Ejemplo de Configuración de la Transferencia de Archivos ASA con FXP

Contenido

Introducción

Este documento describe cómo configurar File eXchange Protocol (FXP) en Cisco Adaptive Security Appliance (ASA) a través de la CLI.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre el protocolo de transferencia de archivos (FTP) (modos Activo/Pasivo).

Componentes Utilizados

La información de este documento se basa en Cisco ASA que ejecuta las versiones de software 8.0 y posteriores.

Nota: Este ejemplo de configuración utiliza dos estaciones de trabajo de Microsoft Windows que actúan como servidores FXP y ejecutan servicios FTP (3C Daemon). También tienen FXP activado. También se utiliza otra estación de trabajo de Microsoft Windows que ejecuta el software cliente FXP (FTP Rush).

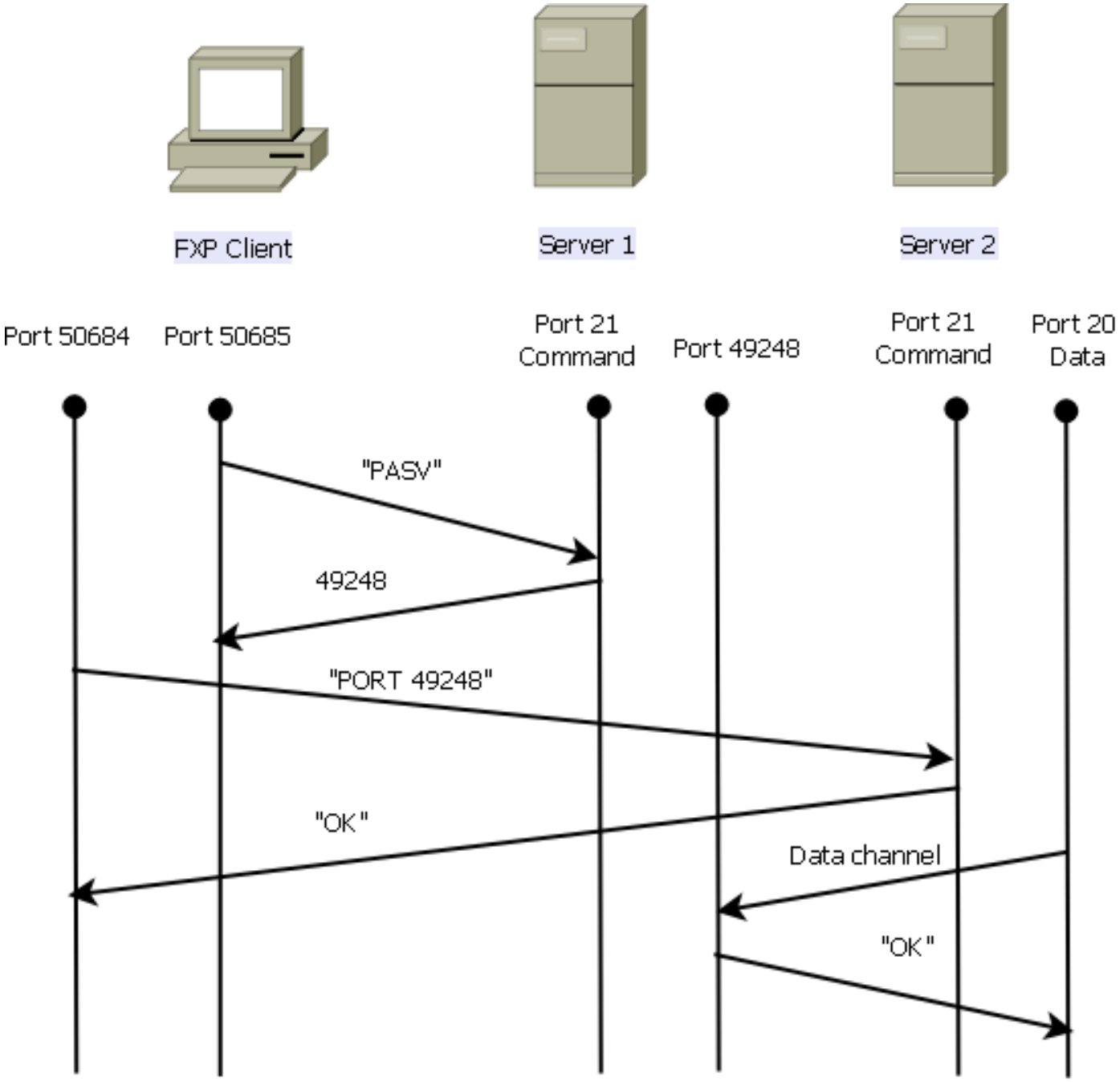
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

FXP permite transferir archivos de un servidor FTP a otro servidor FTP a través de un cliente FXP sin necesidad de depender de la velocidad de conexión a Internet del cliente. Con FXP, la velocidad máxima de transferencia depende solamente de la conexión entre los dos servidores, que generalmente es mucho más rápida que la conexión del cliente. Puede aplicar FXP en escenarios donde un servidor de ancho de banda alto requiere recursos de otro servidor de ancho de banda alto, pero sólo un cliente de ancho de banda bajo como un administrador de red que trabaja de forma remota tiene la autoridad para acceder a los recursos en ambos servidores.

El FXP funciona como una extensión del protocolo FTP y el mecanismo se indica en la sección 5.2 del RFC 959 FTP. Básicamente, el cliente FXP inicia una conexión de control con un servidor FTP1, abre otra conexión de control con el servidor FTP2 y luego modifica los atributos de conexión de los servidores de modo que se apunten entre sí para que la transferencia tenga lugar directamente entre los dos servidores.

Mecanismo de transferencia de archivos a través de FXP



A continuación se presenta una descripción general del proceso:

1. El cliente abre una conexión de control con server1 en el puerto TCP 21.

   El cliente envía el comando **PASV** al servidor1.

   Server1 responde con su dirección IP y el puerto en el que escucha.

2. El cliente abre una conexión de control con el servidor 2 en el puerto TCP 21.

   El cliente pasa la dirección/puerto que se recibe del servidor1 al servidor2 en un comando **PORT**.

   Server2 responde para informar al cliente que el comando **PORT** es exitoso. Server2 ahora sabe dónde enviar los datos.

3. Para iniciar el proceso de transmisión desde el servidor1 al servidor2:

   El cliente envía el comando **STOR** al servidor 2 y le ordena almacenar la fecha que recibe.

   El cliente envía el comando **RETR** al server1 y le indica que recupere o transmita el archivo.

4. Todos los datos ahora van directamente del origen al servidor FTP de destino. Ambos servidores solo informan al cliente de los mensajes de estado de error/éxito.

Así es como aparece la tabla de conexión:

```
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
```

Inspección FTP y FXP

La transferencia de archivos a través de ASA a través de FXP sólo se realiza correctamente cuando la inspección FTP se **inhabilita** en el ASA.

Cuando el cliente FXP especifica una dirección IP y un puerto TCP que difieren de los del cliente en el comando FTP **PORT**, se crea una situación insegura donde un atacante puede realizar un escaneo de puerto contra un host en Internet desde un servidor FTP de terceros. Esto se debe a que se indica al servidor FTP que abra una conexión a un puerto en una máquina que podría no ser el cliente que origina. Esto se denomina **ataque de rebote FTP** y la inspección FTP cierra la conexión porque considera que se trata de una violación de seguridad.

Aquí tiene un ejemplo:

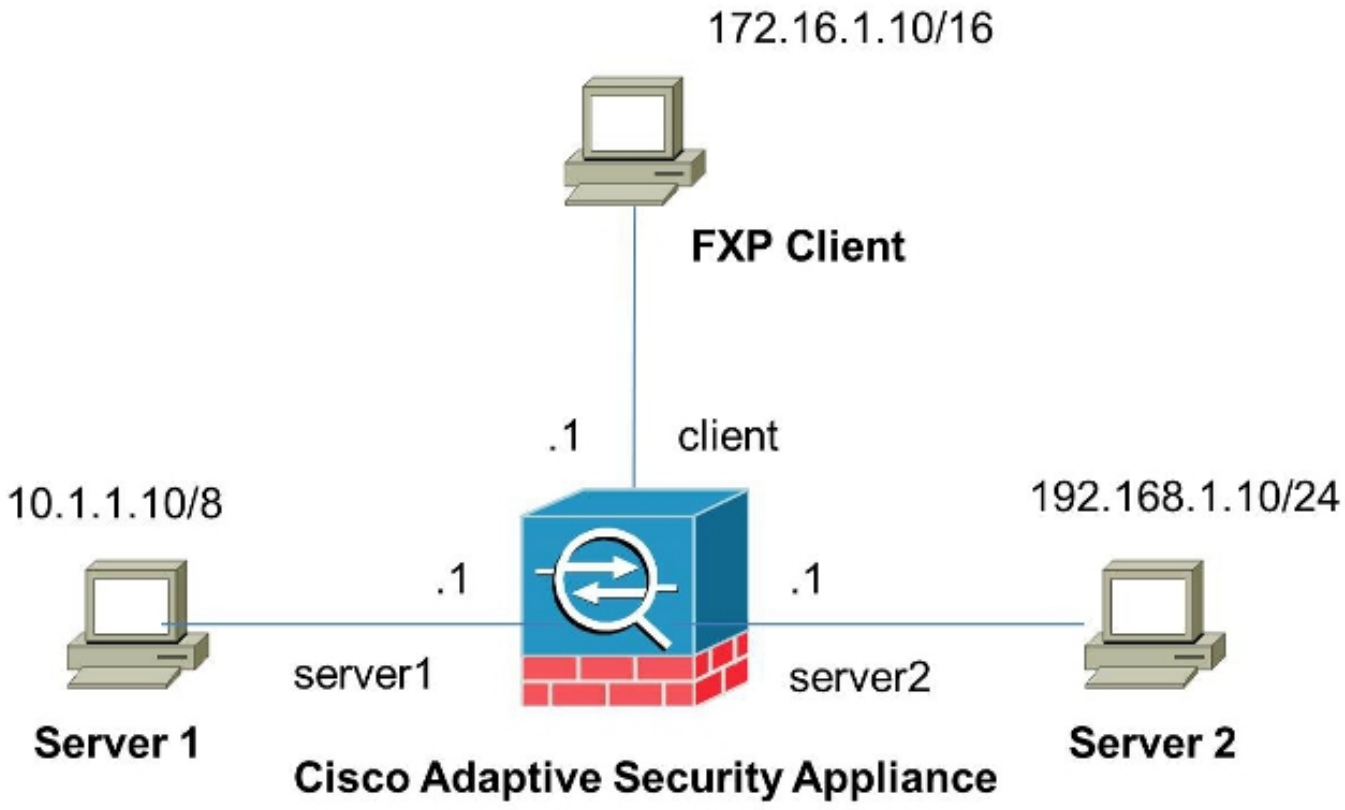
```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: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

Utilice la información que se describe en esta sección para configurar FXP en el ASA.

> **Nota:** Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



Configuración de ASA mediante CLI

Complete estos pasos para configurar el ASA:

1. Desactivar inspección 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 las listas de acceso para permitir la comunicación entre el cliente FXP y los dos 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 las listas de acceso en las 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
```

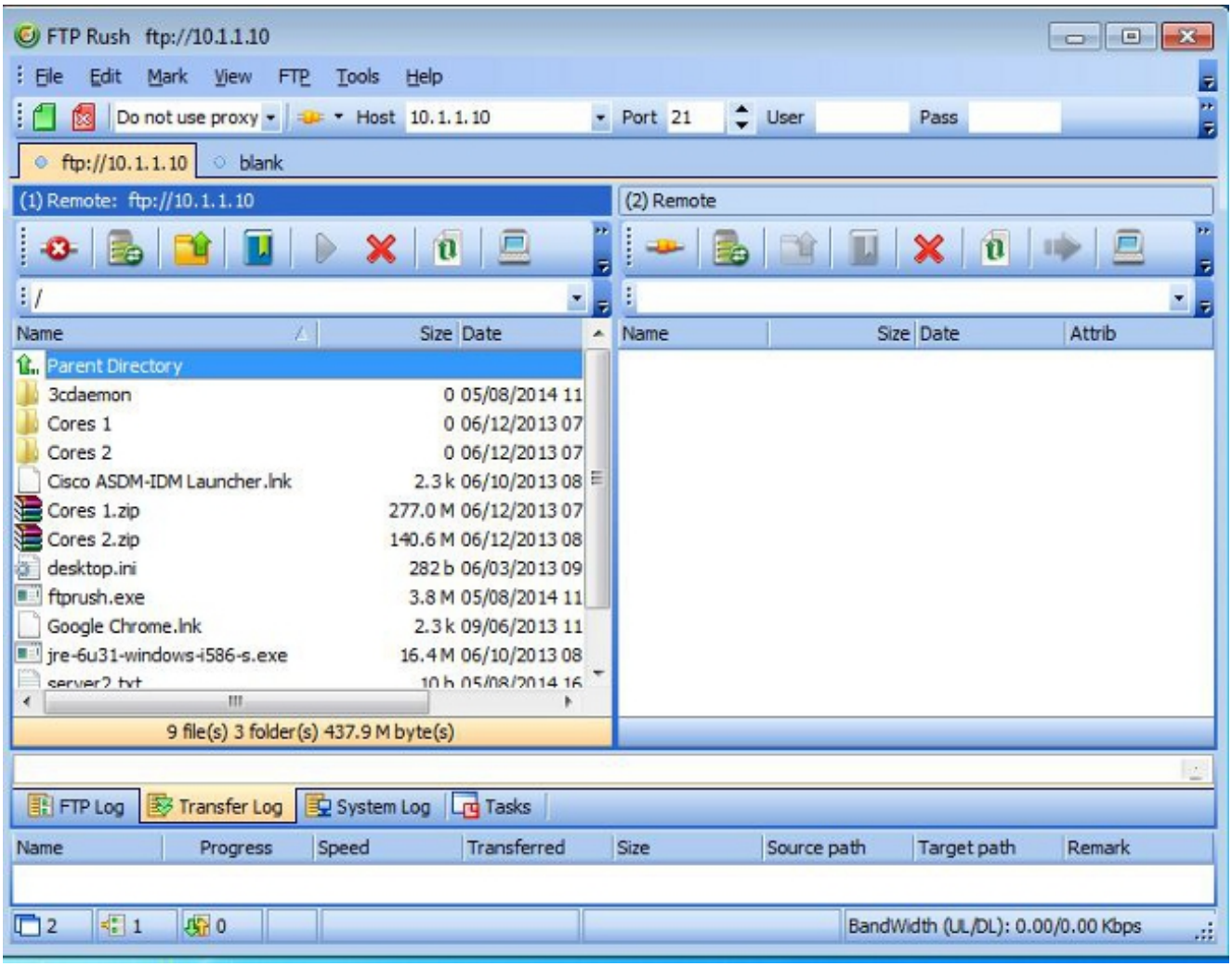
Verificación

Utilice la información que se describe en esta sección para verificar que su configuración funcione correctamente.

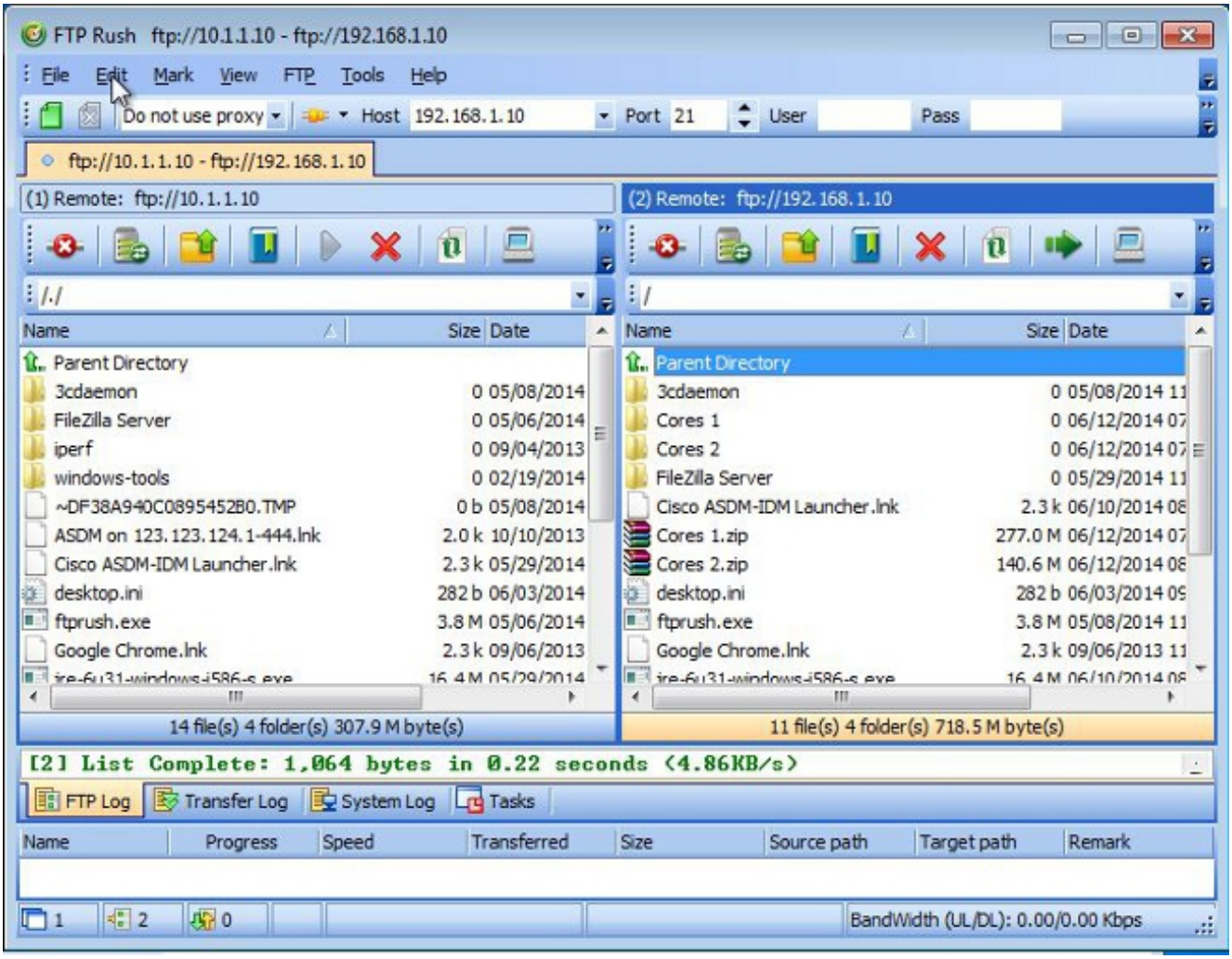
Proceso de transferencia de archivos

Complete estos pasos para verificar la transferencia exitosa de archivos entre los dos servidores FTP:

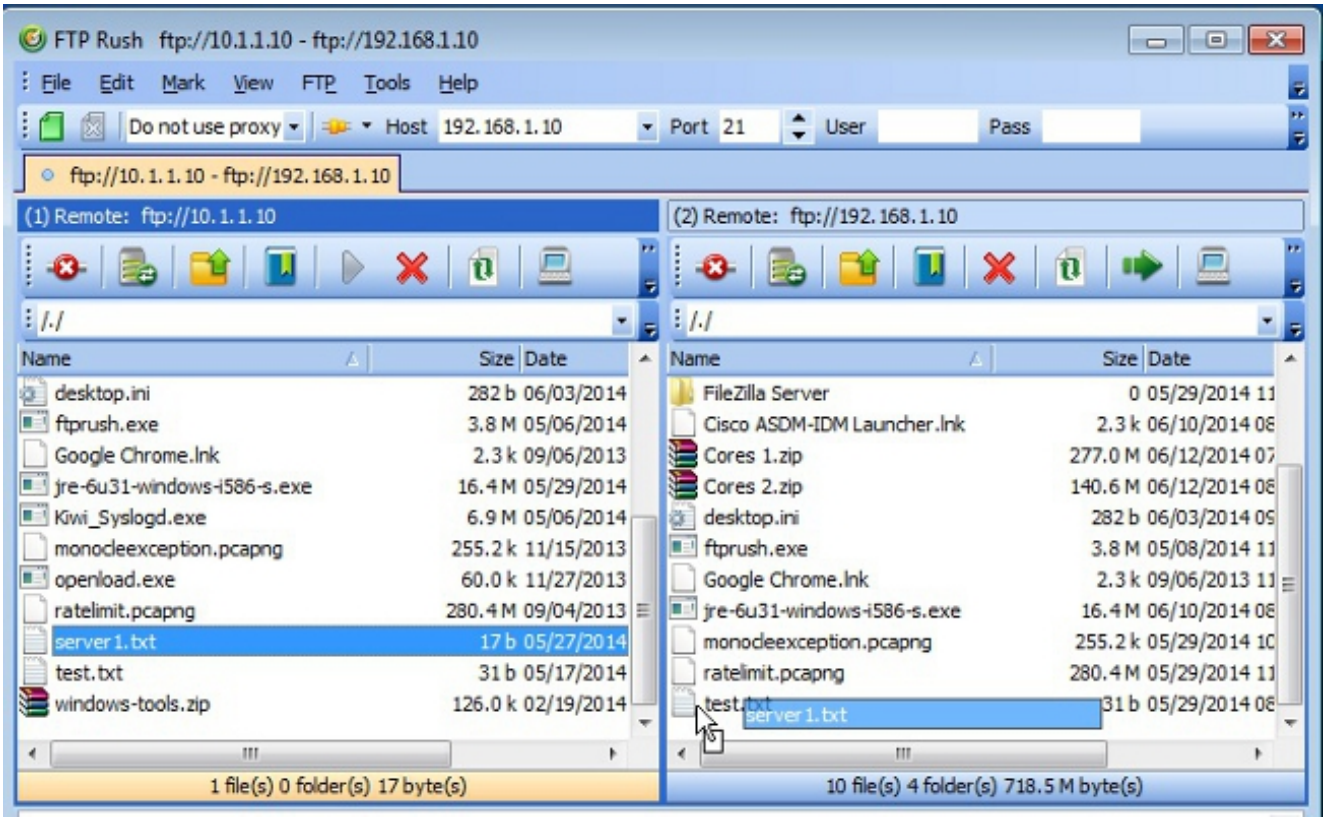
1. Conéctese al servidor 1 desde el equipo cliente FXP:



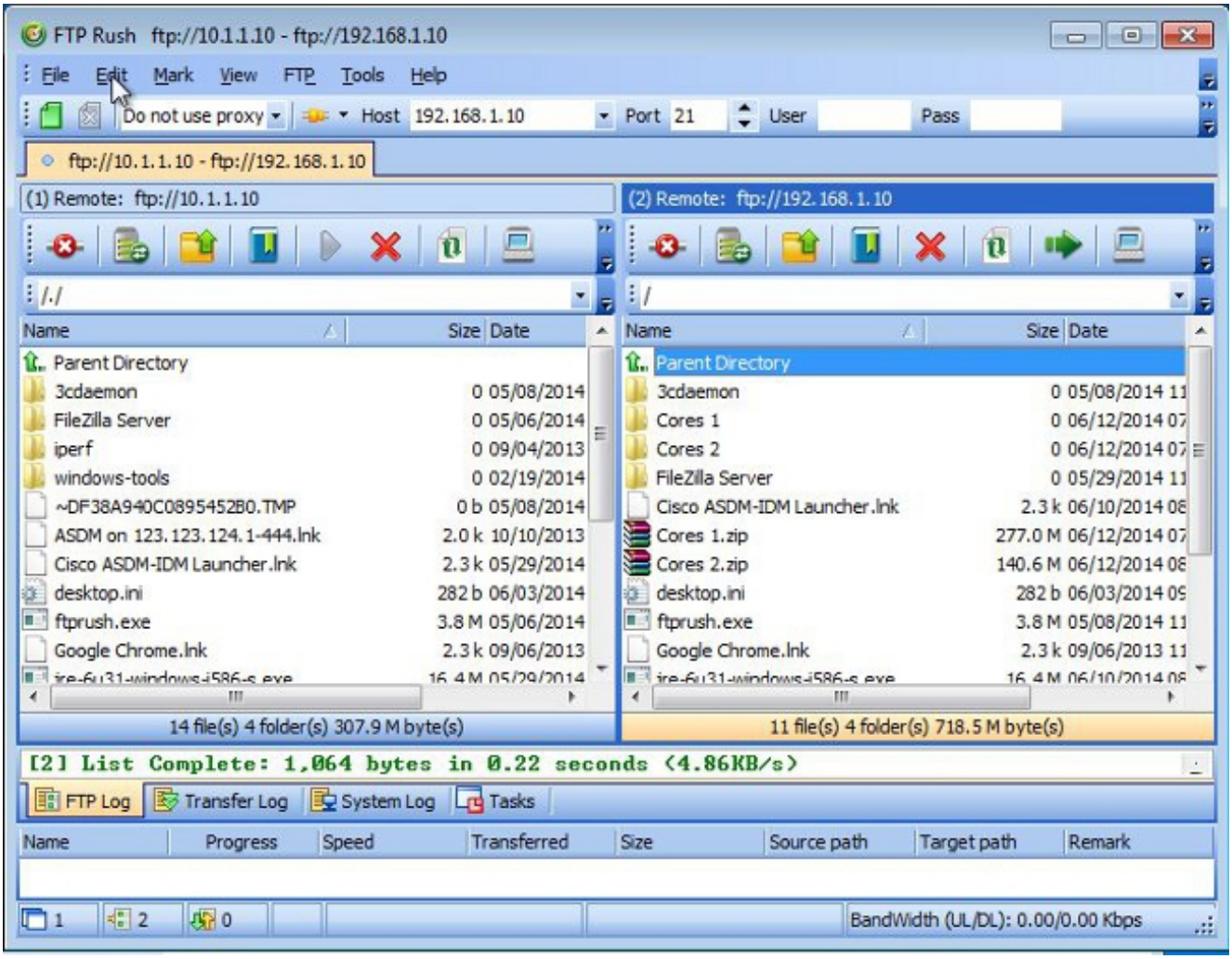
2. Conéctese al servidor 2 desde el equipo cliente FXP:



3. Arrastre y suelte el archivo que se va a transferir desde la ventana server1 a la ventana server2:



4. Verifique que la transferencia de archivos sea exitosa:



Troubleshoot

Esta sección proporciona capturas de dos escenarios diferentes que puede utilizar para resolver problemas de su configuración.

Situación Desactivada de Inspección FTP

Cuando se inhabilita la inspección FTP, como se detalla en la sección Inspección FTP y FXP de este documento, estos datos aparecen en la interfaz 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.
```

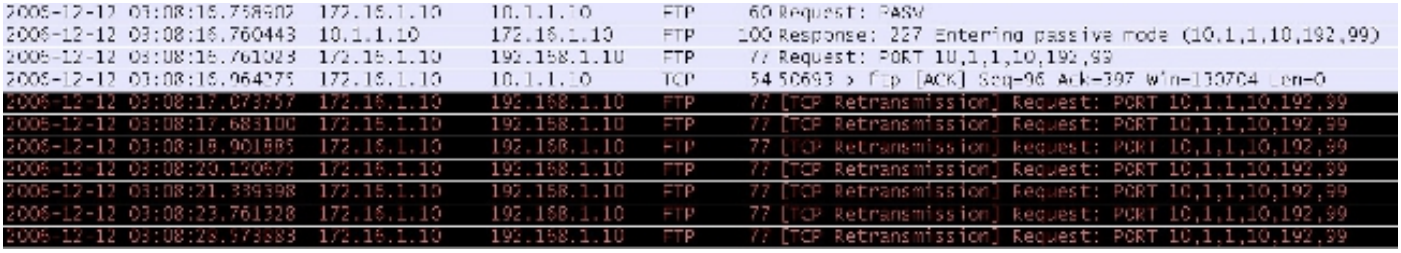
Acá algunas notas sobre estos datos:

- La dirección IP del cliente es **172.16.1.10**.
- La dirección IP Server1 es **10.1.1.10**.
- La dirección IP Server2 es **192.168.1.10**.

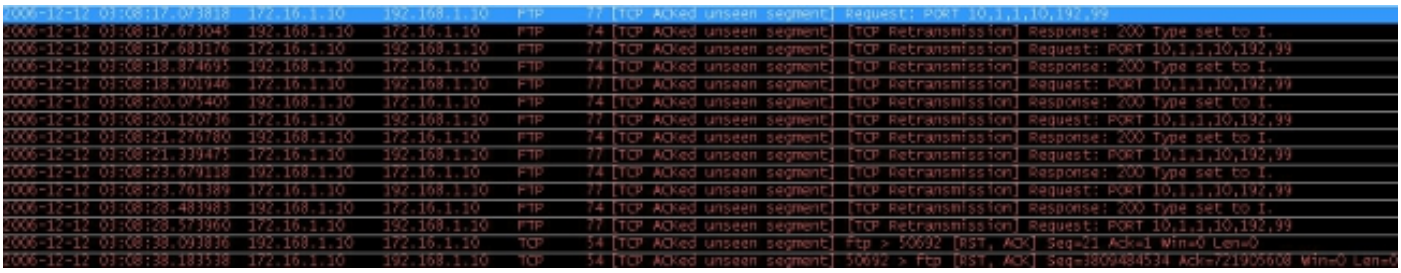
En este ejemplo, el archivo denominado **Kiwi_Syslogd.exe** se transfiere del servidor 1 al servidor 2.

Inspección FTP habilitada

Cuando se habilita la inspección FTP, estos datos aparecen en la interfaz cliente ASA:



Estas son las capturas de caídas de ASA:



La inspección FTP descarta la solicitud **PORT** porque contiene una dirección IP y un puerto que difieren de la dirección IP y el puerto del cliente. Posteriormente, la inspección finaliza la conexión de control al servidor.