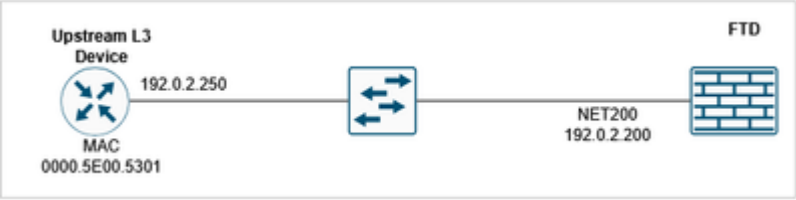
排除FTD故障，即使存在ARP条目，也无法Ping上游设备

目录

问题

防火墙威胁防御(FTD)无法ping通上游设备的IP地址，尽管防火墙能够观察上游IP地址的ARP条目。ARP表显示了预期的条目，表明第2层连接正常，但第3层ping流量被阻止。

拓扑



FTD CLI症状

对上游IP地址执行ping操作失败：

```
<#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地址有一个ARP条目：

```
<#root>
device#
show arp


NET200 192.0.2.250 0000.5e00.5301
 47
```

在FTD接口上启用带有跟踪的捕获：

```
<#root>
device#
capture CAPI interface NET200 trace match icmp host 192.0.2.200 host 192.0.2.250
```

FTD LINA在ping测试期间的系统日志：

```
<#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
...
```

数据包捕获显示到达的ICMP回应应答：

```
<#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回应应答的数据包跟踪显示数据包按预期匹配现有连接，并且输出接口为FTD接口（NP身份lfc）：

```
<#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显示ICMP回应应答被拒绝：

<#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)
```

⚠警告：请谨慎使用调试！

要关闭ICMP调试，请执行以下操作：

<#root>

device#

no debug icmp trace

debug icmp trace disabled.

环境

FTD 10.x。其他软件版本也会受到影响。

分辨率

通过在拒绝ping流量的平台设置中识别和纠正ICMP规则配置，解决了此问题。

解决方案涉及以下步骤：

步骤1.检验ARP表条目

确认上游IP地址的ARP条目在防火墙的ARP表中可见，表明第2层连接运行正常：

<#root>

device#

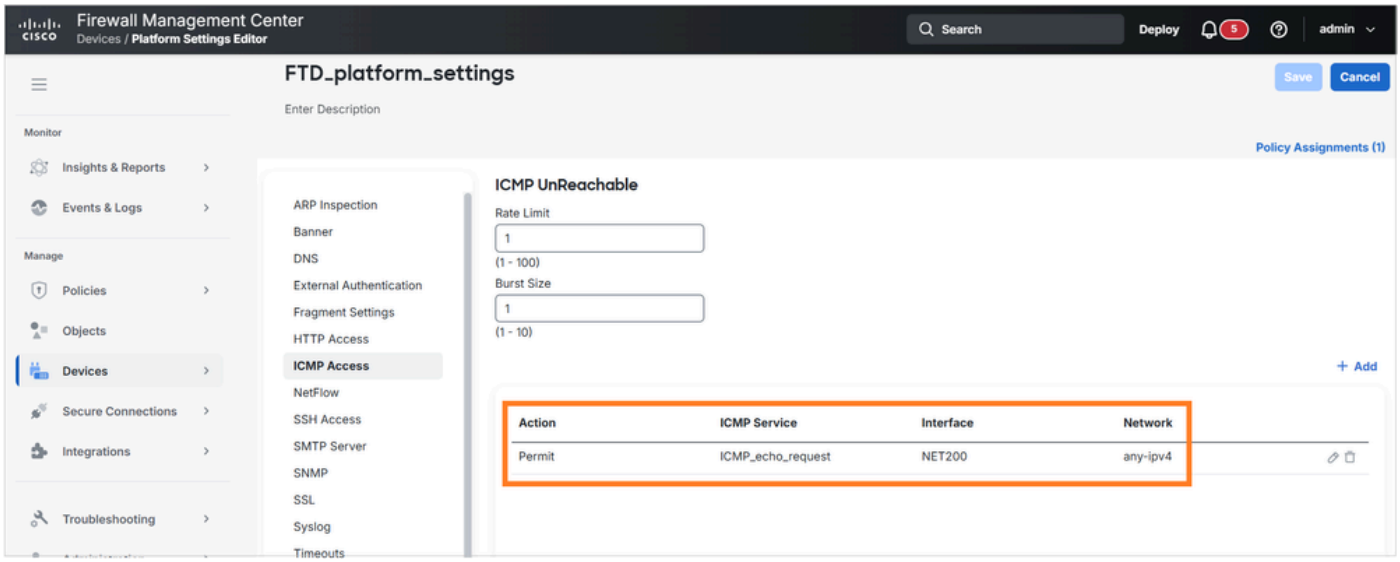
show arp

步骤2.检查ICMP规则的平台设置

导航到平台设置配置并检查可能影响ping流量的ICMP规则策略。请具体查找可能阻止或拒绝ICMP回应请求/应答数据包的规则。

步骤3.识别并修改阻止ICMP规则

在配置为拒绝ping流量的平台设置中找到ICMP规则。



在本示例中，ICMP规则仅允许FTD接口接受ICMP回应请求。

FTD CLI验证：

<#root>

device#

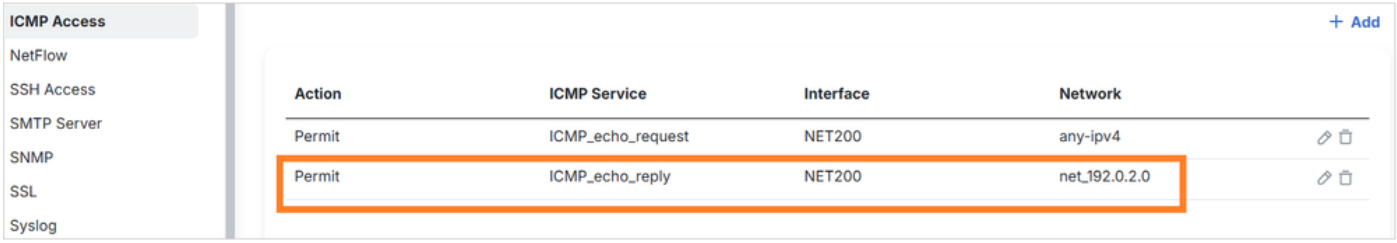
show run icmp

icmp unreachable rate-limit 1 burst-size 1

icmp permit any echo NET200

步骤4.更新ICMP规则配置

根据网络安全要求和运行需要，修改识别的ICMP规则以允许ping流量或删除阻止配置。



生成的ICMP规则：

<#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

步骤5.测试连通性

更改配置后，测试对上游IP地址的ping连接，以检验问题是否已解决以及ICMP流量现在是否正常流动：

<#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

此问题的根本原因是平台设置中配置的ICMP规则明确拒绝ICMP回应应答流量。虽然防火墙保持正确的第2层连接（通过可见的ARP条目证明），但平台级ICMP规则阻止了第3层ICMP回应应答数据包，阻止对上游IP地址成功执行ping操作。当实施安全策略以限制ICMP流量但可能会无意中影响合法网络连接测试和监控时，就会发生此类配置。

相关内容

- 配置ICMP访问
- icmp
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。