ゾーンベース ポリシー ファイアウォールの設計と適用ガイド

目次

概要

Cisco IOS® ソフトウェア リリース 12.4(6)T では、Cisco IOS Firewall フィーチャ セットの新しい設定モデルである Zone-Based Policy Firewall（ZFW; ゾーンベース ポリシー ファイアウォール）が導入されました。 この新しい設定モデルでは、複数インターフェイスのルータで直感的に

使用できるポリシー、ファイアウォール ポリシー適用の精度の増加、および望ましいトラフィックを許可する明示的なポリシーが適用されるまでファイアウォールのセキュリティ ゾーン間のトラフィックを禁止するデフォルトの deny-all ポリシーが提供されます。

Cisco IOS ソフトウェア リリース 12.4(6)T よりも前に実装されていたほぼすべての Cisco IOS Classic Firewall の機能は、新しいゾーンベース ポリシー検査インターフェイスでサポートされています。

- ステートフル パケット検査
- VRF 対応 Cisco IOS Firewall
- URL フィルタリング
- Denial-of-Service（DoS; サービス拒絶）の緩和

Cisco IOS ソフトウェア リリース 12.4(9)T の ZFW では、クラスごとのセッション/接続、スループットの制限に加え、次のアプリケーションの検査と制御に対するサポートが追加されました。

- HTTP
- Post Office Protocol（POP3）、Internet Mail Access Protocol（IMAP）、Simple Mail Transfer Protocol/Enhanced Simple Mail Transfer Protocol（SMTP/ESMTP）
- Sun Remote Procedure Call（RPC; リモート プロシージャ コール）
- Instant Messaging（IM; インスタント メッセージ）アプリケーション：Microsoft MessengerYahoo! MessengerAOL Instant Messenger
- Peer-to-Peer（P2P; ピアツーピア）ファイル共有：BitTorrentKaZaAGnutellaedonkey

Cisco IOS ソフトウェア リリース 12.4(11)T では、より簡単な DoS 防御調整のための統計情報が追加されました。

次のように Cisco IOS Classic Firewall の機能の中には、Cisco IOS ソフトウェア リリース 12.4(15)T の ZFW ではまだサポートされないものもあります。

- 認証プロキシ
- ステートフル ファイアウォール フェールオーバー
- 統合ファイアウォール MIB
- IPv6 ステートフル検査
- TCP 順序入れ替わりサポート

ZFW は、一般に、ほとんどのファイアウォール検査アクティビティに対して Cisco IOS パフォーマンスを向上させます。

Cisco IOS ZFW も Classic Firewall も、マルチキャスト トラフィックに対するステートフル検査のサポートは行いません。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

ゾーンベース ポリシーの概要

Cisco IOS Classic Firewall ステートフル検査（以前は Context-Based Access Control（CBAC; コンテキストベース アクセス制御）と呼ばれていたもの）は、インターフェイスベースの設定モデルを採用しており、そこでは 1 つのステートフル検査ポリシーが 1 つのインターフェイスに適用されていました。 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は同一の検査ポリシーを受信しました。 この設定モデルはファイアウォール ポリシーの精度を限定し、ファイアウォール ポリシーの適切な適用を混乱させる原因となり、特に、ファイアウォール ポリシーを複数のインターフェイス間で適用する必要があるときに混乱が発生しました。

ゾーンベース ポリシー ファイアウォール（または Zone-Policy Firewall（ZFW））は、以前のインターフェイスベースのモデルから、より柔軟性があり、簡単に理解できるゾーンベースのモデルへとファイアウォールの設定を変更しました。 インターフェイスはゾーンに割り当てられ、検査ポリシーはゾーン間を移動するトラフィックに適用されます。 ゾーン間ポリシーでは十分な柔軟性と精度が提供されるので、同一のルータ インターフェイスに接続された複数のホスト グループにさまざまな検査ポリシーを適用できます。

ファイアウォール ポリシーは Cisco® Policy Language（CPL; シスコ ポリシー言語）で設定されます。CPL は、階層構造を採用して、検査が適用されるネットワーク プロトコルとホストのグループに検査を定義します。

ゾーンベース ポリシー設定モデル

ZFW は、Cisco IOS Classic Firewall に比べ、Cisco IOS Firewall 検査の設定方法を全面的に変更しました。

ファイアウォール設定の主な変更の第 1 は、ゾーンベースの設定を導入したことです。 Cisco IOS Firewall は、ゾーン設定モデルを実装した最初の Cisco IOS ソフトウェア脅威防御機能です。 その他の機能でもそのうちにゾーン モデルが採用される可能性があります。 **ip inspect** コマンド セットを採用している Cisco IOS Classic Firewall ステートフル検査（または CBAC）インターフェイスベースの設定モデルは、一定期間維持されます。 ただし、新しい機能のうち、従来の Command-Line Interface（CLI; コマンドライン インターフェイス）で設定可能なものは、あるとしてもわずかしかありません。 ZFW は、ステートフル検査や CBAC コマンドを使用しません。 この 2 つの設定モデルは、ルータ上で同時に使用できますが、インターフェイス上で組み合わせることはできません。 1 つのインターフェイスを、セキュリティ ゾーン メンバとして設定し、同時に **ip inspect** 用に設定することはできません。

ゾーンは、ネットワークのセキュリティ境界を確立します。 ゾーンは、トラフィックがネットワークの別の領域へ移動するときに、トラフィックがポリシーの制約を受ける境界を定義します。 ZFW のゾーン間のデフォルト ポリシーは「すべて拒否」です。 明示的に設定されるポリシーが何もない場合、ゾーン間を移動するすべてのトラフィックはブロックされます。 これは、Access Control List（ACL; アクセス コントロール リスト）で明示的にブロックされるまでトラフィックが暗黙で許可されているステートフル検査のモデルからは、かなり逸脱しています。

第 2 重要な変更点は Cisco IOSソフトウェア モジュラー クオリティオブサービス（QoS）を CLI（MQC）よく知っている CPL. Users として知られている新しい構成ポリシー言語の概要どのトラフィックがポリシーマップで適用された操作から影響を受けるか規定 するために形式が QoS

のクラスマップの使用に類似したであることを認識するかもしれません。

ゾーンベース ポリシー ファイアウォールの適用規則

ゾーン内でのルータ ネットワーク インターフェイスのメンバシップは、ゾーン メンバ インターフェイス間でトラフィックが移動するときにインターフェイスの動作を管理する次のいくつかの規則に従います。

- ゾーンは、インターフェイスがゾーンに割り当てられるようになる前に設定する必要があります。
- インターフェイスは、1 つのセキュリティ ゾーンにだけ割り当てることができます。
- あるインターフェイスを行き来するすべてのトラフィックは、そのインターフェイスが 1 つのゾーンに割り当てられると暗黙でブロックされます。その例外としてブロックされないものは、同じゾーン内の他のインターフェイスを行き来するトラフィックと、ルータ上のインターフェイスへのトラフィックです。
- トラフィックは、同一ゾーンのメンバであるインターフェイス間にデフォルトで転送されることを暗黙で許可されています。
- あるゾーン メンバ インターフェイスをトラフィックが行き来することを許可するには、トラフィックを許可または検査するポリシーをそのゾーンと他の任意のゾーンの間で設定する必要があります。
- セルフ ゾーンは、デフォルトの「すべて拒否」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。
- トラフィックはゾーン メンバ インターフェイス間およびゾーン メンバではないインターフェイスの間は行き来できません。 通過、検査、廃棄のアクションは、2 つのゾーンの間だけで適用できます。
- ゾーンに割り当てられていないインターフェイスは、従来のルータ ポートとして機能し、また、それらのインターフェイスは従来型のステートフル検査または CBAC 設定を引き続き使用している可能性があります。
- ルータ上のインターフェイスをゾーン設定やファイアウォール ポリシーの一部としないことが必要とされている場合。 あるゾーン内にそのインターフェイスを置き、そのゾーンと、トラフィック フローが望まれる他のゾーンとの間ですべて通過ポリシー（ダミー ポリシーの一種）を設定することが引き続き必要である可能性もあります。
- 前述に従い、トラフィックが 1 つのルータ内のすべてのインターフェイスの間を移動する予定の場合、すべてのインターフェイスがゾーン設定モデルの一部になる必要があります（それぞれのインターフェイスは 1 つのゾーンまたは別のゾーンのメンバである必要があります）。
- 前述のデフォルトで拒否のアプローチの唯一の例外は、ルータを行き来するトラフィックであり、それは、デフォルトで許可されます。 そのようなトラフィックを制限するために、明示的なポリシーを設定できます。

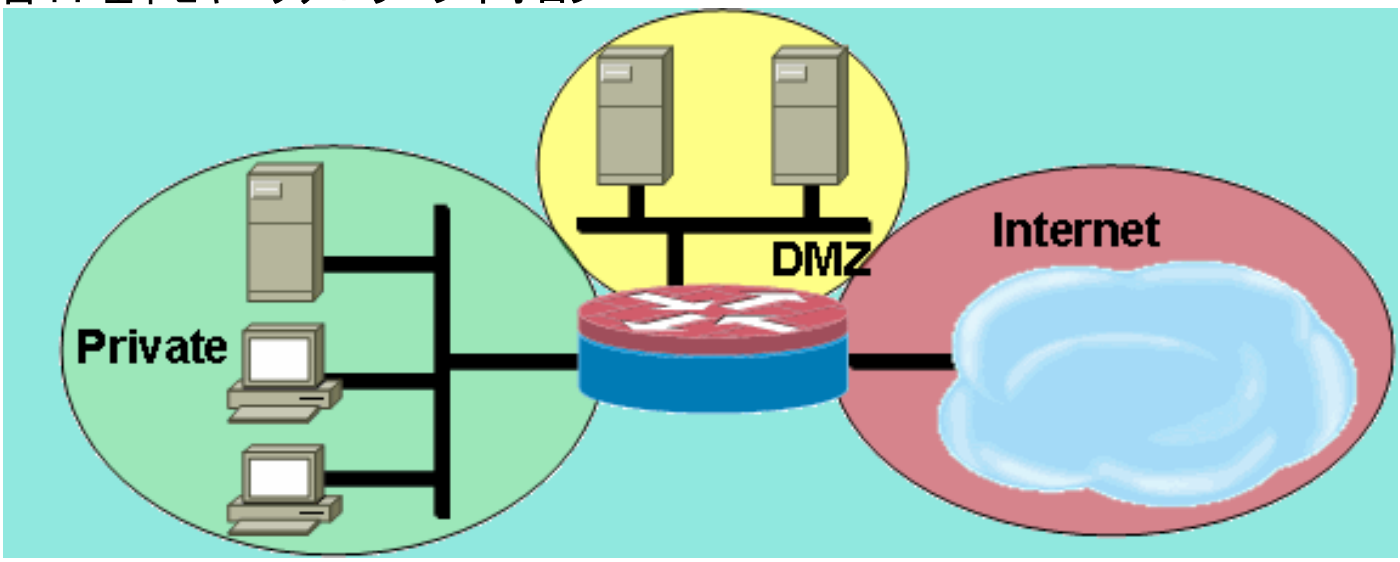
ゾーンベース ポリシー ネットワーク セキュリティの設計

セキュリティ ゾーンは、そのセキュリティ ゾーンに割り当てられるすべてのインターフェイスが類似のセキュリティ レベルで保護されるように、ネットワーク内の相対的セキュリティの各領域用に設定する必要があります。 たとえば、次のように 3 つのインターフェイスのあるアクセス ルータの場合を検討します。

- 1 つのインターフェイスはパブリック インターネットに接続されている
- 1 つのインターフェイスはパブリック インターネットからはまったくアクセスできないプライベート LAN に接続されている
- 1 つのインターフェイスは、Web サーバ、Domain Name System (DNS; ドメイン ネーム システム) サーバ、電子メール サーバがパブリック インターネットにアクセス可能である必要がある、インターネット サービス Demilitarized Zone (DMZ; 非武装地帯) に接続されている

このネットワークの各インターフェイスは、それ自体のゾーンに割り当てられますが、DMZ 内の特定のホストへのパブリック インターネットからのさまざまなアクセスと、保護された LAN 内のホストのさまざまなアプリケーション使用ポリシーを許可したい場合もあります (図 1 を参照) 。

図 1 : 基本セキュリティ ゾーン トポロジ



この例で、それぞれのゾーンは 1 つのインターフェイスだけを保持しています。 プライベート ゾーンにインターフェイスが 1 つ追加された場合、ゾーン内の新しいインターフェイスに接続されたホストは、同一のゾーン内の既存のインターフェイス上のすべてのホストへとトラフィックを通過させることができます。 また、他のゾーン内のホストへのこれらのホストのトラフィックは、同様に既存のポリシーの影響を受けます。

通常、サンプル ネットワークには次のように 3 つのメイン ポリシーがあります。

- インターネットへのプライベート ゾーン接続
- DMZ ホストへのプライベート ゾーン接続
- DMZ ホストへのインターネット ゾーン接続

DMZ はパブリック インターネットに開示されているので、DMZ ホストは、1 つ以上の DMZ ホストの信頼性を低下させることに成功する可能性のある悪意のある個人からの望ましくないアクティビティにさらされる恐れがあります。 プライベート ゾーン ホストまたはインターネット ゾーン ホストのどちらかに到達するアクセス ポリシーが DMZ ホストに提供されない場合、DMZ ホストの信頼性を低下させた個人は、プライベート ホストまたはインターネット ホストに対してさらに攻撃を続けるために DMZ ホストを使用することはできません。 ZFW は、禁止デフォルト セキュリティ ポスチャを含んでいます。 そのため、DMZ ホストが他のネットワークへのアクセスを具体的に提供されない場合、他のネットワークは DMZ ホストの接続から保護されます。 同様に、プライベート ゾーン ホストをアクセスするためにインターネット ホストにはアクセスは提供されないので、プライベート ゾーン ホストは、インターネット ホストによる不要なアクセスからは保護されます。

ゾーンベース ポリシー ファイアウォールでの IPSec VPN の使

用

IPSec VPN への最新の機能拡張は、VPN 接続のためのファイアウォール ポリシー設定を簡素化します。 IPSec Virtual Tunnel Interface（VTI）と GRE+IPSec は、指定されたセキュリティ ゾーンにトンネル インターフェイスを配置することで、VPN のサイト間およびクライアント接続の特定のセキュリティ ゾーンへの限定を許可します。 接続を特定のポリシーに限定する必要がある場合、接続は VPN DMZ 内で隔離できます。 または、VPN 接続が暗黙で信頼される場合、VPN 接続は信頼された内部ネットワークとして同一のセキュリティ ゾーンに配置できます。

非 VTI IPSec が適用される場合、VPN 接続ファイアウォール ポリシーはセキュリティを維持するために厳重な検査を必要とします。 ゾーン ポリシーは、セキュリティ ホストが VPN クライアントのルータへの暗号化された接続とは異なるゾーン内にある場合、リモート サイトのホストまたは VPN クライアント用の IP アドレスによるアクセスを具体的に許可する必要があります。 アクセス ポリシーが適切に設定されていない場合、保護される必要のあるホストは、望ましくない、敵対する可能性のあるホストに公開されてしまうことがあります。 概念と設定の詳細は、『VPN でのゾーンベース ポリシー ファイアウォールの使用』を参照してください。

Cisco Policy Language（CPL）の設定

この手順は ZFW を設定するときに使用できます。 ステップの順序は重要ではありませんが、いくつかのイベントは順番に実行する必要があります。 たとえば、クラスマップを設定してから、クラスマップをポリシーマップに割り当てる必要があります。 同様に、ポリシーを設定してからでないと、ポリシーマップをゾーンペアに割り当てることはできません。 まだ設定していない設定の別の部分に依存するセクションを設定しようとすると、ルータはエラー メッセージを返します。

1. ゾーンを定義します。
2. ゾーンペアを定義します。
3. トラフィックがゾーンペアを移動するときにポリシーがあらかじめ適用されている必要のあるトラフィックを説明するクラスマップを定義します。
4. クラスマップのトラフィックにアクションを適用するためにポリシーマップを定義します。
5. ポリシーマップをゾーンペアに適用します。
6. インターフェイスをゾーンに割り当てます。

ゾーンベース ポリシー ファイアウォール クラスマップの設定

クラスマップは、ファイアウォールがポリシー適用のために選択するトラフィックを定義します。 レイヤ 4 のクラスマップは、ここで示す次の基準をベースにしてソートします。 これらの基準は、クラスマップ（class-map）の **match** コマンドを使って指定されます。

- アクセスグループ：標準、拡張、または名前付き ACL は、送信元 IP および宛先 IP のアドレスと、送信元ポートおよび宛先ポートをベースにしてトラフィックをフィルタリングできます。
- プロトコル：レイヤ 4 プロトコル（TCP、UDP、および ICMP）と、HTTP、SMTP、DNS などのアプリケーション サービス。 ポートアプリケーション マッピングに知られている、既知のサービスまたはユーザ定義サービスを指定できます。
- クラスマップ：追加の照合基準を提供する下位のクラスマップは、別のクラスマップの内部にネストできます。
- 否定：*not* 基準は、指定されたサービス（プロトコル）、アクセスグループまたは下位のクラ

スマップに一致しないトラフィックがクラスマップに選択されることを指定します。

「match」基準の組み合わせ：「match-any」と「match-all」の比較

クラスマップは、照合基準を適用する方法を判断するために、match-any または match-all 演算子を適用できます。 match-any が指定された場合、トラフィックは、クラスマップ内の照合基準のうちの 1 つだけと一致する必要があります。 match-all が指定された場合、トラフィックは、その特定クラスに所属するためにクラスマップの基準のすべてと一致する必要があります。

照合基準は、トラフィックが複数の基準と一致する場合には、より具体的なものからそれほど具体的ではないものへの順番に適用する必要があります。 たとえば、次のクラスマップ（class-map）を検討しましょう。

```
class-map type inspect match-any my-test-cmap
 match protocol http
 match protocol tcp
```

HTTP トラフィックは、トラフィックが HTTP 検査のサービス固有の機能によって確実に処理されるよう、先に match protocol http に遭遇する必要があります。 この照合行が逆になり、トラフィックが match protocol tcp 文を検出してからそれを match protocol http と比較する場合、トラフィックは単純に TCP トラフィックとして分類され、ファイアウォールの TCP 検査コンポーネントの機能に従って検査されます。 これは、FTP、TFTP などの特定のサービスや、H.323、SIP、Skinny、RTSP その他などのいくつかのマルチメディアと音声の信号送出サービスで問題になります。 これらのサービスでは、これらのサービスのより複雑なアクティビティを認識するための追加の検査機能が必要になります。

照合基準としての ACL の適用

クラスマップは、ポリシー適用の照合基準の 1 つとして ACL を適用できます。 クラスマップの唯一の照合基準が ACL で、クラスマップが検査アクションを適用するポリシーマップに関連する場合、ルータは、ZFW がアプリケーション対応の検査を提供することを除き、ACL で許可されているすべてのトラフィック用の基本的な TCP または UDP 検査を適用します。 これには FTP、SIP、Skinny（SCCP）、H.323、Sun RPC、TFTP が含まれます（ただし、これに限りません）。 アプリケーション固有の検査が利用可能であり、ACL がプライマリ チャネルまたはコントロール チャネルを許可する場合、ACL がトラフィックを許可するかどうかに関係なく、プライマリ/コントロール チャネルに関連付けられたセカンダリ チャネルまたはメディア チャネルが許可されます。

クラスマップが照合基準として ACL 101 だけを適用する場合、ACL 101 は次のようになります。

```
access-list 101 permit ip any any
```

すべてのトラフィックは、指定のゾーンペアに適用された service-policy の方向で許可され、対応するリターン トラフィックは逆の方向で許可されます。 そのため、ACL は、トラフィックを具体的な希望のタイプに限定する制限を適用する必要があります。 PAM リストには、HTTP、NetBIOS、H.323、DNS などのアプリケーション サービスが含まれることに注意してください。 ただし、指定のポートに関する特定のアプリケーションの用途についての PAM の情報にもかかわらず、ファイアウォールは、アプリケーション トラフィックの既知の要件に対処するのに十分なアプリケーション固有の機能を適用するだけです。 つまり、telnet、SSH、その他の単一チャネル アプリケーションなどのシンプルなアプリケーション トラフィックは TCP として検査され、その統計情報は **show** コマンド出力に組み合わされます。 ネットワーク アクティビティへのアプリケーション固有の可視性が求められる場合、アプリケーション名ごとにサービスの検査を設定する必要があります（configure match protocol http、match protocol telnet など）。

この設定からの **show policy-map type inspect zone-pair** コマンド出力で利用できる統計情報と、後述するより明示的なファイアウォール ポリシーを比較してください。 この設定は、Cisco IP Phone からのトラフィックと、http、ftp、netbios、ssh、dns を含むさまざまなトラフィックを使用するいくつかのワークステーションを検査するために使用されます。

```
class-map type inspect match-all all-private
 match access-group 101
!
policy-map type inspect priv-pub-pmap
 class type inspect all-private
  inspect
 class class-default
!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect priv-pub-pmap
!
interface FastEthernet4
 ip address 172.16.108.44 255.255.255.0
 zone-member security public
!
interface Vlan1
 ip address 192.168.108.1 255.255.255.0
 zone-member security private
!
access-list 101 permit ip 192.168.108.0 0.0.0.255 any
```

この設定はプライベート ゾーンで発信するすべてのトラフィックを定義して対処するのが容易である（トラフィックが標準の PAM で認識される宛先ポートを確認する限り）一方で、サービス アクティビティへの可視性は限定されており、特定のタイプのトラフィックに対しては ZFW の帯域幅とセッション制限を適用する機会を提供しません。 この **show policy-map type inspect zone-pair priv-pub** コマンド出力は、ゾーンペア間の permit ip [サブネット] any ACL だけを使用する以前のシンプルな設定の結果です。 見てわかるように、ほとんどのワークステーション トラフィックは基本的な TCP または UDP 統計情報でカウントされます。

```
stg-871-L#show policy-map type insp zone-pair priv-pub Zone-pair: priv-pub Service-policy
inspect : priv-pub-pmap Class-map: all-private (match-all) Match: access-group 101 Inspect
Packet inspection statistics [process switch:fast switch] tcp packets: [413:51589] udp packets:
[74:28] icmp packets: [0:8] ftp packets: [23:0] tftp packets: [3:0] tftp-data packets: [6:28]
skinny packets: [238:0] Session creations since subsystem startup or last reset 39 Current
session counts (estab/half-open/terminating) [3:0:0] Maxever session counts (estab/half-
open/terminating) [3:4:1] Last session created 00:00:20 Last statistic reset never Last session
creation rate 2 Maxever session creation rate 7 Last half-open session total 0 Class-map: class-
default (match-any) Match: any Drop (default action) 0 packets, 0 bytes
```

それに比べて、アプリケーション固有のクラスを追加する類似の設定は、より細かいアプリケーション統計情報と制御を提供し、また、ポリシーマップの最後のチャンスとして ACL だけを照合する最後のチャンスのクラスマップを定義することで最初の例に表示されたのと同じ幅のサービスを引き続き提供します。

```
class-map type inspect match-all all-private
 match access-group 101
class-map type inspect match-all private-ftp
 match protocol ftp
 match access-group 101
class-map type inspect match-any netbios
 match protocol msrpc
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
class-map type inspect match-all private-netbios
```

```
 match class-map netbios
 match access-group 101
class-map type inspect match-all private-ssh
 match protocol ssh
 match access-group 101
class-map type inspect match-all private-http
 match protocol http
 match access-group 101
!
policy-map type inspect priv-pub-pmap
 class type inspect private-http
  inspect
 class type inspect private-ftp
  inspect
 class type inspect private-ssh
  inspect
 class type inspect private-netbios
  inspect
 class type inspect all-private
  inspect
 class class-default!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect priv-pub-pmap
!
interface FastEthernet4
 ip address 172.16.108.44 255.255.255.0
 zone-member security public
!
interface Vlan1
 ip address 192.168.108.1 255.255.255.0
 zone-member security private
!
access-list 101 permit ip 192.168.108.0 0.0.0.255 any
```

より詳細な設定は、**show policy-map type inspect zone-pair priv-pub** コマンドに対して次の下位の細かい出力を提供します。

```
stg-871-L#sh policy-map type insp zone-pair priv-pub Zone-pair: priv-pub Service-policy inspect
: priv-pub-pmap Class-map: private-http (match-all) Match: protocol http Match: access-group 101
Inspect Packet inspection statistics [process switch:fast switch] tcp packets: [0:2193] Session
creations since subsystem startup or last reset 731 Current session counts (estab/half-
open/terminating) [0:0:0] Maxever session counts (estab/half-open/terminating) [0:3:0] Last
session created 00:29:25 Last statistic reset never Last session creation rate 0 Maxever session
creation rate 4 Last half-open session total 0 Class-map: private-ftp (match-all) Match:
protocol ftp Inspect Packet inspection statistics [process switch:fast switch] tcp packets:
[86:167400] ftp packets: [43:0] Session creations since subsystem startup or last reset 7
Current session counts (estab/half-open/terminating) [0:0:0] Maxever session counts (estab/half-
open/terminating) [2:1:1] Last session created 00:42:49 Last statistic reset never Last session
creation rate 0 Maxever session creation rate 4 Last half-open session total 0 Class-map:
private-ssh (match-all) Match: protocol ssh Inspect Packet inspection statistics [process
switch:fast switch] tcp packets: [0:62] Session creations since subsystem startup or last reset
4 Current session counts (estab/half-open/terminating) [0:0:0] Maxever session counts
(estab/half-open/terminating) [1:1:1] Last session created 00:34:18 Last statistic reset never
Last session creation rate 0 Maxever session creation rate 2 Last half-open session total 0
Class-map: private-netbios (match-all) Match: access-group 101 Match: class-map match-any
netbios Match: protocol msrpc 0 packets, 0 bytes 30 second rate 0 bps Match: protocol netbios-
dgm 0 packets, 0 bytes 30 second rate 0 bps Match: protocol netbios-ns 0 packets, 0 bytes 30
second rate 0 bps Match: protocol netbios-ssn 2 packets, 56 bytes 30 second rate 0 bps Inspect
Packet inspection statistics [process switch:fast switch] tcp packets: [0:236] Session creations
since subsystem startup or last reset 2 Current session counts (estab/half-open/terminating)
[0:0:0] Maxever session counts (estab/half-open/terminating) [1:1:1] Last session created
00:31:32 Last statistic reset never Last session creation rate 0 Maxever session creation rate 1
```

```
Last half-open session total 0 Class-map: all-private (match-all) Match: access-group 101
Inspect Packet inspection statistics [process switch:fast switch] tcp packets: [51725:158156]
udp packets: [8800:70] tftp packets: [8:0] tftp-data packets: [15:70] skinny packets: [33791:0]
Session creations since subsystem startup or last reset 2759 Current session counts (estab/half-
open/terminating) [2:0:0] Maxever session counts (estab/half-open/terminating) [2:6:1] Last
session created 00:22:21 Last statistic reset never Last session creation rate 0 Maxever session
creation rate 12 Last half-open session total 0 Class-map: class-default (match-any) Match: any
Drop (default action) 4 packets, 112 bytes
```

より細かいクラスマップとポリシーマップの設定を使用するその他のメリットは、前述のように、セッションとレート値にクラス固有の制限を適用する可能性と、各クラスの検査動作を調整するためにパラメータマップを適用することによって検査パラメータを調整する可能性です。

ゾーンベース ポリシー ファイアウォール ポリシーマップの設定

ポリシーマップは、1 つ以上のクラスマップにファイアウォール ポリシー アクションを適用して、セキュリティ ゾーンペアに適用されるサービスポリシーを定義します。 inspect タイプのポリシーマップが作成されるときに、class class-default という名前のデフォルト クラスがクラスの最後で適用されます。 class class-default のデフォルト ポリシー アクションは廃棄ですが、通過に変更できます。 log オプションに廃棄アクションを追加することもできます。 inspect は class class-default には適用できません。

ゾーンベース ポリシー ファイアウォール アクション

ZFW は、あるゾーンから別のゾーンに移動するトラフィックに 3 つのアクションを提供します。

- **廃棄（drop）**：これは、すべての inspect タイプ ポリシーマップを終了させる「class class-default」によって適用される、すべてのトラフィックに対するデフォルトのアクションです。 ポリシーマップ内の他のクラスマップは、不必要なトラフィックを廃棄するためにも設定できます。 廃棄アクションによって処理されるトラフィックは ZFW によって「静かに」廃棄され（廃棄の通知が対応するエンドホストに送信されない）、これは、拒否されたトラフィックを送信したホストに ICMP の「host unreachable」メッセージを送信する ACL の動作とは逆です。 現在、「静かに廃棄する」動作を変更するオプションはありません。 log オプションには、トラフィックがファイアウォールによって廃棄されたという syslog 通知用の廃棄を追加できます。
- **通過（pass）**：このアクションは、1 つのゾーンから別のゾーンにトラフィックを転送することをルータに許可します。 通過アクションは、トラフィック内の接続またはセッションの状態を追跡しません。 通過は、一方向のトラフィックだけを許可します。 逆の方向でリターン トラフィックが通過することを許可するように、対応するポリシーを適用する必要があります。 通過アクションは、IPSec ESP、IPSec AH、ISAKMP、予測可能な動作を含む他の本質的にセキュアなプロトコルなどのプロトコルには便利です。 しかし、ほとんどのアプリケーション トラフィックは検査アクションを指定したほうが ZFW でより適切に処理されます。
- **検査（inspect）**：検査アクションは、状態ベースでトラフィックを制御します。 たとえば、前述のサンプル ネットワークにあるプライベート ゾーンからインターネット ゾーンへのトラフィックが検査された場合、ルータは TCP および User Datagram Protocol（UDP; ユーザ データグラム プロトコル）トラフィック用の接続またはセッションの情報を維持します。 そのため、ルータは、プライベート ゾーン接続要求の応答でインターネットゾーン ホストから送信されるリターン トラフィックを許可します。 また、脆弱性または機密性のあるアプリケーション トラフィックを含む可能性のある特定のサービス プロトコルを、アプリケーション検査および制御の対象にすることもできます。 監査証跡は、接続/セッションの開始、停止、

期間、転送されるデータ ボリューム、および送信元と宛先のアドレスを記録するためにパラメータマップで適用できます。

アクションは、ポリシーマップ内のクラスマップと関連付けられます。

```
conf t
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [service-parameter-map]
```

パラメータマップは、指定されたクラスマップの検査ポリシー用の接続パラメータを変更するオプションを提供します。

ゾーンポリシー ファイアウォール パラメータマップの設定

パラメータマップは、ZFW 用の検査動作、DoS 保護、TCP 接続/UDP セッション タイマー、および監査証跡ロギング設定などのパラメータを指定します。 また、パラメータマップは、HTTP オブジェクト、POP3 および IMAP 認証要件、および他のアプリケーション固有の情報などのアプリケーション固有の動作を定義するために、レイヤ 7 クラスとポリシーマップで適用されます。

ZFW 用の検査パラメータマップは、他の ZFW クラスとポリシーオブジェクトに似た **type inspect** として設定されます。

```
stg-871-L(config)#parameter-map type inspect z1-z2-pmap stg-871-L(config-profile)#? parameter-map commands: alert Turn on/off alert audit-trail Turn on/off audit trail dns-timeout Specify timeout for DNS exit Exit from parameter-map icmp Config timeout values for icmp max-incomplete Specify maximum number of incomplete connections before clamping no Negate or set default values of a command one-minute Specify one-minute-sample watermarks for clamping sessions Maximum number of inspect sessions tcp Config timeout values for tcp connections udp Config timeout values for udp flows
```

パラメータマップの特定のタイプは、レイヤ 7 アプリケーション検査ポリシーによって適用されたパラメータを指定します。 regex タイプのパラメータマップは、正規表現でトラフィックをフィルタリングする HTTP アプリケーション検査で使用するための正規表現を定義します。

```
parameter-map type regex [parameter-map-name]
```

protocol-info タイプのパラメータマップは、インスタント メッセージ アプリケーション検査で使用するためにサーバ名を定義します。

```
parameter-map type protocol-info [parameter-map-name]
```

HTTP および IM アプリケーション検査用の設定詳細一式は、このドキュメントの対応するアプリケーション検査セクションで提供します。

DoS 保護の調整は、このドキュメントの後のセクションで説明します。

アプリケーション検査の設定は、このドキュメントの後のセクションで説明します。

ゾーンベース ポリシー ファイアウォールのポリシーに対する口ギングの適用

ZFW は、デフォルトで廃棄または検査されるトラフィック、または設定されたファイアウォール ポリシー アクションに対して口ギング オプションを提供します。 ZFW が検査するトラフィックには、監査証跡口ギングが利用できます。 監査証跡は、パラメータマップに audit-trail を定義し、ポリシーマップの検査アクションにパラメータマップを適用することで適用されます。

```
conf t
 policy-map type inspect z1-z2-pmap
```

```
  class type inspect service-cmap
   inspect|drop|allow [parameter-map-name (optional)]
```

廃棄ロギングは、ZFW が廃棄するトラフィックで利用可能です。 廃棄ロギングは、ポリシーマップの廃棄アクションにログを追加することで設定されます。

```
conf t
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [service-parameter-map]
```

ゾーンポリシー ファイアウォール クラスマップおよびポリシーマップの編集

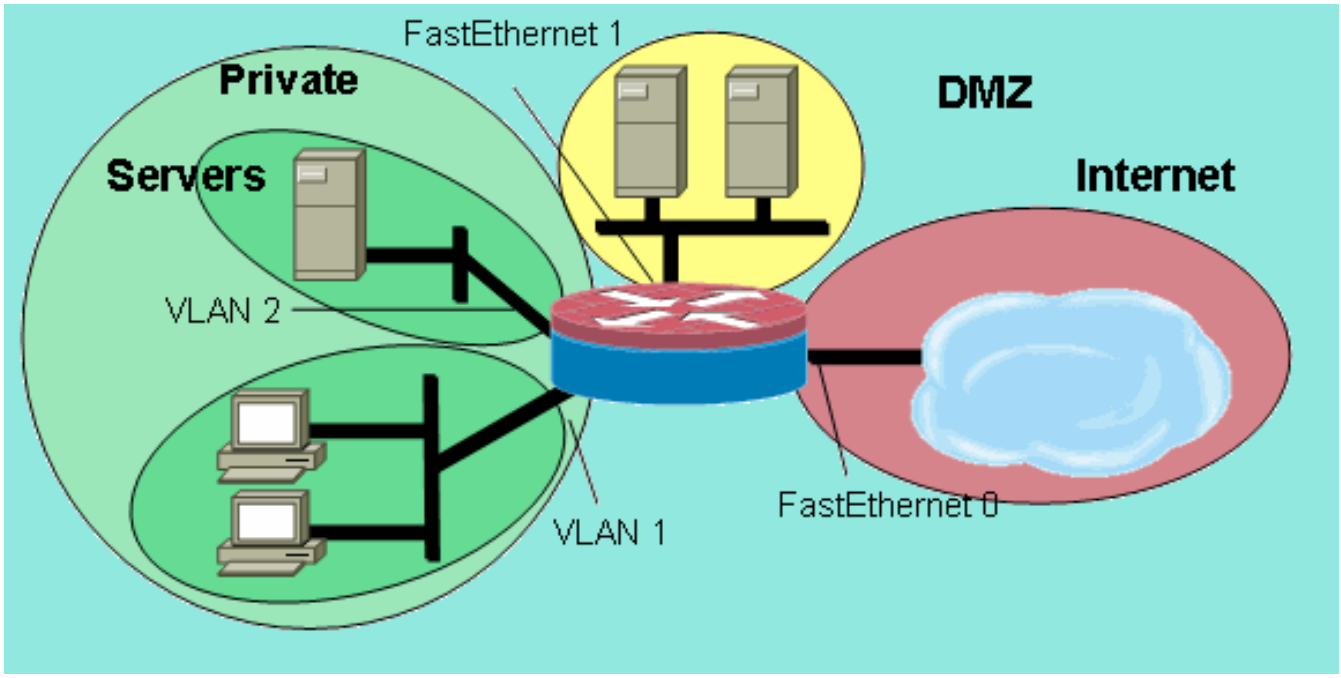
現在、ZFW は、ポリシーマップ、クラスマップ、パラメータマップなどのさまざまな ZFW 構造を変更できるエディタは組み込んでいません。 クラスマップまたはアクション アプリケーション内の match 文をポリシーマップ内に含まれるさまざまなクラスマップに再調整するために、次のステップを実行する必要があります。

1. 既存の構造を Microsoft Windows のメモ帳などのテキスト エディタまたは Linux/Unix プラットフォームの vi などのエディタにコピーします。
2. 既存の構造をルータの設定から削除します。
3. 構造をテキスト エディタで編集します。
4. 編集した構造をルータの CLI にコピーし戻します。

設定例

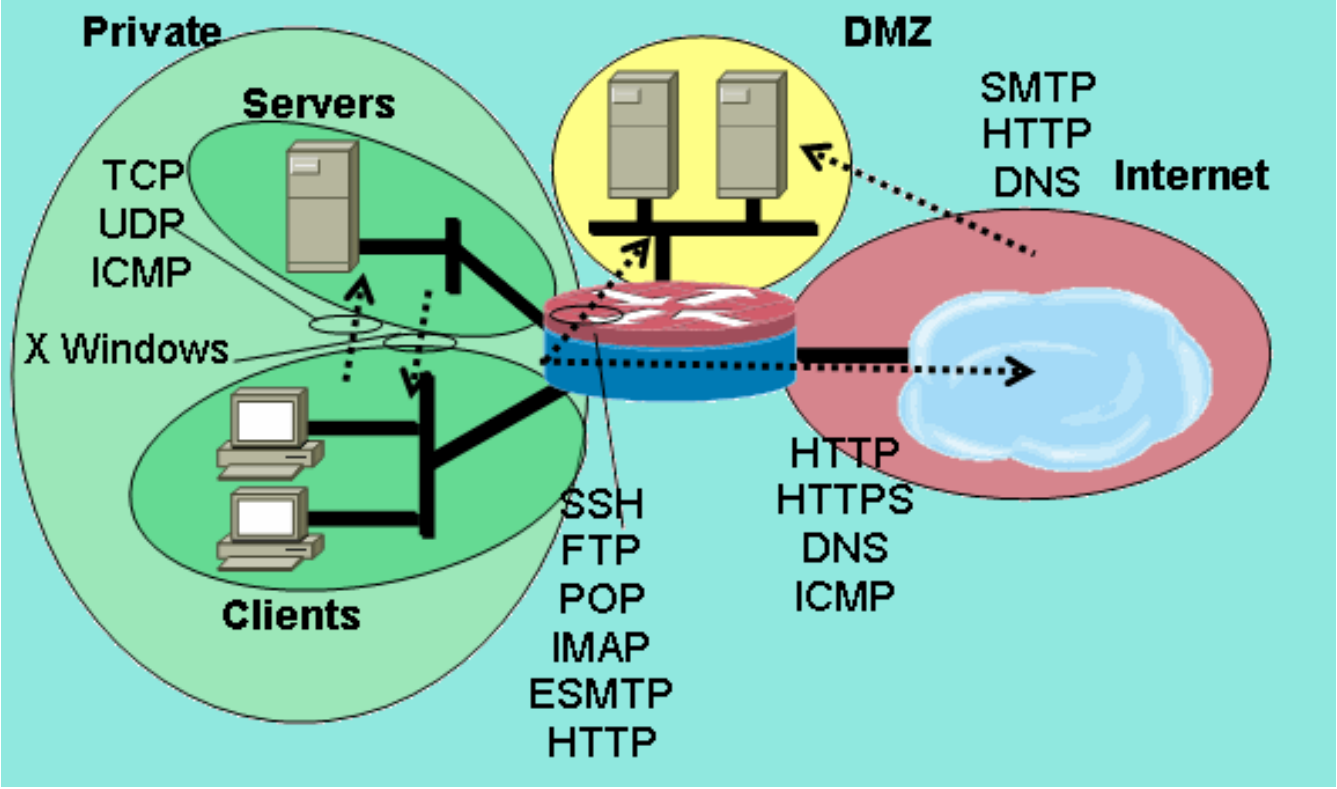
この設定例では、Cisco 1811 Integrated Services Router（ISR; サービス統合型ルータ）を使用しています。 IP 接続、VLAN 設定、2 つのプライベート イーサネット LAN セグメント間のトランスペアレント ブリッジの基本的な設定については、「付録 A」を参照してください。 ルータは次のように 5 つのゾーンに分けられます。

- パブリック インターネットは FastEthernet 0（インターネット ゾーン）に接続されています。
- 2 つのインターネット サーバは FastEthernet 1（DMZ ゾーン）に接続されています。
- イーサネット スイッチは次の 2 つの VLAN で設定されています。ワークステーションは VLAN1（クライアント ゾーン）に接続されています。サーバは VLAN2（サーバ ゾーン）に接続されています。クライアントとサーバのゾーンは同じサブネット内にあります。 トランスペアレント ファイアウォールは、ゾーン間に適用されるので、それら 2 つのインターフェイスのゾーン間ポリシーは、クライアント ゾーンとサーバ ゾーンの間のトラフィックにだけ影響します。
- VLAN1 と VLAN2 のインターフェイスは、ブリッジ仮想インターフェイス（BVI1）経由で他のネットワークと通信します。 このインターフェイスはプライベート ゾーンに割り当てられます（図 2 を参照してください）**図 2： ゾーン トポロジ詳細**



これらのポリシーは、以前に定義されたネットワーク ゾーンを使用して適用されます。

- インターネット ゾーン内のホストは、DMZ 内の 1 つのサーバ上の DNS、SMTP、および SSH サービスに到達できます。 もう 1 つのサーバは、SMTP、HTTP、および HTTPS のサービスを提供します。 ファイアウォール ポリシーは、各ホスト上で利用可能な具体的なサービスへのアクセスを制限します。
- DMZ ホストは、他のいずれのゾーンにあるホストにも接続できません。
- クライアント ゾーンのホストは、すべての TCP、UDP、ICMP サービスでサーバ ゾーンのホストに接続できます。
- サーバ ゾーン内のホストは、クライアント ゾーン内のホストには接続できません。ただし、例外的に、UNIX ベースのアプリケーション サーバは、X Windows クライアント セッションを、クライアント ゾーン内のデスクトップ PC の X Windows サーバへとポート 6900 ~ 6910 で開くことができます。
- プライベート ゾーン内のすべてのホスト（クライアントとサーバの組み合わせ）は、SSH、FTP、POP、IMAP、ESMTP、HTTP のサービス上の DMZ のホストと、HTTP、HTTPS、および DNS のサービスと ICMP 上のインターネット ゾーン内のホストにアクセスできます。さらには、サポートされるインターネット メッセージと P2P アプリケーションがポート 80 では運搬されないことを確実にするために、アプリケーション検査がプライベート ゾーンからインターネット ゾーンまでの HTTP 接続に適用されます（図 3.参照して下さい）**図 3：設定例に適用されるゾーンペア サービス権限**



これらのファイアウォール ポリシーは複雑度の順番で設定されます。

1. クライアントとサーバの TCP/UDP/ICMP 検査
2. プライベートと DMZ の SSH/FTP/POP/IMAP/ESMTP/HTTP 検査
3. ホスト アドレスで制限される インターネットと DMZ の SMTP/HTTP/DNS 検査
4. Port-Application Mapping (PAM; ポートアプリケーション マッピング) で指定されたサービスを伴うサーバとクライアントの X Windows 検査
5. HTTP アプリケーション検査を伴うプライベートとインターネットの HTTP/HTTPS/DNS/ICMP

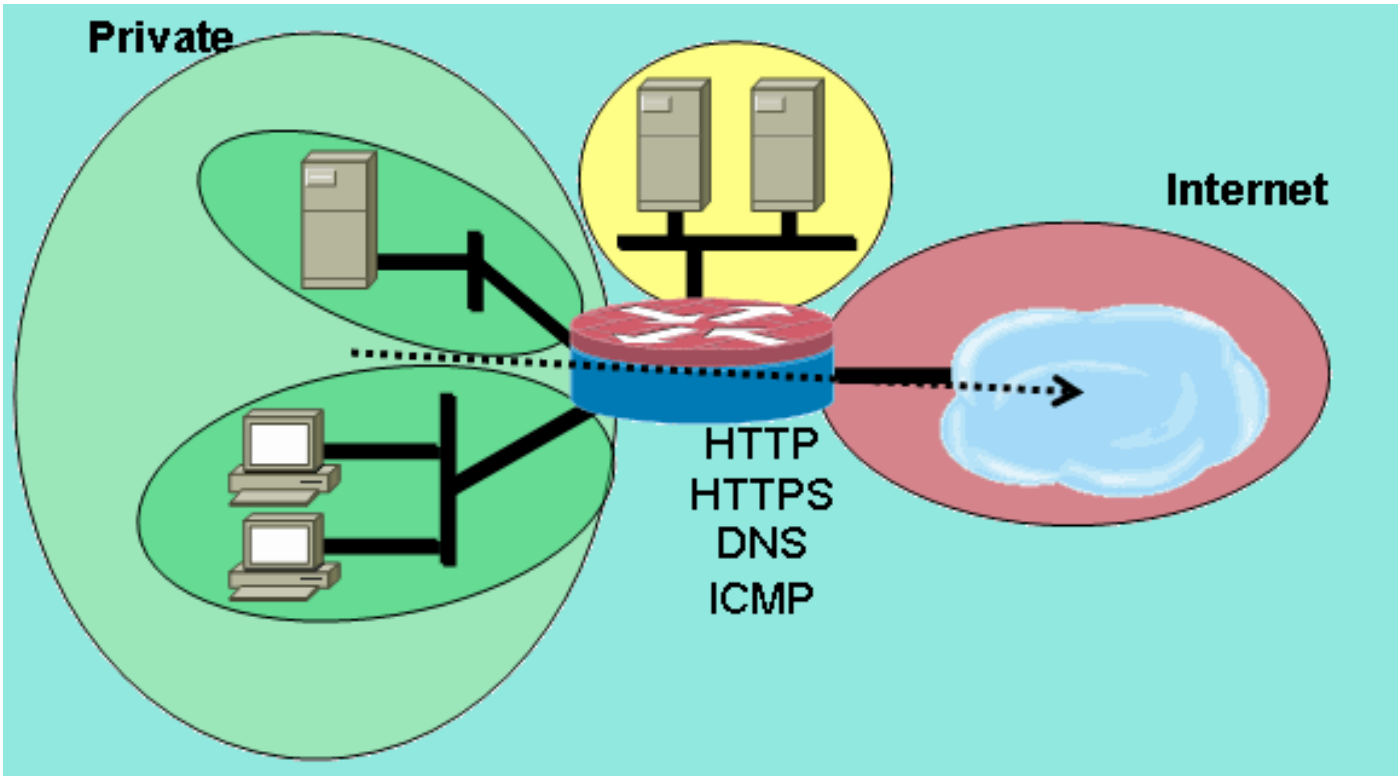
設定の部分を適用するのは異なる時で異なるネットワーク セグメントであるため、ネットワーク セグメントがゾーンに配置されたときには他のセグメントへの接続を失うと覚えておくことが重要です。 たとえば、プライベート ゾーンが設定されるときには、プライベート ゾーン内のホストは、対応するポリシーが定義されるまで DMZ ゾーンとインターネット ゾーンへの接続を失います。

ステートフル検査ルーティング ファイアウォール

プライベート インターネット ポリシーの設定

図 4 は、プライベート インターネット ポリシーの設定を示しています。

図 4 : プライベート ゾーンからインターネット ゾーンへのサービス検査



プライベート インターネット ポリシーは、プライベート ゾーンからインターネット ゾーンへの ICMP 用の HTTP、HTTPS、DNS、およびレイヤ 4 検査を適用します。 これによって、プライベート ゾーンからインターネット ゾーンへの接続が許可され、また、リターン トラフィックが許可されます。 レイヤ 7 検査は、より堅牢なアプリケーション制御、より良いセキュリティ、フィックスアップを必要とするアプリケーションのサポートのメリットを含んでいます。 ただし、検査用には設定されていないレイヤ 7 プロトコルはゾーン間では許可されないので、前述のようにレイヤ 7 検査はネットワーク アクティビティについて詳しく理解していることを必要とします。

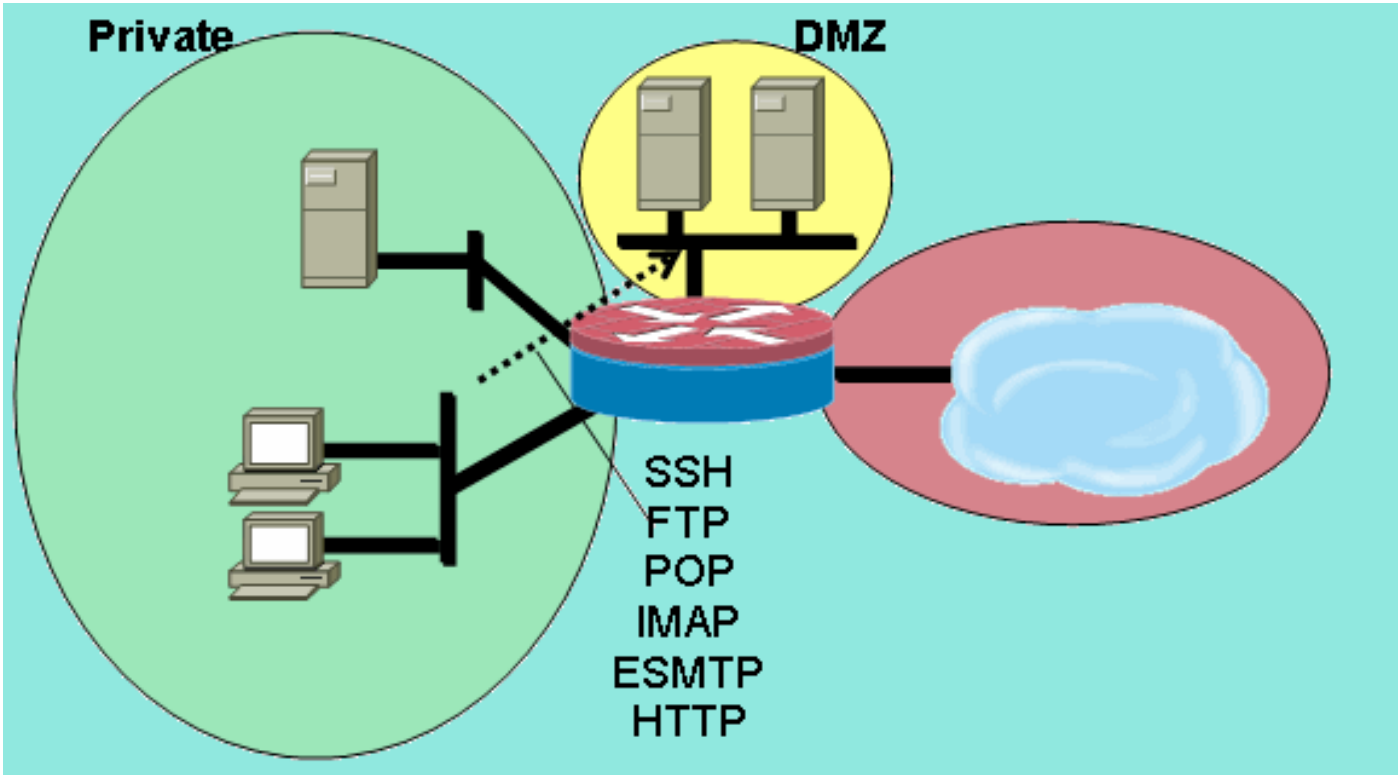
1. 前述したポリシーに従い、ゾーン間で許可したいトラフィックを説明するクラスマップを定義します。conf t
```
 class-map type inspect match-any internet-traffic-class
  match protocol http
  match protocol https
  match protocol dns
  match protocol icmp
```
2. 定義したばかりのクラスマップにトラフィックを検査するポリシーマップを設定します。
```
conf t
 policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
```
3. プライベート ゾーンとインターネット ゾーンを設定し、それぞれのゾーンにルータ インターフェイスを割り当てます。conf t
```
zone security private
zone security internet
int bvi1
zone-member security private
int fastethernet 0
zone-member security internet
```
4. ゾーンペアを設定し、適切なポリシーマップを適用します。**注:** 必要な操作は、プライベート ゾーンを送信元としてインターネット ゾーンに転送される接続を検査するために、現在のプライベート インターネット ゾーン ペアを設定することだけです。conf t
```
 zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
```
これは、プライベートとインターネットのゾーンペア上にレイヤ 7 検査ポリシーの設定を完了して、クライアント ゾーンからサ

ーバ ゾーンに HTTP、HTTPS、DNS、ICMP 接続を許可して、不必要なトラフィックが HTTP のサービス ポートである TCP 80 上を通過させないことを確実にするためにアプリケーション検査を HTTP トラフィックに適用します。

プライベート DMZ ポリシーの設定

図 5 は、プライベート DMZ ポリシーの設定を示しています。

図 5： プライベート ゾーンから DMZ ゾーンへのサービス検査



プライベート DMZ ポリシーは、ゾーン間のネットワーク トラフィックを詳しく理解することが必要なので、複雑度が増します。 このポリシーは、プライベート ゾーンから DMZ へとレイヤ 7 検査を適用します。 これによって、プライベート ゾーンから DMZ への接続が許可され、また、リターン トラフィックが許可されます。 レイヤ 7 検査は、より堅牢なアプリケーション制御、より良いセキュリティ、フィックスアップを必要とするアプリケーションのサポートのメリットを含んでいます。 ただし、検査用には設定されていないレイヤ 7 プロトコルはゾーン間では許可されないので、前述のようにレイヤ 7 検査はネットワーク アクティビティについて詳しく理解していることを必要とします。

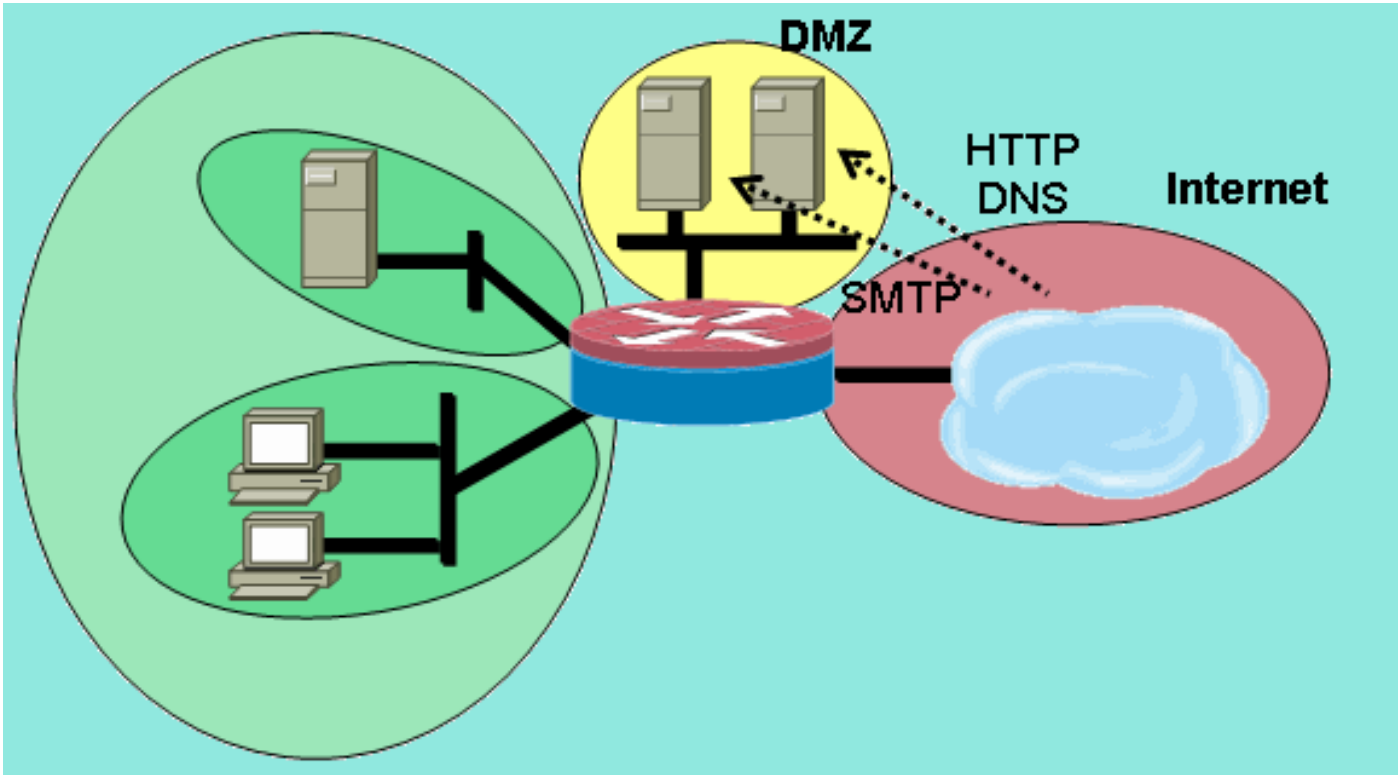
1. 前述したポリシーに従い、ゾーン間で許可したいトラフィックを説明するクラスマップを定義します。`conf t`
```
 class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol pop
  match protocol imap
  match protocol esmtp
  match protocol http
```
2. 先ほど定義したクラスマップにトラフィックを検査するポリシーマップを設定します。`conf t`
```
 policy-map type inspect private-dmz-policy
  class type inspect L7-inspect-class
   inspect
```

3. プライベート ゾーンと DMZ ゾーンを設定し、それぞれのゾーンにルータ インターフェイスを割り当てます。conf t
```
zone security private
zone security dmz
int bvi1
zone-member security private
int fastethernet 1
zone-member security dmz
```
4. ゾーンペアを設定し、適切なポリシーマップを適用します。**注:** 必要な操作は、プライベート ゾーンを送信元として DMZ に転送される接続を検査するために、現在のプライベート DMZ ゾーンペアを設定することだけです。conf t
```
 zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
```
これによって、プライベート DMZ 上のレイヤ 7 検査ポリシーの設定が完了し、クライアント ゾーンからサーバ ゾーンへのすべての TCP、UDP、ICMP 接続が許可されます。 ポリシーは下位チャネルにはフィックスアップを適用しませんが、ほとんどのアプリケーション接続に対処するシンプルなポリシーの例を提供します。

インターネット DMZ ポリシーの設定

図 6 は、インターネット DMZ ポリシーの設定を示しています。

図 6： インターネット ゾーンから DMZ ゾーンへのサービス検査



このポリシーは、インターネット ゾーンから DMZ へのレイヤ 7 検査を適用します。 これは、インターネット ゾーンから DMZ への接続を許可し、DMZ ホストから接続を発信したインターネット ホストへのリターン トラフィックを許可します。 インターネット DMZ ポリシーは、特定のホスト、ホストのグループ、またはサブネットの特定のサービスへのアクセスを制限するために、ACL で定義されているアドレス グループとレイヤ 7 検査を組み合わせます。 これは、IP アドレスを指定するために ACL を参照している別のクラスマップ内のサービスを指定するクラスマップをネストすることによって実現されます。

1. 前述したポリシーに従い、ゾーン間で許可したいトラフィックを説明するクラスマップと ACL を定義します。異なるアクセス ポリシーが 2 つの異なるサーバへのアクセスに適用されるので、サービス用の複数のクラスマップを使用する必要があります。 インターネット ホストは 172.16.2.2 への DNS および HTTP 接続に許可され、SMTP 接続は 172.16.2.3 に許可されます。 クラスマップ内の違いに注意してください。 サービスを指定するクラスマップは、リストされている任意のサービスを許可するために **match-any** キーワードを使用します。 ACL をサービス クラスマップに関連付けるクラスマップは、**match-all** キーワードを使用することで、クラスマップ内の両方の状態がトラフィックを許可するように必ず一致することを要求します。`conf t`

```
access-list 110 permit ip any host 172.16.2.2
access-list 111 permit ip any host 172.16.2.3
class-map type inspect match-any dns-http-class
 match protocol dns
 match protocol http
class-map type inspect match-any smtp-class
 match protocol smtp
class-map type inspect match-all dns-http-acl-class
 match access-group 110
 match class-map dns-http-class
class-map type inspect match-all smtp-acl-class
 match access-group 111
 match class-map smtp-class
```

2. 先ほど定義したクラスマップにトラフィックを検査するポリシーマップを設定します。`conf t`

```
policy-map type inspect internet-dmz-policy
 class type inspect dns-http-acl-class
  inspect
 class type inspect smtp-acl-class
  inspect
```

3. インターネット ゾーンと DMZ ゾーンを設定し、それぞれのゾーンにルータ インターフェイスを割り当てます。 以前のセクションで設定済みの場合、DMZ 設定は省略します。`conf t`

```
zone security internet
zone security dmz
int fastethernet 0
 zone-member security internet
int fastethernet 1
 zone-member security dmz
```

4. ゾーンペアを設定し、適切なポリシーマップを適用します。**注:** インターネット ゾーンから発信されて DMZ ゾーンに移動する接続を検査するために必要なのは、現在のインターネット DMZ ゾーン ペアを設定することだけです。`conf t`

```
zone-pair security internet-dmz source internet destination dmz
 service-policy type inspect internet-dmz-policy
```

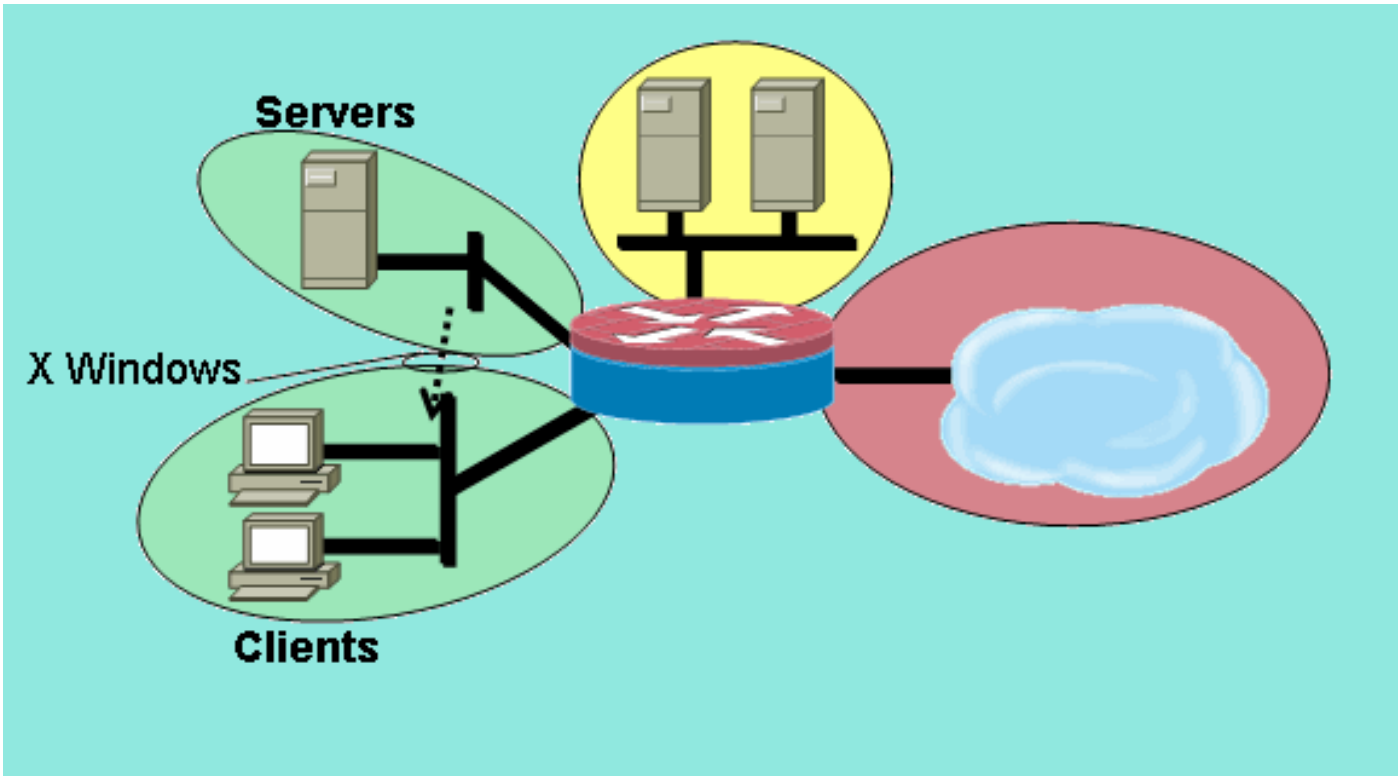
これによって、インターネット DMZ ゾーンペア上のアドレス固有のレイヤ 7 検査ポリシーの設定が完了します。

ステートフル検査トランスペアレント ファイアウォール

サーバ クライアント ポリシーの設定

図 7 は、サーバ クライアント ポリシーの設定を示しています。

図 7： サーバ ゾーンからクライアント ゾーンへのサービス検査



サーバ クライアント ポリシーは、ユーザ定義のサービスを使った検査を適用します。 レイヤ 7 検査は、サーバ ゾーンからクライアント ゾーンに適用されます。 これによって、サーバ ゾーンからクライアント ゾーンへの特定のポートへの X Windows 接続が許可され、また、リターン トラフィックも許可されます。 X Windows は、PAM で本来サポートされているプロトコルではないので、PAM のユーザ設定サービスを定義して ZFW が適切なトラフィックを認識して検査できるようにする必要があります。

2 つ以上のルータ インターフェイスが Integrated Routing and Bridging（IRB）を提供するために IEEE ブリッジグループで設定されて、Bridge Virtual Interface（BVI; ブリッジ仮想インターフェイス）経由でブリッジグループ内のインターフェイス間をブリッジすることと、他のサブネットへのルーティングすることを提供します。 トランスペアレント ファイアウォール ポリシーは、「ブリッジを通過する」トラフィックには適用ファイアウォール検査を提供しますが、BVI 経由でブリッジグループを離れるトラフィックには提供しません。 検査ポリシーは、ブリッジグループを通過するトラフィックだけに適用されます。 そのため、このシナリオでは、検査は、プライベート ゾーンの内部にネストされるクライアント ゾーンとサーバ ゾーンの間を移動するトラフィックにだけ適用されます。 プライベート ゾーン、パブリック ゾーン、および DMZ ゾーンの間に適用されるポリシーは、トラフィックが BVI 経由でブリッジグループを離れるときにだけ関与します。 トラフィックが BVI 経由でクライアント ゾーンまたはサーバ ゾーンから離れるときには、トランスペアレント ファイアウォール ポリシーは起動されません。

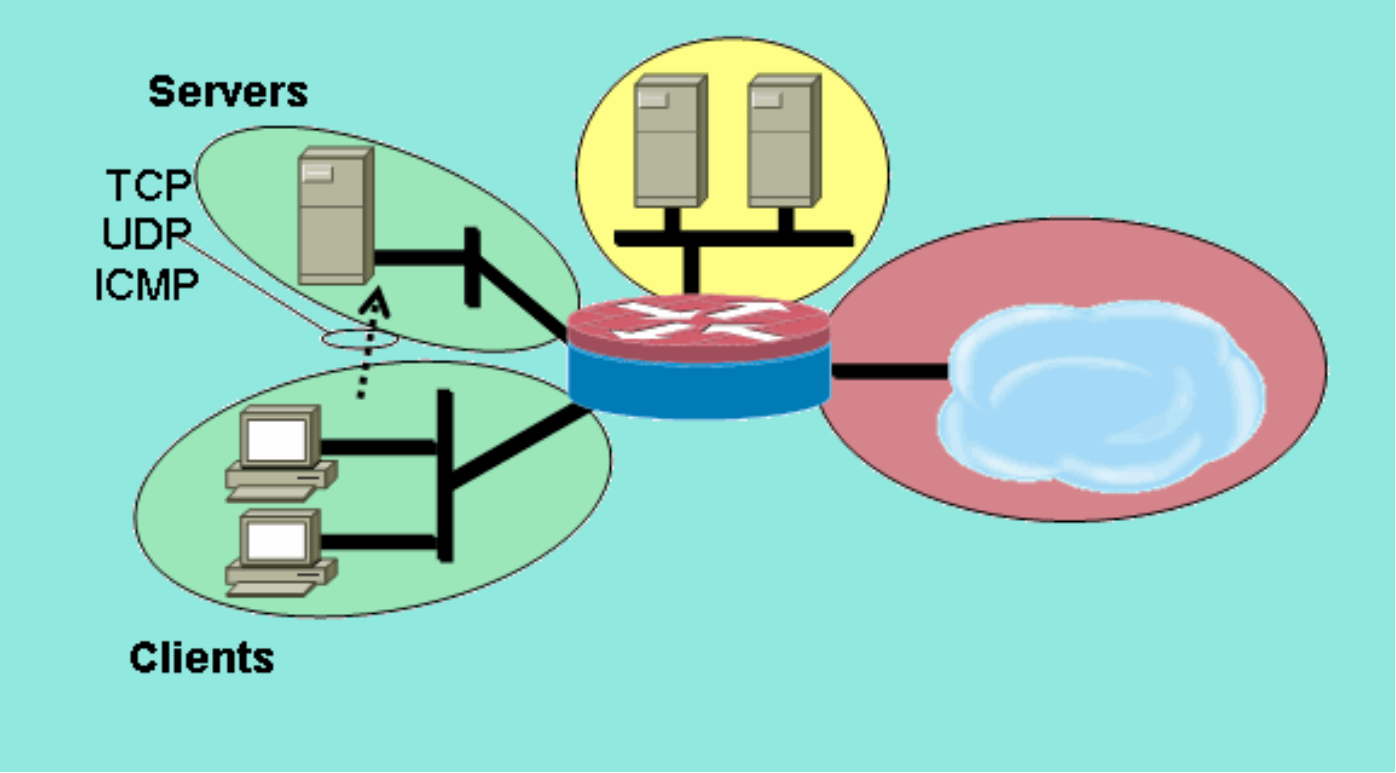
1. X Windows 用のユーザ定義エントリで PAM を設定します。X Windows クライアント（アプリケーションが存在する場所）は、ポート 6900 から始まる範囲でクライアント（ユーザが作業をしている場所）に情報を表示する接続を開きます。追加される各接続は連続するポートを使用するので、クライアントが 1 つのホストで 10 の異なるセッションを表示する場合、サーバはポート 6900 ~ 6909 を使用します。 そのため、6900 ~ 6909 の範囲のポートを検査する場合、6909 よりも上のポートに対して開かれた接続は失敗します。`conf t ip port-map user-Xwindows port tcp from 6900 to 6910`
2. 追加の PAM の質問に対処するには PAM のドキュメントを参照し、また、PAM と Cisco IOS Firewall ステートフル検査の間の相互運用性の詳細は、細かいプロトコル検査のドキュメントを確認してください。
3. 前述したポリシーに従い、ゾーン間で許可したいトラフィックを説明するクラスマップを定

義します。conf t
```
 class-map type inspect match-any Xwindows-class
  match protocol user-Xwindows
```
4. 先ほど定義したクラスマップにトラフィックを検査するポリシーマップを設定します。conf t
```
 policy-map type inspect servers-clients-policy
  class type inspect Xwindows-class
   inspect
```
5. クライアント ゾーンとサーバ ゾーンを設定し、それぞれのゾーンにルータ インターフェイスを割り当てます。これらのゾーンを設定して、クライアント サーバ ポリシー設定セクションにインターフェイスを割り当てた場合、ゾーンペア定義に直接進みます。 IRB 設定のブリッジは、完全性のために提供されます。conf t
```
bridge irb
bridge 1 protocol ieee
bridge 1 route ip
zone security clients
zone security servers
 int vlan 1
 bridge-group 1
 zone-member security clients
int vlan 2
 bridge-group 1
 zone-member security servers
```
6. ゾーンペアを設定し、適切なポリシーマップを適用します。**注:** 必要な操作は、サーバ ゾーンを送信元としてクライアント ゾーンに転送される接続を検査するために、現在のサーバ クライアント ゾーン ペアを設定することだけです。conf t
```
 zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
```
これによって、サーバ クライアント ゾーンペアのユーザ定義検査ポリシーの設定が完了して、サーバ ゾーンからクライアント ゾーンへの X Windows 接続が許可されます。

クライアント サーバ ポリシーの設定

図 8 は、クライアント サーバ ポリシーの設定を示しています。

図 8： クライアント ゾーンからサーバ ゾーンへのサービス検査



クライアント サーバ ポリシーは、他のポリシーよりも複雑度が低くなっています。 レイヤ 4 検査は、クライアント ゾーンからサーバ ゾーンに適用されます。 これによって、クライアント ゾーンからサーバ ゾーンへの接続が許可され、また、リターン トラフィックが許可されます。 レイヤ 4 検査は、ほとんどのアプリケーション トラフィックを許可するために 2、3 の規則だけが必要であるという、ファイアウォール設定の単純さのメリットを備えています。 ただし、レイヤ 4 検査は、次のような 2 つの大きな欠点も備えています。

- FTP やストリーミング メディア サービスなどのアプリケーションは、サーバからクライアントへの追加の下位チャネルと頻繁にネゴシエートします。 この機能は、通常はコントロール チャネル ダイアログを監視し、下位のチャネルを許可するサービス フィックスアップで対処されます。 この機能は、レイヤ 4 検査では利用できません。
- レイヤ 4 検査では、ほとんどすべてのアプリケーションレイヤ トラフィックが許可されます。 2、3 のアプリケーションだけがファイアウォールの通過を許可されるようにネットワークの用途を制御する必要がある場合、ACL はファイアウォール経由で許可されるサービスを限定するための発信トラフィックに設定する必要があります。

両方のルータ インターフェイスは IEEE ブリッジ グループで設定されるので、このファイアウォール ポリシーはトランスペアレント ファイアウォール検査に適用されます。 このポリシーは、IEEE IP ブリッジ グループの 2 つのインターフェイスに適用されます。 検査ポリシーは、ブリッジ グループを通過するトラフィックにだけ適用されます。 これが、クライアント ゾーンとサーバ ゾーンがプライベート ゾーン内部にネストされる理由です。

1. 前述したポリシーに従い、ゾーン間で許可したいトラフィックを説明するクラスマップを定義します。conf t
```
 class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
```
2. 先ほど定義したクラスマップにトラフィックを検査するポリシーマップを設定します。conf t
```
 policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
```

3. クライアント ゾーンとサーバ ゾーンを設定し、それぞれのゾーンにルータ インターフェイスを割り当てます。
```
conf t
zone security clients
zone security servers
int vlan 1
zone-member security clients
int vlan 2
zone-member security servers
```
4. ゾーンペアを設定し、適切なポリシーマップを適用します。**注:** クライアント ゾーンから発信されてサーバ ゾーンに移動する接続を検査するために必要なのは、現在のクライアント サーバ ゾーンペアを設定することだけです。
```
conf t
 zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
```
これによって、クライアント ゾーンからサーバ ゾーンへのすべての TCP、UDP、ICMP 接続を許可するクライアントサーバ ゾーンペア用のレイヤ 4 検査ポリシーの設定が完了します。 ポリシーは下位チャネルにはフィックスアップを適用しませんが、ほとんどのアプリケーション接続に対処するシンプルなポリシーの例を提供します。

ゾーンベース ポリシー ファイアウォールのためのレート ポリシング

ネットワーク トラフィックの特定のタイプの転送レートを制限し、より多くのビジネスの基本となる低優先順位のトラフィックを限定する能力によって、データ ネットワークは頻繁にメリットを得ます。 Cisco IOS ソフトウェアは、トラフィック ポリシングのあるこの機能を提供して、それによってトラフィックの名目上のレートとバーストに制限を設けます。 Cisco IOS ソフトウェアは、Cisco IOS リリース 12.1(5)T からトラフィック ポリシングをサポートしています。

Cisco IOS ソフトウェア リリース 12.4(9)T は、トラフィックが 1 つのセキュリティ ゾーンから別のセキュリティ ゾーンに移動するときに、特定のクラスマップの定義と一致するトラフィックをポリシングする機能を追加することで、ZFW をレート限定機能で強化します。 これは、特定のトラフィックを説明し、ファイアウォール ポリシーを適用して、そのトラフィックの帯域幅消費をポリシングする、1 つの設定点を示す利便性を提供します。 ZFW ポリシングは、ポリシー適合性のための転送アクションとポリシー違反のための廃棄アクションだけを提供する点において、インターフェイスベースのポリシングとは異なります。 ZFW ポリシングは、トラフィックを DSCP 用にマーキングできません。

ZFW ポリシングができるのは、バイト/秒、パケット/秒単位で帯域幅を指定することだけであり、帯域幅比率のポリシングは提供されません。 ZFW ポリシングは、インターフェイスベースのポリシングがあってもなくても適用できます。 そのため、追加のポリシング機能が必要とされた場合、これらの機能はインターフェイスベースのポリシングによって適用できます。 インターフェイスベースのポリシングがファイアウォール ポリシングとともに使用された場合、それらのポリシーが競合しないようにする必要があります。

ZFW ポリシングの設定

ZFW ポリシングは、ポリシーマップのクラスマップにあるトラフィックを、1,000 ~ 512,000,000 バイトの範囲の設定可能なバースト値で、8,000 ~ 2,000,000,000 ビット/秒のユーザ定義のレート値に限定します。

ZFW ポリシングは、ポリシーマップの設定の追加の行によって設定可能であり、これはポリシーアクションの後に適用されます。

```
policy-map type inspect private-allowed-policy
```

```
 class type inspect http-class
  inspect
  police rate [bps rate value <8000-2000000000>] burst [value in bytes <1000-512000000>]
```

セッション制御

また、ZFW ポリシーは、クラスマップと一致するポリシーマップでトラフィックのセッション カウントを制限するために、セッション制御も導入しています。 これによって、既存の機能にクラスマップごとの DoS 保護ポリシーを適用することが追加されました。 事実上、これによって、ゾーンペアを通過する任意のクラスマップに一致するいくつものセッションに対して細かい制御を行うことができます。 複数のポリシーマップまたはゾーンペアで同一のクラスマップが使用された場合、さまざまなクラスマップ アプリケーションに異なるセッション制限を適用できます。

セッション制御は、希望するセッション ボリュームを含むパラメータマップを設定して、その後、そのパラメータマップを 1 つのポリシーマップの下の 1 つのクラスマップに適用する検査アクションに追加することで適用されます。

```
parameter-map type inspect my-parameters
 sessions maximum [1-2147483647]

policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect my-parameters
```

パラメータマップは、検査アクションにだけ適用でき、通過アクションまたは廃棄アクションでは利用できません。

ZFW のセッション制御とポリシング アクティビティは、次のコマンドで表示できます。

```
show policy-map type inspect zone-pair
```

アプリケーション検査

アプリケーション検査は、ZFW に追加の機能を導入します。 アプリケーション検査ポリシーは、OSI モデルのレイヤ 7 で適用され、このレイヤではユーザ アプリケーションが、便利な機能を提供できるメッセージを送受信します。 アプリケーションの中には、望ましくない機能または脆弱な機能を提供する可能性があるものもあるので、これらの機能に関連するメッセージは、アプリケーション サービスでのアクティビティを制限するためにフィルタリングする必要があります。

Cisco IOS ソフトウェア ZFW は、次のアプリケーション サービスに対するアプリケーション検査および制御を提供します。

- HTTP
- SMTP
- POP3
- IMAP
- Sun RPC
- P2P アプリケーション トラフィック
- IM アプリケーション

Application inspection and control（AIC; アプリケーション検査および制御）の機能はサービスによってさまざまです。 HTTP 検査は、いくつかのタイプのアプリケーション アクティビティに対して細かいフィルタリングを行い、アプリケーション動作基準への準拠を強制し、このサービス

経由で転送されるコンテンツのタイプを制限するために、転送サイズ、Web アドレス長、ブラウザ アクティビティを制限する機能を提供します。 SMTP 用の AIC は、コンテンツ長を限定してプロトコル準拠を強制できます。 POP3 と IMAP の検査は、ユーザ クレデンシャルを危険にさらさないように、ユーザが安全な認証メカニズムを使用していることを確認できます。

アプリケーション検査は、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の追加のセットとして設定され、そのセットはその後、検査ポリシーマップにアプリケーション サービス ポリシーを定義することによって、既存の検査クラスマップとポリシーマップに適用されます。

HTTP アプリケーション検査

アプリケーション検査は、IM、P2P ファイル共有、TCP 80 経由でファイアウォールが適用されるアプリケーションにリダイレクトできるアプリケーションのトンネリングなど、他のアプリケーションに対する HTTP のサービス ポートの不必要な使用を制御するために HTTP トラフィックに適用できます。

許可された HTTP トラフィックに違反するトラフィックを記述するためにアプリケーション検査クラスマップを設定します。

```
! configure the actions that are not permitted
class-map type inspect http match-any http-aic-cmap
 match request port-misuse any
 match req-resp protocol-violation
! define actions to be applied to unwanted traffic
policy-map type inspect http http-aic-pmap
 class type insp http http-aic-cmap
  reset
  log
! define class-map for stateful http inspection
class-map type inspect match-any http-cmap
 match protocol http
! define class-map for stateful inspection for other traffic
class-map type inspect match-any other-traffic-cmap
 match protocol smtp
 match protocol dns
 match protocol ftp
! define policy-map, associate class-maps and actions
policy-map type inspect priv-pub-pmap
 class type inspect http-cmap
  inspect
  service-policy http http-aic-pmap
 class type inspect other-traffic-cmap
  inspect
```

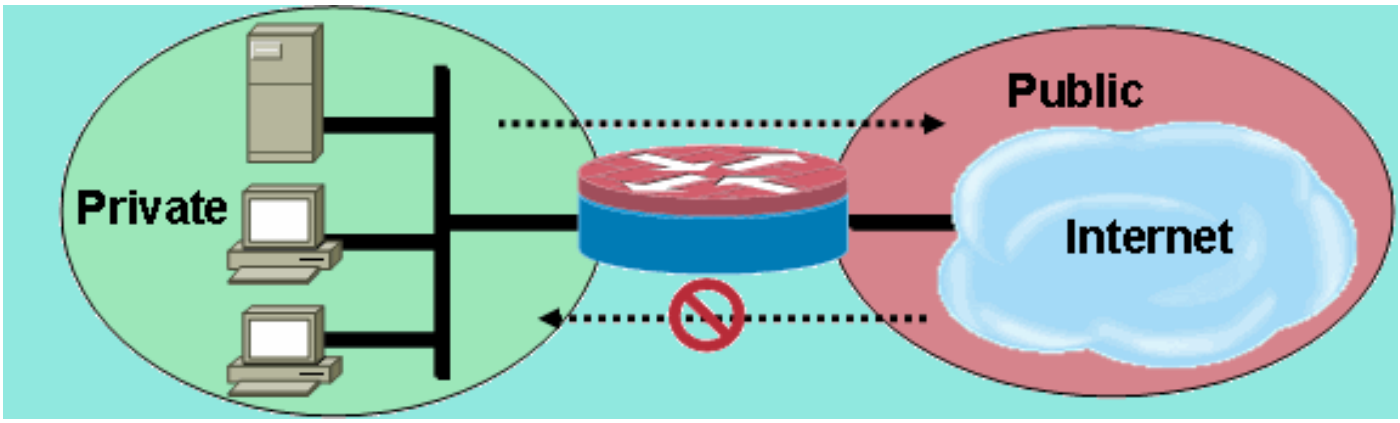
HTTP アプリケーション検査の改良

Cisco IOS ソフトウェア リリース 12.4(9)T は、ZFW の HTTP 検査機能への改良を導入しています。 Cisco IOS Firewall は、Cisco IOS ソフトウェア リリース 12.3(14)T に HTTP アプリケーション検査を導入しています。 Cisco IOS ソフトウェア リリース 12.4(9)T は、次を追加することで既存の機能を補強します。

- ヘッダー名とヘッダー値に基づいて要求と応答を許可、拒否、監視する機能。 これは、脆弱なヘッダー フィールドを含む要求と応答をブロックするには便利です。
- 最大 URL 長、最大ヘッダー長、最大ヘッダー数、最大ヘッダー行長などの HTTP 要求および応答ヘッダー内のさまざまな要素のサイズを制限する機能。 これは、バッファ オーバーフローを避けるには便利です。

- 同一タイプの複数のヘッダーを含む要求と応答をブロックする機能。 たとえば、2 つのコンテンツ長ヘッダーを含む要求などがあります。
- ASCII 以外のヘッダーを含む要求と応答をブロックする機能。 これは、Web サーバにワームやその他の悪意のあるコンテンツを配信しようとする、バイナリや他の ASCII 以外の文字を使用するさまざまな攻撃を防御するのに便利です。
- ユーザ指定のカテゴリに HTTP メソッドをグループ化する機能と、その各グループをブロック/許可/監視する柔軟性が提供されます。 HTTP RFC は、HTTP メソッドの限定されたセットを許可します。 標準メソッドの一部は、Web サーバ上で脆弱性を悪用するために使用される可能性があるので、安全ではないとみなされています。 非標準メソッドの多くには不正なセキュリティ レコードがあります。
- ユーザが設定した正規表現をベースにする特定の URI をブロックするメソッド。 この機能は、カスタム URI とクエリーをブロックする機能をユーザに提供します。
- ユーザがカスタマイズできる文字列でヘッダー タイプ（特にサーバ ヘッダー タイプ）をスプーフィングする機能。 攻撃者が Web サーバ応答を分析し、できるだけ多くの情報を吟味してから、その特定の Web サーバの弱点を悪用する攻撃を開始するような場合に便利です。
- 正規表現としてユーザが入力した値と 1 つ以上の HTTP パラメータ値が一致する場合、HTTP 接続のアラートをブロックするか、発行する機能。 可能な HTTP 値のコンテキストのいくつかには、ヘッダー、本体、ユーザ名、パスワード、ユーザ エージェント、要求行、ステータス行、デコードされた CGI 変数を含んでいます。

HTTP アプリケーション検査の改善の設定例では、次のようにシンプルなネットワークを想定します。



ファイアウォールは、トラフィックを 2 つのクラスにグループ化します。

- HTTP トラフィック
- 他のすべてのシングルチャネル TCP、UDP、ICMP トラフィック

HTTP は、Web トラフィックの特定の検査を許可するために分離されています。 これによって、このドキュメントの最初のセクションでポリシングを設定できるようになり、2 番目のセクションで HTTP アプリケーション検査が設定できるようになります。 このドキュメントの 3 番目のセクションでは P2P と IM トラフィック用に具体的なクラスマップとポリシーマップを設定します。 接続は、プライベート ゾーンからパブリック ゾーンへの方向で許可されています。 パブリック ゾーンからプライベート ゾーンへの接続は何も提供されません。

初期ポリシーを実装する設定一式は、「付録 C：2 つのゾーン用の基本ゾーンポリシー ファイアウォール設定」を参照してください。

HTTP アプリケーション検査機能強化の設定

(他のアプリケーション検査ポリシーと同様) HTTP アプリケーション検査は、基本 レイヤ 4 設定よりも複雑な設定を必要とします。 制御する具体的なトラフィックを認識し、望ましいトラフィックと望ましくないトラフィックに希望のアクションを適用するために、レイヤ 7 トラフィック分類とポリシーを設定する必要があります。

(他のタイプのアプリケーション検査と類似している) HTTP アプリケーション検査は、HTTP トラフィックだけに適用できます。 つまり、特定の HTTP トラフィックにレイヤ 7 のクラスマップとポリシーマップを定義してから、HTTP に具体的にレイヤ 4 クラスマップを定義し、次のようにレイヤ 7 ポリシーをレイヤ 4 ポリシーマップの HTTP 検査に適用する必要があります。

```
!configure the layer-7 traffic characteristics:
class-map type inspect http match-any http-l7-cmap
 match  req-resp protocol-violation
 match  request body length gt 4096
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect http http-l7-pmap
 class type inspect http http-l7-cmap
  reset
  log
!
!define the layer-4 inspection policy
class-map type inspect match-all http-l4-cmap
 match protocol http
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
 class type inspect http-l4-cmap
  inspect
  service-policy http http-l7-pmap
```

これらの HTTP アプリケーション検査トラフィックの特長は、すべてレイヤ 7 クラスマップに定義されています。

- **ヘッダー検査**：このコマンドは、設定された正規表現にヘッダーが一致する要求または応答を許可/拒否/監視する機能を提供します。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-6-HTTP_HDR_REGEX_MATCHED*コマンドの使用方法：*match {request|response|req-resp} header regex <parameter-map-name> *サンプルの使用例*ヘッダーに ASCII 以外の文字が含まれている要求または応答をブロックするように、http appfw ポリシーを設定します。
```
parameter-map type regex non_ascii_regex
   pattern “[^\x00-\x80]”
class-map type inspect http non_ascii_cm
   match req-resp header regex non_ascii_regex
policy-map type inspect http non_ascii_pm
   class type inspect http non_ascii_cm
      reset
```
- **ヘッダー長検査**：このコマンドは、要求または応答のヘッダー長が、設定済みのしきい値を超過する場合、その長さをチェックしてアクションを適用します。 アクションは許可またはリセットです。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-4- HTTP_HEADER_LENGTH*コマンドの使用方法：*match {request|response|req-resp} header length gt <bytes> *サンプルの使用例*4096 バイトよりも長いヘッダー長の要求と応答をブロックするように、http appfw ポリシーを設定します。
```
class-map type inspect http hdr_len_cm
   match req-resp header length gt 4096

policy-map type inspect http hdr_len_pm
```

```
   class type inspect http hdr_len_cm
      reset
```

- **ヘッダー カウント検査**：このコマンドは、要求/応答内のヘッダー行 (フィールド) の数が、設定済みのしきい値を超過する場合、その数を確認してアクションを適用します。 アクションは許可またはリセットです。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-6- HTTP_HEADER_COUNT.*コマンドの使用方法：*match {request|response|req-resp} header count gt <number> *サンプルの使用例*16 ヘッダー フィールドを超える要求をブロックするように、http appfw ポリシーを設定します。class-map type inspect http hdr_cnt_cm
   match request header count gt 16

policy-map type inspect http hdr_cnt_pm
   class type inspect http hdr_cnt_cm
      reset

- **ヘッダー フィールド検査**：このコマンドは、特定の HTTP ヘッダー フィールドと値を含む要求/応答を許可/拒否/監視する機能を提供します。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-6- HTTP_HDR_FIELD_REGEX_MATCHED*コマンドの使用方法：*match {request|response|req-resp} header <header-name> *サンプルの使用例*http アプリケーション検査を設定して、スパイウェア/アドウェアをブロックします。parameter-map type regex ref_regex
   pattern “\.delfinproject\.com”
   pattern “\.looksmart\.com”

parameter-map type regex host_regex
   pattern “secure\.keenvalue\.com”
   pattern “\.looksmart\.com”

parameter-map type regex usragnt_regex
   pattern “Peer Points Manager”

class-map type inspect http spy_adwr_cm
   match request header refer regex ref_regex
   match request header host regex host_regex
   match request header user-agent regex usragnt_regex

policy-map type inspect http spy_adwr_pm
   class type inspect http spy_adwr_cm
      reset

- **ヘッダー フィールド長検査**：このコマンドは、ヘッダー フィールド行の長さを制限する機能を提供します。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-6- HTTP_HDR_FIELD_LENGTH.*コマンドの使用方法：*match {request|response|req-resp} header <header-name> length gt <bytes> *サンプルの使用例*Cookie およびユーザエージェント フィールドの長さがそれぞれ 256 および 128 を超える要求をブロックするように、http appfw ポリシーを設定します。class-map type inspect http hdrline_len_cm
   match request header cookie length gt 256
   match request header user-agnet length gt 128

policy-map type inspect http hdrline_len_pm
   class type inspect http hdrline_len_cm
      reset

- **ヘッダー フィールド繰り返しの検査**：このコマンドは、要求または応答がヘッダー フィールドを繰り返しているかどうかをチェックします。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 イネーブルにすると、ログ アクションが syslog メッセージを発生させます。APPFW-6- HTTP_REPEATED_HDR_FIELDS.*コマンドの使用方法：*match {request|response|req-resp} header <header-name> *サンプルの使用例*複数のコン

テンツ長ヘッダー行を含む要求または応答をブロックするように、http appfw ポリシーを設定します。 これは、セッションをこっそり伝送することを防ぐために使われる最も便利な機能の 1 つです。
```
class-map type inspect http multi_occrns_cm
   match req-resp header content-length count gt 1

policy-map type inspect http multi_occrns_pm
   class type inspect http multi_occrns_cm
      reset
```

- **メソッド検査**：HTTP RFC では、限定された HTTP メソッドのセットが許可されます。 ただし、一部のメソッドは Web サーバ上の脆弱性を悪用するために使用できるため、標準メソッドの一部は安全ではないとみなされています。 非標準メソッドの多くは悪意のあるアクティビティに頻繁に使用されます。 このことにより、メソッドをさまざまなカテゴリにグループ化し、各カテゴリのアクションをユーザに選択させることが必要になります。 このコマンドは、安全なメソッド、安全ではないメソッド、webdav メソッド、rfc メソッド、拡張メソッドなど、さまざまなカテゴリにメソッドをグループ化する柔軟な方法をユーザに提供します。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-6-HTTP_METHOD.*コマンドの使用方法：*match request method <method> *サンプルの使用例*HTTP メソッドを次の 3 つのカテゴリにグループ化するように、http appfw ポリシーを設定します。 すなわち、「安全なメソッド」、「安全ではないメソッド」、「webdav メソッド」です。 これらを表に示します。 次のようにアクションを設定します。すべての安全なメソッドが口グなしで許可されるすべての安全ではないメソッドが口グ付きで許可されるすべての webdav メソッドが口グ付きでブロックされるhttp policy:

```
class-map type inspect http safe_methods_cm
   match request method get
   match request method head
   match request method option

class-map type inspect http unsafe_methods_cm
   match request method post
   match request method put
   match request method connect
   match request method trace

class-map type inspect http webdav_methods_cm
   match request method bcopy
   match request method bdelete
   match request method bmove

policy-map type inspect http methods_pm
   class type inspect http safe_methods_cm
      allow
   class type inspect http unsafe_methods_cm
      allow log
      class type inspect http webdav_methods_cm
      reset log
```

- **URI 検査**：このコマンドは、URI が設定済みの通常の検査と一致する要求を、許可/拒否/監視する機能を提供します。 これは、カスタム URL とクエリーをブロックする機能をユーザに提供します。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-6- HTTP_URI_REGEX_MATCHED*コマンドの使用方法：*match request uri regex <parameter-map-name> *サンプルの使用例*URI が次の正規表現に一致する要求をブロックするように、http appfw ポリシーを設定します。を探します。*cmd.exeを探します。*sexを探します。*gamblingparameter-map type regex uri_regex_cm

```
   pattern “.*cmd.exe”
   pattern “.*sex”
   pattern “.*gambling”

class-map type inspect http uri_check_cm
   match request uri regex uri_regex_cm

policy-map type inspect http uri_check_pm
   class type inspect http uri_check_cm
      reset
```

- **URI 長検査**：このコマンドは、要求で送信される URI の長さを確認し、その長さが設定済みのしきい値を超過したときに設定済みのアクションを適用します。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-6- HTTP_URI_LENGTH.*コマンドの使用方法：*match request uri length gt <bytes> *サンプルの使用例*要求の URI 長が 3076 バイトを超えたときにはいつでもアラームを起動するように、http appfw ポリシーを設定します。
```
class-map type inspect http uri_len_cm
   match request uri length gt 3076

policy-map type inspect http uri_len_pm
   class type inspect http uri_len_cm
      log
```
- **引数検査**：このコマンドは、引数（パラメータ）が設定済みの通常の検査と一致する要求を許可/拒否/監視する機能を提供します。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-6- HTTP_ARG_REGEX_MATCHED*コマンドの使用方法：*match request arg regex <parameter-map-name> *サンプルの使用例*引数が次の正規表現に一致する要求をブロックするように、http appfw ポリシーを設定します。を探します。*coderedを探します。*attackparameter-map type regex arg_regex_cm
```
   pattern “.*codered”
   pattern “.*attack”

class-map type inspect http arg_check_cm
   match request arg regex arg_regex_cm

policy-map type inspect http arg_check_pm
   class type inspect http arg_check_cm
      reset
```
- **引数長検査**：このコマンドは、要求で送信される引数の長さを確認し、その長さが設定済みのしきい値を超過したときに設定済みのアクションを適用します。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-6- HTTP_ARG_LENGTH.*コマンドの使用方法：*match request arg length gt <bytes> *サンプルの使用例*要求の引数長が 512 バイトを超えたときにはいつでもアラームを起動するように、http appfw ポリシーを設定します。
```
class-map type inspect http arg_len_cm
   match request arg length gt 512

policy-map type inspect http arg_len_pm
   class type inspect http arg_len_cm
      log
```
- **本体検査**：この CLI で、ユーザは、要求または応答の本体に対して正規表現のリストを照合するように指定できます。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-6- HTTP_BODY_REGEX_MATCHED*コマンドの使用方法：*match {request|response|reg-resp} body regex <parameter-map-name> *サンプルの使用例*本文がパター

ンが含まれている応答をブロックするために http appfw を設定して下さい。* [Aa] [TT] [TT] [Aa] [Cc] [Kk]parameter-map type regex body_regex
   pattern “.*[Aa][Tt][Tt][Aa][Cc][Kk]”

class-map type inspect http body_match_cm
   match response body regex body_regex

policy-map type inspect http body_match_pm
   class type inspect http body_match_cm
      reset

- **本体 (コンテンツ) 長検査**：このコマンドは、要求または応答で送信されるメッセージのサイズを確認します。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-4- HTTP_CONTENT_LENGTH*コマンドの使用方法：*match {request|response|req-resp} body length lt <bytes> gt <bytes> *サンプルの使用例*要求または応答で 10K バイトを超えるメッセージを含む http セッションをブロックするように、http appfw ポリシーを設定します。
class-map type inspect http cont_len_cm
   match req-resp header content-length gt 10240

policy-map type inspect http cont_len_pm
   class type inspect http cont_len_cm
      reset

- **ステータス行検査**：このコマンドで、ユーザは、応答のステータス行に対して照合する正規表現のリストを指定できます。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-6-HTTP_STLINE_REGEX_MATCHED.*コマンドの使用方法：*match response status-line regex <class-map-name> *サンプルの使用例*禁止されたページへのアクセスが試行されたときにはいつでもアラームを記録するように、http appfw ポリシーを設定します。 禁止されたページは、通常は 403 ステータスコードを含んでおり、そのステータス行は HTTP/1.0 403 page forbidden\r\n のような内容です。parameter-map type regex status_line_regex
   pattern “[Hh][Tt][Tt][Pp][/][0-9][.][0-9][\t]+403”

class-map type inspect http status_line_cm
   match response status-line regex status_line_regex

policy-map type inspect http status_line_pm
   class type inspect http status_line_cm
      log

- **content-type 検査**：このコマンドは、メッセージ ヘッダーの content-type がサポートされているコンテンツタイプのリストに存在するかどうかを確認します。 また、ヘッダーの content-type がメッセージ データまたはエンティティ本体部分のコンテンツに一致することを確認します。 キーワード **mismatch** が設定される場合、コマンドは要求メッセージの受け付け済みのフィールド値に対する応答メッセージの content-type を確認します。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、適切な syslog メッセージが発生します。APPFW-4- HTTP_CONT_TYPE_VIOLATION,
APPFW-4- HTTP_CONT_TYPE_MISMATCH,
APPFW-4- HTTP_CONT_TYPE_UNKNOWN*コマンドの使用方法：*match {request|response|req-resp} header content-type [mismatch|unknown|violation] *サンプルの使用例*未知の content-type の要求と応答を含む http セッションをブロックするように、http appfw ポリシーを設定します。
class-map type inspect http cont_type_cm
   match req-resp header content-type unknown

policy-map type inspect http cont_type_pm

```
   class type inspect http cont_type_cm
      reset
```

- **ポート誤用インスペクション**—このコマンドが HTTPポートを防ぐのに使用されています（IM、P2P、トンネリング、等割り当てまたはリセットされた操作のような他のアプリケーションのために 80）誤用されて class-map 条件を満たすことは要求か応答に適用することができます。 ログ アクションを追加すると、適切な syslog メッセージが発生します。APPFW-4-HTTP_PORT_MISUSE_TYPE_IM
APPFW-4-HTTP_PORT_MISUSE_TYPE_P2P
APPFW-4-HTTP_PORT_MISUSE_TYPE_TUNNEL*コマンドの使用方法：*match request port-misuse {im|p2p|tunneling|any}*サンプルの使用例*http セッションが IM アプリケーションで誤使用されるのをブロックするように、http appfw ポリシーを設定します。class-map type inspect http port_misuse_cm
   match request port-misuse im

policy-map type inspect http port_misuse_pm
   class type inspect http port_misuse_cm
      reset
- **厳密な http 検査**：このコマンドは、HTTP 要求と応答に対する厳密なプロトコル一致チェックをイネーブルにします。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-4- HTTP_PROTOCOL_VIOLATION*コマンドの使用方法：*match req-resp protocol-violation*サンプルの使用例*RFC 2616 に違反する要求や応答をブロックするように、http appfw ポリシーを設定します。class-map type inspect http proto-viol_cm
   match req-resp protocol-violation

policy-map type inspect http proto-viol_pm
   class type inspect http proto-viol_cm
      reset
- **転送エンコーディング検査**：このコマンドは、転送エンコーディング タイプが設定済みのタイプと一致する要求/応答を許可/拒否/監視する機能を提供します。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-6- HTTP_TRANSFER_ENCODING*コマンドの使用方法：*match {request|response|req-resp} header transfer-encoding {regex <parameter-map-name> |gzip|deflate|chunked|identity|all} *サンプルの使用例*圧縮タイプのエンコーディングを含む要求また応答をブロックするように、http appfw ポリシーを設定します。class-map type inspect http trans_encoding_cm
   match req-resp header transfer-encoding type compress

policy-map type inspect http trans_encoding_pm
   class type inspect http trans_encoding_cm
      reset
- **Java アプレット検査**：このコマンドは、応答が Java アプレットを持つかどうかをチェックし、アプレットを検出したときには設定済みのアクションを適用します。 許可またはリセットのアクションは、クラスマップ基準に一致する要求または応答に適用できます。 ログ アクションを追加すると、次の syslog メッセージが発生します。APPFW-4- HTTP_JAVA_APPLET *コマンドの使用方法：*match response body java-applet*サンプルの使用例*Java アプレットをブロックするように、http appfw ポリシーを設定します。class-map type inspect http java_applet_cm
   match response body java-applet

policy-map type inspect http java_applet_pm
   class type inspect http java_applet_cm
      reset
```
```

インスタント メッセージとピアツーピア アプリケーション制御の ZFW サポート

Cisco IOS ソフトウェア リリース 12.4(9)T は、IM と P2P アプリケーションの ZFW サポートを導入しました。

Cisco IOS ソフトウェアは、最初に、Cisco IOS ソフトウェア リリース 12.4(4)T で IM アプリケーション制御のサポートを提供しました。 ZFW の最初のリリースでは、ZFW インターフェイスで IM アプリケーションをサポートしませんでした。 IM アプリケーション制御が望ましい場合に、ユーザは ZFW 設定インターフェイスに移行することができませんでした。 Cisco IOS ソフトウェア リリース 12.4(9)T は、Yahoo! Messenger（YM）、MSN Messenger（MSN）、および AOL Instant Messenger（AIM）をサポートしている IM 検査の ZFW サポートを導入しています。

Cisco IOS ソフトウェア リリース 12.4(9)T が、P2P ファイル共有アプリケーション向けのネイティブの IOS Firewall サポートを行った最初の Cisco IOS ソフトウェアのバージョンです。

IM と P2P の検査はどちらもアプリケーション トラフィック向けにレイヤ 4 とレイヤ 7 のポリシーを提供します。 つまり、他のアクティビティが拒否されても特定のアプリケーション アクティビティは許可されるように、ZFW が、トラフィックの許可または拒否を許すための基本のステートフル検査と、さまざまなプロトコルの具体的なアクティビティに対する細かいレイヤ 7 制御を提供できることを意味します。

P2P アプリケーション検査および制御

SDM 2.2 は、そのファイアウォール設定セクションに P2P アプリケーション制御を導入しました。 SDM は、Network-Based Application Recognition（NBAR）と QoS ポリシーを適用して、0 のライン レートへの P2P アプリケーション アクティビティを検出してポリシングし、すべての P2P トラフィックをブロックしました。 これによって、IOS Firewall CLI での P2P サポートを期待している CLI ユーザが、必要な NBAR/QoS 設定を意識しない限り CLI で P2P ブロッキングを設定できないという問題が発生しました。 Cisco IOS ソフトウェア リリース 12.4(9)T では、ZFW CLI にネイティブの P2P 制御を導入し、NBAR を活用して P2P アプリケーション アクティビティを検出しています。 このソフトウェア リリースは、次のようにいくつもの P2P アプリケーション プロトコルをサポートしています。

- BitTorrent
- edonkey
- fasttrack
- Gnutella
- KaZaA / KaZaA2
- WinMX

P2P アプリケーションは、「ポートホッピング」動作および検出を避ける他のテクニックの結果、プロトコルの動作を変更する P2P アプリケーションへの頻繁な変更と更新によって引き起こされた問題と同様、特に検出するのが難しくなっています。 ZFW は、ネイティブのファイアウォール ステートフル検査と NBAR のトラフィック認識機能を組み合わせることで、ZFW の CPL 設定インターフェイスに P2P アプリケーション制御を提供します。 NBAR には次の 2 つの卓越したメリットがあります。

- 複雑で検出が困難な動作にもかかわらずアプリケーションを認識する、オプションのヒューリスティックベースのアプリケーション認識
- プロトコル更新および変更と並び、更新メカニズムを提供する拡張性に富んだインフラストラクチャ

P2P 検査の設定

前述したように、P2P 検査と制御は、レイヤ 4 ステートフル検査とレイヤ 7 アプリケーション制御の両方を提供します。

レイヤ 4 検査は、ネイティブ アプリケーション サービス ポートの検査が適切な場合には、他のアプリケーション サービスと同様に設定されます。

```
class-map type inspect match-any my-p2p-class
match protocol [bittorrent | edonkey | fasttrack | gnutella | kazaa | kazaa2 | winmx ]
[signature (optional)]
!
policy-map type inspect private-allowed-policy
 class type inspect my-p2p-class
  [drop | inspect | pass]
```

match protocol [サービス名] にある追加の signature オプションに注目してください。 match protocol 文の最後に signature オプションを追加することで、具体的な P2P アプリケーション アクティビティを指し示すトラフィック内の暴露部分を検索するように、NBAR ヒューリスティックがトラフィックに適用されます。 これには、ポートホッピングと、トラフィック検出を回避するためのアプリケーション動作内の他の変更が含まれます。 このレベルのトラフィック検査は、CPU 使用率の増加とネットワーク スループット機能の低下を犠牲にして行われます。 signature オプションが適用されない場合、NBAR ベースのヒューリスティック分析はポートホッピング動作の検出には適用されず、同じ程度には CPU の使用率は影響を受けません。

ネイティブ サービス検査には、P2P アプリケーションが非標準の送信元および宛先ポートに「ホップ」した場合や、アプリケーションが認識されていないポート番号でアクションを開始するために更新される場合に、その P2P アプリケーションに対する制御を維持できないというデメリットがあります。

アプリケーションの	ネイティブ ポート（12.4(15)T PAM リストによって認識）
BitTorrent	TCP 6881 ~ 6889
edonkey	TCP 4662
fasttrack	TCP 1214
gnutella	TCP 6346-6349 TCP 6355,5634 UDP 6346-6348
kazaa2	PAM に依存
winmx	TCP 6699

P2P トラフィックを許可（検査）する場合、追加の設定が必要になる可能性があります。 アプリケーションによっては、複数の P2P ネットワークが使用されているか、稼動するためにはファイアウォール設定の調整が必要になる特定の動作が実装されている場合があります。

- BitTorrent クライアントは通常、非標準のポート上で動作している http 経由で「トラッカー」（ピア ディレクトリ サーバ）と通信します。 通常、これは TCP 6969 ですが、トレント固有のトラッカー ポートをチェックすることが必要な場合もあります。 BitTorrent を許可する場合、追加のポートに対処する最良の方式は、照合プロトコルの 1 つとして HTTP を設定し、**ip port-map** コマンドを使用して TCP 6969 を HTTP を追加することです。 **ip port-map http port tcp 6969** クラスマップに適用する照合基準として http と bittorrent を定義する必要があります。
- eDonkey は、eDonkey と Gnutella の両方として検出される接続を初期化するために出現し

ます。
- KaZaA 検査は、NBAR 署名検知にすべて依存しています。

レイヤ 7 (アプリケーション) 検査は、ファイル検索、ファイル転送、および text-chat 機能を選択的にブロックまたは許可するなど、サービス固有のアクションを認識して適用する機能を強化します。 サービス固有機能は、サービスによってさまざまです。

P2P アプリケーション検査は、HTTP アプリケーション検査に似ています。

```
!configure the layer-7 traffic characteristics:
class-map type inspect [p2p protocol] match-any p2p-l7-cmap
 match action
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect [p2p protocol] p2p-l7-pmap
 class type inspect p2p p2p-l7-cmap
  [ reset | allow ]
  log
!
!define the layer-4 inspection policy
class-map type inspect match-all p2p-l4-cmap
 match protocol [p2p protocol]
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
 class type inspect p2p-l4-cmap
  [ inspect | drop | pass ]
  service-policy p2p p2p-l7-pmap
```

P2P アプリケーション検査は、レイヤ 4 検査でサポートされているアプリケーションのサブセット用のアプリケーション固有の機能を提供します。

- edonkey
- fasttrack
- gnutella
- kazaa2

これらの各アプリケーションは、さまざまなアプリケーション固有の照合基準オプションを提供します。

edonkey

```
router(config)#class-map type inspect edonkey match-any edonkey-l7-cmap router(config-
cmap)#match ? file-transfer Match file transfer stream flow Flow based QoS parameters search-
file-name Match file name text-chat Match text-chat
```

fasttrack

```
router(config)#class-map type inspect fasttrack match-any ftrak-l7-cmap router(config-
cmap)#match ? file-transfer File transfer stream flow Flow based QoS parameters
```

gnutella

```
router(config)#class-map type inspect gnutella match-any gtella-l7-cmap router(config-
cmap)#match ? file-transfer Match file transfer stream flow Flow based QoS parameters
```

kazaa2

```
router(config)#class-map type inspect kazaa2 match-any kazaa2-l7-cmap router(config-cmap)#match
? file-transfer Match file transfer stream flow Flow based QoS parameters
```

新しい P2P プロトコル定義または既存の P2P プロトコルへの更新は、NBAR の動的 pdlm 更新を使用してロードできます。 これは、新しい PDLM をロードする設定コマンドです。

ip nbar pdlm *<file-location>*

新しいプロトコルは、クラス タイプ inspect 用の **match protocol** ... コマンドで利用できます。 新しい P2P プロトコルにサービス (サブプロトコル) がある場合、新しいレイヤ 7 inspect クラスマップ タイプは、レイヤ 7 照合基準と同様、利用可能になります。

IM アプリケーション検査および制御

Cisco IOS ソフトウェア リリース 12.4(4)T は、IM アプリケーション検査および制御を導入しました。 IM サポートは 12.4(6)T では ZFW とともには導入されませんでした。そのため、ユーザは同一のファイアウォール ポリシーに IM 制御と ZFW を適用できなかったので、1 つのインターフェイス上では ZFW と従来型のファイアウォール機能は共存できません。

Cisco IOS ソフトウェア リリース 12.4(9)T は、次の IM サービスに対してステートフルな検査とアプリケーション制御をサポートしています。

- AOL Instant Messenger
- MSN Messenger
- Yahoo! Messenger

IM 検査は、各サービスに対するホストの特定のグループへのアクセスを制御することに依存しているため、IM 検査はほとんどのサービスとは少しだけ異なっています。 一般に、IM サービスはディレクトリ サーバの比較的永続的なグループに依存しており、このグループのクライアントは IM サービスにアクセスするために問い合わせができる必要があります。 IM アプリケーションは、プロトコルやサービスの立場からの制御は非常に難しい傾向があります。 これらのアプリケーションを制御する最も効果的な方法は、固定の IM サーバへのアクセスを制限することです。

IM 検査の設定

IM 検査と制御は、レイヤ 4 ステートフル検査とレイヤ 7 アプリケーション制御の両方を提供します。

レイヤ 4 検査は、他のアプリケーション サービスと同様に設定されます。

```
class-map type inspect match-any my-im-class
match protocol [aol | msnmsgr | ymsgr ]
!
policy-map type inspect private-allowed-policy
 class type inspect my-im-class
  [drop | inspect | pass
```

IM アプリケーションは、その機能を維持するためにサーバに複数のポートで問い合わせることができます。 inspect アクションを適用することで指定の IM サービスを許可する場合、IM サービスのサーバに許可されたアクセスを定義するサーバリストは必要ない可能性があります。 ただし、AOL Instant Messenger などの一定の IM サービスを指定するクラスマップを設定することと、関連するポリシーマップに drop アクションを適用することによって、インターネットに対して接続が許可されている別のポートを IM クライアントが検出する可能性があります。 一定のサービスへの接続を許可したくない場合、または IM サービス機能を text-chat に制限したい場合、サーバ リストを定義して ZFW が IM アプリケーションに関連付けられたトラフィックを識別できるようにする必要があります。

```
!configure the server-list parameter-map:
```

```
parameter-map type protocol-info <name>
  server name <name>
  server ip a.b.c.d
  server ip range a.b.c.d a.b.c.d
```
たとえば、Yahoo IM サーバ リストは次のように定義されます。

```
parameter-map type protocol-info ymsgr-pmap
  server name scs.msg.yahoo.com
  server name scsd.msg.yahoo.com
  server ip 66.77.88.99
  server ip range 103.24.5.67 103.24.5.99
```
サーバリストはプロトコル定義に適用する必要があります。

```
class-map type inspect match-any ym-l4-cmap
 match protocol ymsgr ymsgr-pmap
```
名前解決をイネーブルにするには、**ip domain lookup** コマンドと **ip name-server ip.ad.re.ss** コマンドを設定する必要があります。

IM サーバ名はかなり動的です。 設定済みの IM サーバ リストが完成していて正しいかどうかを、定期的にチェックする必要があります。

レイヤ 7 (アプリケーション) 検査は、他のサービス機能を拒否しているときに text-chat 機能を選択的にブロックまたは許可するなど、サービス固有のアクションを認識して適用する機能を強化します。

IM アプリケーション検査は、現在、text-chat アクティビティと他のすべてのアプリケーション サービスを区別する機能を提供しています。 IM アクティビティを text-chat に限定するには、レイヤ 7 ポリシーを次のように設定します。

```
class-map type inspect ymsgr match-any ymsgr-text-cmap
  match service text-chat

class-map type inspect ymsgr match-any ymsgr-default-cmap
  match service any

policy-map type inspect im ymsgr-l7-pmap
  class type inspect im ymsgr-text-cmap
    allow
    [log]
  class type inspect im ymsgr-text-cmap
    reset
    [log]
```
レイヤ 7 ポリシーを、以前設定した Yahoo! Messenger ポリシーに適用します。

```
class-map type inspect match-any my-im-class
match protocol ymsgr
!
policy-map type inspect private-allowed-policy
 class type inspect my-im-class
  inspect
  service-policy im ymsgr-l7-pmap
```

URL フィルタリング

ZFW は、特定のドメインへのアクセスを確認するために、ルータに定義されている優良リストまたはブラックリストによって、または URL フィルタリング サーバにドメイン名を転送することによって、指定された Web コンテンツへのアクセスを制御する URL フィルタリング機能を提供します。 Cisco IOS ソフトウェア リリース 12.4(6)T から 12.4(15)T への ZFW URL フィルタリン

グは、アプリケーション検査に似た追加のポリシー アクションとして適用されます。

サーバベースの URL フィルタリングの場合、**urlfilter** サーバ設定を説明するパラメータマップを定義する必要があります。

```
parameter-map type urlfilter websense-parmap
 server vendor [n2h2 | websense] 10.1.1.1
```

静的な優良リストまたはブラックリストが好まれる場合、具体的に許可または拒否されるドメインまたはサブドメインのリストを定義すると、一方で逆のアクションがそのリストに一致しないトラフィックに適用されます。

```
parameter-map type urlfilter websense-parmap
 exclusive-domain deny .disallowed.com
 exclusive-domain permit .cisco.com
```

URL のブラックリストが排他的なドメイン定義で拒否オプションを使用して定義される場合、他のすべてのドメインが許可されます。 「許可」定義が定義された場合、IP アクセス コントロール リストの機能に似た、許可されるすべてのドメインが明示的に指定される必要があります。

HTTP トラフィックを照合するクラスマップを設定します。

```
class-map type inspect match-any http-cmap
 match protocol http
```

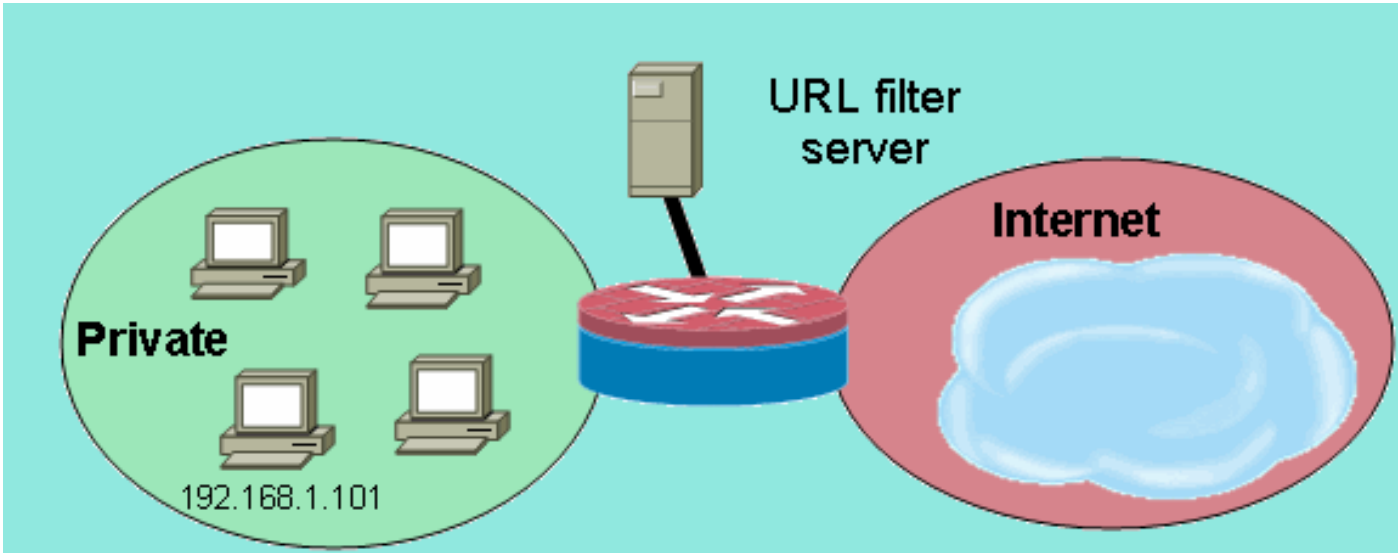
クラスマップを **inspect** アクションおよび **urlfilter** アクションに関連付けるポリシーマップを定義します。

```
policy-map type inspect http-filter-pmap
 class type inspect http-cmap
  inspect
  urlfilter websense-parmap
```

これによって、URL フィルタリング サーバと通信する最小条件が設定されます。 追加の URL フィルタリング動作を定義するために、いくつかのオプションが利用できます。

ネットワーク展開の中には、他のホストに対する URL フィルタリングをバイパスする一方で、いくつかのホストまたはサブネット用に URL フィルタリングを提供するものもあります。 たとえば、図 9 では、プライベート ゾーン内のすべてのホストには具体的なホストである 192.168.1.101 を除き、URL フィルタ サーバによってチェックされる HTTP トラフィックを持つ必要があります。

図 9： URL フィルタリング例のトポロジ



これは、次の 2 つの異なるクラスマップ マップを定義することで実現できます。

- URL フィルタリングを受信する、より大きなグループのホスト用の HTTP トラフィックに照合するだけの 1 つのクラスマップ。
- URL フィルタリングを受信しない、より小さなグループのホスト用の 1 つのクラスマップ。2 番目のクラスマップは、HTTP トラフィックと同時に、URL フィルタリング ポリシーから除外されるホストのリストを照合します。

両方のクラスマップは 1 つのポリシーマップで設定されますが、**urlfilter** アクションを受信するのは片方だけです。

```
class-map type inspect match-any http-cmap
 match protocol http
class-map type inspect match-all http-no-urlf-cmap
 match protocol http
 match access-group 101
!
policy-map type inspect http-filter-pmap
 class type inspect http-no-urlf-cmap
  inspect
 class type inspect http-cmap
  inspect
  urlfilter websense-parmap
!
access-list 101 permit ip 192.168.1.101 any
```

ルータへのアクセスの制御

ほとんどのネットワーク セキュリティ エンジニアは、パブリック インターネットにルータの管理インターフェイス（SSH、Telnet、HTTP、HTTPS、SNMP など）を開示することに警戒心を抱いており、また、特定の状況では、ルータへの LAN アクセスにも制御が必要な場合もあります。 Cisco IOS ソフトウェアは、さまざまなインターフェイスへのアクセスを制限するいくつものオプションを提供します。その中には、Network Foundation Protection（NFP）機能ファミリ、管理インターフェイス用のさまざまなアクセス制御メカニズム、および ZFW のセルフゾーンがあります。 ルータ制御機能のどの組み合わせが具体的なアプリケーションで最適に機能するのかを判断するには、VTY アクセス制御、管理プレーン保護、SNMP アクセス制御などの他の機能を検討してください。

一般に、NFP 機能ファミリは、ルータ自体を宛先とするトラフィックの制御に最適です。 NFP 機能を使用するルータ保護を説明する情報は、『Cisco IOS ソフトウェアにおけるコントロール プレーン セキュリティの概要』を参照してください。

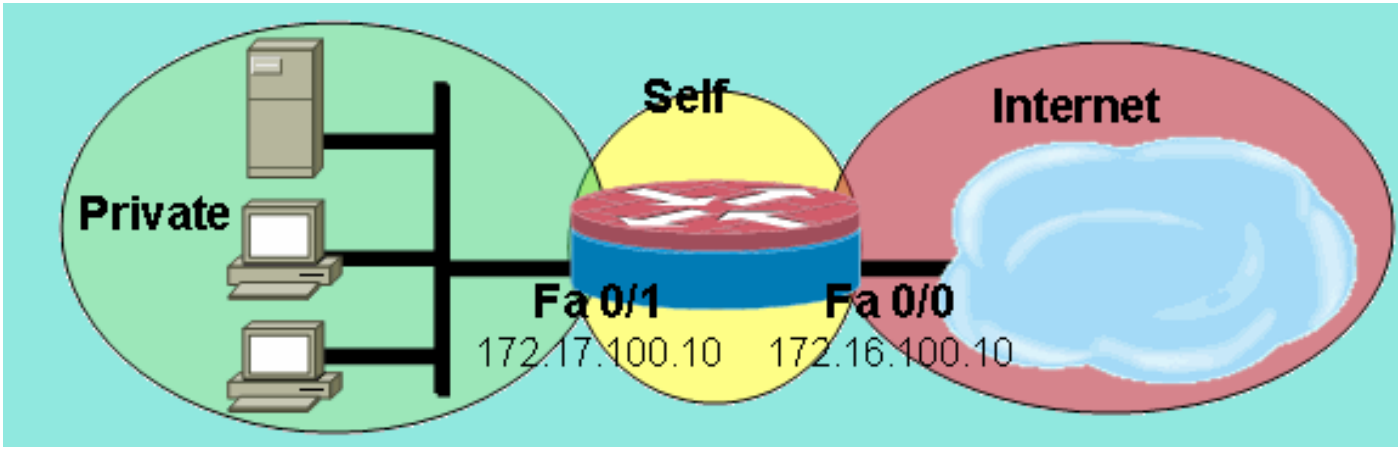
ルータ自体の IP アドレスを行き来するトラフィックを制御するために ZFW を適用すると決定した場合、ファイアウォールのデフォルト ポリシーと機能が、通過トラフィックで利用できるものとは異なることを理解する必要があります。 通過トラフィックは、ルータのインターフェイスのいずれかに適用される IP アドレスと一致しない送信元または宛先の IP アドレスのネットワークトラフィックとして定義され、そのトラフィックは、たとえば、ICMP TTL 期限切れメッセージやネットワーク/ホスト到達不能メッセージなどのネットワーク コントロール メッセージをルータに送信させません。

ZFW は、ゾーン間を移動するトラフィックにデフォルトの deny-all（すべて拒否）ポリシーを適用します。ただし、一般的な規則で説明したように、ルータのインターフェイスのアドレスに直接流れ込む任意のゾーンのトラフィックが暗黙で許可されます。 これは、ルータの管理インターフェイスへの接続が、ゾーン ファイアウォール設定がルータに適用されるときに維持されることを前提とします。 同一の deny-all ポリシーがルータへの直接の接続に影響した場合、管理ポリシー設定一式は、ゾーンがルータに設定される前に適用される必要があります。 これは、ポリシー

が不適切に実装されたまたは間違った順序で適用された場合に、管理接続を中断させる可能性があります。

インターフェイスがゾーン メンバになるように設定されると、インターフェイスに接続されたホストはゾーン内に含まれます。 ただし、ルータのインターフェイスの IP アドレスを行き来するトラフィックは、ゾーン ポリシーによっては制御されません（図 10 の後にある注で説明されている状況を除く）。 その代わり、ルータ上のすべての IP インターフェイスは、ZFW が設定されたときに自動的にセルフ ゾーンの一部になります。 ルータ上のさまざまなゾーンからルータのインターフェイスに移動する IP トラフィックを制御するには、ポリシーを適用して、ゾーンとルータのセルフ ゾーンの間のトラフィックをブロックまたは許可/検査する必要があります（図 10.参照して下さい）

図 10： ネットワーク ゾーンとルータのセルフ ゾーンの間のポリシーの適用



ルータはすべてのゾーンとセルフ ゾーンの間にデフォルト許可ポリシーを提供しますが、ポリシーが任意のゾーンからセルフ ゾーンに設定され、セルフからルータのユーザ定義可能なインターフェイス接続ゾーンには設定されない場合、ルータから発信されたすべてのトラフィックは、そのルータへのリターン時に接続ゾーンからセルフ ゾーンへのポリシーに遭遇し、ブロックされます。 つまり、ルータ発信トラフィックは、セルフ ゾーンへのリターンを許可するために検査される必要があります。

注: Cisco IOS ソフトウェアは、syslog、tftp、telnet、その他のコントロールプレーン サービスなどのトラフィック用に、インターフェイスの「最も近い」宛先ホストと関連付けられた IP アドレスを常に使用し、このトラフィックをセルフゾーン ファイアウォール ポリシーの対象とします。ただしサービスが含んでいるが、**logging source-interface [type number]**、**ip tftp source-interface [type number]**、および **ip telnet source-interface [type number]**に制限されなくて、トラフィックは自己ゾーンに服従しますコマンドを使用してソースインターフェイスと特定のインターフェイスを定義すれば。

注: サービスの中（特にルータの Voice over IP サービス）には、セキュリティ ゾーンに割り当てることのできない一時的なインターフェイスまたは設定できないインターフェイスを使用するものもあります。 これらのサービスは、設定済みのセキュリティ ゾーンにトラフィックを関連付けることができない場合に、適切に機能しない可能性があります。

セルフゾーン ポリシーの制限

セルフゾーン ポリシーには、通過トラフィック ゾーンペアで利用できるポリシーと比べると機能が限定されています。

- 従来型のステートフル検査の場合と同様、ルータが生成したトラフィックは、TCP、UDP、ICMP、および H.323 用の複雑なプロトコル検査に限定されています。

- アプリケーション検査はセルフゾーン ポリシーには利用できません。
- セッションとレートの制限は、セルフゾーン ポリシーには設定できません。

セルフゾーン ポリシー設定

ほとんどの状況で、次に示すのはルータ管理サービスにとって望ましいアクセス ポリシーです。

- Telnet のクリアテキスト プロトコルが簡単にユーザ クレデンシャルとその他の機密情報を開示してしまうので、すべての Telnet 接続を拒否する。
- 任意のゾーンの任意のユーザからの SSH 接続を許可する。 SSH は、ユーザ クレデンシャルとセッション データを暗号化し、それによって、ユーザ アクティビティのスヌーピングを行ったりユーザ クレデンシャルやルータ設定などの機密情報を危険にさらすためにパケットキャプチャ用ツールを利用している悪意のあるユーザからの保護を提供します。 SSH バージョン 2 は、より強力な保護を提供し、SSH バージョン 1 に起因する特定の脆弱性に対処しています。
- プライベート ゾーンが信頼できる場合、プライベート ゾーンからルータへの HTTP 接続を許可する。 信頼できず、プライベート ゾーンが情報を危険にさらす悪意のあるユーザに場所を提供する可能性がある場合、HTTP は管理トラフィックを保護するための暗号化を採用せず、ユーザ クレデンシャルや設定などの機密性のある情報を公開してしまう可能性があります。
- 任意のゾーンからの HTTPS 接続を許可する。 SSH と同様、HTTPS はセッション データとユーザ クレデンシャルを暗号化します。
- SNMP アクセスを特定のホストまたはサブネットに限定する。 SNMP は、ルータ設定を変更し、設定情報を公開するために使用できます。 SNMP は、さまざまなコミュニティのアクセス制御とともに設定する必要があります。
- パブリック インターネットからプライベートゾーン アドレスへの ICMP 要求をブロックする（プライベートゾーン アドレスがルーティング可能であることを前提とする）。 1 つ以上のパブリック アドレスが、必要な場合に、ネットワーク トラブルシューティング向けに ICMP トラフィックのために開示される可能性があります。 いくつかの ICMP 攻撃は、ルータ リソースに高い負荷を与えたり、ネットワーク トポロジやアーキテクチャを偵察したりするために使用されることがあります。

ルータは、制御する必要のある各ゾーン用に 2 つのゾーンペアを追加して、このタイプのポリシーを適用できます。 ルータ セルフゾーンとの間で発信する、または着信するトラフィック用の各ゾーンペアは、トラフィックが逆の方向で発生しない限り、逆の方向の対応するポリシーによって照合される必要があります。 着信および発信のゾーンペアそれぞれ向けの 1 つのポリシーマップをすべてのトラフィックを記述するように適用できるか、ゾーンペアごとの具体的なポリシーマップを適用できます。 ポリシーマップごとの具体的なゾーンペアの設定は、各ポリシーマップを照合するアクティビティを表示する細分性を提供します。

172.17.100.11 に SNMP 管理ステーションがあり、172.17.100.17 に TFTP サーバがあるサンプル ネットワークを想定して、次の出力は管理インターフェイス アクセス ポリシー全体の例を示します。

```
class-map type inspect match-any self—service-cmap
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol h323
!
class-map type inspect match-all to-self-cmap
 match class-map self—service-cmap
```

```
 match access-group 120
!
class-map type inspect match-all from-self-cmap
 match class-map self—service-cmap
!
class-map type inspect match-all tftp-in-cmap
 match access-group 121
!
class-map type inspect match-all tftp-out-cmap
 match access-group 122
!
policy-map type inspect to-self-pmap
 class type inspect to-self-cmap
  inspect
 class type inspect tftp-in-cmap
  pass
!
policy-map type inspect from-self-pmap
 class type inspect from-self-cmap
  inspect
 class type inspect tftp-out-cmap
  pass
!
zone security private
zone security internet
zone-pair security priv-self source private destination self
 service-policy type inspect to-self-pmap
zone-pair security net-self source internet destination self
 service-policy type inspect to-self-pmap
zone-pair security self-priv source self destination private
 service-policy type inspect from-self-pmap
zone-pair security self-net source self destination internet
 service-policy type inspect from-self-pmap

!
interface FastEthernet 0/0
 ip address 172.16.100.10
 zone-member security internet
!
interface FastEthernet 0/1
 ip address 172.17.100.10
 zone-member security private
!
access-list 120 permit icmp 172.17.100.0 0.0.0.255 any
access-list 120 permit icmp any host 172.17.100.10 echo
access-list 120 deny icmp any any
access-list 120 permit tcp 172.17.100.0 0.0.0.255 host 172.17.100.10 eq www
access-list 120 permit tcp any any eq 443
access-list 120 permit tcp any any eq 22
access-list 120 permit udp any host 172.17.100.10 eq snmp
access-list 121 permit udp host 172.17.100.17 host 172.17.100.10
access-list 122 permit udp host 172.17.100.10 host 172.17.100.17
```

残念ながら、セルフゾーン ポリシーは TFTP 転送を検査する機能を提供しません。 つまり、TFTP がファイアウォールをパススルーする必要がある場合、ファイアウォールは TFTP サーバを行き来するすべてのトラフィックを通過させる必要があります。

ルータが IPSec VPN 接続を終了させる場合、IPSec ESP、IPSec AH、ISAKMP、および NAT-T IPSec (UDP 4500) を通過させるポリシーを定義する必要もあります。 これは、使用予定のサービスをベースにして何が必要になるかによって異なります。 次のポリシーは、上記のポリシーに追加されて適用できます。 VPN トラフィック用のクラスマップが pass アクションで挿入されているポリシーマップへの変更に注意してください。 通常、暗号化されたトラフィックは、指定された エンドポイントを行き来する暗号化されたトラフィックを許可する必要があるとセキュリテ

ィ ポリシーが指示しない限り、信頼できます。

```
class-map type inspect match-all crypto-cmap
 match access-group 123
!
policy-map type inspect to-self-pmap
 class type inspect crypto-cmap
  pass
 class type inspect to-self-cmap
  inspect
 class type inspect tftp-in-cmap
  pass
!
policy-map type inspect from-self-pmap
 class type inspect crypto-cmap
  pass
 class type inspect from-self-cmap
  inspect
 class type inspect tftp-out-cmap
  pass
!
access-list 123 permit esp any any
access-list 123 permit udp any any eq 4500
access-list 123 permit ah any any
access-list 123 permit udp any any eq 500
```

ゾーンベース ファイアウォールとワイドエリア アプリケーション サービス

設定例と用例のガイドを提供するアプリケーション ノートについては、『Cisco Wide Area Application Services (ソフトウェア バージョン 4.0.13) のリリース ノート - ソフトウェア バージョン 4.0.13 の新機能』を参照してください。

show コマンドと debug コマンドによるゾーンベース ポリシー ファイアウォールの監視

ZFW は、ポリシー設定を表示し、ファイアウォール アクティビティを監視するための新しいコマンドを導入しました。

指定されたゾーンに含まれるゾーン説明とインターフェイスを表示します。

show zone security *[<zone-name>]*
ゾーン名が含まれていない場合、コマンドは設定されたすべてのゾーンの情報を表示します。

```
Router#show zone security z1 zone z1 Description: this is test zone1 Member Interfaces:
Ethernet0/0
```

送信元ゾーン、宛先ゾーン、ゾーンペアに添付されたポリシーを表示します。

show zone-pair security [source *<source-zone-name>***] [destination** *<destination-zone-name>***]**
送信元や宛先が指定されていないときには、すべてのゾーンペアが送信元、宛先、関連するポリシー付きで表示されます。 送信元/宛先ゾーンだけが指定された場合、送信元/宛先にこのゾーンを含むすべてのゾーンペアが表示されます。

```
Router#show zone-pair security zone-pair name zp Source-Zone z1 Destination-Zone z2 service-
```

`policy p1`
指定されたポリシーマップを表示します。

show policy-map type inspect [*<policy-map-name>* **[class** *<class-map-name>***]]**
ポリシーマップの名前が指定されていない場合、inspect タイプのすべてのポリシーマップが表示されます（サブタイプを含むレイヤ 7 ポリシーマップを含む）。

`Router#`**`show policy-map type inspect p1`** `Policy Map type inspect p1 Class c1 Inspect`
指定されたゾーンペアに存在するランタイム inspect タイプのポリシーマップ統計情報を表示します。

show policy-map type inspect zone-pair [*zone-pair-name***] [sessions]**
no zone-pair name が指定されると、すべてのゾーンペアのポリシーマップが表示されます。

sessions オプションは、指定されたゾーンペアのポリシーマップ適用によって作成された検査セッションを表示します。

`Router#`**`show policy-map type inspect zone-pair zp`** `Zone-pair: zp Service-policy : p1 Class-map: c1 (match-all) Match: protocol tcp 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 Last half-open session total 0 Class-map: c2 (match-all) Match: protocol udp Pass 0 packets, 0 bytes Class-map: class-default (match-any) Match: any Drop 0 packets, 0 bytes`
urlfilter キーワードは、指定されたポリシーマップ（またはゾーンペア名が何も指定されないときはすべてのターゲットのポリシーマップ）に付属する urlfilter 関連の統計情報を表示します。

show policy-map type inspect zone-pair [*zone-pair-name***] [urlfilter [cache]]**
cache キーワードは、**urlfilter** とともに指定されると、（IP アドレスの）**urlfilter** キャッシュを表示します。

inspect ポリシーマップ用の **show policy-map** コマンドの要約は次のとおりです。

show policy-map type inspect inspect { <policy name> [class <class name>] | zone-pair [<zone-pair name>] [sessions | urlfilter cache] }

ゾーンベース ポリシー ファイアウォール サービス拒否保護の調整

ZFW は、ネットワーク アクティビティの大幅な変更についてネットワーク エンジニアに警告し、ネットワーク アクティビティ変更の影響を削減するために DoS 保護を提供して不必要なアクティビティを軽減します。 ZFW は、すべてのポリシーマップのクラスマップ用の独立したカウンタを維持します。 つまり、1 つのクラスマップが 2 つの異なるゾーンペアのポリシーマップに使用された場合、DoS 保護カウンタの 2 つの異なるセットが適用されます。

ZFW は、Cisco IOS ソフトウェア リリースが 12.4(11)T になる前に、デフォルトとして DoS 攻撃軽減を提供します。 デフォルトの DoS 保護動作は Cisco IOS ソフトウェア リリース 12.4(11)T で変更されました。 ZFW DoS 保護の詳細と手順は、『Cisco IOS Firewall サービス拒否保護の調整』を参照してください。

TCP SYN DoS 攻撃の詳細は、『TCP SYN サービス拒否攻撃から保護するための戦略の定義』を

参照してください。

付録

付録 A： 基本設定

```
ip subnet-zero
ip cef
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2
 switchport access vlan 2
!
interface FastEthernet3
 switchport access vlan 2
!
interface FastEthernet4
 switchport access vlan 1
!
interface FastEthernet5
 switchport access vlan 1
!
interface FastEthernet6
 switchport access vlan 1
!
interface FastEthernet7
 switchport access vlan 1
!
interface Vlan1
 no ip address
 bridge-group 1
!
interface Vlan2
 no ip address
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.254 255.255.255.0
 ip route-cache flow
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
bridge 1 protocol ieee
bridge 1 route ip
!
end
```

付録 B： 最終 (全) 設定

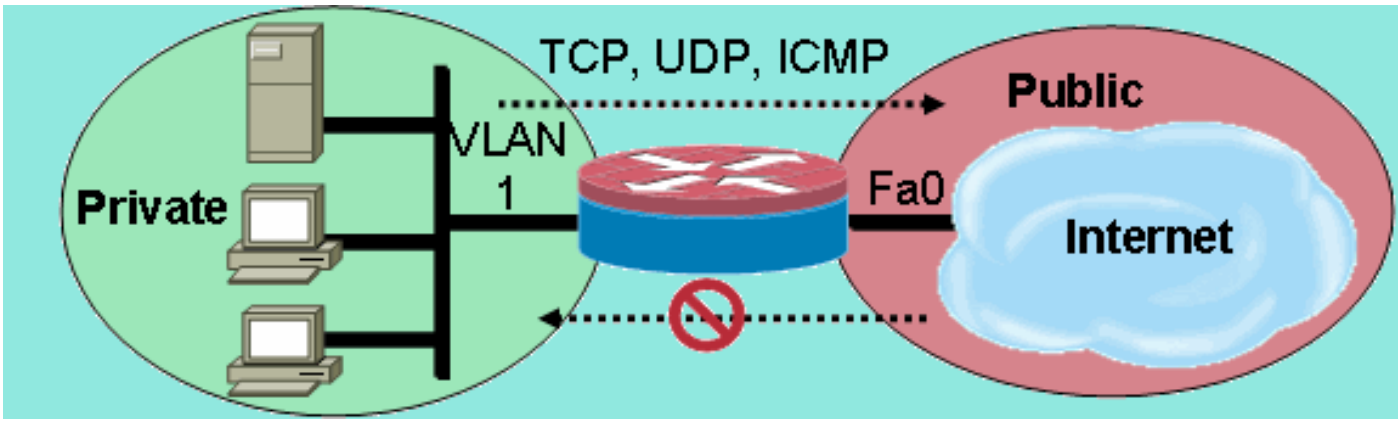
```
ip subnet-zero
ip cef
!
ip port-map user-Xwindows port tcp from 6900 to 6910
!
class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol pop
  match protocol imap
  match protocol esmtp
  match protocol http
class-map type inspect match-any dns-http-class
 match protocol dns
 match protocol http
class-map type inspect match-any smtp-class
 match protocol smtp
class-map type inspect match-all dns-http-acl-class
 match access-group 110
 match class-map dns-http-class
class-map type inspect match-all smtp-acl-class
 match access-group 111
 match class-map smtp-class
class-map type inspect match-any Xwindows-class
 match protocol user-Xwindows
class-map type inspect match-any internet-traffic-class
 match protocol http
 match protocol https
 match protocol dns
 match protocol icmp
class-map type inspect http match-any bad-http-class
 match  port-misuse all
 match  strict-http
!
policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
policy-map type inspect private-dmz-policy
  class type inspect L7-inspect-class
   inspect
policy-map type inspect internet-dmz-policy
 class type inspect dns-http-acl-class
  inspect
 class type inspect smtp-acl-class
  inspect
policy-map type inspect servers-clients-policy
 class type inspect Xwindows-class
  inspect
policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
  class type inspect bad-http-class
   drop
!
zone security clients
zone security servers
zone security private
zone security internet
zone security dmz
zone-pair security private-internet source private destination internet
```

```
  service-policy type inspect private-internet-policy
zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 zone-member internet
!
interface FastEthernet1
 ip address 172.16.2.1 255.255.255.0
 zone-member dmz
!
interface FastEthernet2
 switchport access vlan 2
!
interface FastEthernet3
 switchport access vlan 2
!
interface FastEthernet4
 switchport access vlan 1
!
interface FastEthernet5
 switchport access vlan 1
!
interface FastEthernet6
 switchport access vlan 1
!
interface FastEthernet7
 switchport access vlan 1
!
interface Vlan1
 no ip address
 zone-member clients
 bridge-group 1
!
interface Vlan2
 no ip address
 zone-member servers
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.254 255.255.255.0
 zone-member private
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
access-list 110 permit ip any host 172.16.2.2 access-list 111 permit ip any host 172.16.2.3 !
bridge 1 protocol ieee bridge 1 route ip ! End
```

付録 C： 2 つのゾーン用の基本ゾーンポリシー ファイアウォール設定

この例では、Cisco IOS ソフトウェア ZFW への機能強化をテストする機能の基本として簡単な設定を提供します。 この設定は、1811 ルータで設定する、2 つのゾーン用のモデル設定です。 プライベート ゾーンがルータの修正されたスイッチ ポートに適用されるので、スイッチ ポート上

のすべてのホストは VLAN 1 に接続されます。 パブリック ゾーンは FastEthernet 0 で適用されます。




```
class-map type inspect match-any private-allowed-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all http-class
 match protocol http
!
policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect my-parameters class type inspect private-allowed-class inspect ! zone security private
zone security public zone-pair security priv-pub source private destination public service-
policy type inspect private-allowed-policy ! interface fastethernet 0 zone-member security
public ! Interface VLAN 1 zone-member security private
```

関連情報

- テクニカルサポートとドキュメント - Cisco Systems