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 ファイアウォールが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。

（注） Cisco IOS XE は、ゾーンベース ファイアウォール設定上で Virtual Fragmentation Reassembly（VFR）をサポートします。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有効にすると、VFR は同じインターフェイス上で自動的に設定されます。

ゾーンベース ポリシー ファイアウォールに関する機能情報

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 ファイアウォールに関する機能情報

機能名	リリース	機能情報
ゾーンベース ファイアウォールの再分類	Cisco IOS XE Bengaluru 17.6.1	ゾーンベース ファイアウォールの再分類機能が導入されました。この機能は、既存のセッションでポリシー設定に変更がある場合に、その変更を適用します。
ASR1000 上のゾーンベース ファイアウォールに対するスマートライセンスサポート	Cisco IOS XE Denali 16.3.1	**show license all** コマンドが変更されました。
ゾーンベース ポリシー ファイアウォールでの Out-of-Order パケット処理	Cisco IOS XE リリース 3.5S	Out-of-Order パケット処理機能は、セッションに DPI が必要ない場合に、OoO パケットのルータの通過を許可し、宛先への到達を可能にします。OoO パケットが含まれるすべてのレイヤ 4 トラフィックに、宛先へのパス スルーが許可されます。ただし、セッションでレイヤ 7 インスペクションが必要な場合は、OoO パケットがドロップされます。
IOS-XE ZBFW と暗号 VPN の相互運用	Cisco IOS XE リリース 3.17S	IOS-XE ZBFW と暗号 VPN の相互運用機能は、FlexVPN DVTI 上でのゾーンベース ファイアウォールの有効化をサポートします。
マルチパス TCP のゾーンベース ファイアウォール サポート	Cisco IOS XE リリース 3.13S	マルチポイント TCP は、ゾーンベース ファイアウォール レイヤ 4 インスペクションとシームレスに連動します。マルチポイント TCP は、アプリケーション レイヤ ゲートウェイ（ALG）とアプリケーション インスペクションおよびコントロール（AIC）とは連動しません。
Firewall：NetMeeting Directory (LDAP) ALG サポート	Cisco IOS XE Release 3.1S	LDAP は、ディレクトリ サービスに保存されている情報の照会および更新に使用されるアプリケーション プロトコルです。ファイアウォール - Netmeeting（LDAP）Directory ALG サポート機能は、Cisco ファイアウォールでレイヤ 4 LDAP インスペクションをデフォルトでサポートできるようにします。 次のコマンドが導入されました。**match protocol**
ゾーンベース ファイアウォールでのデバッグ可能性強化（フェーズ II）	Cisco IOS XE Release 3.10S	デバッグ可能性強化ゾーンベースファイアウォール機能は、デバッグログのシビラティ（重大度）レベルを提供します。

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 - デフォルト ゾーン	Cisco IOS リリース 2.6	ゾーンベース ファイアウォール - デフォルト ゾーン機能は、ゾーンとデフォルト ゾーンを構成するゾーン ペアでファイアウォール ポリシーを設定可能にするデフォルト ゾーンを導入します。明示的なゾーンメンバーシップのないインターフェイスがデフォルトゾーンに属します。
ゾーンベースポリシーファイアウォール	Cisco IOS リリース 2.1	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のグループ間に Cisco IOS XE ソフトウェアの単方向ファイアウォール ポリシーを提供します。

ゾーンベース ポリシー ファイアウォールについて

以下のセクションでは、ゾーンベースポリシーファイアウォールについて詳しく説明します。

トップレベル 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。これを実現するには、**match access-group** コマンドおよび **match protocol** コマンドを使用します。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**、および **pass** コマンドを使用して、ハイレベルのアクションを定義できます。ポリシー マップは、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。

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。ゾーンを利用して、Cisco IOS XE ファイアウォールをどこに適用するかを指定できます。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。そのため、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の制約を受けず、自由にゾーンを通過できます。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。

ダイナミックマルチポイントVPN（DMVPN）トンネルの場合、ゾーンベース ファイアウォールは、内部パケットを検査し、評価のみを行います。内部パケットがGeneric Routing Encapsulation（GRE）およびカプセル化セキュリティペイロード（ESP）ペイロードにカプセル化されると、それ以上の検査なしで転送されます。着信パケットの場合、ZBF 評価の前に ESP と GRE のカプセル化が解除されます。セルフから外部または外部からセルフのゾーンペアでのESPおよびGRE トラフィックに関する明示的なルールを設定する必要はありません。

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にあるインターフェイスの間を通るすべてのトラフィック（デバイスに送信されるか、デバイスによって開始された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および別のインターフェイスに対する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。ポリシーがinspectまたはpassアクションによってトラフィックを許可する場合、トラフィックはインターフェイスを通過できます。

ゾーンを設定するときに考慮する基本的な規則を次に示します。

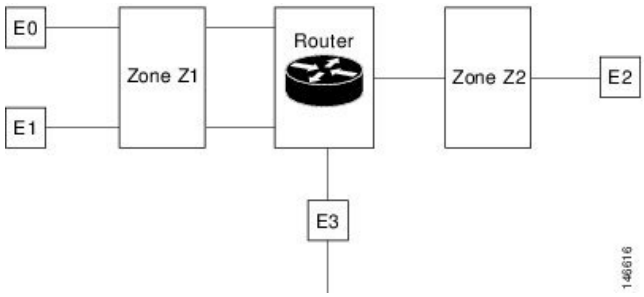
- ゾーンインターフェイスからゾーン外のインターフェイスへのトラフィックまたはゾーン外のインターフェイスからゾーンインターフェイスへのトラフィックは常にドロップされます。ただし、デフォルトゾーンが有効でないことが条件です（デフォルトゾーンはゾーン外のインターフェイスです）。
- 2 つのゾーンインターフェイス間のトラフィックは、各ゾーンにゾーンペアの関係があるかどうか、およびそのゾーンペアにポリシーが設定されているかどうかが検査されます。
- デフォルトでは、同一ゾーン内の2つのインターフェイス間のすべてのトラフィックは常に許可されます。
- ゾーンペアは、ゾーンを送信元ゾーンおよび宛先ゾーン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、2 つのゾーン間のトラフィックを検査、転送、またはドロップできます。
- 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。
- トラフィックがデバイスのすべてのインターフェイス間を通過するようにするには、これらのインターフェイスが1つのセキュリティゾーンまたは別のセキュリティゾーンのメンバーである必要があります。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。
- ゾーンに関連付けられたすべてのインターフェイスは、同じ仮想ルーティングおよび転送（VRF）に含まれている必要があります。

図 1 には、次のことが示されています。

- 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



- ゾーン ペアとポリシーは、同じゾーンで設定されます。インターフェイス E0 と E1 は同じセキュリティ ゾーン（Z1）のメンバーなので、2つのインターフェイス間のトラフィックは自由に流れます。
- 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 の間、E1 と E2 の間、E3 と E1 の間、E3 と E2 の間など）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有効になっていないかぎり、E3 と E0、E1、または E2 の間でトラフィックは流れません。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、ファイアウォールは最大 4000 のゾーンをサポートします。

セキュリティ ゾーン ファイアウォール ポリシー

クラスは、一連のパケットをその内容に基づいて識別します。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。

アクションは、通常はトラフィック クラスに関連付けられる機能です。ファイアウォールは、次のタイプのアクションをサポートしています。

inspect：分類されると、ファイアウォールセッションが接続テーブルに作成され、パケットの内容が検査されます。

pass：パケットが分類され、トラフィックは、それ以上の検査なしでシステムを通過できます。

drop：パケットが分類されてドロップされます。

セキュリティ ゾーン 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。

- 一致基準の定義（クラス マップ）。
- 一致基準とアクションの関連付け（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 コマンドは、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、または修正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が定義されているクラスのポリシーを設定します。

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が RADIUS サーバーから取得され、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** コマンドは、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。

LNS の加入者単位のファイアウォール機能の詳細については、『Release Notes for Cisco ASR 1000 Series Aggregation Services Routers for Cisco IOS XE Release 2』を参照してください。

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で指定されます。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 ゾーンまたはセルフ ゾーンを送信元ゾーンと宛先ゾーンのどちらかとして選択することができます。セルフゾーンは、メンバーとしてインターフェイスを何も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、デバイス宛て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。デバイスを通過するトラフィックには適用されません。

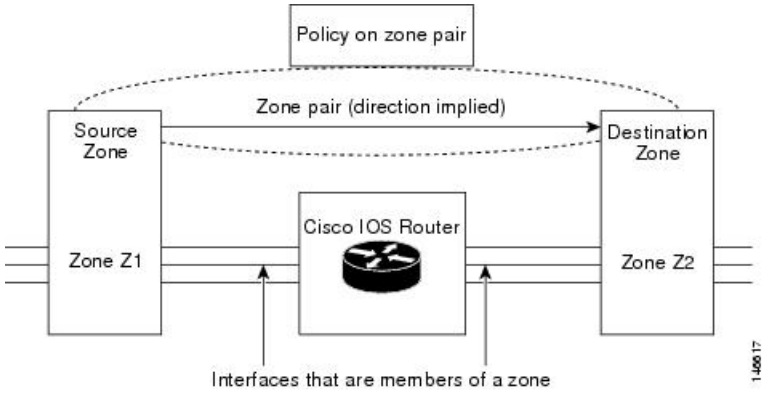
デフォルトゾーンは、セキュリティゾーンが関連付けられていないインターフェイスに適用されます。デフォルトゾーンは、デフォルトでは有効になっていません。デフォルトゾーンを有効にするには、**zone security default** コンフィギュレーション コマンドを使用します。

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。そのため、少なくとも 2 つのゾーンが必要になります。デバイスとの間のトラフィックの場合、ZBF はセルフゾーンの概念をサポートします。

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の間のトラフィックを許可（検査または転送）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アタッチするには、**service-policy type inspect** コマンドを使用します。

次の図は、ゾーン Z1 からゾーン Z2 に流れ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ています。ここでは、トラフィックの入力インターフェイスはゾーン Z1 のメンバー、出力インターフェイスはゾーン Z2 のメンバーです。

図 *2:* ゾーン ペア



2 つのゾーンがあるため、両方向（Z1 から Z2 および Z2 から Z1）のトラフィックにポリシーが必要になる場合があります。トラフィックがいずれかの方向から開始される場合は、2 つのゾーンペアを設定する必要があります。

ゾーン ペア間でポリシーが設定されていない場合は、トラフィックがドロップされます。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、リターン トラフィックは許可されません。サービスポリシーでイニシエータ方向のトラフィックが検査され、リターントラフィック用のゾーンペアとサービスポリシーが存在しない場合は、リターントラフィックが検査されます。

サービス ポリシーで順方向のトラフィックが許可され、リターン トラフィック用のゾーン ペアとサービス ポリシーが存在しない場合は、リターン トラフィックがドロップされます。どちらの場合も、リターン トラフィックを許可するようにゾーン ペアとサービス ポリシーを設定する必要があります。図 2 では、Z2 から Z1 へのリターントラフィックを許可するようにゾーンペアの送信元と宛先を設定する必要はありません。Z1 から Z2 へのゾーンペアに対するサービスポリシーがその役割を果たします。pass アクションの場合は各方向のパケットに対するポリシーが存在する必要があり、inspect アクションの場合はイニシエータからのトラフィックに対するポリシーが存在する必要があります。

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 ファイアウォールの場合は、内部ゾーンと外部ゾーン間を流れるトラフィックによって、ゾーン内で生成される断続的な Internet Control Message Protocol（ICMP）応答を処理するときの動作が異なります。

Internet Control Message Protocol（ICMP）エラーパケットにはポリシーは必要ありません。

（注） ポリシーは、イニシエータから着信するパケットの ICMP_ECHO（ping）などの ICMP 情報メッセージに対して必要です。

セルフゾーンを送信元とするゾーンペア、および内部ゾーンと外部ゾーン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、ICMP_EHCO_REQUEST などの情報 ICMP パケットが生成された場合、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。

ゾーンとインスペクション

ゾーンベース ポリシー ファイアウォールは、ファイアウォール ポリシーに照らして、入力インターフェイスと出力インターフェイスから送信元ゾーンと宛先ゾーンを検査します。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。検査アクションを伴うトラフィックは、ファイアウォールテーブル内に接続を構築し、状態チェックの対象になります。通過アクションを伴うトラフィックは、ゾーン ファイアウォールを完全にバイパスして、どのセッションも作成しません。ファイアウォール接続が作成されると、パケットは分類されなくなります。つまり、ポリシーマップが変更されると、基盤となる接続が

認識されなくなります。接続が確立されないため、逆方向のパケットに対するpassアクションを使用して、ミラーリングされたポリシーを作成する必要があります。

TCP しきい値やタイムアウトなどの inspect パラメータをフローあたりで設定することもできます。

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制御リスト（ACL）は、ファイアウォールポリシーがゾーンペアに適用される前に処理されます。送信元ゾーンと宛先ゾーンの間にポリシーが適用されている場合は、そのインターフェイス ACL がポリシー ファイアウォール トラフィックと干渉していないことを確認する必要があります。クラスマップにアクセスリストだけが含まれていて、照合プロトコルが含まれていない場合、ファイアウォールは、フロープロトコルを既知のアプリケーションレベル ゲートウェイ（ALG）と照合し、必要に応じて処理しようとします。

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制御アクセスを許可するファイアウォール経由で開かれるポート）は、インターフェイス ACL 内のリターントラフィックに対して開かれません。

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 マップのタイプは inspect であり、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、pass、および 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。

次に、ACL 101 と HTTP プロトコルの一致基準を含むクラスマップ c1 を設定する例を示します。このコマンドにより、パケットが c1 でトラフィックの一部としてドロップされることを指定する、p1 という名前の検査ポリシーマップも作成されます。

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

```
Device(config-pmap-c)# drop
```

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、ファイアウォールが最大 1000 のポリシーマップをサポートし、ポリシーマップあたり 8 のクラスをサポートします。設定できるマッチング ステートメントは、クラス マップごとに最大 16、全体では 1000 です。

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 マップの例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、最初に **match protocol http** コマンドが HTTP トラフィックに適用されます。match 行が逆になっており、**match protocol http** コマンドの前に **match protocol tcp** コマンドがトラフィックに適用されると、そのトラフィックは 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 が最初に設定されると、FTP や TFTP などのサービスの問題や、H.323、Real Time Streaming Protocol（RTSP）、Session Initiation Protocol（SIP）、Skinny Client Control Protocol（SCCP）などのマルチメディアおよび音声シグナリングサービスの問題が発生します。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。

（注） TCP トラフィックフローのウィンドウサイズが 65k を超えないように、デバイスでゾーンベース ファイアウォールを設定します。

class-default クラス マップ

ユーザー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、ポリシーのユーザー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。

どのユーザ定義クラスにも一致しないパケットのグループに対する明示的な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 に対して設定できるアクションは drop と pass だけです。

次の例は、ポリシーマップで class-default クラス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 クラス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-cmap)# exit
Device(config)# policy-map type inspect p1
Device(config-pmap)# class type inspect c1
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# drop
```

レイヤ 3 とレイヤ 4 のサポートされるプロトコル

次のプロトコルがサポートされています。

- FTP
- H.323
- リアルタイム ストリーミング プロトコル（RTSP）
- Skinny Client Control Protocol（SCCP）
- Session Initiation Protocol（SIP）
- Trivial File Transfer Protocol（TFTP）
- ルート収束モニタリングおよび診断（RCMD）
- Lightweight Directory Access Protocol（LDAP）
- HTTP
- ドメイン ネーム システム（DNS）
- Simple Mail Transfer Protocol（SMTP/ESMTP）
- Post Office Protocol 3（POP3）
- Internet Mail Access Protocol（IMAP）
- SUN リモートプロシージャコール（SUNRPC）
- GPRS トンネル プロトコル バージョン 0/1（GTPv1）
- GPRS トンネル プロトコル バージョン 2（GTPv2）
- ポイントツーポイント トンネリング プロトコル（PPTP）

アクセス コントロール リストとクラス マップ

アクセス リストは、パケット分類メカニズムです。アクセスリストでは、ACL が特定のクラスマップに適用されたときに許可または拒否される実際のネットワークトラフィックを定義します。つまり、ACLは、パケットに適用される許可および拒否条件を順番に集めたものです。

ルータは、一度に 1 つずつ ACL の条件に基づいてパケットをテストします。拒否条件は「一致しない」と解釈されます。拒否アクセス制御エントリ（ACE）と一致するパケットの場合、ACL 処理が終了し、クラス内の次の match ステートメントが調べられます。

（注） ACL の変数の範囲をクラスマップの一致基準として設定できます。ファイアウォールでは 5 タプル一致基準だけがサポートされているため、サポートされている一致基準は送信元アドレス、送信元ポート、宛先アドレス、宛先ポート、およびプロトコルだけです。CLI で設定および受け入れられるその他のすべての一致基準は、ファイアウォールではサポートされていません。

クラスマップは、次の基準に基づいて、ACL の一連の変数を照合するために使用されます。

- クラス マップが許可条件または拒否条件に一致しない場合、ACL は失敗します。
- match-all または match-any 条件は、クラスマップ内に含まれる match ステートメントに適用されます。ACL は通常どおりに処理され、その結果が、match-all または match-any と比較するときに使用されます。
- match-all 属性が指定され、どの一致条件、ACL、またはプロトコルもパケットと一致しない場合、現在のクラスの評価はその時点で停止され、ポリシーの次のクラスが調べられます。
- match-any 属性でいずれかの match が成功した場合、class-map 基準が満たされ、ポリシーで定義されたアクションが実行されます。
- ACL が match-any 属性と一致した場合、ファイアウォールは宛先ポートに基づいてレイヤ 7 プロトコルの確認を試みます。

クラスマップで match-all 属性を指定した場合、レイヤ 4 の一致基準（ICMP、TCP、UDP）は設定されますが、レイヤ 7 の一致基準は設定されません。したがって、レイヤ 4 インスペクションが実行され、レイヤ 7 インスペクションは省略されます。

アクセスリストには、「標準アクセスリスト」と「拡張アクセスリスト」という異なる形式があります。標準アクセス リストでは、IP アドレスまたは IP アドレスの範囲を許可または拒否するように定義します。拡張アクセス リストでは、送信元と宛先両方の IP アドレスまたは IP アドレス範囲を定義します。拡張アクセス リストは、パケットの ICMP、TCP、および UDP プロトコルタイプと宛先ポート番号に基づいて、パケットの許可または拒否を定義することもできます。

次に、IP アドレス 10.2.3.4 から受信したパケットを、クラス test1 と照合する例を示します。この例では、アクセス リスト 102 が拒否条件と一致し、アクセス リストの他のエントリの処理を停止します。クラスマップは match all 属性で指定されているため、クラスマップ test1 の照合は失敗します。ただし、このクラスマップがクラスマップ test1 にリストされているプロトコルのいずれかと一致するかどうかが検査されます。

クラスマップ test1 が match-all ではなく match-any 属性を使用していた場合は、ACL は拒否と一致して失敗しますが、HTTP プロトコルと一致し、pmap1 を使用した検査が実行されます。

```
access-list 102 deny ip 10.2.3.4 0.0.0.0 any
access-list 102 permit any any
class-map type inspect match-all test1
 match access-list 102
 match protocol http
!
class-map type inspect match-any test2
 match protocol sip
 match protocol ftp
 match protocol http
!
parameter-map type inspect pmap1
 tcp idle-time 15
!
parameter-map type inspect pmap2
 udp idle-time 3600
!
policy-map type inspect test
 class type inspect test1
  inspect pmap1
!
 class type inspect test2
  inspect pmap2
!
 class type inspect class-default
  drop log
```

階層型ポリシー マップ

ポリシーを別のポリシー内にネストできます。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、1 つの子ポリシーと 1 つの親ポリシーが含まれています。子ポリシーは、以前定義したポリシーであり、**service-policy** コマンドを使用して新しいポリシーに関連付けられています。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。

たとえば、マーケティングとエンジニアリングの2つのアクセスリストを定義します。2 つのアクセスグループのいずれかと一致するクラスマップを作成します。その後、match-all 条件を持つ前のクラスマップを含み、プロトコル HTTP と一致する、別のクラスマップを作成します。

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 2 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、すべてのマップに適用されます。上位レベルと下位レベルの両方でパラメータが指定されている場合、下位レベルのパラメータが優先されます。
- 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必要なパラメータマップです。

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（通常、2 つのネットワークを接続するもの）で動作し、パケットを別のネットワークに転送する前に、社内ネットワークの（グローバルに一意のアドレスではなく）プライベートアドレスを正規のアドレスに変換します。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、内部ネットワークと外部ネットワークのそれぞれに接続するインターフェイスが少なくとも 1 つずつあります。

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で一意の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際は、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、パケットに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、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、ホストのアドレスは 1 つのアドレス空間に含まれます。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 209.168.1.1 および宛先アドレス 10.1.1.1 を使用して内部 NAT 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、外部 NAT から応答が返されると、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 209.168.1.1 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（内部ローカルアドレスおよび外部グローバルアドレス）209.168.1.1 と 209.165.200.224 を使用する必要があります。一般に、外部グローバルアドレスのマッピングは推奨されません。

Cisco ファイアウォールに対する WAAS サポート

リリースによっては、Wide Area Application Services（WAAS）ファイアウォール ソフトウェアが、セキュリティ対応 WAN およびアプリケーション アクセラレーション ソリューションを最適化する統合型ファイアウォールに次のようなメリットを提供します。

- WAAS ネットワークを透過的に統合します。
- 透過的な WAN 加速化トラフィックを保護します。
- フル ステートフル インスペクション機能を通して WAN を最適化します。
- Payment Card Industry（PCI）コンプライアンスを簡略化します。
- Network Management Equipment-Wide Area Application Engine（NME-WAE）モジュールまたはスタンドアロン WAAS デバイス展開をサポートします。

WAAS は、初期の 3 方向ハンドシェイク中に TCP オプションを使用して WAE デバイスを透過的に識別する自動検出メカニズムを備えています。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 は、Cisco ファイアウォールで、内部ファイアウォール TCP 状態変数を含む 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することによって、最適化されたトラフィックを自動的に検出できるようにします。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 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、最適化されていないトラフィックに対しても実行できます。

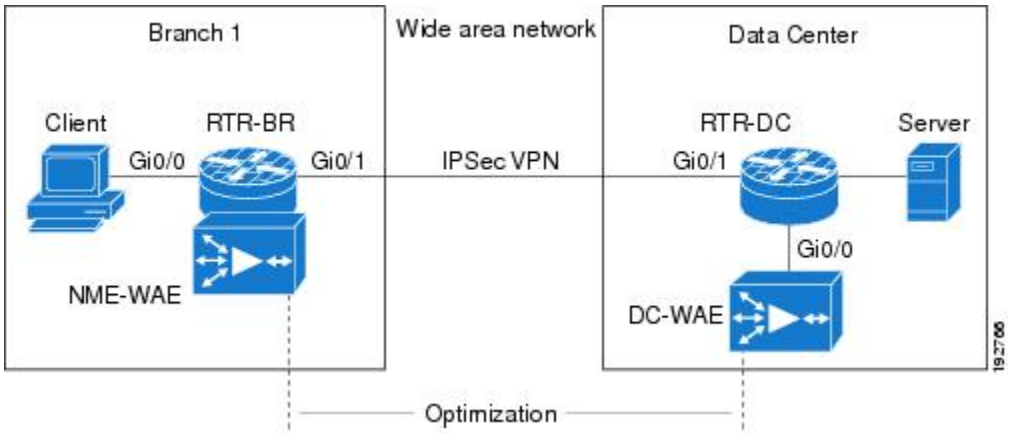
WAAS トラフィック フロー最適化展開シナリオ

ここでは、ブランチ オフィス展開に関する 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 フロー最適化は、Cisco サービス統合型ルータ（ISR）上の Cisco ファイアウォール機能と連動します。ZBF は、WAAS がパケットの最適化を解除した後に、クリアテキストを検査します。

次の図に、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ます。この特定の展開では、NME-WAE が Cisco ファイアウォールと同じデ

バイスに展開されます。Web Cache Communication Protocol（WCCP）が代行受信用にトラフィックをリダイレクトするために使用されます。

図 *3:* エンドツーエンドの *WAAS* 最適化パス

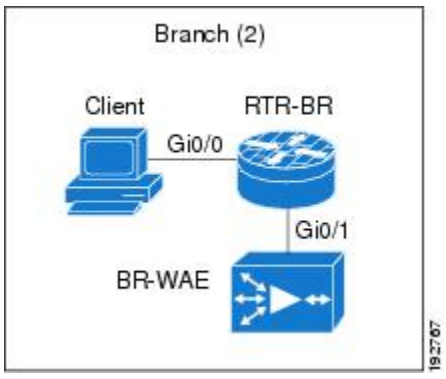


オフパス デバイスを使用した WAAS ブランチ展開

このセクションにある Wide Area Application Services（WAAS）ブランチ展開の図のように、WAE デバイスは、スタンドアロン WAE デバイスにすることも、ISR に統合型サービスエンジンとしてインストールされた NME-WAE デバイスにすることもできます。

次の図は、トラフィックの代行受信のために、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 支店の展開例です。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。

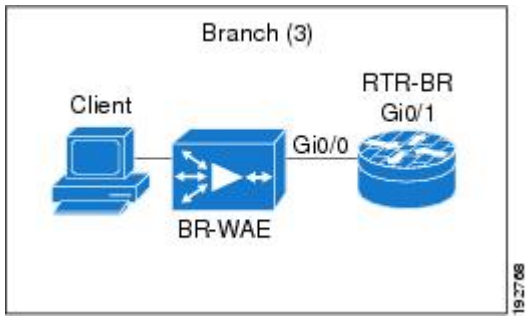
図 *4:* *WAAS* オフパス ブランチ展開



インライン デバイスを使用した WAAS ブランチ展開

次の図に、インライン WAE デバイスがサービス統合型ルータ（ISR）の前に配置された WAAS ブランチ展開を示します。WAE デバイスがデバイスの前に配置されているため、Cisco ファイアウォールが WAAS 最適化パケットを受信し、結果的に、クライアント側のレイヤ 7 インスペクションがサポートされません。

図 *5 : WAAS* インライン パス ブランチ展開



Cisco ファイアウォールを使用したエッジ WAAS デバイスを、WAN 接続との間で転送されるトラフィックを検査する必要があるブランチ オフィス サイトで使用します。Cisco ファイアウォールは、トラフィックで最適化インジケータ（TCP オプションと後続の TCP シーケンス番号の変更）をモニターして、最適化されたトラフィックが通過できるようにします。一方、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適用し、セキュリティを確保することで、WAAS最適化のメリットを享受します。

（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最適化に直接関与しませんが、最適化インジケータが存在する場合は、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アクティビティを考慮に入れるために、WAAS最適化がトラフィックに適用されていることを認識している必要があります。

ゾーンベースファイアウォールでのOut-of-Orderパケット処理のサポート

デフォルトでは、レイヤ 7 ディープ パケット インスペクションが有効にされている場合、またはレイヤ 7 プロトコルマッチングでレイヤ 4 インスペクションが有効にされている場合、Cisco IOS XE ファイアウォールはすべての Out-of-Order（OoO）パケットをドロップします。Out-of-Order パケットのドロップは（送信者の代わりとなる）再送信タイマーが満了するまで行われないため、Out-of-Order パケットがドロップされると終端アプリケーションで大幅な遅延が発生する可能性があります。レイヤ 7 インスペクションはステートフル パケット インスペクションであり、TCP パケットの順序が正しくなければ機能しません。

Cisco IOS XE リリース 3.5S では、セッションに DPI が必要ない場合、OoO パケットは許可されて、ルータをパス スルーして宛先に到達できます。OoO パケットが含まれるすべてのレイヤ4トラフィックに、宛先へのパス スルーが許可されます。一方、セッションにレイヤ7インスペクションが必要な場合は、やはり OoO パケットはドロップされます。DPI が必要ない場合は OoO パケットをドロップしないようにすることで、ドロップされたパケットを再送信する必要がなくなるため、再送信に必要なネットワーク上の帯域幅が削減されます。

デバッグ メッセージのシビラティ（重大度）

デバッグ メッセージのシビラティ（重大度）により、メッセージが記録される問題のタイプが指定されます。ファイアウォールのデバッグを有効にする場合は、ログに記録するメッセージのレベルを指定できます。次の表に、デバッグ メッセージのシビラティ（重大度）の詳細を示します。

表 *2:* ファイアウォール デバッグ メッセージのシビラティ（重大度）

トレース レベル	シビラティ（重大度）	説明
深刻	1	ゾーンベース ポリシー ファイアウォールが使用できない原因、またはパケットを転送できない原因である問題に適用されます。これはデフォルトです。Critical イベントの例を次に示します。 • ログ メカニズムによりトリガーされたバック プレッシャ。 • リソース制限の超過。 • メモリ割り当ての失敗。 • 新しいセッションを実行できないハイアベイラビリティ状態。
Error	2	すべてのエラー条件とパケット ドロップ条件に適用されます。Error イベントの例を次に示します。 • 同期（SYN）Cookie：最大宛先数に達した。 • イニシエータ パケットではない。 • パケットを送信できなかった。 • アプリケーション レイヤ ゲートウェイ（ALG）のエラー状態。

トレース レベル	シビラティ（重大度）	説明
Information	3	情報メッセージに適用されます。Information イベントの例を次に示します。 • 誤ったポリシー設定、ゾーンチェック失敗、不正なパケット、またはハードコーディングされている制限またはしきい値が原因で発生したパケットドロップ。 • ステート マシン遷移。 • セッションまたは不明確チャネルデータベース情報、検索結果など。 • パケット分類のステータスまたは結果。 • パケット パスまたはパケット ドロップのステータス。 • セッション ヒットまたはセッション ミス。 • 送信されたパケットが TCP リセット（RST）パケットである。 • SYN Cookie イベント。
Detail	4	すべてのログ メッセージを出力します。Detail イベントの例を次に示します。 • データ構造。 • TCAM（Ternary Content Addressable Memory）検索キーと結果構造。 • ファイアウォール イベントの詳細。

ゾーンベース ポリシー ファイアウォールのスマート ライセンスのサポート

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータのゾーンベース ポリシー ファイアウォール機能は、セキュリティパッケージとは別にパッケージ化されているので、ゾーンベースポリシーファイアウォールでは機能を有効または無効にするためのライセンスが必要です。ASR1000 のゾーンベース ファイアウォールのスマートライセンスサポート機能は、Cisco UniversalK9 IOS ソフトウェアイメージにより、Cisco ASR 1000 シリーズアグリゲーション サービス ルータのスマートライセンスを機能レベルで実現します。

この機能を有効にするためにデバイスをリロードする必要はありません。スマート ライセンスは、デフォルトではオンになっていません。スマートラインセンスは、**license smart enable** コマンド、または **zone security** コマンドを使用したゾーンベース ポリシー ファイアウォールの

設定により、グローバルにオンとオフが切り替えられます。スマートライセンスの実装時に **show license all** コマンドを実行すると、スマートライセンスのステータスが表示されます。スマートライセンスがグローバルに有効である場合の **show license all** コマンドの出力例を次に示します。

```
Device# show license all

License Store: Primary License Storage
StoreIndex: 0   Feature: internal_service                 Version: 1.0
        License Type: Evaluation
        License State: Active, In Use
            Evaluation total period: 1  day  0  hour
            Evaluation period left: 18 hours 57 minutes
            Period used: 5  hours 2  minutes
            Expiry date: Mar 18 2016 14:15:02
        License Count: Non-Counted
        License Priority: Low
License Store: Built-In License Storage
StoreIndex: 0   Feature: adventerprise                    Version: 1.0
        License Type: EvalRightToUse
        License State: Active, In Use
            Evaluation total period: 8  weeks 4  days
            Evaluation period left: 8  weeks 3  days
            Period used: 5  hours 13 minutes
            Transition date: May 16 2016 14:03:52
        License Count: Non-Counted
        License Priority: Low          <-- (CSL mode license)

Device(config)# license smart enable
Device(config)# zone security z1
Device(config)# exit
Device# show license all

Smart Licensing Status
----------------------------
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 65 days, 14 hours, 19 minutes, 47 seconds

License Usage
--------------

(ASR_1000_AdvEnterprise):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE

(ASR_1000_firewall):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE

Product Information
----------------------
UDI: PID:ASR1013,SN:NWG165000A9
```

```
Agent Version
---------------
Smart Agent for Licensing: 1.5.1_rel/29
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel5)1.0.3, PK:(dev18)1.0.3
```

次に、スマートライセンスが無効な場合の出力例を示します。

```
Device(config)# no zone security z1
Device(config)# exit
Device# show license all

Smart Licensing Status
----------------------

Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 65 days, 14 hours, 18 minutes, 58 seconds

License Usage
--------------

(ASR_1000_AdvEnterprise):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE

Product Information
--------------------
UDI: PID:ASR1013,SN:NWG165000A9

Agent Version
-------------
Smart Agent for Licensing: 1.5.1_rel/29
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel5)1.0.3, PK:(dev18)1.0.3

Device(config)# no license smart enable
Device(config)# exit
Device# show license all

License Store: Primary License Storage
StoreIndex: 0   Feature: internal_service                 Version: 1.0
        License Type: Evaluation
        License State: Active, Not in Use, EULA accepted
            Evaluation total period: 1  day  0  hour
            Evaluation period left: 18 hours 54 minutes
            Period used: 5  hours 5  minutes
        License Count: Non-Counted
        License Priority: Low
License Store: Built-In License Storage
StoreIndex: 0   Feature: adventerprise                    Version: 1.0
        License Type: EvalRightToUse
        License State: Active, Not in Use, EULA accepted
            Evaluation total period: 8  weeks 4  days
            Evaluation period left: 8  weeks 3  days
            Period used: 5  hours 17 minutes
```

```
License Count: Non-Counted
License Priority: Low                <--- (back to CSL mode)
```

ゾーンベース ファイアウォールの再分類

Cisco IOS XE 17.6.1 以降では、ZBFW セッションの再分類を設定できます。ZBFW 再分類機能により、ポリシー設定の変更が既存のファイアウォールセッションに適用されます。確立されたセッションでセッションイニシエータからパケットを受信すると、特定のフローが再分類されます。

次に、これが発生する可能性のあるいくつかの例を示します。

- クラスマップでフィルタを追加、削除、または編集するには、次の作業を実行します。
  - 一致プロトコルの削除。
  - アクセスグループの削除。
  - アクセスグループでのアクセス制御エントリ（ACE）の編集。
  - オブジェクトグループの編集。
- Application Visibility and Control（AVC）ポリシーの追加、削除、または編集。

ポリシーへの変更に応じて、次のいずれかのアクションが発生する可能性があります。

- 検査してドロップ：既存のセッションが破棄され、セッションがセッションテーブルから削除されます。
- 検査して転送：ゾーンベース ファイアウォールがフローを検査しないため、既存のセッションが破棄されます。ただし、このシナリオでは、トラフィックフローは続きます。
- 検査して検査：既存のセッションが新しいクラスマップの下に移動されます。
- 転送して検査/ドロップして検査：既存の動作が続行され、フローの途中での再分類がサポートされていないためにフローがブロックされます。

（注） ポリシーの変更がある場合、フローの途中でデータを確立することはできません。

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、セキュリティの観点から見ると同様のインターフェイスをグループ化する必要があります。

ゾーンベース ポリシー ファイアウォールの制約事項

- Cisco Wide Area Application Services（WAAS）と Cisco IOS XE ファイアウォール設定では、WAE デバイスによって処理されるすべてのパケットは、両方向とも Cisco IOS XE ファイアウォールを通過して、WCCP 総称ルーティングカプセル化（GRE）リダイレクトをサポートする必要があります。この状況は、レイヤ2リダイレクトが使用できない場合に発生します。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、GRE リダイレクトを続行させます。
- WCCPがレイヤ2リダイレクト方式で設定されている場合、ゾーンベースファイアウォールは、WAAS および WCCP と相互運用できません。
- ゾーンベース ファイアウォール設定は、Cisco Unity Express Virtual（vCUE）コールフローを含むブリッジ ドメイン インターフェイス（BDI）には適用できません。
- セルフゾーンは、デフォルトの「deny all」ポリシーの唯一の例外です。ルータインターフェイスへのすべてのトラフィックは、トラフィックが明示的に拒否されるまで許可されます。
- WAAS および Cisco IOS XE ファイアウォール構成では、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のリダイレクトをサポートしていません。
- Cisco ISR-WAAS I/O モジュールを使用して構成された ASR で、汎用 GRE を使用したゾーンベース ポリシー ファイアウォールが有効になっている場合、WCCP トラフィック リダイレクションは機能しません。この構成は、WAN の最適化ソリューションです。WCCP トラフィック リダイレクションを機能させるには、インターフェイスからゾーンベース ポリシーファイアウォール設定を削除します。WAEデバイスを使用している場合、WCCP トラフィック リダイレクションは正しく動作します。

  WAAS の場合、汎用 GRE は最適化が完了すると、WAAS WAE からのパケットを GRE トンネル経由で最初にリダイレクトされたデバイスと同じデバイスに返すのに役立つ、アウトオブパス導入のメカニズムです。
- 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 ゾーンを含め、すべてのゾーン間でサポートされません。コントロールプレーンをマルチキャスト トラフィックから保護するには、コントロール プレーン ポリシングを使用します。
- 内部から外部へのゾーンベースポリシーがWindowsシステムのICMPに一致するように設定されている場合、**traceroute** コマンドは機能します。ただし Apple システムでは、UDP ベースの traceroute を使用するため、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** コマンドおよび **icmp host unreachable** コマンドを **pass** コマンド（**inspect** コマンドではない）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。この制限は Cisco IOS XE リリース 3.1S 以前のリリースに適用されます。
- クラスマップでは ACL がサポートされます。ただし、ACL ベースのパケットカウントはデフォルトで無効になっています。Perfilter の統計情報は Cisco IOS XE リリース 3.13S 以降のゾーンベース ファイアウォールで使用できます。

- オブジェクトグループを使用する ACL ステートメントは、処理のためにランデブーポイント（RP）に送信されるパケットでは無視されます。
- ブリッジドメイン インターフェイスは、すべてのレイヤ4およびレイヤ7インスペクションを含む、ゾーンベース ファイアウォール インスペクションをサポートしていません。
- デバイスで NAT NVI が有効になっている場合、ZBF はトラフィックを検査できません。
- トラフィックがゾーンペアに入ると、ファイアウォールは接続テーブル全体を調べ、入力インターフェイスがゾーンペアに一致しなくても、表内のすべての接続とトラフィックを照合します。このシナリオでは、検査アクションが設定されている場合、ファイアウォール上の非対称にルーティングされたトラフィックがパケットをドロップする可能性があります。

  Cisco IOS XE リリース 3.15S 以降のリリースでは、zone-mismatch drop はクラスパラメータマップで設定されます。zone-mismatch drop が設定されている場合、ゾーンは、パケットの分類時に使用された元のゾーンに対してチェックされます。ゾーンがゾーンペアの一方ではない場合、パケットはドロップされます。zone-mismatch drop が設定されていない場合、ゾーンはチェックされません。
- ZBF が設定されている場合、ゾーンペアの一部であるすべてのインターフェイスに RII が設定されている必要があります。ピアデバイスと一致するインターフェイスには、同じ RII が設定されている必要があります。さらに、2 つのインターフェイス間で開始されたフローは、一方のインターフェイスだけでも RII が割り当てられていない場合、スタンバイに同期されません。
- ゾーンベース ファイアウォールは、デフォルトゾーンのダイナミック インターフェイスでのみサポートされます。これらのインターフェイスは、トラフィックが IPsec または VPN セキュアトンネルにトンネリングされると、動的に作成または削除されます。仮想テンプレートは、特定のタイプのダイナミックインターフェイスをサポートするために使用されます。詳細については、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 （6 ページ）を参照してください。
- インターフェイスに適用されているゾーンベースファイアウォールの設定を無効にするには、**platform inspect disable-all** コマンドを使用します。同様に、インターフェイスでゾーンベース ファイアウォールを有効にするには、**no platform inspect disable-all** コマンドを使用します。

  platform inspect disable-all コマンドが適用されているかどうかを確認するには、次の **show running** 設定を使用します。

```
show run | sec disable
platform inspect disable-all
```

（注） デフォルトでは、ゾーンベース ファイアウォールは常に有効になっています。

- ユーザー定義クラスまたはポリシーのデフォルトクラスで **droplog** コマンドが設定されていると、**drop** コマンドを設定してドロップされたパケットのロギングを無効にしても、ログメッセージは停止されません。これは既知の問題であり、回避策は、**nodroplog** コマンドを設定した後で、**drop** コマンドを設定し、メッセージのロギングを停止することです。この問題は **pass** コマンドにも適用されます。次の例は問題を示しています。

```
! Logging of dropped packets is enabled by configuring the drop log command.
policy-map type inspect INT-EXT
 class type inspect INT-EXT
  pass
 class class-default
  drop log
!
```

次の例は回避策を示しています。

```
! In this example, the no drop log command is configured before the drop command.
policy-map type inspect INT-EXT
 class type inspect INT-EXT
  pass
 class class-default
  drop log
  no drop log
  drop
!
```

- ZBFWセッション再分類機能を使用する場合、ステートフルトラフィックのフロー途中の検査はサポートされません。たとえば、ポリシー設定の変更により、既存のフローのアクションが、ドロップから検査に変更される可能性があります。この場合、ZBFWは、既存のフローを検査しません。
- ハイアベイラビリティは、ゾーンベース ファイアウォール ポリシー再分類ではサポートされません。

ゾーンベース ポリシー ファイアウォールの設定方法

以下のセクションでは、ゾーンベース ポリシー ファイアウォールの設定を指定するさまざまな作業について説明します。

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「最上位」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、次の作業を行います。

（注） ステップ 4、5、6 のうち、少なくとも 1 つのマッチング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 ファイアウォール ポリシーでは、ポリシーと一致するのは、セッションを作成した最初のパケットのみです。このフローの後続パケットは、設定されたポリシー内のフィルタと一致しませんが、セッションとは直接一致します。後続パケットに関連する統計情報は、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 モードを有効にします。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	**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、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 access-group** {*access-group* | **name** *access-group-name*} 例： `Device(config-cmap)# match access-group 101`	ACL 名または番号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	**match protocol** *protocol-name* [**signature**] 例：	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。

	コマンドまたはアクション	目的
	`Device(config-cmap)# match protocol http`	• 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 6	**match class-map** *class-map-name* 例： `Device(config-cmap)# match class-map c1`	すで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`	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 モードに戻ります。
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`	（オプション）指定されたゾーン ペアにポリシーマップが適用されたために作成された、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） **Class-map** 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 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、次の手順を実行します。

検査タイプのポリシーマップを作成する場合、許容されるアクションは drop、inspect、pass、および service-policy のみである点に注意してください。

（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. **drop** [**log**]
7. **pass**
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： `Device> enable`	特権 EXEC モードを有効にします。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	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p1`	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 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、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	**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） **drop** アクションと **pass** アクションは排他的であり、**inspect** アクションと **drop** アクションは相互に排他的です。つまり、両方を同時に指定することはできません。どちらか 1 つだけを指定できます。
ステップ 7	**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。

	コマンドまたはアクション	目的
ステップ 8	**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 9	**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。

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。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。

	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* | **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ときにDNSルックアップセッションを管理する時間の長さ）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）ICMPセッションのタイムアウトを設定します。
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、セッションによって使用される帯域幅を制限します。

	コマンドまたはアクション	目的
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-exchange（FIN-exchange）を検出した後、TCP セッションを管理する時間を指定します。
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妨害（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。
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しきい値を設定します。
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 モードを終了して、特権 EXEC コンフィギュレーション 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、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。

ゾーンペアでは、送信元ゾーンと宛先ゾーンを同じゾーンにすることができます。デフォルトでは、ゾーン内に留まるトラフィックは検査されません。さらに、デフォルトゾーン（ゾーン割り当てのないインターフェイス）が存在し、これも指定できます。

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. **interface** *type number*
7. **zone-member security** *zone-name*
8. **exit**
9. **zone-pair security** *zone-pair name* [**source** *source-zone-name* | **self** | *default*] **destination** [**self** | *default* | *destination-zone-name*]
10. **description** *line-of-description*
11. **service-policy type inspect** *policy-map-name*
12. **platform inspect match-statistics per-filter**
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。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	**zone security** *zone-name* 例： `Device(config)# zone security z1`	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	**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 モードに戻ります。
ステップ 6	**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 7	**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、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除きます）。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	**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 9	**zone-pair security** *zone-pair name* [**source** *source-zone-name* | **self** | *default*] **destination** [**self** | *default* | *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 10	**description** *line-of-description* 例： `Device(config-sec-zone-pair)# description accounting network to internet`	（任意）ゾーン ペア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 11	**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 12	**platform inspect match-statistics per-filter** 例： `Device(config-sec-zone-pair)# platform inspect match-statistics per-filter`	ゾーンベース ファイアウォールのフィルタごとの統計を有効にします。 （注） デバイスでフィルタごとの統計を有効にするには、次の手順を実行します。 • デバイスをリロードします。または • すべてのサービスポリシーを削除し、統計に変更を再適用します。**platform inspect match-statistics per-filter** コマンドをアクティブにするには、すべてのサービスポリシーを再適用します。
ステップ 13	**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 モードに戻ります。

NetFlow イベント ロギングの設定

グローバル パラメータ マップは、NetFlow イベント ロギングに使用されます。NetFlow イベント ロギングをイネーブルにすると、装置外の高速ログ コレクタにログが送信されます。デフォルトでは、この機能はイネーブルになっていません。この機能をイネーブルにしない場合、ファイアウォールのログは、ルートプロセッサまたはコンソールのロガーバッファに送信されます。

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** *ipv4-address port*
6. **log flow-export template timeout-rate** *seconds*
7. **end**

8. **show parameter-map type inspect-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 モードを有効にします。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	**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`	ファイアウォールによってドロップされるすべての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** *ipv4-address port* 例： `Device(config-profile)# log flow-export v9 udp destination 192.0.2.0 5000`	NetFlow イベント ロギングをイネーブルにして、コレクタの IP アドレスとポートを指定します。
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`	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。
ステップ 8	**show parameter-map type inspect-global** 例： `Device# show parameter-map type inspect-global`	グローバル検査タイプパラメータマップ情報を表示します。

WAAS を使用したファイアウォールの設定

トラフィックをインターセプトするために L2 を使用してトラフィックを WAE デバイスにリダイレクトするファイアウォール用のエンドツーエンド WAAS トラフィックフロー最適化を設定するには、次の作業を実行します。ZBFW 環境で WCCP を設定する場合は、L2 または

GRE カプセル化が使用されます。ただし、このシナリオでは、ゾーン ベース ファイアウォールに GRE が必要であるため、L2 リダイレクションが重要です。

Cisco IOS XE ソフトウェアでは WAAS のサポートがデフォルトで有効になっており、WAAS 処理が検出されます。

（注） WAAS を使用したファイアウォールの設定（手順 5 ～ 13）は、Cisco IOS XE リリース 3.5S 以降では必要ありません。手順 5 ～ 12 のコマンドは、Cisco IOS XE リリース 3.5S 以降では廃止されています。

手順の概要

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

31. 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	**ip wccp** *service-id* 例： `Device(config)# ip wccp 61`	WCCP のダイナミック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 wccp** *service-id* 例： `Device(config)# ip wccp 62`	WCCP のダイナミックに定義されたサービス識別番号を入力します。
ステップ 5	**log dropped-packets enable** 例： `Device(config-profile)# log dropped-packets enable`	
ステップ 6	**max-incomplete low** 例： `Device(config)# max-incomplete low 18000`	
ステップ 7	**max-incomplete high** 例： `Device(config)# max-incomplete high 20000`	
ステップ 8	**class-map type inspect** *class-name* 例： `Device(config)# class-map type inspect most-traffic`	トラフィック クラス用の検査タイプ 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。 （注） **class-map type inspect most-traffic** コマンドは非表示になっています。
ステップ 9	**match protocol** *protocol-name* [**signature**] 例： `Device(config-cmap)# match protocol http`	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 10	**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 11	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p1`	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 12	**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は、未分類のパケットが照合されます。
ステップ 13	**class-map type inspect** *class-name* 例： `Device(config-pmap)# class-map type inspect most-traffic`	アクションの実行対象となるファイアウォール トラフィック（クラス）マップを指定し、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** 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 15	**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 16	**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 モードに戻ります。
ステップ 17	**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 18	**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 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 モードに戻ります。

	コマンドまたはアクション	目的
ステップ 20	**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 21	**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 22	**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 23	**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 24	**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の説明を入力します。
ステップ 25	**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、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除きます）。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 26	**ip address** *ip-address* 例： `Device(config-if)# ip address 10.70.0.1 255.255.255.0`	セキュリティ ゾーン用のインターフェイス IP アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 27	**ip wccp** *service-id* {**group-listen** | **redirect** {**in** | **out**}} 例： `Device(config-if)# ip wccp 61 redirect in`	インターフェイスで WCCP パラメータを指定します。
ステップ 28	**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 29	**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 30	**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 31	**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 モードに戻ります。

ゾーンベース ファイアウォールの再分類の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** {*parameter-map-name* | **global** | session-reclassify-allow}

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：	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
	`Device# configure terminal`	
ステップ 3	**parameter-map type inspect** {*parameter-map-name* | **global** | session-reclassify-allow}	**parameter-map type inspect-global** モードで **session-reclassify-allow** 属性を設定して、セッションの再分類を有効にします。 この設定を無効にするには、**session-reclassify-allow** コマンドの **no** 形式を使用します。

ゾーンベース ポリシー ファイアウォールの設定例

ここでは、ゾーンベース ポリシー ファイアウォールの設定に関連する例を示します。

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 ACL 199 と一致し、ディープパケット HTTP インスペクションが設定されます。**match access-group 101** を設定すると、レイヤ 4 インスペクションが有効になります。その結果、クラスマップのタイプが match-all である場合を除いて、レイヤ 7 インスペクションが省略されます。

```
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：検査パラメータ マップの作成

次の設定例は、検査パラメータマップの作成を示しています。

```
parameter-map type inspect eng-network-profile
 alert on
 audit-trail on
 dns-timeout 60
 icmp idle-timeout 90
 max-incomplete low 800
 one-minute low 300
 sessions maximum 200
 tcp finwait-time 5
 tcp idle-time 90
 tcp max-incomplete host 500 block-time 10
 tcp synwait-time 3
 udp idle-time 75
```

例：セキュリティ ゾーンとゾーン ペアの作成とゾーン ペアへのポリシー マップのアタッチ

例：セキュリティ ゾーンの作成

次に、finance department networks という名前のセキュリティ ゾーン z1 と engineering services network という名前のセキュリティ ゾーン z2 を作成する例を示します。

```
zone security z1
 description finance department networks
!
zone security z2
 description engineering services network
```

例：ゾーン ペアの作成

次に、ゾーン z1 とゾーン z2 を作成し、ゾーン z2 でゾーン間を流れるトラフィックにファイアウォール ポリシー マップが適用されるように指定する例を示します。

```
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

次に、イーサネット インターフェイス 0 をゾーン z1 に、イーサネット インターフェイス 1 をゾーン z2 にアタッチする例を示します。

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

例：ゾーンベース ファイアウォールのフィルタごとの統計

次の設定例は、多数のファイアウォールフィルタが作成される場合にメモリ不足を回避する方法を示しています。メモリ不足を防ぐために、**platform inspect match-statistics per-filter** コマンドを使用してゾーンベース ファイアウォールのフィルタごとの統計を有効にすることができます。この例では、フィルタ（ACL または UDP）ごとに、ゾーンベース ファイアウォールを通過したパケット数とバイト数について使用可能な統計が存在します。

```
Device# show policy-map type inspect zone-pair ogacl_zp
 Zone-pair: ogacl_zp
  Service-policy inspect : ogacl_pm
Class-map: ogacl_cm (match-any)
  Match: access-group name ogacl
        xxx packets, xxx bytes
      Match: protocol udp
        xxx packets, xxx bytes
```

（注） フィルタごとの統計は、match-any フィルタについてのみ使用でき、match-all の場合には適用されません。

（注） Cisco IOS XE 16.3 リリースおよび Cisco IOS XE 16.4 リリースの場合、フィルタごとの統計を有効にするには、**platform inspect match-statistics per-filter** コマンドをアクティブにする前に、デバイスをリロードするかサービスポリシーを削除してから、ゾーンペアにサービスポリシーを再適用します。

Cisco IOS XE 3.17 リリースの場合、このコマンドをアクティブにするには、設定を保存し、システムをリロードする必要があります。

（注） 同様に、フィルタごとの統計を無効にするには、デバイスをリロードするかサービスポリシーを削除してから、ゾーンペアにサービスポリシーを再適用します。

デバイスで使用されている TCAM メモリを確認するには、**show platform hardware qfp active classification feature-manager shm-stats-counter** コマンドを使用します。

```
Device# show platform hardware qfp active classification feature-manager shm-stats-counter
    Shared Memory Information:
    Total shared memory size: 16777216
    Used shared memory size: 14703656
```

（注） トラフィックドロップまたはフィルタごとの統計のカウンタが表示されないときは、多くの場合、使用されている TCAM 共有メモリが TCAM 合計の 75% を超えています。

（注） デバイスで使用されている共有メモリがキャパシティの 75% を超えると、次の警告メッセージが表示されます。

```
%CPP_FM-3-CPP_FM_TCAM_WARNING: SIP1: cpp_sp_svr: TCAM limit exceeded: Already used 75
percent shared memory for per-filter stats.
```

デバイスで使用されている共有メモリが 100% の場合は、次の警告メッセージが表示されます。

```
%CPP_FM-3-CPP_FM_TCAM_WARNING: SIP1: cpp_sp_svr: TCAM limit exceeded: Shared memory for
per-filter stats overflow!
```

例：NetFlow イベント ロギングの設定

次に、NetFlow イベントロギングを設定する例を示します。

```
parameter-map type inspect global
 log dropped-packets
 log flow-export v9 udp destination 192.0.2.0 5000
 log flow-export template timeout rate 5000
```

例：WAAS を使用した Cisco ファイアウォールの設定

次に、WCCP を使用してトラフィックを検査のために WAE デバイスにトラフィックをリダイレクトするファイアウォールのエンドツーエンドの WAAS トラフィックフローを最適化する設定の例を示します。

次に、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に、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する設定例を示します。

```
! Zone-based firewall configuration on your router.
ip wccp 61
ip wccp 62
parameter-map type inspect global
 log dropped-packets enable
 max-incomplete low 18000
 max-incomplete high 20000
!
class-map type inspect match-any 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
  drop
!
zone security in
!
zone security out
!
zone security waas
!
zone-pair security in-out source in destination out
 service-policy type inspect p1
!
zone-pair security out-in source out destination in
 service-policy type inspect p1
!
zone-pair security waas-out source waas destination out
 service-policy type inspect p1
!
zone-pair security in-waas source in destination waas
 service-policy type inspect p1
```

```
!
interface GigabitEthernet0/0
 description WAN Connection
 no ip dhcp client request tftp-server-address
 no ip dhcp client request router
 ip address dhcp
 ip wccp 62 redirect in
 ip wccp 61 redirect out
 ip flow ingress
 ip nat outside
 ip virtual-reassembly in
 ip virtual-reassembly out
 zone-member security out
 load-interval 30
 delay 30
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description Clients
 ip address 172.25.50.1 255.255.255.0
 ip pim sparse-mode
 ip nat inside
 ip virtual-reassembly in
 zone-member security in
 ip igmp version 3
 delay 30
 duplex auto
 speed auto
!
interface Vlan1
 description WAAS Interface
 ip address 172.25.60.1 255.255.255.0
 ip wccp redirect exclude in
 ip nat inside
 ip virtual-reassembly in
 zone-member security waas
 load-interval 30
!
```

次に、ゾーンベース ファイアウォール サポートするための WAE 上での設定例を示します。この設定は、ルータでは行うことができず、WAE でのみ行うことができることに注意してください。

```
!Configuration on the WAE.
primary-interface Virtual 1/0
interface Virtual 1/0
 ip address 172.25.60.12 255.255.255.0
!
ip default-gateway 172.25.60.1
wccp router-list 1 172.25.60.1
wccp tcp-promiscuous service-pair 61 62
 router-list-num 1
 redirect-method gre
 egress-method ip-forwarding
 enable
!
```

例：同じゾーン内の FlexVPN と DVTI を使用したファイアウォールの設定

次に、FlexVPN およびダイナミック仮想トンネルインターフェイス（DVTI）が同じゾーンに設定されたファイアウォールの例を示します。

```
crypto ikev2 proposal PROP
 encryption 3des
 integrity sha256
 group 5
crypto ikev2 policy POL
 match fvrf any
 proposal PROP
crypto ikev2 keyring keyring1
 peer peer
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco
crypto ikev2 profile prof1
 authentication remote pre-share
 authentication local pre-share
 match identity remote address 0.0.0.0
 match address local interface loopback1
 keyring local keyring1
 no shutdown
 Virtual-Template 1
class-map type inspect match-any cmap
 match protocol icmp
 match protocol tcp
 match protocol udp
policy-map type inspect pmap
 class type inspect cmap
 inspect
 class class-default
 drop log
zone security in
zone security zone1
zone-pair security zp1 source zone1 destination in
 service-policy type inspect pmap
crypto ipsec profile ipsec1
 set ikev2-profile prof1
interface Loopback1
 ip address 51.1.1.1 255.255.255.0
interface Gi0/0/0.2
 encapsulation dot1q 2
 ip address 100.1.1.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.3
 encapsulation dot1q 3
 ip address 100.1.2.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.4
 encapsulation dot1q 4
 ip address 100.1.3.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.5
 encapsulation dot1q 5
 ip address 100.1.4.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.6
 encapsulation dot1q 6
 ip address 100.1.5.1 255.255.255.0
```

```
 zone-member security in
interface Virtual-Template1 type tunnel
 ip unnumbered loopback1
 zone-member security zone1
 tunnel source loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec1
ip route 60.0.0.0 255.0.0.0 192.168.2.2
```

例：別のゾーン内の FlexVPN と DVTI を使用したファイアウォールの設定

次に、FlexVPN およびダイナミック仮想トンネルインターフェイス（DVTI）が別のゾーンに設定されたファイアウォールの例を示します。

```
crypto ikev2 proposal PROP
 encryption 3des
 integrity sha256
 group 5
crypto ikev2 policy POL
 match fvrf any
 proposal PROP
crypto ikev2 keyring keyring1
 peer peer1
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco1
crypto ikev2 keyring keyring2
 peer peer2
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco2
crypto ikev2 keyring keyring3
 peer peer3
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco3
crypto ikev2 keyring keyring4
 peer peer4
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco4
crypto ikev2 keyring keyring5
 peer peer5
 address 0.0.0.0 0.0.0.0
 pre-shared-key cisco5
crypto ikev2 profile prof1
 authentication remote pre-share
 authentication local pre-share
 match identity remote address 0.0.0.0
 match address local interface loopback1
 keyring local keyring1
 no shutdown
 Virtual-Template 1
crypto ikev2 profile prof2
 authentication remote pre-share
 authentication local pre-share
 match identity remote address 0.0.0.0
 match address local interface loopback2
 keyring local keyring2
 no shutdown
 Virtual-Template 2
crypto ikev2 profile prof3
 authentication remote pre-share
 authentication local pre-share
```

```
 match identity remote address 0.0.0.0
 match address local interface loopback3
 keyring local keyring3
crypto ikev2 profile prof4
 authentication remote pre-share
 authentication local pre-share
 match identity remote address 0.0.0.0
 match address local interface loopback4
 keyring local keyring4
 no shutdown
 Virtual-Template 4
crypto ikev2 profile prof5
 authentication remote pre-share
 authentication local pre-share
 match identity remote address 0.0.0.0
 match address local interface loopback5
 keyring local keyring5
 no shutdown
 Virtual-Template 5
class-map type inspect match-any cmap
 match protocol icmp
 match protocol tcp
 match protocol udp
policy-map type inspect pmap
 class type inspect cmap
 inspect
 class class-default
 drop log
zone security in
zone security zone1
zone security zone2
zone security zone3
zone security zone4
zone security zone5
zone-pair security zp1 source zone1 destination in
 service-policy type inspect pmap
zone-pair security zp2 source zone2 destination in
 service-policy type inspect pmap
zone-pair security zp3 source zone3 destination in
 service-policy type inspect pmap
zone-pair security zp4 source zone4 destination in
 service-policy type inspect pmap
zone-pair security zp5 source zone5 destination in
 service-policy type inspect pmap
crypto ipsec profile ipsec1
 set ikev2-profile prof1
crypto ipsec profile ipsec2
 set ikev2-profile prof2
crypto ipsec profile ipsec3
 set ikev2-profile prof3
crypto ipsec profile ipsec4
 set ikev2-profile prof4
crypto ipsec profile ipsec5
 set ikev2-profile prof5
interface Loopback1
 ip address 50.1.1.1 255.255.255.0
interface Loopback2
 ip address 50.1.2.1 255.255.255.0
interface Loopback3
 ip address 50.1.3.1 255.255.255.0
interface Loopback4
 ip address 50.1.4.1 255.255.255.0
interface Loopback5
 ip address 50.1.5.1 255.255.255.0
```

```
interface Gi0/0/0.2
 encapsulation dot1q 2
 ip address 100.1.1.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.3
 encapsulation dot1q 3
 ip address 100.1.2.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.4
 encapsulation dot1q 4
 ip address 100.1.3.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.5
 encapsulation dot1q 5
 ip address 100.1.4.1 255.255.255.0
 zone-member security in
interface Gi0/0/0.6
 encapsulation dot1q 6
 ip address 100.1.5.1 255.255.255.0
 zone-member security in
interface Virtual-Template1 type tunnel
 ip unnumbered loopback1
 zone-member security zone1
 tunnel source loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec1
interface Virtual-Template2 type tunnel
 ip unnumbered loopback2
 zone-member security zone2
 tunnel source loopback2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec2
interface Virtual-Template3 type tunnel
 ip unnumbered loopback3
 zone-member security zone3
 tunnel source loopback3
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec3
interface Virtual-Template4 type tunnel
 ip unnumbered loopback4
 zone-member security zone4
 tunnel source loopback4
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec4
interface Virtual-Template5 type tunnel
 ip unnumbered loopback5
 zone-member security zone5
 tunnel source loopback5
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile ipsec5
ip route 60.0.0.0 255.0.0.0 192.168.2.2
```

ゾーンベース ポリシー ファイアウォールに関する追加情報

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 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 を使用して無効にすることができます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。