Identificar e Solucionar Problemas do Traceroute do FTD que Não Exiba Informações de Salto apesar do Ping ICMP Bem-sucedido

Problema

Todos estes sintomas são observados:

- Falha de Traceroute: Os comandos traceroute iniciados diretamente do dispositivo FTD (Firewall Threat Defense) da Cisco retornam consistentemente apenas * * * para todos os saltos quando o destino for endereços IP externos.
- Conectividade bem-sucedida: Os testes de ping do ICMP para o mesmo destino são bem-sucedidos, e o tráfego do ICMP é explicitamente permitido na Política de Controle de Acesso.

Esse comportamento impede a visibilidade dos saltos de caminho para o tráfego originário do dispositivo FTD, impactando os esforços de solução de problemas de caminho de rede.

Exemplo

O ping no destino está funcionando:

<#root>

```
firepower#

ping 192.168.203.89

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.203.89, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Mas traceroute não é:

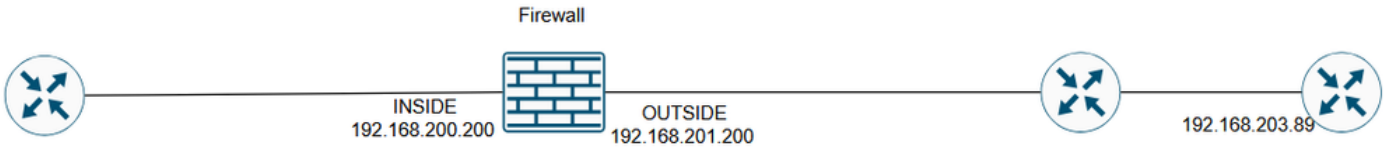
<#root>

```
firepower#

traceroute 192.168.203.89

Type escape sequence to abort.
Tracing the route to 192.168.203.89
 1*  *  *
 2*  *  *
 3*  *  *
...
 30*  *  *
firepower#
```

Ambiente

- Cisco Secure Firewall Threat Defense (FTD).
- Primeira vez em: 7.4, 7.4.2.3, 7.6.2. Outras versões também podem ser afetadas.
- Cisco Secure Firewall Management Center (FMC / cdFMC / FDM) para gerenciamento.
- Regras de NAT estático em uso, incluindo configurações bidirecionais.
- Comandos Traceroute executados da CLI do FTD (modo Lina).
- ICMP permitido na política de controle de acesso.

Topologia



inline_image_0.png

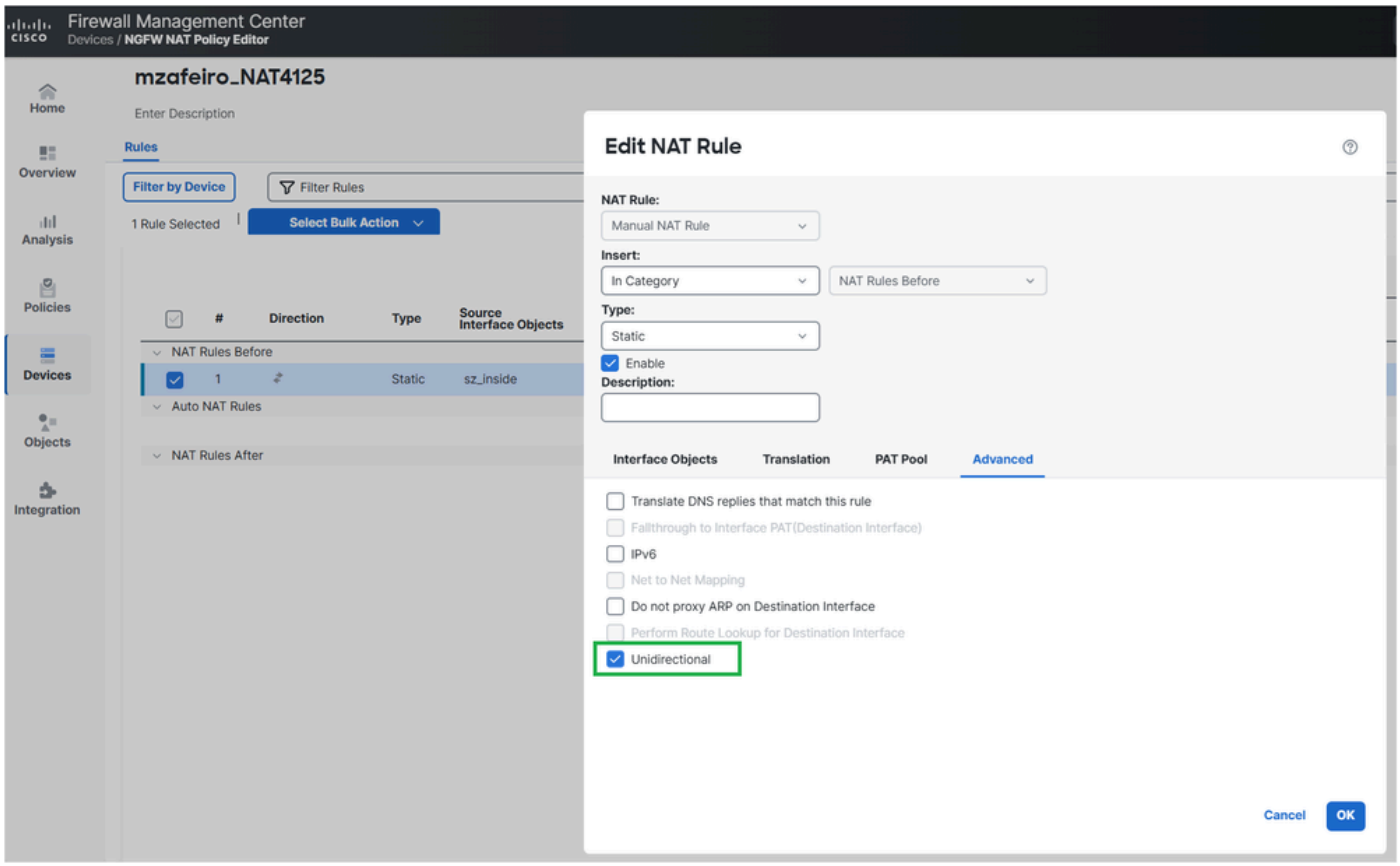
Resolução

As soluções possíveis dependem da finalidade da regra de NAT configurada.

Solução 1

Se o objetivo era converter o IP do servidor interno somente para acesso de saída, você pode configurar a regra NAT como unidirecional.

No FMC, isso pode ser feito nas opções Advanced da regra de NAT:



inline_image_0.png

A configuração NAT implantada:

<#root>

```
firepower#
```

`show run nat`

```
nat (INSIDE,OUTSIDE) source static server_host interface unidirectional
firepower#
```

Verificação

<#root>

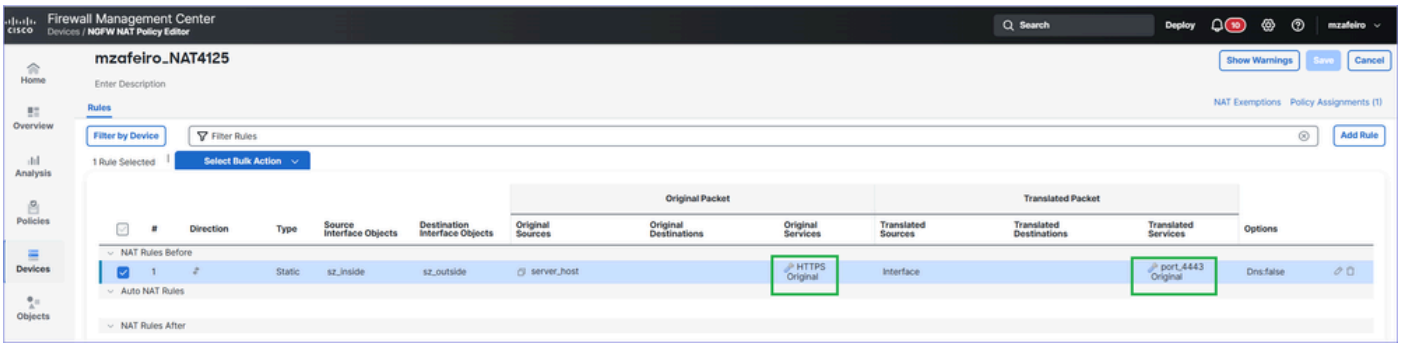
```
firepower#
```

traceroute 192.168.203.89

```
Type escape sequence to abort.
Tracing the route to 192.168.203.89
 1  192.168.201.88 2 msec 2 msec 2 msec
 2  192.168.203.89 1 msec *  1 msec
```

Solução 2

Se o objetivo for que o servidor interno seja alcançável de fora, você pode tornar a regra NAT mais específica configurando o encaminhamento de portas:



inline_image_0.png

A configuração NAT implantada:

<#root>

```
firepower#
```

show run nat

```
nat (INSIDE,OUTSIDE) source static server_host interface service SVC_25769850586 SVC_25769850587
```

Verificação

<#root>

```
firepower#

traceroute 192.168.203.89

Type escape sequence to abort.
Tracing the route to 192.168.203.89
 1  192.168.201.88 2 msec 2 msec 2 msec
 2  192.168.203.89 1 msec *  1 msec
```

Como funciona

Como funciona

Ping

1. O firewall envia uma mensagem de solicitação de eco (Código 0 do ICMP Tipo 8).
2. Uma nova conexão de firewall é criada para o ICMP.
3. O firewall recebe uma mensagem de resposta de eco (Código 0 do tipo 0 do ICMP).
4. A mensagem corresponde à conexão criada na etapa 2.
5. A mensagem de resposta de eco é consumida pelo firewall.

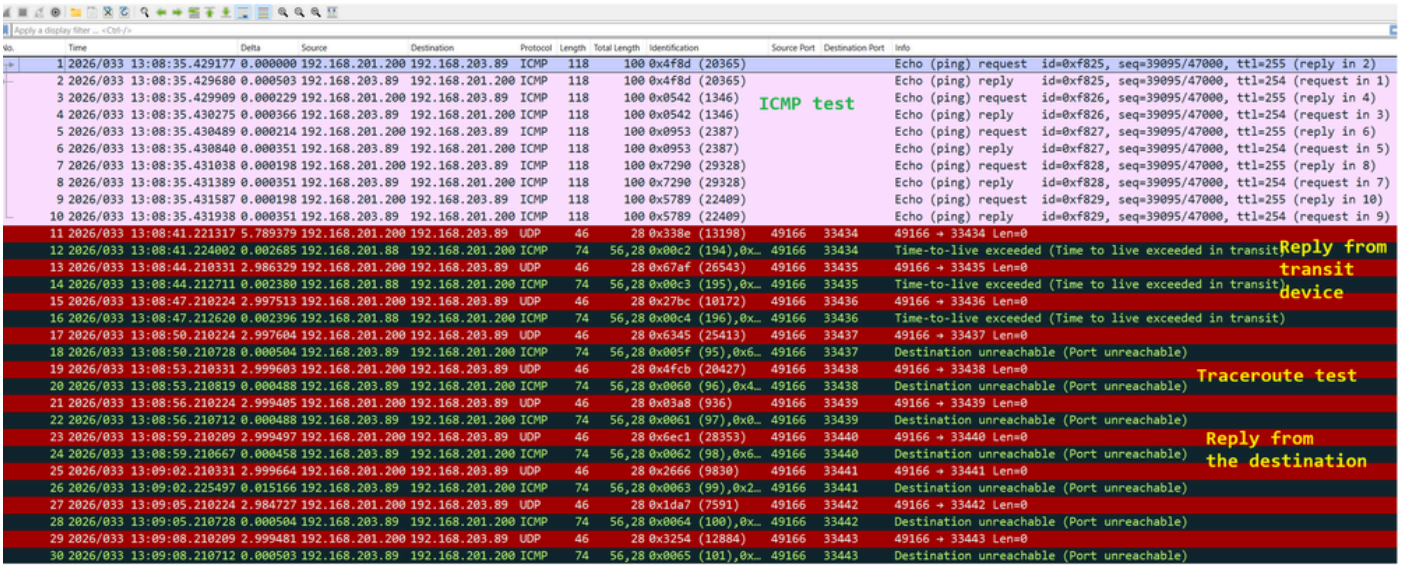
Traceroute

1. O firewall envia três pacotes UDP iniciando a partir de portas, 33434, 33435 e 33436 para o destino com TTL 1.
2. Uma nova conexão de firewall é criada para UDP.

3. O firewall recebe um TTL ICMP excedido em trânsito (Código do tipo 11 0) ou uma Porta ICMP inalcançável (Código do tipo 3 3).

4. Quando os pacotes ICMP chegam ao firewall, eles são tratados como conexões diferentes dos pacotes UDP da etapa 2.

Isso pode ser visto no Wireshark:



inline_image_0.png

Troubleshooting

Passo 1

Ative as capturas de pacotes na interface de saída do firewall com trace para ver como o firewall trata os pacotes de entrada:

<#root>

```
firepower#
```

```
capture CAPI trace interface OUTSIDE match ip host 192.168.203.89 host 192.168.201.100
```

Passo 2

Teste usando ping:

<#root>

```
firepower#

ping 192.168.203.89


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.203.89, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Em seguida, teste com traceroute:

<#root>

```
firepower#

traceroute 192.168.203.89


Type escape sequence to abort.
Tracing the route to 192.168.203.89
 1*  *  *
 2*  *  *
 3*  *  *
 4*  *  *
 5*  *  *
 6*  *  *
 7*  *  *
…
```

Etapa 3

Verifique o conteúdo da captura:

- Os pacotes de 1 a 10 estão relacionados ao teste de ping do ICMP.
- Os pacotes 11-16 estão relacionados ao traceroute. As respostas são do primeiro salto.

- Os pacotes 17-28 também estão relacionados ao traceroute. As respostas são do ponto final de destino.

<#root>

```
firepower#

show capture CAPI

190 packets captured
1: 13:50:27.345471       802.1Q vlan#201 P0 192.168.201.200 > 192.168.203.89 icmp: echo request
2: 13:50:27.345975       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: echo reply
3: 13:50:27.346219       802.1Q vlan#201 P0 192.168.201.200 > 192.168.203.89 icmp: echo request
4: 13:50:27.346600       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: echo reply
5: 13:50:27.346814       802.1Q vlan#201 P0 192.168.201.200 > 192.168.203.89 icmp: echo request
6: 13:50:27.347165       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: echo reply
7: 13:50:27.347378       802.1Q vlan#201 P0 192.168.201.200 > 192.168.203.89 icmp: echo request
8: 13:50:27.347714       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: echo reply
9: 13:50:27.347928       802.1Q vlan#201 P0 192.168.201.200 > 192.168.203.89 icmp: echo request
10: 13:50:27.348279       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: echo reply
11: 13:50:33.229724       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33434:  udp 0
12: 13:50:33.232562       802.1Q vlan#201 P0 192.168.201.88 > 192.168.201.200 icmp: time exceeded in-tra
13: 13:50:36.220279       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33435:  udp 0
14: 13:50:36.222827       802.1Q vlan#201 P0 192.168.201.88 > 192.168.201.200 icmp: time exceeded in-tra
15: 13:50:39.220172       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33436:  udp 0
16: 13:50:39.222675       802.1Q vlan#201 P0 192.168.201.88 > 192.168.201.200 icmp: time exceeded in-tra
17: 13:50:42.220157       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33437:  udp 0
18: 13:50:42.220737       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
19: 13:50:45.220264       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33438:  udp 0
20: 13:50:45.220752       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
21: 13:50:48.220157       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33439:  udp 0
22: 13:50:48.220645       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
23: 13:50:51.220157       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33440:  udp 0
24: 13:50:51.220645       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
25: 13:50:54.220264       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33441:  udp 0
26: 13:50:54.220752       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
27: 13:50:57.220157       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33442:  udp 0
28: 13:50:57.220645       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
```

Passo 4

Rastreie os pacotes ICMP de entrada a partir do teste de ping.

Packet #2 é a resposta na solicitação de ping do ICMP enviada no Packet #1.

<#root>

```
firepower#
```

```
show capture CAPI packet-number 2 trace

190 packets captured
2: 13:50:27.345975       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: echo reply
…
Phase: 4
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 488 ns
Config:
Additional Information:
Found flow with id 143799, using existing flow
…
Phase: 6
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 1952 ns
Config:
Additional Information:
Found adjacency entry for Next-hop 0.0.0.0 on interface  identity
Adjacency :Active
MAC address 0000.0000.0000 hits 483359 reference 2

Result:
input-interface: OUTSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
Time Taken: 18056 ns
1 packet shown
```

Os pontos principais do rastreamento são:

- O pacote correspondeu a um fluxo existente.
- A interface de saída é o próprio firewall (interface de identidade).

Etapa 5

Rastreie os pacotes ICMP de entrada do teste de traceroute.

O pacote #12 é a resposta do host de trânsito:

<#root>

```
firepower#
```

show capture CAPI packet-number 12 trace

```
190 packets captured
12: 13:50:33.232562       802.1Q vlan#201 P0 192.168.201.88 > 192.168.201.200 icmp: time exceeded in-tra

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 6344 ns
Config:
nat (INSIDE,OUTSIDE) source static server_host interface
Additional Information:
NAT divert to egress interface INSIDE(vrfid:0)
Untranslate 192.168.201.200/49168 to 192.168.200.50/49168

Phase: 7
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 97 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268436480
access-list CSM_FW_ACL_ remark rule-id 268436480: ACCESS POLICY: mzafeiro_empty - Default
access-list CSM_FW_ACL_ remark rule-id 268436480: L4 RULE: DEFAULT ACTION RULE
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 18
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 16104 ns
Config:
Additional Information:
New flow created with id 143805, packet dispatched to next module
...
Phase: 20
Type: SNORT
Subtype: identity
Result: ALLOW
Elapsed time: 39496 ns
Config:
Additional Information:
user id: no auth, realm id: 0, device type: 0, auth type: invalid, auth proto: basic, username: none, A
src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, abp src: none, abp dst: none, loc

Result:
input-interface: OUTSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: INSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 158341 ns
```

- O pacote faz parte de uma nova conexão (não correspondeu a um fluxo existente).

- O pacote está sujeito à Tradução de Endereço de Rede (especificamente, o UN-NAT significa NAT de destino).
- O pacote é tratado como um tráfego de trânsito de firewall e está sujeito à Política de Controle de Acesso (ACP) e à inspeção Snort.
- A interface de saída (saída) é INSIDE. Isso se deve à conversão de NAT.

Causa

Nesse caso, o problema é causado por esta regra de NAT estático:

<#root>

```
firepower#

show run nat

nat (INSIDE,OUTSIDE) source static server_host interface
```

Conteúdo relacionado

- Permitir Traceroute através do Firepower Threat Defense (FTD)
- 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.