

PIX/ASA 7.x : Exemple de configuration de l'activation des services FTP/TFTP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Produits connexes](#)

[Conventions](#)

[Informations générales](#)

[Prendre en charge le Protocole avancé](#)

[Configurez l'inspection de base de l'application FTP](#)

[Exemple de configuration](#)

[Configurez l'inspection de protocole FTP sur le port TCP non standard](#)

[Configurez l'inspection de base de l'application TFTP](#)

[Exemple de configuration](#)

[Vérifiez](#)

[Dépannez](#)

[Problème : La syntaxe dans la configuration ne fonctionne pas et une 'erreur d'inspection de class-map est reçue](#)

[Solution](#)

[Incapable d'exécuter FTPS \(FTP au-dessus de SSL\) à travers l'ASA](#)

[Informations connexes](#)

Introduction

Ce document explique les étapes nécessaires pour que des utilisateurs en dehors de votre réseau puissent accéder au FTP et aux services TFTP dans votre réseau DMZ.

File Transfer Protocol FTP

Il y a deux formes de FTP:

- Mode actif
- Mode passif

En mode actif FTP, le client se connecte d'un port non privilégié aléatoire (N>1023) au port de commande (21) du serveur FTP. Puis le client commence à écouter le port N+1 et envoie la commande FTP du port N +1 au serveur FTP. Le serveur se connecte alors à nouveau aux ports spécifiés de données du client à partir de son port local de données, qui est le port 20.

En mode de FTP passif, le client lance les deux connexions au serveur, ce qui résout le problème d'un Pare-feu qui filtre la connexion du port de données entrantes au client à partir du serveur. Quand une connexion FTP est ouverte, le client ouvre deux ports non privilégiés aléatoires localement (N>1023 et N+1). Le premier port contacte le serveur sur le port 21. Mais au lieu d'émettre alors une commande de **port** et de permettre au serveur de se connecter de nouveau à son port de données, le client lance la commande **PASV**. Ceci fait que le serveur ouvre alors un port non privilégié aléatoire (P>1023) et renvoie la commande du **port P** au client. Le client lance alors la connexion du port N+1 pour mettre en communication P sur le serveur pour transférer des données. Sans la configuration de la commande d'**inspection** sur l'Appliance de sécurité, le FTP à partir des utilisateurs internes dirigés vers l'extérieur fonctionne seulement en mode passif. En outre, l'accès est refusé aux utilisateurs dirigés en entrée vers votre serveur FTP.

Référez-vous à [ASA 8.3 et plus tard : Activez l'exemple de configuration de services FTP/TFTP](#) pour plus d'informations sur la configuration identique utilisant l'ASDM avec l'appliance de sécurité adaptable Cisco (ASA) avec la version 8.3 et ultérieures.

Trivial File Transfer Protocol (TFTP)

Le TFTP, comme décrit dans [RFC 1350](#), est un protocole de routage simple pour lire et écrire des fichiers entre un serveur TFTP et un client. Le TFTP utilise le port UDP 69.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Il y a transmission de base entre les interfaces requises.
- Vous avez un serveur FTP configuré situé à l'intérieur de votre réseau DMZ.

Composants utilisés

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

- Appliance de sécurité adaptable de la gamme ASA 5500 qui exécute l'image logicielle 7.2(2)
- Serveur Windows 2003 qui dirige des services FTP
- Serveur Windows 2003 qui dirige des services TFTP
- PC client situé à l'extérieur du réseau

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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

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.

Produits connexes

Cette configuration peut également être utilisée avec PIX Security Appliance 7.x.

Conventions

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

Informations générales

Le dispositif de sécurité prend en charge l'inspection d'application via la fonction d'algorithme de sécurité adaptatif. Par l'inspection d'application avec état utilisée par l'algorithme de sécurité adaptatif, le dispositif de sécurité suit chaque connexion qui traverse le pare-feu et s'assure qu'elle est valide. Le pare-feu, par l'inspection avec état, surveille également l'état de la connexion pour compiler des informations à placer dans une table des états. Avec l'utilisation de la table des états en plus des règles définies par l'administrateur, les décisions de filtrage sont basées sur le contexte qui est établi par les paquets qui sont précédemment passés à travers le pare-feu. La mise en œuvre des inspections d'application consiste en ces actions :

- Identifier le trafic.
- Appliquer des inspections au trafic.
- Activer des inspections sur une interface.

Prendre en charge le Protocole avancé

FTP

Certaines applications requièrent une prise en charge spéciale par la fonction d'inspections de l'Appliance de sécurité Cisco. Ces types d'applications incluent habituellement les informations d'adressage IP dans le paquet de données utilisateur ou les canaux auxiliaires ouverts sur les ports dynamiquement attribués. La fonction d'inspection d'application fonctionne avec la Traduction d'adresses de réseau (NAT) pour aider à identifier l'emplacement des informations d'adressage incluses.

Outre l'identification des informations d'adressage incluses, la fonction de l'inspection de l'application contrôle les sessions pour déterminer les numéros de port pour les canaux auxiliaires. Plusieurs protocoles de routage ouvrent les ports auxiliaires TCP ou UDP pour améliorer des performances. La session initiale sur un port connu est utilisée pour négocier les numéros de port dynamiquement attribués. La fonction d'inspection d'application contrôle ces sessions, identifie les affectations des ports dynamiques et permet des échanges de données sur ces ports pour la durée des sessions spécifiques. Les applications Multimédia et les applications FTP montrent ce genre de comportement.

Le protocole FTP requiert une prise en charge spéciale en raison de son utilisation de deux ports par session FTP. Le protocole FTP utilise deux ports une fois activés pour transférer des données: un canal de contrôle et un canal de transmission de données qui utilise les ports 21 et 20, respectivement. L'utilisateur qui lance la session FTP sur le canal de contrôle effectue toutes les

requêtes de données par ce canal. Le serveur FTP lance alors une requête pour ouvrir un port à partir du port 20 du serveur vers l'ordinateur de l'utilisateur. FTP utilise toujours le port 20 pour les transmissions du canal de données. Si l'inspection FTP n'a pas été activée sur l'Appliance de sécurité, cette requête de routage est ignorée et les sessions FTP ne transmettent aucune des données demandées. Si l'inspection FTP est activée sur l'Appliance de sécurité, l'Appliance de sécurité contrôle le canal de contrôle et essaie d'identifier une requête pour ouvrir le canal de transmission de données. Le protocole FTP inclut les caractéristiques de port du canal de données dans le trafic du canal de contrôle, en demandant à l'Appliance de sécurité d'inspecter le canal de contrôle pour des modifications du port de données. Si l'Appliance de sécurité identifie une requête, elle crée temporairement une ouverture pour le trafic du canal de données qui dure pour la vie de la session. De cette façon, la fonction d'inspection de FTP contrôle le canal de contrôle, identifie une affectation du port de données et permet aux données d'être échangées sur le port de données pour la durée de la session.

L'Appliance de sécurité inspecte des connexions du port 21 pour le trafic FTP par défaut par l'intermédiaire du class-map de l'inspection globale. L'Appliance de sécurité identifie également la différence entre une session FTP active et une session FTP passive. Si les sessions FTP prennent en charge le transfert des données de FTP passif, l'Appliance de sécurité par la commande **inspect FTP**, identifie la requête du port de données de l'utilisateur et ouvre un nouveau port de données supérieur à 1023.

L'inspection d'application FTP inspecte les sessions FTP et exécute quatre tâches:

- Prépare une connexion de données secondaire dynamique
- Suit la séquence des commandes-réponses de FTP
- Génère une vérification rétrospective
- Traduit l'adresse IP incluse en utilisant NAT

L'inspection d'application FTP prépare des canaux auxiliaires pour le transfert des données de FTP. Les canaux sont alloués en réponse au téléchargement d'un fichier, ou à un événement d'énumération du répertoire et ils doivent être les pré-négociés. Le port est négocié par les commandes (227) **PORT** ou **PASV** (.).

TFTP

L'inspection TFTP est activée par défaut.

L'Appliance de sécurité inspecte le trafic TFTP et crée dynamiquement des connexions et des routages de traduction s'il y a lieu, pour permettre le transfert de fichiers entre un client TFTP et le serveur. En particulier, le moteur d'inspection inspecte les requêtes lues TFTP (RRQ), écrit des requêtes de routage (WRQ) et les notifications d'erreur (ERREUR).

Un canal auxiliaire dynamique et une traduction PAT s'il y a lieu, sont alloués sur une réception d'un RRQ ou d'un WRQ valide. Ce canal auxiliaire est ultérieurement utilisé par TFTP pour le transfert de fichiers ou la notification d'erreur.

Seul le serveur TFTP peut lancer le trafic de routage au-dessus du canal auxiliaire, et tout au plus un canal auxiliaire inachevé peut exister entre le client TFTP et le serveur. Une notification d'erreur du serveur ferme le canal auxiliaire.

L'inspection TFTP doit être activée si le PAT statique est utilisé pour rediriger le trafic de routage TFTP.

Configurez l'inspection de base de l'application FTP

Par défaut, la configuration inclut une stratégie qui correspond à tout le trafic de l'inspection d'application par défaut et applique une inspection au trafic sur toutes les interfaces (une stratégie globale). Le trafic de l'inspection d'application par défaut inclut le trafic vers les ports par défaut pour chaque protocole. Vous pouvez seulement appliquer une stratégie globale, ainsi si vous voulez modifier la stratégie globale, par exemple, pour appliquer l'inspection aux ports non standard, ou pour ajouter des inspections qui ne sont pas activées par défaut, vous devez soit modifier la stratégie par défaut soit la désactiver et en appliquer une nouvelle. Pour une liste de tous les ports par défaut, référez-vous à la [Stratégie d'inspection par défaut](#).

1. Émettez la commande **policy-map global_policy**.ASAwAIP-CLI(config)#**policy-map global_policy**
2. Émettez la commande **class inspection_default**.ASAwAIP-CLI(config-pmap)#**class inspection_default**
3. Lancez la commande **inspect FTP**.ASAwAIP-CLI(config-pmap-c)#**inspect FTP** Il y a une option d'utilisation de la commande **inspect FTP strict**. Cette commande augmente la sécurité des réseaux protégés en empêchant un navigateur Web d'envoyer des commandes incluses dans les requêtes FTP. Après que vous activez l'option **strict** sur une interface, l'inspection de FTP impose ce comportement: Une commande FTP doit être reconnue avant que l'Appliance de sécurité autorise une nouvelle commande. L'Appliance de sécurité dépose une connexion qui envoie des commandes incluses. Les commandes **227** et les commandes **PORT** sont vérifiées afin de garantir qu'elles n'apparaîtront pas dans une chaîne d'erreur. **Avertissement** : L'utilisation de l'option **strict** pourrait entraîner l'échec des clients FTP qui ne sont pas strictement conformes avec les RFCs de FTP. Consultez [Utiliser l'option stricte](#) pour plus d'informations sur l'utilisation de l'option **stricte**.

Exemple de configuration

Nom du périphérique 1

```
ASA-AIP-CLI(config)#show running-config ASA Version
7.2(2) ! hostname ASA-AIP-CLI domain-name corp.com
enable password WwXYvtKrnjXqGbul encrypted names !
interface Ethernet0/0 nameif Outside security-level 0 ip
address 192.168.1.2 255.255.255.0 ! interface
Ethernet0/1 nameif Inside security-level 100 ip address
10.1.1.1 255.255.255.0 ! interface Ethernet0/2 nameif
DMZ security-level 50 ip address 172.16.1.12
255.255.255.0 ! interface Ethernet0/3 no nameif no
security-level no ip address ! interface Management0/0
no nameif no security-level no ip address ! !--- Output
is suppressed. !-- Permit inbound FTP control traffic.
access-list 100 extended permit tcp any host 192.168.1.5
eq ftp !-- Permit inbound FTP data traffic. access-list
100 extended permit tcp any host 192.168.1.5 eq ftp-data
! !-- Command to redirect the FTP traffic received on
IP 192.168.1.5 !-- to IP 172.16.1.5. static
(DMZ,outside) 192.168.1.5 172.16.1.5 netmask
255.255.255.255 access-group 100 in interface outside
class-map inspection_default match default-inspection-
traffic ! ! policy-map type inspect dns preset_dns_map
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
preset_dns_map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
```

```
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! !---
This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end
ASA-AIP-CLI(config)#
```

Configurez l'inspection de protocole FTP sur le port TCP non standard

Vous pouvez configurer l'inspection de protocole FTP pour les ports TCP non standard avec ces lignes de configuration (remplacer XXXX par le nouveau numéro de port):

```
access-list ftp-list extended permit tcp any any eq XXXX
!
class-map ftp-class
  match access-list ftp-list
!
policy-map global_policy
  class ftp-class
    inspect ftp
```

Configurez l'inspection de base de l'application TFTP

Par défaut, la configuration inclut une stratégie qui correspond à tout le trafic de l'inspection d'application par défaut et applique une inspection au trafic sur toutes les interfaces (une stratégie globale). Le trafic de l'inspection d'application par défaut inclut le trafic vers les ports par défaut pour chaque protocole. Vous ne pouvez appliquer qu'une seule stratégie globale. Par conséquent, si vous voulez modifier la stratégie globale, par exemple, pour appliquer l'inspection à des ports non standard, ou pour ajouter des inspections qui ne sont pas activées par défaut, vous devez soit modifier la stratégie par défaut, soit la désactiver et en appliquer une nouvelle. Pour une liste de tous les ports par défaut, référez-vous à la [Stratégie d'inspection par défaut](#).

1. Émettez la commande `policy-map global_policy`.ASA-AIP-CLI(config)#`policy-map global_policy`
2. Émettez la commande `class inspection_default`.ASA-AIP-CLI(config-pmap)#`class inspection_default`
3. Lancez la commande `inspect TFTP`.ASA-AIP-CLI(config-pmap-c)#`inspect TFTP`

Exemple de configuration

Nom du périphérique 1

```
ASA-AIP-CLI(config)#show running-config ASA Version
7.2(2) ! hostname ASA-AIP-CLI domain-name corp.com
enable password WwXYvtKrnjXqGbul encrypted names !
interface Ethernet0/0 nameif Outside security-level 0 ip
address 192.168.1.2 255.255.255.0 ! interface
Ethernet0/1 nameif Inside security-level 100 ip address
10.1.1.1 255.255.255.0 ! interface Ethernet0/2 nameif
DMZ security-level 50 ip address 172.16.1.12
255.255.255.0 ! interface Ethernet0/3 no nameif no
security-level no ip address ! interface Management0/0
no nameif no security-level no ip address ! !--- Output
is suppressed. !--- Permit inbound TFTP traffic. access-
list 100 extended permit udp any host 192.168.1.5 eq
```

```
tftp ! !--- Command to redirect the TFTP traffic
received on IP 192.168.1.5 !--- to IP 172.16.1.5. static
(DMZ,outside) 192.168.1.5 172.16.1.5 netmask
255.255.255.255 access-group 100 in interface outside
class-map inspection_default match default-inspection-
traffic ! ! policy-map type inspect dns preset_dns_map
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
preset_dns_map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! !---
This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end
ASA-AIP-CLI(config)#
```

Vérifiez

Afin de s'assurer que la configuration a réussi, utilisez la commande **show service-policy** et limitez la sortie à l'inspection FTP seulement, en utilisant la commande **show service-policy inspect FTP**.

Dépannez

Problème : La syntaxe dans la configuration ne fonctionne pas et une 'erreur d'inspection de class-map est reçue

La syntaxe présentée dans la partie Configuration ne fonctionne pas et vous recevez une erreur de ce type:

```
ERROR: % class-map inspection_default not configured
```

Solution

Cette configuration se fonde sur les inspections par défaut dans la configuration. Si elles ne sont pas dans la configuration, recréez-les avec ces commandes:

1. **class-map inspection_default match default-inspection-traffic**
2. **policy-map type inspect dns preset_dns_map parameters message-length maximum 512**
3. **policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect le xdmcp inspect sip inspect netbios inspect tftp**
4. **service-policy global_policy global**

Avertissement : Si les inspections par défaut ont été précédemment supprimées pour résoudre un autre problème, ce problème peut réapparaître quand les inspections par défaut sont réactivées. Vous ou votre administrateur devriez savoir si les inspections par défaut ont été supprimées précédemment dans une étape de dépannage.

Incapable d'exécuter FTPS (FTP au-dessus de SSL) à travers l'ASA

Le FTP avec TLS/SSL (SFTP/FTPS) n'est pas pris en charge par l'intermédiaire de l'Appliance de

sécurité. La connexion FTP est chiffrée, ainsi il est tout-à-fait impossible que le pare-feu puisse déchiffrer le paquet. Reportez-vous à la section [PIX/ASA : FAQ sur l'Appliance de sécurité pour plus d'informations](#).

Informations connexes

- [Appliances de sécurité adaptables de la gamme ASA 5500](#)
- [Référence des commandes de l'Appliance de sécurité Cisco](#)
- [Appliances de sécurité de la gamme PIX 500](#)
- [Notifications et avis de sécurité Cisco](#)
- [Support et documentation techniques - Cisco Systems](#)