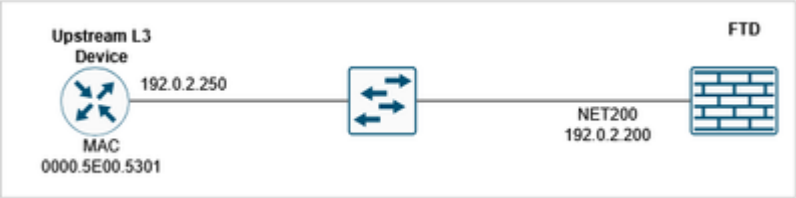
疑難排解FTD無法對ARP專案所在的上游裝置執行Ping操作

目錄

問題

防火牆威脅防禦(FTD)無法ping通上游裝置IP地址，儘管防火牆能夠觀察上游IP地址的ARP條目。ARP表顯示了預期的條目，表明第2層連線正常，但第3層ping流量被阻止。

拓撲



FTD CLI症狀

對上游IP地址執行ping操作失敗：

<#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)
```

上游IP地址有一個ARP條目：

```
<#root>

device#

show arp



NET200 192.0.2.250 0000.5e00.5301

 47
```

在FTD介面上啟用含有追蹤軌跡的擷取：

```
<#root>

device#

capture CAPI interface NET200 trace match icmp host 192.0.2.200 host 192.0.2.250
```

FTD LINA在ping測試期間的系統日誌：

```
<#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
...
```

封包擷取顯示到達的ICMP回應回應：

<#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

...

ICMP回應回覆的封包追蹤軌跡顯示封包正按預期與現有連線相符，而輸出介面是FTD介面（NP身分識別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
```

Debug ICMP trace顯示ICMP回應回覆被拒絕：

<#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)
```

注意：請謹慎使用debug!

關閉ICMP調試：

```
<#root>
device#
no debug icmp trace

debug icmp trace disabled.
```

環境

FTD 10.x。其他軟體版本也會受到影響。

解析

通過識別並更正平台設定中拒絕ping流量的ICMP規則配置解決了此問題。決議涉及以下步驟：

步驟1.檢驗ARP表條目

確認上游IP地址的ARP條目在防火牆的ARP表中可見，這表明第2層連線運行正常：

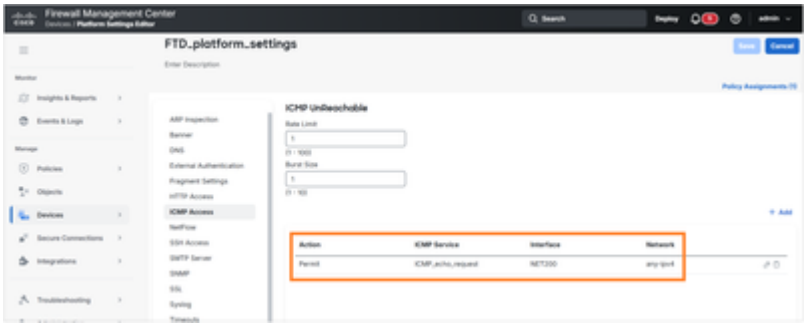
```
<#root>
device#
show arp
```

步驟2.檢查ICMP規則的平台設定

導航到平台設定配置並檢查可能影響ping流量的ICMP規則策略。請特別查詢可能阻塞或拒絕ICMP回應請求/應答資料包的規則。

步驟3.識別並修改阻塞ICMP規則

在配置為拒絕ping流量的平台設定中找到ICMP規則。



在本範例中，ICMP規則僅允許FTD介面接受ICMP回應要求。

FTD CLI驗證：

<#root>

device#

show run icmp

icmp unreachable rate-limit 1 burst-size 1

icmp permit any echo NET200

步驟4.更新ICMP規則配置

根據網路安全要求和運行需要，修改識別的ICMP規則以允許ping流量或刪除阻塞配置。

產生的ICMP規則：

<#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

步驟5.測試連通性

更改配置後，測試對上游IP地址的ping連通性，以驗證問題是否已解決以及ICMP流量現在是否正常流動：

<#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

原因

此問題的根本原因是平台設定中配置的ICMP規則明確拒絕ICMP回應應答流量。雖然防火牆維持了正確的第2層連線（以可見的ARP條目為證據），但平台級ICMP規則阻塞了第3層ICMP回應應答資料包，阻止對上游IP地址成功執行ping操作。當實施安全策略以限制ICMP流量但可能無意中影響合法網路連線測試和監控時，可能會發生此類配置。

相關內容

- 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
- 思科技術支援與下載

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）。