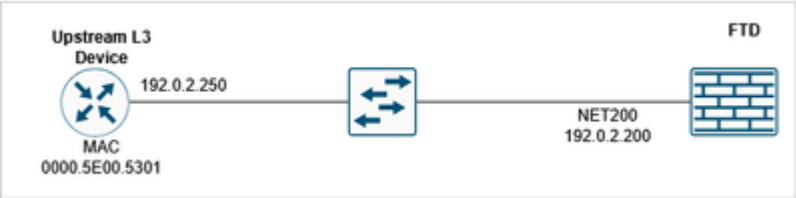
ARPエントリがあるにもかかわらずアップストリームデバイスにpingできないFTDのトラブルシューティング

内容

お問い合わせ内容

ファイアウォールでアップストリームIPアドレスのARPエントリを監視できても、ファイアウォール脅威対策(FTD)はアップストリームデバイスのIPアドレスにpingを実行できませんでした。ARPテーブルには予期されたエントリが表示され、レイヤ2接続は機能しているものの、レイヤ3 pingトラフィックがブロックされていることが示されました。

トポロジ



FTD CLIの症状

アップストリームIPアドレスへのpingが失敗します。

<#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)
```

アップストリームIPアドレスのARPエントリがあります。

<#root>

```
device#
```

show arp

NET200 192.0.2.250 0000.5e00.5301

47

FTDインターフェイスでトレースによるキャプチャを有効にします。

<#root>

```
device#
```

capture CAPI interface NET200 trace match icmp host 192.0.2.200 host 192.0.2.250

pingテスト中のFTD LINA syslog:

<#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
...
```

パケットキャプチャは、ICMPエコー応答が到着したことを示しています。

```
<#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エコー応答のパケットトレースは、パケットが予期したとおりに既存の接続と一致しており、出力インターフェイスがFTDインターフェイス(NP Identity Ifc)であることを示しています。

```
<#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は、ICMPエコー応答が拒否されていることを示します。

```
<#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：デバッグは注意して使用してください。

ICMPデバッグをオフにするには、次のコマンドを実行します。

```
<#root>

device#

no debug icmp trace

debug icmp trace disabled.
```

環境

FTD 10.xがインストールされています。他のソフトウェアバージョンも該当します。

解決策

この問題は、pingトラフィックを拒否するプラットフォーム設定でICMPルール設定を特定して修正することで解決されました。この解決策には、次の手順が含まれています。

ステップ 1：ARPテーブルエントリの確認

アップストリームIPアドレスのARPエントリがファイアウォールのARPテーブルに表示されていることを確認します。これは、レイヤ2接続が正常に機能していることを示します。

```
<#root>

device#
```

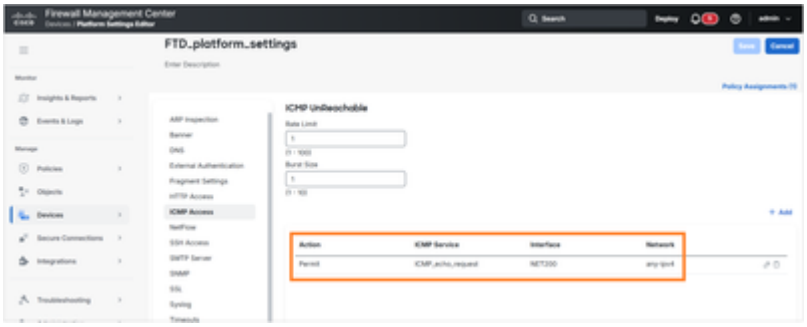
```
show arp
```

ステップ 2プラットフォーム設定でのICMPルールの確認

プラットフォーム設定の設定に移動し、pingトラフィックに影響を与える可能性があるICMPルールポリシーを調べます。特に、ICMPエコー要求/応答パケットをブロックまたは拒否している可能性があるルールを探します。

ステップ 3ブロッキングICMPルールの識別と変更

pingトラフィックを拒否するように設定されたプラットフォーム設定でICMPルールを見つけます。



この例では、ICMPルールにより、FTDインターフェイスでICMPエコー要求の受け入れだけが許可されます。

FTD CLIの検証：

<#root>

device#

```
show run icmp
```

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

```
icmp permit any echo NET200
```

ステップ 4ICMPルール設定の更新

ネットワークセキュリティ要件と運用ニーズに応じて、pingトラフィックを許可するように特定されたICMPルールを変更するか、ブロッキング設定を削除します。

結果のICMPルール：

<#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

ステップ 5接続のテスト

設定を変更した後、アップストリームIPアドレスへのping接続をテストして、問題が解決され、ICMPトラフィックが正しく流れていることを確認します。

<#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

この問題の根本原因は、ICMPエコー応答トラフィックを明示的に拒否するICMPルールがプラットフォーム設定に設定されていたことにあります。ファイアウォールが適切なレイヤ2接続を維持している間（ARPエントリが表示されていることから明らかです）、プラットフォームレベルのICMPルールがレイヤ3 ICMPエコー応答パケットをブロックし、アップストリームIPアドレスに対するping操作の成功を妨げています。このタイプの設定は、ICMPトラフィックを制限するセキュリティポリシーが実装されているときに、正当なネットワーク接続のテストと監視に誤って影響を与える可能性がある場合に発生します。

関連コンテンツ

- 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
- シスコのテクニカルサポートとダウンロード

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。