Exemplo de configuração de transferência de arquivo ASA com FXP

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Mecanismo de transferência de arquivos via FXP Inspeção FTP e FXP Configurar Diagrama de Rede Configurar o ASA via CLI Verificar Processo de transferência de arquivos Troubleshoot Cenário de inspeção de FTP desativado Inspeção de FTP habilitada

Introduction

Este documento descreve como configurar o File eXchange Protocol (FXP) no Cisco Adaptive Security Appliance (ASA) via CLI.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico do FTP (File Transfer Protocol, protocolo de transferência de arquivos) (modos ativo/passivo).

Componentes Utilizados

As informações neste documento são baseadas no Cisco ASA que executa o software versões 8.0 e posteriores.

Note: Este exemplo de configuração usa duas estações de trabalho do Microsoft Windows que atuam como servidores FXP e executam serviços FTP (3C Daemon). Eles também têm o FXP ativado. Outra estação de trabalho do Microsoft Windows que executa o software cliente FXP (FTP Rush) também é usada.

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.

Informações de Apoio

O FXP permite que você transfira arquivos de um servidor FTP para outro servidor FTP por meio de um cliente FXP sem a necessidade de depender da velocidade da conexão com a Internet do cliente. Com o FXP, a velocidade máxima de transferência depende apenas da conexão entre os dois servidores, que geralmente é muito mais rápida que a conexão do cliente. Você pode aplicar o FXP em cenários onde um servidor de alta largura de banda exige recursos de outro servidor de alta largura de banda, mas apenas um cliente de baixa largura de banda, como um administrador de rede que trabalha remotamente, tem autoridade para acessar os recursos em ambos os servidores.

O FXP funciona como uma extensão do protocolo FTP, e o mecanismo é indicado na seção 5.2 do FTP RFC 959. Basicamente, o cliente FXP inicia uma conexão de controle com um servidor FTP1, abre outra conexão de controle com o servidor FTP2 e modifica os atributos de conexão dos servidores para que eles apontem um para o outro de modo que a transferência ocorra diretamente entre os dois servidores.

Mecanismo de transferência de arquivos via FXP



Aqui está uma visão geral do processo:

1. O cliente abre uma conexão de controle com server1 na porta TCP 21.

O cliente envia o comando PASV para server1.

Server1 responde com seu endereço IP e a porta na qual escuta.

2. O cliente abre uma conexão de controle com o servidor2 na porta TCP 21.

O cliente passa o endereço/porta recebido do servidor1 para o servidor2 em um comando **PORT**.

O Servidor2 responde para informar ao cliente que o comando **PORT** foi bem-sucedido. O Servidor2 agora sabe para onde enviar os dados.

3. Para iniciar o processo de transmissão de server1 para server2:

O cliente envia o comando STOR ao servidor2 e o instrui a armazenar a data que recebe.

O cliente envia o comando RETR ao servidor1 e o instrui a recuperar ou transmitir o arquivo.

4. Todos os dados agora vão diretamente da origem para o servidor FTP de destino. Ambos os servidores relatam ao cliente apenas mensagens de status de falha/sucesso.

Éassim que a tabela de conexão aparece:

```
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
```

Inspeção FTP e FXP

A transferência de arquivos através do ASA via FXP é bem-sucedida somente quando a inspeção de FTP é **desabilitada** no ASA.

Quando o cliente FXP especifica um endereço IP e uma porta TCP diferentes dos do cliente no **comando PORT** FTP, uma situação insegura é criada quando um invasor é capaz de realizar uma verificação de porta em um host na Internet a partir de um servidor FTP de terceiros. Isso ocorre porque o servidor FTP é instruído a abrir uma conexão a uma porta em uma máquina que pode não ser o cliente que se origina. Isso é chamado de **ataque de devolução de FTP**, e a inspeção de FTP desliga a conexão porque considera isso uma violação de segurança.

Aqui está um exemplo:

```
%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
```

Configurar

Use as informações descritas nesta seção para configurar o FXP no ASA.

Note: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.



Configurar o ASA via CLI

Conclua estes passos para configurar o ASA:

1. Desativar inspeção de FTP:

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

 Configure as listas de acesso para permitir a comunicação entre o cliente FXP e os dois servidores 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. Aplique as listas de acesso nas respectivas interfaces:

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

Verificar

Use as informações descritas nesta seção para verificar se sua configuração funciona corretamente.

Processo de transferência de arquivos

Conclua estes passos para verificar a transferência de arquivos bem-sucedida entre os dois servidores FTP:

1. Conecte-se ao server1 a partir da máquina cliente FXP:



2. Conecte-se ao servidor2 a partir da máquina cliente FXP:

| G 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 |
| | 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 | 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: 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. Arraste e solte o arquivo a ser transferido da janela server1 para a janela 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 | ٠ | 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 | - | -8- 🔂 | 🗎 🖬 | × 🛛 🕯 🕨 | ▶ 😐 📲 |
| : /./ | | Ŧ | : 1.1 | | | |
| Name 🔺 | Size Date | ^ | Name | , | 🛆 📔 Size | e Date 🔺 |
| a desktop.ini | 282 b 06/03/2014 | | 鷆 FileZilla Servi | er | | 0 05/29/2014 11 |
| 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 | 4 06/12/2014 07 |
| ire-6u31-windows-i586-s.exe | 16.4 M 05/29/2014 | | Cores 2.zip | | 140.6 M | 4 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 | | E ftprush.exe | | 3.8 M | 4 05/08/2014 11 |
| openload.exe | 60.0 k 11/27/2013 | | Google Chron | me.lnk | 2.3 | k 09/06/2013 11 ≘ |
| ratelimit.pcapng | 280.4 M 09/04/2013 | Ε | ire-6u31-win | dows-i586-s.exe | 16.4 M | 4 06/10/2014 08 |
| server1.txt | 17 b 05/27/2014 | | monodeexce | eption.pcapng | 255.2 | k 05/29/2014 10 |
| iest.txt | 31b 05/17/2014 | | 📄 ratelimit.pca | png | 280.41 | 4 05/29/2014 11 |
| indows-tools.zip | 126.0 k 02/19/2014 | - | test txt | .txt | 311 | b 05/29/2014 08 |
| ۰ III. | + | | < 🗳 | III | | • |
| 1 file(s) 0 folder(s) 17 byte | | | 10 file(s) 4 folder | (s) 718.5 M byte(s | 5) | |

4. Verifique se a transferência do arquivo foi bem-sucedida:

| G FTP Rush ftp://10.1.1.10 - ftp://192. | 168.1.10 | | | | | |
|---|-------------------|-----|-----------------|--------------------|-----------------|--|
| Eile Edit Mark View FTP Tool | s <u>H</u> elp | | | | | |
| 🕴 📶 🔞 Do not use proxy 🔹 🛥 🔹 He | ost 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 |) | |
| | 🗙 🔁 💻 | • | -8- | 6 📬 🖬 | X 0 | |
| i /./ | | Ŧ | :/ | | | • |
| Name A | Size Date | | Name | | 6 | Size Date |
| 1 Parent Directory | | | 1. Parent D | irectory | | |
| 🗼 3cdaemon | 0 05/08/2014 | | 📕 3cdaemo | n | | 0 05/08/2014 11 |
| FileZilla Server | 0 05/06/2014 | - | Cores 1 | | | 0 06/12/2014 07 |
| 🍌 iperf | 0 09/04/2013 | = | Cores 2 | | | 0 06/12/2014 07 = |
| indows-tools | 0 02/19/2014 | | 📕 FileZila S | erver | | 0 05/29/2014 11 |
| ~DF38A940C0895452B0.TMP | 0 b 05/08/2014 | | Cisco ASI | DM-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 | | Cores 1.: | zip | 27 | 7.0 M 06/12/2014 07 |
| Cisco ASDM-IDM Launcher.lnk | 2.3 k 05/29/2014 | | Cores 2.: | zip | 14 | 0.6 M 06/12/2014 08 |
| desktop.ini | 282 b 06/03/2014 | | desktop. | ini | | 282 b 06/03/2014 09 |
| ftprush.exe | 3.8 M 05/06/2014 | | Ftprush.e | exe | | 3.8 M 05/08/2014 11 |
| Google Chrome.Ink | 2.3 k 09/06/2013 | | Google C | hrome.Ink | | 2.3 k 09/06/2013 11 |
| ire-6u31-windows-i586-s eve | 16 4 M 05/29/2014 | - | ire-fui31 | -windows-i586-s ev | e 1 | 6.4M 06/10/2014 08 |
| 14 fla(a) 4 falder(a) 207 (| M huta(a) | | • | 11 flo(s) 4 fels | lor(c) 710 EM h | to(a) |
| | mbyte(s) | | II me(s) + roid | ler(s) / 16.5 M D | yte(s) | |
| [2] List Complete: 1,064 b | ytes in 0.22 se | COL | ids (4.86 | KB/s) | | |
| FTP Log 🔯 Transfer Log 🔁 Syst | em Log Log Tasks | | | | | |
| Name Progress Speed | Transferred | | Size | Source path | Target path | Remark |
| | | | | | | |
| | | | | Ran | Width (UL/DL) | 0.00/0.00 Kbos |
| | | - | | Dank | annau (ochoc). | algebrage in the state of the s |

Troubleshoot

Esta seção fornece capturas de dois cenários diferentes que você pode usar para solucionar problemas de sua configuração.

Cenário de inspeção de FTP desativado

Quando a inspeção de FTP é desabilitada, conforme detalhado na seção <u>Inspeção de FTP e FXP</u> deste documento, esses dados aparecem na interface do cliente 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 | 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] Seg=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. |

Aqui estão algumas observações sobre estes dados:

- O endereço IP do cliente é 172.16.1.10.
- O endereço IP do Server1 é 10.1.1.10.
- O endereço IP do Server2 é 192.168.1.10.

Neste exemplo, o arquivo Kiwi_Syslogd.exe é transferido do servidor1 para o servidor2.

Inspeção de FTP habilitada

Quando a inspeção de FTP está habilitada, esses dados aparecem na interface do cliente ASA:

| 2005-12-12 | 03:08:15.758902 | 172.15.1.10 | 10.1.1.10 | ETP | 60 Request: PASM |
|----------------|-----------------|-------------|--------------|-----|--|
| 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: PORT 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 | 192.18B.1.10 | ETP | 77 [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2005 - 12 - 12 | 03:08:20.120575 | 172.16.1.10 | 192.158.1.10 | FTP | 77 [TCP Retransmission] Request: PCRT 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: PORT 10,1,1,10,192,99 |
| 2008-12-12 | 03:08:23.761328 | 172.18.1.10 | 192.18B.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 [TCF Retransmission] Request: PCRT 10,1.1,10.192.39 |

Aqui estão as capturas de queda do ASA:

| 2000-12-12 03:08:17.073818 | | | | <pre>r/ [tcP Acked unseen segment] Request; PORT 10,1,1,10,192,99</pre> |
|---------------------------------|--------------|-----------------|---|--|
| 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 03:00:17.603176 | 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 | 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 | PTP | 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 03:08:21.276780 | 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 03:08:21.339475 | 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 | FTP | 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. |
| 2006-12-12-03:08:28.573960 | 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] Seq=21 Ack=1 Win=0 Len=0 |
| 1000 12 12 00 00 00 10 10 10 10 | 172 16 1 10 | 1002 1002 1 100 | and the second se | A DIT ACKed uppear command \$0500 - Eta DIST ACCI Sec. 1900/04514 Adv. 7210/5500 Min. A Lan. O |

A solicitação **PORT** é liberada pela inspeção FTP porque contém um endereço IP e uma porta diferentes do endereço IP e da porta do cliente. Subsequentemente, a conexão de controle com o servidor é encerrada pela inspeção.