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

Table des matières

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 ne fonctionne pas :

<#root>

```
firepower#

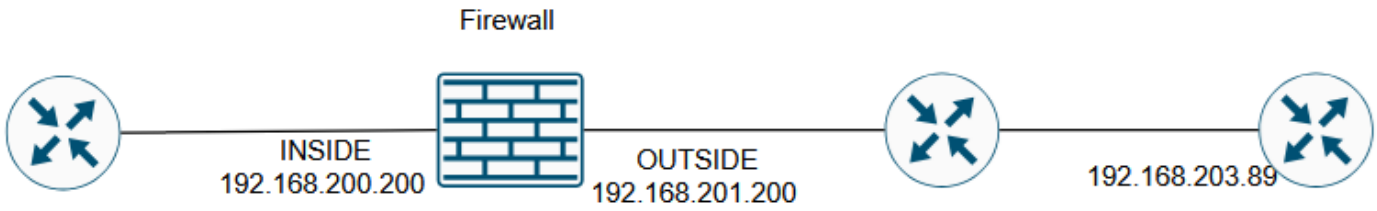
traceroute 192.168.203.89


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 observation à : 7.4, 7.4.2.3, 7.6.2. D’autres versions peuvent 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



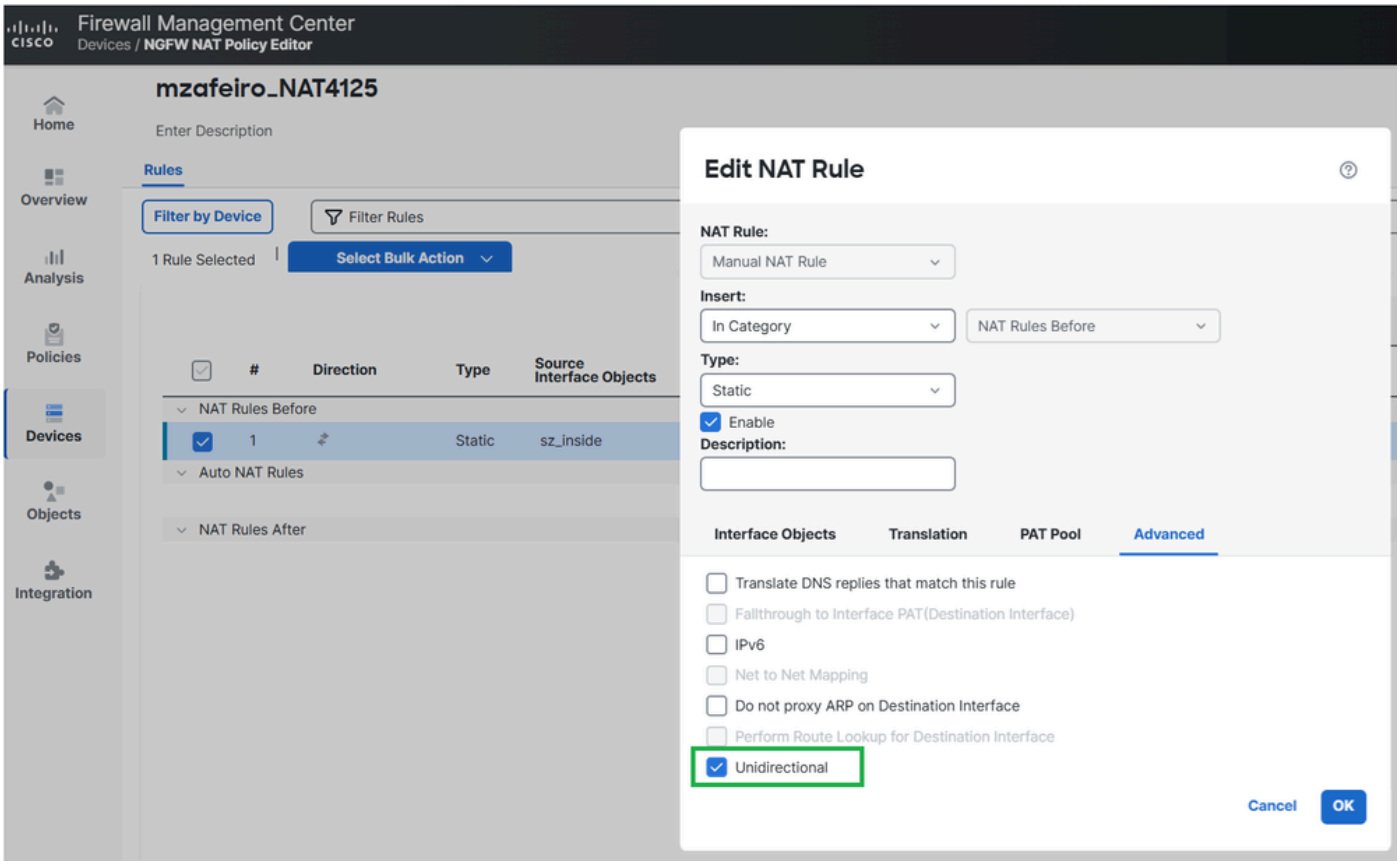
Résolution

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 :



La configuration NAT déployée :

```
<#root>

firepower#

show run nat


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

Vérification

```
<#root>

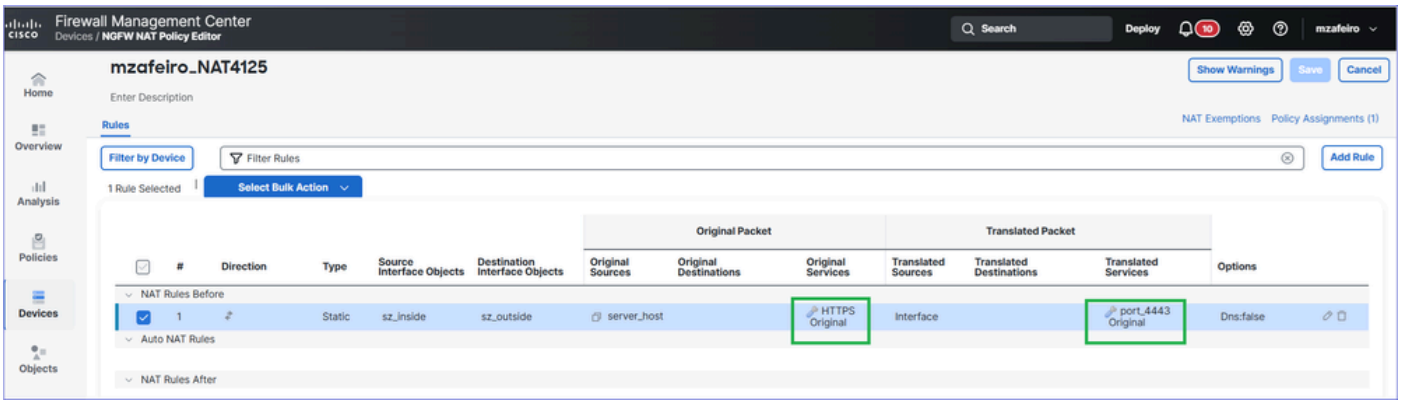
firepower#

 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 :



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

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.

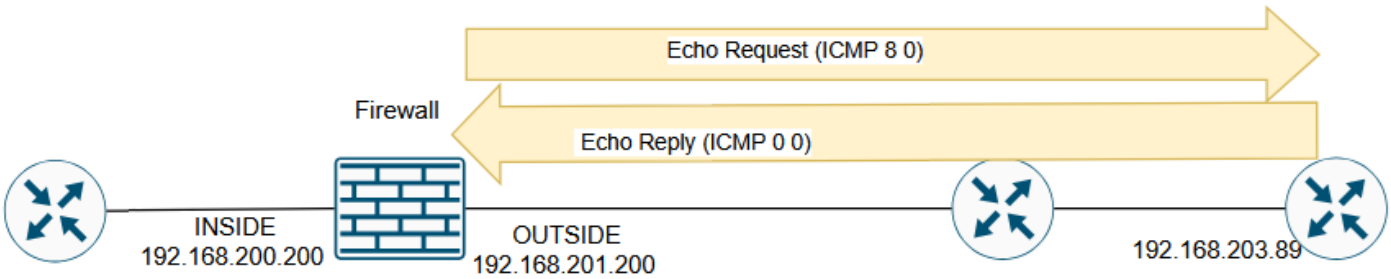
Traceroute

1.- Le pare-feu envoie trois paquets UDP à partir des ports 33434, 33435 et 33436 vers la destination avec TTL 1.

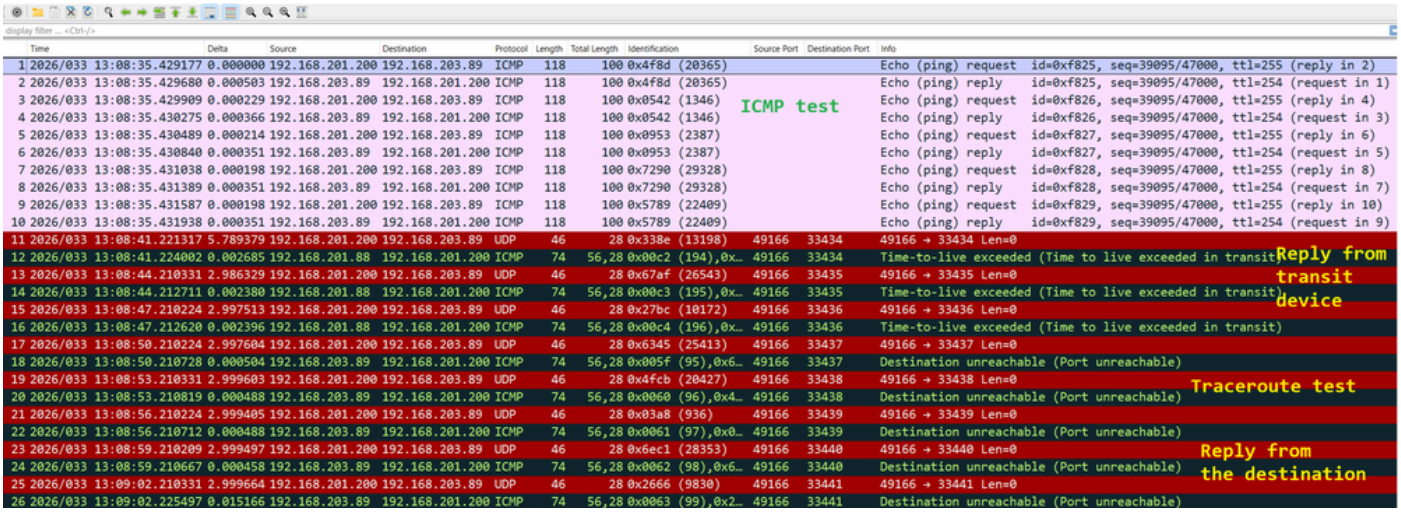
2.- Une nouvelle connexion de pare-feu est créée pour UDP.

3.- Le pare-feu reçoit soit un ICMP TTL dépassé en transit (Type 11 Code 0) soit un ICMP Port inaccessible (Type 3 Code 3).

4.- 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 :



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 17-28 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 (de 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.