ASA 7.x/PIX 6.x et versions ultérieures : Exemple de configuration d'ouverture ou de blocage des ports

Contenu

Introduction

Ce document fournit un exemple de configuration pour ouvrir ou bloquer les ports pour les différents types de trafic, tel que le trafic HTTP ou FTP, dans l'appliance de sécurité.

Note : Les termes « ouverture du port » et « autorisation du port » ont la même signification. De même, « bloquer le port » et « restreindre le port » ont aussi la même signification.

Conditions préalables

Conditions requises

Ce document suppose que PIX/ASA est configuré et fonctionne correctement.

Components Used

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

- Appareil de sécurité adaptatif (ASA) de la gamme Cisco 5500 qui exécute la version 8.2(1)

- Cisco Adaptive Security Device Manager (ASDM) version 6.3(5)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Cette configuration peut également être utilisée avec l'appliance de pare-feu PIX de la gamme Cisco 500 avec les versions 6.x et ultérieures du logiciel.

Conventions

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

Configuration

Chaque interface doit avoir un niveau de sécurité compris entre 0 (inférieur) et 100 (supérieur). Par exemple, vous devez affecter votre réseau le plus sécurisé, tel que le réseau hôte interne, au niveau 100. Alors que le réseau externe connecté à Internet peut être de niveau 0, d'autres réseaux, tels que les DMZ, peuvent être placés entre les deux. Vous pouvez affecter plusieurs interfaces au même niveau de sécurité.

Par défaut, tous les ports sont bloqués sur l'interface externe (niveau de sécurité 0) et tous les ports sont ouverts sur l'interface interne (niveau de sécurité 100) du dispositif de sécurité. De cette manière, tout le trafic sortant peut passer par l'appliance de sécurité sans aucune configuration, mais le trafic entrant peut être autorisé par la configuration de la liste d'accès et des commandes statiques dans l'appliance de sécurité.

Remarque : En général, tous les ports sont bloqués de la zone de sécurité inférieure à la zone de sécurité supérieure et tous les ports sont ouverts de la zone de sécurité supérieure à la zone de sécurité inférieure, à condition que l'inspection dynamique soit activée pour le trafic entrant et sortant.

Cette section comprend les sous-sections suivantes :

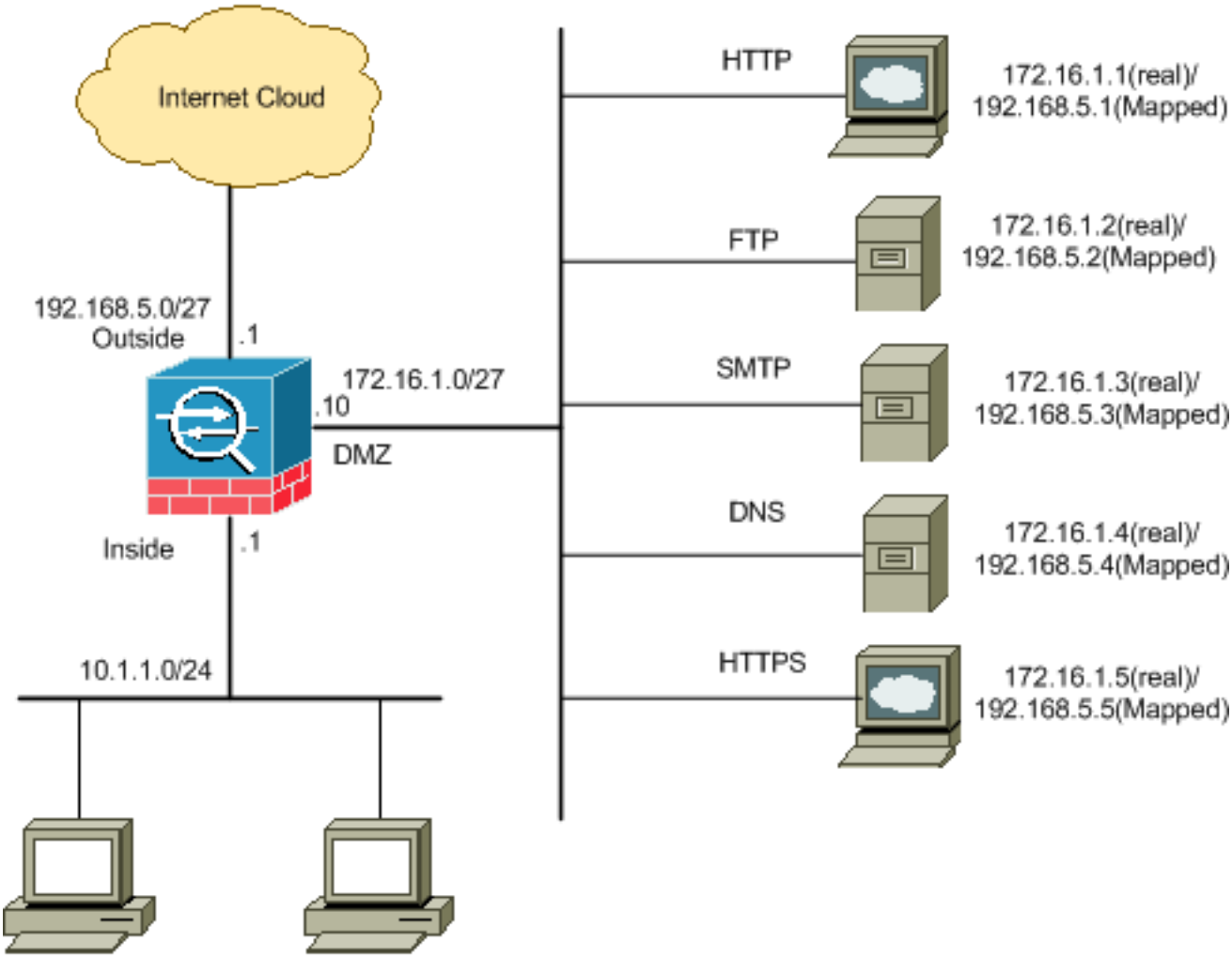
- Diagramme du réseau
- Blocage de la configuration des ports
- Ouverture de la configuration des ports

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Blocage de la configuration des ports

L'appliance de sécurité autorise tout trafic sortant, sauf s'il est explicitement bloqué par une liste de contrôle d'accès étendue.

Une liste d'accès est constituée d'une ou plusieurs entrées de contrôle d'accès. Selon le type de liste d'accès, vous pouvez spécifier les adresses source et de destination, le protocole, les ports (pour TCP ou UDP), le type ICMP (pour ICMP) ou EtherType.

Remarque : Pour les protocoles non orientés connexion, tels qu'ICMP, l'appliance de sécurité établit des sessions unidirectionnelles. Vous avez donc besoin de listes d'accès pour autoriser ICMP dans les deux directions (en appliquant des listes d'accès aux interfaces source et de destination) ou vous devez activer le moteur d'inspection ICMP. Le moteur d'inspection ICMP traite les sessions ICMP comme des connexions bidirectionnelles.

Complétez ces étapes afin de bloquer les ports, qui s'appliquent généralement au trafic provenant de l'intérieur (zone de sécurité supérieure) vers la zone DMZ (zone de sécurité inférieure) ou la zone DMZ vers l'extérieur.

1. Créez une liste de contrôle d'accès de manière à bloquer le trafic de port spécifié.

```
access-list
```

2. Ensuite, liez la liste d'accès à la commande **access-group** afin d'être active.

```
access-group
```

Exemples:

1. **Bloquer le trafic du port HTTP :** Afin de bloquer l'accès au réseau interne 10.1.1.0 via http (serveur Web) avec IP 172.16.1.1 placé dans le réseau DMZ, créez une liste de contrôle d'accès comme indiqué :

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.1  eq 80
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

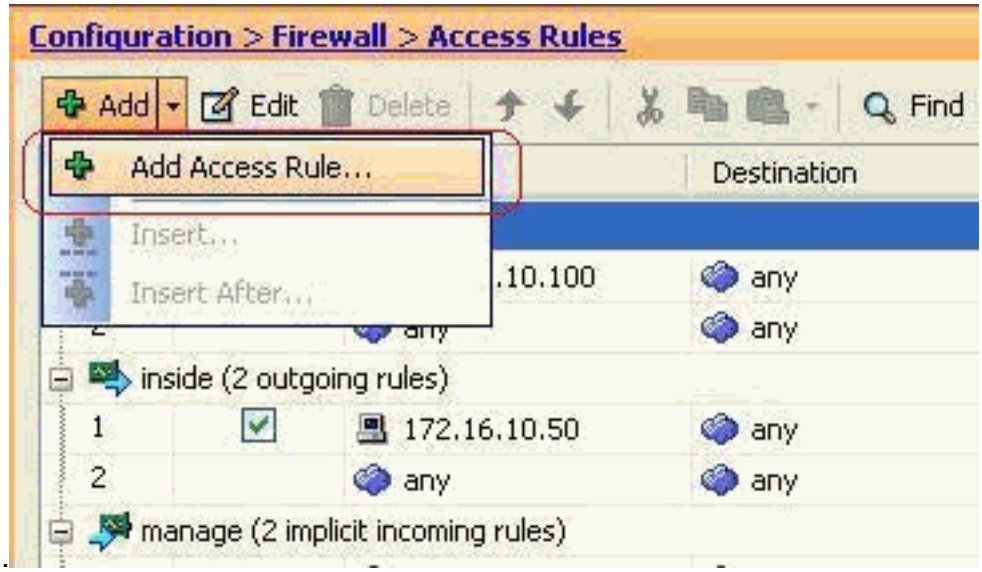
   Remarque : Utilisez **no** suivi des commandes de liste d'accès afin de supprimer le blocage des ports.
2. **Bloquer le trafic du port FTP :** Afin de bloquer l'accès au FTP (serveur de fichiers) du réseau interne 10.1.1.0 avec l'adresse IP 172.16.1.2 placée dans le réseau DMZ, créez une liste de contrôle d'accès comme indiqué :

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.2  eq 21
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

Remarque : référez-vous à ports IANA afin d'en savoir plus sur les affectations de ports.

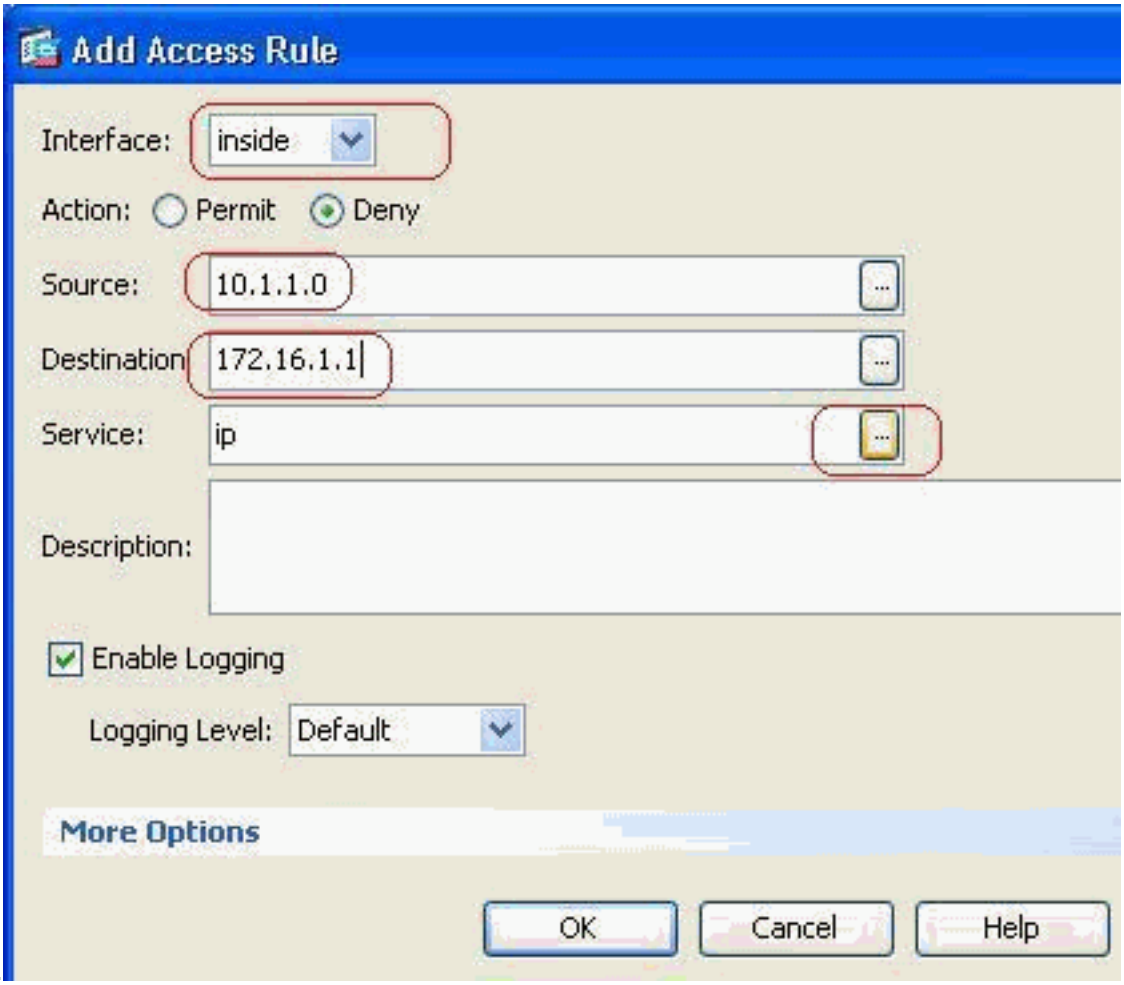
La configuration pas à pas pour effectuer cette opération via l'ASDM est présentée dans cette section.

1. Accédez à **Configuration > Firewall > Access Rules**. Cliquez sur **Ajouter une règle d'accès** pour créer la liste d'accès.



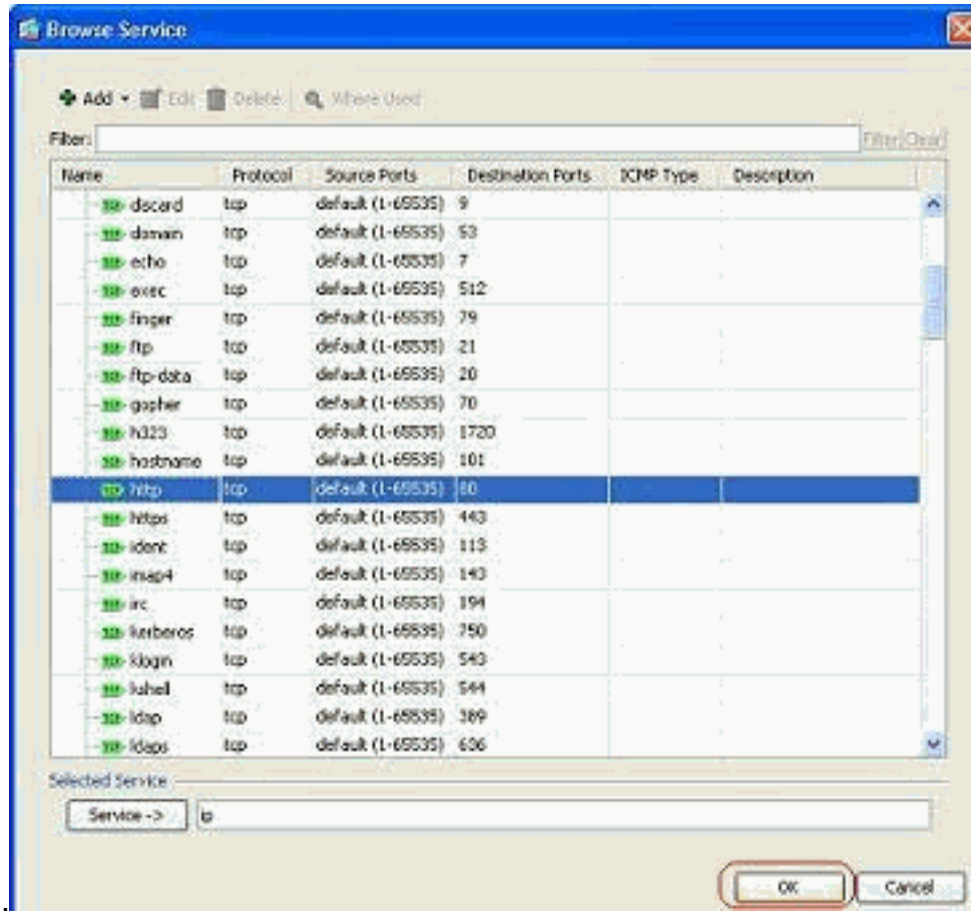
2. Définissez la source et la destination et l'action de la règle d'accès ainsi que l'interface à

laquelle cette règle d'accès sera associée. Sélectionnez les détails pour choisir le port spécifique à



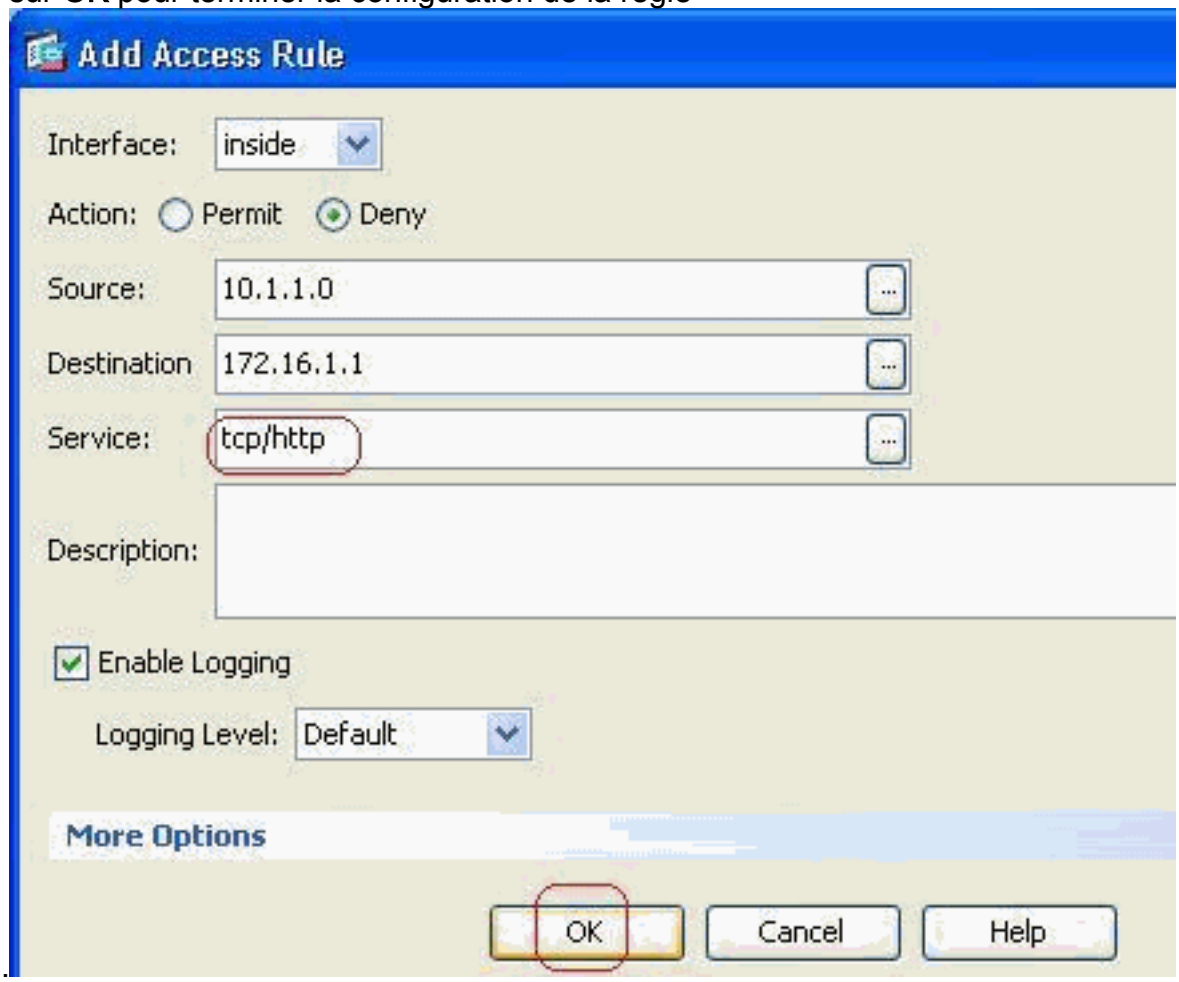
bloquer.

3. Choisissez **http** dans la liste des ports disponibles, puis cliquez sur **OK** pour revenir à la fenêtre Ajouter une règle



d'accès.

4. Cliquez sur **OK** pour terminer la configuration de la règle

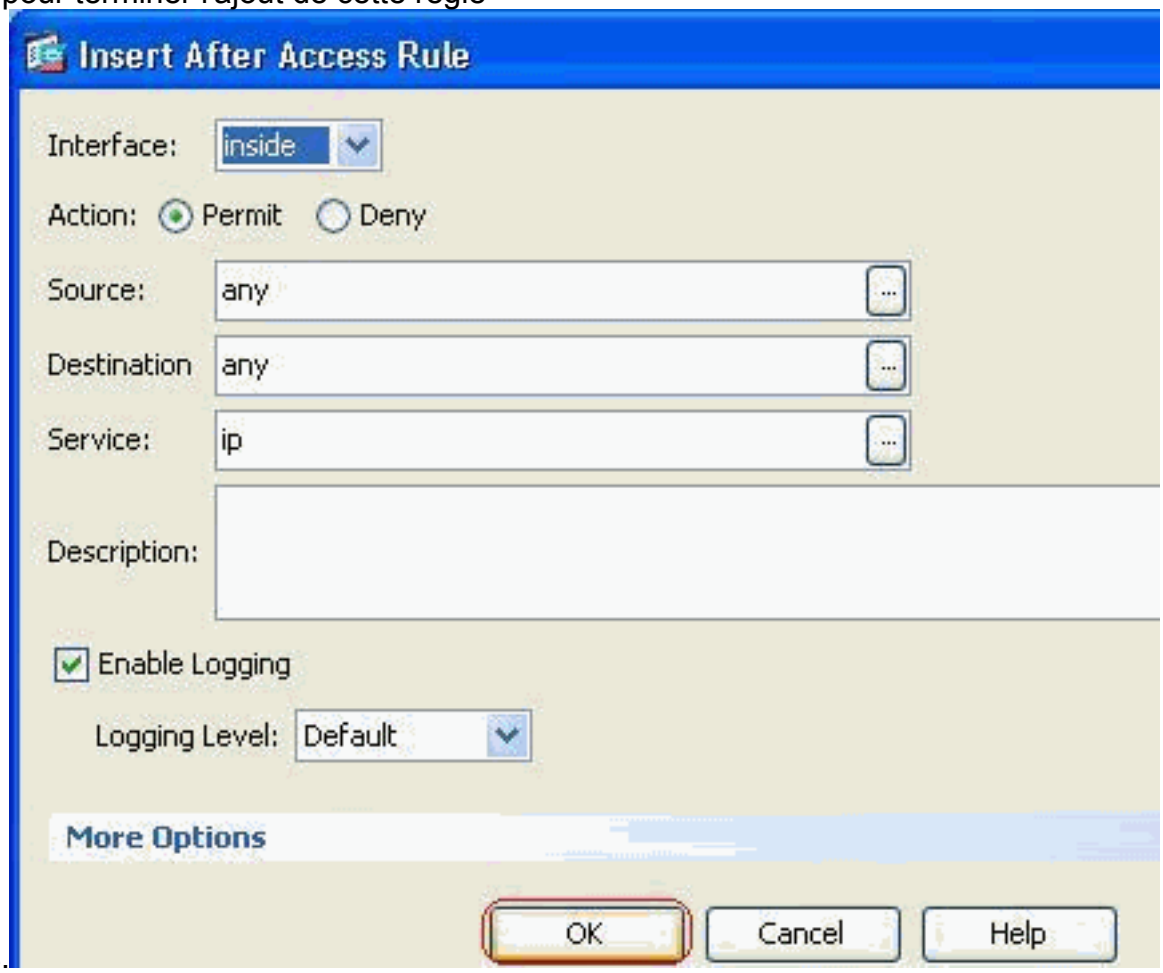


d'accès.

5. Cliquez sur **Insérer après** pour ajouter une règle d'accès à la même liste

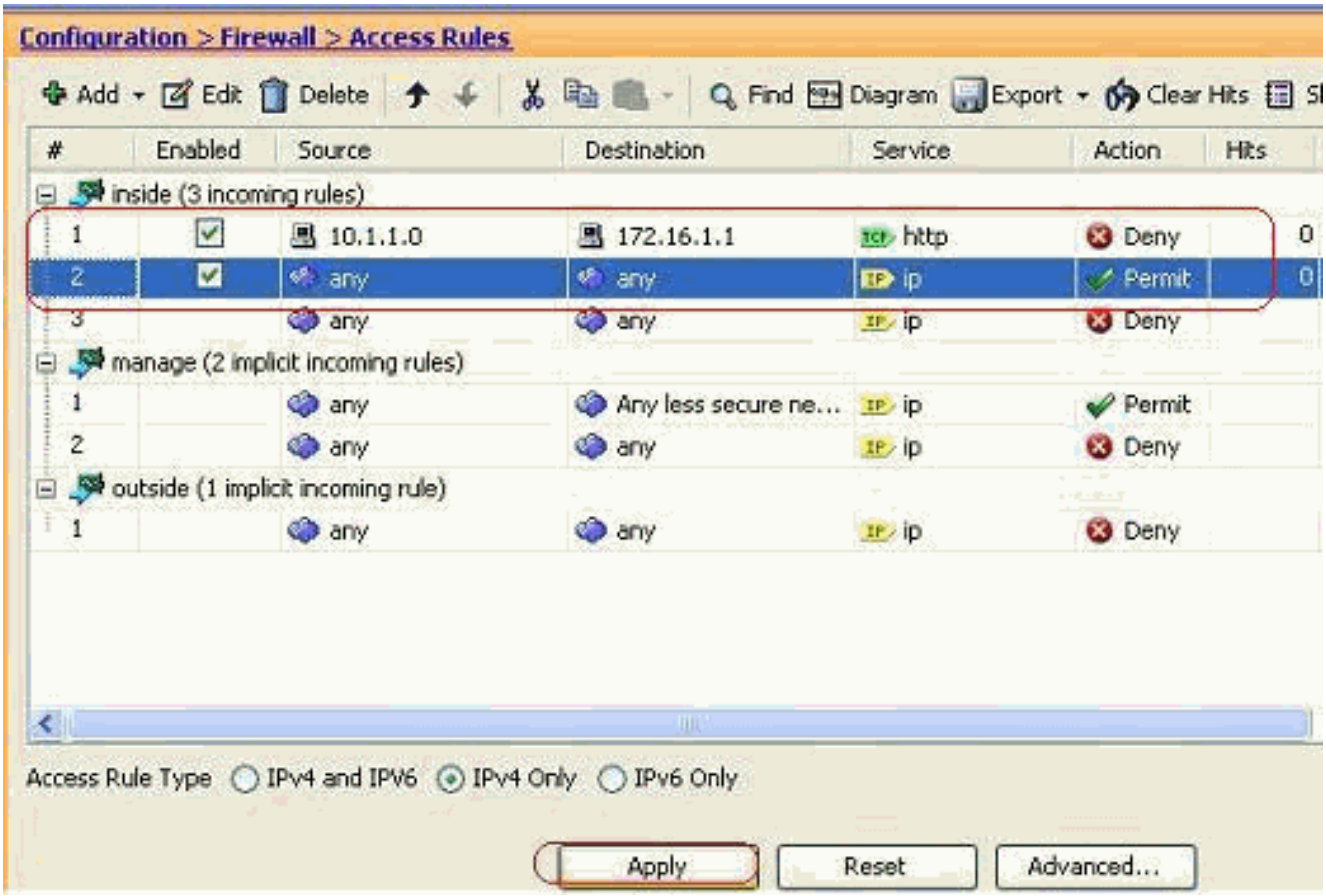
d'accès.

6. Autoriser le trafic de « any » à « any » pour empêcher le « implicit deny ». Cliquez ensuite sur **OK** pour terminer l'ajout de cette règle



d'accès.

7. La liste d'accès configurée est visible dans l'onglet Règles d'accès. Cliquez sur **Apply** pour envoyer cette configuration à l'appliance de sécurité.



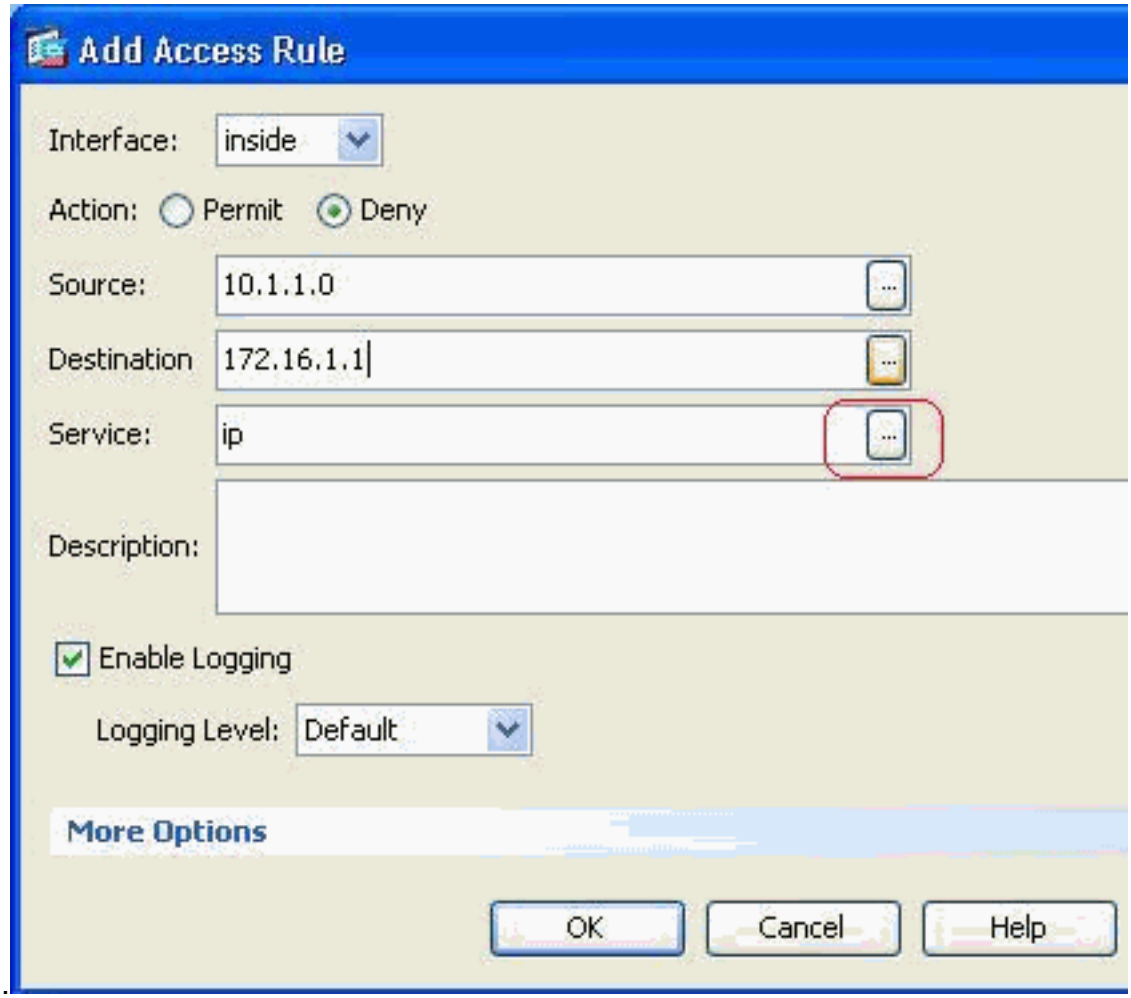
La configuration envoyée à partir de l'ASDM génère cet ensemble de commandes sur l'interface de ligne de commande (CLI) de l'ASA.

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

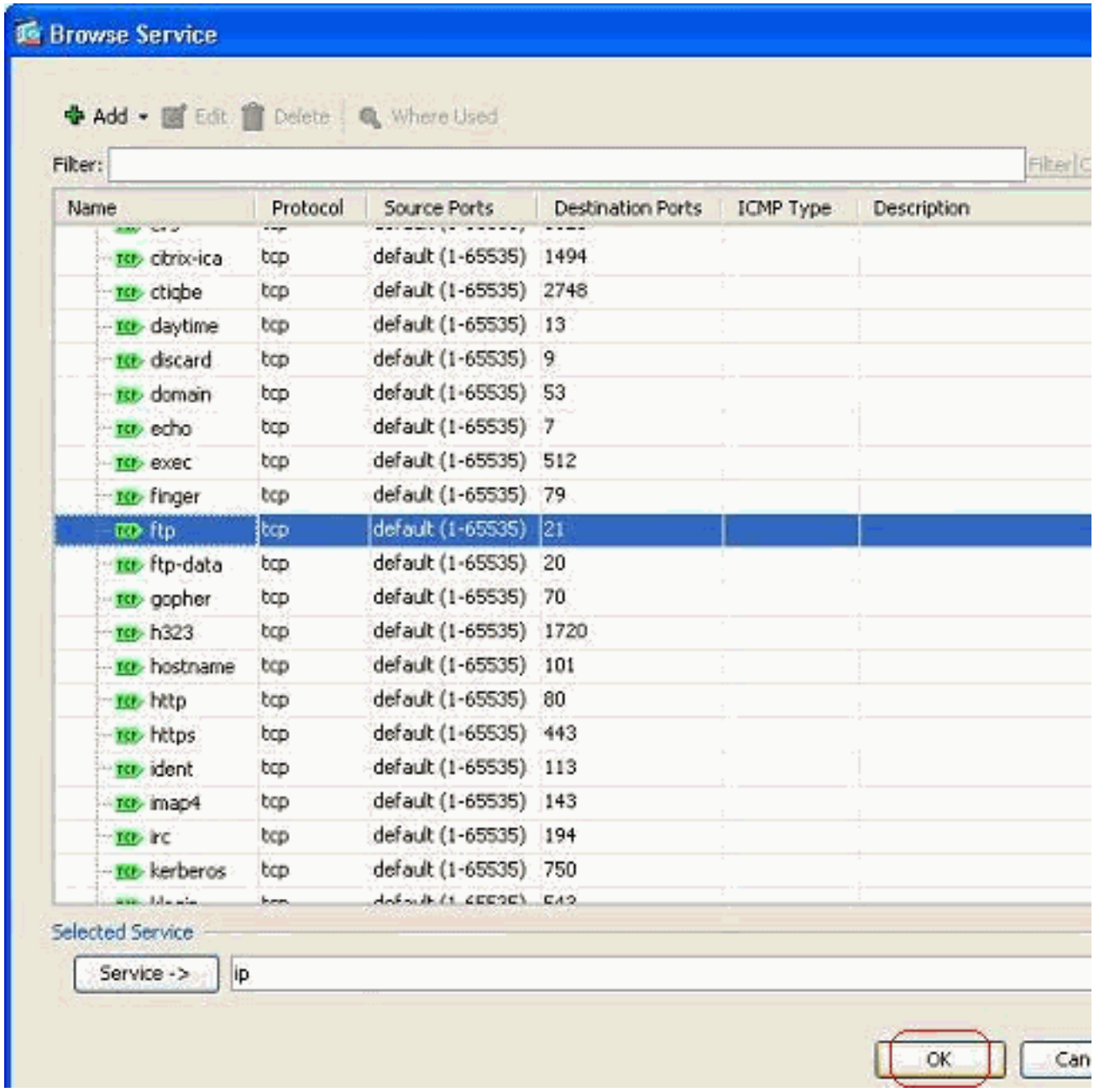
Au cours de ces étapes, l'exemple 1 a été exécuté via ASDM pour empêcher le réseau 10.1.1.0 d'accéder au serveur Web, 172.16.1.1. L'exemple 2 peut également être réalisé de la même manière pour empêcher l'accès au serveur FTP (172.16.1.2) sur l'ensemble du réseau 10.1.1.0. La seule différence sera au moment de choisir le port.**Remarque :** cette configuration de règle d'accès par exemple 2 est supposée être une nouvelle configuration.

8. Définissez la règle d'accès pour bloquer le trafic FTP, puis cliquez sur l'onglet **Détails** pour choisir le port de

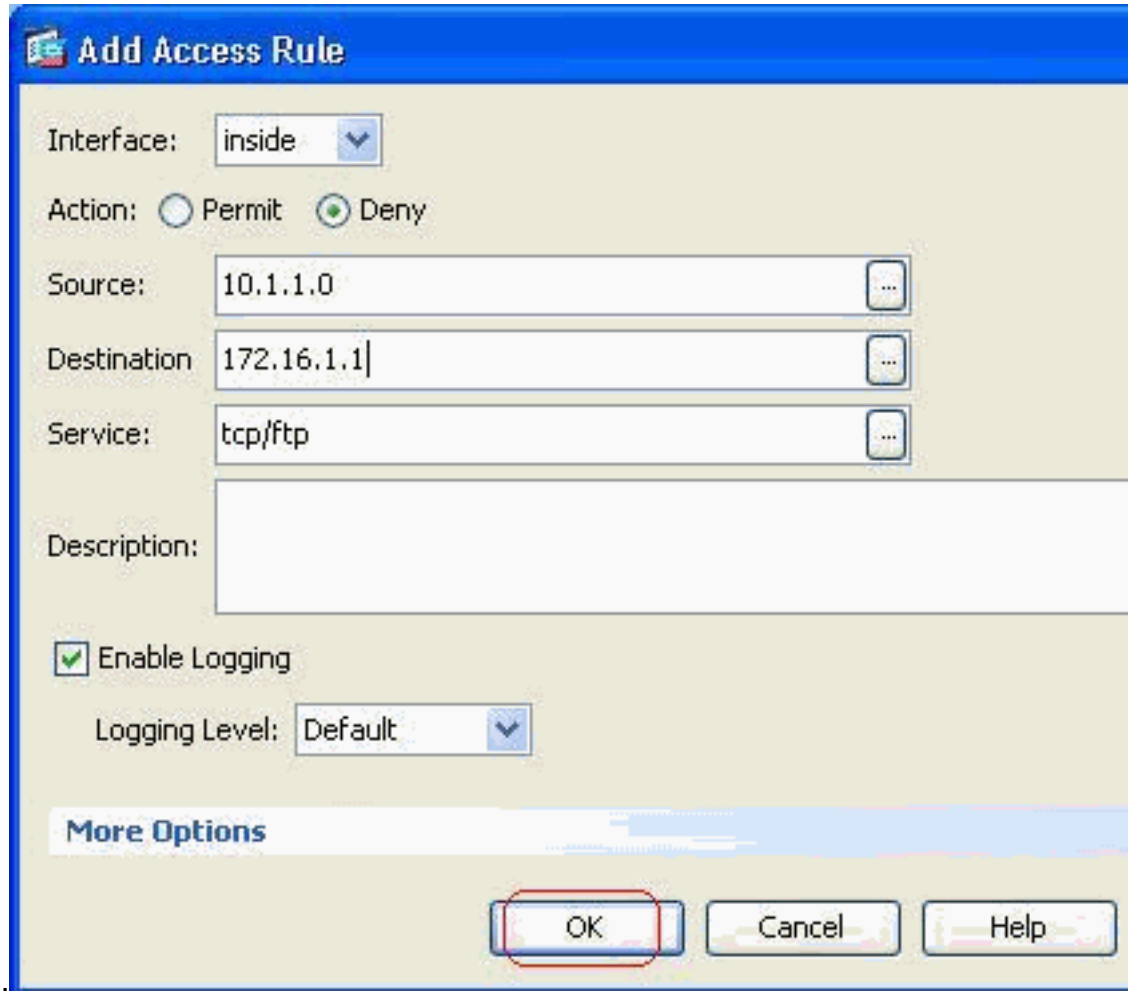
destination.



9. Choisissez le port **ftp** et cliquez sur **OK** pour revenir à la fenêtre Ajouter une règle d'accès.

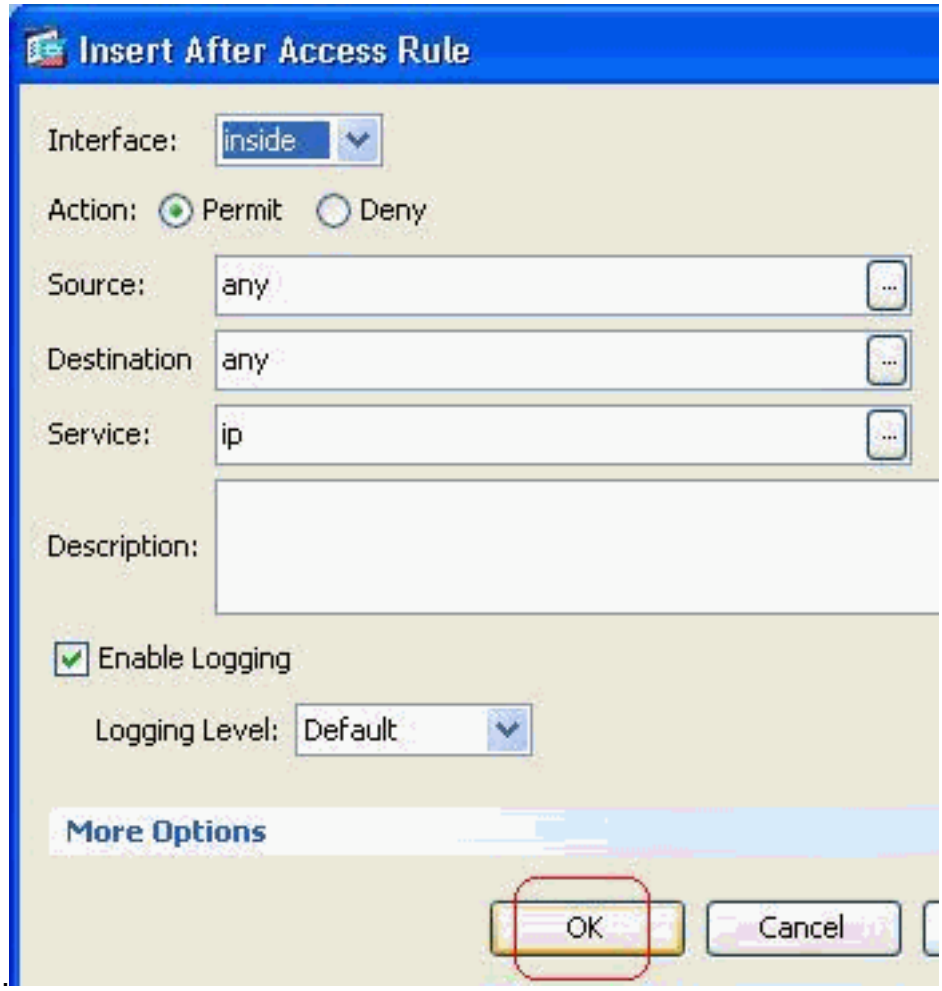


10. Cliquez sur **OK** pour terminer la configuration de la règle



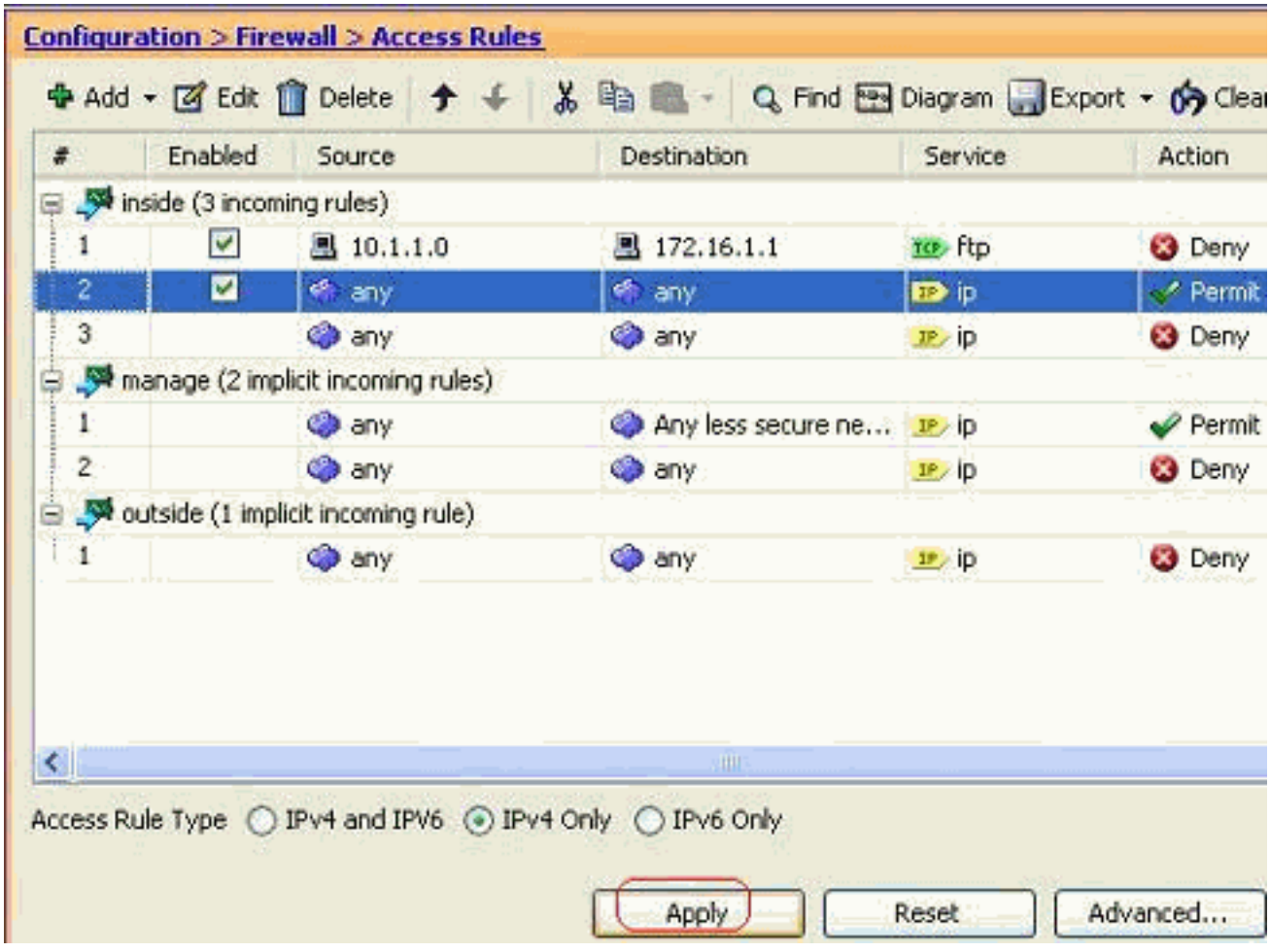
d'accès.

11. Ajoutez une autre règle d'accès pour autoriser tout autre trafic. Sinon, la règle de refus implicite bloquera tout le trafic sur cette



interface.

12. La configuration complète de la liste d'accès ressemble à ceci sous l'onglet Règles d'accès.



13. Cliquez sur **Apply** pour envoyer la configuration à l'ASA. La configuration CLI équivalente ressemble à ceci :

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

Ouverture de la configuration des ports

Le dispositif de sécurité n'autorise aucun trafic entrant, sauf s'il est explicitement autorisé par une liste de contrôle d'accès étendue.

Si vous voulez autoriser un hôte externe à accéder à un hôte interne, vous pouvez appliquer une liste d'accès entrante sur l'interface externe. Vous devez spécifier l'adresse traduite de l'hôte interne dans la liste de contrôle d'accès, car l'adresse traduite est l'adresse qui peut être utilisée sur le réseau externe. Complétez ces étapes afin d'ouvrir les ports de la zone de sécurité inférieure à la zone de sécurité supérieure. Par exemple, autorisez le trafic de l'extérieur (zone de sécurité inférieure) vers l'interface interne (zone de sécurité supérieure) ou la DMZ vers l'interface interne.

1. La NAT statique crée une traduction fixe d'une vraie adresse pour une adresse mappée. Cette adresse mappée est une adresse qui héberge sur Internet et peut être utilisée pour accéder au serveur d'applications sur la DMZ sans avoir besoin de connaître l'adresse réelle du serveur.

   ```
   static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] |
      access-list access_list_name | interface}
   ```

   Référez-vous à la section NAT statique de la référence de commande pour PIX/ASA afin d'en savoir plus.
2. Créez une liste de contrôle d’accès afin d’autoriser le trafic de port spécifique.

   ```
   access-list
   ```

3. Liez la liste d'accès à la commande **access-group** afin d'être active.

   ```
   access-group
   ```

Exemples:

1. **Ouvrez le trafic du port SMTP :** Ouvrez le port **tcp 25** afin de permettre aux hôtes de l'extérieur (Internet) d'accéder au serveur de messagerie situé dans le réseau DMZ.La commande **Static** mappe l'adresse externe 192.168.5.3 à l'adresse DMZ réelle 172.16.1.3.

   ```
   ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3
    netmask 255.255.255.255
   ```

```
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.3 eq 25
ciscoasa(config)#access-group 100 in interface outside
```

2. **Ouvrez le trafic du port HTTPS :** Ouvrez le port **tcp 443** afin de permettre aux hôtes de l'extérieur (Internet) d'accéder au serveur Web (sécurisé) situé dans le réseau DMZ.
```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.5  eq 443
ciscoasa(config)#access-group 100 in interface outside
```

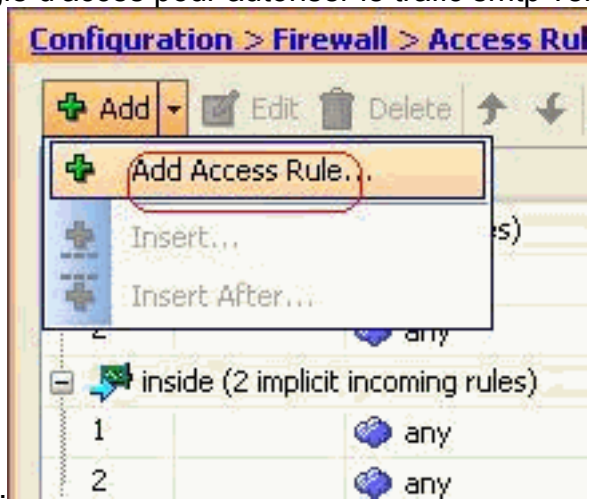
3. **Autoriser le trafic DNS :** Ouvrez le port **udp 53** afin de permettre aux hôtes de l'extérieur (Internet) d'accéder au serveur DNS (sécurisé) placé dans le réseau DMZ.
```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit udp
 any host 192.168.5.4  eq 53
ciscoasa(config)#access-group 100 in interface outside
```

Remarque : référez-vous à ports IANA afin d'en savoir plus sur les affectations de ports.

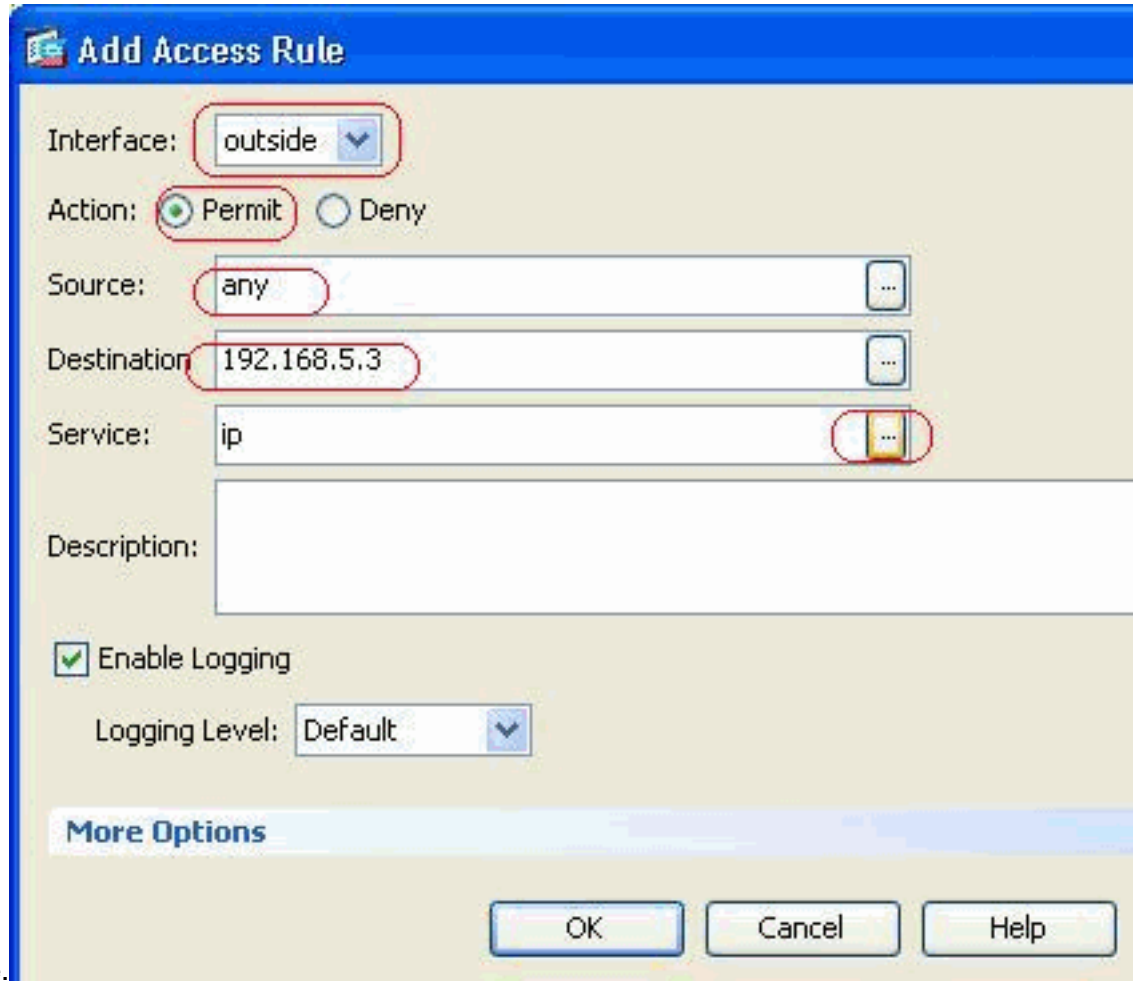
Configuration via ASDM

Cette section présente une approche pas à pas pour effectuer les tâches mentionnées ci-dessus via ASDM.

1. Créez la règle d'accès pour autoriser le trafic smtp vers le serveur 192.168.5.3.

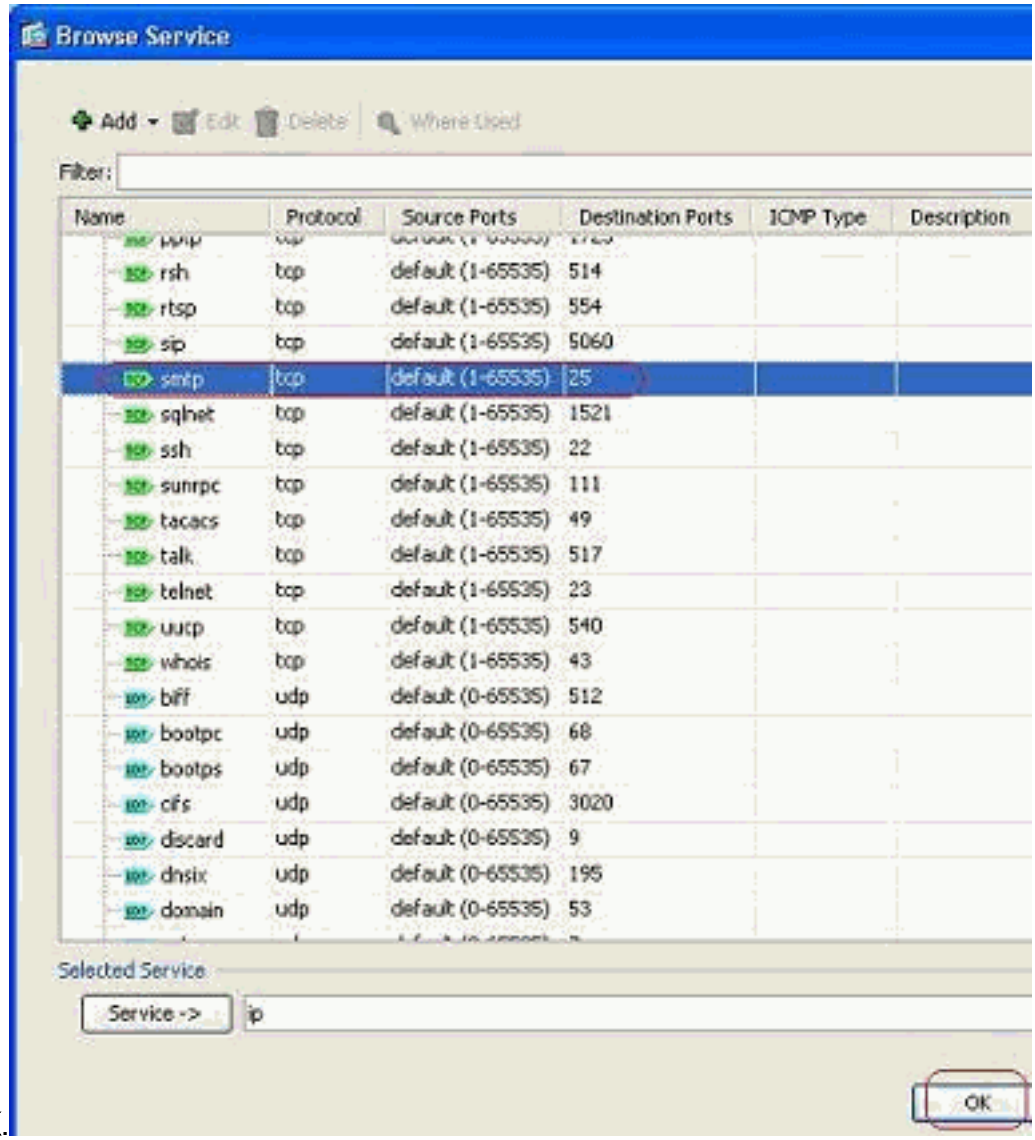


2. Définissez la source et la destination de la règle d'accès, ainsi que l'interface avec laquelle cette règle est liée. Définissez également l'action comme



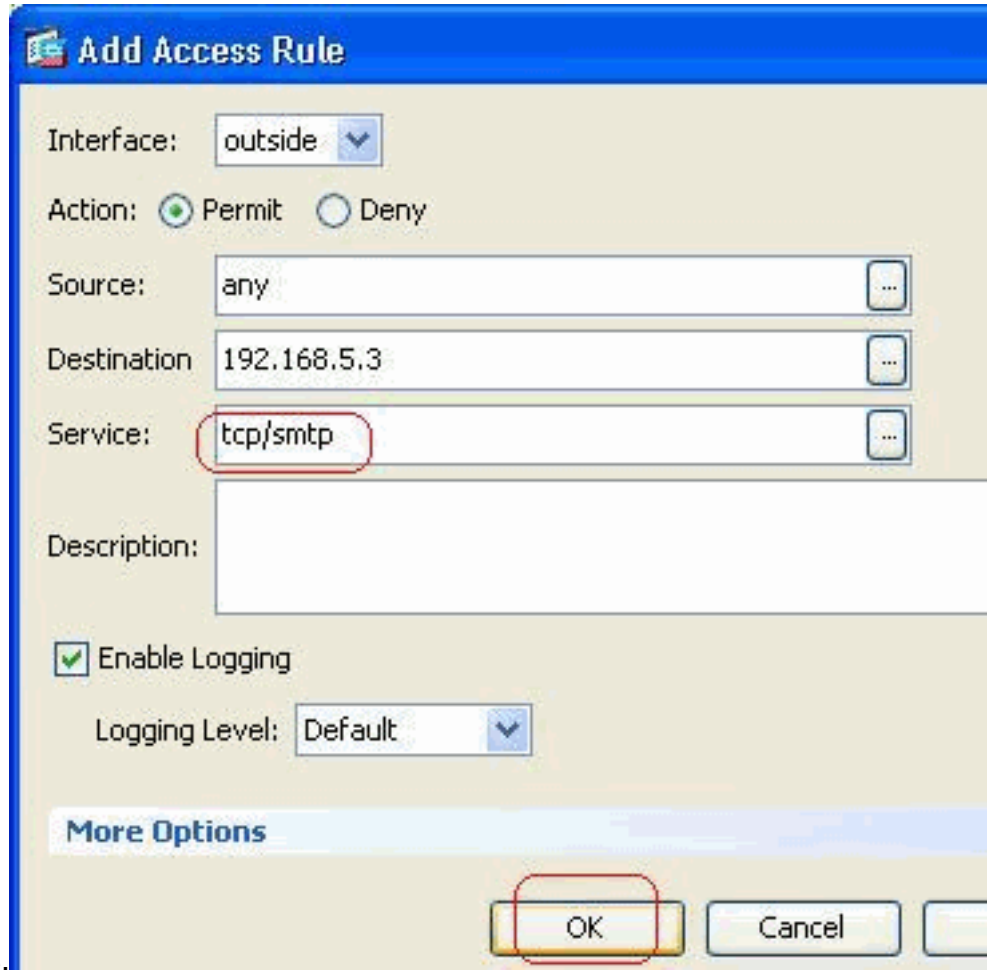
Autorisé.

3. Choisissez **SMTP** comme port, puis cliquez sur



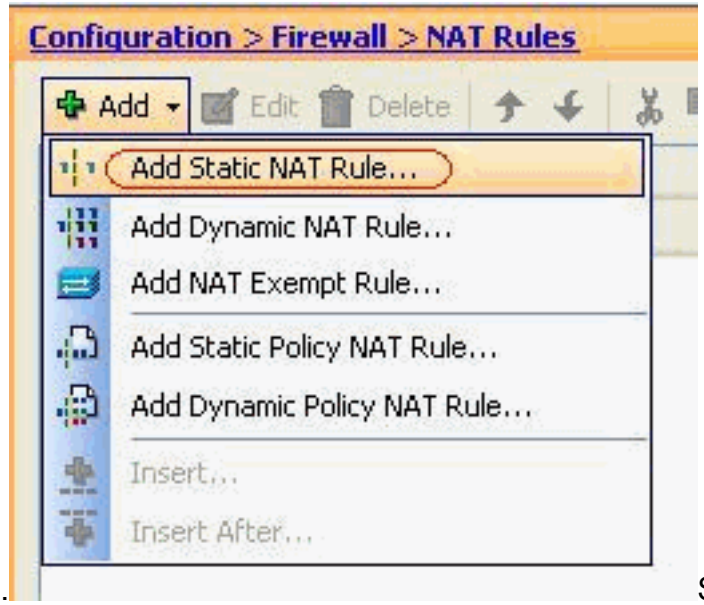
OK.

4. Cliquez sur **OK** pour terminer la configuration de la règle

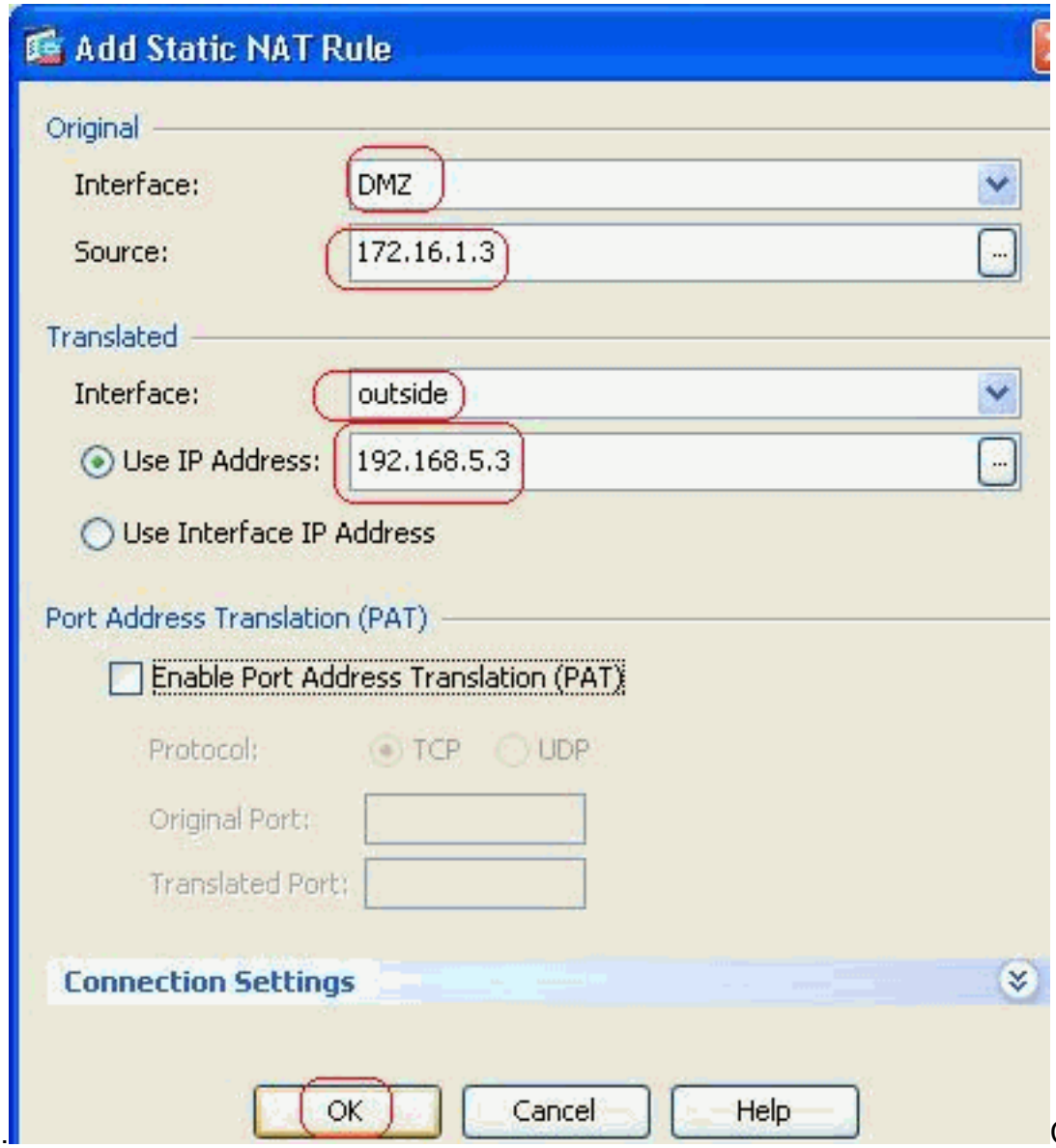


d'accès.

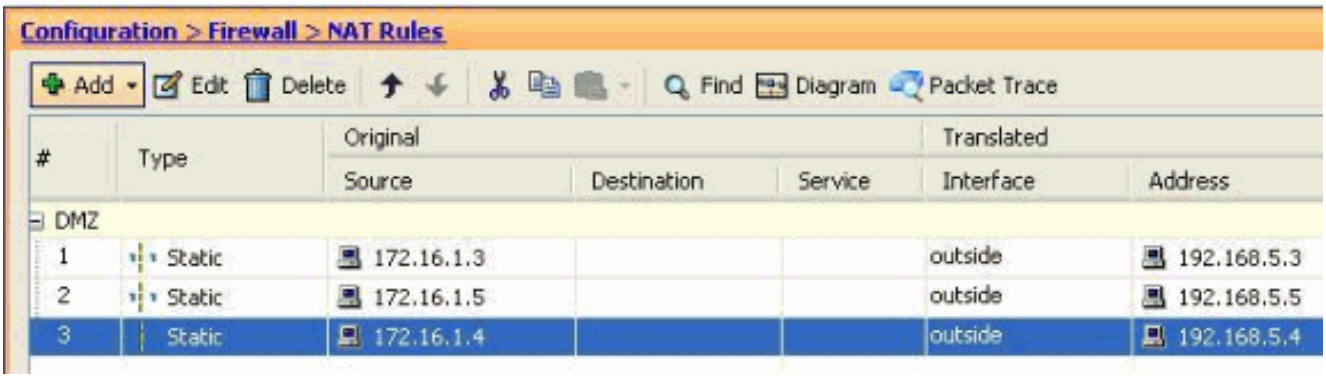
5. Configurez la NAT statique afin de traduire 172.16.1.3 en 192.168.5.3Accédez à **Configuration > Firewall > NAT Rules > Add Static NAT Rule** afin d'ajouter une entrée NAT



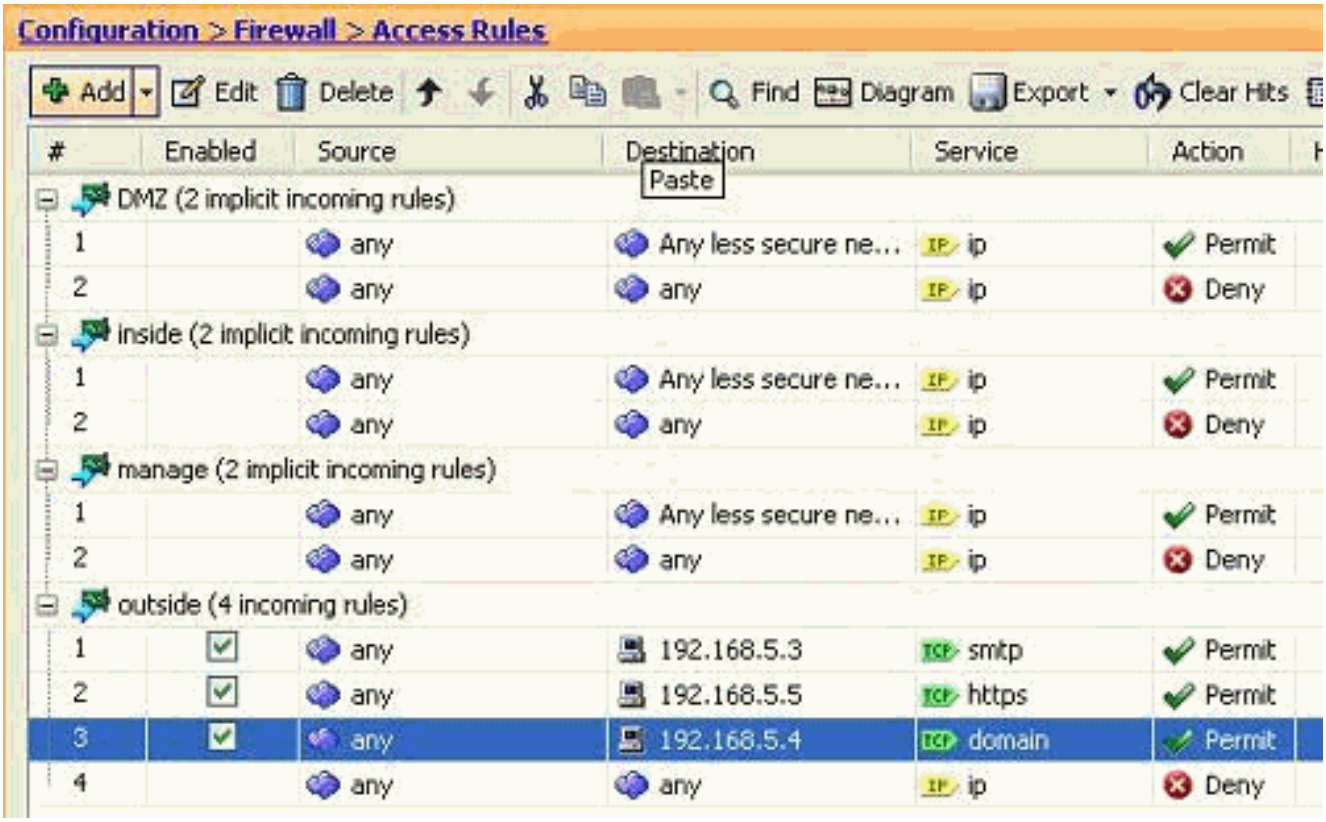
statique. Sélectionnez l'adresse IP source d'origine et traduite ainsi que les interfaces associées, puis cliquez sur **OK** pour terminer la configuration de la règle NAT



statique. Cette image représente les trois règles statiques répertoriées dans la section Exemples :



Cette image représente les trois règles d'accès répertoriées dans la section Exemples :



Vérification

Vous pouvez vérifier avec certaines commandes **show**, comme indiqué :

- **show xlate :** affiche les informations de traduction actuelles
- **show access-list** : affiche les compteurs de succès pour les stratégies d'accès
- **show logging** : affiche les journaux dans la mémoire tampon.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Dépannage

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

Informations connexes

- PIX/ASA 7.x : Activer/Désactiver la communication entre les interfaces
- PIX 7.0 et Redirection de port de l'appliance de sécurité adaptative (transfert) avec les commandes nat, global, static, conduit et access-list
- Utilisation des commandes nat, global, static, conduit et access-list et de la redirection (transfert) de port sur le pare-feu PIX
- PIX/ASA 7.x : Exemple de configuration de l'activation des services FTP/TFTP
- PIX/ASA 7.x : Exemple de configuration de l'activation des services VoIP (SIP, MGCP, H323, SCCP)
- PIX/ASA 7.x : Exemple de configuration de l'accès au serveur de messagerie sur la DMZ
- Support et documentation techniques - Cisco Systems