Transferência de arquivo ASA com exemplo de configuração FXP

Índice

Introdução

Este documento descreve como configurar o protocolo de intercâmbio do arquivo (FXP) na ferramenta de segurança adaptável de Cisco (ASA) através do CLI.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico do File Transfer Protocol (FTP) (modos ativo/passivo).

Componentes Utilizados

A informação neste documento é baseada em Cisco ASA que executa as versões de software 8.0 e mais atrasado.

Nota: Este exemplo de configuração usa duas estações de trabalho de Microsoft Windows que atuam como server FXP e serviços de FTP da corrida (demônio 3C). Igualmente têm FXP permitido. Uma outra estação de trabalho de Microsoft Windows que execute o software do cliente FXP (precipitação FTP) é usada igualmente.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O FXP permite que você transfira arquivos de um servidor FTP a um outro servidor FTP através de um cliente FXP sem a necessidade de depender da velocidade de conexão com o Internet do cliente. Com FXP, a velocidade máxima de transferência depende somente da conexão entre os dois server, que é geralmente muito mais rápida do que a conexão de cliente. Você pode aplicar FXP nas encenações onde um server da largura de banda elevada exige recursos de um outro server da largura de banda elevada, mas somente um cliente da largura de banda baixa tal como um administrador de rede que trabalhe remotamente tem a autoridade para alcançar os recursos em ambos os server.

O FXP trabalha como uma extensão do protocolo de FTP, e o mecanismo é indicado na seção 5.2 do RFC 959 FTP. Basicamente, o cliente FXP inicia uma conexão de controle com um servidor1 FTP, abre uma outra conexão de controle com servidor2 FTP, a seguir altera os atributos de conexão dos server de modo que apontem entre si tais que transferência ocorre diretamente entre os dois server.

Mecanismo de transferência de arquivo através de FXP

Está aqui uma vista geral do processo:

1. O cliente abre uma conexão de controle com o servidor1 na porta TCP 21.

   O cliente envia o **comando pasv ao** servidor1.

   O servidor1 responde com seu endereço IP de Um ou Mais Servidores Cisco ICM NT e a porta em que escuta.

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

   O cliente passa a /porta do endereço que é recebida do servidor1 ao servidor2 em um **comando port**.

   O servidor2 responde a fim informar o cliente que o **comando port** é bem sucedido. O servidor2 sabe agora onde enviar os dados.

3. A fim começar o processo da transmissão do servidor1 ao servidor2:

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

O cliente envia o **comando RETR ao** servidor1 e instrui-o para recuperar ou transmitir o arquivo.

4. Todos os dados vão agora diretamente da fonte ao servidor FTP de destino. Ambos os server relatam somente mensagens de status na falha/sucesso ao cliente.

Isto é como 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

Transferência de arquivo com o ASA através de FXP é bem sucedida somente quando a inspeção FTP **é desabilitada no** ASA.

Quando o cliente FXP especifica um endereço IP de Um ou Mais Servidores Cisco ICM NT e uma porta TCP que difiram daqueles do cliente no **comando port** FTP, uma situação incerta é criada onde um atacante pode realizar uma varredura da porta contra um host no Internet de um servidor FTP da terceira. Isto é porque o servidor FTP é instruído para abrir uma conexão a uma porta em uma máquina que não possa ser o cliente que origina. Isto é chamado um **ataque do salto FTP**, e a inspeção FTP fechou a conexão porque considera esta 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 a informação que é descrita nesta seção a fim configurar FXP no ASA.

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

Diagrama de Rede

Configurar o ASA através do CLI

Termine estas etapas a fim configurar o ASA:

1. Desabilite a inspeção FTP:
```
FXP-ASA(config)# policy-map global_policy
FXP-ASA(config-pmap)#  class inspection_default
FXP-ASA(config-pmap-c)# no inspect ftp
```
2. Configurar Listas de acesso a fim permitir uma 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 interfaces respectivas:
```
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 a informação que é descrita nesta seção a fim verificar que sua configuração trabalha corretamente.

Processo de transferência de arquivo

Termine estas etapas a fim verificar transferência de arquivo bem sucedida entre os dois servidores FTP:

1. Conecte ao servidor1 da máquina cliente FXP:

2. Conecte ao servidor2 da máquina cliente FXP:

3. Arraste e deixe cair o arquivo a ser transferido do indicador do servidor1 ao indicador do servidor2:

4. Verifique que transferência de arquivo é bem sucedida:

Troubleshooting

Esta seção fornece captações de duas encenações diferentes que você pode usar a fim pesquisar defeitos sua configuração.

Encenação desabilitada inspeção FTP

Quando a inspeção FTP é desabilitada, como detalhado na inspeção FTP e na seção FXP deste documento, estes dados aparecem na interface de cliente ASA:

Estão aqui algumas notas sobre estes dados:

- O endereço IP cliente é **172.16.1.10**.
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor1 é **10.1.1.10**.
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor2 é **192.168.1.10**.

Neste exemplo, o arquivo nomeado **Kiwi_Syslogd.exe** é transferido do servidor1 ao servidor2.

Inspeção FTP permitida

Quando a inspeção FTP é permitida, estes dados aparecem na interface de cliente ASA:

Estão aqui as captações da gota ASA:

O pedido da **PORTA** é deixado cair pela inspeção FTP porque contém um endereço IP de Um ou Mais Servidores Cisco ICM NT e uma porta que difiram do endereço IP cliente e da porta. Subseqüentemente, a conexão de controle ao server é terminada pela inspeção.