使用FXP的ASA檔案傳輸配置示例

目錄

簡介

本文說明如何通過CLI在思科自適應安全裝置(ASA)上配置檔案交換協定(FXP)。

必要條件

需求

思科建議您瞭解檔案傳輸通訊協定(FTP)（主動/被動模式）的基本知識。

採用元件

本文檔中的資訊基於運行軟體版本8.0及更高版本的Cisco ASA。

> **附註**：此配置示例使用兩個充當FXP伺服器並運行FTP服務（3C守護程式）的Microsoft Windows工作站。 它們還啟用了FXP。還使用另一個運行FXP客戶端軟體(FTP Rush)的Microsoft Windows工作站。

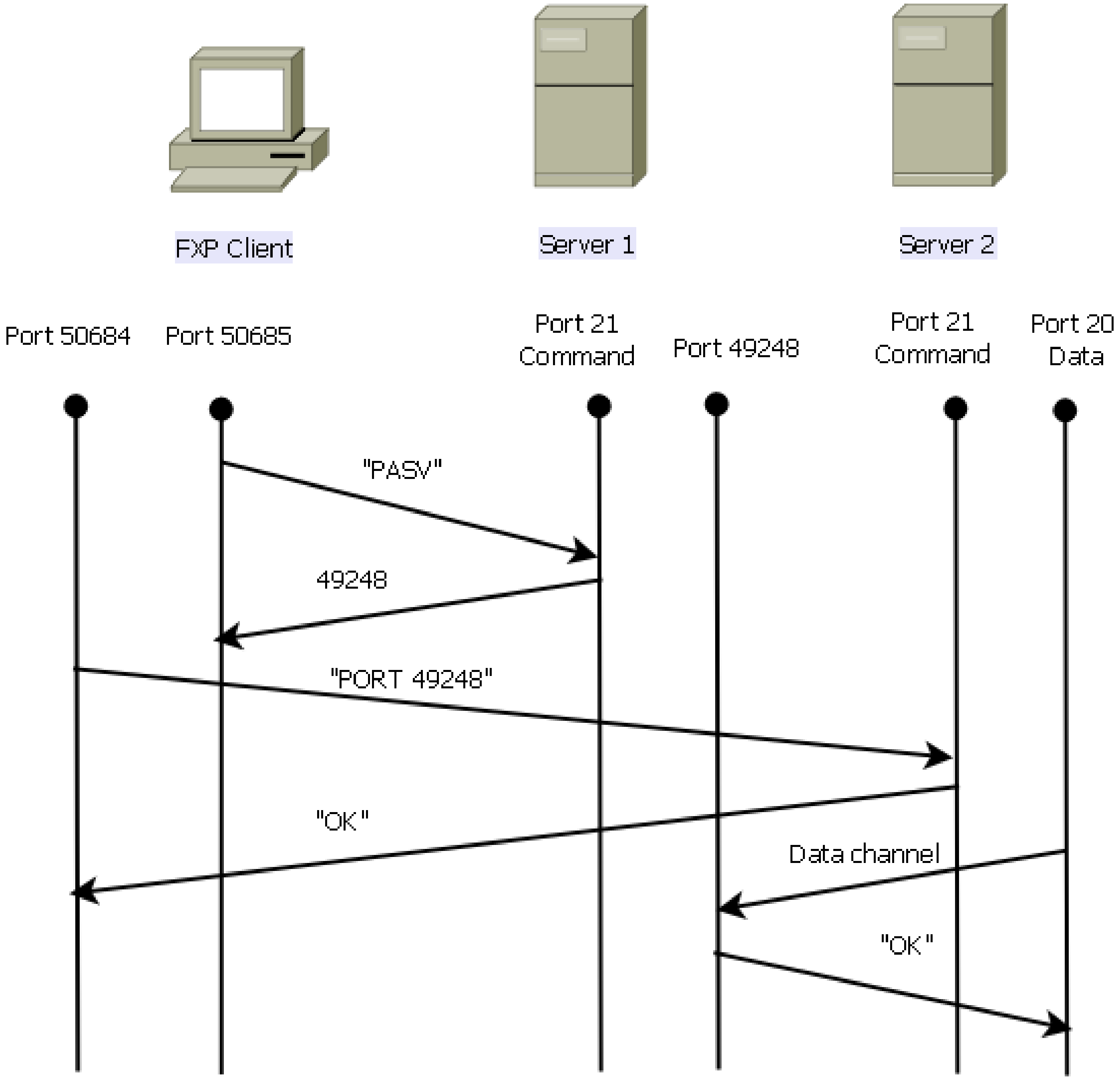
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

FXP允許您通過FXP客戶端將檔案從一個FTP伺服器傳輸到另一個FTP伺服器，而無需依賴於客戶端網際網路連線速度。使用FXP時，最大傳輸速度僅取決於兩個伺服器之間的連線，通常比客戶端連線快得多。您可以在高頻寬伺服器要求其他高頻寬伺服器提供資源的情況下應用FXP，但只有低頻寬客戶端（如遠端工作的網路管理員）有權訪問兩台伺服器上的資源。

FXP作為FTP協定的擴展，其機制在FTP RFC 959第5.2節中說明。基本上，FXP客戶端發起與FTP伺服器1的控制連線，開啟與FTP伺服器2的另一個控制連線，然後修改伺服器的連線屬性，以便它們相互指向使得直接在兩個伺服器之間發生傳輸。

FXP檔案傳輸機制



以下是流程概述：

1. 客戶端在TCP埠21上開啟與server1的控制連線。

   使用者端將**PASV**命令傳送到server1。

   Server1使用其IP地址和偵聽的埠做出響應。

2. 客戶端在TCP埠21上開啟與server2的控制連線。

   客戶端通過**PORT**命令將從server1接收的地址/埠傳遞給server2。

   Server2做出響應，以通知客戶端**PORT**命令成功。Server2現在知道將資料傳送到何處。

3. 若要開始從server1到server2的傳輸過程：

客戶端向server2傳送**STOR**命令，並指示它儲存收到的日期。

客戶端將**RETR**命令傳送到server1，並指示其檢索或傳輸檔案。

4. 現在，所有資料都直接從源傳輸到目標FTP伺服器。兩台伺服器都只向客戶端報告失敗/成功的狀態消息。

連線表的顯示方式如下：

```
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檢查和FXP

僅當在ASA上禁用FTP檢查時，通過FXP通過ASA的文**件傳輸**才會成功。

當FXP客戶端在FTP **PORT**命令中指定了與客戶端不同的IP地址和TCP埠時，會出現一種不安全的情況，即攻擊者能夠從第三方FTP伺服器對Internet上的主機進行埠掃描。這是因為已指示FTP伺服器開啟與電腦上埠的連線，該電腦可能不是源客戶端。這稱為**FTP退回攻擊**,FTP檢查會關閉連線，因為它認為這違反了安全規定。

以下是範例：

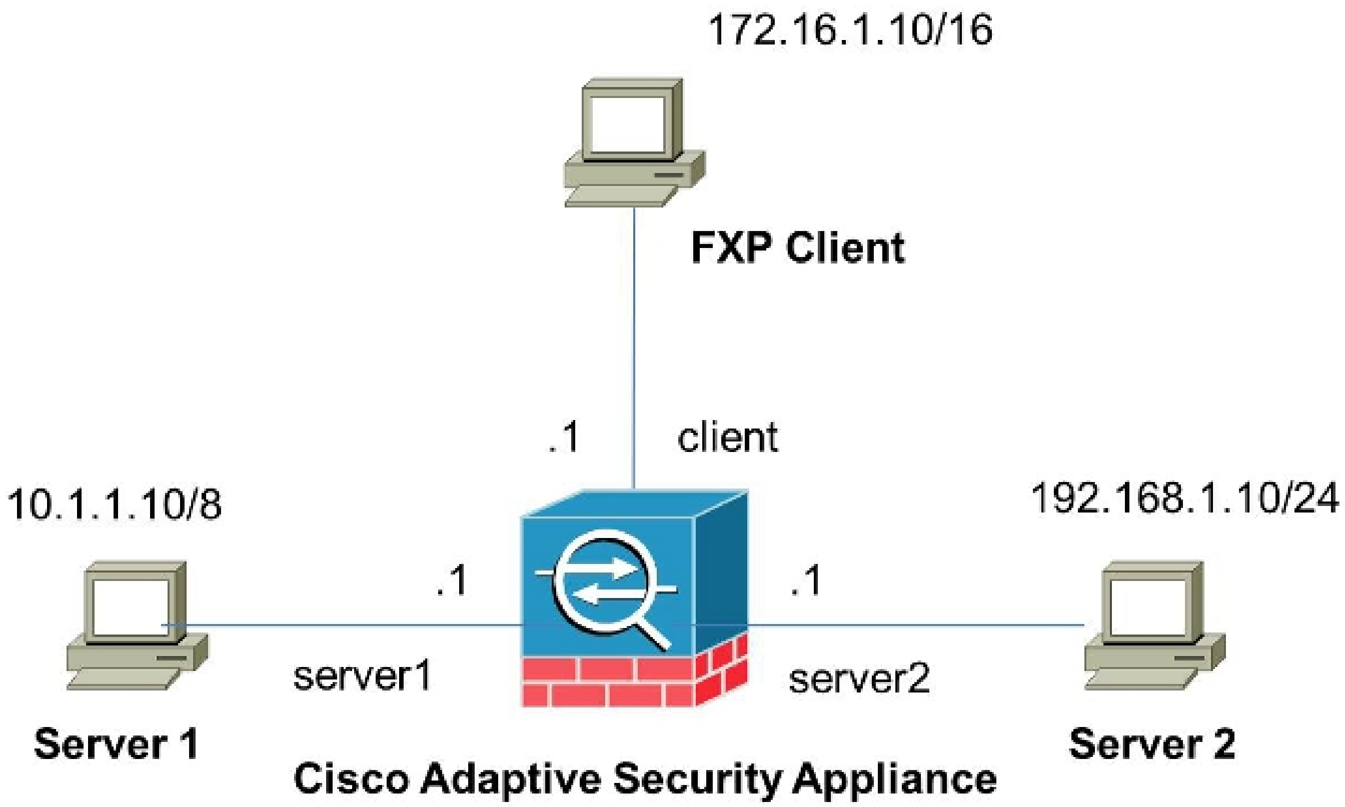
```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: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

使用本節中介紹的資訊在ASA上配置FXP。

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表



通過CLI配置ASA

完成以下步驟以配置ASA:

1. 禁用FTP檢測：

   ```
   FXP-ASA(config)# policy-map global_policy
   FXP-ASA(config-pmap)#  class inspection_default
   FXP-ASA(config-pmap-c)# no inspect ftp
   ```
2. 配置訪問清單以允許FXP客戶端與兩個FTP伺服器之間的通訊：

   ```
   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. 在各自的介面上套用存取清單：

   ```
   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
   ```

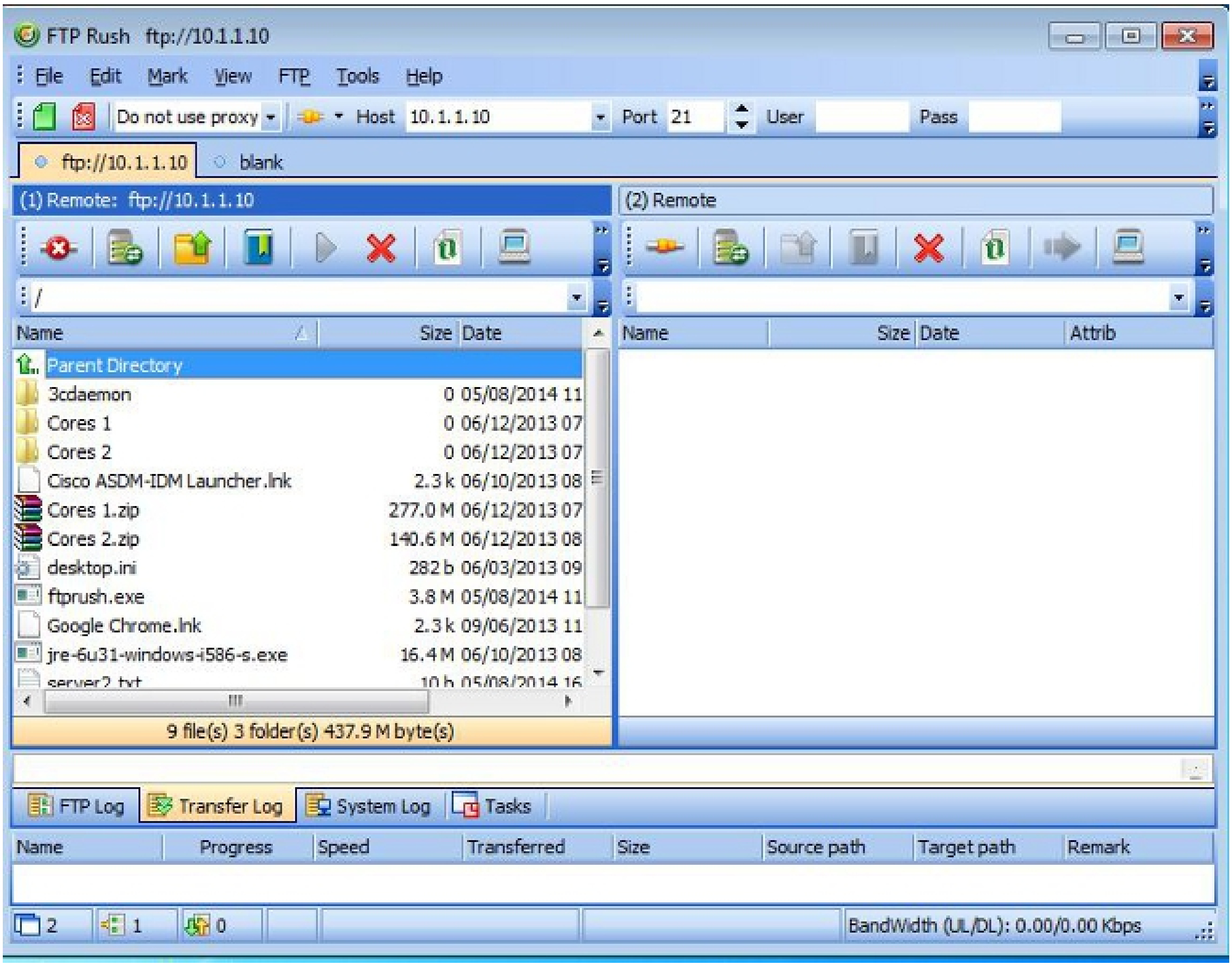
驗證

使用本節所述的資訊來驗證您的組態是否正常運作。

檔案傳輸過程

完成以下步驟，確認兩台FTP伺服器之間的檔案傳輸是否成功：

1. 從FXP客戶端電腦連線到server1:



Do not use proxy
Host 10.1.1.10
Port 21
User
Pass

(1) Remote: ftp://10.1.1.10

/

Name	Size	Date
Parent Directory		
3cdaemon	0	05/08/2014 11
Cores 1	0	06/12/2013 07
Cores 2	0	06/12/2013 07
Cisco ASDM-IDM Launcher.lnk	2.3 k	06/10/2013 08
Cores 1.zip	277.0 M	06/12/2013 07
Cores 2.zip	140.6 M	06/12/2013 08
desktop.ini	282 b	06/03/2013 09
ftprush.exe	3.8 M	05/08/2014 11
Google Chrome.lnk	2.3 k	09/06/2013 11
jre-6u31-windows-i586-s.exe	16.4 M	06/10/2013 08
server2.txt	10 b	05/08/2014 16

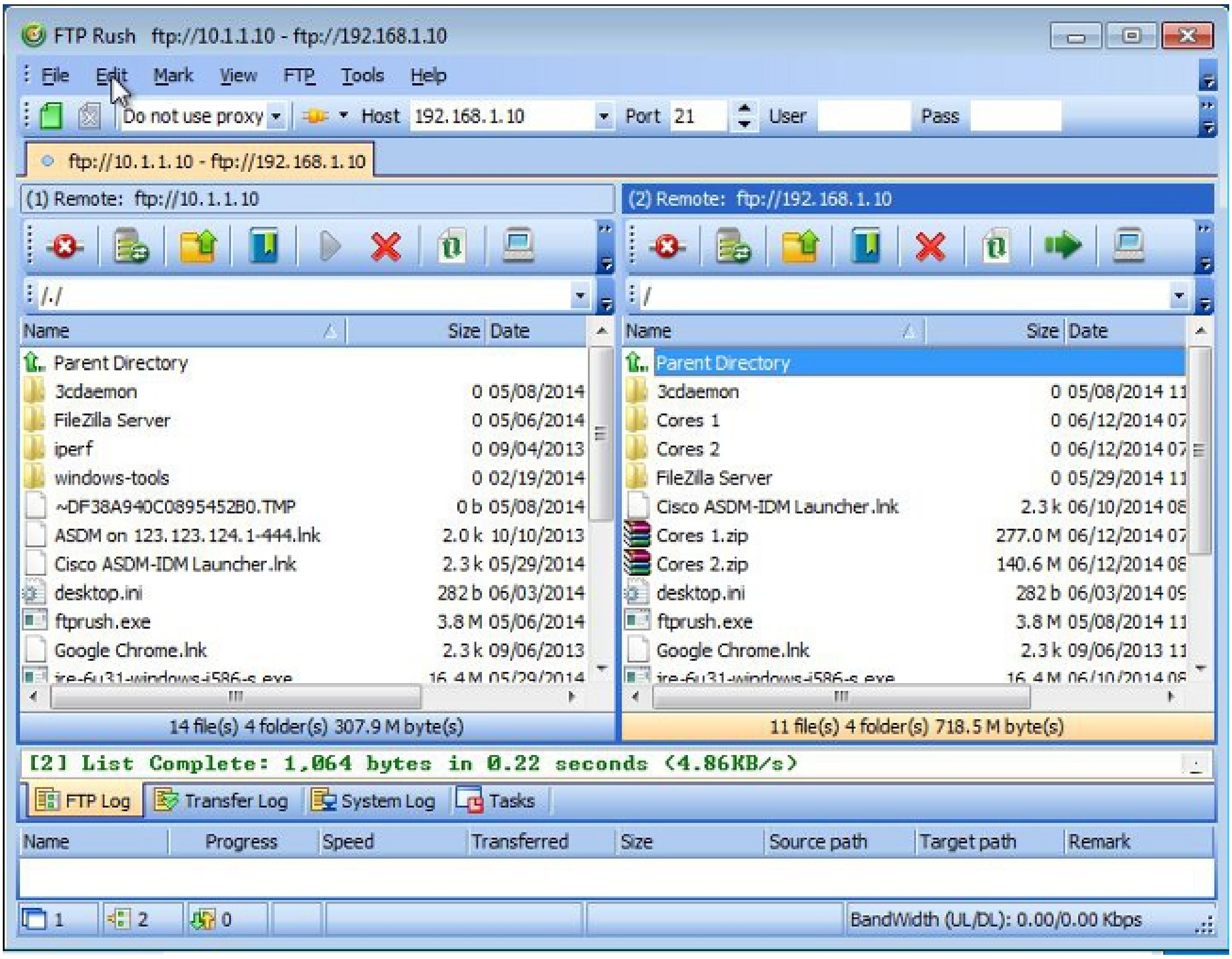
9 file(s) 3 folder(s) 437.9 M byte(s)

Name	Size	Date	Attrib

Name	Progress	Speed	Transferred	Size	Source path	Target path	Remark

BandWidth (UL/DL): 0.00/0.00 Kbps

2. 從FXP客戶端電腦連線到server2:



Do not use proxy | Host 192.168.1.10 | Port 21 | User | Pass

(1) Remote: ftp://10.1.1.10

/./

Name	Size	Date
Parent Directory		
3cdaemon	0	05/08/2014
FileZilla Server	0	05/06/2014
iperf	0	09/04/2013
windows-tools	0	02/19/2014
~DF38A940C0895452B0.TMP	0 b	05/08/2014
ASDM on 123.123.124.1-444.lnk	2.0 k	10/10/2013
Cisco ASDM-IDM Launcher.lnk	2.3 k	05/29/2014
desktop.ini	282 b	06/03/2014
ftprush.exe	3.8 M	05/06/2014
Google Chrome.lnk	2.3 k	09/06/2013
jre-6u31-windows-i586-s.exe	16.4 M	05/29/2014

14 file(s) 4 folder(s) 307.9 M byte(s)

(2) Remote: ftp://192.168.1.10

/

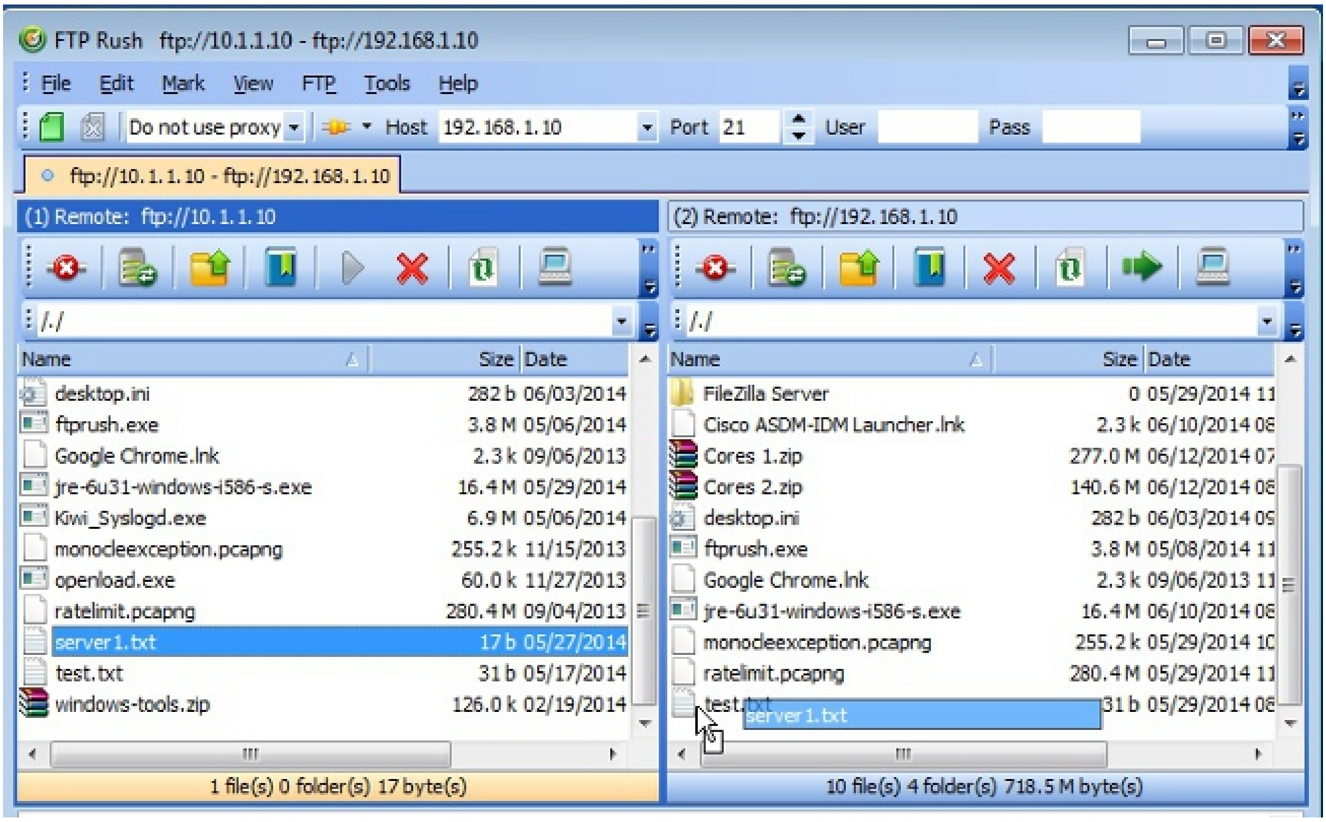
Name	Size	Date
Parent Directory		
3cdaemon	0	05/08/2014 11
Cores 1	0	06/12/2014 07
Cores 2	0	06/12/2014 07
FileZilla Server	0	05/29/2014 11
Cisco ASDM-IDM Launcher.lnk	2.3 k	06/10/2014 08
Cores 1.zip	277.0 M	06/12/2014 07
Cores 2.zip	140.6 M	06/12/2014 08
desktop.ini	282 b	06/03/2014 09
ftprush.exe	3.8 M	05/08/2014 11
Google Chrome.lnk	2.3 k	09/06/2013 11
jre-6u31-windows-i586-s.exe	16.4 M	06/10/2014 08

11 file(s) 4 folder(s) 718.5 M byte(s)

```
[2] List Complete: 1,064 bytes in 0.22 seconds (4.86KB/s)
```

BandWidth (UL/DL): 0.00/0.00 Kbps

3. 將要傳輸的檔案從server1視窗拖放到server2視窗：


FTP Rush ftp://10.1.1.10 - ftp://192.168.1.10
File
Edit
Mark
View
FTP
Tools
Help
ftp://10.1.1.10 - ftp://192.168.1.10
server1.txt

Do not use proxy | Host 192.168.1.10 | Port 21 | User | Pass

(1) Remote: ftp://10.1.1.10

/./

Name	Size	Date
desktop.ini	282 b	06/03/2014
ftprush.exe	3.8 M	05/06/2014
Google Chrome.lnk	2.3 k	09/06/2013
jre-6u31-windows-i586-s.exe	16.4 M	05/29/2014
Kiwi_Syslogd.exe	6.9 M	05/06/2014
monocleexception.pcapng	255.2 k	11/15/2013
openload.exe	60.0 k	11/27/2013
ratelimit.pcapng	280.4 M	09/04/2013
server1.txt	17 b	05/27/2014
test.txt	31 b	05/17/2014
windows-tools.zip	126.0 k	02/19/2014

1 file(s) 0 folder(s) 17 byte(s)

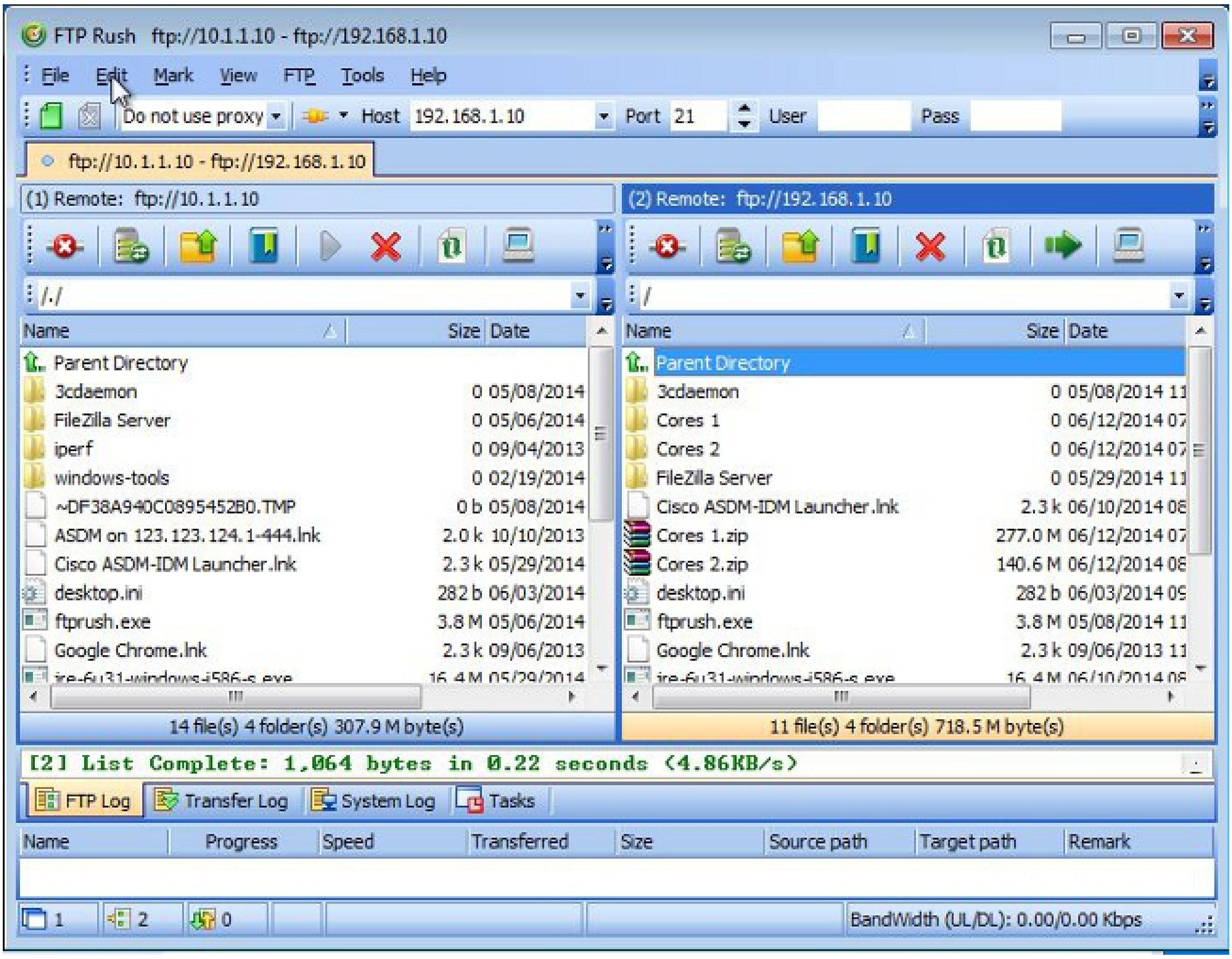
(2) Remote: ftp://192.168.1.10

/./

Name	Size	Date
FileZilla Server	0	05/29/2014 11
Cisco ASDM-IDM Launcher.lnk	2.3 k	06/10/2014 08
Cores 1.zip	277.0 M	06/12/2014 07
Cores 2.zip	140.6 M	06/12/2014 08
desktop.ini	282 b	06/03/2014 09
ftprush.exe	3.8 M	05/08/2014 11
Google Chrome.lnk	2.3 k	09/06/2013 11
jre-6u31-windows-i586-s.exe	16.4 M	06/10/2014 08
monocleexception.pcapng	255.2 k	05/29/2014 10
ratelimit.pcapng	280.4 M	05/29/2014 11
test.txt	31 b	05/29/2014 08

10 file(s) 4 folder(s) 718.5 M byte(s)

4. 驗證檔案傳輸是否成功：



FTP Rush ftp://10.1.1.10 - ftp://192.168.1.10

Do not use proxy　Host 192.168.1.10　Port 21　User　Pass

ftp://10.1.1.10 - ftp://192.168.1.10

(1) Remote: ftp://10.1.1.10

/./

Name	Size	Date
Parent Directory		
3cdaemon	0	05/08/2014
FileZilla Server	0	05/06/2014
iperf	0	09/04/2013
windows-tools	0	02/19/2014
~DF38A940C0895452B0.TMP	0 b	05/08/2014
ASDM on 123.123.124.1-444.lnk	2.0 k	10/10/2013
Cisco ASDM-IDM Launcher.lnk	2.3 k	05/29/2014
desktop.ini	282 b	06/03/2014
ftprush.exe	3.8 M	05/06/2014
Google Chrome.lnk	2.3 k	09/06/2013
jre-6u31-windows-i586-s.exe	16.4 M	05/29/2014

14 file(s) 4 folder(s) 307.9 M byte(s)

(2) Remote: ftp://192.168.1.10

/

Name	Size	Date
Parent Directory		
3cdaemon	0	05/08/2014 11
Cores 1	0	06/12/2014 07
Cores 2	0	06/12/2014 07
FileZilla Server	0	05/29/2014 11
Cisco ASDM-IDM Launcher.lnk	2.3 k	06/10/2014 08
Cores 1.zip	277.0 M	06/12/2014 07
Cores 2.zip	140.6 M	06/12/2014 08
desktop.ini	282 b	06/03/2014 09
ftprush.exe	3.8 M	05/08/2014 11
Google Chrome.lnk	2.3 k	09/06/2013 11
jre-6u31-windows-i586-s.exe	16.4 M	06/10/2014 08

11 file(s) 4 folder(s) 718.5 M byte(s)

```
[2] List Complete: 1,064 bytes in 0.22 seconds (4.86KB/s)
```

Name	Progress	Speed	Transferred	Size	Source path	Target path	Remark

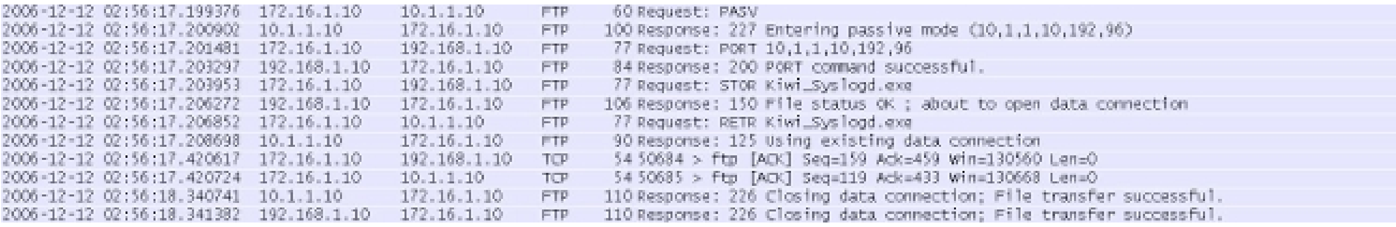
BandWidth (UL/DL): 0.00/0.00 Kbps

疑難排解

本節提供兩種不同情景的擷取，可用於對組態進行疑難排解。

禁用FTP檢測方案

如本檔案的FTP檢查和FXP一節所述，FTP檢查被禁用時，此資料會顯示在ASA客戶端介面上：



```
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.
```

以下是關於此資料的一些註解：

- 客戶端IP地址為**172.16.1.10**。

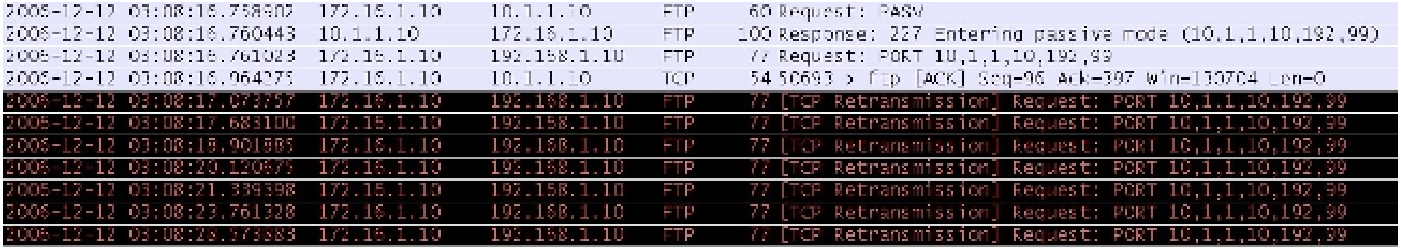
- Server1的IP地址為**10.1.1.10**。

- Server2 IP地址為**192.168.1.10**。

在本示例中，名為**Kiwi_Syslogd.exe**的檔案從server1傳輸到server2。

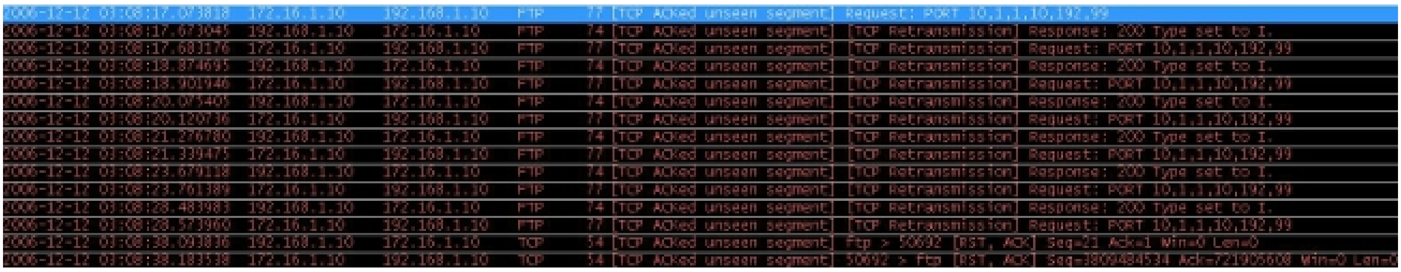
已啟用FTP檢測

啟用FTP檢測時，此資料顯示在ASA客戶端介面上：



```
2006-12-12 03:08:15.758902  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 03:08:28.573583  172.16.1.10   192.168.1.10  FTP    77 [TCP Retransmission] Request: PORT 10,1,1,10,192,99
```

以下是ASA丟棄捕獲：



```
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
```

FTP檢查會捨棄**PORT**請求，因為它包含與使用者端IP位址和連線埠不同的IP位址和連線埠。隨後，通過檢查終止與伺服器的控制連線。