Nexus 7000 Series 스위치 ACL 캡처 예

목차

소개

ACL(Access Control List) 캡처는 인터페이스 또는 VLAN(Virtual Local Area Network)에서 트래픽을 선택적으로 캡처할 수 있는 기능을 제공합니다. ACL 규칙에 대해 캡처 옵션을 활성화하면 이 규칙과 일치하는 패킷은 지정된 허용 또는 거부 작업에 따라 전달 또는 삭제되며 추가 분석을 위해 대체 대상 포트로 복사할 수도 있습니다. 캡처 옵션이 있는 ACL 규칙을 적용할 수 있습니다.

1. VLAN에서는
2. 모든 인터페이스의 인그레스 방향에서는
3. 모든 레이어 3 인터페이스의 이그레스 방향에서

이 기능은 Nexus 7000 NX-OS 릴리스 5.2 이상에서 지원됩니다. 이 문서에서는 이 기능을 구성하는 방법에 대한 빠른 참조 설명서의 예를 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Nexus 7000(릴리스 5.2.x 이상)
- M1 시리즈 라인 카드

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

ACL 컨피그레이션 예

다음은 가상 LAN VACL(Access Control List) 캡처라고도 하는 VLAN에 적용되는 ACL 캡처의 예제 컨피그레이션입니다.지정된 10기가비트 스니퍼는 모든 스캐너에서 적합하지 않을 수 있습니다.트래픽 양이 많은 경우 문제 해결 과정에서 선택적인 트래픽 캡처가 특히 이러한 시나리오에서 매우 유용할 수 있습니다.

```
!! Global command required to enable ACL-capture feature (on default VDC)
hardware access-list capture

monitor session 1 type acl-capture
destination interface ethernet 2/1
no shut
exit
!!
ip access-list TEST_ACL
10 permit ip 216.113.153.0/27 any capture session 1
20 permit ip 198.113.153.0/24 any capture session 1
30 permit ip 47.113.0.0/16 any capture session 1
40 permit ip any any
!!
!! Note: Capture session ID matches with the monitor session ID
!!
vlan access-map VACL_TEST 10
match ip address TEST_ACL
action forward
statistics per-entry
!!
vlan filter VACL_TEST vlan-list 500
```

액세스 목록의 TCAM(Ternary Content Addressable Memory) 프로그래밍도 확인할 수 있습니다.이 출력은 모듈 1의 VLAN 500에 대한 것입니다.

```
N7k2-VPC1# show system internal access-list vlan 500 input statistics

slot 1
=======

INSTANCE 0x0
---------------

Tcam 1 resource usage:
----------------------
Label_b = 0x802
Bank 0
------
IPv4 Class
Policies: VACL(VACL_TEST)
```

```
Netflow profile: 0
Netflow deny profile: 0
Entries:
[Index] Entry [Stats]
---------------------
[0006:0005:0005] permit ip 216.113.153.0/27 0.0.0.0/0 capture [0]
[0009:0008:0008] permit ip 198.113.153.0/24 0.0.0.0/0 capture [0]
[000b:000a:000a] permit ip 47.113.0.0/16 0.0.0.0/0 capture [0]
[000c:000b:000b] permit ip 0.0.0.0/0 0.0.0.0/0 [0]
[000d:000c:000c] deny ip 0.0.0.0/0 0.0.0.0/0 [0]
```

주의 사항

1. VDC(Virtual Device Contexts)를 통해 시스템에서 지정된 시간에 하나의 ACL 캡처 세션만 활성화할 수 있습니다.
2. Nexus 7000 F1 Series 모듈은 ACL 캡처를 지원하지 않습니다.
3. Nexus 7000 F2 Series 모듈은 현재 ACL 캡처를 지원하지 않지만 로드맵에 있을 수 있습니다.
4. Nexus 7000 M2 시리즈 모듈의 ACL 캡처는 Cisco NX-OS 릴리스 6.1(1) 이상에서 지원됩니다.
5. Nexus 7000 M1-Series 모듈의 ACL 캡처는 Cisco NX-OS 릴리스 5.2(1) 이상에서 지원됩니다.
6. ACL 캡처는 ACL 로깅과 호환되지 않습니다. 따라서 **log** 키워드가 있는 ACL이 있는 경우 **하드웨어 액세스 목록 캡처**를 전역적으로 입력한 후에는 작동하지 않습니다.
7. 버그 CSCug20139로 인해 이 문서의 예제는 버그가 해결될 때까지 ACL이 아닌 ACE당 **캡처 세션**으로 문서화됩니다.

관련 정보

- Cisco Nexus 7000 Series NX-OS 보안 컨피그레이션 가이드, 릴리스 6.x, IP ACL의 컨피그레이션 예
- 기술 지원 및 문서 – Cisco Systems