Configurez l'expédition de port de version 9.x ASA avec NAT

Contenu

Introduction

Ce document explique comment configurer le Port Redirection(Forwarding) et les caractéristiques extérieures de Traduction d'adresses de réseau (NAT) dans la version de logiciel 9.x de l'appliance de sécurité adaptable (ASA), avec l'utilisation du CLI ou de l'Adaptive Security Device Manager (ASDM).

Référez-vous au guide de configuration du Pare-feu ASDM de gamme de Cisco ASA pour information les informations complémentaires.

Conditions préalables

Conditions requises

Référez-vous à configurer la Gestion Access afin de permettre le périphérique à configurer par l'ASDM.

Composants utilisés

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

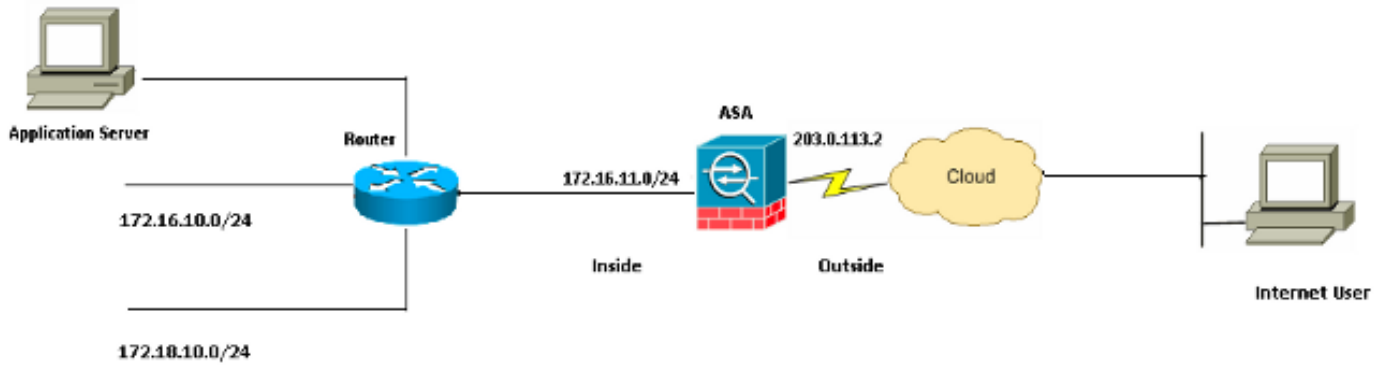
logiciel suivantes :

- Version de logiciel 9.x d'appareils de Sécurité de gamme 5525 de Cisco ASA et plus tard
- Version 7.x et ultérieures ASDM

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.

Configurez

Diagramme du réseau



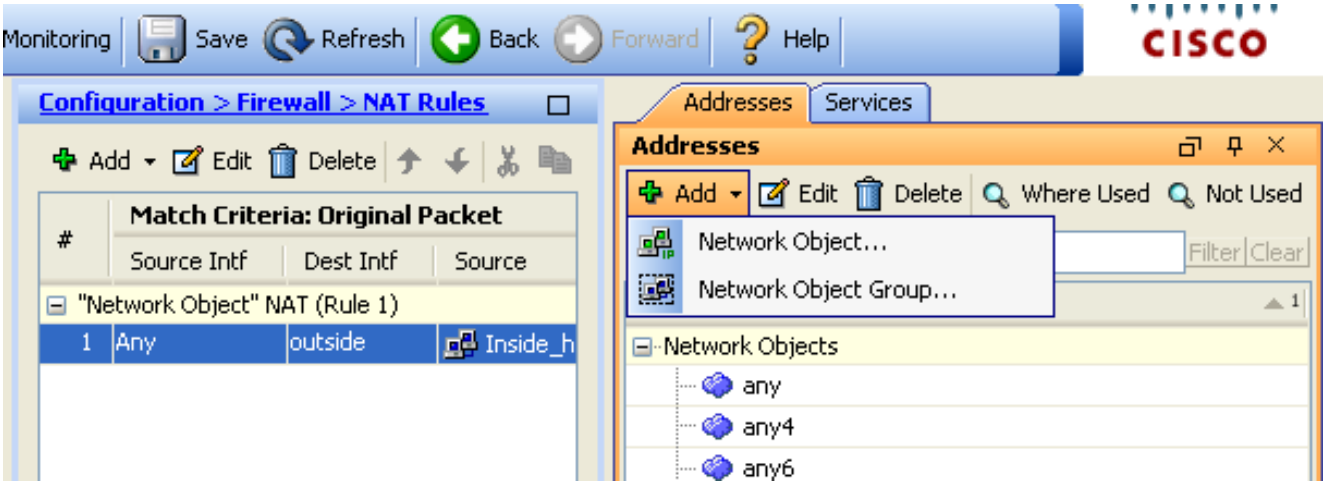
Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Permettez à des hôtes internes Access aux réseaux extérieurs avec PAT

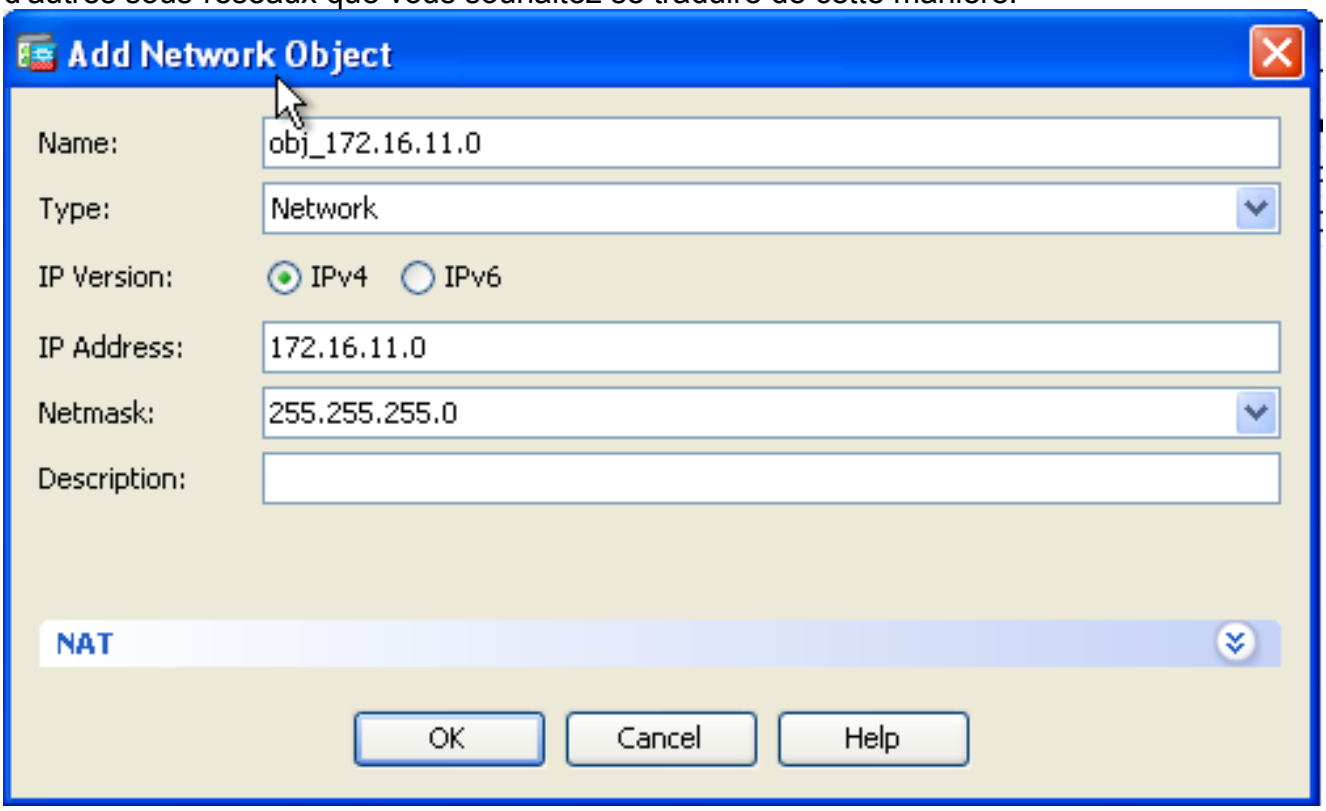
Si vous voulez que les hôtes internes partagent une annonce publique simple pour la traduction, utilisez la translation d'adresses d'adresse du port (PAT). Une des configurations PAT les plus simples comporte la traduction de tous les hôtes internes pour ressembler à l'adresse IP extérieure d'interface. C'est la configuration PAT typique qui est utilisée quand le nombre d'adresses IP routable fournies par l'ISP est limité seulement à quelques uns, ou peut-être juste un.

Terminez-vous ces étapes afin de permettre à des hôtes internes l'accès aux réseaux extérieurs avec PAT :

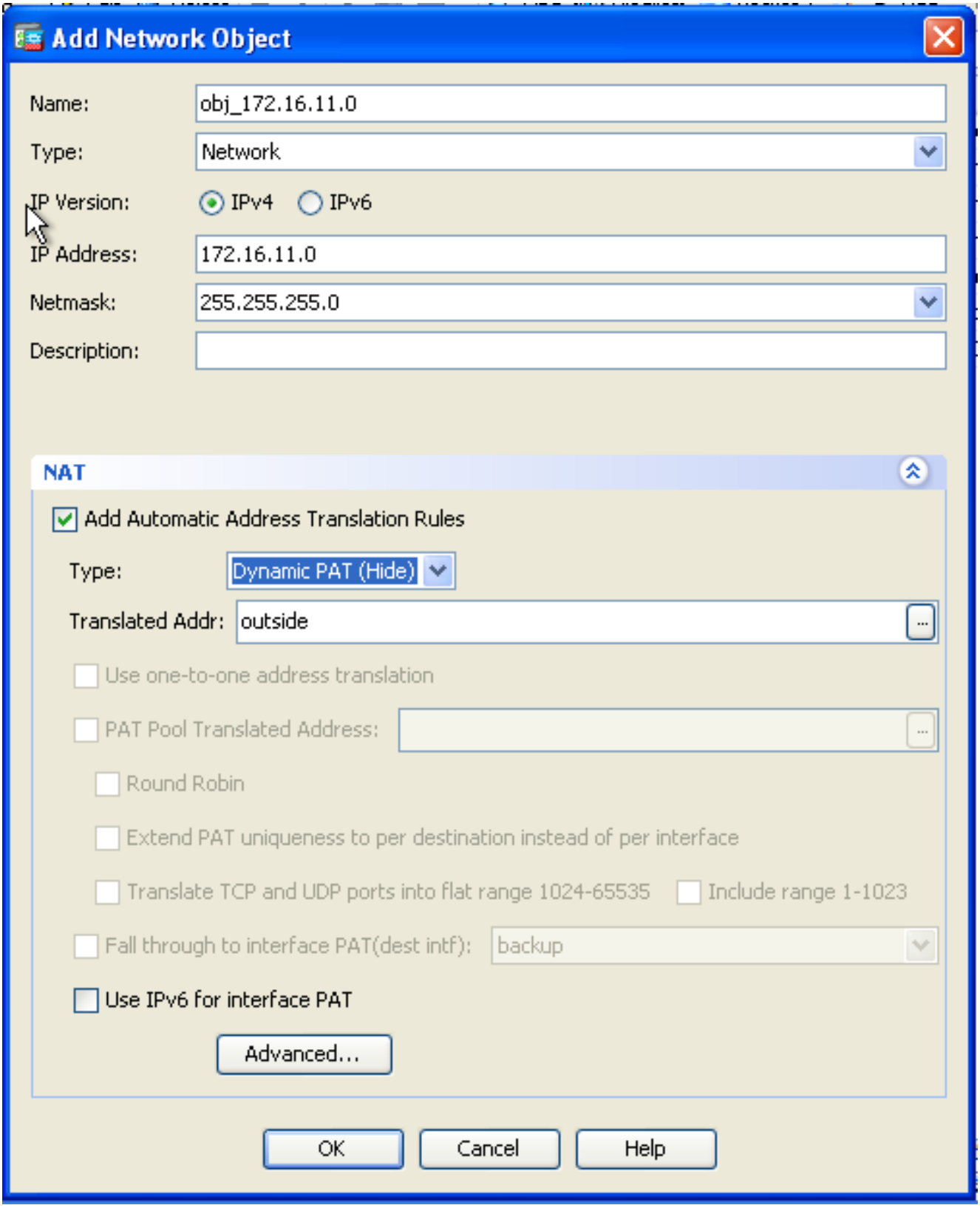
1. Choisissez la **configuration** > le **Pare-feu** > les **règles NAT**. Cliquez sur Add et puis choisissez l'**objet de réseau** afin de configurer une règle NAT dynamique.



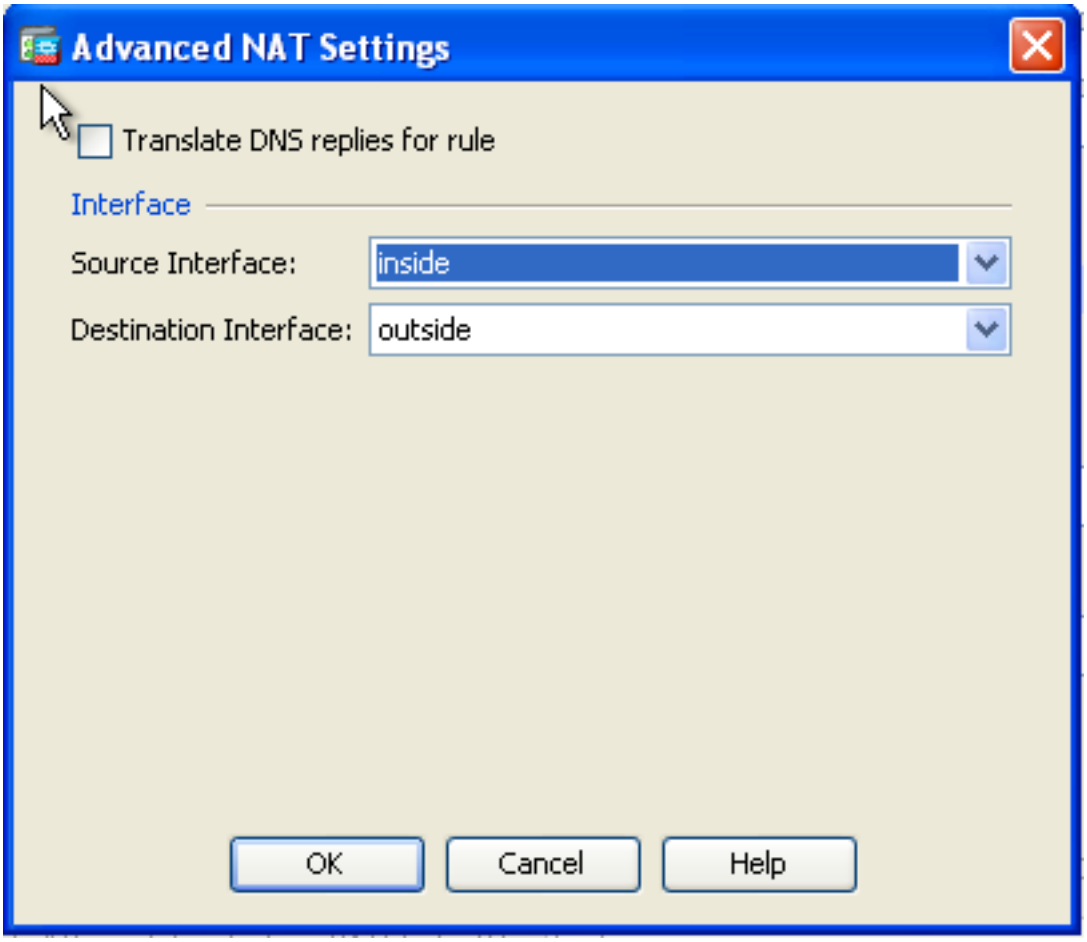
2. Configurez le réseau/hôte/plage pour laquelle **PAT dynamique** est prié. Dans cet exemple, un des sous-réseaux intérieurs a été sélectionné. Ce processus peut être répété pour d'autres sous-réseaux que vous souhaitez se traduire de cette manière.



3. Développez NAT. Cochez la case **automatique de règles de traduction d'adresses d'ajouter**. Dans la liste déroulante de type, choisissez **PAT dynamique (peau)**. Dans le domaine **traduit d'adr**, choisissez l'option de refléter l'interface extérieure. Cliquez sur **Advanced**.



4. Dans les listes déroulantes d'interface de source et d'interface de destination, choisissez les interfaces appropriées. Cliquez sur OK et cliquez sur Apply pour les modifications pour le prendre effet.



C'est le CLI équivalent sorti 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
```

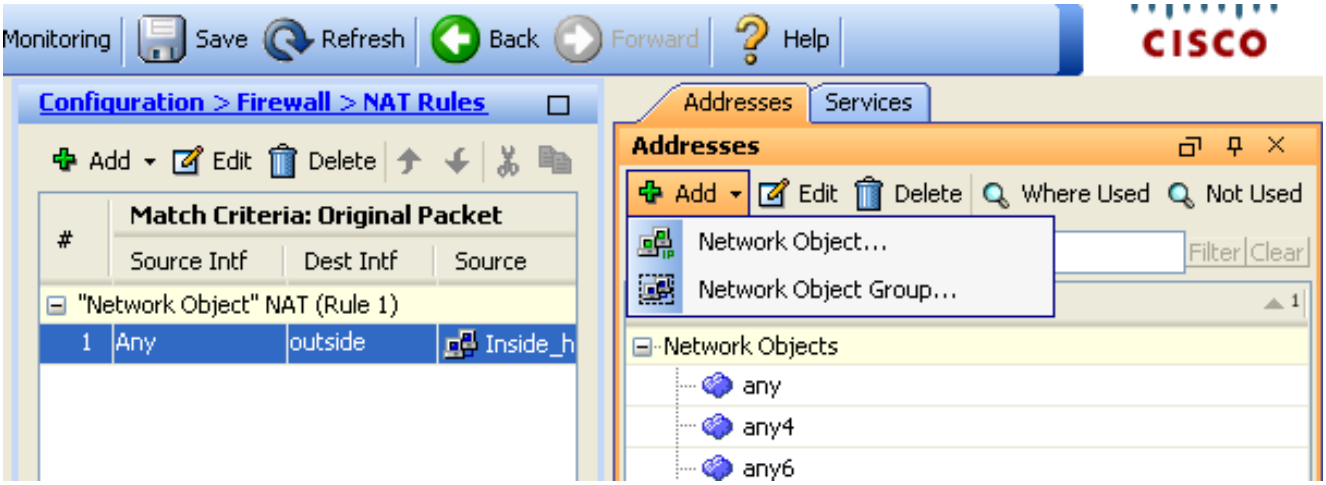
Autoriser les hôtes internes à accéder aux réseaux externes à l'aide de NAT

Vous pourriez permettre à un groupe d'hôtes internes/de réseaux pour accéder au monde extérieur avec la configuration des règles NAT dynamiques. À la différence de PAT, NAT dynamique alloue des adresses traduites d'un groupe d'adresses. En conséquence, un hôte est tracé à sa propre adresse IP traduite et deux hôtes ne peuvent pas partager la même adresse IP traduite.

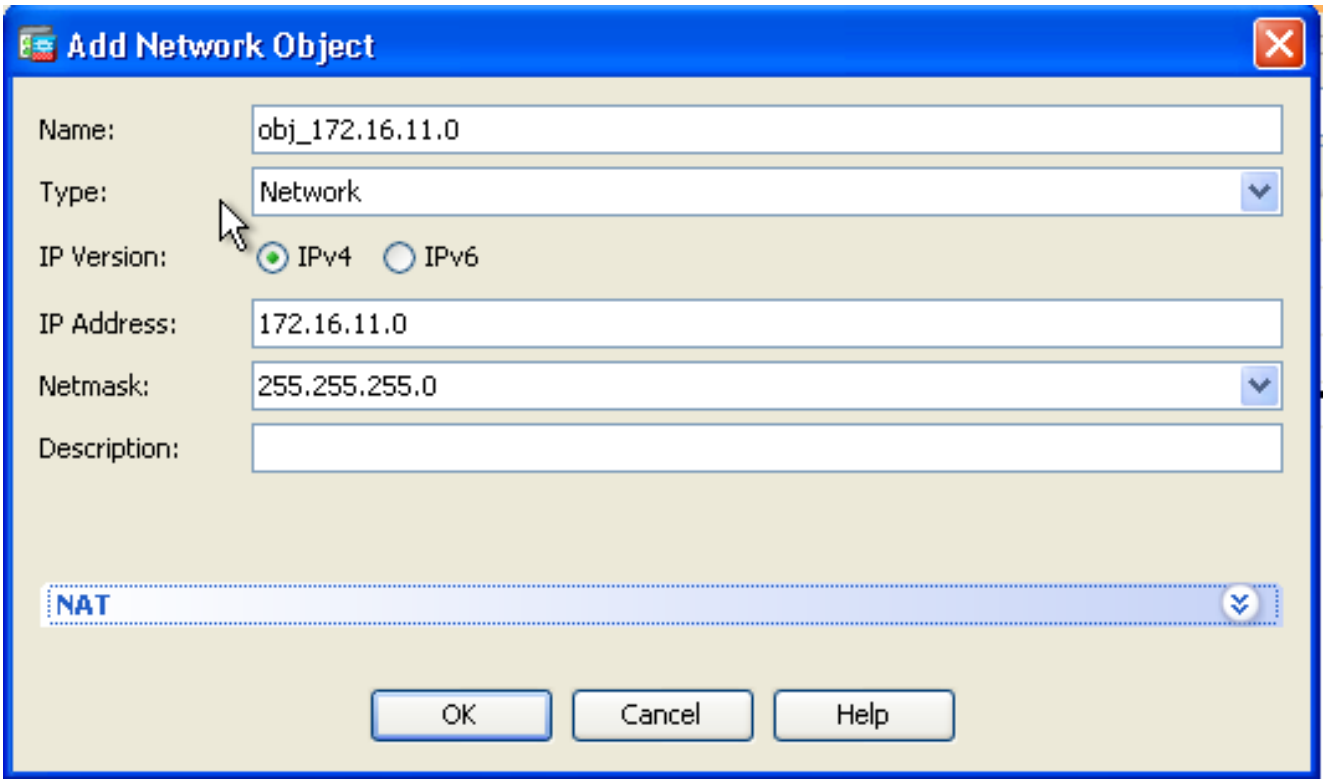
Afin d'accomplir ceci, vous devez sélectionner la vraie adresse des hôtes/des réseaux pour donner l'accès et ils alors doivent être tracés à un groupe d'adresses IP traduites.

Terminez-vous ces étapes afin de permettre à des hôtes internes l'accès aux réseaux extérieurs avec NAT :

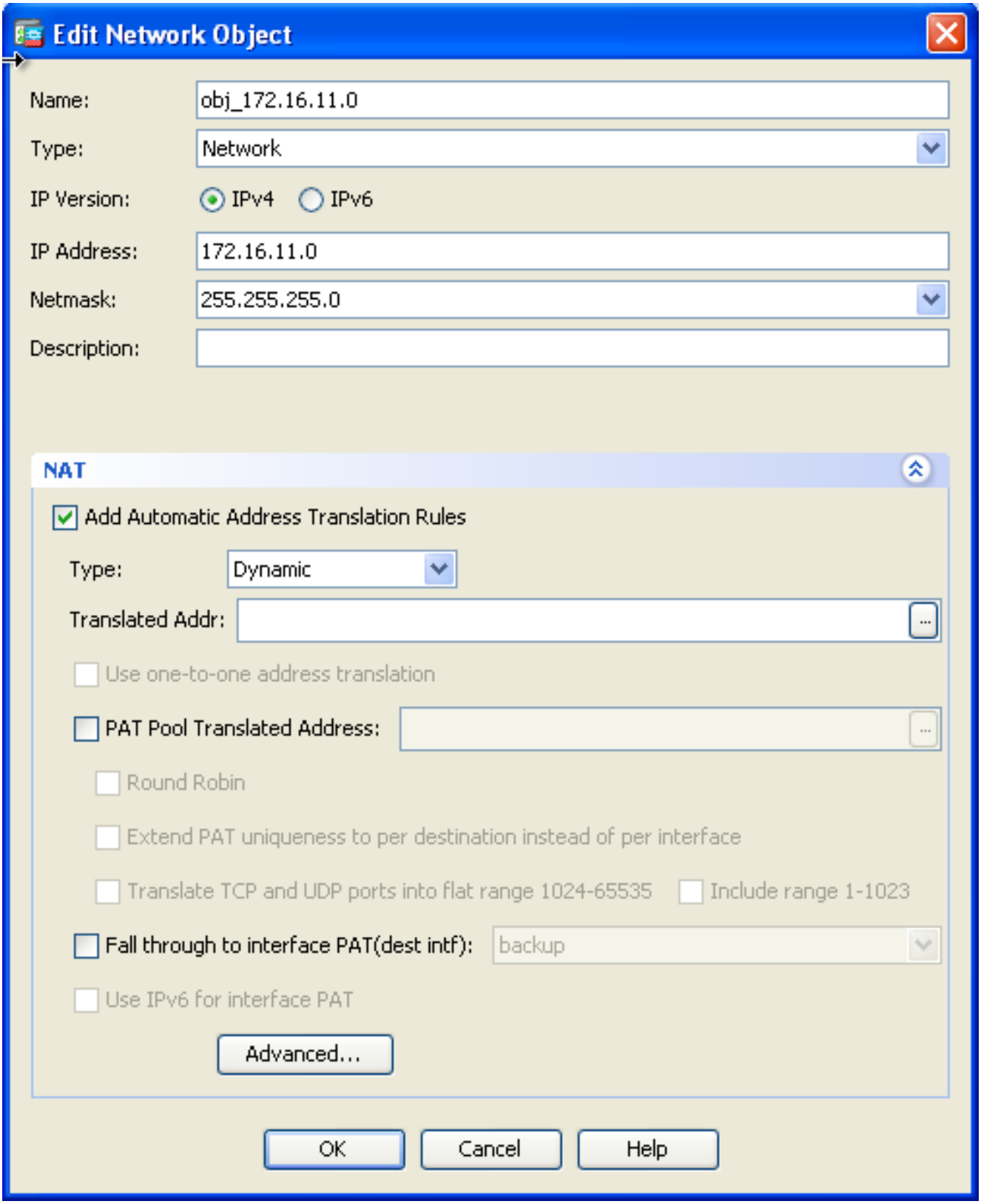
1. Choisissez la **configuration** > le **Pare-feu** > les **règles NAT**. Cliquez sur Add et puis choisissez l'**objet de réseau** afin de configurer une règle NAT dynamique.



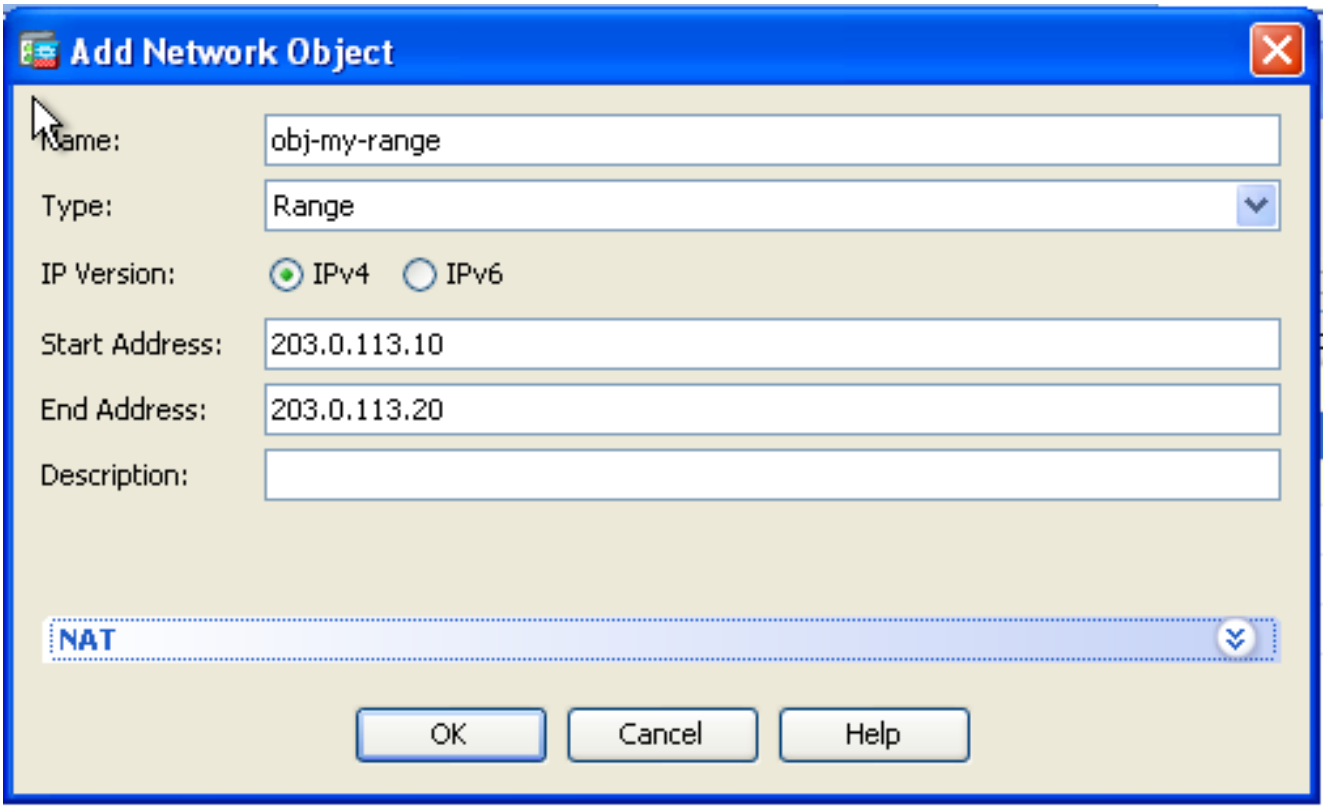
2. Configurez le réseau/hôte/plage pour laquelle PAT dynamique est prié. Dans cet exemple, l'à l'intérieur-*réseau* entier a été sélectionné.



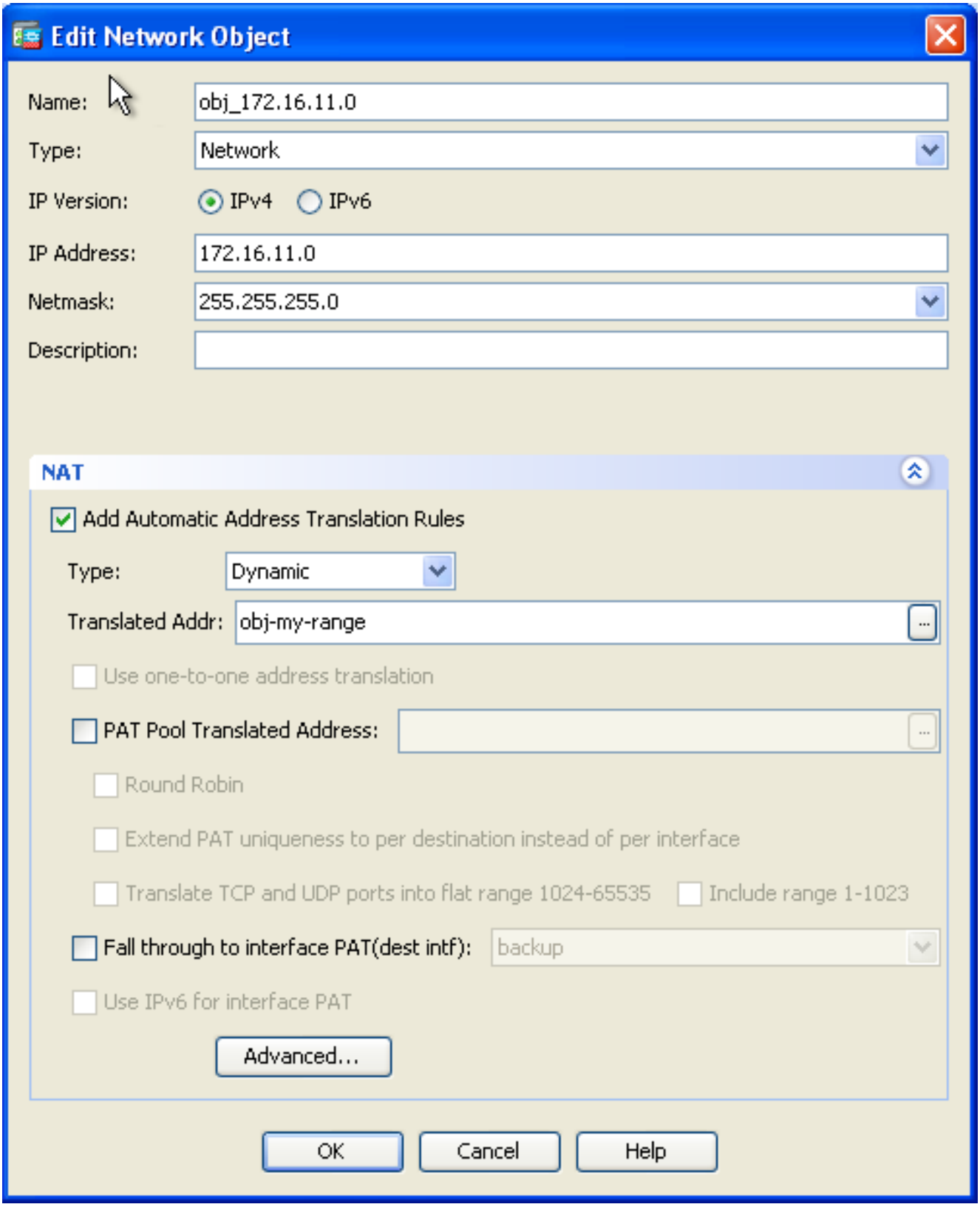
3. Développez NAT. Cochez la case **automatique de règles de traduction d'adresses d'ajouter**. Dans la liste déroulante de type, choisissez **dynamique**. Dans le domaine traduit d'adr, choisissez la sélection appropriée. Cliquez sur **Advanced**.



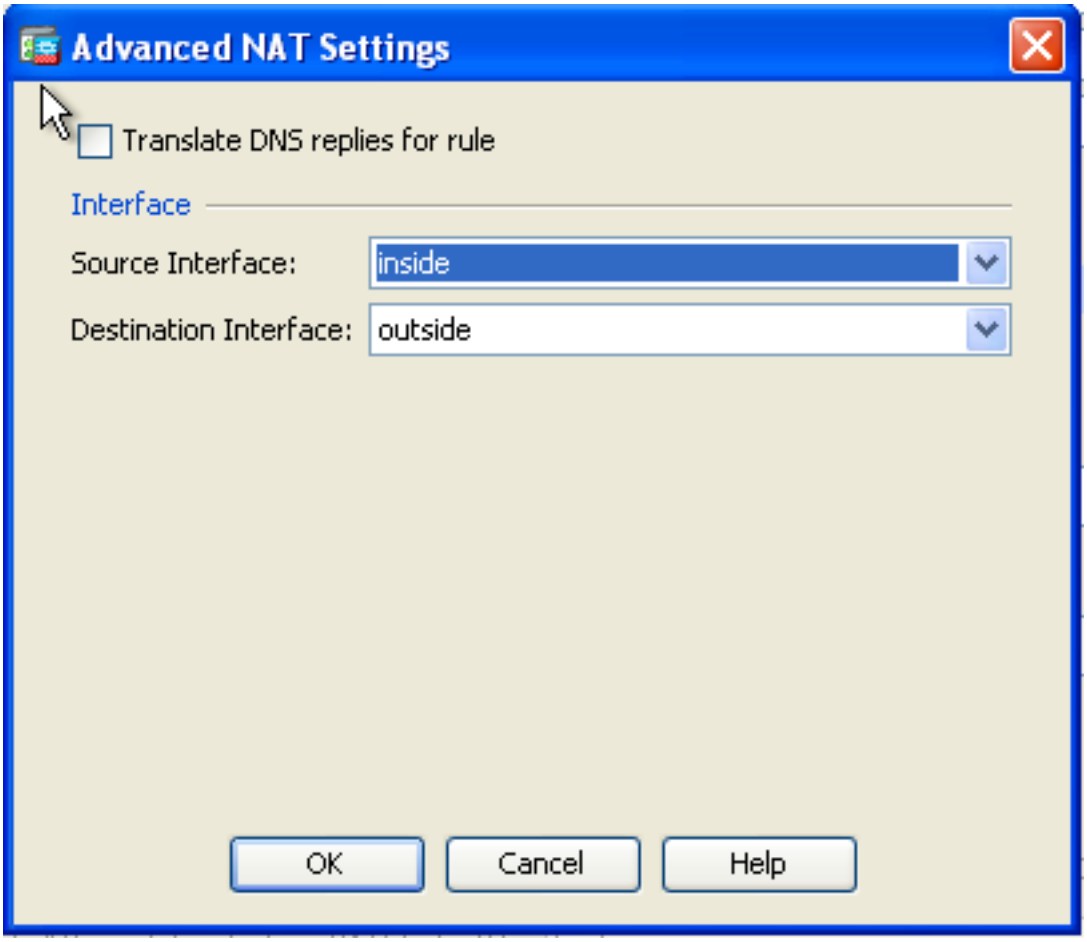
4. Cliquez sur Add pour ajouter l'objet de réseau. Dans la liste déroulante de type, choisissez la **plage**. Dans l'adresse de début et les zones adresses de fin, écrivez les adresses IP commençantes et finissantes de PAT. Cliquez sur **OK**.



5. Dans le domaine traduit d'adr, choisissez l'objet d'adresse. Cliquez sur **avancé** afin de sélectionner la source et les interfaces de destination.



6. Dans les listes déroulantes d'interface de source et d'interface de destination, choisissez les interfaces appropriées. Cliquez sur OK et cliquez sur Apply pour les modifications pour le prendre effet.

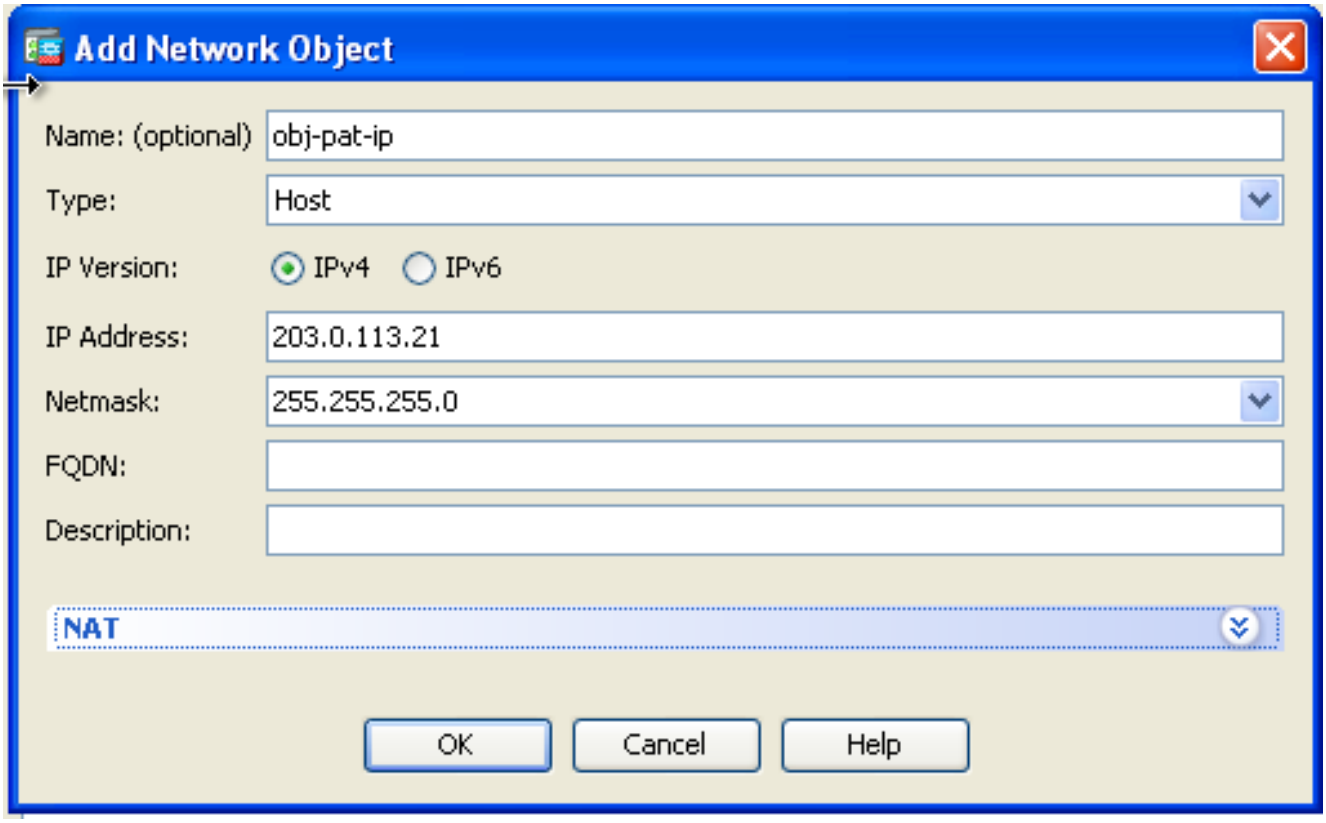


C'est le CLI équivalent sorti pour cette configuration ASDM :

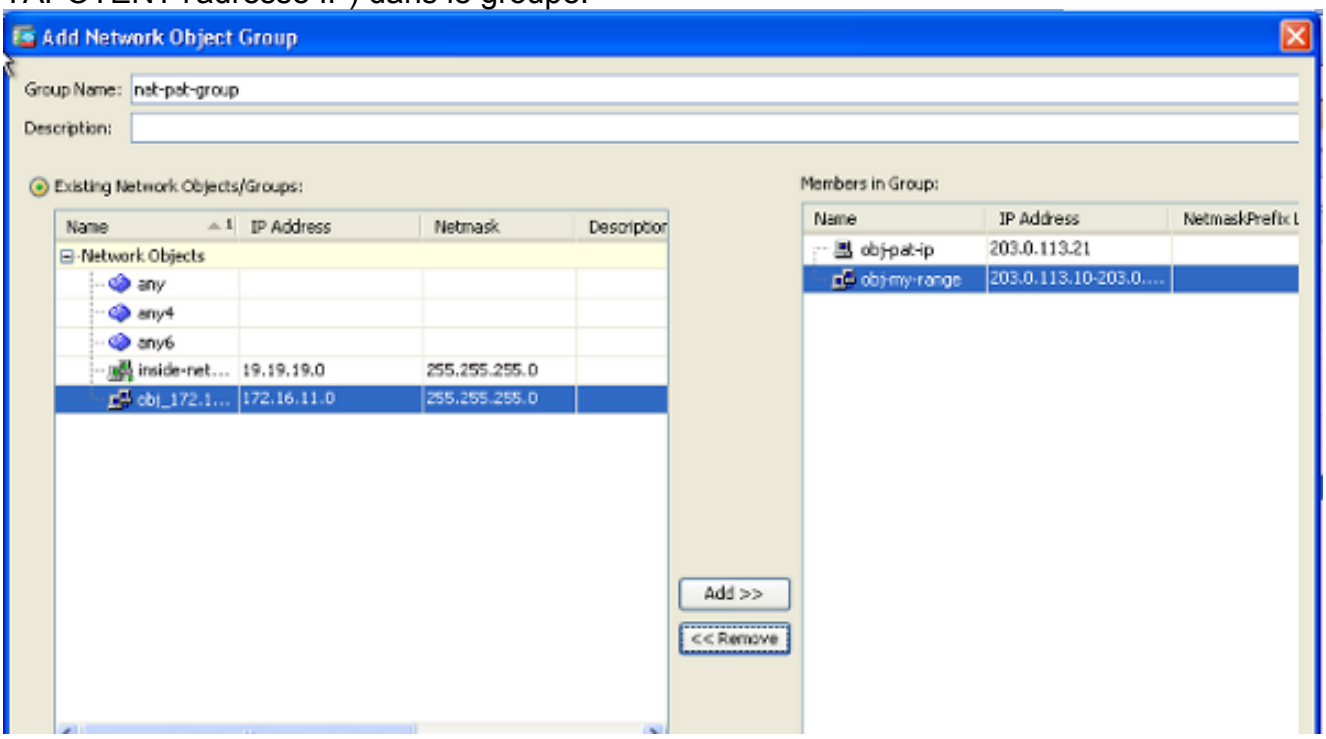
```
object network obj-my-range
range 203.0.113.10 203.0.113.20

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 dans le réseau de 172.16.11.0 obtiendront traduit à n'importe quelle adresse IP du groupe NAT, 203.0.113.10 - 203.0.113.20. Si le groupe tracé a moins d'adresses que le vrai groupe, vous pourriez manquer d'adresses. En conséquence, vous pourriez essayer d'implémenter NAT dynamique avec PAT dynamique de sauvegarde ou vous pourriez essayer de développer le groupe existant.

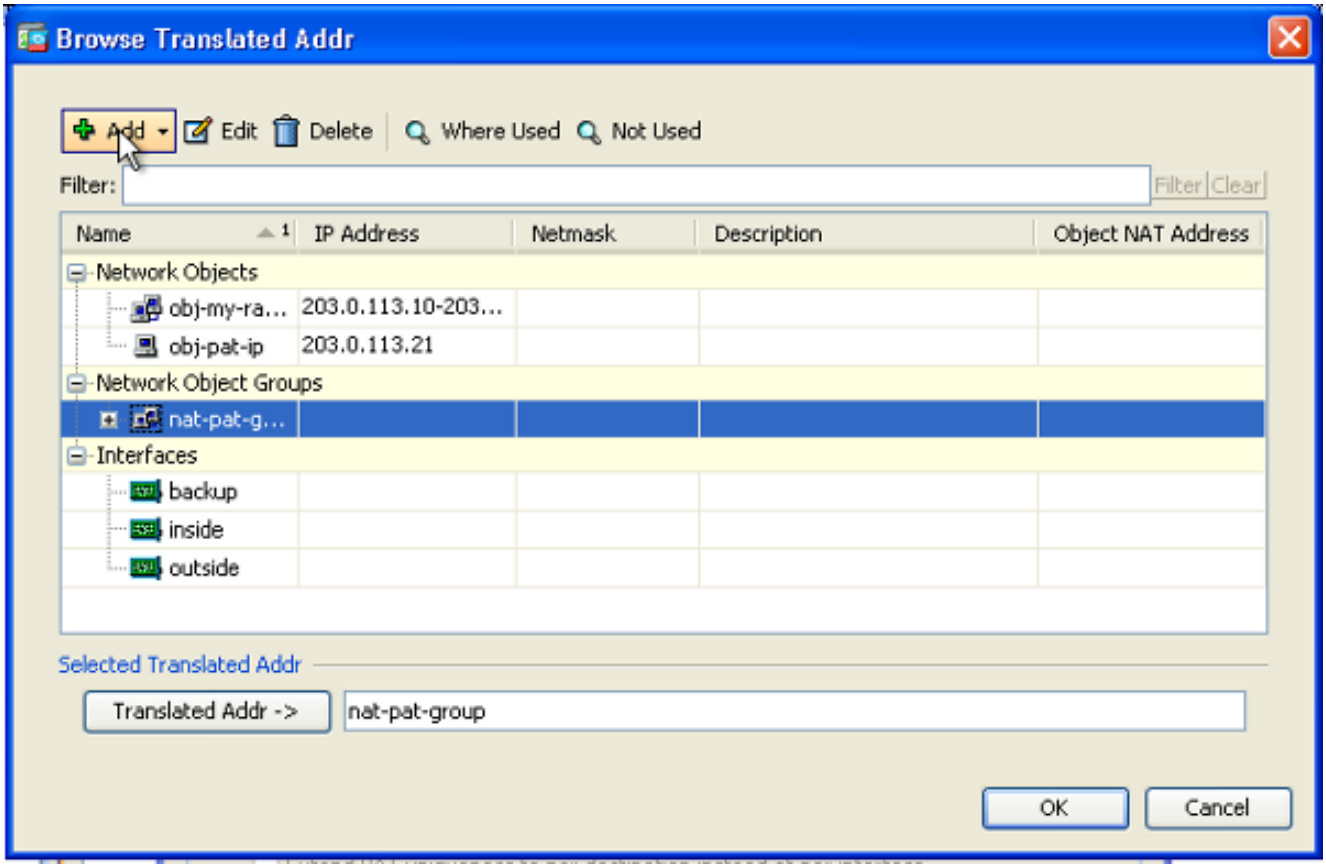
1. Répétez les étapes 1 3 dans la configuration précédente et cliquez sur Add de nouveau afin d'ajouter un objet de réseau. Dans la liste déroulante de type, choisissez l'**hôte**. Dans le champ IP Address, écrivez l'adresse IP de sauvegarde de PAT. Cliquez sur **OK**.



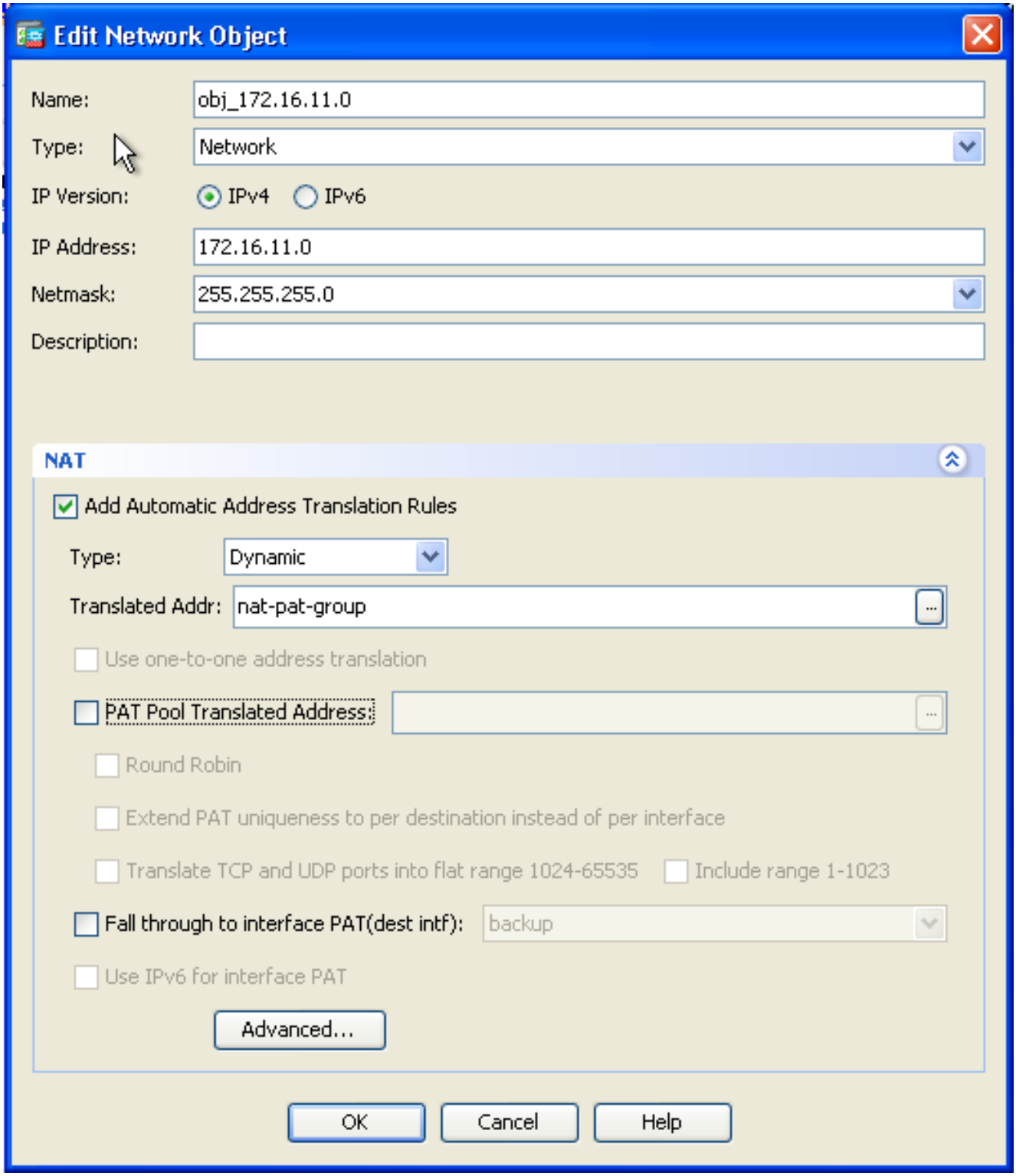
2. Cliquez sur Add pour ajouter un groupe d'objet de réseau. Dans la zone d'identification de groupe, écrivez un nom de groupe et **ajoutez** les deux objets d'adresse (la plage NAT et TAPOTENT l'adresse IP) dans le groupe.



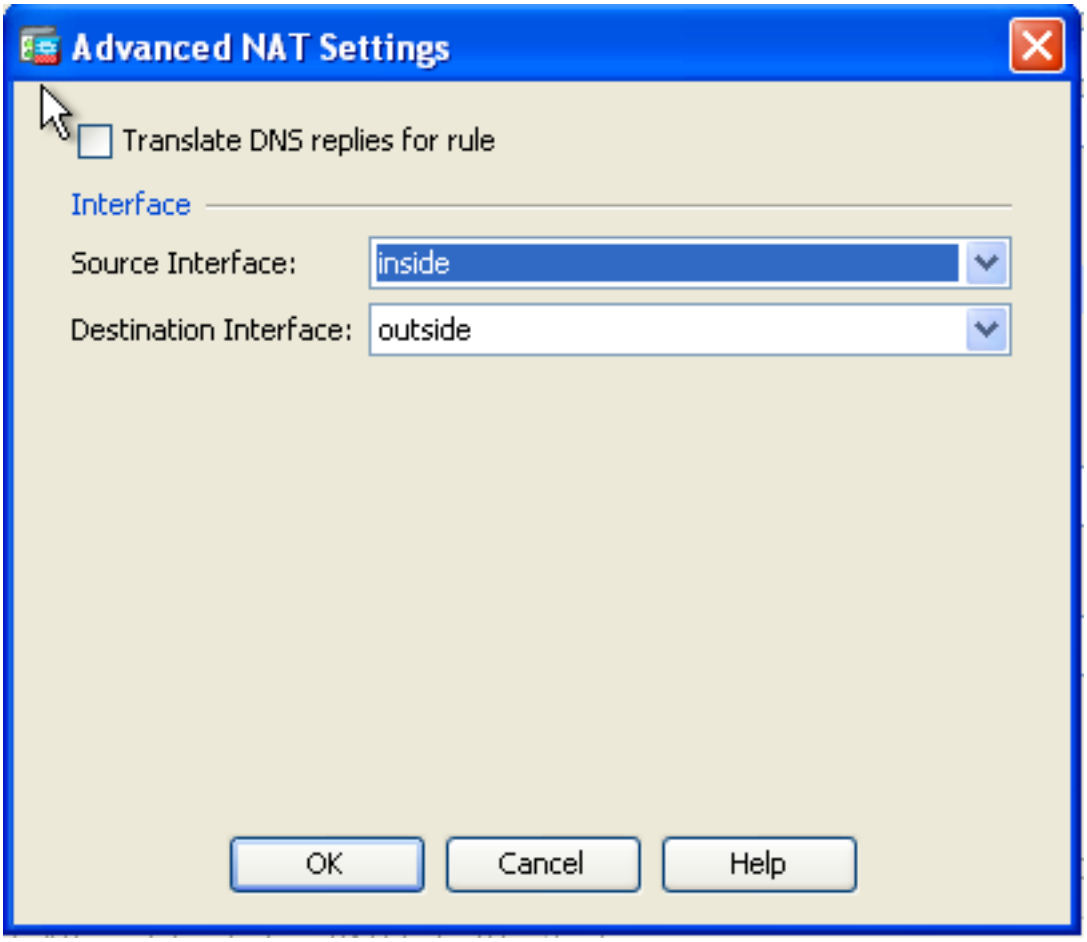
3. Choisissez la règle NAT configurée et changez l'adr traduit pour être « nat-Pat-groupe » du groupe nouvellement configuré (était précédemment la « obj-mon-plage "). Cliquez sur **OK**.



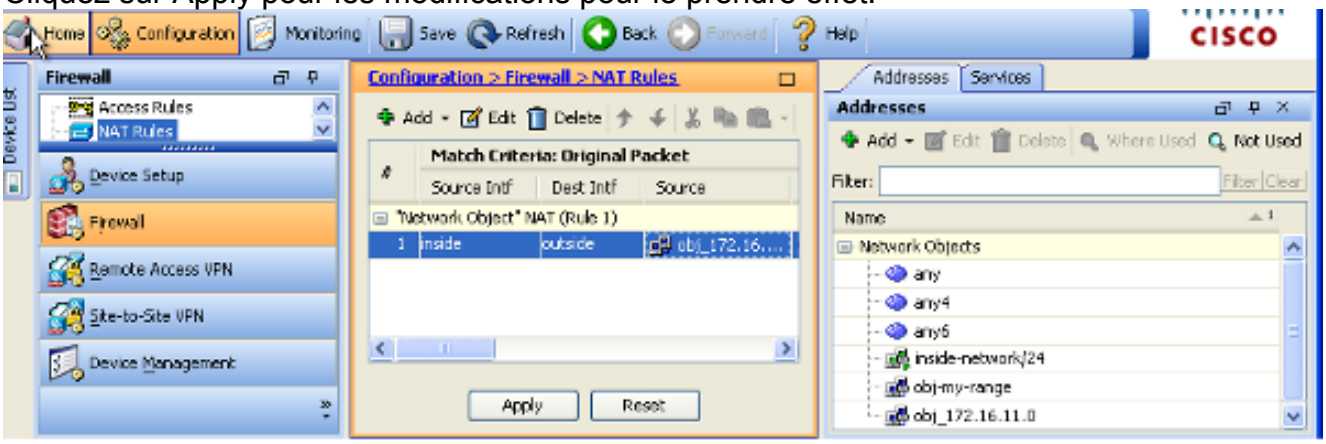
4. Cliquez sur OK afin d'ajouter la règle NAT. Cliquez sur **avancé** afin de sélectionner la source et les interfaces de destination.



5. Dans les listes déroulantes d'interface de source et d'interface de destination, choisissez les interfaces appropriées. Cliquez sur **OK**.



6. Cliquez sur Apply pour les modifications pour le prendre effet.



C'est le CLI équivalent sorti pour cette configuration ASDM :

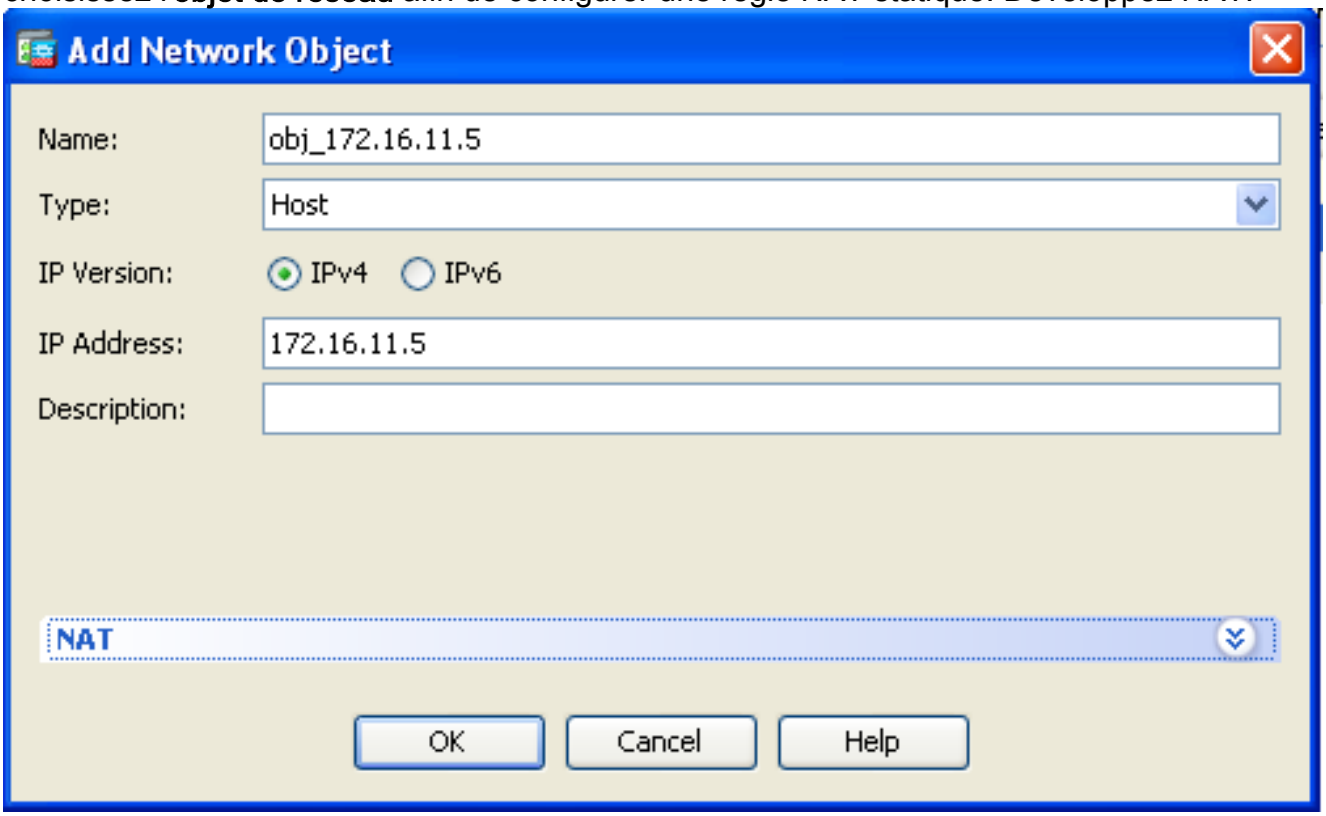
```
object network obj-my-range
range 203.0.113.10 203.0.113.20

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
```

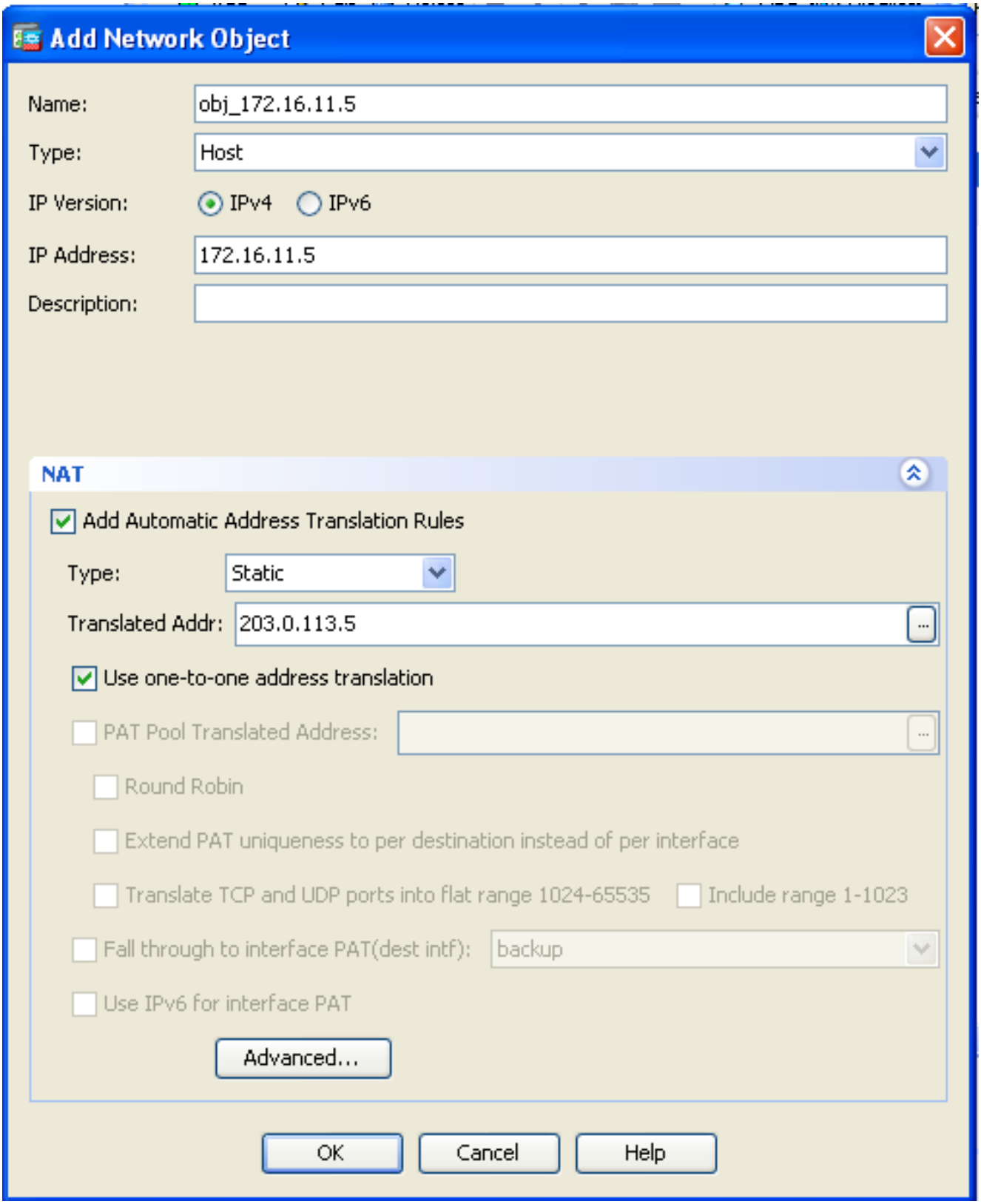
Autoriser les hôtes non approuvés à accéder à des hôtes sur votre réseau approuvé

Ceci peut être réalisé par l'application d'une traduction NAT statique et d'une règle d'accès de permettre ces hôtes. Vous êtes requis de configurer ceci toutes les fois qu'un utilisateur externe voudrait accéder à n'importe quel serveur qui se repose dans votre réseau interne. Le serveur dans le réseau interne aura une adresse IP privée qui n'est pas routable sur l'Internet. En conséquence, vous devez traduire cette adresse IP privée à une adresse IP publique par une règle NAT statique. Supposez que vous avez un serveur interne (172.16.11.5). Afin de faire ce travail, vous devez traduire cette adresse IP du serveur privée à une adresse IP publique. Cet exemple décrit comment implémenter le NAT statique bidirectionnel pour traduire 172.16.11.5 à 203.0.113.5.

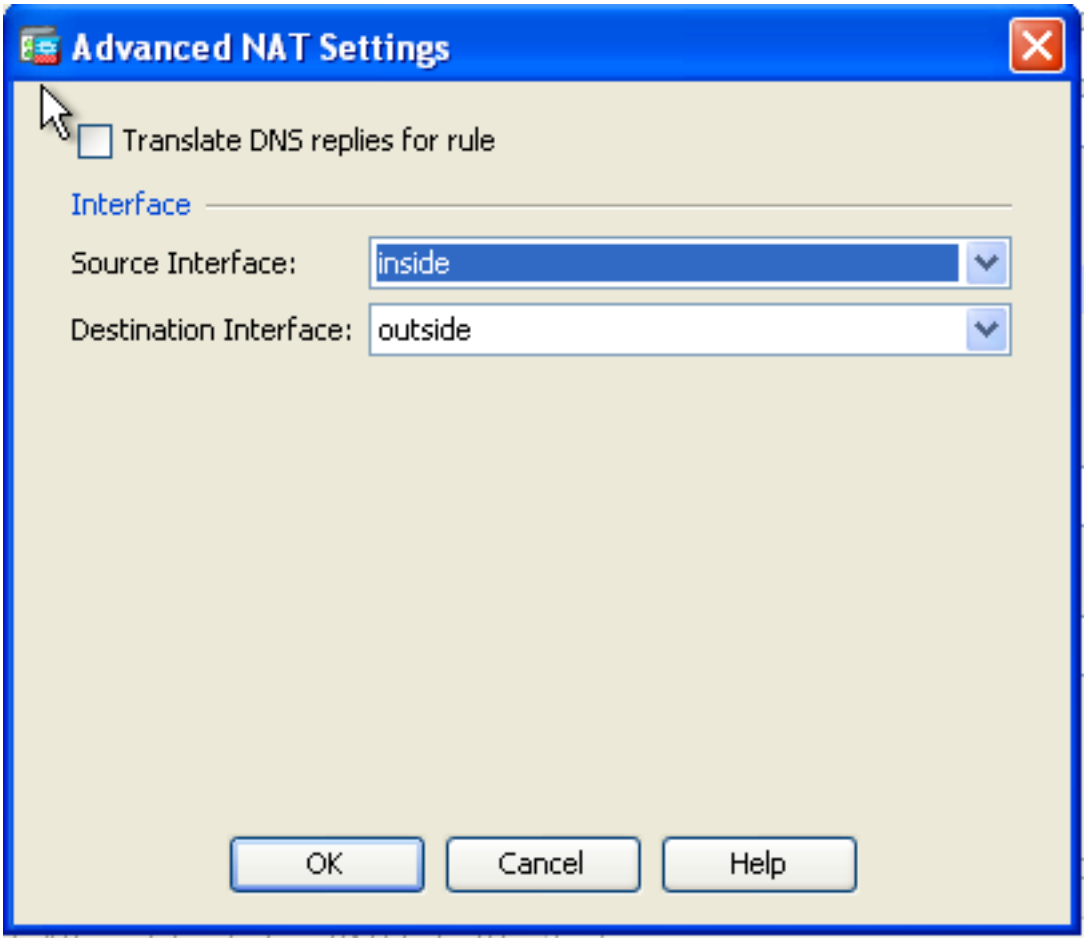
1. Choisissez la **configuration** > le **Pare-feu** > les **règles NAT**. Cliquez sur Add et puis choisissez l'**objet de réseau** afin de configurer une règle NAT statique. Développez NAT.



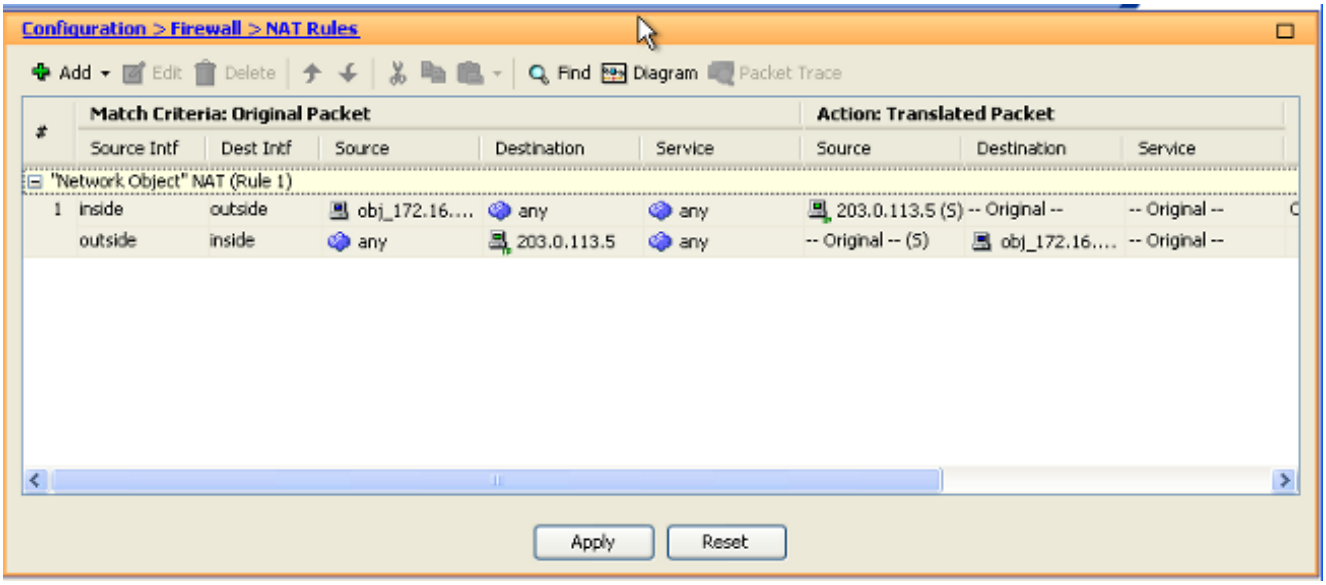
2. Cochez la case **automatique de règles de traduction d'adresses d'ajouter**. Dans la liste déroulante de type, choisissez la **charge statique.** Dans le domaine traduit d'adr, écrivez l'adresse IP. Cliquez sur **avancé** afin de sélectionner la source et les interfaces de destination.



3. Dans les listes déroulantes d'interface de source et d'interface de destination, choisissez les interfaces appropriées. Cliquez sur **OK**.



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



C'est le CLI équivalent sorti pour cette configuration NAT :

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

Identité statique NAT

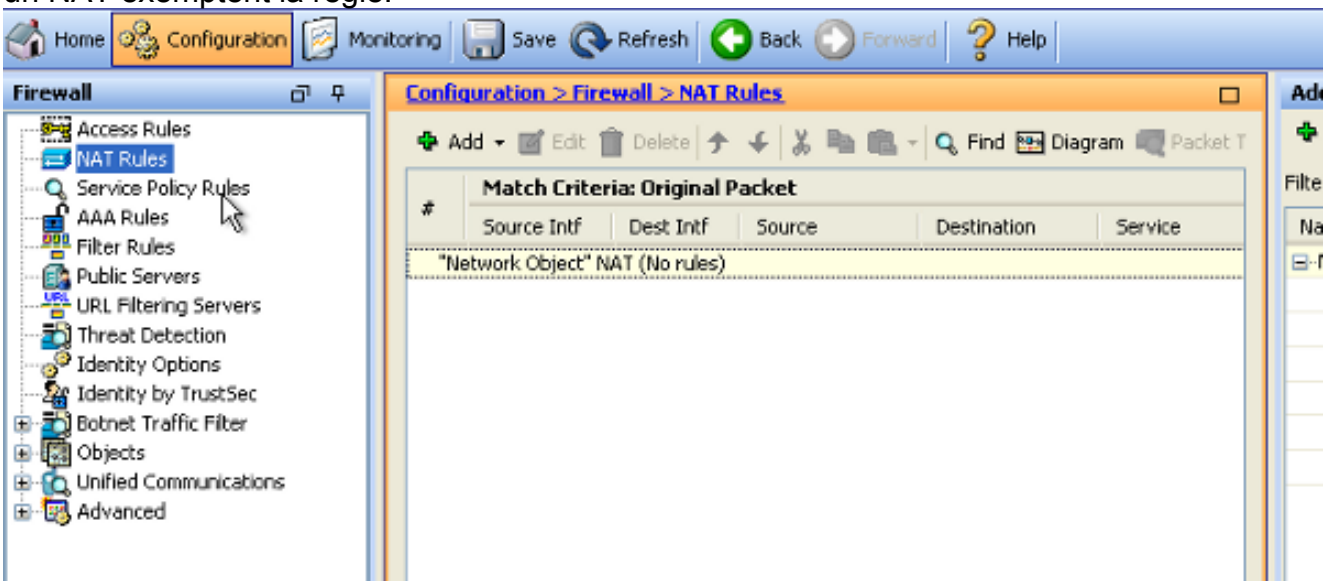
Exempt NAT est une fonctionnalité utile où l'essai intérieur d'utilisateurs en accéder à un hôte/serveur ou du distant VPN hébergent/serveurs hébergés derrière n'importe quelle autre

interface de l'ASA sans fin d'un NAT. Afin de réaliser ceci, le serveur interne, qui a une adresse IP privée, sera identité traduite à elle-même et qui consécutivement est permis pour accéder à la destination qui exécute un NAT.

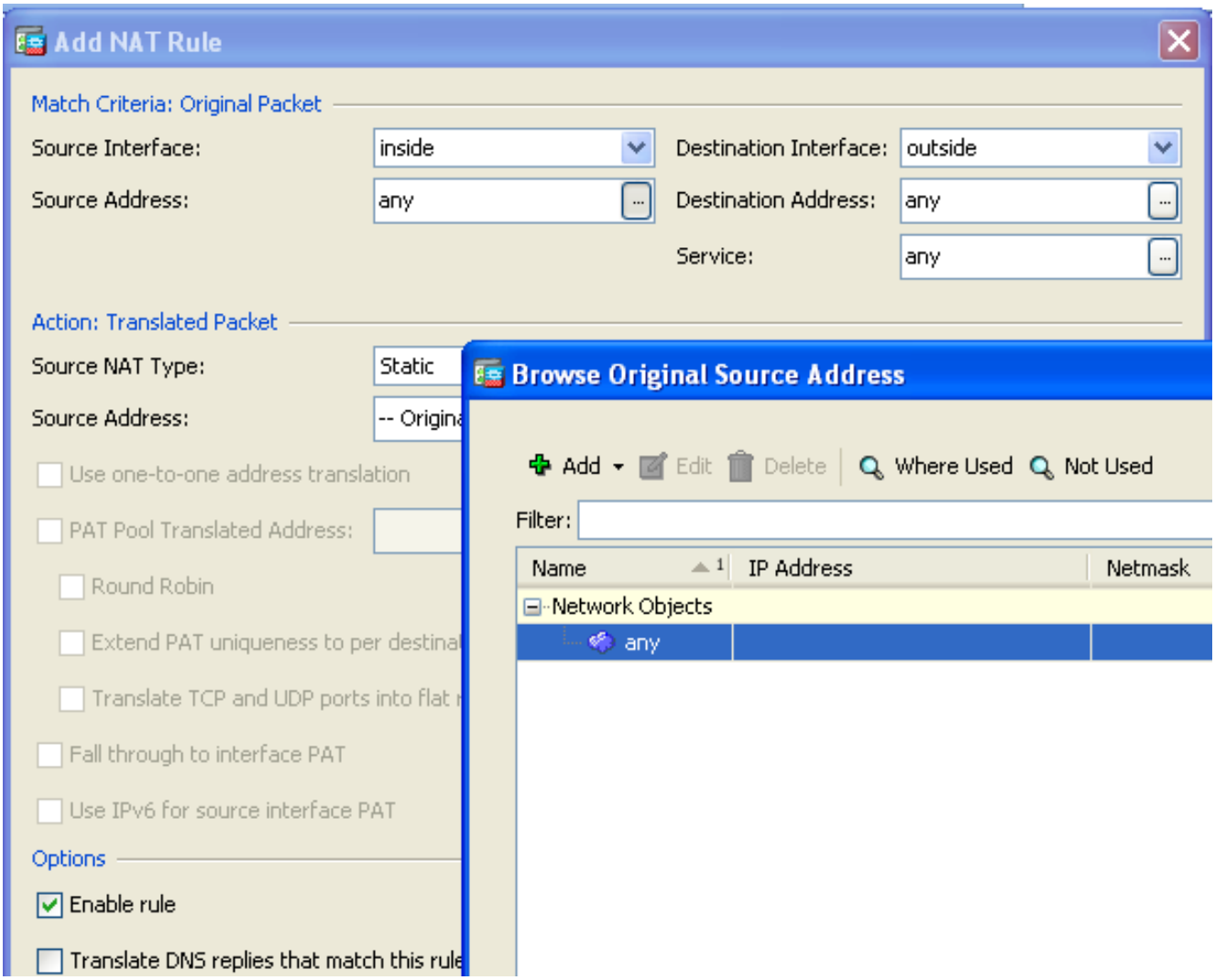
Dans cet exemple, l'hôte interne 172.16.11.15 doit accéder au serveur VPN distant 172.20.21.15.

Terminez-vous ces étapes afin de permettre à des hôtes internes l'accès au réseau VPN distant avec la fin d'un NAT :

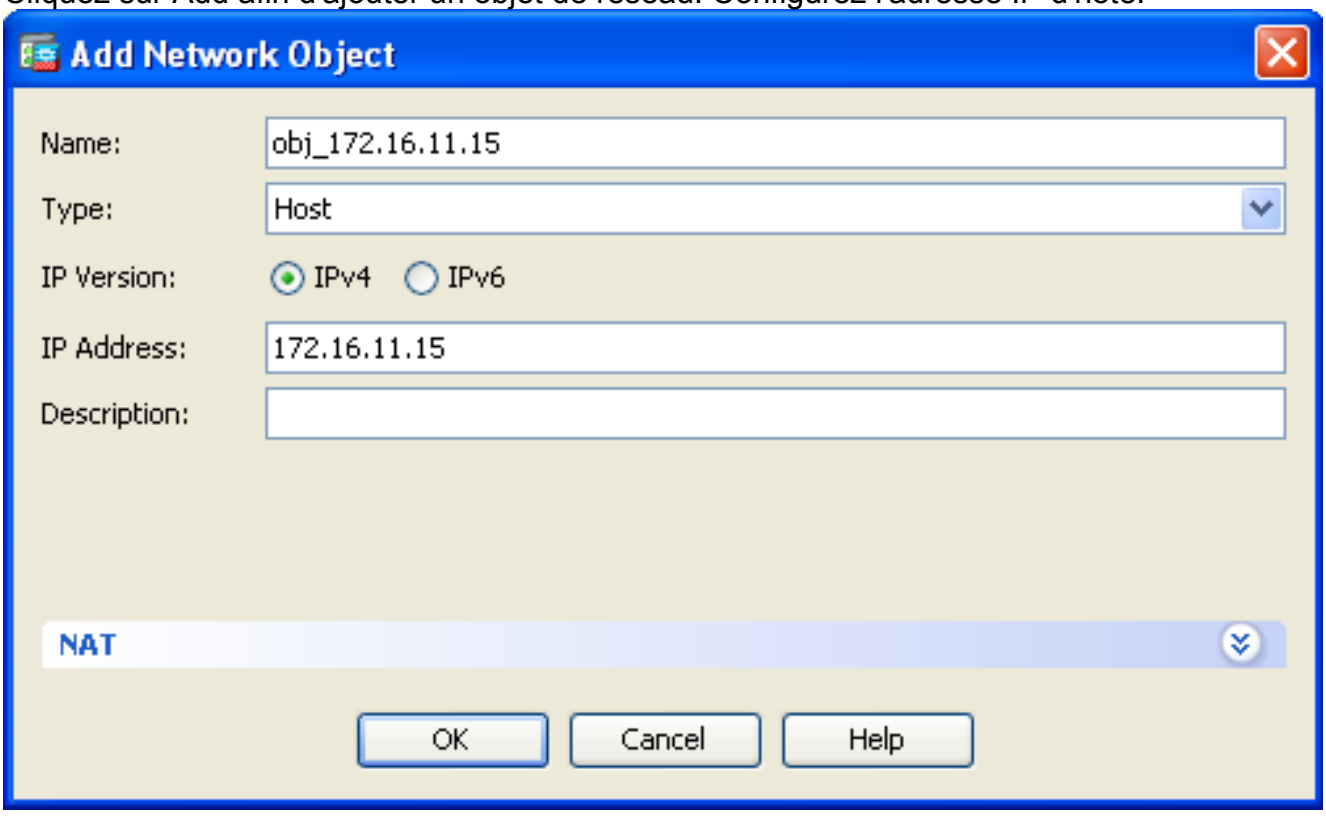
1. Choisissez la **configuration** > le **Pare-feu** > les **règles NAT**. Cliquez sur Add afin de configurer un NAT exemptent la règle.



2. Dans les listes déroulantes d'interface de source et d'interface de destination, choisissez les interfaces appropriées. Dans la zone adresse d'adresse source, choisissez l'entrée appropriée.

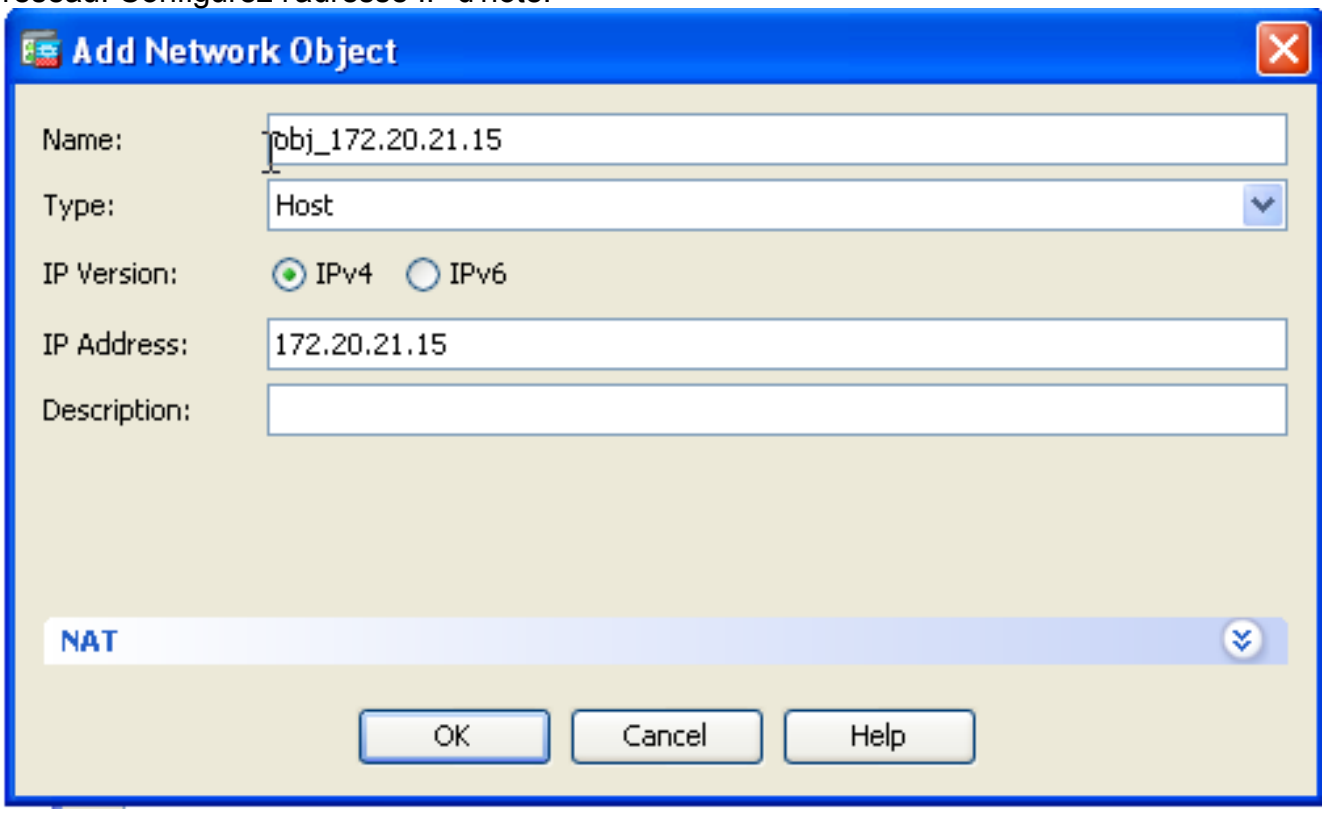


3. Cliquez sur Add afin d'ajouter un objet de réseau. Configurez l'adresse IP d'hôte.

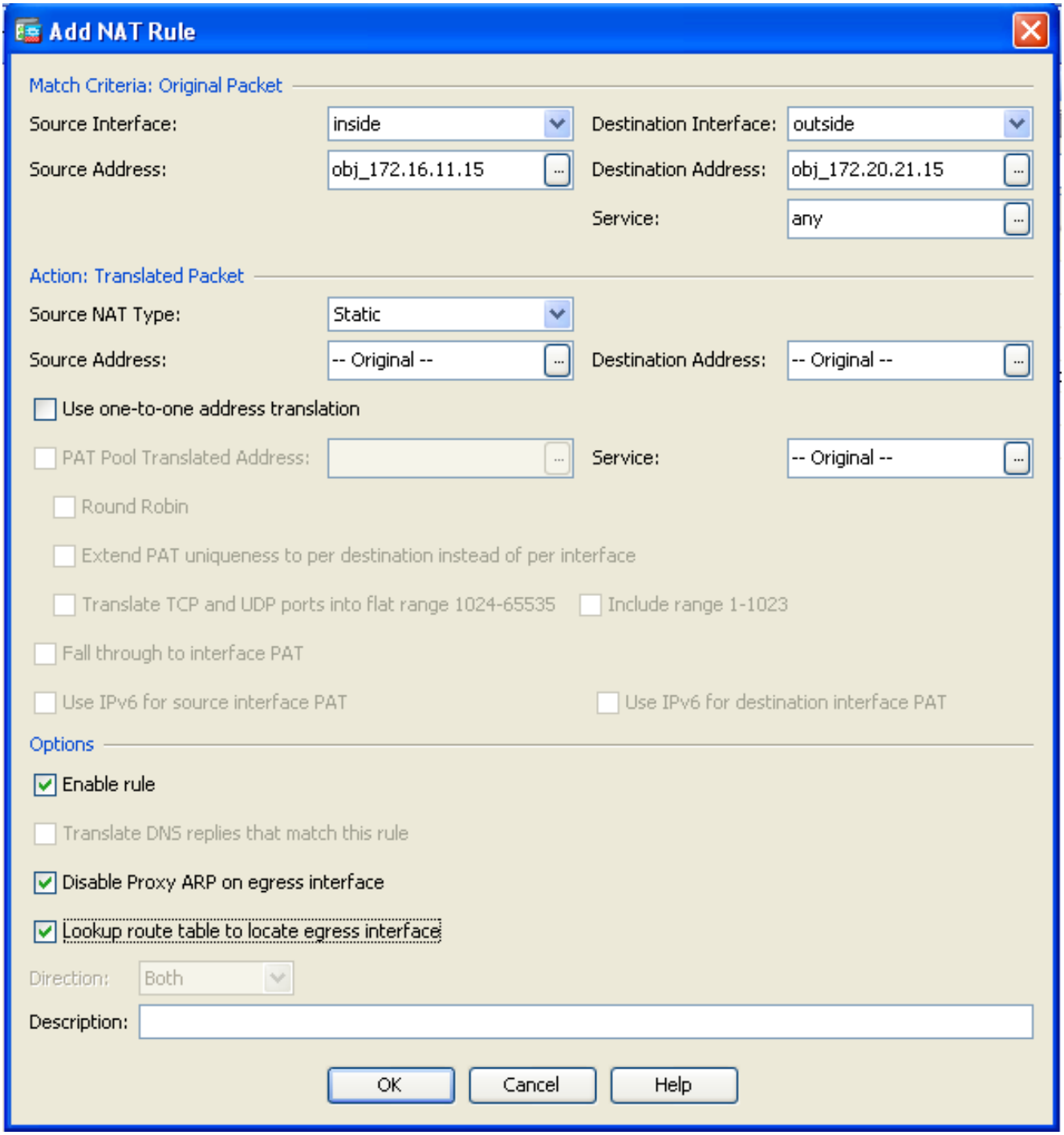


4. De même, parcourez l'**adresse de destination**. Cliquez sur Add afin d'ajouter un objet de

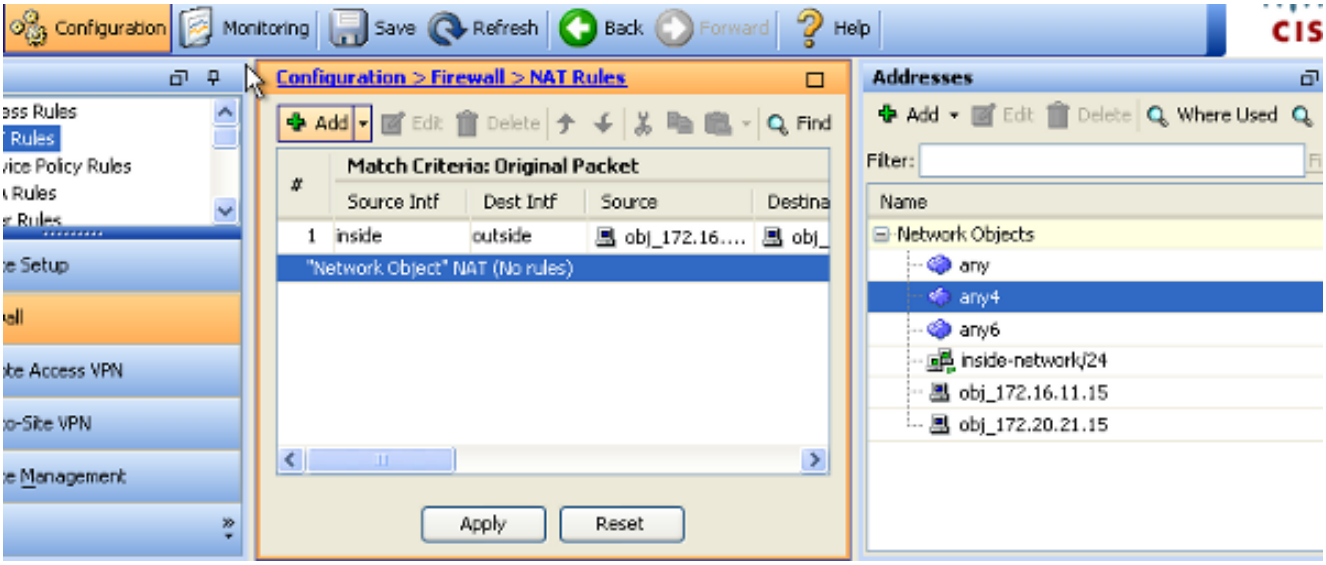
réseau. Configurez l'adresse IP d'hôte.



5. Choisissez les objets configurés d'adresse source et d'adresse de destination. Vérifiez le **proxy ARP de débronchement sur l'interface de sortie** et la **table de routage de consultation pour localiser des** cases d'**interface de sortie**. Cliquez sur **OK**.



6. Cliquez sur Apply pour les modifications pour le prendre effet.



C'est le CLI équivalent sorti pour le NAT configuration NAT exemptent ou d'identités :

```
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
```

Port Redirection(Forwarding) avec la charge statique

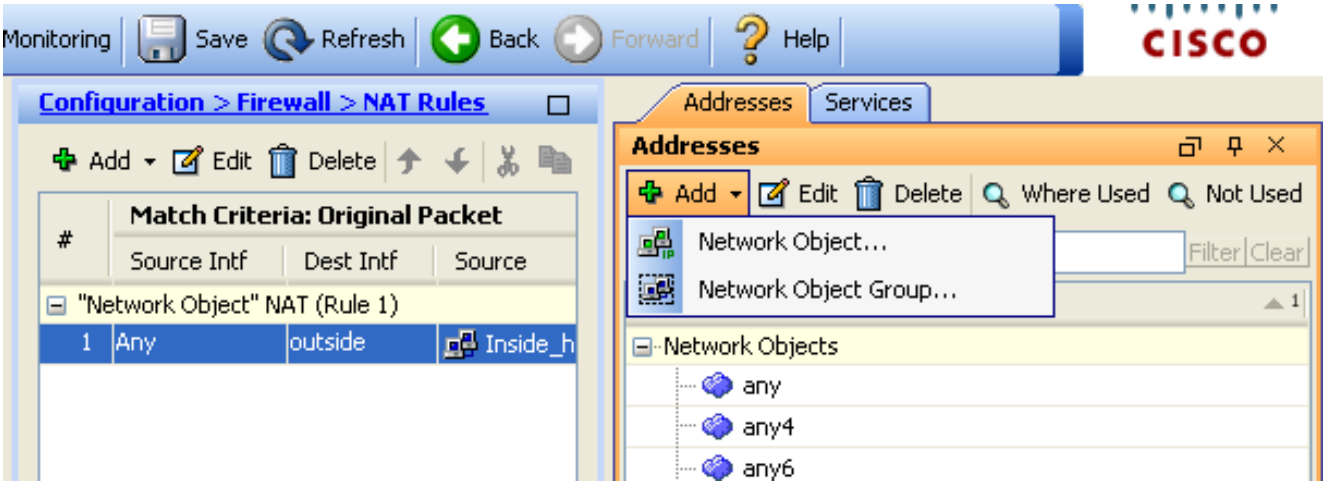
La transmission du port ou la redirection de port est une fonctionnalité utile où l'essai d'utilisateurs externes accéder à un serveur interne sur un port spécifique. Afin de réaliser ceci, le serveur interne, qui a une adresse IP privée, sera traduit à une adresse IP publique qui consécutivement est permis l'accès pour le port spécifique.

Dans cet exemple, l'utilisateur externe veut accéder au serveur SMTP, 203.0.115.15 au port 25. Ceci est accompli dans deux étapes :

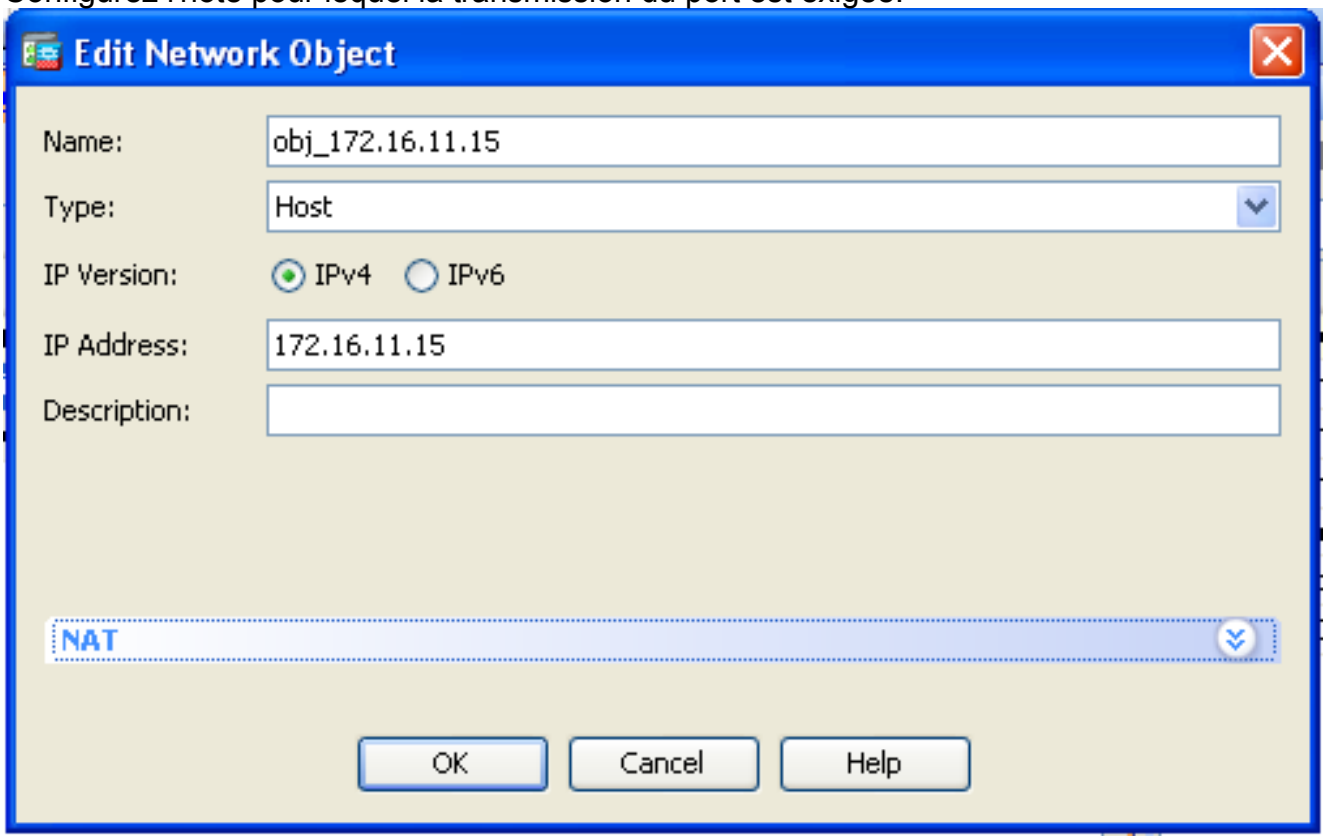
1. Traduisez le serveur de messagerie interne, 172.16.11.15 sur le port 25, à l'adresse IP publique, 203.0.115.15 au port 25.
2. Permettez l'accès au serveur de messagerie public, 203.0.115.15 au port 25.

Quand les essais d'utilisateur externe pour accéder au serveur, 203.0.115.15 au port 25, ce trafic est réorientés au serveur de messagerie interne, 172.16.11 15 au port 25.

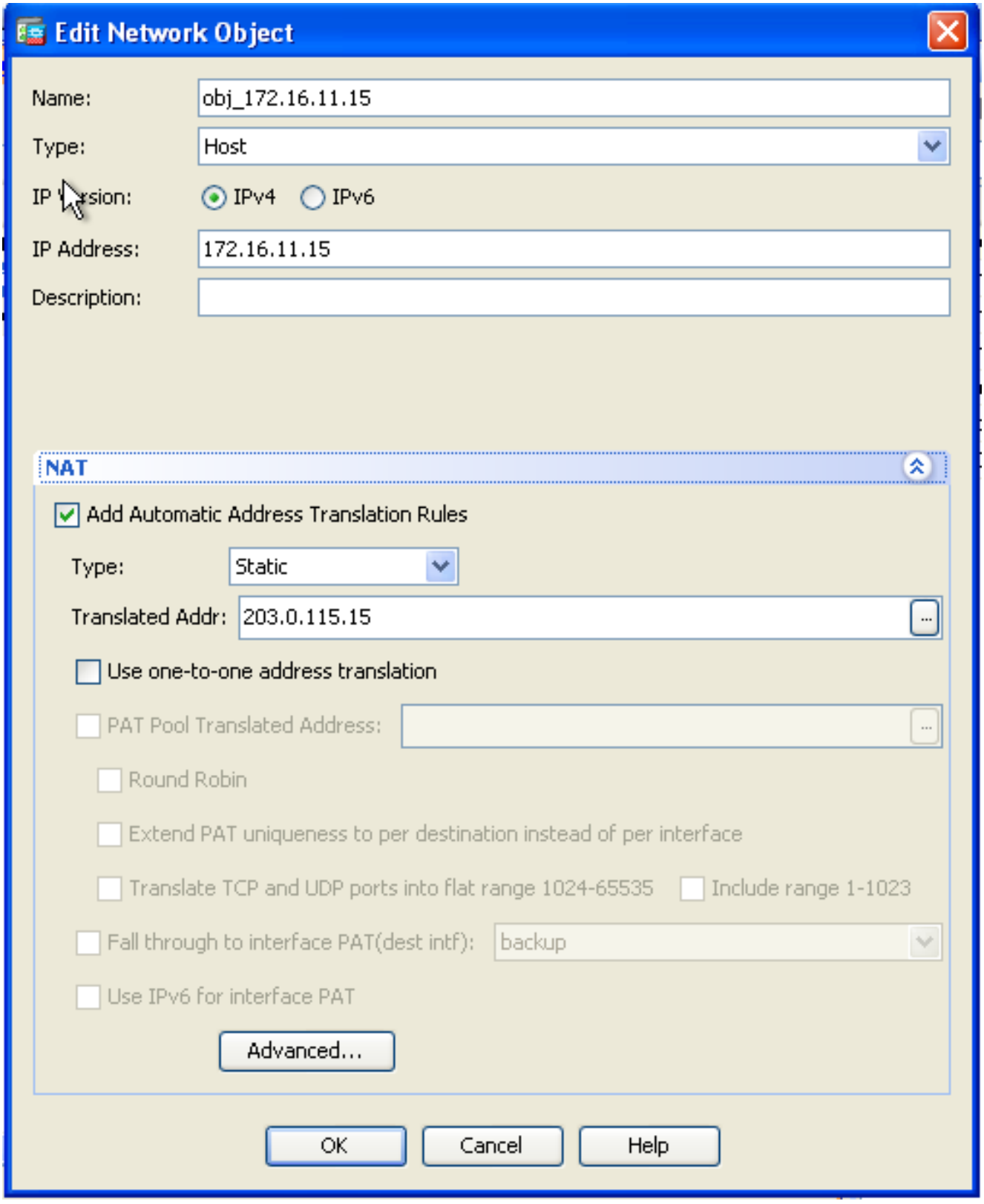
1. Choisissez la **configuration > le Pare-feu > les règles NAT**. Cliquez sur Add et puis choisissez l'**objet de réseau** afin de configurer une règle NAT statique.



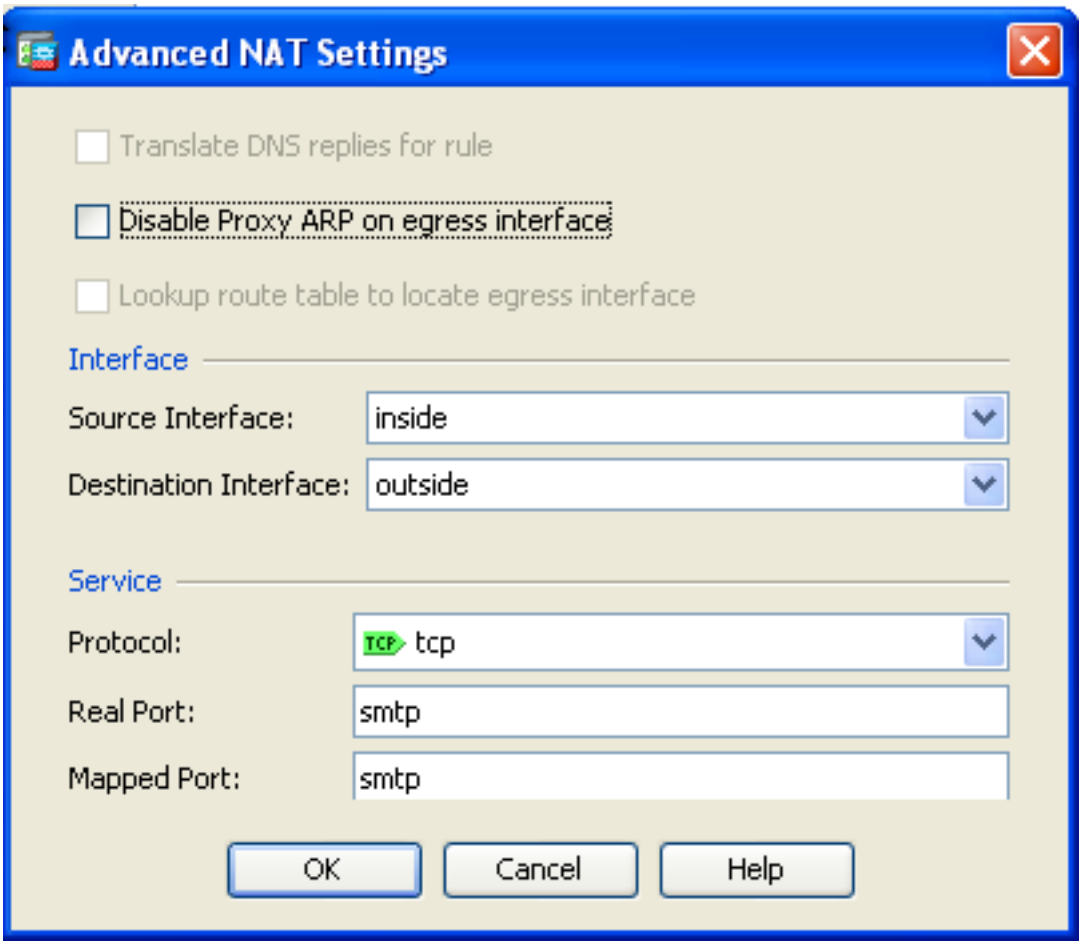
2. Configurez l'hôte pour lequel la transmission du port est exigée.



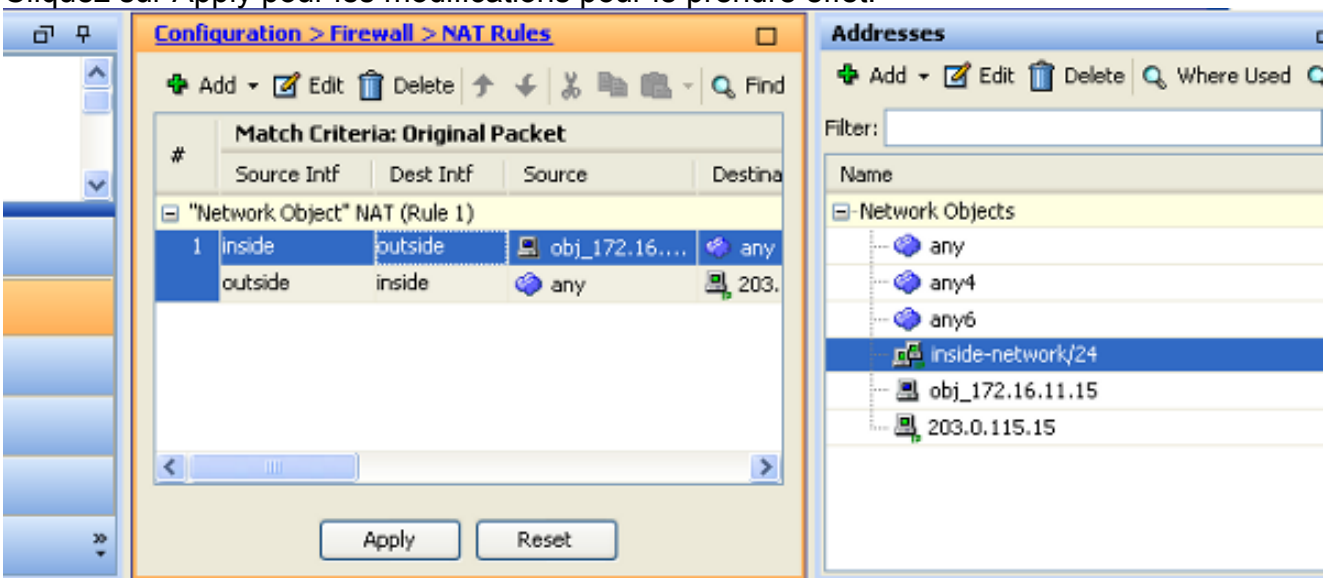
3. Développez NAT. Cochez la case **automatique de règles de traduction d'adresses d'ajouter**. Dans la liste déroulante de type, choisissez la **charge statique**. Dans le domaine traduit d'adr, écrivez l'adresse IP. Cliquez sur **avancé** afin de sélectionner le service et la source et les interfaces de destination.



4. Dans les listes déroulantes d'interface de source et d'interface de destination, choisissez les interfaces appropriées. Configurez le service. Cliquez sur **OK**.



5. Cliquez sur Apply pour les modifications pour le prendre effet.



C'est le CLI équivalent sorti pour cette configuration NAT :

```
object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.115.15 service tcp smtp smtp
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'analyseur de Cisco CLI (clients enregistrés seulement) prend en charge certaines **commandes**

show. Employez l'analyseur de Cisco CLI afin de visualiser une analyse de sortie de commande show.

Accédez à un site Web par l'intermédiaire du HTTP avec un navigateur Web. Cet exemple utilise un site qui est hébergé chez 198.51.100.100. Si la connexion est réussie, cette sortie peut être vue sur l'ASA CLI.

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 dynamique, et le trafic de retour du web server est permis de retour par le Pare-feu parce qu'il apparie une ***connexion*** dans la table de connexion de Pare-feu. Trafiquez qu'apparie une connexion qui préexiste est autorisée par le Pare-feu sans être bloqué par un ACL d'interface.

Dans la sortie précédente, le client sur l'interface interne a établi une connexion à l'hôte de 198.51.100.100 hors fonction de l'interface extérieure. Ce rapport est établi avec le protocole TCP et a été de veille pendant six secondes. Les indicateurs de connexion indiquent l'état actuel de cette connexion. Plus d'informations sur des indicateurs de connexion peuvent être trouvées dans des indicateurs de connexion TCP ASA.

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 ASA génère des Syslog pendant le fonctionnement normal. Les Syslog s'étendent dans la verbosité basée sur la configuration de journalisation. La sortie affiche deux Syslog qui sont vus au niveau six, ou le de niveau « informationnel ».

Dans cet exemple, il y a deux Syslog générés. Le premier est un message de log qui indique que le Pare-feu a établi une traduction, spécifiquement une traduction dynamique de TCP (PAT). Il indique l'adresse IP source et le port et l'adresse IP et le port traduits pendant que le trafic traverse de l'intérieur aux interfaces extérieures.

Le deuxième Syslog indique que le Pare-feu a établi une connexion dans sa table de connexion pour ce trafic spécifique entre le client et serveur. Si le Pare-feu était configuré afin de bloquer cette tentative de connexion, ou un autre facteur empêchait la création de cette connexion (des contraintes de ressource ou une mauvaise configuration possible), le Pare-feu ne génèrerait pas un log qui indique que la connexion a été établie. Au lieu de cela il se connecterait une raison pour que la connexion soit refusée ou une indication au sujet de quel facteur a empêché la connexion de l'création.

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 de traceur de paquet sur l'ASA te permet pour spécifier un paquet *simulé* et pour voir tous les divers étapes, contrôles, et fonctions par lesquelles le Pare-feu passe quand il traite le trafic. Avec cet outil, il est utile d'identifier un exemple du trafic que vous croyez *devriez* être laissé traverser le Pare-feu, et l'utilise que 5-tupple afin de simuler le trafic. Dans l'exemple précédent, le traceur de paquet est utilisé afin de simuler une tentative de connexion qui répond à ces critères :

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

Notez qu'il n'y avait aucune mention de l'interface dehors dans la commande. C'est par conception de traceur de paquet. L'outil vous indique comment les processus de Pare-feu qui type de tentative de connexion, qui inclut comment elle la conduirait, et hors de quelle interface. Plus d'informations sur le traceur de paquet peuvent être trouvées en paquets de suivi avec Packet Tracer.

Capture

Appliquez 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 qui écrit ou laisse ses interfaces. Cette fonctionnalité de capture est fantastique parce qu'elle peut définitivement prouver si le trafic arrive à, ou des feuilles de, un Pare-feu. L'exemple précédent a affiché la configuration de deux captures nommées capin et capout sur les interfaces internes et externes respectivement. Les ordres de capture ont utilisé le mot clé de correspondance, qui te permet pour être spécifique au sujet de quel trafic vous voulez capturer.

Pour le capin de capture**,** vous avez indiqué que vous avez voulu apparier le trafic vu sur l'interface interne (d'entrée ou de sortie) cet hôte 198.51.100.100 de 172.16.11.5 d'hôte TCP de correspondances. En d'autres termes, vous voulez capturer n'importe quel trafic TCP qui est envoyé de l'hôte 172.16.11.5 pour héberger 198.51.100.100 ou vice versa. L'utilisation du mot clé de correspondance permet au Pare-feu pour capturer ce trafic bidirectionnel. L'ordre de capture défini pour l'interface extérieure ne met pas en référence l'adresse IP de client interne parce que les attitudes PAT de Pare-feu sur cette adresse IP de client. En conséquence, vous ne pouvez pas être assortie avec cette adresse IP de client. Au lieu de cela, cet exemple en emploie afin d'indiquer que toutes les adresses IP possibles apparieraient cette condition.

Après que vous configuriez les captures, vous tenteriez alors d'établir une connexion de nouveau, et poursuivez pour visualiser les captures avec la commande de ***<capture_name> de show capture***. Dans cet exemple, vous pouvez voir que le client pouvait se connecter au serveur comme évident par la prise de contact à trois voies de TCP vue dans les captures.

Dépannez

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

Informations connexes

- Exemple de configuration de Syslog ASA
- Captures de paquet ASA avec l'exemple de configuration CLI et ASDM
- Support et documentation techniques - Cisco Systems