Nexus 7000 ACL 캡처/VACL 지원 및 제한 사항 FAQ

목차

소개
Q. ACL 캡처의 활용 사례는 무엇입니까?
Q. Nexus 7000 스위치에서 구성할 수 있는 ACL 캡처 세션은 몇 개입니까?
Q. M1 모듈은 ACL 캡처를 지원합니까?
Q. M2 모듈은 ACL 캡처를 지원합니까?
Q. F1 모듈은 ACL 캡처를 지원합니까?
Q. F2 모듈은 ACL 캡처를 지원합니까?
Q. ACL 캡처를 적용할 수 있는 인터페이스와 방향은 무엇입니까?
Q. ACL 캡처 기능에 특별한 제한이 있습니까?
Q. ACL 캡처를 수행하고 특정 트래픽이 목적지 인터페이스 X로 나가고, 특정 트래픽이 목적지 인터페이스 Y로 나가고, 다른 트래픽이 목적지 인터페이스 Z로 나가는 것을 허용할 수 있습니까?
Q. 단일 소스 VLAN 이상에 ACL 캡처를 적용할 수 있습니까?
Q. Nexus 7010에서 구성할 수 있는 활성 L2 VACL은 몇 개입니까?
Q. VACL 캡처는 라우티드 트래픽에 어떻게 적용됩니까?
Q. 섀시에 M1과 M2 카드를 혼합하면 VACL 사용에 영향을 줍니까?
Q. Nexus 7000의 ACL 캡처 기능에 대한 몇 가지 샘플 컨피그레이션은 무엇입니까?
관련 정보

소개

이 문서에서는 인터페이스 또는 VLAN의 트래픽을 선택적으로 모니터링하기 위해 사용되는 ACL(Access Control List) 캡처 기능에 대해 설명합니다.ACL 규칙에 대해 캡처 옵션을 활성화하면 이 규칙과 일치하는 패킷은 지정된 작업에 따라 전달 또는 삭제되며 추가 분석을 위해 대체 대상 포트로 복사될 수도 있습니다.

Q. ACL 캡처의 활용 사례는 무엇입니까?

A. 이 기능은 Catalyst 6000 Series 스위치 플랫폼에서 지원되는 VACL(VLAN Access Control List) 캡처 기능과 유사합니다.인터페이스 또는 VLAN에서 트래픽을 선택적으로 모니터링하도록 ACL 캡처를 구성할 수 있습니다.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 복사될 수도 있습니다.

Q. Nexus 7000 스위치에서 구성할 수 있는 ACL 캡처 세션은 몇

개입니까?

A. VDC(Virtual Device Contexts) 전체에서 시스템에서 지정된 시간에 하나의 ACL 캡처 세션만 활성화할 수 있습니다. ACL TCAM(Ternary Content Addressable Memory)은 VACL에 가능한 한 많은 ACE(Application Control Engine)를 포함할 수 있습니다.

Q. M1 모듈은 ACL 캡처를 지원합니까?

A. 네.M1 모듈의 ACL 캡처는 Cisco NX-OS Release 5.2(1) 이상에서 지원됩니다.

Q. M2 모듈은 ACL 캡처를 지원합니까?

A. 네.M2 모듈의 ACL 캡처는 Cisco NX-OS 릴리스 6.1(1) 이상에서 지원됩니다.

Q. F1 모듈은 ACL 캡처를 지원합니까?

A. F1-Series 모듈은 ACL 캡처를 지원하지 않습니다.

Q. F2 모듈은 ACL 캡처를 지원합니까?

A. F2-Series 모듈은 현재 ACL 캡처를 지원하지 않지만 로드맵에 있을 수 있습니다.BU(Business Unit)에 문의하여 확인합니다.

Q. ACL 캡처를 적용할 수 있는 인터페이스와 방향은 무엇입니까?

A. 캡처 옵션이 있는 ACL 규칙을 적용할 수 있습니다.

- VLAN에서
- 모든 인터페이스의 인그레스 방향
- 모든 레이어 3 인터페이스의 이그레스 방향

Q. ACL 캡처 기능에 특별한 제한이 있습니까?

A. 네.ACL 캡처 기능의 몇 가지 제한 사항은 다음과 같습니다.

- ACL 캡처는 하드웨어 지원 기능이며 관리 인터페이스 또는 수퍼바이저에서 시작되는 제어 패킷에 대해 지원되지 않습니다.또한 SNMP 커뮤니티 ACL 및 vty ACL과 같은 소프트웨어 ACL에는 지원되지 않습니다.
- 포트 채널 및 수퍼바이저 인밴드 포트는 ACL 캡처의 대상으로 지원되지 않습니다.
- ACL 캡처 세션 대상 인터페이스는 인그레스 포워딩 및 인그레스 MAC 학습을 지원하지 않습니다.대상 인터페이스가 이러한 옵션으로 구성된 경우 모니터는 ACL 캡처 세션을 중지합니다

.show monitor **session all** 명령을 사용하여 인그레스 포워딩 및 MAC 학습이 활성화되었는지 확인합니다.

- 패킷의 소스 포트와 ACL 캡처 대상 포트는 동일한 패킷 복제 ASIC에 속할 수 없습니다.두 포트가 동일한 ASIC에 속할 경우 패킷이 캡처되지 않습니다.show **monitor session** 명령은 ACL 캡처 대상 포트와 동일한 ASIC에 연결된 모든 포트를 나열합니다.
- **hardware access-list capture** 명령을 입력하기 전에 ACL 캡처 모니터 세션을 구성하는 경우, 세션을 시작하려면 모니터 세션을 종료하고 다시 가동해야 합니다.
- ACL 캡처가 활성화되면 모든 VDC에 대해 ACL을 로깅하고 속도 제한을 사용하는 기능이 비활성화됩니다.

Q. ACL 캡처를 수행하고 특정 트래픽이 목적지 인터페이스 X로 나가고, 특정 트래픽이 목적지 인터페이스 Y로 나가고, 다른 트래픽이 목적지 인터페이스 Z로 나가는 것을 허용할 수 있습니까?

A. 아니오. 대상은 **hardware access-list capture** 명령으로 구성된 하나의 인터페이스만 될 수 있습니다.

Q. 단일 소스 VLAN 이상에 ACL 캡처를 적용할 수 있습니까?

A. 네.VLAN 목록에 여러 VLAN을 지정할 수 있습니다.예를 들면 다음과 같습니다.

```
vlan access-map acl-vlan-first
  match ip address acl-ipv4-first
  match mac address acl-mac-first
  action forward
  statistics per-entry
  vlan filter acl-vlan-first vlan-list 1,2,3
```

Q. Nexus 7010에서 구성할 수 있는 활성 L2 VACL은 몇 개입니까?

A. 지원되는 최대 IP ACL 항목 수는 XL 라인 카드가 없는 디바이스의 경우 64,000이고, XL 라인 카드가 있는 디바이스의 경우 128,000개입니다.

Q. VACL 캡처는 라우티드 트래픽에 어떻게 적용됩니까?

A. VACL 캡처는 재작성 후 발생하므로 VLAN X를 인그레스(ingress)하고 VLAN Y를 이그레스(egress)하는 프레임이 VLAN Y에 캡처됩니다.

Q. 섀시에 M1과 M2 카드를 혼합하면 VACL 사용에 영향을 줍니까?

A. 섀시에 M1과 M2 카드를 혼합하면 VACL 사용에 아무런 영향을 미치지 않습니다.

Q. Nexus 7000의 ACL 캡처 기능에 대한 몇 가지 샘플 컨피그레이션은 무엇입니까?

A. ACL 캡처 지침은 Cisco Nexus 7000 Series NX-OS 보안 컨피그레이션 가이드, 릴리스 6.x에서 확인할 수 있습니다.

다음 예에서는 기본 VDC에서 ACL 캡처를 활성화하고 ACL 캡처 패킷에 대한 대상을 구성하는 방법을 보여줍니다.

```
hardware access-list capture
    monitor session 1 type acl-capture
    destination interface ethernet 2/1
    no shut
    exit
    show ip access-lists capture session 1
```

다음 예에서는 ACL의 ACE에 대한 캡처 세션을 활성화한 다음 인터페이스에 ACL을 적용하는 방법을 보여 줍니다.

```
ip access-list acl1
      permit tcp any any capture session 1
      exit
      interface ethernet 1/11
      ip access-group acl1 in
      no shut
      show running-config aclmgr
```

다음 예에서는 캡처 세션 ACE가 있는 ACL을 VLAN에 적용하는 방법을 보여 줍니다.

```
vlan access-map acl-vlan-first
      match ip address acl-ipv4-first
      match mac address acl-mac-first
      action foward
      statistics per-entry
      vlan filter acl-vlan-first vlan-list 1
      show running-config vlan 1
```

다음 예에서는 전체 ACL에 대해 캡처 세션을 활성화한 다음 인터페이스에 ACL을 적용하는 방법을 보여 줍니다.

```
ip access-list acl2
      capture session 2
      exit
      interface ethernet 7/1
      ip access-group acl1 in
      no shut
      show running-config aclmg
```

관련 정보

- 기술 지원 및 문서 – Cisco Systems