

Configurar serviços de FTP/TFTP: ASA 9.X

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Gerenciamento Avançado de Protocolos](#)

[Configuração](#)

[Cenário 1. Cliente FTP configurado para o modo ativo](#)

[Diagrama de Rede](#)

[Cenário 2. Cliente FTP configurado para o modo passivo](#)

[Diagrama de Rede](#)

[Cenário 3. Cliente FTP configurado para o modo ativo](#)

[Diagrama de Rede](#)

[Cenário 4. Cliente FTP executando modo passivo](#)

[Diagrama de Rede](#)

[Configuração da Inspeção Básica de Aplicativos de FTP](#)

[Configurar a Inspeção do Protocolo FTP na Porta TCP Não Padrão](#)

[Verificar](#)

[TFTP](#)

[Configuração da Inspeção Básica de Aplicativos de TFTP](#)

[Diagrama de Rede](#)

[Verificar](#)

[Troubleshooting](#)

[Cliente dentro da rede](#)

[Cliente na Rede Externa](#)

Introdução

Este documento descreve diferentes cenários de inspeção de FTP e TFTP no ASA, configuração de inspeção de FTP/TFTP do ASA e Troubleshooting básico.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Comunicação básica entre as interfaces necessárias
- Configuração do servidor FTP localizado na rede DMZ

Componentes Utilizados

Este documento descreve diferentes cenários de inspeção de FTP e TFTP no Adaptive Security Appliance (ASA) e também aborda a configuração de inspeção de FTP/TFTP do ASA e a solução básica de problemas.

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA 5500 ou ASA 5500-X Series ASA que executa a imagem de software 9.1(5)
- Qualquer servidor FTP
- Qualquer cliente FTP

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Security Appliance oferece suporte à inspeção de aplicativos por meio da função Adaptive Security Algorithm.

Ao usar a inspeção stateful de aplicativos do Adaptive Security Algorithm, o Security Appliance controla todas as conexões que cruzam o firewall e garante que elas sejam válidas.

O firewall, por meio da inspeção stateful, também monitora o estado da conexão para compilar informações e colocá-las em uma tabela de estados.

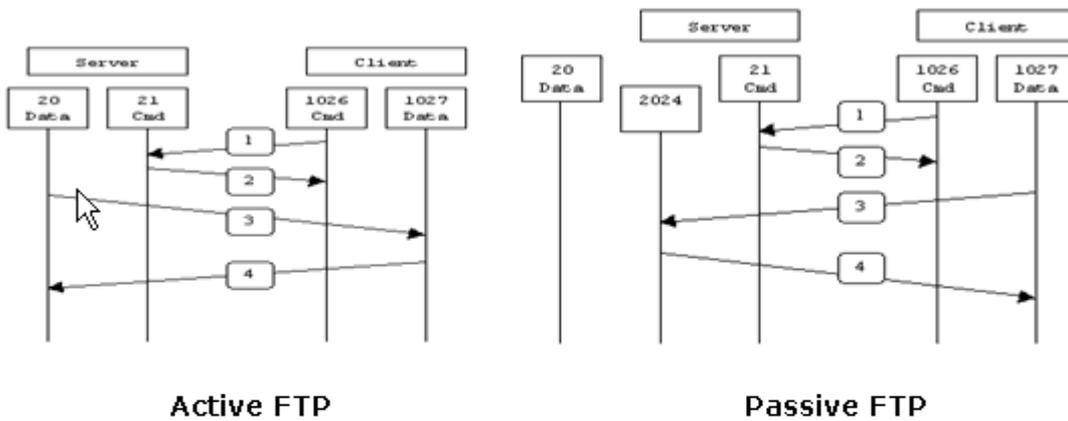
Com o uso da tabela de estados além das regras definidas pelo administrador, as decisões de filtragem baseiam-se no contexto que é estabelecido pelos pacotes transmitidos previamente pelo firewall.

A implementação de inspeções de aplicativos consiste nas seguintes ações:

- Identificar o tráfego
- Aplicar inspeções ao tráfego
- Ativar as inspeções em uma interface

Há duas formas de FTP, como mostrado na imagem.

- Modo ativo
- Modo passivo



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 ativo

No modo de FTP ativo, o cliente se conecta de uma porta sem privilégios aleatória ($N > 1023$) à porta de comandos (21) do servidor FTP. Em seguida, o cliente começa a escutar a porta $N > 1023$ e envia a porta do comando FTP $N > 1023$ para o servidor FTP. O servidor então se conecta de volta às portas de dados especificadas do cliente com sua porta de dados local, a porta 20.

FTP passivo

No modo de FTP passivo, o cliente inicia ambas as conexões para o servidor, o que resolve o problema de um firewall que filtra a conexão da porta de dados de entrada para o cliente do servidor. Quando uma conexão FTP é aberta, o cliente abre duas portas não privilegiadas aleatórias localmente. A primeira porta entra em contato com o servidor na porta 21. Mas, em vez de executar um comando **port** e permitir que o servidor se conecte novamente à sua porta de dados, o cliente executa o comando **PASV**. O resultado é que o servidor abre uma porta não privilegiada aleatória ($P > 1023$) e envia o comando **port P** para o cliente. O cliente então inicia a conexão da porta $N > 1023$ à porta P no servidor para transferir dados. Sem o comando de configuração **inspection** no Security Appliance, o FTP de usuários internos direcionado para fora da rede funciona somente no modo passivo. Além disso, os usuários externos que tentarem acessar seu servidor FTP interno terão o acesso negado.

TFTP

O TFTP, conforme descrito na [RFC 1350](#), é um protocolo simples para ler e gravar arquivos entre um servidor e um cliente TFTP. O TFTP usa a porta 69 do UDP.

Gerenciamento Avançado de Protocolos

Por que você precisa de inspeção de FTP?

Alguns aplicativos necessitam de gerenciamento especial pelas funções de inspeção de aplicativos do Cisco Security Appliance. Esses tipos de aplicativos normalmente incorporam informações de endereçamento IP no pacote de dados do usuário ou abrem canais secundários em portas atribuídas dinamicamente. A função

de inspeção de aplicativos trabalha com a Network Address Translation (NAT) para ajudar a identificar o local das informações de endereçamento incorporadas.

Além da identificação de informações de endereçamento incorporadas, a função de inspeção de aplicativos monitora as sessões para determinar os números de porta dos canais secundários. Muitos protocolos abrem portas TCP ou UDP secundárias para aprimorar o desempenho. A sessão inicial em uma porta bem conhecida é usada para negociar números de portas atribuídos dinamicamente.

A função de inspeção de aplicativos monitora essas sessões, identifica as atribuições de portas dinâmicas e permite a troca de dados nessas portas pela duração das sessões específicas. Aplicativos multimídia e de FTP exibem esse tipo de comportamento.

Se a inspeção de FTP não tiver sido habilitada no Security Appliance, essa solicitação será descartada e as sessões de FTP não transmitirão os dados solicitados.

Se a inspeção de FTP estiver habilitada no ASA, o ASA monitorará o canal de controle e tentará reconhecer uma solicitação para abrir o canal de dados. O protocolo FTP incorpora as especificações de porta do canal de dados no tráfego do canal de controle, o que exige que o Security Appliance inspecione o canal de controle em busca de alterações nas portas de dados.

Quando o ASA reconhece uma solicitação, ele cria temporariamente uma abertura para o tráfego do canal de dados que dura a duração da sessão. Desta forma, a função de inspeção de FTP monitora o canal de controle, identifica uma atribuição de porta de dados e permite que os dados sejam trocados na porta de dados durante a sessão.

O ASA inspeciona as conexões da porta 21 para o tráfego FTP por padrão através do mapa de classe de inspeção global. O Security Appliance também reconhece a diferença entre sessões de FTP ativas e passivas.

Se as sessões de FTP oferecerem suporte à transferência de dados FTP passiva, o ASA, por meio do comando **inspect ftp**, reconhecerá a solicitação de porta de dados do usuário e abrirá uma nova porta de dados maior que 1023.

A inspeção do comando **inspect ftp** inspeciona as sessões de FTP e executa quatro tarefas:

- Prepara uma conexão de dados secundária dinâmica.
- Acompanha a seqüência de comandos e respostas do FTP.
- Gera uma trilha de auditoria.
- Converte os endereços IP incorporados usando o NAT.

A inspeção de aplicativos de FTP prepara os canais de dados secundários para a transferência de dados de FTP. Os canais são alocados em resposta a um upload de arquivo, a um download de arquivo ou a um evento de listagem de diretório, e todos devem ser pré-negociados. A porta é negociada por meio dos comandos **PORT** ou **PASV** (227).

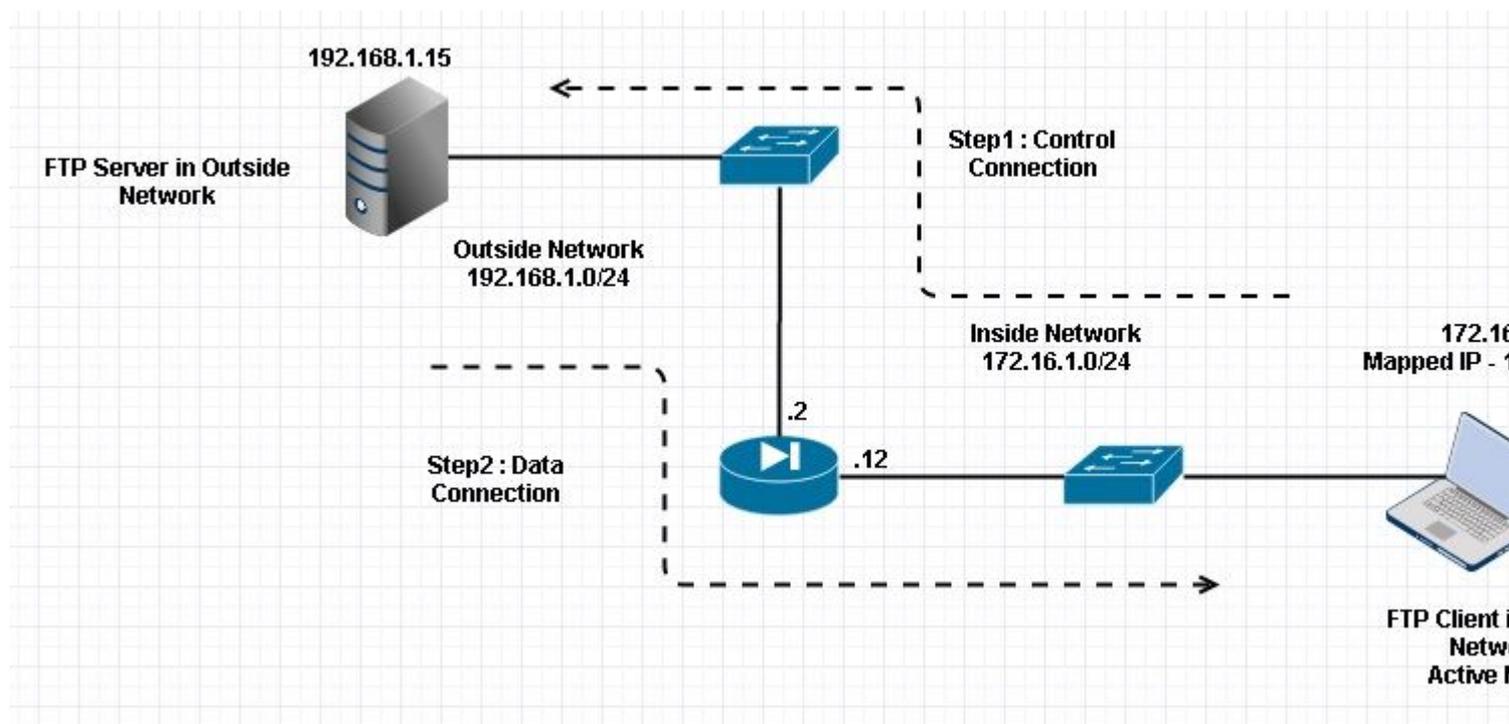
Configuração

Observação: todos os cenários de rede são explicados com a inspeção de FTP habilitada no ASA.

Cenário 1. Cliente FTP configurado para o modo ativo

Cliente conectado à rede interna do ASA e servidor na rede externa.

Diagrama de Rede



Observação: os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet.

Como mostrado nesta imagem, a configuração de rede usada tem o ASA com cliente na rede interna com IP 172.16.1.5. O servidor está na rede externa com IP 192.168.1.15. O cliente tem um IP 192.168.1.5 mapeado na rede externa .

Não há necessidade de permitir nenhuma lista de acesso na interface externa, pois a inspeção de FTP abre o Dynamic Port Channel.

Exemplo de configuração:

```
<#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)#
```

Verificar

Conexão

```
<#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
```

Aqui, o cliente interno inicia a conexão com a porta origem 61854 à porta destino 21. O cliente envia o comando **Port** com um valor de 6 tuplas. O servidor, por sua vez, inicia a conexão Secundária/de Dados com a Porta de Origem 20 e a Porta de Destino é calculada a partir das etapas mencionadas após essas capturas.

Capture a Interface Interna conforme mostrado nesta imagem.

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	.AO"@... <.....
0020	01 0f f1 9e 00 15 3e b4	d4 c8 67 97 6b e3 50 18> ..g.k.P.
0030	7f c5 4e 16 00 00 50 4f	52 54 20 31 37 32 2c 31	..N...PO RT 172,1
0040	36 2c 31 2c 35 2c 32 34	31 2c 31 35 39 0d 0a	6,1,5,24 1,159..

Capture a Interface Externa conforme mostrado nesta imagem.

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 18n. 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..

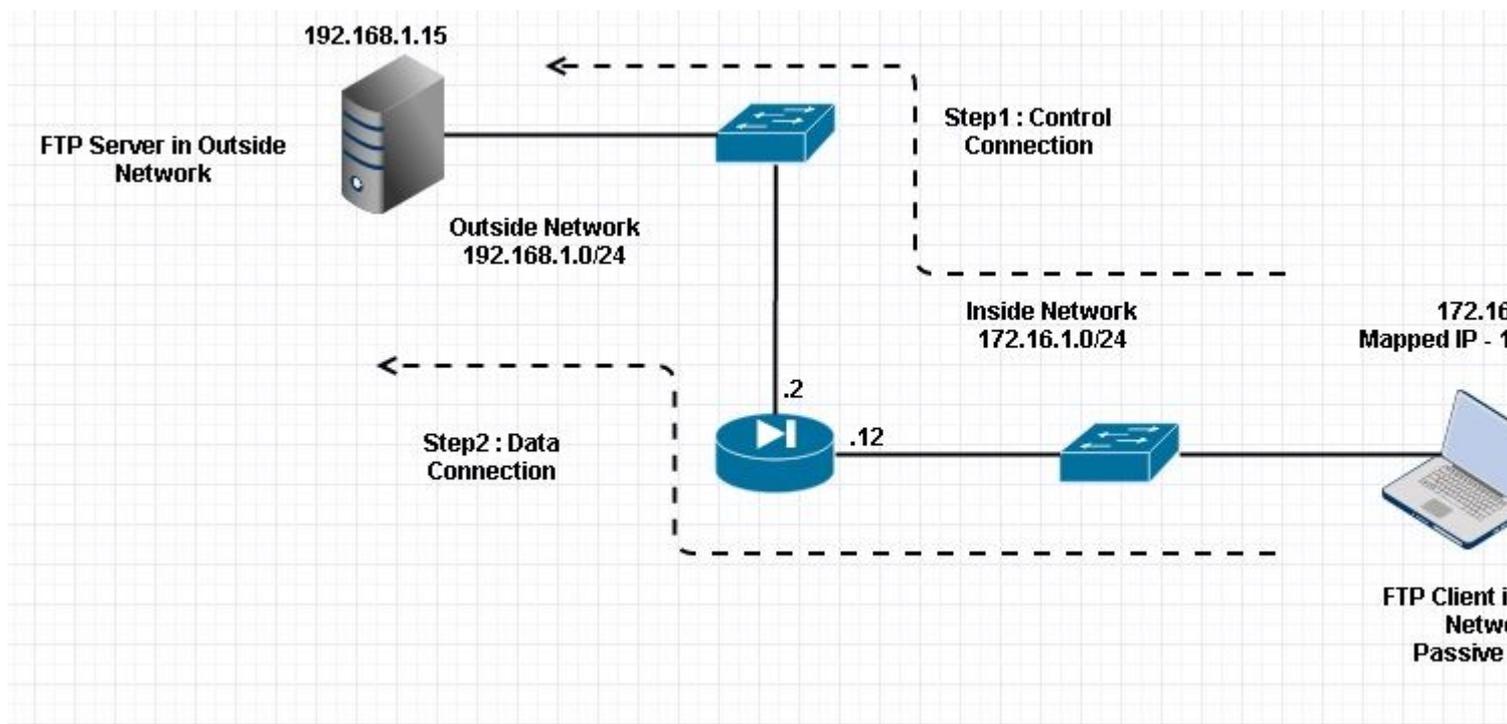
O valor da porta é calculado usando os dois últimos tuplos de seis. As 4 tuplas à esquerda são endereço IP e as 2 tuplas são para Porta. Como mostrado nesta imagem, o endereço IP é 192.168.1.5 e $241 * 256 + 159 = 61855$.

A captura também mostra que os valores com comandos de porta são alterados quando a inspeção de FTP está habilitada. A Captura da Interface Interna mostra o valor real do IP e a porta enviada pelo Cliente para Servidor para se conectar ao Cliente para Canal de Dados e a Captura da Interface Externa mostra o endereço mapeado.

Cenário 2. Cliente FTP configurado para o modo passivo

Cliente na Rede Interna do ASA e Servidor na Rede Externa.

Diagrama de Rede



Conexão

```
<#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

Aqui, o cliente interno inicia uma conexão com a Porta origem 61838 a Porta destino 21. Como é um FTP passivo, o cliente inicia ambas as conexões. Portanto, depois que o cliente envia o comando **PASV**, o servidor responde com seu valor de tupla 6 e o cliente se conecta a esse soquete para conexão de dados.

Capture a Interface Interna conforme mostrado nesta imagem.

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=13110
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 W
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 a Interface Externa conforme mostrado nesta imagem.

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=13108
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=13108
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=13082
64	37.549569	192.168.1.5	192.168.1.15	FTP	62	Request: TYPE I
65	37.550622	192.168.1.15	192.168.1.5	FTP	73	Response: 200 Type set to I
66	37.551262	192.168.1.5	192.168.1.15	FTP	60	Request: PASV
67	37.554818	192.168.1.15	192.168.1.5	FTP	104	Response: 227 Entering Passive Mode (192,168,1,15,234,238)
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=262144 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)..

```

O cálculo das portas permanece o mesmo.

Como mencionado anteriormente, o ASA regrava os valores IP incorporados se a inspeção de FTP estiver habilitada. Além disso, ele abre um canal de porta dinâmico para conexão de dados.

Estes são os detalhes da conexão se **Inspeção de FTP desabilitada**

Conexão:

<#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

```

Sem inspeção de FTP, ele apenas tenta enviar o comando **port** de novo e de novo, mas não há resposta, pois

o exterior recebe a PORTA com IP original não NAT um. O mesmo foi mostrado no despejo.

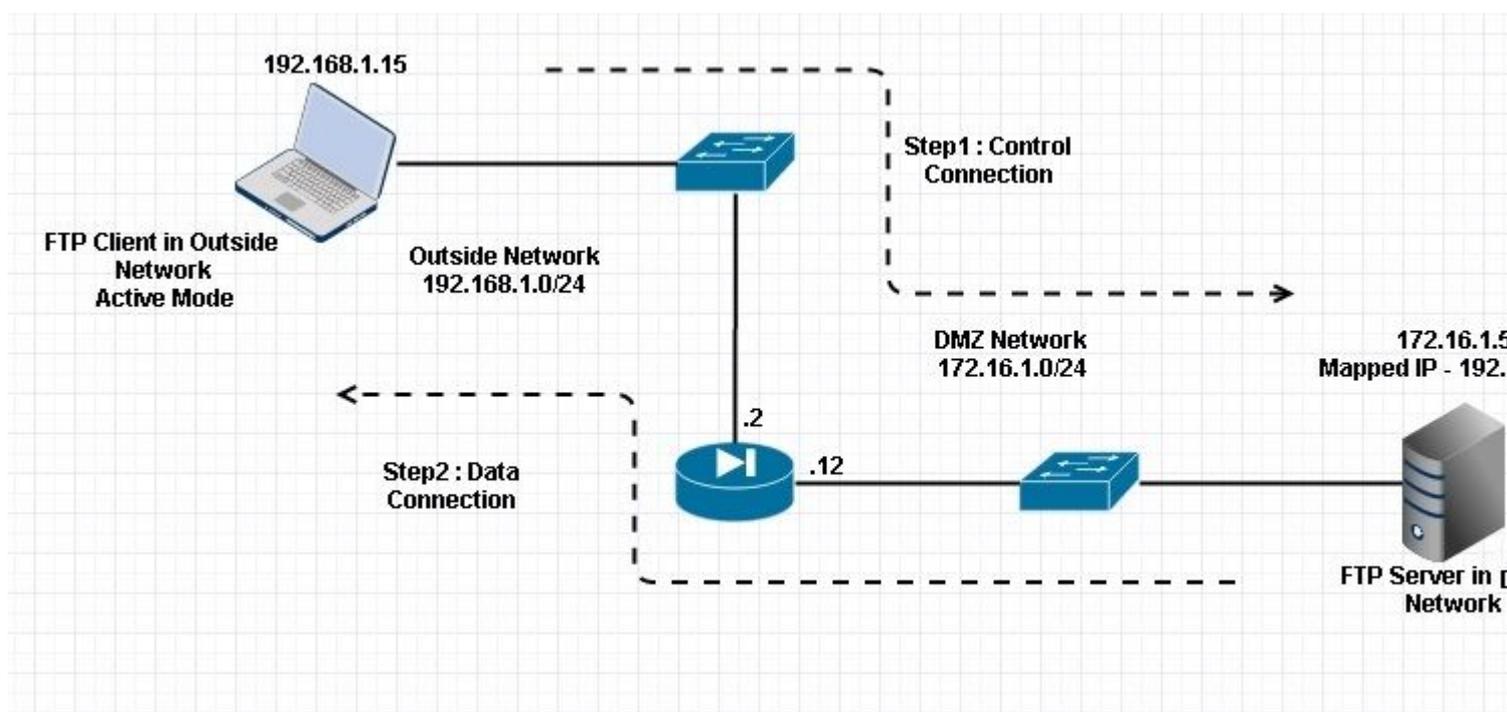
A inspeção de FTP pode ser desativada com o comando **no fixup protocol ftp 21** no modo terminal de configuração.

Sem a inspeção de FTP, somente o comando **PASV** funciona quando o cliente está dentro, pois não há nenhum comando **port** vindo de dentro que precise ser incorporado e ambas as conexões são iniciadas de dentro.

Cenário 3. Cliente FTP configurado para o modo ativo

Cliente na Rede Externa do ASA e Servidor na Rede DMZ.

Diagrama de Rede



Configuração:

```
<#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)#
```

Verificar

Conexão:

```
<#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 a interface DMZ conforme mostrado nesta imagem.

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 18P.
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 a Interface Externa conforme mostrado nesta imagem.

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

```

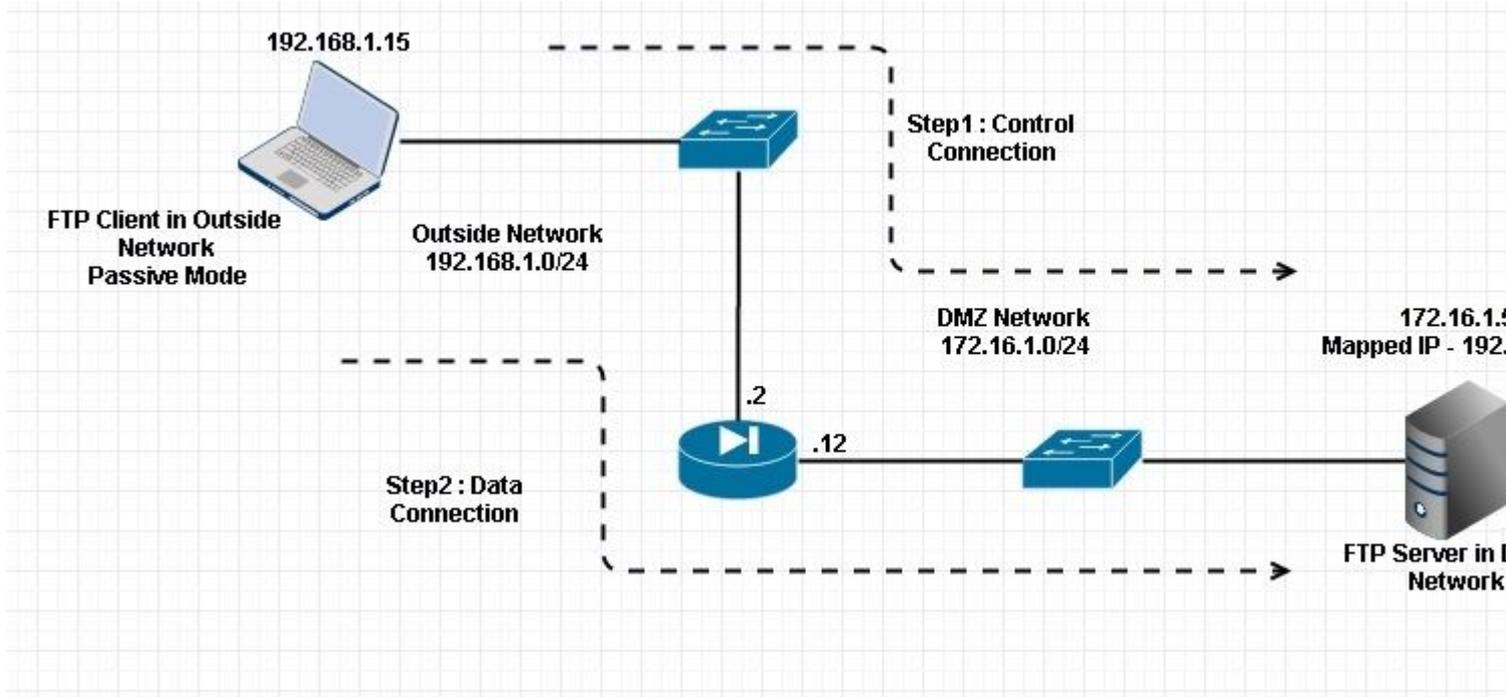
0010	00 42 7a 10 40 00 80 06	fd 40 c0 a8 01 0f c0 a8	.8z.@... .@.....
0020	01 05 da 1c 00 15 92 fd	a7 32 2b 4a 2d 85 50 182+)-.P.
0030	7f bd a9 bf 00 00 50 4f	52 54 20 31 39 32 2c 31PO RT 192,1
0040	36 38 2c 31 2c 31 35 2c	32 31 38 2c 32 39 0d 0a	68,1,15, 218,29..

Aqui, o cliente executa o Cliente do Modo Ativo 192.168.1.15 e inicia a conexão com o servidor na DMZ na porta 21. O cliente envia o comando **port** com seis valores de tupla para o servidor para se conectar a essa porta dinâmica específica. Em seguida, o servidor inicia a conexão de dados com a Porta de origem como 20.

Cenário 4. Cliente FTP executando modo passivo

Cliente na Rede Externa do ASA e Servidor na Rede DMZ.

Diagrama de Rede



Conexão

<#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 a interface DMZ conforme mostrado nesta imagem.

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 a Interface Externa conforme mostrado nesta imagem.

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=0 Len=0
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=0 Len=0
49	23.556740	192.168.1.15	192.168.1.5	TCP	54	60071→61781 [ACK] Seq=3795016103 Ack=1047360619 Win=0 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=0 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

▣ Frame 45: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
 ▣ Ethernet II, Src: Cisco_c9:92:88 (00:19:e8:c9:92:88), Dst: Vmware_ad:24:76 (00:50:56:ad:24:76)
 ▣ Internet Protocol Version 4, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.15 (192.168.1.15)
 ▣ Transmission Control Protocol, Src Port: 21 (21), Dst Port: 60070 (60070), Seq: 1496462070, Ack: 2627142506, Len: 48
 ▣ File Transfer Protocol (FTP)
 ▣ 227 Entering Passive Mode (192,168,1,5,241,85)\r\n
 Response code: Entering Passive Mode (227)
 Response arg: Entering Passive Mode (192,168,1,5,241,85)

```

0030 01 ff c3 f5 00 00 32 32 37 20 45 6e 74 65 72 69 .....22 7 Enteri
0040 6e 67 20 50 61 73 73 69 76 65 20 4d 6f 64 65 20 ng Passi ve Mode
0050 28 31 39 32 2c 31 36 38 2c 31 2c 35 2c 32 34 31 (192,168 ,1,5,241
0060 2c 38 35 29 0d 0a ,85)..
  
```

Configuração da Inspeção Básica de Aplicativos de FTP

Por padrão, a configuração inclui uma política que corresponde a todo o tráfego de inspeção de aplicativos padrão e aplica a inspeção ao tráfego em todas as interfaces (uma política global). O tráfego de inspeção de aplicativos padrão inclui o tráfego para as portas padrão para cada protocolo.

É possível aplicar somente uma política global. Assim, se desejar alterar a política global, por exemplo, para aplicar inspeção a portas não padrão ou adicionar inspeções que não são habilitadas por padrão, você deverá editar a política padrão ou desabilitá-la e aplicar uma nova política. Para obter uma lista de todas as portas padrão, consulte [Política de Inspeção Padrão](#).

1. Execute o comando **policy-map global_policy**.

```

<#root>

ASA(config)#

policy-map global_policy
  
```

2. Execute o comando **class inspection_default**.

```

<#root>

ASA(config-pmap)#
  
```

```
class inspection_default
```

3. Execute o comando **inspect FTP**.

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

4. Há a opção de usar o comando **inspect FTP strict**. Esse comando aumenta a segurança das redes protegidas ao impedir que um navegador da Web envie comandos incorporados em solicitações de FTP.

Após você habilitar a opção **strict em uma interface, a inspeção de FTP passará a impor este comportamento.**

- Um comando de FTP deverá ser confirmado para que o Security Appliance permita um novo comando
- O Security Appliance descarta conexões que enviam comandos incorporados
- Os comandos **227** e **PORT** são verificados para garantir que eles não apareçam em uma string de erro

Aviso: o uso da opção **strict** possivelmente causa a falha de clientes FTP que não são estritamente compatíveis com RFCs FTP. Consulte [Uso da Opção strict](#) para obter mais informações sobre o uso da opção **strict**.

Configurar a Inspeção do Protocolo FTP na Porta TCP Não Padrão

Você pode configurar a inspeção de protocolo FTP para portas TCP não padrão com estas linhas de configuração (substitua XXXX pelo novo número de porta):

```
<#root>  
  
access-list ftp-list extended permit tcp any any eq XXXX  
!  
class-map ftp-class  
  match access-list ftp-list  
!  
policy-map global_policy  
  class ftp-class  
  
inspect ftp
```

Verificar

Para garantir que a configuração tenha sido realizada com êxito, execute o comando **show service-policy**. Além disso, limite a saída à inspeção de FTP executando o 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

A inspeção de TFTP é habilitada por padrão.

O Security Appliance inspeciona o tráfego de TFTP e cria dinamicamente conexões e conversões e, se necessário, permite a transferência de arquivos entre um cliente e um servidor TFTP. Especificamente, o mecanismo de inspeção inspeciona solicitações de leitura (RRQ), solicitações de gravação (WRQ) e notificações de erro (ERROR) do TFTP.

Um canal secundário dinâmico e uma conversão PAT, se necessários, são alocados mediante o recebimento de uma RRQ ou WRQ válida. Este canal secundário é subseqüentemente usado pelo TFTP para a transferência de arquivos ou a notificação de erros.

Somente o servidor TFTP pode iniciar o tráfego via canal secundário, e no máximo um canal secundário incompleto pode existir entre o cliente e o servidor TFTP. Uma notificação de erro do servidor fecha o canal secundário.

A inspeção de TFTP deve ser habilitada se o PAT estático for usado para redirecionar o tráfego de TFTP.

Configuração da Inspeção Básica de Aplicativos de TFTP

Por padrão, a configuração inclui uma política que corresponde a todo o tráfego de inspeção de aplicativos padrão e aplica a inspeção ao tráfego em todas as interfaces (uma política global). O tráfego de inspeção de aplicativos padrão inclui o tráfego para as portas padrão para cada protocolo.

É possível aplicar somente uma política global. Assim, se desejar alterar a política global, por exemplo, para aplicar inspeção a portas não padrão ou adicionar inspeções que não são habilitadas por padrão, você deverá editar a política padrão ou desabilitá-la e aplicar uma nova política. Para obter uma lista de todas as portas padrão, consulte [Política de Inspeção Padrão](#).

1. Execute o comando **policy-map global_policy**.

```
<#root>
ASA(config)#
```

```
policy-map global_policy
```

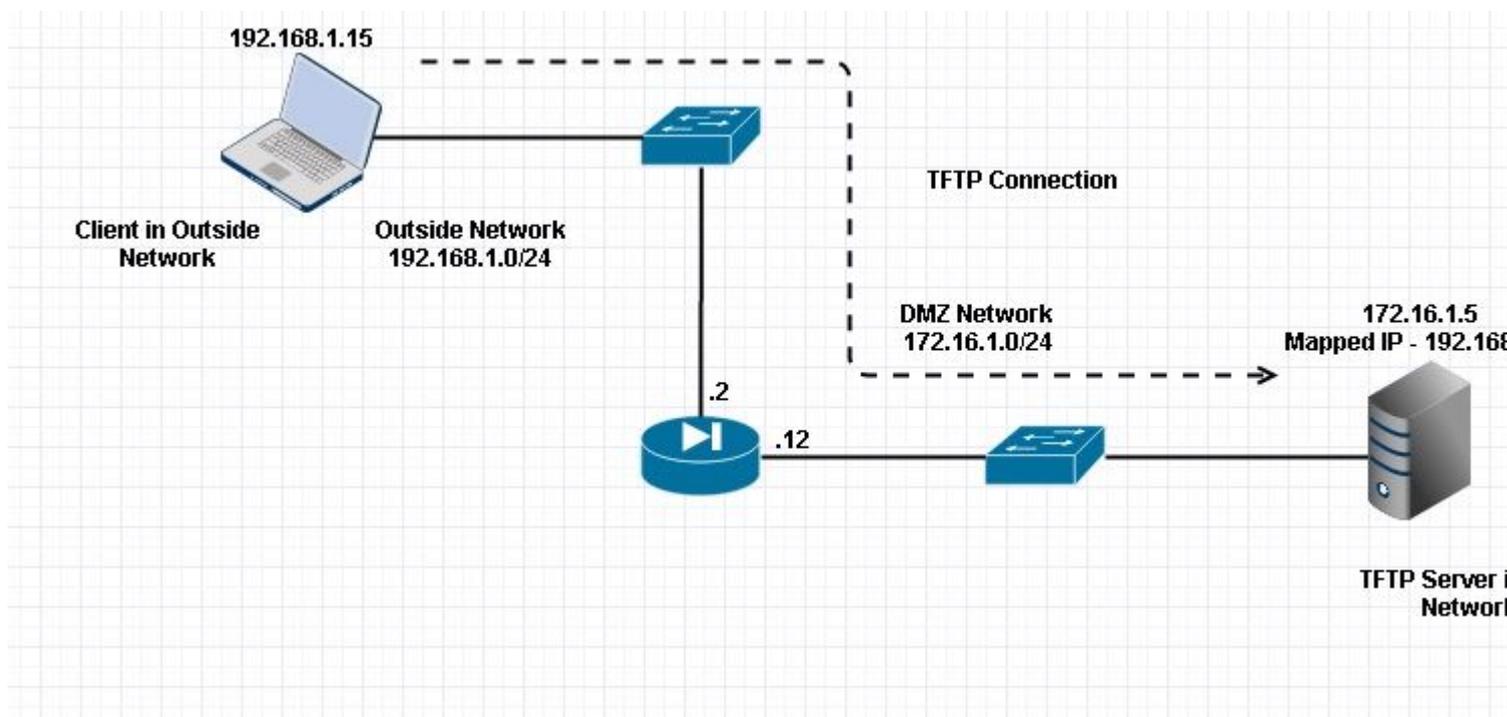
2. Execute o comando **class inspection_default** .

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

3. Execute o comando **inspect TFTP**.

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

Diagrama de Rede



Aqui o cliente é configurado na rede externa. O servidor TFTP é colocado na rede DMZ. O servidor é mapeado para o IP 192.168.1.5 que está na sub-rede externa.

Exemplo de configuração:

<#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)#

```

Verificar

Para garantir que a configuração tenha sido realizada com êxito, execute o comando **show service-policy**. Além disso, limite a saída à inspeção de TFTP somente executando o 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#
```

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Packet Tracer

Cliente dentro da rede

<#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 na Rede 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 visto nos rastreadores de pacotes, o tráfego atinge suas respectivas instruções NAT e Política de inspeção de FTP. Eles também deixam suas interfaces necessárias.

Durante a solução de problemas, você pode tentar capturar as interfaces de entrada e saída do ASA e ver se a regulação do endereço IP incorporado do ASA está funcionando bem e verificar a conexão se a porta dinâmica está sendo permitida no ASA.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.