ACLを介したループバックへのCPUバウンドトラフィックのブロック

内容

はじめに

このドキュメントでは、Loopbackインターフェイスに適用される「ACL」を介してCPUに送られるトラフィックをブロックする際の制限事項について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

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

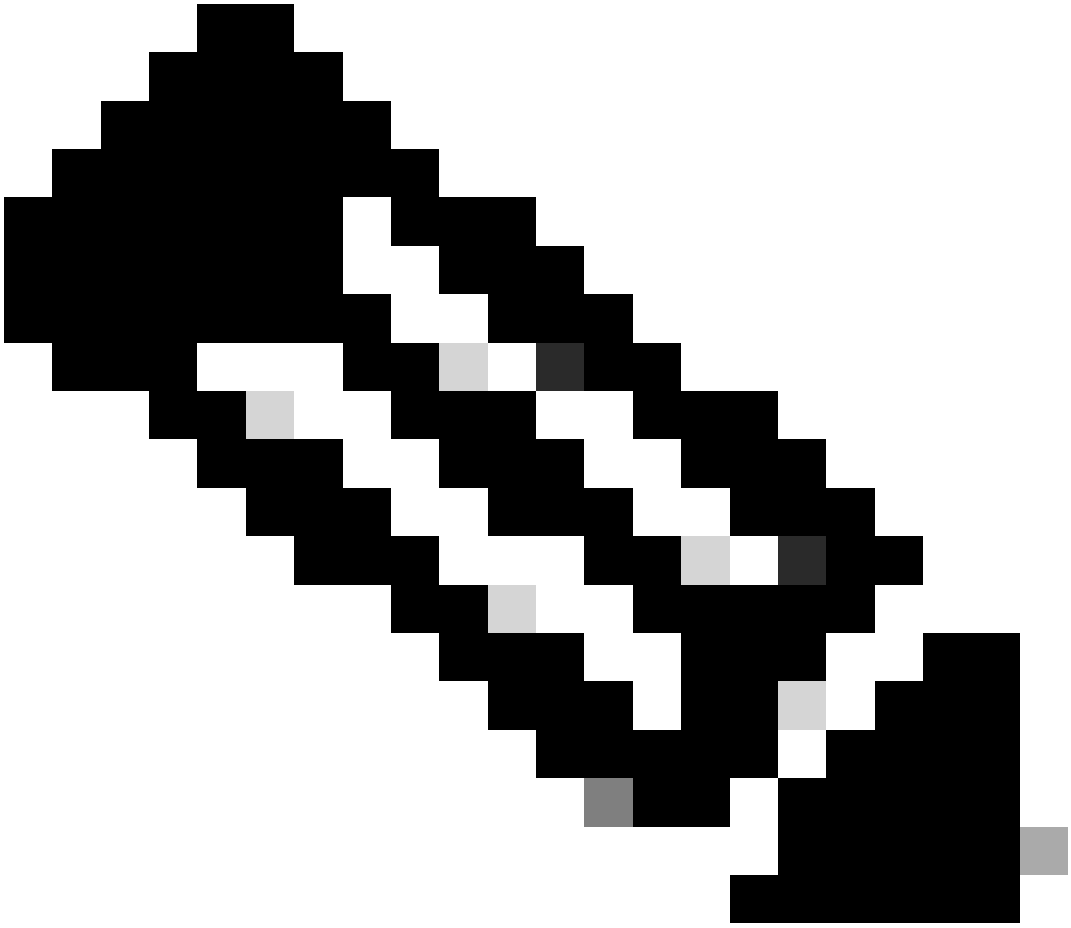
使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- C8000Vバージョン17.12.2
- vManageバージョン20.12.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

Q. Access Control List (ACL)を使用して、Loopbackインターフェイス宛てのCPUバウンドトラフィック(「ICMP」など)をブロックできますか。



注：この回答は、コントローラ、自律、およびSDルーティングモードのCisco IOS®ルータに適用されます。コントローラモードデバイスの場合、この答えはポリシーまたはCisco IOS設定の明示的ACLに適用されます。

A.いいえ。ACLsがLoopbackインターフェイスに適用されていても、ルータのコントロールプレーンを宛先とするトラフィック（つまり、パントされたトラフィック）はブロックされません。

これは、ルータが、Loopback IPに向かうトラフィックはすべてコントロールプレーンに向けられることを認識し、効率を高めるために、トラフィックを直接CPUに送信し、Loopbackインターフェイスをすべてバイパスするようにハードウェアをプログラムしているためです。これは、トラフィックが技術的にはインターフェイスに入ってこないため、Loopbackインターフェイスの入力に適用されるもの(たとえば、 ACLs)はトリガーされないことを意味しLoopbackます。ハードウェアのプログラミングは、「Cisco Express Forwarding® (CEF)」コマンドを使用して確認できます。

```
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パケットでFIAトレースを取得すると、トラフィックがCPUに送信され、ACLがヒットさえしていないことがわかります。

```
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に送られるトラフィックをブロックするには、パケットが最初に入力するインターフェイスにACLを適用する必要があります。たとえば、物理インターフェイスやport channelなどです。ここでは、物理インターフェイスにACLを適用した結果を確認できます。

```
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
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。