Exemplo de configuração de registro de ACL otimizada dos switches Nexus 7000 e 7700 Series

Contents

Introduction

Este documento descreve como configurar o OAL (Otimized Access Control List, lista de controle de acesso otimizada) nos switches Cisco Nexus 7000 e 7700 Series.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento das configurações do Nexus com ACLs básicas antes de tentar a configuração descrita neste documento.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- Switches Cisco Nexus 7000 Series
- Switches Cisco Nexus 7700 Series

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.

Informações de Apoio

As ACLs habilitadas para registro fornecem informações sobre o tráfego à medida que ele atravessa a rede ou é descartado por dispositivos de rede. Infelizmente, o registro da ACL pode ser intensivo da CPU e afetar negativamente outras funções do dispositivo de rede. Para reduzir os ciclos da CPU, o switch Cisco Nexus 7000 Series usa OALs.

O uso de OALs fornece suporte de hardware para o registro de ACL. A OAL permite ou descarta pacotes no hardware e usa uma rotina otimizada para enviar informações ao Supervisor para que ele possa gerar as mensagens de registro. Por exemplo, quando um pacote atinge uma ACL com registro ativado enquanto é encaminhado no hardware, uma cópia do pacote é criada no hardware e o pacote é direcionado ao Supervisor para registro de acordo com o intervalo de tempo configurado.

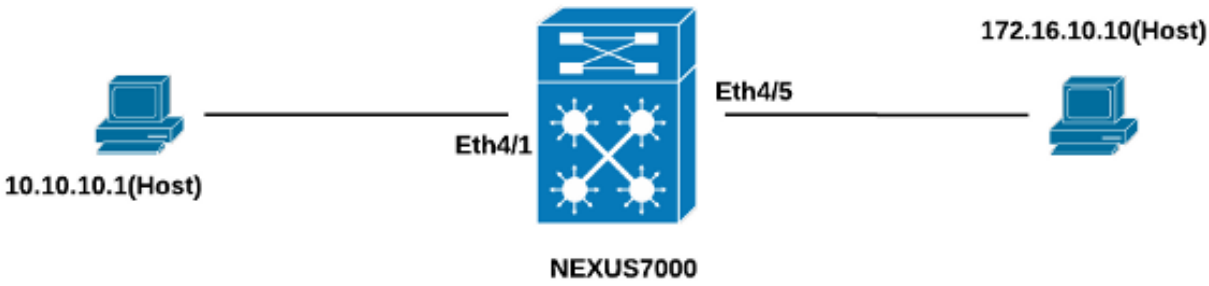
Configurar

Esta seção fornece informações que você pode usar para configurar o switch Nexus para o uso de OALs.

No exemplo descrito nesta seção, há um host no endereço IP 10.10.10.1 que envia tráfego para outro host no endereço IP 172.16.10.10 através de uma interface Nexus 7000 Series, que tem uma ACL com registro configurado.

Diagrama de Rede

A conexão entre os hosts e o switch Nexus 7000 Series ocorre de acordo com essa topologia:



Configurações

Conclua estes passos para configurar o switch para o uso de OALs:

1. Configure estes comandos globais para ativar o OAL:

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

   Aqui está um exemplo:

```
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 configuração para registro:

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

   Aqui está um exemplo:

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

3. Configure a ACL para ativar o registro. As entradas devem ser configuradas com a palavra-chave **log** ativada, como mostrado neste exemplo:

```
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 a ACL configurada na etapa anterior à interface necessária:

```
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)#
```

Verificar

Use as informações fornecidas nesta seção para verificar se a configuração funciona

corretamente.

No exemplo usado neste documento, o ping é iniciado do host no endereço IP 10.10.10.1 para o host no endereço IP 172.16.10.1. Insira o comando **show logging ip access-list cache** na CLI para verificar o fluxo de tráfego:

```
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#
```

Você pode ver o log a cada 300 segundos, pois esse é o intervalo de tempo padrão:

```
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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Notas de configuração

Esta seção fornece informações adicionais sobre a configuração descrita neste documento.

Registro de ACL detalhado

Nas versões 6.2(6) e posteriores do Nexus Operating System (NX-OS), o registro da ACL *detalhado* está disponível. O recurso registra estas informações:

- Endereços IP de origem e de destino
- Portas de origem e de destino
- Interface de origem
- Protocolo
- nome da ACL

- Ação da ACL (permitir ou negar)
- Interface aplicada
- Contagem de pacotes

Insira o comando **logging ip access-list detailed** na CLI para ativar o registro detalhado. Aqui está um exemplo:

```
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)#
```

Aqui está um exemplo de saída de registro depois que o registro detalhado é ativado:

```
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
```

Descrições globais do comando OAL

Esta seção descreve os comandos globais OAL usados para configurar o switch Nexus 7000 Series para o uso de OALs.

Comando	Descrição
Switch(config)# logging ip access-list cache {{entry number_of_entries} | {intervalo segundos} | {rate-limit number_of_packets} | {threshold number_of_packets}	Esse comando define os parâmetros globais OAL.
Switch(config)#no logging ip access-list cache {entries | intervalo | limite de taxa | limiar}	Esse comando reverte os parâmetros globais OAL para as configura padrão.
entradas num_entries	Esses parâmetros especificam o número máximo de entradas de log estão em cache no software. O intervalo é 0 a 1,048,576. O valor pa é 8.000 entradas.
intervalo segundos	Esses parâmetros especificam o intervalo de tempo máximo antes d uma entrada ser enviada a um syslog. O intervalo é 5 a 86,400. O va padrão é de 300 segundos.
limite num_packets	Esses parâmetros especificam o número de correspondências de pa (acertos) antes de uma entrada ser enviada a um syslog. O intervalo 1,000,000. O valor padrão é 0 pacote (a limitação de taxa está desativada), o que significa que o registro do sistema não é disparad pelo número de correspondências de pacote.

Note: A forma *no* desses comandos CLI reverte os parâmetros somente para as configurações padrão se eles tiverem sido alterados; ele não remove a configuração, pois o switch Nexus 7000 Series tem apenas a opção OAL.

Descrições dos comandos de registro

Esta seção descreve os comandos de registro que são usados para configurar o switch Nexus 7000 Series para o uso de OALs.

Comando	Descrição
switch(config)# acllog match-log-level number Exemplo: switch(config)# acllog match-log - nível 3	Esse comando especifica o nível de registro que deve ser correspondido das entradas serem registradas no log da ACL (registro de chamadas). C intervalo é 0 a 7. O valor padrão é 6.
Switch(config)#no acllog match-log-level number Exemplo: switch(config)# no acllog match-log - level 6	Esse comando reverte o nível de registro para a configuração padrão (6).
Switch(config)#nível de gravidade da instalação de registro Exemplo: switch(config)#logging level log 3	Esse comando permite registrar mensagens do recurso especificado que tenham o nível de gravidade especificado ou superior. No exemplo que é usado neste documento, o nível de *registro de chamadas* é definido como enquanto a configuração padrão é 2.
Switch(config)#no logging level [nível de gravidade da instalação] Exemplo: switch(config)#no logging level acllog 3	Esse comando redefine o nível de gravidade de registro do recurso especificado para o seu nível padrão. Se você não especificar um recurso uma severidade nível, o dispositivo redefine todas as instalações para seus níveis padrão exemplo que é usado neste documento, o registro da chamada é revertid para o padrão (2).
Switch(config)# logging arquivo de log nome do arquivo gravidade-nível [tamanho bytes] Exemplo: switch(config)# logging log 3	Esse comando configura o nome do arquivo de log usado para armazena mensagens do sistema e o nível mínimo de gravidade antes do registro. Opcionalmente, você pode especificar um tamanho máximo de arquivo. C nível de gravidade padrão é 5 e o tamanho padrão do arquivo é 10.485.7
Switch(config)# no logging logfile [logfile-name nível de gravidade [tamanho bytes]] Exemplo: switch(config)#no logging logfile log 3	Esse comando desabilita o registro no arquivo de log.

> **Note**: Para que as mensagens de log sejam inseridas nos logs, o nível de log do recurso de log da ACL (acllog) e o nível de gravidade do log do arquivo de log devem ser maiores ou iguais à configuração do nível de *correspondência de log* da ACL.

Diretrizes e limitações

Aqui estão algumas diretrizes e limitações importantes que você deve considerar antes de aplicar a configuração descrita neste documento:

- Os switches Nexus 7000 e 7700 Series suportam apenas OAL.
- O registro de ACL não funciona com o recurso Captura de ACL.
- A opção *log* nas ACLs de saída não é suportada para pacotes multicast.

- O suporte de registro detalhado não está disponível para pacotes IPv6.

- O nível de registro do recurso *acllog* e a gravidade do *arquivo de log* devem ser configurados de modo que sejam maiores ou iguais à configuração *de nível de log de correspondência*.

- Não use o comando **hardware access-list capture** enquanto OAL for usado. Quando esse comando é usado junto com OAL e você habilita a captura de ACL, uma mensagem de aviso é exibida para informá-lo de que o registro de ACL está sendo desabilitado para todos os Virtual Device Context (VDCs). Quando você desabilita a captura de ACL, o registro de ACL é habilitado. Para que esse processo funcione corretamente, desative com o uso do comando **no hardware access-list capture**.