Nexus 7000 및 7700 Series 스위치 최적화 ACL 로깅 컨피그레이션 예

목차

소개

이 문서에서는 Cisco Nexus 7000 및 7700 Series 스위치에 OAL(Optimized Access Control List) 로깅을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 설명된 컨피그레이션을 시도하기 전에 기본 ACL이 포함된 Nexus 컨피그레이션에 대한 지식을 가지고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Cisco Nexus 7000 Series 스위치

- Cisco Nexus 7700 Series 스위치

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

로깅 지원 ACL은 네트워크를 통과하거나 네트워크 디바이스에서 삭제하는 트래픽에 대한 통찰력을 제공합니다.안타깝게도 ACL 로깅은 CPU 집약적일 수 있으며 네트워크 디바이스의 다른 기능에 부정적인 영향을 미칠 수 있습니다.CPU 주기를 줄이기 위해 Cisco Nexus 7000 Series 스위치는 OAL을 사용합니다.

OAL을 사용하면 ACL 로깅을 위한 하드웨어 지원이 제공됩니다.OAL은 하드웨어에서 패킷을 허용하거나 삭제하고, Supervisor에 정보를 전송하기 위해 최적화된 루틴을 사용하여 로깅 메시지를 생성할 수 있습니다.예를 들어 패킷이 하드웨어에서 전달되는 동안 로깅이 활성화된 상태로 ACL에 도달하면 패킷의 복사본이 하드웨어에 생성되고 구성된 시간 간격에 따라 로깅하기 위해 패킷이 수퍼바이저에게 펀딩됩니다.

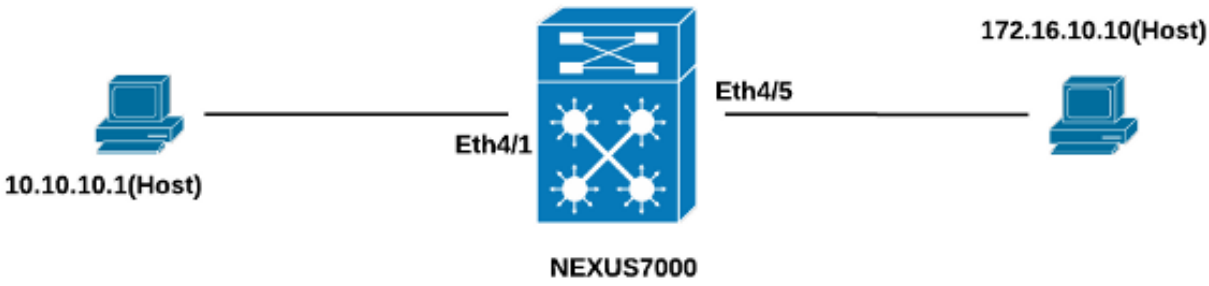
구성

이 섹션에서는 OAL 사용을 위해 Nexus 스위치를 구성하는 데 사용할 수 있는 정보를 제공합니다.

이 섹션에 설명된 예에는 IP 주소 10.10.10.1의 호스트가 있으며, 이 호스트는 Nexus 7000 Series 인터페이스를 통해 IP 주소 172.16.10.10의 다른 호스트로 트래픽을 전송합니다. 이 호스트는 로깅이 구성된 ACL이 있습니다.

네트워크 다이어그램

호스트와 Nexus 7000 Series 스위치 간의 연결은 이 토폴로지에 따라 발생합니다.



구성

OAL을 사용하도록 스위치를 구성하려면 다음 단계를 완료하십시오.

1. OAL을 활성화하려면 다음 전역 명령을 구성합니다.

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

예를 들면 다음과 같습니다.

```
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. 로깅을 위해 이 컨피그레이션을 적용합니다.

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

예를 들면 다음과 같습니다.

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

3. 로깅을 활성화하려면 ACL을 구성합니다.다음 예와 같이 log 키워드를 활성화하여 항목을 구성해야 합니다.

```
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. 이전 단계에서 구성한 ACL을 필수 인터페이스에 적용합니다.

```
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)#
```

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 이 섹션에 제공된 정보를 사용하십시오.

이 문서에서 사용되는 예에서 ping은 IP 주소 10.10.10.1의 호스트에서 IP 주소 172.16.10.1의 호스

트로 시작됩니다. 트래픽 흐름을 확인하려면 CLI에 **show logging ip access-list cache** 명령을 입력합니다.

```
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#
```

기본 시간 간격이므로 300초마다 로깅을 볼 수 있습니다.

```
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
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

구성 메모

이 섹션에서는 이 문서에 설명된 구성에 대한 추가 정보를 제공합니다.

자세한 ACL 로깅

Nexus 운영 체제(NX-OS) 릴리스 6.2(6) 이상에서 *자세한* ACL 로깅을 사용할 수 있습니다.이 기능은 다음 정보를 기록합니다.

- 소스 및 대상 IP 주소
- 소스 및 대상 포트
- 소스 인터페이스
- 프로토콜
- ACL 이름
- ACL 작업(허용 또는 거부)
- 적용된 인터페이스
- 패킷 수

자세한 로깅을 **활성화하려면 logging ip access-list detailed** 명령을 CLI에 입력합니다.예를 들면 다음과 같습니다.

```
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)#
```

자세한 로깅이 활성화된 후 출력 로깅 예는 다음과 같습니다.

```
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
```

전역 OAL 명령 설명

이 섹션에서는 OAL 사용을 위해 Nexus 7000 Series 스위치를 구성하는 데 사용되는 전역 OAL 명령에 대해 설명합니다.

명령	설명
Switch(config)# logging ip access-list cache {{entries number_of_entries} | {간격 초} | {rate-limit number_of_packets} | {threshold number_of_packets}}	이 명령은 OAL 전역 매개변수를 설정합니다.
Switch(config)# no logging ip access-list cache {entries | 간격 | 속도 제한 | 임계값}	이 명령은 OAL 전역 매개변수를 기본 설정으로 되돌립니다.
항목 num_entries	이러한 매개변수는 소프트웨어에 캐시된 로그 항목의 최대 수 정합니다.범위는 0~1,048,576입니다. 기본값은 8,000개의 항 니다.
간격 초	이러한 매개변수는 항목이 syslog로 전송되기 전의 최대 시간 을 지정합니다.범위는 5~86,400이고 기본값은 300초입니다.
임계값 num_packets	이러한 매개변수는 항목이 syslog로 전송되기 전의 패킷 일치) 수를 지정합니다.범위는 0~1,000,000입니다. 기본값은 0개. 킷(속도 제한은 해제됨)입니다. 즉, 패킷 일치 수에 의해 시스 그가 트리거되지 않습니다.

참고:이러한 CLI 명령의 no 형식은 매개변수가 변경된 경우에만 기본 설정으로 되돌립니다 .Nexus 7000 Series 스위치에는 OAL 옵션만 있으므로 컨피그레이션은 제거되지 않습니다.

로깅 명령 설명

이 섹션에서는 OAL 사용을 위해 Nexus 7000 Series 스위치를 구성하는 데 사용되는 로깅 명령에 대해 설명합니다.

명령	설명
switch(config)# acllog match-log 레벨 번호 예:switch(config)# acllog match-log-level 3	이 명령은 엔트리가 ACL 로그(acllog)에 기록되기 전에 일치해야 하 깅 레벨을 지정합니다. 범위는 0~7이고 기본값은 6입니다.
Switch(config)# no acllog match-log-level number	이 명령은 로깅 수준을 기본 설정(6)으로 되돌립니다.

예:switch(config) # acllog match-log 레벨 6 없음	
Switch(config)# 로깅 수준 기능 심각도 수준 예:switch(config)# 로깅 레벨 acllog 3	이 명령을 사용하면 지정된 심각도 수준 이상의 지정된 협업공간에서 시지를 로깅할 수 있습니다.이 문서에서 사용되는 예에서 *acllog* 레벨 3으로 설정되고 기본 설정은 2입니다.
Switch(config)# no logging level [facility severity-level](로깅 레벨 없음) 예:switch(config) # 로깅 수준이 없습니다. acl로그 3	이 명령은 지정된 협업공간의 로깅 심각도 수준을 기본 레벨로 재설정 니다.협업공간과 심각도를 지정하지 않은 경우 레벨, 디바이스는 모든 시설을 기본 레벨로 재설정합니다.이 문서에서 용되는 예에서는 acllog가 기본값(2)으로 돌아갑니다.
Switch(config)# logfile logfile-name severity-level [size bytes] 로깅 예:switch(config)# 로그 파일 로깅 acllog 3	이 명령은 시스템 메시지를 저장하기 위해 사용되는 로그 파일의 이름 로깅이 발생하기 전의 최소 심각도 수준을 구성합니다.선택적으로 최 파일 크기를 지정할 수 있습니다.기본 심각도 수준은 5이고 기본 파일 기는 10,485,760입니다.
Switch(config)# 로그 파일 없음 [logfile-name severity-level [size bytes]] 예:switch(config)# 로그 파일 로그 파일 없음 acllog 3	이 명령은 로그 파일에 대한 로깅을 비활성화합니다.

참고:로그 메시지를 로그에 입력하려면 ACL 로그 기능(acllog) 및 로그 파일의 로깅 심각도 수준이 ACL 로그 *일치/ 로그* 수준 설정보다 크거나 같아야 합니다.

지침 및 제한 사항

다음은 이 문서에 설명된 컨피그레이션을 적용하기 전에 고려해야 할 몇 가지 중요한 지침과 제한 사항입니다.

- Nexus 7000 및 7700 Series 스위치는 OAL만 지원합니다.
- ACL 로깅은 ACL 캡처 기능에서 작동하지 않습니다.
- 이그레스 ACL의 log 옵션은 멀티캐스트 패킷에 지원되지 않습니다.
- IPv6 패킷에는 자세한 로깅 지원을 사용할 수 없습니다.
- acllog *기능* 및 *로깅 로그* 심각도에 대한 로깅 수준은 acllog match-log-level 설정보다 크거나 같도록 구성해야 합니다.
- OAL이 사용되는 동안 **hardware access-list capture** 명령을 사용하지 마십시오. 이 명령을 OAL과 함께 사용하고 ACL 캡처를 활성화하면 모든 VDC(가상 장치 컨텍스트)에 대해 ACL 로깅이 비활성화되고 있음을 알리는 경고 메시지가 나타납니다. ACL 캡처를 비활성화하면 ACL 로깅이 활성화됩니다.이 프로세스가 제대로 작동하려면 no **hardware access-list capture** 명령을 사용하여 **비활성화합니다**.