Configurer la traduction d’adresse réseau

Table des matières

Introduction

Ce document décrit comment configurer la traduction d’adresses réseau (NAT) sur un routeur Cisco.

Conditions préalables

Exigences

Ce document exige une connaissance de base des termes utilisés en relation avec NAT.

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

- Cisco IOS® Version du logiciel 12.2(10b)

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

Conventions

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

Étapes de démarrage rapide pour configurer et déployer la fonction NAT

Remarque : dans ce document, lorsqu'on parle d'Internet ou d'un périphérique Internet, il s'agit d'un périphérique situé sur n'importe quel réseau externe.

Quand vous configurez NAT, il est parfois difficile de savoir où commencer, particulièrement si vous débutez avec NAT. Ces étapes vous guident pour définir ce que vous voulez que NAT fasse et comment le configurer :

1. Définissez les interfaces internes et externes de NAT.
    - Les utilisateurs existent-ils outre plusieurs interfaces ?
    - Internet dispose-t-il de plusieurs interfaces ?
2. Définissez ce que vous voulez accomplir avec la fonction NAT.
    - Voulez-vous autoriser les utilisateurs internes à accéder à Internet ?
    - Voulez-vous autoriser Internet à accéder aux périphériques internes (tels qu'un serveur de messagerie ou un serveur Web) ?
    - Voulez-vous rediriger le trafic TCP vers un autre port ou une autre adresse TCP ?
    - Voulez-vous utiliser la NAT pendant une transition réseau (par exemple, vous avez modifié une adresse IP de serveur et jusqu'à ce que vous puissiez mettre à jour tous les clients que vous voulez que les clients non mis à jour puissent accéder au serveur avec l'adresse IP d'origine et permettre aux clients mis à jour d'accéder au serveur avec la nouvelle adresse) ?
    - Voulez-vous utiliser pour autoriser les réseaux qui se chevauchent à communiquer ?
3. Configurez la NAT afin d'accomplir ce que vous avez défini précédemment. En fonction de ce que vous avez défini à l'étape 2, vous devez déterminer les fonctionnalités suivantes à utiliser :

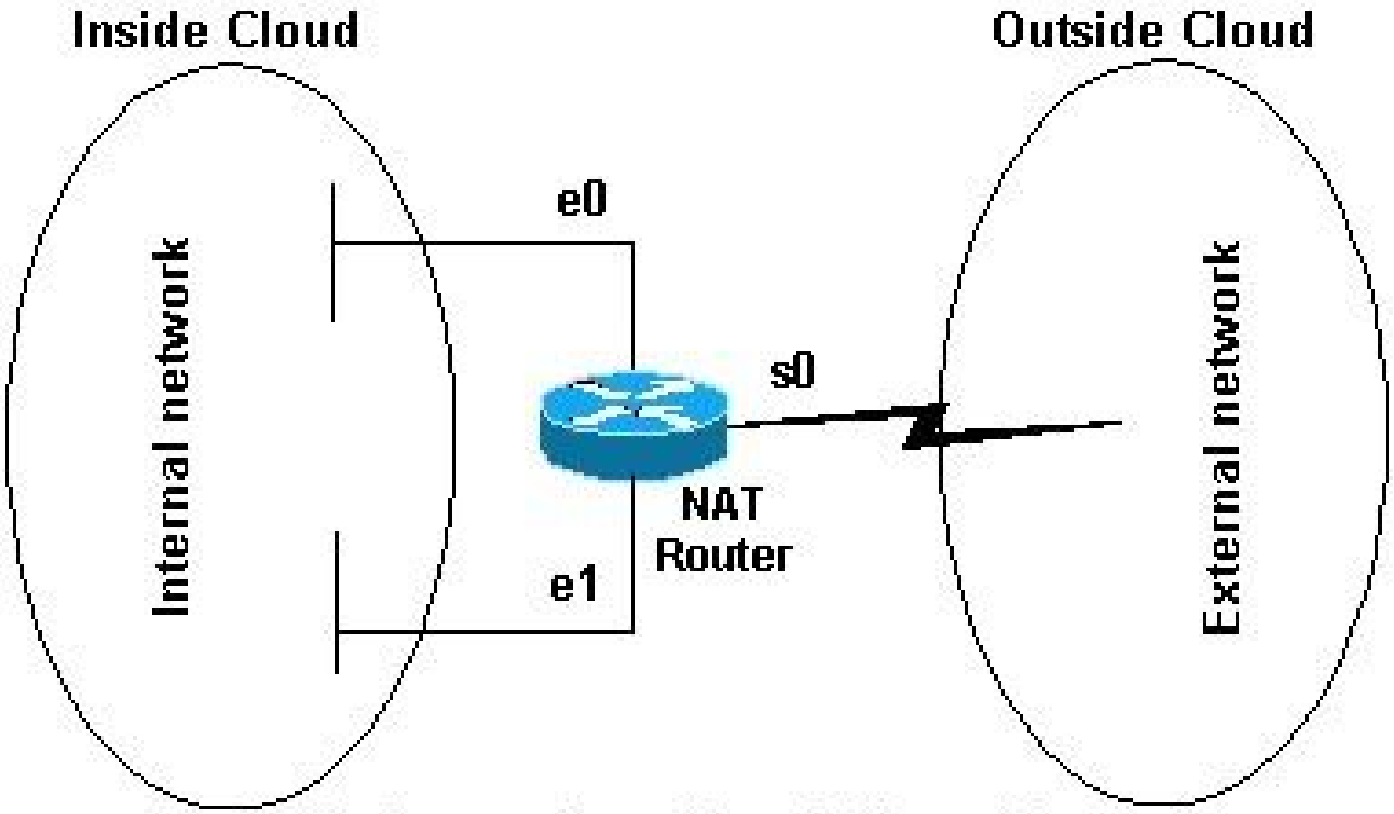
- NAT statique
- NAT dynamique
- Overloading
- Toute combinaison de ces fonctionnalités.

4. Vérifiez l'opération de NAT .

Chacun de ces exemples NAT vous guide tout au long des étapes 1 à 3 des étapes de démarrage rapide de l'image précédente. Ces exemples décrivent quelques scénarios communs dans lesquels Cisco vous recommande de déployer NAT.

Définition des interfaces NAT internes et externes

La première étape du déploiement de la fonction NAT consiste à définir les interfaces NAT internes et externes. Il est plus facile de définir votre réseau interne comme interne et le réseau externe comme externe. Cependant, les termes internes et externes sont également sujets à arbitrage. La figure ci-contre en est un exemple.



In this figure, ethernet 0 and ethernet 1 will be defined as NAT inside interfaces and serial 0 will be defined as a NAT outside interface.

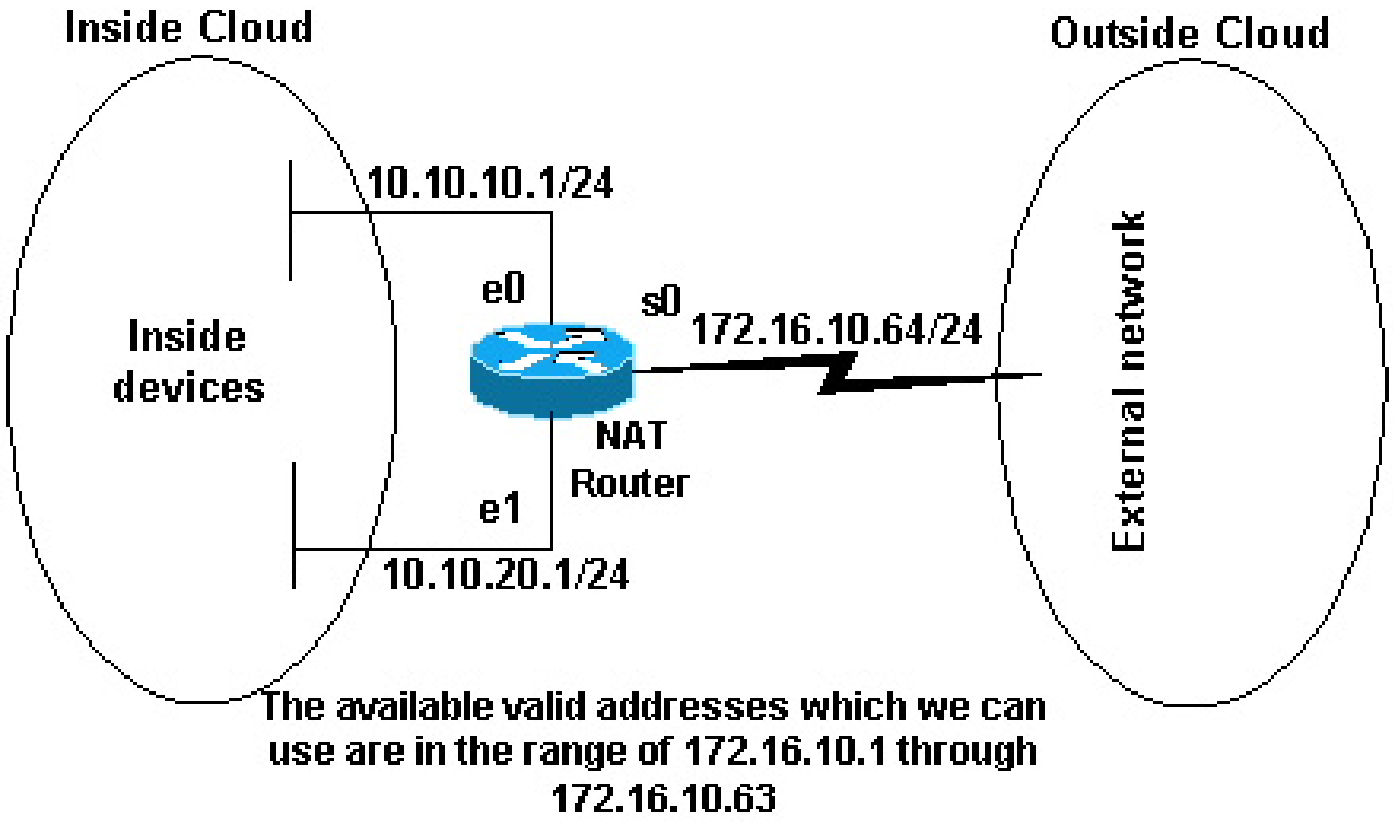
Topologie NAT

Exemples

1. Autoriser les utilisateurs internes à accéder à Internet

Il est possible que vous souhaitiez autoriser les utilisateurs internes à accéder à Internet, mais vous ne disposez pas d'adresses valides suffisantes pour accueillir tout le monde. Si toutes les communications avec les périphériques sur Internet proviennent des périphériques internes, vous avez besoin d'une adresse valide unique ou d'un pool d'adresses valides.

Cette image présente un schéma de réseau simple avec les interfaces de routeur définies comme interne et externe.



Adresses valides disponibles

Dans cet exemple, vous voulez que la fonction NAT autorise certains périphériques (les 31 premiers de chaque sous-réseau) à l'intérieur à établir une communication avec des périphériques à l'extérieur et à traduire leur adresse non valide en une adresse ou un pool d'adresses valide. Le groupe a été défini tel que la plage d'adresses 172.16.10.1 par 172.16.10.63.

Vous pouvez maintenant configurer NAT. Afin d'accomplir ce qui est défini dans l'image précédente, utilisez la NAT dynamique. Avec NAT dynamique, la table de traduction dans le routeur est initialement vide et devient peuplée une fois que le trafic qui doit être traduit passe par le routeur. Contrairement à la NAT statique, où une traduction est configurée de manière statique

et est placée dans la table de traduction sans nécessiter de trafic.

Dans cet exemple, vous pouvez configurer NAT pour traduire chacun des périphériques internes en une adresse valide unique, ou pour traduire chacun des périphériques internes en la même adresse valide. Cette seconde méthode est appelée overloading . Un exemple de configuration de chaque méthode est donné ici.

Configurer NAT pour autoriser les utilisateurs internes à accéder à Internet

Routeur NAT

```
interface ethernet 0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.


interface ethernet 1
 ip address 10.10.20.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.


interface serial 0
 ip address 172.16.10.64 255.255.255.0
 ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.


ip nat pool no-overload 172.16.10.1 172.16.10.63 prefix 24


!--- Defines a NAT pool named no-overload with a range of addresses
!--- 172.16.10.1 - 172.16.10.63.


ip nat inside source list 7 pool no-overload


!--- Indicates that any packets received on the inside interface that
!--- are permitted by access-list 7 has
!--- the source address translated to an address out of the
!--- NAT pool "no-overload".


access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Access-list 7 permits packets with source addresses ranging from
!--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

Remarque : Cisco recommande vivement de ne pas configurer les listes d'accès référencées par les commandes NAT avec permit any. Si vous utilisez permit any dans NAT, il consomme trop de ressources de routeur qui peuvent causer des problèmes de réseau.

Notez que dans la configuration précédente, seules les 32 premières adresses du sous-réseau 10.10.10.0 et les 32 premières adresses du sous-réseau 10.10.20.0 sont autorisées par la liste d'accès 7. Par conséquent, seulement ces adresses sources sont traduites. Il peut y avoir d'autres périphériques avec d'autres adresses sur le réseau interne, mais ceux-ci ne sont pas traduits.

La dernière étape consiste à vérifier que la fonction NAT fonctionne comme prévu .

Configurer NAT pour permettre aux utilisateurs internes d'accéder à Internet avec surcharge

Routeur NAT

```
interface ethernet 0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.


interface ethernet 1
 ip address 10.10.20.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.


interface serial 0
 ip address 172.16.10.64 255.255.255.0
 ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.


ip nat pool ovrld 172.16.10.1 172.16.10.1 prefix 24


!--- Defines a NAT pool named ovrld with a range of a single IP
!--- address, 172.16.10.1.


ip nat inside source list 7 pool ovrld overload


!--- Indicates that any packets received on the inside interface that
!--- are permitted by access-list 7 has the source address
!--- translated to an address out of the NAT pool named ovrld.
!--- Translations are overloaded, which allows multiple inside
!--- devices to be translated to the same valid IP address.

access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Access-list 7 permits packets with source addresses ranging from
```

```
!--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

Notez que dans la deuxième configuration précédente, le pool ovrld NAT n'a qu'une plage d'une adresse. Le mot clé overload utilisé dans la commande ip nat inside source list 7 pool ovrld overload permet à NAT de traduire plusieurs périphériques internes en l'adresse unique dans le groupe.

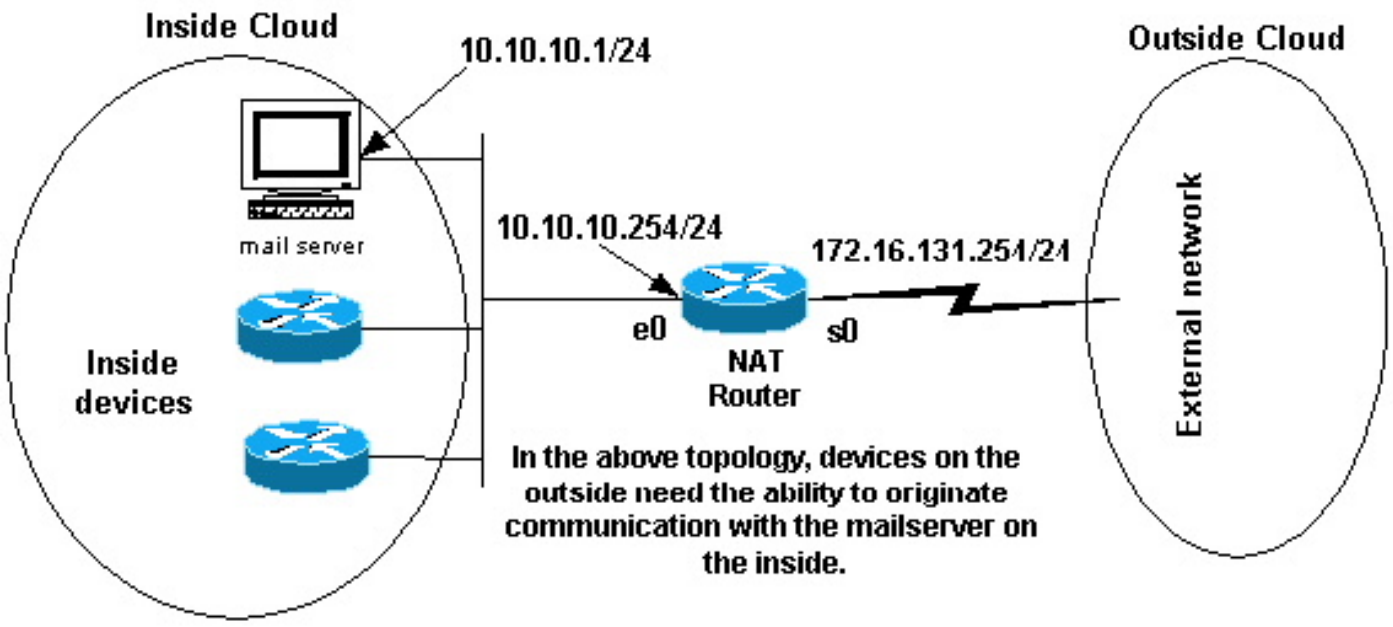
Une autre variante de cette commande isip nat inside source list 7 interface serial 0 overload, qui configure la NAT pour la surcharge sur l'adresse qui est assignée à l'interface Serial 0.

Lorsque overloading est configuré, le routeur conserve suffisamment d'informations provenant de protocoles de niveau supérieur (par exemple, les numéros de port TCP ou UDP) pour retraduire l'adresse globale en l'adresse locale correcte. Pour les définitions d'adresse globale et locale, référez-vous à NAT : Global and Local Definitions .

La dernière étape consiste à vérifier que la fonction NAT fonctionne comme prévu .

2. Autoriser Internet à accéder aux périphériques internes

Vous pouvez avoir besoin de périphériques internes pour échanger des informations avec des périphériques sur Internet, où la communication est initiée à partir des périphériques Internet, par exemple, le courrier électronique. Il est courant que des périphériques sur Internet envoient des e-mails à un serveur de messagerie qui réside sur le réseau interne.



Émettre des communications

Configurer la fonction NAT pour autoriser Internet à accéder aux périphériques internes

Dans cet exemple, vous devez d'abord définir les interfaces NAT internes et externes, comme

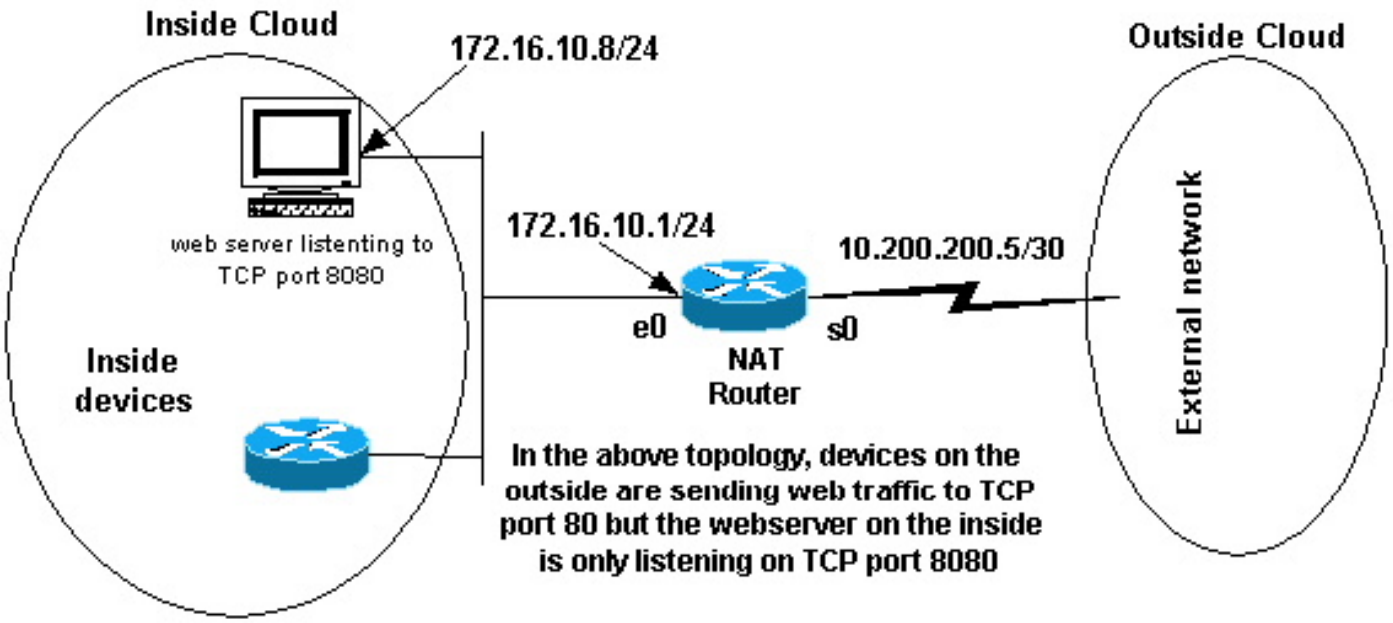
indiqué dans le schéma de réseau précédent.

Ensuite, vous définissez que vous voulez que les utilisateurs internes puissent établir une communication avec l'extérieur. Les périphériques externes doivent pouvoir établir une communication uniquement avec le serveur de messagerie interne.

La troisième étape est de configurer NAT. Pour accomplir ce que vous avez défini, vous pouvez configurer la NAT statique et la NAT dynamique ensemble. Pour plus d'informations sur la façon de configurer cet exemple, référez-vous à Configurer la NAT statique et dynamique simultanément . La dernière étape consiste à vérifier que la fonction NAT fonctionne comme prévu .

3. Rediriger le trafic TCP vers un autre port ou une autre adresse TCP

Un serveur Web sur le réseau interne est un autre exemple de cas où il peut être nécessaire pour des périphériques sur Internet d'initier une communication avec des périphériques internes. Dans certains cas, le serveur Web interne peut être configuré pour écouter le trafic Web sur un port TCP autre que le port 80. Par exemple, le serveur Web interne peut être configuré pour écouter le port TCP 8080. Dans ce cas, vous pouvez utiliser NAT pour rediriger le trafic destiné au port TCP 80 au port TCP 8080.



Port TCP du trafic Web

Après avoir défini les interfaces comme indiqué dans le schéma de réseau précédent, vous pouvez décider que vous voulez que la NAT redirige les paquets de l'extérieur destinés à 172.16.10.8:80 vers 172.16.10.8:8080. Vous pouvez utiliser une commande static nat afin de traduire le numéro de port TCP pour y parvenir. Un exemple de configuration est présenté ici.

Configurer NAT pour rediriger le trafic TCP vers un autre port ou une autre adresse TCP

Routeur NAT

```
interface ethernet 0
 ip address 172.16.10.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.


interface serial 0
 ip address 10.200.200.5 255.255.255.252
 ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.


ip nat inside source static tcp 172.16.10.8 8080 172.16.10.8 80

!--- Static NAT command that states any packet received in the inside
!--- interface with a source IP address of 172.16.10.8:8080 is
!--- translated to 172.16.10.8:80.
```

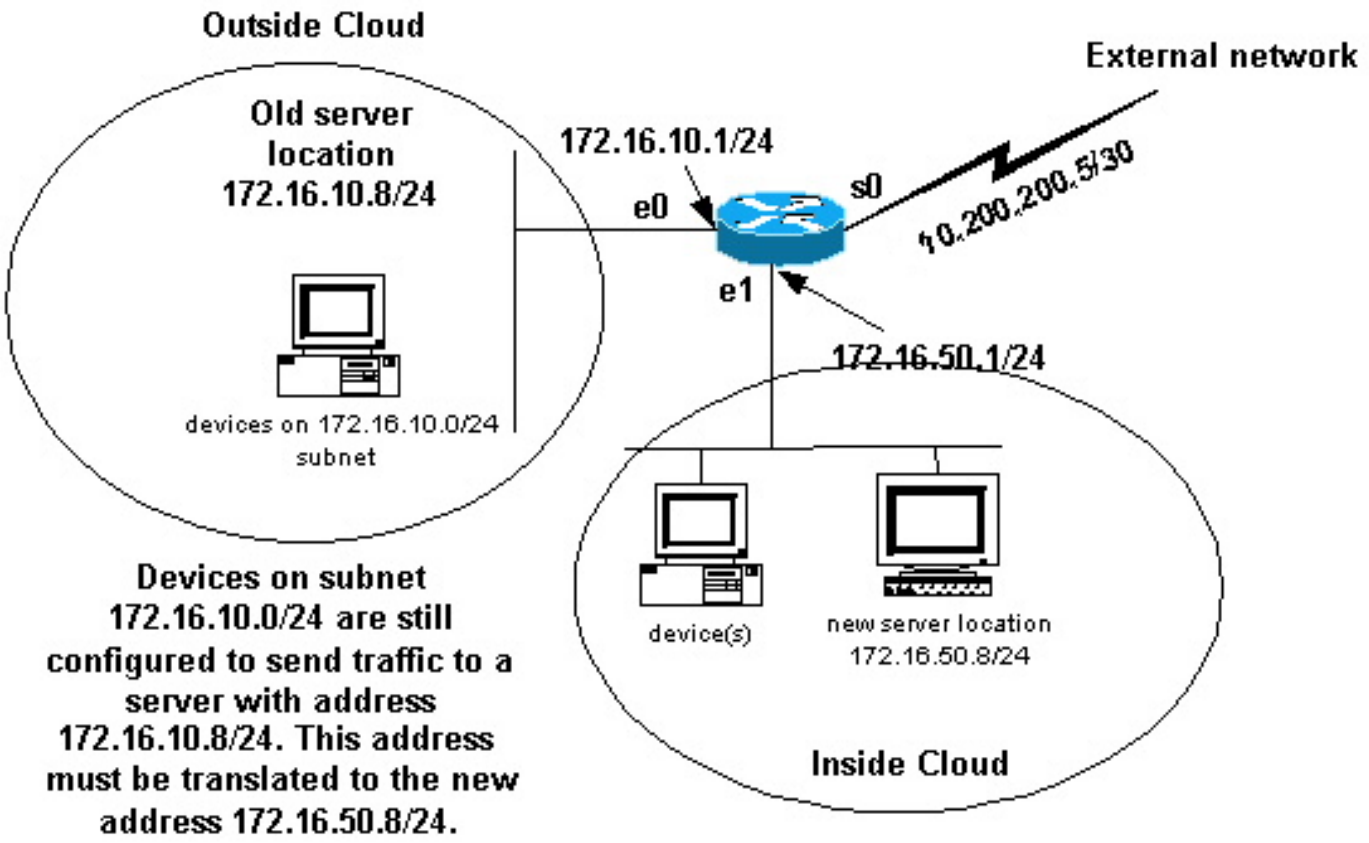
Remarque : la description de configuration de la commande NAT statique indique que tout paquet reçu dans l'interface interne avec l'adresse source 172.16.10.8:8080 est traduit en 172.16.10.8:80. Cela implique également que tout paquet reçu sur l'interface externe avec une adresse de destination de 172.16.10.8:80 a la destination traduite en 172.16.10.8:8080.

La dernière étape consiste à vérifier que la fonction NAT fonctionne comme prévu .

```
show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 172.16.10.8:80     172.16.10.8:8080   ---                ---
```

4. Utiliser la fonction NAT pour une transition de réseau

La fonction NAT est utile lorsque vous devez réadresser des périphériques sur le réseau ou lorsque vous remplacez un périphérique par un autre. Par exemple, si tous les périphériques du réseau utilisent un serveur particulier et que ce serveur doit être remplacé par un nouveau qui a une nouvelle adresse IP, la reconfiguration de tous les périphériques réseau pour utiliser la nouvelle adresse du serveur prend un certain temps. En attendant, vous pouvez utiliser la NAT afin de configurer les périphériques avec l'ancienne adresse pour traduire leurs paquets pour communiquer avec le nouveau serveur.



Transition du réseau NAT

Une fois que vous avez défini les interfaces NAT comme l'illustre l'image précédente, vous pouvez décider que vous voulez que NAT autorise les paquets de l'extérieur destinés à l'ancienne adresse de serveur (172.16.10.8) à être traduits et envoyés à la nouvelle adresse de serveur. Notez que le nouveau serveur se trouve sur un autre réseau local et que les périphériques de ce réseau local ou tout périphérique accessible via ce réseau local (périphériques situés à l'intérieur du réseau) doivent être configurés pour utiliser la nouvelle adresse IP du serveur si possible.

Vous pouvez utiliser NAT statique pour effectuer ce dont vous avez besoin. Ceci est un exemple de configuration.

Configuration de la NAT pour une utilisation via une transition réseau

Routeur NAT

```
interface ethernet 0
 ip address 172.16.10.1 255.255.255.0
 ip nat outside

!--- Defines Ethernet 0 with an IP address and as a NAT outside interface.


interface ethernet 1
 ip address 172.16.50.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.
```

```
interface serial 0
 ip address 10.200.200.5 255.255.255.252

!--- Defines serial 0 with an IP address. This interface is not
!--- participating in NAT.


ip nat inside source static 172.16.50.8 172.16.10.8

!--- States that any packet received on the inside interface with a
!--- source IP address of 172.16.50.8 is translated to 172.16.10.8.
```

Remarque : la commande NAT source interne dans cet exemple implique également que les paquets reçus sur l'interface externe avec une adresse de destination de 172.16.10.8 ont l'adresse de destination traduite en 172.16.50.8.

La dernière étape consiste à vérifier que la fonction NAT fonctionne comme prévu .

5. Utiliser NAT pour les réseaux qui se chevauchent

Les réseaux qui se chevauchent se produisent lorsque vous attribuez des adresses IP à des périphériques internes qui sont déjà utilisés par d'autres périphériques sur Internet. Ces réseaux se produisent également lorsque deux entreprises, qui utilisent toutes deux des adresses IP RFC 1918 dans leurs réseaux, fusionnent. Ces deux réseaux doivent communiquer, de préférence sans que tous leurs périphériques ne soient réadressés.

Différence entre le mappage un-à-un et plusieurs-à-plusieurs

A configuration de NAT statique crée un mappage linéaire et traduit une adresse spécifique en une autre adresse. Ce type de configuration crée une entrée permanente dans la table NAT tant que la configuration est présente et permet aussi bien à des hôtes internes qu'externes d'initier une connexion. Ceci est en grande partie utile pour les hôtes qui fournissent des services d'application comme le courrier, Web, FTP et ainsi de suite. Exemple :

<#root>

```
Router(config)#
ip nat inside source static 10.3.2.11 10.41.10.12
Router(config)#
ip nat inside source static 10.3.2.12 10.41.10.13
```

NAT dynamique est utile quand moins d'adresses sont disponibles que le nombre réel d'hôtes à

traduire. Il crée une entrée dans la table NAT quand l'hôte lance une connexion et établit un mappage linéaire entre les adresses. Cependant, le mappage peut varier et dépend des adresses enregistrées disponibles dans le pool au moment de la transmission. NAT dynamique permet à des sessions d'être lancées seulement de l'intérieur ou de l'extérieur de réseaux externes pour lesquels elle est configurée. Des entrées de NAT dynamique sont supprimées de la table de traduction si l'hôte ne communique pas pendant une période spécifique qui est configurable. L'adresse est alors retournée au pool à l'usage d'un autre hôte.

Par exemple, complétez ces étapes de la configuration détaillée :

1. Créez un groupe d'adresses.

   <#root>

   ```
   Router(config)#
   ip nat pool MYPOOLEXAMPLE 10.41.10.1 10.41.10.41 netmask 255.255.255.0
   ```

2. Créez une liste d'accès pour les réseaux internes qui doivent être mappés.

   <#root>

   ```
   Router(config)#
   access-list 100 permit ip 10.3.2.0 0.0.0.255 any
   ```

3. Associez la liste d'accès 100 qui sélectionne le réseau interne 10.3.2.0 0.0.0.255 à attribuer au pool MYPOOLEXAMPLE, puis surchargez les adresses.

   <#root>

   ```
   Router(config)#
   ip nat inside source list 100 pool MYPOOLEXAMPLE overload
   ```

Vérifiez l'opération de NAT

Une fois la fonction NAT configurée, vérifiez qu'elle fonctionne comme prévu. Vous pouvez le faire de plusieurs manières : avec un analyseur de réseau, des commandes show ou des commandes debug. Pour un exemple détaillé de vérification NAT, référez-vous à Vérifier le fonctionnement NAT et NAT de base .

Conclusion

Les exemples de ce document illustrent les étapes de démarrage rapide qui peuvent vous aider à configurer et déployer la fonction NAT.

Ces étapes de démarrage rapide comprennent :

1. Définissez les interfaces internes et externes de NAT.
2. Que voulez-vous accomplir avec la fonction NAT ?
3. Configurez la NAT afin d'accomplir ce que vous avez défini à l'étape 2.
4. Vérifiez l'opération de NAT .

Dans chacun des exemples précédents, différentes formes de la commande ip nat insidecommand ont été utilisées. Vous pouvez également utiliser la commande ip nat outside afin d'accomplir les mêmes objectifs, mais gardez à l'esprit l'ordre des opérations NAT. Pour des exemples de configuration qui utilisent les commandes ip nat outsidecommandes, référez-vous à Exemple de configuration qui utilise la commande IP NAT Outside Source List .

Les exemples précédents ont également démontré ces actions :

Commande	Action
ip nat inside source	• Traduit la source des paquets IP se déplaçant de l'intérieur vers l'extérieur. • Traduit la destination des paquets IP se déplaçant de l'extérieur vers l'intérieur.
ip nat outside source	• Traduit la source des paquets IP se déplaçant de l'extérieur vers l'intérieur. • Traduit la destination des paquets IP se déplaçant de l'intérieur vers l'extérieur.

Informations connexes

- NAT : définitions locales et globales.
- Page de support NAT
- Page d'assistance pour les protocoles de routage IP
- Page de support pour le routage IP
- Services d’adressage IP
- Ordre des opérations NAT
- Questions fréquentes au sujet de Cisco IOS NAT
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.