Blockieren von CPU-gebundenem Datenverkehr zum Loopback über ACL

Inhalt

Einleitung

Dieses Dokument beschreibt eine Beschränkung bei der Blockierung von CPU-gebundenem Datenverkehr über eine ACL Schnittstelle, die auf eine Loopback Schnittstelle angewendet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

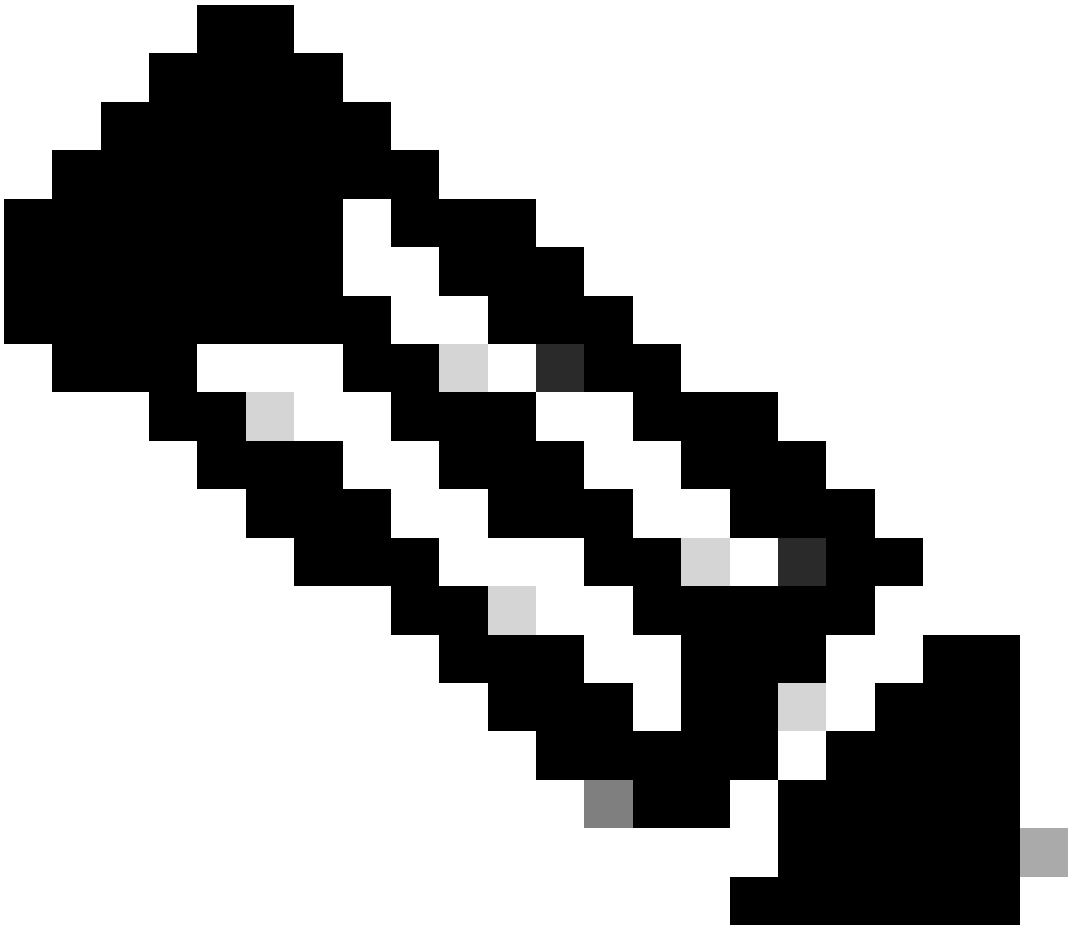
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C8000V Version17.12.2
- vManage, Version 20.12.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Frage: Können Sie CPU-gebundenen Datenverkehr (z. B. ICMP) blockieren, der über eine an eine Loopback Schnittstelle gerichtet ist

Access Control List (ACL) ?



Anmerkung: Diese Antwort gilt für Cisco IOS®-Router im Controller-, autonomen und SD-Routing-Modus. Bei Geräten im Controller-Modus gilt diese Antwort für explizite ACLs in der Richtlinie oder Cisco IOS-Konfiguration.

A. Nein. Bei ACLs Loopback Schnittstellen wird kein Datenverkehr blockiert, der für die Kontrollebene des Routers bestimmt ist, d. h. blockierter Datenverkehr.

Dies liegt daran, dass der Router in der Erkenntnis, dass jeder Datenverkehr, der an die Loopback IP-Adresse gerichtet ist, für die Kontrollebene bestimmt ist, die Hardware so programmiert, dass der Datenverkehr direkt an die CPU gesendet wird, und die Loopback Schnittstelle gemeinsam umgeht, um die Effizienz zu erhöhen. Dies bedeutet, dass alle Daten, die beim Eingang der Loopback Schnittstelle angewendet werden (z. B. ACLs), nicht ausgelöst werden, da der

Datenverkehr technisch gesehen nie in die Loopback Schnittstelle eindringt. Sie können die Hardwareprogrammierung mit einem Cisco Express Forwarding® (CEF) Befehl überprüfen.

```
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
```

Wenn wir einen FIA-Trace auf einem Ping-Paket verwenden, stellen wir fest, dass der Datenverkehr an die CPU gesendet wird und die ACL nicht einmal betroffen ist.

```
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#
```

Um CPU-gebundenen Datenverkehr zu blockieren, müssen Sie die ACL auf die Schnittstelle anwenden, die das Paket zuerst erreicht, z. B. die physische Schnittstelle oder port channel . Hier sehen wir das Ergebnis der Anwendung des auf der physischen ACL Schnittstelle.

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.