Nexus 7000 en 7700 Series-switches - Geoptimaliseerd ACL-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u Optimized Access Control List (ACL) vastlegging (OAL) kunt configureren op de Cisco Nexus 7000 en 7700 Series-switches.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben van Nexus-configuraties met basis-ACL's voordat u probeert de configuratie te wijzigen die in dit document wordt beschreven.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- Cisco Nexus 7000 Series-switches

- Cisco Nexus 7700 Series-switches

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Logging-enabled ACL's bieden inzicht in verkeer aangezien het het netwerk overbrengt of door netwerkapparaten wordt gedropt. Helaas kan ACL-loggen CPU-intensief zijn en kan dit negatieve gevolgen hebben voor andere functies van het netwerkapparaat. Om CPU-cycli te reduceren, gebruikt de Cisco Nexus 7000 Series-switch OAL's.

Het gebruik van OALs biedt hardwareondersteuning voor ACL-vastlegging. De OAL staat of daalt pakketten in de hardware toe en gebruikt een geoptimaliseerde routine om informatie naar de supervisor te verzenden zodat het de houtkapberichten kan produceren. Bijvoorbeeld, wanneer een pakket een ACL met houtkap bereikt die wordt toegestaan terwijl het in de hardware wordt doorgestuurd, wordt een kopie van het pakket gemaakt in de hardware en het pakket wordt aan de supervisor voor loggen gestraft in overeenstemming met het tijdinterval dat wordt ingesteld.

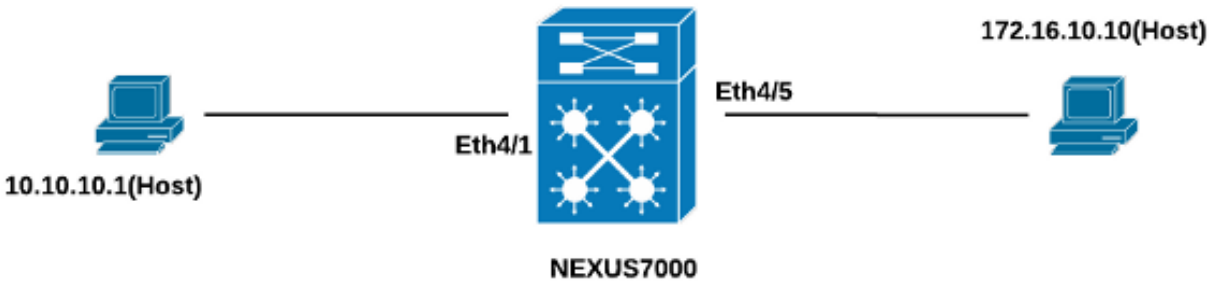
Configureren

Deze sectie verschaft informatie die u kunt gebruiken om de Nexus-schakelaar te configureren voor het gebruik van OALs.

In het voorbeeld dat in deze sectie wordt beschreven, is er een host op IP-adres 10.10.10.1 die verkeer naar een andere host op IP-adres 172.16.10.10 stuurt via een Nexus 7000 Series-interface, die een ACL met houtkap heeft geconfigureerd.

Netwerkdiagram

De verbinding tussen de hosts en de Nexus 7000 Series-switch kan plaatsvinden zoals per deze topologie:



Configuraties

Volg deze stappen om de schakelaar voor het gebruik van ALs te configureren:

1. Configureer deze globale opdrachten om OAL in te schakelen:

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

   Hierna volgt een voorbeeld:

```
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. Pas deze configuratie toe voor houtkap:

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

   Hierna volgt een voorbeeld:

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

3. Configureer de ACL om vastlegging mogelijk te maken. De ingangen moeten worden gevormd met het toegelaten **logsleutelwoord**, zoals in dit voorbeeld wordt getoond:

```
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. Pas ACL toe die u in de vorige stap hebt ingesteld op de gewenste interface:

```
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)#
```

Verifiëren

Gebruik de informatie in deze sectie om te controleren of uw configuratie correct werkt.

In het voorbeeld dat in dit document wordt gebruikt, wordt ping van de host op IP-adres 10.10.10.1 naar de host op IP-adres 172.16.10.1 gestart. Voer de opdracht bloggingip **access-list cache** in om de verkeersstroom te controleren:

```
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#
```

U kunt de houtkap elke 300 seconden zien, omdat dit het standaard tijdsinterval is:

```
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
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Configuratieopmerkingen

Deze sectie verschaft extra informatie over de configuratie die in dit document wordt beschreven.

Gedetailleerde ACL-vastlegging

In Nexus Operating System (NX-OS) releases 6.2(6) en later is *gedetailleerde* ACL-vastlegging beschikbaar. Deze informatie is te vinden op de website:

- IP-adressen van bron en bestemming
- Bron- en doelpoorten
- Broninterface
- Protocol
- ACL-naam
- Handeling ACL (licentie of ontkenning)
- Toepasselijke interface
- Packet-telling

Typ de **gedetailleerde** opdracht voor **logip-toegangslijst** in de CLI om gedetailleerde vastlegging mogelijk te maken. Hierna volgt een voorbeeld:

```
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)#
```

Hier is een voorbeeld van het registreren van output nadat het gedetailleerd registreren is toegelaten:

```
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
```

Algemene beschrijving van commando's

In dit gedeelte worden de OAL-opdrachten beschreven die worden gebruikt om de Nexus 7000 Series-switch te configureren voor gebruik van AL-toetsen.

Opdracht	Beschrijving
Switch (configuratie)# loggingip access-list cache {{{lemma_of_items} | {intervallen seconden} | {rate-limit number_of_Packets} | {drempelnummer_of_pakketten}	Deze opdracht stelt de OAL global parameters in.
Switch (configuratie)# geen logingip access-list cache {items | interval | tarieflimiet | drempel}	Deze opdracht converteert de OAL global parameters naar de standaardinstellingen.
inzendingen num_items	Deze parameters specificeren het maximale aantal logitems dat in d software gecached wordt. Het bereik is 0 tot 1.048.576. De standaardwaarde is 8.000 items.
interval seconden	Deze parameters specificeren het maximale tijdsinterval voordat een ingang naar een syslog wordt verzonden. Het bereik is 5 tot 86.400. standaardwaarde is 300 seconden.
drempel num_pakketten	Deze parameters specificeren het aantal pakketovereenkomsten (hi voordat een artikel naar een syslog wordt verzonden. Het bereik is 0 1.000.000. De standaardwaarde is 0 pakketten (snelheidsbeperking uit), wat betekent dat het systeemlogbestand niet wordt geactiveerd het aantal pakketovereenkomsten.

> Opmerking: De *geen* vorm van deze CLI-opdrachten geeft alleen de parameters om in de standaardinstellingen als deze zijn gewijzigd; het verwijdert de configuratie niet, aangezien de Nexus 7000 Series-switch alleen de optie OAL heeft.

Beschrijving van vastlegging

In dit gedeelte worden de logopdrachten beschreven die worden gebruikt om de Nexus 7000 Series-switch te configureren voor gebruik van OAL's.

Opdracht	Beschrijving
schakelaar (fig)# tekens op het aansluitingsniveau Voorbeeld: schakelaar ()# aaneenschakeling Switch (configuratie)# geen overeenkomend-log-level nummer	Deze opdracht specificeert het logniveau dat moet worden aangepast vo de items worden inlogd in het ACL-logbestand (ACL-logbestand). Het be is 0 tot 7. De standaard is waarde 6.
Voorbeeld: schakelaar (totaal)# geen overeenkomend-log-niveau 6	Deze opdracht keert het logniveau terug naar de standaardinstelling (6).
Switch ()# controleniveaus van de faciliteit Voorbeeld: schakelaar (wijzig)# loggingniveau 3	Deze opdracht maakt houtkapberichten van de gespecificeerde voorzien mogelijk die het gespecificeerde ernst niveau of hoger hebben. In het voorbeeld dat in dit document wordt gebruikt, is het opnameniveau inges op 3 terwijl de standaardinstelling 2 is.
Switch (configuratie)# op houtkapniveau [faciliteit ernst-niveau] Voorbeeld: schakelaar ()# op loggineniveau 3	Deze opdracht stelt het niveau van de logernst voor de gespecificeerde faciliteit op zijn standaard niveau in. Indien u geen faciliteit en ernst specificeert Zet de machine opnieuw in op het standaard niveau. In het voorbeeld da dit document wordt gebruikt, wordt de werkbalk teruggezet naar de stan (2).
Switch (configuratie)# logbestand logbestand-naam ernst-niveau [size bytes] Voorbeeld: schakelaar (fig)# logbestand 3	Deze opdracht vormt de naam van het logbestand dat wordt gebruikt om systeemmeldingen en het minimale ernst-niveau op te slaan voordat hou voorkomt. U kunt optioneel een maximale bestandsgrootte instellen. De standaardernst is 5, en de standaardbestandsgrootte is 10.485.760.
Switch (fig)# geen logbestand [logfile-naam ernst-niveau [size bytes]] Voorbeeld: schakelaar (fig)# geen logbestand 3	Deze opdracht schakelt het logbestand in.

> Opmerking: Om de logberichten in de logbestanden te kunnen invoeren, moeten het logniveau voor de ACL-logfaciliteit (logbestand) en het niveau van de logernst voor het logbestand groter zijn dan of gelijk aan de instelling *van het* ACL-logbestand.

Richtsnoeren en beperkingen

Hier zijn een aantal belangrijke richtlijnen en beperkingen die u moet overwegen voordat u de configuratie toepast die in dit document wordt beschreven:

- De Nexus 7000 en 7700 Series switches ondersteunen alleen OAL.
- ACL-loggen werkt niet met de ACL-opnamefunctie.
- De logoptie in grotere ACL's wordt niet ondersteund voor multicast pakketten.
- Gedetailleerde logondersteuning is niet beschikbaar voor IPv6-pakketten.
- Het logniveau voor de opslagfaciliteit en de ernst van het *logbestand* moeten zodanig worden

geconfigureerd dat ze groter zijn dan of gelijk zijn aan de instelling *van het gekoppelde matlogniveau*.

- Gebruik de opdracht **hardware access-list** niet terwijl OAL wordt gebruikt. Wanneer deze opdracht naast OAL wordt gebruikt en u ACL Capture toestaat, verschijnt er een waarschuwingsbericht om u te informeren dat ACL logging wordt uitgeschakeld voor alle Virtual Devices (VDC's). Wanneer u ACL-opname uitschakelt, is ACL-vastlegging ingeschakeld. Om dit proces naar behoren te laten werken, schakelt u deze optie uit met behulp van de opdracht **geen hardware access-list** op.