配置FTP/TFTP服務：ASA 9.X

目錄

簡介

本文檔介紹ASA上的不同FTP和TFTP檢測方案、ASA FTP/TFTP檢測配置和基本故障排除。

必要條件

需求

思科建議瞭解以下主題：

- 所需介面之間的基本通訊

- 位於DMZ網路中的FTP伺服器的組態

採用元件

本文檔介紹了自適應安全裝置(ASA)上的不同FTP和TFTP檢測方案，還介紹了ASA FTP/TFTP檢測配置和基本故障排除。

本文中的資訊係根據以下軟體和硬體版本：

- 運行9.1(5)軟體映像的ASA 5500或ASA 5500-X系列ASA
- 任何FTP伺服器
- 任何FTP使用者端

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

安全裝置通過自適應安全演算法功能支援應用檢測。

通過自適應安全演算法使用的狀態應用檢測，安全裝置會跟蹤穿越防火牆的每個連線，並確保它們有效。

通過狀態檢查，防火牆還會監視連線的狀態，以編譯資訊以放入狀態表中。

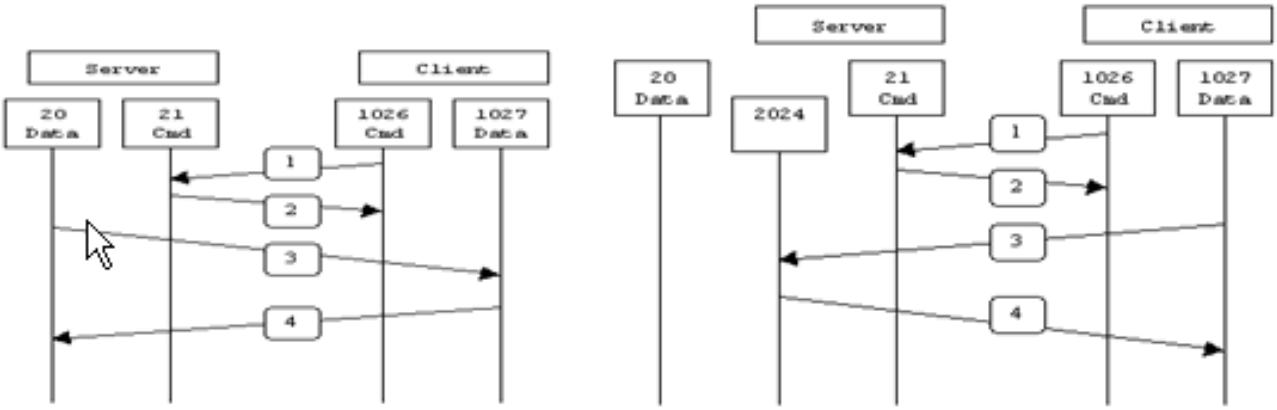
除了使用管理員定義的規則外，還使用狀態表，過濾決策將基於以前通過防火牆的資料包建立的上下文。

應用檢查的實施包括以下操作：

- 識別流量
- 對流量應用檢查
- 啟用介面檢測

FTP有兩種形式，如下圖所示。

- 活動模式
- 被動模式



Active FTP　　Passive FTP

Active FTP :
command : client >1023 -> server 21
data　: client >1023 <- server 20

Passive FTP :
command : client >1023 -> server 21
data　: client >1023 -> server >1023

主動式FTP

在主動式FTP模式下，使用者端從隨機非特權連線埠(N>1023)連線到FTP伺服器的指令連線埠(21)。然後使用者端開始監聽連線埠N>1023，並將FTP命令連線埠N>1023傳送到FTP伺服器。然後，伺服器從其本地資料埠（即埠20）連線回客戶端的指定資料埠。

被動FTP

在被動式FTP模式下，客戶端發起到伺服器的兩個連線，這解決了防火牆過濾從伺服器到客戶端的傳入資料埠連線的問題。開啟FTP連線時，使用者端會在本機開啟兩個隨機非特權連線埠。第一埠與埠21上的伺服器聯絡。但是，客戶端不會運行port命令並允許伺服器連線回其資料埠，而是發出PASV命令。如此一來，伺服器就會開啟一個隨機的未授權連線埠(P>1023)，並將port P命令傳送回使用者端。然後客戶端發起從埠N>1023到伺服器埠P的連線以傳輸資料。如果安全裝置上未配置inspection命令，則從內部使用者傳出郵件的FTP僅在被動模式下工作。此外，外部使用者傳入FTP伺服器時，會遭到拒絕存取。

TFTP

如RFC 1350所述，TFTP是一種在TFTP伺服器和使用者端之間讀取和寫入檔案的簡單通訊協定。TFTP使用UDP埠69。

進階通訊協定處理

為什麼需要FTP檢測？

某些應用需要思科安全裝置應用檢查功能進行特殊處理。這些型別的應用程式通常在使用者資料包中嵌入IP編址資訊，或在動態分配的埠上開啟輔助通道。應用檢測功能與網路地址轉換(NAT)配合使用，可幫助識別嵌入編址資訊的位置。

除了識別嵌入式編址資訊外，應用檢查功能還監控會話，以確定輔助通道的埠號。許多協定會開啟輔助TCP或UDP埠以提高效能。公認連線埠上的初始作業階段用於交涉動態分配的連線埠號碼。

應用檢查功能會監視這些會話、識別動態埠分配並在特定會話期間允許在這些埠上進行資料交換。多媒體和FTP應用都表現出這種行為。

如果尚未在安全裝置上啟用FTP檢測，則會放棄此請求，並且FTP會話不會傳輸任何請求的資料。

如果在ASA上啟用了FTP檢測，則ASA會監控控制通道並嘗試識別開啟資料通道的請求。FTP協定將資料通道埠規範嵌入控制通道流量，要求安全裝置檢查控制通道的資料埠更改。

ASA識別請求後，會為會話期間的資料通道流量臨時建立一個開口。這樣，FTP檢查功能監視控制通道，識別資料埠分配，並允許資料埠上交換會話長度的資料。

預設情況下，ASA通過global-inspection class-map檢查FTP流量的埠21連線。安全裝置還可以識別主動和被動FTP會話之間的區別。

如果FTP會話支援被動FTP資料傳輸，則ASA通過inspect ftp命令識別來自使用者的資料埠請求，並開啟一個大於1023的新資料埠。

inspect ftp命令檢查會檢查FTP會話並執行四項任務：

- 準備動態輔助資料連線
- 跟蹤FTP命令 — 響應序列
- 生成稽核跟蹤
- 使用NAT轉換嵌入式IP地址

FTP應用檢查為FTP資料傳輸準備輔助通道。通道是響應於檔案上傳、檔案下載或目錄清單事件而分配的，並且它們必須預先協商。連線埠是透過PORT或PASV(227)命令交涉。

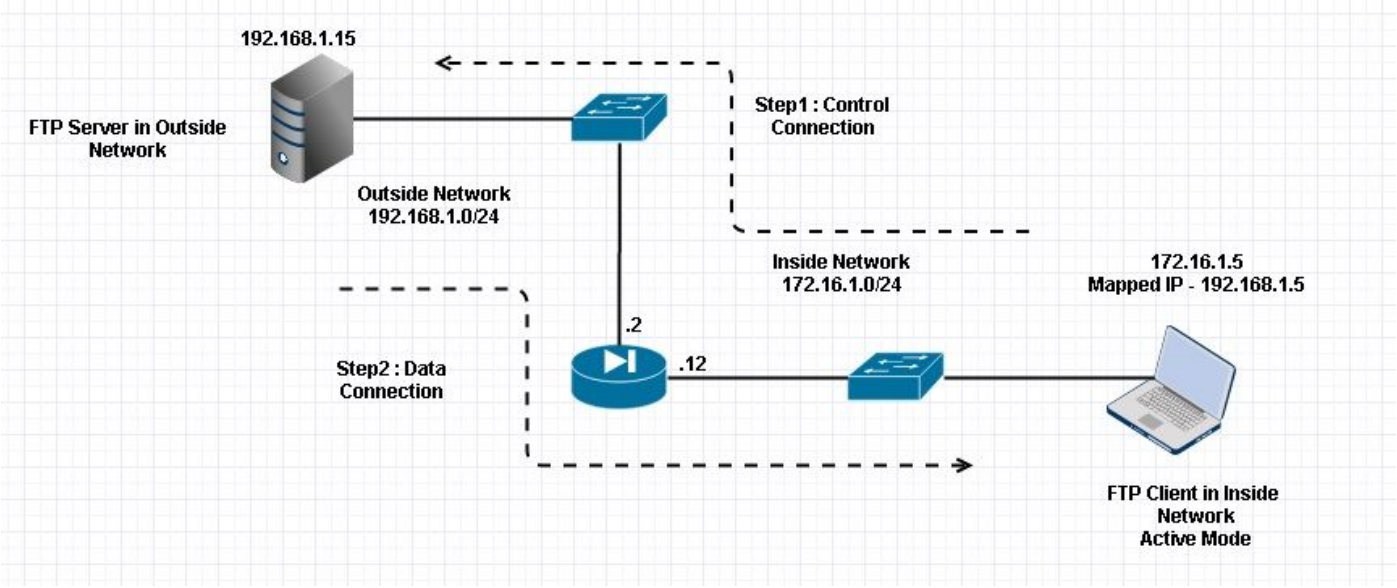
組態

注意：在ASA上啟用FTP檢測後，將解釋所有網路方案。

案例 1.為活動模式配置的FTP客戶端

客戶端連線到ASA的內部網路以及外部網路中的伺服器。

網路圖表



注意：此配置中使用的IP編址方案在Internet上不能合法路由。

如本圖所示，使用的網路設定具有在IP為172.16.1.5的內部網路中帶有客戶端的ASA。伺服器位於IP為192.168.1.15的外部網路中。客戶端在外部網路中有一個對映的IP 192.168.1.5。

因為FTP檢查會開啟動態埠通道，所以無需允許外部介面上的任何訪問清單。

組態範例:

<#root>

```
 ASA Version 9.1(5)
!
hostname ASA
domain-name corp. com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface GigabitEthernet0/0
  nameif Outside
  security-level 0
  ip address 192.168.1.2 255.255.255.0
 !
 interface GigabitEthernet0/1
  nameif Inside
  security-level 50
  ip address 172.16.1.12 255.255.255.0
 !
 interface GigabitEthernet0/2
  shutdown
  no nameif
  no security-level
  no ip address
 !
 interface GigabitEthernet0/3
  shutdown
  no nameif
  no security-level
```

```
  no ip address
 !
 interface Management0/0
  management-only
  shutdown
  no nameif
  no security-level
  no ip address


 !--- Output is suppressed.


 !--- Object groups is created to define the host.


object network obj-172.16.1.5
 subnet 172.16.1.0 255.255.255.0




 !--- Object NAT is created to map Inside Client to Outside subnet IP.



object network obj-172.16.1.5
 nat (Inside,Outside) dynamic 192.168.1.5

class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512


policy-map global_policy



class inspection_default

  inspect dns preset_dns_map


inspect ftp


  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
```

```
 !--- This command tells the device to
!--- use the "global_policy" policy-map on all interfaces.


service-policy global_policy global

prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
: end
ASA(config)#
```

驗證

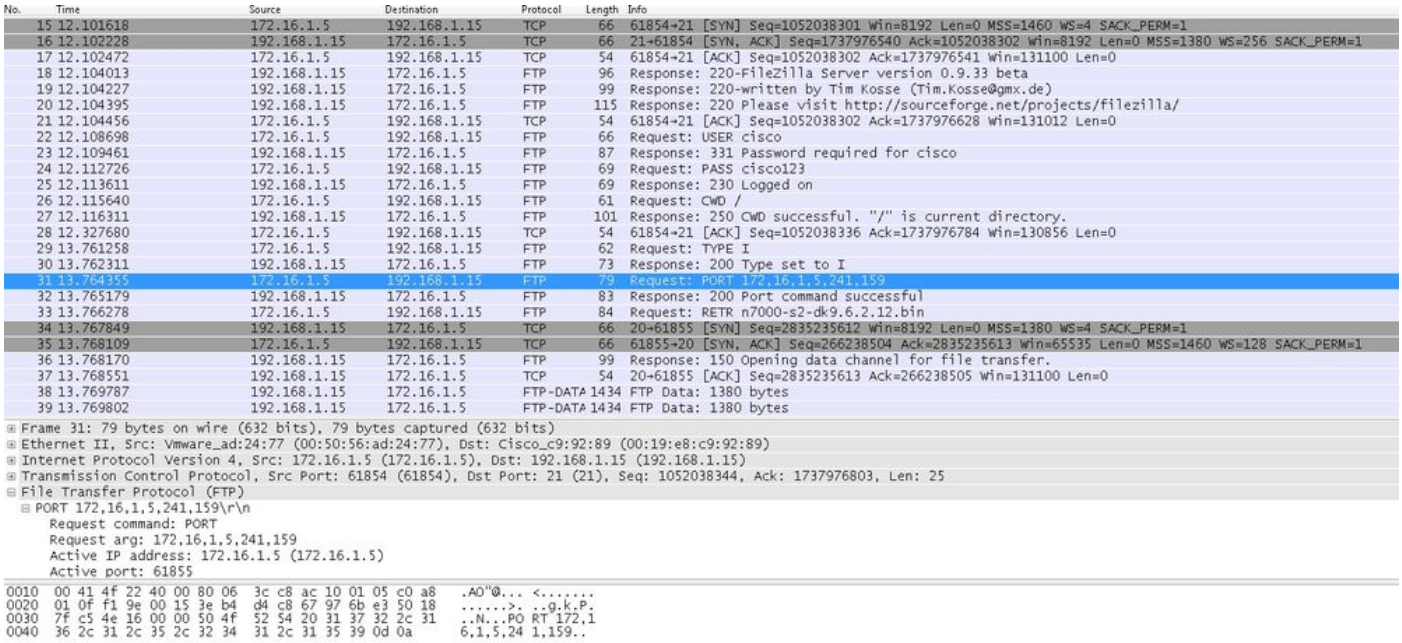
連線

<#root>

```
 Client in Inside Network running ACTIVE FTP:



 Ciscoasa(config)# sh conn
 3 in use, 3 most used

 TCP Outside

192.168.1.15:20 inside 172.16.1.5:61855

, idle 0:00:00, bytes 145096704, flags UIB

<--- Dynamic Connection Opened



 TCP Outside

192.168.1.15:21 inside 172.16.1.5:61854

, idle 0:00:00, bytes 434, flags UIO
```

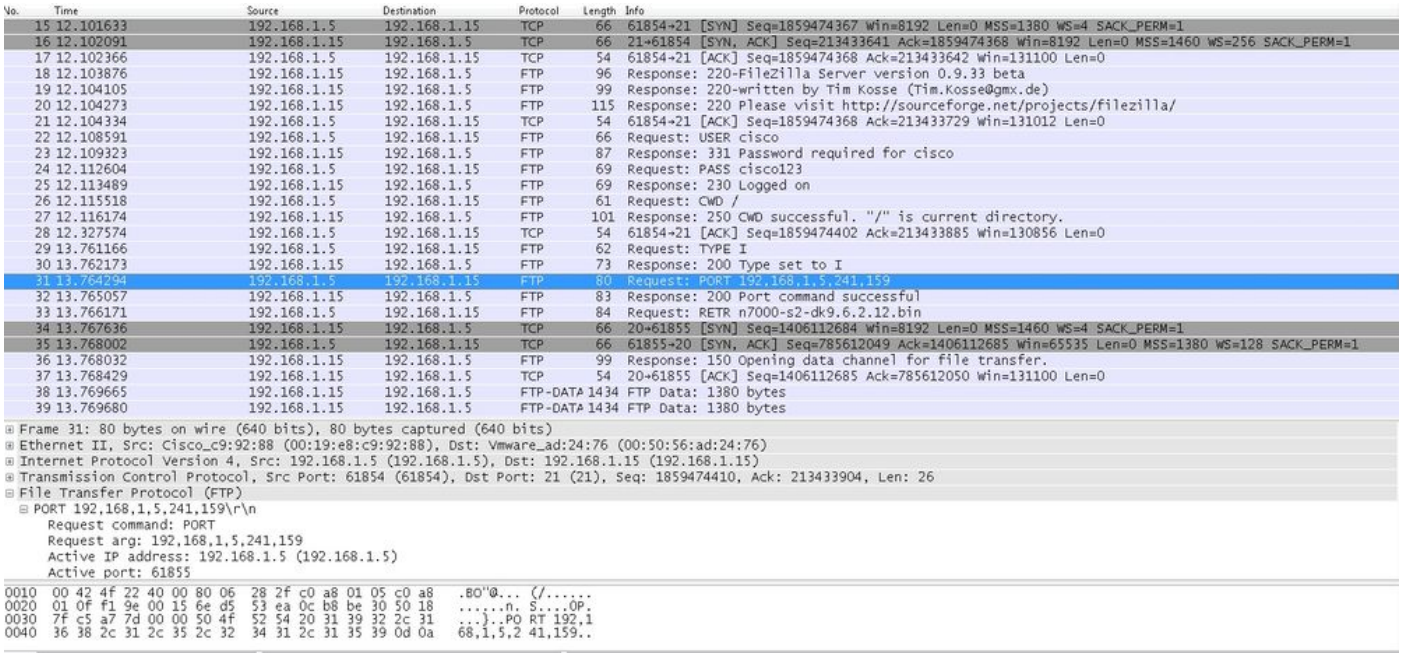
此處，Inside中的客戶端啟動與源埠61854到目標埠21的連線。然後使用者端會傳送含6個元組值的Port命令。伺服器反過來啟動輔助/資料連線，源埠為20，目的地埠則按照這些捕獲後提到的步驟進行計算。

Capture Inside Interface（捕獲內部介面），如下圖所示。



```
No.  Time       Source          Destination     Protocol Length Info
  15 12.101618  172.16.1.5      192.168.1.15    TCP      66     61854→21 [SYN] Seq=1052038301 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  16 12.102228  192.168.1.15    172.16.1.5      TCP      66     21→61854 [SYN, ACK] Seq=1737976540 Ack=1052038302 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
  17 12.102472  172.16.1.5      192.168.1.15    TCP      54     61854→21 [ACK] Seq=1052038302 Ack=1737976541 Win=131100 Len=0
  18 12.104013  192.168.1.15    172.16.1.5      FTP      96     Response: 220-FileZilla Server version 0.9.33 beta
  19 12.104227  192.168.1.15    172.16.1.5      FTP      99     Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
  20 12.104395  192.168.1.15    172.16.1.5      FTP      115    Response: 220 Please visit http://sourceforge.net/projects/filezilla/
  21 12.104456  172.16.1.5      192.168.1.15    TCP      54     61854→21 [ACK] Seq=1052038302 Ack=1737976628 Win=131012 Len=0
  22 12.108698  172.16.1.5      192.168.1.15    FTP      66     Request: USER cisco
  23 12.109461  192.168.1.15    172.16.1.5      FTP      87     Response: 331 Password required for cisco
  24 12.112726  172.16.1.5      192.168.1.15    FTP      69     Request: PASS cisco123
  25 12.113611  192.168.1.15    172.16.1.5      FTP      69     Response: 230 Logged on
  26 12.115640  172.16.1.5      192.168.1.15    FTP      61     Request: CWD /
  27 12.116311  192.168.1.15    172.16.1.5      FTP      101    Response: 250 CWD successful. "/" is current directory.
  28 12.327680  172.16.1.5      192.168.1.15    TCP      54     61854→21 [ACK] Seq=1052038336 Ack=1737976784 Win=130856 Len=0
  29 13.761258  172.16.1.5      192.168.1.15    FTP      62     Request: TYPE I
  30 13.762311  192.168.1.15    172.16.1.5      FTP      73     Response: 200 Type set to I
  31 13.764355  172.16.1.5      192.168.1.15    FTP      79     Request: PORT 172,16,1,5,241,159
  32 13.765179  192.168.1.15    172.16.1.5      FTP      83     Response: 200 Port command successful
  33 13.766278  172.16.1.5      192.168.1.15    FTP      84     Request: RETR n7000-s2-dk9.6.2.12.bin
  34 13.767849  192.168.1.15    172.16.1.5      TCP      66     20→61855 [SYN] Seq=2835235612 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
  35 13.768109  172.16.1.5      192.168.1.15    TCP      66     61855→20 [SYN, ACK] Seq=266238504 Ack=2835235613 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
  36 13.768170  192.168.1.15    172.16.1.5      FTP      99     Response: 150 Opening data channel for file transfer.
  37 13.768551  192.168.1.15    172.16.1.5      TCP      54     20→61855 [ACK] Seq=2835235613 Ack=266238505 Win=131100 Len=0
  38 13.769787  192.168.1.15    172.16.1.5      FTP-DATA 1434   FTP Data: 1380 bytes
  39 13.769802  192.168.1.15    172.16.1.5      FTP-DATA 1434   FTP Data: 1380 bytes

⊞ Frame 31: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
⊞ Ethernet II, Src: Vmware_ad:24:77 (00:50:56:ad:24:77), Dst: Cisco_c9:92:89 (00:19:e8:c9:92:89)
⊞ Internet Protocol Version 4, Src: 172.16.1.5 (172.16.1.5), Dst: 192.168.1.15 (192.168.1.15)
⊞ Transmission Control Protocol, Src Port: 61854 (61854), Dst Port: 21 (21), Seq: 1052038344, Ack: 1737976803, Len: 25
⊟ File Transfer Protocol (FTP)
  ⊟ PORT 172,16,1,5,241,159\r\n
      Request command: PORT
      Request arg: 172,16,1,5,241,159
      Active IP address: 172.16.1.5 (172.16.1.5)
      Active port: 61855

0010  00 41 4f 22 40 00 80 06  3c c8 ac 10 01 05 c0 a8   .AO"@... <.......
0020  01 0f f1 9e 00 15 3e b4  d4 c8 67 97 6b e3 50 18   ......>. ..g.k.P.
0030  7f c5 4e 16 00 00 50 4f  52 54 20 31 37 32 2c 31   ..N...PO RT 172,1
0040  36 2c 31 2c 35 2c 32 34  31 2c 31 35 39 0d 0a      6,1,5,24 1,159..
```

捕獲外部介面，如下圖所示。



```
No.  Time       Source          Destination     Protocol Length Info
  15 12.101633  192.168.1.5     192.168.1.15    TCP      66     61854→21 [SYN] Seq=1859474367 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
  16 12.102091  192.168.1.15    192.168.1.5     TCP      66     21→61854 [SYN, ACK] Seq=213433641 Ack=1859474368 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
  17 12.102366  192.168.1.5     192.168.1.15    TCP      54     61854→21 [ACK] Seq=1859474368 Ack=213433642 Win=131100 Len=0
  18 12.103876  192.168.1.15    192.168.1.5     FTP      96     Response: 220-FileZilla Server version 0.9.33 beta
  19 12.104105  192.168.1.15    192.168.1.5     FTP      99     Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
  20 12.104273  192.168.1.15    192.168.1.5     FTP      115    Response: 220 Please visit http://sourceforge.net/projects/filezilla/
  21 12.104334  192.168.1.5     192.168.1.15    TCP      54     61854→21 [ACK] Seq=1859474368 Ack=213433729 Win=131012 Len=0
  22 12.108591  192.168.1.5     192.168.1.15    FTP      66     Request: USER cisco
  23 12.109323  192.168.1.15    192.168.1.5     FTP      87     Response: 331 Password required for cisco
  24 12.112604  192.168.1.5     192.168.1.15    FTP      69     Request: PASS cisco123
  25 12.113489  192.168.1.15    192.168.1.5     FTP      69     Response: 230 Logged on
  26 12.115518  192.168.1.5     192.168.1.15    FTP      61     Request: CWD /
  27 12.116174  192.168.1.15    192.168.1.5     FTP      101    Response: 250 CWD successful. "/" is current directory.
  28 12.327574  192.168.1.5     192.168.1.15    TCP      54     61854→21 [ACK] Seq=1859474402 Ack=213433885 Win=130856 Len=0
  29 13.761166  192.168.1.5     192.168.1.15    FTP      62     Request: TYPE I
  30 13.762173  192.168.1.15    192.168.1.5     FTP      73     Response: 200 Type set to I
  31 13.764294  192.168.1.5     192.168.1.15    FTP      80     Request: PORT 192,168,1,5,241,159
  32 13.765057  192.168.1.15    192.168.1.5     FTP      83     Response: 200 Port command successful
  33 13.766171  192.168.1.5     192.168.1.15    FTP      84     Request: RETR n7000-s2-dk9.6.2.12.bin
  34 13.767636  192.168.1.15    192.168.1.5     TCP      66     20→61855 [SYN] Seq=1406112684 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
  35 13.768002  192.168.1.5     192.168.1.15    TCP      66     61855→20 [SYN, ACK] Seq=785612049 Ack=1406112685 Win=65535 Len=0 MSS=1380 WS=128 SACK_PERM=1
  36 13.768032  192.168.1.15    192.168.1.5     FTP      99     Response: 150 Opening data channel for file transfer.
  37 13.768429  192.168.1.15    192.168.1.5     TCP      54     20→61855 [ACK] Seq=1406112685 Ack=785612050 Win=131100 Len=0
  38 13.769665  192.168.1.15    192.168.1.5     FTP-DATA 1434   FTP Data: 1380 bytes
  39 13.769680  192.168.1.15    192.168.1.5     FTP-DATA 1434   FTP Data: 1380 bytes

⊞ Frame 31: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
⊞ Ethernet II, Src: Cisco_c9:92:88 (00:19:e8:c9:92:88), Dst: Vmware_ad:24:76 (00:50:56:ad:24:76)
⊞ Internet Protocol Version 4, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.15 (192.168.1.15)
⊞ Transmission Control Protocol, Src Port: 61854 (61854), Dst Port: 21 (21), Seq: 1859474410, Ack: 213433904, Len: 26
⊟ File Transfer Protocol (FTP)
  ⊟ PORT 192,168,1,5,241,159\r\n
      Request command: PORT
      Request arg: 192,168,1,5,241,159
      Active IP address: 192.168.1.5 (192.168.1.5)
      Active port: 61855

0010  00 42 4f 22 40 00 80 06  28 2f c0 a8 01 05 c0 a8   .BO"@... (/......
0020  01 0f f1 9e 00 15 6e d5  53 ea 0c b8 be 30 50 18   ......n. S....0P.
0030  7f c5 a7 7d 00 00 50 4f  52 54 20 31 39 32 2c 31   ...}..PO RT 192,1
0040  36 38 2c 31 2c 35 2c 32  34 31 2c 31 35 39 0d 0a   68,1,5,2 41,159..
```

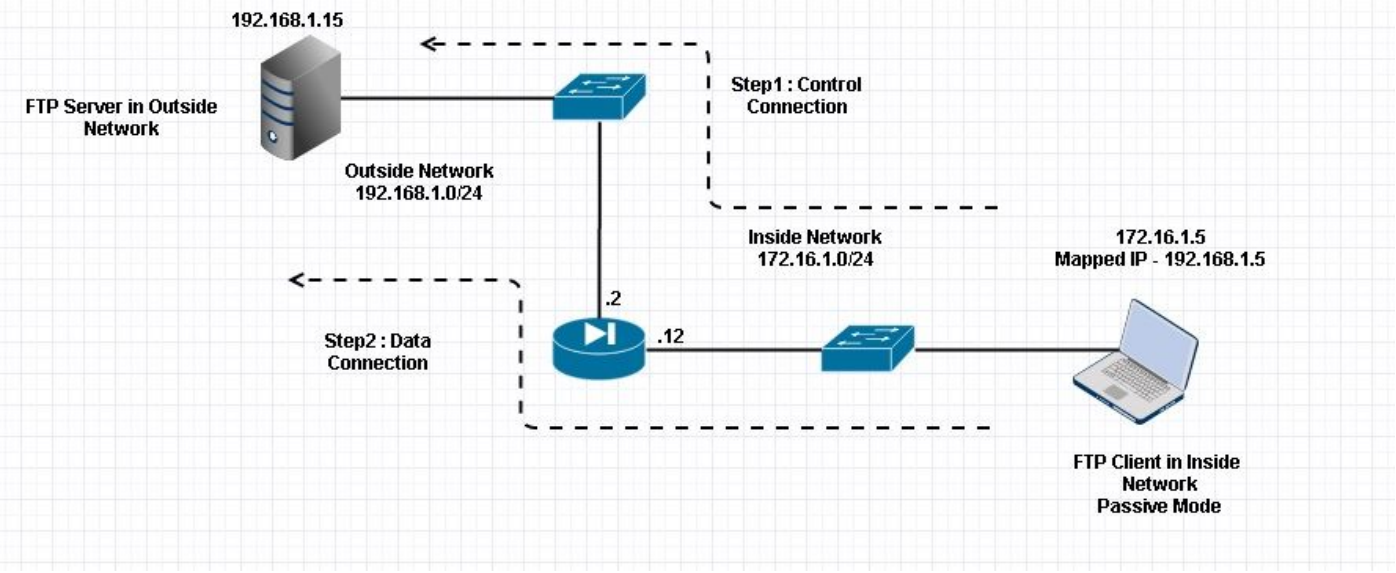
埠值使用最後兩個（共六個）的示例進行計算。剩餘4個元組是IP地址，2個元組用於埠。如圖所示，IP地址為192.168.1.5和241*256 + 159 = 61855。

Capture（捕獲）還顯示，啟用FTP檢測後，埠命令的值會發生更改。Inside Interface Capture顯示IP的實際值，而Client for Server傳送的埠則用於連線到客戶端的資料通道，Outside Interface Capture則顯示對映地址。

案例 2.為被動模式配置的FTP客戶端

ASA內部網路中的客戶端和外部網路中的伺服器。

網路圖表



連線

<#root>

Client in Inside Network running Passive Mode FTP:

ciscoasa(config)# sh conn
3 in use, 3 most used

TCP Outside

192

.168.1.15:60142 inside 172.16.1.5:61839

, idle 0:00:00, bytes 184844288, flags UI

<--- Dynamic Connection Opened.

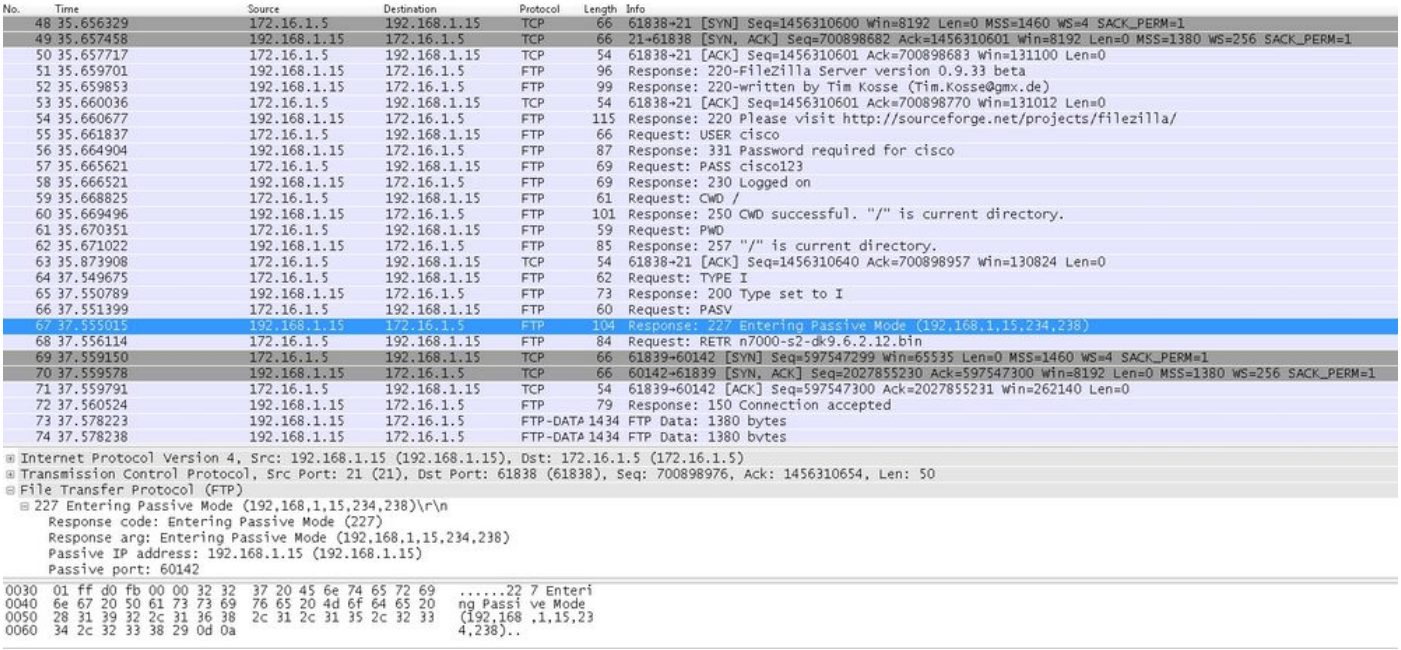
TCP Outside

192.168.1.15:21 inside 172.16.1.5:61838

, idle 0:00:00, bytes 451, flags UIO

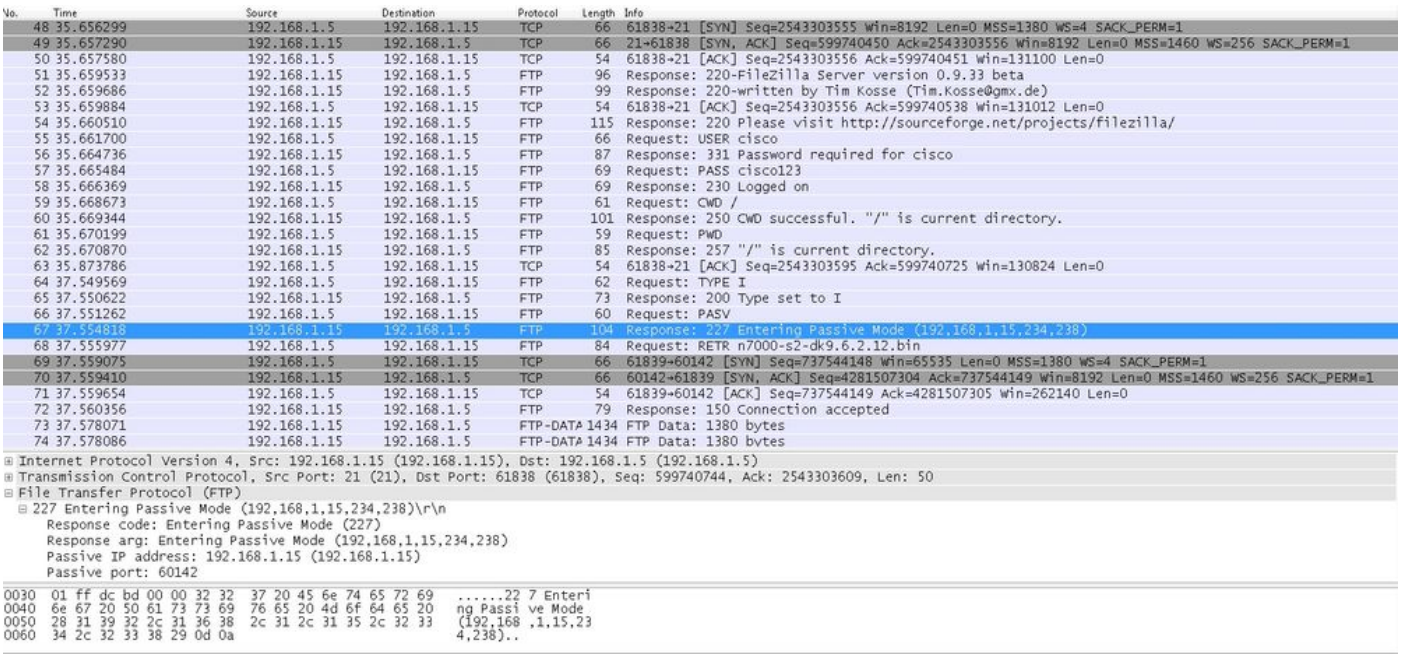
這裡，內部客戶端啟動與源埠和目61838埠21的連線。由於是被動式FTP，使用者端會啟動兩個連線。因此，在客戶端傳送PASV命令後，伺服器會使用其6元組值進行回覆，並且客戶端會連線到該套接字以進行資料連線。

Capture Inside Interface（捕獲內部介面），如下圖所示。



```
No.     Time           Source          Destination     Protocol Length Info
    48 35.656329      172.16.1.5      192.168.1.15    TCP      66     61838→21 [SYN] Seq=1456310600 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    49 35.657458      192.168.1.15    172.16.1.5      TCP      66     21→61838 [SYN, ACK] Seq=700898682 Ack=1456310601 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
    50 35.657717      172.16.1.5      192.168.1.15    TCP      54     61838→21 [ACK] Seq=1456310601 Ack=700898683 Win=131100 Len=0
    51 35.659701      192.168.1.15    172.16.1.5      FTP      96     Response: 220-FileZilla Server version 0.9.33 beta
    52 35.659853      192.168.1.15    172.16.1.5      FTP      99     Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
    53 35.660036      172.16.1.5      192.168.1.15    TCP      54     61838→21 [ACK] Seq=1456310601 Ack=700898770 Win=131012 Len=0
    54 35.660677      192.168.1.15    172.16.1.5      FTP      115    Response: 220 Please visit http://sourceforge.net/projects/filezilla/
    55 35.661837      172.16.1.5      192.168.1.15    FTP      66     Request: USER cisco
    56 35.664904      192.168.1.15    172.16.1.5      FTP      87     Response: 331 Password required for cisco
    57 35.665621      172.16.1.5      192.168.1.15    FTP      69     Request: PASS cisco123
    58 35.666521      192.168.1.15    172.16.1.5      FTP      69     Response: 230 Logged on
    59 35.668825      172.16.1.5      192.168.1.15    FTP      61     Request: CWD /
    60 35.669496      192.168.1.15    172.16.1.5      FTP      101    Response: 250 CWD successful. "/" is current directory.
    61 35.670351      172.16.1.5      192.168.1.15    FTP      59     Request: PWD
    62 35.671022      192.168.1.15    172.16.1.5      FTP      85     Response: 257 "/" is current directory.
    63 35.873908      172.16.1.5      192.168.1.15    TCP      54     61838→21 [ACK] Seq=1456310640 Ack=700898957 Win=130824 Len=0
    64 37.549675      172.16.1.5      192.168.1.15    FTP      62     Request: TYPE I
    65 37.550789      192.168.1.15    172.16.1.5      FTP      73     Response: 200 Type set to I
    66 37.551399      172.16.1.5      192.168.1.15    FTP      60     Request: PASV
    67 37.555015      192.168.1.15    172.16.1.5      FTP      104    Response: 227 Entering Passive Mode (192,168,1,15,234,238)
    68 37.556114      172.16.1.5      192.168.1.15    FTP      84     Request: RETR n7000-s2-dk9.6.2.12.bin
    69 37.559150      172.16.1.5      192.168.1.15    TCP      66     61839→60142 [SYN] Seq=597547299 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
    70 37.559578      192.168.1.15    172.16.1.5      TCP      66     60142→61839 [SYN, ACK] Seq=2027855230 Ack=597547300 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
    71 37.559791      172.16.1.5      192.168.1.15    TCP      54     61839→60142 [ACK] Seq=597547300 Ack=2027855231 Win=262140 Len=0
    72 37.560524      192.168.1.15    172.16.1.5      FTP      79     Response: 150 Connection accepted
    73 37.578223      192.168.1.15    172.16.1.5      FTP-DATA 1434   FTP Data: 1380 bytes
    74 37.578238      192.168.1.15    172.16.1.5      FTP-DATA 1434   FTP Data: 1380 bytes
⊞ Internet Protocol Version 4, Src: 192.168.1.15 (192.168.1.15), Dst: 172.16.1.5 (172.16.1.5)
⊞ Transmission Control Protocol, Src Port: 21 (21), Dst Port: 61838 (61838), Seq: 700898976, Ack: 1456310654, Len: 50
⊟ File Transfer Protocol (FTP)
  ⊟ 227 Entering Passive Mode (192,168,1,15,234,238)\r\n
      Response code: Entering Passive Mode (227)
      Response arg: Entering Passive Mode (192,168,1,15,234,238)
      Passive IP address: 192.168.1.15 (192.168.1.15)
      Passive port: 60142
0030  01 ff d0 fb 00 00 32 32  37 20 45 6e 74 65 72 69   ......22 7 Enteri
0040  6e 67 20 50 61 73 73 69  76 65 20 4d 6f 64 65 20   ng Passi ve Mode
0050  28 31 39 32 2c 31 36 38  2c 31 2c 31 35 2c 32 33   (192,168 ,1,15,23
0060  34 2c 32 33 38 29 0d 0a                           4,238)..
```

捕獲外部介面，如下圖所示。



```
No.     Time           Source          Destination     Protocol Length Info
    48 35.656299      192.168.1.5     192.168.1.15    TCP      66     61838→21 [SYN] Seq=2543303555 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
    49 35.657290      192.168.1.15    192.168.1.5     TCP      66     21→61838 [SYN, ACK] Seq=599740450 Ack=2543303556 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    50 35.657580      192.168.1.5     192.168.1.15    TCP      54     61838→21 [ACK] Seq=2543303556 Ack=599740451 Win=131100 Len=0
    51 35.659533      192.168.1.15    192.168.1.5     FTP      96     Response: 220-FileZilla Server version 0.9.33 beta
    52 35.659686      192.168.1.15    192.168.1.5     FTP      99     Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
    53 35.659884      192.168.1.5     192.168.1.15    TCP      54     61838→21 [ACK] Seq=2543303556 Ack=599740538 Win=131012 Len=0
    54 35.660510      192.168.1.15    192.168.1.5     FTP      115    Response: 220 Please visit http://sourceforge.net/projects/filezilla/
    55 35.661700      192.168.1.5     192.168.1.15    FTP      66     Request: USER cisco
    56 35.664736      192.168.1.15    192.168.1.5     FTP      87     Response: 331 Password required for cisco
    57 35.665484      192.168.1.5     192.168.1.15    FTP      69     Request: PASS cisco123
    58 35.666369      192.168.1.15    192.168.1.5     FTP      69     Response: 230 Logged on
    59 35.668673      192.168.1.5     192.168.1.15    FTP      61     Request: CWD /
    60 35.669344      192.168.1.15    192.168.1.5     FTP      101    Response: 250 CWD successful. "/" is current directory.
    61 35.670199      192.168.1.5     192.168.1.15    FTP      59     Request: PWD
    62 35.670870      192.168.1.15    192.168.1.5     FTP      85     Response: 257 "/" is current directory.
    63 35.873786      192.168.1.5     192.168.1.15    TCP      54     61838→21 [ACK] Seq=2543303595 Ack=599740725 Win=130824 Len=0
    64 37.549569      192.168.1.5     192.168.1.15    FTP      62     Request: TYPE I
    65 37.550622      192.168.1.15    192.168.1.5     FTP      73     Response: 200 Type set to I
    66 37.551262      192.168.1.5     192.168.1.15    FTP      60     Request: PASV
    67 37.554818      192.168.1.15    192.168.1.5     FTP      104    Response: 227 Entering Passive Mode (192,168,1,15,234,238)
    68 37.555977      192.168.1.5     192.168.1.15    FTP      84     Request: RETR n7000-s2-dk9.6.2.12.bin
    69 37.559075      192.168.1.5     192.168.1.15    TCP      66     61839→60142 [SYN] Seq=737544148 Win=65535 Len=0 MSS=1380 WS=4 SACK_PERM=1
    70 37.559410      192.168.1.15    192.168.1.5     TCP      66     60142→61839 [SYN, ACK] Seq=4281507304 Ack=737544149 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
    71 37.559654      192.168.1.5     192.168.1.15    TCP      54     61839→60142 [ACK] Seq=737544149 Ack=4281507305 Win=262140 Len=0
    72 37.560356      192.168.1.15    192.168.1.5     FTP      79     Response: 150 Connection accepted
    73 37.578071      192.168.1.15    192.168.1.5     FTP-DATA 1434   FTP Data: 1380 bytes
    74 37.578086      192.168.1.15    192.168.1.5     FTP-DATA 1434   FTP Data: 1380 bytes
⊞ Internet Protocol Version 4, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.5 (192.168.1.5)
⊞ Transmission Control Protocol, Src Port: 21 (21), Dst Port: 61838 (61838), Seq: 599740744, Ack: 2543303609, Len: 50
⊟ File Transfer Protocol (FTP)
  ⊟ 227 Entering Passive Mode (192,168,1,15,234,238)\r\n
      Response code: Entering Passive Mode (227)
      Response arg: Entering Passive Mode (192,168,1,15,234,238)
      Passive IP address: 192.168.1.15 (192.168.1.15)
      Passive port: 60142
0030  01 ff dc bd 00 00 32 32  37 20 45 6e 74 65 72 69   ......22 7 Enteri
0040  6e 67 20 50 61 73 73 69  76 65 20 4d 6f 64 65 20   ng Passi ve Mode
0050  28 31 39 32 2c 31 36 38  2c 31 2c 31 35 2c 32 33   (192,168 ,1,15,23
0060  34 2c 32 33 38 29 0d 0a                           4,238)..
```

連線埠的計算方式保持不變。

如前所述，如果啟用了FTP檢測，ASA將重寫嵌入的IP值。此外，它還會為資料連線開啟動態埠通道。

以下是連線詳細資訊，如果 FTP檢測已禁用

Connection:

<#root>

```
ciscoasa(config)# sh conn
2 in use, 3 most used
```

```
 TCP Outside
```

192.168.1.15:21 inside 172.16.1.5:61878

```
, idle 0:00:09, bytes 433, flags UIO
 TCP Outside
```

192.168.1.15:21 inside 172.16.1.5:61875

```
, idle 0:00:29, bytes 259, flags UIO
```

如果沒有FTP檢查，它只會嘗試反複傳送port命令，但是沒有應答，因為外部接收的PORT帶有原始IP且沒有NAT地址。垃圾場上也出現了同樣的現象。

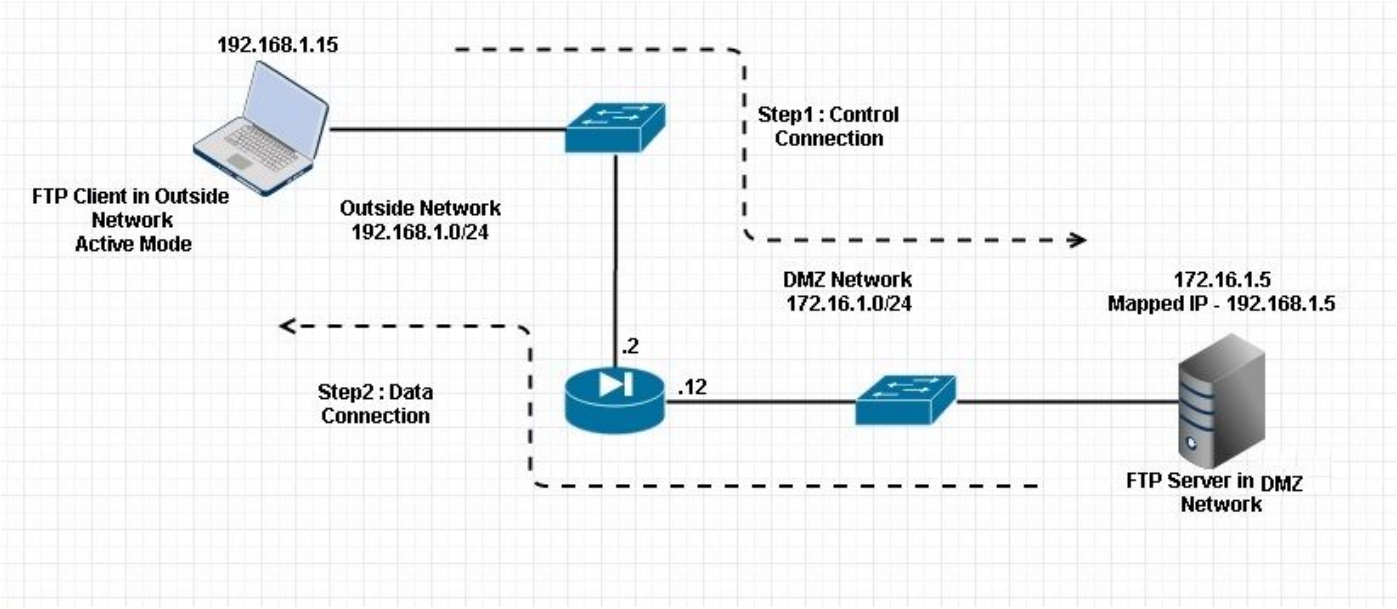
在配置終端模式下可使用no fixup protocol ftp 21命令禁用FTP檢查。

如果沒有FTP檢查，則只有PASV命令在客戶端位於Inside時有效，因為沒有port命令來自Inside，需要嵌入該命令，並且兩個連線都是從Inside發起的。

案例 3.為活動模式配置的FTP客戶端

ASA外部網路中的客戶端和DMZ網路中的伺服器。

網路圖表



組態:

<#root>

```
 ASA(config)#
```

show running-config

```
 ASA Version 9.1(5)
!
hostname ASA
domain-name corp .com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface GigabitEthernet0/0
  nameif Outside
  security-level 0
  ip address 192.168.1.2 255.255.255.0
 !
 interface GigabitEthernet0/1
  nameif DMZ
  security-level 50
  ip address 172.16.1.12 255.255.255.0
 !
 interface GigabitEthernet0/2
  shutdown
  no nameif
  no security-level
  no ip address
 !
 interface GigabitEthernet0/3
  shutdown
  no nameif
  no security-level
  no ip address
 !
 interface Management0/0
  management-only
  shutdown
  no nameif
  no security-level
  no ip address

 !--- Output is suppressed.

 !--- Permit inbound FTP control traffic.
```

access-list 100 extended permit tcp any host 192.168.1.5 eq ftp

```
 !--- Object groups are created to define the hosts.
```

object network obj-172.16.1.5
host 172.16.1.5

```
 !--- Object NAT is created to map FTP server with IP of Outside Subnet.
```

object network obj-172.16.1.5
nat (DMZ,Outside) static 192.168.1.5

```
access-group 100 in interface outside



class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512


policy-map global_policy



class inspection_default

  inspect dns preset_dns_map


inspect ftp


  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
 !--- This command tells the device to
!--- use the "global_policy" policy-map on all interfaces.


service-policy global_policy global

prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
: end
ASA(config)#
```

驗證

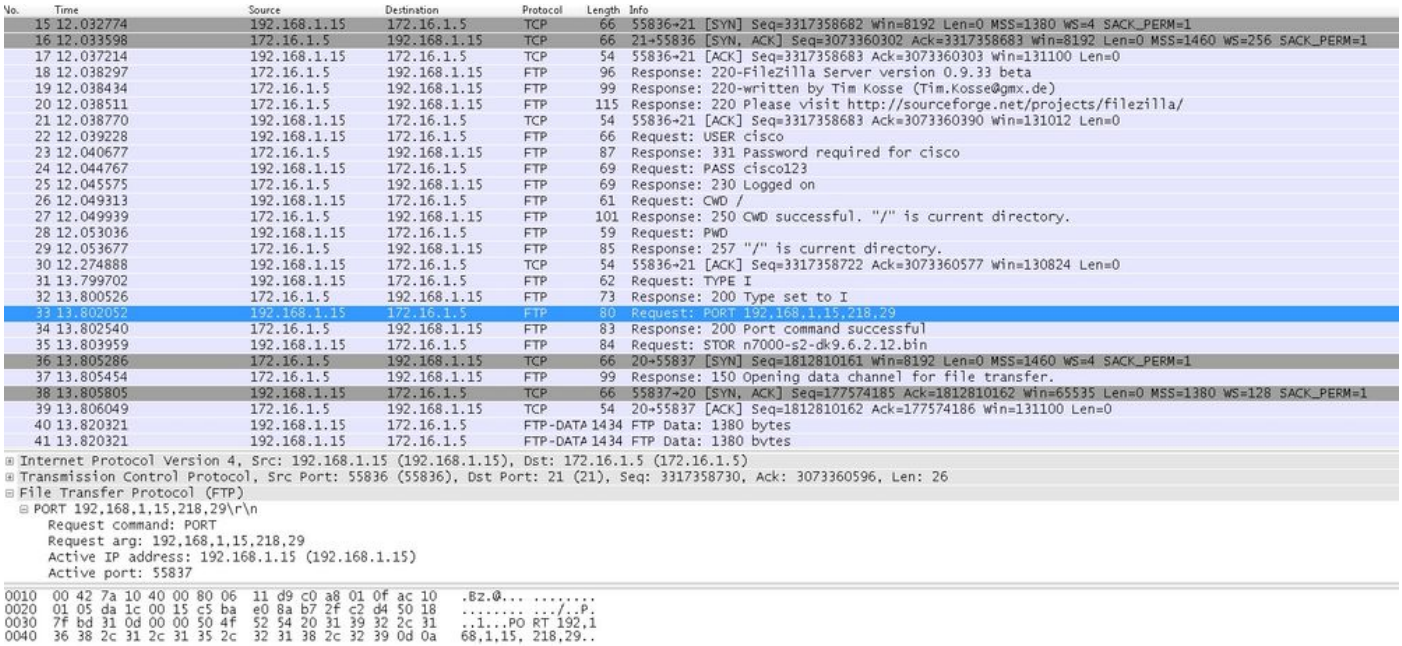
Connection:

<#root>

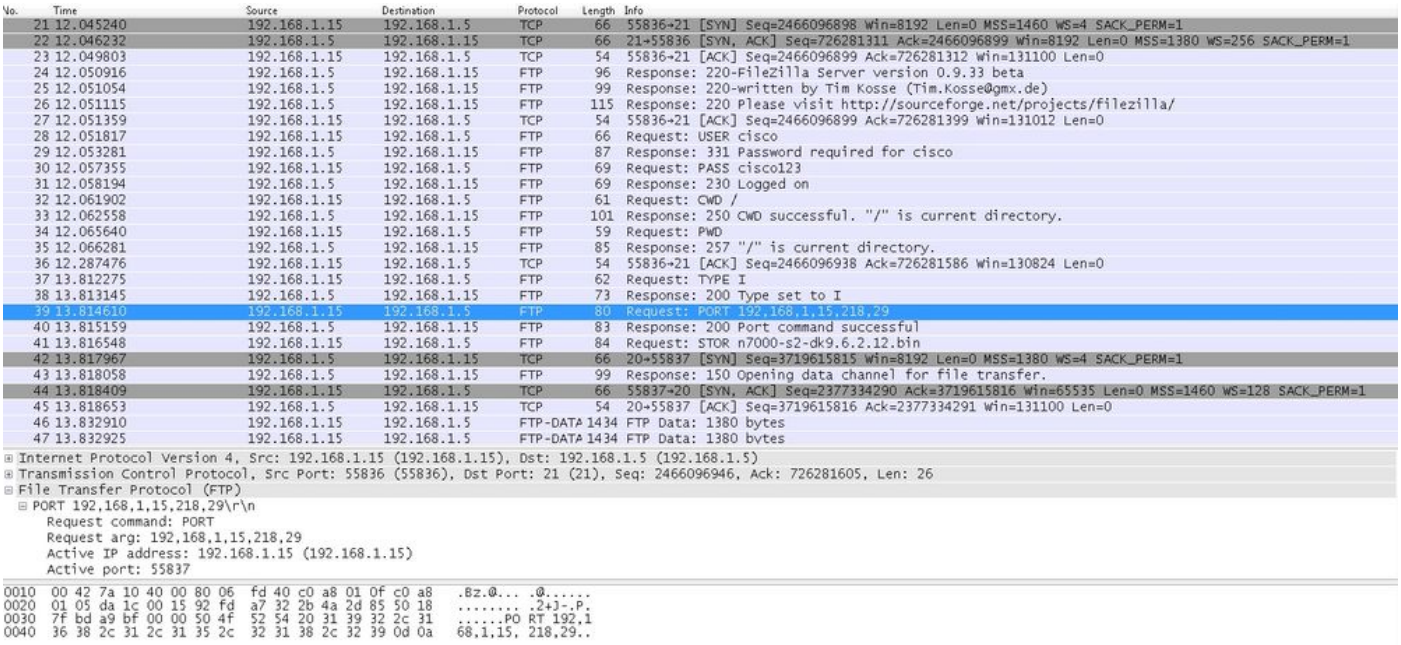
Client in Outside Network running in Active Mode FTP:

```
ciscoasa(config)# sh conn
3 in use, 3 most used

TCP outside 192.168.1.15:55836 DMZ 172.16.1.5:21,

idle 0:00:00, bytes 470, flags UIOB


TCP outside 192.168.1.15:55837 DMZ 172.16.1.5:20,

idle 0:00:00, bytes 225595694, flags UI

<--- Dynamic Port channel
```

擷取DMZ介面，如下圖所示。



捕獲外部介面，如下圖所示。



No.	Time	Source	Destination	Protocol	Length	Info
21	12.045240	192.168.1.15	192.168.1.5	TCP	66	55836→21 [SYN] Seq=2466096898 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
22	12.046232	192.168.1.5	192.168.1.15	TCP	66	21→55836 [SYN, ACK] Seq=726281311 Ack=2466096899 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
23	12.049803	192.168.1.15	192.168.1.5	TCP	54	55836→21 [ACK] Seq=2466096899 Ack=726281312 Win=131100 Len=0
24	12.050916	192.168.1.5	192.168.1.15	FTP	96	Response: 220-FileZilla Server version 0.9.33 beta
25	12.051054	192.168.1.5	192.168.1.15	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
26	12.051115	192.168.1.5	192.168.1.15	FTP	115	Response: 220 Please visit http://sourceforge.net/projects/filezilla/
27	12.051359	192.168.1.15	192.168.1.5	TCP	54	55836→21 [ACK] Seq=2466096899 Ack=726281399 Win=131012 Len=0
28	12.051817	192.168.1.15	192.168.1.5	FTP	66	Request: USER cisco
29	12.053281	192.168.1.5	192.168.1.15	FTP	87	Response: 331 Password required for cisco
30	12.057355	192.168.1.15	192.168.1.5	FTP	69	Request: PASS cisco123
31	12.058194	192.168.1.5	192.168.1.15	FTP	69	Response: 230 Logged on
32	12.061902	192.168.1.15	192.168.1.5	FTP	61	Request: CWD /
33	12.062558	192.168.1.5	192.168.1.15	FTP	101	Response: 250 CWD successful. "/" is current directory.
34	12.065640	192.168.1.15	192.168.1.5	FTP	59	Request: PWD
35	12.066281	192.168.1.5	192.168.1.15	FTP	85	Response: 257 "/" is current directory.
36	12.287476	192.168.1.15	192.168.1.5	TCP	54	55836→21 [ACK] Seq=2466096938 Ack=726281586 Win=130824 Len=0
37	13.812275	192.168.1.15	192.168.1.5	FTP	62	Request: TYPE I
38	13.813145	192.168.1.5	192.168.1.15	FTP	73	Response: 200 Type set to I
39	13.814610	192.168.1.15	192.168.1.5	FTP	80	Request: PORT 192,168,1,15,218,29
40	13.815159	192.168.1.5	192.168.1.15	FTP	83	Response: 200 Port command successful
41	13.816548	192.168.1.15	192.168.1.5	FTP	84	Request: STOR n7000-s2-dk9.6.2.12.bin
42	13.817967	192.168.1.5	192.168.1.15	TCP	66	20→55837 [SYN] Seq=3719615815 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
43	13.818058	192.168.1.5	192.168.1.15	FTP	99	Response: 150 Opening data channel for file transfer.
44	13.818409	192.168.1.15	192.168.1.5	TCP	66	55837→20 [SYN, ACK] Seq=2377334290 Ack=3719615816 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
45	13.818653	192.168.1.5	192.168.1.15	TCP	54	20→55837 [ACK] Seq=3719615816 Ack=2377334291 Win=131100 Len=0
46	13.832910	192.168.1.15	192.168.1.5	FTP-DATA	1434	FTP Data: 1380 bytes
47	13.832925	192.168.1.15	192.168.1.5	FTP-DATA	1434	FTP Data: 1380 bytes

```
⊞ Internet Protocol Version 4, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.5 (192.168.1.5)
⊞ Transmission Control Protocol, Src Port: 55836 (55836), Dst Port: 21 (21), Seq: 2466096946, Ack: 726281605, Len: 26
⊟ File Transfer Protocol (FTP)
  ⊟ PORT 192,168,1,15,218,29\r\n
      Request command: PORT
      Request arg: 192,168,1,15,218,29
      Active IP address: 192.168.1.15 (192.168.1.15)
      Active port: 55837
```

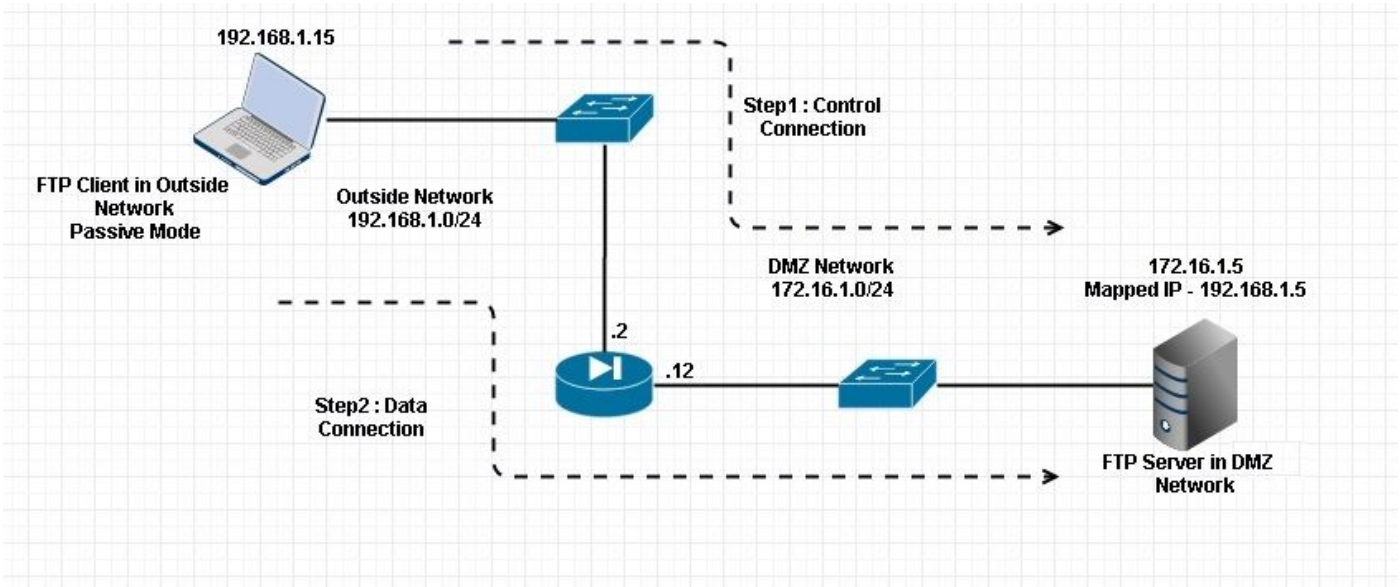
```
0010  00 42 7a 10 40 00 80 06  fd 40 c0 a8 01 0f c0 a8   .Bz.@... .@......
0020  01 05 da 1c 00 15 92 fd  a7 32 2b 4a 2d 85 50 18   ........ .2+J-.P.
0030  7f bd a9 bf 00 00 50 4f  52 54 20 31 39 32 2c 31   ......PO RT 192,1
0040  36 38 2c 31 2c 31 35 2c  32 31 38 2c 32 39 0d 0a   68,1,15, 218,29..
```

在這裡，客戶端運行活動模式客戶端192.168.1.15，並在埠21上啟動到DMZ中伺服器的連線。然後使用者端將包含六個元組值的port命令傳送到伺服器以連線到該特定動態連線埠。然後，伺服器啟動源埠為20的資料連線。

案例 4.FTP客戶端運行被動模式

ASA外部網路中的客戶端和DMZ網路中的伺服器。

網路圖表



連線

<#root>

Client in Outside Network running in Passive Mode FTP:

```
 ciscoasa(config)# sh conn
 3 in use, 3 most used

 TCP
```

Outside 192.168.1.15:60071 DMZ 172.16.1.5:61781

```
, idle 0:00:00, bytes 184718032, flags UOB
```

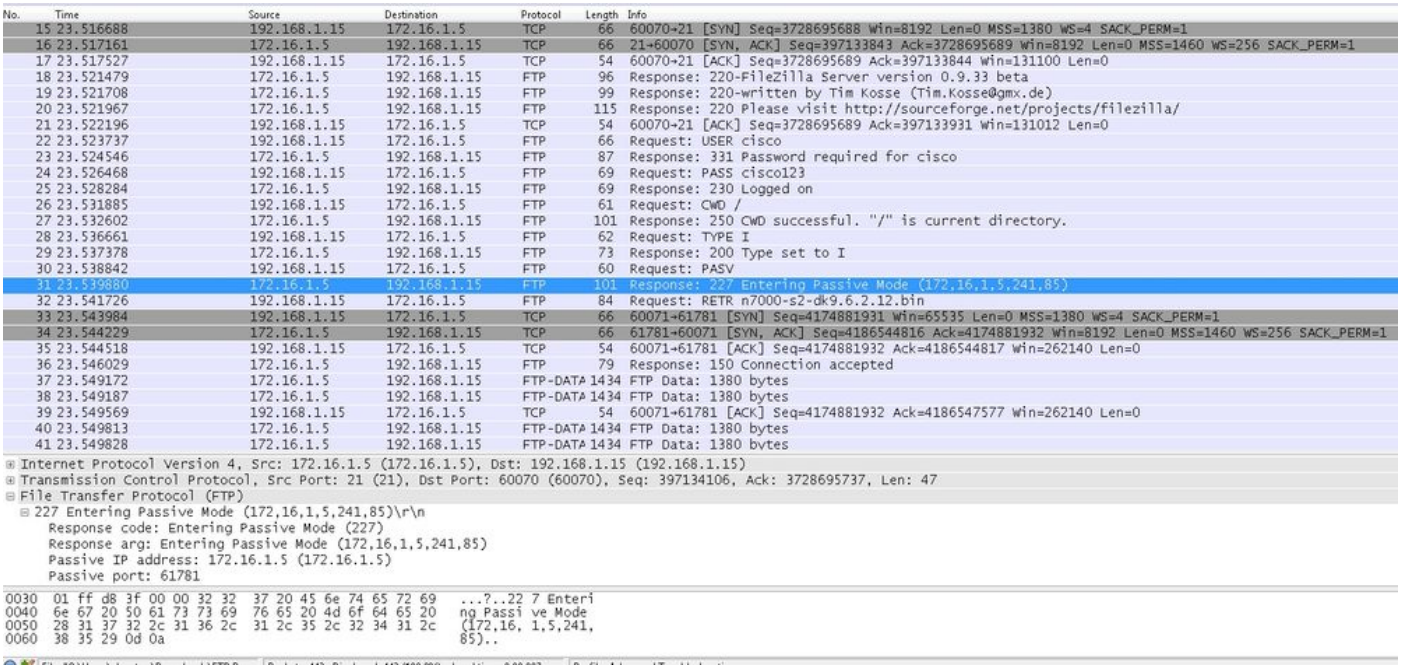
<--- Dynamic channel Open

```
 TCP
```

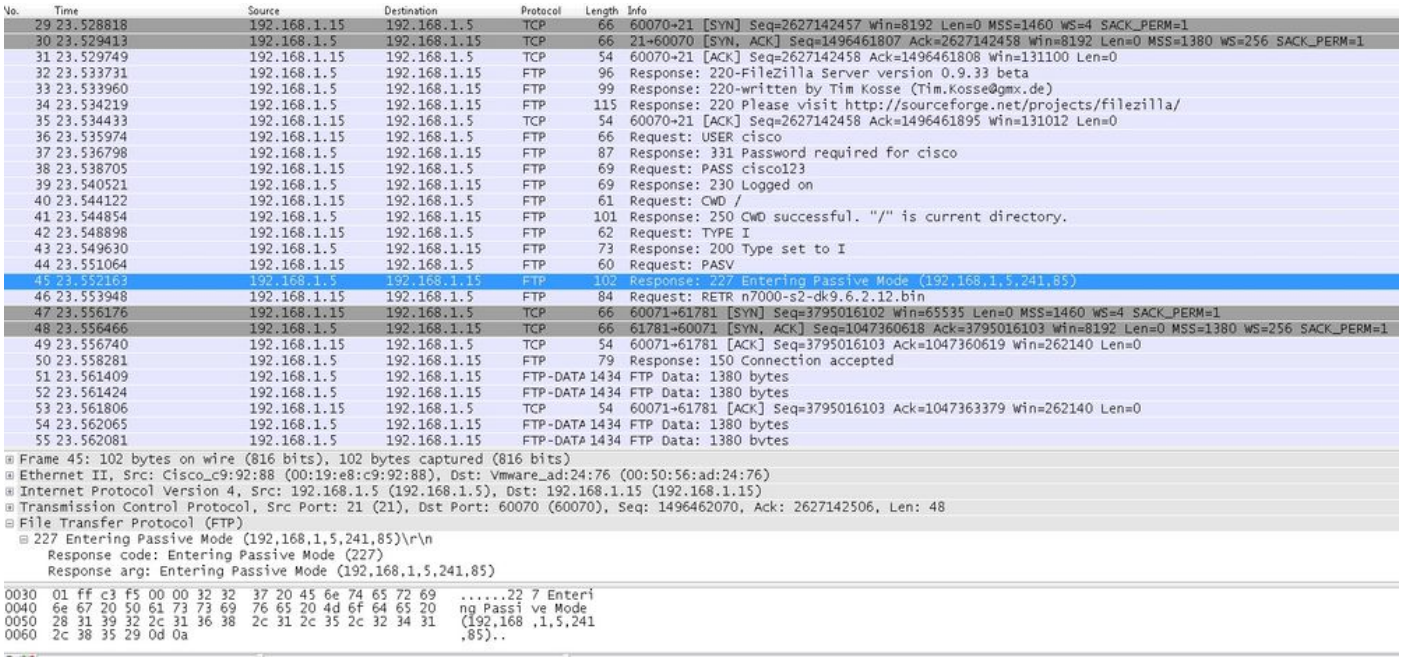
Outside 192.168.1.15:60070 DMZ 172.16.1.5:21

```
, idle 0:00:00, bytes 413,
flags UIOB
```

擷取DMZ介面，如下圖所示。



捕獲外部介面，如下圖所示。



配置基本FTP應用檢測

預設情況下，配置包含與所有預設應用檢測流量匹配並將檢測應用於所有介面上的流量的策略（全域性策略）。預設應用檢測流量包括到每個協定的預設埠的流量。

您只能應用一個全域性策略，因此，如果要更改全域性策略（例如，將檢測應用於非標準埠，或新增預設情況下未啟用的檢測），則需要編輯預設策略或禁用該策略並應用新的策略。有關所有預設埠的清單，請參閱預設檢測策略。

1. 運行policy-map global_policy命令。

<#root>

ASA(config)#

policy-map global_policy

2. 運行class inspection_default命令。

<#root>

ASA(config-pmap)#

class inspection_default

3. 執行inspect FTP 指令。

<#root>

ASA(config-pmap-c)#

inspect FTP

4. 有一個選項可用於使用inspect FTP strict命令。此命令通過阻止Web瀏覽器在FTP請求中傳送嵌入式命令，提高了受保護網路的安全。

   在介面上啟用 strict選項後，FTP檢查會強制執行以下行為：

   - 必須在安全裝置允許新命令之前確認FTP命令
   - 安全裝置會丟棄傳送嵌入式命令的連線
   - 會檢查227和PORT命令，以確保它們不會顯示在錯誤字串中

   警告：使用strict選項可能會導致嚴格符合FTP RFC的FTP客戶端出現故障。請參閱使用strict選項，瞭解有關使用strict選項的詳細資訊。

在非標準TCP埠上配置FTP協定檢測

您可以使用以下配置行為非標準TCP埠配置FTP協定檢測（用新埠號替換XXXX）：

<#root>

```
 access-list ftp-list extended permit tcp any any eq XXXX
!
class-map ftp-class
  match access-list ftp-list
!
policy-map global_policy
  class ftp-class
```

inspect ftp

驗證

要確保配置已成功執行，請運行show service-policy命令。此外，通過運行show service-policy inspect ftp 命令將輸出限製為FTP檢查。

<#root>

ASA#

```
show service-policy inspect ftp

         Global Policy:
          Service-policy: global_policy
           Class-map: inspection_default
            Inspect: ftp, packet 0, drop 0, reste-drop 0
        ASA#
```

TFTP

預設情況下啟用TFTP檢測。

安全裝置會檢查TFTP流量，並在必要時動態建立連線和轉換，以允許在TFTP客戶端和伺服器之間傳輸檔案。具體來說，檢查引擎檢查TFTP讀取請求(RRQ)、寫入請求(WRQ)和錯誤通知(ERROR)。

如果需要，在接收有效RRQ或WRQ時分配動態輔助通道和PAT轉換。TFTP隨後會使用此輔助通道進行檔案傳輸或錯誤通知。

只有TFTP伺服器可以通過輔助通道發起流量，而且TFTP客戶端和伺服器之間最多只能存在一個不完整的輔助通道。來自伺服器的錯誤通知將關閉輔助通道。

如果使用fstatic PAT重新導向TFTP流量，則必須啟用TFTP檢查。

配置基本TFTP應用檢測

預設情況下，配置包含與所有預設應用檢測流量匹配並將檢測應用於所有介面上的流量的策略（全域性策略）。預設應用檢測流量包括到每個協定的預設埠的流量。

只能應用一個全域性策略。因此，如果要更改全域性策略，例如將檢測應用於非標準埠，或新增預設情況下未啟用的檢測，則需要編輯或禁用預設策略並應用新的策略。有關所有預設埠的清單，請參閱預設檢測策略。

1. 運行policy-map global_policy命令。

   <#root>

   ```
   ASA(config)#
   policy-map global_policy
   ```

2. 運行class inspection_default 命令。

   <#root>

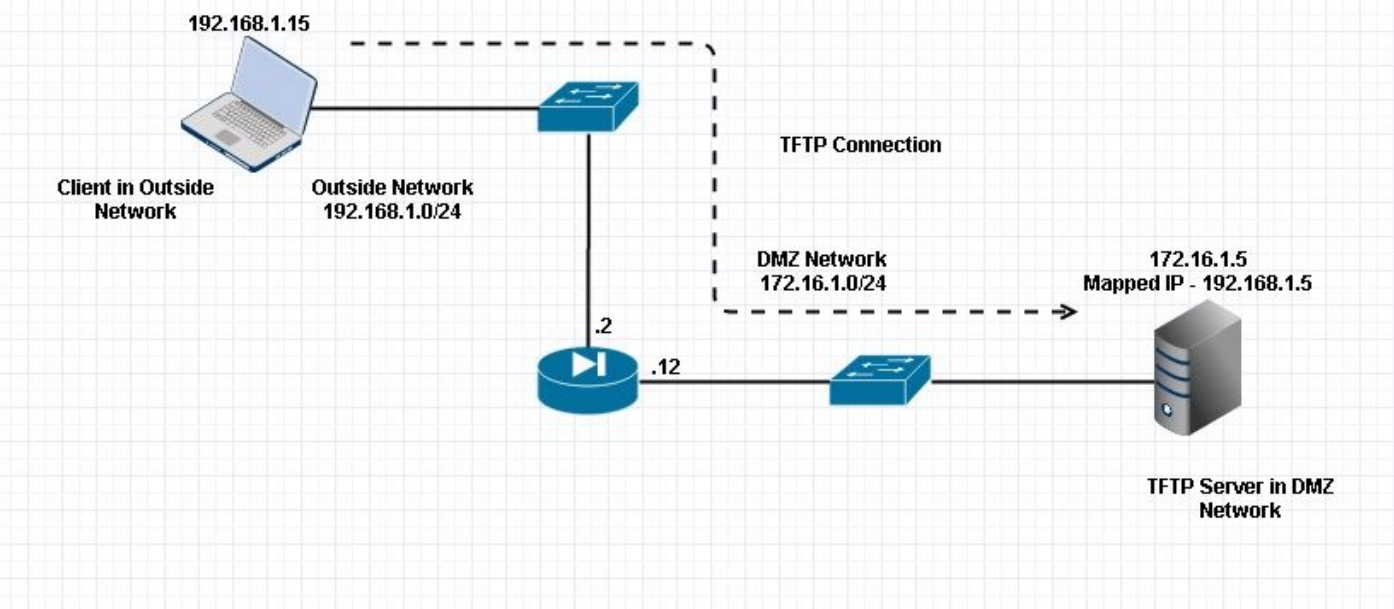
   ```
   ASA(config-pmap)#
   ```

```
class inspection_default
```

3. 執行inspect TFTP命令。

```
<#root>
 ASA(config-pmap-c)#
inspect TFTP
```

網路圖表



這裡是在外部網路中配置的客戶端。TFTP伺服器位於DMZ網路中。伺服器對映到位於外部子網中的IP 192.168.1.5。

組態範例:

```
<#root>
 ASA(config)#
show running-config

 ASA Version 9.1(5)
!
hostname ASA
domain-name corp. com
enable password WwXYvtKrnjXqGbu1 encrypted
```

```
names
!
interface GigabitEthernet0/0
 nameif Outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet0/1
 nameif DMZ
 security-level 50
 ip address 172.16.1.12 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 shutdown
 no nameif
 no security-level
 no ip address

 !--- Output is suppressed.


 !--- Permit inbound TFTP traffic.


access-list 100 extended permit udp any host 192.168.1.5 eq tftp

!

 !--- Object groups are created to define the hosts.


object network obj-172.16.1.5
 host 172.16.1.5


 !--- Object NAT     to map TFTP server to IP in Outside Subnet.


object network obj-172.16.1.5
 nat (DMZ,Outside) static 192.168.1.5



access-group 100 in interface outside


class-map inspection_default

match default-inspection-traffic

!
```

```
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum 512

policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc


inspect tftp


 inspect sip
 inspect xdmcp
!

!--- This command tells the device to
!--- use the "global_policy" policy-map on all interfaces.

service-policy global_policy global
prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
: end
ASA(config)#
```

驗證

要確保配置已成功執行，請運行show service-policy命令。此外，請僅通過運行show service-policy inspect tftp 命令來將輸出限製為TFTP檢查。

```
<#root>

 ASA#

show service-policy inspect tftp

          Global Policy:
           Service-policy: global_policy
            Class-map: inspection_default
              Inspect: tftp, packet 0, drop 0, reste-drop 0
         ASA#
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

Packet Tracer

內部網路中的客戶端

<#root>

FTP client Inside - Packet Tracer for Control Connection : Same Flow for Active and Passive.

 # packet-tracer input inside tcp 172.16.1.5 12345 192.168.1.15 21 det

-----Omitted------

Phase: 5
Type: INSPECT

Subtype: inspect-ftp

Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
 inspect ftp
service-policy global_policy global
Additional Information:
 Forward Flow based lookup yields rule:
 in id=0x76d9a120, priority=70, domain=inspect-ftp, deny=false
 hits=2, user_data=0x76d99a30, cs_id=0x0, use_real_addr, flags=0x0, protocol=6
 src ip/id=0.0.0.0, mask=0.0.0.0, port=0
 dst ip/id=0.0.0.0, mask=0.0.0.0, port=21, dscp=0x0
 input_ifc=inside, output_ifc=any

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:

object network obj-172.16.1.5

nat (inside,outside) static 192.168.1.5

Additional Information:
NAT divert to egress interface DMZ
translate 172.16.1.5/21 to 192.168.1.5/21

Phase: 7
Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

object network obj-172.16.1.5

nat (inside,outside) static 192.168.1.5

Additional Information:
Forward Flow based lookup yields rule:
out id=0x76d6e308, priority=6, domain=nat-reverse, deny=false
hits=15, user_data=0x76d9ef70, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0
dst ip/id=172.16.1.5, mask=255.255.255.255, port=0, dscp=0x0
input_ifc=inside, output_ifc=outside

----Omitted----

Result:
input-interface:

inside

input-status: up
input-line-status: up
output-interface:

Outside

output-status: up
output-line-status: up
Action: allow

外部網路中的客戶端

<#root>

FTP client Outside - Packet Tracer for Control Connection : Same Flow for Active and Passive

 # packet-tracer input outside tcp 192.168.1.15 12345 192.168.1.5 21 det

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW

Config:

object network obj-172.16.1.5

nat (DMZ,outside) static 192.168.1.5

Additional Information:
NAT divert to egress interface DMZ
Untranslate 192.168.1.5/21 to 172.16.1.5/21

-----Omitted-----

Phase: 4
Type: INSPECT
Subtype:

inspect-ftp

Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
 inspect ftp
service-policy global_policy global
Additional Information:
 Forward Flow based lookup yields rule:
 in id=0x76d84700, priority=70, domain=inspect-ftp, deny=false
 hits=17, user_data=0x76d84550, cs_id=0x0, use_real_addr, flags=0x0, protocol=6
 src ip/id=0.0.0.0, mask=0.0.0.0, port=0
 dst ip/id=0.0.0.0, mask=0.0.0.0, port=21, dscp=0x0
 input_ifc=outside, output_ifc=any

Phase: 5
Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

object network obj-172.16.1.5

```
  nat (DMZ,outside) static 192.168.1.5


 Additional Information:
  Forward Flow based lookup yields rule:
  out id=0x76d6e308, priority=6, domain=nat-reverse, deny=false
  hits=17, user_data=0x76d9ef70, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0
  dst ip/id=172.16.1.5, mask=255.255.255.255, port=0, dscp=0x0
  input_ifc=outside, output_ifc=DMZ

  ----Omitted-----

 Result:
 input-interface:
```

Outside

```
 input-status: up
 input-line-status: up
 output-interface:
```

DMZ

```
 output-status: up
 output-line-status: up
 Action: allow
```

如資料包跟蹤器所示，流量會到達各自的NAT語句和FTP檢查策略。它們還會保留其所需的介面。

在故障排除期間，您可以嘗試捕獲ASA入口和出口介面，並檢視ASA嵌入式IP地址重寫是否工作正常，並檢查是否允許在ASA上使用動態埠。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。