PVLANとVACLによるセキュアネットワーク

内容

概要

ネットワーク セキュリティ設計を成功させるために重要な要素の 1 つは、適切な信頼モデルを特定し、それを実行することです。適切な信頼モデルでは、誰が誰に通信する必要があるか、およびどのようなトラフィックを交換する必要があるかが定義されます。その他のトラフィックはすべて拒否する必要があります。適切な信頼モデルが決まったら、セキュリティ設計者はこのモデルを実行する方法を決定します。多くのクリティカルなリソースがグローバルに入手可能になり、ネットワーク攻撃の新しい形態が発展するにつれて、ネットワーク セキュリティのインフラストラクチャはより高度になり、利用可能な製品も増えています。信頼モデルを実行するには、ファイアウォール、ルータ、LAN スイッチ、侵入検知システム、AAA サーバ、VPN などのテクノロジーおよび製品が役立ちます。当然、これらの製品およびテクノロジーは、セキュリティ実装全体の中でそれぞれが固有の役割を担います。設計者は、これらの要素をどのように展開できるかを理解する必要があります。

はじめに

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。

前提条件

この文書では、CatOS を実行するスイッチでの PVLAN の設定についてだけ説明します。Cisco

IOS および CatOS を実行するスイッチの PVLAN のさまざまな設定例は、「Catalyst Switch 上の独立したプライベート VLAN の設定」を参照してください。

すべてのスイッチとソフトウェア バージョンが PVLAN をサポートしているわけではありません。ご使用のプラットフォームとソフトウェアのバージョンでPVLANがサポートされているかどうかを確認するには、『プライベートVLAN Catalystスイッチのサポート一覧』を参照してください。

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。

背景説明

適切な信頼モデルの特定と実行は非常に基本的なタスクのように思われますが、セキュリティ実装を数年にわたってサポートしてきた経験から言えば、セキュリティ事故がセキュリティ設計の問題に起因することは少なくありません。通常こうした設計の問題は、必要なことが理解されていないか、関連するテクノロジーが正しく理解または使用されていなかったために、適切な信頼モデルが実行されていないことが直接の原因になっています。

この文書では、企業環境およびサービス プロバイダー環境で適切な信頼モデルを確実に実行するために、Catalyst スイッチで使用可能な Private VLAN（PVLAN）と VLAN Access Control List（VACL）の 2 つの機能の利用する方法を説明します。

適切な信頼モデルを実施する重要性

適切な信頼モデルを実行しない場合の直接的な影響は、悪質な活動に対するセキュリティ実装全体の耐性が低下することです。一般に Demilitarized Zone（DMZ）を実装する際は正しいポリシーが実行されないため、潜在的な侵入者が容易に活動できます。この項では、DMZ の一般的な実装方法と、不適切な設計がもたらす影響について分析します。さらに、こうした問題を軽減し、可能であれば回避する方法を説明します。

通常、DMZ サーバに要求されているのは、インターネットからの着信要求を処理し、最終的に内部または他の DMZ セグメントのバックエンド サーバ（データベース サーバなど）への接続を開始することだけです。それと同時に、DMZ サーバは互いに通信したり、外部への接続を開始したりしないことが要求されます。これにより、単純な信頼モデルで必要なトラフィックフローが明確に定義されます。しかし、この種のモデルは適切に実施されていないことがよくあります。

多くの設計者は、DMZ 同士のトラフィックを制御せず、すべてのサーバに共通のセグメントを使用して DMZ を実装する傾向があります。たとえば、すべてのサーバが共通の VLAN に配置されたりします。同じ VLAN 内ではトラフィックを制御するものがないため、サーバの 1 台が手を加えられて安全性が損なわれると、このサーバを利用して、同じセグメントに属するサーバおよびホストが攻撃される可能性があります。こうすれば、潜在的な侵入者がポート リダイレクションやアプリケーション層攻撃を容易に実行できるのは明らかです。

通常、ファイアウォールとパケット フィルタは着信接続の制御のみに使用されます。DMZ から開始される接続を制限するためには、通常は何も行われません。少し前にcgi-binスクリプトに既知の脆弱性があり、侵入者がHTTPストリームを送信するだけでX項セッションを開始できるようになりました。これは、ファイアウォールで許可される必要があるトラフィックです。侵入者は、運がよければ別の方法（通常はある種のバッファ オーバーフロー攻撃）を使用してルート プロ

ンプトを乗っ取ることもできます。ほとんどの場合、これらのタイプの問題は適切な信頼モデルを実行することによって回避できます。適切な信頼モデルでは、第 1 にサーバ同士が互いに通信しないこと、第 2 にこれらのサーバから外部への接続はいっさい開始しないことが要求されます。

信頼のない通常のセグメントからアプリケーション サービス プロバイダーのサーバ ファームまで、他の多くのシナリオにも同じことが当てはまります。

Catalyst スイッチでは、適切な信頼モデルを確実に実行するために、PVLAN と VACL を利用できます。PVLAN は、共通セグメント内でホスト間のトラフィックを制限します。一方 VACL は、特定のセグメント発または特定のセグメント宛てのあらゆるトラフィック フローをより厳格に制御します。これらの機能について、次の項で説明します。

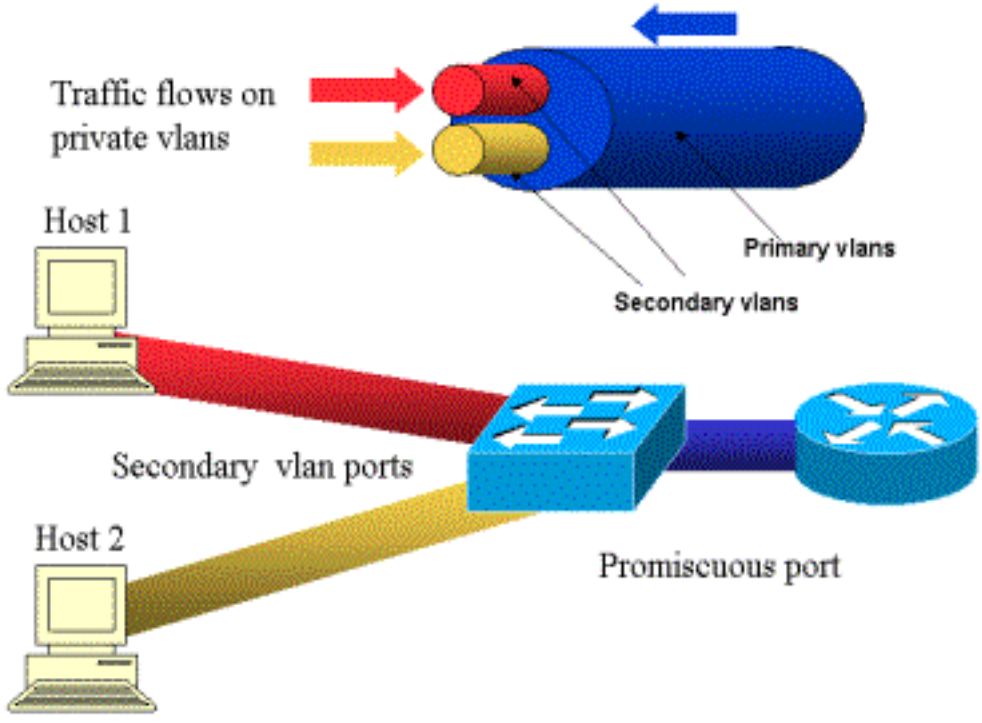
プライベート VLAN

PVLAN は、CatOS 5.4 以降が動作している Catalyst 6000 と、CatOS 6.2 以降が動作している Catalyst 4000、2980G、2980G-A、2948G、および 4912G で利用できます。

ここでは PVLAN を、レイヤ 2（L2）でトラフィックを分離し、ブロードキャスト セグメントを非ブロードキャスト マルチアクセスのようなセグメントに変えることを可能にするツールととらえます。プロミスキャス ポート（プライマリ VLAN とセカンダリ VLAN の両方の転送が可能なポート）からスイッチに到達したトラフィックは、同じプライマリ VLAN に所属するすべてのポートに伝送できます。セカンダリ VLAN（隔離 VLAN、コミュニティ VLAN、または双方向コミュニティ VLAN）にマップされたポートからスイッチに到達したトラフィックは、プロミスキャス ポートまたは同じコミュニティ VLAN に所属するポートに転送できます。同じ隔離 VLAN にマップされたポート同士は、トラフィックをいっさい交換できません。

以上の概念を図示すると、次のようになります。

図 1：プライベート VLAN



プライマリVLANは青色で表示されます。セカンダリVLANは赤と黄色で表示されます。Host 1 は、セカンダリ VLAN 赤に所属するスイッチのポートに接続されています。Host 2 は、セカンダリ VLAN 黄色に所属するスイッチのポートに接続されています。

ホストが送信しているときは、トラフィックはセカンダリ VLAN 内を伝送されます。たとえば、Host 2 が送信するときは、そのトラフィックは VLAN 黄色を通ります。これらのホストが受信しているときは、トラフィックはプライマリ VLAN である VLAN 青から到達します。

ルータとファイアウォールが接続されているポートはプロミスキャス ポートです。これは、プライマリ VLAN からのトラフィックだけでなく、マッピング内で定義されたすべてのセカンダリ VLAN からのトラフィックを転送できるためです。各ホストに接続されたポートは、プライマリ VLAN からのトラフィックと、そのポートで設定されたセカンダリ VLAN からのトラフィックのみを転送できます。

この図面は、ルータとホストを接続する異なるパイプとしてプライベートVLANを表しています。その他すべてを束ねるパイプはプライマリVLAN（青）であり、VLAN blue上のトラフィックはルータからホストに流れます。プライマリ VLAN の内部のパイプがセカンダリ VLAN で、これらのパイプを通るトラフィックはホストからルータに流れます。

図に示されているように、プライマリ VLAN は 1 つ以上のセカンダリ VLAN を束ねることができます。

前述したように、PVLAN は、単に共通セグメント内部でホストを確実に分離することにより、適切な信頼モデルを実行します。プライベート VLAN について詳しくわかったところで、最初の DMZ シナリオでこれをどのように実装できるかを説明します。サーバは互いに通信しないことが要求されますが、接続されているファイアウォールまたはルータとは通信する必要があります。この場合、サーバは隔離ポートに接続し、なおかつルータとファイアウォールはプロミスキャス ポートに接続する必要があります。これにより、サーバの 1 台が手を加えられて安全性が損なわれた場合でも、侵入者はこのサーバを同じセグメント内の他のサーバに攻撃を仕掛ける拠点として利用できなくなります。スイッチは、パフォーマンスを低下させることなくワイヤ スピードでパケットを廃棄します。

もう 1 つの重要な注意事項は、この種の制御は L2 デバイスでしか実装できないということです。すべてのサーバが同じサブネットに属しているからです。サーバは直接通信を試みるため、ファイヤウォールやルータにできることはありません。その他に、サーバごとにファイアウォール ポートを 1 つずつ確保する方法もありますが、これはコストがかかり、実装が難しく、拡張性に欠ける傾向があります。

後の項で、この機能を使用できる他の典型的なシナリオについて詳細に説明します。

VLAN アクセス・コントロール・リスト

VACL は、CatOS 5.3 以降が動作する Catalyst 6000 シリーズで利用できます。

VACL は Catalyst 6500 の L2 で設定できます。ルータは必要ありません（必要なのは Policy Feature Card（PFC）のみです）。 これらはワイヤスピードで適用されるため、Catalyst 6500でのVACLの設定にパフォーマンスの低下はありません。VACLのルックアップはハードウェアで実行されるため、アクセスリストのサイズに関係なく、転送レートは変更されません。

VACL は、複数のプライマリまたはセカンダリ VLAN に別々にマップできます。セカンダリ VLAN に VACL を設定すると、ルータまたはファイアウォールによって生成されたトラフィックに影響を与えることなく、ホストによって発信されたトラフィックをフィルタリングできます。

VACL とプライベート VLAN を組み合せることにより、トラフィック自体の方向に基づいてトラフィックをフィルタリングすることが可能になります。たとえば、2 台のルータが数台のホスト（たとえばサーバ）と同じセグメントに接続されている場合、セカンダリ VLAN に VACL を設定することにより、ホストによって生成されたトラフィックのみがフィルタリングされ、ルータ間で交換されるトラフィックは影響を受けないようにすることができます。

VACL を配備することにより、適切な信頼モデルを容易に実行できます。ここで、DMZ のケースを分析します。DMZ のサーバは着信接続のみを処理し、外部への接続を開始しないことが要求されます。これらのサーバから送出されるトラフィックを制御するために、これらのサーバのセカンダリ VLAN に VACL を適用することができます。VACL を使用するときは、ルータおよびスイッチの CPU に影響を与えないようにハードウェアでトラフィックが廃棄される点に注意してください。これらのサーバの 1 台が Distributed Denial of Service（DDoS）攻撃の送信元として使用されても、スイッチはすべての不正なトラフィックをワイヤ スピードで廃棄します。これによるパフォーマンスの低下はありません。同様のフィルタは、サーバが接続されたルータまたはファイアウォールにも適用できます。ただし、通常これはパフォーマンスに重大な影響を与えます。

MACベースのACLはIPトラフィックでは適切に動作しないため、PVLANの監視と追跡にはVACLを使用することを推奨します。

VACL およびPVLAN の既知の制限

VACL によるフィルタリングを設定するときは、PFC でのフラグメント処理に注意する必要があります。また、設定はハードウェアの仕様に従ってチューニングされる点にも注意が必要です。

Catalyst 6500 の Supervisor 1 の PFC のハードウェア設計を考えると、icmp フラグメントを明示的に拒否することをお勧めします。これは、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）のフラグメントとエコー応答がこのハードウェアによって同じものと見なされ、またこのハードウェアはデフォルトでフラグメントを明示的に許可するようにプログラムされているためです。このため、エコー応答パケットがサーバから発信されないようにする場合は、deny icmp any any fragment 行を使用して、明示的に設定する必要があります。この文書の設定ではこの点が考慮されています。

PVLAN にはよく知られたセキュリティ上の限界があります。それは、ルータがトラフィックを、そのトラフィックの送信元と同じサブネットに戻すというものです。ルータは、PVLAN の目的に反して、隔離ポートを横断してトラフィックをルーティングする可能性があります。この限界は、PVLAN が、レイヤ 3（L3）ではなく L2 で分離を提供するツールであるという事情によるものです。

Unicast Reverse Path Forwarding(uRPF)はPVLANホストポートでは正常に動作しないため、uRPFをPVLANと組み合わせて使用することはできません。

この問題は、プライマリ VLAN に VACL を設定することで解決します。ケース スタディでは、同じサブネットから発信されて同じサブネットに戻されたトラフィックを廃棄するために、プライマリ VLAN 上で必要な VACL を設定しています。

一部のラインカードでは、PVLAN マッピング/マップ/トランキング ポートを設定するために、複数の PVLAN マッピングが異なるポート Application-Specific Integrated Circuit（ASIC; 特定用途集積回路）に所属する必要があります。これらの制限は、新しいポートASIC Coil3では削除されています。詳細については、ソフトウェア設定に関する最新のCatalystスイッチのマニュアルを参照してください。

ケーススタディの例

次の項では、PVLAN と VACL によるセキュリティの配備について詳しく説明するために、ほとんどの実装を代表すると思われる 3 つの事例を取り上げています。

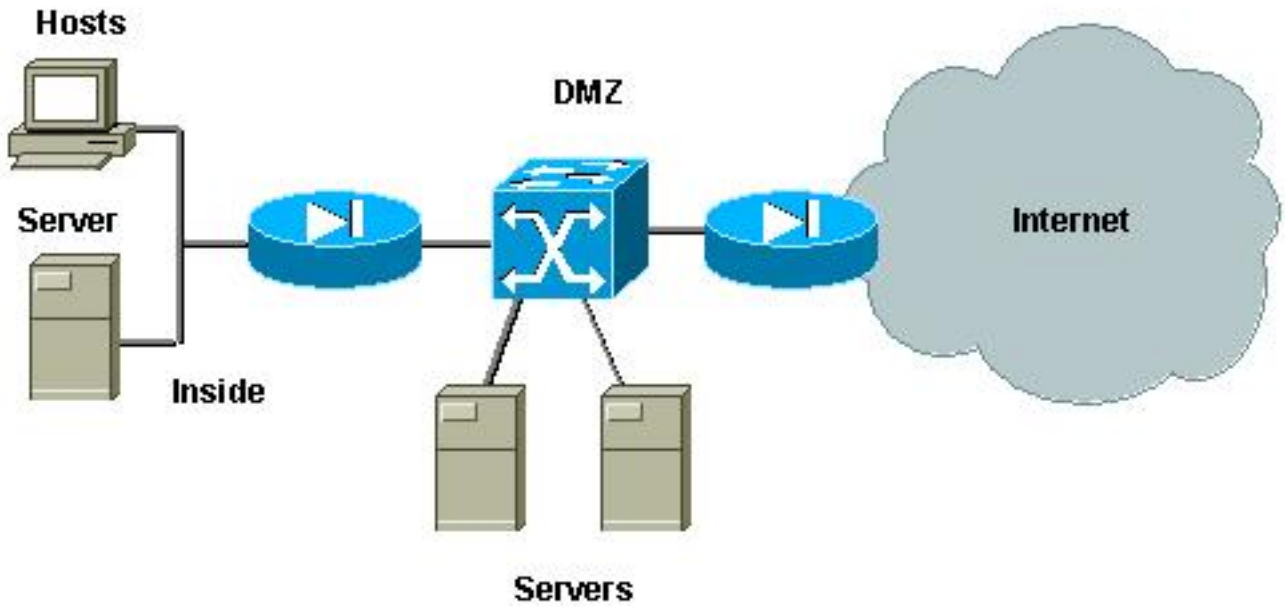
取り上げるのは次の 3 つのシナリオです。

- パススルーDMZ
- 外部DMZ
- ファイアウォールと並列に配置されるVPN コンセントレータ

パススルーDMZ

これは最も一般的に展開されるシナリオの 1 つです。この例では、DMZ は次の図のように 2 台のファイアウォール ルータ間のトランジット エリアとして実装されます。

図 2：パススルーDMZ



この例では、DMZ サーバは内部ユーザからも外部ユーザからもアクセス可能である必要がありますが、サーバ同士が互いに通信する必要はありません。場合によっては、DMZ サーバは内部ホストに対してなんらかの接続を開始する必要があります。また、内部クライアントはインターネットに制約なしにアクセスできる必要があります。DMZ に Web サーバがある場合がその好例です。DMZ の Web サーバは内部ネットワークに位置するデータベース サーバと通信する必要があり、内部クライアントからインターネットへのアクセスを可能にします。

外部ファイアウォールは、DMZ 内のサーバへの着信接続は許可し、発信トラフィック（特に DMZ 内で発信されたトラフィック）には通常はフィルタや制約を適用しないように設定されています。この文書で前述したように、これは 2 つの理由で潜在的に攻撃者の活動を助長することになります。1つ目は、DMZホストの1つに侵入するとすぐに、他のすべてのDMZホストが公開されます。2つ目の方法は、攻撃者が簡単に発信接続を不正利用する可能性があることです。

DMZサーバは相互に通信する必要がないため、L2で隔離することを推奨します。サーバポートは

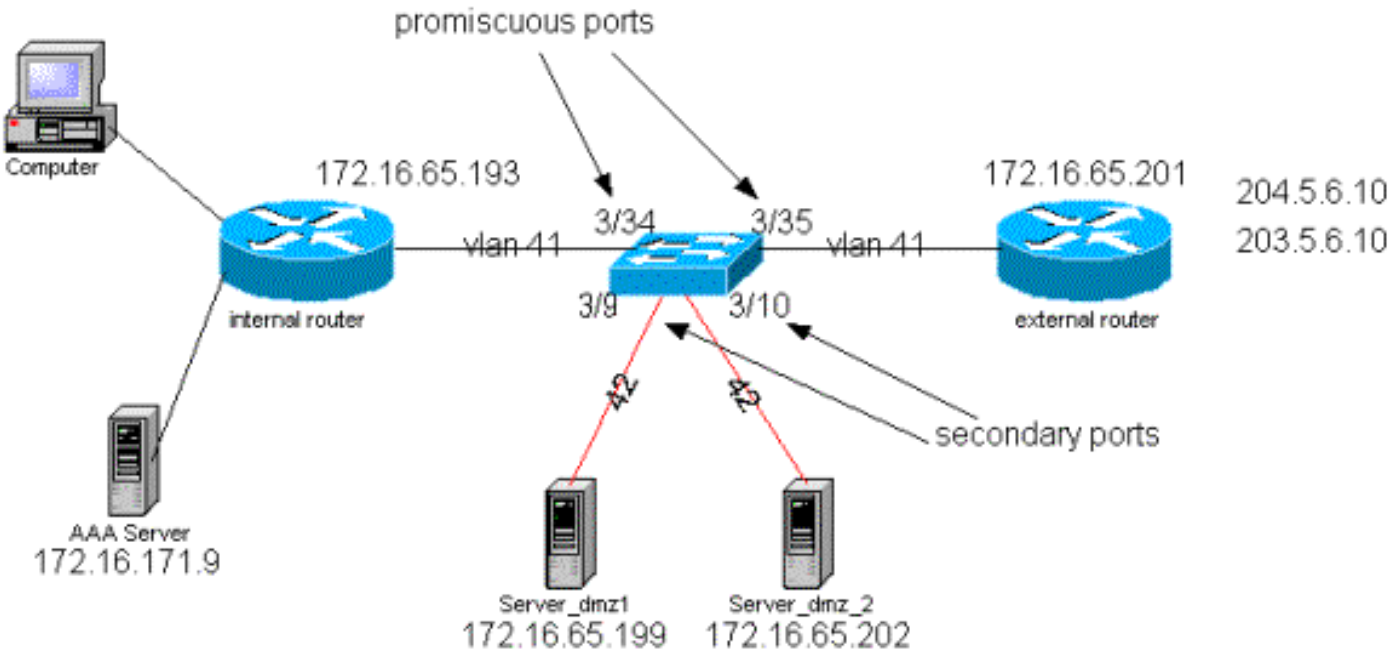
PVLAN隔離ポートとして定義し、2つのファイアウォールに接続するポートは混合ポートとして定義します。ファイアウォールにプライマリ VLAN を定義し、DMZ サーバにセカンダリ VLAN を定義することにより、これが実現されます。

VACL は、DMZ 内で発信されるトラフィックを制御するために使用されます。これにより、攻撃者が不正な発信接続を開始できなくなります。DMZ サーバはクライアント セッションに応答するトラフィックを返すだけでなく、Domain Name System (DNS; ドメイン ネーム システム) や Maximum Transmission Unit (MTU; 最大伝送ユニット) パス ディスカバリなどのサービスを提供する必要もある点に注意してください。したがって、ACL は DMZ サーバが必要とするすべてのサービスを許可する必要があります。

パススルー DMZ のテスト

このテストベッドでは、2台のルータをベッドサーバとして設定したDMZセグメントserver_dmz1とserver_dmz2を実装しました。これらのサーバは外部クライアントと内部クライアントからアクセスされ、すべてのHTTP接続は内部RADIUSサーバ(CiscoSecure ACS for UNIX)を)を)で認証します。 内部ルータも外部ルータもパケット フィルタ ファイアウォールとして設定されています。次の図は、このテストベッドと、使用されるアドレッシング方式を示しています。

図 3 : パススルー DMZ のテストベッド



次のリストは、PVLAN の基本的な設定手順を示しています。Catalyst 6500 は DMZ 内で L2 スイッチとして使用されます。

- Server_dmz_1 をポート 3/9 に接続する。
- Server_dmz_2 をポート 3/10 に接続する。
- 内部ルータをポート 3/34 に接続する。
- 外部ルータをポート 3/35 に接続する。

ここでは次の VLAN を使用します。

- 41 (プライマリ VLAN)
- 42 (隔離 VLAN)

プライベート VLAN の設定

次の設定は、関連するポートに PVLAN を設定します。

```
ecomm-6500-2 (enable) set vlan 41 pvlan primary
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 41 configuration successful

ecomm-6500-2 (enable) sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
41      -         -
ecomm-6500-2 (enable) set vlan 42 pvlan isolated
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 42 configuration successful
ecomm-6500-2 (enable) set pvlan 41 42 3/9-10
Successfully set the following ports to Private Vlan 41,42:
3/9-10

ecomm-6500-2 (enable) set pvlan mapping 41 42 3/35
Successfully set mapping between 41 and 42 on 3/35
ecomm-6500-2 (enable) set pvlan mapping 41 42 3/34
Successfully set mapping between 41 and 42 on 3/34

Port  Name                 Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/9  server_dmz1       connected  41,42      a-half  a-10 10/100BaseTX
 3/10 server_dmz2       connected  41,42      a-half  a-10 10/100BaseTX

 3/34 to_6500_1         connected   41        auto  auto 10/100BaseTX
 3/35 external_router_dm connected  41        a-half  a-10 10/100BaseTX
```

プライマリ VLAN での VACL の設定

この項は、DMZ のセキュリティを向上させるために非常に重要です。「VACL および PVLAN の既知の制限事項」の項で説明されているように、サーバが 2 つの異なるセカンダリ VLAN や同一の孤立 VLAN に属している場合でも、攻撃者がこれらを互いに通信させるために使用できる方法はあります。サーバ同士が直接通信しようとしても、PVLAN があるために L2 では通信することはできません。サーバが手を加えられて安全性が損なわれ、侵入者によって同じサブネットに対するトラフィックがルータに送信されるように設定された場合、これはトラフィックを元の同じサブネット上にルーティングすることになり、PVLAN の目的が無効化されます。

したがって、プライマリ VLAN (ルータからトラフィックを伝送する VLAN) で次のポリシーに基づく VACL を設定する必要があります。

- 送信元 IP がルータの IP であるトラフィックは許可する。
- 送信元と宛先の両方の IP が DMZ サブネットであるトラフィックは拒否する。
- 残りのトラフィックはすべて許可する。

```
ecomm-6500-2 (enable) sh sec acl info protect_pvlan
set security acl ip protect_pvlan
---------------------------------------------------
1. permit ip host 172.16.65.193 any
2. permit ip host 172.16.65.201 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any
```

```
ecomm-6500-2 (enable) sh sec acl
ACL                              Type VLANS
-------------------------------  ---- -----
protect_pvlan                    IP   41
```

このACLは、サーバによって生成されるトラフィックには影響しません。ルータがサーバからのトラフィックを同じVLANにルーティングすることを防ぐだけです。最初の 2 つの文では、ルータが icmp redirect や icmp unreachable などのメッセージをサーバに送信することを許可します。

セカンダリ VLAN での VACL の設定

次のコンフィギュレーション ログは、サーバが生成したトラフィックをフィルタリングするための VACL の設定方法を示しています。この VACL を設定する目的は次のとおりです。

- サーバからの ping を許可する（echo を許可する）。
- サーバから発信されるエコー応答を禁止する。
- 外部から開始された HTTP 接続を許可する。
- RADIUS 認証（UDP ポート 1645）およびアカウンティング（UDP ポート 1646）トラフィックを許可する。
- DNS トラフィック（UDP ポート 53）を許可する。

上記以外のトラフィックはすべて禁止する必要があります。

フラグメンテーションについては、サーバ セグメントでは次のように想定します。

- サーバは断片化したトラフィックを生成しない。
- サーバは断片化したトラフィックを受信する可能性がある。

Catalyst 6500 の Supervisor 1 の PFC のハードウェア設計を考えると、icmp フラグメントを明示的に拒否することをお勧めします。これは、ICMP のフラグメントとエコー応答がこのハードウェアによって同じものと見なされ、またこのハードウェアはデフォルトでフラグメントを明示的に許可するようにプログラムされているためです。このため、エコー応答パケットがサーバから発信されないようにする場合は、deny icmp any any fragment 行を使用して、明示的に設定する必要があります。

```
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out deny icmp any any fragment
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit icmp host 172.16.65.199 any echo
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit icmp host 172.16.65.202 any echo
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit tcp host 172.16.65.199 eq 80 any
established
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit tcp host 172.16.65.202 eq 80 any
established
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199
eq 1645 host 172.16.171.9 eq 1645
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202
eq 1645 host 172.16.171.9 eq 1645
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199
eq 1646 host 172.16.171.9 eq 1646
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202
eq 1646 host 172.16.171.9 eq 1646
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199 any eq 53
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202 any eq 53

ecomm-6500-2 (enable) Commit sec acl all

ecomm-6500-2 (enable) Set sec acl map dmz_servers_out 42
```

```
ecomm-6500-2 (enable) sh sec acl
ACL                              Type VLANS
-------------------------------  ---- -----
protect_pvlan                    IP   41
dmz_servers_out                  IP   42

ecomm-6500-2 (enable) sh sec acl info dmz_servers_out
set security acl ip dmz_servers_out
------------------------------------------------
1. deny icmp any any fragment
2. permit icmp host 172.16.65.199 any echo
3. permit icmp host 172.16.65.202 any echo
4. permit tcp host 172.16.65.199 eq 80 any established
5. permit tcp host 172.16.65.202 eq 80 any established
6. permit udp host 172.16.65.199 eq 1645 host 172.16.171.9 eq 1645
7. permit udp host 172.16.65.202 eq 1645 host 172.16.171.9 eq 1645
8. permit udp host 172.16.65.199 eq 1646 host 172.16.171.9 eq 1646
9. permit udp host 172.16.65.202 eq 1646 host 172.16.171.9 eq 1646
10. permit udp host 172.16.65.199 any eq 53
11. permit udp host 172.16.65.202 any eq 53
```

設定のテスト

次の出力は、PVLAN は設定されているものの、VACL はまだ適用されていないときにキャプチャされたものです。このテストでは、外部ルータからユーザがサーバだけでなく内部ルータに ping できることを示しています。

```
external_router#ping 172.16.65.193
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds:
!!!!

external_router#ping 172.16.65.202
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.202, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
external_router#ping 172.16.65.199
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.199, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

次の例は、サーバから外部ネットワーク、デフォルト ゲートウェイへの ping は可能ではあるが、同じセカンダリ VLAN に属しているサーバには ping できないことを示しています。

```
server_dmz1#ping 203.5.6.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 203.5.6.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

server_dmz1#ping 172.16.65.202
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.65.202, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

VACL のマッピング後は、外部ルータからの ping は、実行できなくなります。

```
external_router#ping 172.16.65.199
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.199, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

次の例は、サーバが内部ネットワークから HTTP GET 要求を受信することを示しています。

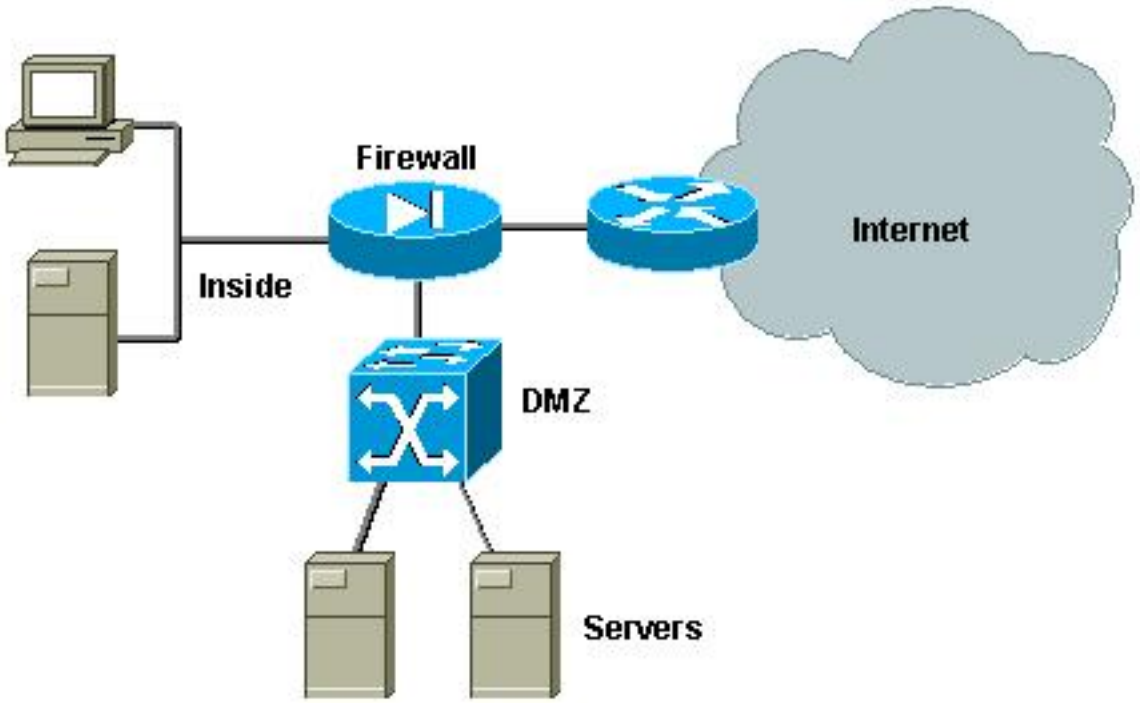
```
server_dmz1#debug ip http url
HTTP URL debugging is on
server_dmz1#debug ip hhtp tran
HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
*Mar  7 09:24:03.092 PST: HTTP: parsed uri '/'
*Mar  7 09:24:03.092 PST: HTTP: client version 1.0
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Connection
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:03.092 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:03.092 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Host
*Mar  7 09:24:03.092 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept
*Mar  7 09:24:03.092 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:03.092 PST: HTTP: parsed line  gzip
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:03.096 PST: HTTP: parsed line  en
*Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:03.096 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:03.096 PST: HTTP: authentication required, no authentication information was
provided
*Mar  7 09:24:03.096 PST: HTTP: authorization rejected
*Mar  7 09:24:22.528 PST: HTTP: parsed uri '/'
*Mar  7 09:24:22.532 PST: HTTP: client version 1.0
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Connection
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Keep-Alive
*Mar  7 09:24:22.532 PST: HTTP: parsed extension User-Agent
*Mar  7 09:24:22.532 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Host
*Mar  7 09:24:22.532 PST: HTTP: parsed line  172.16.65.199
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept
*Mar  7 09:24:22.532 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding
*Mar  7 09:24:22.532 PST: HTTP: parsed line  gzip
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Language
*Mar  7 09:24:22.532 PST: HTTP: parsed line  en
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset
*Mar  7 09:24:22.532 PST: HTTP: parsed line  iso-8859-1,*,utf-8
*Mar  7 09:24:22.532 PST: HTTP: parsed extension Authorization
*Mar  7 09:24:22.532 PST: HTTP: parsed authorization type Basic
*Mar  7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15  privless '/'
*Mar  7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =
aaa
```

```
*Mar  7 09:24:22.904 PST: HTTP: received GET ''
```

外部DMZ

外部 DMZ のシナリオは、おそらく最も一般的な実装です。外部 DMZ は、下の図のようにファイアウォールのインターフェイスを 1 つ以上使用して実装します。

図 4：外部DMZ



DMZ の要件は、通常は実装設計にかかわらず常に同じです。前のケースと同様に、DMZ サーバは、内部ネットワークからも外部クライアントからもアクセスできる必要があります。DMZ サーバは、最終的にいくつかの内部リソースにアクセスする必要があります。また、DMZ サーバ同士は通信しないことが要求されます。同時に、DMZからインターネットへのトラフィックは開始されません。これらのDMZサーバは、着信接続に対応するトラフィックでのみ応答する必要があります。

前のケース スタディと同様に、設定の最初のステップは、PVLAN によって L2 で分離し、DMZ サーバ同士が通信できないようにするとともに、内部ホストおよび外部ホストは DMZ サーバに接続できるようにすることです。これを実装するには、セカンダリ VLAN 内のサーバが隔離ポートを使用するように設定します。ファイアウォールは、プライマリ VLAN でプロミスキャス ポートを使用するように定義する必要があります。ファイアウォールは、このプライマリ VLAN 内で唯一のデバイスになります。

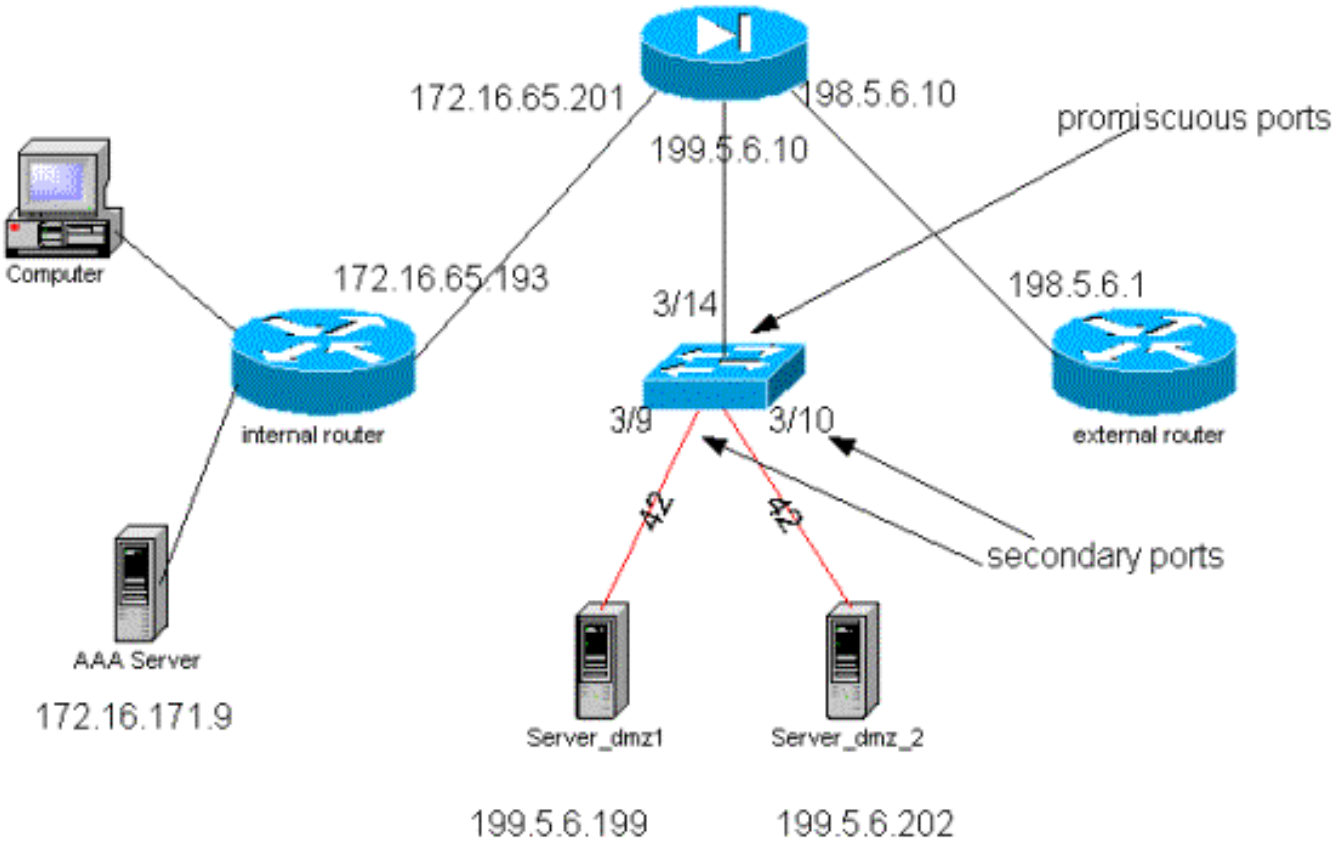
次のステップでは、DMZ 内で発信されるトラフィックを制御するように ACL を定義します。この ACL を定義するときは、必ず必要なトラフィックのみが許可されるようにします。

外部 DMZ のテスト

下の図は、このケース スタディのためのテストベッドを示しています。ここでは、DMZ 用の 3 つめのインターフェイスが装備された PIX ファイアウォールを使用しました。同じ一群のルータは Web サーバとしても使用されます。すべての HTTP セッションは同じ RADIUS サーバで認証

されます。

図 5：外部 DMZ のテストベッド



PVLAN および VACL の設定の詳細については前のケース スタディで説明したため、このシナリオでは関係のある部分のみをコンフィギュレーション ファイルから抜粋します。

PIX の設定

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
ip address outside 198.5.6.10 255.255.255.0
ip address inside 172.16.65.201 255.255.255.240
ip address dmz 199.5.6.10 255.255.255.0
global (outside) 1 198.5.6.11
global (dmz) 1 199.5.6.11
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (dmz,outside) 199.5.6.199 199.5.6.199 netmask 255.255.255.255 0 0
static (dmz,outside) 199.5.6.202 199.5.6.202 netmask 255.255.255.255 0 0
static (inside,dmz) 172.16.171.9 172.16.171.9 netmask 255.255.255.255 0 0
static (inside,dmz) 171.68.10.70 171.68.10.70 netmask 255.255.255.255 0 0
static (inside,dmz) 171.69.0.0 171.69.0.0 netmask 255.255.0.0 0 0
conduit permit tcp host 199.5.6.199 eq www any
conduit permit tcp host 199.5.6.202 eq www any
conduit permit udp any eq domain any
conduit permit icmp any any echo-reply
conduit permit icmp any any unreachable
conduit permit udp host 172.16.171.9 eq 1645 host 199.5.6.199
conduit permit udp host 172.16.171.9 eq 1646 host 199.5.6.199
conduit permit udp host 172.16.171.9 eq 1646 host 199.5.6.202
conduit permit udp host 172.16.171.9 eq 1645 host 199.5.6.202
conduit permit icmp any host 199.5.6.199 echo
```

```
conduit permit icmp any host 199.5.6.202 echo
route outside 0.0.0.0 0.0.0.0 198.5.6.1 1
route inside 171.69.0.0 255.255.0.0 172.16.65.193 1
route inside 171.68.0.0 255.255.0.0 172.16.65.193 1
route inside 172.16.0.0 255.255.0.0 172.16.65.193 1
```

RADIUSの設定

NAS の設定

```
aaa new-model
aaa authentication login default radius local
aaa authentication login consoleauth none
aaa authorization exec default radius local
aaa authorization exec consoleautho none
aaa accounting exec default start-stop radius
aaa accounting exec consoleacct none
radius-server host 172.16.171.9 auth-port 1645 acct-port 1646
radius-server key cisco123
!
line con 0
 exec-timeout 0 0
 password ww
 authorization exec consoleautho
 accounting exec consoleacct
 login authentication consoleauth
 transport input none
line aux 0
line vty 0 4
 password ww
!
end
```

RADIUS サーバの CSUX

```
User Profile Information
user = martin{
profile_id = 151
profile_cycle = 5
radius=Cisco {
check_items= {
2=cisco
}
reply_attributes= {
6=6
}
}

}

User Profile Information
user = NAS.172.16.65.199{
profile_id = 83
profile_cycle = 2
NASName="172.16.65.199"
SharedSecret="cisco123"
RadiusVendor="Cisco"
Dictionary="DICTIONARY.Cisco"

}
```

Catalyst Configuration

この設定では、PIX がトラフィックを受信したのと同じインターフェイスからトラフィックをリダイレクトすることがないため、プライマリ VLAN で VACL を設定する必要がない点に注意してください。「プライマリ VLAN での VACL の設定」の項で説明されているような VACL は、冗長になります。

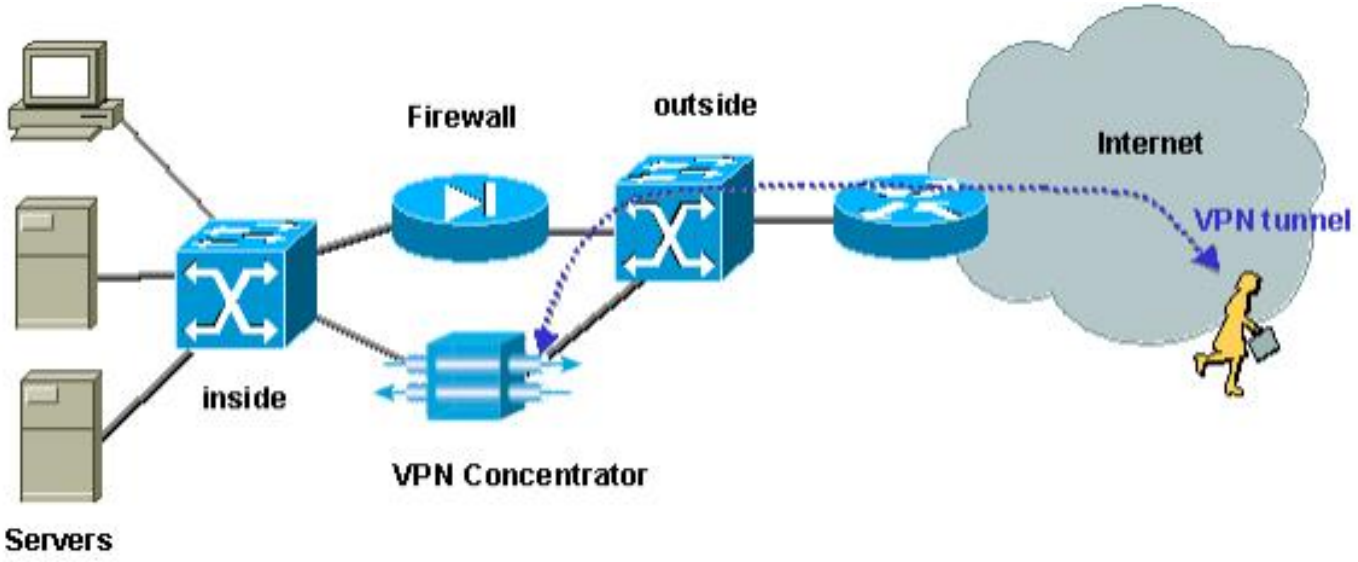
```
set security acl ip dmz_servers_out
-----------------------------------------------
1. deny icmp any any fragment
2. permit icmp host 199.5.6.199 any echo
3. permit icmp host 199.5.6.202 any echo
4. permit tcp host 199.5.6.199 eq 80 any established
5. permit tcp host 199.5.6.202 eq 80 any established
6. permit udp host 199.5.6.199 eq 1645 host 172.16.171.9 eq 1645
7. permit udp host 199.5.6.202 eq 1645 host 172.16.171.9 eq 1645
8. permit udp host 199.5.6.199 eq 1646 host 172.16.171.9 eq 1646
9. permit udp host 199.5.6.202 eq 1646 host 172.16.171.9 eq 1646
10. permit udp host 199.5.6.199 any eq 53
11. permit udp host 199.5.6.202 any eq 53
ecomm-6500-2 (enable) sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
41      42        isolated         3/9-10

ecomm-6500-2 (enable) sh pvlan mapping
Port Primary Secondary
---- ------- ---------
 3/14 41      42
 3/34 41      42
 3/35 41      42
ecomm-6500-2 (enable) sh port
Port  Name                 Status     Vlan       Duplex Speed Type
----- -------------------- ---------- ---------- ------ ----- ------------
 3/9  server_dmz1          connected  41,42      a-half  a-10 10/100BaseTX
 3/10 server_dmz2          connected  41,42      a-half  a-10 10/100BaseTX
 3/14 to_pix_port_2        connected  41           full   100 10/100BaseTX
 3/35 external_router_dm notconnect 41           auto  auto 10/100BaseTX
```

ファイアウォールと並列に配置されるVPN コンセントレータ

アクセス Virtual Private Network (VPN; バーチャル プライベート ネットワーク) を実装する場合、下の図のようなパラレル設計のアプローチがよく使用されていることは間違いありません。この設計アプローチが一般的に望まれている理由は、既存のインフラストラクチャにほとんど影響せず簡単に実装できるため、また、柔軟なデバイスなので比較的容易に拡張できるためです。

パラレル アプローチでは、VPN コンセントレータは内部と外部の両方のセグメントに接続されます。すべての VPN セッションは、ファイアウォールを通過せずにコンセントレータで終了します。VPN クライアントは、通常は内部ネットワークへのアクセスを制限されないことが必要ですが、ある内部サーバのセット (サーバ ファーム) へのアクセスは制限されることがあります。望ましい機能の 1 つは、VPN トラフィックが通常のインターネット トラフィックから分離され、そのために、たとえば VPN クライアントが企業のファイアウォール経由でインターネットにアクセスできないことです。

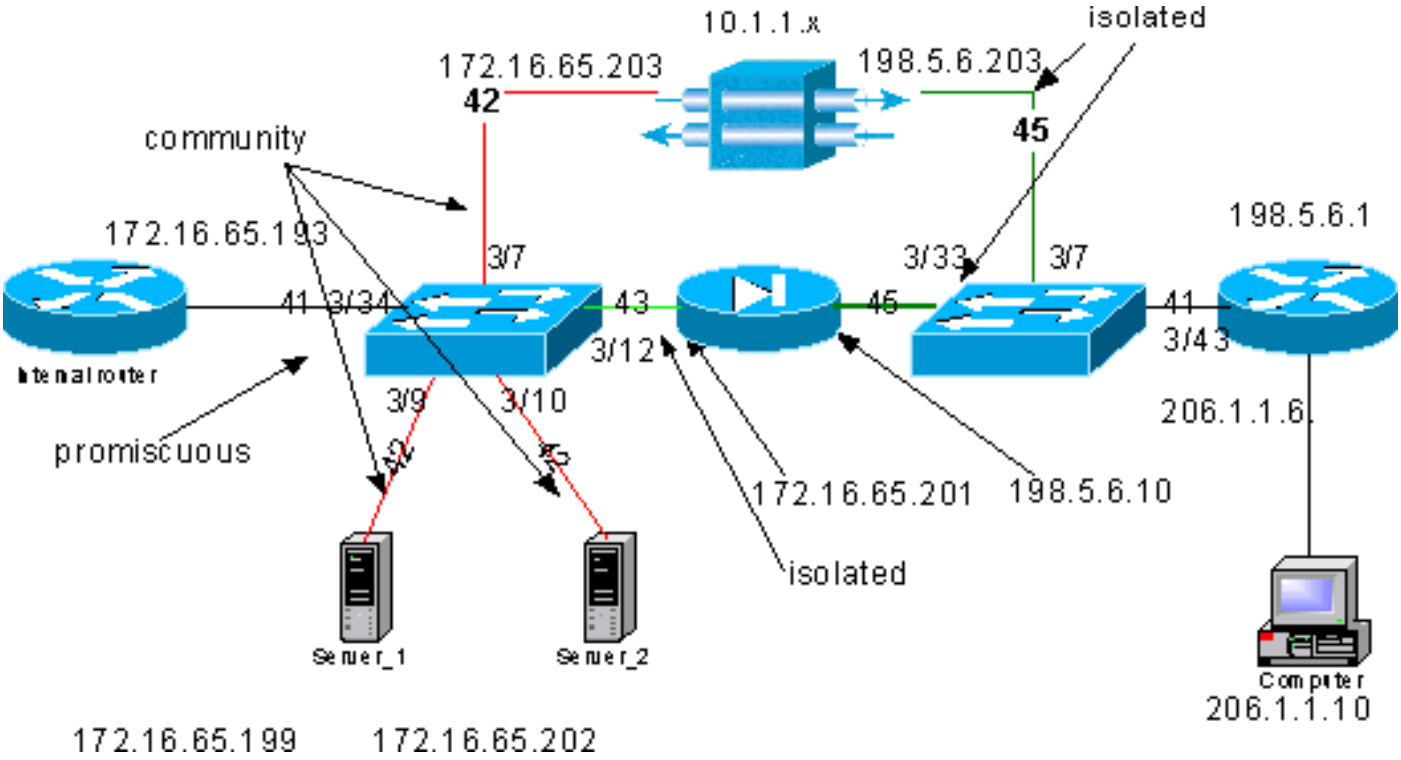
図 6 : ファイアウォールと並列に配置されるVPN コンセントレータ



ファイアウォールと並行する VPN コンセントレータのテスト

この例では、VPN 5000 コンセントレータを PIX ファイアウォールと並行して取り付けて使用しました。Web サーバとして設定された 2 台のルータは、内部サーバ ファームとして内部セグメントに取り付けられています。VPN クライアントは、サーバ ファームへのアクセスのみを許可されます。インターネット トラフィックは VPN トラフィックから分離されます (IPSec) 。 次の図は、このテストベッドを示しています。

図 7 : ファイアウォールに対するパラレルの VPN コンセントレータのテストベッド



このシナリオでは、興味深い主要な エリアが 2 つあります。

- 内部 L2 スイッチ
- 外部 L2 スイッチ

内部 L2 スイッチのトラフィック フローは、次の文に基づいて定義されます。

- VPN クライアントは、事前定義された内部サーバのセット（サーバ ファーム）に完全にアクセスできる。
- 内部クライアントもサーバ ファームへのアクセスを許可される。
- 内部クライアントはインターネットへのアクセスを制限されない。
- VPN コンセントレータからのトラフィックは PIX ファイアウォールから分離される必要がある。

外部 L2 スイッチのトラフィック フローは次のように定義さます。

- ルータからのトラフィックは VPN コンセントレータまたは PIX に到達できる必要がある。
- PIX からのトラフィックは VPN からのトラフィックから分離される必要がある。

また、内部ネットワークからのトラフィックが VPN ホストに到達するのを管理者が禁止したい場合があります。これを実現するには、プライマリ VLAN で設定される VACL を利用します（VACL は内部ルータから送出されるトラフィックのみをフィルタリングし、他のトラフィックには影響を与えません）。

PVLAN の設定

この設計の主な目的は、PIX からのトラフィックをサーバおよび VPN コンセントレータからのトラフィックと分離することなので、ここではサーバおよび VPN コンセントレータが設定される PVLAN とは異なる PVLAN で PIX を設定します。

内部ネットワークからのトラフィックは、VPN コンセントレータおよび PIX だけでなく、サーバ ファームにもアクセスできる必要があります。したがって、内部ネットワークに接続するポートはプロミスキャス ポートになります。

サーバと VPN コンセントレータは互いに通信できる必要があるため、同じセカンダリ VLAN に所属します。

外部L2スイッチについては、インターネットへのアクセスを提供するルータ(通常はインターネットサービスプロバイダー(ISP)に属する)は、混合ポートに接続され、VPNコンセントレータとPIXは同じプライベートおよび隔離VLANに属します（トラフィックを交換できません）。 これにより、サービス プロバイダーからのトラフィックは VPN コンセントレータへのパスまたは PIX へのパスのどちらかに流れます。PIX と VPN コンセントレータが分離されるため、セキュリティ保護が向上します。

内部 L2 スイッチの PVLAN の設定

```
sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- -----------
41      42        community        3/7,3/9-10
41      43        isolated         3/12

ecomm-6500-2 (enable) sh pvlan map
Port Primary Secondary
---- ------- ---------
 3/34 41      42-43

ecomm-6500-2 (enable) sh port 3/7
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
```

```
 3/7  to_vpn_conc        connected  41,42      a-half  a-10 10/100BaseTX

ecomm-6500-2 (enable) sh port 3/9
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/9  server_1           connected  41,42      a-half  a-10 10/100BaseTX


ecomm-6500-2 (enable) sh port 3/10
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/10 server_2           connected  41,42      a-half  a-10 10/100BaseTX

ecomm-6500-2 (enable) sh port 3/12
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/12 to_pix_intf1       connected  41,43      a-full a-100 10/100BaseTX


ecomm-6500-2 (enable) sh pvlan map
Port Primary Secondary
---- ------- ---------
 3/34 41      42-43

ecomm-6500-2 (enable) sh port 3/34
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/34 to_int_router      connected  41         a-full a-100 10/100BaseTX
```

外部 L2 スイッチの PVLAN の設定

```
sh pvlan
Primary Secondary Secondary-Type   Ports
------- --------- ---------------- ------------
41      45        isolated         3/7,3/33

ecomm-6500-1 (enable) sh pvlan mapping
Port Primary Secondary
---- ------- ---------
 3/43 41      45

ecomm-6500-1 (enable) sh port 3/7
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/7  from_vpn           connected  41,45      a-half  a-10 10/100BaseTX

ecomm-6500-1 (enable) sh port 3/33
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/33 to_pix_intf0       connected  41,45      a-full a-100 10/100BaseTX

ecomm-6500-1 (enable) sh pvlan map
Port Primary Secondary
---- ------- ---------
 3/43 41      45
ecomm-6500-1 (enable) sh port 3/43
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/43 to_external_router connected  41         a-half  a-10 10/100BaseTX
```

設定のテスト

この実験では、内部ルータがファイアウォールを通過して外部ルータ (インターフェイスが 198.5.6.1 の外部ファイアウォール ルータ) に到達できることを示します。

```
ping 198.5.6.1
Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

この実験は、Server 1 から見て次のことを示しています。

- Server 1 は内部ルータに ping できる。

```
server_1#ping 172.16.65.193

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

- Server 1 は VPN に ping できる。

```
server_1#ping 172.16.65.203

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.203, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

- Server 1 は PIX 内部インターフェイスに ping できない。

```
server_1#ping 172.16.65.201

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.201, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

- Server 1 は外部ルータに ping できない。

```
server_1#ping 198.5.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

次の実験は、内部ネットワークからサーバ ファームに HTTP セッションを開始できることを示しています。

```
server_2#
1w1d: HTTP: parsed uri '/'
1w1d: HTTP: processing URL '/' from host 171.68.173.3
1w1d: HTTP: client version 1.0
1w1d: HTTP: parsed extension Connection
1w1d: HTTP: parsed line  Keep-Alive
1w1d: HTTP: parsed extension User-Agent
1w1d: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
1w1d: HTTP: parsed extension Host
1w1d: HTTP: parsed line  172.16.65.202
1w1d: HTTP: parsed extension Accept
1w1d: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
1w1d: HTTP: parsed extension Accept-Encoding
1w1d: HTTP: parsed line  gzip
1w1d: HTTP: parsed extension Accept-Language
1w1d: HTTP: parsed line  en
```

```
1w1d: HTTP: parsed extension Accept-Charset
1w1d: HTTP: parsed line  iso-8859-1,*,utf-8
1w1d: HTTP: Authentication for url '/' '/' level 15  privless '/'
1w1d: HTTP: authentication required, no authentication information was provided
1w1d: HTTP: authorization rejected
1w1d: HTTP: parsed uri '/'
1w1d: HTTP: processing URL '/' from host 171.68.173.3
1w1d: HTTP: client version 1.0
1w1d: HTTP: parsed extension Connection
1w1d: HTTP: parsed line  Keep-Alive
1w1d: HTTP: parsed extension User-Agent
1w1d: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u)
1w1d: HTTP: parsed extension Host
1w1d: HTTP: parsed line  172.16.65.202
1w1d: HTTP: parsed extension Accept
1w1d: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
1w1d: HTTP: parsed extension Accept-Encoding
1w1d: HTTP: parsed line  gzip
1w1d: HTTP: parsed extension Accept-Language
1w1d: HTTP: parsed line  en
1w1d: HTTP: parsed extension Accept-Charset
1w1d: HTTP: parsed line  iso-8859-1,*,utf-8
1w1d: HTTP: parsed extension Authorization
1w1d: HTTP: parsed authorization type Basic
1w1d: HTTP: Authentication for url '/' '/' level 15  privless '/'
1w1d: HTTP: Authentication username = 'maurizio' priv-level = 15 auth-type = aaa
1w1d: HTTP: received GET ''
```

次の実験は、VPN ネットワークからの HTTP トラフィックがサーバ ファームに到達できることを示しています (アドレス 10.1.1.1 に注目してください) 。

```
1w1d: HTTP: parsed uri '/'
1w1d: HTTP: processing URL '/' from host 10.1.1.1
1w1d: HTTP: client version 1.0
1w1d: HTTP: parsed extension Connection
1w1d: HTTP: parsed line  Keep-Alive
1w1d: HTTP: parsed extension User-Agent
1w1d: HTTP: parsed line  Mozilla/4.76 [en] (Windows NT 5.0; U)
1w1d: HTTP: parsed extension Host
1w1d: HTTP: parsed line  172.16.65.202
1w1d: HTTP: parsed extension Accept\
1w1d: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image/
1w1d: HTTP: parsed extension Accept-Encoding
1w1d: HTTP: parsed line  gzip
1w1d: HTTP: parsed extension Accept-Language
1w1d: HTTP: parsed line  en
1w1d: HTTP: parsed extension Accept-Charset
1w1d: HTTP: parsed line  iso-8859-1,*,utf-8
1w1d: HTTP: Authentication for url '/' '/' level 15  privless '/'
1w1d: HTTP: authentication required, no authentication information was provided
```

次に VPN コンセントレータの設定を示します。

```
[ IP Ethernet 0:0 ]
ipbroadcast = 172.16.65.255
mode = routedSubnetMask = 255.255.255.240
IPAddress               = 172.16.65.203

[ General ]
IPsecGateway = 198.5.6.1
DeviceName              = "VPN5008"
EnablePassword          = "ww"
```

```
Password                 = "ww"
EthernetAddress          = 00:30:85:14:5c:40
DeviceType               = VPN 5002/8
ConcentratorConfiguredOn             = Timeserver not configured
ConfiguredFrom           = Command Line, from 171.68.173.3

[ IP Static ]
206.1.1.0 255.255.255.0
198.5.6.1 10.0.0.0
0.0.0.0 172.16.65.193 1

[ IP Ethernet 1:0 ]
ipbroadcast = 172.16.65.255
mode = routedSubnetMask               = 255.255.255.0
IPAddress                = 198.5.6.203

[ IKE Policy ]
Protecction = MD5_DES_G1

[ VPN Group "RemoteUsers" ]
maxconnections = 10IPNet                    = 172.16.65.0/24
LocalIPNet               = 10.1.1.0/24
Transform = esp(des,md5)

[ VPN Users ]
martin Config="RemoteUsers"
SharedKey="mysecretkey"
maurizio Config="RemoteUsers"
SharedKey="mysecretkey"
```

次のコマンドは、接続しているユーザのリストを示します。

```
sh VPN user
Port        User            Group           Client          Local           ConnectNumber
                                            Address         Address         Time
-------------------------------------------------------------------------------
VPN 0:1     martin          RemoteUsers     206.1.1.10      10.1.1.1        00:00:11:40
```

サーバ上のデフォルトゲートウェイは内部ルータ172.16.65.193で、icmpリダイレクトを172.16.65.203に発行します。この実装では、最適でないトラフィックフローが発生します。これは、ホストがフローの最初のパケットをルータに送信し、リダイレクトを受信すると、その後のパケットを処理します。代替手段として、10.x.x.x のアドレスに対しては VPN を指し示し、他のトラフィックに対しては 172.16.65.193 を指し示すように、それぞれのサーバで 2 つの異なる経路を設定することもできます。サーバでデフォルト ゲートウェイのみが設定されている場合は、ルータ インターフェイスに「ip redirect」が設定されていることを確認する必要があります。

テスト中に次のような興味深い点が見られました。198.5.6.1 のような外部アドレスにサーバまたは VPN から ping を試みる場合、デフォルト ゲートウェイは icmp を 172.16.65.201 にリダイレクトして送信します。

```
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201.
1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201.
1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201.
1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201.
1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201.
Success rate is 0 percent (0/5)
```

この時点で、サーバまたはVPNは172.16.65.201に対するアドレス解決プロトコル(ARP)要求を送信し、別のセカンダリVLAN上にあるため201からの応答を受信しません。これは、PVLANが提供

するものです。実際には、これは宛先 IP が 172.16.65.201 のトラフィックを .193 の MAC に送信することで簡単に回避できます。

ルータ .193 はトラフィックを同じインターフェイスに戻しますが、ルータ インターフェイスがプロミスキャス ポートであるため、このトラフィックは .201 に到達します。これは禁止したい動作です。この問題は、「VACL および PVLAN の既知の制限事項」の項で説明しました。

VACL の設定

この項は、サーバ ファームのセキュリティを向上させるために非常に重要です。「VACL および PVLAN の既知の制限事項」の項で説明されているように、サーバと PIX が 2 つの異なるセカンダリ VLAN に属している場合でも、攻撃者がこれらを互いに通信させるために使用できる方法はあります。サーバと PIX が直接通信しようとしても、PVLAN があるために通信することはできません。サーバが手を加えられて安全性が損なわれ、侵入者によって同じサブネットに対するトラフィックがルータに送信されるように設定された場合、これはトラフィックを元の同じサブネット上にルーティングすることになり、PVLAN の目的が無効化されます。

したがって、プライマリ VLAN (ルータからトラフィックを伝送する VLAN) で次のポリシーに基づく VACL を設定する必要があります。

- 送信元 IP がルータの IP であるトラフィックは許可する。
- 送信元と宛先の両方の IP がサーバ ファームのサブネットであるトラフィックは拒否する。
- 残りのトラフィックはすべて許可する。

```
ecomm-6500-2 (enable) sh sec acl info protect_pvlan
set security acl ip protect_pvlan
------------------------------------------------
1. permit ip host 172.16.65.193 any
2. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
3. permit ip any any

ecomm-6500-2 (enable) sh sec acl
ACL                              Type VLANS
-------------------------------  ---- -----
protect_pvlan                    IP   41
```

このACLは、サーバやPIXによって生成されたトラフィックには影響しません。ルータがサーバからのトラフィックを同じVLANにルーティングすることを防ぐだけです。最初の 2 つの文では、ルータが icmp redirect や icmp unreachable などのメッセージをサーバに送信することを許可します。

管理者が VACL によって禁止したいと思われるトラフィック フローがもう 1 つあります。これは内部ネットワークから VPN ホストへのトラフィック フローです。これを禁止するためには、VACL をプライマリ VLAN (41) にマップし、前のものと組み合せます。

```
show sec acl info all

set security acl ip protect_pvlan

1. deny ip any 10.1.1.0 0.0.0.255
2. permit ip host 172.16.65.193 any
3. deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15
4. permit ip any any
```

設定のテスト

ここではルータ .193 (zundapp) から 10.1.1.1 ホストに ping を発行します。 VACL をマッピングする前、ping は成功します。

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

VACL を VLAN 41 上でマッピングした後、同じ ping は実行できなくなります。

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

ただし、外部ルータはまだ ping できます。

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/171/192 ms
```

関連情報

- アクセス コントロール リストの設定 - Catalyst 6000 資料
- テクニカルサポート - Cisco Systems