

# 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*  *  *
```

```
... 
```

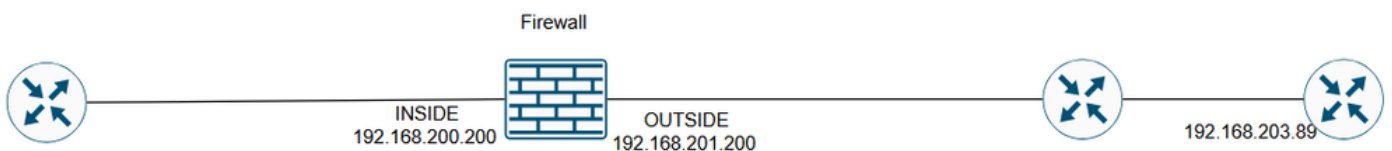
```
30*  *  *
```

```
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

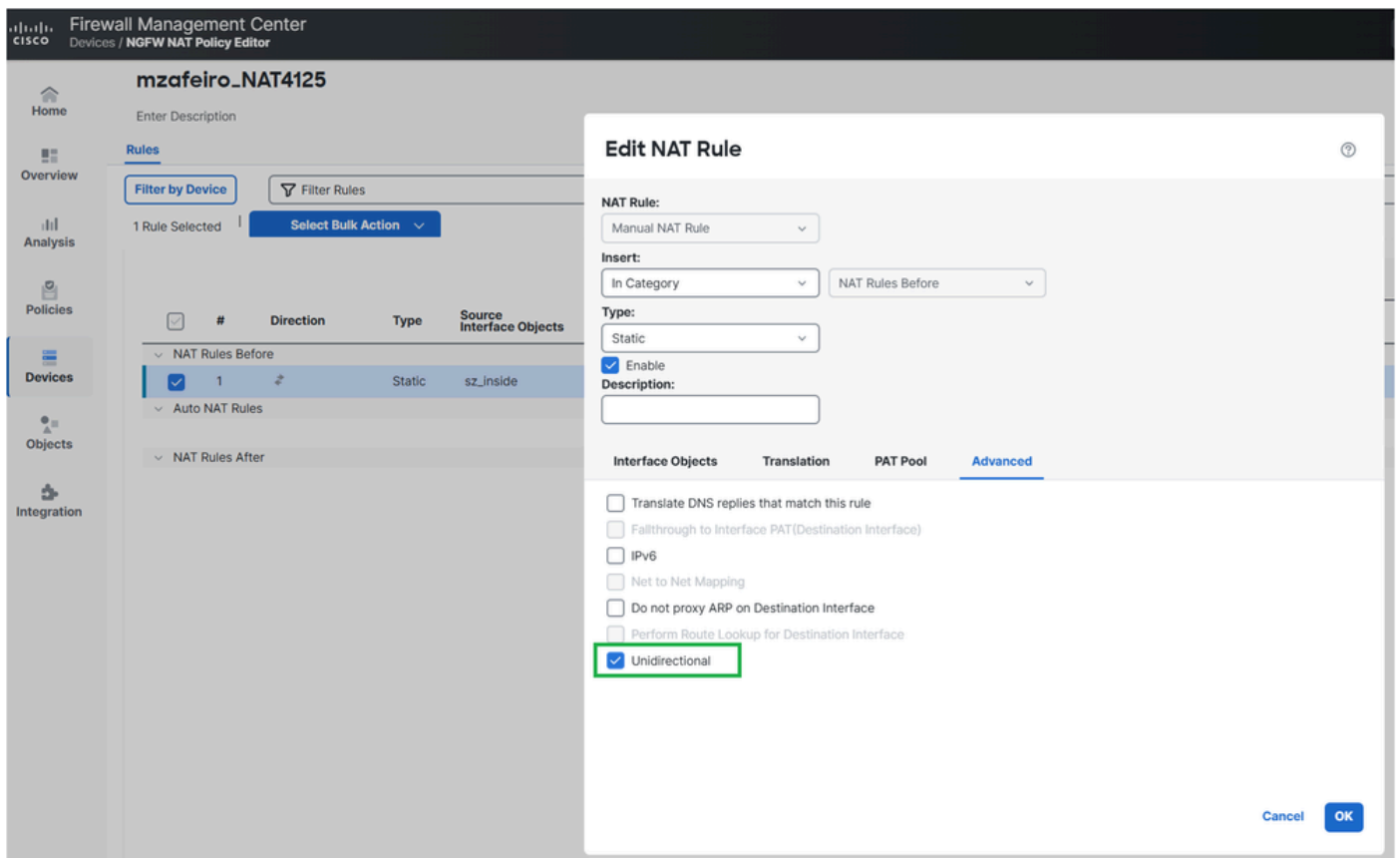
## Resolução

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
```

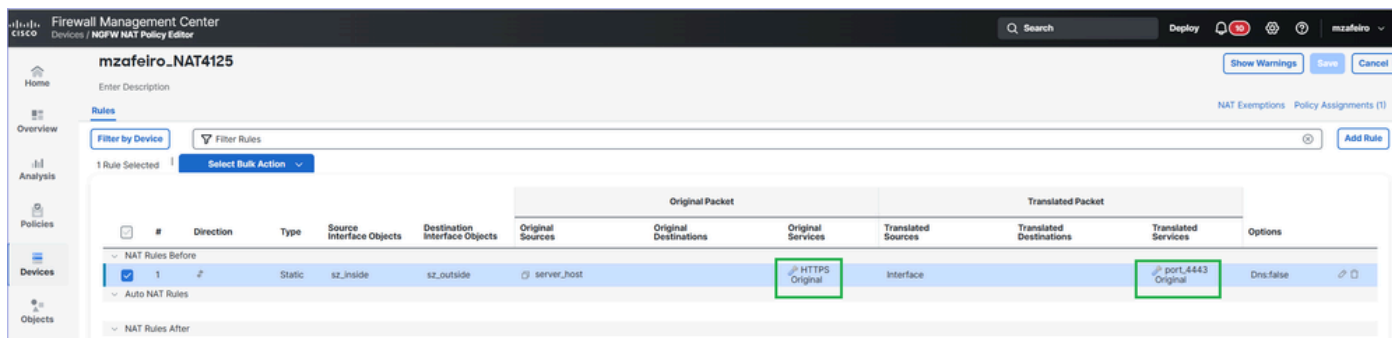
Type escape sequence to abort.

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.

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

No.	Time	Delta	Source	Destination	Protocol	Length	Total Length	Identification	Source Port	Destination Port	Info
1	2026/033 13:08:35.429177	0.000000	192.168.201.200	192.168.203.89	ICMP	118	100	0x4f8d (20365)			Echo (ping) request id=0xf825, seq=39095/47000, ttl=255 (reply in 2)
2	2026/033 13:08:35.429680	0.000503	192.168.203.89	192.168.201.200	ICMP	118	100	0x4f8d (20365)			Echo (ping) reply id=0xf825, seq=39095/47000, ttl=254 (request in 1)
3	2026/033 13:08:35.429989	0.000229	192.168.201.200	192.168.203.89	ICMP	118	100	0x0542 (1346)			Echo (ping) request id=0xf826, seq=39095/47000, ttl=255 (reply in 4)
4	2026/033 13:08:35.430275	0.000366	192.168.203.89	192.168.201.200	ICMP	118	100	0x0542 (1346)			Echo (ping) reply id=0xf826, seq=39095/47000, ttl=254 (request in 3)
5	2026/033 13:08:35.430489	0.000214	192.168.201.200	192.168.203.89	ICMP	118	100	0x0953 (2387)			Echo (ping) request id=0xf827, seq=39095/47000, ttl=255 (reply in 6)
6	2026/033 13:08:35.430840	0.000351	192.168.203.89	192.168.201.200	ICMP	118	100	0x0953 (2387)			Echo (ping) reply id=0xf827, seq=39095/47000, ttl=254 (request in 5)
7	2026/033 13:08:35.431038	0.000198	192.168.201.200	192.168.203.89	ICMP	118	100	0x7290 (29328)			Echo (ping) request id=0xf828, seq=39095/47000, ttl=255 (reply in 8)
8	2026/033 13:08:35.431389	0.000351	192.168.203.89	192.168.201.200	ICMP	118	100	0x7290 (29328)			Echo (ping) reply id=0xf828, seq=39095/47000, ttl=254 (request in 7)
9	2026/033 13:08:35.431587	0.000198	192.168.201.200	192.168.203.89	ICMP	118	100	0x5789 (22409)			Echo (ping) request id=0xf829, seq=39095/47000, ttl=255 (reply in 10)
10	2026/033 13:08:35.431938	0.000351	192.168.203.89	192.168.201.200	ICMP	118	100	0x5789 (22409)			Echo (ping) reply id=0xf829, seq=39095/47000, ttl=254 (request in 9)
11	2026/033 13:08:41.221317	5.789379	192.168.201.200	192.168.203.89	UDP	46	28	0x338e (13198)	49166	33434	49166 → 33434 Len=0
12	2026/033 13:08:41.224092	0.002685	192.168.201.88	192.168.201.200	ICMP	74	56	28 0x00c2 (194),0x...	49166	33434	Time-to-live exceeded (Time to live exceeded in transit) Reply from
13	2026/033 13:08:44.210331	2.986329	192.168.201.200	192.168.203.89	UDP	46	28	0x67af (26543)	49166	33435	49166 → 33435 Len=0
14	2026/033 13:08:44.212711	0.002380	192.168.201.88	192.168.201.200	ICMP	74	56	28 0x00c3 (195),0x...	49166	33435	Time-to-live exceeded (Time to live exceeded in transit) transit device
15	2026/033 13:08:47.210224	2.997513	192.168.201.200	192.168.203.89	UDP	46	28	0x27bc (10172)	49166	33436	49166 → 33436 Len=0
16	2026/033 13:08:47.212620	0.002396	192.168.201.88	192.168.201.200	ICMP	74	56	28 0x00c4 (196),0x...	49166	33436	Time-to-live exceeded (Time to live exceeded in transit)
17	2026/033 13:08:50.210224	2.997684	192.168.201.200	192.168.203.89	UDP	46	28	0x6345 (25413)	49166	33437	49166 → 33437 Len=0
18	2026/033 13:08:50.210728	0.000504	192.168.203.89	192.168.201.200	ICMP	74	56	28 0x00f5 (95),0x6...	49166	33437	Destination unreachable (Port unreachable)
19	2026/033 13:08:53.210331	2.999603	192.168.201.200	192.168.203.89	UDP	46	28	0x4fcb (20427)	49166	33438	49166 → 33438 Len=0
20	2026/033 13:08:53.210819	0.000488	192.168.203.89	192.168.201.200	ICMP	74	56	28 0x0060 (96),0x4...	49166	33438	Destination unreachable (Port unreachable) Traceroute test
21	2026/033 13:08:56.210224	2.999485	192.168.201.200	192.168.203.89	UDP	46	28	0x03a8 (936)	49166	33439	49166 → 33439 Len=0
22	2026/033 13:08:56.210712	0.000488	192.168.203.89	192.168.201.200	ICMP	74	56	28 0x0061 (97),0x0...	49166	33439	Destination unreachable (Port unreachable)
23	2026/033 13:08:59.210209	2.999497	192.168.201.200	192.168.203.89	UDP	46	28	0x6ec1 (28353)	49166	33440	49166 → 33440 Len=0
24	2026/033 13:08:59.210667	0.000458	192.168.203.89	192.168.201.200	ICMP	74	56	28 0x0062 (98),0x6...	49166	33440	Destination unreachable (Port unreachable) Reply from the destination
25	2026/033 13:09:02.210331	2.999664	192.168.201.200	192.168.203.89	UDP	46	28	0x2666 (9830)	49166	33441	49166 → 33441 Len=0
26	2026/033 13:09:02.225497	0.015166	192.168.203.89	192.168.201.200	ICMP	74	56	28 0x0063 (99),0x2...	49166	33441	Destination unreachable (Port unreachable)
27	2026/033 13:09:05.210224	2.984727	192.168.201.200	192.168.203.89	UDP	46	28	0x1da7 (7591)	49166	33442	49166 → 33442 Len=0
28	2026/033 13:09:05.210728	0.000504	192.168.203.89	192.168.201.200	ICMP	74	56	28 0x0064 (100),0x...	49166	33442	Destination unreachable (Port unreachable)
29	2026/033 13:09:08.210209	2.999481	192.168.201.200	192.168.203.89	UDP	46	28	0x3254 (12884)	49166	33443	49166 → 33443 Len=0
30	2026/033 13:09:08.210712	0.000503	192.168.203.89	192.168.201.200	ICMP	74	56	28 0x0065 (101),0x...	49166	33443	Destination unreachable (Port unreachable)

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-tr
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-tr
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-tr
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-tr
```

```
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.