

Ejemplo de Captura de ACL del Switch Nexus serie 7000

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Ejemplo de Configuración de ACL](#)

[Advertencias](#)

[Información Relacionada](#)

Introducción

La captura de la lista de control de acceso (ACL) proporciona la capacidad de capturar selectivamente el tráfico en una interfaz o en una red de área local virtual (VLAN). Cuando habilita la opción de captura para una regla de ACL, los paquetes que coinciden con esta regla se reenvían o se descartan en función de la acción especificada permit o deny y también se pueden copiar en un puerto de destino alternativo para un análisis adicional. Se puede aplicar una regla ACL con la opción de captura:

1. En una VLAN,
2. En la dirección de ingreso en todas las interfaces,
3. En la dirección de salida en todas las interfaces de Capa 3.

Esta función es compatible con Nexus 7000 NX-OS versión 5.2 y posteriores. Este documento proporciona un ejemplo como guía de referencia rápida sobre cómo configurar esta función.

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.

- Nexus 7000 con versión 5.2.x y posteriores.
- Tarjeta de línea de la serie M1.

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 Técnicos de Cisco para obtener información sobre las convenciones sobre documentos.

Ejemplo de Configuración de ACL

A continuación se muestra un ejemplo de configuración de captura de ACL aplicada a una VLAN, también conocida como captura de lista de control de acceso (VACL) de LAN virtual. Los 10 rastreadores gigabit designados pueden no ser factibles para todos los escenarios. La captura selectiva de tráfico puede ser muy útil en tales escenarios, especialmente durante la resolución de problemas cuando los volúmenes de tráfico son altos.

```
!! Global command required to enable ACL-capture feature (on default VDC)
hardware access-list capture

monitor session 1 type acl-capture
destination interface ethernet 2/1
no shut
exit
!!
ip access-list TEST_ACL
10 permit ip 216.113.153.0/27 any capture session 1
20 permit ip 198.113.153.0/24 any capture session 1
30 permit ip 47.113.0.0/16 any capture session 1
40 permit ip any any
!!
!! Note: Capture session ID matches with the monitor session ID
!!
vlan access-map VACL_TEST 10
match ip address TEST_ACL
action forward
statistics per-entry
!!
vlan filter VACL_TEST vlan-list 500
```

También puede comprobar la programación de memoria direccionable de contenido ternario (TCAM) de la lista de acceso. Este resultado es para la VLAN 500 para el Módulo 1.

```
N7k2-VPC1# show system internal access-list vlan 500 input statistics
```

```
slot 1
=====
```

```
INSTANCE 0x0
-----
```

```
Tcam 1 resource usage:
-----
Label_b = 0x802
Bank 0
-----
IPv4 Class
Policies: VACL(VACL_TEST)
Netflow profile: 0
Netflow deny profile: 0
Entries:
[Index] Entry [Stats]
-----
[0006:0005:0005] permit ip 216.113.153.0/27 0.0.0.0/0 capture [0]
[0009:0008:0008] permit ip 198.113.153.0/24 0.0.0.0/0 capture [0]
[000b:000a:000a] permit ip 47.113.0.0/16 0.0.0.0/0 capture [0]
[000c:000b:000b] permit ip 0.0.0.0/0 0.0.0.0/0 [0]
[000d:000c:000c] deny ip 0.0.0.0/0 0.0.0.0/0 [0]
```

Advertencias

1. Sólo una sesión de captura de ACL puede estar activa en un momento dado del sistema en contextos de dispositivos virtuales (VDC).
2. Los módulos de la serie F1 de Nexus 7000 no admiten captura ACL.
3. Los módulos F2 de Nexus 7000 no admiten actualmente captura ACL, pero esto podría estar en la hoja de ruta.
4. La captura de ACL en los módulos M2 de Nexus 7000 es compatible con Cisco NX-OS versión 6.1(1) y posteriores.
5. La captura de ACL en los módulos M1 Nexus serie 7000 es compatible con Cisco NX-OS versión 5.2(1) y posteriores.
6. La captura de ACL no es compatible con el registro de ACL. Por lo tanto, si tiene ACL con una palabra clave **log**, éstas no funcionan después de que haya ingresado globalmente **captura de lista de acceso de hardware**.
7. Debido al [error CSCug20139](#), el ejemplo en este documento se documenta con una **sesión de captura** por ACE en lugar de por ACL, hasta que se resuelva el error.

Información Relacionada

- [Guía de Configuración de Seguridad de Cisco Nexus 7000 Series NX-OS, Versión 6.x, Ejemplos de Configuración de ACL IP](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)