通過ACL阻止發往環回的CPU流量

目錄

簡介

本文檔介紹通過介面上應用的來阻止CPU傳ACL輸流量的限Loopback制。

必要條件

需求

思科建議您瞭解以下主題：

- 思科軟體定義廣域網路(SD-WAN)

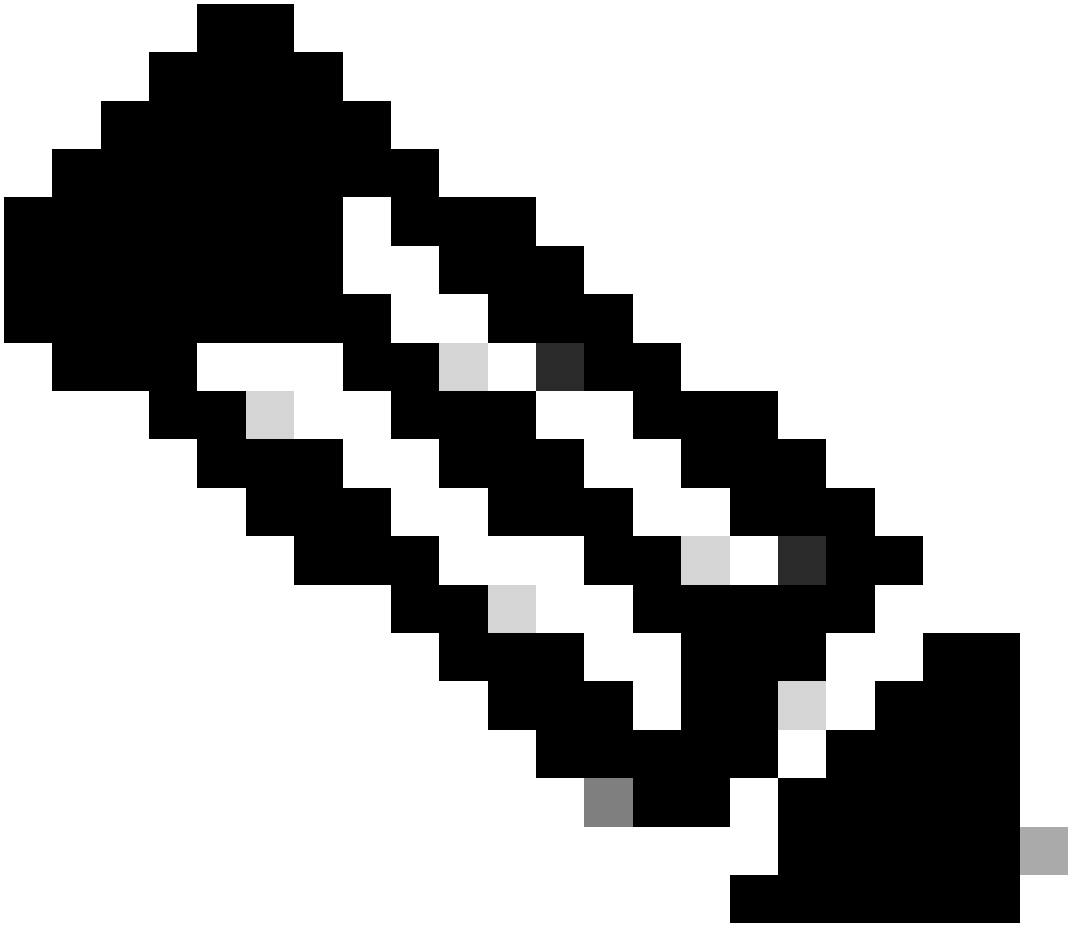
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- C8000V版本17.12.2
- vManage版本20.12.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問：是否可以阻止通過介面發往介面的ICMP發往CPU的流Loopback量(例如Access Control List (ACL))?



附註：此答案適用於控制器、自治和SD路由模式Cisco IOS®路由器。對於控制器模式裝置，此答案適用於策略或Cisco IOS配置中的顯式ACL。

答：否。ACLs應用Loopback於介面不會阻止發往路由器控制平面的流量，即轉發流量。

Loopback這是因為路由器意識到任何目的地為IP的流量都以控制平面為目的地，因此對硬體進行程式設計，以將流量直接傳送到CPU，同時繞過介面以提高效Loopback率。這表示應用於介面輸入的任何內容(例LoopbackACLs如)，都不會被觸發，因為流量從技術角度而言從未進入介Loopback面。您可以通過命令驗證硬體編Cisco Express Forwarding® (CEF)程。

```
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
```

如果對ping資料包進行FIA跟蹤，我們會看到流量被傳送到CPU，ACL甚至未命中。

```
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#
```

為了阻止傳入CPU的流量，您需要將ACL應用到資料包首先接收的介面，例如物理介面或port channel。在這裡，我們可以看到在物理介面ACL上應用的結果。

```
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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。