Ejemplo de Configuración del Registro de ACL Optimizado de los Switches Nexus Serie 7000 y 7700

Contenido

Introducción

Este documento describe cómo configurar el registro de lista de control de acceso (ACL) optimizado (OAL) en los switches Nexus de Cisco serie 7000 y 7700.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de las configuraciones de Nexus con ACL básicas antes de intentar 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 de la serie Cisco Nexus 7000
- Switches de la serie Cisco Nexus 7700

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.

Antecedentes

Las ACL habilitadas para el registro proporcionan información sobre el tráfico a medida que atraviesa la red o que los dispositivos de red las descartan. Desafortunadamente, el registro de ACL puede requerir un uso intensivo de la CPU y puede afectar negativamente a otras funciones del dispositivo de red. Para reducir los ciclos de CPU, el switch Nexus de Cisco serie 7000 utiliza OAL.

El uso de OAL proporciona soporte de hardware para el registro de ACL. El OAL permite o descarta paquetes en el hardware y utiliza una rutina optimizada para enviar información al Supervisor de modo que pueda generar los mensajes de registro. Por ejemplo, cuando un paquete llega a una ACL con el registro habilitado mientras se reenvía en el hardware, se crea una copia del paquete en el hardware y el paquete se envía al Supervisor para que lo registre de acuerdo con el intervalo de tiempo configurado.

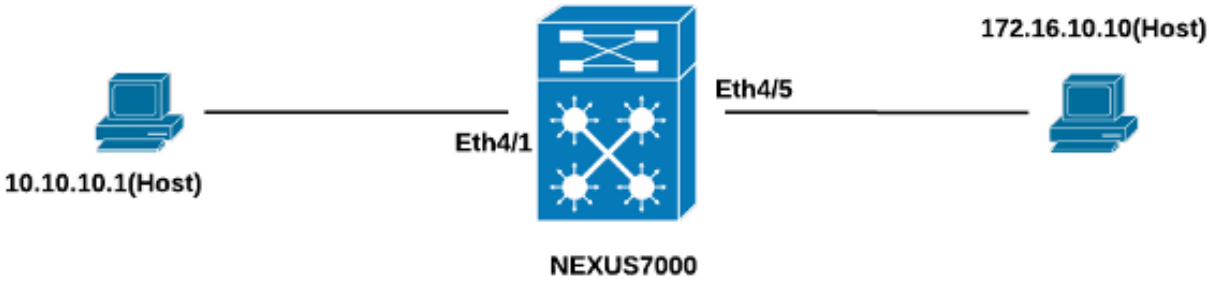
Configurar

Esta sección proporciona información que puede utilizar para configurar el switch Nexus para el uso de OAL.

En el ejemplo que se describe en esta sección, hay un host en la dirección IP 10.10.10.1 que envía tráfico a otro host en la dirección IP 172.16.10.10 a través de una interfaz Nexus serie 7000, que tiene configurada una ACL con registro.

Diagrama de la red

La conexión entre los hosts y el switch Nexus serie 7000 se produce según esta topología:



Configuraciones

Complete estos pasos para configurar el switch para el uso de OAL:

1. Configure estos comandos globales para habilitar OAL:

```
logging ip access-list cache entries 8000
logging ip access-list cache interval 300
logging ip access-list cache threshold 0
```

   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 el registro:

```
logging level acllog <number>
acllog match-log-level <number>
logging logfile [name] <number>
```

   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 la ACL para habilitar el registro. Las entradas se deben configurar con la palabra clave **log** habilitada, como se muestra en 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 la ACL que configuró en el paso anterior a la interfaz requerida:

```
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 proporcionada en esta sección para verificar que su configuración funcione

correctamente.

En el ejemplo que se utiliza en este documento, el ping se inicia desde el host en la dirección IP 10.10.10.1 al host en la dirección IP 172.16.10.1. Ingrese el comando **show logging ip access-list cache** en la 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#
```

Puede ver el registro cada 300 segundos, ya que 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
```

Troubleshoot

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

Notas de configuración

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

Registro de ACL detallado

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

- Direcciones IP de origen y de destino
- Puertos de origen y de destino
- Interfaz de origen
- Protocolo
- nombre ACL

- Acción de ACL (permitir o denegar)
- Interfaz aplicada
- Recuento de paquetes

Ingrese el comando **logging ip access-list detailed** en la CLI para habilitar el registro detallado. 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)#
```

A continuación se muestra un ejemplo de salida de registro después de habilitar el registro detallado:

```
2014 Jul 18 02:20:38 Nexus7k-1-oal %ACLLOG-6-ACLLOG_FLOW_INTERVAL: Src IP: 10.10.10.1,
Dst IP: 172.16.10.10, Src Port: 0, Dst Port: 0, Src Intf: Ethernet4/5, Protocol:
"ICMP"(1), ACL Name: test1, ACE Action: Permit, Appl Intf: Ethernet4/5, Hit-count: 69
```

Descripciones del comando global OAL

Esta sección describe los comandos OAL globales que se utilizan para configurar el switch Nexus serie 7000 para el uso de OAL.

Comando	Descripción
Switch(config)# logging ip access-list cache {{entries number_of_entries} | {interval seconds} | {rate-limit number_of_packets} | {threshold number_of_packets}}	Este comando establece los parámetros globales OAL.
Switch(config)# no logging ip access-list cache {entries | intervalo | rate-limit | threshold}	Este comando devuelve los parámetros globales OAL a la configurac predeterminada.
entradas num_entries	Estos parámetros especifican el número máximo de entradas de regi almacenadas en la memoria caché del software. El rango es 0 a 1,048,576. El valor predeterminado es 8,000 entradas.
intervalo segundos	Estos parámetros especifican el intervalo de tiempo máximo antes de enviar una entrada a un syslog. El rango es 5 a 86,400. El valor predeterminado es 300 segundos.'
umbral num_packets	Estos parámetros especifican el número de coincidencias de paquete (aciertos) antes de enviar una entrada a un syslog. El rango es 0 a 1,000,000. El valor predeterminado es 0 paquetes (la limitación de velocidad está desactivada), lo que significa que el registro del sistem se activa por el número de coincidencias de paquetes.

> **Nota:** La forma *no* de estos comandos CLI sólo revierte los parámetros a la configuración predeterminada si se han cambiado; no elimina la configuración, ya que el switch Nexus serie 7000 solo tiene la opción de OAL.

Descripciones de los comandos de registro

Esta sección describe los comandos de registro que se utilizan para configurar el switch Nexus serie 7000 para el uso de OAL.

Comando	Descripción
switch(config)# acllog match-log-level number Ejemplo: switch(config)# acllog match-log- nivel 3	Este comando especifica el nivel de registro que debe coincidir antes de qu entradas se registren en el registro ACL (registro de ACL). El rango es 0 a 7 valor predeterminado es 6.
Switch(config)# no acllog match-log-level number Ejemplo: switch(config)# no acllog match-log-level 6	Este comando devuelve el nivel de registro a la configuración predetermina (6).
Switch(config)# nivel de registro nivel nivel de gravedad de la instalación Ejemplo: switch(config)# logging level acllog 3	Este comando habilita el registro de mensajes de la función especificada qu tienen el nivel de gravedad especificado o superior. En el ejemplo que se ut en este documento, el nivel *acllog* se establece en 3, mientras que el valor predeterminado es 2.
Switch(config)# sin nivel de registro [nivel de gravedad de la instalación] Ejemplo: switch(config)# no logging level acllog 3	Este comando restablece el nivel de gravedad de registro para la instalación especificada a su nivel predeterminado. Si no especifica una función y grav , el dispositivo restablece todas las instalaciones a sus niveles predetermina En el ejemplo que se utiliza en este documento, el registro de llamadas se v al valor predeterminado (2).
Switch(config)# logging logfile logfile-name severity-level [size bytes] Ejemplo: switch(config)# logging logfile acllog 3	Este comando configura el nombre del archivo de registro que se utiliza par almacenar los mensajes del sistema y el nivel de gravedad mínimo antes de se produzca el registro. Opcionalmente, puede especificar un tamaño máxi archivo. El nivel de gravedad predeterminado es 5 y el tamaño predetermin del archivo es 10 485 760.
Switch(config)# no logging logfile [logfile-name severity-level [size bytes]] Ejemplo: switch(config)# no logging logfile acllog 3	Este comando inhabilita el registro en el archivo de registro.

> **Nota:** Para que los mensajes de registro se ingresen en los registros, el nivel de registro para la función de registro ACL (registro de ACL) y el nivel de gravedad de registro para el archivo de registro deben ser mayores o iguales a la configuración de nivel de *coincidencia de registro de ACL*.

Pautas y limitaciones

Estas son algunas pautas y limitaciones importantes que debe tener en cuenta antes de aplicar la configuración que se describe en este documento:

- Los switches Nexus serie 7000 y 7700 solo admiten OAL.
- El registro de ACL no funciona con la función Captura de ACL.
- La opción *log* en las ACL de salida no se soporta para los paquetes multicast.
- El soporte de registro detallado no está disponible para los paquetes IPv6.

- El nivel de registro para la función *acllog* y la gravedad del *archivo de registro de registro* deben configurarse de modo que sean mayores o iguales a la configuración *acllog match-log-level*.

- No utilice el comando **hardware access-list capture** mientras se utiliza OAL. Cuando se utiliza este comando junto con OAL y se habilita la captura de ACL, aparece un mensaje de advertencia para informarle de que el registro de ACL se está inhabilitando para todos los contextos de dispositivos virtuales (VDC). Cuando inhabilita la captura de ACL, el registro de ACL está habilitado. Para que este proceso funcione correctamente, inhabilite con el uso del comando **no hardware access-list capture**.