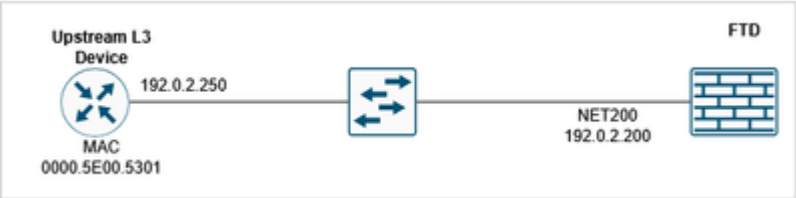
Resolución de problemas FTD No se puede hacer ping al dispositivo ascendente a pesar de tener una entrada ARP

Contenido

Problema

Firewall Threat Defence (FTD) no pudo realizar un ping en la dirección IP del dispositivo ascendente, a pesar de que el firewall pudo observar la entrada ARP de la dirección IP ascendente. La tabla ARP mostró las entradas esperadas, lo que indica que la conectividad de la Capa 2 estaba funcionando pero que el tráfico ping de la Capa 3 estaba siendo bloqueado.

Topología



Síntomas de FTD CLI

El ping enviado a la dirección IP de flujo ascendente está fallando:

<#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)
```

Hay una entrada ARP para la dirección IP de flujo ascendente:

<#root>

```
device#
```

show arp

NET200 192.0.2.250 0000.5e00.5301

47

Habilite una captura con seguimiento en la interfaz FTD:

<#root>

```
device#
```

capture CAPI interface NET200 trace match icmp host 192.0.2.200 host 192.0.2.250

Registros del sistema LINA de FTD durante la prueba de ping:

<#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
...
```

La captura de paquetes muestra las respuestas de eco ICMP que llegan:

```
<#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



...
```

El seguimiento de paquetes de la respuesta de eco ICMP muestra que el paquete coincide con una conexión existente como se esperaba y la interfaz de salida es la interfaz FTD (NP Identity 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
```

El seguimiento ICMP de depuración muestra que se está denegando la respuesta de eco ICMP:

```
<#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)
```

⚠ Precaución: Utilice los debugs con precaución!

Para desactivar la depuración ICMP:

<#root>

```
device#

no debug icmp trace


debug icmp trace disabled.
```

Entorno

FTD 10.x. Otras versiones de software también se ven afectadas.

Resolución

El problema se resolvió al identificar y corregir una configuración de regla ICMP en la configuración de la plataforma que denegaba el tráfico ping. La resolución implicó estos pasos:

Paso 1. Verificar las Entradas de la Tabla ARP

Confirme que las entradas ARP para la dirección IP de flujo ascendente estén visibles en la tabla ARP del firewall, lo que indica que la conectividad de Capa 2 está funcionando correctamente:

<#root>

device#

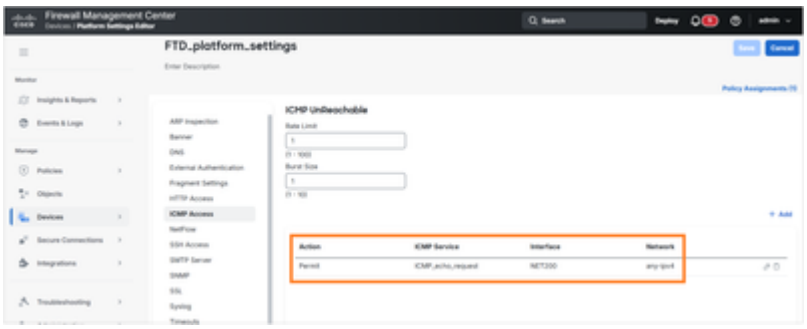
show arp

Paso 2. Compruebe la configuración de la plataforma para las reglas ICMP

Desplácese hasta la configuración de la plataforma y examine las directivas de regla ICMP que pueden afectar al tráfico de ping. Busque específicamente reglas que podrían estar bloqueando o denegando paquetes de solicitud/respuesta de eco ICMP.

Paso 3. Identificar y modificar la regla de bloqueo ICMP

Localice la regla ICMP en la configuración de la plataforma que está configurada para denegar el tráfico de ping.



En este ejemplo, la regla ICMP permite que la interfaz FTD acepte solamente las solicitudes de eco ICMP.

Verificación CLI de FTD:

<#root>

device#

show run icmp

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

icmp permit any echo NET200
```

Paso 4. Actualizar configuración de regla ICMP

Modifique la regla ICMP identificada para permitir el tráfico de ping o quite la configuración de bloqueo según corresponda según los requisitos de seguridad de la red y las necesidades operativas.

La regla ICMP resultante:

<#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
```

Paso 5. Pruebe la conectividad

Después de realizar los cambios de configuración, pruebe la conectividad de ping con la dirección IP ascendente para verificar que el problema se haya resuelto y que el tráfico ICMP esté fluyendo correctamente:

<#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
```

Causa

La causa raíz de este problema fue una regla ICMP configurada en la configuración de la plataforma que denegaba explícitamente el tráfico de respuestas de eco ICMP. Mientras el firewall mantenía una conectividad de Capa 2 adecuada (evidenciada por las entradas ARP visibles), la regla ICMP de nivel de plataforma estaba bloqueando los paquetes de respuesta de eco ICMP de Capa 3, lo que impedía operaciones de ping exitosas a la dirección IP ascendente. Este tipo de configuración puede producirse cuando se implementan políticas de seguridad para restringir el tráfico ICMP, pero puede afectar de forma inadvertida a la supervisión y las pruebas de conectividad de red legítimas.

Contenido relacionado

- 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
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).