Dépannage de la traduction d'adresses réseau avec les questions fréquentes

Table des matières

Introduction

Ce document décrit le fonctionnement du processus du routeur de traduction d'adresses de réseau (NAT) et fournit des réponses à certaines questions courantes.

NAT générique

Q. Qu’est-ce que la NAT ?

R. La traduction d’adresses de réseau (NAT) est conçue pour la conservation des adresses IP. Elle active les réseaux IP privés qui utilisent des adresses IP non enregistrées pour se connecter à Internet. La fonction NAT fonctionne sur un routeur, généralement lorsque vous connectez deux réseaux ensemble, et traduit les adresses privées (non uniques au niveau mondial) du réseau interne en adresses légales, avant que les paquets ne soient transférés vers un autre réseau.

Dans le cadre de cette fonction, la traduction d'adresses de réseau (NAT) peut être configurée pour publier une seule adresse pour l'intégralité du réseau au monde extérieur. Cela permet de

masquer efficacement l'ensemble du réseau interne derrière cette adresse, ce qui renforce la sécurité. NAT offre la double fonction de sécurité et de conservation d'adresses et est généralement mise en œuvre dans des environnements d'accès distant.

Q. Comment fonctionne la fonction NAT ?

R.En gros, la fonction NAT permet à un périphérique unique, tel qu'un routeur, d'agir en tant qu'agent entre Internet (ou réseau public) et un réseau local (ou réseau privé), ce qui signifie qu'une seule adresse IP unique est nécessaire pour représenter un groupe entier d'ordinateurs vers n'importe quel élément en dehors de leur réseau.

Q. Comment configurer la fonction NAT ?

R.Afin de configurer la NAT traditionnelle, vous devez créer au moins une interface sur un routeur (NAT externe) et une autre interface sur le routeur (NAT interne) et un ensemble de règles de traduction pour les adresses IP dans les en-têtes de paquet (et les charges utiles si désiré) et elles doivent être configurées. Afin de configurer l'interface virtuelle NAT (NVI), vous avez besoin au moins d'une interface configurée avec NAT activée et le même ensemble de règles que celui mentionné ci-dessus.

Pour plus d'informations, référez-vous au Guide de configuration des services d'adressage IP de Cisco IOS ou à sa section surConfiguration de l'interface virtuelle NAT.

Q. Quelles sont les principales différences entre les mises en oeuvre du logiciel Cisco IOS® et du dispositif de sécurité adaptatif Cisco (ASA) de la fonction NAT ?

R.La fonction NAT basée sur le logiciel Cisco IOS n'est pas fondamentalement différente de la fonction NAT dans Cisco ASA. Les principales différences incluent les différents types de trafic pris en charge dans les implémentations et les exigences de conception. Référez-vous à Exemples de configuration NAT pour plus d'informations sur la configuration de NAT sur les périphériques Cisco ASA (inclut les types de trafic pris en charge).

Q. Sur quel matériel de routage Cisco Cisco IOS NAT est-il disponible ? Comment le matériel peut-il être commandé ?

R.L'outil Cisco Feature Navigator permet aux clients d'identifier une fonctionnalité (NAT) et de trouver sur quelle version et sur quelle version matérielle cette fonctionnalité du logiciel Cisco IOS est disponible. Référez-vous àCisco Feature Navigator afin d'utiliser cet outil.

Q. La NAT intervient-elle avant ou après le routage ?

R. L'ordre dans lequel les transactions sont traitées par la fonction NAT dépend du fait qu'un paquet circule du réseau interne au réseau externe ou du réseau externe au réseau interne. La traduction interne vers externe se produit après le routage, alors que la traduction externe vers interne a lieu avant le routage. Référez-vous à Ordre d'opération NAT pour plus d'informations.

Q. La fonction NAT peut-elle être déployée dans un environnement LAN sans fil public ?

R.Oui. La fonction NAT - Static IP Support (Prise en charge d'adresses IP statiques) prend en charge les utilisateurs possédant des adresses IP statiques et leur permet d'établir une session IP dans un environnement LAN sans fil public.

Q. La fonction NAT effectue-t-elle l’équilibrage de charge TCP pour les serveurs sur le réseau interne ?

R.Oui. Avec la fonction NAT, vous pouvez établir un hôte virtuel sur le réseau interne qui coordonne les équilibres de charge entre les hôtes réels.

Q. Puis-je limiter le nombre de traductions NAT ?

R.Oui. La fonctionnalité Rate-Limiting NAT Translation permet de limiter le nombre maximal d'opérations NAT simultanées sur un même routeur. Cela permet aux utilisateurs de mieux contrôler la manière dont les adresses NAT sont utilisées. La fonction de traduction NAT de limitation de débit peut être utilisée pour limiter les effets des virus, des vers et des attaques par déni de service.

Q. Comment le routage est-il appris ou propagé pour les sous-réseaux IP ou les adresses utilisés par la fonction NAT ?

R. Le routage pour les adresses IP créées par NAT est appris si :

- Le pool d'adresses globales internes est dérivé du sous-réseau d'un routeur du saut suivant.
- L'entrée de route statique est configurée sur le routeur du saut suivant et redistribuée dans le réseau de routage.

Lorsque l'adresse globale interne correspond à l'interface locale, la fonction NAT installe un alias IP et une entrée ARP, auquel cas le routeur **peut proxy-**arp pour ces adresses. Si ce comportement n'est pas souhaité, utilisez **le mot-clé no-**aliaskeyword.

Quand un pool NAT est configuré, l'option **add-route peut être utilisée pour l'injection de routes automatique.**

Q. Combien de sessions NAT simultanées sont prises en charge dans Cisco IOS NAT ?

R.La limite de session NAT est limitée par la quantité de DRAM disponible dans le routeur. Chaque traduction NAT consomme environ 312 octets de DRAM. En conséquence, 10 000 traductions (plus qu'un seul routeur gère habituellement) consomment environ 3 Mo. Par conséquent, le matériel de routage classique dispose de suffisamment de mémoire pour prendre en charge des milliers de traductions NAT. Cependant, il est également recommandé de vérifier les spécifications de la plate-forme.

Q. Quel type de performances de routage peut être attendu avec la fonction NAT de Cisco IOS ?

R.Cisco IOS NAT prend en charge la commutation CEF (Cisco Express Forwarding), la commutation rapide et la commutation de processus. Pour la version 12.4T et les versions ultérieures, le chemin de commutation rapide n'est plus pris en charge. Pour la plate-forme Cat6k,

l'ordre de commutation est Netflow (chemin de commutation HW), CEF, chemin du processus.

Les performances dépendent de plusieurs facteurs :

- le type d'application et son type de trafic,
- si les adresses IP sont intégrées,
- l'échange et l'inspection de plusieurs messages,
- le port source requis,
- le nombre de traductions,
- Autres applications qui s'exécutent à ce moment-là
- le type de matériel et de processeur.

Q. La fonction NAT de Cisco IOS peut-elle être appliquée aux sous-interfaces ?

R.Oui. Les traductions NAT source et/ou de destination peuvent être appliquées à n'importe quelle interface ou sous-interface ayant une adresse IP (y compris les interfaces de numérotation). NAT ne peut pas être configurée avec une interface virtuelle sans fil. L'interface virtuelle sans fil n'existe pas au moment de l'écriture dans la mémoire NVRAM. Ainsi, après le redémarrage, le routeur perd la configuration NAT sur l'interface virtuelle sans fil.

Q. La fonction NAT de Cisco IOS peut-elle être utilisée avec le protocole HSRP (Hot Standby Router Protocol) pour fournir des liaisons redondantes à un FAI ?

R.Oui. NAT fournit la redondance HSRP. Cependant, elle est différente de SNAT (Stateful NAT, NAT avec état). NAT avec le protocole HSRP est un système sans état. La session en cours n'est pas conservée en cas de défaillance. Au cours de la configuration de NAT statique (quand un paquet ne correspond à aucune configuration de règle STATIC), le paquet est envoyé sans traduction.

Q. La fonction NAT de Cisco IOS prend-elle en charge les traductions entrantes sur une interface Frame Relay ? Les traductions sortantes sont-elles prises en charge du côté Ethernet ?

R.Oui. L'encapsulation n'entre pas en compte pour NAT. NAT peut être effectuée lorsqu'une adresse IP est présente sur une interface et que l'interface est interne ou externe de NAT. Une partie intérieure et une partie extérieure doivent exister pour que NAT fonctionne. Si vous utilisez NVI, NAT doit être activée au moins pour une interface. Reportez-vous à la question précédente, Comment configurer la fonction NAT ? pour plus de détails.

Q. Un seul routeur compatible NAT peut-il permettre à certains utilisateurs d’utiliser la fonction NAT et à d’autres utilisateurs de la même interface Ethernet de continuer à utiliser leurs propres adresses IP ?

R.Oui. Pour ce faire, vous pouvez utiliser une liste de contrôle d’accès décrivant l’ensemble des hôtes ou des réseaux qui nécessitent la fonction NAT. Toutes les sessions du même hôte peuvent être traduites ou transiter par le routeur et ne pas être traduites.

Les listes d’accès, les listes d’accès étendues et les cartes de routage peuvent être utilisées pour définir les règles de traduction des périphériques IP. L'adresse réseau et le masque de sous-

réseau approprié doivent toujours être spécifiés. Le mot-clé any ne doit pas être utilisé à la place de l'adresse réseau ou du masque de sous-réseau. Avec la configuration NAT statique, lorsque le paquet ne correspond à aucune configuration de règle STATIC, le paquet peut être envoyé sans traduction.

Q. Lorsque la fonction PAT (surcharge) est configurée, quel est le nombre maximal de traductions pouvant être créées par adresse IP globale interne ?

A.PAT (surcharge) divise les ports disponibles par adresse IP globale en trois plages : 0-511, 512-1023 et 1024-65535. PAT assigne un seul port source à chaque session UDP ou TCP. Il tente d'assigner la même valeur de port de la requête d'origine, mais si le port source d'origine a déjà été utilisé, il commence l'analyse à partir du début de la plage de ports particulière pour trouver le premier port disponible et l'assigne à la conversation.

Q. Comment fonctionne la PAT ?

A.PAT fonctionne avec une adresse IP globale ou plusieurs adresses.

PAT avec une table d'adresses IP

Condition	Description
1	NAT/PAT inspecte le trafic et l'apparie à la règle de traduction.
2	La règle correspond à la configuration PAT.
3	Si la PAT connaît le type de trafic et si ce type de trafic a « un ensemble de ports spécifiques o ports qu'elle négocie » qu'elle peut utiliser, elle les met de côté et ne les alloue pas en tant qu'identificateurs uniques.
4	Si une session sans exigences de port spécifiques tente de se connecter avec l'extérieur, PAT traduit l'adresse source IP et vérifie la disponibilité du port source d'origine (433, par exemple). la **remarque**.
5	Si le port source demandé est disponible, PAT assigne le port source et la session continue.
6	Si le port source demandé n'est pas disponible, la fonction PAT commence la recherche à parti début du groupe concerné (à partir de 1 pour les applications TCP ou UDP et de 0 pour ICMP).
7	Si un port est disponible, il est assigné et la session continue.
8	Si aucun port n'est disponible, le paquet est abandonné.

> **Remarque** : pour les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol), les plages sont les suivantes : 1-511, 512-1023, 1024-65535. Pour le protocole ICMP (Internet Control Message Protocol), le premier groupe commence à 0.

PAT avec plusieurs adresses IP

Condition	Description
1-7	Les sept premières conditions sont identiques à la configuration avec une seule adresse IP.
8	Si aucun port n'est disponible dans le groupe approprié de la première adresse IP, NAT passe l'adresse IP suivante dans le pool et essaie d'allouer le port source d'origine demandé.
9	Si le port source demandé est disponible, NAT attribue le port source et la session se poursuit.
10	Si le port source demandé n'est pas disponible, la fonction NAT commence la recherche à parti début du groupe concerné (à partir de 1 pour les applications TCP ou UDP et de 0 pour ICMP).
11	Si un port est disponible, il est attribué et la session se poursuit.
12	Si aucun port n'est disponible, le paquet est abandonné, sauf si une autre adresse IP est dispo dans le pool.

Q. Que sont les pools d’adresses IP NAT ?

R.Les pools d'adresses IP NAT sont une plage d'adresses IP qui sont allouées pour la traduction NAT selon les besoins. Pour définir un pool, la commande de configuration est utilisée :

```
ip nat pool <name> <start-ip> <end-ip> {netmask <netmask> | prefix-length <prefix-length>} [type {rotary}]
```

Exemple 1

L’exemple suivant traduit entre des hôtes internes adressés à partir du réseau 192.168.1.0 ou 192.168.2.0 vers le réseau 10.69.233.208/28 globalement unique :

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Exemple 2

Dans l'exemple suivant, l'objectif est de définir une adresse virtuelle, à laquelle des connexions sont distribuées parmi un ensemble d'hôtes réels. Le pool définit les adresses des hôtes réels. La liste d'accès définit l'adresse virtuelle. Si une traduction n'existe pas encore, les paquets TCP de l'interface série 0 (l'interface externe) dont la destination correspond à la liste d'accès sont traduits vers une adresse du pool.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
 ip address 192.168.15.129 255.255.255.240
 ip nat outside
!
interface ethernet 0
 ip address 192.168.15.17 255.255.255.240
 ip nat inside
!
access-list 2 permit 192.168.15.1
```

Q. Quel est le nombre maximal de pools IP NAT configurables (ip nat pool « name ») ?

R. Dans la pratique, le nombre maximal de pools d’adresses IP configurables est limité par la quantité de mémoire DRAM disponible sur le routeur concerné. (Cisco recommande de configurer une taille de pool de 255.) Chaque pool ne doit pas comporter plus de 16 bits. Dans la version 12.4(11)T et ultérieure, Cisco IOS a introduit CCE (Common Classification Engine). Ce module ne

permet pas à NAT d'avoir plus de 255 pools.

Q. Quel est l'avantage d'une carte de routage par rapport à une liste de contrôle d'accès sur un pool NAT ?

R.Une route-map protège les utilisateurs externes indésirables pour atteindre les utilisateurs/serveurs internes. Il permet également de mapper une adresse IP interne unique à différentes adresses globales internes en fonction de la règle. Référez-vous à Prise en charge NAT pour plusieurs pools à l'aide de mappages de route pour plus d'informations.

Q. Qu'est-ce que le « chevauchement » d'adresses IP dans le contexte de la NAT ?

Un chevauchement d'adresses IP fait référence à une situation où deux emplacements qui veulent s'interconnecter utilisent le même schéma d'adresses IP. Ce n'est pas inhabituel ; cela arrive souvent lorsque des entreprises fusionnent ou sont rachetées. Sans assistance spéciale, les deux emplacements ne peuvent pas se connecter et établir des sessions. L'adresse IP qui se chevauche peut être une adresse publique attribuée à une autre société, une adresse privée attribuée à une autre société ou peut provenir de la plage d'adresses privées définie dans la RFC 1918.

Les adresses IP privées ne sont pas routables et nécessitent des traductions NAT pour permettre les connexions au monde extérieur. La solution implique l'interception des réponses de requête de nom DNS (Domain Name System) de l'extérieur vers l'intérieur, une configuration de traduction pour l'adresse externe, et la réponse DNS doit être corrigée avant d'être transmise à l'hôte interne. Un serveur DNS doit être impliqué des deux côtés du périphérique NAT pour résoudre les utilisateurs qui veulent avoir une connexion entre les deux réseaux.

La fonction NAT est capable d'inspecter et d'effectuer la traduction d'adresses sur le contenu des enregistrements DNSAandPTR, comme indiqué dans Utilisation de la fonction NAT dans les réseaux en chevauchement.

Q. Que sont les traductions NAT statiques ?

A. Les traductions NAT statiques ont un mappage un-à-un entre les adresses locales et globales. Les utilisateurs peuvent également configurer des traductions d'adresses statiques au niveau du port et utiliser le reste de l'adresse IP pour d'autres traductions. Cela se produit généralement lorsque vous effectuez la traduction d'adresses de port (PAT).

L'exemple suivant montre comment configurer route-map pour permettre la traduction externe-interne pour la NAT statique :

```
ip nat inside source static 10.1.1.1 10.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.1 0.0.0.127
route-map R1 permit 10
 match ip address ACL-A
```

Q. Que signifie le terme *NATOverloading* ; est-ce PAT ?

R.Oui. La surcharge NAT est PAT, qui implique l'utilisation d'un pool avec une plage d'une ou

plusieurs adresses ou l'utilisation d'une adresse IP d'interface en combinaison avec le port. En cas de surcharge, vous créez une traduction entièrement étendue. Il s'agit d'une entrée de table de traduction qui contient des informations d'adresse IP et de port source/de destination, communément appelées PAT ou surcharge.

PAT (ou surcharge) est une fonctionnalité de la fonction NAT de Cisco IOS qui est utilisée pour *traduire les* adresses privées *internes* (locales internes) en une ou *plusieurs* adresses IP *externes* (globales internes, généralement enregistrées). Des numéros de port source uniques pour chaque traduction sont utilisés pour distinguer les conversations.

Q. Que sont les traductions NAT dynamiques ?

A. Dans les traductions NAT dynamiques, les utilisateurs peuvent établir un mappage dynamique entre les adresses locales et globales. Le mappage dynamique est effectué lorsque vous définissez les adresses locales à traduire et le pool d'adresses ou l'adresse IP d'interface à partir duquel allouer des adresses globales et lorsque vous associez les deux.

Q. Qu'est-ce que ALG ?

A.ALG est une passerelle de couche application (ALG). NAT exécute le service de traduction sur tout trafic TCP/UDP (Transmission Control Protocol/User Datagram Protocol) qui ne diffusent pas les adresses IP source/de destination dans le flux de données de l'application.

Ces protocoles incluent FTP, HTTP, SKINNY, H232, DNS, RAS, SIP, TFTP, telnet, archie, finger, NTP, NFS, rlogin, rsh et rcp. Les protocoles spécifiques qui incluent les informations d'adresse IP dans la charge utile exigent la prise en charge de la passerelle au niveau de l'application (ALG).

Référez-vous àUtilisation des passerelles de niveau application avec NAT pour plus d'informations.

Q. Est-il possible de créer une configuration avec des traductions NAT statiques et dynamiques ?

R.Oui. Cependant, la même adresse IP ne peut pas être utilisée pour la configuration statique NAT et dans le pool pour la configuration dynamique NAT. Toutes les adresses IP publiques doivent être uniques. Notez que les adresses globales utilisées dans les traductions statiques ne sont pas automatiquement exclues avec les pools dynamiques qui contiennent ces mêmes adresses globales. Des pools dynamiques doivent être créés pour exclure les adresses assignées par des entrées statiques. Pour plus d'informations, référez-vous àConfiguration simultanée de la NAT statique et dynamique.

Q. Lorsqu'une commande traceroute est exécutée via un routeur NAT, la commande traceroute doit-elle afficher l'adresse NAT-globale ou doit-elle laisser passer l'adresse NAT-locale ?

A.La commande traceroute doit toujours renvoyer l'adresse globale.

Q. Comment la PAT alloue-t-elle le port ?

A.NAT introduit des fonctionnalités de port supplémentaires : plage complète et carte de port.

- La fonctionnalité de plage complète permet à NAT d'utiliser tous les ports indépendamment de sa plage de ports par défaut.
- La fonctionnalité de mappage de ports permet à NAT de réserver une plage de ports définie par l'utilisateur pour une application spécifique.

Référez-vous à Plages de ports source définies par l'utilisateur pour PATpour plus d'informations.

Àpartir de la version 12.4(20)T2, NAT introduit la randomisation des ports pour les ports L3/L4 et symétriques.

- La randomisation des ports permet à NAT de sélectionner au hasard un port global pour la demande de port source.
- Le port symétrique permet à la NAT de prendre en *charge* les *terminaux indépendants*.

Q. Quelle est la différence entre la fragmentation IP et la segmentation TCP ?

A.La fragmentation IP se produit au niveau de la couche 3 (IP) ; la segmentation TCP se produit au niveau de la couche 4 (TCP). La fragmentation IP a lieu lorsque des paquets plus volumineux que l'unité de transmission maximale (MTU) d'une interface sont envoyés hors de cette interface. Ces paquets doivent être fragmentés ou éliminés lorsqu'ils sont envoyés à l'interface. Si la Don't Fragment (DF) n'est pas défini dans l'en-tête IP du paquet, le paquet peut être fragmenté. Si le bit DF est défini dans l'en-tête IP du paquet, le paquet est abandonné et un message d'erreur ICMP indique la valeur MTU du tronçon suivant qui est renvoyée à l'expéditeur. Tous les fragments d'un paquet IP portent la même identification dans l'en-tête IP, qui permet au destinataire final de rassembler les fragments dans le paquet IP d'origine. Référez-vous àRésoudre les problèmes de fragmentation IP, MTU, MSS et PMTUD avec GRE et IPsec pour plus d'informations.

La segmentation TCP se produit lorsqu'une application d'une station d'extrémité envoie des données. Les données d'application sont divisées en ce que le TCP considère comme étant des morceaux de taille optimale à envoyer. Cette unité de données transmises du protocole TCP au protocole IP s'appelle un segment. Les segments TCP sont envoyés dans des datagrammes IP. Ces datagrammes IP peuvent alors devenir des fragments IP lorsqu'ils traversent le réseau et rencontrent des liaisons MTU trop petites pour pouvoir les traverser.

Le protocole TCP peut d'abord segmenter ces données en segments TCP (en fonction de la valeur MSS du protocole TCP), puis ajouter l'en-tête TCP et transmettre ce segment TCP au protocole IP. Ensuite, IP peut ajouter un en-tête IP pour envoyer le paquet à l'hôte d'extrémité distant. Si le paquet IP avec le segment TCP est plus grand que le MTU IP sur une interface sortante sur le chemin entre les hôtes TCP, alors IP peut fragmenter le paquet IP/TCP afin de s'adapter. Ces fragments de paquets IP peuvent être réassemblés sur l'hôte distant par la couche IP et le segment TCP complet (qui a été envoyé à l'origine) peut être transmis à la couche TCP. La couche TCP ne voit pas que le protocole IP avait fragmenté le paquet lors du transfert.

NAT prend en charge les fragments IP, mais pas les segments TCP.

Q. La NAT prend-elle en charge la fragmentation IP et la segmentation TCP dans le désordre ?

A.NAT ne prend en charge que les fragments IP désordonnés car **ofip virtual-reassembly**.

Q. Comment déboguer la fragmentation IP et la segmentation TCP ?

A.NAT utilise la même interface de ligne de commande de débogage pour la fragmentation IP et la segmentation TCP : **debug ip nat frag**.

Q. Existe-t-il une MIB NAT prise en charge ?

R.Non. NAT MIB n'est pas pris en charge et CISCO-IETF-NAT-MIB ne l'est pas non plus.

Q. Qu'*est*-ce que le *délai d'attente TCP*, et comment le relie-t-il au minuteur TCP NAT ?

R.Si la connexion en trois étapes n'est pas terminée et que la fonction NAT détecte un paquet TCP, la fonction NAT peut démarrer un minuteur de 60 secondes. Lorsque la connexion en trois temps est terminée, NAT utilise une minuterie de 24 heures pour une entrée NAT par défaut. Si un hôte final envoie un paquet RESET, NAT change la minuterie par défaut de 24 heures à 60 secondes. En cas de paquet FIN, NAT change la minuterie par défaut de 24 heures à 60 secondes lorsqu'il reçoit les paquets FIN et FIN-ACK.

Q. Puis-je modifier la durée nécessaire à une traduction NAT pour qu'elle expire dans la table de traduction NAT ?

R.Oui. Vous pouvez modifier les valeurs de délai d'attente NAT pour toutes les entrées ou pour différents types de traductions NAT (tels que udp-timeout, dns-timeout, tcp-timeout, finrst-timeout, icmp-timeout, pptp-timeout, syn-timeout, port-timeout et arp-ping-timeout).

Q. Comment puis-je arrêter le protocole LDAP (Lightweight Directory Access Protocol) lorsqu'il joint des octets supplémentaires à chaque paquet de réponse LDAP ?

R.Le LDAP est configuré pour ajouter les octets supplémentaires (résultats de la recherche LDAP) pendant qu'il traite les messages de type Search-Res-Entry. Le protocole LDAP joint 10 octets de résultats de la recherche à chaque paquet de réponse LDAP. Si ces 10 octets de données supplémentaires génèrent le paquet et dépassent l'unité de transmission maximale (MTU) dans un réseau, le paquet est abandonné. Dans ce cas, Cisco recommande que vous désactiviez ce comportement LDAP avec la commande **CLIno ip nat service append-ldap-search-**rescommand afin que les paquets soient envoyés et reçus.

Q. Quelle est la recommandation de route pour l'adresse IP globale interne/locale externe sur la boîte NAT ?

R.Une route doit être spécifiée dans la zone NAT configurée pour l'adresse IP globale interne pour les fonctionnalités telles que NAT-NVI. De même, une route doit également être spécifiée dans la zone NAT pour l'adresse IP locale externe. Dans ce cas, tout paquet provenant d'une direction d'entrée en sortie avec la règle statique externe nécessite ce type de route. Dans de tels scénarios, bien qu'il fournisse la route pour IG/OL, l'adresse IP du tronçon suivant doit également être configurée. Si la configuration du tronçon suivant est introuvable, cela est considéré comme une erreur de configuration et entraîne un comportement non défini.

NAT-NVI est présente dans le chemin d'accès de la fonctionnalité de sortie uniquement. Si vous avez connecté directement le sous-réseau avec NAT-NVI ou la règle de traduction NAT externe configurée dans la zone, vous devez alors fournir une adresse IP de saut suivant factice ainsi

qu'un ARP associé pour le saut suivant. Cela est nécessaire pour que l'infrastructure sous-jacente remette le paquet à NAT pour la traduction.

Q. La fonction NAT de Cisco IOS prend-elle en charge les listes de contrôle d'accès avec un mot clé *log* ?

R.Lorsque vous configurez la NAT de Cisco IOS pour la traduction NAT dynamique, une liste de contrôle d'accès est utilisée pour identifier les paquets qui peuvent être traduits. L'architecture NAT actuelle ne prend pas en charge les ACL avec un mot clé **log**.

Voix-NAT

Q. La NAT prend-elle en charge le protocole Skinny Client Control Protocol (SCCP) v17 livré avec Cisco Unified Communications Manager (CUCM) V7 ?

A.CUCM 7 et toutes les charges de téléphone par défaut de CUCM 7 prennent en charge SCCPv17. La version du SCCP utilisée est déterminée par la version commune la plus élevée utilisée entre CUCM et le téléphone lorsque le téléphone est enregistré.

NAT ne prend pas encore en charge SCCP v17. Jusqu'à ce que la prise en charge NAT de SCCP v17 soit implémentée, le microprogramme doit être rétrogradé à la version 8-3-5 ou inférieure afin que SCCP v16 soit négocié. CUCM6 ne peut pas rencontrer le problème NAT avec une charge de téléphone tant qu'il utilise SCCP v16. Le logiciel Cisco IOS ne prend actuellement pas en charge SCCP version 17.

Q. Quelles versions de chargement CUCM /SCCP/firmware sont prises en charge par la fonction NAT ?

A.NAT prend en charge CUCM version 6.x et versions antérieures. Ces versions CUCM sont publiées avec le microprogramme de téléphone 8.3.x (ou version antérieure) par défaut qui prend en charge SCCP v15 (ou version antérieure).

NAT ne prend pas en charge les versions 7.x ou ultérieures de CUCM. Ces versions CUCM sont publiées avec le microprogramme de téléphone 8.4.x par défaut qui prend en charge SCCP v17 (ou version ultérieure).

Si CUCM 7.x ou version ultérieure est utilisé, un microprogramme plus ancien doit être installé sur le serveur TFTP CUCM de sorte que les téléphones utilisent un microprogramme avec SCCP v15 ou version antérieure afin d'être pris en charge par NAT.

Q. En quoi consiste l'amélioration de l'allocation des ports PAT pour RTP et RTCP ?

R. L'amélioration de l'allocation des ports PAT pour RTP et RTCP garantit que pour les appels vocaux SIP, H.323 et Skinny. Les numéros de port utilisés pour les flux RTP sont des numéros de port pairs, et les flux RTCP sont les numéros de port impairs suivants. Le numéro de port est traduit en un numéro compris dans la plage spécifiée et conforme à la norme RFC-1889. Un appel avec un numéro de port compris dans la plage peut entraîner une traduction PAT vers un autre numéro de port compris dans cette plage. De même, une traduction PAT pour un numéro de port

en dehors de cette plage ne peut pas aboutir à une traduction vers un numéro dans la plage donnée.

Q. Qu'est-ce que le protocole SIP (Session Initiation Protocol) et les paquets SIP peuvent-ils être routés avec NAT ?

R.Le protocole SIP (Session Initiation Protocol) est un protocole de contrôle de couche application basé sur ASCII qui peut être utilisé pour établir, maintenir et terminer des appels entre deux points d'extrémité ou plus. Le protocole SIP est une alternative développée par l'Internet Engineering Task Force (IETF) pour les conférences multimédia sur IP. La mise en œuvre de Cisco SIP permet aux plates-formes Cisco prises en charge de signaler la configuration d'appels vocaux et multimédia sur des réseaux IP. Les paquets SIP peuvent être traduits par NAT.

Q. Quelle est la prise en charge de la traversée NAT hébergée pour le contrôleur de frontière de session (SBC) ?

R.La fonctionnalité de traversée NAT hébergée Cisco IOS pour SBC permet à un routeur Cisco IOS NAT SIP Application-Level Gateway (ALG) d'agir en tant que SBC sur une passerelle IP à IP multiservice Cisco, ce qui permet d'assurer une livraison fluide des services de voix sur IP (VoIP).

Référez-vous àConfiguration de la traversée NAT hébergée de Cisco IOS pour le contrôleur de frontière de session pour plus d'informations.

Q. Combien d'appels SIP, Skinny et H323 un routeur peut-il traiter avec la mémoire et le processeur avec la fonction NAT ?

R. Le nombre d'appels traités par un routeur NAT dépend de la quantité de mémoire disponible sur le boîtier et de la puissance de traitement du processeur.

Q. Un routeur NAT prend-il en charge la segmentation TCP des paquets Skinny et H323 ?

R. Cisco IOS-NAT prend en charge la segmentation TCP pour H323 et la segmentation TCP pour SKINNY.

Q. Y a-t-il des avertissements à prendre en compte lorsque vous utilisez une configuration de surcharge NAT dans un déploiement vocal ?

R.Oui. Lorsque vous êtes en présence de configurations de surcharge NAT et d'un déploiement vocal, le message d'enregistrement doit passer par NAT et une association externe-interne doit être créée pour pouvoir accéder à ce périphérique interne. Le périphérique interne envoie cet enregistrement de manière périodique et la NAT met à jour cette association/goupille à partir des informations comme dans le message de signalisation.

Q. Existe-t-il des problèmes connus provoqués par l'utilisation de la commande lear ip nat trans * ou de la commande lear ip nat trans forced dans un déploiement vocal ?

R. Dans les déploiements vocaux, lorsque vous émettez la commande **aclear ip nat trans *** ou la

commande **aclear ip nat trans** forced et que vous avez la NAT dynamique, vous effacez le trou de broche/association et devez attendre le prochain cycle d'enregistrement du périphérique interne pour l'établir à nouveau. Cisco recommande de ne pas utiliser ces commandes clear dans les déploiements vocaux.

Q. La fonction NAT prend-elle en charge la solution vocale colocalisée ?

R.Non. La solution hébergée conjointement n'est pas prise en charge pour le moment. Le déploiement suivant avec NAT (sur le même boîtier) est considéré comme une solution colocalisée : CME/DSP-Farm/SCCP/H323.

Q. NVI prend-il en charge Skinny ALG, H323 ALG et TCP SIP ALG ?

R.Non. Notez que le protocole UDP SIP ALG (utilisé par la plupart des déploiements) n'est pas affecté.

NAT avec VRF/MPLS

Q. Un routeur NAT peut-il jamais se prendre en charge dans le même espace d'adressage dans un VRF et dans un espace d'adressage global ? Actuellement, je reçois cet avertissement :*"% similar static entry (10.1.1.1 —> 10.2.2.2) existing already"* when I try to configure the this:

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED
```

R. La fonction NAT héritée prend en charge la configuration d'adresses chevauchantes sur différents VRF. Vous devez configurer le chevauchement à la règle avec **l'option match-in-**vrf et définir **upip nat inside/**outside dans le même VRF pour le trafic sur ce VRF spécifique. La prise en charge du chevauchement n'inclut pas la table de routage globale.

Vous devez ajouter **le mot-clé match-in-**vrf pour les entrées NAT statiques VRF qui se chevauchent pour différents VRF. Cependant, il n'est pas possible de superposer des adresses globales et NAT VRF.

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

Q. La fonction NAT héritée prend-elle en charge VRF-Lite (la route entre un VRF et un autre VRF) ?

R.Non. Vous devez utiliser NVI pour NAT entre différents VRF. Vous pouvez utiliser la NAT héritée pour effectuer la NAT de VRF à globale ou la NAT au sein du même VRF.

NAT-NVI

Q. Qu'est-ce que NAT NVI ?

A.NVI est l'acronyme de NAT Virtual Interface. Elle permet à NAT d'effectuer la traduction entre deux VRF. Cette solution doit être utilisée à la place de la traduction d'adresses réseau sur un bâton.

Q. L’interface NAT NVI doit-elle être utilisée pour effectuer le routage entre une interface globale et une interface dans un VRF ?

R.Cisco vous recommande d'utiliser la NAT héritée pour la VRF vers la NAT globale (ip nat inside/out) et entre les interfaces dans le même VRF. La NVI est utilisée pour NAT entre différents VRF.

Q. La segmentation TCP pour NAT-NVI est-elle prise en charge ?

R.Il n'y a pas de prise en charge de la segmentation TCP pour NAT-NVI.

Q. NVI prend-il en charge Skinny ALG, H323 ALG et TCP SIP ALG ?

R.Non. Notez que le protocole UDP SIP ALG (utilisé par la plupart des déploiements) n'est pas affecté.

Q. La segmentation TCP est-elle prise en charge avec SNAT ?

R.SNAT ne prend pas en charge les ALG TCP (tels que SIP, SKINNY, H323 ou DNS). Par conséquent, la segmentation TCP n'est pas prise en charge. Cependant, UDP SIP et DNS sont pris en charge.

NAT par états (SNAT)

Q. Qu’est-ce que la NAT avec état (SNAT) ?

A.SNAT permet à deux ou plusieurs traducteurs d’adresses réseau de fonctionner comme un groupe de traduction. Un membre du groupe de traduction gère le trafic qui nécessite la traduction des informations d'adresse IP. De plus, il informe le traducteur de secours de la présence de flux actifs au fur et à mesure qu'ils se produisent. Le traducteur de secours peut alors utiliser l'information du traducteur actif pour préparer des entrées de table de traduction en double. Par conséquent, si le traducteur actif est gêné par une défaillance critique, le trafic peut rapidement être envoyé vers le traducteur de secours. Le flux de trafic continue puisque les mêmes traductions d'adresses de réseau sont utilisées et que l'état de ces traductions a été précédemment défini.

Q. La segmentation TCP est-elle prise en charge avec SNAT ?

R.SNAT ne prend pas en charge les ALG TCP (tels que SIP, SKINNY, H323 ou DNS). Par conséquent, la segmentation TCP n'est pas prise en charge. Cependant, UDP SIP et DNS sont pris en charge.

Q. La fonction SNAT est-elle prise en charge pour le routage asymétrique ?

A. Le routage asymétrique prend en charge NAT lorsqu'il active as-queuing . Par défaut, l'option « as-queueing » est activée. Toutefois, à partir de la version 12.4(24)T, as-queuing n'est plus pris en charge. Les clients doivent s'assurer que les paquets sont routés correctement et qu'un retard approprié est ajouté pour que le routage asymétrique fonctionne correctement.

NAT-PT (v6 à v4)

Q. Qu'est-ce que NAT-PT ?

A.NAT-PT est une traduction de v4 à v6 pour NAT. La traduction de protocole (NAT-PT) est un mécanisme de traduction IPv6-IPv4, tel que défini dans les documents RFC 2765 et RFC 2766, et permet aux périphériques IPv6 uniquement de communiquer avec des périphériques IPv4 uniquement et vice versa.

Q. NAT-PT est-il pris en charge dans le chemin CEF (Cisco Express Forwarding) ?

A.NAT-PT n'est pas pris en charge dans le chemin CEF.

Q. Quels ALG sont pris en charge dans NAT-PT ?

A.NAT-PT prend en charge TFTP/FTP et DNS. NAT-PT ne prend en charge ni la voix ni SNAT.

Q. Le routeur ASR 1004 prend-il en charge NAT-PT ?

R.Les routeurs à services d'agrégation (ASR) utilisent NAT64.

Cisco 7600/6k dépendant de la plate-forme

Q. La fonction NAT avec état (SNAT) est-elle disponible sur le Catalyst 6500 sur le train SX ?

R.SNAT n'est pas disponible sur Catalyst 6500 sur la ligne SX.

Q. La fonction NAT compatible VRF est-elle prise en charge dans le matériel sur le 6000 ?

La fonction NAT compatible VRF n'est pas prise en charge dans le matériel sur cette plate-forme.

Q. Les modèles 7600 et Cat6000 prennent-ils en charge la fonction NAT compatible VRF ?

R.Sur la plate-forme 65xx/76xx, la fonction NAT compatible VRF n'est pas prise en charge et les CLI sont bloquées.

> **Remarque** : vous pouvez implémenter une conception si vous utilisez un FWSM qui s'exécute en mode transparent de contexte virtuel.

Cisco 850 et plate-forme compatible

Q. Le Cisco 850 prend-il en charge Skinny NAT ALG dans la version 12.4T ?

R.Non. Il n'existe aucune prise en charge pour l'ALG NAT Skinny dans la version 12.4T de la série 850.

Déploiement de NAT

Q. Comment mettre en oeuvre la fonction NAT ?

A.NAT permet aux interréseaux IP privés qui utilisent des adresses IP non enregistrées de se connecter à Internet. NAT traduit l'adresse privée (RFC1918) dans le réseau interne en adresses routables légales avant que les paquets ne soient transférés vers un autre réseau.

Q. Comment puis-je mettre en oeuvre NAT avec la voix ?

R.La prise en charge NAT pour la fonctionnalité vocale permet de retraduire les messages intégrés SIP qui passent par un routeur configuré avec la traduction d'adresses de réseau (NAT) en paquet. Une passerelle de couche applicative (ALG) est utilisée avec NAT pour traduire les paquets de voix.

Q. Comment puis-je intégrer la NAT avec les VPN MPLS ?

R. L'intégration NAT avec les VPN MPLS permet à plusieurs VPN MPLS d'être configurés sur un seul périphérique pour fonctionner ensemble. NAT peut distinguer le VPN MPLS dont il reçoit le trafic IP même si tous les VPN MPLS utilisent le même système d'adressage IP. Cette amélioration permet à plusieurs clients VPN MPLS de partager des services tout en s'assurant que chaque VPN MPLS est complètement séparé de l'autre.

Q. Le mappage statique NAT prend-il en charge HSRP pour une haute disponibilité ?

R.Lorsqu'une requête ARP (Address Resolution Protocol) est déclenchée pour une adresse configurée avec le mappage statique NAT (Network Address Translation) et appartenant au routeur, NAT répond avec l'adresse MAC BIA sur l'interface vers laquelle l'ARP pointe. Deux routeurs agissent en tant que HSRP actif et de secours. Leurs interfaces internes NAT doivent être activées et configurées pour appartenir à un groupe.

Q. Comment puis-je mettre en oeuvre NAT NVI ?

R.La fonctionnalité NAT virtual interface (NVI) supprime la nécessité de configurer une interface comme NAT interne ou NAT externe.

Q. Comment puis-je mettre en oeuvre l'équilibrage de charge avec NAT ?

R. Il existe deux types d'équilibrage de charge qui peuvent être effectués avec la NAT : vous

pouvez équilibrer la charge en entrée vers un ensemble de serveurs pour distribuer la charge sur les serveurs et vous pouvez équilibrer la charge de votre trafic utilisateur vers Internet sur deux FAI ou plus.

Pour plus d'informations sur l'équilibrage de charge sortant, référez-vous à Équilibrage de charge NAT Cisco IOS pour deux connexions FAI.

Q. Comment mettre en oeuvre la fonction NAT avec IPSec ?

R. Il existe un soutien pour IP Security (IPSec) Encapsulating Security Payload (ESP) through NAT et la transparence NAT IPSec.

La fonctionnalité IPSec ESP through NAT permet de prendre en charge plusieurs tunnels ou connexions ESP IPSec simultanés à l'aide d'un périphérique NAT de Cisco IOS configuré en mode de surcharge ou de traduction d'adresse de port (PAT). La fonction de transparence NAT IPSec prend en charge le trafic IPSec qui traverse les points NAT ou PAT du réseau lorsqu'il résout de nombreuses incompatibilités connues entre NAT et IPSec.

Q. Comment puis-je mettre en oeuvre NAT-PT ?

A.NAT-PT (Network Address Translation—Protocol Translation) est un mécanisme de traduction IPv6-IPv4, tel que défini dans les documents RFC 2765 et RFC 2766, qui permet aux périphériques IPv6 uniquement de communiquer avec des périphériques IPv4 uniquement et vice versa.

Q. Comment puis-je mettre en oeuvre la NAT de multidiffusion ?

R.Il est possible d'effectuer une NAT sur l'adresse IP source pour un flux de multidiffusion. Une route-map ne peut pas être utilisée lorsqu'une NAT dynamique pour la multidiffusion est effectuée, seule une liste d'accès est prise en charge pour cela.

Pour plus d'informations, référez-vous àComment fonctionne la NAT multidiffusion sur les routeurs Cisco. Le groupe de multidiffusion de destination utilise NAT avec une solution de réflexion de service multidiffusion.

Q. Comment mettre en oeuvre la NAT avec état (SNAT) ?

A.SNAT active un service continu pour les sessions NAT mappées dynamiquement. Les sessions définies statiquement tirent profit de la redondance sans devoir recourir à SNAT. Faute de SNAT, les sessions qui utilisent les mappages NAT dynamiques seraient interrompues en cas de panne critique et devraient être rétablies. Seule la configuration SNAT minimale est prise en charge. Les déploiements futurs ne doivent être effectués qu'après avoir consulté votre équipe de compte Cisco afin de valider la conception par rapport aux restrictions actuelles.

La fonction SNAT est recommandée pour les scénarios suivants :

- Le mode principal/de sauvegarde n'est pas recommandé car certaines fonctionnalités sont absentes par rapport à HSRP.
- Pour les scénarios de basculement et la configuration à deux routeurs. Ainsi, si un routeur s'arrête, l'autre routeur lui succède sans interruption. (L'architecture SNAT n'est pas conçue

pour gérer les basculements d'interfaces.)
- Le scénario de routage non asymétrique est pris en charge. Le routage asymétrique peut être géré uniquement si la latence du paquet de réponse est supérieure à celle connue entre les deux routeurs SNAT lors de l'échange de messages SNAT.

Actuellement, l'architecture SNAT n'est pas conçue pour gérer la robustesse. Par conséquent, ces tests ne devraient pas réussir :

- Lorsque les entrées NAT sont effacées alors qu'il y a du trafic.
- Lorsque les paramètres de l'interface (comme la modification de l'adresse IP, l'arrêt/la non-fermeture, etc.) sont modifiés alors qu'il y a du trafic.
- Les commandes clearorshowspécifiques à SNAT ne sont pas censées s'exécuter correctement et ne sont pas recommandées.Voici quelques-unes des commandes clearandshowassociées à SNAT :

```
clear ip snat sessions *
clear ip snat sessions
```

```
clear ip snat translation distributed *
clear ip snat translation peer < IP address of SNAT peer>
sh ip snat distributed verbose
sh ip snat peer < IP address of peer>
```

- Si l'utilisateur souhaite effacer des entrées, **les** commandes **clear ip nat trans forcedorclear ip nat trans *** peuvent être utilisées.Si l'utilisateur veut afficher les entrées, les commandes **show ip nat translation**, **show ip nat translations verbose**, **et show ip nat** statspeuvent être utilisées. *Si le service* interne est configuré, il peut également afficher des informations spécifiques à SNAT.
- Les traductions NAT sont effacées au niveau du routeur de secours, ce qui n'est pas recommandé. Effacez toujours les entrées NAT sur le routeur SNAT principal.
- La fonction SNAT n'est pas à haute disponibilité. Par conséquent, les configurations sur les deux routeurs doivent être identiques. Les deux routeurs doivent exécuter la même image. Assurez-vous également que la plate-forme sous-jacente utilisée pour les deux routeurs SNAT est identique.

Meilleures pratiques NAT

Q. Existe-t-il des meilleures pratiques NAT ?

R.Oui. Voici les meilleures pratiques NAT :

1. Lorsque vous utilisez la NAT dynamique et statique, la liste de contrôle d'accès qui définit la règle pour la NAT dynamique doit exclure les hôtes locaux statiques afin qu'il n'y ait pas de chevauchement.
2. Si vous utilisez ACL pour NAT **avec permit ip any any** vous pouvez obtenir des résultats imprévisibles. Après 12.4(20)T, la NAT peut traduire les paquets HSRP et de protocole de routage générés localement s'ils sont envoyés par l'interface externe, ainsi que les paquets chiffrés localement qui correspondent à la règle NAT.

3. Lorsque vous avez des réseaux qui se chevauchent pour NAT, utilisez **le mot-clé match-in-**vrfkeyword.Vous devez ajouter **le mot-clé match-in-**vrf pour les entrées NAT statiques VRF qui se chevauchent pour différents VRF, mais il n'est pas possible de chevaucher des adresses NAT globales et VRF.

```
Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf RED match-in-vrf


Router(config)#ip nat inside source static 10.1.1.1 10.2.2.2 vrf BLUE match-in-vrf
```

4. Les pools NAT avec la même plage d'adresses ne peuvent pas être utilisés dans différents VRF, sauf si **le mot-clé match-in-**vrf est utilisé. Exemple :

```
ip nat pool poolA 172.31.1.1 172.31.1.10 prefix-length 24
ip nat pool poolB 172.31.1.1 172.31.1.10 prefix-length 24
ip nat inside source list 1 poolA vrf A match-in-vrf
ip nat inside source list 2 poolB vrf B match-in-vrf
```

   Remarque : même si la configuration CLI est valide, sans le mot clé **match-in-vrf**, la configuration n'est pas prise en charge.
5. Lorsque vous déployez l'équilibrage de charge des FAI avec surcharge d'interface NAT, la meilleure pratique consiste à utiliser la route-map avec correspondance d'interface sur correspondance d'ACL.
6. Lorsque vous utilisez le mappage de pool, vous ne devez pas utiliser deux mappages différents (ACL ou route-map) pour partager la même adresse de pool NAT.
7. Lorsque vous déployez les mêmes règles NAT sur deux routeurs différents dans le scénario de basculement, vous devez utiliser la redondance HSRP.
8. Ne définissez pas la même adresse globale interne avec une NAT statique et une plage dynamique, car cela pourrait entraîner des résultats indésirables.

Informations connexes

- Assistance et documentation techniques - Cisco Systems

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.