

Prise en charge de la NAT sur plusieurs pools à l'aide de cartes de routage

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Approche de liste d'accès](#)

[Hôte 1 pour héberger 2](#)

[Hôte 1 à Lhôte3](#)

[Approche de mappage de route](#)

[Hôte 1 pour héberger 2](#)

[Hôte 1 à Lhôte3](#)

[Informations connexes](#)

[Introduction](#)

Ce document explique comment l'utilisation des listes d'accès versus les mappages de route change la fonctionnalité de la traduction d'adresses de réseau (NAT). Pour plus d'informations sur NAT, référez-vous au [Cisco IOS NAT](#).

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeurs de la gamme Cisco 2500.
- Version de logiciel 12.3(3) de Cisco IOS®.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

Seulement Listes d'accès NAT et mappages de route d'utilisations quand il doit créer une entrée de traduction. Si une entrée de traduction existe déjà qu'apparie le trafic puis l'entrée de traduction sera utilisée ; aucunes Listes d'accès ou mappage de route ne seront consultés. La différence entre utiliser une liste d'accès ou un mappage de route est le type d'entrée de traduction qui sera créé.

Mise en correspondance de route

Si NAT emploie un mappage de route pour décider de créer une entrée de traduction, il créera toujours « a entièrement étendu » l'entrée de traduction. Cette entrée de traduction contiendra chacun des deux les entrées (locales et globales) d'adresse d'intérieur et d'extérieur et n'importe quel TCP ou informations de port UDP. Référez-vous à [NAT : Gens du pays et définitions globales](#) pour plus d'informations sur des adresses (locales et globales) d'intérieur et d'extérieur.

Listes d'accès (aucune surcharge)

Si NAT emploie une liste d'accès pour décider de créer une entrée de traduction, il créera une entrée « simple » de traduction. Cette entrée « simple » contiendra seulement les entrées locales et globales d'adresse IP pour juste l'intérieur ou l'extérieur selon si l'**ip nat intérieur** ou la commande d'**ip nat outside** est configuré. En outre, il n'inclura aucun TCP ou informations de port UDP.

Listes d'accès (avec la surcharge)

Si NAT utilise une liste d'accès, et la surcharge a été également spécifiée, NAT créera une entrée « entièrement étendue » de traduction. (Voir le [Note1](#)). L'exécution est semblable dans la caisse de route-map sauf que le route-map a quelques fonctionnalités supplémentaires. Voir la [note 2](#) pour plus de détails. Vous pouvez voir un exemple d'une entrée simple dans la table de traduction NAT et entièrement d'une entrée de traduction NAT étendue en sélectionnant un de ces liens :

- [Entrée simple dans la table de traduction NAT](#)
- [Entièrement entrée de traduction NAT étendue](#)

C'est un exemple de diagramme de réseau utilisé pour illustrer la différence entre utiliser un mappage de route et une liste d'accès avec NAT :

Dans cet exemple de diagramme de réseau, on l'exige que des hôtes sur 10.1.1.0 soient traduits à ce qui suit :

- 131.108.2.0 en allant à 131.108.1.0
- 131.118.2.0 en allant à 131.118.1.0

Approche de liste d'accès

Avec une approche de liste d'accès, vous feriez le suivant pour traduire les hôtes sur 10.1.1.0 :

```
ip nat pool pool108 131.108.2.1 131.108.2.254 prefix-length 24
!--- Defines a pool of global addresses to be allocated as needed. ip nat pool pool118
131.118.2.1 131.118.2.254 prefix-length 24 ip nat inside source list 108 pool pool108 !---
Establishes dynamic source translation, specifying the !--- access list defined below. ip nat
inside source list 118 pool pool118 interface ethernet0 ip address 10.1.1.1 255.255.255.0 ip nat
inside !--- Marks the interface as connected to the inside. interface ethernet1 ip address
10.1.2.1 255.255.255.0 ip nat outside !--- Marks the interface as connected to the outside.
access-list 108 permit ip 10.1.1.0 0.0.0.255 131.108.1.0 0.0.0.255 !--- Defines the access-list
mentioning those addresses !--- that are to be translated. access-list 118 permit ip 10.1.1.0
0.0.0.255 131.118.1.0 0.0.0.255
```

Référez-vous à [l'adressage IP et entretenez des commandes](#) pour plus d'informations sur ces commandes.

Hôte 1 pour héberger 2

Voici ce qui s'avère justement quand des telnets de l'hôte 1 héberger 2.

```
Packet on (Network 1) s:10.1.1.2(1024) d:131.108.1.2(23)
Packet on (Network 2) s:131.108.2.1(1024) d:131.108.1.2(23) (after NAT)
```

Puisqu'une liste d'accès a été utilisée par NAT pour appairier ce trafic une entrée de traduction simple est créée, qui n'inclut seulement les informations privilégiées de traduction et aucun protocole ou informations de port :

inside		outside	
local	global	global	local
10.1.1.2	131.108.2.1	----	----

Renvoyez le paquet : Hôte 2 pour héberger 1 :

```
Packet on (Network 2) s:131.108.1.2(23) d:131.108.2.1(1024)
Packet on (Network 1) s:131.108.1.2(23) d:10.1.1.2(1024) (after NAT)
```

Hôte 1 à Lhôte3

Avec la traduction simple ci-dessus en place, voici ce qui se produit quand des telnets de l'hôte 1 aussi à Lhôte3 :

```
Packet on (Network 1) s:10.1.1.2(1025) d:131.118.1.2(23)
Packet on (Network 2) s:131.108.2.1(1025) d:131.118.1.2(23) (after NAT)
```

Vous pouvez voir qu'il y a un problème. Les paquets allant des hôtes de 10.1.1.0 aux hôtes de 131.118.1.0 devraient obtenir traduit dans 131.118.2.0, **pas** 131.108.2.0. La raison pour laquelle ceci se produit est parce qu'il y a déjà une entrée de traduction NAT pour 10.1.1.2 <--> 131.108.2.1 qui apparie également le trafic entre l'hôte 1 et Lhôte3. Par conséquent, cette entrée de traduction sera utilisée et les Listes d'accès 108 et 118 ne sont pas vérifiées.

Tandis que l'entrée de traduction simple est en place dans la table de traduction NAT, elle peut être utilisée par **n'importe quel** utilisateur externe sur n'importe quel hôte d'extérieur pour envoyer un paquet pour héberger 1 tant que l'utilisateur externe utilise l'adresse globale interne (131.108.2.1) pour l'hôte 1. normalement qu'une traduction NAT statique est nécessaire pour permettre ceci.

Approche de mappage de route

La manière correcte de configurer l'exemple dans ce document est d'utiliser des mappages de

route. Avec une approche de mappage de route, vous feriez le suivant pour traduire les hôtes sur 10.1.1.0 :

```
ip nat pool pool-108 131.108.2.1 131.108.2.254 prefix-length 24
ip nat pool pool-118 131.118.2.1 131.118.2.254 prefix-length 24

ip nat inside source route-map MAP-108 pool pool-108
!--- Establishes dynamic source translation, specifying !--- the route-map MAP-108 which is
defined below. ip nat inside source route-map MAP-118 pool pool-118 !--- Establishes dynamic
source translation, specifying the route-map MAP-118. !--- Here, the route-maps are consulted
instead of !--- access-lists (as in the previous case). interface ethernet0 ip address 10.1.1.1
255.255.255.0 ip nat inside interface ethernet1 ip address 10.1.2.1 255.255.255.0 ip nat outside
access-list 108 permit ip 10.1.1.0 0.0.0.255 131.108.1.0 0.0.0.255 access-list 118 permit ip
10.1.1.0 0.0.0.255 131.118.1.0 0.0.0.255 route-map MAP-108 permit 10 !--- Defines the Route-map
MAP-108. match ip address 108 !--- Specifies the criteria for translation. Here, the IP !---
address mentioned in the access-list 108 is translated. !--- The translation is defined in the
!--- ip nat inside source route-map MAP-108 pool pool-108 command. route-map MAP-118 permit 10
!--- Defines the Route-map MAP-108. match ip address 118 !--- The IP address mentioned in the
access-list 118 is translated. !--- The translation is defined in the !--- ip nat inside source
route-map MAP-118 pool pool-118 command.
```

Référez-vous à l'[adressage IP et entretenez des commandes](#) pour plus d'informations sur ces commandes.

Hôte 1 pour héberger 2

Voici ce qui se produit quand des telnets de l'hôte 1 pour héberger 2 :

```
Packet on (Network 1) s:10.1.1.2(1024) d:131.108.1.2(23)
Packet on (Network 2) s:131.108.2.1(1024) d:131.108.1.2(23) (after NAT)
```

Dans ce cas, parce qu'un mappage de route a été utilisé par NAT pour appairer le trafic à traduire, NAT créera entièrement une entrée de traduction étendue, qui inclut à l'intérieur et à l'extérieur des informations de traduction :

inside		outside		
local	global	global	local	
10.1.1.2:1024	131.108.2.1:1024	131.108.1.2:23	131.108.1.2:23	

Renvoyez le paquet : Hôte 2 pour héberger 1 :

```
Packet on (Network 2) s:131.108.1.2(23) d:131.108.2.1(1024)
Packet on (Network 1) s:131.108.1.2(23) d:10.1.1.2(1024) (after NAT)
```

Hôte 1 à Lhôte3

Maintenant où l'hôte 1 envoie un paquet à Lhôte3, c'est ce qui apparaît :

```
Packet on (Network 1) s:10.1.1.2(1025) d:131.118.1.2(23)
Packet on (Network 2) s:131.118.2.1(1025) d:131.118.1.2(23) (after NAT)
```

La traduction a fonctionné correctement parce que le paquet en fonction (N1) n'apparie pas entièrement l'entrée de traduction étendue qui a été utilisée pour l'hôte 1 pour héberger le trafic 2. Puisque la traduction existante ne s'assortit pas, NAT crée une autre entrée de traduction pour l'hôte 1 Lhôte3 pour trafiquer.

Ce sont entièrement les entrées de traduction étendue sur le routeur NAT :

inside		outside		
local	global	global	local	
10.1.1.2:1024	131.108.2.1:1024	131.108.1.2:23	131.108.1.2:23	

10.1.1.2:1025 131.118.2.1:1025 131.118.1.2:23 131.118.1.2:23

Puisque la table de traduction NAT a deux pleines entrées, elle traduira correctement le trafic allant aux deux destinations différentes de la même source.

À la différence de l'entrée de traduction simple qui a été créée par l'intermédiaire de la liste d'accès, entièrement l'entrée de traduction étendue créée par l'intermédiaire du mappage de route ne peut pas n'être utilisée par aucun autre utilisateur externe pour envoyer un paquet pour héberger 1. Une traduction NAT statique est nécessaire pour permettre ceci.

[Note 1](#)

Dans le cas de la liste d'accès avec la surcharge, la configuration est semblable à la liste d'accès sans cas de surcharge. L'exception est que vous devez ajouter la **surcharge de mot clé** au **groupe pool108 de la liste 108 d'ip nat inside source de commande** et au **groupe pool118 de la liste 118 d'ip nat inside source**.

[Note 2](#)

L'avantage d'utiliser des route-map est celui sous la **commande match** que vous pouvez avoir plus d'options autres que l'adresse IP source. Par exemple, sous le route-map, le **match interface** ou le **match ip next-hop** peut être spécifié. À l'aide des route-map, vous pouvez spécifier l'adresse IP aussi bien que l'interface ou l'adresse du prochain saut auxquelles le paquet doit être expédié. Par conséquent, des route-map avec NAT sont utilisés dans un scénario où l'abonné est multihébergement aux autres FAI.

[Informations connexes](#)

- [NAT — Capacité d'utiliser des mappages de route avec les traductions statiques](#)
- [Traduction d'adresses réseau Cisco IOS](#)
- [Configurer la traduction d'adresses réseau](#)
- [NAT : Définitions locales et globales](#)
- [Référence de commandes IP de Cisco IOS pour l'adressage et les services, version 12.3](#)
- [Support et documentation techniques - Cisco Systems](#)