Exemple de configuration du transfert de fichiers ASA avec FXP

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Mécanisme de transfert de fichiers via FXP Inspection FTP et FXP Configuration Diagramme du réseau Configurez l'ASA par l'intermédiaire du CLI Vérification Processus de transfert de fichiers Dépannage Scénario d'inspection FTP désactivé Inspection FTP activée

Introduction

Ce document décrit comment configurer le protocole FXP (File eXchange Protocol) sur l'appareil de sécurité adaptatif Cisco (ASA) via l'interface de ligne de commande.

Conditions préalables

Conditions requises

Cisco vous recommande d'avoir une connaissance de base du protocole FTP (File Transfer Protocol) (modes actif/passif).

Components Used

Les informations de ce document sont basées sur Cisco ASA qui exécute les versions 8.0 et ultérieures du logiciel.

Note: Cet exemple de configuration utilise deux stations de travail Microsoft Windows qui agissent en tant que serveurs FXP et exécutent des services FTP (Démon 3C). FXP est également activé. Une autre station de travail Microsoft Windows qui exécute le logiciel client FXP (FTP Rush) est également utilisée.

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.

Informations générales

Le FXP vous permet de transférer des fichiers d'un serveur FTP à un autre serveur FTP via un client FXP sans avoir à dépendre de la vitesse de connexion Internet du client. Avec FXP, la vitesse de transfert maximale dépend uniquement de la connexion entre les deux serveurs, qui est généralement beaucoup plus rapide que la connexion client. Vous pouvez appliquer FXP dans des scénarios où un serveur à bande passante élevée demande des ressources à un autre serveur à bande passante élevée, mais seul un client à bande passante faible, tel qu'un administrateur réseau qui travaille à distance, a l'autorité d'accéder aux ressources sur les deux serveurs.

Le protocole FXP fonctionne comme une extension du protocole FTP, et le mécanisme est indiqué dans la section 5.2 du document FTP RFC 959. Fondamentalement, le client FXP initie une connexion de contrôle avec un serveur FTP1, ouvre une autre connexion de contrôle avec le serveur FTP2, puis modifie les attributs de connexion des serveurs de sorte qu'ils pointent l'un vers l'autre de sorte que le transfert ait lieu directement entre les deux serveurs.

Mécanisme de transfert de fichiers via FXP



Voici un aperçu du processus :

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

Le client envoie la commande PASV au serveur 1.

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

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

Le client passe l'adresse/le port qui est reçu du serveur1 au serveur2 dans une commande **PORT**.

Server2 répond afin d'informer le client que la commande **PORT** a réussi. Le serveur 2 sait maintenant où envoyer les données.

3. Afin de commencer le processus de transmission du serveur1 au serveur2 :

Le client envoie la commande **STOR** au serveur2 et lui demande de stocker la date qu'il reçoit.

Le client envoie la commande **RETR** au serveur 1 et lui demande de récupérer ou de transmettre le fichier.

 Toutes les données vont maintenant directement de la source au serveur FTP de destination. Les deux serveurs signalent uniquement au client les messages d'état en cas d'échec ou de réussite.

Voici comment apparaît la table de connexion :

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 FTP et FXP

Le transfert de fichiers via ASA via FXP ne réussit que lorsque l'inspection FTP est **désactivée** sur l'ASA.

Lorsque le client FXP spécifie une adresse IP et un port TCP qui diffèrent de ceux du client dans la commande **PORT** FTP, une situation non sécurisée se crée lorsqu'un pirate est en mesure d'effectuer une analyse de port contre un hôte sur Internet à partir d'un serveur FTP tiers. Cela est dû au fait que le serveur FTP est invité à ouvrir une connexion à un port sur une machine qui n'est peut-être pas le client d'origine. Il s'agit d'une **attaque de renvoi FTP**, et l'inspection FTP arrête la connexion car elle considère qu'il s'agit d'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

Configuration

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

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



Configurez l'ASA par l'intermédiaire du CLI

Complétez ces étapes afin de configurer l'ASA :

1. Désactiver l'inspection FTP :

```
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 d'autoriser la communication entre le client FXP et les deux serveurs 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
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
```

Vérification

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

Processus de transfert de fichiers

Complétez ces étapes afin de vérifier le transfert de fichiers réussi entre les deux serveurs FTP :

1. Connectez-vous au serveur 1 à partir de la machine cliente FXP :

G FTP Rush ftp://10.1.1.10						-0	
Eile Edit Mark View FTP Tool	s <u>H</u> elp						
🕴 📶 🔯 🛛 Do not use proxy 🔹 🐲 🝷 Hi	ost 10.1.1.10		Port 21	User	Pass		2
● ftp://10.1.1.10 ● blank							
(1) Remote: ftp://10.1.1.10			(2) Remote				
😔 🛃 📬 📃 🕨 🗧	× 🖸 💻		-			0 া 🕨	₽.
E /	-	Ŧ	1				
Name 🛆	Size Date	*	Name	1	Size Date	Attr	ib
🔒 Parent Directory		1					
🍌 3cdaemon	0 05/08/2014 11						
Lores 1	0 06/12/2013 07						
b Cores 2	0 06/12/2013 07						
Cisco ASDM-IDM Launcher.lnk	2.3 k 06/10/2013 08	Е					
Cores 1.zip	277.0 M 06/12/2013 07						
Cores 2.zip	140.6 M 06/12/2013 08						
desktop.ini	282 b 06/03/2013 09						
E ftprush.exe	3.8 M 05/08/2014 11						
Google Chrome.Ink	2.3 k 09/06/2013 11						
jre-6u31-windows-i586-s.exe	16.4 M 06/10/2013 08						
server? tvt	10 h 05/08/2014 16	-					
	• • •						
9 file(s) 3 folder(s) 437.9	M byte(s)						
🛐 FTP Log 🚯 Transfer Log 🖳 Syst	em Log						
Name Progress Speed	Transferred		Size	Source p	ath Target	path Rem	iark
					BandWidth () = /		Khoe
					Danovviour (OL)	01.0.00/0.00	Tupo .::

2. Connectez-vous au serveur 2 à partir de la machine cliente FXP :

6 FTP Rush ftp://10.1.1.10 - ftp://192.16	58.1.10			
Eile Edit Mark View FTP Tools	Help			-
🗄 🗐 🖄 Ďo not use proxy 🔹 🧈 🔻 Hos	t 192.168.1.10	•	Port 21 🗘 User	Pass
• ftp://10.1.1.10 - ftp://192.168.1.10				
(1) Remote: ftp://10.1.1.10			(2) Remote: ftp://192.168.1.10	
🕹 💼 📬 🔳 🕨 🗙	() 1 📃	1	•	🗙 📵 🏎 💻 📲
1.1	•	Ŧ	:/	
Name 🛆	Size Date	*	Name 🕢	Size Date 🔺
 Parent Directory 3cdaemon FileZilla Server iperf windows-tools ~DF38A940C089545280.TMP ASDM on 123.123.124.1-444.lnk Cisco ASDM-IDM Launcher.lnk desktop.ini ftprush.exe Google Chrome.lnk ize-6131-windows-i586-s.eve III 	0 05/08/2014 0 05/06/2014 0 09/04/2013 0 02/19/2014 0 b 05/08/2014 2.0 k 10/10/2013 2.3 k 05/29/2014 282 b 06/03/2014 3.8 M 05/06/2014 2.3 k 09/06/2013 16 4 M 05/29/2014	H	Image: Constant C	0 05/08/2014 11 0 06/12/2014 07 0 06/12/2014 07 0 05/29/2014 11 2.3 k 06/10/2014 08 277.0 M 06/12/2014 08 282 b 06/03/2014 08 282 b 06/03/2014 09 3.8 M 05/08/2014 11 2.3 k 09/06/2013 11 16 4 M 06/10/2014 08
14 file(s) 4 folder(s) 307.9 M	1 byte(s)		11 file(s) 4 folder(s	;) 718.5 M byte(s)
I2l List Complete: 1,064 by FTP Log Transfer Log Name Progress Speed	tes in 0.22 sea nLog Tasks Transferred	con	nds 〈4.86KB/s〉 Size Source path	⊥ Target path Remark
1 2 1 0			BandWid	ith (UL/DL): 0.00/0.00 Kbps ,;;

3. Faites glisser le fichier à transférer de la fenêtre server1 vers la fenêtre server2 :

6 FTP Rush ftp://10.1.1.10 - ftp://192.168	1.10						
Eile Edit Mark View FTP Tools	<u>H</u> elp						÷
🗄 📋 🔯 🛛 Do not use proxy 💌 🐲 👻 Host	192.168.1.10	•	Port 21	User	Pass		
• ftp://10.1.1.10 - ftp://192.168.1.10							
(1) Remote: ftp://10.1.1.10			(2) Remote: f	tp://192.168.1.10			
🛛 🕹 📑 🔲 🕨 🗙	0	-	-8-	ə 📔 🔟	×	ti 🕪 🛙	2 [
: /./	•	Ŧ	: 1.1				• =
Name 🛆	Size Date	^	Name		4	Size Date	*
@ desktop.ini	282 b 06/03/2014		🍌 FileZilla Ser	rver		0 05/29/2	014 11
E ftprush.exe	3.8 M 05/06/2014		Cisco ASDI	M-IDM Launcher.lnk		2.3 k 06/10/2	2014 08
Google Chrome.Ink	2.3 k 09/06/2013		Cores 1.zip	0		277.0 M 06/12/2	01407
ire-6u31-windows-i586-s.exe	16.4 M 05/29/2014		Cores 2.zip	0		140.6 M 06/12/2	2014 08
Kiwi_Syslogd.exe	6.9 M 05/06/2014		desktop.ini	i		282 b 06/03/2	2014 05
monocleexception.pcapng	255.2 k 11/15/2013		E ftprush.ex	e		3.8 M 05/08/2	2014 11
💷 openload.exe	60.0 k 11/27/2013		Google Chr	rome.lnk		2.3 k 09/06/2	013 11 =
ratelimit.pcapng	280.4 M 09/04/2013	Ξ	ire-6u31-w	indows-i586-s.exe		16.4 M 06/10/2	014 08
server 1. txt	17 b 05/27/2014		monodeex	ception.pcapng		255.2 k 05/29/2	2014 10
test.txt	31b 05/17/2014		ratelimit.pd	apng		280.4 M 05/29/2	014 11
indows-tools.zip	126.0 k 02/19/2014	-	test	r 1. txt		31 b 05/29/2	01408
•	4		< ۲	III			•
1 file(s) 0 folder(s) 17 byte		10 file(s) 4 folder(s) 718.5 M byte(s)					

4. Vérifiez que le transfert de fichiers a réussi :

6 FTP Rush ftp://10.1.1.10 - ftp://192.10	58.1.10					
Eile Edit Mark View FTP Tools	Help					
🗄 📶 🔯 🚺 Do not use proxy 🗸 💷 🔻 Hos	t 192.168.1.10	-	Port 21	User	Pass	1
• ftp://10.1.1.10 - ftp://192.168.1.10						
(1) Remote: ftp://10.1.1.10			(2) Remote: 1	ftp://192.168.1.1	D	
😔 🛃 📬 🔳 🕨 🗴	(O 💻		8	s 📬 🖬	× 1	•
: /./		-	:/			
Name 🔬	Size Date		Name		4	Size Date
R. Parent Directory			1. Parent Dir	ectory		
3cdaemon	0 05/08/2014	4	3cdaemon			0 05/08/2014 11
FileZilla Server	0 05/06/2014	ŧ	Cores 1			0 06/12/2014 07
🗼 iperf	0 09/04/2013	3	Cores 2			0 06/12/2014 07
📙 windows-tools	0 02/19/2014	4	🔒 FileZila Se	rver		0 05/29/2014 11
~DF38A940C0895452B0.TMP	0 b 05/08/2014	4	Cisco ASDI	M-IDM Launcher.lr	nk	2.3 k 06/10/2014 08
ASDM on 123.123.124.1-444.lnk	2.0 k 10/10/2013	3	Cores 1.zi	p	277	.0 M 06/12/2014 07
Cisco ASDM-IDM Launcher.lnk	2.3 k 05/29/2014	4	Cores 2.zi	p	140	.6 M 06/12/2014 08
👔 desktop.ini	282 b 06/03/2014	1	desktop.in	i	2	82 b 06/03/2014 09
ftprush.exe	3.8 M 05/06/2014	ŧ	Ftprush.ex	e	3	.8 M 05/08/2014 11
Google Chrome.lnk	2.3 k 09/06/2013	3	Google Ch	rome.Ink		2.3 k 09/06/2013 11
ire-6u31-windows-i586-s eve	16 4 M 05/29/2014	4 *	ire-6(131-//	vindows-i586-s ev III	e 16	4M 06/10/2014 08
14 file(s) 4 folder(s) 307.9 f	4 byte(s)			11 file(s) 4 fold	der(s) 718.5 M by	te(s)
[2] List Complete: 1,064 by	tes in 0.22 se	cor	nds (4.86)	(B/s)		1
FTP Log 💽 Transfer Log 🖳 System	m Log G Tasks					
Name Progress Speed	Transferred		Size	Source path	Target path	Remark
11 42 490				Ban	dWidth (UL/DL): (1.00/0.00 Kbps

Dépannage

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

Scénario d'inspection FTP désactivé

Lorsque l'inspection FTP est désactivée, comme indiqué dans la section <u>Inspection FTP et FXP</u> de ce document, ces données apparaissent sur l'interface client ASA :

2006-12-12	02:56:17.199376	172.16.1.10	10.1.1.10	FTP	60 Request: PASV
2006-12-12	02:56:17.200902	10.1.1.10	172.16.1.10	FTP	100 Response: 227 Entering passive mode (10,1,1,10,192,96)
2006-12-12	02:56:17.201481	172.16.1.10	192.168.1.10	FTP	77 Request: PORT 10,1,1,10,192,96
2006-12-12	02:56:17.203297	192.168.1.10	172.16.1.10	FTP	84 Response: 200 PORT command successful.
2006-12-12	02:56:17.203953	172.16.1.10	192.168.1.10	FTP	77 Request: STOR Kiwi_Syslogd.exe
2006-12-12	02:56:17.206272	192.168.1.10	172.16.1.10	FTP	106 Response: 150 File status OK ; about to open data connection
2006-12-12	02:56:17.206852	172.16.1.10	10.1.1.10	FTP	77 Request: RETR Kiwi_Syslogd.exe
2006-12-12	02:56:17.208698	10.1.1.10	172.16.1.10	PTP	90 Response: 125 Using existing data connection
2006-12-12	02:56:17.420617	172.16.1.10	192.168.1.10	TOP	54 50684 > ftp [ACK] Seg=159 Ack=459 Win=130560 Len=0
2006-12-12	02:56:17.420724	172.16.1.10	10.1.1.10	TCP	54 50685 > ftp [ACK] 5eq=119 Ack=433 Win=130668 Len=0
2006-12-12	02:56:18.340741	10.1.1.10	172.16.1.10	FTP	110 Response: 226 Closing data connection; File transfer successful.
2006-12-12	02:56:18.341382	192.168.1.10	172.16.1.10	FTP	110 Response: 226 Closing data connection: File transfer successful.

Voici quelques notes sur ces données :

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

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

Inspection FTP activée

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

2005-12-12 03:0	NB:16.7589N2	172.15.1.10	10.1.1.10	ETP	60 Request: PASM
2006-12-12 03:0	08:16.760443	10.1.1.10	172.18.1.10	FTP	100 Response: 227 Entering passive mode (10,1,1,10,192,99)
2005-12-12 03:0	08:16.761023	172.15.1.10	192.158.1.10	FTP	/7 Request: PORT 10,1,1,10,192,99
2005-12-12 03:0	08:15.964275	172.15.1.10	10.1.1.10	TCP	54 50693 > ftp [ACK] Seq=96 Ack=397 Win=130704 Len=0
2006-12-12 03:0	08:17.073757	172.16.1.10	192.168.1.10	FTP	77 [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:0	08:17.683100	172.15.1.10	192.158.1.10	FTP	77 [TCP Retransmission] Request: PCRT 10,1,1,10,192,99
2008-12-12 03:0	08:18.901885	172.16.1.10	192.188.1.10	ETP	77 [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12-03:0	08:20.120875	172.16.1.10	192.168.1.10	FTP	77 [TCP Retransmission] Request: PORT 10,1,1,10,192,39
2005-12-12 03:1	08:21.339398	172.15.1.10	192.158.1.10	FTP	77 [TCP Retransmission] Request: PCRT 10,1,1,10,192,99
2008-12-12 03:0	08:23.761328	172.16.1.10	192.168.1.10	FTP	77 [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:0	08:28.573883	172.16.1.10	192.168.1.10	FTP	77 [TCP Retransmission] Request: PCRT 10.1.1.10.192.39

Voici les captures d'écran ASA :

2000-12-12 03:08:17.073818				// [TCP Acked unseen segment] Request: PORT 10,1,1,10,192,99
2006-12-12 03:08:17.673045	192.168.1.10	172.16.1.10	PTP	74 [TCP ACKed unseen segment] [TCP Retransmission] Response: 200 Type set to I.
2006-12-12 01:00:17.683176	172 16 1.10	192.168.1.10	ETP	77 [TCP ACKed unseen segment] [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2006-12-12 03:08:18.874695	192.168.1.10	172.16.1.10	FTP	74 [TCP ACKed unseen segment] [TCP Retransmission] Response: 200 Type set to I.
2006-12-12 03:08:18.901946	172.16.1.10	192.168.1.10	FTP	77 [TCP ACKed unseen segment] [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2006-12-12 03:08:20.075405	192.168.1.10	172.16.1.10	FTP	74 [TCP ACKed unseen segment] [TCP Retransmission] Response: 200 Type set to I.
2006-12-12 03:08:20.120736	172.16.1.10	192.168.1.10	PTP	77 [TCP ACked unseen segment] [TCP Retransmission] Request: PORT 10.1.1.10.192.99
2006-12-12 01:08:21.276780	192 168 1.10	172.16.1.10	PTP .	74 [TCP ACKed unseen segment] [TCP Retransmission] Response: 200 Type set to I.
2006-12-12 01:08:21.339475	172.16.1.10	192.168.1.10	FTP	77 [TCP ACKed unseen segment] [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2006-12-12 03:08:23.679118	192.168.1.10	172.16.1.10	FTP	74 [TCP ACKed unseen segment] [TCP Retransmission] Response: 200 Type set to I.
2006-12-12 03:08:23.761389	172.16.1.10	192, 168, 1, 10	ETP.	77 [TCP ACked unseen segment] [TCP Retransmission] Request: PORT 10.1.1.30.192.99
2006-12-12 03:08:28.483983	192.168.1.10	172.16.1.10	PTP .	74 [TCP ACKed unseen segment] [TCP Retransmission] Response: 200 Type set to I.
2006-12-12 03:08:28.573960	172.16.1.10	192.168.1.10	PTP	77 [TCP ACKed unseen segment] [TCP Retransmission] Request: FORT 10,1,1,10,192,99
2006-12-12 03:08:38.093836	192.168.1.10	172.16.1.10	TOP	54 [TCP ACKed unseen segment] Ftp > 50692 [RST, ACK] Seq=21 Ack=1 Win=0 Len=0
1000 State 12 - 12 - 20 - 20 - 10 10 10 10	172 18 1 10	A REAL PROPERTY AND A REAL	and so the	U. DTCD ACKed uppears reasonabl \$0500 > Ebs [057 ACK] See 1900/04514 Adv 721005500 Min-A Lan-A

La demande **PORT** est abandonnée par l'inspection FTP car elle contient une adresse IP et un port qui diffèrent de l'adresse IP et du port du client. Par la suite, la connexion de contrôle au serveur est interrompue par l'inspection.