配置FTP/TFTP服务：ASA 9.X

目录

简介

本文档介绍ASA上的不同FTP和TFTP检测场景、ASA FTP/TFTP检测配置和基本故障排除。

先决条件

要求

建议掌握下列主题的相关知识：

- 所需接口之间的基本通信

- 位于DMZ网络中的FTP服务器的配置

使用的组件

本文档介绍自适应安全设备(ASA)上的不同FTP和TFTP检测场景，还介绍ASA FTP/TFTP检测配置和基本故障排除。

本文档中的信息基于以下软件和硬件版本：

- 运行9.1(5)软件映像的ASA 5500或ASA 5500-X系列ASA
- 任何FTP服务器
- 任何FTP客户端

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

安全设备支持通过自适应安全算法功能进行应用程序检查。

通过自适应安全算法所使用的状态应用程序检查，安全设备可跟踪穿过防火墙的每个连接，并确保这些连接有效。

防火墙也通过状态检查来监控连接的状态，以便编译信息并放入状态表中。

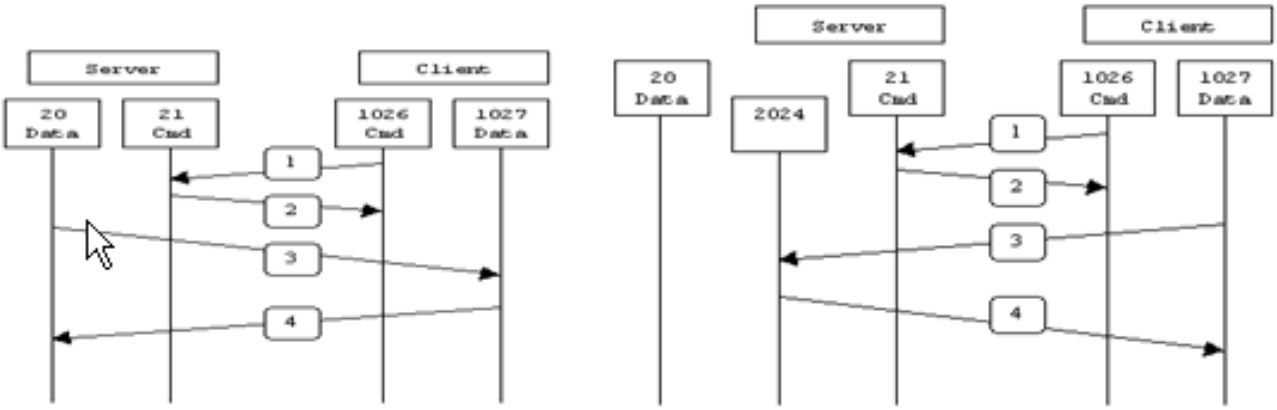
如果使用除了管理员定义的规则之外还使用状态表，则过滤决策将基于先前穿过防火墙的数据包所建立的上下文。

实施应用程序检查包括下列操作：

- 识别流量
- 对流量应用检测
- 在接口上激活检测

如图所示，FTP有两种形式。

- 主动模式
- 被动模式



Active FTP

Passive FTP

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

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

主动式 FTP

在主动 FTP 模式下，客户端从一个随机的非特权端口 N (N>1023) 连接到 FTP 服务器的命令端口 (21)。然后，客户端开始侦听端口N>1023，并将FTP命令port N>1023发送到FTP服务器。接下来，服务器从其本地数据端口（端口 20）连接回客户端的指定数据端口。

被动式 FTP

在被动 FTP 模式下，客户端向服务器同时发起这两种连接，这将解决从服务器到客户端的数据端口传入连接被防火墙过滤掉的问题。打开FTP连接时，客户端会在本地打开两个随机非特权端口。第一个端口联系服务器的端口 21。但是，客户端不会运行port命令并允许服务器连接回其数据端口，而是发出PASV命令。这样做的结果是服务器会打开一个随机的非特权端口 P (P>1023)，并将 port P 命令发送回客户端。然后，客户端发起从端口N>1023到服务器端口P的连接以传输数据。如果安全设备上未配置 inspection 命令，内部用户发起的出站 FTP 只能以被动方式工作。此外，外部用户发起的访问 FTP 服务器的入站请求将被拒绝。

TFTP

如 RFC 1350 中所述，TFTP 是一种用于在 TFTP 服务器与客户端之间读写文件的简单协议。TFTP 使用 UDP 端口 69。

高级协议处理

为什么需要FTP检测？

某些应用程序要求由 Cisco 安全设备应用程序检查功能进行的特殊处理。此类应用程序通常将 IP 编址信息嵌入在用户数据包中，或者在动态分配的端口上打开辅助信道。应用检测功能与网络地址转换(NAT)配合使用，以帮助识别嵌入式编址信息的位置。

除了识别嵌入式编址信息外，应用检测功能还监控会话，以确定辅助信道的端口号。许多协议会打开辅助 TCP 或 UDP 端口以提高性能。某个已知端口上的初始会话用于协商动态分配的端口号。

应用程序检查功能监控这些会话、标识动态端口分配，并允许在特定会话持续时间内通过这些端口进行数据交换。多媒体和 FTP 应用程序展示了这种行为。

如果安全设备上未启用FTP检查，则会丢弃此请求，并且FTP会话不会传输任何请求的数据。

如果在ASA上启用FTP检查，则ASA监控控制信道并尝试识别打开数据信道的请求。FTP 协议将数据信道端口规范嵌入在控制信道流量中，并要求安全设备检查控制信道中是否进行了数据端口更改。

一旦ASA识别到请求，它会临时为会话期间持续的数据通道流量创建一个开口。通过这种方式，FTP 检查功能可监控控制信道、标识数据端口分配，并允许在会话持续时间内通过数据端口交换数据。

默认情况下，ASA通过global-inspection class-map检查FTP流量的端口21连接。安全设备还能识别出主动 FTP 会话与被动 FTP 会话之间的差别。

如果FTP会话支持被动FTP数据传输，则ASA通过inspect ftp命令识别来自用户的数据端口请求，并打开一个大于1023的新数据端口。

inspect ftp命令检测检查FTP会话并执行四项任务：

- 准备动态辅助数据连接
- 跟踪 FTP 命令响应顺序
- 生成审计线索
- 使用 NAT 转换嵌入式 IP 地址

FTP 应用程序检查准备辅助信道以进行 FTP 数据传输。响应文件上载、文件下载或目录列表事件时会分配信道，但必须预先协商这些信道。可通过 PORT 或 PASV (227) 命令协商端口。

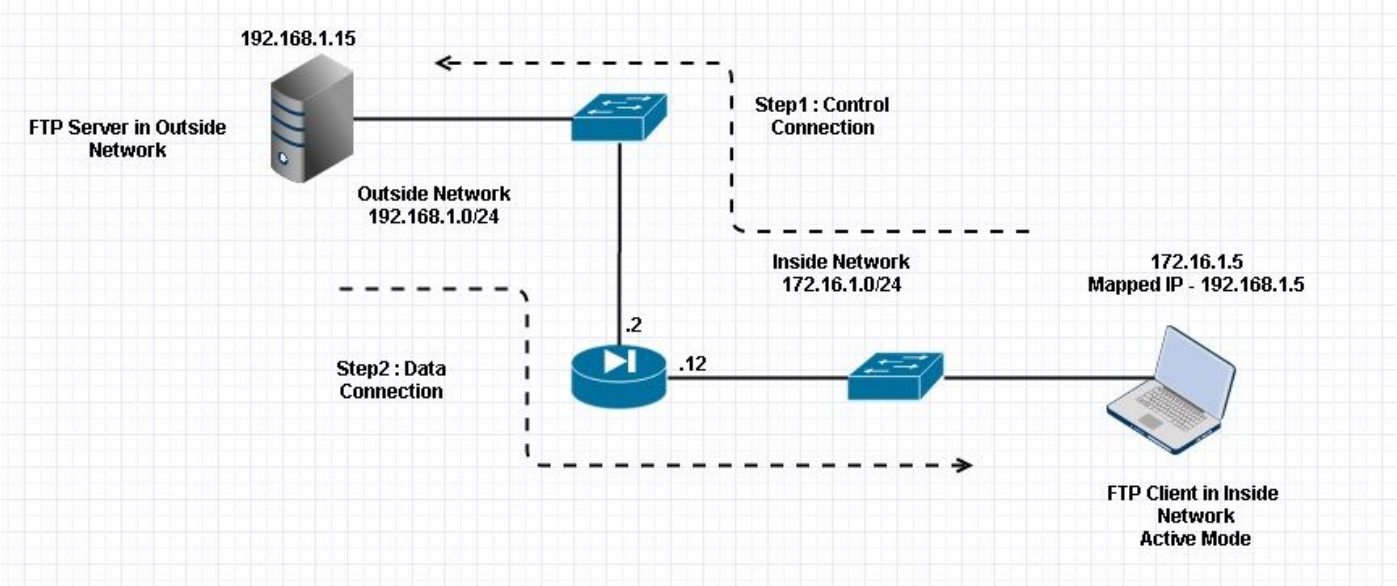
配置

注意：在ASA上启用FTP检测后，将解释所有网络场景。

场景 1.为活动模式配置的FTP客户端

连接到ASA内部网络的客户端和外部网络中的服务器。

网络图



注意：此配置中使用的IP编址方案在Internet上不能合法路由。

如本图所示，使用的网络设置在IP为172.16.1.5的内部网络中具有客户端的ASA。服务器位于IP为192.168.1.15的外部网络中。客户端在外部网络中有映射IP 192.168.1.5。

由于FTP检测会打开动态端口通道，因此无需允许外部接口上的任何访问列表。

配置示例：

<#root>

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

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


 !--- Output is suppressed.


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


object network obj-172.16.1.5
 subnet 172.16.1.0 255.255.255.0




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



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

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


policy-map global_policy



class inspection_default

  inspect dns preset_dns_map


inspect ftp


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

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


service-policy global_policy global

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

验证

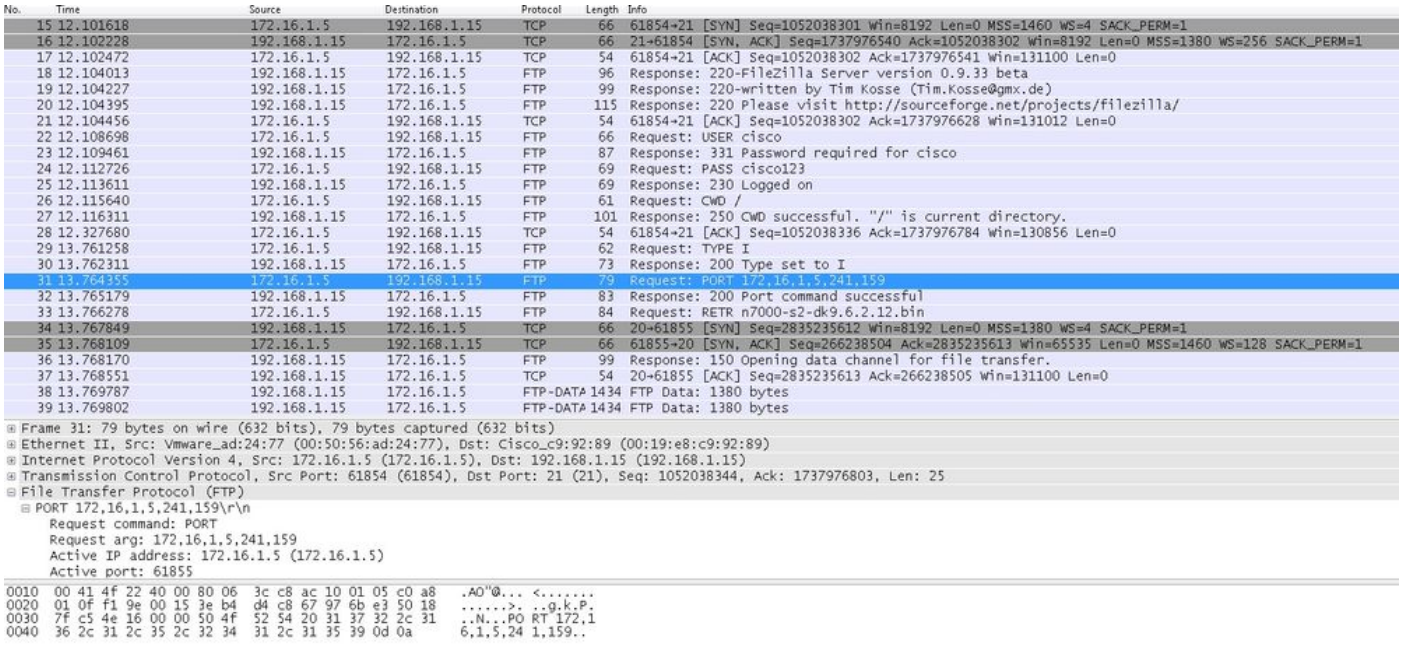
连接

<#root>

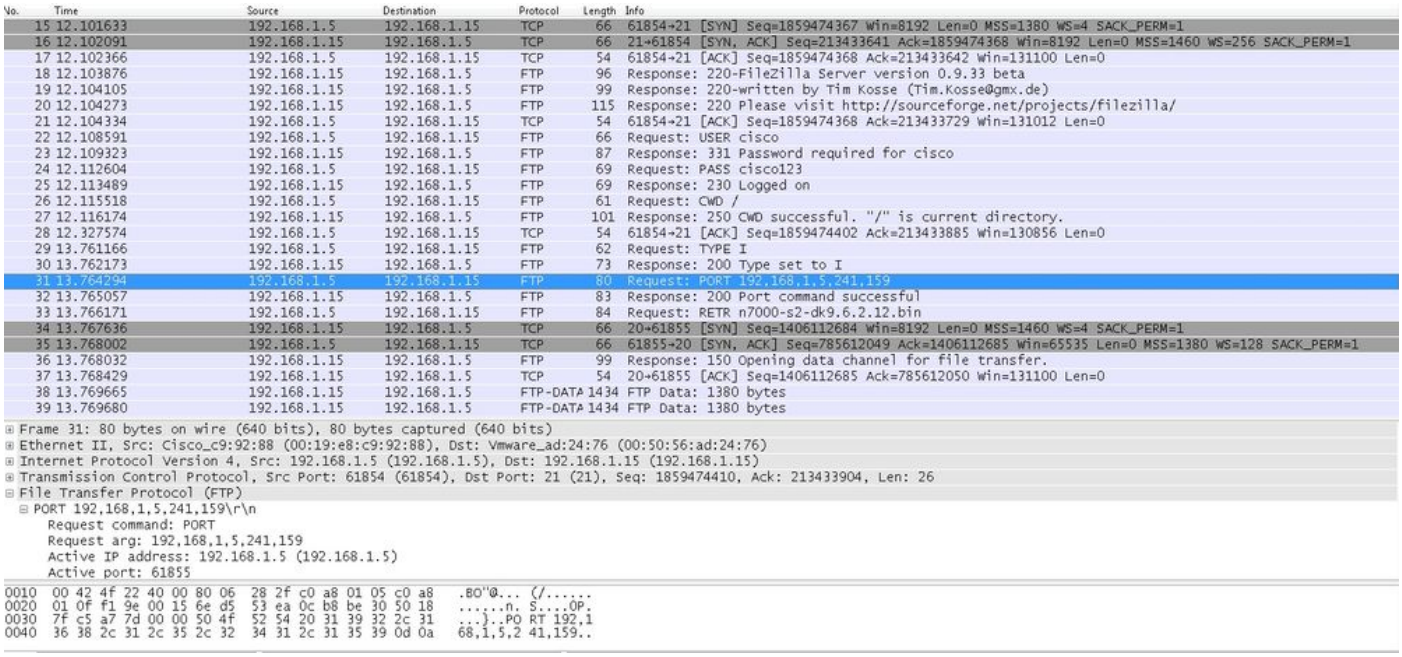
```
 Client in Inside Network running ACTIVE FTP:



 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
```

这里，Inside中的客户端启动与源端口61854到目标端口21的连接。然后，客户端发送带有6元组值的Port命令。然后，服务器启动辅助/数据连接，源端口为20，目标端口则按照这些捕获后提到的步骤进行计算。

捕获内部接口，如图所示。



捕获外部接口，如图所示。



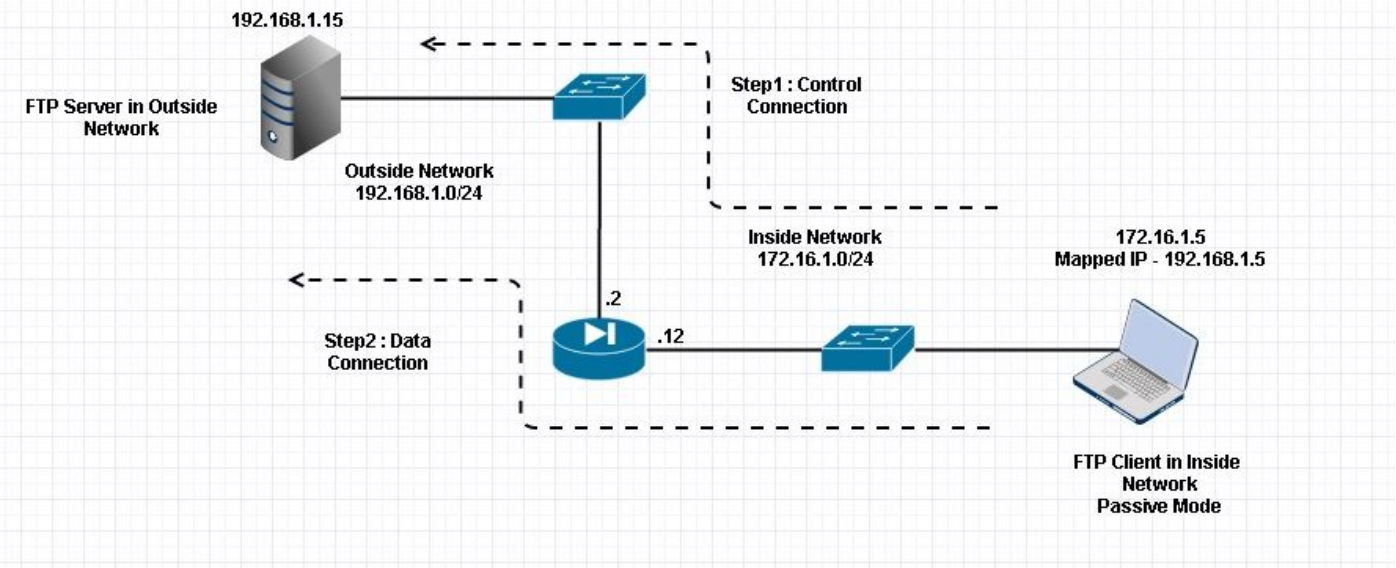
端口值使用最后两个输出进行计算（共六个）。剩下的4个元组是IP地址，2个元组是端口。如图所示，IP地址为192.168.1.5和241*256 + 159 = 61855。

捕获还显示，启用FTP检测时，端口命令的值会更改。Inside Interface Capture显示IP的实际值，而Client为服务器发送的端口为数据通道连接到客户端，Outside Interface Capture显示映射地址。

场景 2：配置为被动模式的FTP客户端

ASA内部网络中的客户端和外部网络中的服务器。

网络图



连接

<#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.

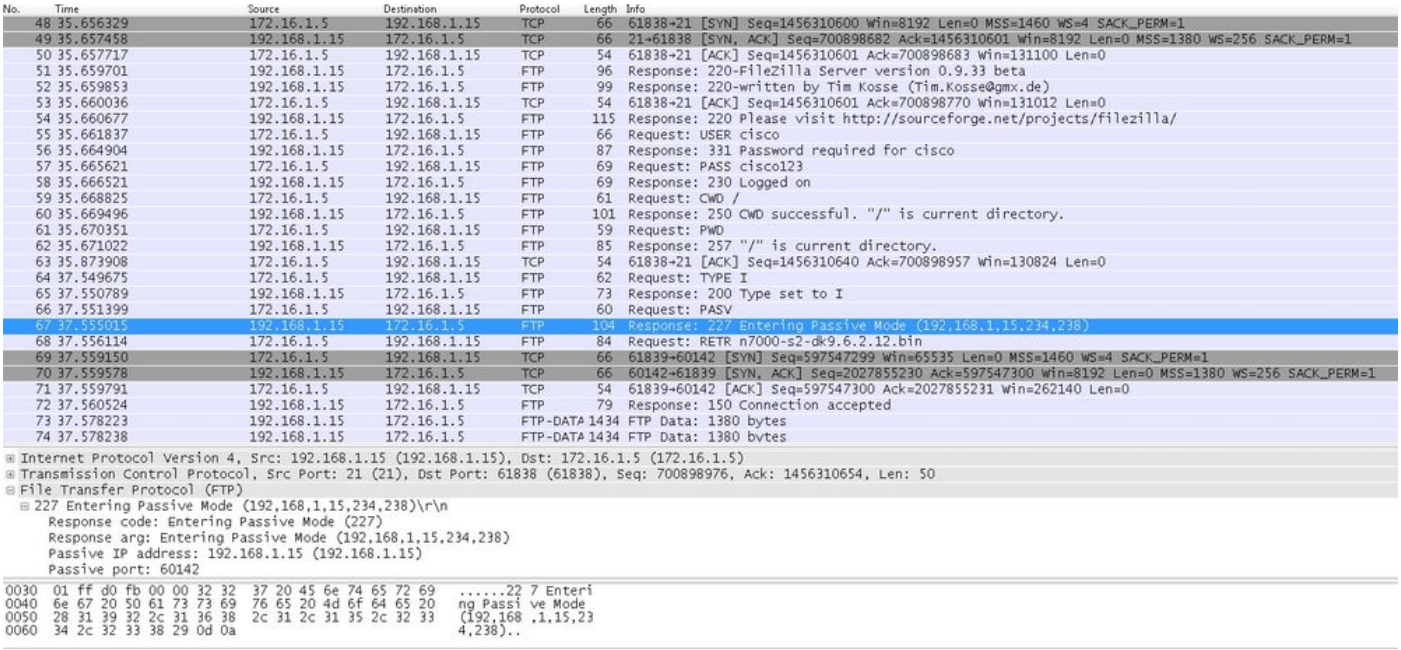
TCP Outside

192.168.1.15:21 inside 172.16.1.5:61838

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

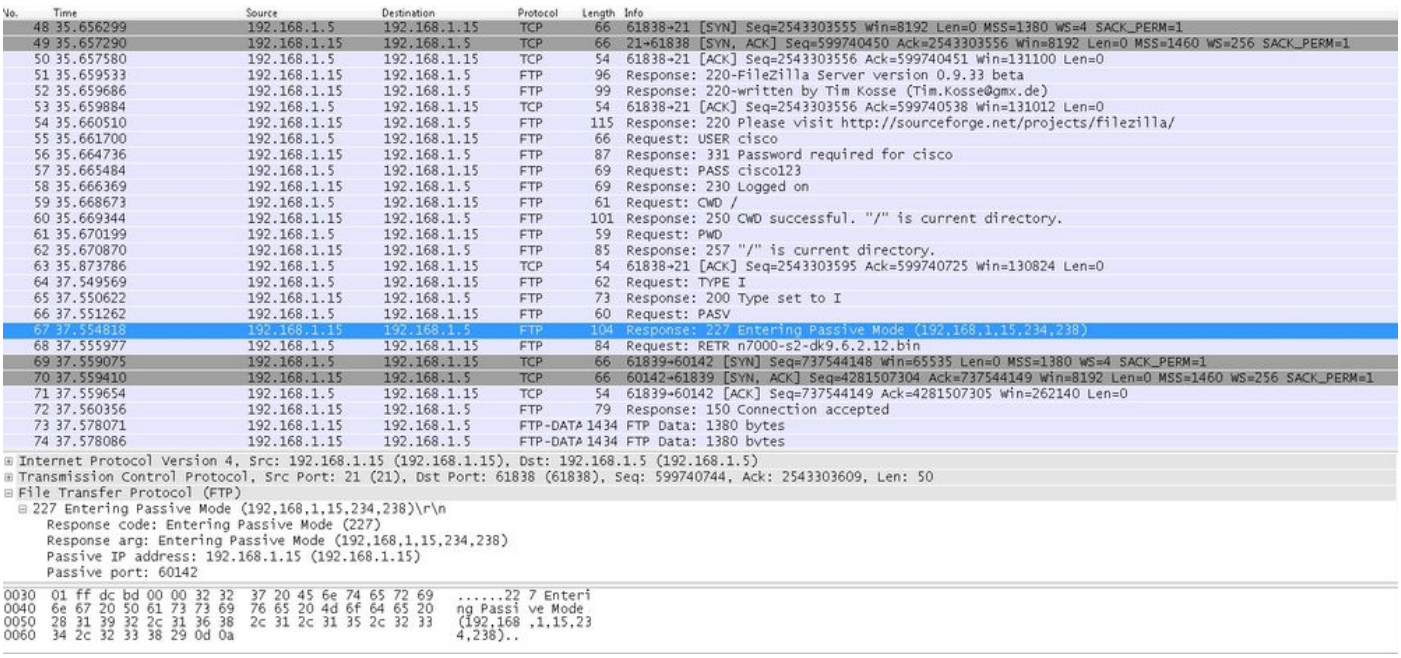
这里，内部客户端发起与源端口和61838标端口21的连接。由于它是被动FTP，客户端发起两个连接。因此，在客户端发送PASV命令后，服务器会回复其6元组值，并且客户端会连接到该套接字以进行数据连接。

捕获内部接口，如图所示。



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

捕获外部接口，如图所示。



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

端口的计算方法保持不变。

如前所述，如果启用了FTP检测，则ASA会重写嵌入式IP值。此外，它还会为数据连接打开动态端口通道。

以下是连接详细信息，如果 FTP检测已禁用

连接:

<#root>

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

```
 TCP Outside
192.168.1.15:21 inside 172.16.1.5:61878
, idle 0:00:09, bytes 433, flags UIO
 TCP Outside
192.168.1.15:21 inside 172.16.1.5:61875
, idle 0:00:29, bytes 259, flags UIO
```

如果没有FTP检测，它只尝试一次又一次发送port命令，但是没有应答，因为外部接收的PORT带有原始IP而不是NAT一个。转储中显示了同样的信息。

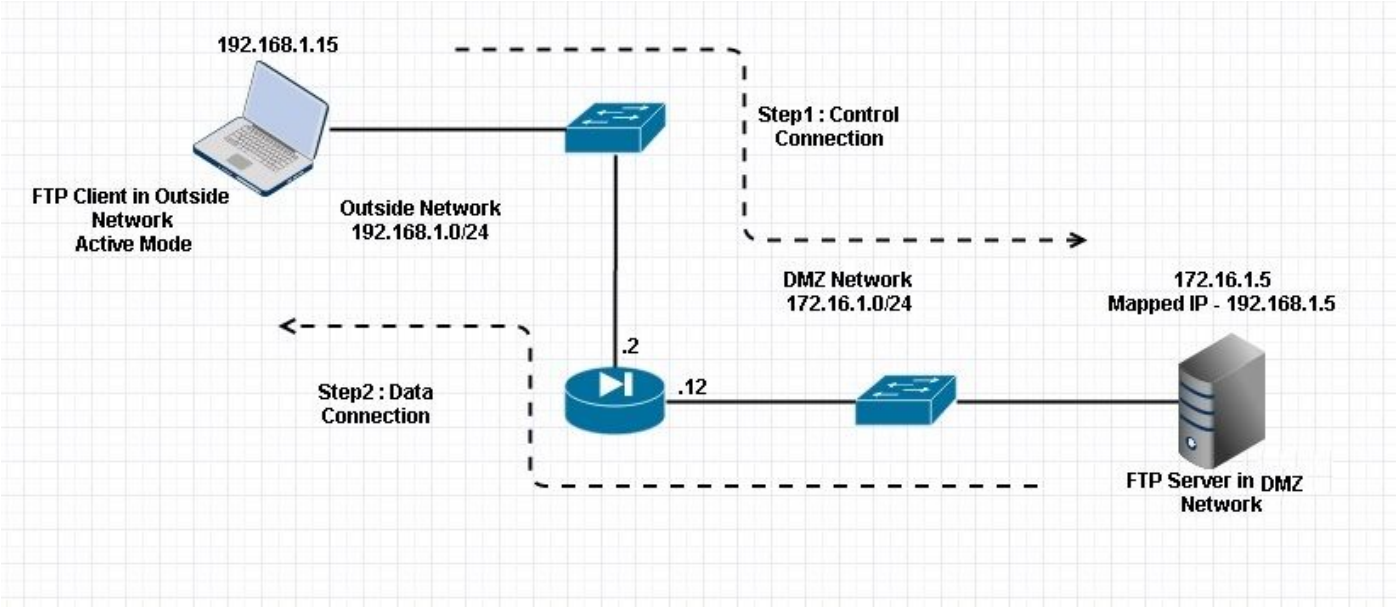
在配置终端模式下，可使用no fixup protocol ftp 21命令禁用FTP检查。

如果没有FTP检测，当客户端位于Inside时，只有PASV命令起作用，因为没有port命令来自Inside，需要嵌入该命令，并且两个连接都是从Inside发起的。

场景 3：为活动模式配置的FTP客户端

ASA外部网络中的客户端和DMZ网络中的服务器。

网络图



配置:

<#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)#
```

验证

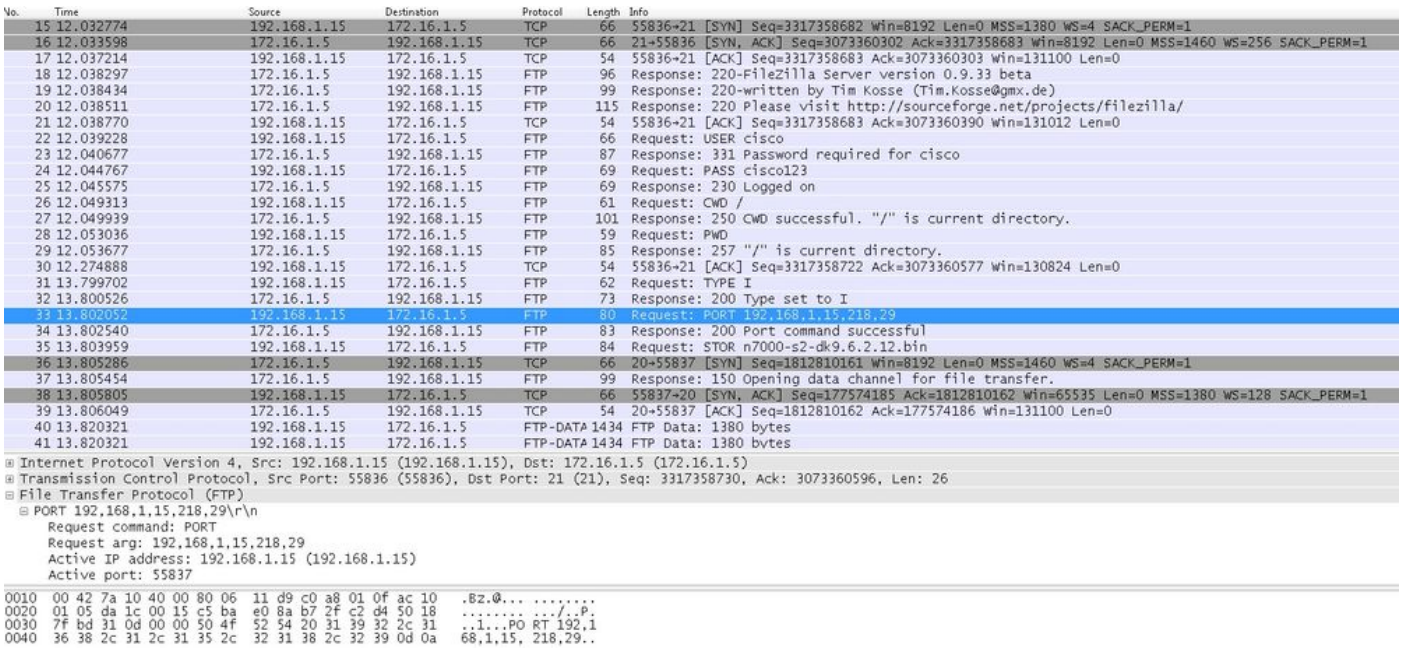
连接:

<#root>

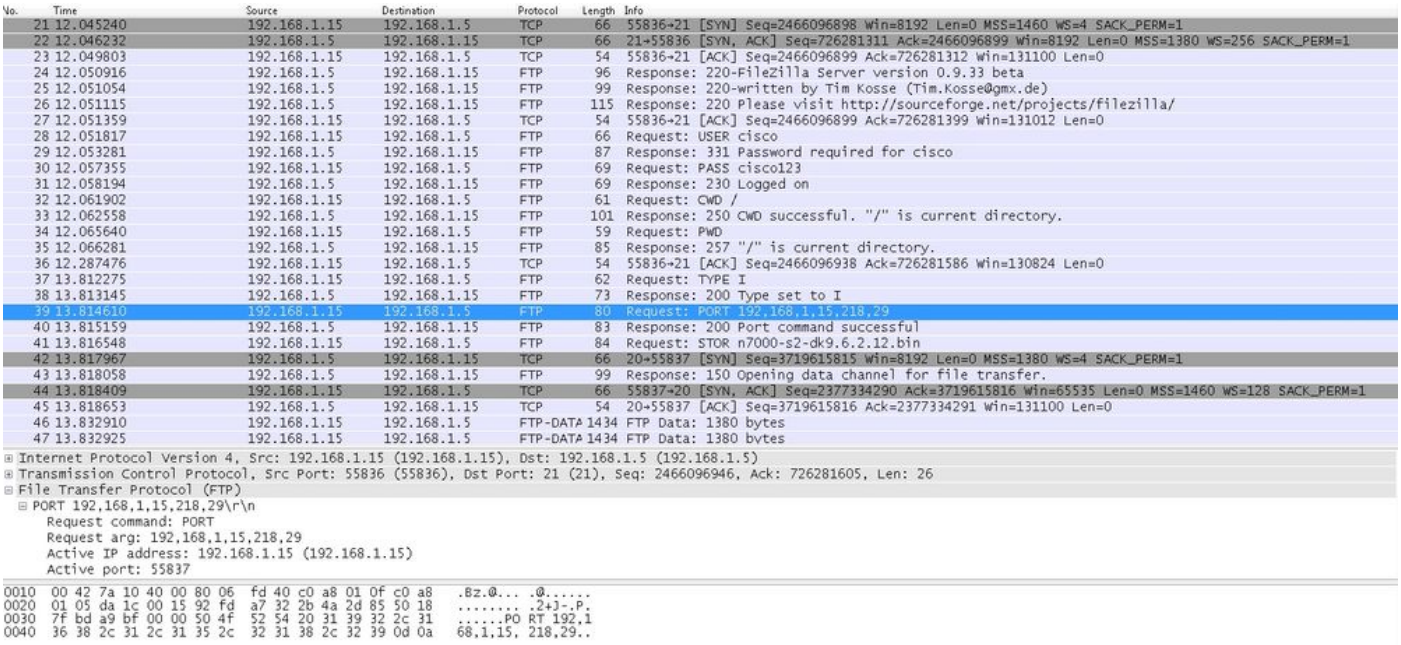
Client in Outside Network running in Active Mode FTP:

```
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
```

捕获DMZ接口（如图所示）。



捕获外部接口，如图所示。

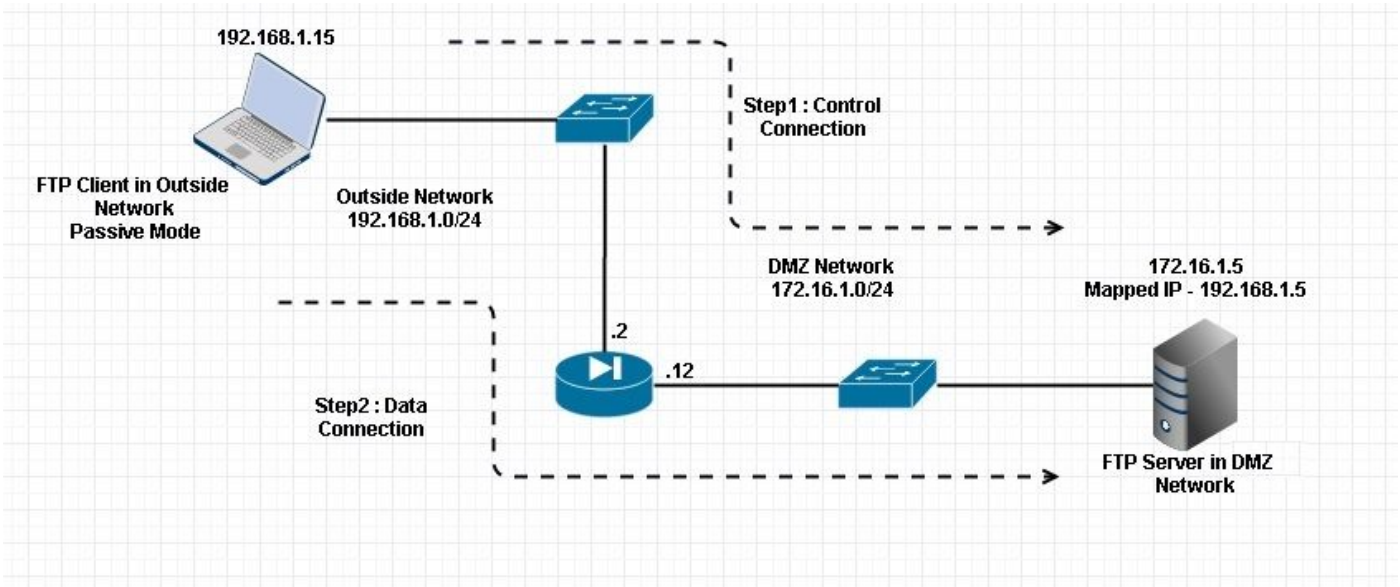


此时，客户端运行活动模式客户端192.168.1.15，并在端口21上发起到DMZ中服务器的连接。然后，客户端向服务器发送port命令（带有六个元组值）以连接到该特定动态端口。然后，服务器启动源端口为20的数据连接。

场景 4.运行被动模式的FTP客户端

ASA外部网络中的客户端和DMZ网络中的服务器。

网络图



连接

<#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
```

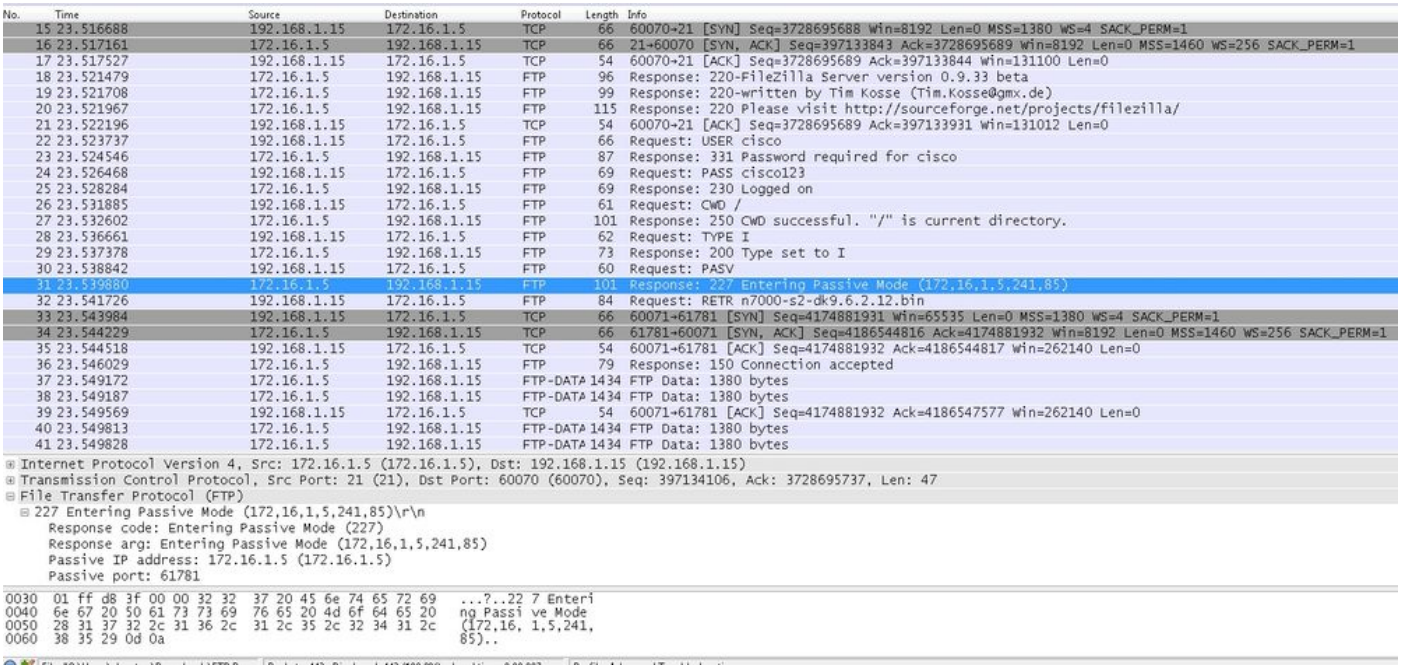
<--- Dynamic channel Open

```
 TCP
```

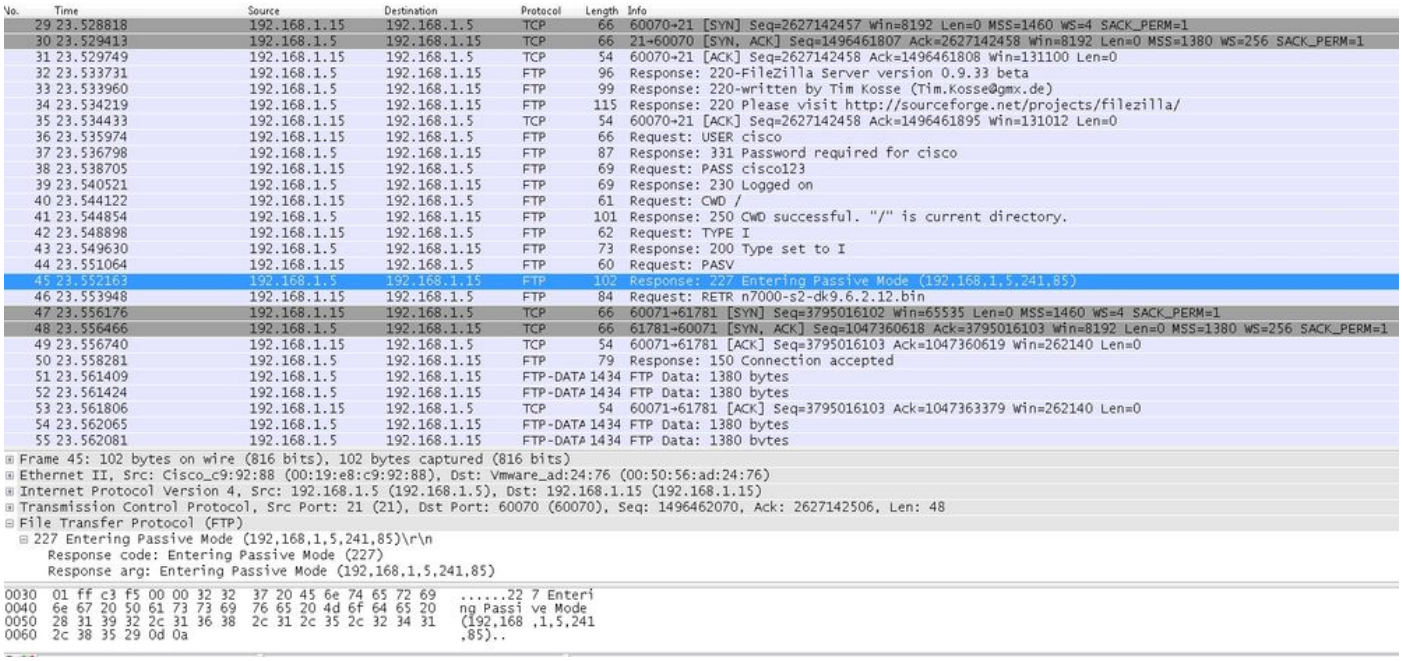
Outside 192.168.1.15:60070 DMZ 172.16.1.5:21

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

捕获DMZ接口（如图所示）。



捕获外部接口，如图所示。



配置基本的 FTP 应用程序检查

默认情况下，配置中包括一个与所有的默认应用程序检查流量匹配且对所有接口上的流量应用检查的策略（全局策略）。默认应用程序检查流量包括到每个协议的默认端口的流量。

只能应用一个全局策略。因此，如果要改变全局策略（例如，对非标准端口应用检查，或者添加默认情况下未启用的检查），则需要编辑默认策略，或者禁用默认策略并应用新的策略。有关所有默认端口的列表，请参阅默认检查策略。

1. 运行policy-map global_policy命令。

```
<#root>

 ASA(config)#

policy-map global_policy
```

2. 运行class inspection_default命令。

```
<#root>

 ASA(config-pmap)#

class inspection_default
```

3. 运行inspect FTP命令。

<#root>

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

4. 可以选择使用 inspect FTP strict 命令。此命令通过阻止 Web 浏览器在 FTP 请求中发送嵌入式命令，提高了受保护网络的安全性。

   在接口上启用 strict 选项后，FTP 检查功能将强制执行以下行为：

   - 必须先确认FTP命令，安全设备才能允许使用新命令
   - 安全设备会丢弃发送嵌入式命令的连接
   - 检查227和PORT命令以确保它们不会出现在错误字符串中

   警告：使用strict选项可能导致不完全符合FTP RFC的FTP客户端出现故障。有关使用 strict 选项的详细信息，请参阅使用 strict 选项。

在非标准 TCP 端口上配置 FTP 协议检查

您可以使用这些配置行，为非标准 TCP 端口配置 FTP 协议检查（请用新端口号替换 XXXX）：

<#root>

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

inspect ftp
```

验证

要确保配置已成功执行，请运行show service-policy命令。此外，通过运行show service-policy inspect ftp命令将输出限制为FTP检查。

<#root>

```
 ASA#
```

```
show service-policy inspect ftp

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

TFTP

默认情况下 TFTP 检查功能已启用。

安全设备检查 TFTP 流量并动态地创建连接和转换（如果需要），以便允许在 TFTP 客户端与服务器之间传输文件。具体而言，检查引擎会检查 TFTP 读请求 (RRQ)、写请求 (WRQ) 和错误通知 (ERROR)。

在收到有效的 RRQ 或 WRQ 时会分配动态辅助信道和 PAT 转换（如果需要）。随后，TFTP 使用此辅助信道进行文件传输或错误通知。

只有 TFTP 服务器才能通过辅助信道发起流量，并且 TFTP 客户端与服务器之间最多只能存在一个不完整的辅助信道。服务器发出的错误通知会关闭辅助信道。

如果使用fstatic PAT重定向TFTP流量，则必须启用TFTP检查。

配置基本的 TFTP 应用程序检查

默认情况下，配置中包括一个与所有的默认应用程序检查流量匹配且对所有接口上的流量应用检查的策略（全局策略）。默认应用程序检查流量包括到每个协议的默认端口的流量。

只能应用一个全局策略。因此，如果要改变全局策略（例如，对非标准端口应用检查，或者添加默认情况下未启用的检查），则需要编辑默认策略，或者禁用默认策略并应用新的策略。有关所有默认端口的列表，请参阅默认检查策略。

1. 运行policy-map global_policy命令。

   <#root>

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

2. 运行class inspection_default命令。

   <#root>

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

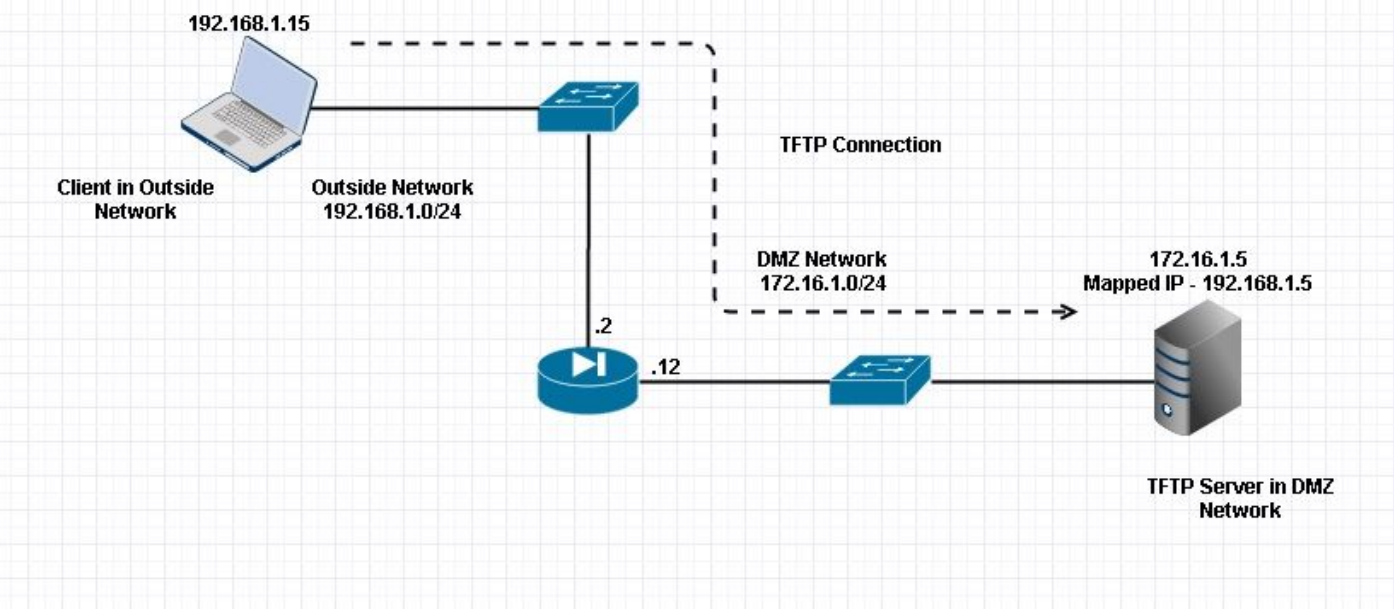
```
class inspection_default
```

3. 运行inspect TFTP命令。

<#root>

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

网络图



此处是在外部网络中配置的客户端。TFTP服务器位于DMZ网络中。服务器映射到位于外部子网中的IP 192.168.1.5。

配置示例：

<#root>

```
 ASA(config)#
show running-config
```

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

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

 !--- Output is suppressed.


 !--- Permit inbound TFTP traffic.


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

!

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


object network obj-172.16.1.5
 host 172.16.1.5


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


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



access-group 100 in interface outside


class-map inspection_default

match default-inspection-traffic

!
```

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

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


inspect tftp


 inspect sip
 inspect xdmcp
!

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

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

验证

要确保配置已成功执行，请运行show service-policy命令。此外，通过运行show service-policy inspect tftp命令将输出限制为TFTP检查。

```
<#root>

 ASA#

show service-policy inspect tftp

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

故障排除

本部分提供了可用于对配置进行故障排除的信息。

packet tracer

内部网络中的客户端

<#root>

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

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

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

Phase: 5
Type: INSPECT

Subtype: inspect-ftp

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

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

object network obj-172.16.1.5

nat (inside,outside) static 192.168.1.5

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

```
 Phase: 7
 Type: NAT
 Subtype: rpf-check

 Result: ALLOW

 Config:

object network obj-172.16.1.5

 nat (inside,outside) static 192.168.1.5

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

 ----Omitted----

 Result:
 input-interface:
inside

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

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

外部网络中的客户端

<#root>

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

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

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

Config:

object network obj-172.16.1.5

nat (DMZ,outside) static 192.168.1.5

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

-----Omitted-----

Phase: 4
Type: INSPECT
Subtype:

inspect-ftp

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

Phase: 5
Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

object network obj-172.16.1.5

```
  nat (DMZ,outside) static 192.168.1.5


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

  ----Omitted-----

 Result:
 input-interface:
```

Outside

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

DMZ

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

如数据包跟踪器中所见，流量到达其各自的NAT语句和FTP检测策略。它们还会离开其所需的接口。

在故障排除期间，您可以尝试捕获ASA入口和出口接口，并查看ASA嵌入式IP地址重写是否工作正常，并检查是否允许在ASA上使用动态端口。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。