# ASA File Transfer met FXP-configuratievoorbeeld

## Inhoud



## Inleiding

Dit document beschrijft hoe u File eXchange Protocol (FXP) kunt configureren op de Cisco adaptieve security applicatie (ASA) via de CLI.

## Voorwaarden

### Vereisten

Cisco raadt u aan basiskennis van File Transfer Protocol (FTP) (actieve/passieve modi) te hebben.

### Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ASA dat softwareversies 8.0 en hoger uitvoert.

Opmerking: Dit configuratievoorbeeld gebruikt twee Microsoft Windows-werkstations die fungeren als FXP-servers en FTP-services (3C Daemon) uitvoeren. Ze hebben ook FXP ingeschakeld. Een ander Microsoft Windows-werkstation dat FXP-clientsoftware (FTP Rusland) draait, wordt ook gebruikt.

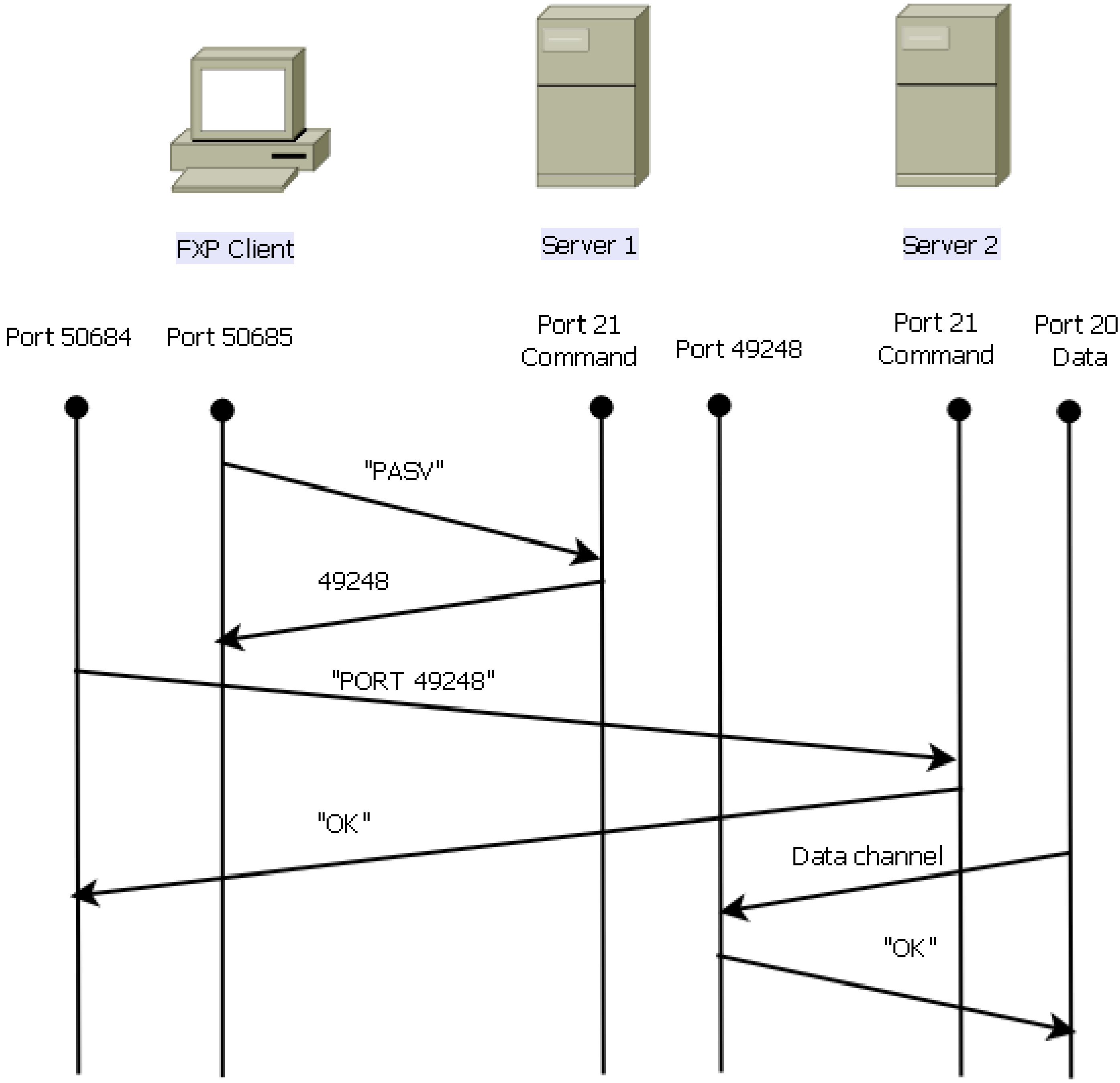
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

# Achtergrondinformatie

Met FXP kunt u bestanden van een FTP-server naar een andere FTP-server overdragen via een FXP-client zonder dat u afhankelijk bent van de snelheid van de client-internet-verbinding. Bij FXP hangt de maximale overdrachtsnelheid alleen af van de verbinding tussen de twee servers, die meestal veel sneller is dan de clientverbinding. U kunt FXP toepassen in scenario's waar een server met hoge bandbreedte middelen van een andere server met hoge bandbreedte vraagt, maar slechts een client met lage bandbreedte zoals een netwerkbeheerder die extern werkt heeft het recht om de middelen op beide servers te gebruiken.

FXP werkt als een uitbreiding van het FTP-protocol, en het mechanisme wordt vermeld in sectie 5.2 van de FTP RFC 959. De FXP client start een controle verbinding met een FTP server1, opent een andere controle verbinding met FTP server2 en wijzigt vervolgens de verbindingseigenschappen van de servers zodat ze naar elkaar wijzen zodat de overdracht rechtstreeks tussen de twee servers plaatsvindt.

## Mechanisme voor bestandsoverdracht via FXP




Hier volgt een overzicht van het proces:

1. De client opent een controle verbinding met server1 op TCP poort 21.

   De client stuurt de **PASV** opdracht naar server1.

   Server1 antwoordt met zijn IP adres en de haven waarop het luistert.

2. De client opent een controle verbinding met server2 op TCP poort 21.

   De client geeft het adres/poort door dat van server1 naar server2 wordt ontvangen in een **POORT** opdracht.

   Server2 reageert om de client te informeren dat de **PORT**-opdracht succesvol is. Server2 weet nu waar de gegevens moeten worden verzonden.

3. Zo begint het transmissieproces van server1 naar server2:

   De client stuurt de **STOR** opdracht naar server2 en geeft de opdracht de datum op te slaan die hij ontvangt.

   De client stuurt de **RETR** opdracht naar server1 en geeft de opdracht het bestand op te halen of te verzenden.

4. Alle gegevens gaan nu rechtstreeks van de bron naar de FTP-server van de bestemming. Beide servers rapporteren alleen statusberichten bij falen/succes aan de client.

Zo verschijnt de verbindingstabel:

```
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-inspectie en FXP

Bestandsoverdracht via ASA via FXP is alleen succesvol wanneer FTP-inspectie is **uitgeschakeld** in de ASA.

Wanneer de FXP client een IP-adres en TCP-poort specificeert die verschillen van die van de client in de FTP-POORT-opdracht, wordt er een onveilige situatie gecreëerd waarin een aanvaller een poortscan kan uitvoeren tegen een host op het internet vanuit een FTP-server van derden. Dit komt doordat de FTP server is geïnstrueerd om een verbinding met een poort op een machine te openen die niet de client is die er vandaan komt. Dit wordt een **aanval** van de **FTP-aanval** genoemd, en de FTP-inspectie sluit de verbinding af omdat het dit als een schending van de beveiliging beschouwt.

Hierna volgt een voorbeeld:

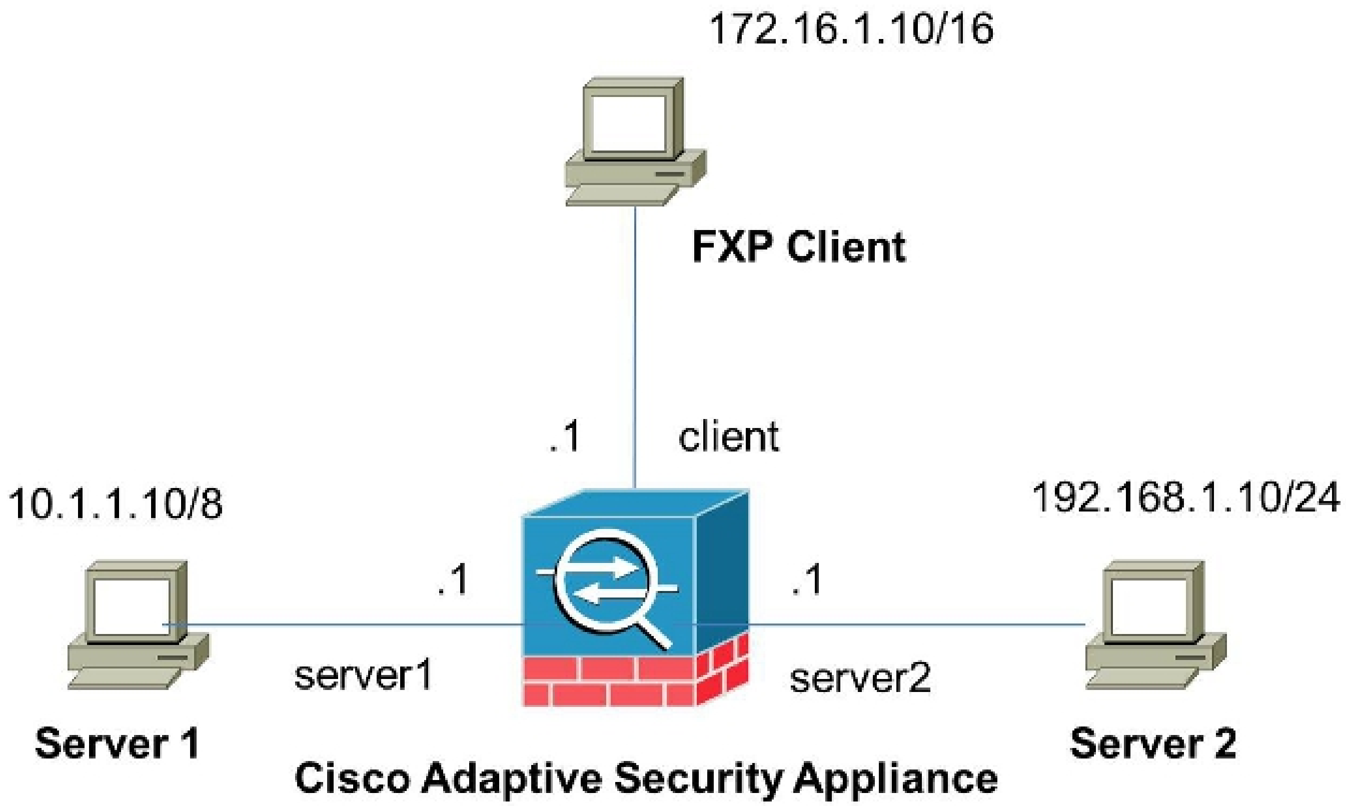
```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: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

# Configureren

Gebruik de informatie die in deze sectie wordt beschreven om FXP op de ASA te configureren.

> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

### Netwerkdiagram




### ASA via CLI configureren

Voltooi deze stappen om de ASA te configureren:

1. FTP-inspectie uitschakelen:

   ```
   FXP-ASA(config)# policy-map global_policy
   FXP-ASA(config-pmap)#  class inspection_default
   FXP-ASA(config-pmap-c)# no inspect ftp
   ```
2. Configureer toegangslijsten om communicatie tussen de FXP-client en de twee FTP-servers mogelijk te maken:

   ```
   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. Pas de toegangslijsten op de respectieve interfaces toe:

   ```
   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
   ```

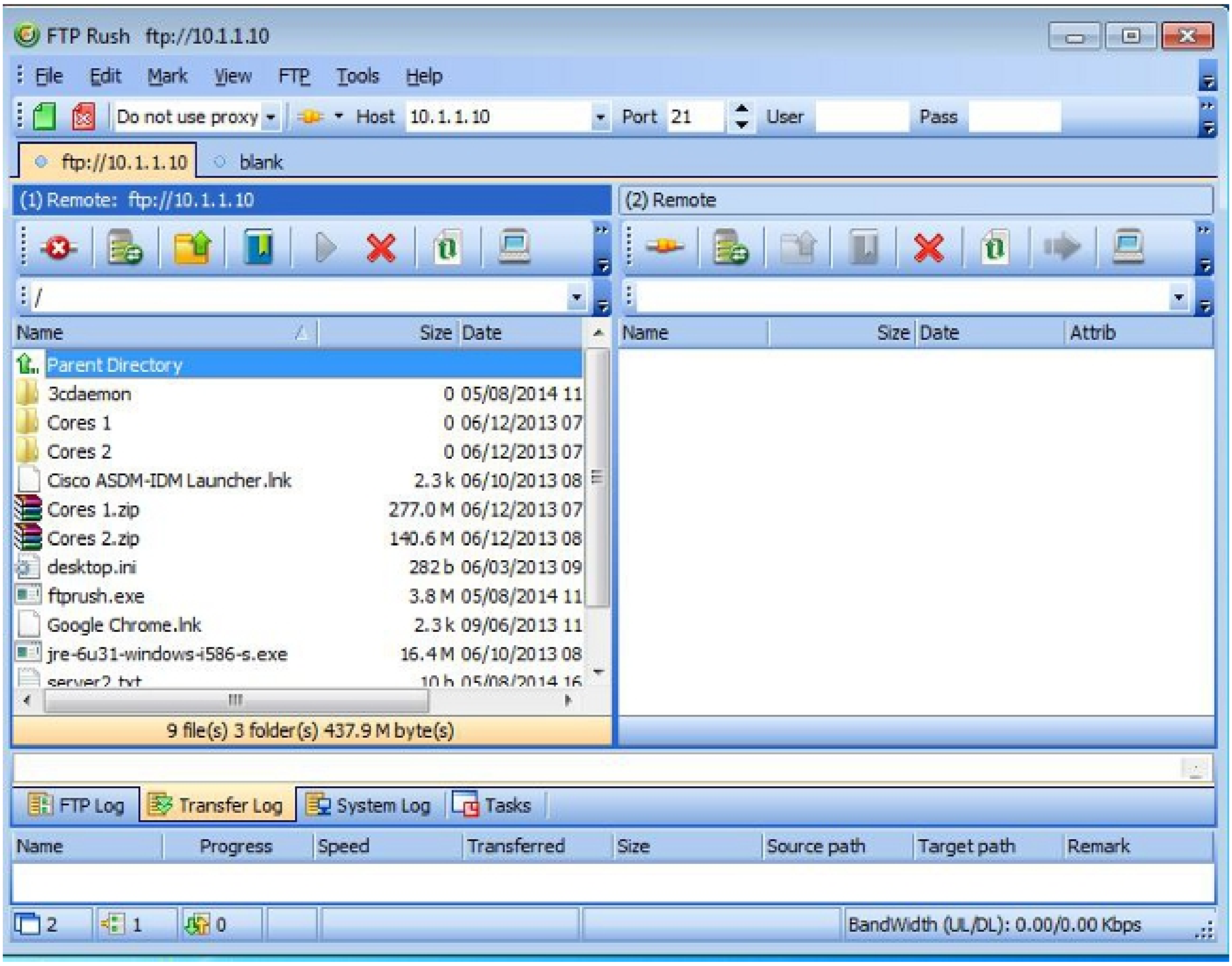
## Verifiëren

Gebruik de informatie die in dit gedeelte wordt beschreven om te controleren of uw configuratie correct werkt.

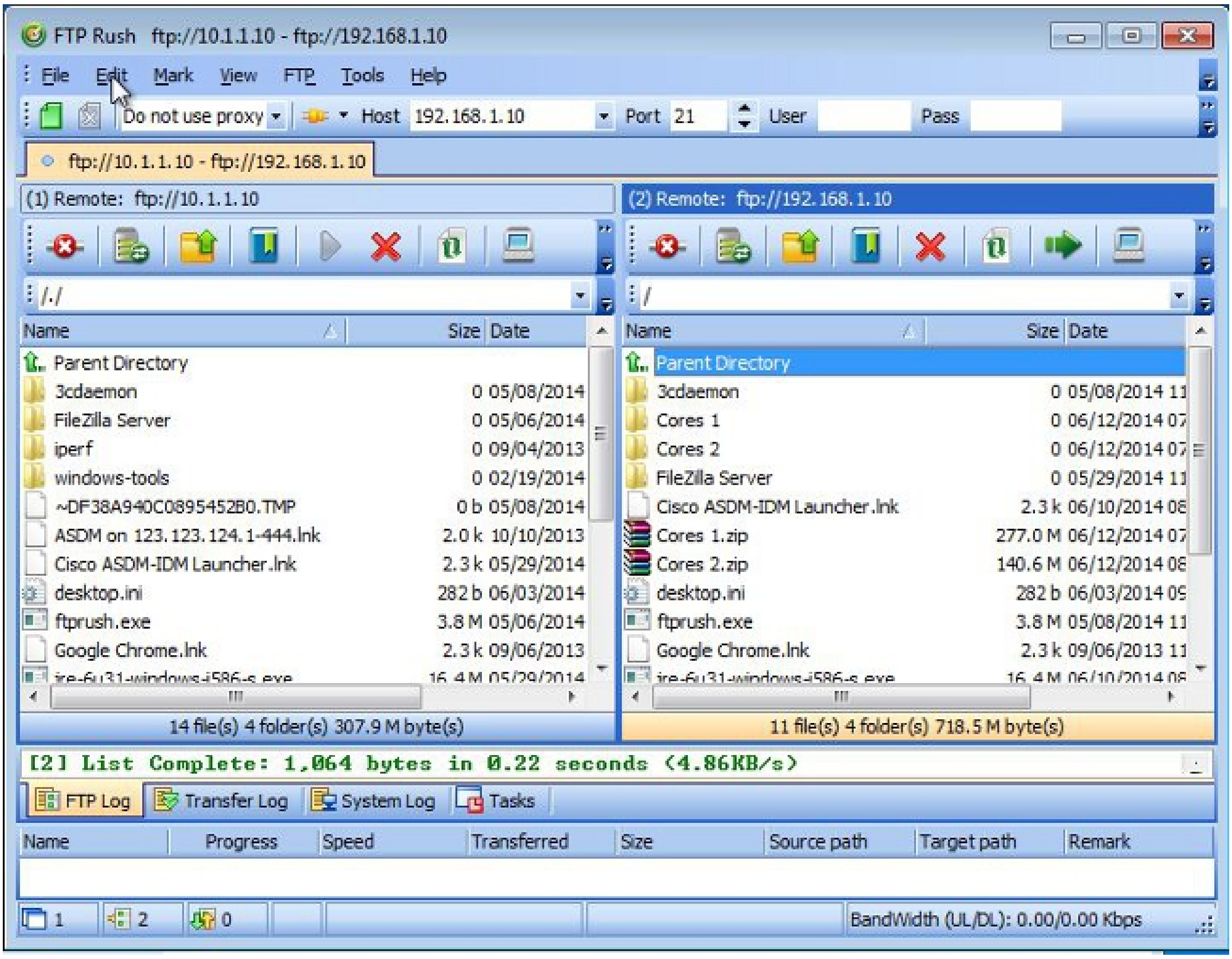
## File Transfer-proces

Voltooi deze stappen om een succesvolle bestandsoverdracht tussen de twee FTP-servers te controleren:

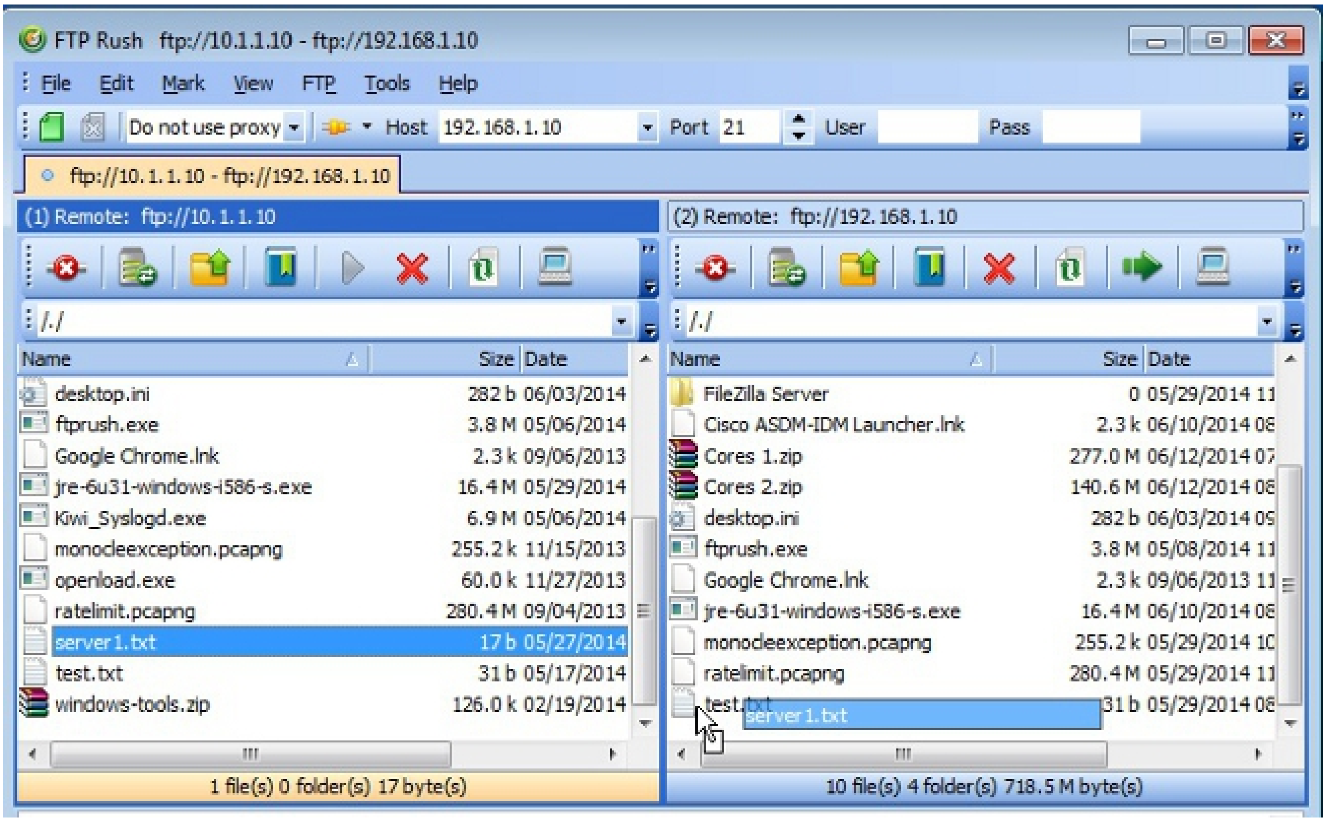
1. Aansluiting voor server1 vanaf de FXP-clientmachine:



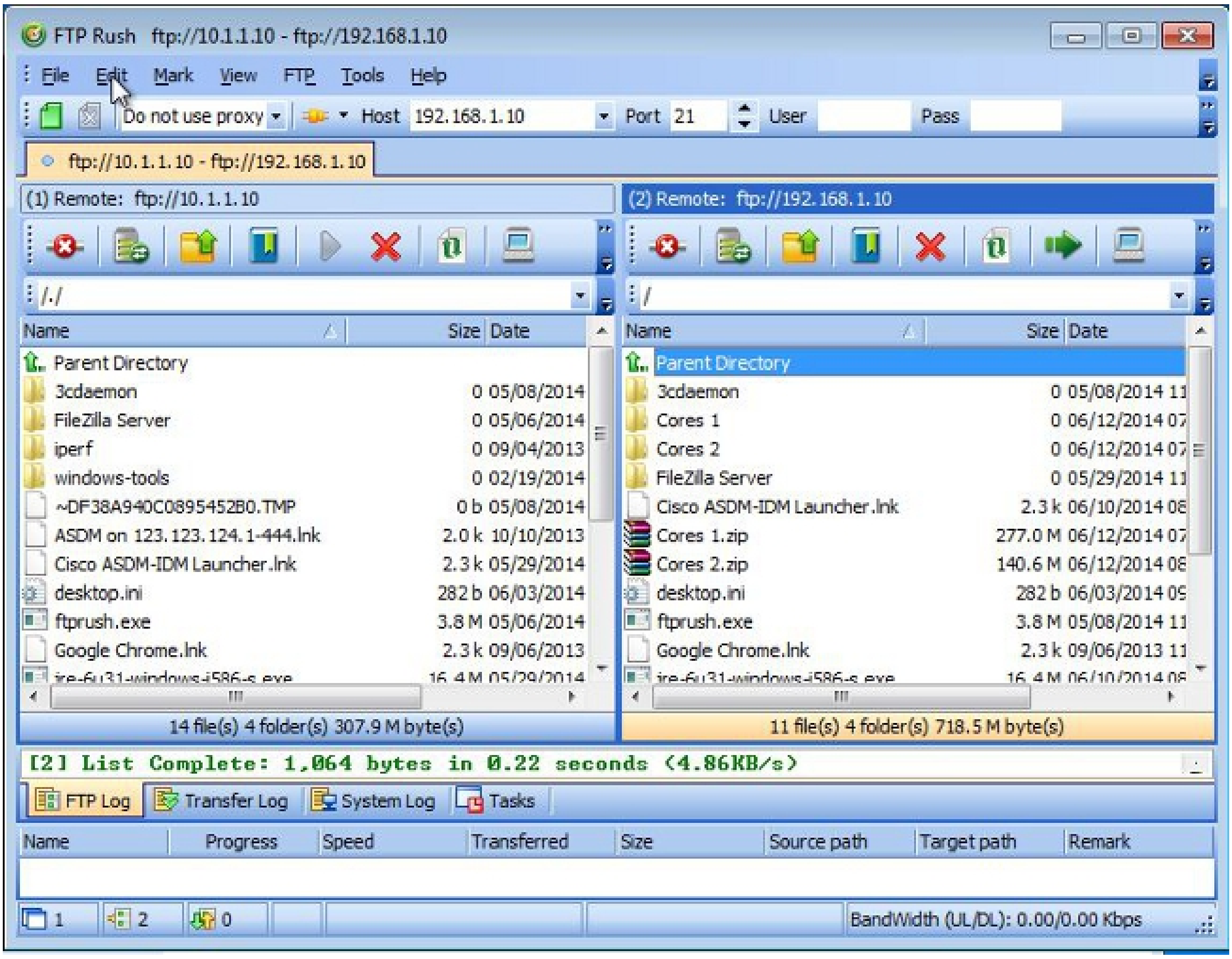

2. Aansluiting voor server2 vanaf de FXP client machine:




3. Sleep het bestand dat u vanuit het server1-venster naar het server2-venster wilt verplaatsen:



4. Controleer of de bestandsoverdracht geslaagd is:




# Problemen oplossen

Deze sectie verschaft opnames van twee verschillende scenario's die u kunt gebruiken om uw configuratie problemen op te lossen.

## Scenario voor FTP-inspectie uitgeschakeld

Als de FTP-inspectie is uitgeschakeld, zoals wordt beschreven in het gedeelte FTP-inspectie en FXP van dit document, verschijnen deze gegevens in de 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.
```

Hier volgen wat opmerkingen over deze gegevens:

- Het IP-adres van de client is **172.16.1.10**.

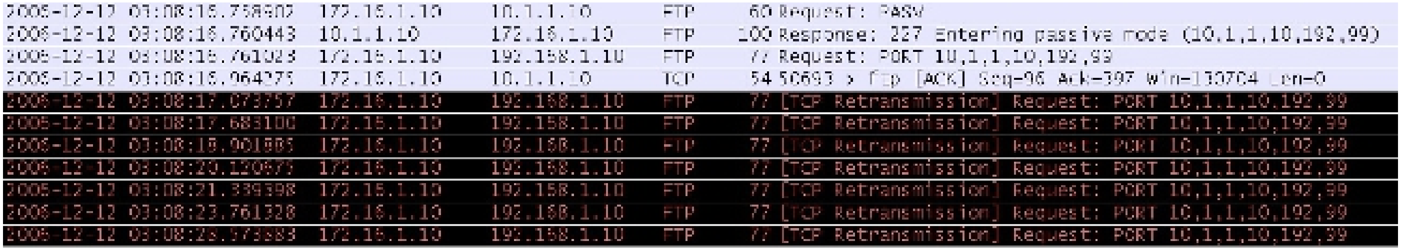
- Het Server1 IP-adres is **10.1.1.10**.

- Het Server2 IP adres is **192.168.1.10**.

In dit voorbeeld, het bestand genaamd **Kiwi_Syslogd.exe** wordt overgebracht van server1 naar server2.

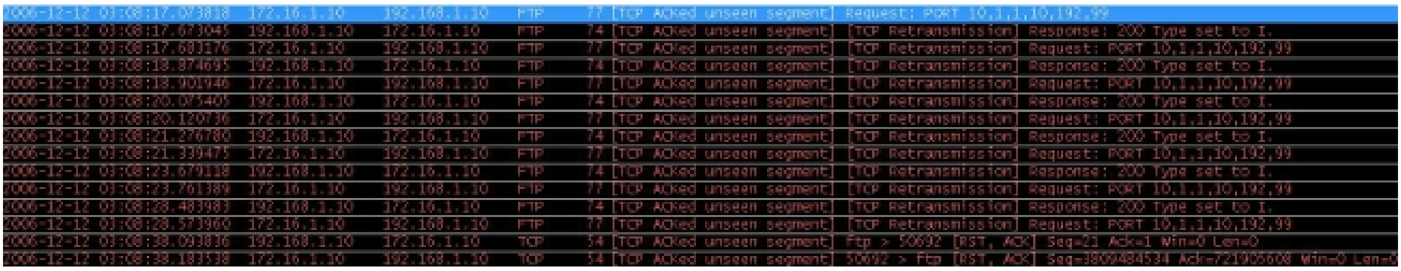
## FTP-inspectie ingeschakeld

Als FTP-inspectie is ingeschakeld, verschijnen deze gegevens in de ASA client-interface:



| | | | | | |
|---|---|---|---|---|---|
| 2006-12-12 03:08:16.758902 | 172.16.1.10 | 10.1.1.10 | FTP | 60 | Request: PASV |
| 2006-12-12 03:08:16.760443 | 10.1.1.10 | 172.16.1.10 | FTP | 100 | Response: 227 Entering passive mode (10,1,1,10,192,99) |
| 2006-12-12 03:08:16.761023 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:16.964275 | 172.16.1.10 | 10.1.1.10 | TCP | 54 | 50693 > ftp [ACK] Seq=96 Ack=397 Win=130704 Len=0 |
| 2006-12-12 03:08:17.073757 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:17.683100 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:18.901885 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:20.120675 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:21.339398 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:23.761328 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:28.573883 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |

Hier zijn de ASA druppelopnamen:



| | | | | | |
|---|---|---|---|---|---|
| 2006-12-12 03:08:17.073818 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP ACKed unseen segment] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:17.673045 | 192.168.1.10 | 172.16.1.10 | FTP | 74 | [TCP ACKed unseen segment] [TCP Retransmission] Response: 200 Type set to I. |
| 2006-12-12 03:08:17.683176 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP ACKed unseen segment] [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:18.874695 | 192.168.1.10 | 172.16.1.10 | FTP | 74 | [TCP ACKed unseen segment] [TCP Retransmission] Response: 200 Type set to I. |
| 2006-12-12 03:08:18.901946 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP ACKed unseen segment] [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:20.075405 | 192.168.1.10 | 172.16.1.10 | FTP | 74 | [TCP ACKed unseen segment] [TCP Retransmission] Response: 200 Type set to I. |
| 2006-12-12 03:08:20.120736 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP ACKed unseen segment] [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:21.276780 | 192.168.1.10 | 172.16.1.10 | FTP | 74 | [TCP ACKed unseen segment] [TCP Retransmission] Response: 200 Type set to I. |
| 2006-12-12 03:08:21.339475 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP ACKed unseen segment] [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:23.679118 | 192.168.1.10 | 172.16.1.10 | FTP | 74 | [TCP ACKed unseen segment] [TCP Retransmission] Response: 200 Type set to I. |
| 2006-12-12 03:08:23.761389 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP ACKed unseen segment] [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:28.483983 | 192.168.1.10 | 172.16.1.10 | FTP | 74 | [TCP ACKed unseen segment] [TCP Retransmission] Response: 200 Type set to I. |
| 2006-12-12 03:08:28.573960 | 172.16.1.10 | 192.168.1.10 | FTP | 77 | [TCP ACKed unseen segment] [TCP Retransmission] Request: PORT 10,1,1,10,192,99 |
| 2006-12-12 03:08:38.093836 | 192.168.1.10 | 172.16.1.10 | TCP | 54 | [TCP ACKed unseen segment] ftp > 50692 [RST, ACK] Seq=21 Ack=1 Win=0 Len=0 |
| 2006-12-12 03:08:38.183538 | 172.16.1.10 | 192.168.1.10 | TCP | 54 | [TCP ACKed unseen segment] 50692 > ftp [RST, ACK] Seq=3809484534 Ack=721905608 Win=0 Len=0 |

Het POORTverzoek wordt door de FTP-inspectie ingetrokken omdat het een IP-adres en -poort bevat die afwijken van het IP-adres en de poort van de client. Vervolgens wordt de verbinding met de server afgesloten door de inspectie.