ASA File Transfer with FXP 컨피그레이션 예

목차

소개

이 문서에서는 CLI를 통해 Cisco ASA(Adaptive Security Appliance)에서 FXP(File eXchange Protocol)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

FTP(File Transfer Protocol)(Active/Passive 모드)에 대한 기본적인 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 8.0 이상을 실행하는 Cisco ASA를 기반으로 합니다.

> **참고:**이 컨피그레이션 예에서는 FXP 서버 역할을 하고 FTP 서비스(3C 데몬)를 실행하는 두 개의 Microsoft Windows 워크스테이션을 사용합니다. 또한 FXP가 활성화되어 있습니다.FXP 클라이언트 소프트웨어(FTP Rush)를 실행하는 또 다른 Microsoft Windows 워크스테이션도 사용됩니다.

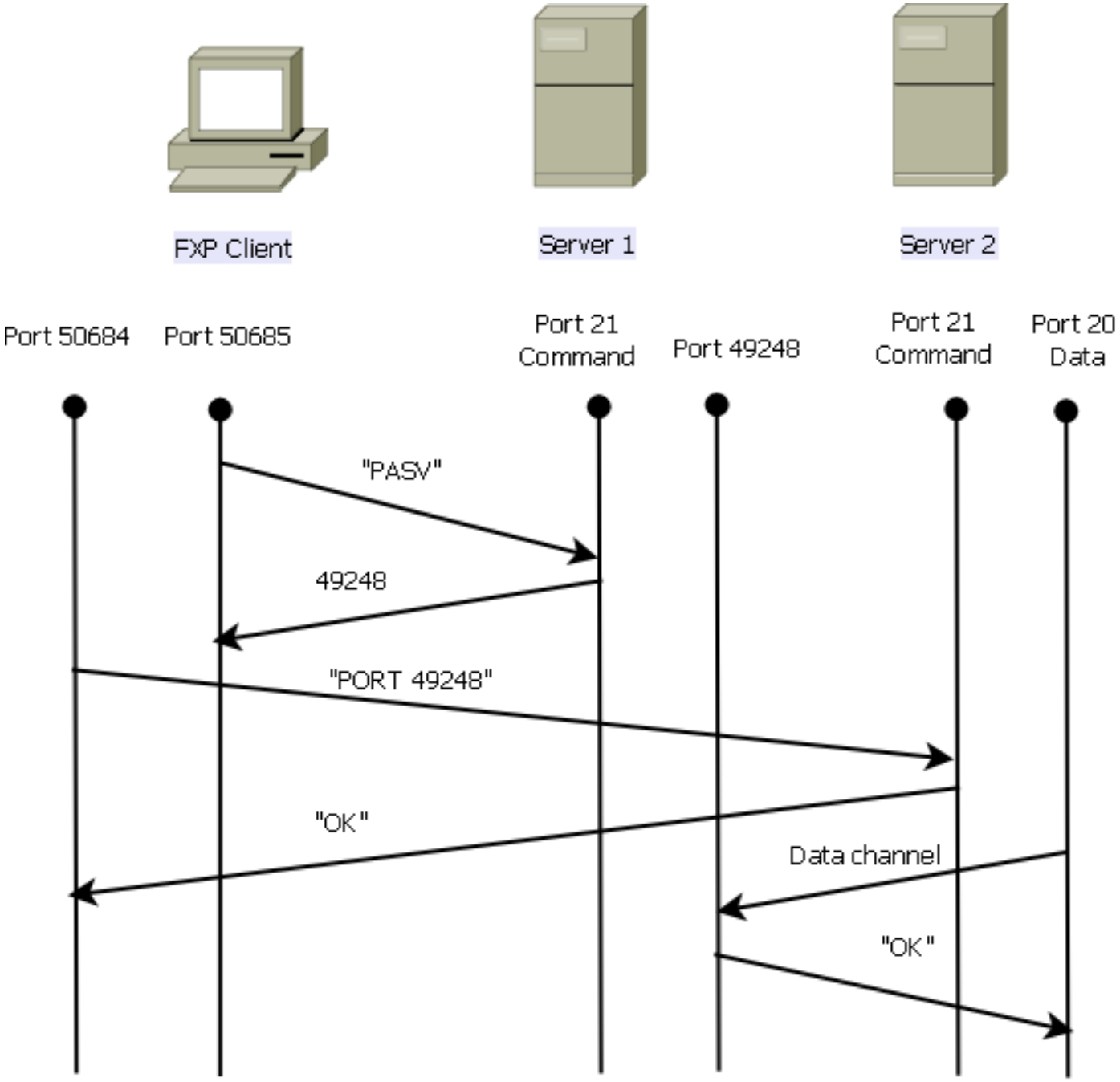
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

FXP를 사용하면 클라이언트 인터넷 연결 속도에 의존하지 않고도 FXP 클라이언트를 통해 한 FTP 서버에서 다른 FTP 서버로 파일을 전송할 수 있습니다.FXP의 경우 최대 전송 속도는 두 서버 간의 연결에만 의존하며, 이는 일반적으로 클라이언트 연결보다 훨씬 빠릅니다.고대역폭 서버가 다른 고대역폭 서버의 리소스를 필요로 하는 경우 FXP를 적용할 수 있지만, 원격으로 작동하는 네트워크 관리자와 같은 저대역폭 클라이언트만이 두 서버의 리소스에 액세스할 수 있습니다.

FXP는 FTP 프로토콜의 확장으로 작동하며 메커니즘은 FTP RFC 959의 섹션 5.2에 설명되어 있습니다. 기본적으로 FXP 클라이언트는 FTP server1과의 제어 연결을 시작하고 FTP server2와의 다른 제어 연결을 연 다음 서버의 연결 특성을 수정하여 두 서버 간에 전송이 직접 이루어지도록 합니다.

FXP를 통한 파일 전송 메커니즘



프로세스 개요는 다음과 같습니다.

1. 클라이언트는 TCP 포트 21에서 server1과의 제어 연결을 엽니다.

   클라이언트는 PASV 명령을 server1에 전송합니다.

   Server1은 IP 주소 및 수신 대기하는 포트로 응답합니다.

2. 클라이언트는 TCP 포트 21에서 server2와의 제어 연결을 엽니다.

   클라이언트는 server1에서 server2로 수신되는 주소/포트를 PORT 명령에서 **전달합니다**.

   Server2는 클라이언트에 **PORT** 명령이 성공했음을 알리기 위해 응답합니다.이제 Server2에서 데이터를 전송할 위치를 알 수 있습니다.

3. server1에서 server2로의 전송 프로세스를 시작하려면

클라이언트는 **STOR** 명령을 server2에 전송하고 수신한 날짜를 저장하도록 지시합니다.

클라이언트는 RETR 명령**을 server**1에 전송하고 파일을 검색하거나 전송하도록 지시합니다.

4. 이제 모든 데이터가 소스에서 대상 FTP 서버로 직접 이동합니다.두 서버 모두 실패/성공 시 상태 메시지만 클라이언트에 보고합니다.

연결 테이블이 표시되는 방식은 다음과 같습니다.

```
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 검사 및 FXP

FXP를 통해 ASA를 통한 파일 전송은 ASA에서 FTP 검사가 **비활성화된** 경우에만 성공합니다.

FXP 클라이언트가 FTP **PORT** 명령의 클라이언트 포트와 다른 IP 주소 및 TCP 포트를 지정하는 경우 공격자가 서드파티 FTP 서버에서 인터넷의 호스트에 대해 포트 스캔을 수행할 수 있는 비보안 상황이 생성됩니다.이는 FTP 서버가 시작된 클라이언트가 아닐 수 있는 시스템의 포트에 대한 연결을 열도록 지시되기 때문입니다.이를 **FTP 바운스 공격**이라고 하며, FTP 검사는 이를 보안 위반이라고 간주하여 연결을 종료합니다.

예를 들면 다음과 같습니다.

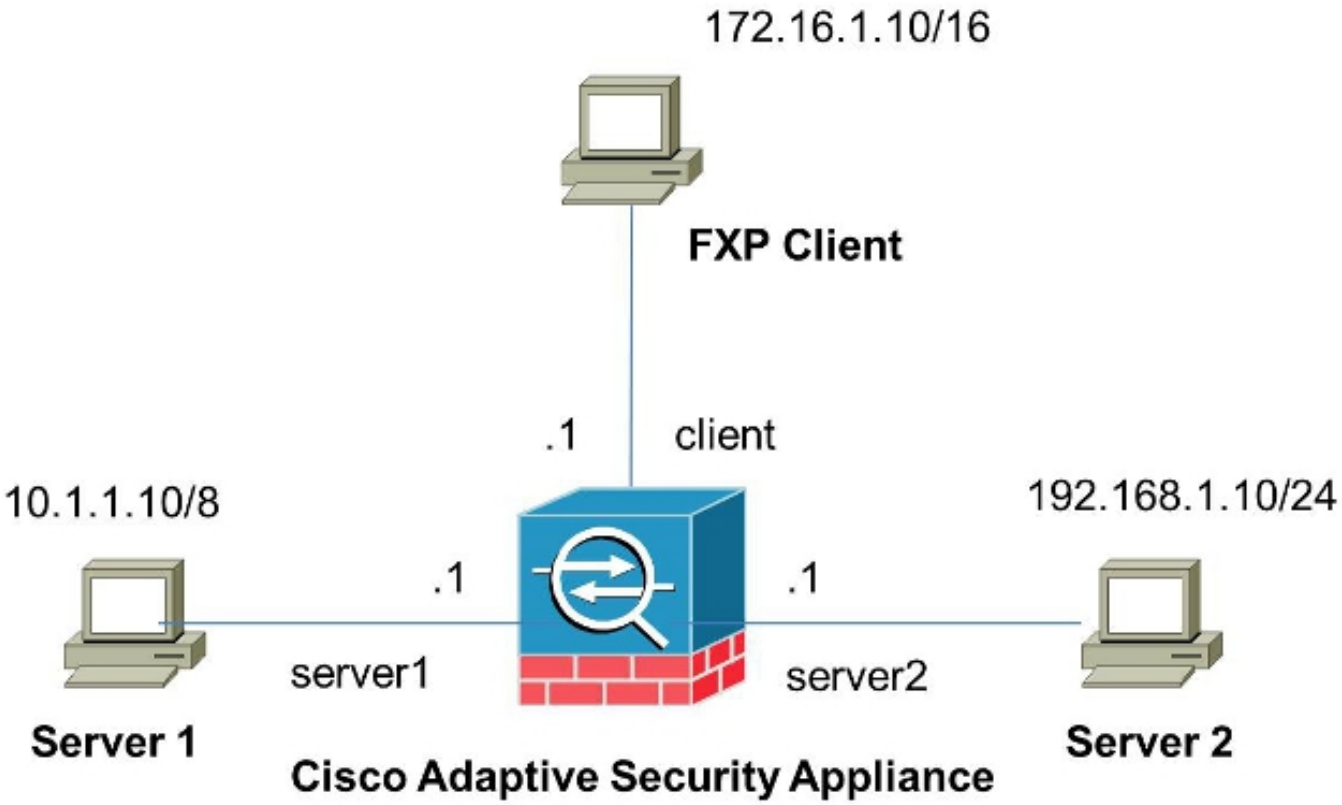
```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: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

구성

ASA에서 FXP를 구성하려면 이 섹션에 설명된 정보를 사용합니다.

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램



CLI를 통해 ASA 구성

ASA를 구성하려면 다음 단계를 완료합니다.

1. FTP 검사 사용 안 함:

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

2. FXP 클라이언트와 두 FTP 서버 간의 통신을 허용하려면 액세스 목록을 구성합니다.

```
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. 각 인터페이스에 액세스 목록을 적용합니다.

```
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
```

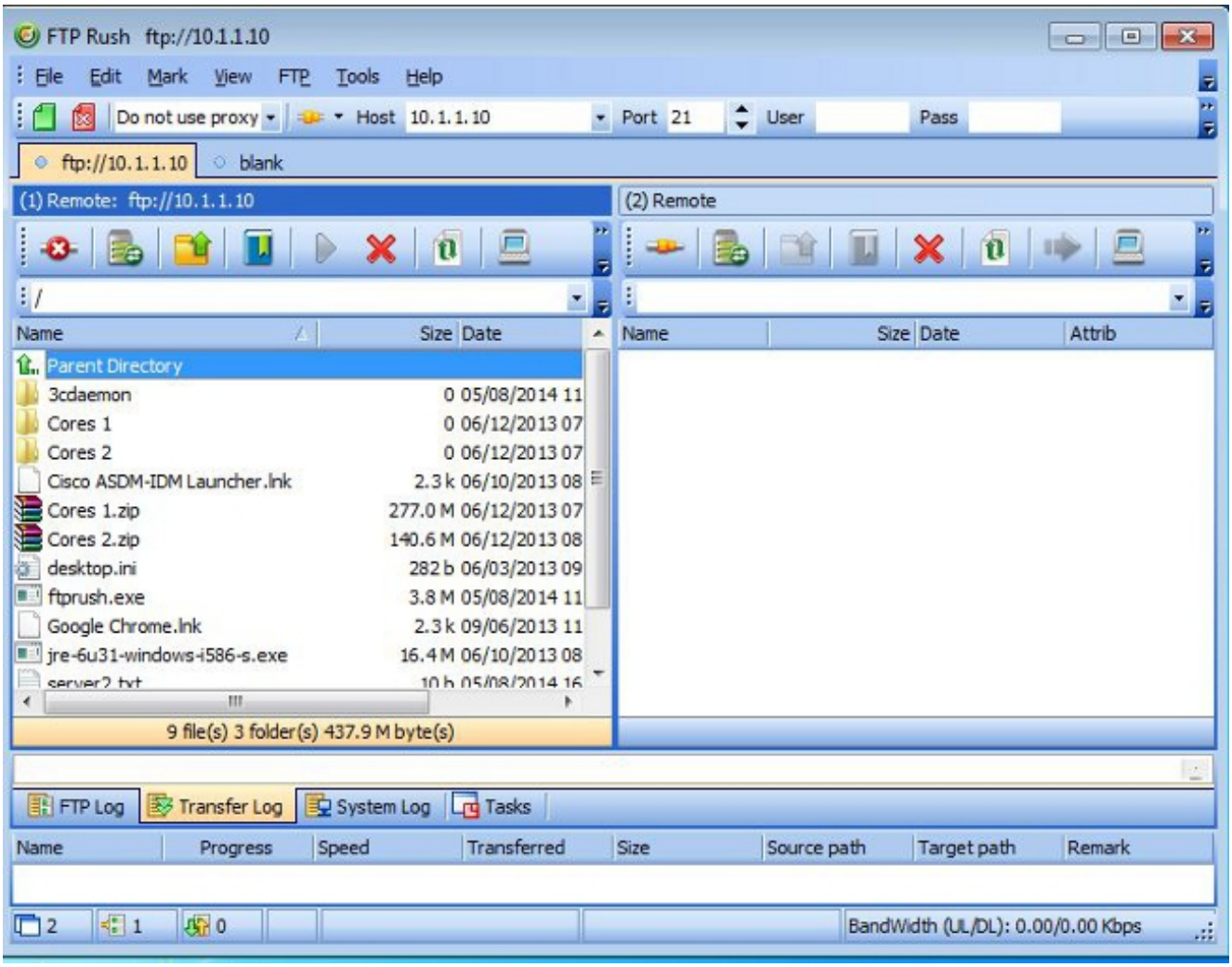
다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 이 섹션에 설명된 정보를 사용하십시오.

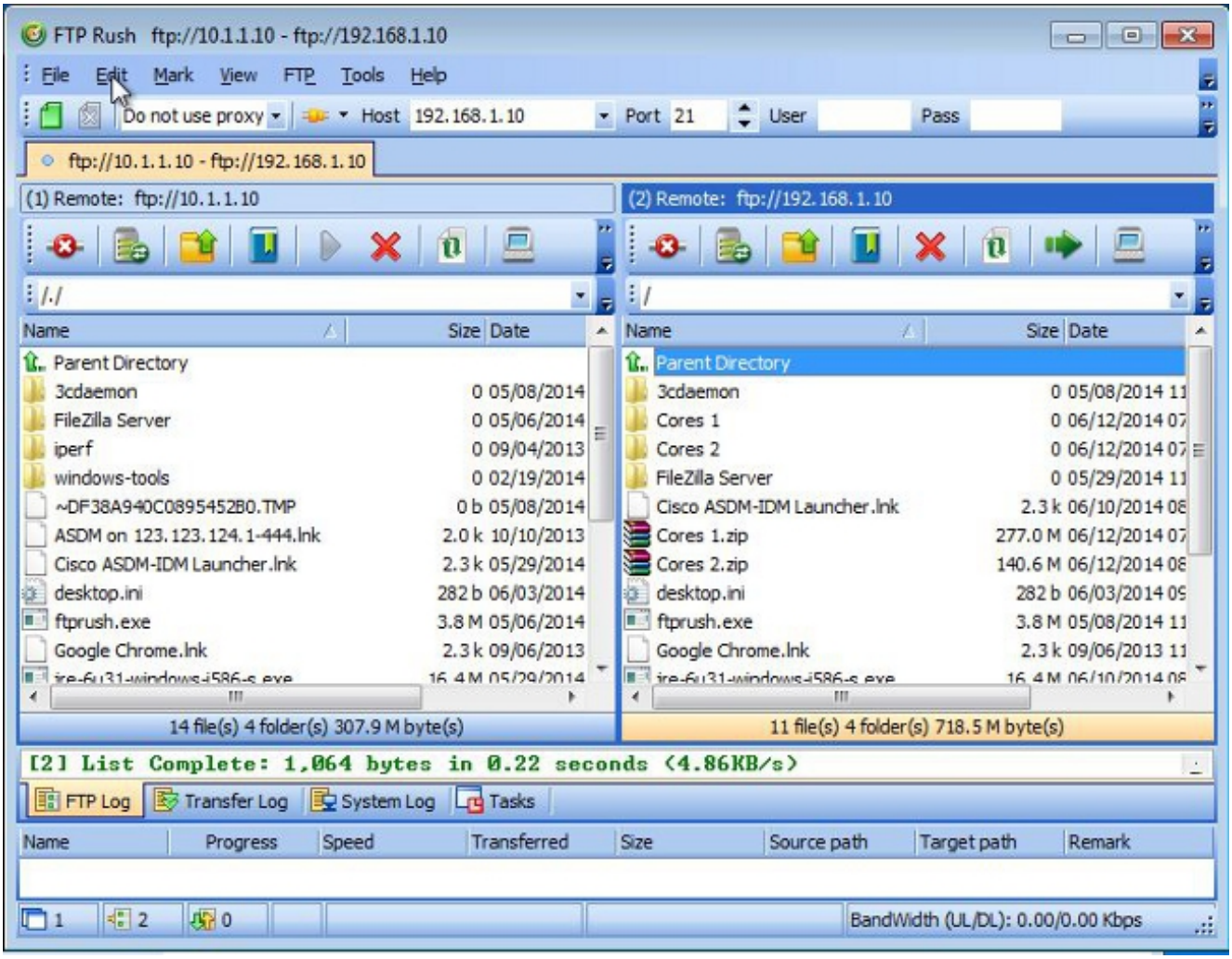
파일 전송 프로세스

두 FTP 서버 간에 파일 전송이 성공했는지 확인하려면 다음 단계를 완료하십시오.

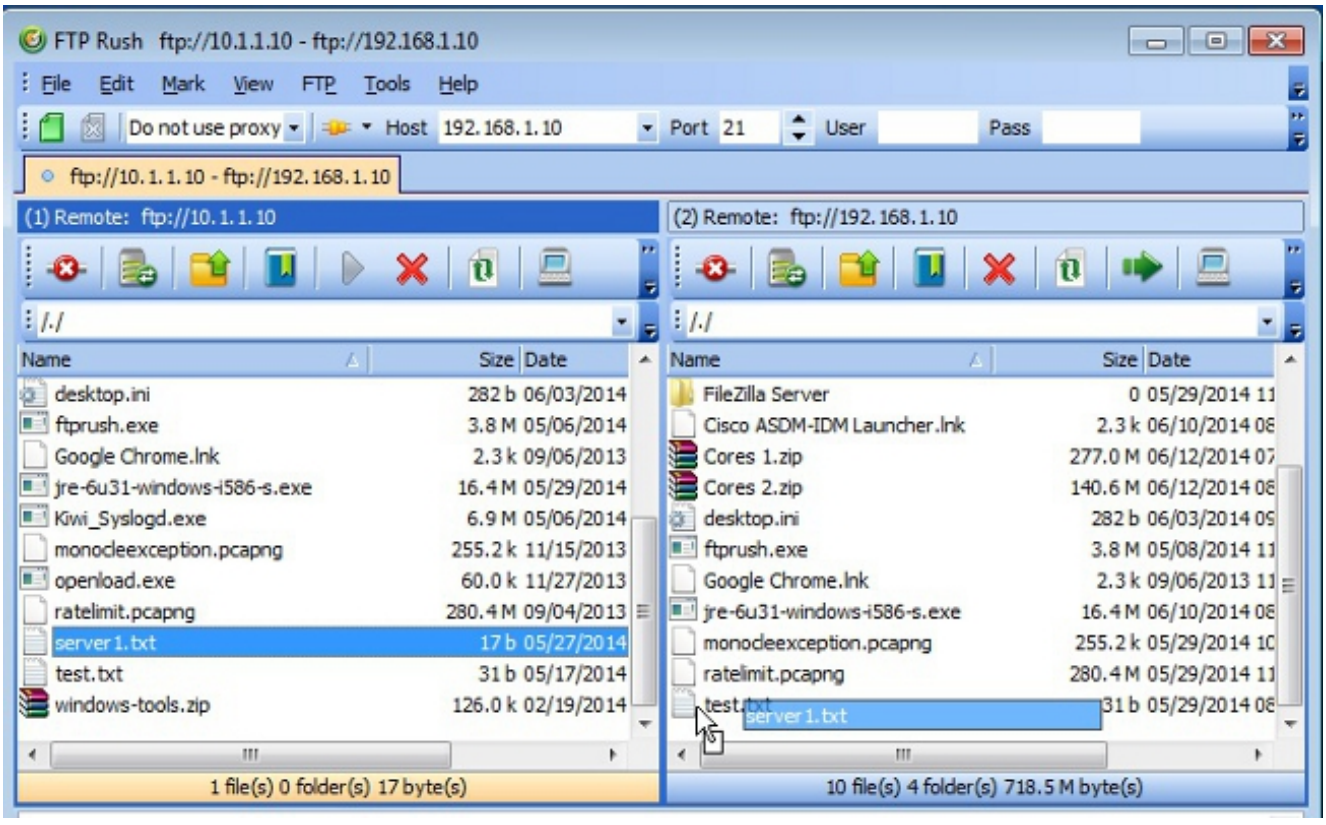
1. FXP 클라이언트 시스템에서 server1에 연결합니다.



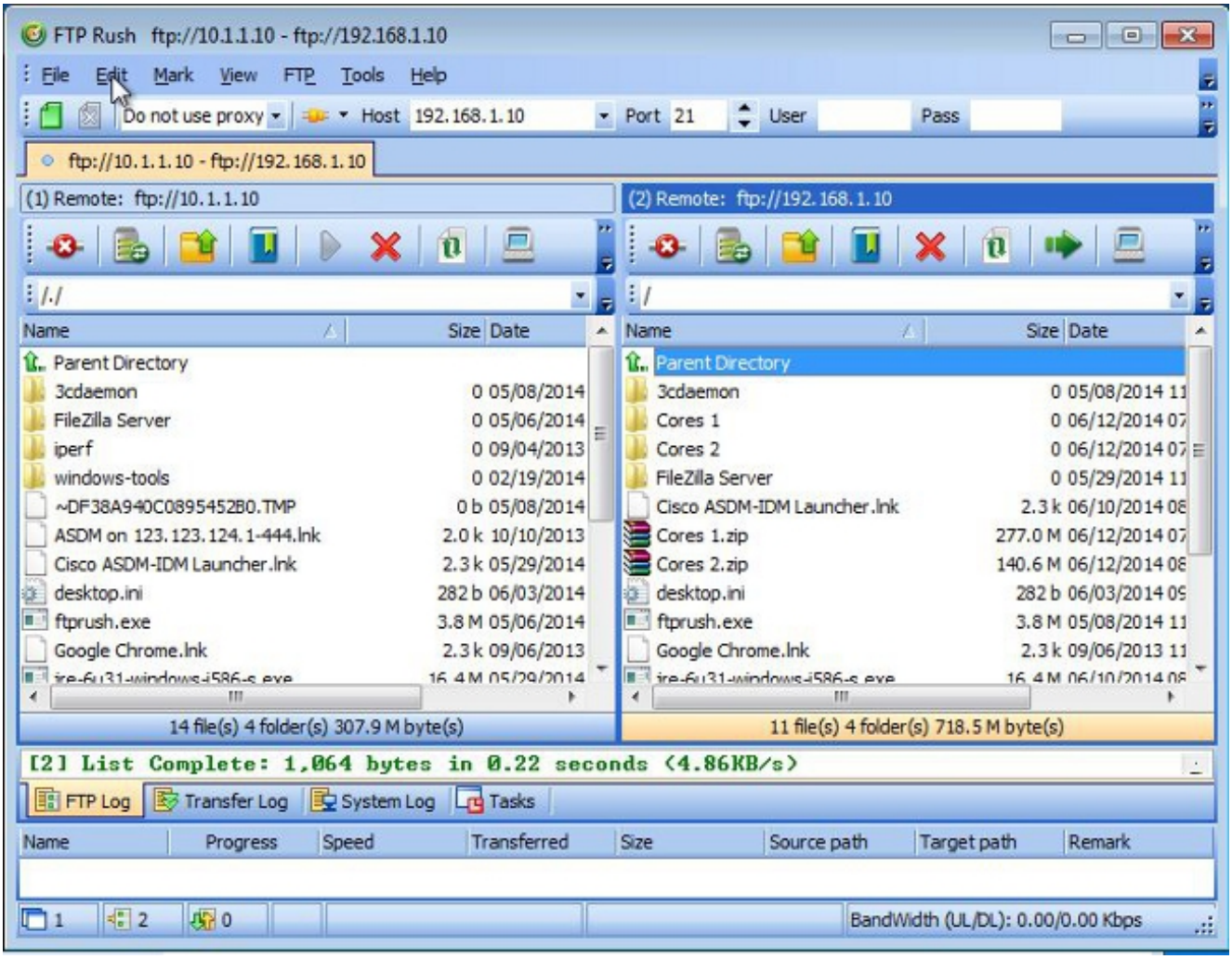
2. FXP 클라이언트 시스템에서 server2에 연결:



3. server1 창에서 server2 창으로 전송할 파일을 끌어서 놓습니다.



4. 파일 전송이 성공했는지 확인합니다.



문제 해결

이 섹션에서는 컨피그레이션 트러블슈팅을 위해 사용할 수 있는 두 가지 시나리오의 캡처를 제공합니다.

FTP 검사 사용 안 함 시나리오

FTP 검사가 비활성화되면 이 문서의 FTP Inspection 및 FXP 섹션에 자세히 설명된 대로 이 데이터가 ASA 클라이언트 인터페이스에 나타납니다.

```
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.
```

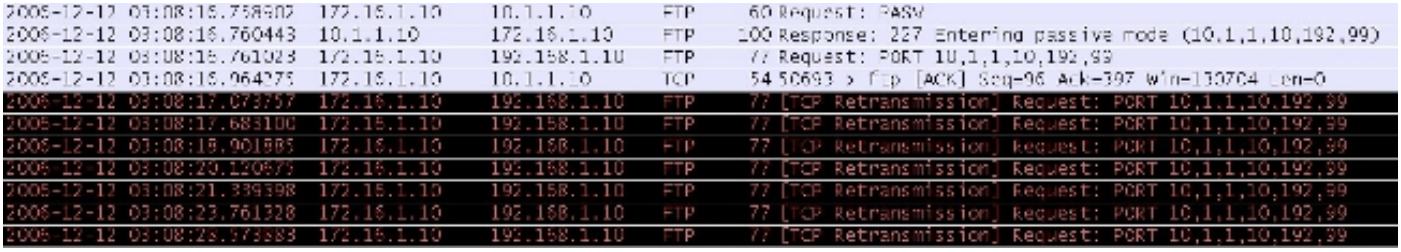
다음은 이 데이터에 대한 몇 가지 참고 사항입니다.

- 클라이언트 IP 주소는 **172.16.1.10입니다**.
- Server1 IP 주소는 **10.1.1.10입니다**.
- Server2 IP 주소는 **192.168.1.10입니다**.

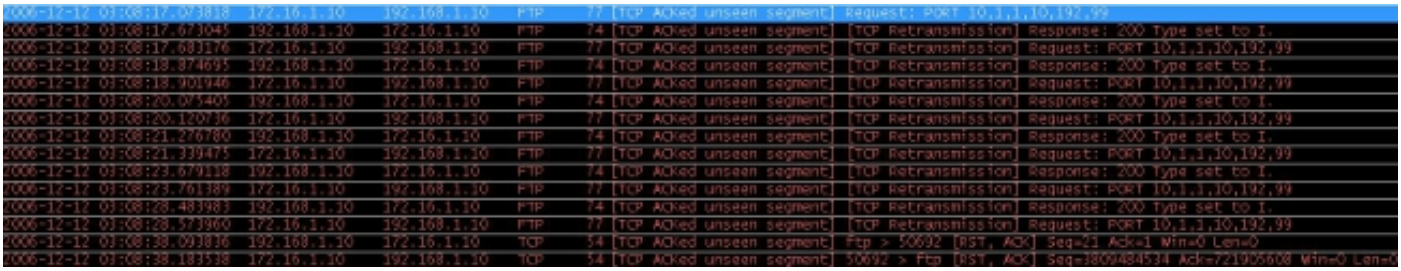
이 예에서 Kiwi_**Syslogd.exe**라는 파일이 server1에서 server2로 전송됩니다.

FTP 검사 사용

FTP 검사가 활성화되면 이 데이터가 ASA 클라이언트 인터페이스에 나타납니다.



다음은 ASA 삭제 캡처입니다.



PORT 요청은 클라이언트 IP 주소 및 포트와 다른 IP 주소 및 포트를 포함하므로 FTP 검사에 의해 삭제됩니다.그런 다음 검사 때문에 서버에 대한 제어 연결이 종료됩니다.