ASA-Dateiübertragung mit FXP-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie das File eXchange Protocol (FXP) auf der Cisco Adaptive Security Appliance (ASA) über die CLI konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse des File Transfer Protocol (FTP) (Aktiv/Passiv-Modus) zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ASA, die Softwareversionen 8.0 und höher ausführt.

Hinweis: In diesem Konfigurationsbeispiel werden zwei Microsoft Windows-Workstations verwendet, die als FXP-Server fungieren und FTP-Dienste ausführen (3C Daemon). FXP ist ebenfalls aktiviert. Eine andere Microsoft Windows-Workstation, auf der FXP-Clientsoftware ausgeführt wird (FTP Rush), wird ebenfalls verwendet.

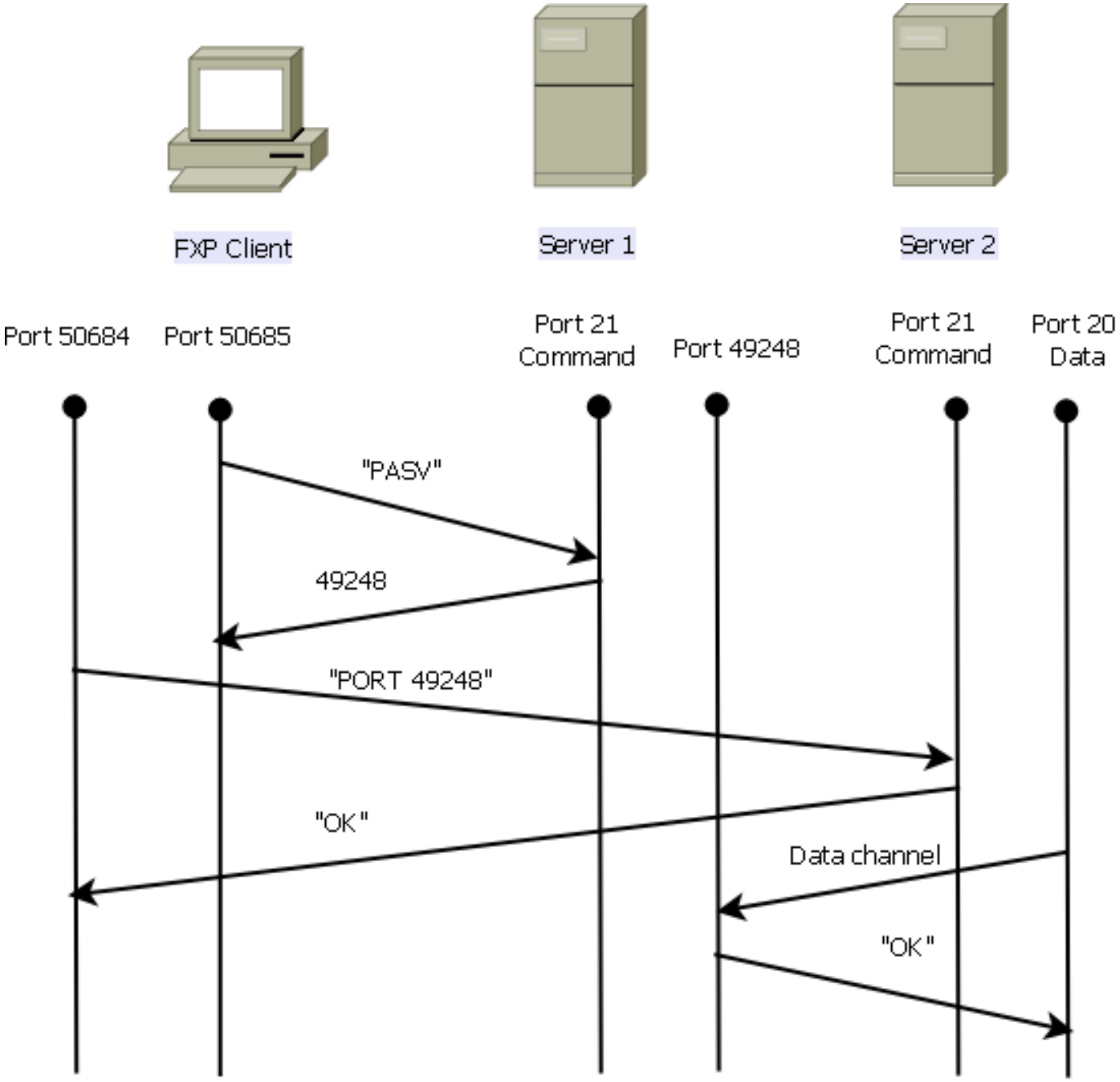
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Mit FXP können Sie Dateien von einem FTP-Server auf einen anderen FTP-Server über einen FXP-Client übertragen, ohne dass die Geschwindigkeit der Internetverbindung des Clients davon abhängen muss. Bei FXP hängt die maximale Übertragungsgeschwindigkeit nur von der Verbindung zwischen den beiden Servern ab, die normalerweise viel schneller ist als die Client-Verbindung. Sie können FXP in Szenarien anwenden, in denen ein Server mit hoher Bandbreite Ressourcen von einem anderen Server mit hoher Bandbreite benötigt, jedoch nur von einem Client mit niedriger Bandbreite, z. B. einem Netzwerkadministrator, der remote arbeitet, die Berechtigung hat, auf die Ressourcen auf beiden Servern zuzugreifen.

FXP dient als Erweiterung des FTP-Protokolls, und der Mechanismus ist in Abschnitt 5.2 des FTP-RFC 959 angegeben. Grundsätzlich initiiert der FXP-Client eine Steuerverbindung mit einem FTP-Server1, öffnet eine andere Steuerverbindung mit dem FTP-Server2 und ändert dann die Verbindungsattribute der Server, sodass sie aufeinander zeigen, sodass die Übertragung direkt zwischen den beiden Servern erfolgt.

Dateiübertragungsmechanismus über FXP



Im Folgenden finden Sie eine Übersicht über den Prozess:

1. Der Client öffnet eine Steuerverbindung mit Server1 am TCP-Port 21.

   Der Client sendet den **PASV-**Befehl an server1.

   Server1 antwortet mit seiner IP-Adresse und dem Port, an dem er abhört.

2. Der Client öffnet eine Steuerverbindung mit Server2 am TCP-Port 21.

   Der Client übergibt die Adresse/den Port, die von server1 an server2 über einen **PORT-**Befehl empfangen wird.

   Server2 antwortet, um den Client darüber zu informieren, dass der Befehl **PORT** erfolgreich ist. Server2 weiß jetzt, wo die Daten gesendet werden sollen.

3. So starten Sie den Übertragungsprozess von Server 1 zu Server 2:

   Der Client sendet den **STOR-**Befehl an server2 und weist ihn an, das empfangene Datum zu speichern.

   Der Client sendet den **RETR-**Befehl an server1 und weist ihn an, die Datei abzurufen oder zu übertragen.

4. Alle Daten werden jetzt direkt von der Quelle zum Ziel-FTP-Server übertragen. Beide Server melden Statusmeldungen nur bei Ausfall/Erfolg an den Client.

So wird die Verbindungstabelle angezeigt:

```
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-Prüfung und FXP

Die Dateiübertragung über ASA über FXP ist nur erfolgreich, wenn die FTP-Prüfung auf der ASA **deaktiviert** ist.

Wenn der FXP-Client eine IP-Adresse und einen TCP-Port angibt, die sich vom Client im FTP **PORT-**Befehl unterscheiden, wird eine unsichere Situation erstellt, in der ein Angreifer in der Lage ist, einen Port-Scan auf einen Host im Internet von einem FTP-Server eines Drittanbieters durchzuführen. Der Grund hierfür ist, dass der FTP-Server angewiesen wird, eine Verbindung zu einem Port auf einem Computer zu öffnen, der nicht der Client ist, von dem er stammt. Dies wird als **FTP-Bounce-Angriff** bezeichnet, und die FTP-Prüfung schließt die Verbindung, da sie dies als Sicherheitsverletzung betrachtet.

Hier ein Beispiel:

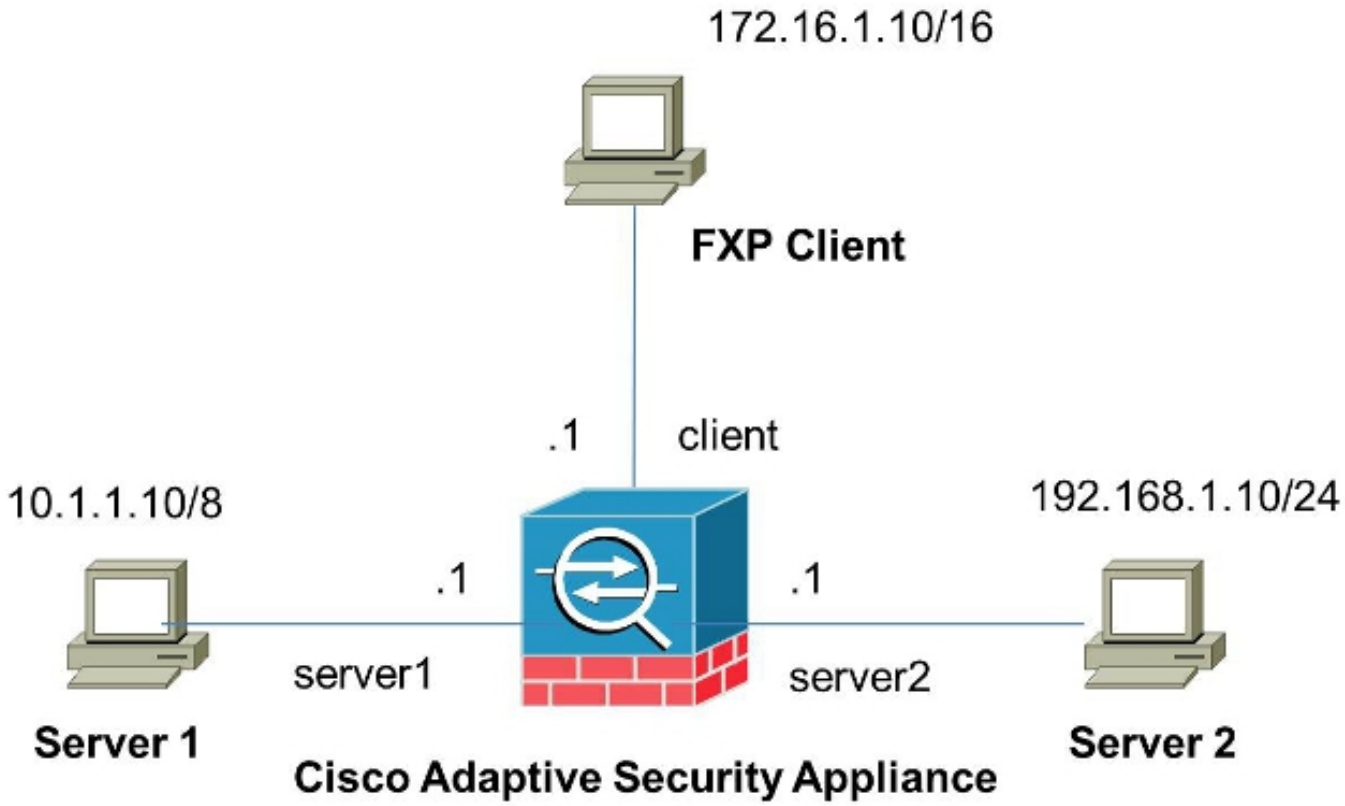
```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: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

Konfigurieren

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um FXP auf der ASA zu konfigurieren.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm



Konfigurieren der ASA über die CLI

Gehen Sie wie folgt vor, um die ASA zu konfigurieren:

1. FTP-Prüfung deaktivieren:

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

2. Konfigurieren Sie Zugriffslisten, um die Kommunikation zwischen dem FXP-Client und den beiden FTP-Servern zu ermöglichen:

```
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. Anwenden der Zugriffslisten auf die entsprechenden Schnittstellen:

```
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
```

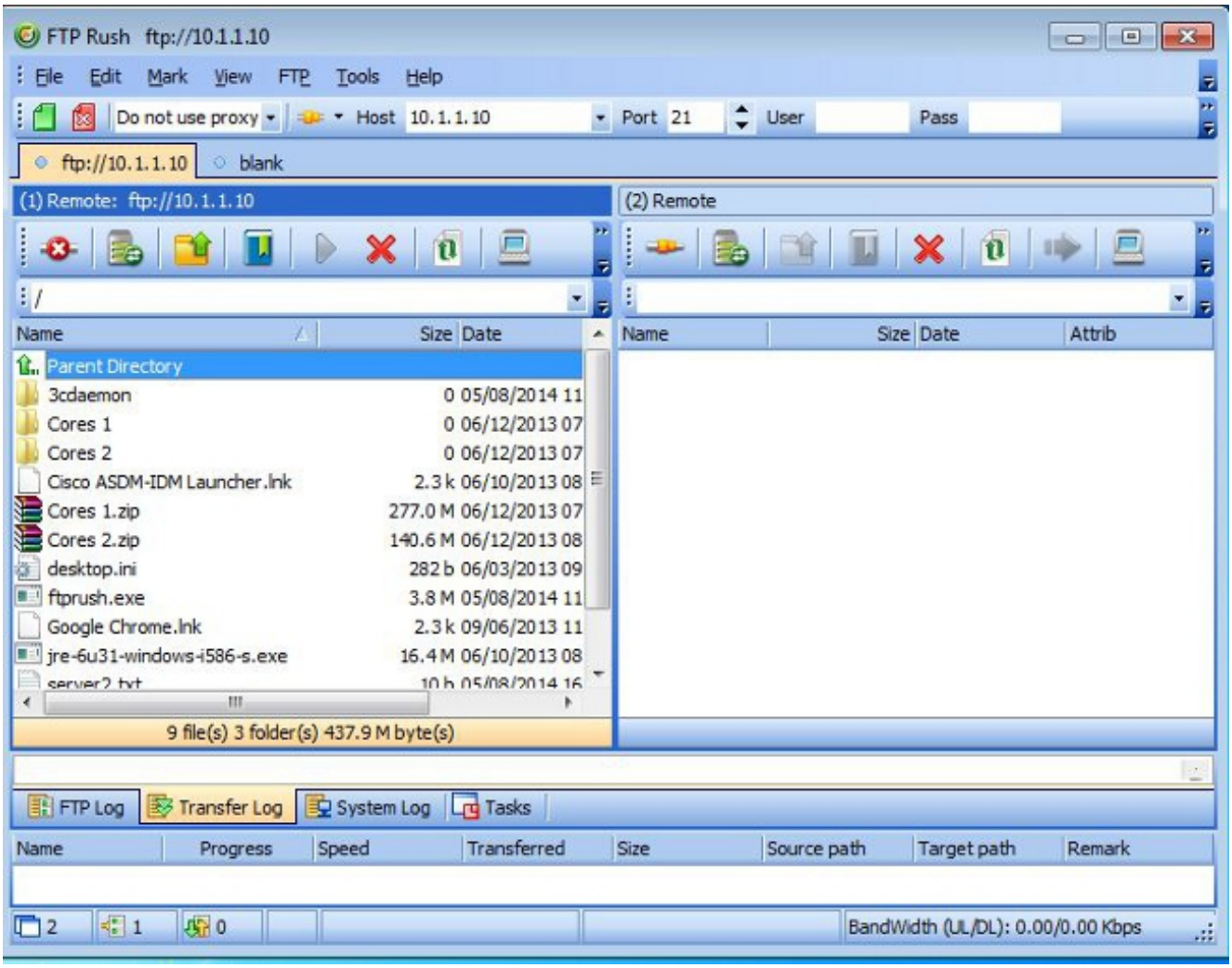
Überprüfen

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um sicherzustellen, dass Ihre Konfiguration ordnungsgemäß funktioniert.

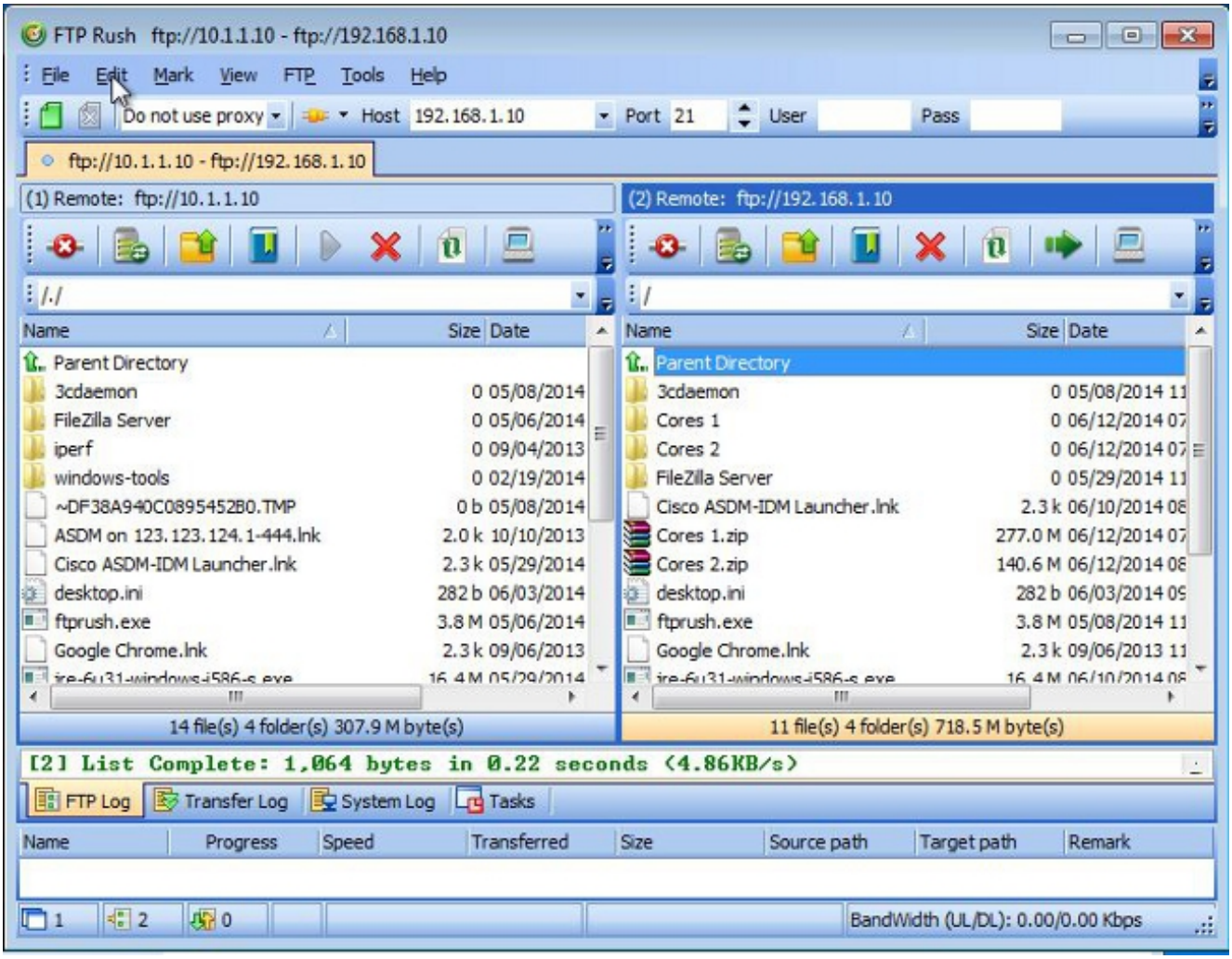
Dateiübertragungsvorgang

Gehen Sie wie folgt vor, um die erfolgreiche Dateiübertragung zwischen den beiden FTP-Servern zu überprüfen:

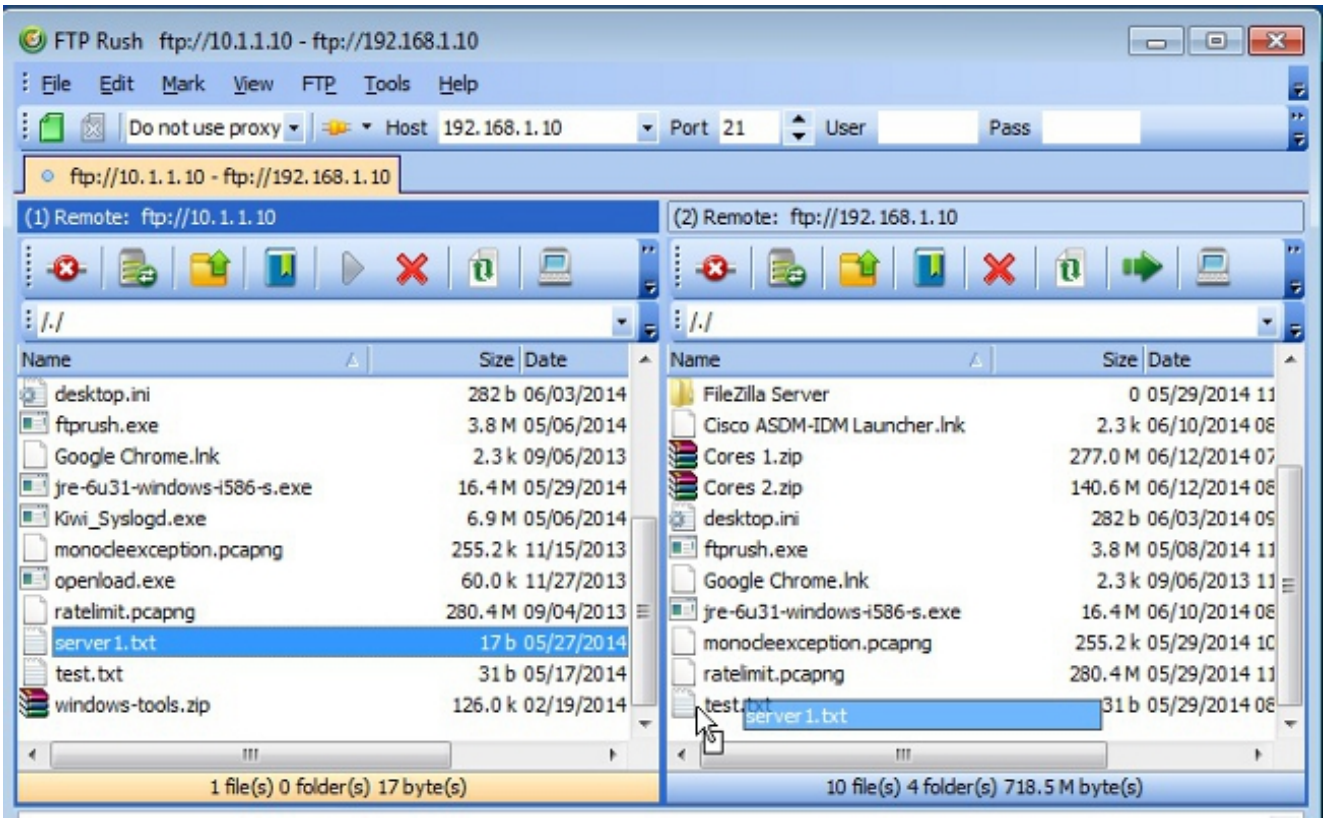
1. Stellen Sie vom FXP-Client-Computer eine Verbindung mit Server1 her:



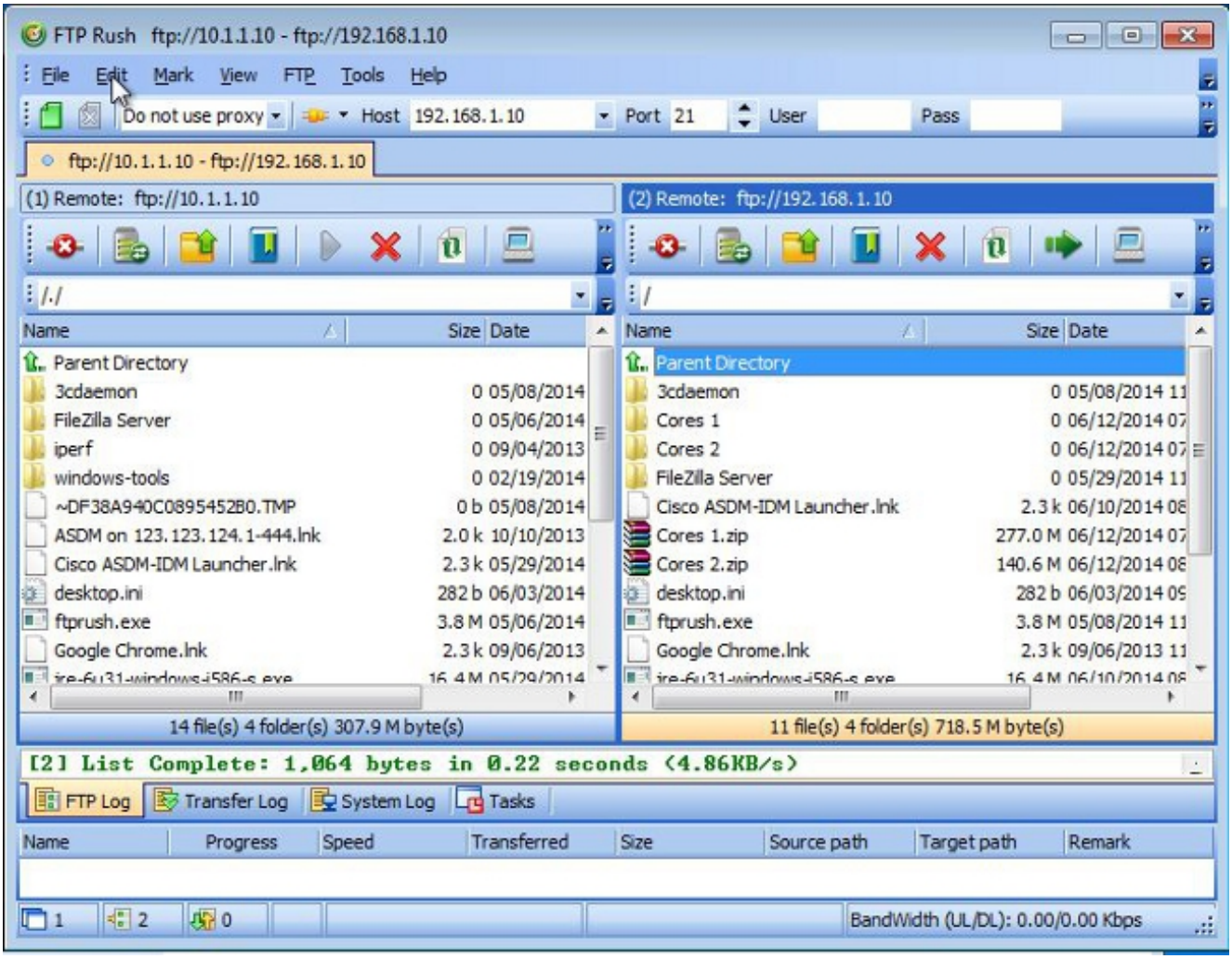
2. Stellen Sie vom FXP-Client-Computer eine Verbindung mit Server2 her:



3. Ziehen Sie die zu übertragende Datei aus dem Fenster server1 in das Fenster server2:



4. Überprüfen Sie, ob die Dateiübertragung erfolgreich verläuft:



Fehlerbehebung

Dieser Abschnitt enthält zwei verschiedene Szenarien, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

FTP-Prüfung deaktiviert

Wenn die FTP-Prüfung deaktiviert ist (siehe FTP Inspection und FXP Abschnitt dieses Dokuments), werden diese Daten auf der ASA-Client-Schnittstelle angezeigt:

```
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.
```

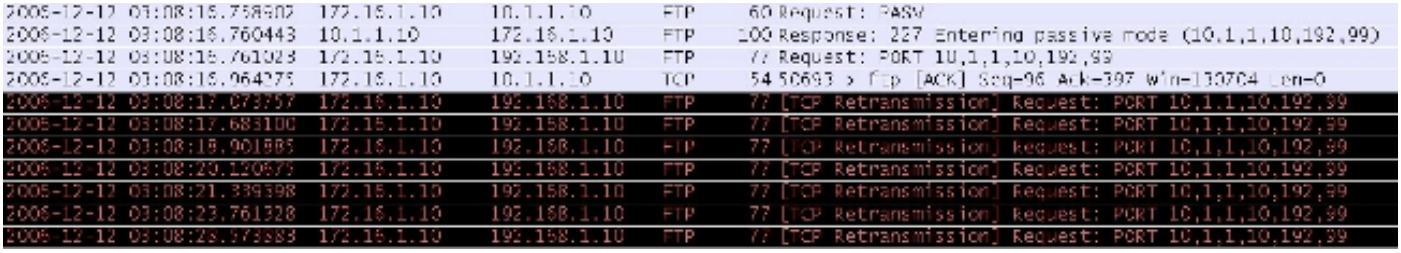
Hier einige Hinweise zu diesen Daten:

- Die Client-IP-Adresse lautet **172.16.1.10**.
- Die IP-Adresse von Server1 lautet **10.1.1.10**.
- Die IP-Adresse von Server2 lautet **192.168.1.10**.

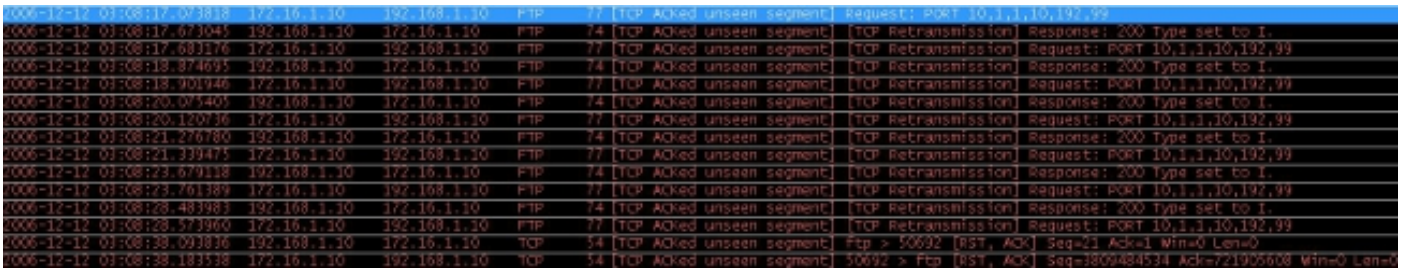
In diesem Beispiel wird die Datei **Kiwi_Syslogd.exe** von server1 auf server2 übertragen.

FTP-Prüfung aktiviert

Wenn die FTP-Prüfung aktiviert ist, werden diese Daten auf der ASA-Client-Schnittstelle angezeigt:



Hier sind die ASA-Drop-Capture:



Die **PORT-**Anforderung wird von der FTP-Prüfung verworfen, da sie eine IP-Adresse und einen Port enthält, die von der Client-IP-Adresse und dem Port abweichen. Anschließend wird die Steuerungsverbindung zum Server durch die Prüfung beendet.