Bloqueo del tráfico enlazado a la CPU al loopback a través de ACL

Contenido

Introducción

Este documento describe una limitación en el bloqueo del tráfico enlazado a la CPU a través de una ACL aplicación en una Loopback interfaz.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software (SD-WAN) de Cisco

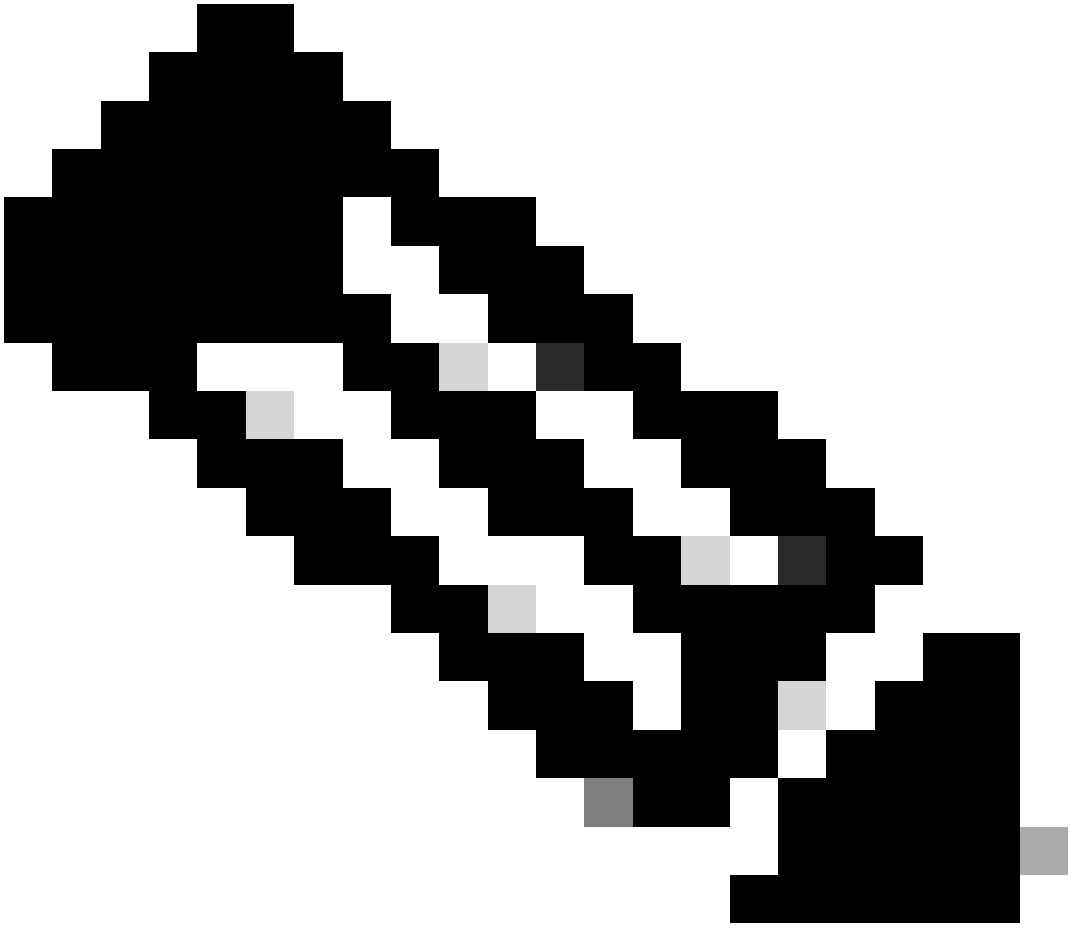
Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- C8000V versión 17.12.2
- vManage versión 20.12.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

P. ¿Puede bloquear el tráfico destinado a la CPU (como ICMP) destinado a una Loopback interfaz a través de Access Control List (ACL) ?



Nota: Esta respuesta se aplica a los routers Cisco IOS® en modo de controlador, autónomo y routing de definición estándar. Para los dispositivos en modo de controlador, esta respuesta se aplica a las ACL explícitas en la configuración de políticas o de Cisco IOS.

R. No. ACLs aplicado a las Loopback interfaces no bloquea el tráfico que está destinado al plano de control del router, es decir, el tráfico impulsado.

Esto se debe a que el router, al darse cuenta de que todo el tráfico destinado hacia la Loopback IP está destinado al plano de control, programa el hardware para enviar el tráfico directamente a la CPU y omitir la Loopback interfaz en conjunto para lograr eficiencia. Esto significa que cualquier cosa que se aplique en el ingreso de la Loopback interfaz (por ejemplo, ACLs) no se activa ya que el tráfico técnicamente nunca ingresa a la Loopback interfaz. Puede verificar la programación de hardware mediante un Cisco Express Forwarding® (CEF) comando.

```
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
```

Si tomamos un Seguimiento FIA en un paquete ping, vemos que el tráfico se envía a la CPU y que la ACL ni siquiera es alcanzada.

```
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#
```

Para bloquear el tráfico enlazado a la CPU, debe aplicar la ACL a la interfaz a la que ingresa el paquete por primera vez, por ejemplo, la interfaz física o port channel . Aquí, podemos ver el resultado de aplicar el ACL en la interfaz física.

```
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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).