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.

Remarque: Les termes « ouvrant le port » et « permettant le port » fournissent la même signification. De même, le « blocage du port » et « limiter le port » fournissent également la même signification.

Conditions préalables

Conditions requises

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

Composants utilisés

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

- L'appliance de sécurité adaptable de gamme Cisco 5500 (ASA) cette exécute la version 8.2(1)
- Version 6.3(5) du Cisco Adaptive Security Device Manager (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.

Produits connexes

Cette configuration peut également être utilisée avec l'appliance de Pare-feu de la gamme Cisco 500 PIX avec la version de logiciel 6.x et en haut.

Conventions

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

Configurez

Chaque interface doit avoir un niveau de Sécurité de 0 (le plus bas) à 100 (le plus élevé). Par exemple, vous devez assigner votre la plupart de réseau sécurisé, tel que le réseau d'hôte interne, au niveau 100. Tandis que le réseau extérieur qui est connecté à l'Internet peut être le niveau 0, d'autres réseaux, tels que DMZs, peuvent être placés dans l'intervalle. Vous pouvez assigner des plusieurs interfaces au même niveau de Sécurité.

Par défaut, tous les ports sont bloqués sur l'interface extérieure (niveau de Sécurité 0), et tous les ports sont ouverts sur l'interface interne (niveau de Sécurité 100) des dispositifs de sécurité. De cette façon, tout le trafic sortant peut traverser les dispositifs de sécurité sans n'importe quelle configuration, mais on peut permettre le trafic d'arrivée par la configuration de la liste d'accès et des commandes statiques dans les dispositifs de sécurité.

Remarque: Généralement tous les ports sont bloqués de la zone de Sécurité inférieure à la zone de Sécurité plus élevée, et tous les ports sont ouverts de la zone de Sécurité plus élevée de zone de Sécurité inférieure fournissant que l'inspection avec état est activée pour des les deux le trafic en entrée et en sortie.

Cette section comprend les paragraphes comme affichés :

- Diagramme du réseau
- Blocage de la configuration de ports
- Ouvrir la configuration de ports

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) 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 de ports

Les dispositifs de sécurité permettent n'importe quel trafic sortant à moins qu'ils soient explicitement bloqués par une liste d'accès étendue.

Une liste d'accès se compose d'un ou plusieurs entrées de contrôle d'accès. Personne à charge sur le type de liste d'accès, vous pouvez spécifier la source et les adresses de destination, protocole, ports (pour le TCP ou l'UDP), type ICMP (pour l'ICMP), ou EtherType.

Remarque: Pour des protocoles sans connexions, tels que l'ICMP, les dispositifs de sécurité établissent des sessions unidirectionnelles, ainsi vous ou avez besoin de Listes d'accès pour permettre l'ICMP dans les deux directions (par l'application des Listes d'accès à la source et aux interfaces de destination), ou vous devez activer l'engine d'inspection d'ICMP. L'engine d'inspection d'ICMP traite des sessions d'ICMP en tant que connexions bidirectionnelles.

Terminez-vous ces étapes afin de bloquer les ports, qui s'appliquent habituellement pour trafiquer cela proviennent de l'intérieur (zone de Sécurité plus élevée) au DMZ (zone de Sécurité inférieure) ou au DMZ à l'extérieur.

1. Créez une liste de contrôle d'accès de telle manière que vous bloquiez le trafic portuaire spécifié.
   access-list <name> extended deny <protocol> <source-network/source IP> <source-netmask> <destination-network/destination IP> <destinamtion-netmask> eq <port number> access-list <name> extended permit ip any any
2. Liez alors la liste d'accès avec l'ordre d'**access-group** afin d'être en activité.
   access-group <access list name> in interface <interface name>

Exemples :

1. **Bloquez le trafic de port HTTP :** Afin de bloquer le réseau intérieur 10.1.1.0 de l'accès au HTTP (web server) avec IP 172.16.1.1 placé dans le réseau DMZ, créez un ACL comme affiché :`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 l'**aucun** suivi des commandes de liste d'accès afin d'enlever le blocage de port.
2. **Bloquez le trafic portuaire de FTP :** Afin de bloquer le réseau intérieur 10.1.1.0 de l'accès au FTP (serveur de fichiers) avec IP 172.16.1.2 placé dans le réseau DMZ, créez un ACL comme affiché :`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 aux ports IANA afin d'apprendre plus d'informations sur des affectations de port.

La configuration pas à pas pour exécuter ceci par l'ASDM est affichée dans cette section.

1. Allez à la **configuration > au Pare-feu > aux règles d'accès**. Cliquez sur Add la **règle d'accès** de créer la liste d'accès.
2. Définissez la source et la destination et l'action de règle d'accès avec l'interface que cette règle d'accès sera associée. Sélectionnez les détails pour choisir le port spécifique pour bloquer.

3. Choisissez le **HTTP de la** liste de ports disponibles, puis cliquez sur OK pour revenir à la fenêtre de règle d'accès d'ajouter.
4. Cliquez sur OK pour se terminer la configuration de la règle d'accès.
5. Cliquez sur l'**insertion ensuite** pour ajouter une règle d'accès à la même liste d'accès.
6. Permettez au trafic de « » à « » pour empêcher le « implicite refusent ». Puis, cliquez sur OK pour se terminer en ajoutant cette règle d'accès.
7. La liste d'accès configurée peut être vue dans les règles d'accès que tableau cliquent sur Apply pour envoyer cette configuration aux dispositifs de sécurité.La configuration envoyée de l'ASDM a comme conséquence 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`Par ces étapes, l'exemple 1 a été exécuté par l'ASDM pour bloquer le réseau de 10.1.1.0 d'accéder au web server, 172.16.1.1. L'exemple 2 peut également être réalisé de la même manière pour bloquer le réseau entier de 10.1.1.0 d'accéder au ftp server, 172.16.1.2. La seule différence sera au moment où choisir le port.**Remarque:** On assume que cette configuration par exemple 2 de règle d'accès est une configuration fraîche.
8. Définissez la règle d'accès pour bloquer le trafic FTP, puis cliquez sur l'onglet de **détails** pour choisir la destination port.
9. Choisissez le port de **FTP** et cliquez sur OK pour revenir à la fenêtre de règle d'accès d'ajouter.
10. Cliquez sur OK pour se terminer la configuration de la règle d'accès.
11. Ajoutez une autre règle d'accès de permettre n'importe quel autre trafic. Autrement, les implicites refusent la règle bloqueront tout le trafic sur cette interface.
12. La configuration de liste d'accès complète ressemble à ceci sous l'onglet de règles d'accès.
13. Cliquez sur Apply pour envoyer la configuration à l'ASA. La configuration équivalente CLI 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`

Ouvrir la configuration de ports

Les dispositifs de sécurité ne permettent aucun trafic d'arrivée à moins qu'on leur permette explicitement par une liste d'accès étendue.

Si vous voulez permettre à un hôte d'extérieur pour accéder à un hôte interne, vous pouvez appliquer une liste d'accès en entrée sur l'interface extérieure. Vous devez spécifier l'adresse traduite de l'hôte interne dans la liste d'accès parce que l'adresse traduite est l'adresse qui peut être utilisée sur le réseau extérieur. Terminez-vous ces étapes afin d'ouvrir les ports de la zone de Sécurité inférieure à la zone de Sécurité plus élevée. Par exemple, permettez le trafic de l'extérieur (zone de Sécurité inférieure) à l'interface interne (zone de Sécurité plus élevée) ou du DMZ à l'interface interne.

1. La NAT statique crée une traduction fixe d'une vraie adresse pour une adresse mappée. Cette adresse tracée est une adresse qui héberge sur l'Internet et peut être utilisée pour accéder au serveur d'applications sur le DMZ sans nécessité de connaître la vraie adresse 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 commandes pour PIX/ASA afin d'apprendre plus d'informations.

2. Créez un ACL afin de permettre le trafic portuaire spécifique.
   access-list <name> extended permit <protocol> <source-network/source IP> <source-netmask> <destination-network/destination IP> <destinamtion-netmask> eq <port number>
3. Liez la liste d'accès avec l'ordre d'**access-group** afin d'être en activité.
   access-group <access-list name> in interface <interface name>

Exemples :

1. **Ouvrez le trafic portuaire de SMTP :** Ouvrez le **TCP 25 de** port afin de permettre aux hôtes de l'extérieur (Internet) pour accéder au serveur de messagerie placé dans le réseau DMZ.La commande de **charge statique** trace l'adresse 192.168.5.3 d'extérieur à la vraie adresse 172.16.1.3 DMZ.`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 portuaire HTTPS :** Ouvrez le **TCP 443 de** port afin de permettre aux hôtes de l'extérieur (Internet) pour accéder au web server (sécurisez) placé 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. **Permettez le trafic DNS :** Ouvrez l'**UDP 53 de** port afin de permettre aux hôtes de l'extérieur (Internet) pour accéder au serveur DNS (sécurisez) 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 aux ports IANA afin d'apprendre plus d'informations sur des affectations de port.

Configuration par l'ASDM

Une approche pas à pas pour effectuer les tâches mentionnées ci-dessus par l'ASDM est affichée dans cette section.

1. Créez la règle d'accès de permettre le trafic de SMTP au serveur de 192.168.5.3.
2. Définissez la source et la destination de règle d'accès, et l'interface des grippages de cette règle avec. En outre, définissez l'action en tant qu'**autorisation**.
3. Choisissez le **SMTP** comme port, puis cliquez sur OK.
4. Cliquez sur OK pour se terminer en configurant la règle d'accès.
5. Configurez le NAT statique afin de traduire 172.16.1.3 à 192.168.5.3Allez à la **configuration > au Pare-feu > aux règles NAT > ajoutent la règle NAT statique** afin d'ajouter une entrée NAT statique.Sélectionnez la source d'origine et l'adresse IP traduite avec leurs interfaces associées, puis cliquez sur OK pour terminer configurer la règle NAT statique.Cette image dépeint chacune des trois règles statiques qui sont répertoriées dans la section d'exemples :Cette image dépeint chacune des trois règles d'accès qui sont répertoriées dans la section d'exemples :

Vérifiez

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

- **show xlate** — les informations en cours de traduction d'affichage
- **liste d'accès d'exposition** — affichez les compteurs de hit pour des stratégies d'accès
- **show logging** — affichez les logins 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** .

Dépannez

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 Port Redirection(Forwarding) d'appliance de sécurité adaptable avec nat, global, statique, le conduit, et les commandes 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 services de l'enable VoIP (SIP,MGCP,H323,SCCP)
- PIX/ASA 7.x : Serveur de messagerie Access sur l'exemple de configuration DMZ
- Support et documentation techniques - Cisco Systems