Esempio di configurazione di ASA File Transfer con FXP

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Meccanismo di trasferimento file tramite FXP Controllo FTP e FXP Configurazione Esempio di rete Configurazione dell'ASA tramite CLI Verifica Processo di trasferimento file Risoluzione dei problemi Scenario di disattivazione ispezione FTP Ispezione FTP abilitata

Introduzione

Questo documento descrive come configurare il protocollo File eXchange Protocol (FXP) su Cisco Adaptive Security Appliance (ASA) tramite la CLI.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base del protocollo FTP (File Transfer Protocol) (modalità attiva/passiva).

Componenti usati

Per questo documento, è stato usato un Cisco ASA con software versione 8.0 e successive.

Nota: In questo esempio di configurazione vengono utilizzate due workstation Microsoft

Windows che fungono da server FXP e eseguono i servizi FTP (Daemon 3C). Inoltre, FXP è abilitato. Viene utilizzata anche un'altra workstation Microsoft Windows con software client FXP (FTP Rush).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

FXP consente di trasferire i file da un server FTP a un altro server FTP tramite un client FXP senza la necessità di dipendere dalla velocità della connessione Internet del client. Con FXP, la velocità massima di trasferimento dipende solo dalla connessione tra i due server, che in genere è molto più veloce della connessione client. È possibile applicare FXP in scenari in cui un server a larghezza di banda elevata richiede risorse da un altro server a larghezza di banda elevata, ma solo un client a larghezza di banda ridotta, ad esempio un amministratore di rete che lavora in remoto, dispone dell'autorizzazione per accedere alle risorse su entrambi i server.

FXP funge da estensione del protocollo FTP e il meccanismo è indicato nella sezione 5.2 della RFC 959 FTP. In pratica, il client FXP avvia una connessione di controllo con un server FTP1, apre un'altra connessione di controllo con il server FTP2, quindi modifica gli attributi di connessione dei server in modo che puntino l'uno verso l'altro in modo che il trasferimento avvenga direttamente tra i due server.

Meccanismo di trasferimento file tramite FXP



Ecco una panoramica del processo:

1. Il client apre una connessione di controllo con server1 sulla porta TCP 21.

Il client invia il comando PASV a server1.

Server1 risponde con il proprio indirizzo IP e la porta su cui è in ascolto.

2. Il client apre una connessione di controllo con server2 sulla porta TCP 21.

Il client passa l'indirizzo/la porta ricevuta dal server1 al server2 in un comando PORT.

Server2 risponde per informare il client che il comando **PORT** ha esito positivo. Server2 ora sa dove inviare i dati.

3. Per avviare il processo di trasmissione da server1 a server2:

Il client invia il comando STOR al server2 e gli ordina di memorizzare la data che riceve.

Il client invia il comando RETR a server1 e gli ordina di recuperare o trasmettere il file.

 Tutti i dati ora vanno direttamente dall'origine al server FTP di destinazione. Entrambi i server segnalano al client solo i messaggi di stato in caso di esito negativo/positivo.
 La tabella di connessione viene visualizzata nel modo seguente:

```
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
```

Controllo FTP e FXP

Il trasferimento di file tramite ASA tramite FXP ha esito positivo solo quando l'ispezione FTP è **disabilitata** sull'appliance ASA.

Quando il client FXP specifica un indirizzo IP e una porta TCP diversi da quelli del client nel comando **PORT** FTP, si crea una situazione non sicura in cui un utente non autorizzato è in grado di eseguire una scansione della porta su un host su Internet da un server FTP di terze parti. Questo accade perché il server FTP riceve istruzioni per aprire una connessione a una porta su un computer che potrebbe non essere il client da cui proviene. Questo tipo di attacco viene chiamato **attacco di tipo rimbalzo FTP** e l'ispezione FTP chiude la connessione in quanto la considera una violazione della sicurezza.

Di seguito è riportato un esempio:

```
%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
```

Configurazione

Per configurare FXP sull'appliance ASA, usare le informazioni descritte in questa sezione.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).



Configurazione dell'ASA tramite CLI

Per configurare l'ASA, effettuare i seguenti passaggi:

1. Disabilita ispezione FTP:

FXP-ASA(config)# policy-map global_policy
FXP-ASA(config-pmap)# class inspection_default
FXP-ASA(config-pmap-c)# no inspect ftp

2. Configurare gli elenchi degli accessi per consentire la comunicazione tra il client FXP e i due server 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

Applicare gli elenchi degli accessi alle rispettive interfacce:

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

Verifica

Per verificare che la configurazione funzioni correttamente, consultare le informazioni descritte in questa sezione.

Processo di trasferimento file

Per verificare la riuscita del trasferimento di file tra i due server FTP, completare i seguenti passaggi:

1. Connettersi al server1 dal computer client FXP:



2. Connettersi al server2 dal computer client FXP:

| © FTP Rush ftp://10.1.1.10 - ftp://192.168.1.10 | | | | | | |
|---|---|-----|---|--|--|--|
| 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 | | |
| | 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 2.8 M 05/06/2014 3.8 M 05/06/2014 2.3 k 09/06/2013 16 4 M 05/29/2014 | m + | Image: Cores 1 Cores 1 Cores 2 FileZila Server Cisco ASDM-IDM Launcher.Ink Cores 1.zip Cores 2.zip desktop.ini Image: FileZila Server Google Chrome.Ink ire_fur31-windows-i586-s.eve Image: Size Server | 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 3.8 M 05/08/2014 11 2.3 k 09/06/2013 11 16 4 M 06/10/2014 08 b | | |
| 14 file(s) 4 folder(s) 307.9 M | 4 byte(s) | | 11 file(s) 4 folder(s | s) 718.5 M byte(s) | | |
| [2] List Complete: 1,064 by FTP Log Transfer Log System Name Progress Speed | tes in 0.22 sea mLog GTasks Transferred | con | nds 〈4.86KB/s〉 Size Source path | - Target path Remark | | |
| 1 2 1 0 | | | BandWir | dth (UL/DL): 0.00/0.00 Kbps _;; | | |

3. Trascinare il file da trasferire dalla finestra server1 alla finestra server2:

| 6 FTP Rush ftp://10.1.1.10 - ftp://192.168 | 1.10 | | | | [| - • × |
|--|--------------------|---|---------------------|--------------------|-----------|-----------------|
| Eile Edit Mark View FTP Tools | Help | | | | | - |
| 🗄 👩 🔯 🛛 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: ftp | 0://192.168.1.10 | | |
| 🛛 🕹 📑 🔲 🕨 🗙 | 0 🖻 | - | -8- 🛃 | | × 🛛 • | ▶ 😐 📲 |
| : /./ | | Ŧ | : [.] | | | |
| Name 🔺 | Size Date | - | Name | 1 | 4 Size | Date 🔺 |
| @ desktop.ini | 282 b 06/03/2014 | | 鷆 FileZilla Serv | er | (| 0 05/29/2014 11 |
| 💷 ftprush.exe | 3.8 M 05/06/2014 | | Cisco ASDM- | IDM Launcher.lnk | 2.3 | 06/10/2014 08 |
| Google Chrome.Ink | 2.3 k 09/06/2013 | | Cores 1.zip | | 277.0 N | 1 06/12/2014 07 |
| ire-6u31-windows-i586-s.exe | 16.4 M 05/29/2014 | | Cores 2.zip | | 140.6 N | 1 06/12/2014 08 |
| Kiwi_Syslogd.exe | 6.9 M 05/06/2014 | - | desktop.ini | | 282 8 | 06/03/2014 05 |
| monocleexception.pcapng | 255.2 k 11/15/2013 | | E ftprush.exe | | 3.8 N | 1 05/08/2014 11 |
| openload.exe | 60.0 k 11/27/2013 | | Google Chro | me.lnk | 2.3 | 09/06/2013 11 = |
| ratelimit.pcapng | 280.4 M 09/04/2013 | Ξ | ire-6u31-win | dows-i586-s.exe | 16.4 N | 1 06/10/2014 08 |
| server 1. txt | 17 b 05/27/2014 | | monodeexce | eption.pcapng | 255.2 | 05/29/2014 10 |
| test.txt | 31b 05/17/2014 | | ratelimit.pca | png | 280.4 N | 1 05/29/2014 11 |
| indows-tools.zip | 126.0 k 02/19/2014 | - | test tot | l.txt | 311 | 05/29/2014 08 |
| ٠ III | + | | < 🗳 | | | P . |
| 1 file(s) 0 folder(s) 17 byte | | | 10 file(s) 4 folder | (s) 718.5 M byte(s |) | |

4. Verificare che il trasferimento del file sia stato completato:

| G 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 | | |
| • ftp://10.1.1.10 - ftp://192.168.1.10 | | | | | | | |
| (1) Remote: ftp://10.1.1.10 | | | (2) Remote: | ftp://192.168.1.1 | D | | |
| | (T 💻 | - | -8- | 6 📬 🔟 | X 1 | 1 🕪 🛙 | 2 |
| i /./ | • | Ŧ | :/ | | | | - |
| Name 🔬 | Size Date | | Name | | 6 | 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 | m | 11. Parent D 3cdaemo Cores 1 Cores 2 FileZila S Cisco ASI Cores 1.: Cores 2 | rectory n erver DM-IDM Launcher.lr zip zin | nk | 0 05/08/2 0 06/12/2 0 06/12/2 0 05/29/2 2.3 k 06/10/2 277.0 M 06/12/2 140 6 M 06/12/2 | 2014 11 2014 07 2014 07 = 2014 11 2014 08 2014 08 2014 05 |
| desktop.ini ftprush.exe Google Chrome.lnk ire-6u31-windows-i586-s.eve | 282 b 06/03/2014 3.8 M 05/06/2014 2.3 k 09/06/2013 16 4 M 05/29/2014 | + | desktop. ftprush.e Google C ire-6u31 | ini Exe hrome.lnk -windows-1586-s ev | e | 282 b 06/03/2 3.8 M 05/08/2 2.3 k 09/06/2 16,4 M 06/10/2 | 2014 05 2014 11 2013 11 2014 05 |
| 14 fb/c) 4 folder(c) 207 0 l | M hute(a) | | · | 11 file(s) 4 fol | dor(a) 710 E M | (byte(c) | + |
| | Hoyte(s) | | 1 (4.00 | IT me(s) + ion | Jer (s) 7 10.5 P | i byte(s) | |
| FTP Log Transfer Log System | mLog G Tasks | cor | ias (4.86 | KB/S) | | | 12 |
| Name Progress Speed | Transferred | | Size | Source path | Target pa | th Remark | (|
| 1 4 2 4 0 | | | | Ban | dwidth (UL/DI | .): 0.00/0.00 Кbj | ps " |

Risoluzione dei problemi

In questa sezione vengono acquisiti due diversi scenari che è possibile utilizzare per risolvere i problemi relativi alla configurazione.

Scenario di disattivazione ispezione FTP

Quando l'ispezione FTP è disabilitata, come descritto nella sezione <u>Ispezione FTP e FXP</u> di questo documento, i dati vengono visualizzati sull'interfaccia 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 | 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 | FTP | 110 Response: 226 Closing data connection: File transfer successful. |

Ecco alcune note relative a questi dati:

- L'indirizzo IP del client è **172.16.1.10**.
- L'indirizzo IP di Server1 è 10.1.1.10.
- L'indirizzo IP di Server2 è 192.168.1.10.

In questo esempio, il file Kiwi_Syslogd.exe viene trasferito da server1 a server2.

Ispezione FTP abilitata

Quando l'ispezione FTP è abilitata, questi dati vengono visualizzati sull'interfaccia client ASA:

| 2005-12-12 | 03:08:15.758902 | 172.15.1.10 | 10.1.1.10 | ETP | 60 Request: PASV |
|----------------|-----------------|-------------|--------------|-----|--|
| 2006-12-12 | 03:08:16.760443 | 10.1.1.10 | 172.18.1.10 | FTP | 100 Response: 227 Entering passive mode (10,1,1,10,192,99) |
| 2005-12-12 | 03:08:15.761023 | 172.15.1.10 | 192.158.1.10 | FTP | 77 Request: PORT 10,1,1,10,192,99 |
| 2005-12-12 | 03:08:15.964275 | 172.15.1.10 | 10.1.1.10 | TCP | 54 50693 → ftp [ACK] Seq=96 Ack=397 Win=130704 Len=0 |
| 2006-12-12 | 03:08:17.073757 | 172.16.1.10 | 192.168.1.10 | FTP | 77 [TCP Retransmission] Request: PCRT 10,1,1,10,192,99 |
| 2005-12-12 | 03:08:17.683100 | 172.15.1.10 | 192.158.1.10 | FTP | 77 [TCP Retransmission] Request: PCRT 10,1,1,10,192,99 |
| 2008-12-12 | 03:08:18.901885 | 172.18.1.10 | 192.16B.1.10 | ETP | 77 [TCP Retransmission] Request: PCRT 10,1,1,10,192,99 |
| 2005-12-12 | 03:08:20.120575 | 172.16.1.10 | 192.168.1.10 | FTP | 77 [TCP Retransmission] Request: PORT 10,1,1,10,192,39 |
| 2005-12-12 | 03:08:21.339398 | 172.15.1.10 | 192.158.1.10 | FTP | 77 [TCP Retransmission] Request: PCRT 10,1,1,10,192,99 |
| 2008-12-12 | 03:08:23.761328 | 172.18.1.10 | 192.188.1.10 | FTP | 77 [TCP Retransmission] Request: PCRT 10,1,1,10,192,99 |
| 2005 - 12 - 12 | 03:08:28.573883 | 172.16.1.10 | 192.158.1.10 | FTP | 77 [TCP Retransmission] Request: PCRT 10.1.1.10.192.39 |

Di seguito sono riportate le acquisizioni della drop dell'ASA:

| CANA TE TE ANYAGITI PALADIA | | | | |
|---|--------------|-----------------------------|--|--|
| 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 | FTP | 77 [TCP ACKed unseen segment] [TCP Retransmission] Request: FORT 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: FORT 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 10,1,1,10,192,99 |
| 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 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 01:08:38.093816 | 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 |
| The second se | 172 18 1 10 | THE REPORT OF THE REPORT OF | and an effect of the local division of the l | 54 [TCL #CVed upsage segment] 50502 > Etc [DST_ #CV] 5ag 1900/94514 #ck-721025509 Http-A Lag-0 |

La richiesta **PORT** viene scartata dall'ispezione FTP perché contiene un indirizzo IP e una porta diversi dall'indirizzo IP e dalla porta del client. Successivamente, la connessione di controllo al server viene interrotta dall'ispezione.