Configurer la traduction d’adresse réseau

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés
- Conventions

Étapes de démarrage rapide pour configurer et déployer la NAT

Définir la NAT sur les interfaces intérieure et extérieure

Exemples

- 1. Autoriser les utilisateurs internes à accéder à Internet
  - Configurer la NAT pour permettre aux utilisateurs internes d’accéder à Internet
  - Configurer la NAT pour permettre aux utilisateurs internes d’accéder à Internet en cas de surcharge
- 2. Autoriser Internet à accéder aux périphériques internes
  - Configurer la NAT pour permettre à Internet d’accéder aux périphériques internes
- 3. Rediriger le trafic TCP vers un autre port TCP ou une autre adresse
  - Configurer la NAT pour rediriger le trafic TCP vers un autre port TCP ou une autre adresse
- 4. Utiliser la NAT pour une transition réseau
  - Configurer la NAT pour une utilisation pendant une transition réseau
- 5. Utilisez la NAT pour les réseaux qui se chevauchent

Différence entre les mappages un-à-un et plusieurs-à-plusieurs

Vérifiez l'opération de NAT

Conclusion

Informations connexes

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 NAT


Remarque : Dans ce document, quand Internet ou un périphérique d'Internet est mentionné, cela renvoie à un périphérique 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 ?
    - Existe-t-il plusieurs interfaces pour Internet?
2. Définissez ce que vous souhaitez réaliser avec la NAT.
    - Voulez-vous autoriser les utilisateurs internes à accéder à Internet ?
    - Voulez-vous autoriser Internet à accéder aux périphériques internes (comme un serveur de messagerie ou un serveur Web)?
    - Voulez-vous rediriger le trafic TCP vers un autre port TCP ou une autre adresse ?
    - Voulez-vous utiliser la fonction NAT pendant une transition réseau (par exemple, vous avez modifié l'adresse IP d'un serveur et, jusqu'à ce que vous puissiez mettre à jour tous les clients, vous voulez que les clients non mis à jour puissent accéder au serveur avec l'adresse IP d'origine et autoriser les clients mis à jour à accéder au serveur avec la nouvelle adresse) ?
    - Voulez-vous 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 laquelle des prochaines fonctionnalités utiliser :

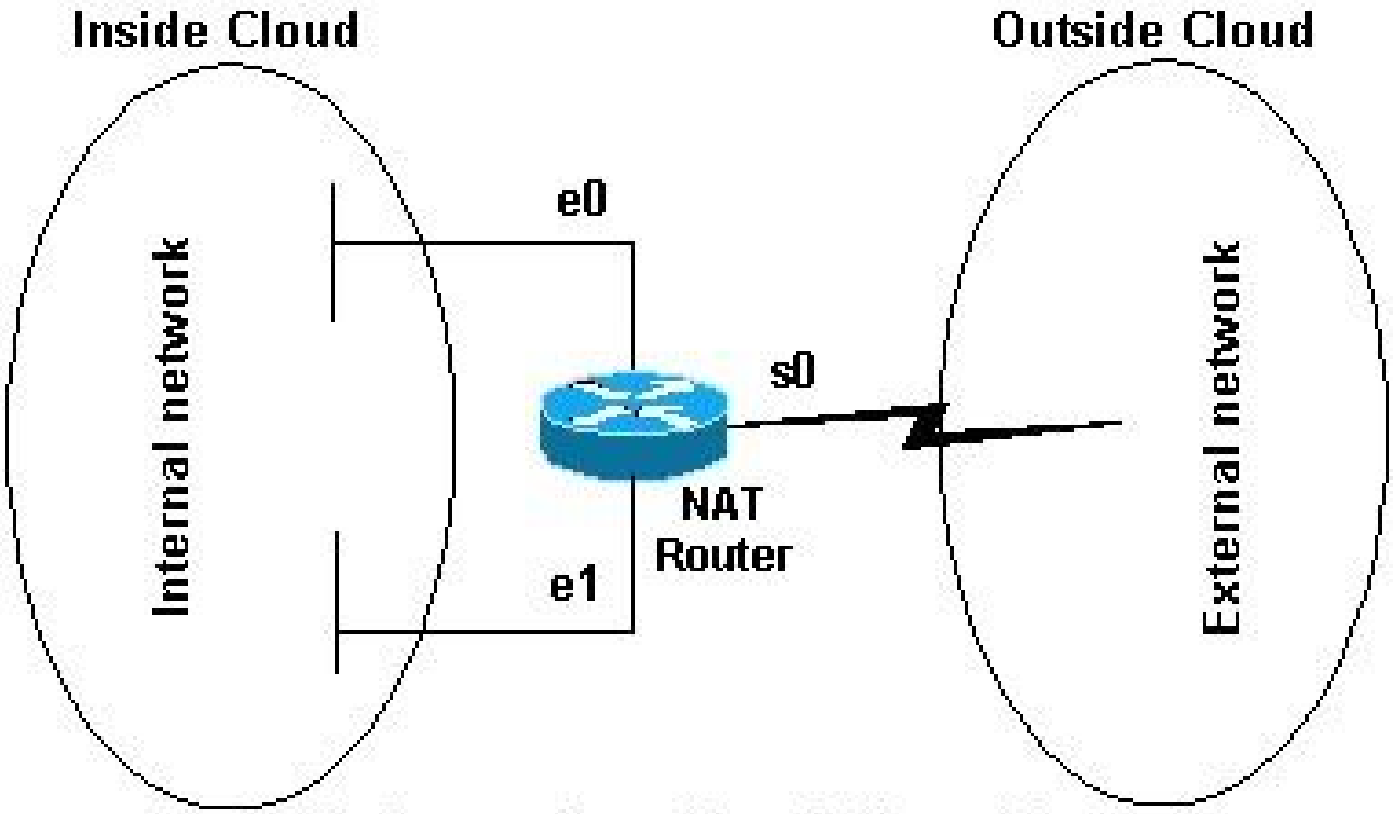
- NAT statique
- NAT dynamique
- Overloading
- Toute combinaison de ces fonctionnalités.

4. Vérifiez l'opération de NAT .

Chacun de ces exemples de 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.

Définir la NAT sur les interfaces intérieure et extérieure

La première étape du déploiement de la NAT consiste à définir les interfaces internes et externes de la NAT. Vous trouverez 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 en montre un exemple.



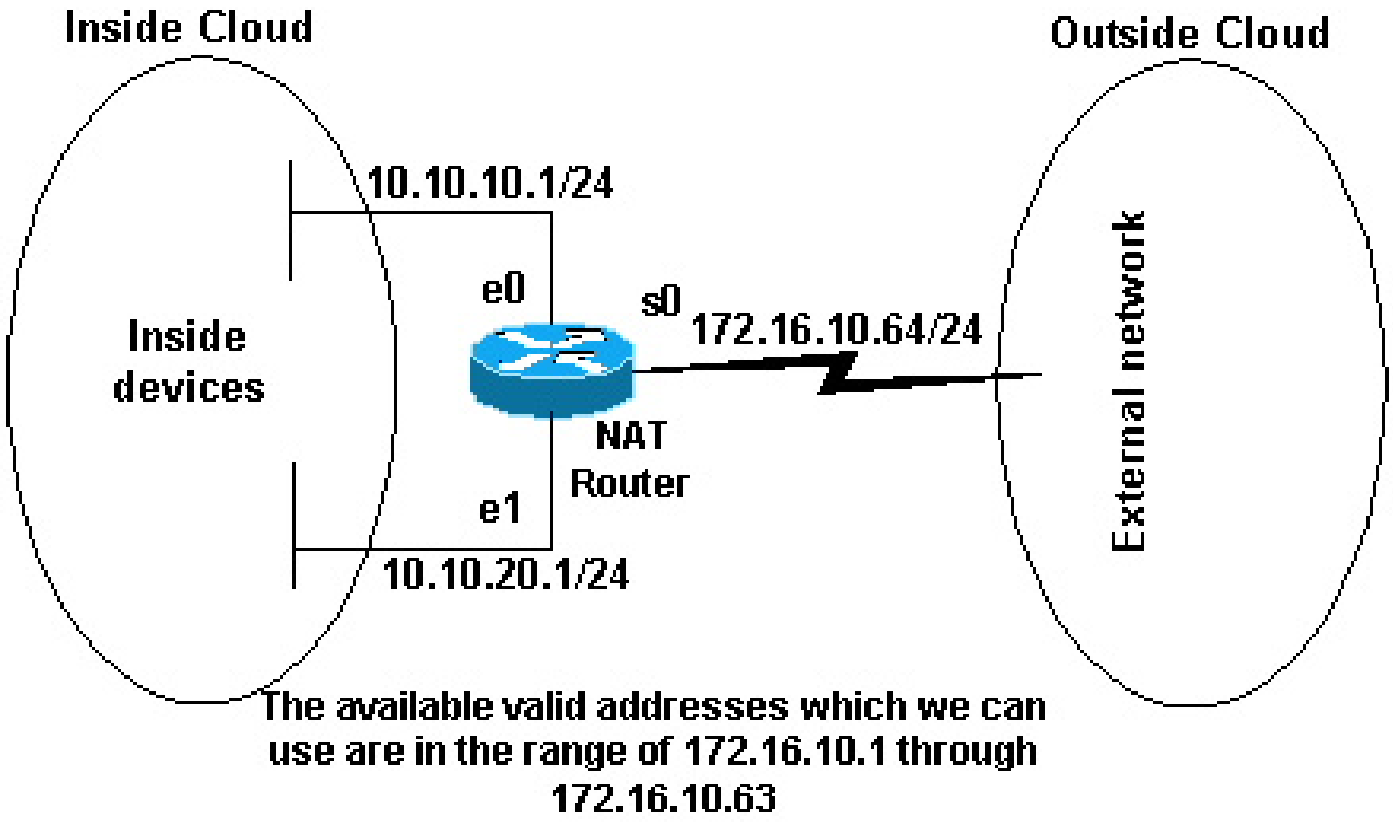
Topologie NAT

Exemples

1. Autoriser les utilisateurs internes à accéder à Internet

Est-il possible que vous souhaitiez autoriser les utilisateurs internes à accéder à Internet, mais que vous ne disposiez pas d'adresses valides suffisantes pour accueillir tout le monde ? Si toutes les communications avec les appareils Internet proviennent d'appareils internes, vous avez besoin d'une adresse unique valide ou d'un ensemble d'adresses valides.

Cette image montre un diagramme de réseau simple avec les interfaces de routeur définies comme internes et externes.



Adresses valides disponibles

Dans cet exemple, vous voulez que la fonction NAT autorise certains périphériques internes (les 31 premiers de chaque sous-réseau) à établir une communication avec des périphériques externes 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 la NAT. Afin de réaliser 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. Par opposition à la NAT statique, où une traduction est configurée de manière statique

et placée dans la table de traduction sans qu'il soit nécessaire de générer du trafic.

Dans cet exemple, vous pouvez configurer la NAT pour traduire chacun des périphériques internes en une adresse valide unique, ou pour traduire chacun des périphériques internes vers la même adresse valide. Cette deuxième méthode est connue sous le nom de . overloading Un exemple de la façon de configurer chaque méthode est donné ici.

Configurer la NAT pour permettre aux utilisateurs internes d'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 fortement 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 réseau.

Dans la configuration précédente, notez que 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, seules ces adresses source sont traduites. Il peut y avoir d'autres appareils avec d'autres adresses sur le réseau interne, mais ceux-ci ne sont pas traduits.

Configurer la NAT pour permettre aux utilisateurs internes d'accéder à Internet en cas de 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.
```

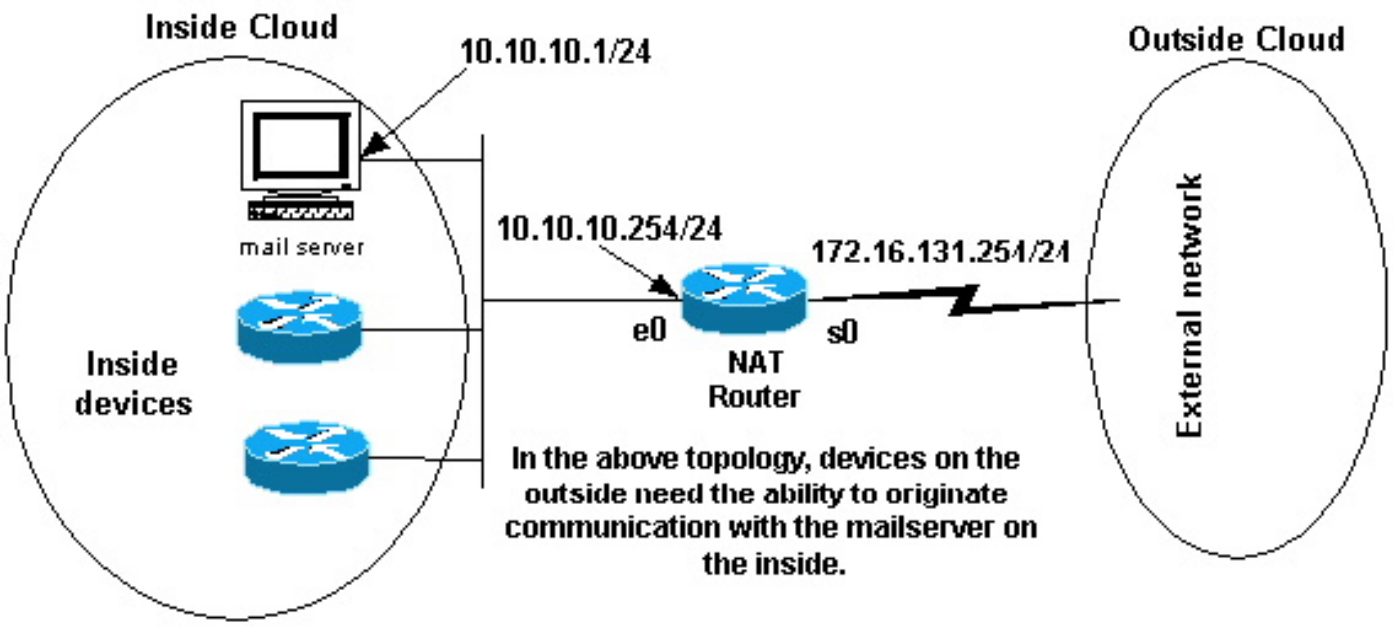
Remarquez que dans la deuxième configuration précédente, le pool NAT n'a qu'une seule adresse. ovrld Le mot clé overload utilisé dans la commande ip nat inside source list 7 pool ovrld overload permet à NAT de traduire plusieurs périphériques internes en l'adresse unique dans le groupe.

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

Lorsque est configuré, le routeur conserve suffisamment d'informations des protocoles de niveau supérieur (par exemple, les numéros de port TCP ou UDP) pour traduire l'adresse globale en adresse locale correcte.overloading Pour les définitions d'adresse globale et locale, référez-vous à NAT : Définitions locales et globales.

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 d'appareils Internet, par exemple, pour échanger des courriels. Il est courant que les périphériques Internet envoient des courriels à un serveur de messagerie qui réside sur le réseau interne.



Origine des communications

Configurer la NAT pour permettre à Internet d'accéder aux périphériques internes

Dans cet exemple, vous définissez d'abord les interfaces interne et externe de la NAT, comme illustré dans le diagramme de réseau précédent.

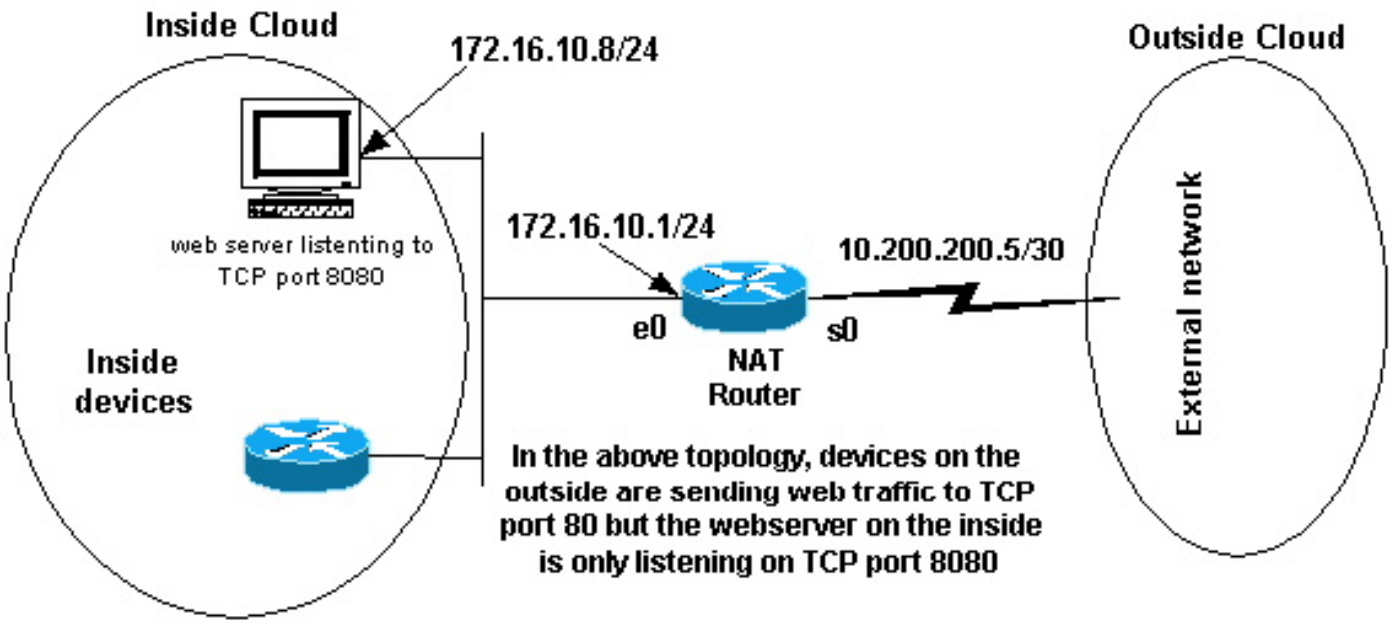
Ensuite, vous définissez que vous souhaitez que les utilisateurs internes puissent établir des

communications avec l'extérieur. Les périphériques externes doivent pouvoir communiquer avec le serveur de messagerie uniquement à l'intérieur.

La troisième étape est de configurer NAT. Pour réaliser ce que vous avez défini, vous pouvez configurer ensemble la NAT statique et dynamique. Pour plus d'informations sur la façon de configurer cet exemple, référez-vous à Configurer la NAT statique et dynamique simultanément.

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

Un serveur Web sur le réseau interne est un autre exemple où il peut être nécessaire que des périphériques Internet établissent la 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 diagramme de réseau précédent, vous pouvez décider que vous souhaitez 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 pour traduire le numéro de port TCP pour y parvenir. Un exemple de configuration est présenté ici.

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

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.
```

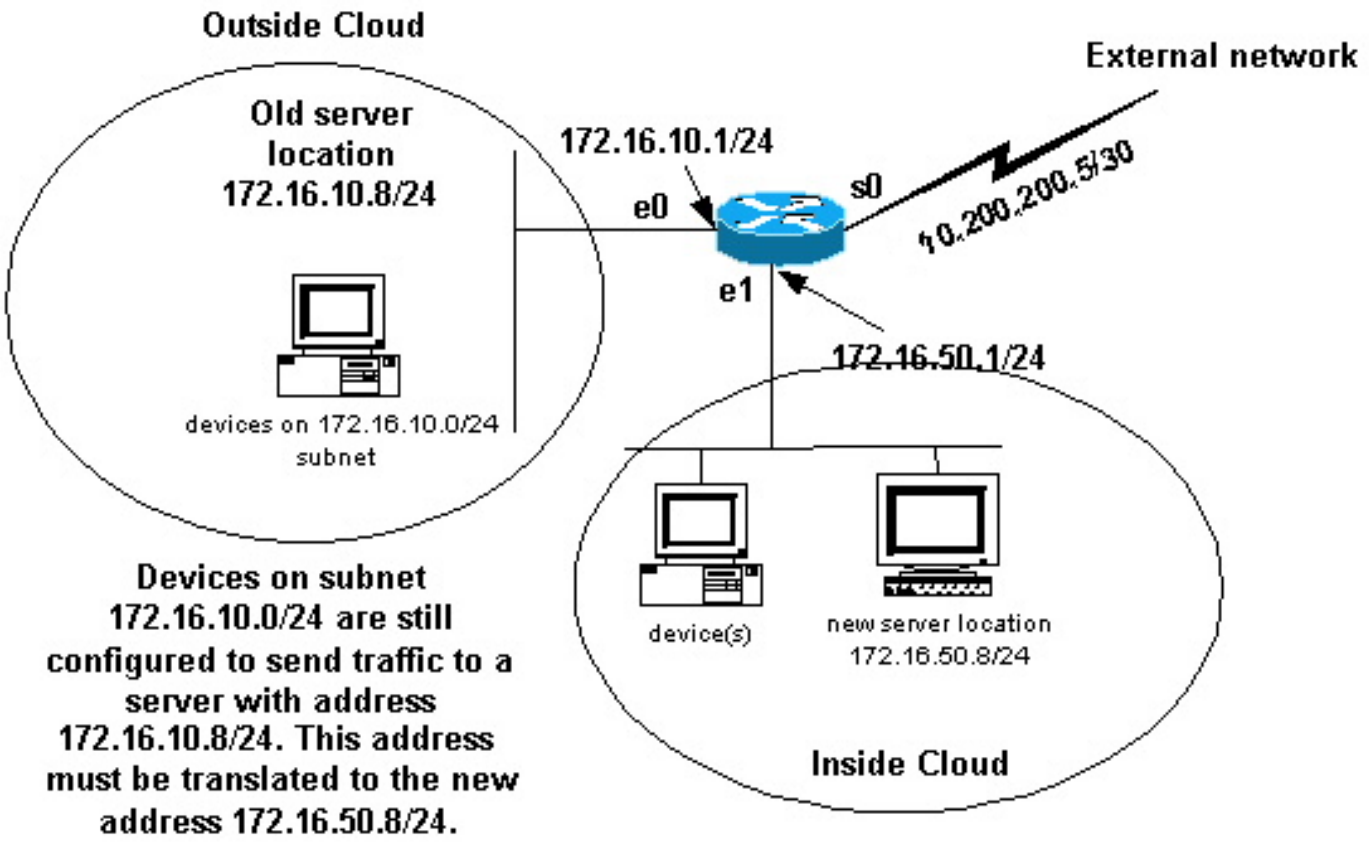


Remarque : La description de la configuration pour la commande NAT statique indique que tout paquet reçu dans l'interface interne avec une adresse source de 172.16.10.8:8080 est traduit en 172.16.10.8:80. Cela implique également que tout paquet reçu sur l'interface externe avec une adresse de destination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

```
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 NAT pour une transition réseau

La 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 serveur qui a une nouvelle adresse IP, la reconfiguration de tous les périphériques du réseau pour utiliser la nouvelle adresse de serveur prendra un certain temps. En attendant, vous pouvez utiliser la NAT pour configurer les périphériques avec l'ancienne adresse pour traduire leurs paquets afin de communiquer avec le nouveau serveur.



Transition du réseau NAT

Une fois que vous avez défini les interfaces NAT, comme illustré à l'image précédente, vous pouvez décider que vous souhaitez que la NAT permette que les paquets de l'extérieur destinés à l'ancienne adresse du serveur (172.16.10.8) soient traduits et envoyés à la nouvelle adresse du serveur. N'oubliez pas que le nouveau serveur se trouve sur un autre réseau local et que les périphériques de ce réseau local ou les périphériques accessibles 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. Voici un exemple de configuration.

Configurer la NAT pour une utilisation pendant 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.

5. Utilisez la NAT pour les réseaux qui se chevauchent

Des réseaux peuvent en venir à se chevaucher lorsque vous attribuez des adresses IP à des appareils internes qui sont déjà utilisées par d'autres appareils sur Internet. Cela peut également se produire lorsque deux entreprises, qui utilisent toutes deux les adresses IP [RFC 1918](#) dans leurs réseaux, fusionnent. Ces deux réseaux doivent communiquer, de préférence sans que tous leurs périphériques 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 pour le déploiement de la fonction NAT pour le 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 que vous avez configuré la NAT, vérifiez qu’elle fonctionne comme prévu. Vous pouvez faire ceci de diverses façons : avec un analyseur de réseau, des commandes show ou des commandes debug. Pour obtenir un exemple détaillé de vérification NAT, reportez-vous àVérification du fonctionnement NAT et NAT de base.

Conclusion

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

Ces étapes de démarrage rapide comprennent :

1. Définissez les interfaces internes et externes de NAT.
2. Que voulez-vous réaliser avec 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, diverses formes de la commande ip nat Insideont été utilisées. Vous pouvez également utiliser la commande ip nat Outsidepour réaliser les mêmes objectifs, mais gardez à l'esprit l'ordre des opérations de la NAT. Pour des exemples de configuration qui utilisent les commandes ip nat outsidecommandes, référez-vous à Configurer la commande IP NAT Outside Source List.

Les exemples précédents ont également montré 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.