

Configuration des services FTP/TFTP : ASA 9.X

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Prendre en charge le Protocole avancé](#)

[Configuration](#)

[Scénario 1. Client FTP configuré pour le mode actif](#)

[Diagramme du réseau](#)

[Scénario 2. Client FTP configuré pour le mode passif](#)

[Diagramme du réseau](#)

[Scénario 3. Client FTP configuré pour le mode actif](#)

[Diagramme du réseau](#)

[Scénario 4 . Client FTP en mode passif](#)

[Diagramme du réseau](#)

[Configurez l'inspection de base de l'application FTP](#)

[Configuration de l'inspection du protocole FTP sur le port TCP non standard](#)

[Vérifier](#)

[TFTP](#)

[Configurez l'inspection de base de l'application TFTP](#)

[Diagramme du réseau](#)

[Vérifier](#)

[Dépannage](#)

[Client dans le réseau interne](#)

[Client dans le réseau externe](#)

Introduction

Ce document décrit différents scénarios d'inspection FTP et TFTP sur l'ASA, la configuration d'inspection FTP/TFTP ASA et le dépannage de base.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Communication de base entre les interfaces requises

- Configuration du serveur FTP situé sur le réseau DMZ

Composants utilisés

Ce document décrit différents scénarios d'inspection FTP et TFTP sur l'apppliance de sécurité adaptative (ASA) et couvre également la configuration d'inspection FTP/TFTP ASA et le dépannage de base.

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA 5500 ou ASA 5500-X qui exécute l'image logicielle 9.1(5)
- Tout serveur FTP
- Tout client FTP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le dispositif de sécurité prend en charge l'inspection d'application via la fonction d'algorithme de sécurité adaptatif.

Par l'inspection d'application avec état utilisée par l'algorithme de sécurité adaptatif, le dispositif de sécurité suit chaque connexion qui traverse le pare-feu et s'assure qu'elle est valide.

Le pare-feu, par l'inspection avec état, surveille également l'état de la connexion pour compiler des informations à placer dans une table des états.

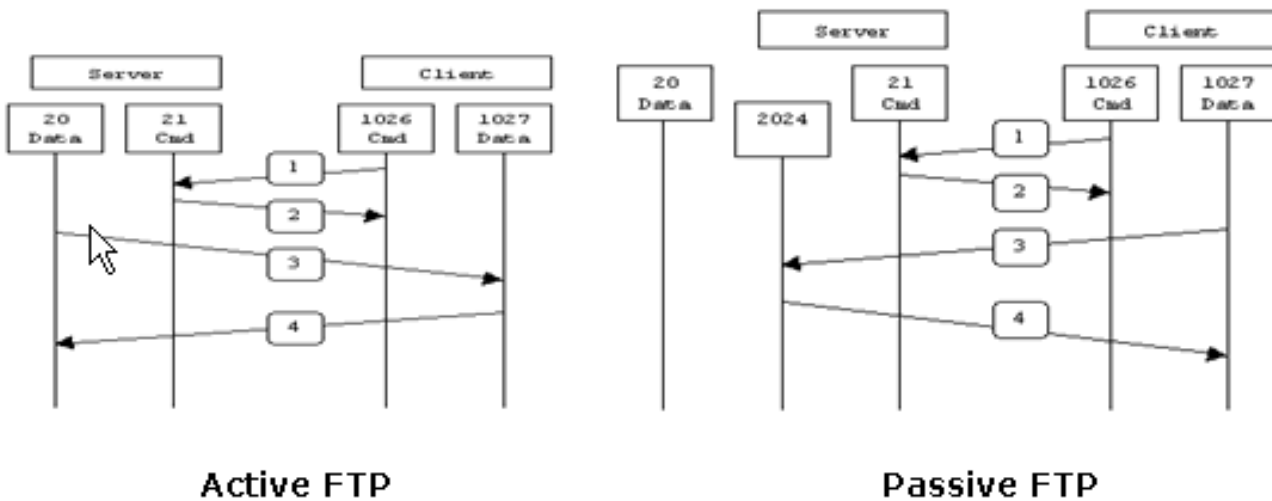
Avec l'utilisation de la table des états en plus des règles définies par l'administrateur, les décisions de filtrage sont basées sur le contexte qui est établi par les paquets qui sont précédemment passés à travers le pare-feu.

La mise en œuvre des inspections d'application consiste en ces actions :

- Identifier le trafic
- Appliquer des inspections au trafic
- Activer des inspections sur une interface

Il existe deux formes de FTP, comme illustré dans l'image.

- Mode actif
- Mode passif



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 actif

En mode actif FTP, le client se connecte d'un port non privilégié aléatoire ($N > 1023$) au port de commande (21) du serveur FTP. Ensuite, le client commence à écouter le port $N > 1023$ et envoie la commande FTP port $N > 1023$ au serveur FTP. Le serveur se connecte alors à nouveau aux ports spécifiés de données du client à partir de son port local de données, qui est le port 20.

FTP passif

En mode de FTP passif, le client lance les deux connexions au serveur, ce qui résout le problème d'un Pare-feu qui filtre la connexion du port de données entrantes au client à partir du serveur. Lorsqu'une connexion FTP est ouverte, le client ouvre deux ports aléatoires non privilégiés localement. Le premier port contacte le serveur sur le port 21. Mais au lieu d'exécuter une commande port et de permettre au serveur de se reconnecter à son port de données, le client émet la commande PASV. Ceci fait que le serveur ouvre alors un port non privilégié aléatoire ($P > 1023$) et renvoie la commande du port P au client. Le client initie alors la connexion du port $N > 1023$ au port P sur le serveur pour transférer des données. Sans la configuration de la commande d'inspection sur l'Appliance de sécurité, le FTP à partir des utilisateurs internes dirigés vers l'extérieur fonctionne seulement en mode passif. En outre, l'accès est refusé aux utilisateurs dirigés en entrée vers votre serveur FTP.

TFTP

Le TFTP, comme décrit dans [RFC 1350](#), est un protocole de routage simple pour lire et écrire des fichiers entre un serveur TFTP et un client. Le TFTP utilise le port UDP 69.

Prendre en charge le Protocole avancé

Pourquoi avez-vous besoin d'une inspection FTP ?

Certaines applications requièrent une prise en charge spéciale par la fonction d'inspections de l'Appliance de sécurité Cisco. Ces types d'applications incluent habituellement les informations d'adressage IP dans le paquet de données utilisateur ou les canaux auxiliaires ouverts sur les ports dynamiquement attribués. La fonction d'inspection d'application fonctionne avec la traduction d'adresses de réseau (NAT) afin d'aider à identifier l'emplacement des informations d'adressage intégrées.

En plus de l'identification des informations d'adressage intégrées, la fonction d'inspection d'application surveille les sessions afin de déterminer les numéros de port pour les canaux secondaires. Plusieurs protocoles de routage ouvrent les ports auxiliaires TCP ou UDP pour améliorer des performances. La session initiale sur un port connu est utilisée pour négocier les numéros de port dynamiquement attribués.

La fonction d'inspection d'application contrôle ces sessions, identifie les affectations des ports dynamiques et permet des échanges de données sur ces ports pour la durée des sessions spécifiques. Les applications Multimédia et les applications FTP montrent ce genre de comportement.

Si l'inspection FTP n'a pas été activée sur l'appliance de sécurité, cette demande est rejetée et les sessions FTP ne transmettent aucune donnée demandée.

Si l'inspection FTP est activée sur l'ASA, l'ASA surveille le canal de contrôle et tente de reconnaître une demande d'ouverture du canal de données. Le protocole FTP inclut les caractéristiques de port du canal de données dans le trafic du canal de contrôle, en demandant à l'Appliance de sécurité d'inspecter le canal de contrôle pour des modifications du port de données

Une fois que l'ASA reconnaît une requête, il crée temporairement une ouverture pour le trafic du canal de données qui dure toute la durée de la session. De cette façon, la fonction d'inspection de FTP contrôle le canal de contrôle, identifie une affectation du port de données et permet aux données d'être échangées sur le port de données pour la durée de la session.

ASA inspecte les connexions du port 21 pour le trafic FTP par défaut via la carte-classe d'inspection globale. L'Appliance de sécurité identifie également la différence entre une session FTP active et une session FTP passive.

Si les sessions FTP prennent en charge le transfert de données FTP passif, l'ASA via la commande `inspect ftp`, reconnaît la demande de port de données de l'utilisateur et ouvre un nouveau port de données supérieur à 1023.


La commande `inspect ftp inspection` inspecte les sessions FTP et effectue quatre tâches :

- Prépare une connexion de données secondaire dynamique
- Suit la séquence des commandes-réponses de FTP

- Génère une vérification rétrospective
- Traduit l'adresse IP incluse en utilisant NAT

L'inspection d'application FTP prépare des canaux auxiliaires pour le transfert des données de FTP. Les canaux sont alloués en réponse au téléchargement d'un fichier, ou à un événement d'énumération du répertoire et ils doivent être les pré-négociés. Le port est négocié par les commandes (227) PORT ou PASV (.

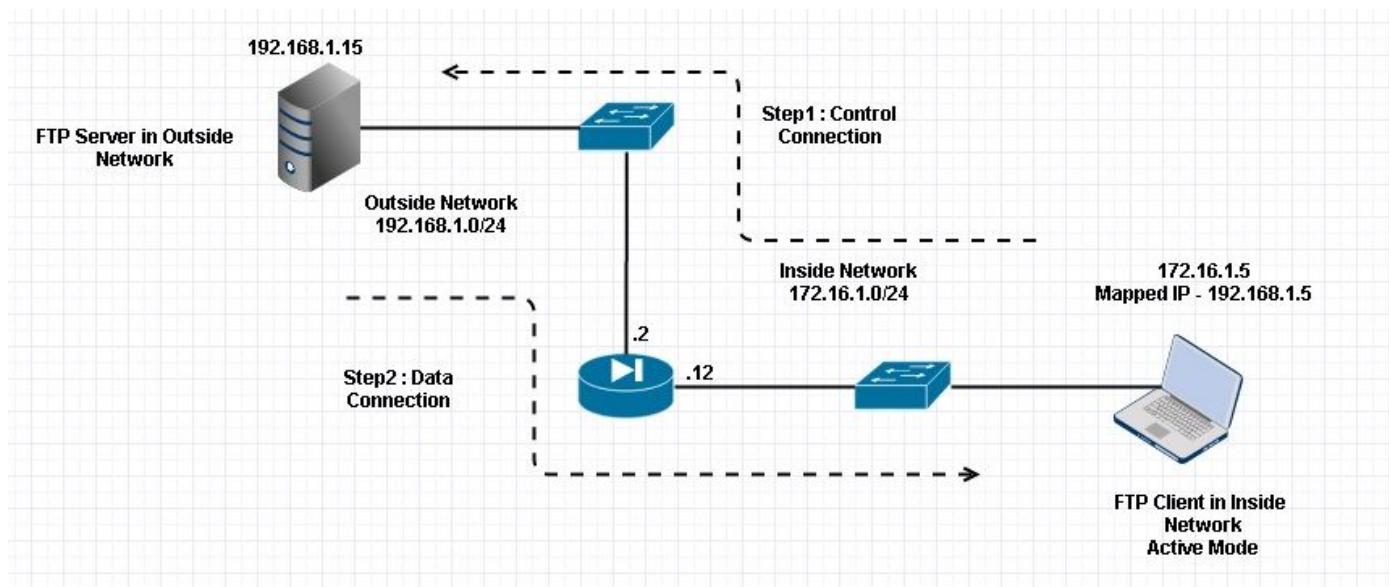
Configuration


 Remarque : tous les scénarios réseau sont expliqués lorsque l'inspection FTP est activée sur l'ASA.

Scénario 1. Client FTP configuré pour le mode actif

Client connecté au réseau interne de l'ASA et au serveur dans le réseau externe.

Diagramme du réseau



 Remarque : les schémas d'adressage IP utilisés dans cette configuration ne sont pas légalement routables sur Internet.

Comme l'illustre cette image, la configuration réseau utilisée comporte l'ASA avec client dans le réseau interne avec IP 172.16.1.5. Le serveur se trouve dans le réseau externe avec l'adresse IP 192.168.1.15. Le client a une adresse IP mappée 192.168.1.5 dans le réseau externe .

Il n'est pas nécessaire d'autoriser une liste d'accès sur l'interface externe car l'inspection FTP ouvre le canal de port dynamique.

Exemple de configuration :

<#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)#
```

Vérifier

Connexion

<#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

Ici, le client dans Inside initie la connexion avec le port source 61854 au port de destination 21. Le client envoie ensuite la commande Port avec 6 valeurs de tuple. Le serveur à son tour initie la connexion secondaire/données avec le port source 20 et le port de destination est calculé à partir des étapes mentionnées après ces captures.

Capturez l'interface interne comme illustré dans cette image.

No.	Time	Source	Destination	Protocol	Length	Info
15	12.101618	172.16.1.5	192.168.1.15	TCP	66	61854->21 [SYN] Seq=1052038301 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
16	12.102228	192.168.1.15	172.16.1.5	TCP	66	21->61854 [SYN, ACK] Seq=1737976540 Ack=1052038302 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
17	12.102472	172.16.1.5	192.168.1.15	TCP	54	61854->21 [ACK] Seq=1052038302 Ack=1737976541 Win=131100 Len=0
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/projects/filezilla/
21	12.104456	172.16.1.5	192.168.1.15	TCP	54	61854->21 [ACK] Seq=1052038302 Ack=1737976628 Win=131012 Len=0
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 directory.
28	12.327680	172.16.1.5	192.168.1.15	TCP	54	61854->21 [ACK] Seq=1052038336 Ack=1737976784 Win=130856 Len=0
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=1380 WS=4 SACK_PERM=1
35	13.768109	172.16.1.5	192.168.1.15	TCP	66	61855->20 [SYN, ACK] Seq=266238504 Ack=2835235613 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
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=131100 Len=0
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 04 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..
```

Capturez l'interface externe comme illustré dans cette image.

No.	Time	Source	Destination	Protocol	Length	Info
15	12.101633	192.168.1.5	192.168.1.15	TCP	66	61854->21 [SYN] Seq=1859474367 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
16	12.102091	192.168.1.15	192.168.1.5	TCP	66	21->61854 [SYN, ACK] Seq=213433641 Ack=1859474368 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	12.102366	192.168.1.5	192.168.1.15	TCP	54	61854->21 [ACK] Seq=1859474368 Ack=213433642 Win=131100 Len=0
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/projects/filezilla/
21	12.104334	192.168.1.15	192.168.1.15	TCP	54	61854->21 [ACK] Seq=1859474368 Ack=213433729 Win=131012 Len=0
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 directory.
28	12.327574	192.168.1.5	192.168.1.15	TCP	54	61854->21 [ACK] Seq=1859474402 Ack=213433885 Win=130856 Len=0
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=1460 WS=4 SACK_PERM=1
35	13.768002	192.168.1.5	192.168.1.15	TCP	66	61855->20 [SYN, ACK] Seq=785612049 Ack=1406112685 Win=65535 Len=0 MSS=1380 WS=128 SACK_PERM=1
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=131100 Len=0
38	13.769665	192.168.1.15	192.168.1.5	FTP-DATA 1434	1434	FTP Data: 1380 bytes
39	13.769680	192.168.1.15	192.168.1.5	FTP-DATA 1434	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%0... (/.....
0020 01 0f f1 9e 00 15 6e d5 53 ea 0c b8 be 30 50 18 .....n. S....OP.
0030 7f c5 a7 7d 00 00 50 4f 52 54 20 31 39 32 2c 31 ...).PO RT 192,1
0040 36 38 2c 31 2c 35 2c 32 34 31 2c 31 35 39 0d 0a 68,1,5,2 41,159..

```

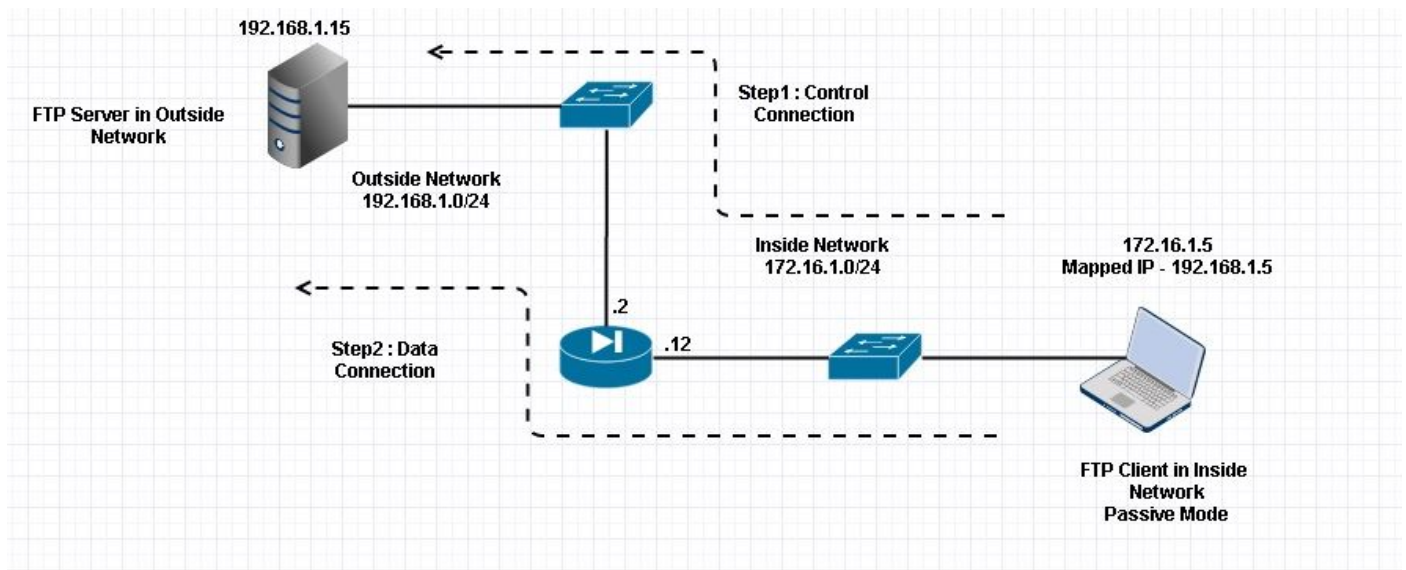
La valeur de port est calculée à l'aide des deux derniers nombres sur six. Les 4 tuples gauches correspondent à l'adresse IP et les 2 tuples correspondent au port. Comme l'illustre cette image, l'adresse IP est 192.168.1.5 et $241 \times 256 + 159 = 61855$.

Capture indique également que les valeurs des commandes de port sont modifiées lorsque l'inspection FTP est activée. La capture d'interface interne montre la valeur réelle de l'IP et le port envoyé par le client pour le serveur pour se connecter au client pour le canal de données et la capture d'interface externe montre l'adresse mappée.

Scénario 2. Client FTP configuré pour le mode passif

Client dans le réseau interne de l'ASA et serveur dans le réseau externe.

Diagramme du réseau



Connexion

<#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

Ici, le client à l'intérieur initie une connexion avec le port source 61838 et le port de destination 21. Comme il s'agit d'un FTP passif, le client initie les deux connexions. Par conséquent, après la commande Client Sends PASV, le serveur répond avec sa valeur de tuple 6 et le client se connecte à ce Socket pour la connexion de données.

Capturez l'interface interne comme illustré dans cette image.

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 6922 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)..			

Capturez l'interface externe comme illustré dans cette image.

No.	Time	Source	Destination	Protocol	Length	Info
48	35.656299	192.168.1.5	192.168.1.15	TCP	66	61838->21 [SYN] Seq=2543303555 Win=8192 Len=0 MSS=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
<pre> 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 6922 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).. </pre>						

Le calcul pour les ports reste le même.

Comme mentionné précédemment, l'ASA réécrit les valeurs IP intégrées si l'inspection FTP est activée. En outre, il ouvre un canal de port dynamique pour la connexion de données.

Voici les détails de la connexion si Inspection FTP désactivée

Connexion:

<#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
```

Sans inspection FTP, Il essaie seulement d'envoyer la commande port encore et encore mais il n'y a pas de réponse car l'extérieur reçoit le PORT avec l'IP d'origine non NATted un. La même chose a été montrée dans le vidage.

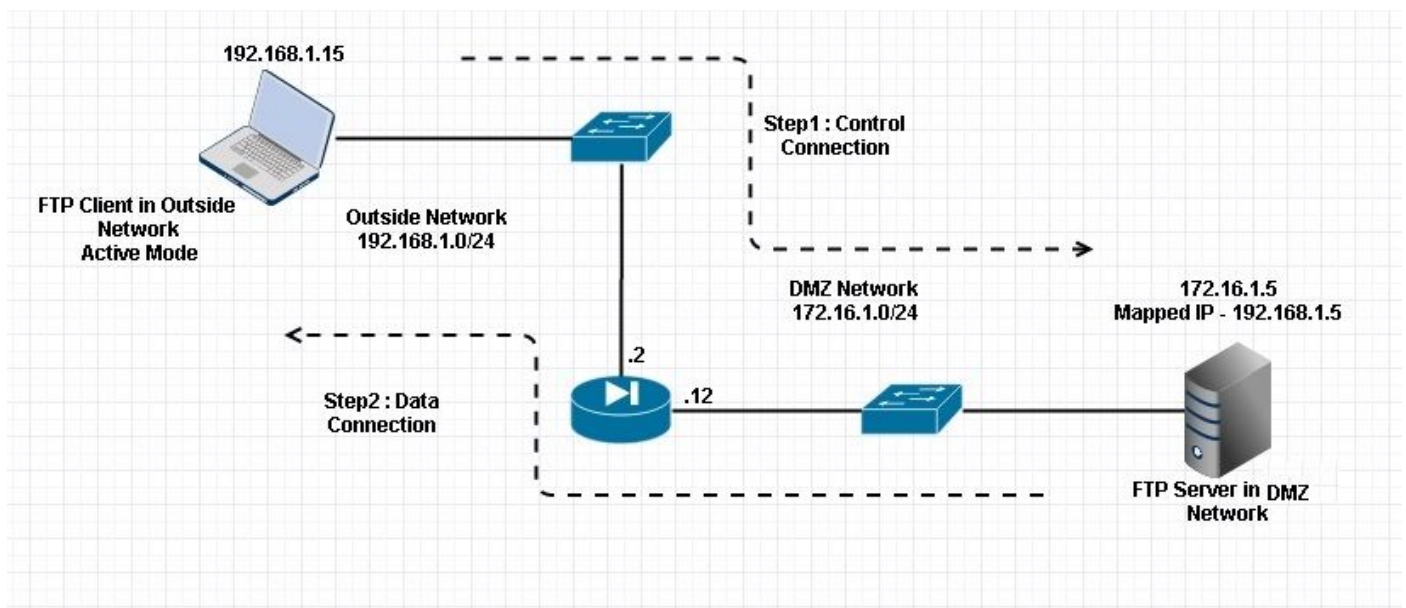
L'inspection FTP peut être désactivée avec la commande no fixup protocol ftp 21 en mode terminal de configuration.

Sans l'inspection FTP, seule la commande PASV fonctionne quand le client est à l'intérieur car il n'y a aucune commande de port provenant de l'intérieur qui doit être incorporée et les deux connexions sont initiées de l'intérieur.

Scénario 3. Client FTP configuré pour le mode actif

Client du réseau externe de l'ASA et serveur du réseau DMZ.

Diagramme du réseau



Configuration:

```
<#root>
```

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

ASA Version 9.1(5)
!
hostname ASA
domain-name corp .com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface GigabitEthernet0/0
 nameif Outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet0/1
 nameif DMZ
 security-level 50
```

```
ip address 172.16.1.12 255.255.255.0
!  
interface GigabitEthernet0/2  
shutdown  
no nameif  
no security-level  
no ip address  
!  
interface GigabitEthernet0/3  
shutdown  
no nameif  
no security-level  
no ip address  
!  
interface Management0/0  
management-only  
shutdown  
no nameif  
no security-level  
no ip address
```

!--- Output is suppressed.

!--- Permit inbound FTP control traffic.

```
access-list 100 extended permit tcp any host 192.168.1.5 eq ftp
```

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

```
object network obj-172.16.1.5  
host 172.16.1.5
```

!--- Object NAT is created to map FTP server with IP of Outside Subnet.

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

```
access-group 100 in interface outside
```

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

```
policy-map global_policy
```

```
class inspection_default
```

```
inspect dns preset_dns_map
```

```
inspect ftp
```

```
inspect h323 h225
```

```
inspect h323 ras
```

```
inspect netbios
```

```
inspect rsh
```

```
inspect rtsp
```

```
inspect skinny
```

```
inspect esmtp
```

```
inspect sqlnet
```

```
inspect sunrpc
```

```
inspect tftp
```

```
inspect sip
```

```
inspect xdmcp
```

```
!
```

```
!--- This command tells the device to
```

```
!--- use the "global_policy" policy-map on all interfaces.
```

```
service-policy global_policy global
```

```
prompt hostname context
```

```
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
```

```
: end
```

```
ASA(config)#
```

Vérifier

Connexion:

<#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
```

Capturez l'interface DMZ comme illustré dans cette image.

No.	Time	Source	Destination	Protocol	Length	Info
15	12.032774	192.168.1.15	172.16.1.5	TCP	66	55836->21 [SYN] Seq=3317358682 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
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=1460 WS=256 SACK_PERM=1
17	12.037214	192.168.1.15	172.16.1.5	TCP	54	55836->21 [ACK] Seq=3317358683 Ack=3073360303 Win=131100 Len=0
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=131012 Len=0
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=130824 Len=0
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=1460 WS=4 SACK_PERM=1
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=65535 Len=0 MSS=1380 WS=128 SACK_PERM=1
39	13.806049	172.16.1.5	192.168.1.15	TCP	54	20->55837 [ACK] Seq=1812810162 Ack=177574186 Win=131100 Len=0
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 .8z.0... ..
0020 01 05 da 1c 00 15 c5 ba e0 8a b7 2f c2 d4 50 18 ..... ..P.
0030 7f bd 31 0d 00 00 50 4f 52 54 20 31 39 32 2c 31 .....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..

```

Capturez l'interface externe comme illustré dans cette image.

No.	Time	Source	Destination	Protocol	Length	Info
21	12.045240	192.168.1.15	192.168.1.5	TCP	66	55836->21 [SYN] Seq=2466096898 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
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=1380 WS=256 SACK_PERM=1
23	12.049803	192.168.1.15	192.168.1.5	TCP	54	55836->21 [ACK] Seq=2466096899 Ack=726281312 Win=131100 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=131012 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=130824 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 WS=4 SACK_PERM=1
43	13.818058	192.168.1.5	192.168.1.15	FTP	99	Response: 150 Opening data channel for file transfer.
44	13.818409	192.168.1.15	192.168.1.5	TCP	66	55837->20 [SYN, ACK] Seq=2377334290 Ack=3719615816 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
45	13.818653	192.168.1.5	192.168.1.15	TCP	54	20->55837 [ACK] Seq=3719615816 Ack=2377334291 Win=131100 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.0... .0.....
0020 01 05 da 1c 00 15 92 fd a7 32 2b 4a 2d 85 50 18 ..... .2+-.P.
0030 7f bd a9 bf 00 00 50 4f 52 54 20 31 39 32 2c 31 .....PO RT 192,1
0040 36 38 2c 31 2c 31 35 2c 32 31 38 2c 32 39 0d 0a 68,1,15, 218,29..

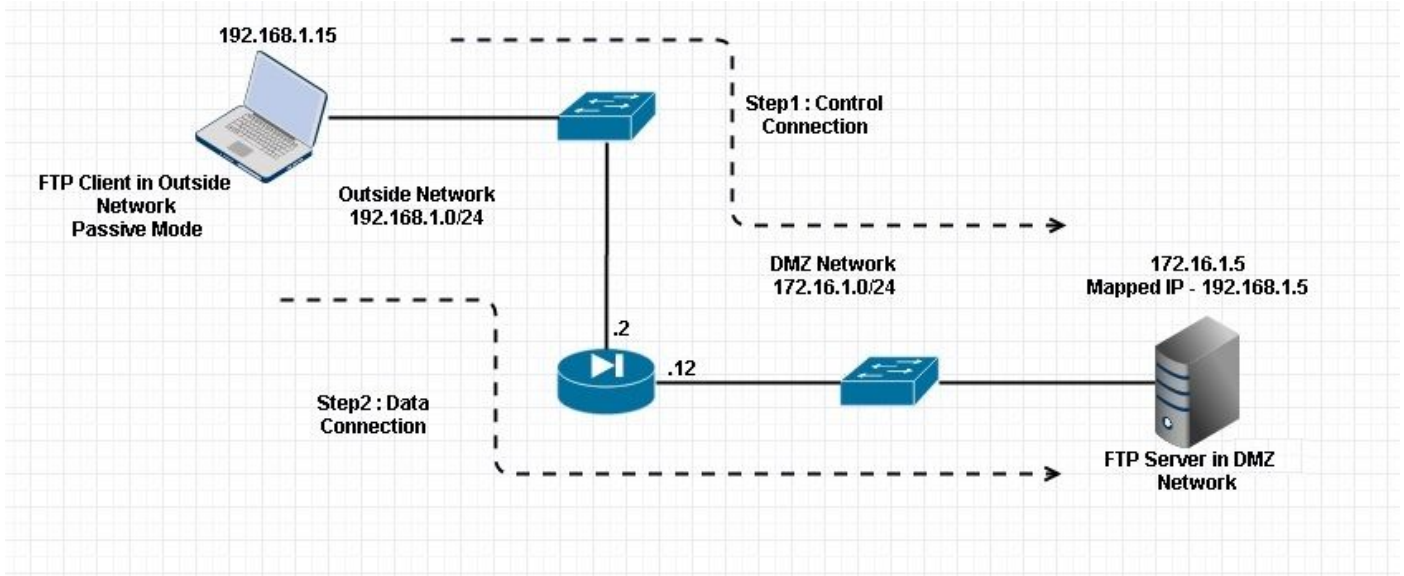
```

Ici, le client exécute le client en mode actif 192.168.1.15 et initie la connexion au serveur dans la zone DMZ sur le port 21. Le client envoie ensuite la commande port avec six valeurs de tuple au serveur pour se connecter à ce port dynamique spécifique. Le serveur lance alors la connexion de données avec le port source 20.

Scénario 4 . Client FTP en mode passif

Client du réseau externe de l'ASA et serveur du réseau DMZ.

Diagramme du réseau



Connexion

<#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
```

Capturez l'interface DMZ comme illustré dans cette image.

No.	Time	Source	Destination	Protocol	Length	Info
15	23.516688	192.168.1.15	172.16.1.5	TCP	66	60070->21 [SYN] Seq=3728695688 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
16	23.517161	172.16.1.5	192.168.1.15	TCP	66	21->60070 [SYN, ACK] Seq=397133843 Ack=3728695689 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	23.517527	192.168.1.15	172.16.1.5	TCP	54	60070->21 [ACK] Seq=3728695689 Ack=397133844 Win=131100 Len=0
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/projects/filezilla/
21	23.522196	192.168.1.15	172.16.1.5	TCP	54	60070->21 [ACK] Seq=3728695689 Ack=397133931 Win=131012 Len=0
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 directory.
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 (172,16,1,5,241,85)
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=1380 WS=4 SACK_PERM=1
34	23.544229	172.16.1.5	192.168.1.15	TCP	66	61781->60071 [SYN, ACK] Seq=4186544816 Ack=4174881932 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
35	23.544518	192.168.1.15	172.16.1.5	TCP	54	60071->61781 [ACK] Seq=4186544817 Win=262140 Len=0
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=4186544817 Win=262140 Len=0
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
<pre> 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: 60070 (60070), 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 0e 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).. </pre>						

Capturez l'interface externe comme illustré dans cette image.

No.	Time	Source	Destination	Protocol	Length	Info
29	23.528818	192.168.1.15	192.168.1.5	TCP	66	60070->21 [SYN] Seq=2627142457 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
30	23.529413	192.168.1.5	192.168.1.15	TCP	66	21->60070 [SYN, ACK] Seq=1496461807 Ack=2627142458 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
31	23.529749	192.168.1.15	192.168.1.5	TCP	54	60070->21 [ACK] Seq=2627142458 Ack=1496461808 Win=131100 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=131012 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 WS=4 SACK_PERM=1
48	23.556466	192.168.1.5	192.168.1.15	TCP	66	61781->60071 [SYN, ACK] Seq=1047360618 Ack=3795016103 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
49	23.556740	192.168.1.15	192.168.1.5	TCP	54	60071->61781 [ACK] Seq=3795016103 Ack=1047360619 Win=262140 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=262140 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
<pre> Frame 45: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) Ethernet II, Src: Cisco_c9:92:88 (00:19:e8:c9:92:88), Dst: Vmware_ad:24:76 (00:50:56:ad:24:76) Internet Protocol Version 4, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.15 (192.168.1.15) Transmission Control Protocol, Src Port: 21 (21), Dst Port: 60070 (60070), Seq: 1496462070, Ack: 2627142506, Len: 48 File Transfer Protocol (FTP) 227 Entering Passive Mode (192,168,1,5,241,85)\r\n Response code: Entering Passive Mode (227) Response arg: Entering Passive Mode (192,168,1,5,241,85) 0030 01 ff c3 f5 00 00 32 32 37 20 45 6e 74 65 72 6922 7 Enteri 0040 0e 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 38 2c 31 2c 35 2c 32 34 31 (192,168,1,5,241, 0060 2c 38 35 29 0d 0a 85).. </pre>						

Configurez l'inspection de base de l'application FTP

Par défaut, la configuration inclut une stratégie qui correspond à tout le trafic de l'inspection d'application par défaut et applique une inspection au trafic sur toutes les interfaces (une stratégie globale). Le trafic de l'inspection d'application par défaut inclut le trafic vers les ports par défaut pour chaque protocole.

Vous pouvez seulement appliquer une stratégie globale, ainsi si vous voulez modifier la stratégie globale, par exemple, pour appliquer l'inspection aux ports non standard, ou pour ajouter des inspections qui ne sont pas activées par défaut, vous devez soit modifier la stratégie par défaut soit la désactiver et en appliquer une nouvelle. Pour une liste de tous les ports par défaut, référez-vous à la [Stratégie d'inspection par défaut](#).

1. Exécutez la commande `policy-map global_policy`.

```
<#root>
ASA(config)#
policy-map global_policy
```

2. Exécutez la commande `class inspection_default`.

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

3. Exécutez la commande `inspect FTP`.

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

4. Il y a une option d'utilisation de la commande `inspect FTP strict`. Cette commande augmente la sécurité des réseaux protégés en empêchant un navigateur Web d'envoyer des commandes incluses dans les requêtes FTP.

Après que vous activez l'option `strict` sur une interface, l'inspection de FTP impose ce comportement:

- Une commande FTP doit être reconnue avant que l'Appliance de sécurité autorise une nouvelle commande
- L'Appliance de sécurité dépose une connexion qui envoie des commandes incluses
- Les commandes 227 et PORT sont vérifiées pour s'assurer qu'elles n'apparaissent pas dans une chaîne d'erreur



Avertissement : l'utilisation de l'option `strict` peut entraîner la défaillance des clients FTP qui ne sont pas strictement conformes aux RFC FTP. Consultez [Utiliser l'option](#)



[stricte pour plus d'informations sur l'utilisation de l'option stricte.](#)

Configuration de l'inspection du protocole FTP sur le port TCP non standard

Vous pouvez configurer l'inspection du protocole FTP pour les ports TCP non standard avec ces lignes de configuration (remplacez XXXX par le nouveau numéro de port) :

```
<#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
```

Vérifier

Afin de s'assurer que la configuration a bien été prise, exécutez la commande `show service-policy`. En outre, limitez le résultat à l'inspection FTP en exécutant la commande `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

L'inspection TFTP est activée par défaut.

L'Appliance de sécurité inspecte le trafic TFTP et crée dynamiquement des connexions et des routages de traduction s'il y a lieu, pour permettre le transfert de fichiers entre un client TFTP et le serveur. En particulier, le moteur d'inspection inspecte les requêtes lues TFTP (RRQ), écrit des

requêtes de routage (WRQ) et les notifications d'erreur (ERREUR).

Un canal auxiliaire dynamique et une traduction PAT s'il y a lieu, sont alloués sur une réception d'un RRQ ou d'un WRQ valide. Ce canal auxiliaire est ultérieurement utilisé par TFTP pour le transfert de fichiers ou la notification d'erreur.

Seul le serveur TFTP peut lancer le trafic de routage au-dessus du canal auxiliaire, et tout au plus un canal auxiliaire inachevé peut exister entre le client TFTP et le serveur. Une notification d'erreur du serveur ferme le canal auxiliaire.

L'inspection TFTP doit être activée si la fonction Fstatic PAT est utilisée pour rediriger le trafic TFTP.

Configurez l'inspection de base de l'application TFTP

Par défaut, la configuration inclut une stratégie qui correspond à tout le trafic de l'inspection d'application par défaut et applique une inspection au trafic sur toutes les interfaces (une stratégie globale). Le trafic de l'inspection d'application par défaut inclut le trafic vers les ports par défaut pour chaque protocole.

Vous ne pouvez appliquer qu'une seule stratégie globale. Par conséquent, si vous voulez modifier la stratégie globale, par exemple, pour appliquer l'inspection à des ports non standard, ou pour ajouter des inspections qui ne sont pas activées par défaut, vous devez soit modifier la stratégie par défaut, soit la désactiver et en appliquer une nouvelle. Pour une liste de tous les ports par défaut, référez-vous à la [Stratégie d'inspection par défaut](#).

1. Exécutez la commande `policy-map global_policy`.

```
<#root>
ASA(config)#
policy-map global_policy
```

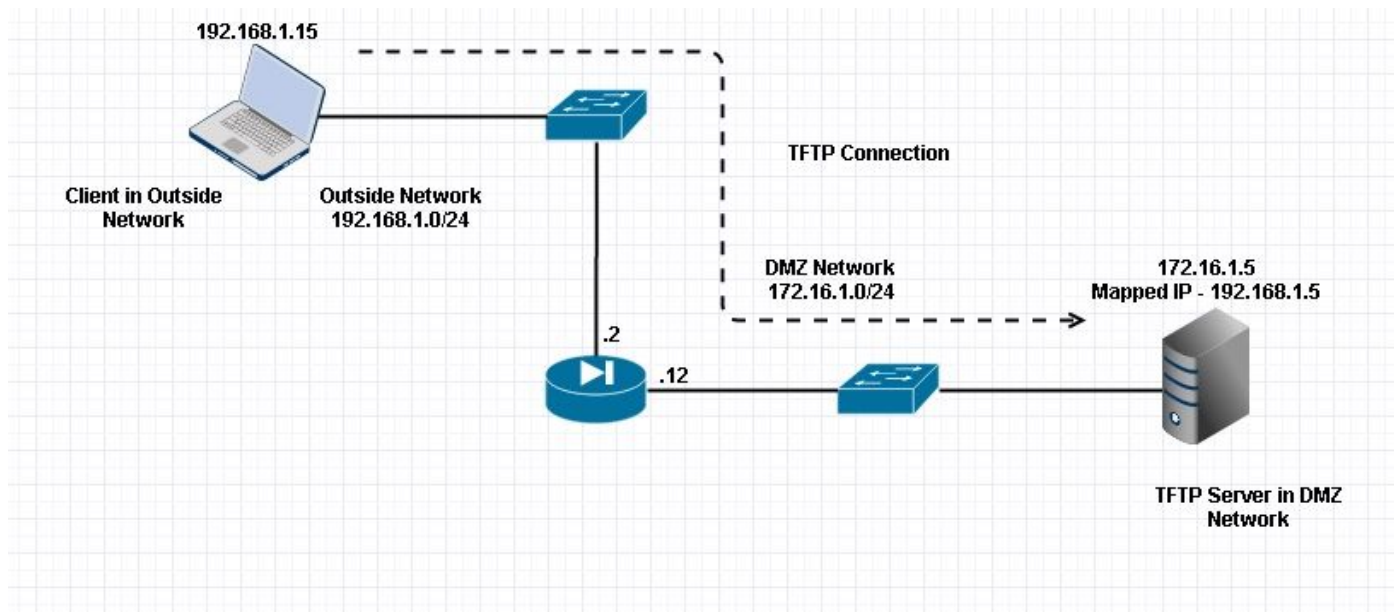
2. Exécutez la commande `class inspection_default`.

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

3. Exécutez la commande `inspect TFTP`.

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

Diagramme du réseau



Ici, le client est configuré dans Réseau externe. Le serveur TFTP est placé dans le réseau DMZ. Le serveur est mappé à l'adresse IP 192.168.1.5 qui se trouve dans le sous-réseau externe.

Exemple de configuration :

```
<#root>
ASA(config)#
show running-config

ASA Version 9.1(5)
!
hostname ASA
domain-name corp. com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface GigabitEthernet0/0
 nameif Outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet0/1
```

```
nameif DMZ
security-level 50
ip address 172.16.1.12 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
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)#
```

Vérifier

Afin de s'assurer que la configuration a bien été prise, exécutez la commande `show service-policy`. En outre, limitez le résultat à l'inspection TFTP uniquement en exécutant la commande `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#
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Packet Tracer

Client dans le réseau interne

<#root>

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

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

-----Omitted-----

Phase: 5

Type: INSPECT

Subtype: inspect-ftp

Result: ALLOW

Config:

```
class-map inspection_default
  match default-inspection-traffic
policy-map global_policy
  class inspection_default
    inspect ftp
```

```
service-policy global_policy global
```

Additional Information:

Forward Flow based lookup yields rule:

in id=0x76d9a120, priority=70, domain=inspect-ftp, deny=false

hits=2, user_data=0x76d99a30, cs_id=0x0, use_real_addr, flags=0x0, protocol=6

src ip/id=0.0.0.0, mask=0.0.0.0, port=0

dst ip/id=0.0.0.0, mask=0.0.0.0, port=21, dscp=0x0

input_ifc=inside, output_ifc=any

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

```
object network obj-172.16.1.5
```

```
  nat (inside,outside) static 192.168.1.5
```

Additional Information:

NAT divert to egress interface DMZ

translate 172.16.1.5/21 to 192.168.1.5/21

Phase: 7

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
object network obj-172.16.1.5
```

```
nat (inside,outside) static 192.168.1.5
```

Additional Information:

Forward Flow based lookup yields rule:

```
out id=0x76d6e308, priority=6, domain=nat-reverse, deny=false  
hits=15, user_data=0x76d9ef70, cs_id=0x0, use_real_addr, flags=0x0, protocol=0  
src ip/id=0.0.0.0, mask=0.0.0.0, port=0  
dst ip/id=172.16.1.5, mask=255.255.255.255, port=0, dscp=0x0  
input_ifc=inside, output_ifc=outside
```

----Omitted----

Result:

input-interface:

inside

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

Outside

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

Client dans le réseau externe

<#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

Comme on le voit dans les deux traceurs de paquets, le trafic atteint leurs instructions NAT respectives et la politique d'inspection FTP. Ils laissent également leurs interfaces requises.

Pendant le dépannage, vous pouvez essayer de capturer les interfaces d'entrée et de sortie ASA et voir si la réécriture de l'adresse IP intégrée ASA fonctionne correctement et vérifier la connexion si le port dynamique est autorisé sur ASA.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.