CPU-gebonden verkeer naar Loopback blokkeren via ACL

Inhoud

Inleiding

In dit document wordt een beperking beschreven voor het blokkeren van CPU-gebonden verkeer via een ACL toepassing op een Loopback interface.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Software-defined Wide Area Network (SD-WAN)

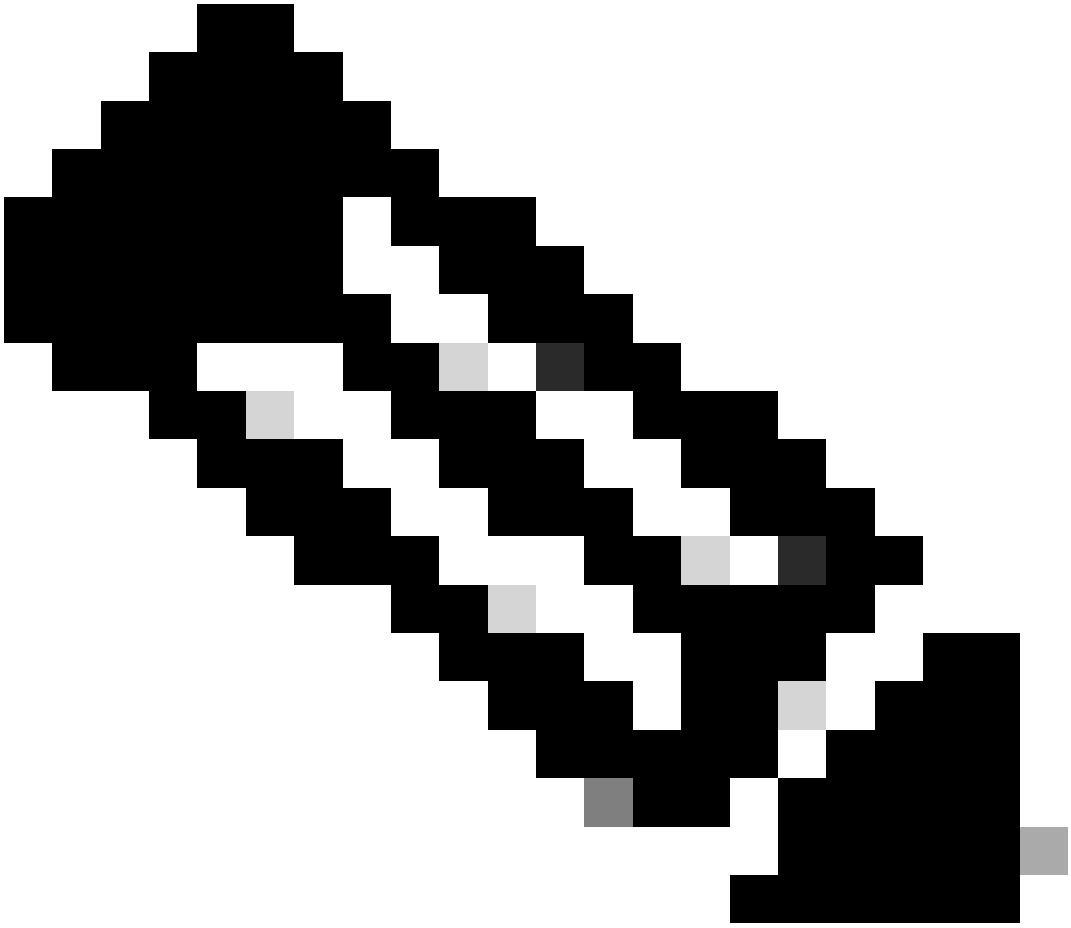
Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C8000V versie 17.12.2
- vManage versie 20.12.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

V. Kunt u CPU-gebonden verkeer (zoals ICMP) blokkeren dat via een interface naar een Loopback andere Access Control List (ACL) interface is gericht?



Opmerking: Dit antwoord is van toepassing op Cisco IOS®-routers met controller-, autonome en SD-routeringsmodus. Voor apparaten in de controllermodus is dit antwoord van toepassing op expliciete ACL's in het beleid of Cisco IOS-configuratie.

A. Nee. ACLs toegepast op Loopback interfaces blokkeren geen verkeer dat bestemd is voor het besturingsvlak van de router, dat wil zeggen puntverkeer.

Dit komt omdat de router, zich realiserend dat elk verkeer dat bestemd is voor het Loopback IP-adres bestemd is voor het besturingsvlak, de hardware programmeert om het verkeer rechtstreeks naar de CPU te sturen en de Loopback interface helemaal te omzeilen voor efficiëntie. Dit betekent dat alles wat wordt toegepast bij het binnendringen van de Loopback interface (bijvoorbeeld ACLs) niet wordt geactiveerd omdat het verkeer technisch nooit de Loopback interface binnendringt. U kunt de programmering van de hardware controleren via een Cisco Express Forwarding® (CEF) opdracht.

```
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
```

Als we een FIA Trace op een ping-pakket nemen, zien we dat het verkeer naar de CPU wordt verzonden en de ACL niet eens wordt geraakt.

```
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#
```

Om CPU-gebonden verkeer te blokkeren, moet u de ACL toepassen op de interface die het pakket voor het eerst binnendringt, bijvoorbeeld de fysieke interface of port channel . Hier zien we het resultaat van het toepassen van de ACL code op de fysieke interface.

```
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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.