Captura VACL para la análisis del tráfico granular con el Cisco Catalyst 6000/6500 software CatOS corriente

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 captura VACL vire la característica hacia el lado de babor en eso del Cisco Catalyst 6000/6500 funciona con el software de Cisco IOS®, refieren a la captura VACL para la análisis del tráfico granular con el Cisco Catalyst 6000/6500 Cisco IOS Software corriente.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- LAN virtual — Refiera al LAN virtuales/VLAN Trunking Protocol (VLANs/VTP) - Introducción para más información.
- Listas de acceso — Refiera a configurar el control de acceso para más información.

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con el Cisco Catalyst 6000/6500 Series Switch que funciona con la versión de OS de Catalyst 6.3 y posterior.

Convenciones

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

Antecedentes

SPAN VLAN basado

ATRAVIESE las copias trafican de uno o más puertos de origen en cualquier VLA N o de uno o más VLA N a un puerto destino para el análisis. El SPAN local soporta los puertos de origen, los VLA N de la fuente, y los puertos destino en el mismo Catalyst 6500 Series Switch.

Un puerto de origen es un puerto monitoreado para el análisis de tráfico de la red. Un VLA N de la fuente es un VLA N monitoreado para el análisis de tráfico de la red. El SPAN VLAN basado (VSPAN) es análisis del tráfico de la red en uno o más VLA N. Usted puede configurar el VSPAN como el SPAN de ingreso, el SPAN de egreso, o ambos. Todos los puertos en los VLA N de la fuente se convierten en los puertos de origen operativos para la sesión VSPAN. Los puertos destino, si pertenecen a los VLA N uces de los de la fuente administrativa, se excluyen de la fuente operativa. Si usted agrega o quita los puertos de los VLA N de la fuente administrativa, las fuentes operativas se modifican por consiguiente.

Guías de consulta para las sesiones VSPAN:

- Los puertos troncales se incluyen como los puertos de origen para las sesiones VSPAN, pero solamente se monitorean los VLA N que están en la lista de Admin Source si estos VLA N son activos para el trunk.
- Para las sesiones VSPAN con el ingreso y el SPAN de egreso configurados, el sistema actúa basado en el tipo de Supervisor Engine que usted 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 remitidos por el puerto destino del SPAN si los paquetes consiguen conmutados en el mismo VLA N.WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE — Solamente un paquete es remitido por el puerto destino del SPAN.

- Un puerto inband no se incluye como Fuente operacional para las sesiones VSPAN.
- Cuando se borra un VLA N, se quita de la lista de origen para las sesiones VSPAN.
- Se inhabilita una sesión VSPAN si la lista de los VLA N del Admin Source está vacía.
- Los VLA N inactivos no se permiten para la configuración VSPAN.
- Una sesión VSPAN se hace inactiva si los VLA N uces de los de la fuente se convierten en los VLA N RSPAN.

Refiera a las características del VLA N de la fuente para más información sobre los VLA N de la fuente.

VLA N ACL

Los VACL pueden el control de acceso todo el tráfico. Usted puede configurar los VACL en el Switch para aplicarse a todos los paquetes en los cuales se ruteen o fuera de un VLA N o se interliguen dentro de un VLA N. Los VACL están estrictamente para el filtrado de paquetes de la Seguridad y tráfico de la reorientación a los puertos del switch físicos específicos. A diferencia del Cisco IOS ACL, los VACL no son definidos por la dirección (entrada o salida).

Usted puede configurar los VACL en los direccionamientos de la capa 3 para el IP y el IPX. El resto de los protocolos son acceso controlado a través de las direcciones MAC y Ethertype usando el MAC VACL. El tráfico IP y el tráfico IPX no son acceso controlado por el MAC VACL. Clasifican al resto de los tipos de tráfico (APPLETALK, DECNet, y así sucesivamente) como tráfico MAC. El MAC VACL se utiliza al control de acceso este tráfico.

ACE soportados en los VACL

El VACL contiene una lista ordenada de las entradas de control de acceso (ACE). Cada VACL puede contener los ACE de solamente un tipo. Cada ACE contiene varios campos que se correspondan con contra el contenido de un paquete. Cada campo puede tener una máscara de bits asociada para indicar qué bits son relevantes. Una acción se asocia a cada ACE que describe lo que debe hacer el sistema con el paquete cuando ocurre una coincidencia. La acción es dependiente de la característica. Los Catalyst 6500 Series Switch apoyan tres tipos de aces en el hardware:

- IP ACE
- IPX ACE
- Ethernetes ACE

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

ACE teclea	TCP o UDP	ICMP	El otro IP	IPX	Ethernet
Parámetros de la capa 4	Puerto de Origen	-	-	-	-
	Operador del puerto de origen	-	-	-	-
	Puerto de	-	-	-	-

	Destino				
	Operador del puerto destino	Código ICMP	-	-	-
	N/A	Tipo de ICMP	N/A	-	-
Parámetros de la 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	El otro protocolo	Tipo del paquete IPX	-
Parámetros de la capa 2	-	-	-	-	Ethertype
	-	-	-	-	Dirección de origen de los Ethernetes
	-	-	-	-	Dirección destino de los Ethernetes

Ventajas del uso VACL sobre el uso VSPAN

Hay varias limitaciones del uso VSPAN para la análisis del tráfico:

- Todos acodan el tráfico 2 que los flujos en un VLA N se capturan. Esto aumenta la cantidad de datos que se analizarán.
- Las cantidades de sesión de SPAN que pueden ser configuradas en los Catalyst 6500 Series Switch son limitadas. Refiera a las Limitaciones y resumen de características para 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 característica del puerto de la captura VACL puede ayudar a superar algunas de estas limitaciones. Los VACL no se diseñan sobre todo para monitorear el tráfico. Sin embargo, con una amplia gama de capacidad para clasificar el tráfico, la característica del puerto de la captura fue introducida de modo que el análisis de tráfico de la red pueda llegar a ser mucho más simple. Éstas son las ventajas del uso del puerto de la captura VACL sobre el VSPAN:

- Análisis del tráfico granularLos VACL pueden hacer juego basado en la dirección IP de origen, IP Address de destino, acodan los 4 Tipo de protocolo, los puertos de la fuente y de la capa de destino 4, y la otra información. Esta capacidad hace los VACL muy útiles para la identificación y la filtración granulares del tráfico.
- Número de sesionesLos VACL se aplican en hardware. El número de ACE que puedan ser creados depende del TCAM disponible en el Switches.
- Oversubscription del puerto destinoLa identificación granular del tráfico reduce el número de bastidores que se remitirán al puerto destino y de tal modo minimiza la probabilidad de su oversubscription.
- RendimientoLos VACL se aplican en hardware. No hay multa de rendimiento para la aplicación de los VACL a un VLA N en los Cisco Catalyst 6500 Series Switch.

Configurar

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

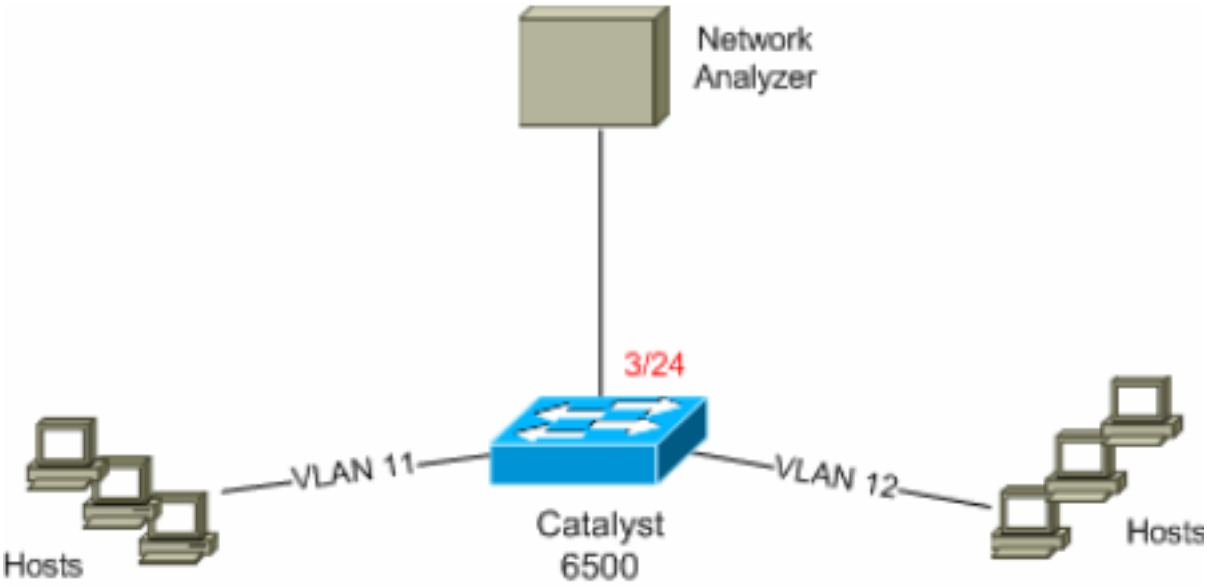
En este documento, se utilizan estas configuraciones:

- Configuración con el SPAN VLAN basado
- Configuración con el VACL

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) 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 el SPAN VLAN basado

Este ejemplo de configuración enumera los pasos requeridos para capturar todo el tráfico de la capa 2 que los flujos en el VLAN 11 y el VLAN 12 y les envíen al dispositivo del analizador de red.

1. Especifique el tráfico interesante.En este ejemplo, es el tráfico que fluye en el VLAN 100 y el VLA N 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 la capa 2 que pertenece al VLAN 11 y al VLAN 12 se copia y se envía al puerto 3/24.
2. Verifique su configuración de SPAN con el **comando all del palmo de la demostración**.`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 el VACL

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

- El tráfico HTTP de un rango de los host (10.12.12.128/25) en el VLAN 12 a un servidor específico (10.11.11.100) en el VLAN 11 necesita ser capturado.
- El tráfico del User Datagram Protocol (UDP) del Multicast en la dirección de transmisión destinada para el grupo de dirección 239.0.0.100 necesita ser capturado del VLAN 11.

1. Defina el tráfico interesante usando los ACL de seguridades. Recuerde mencionar la **captura de la** palabra clave para todos los ACE definida.`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 de ACE está correcta y en la orden apropiada.`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. Confíe el 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 estatus del 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 la correspondencia del acceso de VLAN a los VLA N apropiados.`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 el ACL a la asignación del VLA N.`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 la 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

un ACL se asocia a los VLAN múltiples, después el puerto de la captura se debe configurar a todos esos VLA N. Para hacer que el puerto de la captura permite los VLAN múltiples, configura el puerto como trunk y permite solamente los VLA N asociados al ACL. Por ejemplo, si el ACL se asocia a los VLA N 11 y 12, después 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 la 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.

- **muestre a presentaciones de la información acl de la Seguridad el** contenido del VACL que se configura o la más recientes están confiados actualmente al NVRAM y al 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)`
- **muestre la correspondencia acl de la Seguridad** — Visualiza la asignación del ACL-a-VLA N o del ACL-a-puerto para un ACL, un puerto, o un VLA N específico.`6K-CatOS> (enable) show security acl map all ACL Name Type Vlans ---------- ---- ----- HttpUdp_Acl IP 11 6K-CatOS> (enable)`
- **muestre los captura-puertos acl de la Seguridad** — Visualiza la lista de puertos de la captura.`6K-CatOS> (enable) show security acl capture-ports ACL Capture Ports: 3/24 6K-CatOS> (enable)`

Troubleshooting

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

Información Relacionada

- Captura VACL para la análisis del tráfico granular con el Cisco Catalyst 6000/6500 Cisco IOS Software corriente
- Configurando el control de acceso - Guía de configuración de software de las Catalyst 6500 Series, 8.6
- Páginas de Soporte de Productos de LAN
- Página de Soporte de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems