Captura de VACL para análisis granular del tráfico con Cisco Catalyst 6000/6500 que ejecuta Cisco IOS Software

Contenido

Introducción

Este documento suministra una configuración de ejemplo para el uso de la función 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 explica la ventaja del uso de Capture Port de VACL frente al uso de SPAN basado en VLAN (VSPAN).

Para configurar la función Captura-puerto VACL en Cisco Catalyst 6000/6500 que ejecuta el software Catalyst OS, consulte Captura VACL para Análisis Granular del Tráfico con Cisco Catalyst 6000/6500 que Ejecuta el Software CatOS.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware. Switch Catalyst de Cisco serie 6506 que ejecuta Cisco IOS® Software Release 12.2(18)SXF8.

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 Cisco IOS Software Release 12.1(13)E y posteriores.

Convenciones

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

Antecedentes

SPAN basado en VLAN

SPAN (analizador de puerto conmutado) 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.

Una VLAN de origen es una VLAN supervisada para el análisis del tráfico de red. El SPAN (VSPAN) basado en VLAN utiliza una VLAN como origen de SPAN. Todos los puertos en las VLAN de origen se convierten en puertos de origen. Un puerto de origen es un puerto monitoreado para el análisis del tráfico de red. Los puertos troncales se pueden configurar como puertos de origen y mezclarse con puertos de origen no troncales, pero SPAN no copia la encapsulación de un puerto troncal de origen.

Para las sesiones VSPAN con entrada y salida configuradas, se reenvían dos paquetes desde el puerto de destino si los paquetes se conmutan en la misma VLAN (uno como tráfico de ingreso desde el puerto de ingreso y otro como tráfico de egreso desde el puerto de egreso).

VSPAN sólo monitorea el tráfico que sale o entra en los puertos de Capa 2 en la VLAN.

- Si configura una VLAN como un origen de ingreso y el tráfico se enruta a la VLAN monitoreada, el tráfico ruteado no se monitorea porque nunca aparece como tráfico de

ingreso que ingresa a un puerto de Capa 2 en la VLAN.
- Si configura una VLAN como un origen de egreso y el tráfico se enruta fuera de la VLAN monitoreada, el tráfico ruteado no se monitorea porque nunca aparece como tráfico de egreso que sale de un puerto de Capa 2 en la VLAN.

Para obtener más información sobre las VLAN de origen, consulte Características de la VLAN de Origen.

ACL de VLAN

Las VACL pueden proporcionar control de acceso para todos los paquetes que se puentean dentro de una VLAN o que se enrutan hacia o desde una VLAN o una interfaz WAN para la captura de VACL. A diferencia de las ACL estándar o extendidas de Cisco IOS que se configuran solamente en las interfaces del router y se aplican sólo en los paquetes ruteados, las VACL se aplican a todos los paquetes y se pueden aplicar a cualquier VLAN o interfaz WAN. Las VACL se procesan en hardware. Las VACL utilizan ACL de Cisco IOS. Las VACL ignoran cualquier campo de ACL de Cisco IOS que no se admita en el hardware.

Puede configurar las VACL para el tráfico IP, IPX y de capa MAC. Las VACL aplicadas a las interfaces WAN soportan solamente el tráfico IP para la captura de VACL.

Cuando configura una VACL y la aplica a una VLAN, todos los paquetes que ingresan a la VLAN se comprueban con esta VACL. Si aplica una VACL a la VLAN y una ACL a una interfaz ruteada en la VLAN, primero se verifica un paquete que entra en la VLAN con la VACL y, si se permite, se verifica con la ACL de entrada antes de que la interfaz ruteada lo maneje. Cuando el paquete se rutea a otra VLAN, primero se verifica con la ACL de salida que se aplica a la interfaz ruteada y, si se permite, se aplica la VACL configurada para la VLAN de destino. Si se configura una VACL para un tipo de paquete y un paquete de ese tipo no coincide con la VACL, la acción predeterminada es deny. Estas son las pautas para la opción de captura en VACL.

- El puerto de captura no puede ser un puerto ATM.
- El puerto de captura debe estar en el estado de reenvío del árbol de expansión para la VLAN.
- El switch no tiene ninguna restricción sobre el número de puertos de captura.
- El puerto de captura captura sólo los paquetes permitidos por la ACL configurada.
- Los puertos de captura sólo transmiten el tráfico que pertenece a la VLAN del puerto de captura. Configure el puerto de captura como un trunk que transporta las VLAN necesarias para capturar el tráfico que va a muchas VLAN.

Precaución: La combinación incorrecta de ACL puede interrumpir el flujo de tráfico. Tenga más cuidado al configurar las ACL en su dispositivo.

Nota: VACL no se soporta con IPv6 en un Catalyst 6000 Series Switch. En otras palabras, la redirección de VLAN ACL e IPv6 no son compatibles, por lo que no se puede utilizar ACL para que coincida con el tráfico IPv6.

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 Límites de Sesión de SPAN Local y RSPAN 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, pero, con una amplia gama de capacidades para clasificar el tráfico, se introdujo la función Capture Port para que el análisis del tráfico de red pueda volverse mucho más simple. 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 hardware; el número de entradas de control de acceso (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 hardware; no hay penalización del rendimiento para la aplicación de VACL a una VLAN en los switches Catalyst de Cisco serie 6500

Configurar

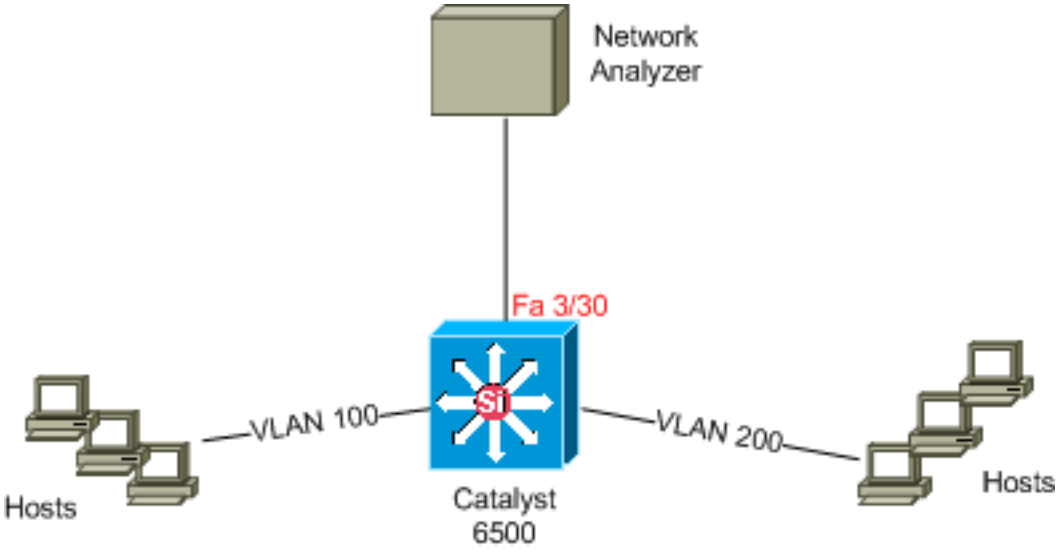
En esta sección encontrará la información para configurar las funciones descritas en este documento.

- Configuración con SPAN basado en VLAN
- Configuración con VACL

Nota: Use la Command Lookup Tool (sólo clientes registrados) para obtener más información sobre los comandos utilizados en este documento.

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 100 y VLAN 200 y enviarlos al dispositivo Analizador de Red.

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

```
Cat6K-IOS#conf t
Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200 ?
  ,     Specify another range of VLANs
  -     Specify a range of VLANs
  both  Monitor received and transmitted traffic
  rx    Monitor received traffic only
  tx    Monitor transmitted traffic only
  <cr>

 !--- Default is to monitor both received and transmitted traffic

Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200
Cat6K-IOS(config)#
```

2. Especifique el puerto de destino para el tráfico capturado.

```
Cat6K-IOS(config)#monitor session 50 destination interface Fa3/30
Cat6K-IOS(config)#
```

Con esto, todo el tráfico de capa 2 que pertenece a VLAN 100 y VLAN 200 se copia y se envía al puerto Fa3/30. Si el puerto de destino es parte de la misma VLAN cuyo tráfico se monitorea, el tráfico que sale del puerto de destino no se captura.

Verifique su configuración SPAN con el comando **show monitor**.

```
Cat6K-IOS#show monitor detail
Session 50
----------
Type              : Local Session
Source Ports      :
    RX Only       : None
    TX Only       : None
    Both          : None
Source VLANs      :
    RX Only       : None
    TX Only       : None
```

```
    Both          : 100,200
Source RSPAN VLAN : None
Destination Ports : Fa3/30
Filter VLANs      : None
Dest RSPAN VLAN   : None
```

Configuración con VACL

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

- El tráfico HTTP de un rango de hosts (10.20.20.128/25) en VLAN 200 a un servidor específico (10.10.10.101) en VLAN 100 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 100.

1. Defina el tráfico interesante que se va a capturar y enviar al análisis.
```
Cat6K-IOS(config)#ip access-list extended HTTP_UDP_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit tcp 10.20.20.128 0.0.0.127 host 10.10.10.101 eq www
Cat6K-IOS(config-ext-nacl)#permit udp any host 239.0.0.100
Cat6K-IOS(config-ext-nacl)#exit
```
2. Defina una ACL de umberlla para asignar el resto del tráfico.
```
Cat6K-IOS(config)#ip access-list extended ALL_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit ip any any
Cat6K-IOS(config-ext-nacl)#exit
```
3. Defina el mapa de acceso de VLAN.
```
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 10
Cat6K-IOS(config-access-map)#match ip address HTTP_UDP_TRAFFIC
Cat6K-IOS(config-access-map)#action forward capture
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 20
Cat6K-IOS(config-access-map)#match ip address ALL_TRAFFIC
Cat6K-IOS(config-access-map)#action forward
Cat6K-IOS(config-access-map)#exit
```
4. Aplique el mapa de acceso de VLAN a las VLAN apropiadas.
```
Cat6K-IOS(config)#vlan filter HTTP_UDP_MAP vlan-list 100
!--- Here 100 is the ID of VLAN on which the VACL is applied.
```
5. Configure el puerto de captura.
```
Cat6K-IOS(config)#int fa3/30
Cat6K-IOS(config-if)#switchport capture allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this po
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  remove  remove VLANs from the current list

Cat6K-IOS(config-if)#switchport capture allowed vlan 100
Cat6K-IOS(config-if)#switchport capture
Cat6K-IOS(config-if)#exit
```

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 vlan access-map**: muestra el contenido de los mapas de acceso de VLAN.

```
Cat6K-IOS#show vlan access-map HTTP_UDP_MAP
Vlan access-map "HTTP_UDP_MAP"  10
        match: ip address HTTP_UDP_TRAFFIC
        action: forward capture
Vlan access-map "HTTP_UDP_MAP"  20
        match: ip address ALL_TRAFFIC
        action: forward
```

- **show vlan filter** — Muestra información sobre los filtros VLAN.

```
Cat6K-IOS#show vlan filter
VLAN Map HTTP_UDP_MAP:
        Configured on VLANs:  100
            Active on VLANs:  100
```

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 el software CatOS
- Compatibilidad con switches Catalyst de Cisco serie 6500
- Soporte de Producto de LAN
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems