SPAN basado en flujo alternativo a la captura VACL

Contenido

Introducción

Este documento describe cómo utilizar un analizador de puertos conmutados (FSPAN) basado en flujo para capturar el tráfico filtrado en switches Cisco Catalyst que no admiten captura de lista de control de acceso (VACL) de VLAN.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Switches Cisco Catalyst serie 3750-X
- Switches Cisco Catalyst serie 3560-X
- Switches Cisco Catalyst serie 3750-E
- Switches Cisco Catalyst serie 3560-E
- Switches Catalyst de Cisco de la serie 2960-X que ejecutan una licencia de aislamiento
- Cisco IOS® versión 12.2(44)SE y posteriores

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.

Convenciones

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

Procedimiento

Los switches Catalyst de Cisco serie 3750-X, 3560-X, 3750-E, 3560-E y 2960-X (licencia de aislamiento) no admiten captura de VACL; sin embargo, estos switches admiten SPAN basado en flujos y SPAN remoto basado en flujos (RSPAN), que pueden lograr resultados similares a la captura de VACL.

El SPAN basado en el flujo proporciona un mecanismo para utilizar filtros especificados a fin de capturar los datos requeridos entre los hosts finales.

Puede asociar tres tipos de listas de control de acceso (ACL) FSPAN a la sesión SPAN:

- ACL IPv4 FSPAN: filtra sólo paquetes IPv4.
- IPv6 FSPAN ACL: filtra sólo paquetes IPv6.
- MAC FSPAN ACL: filtra solamente los paquetes que no son IP.

Las ACL de seguridad tienen mayor prioridad que las ACL de FSPAN en un switch. Si aplica ACL de FSPAN y luego agrega más ACL de seguridad que no pueden caber en la memoria de hardware, las ACL de FSPAN se quitan de la memoria para permitir espacio para las ACL de seguridad. Un mensaje del sistema notifica al usuario esta acción, que se denomina descarga.

Cuando el espacio vuelve a estar disponible, las ACL de FSPAN se agregan de nuevo a la memoria de hardware del switch. Un mensaje del sistema notifica al usuario esta acción, que se denomina recarga.

Los switches 3750-X admiten hasta dos sesiones SPAN y el FSPAN no puede evitar esta limitación. FSPAN utiliza la misma replicación ASIC que un SPAN normal.

Este es un ejemplo del uso de FSPAN en un switch 3750-X:

```
3750X(config)#ip access-list extended FILTER
3750X(config-ext-nacl)#permit ip host 192.168.1.1 host 172.16.1.1
3750X(config-ext-nacl)#exit
3750X(config)#monitor session 1 source interface gi1/0/1 both3750X
(config)#monitor session 1 destination interface gi1/0/2 3750X
(config)#monitor session 1 filter ip access-group FILTER

3750X(config)##exit3750X#show monitor session
sh mon session  1
Session 1
---------
Type                   : Local Session
Source Ports           :
   Both               : Gi1/0/1Destination Ports      : Gi1/0/2
   Encapsulation      : Native
```

```
        Ingress      : Disabled
IP Access-group       : FILTER
```

Restricciones

- El FSPAN no es compatible con los switches 3750, 3750G, 2950, 2960 y 2960-S.
- 2960-X que ejecuta la licencia de iplite sólo admite FSPAN.
- Puede asociar ACL a una sola sesión SPAN o RSPAN a la vez.
- Cuando no hay ACL de FSPAN conectadas, el FSPAN se inhabilita y todo el tráfico se copia en los puertos de destino de SPAN.
- Cuando se conecta al menos una ACL de FSPAN, se habilita FSPAN.
- Cuando se conecta una ACL FSPAN vacía a una sesión SPAN, no filtra los paquetes y se monitorea todo el tráfico.
- Los puertos Catalyst 3750 se pueden agregar como puertos de destino en una sesión FSPAN.
- Las sesiones FSPAN basadas en VLAN no se pueden configurar en una pila que incluya switches Catalyst 3750.
- Los EtherChannels no se soportan en una sesión FSPAN.
- Las ACL FSPAN con indicadores TCP o la palabra clave **log** no se soportan.
- Las sesiones FSPAN basadas en puerto se pueden configurar en una pila que incluya switches Catalyst 3750 siempre y cuando la sesión incluya solamente puertos Catalyst 3750-E como puertos de origen. Si la sesión tiene algún puerto Catalyst 3750 como puertos de origen, se rechaza el comando FSPAN ACL.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems