

Dépanner Traceroute à partir de FTD qui n'affiche pas les informations de saut malgré une requête ping ICMP réussie

Problème

Tous ces symptômes sont visibles :

- Échec de traceroute : Les commandes traceroute lancées directement à partir du périphérique Cisco Firewall Threat Defense (FTD) ne renvoient systématiquement que * * * pour tous les sauts lors du ciblage d'adresses IP externes.
- Connectivité réussie : Les tests ping ICMP vers la même destination aboutissent et le trafic ICMP est explicitement autorisé dans la stratégie de contrôle d'accès.

Ce comportement empêche la visibilité des sauts de chemin pour le trafic provenant du périphérique FTD, ce qui a un impact sur les efforts de dépannage de chemin réseau.

Exemple

La commande ping vers la destination fonctionne :

```
<#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
```

Mais traceroute n'est pas :

```
<#root>
```

```
firepower#
```

```
traceroute 192.168.203.89
```

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

```
Tracing the route to 192.168.203.89
```

```
1* * *
```

```
2* * *
```

```
3* * *
```

```
...
```

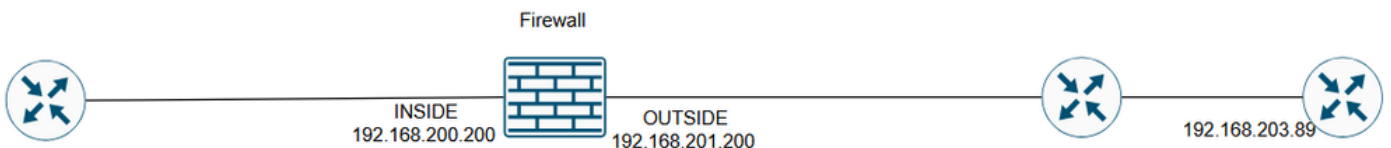
```
30* * *
```

```
firepower#
```

Environnement

- Cisco Secure Firewall Threat Defense (FTD).
- Première fois observée à : 7.4, 7.4.2.3, 7.6.2. D'autres versions pourraient également être affectées.
- Cisco Secure Firewall Management Center (FMC / cdFMC / FDM) pour la gestion.
- Règles NAT statiques utilisées, y compris les configurations bidirectionnelles.
- Commandes traceroute exécutées à partir de l'interface de ligne de commande FTD (mode Lina).
- ICMP autorisé dans la stratégie de contrôle d'accès.

Topologie



image_en_ligne_0.png

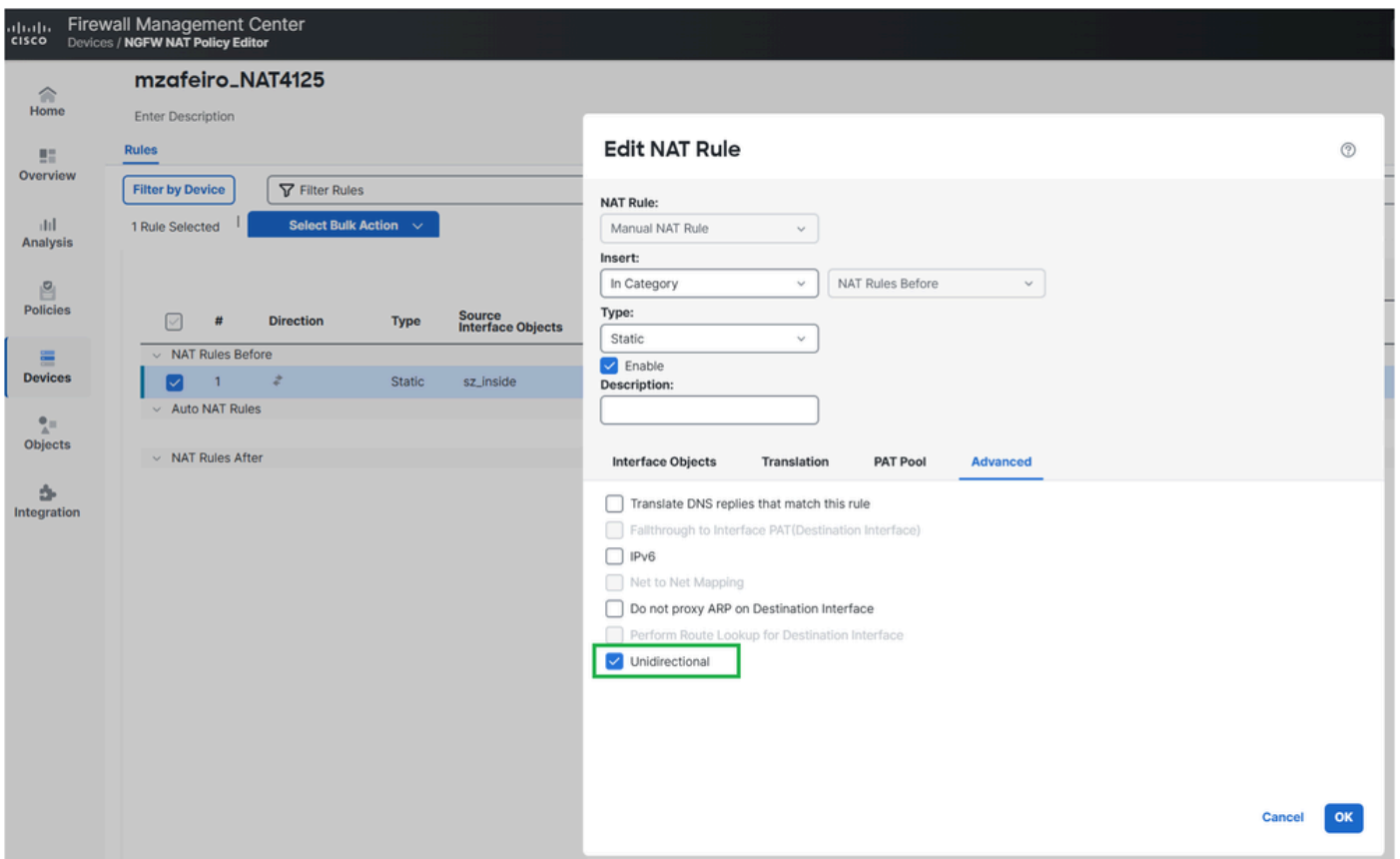
Résolution

Les solutions possibles dépendent de l'objectif de la règle NAT configurée.

Solution 1

Si l'objectif était de traduire l'adresse IP du serveur interne uniquement pour l'accès sortant, vous pouvez configurer la règle NAT comme étant unidirectionnelle.

Sur FMC, ceci peut être fait à partir des options avancées de la règle NAT :



image_en_ligne_0.png

La configuration NAT déployée :

```
<#root>
```

```
firepower#
```

```
show run nat
```

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

Vérification

```
<#root>
```

```
firepower#
```

```
traceroute 192.168.203.89
```

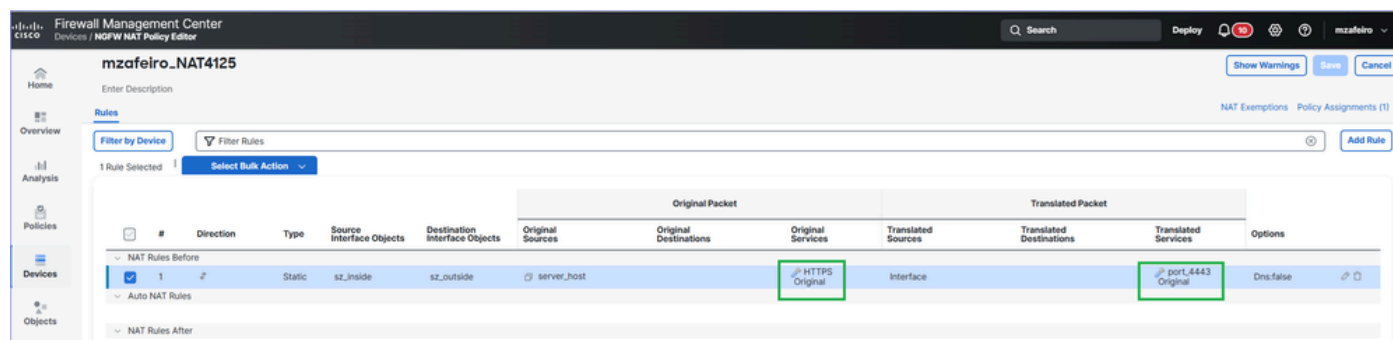
Type escape sequence to abort.

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
```

Solution 2

Si l'objectif est que le serveur interne soit accessible de l'extérieur, vous pouvez rendre la règle NAT plus spécifique en configurant le transfert de port :



image_en_ligne_0.png

La configuration NAT déployée :

```
<#root>
```

```
firepower#
```

```
show run nat
```

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

Vérification

```
<#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
```

Comment ça fonctionne

Comment ça fonctionne

Ping

1. Le pare-feu envoie un message de requête d'écho (ICMP Type 8 Code 0).
2. Une nouvelle connexion de pare-feu est créée pour ICMP.
3. Le pare-feu reçoit un message de réponse d'écho (ICMP Type 0 Code 0).
4. Le message correspond à la connexion créée à l'étape 2.
5. Le message de réponse d'écho est utilisé par le pare-feu.

Traceroute

1. Le pare-feu envoie trois paquets UDP à partir des ports 33434, 33435 et 33436 vers la destination avec TTL 1.
2. Une nouvelle connexion de pare-feu est créée pour UDP.

- Le pare-feu reçoit soit une durée de vie ICMP dépassée en transit (code 0 de type 1), soit un port ICMP inaccessible (code 3 de type 3).
- Une fois que les paquets ICMP arrivent sur le pare-feu, ils sont traités comme des connexions différentes des paquets UDP de l'étape 2.

Ceci peut être vu dans Wireshark :

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 transit device
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
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) Reply from transit device
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 the destination
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
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)

image_en_ligne_0.png

Dépannage

Étape 1

Activez les captures de paquets sur l'interface de sortie du pare-feu avec le suivi pour voir comment le pare-feu traite les paquets entrants :

```
<#root>
```

```
firepower#
```

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

Étape 2

Testez à l'aide de 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
```

Testez ensuite avec 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*  *  *
```

```
...
```

Étape 3

Vérifiez le contenu de la capture :

- Les paquets 1 à 10 sont liés au test ping ICMP.
- Les paquets 11 à 16 sont liés à traceroute. Les réponses proviennent du premier saut.

- Les paquets 17 à 28 sont également liés à traceroute. Les réponses proviennent du point d'extrémité de destination.

```
<#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
```

Étape 4

Suivez les paquets ICMP entrants à partir du test ping.

Le paquet #2 est la réponse à la requête ping ICMP envoyée dans le paquet #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
```

Les points clés de la trace sont les suivants :

- Le paquet correspondait à un flux existant.
- L'interface de sortie est le pare-feu lui-même (interface d'identité).

Étape 5

Suivez les paquets ICMP entrants à partir du test traceroute.

Le paquet #12 est la réponse de l'hôte de transit :

```
<#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
```

- Le paquet fait partie d'une nouvelle connexion (il ne correspond pas à un flux existant).

- Le paquet est soumis à la traduction d'adresses réseau (plus précisément, l'UN-NAT signifie NAT de destination).
- Le paquet est traité comme un trafic de transit de pare-feu et est soumis à la politique de contrôle d'accès (ACP) et à l'inspection Snort.
- L'interface de sortie (sortie) est INSIDE. Cela est dû à la traduction NAT.

Motif

Dans ce cas, le problème est causé par cette règle NAT statique :

```
<#root>
```

```
firepower#
```

```
show run nat
```

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

Autres informations utiles

- [Autoriser Traceroute via Firepower Threat Defense \(FTD\)](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.