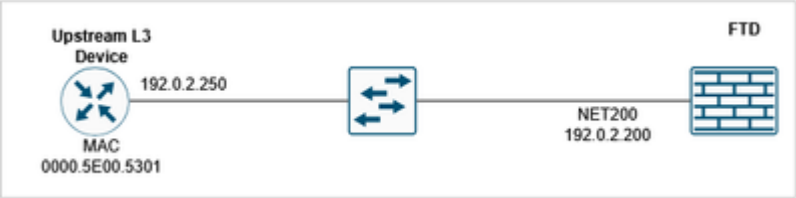
Problemen oplossen FTD Kan upstream-apparaat niet pingen ondanks ARP-vermelding

Inhoud

uitgeven

De Firewall Threat Defense (FTD) kon het IP-adres van het upstream-apparaat niet pingen, ondanks dat de firewall de ARP-vermelding voor het upstream IP-adres kon waarnemen. De ARP-tabel toonde de verwachte vermeldingen, wat aangeeft dat Layer 2-connectiviteit functioneerde, maar dat Layer 3-pingverkeer werd geblokkeerd.

Topologie



FTD CLI-symptomen

Ping naar het upstream IP-adres mislukt:

<#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)
```

Er is een ARP-vermelding voor het upstream IP-adres:

```
<#root>
device#

show arp



NET200 192.0.2.250 0000.5e00.5301

 47
```

Een opname met trace inschakelen in de FTD-interface:

```
<#root>
device#

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

FTD LINA-syslogs tijdens de ping-test:

```
<#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
...
```

Packet capture laat zien dat ICMP echo-antwoorden aankomen:

```
<#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



...
```

Packet trace van het ICMP-echoantwoord laat zien dat het pakket overeenkomt met een bestaande verbinding zoals verwacht en dat de uitvoerinterface de FTD-interface (NP Identity Ifc) is:

```
<#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 laat zien dat het ICMP echo antwoord wordt geweigerd:

<#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)
```

⚠ Let op: gebruik debugs met voorzichtigheid!

Het ICMP-foutopsporingsbericht uitschakelen:

<#root>

```
device#

no debug icmp trace


debug icmp trace disabled.
```

milieu

FTD 10.x. Ook andere software versies zijn hierbij betrokken.

resolutie

Het probleem werd opgelost door een ICMP-regelconfiguratie in de platforminstellingen te identificeren en te corrigeren die pingverkeer ontkende. De resolutie omvatte deze stappen:

Stap 1. ARP-tabelitems verifiëren

Bevestig dat de ARP-vermeldingen voor het upstream IP-adres zichtbaar zijn in de ARP-tabel van de firewall, wat aangeeft dat de Layer 2-connectiviteit naar behoren functioneert:

<#root>

device#

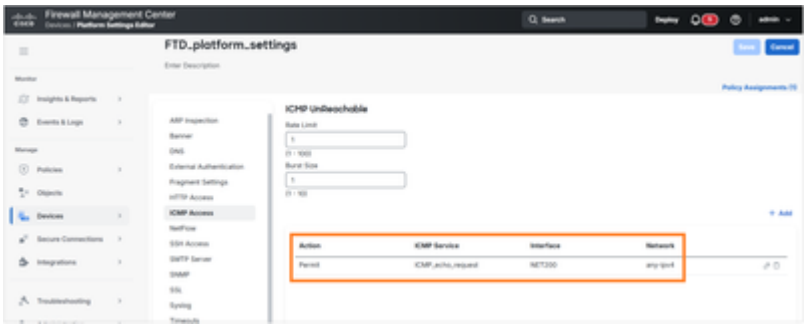
show arp

Stap 2. Controleer de platforminstellingen voor de ICMP-regels

Navigeer naar de configuratie van de platforminstellingen en bekijk het ICMP-regelbeleid dat van invloed kan zijn op het pingverkeer. Kijk specifiek naar regels die ICMP-echoverzoek- / antwoordpakketten kunnen blokkeren of weigeren.

Stap 3. Blokkering ICMP-regel identificeren en wijzigen

Zoek de ICMP-regel in de platforminstellingen die is geconfigureerd om ping-verkeer te weigeren.



In dit voorbeeld staat de ICMP-regel toe dat alleen ICMP-echoverzoeken door de FTD-interface worden geaccepteerd.

FTD CLI-verificatie:

<#root>

device#

show run icmp

icmp unreachable rate-limit 1 burst-size 1

```
icmp permit any echo NET200
```

Stap 4. ICMP-regelconfiguratie bijwerken

Wijzig de geïdentificeerde ICMP-regel om pingverkeer toe te staan of verwijder de blokkeringsconfiguratie indien dit passend is voor de netwerkbeveiligingsvereisten en operationele behoeften.

De resulterende 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
```

Stap 5. Connectiviteit testen

Nadat u de configuratiewijzigingen hebt aangebracht, test u de ping-connectiviteit met het upstream-IP-adres om te controleren of het probleem is opgelost en of het ICMP-verkeer nu goed verloopt:

<#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
```

Oorzaak

De hoofdoorzaak van dit probleem was een ICMP-regel die was geconfigureerd in de platforminstellingen en die expliciet het ICMP-echoantwoordverkeer ontkende. Terwijl de firewall de juiste Layer 2-connectiviteit behield (zoals blijkt uit de zichtbare ARP-vermeldingen), blokkeerde de ICMP-regel op platformniveau Layer 3 ICMP-echoantwoordpakketten, waardoor succesvolle ping-bewerkingen naar het upstream IP-adres werden voorkomen. Dit type configuratie kan optreden wanneer beveiligingsbeleid wordt geïmplementeerd om het ICMP-verkeer te beperken, maar kan per ongeluk invloed hebben op het testen en bewaken van legitieme netwerkconnectiviteit.

Verwante inhoud

- 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
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.