Transfert de fichiers ASA avec l'exemple de configuration FXP

Contenu

Introduction

Ce document décrit comment configurer le protocole d'échange de fichier (FXP) relatif à l'appliance de sécurité adaptable Cisco (ASA) par l'intermédiaire du CLI.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de base de modes (actifs/passifs) de Protocole FTP (File Transfer Protocol).

[Composants utilisés](#)

Les informations dans ce document sont basées sur Cisco ASA qui exécute les versions de logiciel 8.0 et plus tard.

Remarque: Cet exemple de configuration utilise deux postes de travail de Microsoft Windows qui agissent en tant que serveurs FXP et services de FTP de passage (démon 3C). Ils font également activer FXP. Un autre poste de travail de Microsoft Windows qui exécute le logiciel client FXP (précipitation de FTP) est également utilisé.

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.

Informations générales

Le FXP te permet pour transférer des fichiers d'un ftp server vers un autre ftp server par l'intermédiaire d'un client FXP sans nécessité de dépendre de la vitesse de connexion internet de client. Avec FXP, la vitesse maximum de transfert dépend seulement de la connexion entre les deux serveurs, qui est habituellement beaucoup plus rapide que la connexion client. Vous pouvez appliquer FXP dans les scénarios où un serveur de bande passante élevée exige des ressources d'un autre serveur de bande passante élevée, mais seulement un client de faible bande passante tel qu'un administrateur réseau qui travaille à distance a l'autorité pour accéder aux ressources sur les deux serveurs.

Le FXP fonctionne comme extension du protocole de FTP, et le mécanisme est énoncé dans la section 5.2 du RFC 959 de FTP. Fondamentalement, le client FXP initie une connexion de contrôle avec un FTP server1, ouvre une autre connexion de contrôle avec le FTP server2, puis modifie les attributs de connexion des serveurs de sorte qu'ils dirigent entre eux tels que le transfert a lieu directement entre les deux serveurs.

Mécanisme du transfert de fichiers par l'intermédiaire de FXP

Voici un aperçu du processus :

1. Le client ouvre une connexion de contrôle avec server1 sur le port TCP 21.

   Le client envoie la commande **PASV à** server1.

   Server1 répond avec son adresse IP et le port sur lesquels il écoute.

2. Le client ouvre une connexion de contrôle avec server2 sur le port TCP 21.

   Le client passe l'adresse/port qui est reçu de server1 à server2 dans une commande de **PORT**.

   Server2 répond afin d'informer le client que la commande de **PORT** est réussie. Server2 sait maintenant où envoyer les données.

3. Afin de commencer le processus de transmission de server1 à server2 :

Le client envoie la commande **STOR à** server2 et lui demande pour enregistrer la date qu'elle reçoit.

Le client envoie la commande **RETR à** server1 et lui demande pour récupérer ou transmettre le fichier.

4. Toutes les données vont maintenant directement de la source au serveur FTP de destination. Les deux serveurs signalent seulement des messages d'état sur l'échouer/succès au client.

C'est comment la table de connexion apparaît :

```
TCP server2 192.168.1.10:21 client 172.16.1.10:50684, idle 0:00:04, bytes 694,
flags UIOB
TCP client 172.16.1.10:50685 server1 10.1.1.10:21, idle 0:00:04, bytes 1208,
flags UIOB
```

Inspection de FTP et FXP

Le transfert de fichiers par l'ASA par l'intermédiaire de FXP est réussi seulement quand l'inspection de FTP **est désactivée** sur l'ASA.

Quand le client FXP spécifie une adresse IP et un port TCP qui diffèrent de ceux du client dans la commande de **PORT de** FTP, une situation non sécurisée est créée où un attaquant peut effectuer un balayage de port contre un hôte sur l'Internet d'un tiers ftp server. C'est parce que le ftp server est chargé pour ouvrir une connexion à un port sur un ordinateur qui ne pourrait pas être le client qui commence. Ceci s'appelle une **attaque de rebond de FTP**, et l'inspection de FTP a arrêté la connexion parce qu'elle considère ceci une violation de sécurité.

Voici un exemple :

```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: Teardown TCP connection 24889 for client:172.16.1.10/49190 to
server2:192.168.1.10/49159 duration 0:00:00 bytes 1078 TCP FINs
%ASA-4-406002: FTP port command different address: 172.16.1.10(10.1.1.10) to
192.168.1.10 on interface client
%ASA-6-302014: Teardown TCP connection 24886 for client:172.16.1.10/49187 to
server2:192.168.1.10/21 duration 0:00:00 bytes 649 Flow closed by inspection
```

Configurez

Utilisez les informations qui sont décrites dans cette section afin de configurer FXP sur l'ASA.

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Configurez l'ASA par l'intermédiaire du CLI

Terminez-vous ces étapes afin de configurer l'ASA :

1. Inspection de FTP de débronchement :
```
FXP-ASA(config)# policy-map global_policy
FXP-ASA(config-pmap)#  class inspection_default
FXP-ASA(config-pmap-c)# no inspect ftp
```
2. Configurez les Listes d'accès afin de permettre la transmission entre le client FXP et les deux serveurs de FTP :
```
FXP-ASA(config)#access-list serv1 extended permit ip host 10.1.1.10 any
FXP-ASA(config)#access-list serv1 extended permit ip any host 10.1.1.10
FXP-ASA(config)#access-list serv2 extended permit ip host 192.168.1.10 any
FXP-ASA(config)#access-list serv2 extended permit ip any host 192.168.1.10
FXP-ASA(config)#access-list client extended permit ip host 172.16.1.10 any
FXP-ASA(config)#access-list client extended permit ip any host 172.16.1.10
```
3. Appliquez les Listes d'accès sur les interfaces respectives :
```
FXP-ASA(config)#access-group serv1 in interface server1
FXP-ASA(config)#access-group client in interface client
FXP-ASA(config)#access-group serv2 in interface server2
```

Vérifiez

Utilisez les informations qui sont décrites dans cette section afin de vérifier que votre configuration fonctionne correctement.

Procédé de transfert de fichiers

Terminez-vous ces étapes afin de vérifier le transfert de fichiers réussi entre les deux serveurs de FTP :

1. Connectez à server1 de la machine cliente FXP :

2. Connectez à server2 de la machine cliente FXP :

3. Glissez-déplacez le fichier à transférer de la fenêtre server1 vers la fenêtre server2 :

4. Vérifiez que le transfert de fichiers est réussi :

Dépannez

Cette section fournit des captures de deux scénarios différents que vous pouvez employer afin de dépanner votre configuration.

Scénario désactivé par inspection de FTP

Quand l'inspection de FTP est désactivée, comme détaillé dans l'inspection de FTP et la section FXP de ce document, ces données apparaissent sur l'interface client ASA :

Voici quelques notes au sujet de ces données :

- L'adresse IP de client est **172.16.1.10**.
- L'adresse IP Server1 est **10.1.1.10**.
- L'adresse IP Server2 est **192.168.1.10**.

Dans cet exemple, le fichier nommé **Kiwi_Syslogd.exe** est transféré de server1 vers server2.

Inspection de FTP activée

Quand l'inspection de FTP est activée, ces données apparaissent sur l'interface client ASA :

Voici les captures de baisse ASA :

La demande de **PORT** est abandonnée par l'inspection de FTP parce qu'elle contient une adresse IP et un port qui diffèrent de l'adresse IP et du port de client. Ultérieurement, la connexion de contrôle au serveur est terminée par l'inspection.