

# Configuración de servicios FTP/TFTP: ASA 9.X

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Gestión avanzada de protocolos](#)

[Configuración](#)

[Escenario 1. Cliente FTP configurado para modo activo](#)

[Diagrama de la red](#)

[Situación hipotética 2. Cliente FTP configurado para modo pasivo](#)

[Diagrama de la red](#)

[Situación hipotética 3. Cliente FTP configurado para modo activo](#)

[Diagrama de la red](#)

[Situación hipotética 4. Cliente FTP que ejecuta el modo pasivo](#)

[Diagrama de la red](#)

[Configurar inspección básica de aplicaciones FTP](#)

[Configuración de la inspección de protocolo FTP en puerto TCP no estándar](#)

[Verificación](#)

[TFTP](#)

[Configurar inspección básica de la aplicación TFTP](#)

[Diagrama de la red](#)

[Verificación](#)

[Troubleshoot](#)

[Cliente en la red interna](#)

[Cliente en red externa](#)

## Introducción

Este documento describe diferentes escenarios de inspección de FTP y TFTP en ASA, la configuración de inspección de FTP/TFTP de ASA y la resolución de problemas básica.

## Prerequisites

## Requirements

Cisco recomienda conocer estos temas:

- Comunicación básica entre interfaces requeridas
- Configuración del servidor FTP ubicado en la red DMZ

## Componentes Utilizados

Este documento describe diferentes escenarios de inspección de FTP y TFTP en el Adaptive Security Appliance (ASA) y también cubre la configuración de inspección de FTP/TFTP de ASA y la resolución de problemas básica.

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA serie 5500 o ASA serie 5500-X que ejecuta la imagen de software 9.1(5)
- Cualquier servidor FTP
- Cualquier cliente FTP

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## **Antecedentes**

El dispositivo de seguridad admite la inspección de aplicaciones mediante la función de algoritmo de seguridad adaptable.

A través de la inspección de aplicación con estado utilizada por el algoritmo de seguridad adaptable, el dispositivo de seguridad realiza un seguimiento de cada conexión que atraviesa el firewall y garantiza que son válidas.

El firewall, a través de la inspección con estado, también supervisa el estado de la conexión para compilar la información y colocarla en una tabla de estado.

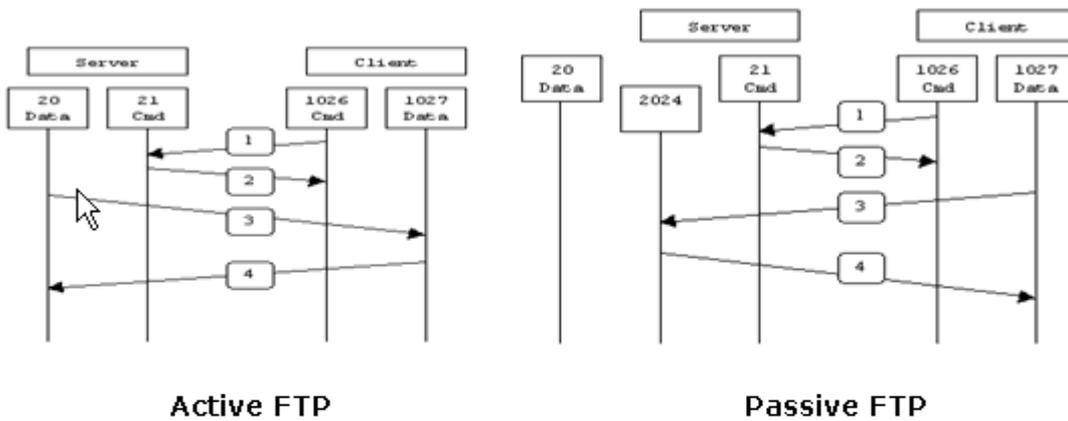
Con el uso de la tabla de estados además de las reglas definidas por el administrador, las decisiones de filtrado se basan en el contexto establecido por los paquetes que previamente pasaron a través del firewall.

La aplicación de las inspecciones de aplicación consiste en las siguientes acciones:

- Identificar el tráfico
- Aplicar inspecciones al tráfico
- Activar inspecciones en una interfaz

Hay dos formas de FTP, como se muestra en la imagen.

- Modo activo
- Modo pasivo



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 activo

En el modo FTP activo, el cliente se conecta desde un puerto aleatorio no privilegiado ( $N > 1023$ ) al puerto de comando (21) del servidor FTP. Luego, el cliente comienza a escuchar el puerto  $N > 1023$  y envía el comando FTP `port N > 1023` al servidor FTP. A continuación, el servidor vuelve a conectarse a los puertos de datos especificados del cliente desde su puerto de datos local, que es el puerto 20.

### FTP pasivo

En el modo FTP pasivo, el cliente inicia ambas conexiones al servidor, lo que soluciona el problema de un firewall que filtra la conexión del puerto de datos entrante al cliente desde el servidor. Cuando se abre una conexión FTP, el cliente abre dos puertos aleatorios no privilegiados localmente. El primer puerto entra en contacto con el servidor en el puerto 21. Pero en lugar de ejecutar un comando **port** y permitir que el servidor se conecte nuevamente a su puerto de datos, el cliente ejecuta el comando **PASV**. El resultado de esto es que el servidor abre un puerto aleatorio sin privilegios ( $P > 1023$ ) y envía el comando **port P** al cliente. A continuación, el cliente inicia la conexión desde el puerto  $N > 1023$  al puerto P del servidor para transferir datos. Sin la configuración del comando **inspection** en el dispositivo de seguridad, el FTP de los usuarios internos que salen funciona solamente en el modo pasivo. Además, se deniega el acceso a los usuarios externos que entran en el servidor FTP.

### TFTP

TFTP, como se describe en [RFC 1350](#), es un protocolo simple para leer y escribir archivos entre un servidor TFTP y un cliente. TFTP utiliza el puerto UDP 69.

## Gestión avanzada de protocolos

¿Por qué necesita la inspección de FTP?

Algunas aplicaciones requieren una gestión especial por parte de la función de inspección de aplicaciones del appliance de seguridad de Cisco. Estos tipos de aplicaciones suelen incrustar información de direccionamiento IP en el paquete de datos del usuario o abrir canales secundarios en puertos asignados

dinámicamente. La función de inspección de aplicaciones funciona con la traducción de direcciones de red (NAT) para ayudar a identificar la ubicación de la información de direccionamiento incrustada.

Además de la identificación de la información de direccionamiento incorporada, la función de inspección de la aplicación monitorea las sesiones para determinar los números de puerto para los canales secundarios. Muchos protocolos abren puertos TCP o UDP secundarios para mejorar el rendimiento. La sesión inicial en un puerto conocido se utiliza para negociar números de puerto asignados dinámicamente.

La función de inspección de aplicaciones supervisa estas sesiones, identifica las asignaciones de puertos dinámicos y permite el intercambio de datos en estos puertos durante las sesiones específicas. Las aplicaciones multimedia y FTP muestran este tipo de comportamiento.

Si la inspección FTP no se ha habilitado en el dispositivo de seguridad, esta solicitud se descarta y las sesiones FTP no transmiten los datos solicitados.

Si la inspección FTP está habilitada en el ASA, el ASA monitorea el canal de control e intenta reconocer una solicitud para abrir el canal de datos. El protocolo FTP integra las especificaciones del puerto del canal de datos en el tráfico del canal de control, lo que requiere que el dispositivo de seguridad inspeccione el canal de control en busca de cambios en el puerto de datos.

Una vez que ASA reconoce una solicitud, crea temporalmente una apertura para el tráfico del canal de datos que dura toda la sesión. De esta manera, la función de inspección FTP monitorea el canal de control, identifica una asignación de puerto de datos y permite el intercambio de datos en el puerto de datos durante toda la sesión.

ASA inspecciona las conexiones del puerto 21 para el tráfico FTP de forma predeterminada a través del mapa de clase de inspección global. El dispositivo de seguridad también reconoce la diferencia entre una sesión FTP activa y una pasiva.

Si las sesiones FTP soportan la transferencia de datos FTP pasiva, el ASA a través del comando **inspect ftp**, reconoce la solicitud de puerto de datos del usuario y abre un nuevo puerto de datos mayor que 1023.

El comando **inspect ftp** inspecciona las sesiones FTP y realiza cuatro tareas:

- Prepara una conexión de datos secundaria dinámica
- Realiza un seguimiento de la secuencia de respuesta a comandos FTP
- Genera una pista de auditoría
- Traduce la dirección IP incrustada mediante NAT

La inspección de la aplicación FTP prepara los canales secundarios para la transferencia de datos FTP. Los canales se asignan en respuesta a una carga de archivo, una descarga de archivo o un evento de listado de directorio, y deben negociarse previamente. El puerto se negocia a través de los comandos **PORT** o **PASV** (227).

## Configuración

---

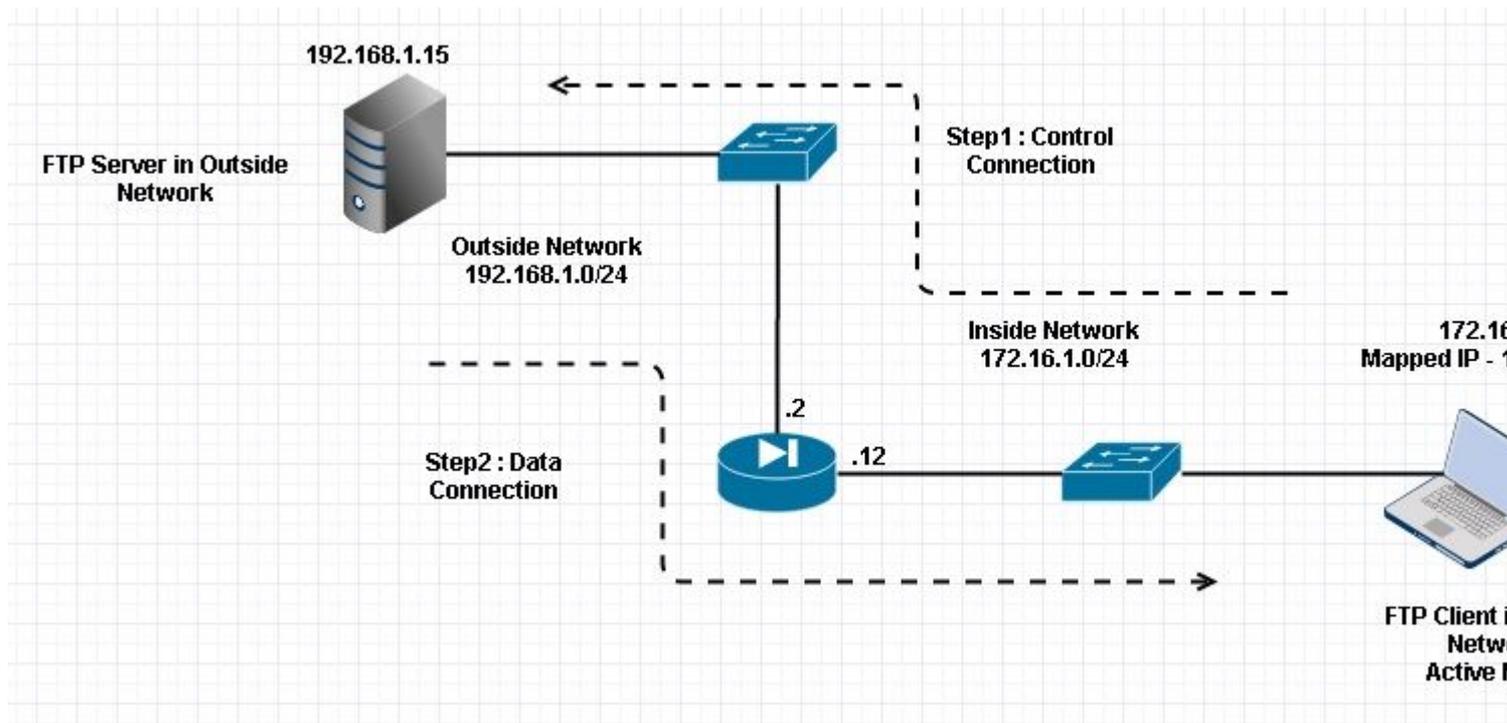
**Nota:** Todos los escenarios de red se explican con la inspección FTP habilitada en el ASA.

---

### Escenario 1. Cliente FTP configurado para modo activo

Cliente conectado a la red interna del ASA y servidor en la red externa.

## Diagrama de la red



**Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet.**

Como se muestra en esta imagen, la configuración de red utilizada tiene ASA con cliente en la red interna con IP 172.16.1.5. El servidor está en una red externa con IP 192.168.1.15. El cliente tiene una IP asignada 192.168.1.5 en la red externa .

No es necesario permitir ninguna lista de acceso en la interfaz externa ya que la inspección FTP abre el canal de puerto dinámico.

Ejemplo de configuración:

```
<#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)#
```

## Verificación

### Conexión

```
<#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
```

Aquí el cliente en Inside inicia la conexión con el puerto de origen 61854 al puerto de destino 21. El cliente luego envía el comando **Port** con un valor de 6 tuplas. El servidor, a su vez, inicia la conexión de datos/secundarios con el puerto de origen 20 y el puerto de destino se calcula a partir de los pasos mencionados después de estas capturas.

Capture Inside Interface como se muestra en esta imagen.

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 Win=
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	.AD"@... <.....
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 como se muestra en esta imagen.

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 director
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	.80"@... (/.....
0020	01 0f f1 9e 00 15 6e d5	53 ea 0c b8 be 30 50 18	.....n. S...OP.
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..

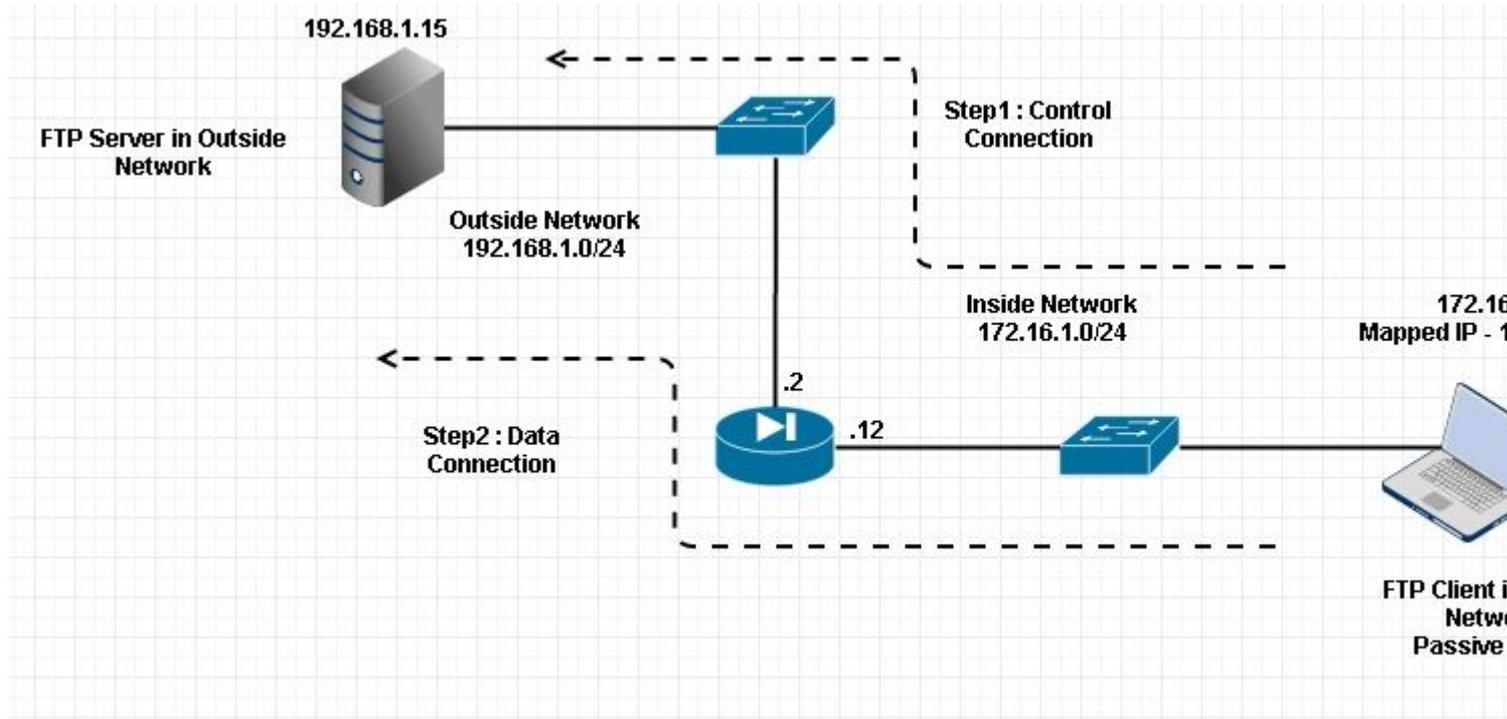
El valor del puerto se calcula utilizando los dos últimos puntos de seis. Izquierda 4 tuplas son dirección IP y 2 tuplas son para puerto. Como se muestra en esta imagen, la dirección IP es 192.168.1.5 y  $241 * 256 + 159 = 61855$ .

La captura también muestra que los valores con los comandos de puerto cambian cuando se habilita la inspección FTP. La captura de interfaz interna muestra el valor real de IP y el puerto enviado por el cliente para que el servidor se conecte con el cliente para el canal de datos y la captura de interfaz externa muestra la dirección asignada.

## Situación hipotética 2. Cliente FTP configurado para modo pasivo

Cliente en la red interna del ASA y Servidor en la red externa.

### Diagrama de la red



### Conexión

```
<#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

Aquí el cliente en el interior inicia una conexión con el Puerto de Origen 61838 el Puerto de Destino de 21. Como es un FTP pasivo, el cliente inicia ambas conexiones. Por lo tanto, después de que el cliente envía el comando **PASV**, el servidor responde con su valor de 6 tuplas y el cliente se conecta a ese Socket para la conexión de datos.

Capture Inside Interface como se muestra en esta imagen.

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
49	35.657458	192.168.1.15	172.16.1.5	TCP	66	21+61838 [SYN, ACK] Seq=700898682 Ack=1456310601 Win=
50	35.657717	172.16.1.5	192.168.1.15	TCP	54	61838+21 [ACK] Seq=1456310601 Ack=700898683 win=1310
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=1310
54	35.660677	192.168.1.15	172.16.1.5	FTP	115	Response: 220 Please visit http://sourceforge.net/pro
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 director
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=1308
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=
70	37.559578	192.168.1.15	172.16.1.5	TCP	66	60142+61839 [SYN, ACK] Seq=2027855230 Ack=597547300
71	37.559791	172.16.1.5	192.168.1.15	TCP	54	61839+60142 [ACK] Seq=597547300 Ack=2027855231 win=2
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)..

Capture Outside Interface como se muestra en esta imagen.

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
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=1380
50	35.657580	192.168.1.5	192.168.1.15	TCP	54	61838+21 [ACK] Seq=2543303556 Ack=599740451 win=1310
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=1310
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=1308
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
70	37.559410	192.168.1.15	192.168.1.5	TCP	66	60142+61839 [SYN, ACK] Seq=4281507304 Ack=737544149 Win=65535 Len=0 MSS=1380
71	37.559654	192.168.1.5	192.168.1.15	TCP	54	61839+60142 [ACK] Seq=737544149 Ack=4281507305 win=260
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)..

```

El cálculo de los puertos no varía.

Como se mencionó anteriormente, ASA vuelve a escribir los valores de IP integrados si la inspección FTP está habilitada. Además, abre un canal de puerto dinámico para la conexión de datos.

Estos son los detalles de conexión si **La inspección de FTP está desactivada**

Conexión:

<#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

```

Sin la inspección FTP, solamente intenta enviar el comando **port** una y otra vez, pero no hay respuesta ya

que el exterior recibe el PORT con la IP original no NATted uno. Lo mismo se ha mostrado en el vertedero.

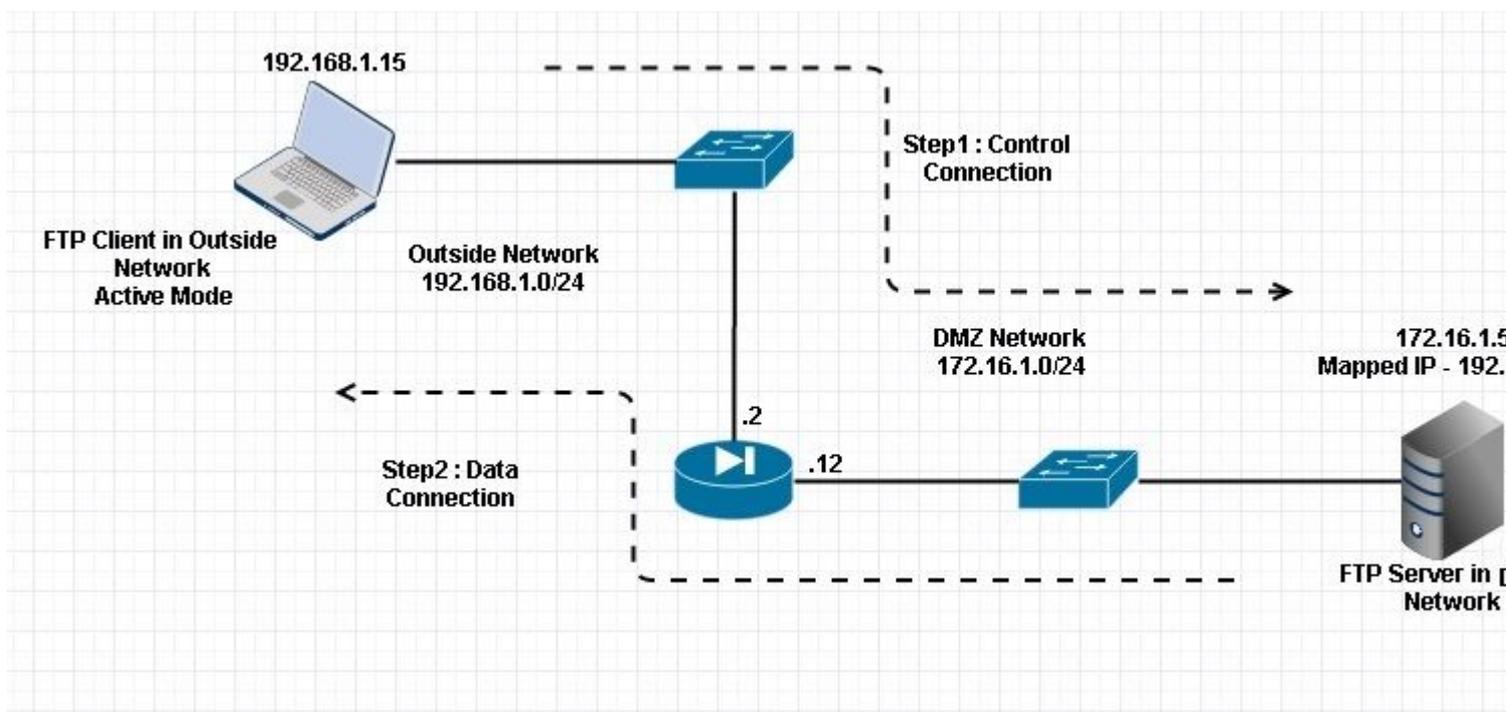
La inspección FTP se puede inhabilitar con el comando **no fixup protocol ftp 21** en el modo de terminal de configuración.

Sin la inspección FTP, sólo funciona el comando **PASV** cuando el cliente está en Inside ya que no hay ningún comando **port** proveniente de Inside que deba ser embebido y ambas conexiones se inician desde Inside.

### Situación hipotética 3. Cliente FTP configurado para modo activo

Cliente en red externa de ASA y servidor en red DMZ.

#### Diagrama de la red



Configuración:

```
<#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)#
```

## Verificación

Conexión:

```
<#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 la interfaz DMZ como se muestra en esta imagen.

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 Win=8192 Len=0 MSS=138
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/projects/filezilla
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 directory
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=131
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=8192 Len=0 MSS=146
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	.82.@... .....
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 como se muestra en esta imagen.

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
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=1460
23	12.049803	192.168.1.15	192.168.1.5	TCP	54	55836→21 [ACK] Seq=2466096899 Ack=726281312 Win=131080 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=131080 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=130800 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
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	20→55837 [ACK] Seq=3719615816 Ack=2377334290 Win=131080 Len=0
45	13.818653	192.168.1.5	192.168.1.15	TCP	54	20→55837 [ACK] Seq=3719615816 Ack=2377334291 Win=131080 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 .8z.@... .@.....
0020 01 05 da 1c 00 15 92 fd a7 32 2b 4a 2d 85 50 18 ..... .2+)-.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..

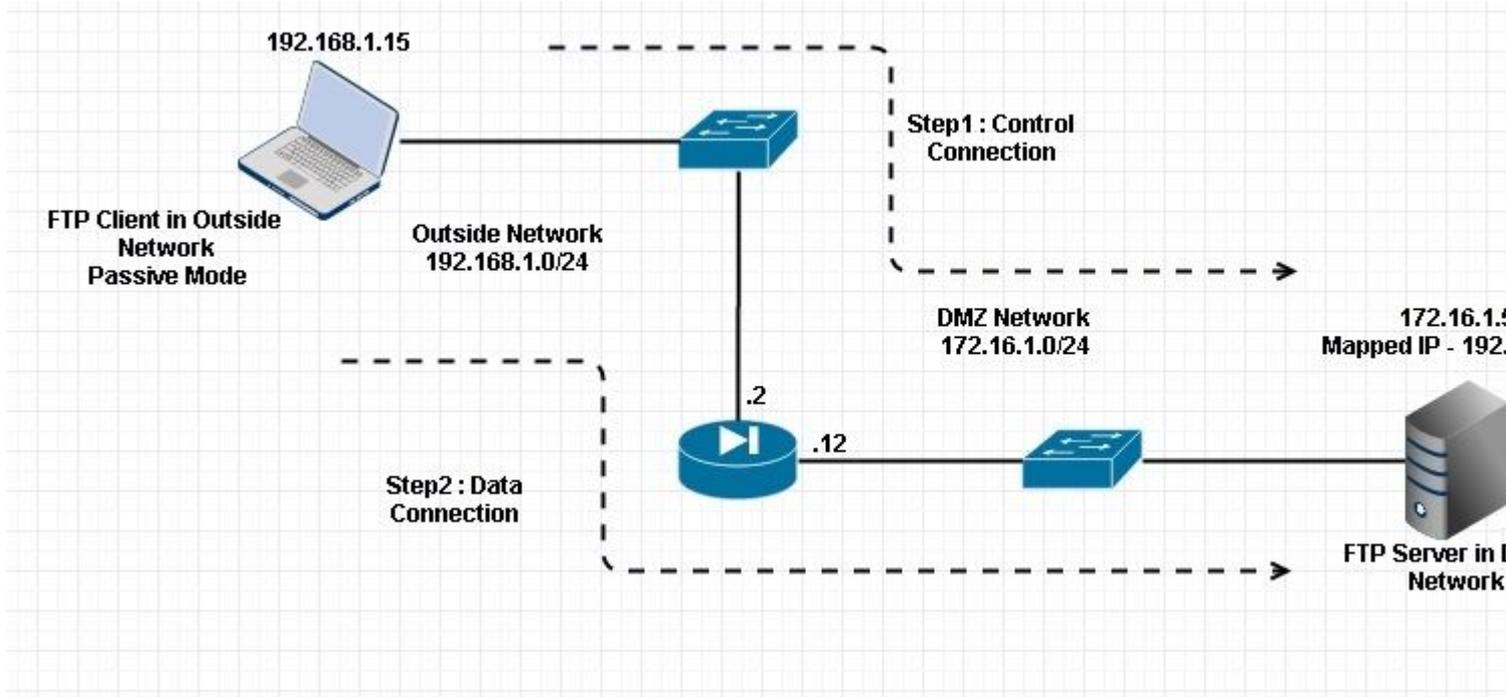
```

Aquí, el cliente ejecuta el cliente de modo activo 192.168.1.15 e inicia la conexión con el servidor en DMZ en el puerto 21. A continuación, el cliente envía el comando **port** con un valor de seis tuplas al servidor para conectarse a ese puerto dinámico específico. El servidor inicia la conexión de datos con el puerto de origen como 20.

#### Situación hipotética 4. Cliente FTP que ejecuta el modo pasivo

Cliente en red externa de ASA y servidor en red DMZ.

#### Diagrama de la red



Conexión

<#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 la interfaz DMZ como se muestra en esta imagen.

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 como se muestra en esta imagen.

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=1460
30	23.529413	192.168.1.5	192.168.1.15	TCP	66	21→60070 [SYN, ACK] Seq=1496461807 Ack=2627142458 Win=65535 Len=0 MSS=1460
31	23.529749	192.168.1.15	192.168.1.5	TCP	54	60070→21 [ACK] Seq=2627142458 Ack=1496461808 Win=131080 Len=0
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/projects/filezilla
35	23.534433	192.168.1.15	192.168.1.5	TCP	54	60070→21 [ACK] Seq=2627142458 Ack=1496461895 Win=131080 Len=0
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 directory
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 (192,168,1,5,241,85)
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=1460
48	23.556466	192.168.1.5	192.168.1.15	TCP	66	61781→60071 [SYN, ACK] Seq=1047360618 Ack=3795016103 Win=65535 Len=0 MSS=1460
49	23.556740	192.168.1.15	192.168.1.5	TCP	54	60071→61781 [ACK] Seq=3795016103 Ack=1047360619 Win=65535 Len=0
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=65535 Len=0
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

[E] Frame 45: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface...  
 [E] Ethernet II, Src: Cisco\_c9:92:88 (00:19:e8:c9:92:88), Dst: Vmware\_ad:24:76 (00:50:56:ad:24:76)  
 [E] Internet Protocol Version 4, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.15 (192.168.1.15)  
 [E] Transmission Control Protocol, Src Port: 21 (21), Dst Port: 60070 (60070), Seq: 1496462070, Ack: 2627142506, Len: 48  
 [E] File Transfer Protocol (FTP)  
 [E] 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)..
  
```

## Configurar inspección básica de aplicaciones FTP

De forma predeterminada, la configuración incluye una política que coincide con todo el tráfico de inspección de aplicaciones predeterminado y aplica la inspección al tráfico en todas las interfaces (una política global). El tráfico de inspección de aplicaciones predeterminado incluye el tráfico a los puertos predeterminados para cada protocolo.

Sólo puede aplicar una política global, por lo que si desea modificar la política global, por ejemplo, para aplicar la inspección a puertos no estándar, o para agregar inspecciones que no están activadas de forma predeterminada, debe editar la política predeterminada o desactivarla y aplicar una nueva. Para obtener una lista de todos los puertos predeterminados, consulte la [Política de inspección predeterminada](#).

1. Ejecute el comando **policy-map global\_policy**.

```

<#root>

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

2. Ejecute el comando **class inspection\_default**.

```

<#root>
  
```

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

### 3. Ejecute el comando **inspect FTP**.

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

### 4. Hay una opción para utilizar el comando **inspect FTP strict**. Este comando aumenta la seguridad de las redes protegidas al impedir que un explorador web envíe comandos incrustados en solicitudes FTP.

Después de habilitar la opción **strict** en una interfaz, la inspección FTP aplica este comportamiento:

- Se debe confirmar un comando FTP antes de que el dispositivo de seguridad permita un nuevo comando
- El dispositivo de seguridad descarta una conexión que envía comandos incrustados
- Los comandos **227** y **PORT** se verifican para asegurarse de que no aparezcan en una cadena de error

---

**Advertencia:** El uso de la opción **strict** posiblemente cause la falla de clientes FTP que no cumplen estrictamente con RFCs FTP. Consulte [Uso de la Opción Strict](#) para obtener más información sobre el uso de la opción **Strict**.

---

## Configuración de la inspección de protocolo FTP en puerto TCP no estándar

Puede configurar la inspección de protocolo FTP para puertos TCP no estándar con estas líneas de configuración (sustituya XXXX por el nuevo número de puerto):

```
<#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
```

## Verificación

Para asegurarse de que la configuración se haya realizado correctamente, ejecute el comando **show service-policy**. Además, limite la salida a la inspección FTP ejecutando el 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

La inspección TFTP está habilitada de forma predeterminada.

El dispositivo de seguridad inspecciona el tráfico TFTP y crea dinámicamente conexiones y traducciones, si es necesario, para permitir la transferencia de archivos entre un cliente TFTP y un servidor.

Específicamente, el motor de inspección inspecciona las solicitudes de lectura de TFTP (RRQ), las solicitudes de escritura (WRQ) y las notificaciones de error (ERROR).

Un canal secundario dinámico y una traducción PAT, si es necesario, se asignan en una recepción de una RRQ o WRQ válida. Este canal secundario es utilizado posteriormente por TFTP para la transferencia de archivos o la notificación de errores.

Solamente el servidor TFTP puede iniciar tráfico sobre el canal secundario, y como máximo puede existir un canal secundario incompleto entre el cliente TFTP y el servidor. Una notificación de error del servidor cierra el canal secundario.

La inspección TFTP debe estar habilitada si se utiliza la PAT estática para redirigir el tráfico TFTP.

### Configurar inspección básica de la aplicación TFTP

De forma predeterminada, la configuración incluye una política que coincide con todo el tráfico de inspección de aplicaciones predeterminado y aplica la inspección al tráfico en todas las interfaces (una política global). El tráfico de inspección de aplicaciones predeterminado incluye el tráfico a los puertos predeterminados para cada protocolo.

Sólo puede aplicar una política global. Por lo tanto, si desea modificar la política global, por ejemplo, para aplicar la inspección a los puertos no estándar, o para agregar inspecciones que no están habilitadas de forma predeterminada, debe editar la política predeterminada o desactivarla y aplicar una nueva. Para obtener una lista de todos los puertos predeterminados, consulte la [Política de inspección predeterminada](#).

1. Ejecute el comando **policy-map global\_policy**.

```
<#root>
```

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

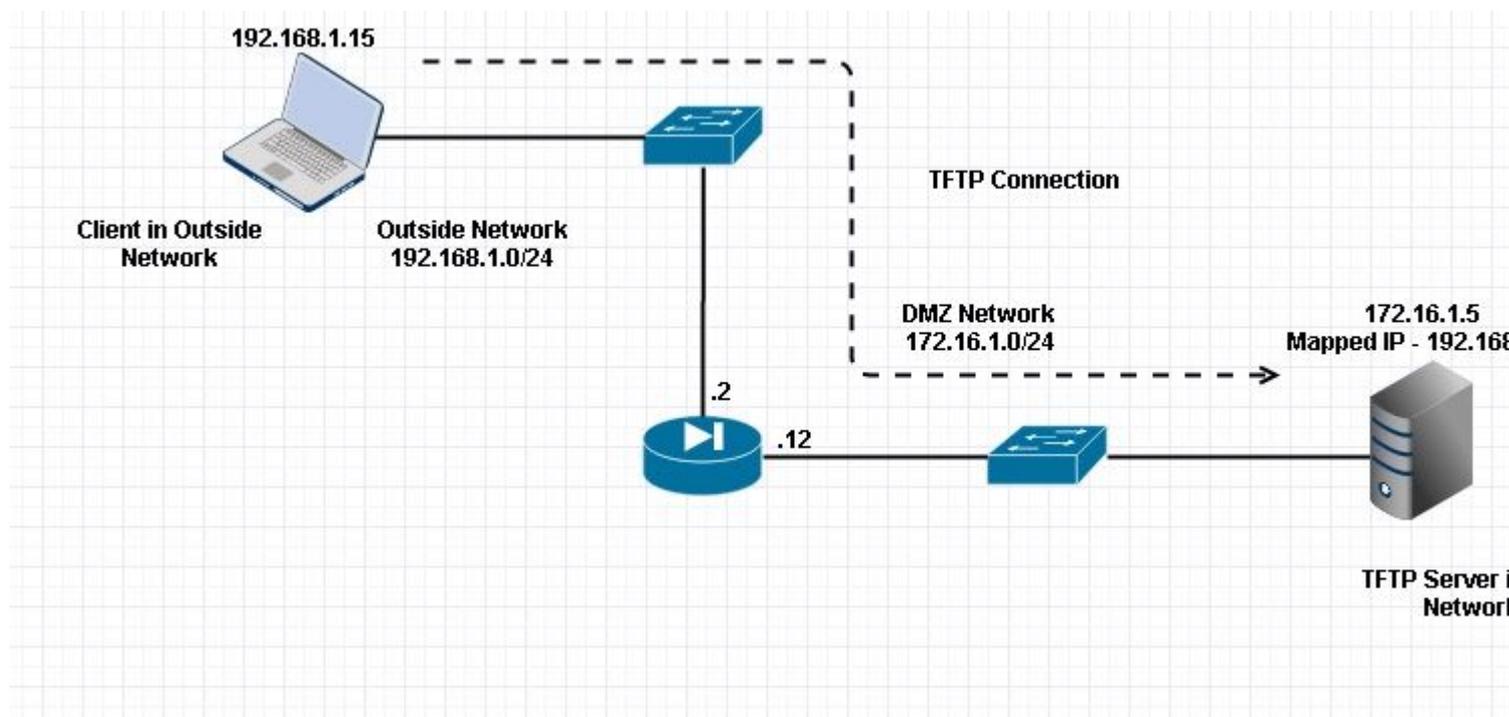
2. Ejecute el comando **class inspection\_default**.

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

3. Ejecute el comando **inspect TFTP**.

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

## Diagrama de la red



Aquí el cliente está configurado en Red externa. El servidor TFTP se coloca en la red DMZ. El servidor está asignado a la IP 192.168.1.5 que está en la subred externa.

## Ejemplo de configuración:

<#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)#

```

## Verificación

Para asegurarse de que la configuración se haya realizado correctamente, ejecute el comando **show service-policy**. Además, limite la salida a la inspección TFTP solamente ejecutando el 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#
```

## Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Packet Tracer

### Ciente en la red 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

## Ciente en red externa

<#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
```

Como se ve en ambos rastreadores de paquetes, el tráfico llega a sus respectivas declaraciones NAT y política de inspección FTP. También dejan las interfaces necesarias.

Durante la resolución de problemas, puede intentar capturar las interfaces de ingreso y egreso de ASA y ver si la reescritura de la dirección IP incorporada de ASA funciona correctamente y verificar la conexión si se permite el puerto dinámico en ASA.

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).