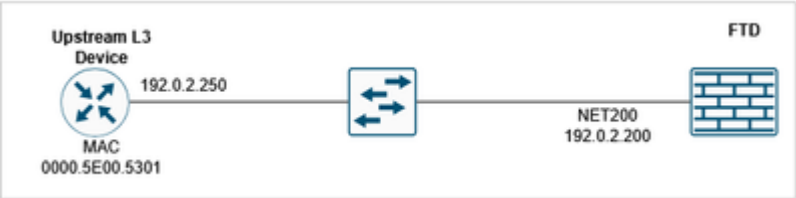
Troubleshooting de FTD Incapaz de Fazer Ping em Dispositivo Upstream Apesar de Ter uma Entrada ARP

Contents

Problema

O Firewall Threat Defense (FTD) não conseguiu fazer ping no endereço IP do dispositivo upstream, apesar do firewall poder observar a entrada ARP para o endereço IP upstream. A tabela ARP mostrou as entradas esperadas, indicando que a conectividade da Camada 2 estava funcionando, mas o tráfego de ping da Camada 3 estava sendo bloqueado.

Topologia



Sintomas de FTD CLI

O ping para o endereço IP de upstream está falhando:

<#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)
```

Há uma entrada ARP para o endereço IP upstream:

```
<#root>

device#

show arp



NET200 192.0.2.250 0000.5e00.5301

 47
```

Habilite uma captura com rastreamento na interface FTD:

```
<#root>

device#

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

Syslogs de FTD LINA durante o teste 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
...
```

A captura de pacotes mostra as respostas de eco ICMP que chegam:

```
<#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



...
```

O rastreamento de pacote da resposta de eco ICMP mostra que o pacote está correspondendo a uma conexão existente como esperado e a interface de saída é a interface 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

O comando debug ICMP trace mostra que a resposta de eco ICMP está sendo negada:

<#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)

⚠ Caution: Use as depurações com cuidado!

Para desativar a depuração ICMP:

<#root>

```
device#

no debug icmp trace

debug icmp trace disabled.
```

Ambiente

FTD 10.x. Outras versões de software também são afetadas.

Resolução

O problema foi resolvido identificando e corrigindo uma configuração de regra ICMP nas configurações da plataforma que estava negando o tráfego de ping. A resolução envolveu estas etapas:

Etapa 1. Verificar Entradas da Tabela ARP

Confirme se as entradas ARP para o endereço IP de upstream estão visíveis na tabela ARP do firewall, que indica que a conectividade da Camada 2 está funcionando corretamente:

<#root>

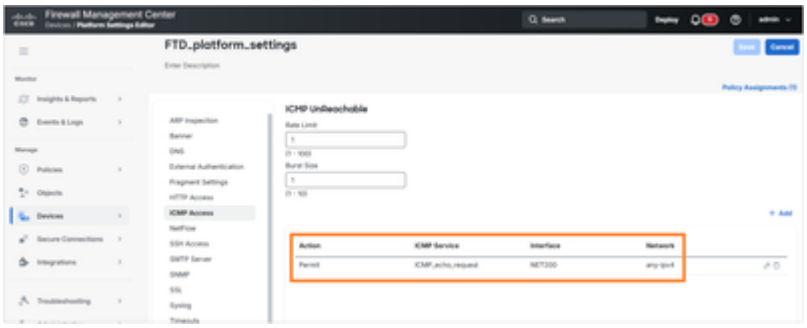
```
device#

show arp
```

Etapa 2. Verificar as Configurações da Plataforma para Regras ICMP

Navegue até a configuração das configurações da plataforma e examine as políticas de regra ICMP que podem afetar o tráfego de ping. Procure especificamente por regras que possam estar bloqueando ou negando pacotes ICMP de solicitação/resposta de eco.

Etapa 3. Identificar e Modificar a Regra de Bloqueio ICMP

Localize a regra ICMP nas configurações da plataforma que está configurada para negar o tráfego de ping.



Neste exemplo, a regra ICMP permite que somente solicitações de eco ICMP sejam aceitas pela interface FTD.

Verificação CLI de FTD:

<#root>

```
device#

show run icmp


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

```
icmp permit any echo NET200
```

Etapa 4. Atualizar a configuração de regras do ICMP

Modifique a regra ICMP identificada para permitir o tráfego de ping ou remover a configuração de bloqueio conforme apropriado para os requisitos de segurança de rede e as necessidades operacionais.

A regra 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
```

Etapa 5. Testar a conectividade

Depois de fazer as alterações de configuração, teste a conectividade do ping com o endereço IP de upstream para verificar se o problema foi resolvido e se o tráfego ICMP está fluindo corretamente:

<#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

A causa raiz desse problema foi uma regra ICMP configurada nas configurações da plataforma que negava explicitamente o tráfego de respostas de eco ICMP. Enquanto o firewall mantinha a conectividade apropriada da camada 2 (evidenciada pelas entradas ARP visíveis), a regra ICMP no nível da plataforma bloqueava os pacotes de resposta de eco ICMP da camada 3, impedindo operações de ping bem-sucedidas para o endereço IP de upstream. Esse tipo de configuração pode ocorrer quando políticas de segurança são implementadas para restringir o tráfego ICMP, mas pode afetar inadvertidamente o monitoramento e o teste de conectividade de rede legítimos.

Conteúdo 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
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.