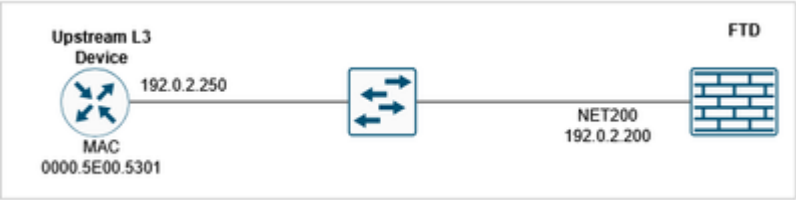
Risoluzione dei problemi relativi a FTD Impossibile eseguire il ping del dispositivo upstream nonostante si disponga di una voce ARP

Sommario

Problema

Firewall Threat Defense (FTD) non è stato in grado di eseguire il ping dell'indirizzo IP del dispositivo upstream, nonostante il firewall sia in grado di osservare la voce ARP dell'indirizzo IP upstream. La tabella ARP mostra le voci previste, indicando che la connettività di layer 2 funziona ma il traffico ping di layer 3 è bloccato.

Topologia



Sintomi FTD CLI

Ping sull'indirizzo IP upstream non riuscito:

<#root>

```
device#
```

ping 192.0.2.250

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.250, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

Esiste una voce ARP per l'indirizzo IP a monte:

<#root>

```
device#
```

show arp

NET200 192.0.2.250 0000.5e00.5301

47

Abilitare un'acquisizione con traccia sull'interfaccia FTD:

<#root>

```
device#
```

capture CAPI interface NET200 trace match icmp host 192.0.2.200 host 192.0.2.250

I syslog di FTD LINA durante il test ping:

<#root>

```
device#
```

show log | include 192.0.2.250

```
May 15 2026 09:46:26: %FTD-6-302020: Built outbound ICMP connection for faddr 192.0.2.250/0 gaddr 192.0
May 15 2026 09:46:26: %FTD-3-313001:
```

Denied ICMP type=0, code=0 from 192.0.2.250 on interface NET200

```
May 15 2026 09:46:26: %FTD-6-302021: Teardown ICMP connection for faddr 192.0.2.250/0 gaddr 192.0.2.200
...
```

L'acquisizione del pacchetto mostra l'arrivo di risposte echo ICMP:

<#root>

```
device#

show capture CAPI


10 packets captured
   1: 09:46:26.649456       802.1Q vlan#200 P0 192.0.2.200 > 192.0.2.250 icmp: echo request
   2: 09:46:26.649883       802.1Q vlan#200 P0 192.0.2.250 > 192.0.2.200 icmp:

echo reply


   3: 09:46:28.642621       802.1Q vlan#200 P0 192.0.2.200 > 192.0.2.250 icmp: echo request
   4: 09:46:28.643002       802.1Q vlan#200 P0 192.0.2.250 > 192.0.2.200 icmp:

echo reply


...
```

La traccia del pacchetto della risposta echo ICMP mostra che il pacchetto corrisponde a una connessione esistente come previsto e l'interfaccia di output è l'interfaccia FTD (NP Identity Ifc):

<#root>

```
device#

show capture CAPI packet-number 2 trace


10 packets captured
   2: 09:46:26.649883       802.1Q vlan#200 P0 192.0.2.250 > 192.0.2.200 icmp:

echo reply


...
Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 4096 ns
Config:
```

```
Additional Information:

Found flow with id 1400, using existing flow


...

Result:
input-interface: NET200(vrfid:0)
input-status: up
input-line-status: up

output-interface: NP Identity Ifc


Action: allow
Time Taken: 28672 ns
```

La traccia di debug ICMP indica che la risposta echo ICMP è stata negata:

<#root>

```
FTD220-5#

debug icmp trace


debug icmp trace enabled at level 1

FTD220-5#

ping 192.0.2.250


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.250, timeout is 2 seconds:
ICMP echo request from self:192.0.2.200 to NET200:192.0.2.250 ID=49503 seq=15001 len=72

ICMP echo reply




from NET200:192.0.2.250 to self:192.0.2.200


 ID=49503 seq=15001 len=72

Denied ICMP type = 0, code = 0 from 192.0.2.250on interface 4


?
```

```
...
Success rate is 0 percent (0/5)
```

⚠ Attenzione: Utilizzare i debug con cautela.

Per disattivare il debug ICMP:

<#root>

```
device#

no debug icmp trace

debug icmp trace disabled.
```

Ambiente

FTD 10.x Il problema riguarda anche altre versioni del software.

Risoluzione

Il problema è stato risolto identificando e correggendo una configurazione di regola ICMP nelle impostazioni della piattaforma che negava il traffico ping. La risoluzione prevedeva le seguenti fasi:

Passaggio 1. Verifica delle voci della tabella ARP

Confermare che le voci ARP per l'indirizzo IP upstream siano visibili nella tabella ARP del firewall, a indicare che la connettività di layer 2 funziona correttamente:

<#root>

device#

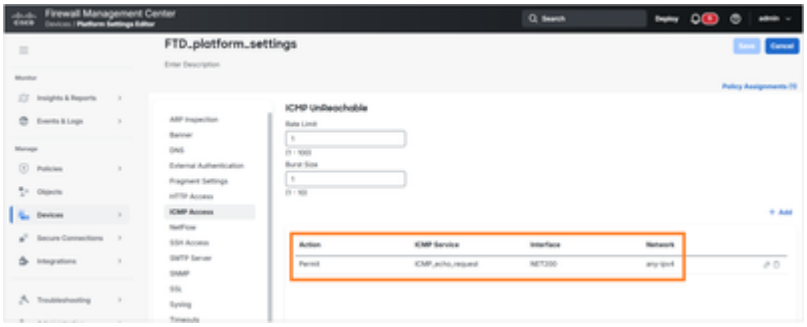
show arp

Passaggio 2. Controllare le impostazioni della piattaforma per le regole ICMP

Passare alla configurazione delle impostazioni della piattaforma ed esaminare i criteri delle regole ICMP che possono influire sul traffico ping. Cercare in modo specifico le regole che potrebbero bloccare o negare i pacchetti di richiesta/risposta echo ICMP.

Passaggio 3. Identificare e modificare la regola ICMP di blocco

Individuare la regola ICMP nelle impostazioni della piattaforma configurate per impedire il traffico ping.



Nell'esempio, la regola ICMP consente solo alle richieste echo ICMP di essere accettate dall'interfaccia FTD.

Verifica CLI FTD:

<#root>

device#

show run icmp

```
icmp unreachable rate-limit 1 burst-size 1

icmp permit any echo NET200
```

Passaggio 4. Aggiornamento della configurazione della regola ICMP

Modificare la regola ICMP identificata in modo da consentire il traffico ping o rimuovere la configurazione di blocco in base ai requisiti di sicurezza della rete e alle esigenze operative.

Regola ICMP risultante:

<#root>

```
device#

show run icmp


icmp unreachable rate-limit 1 burst-size 1
icmp permit any echo NET200

icmp permit 192.0.2.0 255.255.255.0 echo-reply NET200
```

Passaggio 5. Verifica della connettività

Dopo aver apportato le modifiche alla configurazione, verificare la connettività ping all'indirizzo IP upstream per verificare che il problema sia stato risolto e che il traffico ICMP stia ora scorrendo correttamente:

<#root>

```
device#

ping 192.0.2.250


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.250, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5)

, round-trip min/avg/max = 1/1/1 ms
```

Causa

La causa principale di questo problema è stata una regola ICMP configurata nelle impostazioni della piattaforma che negava esplicitamente il traffico delle risposte echo ICMP. Mentre il firewall manteneva la corretta connettività di layer 2 (evidenziata dalle voci ARP visibili), la regola ICMP a livello di piattaforma bloccava i pacchetti di risposta echo ICMP di layer 3, impedendo il corretto completamento delle operazioni ping sull'indirizzo IP upstream. Questo tipo di configurazione può verificarsi quando vengono implementati criteri di sicurezza per limitare il traffico ICMP, ma può influire inavvertitamente su test e monitoraggio legittimi della connettività di rete.

Contenuto correlato

- https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/100/management-center-device-config-10-0/interfaces-settings-platform.html#task_42BBA666CD604517ADA18B32CA162F62
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/I-R/asa-command-ref-I-R/ia-inr-commands.html#wp1366339900
- Supporto tecnico Cisco e download

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).