Configurazione servizi FTP/TFTP: ASA 9.X

Sommario

Introduzione

Questo documento descrive diversi scenari di ispezione FTP e TFTP sull'appliance ASA, configurazione dell'ispezione FTP/TFTP ASA e risoluzione dei problemi di base.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Comunicazione di base tra le interfacce richieste
- Configurazione del server FTP nella rete DMZ

Componenti usati

Questo documento descrive i diversi scenari di ispezione FTP e TFTP sull'appliance ASA (Adaptive Security Appliance) e descrive la configurazione dell'ispezione FTP/TFTP e la risoluzione dei problemi di base dell'appliance ASA.

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA serie 5500 o ASA serie 5500-X ASA con immagine software 9.1(5)
- Qualsiasi server FTP
- Qualsiasi client FTP

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

Appliance di sicurezza supporta l'ispezione delle applicazioni mediante la funzione Adaptive Security Algorithm.

Mediante l'ispezione delle applicazioni con conservazione dello stato utilizzata dall'algoritmo Adaptive Security, Appliance di sicurezza tiene traccia di tutte le connessioni che attraversano il firewall e ne verifica la validità.

Tramite l'ispezione con conservazione dello stato, il firewall controlla inoltre lo stato della connessione per compilare le informazioni da inserire in una tabella di stato.

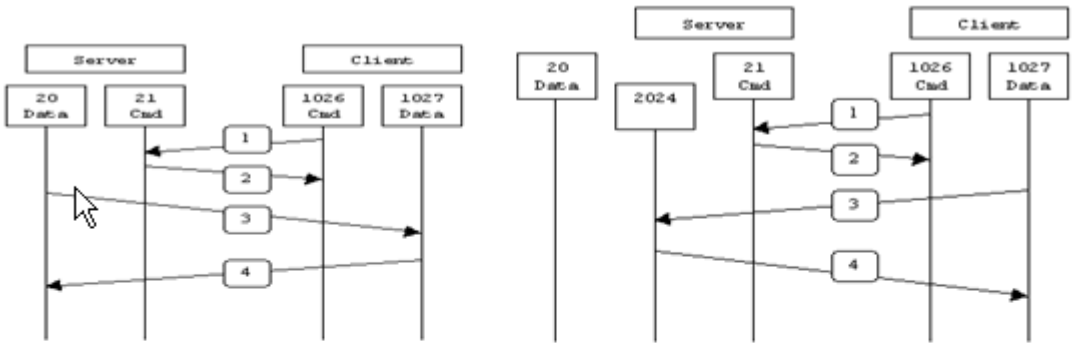
Se si utilizza la tabella di stato oltre alle regole definite dall'amministratore, le decisioni di filtraggio si basano sul contesto stabilito dai pacchetti passati precedentemente attraverso il firewall.

L'esecuzione delle ispezioni delle applicazioni comprende le seguenti azioni:

- Identifica il traffico
- Eseguire ispezioni sul traffico
- Attiva ispezioni su un'interfaccia

Sono disponibili due tipi di FTP, come mostrato nell'immagine.

- Modalità attiva
- Modalità passiva



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

FTP attivo

In modalità FTP attivo, il client si connette da una porta casuale senza privilegi (N>1023) alla porta di comando (21) del server FTP. Il client inizia quindi ad ascoltare la porta N>1023 e invia la porta di comando FTP N>1023 al server FTP. Il server si connette quindi alle porte dati specificate del client dalla porta dati locale, ovvero la porta 20.

FTP passivo

In modalità FTP passivo, il client avvia entrambe le connessioni al server, risolvendo il problema di un firewall che filtra la connessione della porta dati in ingresso dal server al client. Quando si apre una connessione FTP, il client apre due porte casuali senza privilegi in locale. La prima porta contatta il server sulla porta 21. Tuttavia, invece di eseguire un comando **port** e consentire al server di riconnettersi alla propria porta dati, il client esegue il comando **PASV**. Di conseguenza, il server apre una porta casuale senza privilegi (P>1023) e invia il comando **port P** al client. Il client avvia quindi la connessione dalla porta N>1023 alla porta P sul server per trasferire i dati. Se non si configura il comando **survey** sull'appliance di sicurezza, l'FTP inviato dagli utenti verso l'esterno funziona solo in modalità passiva. Inoltre, agli utenti esterni al server FTP viene negato l'accesso.

TFTP

Il protocollo TFTP, come descritto nella RFC 1350, è un protocollo semplice per leggere e scrivere file tra un server TFTP e un client. Il TFTP utilizza la porta UDP 69.

Gestione avanzata del protocollo

Perché è necessaria l'ispezione FTP?

alcune applicazioni richiedono una gestione speciale da parte della funzione di ispezione delle applicazioni di Cisco Security Appliance. Questi tipi di applicazioni in genere incorporano le informazioni sugli indirizzi IP nel pacchetto dati utente o nei canali secondari aperti su porte assegnate dinamicamente. La funzione di ispezione delle applicazioni opera in combinazione con Network Address Translation (NAT) per identificare

la posizione delle informazioni sull'indirizzamento incorporate.

Oltre all'identificazione delle informazioni di indirizzamento incorporate, la funzione di ispezione delle applicazioni controlla le sessioni per determinare i numeri di porta per i canali secondari. Molti protocolli aprono porte TCP o UDP secondarie per migliorare le prestazioni. La sessione iniziale su una porta nota viene utilizzata per negoziare i numeri di porta assegnati in modo dinamico.

La funzione di ispezione delle applicazioni controlla queste sessioni, identifica le assegnazioni dinamiche delle porte e consente lo scambio di dati su queste porte per la durata delle sessioni specifiche. Le applicazioni multimediali e FTP mostrano questo tipo di comportamento.

Se l'ispezione FTP non è stata attivata sull'appliance di sicurezza, la richiesta viene ignorata e le sessioni FTP non trasmettono i dati richiesti.

Se l'ispezione FTP è abilitata sull'appliance ASA, l'appliance controlla il canale di controllo e cerca di riconoscere una richiesta di apertura del canale dati. Il protocollo FTP incorpora le specifiche delle porte del canale dati nel traffico del canale di controllo, richiedendo all'appliance di sicurezza di ispezionare il canale di controllo per verificare se sono state apportate modifiche alle porte dati.

Quando l'ASA riconosce una richiesta, crea temporaneamente un'apertura per il traffico del canale dati che dura per la durata della sessione. In questo modo, la funzione di ispezione FTP monitora il canale di controllo, identifica l'assegnazione di una porta dati e consente lo scambio dei dati sulla porta dati per la durata della sessione.

Per impostazione predefinita, l'ASA controlla le connessioni alla porta 21 per il traffico FTP tramite la mappa delle classi dell'ispezione globale. Security Appliance riconosce inoltre la differenza tra una sessione FTP attiva e una sessione FTP passiva.

Se le sessioni FTP supportano il trasferimento di dati FTP passivo, l'ASA, tramite il comando **inspect ftp**, riconosce la richiesta della porta dati proveniente dall'utente e apre una nuova porta dati maggiore di 1023.

Il comando **inspect ftp** controlla le sessioni FTP ed esegue quattro attività:

- Prepara una connessione dati secondaria dinamica
- Tiene traccia della sequenza di risposta dei comandi FTP
- Genera un audit trail
- Traduce l'indirizzo IP incorporato utilizzando NAT

L'ispezione dell'applicazione FTP prepara i canali secondari per il trasferimento dei dati FTP. I canali vengono allocati in risposta a un evento di caricamento di file, di download di file o di elencazione di directory e devono essere pre-negoziati. La porta viene negoziata tramite i comandi **PORT** o **PASV** (227).

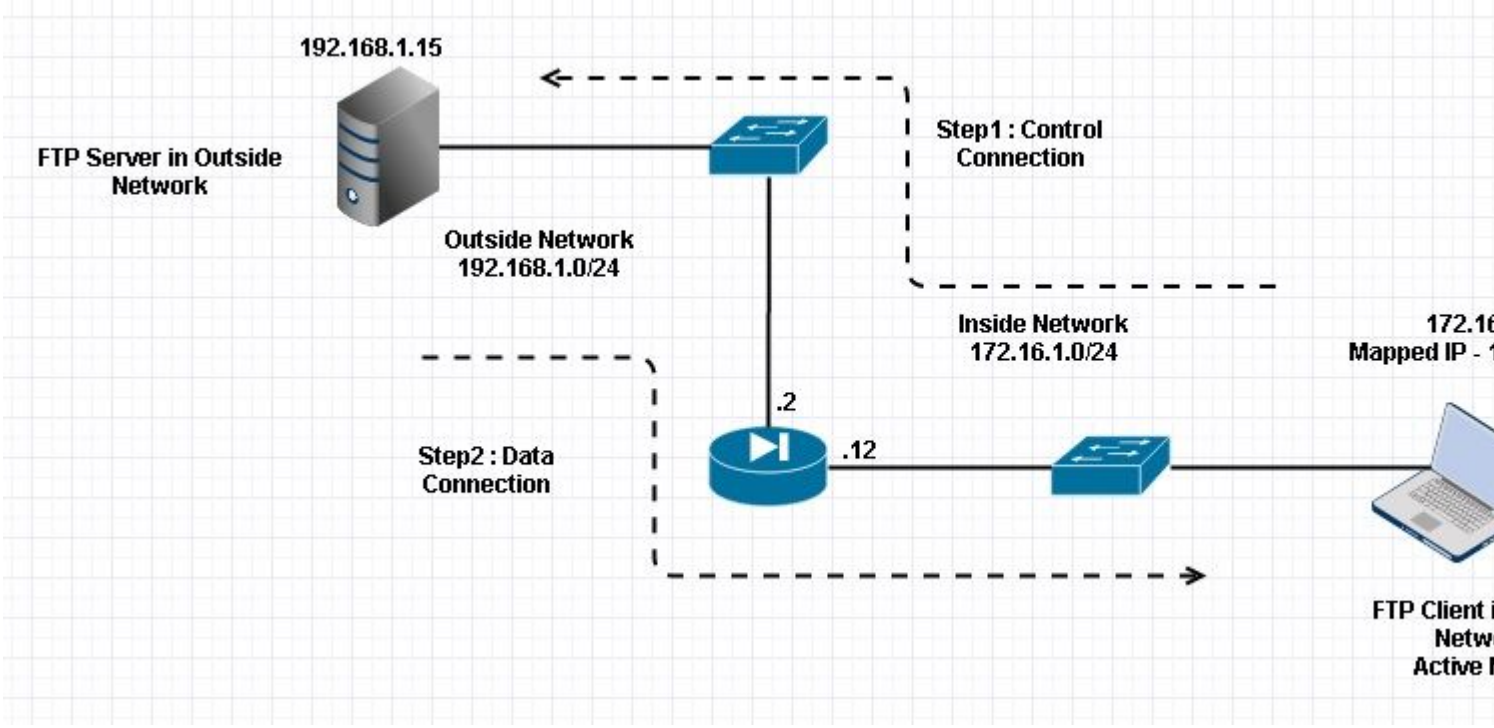
Configurazione

Nota: tutti gli scenari della rete vengono spiegati con l'ispezione FTP abilitata sull'appliance ASA.

Scenario 1. Client FTP configurato per la modalità attiva

Il client si è connesso alla rete interna dell'appliance ASA e il server alla rete esterna.

Esempio di rete



> **Nota**: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono indirizzabili legalmente su Internet.

Come mostrato in questa immagine, la configurazione di rete usata ha l'ASA con il client nella rete interna con IP 172.16.1.5. Il server si trova nella rete esterna con IP 192.168.1.15. Il client ha mappato l'IP 192.168.1.5 nella rete esterna.

Non è necessario autorizzare alcun elenco degli accessi sull'interfaccia esterna perché l'ispezione FTP apre Dynamic Port Channel.

Esempio di configurazione:

<#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)#
```

Verifica

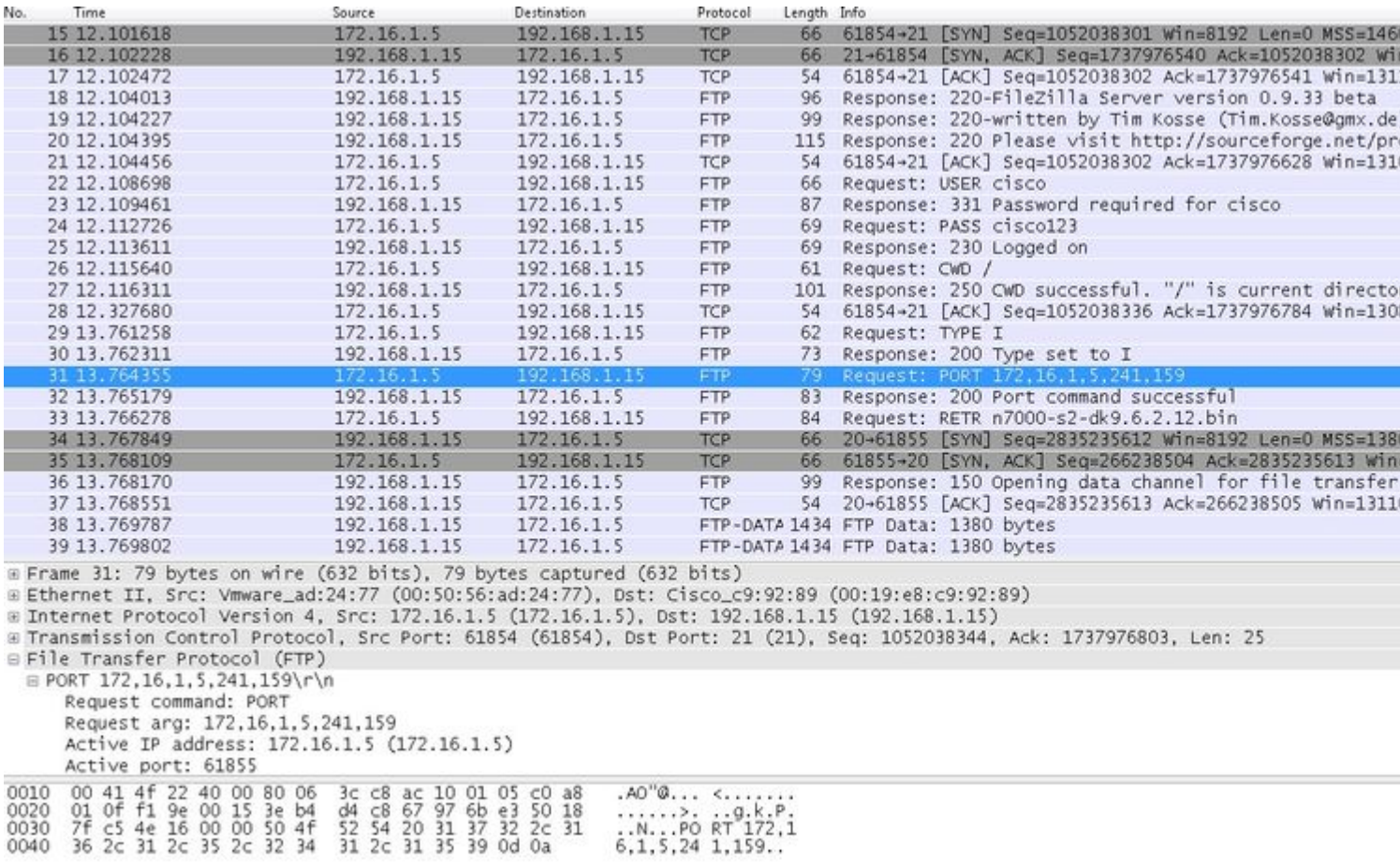
Connessione

<#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
```

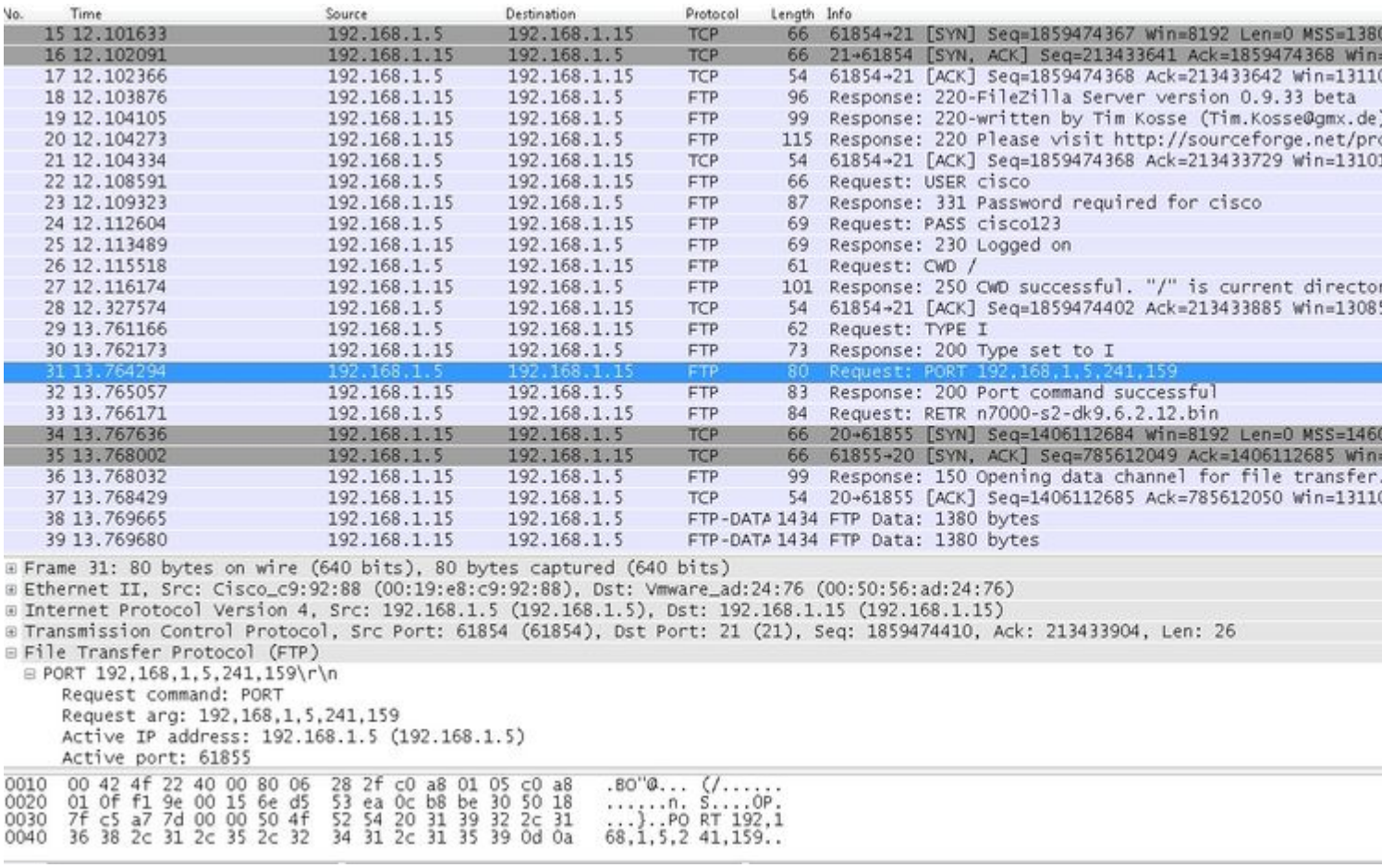
Qui il client in Inside avvia la connessione con la porta di origine 61854 alla porta di destinazione 21. Il client invia quindi il comando **Port** con il valore di 6 tuple. Il server a sua volta avvia la connessione dati/secondaria con la porta di origine 20 e la porta di destinazione viene calcolata in base ai passaggi indicati dopo queste acquisizioni.

Acquisisci interfaccia interna come mostrato nell'immagine.



```
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=146
  16 12.102228     192.168.1.15    172.16.1.5      TCP         66   21→61854 [SYN, ACK] Seq=1737976540 Ack=1052038302 Wi
  17 12.102472     172.16.1.5      192.168.1.15    TCP         54   61854→21 [ACK] Seq=1052038302 Ack=1737976541 Win=131
  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/pr
  21 12.104456     172.16.1.5      192.168.1.15    TCP         54   61854→21 [ACK] Seq=1052038302 Ack=1737976628 Win=131
  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 directo
  28 12.327680     172.16.1.5      192.168.1.15    TCP         54   61854→21 [ACK] Seq=1052038336 Ack=1737976784 Win=130
  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=138
  35 13.768109     172.16.1.5      192.168.1.15    TCP         66   61855→20 [SYN, ACK] Seq=266238504 Ack=2835235613 Win
  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=1311
  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..
```

Acquisire l'interfaccia esterna come mostrato nell'immagine.



```
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=138
  16 12.102091     192.168.1.15    192.168.1.5     TCP         66   21→61854 [SYN, ACK] Seq=213433641 Ack=1859474368 Win
  17 12.102366     192.168.1.5     192.168.1.15    TCP         54   61854→21 [ACK] Seq=1859474368 Ack=213433642 Win=1311
  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/pr
  21 12.104334     192.168.1.5     192.168.1.15    TCP         54   61854→21 [ACK] Seq=1859474368 Ack=213433729 Win=1310
  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 directo
  28 12.327574     192.168.1.5     192.168.1.15    TCP         54   61854→21 [ACK] Seq=1859474402 Ack=213433885 Win=1308
  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=146
  35 13.768002     192.168.1.5     192.168.1.15    TCP         66   61855→20 [SYN, ACK] Seq=785612049 Ack=1406112685 Win
  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=1311
  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..
```

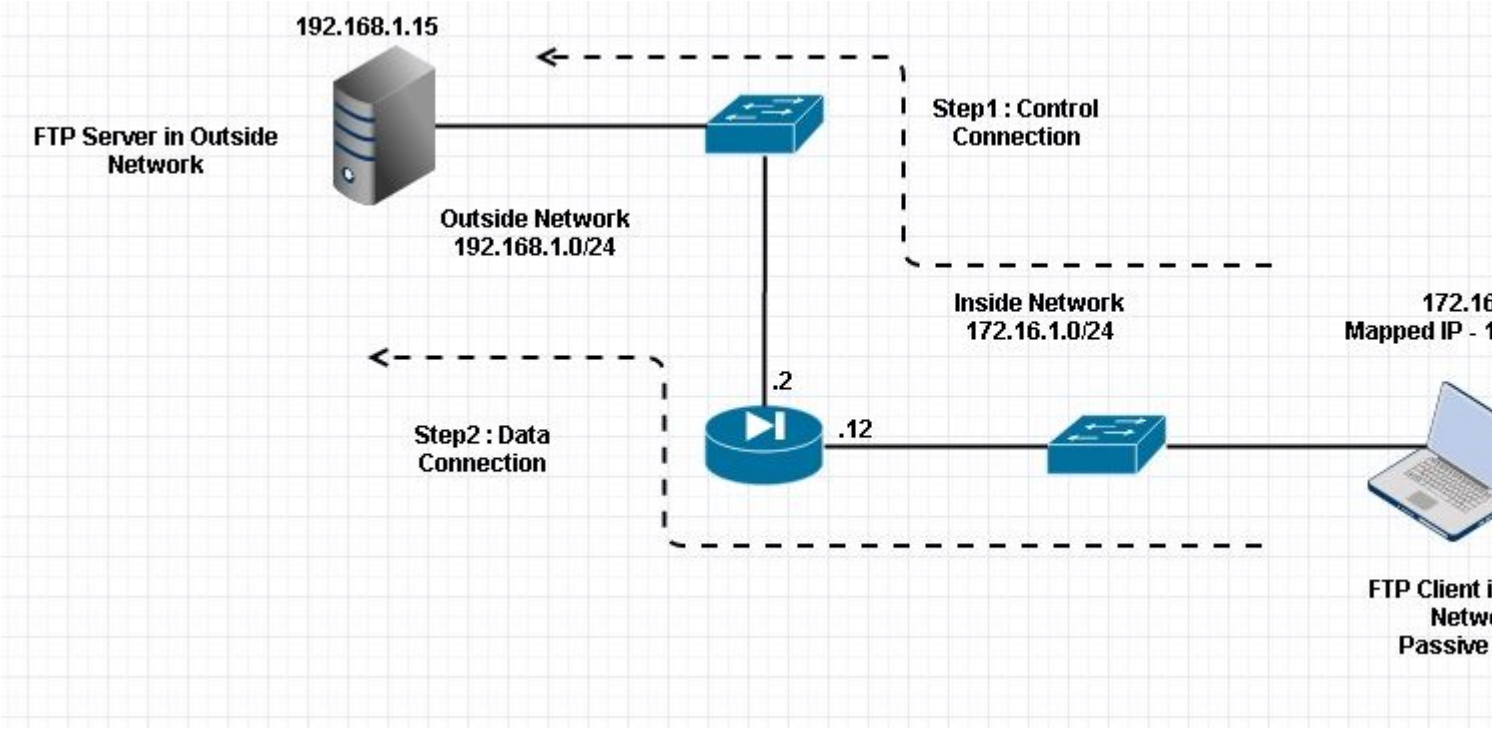
Il valore della porta viene calcolato utilizzando gli ultimi due tocchi su sei. Le quattro tuple a sinistra sono l'indirizzo IP e le due tuple sono per Port. Come mostrato in questa immagine, l'indirizzo IP è 192.168.1.5 e 241*256 + 159 = 61855.

L'opzione Cattura (Capture) indica inoltre che i valori di Comandi porta (Port Commands) vengono modificati quando l'ispezione FTP è abilitata. Inside Interface Capture mostra il valore reale dell'IP e la porta inviata dal client al server per la connessione al client per il canale dati, mentre Outside Interface Capture mostra l'indirizzo mappato.

Scenario 2. Client FTP configurato per la modalità passiva

Client nella rete interna dell'appliance ASA e server nella rete esterna.

Esempio di rete



Connessione

<#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.

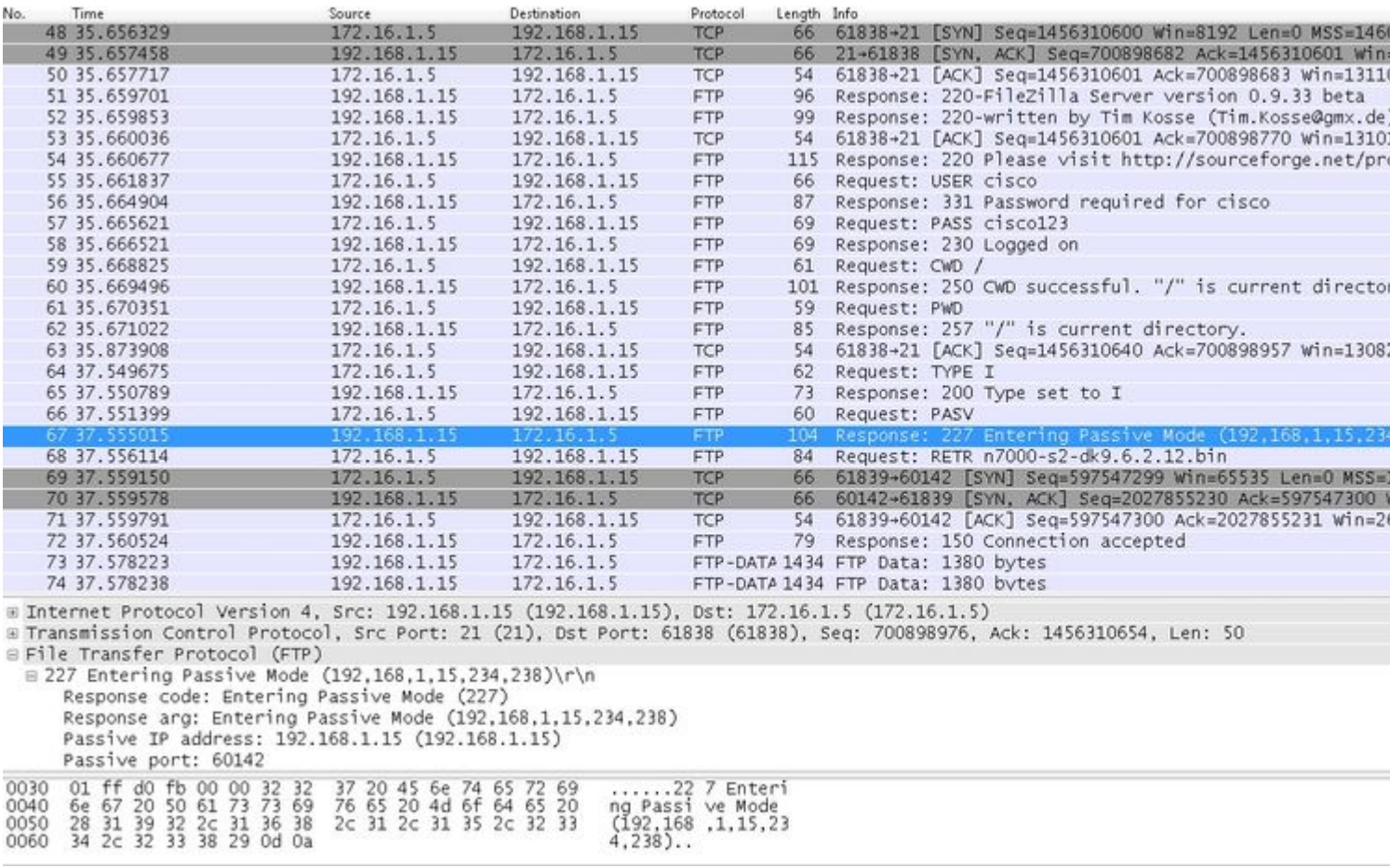
```
 TCP Outside
```

192.168.1.15:21 inside 172.16.1.5:61838

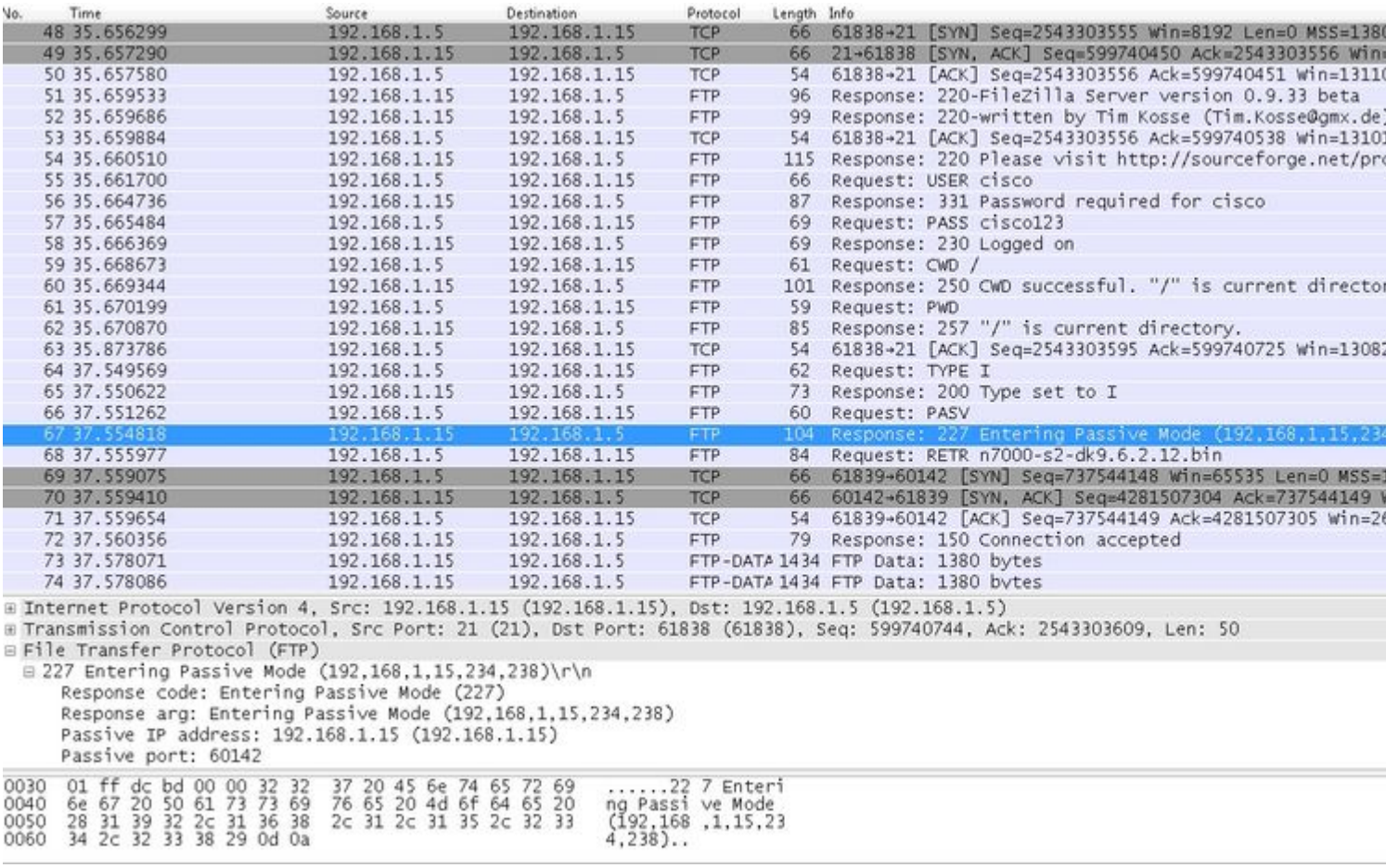
```
, idle 0:00:00, bytes 451, flags UIO
```

Il client all'interno di avvia una connessione con la porta di origine 61838 e la porta di destinazione 21. Trattandosi di un FTP passivo, il client avvia entrambe le connessioni. Pertanto, dopo l'invio del comando **PASV da parte del** client, il server risponde con il valore di 6 tuple e il client si connette a tale socket per la connessione dati.

Acquisisci interfaccia interna come mostrato nell'immagine.



Acquisire l'interfaccia esterna come mostrato nell'immagine.



Il calcolo per le porte rimane invariato.

Come accennato in precedenza, l'ASA riscrive i valori IP incorporati se l'ispezione FTP è abilitata. Inoltre, apre un canale di porta dinamico per la connessione dati.

Questi sono i dettagli di connessione se **Ispezione FTP disabilitata**

Connessione:

<#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
```

Senza ispezione FTP, tenta di inviare ripetutamente il comando **port**, ma non vi è alcuna risposta in quanto

all'esterno riceve il comando PORT with Original IP not NATTed. Lo stesso è stato visualizzato nel dump.

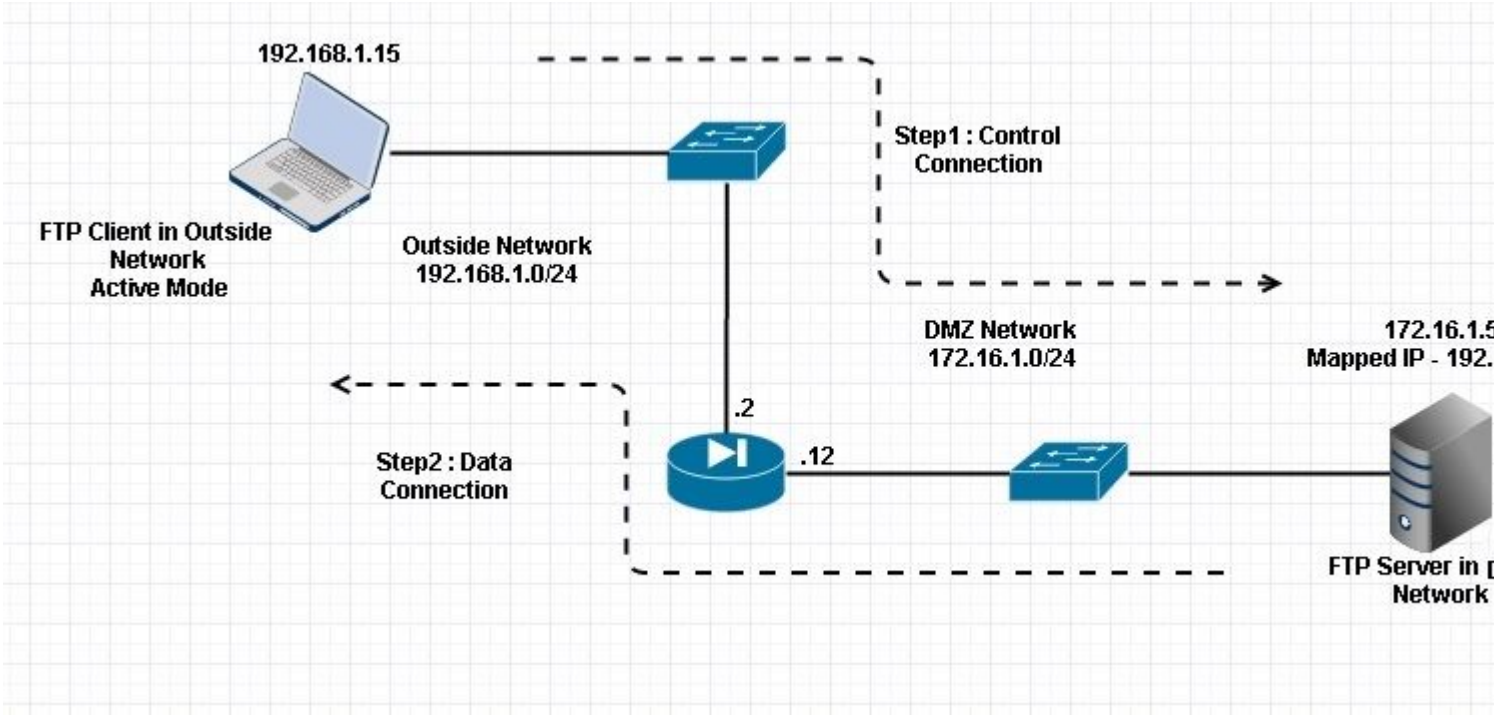
L'ispezione FTP può essere disabilitata senza il comando **ftp 21 del protocollo di correzione** in modalità terminale di configurazione.

Senza l'ispezione FTP, solo il comando **PASV** funziona quando il client si trova all'interno, in quanto non vi è alcun comando **port** proveniente dall'interno che deve essere integrato ed entrambe le connessioni sono avviate dall'interno.

Scenario 3. Client FTP configurato per la modalità attiva

Client nella rete esterna dell'ASA e server nella rete DMZ.

Esempio di rete



Configurazione:

<#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)#
```

Verifica

Connessione:

<#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,

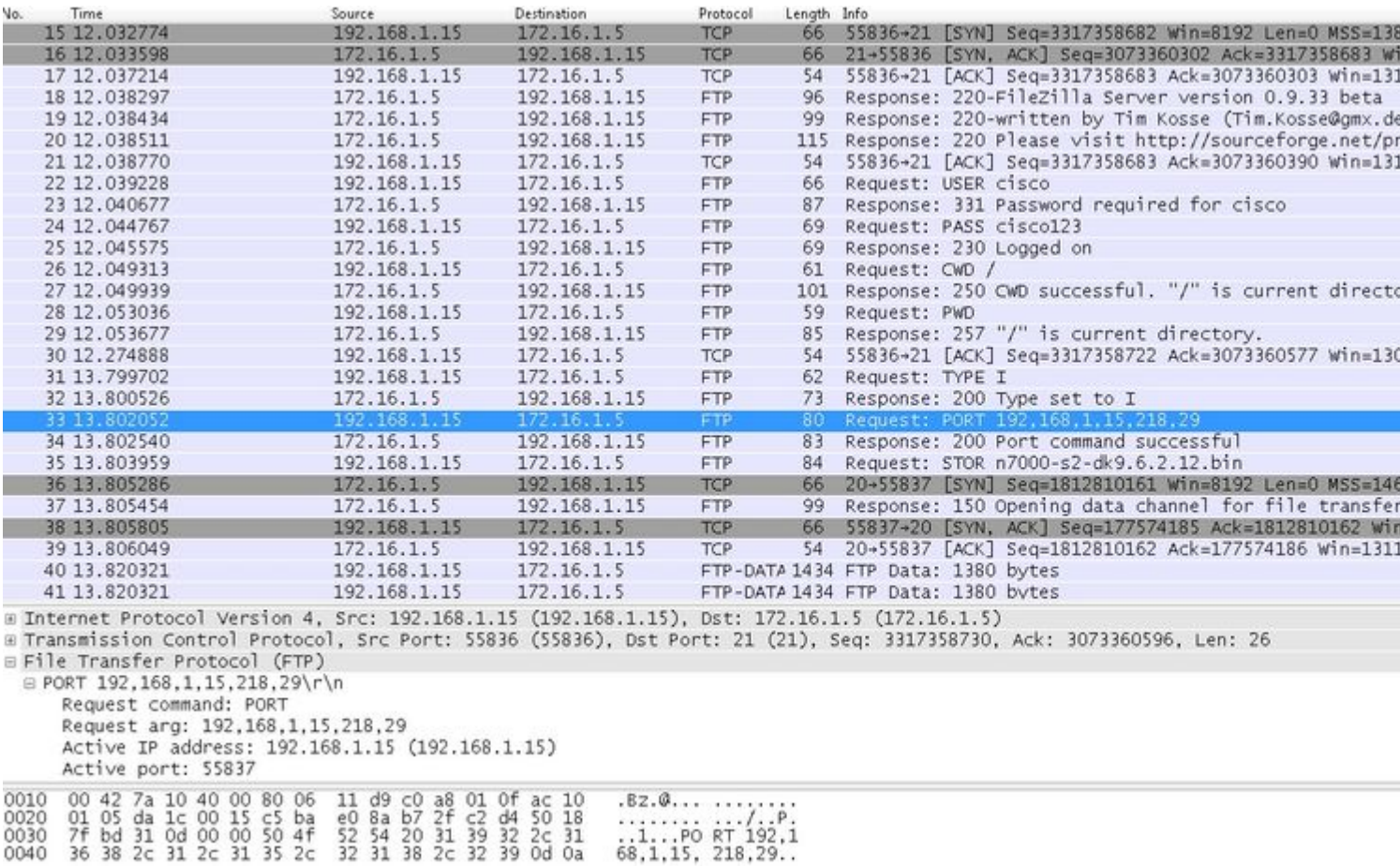
```
 idle 0:00:00, bytes 470, flags UIOB
```

TCP outside 192.168.1.15:55837 DMZ 172.16.1.5:20,

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

<--- Dynamic Port channel

Acquisire l'interfaccia DMZ come mostrato in questa immagine.

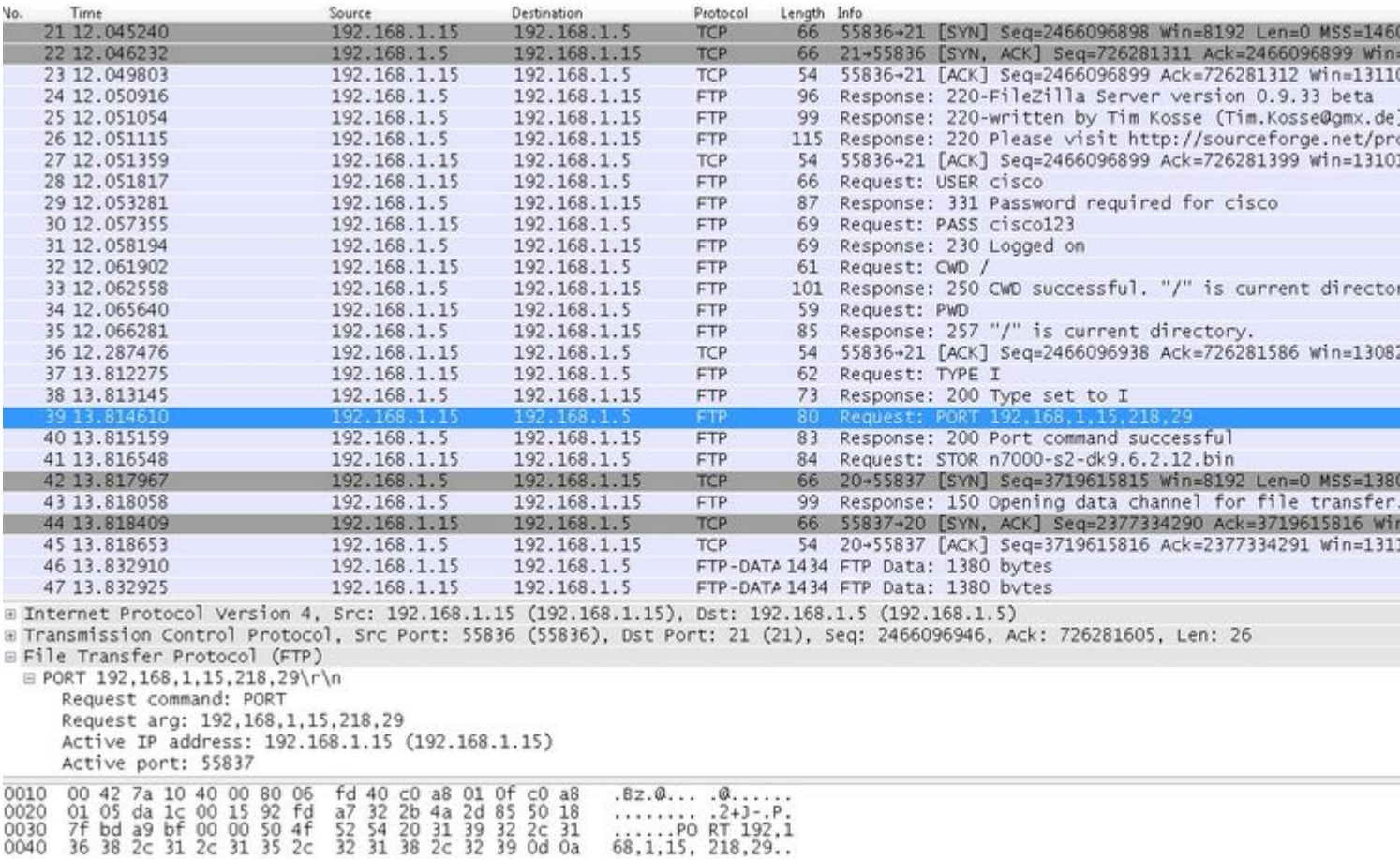


No.	Time	Source	Destination	Protocol	Length	Info
15	12.032774	192.168.1.15	172.16.1.5	TCP	66	55836→21 [SYN] Seq=3317358682 Win=8192 Len=0 MSS=138
16	12.033598	172.16.1.5	192.168.1.15	TCP	66	21→55836 [SYN, ACK] Seq=3073360302 Ack=3317358683 Wi
17	12.037214	192.168.1.15	172.16.1.5	TCP	54	55836→21 [ACK] Seq=3317358683 Ack=3073360303 Win=131
18	12.038297	172.16.1.5	192.168.1.15	FTP	96	Response: 220-FileZilla Server version 0.9.33 beta
19	12.038434	172.16.1.5	192.168.1.15	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de
20	12.038511	172.16.1.5	192.168.1.15	FTP	115	Response: 220 Please visit http://sourceforge.net/pr
21	12.038770	192.168.1.15	172.16.1.5	TCP	54	55836→21 [ACK] Seq=3317358683 Ack=3073360390 Win=131
22	12.039228	192.168.1.15	172.16.1.5	FTP	66	Request: USER cisco
23	12.040677	172.16.1.5	192.168.1.15	FTP	87	Response: 331 Password required for cisco
24	12.044767	192.168.1.15	172.16.1.5	FTP	69	Request: PASS cisco123
25	12.045575	172.16.1.5	192.168.1.15	FTP	69	Response: 230 Logged on
26	12.049313	192.168.1.15	172.16.1.5	FTP	61	Request: CWD /
27	12.049939	172.16.1.5	192.168.1.15	FTP	101	Response: 250 CWD successful. "/" is current directo
28	12.053036	192.168.1.15	172.16.1.5	FTP	59	Request: PWD
29	12.053677	172.16.1.5	192.168.1.15	FTP	85	Response: 257 "/" is current directory.
30	12.274888	192.168.1.15	172.16.1.5	TCP	54	55836→21 [ACK] Seq=3317358722 Ack=3073360577 Win=130
31	13.799702	192.168.1.15	172.16.1.5	FTP	62	Request: TYPE I
32	13.800526	172.16.1.5	192.168.1.15	FTP	73	Response: 200 Type set to I
33	13.802052	192.168.1.15	172.16.1.5	FTP	80	Request: PORT 192,168,1,15,218,29
34	13.802540	172.16.1.5	192.168.1.15	FTP	83	Response: 200 Port command successful
35	13.803959	192.168.1.15	172.16.1.5	FTP	84	Request: STOR n7000-s2-dk9.6.2.12.bin
36	13.805286	172.16.1.5	192.168.1.15	TCP	66	20→55837 [SYN] Seq=1812810161 Win=8192 Len=0 MSS=146
37	13.805454	172.16.1.5	192.168.1.15	FTP	99	Response: 150 Opening data channel for file transfer
38	13.805805	192.168.1.15	172.16.1.5	TCP	66	55837→20 [SYN, ACK] Seq=177574185 Ack=1812810162 Win
39	13.806049	172.16.1.5	192.168.1.15	TCP	54	20→55837 [ACK] Seq=1812810162 Ack=177574186 Win=1311
40	13.820321	192.168.1.15	172.16.1.5	FTP-DATA	1434	FTP Data: 1380 bytes
41	13.820321	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: 55836 (55836), Dst Port: 21 (21), Seq: 3317358730, Ack: 3073360596, 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  11 d9 c0 a8 01 0f ac 10   .Bz.@... ........
0020  01 05 da 1c 00 15 c5 ba  e0 8a b7 2f c2 d4 50 18   ........ .../..P.
0030  7f bd 31 0d 00 00 50 4f  52 54 20 31 39 32 2c 31   ..1...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..
```

Acquisire l'interfaccia esterna come mostrato nell'immagine.

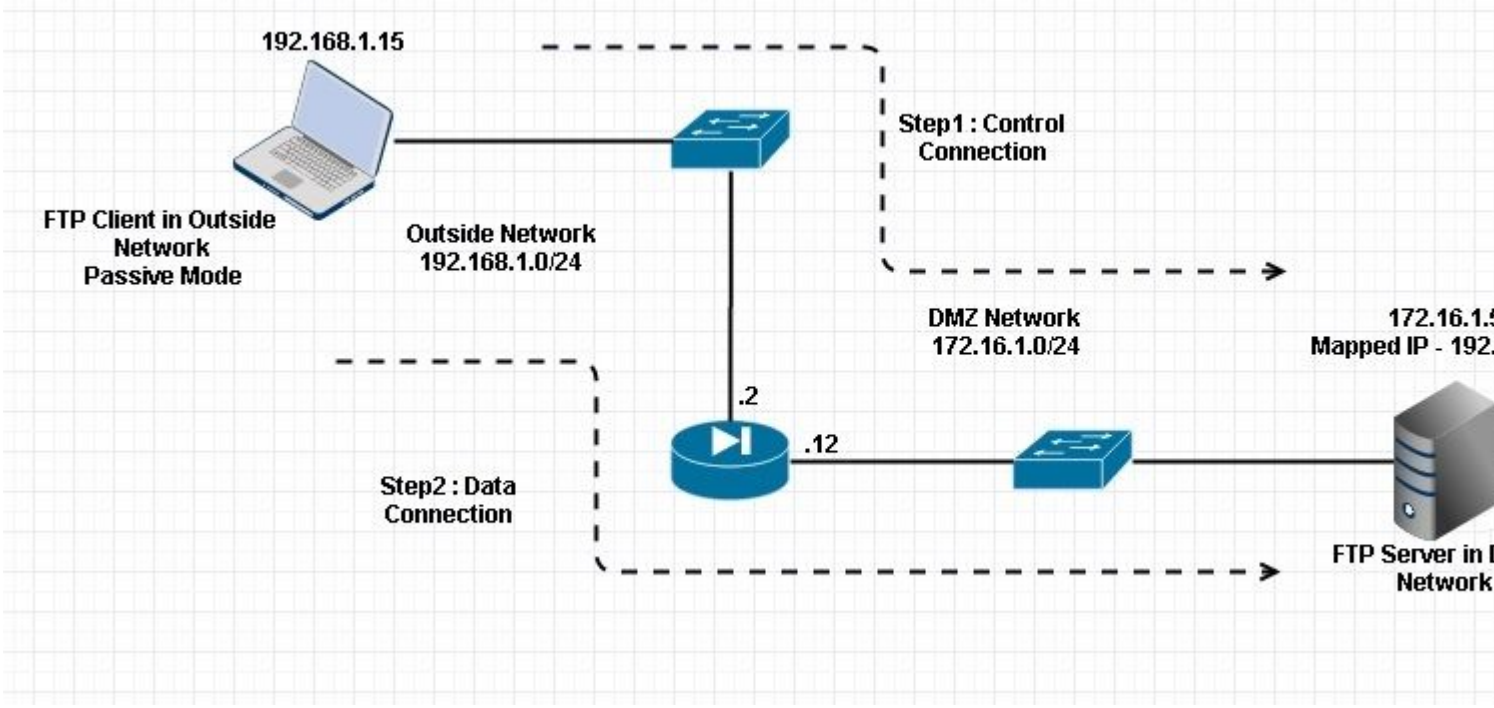


In questo caso, il client esegue il client in modalità attiva 192.168.1.15 e avvia la connessione al server nella DMZ sulla porta 21. Il client invia quindi il comando **port** con sei valori di tupla al server per connettersi a quella specifica porta dinamica. Il server avvia quindi la connessione dati con la porta di origine impostata su 20.

Scenario 4. Client FTP in modalità passiva

Client nella rete esterna dell'ASA e server nella rete DMZ.

Esempio di rete



Connessione

<#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
```

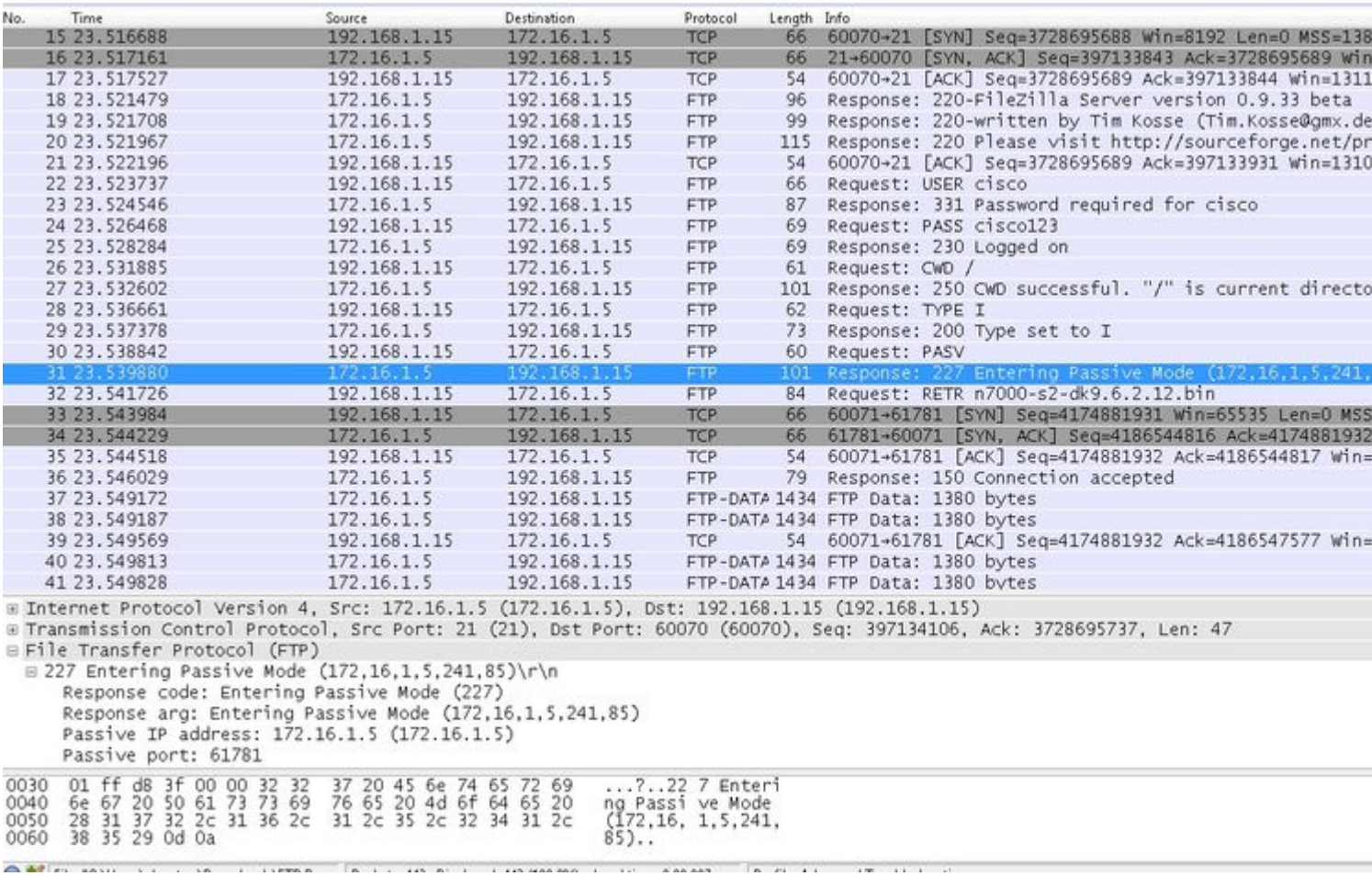
<--- Dynamic channel Open

```
TCP
```

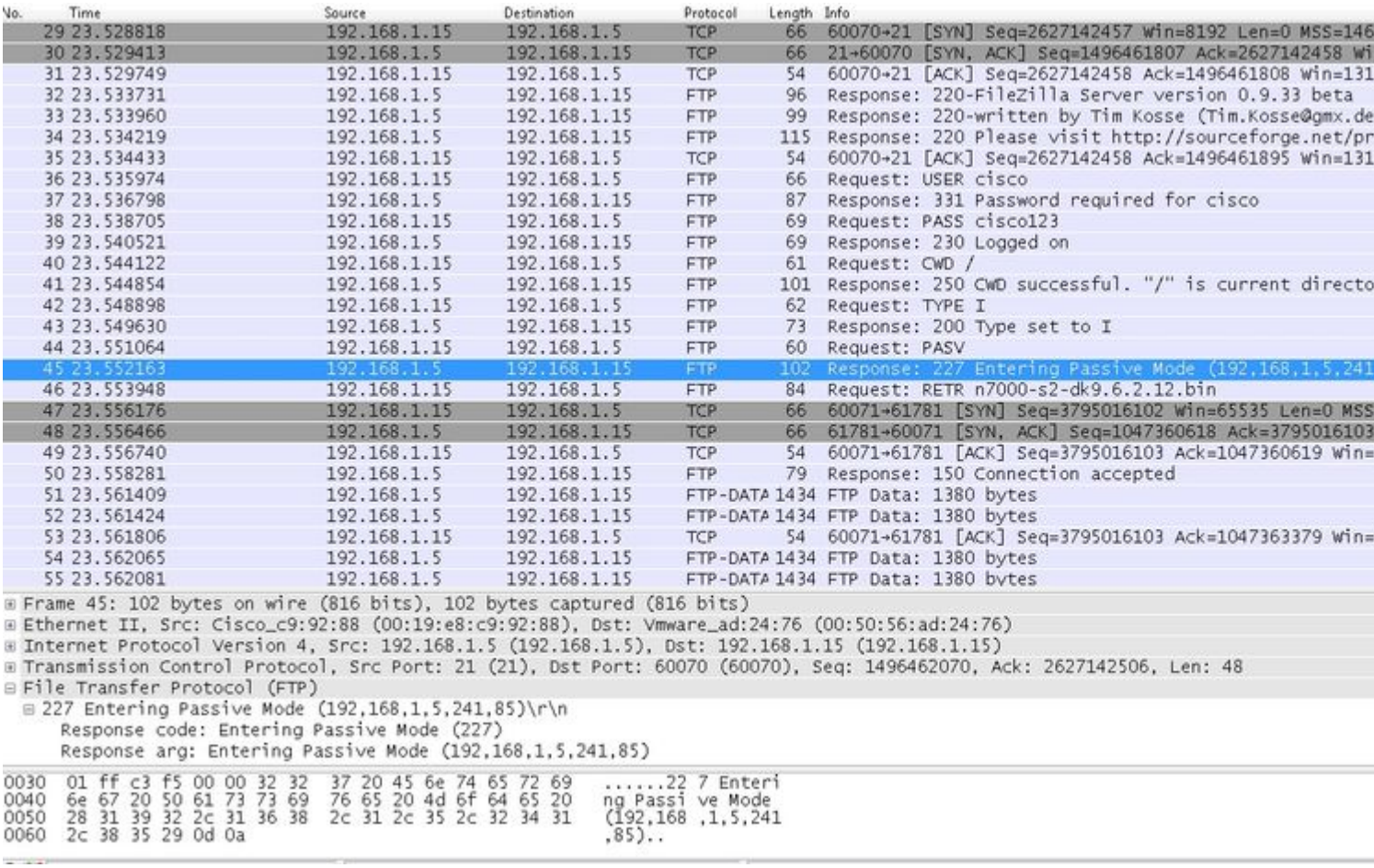
Outside 192.168.1.15:60070 DMZ 172.16.1.5:21

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

Acquisire l'interfaccia DMZ come mostrato in questa immagine.



Acquisire l'interfaccia esterna come mostrato nell'immagine.



Configura ispezione applicazione FTP di base

Per impostazione predefinita, la configurazione include un criterio che corrisponde a tutto il traffico di ispezione delle applicazioni predefinito e applica l'ispezione al traffico su tutte le interfacce (un criterio globale). Il traffico di ispezione delle applicazioni predefinito include il traffico verso le porte predefinite per ogni protocollo.

È possibile applicare un solo criterio globale, pertanto se si desidera modificare il criterio globale, ad esempio per applicare l'ispezione a porte non standard o per aggiungere ispezioni non abilitate per impostazione predefinita, è necessario modificare il criterio predefinito oppure disabilitarlo e applicarne uno nuovo. Per un elenco di tutte le porte predefinite, vedere Criteri di ispezione predefiniti.

1. Eseguire il comando **policy-map global_policy**.

```
<#root>

 ASA(config)#

policy-map global_policy
```

2. Eseguire il comando **class inspection_default**.

```
<#root>
```

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

3. Eseguire il comando **inspect FTP**.

<#root>

```
 ASA(config-pmap-c)#
inspect FTP
```

4. È possibile utilizzare il comando **inspect FTP strict**. Questo comando aumenta la sicurezza delle reti protette impedendo a un browser Web di inviare comandi incorporati nelle richieste FTP.

   Dopo aver abilitato l'opzione **strict** su un'interfaccia, l'ispezione FTP applica questo comportamento:

   - Prima che Appliance di sicurezza consenta un nuovo comando, è necessario confermare il comando FTP
   - Appliance di sicurezza interrompe una connessione che invia comandi incorporati
   - I comandi **227** e **PORT** vengono controllati per verificare che non vengano visualizzati in una stringa di errore

---

Avviso: l'uso dell'opzione **strict** può causare il malfunzionamento dei client FTP non strettamente conformi alle RFC FTP. Per ulteriori informazioni sull'uso dell'opzione **strict**, consultare Uso dell'opzione strict.

Configurazione dell'ispezione del protocollo FTP sulla porta TCP non standard

È possibile configurare l'ispezione del protocollo FTP per le porte TCP non standard con queste righe di configurazione (sostituire XXXX con il nuovo numero di porta):

<#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
```

Verifica

Per verificare che la configurazione sia stata eseguita correttamente, eseguire il comando **show service-policy**. Inoltre, limitare l'output all'ispezione FTP eseguendo il comando **show service-policy inspect ftp**.

```
<#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

L'ispezione TFTP è abilitata per impostazione predefinita.

L'appliance di sicurezza controlla il traffico TFTP e, se necessario, crea connessioni e conversioni dinamiche per consentire il trasferimento di file tra un client TFTP e un server. In particolare, il modulo di controllo controlla le richieste di lettura TFTP (RQ), le richieste di scrittura (WRQ) e le notifiche di errore (ERROR).

Un canale secondario dinamico e una traduzione PAT, se necessario, vengono allocati su una ricezione di una RRQ o WRQ valida. Questo canale secondario viene successivamente utilizzato dal TFTP per il trasferimento di file o la notifica degli errori.

Solo il server TFTP può avviare il traffico sul canale secondario e tra il client TFTP e il server può esistere al massimo un canale secondario incompleto. Una notifica di errore dal server chiude il canale secondario.

L'ispezione TFTP deve essere abilitata se si utilizza Fstatic PAT per reindirizzare il traffico TFTP.

Configura ispezione applicazione TFTP di base

Per impostazione predefinita, la configurazione include un criterio che corrisponde a tutto il traffico di ispezione delle applicazioni predefinito e applica l'ispezione al traffico su tutte le interfacce (un criterio globale). Il traffico di ispezione delle applicazioni predefinito include il traffico verso le porte predefinite per ogni protocollo.

È possibile applicare un solo criterio globale. Pertanto, se si desidera modificare il criterio globale, ad esempio per applicare l'ispezione a porte non standard o per aggiungere ispezioni non abilitate per impostazione predefinita, è necessario modificare il criterio predefinito oppure disabilitarlo e applicarne uno nuovo. Per un elenco di tutte le porte predefinite, vedere Criteri di ispezione predefiniti.

1. Eseguire il comando **policy-map global_policy**.

```
<#root>

 ASA(config)#
```

```
policy-map global_policy
```

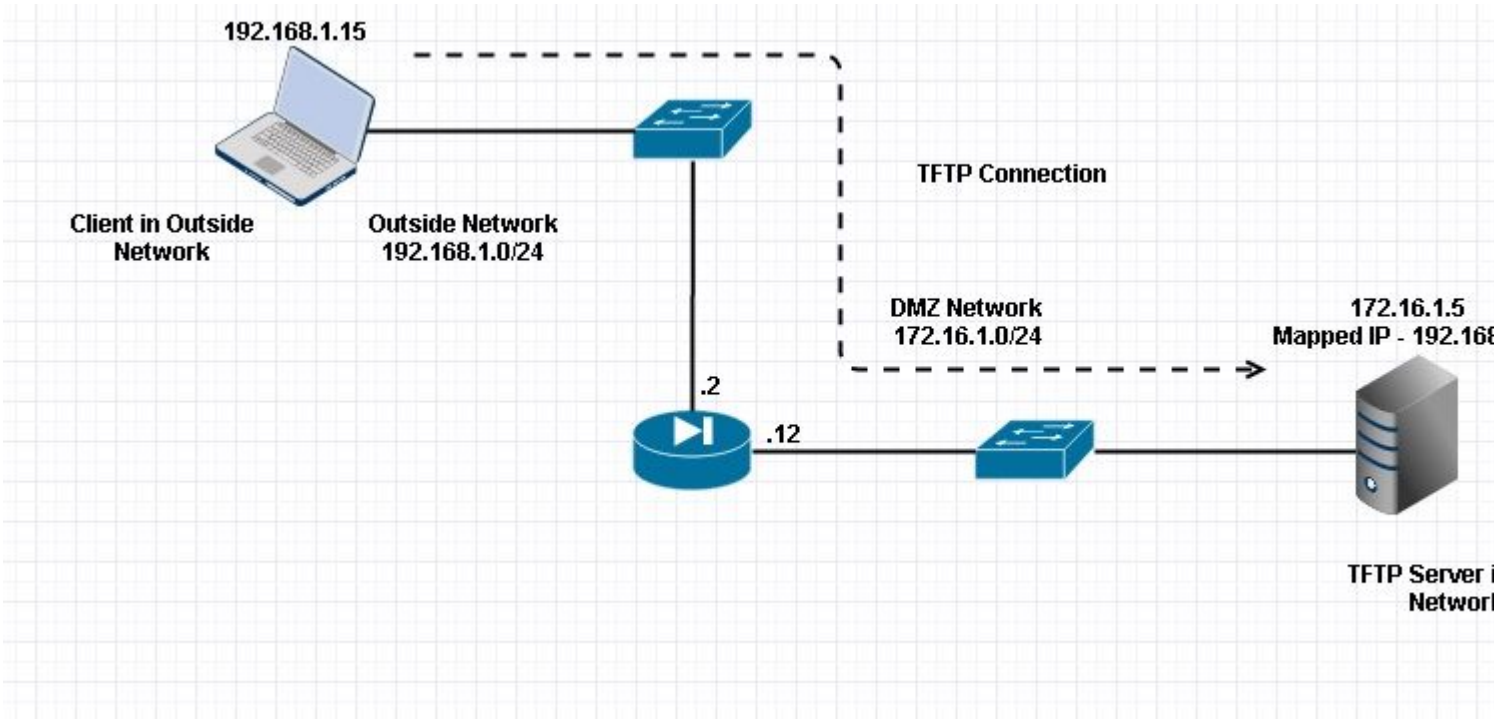
2. Eseguire il comando **class inspection_default**.

```
<#root>
 ASA(config-pmap)#
class inspection_default
```

3. Eseguire il comando **inspect TFTP**.

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

Esempio di rete



Qui il client è configurato nella rete esterna. Il server TFTP si trova nella rete DMZ. Il server è mappato all'IP 192.168.1.5 che si trova nella subnet esterna.

Esempio di configurazione:

<#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)#
```

Verifica

Per verificare che la configurazione sia stata eseguita correttamente, eseguire il comando **show service-policy**. Inoltre, limitare l'output all'ispezione TFTP solo eseguendo il comando **show service-policy inspect tftp**.

<#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#
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Packet Tracer

Client nella rete interna

<#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

Client nella rete esterna

<#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
```

Come si vede nei tracciatori dei pacchetti, il traffico raggiunge le rispettive dichiarazioni NAT e la politica di ispezione FTP. e lasciano le interfacce obbligatorie.

Durante la risoluzione dei problemi, è possibile provare a acquisire le interfacce ASA in entrata e in uscita e verificare se la riscrittura dell'indirizzo IP incorporato nell'appliance ASA funziona correttamente. Inoltre, è possibile controllare la connessione se la porta dinamica è consentita sull'appliance ASA.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).