ASA File Transfer with FXP Configuration Example

Contents

Introduction

This document describes how to configure File eXchange Protocol (FXP) on the Cisco Adaptive Security Appliance (ASA) via the CLI.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of File Transfer Protocol (FTP) (Active/Passive modes).

Components Used

The information in this document is based on the Cisco ASA that runs software Versions 8.0 and later.

Note: This configuration example uses two Microsoft Windows workstations that act as FXP servers and run FTP services (3C Daemon). They also have FXP enabled. Another Microsoft Windows workstation that runs FXP client software (FTP Rush) is also used.

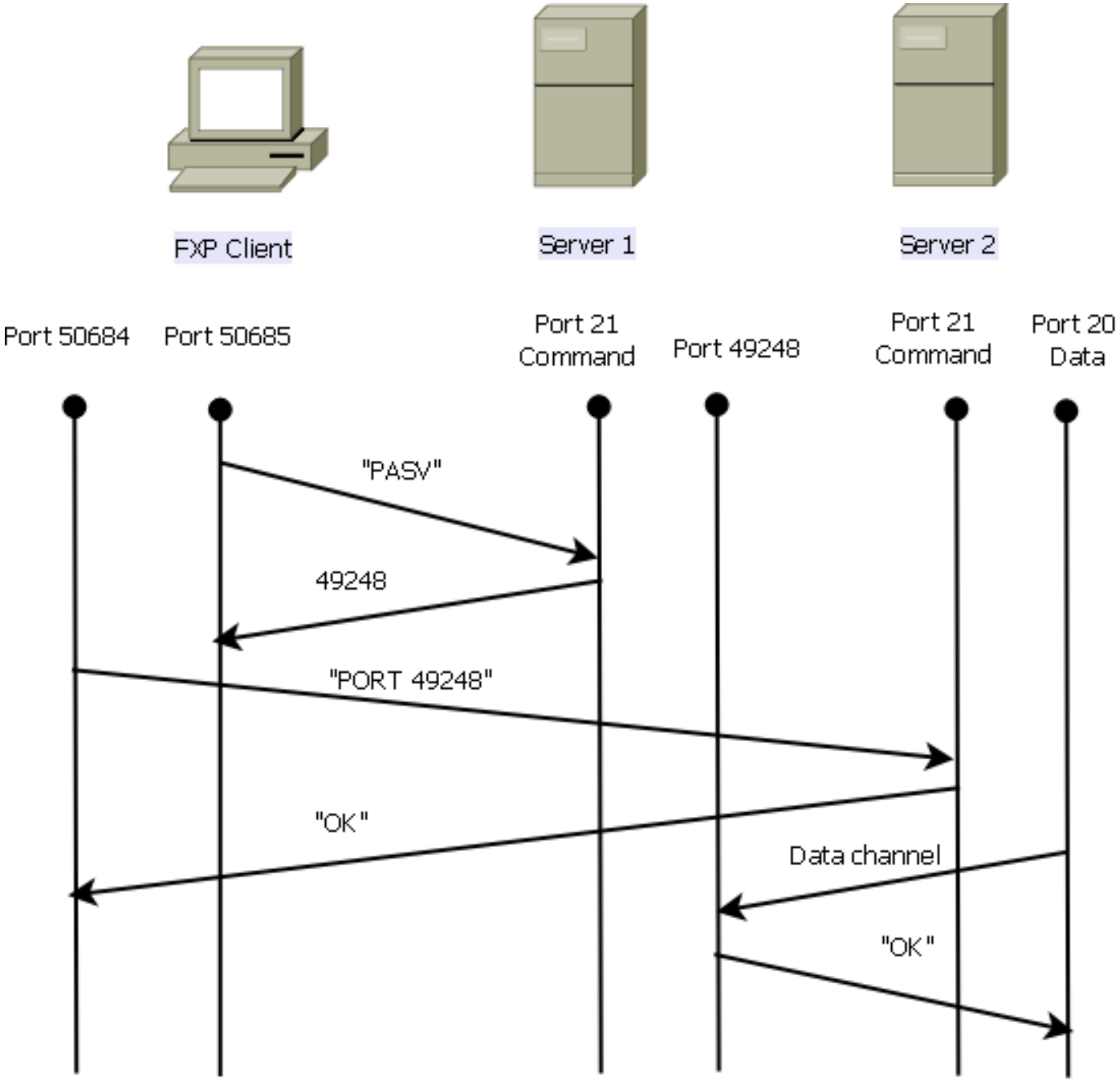
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

The FXP allows you to transfer files from one FTP server to another FTP server via an FXP client without the need to depend on the client internet connection speed. With FXP, the maximum transfer speed depends only on the connection between the two servers, which is usually much faster than the client connection. You can apply FXP in scenarios where a high-bandwidth server demands resources from another high-bandwidth server, but only a low-bandwidth client such as a network administrator that works remotely has the authority to access the resources on both servers.

The FXP works as an extension of the FTP protocol, and the mechanism is stated in section 5.2 of the FTP RFC 959. Basically, the FXP client initiates a control connection with an FTP server1, opens another control connection with FTP server2, then modifies the connection attributes of the servers so that they point to each other such that the transfer takes place directly between the two servers.

Mechanism of File Transfer Via FXP



Here is an overview of the process:

1. The client opens a control connection with server1 on TCP port 21.

   The client sends the **PASV** command to server1.

   Server1 responds with its IP address and the port on which it listens.

2. The client opens a control connection with server2 on TCP port 21.

   The client passes the address/port that is received from server1 to server2 in a **PORT** command.

   Server2 responds in order to inform the client that the **PORT** command is successful. Server2 now knows where to send the data.

3. In order to begin the transmission process from server1 to server2:

   The client sends the **STOR** command to server2 and instructs it to store the date that it receives.

   The client sends the **RETR** command to server1 and instructs it to retrieve or transmit the file.

4. All of the data now goes directly from the source to the destination FTP server. Both servers only report status messages on fail/success to the client.

This is how the connection table appears:

```
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 Inspection and FXP

File transfer through ASA via FXP is successful only when FTP inspection is **disabled** on the ASA.

When the FXP client specifies an IP address and TCP port that differ from those of the client in the FTP **PORT** command, an insecure situation is created where an attacker is able to carry out a port scan against a host on the Internet from a third-party FTP server. This is because the FTP server is instructed to open a connection to a port on a machine that might not be the client that originates. This is called an **FTP bounce attack**, and the FTP inspection shuts down the connection because it considers this a security violation.

Here is an example:

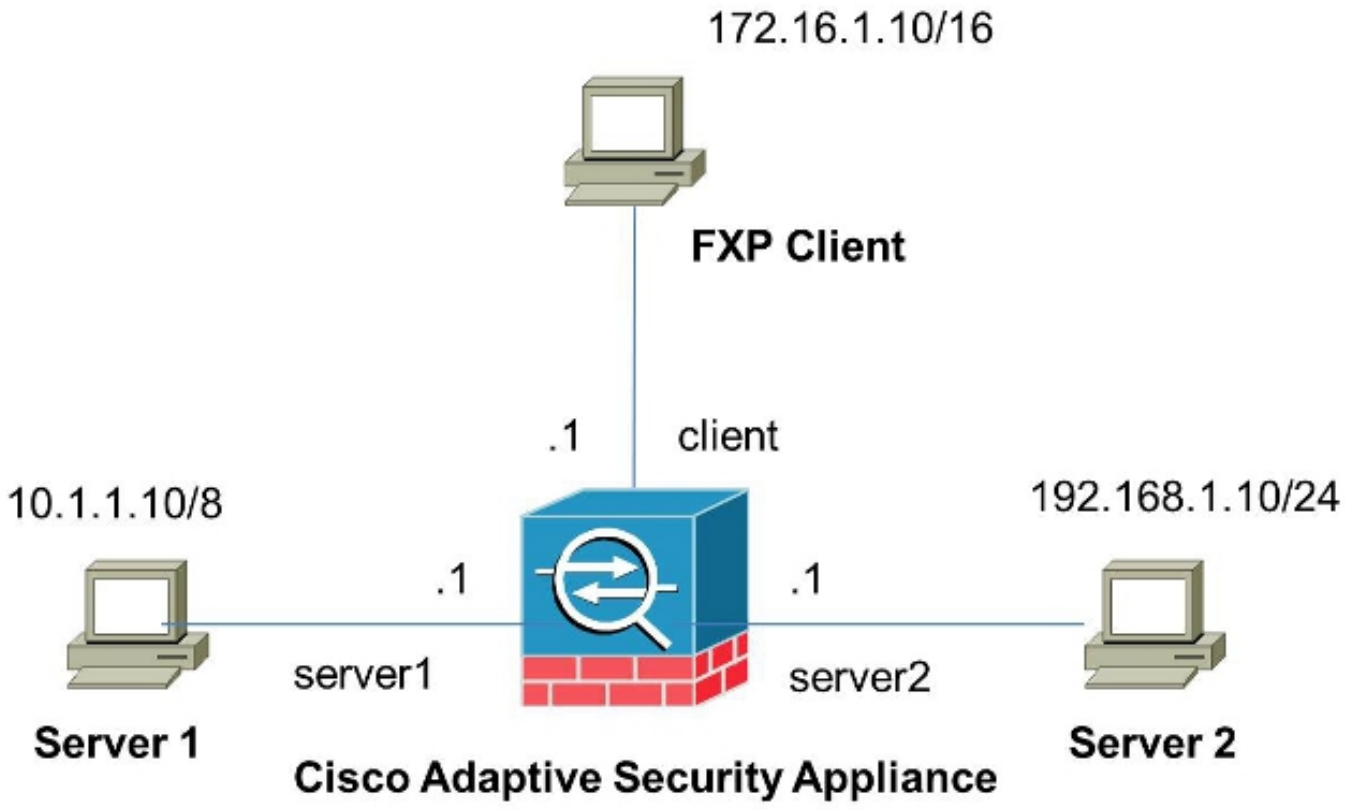
```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: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

Configure

Use the information that is described in this section in order to configure FXP on the ASA.

> **Note**: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram



Configure the ASA Via CLI

Complete these steps in order to configure the ASA:

1. Disable FTP inspection:
```
FXP-ASA(config)# policy-map global_policy
FXP-ASA(config-pmap)#  class inspection_default
FXP-ASA(config-pmap-c)# no inspect ftp
```
2. Configure access lists in order to allow communication between the FXP client and the two FTP servers:
```
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. Apply the access lists on the respective 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
```

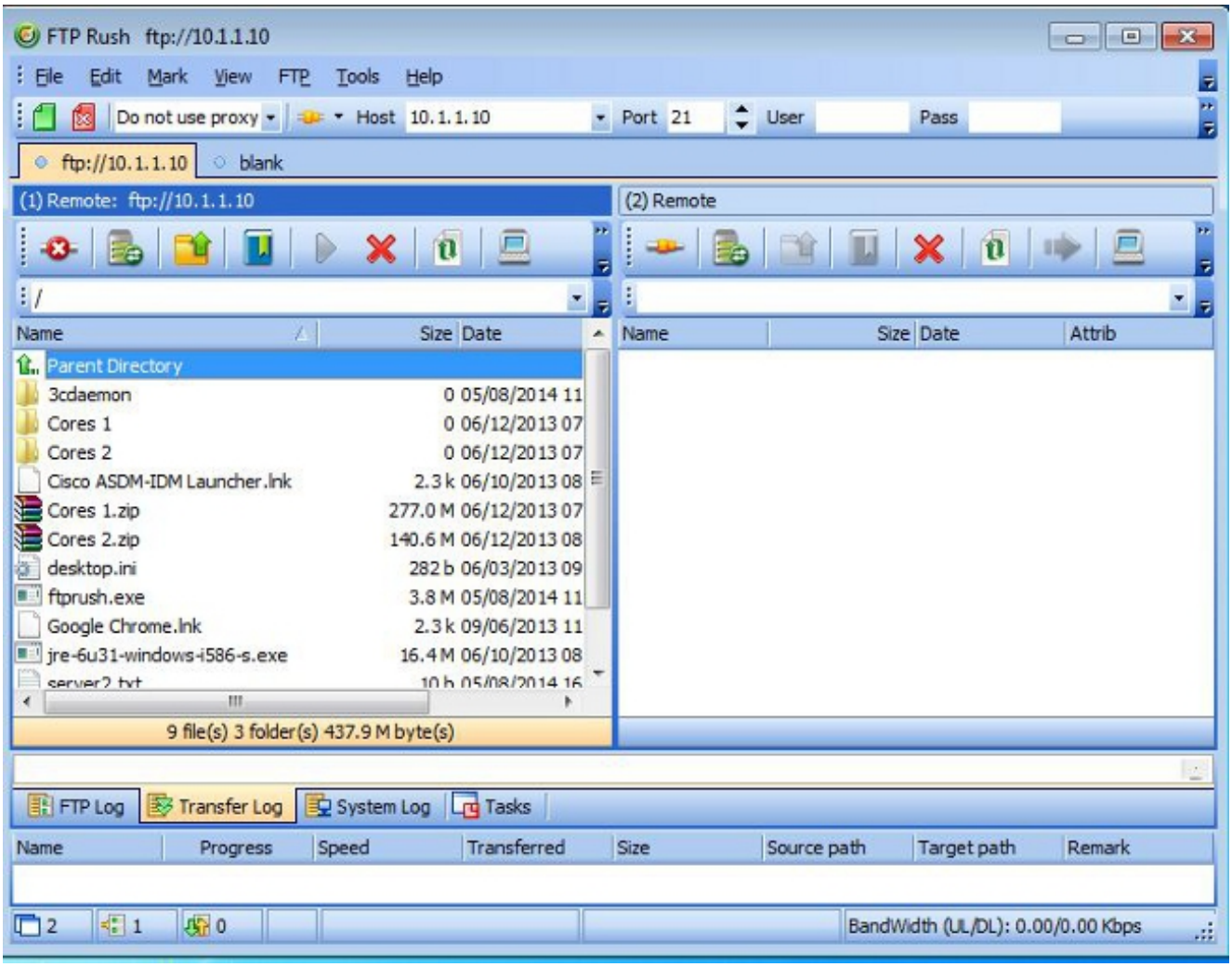
Verify

Use the information that is described in this section in order to verify that your configuration works properly.

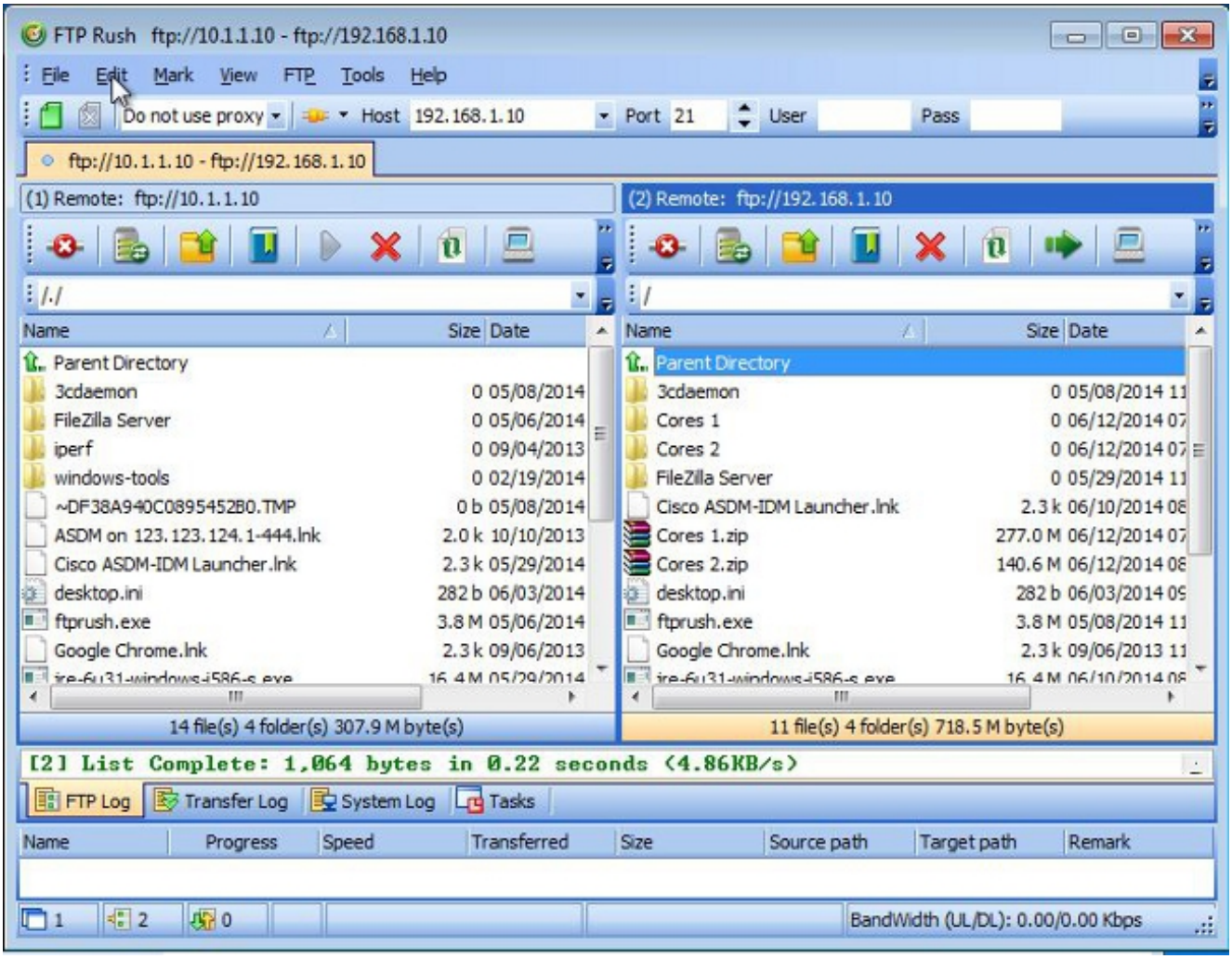
File Transfer Process

Complete these steps in order to verify successful file transfer between the two FTP servers:

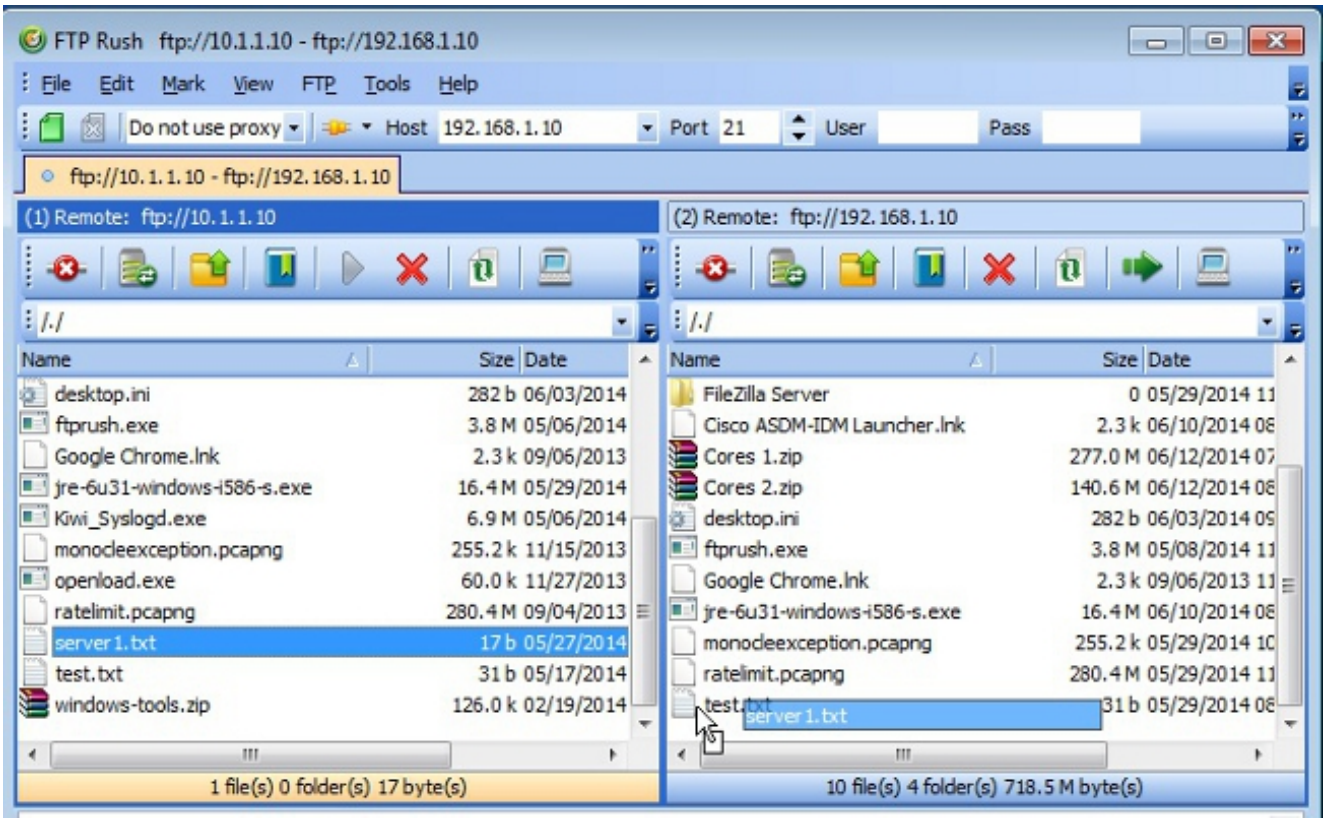
1. Connect to server1 from the FXP client machine:



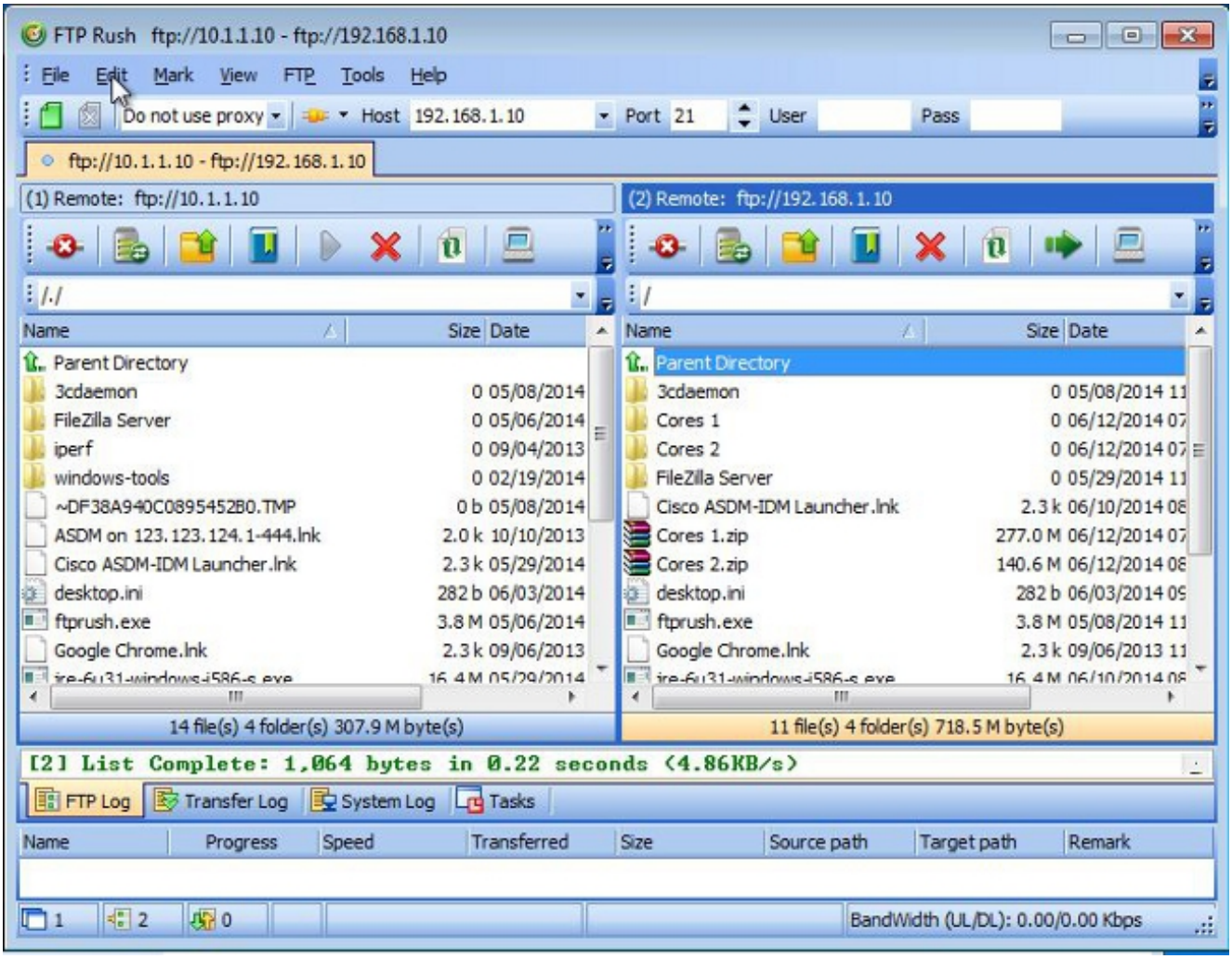
2. Connect to server2 from the FXP client machine:



3. Drag and drop the file to be transferred from the server1 window to the server2 window:



4. Verify that the file transfer is successful:



Troubleshoot

This section provides captures of two different scenarios that you can use in order to troubleshoot your configuration.

FTP Inspection Disabled Scenario

When FTP inspection is disabled, as detailed in the FTP Inspection and FXP section of this document, this data appears on the ASA client interface:

```
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.
```

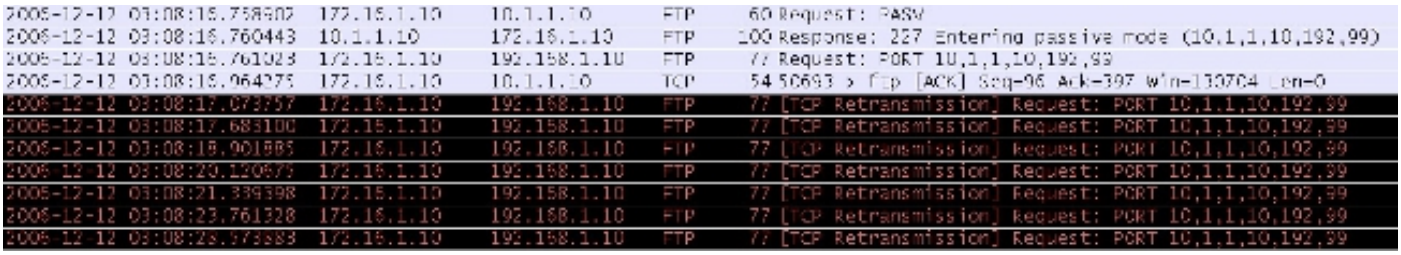
Here are some notes about this data:

- The client IP address is **172.16.1.10**.
- The Server1 IP address is **10.1.1.10**.
- The Server2 IP address is **192.168.1.10**.

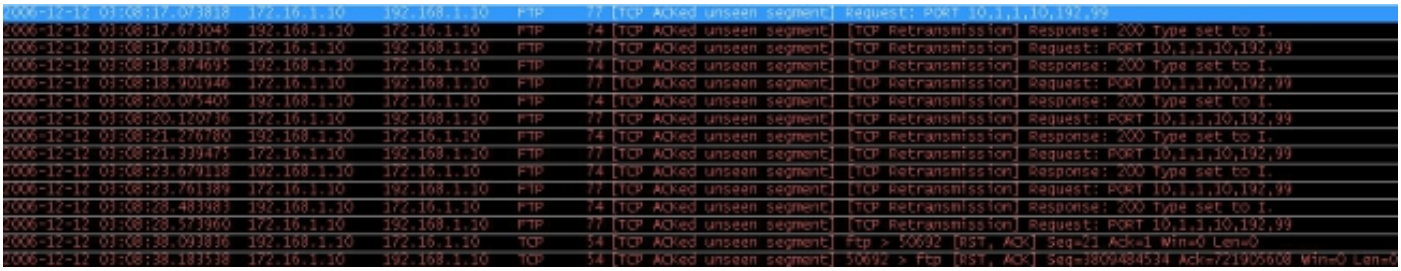
In this example, the file named **Kiwi_Syslogd.exe** is transferred from server1 to server2.

FTP Inspection Enabled

When FTP inspection is enabled, this data appears on the ASA client interface:



Here are the ASA drop captures:



The **PORT** request is dropped by the FTP inspection because it contains an IP address and port that differ from the client IP address and port. Subsequently, the control connection to the server is terminated by the inspection.