FXP を使用した ASA ファイル転送の設定例

内容

概要 <u>前提条件</u> <u>要件</u> 使用するコンポーネント 背景説明 FXP によるファイル転送のメカニズム FTP インスペクションおよび FXP 設定 ネットワーク図 CLI による ASA の設定 確認 ファイル転送プロセス トラブルシュート FTP インスペクションが無効なシナリオ FTP インスペクションが有効

概要

このドキュメントでは、CLI で Cisco 適応型セキュリティ アプライアンス(ASA)の File eXchange Protocol(FXP)を設定する方法について説明します。

前提条件

要件

このドキュメントの読者は File Transfer Protocol(FTP)(アクティブ/パッシブ モード)の基本 的な知識を持っていることを推奨します。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 8.0.x 以降が稼働する Cisco ASA に基づい ています。

注:この設定例は、FXP サーバおよび実行 FTP サービス(3C デーモン)として機能する 2 つの Microsoft Windows ワークステーションを使用します。 また、それぞれの FXP を有効 化します。FXP クライアント ソフトウェア(FTP Rush)を実行する別の Microsoft Windows ワークステーションも使用します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

背景説明

FXP はクライアントのインターネット接続速度に依存することなく、FXP クライアントを経由し て FTP サーバから別の FTP サーバにファイルを転送することができます。FXP では、最大転送 速度は、2つのサーバ間の接続のみに依存し、通常、クライアント接続よりもはるかに高速です 。高帯域幅のサーバが別の高帯域幅サーバからリソースを要求する場合に FXP を適用できますが 、リモートで動作するネットワーク管理者などの低帯域幅のクライアントのみに両方のサーバの リソースにアクセスする権限があります。

FXPはFTPプロトコルの拡張として動作し、機構はFTP RFC 959のセクション5.2に記載されてい ます。基本的に、FTP server1との制御接続を開始し、FTP server2との別の制御接続を開き、2台 のサーバ間で転送が直接行われるようにわれます。

FXP によるファイル転送のメカニズム



プロセスの概要を次に示します。

1. クライアントが server1 の TCP ポート 21 で制御接続を開きます。

クライアントは server1 にPASV コマンドを送信します。

server1 が IP アドレスとリッスンしているポートで応答します。

2. クライアントが server2 の TCP ポート 21 で制御接続を開きます。

クライアントは PORT コマンドで server1 から受信したアドレスとポートを server2 に渡します。

server2 は PORT コマンドが正常であることをクライアントに通知するために応答します。 これで、server2 はデータの送信先を確認できました。 3. server1 から server2 への送信プロセスを開始するために次の動作が実行されます。

クライアントは server2 に STOR コマンドを送信し、受信した日付を保存するように指示します。

クライアントは server1 に RETR コマンドを送信し、ファイルの取得または送信を指示します。

4. これで、データはすべて、送信元から宛先 FTP サーバに直接送信されます。両方のサーバ はクライアントに失敗または成功のステータス メッセージを報告するだけます。 接続テーブルの表示は次のとおりです。

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

FTP インスペクションおよび FXP

FXP 経由の ASA までのファイル転送は FTP インスペクションが ASA で**無効の場合にのみ成功** します。

FXP クライアントが FTP PORT コマンドのクライアントのものとは異なる IP アドレスおよび TCP ポートを指定する場合、攻撃者がサードパーティの FTP サーバからインターネットにある ホストに対してポート スキャンを実行できるというセキュリティに問題がある状況になります。 これは、FTP サーバが、発信元ではないクライアントの可能性があるマシンのポートに対し接続 を開くことをに指示されるためです。これは FTP バウンス攻撃と呼ばれ、FTP インスペクショ ンはこれをセキュリティ違反と見なして接続をシャットダウンします。

以下が一例です。

%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

設定

ASA の FXP を設定するためにこの項で説明されている情報を活用してください。

注:このセクションで使用されるコマンドの詳細については、Command Lookup Tool(登 録ユーザ専用)を使用してください。



CLI による ASA の設定

ASA を設定するには、次の手順を実行します。

1. FTP インスペクションを無効にします。

2. FXP クライアントと 2 つの FTP サーバ間の通信を許可するアクセス リストを設定します。

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 any FXP-ASA(config)#access-list client extended permit ip any host 172.16.1.10
3. アクセス リストをそれぞれのインターフェイスに適用します。

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

確認

設定が適切に機能することを検証するためにこの項で説明されている情報を活用してください。

ファイル転送プロセス

2 つの FTP サーバ間の正常なファイル転送を検証するには、次の手順を実行します。

1. FXP クライアント マシンから server1 に接続します。

STP Rush ftp://10.1.1.10						
Ele Edit Mark View FTP Tools Help						-
🚰 👩 Do not use proxy 🔹 🧈 🕶 Host 10.1.1.10	-	Port 21 🌲	User		Pass	
● ftp://10.1.1.10 ◎ blank						
(1) Remote: ftp://10.1.1.10		(2) Remote				
🛿 🕹 📑 🔳 🕨 🗶 🔞 💻	22 19	-			× 1	•
:/	=	1				
Name / Size Date	*	Name	1	Size	Date	Attrib
1. Parent Directory						
3cdaemon 0 05/08/2014 11						
Cores 1 0 06/12/2013 07						
Cores 2 0 06/12/2013 07						
Cisco ASDM-IDM Launcher.lnk 2.3 k 06/10/2013 08	III					
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.lnk 2.3 k 09/06/2013 11						
ire-6u31-windows-i586-s.exe 16.4 M 06/10/2013 08						
server2 tvt 10 h 05/08/2014 16	-					
9 file(s) 3 folder(s) 437 9 M hyte(s)	-					
s metal s tonici (s) tonici (s)	-					1.2
						12
E FTP Log Fransfer Log System Log Log Tasks						
Name Progress Speed Transferred		Size	Source pa	ath	Target path	Remark
				BandWie	dth (UL/DL): 0.	00/0.00 Kbps .:

2. FXP クライアント マシンから server2 に接続します。

6 FTP Rush ftp://10.1.1.10 - ftp://192.1	68.1.10			
Eile Edit Mark View FTP Tools	Help			-
🗄 👩 🖄 Do not use proxy 🔹 🧈 🔻 Ho	st 192.168.1.10	-	Port 21 🗘 User Pa	ss
• ftp://10.1.1.10 - ftp://192.168.1.10				
(1) Remote: ftp://10.1.1.10			(2) Remote: ftp://192.168.1.10	
	🕻 🛛 🔁 👘		🕹 🛃 🖬 🖬 🗙	: 🔞 🕩 🚊 📲
± /./		Ţ	1/	• =
Name	Size Date		Name 🗸 📔	Size Date 🔺
	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 3.8 M 05/06/2014 3.8 M 05/06/2014 2.3 k 09/06/2013	H H	Parent Directory 3cdaemon Cores 1 Cores 2 FileZila Server Cisco ASDM-IDM Launcher.Ink Cores 1.zip Cores 2.zip desktop.ini ftprush.exe Google Chrome.Ink ire-ful31-windows-i586-s.eve Image: State Sta	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 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 byte(s)		11 file(s) 4 folder(s) 7	18.5 M byte(s)
[2] List Complete: 1,064 by FTP Log Transfer Log System Name Progress Speed	mLog G Tasks	cor	ads (4.86KB/s)	rget path Remark
🗖 1 📲 2 🐙 0			BandWidth	(UL/DL): 0.00/0.00 Kbps ,;;

3. server1 のウィンドウから server2 のウィンドウに転送するファイルをドラッグ アンド ドロ ップします。

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 7
• ftp://10.1.1.10 - ftp://192.168.1.10				
(1) Remote: ftp://10.1.1.10			(2) Remote: ftp://192.168.1.10	
🛛 🕹 📑 🔲 🕨 🗙	0	••	🔹 🛃 📬 🔳 🗧	🗙 🔞 🕩 🚊 📲
i /./		Ţ	: [.]	
Name 🗸	Size Date	*	Name 🕹	Size Date
@ desktop.ini	282 b 06/03/2014		鷆 FileZilla Server	0 05/29/2014 11
E ftprush.exe	3.8 M 05/06/2014		Cisco ASDM-IDM Launcher.lnk	2.3 k 06/10/2014 08
Google Chrome.Ink	2.3 k 09/06/2013		Cores 1.zip	277.0 M 06/12/2014 07
jre-6u31-windows-i586-s.exe	16.4 M 05/29/2014		Cores 2.zip	140.6 M 06/12/2014 08
Kiwi_Syslogd.exe	6.9 M 05/06/2014		💓 desktop.ini	282 b 06/03/2014 09
monocleexception.pcapng	255.2 k 11/15/2013		ftprush.exe	3.8 M 05/08/2014 11
openload.exe	60.0 k 11/27/2013		Google Chrome.Ink	2.3 k 09/06/2013 11 =
ratelimit.pcapng	280.4 M 09/04/2013	Ξ	💷 jre-6u31-windows-i586-s.exe	16.4 M 06/10/2014 08
server 1. txt	17 b 05/27/2014		monodeexception.pcapng	255.2 k 05/29/2014 10
test.txt	31b 05/17/2014		ratelimit.pcapng	280.4 M 05/29/2014 11
indows-tools.zip	126.0 k 02/19/2014	Ŧ	test.txt server1.txt	31 b 05/29/2014 08
<	•		< <u>۲</u>	•
1 file(s) 0 folder(s) 17 byte	e(s)	10 file(s) 4 folder(s	s) 718.5 M byte(s)	

4. ファイル転送が成功することを検証します。

G FTP Rush ftp://10.1.1.10 - ftp://192.16	8.1.10						X
Eile Edit Mark View FTP Tools	Help						-
🗄 📶 🖄 Ďo not use proxy 🔹 💷 💌 Host	192, 168, 1, 10	-	Port 21	User	Pass		2
• ftp://10.1.1.10 - ftp://192.168.1.10							
(1) Remote: ftp://10.1.1.10			(2) Remote: ft	o://192.168.1.10			
🛛 🕹 📑 🔳 🕨 🗙	0 🖻	11 14	•		× 0		
: /./	•	Ţ	:/				
Name 🛆	Size Date		Name		4	Size Date	
1 Parent Directory			🔒 Parent Direc	tory			
🗼 3cdaemon	0 05/08/2014		📕 3cdaemon			0 05/08/20	14 11
📕 FileZilla Server	0 05/06/2014	-	Cores 1			0 06/12/20	14 07
🍌 iperf	0 09/04/2013	=	l Cores 2			0 06/12/20	1407 ≣
🎍 windows-tools	0 02/19/2014		📕 FileZilla Serv	er		0 05/29/20	14 11
~DF38A940C0895452B0.TMP	0 b 05/08/2014		Cisco ASDM	IDM Launcher.lnk	8	2.3 k 06/10/20	14 08
ASDM on 123.123.124.1-444.lnk	2.0 k 10/10/2013		Cores 1.zip		27	7.0 M 06/12/20	14 07
Cisco ASDM-IDM Launcher.lnk	2.3 k 05/29/2014		Cores 2.zip		14	10.6 M 06/12/20	14 08
desktop.ini	282 b 06/03/2014		desktop.ini			282 b 06/03/20	14 05
ftprush.exe	3.8 M 05/06/2014		ftprush.exe			3.8 M 05/08/20	14 11
Google Chrome.Ink	2.3 k 09/06/2013		Google Chro	me.lnk		2.3 k 09/06/20	13 11
ire-6u31-windows-i586-s eve	16 4 M 05/29/2014	-	ire-Au31-wir	ndowie-1586-e eve		6 4 M 06/10/20	14 05 *
< m	<u> </u>		<		() 740 544		•
14 file(s) 4 folder(s) 307.9 M	byte(s)			11 file(s) 4 folde	r(s) /18.5 M t	lyte(s)	
[2] List Complete: 1,064 by	tes in 0.22 se	cor	nds (4.86KB	l/s)			12
FTP Log Transfer Log 🔛 System	Log G Tasks						
Name Progress Speed	Transferred		Size	Source path	Target pat	n Remark	
				Bandt	Midth () II (D))-	0.00/0.00 Khoe	
				Danuv	waar (oc/oc).	0.0010.001005	.::

トラブルシュート

この項では、設定のトラブルシューティングに役立つ2つのシナリオのキャプチャを提示します。

FTP インスペクションが無効なシナリオ

このドキュメントの「FTP インスペクションおよび FXP」の項の記載のとおり、FTP インスペク ションが無効な場合、ASA クライアント インターフェイスにデータが表示されます。

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	TCP	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	TOP	54 50685 > ftp [ACK] seq=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	ETP	110 Response: 226 Closing data connection: File transfer successful.

このデータについてのポイントを次に示します。

• クライアントの IP アドレスは 172.16.1.10 です。

• server1 の IP アドレスは 10.1.1.10 です。

• server2 の IP アドレスは 192.168.1.10 です。

この例では、Kiwi_Syslogd.exe というファイルが server1 から server2 に転送されます。

FTP インスペクションが有効

FTP インスペクションが有効な場合、このデータは ASA クライアント インターフェイスに表示 されます。

2005-12-12 03:00	8:16.758902	172.15.1.10	10.1.1.10	ETP	60 Request: PASV
2006-12-12 03:00	8:16.760443	10.1.1.10	172.18.1.10	FTP	100 Response: 227 Entering passive mode (10,1,1,10,192,99)
2005-12-12 03:03	8:15.761023	172.15.1.10	192.158.1.10	FTP	// Request: PORT 10,1,1,10,192,99
2005-12-12 03:00	8:15.964275	172.15.1.10	10.1.1.10	TCP	54 50693 → ftp [ACK] Seq=96 Ack=397 Win=130704 Len=0
2006-12-12-03:00	8:17.073757	172.16.1.10	192.168.1.10	FTP	77 [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:00	8:17.683100	172.15.1.10	192.158.1.10	FTP	77 [TCP Retransmission] Request: PCRT 10,1,1,10,192,99
2008-12-12 03:00	8:18,901885	172.18.1.10	192.188.1.10	FTP	77 [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12-03:03	8:20.120575	172.16.1.10	192.168.1.10	FTP	77 [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:00	8:21.339398	172.15.1.10	192.158.1.10	FTP	77 [TCP Retransmission] Request: PCRT 10,1,1,10,192,99
2008-12-12 03:00	8:23.761328	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	8:28.573883	172.16.1.10	192.168.1.10	FTP	77 [TCP Retransmission] Request: PCRT 10.1.1.10.192.39

ASA ドロップのキャプチャは次のとおりです。

2006-12-12 03:08:17.073818				
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 03:08:17.683176	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 03:08:18.874695	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	ETP.	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	ETP	77 [TCP ACKed unseen segment] [TCP Retransmission] Request: RORT 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 10.1.1,10.192,99
2006-12-12 03:08:28.483983	192.168.1.10	172.16.1.10	PTP	74 [TCM ACKed unseen segment] [TCM Retransmission] Response: 200 Type set to I.
2006-12-12 01:08:28.573960	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 03:08:38 093836	192.168.1.10	172 16 1 10	TOP	54 [TCP ACKed unseen segment] Ftp > 50692 [RST, ACK] Seg=21 Ack=1 Win=0 Len=0
2006-12-12 01:08:38 183538	172 16 1.10	192 168 1 10	1015	54 [TCP_ACKed_unseen_segment] 50692 > ftp_[PST_ACK]_seg=3809484534_Ack=721905608_Min=0_Len=

クライアント IP アドレスおよびポートとは異なる IP アドレスおよびポートが含まれているため、 PORT 要求は FTP インスペクションによってドロップされます。その後、サーバへの制御接続はそのインスペクションで終了します。