IPv6 ACL이 사용 중인 전체 IPv6 패킷 삭제 확인

목차

소개

이 문서에서는 ACE에 접두사가 모두 0인 IPv6 ACL이 모든 IPv6 패킷과 해당 해결 방법과 일치할 수 있음을 설명합니다.

사전 요구 사항

요구 사항

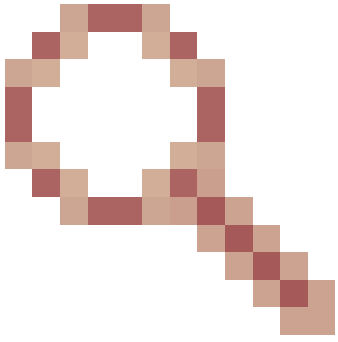
다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS® XR 라우터의 IPv6 ACL(Access Control List) 컨피그레이션
- Cisco IOS® XR 라우터의 ACL 하드웨어 프로그래밍

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IPv6 ACL은 압축 레벨 2 또는 3과 함께 적용됩니다.



- Cisco 버그 ID CSCwe를 수정하지 않은 Cisco IOS® XR [릴리스08250](#)

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

배경 정보

IPv6 주소 ::/128은 RFC(Request For Comments) 4291에서 지정되지 않은 주소로 예약되어 있습니다. 어떤 노드에도 할당해서는 안 되므로 IPv6 Bogon 필터링에서 이 주소를 거부하는 것이 좋습니다.

문제

::/128의 ACE(Access Control Entry)를 포함하는 IPv6 ACL은 적용된 인터페이스의 모든 IPv6 패킷과 일치할 수 있습니다.

실험실에서 이러한 관찰의 예는 아래와 같다.

IPv6 소스 및 목적지 주소와 각각 매칭하는 ::/128을 사용하여 IPv6 ACL 구성:

```
ipv6 access-list PREFIX_ALL_ZERO
 10 remark ** HOST MASK **
 11 deny ipv6 any host :: log
 12 deny ipv6 host :: any log
```

0이 아닌 IPv6 대상 주소로 PING(패킷 인터넷 또는 네트워크 간 그로퍼) 트래픽 전송:

```
RP/0/RP0/CPU0:router#ping fd00:4860:1:1::150 count 100 timeout 0
Thu Sep 14 12:30:23.412 UTC
pings with timeout=0 may result in system instability and
control protocol flaps resulting in traffic impact.
Do you really want to continue[confirm with only 'y' or 'n'] [y/n] :y
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to FD00:4860:1:1::150, timeout is 0 seconds:
....................................................................................................
Success rate is 0 percent (0/100)
```

ACE11에서 패킷을 삭제했습니다.

```
RP/0/RP0/CPU0:router#show access-lists ipv6 PREFIX_ALL_ZERO hardware ingress lo
```

Thu Sep 14 12:30:46.346 UTC
ipv6 access-list PREFIX_ALL_ZERO
11 deny ipv6 any host :: log (100 matches)
12 deny ipv6 host :: any log

ACE 11을 제거할 때 ACE 12로 드롭이 이동합니다.

RP/0/RP0/CPU0:router#clear access-list ipv6 PREFIX_ALL_ZERO hardware ingress location 0/RP0/CPU0
Thu Sep 14 12:31:34.899 UTC

RP/0/RP0/CPU0:router#ping fd00:4860:1:1::150 count 100 timeout 0
Thu Sep 14 12:31:39.482 UTC
pings with timeout=0 may result in system instability and
control protocol flaps resulting in traffic impact.
Do you really want to continue[confirm with only 'y' or 'n'] [y/n] :y
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to FD00:4860:1:1::150, timeout is 0 seconds:
.....
Success rate is 0 percent (0/100)

RP/0/RP0/CPU0:router#show access-lists ipv6 PREFIX_ALL_ZERO hardware ingress location 0/RP0/CPU0
Thu Sep 14 12:31:45.229 UTC
ipv6 access-list PREFIX_ALL_ZERO
12 deny ipv6 host :: any log (100 matches)

이러한 ACE는 소스 또는 목적지 주소가 모두 0인 패킷만 삭제하도록 되어 있습니다.
그러나 모든 트래픽이, 모든 0이 아닌 소스 또는 목적지에서도 삭제되고 있었습니다.

주의: 이 불일치 동작은 예제의 /128뿐만 아니라 ACE의 IPv6 서브넷 마크 길이인 /1에서 /128까지 적용됩니다.

솔루션

Cisco 버그 ID CSCwe08250이 수정된 Cisco IOS® XR 릴리스는 이러한 잘못된 동작을 수정합니다.

해당 수정 없이 실행되는 Cisco IOS® XR 라우터에서는 다음과 같은 해결 방법이 있습니다.

- 하이브리드 ACL을 사용하고 ::/<x>를 ACL에서 네트워크 객체 그룹으로 이동하여 소스 또는 목적지 주소를 모두 0으로 일치시킵니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.