Cómo asegurar redes con una VLAN privada y listas de control de acceso de VLAN

Contenido

Introducción

Uno de los factores claves en la construcción de un diseño exitoso de seguridad de red es identificar y fortalecer un modelo de confianza adecuado. El modelo de confianza adecuado define quién debe hablar con quién y qué tipo de tráfico debe ser intercambiado; el resto del tráfico debe ser denegado. Una vez que se ha identificado el modelo de confianza apropiado, el diseñador de seguridad debe decidir cómo exigir el modelo. A medida que están disponibles globalmente más recursos críticos y evolucionan las nuevas formas de los ataques de red, la infraestructura de seguridad de la red tiende a volverse más sofisticada y hay más productos disponibles. Los firewalls, los routers, los switches de LAN, los sistemas de detección de intrusiones, los servidores AAA, y las VPN son algunas de las tecnologías y productos que pueden ayudar a imponer el modelo. Por supuesto, cada uno de estos productos y tecnologías cumple una función particular dentro de la implementación de seguridad general, y es muy importante que el diseñador comprenda cómo pueden implementarse estos elementos.

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

prerrequisitos

Este documento describe las configuraciones de PVLAN en switches que sólo ejecutan CatOS. Para ver ejemplos de configuración conjunta de redes PVLAN en switches que ejecutan el IOS y CatOS de Cisco, consulte el documento Configuración de Redes VLAN Privadas Aisladas en Switches Catalyst.

No todos los switches y las versiones de software son compatibles con PVLAN. Consulte Matriz de Soporte de Switch Catalyst para VLAN Privada para determinar si su plataforma y versión de software soportan PVLAN.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Antecedentes

Identificar e imponer un modelo de confianza apropiado parece ser una tarea básica, sin embargo, después de varios años de soportar las implementaciones de seguridad, nuestra experiencia indica que los incidentes de seguridad en general están relacionados con diseños deficientes de seguridad. Por lo general estos diseños de baja calidad son consecuencia directa de no aplicar un modelo de confianza adecuado, en algunas ocasiones debido a que no se lo comprende y en otras simplemente porque las tecnologías involucradas no se entienden completamente o se utilizan de manera incorrecta.

Este documento explica en detalle cómo dos funciones disponibles en nuestros switches de Catalyst, VLAN Privadas (PVLAN) y Listas de Control de Acceso a VLAN (VACL), pueden garantizar un modelo de confianza adecuado en las empresas y en entornos de proveedores de servicios.

La importancia de aplicar un modelo de confianza apropiado

Una consecuencia inmediata de no aplicar un modelo de confianza adecuado es que la implementación general de seguridad se torna menos inmune a las actividades malintencionadas. Las zonas desmilitarizadas (DMZ) son normalmente implementadas sin que se apliquen las políticas correctas y de este modo se facilita la actividad de un potencial intruso. Esta sección analiza cómo se implementan con frecuencia las DMZ y las consecuencias de un diseño deficiente. Más adelante explicaremos cómo mitigar, o en el mejor de los casos, evitar estas consecuencias.

Por lo general, se supone que los servidores DMZ sólo procesan peticiones procedentes de Internet y que eventualmente inician conexiones con algunos servidores de extremo posterior ubicados en un segmento interior u otro segmento DZN como un servidor de base de datos. Al mismo tiempo, los servidores DMZ no deben comunicarse entre sí ni iniciar conexiones hacia el exterior. Esto define claramente los flujos de tráfico necesarios en un modelo de confianza simple; sin embargo, a menudo se observa que esta clase de modelo no se impone de forma adecuada.

Por lo general, los diseñadores tienden a implementar DMZ utilizando un segmento común para todos los servidores sin ningún control sobre el tráfico entre ellos. Por ejemplo, todos los servidores están localizados en una VLAN común. Dado que nada controla el tráfico dentro de la

misma VLAN, si uno de los servidores está comprometido, se puede aprovechar el mismo servidor para originar un ataque a cualquiera de los servidores o los hosts en el mismo segmento. Esto claramente facilita la actividad de un intruso potencial que realiza un redireccionamiento de puerto o un ataque a la Capa de Aplicación.

Típicamente, los firewalls y los filtros de paquete se utilizan solamente para controlar las conexiones entrantes, pero generalmente no se realiza ninguna acción para restringir las conexiones que se originan en la DMZ. Hace algún tiempo existía una vulnerabilidad reconocida en una secuencia cgi-bin que permitía que un intruso comenzara una sesión X-term sólo enviando una secuencia HTTP; este tipo de tráfico debe permitir firewall. Si el intruso tuvo suerte, puede usar otra invitación para obtener un mensaje de raíz, normalmente algún tipo de ataque de desbordamiento de búfer. La mayoría de las veces, estos tipos de problemas pueden ser evitados mediante la implementación del modelo de confianza adecuado. Primero, los servidores no deben comunicarse entre sí y segundo, no debe originarse ninguna conexión desde estos servidores hacia el exterior.

Los mismos comentarios se aplican a muchos otros escenarios, desde un segmento no confiable irregular hasta bloques de servidores en los proveedores de servicios de aplicación.

Las PVLAN y las VACL en los switches de Catalyst pueden garantizar un modelo de confianza adecuado. Las PVLAN ayudarán al restringir el tráfico entre los hosts en un segmento común, mientras que las VACL contribuirán proveyendo más control en cualquier flujo de tráfico originado o destinado a un segmento en particular. Estas funciones se tratan en las secciones a continuación.

VLAN privadas

Las PVLAN están disponibles en el router Catalyst 6000 que ejecuta CatOS 5.4 o una versión posterior, en el Catalyst 4000, 2980G, 2980G-A, 2948G y en el 4912G que ejecuta CatOS 6.2 o posterior.

Desde nuestra perspectiva, las PVLAN son una herramienta que permiten segregar el tráfico en la Capa 2 (L2) al convertir unsegmento de difusión en un segmento sin difusión de acceso múltiple. El tráfico que ingresa a un switch desde un puerto promiscuo (es decir, un puerto capaz de reenviar VLAN tanto primarias como secundarias) puede salir de todos los puertos que pertenecen a la misma VLAN primaria. El tráfico que llega a un switch proveniente de un puerto correlacionado con una VLAN secundaria (puede ser una VLAN de comunidad aislada, comunitaria o bidireccional) puede reenviarse a un puerto promiscuo o a un puerto perteneciente a la misma VLAN de comunidad. Los puertos múltiples correlacionados en la misma VLAN no pueden intercambiar tráfico.

La siguiente imagen muestra el concepto.

Figura 1: VLAN privadas

La VLAN principal se muestra en azul; las VLAN secundarias se muestran en rojo y amarillo. El Host 1 se conecta a un puerto del switch que pertenece a la VLAN roja secundaria. El Host 2 se conecta a un puerto del switch que pertenece a la VLAN amarilla secundaria.

Cuando un host está en el proceso de transmisión, el tráfico se transporta en la VLAN secundaria. Por ejemplo, cuando el Host 2 está en el proceso de transmisión, su tráfico se transporta en la VLAN amarilla. Cuando dichos hosts están en proceso de recepción, el tráfico se transporta en la

VLAN azul, que es la VLAN principal.

Los puertos donde se conectan los routers y los firewalls son puertos promiscuos porque pueden reenviar el tráfico que proviene de todas las VLAN secundarias definidas en el mapping y la VLAN principal. Los puertos conectados a cada host pueden reenviar solamente el tráfico que proviene de la VLAN principal y la VLAN secundaria configurada en ese puerto.

El gráfico representa las VLAN privadas como diversos conductos que se conectan a los routers y los hosts: el conducto que agrupa a todas las otras VLAN es la VLAN principal (azul), y el tráfico en las VLAN azules fluye de los routers a los hosts. Los conductos internos a la VLAN principal son las VLAN secundarias, y el tráfico viaja en esos conductos desde los hosts hacia el router.

Tal como ilustra la imagen, una VLAN primaria puede agrupar una o más VLAN secundarias.

Más arriba en este documento afirmamos que las PVLAN contribuyen a reafirmar el modelo de confianza adecuado simplemente al garantizar la segregación de los hosts dentro de un segmento común. Ahora que conoce más acerca de las VLAN privadas, veamos como se puede implementar en nuestro escenario inicial DMZ. No se supone que los servidores se comuniquen entre sí, pero necesitan comunicarse con el firewall o router al cual están conectados. En este caso, los servidores deben estar conectados a puertos aislados mientras los routers y los firewall se conectan a puertos promiscuos. Al hacer esto, si uno de los servidores se ve afectado, el intruso no podrá utilizar el mismo servidor para originar un ataque a otro servidor dentro del mismo segmento. El switch descartará cualquier paquete a velocidad de cable, sin ninguna penalidad de rendimiento.

Otra observación importante es que este tipo de control puede implementarse solamente en el dispositivo L2 ya que todos los servidores pertenecen a la misma subred. Los firewall o los routers nada pueden hacer ya que los servidores intentarán comunicarse directamente. Otra opción es dedicar un puerto de firewall por servidor, pero esto puede ser costoso, difícil de implementar y no puede ampliarse.

En una sección posterior, describimos en detalle algunos otros escenarios típicos en los cuales puede utilizar esta característica.

Lista de control de acceso de VLAN

Están disponibles las VACL en la serie Catalyst 6000 que corre CatOS 5.3 o posterior.

Las VACL pueden configurarse en un Catalyst 6500 en L2 sin necesidad de tener un router (sólo necesita una Tarjeta de función de política (PFC)). Se exigen a velocidad de cable por lo que el rendimiento no se ve afectado al configurar las VACL en un Catalyst 6500. Como la búsqueda de VACL se realiza en hardware, independientemente del tamaño de la lista de acceso, la velocidad de reenvío permanece igual.

Las VACL se mapean por separado a las VLAN primarias y secundarias. Tener una VACL configurada en una VLAN secundaria permite el filtrar del tráfico originado por los hosts principales sin tocar el tráfico generado por los routers o los firewalls.

Al combinar las VACL y las VLAN Privadas es posible filtrar tráfico en función de la dirección del tráfico mismo. Por ejemplo, si dos routers están conectados al mismo segmento como algunos hosts (los servidores, por ejemplo), las VACL se pueden configurar en las VLAN secundarias de forma que sólo se filtre el tráfico que generan los hosts, mientras que el tráfico que se intercambia

entre los routers no se modifique.

Las VACL se pueden instrumentar con facilidad para imponer el modelo de confianza adecuado. Analicemos nuestro caso de DMZ. Se supone que los servidores en DMZ solamente suministran conexiones de entrada y no se espera que inicien conexiones con el mundo exterior. Es posible aplicar un VACL a su VLAN secundaria a fin de controlar el tráfico que egresa de estos servidores. Es importante tener en cuenta que al utilizar VACL, el tráfico se coloca en hardware para que no tenga un impacto en la CPU del router o del switch. Incluso en caso de que uno de los servidores se encuentre involucrado en un ataque de Negación de Servicio (DDoS) como origen, el switch descartará todo el tráfico ilegítimo a velocidad de cable, sin afectar el rendimiento. Filtros similares pueden aplicarse en el router o el firewall donde se conectan los servidores, pero esta acción generalmente afecta de forma significativa el rendimiento.

Las ACL basadas en MAC no funcionan bien con el tráfico IP, por lo que se recomiendanVACL para controlar / realizar un seguimiento de las PVLAN.

Limitaciones conocidas de VACL y PVLAN

Cuando configure el filtro con VACL, debe tener cuidado con respecto al manejo de fragmentos en la PFC, que la configuración esté ajustada de acuerdo con la especificación del hardware.

Dado el diseño de hardware del PFC del Supervisor 1 del Catalyst 6500, es mejor impedir explícitamente los fragmentos icmp. El motivo es que el hardware no distingue entre los fragmentos y la respuesta de eco del Protocolo de mensajes de control de Internet (ICMP) y, como opción predeterminada, el hardware está programado para permitir explícitamente los fragmentos. Así que si quiere evitar que los paquetes de respuesta de eco abandonen los servidores, debe configurar esto de forma explícita mediante la línea deny icmp any any fragment. Las configuraciones de este documento tienen en cuenta este hecho.

Una limitación de seguridad muy conocida de las PVLAN es la posibilidad de que un router envíe tráfico desde la misma subred de la cual vino. Un router puede rutear tráfico a través de puertos aislados, con lo cual evita ser afectado por las PVLAN. Esta limitación se debe al hecho de que las PVLAN constituyen una herramienta que ofrece aislamiento en L2, no en la Capa 3 (L3).

El Reenvío de Trayecto Inverso Unicast (uRPF) no funciona bien con los puertos de host PVLAN, por lo que el uRPF no se debe utilizar junto con la PVLAN.

Este problema tiene solución,que consiste en configurar la VACL en las VLAN principales. El caso práctico proporciona las VACL que necesitan ser configuradas en la VLAN principal para disminuir el tráfico originado por la misma subred y el enrutado de regreso a la misma subred.

En algunas tarjetas de línea, la configuración de mapeos PVLAN / mapas / puertos troncales está sujeta a algunas restricciones en las que los mapeos PVLAN múltiples tienen que pertenecer a diferentes circuitos integrados de aplicación específica de puertos (ASIC) para que sean configurados. Esas restricciones se eliminan en el nuevo puerto Coil3 del circuito integrado específico de la aplicación (ASIC). Para estos detalles, consulte la documentación más reciente del switch Catalyst sobre la configuración del software.

Estudios de casos de ejemplo

La siguiente sección describe tres casos de estudios que creemos son representativos en la

mayoría de las implementaciones y brindan detalles relacionados a la implementación de seguridad del las PVLAN y las VACL.

Estos escenarios son:

- Transferencia por DMZ
- DMZ (zona desmilitarizada) externa
- Concentrador VPN Paralelo al Firewall

Transferencia por DMZ

Este es uno de los escenarios más comunes. En este ejemplo, el DMZ se implementa como área de tránsito entre dos routers firewall, como se ilustra en la siguiente imagen.

Figura 2: Transferencia por DMZ

En este ejemplo, se supone que tanto los usuarios internos como externos pueden acceder a los servidores DMZ, pero no necesitan comunicarse. En algunos casos, los servidores DMZ necesitan abrir algún tipo de conexión a un host interno. Al mismo tiempo, se supone que los clientes internos pueden acceder a Internet sin restricciones. Un buen ejemplo es el de los servidores Web en la DMZ, que necesitan comunicarse con un servidor de bases de datos ubicado en la red interna, y en el que los clientes internos pueden acceder a Internet.

El firewall externo se configura para permitir las conexiones entrantes al servidor ubicado en el DMZ, pero en general no se aplican filtros o restricciones al tráfico saliente, particularmente al tráfico originado en el DMZ. Como se mencionó más arriba en este documento, este hecho puede facilitar potencialmente la actividad de un atacante por dos razones: la primera, cuando uno de los hosts de DMZ se vea afectado, el resto de los hosts de DMZ se expone; la segunda razón es que un atacante puede aprovechar fácilmente una conexión saliente.

Como los servidores DMZ no necesitan comunicarse, se recomienda que estén aislados en la L2. Los puertos de servidores serán definidos como puertos aislados PVLAN, mientras que los puertos que conectan los dos firewalls serán definidos como promiscuos. Definir una VLAN primaria para los firewalls y una VLAN secundaria para los servidores DMZ lo logrará.

Se usarán VACL para controlar el tráfico originado en el DMZ. Esto impedirá que un atacante pueda abrir una conexión saliente de forma ilegítima. Es importante tener en cuenta que los servidores DMZ no sólo deberán responder al tráfico correspondiente a las sesiones de cliente, sino también necesitarán algunos servicios adicionales, tales como detección de trayecto del Sistema de Nombres del Dominio (DN) y unidad máxima de transmisión (MTU) (MTU). Por lo tanto, la ACL debe permitir todos los servicios que necesitan los servidores DMZ.

Prueba de transferencia por DMZ

En nuestra plataforma de ensayo, implementamos un segmento DMZ con dos routers configurados como servidores de plataforma de ensayo, servidor_dmz1 y servidor_dmz2. Se supone que se accede a estos servidores tanto desde afuera como desde dentro de los clientes y todas las conexiones http se autentican utilizando un servidor RADIUS (CiscoSecure ACS para UNIX). Tanto el router interno como el externo están configurados como firewalls de filtrado de paquetes. La siguiente imagen ilustra la plataforma de ensayo banco, incluido el esquema de direccionamiento usado.

Figura 3: Base de prueba de DMZ de transferencia

La lista que se muestra a continuación muestra los pasos esenciales de configuración de las PVLAN. El Catalyst 6500 se utiliza como el switch L2 en la DMZ.

- Server_dmz_1 está conectado al puerto 3/9
- Server_dmz_2 está conectado al puerto 3/10
- El router interno está conectado al puerto 3/34
- El router externo está conectado al puerto 3/35

Elegimos las siguientes VLAN:

- 41 es la VLAN primaria
- 42 es la VLAN aislada

Configuración de la VLAN Privada

La siguiente configuración establece las PVLAN en los puertos involucrados.

```
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
```

Configuración VACL en la VLAN primaria

Esta sección es fundamental para mejorar la seguridad en el DMZ. Según lo descrito en las limitaciones conocidas de la sección de VACL y PVLAN, incluso si los servidores pertenecen a dos VLAN secundarias diferentes o la misma VLAN aislada, aún existe la posibilidad de que un atacante haga que se comuniquen. Si los servidores tratan de comunicarse directamente, no podrán hacerlo en L2 por motivo de las PVLAN. Si los servidores son comprometidos y luego configurados por un intruso de manera tal que el tráfico para la misma subred sea enviado al router, éste enviará el tráfico de vuelta en la misma subred y así, rechazará el propósito de las

PVLAN.

Por lo tanto, un VACL necesita ser configurado en el VLAN principal (el VLA N que lleva el tráfico del Routers) con las directivas siguientes:

- Permitir el tráfico cuya IP de origen es la IP del router
- Negar el tráfico con los IP de origen y de destino que constituyen la subred DMZ
- Permitir todo el resto del tráfico

```
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
```

Esa ACL no afectará el tráfico generado por los servidores; impedirá solamente que los routers ruteen el tráfico que proviene de los servidores a la misma VLAN. Los primeros dos enunciados permiten que los routers envíen los mensajes tales como icmp redirect o icmp unreachable to the servers.

Configuración VACL en la VLAN secundaria

Los siguientes registros de configuración se utilizan para demostrar cómo se configura una VACL para filtrar el tráfico que generan los servidores. Al configurar esta VACL, el objetivo es lograr lo siguiente:

- Permita realizar ping desde los servidores (permita el eco).
- Impida que las respuestas de eco dejen los servidores
- Permita las conexiones HTTP originadas del exterior
- Permita la autenticación de RADIUS (puerto 1645 UDP) y el tráfico de la contabilidad (puerto 1646 UDP)
- Permita el tráfico DNS (puerto UDP 53)

Deseamos evitar todo el resto del tráfico.

Con respecto a la fragmentación, suponemos lo siguiente en el segmento del servidor:

- Los servidores no generarán tráfico fragmentado
- Los servidores deben recibir tráfico fragmentado

Dado el diseño del hardware de la PFC del supervisor 1 del Catalyst 6500, es mejor negar explícitamente los fragmentos icmp. El motivo es que el hardware considera que los fragmentos ICMP y la respuesta de eco son iguales y el hardware está programado predeterminadamente para permitir explícitamente los fragmentos. Por lo tanto, si desea impedir que los paquetes de respuesta de eco abandonen los servidores, debe configurarlo explícitamente mediante la línea 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
```

Prueba de la configuración

La siguiente salida fue capturada cuando se configuraron las PVLAN pero aún no se habían aplicado las VACL. Esta prueba muestra que desde el router externo el usuario puede **realizar un ping del** router interno y los 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
```

El siguiente ejemplo muestra que podemos hacer ping desde los servidores a la red externa, a la gateway predeterminada, pero no a los servidores que pertenecen a la misma VLAN secundaria.

```
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)
```

Después de mapear las VACL, el ping del router externo ya no tendrá éxito:

```
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)
```

El siguiente ejemplo muestra cómo el servidor recibe las solicitudes de HTTP GET de la red 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 (zona desmilitarizada) externa

Es probable que el escenario de DMZ externo sea la implementación más ampliamente aceptada e instrumentada. Se implementa un DMZ externo mediante una o más interfaces de un firewall, según muestra la siguiente figura.

Figura 4: DMZ (zona desmilitarizada) externa

Por lo general, los requisitos para las DMZ suelen ser los mismos independientemente de la implementación del diseño. Como en el caso anterior, se supone que los clientes externos pueden acceder a los servidores DMZ también se puede acceder desde la red interna. Los servidores DMZ necesitarán, en algún momento, acceso a algunos recursos internos y no deben comunicarse entre ellos. Al mismo tiempo, no debe iniciarse tráfico desde la DMZ a Internet; estos servidores DMZ deben contestar solamente con el tráfico correspondiente a las conexiones entrantes.

Como en el caso práctico anterior, el primer paso para la configuración consiste en la realización del aislamiento en la L2 mediante las PVLAN, y en garantizar que servidores DMZ no puedan comunicarse cuando los hosts internos y externos pueden acceder a ellos. Esto se implementa configurando los servidores en una VLAN secundaria con puertos aislados. El firewall se debe definir en una VLAN principal con un puerto promiscuo. El firewall será el único dispositivo dentro de esta VLAN principal.

El segundo paso es definir las ACL para controlar el tráfico originado en la DMZ. Al definir estas ACL debemos asegurarnos de que solamente se permita el tráfico necesario.

Prueba de DMZ externa

La imagen proporcionada a continuación muestra la implementación de la plataforma de ensayo para este caso práctico, donde hemos utilizado un firewall PIX con una tercera interfaz para el DMZ. El mismo conjunto de routers se utiliza como servidores Web, y autentican a todas las sesiones HTTP con el mismo servidor RADIUS.

Figura 5: Base de prueba de DMZ externa

Para este escenario sólo adjuntamos los extractos más interesantes de los archivos de configuración, ya que las configuraciones de PVLAN y VACL se han explicado en detalle en el caso práctico anterior.

Configuración de PIX

```
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 ''
```

Configuración RADIUS

Configuración de NAS

```
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 ''
```

Servidor RADIUS CSUX

```
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 ''
```

Configuración de Catalyst

Debe tenerse en cuenta que en esta configuración no existe la necesidad de configurar una VACL en la VLAN principal debido a que el PIX no redirecciona el tráfico de salida por la misma interfaz por la que ingresó. Una VACL, como la descrita en la sección Configuración de VACL en la VLAN principal, sería 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
```

Concentrador VPN Paralelo al Firewall

Al implementar el Acceso a las Redes Privadas Virtuales (VPN), indudablemente uno de los enfoques preferidos es el diseño paralelo (ilustrado en la siguiente imagen). Los clientes en general prefieren este enfoque de diseño ya que es fácil de implementar, con casi ningún impacto en la infraestructura existente, y porque es relativamente fácil de escalar en función de la flexibilidad del dispositivo.

En el enfoque paralelo, el concentrador VPN se conecta con ambos segmentos, el interior y el exterior. Todas las sesiones VPN finalizan en el concentrador sin necesidad de pasar por el firewall. Generalmente, se espera que los clientes VPN tengan acceso irrestricto a la red interna, pero a veces su acceso puede estar limitado a un conjunto de servidores internos (bloque de servidores). Una de las acciones recomendadas es segregar el tráfico VPN del tráfico de Internet habitual, de manera que, por ejemplo, los clientes VPN no puedan acceder a Internet a través del firewall corporativo.

Figura 6: Concentrador VPN Paralelo al Firewall

Prueba de Concentrador VPN en Paralelo al Firewall

En este ejemplo, utilizamos un concentrador VPN 5000, que fue instalado en paralelo a un firewall de PIX. Los dos routers configurados como servidores Web se instalaron en el segmento interno como bloque de servidores internos. Solamente se permite que los clientes VPN accedan a la granja de servidores y el tráfico de Internet debería estar separado del tráfico de VPN (IPSec). La siguiente figura muestra la plataforma de ensayo.

Figura 7: Concentrador VPN paralelo a la Base de Prueba del Firewall

En este escenario tenemos dos áreas importantes de interés:

- El switch interno L2
- El switch externo L2

Los flujos de tráfico para el switch interno L2 se definen según los siguientes enunciados:

- Los clientes VPN cuentan con acceso total a un conjunto de servidores internos predefinido (bloque de servidores)
- Los clientes internos también tienen permitido el acceso al bloque del servidor.
- Los clientes internos poseen acceso ilimitado a Internet
- El tráfico que proviene del concentrador VPN debe aislarse del firewall PIX

Los flujos de tráfico por el switch externo L2 están definidos de la siguiente manera:

- El tráfico proveniente del router debe poder dirigirse al concentrador VPN o al PIX
- El tráfico proveniente de PIX debe ser aislado del proveniente de la VPN

También es posible que el administrador quiera impedir que el tráfico de la red interna llegue a los hosts de VPN; esto se puede lograr mediante VACL configuradas en la VLAN principal (la VACL

filtrará sólo el tráfico que sale del router interno; el resto del tráfico no se verá afectado).

Configuración de PVLAN

Dado que el objetivo principal en este diseño es impedir el paso del tráfico del PIX segregado del tráfico que proviene de los servidores y del VPN Concentrator, configuraremos el PIX en una PVLAN diferente a la PVLAN en la que se configuran los servidores y el VPN Concentrator.

El tráfico que proviene de la red interna debe poder acceder al bloque de servidores, el VPN Concentrator y el PIX. Como consecuencia, el puerto que se conecta a la red interna será un puerto promiscuo.

Los servidores y el concentrador VPN corresponden a la misma VLAN secundaria porque se podrán comunicar entre sí.

En cuanto al switch externo L2, el router que brinda acceso a Internet (que pertenece habitualmente a un Proveedor de Servicios de Internet (ISP)) está conectado con un puerto promiscuo mientras que el VPN Concentrator y el PIX pertenecen a las mismas VLAN aisladas y privadas (de modo que no pueden intercambiar tráfico). Al realizar esto, el tráfico procedente del proveedor de servicio puede tomar la trayectoria hacia el concentrador VPN o la trayectoria hacia PIX. Los concentradores PIX y VPN se encuentran más protegidos porque están aislados.

Configuración PVLAN del 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
```

Configuración PVLAN del switch externo L2

```
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
```

Prueba de la configuración

Este experimento muestra que el router interno puede pasar por el firewall y alcanza el router externo (el router del firewall externo cuya interfaz es 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
```

Este experimento muestra lo siguiente, todo en relación con el servidor 1:

- El servidor 1 puede realizar un ping al router 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
  ```

- El Servidor 1 puede realizar un ping de la 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
```

- El Servidor 1 no puede realizar un ping a la interfaz interna del 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)
```

- El servidor 1 no puede realizar un ping al router interno:`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)
```

La siguiente prueba muestra que se pueden abrir las sesiones HTTP desde la red interna hacia el bloque de servidores.

```
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)
```

El siguiente experimento muestra que el tráfico HTTP de la red VPN puede acceder al bloque de servidores (tenga en cuenta la dirección 10.1.1.1).

```
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)
```

La siguiente es la configuración del concentrador VPN:

```
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)
```

El siguiente comando muestra la lista de usuarios 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
```

Debe señalarse que el gateway predeterminado en los servidores es el router interno 172.16.65.193, que enviará un icmp redireccionado a 172.16.65.203. Esta implementación ocasiona flujos de tráfico no óptimos, porque el host envía el primer paquete de flujo al router y, al recibir la redirección, envía los paquetes siguientes a el gateway más apropiada para manejar el tráfico. Otra alternativa es configurar dos rutas diferentes en los servidores mismos para dirigirse a la VPN para las direcciones 10.x.x.x y a 172.16.65.193 para el resto del tráfico. Si se configura

solamente el gateway predeterminado en los servidores, debemos asegurarnos de que la interfaz del router esté configurada con “ redireccionamiento IP.”

Una de las cosas interesantes que notamos durante las pruebas fue la siguiente: Si intentamos hacer ping en una dirección externa como 198.5.6.1 desde los servidores o desde la VPN, el gateway predeterminada enviará y redirigirá ICMP a 172.16.65.201.

```
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
```

Los servidores o la VPN en este momento enviarán una solicitud de Protocolo de Resolución de Direcciones (ARP) para 172.16.65.201 y no obtendrán respuesta de 201 porque está en otra VLAN secundaria; esto es lo que nos proporciona la PVLAN. En realidad existe una manera simple de sortear esto, que consiste en enviar tráfico a la MAC of. 193 y con el IP de destino 172.16.65.201.

El router .193 enviará de regreso el tráfico a la misma interfaz, pero como la interfaz del router es un puerto promiscuo, el tráfico llegará a 201, cosa que queríamos evitar. Este problema se explicó en la sección Limitaciones conocidas de VACL y PVLAN.

Configuración de VACL

Esta sección es fundamental para mejorar la seguridad del bloque de servidores. Según lo descrito en las limitaciones conocidas de la sección de VACL y PVLAN, incluso si los servidores y el PIX pertenecen a dos VLAN secundaras, diferentes aún existe un método que un atacante puede utilizar para hacer que se comuniquen entre sí. Si intentan comunicarse directamente, no podrán hacerlo debido a las PVLAN. Si los servidores son comprometidos y luego configurados por un intruso de manera tal que el tráfico para la misma subred sea enviado al router, éste enviará el tráfico de vuelta en la misma subred y así, rechazará el propósito de las PVLAN.

Por lo tanto, una VACL debe ser configurada en la VLAN principal (la VLAN que lleva el tráfico de los routers) con las siguientes políticas:

- Permitir el tráfico cuya IP de origen es la IP del router
- Deniegue el tráfico tanto con la IP de origen como con la de destino que son la subred del bloque de servidor
- Permitir todo el resto del tráfico

```
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
```

Este ACL no afectará el tráfico generado por los servidores ni por el PIX; impedirá solamente que los routers ruteen el tráfico que proviene de los servidores a la misma VLAN. Los primeros dos enunciados permiten que los routers envíen mensajes como icmp redirect o icmp unreachable to

the servers.

Identificamos otro flujo de tráfico que el administrador podría desear detener mediante el uso de VACL, y este flujo proviene de la red interna hacia los hosts VPN. Para lograrlo, una VACL se puede mapear a la VLAN principal (41) y combinarse con la 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
```

Prueba de la configuración

Ahora estamos haciendo un ping del host de 10.1.1.1 desde el router .193 (zundapp). Antes de mapear la VACL, el ping es exitoso.

```
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
```

Luego del mapeo de la VACL en la VLAN 41, el mismo ping no será exitoso:

```
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
```

Sin embargo, todavía se puede hacer una prueba de ping al router externo.

```
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
```

Información Relacionada

- Configuración de las listas de control de acceso - Documentación de Catalyst 6000.
- Soporte Técnico - Cisco Systems