Captura de VACL para análisis granular del tráfico con Cisco Catalyst 6000/6500 que ejecuta el software CatOS

Contenido

Introducción

Este documento suministra una configuración de ejemplo para el uso de la característica Capture Port de Lista de Control de Acceso (ACL) de VLAN (VACL) para el análisis del tráfico de la red de una manera más granular. Este documento también indica la ventaja del uso de Capture Port de VACL frente al uso del Switched Port Analyzer (SPAN) basado en VLAN (VSPAN).

Para configurar la función VACL Capture Port en Cisco Catalyst 6000/6500 que ejecuta Cisco IOS® Software, consulte Captura VACL para Análisis Granular del Tráfico con Cisco Catalyst 6000/6500 que Ejecuta Cisco IOS Software.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- LAN virtual: consulte Virtual LANs/VLAN Trunking Protocol (VLAN/VTP) - Introducción para obtener más información.
- Listas de Acceso: Consulte Configuración del Control de Acceso para obtener más información.

Componentes Utilizados

La información de este documento se basa en el Cisco Catalyst 6506 Series Switch que ejecuta Catalyst OS versión 8.1(2).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Productos Relacionados

Esta configuración también se puede utilizar con los Cisco Catalyst 6000 / 6500 Series Switches que ejecutan Catalyst OS versión 6.3 y posteriores.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

SPAN basado en VLAN

SPAN copia el tráfico de uno o más puertos de origen en cualquier VLAN o de una o más VLAN a un puerto de destino para su análisis. El SPAN local admite puertos de origen, VLAN de origen y puertos de destino en el mismo switch Catalyst serie 6500.

Un puerto de origen es un puerto monitoreado para el análisis del tráfico de red. Una VLAN de origen es una VLAN supervisada para el análisis del tráfico de red. El SPAN basado en VLAN (VSPAN) analiza el tráfico de red en una o más VLAN. Puede configurar VSPAN como SPAN de ingreso, SPAN de egreso o ambos. Todos los puertos en las VLAN de origen se convierten en los puertos de origen operativos para la sesión VSPAN. Los puertos de destino, si pertenecen a alguna de las VLAN de origen administrativas, se excluyen del origen operativo. Si agrega o quita los puertos de las VLAN de origen administrativas, los orígenes operativos se modifican en consecuencia.

Pautas para las sesiones de VSPAN:

- Los puertos trunk se incluyen como los puertos de origen para las sesiones VSPAN, pero solamente las VLAN que están en la lista de origen Admin se monitorean si estas VLAN están activas para el trunk.
- Para las sesiones de VSPAN con SPAN de ingreso y de egreso configurado, el sistema funciona según el tipo de Supervisor Engine que tiene:WS-X6K-SUP1A-PFC, WS-X6K-SUP1A-MSFC, WS-X6K-S1A-MSFC2, WS-X6K-S2-PFC2, WS-X6K-S1A-MSFC2, WS-

SUP720, WS-SUP32-GE-3B: dos paquetes son reenviados por Puerto de destino SPAN si los paquetes se conmutan en la misma VLAN.WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE: el puerto de destino de SPAN sólo reenvía un paquete.

- Un puerto dentro de la banda no se incluye como fuente operativa para las sesiones VSPAN.
- Cuando se borra una VLAN, se elimina de la lista de origen para las sesiones VSPAN.
- Una sesión VSPAN se inhabilita si la lista de VLAN de origen de administración está vacía.
- No se permiten las VLAN inactivas para la configuración de VSPAN.
- Una sesión VSPAN se hace inactiva si alguna de las VLAN de origen se convierte en las VLAN RSPAN.

Consulte Características de la VLAN de Origen para obtener más información sobre las VLAN de Origen.

ACL de VLAN

Las VACL pueden controlar todo el tráfico. Puede configurar las VACL en el switch para que se apliquen a todos los paquetes que se rutean dentro o fuera de una VLAN o que se puentean dentro de una VLAN. Las VACL son estrictamente para el filtrado de paquetes de seguridad y el redireccionamiento del tráfico a puertos de switch físicos específicos. A diferencia de las ACL de Cisco IOS, las VACL no se definen por dirección (entrada o salida).

Puede configurar las VACL en las direcciones de Capa 3 para IP e IPX. Todos los demás protocolos son de acceso controlado a través de las direcciones MAC y EtherType mediante las VACL MAC. El tráfico IP y el tráfico IPX no son controlados por las VACL MAC. Todos los demás tipos de tráfico (AppleTalk, DECnet, etc.) se clasifican como tráfico MAC. Las VACL MAC se utilizan para controlar este tráfico.

ACE admitidas en VACL

VACL contiene una lista ordenada de entradas de control de acceso (ACE). Cada VACL puede contener ACE de un solo tipo. Cada ACE contiene un número de campos que coinciden con el contenido de un paquete. Cada campo puede tener una máscara de bits asociada para indicar qué bits son relevantes. Se asocia una acción a cada ACE que describe lo que el sistema debe hacer con el paquete cuando se produce una coincidencia. La acción depende de la función. Los switches Catalyst serie 6500 admiten tres tipos de ACE en el hardware:

- IP ACE
- ACE IPX
- ACE Ethernet

Esta tabla enumera los parámetros que se asocian con cada tipo ACE:

Tipo ACE	¿TCP o UDP	ICMP	Otra IP	IPX	Ethernet
Parámetros de capa 4	Puerto de Origen	-	-	-	-
	Operador de puerto de origen	-	-	-	-
	Puerto de Destino	-	-	-	-
	Operador	Código	-	-	-

	de puerto de destino	ICMP			
	N/A	Tipo de ICMP	N/A	-	-
Parámetros de capa 3	Byte ToS IP	Byte ToS IP	Byte ToS IP	-	-
	Dirección IP de Origen	Dirección IP de Origen	Dirección IP de Origen	Red de Origen IPX	-
	Dirección IP de destino	Dirección IP de destino	Dirección IP de destino	Red de destino IP	-
	-	-	-	Nodo de destino IP	-
	¿TCP o UDP	ICMP	Otro protocolo	Tipo de paquete IPX	-
Parámetros de capa 2	-	-	-	-	EtherType
	-	-	-	-	Dirección de origen Ethernet
	-	-	-	-	Dirección de destino Ethernet

Ventajas del uso de VACL sobre el uso de VSPAN

Hay varias limitaciones en el uso de VSPAN para el análisis del tráfico:

- Se captura todo el tráfico de Capa 2 que fluye en una VLAN. Esto aumenta la cantidad de datos que se analizarán.
- El número de sesiones SPAN que se pueden configurar en los Catalyst 6500 Series Switches es limitado. Refiérase a Resumen de Funciones y Limitaciones para obtener más información.
- Un puerto de destino recibe copias del tráfico enviado y recibido para todos los puertos de origen monitoreados. Si un puerto de destino tiene exceso de suscriptores, puede congestionarse. Esta congestión puede afectar al reenvío de tráfico en uno o más de los puertos de origen.

La función VACL Capture Port puede ayudar a superar algunas de estas limitaciones. Las VACL no están diseñadas principalmente para monitorear el tráfico. Sin embargo, con una amplia gama de funciones para clasificar el tráfico, se introdujo la función Capture Port de modo que el análisis del tráfico de la red pueda volverse mucho más sencillo. Estas son las ventajas del uso del puerto

de captura VACL sobre VSPAN:

- Análisis de tráfico granularLas VACL pueden coincidir en función de la dirección IP de origen, la dirección IP de destino, el tipo de protocolo de capa 4, los puertos de capa 4 de origen y de destino y otra información. Esta capacidad hace que las VACL sean muy útiles para la identificación y el filtrado granulares del tráfico.
- Número de sesionesLas VACL se aplican en el hardware. El número de ACE que se pueden crear depende del TCAM disponible en los switches.
- Sobresuscripción al puerto de destinoLa identificación granular del tráfico reduce el número de tramas que se reenviarán al puerto de destino y, por lo tanto, minimiza la probabilidad de su exceso de suscripción.
- RendimientoLas VACL se aplican en el hardware. No hay penalización del rendimiento para la aplicación de VACL a una VLAN en los switches Catalyst de Cisco serie 6500.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

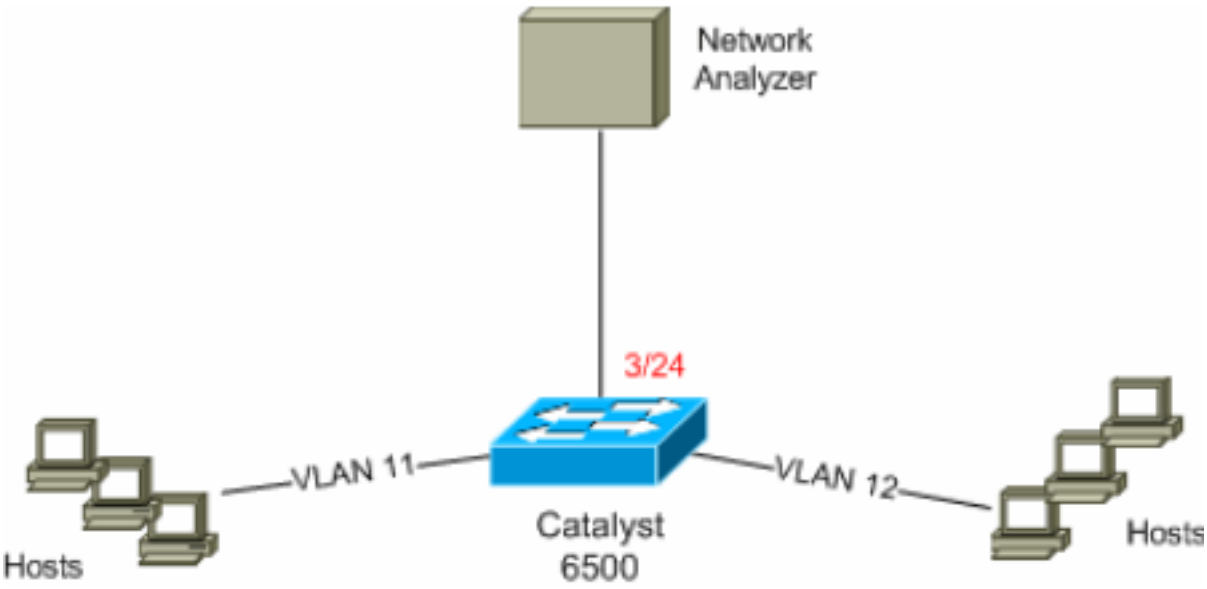
En este documento, se utilizan estas configuraciones:

- Configuración con SPAN basado en VLAN
- Configuración con VACL

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración con SPAN basado en VLAN

Este ejemplo de configuración enumera los pasos necesarios para capturar todo el tráfico de

Capa 2 que fluye en VLAN 11 y VLAN 12 y enviarlo al dispositivo del Analizador de Red.

1. Especifique el tráfico interesante.En este ejemplo, es el tráfico el que fluye en VLAN 100 y VLAN 200.

```
6K-CatOS> (enable) set span 11-12 3/24
!--- where 11-12 specifies the range of source VLANs and 3/24 specify the destination port.

2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span session inactive for des
tination port 3/24

Destination     : Port 3/24
Admin Source    : VLAN 11-12
Oper Source     : Port 3/11-12,16/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active

6K-CatOS> (enable) 2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span sessi
on active for destination port 3/24
```

   Con esto, todo el tráfico de Capa 2 que pertenece a VLAN 11 y VLAN 12 se copia y se envía al puerto 3/24.
2. Verifique su configuración de SPAN con el comando **show span all**.

```
6K-CatOS> (enable) show span all

Destination     : Port 3/24
Admin Source    : VLAN 11-12
Oper Source     : Port 3/11-12,16/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active


Total local span sessions:  1

No remote span session configured
6K-CatOS> (enable)
```

Configuración con VACL

En este ejemplo de configuración, hay varios requisitos del administrador de red:

- El tráfico HTTP de un rango de hosts (10.12.12.128/25) en VLAN 12 a un servidor específico (10.11.11.100) en VLAN 11 debe capturarse.
- El tráfico de protocolo de datagramas de usuario de multidifusión (UDP) en la dirección de transmisión destinada a la dirección de grupo 239.0.0.100 debe capturarse desde la VLAN 11.

1. Defina el tráfico interesante mediante las ACL de seguridad. Recuerde mencionar la palabra clave **capture** para todas las ACE definidas.

```
6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit tcp 10.12.12.128 0.0.0.127 host
10.11.11.100 eq www capture
!--- Command wrapped to the second line. HttpUdp_Acl editbuffer modified. Use 'commit'
```

```
command to apply changes. 6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit udp any
host 239.0.0.100 capture
HttpUdp_Acl editbuffer modified. Use 'commit' command to apply changes.
```

2. Verifique si la configuración ACE es correcta y está en el orden correcto.

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
-------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Not Committed
6K-CatOS> (enable)
```

3. Comunique la ACL al hardware.

```
6K-CatOS> (enable) commit security acl HttpUdp_Acl
ACL commit in progress.

ACL 'HttpUdp_Acl' successfully committed.
6K-CatOS> (enable)
```

4. Verifique el estado de la ACL.

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
-------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Committed
6K-CatOS> (enable)
```

5. Aplique el mapa de acceso de VLAN a las VLAN apropiadas.

```
6K-CatOS> (enable) set security acl map HttpUdp_Acl ?
  <vlans>                    Vlan(s) to be mapped to ACL
6K-CatOS> (enable) set security acl map HttpUdp_Acl 11
Mapping in progress.

ACL HttpUdp_Acl successfully mapped to VLAN 11.
6K-CatOS> (enable)
```

6. Verifique la asignación de ACL a VLAN.

```
6K-CatOS> (enable) show security acl map HttpUdp_Acl
ACL HttpUdp_Acl is mapped to VLANs:
11
6K-CatOS> (enable)
```

7. Configure el puerto de captura.

```
6K-CatOS> (enable) set vlan 11 3/24
VLAN  Mod/Ports
---- ----------------------
11    3/11,3/24
6K-CatOS> (enable)


6K-CatOS> (enable) set security acl capture-ports 3/24
Successfully set 3/24 to capture ACL traffic.
6K-CatOS> (enable)
```

Nota: Si una ACL se mapea a varias VLAN, el puerto de captura debe configurarse en todas esas VLAN. Para hacer que el puerto de captura permita varias VLAN, configure el puerto como trunk y permita solamente las VLAN asignadas a la ACL. Por ejemplo, si la ACL está asignada a las VLAN 11 y 12, complete la configuración.

```
6K-CatOS> (enable) clear trunk 3/24 1-10,13-1005,1025-4094
6K-CatOS> (enable) set trunk 3/24 on dot1q 11-12
6K-CatOS> (enable) set security acl capture-ports 3/24
```

8. Verifique la configuración del puerto de captura.

```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
```

```
6K-CatOS> (enable)
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show security acl info**—Muestra el contenido de la VACL configurada actualmente o comprometida por última vez con NVRAM y hardware.
```
6K-CatOS> (enable) show security acl info HttpUdp_Acl
set security acl ip HttpUdp_Acl
---------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
6K-CatOS> (enable)
```
- **show security acl map**—Muestra la asignación de ACL a VLAN o de ACL a puerto para una ACL, puerto o VLAN específicos.
```
6K-CatOS> (enable) show security acl map all
ACL Name                        Type Vlans
------------------------------- ---- -----
HttpUdp_Acl                        IP   11
6K-CatOS> (enable)
```
- **show security acl capture-ports**: muestra la lista de puertos de captura.
```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Captura de VACL para análisis granular del tráfico con Cisco Catalyst 6000/6500 que ejecuta Cisco IOS Software
- Configuración del control de acceso: Guía de configuración del software Catalyst serie 6500, 8.6
- Páginas de Soporte de Productos de LAN
- Página de Soporte de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems