Configure FTP/TFTP Services: ASA 9.X

Contents

Introduction

This document describes different FTP and TFTP inspection scenarios on the ASA, ASA FTP/TFTP inspection configuration, and basic troubleshooting.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Basic communication between required interfaces

- Configuration of the FTP server located in the DMZ network

Components Used

This document describes different FTP and TFTP inspection scenarios on the Adaptive Security Appliance (ASA) and it also covers ASA FTP/TFTP inspection configuration and basic troubleshooting.

The information in this document is based on these software and hardware versions:

- ASA 5500 or ASA 5500-X Series ASA that runs the 9.1(5) software image

- Any FTP Server

- Any FTP Client

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Security Appliance supports application inspection through the Adaptive Security Algorithm function.

Through the stateful application inspection used by the Adaptive Security Algorithm, the Security Appliance tracks each connection that traverses the firewall and ensures that they are valid.

The firewall, through stateful inspection, also monitors the state of the connection to compile information to place in a state table.

With the use of the state table in addition to administrator-defined rules, filtering decisions are based on context that is established by packets previously passed through the firewall.

The implementation of application inspections consists of these actions:

- Identify the traffic

- Apply inspections to the traffic

- Activate inspections on an interface

There are two forms of FTP as shown in the image.

- Active mode

- Passive mode
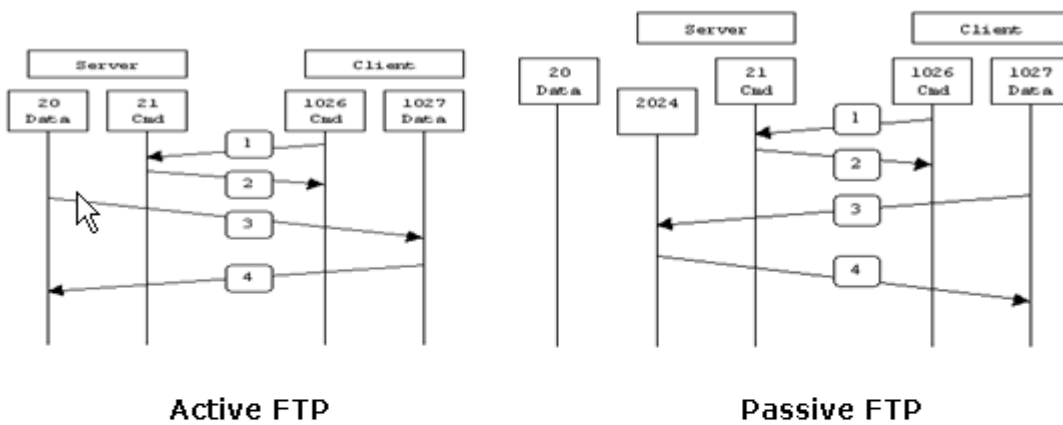
Active FTP

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

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

Active FTP

In Active FTP mode, the client connects from a random unprivileged port (N>1023) to the command port (21) of the FTP server. Then the client starts to listen to port N>1023 and sends the FTP command port N>1023 to the FTP server. The server then connects back to the specified data ports of the client from its local data port, which is port 20.

Passive FTP

In Passive FTP mode, the client initiates both connections to the server, which solves the problem of a firewall that filters the incoming data port connection to the client from the server. When an FTP connection is opened, the client opens two random unprivileged ports locally. The first port contacts the server on port 21. But instead of running a **port** command and allowing the server to connect back to its data port, the client issues the **PASV** command. The result of this is that the server then opens a random unprivileged port (P>1023) and sends the **port P** command back to the client. The client then initiates the connection from port N>1023 to port P on the server to transfer data. Without the **inspection** command configuration on the Security Appliance, FTP from inside users headed outbound works only in Passive mode. Also, users outside headed inbound to your FTP server are denied access.

TFTP

TFTP, as described in [RFC 1350](#), is a simple protocol to read and write files between a TFTP server and client. TFTP uses UDP port 69.

Advanced Protocol Handling

Why do you need FTP inspection?

Some applications require special handling by the Cisco Security Appliance application inspections function. These types of applications typically embed IP addressing information in the user data packet or open secondary channels on dynamically assigned ports. The application inspection function works with Network Address Translation (NAT) in order to help identify the location of embedded addressing

information.

In addition to the identification of embedded addressing information, the application inspection function monitors sessions in order to determine the port numbers for secondary channels. Many protocols open secondary TCP or UDP ports to improve performance. The initial session on a well-known port is used to negotiate dynamically assigned port numbers.

The application inspection function monitors these sessions, identifies the dynamic port assignments and permits data exchange on these ports for the duration of the specific sessions. Multimedia and FTP applications exhibit this kind of behavior.

If the FTP inspection has not been enabled on the Security Appliance, this request is discarded and the FTP sessions do not transmit any requested data.

If the FTP inspection is enabled on the ASA, then the ASA monitors the control channel and tries to recognize a request to open the data channel. The FTP protocol embeds the data-channel port specifications in the control channel traffic, requiring the Security Appliance to inspect the control channel for data-port changes.

Once the ASA recognizes a request, it temporarily creates an opening for the data-channel traffic that lasts for the life of the session. In this way, the FTP inspection function monitors the control channel, identifies a data-port assignment, and allows data to be exchanged on the data port for the length of the session.

ASA inspects port 21 connections for FTP traffic by default through the global-inspection class-map. The Security Appliance also recognizes the difference between an active and a passive FTP session.

If the FTP sessions support passive FTP data transfer, the ASA through the **inspect ftp** command, recognizes the data port request from the user and opens a new data port greater than 1023.

The **inspect ftp** command inspection inspects FTP sessions and performs four tasks:

- Prepares a dynamic secondary data connection
- Tracks the FTP command-response sequence
- Generates an audit trail
- Translates the embedded IP address using NAT

FTP application inspection prepares secondary channels for FTP data transfer. The channels are allocated in response to a file upload, a file download, or a directory listing event, and they must be pre-negotiated. The port is negotiated through the **PORT** or **PASV** (227) commands.
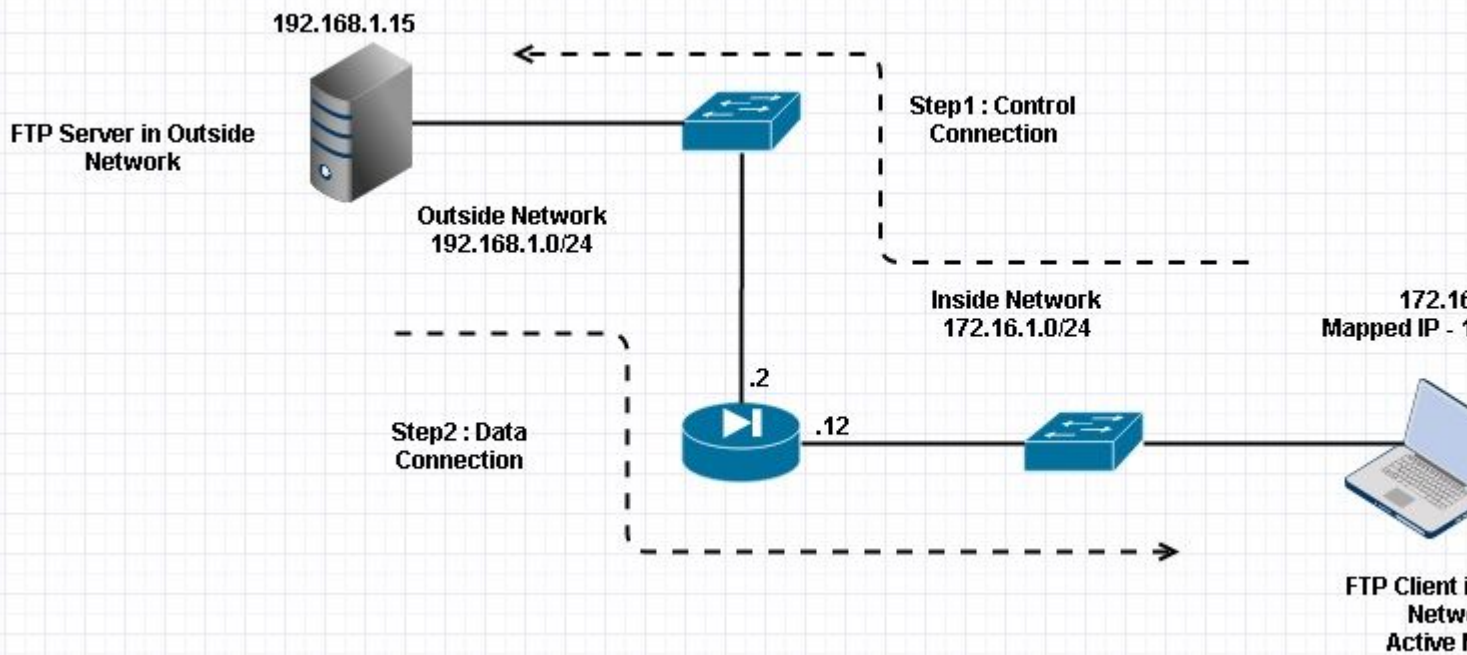
Configuration

> **Note**: All the network scenarios are explained with FTP inspection enabled on the ASA.

Scenario 1. FTP Client Configured for Active Mode

Client connected to Inside Network of the ASA and Server in Outside Network.

Network Diagram

Note: The IP addressing schemes used in this configuration are not legally routable on the Internet.

As shown in this image, the network setup used has the ASA with Client in the Inside Network with IP 172.16.1.5. Server is in Outside Network with IP 192.168.1.15. Client has a mapped IP 192.168.1.5 in the Outside Network .

There is no need to permit any Access-list on Outside Interface as FTP inspection opens Dynamic Port Channel.

Configuration Example:

```
<#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)#
```

Verify

Connection

<#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
```

Here the client in Inside initiates the connection with source port 61854 to the destination port 21. Client then sends **Port** command with 6 tuple value. Server in turn initiates the Secondary/Data connection with Source Port of 20 and Destination Port is calculated from the steps mentioned after these captures.

Capture Inside Interface as shown in this image.

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..
```

Capture Outside Interface as shown in this image.

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/pro
21	12.104334	192.168.1.5	192.168.1.15	TCP	54	61854→21 [ACK] Seq=1859474368 Ack=213433729 Win=13101
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 director
28	12.327574	192.168.1.5	192.168.1.15	TCP	54	61854→21 [ACK] Seq=1859474402 Ack=213433885 Win=13085
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..
```

Port Value is calculated using last two touple out of six. Left 4 tuple are IP address and 2 touple are for Port. As shown in this image, IP address is 192.168.1.5 and 241*256 + 159 = 61855.

Capture also shows that the values with Port Commands are changed when FTP inspection is enabled. Inside Interface Capture shows the real value of IP and the port sent by Client for Server to connect to Client for Data Channel and Outside Interface Capture shows mapped address.

Scenario 2. FTP Client Configured for Passive Mode

Client in Inside Network of the ASA and Server in Outside Network.

Network Diagram
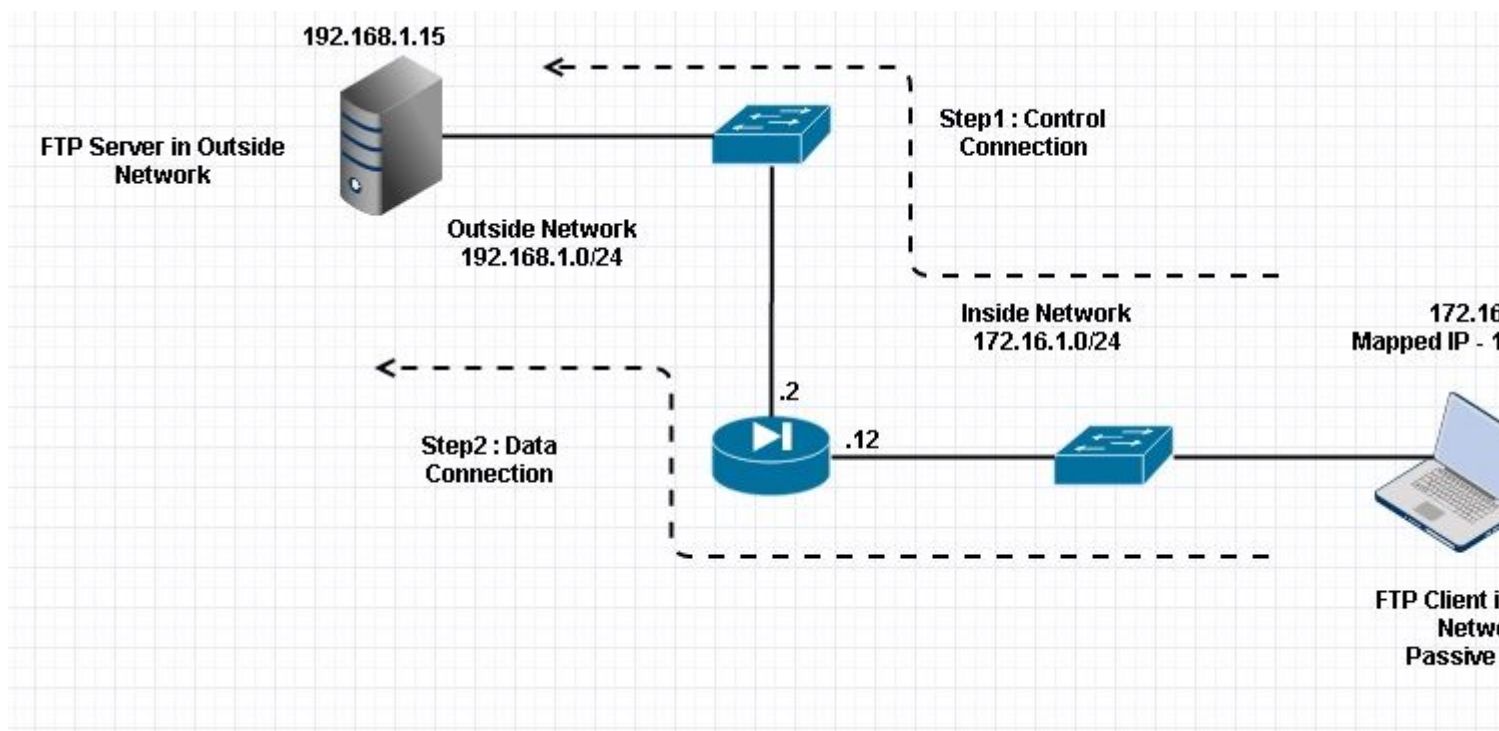
Connection

<#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
```

Here the client in inside initiates a connection with Source Port 61838 the Destination Port of 21. As it is a Passive FTP, client initiates both the connections. Therefore, after Client Sends **PASV** command, server replies with its 6 tuple value and client connects to that Socket for Data connection.

Capture Inside Interface as shown in this image.

Capture Outside Interface as shown in this image.

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=138(
49	35.657290	192.168.1.15	192.168.1.5	TCP	66	21→61838 [SYN, ACK] Seq=599740450 Ack=2543303556 Win=
50	35.657580	192.168.1.5	192.168.1.15	TCP	54	61838→21 [ACK] Seq=2543303556 Ack=599740451 Win=13110
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=13101
54	35.660510	192.168.1.15	192.168.1.5	FTP	115	Response: 220 Please visit http://sourceforge.net/pr(
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 director
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=13082
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
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=1
70	37.559410	192.168.1.15	192.168.1.5	TCP	66	60142→61839 [SYN, ACK] Seq=4281507304 Ack=737544149 V
71	37.559654	192.168.1.5	192.168.1.15	TCP	54	61839→60142 [ACK] Seq=737544149 Ack=4281507305 Win=26
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)..
```

Calculation for the Ports remains the same.

As mentioned earlier, the ASA re-writes the embedded IP values if FTP inspection is enabled. Also, it does open a dynamic port channel for data connection.

These are the connection details if **FTP Inspection is Disabled**

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
```

Without FTP inspection, It only tries to send **port** command again and again but there is no reply as outside

receives the PORT with Original IP not NATTed one. Same has been shown in the dump.

FTP inspection can be disabled with **no fixup protocol ftp 21** command in configuration terminal mode.

Without FTP inspection, only **PASV** command works when client is in Inside as there is there is no **port** command coming from Inside which needs to be embedded and both the connections are initiated from Inside.

Scenario 3. FTP Client Configured for Active Mode

Client in Outside Network of the ASA and Server in DMZ Network.

Network Diagram
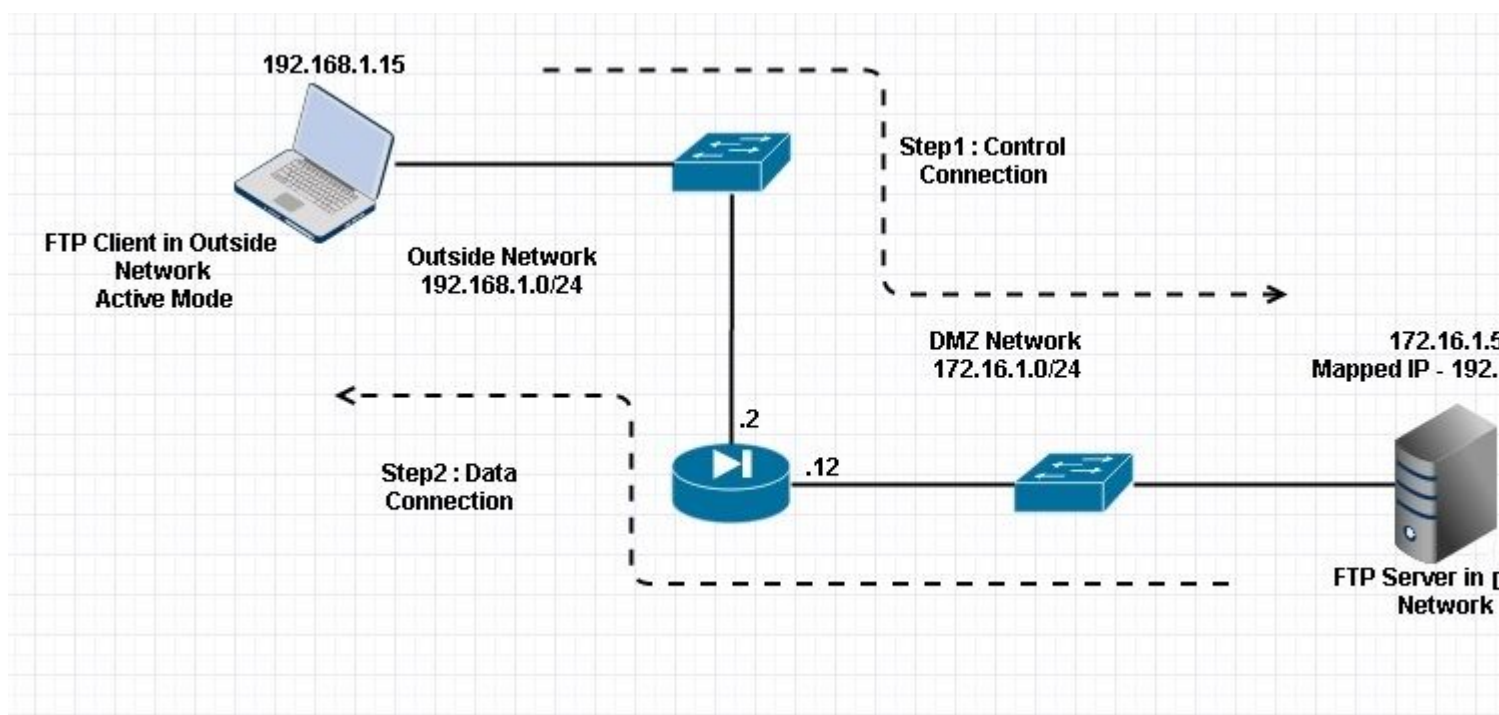
Configuration:

<#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)#

Verify

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

Capture DMZ Interface as shown in this image.

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	12.039239	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 Wir
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..
```

Capture Outside Interface as shown in this image.

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=146(
22	12.046232	192.168.1.5	192.168.1.15	TCP	66	21→55836 [SYN, ACK] Seq=726281311 Ack=2466096899 Win
23	12.049803	192.168.1.15	192.168.1.5	TCP	54	55836→21 [ACK] Seq=2466096899 Ack=726281312 Win=1311(
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/pro
27	12.051359	192.168.1.15	192.168.1.5	TCP	54	55836→21 [ACK] Seq=2466096899 Ack=726281399 Win=1310:
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 director
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=13082
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=138(
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 Wir
45	13.818653	192.168.1.5	192.168.1.15	TCP	54	20→55837 [ACK] Seq=3719615816 Ack=2377334291 Win=1311
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..
```

Here, the client is runs Active Mode Client 192.168.1.15 and initiates connection to server in DMZ on port 21. Client then sends **port** command with six tuple value to server to connect to that specific dynamic port. Server then initiates the data connection with Source Port as 20.

Scenario 4. FTP Client Running Passive Mode

Client in Outside Network of the ASA and Server in DMZ Network.

Network Diagram
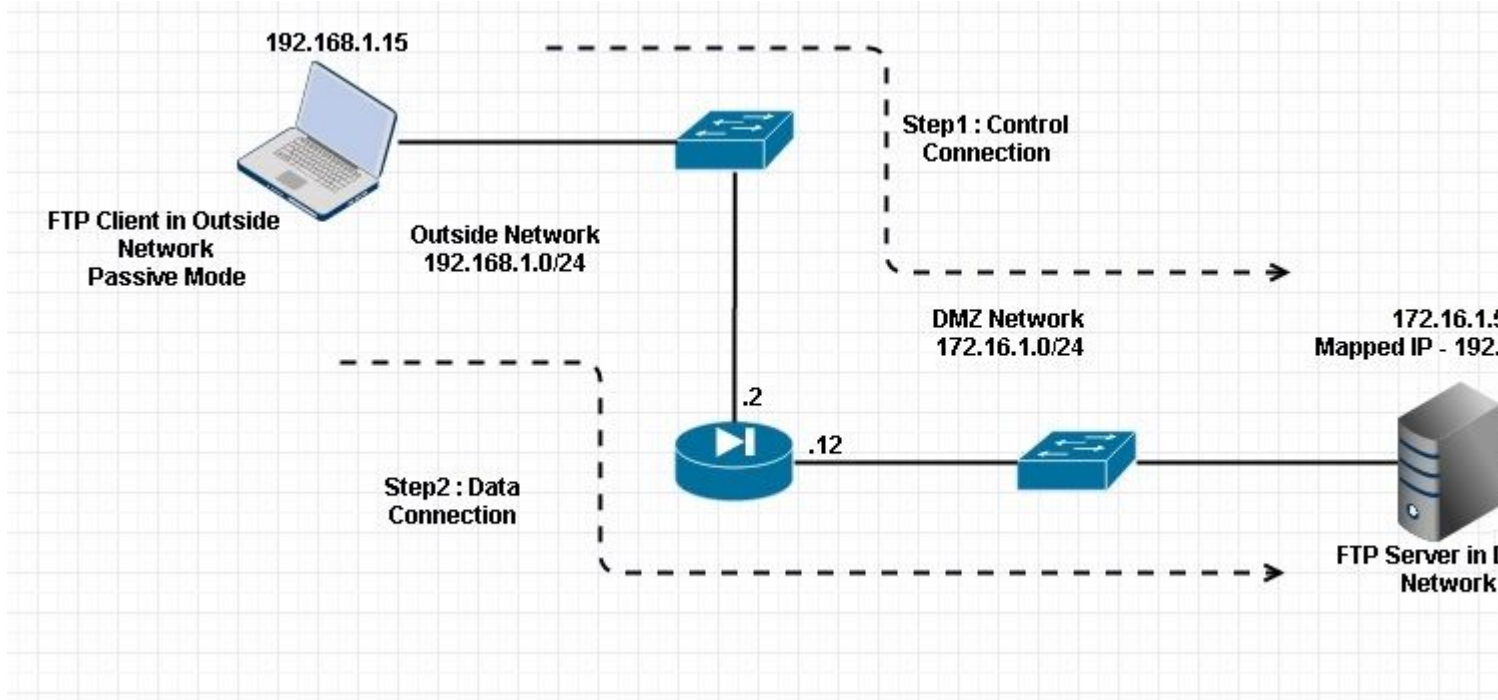
Connection

<#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
```

Capture DMZ Interface as shown in this image.

No.	Time	Source	Destination	Protocol	Length	Info
15	23.516688	192.168.1.15	172.16.1.5	TCP	66	60070→21 [SYN] Seq=3728695688 Win=8192 Len=0 MSS=138
16	23.517161	172.16.1.5	192.168.1.15	TCP	66	21→60070 [SYN, ACK] Seq=397133843 Ack=3728695689 Win=
17	23.517527	192.168.1.15	172.16.1.5	TCP	54	60070→21 [ACK] Seq=3728695689 Ack=397133844 Win=1311
18	23.521479	172.16.1.5	192.168.1.15	FTP	96	Response: 220-FileZilla Server version 0.9.33 beta
19	23.521708	172.16.1.5	192.168.1.15	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de
20	23.521967	172.16.1.5	192.168.1.15	FTP	115	Response: 220 Please visit http://sourceforge.net/pr
21	23.522196	192.168.1.15	172.16.1.5	TCP	54	60070→21 [ACK] Seq=3728695689 Ack=397133931 Win=1310
22	23.523737	192.168.1.15	172.16.1.5	FTP	66	Request: USER cisco
23	23.524546	172.16.1.5	192.168.1.15	FTP	87	Response: 331 Password required for cisco
24	23.526468	192.168.1.15	172.16.1.5	FTP	69	Request: PASS cisco123
25	23.528284	172.16.1.5	192.168.1.15	FTP	69	Response: 230 Logged on
26	23.531885	192.168.1.15	172.16.1.5	FTP	61	Request: CWD /
27	23.532602	172.16.1.5	192.168.1.15	FTP	101	Response: 250 CWD successful. "/" is current directo
28	23.536661	192.168.1.15	172.16.1.5	FTP	62	Request: TYPE I
29	23.537378	172.16.1.5	192.168.1.15	FTP	73	Response: 200 Type set to I
30	23.538842	192.168.1.15	172.16.1.5	FTP	60	Request: PASV
31	23.539880	172.16.1.5	192.168.1.15	FTP	101	Response: 227 Entering Passive Mode (172,16,1,5,241,
32	23.541726	192.168.1.15	172.16.1.5	FTP	84	Request: RETR n7000-s2-dk9.6.2.12.bin
33	23.543984	192.168.1.15	172.16.1.5	TCP	66	60071→61781 [SYN] Seq=4174881931 Win=65535 Len=0 MSS
34	23.544229	172.16.1.5	192.168.1.15	TCP	66	61781→60071 [SYN, ACK] Seq=4186544816 Ack=4174881932
35	23.544518	192.168.1.15	172.16.1.5	TCP	54	60071→61781 [ACK] Seq=4174881932 Ack=4186544817 Win=
36	23.546029	172.16.1.5	192.168.1.15	FTP	79	Response: 150 Connection accepted
37	23.549172	172.16.1.5	192.168.1.15	FTP-DATA	1434	FTP Data: 1380 bytes
38	23.549187	172.16.1.5	192.168.1.15	FTP-DATA	1434	FTP Data: 1380 bytes
39	23.549569	192.168.1.15	172.16.1.5	TCP	54	60071→61781 [ACK] Seq=4174881932 Ack=4186547577 Win=
40	23.549813	172.16.1.5	192.168.1.15	FTP-DATA	1434	FTP Data: 1380 bytes
41	23.549828	172.16.1.5	192.168.1.15	FTP-DATA	1434	FTP Data: 1380 bytes

⊞ 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: 21 (21), Dst Port: 60070 (60070), Seq: 397134106, Ack: 3728695737, Len: 47
⊟ File Transfer Protocol (FTP)
  ⊟ 227 Entering Passive Mode (172,16,1,5,241,85)\r\n
    Response code: Entering Passive Mode (227)
    Response arg: Entering Passive Mode (172,16,1,5,241,85)
    Passive IP address: 172.16.1.5 (172.16.1.5)
    Passive port: 61781

```
0030   01 ff d8 3f 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 37 32 2c 31 36 2c   31 2c 35 2c 32 34 31 2c    (172,16, 1,5,241,
0060   38 35 29 0d 0a                                       85)..
```

Capture Outside Interface as shown in this image.

No.	Time	Source	Destination	Protocol	Length	Info
29	23.528818	192.168.1.15	192.168.1.5	TCP	66	60070→21 [SYN] Seq=2627142457 Win=8192 Len=0 MSS=146
30	23.529413	192.168.1.5	192.168.1.15	TCP	66	21→60070 [SYN, ACK] Seq=1496461807 Ack=2627142458 Wi
31	23.529749	192.168.1.15	192.168.1.5	TCP	54	60070→21 [ACK] Seq=2627142458 Ack=1496461808 Win=131
32	23.533731	192.168.1.5	192.168.1.15	FTP	96	Response: 220-FileZilla Server version 0.9.33 beta
33	23.533960	192.168.1.5	192.168.1.15	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de
34	23.534219	192.168.1.5	192.168.1.15	FTP	115	Response: 220 Please visit http://sourceforge.net/pr
35	23.534433	192.168.1.15	192.168.1.5	TCP	54	60070→21 [ACK] Seq=2627142458 Ack=1496461895 Win=131
36	23.535974	192.168.1.15	192.168.1.5	FTP	66	Request: USER cisco
37	23.536798	192.168.1.5	192.168.1.15	FTP	87	Response: 331 Password required for cisco
38	23.538705	192.168.1.15	192.168.1.5	FTP	69	Request: PASS cisco123
39	23.540521	192.168.1.5	192.168.1.15	FTP	69	Response: 230 Logged on
40	23.544122	192.168.1.15	192.168.1.5	FTP	61	Request: CWD /
41	23.544854	192.168.1.5	192.168.1.15	FTP	101	Response: 250 CWD successful. "/" is current directo
42	23.548898	192.168.1.15	192.168.1.5	FTP	62	Request: TYPE I
43	23.549630	192.168.1.5	192.168.1.15	FTP	73	Response: 200 Type set to I
44	23.551064	192.168.1.15	192.168.1.5	FTP	60	Request: PASV
45	23.552163	192.168.1.5	192.168.1.15	FTP	102	Response: 227 Entering Passive Mode (192,168,1,5,241
46	23.553948	192.168.1.15	192.168.1.5	FTP	84	Request: RETR n7000-s2-dk9.6.2.12.bin
47	23.556176	192.168.1.15	192.168.1.5	TCP	66	60071→61781 [SYN] Seq=3795016102 Win=65535 Len=0 MSS
48	23.556466	192.168.1.5	192.168.1.15	TCP	66	61781→60071 [SYN, ACK] Seq=1047360618 Ack=3795016103
49	23.556740	192.168.1.15	192.168.1.5	TCP	54	60071→61781 [ACK] Seq=3795016103 Ack=1047360619 Win=
50	23.558281	192.168.1.5	192.168.1.15	FTP	79	Response: 150 Connection accepted
51	23.561409	192.168.1.5	192.168.1.15	FTP-DATA	1434	FTP Data: 1380 bytes
52	23.561424	192.168.1.5	192.168.1.15	FTP-DATA	1434	FTP Data: 1380 bytes
53	23.561806	192.168.1.15	192.168.1.5	TCP	54	60071→61781 [ACK] Seq=3795016103 Ack=1047363379 Win=
54	23.562065	192.168.1.5	192.168.1.15	FTP-DATA	1434	FTP Data: 1380 bytes
55	23.562081	192.168.1.5	192.168.1.15	FTP-DATA	1434	FTP Data: 1380 bytes

```
⊞ Frame 45: 102 bytes on wire (816 bits), 102 bytes captured (816 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: 21 (21), Dst Port: 60070 (60070), Seq: 1496462070, Ack: 2627142506, Len: 48
⊟ File Transfer Protocol (FTP)
  ⊟ 227 Entering Passive Mode (192,168,1,5,241,85)\r\n
       Response code: Entering Passive Mode (227)
       Response arg: Entering Passive Mode (192,168,1,5,241,85)
```

```
0030  01 ff c3 f5 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 35 2c 32 34 31    (192,168 ,1,5,241
0060  2c 38 35 29 0d 0a                                   ,85)..
```

Configure Basic FTP Application Inspection

By default, the configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy). Default application inspection traffic includes traffic to the default ports for each protocol.

You can only apply one global policy, so if you want to alter the global policy, for example, to apply inspection to non-standard ports, or to add inspections that are not enabled by default, you need to either edit the default policy or disable it and apply a new one. For a list of all default ports, refer to the Default Inspection Policy.

1. Run the **policy-map global_policy** command.

<#root>

```
ASA(config)#
```

policy-map global_policy

2. Run the **class inspection_default** command.

<#root>

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

```
    class inspection_default
```

3. Run the **inspect FTP** command.

```
<#root>

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

4. There is an option to use the **inspect FTP strict** command. This command increases the security of protected networks by preventing a web browser from sending embedded commands in FTP requests.

   After you enable the **strict** option on an interface, FTP inspection enforces this behavior:

   - An FTP command must be acknowledged before the Security Appliance allows a new command

   - The Security Appliance drops a connection that sends embedded commands

   - The **227** and **PORT** commands are checked to ensure that they do not appear in an error string

   ---

   Warning: The use of the **strict** option possibly causes the failure of FTP clients that are not strictly compliant with FTP RFCs. Refer to Using the strict Option for more information on the use of the **strict** option.

Configure FTP Protocol Inspection on Non-Standard TCP Port

You can configure the FTP Protocol Inspection for non-standard TCP ports with these configuration lines (replace XXXX with the new port number):

```
<#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
```

Verify

In order to ensure that the configuration has successfully taken, run the **show service-policy** command. Also, limit the output to the FTP inspection by running the **show service-policy inspect ftp** command.

```
<#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

TFTP inspection is enabled by default.

The security appliance inspects TFTP traffic and dynamically creates connections and translations, if necessary, to permit file transfer between a TFTP client and server. Specifically, the inspection engine inspects TFTP Read Requests (RRQ), Write Requests (WRQ), and Error Notifications (ERROR).

A dynamic secondary channel and a PAT translation, if necessary, are allocated on a reception of a valid RRQ or WRQ. This secondary channel is subsequently used by TFTP for file transfer or error notification.

Only the TFTP server can initiate traffic over the secondary channel, and at most one incomplete secondary channel can exist between the TFTP client and server. An error notification from the server closes the secondary channel.

TFTP inspection must be enabled if fstatic PAT is used to redirect TFTP traffic.

Configure Basic TFTP Application Inspection

By default, the configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy). Default application inspection traffic includes traffic to the default ports for each protocol.

You can only apply one global policy. So if you want to alter the global policy, for example, to apply inspection to non-standard ports, or to add inspections that are not enabled by default, you need to either edit the default policy or disable it and apply a new one. For a list of all default ports, refer to the Default Inspection Policy.

1. Run the **policy-map global_policy** command.

```
<#root>

 ASA(config)#

policy-map global_policy
```
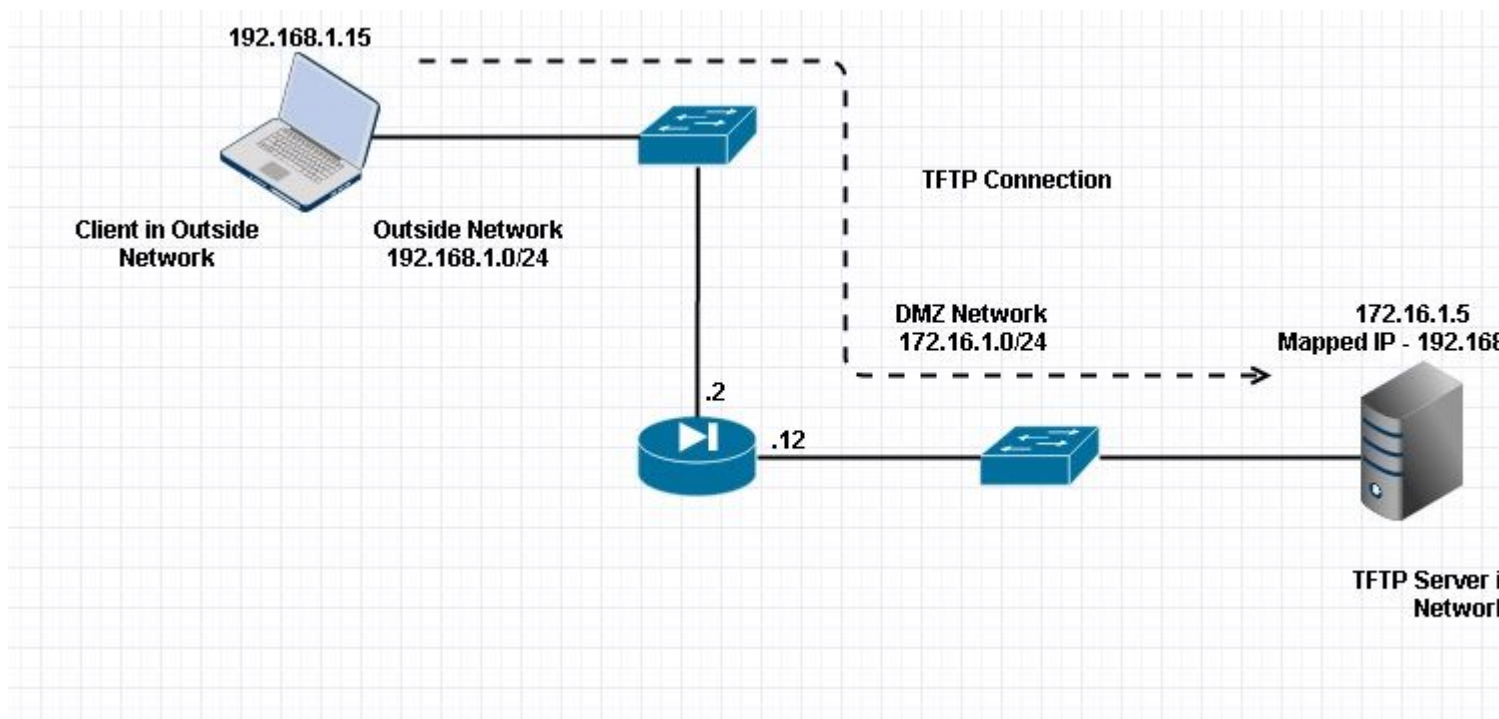
2. Run the **class inspection_default** command.

```
<#root>

 ASA(config-pmap)#

class inspection_default
```

3. Run the **inspect TFTP** command.

```
<#root>

 ASA(config-pmap-c)#

inspect TFTP
```

Network Diagram

Here the client in configured in Outside Network. TFTP server is placed in DMZ Network. Server is mapped to the IP 192.168.1.5 which is in Outside Subnet.

Configuration Example:

```
<#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)#
```

Verify

In order to ensure the configuration has successfully taken, run the **show service-policy** command. Also, limit the output to the TFTP inspection only by running the **show service-policy inspect tftp** command.

```
<#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#
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Packet Tracer

Client in Inside Network

<#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 in Outside Network

<#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
```

As seen in both the packet-tracers, the traffic hits their respective NAT statements and FTP inspection Policy. They also leave their required interfaces.

During troubleshooting, you can try to capture the ASA Ingress and Egress interfaces and see if the ASA Embedded IP address re-write is working fine and check the connection if the dynamic port is being allowed on ASA.