

# Exemple de configuration du transfert de fichiers ASA avec FXP

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Mécanisme de transfert de fichiers via FXP](#)

[Inspection FTP et FXP](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurez l'ASA par l'intermédiaire du CLI](#)

[Vérification](#)

[Processus de transfert de fichiers](#)

[Dépannage](#)

[Scénario d'inspection FTP désactivé](#)

[Inspection FTP activée](#)

## Introduction

Ce document décrit comment configurer le protocole FXP (File eXchange Protocol) sur l'appareil de sécurité adaptatif Cisco (ASA) via l'interface de ligne de commande.

## Conditions préalables

### Conditions requises

Cisco vous recommande d'avoir une connaissance de base du protocole FTP (File Transfer Protocol) (modes actif/passif).

### Components Used

Les informations de ce document sont basées sur Cisco ASA qui exécute les versions 8.0 et ultérieures du logiciel.

**Note:** Cet exemple de configuration utilise deux stations de travail Microsoft Windows qui agissent en tant que serveurs FXP et exécutent des services FTP (Démon 3C). FXP est également activé. Une autre station de travail Microsoft Windows qui exécute le logiciel client FXP (FTP Rush) est également utilisée.

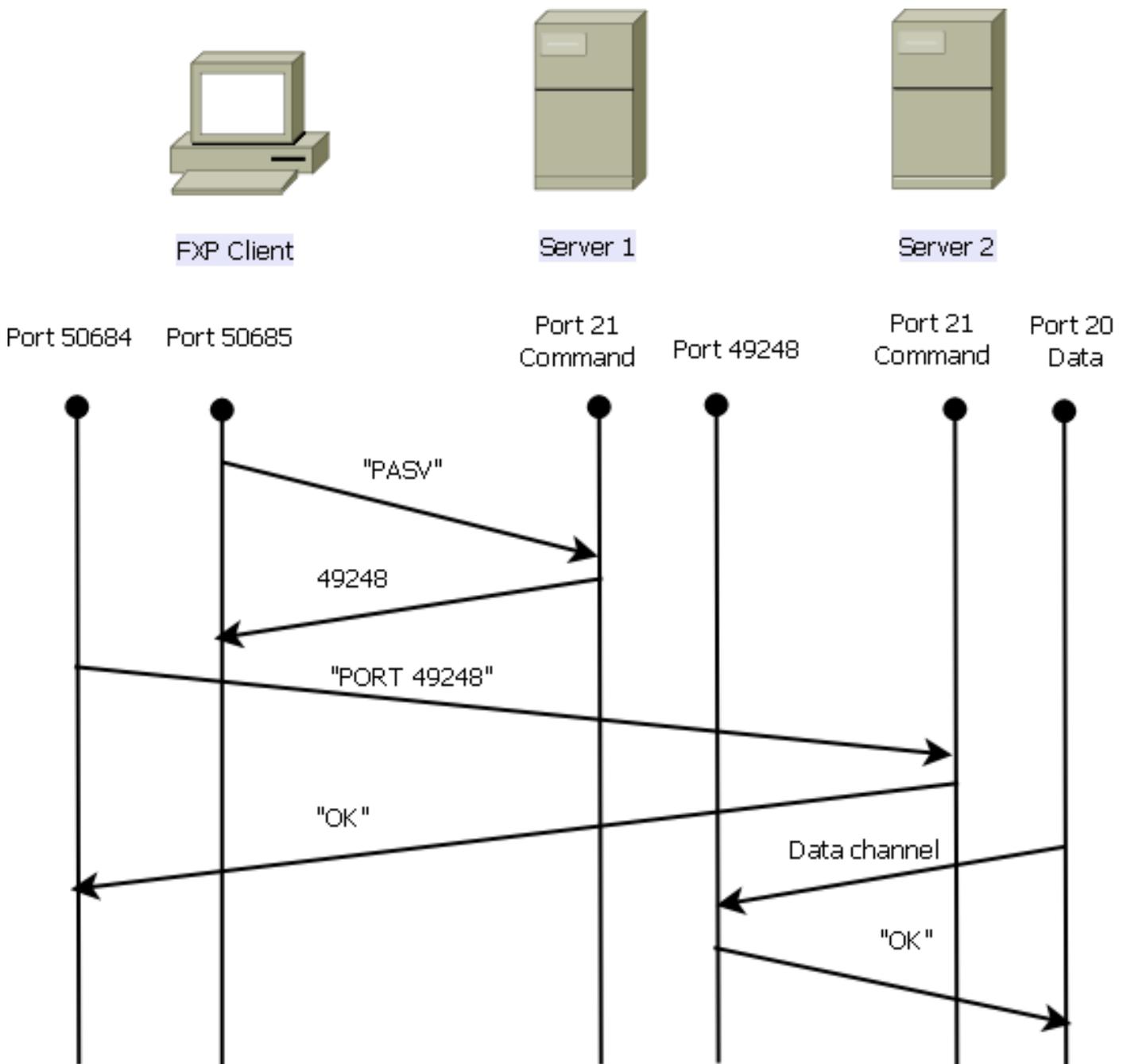
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Informations générales

Le FXP vous permet de transférer des fichiers d'un serveur FTP à un autre serveur FTP via un client FXP sans avoir à dépendre de la vitesse de connexion Internet du client. Avec FXP, la vitesse de transfert maximale dépend uniquement de la connexion entre les deux serveurs, qui est généralement beaucoup plus rapide que la connexion client. Vous pouvez appliquer FXP dans des scénarios où un serveur à bande passante élevée demande des ressources à un autre serveur à bande passante élevée, mais seul un client à bande passante faible, tel qu'un administrateur réseau qui travaille à distance, a l'autorité d'accéder aux ressources sur les deux serveurs.

Le protocole FXP fonctionne comme une extension du protocole FTP, et le mécanisme est indiqué dans la section 5.2 du document FTP RFC 959. Fondamentalement, le client FXP initie une connexion de contrôle avec un serveur FTP1, ouvre une autre connexion de contrôle avec le serveur FTP2, puis modifie les attributs de connexion des serveurs de sorte qu'ils pointent l'un vers l'autre de sorte que le transfert ait lieu directement entre les deux serveurs.

## Mécanisme de transfert de fichiers via FXP



Voici un aperçu du processus :

1. Le client ouvre une connexion de contrôle avec le serveur 1 sur le port TCP 21.

Le client envoie la commande **PASV** au serveur 1.

Server1 répond avec son adresse IP et le port sur lequel il écoute.

2. Le client ouvre une connexion de contrôle avec server2 sur le port TCP 21.

Le client passe l'adresse/le port qui est reçu du serveur1 au serveur2 dans une commande **PORT**.

Server2 répond afin d'informer le client que la commande **PORT** a réussi. Le serveur 2 sait maintenant où envoyer les données.

### 3. Afin de commencer le processus de transmission du serveur1 au serveur2 :

Le client envoie la commande **STOR** au serveur2 et lui demande de stocker la date qu'il reçoit.

Le client envoie la commande **RETR** au serveur 1 et lui demande de récupérer ou de transmettre le fichier.

### 4. Toutes les données vont maintenant directement de la source au serveur FTP de destination. Les deux serveurs signalent uniquement au client les messages d'état en cas d'échec ou de réussite.

Voici comment apparaît la table de connexion :

```
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
```

## Inspection FTP et FXP

Le transfert de fichiers via ASA via FXP ne réussit que lorsque l'inspection FTP est **désactivée** sur l'ASA.

Lorsque le client FXP spécifie une adresse IP et un port TCP qui diffèrent de ceux du client dans la commande **PORT** FTP, une situation non sécurisée se crée lorsqu'un pirate est en mesure d'effectuer une analyse de port contre un hôte sur Internet à partir d'un serveur FTP tiers. Cela est dû au fait que le serveur FTP est invité à ouvrir une connexion à un port sur une machine qui n'est peut-être pas le client d'origine. Il s'agit d'une **attaque de renvoi FTP**, et l'inspection FTP arrête la connexion car elle considère qu'il s'agit d'une violation de sécurité.

Voici un exemple :

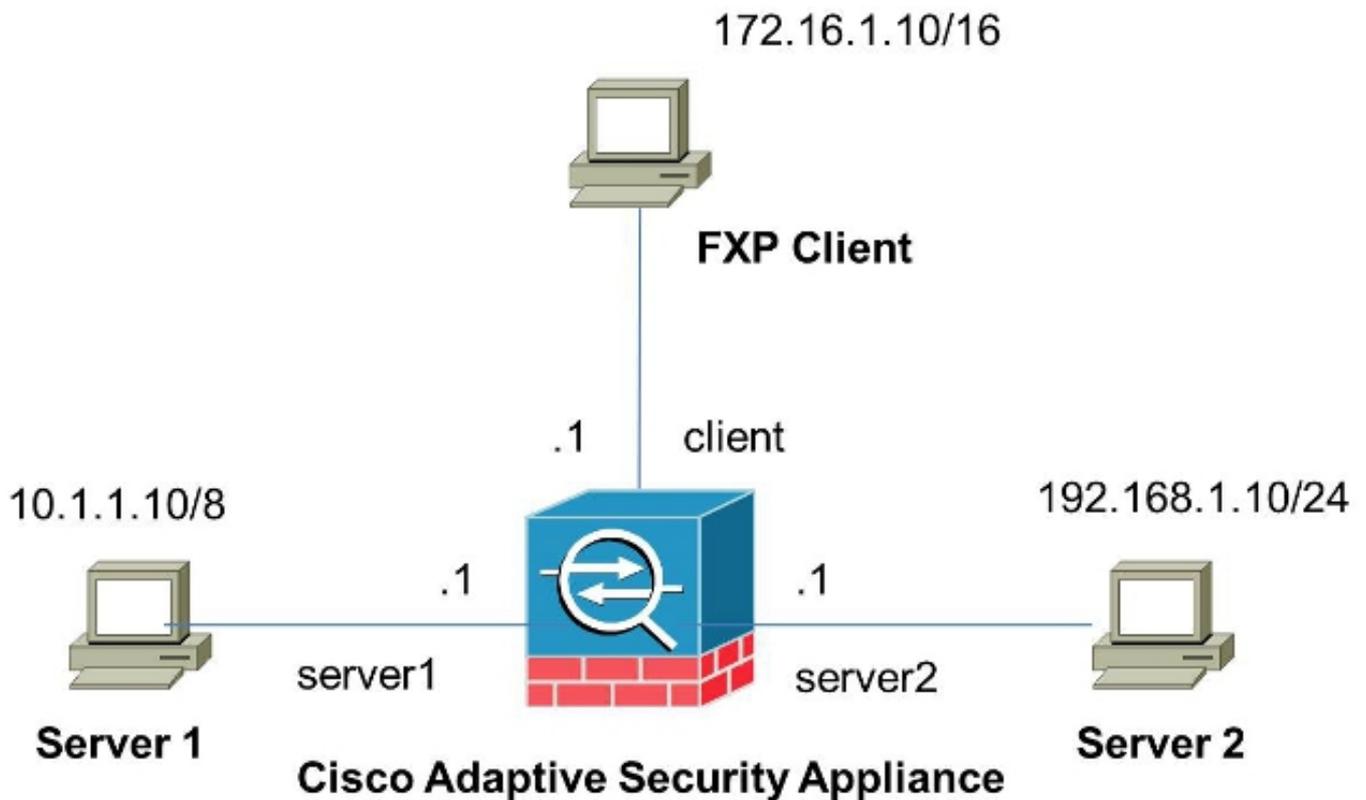
```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: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

## Configuration

Utilisez les informations décrites dans cette section afin de configurer FXP sur l'ASA.

**Note:** Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

## Diagramme du réseau



## Configurez l'ASA par l'intermédiaire du CLI

Complétez ces étapes afin de configurer l'ASA :

1. Désactiver l'inspection FTP :

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

2. Configurez les listes d'accès afin d'autoriser la communication entre le client FXP et les deux serveurs 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. Appliquez les listes d'accès sur les interfaces respectives :

```
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
```

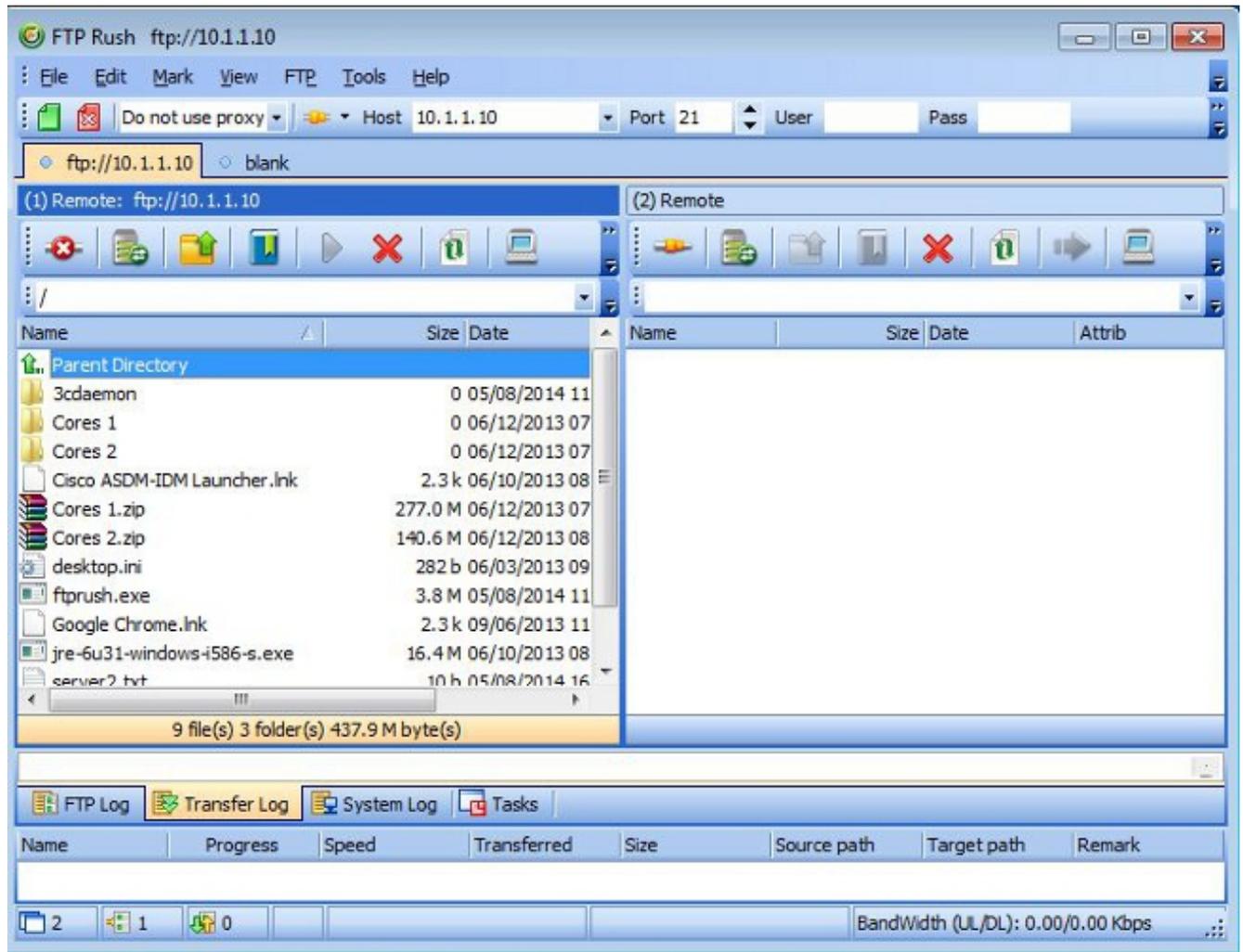
## Vérification

Utilisez les informations décrites dans cette section afin de vérifier que votre configuration fonctionne correctement.

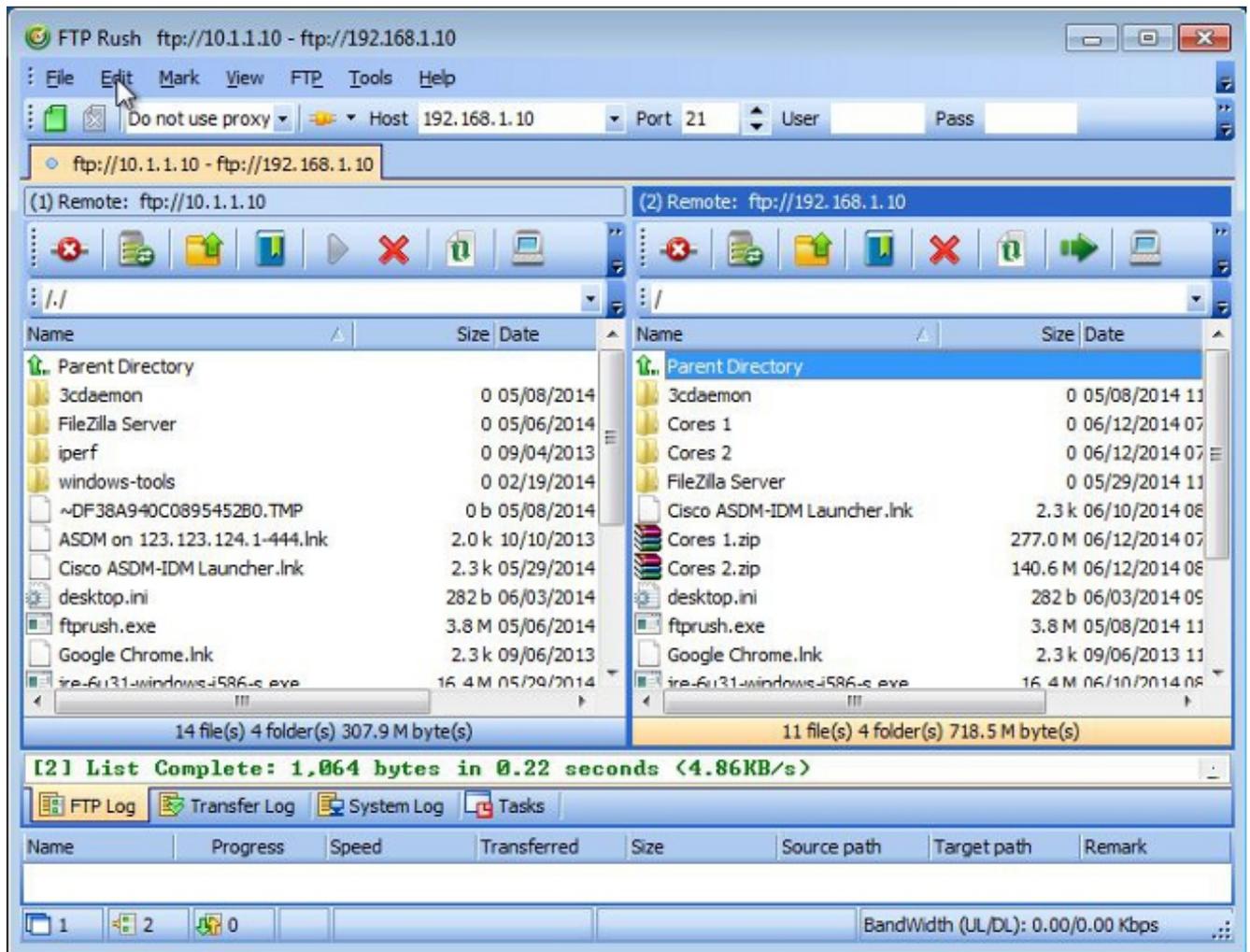
## Processus de transfert de fichiers

Complétez ces étapes afin de vérifier le transfert de fichiers réussi entre les deux serveurs FTP :

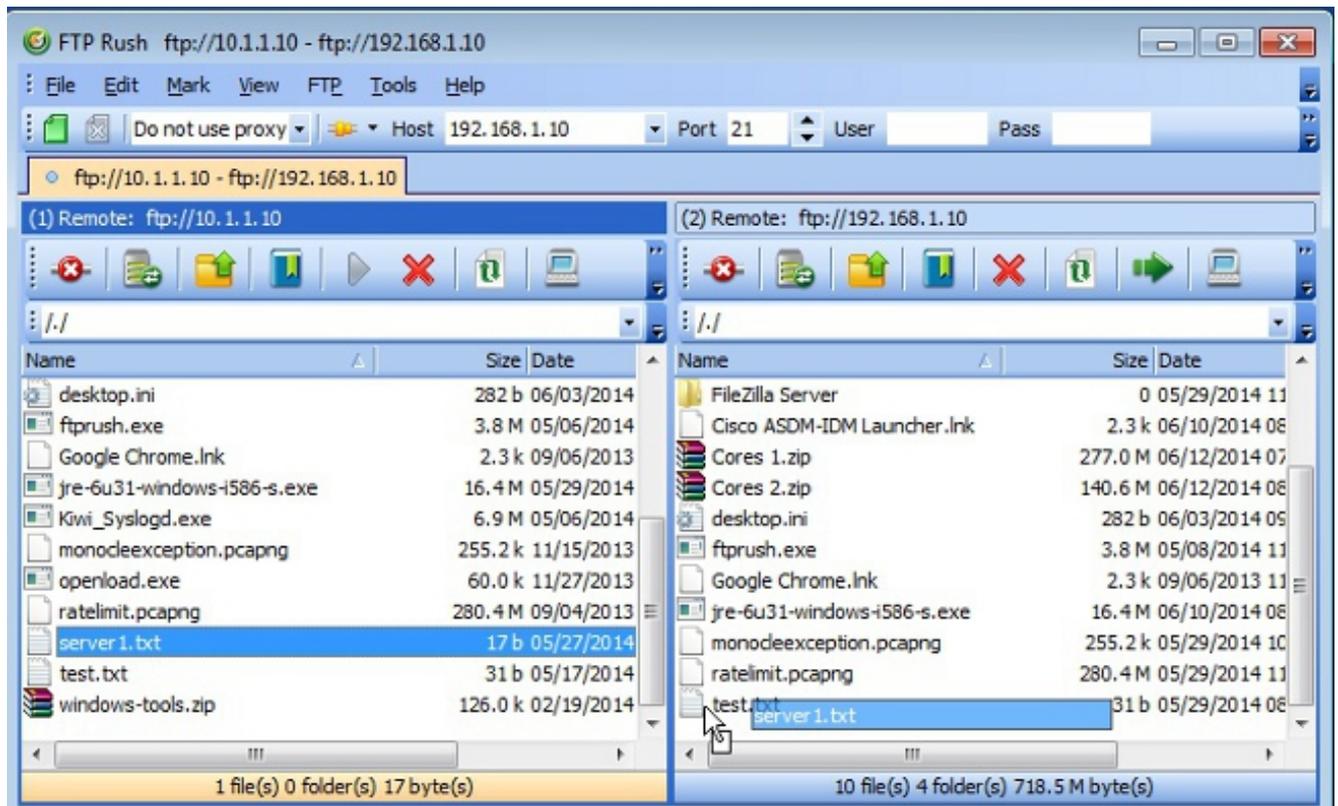
1. Connectez-vous au serveur 1 à partir de la machine cliente FXP :



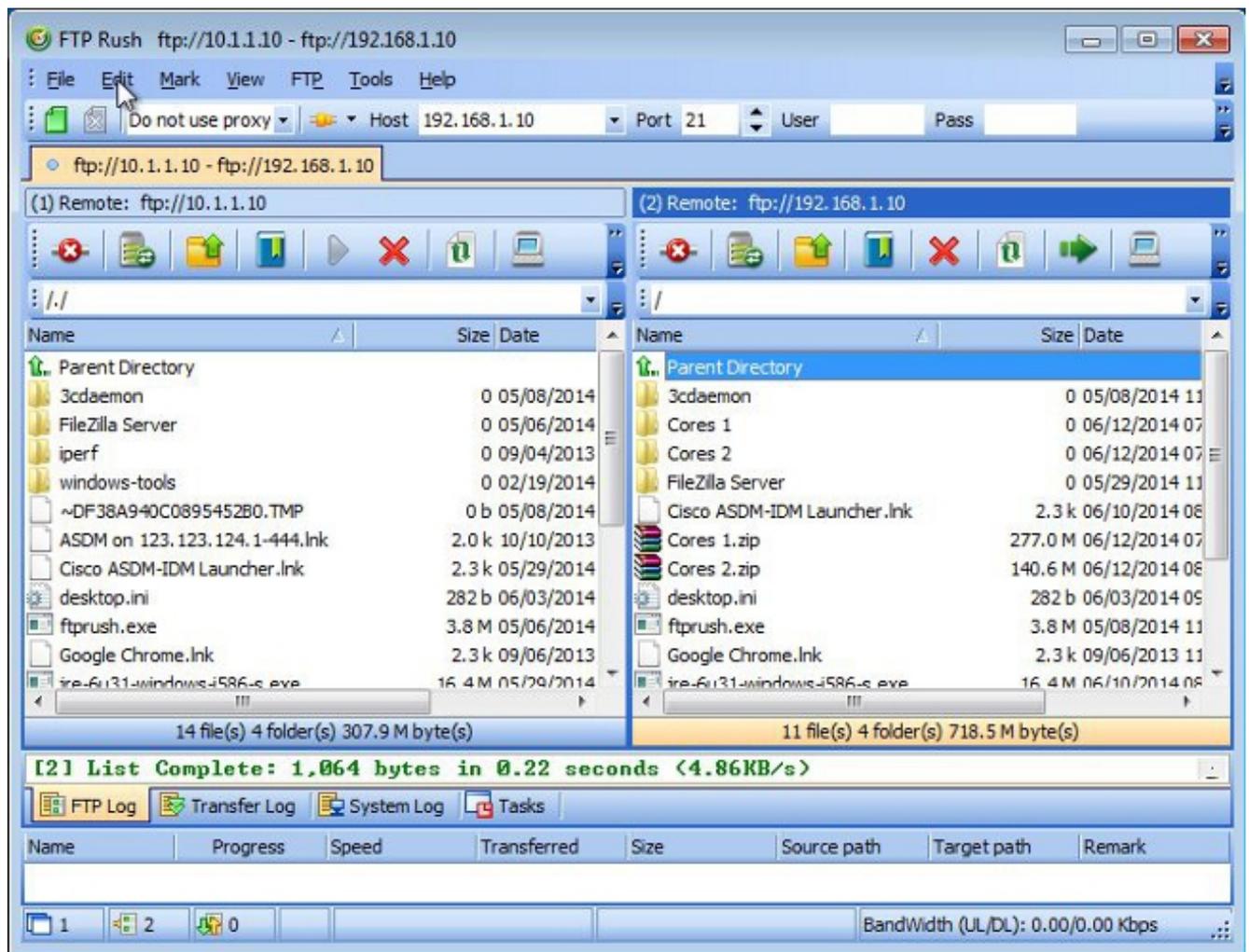
2. Connectez-vous au serveur 2 à partir de la machine cliente FXP :



3. Faites glisser le fichier à transférer de la fenêtre server1 vers la fenêtre server2 :



4. Vérifiez que le transfert de fichiers a réussi :



## Dépannage

Cette section fournit des captures de deux scénarios différents que vous pouvez utiliser pour dépanner votre configuration.

### Scénario d'inspection FTP désactivé

Lorsque l'inspection FTP est désactivée, comme indiqué dans la section [Inspection FTP et FXP](#) de ce document, ces données apparaissent sur l'interface client 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.
```

Voici quelques notes sur ces données :

- L'adresse IP du client est **172.16.1.10**.
- L'adresse IP de Server1 est **10.1.1.10**.
- L'adresse IP de Server2 est **192.168.1.10**.

Dans cet exemple, le fichier nommé **Kiwi\_Syslogd.exe** est transféré de server1 vers server2.

## Inspection FTP activée

Lorsque l'inspection FTP est activée, ces données apparaissent sur l'interface client ASA :

2005-12-12 03:08:15.758502	172.16.1.10	10.1.1.10	FTP	60	Request: PASV
2005-12-12 03:08:15.760443	10.1.1.10	172.16.1.10	FTP	100	Response: 227 Entering passive mode (10,1,1,10,192,99)
2005-12-12 03:08:15.761023	172.16.1.10	192.168.1.10	FTP	77	Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:15.964275	172.16.1.10	10.1.1.10	TCP	54	50693 > [Fin] [ACK] Seq=96 Ack=397 win=130704 len=0
2005-12-12 03:08:17.073757	172.16.1.10	192.168.1.10	FTP	77	[TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:17.683100	172.16.1.10	192.168.1.10	FTP	77	[TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:18.901985	172.16.1.10	192.168.1.10	FTP	77	[TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:20.120879	172.16.1.10	192.168.1.10	FTP	77	[TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:21.339498	172.16.1.10	192.168.1.10	FTP	77	[TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:23.761328	172.16.1.10	192.168.1.10	FTP	77	[TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:25.572883	172.16.1.10	192.168.1.10	FTP	77	[TCP Retransmission] Request: PORT 10,1,1,10,192,99

Voici les captures d'écran ASA :

2005-12-12 03:08:17.073818	172.16.1.10	192.168.1.10	FTP	77	TCP Ached unseen segment [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:17.673044	192.168.1.10	172.16.1.10	FTP	74	TCP Ached unseen segment [TCP Retransmission] Response: 200 Type set to I
2005-12-12 03:08:17.683176	172.16.1.10	192.168.1.10	FTP	77	TCP Ached unseen segment [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:18.374693	192.168.1.10	172.16.1.10	FTP	74	TCP Ached unseen segment [TCP Retransmission] Response: 200 Type set to I
2005-12-12 03:08:18.901946	172.16.1.10	192.168.1.10	FTP	77	TCP Ached unseen segment [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:20.073400	192.168.1.10	172.16.1.10	FTP	74	TCP Ached unseen segment [TCP Retransmission] Response: 200 Type set to I
2005-12-12 03:08:20.120736	172.16.1.10	192.168.1.10	FTP	77	TCP Ached unseen segment [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:21.276780	192.168.1.10	172.16.1.10	FTP	74	TCP Ached unseen segment [TCP Retransmission] Response: 200 Type set to I
2005-12-12 03:08:21.339475	172.16.1.10	192.168.1.10	FTP	77	TCP Ached unseen segment [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:23.679138	192.168.1.10	172.16.1.10	FTP	74	TCP Ached unseen segment [TCP Retransmission] Response: 200 Type set to I
2005-12-12 03:08:23.761389	172.16.1.10	192.168.1.10	FTP	77	TCP Ached unseen segment [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:25.483381	192.168.1.10	172.16.1.10	FTP	74	TCP Ached unseen segment [TCP Retransmission] Response: 200 Type set to I
2005-12-12 03:08:25.573960	172.16.1.10	192.168.1.10	FTP	77	TCP Ached unseen segment [TCP Retransmission] Request: PORT 10,1,1,10,192,99
2005-12-12 03:08:30.093036	192.168.1.10	172.16.1.10	TCP	54	TCP Ached unseen segment Ftp > 50692 [RST, ACK] Seq=21 Ack=1 Win=0 Len=0
2005-12-12 03:08:38.183138	172.16.1.10	192.168.1.10	TCP	54	TCP Ached unseen segment 50692 > Fcp [RST, ACK] Seq=3009484524 Ack=721005608 Win=0 Len=0

La demande **PORT** est abandonnée par l'inspection FTP car elle contient une adresse IP et un port qui diffèrent de l'adresse IP et du port du client. Par la suite, la connexion de contrôle au serveur est interrompue par l'inspection.