ASR1k NAT par intermittence ne traduit pas quelques paquets

Contenu

Introduction

Cet article explique une situation où des paquets qui devraient être traduits par NAT sur un ASR1k ne sont pas traduits (NAT étant sauté). Ceci pourrait avoir comme conséquence la panne du trafic car le prochain saut est probable non configuré pour permettre les paquets non traduits à traiter.

Informations générales

Dans la version de logiciel 12.2(33)XND une caractéristique appelée le garde-porte de NAT a été introduite et activée par défaut. (Notez ceci n'a rien à faire avec H.323). Le garde-porte NAT a été conçu pour empêcher des écoulements de non-NAT-ed d'utiliser la CPU excessive dans un effort de créer une traduction NAT. Pour réaliser ceci, deux petits caches (un pour la direction in2out et un pour la direction out2in) sont créés ont basé sur l'adresse source. Chaque entrée de cache se compose d'une adresse source, d'un ID de VRF, d'une valeur de temporisateur (utilisée pour infirmer l'entrée après 10 secondes), et d'un compteur de trame. Il y a 256 entrées dans la table qui compose le cache. S'il y a des écoulements du trafic multiple de la même adresse source où quelques paquets en exigent NAT et ne font pas, il pourrait avoir comme conséquence les paquets n'étant pas Nat-ed et envoyé par le routeur non traduit. Cisco recommande que les clients devraient éviter d'avoir le Nat-ed et le non-NAT-ed circule sur la même interface dans la mesure du possible.

Démonstration de NAT étant sauté

La section suivante décrit combien NAT peut être en raison sauté de la caractéristique NAT de garde-porte. Veuillez examiner le diagramme en détail. Nous pouvons voir qu'il y a un routeur de source, un Pare-feu ASA, les ASR1k, et le routeur de destination.

La circulation à la destination de Non-NAT-ed :

1) Le ping est initié de la source : Source : Destination de 172.17.250.201 : 198.51.100.11
2) Le paquet arrive sur l'interface interne de l'ASA qui exécute la translation d'adresses d'adresse source. Le paquet aura maintenant la source : Destination de 203.0.113.231 : 198.51.100.11
3) Le paquet arrive à l'ASR1k sur l'interface NAT d'externe vers interne. La traduction NAT ne trouve aucune traduction pour l'adresse de destination et ainsi le garde-porte « » cachent est rempli avec l'adresse source 203.0.113.231
4) Le paquet arrive à la destination. La destination reçoit le paquet d'ICMP et renvoie une réponse d'écho d'ICMP ayant pour résultat le succès de ping.

Le trafic des mêmes tentatives de source d'envoyer la destination de Nat-ed :

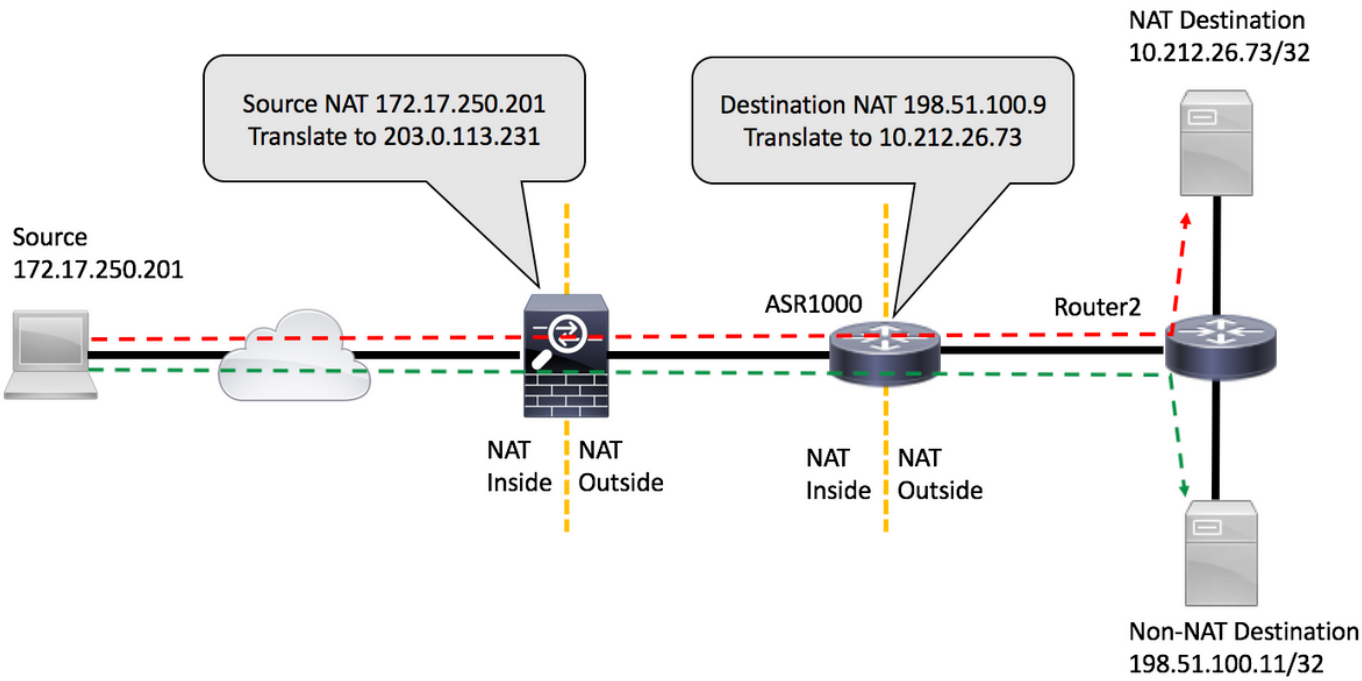
1) Le ping est initié de la source : Source : Destination de 172.17.250.201 : 198.51.100.9
2) Le paquet arrive sur l'interface interne de l'ASA qui exécute la translation d'adresses d'adresse source. Le paquet aura maintenant la source : Destination de 203.0.113.231 : 198.51.100.9
3) Le paquet arrive à l'ASR1k sur l'interface NAT d'externe vers interne. Le premier NAT recherche une traduction pour la source et la destination. Ne trouvant pas un, il vérifie le garde-porte « » cachent et découvrent l'adresse source 203.0.113.231. Il (incorrectement) suppose que le paquet n'a pas besoin de la traduction et non plus en avant du paquet si une artère existe pour la destination ou relâche le paquet. L'un ou l'autre de manière, le paquet n'atteindra pas la destination destinée.

Restauration du trafic de Nat-ed

1) Après 10 secondes, l'entrée pour l'adresse source 203.0.113.231 chronomètre dans le garde-porte cachent. (Note que l'entrée existe toujours physiquement dans le cache mais parce qu'elle a expiré, il n'est pas utilisé).

2) Maintenant si la même source : 172.17.250.201 envoie à la destination 198.51.100.9 de Nat-ed, quand le paquet arrive à l'interface out2in sur l'ASR1K, aucune traduction sera trouvé. Quand nous vérifions le garde-porte cachons, nous ne trouverons pas une entrée active et ainsi nous créerons la traduction pour l'écoulement de willl de destination et de paquets comme prévu.

3) Le trafic dans cet écoulement continuera tant que les traductions ne sont pas chronométré dues à l'inactivité. Si dans le même temps, la source envoie de nouveau le trafic à une destination de non-NAT-ed, causant une autre entrée d'être rempli dans le garde-porte cachez, il n'affectera pas a établi des sessions mais il y aura une seconde période 10 l'où les nouvelles sessions de cette même source aux destinations de Nat-ed échoueront.



Exemple de la question

1) Le ping est initié du routeur de source : Source : Destination de 172.17.250.201 : 198.51.100.9. Le ping est émis avec le compte de répétition de 2, à plusieurs reprises [FLOW1].

2) Cinglez alors une destination différente qui n'est pas Nat-ed par la source ASR1k : 172.17.250.201 Destination:198.51.100.11 [FLOW2].

3) Envoyez alors plus de paquets à 198.51.100.9 [FLOW1]. Les paquets premiers de cet écoulement sauteront NAT comme vu par la liste d'accès s'assortissant sur le routeur de destination.

```
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 d'ACL sur les routeurs show de destination les 3 paquets qui ont manqué, n'ont pas été traduites :

```
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 ASR1k nous pouvons vérifier le cache entries de garde-porte :

```
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
```

Contournement/difficulté :

Dans la plupart des environnements la fonctionnalité NAT de garde-porte fonctionne bien sans entraîner des questions. Cependant si vous rencontrez ce problème il y a quelques manières de le résoudre.

Solution #1 :

L'option préférée serait d'améliorer IOS-XE à une version qui inclut l'amélioration de garde-porte :

Durcissement de garde-porte CSCun06260 XE3.13

Cette amélioration tient compte pour que le garde-porte NAT cache la source **et les** adresses de destination, aussi bien que rend la taille de mise en cache configurable. Afin d'activer le mode étendu, vous devez augmenter la taille de mise en cache avec les commandes suivantes. Vous pouvez surveillez également le cache pour voir si vous devez augmenter la taille.

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

Le mode étendu peut être vérifié en vérifiant les commandes suivantes :

```
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 releases qui n'ont pas la difficulté pour CSCun06260, la seule option est d'arrêter la caractéristique de garde-porte. La seule incidence négative sera représentation légèrement réduite pour le trafic de non-NAT-ed aussi bien qu'une utilisation du processeur plus élevée sur le QFP.

```
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 QFP peut être surveillée avec :

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

Solution #3 :

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

Résumé

L'ordre NAT de garde-porte a été introduit d'améliorer la représentation du routeur pour des écoulements de non-NAT-ed. Dans certaines conditions la caractéristique peut poser des problèmes quand un mélange de paquets NAT et non-NAT arrivent de la même source. La solution est d'utiliser la fonctionnalité améliorée de garde-porte, ou si ce n'est pas possible, désactive la configuration de garde-porte.

Références

Modifications de logiciel qui ont permis le garde-porte à arrêter :

CSCty67184 ASR1k CLI NAT - Garde-porte "Marche/Arrêt"

CSCth23984 ajoutent la capacité cli pour activer/désactiver la fonctionnalité nat de garde-porte

Amélioration NAT de garde-porte

Durcissement de garde-porte CSCun06260 XE3.13