# Konfigurationsbeispiel für die optimierte ACL-Protokollierung für Nexus Switches der Serien 7000 und 7700

## Inhalt



## Einführung

In diesem Dokument wird beschrieben, wie die OAL-Protokollierung (Optimized Access Control List) für die Cisco Nexus Switches der Serien 7000 und 7700 konfiguriert wird.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, vor dem Versuch der Konfiguration, die in diesem Dokument beschrieben wird, über Kenntnisse der Nexus-Konfigurationen mit grundlegenden ACLs zu verfügen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und

Softwareversionen:

- Cisco Nexus Switches der Serie 7000
- Cisco Nexus Switches der Serie 7700

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# Hintergrundinformationen

Protokollierungsfähige ACLs bieten Einblicke in den Datenverkehr, der das Netzwerk passiert oder von Netzwerkgeräten verworfen wird. Leider kann die ACL-Protokollierung CPU-intensiv sein und andere Funktionen des Netzwerkgeräts beeinträchtigen. Um die CPU-Zyklen zu reduzieren, verwendet der Cisco Nexus Switch der Serie 7000 OALs.

Die Verwendung von OALs bietet Hardwareunterstützung für die ACL-Protokollierung. Die OAL-Funktion erlaubt oder verwirft Pakete in der Hardware und verwendet eine optimierte Routine, um Informationen an den Supervisor zu senden, sodass er die Protokollierungsnachrichten generieren kann. Wenn beispielsweise ein Paket auf eine ACL trifft, bei der die Protokollierung aktiviert ist, während es in der Hardware weitergeleitet wird, wird eine Kopie des Pakets in der Hardware erstellt, und das Paket wird zur Protokollierung gemäß dem konfigurierten Zeitintervall an den Supervisor übergeben.

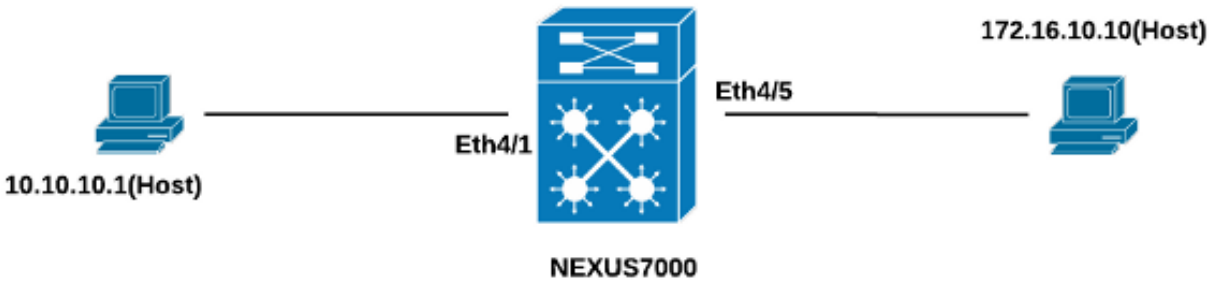
# Konfigurieren

Dieser Abschnitt enthält Informationen, die Sie verwenden können, um den Nexus-Switch für die Verwendung von OALs zu konfigurieren.

Im Beispiel, das in diesem Abschnitt beschrieben wird, gibt es einen Host mit der IP-Adresse 10.10.10.1, der Datenverkehr an einen anderen Host unter der IP-Adresse 172.16.10.10 über eine Schnittstelle der Nexus 7000-Serie sendet, die über eine ACL mit konfigurierter Protokollierung verfügt.

## Netzwerkdiagramm

Die Verbindung zwischen den Hosts und dem Switch der Nexus 7000-Serie erfolgt gemäß der folgenden Topologie:




## Konfigurationen

Gehen Sie wie folgt vor, um den Switch für die Verwendung von OALs zu konfigurieren:

1. Konfigurieren Sie diese globalen Befehle, um OAL zu aktivieren:

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

   Hier ein Beispiel:

```
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. Wenden Sie diese Konfiguration für die Protokollierung an:

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

   Hier ein Beispiel:

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

3. Konfigurieren Sie die ACL, um die Protokollierung zu aktivieren. Die Einträge müssen so konfiguriert werden, dass das **log-**Schlüsselwort aktiviert ist, wie in diesem Beispiel gezeigt:

```
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. Wenden Sie die im vorherigen Schritt konfigurierte ACL auf die erforderliche Schnittstelle an:

```
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)#
```

# Überprüfen

Verwenden Sie die Informationen in diesem Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

In dem in diesem Dokument verwendeten Beispiel wird der Ping vom Host unter der IP-Adresse 10.10.10.1 an den Host unter der IP-Adresse 172.16.10.1 initiiert. Geben Sie den Befehl **show logging ip access-list cache** in die CLI ein, um den Datenverkehrsfluss zu überprüfen:

```
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#
```

Sie sehen die Protokollierung alle 300 Sekunden, da dies das Standardzeitintervall ist:

```
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
```

# Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

# Konfigurationshinweise

Dieser Abschnitt enthält zusätzliche Informationen zur Konfiguration, die in diesem Dokument beschrieben wird.

## Detaillierte ACL-Protokollierung

In Nexus Operating System (NX-OS) Release 6.2(6) und höher ist *detaillierte* ACL-Protokollierung verfügbar. Diese Informationen werden protokolliert:

- Quell- und Ziel-IP-Adressen
- Quell- und Ziel-Ports
- Quellschnittstelle
- Protokoll
- ACL-Name
- ACL-Aktion (Zulassen oder Ablehnen)
- Angewendete Schnittstelle
- Paketanzahl

Geben Sie den **Detailbefehl logging ip access-list** in die CLI ein, um eine detaillierte Protokollierung zu ermöglichen. Hier ein Beispiel:

```
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)#
```

Nachfolgend finden Sie ein Beispiel für die Protokollierung, wenn die detaillierte Protokollierung aktiviert ist:

```
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
```

## Globale OAL-Befehlsbeschreibungen

In diesem Abschnitt werden die globalen OAL-Befehle beschrieben, die zur Konfiguration des Switches der Serie Nexus 7000 für die Verwendung von OALs verwendet werden.

| Befehl | Beschreibung |
|---|---|
| Switch(config)# logging ip access-list cache {{entries number_of_entries} \| {interval seconds} \| {rate limit number_of_packages} \| {threshold number_of_packages} | Mit diesem Befehl werden die globalen OAL-Parameter festgelegt. |
| Switch(config)# no logging ip access-list cache {entries \| Intervall \| Höchstsatz \| threshold} | Mit diesem Befehl werden die globalen OAL-Parameter auf die Standardeinstellungen zurückgesetzt. |
| Einträge Num_Einträge | Diese Parameter geben die maximale Anzahl an Protokolleinträgen an in der Software zwischengespeichert werden. Der Bereich liegt zwisch und 1.048.576. Der Standardwert ist 8.000 Einträge. |
| Intervall | Diese Parameter geben das maximale Zeitintervall an, bevor ein Eintr |

| | |
|---|---|
| Sekunden | ein Syslog gesendet wird. Der Bereich liegt zwischen 5 und 86.400. D Standardwert ist 300 Sekunden. |
| Schwellenwert Anzahl der Pakete | Diese Parameter geben die Anzahl der Paketübereinstimmungen (Tre an, bevor ein Eintrag an ein Syslog gesendet wird. Der Bereich liegt zwischen 0 und 1.000.000. Der Standardwert ist 0 Pakete (die Ratenbeschränkung ist deaktiviert). Das bedeutet, dass das Systemprotokoll nicht durch die Anzahl der Paketübereinstimmungen ausgelöst wird. |

**Hinweis**: Die *no*-Form dieser CLI-Befehle setzt die Parameter nur dann auf die Standardeinstellungen zurück, wenn sie geändert wurden. die Konfiguration wird dabei nicht entfernt, da der Nexus Switch der Serie 7000 nur die Option OAL bietet.

## Beschreibungen von Protokollbefehlen

In diesem Abschnitt werden die Protokollierungsbefehle beschrieben, die zur Konfiguration des Switches der Serie Nexus 7000 für die Verwendung von OALs verwendet werden.

| Befehl | Beschreibung |
|---|---|
| switch(config)# acllog match-log-level number<br>Beispiel: switch(config)# acllog match-log-Ebene 3 | Dieser Befehl gibt die Protokollierungsebene an, die zugeordnet werden muss, bevor Einträge im ACL-Protokoll (ACL-Protokoll) protokolliert werden. Der Bereich liegt zwischen 0 und 7. Der Standardwert ist 6. |
| Switch(config)# keine Protokollabgleichs-Protokollnummer<br>Beispiel: switch(config)# no acllog match-log-Ebene 6 | Mit diesem Befehl wird die Protokollierungsebene auf die Standardeinstellung zurückgesetzt (6). |
| Switch(config)#-Protokollierungsebene - Schweregrad<br>Beispiel: switch(config)# Protokollierungsebenenprotokoll 3 | Dieser Befehl ermöglicht die Protokollierung von Meldungen der angegebenen Einrichtung, die den angegebenen Schweregrad oder höher haben. In dem in diesem Dokument verwendeten Beispiel ist die Protokollstufe auf 3, die Standardeinstellung auf 2 festgelegt. |
| Switch(config)# keine Protokollierungsebene [Facility-Schweregrad]<br>Beispiel: switch(config)# kein Protokollierungsebenenprotokoll 3 | Mit diesem Befehl wird der Protokollierungsschweregrad für die angegebene Einrichtung auf die Standardstufe zurückgesetzt. Wenn Sie keine Einrichtung und keinen Schweregrad angeben -Ebene setzt das Gerät alle Einrichtungen auf die Standardstufe zurück. In dem in diesem Dokument verwendeten Beispiel wird das Protokoll auf den Standardwert (2) zurückgesetzt. |
| Switch(config)# logfile logfile name Severity-level [size bytes]<br>Beispiel: switch(config)# logfile acllog 3 zur Protokollierung | Mit diesem Befehl wird der Name der Protokolldatei konfiguriert, die zum Speichern der Systemmeldungen verwendet wird, sowie der Mindestschweregrad, bevor die Protokollierung erfolgt. Sie können optional eine maximale Dateigröße angeben. Der Standardschweregrad ist 5, und die Standarddateigröße ist 10.485.760. |
| Switch(config)# no logging logfile | Dieser Befehl deaktiviert die Protokollierung in der |

| | |
|---|---|
| [logfile name Severity-level [size bytes]]<br>Beispiel: switch(config)# no logging logfile acllog 3 | Protokolldatei. |

**Hinweis**: Damit die Protokollmeldungen in die Protokolle eingegeben werden können, müssen die Protokollierungsebene für die ACL-Protokolleinrichtung (ACL-Protokoll) und der Protokollierungsschweregrad für die Protokolldatei größer oder gleich der Einstellung *für die* ACL-*Protokollabgleichs*-Ebene sein.

## Richtlinien und Einschränkungen

Hier einige wichtige Richtlinien und Einschränkungen, die Sie beachten sollten, bevor Sie die in diesem Dokument beschriebene Konfiguration anwenden:

- Die Nexus Switches der Serien 7000 und 7700 unterstützen nur OAL.
- Die ACL-Protokollierung funktioniert nicht mit der Funktion zur ACL-Erfassung.
- Die *Log*-Option in Ausgangs-ACLs wird für Multicast-Pakete nicht unterstützt.
- Für IPv6-Pakete ist keine detaillierte Protokollierungsunterstützung verfügbar.
- Die Protokollierungsebene für die *Protokolleinrichtung* und der Schweregrad der *Protokolldatei* müssen so konfiguriert werden, dass sie größer oder gleich der Einstellung *für die Protokollabgleichsprotokollstufe sind*.
- Verwenden Sie nicht den Befehl **zur Erfassung der Hardware-Zugriffslisten**, während OAL verwendet wird. Wenn dieser Befehl zusammen mit OAL verwendet wird und Sie die ACL-Erfassung aktivieren, wird eine Warnmeldung angezeigt, die Sie darüber informiert, dass die ACL-Protokollierung für alle Virtual Device Contexts (VDCs) deaktiviert wird. Wenn Sie die ACL-Erfassung deaktivieren, wird die ACL-Protokollierung aktiviert. Damit dieser Prozess ordnungsgemäß ausgeführt werden kann, deaktivieren Sie die Anwendung mit dem Befehl **no hardware access-list capture** (Keine Zugriffslistenerfassung für Hardware).