ゾーンベースポリシーファイアウォール設計について

内容

概要

このドキュメントでは、Cisco IOS® Firewallフィーチャセット、ゾーンベースポリシーファイアウォール(ZFW)の設定モデルについて説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、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。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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。

背景説明

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。

次に示す Cisco IOS Software Release 12.4(6)T 以前のほぼすべての従来の Cisco IOS ファイアウォール機能は、新しいゾーンベース ポリシー インスペクション インターフェイスでサポートされます。

- ステートフル パケット インスペクション
- VRF 認識型 Cisco IOS Firewall
- URL フィルタリング
- サービス妨害（DoS）の軽減

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

- HTTP
- Post Office Protocol（POP3）、インターネット メール アクセス プロトコル（IMAP）、SMTP/SMTP（SMTP/ESMTP）
- Sun リモート プロシージャ コール（RPC）
- インスタント メッセージング（IM）アプリケーション：Microsoft MessengerYahoo! MessengerAOL Instant Messenger
- ピアツーピア（P2P）でのファイル共有BittorrentKaZaAGnutellaeDonkey

Cisco IOS Software Release 12.4(11)T では、より容易な DoS 保護の調整用の統計情報が追加されました。

次に示す従来の Cisco IOS ファイアウォール機能と能力は、Cisco IOS Software Release 12.4(15)T の ZFW ではまだサポートされていません。

- 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 インスペクション
- TCP の順番の狂いに対するサポート

通常、ZFW はほとんどのファイアウォール インスペクション 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インスペクションサポートを備えていません。

ゾーンベース ポリシーの概要

従来の Cisco IOS ファイアウォール ステートフル インスペクション（以前はコンテキストベースのアクセス制御（CBAC））は、インターフェイスベースの設定モデルを採用していました。この設定モデルにおいて、ステートフル インスペクション ポリシーがインターフェイスに適用されていました。すべてのトラフィックがそのインターフェイスを通過し、同じ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 ポリシーの精度を制限し、ファイアウォール ポリシーの適切な適用にあたって混乱をきたす原因となり、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シナリオにおいて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 モデルから、より柔軟性があり、より簡単に理解できるゾーンベース 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、インスペクション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)で設定されます。CPLは、階層構造を採用して、ネットワークプロトコルのインスペクションと、インスペクションを適用できるホストのグループを定義します。

ゾーンベース ポリシー設定モデル

ZFW では、従来の Cisco IOS Firewall と比べて、Cisco IOS Firewall インスペクションの設定方法を全面的に変更しました。

ファイアウォールの設定の第一の主な変更は、ゾーンベースの設定をサポートしたことです。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。その他の機能は、時間の経過とともにゾーンモデルを採用できます。ip inspect コマンドを採用する従来の Cisco IOS ファイアウォール ステートフル インスペクション (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、従来のコマンドライン インターフェイス (CLI) で設定できる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 インスペクション コマンドや 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。インターフェイスをセキュリティゾーンメンバーとして設定し、同時にip inspect用に設定することはできません (インターフェイスのIPアドレスを指定する必要があります) 。

ゾーンは、ネットワークのセキュリティ境界を設定します。ゾーンは、トラフィックがネットワークの別の領域に移動するときにポリシーの制限の対象となる境界を定義します。ゾーン間のZFWデフォルトポリシーはdeny allです。ポリシーが明示的に設定されていない場合、ゾーン間を移動するすべてのトラフィックがブロックされます。これは、アクセスコントロールリスト(ACL)で明示的にブロックされるまでトラフィックが暗黙的に許可されるステートフル検査モデルとは大きく異なります。

主な変更の第 2 は、CPL という新しい設定ポリシー言語の導入です。Cisco IOSソフトウェアのモジュラQoS(Quality-of-Service)CLI(MQC)に精通しているユーザであれば、この形式がクラスマップのQoS使用に類似していることを認識し、ポリシーマップで適用されるアクションによって影響を受けるトラフィックを指定できます。

ゾーンベースポリシーファイアウォールアプリケーションのルール

ゾーン内のルータネットワークインターフェイスメンバーシップは、ゾーンメンバーインターフェイス間を移動するトラフィックと同様に、インターフェイスの動作を制御する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。
- 特定の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ゾーンに割り当てられると黙示的にブロックされます (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、ルータのインターフェイスへのトラフィックを除く) 。
- トラフィックは、デフォルトで、同じゾーンのメンバーであるインターフェイス間で行き来することを黙示的に許可されています。

- ゾーンメンバーインターフェイスとの間のトラフィックを許可するには、そのゾーンと他のゾーンとの間でトラフィックを許可または検査するポリシーを設定する必要があります。
- 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。
- トラフィックは、ゾーン メンバー インターフェイスと、ゾーン メンバーではないインターフェイス間を行き来できません。pass、inspect、drop 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、従来のステートフルインスペクション/CBAC設定を引き続き使用できます。
- ボックス上のインターフェイスがゾーン/ファイアウォールポリシーの一部にならないことが必要な場合。そのインターフェイスをゾーンに配置し、そのゾーンとトラフィックフローが必要な他のゾーンとの間にパスオールポリシー（ダミーポリシーの一種）を設定する必要が生じる場合もあります。
- 前述の動作から、トラフィックがルータ内のすべてのインターフェイス間を流れる場合、すべてのインターフェイスがゾーニングモデルの一部である必要があります（各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ーである必要があります）。
- 前述の動作の唯一の例外であるデフォルトの拒否方法は、ルータとの間のトラフィックです。これはデフォルトで許可されています。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。

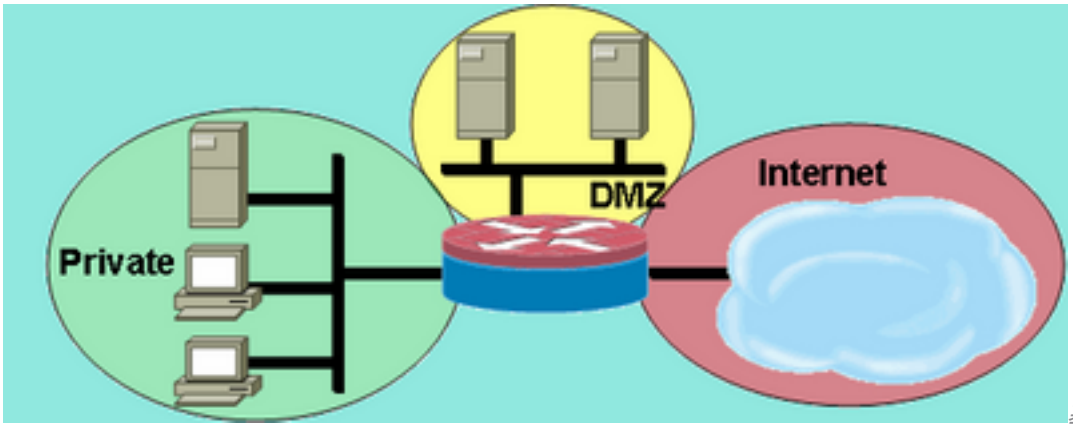
ゾーンベースポリシーネットワークセキュリティの設計

セキュリティゾーンは、ネットワーク内の相対的なセキュリティの領域ごとに設定する必要があります。これにより、同じゾーンに割り当てられたすべてのインターフェイスが同様のセキュリティレベルで保護されます。たとえば、次のように 3 つのインターフェイスを持つアクセス ルータを考えます。

- 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アクセスできてはいけないプライベート 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、ドメイン ネーム システム（DNS）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 サービスの Demilitarized Zone（DMZ; 緩衝地帯）に接続されている

パブリックインターネットからDMZ内の特定のホストへのさまざまなアクセスを許可し、保護されたLAN内のホストに対して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が、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（図1を参照）。

図 1：基本セキュリティ ゾーン トポロジ



基本セキュリティ ゾーン トポロジ

この例では、各ゾーンは、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を追加すると、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、同じゾーン内の現在のインターフェイス上のすべてのホストにトラフィックを渡すことができます。また、他のゾーン内のホストへのホストトラフィックも、同様に現在のポリシーの影響を受けます。

通常、この例のネットワークには3つの主要な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公開されるため、DMZホストは、1つ以上のDMZホストに損害を与える可能性のある悪意のある個人による望ましくないアクティビティの対象となる可能性があります。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 ホストのいずれ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なる攻撃を実行するために 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 ポスチャを含みます。したがって、DMZ ホストが他のネットワークへのアクセスを明示的に許可されている場合を除いて、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 ゾーンにアクセスする権限がインターネット ホストに付与されないため、プライベート ゾーン ホストはインターネット ホストによる望ましくないアクセスから保護されます。

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

最近行われた IPsec VPN 強化により、VPN 接続に関するファイアウォール ポリシー設定が簡略化されました。IPSec仮想トンネルインターフェイス(VTI)およびGRE+IPSecでは、指定し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、特定のセキュリティゾーンへのVPNサイト間およびクライアント接続を限定できます。接続が特定のポリシーによって制限される必要がある場合は、接続を VPN DMZ 内で隔離できます。または、VPN 接続が黙示的に信頼されている場合は、ネットワーク内で信頼されている接続と同じセキュリティ ゾーンに VPN 接続を配置できます。

非 VTI IPSec が適用される場合、セキュリティを維持するために、VPN 接続ファイアウォール ポリシーは厳重な精査が必要です。ゾーンポリシーは、リモートサイトホストまたはVPNクライアントのIPアドレスによるアクセスを明示的に許可する必要があります。これは、セキュアホストがルータへのVPNクライアント暗号化接続とは異なるゾーンにある場合に行われます。アクセスポリシーが正しく設定されていないと、保護する必要があるホストが、望ましくない、潜在的に悪意のあるホストにさらされてしまう可能性があります。概念と設定に関する詳細な説明については、『VPN とゾーンベース ポリシー ファイアウォールの併用』を参照してください。

シスコ ポリシー言語（CPL）の設定

この手順は ZFW の設定に使用できます。手順の順番は重要ではありませんが、一部のイベントは順番どおりに完了する必要があります。たとえば、クラスマップをポリシーマップに割り当てる前に、クラスマップを設定する必要があります。同様に、ポリシーを設定しない限り、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. 通過するゾーン ペアをそれとして適用されるポリシーを持つ必要が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. クラスマップトラフィックにアクションを適用するポリシーマップを定義します。
5. ゾーン ペアにポリシーマップを適用します。
6. ゾーンにインターフェイスを割り当てます。

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、ポリシー アプリケーションに対してファイアウォールが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、ここに記載される次の基準に基づいてトラフィックをソートします。これらの基準は、クラスマップのmatchコマンドで指定されます。

- Access-group：標準、拡張、または名前付き ACL は、送信元と宛先の IP アドレスおよび送信元と宛先ポートに基づい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既知の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。
- Class-map：追加の一致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。
- Not: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。

「一致」基準の組み合わせ：「Match-Any」 対 「Match-All」

クラスマップは、一致基準を適用する方法を決定するための match-any または match-all 演算子を適用できます。match-anyを指定した場合、トラフィックはクラスマップ内の一致基準の1つのみを満たす必要があります。match-allを指定した場合、トラフィックはその特定のクラスに属するために、クラスマップのすべての基準に一致する必要があります。

トラフィックが複数の基準を満たす場合は、一致基準を詳細から非詳細の順に適用する必要があります。たとえば、次のクラスマップについて考えてみましょう。

```
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 インスペクション サービス固有の機能によって確実に処理されるよう、match protocol http に最初に遭遇する必要があります。照合行が逆になり、トラフィックがmatch protocol httpと比較する前にmatch protocol TCP文に遭遇する場合、トラ

フィックは単にTCPトラフィックとして分類され、ファイアウォールTCPインスペクションコンポーネントの機能に基づいて検査されます。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シグナリング サービスで問題になります。これらのサービスには、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インスペクション機能が必要です。

一致基準としてのACLの適用

クラスマップは、ポリシー アプリケーションの一致基準の 1 つとして ACL を適用できます。クラスマップが基準のみに一致するACLで、クラスマップがインスペクションアクションを適用するポリシーマップに関連付けられている場合、ルータは、ZFWがアプリケーション対応のインスペクションを提供する場合を除き、ACLで許可されているすべてのトラフィックに対して基本的なTCPまたはUDPインスペクションを適用します。これには、FTP、SIP、Skinny(SCCP)、H.323、Sun RPC、およびTFTPが含まれますが、これらに限定されません。アプリケーション固有のインスペクションが利用可能であり、ACL がプライマリまたは制御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/制御に関連付けられたセカンダリまたはメディア チャネルが許可されます。

クラスマップが一致基準として 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、特定のゾーンペアに適用されるサービスポリシーの方向で許可され、これに対応するリターントラフィックは反対方向で許可されます。したがって、ACL は、特定目的のタイプにトラフィックを限定するための制限を適用する必要があります。PAMリストにHTTP、NetBIOS、H.323、DNSなどのアプリケーションサービスが含まれていることに注意してください。ただし、特定のポートの特定のアプリケーション使用に関するPAMの知識にもかかわらず、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応するために十分なアプリケーション固有の機能のみを適用します。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 コマンド出力にまとめて統合されます。ネットワークアクティビティに対するアプリケーション固有の可視性が必要な場合は、アプリケーション名でサービスのインスペクションを設定する必要があります（match protocol HTTPの設定、match protocol telnetの設定など）。

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 ゾーンで発信されるすべてのトラフィックを定義し、これに対処するのが容易である一方 (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)、サービス アクティビティへの可視性は限定され、特定のタイプのトラフィックに対して 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、ゾーンペア間で 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
```

対照的に、アプリケーション固有のクラスを追加する同様の設定では、より細かいアプリケーション統計情報と制御が提供され、ポリシーマップの最後のチャンスとしてACLのみに一致する最後のチャンスのクラスマップを定義するときに最初の例に示したのと同じ幅広いサービスが引き続き提供されます。

```
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
```

より詳細な設定により、show policy-map type inspect zone-pair priv-pub コマンドに対して、次のような細かい下位出力を提供します。

```
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
```

前述のように、より詳細なクラスマップおよびポリシーマップ設定を使用する場合のもう1つの利点は、セッション値とレート値にクラス固有の制限を適用できることです。そして、パラメータマップを適用して検査パラメータを具体的に調整し、各クラスの検査動作を調整する。

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、class class-default という名前のデフォルト クラスがクラスの最後に適用されます。class class-defaultデフォルトポリシーアクションはdropですが、passに変更できます。ログ オプションに drop アクションを追加することもできます。インスペクトは 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、1 つの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。

- Drop：これは、すべてのinspect-typeポリシーマップを終了する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についても、不必要なトラフィックをドロップするために設定できます。ZFW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動作とは対照的に、廃棄アクションによって処理されるトラフィックを通知なしに廃棄します（つまり、廃棄の通知が関連するエンドホストに送信されません）。現在、サイレントドロップ動作を変更するオプションはありません。ログ オプションに、トラフィックがファイアウォールによってドロップされた旨の syslog 通知用のドロップを追加できます。
- Pass：このアクションは、ルータが 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許可します。pass 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。pass は、一方向のトラフィックのみを許可します。リターントラフィックが反対方向に通過できるようにするには、パラレルポリシーを適用する必要があります。pass アクションは、IPSec ESP、IPSec AH、ISAKMP、および予測可能な動作を伴うその他の本来的にセキュアなプロトコルに便利です。ただし、ほとんどのアプリケーション トラフィック

は ZFW 内でインスペクト アクションを使用してより適切に処理されます。

- Inspect：inspect アクションは、状態に基づいてトラフィックを制御します。たとえば、前述の例のネットワーク内のプライベート ゾーンからインターネット ゾーンへのトラフィックのインスペクションを行う場合、ルータは TCP および User Datagram Protocol（UDP）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。したがって、ルータは、プライベート ゾーン接続要求に応じて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、inspectは、脆弱または機密性の高いアプリケーショントラフィックを伝送できる特定のサービスプロトコルに対して、アプリケーションの検査と制御を提供できます。監査証跡にパラメータマップを適用し、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ことができます。

アクションは、ポリシーマップの内のクラスマップと関連付けられます。

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

パラメータマップには、特定のクラスマップ検査ポリシーの接続パラメータを変更するためのオプションがあります。

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、DoS保護、TCP接続/UDPセッションタイマー、監査証跡ロギング設定などのパラメータについて、ZFWのインスペクション動作を指定します。また、パラメータマップには、HTTP オブジェクト、POP3 および IMAP 認証要件、他のアプリケーション固有の情報など、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も適用されます。

ZFW のインスペクション 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類似する 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
```

特定のタイプのパラメータマップは、レイヤ 7 アプリケーション インスペクション ポリシーによって適用されたパラメータを指定します。正規表現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アプリケーションインスペクションで使用する正規表現を定義します。

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

protocol-info-typeパラメータマップは、IMアプリケーションインスペクションで使用する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 インスペクションの設定の詳細情報については、このドキュメントのそれぞれのアプリケーション インスペクション 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ポリシーのロギングの適用

ZFW は、デフォルトでドロップまたはインスペクションが行われるトラフィック、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。監査証跡口ギングは、ZFW がインスペクションを行うトラフィックに利用可能です。監査証跡は、監査証跡がパラメータマップで定義され、検査アクションを含むパラメータマップがポリシーマップで適用されるときに適用されます。

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [parameter-map-name (optional)]
```

ドロップ ロギングは、ZFW がドロップするトラフィックに利用可能です。廃棄口ギングは、ポリシーマップで廃棄アクションを含む口グを追加するときに、次のように設定されます。

```
configure terminal
 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と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 構造を変更できる工ディタを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 ステートメント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配置するために、次のステップを実行する必要があります。

1. 現在の構造をMicrosoft Windowsのメモ帳などのテキスト工ディタまたはLinux/Unixプラットフォームのviなどの工ディタにコピーします。
2. 現在の構造をルータ設定から削除します。
3. 構造をテキスト 工ディタで編集します。
4. 構造をルータのCLIにコピーし直します。

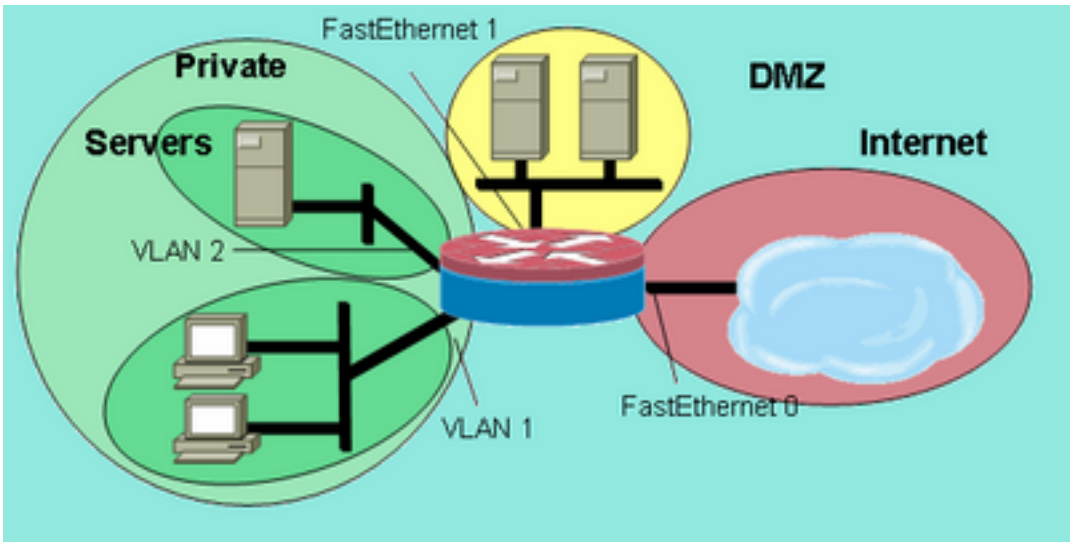
設定例

この設定例では、Cisco 1811 サービス統合型ルータを採用しています。IP接続、VLAN設定、および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ングの基本設定については、「付録A」を参照してください。ルータは次の 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ため、これらの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間のトラフィックにのみ影響します。
- 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）。

図 2：ゾーン トポロジの詳細

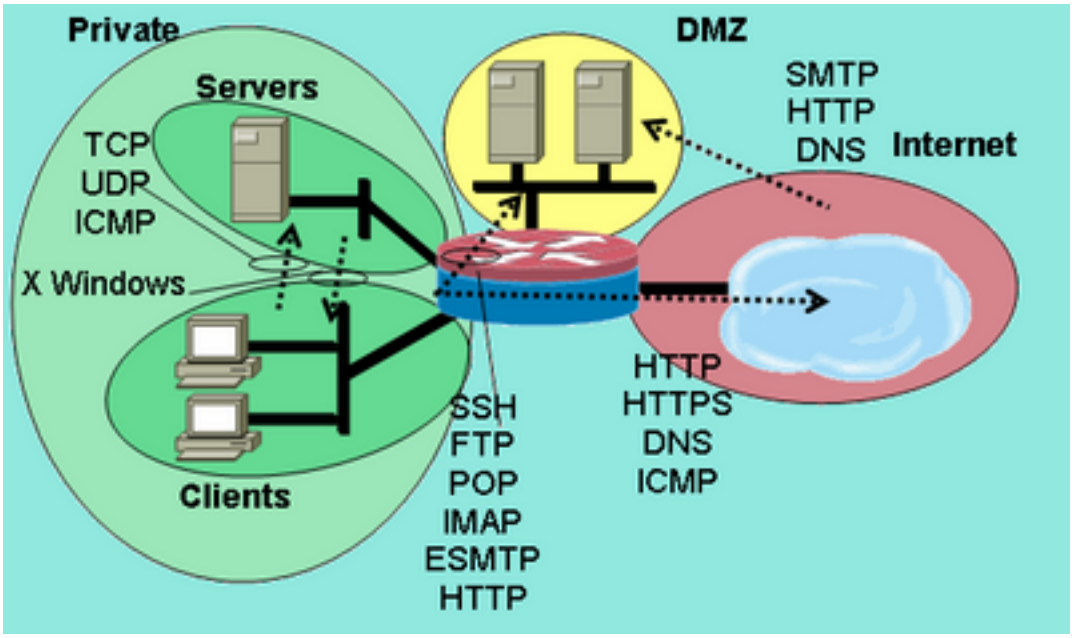


ゾーン トポロジの詳細

次のポリシーが適用され、以前に定義したネットワークゾーンが適用されます。

- 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。もう一方のサーバは、SMTP、HTTP、およびHTTPSサービスを提供します。ファイアウォールポリシーは、各ホストで使用可能な特定の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 ゾーン内のホストは、すべての TCP、UDP、ICMP サービスでサーバ ゾーン内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、例外として、UNIX ベースのアプリケーション サーバは、ポート 6900 ~ 6910 上にあるクライアント ゾーン内のデスクトップ PC 上で X Windows クライアント セッションを X Windows サーバ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、および 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、サポートされているIMおよびP2Pアプリケーションがポート80で伝送されないように、プライベートゾーンからインターネットゾーンへのHTTP接続にアプリケーションインスペクションが適用されます（図3を参照）。

図 3：設定例に適用されるゾーンペア サービス権限



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、次の複雑度の順番で設定されます。

1. クライアントとサーバ間の TCP/UDP/ICMP インスペクション
2. プライベートと DMZ 間の SSH/FTP/POP/IMAP/ESMTP/HTTP インスペクション
3. ホスト アドレスで制限されたインターネットと DMZ 間の SMTP/HTTP/DNS インスペクション
4. ポートアプリケーション マッピング（PAM）で指定されたサービスを伴うサーバとクライアント間の X Windows インスペクション
5. HTTP アプリケーション インスペクションを伴うプライベートとインターネット間の HTTP/HTTPS/DNS/ICMP

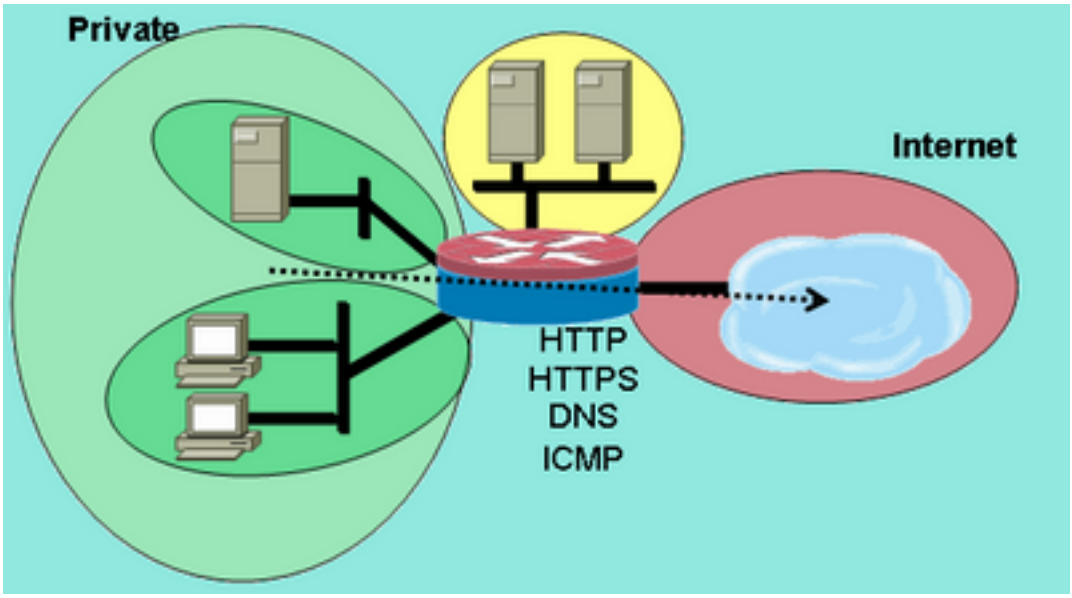
設定の一部を異なる時間に異なるネットワークセグメントに適用するため、ネットワークセグメントをゾーンに配置すると、他のセグメントへの接続が失われることに注意してください。たとえば、プライベートゾーンが設定されると、プライベートゾーン内のホストは、それぞれのポリシーが定義されるまで、DMZゾーンとインターネットゾーンへの接続を失います。

ステートフル インスペクション 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 ゾーンまでのサービス インスペクション



プライベート ゾーンからインターネット ゾーンまでのサービス インスペクション

プライベート インターネット ポリシーは、HTTP、HTTPS、DNS、およびプライベート ゾーンからインターネット ゾーンまでの ICMP に対するレイヤ 4 インスペクションにレイヤ 4 インスペクションを適用します。これにより、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、リターントラフィックが許可されます。レイヤ7インスペクションには、アプリケーション制御の強化、セキュリティの向上、および修正が必要なアプリケーションのサポートという利点があります。ただし、検査用に設定されていないレイヤ7プロトコルはゾーン間で許可されないため、前述のようにレイヤ7検査を行うには、ネットワークアクティビティをより深く理解する必要があります。

1. 前述のポリシーに基づいて、ゾーン間で許可するトラフィックを説明するクラスマップを定義します。
```
configure terminal
 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のインスペクションを行うポリシーマップを設定します。
```
configure terminal
 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。
```
configure terminal
 zone security private
 zone security internet
 int bvi1
  zone-member security private
 int fastethernet 0
  zone-member security internet
```

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：次に示すように、プライベートゾーンを発信元とし、インターネット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。

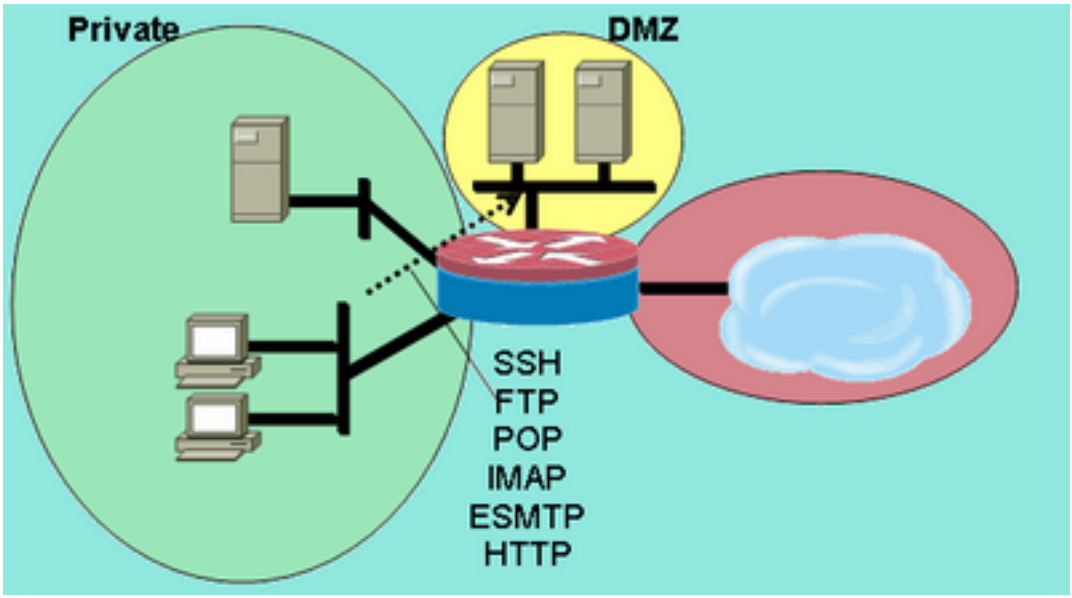
```
configure terminal
 zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
```

これで、クライアント ゾーンからサーバ ゾーンへの HTTP、HTTPS、DNS、および ICMP の接続を許可し、HTTP トラフィックにアプリケーション インスペクションを適用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 上を通過しないことを確実にするための、プライベート インターネット ゾーン ペアに対するレイヤ 7 インスペクション ポリシーの設定が完了します。

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 ゾーンまでのサービス インスペクション



プライベート ゾーンから DMZ ゾーンまでのサービス インスペクション

プライベート DMZ ポリシーの場合、ゾーン間のネットワーク トラフィックをより深く理解することが必要となるため、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 ゾーンまでレイヤ 7 インスペクションを適用します。これにより、プライベートゾーンからDMZへの接続が許可され、リターントラフィックが許可されます。レイヤ7インスペクションには、アプリケーション制御の強化、セキュリティの向上、および修正が必要なアプリケーションのサポートという利点があります。ただし、検査用に設定されていないレイヤ7プロトコルはゾーン間で許可されないため、前述のようにレイヤ7検査を行うには、ネットワークアクティビティをより深く理解する必要があります。

1. 前述のポリシーに基づいて、ゾーン間で許可するトラフィックを説明するクラスマップを定義します。
   ```
   configure terminal
    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. 定義したばかりのクラスマップにトラフィックのインスペクションを行うポリシーマップを

設定します。

```
configure terminal
 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。

```
configure terminal
 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：次に示すように、現在のプライベートDMZゾーンペアを設定するだけで、DMZに移動するプライベートゾーンを送信元とする接続を検査できます。

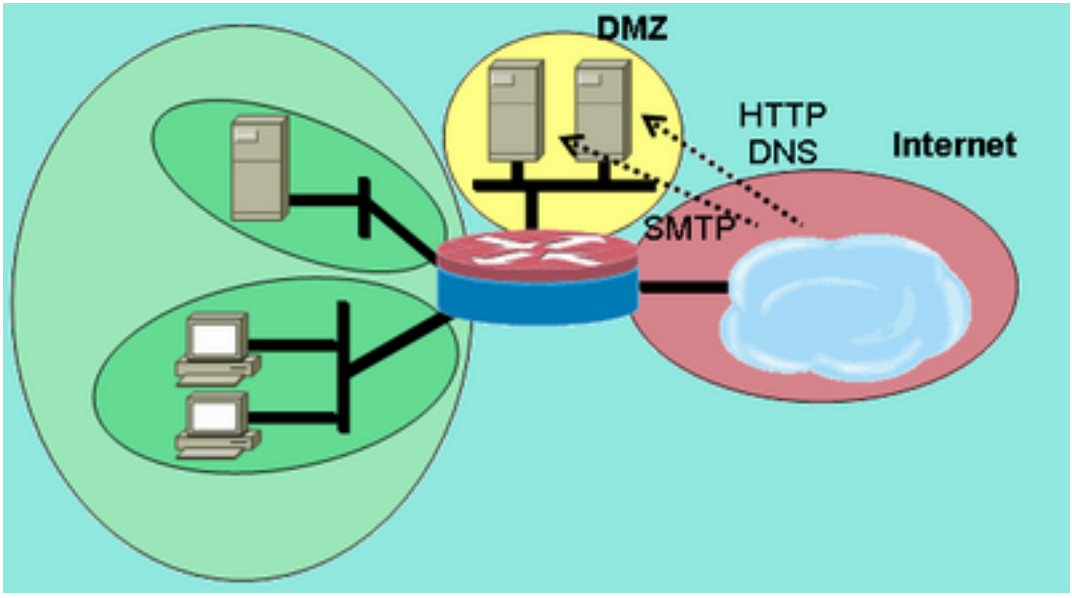
```
configure terminal
 zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
```

これで、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、および ICMP の接続を許可するための、プライベート DMZ に対するレイヤ 7 インスペクション 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対しては修正を適用しませんが、ほとんどのアプリケーション接続に対応する単純なポリシーの例を示します。

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 ゾーンまでのサービス インスペクション



インターネット ゾーンから DMZ ゾーンまでのサービス インスペクション

このポリシーは、インターネット ゾーンから DMZ ゾーンまでレイヤ 7 インスペクションを適用します。これにより、インターネットゾーンからDMZへの接続が許可され、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が許可されます。インターネット

DMZ ポリシーは、特定のホスト上の特定のサービス、ホスト グループ、またはサブネットへのアクセスを制限するために、レイヤ 7 インスペクションと ACL によって定義されたアドレス グループを組み合わせます。これを実現するには、IPアドレスを指定するACLを参照す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します。

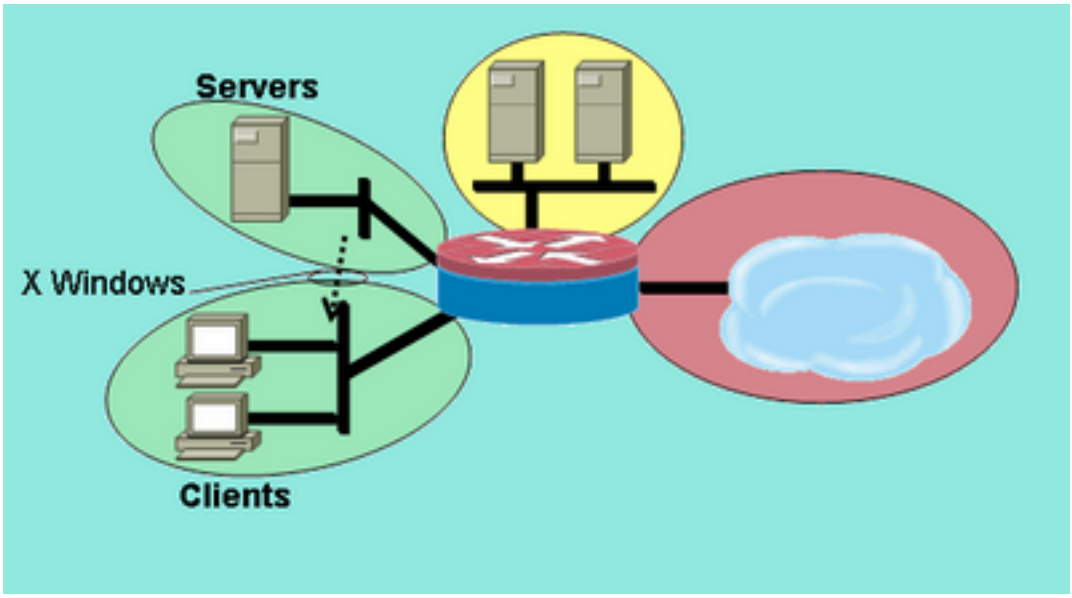
1. 前述のポリシーに基づいて、ゾーン間で許可するトラフィックを記述するクラスマップとACLを定義します。2台の異なるサーバへのアクセスには異なるアクセスポリシーが適用されるため、サービスに対して複数のクラスマップを使用する必要があります。インターネットホストは172.16.2.2へのDNSおよびHTTP接続が許可され、SMTP接続は172.16.2.3への接続が許可されます。クラスマップの違いに注意してください。サービスを指定するクラスマップは match-any キーワードを使用してリストされているサービスを許可します。ACL をサービス クラスマップと関連付けるクラスマップは match-all キーワードを使用して、トラフィックを許可するためにクラスマップ内の両方の条件が満たされる必要があると要求します。
```
configure terminal
 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. 定義したばかりのクラスマップにトラフィックのインスペクションを行うポリシーマップを設定します。
```
configure terminal
 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。前のセクションで設定した場合は、DMZ の設定をスキップします。
```
configure terminal
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**：現在のインターネットDMZゾーンペアを設定して、次に示すように、インターネットゾーンを送信元とし、DMZゾーンに移動する接続を検査するだけです。
```
configure terminal
 zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
```
これで、インターネット DMZ ゾーンペアに対するアドレス固有のレイヤ 7 インスペクション ポリシーの設定が完了します。

ステートフル インスペクション トランスペアレント ファイアウォール

クライアントとサーバ間のポリシーの設定

次の図に、サーバクライアントポリシーの設定を示します。

図 7：サーバ ゾーンからクライアント ゾーンまでのサービス インスペクション



サーバ ゾーンからクライアント ゾーンまでのサービス インスペクション

サーバクライアントポリシーは、ユーザ定義のサービスで検査を適用します。レイヤ 7 インスペクションは、サーバ ゾーンからクライアント ゾーンまで適用されます。これにより、サーバゾーンからクライアントゾーンまでの特定のポート範囲へのX Windows接続が許可され、リターントラフィックが許可されます。X WindowsはPAMでネイティブにサポートされるプロトコルではないため、ZFWが適切なトラフィックを認識して検査できるように、PAMでユーザ設定サービスを定義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は、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、ブリッジグループ内のインターフェイス間のブリッジングを提供し、Bridge Virtual Interface(BVI)を介して他のサブネットにルーティングします。 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」トラフィックにはファイアウォールインスペクションを適用しますが、BVI経由でブリッジグループから出るトラフィックには適用しません。インスペクション ポリシーは、ブリッジグループを通過するトラフィックのみに適用されます。したがって、このシナリオでは、インスペクションは、プライベートゾーン内にネストされてい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のみ適用されます。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のみ関与します。クライアントゾーンまたはサーバゾーンからBVIを介してトラフィックが発信される場合、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ホストされているクライアント）は、ポート6900から始まる範囲のクライアント（ユーザが作業するクライアント）に対して表示情報の接続を開きます。追加される各接続は連続するポートを使用するため、クライアントが 1 つのホスト上で 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。したがって、6900 ～ 6909のポート範囲を検査すると、6909を超えるポートに対して開かれた接続は失敗します。

```
configure terminal
 ip port-map user-Xwindows port tcp from 6900 to 6910
```

2. PAM のドキュメントを確認または、PAM と Cisco IOS Firewall ステートフル インスペクション間の相互運用性の詳細についての情報に関する粒度の細かいプロトコル インスペクションのドキュメンテーションをチェックして、追加の PAM の質問に対処してください。
3. 前述のポリシーに基づいて、ゾーン間で許可するトラフィックを説明するクラスマップを定義します。

```
configure terminal
 class-map type inspect match-any Xwindows-class
  match protocol user-Xwindows
```

4. 定義したばかりのクラスマップにトラフィックのインスペクションを行うポリシーマップを設定します。

```
configure terminal
 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、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は、ゾーンペア定義までスキップします。IRB 設定のブリッジングは、完全性のために提供されます。

```
configure terminal
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：**次に示すように、現在のサーバとクライアントのゾーンペアを設定するだけで、サーバゾーンを送信元とし、クライアントゾーンに移動する接続を検査できます。

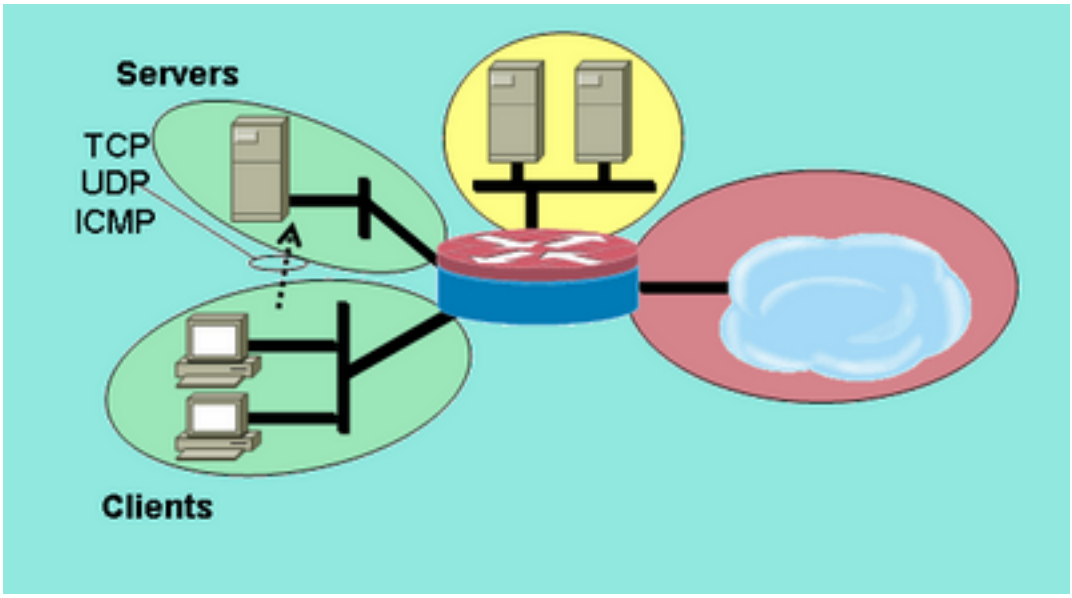
```
configure terminal
 zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
```

これで、サーバ ゾーンからクライアント ゾーンへの X Windows 接続を許可するためのクライアント サーバ間ゾーン ペア内のユーザ定義インスペクション ポリシーの設定が完了します。

クライアント サーバ間ポリシーの設定

図 8 は、クライアント サーバ間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 ゾーンまでのサービス インスペクション



クライアント ゾーンからサーバ ゾーンまでのサービス インスペクション

クライアント サーバ間ポリシーは他のものよりも複雑度が低くなります。レイヤ 4 インスペクションは、クライアント ゾーンからサーバ ゾーンまで適用されます。これにより、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、リターントラフィックが許可されます。レイヤ 4 インスペクションは、ファイアウォールの設定のシンプルさと、アプリケーション トラフィックを許可するためにわずかなルールだけを必要とするメリットを備えています。ただし、レイヤ 4 インスペクションは、次の 2 つの大きな欠点も抱えています。

- FTPや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を頻繁にネゴシエートします。この機能は通常、制御チャネルダイアログを監視し、下位チャネルを許可するサービスフィックスアップに対応します。この機能は、レイヤ 4 インスペクションでは利用できません。
- レイヤ 4 インスペクションでは、ほぼすべてのアプリケーション層のトラフィックが許可されています。ファイアウォール経由で少数のアプリケーションだけを許可するようネットワーク利用を制御する必要がある場合は、ACL を発信トラフィック上で設定し、ファイアウォール経由で許可されるサービスを制限する必要があります。

両方のルータインターフェイスがIEEEブリッジグループで設定されているため、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インスペクションを適用します。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のみ適用されます。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. 前述のポリシーに基づいて、ゾーン間で許可するトラフィックを説明するクラスマップを定義します。
```
configure terminal
 class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 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のインスペクションを行うポリシーマップを設定します。
```
configure terminal
 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。

```
configure terminal
 zone security clients
 zone security servers
 interface vlan 1
  zone-member security clients
 interface 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：**必要な操作は、現在のクライアント/サーバゾーンペアを設定して、次に示すように、クライアントゾーンを送信元とし、サーバゾーンに移動する接続を検査することだけです。

```
configure terminal
 zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
```

これで、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、および ICMP の接続を許可するための、クライアント サーバ間ゾーンペアに対するレイヤ 4 インスペクション 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応する単純なポリシーの例を示します。

ゾーンベースポリシーファイアウォールのレートポリシー

データネットワークは、特定の種類のネットワークトラフィックの伝送速度を制限する機能や、優先順位の低いトラフィックがビジネスに不可欠なトラフィックに与える影響を制限する機能によって、多くの場合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（TPおよびTPプライオリティ）を使用してこの機能を提供し、トラフィックの公称レートとバーストを制限します。Cisco IOSソフトウェアは、Cisco IOSリリース12.1(5)T以降、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では、あるセキュリティゾーンから別のセキュリティゾーンにファイアウォールを通過する際に、特定のクラスマップの定義に一致する適用トラフィックをポリシングする機能を追加すると、レート制限によりZFWが強化されます。これにより、特定のトラフィックを記述し、ファイアウォールポリシーを適用し、そのトラフィックの帯域幅消費をポリシングする1つの設定ポイントという利便性が提供されます。ZFWは、ポリシー準拠のための送信アクションとポリシー違反のための廃棄アクションのみを提供するという点で、インターフェイスベースとは異なります。ZFWはトラフィックをDSCPにマークできません。

ZFWは、バイト/秒、パケット/秒、および帯域幅の割合で帯域幅の使用のみを指定できます。ZFWは、インターフェイスベースの場合とない場合があります。したがって、追加機能が必要な場合は、これらの機能をインターフェイスベースで適用できます。インターフェイスベースがファイアウォールと組み合わせて使用される場合は、ポリシーが競合しないことを確認します。

ZFWポリシーの設定

ZFWポリシングは、ポリシーマップクラスマップ内のトラフィックを、8,000 ~ 2,000,000,000ビット/秒のユーザ定義レート値に制限します。バースト値は1,000 ~ 512,000,000バイトの範囲で設定できます。

ZFW ポリシングは、ポリシーマップ内に設定の行を追加することによって設定されます。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

ZFWポリシーでは、クラスマップに一致する適用ポリシーマップ内のトラフィックのセッション数を制限するセッション制御も導入されました。これにより、クラスマップごとにDoS保護ポリシーを適用する現在の機能が追加されます。これにより、ゾーンペアを通過する任意のクラスマップに一致する適用セッションの数をきめ細かく制御できます。同じクラスマップを複数のポリシーマップまたはゾーンペアで使用する場合、さまざまなクラスマップのアプリケーションに異なるセッション制限を適用することができます。

セッション制御は、目的のセッションボリュームを含むパラメータマップが設定されると適用され、そのパラメータマップは、ポリシーマップの下のクラスマップに適用されるインスペクションアクションに追加されます。

```
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のみ適用でき、通過または廃棄アクションでは使用できません。

ZFWセッション制御および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 インスペクション

アプリケーション インスペクションは ZFW に追加の機能を提供します。アプリケーション インスペクション ポリシーは、OSI モデルのレイヤ 7 で適用されます。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することを許可するメッセージを送受信します。一部のアプリケーションは、望ましくない機能や脆弱な機能を提供する可能性があるため、これらの機能に関連付けられたメッセージをフィルタリングして、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 サービスに対してアプリケーション インスペクションと制御を行います。

- 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

アプリケーション検査および制御（AIC）の機能はサービスごとに異なります。HTTPインスペクションでは、複数のタイプのアプリケーションアクティビティに対して詳細なフィルタリングを行うことができ、転送サイズ、Webアドレスの長さ、およびブラウザアクティビティを制限する機能を提供して、アプリケーション動作標準への準拠を強制し、サービス経由で転送されるコン

テンツのタイプを制限します。SMTP の AIC はコンテンツ長を制限し、プロトコル コンプライアンスを強制することができます。POP3およびIMAPインスペクションは、ユーザがセキュアな認証メカニズムを使用してユーザクレデンシャルの侵害を防ぐのに役立ちます。

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セットとして設定されます。その後、検査ポリシーマップでアプリケーションサービスポリシーを定義するときに、これらのセットが現在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 インスペクション

アプリケーションインスペクションをHTTPトラフィックに適用して、IM、P2Pファイル共有(P2P File Sharing)、およびファイアウォールで保護されていないアプリケーションをTCP 80経由で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サービスポートの不必要な使用を制御できます。

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ようにアプリケーション インスペクションの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 インスペクションの強化

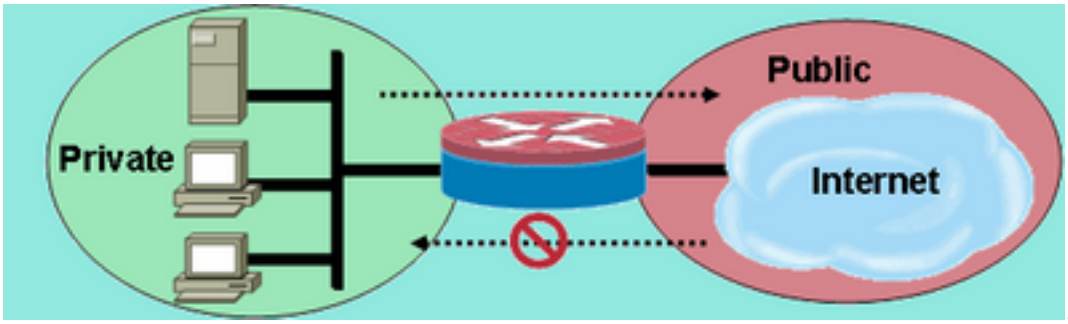
Cisco IOSソフトウェアリリース12.4(9)Tでは、ZFW HTTPインスペクション機能が改善されています。Cisco IOS Firewall では、Cisco IOS Software Release 12.3 (14) T で、HTTP アプリケーション インスペクションがサポートされます。Cisco IOSソフトウェアリリース12.4(9)Tでは、次の機能を追加すると、現在の機能が強化されます。

- 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、モニタする機能。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のに便利です。
- 最大URL長、最大ヘッダー長、最大ヘッダー数、最大ヘッダー行の長さなど、HTTP要求および応答ヘッダー内の異なる要素のサイズを制限する機能バッファオーバーフローを防ぐのに役立ちます。

- 同じ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ぐのに便利です。
- 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/モニタする柔軟性を提供します。HTTP RFC は、HTTP メソッドの制限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、安全ではないと見なされます。標準以外のメソッドの多くに、不正なセキュリティ レコードが含まれます。
- ユーザが設定した正規表現に基づいて特定の URI をブロックするメソッド。この機能により、ユーザはカスタムURIとクエリーをブロックできます。
- 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習得してから、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。
- 1 つ以上の HTTP パラメータ値が正規表現としてユーザが入力した値と一致する場合、HTTP 接続をブロックまたはこれに対してアラートを発行する機能。可能な HTTP 値のコンテキストの一部には、ヘッダー、本文、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 変数が含まれます。

HTTPアプリケーションインスペクションを改善するための設定例では、図9に示すシンプルなネットワークを想定しています。

図 9：シンプルなネットワークを想定したアプリケーション検査



シンプルなネットワークを想定したアプリケーション検査

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 トラフィック上での特定のインスペクションを許可するよう分離されています。これにより、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し、2番目のセクションでHTTPアプリケーションインスペクションを設定できます。P2PおよびIMトラフィック用の特定のクラスマップとポリシーマップは、このドキュメントの3番目のセクションで設定できます。プライベート ゾーンからパブリック ゾーンへの接続が許可されます。パブリックゾーンからプライベート ゾーンへの接続はありません。

初期ポリシーを実装する完全な設定については、付録Cを参照してください。

HTTPアプリケーションインスペクションの拡張機能の設定

HTTP アプリケーション インスペクション（他のアプリケーション インスペクション ポリシー

も含む）では、基本的なレイヤ 4 設定よりも複雑な設定が必要です。制御したい特定のトラフィックを認識し、望ましいおよび望ましくないトラフィックに目的のアクションを適用するように、レイヤ 7 の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 インスペクションに類似している）HTTP アプリケーション インスペクションは、HTTP トラフィックにのみ適用できます。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 に対してレイヤ 4 クラスマップを明示的に定義し、次のとおりレイヤ 4 ポリシーマップ内でレイヤ 7 ポリシーを HTTP インスペクション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
```

次に示す、これらの HTTP アプリケーション インスペクション トラフィックのすべての特性は、レイヤ 7 クラスマップで定義されます。

- Header inspectionコマンドは、ヘッダーが設定された正規表現に一致する要求または応答を許可/拒否/モニタする機能を提供します。許可アクションまたはリセット アクションは、クラスマップの条件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`
  コマンドの使用状況：

```
match {request|response|req-resp} header regex <parameter-map-name>
```

サンプルの使用例

- ヘッダーが ASCII 以外の文字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。

```
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
```

Header length inspection：このコマンドは、要求または応答のヘッダー長をチェックし、設定したしきい値を超過する場合に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されます。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_HEADER_LENGTH
```

コマンドの使用状況：

```
match {request|response|req-resp} header length gt <bytes>
```

サンプルの使用例

ヘッダー長が4096バイトを超える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
```

Header count inspection：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、その数を検証し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されます。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_HEADER_COUNT
```

コマンドの使用状況：

```
match {request|response|req-resp} header count gt <number>
```

サンプルの使用例

16 以上のヘッダー フィールドがある要求をブロックするように http の 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
```

Header field inspection：このコマンドでは、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/モニタできます。許可アクションまたはリセット アクションは、クラスマップの条件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
```

コマンドの使用状況：

```
match {request|response|req-resp} header <header-name>
```
サンプルの使用例

スパイウェア/アドウェアをブロックするように http アプリケーション インスペクション ポリシーを設定します。

```
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
```
Header field length inspection：このコマンドでは、ヘッダー フィールド行の長さを制限できます。許可アクションまたはリセット アクションは、クラスマップの条件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
```
コマンドの使用状況：

```
match {request|response|req-resp} header <header-name> length gt <bytes>
```
サンプルの使用例

クッキーとユーザ エージェントのフィールド長がそれぞれ 256 と 128 を超過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。

```
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
```
Inspection of header field repetition：このコマンドでは、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。許可アクションまたはリセット アクションは、クラスマップの条件に一致する要求または応答に適用できます。有効にすると、ログ アクションが、次の syslog メッセージを発生させます。

```
APPFW-6- HTTP_REPEATED_HDR_FIELDS
```
コマンドの使用状況：

```
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、セッションの密輸を防ぐために使用される最も便利な機能の1つです（CSCCの機能を使用する場合）。

```
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
```

- Method inspection：HTTP RFC は、HTTP メソッドの制限されたセットを許可します。ただし、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、安全ではないと見なされます。標準以外のメソッドの多くは、悪意のあるアクティビティに頻繁に使用されます。これは、メソッドをさまざまなカテゴリにグループ化し、ユーザにカテゴリごとにアクションを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。許可アクションまたはリセット アクションは、クラスマップの条件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
```
コマンドの使用状況：

```
match request method <method>
```
サンプルの使用例

HTTPメソッドを3つのカテゴリにグループ化するhttp appfwポリシーを設定します。安全なメソッド、安全ではないメソッド、および webdav メソッドの 3 つです。これらを次の表に示します。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ログなしで許可されます。
- すべての安全ではないメソッドがログありで許可されます。
- すべての webdav メソッドがログありでブロックされます。

安全	安全ではない	WebDAV
GET、HEAD、OPTION	POST、PUT、CONNECT、TRACE	BCOPY、BDELETE、BMOVE

```
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 インスペクション：このコマンドでは、URI が設定済みの通常のインスペクションと一致する要求を許可/拒否/モニタできます。これにより、ユーザはカスタム URI とクエリをブロックできるようになります。許可アクションまたはリセット アクションは、クラスマップの条件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
```

コマンドの使用状況：

```
match request uri regex <parameter-map-name>
```

サンプルの使用例

URI がこれらの正規表現と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。

- .*cmd.exe
- .*sex
- .*gambling

```
parameter-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、長さが設定されたしきい値を超えたときに設定されたアクションを適用します。許可アクションまたはリセット アクションは、クラスマップの条件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
  ```

  コマンドの使用状況：

  ```
  match request uri length gt <bytes>
  ```

  サンプルの使用例

要求の URI の長さが 3076 バイトを超過するたびに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
```

Argument inspection：このコマンドでは、引数が設定済みの通常のインスペクションと一致する要求を許可/拒否/モニタできます。許可アクションまたはリセット アクションは、クラスマップの条件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
```

コマンドの使用状況：

```
match request arg regex <parameter-map-name>
```

引数がこれらの正規表現と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。

- .*codered
- .*attack

```
parameter-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、長さが設定されたしきい値を超えたときに設定されたアクションを適用します。許可アクションまたはリセットアクションは、クラスマップの条件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
  ```

  コマンドの使用状況：

  ```
  match request arg length gt <bytes>
  ```

  サンプルの使用例

要求の引数の長さが 512 バイトを超過するたびに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
```

- Body inspection：この CLI では、ユーザは要求または応答の本文に一致する正規表現一覧を

指定できます。許可アクションまたはリセット アクションは、クラスマップの条件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
```

コマンドの使用状況：

```
match {request|response|reg-resp} body regex <parameter-map-name>
```

サンプルの使用例

本体に .*[Aa][Tt][Tt][Aa][Cc][Kk] パターンが含まれている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 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
```

Body (Content) length inspection：このコマンドは、要求または応答を介して送信されるメッセージのサイズを確認します。許可アクションまたはリセット アクションは、クラスマップの条件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
```

コマンドの使用状況：

```
match {request|response|req-resp} body length lt <bytes> gt <bytes>
```

サンプルの使用例

要求または応答内に 10K バイト以上のメッセージを含む 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
```

Status line inspection：このコマンドでは、ユーザは応答のステータス行と一致する正規表現一覧を指定できます。許可アクションまたはリセット アクションは、クラスマップの条件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
```

コマンドの使用状況：

```
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みられるたびにアラームをログに記録するよう http appfw ポリシーを設定します。禁止されたページには通常403ステータスコードが含まれ、ステータス行は`HTTP/1.0 403 page forbidden\r\n`のようになります。

```
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 inspection：このコマンドは、メッセージのヘッダー コンテンツ タイプがサポートされるコンテンツ タイプの一覧にあるかどうかを検証します。ヘッダーのコンテンツ タイプがメッセージ データまたはエンティティの本文部分のコンテンツに一致することも検証します。キーワード mismatch が設定されると、コマンドは要求メッセージの受付済みフィールド値に対して応答メッセージのコンテンツタイプを検証します。許可アクションまたはリセット アクションは、クラスマップの条件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
  ```

  コマンドの使用状況：

  ```
  match {request|response|req-resp} header content-type [mismatch|unknown|violation]
  ```

  サンプルの使用例不明なコンテンツタイプを持つ要求と応答を含むhttpセッションをブロックするようにhttp appfwポリシーを構成します。

  ```
  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
  ```

Port-misuse inspection：このコマンドは、httpポート(80)がIM、P2P、トンネリング（P2P、P2P、P2Pなど）などの他のアプリケーションに悪用されるのを防ぐために使用されます。許可アクションまたはリセットアクションは、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
```

コマンドの使用状況：

```
match request port-misuse {im|p2p|tunneling|any}
```

サンプルの使用例

IMアプリケーションに誤使用される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 port_misuse_cm
   match request port-misuse im
```

```
policy-map type inspect http port_misuse_pm
   class type inspect http port_misuse_cm
      reset
```

- Strict-http inspection：このコマンドは、HTTP 要求と応答に対して厳密なプロトコル コンプライアンス チェックを有効にします。許可アクションまたはリセット アクションは、クラスマップの条件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
  コマンドの使用状況：
  match req-resp protocol-violation
  サンプルの使用例RFC 2616に違反す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。

```
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
```

- Transfer- Encoding Inspection：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、またはモニタする機能を提供します。許可アクションまたはリセット アクションは、クラスマップの条件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
  コマンドの使用状況：
  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。

```
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 Applet inspection：このコマンドは、応答に Java アプレットがあるかどうかをチェックし、アプレットが検出された時点で設定済みアクションを適用します。許可アクションまたはリセット アクションは、クラスマップの条件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
  コマンドの使用状況：
  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 Software Release 12.4(9)T では、IM アプリケーションと P2P アプリケーションに対して ZFW がサポートされました。

Cisco IOS ソフトウェアは、Cisco IOS Software Release 12.4(4)T で IM アプリケーション制御を初めてサポートしました。ZFW の最初リリースでは、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を求めても、ユーザは ZFW 設定インターフェイスに移行できませんでした。Cisco IOSソフトウェアリリース12.4(9)Tでは、Yahoo!Messenger(YM)、MSN Messenger(MSN)、およびAOL Instant Messenger(AIM)。Cisco IOSソフトウェアリリース12.4(9)Tは、P2Pファイル共有アプリケーションに対するCisco IOSファイアウォールのネイティブサポートを提供するCisco IOSソフトウェアの最初のバージョンです。

IM と P2P の両方のインスペクションは、アプリケーション トラフィックに対してレイヤ 4 およびレイヤ 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、トラフィックを許可または拒否する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 インスペクションと制御

SDM 2.2 では、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が導入されました。SDMは、Network-Based Application Recognition(NBAR)とQoSポリシーを適用して、P2Pアプリケーションアクティビティを検出してゼロのラインレートにポリシングし、すべてのP2Pトラフィックをブロックしました。これにより、Cisco IOSファイアウォールCLIでP2Pサポートを期待していたCLIユーザが、必要なNBAR/QoS設定を認識していない限り、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P2P制御が導入され、NBARを利用してP2Pアプリケーションアクティビティを検出します。このソフトウェアリリースでは、次のいくつかの 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、「port-hopping（ポートホッピング）」動作と検出を避ける他のトリックの結果、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に、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 インスペクションと 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。

- 複雑で検出が難しい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
- プロトコルの更新や変更に対応できる更新メカニズムを提供する拡張可能なインフラストラクチャ

P2Pインスペクションの設定

前述したとおり、P2P のインスペクションと制御は、レイヤ 4 ステートフル インスペクションとレイヤ 7 アプリケーション制御を提供します。レイヤ4インスペクションは、ネイティブのアプリケーションサービスポートのインスペクションが適切であれば、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 プロトコル [サービス名] に追加の署名オプションがあります。match protocol文の最後にsignatureオプションが追加されると、NBARヒューリスティックがトラフィックに適用され、特定のP2Pアプリケーションアクティビティを示すトラフィック内の暴露部分が検索されます。これには、ポートホッピング、および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のその他の変更が含まれます。このレベルのトラフィック インスペクションは、CPU 使用率の増加およびネットワーク スループットの低減を伴います。シグニチャオプションを適用しない場合、NBARベースのヒューリスティック分析は適用されず、ポートホッピングの動作を検出し、CPU使用率は同じ程度に影響を受けません。

ネイティブ サービス インスペクションは、アプリケーションが、標準以外の送信元と宛先ポートにホッピングする場合または認識されていないポート番号に対してアクションを開始するためにアプリケーションが更新される場合に、P2P アプリケーションの制御を維持できないというデメリットを抱えています。

アプリケーション	ネイティブ ポート（12.4(15)T PAM 一覧によって認識）
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）する場合は、追加の設定を行う必要があります。一部のアプリケーションでは、複数のP2Pネットワークを使用したり、ファイアウォール設定に必要な特定の動作を実装して、アプリケーションを動作させることができます。

- BitTorrentクライアントは通常、非標準ポートで実行される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。これは通常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必要があります。BitTorrentを許可する場合、追加のポートに対応する最善の方法は、HTTPをmatchプロトコルの1つとして設定し、ip port-mapコマンドを使用してTCP 6969をHTTPに追加することです。
  ```
  ip port-map http port tcp 6969
  ```
  クラスマップに適用される一致基準としてhttpとbittorrentを定義する必要があります。
- eDonkey が出現し、eDonkey と Gnutella の両方として検出される接続を開始します。
- KaZaA インスペクションは NBAR 署名の検出に完全依存しています。

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、およびテキストチャット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。サービス固有の機能は、サービスによって異なります。

P2P アプリケーション インスペクションは、HTTP アプリケーション インスペクションと類似しています。

```
!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 インスペクションは、レイヤ 4 インスペクションでサポートされるアプリケーションのサブセットに対して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には、アプリケーション固有の可変一致基準オプションがあります。

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)#
```

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プロトコルの定義または現在のP2Pプロトコルの更新は、NBARのダイナミック pdlm更新機能を使用してロードできます。これは、新しい PDLM をロードするためのコンフィギュレーション コマンドです。

```
ip nbar pdlm <file-location>
```

新しいプロトコルは、class type inspectのmatch protocolコマンドで使用できます。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 インスペクト クラスマップ タイプは、レイヤ 7 の一致基準と同様に利用可能になります。

IM アプリケーション インスペクションと制御

Cisco IOS Software Release 12.4(4)T では、IM アプリケーション インスペクションと制御がサポートされました。IM サポートは 12.4(6) T では ZFW とともには対応されなかったので、ZFW と従来型のファイアウォール機能は特定のインターフェイス上で共存できないため、ユーザは同じファイアウォール ポリシー内に IM 制御と ZFW を適用することができませんでした。

Cisco IOS Software Release 12.4(9)T では、次の IM サービスに対してステートフル インスペクション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メッセンジャー
- Yahoo! Messenger

IMインスペクションは、特定のサービスごとに特定のホストグループへのアクセスを制御するため、ほとんどのサービスとは若干異なります。通常、IM サービスは比較的永続的なディレクトリ サーバのグループに依存しています。クライアントは IM サービスにアクセスするためにこのグループに問い合わせできる必要があります。IM アプリケーションは、プロトコルまたはサービスの観点から見て、非常に制御が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率的な方法は、固定の IM サーバへのアクセスを制限することです。

IMインスペクションの設定

IMインスペクションおよび制御は、レイヤ4ステートフルインスペクションの両方を提供します

レイヤ7アプリケーション制御を実現します

レイヤ 4 インスペクションは、次の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、機能を維持するために複数のポート上にあるサーバに問い合わせすることができます。検査アクションで特定のIMサービスを許可するには、IMサービスのサーバへの許可アクセスを定義するserver-listは必要ありません。ただし、AOL Instant Messengerなどの特定のIMサービスを指定するクラスマップを設定し、関連付けられたポリシーマップでdropアクションを適用すると、IMクライアントがインターネットへの接続が許可されている別のポートを検索

する可能性があります。特定のサービスへの接続を許可したくない場合、または IM サービスの機能をテキストチャットに制限する場合は、サーバー一覧を定義し、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 サーバー一覧は、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 10.0.77.88
  server ip range 172.16.0.77 172.16.0.99
```

プロトコル定義にサーバリストを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
```

名前解決を有効にするには、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。設定したIMサーバリストが完全で正しいことを定期的に確認する必要があります。

レイヤ7 (アプリケーション) 検査は、テキストチャット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、他のサービス機能を拒否します。

IM アプリケーション インスペクションは、テキストチャット 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現在提供しています。IM をテキストチャット アクティビティに制限するには、次のとおりレイヤ 7 ポリシーを設定します。

```
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

ZFW は、Web コンテンツへのアクセスを、ルータ上に定義されるホワイトリストやブラックリストによって、またはドメイン名を URL フィルタリング サーバに転送して特定のドメインへのアクセスを検証することによって指定されたものに制限する 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までのZFW URLフィルタリングは、アプリケーションインスペクションと同様に、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 サーバの構成を説明する次の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
```

静的なホワイトリストまたはブラックリストを優先する場合、リストに一致しないトラフィックに逆のアクションを適用すると同時に、明示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一覧を定義できます。

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

URLブラックリストが除外ドメイン定義で拒否オプションを使用して定義されている場合、他のすべてのドメインが許可されます。「許可」定義が定義されている場合、IPアクセスコントロールリストの機能と同様に、許可されているすべてのドメインを明示的に指定する必要があります。

HTTPトラフィックに一致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
```

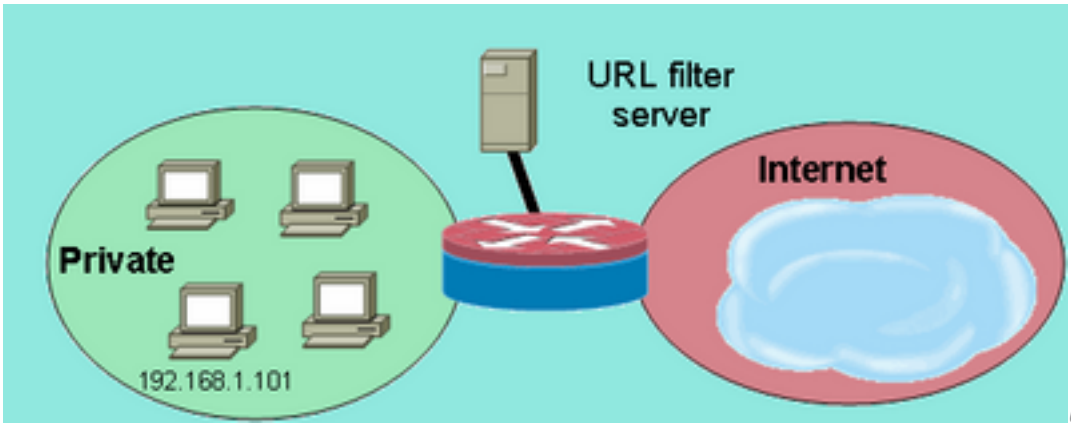
クラスマップをインスペクト アクションと urlfilter アクションに関連付ける次のポリシーマップを定義します。

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

これは、URL フィルタリング サーバと通信する最小要件を設定します。いくつかのオプションは、追加の URL フィルタリング動作を定義するために利用できます。

一部のネットワーク展開では、一部のホストまたはサブネットにURLフィルタリングを適用し、他のホストにはURLフィルタリングをバイパスします。たとえば、図 9 では、プライベート ゾーンのすべてのホストは、特定のホスト 192.168.1.101 を除き、URL フィルタ サーバに HTTP トラフィックをチェックさせる必要があります。

図 10：URL フィルタリング例のトポロジ



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、より大きなホストグループのHTTPトラフィックとだけ一致する1つのクラスマップ。
- URLフィルタリングを受信しない、より小さなホストグループ用の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、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1つだけです。

```
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、ルータの管理インターフェイス (SSH、Telnet、HTTP、HTTPS、SNMPなど) をパブリックインターネットに公開する場合に不安を感じます。また、特定の状況では、ルータへのLANアクセスの制御も必要になります。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ためのオプションを数多く提供します。これらのオプションとして、Network Foundation Protection (NFP; ネットワーク基盤の保護) 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や ZFW のセルフ ゾーンなどがあります。VTYアクセスコントロール、管理プレーン保護、SNMPアクセスコントロールなどの他の機能を確認して、特定のアプリケーションに最適なルータコントロール機能の組み合わせを判断する必要があります。

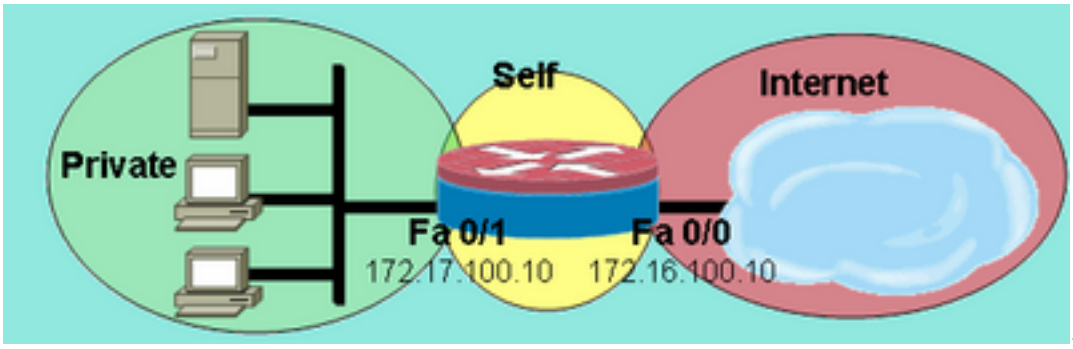
通常、NFP 機能ファミリが、ルータ自体に向けられるトラフィックの制御に最も適しています。NFP機能によるルータ保護について説明している情報は、『Cisco IOSソフトウェアのコントロールプレーンセキュリティの概要』を参照してください。

ルータ自体のIPアドレスとの間のトラフィックを制御するためにZFWを適用する場合は、ファイアウォールのデフォルトポリシーと機能が、通過トラフィックに使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。中継トラフィックは、送信元と宛先のIPアドレスがルータインターフェイスに適用されるIPアドレスのいずれとも一致しないネットワークトラフィックとして定義され、このトラフィックによってルータがICMP TTL期限切れなどのネットワーク制御メッセージやnetwork/host unreachableメッセージなどを送信することはありません。

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る任意のゾーンのトラフィックは暗黙的に許可されます。これにより、ゾーン ファイアウォール設定がルータに適用される場合に、ルータの管理インターフェイスへの接続が維持されることが保証されます。同じ deny-all ポリシーがルータへの直接接続に影響する場合は、ゾーンをルータ上で構成する前に、完全な管理ポリシー設定を適用する必要があります。これは、ポリシーが不適切に実装または正しくない順番で適用されている場合、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 メンバーとして設定されている場合、インターフェイスに接続されるホストはゾーンに含まれます。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制御されません（図10の注で説明されている状況を除く）。 代わりに、ZFWが設定されると、ルータ上のすべてのIPインターフェイスが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、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/検査するポリシーを適用する必要があります（図11を参照）。

図 11：ネットワークゾーンとルータセルフゾーン間でのポリシーの適用



ネットワークゾーンとルータセルフゾーン間でのポリシーの適用

ルータはすべてのゾーンとセルフゾーンの間にdefault-allowポリシーを提供しますが、任意のゾーンからセルフゾーンにポリシーが設定され、ルータのユーザ設定可能なインターフェイス接続ゾーンに対してselfからポリシーが設定されていない場合、ルータから発信されたすべてのトラフィックは、ルータに戻ったときにconnected-zone to self-zoneポリシーに遭遇し、ブロックされます。したがって、ルータから発信されたトラフィックは、セルフゾーンへの戻りを許可するために検査する必要があります。

> **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に対して、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、サービスが特定のインターフェイスを送信元インターフェイスとして定義し、そのコマンドにlogging source-interface [type number] 、 ip tftp source-interface [type number] 、およびip telnet source-interface [type number]が含まれるが、これらに限定されない場合、トラフィックはセルフゾーンの対象となります。

> **注**：一部のサービス(特にルータのVoice-over-IP(VoIP)サービス)は、セキュリティゾーンに

割り当てることができない一時的または設定不可能なインターフェイスを使用します。これらのサービスは、トラフィックを設定されたセキュリティゾーンに関連付けることができない場合、正しく機能しません。

セルフ ゾーン ポリシーの制限

セルフ ゾーン ポリシーは、トランジット トラフィックのゾーン ペアで利用可能なポリシーと比べると機能が制限されています。

- 従来型のステートフル インスペクションの場合と同様に、ルータが生成したトラフィックは、TCP、UDP、ICMP、および H.323 の複雑なプロトコル インスペクションに制限されます。
- アプリケーション インスペクションは、セルフ ゾーンのポリシーには利用できません。
- セッションおよびレート制限は、セルフ ゾーン ポリシーに設定できません。

セルフ ゾーン ポリシーの設定

ほとんどの状況において、次の内容はルータ管理サービスに望ましいアクセス ポリシーです。

- Telnet のクリアテキスト プロトコルは、簡単にユーザ クレデンシャルや他の機密情報を簡単に開示してしまうので、すべての Telnet 接続を拒否する。
- ゾーン内のユーザによる 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 データを暗号化します。これにより、パケット キャプチャ ツールを使用してユーザ アクティビティをスヌーピングし、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悪意あるユーザから保護します。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に固有の特定の脆弱性に対処します。
- プライベートゾーンが信頼できる場合は、プライベートゾーンからルータへのHTTP接続を許可します。そうでない場合、プライベートゾーンが悪意のあるユーザによる情報の侵害の可能性を妨げている場合、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情報を明らかにすることができます。
- すべてのゾーンからの HTTPS 接続を許可する。SSH と同様に、HTTPS 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。
- 特定のホストまたはサブネットに SNMP アクセスを制限する。SNMP を使用して、ルータ設定を修正し、設定情報を公開できます。SNMPは、さまざまなコミュニティのアクセスコントロールを使用して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要求をブロックします（プライベートゾーンアドレスはルーティング可能であると仮定します）。 必要に応じて、ネットワークのトラブルシューティングのために、1つ以上のパブリックアドレスをICMPトラフィックに公開できます。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ゾーンごとに 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。ルータのセルフゾーンとの間で送受信されるトラフィック用の各ゾーンペアは、トラフィックが反対方向から発信されない限り、反対方向の対応するポリシーに一致する必要があります。インバウンドおよびアウトバウンドのゾーンペアそれぞれに、すべてのトラフィックを記述する 1 つのポリシーマップを適用するか、ゾーンペアごとに明示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に特定のゾーンペアを設定すると、各ポリシーマップに一致するアクティビティを詳細に表示できます。

172.17.100.11にSNMP管理ステーションがあり、172.17.100.17にTFTPサーバがあるネットワークの例を示します。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ています。

```
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 転送のインスペクションを行う機能を提供しません。したがって、TFTP がファイアウォールを通過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接続を終了する場合は、IPSec ESP、IPSec AH、ISAKMP、およびNAT-T IPSec(UDP 4500)を渡すポリシーも定義する必要があります。 これは、使用するサービスに基づいて必要なサービスによって異なります。この次のポリシーは、上記のポリシーに加えて適用できます。VPNトラフィックのクラスマップがパスアクションで挿入されたポリシーマップの変更に注目してください。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 ポリシーが指示する場合を除いて、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広域アプリケーションサービス

設定例と使用法のガイダンス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および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 では、ポリシー設定を表示し、ファイアウォール アクティビティをモニタするために、新しいコマンドをサポートします。

ゾーンの説明と指定したゾーンに含まれるインターフェイスを次に示します。

```
show zone security [<zone-name>]
```

ゾーンの名前が含まれない場合は、そのコマンドがすべての設定済み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
```

ゾーンペアにアタッチされる送信元ゾーン、宛先ゾーンおよびポリシーを次に示します。

```
show zone-pair security [source <source-zone-name>] [destination <destination-zone-name>]
```

送信元または宛先が指定されていない場合は、送信元、宛先、関連付けられたポリシーを持つすべてのゾーンペアが表示されます。送信元/宛先のゾーンのみが記載されている場合は、送信元/宛先として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
```

指定したポリシーマップを次に示します。

```
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（サブタイプを含むレイヤ7ポリシーマップとともに）表示されます。

```
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現在存在するランタイム検査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 が記載されている場合は、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上にポリシーマップを適用することによって作成されるインスペクション 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、指定したポリシーマップ（またはゾーンペアの名前が指定されていない場合はすべてのターゲットのポリシーマップ）に関する 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 キーワードが urlfilter とともに指定されている場合は、（IP アドレスの）urlfilter キャッシュを表示します。

インスペクト ポリシーマップの show policy-map コマンドのサマリーは次のとおりです。

```
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のサービス拒否保護の調整

ZFW では、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 アクティビティの変更による影響を軽減して不必要なアクティビティを減らすために、DoS を保護します。ZFW は、すべてのポリシーマップのクラスマップ用に独立したカウンタを維持します。したがって、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る場合、2つの異なるDoS保護カウンタのセットが適用されます。

ZFW は、12.4(11)T 以前の Cisco IOS ソフトウェア リリースの場合、デフォルトとして DoS 攻撃を軽減します。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。

TCP SYN DoS 攻撃の詳細については、『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（完全な）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
```

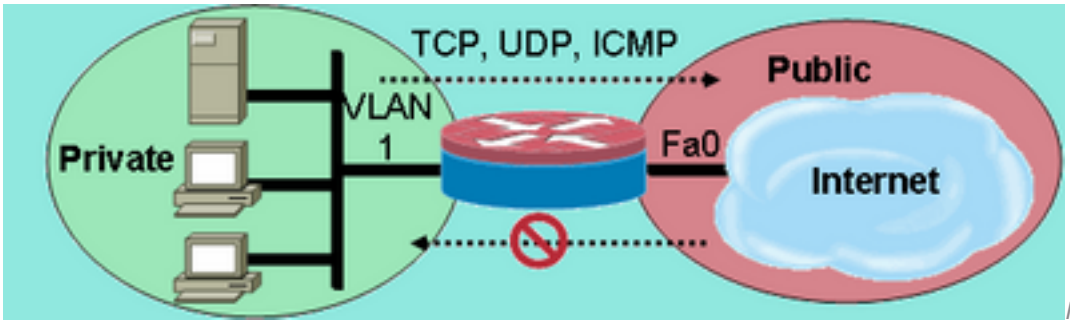
```
  service-policy type inspect private-dmz-policy
zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 zone-member internet
!
interface FastEthernet1
 ip address 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的なゾーン ファイアウォールの設定

この例では、Cisco IOSソフトウェアZFWの拡張機能をテストするための基礎となる簡単な設定を示します。この設定は、1811 ルータ上に設定される 2 つのゾーンのモデル設定です。プライベートゾーンはルータの固定スイッチポートに適用されるため、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ファストイーサネット0に適用されます（図

12を参照）。

図 12：FastEthernet 0に適用されるパブリックゾーン



FastEthernet 0に適用されるパブリックゾーン

```
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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。