Contenido

Introducción

Este documento describe cómo configurar el registro optimizado de la lista de control de acceso (ACL) (OAL) en los 7000 y 7700 Series Switch del nexo de Cisco.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de las configuraciones del nexo con los ACL básicos antes de que usted intente la configuración que se describe en este documento.

Componentes Utilizados

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

- Switches Cisco Nexus de la serie 7000
- 7700 Series Switch del nexo de Cisco

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.

Antecedentes

los ACL Registro-habilitados proporcionan la penetración en el tráfico mientras que atraviesa la red o es caído por los dispositivos de red. Desafortunadamente, el registro de ACL puede ser uso intensivo de la CPU y puede afectar negativamente a otras funciones del dispositivo de red. Para reducir los ciclos de la CPU, el 7000 Series Switch del nexo de Cisco utiliza OALs.

El uso de OALs proporciona el soporte del hardware para el registro de ACL. El OAL permite o cae los paquetes en el hardware y utiliza una rutina optimizada para enviar la información al supervisor de modo que pueda generar los mensajes de registración. Por ejemplo, cuando un paquete golpea un ACL con el registro habilitado mientras que se remite en el hardware, una copia del paquete se crea en el hardware y el paquete se lleva en batea al supervisor para el acuerdo de apertura de sesión con el intervalo de tiempo se configura que.

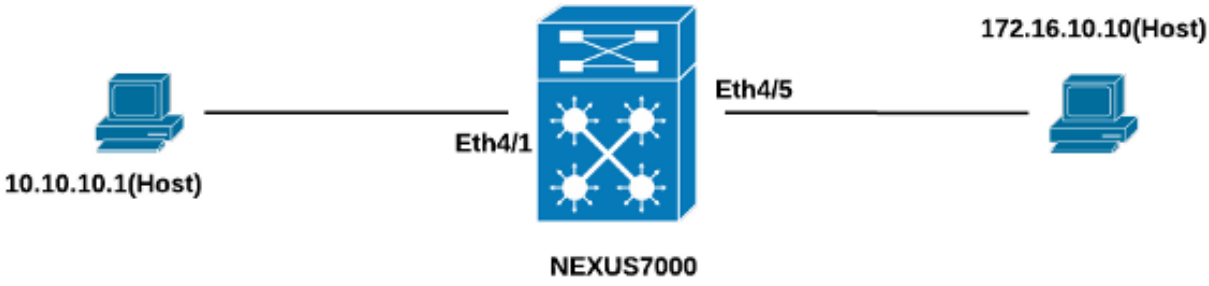
Configurar

Esta sección proporciona la información que usted puede utilizar para configurar el Switch del nexo para el uso de OALs.

En el ejemplo que se describe en esta sección, hay un host en la dirección IP 10.10.10.1 que envía el tráfico a otro host en la dirección IP 172.16.10.10 con las 7000 Series de un nexo interconecta, que tiene un ACL con el registro configurado.

Diagrama de la red

La conexión entre los host y el 7000 Series Switch del nexo ocurre según esta topología:



Configuraciones

Complete estos pasos para configurar el Switch para el uso de OALs:

1. Configure estos comandos global para habilitar el OAL:
   Aquí tiene un ejemplo:

```
Nexus-7000# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Nexus-7000(config)#logging ip access-list cache entries 8000
```

```
Nexus-7000(config)#logging ip access-list cache interval 300
Nexus-7000(config)#logging ip access-list cache threshold 0
```

2. Aplique esta configuración para registrar:

```
Nexus-7000# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Nexus-7000(config)#logging ip access-list cache entries 8000
Nexus-7000(config)#logging ip access-list cache interval 300
Nexus-7000(config)#logging ip access-list cache threshold 0
```

Aquí tiene un ejemplo:

```
Nexus-7000(config)# logging level acllog 5
Nexus-7000(config)# acllog match-log-level  5
Nexus-7000(config)# logging logfile acllog 5
```

3. Configure el ACL para habilitar el registro. Las entradas se deben configurar con la palabra clave del **registro** habilitada, tal y como se muestra en de este ejemplo:

```
Nexus-7000(config)# ip access-list test1
Nexus-7000(config-acl)# 10 permit ip 10.10.10.1/32 172.16.10.10/32 log
Nexus-7000(config-acl)# 20 deny ip any any log
Nexus-7000(config-acl)#
Nexus-7000(config-acl)#show ip access-lists test1 IP access list test1
10 permit ip 10.10.10.1/32 172.16.10.10/32 log
20 deny ip any any log
Nexus-7000(config-acl)#
```

4. Aplique el ACL que usted configuró en el paso anterior a la interfaz necesaria:

```
Nexus-7000# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus-7000(config)# int ethernet 4/1
Nexus-7000(config-if)# ip access-group test1 in
Nexus-7000(config-if)# ip access-group test1 out
Nexus-7000(config-if)#
Nexus-7000(config-if)# show run int ethernet 4/1
!Command: show running-config interface Ethernet4/1
!Time: Mon Jun 30 16:30:38 2014
version 6.2(6)
interface Ethernet4/1
 ip access-group test1 in
 ip access-group test1 out
 ip address 10.10.10.2/24
 no shutdown
Nexus-7000(config-if)#
```

Verificación

Utilice la información que se proporciona en esta sección para verificar que su configuración trabaja correctamente.

En el ejemplo que se utiliza en este documento, el ping se inicia del host en la dirección IP 10.10.10.1 al host en la dirección IP 172.16.10.1. Ingrese el **comando cache de registración de la lista de acceso del IP de la demostración** en el CLI para verificar el flujo de tráfico:

```
Nexus-7000# show logging ip access-list cache
Src IP Dst IP S-Port D-Port Src Intf Protocol Hits
------------------------------------------------------------
10.10.10.1 172.16.10.10 0 0 Ethernet4/1 (1)ICMP 368
Number of cache entries: 1
------------------------------------------------------------
Nexus-7000#
Nexus-7000# show logging ip access-list status Max flow = 8000
Alert interval = 300
Threshold value = 0
Nexus-7000#
```

Usted puede ver el registro cada 300 segundos, como éste es el intervalo de tiempo predeterminado:

```
Nexus-7000# show logging logfile
2014 Jun 29 19:19:01 Nexus-7000 %SYSLOG-1-SYSTEM_MSG : Logging logfile (acllog)
cleared by user
2014 Jun 29 19:20:57 Nexus-7000 %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configured from vty by
admin on console0
2014 Jun 29 19:21:18 Nexus-7000 %ACLLOG-5-ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol:
"ICMP"(1), Hit-count = 2589
2014 Jun 29 19:26:18 Nexus-7000 %ACLLOG-5-ACLLOG_FLOW_INTERVAL: Src IP: 10.1 0.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/1, Pro tocol:
"ICMP"(1), Hit-count = 4561
```

Troubleshooting

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

Notas de configuración

Esta sección proporciona la información adicional sobre la configuración que se describe en este documento.

Registro de ACL detallado

En las versiones del sistema operativo del nexo (NX-OS) 6.2(6) y posterior, registro de ACL *detallado* está disponible. La característica registra esta información:

- Direcciones IP de origen y de destino
- Puertos de origen y de destino
- Interfaz de origen
- Protocolo
- Nombre ACL
- Acción ACL (permit or deny)
- Interfaz aplicada
- Cuenta de paquetes

Ingrese el **comando detailed de registración de la lista de acceso del IP** en el CLI para habilitar la registración detallada. Aquí tiene un ejemplo:

```
Nexus-7000(config)# logging ip access-list detailed
ACL Log detailed Logging feature is enabled. Hit-count of existing ACL Flow entry will
be reset to zero and will contain Hit Count per ACL type Flow.
Nexus-7000(config)#
```

Aquí está una salida de registro del ejemplo después de que se habilite el registro detallado:

```
Nexus-7000(config)# logging ip access-list detailed
ACL Log detailed Logging feature is enabled. Hit-count of existing ACL Flow entry will
be reset to zero and will contain Hit Count per ACL type Flow.
Nexus-7000(config)#
```

Descripciones de comandos globales del OAL

Esta sección describe los comandos globales del OAL que se utilizan para configurar el 7000 Series Switch del nexo para el uso de OALs.

Comando	Descripción
Caché de la lista de acceso del IP del registro de Switch(config)# {{number_of_entries de las entradas} | {segundos del intervalo} | {number_of_packets del tarifa-límite} | {number_of_packets del umbral}}	Este comandos estableces los Parámetros globales del OAL.
Switch(config)# ningún caché de la lista de acceso del IP del registro {entradas | intervalo | tarifa-límite | umbral}	Este comando invierte los Parámetros globales del OAL a las configuraciones predeterminadas.
entradas num_entries	Estos parámetros especifican el número máximo de entradas d registro que se oculten en el software. El rango es 0 a 1,048,57 valor predeterminado es 8,000 entradas.
intervalo segundos	Estos parámetros especifican el intervalo de tiempo máximo an de que una entrada se envíe a un Syslog. El rango es 5 a 86,40 valor predeterminado es 300 segundos.
umbral num_packets	Estos parámetros especifican el número de coincidencias del paquete (golpes) antes de que una entrada se envíe a un Syslo rango es 0 a 1,000,000. El valor predeterminado es los paquete (la limitación de la tarifa está apagada), así que significa que el registro del sistema no es accionado por el número de coincide del paquete.

Nota: *La ninguna* forma de estos comandos CLI invierte solamente los parámetros a las configuraciones predeterminadas si se han cambiado; no quita la configuración, pues el 7000 Series Switch del nexo tiene solamente la opción del OAL.

Descripciones del comando logging

Esta sección describe los comandos logging que se utilizan para configurar el 7000 Series Switch del nexo para el uso de OALs.

Comando	Descripción
número de nivel del coincidencia-registro del acllog del switch(config)# Ejemplo: nivel 3 del coincidencia-registro del acllog del switch(config)#	Este comando especifica el nivel de registro que debe ser correspondido con antes de que las entradas se abran una sesión registro ACL (acllog). El rango es 0 a 7. El valor por defecto es val 6.
Switch(config)# ningún número de nivel del coincidencia-registro del acllog Ejemplo: switch(config)# ningún nivel 6 del coincidencia-registro del acllog	Este comando invierte el nivel de registro a la configuración predeterminada (6).
Nivel de gravedad del recurso del nivel de registro de Switch(config)# Ejemplo: acllog 3 del nivel de registro del switch(config)#	Este comando habilita los mensajes de registración del recurso especificado que tienen el nivel de gravedad especificado o más a En el ejemplo que se utiliza en este documento, el nivel del *acllog* a 3, mientras que la configuración predeterminada es 2.

Switch(config)# ningún [facility severity-level] del nivel de registro Ejemplo: switch(config)# ningún acllog 3 del nivel de registro	Este comando reajusta el nivel de gravedad del registro para el rec especificado a su nivel predeterminado. Si usted no especifica un recurso y una gravedad nivele, el dispositivo reajusta todos los recursos a sus niveles predeterminados. En el ejemplo que se utiliza en este documento, acllog se invierte al (2) predeterminado.
[size bytes] del nivel de gravedad del fichero de diario-nombre del fichero de diario del registro de Switch(config)# Ejemplo: acllog 3 del fichero de diario del registro del switch(config)#	Este comando configura el nombre del archivo del registro que se para salvar los mensajes del sistema y el nivel de gravedad mínim antes de que ocurra la registración. Usted puede especificar opcionalmente un tamaño del archivo máximo. El nivel de graveda predeterminado es 5, y el tamaño del archivo predeterminado es 10,485,760.
Switch(config)# ningún [logfile-name severity-level [size bytes] del fichero de diario del registro] Ejemplo: switch(config)# ningún acllog 3 del fichero de diario del registro	Este comando inhabilita el registro al archivo del registro.

Nota: Para que los mensajes del registro sean ingresados en los registros, el nivel de registro para el recurso del registro ACL (acllog) y el nivel de gravedad de registración para el fichero de diario deben ser mayor o igual la configuración del coincidencia-registro-*nivel del* registro ACL.

Guías de consulta y limitaciones

Aquí están algunas guías de consulta y limitaciones importantes que usted debe considerar antes de que usted aplique la configuración que se describe en este documento:

- Los 7000 y 7700 Series Switch del nexo soportan solamente el OAL.
- El registro de ACL no funciona con la característica de la captura ACL.
- La opción del *registro* en la salida ACL no se soporta para los paquetes de multidifusión.
- El soporte detallado del registro no está disponible para los paquetes del IPv6.
- El nivel de registro para el recurso del *acllog* y la gravedad del *fichero de diario del registro* debe ser configurado tales que son mayor o igual la configuración del coincidencia-registro-*nivel del acllog*.
- No utilice el **comando capture de la lista de acceso del hardware** mientras que se utiliza el OAL. Cuando este comando se utiliza junto al OAL, y a usted captura del permiso ACL, un mensaje de advertencia aparece para informarle que el registro de ACL se está inhabilitando para todos los contextos del dispositivo virtual (VDC). Cuando usted inhabilita la captura ACL, se habilita el registro de ACL. Para que este de proceso trabaje correctamente, neutralización con el uso del **ningún comando capture de la lista de acceso del hardware**.