Dépannage de la NAT sur les plates-formes Cat8000

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Diagramme du réseau
- Étude de cas NAT Exhausted Exhausted Pool
  - Cause possible
- NAT traduit une étude de cas d'un problème de portier d'adresses IP non natives
  - Identifier le symptôme
    - Résultat Sain
    - Si le résultat n'est pas sain
  - Recommandations
- Informations connexes

Introduction

Ce document décrit comment dépanner les problèmes NAT sur les plates-formes Cat8000.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Traduction d'adresses réseau (NAT)
- Cisco IOS®

Pour plus d'informations sur ces sujets, consultez :

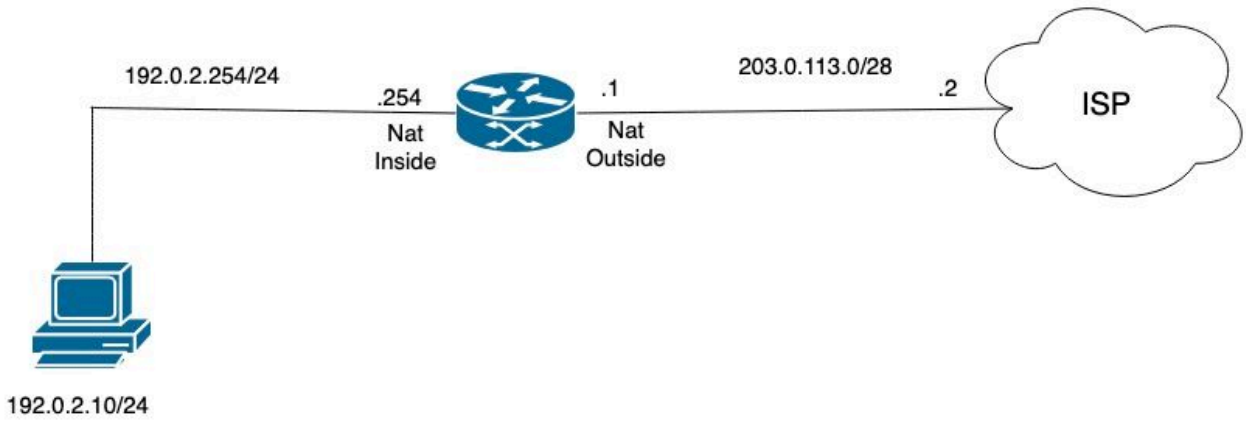
- Configurer la traduction d’adresse réseau
- Comprendre l'ordre de fonctionnement de la NAT
- Traduction d'adresses de réseau (NAT) - Forum aux questions
- Restrictions relatives à la configuration de NAT pour la conservation des adresses IP

Composants utilisés

Les informations contenues dans ce document sont basées sur la plate-forme logicielle Cisco IOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Diagramme du réseau



Topologie NAT

Étude de cas NAT Exhausted Exhausted Pool

Ce message de journal indique que le périphérique a tenté d'allouer une adresse IP pour NAT, par exemple pour une traduction NAT ou PAT dynamique, mais que l'allocation a échoué. Cela se produit généralement lorsqu'il ne reste aucune adresse ou aucun port disponible dans le pool NAT configuré.

Causes courantes :

· Le pool NAT est épuisé (toutes les adresses IP ou ports disponibles sont utilisés).
· La configuration NAT ne dispose pas d'adresses ou de ressources suffisantes pour prendre en charge les demandes de traduction actuelles.

```
%NAT-6-ADDR_ALLOC_FAILURE: Address allocation failed; pool 2 may be exhausted [2] port range: NA, non-P
created by pkt: src_ip 192.0.2.13 dst_ip 192.x.x.40 src_port 0 dst_port 0 proto 1
```

Étape 1 : vérification du pool NAT pour confirmer la plage de traduction d'adresses

<#root>

```
NAT_R1#

show ip nat pool platform


Dump NAT pool config

ID: 2, Name: NAT_Pool, Type: Generic, Mask: 255.255.255.240
Flags: Unknown, Acct name:
Address range blocks: 1

Start: 203.0.113.3, End: 203.0.113.5


Last stats update: 07/31 13:08:43.708061785

Last refcount value: 3
```

Étape 2 : vérification de la table de traduction NAT et détermination du nombre de traductions actives actuellement présentes

<#root>

```
NAT_R1#

show ip nat translations


Pro Inside global Inside local Outside local Outside global
--- 203.0.113.3 192.0.2.10 --- ---
--- 203.0.113.5 192.0.2.12 --- ---
--- 203.0.113.4 192.0.2.11 --- ---
```

```
icmp 203.0.113.5:0 192.0.2.12:0 198.51.100.30:0 198.51.100.30:0
icmp 203.0.113.3:0 192.0.2.10:0 198.51.100.10:0 198.51.100.10:0
icmp 203.0.113.4:0 192.0.2.11:0 198.51.100.20:0 198.51.100.20:0

Total number of translations: 6
```

Étape 3 : vérification de l'affichage des abandons dans les statistiques NAT Ce résultat indique que le trafic entrant nécessite une traduction, mais que des abandons se produisent en raison de problèmes d'allocation NAT.

<#root>

```
NAT_R1#

show ip nat statistics


Total active translations: 6 (0 static, 6 dynamic; 3 extended)
Outside interfaces:
GigabitEthernet0/0/4
Inside interfaces:
GigabitEthernet0/0/3
Hits: 11094661606 Misses: 10
Reserved port setting disabled provisioned no
Expired translations: 1412
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 pool NAT_Pool

refcount 6


 <---- Translations count
pool NAT_Pool: id 2, netmask 255.255.255.240
start 203.0.113.3 end 203.0.113.5
type generic, total addresses 3, allocated 3 (100%), misses 3559386331
nat-limit statistics:
max entry: max allowed 0, used 0, missed 0

In-to-out drops: 3559337007


 Out-to-in drops: 0  <---- drops from in to out
Pool stats drop: 0 Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
NAT_R1#
```

Étape 4. Du point de vue de la plate-forme, passez en revue les statistiques NAT de chemin de données QFP pour déterminer si ces abandons correspondent au problème observé.

<#root>

NAT_R1#

show platform hardware qfp active feature nat datapath stats

Counter	Value
number_of_session	**3**
udp	0
tcp	0
icmp	**3**
non_extended	**3**
statics	0
static_net	0
entry_timeouts	**1**
hits	**585149**
misses	**0**
cgn_dest_log_timeouts	0
ipv4_nat_alg_bind_pkts	0
ipv4_nat_alg_sd_not_found	0
ipv4_nat_alg_sd_tail_not_found	0
ipv4_nat_rx_pkt	**154**
ipv4_nat_tx_pkt	**18791285989**

<snip>

ipv4_nat_non_natted_in2out_pkts	**144**

```
ipv4_nat_non_nated_out2in_pkts                                  0

<snip>

ipv4_nat_cfg_rcvd                                               8


ipv4_nat_cfg_rsp                                                9


Subcode#14 ADDR_ALLOC_FAIL                                5216959285
```

- numéro_de_session : Indique le nombre total de sessions NAT actives actuellement présentes dans le chemin de données QFP. Dans ce résultat, la valeur est 3, ce qui confirme que trois sessions NAT sont actives au moment de la collecte.
- icmp: Affiche le nombre de sessions NAT actives pour le trafic ICMP. Une valeur de 3 indique que toutes les sessions NAT actives dans ce résultat sont des sessions ICMP.
- non_étendu : Indique le nombre de sessions NAT classées par la plate-forme comme entrées non étendues. Dans ce résultat, la valeur est 3, ce qui correspond aux trois sessions ICMP actives affichées dans le chemin de données.
- entry_timeouts : Indique le nombre d'entrées de session NAT qui ont expiré et ont été supprimées du chemin de données. La valeur 1 confirme qu'une entrée NAT a expiré.
- hits : un hit signifie que le paquet correspond à une entrée de session existante dans la table de hachage de session NAT. La valeur 585149 indique que les paquets correspondent à une session NAT existante.
- échecs : Affiche le nombre de recherches NAT qui n'ont pas trouvé de traduction correspondante dans le chemin de données. La valeur 0 indique qu'aucun échec de recherche n'est enregistré dans ce résultat.
- ipv4_nat_rx_pkt : Affiche le nombre de paquets IPv4 reçus par ce chemin de gestion de chemin de données NAT. Une valeur de 154 indique que 154 paquets ont été enregistrés par ce compteur de réception interne.
- ipv4_nat_tx_pkt : Affiche le nombre de paquets IPv4 transmis par ce chemin de gestion de chemin de données NAT. Une valeur de 18791285989 indique une très grande activité de transfert de paquets via ce compteur de transmission interne.
- ipv4_nat_non_natted_in2out_pkts : Indique le nombre de paquets IPv4 vus dans la direction interne-externe qui n'ont pas été traduits par NAT. Une valeur de 144 confirme que 144 paquets ont traversé ce chemin sans que la fonction NAT soit appliquée.
- ipv4_nat_non_nated_out2in_pkts : Indique le nombre de paquets IPv4 vus dans la direction de l'extérieur vers l'intérieur qui n'ont pas été traduits par NAT. La valeur 0 indique qu'aucun paquet de ce type n'est enregistré dans cet instantané.
- ipv4_nat_cfg_rcvd : Affiche le nombre de messages de configuration liés à la NAT reçus par

le chemin de données. La valeur 8 confirme la réception de huit messages de configuration.
- ipv4_nat_cfg_rsp : Affiche le nombre de réponses de configuration liées à la NAT envoyées par le chemin de données. Une valeur de 9 confirme que neuf réponses de configuration ont été envoyées.
- Sous-code#14 ADDR_ALLOC_FAIL : Affiche le nombre d'échecs d'allocation d'adresses de chemin de données NAT. Une valeur de 5216959285 indique que le chemin de données a enregistré un nombre très élevé d'échecs d'allocation au fil du temps. Ce compteur est très pertinent lors de l'étude des problèmes de traduction NAT intermittents et nécessite une corrélation avec les sorties show ip nat statistics, show ip nat translations et QFP NAT datapath supplémentaires.

Étape 5. Vérifiez le nombre actuel d'entrées et comparez les valeurs maxhost_count et maxhost_himark :

- maxhost_count : La présente les entrées actuelles du routeur.
- maxhost_himark : La montre 7, ce qui indique que la limite a été atteinte à un certain point.

<#root>

```
NAT_R1#

show platform hardware qfp active feature nat datapath limit


maxhost_limit 131072

maxhost_count 5

 maxhost_fail 0

maxhost_himark 7


total limit entries 0 hash tbl 0x0 max entries 0 limit_chunk 0x0 allvrf limit 0
acl limit 0 acl count 0 acl fail 0 acl_id 0x0
```

Des informations détaillées sur ce journal fournissent une description complète des événements enregistrés et de l'état opérationnel :

- maxhost_limit : Spécifie le nombre maximal d'entrées d'hôte NAT prises en charge par la plate-forme. Cette valeur représente la limite supérieure des sessions ou des traductions NAT pouvant être traitées.

- maxhost_count : Indique le nombre actuel d'entrées ou de sessions d'hôte NAT actives utilisées.
- maxhost_fail : Affiche le nombre de tentatives infructueuses d'allocation d'une entrée d'hôte NAT en raison de l'atteinte de la limite maximale. La valeur zéro indique qu'aucune erreur d'allocation ne s'est produite.
- maxhost_himark : Représente la limite supérieure, ou le nombre maximal, des entrées d'hôte NAT utilisées depuis la dernière réinitialisation ou redémarrage du système.
- total des entrées de limite : Affiche le nombre total d'entrées de limite NAT configurées ou appliquées.
- hash tbl 0x0 : Affiche l'adresse mémoire ou le pointeur vers la table de hachage utilisée pour les entrées de limite NAT. La valeur 0x0 indique qu'aucune table de hachage n'est actuellement allouée.
- entrées max : Spécifie le nombre maximal d'entrées autorisées dans la table de limites NAT. Une valeur nulle indique qu'aucune limite n'est configurée.
- limit_chunk 0x0 : Indique le pointeur vers un bloc de mémoire alloué pour les entrées de limite NAT. Une valeur de 0x0 signifie qu'aucun bloc de mémoire n'est alloué.
- limite de VRF : Représente la limite NAT appliquée à tous les VRF (instances de routage et de transfert virtuels). Une valeur nulle indique qu'aucune limite globale n'est définie.
- limite acl : Spécifie la limite des entrées NAT imposées par les listes de contrôle d'accès (ACL). Une valeur nulle indique qu'aucune limite basée sur les listes de contrôle d'accès n'est configurée.
- nombre acl : Affiche le nombre actuel d'entrées NAT associées aux listes de contrôle d'accès.
- échec acl : Affiche le nombre d'échecs des entrées NAT en raison des limites ACL.
- acl_id 0x0 : Représente l'identificateur ou le pointeur lié à la configuration de la liste de contrôle d'accès. La valeur 0x0 indique qu’aucune configuration de liste de contrôle d’accès n’est attribuée.

Cause possible

Le nombre d’adresses utilisables dans le pool NAT est compris entre 3 et 5. Des problèmes se produisent lorsque des traductions inactives restent dans la table NAT, ce qui empêche la traduction d’autres trafics. Ce comportement est attendu, car le délai de traduction NAT par défaut est de 24 heures. Pour résoudre ce problème, configurez la commande ip nat translation timeout pour effacer les traductions inactives après cette action, la table NAT doit être claire.

<#root>

```
NAT_R1(config)#
```

ip nat translation timeout 10800

```
NAT_R1(config)#end
NAT_R1#

clear ip nat translation *


NAT_R1#

show ip nat translations


Pro Inside global Inside local Outside local Outside global
--- 203.0.113.5 192.0.2.11 --- ---
--- 203.0.113.4 192.0.2.10 --- ---
icmp 203.0.113.4:0 192.0.2.10:0 198.51.100.10:0 198.51.100.10:0
icmp 203.0.113.5:0 192.0.2.11:0 198.51.100.20:0 198.51.100.20:0
Total number of translations: 4
```

NAT traduit une étude de cas d'un problème de portier d'adresses IP non natives

La fonctionnalité NAT Gatekeeper est conçue pour améliorer les performances du routeur en protégeant le moteur NAT du traitement des flux non NAT. Lorsque des paquets non-NAT traversent une interface NAT, ils subissent généralement des recherches approfondies avant que la NAT ne détermine que la traduction n'est pas requise. Ce processus sollicite énormément le processeur sur le processeur de flux quantique (QFP). Le contrôleur d'accès atténue ce problème en conservant un petit cache de flux non-NAT, permettant à ces paquets de contourner le moteur NAT une fois identifiés, réduisant ainsi la charge du CPU. Les entrées du cache du contrôleur d'accès expirent relativement rapidement, ce qui permet aux flux d'être réévalués par le moteur NAT en cas de changement des conditions du réseau et le flux peut maintenant être soumis à la NAT.

Ce mécanisme permet d'optimiser l'utilisation des ressources et améliore l'efficacité globale du système lors du traitement du trafic NAT et non NAT mixte sur la même interface. La taille du cache du contrôleur d'accès peut être configurée pour prendre en charge le volume du trafic non-NAT, avec des valeurs par défaut basées sur la plate-forme. Il est recommandé de régler la taille du cache lorsque le trafic non NAT est important sur une interface NAT.

En résumé, le contrôleur d'accès NAT :

· Protège le moteur NAT du traitement inutile des flux non NAT.
· Gère un cache de flux non-NAT pour leur permettre de contourner le traitement NAT.

· Utilise des délais d'attente sur les entrées de cache pour permettre la réévaluation des flux.
· Aide à réduire l'utilisation du processeur sur le QFP.
· Prend en charge la taille de cache configurable pour optimiser les performances en fonction des modèles de trafic.

Identifier le symptôme

Les symptômes typiques sont :

- Pertes de trafic intermittentes
- Certains hôtes fonctionnent tandis que d’autres échouent
- Des traductions NAT existent mais le trafic est abandonné
- Réinitialisation inattendue des sessions d'application
- Déploiements PAT à grande échelle affectés
- Compteurs Gatekeeper croissants

Étape 1 : vérification des statistiques NAT pendant la fenêtre d’échec
Cette étape confirme :

- Si NAT reçoit du trafic correspondant
- si des traductions sont créées
- si les ratés augmentent au cours de l'émission
- Indique si le pool d'adresses ou l'état de surcharge est sain

<#root>

```
NAT_R1#

show ip nat statistics



Total active translations: 29477 (736 static, 28741 dynamic; 28741 extended)


Outside interfaces:
GigabitEthernet1
Inside interfaces:
GigabitEthernet2, GigabitEthernet3
```

Hits: 32525856687 Misses: 293948584

Expired translations: 293549953

Dynamic mappings:
-- Inside Source
[Id: 1] route-map INTERNET_PAT interface GigabitEthernet1 refcount 25
nat-limit statistics:

max entry: max allowed 0, used 0, missed 0

In-to-out drops: 0 Out-to-in drops: 867

Pool stats drop: 0 Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0

NAT_R1#

show ip nat statistics | sec Misses

Hits: 32525856687

Misses: 293948584

NAT_R1#show ip nat statistics | sec Misses
Hits: 32527039444

Misses: 293952367

NAT_R1#show ip nat statistics | sec Misses
Hits: 32527308509

Misses: 293953221

NAT_R1#

La section fournit une explication détaillée des informations pertinentes dans le résultat.

- Nombre total de traductions actives : Indique le nombre total d'entrées NAT actuellement installées dans la table de traduction. Dans ce résultat, il y a 29 477 traductions actives.
- 736 statique : Spécifie le nombre d'entrées NAT statiques actuellement actives. Ce sont des mappages fixes configurés manuellement.
- 28741 dynamique : Spécifie le nombre d'entrées NAT dynamiques actuellement actives. Ces entrées ont été créées automatiquement à partir des flux de trafic.
- 28741 étendu : Indique que toutes les entrées dynamiques sont des traductions étendues, ce qui signifie qu'elles incluent des informations de couche 4 telles que le protocole et les numéros de port. Ceci est typique pour le trafic PAT.
- Résultats : Affiche le nombre de paquets correspondant à une entrée de traduction NAT existante. Une valeur de 32 525 856 687 indique que la fonction NAT traite activement une très grande quantité de trafic.
- Échecs : Affiche le nombre de paquets qui ne correspondaient pas à une entrée de traduction NAT existante au moment de la recherche. Dans la NAT/PAT dynamique, cela se produit généralement sur le premier paquet d'un nouveau flux avant la création de la traduction. Une valeur de 293 948 584 reflète un nombre élevé de nouvelles recherches de session au fil du temps.
- Abandons d'entrée-sortie : Affiche le nombre de paquets abandonnés dans le sens intérieur-extérieur pendant le traitement NAT. Une valeur de 0 indique qu'aucune suppression NAT sortante n'a eu lieu.
- Abandons d'appels sortants vers les appels entrants : Affiche le nombre de paquets abandonnés dans le sens extérieur-intérieur pendant le traitement NAT. Une valeur de 867 indique que certains paquets entrants sont arrivés sans traduction correspondante valide ou état NAT valide.
- Statistiques du pool abandonnées : Affiche le nombre de suppressions liées à la gestion du pool NAT. La valeur 0 indique qu'aucune perte liée au pool n'a eu lieu.
- Suppression des statistiques de mappage : Affiche le nombre de abandons liés aux problèmes de mappage NAT. Une valeur de 0 indique qu'aucun abandon lié au mappage n'a eu lieu.
- Échec de l'allocation de bloc de ports : Affiche le nombre d'échecs d'allocation des blocs de ports PAT. La valeur 0 indique qu'aucune défaillance d'allocation de port ne s'est produite et qu'il n'existe aucune preuve d'épuisement du port PAT.
- Échec d'ajout d'alias IP : Affiche le nombre d'échecs liés à la création d'alias IP pour NAT. La valeur 0 indique qu'aucune défaillance liée à un alias ne s'est produite.
- Limite entrée add fail : Affiche le nombre d'échecs d'ajout d'une entrée NAT en raison d'une restriction de limite. La valeur 0 confirme qu'aucune traduction n'a été bloquée par l'application de la limite NAT.

Les statistiques NAT montrent que le compteur d'échecs augmente, mais l'augmentation se produit selon le même modèle que la création de session NAT/PAT dynamique normale.

Pendant l'intervalle observé :

Le nombre de visites est passé de 32 525 856 687 à 32 527 308 509

Incrément : 1,451,822
Le nombre de cas non réglés est passé de 293 948 584 à 293 953 221
Incrément : 4,637

Cela reflète environ 313 résultats supplémentaires pour chaque 1 échec supplémentaire au cours de la même période. Dans un environnement NAT/PAT dynamique, un échec se produit lorsqu'un paquet arrive avant qu'une traduction correspondante existe déjà dans la table. Une fois la traduction créée, les paquets suivants pour ce flux sont comptés comme des occurrences. Sur la base de ce comportement, l'augmentation observée des échecs est cohérente avec la création de session en cours et le désordre de traduction normal.

Étape 2 : vérification de l’existence de la traduction dans la table NAT Filtrez le résultat pour le flux exact affecté, le cas échéant.
Cette étape confirme si la table NAT du processeur de routage (RP) contient une entrée de traduction pour le flux affecté.

Résultat Sain

La traduction existe et reflète :
adresse locale interne correcte
correcte globale interne
adresse extérieure correcte
protocole et mappage de port corrects

Si le résultat n'est pas sain

Interprétation :
Aucune entrée de traduction n'existe
Concentrez-vous sur la correspondance NAT, l’ACL, la route-map ou l’allocation de ressources.
La traduction existe mais le trafic échoue toujours
Passez à l'étape de vérification QFP.

Il s'agit de l'une des branches les plus importantes du workflow.

<#root>

```
NAT_R1#
```

show ip nat translations verbose

```
Pro Inside global Inside local Outside local Outside global
icmp 203.0.113.2:3157 192.0.2.2:3157 x.x.x.x:3157 x.x.x.x:3157
  create: 06/19/26 05:36:53, use: 06/19/26 05:36:53, timeout: 00:00:45
  RuleID : X
  Flags: unknown
  ALG Application Type: NA
  WLAN-Flags: unknown
  Mac-Address: 0000.0000.0000 Input-IDB: GigabitEthernet2
  entry-id: 0xe8a48090, use_count:1
  In_pkts: X In_bytes: 44, Out_pkts: X Out_bytes: X
  Output-IDB: GigabitEthernet1
```

- Protocol | icmp | L'entrée de traduction est pour le trafic ICMP : dans les entrées ICMP, la valeur après le signe deux-points représente l'identificateur ICMP, et non un port TCP ou UDP.
- Globale interne |203.0.113.2:3157 | L'adresse source traduite vue sur le réseau externe. 203.0.113.2 est l'adresse NAT publique utilisée pour ce flux.
- Local interne |192.0.2.2:3157 | Adresse source d'origine de l'hôte interne avant traduction.
- Externe local | x.x.x.x:3157 | L'adresse de destination telle qu'elle apparaît sur le réseau interne.
- Externe global | x.x.x.x:3157 | Adresse de destination réelle sur le réseau externe. Ce champ correspond à la valeur locale externe car aucune traduction externe n'est appliquée.
- IDrègle | X | La règle NAT qui a créé cette entrée de traduction.
- Indicatifs | inconnu | Indicateurs NAT internes associés à l'entrée. L'interface de ligne de commande ne décode pas cette valeur dans le résultat affiché.
- Type d'application ALG | NA | Aucune passerelle de couche application n'est associée à cette traduction ICMP.
- Indicateurs WLAN | inconnu | Indicateurs relatifs au WLAN spécifiques à la plate-forme. Ce champ n'est pas pertinent du point de vue opérationnel pour cette entrée.
- Adresse MAC : |0000.0000.0000 | Le champ d'adresse MAC n'est pas renseigné pour cette entrée de traduction.
- Input-IDB | GigabitEthernet2 | Interface d'entrée dans laquelle le paquet d'origine est entré dans le routeur. Cela confirme que le trafic provient de l'intérieur sur GigabitEthernet2.
- ID entrée | 0xe8a48090 | Identificateur interne de l'entrée de traduction NAT en mémoire.
- Utiliser le nombre | Nombre de références internes pour l'entrée de traduction.
- Par paquets | Nombre de paquets comptés dans une direction pour cette traduction.
- En octets | Nombre d'octets comptés dans la même direction que les paquets entrants.
- Paquets sortants | Nombre de paquets comptés dans la direction opposée pour cette traduction.
- Octets sortants | Nombre d'octets comptés dans la même direction que les paquets sortants.
- Output-IDB | GigabitEthernet1 | Interface de sortie utilisée par le trafic traduit. Cela confirme la sortie du paquet traduit par GigabitEthernet1.

Étape 3. Vérification de la programmation de la traduction dans QFP

Cette étape confirme si la traduction visible dans le RP est également programmée dans le chemin matériel de transfert.

<#root>

```
NAT_R1#

show platform hardware qfp active feature nat datapath gateout


Gatekeeper on
<snip>
sip 192.0.2.35 dip x.x.x.x vrf 0 ts 0xcdd07450 idx 10268
sip 192.0.2.67 dip x.x.x.x vrf 0 ts 0xcdd072de idx 44104
sip 198.51.100.12 vrf 0 cnt 225 ts 0x1b393b5 idx 56738

sip 198.51.100.89 dip x.x.x.x vrf 0 ts 0xcdd071b2 idx 59429 <---------------- Affected Host
```

| 0xcdd07450 | Valeur d'horodatage/âge QFP interne au format hexadécimal.
| idx | 10268 | Index interne de la table de portes.
| cnt | 225 | Nombre d'activités/de références internes pour cet objet de porte. Visible sur certains types d'entrées.

| Entrée 1 | sip 192.0.2.35 dip x.x.x.x vrf 0 ts 0xcdd07450 idx 10268 | Entrée de porte spécifique au tuple pour la source 192.0.2.35 vers la destination x.x.x.x dans VRF 0.
| Entrée 2 | sip 192.0.2.67 dip x.x.x.x vrf 0 ts 0xcdd072de idx 44104 | Entrée de porte spécifique au tuple pour la source 192.0.2.67 vers la destination de multidiffusion x.x.x.x dans VRF 0.
| Entrée 3 | sip 198.51.100.12 vrf 0 cnt 225 ts 0x1b393b5 idx 56738 | Entrée de porte orientée source-hôte pour 198.51.100.12 dans VRF 0, avec activité interne/nombre de référence 225.
| Entrée 4 | sip 198.51.100.89 dip x.x.x.x vrf 0 ts 0xcdd071b2 idx 59429 | Entrée de porte spécifique au tuple pour la source 198.51.100.89 vers la destination x.x.x.x dans VRF 0.

Le résultat confirme que la fonction de contrôleur d'accès de chemin de données NAT est activée sur le périphérique. Il montre également que l'adresse source affectée 198.51.100.89 est présente dans la table de sortie NAT QFP sous la forme d'une entrée spécifique à un tuple associée à un flux de destination dans VRF 0.

Cela indique que le trafic provenant de 198.51.100.89 atteint le chemin de création de traduction NAT dans le chemin de données QFP et est suivi en interne par le processus de gatekeeper. Les valeurs ts et idx sont des références QFP internes pour cette entrée de passerelle.

Ce résultat ne confirme pas qu'une traduction NAT complète a été correctement installée pour le flux affecté. Il confirme uniquement la présence de l'état de gatekeeper interne pour ce tuple source/destination.

Pour le comportement intermittent signalé, l'observation pertinente est que 198.51.100.89 est visible dans la passerelle pendant la fenêtre de problème, ce qui aligne le domaine défaillant avec le gatekeeper du chemin de données NAT ou l'étape de traduction-installation, plutôt qu'avec une absence complète de trafic de l'hôte affecté.

Étape 4 : vérification des statistiques du contrôleur d’accès NAT

Une augmentation rapide des échecs de cache indique que les flux non NAT ne sont pas ajoutés au cache. Cette condition entraîne une utilisation élevée du processeur de flux quantique (QFP).

```
<#root>
NAT_R1#

show platform hardware qfp active feature nat datapath gateout activity


Gatekeeper on
def mode Size 8192, Hits 448492109001,

Miss 53295038401

, Aged 149941327 Added 603614728 Active 1899
```

```
<#root>
NAT_R1#

show platform hardware qfp active feature nat datapath gateout activity


Gatekeeper on
def mode Size 8192, Hits 191540578459,

Miss 3196566091

, Aged 1365537 Added 9 Active 7
```

Étape 5 : validation des abandons au niveau QFP

Recherchez les compteurs d'abandon liés à la NAT

<#root>

```
NAT_R1#

show platform hardware qfp active statistics drop



Last clearing of QFP drops statistics : never

-------------------------------------------------------------------------
Global Drop Stats                                       Packets       Octets
-------------------------------------------------------------------------
NatIn2out                                                  1701       174437
NatOut2in                                                  4838       267167

NAT_R1#

show platform hardware qfp active statistics drop



Last clearing of QFP drops statistics : never

-------------------------------------------------------------------------
Global Drop Stats                                      Packets        Octets
-------------------------------------------------------------------------
NatIn2out                                                8039        823998
NatOut2in                                               26427       1461299

NAT_R1#

show platform hardware qfp active statistics drop



Last clearing of QFP drops statistics : never

-------------------------------------------------------------------------
Global Drop Stats                                     Packets         Octets
-------------------------------------------------------------------------
NatIn2out                                               12498        1281045
NatOut2in                                               41211        2278842
```

Au cours du comportement observé, les compteurs d'abandon QFP NatIn2out et NatOut2in ont augmenté de façon continue, indiquant des abandons de paquets en cours à la fois dans les chemins de traduction NAT interne vers externe et externe vers interne.

Étape 6. Validation avec un paquet Capturez les paquets qui sont affectés.

Une capture de paquets dans ce problème fournit une visibilité détaillée sur le flux et le traitement des paquets à travers le périphérique, permettant d'identifier si les paquets sont traduits ou contournés par NAT, et aidant à isoler la cause racine des problèmes liés au contrôleur d'accès NAT. Cela facilite le dépannage ciblé et la validation des modifications de configuration.

<#root>

ip access-list extended TAC

```
permit ip host 198.51.100.89 <destination IP >
permit ip <destination IP > host 198.51.100.89
```

```
debug platform condition ipv4 access-list TAC both
debug platform packet packet 128 fia-trace circular
debug platform packet-trace copy packet both
debug platform condition start
debug platform condition stop
```



Remarque : Ce document ne fournit pas une description détaillée de la capture de paquets. Pour obtenir des informations détaillées sur la capture de paquets, reportez-vous à ce document : Fonction de suivi des paquets Datapath - Capture de paquets

---

Sur la base de l'analyse de capture de paquets, il est observé que le trafic des hôtes affectés est abandonné par le processus NAT. Plus précisément, le paquet capturé ne correspond à aucune entrée de traduction NAT existante ou aux sous-réseaux définis dans les listes de contrôle d'accès (ACL). Cela indique que le paquet n'est pas soumis à la traduction NAT ou autorisé par les ACL configurées, ce qui peut être la cause du problème de connectivité. Une étude plus approfondie peut se concentrer sur la vérification des règles de traduction NAT et des configurations de liste de contrôle d'accès pour garantir que le trafic affecté est correctement géré.

<#root>

```
NAT_R1#
```

show platform packet-trace packet 122 decode

```
Packet: 122 CBUG ID: 650
Summary
Input     : GigabitEthernet1
Output    : GigabitEthernet2
```

```
State    : FWD
Timestamp
Start    : 6725512391055 ns (07/01/2026 16:56:32.593082 UTC)
Stop     : 6725512441820 ns (07/01/2026 16:56:32.593133 UTC)
Path Trace
Feature  : IPV4(Input)
Input           : GigabitEthernet1
Output          : GigabitEthernet2
Source          : 198.51.100.89
Destination     : <remote Host>
Protocol        : 6 (TCP)
SrcPort         : 16130
DstPort         : 1560
<snip>
```

Feature : NAT

```
Direction    : OUT to IN
Action       : FWD
```

FWD-POINT   : GATEKEEPER_BLOCKED

```
VRF          : 2
Feature: IPV4_NAT_INPUT_FIA
Entry         : Input - 0x700140f0
Input         : GigabitEthernet1
Output        : <unknown>
Lapsed time   : 8970 ns
<snip>
Packet Copy In
<snip>
ARPA
Destination MAC       : aaaa.bbbb.cccc
Source MAC            : bbbb.bbbb.aaaa
<snip>
Packet Copy Out
<snip>>
```

Found the issue to be gatekeeper:

```
Feature: NAT
Direction     : IN to OUT
Action        : FWD
```

FWD-POINT   : GATEKEEPER_BLOCKED

Recommandations

Cisco recommande de séparer le trafic NATed et non NATed sur différentes interfaces ou

périphériques pour éviter les problèmes liés à la fonctionnalité NAT Gatekeeper. Cette séparation permet d'éviter un traitement excessif dû à des types de trafic mixtes sur la même interface.

En outre, Cisco recommande la mise à niveau vers une version Cisco qui inclut des améliorations à la fonctionnalité NAT Gatekeeper. Ces améliorations permettent la mise en cache des adresses IP source et de destination et permettent de configurer la taille du cache. La taille du cache peut être ajustée à l'aide de la commande en mode de configuration globale :

```
ip nat settings gatekeeper-size <value>
```

La valeur doit être une puissance de deux, et il est recommandé de commencer par une taille proche du paramètre par défaut. Après avoir ajusté la taille du cache, surveillez les occurrences et les échecs du cache pour garantir des performances optimales et une utilisation optimale des ressources.

L'augmentation de la taille du cache peut réduire le nombre d'échecs de cache et améliorer l'efficacité du traitement NAT, mais elle consomme également de la mémoire supplémentaire sur le processeur de flux quantique (QFP). Il est donc possible de procéder à des ajustements graduels en exerçant une surveillance attentive.

Ces recommandations visent à optimiser les performances du contrôleur d'accès NAT et à réduire les problèmes potentiels causés par des flux de trafic NAT et non NAT mixtes.

Informations connexes

- Dépanner une utilisation QFP élevée due à la configuration par défaut du portier NAT
- Dépannage de l'échec intermittent de traduction de paquets IOS NAT

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.