Esempio di configurazione di ASA File Transfer con FXP

Sommario

Introduzione

Questo documento descrive come configurare il protocollo File eXchange Protocol (FXP) su Cisco Adaptive Security Appliance (ASA) tramite la CLI.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base del protocollo FTP (File Transfer Protocol) (modalità attiva/passiva).

Componenti usati

Per questo documento, è stato usato un Cisco ASA con software versione 8.0 e successive.

Nota: In questo esempio di configurazione vengono utilizzate due workstation Microsoft

Windows che fungono da server FXP e eseguono i servizi FTP (Daemon 3C). Inoltre, FXP è abilitato. Viene utilizzata anche un'altra workstation Microsoft Windows con software client FXP (FTP Rush).

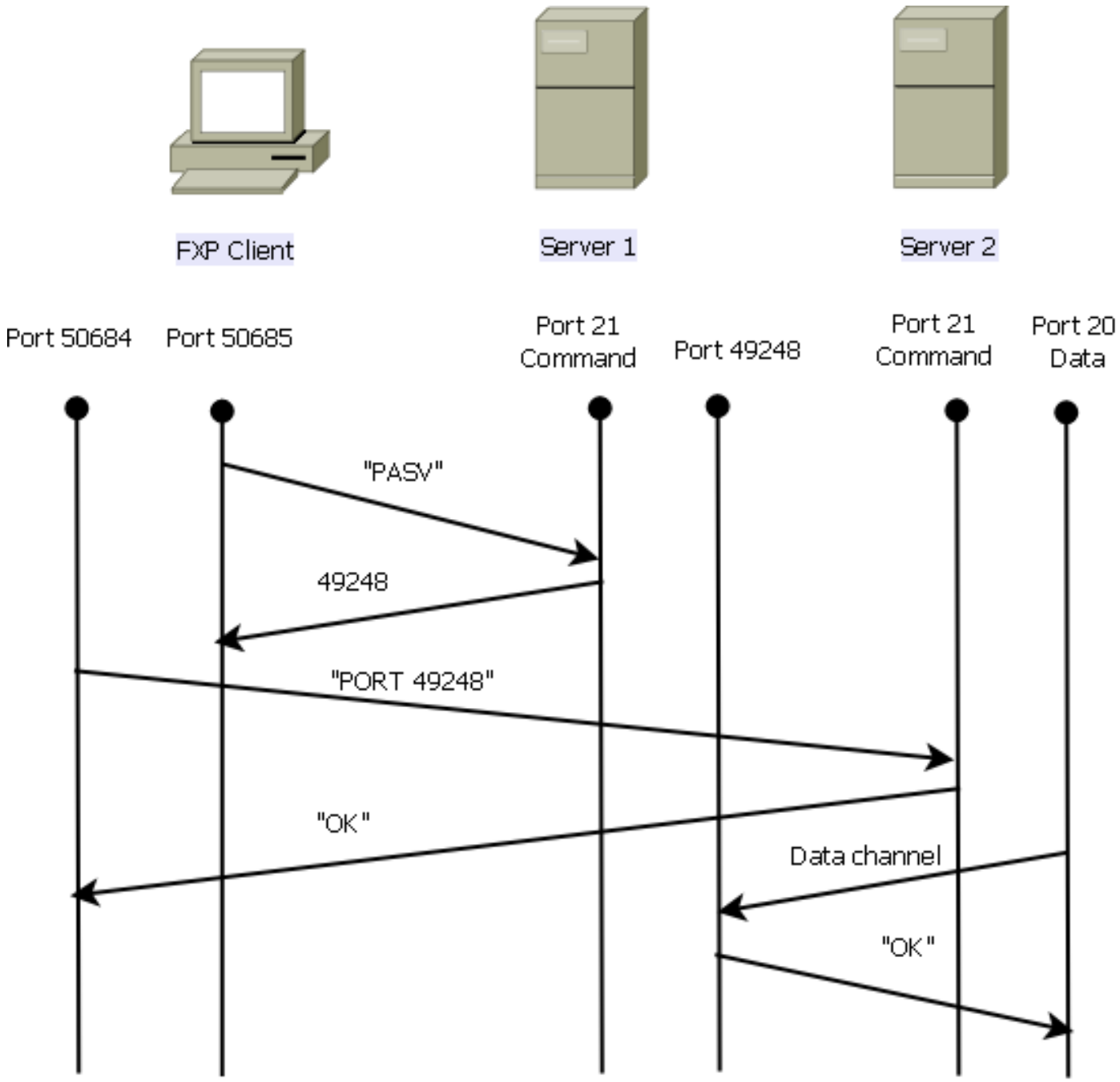
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

FXP consente di trasferire i file da un server FTP a un altro server FTP tramite un client FXP senza la necessità di dipendere dalla velocità della connessione Internet del client. Con FXP, la velocità massima di trasferimento dipende solo dalla connessione tra i due server, che in genere è molto più veloce della connessione client. È possibile applicare FXP in scenari in cui un server a larghezza di banda elevata richiede risorse da un altro server a larghezza di banda elevata, ma solo un client a larghezza di banda ridotta, ad esempio un amministratore di rete che lavora in remoto, dispone dell'autorizzazione per accedere alle risorse su entrambi i server.

FXP funge da estensione del protocollo FTP e il meccanismo è indicato nella sezione 5.2 della RFC 959 FTP. In pratica, il client FXP avvia una connessione di controllo con un server FTP1, apre un'altra connessione di controllo con il server FTP2, quindi modifica gli attributi di connessione dei server in modo che puntino l'uno verso l'altro in modo che il trasferimento avvenga direttamente tra i due server.

Meccanismo di trasferimento file tramite FXP



Ecco una panoramica del processo:

1. Il client apre una connessione di controllo con server1 sulla porta TCP 21.

   Il client invia il comando **PASV** a server1.

   Server1 risponde con il proprio indirizzo IP e la porta su cui è in ascolto.

2. Il client apre una connessione di controllo con server2 sulla porta TCP 21.

   Il client passa l'indirizzo/la porta ricevuta dal server1 al server2 in un comando **PORT**.

   Server2 risponde per informare il client che il comando **PORT** ha esito positivo. Server2 ora sa dove inviare i dati.

3. Per avviare il processo di trasmissione da server1 a server2:

Il client invia il comando **STOR** al server2 e gli ordina di memorizzare la data che riceve.

Il client invia il comando **RETR** a server1 e gli ordina di recuperare o trasmettere il file.

4. Tutti i dati ora vanno direttamente dall'origine al server FTP di destinazione. Entrambi i server segnalano al client solo i messaggi di stato in caso di esito negativo/positivo.

La tabella di connessione viene visualizzata nel modo seguente:

```
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
```

Controllo FTP e FXP

Il trasferimento di file tramite ASA tramite FXP ha esito positivo solo quando l'ispezione FTP è **disabilitata** sull'appliance ASA.

Quando il client FXP specifica un indirizzo IP e una porta TCP diversi da quelli del client nel comando **PORT** FTP, si crea una situazione non sicura in cui un utente non autorizzato è in grado di eseguire una scansione della porta su un host su Internet da un server FTP di terze parti. Questo accade perché il server FTP riceve istruzioni per aprire una connessione a una porta su un computer che potrebbe non essere il client da cui proviene. Questo tipo di attacco viene chiamato **attacco di tipo rimbalzo FTP** e l'ispezione FTP chiude la connessione in quanto la considera una violazione della sicurezza.

Di seguito è riportato un esempio:

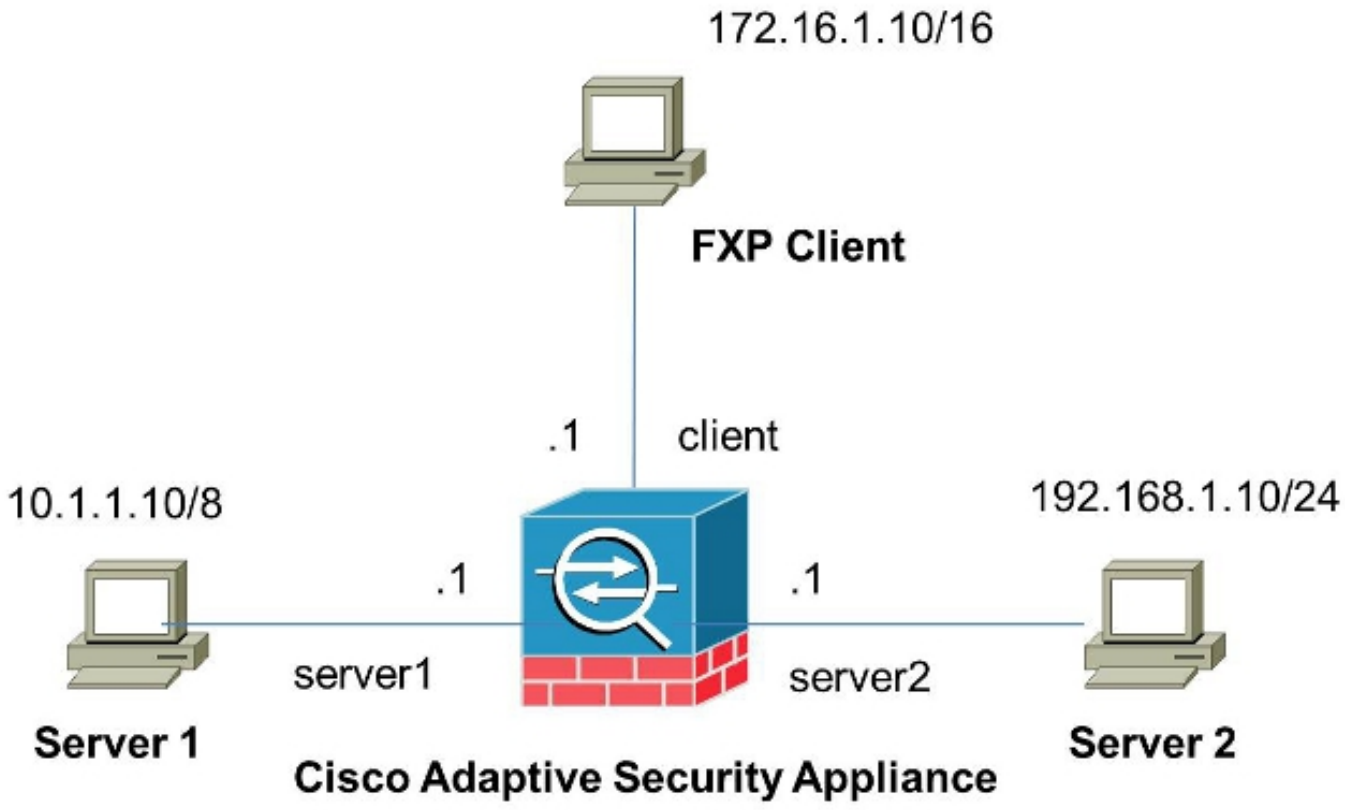
```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: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

Configurazione

Per configurare FXP sull'appliance ASA, usare le informazioni descritte in questa sezione.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete



Configurazione dell'ASA tramite CLI

Per configurare l'ASA, effettuare i seguenti passaggi:

1. Disabilita ispezione FTP:

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

2. Configurare gli elenchi degli accessi per consentire la comunicazione tra il client FXP e i due server 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. Applicare gli elenchi degli accessi alle rispettive interfacce:

```
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
```

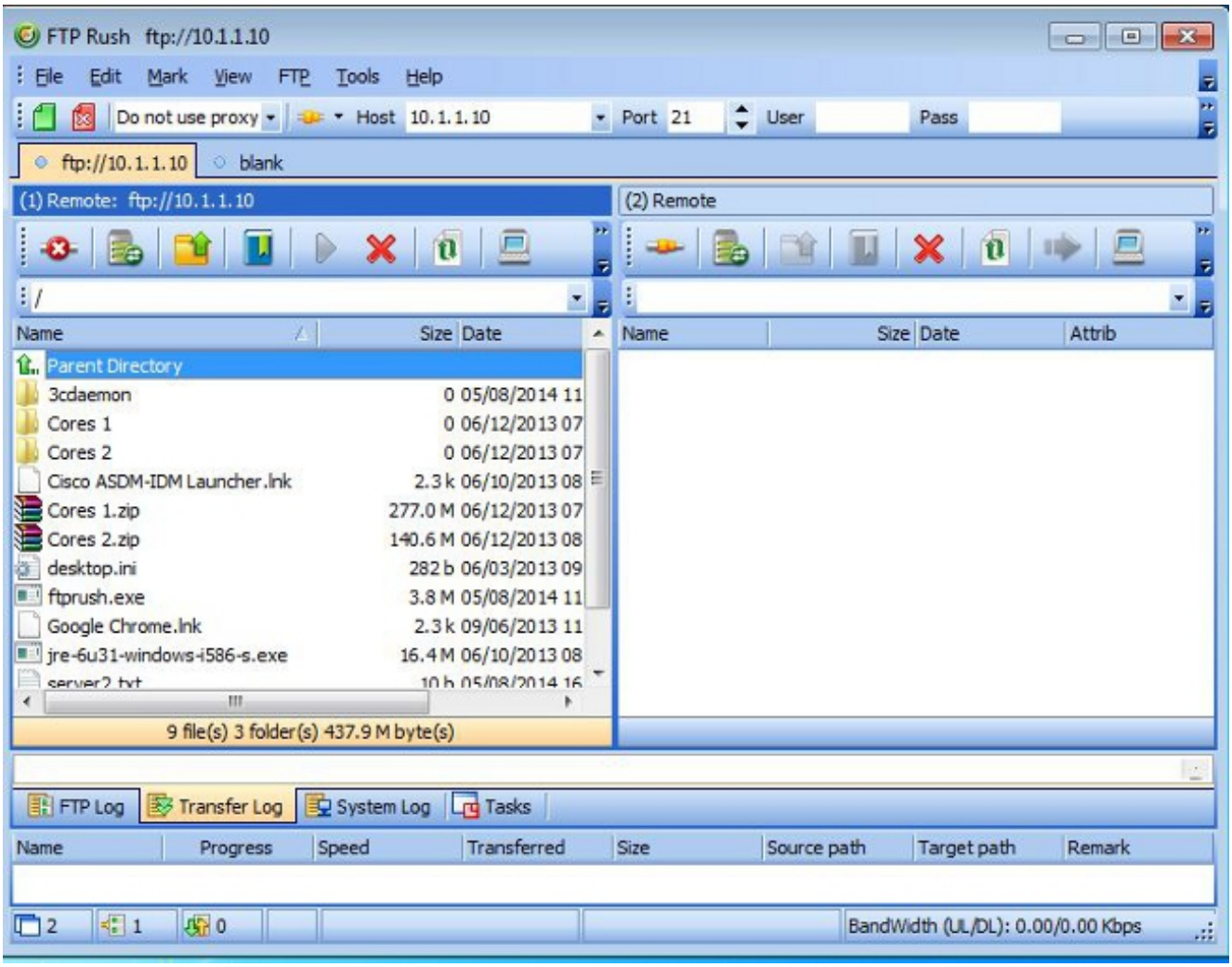
Verifica

Per verificare che la configurazione funzioni correttamente, consultare le informazioni descritte in questa sezione.

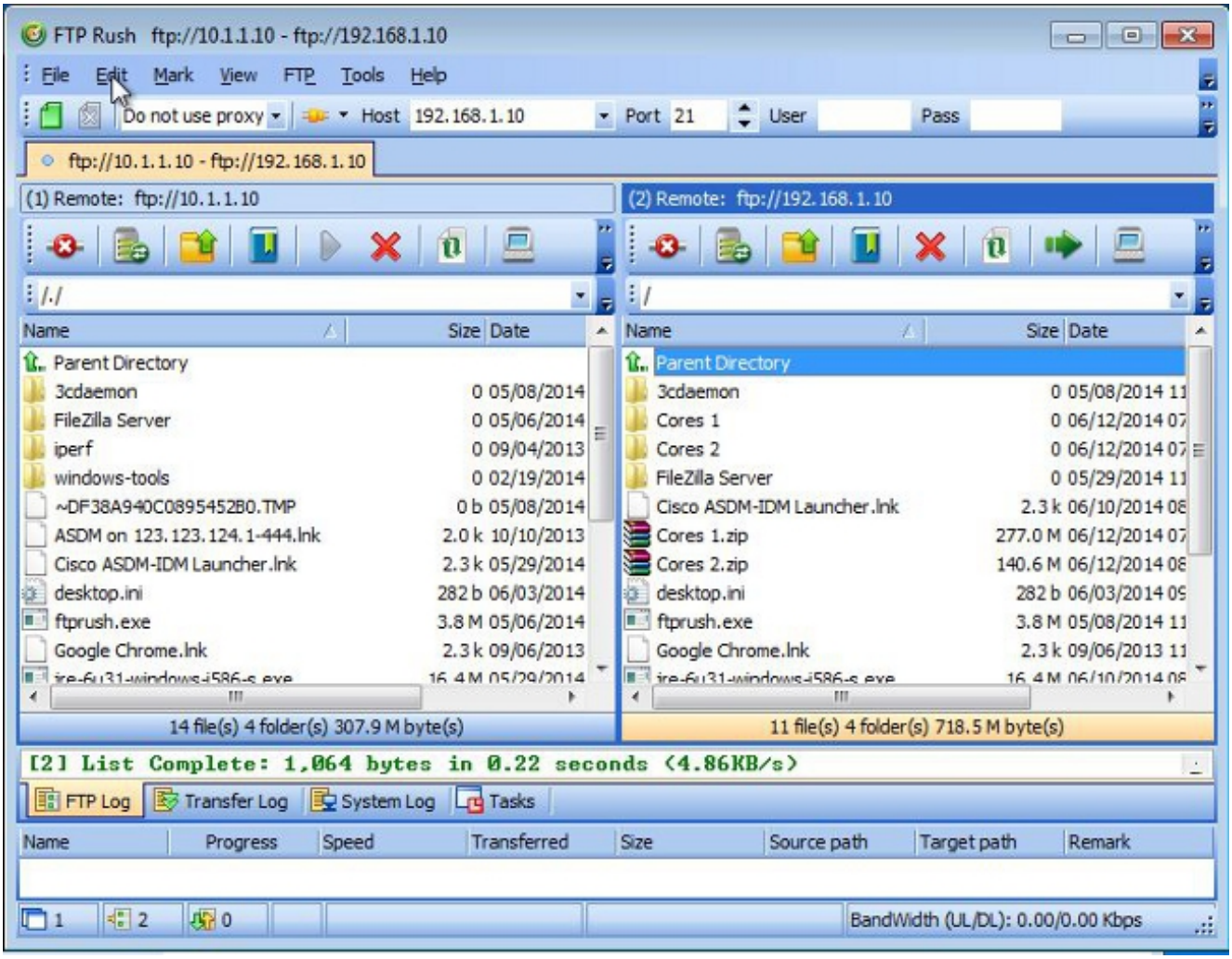
Processo di trasferimento file

Per verificare la riuscita del trasferimento di file tra i due server FTP, completare i seguenti passaggi:

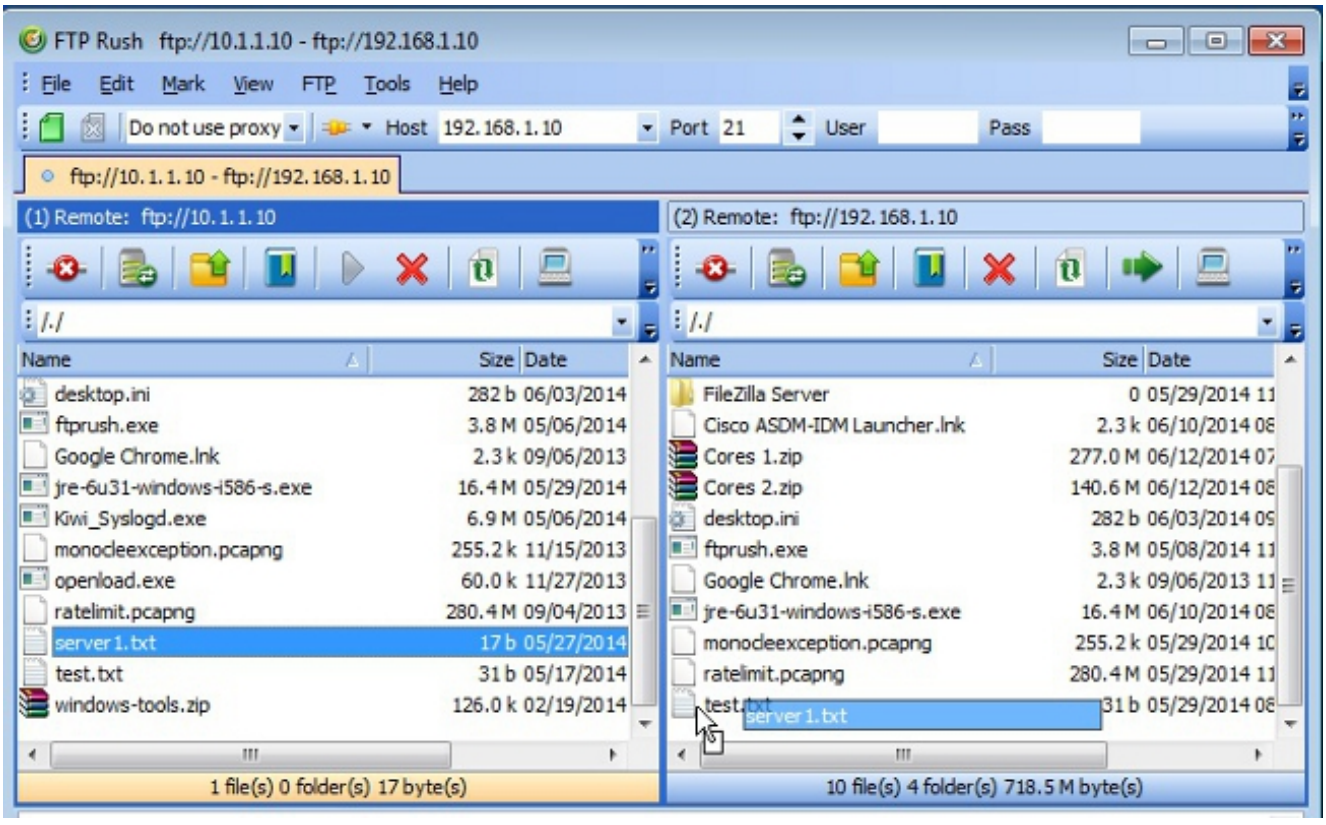
1. Connettersi al server1 dal computer client FXP:



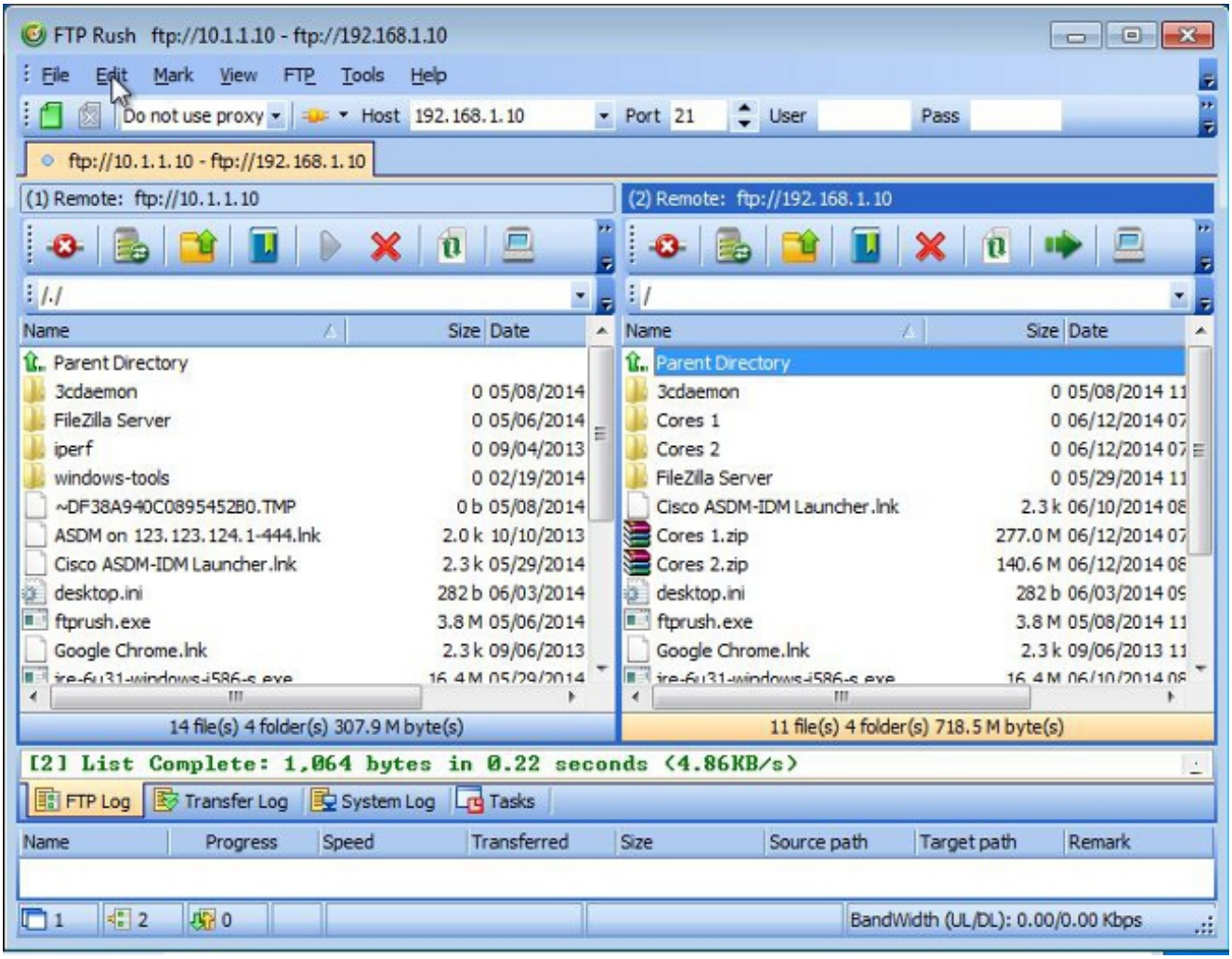
2. Connettersi al server2 dal computer client FXP:



3. Trascinare il file da trasferire dalla finestra server1 alla finestra server2:



4. Verificare che il trasferimento del file sia stato completato:



Risoluzione dei problemi

In questa sezione vengono acquisiti due diversi scenari che è possibile utilizzare per risolvere i problemi relativi alla configurazione.

Scenario di disattivazione ispezione FTP

Quando l'ispezione FTP è disabilitata, come descritto nella sezione Ispezione FTP e FXP di questo documento, i dati vengono visualizzati sull'interfaccia 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.
```

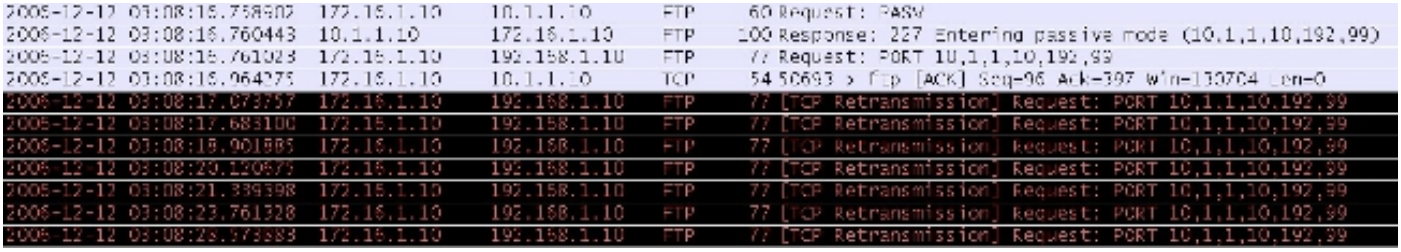
Ecco alcune note relative a questi dati:

- L'indirizzo IP del client è **172.16.1.10**.
- L'indirizzo IP di Server1 è **10.1.1.10**.
- L'indirizzo IP di Server2 è **192.168.1.10**.

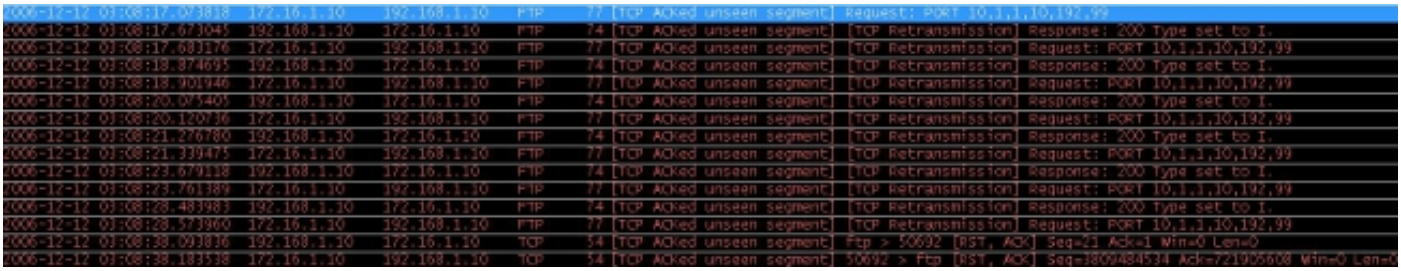
In questo esempio, il file **Kiwi_Syslogd.exe** viene trasferito da server1 a server2.

Ispezione FTP abilitata

Quando l'ispezione FTP è abilitata, questi dati vengono visualizzati sull'interfaccia client ASA:



Di seguito sono riportate le acquisizioni della drop dell'ASA:



La richiesta **PORT** viene scartata dall'ispezione FTP perché contiene un indirizzo IP e una porta diversi dall'indirizzo IP e dalla porta del client. Successivamente, la connessione di controllo al server viene interrotta dall'ispezione.