ACL을 통해 루프백에 대한 CPU 바운드 트래픽 차단

목차

소개

이 문서에서는 인터페이스에 적용된 를 통해 CPU 바인딩된 트래픽을 차단하는 데 ACL 대한 제한을 Loopback 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SD-WAN(소프트웨어 정의 WAN)

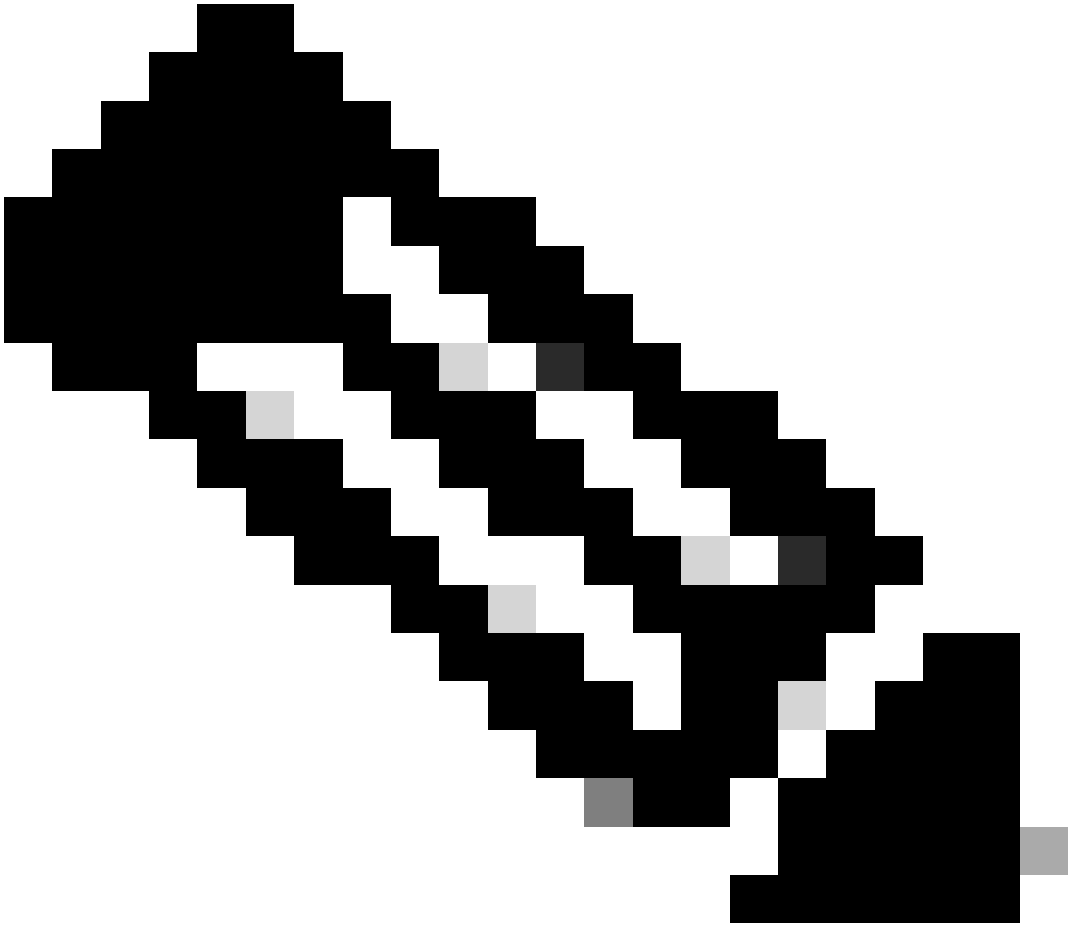
사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- C8000V 버전 17.12.2
- vManage 버전 20.12.2

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.

Q. 를 통해 인터페이스로 향하는 CPU 바인딩 트래픽(예:)ICMP을 Loopback 차단할 수 Access Control List (ACL) 있습니까?



참고: 이 답변은 컨트롤러, 자동 및 SD 라우팅 모드 Cisco IOS® 라우터에 적용됩니다. 컨트롤러 모드 디바이스의 경우 이 응답은 정책 또는 Cisco IOS 컨피그레이션의 명시적 ACL에 적용됩니다.

A. 아닙니다. 인터페이스에 ACLs 적용된 Loopback 트래픽은 라우터의 컨트롤 플레인으로 향하는 트래픽, 즉, punted 트래픽을 차단하지 않습니다.

이는 라우터가 IP로 향하는 모든 트래픽이 제어 평면으로 Loopback 향하는 것임을 깨닫고 하드웨어가 트래픽을 CPU로 직접 전송하고 효율성을 위해 인터페이스를 Loopback 모두 우회하도록 프로그래밍하기 때문입니다. 즉, 트래픽은 인터페이스를 기술적으로 Loopback 인식하지 않으므로 인터페이스의 인그레스(ingress)에 적용되는 모든 것(예: ACLs)이 트리거되지 Loopback 않습니다. 명령을 통해 하드웨어 프로그래밍을 확인할 수 Cisco Express Forwarding® (CEF) 있습니다.

```
Edge#show ip route 10.0.0.1
Routing entry for 10.0.0.1/32
  Known via "connected", distance 0, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Loopback1
      Route metric is 0, traffic share count is 1

Edge#show ip cef exact-route 172.16.0.1 10.0.0.1 protocol 1
172.16.0.1 -> 10.0.0.1 =>receive <<< no mention of Loopback1
```

Ping 패킷에서 FIA 추적을 수행하면 트래픽이 CPU로 전송되고 ACL이 적중되지 않은 것을 확인할 수 있습니다.

```
Edge#show platform packet-trace packet 0 decode
Packet: 0           CBUG ID: 570
Summary
  Input     : GigabitEthernet1
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 1042490936823469 ns (11/26/2024 16:41:12.259675 UTC)
    Stop    : 1042490936851807 ns (11/26/2024 16:41:12.259703 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet1
    Output      :




    Source      : 172.16.0.1
    Destination : 10.0.0.1
    Protocol    : 1 (ICMP)
<... output omitted ...>
  Feature: SDWAN Implicit ACL
    Action : ALLOW
    Reason : SDWAN_SERV_ALL
<... output omitted ...>
  Feature: IPV4_INPUT_LOOKUP_PROCESS_EXT
    Entry       : Input - 0x814f8e80
    Input       : GigabitEthernet1
    Output      : internal0/0/rp:0
    Lapsed time : 2135 ns
<... output omitted ...>
  Feature: INTERNAL_TRANSMIT_PKT_EXT
    Entry       : Output - 0x814cb454
    Input       : GigabitEthernet1
    Output      : internal0/0/rp:0
    Lapsed time : 5339 ns

IOSd Path Flow: Packet: 0    CBUG ID: 570
  Feature: INFRA
  Pkt Direction: IN
    Packet Rcvd From DATAPLANE

  Feature: IP
  Pkt Direction: IN
```

```
    Packet Enqueued in IP layer
    Source      : 172.16.0.1
    Destination : 10.0.0.1
    Interface   : GigabitEthernet1

  Feature: IP
  Pkt Direction: IN
  FORWARDED To transport layer
    Source        : 172.16.0.1
    Destination   : 10.0.0.1
    Interface     : GigabitEthernet1

Edge#show platform packet-trace packet 0 decode | in ACL   <<<<< ACL feature never hit
  Feature: SDWAN Implicit ACL
  Feature: IPV4_SDWAN_IMPLICIT_ACL_EXT

Edge#show platform packet-trace packet 0 decode | in Lo <<<< Loopback1 never mentioned
Edge#
```

CPU 바인딩된 트래픽을 차단하려면 패킷이 먼저 가져오는 인터페이스(예: 물리적 인터페이스 또는)에 ACL을 적용해야 합니다port channel. 여기서는 물리적 인터페이스에 를 적용한 결과를 ACL 볼 수 있다.

```
Edge1#show platform packet-trace packet 0
Packet: 0           CBUG ID: 24
Summary
  Input     : GigabitEthernet1
  Output    : GigabitEthernet1
  State     : DROP 8   (Ipv4Acl)
  Timestamp
    Start   : 5149395094183 ns (11/27/2024 19:48:55.202545 UTC)
    Stop    : 5149395114474 ns (11/27/2024 19:48:55.202565 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet1
    Output      :




    Source      : 172.16.0.1
    Destination : 10.0.0.1
    Protocol    : 1 (ICMP)
<... output omitted ...>
  Feature: IPV4_INPUT_ACL    <<<<
    Entry       : Input - 0x814cc220
    Input       : GigabitEthernet1
    Output      :




    Lapsed time : 15500 ns
```

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.