Configuración de servicios FTP/TFTP: ASA 9.X

Contenido

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.

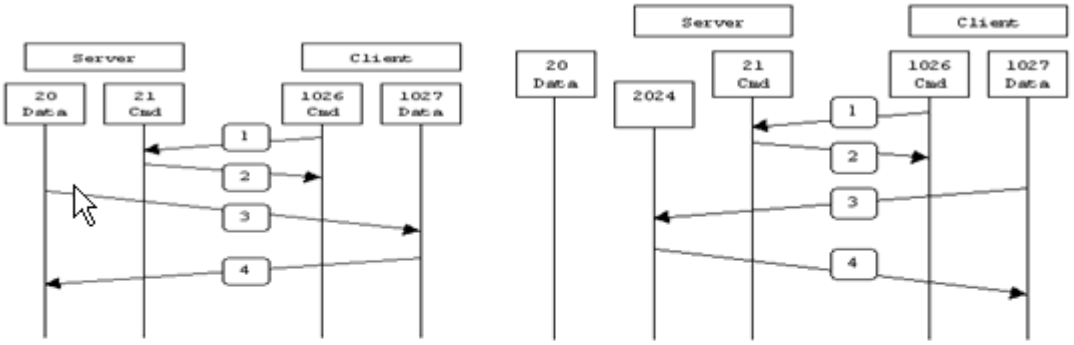
Con el uso de la tabla de estados además de las reglas definidas por el administrador, las decisiones de filtrado se basan en el contexto establecido por los paquetes que previamente pasaron a través del firewall.

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

Passive FTP

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

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

FTP 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).

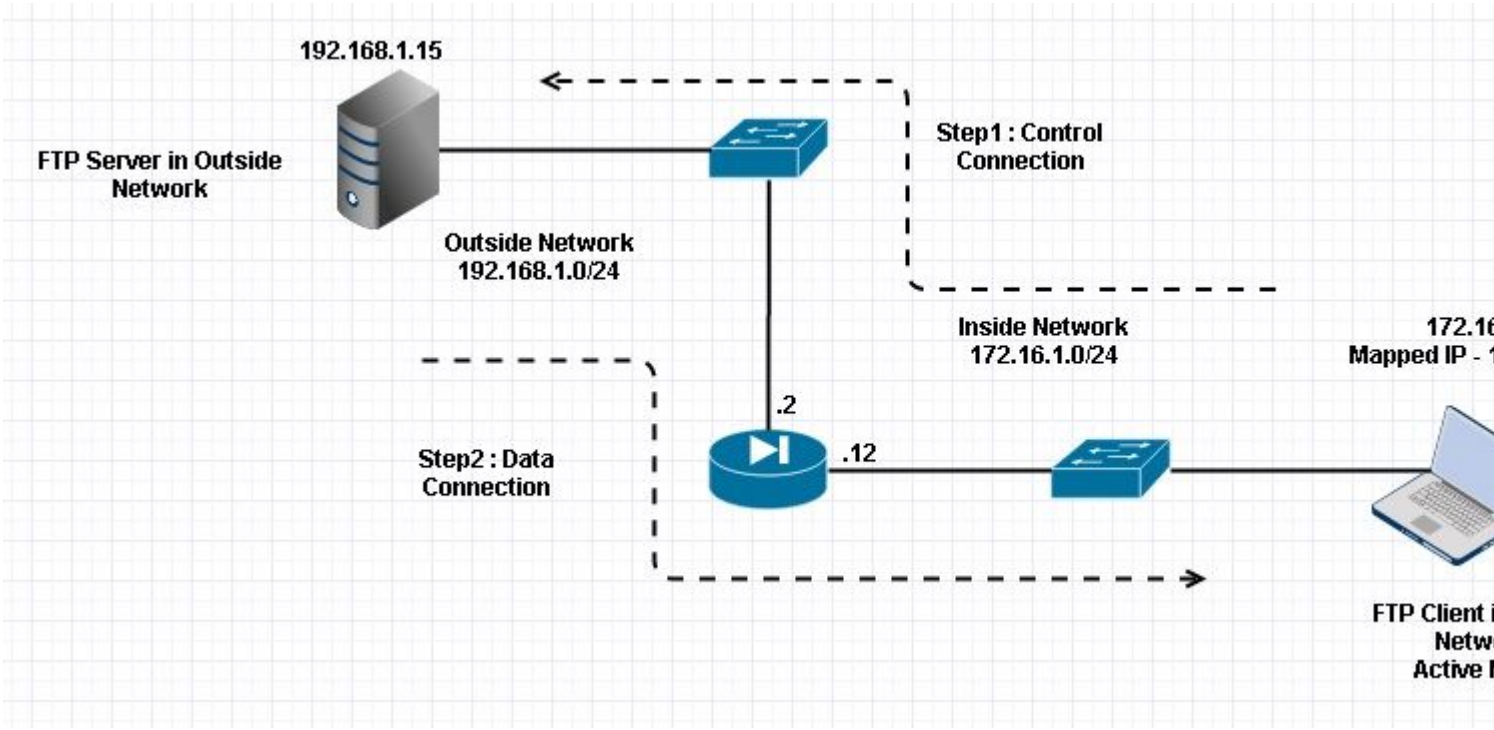
Configuración

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

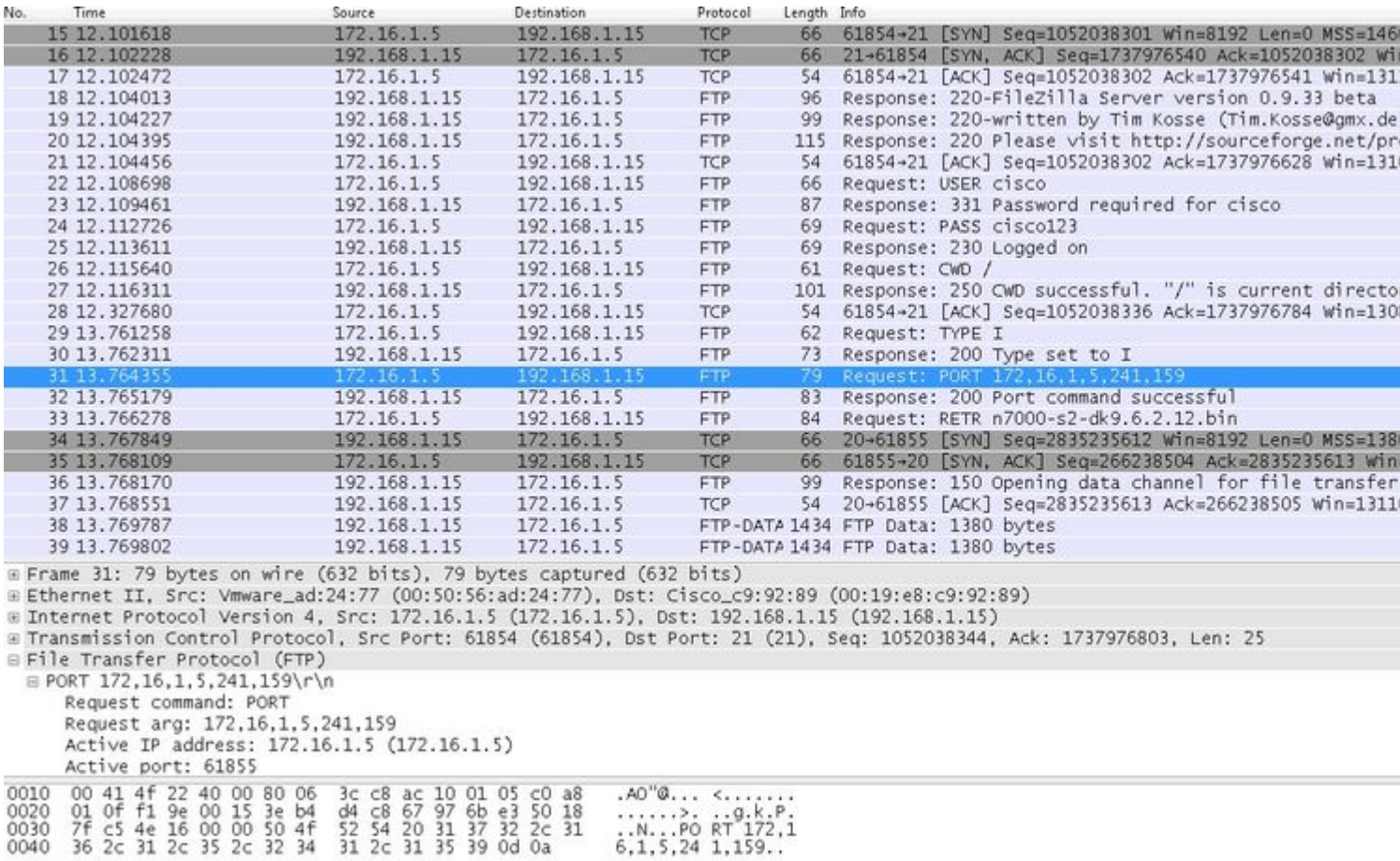
Conexión

<#root>

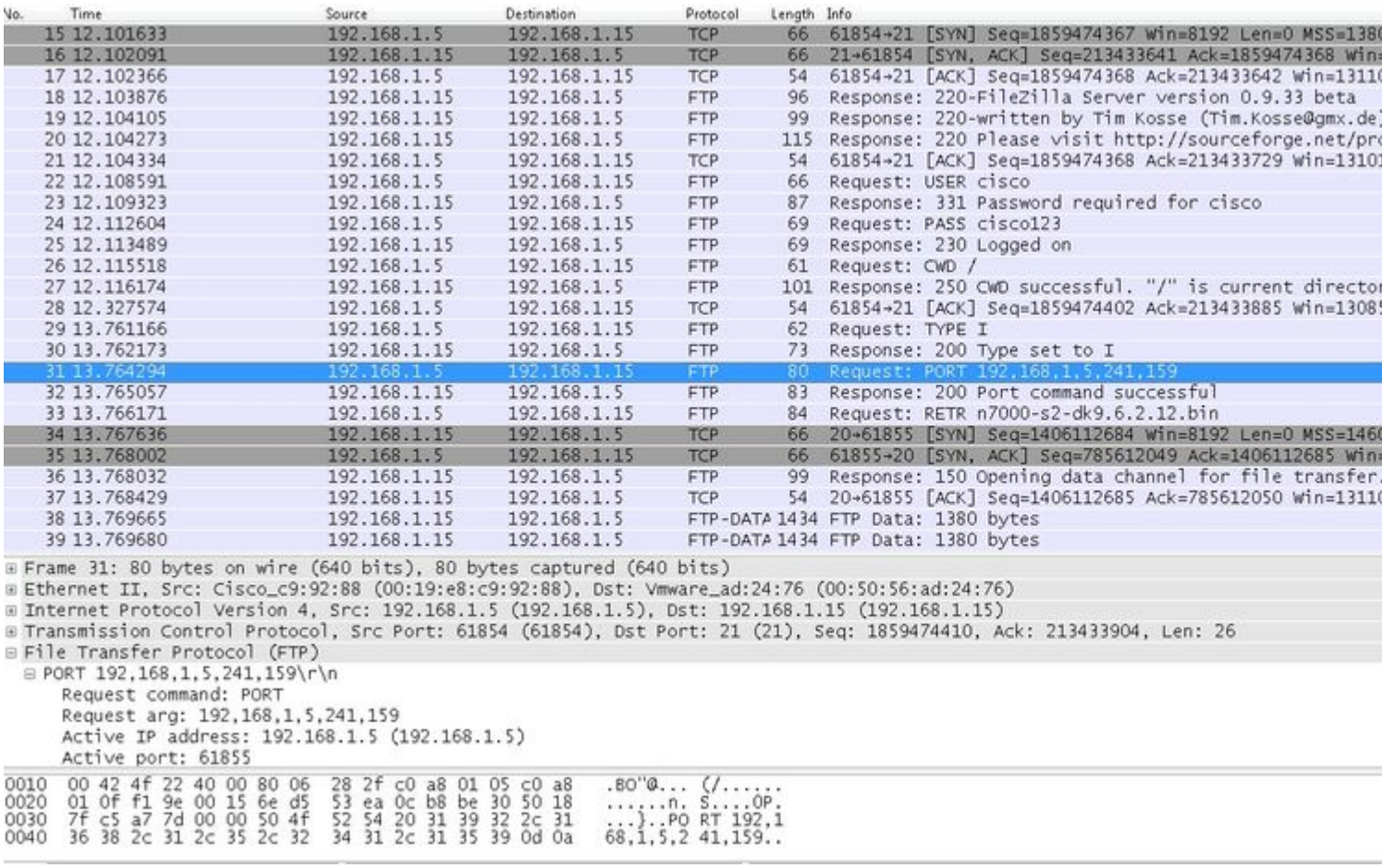
```
 Client in Inside Network running ACTIVE FTP:



 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.



Capture Outside Interface como se muestra en esta imagen.



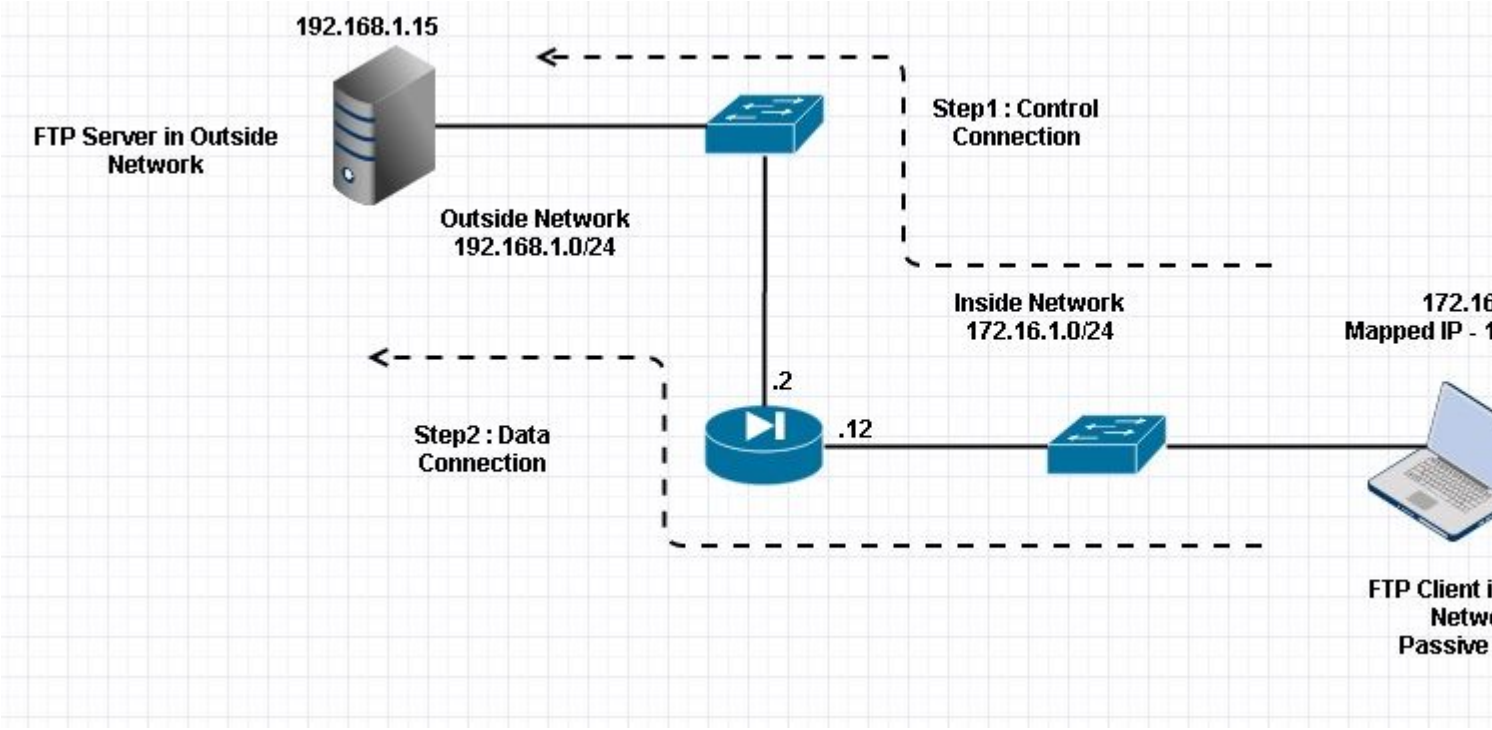
El valor del puerto se calcula utilizando los dos últimos puntos de seis. Izquierda 4 tuplas son dirección IP y 2 tuplas son para puerto. Como se muestra en esta imagen, la dirección IP es 192.168.1.5 y 241*256 + 159 = 61855.

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.

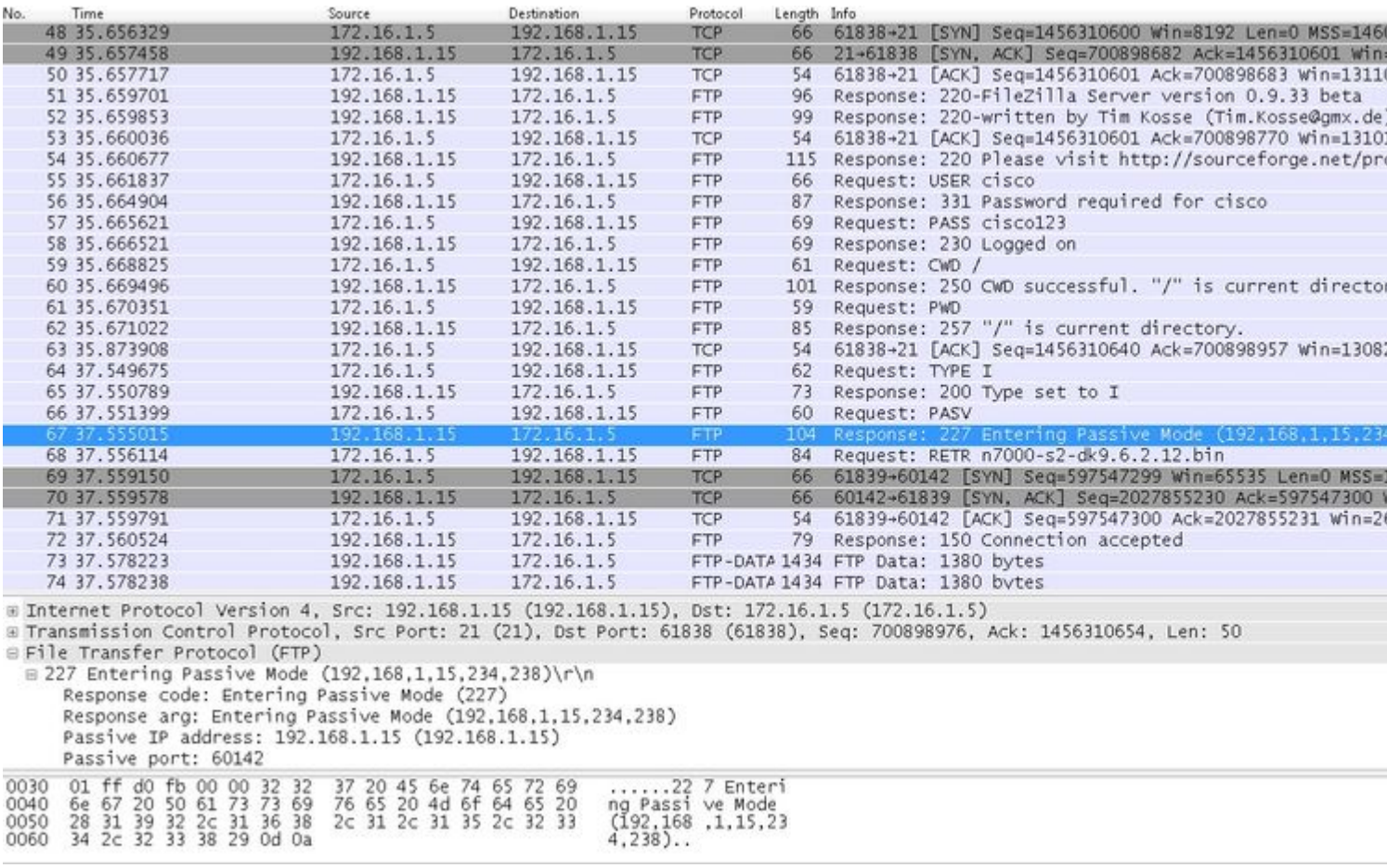
TCP Outside

192.168.1.15:21 inside 172.16.1.5:61838

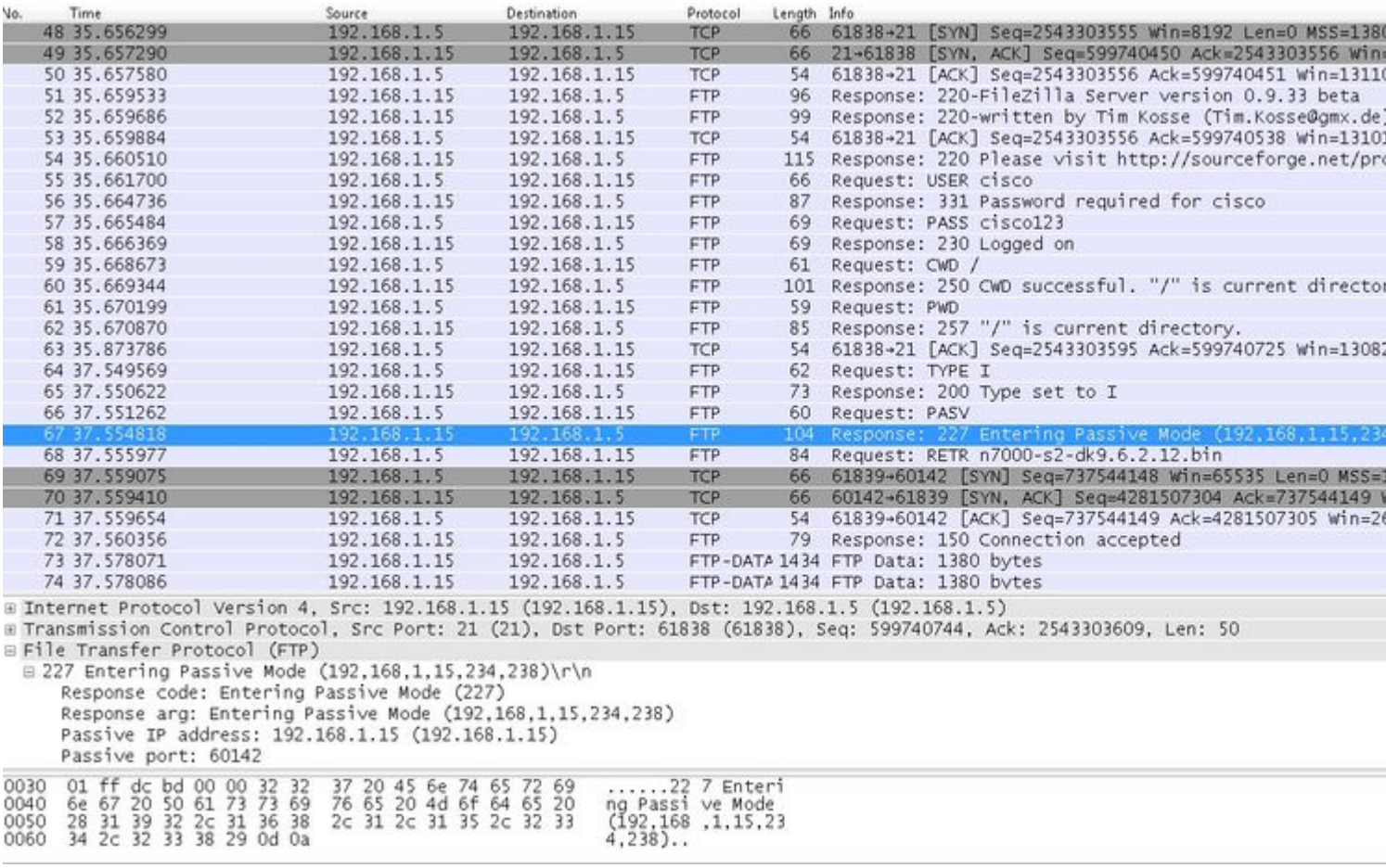
, idle 0:00:00, bytes 451, flags UIO

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.



Capture Outside Interface como se muestra en esta imagen.



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.

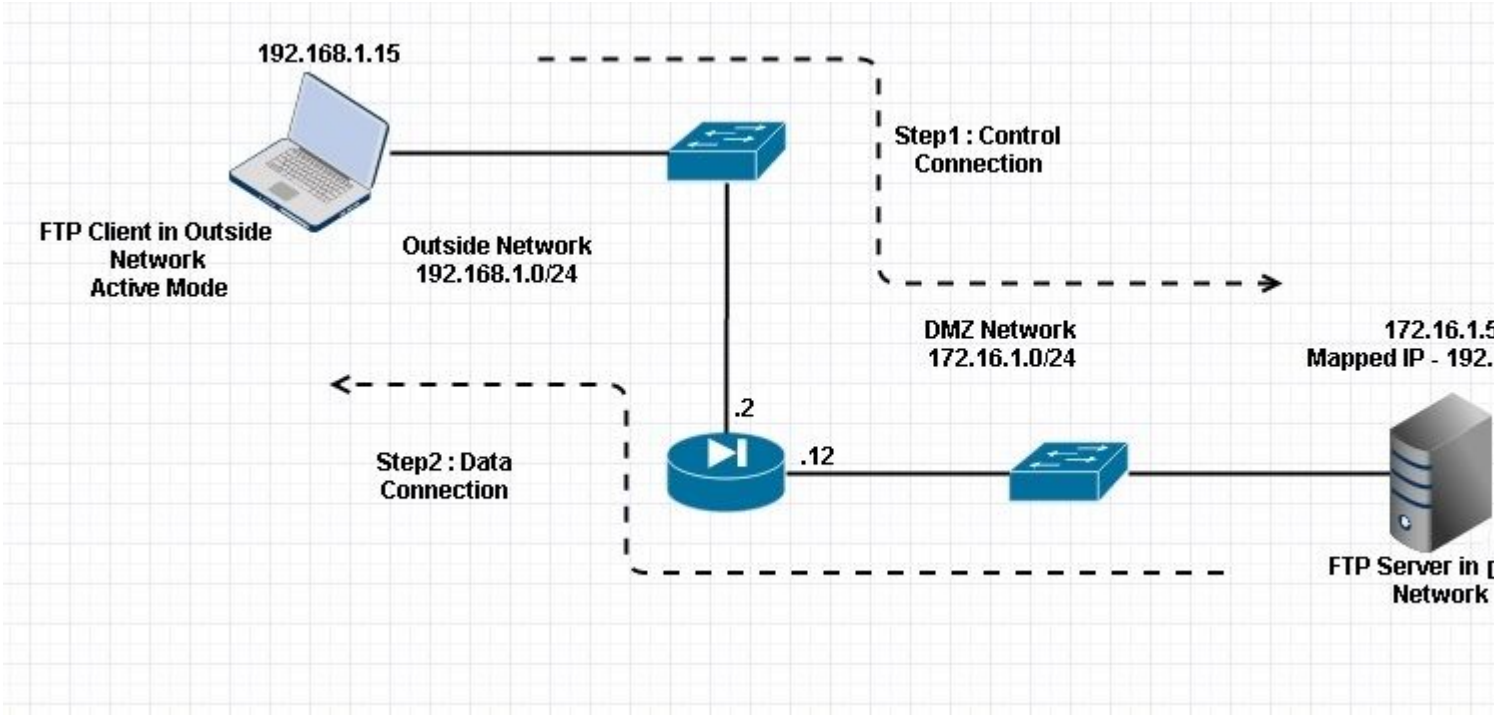
La inspección FTP se puede inhabilitar con el comando **no fixup protocol ftp 21** en el modo de terminal de configuración.

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,

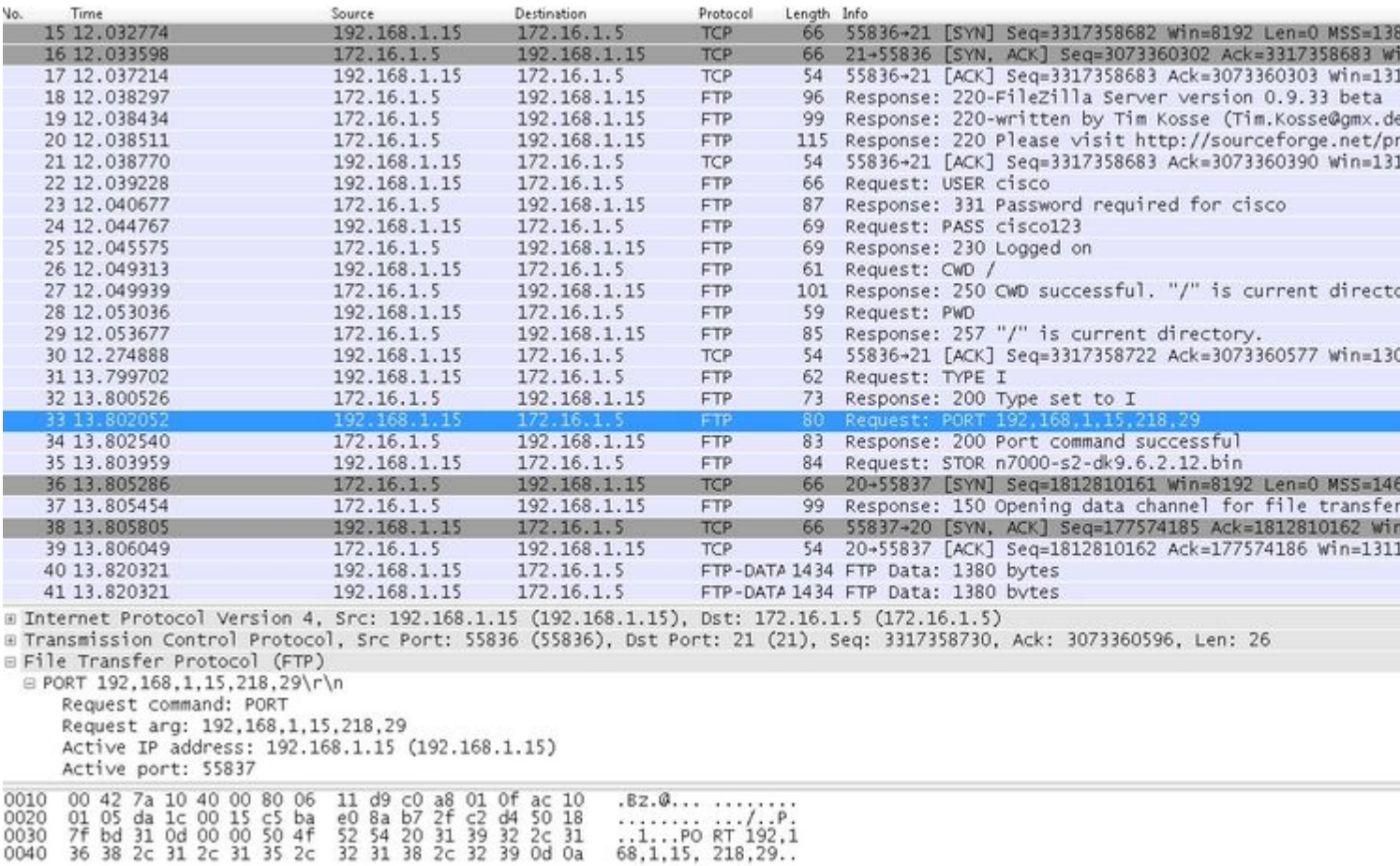
```
 idle 0:00:00, bytes 470, flags UIOB
```

TCP outside 192.168.1.15:55837 DMZ 172.16.1.5:20,

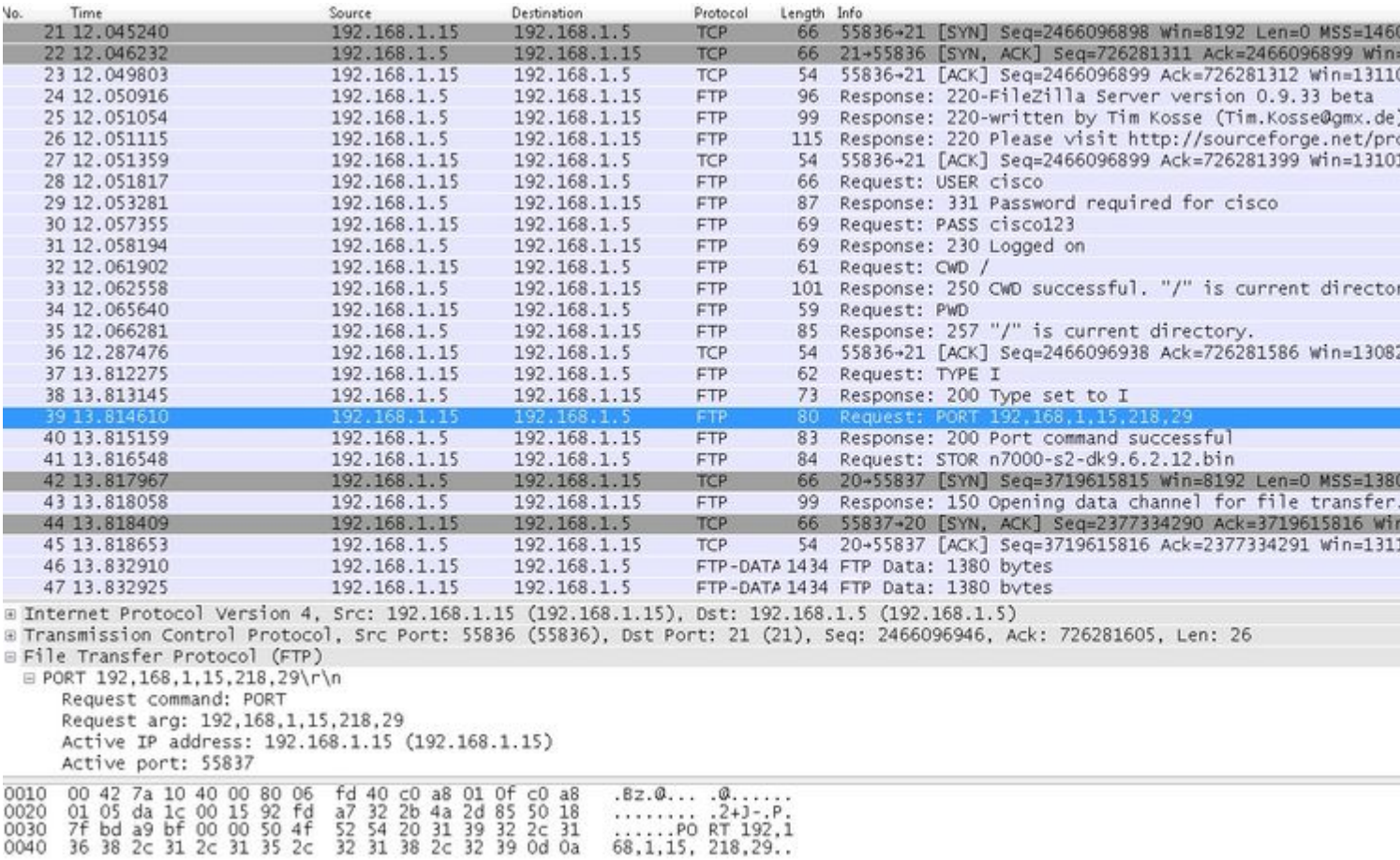
```
idle 0:00:00, bytes 225595694, flags UI
```

<--- Dynamic Port channel

Capture la interfaz DMZ como se muestra en esta imagen.



Capture Outside Interface como se muestra en esta imagen.

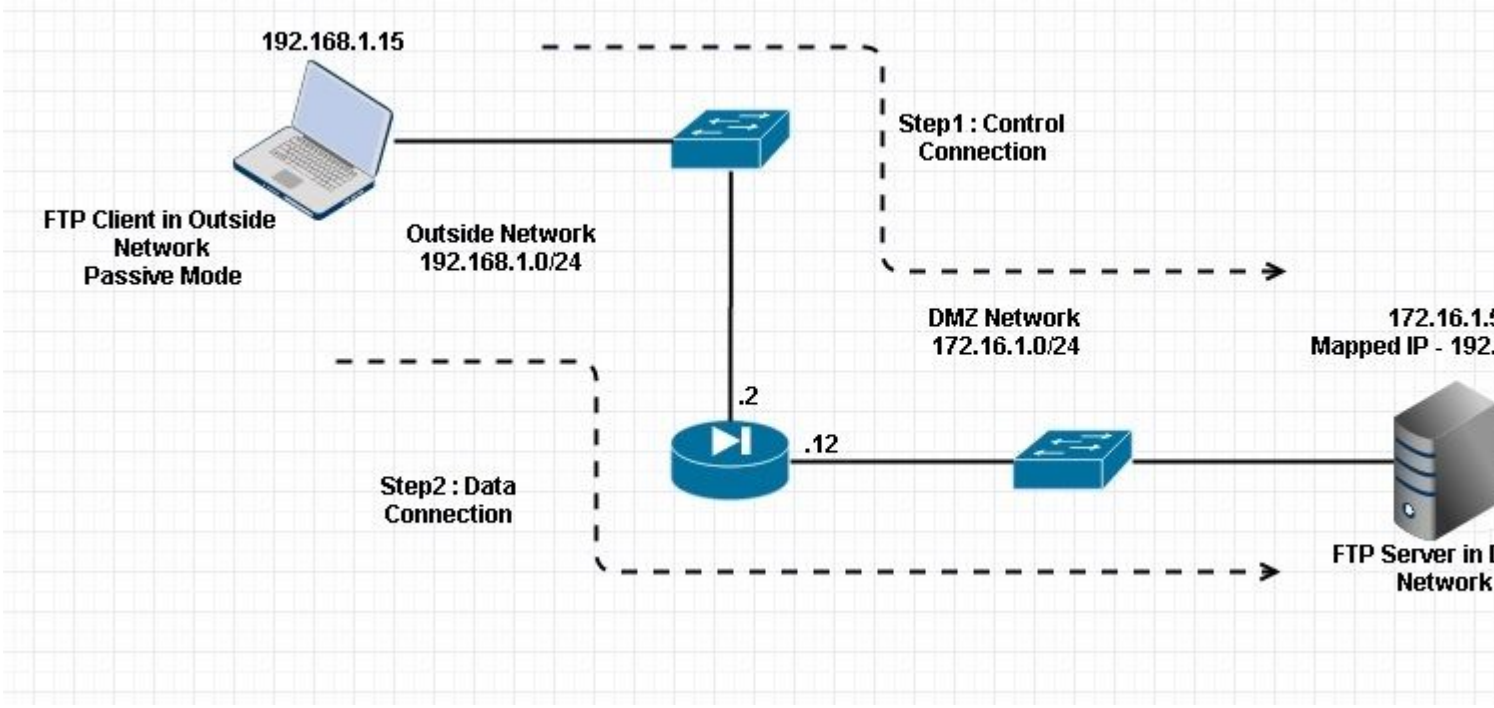


Aquí, el cliente ejecuta el cliente de modo activo 192.168.1.15 e inicia la conexión con el servidor en DMZ en el puerto 21. A continuación, el cliente envía el comando **port** con un valor de seis tuplas al servidor para conectarse a ese puerto dinámico específico. El servidor inicia la conexión de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

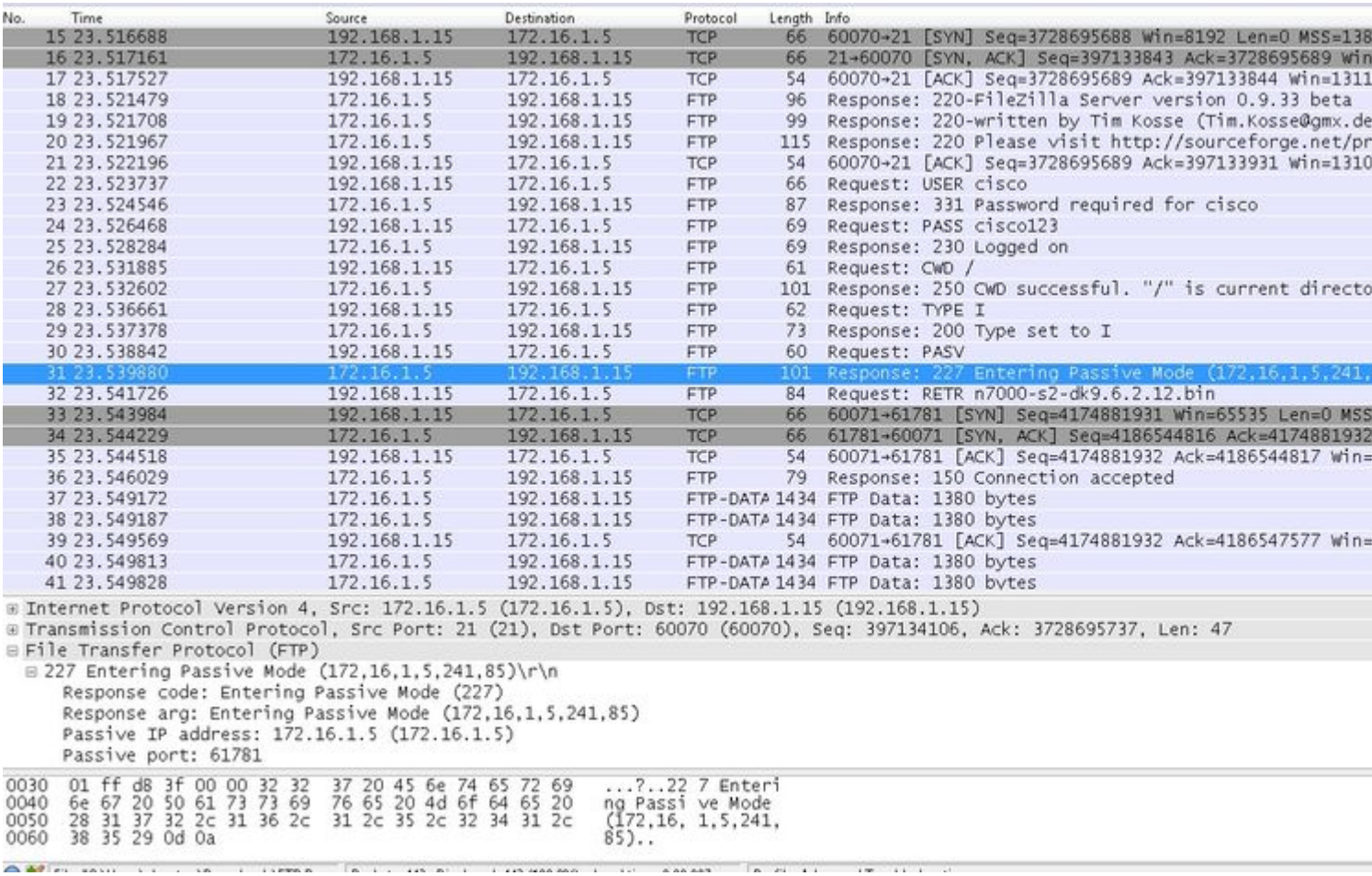
<--- Dynamic channel Open

```
TCP
```

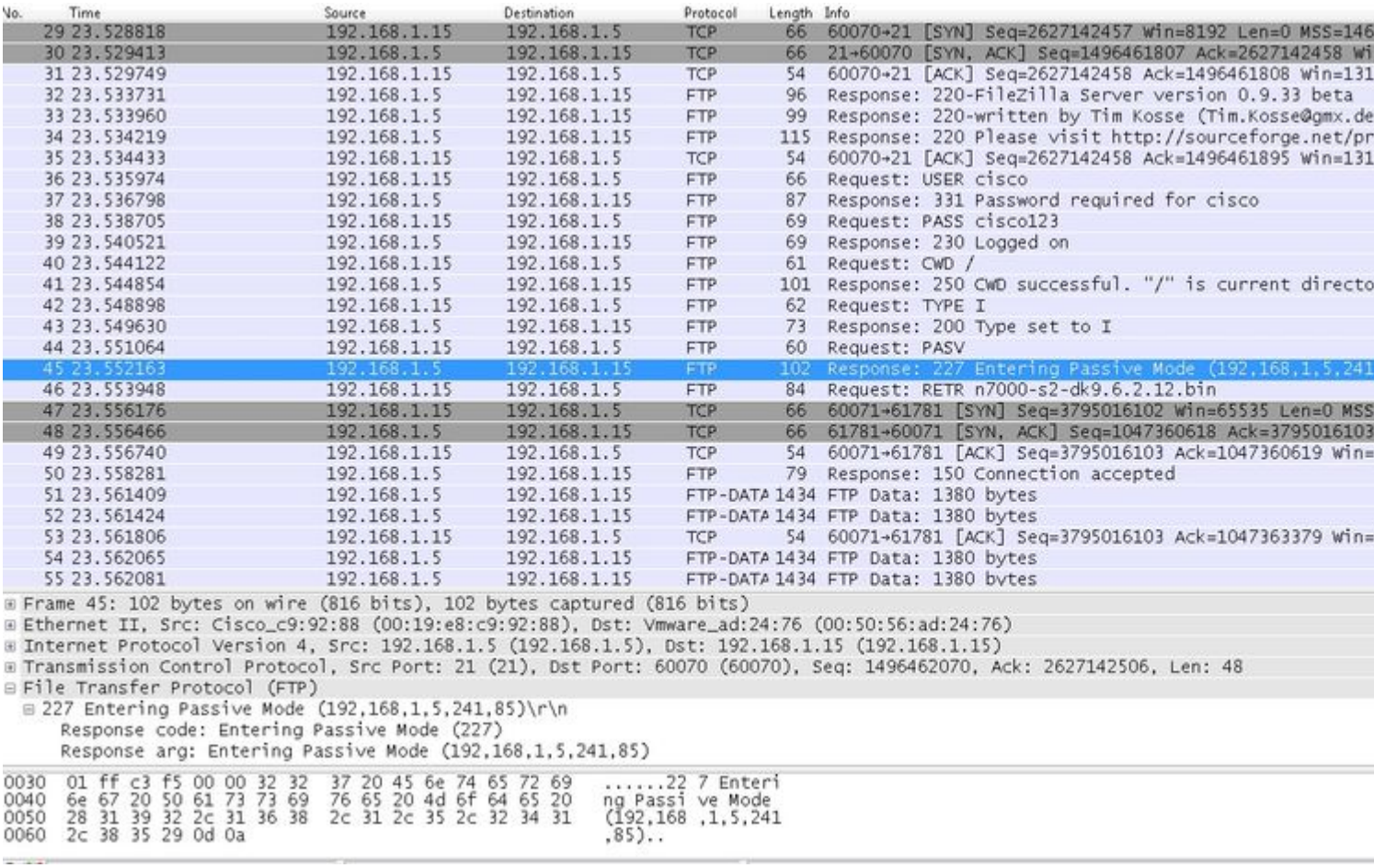
Outside 192.168.1.15:60070 DMZ 172.16.1.5:21

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

Capture la interfaz DMZ como se muestra en esta imagen.



Capture Outside Interface como se muestra en esta imagen.



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
```

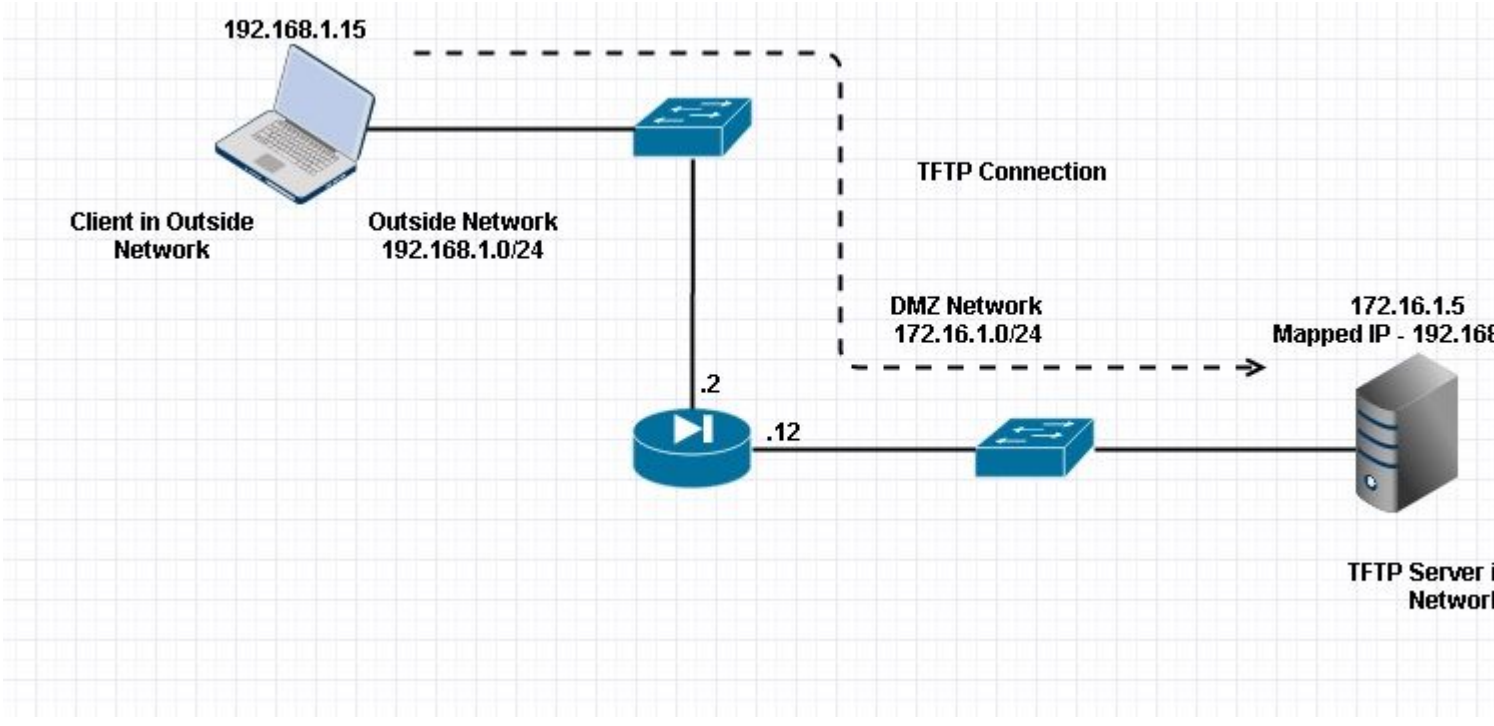
2. Ejecute el comando **class inspection_default**.

```
<#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

Cliente 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

Cliente 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).