使用FXP的ASA文件传输配置示例

目录

简介

本文档介绍如何通过CLI在思科自适应安全设备(ASA)上配置文件交换协议(FXP)。

先决条件

要求

思科建议您对文件传输协议(FTP)（主用/被动模式）有基本的了解。

使用的组件

本文档中的信息基于运行软件版本8.0及更高版本的Cisco ASA。

> **注意**：此配置示例使用两台Microsoft Windows工作站，它们充当FXP服务器并运行FTP服务（3C守护程序）。 他们还启用了FXP。还使用另一台运行FXP客户端软件(FTP Rush)的Microsoft Windows工作站。

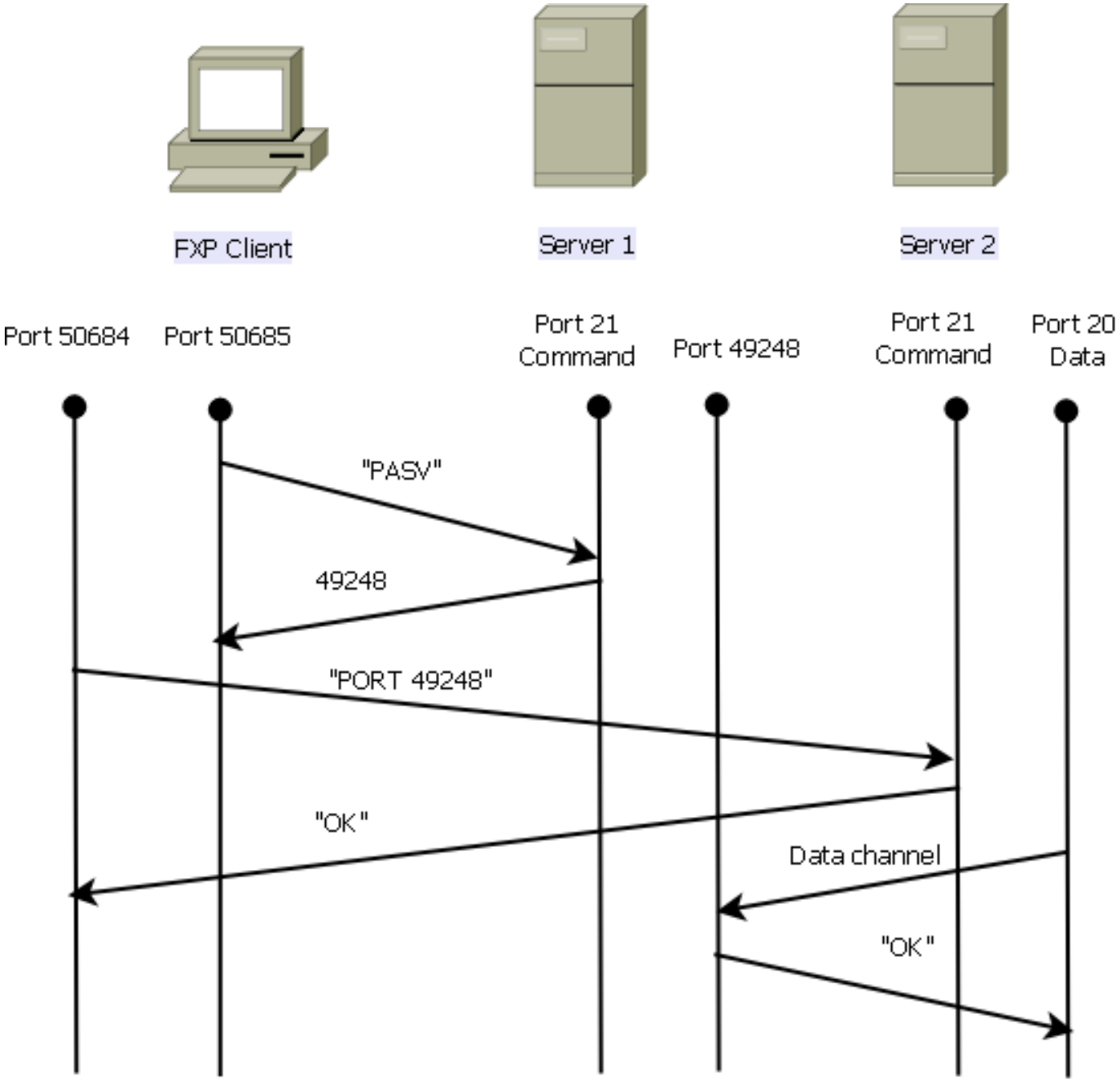
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

FXP允许您通过FXP客户端将文件从一个FTP服务器传输到另一个FTP服务器，而无需依赖客户端互联网连接速度。使用FXP时，最大传输速度仅取决于两台服务器之间的连接，这通常比客户端连接快得多。在高带宽服务器需要来自另一个高带宽服务器的资源的情况下，您可以应用FXP，但只有低带宽客户端（如远程工作的网络管理员）有权访问两台服务器上的资源。

FXP作为FTP协议的扩展，该机制在FTP RFC 959的5.2节中说明。基本上，FXP客户端发起与FTP服务器1的控制连接，打开与FTP服务器2的另一控制连接，然后修改服务器的连接属性，使其指向彼此，使传输直接在两台服务器之间进行。

FXP文件传输机制



以下是流程概述：

1. 客户端在TCP端口21上打开与server1的控制连接。

   客户端将PASV**命令**发送到server1。

   Server1以其IP地址和其侦听的端口作出响应。

2. 客户端在TCP端口21上打开与server2的控制连接。

   客户端使用PORT命令将从server1收到的地址/端口传递到**server2**。

   Server2响应以通知客户端PORT命**令**成功。Server2现在知道将数据发送到何处。

3. 要开始从server1到server2的传输过程，请执行以下操作：

客户端将STOR命令发送到server2，并指示它存储收到的日期。

客户端向server1发送RETR命令，并指示其检索或传输文件。

4. 所有数据现在都直接从源FTP服务器传输到目的FTP服务器。两台服务器只向客户端报告失败/成功时的状态消息。

连接表的显示方式如下：

```
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检测和FXP

仅当在ASA上禁用FTP检测时，通过FXP通过ASA的文件传输才成功。

当FXP客户端指定的IP地址和TCP端口与FTP PORT命令中的客户端不同时，会出现不安全的情况，即攻击者能够从第三方FTP服务器对Internet上的主机执行端口扫描。这是因为FTP服务器被指示打开与可能不是发起客户端的计算机上的端口的连接。这称为FTP退回攻击，而FTP检测会关闭连接，因为它认为这是安全违规。

示例如下：

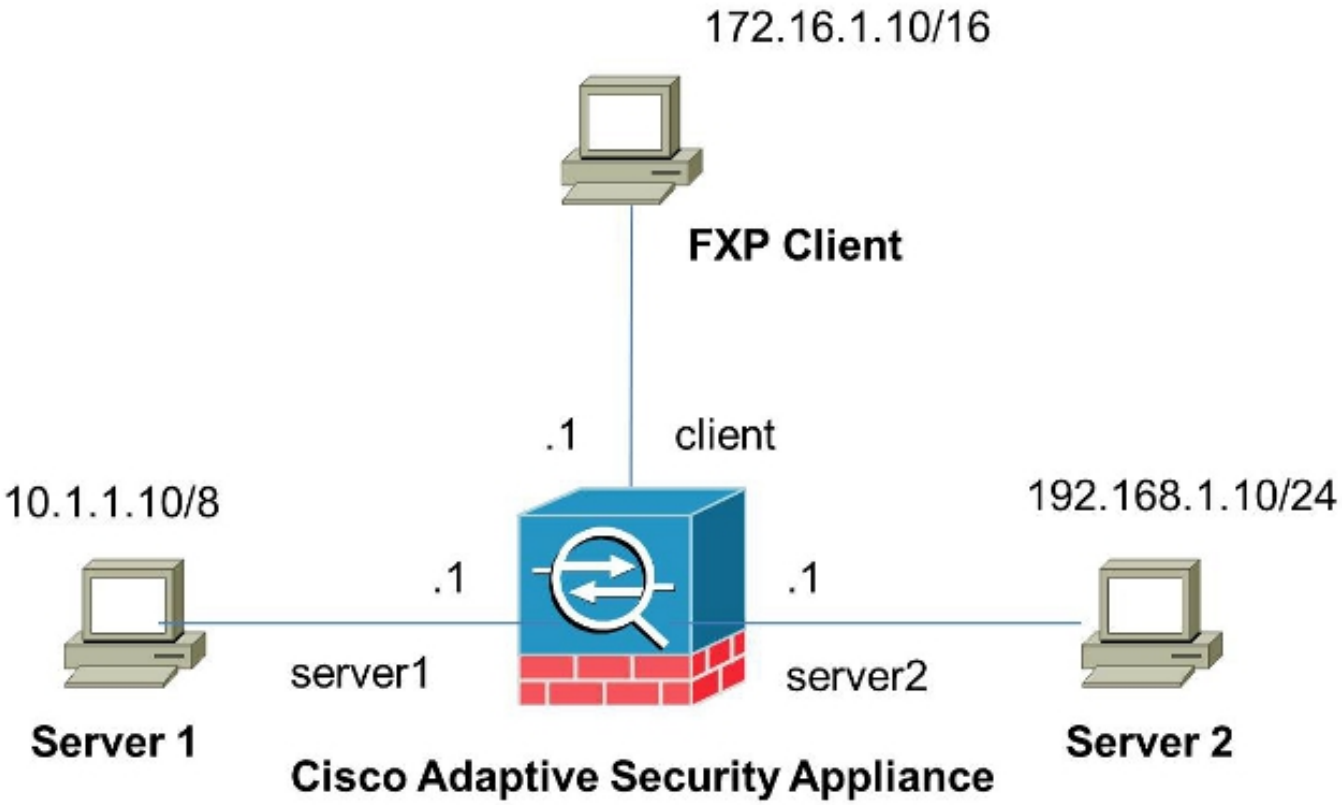
```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: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

配置

使用本节中介绍的信息在ASA上配置FXP。

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图



通过 CLI 配置 ASA

要配置ASA，请完成以下步骤：

1. 禁用FTP检测：

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

2. 配置访问列表以允许FXP客户端和两台FTP服务器之间的通信：

```
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. 将访问列表应用于各个接口：

```
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
```

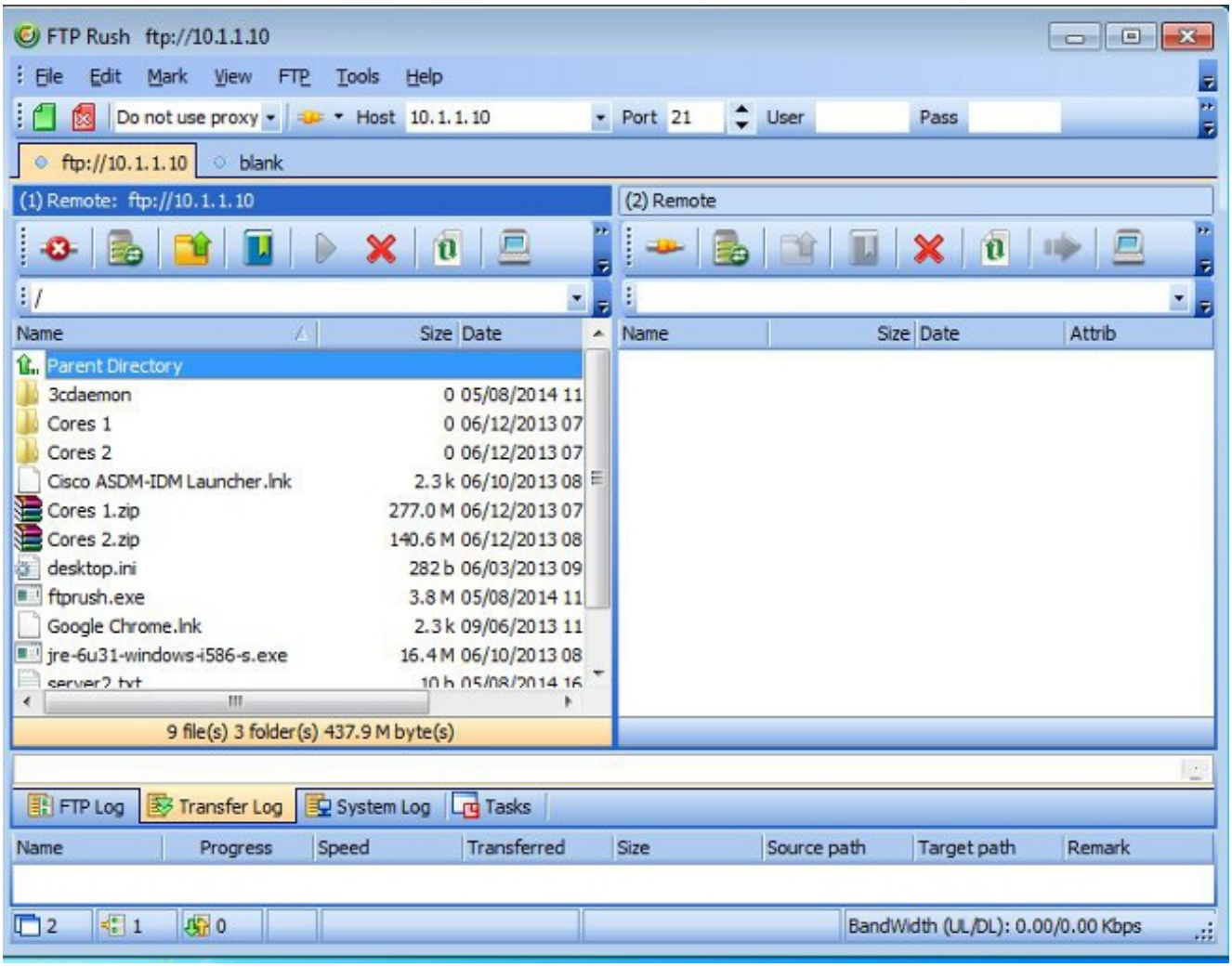
验证

使用本节中介绍的信息验证配置是否正常工作。

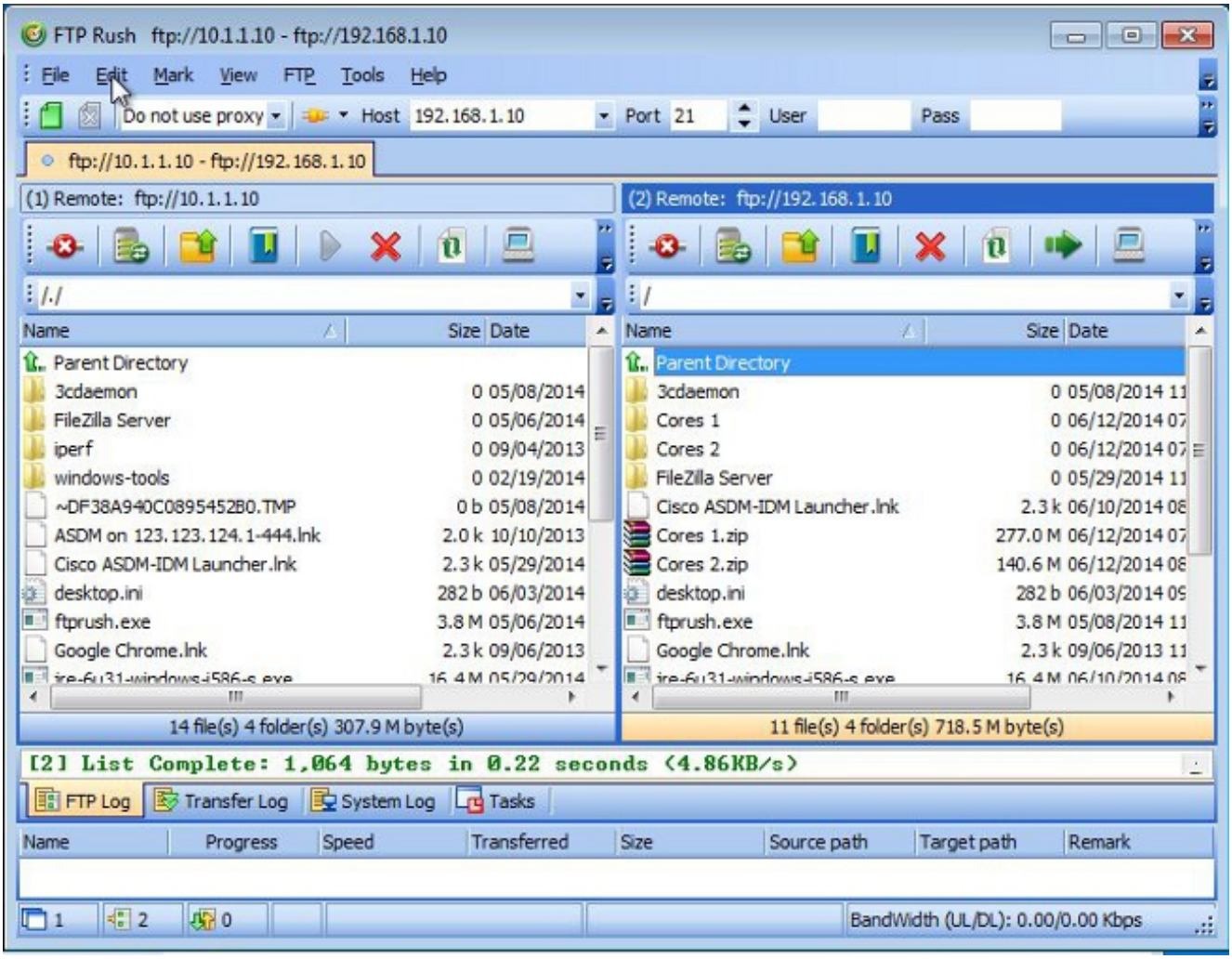
文件传输过程

完成以下步骤，以验证两台FTP服务器之间是否成功传输文件：

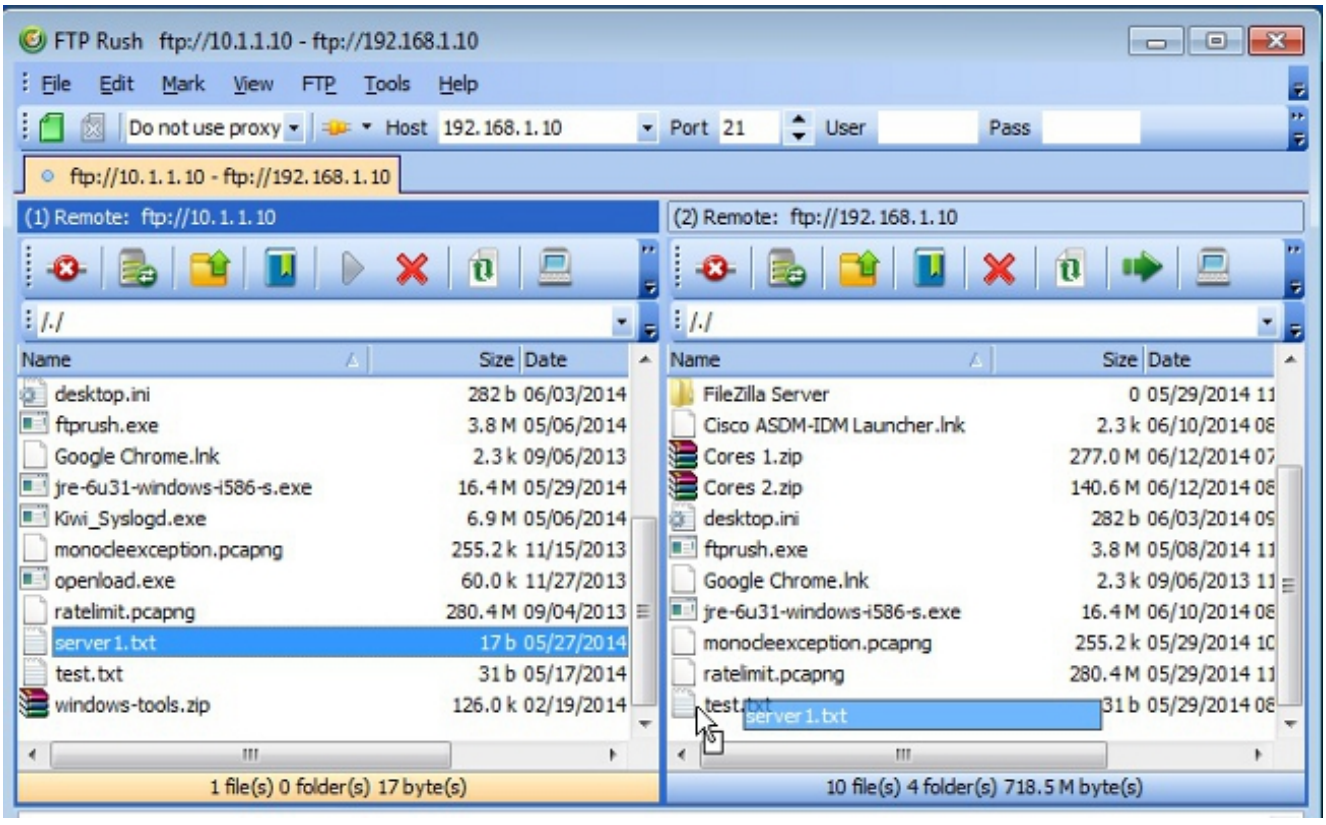
1. 从FXP客户端计算机连接到server1:



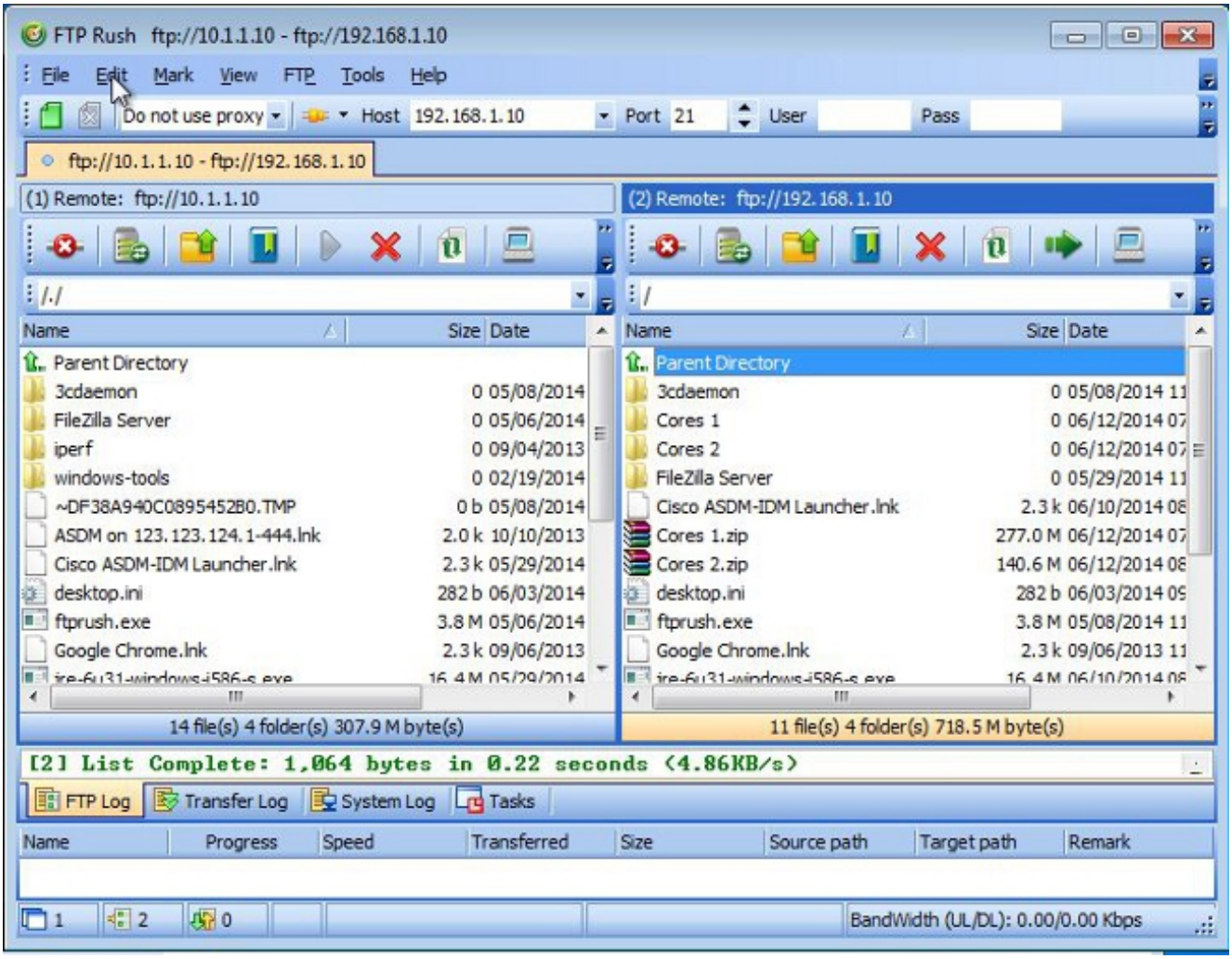
2. 从FXP客户端计算机连接到server2:



3. 将要从server1窗口传输的文件拖放到server2窗口：



4. 验证文件传输是否成功：



故障排除

本节提供可用于排除配置故障的两个不同场景的捕获。

FTP检测禁用场景

如本文档的FTP检查和FXP部分所述，禁用FTP检查时，此数据将显示在ASA客户端接口上：

```
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.
```

以下是有关此数据的一些说明：

- 客户端IP地址为172.16.1.10。

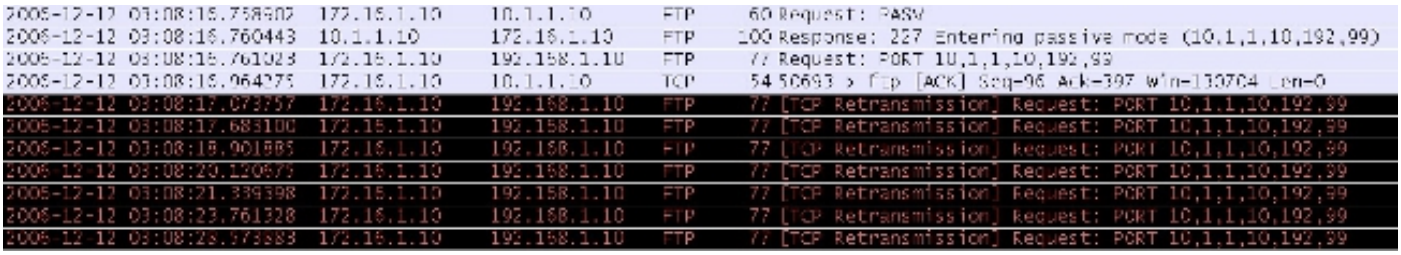
- Server1的IP地址**是10.1.1.10**。

- Server2的IP地址**是192.168.1.10**。

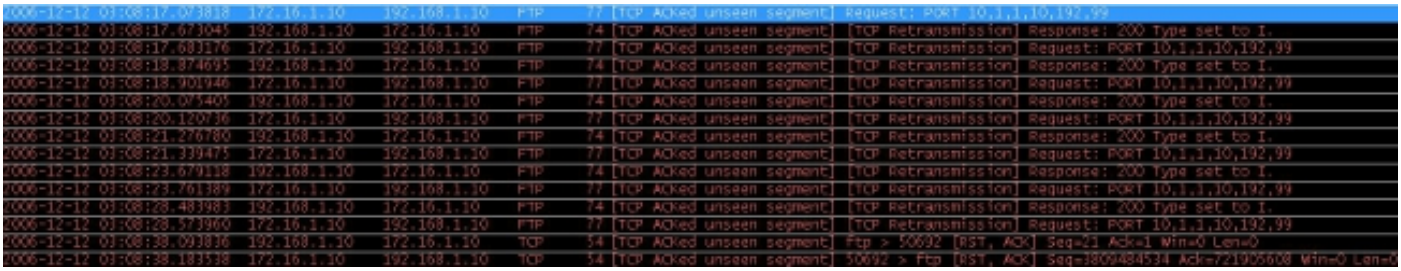
在本示例中，名为Kiwi_Syslogd**.exe的文**件从server1传输到server2。

FTP检测已启用

启用FTP检测时，此数据显示在ASA客户端接口上：



以下是ASA丢弃捕获：



FTP检查**会**丢弃PORT请求，因为它包含的IP地址和端口与客户端IP地址和端口不同。随后，检测终止与服务器的控制连接。