

Configuration du transfert de port ASA version 9 avec NAT

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Autoriser les hôtes internes à accéder aux réseaux externes avec PAT](#)

[Autoriser les hôtes internes à accéder aux réseaux externes à l'aide de NAT](#)

[Autoriser les hôtes non approuvés à accéder à des hôtes sur votre réseau approuvé](#)

[NAT d'identité statique](#)

[Redirection de port \(transfert\) avec statique](#)

[Vérification](#)

[Connexion](#)

[Syslog](#)

[Packet Tracer](#)

[Saisir](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer la redirection de port (redirection) et les fonctionnalités NAT (traduction d'adresses de réseau) externes dans le logiciel ASA (Adaptive Security Appliance) version 9.x, avec l'utilisation de l'interface de ligne de commande ou de l'ASDM (Adaptive Security Device Manager).

Référez-vous au [Guide de configuration ASDM du pare-feu de la gamme Cisco ASA](#) pour plus d'informations.

Conditions préalables

Conditions requises

Référez-vous à [Configuration de l'accès de gestion](#) afin de permettre au périphérique d'être configuré par l'ASDM.

Components Used

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

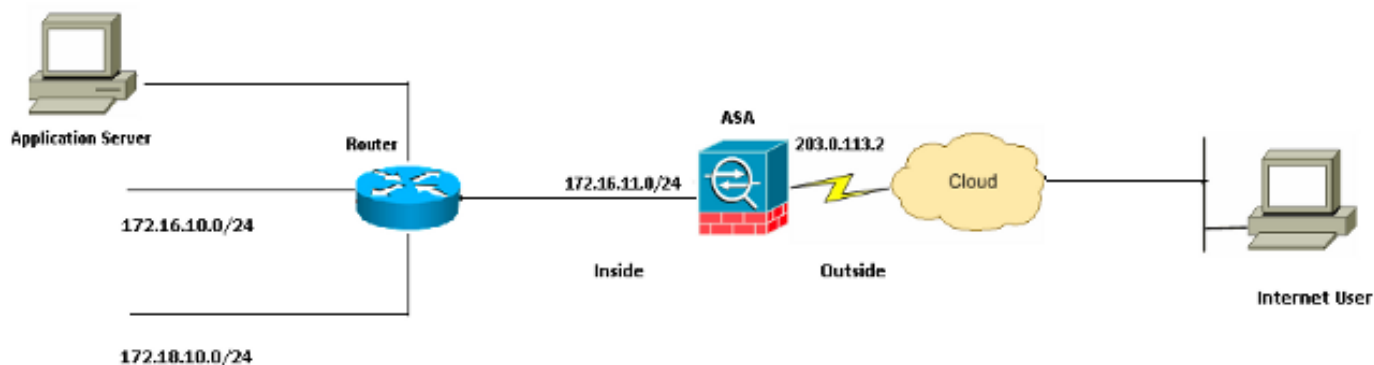
logiciel suivantes :

- Logiciel du dispositif de sécurité de la gamme Cisco ASA 5525, version 9.x et ultérieure
- ASDM version 7.x et ultérieure

"Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel de toute commande. »

Configuration

Diagramme du réseau



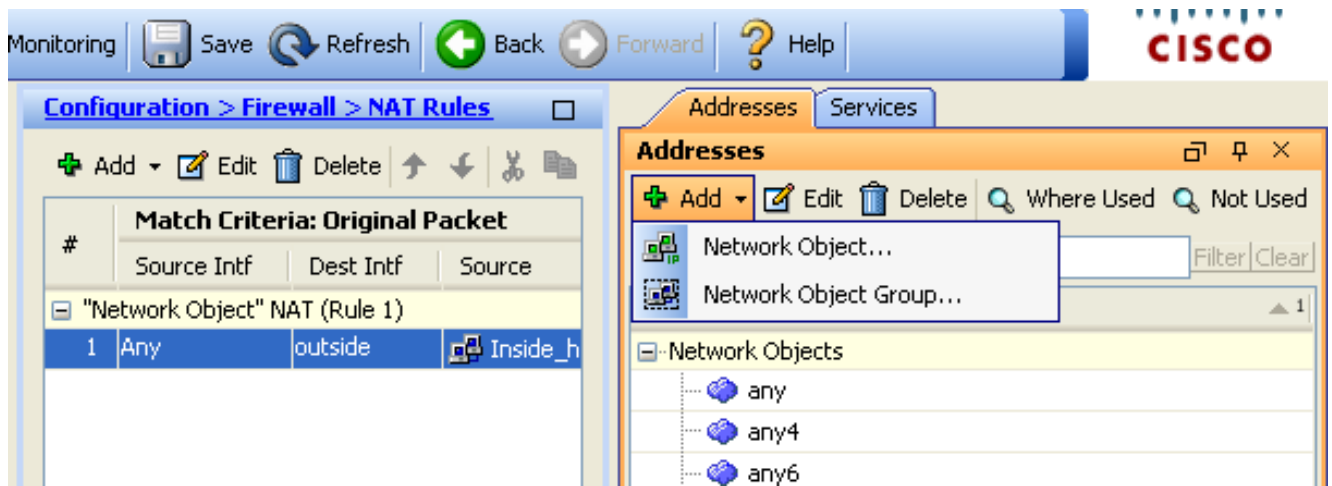
Les systèmes d'adresse IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisés dans un environnement de laboratoire.

Autoriser les hôtes internes à accéder aux réseaux externes avec PAT

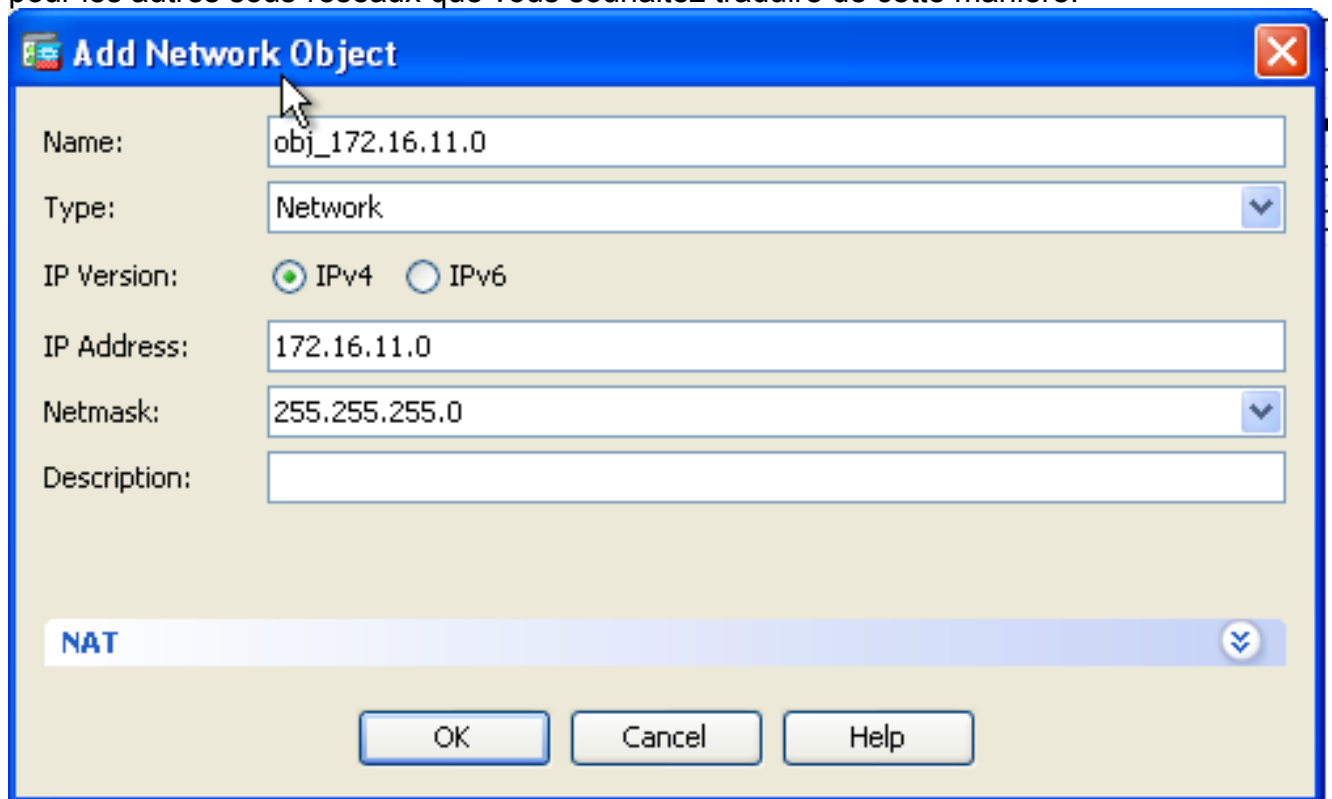
Si vous souhaitez que les hôtes internes partagent une adresse publique unique pour la traduction, utilisez la traduction d'adresses de port (PAT). L'une des configurations PAT les plus simples implique la traduction de tous les hôtes internes pour qu'ils ressemblent à l'adresse IP de l'interface externe. Il s'agit de la configuration PAT type utilisée lorsque le nombre d'adresses IP routables disponibles auprès du FAI est limité à quelques, voire à une seule.

Complétez ces étapes afin de permettre aux hôtes internes d'accéder aux réseaux externes avec la PAT :

1. Choisissez **Configuration > Firewall > NAT Rules**. Cliquez sur **Add**, puis choisissez **Network Object** afin de configurer une règle NAT dynamique.



2. Configurez le réseau/hôte/plage pour lequel la **fonction PAT dynamique** est requise. Dans cet exemple, un des sous-réseaux internes a été sélectionné. Ce processus peut être répété pour les autres sous-réseaux que vous souhaitez traduire de cette manière.



3. Développez NAT. Cochez la case **Ajouter des règles de traduction automatique d'adresses**. Dans la liste déroulante Type, sélectionnez **PAT dynamique (Masquer)**. Dans le champ **Translated Addr**, choisissez l'option pour refléter l'interface externe. Cliquez sur **Advanced**.

Add Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

Add Automatic Address Translation Rules

Type: Dynamic PAT (Hide)

Translated Addr: outside

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

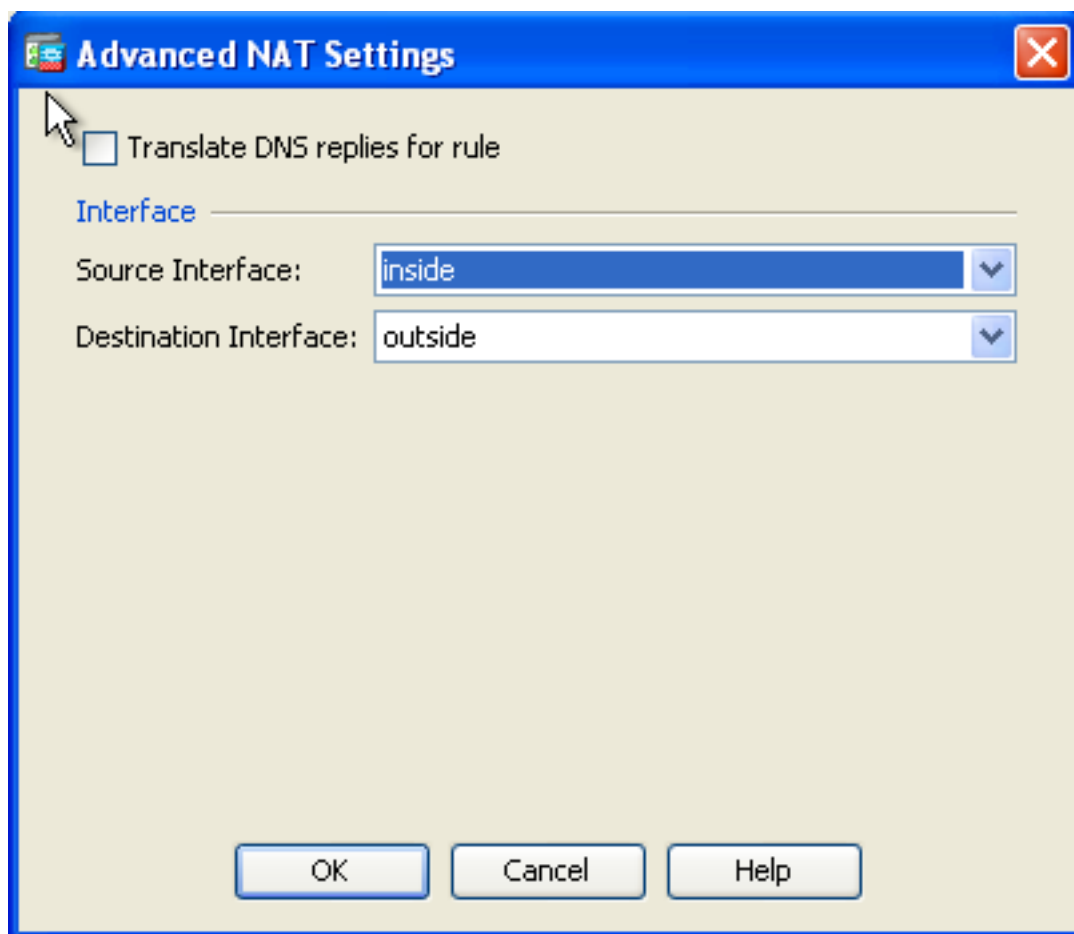
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

4. Dans les listes déroulantes Interface source et Interface de destination, sélectionnez les interfaces appropriées. Cliquez sur **OK** et cliquez sur **Apply** pour que les modifications prennent effet.



Voici la sortie de CLI équivalente pour cette configuration PAT :

```
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat (inside,outside) dynamic interface
```

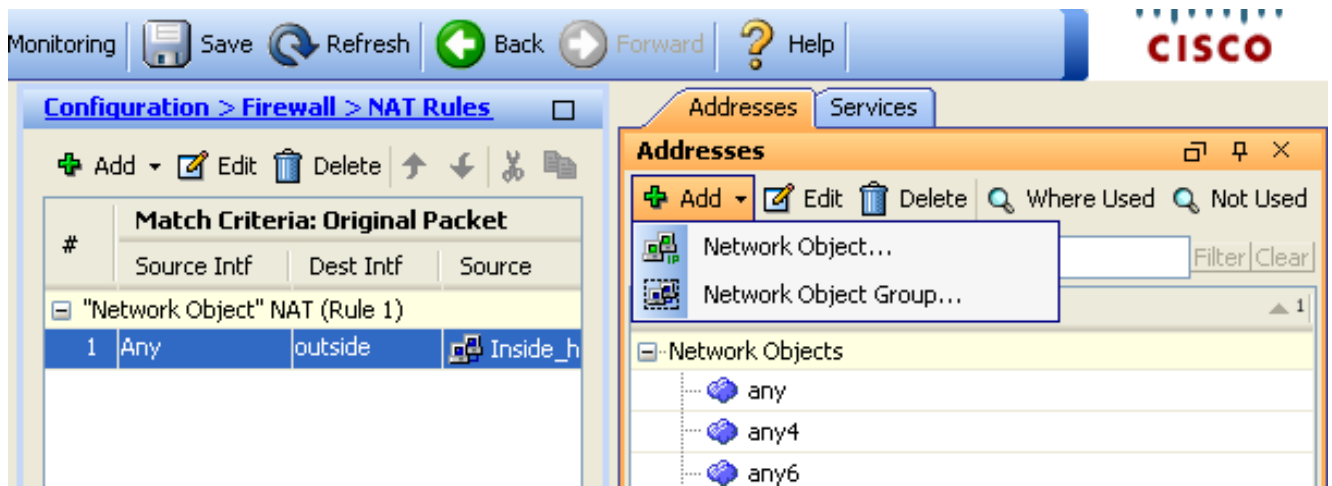
Autoriser les hôtes internes à accéder aux réseaux externes à l'aide de NAT

Vous pouvez autoriser un groupe d'hôtes/réseaux internes à accéder au monde extérieur avec la configuration des règles NAT dynamiques. Contrairement à la fonction PAT, la fonction NAT dynamique attribue les adresses traduites à partir d'un pool d'adresses. Par conséquent, un hôte est mappé à sa propre adresse IP traduite et deux hôtes ne peuvent pas partager la même adresse IP traduite.

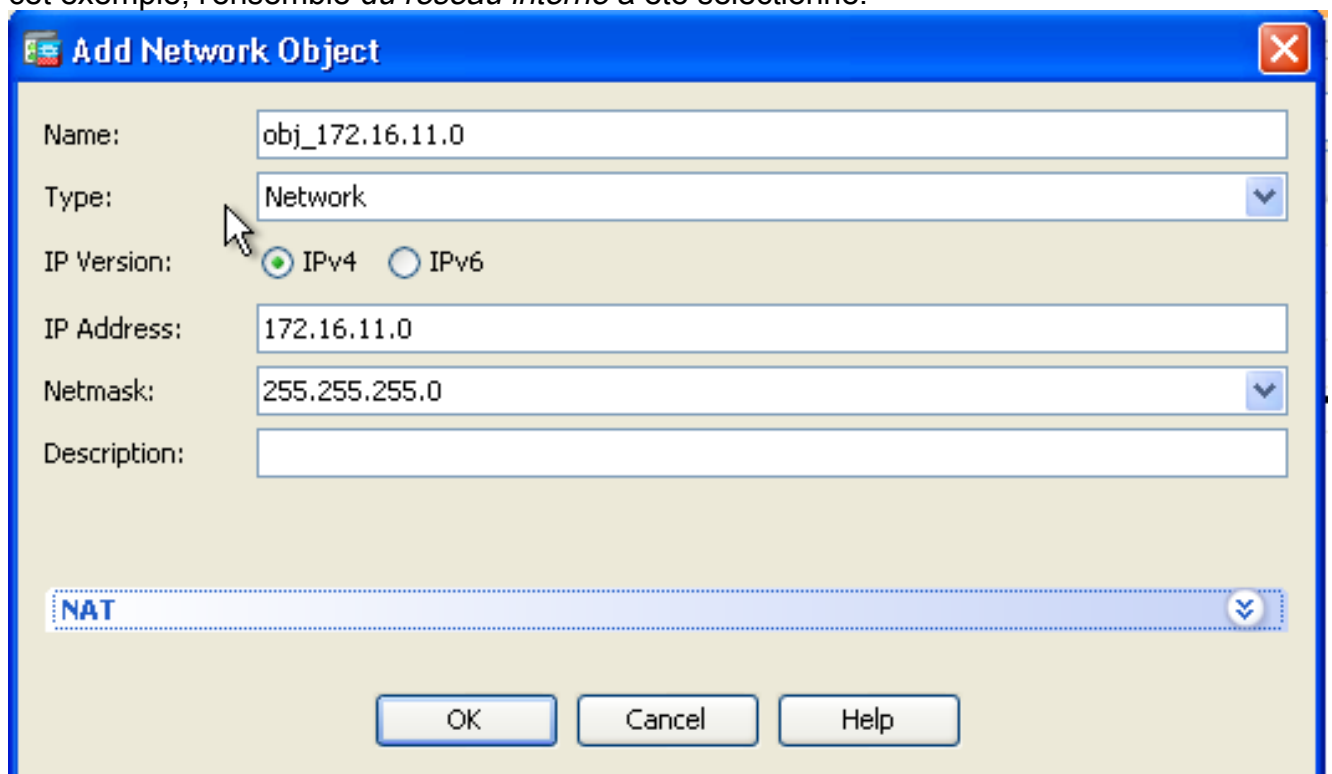
Pour ce faire, vous devez sélectionner l'adresse réelle des hôtes/réseaux auxquels l'accès doit être accordé, puis les mapper à un pool d'adresses IP traduites.

Complétez ces étapes afin de permettre aux hôtes internes d'accéder aux réseaux externes avec NAT :

1. Choisissez **Configuration > Firewall > NAT Rules**. Cliquez sur **Add**, puis choisissez **Network Object** afin de configurer une règle NAT dynamique.



2. Configurez le réseau/hôte/plage pour lequel la fonction PAT dynamique est requise. Dans cet exemple, l'ensemble *du réseau interne* a été sélectionné.



3. Développez NAT. Cochez la case **Ajouter des règles de traduction automatique d'adresses**. Dans la liste déroulante Type, sélectionnez **Dynamic**. Dans le champ Translated Addr, sélectionnez la sélection appropriée. Cliquez sur **Advanced**.

Edit Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

4. Cliquez sur **Add** pour ajouter l'objet réseau. Dans la liste déroulante Type, sélectionnez **Range**. Dans les champs Start Address et End Address, saisissez les adresses IP PAT de début et de fin. Click OK.

Add Network Object

Name: obj-my-range

Type: Range

IP Version: IPv4 IPv6

Start Address: 203.0.113.10

End Address: 203.0.113.20

Description:

NAT

OK Cancel Help

5. Dans le champ Adresse traduite, sélectionnez l'objet d'adresse. Cliquez sur **Advanced** afin de sélectionner les interfaces source et de destination.

Edit Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr: obj-my-range

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

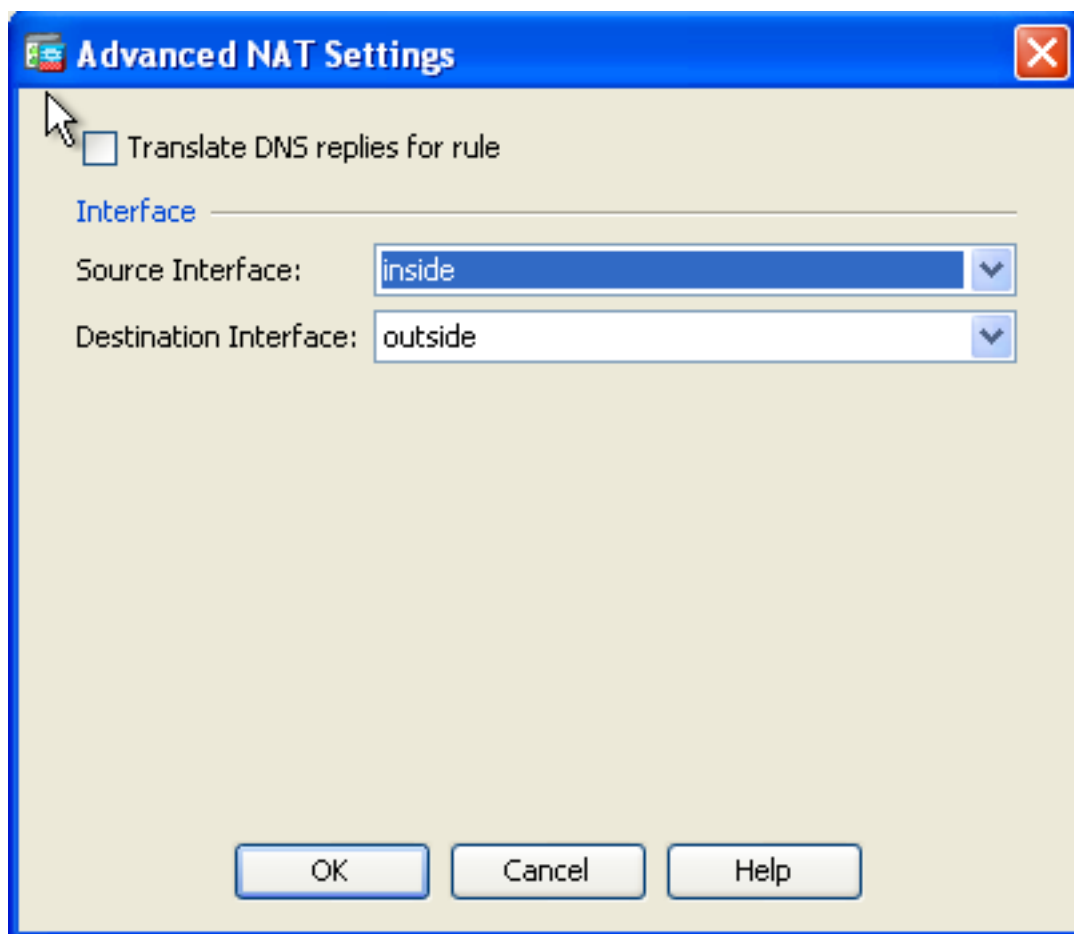
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

6. Dans les listes déroulantes Interface source et Interface de destination, sélectionnez les interfaces appropriées. Cliquez sur **OK** et cliquez sur **Apply** pour que les modifications prennent effet.



Voici la sortie de CLI équivalente pour cette configuration ASDM :

```
object network obj-my-range  
range 203.0.113.10 203.0.113.20
```

```
object network obj_172.16.11.0  
subnet 172.16.11.0 255.255.255.0  
nat(inside,outside) dynamic obj-my-range
```

Selon cette configuration, les hôtes du réseau 172.16.11.0 sont traduits en n'importe quelle adresse IP du pool NAT, 203.0.113.10 - 203.0.113.20. Si le pool mappé a moins d'adresses que le groupe réel, vous pourriez être à court d'adresses. Par conséquent, vous pouvez essayer d'implémenter la NAT dynamique avec la sauvegarde PAT dynamique ou vous pouvez essayer d'étendre le pool actuel.

1. Répétez les étapes 1 à 3 de la configuration précédente et cliquez à nouveau sur **Add** afin d'ajouter un objet réseau. Dans la liste déroulante Type, sélectionnez **Host**. Dans le champ IP Address, saisissez l'adresse IP de sauvegarde PAT. Click OK.

Add Network Object

Name: (optional)

Type:

IP Version: IPv4 IPv6

IP Address:

Netmask:

FQDN:

Description:

NAT

OK Cancel Help

2. Cliquez sur **Add** pour ajouter un groupe d'objets réseau. Dans le champ Group Name, entrez un nom de groupe et **ajoutez** les deux objets d'adresse (plage NAT et adresse IP PAT) dans le groupe.

Add Network Object Group

Group Name:

Description:

Existing Network Objects/Groups:

Name	IP Address	Netmask	Description
- Network Objects			
any			
any4			
any6			
inside-net...	19.19.19.0	255.255.255.0	
obj_172.1...	172.16.11.0	255.255.255.0	

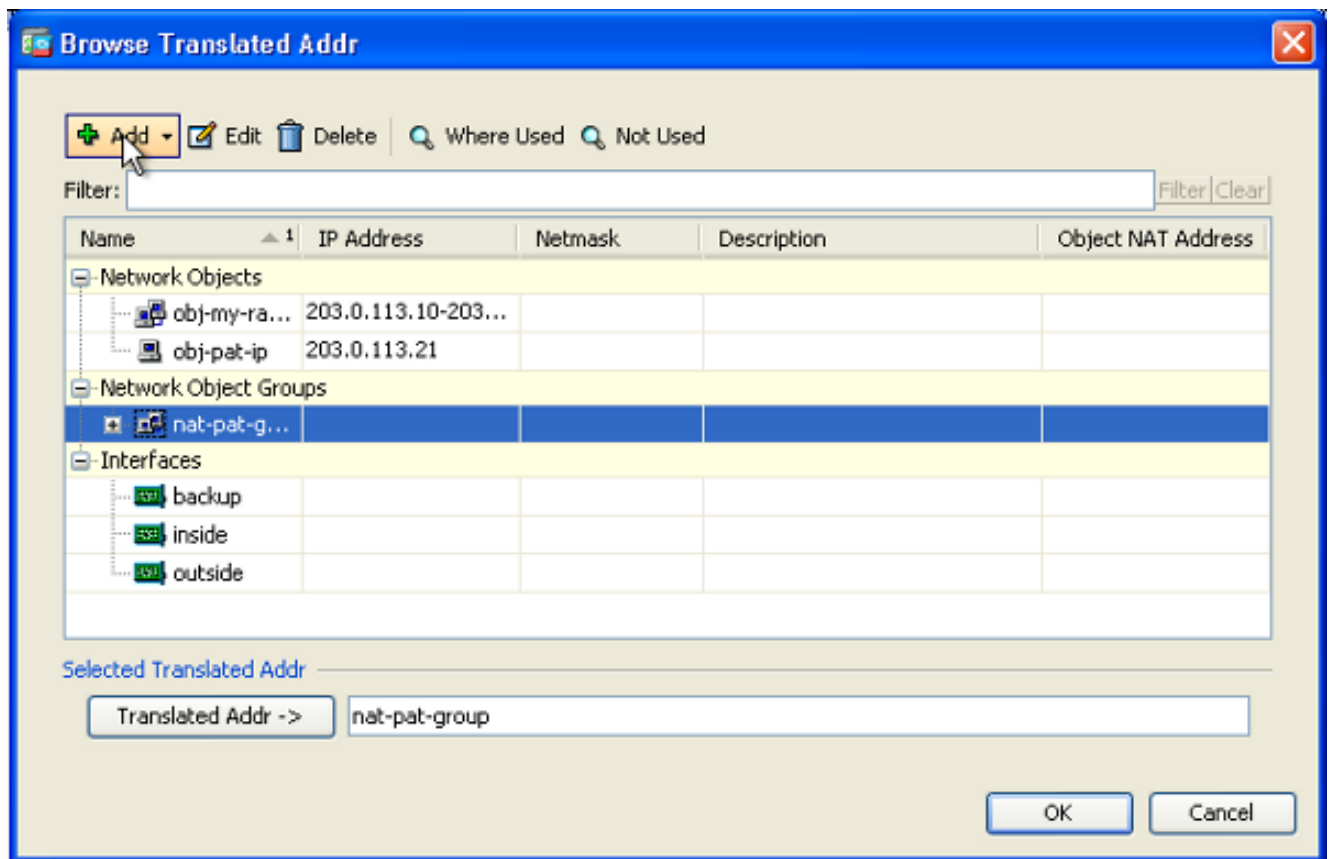
Members in Group:

Name	IP Address	Netmask/Prefix L
obj-pat-ip	203.0.113.21	
obj-my-range	203.0.113.10-203.0.113.254	

Add >>

<< Remove

3. Choisissez la règle NAT configurée et changez l'adresse traduite en groupe nouvellement configuré 'nat-pat-group' (anciennement 'obj-my-range'). Click OK.



4. Cliquez sur **OK** afin d'ajouter la règle NAT. Cliquez sur **Advanced** afin de sélectionner les interfaces source et de destination.

Edit Network Object

Name: obj_172.16.11.0

Type: Network

IP Version: IPv4 IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

NAT

Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr: nat-pat-group

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

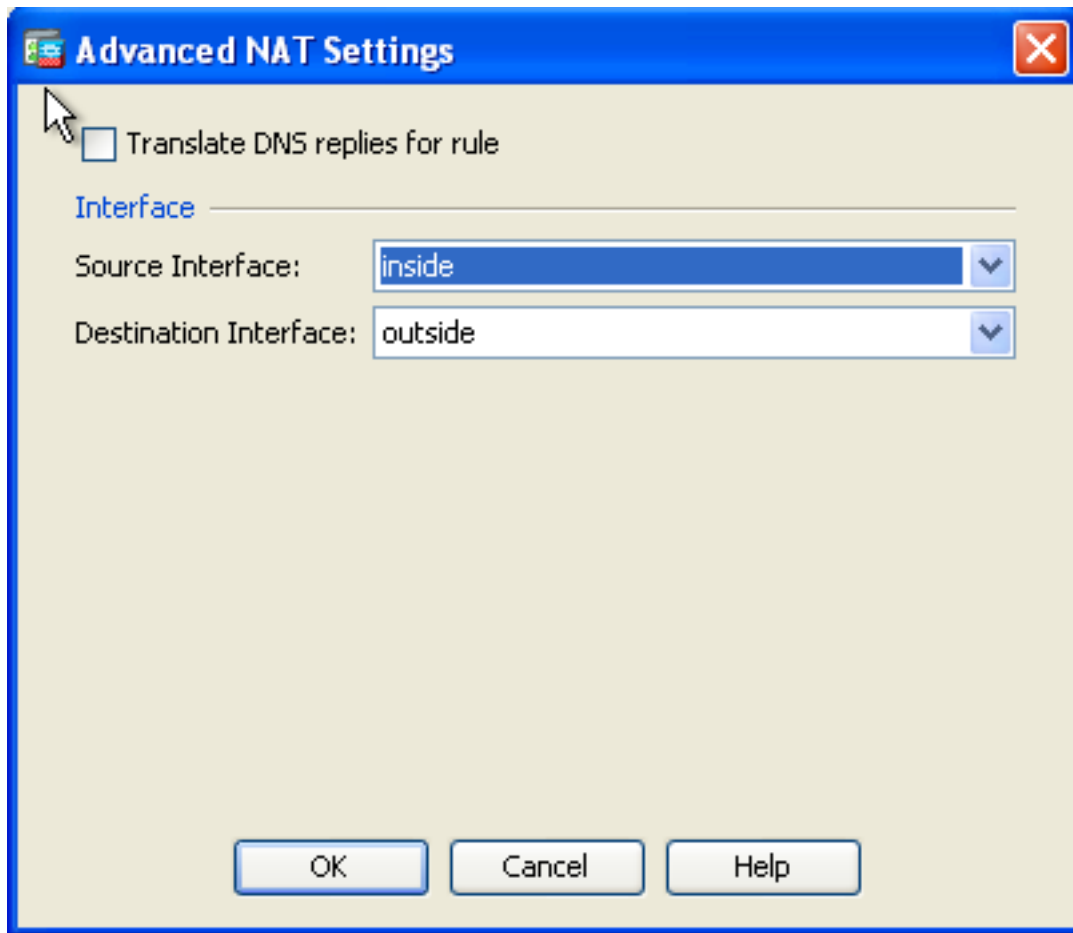
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

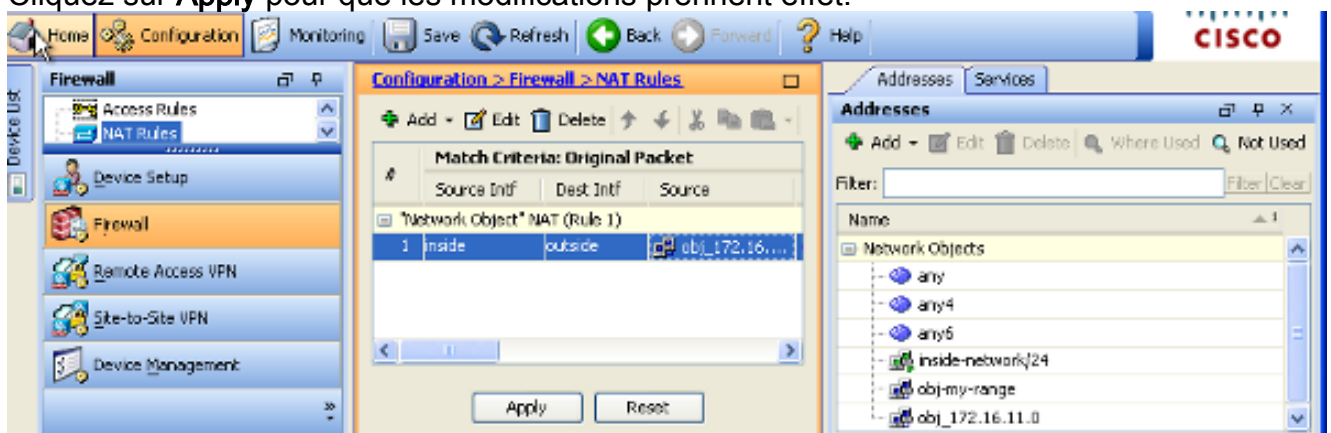
Advanced...

OK Cancel Help

5. Dans les listes déroulantes Interface source et Interface de destination, sélectionnez les interfaces appropriées. Click OK.



6. Cliquez sur **Apply** pour que les modifications prennent effet.



Voici la sortie de CLI équivalente pour cette configuration ASDM :

```
object network obj-my-range
range 203.0.113.10 203.0.113.20
```

```
object network obj-pat-ip
host 203.0.113.21
```

```
object-group network nat-pat-group
network-object object obj-my-range
network-object object obj-pat-ip
```

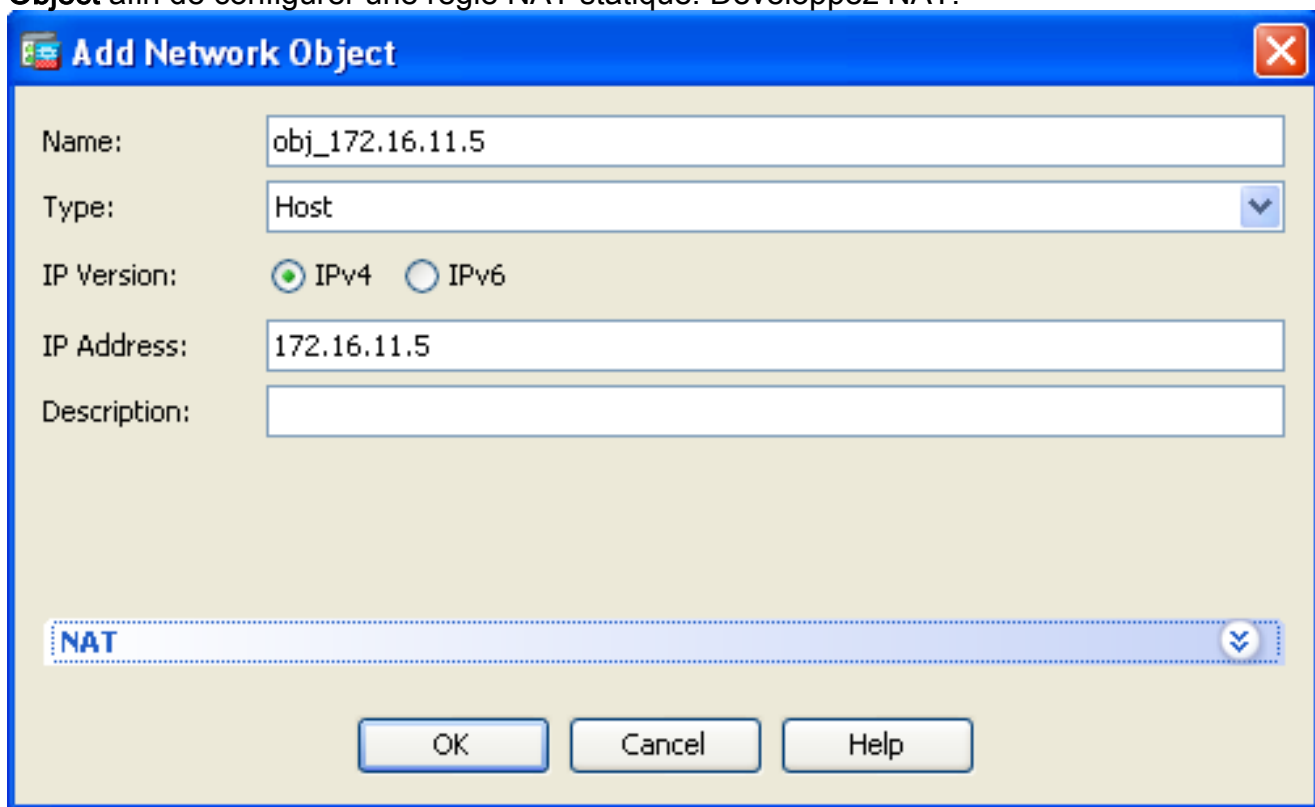
```
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
```

nat (inside,outside) dynamic nat-pat-group

Autoriser les hôtes non approuvés à accéder à des hôtes sur votre réseau approuvé

Cela peut être réalisé par l'application d'une traduction NAT statique et d'une règle d'accès pour autoriser ces hôtes. Vous devez le configurer chaque fois qu'un utilisateur externe souhaite accéder à un serveur de votre réseau interne. Le serveur du réseau interne peut avoir une adresse IP privée qui n'est pas routable sur Internet. Par conséquent, vous devez traduire cette adresse IP privée en adresse IP publique par le biais d'une règle NAT statique. Supposons que vous ayez un serveur interne (172.16.11.5). Pour que cela fonctionne, vous devez traduire cette adresse IP de serveur privé en adresse IP publique. Cet exemple décrit comment implémenter la NAT statique bidirectionnelle pour traduire 172.16.11.5 en 203.0.113.5.

1. Choisissez **Configuration > Firewall > NAT Rules**. Cliquez sur **Add**, puis choisissez **Network Object** afin de configurer une règle NAT statique. Développez NAT.



Add Network Object

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Description:

NAT

OK Cancel Help

2. Cochez la case **Ajouter des règles de traduction automatique d'adresses**. Dans la liste déroulante Type, sélectionnez **Statique**. Dans le champ Translated Addr, saisissez l'adresse IP. Cliquez sur **Advanced** afin de sélectionner les interfaces source et de destination.

Add Network Object

Name: obj_172.16.11.5

Type: Host

IP Version: IPv4 IPv6

IP Address: 172.16.11.5

Description:

NAT

Add Automatic Address Translation Rules

Type: Static

Translated Addr: 203.0.113.5

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

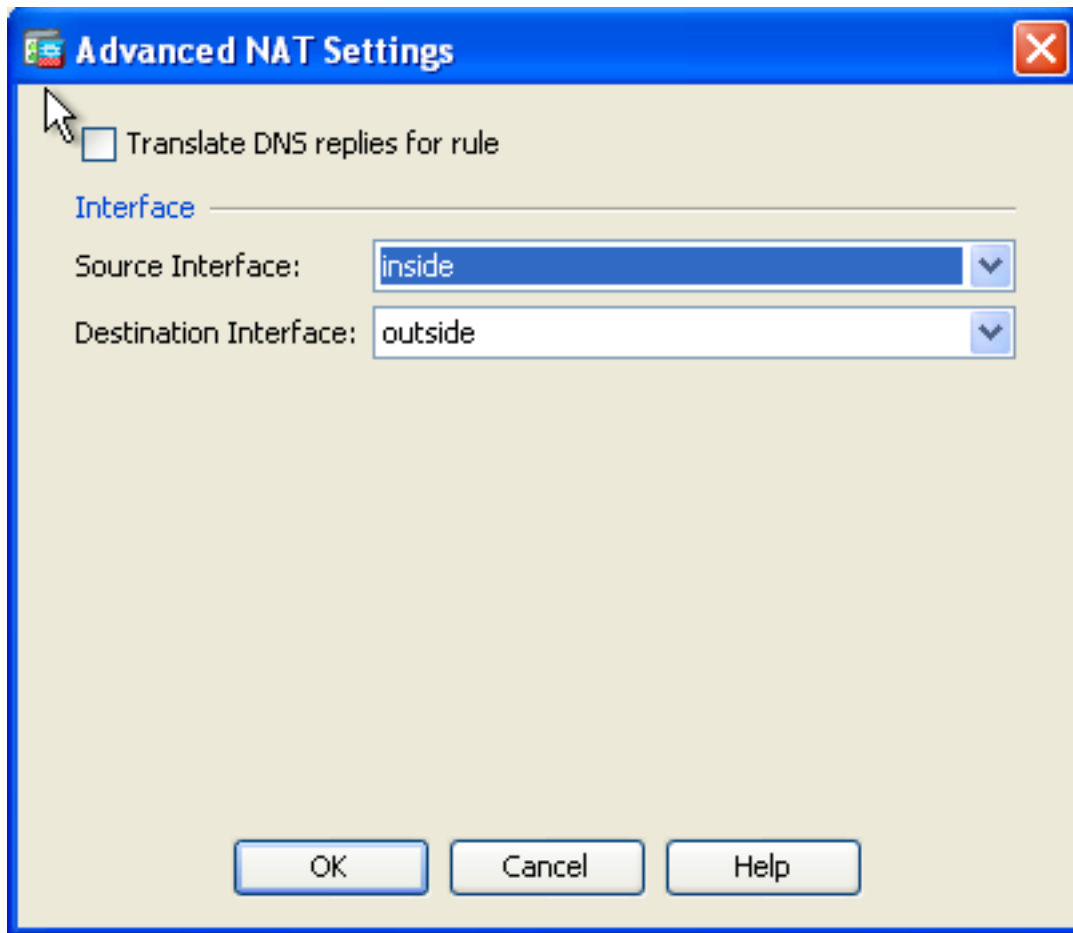
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

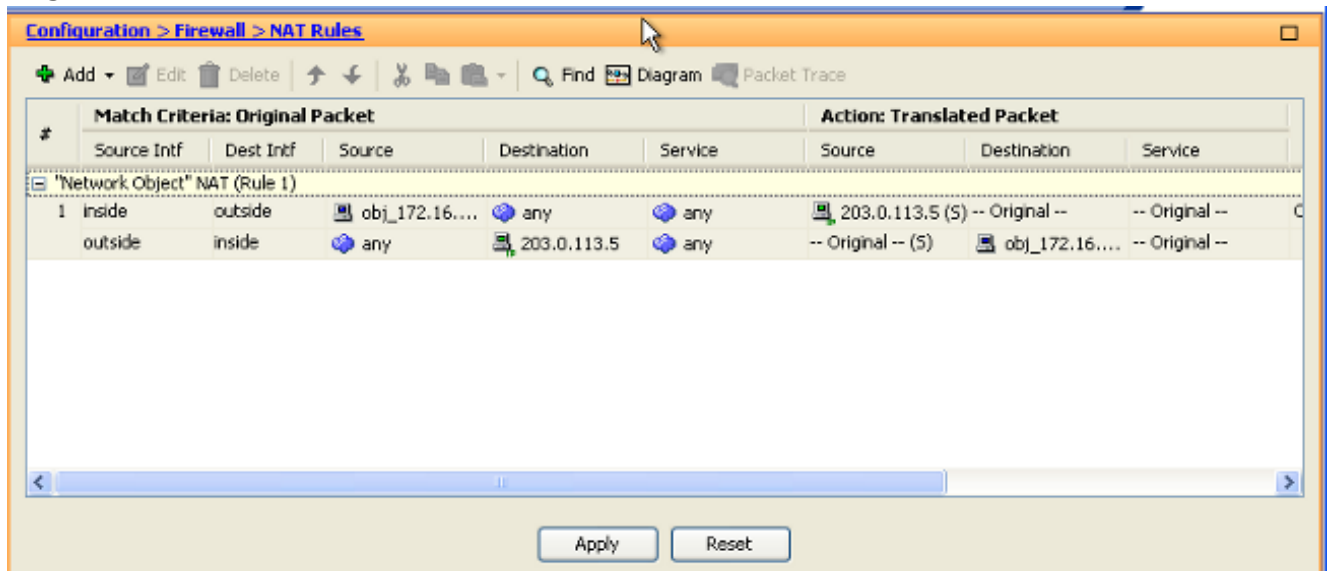
Advanced...

OK Cancel Help

3. Dans les listes déroulantes Interface source et Interface de destination, sélectionnez les interfaces appropriées. Click OK.



4. Vous pouvez voir l'entrée NAT statique configurée ici. Cliquez sur **Apply** afin d'envoyer ceci à l'ASA.



Voici la sortie de l'interface de ligne de commande équivalente pour cette configuration NAT :

```
object network obj_172.16.11.5
host 172.16.11.5
nat (inside,outside) static 203.0.113.5
```

NAT d'identité statique

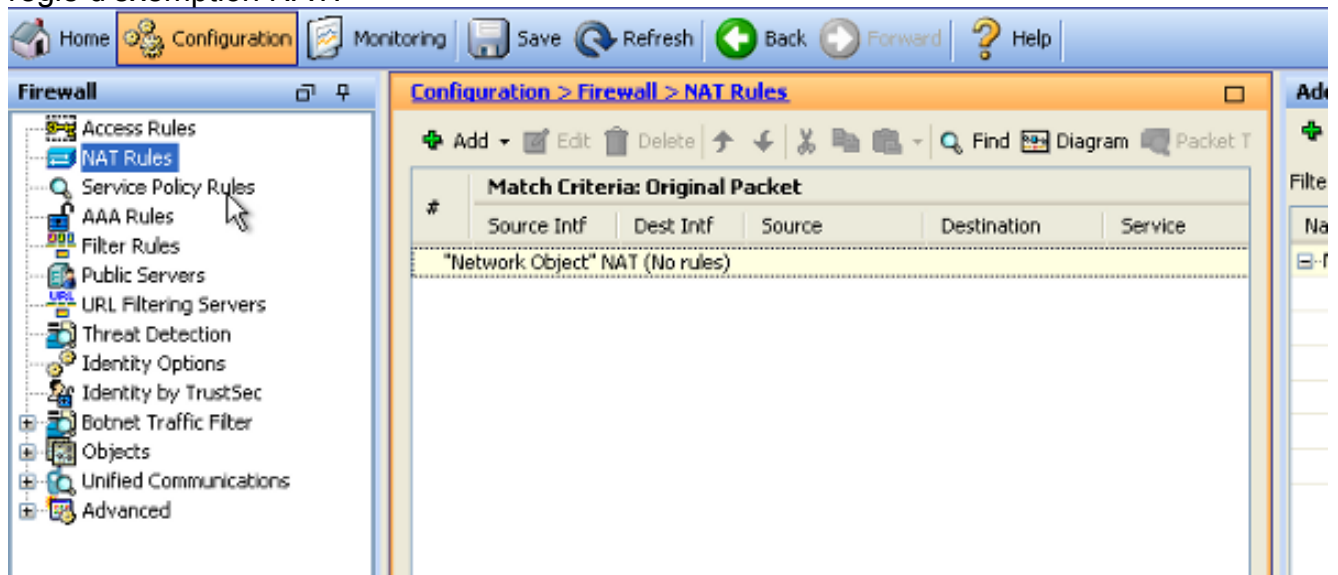
NAT Exempt est une fonctionnalité utile où les utilisateurs internes essaient d'accéder à un hôte/serveur VPN distant ou à un hôte/serveur hébergé derrière toute autre interface de l'ASA

sans effectuer de NAT. Pour ce faire, le serveur interne, qui a une adresse IP privée, peut être traduit en identité vers lui-même et qui à son tour est autorisé à accéder à la destination qui effectue une NAT.

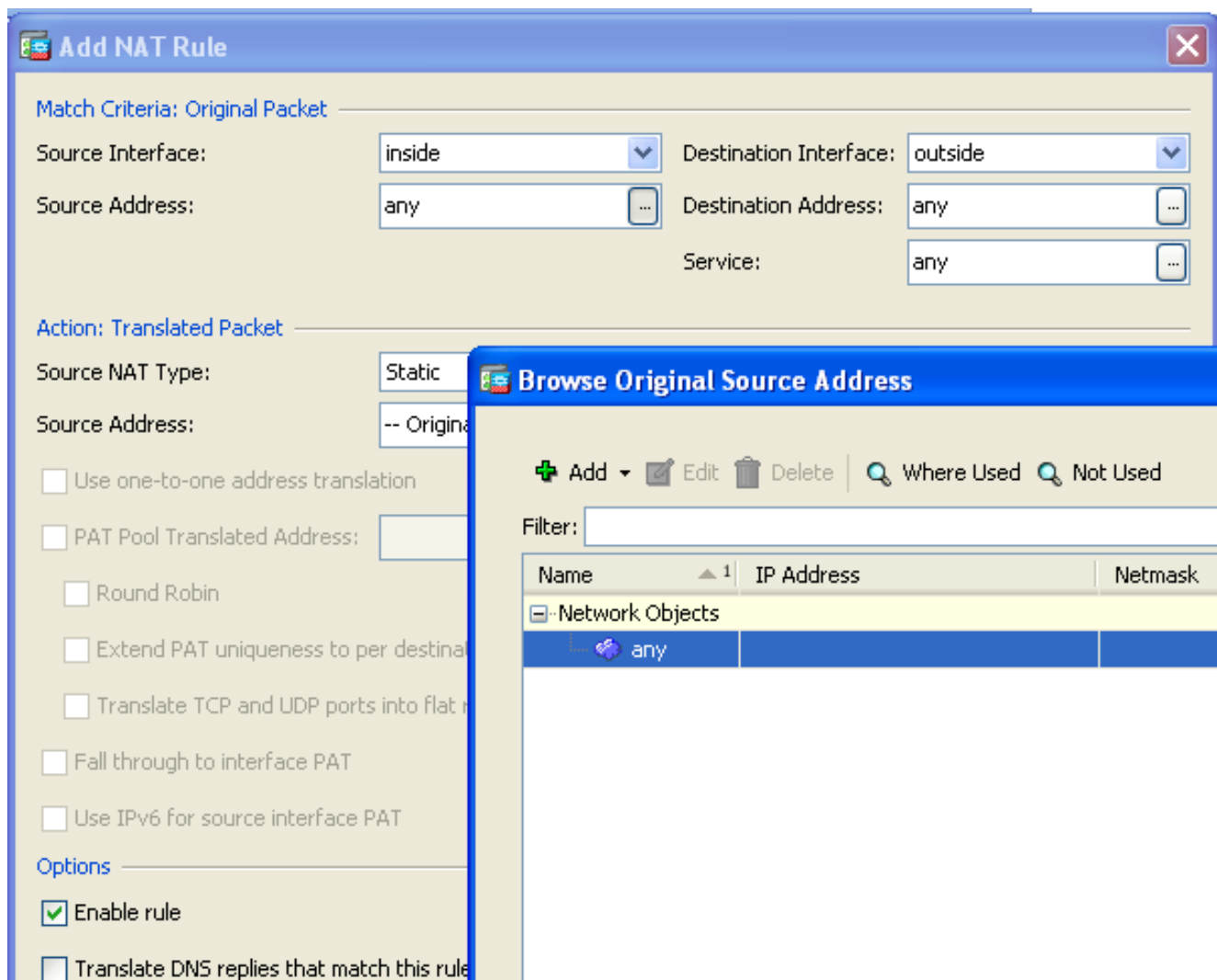
Dans cet exemple, l'hôte interne 172.16.11.15 doit accéder au serveur VPN distant 172.20.21.15.

Complétez ces étapes afin de permettre aux hôtes internes d'accéder au réseau VPN distant avec la réalisation d'une NAT :

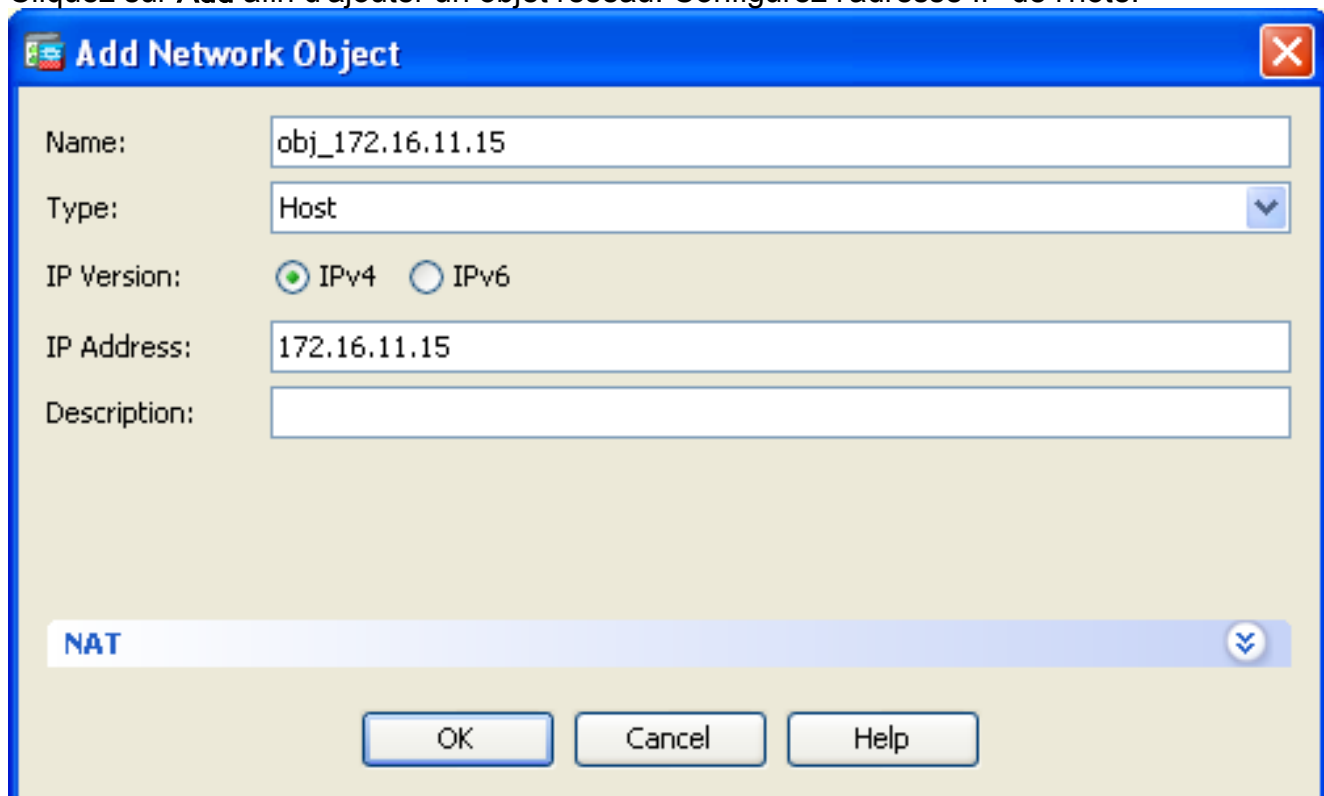
1. Choisissez **Configuration > Firewall > NAT Rules**. Cliquez sur **Add** afin de configurer une règle d'exemption NAT.



2. Dans les listes déroulantes Interface source et Interface de destination, sélectionnez les interfaces appropriées. Dans le champ Adresse source, sélectionnez l'entrée appropriée.



3. Cliquez sur **Add** afin d'ajouter un objet réseau. Configurez l'adresse IP de l'hôte.



4. De même, parcourez l'adresse de destination. Cliquez sur **Add** afin d'ajouter un objet réseau.

Configurez l'adresse IP de l'hôte.

Add Network Object

Name: obj_172.20.21.15

Type: Host

IP Version: IPv4 IPv6

IP Address: 172.20.21.15

Description:

NAT

OK Cancel Help

5. Sélectionnez les objets Adresse source et Adresse de destination configurés. Cochez les cases **Désactiver le proxy ARP sur l'interface de sortie** et **Rechercher la table de routage pour localiser l'interface de sortie**. Click OK.

Add NAT Rule

Match Criteria: Original Packet

Source Interface: Destination Interface:

Source Address: Destination Address:

Service:

Action: Translated Packet

Source NAT Type:

Source Address: Destination Address:

Use one-to-one address translation

PAT Pool Translated Address: Service:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT

Use IPv6 for source interface PAT Use IPv6 for destination interface PAT

Options

Enable rule

Translate DNS replies that match this rule

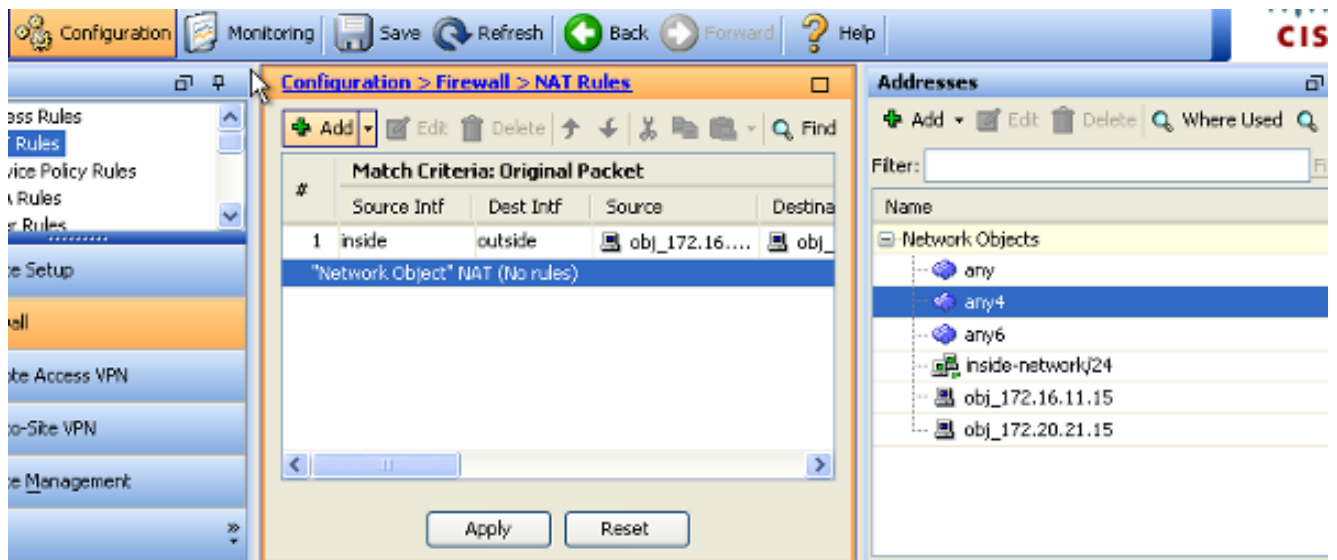
Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Direction:

Description:

6. Cliquez sur **Apply** pour que les modifications prennent effet.



Il s'agit de la sortie CLI équivalente pour la configuration NAT d'identité ou d'exemption NAT :

```
object network obj_172.16.11.15
host 172.16.11.15
object network obj_172.20.21.15
host 172.20.21.15
```

```
nat (inside,outside) source static obj_172.16.11.15 obj_172.16.11.15
destination static obj_172.20.21.15 obj_172.20.21.15 no-proxy-arp route-lookup
```

Redirection de port (transfert) avec statique

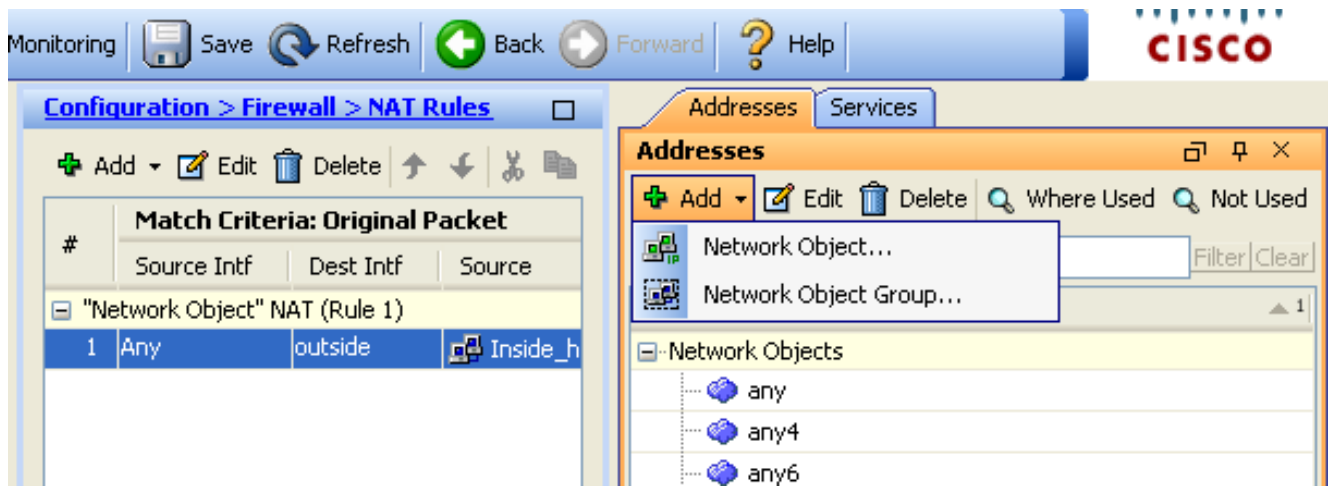
Le transfert de port ou la redirection de port est une fonctionnalité utile où les utilisateurs externes tentent d'accéder à un serveur interne sur un port spécifique. Pour ce faire, le serveur interne, qui a une adresse IP privée, peut être traduit en une adresse IP publique qui à son tour est autorisée à accéder au port spécifique.

Dans cet exemple, l'utilisateur externe souhaite accéder au serveur SMTP 203.0.113.15 sur le port 25. Cette opération s'effectue en deux étapes :

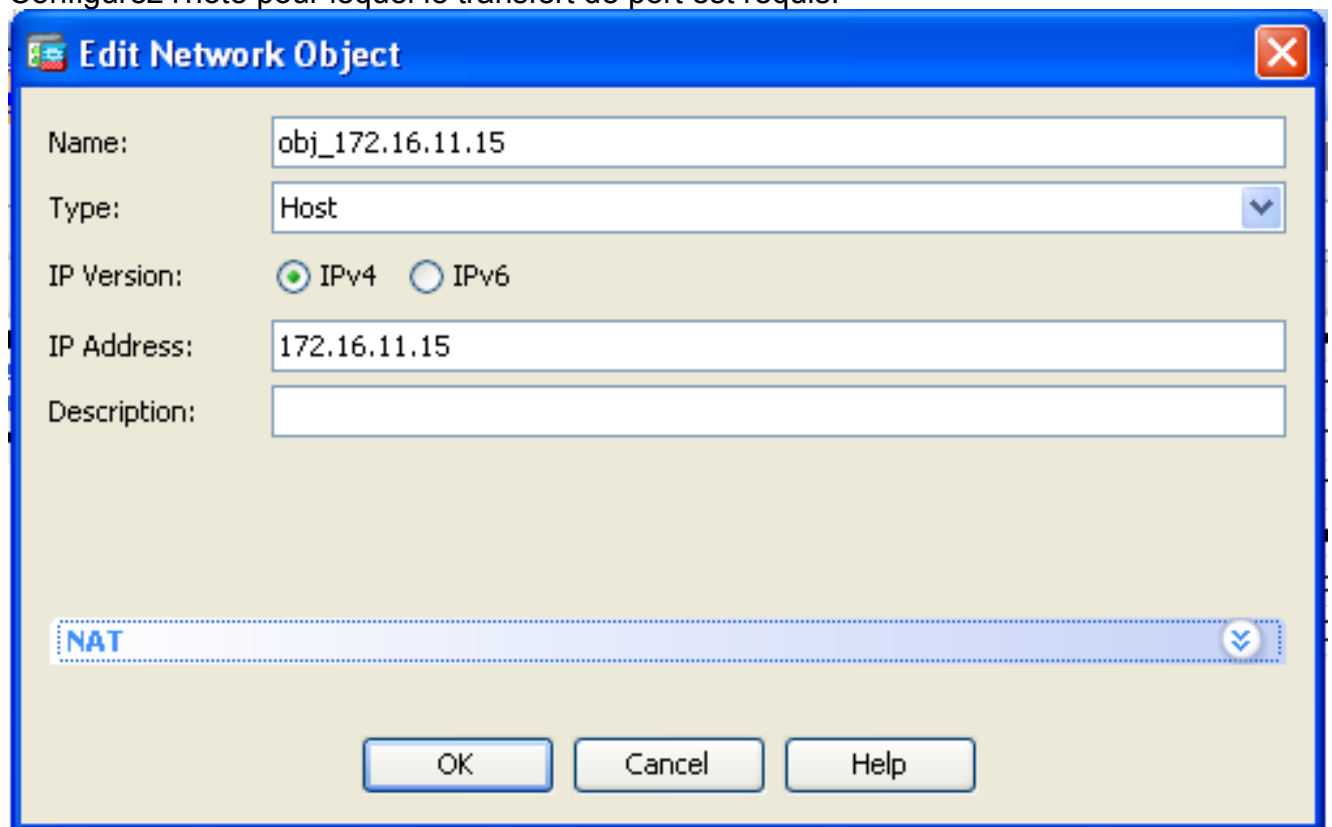
1. Traduisez le serveur de messagerie interne, 172.16.11.15 sur le port 25, en adresse IP publique, 203.0.113.15 sur le port 25.
2. Autorisez l'accès au serveur de messagerie public, 203.0.113.15 au port 25.

Lorsque l'utilisateur externe tente d'accéder au serveur, 203.0.113.15 sur le port 25, ce trafic est redirigé vers le serveur de messagerie interne, 172.16.11.15 sur le port 25.

1. Choisissez **Configuration > Firewall > NAT Rules**. Cliquez sur **Add**, puis choisissez **Network Object** afin de configurer une règle NAT statique.



2. Configurez l'hôte pour lequel le transfert de port est requis.



3. Développez NAT. Cochez la case **Ajouter des règles de traduction automatique d'adresses**. Dans la liste déroulante Type, sélectionnez **Static**. Dans le champ Translated Addr, saisissez l'adresse IP. Cliquez sur **Advanced** afin de sélectionner le service et les interfaces source et de destination.

Edit Network Object [X]

Name:

Type:

IP Version: IPv4 IPv6

IP Address:

Description:

NAT [^]

Add Automatic Address Translation Rules

Type:

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

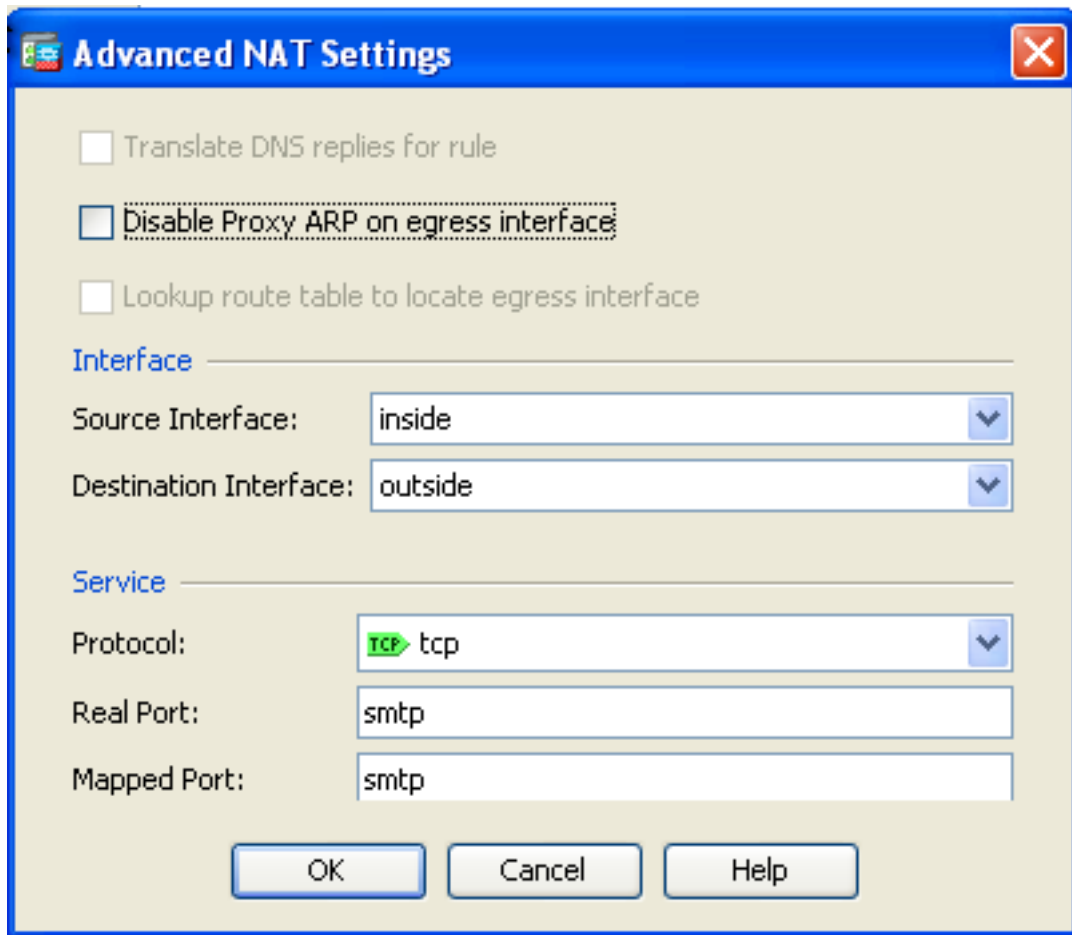
Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

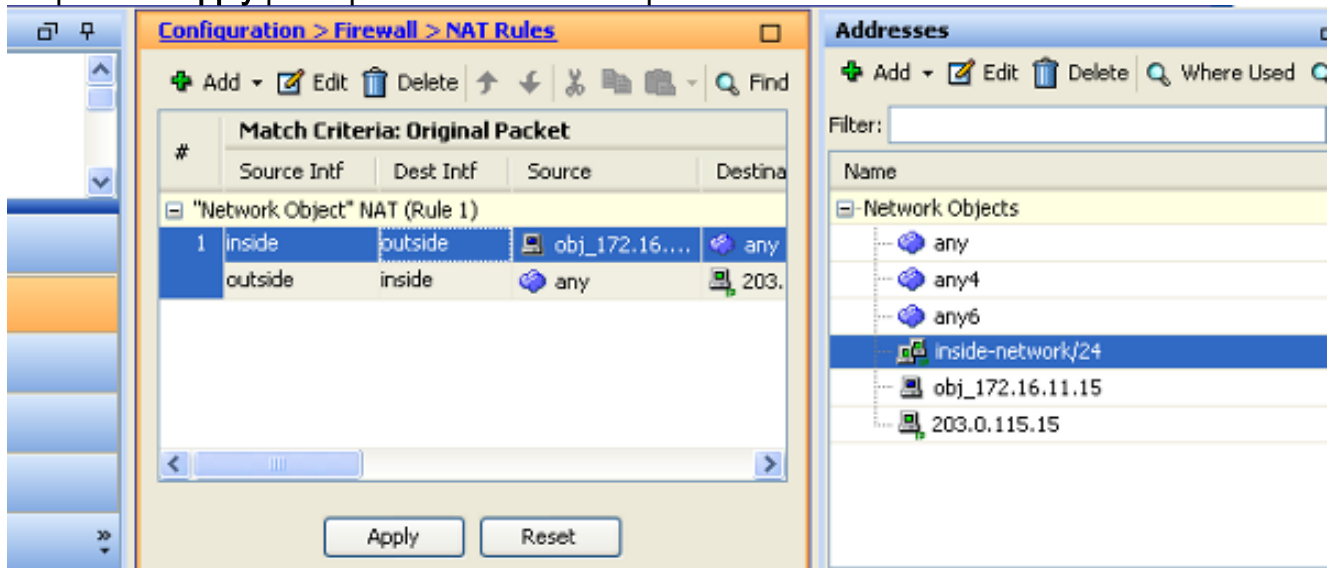
Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

4. Dans les listes déroulantes Interface source et Interface de destination, sélectionnez les interfaces appropriées. Configurez le service. Click OK.



5. Cliquez sur **Apply** pour que les modifications prennent effet.



Voici la sortie de l'interface de ligne de commande équivalente pour cette configuration NAT :

```
object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.113.15 service tcp smtp smtp
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Certaines commandes d'affichage (« show ») sont offertes par l'outil « Cisco CLI Analyzer »

réservé aux clients inscrits. Utilisez cet outil pour obtenir une analyse des rapports produits par ces commandes.

Accéder à un site Web via HTTP à l'aide d'un navigateur Web. Cet exemple utilise un site qui est hébergé sur 198.51.100.100. Si la connexion réussit, ce résultat peut être vu sur l'interface de ligne de commande ASA.

Connexion

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 172.16.11.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

L'ASA est un pare-feu avec état et le trafic de retour du serveur Web est autorisé à traverser le pare-feu car il correspond à une *connexion* dans la table de connexion du pare-feu. Le trafic correspondant à une connexion préexistante est autorisé à traverser le pare-feu sans être bloqué par une liste de contrôle d'accès d'interface.

Dans la sortie précédente, le client sur l'interface interne a établi une connexion à l'hôte 198.51.100.100 à partir de l'interface externe. Cette connexion se fait avec le protocole TCP et est inactive depuis six secondes. Les indicateurs de connexion précisent l'état actuel de la connexion. Pour plus d'informations sur les indicateurs de connexion, consultez [ASA TCP Connection Flags](#).

Syslog

```
ASA(config)# show log | in 172.16.11.5
```

```
Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
172.16.11.5/58799 to outside:203.0.113.2/58799
```

```
Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:172.16.11.5/58799 (203.0.113.2/58799)
```

Le pare-feu de l'ASA génère des SYSLOG pendant le fonctionnement normal. Les SYSLOG varient en verbosité selon la configuration de la journalisation. Le résultat montre deux syslog qui sont vus au niveau six, ou le niveau 'informationnel'.

Dans cet exemple, deux SYSLOG sont générés. Le premier est un message de journal qui indique que le pare-feu a créé une traduction, en particulier une traduction TCP dynamique (PAT). Il indique l'adresse IP source et le port, ainsi que l'adresse IP et le port traduits, lorsque le trafic passe des interfaces internes aux interfaces externes.

Le deuxième SYSLOG indique que le pare-feu a établi une connexion dans sa table de connexions précisément pour ce trafic, entre le client et le serveur. Si le pare-feu a été configuré afin de bloquer cette tentative de connexion, ou si un autre facteur a empêché la création de cette connexion (contraintes de ressources ou erreur de configuration possible), le pare-feu ne générerait pas de journal indiquant que la connexion a été créée. Au lieu de cela, il consigne une raison pour laquelle la connexion est refusée ou une indication sur le facteur qui a empêché la création de la connexion.

Packet Tracer

```
ASA(config)# packet-tracer input inside tcp 172.16.11.5 1234 198.51.100.100 80
```

```
--Omitted--
```

```
Result:
```

```
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

La fonctionnalité Packet Tracer sur l'ASA vous permet de spécifier un paquet *simulé* et de voir toutes les étapes, vérifications et fonctions que le pare-feu traverse quand il traite le trafic. Avec cet outil, il est utile d'identifier un exemple de trafic que vous pensez *pouvoir* être autorisé à traverser le pare-feu, et d'utiliser ce 5-tupple afin de simuler le trafic. Dans l'exemple précédent, Packet Tracer est utilisé pour simuler une tentative de connexion qui répond aux critères suivants :

- Le paquet simulé arrive à l'intérieur.
- Le protocole utilisé est TCP.
- L'adresse IP du client simulé est 172.16.11.5.
- Le client envoie le trafic provenant du port 1234.
- Le trafic est destiné à un serveur ayant l'adresse IP 198.51.100.100.
- Le trafic est destiné au port 80.

Notez que la commande ne mentionne pas l'interface externe. C'est par la conception de Packet Tracer. L'outil vous indique comment le pare-feu traite ce type de tentative de connexion et indiquera comment il l'acheminera et à partir de quelle interface. Pour plus d'informations sur Packet Tracer, consultez [Tracer des paquets avec Packet Tracer](#).

Saisir

Appliquer la capture

```
ASA# capture capin interface inside match tcp host 172.16.11.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100
```

```
ASA#show capture capin
```

```
3 packets captured
```

```
1: 11:31:23.432655 172.16.11.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 172.16.11.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 172.16.11.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768
```

```
ASA#show capture capout
```

```
3 packets captured
```

```
1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
```

```
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

Le pare-feu ASA peut capturer le trafic entrant ou sortant de ses interfaces. Cette fonctionnalité de capture est fantastique, car elle permet de prouver de manière définitive si le trafic arrive à un pare-feu ou en sort. L'exemple précédent a montré la configuration de deux captures nommées capin et capout sur les interfaces interne et externe respectivement. Les commandes de capture utilisaient le mot clé match, qui vous permet d'être précis sur le trafic que vous souhaitez capturer.

Pour le chapeau de capture, vous avez indiqué que vous vouliez faire correspondre le trafic vu sur l'interface interne (entrée ou sortie) qui correspond à l'hôte TCP 172.16.11.5, l'hôte 198.51.100.100. En d'autres termes, vous voulez capturer tout trafic TCP envoyé de l'hôte 172.16.11.5 à l'hôte 198.51.100.100 ou vice versa. L'utilisation du mot-clé match permet au pare-feu de capter ce trafic dans les deux sens. La commande capture définie pour l'interface externe ne fait pas référence à l'adresse IP du client interne, car le pare-feu effectue la PAT sur cette adresse IP du client. Par conséquent, vous ne pouvez pas associer cette adresse IP au client. Plutôt, cet exemple utilise any pour indiquer que toutes les adresses IP possibles correspondent à cette condition.

Une fois les captures configurées, vous tenteriez d'établir à nouveau une connexion et continueriez à afficher les captures avec la commande **show capture <capture_name>**. Dans cet exemple, vous pouvez voir que le client a pu se connecter au serveur comme le montre la connexion TCP en trois étapes vue dans les captures.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Exemple de configuration ASA Syslog](#)
- [Exemple de configuration de capture de paquets ASA avec CLI et ASDM](#)
- [Support 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.