Os 7000 e 7700 Series Switch do nexo aperfeiçoaram o exemplo de configuração do logging ACL

Índice

Introdução

Este documento descreve como configurar o Access Control List aperfeiçoado (ACL) que registra (OAL) nos 7000 e 7700 Series Switch do nexo de Cisco.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento de configurações do nexo com ACL básicos antes que você tente a configuração que está descrita neste documento.

Componentes Utilizados

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

- Switches Cisco Nexus série 7000
- 7700 Series Switch do nexo de Cisco

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

os ACL Registrar-permitidos fornecem a introspecção no tráfego enquanto atravessa a rede ou é deixado cair por dispositivos de rede. Infelizmente, o logging ACL pode ser utilização de CPU e pode negativamente afetar outras funções do dispositivo de rede. A fim reduzir ciclos de CPU, o 7000 Series Switch do nexo de Cisco usa OAL.

O uso dos OAL fornece o suporte a hardware para o logging ACL. O OAL permite ou deixa cair pacotes no hardware e usa uma rotina aperfeiçoada a fim enviar a informação ao supervisor de modo que possa gerar os mensagens de registro. Por exemplo, quando um pacote bate um ACL com o registro permitido quando estiver encaminhado no hardware, uma cópia do pacote é criada no hardware e o pacote punted ao supervisor para o acordo de abertura com o intervalo de tempo que é configurado.

Configurar

Esta seção fornece a informação que você pode usar a fim configurar o interruptor do nexo para o uso dos OAL.

No exemplo que é descrito nesta seção, há um host no endereço IP 10.10.10.1 que envia o tráfego a um outro host no endereço IP 172.16.10.10 com o 7000 Series de um nexo conecta, que tem um ACL com o registro configurado.

Diagrama de Rede

A conexão entre os anfitriões e o 7000 Series Switch do nexo ocorre conforme esta topologia:

Configurações

Termine estas etapas a fim configurar o interruptor para o uso dos OAL:

1. Configurar estes comandos global a fim permitir 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 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
```

   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. Configurar o ACL a fim permitir o registro. As entradas devem ser configuradas com a palavra-chave do **log** permitida, segundo as indicações deste 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 o ACL que você configurou na etapa precedente à interface 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)#
```

Verificar

Use a informação que é fornecida nesta seção a fim verificar que sua configuração trabalha corretamente.

No exemplo que é usado neste documento, o sibilo é iniciado do host no endereço IP 10.10.10.1 ao host no endereço IP 172.16.10.1. Incorpore a **mostra que registra o comando cache da lista de acesso IP no** CLI a fim 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 registro de cada 300 segundos, como este 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
```

Troubleshooting

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

Notas de configuração

Esta seção fornece a informação adicional sobre a configuração que é descrita neste documento.

Logging ACL detalhado

Em liberações do sistema operacional do nexo (NX-OS) 6.2(6) e em um logging ACL mais atrasado, *detalhado* estão disponível. A característica registra esta informação:

- Endereços IP de origem e de destino
- Portas de origem e de destino
- Interface de origem
- Protocolo
- Nome ACL
- Ação ACL (permit or deny)
- Relação aplicada
- Contagem de pacote de informação

Inscreva o **comando detailed de registro da lista de acesso IP no** CLI a fim permitir 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)#
```

Estão aqui umas saídas de registro do exemplo depois que o registro detalhado é permitido:

```
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)#
```

Descrições de comando globais OAL

Esta seção descreve os comandos globais OAL que são usados a fim configurar o 7000 Series Switch do nexo para o uso dos OAL.

Comando	Descrição
Switch(config)# que registra o esconderijo da lista de acesso IP {{number_of_entries das entradas} | {segundos do intervalo} | {number_of_packets do taxa-limite} | {number_of_packets do ponto inicial}}	Este conjuntos de comandos os parâmetros globais OAL.
Switch(config)# nenhum esconderijo de registro da lista de acesso IP {entradas | intervalo | taxa-limite | ponto inicial}	Este comando reverte os parâmetros globais OAL às configurações padrão.
entradas num_entries	Estes parâmetros especificam o número máximo de entradas registro que são postas em esconderijo no software. A escala a 1,048,576. O valor padrão é 8,000 entradas.
intervalo segundos	Estes parâmetros especificam o intervalo de tempo máximo que uma entrada esteja enviada a um Syslog. A escala é 5 a 86,400. O valor padrão é 300 segundos.
ponto inicial num_packets	Estes parâmetros especificam o número de fósforos do paco (batidas) antes que uma entrada esteja enviada a um Syslog escala é 0 a 1,000,000. O valor padrão é os pacotes 0 (a lim da taxa está), assim que significa que o log de sistema não e provocado pelo número de fósforos do pacote.

> **Note**: *Nenhum* formulário destes comandos CLI reverte somente os parâmetros às configurações padrão se foram mudados; não remove a configuração, porque o 7000 Series Switch do nexo tem somente a opção do OAL.

Descrições do comando logging

Esta seção descreve os comandos logging que são usados a fim configurar o 7000 Series Switch do nexo para o uso dos OAL.

Comando	Descrição
número de nível do fósforo-log do acllog do switch(config)# Exemplo: nível 3 do fósforo-log do acllog do switch(config)#	Este comando especifica o nível de registro que deve ser combina antes que as entradas estejam entradas o log ACL (acllog). A esca 0 ao 7. O padrão é valor é 6.
Switch(config)# nenhum número de	Este comando reverte o nível de registro à configuração padrão (6

nível do fósforo-log do acllog Exemplo: switch(config)# nenhum nível 6 do fósforo-log do acllog	
Nível de seriedade da facilidade do nível de registro de Switch(config)# Exemplo: acllog 3 do nível de registro do switch(config)#	Este comando permite os mensagens de registro da facilidade especificada que têm o nível de seriedade especificado ou mais altamente. No exemplo que é usado neste documento, o nível do a é ajustado a 3, visto que a configuração padrão é 2.
Switch(config)# nenhum [facility severity-level] do nível de registro Exemplo: switch(config)# nenhum acllog 3 do nível de registro	Este comando restaura o nível de seriedade de registro para a facilidade especificada a seu nível padrão. Se você não especifica facilidade e uma severidade nivele, o dispositivo restaura todas as facilidades a seus níveis pa No exemplo que é usado neste documento, o acllog é revertido ao padrão (2).
[size bytes] de registro do nível de seriedade do arquivo-nome do arquivo histórico de Switch(config)# Exemplo: acllog de registro 3 do arquivo histórico do switch(config)#	Este comando configura o nome do arquivo de registro que é usad fim armazenar os mensagens de sistema e o nível de seriedade m antes de registrar ocorre. Você pode opcionalmente especificar um tamanho do arquivo máximo. O nível de seriedade do padrão é 5, tamanho de arquivo padrão é 10,485,760.
Switch(config)# nenhum [logfile-name severity-level [size bytes] de registro do arquivo histórico] Exemplo: switch(config)# nenhum acllog de registro 3 do arquivo histórico	Este comando desabilita o registro ao arquivo de registro.

> **Note**: Para que os mensagens de registro sejam entrados nos logs, o nível de registro para a facilidade do log ACL (acllog) e o nível de seriedade de registro para o arquivo histórico devem ser superior ou igual ao ajuste do fósforo-log-*nível do* log ACL.

Diretrizes e limitações

Estão aqui algumas diretrizes e limitações importantes que você deve considerar antes que você aplique a configuração que está descrita neste documento:

- Os 7000 e 7700 Series Switch do nexo apoiam somente o OAL.
- O logging ACL não trabalha com a característica da captação ACL.
- A opção do *log na* saída ACL não é apoiada para pacotes de transmissão múltipla.
- O apoio de registro detalhado não está disponível para pacotes do IPv6.
- O nível de registro para a facilidade do *acllog* e a severidade de *registro do arquivo histórico* deve ser configurado tais que são superior ou igual ao ajuste do fósforo-log-*nível do acllog*.
- Não use o **comando capture da lista de acesso do hardware** quando o OAL for usado. Quando este comando está usado ao lado do OAL, e você permite a captação ACL, um mensagem de advertência aparece a fim informá-lo que o logging ACL está sendo desabilitado para todos os contextos do dispositivo virtual (VDC). Quando você desabilita a

captação ACL, o logging ACL está permitido. Para que este processo trabalhe corretamente, desabilitação com o uso de **nenhum comando capture da lista de acesso do hardware**.