Redes seguras com PVLANs e VACLs

Contents

Introduction

Um dos fatores importantes na criação de um projeto de segurança de rede bem-sucedido é identificar e aplicar um modelo de confiança adequado. O modelo de confiança apropriado define quem precisa falar com quem e que tipo do tráfego precisa ser trocado. Todo tráfego restante deve ser negado. Depois que o modelo de confiança adequado for identificado, o projetista de segurança deve decidir como reforçar o modelo. À medida que recursos críticos se tornam disponíveis globalmente e novas formas de ataques às redes surgem, a infraestrutura de segurança da rede tende a se tornar mais sofisticada, com mais produtos disponíveis. Os firewalls, roteadores, switches de LAN, sistemas de detecção de intrusões, servidores AAA e VPNs são algumas das tecnologias e produtos que podem ajudar a impor o modelo. Naturalmente, cada um desses produtos e tecnologias tem um papel específico dentro da implementação geral da segurança, e é essencial para o projetista compreender como esses elementos podem ser implantados.

Antes de Começar

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Prerequisites

Este documento descreve as configurações de PVLAN nos Switches que executam apenas CatOS. Para exemplos de configuração lado a lado de PVLANs em switches que executam o Cisco IOS e p CatOS, consulte o documento Configurando Isolated Private VLANs em Catalyst Switches.

Nem todos os switches e versões de software oferecem suporte a PVLAN. Consulte a Matriz de Suporte de Catalyst Switches a VLANs Privadas para determinar se a sua plataforma e a versão do software oferecem suporte a PVLAN.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Informações de Apoio

Identificar e impor um modelo de confiança apropriado parecem ser tarefas muito básicas, mas após vários anos de suporte a implementações de segurança, nossa experiência indica que os incidentes de segurança estão frequentemente relacionados aos projetos de segurança deficientes. Geralmente esses projetos deficientes são uma consequência direta da não aplicação de um modelo confiável adequado, algumas vezes porque o que é exatamente necessário não é entendido, outras vezes porque as tecnologias envolvidas não são totalmente compreendidas ou são usadas de maneira inadequada.

Este documento explica em detalhes como duas características disponíveis em nossos Catalyst Switches, VLAN Privadas (PVLAN) e Listas de Controle de Acesso de VLAN (VACL), podem ajudar a assegurar um modelo de confiança adequado nos ambientes da empresa e do provedor de serviços.

Importância da Imposição de um Modelo de Confiança Apropriado

Uma consequência imediata da não aplicação de um modelo de confiança adequado é que a implementação da segurança geral se torna menos imune às atividades maliciosas. Zonas desmilitarizadas (DMZs) são comumente implementadas sem a imposição das políticas apropriadas, o que facilita a atividade de um possível invasor. Esta seção analisa como os DMZs são implementados com freqüência e as conseqüências de um projeto fraco. Explicaremos mais tarde como mitigar ou, no melhor caso, evitar estas consequências.

Geralmente, os servidores DMZ só devem processar solicitações de entrada da Internet e, conseqüentemente, iniciar conexões com alguns servidores de back-end localizados em um segmento DMZ ou outro, como um servidor de banco de dados. Ao mesmo tempo, os servidores da DMZ não devem conversar entre si nem iniciar conexões com o mundo externo. Isso define claramente os fluxos de tráfego necessários em um modelo de confiança simples. No entanto, muitas vezes vemos esse tipo do modelo não ser imposto adequadamente.

Geralmente, os projetistas implementam DMZs usando um segmento comum para todos os servidores sem qualquer controle sobre o tráfego entre eles. Por exemplo, todos os servidores são colocados em uma VLAN comum. Como nada está controlando o tráfego na mesma VLAN, se um dos servidores for comprometido, então o mesmo servidor poderá ser explorado para lançar um ataque a qualquer um dos servidores e hosts no mesmo segmento. Isto facilita

claramente a atividade de um invasor potencial responsável por um redirecionamento de porta ou um ataque de camada de aplicativo.

Tipicamente, os firewalls e os filtros de pacote são usados somente para controlar as conexões recebidas, mas geralmente nada é feito para restringir as conexões provenientes da DMZ. Há algum tempo, uma vulnerabilidade conhecida em um script do cgi-bin permitia que um intruso iniciasse uma sessão de X-term simplesmente ao enviar um fluxo HTTP. Esse é o tráfego que deve ser permitido pelo firewall. Se o invasor tivesse sorte suficiente, ele ou ela poderia usar outra ameaça para obter um prompt de root, normalmente algum tipo de ataque de estouro de buffer. Na maioria das vezes, esses tipos de problemas podem ser evitados aplicando um modelo de confiança adequado. Primeiramente, os servidores não devem se comunicar entre si; segundo, nenhuma conexão deve ser iniciada a partir desses servidores com o mundo exterior.

Os mesmos comentários se aplicam a muitos outros cenários, desde um segmento não confiável regular qualquer a server farms em provedores de serviços de aplicativo.

As PVLAN e VACLs nos Catalyst Switches podem ajudar a garantir um modelo de confiança apropriado. As PVLANs auxiliarão na restrição do tráfego entre os hosts em um segmento comum, enquanto as VACLs contribuirão para o fornecimento um controle adicional sobre o fluxo de tráfego originado ou destinado para um determinado segmento. Esses recursos serão discutidos nas seções a seguir.

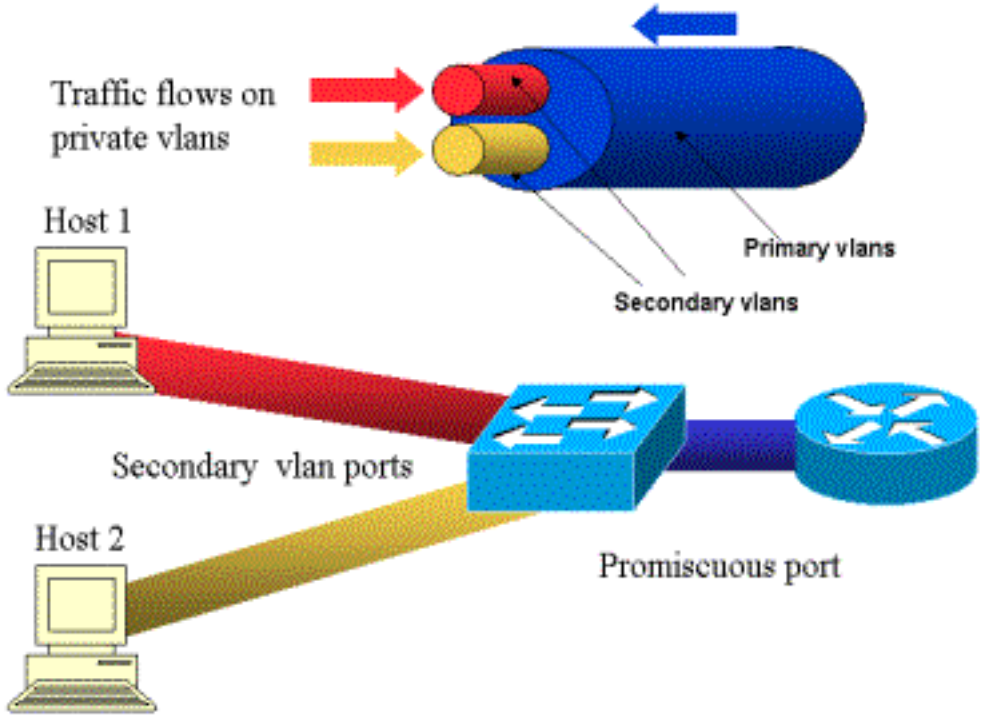
VLANs Privadas

As PVLANs estão disponíveis no Catalyst 6000 com CatOS 5.4 ou mais recente e nos Catalyst 4000, 2980G, 2980G-A, 2948G e 4912G com CatOS 6.2 ou mais recente.

Da nossa perspectiva, as PVLAN são uma ferramenta que permite segregar o tráfego na camada 2 (L2), que transforma um segmento de broadcast em um segmento não broadcast do tipo multiacesso. O tráfego proveniente de uma porta promíscua (isto é, uma porta que seja capaz de encaminhar as VLANs principais e secundárias) de um switch pode sair por todas as portas que pertencem à mesmo VLAN principal. O tráfego de um switch proveniente de uma porta mapeada em uma VLAN secundária (pode ser isolada, uma comunidade ou uma VLAN de comunidade bidirecional) pode ser encaminhado para uma porta promíscua ou a uma porta que pertença à mesma VLAN de comunidade. Várias portas mapeadas para a mesma VLAN isolada não podem trocar nenhum tráfego.

A imagem a seguir mostra o conceito.

Figura 1: VLANs Privadas



A VLAN principal está representado em azul. As VLANs secundárias estão representadas em vermelho e amarelo. O host 1 está conectado a uma porta do switch que pertence à VLAN vermelha secundária. O host 2 está conectado a uma porta do switch que pertence à VLAN amarela secundária.

Quando um host está transmitindo, o tráfego é transportado na VLAN secundária. Por exemplo, quando Host-2 transmite, seu tráfego vai para a VLAN amarela. Quando estes hosts estão recebendo, o tráfego é oriundo da VLAN azul, a VLAN principal.

As portas em que os roteadores e firewalls são conectados são portas promíscuas porque elas podem encaminhar o tráfego proveniente de cada VLAN secundária definida no mapeamento, bem como da VLAN principal. As portas conectadas a cada host podem encaminhar somente o tráfego proveniente da VLAN principal e da VLAN secundária configuradas nessa porta.

O desenho representa as VLAN privadas como os pipes diferentes que conectam roteadores e hosts: O pipe que empacota todos os outros é a VLAN principal (azul), e o tráfego na VLAN azul flui dos roteadores para os hosts. Os pipes internos da VLAN principal são as VLAN secundárias, e o tráfego que viaja nesses pipes é proveniente dos hosts para o roteador.

Conforme a imagem aparece, uma VLAN principal pode empacotar uma ou mais VLANs secundárias.

Já foi dito neste documento que as PVLANs ajudam a aplicar o modelo de confiança adequado, simplesmente garantindo a divisão de hosts em um segmento em comum. Agora que sabemos mais sobre VLANs privadas, vamos ver como isso pode ser implementado em nosso cenário de DMZ inicial. Os servidores não devem se comunicar entre si, mas eles ainda precisam se comunicar com o firewall ou roteador ao qual estão conectados. Nesse caso, os servidores são conectados a portas isoladas, enquanto os roteadores e firewalls são conectados a portas heterogêneas. Assim, se um dos servidores for comprometido, o intruso não poderá usar o mesmo servidor para desferir um ataque a um outro servidor dentro do mesmo segmento. O switch descartará todo o pacote em velocidade de fio, sem nenhuma penalidade de desempenho.

Outra observação importante é que esse tipo de controle pode ser implementado apenas no dispositivo L2 porque todos os servidores pertencem à mesma sub-rede. Não há nada que um firewall ou um roteador possa fazer, uma vez que os servidores tentarão se comunicar diretamente. Outra opção é dedicar uma porta de firewall por servidor, mas isso é provavelmente muito caro, difícil de implementar e não dimensionável.

Em uma seção posterior, descreveremos em detalhes outros cenários típicos nos quais você poderá usar esse recurso.

Listas de controle de acesso de VLAN

As VACLs estão disponíveis no Catalyst 6000 Series com CatOS 5.3 ou mais recente.

As VACLs podem ser configuradas em um Catalyst 6500 na L2 sem a necessidade de um roteador (você precisaria apenas de uma Placa de Recursos de Políticas (PFC)). Elas são impostas em velocidade de fio. Assim não há nenhuma penalidade de desempenho relacionada à configuração de VACLs em um Catalyst 6500. Como a consulta das VACLs é executada no hardware, independentemente do tamanho da lista de acessos, a taxa de encaminhamento permanece inalterada.

As VACLs podem ser mapeadas separadamente para VLANs primárias ou secundárias. Ter uma VACL configurada em uma VLAN secundária permite filtrar o tráfego originado por hosts sem tocar no tráfego gerado por roteadores ou firewalls.

Ao combinar VACLs e VLANs privadas é possível filtrar tráfego com base na direção do tráfego em si. Por exemplo, se dois roteadores estiverem conectados ao mesmo segmento como hosts idênticos (servidores, por exemplo), VACLs poderão ser configurados em VLANs secundárias de forma que apenas o tráfego gerado pelos hosts seja filtrado, enquanto o tráfego trocado entre os roteadores permaneça inalterado.

As VACLs podem ser facilmente distribuídas para impor o modelo de confiança apropriado. Vamos analisar o caso do DMZ. Os servidores na DMZ devem atender apenas a conexões de entrada, e não se espera que eles iniciem conexões para o mundo externo. É possível aplicar uma VACL à VLAN secundária para controlar o tráfego de saída desses servidores. É crucial notar que, ao usar VACLs, o tráfego é descartado por hardware e não há nenhum impacto sobre a CPU do roteador nem do switch. Mesmo no caso em que um dos servidores está envolvido em um ataque de negação de serviços distribuída (DDoS) na condição de uma origem, o switch descartará todo o tráfego ilegítimo em velocidade de fio, sem nenhuma penalidade de desempenho. Filtros similares podem ser aplicados no roteador ou no firewall em que os servidores estão conectados, mas isso geralmente causa implicações de desempenho severas.

As ACLs com base em MAC não trabalham bem com o tráfego IP. Assim recomenda-se usar VACLs para monitorar/controlar PVLANs.

Limitações conhecidas de VACLs e PVLANs

Ao configurar a filtragem com VACLs, você deverá ter cuidado em relação ao tratamento de fragmentos no PFC e garantir que a configuração seja ajustada de acordo com a especificação do hardware.

Com o projeto de hardware do PFC do supervisor 1 do Catalyst 6500, é melhor negar

explicitamente os fragmentos icmp. O motivo é que os fragmentos do protocolo ICMP e a resposta de eco são considerados os mesmos pelo hardware e, por padrão, o hardware é programado para permitir explicitamente os fragmentos. Portanto, se desejar impedir que os pacotes de resposta de eco deixem os servidores, você deverá configurar isso explicitamente com a linha deny icmp any any fragment. As configurações neste documento levam isso em conta.

Esta é uma limitação de segurança conhecida das PVLANs, ou seja, a possibilidade de que um roteador encaminhe o tráfego de volta para a mesma sub-rede da qual é proveniente. Um roteador pode rotear o tráfego em portas isoladas impedindo a finalidade das PVLANs. Essa limitação ocorre devido ao fato de que as PVLANs são uma ferramenta que fornece isolamento em L2 e não na Camada 3 (L3).

O Unicast Reverse Path Forwarding (uRPF) não trabalha bem com portas de host de PVLANs. Assim, o uRPF não deve ser usado em combinação com PVLANs.

Uma correção para esse problema é feita por meio das VACLs configuradas nas VLANs principais. Os estudos de caso fornecem as VACLs que precisam ser configuradas na VLAN principal para descartar o tráfego originado pela mesma sub-rede e roteado de volta para a mesma sub-rede.

Em algumas placas, a configuração de portas de truncamento/mapas/mapeamentos de PVLAN está sujeita a algumas restrições em que vários mapeamentos de PVLAN precisam pertencer a ASICs (Application-Specific Integrated Circuits) de portas diferentes para serem configurados. Essas restrições são removidas na nova porta ASIC Coil3. Consulte a Documentação dos Catalyst Switches na configuração do software para obter detalhes.

Exemplo de estudos de caso

A seção a seguir descreve três estudos de caso que representam a maioria das implementações e fornecem os detalhes relativos à distribuição de segurança das PVLANs e VACLs.

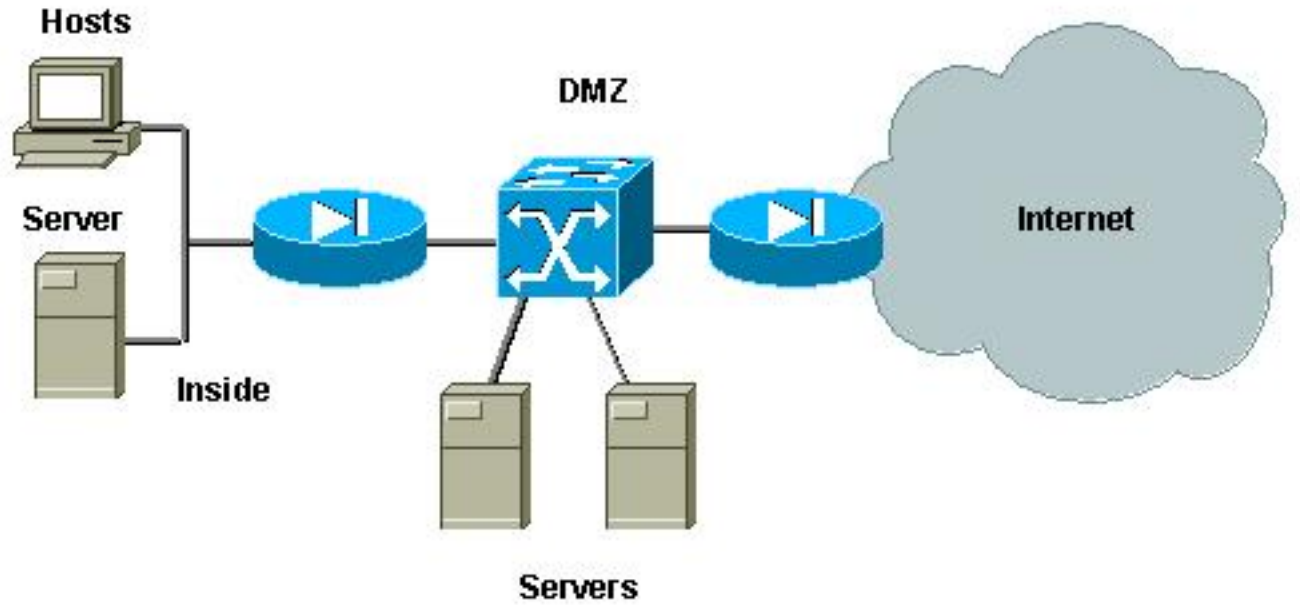
Estes cenários são:

- Passagem DMZ
- DMZ externa
- VPN Concentrator em Paralelo ao Firewall

Passagem DMZ

Esse é um dos cenários implantados mais comuns. Neste exemplo, o DMZ é implementado como uma área de trânsito entre dois roteadores de firewall, conforme ilustrado na imagem abaixo.

Figura 2: Passagem DMZ



Neste exemplo, os servidores da DMZ devem ser acessados pelo meio externo e pelos usuários internos, mas eles não precisam se comunicar um com o outro. Em alguns casos, os servidores DMZ necessitam abrir algum tipo de conexão para um host interno. Ao mesmo tempo, os clientes internos precisam acessar a Internet sem restrições. Um bom exemplo é aquele com servidores Web na DMZ que precisam se comunicar com um servidor de banco de dados situado na rede interna, ao mesmo tempo em que os clientes internos precisam acessar a Internet.

O firewall externo é configurado para permitir conexões recebidas aos servidores localizados no DMZ, mas normalmente nenhum filtro ou restrição é aplicado ao tráfego de saída, particularmente o tráfego originado no DMZ. Como discutimos anteriormente neste documento, isso pode potencialmente facilitar a atividade de um agressor por duas razões: primeiro, assim que um dos hosts da DMZ for comprometido, todos hosts restantes DMZ serão expostos. Segundo, um agressor pode facilmente explorar uma conexão de saída.

Como os servidores da DMZ não precisam falar uns com os outros, a recomendação é garantir que eles estejam isolados em L2. As portas de servidor serão definidas como portas isoladas de PVLANs, enquanto que as portas que se conectam aos firewalls serão definidas como promíscuas. Definir uma VLAN principal para os firewalls e uma VLAN secundária para os servidores DMZ fará com que se obtenha isso.

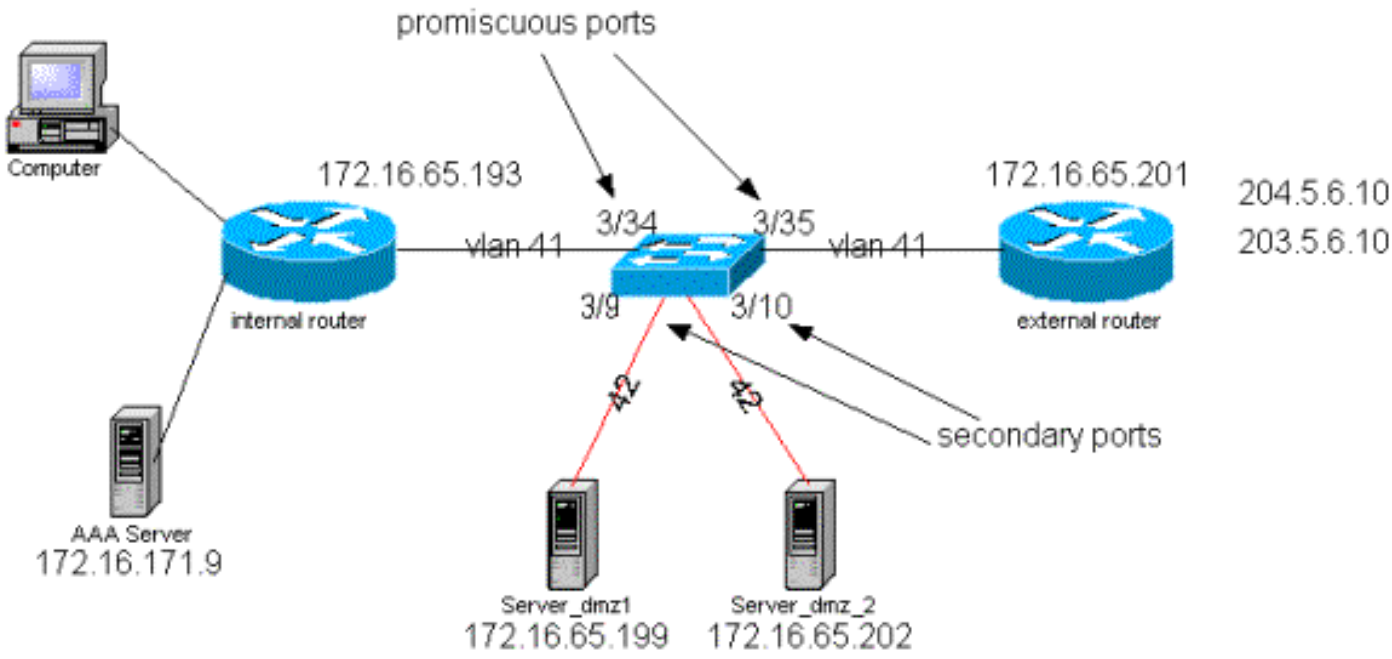
As VACLs serão usadas para controlar o tráfego originado na DMZ. Isso evitará que um agressor consiga abrir uma conexão de saída ilegítima. É importante ter em mente que os servidores da DMZ não somente precisarão responder com tráfego correspondente às sessões de clientes, mas também precisarão de alguns serviços adicionais, tais como Domain Name System (DNS) e a descoberta de caminhos da unidade máxima de transmissão (MTU). Assim, a ACL deve permitir todos os serviços que os servidores DMZ precisam.

Teste de DMZ de Passagem

Em nosso ambiente de teste, implementamos um segmento DMZ com dois roteadores configurados como servidores de campo, server_dmz1 e server_dmz2. Esses servidores devem ser acessados de fora, assim como os clientes internos, e todas as conexões HTTP são autenticadas com o uso de um servidor RADIUS interno (CiscoSecure ACS para UNIX). Tanto o

roteador interno quanto o externo são configurados como firewalls de filtro de pacotes. A imagem a seguir ilustra o ambiente de teste, incluindo o método de endereçamento usado.

Figura 3: Ambiente de Teste do DMZ de Passagem



A lista a seguir reúne as etapas fundamentais da configuração de PVLANs. O Catalyst 6500 é usado como o switch L2 na DMZ.

- O Server_dmz_1 está desconectado da porta 3/9
- Server_dmz_2 está conectado à porta 3/10
- O roteador interno está conectado à porta 3/34
- O roteador externo está conectado à porta 3/35

Escolhemos as seguintes VLANs:

- 41 é a VLAN principal
- 42 é a VLAN isolada

Configuração da VLAN Privada

A seguinte configuração define as PVLANs nas portas envolvidas.

```
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
```

Configuração da VACL na VLAN Principal

Esta seção é crucial para melhorar a segurança no DMZ. Conforme descrito nas Limitações Conhecidas das VACLs e na seção PVLANs, mesmo se os servidores pertencerem a duas VLAN secundárias diferentes ou à mesma VLAN isolada, ainda haverá uma maneira de um atacante fazê-los se comunicar. Se os servidores tentarem se comunicar diretamente, não conseguirão fazê-lo em L2 por causa das PVLANs. Se os servidores estiverem comprometidos e forem configurados por um invasor de tal forma que o tráfego para a mesma sub-rede seja enviado para o roteador, ele roteará o tráfego de volta para a mesma sub-rede, anulando assim a finalidade das PVLANs.

Consequentemente, uma VACL precisa ser configurada na VLAN principal (a VLAN que transporta o tráfego dos roteadores) com as seguintes políticas:

- Permitir o tráfego cujo IP de origem seja o IP do roteador
- Negar o tráfego em que os endereços IP de origem e destino de destino são da sub-rede DMZ
- Permitir todo o resto do tráfego

```
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
```

Essa ACL não afetará o tráfego gerado pelos servidores. Ela impedirá somente que os roteadores distribuam o tráfego provenientes dos servidores de volta para a mesma VLAN. As primeiras duas instruções permitem que os roteadores enviem mensagens como redirecionamento de ICMP ou ICMP não alcançável para os servidores.

Configuração da VACL na VLAN secundária

Os seguintes registros de configuração são utilizados para mostrar como configuramos uma VACL para filtrar o tráfego gerado pelos servidores. Ao configurar essa VACL, queremos:

- Permitir o ping dos servidores (permitir eco)

- Evitar que as respostas de eco saiam dos servidores
- Permitir as conexões de HTTP provenientes do mundo externo
- Permitir a autenticação RADIUS (porta 1645 do UDP) e o tráfego de contabilidade (porta 1646 do UDP)
- Permite o tráfego de DNS (UDP porta 53)

Nosso objetivo é impedir todo o restante do tráfego.

No que se refere à fragmentação, pressupomos o seguinte no segmento do servidor:

- Os servidores não gerarão tráfego fragmentado
- Épossível que os servidores recebam tráfego fragmentado

Considerando o design do hardware do PFC do Supervisor 1 do Catalyst 6500, é melhor negar explicitamente os fragmentos de icmp. O motivo para isso é que os fragmentos de ICMP e echo-reply são considerados iguais pelo hardware e, por padrão, o hardware está programado para permitir fragmentos explicitamente. Portanto, se desejar impedir que os pacotes de resposta de eco deixem os servidores, você deverá configurar isso explicitamente com a linha deny icmp any any fragment.

```
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
```

Teste da Configuração

A saída a seguir foi capturada quando PVLANs estavam configuradas, mas nenhuma VACL havia sido aplicada ainda. Este teste está mostrando que, do roteador externo, o usuário pode efetuar **pings no roteador interno e nos servidores.**

```
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
```

O exemplo abaixo mostra que podemos executar ping pelos servidores para a rede externa, o gateway padrão, mas não os servidores pertencentes à mesma VLAN secundária.

```
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)
```

Após o mapeamento das VACLs, o **ping do roteador externo não será mais permitido:**

```
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)
```

O exemplo a seguir mostra o servidor que recebe pedidos HTTP GET da rede interna:

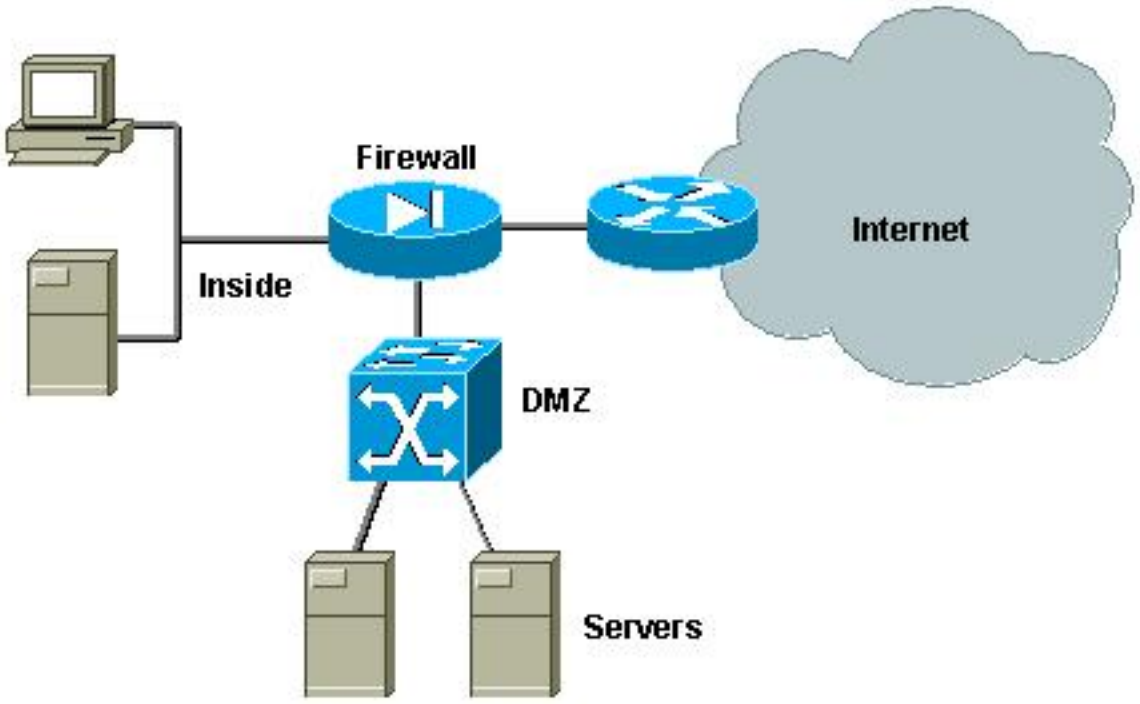
```
server_dmz1#debug ip http url
HTTP URL debugging is on
```

```
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 ''
```

DMZ externa

O cenário de DMZ externa é provavelmente a implementação mais aceita e mais empregada. Uma DMZ externa é implementada com o uso de uma ou mais interfaces de um firewall, conforme mostrado na figura abaixo.

Figura 4: DMZ externa



Normalmente, os requisitos para DMZs tendem a ser os mesmos, independentemente da implementação do projeto. Como no caso anterior, os servidores da DMZ devem poder ser acessados por clientes externos e pela rede interna. Os servidores DMZ finalmente precisarão de acesso a alguns recursos internos, mas esses servidores geralmente não conversam entre si. Ao mesmo tempo, nenhum tráfego deve ser iniciado da DMZ para a Internet. Esses servidores da DMZ devem somente responder com tráfego correspondente às conexões recebidas.

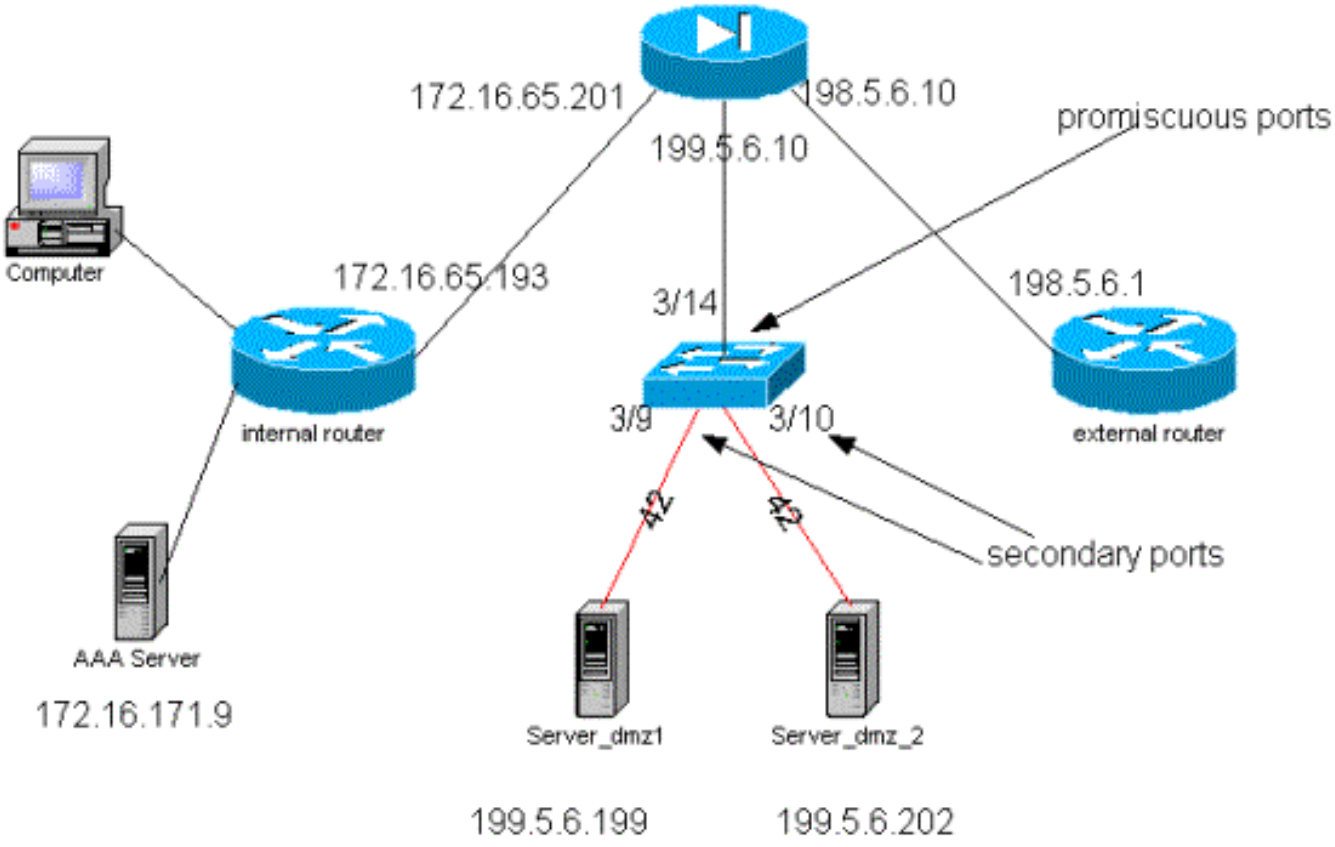
Como nos estudos de caso anteriores, o primeiro passo da configuração consiste em conseguir o isolamento em L2 por meio das PVLANs e garantir que os servidores da DMZ não consigam falar uns com os outros e que os hosts internos e externos possam acessá-los. Isso é implementado com a configuração dos servidores em uma VLAN secundária com portas isoladas. O firewall deve ser definido em um VLAN principal com uma porta promíscua. O firewall será o único dispositivo dentro dessa VLAN principal.

O segundo passo é definir ACLs para controlar o tráfego originado na DMZ. Ao definir essas ACLs, precisamos garantir que somente o tráfego necessário seja permitido.

Teste da DMZ Externa

A imagem a seguir mostra o ambiente de teste implementado para esse estudo de caso, no qual usamos um PIX Firewall com uma terceira interface para a DMZ. O mesmo conjunto de roteadores é usado como servidores Web, e todas as sessões de HTTP são autenticadas com o mesmo servidor RADIUS.

Figura 5: Ambiente de Teste da DMZ Externa



Para esse cenário, anexamos apenas os trechos mais interessantes dos arquivos de configuração, uma vez que as configurações de PVLANs e VACLs foram explicadas em detalhes nos estudos de caso anteriores.

Configuração de PIX

```
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
```

Configuração de RADIUS

Configuração de NAS

```
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
```

Servidor RADIUSCSUX

```
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"

}
```

Configuração do Catalyst

Deve-se observar que, nessa configuração, não há necessidade de configurar uma VACL na

VLAN principal, pois o PIX não redireciona o tráfego para a mesma interface da qual ele é proveniente. Uma VACL como aquela descrita na seção Configuração da VACL na VLAN Principal seria redundante.

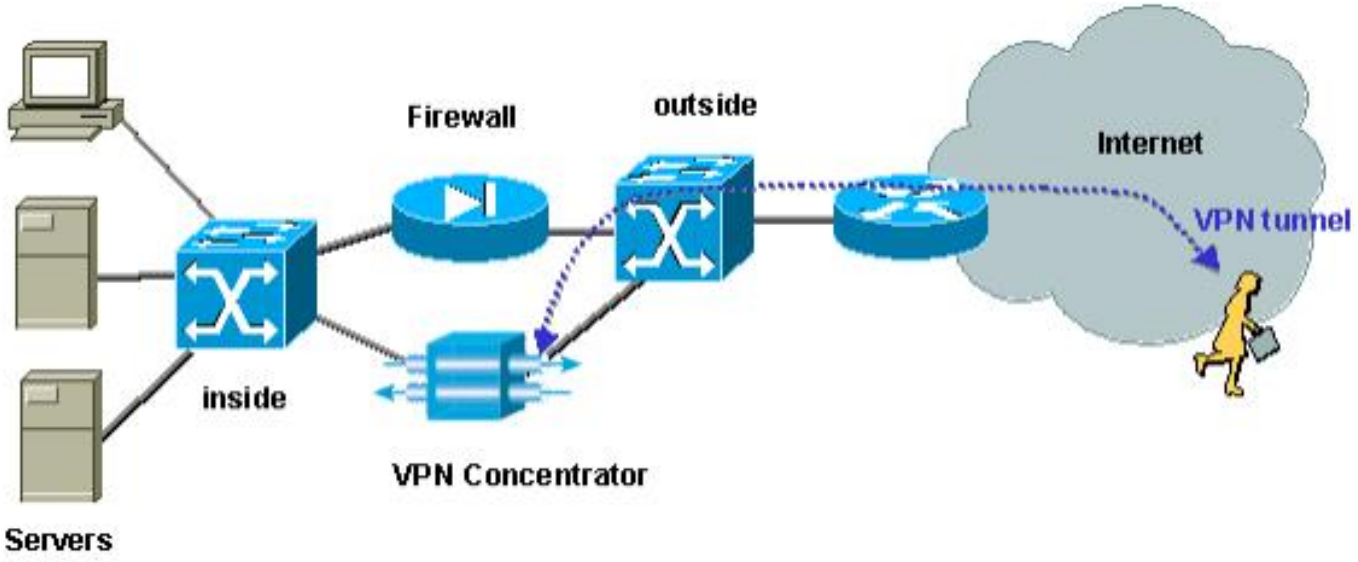
```
set security acl ip dmz_servers_out
------------------------------------------------
1. deny icmp any any fragment
2. permit icmp host 199.5.6.199 any echo
3. permit icmp host 199.5.6.202 any echo
4. permit tcp host 199.5.6.199 eq 80 any established
5. permit tcp host 199.5.6.202 eq 80 any established
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
```

VPN Concentrator em Paralelo ao Firewall

Ao implementar redes privadas virtuais (VPNs) de acesso, sem dúvida uma das abordagens favoritas é o design em paralelo (ilustrado na imagem abaixo). Os clientes geralmente preferem essa abordagem do projeto porque ela é fácil de implementar, com quase nenhum impacto na infraestrutura existente e também porque ela é relativamente fácil de dimensionar com base na flexibilidade do dispositivo.

Na abordagem paralela, o VPN Concentrator se conecta com os segmentos internos e externos. Todas as sessões de VPN terminam no concentrador sem passar pelo firewall. Normalmente, espera-se que os clientes VPN tenham acesso irrestrito à rede interna, mas, às vezes, seu acesso pode ser restrito a um conjunto de servidores internos (server farm). Uma das características desejáveis é segregar o tráfego de VPN do tráfego da Internet regular. Assim, por exemplo, os clientes VPN não têm permissão de acessar a Internet através do firewall corporativo.

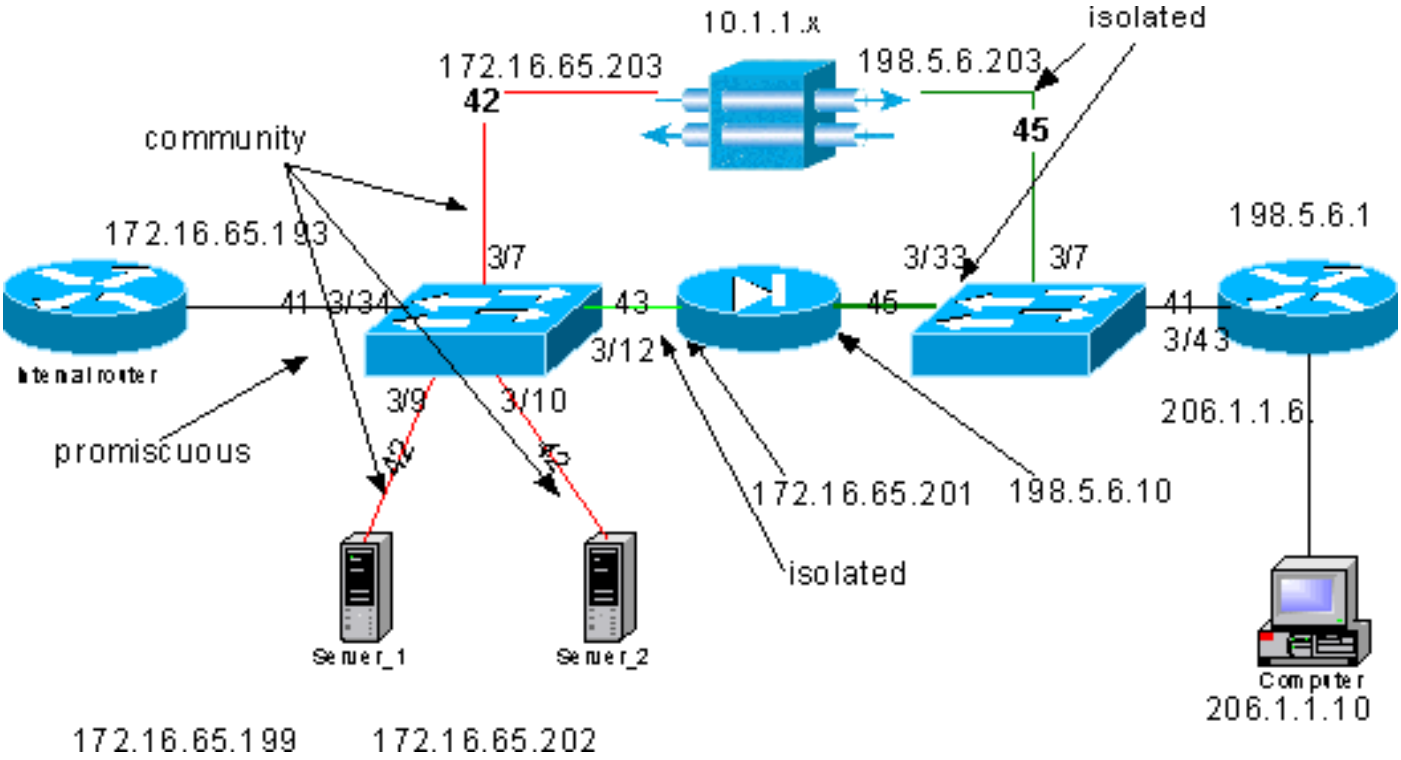
Figura 6: VPN Concentrator em Paralelo ao Firewall



Teste do VPN Concentrator em Paralelo ao Firewall

Nesse exemplo, usamos um VPN 5000 Concentrator, que foi instalado juntamente com um PIX Firewall. Os dois roteadores configurados como servidores Web foram instalados no segmento interno como um server farm interno. Os clientes VPN têm permissão para acessar somente o server farm, e o tráfego de internet deve ser segregado do tráfego VPN (IPSec). A figura abaixo mostra o ambiente de teste.

Figura 7: Ambiente de Teste do VPN Concentrator em Paralelo ao Firewall



Neste cenário, há duas áreas de interesse principais:

- O Switch L2 interno
- O switch L2 externo

Os fluxos de tráfego para o switch L2 interno são definidos com base nas seguintes afirmações:

- Os clientes VPN têm acesso total a um conjunto predefinido de servidores internos (server farm)
- Os clientes internos também recebem permissão para acessar o server farm
- Os clientes internos têm acesso irrestrito à Internet
- O tráfego proveniente do VPN Concentrator deve ser isolado do PIX Firewall

Os fluxos de tráfego referentes ao Switch L2 externo são definidos da seguinte forma:

- O tráfego proveniente do roteador deve poder ir para o VPN Concentrator ou para o PIX.
- O tráfego proveniente do PIX deve ser isolado do tráfego proveniente da VPN

Além disso, é possível que o administrador queira evitar que o tráfego da rede interna chegue aos hosts da VPN, o que pode ser feito por meio das VACLs configurados na VLAN principal (a VACL filtrará somente o tráfego que sai do roteador interno; nenhum outro tráfego será afetado).

Configuração de PVLAN

Como o objetivo principal desse design é manter o tráfego proveniente do PIX segregado do tráfego dos servidores e o VPN Concentrator, configuramos o PIX em uma PVLAN diferente da PVLAN em que os servidores e o VPN Concentrator estão configurados.

O tráfego proveniente da rede interna deve poder acessar a server farm, bem como o VPN Concentrator e o PIX. Como consequência, a porta que se conecta à rede interna será uma porta promíscua.

Os servidores e o VPN Concentrator pertencem à mesma VLAN secundária porque poderão se comunicar um com o outro.

Quanto ao switch L2 externo, o roteador que dá acesso à Internet (que normalmente pertence a um provedor de serviços de Internet (ISP)) é conectado a uma porta promíscua enquanto o concentrador VPN e o PIX pertencem às mesmas VLANs privadas e isoladas (de modo que não possam trocar tráfego). Com isso, o tráfego proveniente do provedor de serviço pode seguir o caminho para o VPN Concentrator ou para o PIX. O PIX e o VPN Concentrator são mais protegidos, desde que estejam isolados.

Configuração de PVLAN do Switch interno L2

```
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
```

Configuração de PVLAN do Switch L2 Externo

```
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
```

Teste da Configuração

Esta experiência mostra que o roteador interno pode atravessar o firewall e acessar o roteador externo (roteador do firewall externo cuja interface é 198.5.6.1).

```
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 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Esta experiência mostra o seguinte, tudo do servidor 1:

- O servidor 1 pode executar ping no roteador interno:
  ```
  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
  ```
- O servidor 1 pode efetuar ping na VPN:
  ```
  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
  ```
- O servidor 1 não pode fazer ping da interface interna PIX:
  ```
  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)
  ```
- O Servidor 1 não consegue efetuar ping no roteador externo:
  ```
  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)
  ```

A experiência a seguir mostra que as sessões de HTTP podem ser abertas da rede interna até o server farm.

```
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 ''
```

A experiência a seguir mostra que o tráfego de HTTP da rede VPN pode encontrar seu caminho para o server farm (observe o endereço 10.1.1.1).

```
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
```

Veja a seguir a configuração do VPN Concentrator:

```
[ 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"
```

O comando a seguir mostra a lista de usuários conectados.

```
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
```

Deve-se observar que o gateway padrão nos servidores é o roteador interno 172.16.65.193, o qual emitirá um icmp redirect para 172.16.65.203. Essa implementação provoca fluxos de tráfego que não são ideais, porque o host envia o primeiro pacote de um fluxo para o roteador, e ao receber o redirecionamento, envia os pacotes subsequentes para o gateway mais adequado para tratar desse tráfego. Alternativamente, é possível configurar duas rotas diferentes nos servidores em si a fim de apontar para a VPN para os endereços 10.x.x.x e para 172.16.65.193 para o resto do tráfego. Se apenas o gateway padrão estiver configurado nos servidores, então será necessário verificar se a interface do roteador está configurada com "ip redirect".

Um ponto interessante observado durante o teste é mostrado a seguir. Se tentarmos efetuar ping em um endereço externo como 198.5.6.1 a partir dos servidores ou da VPN, o gateway padrão enviará e redirecionará esse ping pelo protocolo ICMP para 172.16.65.201.

```
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)
```

Os servidores ou a VPN nesse ponto enviarão uma solicitação do Address Resolution Protocol (ARP) para 172.16.65.201 e não obterão nenhuma resposta de 201 porque ele está em outra VLAN secundária. Isso é o que a PVLAN nos fornece. Na realidade, existe uma maneira fácil de evitar isso, que é enviar o tráfego ao MAC do .193 e com o IP de destino 172.16.65.201.

O roteador .193 encaminhará o tráfego de volta para a mesma interface, desde que a interface de roteador seja uma porta misturada, o tráfego alcançará .201, que queremos evitar. Esse problema foi explicado na seção Limitações conhecidas de VACLs e de PVLANs.

Configuração de VACL

Esta seção é crucial para aprimorar a segurança no server farm. Conforme descrito na seção Limitações Conhecidas das VACLs e PVLANs, mesmo se os servidores e o PIX pertencerem a duas VLANs secundárias diferentes, haverá ainda um método que um atacante pode usar para fazê-los se comunicar uns com os outros. Se eles tentarem se comunicar diretamente, não poderão fazê-lo por causa das PVLANs. Se os servidores estiverem comprometidos e forem configurados por um invasor de tal forma que o tráfego para a mesma sub-rede seja enviado para o roteador, ele roteará o tráfego de volta para a mesma sub-rede, anulando assim a finalidade das PVLANs.

Consequentemente, uma VACL precisa ser configurada na VLAN principal (a VLAN que transporta o tráfego dos roteadores) com as seguintes políticas:

- Permitir o tráfego cujo IP de origem seja o IP do roteador
- Recuse o tráfego cujos IPs de origem e destino são a sub-rede de farm de servidor.
- Permitir todo o resto do tráfego

```
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
```

Essa ACL não afetará o tráfego gerado pelos servidores nem pelo PIX; Ela impedirá somente que os roteadores distribuam o tráfego provenientes dos servidores de volta para a mesma VLAN. As primeiras duas instruções permitem que os roteadores enviem mensagens como redirecionamento de ICMP ou ICMP não alcançável para os servidores.

Identificamos outro fluxo de tráfego que o administrador pode querer interromper por meio de VACLs, e esse fluxo se origina na rede interna e segue em direção aos hosts da VPN. Para fazer isso, uma VACL pode ser mapeada na VLAN principal (41) e ser combinada com a anterior:

```
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
```

Teste da Configuração

Agora estamos efetuando ping no host 10.1.1.1 do roteador .193 (zundapp). Antes de mapearmos a VACL, o ping é bem-sucedido.

```
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
```

Após o mapeamento da VACL na VLAN 41, o mesmo ping não terá êxito.

```
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)
```

Entretanto, ainda podemos efetuar ping no roteador externo:

```
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
```

Informações Relacionadas

- Configuração de Listas de Controle de Acesso - Documentação do Catalyst 6000
- Suporte Técnico - Cisco Systems