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

Table des matières

Introduction

NAT générique

- Q. Qu'est-ce que la NAT?
- Q. Comment fonctionne la NAT?
- Q. Comment configurer la NAT?
- Q. Quelles sont les principales différences entre les mises en oeuvre du logiciel Cisco IOS et du dispositif de sécurité Cisco PIX de la fonction NAT ?
- Q. Sur quel matériel de routage Cisco la NAT Cisco IOS est-elle disponible? Comment peut-on commander le matériel ?
- Q. La NAT se produit-elle avant ou après le routage?
- Q. La NAT peut-elle être déployée dans un environnement LAN sans fil public?
- Q. La NAT fait-elle l'équilibrage de charge TCP pour les serveurs sur le réseau interne?
- Q. Puis-je limiter le nombre de traductions NAT?
- Q. Comment le routage est-il enregistré ou propagé pour les sous-réseaux ou adresses IP utilisés par la NAT?
- Q. Combien de sessions NAT simultanées sont prises en charge avec Cisco IOS?
- Q. À quel type de performances de routage peut-on s'attendre lors de l'utilisation de Cisco IOS NAT?
- Q. Cisco IOS NAT peut-il être appliqué aux sous-interfaces?
- Q. Cisco IOS NAT peut-il être utilisé avec le protocole HSRP (Hot Standby Router Protocol) pour fournir des liaisons redondantes à un FAI?
- Q. Est-ce que Cisco IOS NAT peut prendre en charge les traductions entrantes sur une interface de relayage de trames? Prend-il en charge les traductions sortantes côté Ethernet ?
- Q. Un seul routeur NAT peut-il permettre à certains utilisateurs d'utiliser la NAT et à d'autres utilisateurs sur la même interface Ethernet de continuer d'utiliser leurs propres adresses IP?
- Q. Lors de la configuration pour la traduction d'adresses de port (PAT) en surcharge, quel est le nombre maximal de traductions qui peuvent être créées par adresse IP globale interne?
- Q. Comment fonctionne la PAT?
- Q. Que sont les ensembles d'adresses IP NAT?
- Q. Quel est le nombre maximal de pools IP NAT configurables (ip nat pool)?
- Q. Quel est l'avantage d'utiliser une carte de routage plutôt qu'une liste de contrôle d'accès dans un ensemble de NAT?
- Q. Qu'est-ce que le chevauchement d'adresses IP dans le contexte de la NAT ?
- Q. Que sont les traductions d'adresses réseau statiques?
- Q. Qu'entend-on par surcharge NAT ? est-ce PAT ?
- Q. Que sont les traductions d'adresses réseau dynamiques?
- Q. Qu'est-ce qu'ALG?
- Q. Est-il possible de créer une configuration avec des traductions d'adresses réseau statiques et dynamiques?
- Q. Lorsqu'une commande traceroute est exécutée via un routeur NAT, la commande traceroute affiche-t-elle l'adresse NAT-globale ou l'adresse NAT-locale est-elle divulguée ?

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

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

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

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

Q. Existe-t-il une base d'information de gestion pour la traduction d'adresses réseau prise en charge?

Q. Qu'est-ce que le délai d'expiration TCP, et quel est son rapport avec le temporisateur TCP de la NAT?

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

Q. Comment puis-je empêcher le protocole LDAP (Lightweight Directory Access Protocol) de joindre des octets supplémentaires à chaque paquet de réponse LDAP?

Q. Quelle est la recommandation de routage pour l'adresse IP globale interne ou externe sur le boîtier NAT?

Q. La fonction NAT de Cisco IOS prend-elle en charge les ACL avec un mot clé log ?

Voix-NAT

La NAT prend-elle en charge la version 17 du protocole « Skinny Client Control » (SCCP) qui est livrée avec la version 7 de Cisco Unified Communications Manager (CUCM)?

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

Q. Qu'est-ce que l'amélioration de l'attribution des ports PAT aux fournisseurs de services pour RTP et RTCP?

Q. Qu'est-ce que le protocole d'ouverture de session (Session Initiation Protocol), et les paquets SIP peuvent-ils faire l'objet d'une NAT?

Q. Qu'est-ce que la prise en charge de la fonctionnalité de traversée NAT hébergée Cisco IOS pour le contrôleur de frontière de session (SBC)?

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

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

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

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

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

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

NAT avec VRF/MPLS

Q. Un routeur NAT prend-il en charge la traduction d'adresses réseau (NAT) pour le même espace d'adressage dans un VRF en même temps que la traduction d'adresses réseau (NAT) dans un espace d'adressage global ? Actuellement, je reçois cet avertissement : "% similar static entry (10.1.1.1 —> 10.210.2.2) already exists" lorsque j'essaie de configurer ceci :

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

NAT NVI

Q. Qu'est-ce que la NAT NVI?

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

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

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

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

NAT par états (SNAT)

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

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

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

NAT-PT (v6 à v4)

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

La NAT-PT est-elle prise en charge dans le chemin CEF (Cisco Express Forwarding)?

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

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

Cisco 7300/7600/6k dépendant de la plate-forme

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

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

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

Cisco 850 dépendant de la plate-forme

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

Déploiement NAT

Q. Comment mettre en œuvre la NAT?

Q. Comment mettre en œuvre la NAT avec voix?

Q. Comment intégrer la NAT aux VPN MPLS?

Q. La disponibilité élevée dans le protocole HSRP est-elle prise en charge par une NAT statique?

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

Q. Comment mettre en œuvre l'équilibrage de charge avec la NAT?

Q. Comment puis-je mettre en oeuvre la fonction NAT conjointement avec IPSec ?

Q. Comment mettre en œuvre la NAT-PT?

Q. Comment mettre en œuvre la NAT de multidiffusion?

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

Meilleures pratiques NAT

Q. Existe-t-il de meilleures pratiques en matière de NAT?

Informations connexes

Introduction

Ce document décrit les questions fréquentes sur la traduction d'adresses réseau (NAT).

NAT générique

Q. Qu'est-ce que la NAT?

A. La traduction d'adresses réseau (NAT) est conçue pour préserver les adresses IP. Elle permet aux réseaux IP privés qui utilisent des adresses IP non enregistrées de se connecter à Internet. La fonction NAT fonctionne sur un routeur, connectant généralement 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 fonctionnalité, la fonction NAT peut être configurée pour annoncer au monde extérieur une seule adresse pour l'ensemble du réseau. Cela renforce la sécurité en masquant efficacement l'ensemble du réseau interne derrière cette adresse. La fonction NAT offre la double fonction de sécurité et de conservation d'adresses et est généralement mise en oeuvre dans des environnements d'accès à distance.

Q. Comment fonctionne la NAT?

A. En résumé, elle permet à un seul périphérique, tel qu'un routeur, d'agir en tant qu'agent entre Internet (ou un réseau public) et un réseau local (ou un réseau privé), ce qui signifie qu'une seule adresse IP est nécessaire pour représenter un groupe entier d'ordinateurs hors de leur réseau.

Q. Comment configurer la NAT?

A. Pour configurer la NAT traditionnelle, vous devez créer au moins une interface sur un routeur externe et une autre interface sur un routeur externe. Vous devez ensuite créer un ensemble de règles pour traduire les adresses IP dans les en-têtes de paquets (et les charges utiles, le cas échéant). Afin de configurer l'interface virtuelle NAT (NVI), vous avez besoin d'au moins une interface configurée avec l'activation NAT avec le même ensemble de règles que mentionné ci-dessus.

Pour plus d'informations, référez-vous au 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 la fonction NAT ?

A. Il n'y a pas de différences fondamentales entre ces deux modèles. Les principales différences incluent les différents types de trafic pris en charge dans les implémentations. Reportez-vous aux exemples de configuration de NAT pour plus d'informations sur la configuration de la NAT sur les périphériques Cisco PIX (y compris les types de trafic pris en charge).

Q. Sur quel matériel de routage Cisco la NAT Cisco IOS est-elle disponible? Comment peut-on commander le matériel ?

R. L'outil Cisco Feature Navigator permet aux clients d'identifier une fonctionnalité (NAT) et de trouver dans quelle version et quelle version du matériel cette fonctionnalité du logiciel Cisco IOS

est disponible. Référez-vous à Cisco Feature Navigator afin d'utiliser cet outil.

Remarque : Seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils Cisco internes.

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

A. 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, et la traduction externe vers interne se produit avant le routage. Référez-vous à Ordre des opérations NAT pour plus d'informations.

Q. La 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, ce qui leur permet d'établir une session IP dans un environnement de réseau local sans fil public.

Q. La NAT fait-elle l’équilibrage de charge TCP pour les serveurs sur le réseau interne?

A. Oui. Grâce à la fonction NAT, vous pouvez établir un hôte virtuel sur le réseau interne qui coordonne le partage de charge entre les hôtes réels.

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

R. Oui. La fonction de traduction NAT de limitation de débit permet de limiter le nombre maximal d’opérations NAT simultanées sur un routeur. En plus de permettre aux utilisateurs de mieux contrôler l'utilisation des adresses NAT, 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 enregistré ou propagé pour les sous-réseaux ou adresses IP utilisés par la NAT?

R. Le routage des adresses IP créées par NAT est enregistré dans les situations suivantes :

- Le pool d’adresses globales internes provient du sous-réseau d’un routeur de tronçon suivant.
- L’entrée de route statique est configurée dans le routeur de tronçon suivant et redistribuée au sein du réseau de routage.

Lorsque l'adresse globale interne est mise en correspondance avec l'interface locale, NAT installe un alias IP et une entrée ARP, auquel cas le routeur peut effectuer un proxy-arp pour ces adresses. Si ce comportement n'est pas souhaité, utilisez le mot clé no-alias.

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

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

R. La limite de session NAT est limitée par la mémoire vive dynamique (DRAM) disponible dans le routeur. Chaque traduction NAT consomme environ 312 octets en DRAM. Par conséquent, 10 000 traductions (plus que ce qui serait généralement traité sur un seul routeur) consomment environ 3 Mo. Par conséquent, le matériel de routage type dispose de plus de mémoire que nécessaire pour prendre en charge des milliers de traductions NAT.

Q. À quel type de performances de routage peut-on s’attendre lors de l’utilisation de Cisco IOS NAT?

A. Cisco IOS prend en charge la commutation Cisco Express Forwarding, la commutation rapide et la commutation de processus. Pour les versions 12.4T et ultérieures, le chemin de commutation rapide n'est plus pris en charge. Pour la plate-forme Cat6k, l'ordre de commutation est Netflow (HW switching path), CEF, process path.

Les performances dépendent de plusieurs facteurs :

- Type d'application et type de trafic
- Indique si les adresses IP sont intégrées
- Échange et inspection de plusieurs messages
- Port source requis
- Le nombre de traductions
- Autres applications en cours d'exécution

- Le type de matériel et de processeur

Q. Cisco IOS NAT peut-il être appliqué 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). La fonction NAT ne peut pas être configurée avec l'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. Cisco IOS NAT peut-il être utilisé avec le protocole HSRP (Hot Standby Router Protocol) pour fournir des liaisons redondantes à un FAI?

R. Oui. La NAT fournit une redondance HSRP. Cependant, il est différent de SNAT (Stateful NAT). NAT avec HSRP est un système sans état. La session en cours n'est pas maintenue en cas d'échec. Pendant la configuration NAT statique (lorsqu'un paquet ne correspond à aucune configuration de règle STATIC), le paquet est envoyé sans traduction.

Q. Est-ce que Cisco IOS NAT peut prendre en charge les traductions entrantes sur une interface de relayage de trames? Prend-il en charge les traductions sortantes côté Ethernet ?

R. Oui. L'encapsulation n'est pas importante pour NAT. La fonction NAT peut être exécutée lorsqu'une interface possède une adresse IP et que l'interface est interne ou externe. Il doit y avoir un interne et un externe pour que la NAT fonctionne. Si vous utilisez NVI, il doit y avoir au moins une interface NAT activée. Voir Comment configurer la fonction NAT ? pour plus de détails.

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

A. 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.

Les listes d'accès, les listes d'accès étendues et les cartes de routage peuvent être utilisées pour définir des règles par lesquelles les périphériques IP sont traduits. 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 fonction NAT statique, lorsque le paquet ne correspond à aucune configuration de règle STATIC, le paquet est

envoyé sans traduction.

Q. Lors de la configuration pour la traduction d’adresses de port (PAT) en surcharge, quel est le nombre maximal de traductions qui peuvent être créées par adresse IP globale interne?

R. Lors d’une PAT en surcharge, les ports disponibles sont répartis en trois plages selon leur adresse IP globale : 0-511, 512-1023 et 1024-65535. La PAT attribue un port source unique pour chaque session UDP ou TCP. Il tente d'attribuer 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'attribue à la conversation. Il existe une exception pour la base de code 12.2S. La base de code 12.2S utilise une logique de port différente et il n'y a pas de réservation de port.

Q. Comment fonctionne la PAT?

R. La PAT peut fonctionner avec une seule adresse IP globale ou plusieurs.

PAT avec une adresse IP

Condition	Description
1	La NAT/PAT inspecte le trafic et le fait correspondre à une règle de traduction.
2	La règle correspond à une configuration PAT.
3	Si la PAT connaît le type de trafic et si ce type de trafic a « un ensemble de ports spécifiques ou de ports qu'elle négocie » qu'elle utilise, elle les met de côté et ne les alloue pas en tant qu'identificateurs uniques.
4	Si une session sans configuration de port spéciale tente de se connecter, la fonction PAT traduit l'adresse IP source 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. En ce qui concerne le protocole de message de contrôle Internet (ICMP), le premier groupe commence à 0.
5	Si le port source demandé est disponible, la fonction PAT attribue le port source et la session se poursuit.
6	Si le port source demandé n'est pas disponible, la fonction PAT commence la recherche à partir du début du groupe concerné (en commençant à 1 pour les

	applications TCP ou UDP et à 0 pour ICMP).
7	Si un port est disponible, il est attribué et la session se poursuit.
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 les mêmes que pour une adresse IP unique.
8	Si aucun port n'est disponible dans le groupe approprié sur la première adresse IP, la fonction NAT passe à l'adresse IP suivante dans le pool et tente d'allouer le port source d'origine demandé.
9	Si le port source demandé est disponible, NAT attribue le port source et la session continue.
10	Si le port source demandé n'est pas disponible, la fonction NAT commence la recherche à partir du début du groupe concerné (en commençant à 1 pour les applications TCP ou UDP et à 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 disponible dans le pool.

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

R. Au besoin, la traduction d’adresses réseau peut regrouper les adresses IP en plages. Pour définir un pool, la commande de configuration est utilisée :

<#root>

```
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 cet exemple, 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 aucune traduction n'existe déjà, les paquets TCP de l'interface série 0 (l'interface externe) dont la destination correspond à la liste d'accès sont traduits en 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 groupes d'adresses IP configurables est limité par la mémoire vive dynamique disponible dans le routeur en question. (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 introduit CCE (Common Classification Engine). La fonction NAT est limitée à un maximum de 255 pools. Dans la base de code 12.2S, il n'y a pas de restriction de pools maximum.

Q. Quel est l'avantage d'utiliser une carte de routage plutôt qu'une liste de contrôle d'accès dans un ensemble de NAT?

R. Une carte de routage empêche les utilisateurs externes non désirés d'atteindre les utilisateurs ou les serveurs internes. Il peut également 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 ?

R. Le chevauchement d’adresses IP fait référence à une situation où deux emplacements qui veulent s’interconnecter utilisent tous deux le même schéma d’adresses IP. Il ne s'agit pas d'un événement inhabituel ; cela arrive souvent lorsque des entreprises fusionnent ou sont rachetées. Sans assistance spéciale, les deux sites ne peuvent pas se connecter et établir de 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 consiste à intercepter les réponses de requête de nom DNS (Domain Name System) de l'extérieur vers l'intérieur, à configurer une traduction pour l'adresse externe et à corriger la réponse DNS avant de la transmettre à l'hôte interne. Un serveur DNS doit être impliqué des deux côtés du périphérique NAT pour résoudre les utilisateurs qui souhaitent 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 DNS A et PTR, comme indiqué dans la section Utilisation de la fonction NAT dans les réseaux en chevauchement.

Q. Que sont les traductions d’adresses réseau statiques?

R. La traduction d’adresses réseau statiques crée une correspondance parfaite 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 routemap pour autoriser la traduction externe-interne pour la NAT statique :

<#root>

```
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 10.1.10.128 0.0.0.127'

route-map R1 permit 10
match ip address ACL-A
```

Q. Que signifie le terme NAT en surcharge? est-ce PAT ?

R. Oui. La surcharge NAT est PAT, ce 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. Lorsque vous surchargez, vous créez une traduction entièrement étendue. Il s'agit d'une entrée de table de traduction contenant l'adresse IP et les informations de port source/de destination, généralement appelée PAT ou surcharge.

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

Q. Que sont les traductions d’adresses réseau dynamiques?

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

Q. Qu’est-ce qu’ALG?

R. « ALG » correspond à Application Layer Gateway (passerelle des couches de l'application). NAT effectue un service de traduction sur tout trafic TCP/UDP (Transmission Control Protocol/User Datagram Protocol) qui ne transporte pas les adresses IP source et/ou de destination dans le flux de données d'application.

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

Référez-vous à Utilisation de passerelles de niveau application avec NAT pour plus d'informations.

Q. Est-il possible de créer une configuration avec des traductions d’adresses réseau statiques et dynamiques?

R. Oui. Cependant, la même adresse IP ne peut pas être utilisée pour la configuration NAT

statique ou dans le pool pour la configuration NAT dynamique. 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 contenant ces mêmes adresses globales. Des pools dynamiques doivent être créés pour exclure les adresses attribuées par des entrées statiques. Pour plus d'informations, référez-vous à Configuration simultanée de la NAT statique et dynamique.

Q. Lorsqu'une commande traceroute est exécutée via un routeur NAT, la commande traceroute affiche-t-elle l'adresse NAT-globale ou l'adresse NAT-locale est-elle divulguée ?

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

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

R. La NAT ajoute des fonctionnalités aux ports : full-range et port-map.

- La plage complète permet à la fonction NAT d'utiliser tous les ports, quelle que soit sa plage de ports par défaut.
- La carte de ports permet à la fonction 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.

À partir de la version 12.4(20)T2, la NAT introduit la randomisation des ports pour L3/L4 et le port symétrique.

- La randomisation des ports permet à la fonction NAT de sélectionner aléatoirement n'importe quel port global pour la demande de port source.
- Le port symétrique permet à la NAT de prendre en charge des terminaux indépendants.

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

R. La fragmentation IP se produit sur la couche 3 (IP) et la segmentation TCP se produit sur la couche 4 (TCP). La segmentation TCP se produit au niveau de la couche 4 (TCP). La fragmentation IP se produit lorsque des paquets qui sont plus grands que l'unité de transmission maximale (MTU) d'une interface sont envoyés à partir de cette interface. Ces paquets doivent être

fragmentés ou éliminés lorsqu'ils sont envoyés à l'interface. Si le bit Ne pas fragmenter (DF) 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 tronçon suivant est renvoyé à l'expéditeur. Tous les fragments d'un paquet IP portent le même Ident dans l'en-tête IP, ce qui permet au récepteur final de réassembler 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 se produit lorsqu'une application sur une station d'extrémité envoie des données. Les données d'application sont divisées en ce que le protocole TCP considère comme les segments de taille optimale à envoyer. Cette unité de données transmise du protocole TCP au protocole IP est appelée 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 inférieures à celles qu'ils peuvent traverser.

Le protocole TCP commence par segmenter ces données en segments TCP (en fonction de la valeur MSS du protocole TCP), puis ajoute l'en-tête TCP et transmet ce segment TCP au protocole IP. Le protocole IP ajoute ensuite 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 fragmente le paquet IP/TCP afin de s'adapter. Ces fragments de paquets IP sont réassemblés sur l'hôte distant par la couche IP et le segment TCP complet (qui a été envoyé à l'origine) est transmis à la couche TCP. La couche TCP ne sait pas qu'IP a fragmenté le paquet pendant le transit.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 désordonnées?

R. Seule la fragmentation IP désordonnée est prise en charge, en raison de la commande ip virtual-reassembly.

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

R. La même commande de débogage peut être utilisée dans les deux cas : debug ip nat frag.

Q. Existe-t-il une base d'information de gestion pour la traduction d'adresses réseau prise en charge?

R. Non. Il n'y a aucune base d'information de gestion pour la traduction d'adresses réseau, y compris CISCO-IETF-NAT-MIB.

Q. Qu’est-ce que le délai d’expiration TCP, et quel est son rapport avec le temporisateur TCP de la 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 étapes est terminée, la fonction NAT utilise un minuteur de 24 heures pour une entrée NAT par défaut. Si un hôte final envoie une commande RESET, la fonction NAT fait passer le compteur par défaut de 24 heures à 60 secondes. Dans le cas de FIN, NAT change le compteur par défaut de 24 heures à 60 secondes lorsqu'il reçoit 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 empêcher le protocole LDAP (Lightweight Directory Access Protocol) de joindre des octets supplémentaires à chaque paquet de réponse LDAP?

R. Les paramètres LDAP ajoutent des octets supplémentaires (résultats de recherche LDAP) lors du traitement des messages de type Search-Res-Entry. LDAP joint 10 octets de résultats de recherche à chaque paquet de réponse LDAP. Dans le cas où ces 10 octets de données supplémentaires entraînent un dépassement de l'unité de transmission maximale (MTU) dans un réseau, le paquet est abandonné. Dans ce cas, Cisco recommande que vous désactiviez ce comportement LDAP en utilisant la commande CLI no ip nat service append-ldap-search-res afin que les paquets soient envoyés et reçus.

Q. Quelle est la recommandation de routage pour l’adresse IP globale interne ou externe sur le boîtier NAT?

R. Une route doit être spécifiée dans la zone de configuration de la NAT pour l’adresse IP globale interne pour les fonctionnalités telles que la 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 d’un sens d’entrée vers un sens de sortie utilisant la règle statique externe nécessite ce type de route. Dans de tels scénarios, tout en fournissant la route pour IG/OL, l'adresse IP du tronçon suivant doit également être configurée. Si la configuration du tronçon suivant est manquante, cela est considéré comme une erreur de configuration et entraîne un comportement indéfini.

La fonction NVI-NAT est présente uniquement dans le chemin de la fonction de sortie. Si vous avez connecté directement un sous-réseau avec NAT-NVI ou la règle de traduction NAT externe configurée sur le boîtier, alors dans ces scénarios, vous devez fournir une adresse IP de tronçon suivant factice et également un ARP associé pour le tronçon suivant. Ceci est nécessaire pour que l'infrastructure sous-jacente transmette le paquet à la 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 Cisco IOS pour la traduction dynamique d’adresses réseau, une liste d’accès est utilisée pour identifier les paquets qui peuvent être traduits. L'architecture NAT actuelle ne prend pas en charge les listes de contrôle d'accès avec un mot clé log.

Voix-NAT

La NAT prend-elle en charge la version 17 du protocole « Skinny Client Control » (SCCP) qui est livrée avec la version 7 de Cisco Unified Communications Manager (CUCM)?

R. CUCM 7 et toutes les installations par défaut de CUCM 7 pour les téléphones supportent la version 17 du SCCP. La version de SCCP utilisée est déterminée par la version commune la plus élevée entre CUCM et le téléphone lorsque le téléphone s’inscrit.

Au moment de la création de ce document, 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 antérieure afin que SCCP v16 soit négocié. CUCM6 ne rencontre pas de problème NAT avec une charge de téléphone tant qu'il utilise SCCP v16. Cisco IOS ne prend pas actuellement en charge SCCP version 17.

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

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

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

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

Q. Qu’est-ce que l’amélioration de l’attribution des ports PAT aux fournisseurs de services pour RTP et RTCP?

A. La fonctionnalité d’amélioration de l’allocation des ports PAT du fournisseur de services pour RTP et RTCP garantit cela pour les appels vocaux SIP, H.323 et SCCP. Les numéros de port utilisés pour les flux RTP sont des numéros de port pairs, et les flux RTCP sont le numéro de port impair suivant. Le numéro de port est traduit en un numéro compris dans la plage spécifiée conformément à la RFC-1889. Un appel avec un numéro de port compris dans la plage entraîne 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 n'aboutit pas à une traduction vers un numéro dans la plage donnée.

Q. Qu’est-ce que le protocole d’ouverture de session (Session Initiation Protocol), et les paquets SIP peuvent-ils faire l’objet d’une NAT?

R. Le protocole SIP est un protocole de contrôle de couche d’application basé sur ASCII qui peut être utilisé pour établir, maintenir et terminer des appels entre deux ou plusieurs points d’accès. SIP est un protocole alternatif développé par l'IETF (Internet Engineering Task Force) pour les conférences multimédia sur IP. La mise en oeuvre du SIP de Cisco permet aux plates-formes Cisco prises en charge de signaler la configuration des appels vocaux et multimédia sur les réseaux IP.

Les paquets SIP peuvent être traités par NAT.

Q. Qu’est-ce que la prise en charge de la fonctionnalité de traversée NAT hébergée Cisco IOS 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 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 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 lorsque vous utilisez une configuration de surcharge NAT dans un déploiement vocal?

R. Oui. Lorsque vous avez des configurations de surcharge NAT et un déploiement vocal, vous avez besoin du message d'enregistrement pour passer par NAT et créer une association pour out->in pour atteindre 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 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 un déploiement vocal.

Q. La 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 de colocalisation : 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 prend-il en charge la traduction d’adresses réseau (NAT) pour le même espace d’adressage dans un VRF en même temps que la traduction d’adresses réseau (NAT) dans un espace d’adressage global ? Actuellement, je reçois cet avertissement : "% similar static entry (10.1.1.1 —> 10.210.2.2) already existing" lorsque j'essaie de configurer ceci :

<#root>

```
72UUT(config)#

ip nat inside source static 10.1.1.1 10.210.2.2


72UUT(config)#

ip nat inside source static 10.1.1.1 10.210.2.2 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 configurer 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 VRF qui se chevauchent pour différents VRF. Cependant, il n'est pas possible de chevaucher les adresses NAT globales et VRF.

<#root>

```
72UUT(config)#

ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED match-in-vrf

72UUT(config)#
```

```
ip nat inside source static 10.1.1.1 10.210.2.2 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 la NAT NVI?

R. NVI signifie NAT Virtual Interface. Elle permet à la NAT de traduire entre deux VRF différents. 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 lors de la traduction NAT entre une interface globale et une interface dans un VRF ?

R. Cisco vous recommande d'utiliser la NAT héritée pour VRF vers la NAT globale (ip nat inside/out) et entre les interfaces dans le même VRF. NVI est utilisé pour la 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, les protocoles UDP SIP

et DNS sont pris en charge.

NAT par états (SNAT)

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

R. 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 nécessitant la traduction des informations d'adresse IP. En outre, il informe le convertisseur de sauvegarde des flux actifs lorsqu'ils se produisent. Le traducteur de sauvegarde peut ensuite utiliser les informations du traducteur actif pour préparer des entrées de table de traduction en double. Par conséquent, si le traducteur actif est entravé par une défaillance critique, le trafic peut rapidement être commuté vers la sauvegarde. Le flux de trafic se poursuit car les mêmes traductions d’adresses réseau sont utilisées et l’état de ces traductions a été défini au préalable.

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, les protocoles UDP SIP et DNS sont pris en charge.

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

R. Le routage asymétrique prend en charge NAT en activant comme mise en file d’attente. Par défaut, as-queueing est activé. Cependant, à partir de la version 12.4(24)T, la mise en file d'attente en tant que n'est plus prise en charge. Les clients doivent s'assurer que les paquets sont acheminés correctement et qu'un délai approprié est ajouté afin que le routage asymétrique fonctionne correctement.

NAT-PT (v6 à v4)

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

R. La traduction de protocoles permet à la NAT de passer d’IPv4 à IPv6. La traduction de protocole (NAT-PT) est un mécanisme de traduction IPv6-IPv4, tel que défini dans les RFC 2765 et RFC 2766, permettant aux périphériques IPv6 uniquement de communiquer avec des périphériques IPv4 uniquement et vice versa.

La NAT-PT est-elle prise en charge dans le chemin CEF (Cisco Express Forwarding)?

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

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

R. La NAT-PT prend en charge le TFTP/FTP et le DNS. NAT-PT ne prend pas en charge la voix et SNAT.

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

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

Cisco 7300/7600/6k 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 NAT compatible avec les VRF est-elle prise en charge dans le matériel sur le 6k?

R. Le matériel de cette plate-forme n’est pas compatible avec la NAT pour VRF.

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

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

Remarque : Vous pouvez mettre en oeuvre une conception en exploitant un FWSM qui s'exécute en mode transparent de contexte virtuel.

Cisco 850 dépendant de la plate-forme

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 NAT

Q. Comment mettre en œuvre la NAT?

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

Q. Comment mettre en œuvre la NAT avec voix?

R. La prise en charge de la NAT pour la fonction vocale permet de retraduire les messages SIP intégrés qui passent par un routeur configuré avec la NAT en paquet. Une passerelle de couche application (ALG) est utilisée avec NAT pour traduire les paquets vocaux.

Q. Comment intégrer la NAT aux VPN MPLS?

R. La fonctionnalité d’intégration de la NAT avec les VPN MPLS permet de configurer plusieurs VPN MPLS sur un seul appareil pour qu’ils fonctionnent ensemble. La NAT peut différencier le VPN MPLS duquel elle reçoit le trafic IP même si les VPN MPLS utilisent tous le même schéma 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. La disponibilité élevée dans le protocole HSRP est-elle prise en charge par une NAT statique?

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

appartenir à un groupe.

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

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

Q. Comment mettre en œuvre l'équilibrage de charge avec la NAT?

R. Il existe deux types d'équilibrage de charge qui peuvent être effectués avec la NAT. vous pouvez équilibrer la charge entrante vers un ensemble de serveurs pour répartir la charge sur les serveurs, et vous pouvez équilibrer la charge du trafic utilisateur vers Internet sur deux FAI ou plus.

Pour plus d'informations sur l'équilibrage de charge sortante, 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 une prise en charge de la sécurité IP (IPSec) Encapsulation de la charge utile de sécurité (ESP) par NAT et IPSec NAT Transparency.

La fonctionnalité IPSec ESP via NAT permet de prendre en charge plusieurs tunnels ou connexions IPSec ESP simultanés via un périphérique NAT Cisco IOS configuré en mode de surcharge ou de traduction d'adresses de port (PAT).

La fonction de transparence NAT IPSec prend en charge le trafic IPSec qui traverse les points NAT ou PAT du réseau en corrigeant de nombreuses incompatibilités connues entre NAT et IPSec.

Q. Comment mettre en œuvre la NAT-PT?

R. 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 mettre en œuvre la NAT de multidiffusion?

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

Pour plus d'informations, référez-vous à Comment fonctionne la NAT multidiffusion sur les routeurs Cisco. Le groupe de multidiffusion de destination est traité par NAT à l'aide d'une solution de réflexion de service multidiffusion.

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

R. La SNAT active un service continu pour les sessions NAT mappées dynamiquement. Les sessions définies de manière statique bénéficient de la redondance sans SNAT. En l'absence de SNAT, les sessions qui utilisent des mappages NAT dynamiques seraient interrompues en cas de défaillance critique et devraient être rétablies. Seule la configuration SNAT minimale est prise en charge. Les déploiements futurs doivent être effectués uniquement après avoir contacté 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 manquantes par rapport à HSRP.
- Pour les scénarios de basculement et la configuration à deux routeurs. Autrement dit, si un routeur tombe en panne, l’autre prend le relais de manière transparente. (L'architecture SNAT n'est pas conçue pour gérer les décharges d'interface.)
- Le scénario de routage non asymétrique est pris en charge. Le routage asymétrique ne peut être géré que si la latence dans le paquet de réponse est supérieure à celle entre deux routeurs SNAT pour échanger les messages SNAT.

Actuellement, l'architecture SNAT n'est pas conçue pour gérer la robustesse ; par conséquent, ces tests ne sont pas censés réussir :

- Effacement des entrées NAT en présence de trafic.
- Modification des paramètres d’interface (par exemple, changement d’adresse IP, arrêt/non-arrêt, etc.) en présence de trafic.
- Les commandes clear ou show spécifiques à SNAT ne sont pas censées s'exécuter correctement et ne sont pas recommandées.

Voici quelques-unes des commandes clear< /strong> et show associées à SNAT :

<#root>

```
clear ip snat sessions *
```

```
clear ip snat sessions <ip address of the peer>
```

```
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 forced< /strong> ou clear 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 stats peuvent être utilisées. Si service internal est configuré, il affiche également des informations spécifiques à SNAT.

Il n'est pas recommandé d'effacer les traductions NAT sur le routeur de secours. Effacez toujours les entrées NAT sur le routeur SNAT principal.

SNAT n'est pas HA ; 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 de meilleures pratiques en matière de NAT?

R. Oui. Voici les meilleures pratiques NAT :

- Lors de l’utilisation de 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 d'éviter tout chevauchement.

- Méfiez-vous de l'utilisation de la liste de contrôle d'accès pour NAT avec permit ip any any car vous pouvez obtenir des résultats imprévisibles. Après 12.4(20)T, la NAT traduit les paquets HSRP et de protocole de routage générés localement s'ils sont envoyés par l'interface externe, ainsi que les paquets chiffrés localement correspondant à la règle NAT.
- Lorsque vous avez des réseaux qui 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 VRF qui se chevauchent pour différents VRF, mais il n'est pas possible de chevaucher les adresses NAT globales et VRF.

<#root>

```
Router(config)#

ip nat inside source static 10.1.1.1 10.210.2.2 vrf RED match-in-vrf
```

<#root>

```
Router(config)#

ip nat inside source static 10.1.1.1 10.210.2.2 vrf BLUE match-in-vrf
```

Les 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 :

<#root>

```
  ip nat pool poolA 1710.1.1.1 1710.1.1.10 prefix-length 24

  ip nat pool poolB 1710.1.1.1 1710.1.1.10 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
```

Remarque : Même si la configuration de l’interface de ligne de commande est valide, sans le mot-clé match-in-vrf, la configuration n’est pas prise en charge.

- Lors du déploiement de 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.
- 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.
- Lors du déploiement des mêmes règles NAT sur deux routeurs différents dans le scénario de basculement, vous devez utiliser la redondance HSRP.
- 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 technique de Cisco et téléchargements

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.