

# Fehlerbehebung bei Traceroute von FTD, die trotz erfolgreichem ICMP-Ping keine Hop-Informationen anzeigt

## Problem

Alle diese Symptome treten auf:

- Routenfehler: Direkt vom Cisco Firewall Threat Defense (FTD)-Gerät initiierte Traceroute-Befehle geben beim Anvisieren externer IP-Adressen konsistent nur \* \* \* für alle Hops zurück.
- Erfolgreiche Verbindung: ICMP-Ping-Tests an dasselbe Ziel waren erfolgreich, und ICMP-Datenverkehr ist in der Zugriffskontrollrichtlinie explizit zulässig.

Dieses Verhalten verhindert die Transparenz von Pfad-Hops für Datenverkehr, der vom FTD-Gerät ausgeht, und beeinträchtigt die Fehlerbehebung für Netzwerkpfade.

## Beispiel

Ping an das Ziel funktioniert:

```
<#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
```

Aber Traceroute ist nicht:

```
<#root>
```

```
firepower#
```

```
traceroute 192.168.203.89
```

```
Type escape sequence to abort.
```

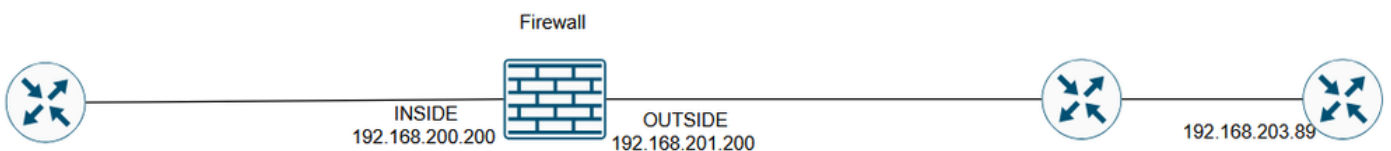
```
Tracing the route to 192.168.203.89
```

```
 1*  *  *  
 2*  *  *  
 3*  *  *  
 ...  
30*  *  *  
firepower#
```

## Umwelt

- Cisco Secure Firewall Threat Defense (FTD)
- Erstmals beobachtet bei: 7.4, 7.4.2.3, 7.6.2. Andere Versionen könnten ebenfalls betroffen sein.
- Cisco Secure Firewall Management Center (FMC/cdFMC/FDM) für die Verwaltung.
- Statische NAT-Regeln im Einsatz, einschließlich bidirektionaler Konfigurationen
- Von FTD CLI (Lina-Modus) ausgeführte Traceroute-Befehle.
- ICMP in der Zugriffskontrollrichtlinie zugelassen.

## Topologie



inline\_image\_0.png

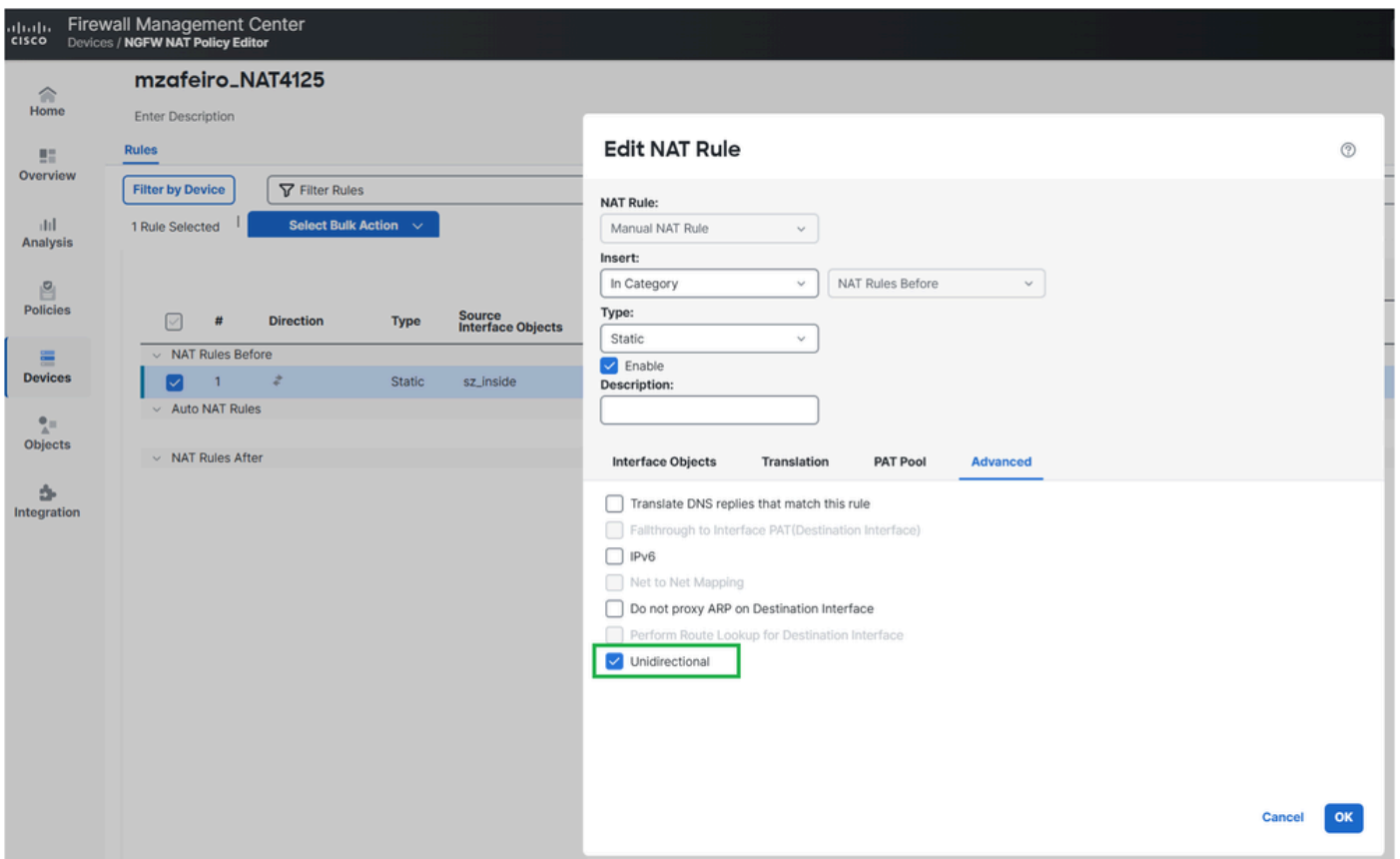
## Auflösung

Die möglichen Lösungen hängen vom Zweck der konfigurierten NAT-Regel ab.

## Lösung 1

Wenn das Ziel darin besteht, die interne Server-IP nur für den ausgehenden Zugriff zu übersetzen, können Sie die NAT-Regel als unidirektional konfigurieren.

Auf FMC kann dies über die NAT-Regel "Erweiterte Optionen" erfolgen:



inline\_image\_0.png

Die bereitgestellte NAT-Konfiguration:

```
<#root>
```

```
firepower#
```

```
show run nat
```

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

## Verifizierung

```
<#root>
```

```
firepower#
```

```
traceroute 192.168.203.89
```

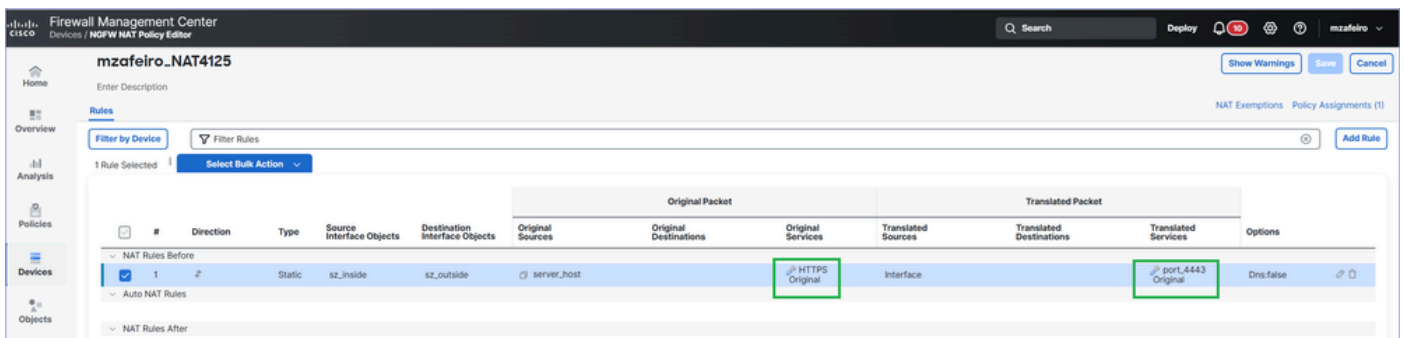
Type escape sequence to abort.

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
```

## Lösung 2

Wenn der interne Server von außen erreichbar sein soll, können Sie die NAT-Regel genauer definieren, indem Sie die Port-Weiterleitung konfigurieren:



inline\_image\_0.png

Die bereitgestellte NAT-Konfiguration:

```
<#root>
```

```
firepower#
```

```
show run nat
```

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

## Verifizierung

```
<#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
```

So funktioniert es

So funktioniert es

## Ping

1. Die Firewall sendet eine Echo-Anfrage (ICMP Typ 8 Code 0).
2. Für ICMP wird eine neue Firewall-Verbindung erstellt.
3. Die Firewall erhält eine Echo-Antwort (ICMP-Code 0 0).
4. Die Nachricht entspricht der in Schritt 2 erstellten Verbindung.
5. Die Echo-Antwort-Nachricht wird von der Firewall verbraucht.

## Routenverfolgung

1. Die Firewall sendet drei UDP-Pakete von den Ports 33434, 33435 und 33436 mit TTL 1 an das Ziel.
2. Für UDP wird eine neue Firewall-Verbindung erstellt.

- Die Firewall empfängt entweder eine übertragene ICMP-TTL (Typ 11 Code 0) oder einen nicht erreichbaren ICMP-Port (Typ 3 Code 3).
- Sobald ICMP-Pakete an der Firewall ankommen, werden sie als andere Verbindungen behandelt als die UDP-Pakete aus Schritt 2.

Dies ist in Wireshark zu sehen:

No.	Time	Delta	Source	Destination	Protocol	Length	Total Length	Identification	Source Port	Destination Port	Info
1	2026/03 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	2026/03 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	2026/03 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	2026/03 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	2026/03 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	2026/03 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	2026/03 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	2026/03 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	2026/03 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	2026/03 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	2026/03 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	2026/03 13:08:41.224002	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	2026/03 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 transit device
14	2026/03 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)
15	2026/03 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	2026/03 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	2026/03 13:08:50.210224	2.997604	192.168.201.200	192.168.203.89	UDP	46	28	0x6345 (25413)	49166	33437	49166 → 33437 Len=0
18	2026/03 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	2026/03 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	2026/03 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	2026/03 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	2026/03 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	2026/03 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	2026/03 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
25	2026/03 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 the destination
26	2026/03 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	2026/03 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	2026/03 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	2026/03 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	2026/03 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

## Fehlerbehebung

### Schritt 1

Aktivieren Sie die Paketerfassung an der Firewall-Ausgangsschnittstelle mit Trace, um festzustellen, wie die Firewall die eingehenden Pakete verarbeitet:

```
<#root>
```

```
firepower#
```

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

## Schritt 2

Test mit 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
```

Anschließend mit Traceroute testen:

```
<#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*  *  *
```

```
...
```

## Schritt 3

Überprüfen Sie den Inhalt der Aufzeichnung:

- Die Pakete 1-10 beziehen sich auf den ICMP-Ping-Test.
- Die Pakete 11-16 beziehen sich auf Traceroute. Die Antworten stammen vom ersten Hop.

- Die Pakete 17-28 beziehen sich ebenfalls auf Traceroute. Die Antworten stammen vom Zielendpunkt.

```
<#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
```

#### Schritt 4

Verfolgen Sie die eingehenden ICMP-Pakete aus dem Ping-Test.

Paket #2 ist die Antwort auf die ICMP-Ping-Anforderung, die in Paket #1 gesendet wurde.

```
<#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
```

Die wichtigsten Punkte der Ablaufverfolgung sind:

- Das Paket stimmt mit einem vorhandenen Datenfluss überein.
- Die Ausgabeschnittstelle ist die Firewall selbst (Identitätsschnittstelle).

Schritt 5

Verfolgen Sie die eingehenden ICMP-Pakete aus dem Traceroute-Test.

Paket #12 ist die Antwort des Transit-Hosts:

```
<#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
```

- Das Paket ist Teil einer neuen Verbindung (entspricht nicht einem vorhandenen Datenfluss).

- Das Paket unterliegt der Network Address Translation (Netzwerkadressumwandlung) (wobei "UN-NAT" die Ziel-NAT bezeichnet).
- Das Paket wird als Firewall-Datenverkehr behandelt und unterliegt den Zugriffskontrollrichtlinien (ACP, Access Control Policy) und der Snort-Überprüfung.
- Die Ausgabe-Schnittstelle (Ausgang) ist INSIDE. Dies ist auf die NAT-Übersetzung zurückzuführen.

## Ursache

In diesem Fall wird das Problem durch die statische NAT-Regel verursacht:

```
<#root>
```

```
firepower#
```

```
show run nat
```

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

## Verwandte Inhalte

- [Routenverfolgung durch FirePOWER Threat Defense \(FTD\) zulassen](#)
- [Technischer Support und Downloads von Cisco](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.