Dépannage de l'échec intermittent de traduction de paquets NAT IOS-XE

Table des matières

- Introduction
- Informations générales
- Plates-formes concernées
- Démonstration du contournement de la NAT
  - Flux de trafic vers une destination non-NAT
  - Le trafic provenant de la même source tente d'envoyer une destination NAT
  - Restauration du trafic lié à la NAT
- Exemple de problème
- Solution/Correction
  - Solution 1
  - Solution 2
  - Solution 3
- Résumé
- Références

Introduction

Ce document décrit les paquets non traduits contournant la NAT sur un routeur Cisco IOS XE, ce qui peut entraîner une panne de trafic.

Informations générales

Dans la version 12.2(33)XND du logiciel, une fonctionnalité appelée contrôleur d'accès NAT (Network Address Translation) a été introduite et activée par défaut. Le contrôleur d'accès NAT a été conçu pour empêcher les flux non-NAT d'utiliser un CPU excessif pour créer une traduction NAT. Pour ce faire, deux petits caches (un pour la direction in2out et un pour la direction out2in) sont créés en fonction de l'adresse source. Chaque entrée de cache se compose d'une adresse source, d'un ID de routage et de transfert virtuel (VRF), d'une valeur de minuteur (utilisée pour invalider l'entrée après 10 secondes) et d'un compteur de trames. La table contient 256 entrées qui constituent le cache. S'il existe plusieurs flux de trafic provenant de la même adresse source, où certains paquets nécessitent la fonction NAT et d'autres non, il est possible que les paquets ne soient pas traités par la fonction NAT et envoyés via le routeur sans être traduits. Cisco recommande aux clients d'éviter autant que possible d'avoir des flux NAT et non NAT sur la même interface.

Remarque : Ce problème n'est pas lié au H.323.

Plates-formes concernées

- ISR1K
- ISR4K
- ASR1K
- C820
- C830
- C850

Démonstration du contournement de la NAT

Cette section décrit comment NAT peut être contournée en raison de la fonctionnalité NAT gatekeeper. Examinez le schéma en détail. Vous pouvez voir un routeur source, un pare-feu ASA (Adaptive Security Appliance), le routeur ASR1K et le routeur de destination.

Flux de trafic vers une destination non-NAT

1. La commande ping est lancée à partir de la source : Source : 172.17.250.201 Destination : 198.51.100.11 .
2. Le paquet arrive sur l'interface interne de l'ASA qui effectue la traduction d'adresse source. Le paquet a maintenant la source suivante : 203.0.113.231 Destination : 198.51.100.11 .
3. Le paquet arrive à l'ASR1K sur l'interface NAT externe à interne. La traduction NAT ne trouve aucune traduction pour l'adresse de destination et le cache « out » du portier est donc rempli avec l'adresse source 203.0.113.231.
4. Le paquet arrive à destination. La destination accepte le paquet ICMP (Internet Control Message Protocol) et renvoie une réponse d’écho ICMP, ce qui entraîne la réussite de la requête ping.

Le trafic provenant de la même source tente d'envoyer une destination NAT

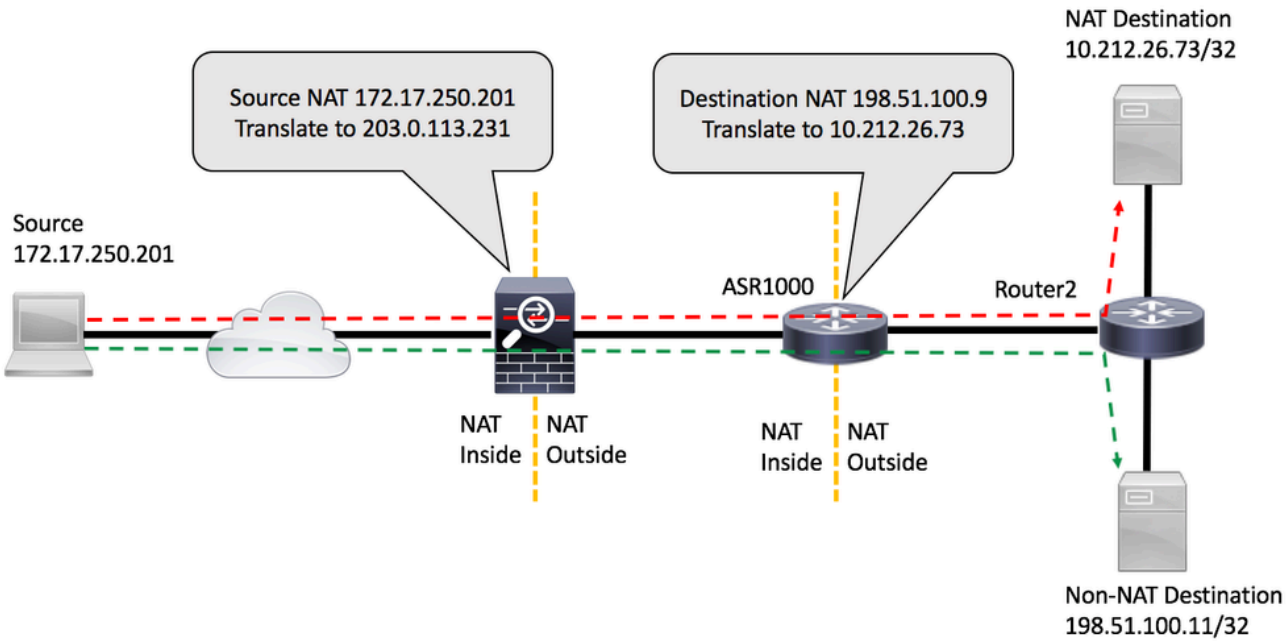
1. .Ping est lancé à partir de la source : Source : 172.17.250.201 Destination : 198.51.100.9 .
2. Le paquet arrive sur l'interface interne de l'ASA qui effectue la traduction d'adresse source. Le paquet a maintenant la source suivante : 203.0.113.231 Destination : 198.51.100.9 .
3. Le paquet arrive à l'ASR1K sur l'interface NAT externe à interne. La fonction NAT recherche d’abord une traduction pour la source et la destination. Comme il n'en trouve pas, il vérifie le cache « out » du portier et trouve l'adresse source 203.0.113.231. Il suppose (à tort) que le paquet n'a pas besoin d'être traduit et transfère le paquet s'il existe une route pour la destination ou abandonne le paquet. Dans les deux cas, le paquet n’atteint pas la destination prévue.

Restauration du trafic lié à la NAT

1. Au bout de 10 secondes, l'entrée de l'adresse source 203.0.113.231 expire dans le cache des appels sortants du contrôleur d'accès.

> Remarque : L'entrée existe toujours physiquement dans le cache, mais comme elle a expiré, elle n'est pas utilisée.

2. Maintenant, si la même source 172.17.250.201 envoie à la destination NAT 198.51.100.9. Lorsque le paquet arrive à l'interface out2in sur l'ASR1K, aucune traduction n'est trouvée. Lorsque vous vérifiez le cache de sortie du portier, vous ne trouvez pas d'entrée active. Vous créez donc la traduction pour la destination et le flux de paquets comme prévu.
3. Le trafic dans ce flux continue tant que les traductions ne sont pas expirées en raison de l'inactivité. Si, entre-temps, la source envoie à nouveau le trafic vers une destination non-NAT, ce qui entraîne le remplissage d'une autre entrée dans le gatekeeper hors du cache, cela n'affecte pas les sessions établies mais il y a une période de 10 secondes pendant laquelle les nouvelles sessions de cette même source vers des destinations NAT échouent.



Exemple de problème

1. Une requête ping est lancée à partir du routeur source : Source : 172.17.250.201 Destination : 198.51.100.9. La requête ping est émise avec un nombre de répétitions égal à deux, en plus de [FLOW1].
2. Envoyez une requête ping à une autre destination qui n'est pas soumise à la fonction NAT par l'ASR1K : Source : 172.17.250.201 Destination : 198.51.100.11 [FLOW2].
3. Envoyez davantage de paquets à 198.51.100.9 [FLOW1]. Les premiers paquets de ce flux contournent la NAT, comme le montre la correspondance de la liste d'accès sur le routeur de destination.

```
<#root>

source#

ping 198.51.100.9 source lo1 rep 2
```

```
Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
source#ping 198.51.100.9 source lo1 rep 2

Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
source#ping 198.51.100.11 source lo1 rep 200000

Type escape sequence to abort.
Sending 200000, 100-byte ICMP Echos to 198.51.100.11, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
Success rate is 99 percent (3007/3008), round-trip min/avg/max = 1/1/16 ms
source#
```

ping 198.51.100.9 source lo1 rep 10

```
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
...!!!!!!!
Success rate is 70 percent (7/10), round-trip min/avg/max = 1/1/1 ms
source#
```

La correspondance ACL sur le routeur de destination indique que les trois paquets qui ont échoué n'ont pas été traduits :

<#root>

```
Router2#
```

show access-list 199

```
Extended IP access list 199
    10 permit udp host 172.17.250.201 host 198.51.100.9
    20 permit udp host 172.17.250.201 host 10.212.26.73
    30 permit udp host 203.0.113.231 host 198.51.100.9
    40 permit udp host 203.0.113.231 host 10.212.26.73 (4 matches)
    50 permit icmp host 172.17.250.201 host 198.51.100.9
    60 permit icmp host 172.17.250.201 host 10.212.26.73
```

70 permit icmp host 203.0.113.231 host 198.51.100.9 (3 matches) <<<<<<<

```
    80 permit icmp host 203.0.113.231 host 10.212.26.73 (42 matches)
    90 permit udp any any log (2 matches)
    100 permit icmp any any log (4193 matches)
    110 permit ip any any (5 matches)
Router2#
```

Sur l'ASR1K, vous pouvez vérifier les entrées du cache du contrôleur d'accès :

<#root>

```
PRIMARY#
```

show platform hardware qfp active feature nat datapath gatein

```
Gatekeeper on
sip 203.0.113.231 vrf 0 cnt 1 ts 0x17ba3f idx 74
sip 10.203.249.226 vrf 0 cnt 0 ts 0x36bab6 idx 218
sip 10.203.249.221 vrf 0 cnt 1 ts 0x367ab4 idx 229

PRIMARY#
```

show platform hardware qfp active feature nat datapath gateout

```
Gatekeeper on
sip 198.51.100.11 vrf 0 cnt 1 ts 0x36db07 idx 60
sip 10.203.249.225 vrf 0 cnt 0 ts 0x36bb7a idx 217
sip 10.203.249.222 vrf 0 cnt 1 ts 0x367b7c idx 230
```

Solution/Correction

Dans la plupart des environnements, la fonctionnalité NAT gatekeeper fonctionne correctement et ne pose aucun problème. Cependant, si vous rencontrez ce problème, il existe plusieurs façons de le résoudre.

Solution 1

L'option privilégiée consiste à mettre à niveau Cisco IOS® XE vers une version qui inclut l'amélioration du contrôleur d'accès :

ID de bogue Cisco CSCun06260 XE3.13 Renforcement du contrôleur d'accès

Cette amélioration permet au contrôleur d'accès NAT de mettre en cache les adresses source et de destination, et rend la taille du cache configurable. Pour activer le mode étendu, vous devez augmenter la taille du cache avec ces commandes. Vous pouvez également surveiller le cache pour voir si vous devez augmenter la taille.

<#root>

```
PRIMARY(config)#
ip nat settings gatekeeper-size 1024

PRIMARY(config)#
end
```

Le mode étendu peut être vérifié en vérifiant ces commandes :

<#root>

```
PRIMARY#
show platform hardware qfp active feature nat datapath gatein

Gatekeeper on

sip 10.203.249.221 dip 10.203.249.222 vrf 0 ts 0x5c437 idx 631
PRIMARY#
show platform hardware qfp active feature nat datapath gateout

Gatekeeper on

sip 10.203.249.225 dip 10.203.249.226 vrf 0 ts 0x5eddf idx 631
PRIMARY#
show platform hardware qfp active feature nat datapath gatein active

Gatekeeper on

ext mode Size 1024
, Hits 2, Miss 4, Aged 0 Added 4 Active 1
PRIMARY#
show platform hardware qfp active feature nat datapath gateout active

Gatekeeper on

ext mode Size 1024
, Hits 0, Miss 1, Aged 1 Added 2 Active 0
```

Solution 2

Pour les versions qui n'ont pas le correctif pour l'ID de bogue Cisco CSCun06260, la seule option est de désactiver la fonctionnalité de garde-barrière. Le seul impact négatif est une légère réduction des performances pour le trafic non-NAT ainsi qu'une utilisation plus élevée du CPU sur le processeur Quantum Flow Processor (QFP).

```
<#root>

PRIMARY(config)#

no ip nat service gatekeeper

PRIMARY(config)#

end

PRIMARY#PRIMARY#

Sh platform hardware qfp active feature nat datapath gatein

Gatekeeper off

PRIMARY#
```

L'utilisation de QFP peut être surveillée avec ces commandes :

```
<#root>

show platform hardware qfp active data utilization summary

show platform hardware qfp active data utilization qfp 0
```

Solution 3

Séparez les flux de trafic de sorte que les paquets NAT et non-NAT n'arrivent pas sur la même interface.

Résumé

La commande NAT Gatekeeper a été introduite pour améliorer les performances du routeur pour les flux non terminés par NAT. Dans certaines conditions, la fonctionnalité peut causer des problèmes lorsqu'un mélange de paquets NAT et non-NAT arrive de la même source. La solution consiste à utiliser la fonctionnalité de gatekeeper améliorée ou, si cela n'est pas possible, à

désactiver la fonctionnalité de gatekeeper.

Références

Modifications logicielles qui ont permis de désactiver le contrôleur d'accès :

- ID de bogue Cisco CSCty67184 : CLI NAT ASR1k - Garde-barrière activé/désactivé
- ID de bogue Cisco CSCth23984 : Ajout de la fonctionnalité CLI pour activer/désactiver la fonctionnalité NAT Gatekeeper

Amélioration de NAT Gatekeeper :

- ID de bogue Cisco CSCun06260 : XE3.13 Renforcement du contrôleur d'accès

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.

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.