FXP を使用した ASA ファイル転送の設定例

内容

概要

このドキュメントでは、CLI で Cisco 適応型セキュリティ アプライアンス（ASA）の File eXchange Protocol（FXP）を設定する方法について説明します。

前提条件

要件

このドキュメントの読者は File Transfer Protocol（FTP）（アクティブ/パッシブ モード）の基本的な知識を持っていることを推奨します。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 8.0.x 以降が稼働する Cisco ASA に基づいています。

> **注**：この設定例は、FXP サーバおよび実行 FTP サービス（3C デーモン）として機能する 2 つの Microsoft Windows ワークステーションを使用します。 また、それぞれの FXP を有効

化します。FXP クライアント ソフトウェア（FTP Rush）を実行する別の Microsoft Windows ワークステーションも使用します。

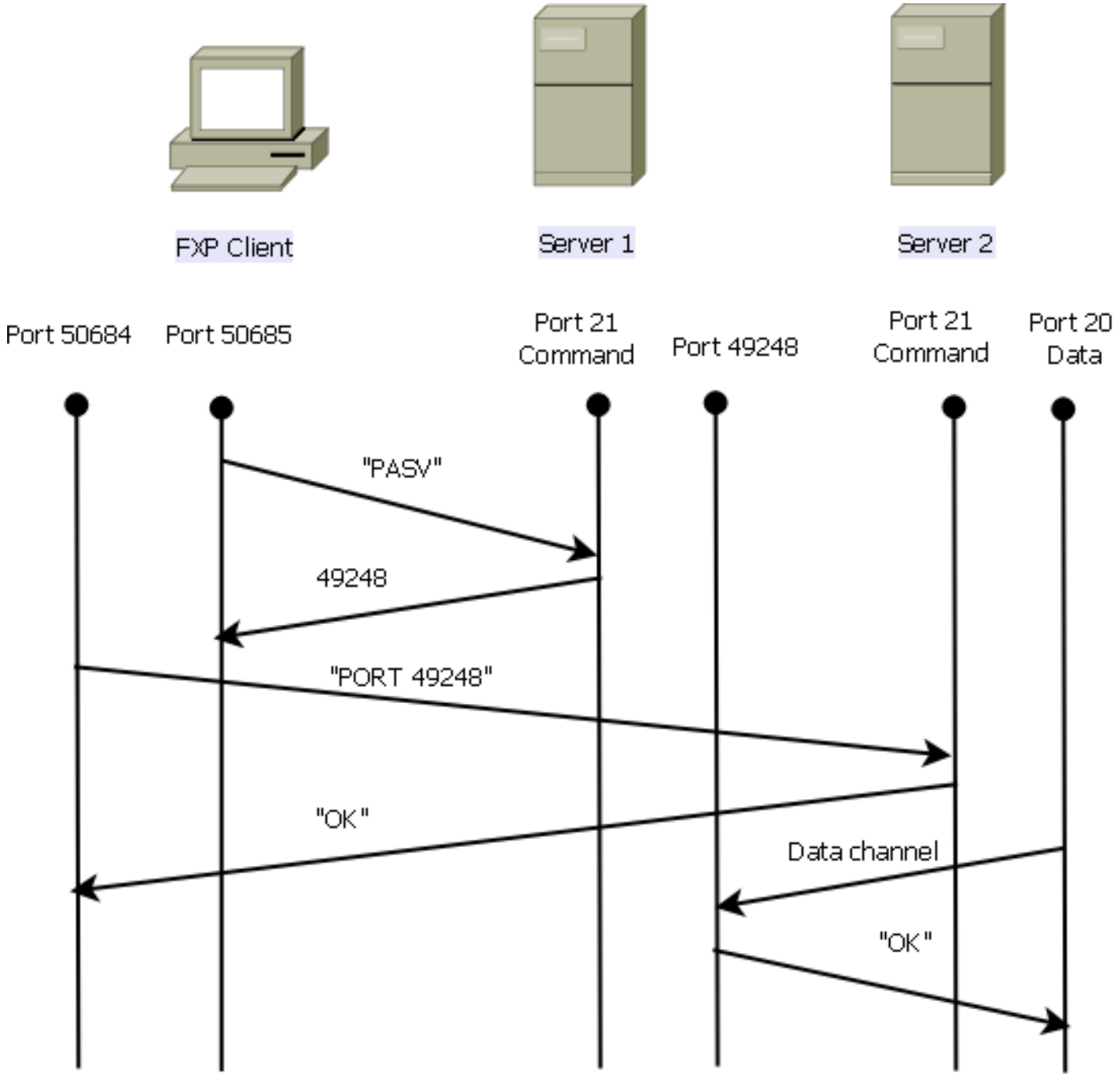
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

FXP はクライアントのインターネット接続速度に依存することなく、FXP クライアントを経由して FTP サーバから別の FTP サーバにファイルを転送することができます。FXP では、最大転送速度は、 2 つのサーバ間の接続のみに依存し、通常、クライアント接続よりもはるかに高速です。高帯域幅のサーバが別の高帯域幅サーバからリソースを要求する場合に FXP を適用できますが、リモートで動作するネットワーク管理者などの低帯域幅のクライアントのみに両方のサーバのリソースにアクセスする権限があります。

FXPはFTPプロトコルの拡張として動作し、機構はFTP RFC 959のセクション5.2に記載されています。基本的に、FTP server1との制御接続を開始し、FTP server2との別の制御接続を開き、2台のサーバ間で転送が直接行われるようにわれます。

FXP によるファイル転送のメカニズム



プロセスの概要を次に示します。

1. クライアントが server1 の TCP ポート 21 で制御接続を開きます。

   クライアントは server1 に**PASV コマンドを送信します。**

   server1 が IP アドレスとリッスンしているポートで応答します。

2. クライアントが server2 の TCP ポート 21 で制御接続を開きます。

   クライアントは **PORT コマンドで server1 から受信したアドレスとポートを server2 に渡します。**

   server2 は PORT コマンドが正常であることをクライアントに通知するために応答します。これで、server2 はデータの送信先を確認できました。

3. server1 から server2 への送信プロセスを開始するために次の動作が実行されます。

   クライアントは server2 に **STOR コマンドを送信し、受信した日付を保存するように指示します。**

   クライアントは server1 に **RETR コマンドを送信し、ファイルの取得または送信を指示します。**

4. これで、データはすべて、送信元から宛先 FTP サーバに直接送信されます。両方のサーバはクライアントに失敗または成功のステータス メッセージを報告するだけます。

接続テーブルの表示は次のとおりです。

```
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 インスペクションおよび FXP

FXP 経由の ASA までのファイル転送は FTP インスペクションが ASA で**無効の場合にのみ成功します。**

FXP クライアントが FTP PORT コマンドのクライアントのものとは異なる IP アドレスおよび TCP ポートを指定する場合、攻撃者がサードパーティの FTP サーバからインターネットにあるホストに対してポート スキャンを実行できるというセキュリティに問題がある状況になります。これは、FTP サーバが、発信元ではないクライアントの可能性があるマシンのポートに対し接続を開くことをに指示されるためです。これは **FTP バウンス攻撃**と呼ばれ、FTP インスペクションはこれをセキュリティ違反と見なして接続をシャットダウンします。

以下が一例です。

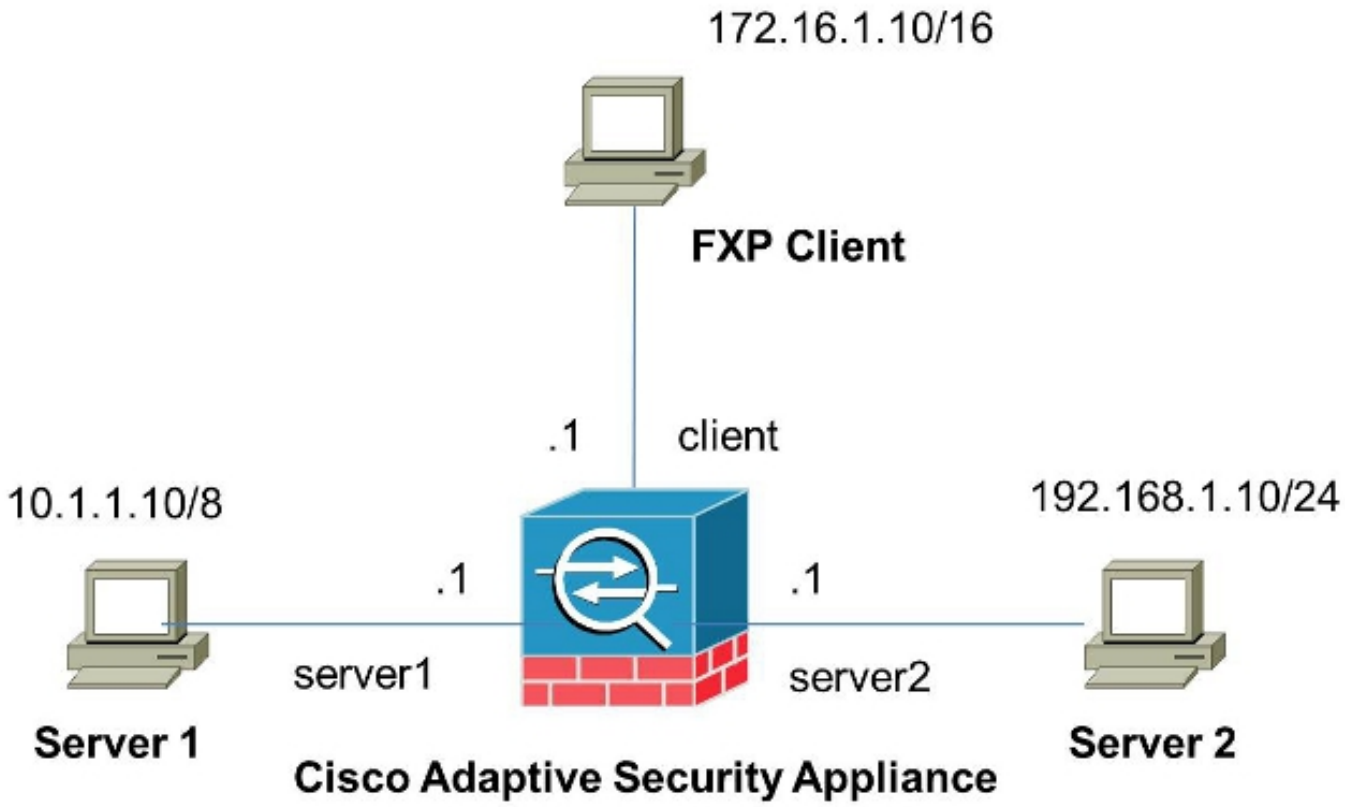
```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: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

設定

ASA の FXP を設定するためにこの項で説明されている情報を活用してください。

> **注：**このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図



CLI による ASA の設定

ASA を設定するには、次の手順を実行します。

1. FTP インスペクションを無効にします。

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

2. FXP クライアントと 2 つの FTP サーバ間の通信を許可するアクセス リストを設定します。

```
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. アクセス リストをそれぞれのインターフェイスに適用します。

```
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
```

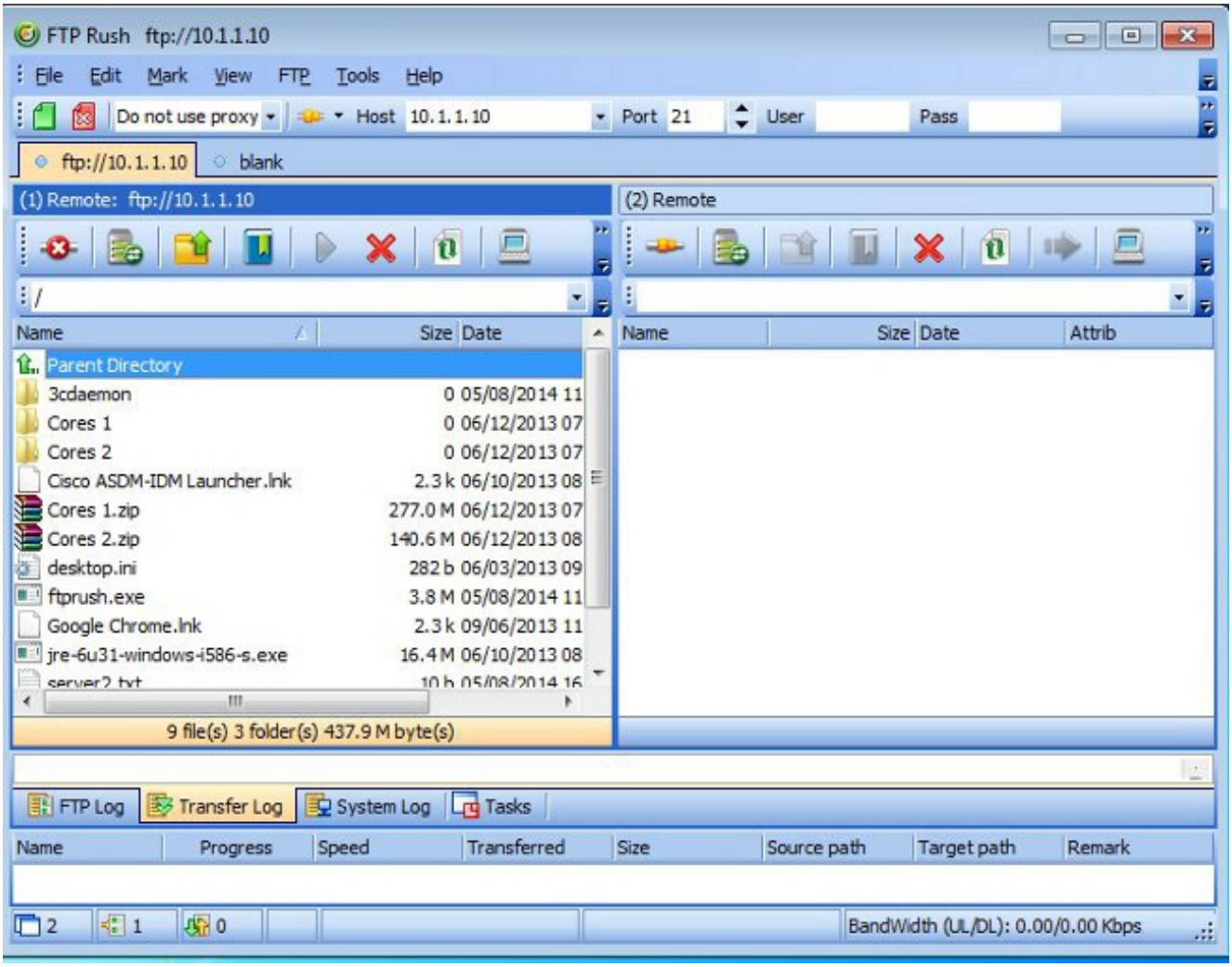
確認

設定が適切に機能することを検証するためにこの項で説明されている情報を活用してください。

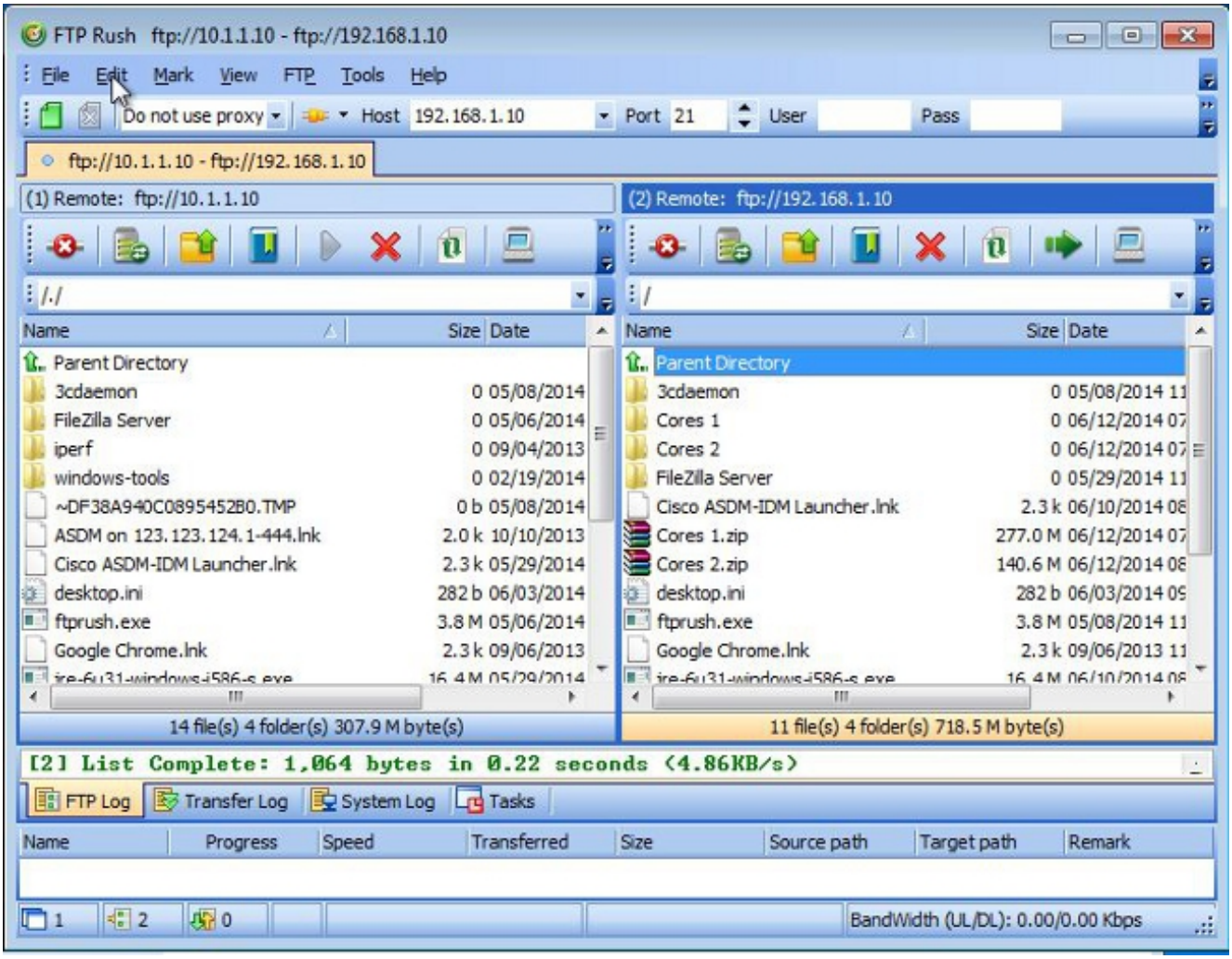
ファイル転送プロセス

2 つの FTP サーバ間の正常なファイル転送を検証するには、次の手順を実行します。

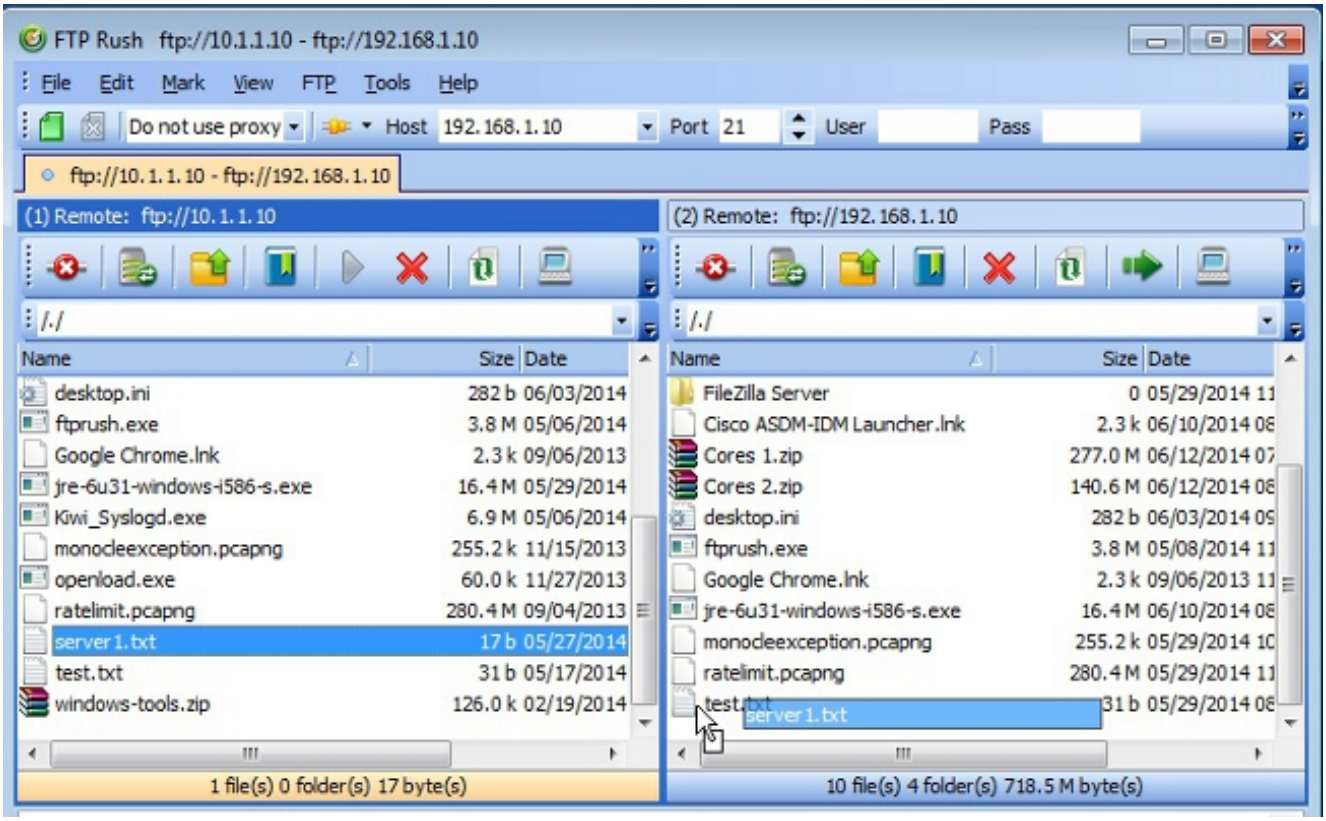
1. FXP クライアント マシンから server1 に接続します。



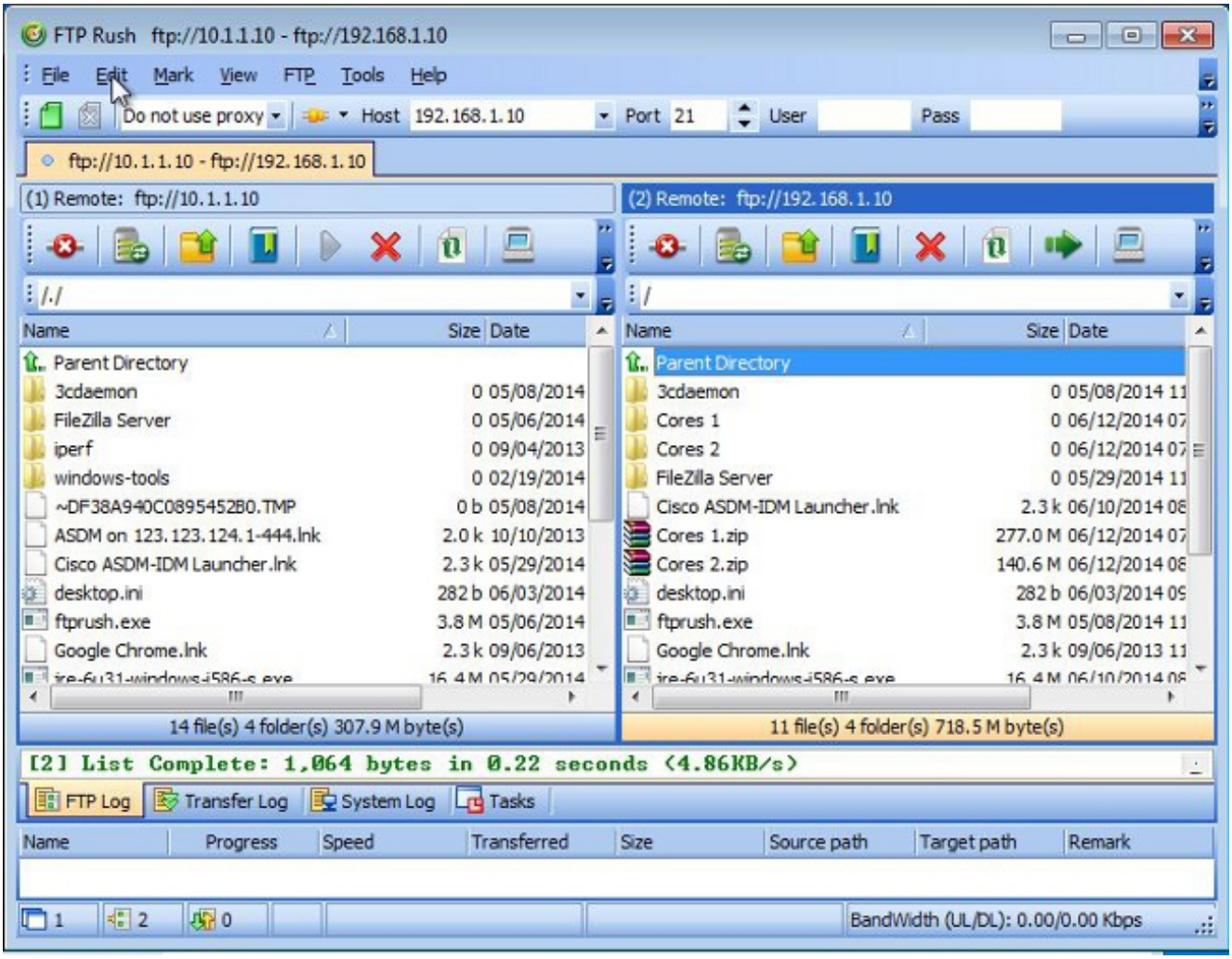
2. FXP クライアント マシンから server2 に接続します。



3. server1 のウィンドウから server2 のウィンドウに転送するファイルをドラッグ アンド ドロップします。



4. ファイル転送が成功することを検証します。



トラブルシュート

この項では、設定のトラブルシューティングに役立つ 2 つのシナリオのキャプチャを提示します。

FTP インスペクションが無効なシナリオ

このドキュメントの「FTP インスペクションおよび FXP」の項の記載のとおり、FTP インスペクションが無効な場合、ASA クライアント インターフェイスにデータが表示されます。

```
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.
```

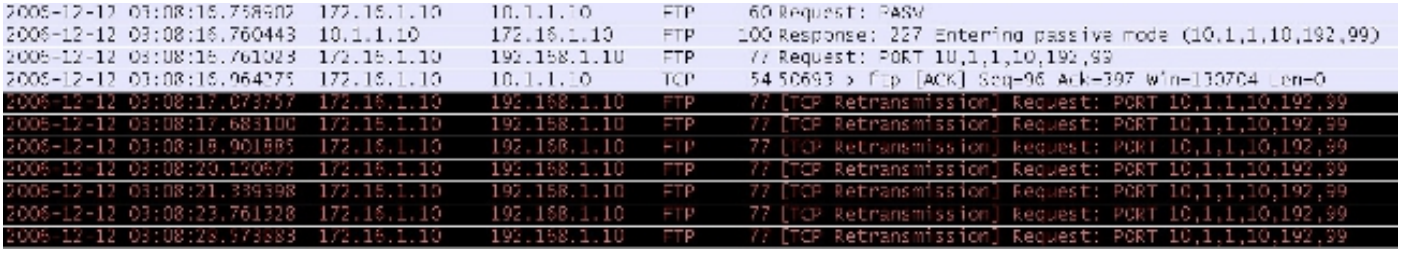
このデータについてのポイントを次に示します。

- クライアントの IP アドレスは **172.16.1.10** です。
- server1 の IP アドレスは **10.1.1.10** です。
- server2 の IP アドレスは **192.168.1.10** です。

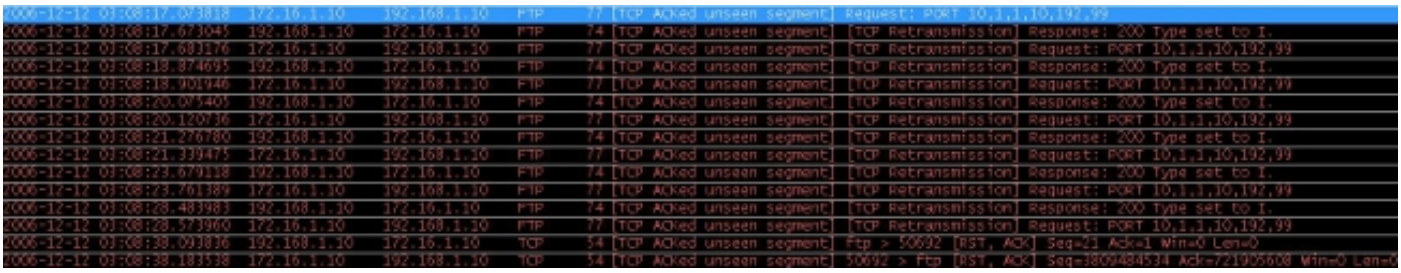
この例では、**Kiwi_Syslogd.exe というファイルが server1 から server2 に転送されます。**

FTP インスペクションが有効

FTP インスペクションが有効な場合、このデータは ASA クライアント インターフェイスに表示されます。



ASA ドロップのキャプチャは次のとおりです。



クライアント IP アドレスおよびポートとは異なる IP アドレスおよびポートが含まれているため、**PORT 要求は FTP インスペクションによってドロップされます。**その後、サーバへの制御接続はそのインスペクションで終了します。