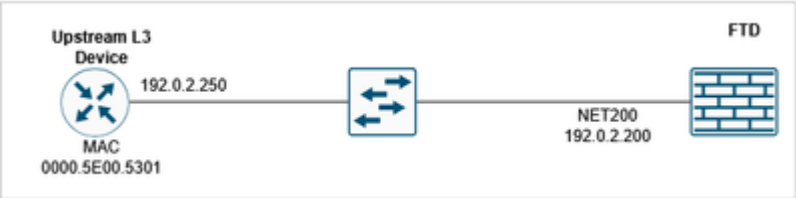
Fehlerbehebung: FTD kann trotz eines ARP-Eintrags keinen Ping an das Upstream-Gerät senden

Inhalt

Problem

Die Firewall Threat Defense (FTD) konnte die IP-Adresse des Upstream-Geräts nicht pingen, obwohl die Firewall den ARP-Eintrag für die Upstream-IP-Adresse überwachen konnte. Die ARP-Tabelle zeigte die erwarteten Einträge an, was darauf hindeutet, dass die Layer-2-Verbindung funktionierte, aber der Layer-3-Ping-Verkehr blockiert wurde.

Topologie



FTD CLI - Symptome

Der Ping an die Upstream-IP-Adresse ist fehlgeschlagen:

<#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)
```

Es gibt einen ARP-Eintrag für die Upstream-IP-Adresse:

<#root>

```
device#
```

show arp

NET200 192.0.2.250 0000.5e00.5301

47

Aktivieren Sie eine Erfassung mit Ablaufverfolgung auf der FTD-Schnittstelle:

<#root>

```
device#
```

capture CAPI interface NET200 trace match icmp host 192.0.2.200 host 192.0.2.250

FTD LINA-Syslogs während des Ping-Tests:

<#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
...
```

Bei der Paketerfassung werden eingehende ICMP-Echoantworten angezeigt:

```
<#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



...
```

Die Paketverfolgung der ICMP-Echoantwort zeigt, dass das Paket erwartungsgemäß mit einer vorhandenen Verbindung übereinstimmt und die Ausgabeschnittstelle die FTD-Schnittstelle (NP Identity Ifc) ist:

```
<#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 zeigt an, dass die ICMP-Echoantwort verweigert wird:

<#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)
```

⚠ Vorsicht: Verwenden Sie Debug-Programme mit Vorsicht!

So deaktivieren Sie das ICMP-Debugging:

<#root>

```
device#

no debug icmp trace


debug icmp trace disabled.
```

Umwelt

FTD 10.x Auch andere Softwareversionen sind betroffen.

Auflösung

Das Problem wurde durch das Identifizieren und Korrigieren einer ICMP-Regelkonfiguration in den Plattformeinstellungen, die Ping-Verkehr verweigerte, behoben. Die Entschließung umfasste folgende Schritte:

Schritt 1: Überprüfen der ARP-Tabelleneinträge

Vergewissern Sie sich, dass die ARP-Einträge für die Upstream-IP-Adresse in der ARP-Tabelle der Firewall sichtbar sind, die anzeigt, dass die Layer-2-Verbindung ordnungsgemäß funktioniert:

<#root>

device#

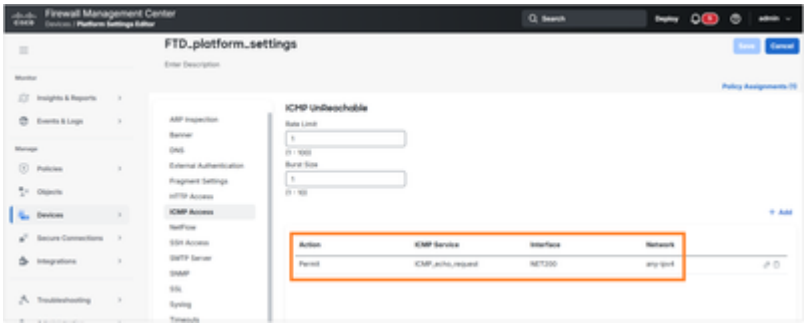
show arp

Schritt 2: Überprüfen der Plattformeinstellungen für ICMP-Regeln

Navigieren Sie zur Konfiguration der Plattformeinstellungen, und überprüfen Sie die ICMP-Regelrichtlinien, die sich auf den Ping-Verkehr auswirken können. Achten Sie speziell auf Regeln, die ICMP-Echoanforderungs-/Antwortpakete blockieren oder ablehnen können.

Schritt 3: ICMP-Blockierungsregel identifizieren und ändern

Suchen Sie die ICMP-Regel in den Plattformeinstellungen, die so konfiguriert ist, dass Ping-Verkehr abgelehnt wird.



In diesem Beispiel erlaubt die ICMP-Regel nur die Annahme von ICMP-Echo-Anfragen durch die FTD-Schnittstelle.

FTD-CLI-Verifizierung:

<#root>

device#

show run icmp

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

icmp permit any echo NET200
```

Schritt 4: ICMP-Regelkonfiguration aktualisieren

Ändern Sie die festgelegte ICMP-Regel, um Ping-Verkehr zuzulassen, oder entfernen Sie die Blockierungskonfiguration entsprechend den Anforderungen an die Netzwerksicherheit und den betrieblichen Anforderungen.

Die resultierende ICMP-Regel:

<#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
```

Schritt 5: Testen der Verbindung

Nachdem Sie die Konfiguration geändert haben, testen Sie die Ping-Verbindung zur Upstream-IP-Adresse, um sicherzustellen, dass das Problem behoben wurde und der ICMP-Datenverkehr nun ordnungsgemäß fließt:

<#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
```

Ursache

Die Ursache dieses Problems war eine in den Plattformeinstellungen konfigurierte ICMP-Regel, die explizit ICMP-Echoantwortverkehr verweigerte. Während die Firewall die richtige Layer-2-Anbindung aufrecht erhielt (was durch die sichtbaren ARP-Einträge belegt wird), blockierte die ICMP-Regel auf Plattformebene ICMP-Echo-Antwortpakete für Layer 3 und verhinderte so erfolgreiche Ping-Vorgänge an die Upstream-IP-Adresse. Diese Art der Konfiguration kann auftreten, wenn Sicherheitsrichtlinien implementiert werden, um den ICMP-Datenverkehr einzuschränken, sie kann sich jedoch unbeabsichtigt auf das Testen und Überwachen legitimer Netzwerkverbindungen auswirken.

Verwandte Inhalte

- 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
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.