Traduction d'adresses réseau (NAT) - Forum aux questions

Table des matières

Introduction

Ce document fournit des réponses aux questions fréquentes à propos de la traduction d'adresses de réseau (NAT).

NAT générique

Q. Qu'est-ce que la NAT ?

R. La traduction d'adresses 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. NAT fonctionne sur un routeur, qui en général connecte deux réseaux ensemble, et traduit les adresses privées (pas globales uniques) au sein du réseau interne en adresses légales, avant que des paquets soient transférés à l'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. Ce comportement fournit une sécurité supplémentaire en cachant efficacement l'ensemble du réseau interne derrière cette adresse. 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 la fonction NAT fonctionne-t-elle ?

R. Fondamentalement, 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 configurer au moins une interface sur un routeur (NAT externe) et une autre interface sur le routeur (NAT interne) et un ensemble de règles pour traduire les adresses IP dans les en-têtes de paquet (et les charges utiles si désiré) 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 à Guide de configuration des services d'adressage IP Cisco IOS ou à Configuration 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 Cisco PIX de NAT ?

R. La fonction NAT basée sur la plate-forme logicielle Cisco IOS n'est pas fondamentalement différente de la fonction NAT de l'appliance de sécurité Cisco PIX. Les principales différences incluent les différents types de trafic pris en charge dans les mises en œuvre. Référez-vous à Exemples de configuration NAT pour plus d'informations sur la configuration de NAT sur les périphériques Cisco PIX (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 à Navigateur de fonctionnalités Cisco afin d'utiliser cet outil.

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

R. L’ordre dans lequel les transactions sont traitées à l’aide de la fonction NAT dépend du fait qu’un paquet passe 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 des opérations NAT pour plus d'informations.

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

R. Oui. La fonctionnalité NAT - Static IP Support assure la prise en charge pour les utilisateurs dotés d'adresses IP statiques, ce qui leur permet d'établir une session IP dans un environnement de réseau 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. À l'aide de NAT, vous pouvez établir un hôte virtuel sur le réseau interne, qui coordonne la répartition de la 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. En plus de permettre aux utilisateurs de mieux contrôler la façon dont les adresses NAT sont utilisées, la fonctionnalité Rate-Limiting NAT Translation permet également de contenir les effets des virus, des vers et des attaques de 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.

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

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.

Q. Quel type de performances de routage peut être attendu lors de l’utilisation de la fonction NAT de Cisco IOS ?

R. Cisco IOS NAT prend en charge la commutation 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,
- les autres applications en cours d'exécution,
- 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 toute 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 NVRAM. Par conséquent, 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. Cisco IOS NAT prend-il 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. Référez-vous à Comment configurer 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, utilisez une liste d'accès qui décrit l'ensemble d'hôtes ou de réseaux ayant besoin de NAT. Toutes les sessions sur un même hôte seront soit traduites soit transférées via le routeur sans être traduites.

Vous pouvez utiliser des listes d'accès, listes d'accès étendues et mappages de routes pour définir les *règles de traduction des périphériques IP.* L'adresse réseau et le masque de sous-réseau approprié devraient 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. Lors d'une configuration NAT statique, lorsque le paquet ne correspond à aucune configuration de règle statique, le paquet sera envoyé sans traduction.

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

R. La PAT (surcharge) divise les ports disponibles par adresse IP globale en trois plages : 0-511, 512-1023 et 1024-65535. La fonction PAT attribue un port source unique à chaque session UDP ou TCP. Elle essaie d'assigner la valeur de port de la demande d'origine, mais si le port source d'origine est déjà utilisé, elle parcourt la plage de ports spécifique à partir de son début pour trouver pour le premier port disponible et assigne ce dernier à la conversation. Une exception

existe pour la base de code 12.2S. La base de code 12.2S utilise une logique de port différente ; il n'existe aucune réservation de port.

Q. Comment fonctionne la PAT ?

R. La PAT fonctionne avec une adresse IP globale ou plusieurs adresses.

PAT avec une seule adresse 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 PAT connaît le type de trafic et si ce type de trafic a « un ensemble de ports spécifiques ou de ports qu'il négocie » à utiliser, PAT les réserve 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). **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.
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, PAT effectue une recherche à partir du début du groupe approprié (commençant à 1 pour les applications TCP ou UDP, et à 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.

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 à

	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 assigne le port source et la session continue.
10	Si le port source demandé n'est pas disponible, NAT effectue une recherche à partir du début du groupe approprié (commençant à 1 pour les applications TCP ou UDP, et à 0 pour ICMP).
11	Si un port est disponible, il est assigné et la session continue.
12	Si aucun port n'est disponible, le paquet est abandonné, sauf si une autre adresse IP est disponible dans le pool.

Q. Que sont les pools 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 effectue la traduction entre des hôtes internes adressés des réseaux 192.168.1.0 ou 192.168.2.0 au réseau global unique 10.69.233.208/28 :

```
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, le but est de définir une adresse virtuelle à laquelle les connexions établies 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 DRAM disponible sur le routeur concerné. (Cisco recommande de configurer une taille de pool de 255.) Chaque pool ne devrait pas dépasser 16 bits. Dans la version 12.4(11)T et ultérieures, le logiciel IOS introduit CCE (Common Classification Engine). Ce module ne permet pas à NAT d'avoir plus de 255 pools. Dans la base de code 12.2S, il n'existe aucune restriction de maximum de pools.

Q. Quel est l'avantage de l'utilisation d'une carte de route 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 de plusieurs pools à l'aide des mappages de routes pour plus d'informations.

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

R. Le chevauchement d'adresses IP fait référence à une situation où deux emplacements qui veulent s'interconnecter utilisent le même schéma d'adresses IP. Cette situation n'est pas exceptionnelle ; elle se produit souvent lors de la fusion ou de l'acquisition des sociétés. Sans prise en charge spéciale, les deux emplacements ne peuvent pas se connecter et établir des sessions. L'adresse IP superposée peut être une adresse publique assignée à une autre société, une adresse privée assignée à une autre société, ou peut appartenir à la plage d'adresses privées comme défini par le document RFC 1918.

Les adresses IP privées ne sont pas routables et exigent que les traductions NAT autorisent les connexions vers le monde extérieur. La solution implique d'intercepter les réponses aux requêtes de nom de système de noms de domaine (DNS) de l'extérieur vers l'intérieur, de configurer une traduction de l'adresse externe, et de corriger la réponse DNS avant de la transférer à l'hôte interne. Un serveur DNS doit être impliqué des deux côtés du périphérique NAT pour résoudre les utilisateurs qui veulent disposer d'une connexion entre les deux réseaux.

NAT peut inspecter et exécuter la traduction d'adresses sur le contenu d'enregistrements DNS *A et* PTR, comme illustré dans Utilisation de NAT dans des réseaux en superposition.

Q. Que sont les traductions NAT statiques ?

R. 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. Cette situation se produit généralement lors de l'exécution de la traduction d'adresses de port (PAT).

L'exemple suivant montre comment configurer le mappage de routes pour permettre la traduction externe-interne pour NAT statique :

```
ip nat inside source static 1.1.1.1 2.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
permit ip any 30.1.10.128 0.0.0.127'
route-map R1 permit 10
match ip address ACL-A
```

Q. Qu'entend-on par *surcharge* NAT ? est-ce la même chose que PAT ?

R. Oui. La surcharge NAT correspond à 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 associée à un 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'adresses IP et des ports source/de destination, qui est généralement appelée PAT ou surcharge.

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

Q. Que sont les traductions NAT dynamiques ?

R. Dans les traductions NAT dynamiques, les utilisateurs peuvent établir un mappage dynamique entre des adresses locales et globales. Le mappage dynamique est obtenu en définissant les adresses locales à traduire et le pool d'adresses ou l'adresse IP de l'interface à partir duquel ou de laquelle allouer les adresses globales et associer les deux.

Q. Qu'est-ce que ALG ?

R. 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 à Utilisation des passerelles au niveau des applications 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 des pools dynamiques contenant 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 à Configurer NAT statique et dynamique simultanément.

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

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

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

R. La NAT introduit des fonctionnalités de port supplémentaires : « plage complète » et « mappage de ports ».

- 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 sources définies par l'utilisateur pour PAT pour 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 NAT de prendre en charge l'*indépendance du point de terminaison*.

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 à 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 devront être fragmentés ou ignorés lors de l'envoi en dehors de l'interface. Si le bit DF (Don't Fragment) n'est pas défini dans l'en-tête IP du paquet, le paquet est fragmenté. Si le bit DF est défini dans l'en-tête IP du paquet, le paquet est abandonné et un message d'erreur ICMP indiquant la valeur MTU du saut suivant est renvoyé 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 à Résoudre les problèmes de fragmentation IP, MTU, MSS et PMTUD avec GRE et IPSec pour plus d'informations.

La segmentation TCP a lieu lorsqu'une application sur 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 segmente tout d'abord ces données en segments TCP (basés sur la valeur de MSS TCP), puis ajoute l'en-tête TCP et transmet ce segment TCP au protocole IP. Le protocole IP ajoute alors une en-tête IP pour envoyer le paquet à l'hôte final distant. Si le paquet IP avec le segment TCP est plus grand que la valeur MTU IP sur une interface sortante sur le chemin d'accès entre les hôtes TCP, le protocole IP fragmente le paquet IP/TCP pour qu'il corresponde. Ces fragments de paquets IP sont rassemblés sur l'hôte distant par la couche IP et le segment TCP complet (initialement envoyé) est remis 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 ?

R. NAT prend uniquement en charge les fragments IP désordonnés en raison de **ip virtual-reassembly**.

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

R. 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. Il n'existe aucune MIB NAT prise en charge, y compris CISCO-IETF-NAT-MIB.

Q. Qu’est-ce que le *délai d’attente TCP*, et comment est-il lié au compteur 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 démarre 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 le délai d’expiration d’une traduction NAT dans la table de traduction NAT ?

R. Oui. Vous pouvez modifier les valeurs d'expiration 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 empêcher le protocole LDAP (Lightweight Directory Access Protocol) d’attacher des octets supplémentaires à chaque paquet de réponse LDAP ?

R. Les paramètres LDAP ajoutent les octets supplémentaires (résultats de la recherche LDAP)

lors du traitement des 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 ont pour conséquence que le paquet dépasse l'unité de transmission maximale (MTU) sur un réseau, le paquet est abandonné. Dans ce cas, Cisco recommande que vous désactiviez ce comportement LDAP à l'aide de la commande **no ip nat service append-ldap-search-res de la CLI pour 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 sur NAT pour l'adresse IP locale externe. Dans ce cas, tout paquet allant de l'intérieur vers l'extérieur et qui utilise une règle statique externe requiert ce type de route. Dans de tels scénarios, outre la route globale interne-locale externe, l'adresse IP du saut suivant doit également être configurée. Si le saut suivant n'est pas configuré, le système considère qu'il s'agit d'une erreur de configuration et le comportement résultant n'est pas 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 ACL 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. elle ne peut donc pas prendre en charge les listes d'accès comportant le 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 ?

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

NAT ne prend pas encore en charge SCCP v17. Tant que la prise en charge NAT de SCCP v17 n'est pas implémentée, le microprogramme doit être rétrogradé à la version 8-3-5 ou inférieure afin que SCCP v16 soit négocié. CUCM6 ne rencontrera pas le problème NAT avec une charge de téléphone tant qu'il utilisera SCCP v16. Cisco IOS ne prend pas actuellement en charge SCCP version 17.

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

R. 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. La fonctionnalité d'allocation de port PAT du fournisseur de services 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 conformément au document RFC-1889. Un appel avec un numéro de port compris dans cette plage entraîne une traduction PAT vers un autre numéro de port de cette plage. De même, une traduction PAT pour un numéro de port en dehors de cette plage n'entraîne pas de traduction en un numéro compris dans la plage donnée.

Q. Qu'est-ce que le protocole SIP (Session Initiation Protocol) et les paquets SIP peuvent-ils être traités par 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 à Configuration de la traversée NAT hébergée 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. IOS-NAT prend en charge la segmentation TCP pour H323 dans 12.4 Mainline et la segmentation TCP pour SKINNY à partir de 12.4(6)T.

Q. Y a-t-il des avertissements à prendre en compte lors de l'utilisation d'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 façon périodique et NAT met à jour ce point/cette association d'information selon le message de signalisation.

Q. Y a-t-il des problèmes connus causés par l'émission de la commande clear ip nat trans * ou de la commande clear ip nat trans forced dans un déploiement vocal ?

R. Dans les déploiements vocaux, lorsque vous émettez une commande **clear ip nat trans *** ou une commande **clear ip nat trans forced** et que vous disposez de la NAT dynamique, vous effacez le trou de broche/association et devez attendre le prochain cycle d'enregistrement du périphérique interne pour le rétablir. Cisco recommande de ne pas utiliser ces commandes clear dans les déploiements vocaux.

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

R. Non. La solution de colocalisation n'est pas prise en charge actuellement. Le déploiement suivant avec NAT (dans le même cadre) est considéré comme une solution hébergée conjointement : 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 prendra-t-il un jour en charge la traduction d’adresses réseau (NAT) avec le même espace d’adressage dans un VRF que dans un espace d’adressage global ? Actuellement, je reçois cet avertissement : *"% similar static entry (1.1.1.1 —> 2.2.2.2) existing already exists" (1.1.1.1 —> 22.2.2.2) existe déjà* lorsque j'essaie de configurer les éléments suivants :

```
72UUT(config)#ip nat inside
 source static 1.1.1.1 22.2.2.2 72UUT(config)#ip nat inside source static
 1.1.1.1 22.2.2.2 vrf RED
```

R. La NAT héritée prend en charge le chevauchement de la configuration des adresses sur

différents VRF. Vous devriez configurer le chevauchement dans la règle avec l'option **match-in-vrf et définir ip 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 du VRF superposées pour les différents VRF.** Cependant, il n'est pas possible de superposer des adresses globales et NAT VRF.

```
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf
```

Q. La fonction NAT héritée prend-elle en charge VRF-Lite (traduction NAT d'un VRF vers un VRF différent) ?

R. Non. Vous devez utiliser NVI pour la traduction NAT entre différents VRF. Vous pouvez utiliser la NAT héritée pour effectuer une traduction NAT VRF-global ou NAT au sein d'un même VRF.

NAT-NVI

Q. Qu'est-ce que NAT NVI ?

R. NVI signifie NAT Virtual Interface. Elle permet à NAT d'effectuer la traduction entre deux VRF. Cette solution devrait être utilisée à la place de la traduction d'adresses de réseau sur un bâton.

Q. La fonction NAT NVI doit-elle être utilisée lors de la traduction NAT entre une interface globale et une interface dans un VRF ?

R. Cisco 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. La segmentation TCP n'est pas prise en charge 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) ?

R. La fonction SNAT permet à deux traducteurs d’adresses réseau ou plus de fonctionner comme un groupe de traduction. Un membre du groupe de traduction gère le trafic nécessitant 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 prend-elle en charge le routage asymétrique ?

R. Le routage asymétrique prend en charge NAT en activant comme mise en file d’attente. Par défaut, l'option « as-queueing » est activée. Cependant, à partir de la version 12.4(24)T, cette option n'est plus prise 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 ?

R. NAT-PT est une traduction de v4 à v6 pour NAT. La conversion de protocole (NAT-PT) est un mécanisme de traduction IPv6-IPv4, comme défini dans les documents RFC 2765 et RFC 2766, qui permet à des 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) ?

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

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

R. 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 7300/7600/6k et plate-forme compatible

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

R. La fonction SNAT n'est pas disponible sur le Catalyst 6500 de la catégorie SX.

Q. La fonction NAT compatible VRF est-elle prise en charge dans le matériel sur le 6k ?

R. La 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 en exploitant 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. Skinny NAT ALG n'est pas pris en charge dans 12.4T sur la gamme 850.

Déploiement de NAT

Q. Comment mettre en oeuvre la fonction NAT ?

R. La 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 mettre en oeuvre la fonction NAT avec la voix ?

R. La prise en charge NAT de la fonctionnalité vocale permet de retraduire en paquet les messages SIP intégrés passant par un routeur configuré avec la traduction d’adresses de réseau (NAT). 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 de configurer plusieurs VPN MPLS 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 tous les VPN MPLS sont bien distincts les uns des autres.

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 mettre en oeuvre l'équilibrage de charge avec la NAT ?

R. Il existe deux types d'équilibrage de charge qui peuvent être effectués avec NAT : vous pouvez équilibrer la charge en arrivée sur un ensemble de serveurs afin de distribuer la charge sur les serveurs, ou équilibrer la charge du trafic utilisateur vers Internet sur plusieurs ISP.

Pour plus d'informations sur l'équilibrage de charge en sortie, référez-vous à Équilibrage de charge NAT du logiciel IOS pour deux connexions ISP.

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

R. La sécurité IP (IPSec), ESP (Encapsulating Security Payload) est prise en charge par 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 fonctionnalité IPSec NAT transparency introduit la prise en charge du trafic IPSec via des points NAT ou PAT dans le réseau en résolvant plusieurs problèmes d'incompatibilité connus entre NAT et IPSec.

Q. Comment mettre en oeuvre NAT-PT ?

A. NAT-PT (traduction d'adresses de réseau - Conversion de protocole) est un mécanisme de traduction IPv6-IPv4, comme défini dans les documents RFC 2765 et RFC 2766, qui permet à des 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 avec l'adresse IP source pour un flux de multidiffusion. Un mappage de routes ne peut pas être utilisé dans le cadre de NAT dynamique pour multicast ; dans ce cas, seule une liste d'accès est prise en charge.

Pour plus d'informations, référez-vous à Comment fonctionne NAT multicast sur les routeurs

Cisco. Le groupe multicast de destination est traduit par NAT à l'aide d'une solution de réflexion de service multicast.

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

R. La fonction SNAT permet 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. De futurs déploiements devraient être exécutés uniquement après avoir contacté votre équipe de compte Cisco afin de valider la conception par rapport aux restrictions applicables.

SNAT est recommandé pour les scénarios suivants :

- Le mode principal/secondaire n'est pas recommandé car certaines fonctionnalités manquent 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 ; on ne s'attend donc pas à ce que ces essais réussissent :

- Effacer les entrées NAT en présence de trafic.
- Modification des paramètres d'interface (comme la modification d'adresse IP, arrêt/pas d'arrêt, etc.) en présence de trafic.
- Les commandes **clear ou show spécifiques à SNAT ne devraient pas s'exécuter correctement et ne sont pas recommandées.**Quelques-unes des commandes **clear et show 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 veut effacer des entrées, il peut utiliser les commandes **clear ip nat trans forced ou clear ip nat trans *.**Si l'utilisateur veut afficher des entrées, il peut utiliser les commandes **show ip nat translation**, **show ip nat translations verbose** et **show ip nat stats.** Si *service internal est configuré, les informations spécifiques à SNAT s'affichent également.*
- Il n'est pas recommandé d'effacer des traductions NAT sur le routeur de secours. Effacez toujours les entrées NAT sur le routeur SNAT principal.
- SNAT est différent de HA ; les configurations sur les deux routeurs doivent donc être identiques. Les deux routeurs doivent exécuter la même image. Assurez-vous également que

les deux routeurs SNAT utilisent la même plate-forme sous-jacente.

Meilleures pratiques NAT

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

R. Oui. Voici les meilleures pratiques NAT :

1. Lorsque vous utilisez NAT dynamique et statique, l'ACL qui définit la règle de NAT dynamique doit exclure les hôtes locaux statiques, afin d'éviter tout chevauchement.
2. Prenez garde lors de l'utilisation d'une ACL pour NAT avec **permit ip any any car les résultats peuvent être inattendus.** Après la version 12.4(20)T, NAT traduit localement les paquets HSRP et de protocole de routage s'ils sont envoyés à l'extérieur de l'interface externe, ainsi que localement les paquets chiffrés qui correspondent à la règle NAT.
3. Lorsque des réseaux se chevauchent pour NAT, utilisez le mot clé **match-in-vrf**.Vous devez ajouter le mot clé **match-in-vrf** pour les entrées NAT statiques de VRF superposées pour différents VRF, mais il n'est pas possible de superposer des adresses globales et NAT VRF.
   ```
   Router(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf


   Router(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf
   ```
4. Des pools NAT avec la même plage d'adresses ne peuvent pas être utilisés dans différents VRF à moins que le mot clé **match-in-vrf** soit utilisé.Exemple :

   ```
   ip nat pool poolA 171.1.1.1 171.1.1.10 prefix-length 24
   ip nat pool poolB 171.1.1.1 171.1.1.10 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
   ```

   Note: Même si la configuration CLI est valide, sans le mot clé **match-in-vrf** la configuration n'est pas prise en charge.
5. Lors du déploiement de l'équilibrage de charge d'ISP avec la surcharge d'interface NAT, la meilleure pratique est d'utiliser le mappage de routes avec une correspondance d'interface plutôt que la correspondance d'ACL.
6. Avec le mappage de pools, n'utilisez pas deux mappages différents (ACL ou mappage de routes) pour partager une même adresse de pool NAT.
7. Lors du déploiement des mêmes règles NAT sur deux routeurs différents dans un scénario de basculement, vous devriez 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

- Technical Support & Documentation - 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.