

PIX/ASA 7.x et FWASM : Instructions NAT et PAT

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Commande nat-control](#)

[Plusieurs déclarations NAT avec NAT 0](#)

[Plusieurs pools globaux](#)

[Diagramme du réseau](#)

[Mélange de déclarations globales NAT et PAT](#)

[Diagramme du réseau](#)

[Plusieurs déclarations NAT avec la liste d'accès NAT 0](#)

[Diagramme du réseau](#)

[Utilisation du NAT de stratégie](#)

[Diagramme du réseau](#)

[NAT statique](#)

[Diagramme du réseau](#)

[Comment contourner le NAT](#)

[Configurer le NAT d'identité](#)

[Configurer le NAT d'identité statique](#)

[Configurer l'exemption NAT](#)

[Vérifier](#)

[Dépanner](#)

[Message d'erreur reçu en ajoutant un PAT statique pour le port 443](#)

[ERREUR : conflit de tracer-adresse avec la charge statique existante](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit des exemples des configurations de base de traduction d'adresses de réseau (NAT) et de traduction d'adresses de port (PAT) sur les dispositifs de sécurité Cisco PIX/ASA. Des diagrammes de réseau simplifiés sont fournis. Pour des informations détaillées, consultez la documentation PIX/ASA correspondant à votre version du logiciel PIX/ASA.

Référez-vous à [Utilisation des commandes nat, global, static, conduit, et access-list et Redirection de port \(transmission\) sur PIX](#) afin d'en savoir plus sur les commandes **nat**, **global**, **static**, **conduit** et **access-list** et la redirection de port (transmission) sur PIX 5.x et versions ultérieures.

Référez-vous à [Utilisation des déclarations NAT et PAT sur le pare-feu Cisco Secure PIX](#) afin d'en

savoir plus sur des exemples de configurations NAT et PAT de base sur le pare-feu Cisco Secure PIX.

Pour plus d'informations sur la configuration NAT dans la version 8.3 et ultérieures ASA, référez-vous aux [informations sur NAT](#).

Remarque: Le NAT en mode transparent est pris en charge à parti de PIX/ASA version 8.x. Référez-vous à [NAT dans le](#) pour en savoir plus de [mode transparent](#).

[Conditions préalables](#)

[Conditions requises](#)

Les lecteurs de ce document doivent bien connaître l'appliance de sécurité Cisco PIX/ASA.

[Composants utilisés](#)

Les informations de ce document se basent sur le logiciel de l'appliance de sécurité de la gamme Cisco PIX 500 version 7.0 ou ultérieure.

Remarque: Ce document a été de nouveau certifié avec PIX/ASA version 8.x.

Remarque: Les commandes utilisées dans ce document s'appliquent à Firewall Service Module (FWSM).

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

[Conventions](#)

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

[Commande nat-control](#)

La commande **nat-control** sur le pare-feu PIX/ASA indique que tout le trafic passant par ce dernier doit avoir une entrée de traduction spécifique (déclaration **nat** avec une déclaration **globale** ou **statique** correspondante) pour que ce trafic passe par le pare-feu. La commande **nat-control** garantit que le comportement de la traduction est identique aux versions du pare-feu PIX antérieures à 7.0. La configuration par défaut de PIX/ASA version 7.0 et ultérieure est spécifiée par la commande **no nat-control**. Avec PIX/ASA version 7.0 et ultérieure, vous pouvez modifier ce comportement lorsque vous émettez la commande **nat-control**.

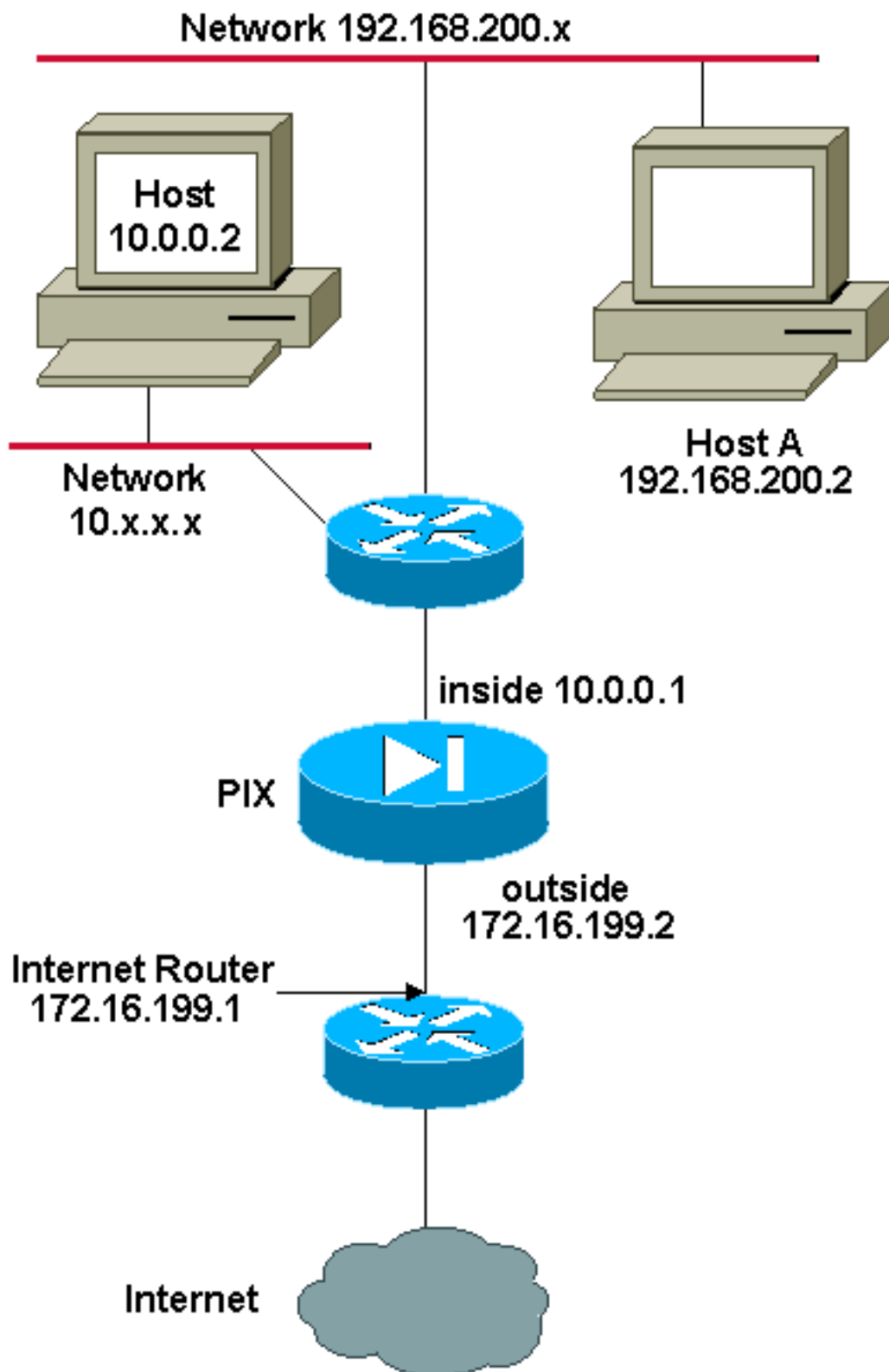
Lorsque **nat-control** est désactivée, le pare-feu PIX/ASA transmet les paquets d'une interface de sécurité supérieure à une inférieure sans entrée de traduction spécifique dans la configuration. Afin de faire passer le trafic d'une interface de niveau de sécurité inférieur à une interface plus élevée, utilisez les listes d'accès. Le pare-feu PIX/ASA transmet ensuite le trafic. Ce document se concentre sur le comportement de l'appliance de sécurité PIX/ASA lorsque- **nat-control** est

activée.

Remarque: Si vous souhaitez supprimer ou désactiver la déclaration nat-control dans le pare-feu PIX/ASA, vous devez supprimer toutes les déclarations NAT de l'appliance de sécurité. Généralement, vous devez supprimer le NAT avant de désactiver le contrôle NAT. Vous devez reconfigurer la déclaration NAT dans le pare-feu PIX/ASA pour qu'il fonctionne comme vous l'entendez.

[Plusieurs déclarations NAT avec NAT 0](#)

[Diagramme du réseau](#)



Remarque: 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.

Dans cet exemple, l'ISP fournit au responsable du réseau une plage d'adresses allant de 172.16.199.1 à 172.16.199.63. Le responsable du réseau décide d'attribuer 172.16.199.1 à l'interface interne du routeur Internet et 172.16.199.2 à l'interface externe du PIX/ASA.

L'administrateur réseau a déjà fait attribuer une adresse de classe C au réseau, 192.168.200.0/24, et quelques postes de travail utilisent ces adresses afin d'accéder à Internet. Les adresses de ces

postes de travail ne doivent pas être traduites. Cependant, des adresses attribuées à de nouveaux postes de travail du réseau 10.0.0.0/8 doivent être traduites.

Afin de s'adapter à cette conception réseau, l'administrateur réseau doit utiliser deux déclarations NAT et un pool global dans la configuration PIX/ASA, comme le montre cette sortie :

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
```

```
nat (inside) 0 192.168.200.0 255.255.255.0 0 0
```

```
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

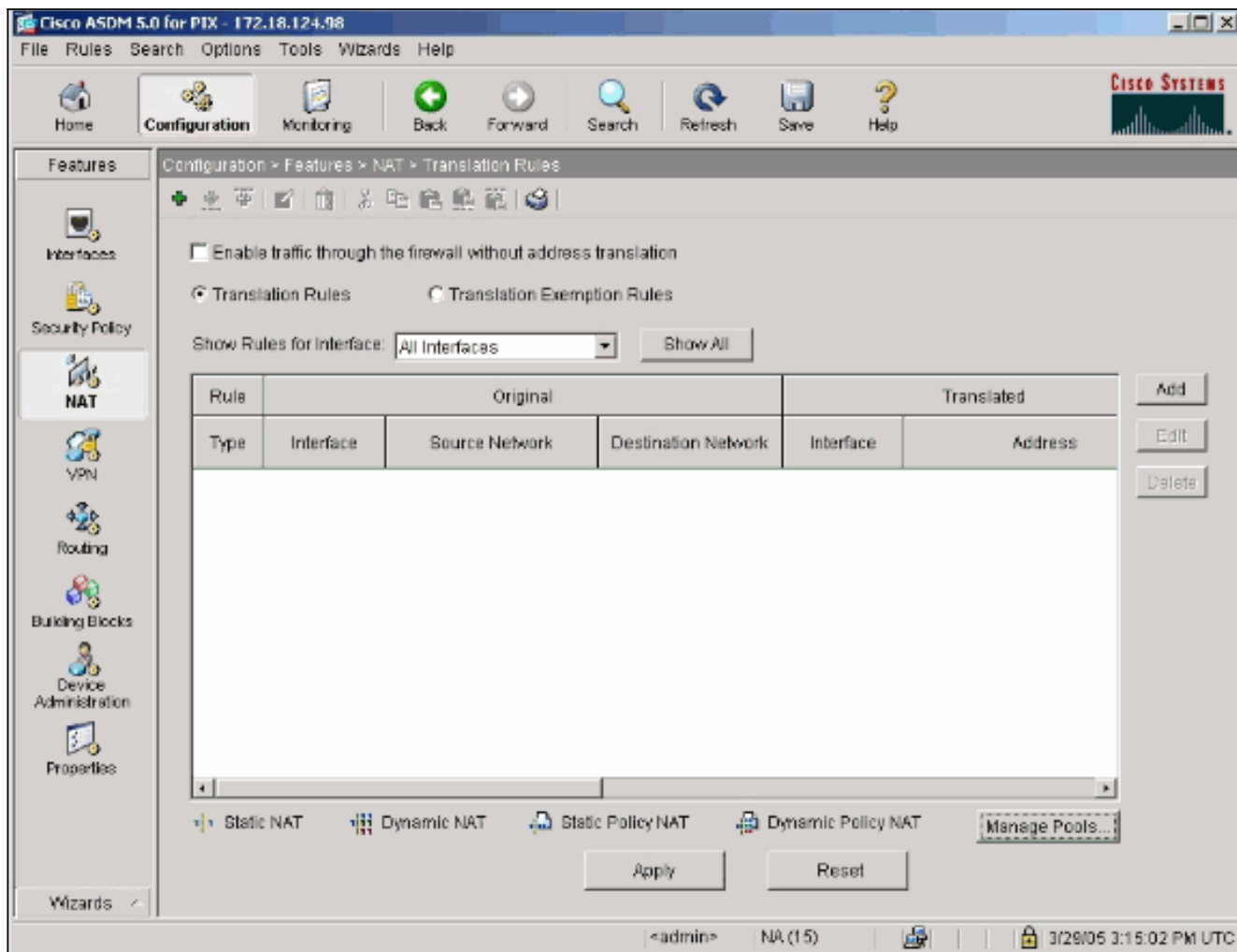
Cette configuration ne traduit pas l'adresse source du trafic sortant du réseau 192.168.200.0/24. Elle traduit une adresse source dans le réseau 10.0.0.0/8 en une adresse de la plage 172.16.199.3 à 172.16.199.62.

Ces étapes expliquent comment appliquer cette même configuration avec l'utilisation de l'Adaptive Security Device Manager (ASDM).

Remarque: Effectuez toutes les modifications de configuration par la CLI ou l'ASDM. L'utilisation de la CLI et d'ASDM pour les modifications de la configuration entraîne une application instable des configurations par ASDM. Ce n'est pas un bogue, mais provient de la façon dont ASDM fonctionne.

Remarque: Lorsque vous ouvrez ASDM, il importe la configuration actuelle depuis PIX/ASA et travaille à partir de cette configuration lorsque vous apportez et appliquez des modifications. Si une modification est apportée au pare-feu PIX/ASA tandis que la session ASDM est ouverte, alors ASDM ne fonctionne plus avec ce qu'il « pense » être la configuration actuelle du PIX/ASA. Assurez-vous de fermer toutes les sessions ASDM si vous effectuez des modifications de configuration par l'intermédiaire de la CLI. Lorsque vous souhaitez travailler par l'intermédiaire de GUI, ouvrez à nouveau ASDM.

1. Lancez ASDM, accédez à l'onglet Configuration et cliquez sur **NAT**.
2. Cliquez sur **Add** pour créer une règle.



Une nouvelle fenêtre permettant à l'utilisateur de modifier les options NAT pour cette entrée NAT s'affiche. Pour cet exemple, exécutez NAT sur les paquets qui arrivent sur l'interface interne et qui proviennent du réseau spécifique 10.0.0.0/24. PIX/ASA traduit ces paquets vers un pool d'IP dynamique sur l'interface externe. Après avoir saisi les informations décrivant quel trafic associer au NAT, définissez un pool d'adresses IP pour le trafic traduit.

3. Cliquez sur **Manage Pools** afin d'ajouter un nouveau pool d'IP.

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:

Translate Address on Interface:


Translate Address To

 Static IP Address:

Redirect port

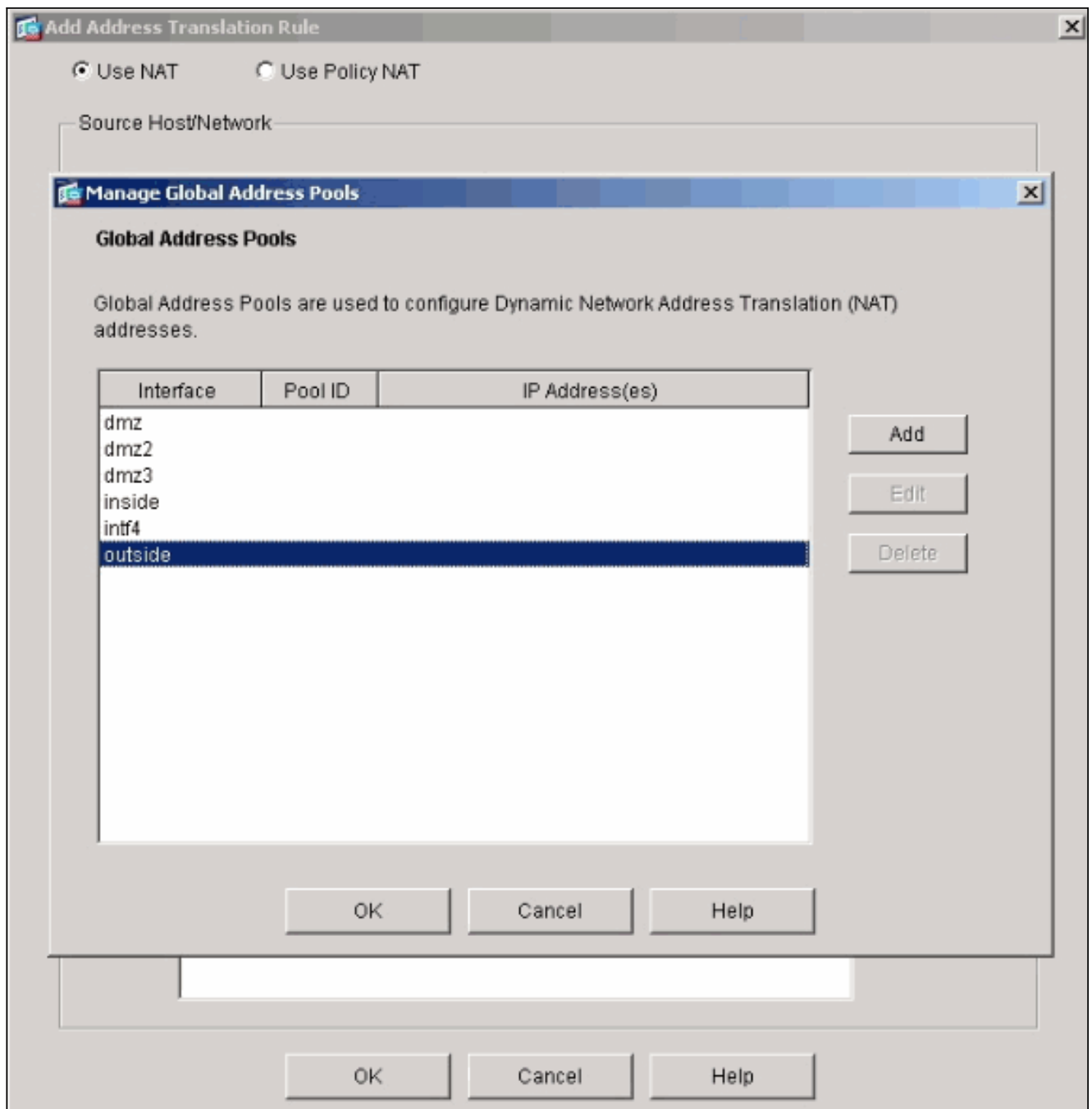
TCP Original port: Translated port:

UDP

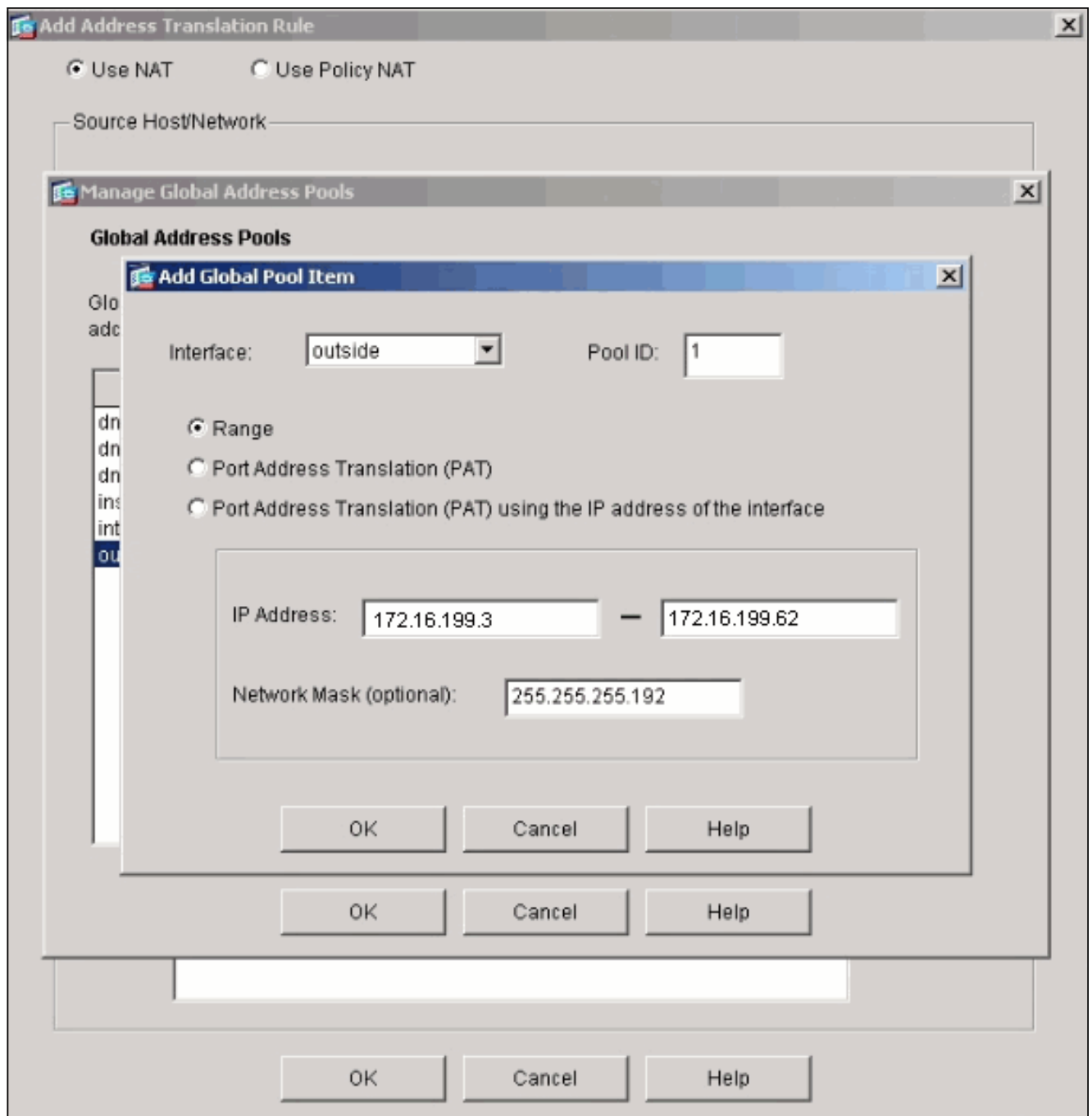
 Dynamic Address Pool:

Pool ID	Address
N/A	No address pool defined

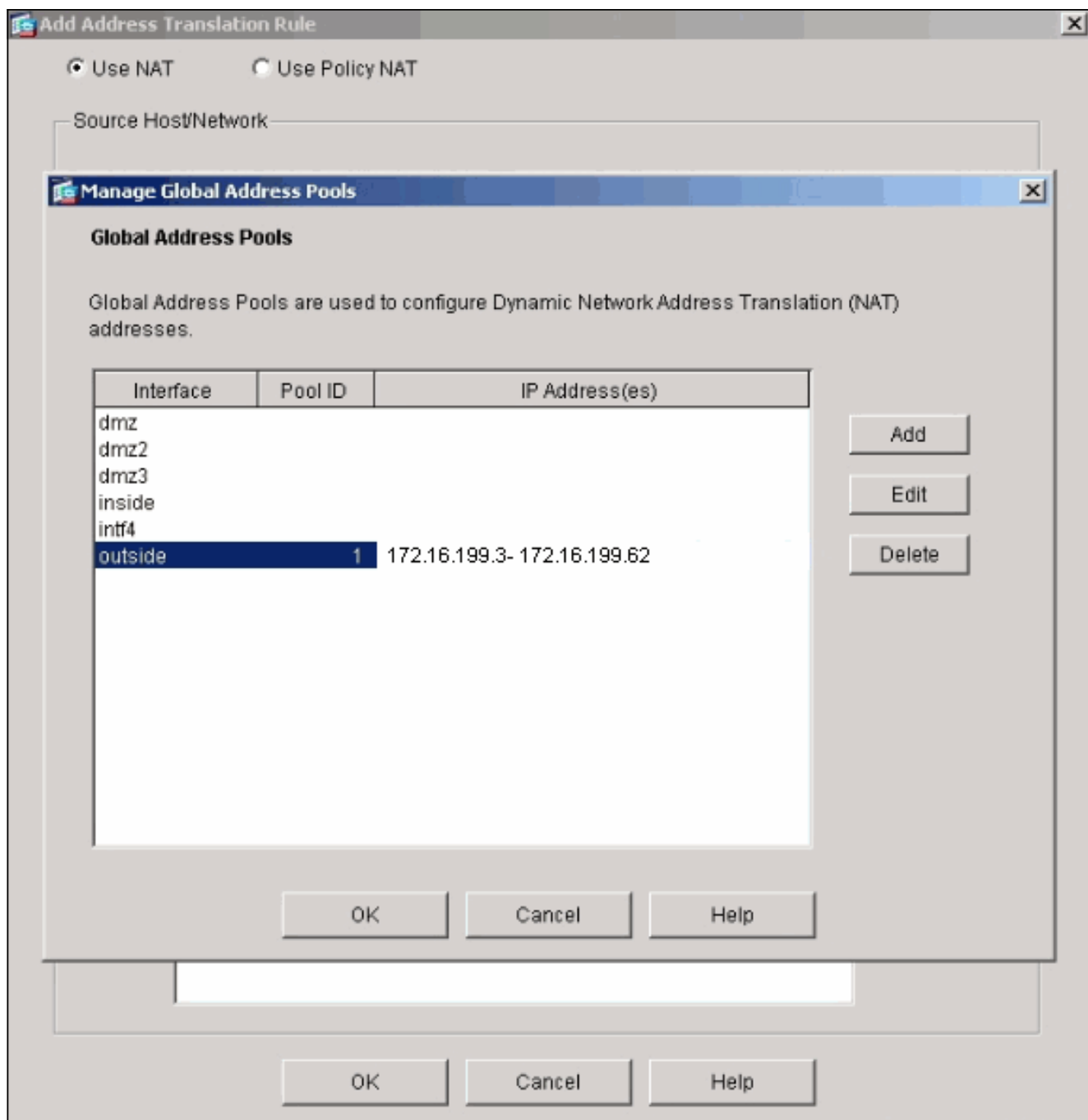
4. Choisissez **outside**, puis cliquez sur **Add**.



5. Spécifiez la plage d'IP pour le pool et attribuez au pool un numéro d'identification entier unique.



6. Saisissez les valeurs adéquates et cliquez sur **OK**. Le nouveau pool est défini pour l'interface externe.



7. Après avoir défini le pool, cliquez sur **OK** afin de retourner à la fenêtre de configuration de la règle NAT. Veillez à choisir le pool que vous venez de créer dans la liste déroulante Address Pool.

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network

Interface:

IP Address:

Mask:

Translate Address on Interface:

Translate Address To

Static IP Address:

Redirect port

TCP Original port: Translated port:

UDP

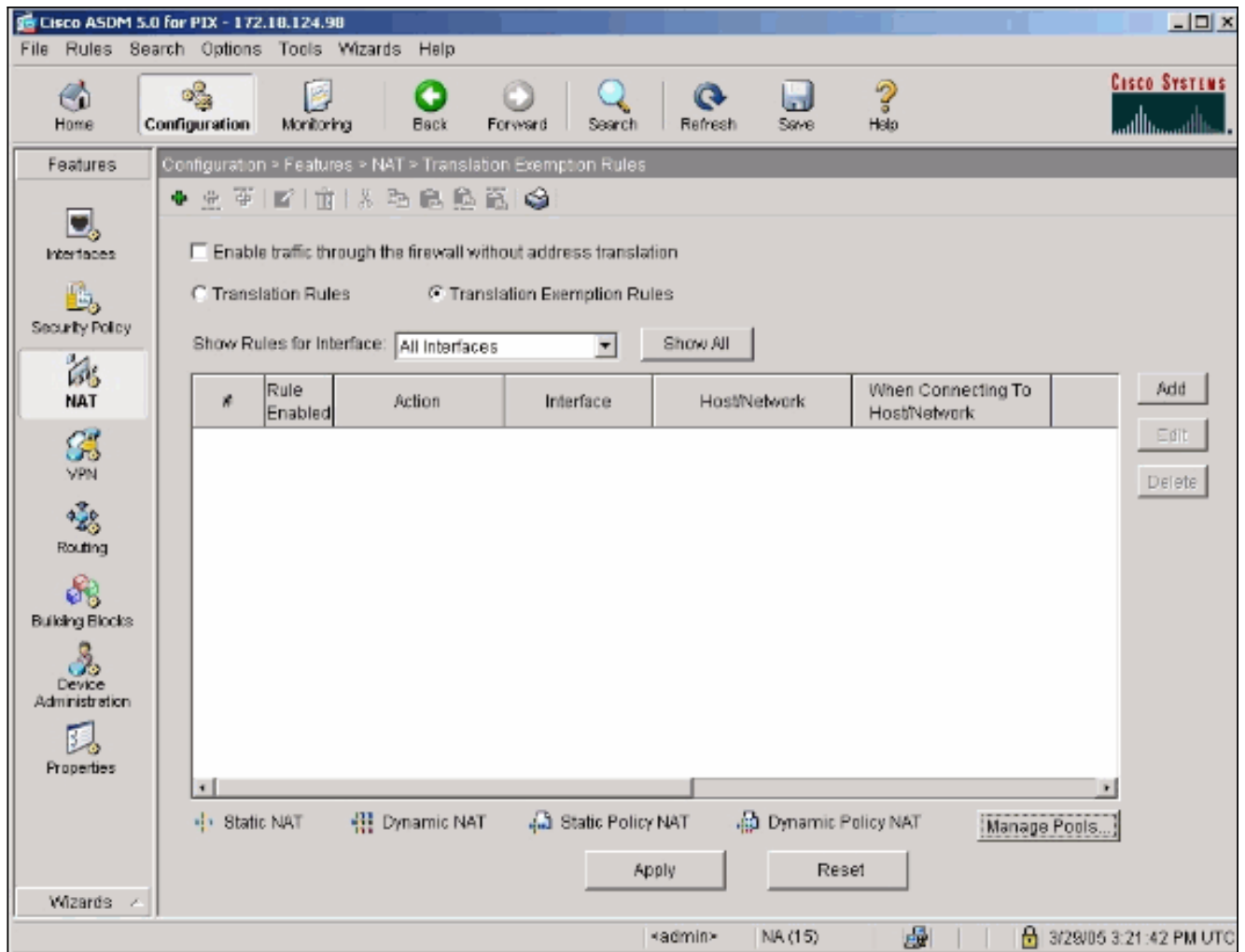
Dynamic Address Pool:

Pool ID	Address
1	172.16.199.3- 172.16.199.62

Vous venez de créer une traduction NAT par l'intermédiaire de l'appareil de sécurité.

Cependant, il vous reste à créer l'entrée NAT qui spécifie quel trafic ne pas associer à NAT.

8. Cliquez sur **Translation Exemption Rules** en haut de la fenêtre, puis sur **Add** pour créer une règle.




9. Choisissez l'*interface interne* en tant que source, et spécifiez le sous-réseau **192.168.200.0/24**. Laissez les valeurs « When connecting » par défaut.

Add Address Exemption Rule

Action
 Select an action:

Host/Network Exempted From NAT
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

When Connecting To
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Rule Flow Diagram
 Rule applied to traffic incoming to source interface


Please enter the description below (optional):

OK Cancel Help

Les règles NAT sont maintenant définies.

10. Cliquez sur **Apply** afin d'appliquer les modifications à la configuration en cours de l'appliance de sécurité. Cette sortie montre les ajouts réels appliqués à la configuration du PIX/ASA. Ils sont légèrement différents des commandes saisies dans la méthode manuelle, mais ils sont équivalents.

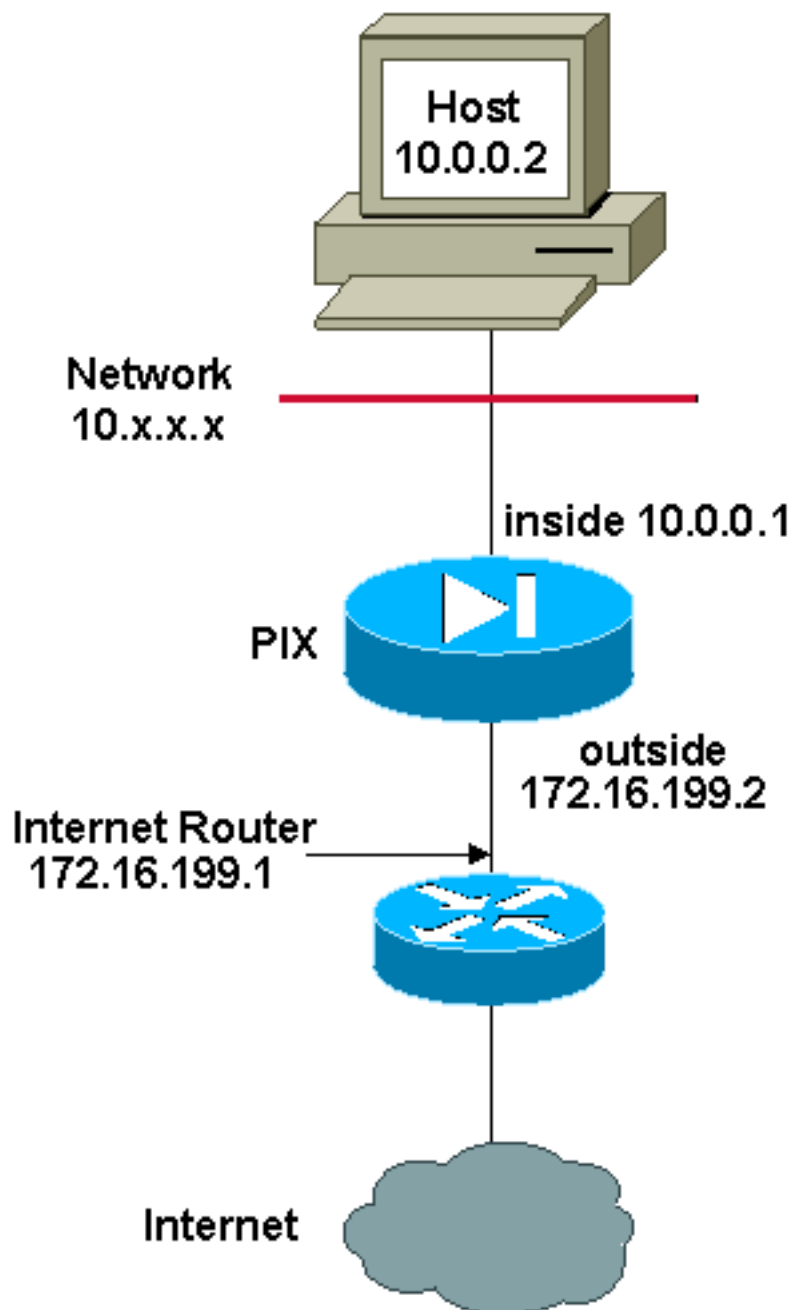
```
access-list inside_nat0_outbound extended permit
ip 192.168.200.0 255.255.255.0 any
```

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
```

```
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 10.0.0.0 255.255.255.0
```

[Plusieurs pools globaux](#)

[Diagramme du réseau](#)



Remarque: 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.

Dans cet exemple, le responsable du réseau a deux plages d'adresses IP qui s'enregistrent sur Internet. Le responsable du réseau doit convertir toutes les adresses internes, qui sont dans la plage 10.0.0.0/8 en adresses enregistrées. Les plages d'adresses IP que le responsable du réseau doit utiliser vont de 172.16.199.1 à 172.16.199.62 et de 192.168.150.1 à 192.168.150.254. Le responsable du réseau peut faire ceci de la façon suivante :

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
```

```
global (outside) 1 192.168.150.1-192.168.150.254 netmask 255.255.255.0
```

```
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

En NAT dynamique, la déclaration la plus spécifique est prioritaire lorsque vous utilisez la même interface en global.

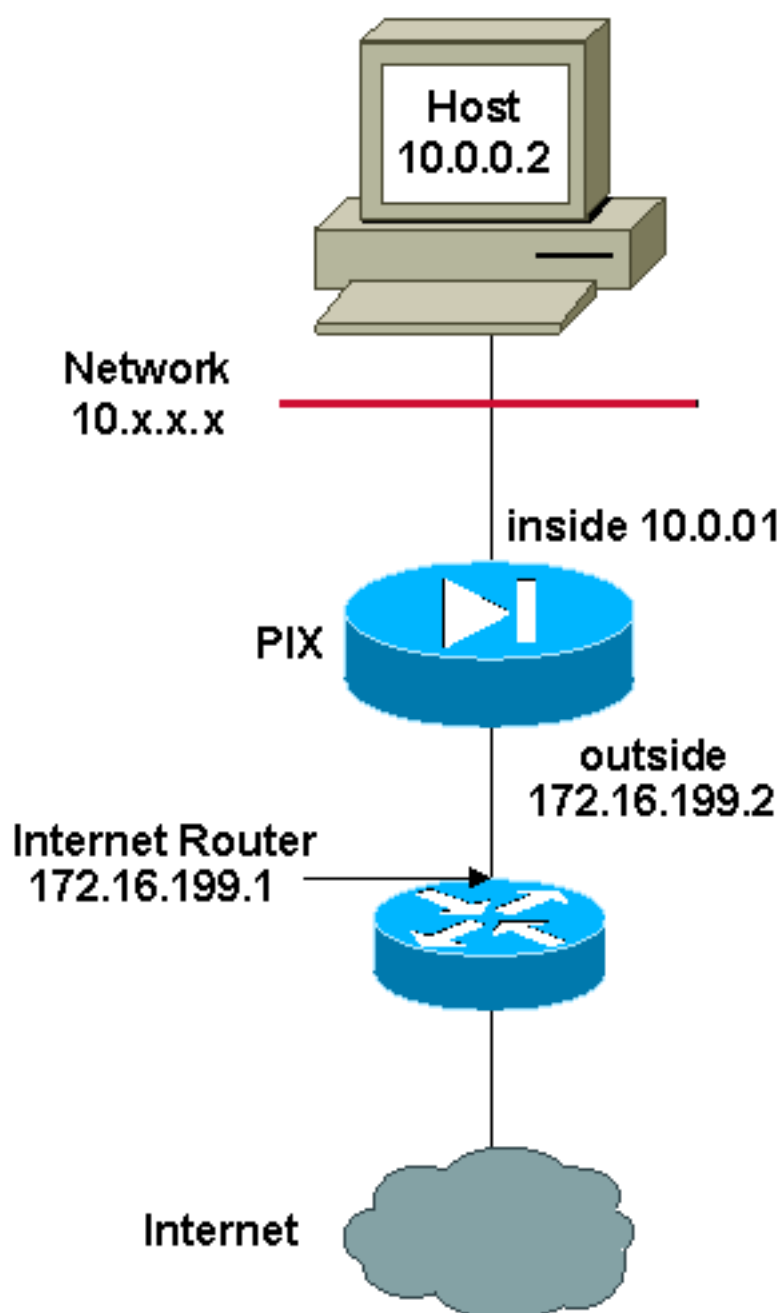
```
nat (inside) 1 10.0.0.0 255.0.0.0
nat (inside) 2 10.1.0.0 255.255.0.0
global (outside) 1 172.16.1.1
global (outside) 2 192.168.1.1
```

Si le réseau interne est sur 10.1.0.0, le NAT global 2 est prioritaire sur 1 car il est plus spécifique pour la traduction.

Remarque: Un système d'adressage générique est utilisé dans la déclaration NAT. Cette déclaration indique à PIX/ASA de traduire n'importe quelle adresse source interne lorsqu'elle accède à Internet. L'adresse de cette commande peut être plus spécifique si vous le désirez.

Mélange de déclarations globales NAT et PAT

Diagramme du réseau



Remarque: 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.

Dans cet exemple, l'ISP fournit au responsable du réseau une plage d'adresses de 172.16.199.1 à 172.16.199.63 à l'usage de la société. Le responsable du réseau décide d'utiliser 172.16.199.1 pour l'interface interne sur le routeur Internet et 172.16.199.2 pour l'interface externe sur le pare-feu PIX/ASA. Vous pouvez utiliser la plage 172.16.199.3 à 172.16.199.62 pour le pool NAT. Cependant, le responsable du réseau sait qu'à n'importe quel moment, plus de soixante personnes peuvent tenter de sortir du PIX/ASA. Par conséquent, le responsable du réseau décide de prendre 172.16.199.62 et d'en faire une adresse PAT de sorte que plusieurs utilisateurs puissent partager une adresse simultanément.

```
global (outside) 1 172.16.199.3-172.16.199.61 netmask 255.255.255.192
```

```
global (outside) 1 172.16.199.62 netmask 255.255.255.192
```

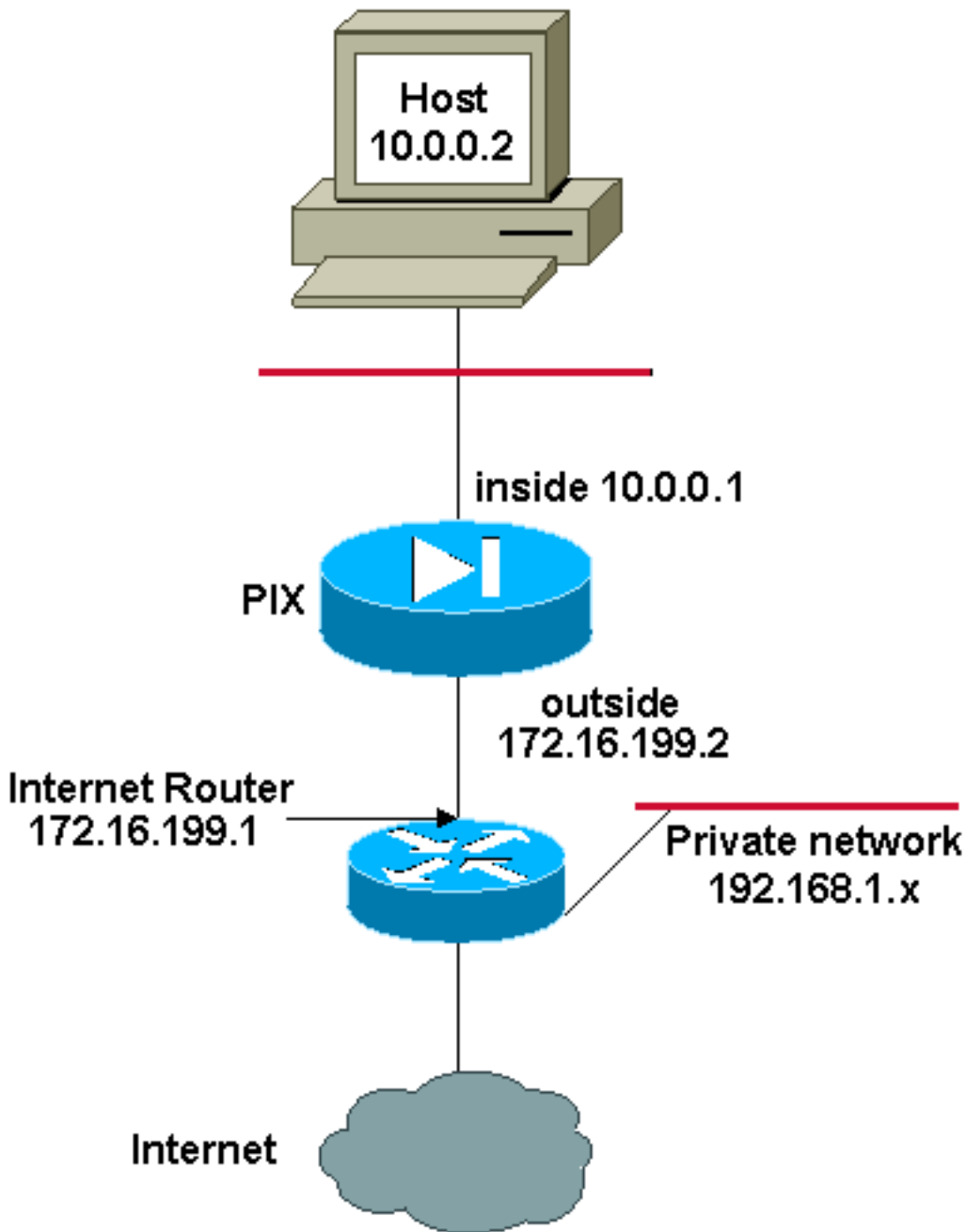
```
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

Ces commandes demandent au PIX/ASA de traduire les adresses source comprise entre 172.16.199.3 et 172.16.199.61 pour que les cinquante-neuf premiers utilisateurs internes passent par PIX/ASA. Une fois ces adresses épuisées, PIX traduit toutes les adresses source vers 172.16.199.62 jusqu'à ce qu'une des adresses du pool NAT devienne libre.

Remarque: Un système d'adressage générique est utilisé dans la déclaration NAT. Cette déclaration indique à PIX/ASA de traduire n'importe quelle adresse source interne lorsqu'elle accède à Internet. L'adresse de cette commande peut être plus spécifique si vous le désirez.

[Plusieurs déclarations NAT avec la liste d'accès NAT 0](#)

[Diagramme du réseau](#)



Remarque: 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.

Dans cet exemple, le FAI fournit au responsable du réseau une plage d'adresses comprises entre 172.16.199.1 et 172.16.199.63. Le responsable du réseau décide d'attribuer 172.16.199.1 à l'interface interne sur le routeur Internet et 172.16.199.2 à l'interface externe du PIX/ASA.

Cependant, dans ce scénario, un autre segment de LAN privé est placé après le routeur Internet. Le responsable du réseau préférerait ne pas gaspiller d'adresses du pool global lorsque des hôtes de ces deux réseaux parlent entre eux. Le responsable du réseau doit toujours traduire l'adresse source pour tous les utilisateurs internes (10.0.0.0/8) lorsqu'ils accèdent à Internet.

```
access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0
```

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
```

```
nat (inside) 0 access-list 101
```

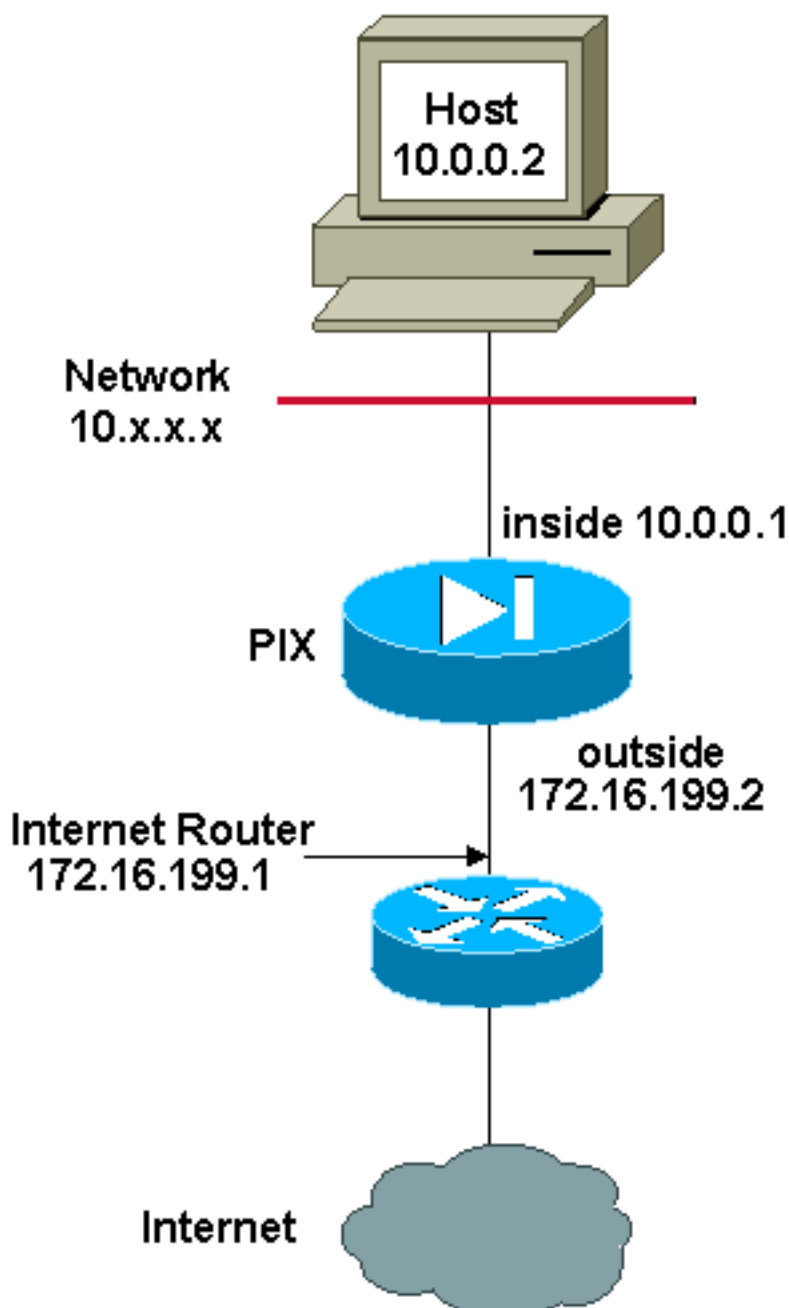
```
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Cette configuration ne traduit pas ces adresses avec une adresse source de 10.0.0.0/8 et une adresse de destination de 192.168.1.0/24. Elle traduit l'adresse source de n'importe quel trafic issu du réseau 10.0.0.0/8 et destiné à n'importe quel emplacement autre que 192.168.1.0/24 en une adresse de la plage comprise entre 172.16.199.3 et 172.16.199.62.

Si vous disposez de la sortie d'une commande **write terminal** de votre périphérique Cisco, vous pouvez utiliser l'outil [Interpréteur de sortie](#) (clients [enregistrés](#) uniquement).

Utilisation du NAT de stratégie

Diagramme du réseau



Remarque: 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.

Lorsque vous utilisez une liste d'accès avec la commande `nat` pour n'importe quel ID NAT autre que 0, vous activez le NAT de stratégie.

Remarque: Le NAT de stratégie a été introduit dans la version 6.3.2.

Le NAT de stratégie vous permet d'identifier le trafic local pour la traduction d'adresses lorsque vous spécifiez les adresses (ou ports) source et de destination dans une liste d'accès. Les NAT standard utilisent uniquement des adresses/ports source, tandis que le NAT de stratégie utilise à la fois les adresses/ports source et de destination.

Remarque: Tous les types de NAT prennent en charge le NAT de stratégie excepté l'exemption NAT (**liste d'accès NAT 0**). L'exemption NAT utilise une liste de contrôle d'accès afin d'identifier les adresses locales, mais diffère du NAT de stratégie, car les ports ne sont pas pris en compte.

Avec le NAT de stratégie, vous pouvez créer plusieurs NAT ou déclarations statiques qui identifient la même adresse locale tant que la combinaison source/port et destination/port est unique pour chaque déclaration. Vous pouvez alors associer plusieurs adresses globales à chaque paire source/port et destination/port.

Dans cet exemple, le responsable du réseau fournit un accès à l'adresse IP de destination 192.168.201.11 pour le port 80 (Web) et le port 23 (Telnet), mais doit utiliser deux adresses IP différentes comme adresse source. L'adresse IP 172.16.199.3 est utilisée comme adresse source pour le Web. L'adresse IP 172.16.199.4 est utilisée pour Telnet, et doit convertir toutes les adresses internes de la plage 10.0.0.0/8. Le responsable du réseau peut faire ceci de la façon suivante :

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 80

access-list TELNET permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB

nat (inside) 2 access-list TELNET

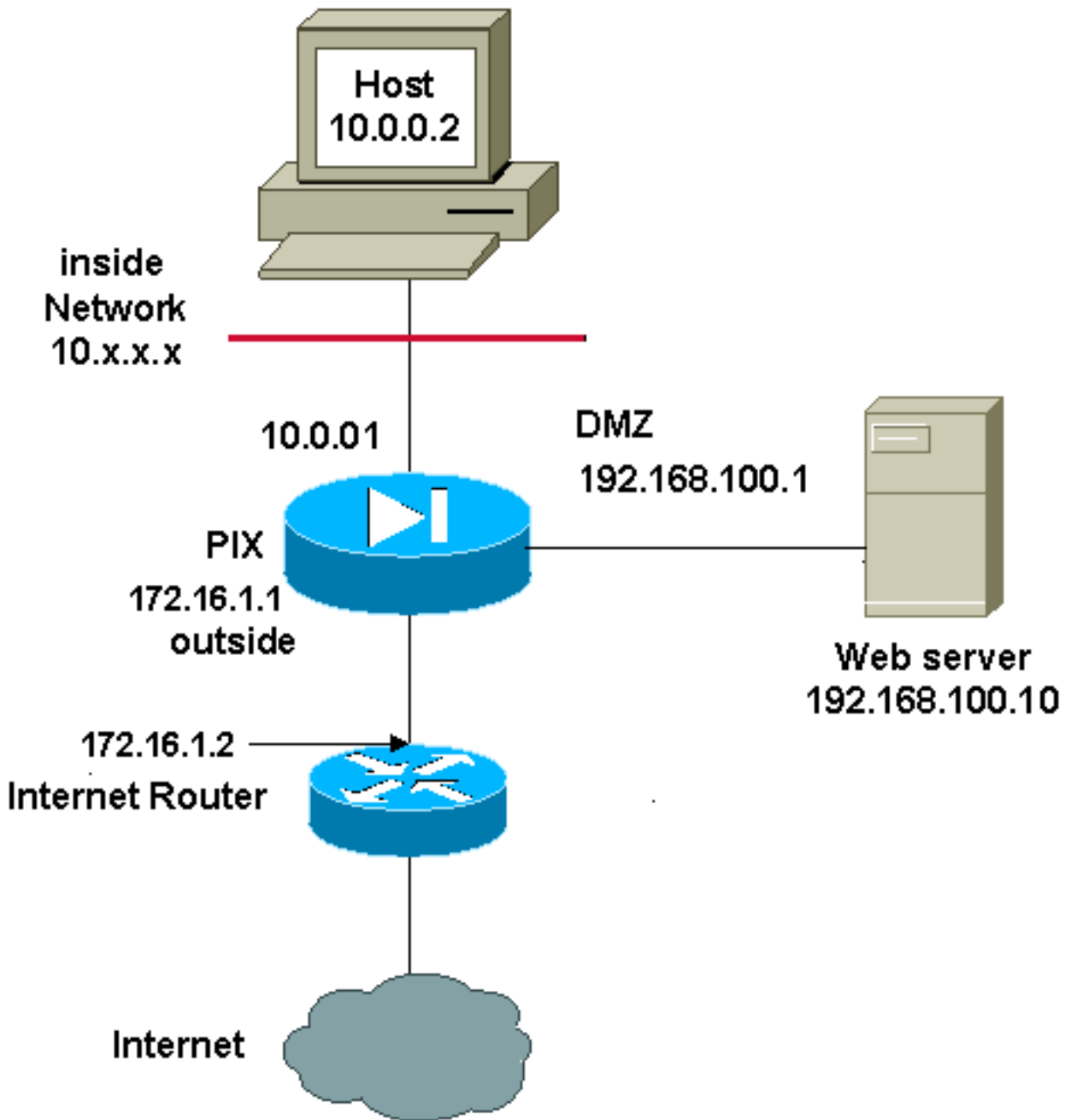
global (outside) 1 172.16.199.3 netmask 255.255.255.192

global (outside) 2 172.16.199.4 netmask 255.255.255.192
```

Vous pouvez utiliser l'outil [Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) afin d'afficher les problèmes et correctifs potentiels.

[NAT statique](#)

[Diagramme du réseau](#)



Remarque: 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.

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. Cela est surtout utile pour les hôtes qui fournissent des services d'application comme le courrier électronique, le Web, le protocole FTP, etc. Dans cet exemple, les déclarations du NAT statique sont configurées pour permettre à des utilisateurs internes et à des utilisateurs externes d'accéder au serveur Web sur la DMZ.

Cette sortie montre comment une déclaration statique est construite. Notez l'ordre des adresses IP mappées et réelles.

```
static (real_interface,mapped_interface) mapped_ip real_ip netmask mask
```

Voici la traduction statique créée pour permettre aux utilisateurs de l'interface interne d'accéder au serveur sur la DMZ. Elle crée un mappage entre une adresse interne et l'adresse du serveur sur la DMZ. Les utilisateurs internes peuvent alors accéder au serveur sur la DMZ par l'intermédiaire de l'adresse interne.

```
static (DMZ,inside) 10.0.0.10 192.168.100.10 netmask 255.255.255.255
```

Voici la traduction statique créée pour permettre aux utilisateurs de l'interface externe d'accéder au serveur sur la DMZ. Elle crée un mappage entre une adresse externe et l'adresse du serveur sur la DMZ. Les utilisateurs externes peuvent alors accéder au serveur sur la DMZ par l'intermédiaire de l'adresse externe.

```
static (DMZ,outside) 172.16.1.5 192.168.100.10 netmask 255.255.255.255
```

Remarque: Puisque l'interface externe a un niveau de sécurité inférieur à la DMZ, une liste d'accès doit également être créée afin de permettre à des utilisateurs externes d'accéder au serveur sur la DMZ. La liste d'accès doit accorder aux utilisateurs l'accès à l'**adresse mappée** dans la traduction statique. Il est recommandé de rendre cette liste d'accès aussi spécifique que possible. Dans ce cas, tous les hôtes peuvent accéder uniquement aux ports 80 (www/http) et 443 (https) sur le serveur Web.

```
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq www
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq https
```

La liste d'accès doit alors être appliquée à l'interface externe.

```
access-group OUTSIDE in interface outside
```

Référez-vous à la [liste d'accès étendue](#) et au [groupe d'accès](#) pour plus d'informations sur les commandes **access-list** et **access-group**.

[Comment contourner le NAT](#)

Cette section décrit comment contourner le NAT. Lorsque vous activez le contrôle NAT, il est possible que vous souhaitiez contourner le NAT. Vous pouvez utiliser le NAT d'identité, le NAT d'identité statique ou l'exemption NAT afin de contourner le NAT.

[Configurer le NAT d'identité](#)

Le NAT d'identité traduit l'adresse IP réelle vers la même adresse IP. Seuls les hôtes « traduits » peuvent créer des traductions NAT et le trafic répondant est à nouveau autorisé.

Remarque: Si vous changez de configuration NAT, et que vous ne souhaitez pas attendre que des traductions existantes expirent pour que les nouvelles informations NAT soient utilisées, utilisez la commande **clear xlate** afin d'effacer la table de traduction. Cependant, toutes les connexions actuelles qui utilisent des traductions sont déconnectées lorsque vous effacez la table de traduction.

Afin de configurer le NAT d'identité, entrez cette commande :

```
hostname(config)#nat (real_interface) 0 real_ip
```

```
[mask [dns] [outside] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp
udp_max_conns]
```

Par exemple, afin d'utiliser le NAT d'identité pour le réseau interne 10.1.1.0/24, entrez cette commande :

```
hostname(config)#nat (inside) 0 10.1.1.0
255.255.255.0
```

Référez-vous à [Référence de commandes des appliances de sécurité Cisco version 7.2](#) pour plus d'informations sur la commande `nat`.

Configurer le NAT d'identité statique

Le NAT d'identité statique traduit l'adresse IP réelle vers la même adresse IP. La traduction est toujours active et les hôtes « traduits » et distants peuvent lancer des connexions. Le NAT d'identité statique vous permet d'utiliser des NAT ou NAT de stratégie standard. Le NAT de stratégie vous permet d'identifier les adresses réelles et de destination en déterminant l'adresse réelle à traduire (voir la section [Utilisation du NAT de stratégie](#) pour plus d'informations sur le NAT de stratégie). Par exemple, vous pouvez utiliser le NAT d'identité statique de stratégie pour une adresse interne lorsqu'elle accède à l'interface externe et que le serveur de destination est le serveur A, mais utilisez une traduction normale lorsque vous accédez au serveur externe B.

Remarque: Si vous supprimez une commande statique, les connexions actuelles qui utilisent la traduction ne sont pas affectées. Pour supprimer ces connexions, entrez la commande [clear local-host](#). Vous ne pouvez pas supprimer les traductions statiques de la table de traduction avec la commande `clear xlate`. Vous devez supprimer la commande statique. Seules les traductions dynamiques créées par les commandes `nat` et `global` peuvent être supprimées avec la commande [clear xlate](#).

Pour configurer le NAT d'identité statique, entrez cette commande :

```
hostname(config)#static
(real_interface,mapped_interface) real_ip access-list acl_id [dns]
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

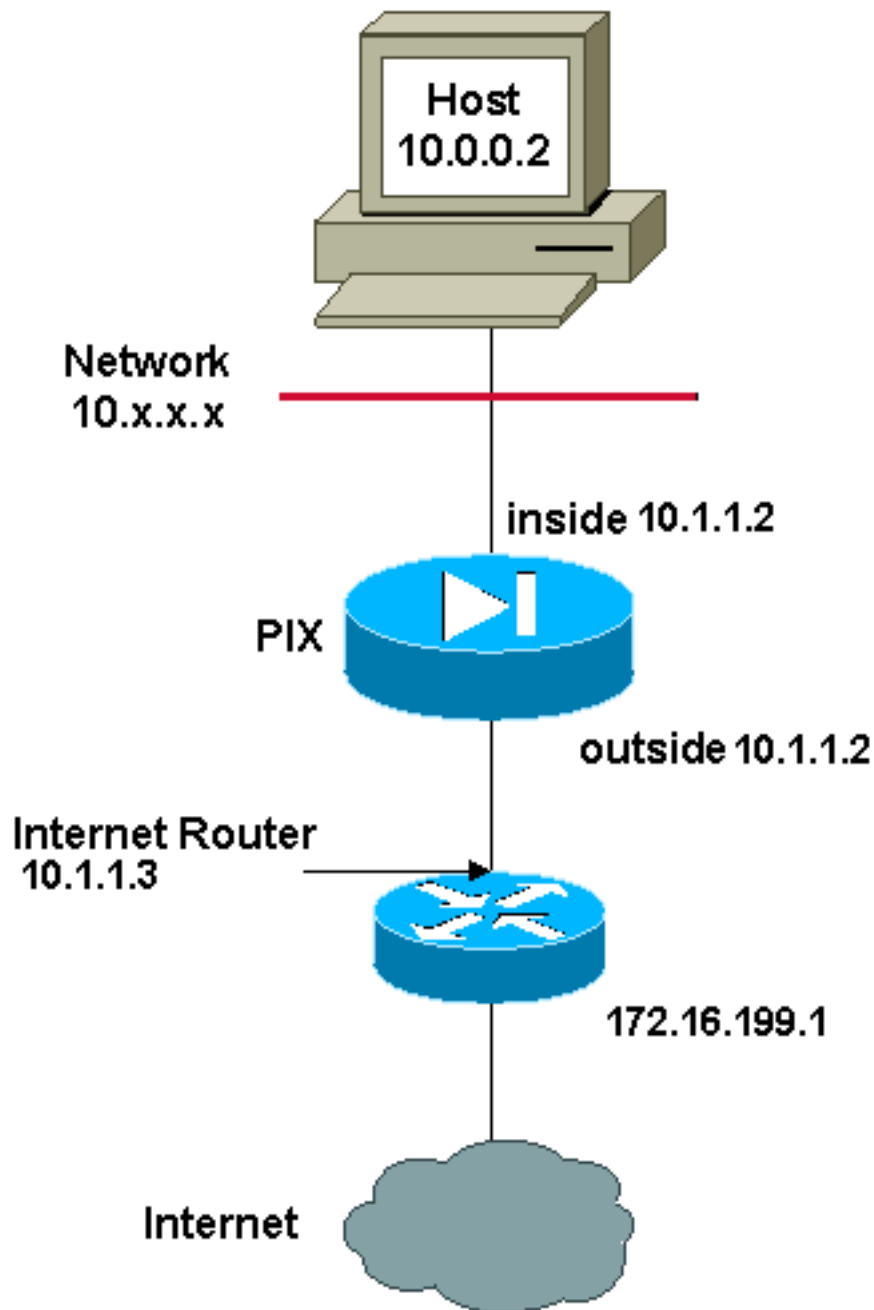
Utilisez la commande `access-list extended` pour créer la [liste d'accès étendue](#). Cette liste d'accès devrait inclure uniquement les ACE autorisés. Assurez-vous que l'adresse source dans la liste d'accès correspond à l'argument `real-ip` de cette commande. Le NAT de stratégie ne prend pas en compte les mots-clés inactifs ou de la plage de temps ; tous les ACE sont considérés actifs pour la configuration du NAT de stratégie. Pour plus d'informations, consultez [Utilisation du NAT de stratégie](#).

Afin de configurer le NAT d'identité statique standard, entrez cette commande :

```
hostname(config)#static
(real_interface,mapped_interface) real_ip real_ip [netmask mask] [dns]
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp
udp_max_conns]
```

Spécifiez la même adresse IP pour les deux arguments `real_ip`.

Diagramme du réseau



Remarque: 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.

Par exemple, cette commande utilise le NAT d'identité statique pour une adresse IP interne (10.1.1.2) lorsqu'elle est consultée depuis l'extérieur :

```
hostname(config)#static (inside,outside) 10.1.1.2  
10.1.1.2 netmask 255.255.255.255
```

Référez-vous à [Référence de commandes des appliances de sécurité Cisco version 7.2](#) pour plus d'informations sur la commande **static**.

Cette commande utilise le NAT d'identité statique pour une adresse externe (172.16.199.1) lorsqu'elle est consultée depuis l'intérieur :

```
hostname(config)#static (outside,inside) 172.16.199.1
172.16.199.1 netmask 255.255.255.255
```

Cette commande mappe statiquement un sous-réseau entier :

```
hostname(config)#static (inside,dmz) 10.1.1.2 10.1.1.2
netmask 255.255.255.0
```

Cet exemple de NAT de stratégie d'identité statique présente une adresse réelle unique qui utilise le NAT d'identité lorsqu'elle accède à une adresse de destination et une traduction lorsqu'elle accède à une autre adresse :

```
hostname(config)#access-list NET1 permit ip host
10.1.1.3 172.16.199.0 255.255.255.224
```

```
hostname(config)#access-list NET2 permit ip host
10.1.1.3 172.16.199.224 255.255.255.224
```

```
hostname(config)#static (inside,outside) 10.1.1.3
access-list NET1
```

```
hostname(config)#static (inside,outside) 172.16.199.1
access-list NET2
```

Remarque: Pour plus d'informations sur la commande **static**, référez-vous à [Dispositif de sécurité adaptatif dédié Cisco ASA 5580, version 8.1](#).

Remarque: Pour plus d'informations sur les listes d'accès, référez-vous à [Guide de configuration de la ligne de commande du dispositif de sécurité adaptatif dédié Cisco ASA 5580, version 8.1](#).

[Configurer l'exemption NAT](#)

L'exemption NAT exempte les adresses de traduction et permet aux hôtes réels et distants de lancer des connexions. L'exemption NAT vous permet de spécifier l'adresse réelle et de destination lorsque vous déterminez le trafic réel à exempter (semblable au NAT de stratégie). Ainsi, l'exemption NAT vous procure un plus grand contrôle que le NAT d'identité. Cependant à la différence du NAT de stratégie, l'exemption NAT ne prend pas en compte les ports dans la liste d'accès. Employez le NAT d'identité statique pour prendre en considération des ports dans la liste d'accès.

Remarque: La suppression d'une configuration d'exemption NAT n'affecte pas les connexions existantes qui utilisent l'exemption NAT. Pour supprimer ces connexions, entrez la commande [clear local host](#).

Pour configurer l'exemption NAT, entrez cette commande :

```
hostname(config)#nat (real_interface) 0 access-list
```



```
acl_name [outside]
```

Créez la [liste d'accès étendue](#) à l'aide de la commande [access-list extended](#). Cette liste d'accès peut inclure à la fois les ACE autorisés et interdits. Ne spécifiez pas le port réel et de destination dans la liste d'accès ; L'exemption NAT ne prend pas en compte les ports. L'exemption NAT ne prend pas non plus en compte les mots-clés inactifs ou de la plage de temps ; tous les ACE sont considérés actifs pour la configuration de l'exemption NAT.

Par défaut, cette commande exempte le trafic de l'intérieur vers l'extérieur. Si vous souhaitez que le trafic de l'extérieur vers l'intérieur contourne le NAT, ajoutez une commande `nat` supplémentaire et entrez « outside » pour identifier l'instance NAT comme NAT externe. Vous pourriez vouloir utiliser l'exemption NAT externe si vous configurez un NAT dynamique pour l'interface externe et souhaitez exempter tout autre trafic.

Par exemple, afin d'exempter un réseau interne lors de l'accès à n'importe quelle adresse de destination, entrez cette commande :

```
hostname(config)#access-list EXEMPT permit ip 10.1.1.0  
255.255.255.0 any
```

```
hostname(config)# nat (inside) 0 access-list  
EXEMPT
```

Afin d'utiliser le NAT externe dynamique pour un réseau DMZ et exempter un autre réseau DMZ, entrez cette commande :

```
hostname(config)#nat (dmz) 1 10.1.1.0 255.255.255.0  
outside dns
```

```
hostname(config)#global (inside) 1  
10.1.1.2
```

```
hostname(config)#access-list EXEMPT permit ip 10.1.1.0  
255.255.255.0 any
```

```
hostname(config)#nat (dmz) 0 access-list  
EXEMPT
```

Afin d'exempter une adresse interne lors de l'accès à deux adresses de destination différentes, entrez cette commande :

```
hostname(config)#access-list NET1 permit ip 10.1.1.0  
255.255.255.0 172.16.199.0 255.255.255.224
```

```
hostname(config)#access-list NET1 permit ip 10.1.1.0  
255.255.255.0 172.16.199.224 255.255.255.224
```

```
hostname(config)#nat (inside) 0 access-list NET1
```

Vérifier

Le trafic qui traverse l'appareil de sécurité passe très probablement par un NAT. Reportez-vous à la section [PIX/ASA : Surveillance et dépannage des problèmes de performances](#) afin de vérifier les traductions en service sur l'appareil de sécurité.

La commande **show xlate count** affiche le nombre actuel et maximal de traductions par PIX. Une traduction est un mappage d'une adresse interne à une adresse externe et peut être un mappage un-à-un, tel que NAT, ou plusieurs-à-un tel que PAT. Cette commande est un sous-ensemble de la commande [show xlate](#) qui indique chaque traduction effectuée par le pare-feu PIX. La sortie de commande présente des traductions « in use », ce qui se rapporte au nombre de traductions actives dans le PIX lorsque la commande est émise ; « most used » se rapporte au maximum de traductions maximum observées sur le PIX depuis sa mise sous tension.

Dépanner

Message d'erreur reçu en ajoutant un PAT statique pour le port 443

Problème

Vous recevez ce message d'erreur quand vous ajoutez un PAT statique pour le port 443 :

```
[ERREUR] (À L'INTÉRIEUR, DEHORS) TCP statique de 255.255.255.255 de netmask de 192.168.1.87 443 de l'interface 443 de TCP 0 0 UDP 0
```

```
incapable de réserver le port 443 pour le PAT statique
```

```
ERREUR : incapable de télécharger la stratégie
```

Solution

Ce message d'erreur se produit quand l'ASDM ou le WEBVPN s'exécute sur le port 443. Afin de résoudre ce problème, ouvrez une session au Pare-feu, et terminez-vous une de ces étapes :

- Afin de changer l'ASDM mettez en communication à n'importe quoi autre que 443, exécutent ces commandes :

```
ASA(config)#no http server enable  
ASA(config)#http server enable 8080
```

- Afin de changer le WEBVPN mettez en communication à n'importe quoi autre que 443, exécutent ces commandes :

```
ASA(config)#webvpn  
ASA(config-webvpn)#enable outside  
ASA(config-webvpn)#port 65010
```

Après que vous exécutiez ces commandes, vous devriez pouvoir ajouter un NAT/PAT sur le port 443 à un autre serveur. Quand vous tentez d'employer l'ASDM pour gérer l'ASA à l'avenir, spécifiez le nouveau port en tant que 8080.

ERREUR : conflit de tracer-adresse avec la charge statique existante

Problème

Vous recevez cette erreur quand vous ajoutez une déclaration statique sur l'ASA :

```
ERREUR : conflit de tracer-adresse avec la charge statique existante
```

Solution

Vérifiez qu'une entrée n'existe pas déjà pour la source statique que vous voulez ajouter.

Informations connexes

- [Page de support PIX](#)
- [Références des commandes du pare-feu PIX](#)
- [ASA Support Page](#)
- [Références des commandes ASA](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)