

```
class-map type inspect match-any sip-class1
 match protocol sip
!
policy-map type inspect sip-policy
 class type inspect sip-class1
  inspect
!
class class-default
```

例：ゾーン ペアの設定および SIP ポリシー マップの付加

```
zone security zone1
!
zone security zone2
!
zone-pair security in-out source zone1 destination zone2
 service-policy type inspect sip-policy
!
interface gigabitethernet 0/0/0
 zone security zone1
!
interface gigabitethernet 0/1/1
 zone security zone2
```

NAT およびファイアウォールの SIP ALG の強化の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
NAT 設定	『*IP Addressing: NAT Configuration Guide*』
ファイアウォールの設定	『*Security Configuration Guide: Zone-Based Policy Firewall*』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

関連項目	マニュアル タイトル
NAT とファイアウォールの ALG のサポート	『NAT and Firewall ALG and AIC Support on Cisco ASR 1000 Series Aggregation Services Routers』マトリクス

標準および RFC

標準/RFC	タイトル
RFC 3261	『*SIP: Session Initiation Protocol*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NAT およびファイアウォールの SIP ALG の強化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *33*：*NAT* およびファイアウォールの *SIP ALG* の強化の機能情報

機能名	リリース	機能情報
NAT およびファイアウォールの SIP ALG の強化	Cisco IOS XE Release 3.8S	NAT およびファイアウォールの SIP ALG の強化機能は、NAT およびファイアウォールの既存の SIP ALG サポートを介してより適切なメモリ管理と RFC 準拠を提供します。

第 26 章

TCP リセット セグメント制御

TCP リセット セグメント制御機能は、ハーフクローズ セッション、ハーフオープン セッション、またはアイドル セッションのセッション削除が発生した場合に TCP リセット（RST）セグメントが送信されるかどうかを設定するメカニズムを提供します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

TCP リセット セグメント制御について

TCP リセット セグメント制御

TCP ヘッダーには、リセット（RST）フラグと呼ばれるフラグが含まれます。 参照される接続の基準を満たさないセグメントが到着するたびに、RST フラグが設定された TCP セグメントが送信されます。 たとえば、接続要求が宛先ポートで受信されたが、そのポートでリッスンしているプロセスがない場合、RST フラグが設定された TCP セグメントが送信されます。

この動作は、ホスト間通信用に RFC 793、『Transmission Control Protocol』で定義され、さまざまなベンダーによって実装されています。 ただし、ホスト間のネットワークに存在するネットワークデバイスの場合、セッション（ハーフオープン、アイドル、ハーフクローズ）がクリアされたときに、デバイスが TCP RST セグメントを接続の開始側、受信側、またはその両方に送信するかどうかを決定する特定のルールは定義されていません。 一部のデバイスは、セッションがクリアされると、送信元ポートおよび受信側ポートの両方に TCP RST セグメントを送信する一方で、一部のデバイスは、TCP RST セグメントを送信せずにセッション テーブル内のセッションを暗黙的に削除します。

TCP リセットセグメント制御機能は、ハーフクローズセッション、ハーフオープンセッション、またはアイドルセッションのセッションがクリアされた場合に TCP RST セグメントを送信するかどうかを設定するメカニズムを提供します。

ハーフオープン セッションは、TCP 同期（SYN）セグメントによって開始されたが、TCP スリーウェイ ハンドシェイクが発生しただけの不完全な未確立セッションであり、タイマーが起動されます。

TCP は、接続の一方の端が、接続の反対の端からのデータを引き続き受信する一方で、その出力を終了する機能を提供します。 この TCP 状態は、ハーフクローズと呼ばれます。 セッションは、最初の TCP FIN セグメントを受信するとハーフクローズ状態になり、タイマーを起動します。 セッションがタイム アウトする前に別のセグメントを受信した場合、タイマーが再起動されます。

tcp synwait-time コマンドを使用して、ハーフオープン セッションとハーフクローズ セッションのタイムアウト値を設定できます。 デフォルトのタイムアウト値は 30 秒です。

アイドル セッションは、2 つのデバイス間でアクティブで、長期にわたっていずれのデバイスからもデータが送信されない TCP セッションです。 **tcp idle-time** コマンドを使用して、アイドル セッションのタイム アウト値を設定できます。 アイドル セッションのデフォルトのタイムアウト値は 3600 秒です。

タイムアウトが TCP セッションで発生し、セッションがクリアされると、TCP RST セグメントが送信され、TCP リセット セグメント制御がセッションに設定されている場合のみ、セッションがリセットされます。

TCP リセット セグメント制御の設定方法

ハーフオープン セッションの TCP リセットの設定

ハーフオープン セッションは、TCP 同期（SYN）セグメントによって開始されたが、スリーウェイ ハンドシェイクが不完全な未確立セッションです。 不完全なスリーウェイ ハンドシェイクが発生するとただちに、タイマーが起動されます。 **tcp synwait-time** コマンドを使用して、ハーフオープン セッション タイムアウトのタイマー値を設定できます。 これらのセッションのデフォルトのタイムアウト値は 30 秒です。

タイムアウトが発生すると、ハーフオープン TCP セッションのセッションはクリアされ、TCP リセット（RST）セグメントが送信され、TCP リセット セグメント制御がセッションで設定されている場合のみ、セッションがリセットされます。

tcp half-open reset on コマンドを設定している場合は、セッションがクリアされると、ハーフオープン セッションの両端に TCP RST セグメントが送信されます。 **tcp half-open reset off** コマンドを設定している場合は、セッションがクリアされても TCP RST セグメントは送信されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **tcp synwait-time** *seconds*
5. **tcp half-open reset** {**off** | **on**}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap-name`	（任意）接続しきい値、タイムアウト、および **inspect** キーワードに関連するその他のパラメータの検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**tcp synwait-time** *seconds* 例： `Device(config-profile)# tcp synwait-time 10`	セッションをドロップする前に、TCP セッションが確立状態に達するまでソフトウェアが待機する時間を指定します。
ステップ 5	**tcp half-open reset** {**off** | **on**} 例： `Device(config-profile)# tcp half-open reset on`	タイムアウトが発生し、ハーフオープン セッションのセッションがクリアされた場合に、TCP RST セグメントが送信されるかどうかを指定します。
ステップ 6	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ハーフクローズ セッションの TCP リセットの設定

TCP は、接続の一方の端が、接続の反対の端からのデータを引き続き受信する一方で、その出力を終了する機能を提供します。 この TCP 状態は、ハーフクローズと呼ばれます。 セッションは、最初の TCP finish（FIN）セグメントを受信するとハーフクローズ状態になり、タイマーを起動します。 セッションがタイムアウトする前に別のセグメントを受信した場合、タイマーが再起動されます。 **tcp synwait-time** コマンドを使用して、ハーフクローズ セッションのタイムアウト値を設定できます。 ハーフクローズ セッションのデフォルトのタイムアウト値は 30 秒です。

タイムアウトがハーフクローズ TCP セッションで発生すると、TCP RST セグメントが送信され、TCP リセット セグメント制御がセッションに設定されている場合のみ、セッションがリセットされます。

tcp half-close reset on コマンドを設定している場合は、タイムアウトが発生し、セッションがクリアされると、ハーフオープン セッションの両端に TCP RST セグメントが送信されます。 **tcp half-close reset off** コマンドを設定している場合は、セッション タイムアウトが発生し、セッションがクリアされても、TCP RST セグメントは送信されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **tcp synwait-time** *seconds*
5. **tcp half-close reset** {**off** | **on**}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap-name`	接続しきい値、タイムアウト、および **inspect** キーワードに関連するその他のパラメータの検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**tcp synwait-time** *seconds* 例： `Device(config-profile)# tcp synwait-time 10`	（任意）セッションをドロップする前に、TCP セッションが設定された状態に達するまで待機する時間を指定します。
ステップ 5	**tcp half-close reset** {**off** | **on**} 例： `Device(config-profile)# tcp half-close reset on`	セッションの削除がハーフオープンセッションで発生した場合に TCP RST セグメントが送信されるかどうかを指定します。
ステップ 6	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

アイドル セッションの TCP リセットの設定

アイドル セッションは、2 つのデバイス間でアクティブで、長期にわたっていずれのデバイスからもデータが送信されていない TCP セッションです。 **tcp idle-time** コマンドを使用して、アイドル セッションのタイム アウト値を設定できます。 アイドル セッションのデフォルトのタイムアウト値は 3600 秒です。

タイムアウトがアイドル TCP セッションで発生すると、TCP RST セグメントが送信され、TCP リセット セグメント制御がセッションに設定されている場合はセッションがリセットされます。

tcp idle reset on コマンドを設定している場合は、タイムアウトが発生し、セッションがクリアされると、アイドル セッションの両端に TCP RST セグメントが送信されます。 **tcp idle reset off** コマンドをしている場合は、セッションタイムアウトが発生し、セッションがクリアされても、TCP RST セグメントは送信されません。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **tcp idle-time** *seconds*
5. **tcp idle reset** {**off** | **on**}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect pmap-name`	接続しきい値、タイムアウト、および **inspect** キーワードに関連するその他のパラメータの検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**tcp idle-time** *seconds* 例： `Device(config-profile)# tcp idle-time 90`	（任意）TCP セッションのタイムアウトを設定します。
ステップ 5	**tcp idle reset** {**off** | **on**} 例： `Device(config-profile)# tcp idle reset on`	セッションの削除がアイドル セッションで発生した場合に TCP RST セグメントが送信されるかどうかを指定します。
ステップ 6	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

TCP リセット セグメント制御の設定例

例：ハーフオープン セッションの TCP リセットの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-name
Device(config-profile)# tcp synwait-time 10
Device(config-profile)# tcp half-open reset on
Device(config-profile)# end
```

例：ハーフクローズ セッションの TCP リセットの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-name
Device(config-profile)# tcp synwait-time 10
Device(config-profile)# tcp half-close reset on
Device(config-profile)# end
```

例：アイドル セッションの TCP リセットの設定

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-name
Device(config-profile)# tcp idle-time 90
Device(config-profile)# tcp idle reset on
```

```
Device(config-profile)# end
```

TCP リセット セグメント制御の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
ファイアウォール コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

標準および RFC

標準/RFC	タイトル
RFC 793	『Transmission Control Protocol』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

TCP リセット セグメント制御の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *34*：*TCP* リセット セグメント制御の機能情報

機能名	リリース	機能情報
TCP リセット セグメント制御	Cisco IOS XE Release 3.8S	TCP リセット セグメント制御機能は、ハーフオープン セッション、ハーフクローズ セッション、およびアイドル セッションのセッションがクリアされた場合に、TCP RST ビットが送信されるかどうかを設定するための一貫したメカニズムを提供します。 次のコマンドが導入または変更されました。**tcp idle reset**、**tcp half-close reset**、および **tcp half-open reset**。

第 27 章

ファイアウォール高速ロギング

ファイアウォール高速ロギング機能は、エクスポート フォーマットとして NetFlow バージョン 9 を使用して、ファイアウォール メッセージの高速ロギング（HSL）をサポートします。

このモジュールでは、ゾーンベース ポリシー ファイアウォールに HSL を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ファイアウォール高速ロギングについて

ファイアウォール高速ロギングの概要

ゾーンベース ファイアウォールは、高速ロギング（HSL）をサポートします。HSL が設定されている場合、ファイアウォールは、（NetFlow バージョン 9 レコードと同様）ルーティング デバイスを介して外部コレクタに伝送されるパケットのログを提供します。 セッションが作成されたとき、および破棄されたときに、レコードが送信されます。 セッション レコードには、完全な 5 タプル情報（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびプロトコル）が含まれます。 タプルは、要素の順序付きリストです。

HSL により、ファイアウォールは、パケット処理への影響を最小限に抑えてレコードをログに記録できます。 ファイアウォールは HSL にバッファ モードを使用します。 バッファ モードでは、ファイアウォールは、高速ロガー バッファに直接記録し、パケットを個別にエクスポートします。

ファイアウォールは、次のタイプのイベントをログに記録します。

- 監査：セッションの作成および削除の通知。
- アラート：ハーフオープンおよび最大オープン TCP セッションの通知。
- ドロップ：パケット ドロップの通知。
- 通過：（設定済みレート制限に基づく）パケット通過の通知。
- サマリー：ポリシー ドロップと通過サマリーの通知。

NetFlow コレクタは、**show platform software interface F0 brief** コマンドを発行して、インターフェイス名に FW_SRC_INTF_ID および FW_DST_INTF_ID インターフェイス ID をマッピングします。

show platform software interface F0 brief コマンドの次の出力例は、[ID] カラムがインターフェイス ID をインターフェイス名（[Name] カラム）にマッピングすることを示しています。

```
Device# show platform software interface F0 brief

Name                          ID      QFP ID
GigabitEthernet0/2/0          16         9
GigabitEthernet0/2/1          17        10
GigabitEthernet0/2/2          18        11
GigabitEthernet0/2/3          19        12
```

NetFlow フィールド ID の説明

次の表に、ファイアウォール Netflow テンプレート内で使用される NetFlow フィールド ID をリストします。

表 *35* : *NetFlow* フィールド *ID*

フィールド ID	タイプ	長さ	説明
NetFlow ID フィールド（レイヤ 3 IPv4）			
FW_SRC_ADDR_IPV4	8	4	発信元 IPv4 アドレス
FW_DST_ADDR_IPV4	12	4	送信先 IPv4 アドレス
FW_SRC_ADDR_IPV6	27	16	発信元 IPv6 アドレス
FW_SRC_ADDR_IPV6	28	16	送信先 IPv6 アドレス
FW_PROTOCOL	4	1	IP プロトコル値
FW_IPV4_IDENT	54	4	IPv4 識別名
FW_IP_PROTOCOL_VERSION	60	1	IP プロトコル バージョン
フロー ID フィールド（レイヤ 4）			
FW_TCP_FLAGS	6	1	TCP フラグ
FW_SRC_PORT	7	2	送信元ポート
FW_DST_PORT	11	2	宛先ポート
FW_ICMP_TYPE	176	1	ICMP [1] タイプ値
FW_ICMP_CODE	177	1	ICMP コード値
FW_ICMP_IPV6_TYPE	178	1	ICMP バージョン 6（ICMPv6）タイプ値
FW_ICMP_IPV6_CODE	179	1	ICMPv6 コード値
FW_TCP_SEQ	184	4	TCP シーケンス番号
FW_TCP_ACK	185	4	TCP 確認応答番号
フロー ID フィールド（レイヤ 7）			
FW_L7_PROTOCOL_ID	95	2	レイヤ 7 プロトコル ID。 ファイアウォールインスペクションで使用されるレイヤ 7 アプリケーション分類を識別します。

フィールド ID	タイプ	長さ	説明
フロー名フィールド（レイヤ 7）			
FLOW_FIELD_L7_PROTOCOL_NAME	96	32	レイヤ 7 プロトコルの名前。 レイヤ 7 プロトコル ID（FW_L7_PROTOCOL_ID）に対応するレイヤ 7 プロトコル名を識別します。
フロー ID フィールド（インターフェイス）			
FW_SRC_INTF_ID	10	2	入力 SNMP [2] ifIndex
FW_DST_INTF_ID	14	2	出力 SNMP ifIndex
FW_SRC_VRF_ID	234	4	入力（発信側）VRF [3] ID
FW_DST_VRF_ID	235	5	出力（応答側）VRF ID
FW_VRF_NAME	236	32	VRF 名
マッピングされたフロー ID フィールド（ネットワーク アドレス変換）			
FW_XLATE_SRC_ADDR_IPV4	225	4	マッピングされた発信元 IPv4 アドレス
FW_XLATE_DST_ADDR_IPV4	226	4	マッピングされた送信先 IPv4 アドレス
FW_XLATE_SRC_PORT	227	2	マッピングされた発信元ポート
FW_XLATE_DST_PORT	228	2	マッピングされた送信先ポート
ステータスおよびイベント フィールド			
FW_EVENT	233	1	高レベルのイベント コード • 0：無視（無効） • 1：フローが作成されました。 • 2：フローが削除されました。 • 3：フローが拒否されました。 • 4：フロー アラート

フィールド ID	タイプ	長さ	説明
FW_EXT_EVENT	35,001	1	拡張イベント コード
タイムスタンプおよび統計情報フィールド			
FW_EVENT_TIME_MSEC	323	8	イベントが発生した時刻。0000 UTC [4] 1970/01/01 からの経過時間がミリ秒単位で表示され、イベントがマイクロ秒単位の場合は 324、ナノ秒単位の場合は 325 を使用します
FW_INITIATOR_OCTETS	231	8	発信側から着信したパケットフロー内のレイヤ 4 ペイロードバイトの総数
FW_RESPONDER_OCTETS	232	8	応答側から着信したパケットフロー内のレイヤ 4 ペイロードバイトの総数
AAA フィールド			
FW_USERNAME	40,000	20	AAA [5] ユーザ名
FW_USERNAME_MAX	40,000	64	最大許可サイズの AAA ユーザ名
アラート フィールド			
FW_HALFOPEN_CNT	35,012	4	ハーフオープンセッションエントリ数
FW_BLACKOUT_SECS	35,004	4	宛先がブラックアウトしていたか、または利用不可であった時間（秒単位）
FW_HALFOPEN_HIGH	35,005	4	1 分間ログに記録される TCP ハーフオープンセッションエントリの設定済み最大レート
FW_HALFOPEN_RATE	35,006	4	1 分間ログに記録される TCP ハーフオープンセッションエントリの現在のレート
FW_MAX_SESSIONS	35,008	4	このゾーン ペアまたはクラス ID に許可されたセッションの最大数

フィールド ID	タイプ	長さ	説明
その他			
FW_ZONEPAIR_ID	35,007	4	ゾーン ペア ID
FW_CLASS_ID	51	4	クラス ID
FW_ZONEPAIR_NAME	35,009	64	ゾーン ペアの名前
FW_CLASS_NAME	100	64	クラス名
FW_EXT_EVENT_DESC	35,010	64	拡張イベントの説明
FW_SUMMARY_PKT_CNT	35,011	4	ドロップ/通過サマリー レコードで表されるパケット数
FW_EVENT_LEVEL	33003	1	記録されたイベントのレベルの定義 • 0x01：ボックス単位 • 0x02：VRF • 0x03：ゾーン • 0x04：クラス マップ • 他の値は未定義
FW_EVENT_LEVEL_ID	33,004	4	FW_EVENT_LEVEL フィールドの識別子の定義 • FW_EVENT_LEVEL が 0x02（VRF）の場合、このフィールドは VRF_ID を表します。 • FW_EVENT_LEVEL が 0x03（ゾーン）の場合、このフィールドは ZONE_ID を表します。 • FW_EVENT_LEVEL が 0x04（クラス マップ）の場合、このフィールドは CLASS_ID を表します。 • その他の場合、フィールド ID は 0（ゼロ）になります。FW_EVENT_LEVEL が存在しない場合、このフィールドの値はゼロである必要があります。

フィールド ID	タイプ	長さ	説明
FW_CONFIGURED_VALUE	33,005	4	設定されたハーフオープン、アグレッシブエージング、およびイベントレートモニタリング制限を表す値です。このフィールド値の解釈は、関連する FW_EXT_EVENT フィールドによって決まります。
FW_ERM_EXT_EVENT	33,006	2	拡張イベント レート モニタリング コード
FW_ERM_EXT_EVENT_DESC	33,007	N（文字列）	拡張イベント レート モニタリング イベントの説明文字列

1 インターネット制御メッセージ プロトコル（ICMP）
2 簡易ネットワーク管理プロトコル
3 仮想ルーティングおよび転送
4 協定世界時
5 認証、許可、アカウンティング

ファイアウォール拡張イベント

ファイアウォール拡張イベントのイベント名は、ファイアウォール拡張イベント値をイベント ID にマッピングします。 イベント名オプション レコードを使用して、イベント値とイベント ID 間のマッピングを取得します。

拡張イベントは、通常のファイアウォール イベント（inspect、pass、または drop）の一部ではありません。

次の表で、Cisco IOS XE Release 3.8S 以前のリリースに適用可能なファイアウォール拡張イベントについて説明します。

表 *36*：*Cisco IOS XE Release 3.9S* よりも前のリリースのファイアウォール拡張イベントおよびイベントの説明

値	イベント ID	説明
0	FW_EXT_LOG_NONE	特定の拡張イベントはありません。
1	FW_EXT_ALERT_UNBLOCK_HOST	指定したホストへの新規 TCP 接続試行がブロックされなくなります。
2	FW_EXT_ALERT_HOST_TCP_ALERT_ON	ハーフオープン TCP 接続の最大不完全ホスト制限を超えました。

値	イベント ID	説明
3	FW_EXT_ALERT_BLOCK_HOST	指定したホストへの以降のすべての新しい TCP 接続試行は拒否されます。これは、ハーフオープン TCP 接続の最大不完全ホストしきい値を超えており、かつ以降の新しい接続をブロックするようにブロッキング オプションが設定されているためです。
4	FW_EXT_SESS_RATE_ALERT_ON	ハーフオープン接続の最大不完全上限しきい値を超えたか、または新しい接続開始レートを超えました。
5	FW_EXT_SESS_RATE_ALERT_OFF	ハーフオープン TCP 接続数が、最大不完全下限しきい値を下回っているか、または新しい接続開始レートが最大不完全下限しきい値を下回りました。
6	FW_EXT_RESET	接続をリセットします。
7	FW_EXT_DROP	接続をドロップします。
10	FW_EXT_L4_NO_NEW_SESSION	新しいセッションは許可されません。
12	FW_EXT_L4_INVALID_SEG	無効な TCP セグメント。
13	FW_EXT_L4_INVALID_SEQ	無効な TCP シーケンス番号。
14	FW_EXT_L4_INVALID_ACK	無効な TCP 確認応答（ACK）。
15	FW_EXT_L4_INVALID_FLAGS	無効な TCP フラグ。
16	FW_EXT_L4_INVALID_CHKSM	無効な TCP チェックサム。
18	FW_EXT_L4_INVALID_WINDOW_SCALE	無効な TCP ウィンドウ スケール。
19	FW_EXT_L4_INVALID_TCP_OPTIONS	無効な TCP オプション。
20	FW_EXT_L4_INVALID_HDR	無効なレイヤ 4 ヘッダー。
21	FW_EXT_L4_OOO_INVALID_SEG	OoO [6] 無効セグメント。
24	FW_EXT_L4_SYNFLOOD_DROP	同期（SYN）フラッドパケットはドロップされます。

値	イベント ID	説明
25	FW_EXT_L4_SCB_CLOSED	セッションは、パケットを受信する一方で、閉じます。
26	FW_EXT_L4_INTERNAL_ERR	ファイアウォールの内部エラーです。
27	FW_EXT_L4_OOO_SEG	OoO セグメント。
28	FW_EXT_L4_RETRANS_INVALID_FLAGS	無効な再送信されたパケット。
29	FW_EXT_L4_SYN_IN_WIN	無効な SYN フラグ。
30	FW_EXT_L4_RST_IN_WIN	無効なリセット（RST）フラグ。
31	FW_EXT_L4_STRAY_SEG	遊離 TCP セグメント。
32	FW_EXT_L4_RST_TO_RESP	応答側へのリセットメッセージの送信。
33	FW_EXT_L4_CLOSE_SCB	セッションの終了。
34	FW_EXT_L4_ICMP_INVAL_RET	無効な ICMP [7] パケット。
37	FW_EXT_L4_MAX_HALFSESSION	最大ハーフオープン セッション制限を超えました。
38	FW_EXT_NO_RESOURCE	リソース（メモリ）は使用できません。
40	FW_EXT_INVALID_ZONE	無効なゾーン。
41	FW_EXT_NO_ZONE_PAIR	ゾーン ペアは使用できません。
42	FW_EXT_NO_TRAFFIC_ALLOWED	トラフィックは許可されません。
43	FW_EXT_FRAGMENT	パケット フラグメントはドロップされます。
44	FW_EXT_PAM_DROP	PAM [8] アクションはドロップされます。

値	イベント ID	説明
45	FW_EXT_NOT_INITIATOR	セッション開始パケットではありません。 次のいずれかの理由により発生します。 • プロトコルが TCP の場合、最初のパケットが SYN パケットではない。 • プロトコルが ICMP の場合、最初のパケットがエコーまたはタイムスタンプ パケットではない。
48	FW_EXT_ICMP_ERROR_PKTS_BURST	ICMP エラー パケットがバースト モードになりました。バーストモードでは、パケットは、応答側インターフェイスからの応答を待機しないで繰り返し送信されます。
49	FW_EXT_ICMP_ERROR_MULTIPLE_UNREACH	「宛先到達不能」タイプの複数の ICMP エラーを受信しました。
50	FW_EXT_ICMP_ERROR_L4_INVALID_SEQ	ICMP エラー メッセージに埋め込まれたパケットに無効なシーケンス番号があります。
51	FW_EXT_ICMP_ERROR_L4_INVALID_ACK	ICMP エラー メッセージに埋め込まれたパケットに無効な確認応答（ACK）番号があります。
52	FW_EXT_MAX	未使用。

6 順序外
7 インターネット制御メッセージ プロトコル（ICMP）
8 ポートツーアプリケーション マッピング

ファイアウォール高速ロギングの設定方法

グローバル パラメータ マップの高速ロギングのイネーブル化

デフォルトでは、高速ロギング（HSL）はイネーブルではなく、ファイアウォールのログはルート プロセッサ（RP）またはコンソールのロガー バッファに送信されます。 HSL をイネーブルに

すると、ログは装置外の高速ログ収集装置に送信されます。パラメータマップは、ファイアウォールに到達するトラフィックに対するアクションを実行する手段を提供し、グローバル パラメータマップは、ファイアウォール セッション テーブル全体に適用されます。 グローバル パラメータマップの高速ロギングをイネーブルにするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**
4. **log dropped-packets**
5. **log flow-export v9 udp destination** *ip-address port-number*
6. **log flow-export template timeout-rate** *seconds*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect global** 例： `Device(config)# parameter-map type inspect global`	グローバル パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**log dropped-packets** 例： `Device(config-profile)# log dropped-packets`	ドロップされたパケットのロギングをイネーブルにします。
ステップ 5	**log flow-export v9 udp destination** *ip-address port-number* 例： `Device(config-profile)# log flow-export v9 udp destination 10.0.2.0 5000`	NetFlow イベント ロギングをイネーブルにし、ログ コレクタの IP アドレスとポート番号を提供します。

	コマンドまたはアクション	目的
ステップ 6	**log flow-export template timeout-rate** *seconds* 例： `Device(config-profile) log flow-export template timeout-rate 5000`	テンプレートのタイムアウト値を指定します。
ステップ 7	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ファイアウォール アクションの高速ロギングのイネーブル化

検査タイプパラメータマップを設定している場合は、この作業を実行して高速ロギングをイネーブルにします。パラメータマップはファイアウォールの検査動作を指定し、ファイアウォールの検査パラメータ マップは検査タイプとして設定されています。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** *parameter-map-name*
4. **audit-trail on**
5. **alert on**
6. **one-minute** {**low** *number-of-connections* | **high** *number-of-connections*}
7. **tcp max-incomplete host** *threshold*
8. **exit**
9. **policy-map type inspect** *policy-map-name*
10. **class type inspect** *class-map-name*
11. **inspect** *parameter-map-name*
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect parameter-map-hsl`	接続しきい値、タイムアウト、および **inspect** キーワードに関連するその他のパラメータの検査パラメータ マップを設定し、パラメータ マップ タイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**audit-trail on** 例： `Device(config-profile)# audit-trail on`	監査証跡メッセージをイネーブルにします。 • パラメータ マップに対する監査証跡をイネーブルにして、接続またはセッションの開始、停止、期間や、送信元と宛先の IP アドレスを記録することができます。
ステップ 5	**alert on** 例： `Device(config-profile)# alert on`	コンソールに表示されるステートフル パケット インスペクション アラート メッセージをイネーブルにします。
ステップ 6	**one-minute** {**low** *number-of-connections* | **high** *number-of-connections*} 例： `Device(config-profile)# one-minute high 10000`	システムによるハーフオープン セッションの削除の開始と停止を起動する新規の未確立セッションの数を定義します。
ステップ 7	**tcp max-incomplete host** *threshold* 例： `Device(config-profile)# tcp max-incomplete host 100`	TCP ホスト固有のサービス拒否（DoS）の検出および回避のために、しきい値とブロックする時間値を指定します。
ステップ 8	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 9	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect policy-map-hsl`	検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect class-map-tcp`	アクションを実行する対象のトラフィック クラスを指定し、ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 11	**inspect** *parameter-map-name* 例： `Device(config-pmap-c)# inspect parameter-map-hsl`	（任意）ステートフルパケットインスペクションをイネーブルにします。
ステップ 12	**end** 例： `Device(config-pmap-c)# end`	ポリシー マップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ファイアウォール高速ロギングの設定例

例：グローバル パラメータ マップの高速ロギングのイネーブル化

次に、ドロップされたパケットのロギングをイネーブルにし、エラー メッセージを NetFlow バージョン 9 フォーマットで外部 IP アドレスに記録する例を示します。

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# log dropped-packets
Device(config-profile)# log flow-export v9 udp destination 10.0.2.0 5000
Device(config-profile)# log flow-export template timeout-rate 5000
Device(config-profile)# end
```

例：ファイアウォール アクションの高速ロギングのイネーブル化

次に、検査タイプ パラメータ マップ parameter-map-hsl に高速ロギング（HSL）を設定する例を示します。

```
Device# configure terminal
Device(config)# parameter-map type inspect parameter-map-hsl
Device(config-profile)# audit trail on
Device(config-profile)# alert on
Device(config-profile)# one-minute high 10000
Device(config-profile)# tcp max-incomplete host 100
Device(config-profile)# exit
Device(config)# poliy-map type inspect policy-map-hsl
Device(config-pmap)# class type inspect class-map-tcp
Device(config-pmap-c)# inspect parameter-map-hsl
Device(config-pmap-c)# end
```

ファイアウォール高速ロギングの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ファイアウォール高速ロギングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *37*：ファイアウォール高速ロギングの機能情報

機能名	リリース	機能情報
ファイアウォール高速ロギング	Cisco IOS XE Release 2.1	ファイアウォール高速ロギング サポート機能は、エクスポート フォーマットとして NetFlow バージョン 9 を使用するファイアウォール HSL に対するサポートを導入します。 次のコマンドが導入または変更されました。**log dropped-packet**、**log flow-export v9 udp destination**、**log flow-export template timeout-rate**、**parameter-map type inspect global**。