Exemplo de configuração de transferência de arquivo ASA com FXP

Contents

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.

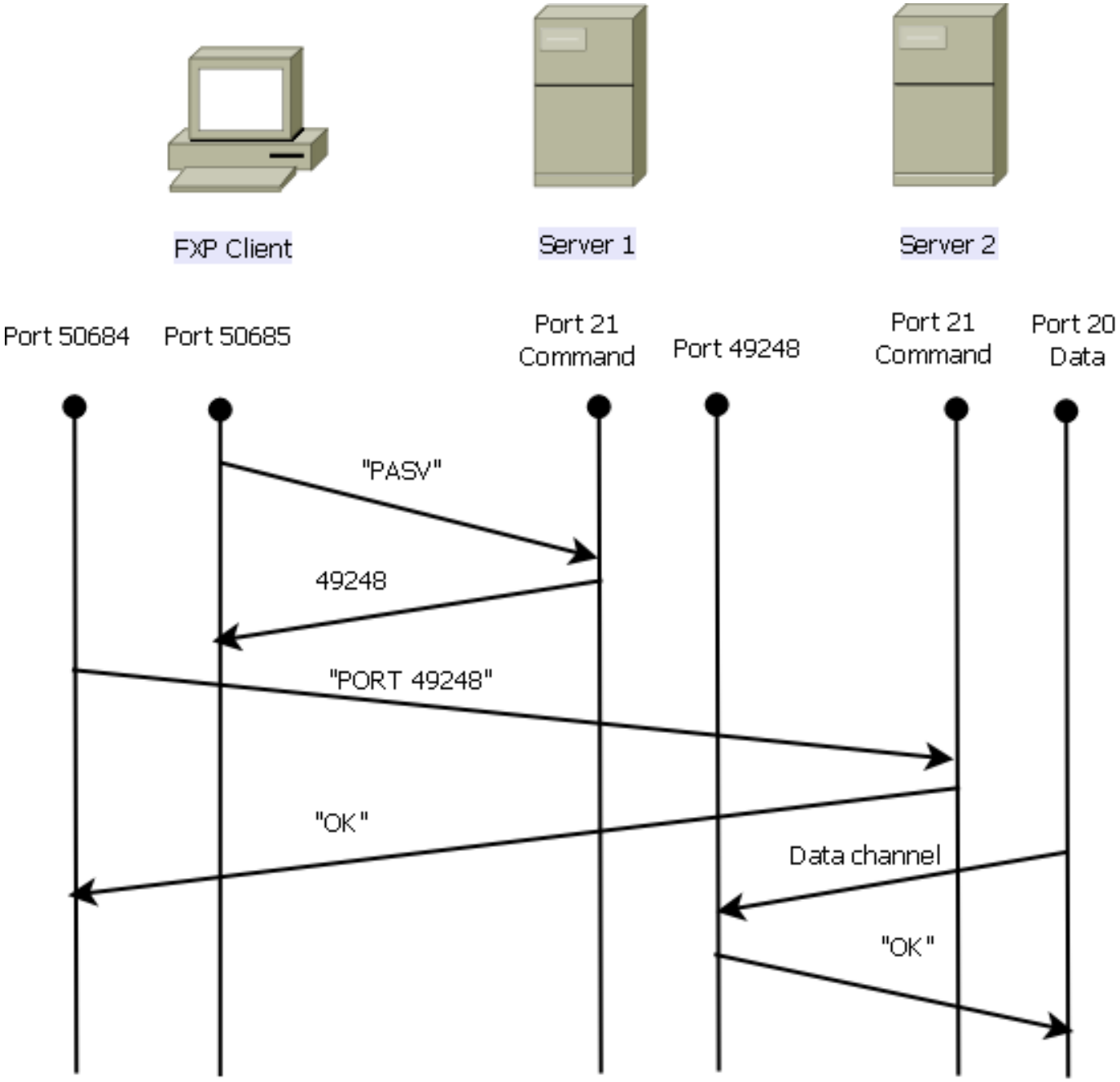
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

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:

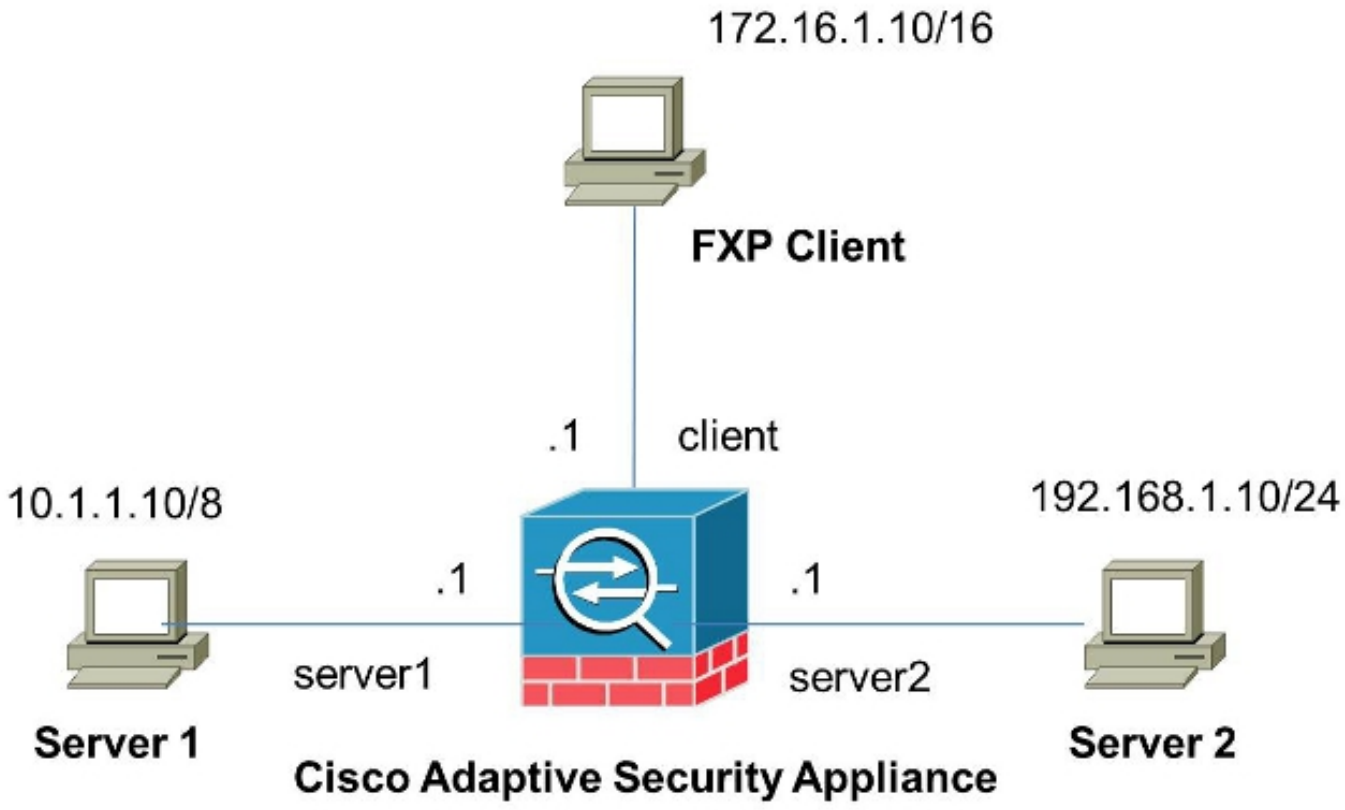
```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: 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.

Diagrama de Rede



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
```

2. 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
```

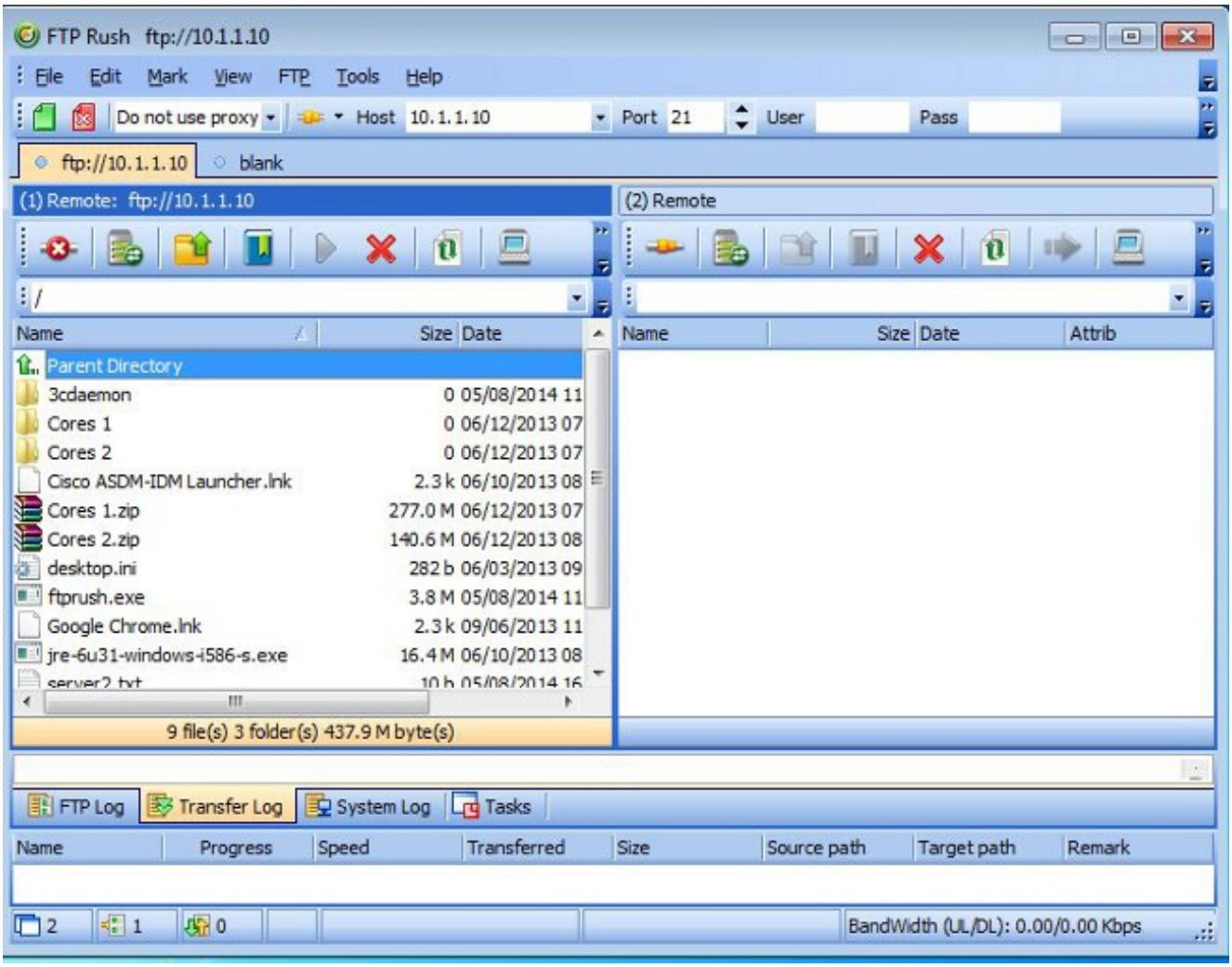
Verificar

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

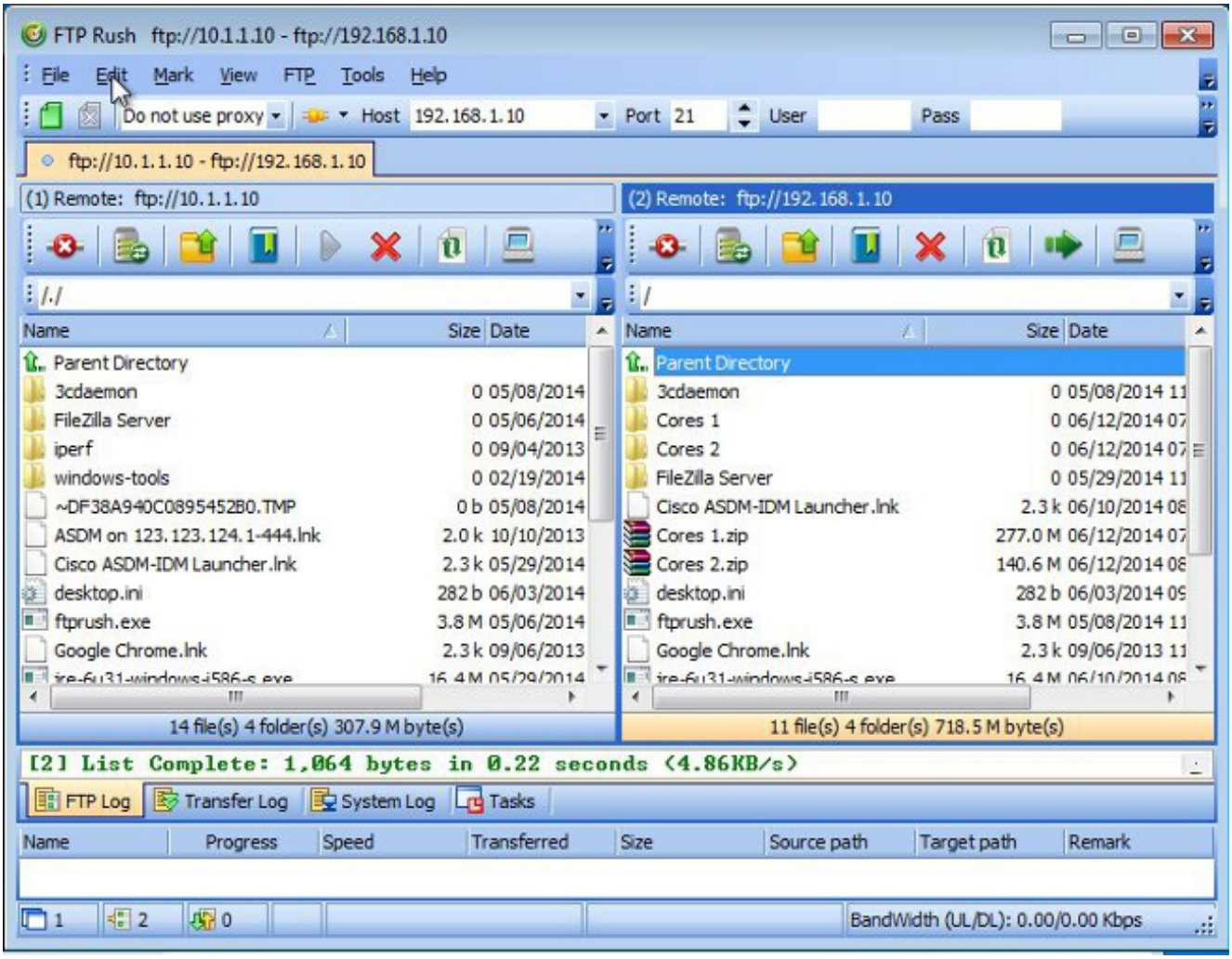
Processo de transferência de arquivos

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

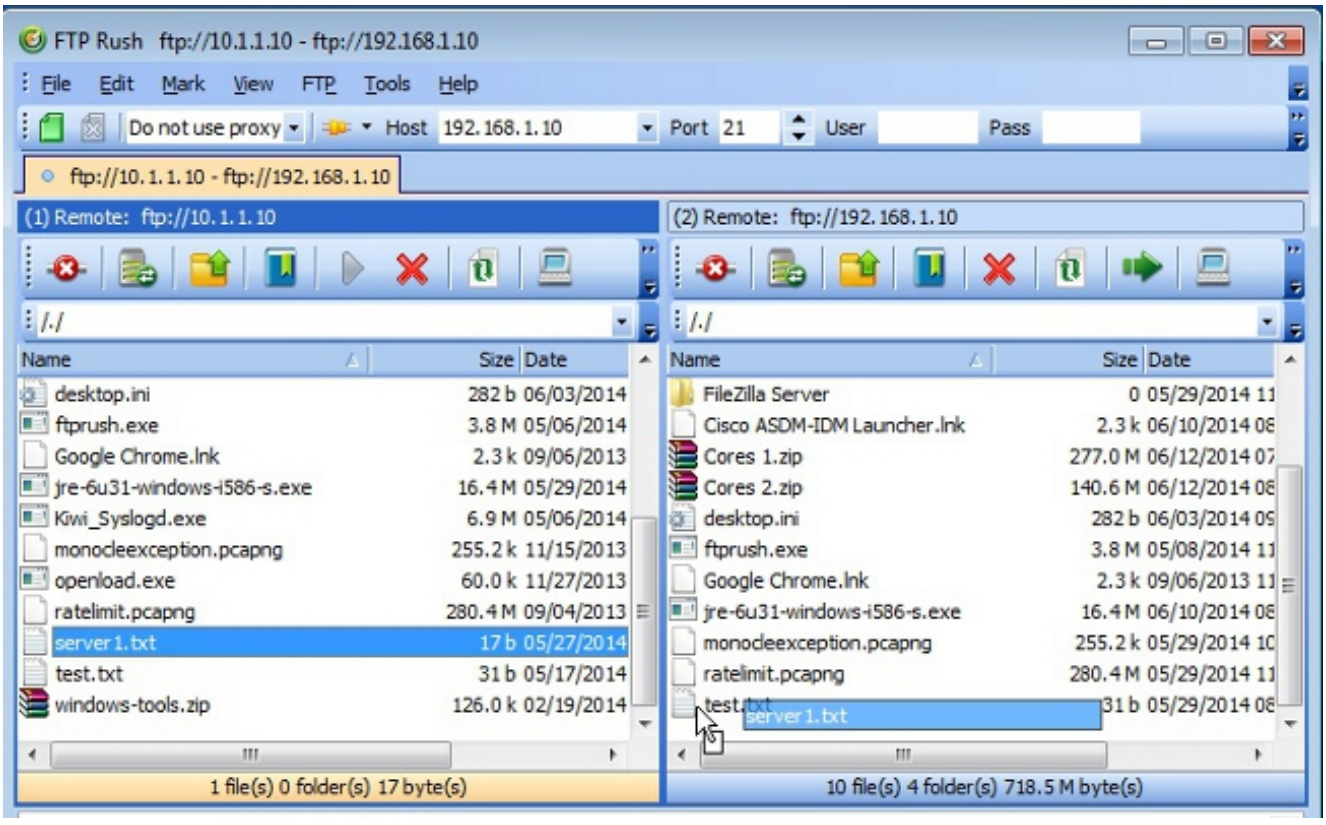
1. Conecte-se ao server1 a partir da máquina cliente FXP:



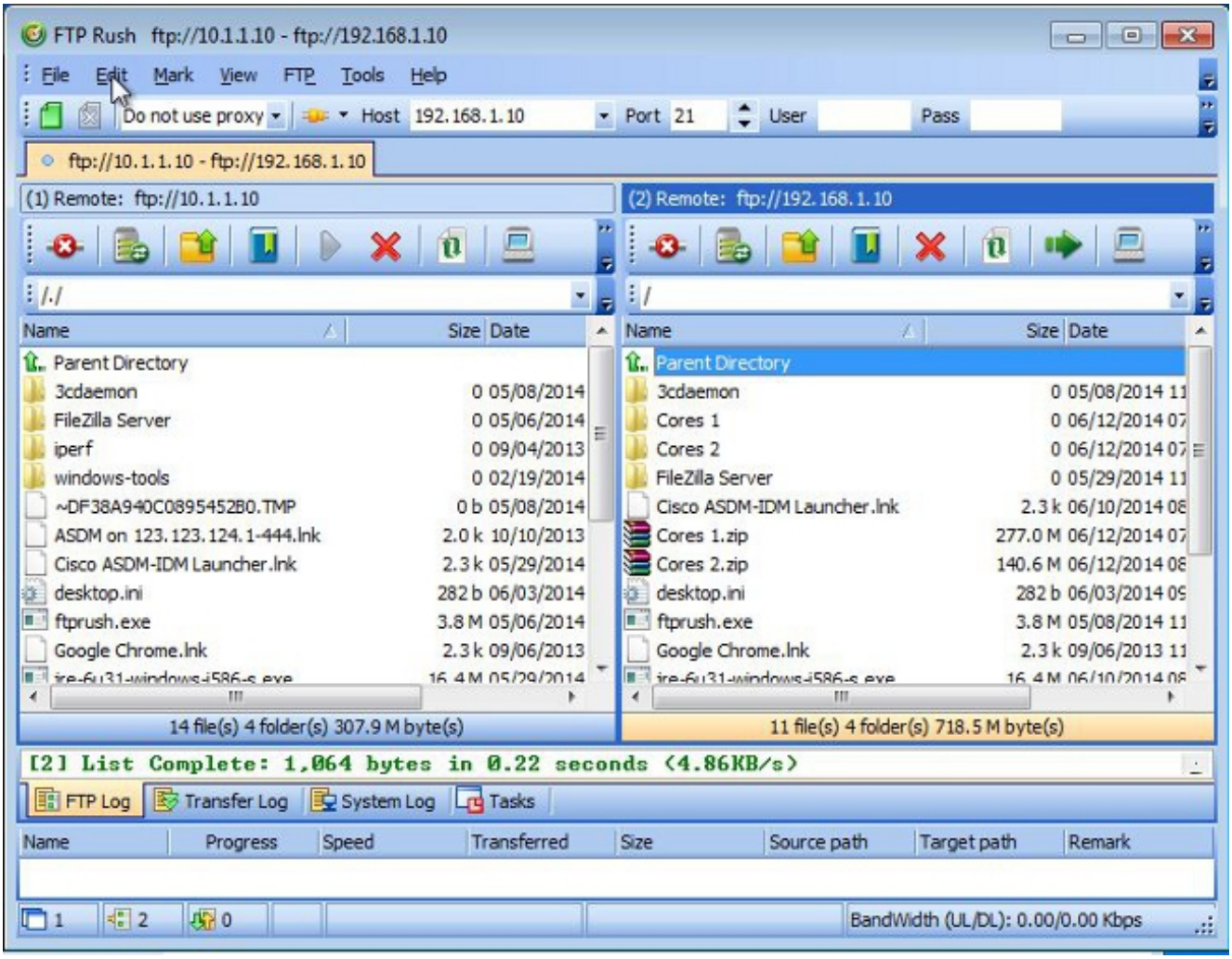
2. Conecte-se ao servidor2 a partir da máquina cliente FXP:



3. Arraste e solte o arquivo a ser transferido da janela server1 para a janela server2:



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



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 Inspeção de FTP e FXP 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    FTP     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] Seq=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] 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.
```

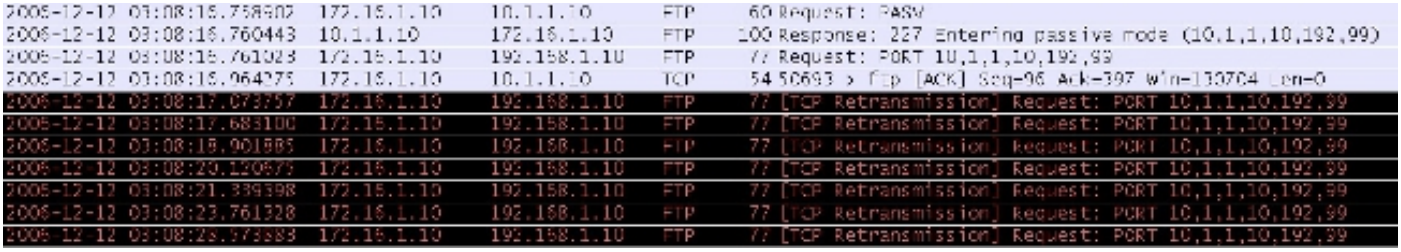
Aqui estão algumas observações sobre estes dados:

- 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**.

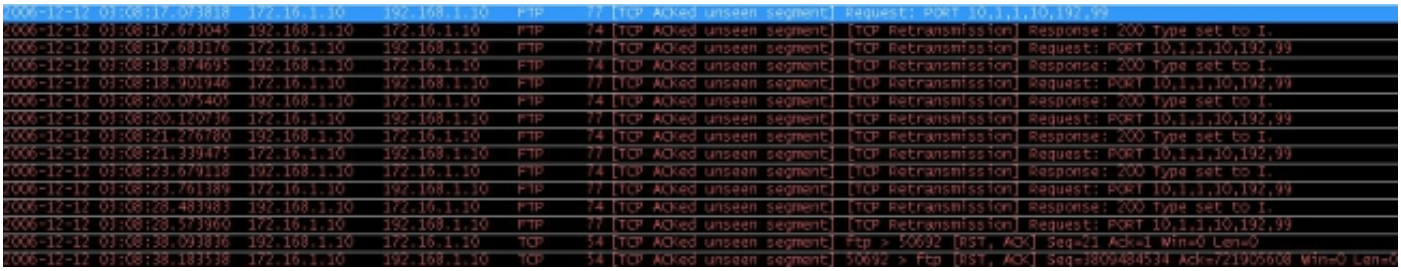
Neste exemplo, o arquivo **Kiwi_Syslogd.exe** é transferido do servidor1 para o servidor2.

Inspeção de FTP habilitada

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



Aqui estão as capturas de queda do ASA:



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.