Blocca traffico associato alla CPU su loopback tramite ACL

Sommario

Introduzione

In questo documento viene descritto un limite nel bloccare il traffico basato sulla CPU tramite un'ACLinterfaccia applicata a un'Loopbackinterfaccia.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

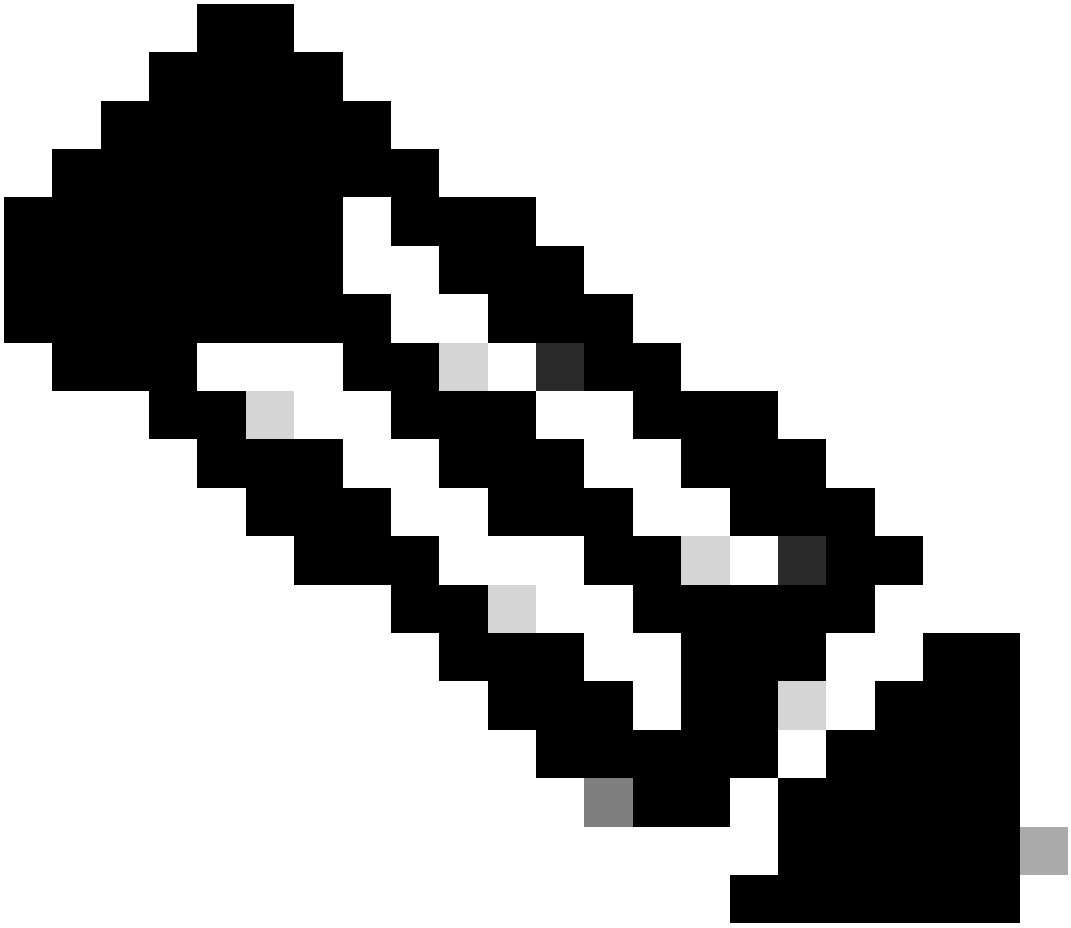
Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- C800V versione 17.12.2
- vManage versione 20.12.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

D. È possibile bloccare il traffico basato sulla CPU (ad esempio ICMP) destinato a un'Loopbackinterfaccia tramite un Access Control List (ACL) ?



Nota: La risposta è valida per i router Cisco IOS® in modalità controller, autonoma e routing SD. Per i dispositivi in modalità controller, questa risposta si applica agli ACL espliciti nella policy o nella configurazione di Cisco IOS.

A. No. ACLs applicato alle Loopback interfacce non blocca il traffico destinato al control plane del router, ossia il traffico puntato.

Infatti, rendendosi conto che il traffico diretto all'LoopbackIP è destinato al control plane, il router programma l'hardware in modo da inviare il traffico direttamente alla CPU e ignorare l'Loopbackinterfaccia per migliorare l'efficienza. Ciò significa che gli elementi applicati all'ingresso dell'Loopbackinterfaccia (ad esempio, ACLs) non vengono azionati in quanto il traffico non entra mai tecnicamente nell'Loopbackinterfaccia. È possibile verificare la programmazione hardware tramite 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
```

Se prendiamo una FIA Trace su un pacchetto ping, vediamo che il traffico viene inviato alla CPU e l'ACL non viene nemmeno colpito.

```
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#
```

Per bloccare il traffico basato sulla CPU, è necessario applicare l'ACL all'interfaccia usata dal pacchetto per primo, ad esempio l'interfaccia fisica o il router port channel . Qui possiamo vedere il risultato dell'applicazione della ACL sull'interfaccia fisica.

```
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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).