FTP/TFTPサービスの設定：ASA 9.X

内容

はじめに

このドキュメントでは、ASA上のさまざまなFTPおよびTFTPインスペクションシナリオ、ASA FTP/TFTPインスペクションの設定、および基本的なトラブルシューティングについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 必須インターフェイス間での基本的な通信
- DMZ ネットワーク内に配置された FTP サーバの設定

使用するコンポーネント

このドキュメントでは、適応型セキュリティ アプライアンス (ASA) でのさまざまな FTP および TFTP インスペクション シナリオについて説明します。さらに、ASA FTP/TFTP インスペクション設定と基本的なトラブルシューティングについても取り上げます。

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 9.1(5) ソフトウェアイメージを実行する ASA 5500 または ASA 5500-X シリーズ ASA
- 任意の FTP サーバ
- 任意の FTP クライアント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

セキュリティ アプライアンスは、アダプティブ セキュリティ アルゴリズム機能によって、アプリケーション インスペクションをサポートしています。

アダプティブ セキュリティ アルゴリズムで使用されるアプリケーションのステートフル インスペクションによって、セキュリティ アプライアンスは、ファイアウォールを通過する各コネクションをトラッキングし、これらのコネクションが有効であることを確認します。

また、ファイアウォールはステートフル インスペクションによってコネクションの状態も監視し、状態テーブルに情報を格納します。

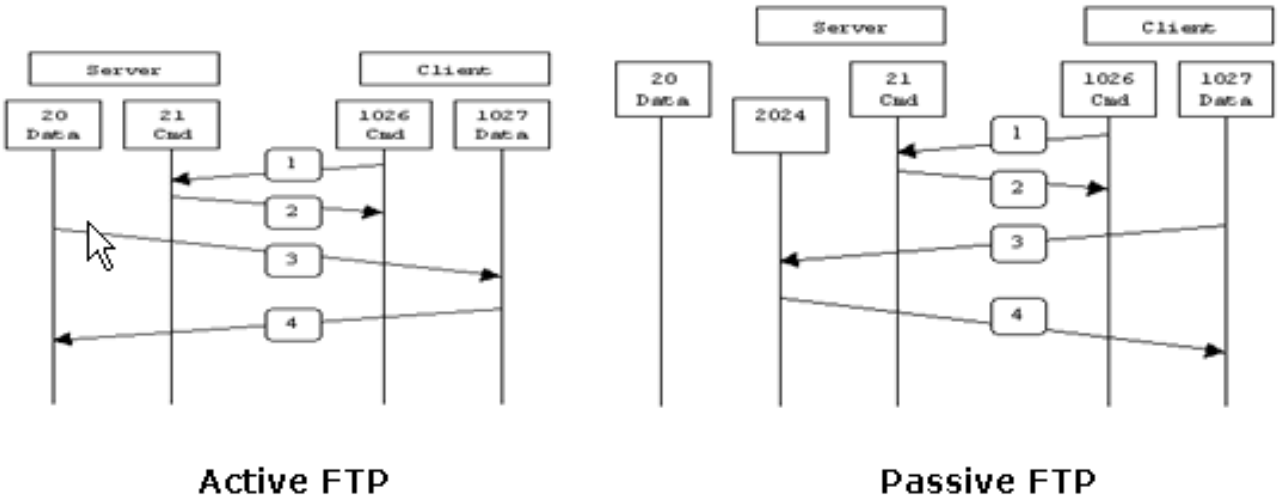
管理者定義のルールに加えて状態テーブルを使用することで、フィルタリングの決定が、過去にファイアウォールを通過したパケットによって確立されたコンテキスト情報に基づいて行われるようになります。

アプリケーション インスペクションの実装は、次の処理で構成されています。

- トラフィックを識別する
- トラフィックに検査を適用する
- インターフェイス上での検査をアクティブ化する

図のように、FTP には次の 2 つの形式があります。

- アクティブ モード
- パッシブ モード



Active FTP **Passive FTP**

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

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

アクティブ FTP

アクティブ FTP モードでは、クライアントがランダムな非特権ポート（N>1023）から FTP サーバのコマンド ポート（21）へ接続します。次に、クライアントによるポート N>1023 のリスニングが開始され、FTP コマンド ポート N>1023 が FTP サーバへ送信されます。次に、サーバによってローカルのデータ ポート（ポート 20）からクライアントの指定されたデータ ポートへ再度接続が行われます。

パッシブ FTP

パッシブ FTP モードでは、クライアントとサーバ間の接続は、どちらの方向でもクライアントによって開始されます。そのため、ファイアウォールでサーバからクライアントへの着信データ ポート接続がフィルタリングされるという問題が解決されます。FTP 接続が開かれると、クライアントによって 2 つのランダムな非特権ポートがローカルに開かれます。最初のポートからポート 21 上でサーバに接続されます。ただし、port コマンドを発行して、そのデータポートへのサーバの接続を許可する代わりに、クライアントから PASV コマンドが発行されます。この結果、サーバによってランダムな非特権ポート（P>1023）が開かれ、port P コマンドがクライアントへ送信されます。次に、データを転送するために、クライアントによってサーバ上でポート N>1023 からポート P への接続が開始されます。セキュリティ アプライアンスで inspection コマンドが設定されていない場合、Inside ユーザからのアウトバウンドに向けた FTP はパッシブ モードでのみ動作します。また、FTP サーバへのインバウンドに向けた Outside ユーザは、アクセスを拒否さ

れます。

TFTP

RFC 1350 で記述されるように、TFTP は、TFTP サーバとクライアントの間でファイルの読み書きを行うための単純なプロトコルです。TFTP では、UDP ポート 69 が使用されます。

高度なプロトコル処理

FTP インスペクションが必要な理由

一部のアプリケーションでは、Cisco セキュリティ アプライアンスのアプリケーション インスペクション機能による特別な処理が必要です。これらのタイプのアプリケーションでは、通常、IP アドレッシング情報がユーザ データ パケットに埋め込まれるか、動的に割り当てられたポートにセカンダリ チャネルが開かれます。アプリケーション検査機能は、ネットワークアドレス変換（NAT）と連動し、埋め込まれたアドレッシング情報の場所を識別するために役立ちます。

埋め込まれたアドレッシング情報の識別に加えて、アプリケーション検査機能ではセッションが監視され、セカンダリチャネルのポート番号が判断されます。多くのプロトコルによってセカンダリの TCP ポートまたは UDP ポートが開かれ、パフォーマンスが向上します。既知のポートで初期セッションが使用され、動的に割り当てられたポート番号がネゴシエーションされます。

アプリケーション インスペクション機能では、これらのセッションが監視され、動的なポート割り当てが識別され、特定のセッションの間にこれらのポートでのデータ交換が許可されます。このような動作は、マルチメディアおよび FTP のアプリケーションでみられます。

FTP インスペクションがセキュリティ アプライアンスで有効になっていない場合、この要求は廃棄され、FTP セッションで要求されたデータが転送されません。

FTP インスペクションがセキュリティ アプライアンスで有効になっていれば、セキュリティ アプライアンスによってコントロール チャネルが監視され、データ チャネルを開く要求が認識されます。FTP プロトコルによって、データ チャネル ポート番号の詳細がコントロール チャネル トラフィックに埋め込まれると、セキュリティ アプライアンスによるデータ ポート変更に対するコントロール チャネルのインスペクションが必要になります。

ASA が要求を認識すると、データ チャネル トラフィック用の窓口が一時的に開かれますが、これはセッションの間中、開かれたままです。この方法で、FTP インスペクション機能によってコントロール チャネルが監視され、データ ポートの割り当てが識別され、セッションの間中、データ ポートでのデータ交換が許可されます。

ASA は、デフォルトではグローバル インスペクション クラスマップによって FTP トラフィックのポート 21 の接続を検査します。また、セキュリティ アプライアンスは、アクティブとパッシブの FTP セッションの間での差異も認識します。

FTP セッションでパッシブ FTP データ転送がサポートされる場合、inspect ftp コマンドにより、ASA はユーザからのデータ ポート要求を認識し、1023 より大きい番号の新規データ ポートを開きます。

inspect ftp コマンドは、FTP セッションを検査して、次の 4 つのタスクを実行します。

- 動的なセカンダリ データ接続の準備
- FTP コマンド応答シーケンスの追跡
- 監査証跡の生成
- NAT を使用した埋め込み IP アドレスの変換

FTP アプリケーション インスペクションによって、FTP データ転送のセカンダリ チャネルが準備されます。ファイルのアップロード、ファイルのダウンロード、またはディレクトリ リストのイベントに応答してチャネルが割り当てられますが、これらのチャネルは事前にネゴシエートされる必要があります。ポートは、PORT コマンド、または PASV (227) コマンドを介してネゴシエートされます。

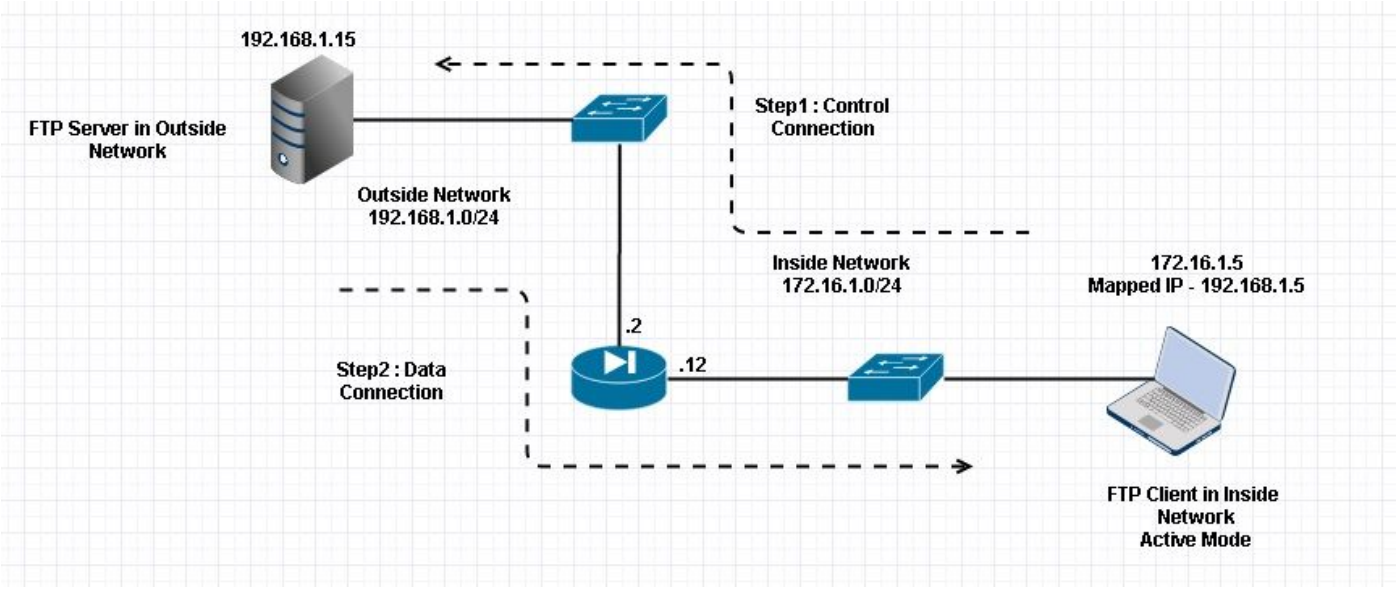
コンフィギュレーション

注：すべてのネットワークシナリオは、ASAでFTPインスペクションが有効になっている状態で説明されています。

シナリオ 1.アクティブ モードに設定された FTP クライアント

クライアントは ASA の内部ネットワークに接続され、サーバは外部ネットワークに配置されます。

ネットワーク図



注：この設定で使用されているIPアドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。

この図に示すように、このシナリオで使用されるネットワーク設定では、ASA のクライアントは内部ネットワークにあり、IP 172.16.1.5 が割り当てられています。サーバは外部ネットワークに

あり、IP 192.168.1.15 が割り当てられています。クライアントのマッピング IP 192.168.1.5 は外部ネットワークにあります。

FTP インスペクションによってダイナミック ポート チャネルが開かれるため、外部インターフェイスのアクセス リストを許可する必要はありません。

設定例：

<#root>

```
 ASA Version 9.1(5)
!
hostname ASA
domain-name corp. com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface GigabitEthernet0/0
  nameif Outside
  security-level 0
  ip address 192.168.1.2 255.255.255.0
 !
 interface GigabitEthernet0/1
  nameif Inside
  security-level 50
  ip address 172.16.1.12 255.255.255.0
 !
 interface GigabitEthernet0/2
  shutdown
  no nameif
  no security-level
  no ip address
 !
 interface GigabitEthernet0/3
  shutdown
  no nameif
  no security-level
  no ip address
 !
 interface Management0/0
  management-only
  shutdown
  no nameif
  no security-level
  no ip address


 !--- Output is suppressed.


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


object network obj-172.16.1.5
 subnet 172.16.1.0 255.255.255.0
```

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


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

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


policy-map global_policy


class inspection_default

  inspect dns preset_dns_map


inspect ftp


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

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


service-policy global_policy global

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

確認

Connection

<#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

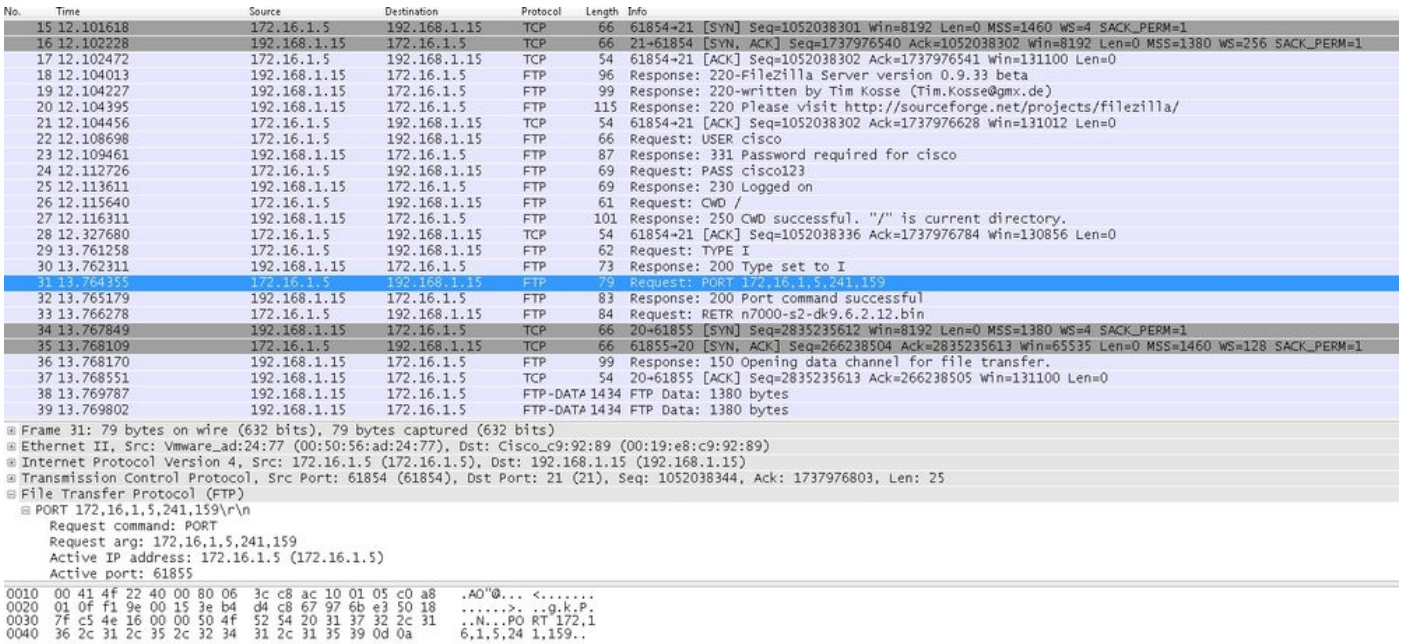
```
 TCP Outside
```

192.168.1.15:21 inside 172.16.1.5:61854

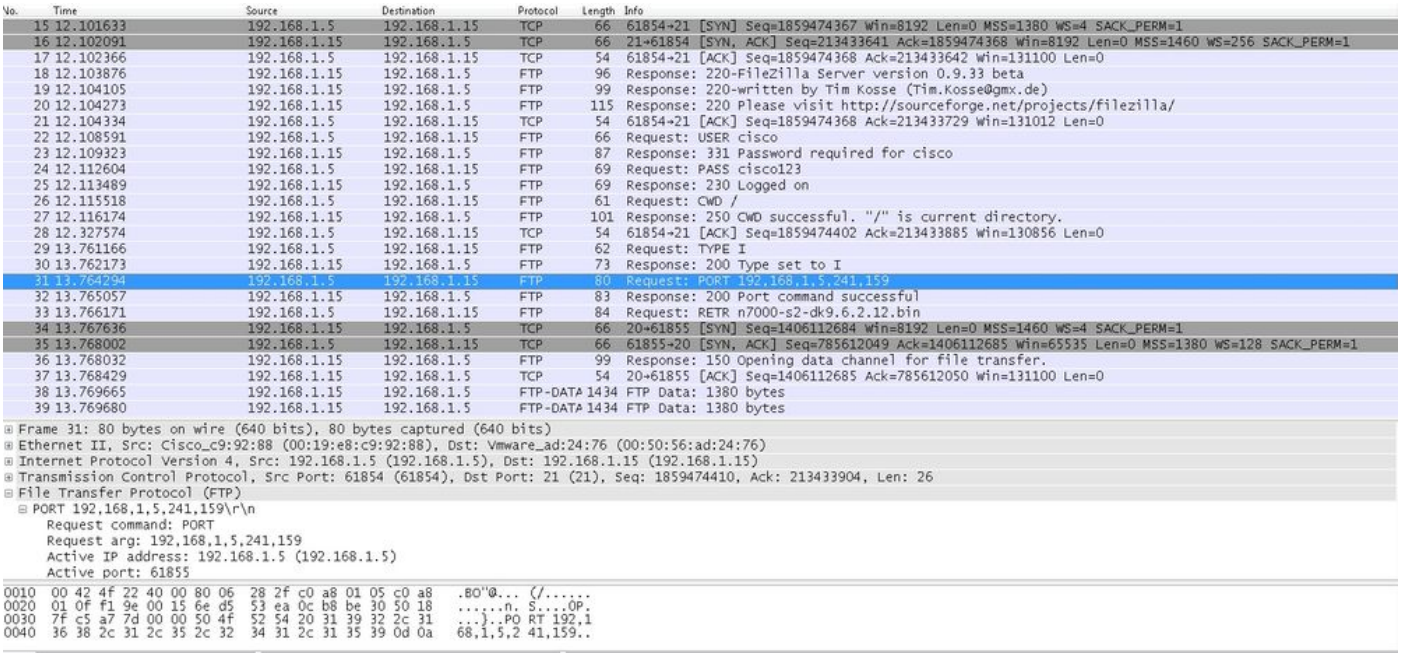
```
, idle 0:00:00, bytes 434, flags UIO
```

内部ネットワークに位置するクライアントが、送信元ポート 61854 を使用して宛先ポート 21 への接続を開始します。続いて、クライアントは 6 タプル値を設定したポート コマンドを送信します。次に、サーバは送信元ポート 20 を使用してセカンダリ/データ接続を開始します。宛先ポートは、以下のキャプチャの後に説明する手順で計算されます。

次の図のように、内部インターフェイスをキャプチャします。



次の図のように、外部インターフェイスをキャプチャします。



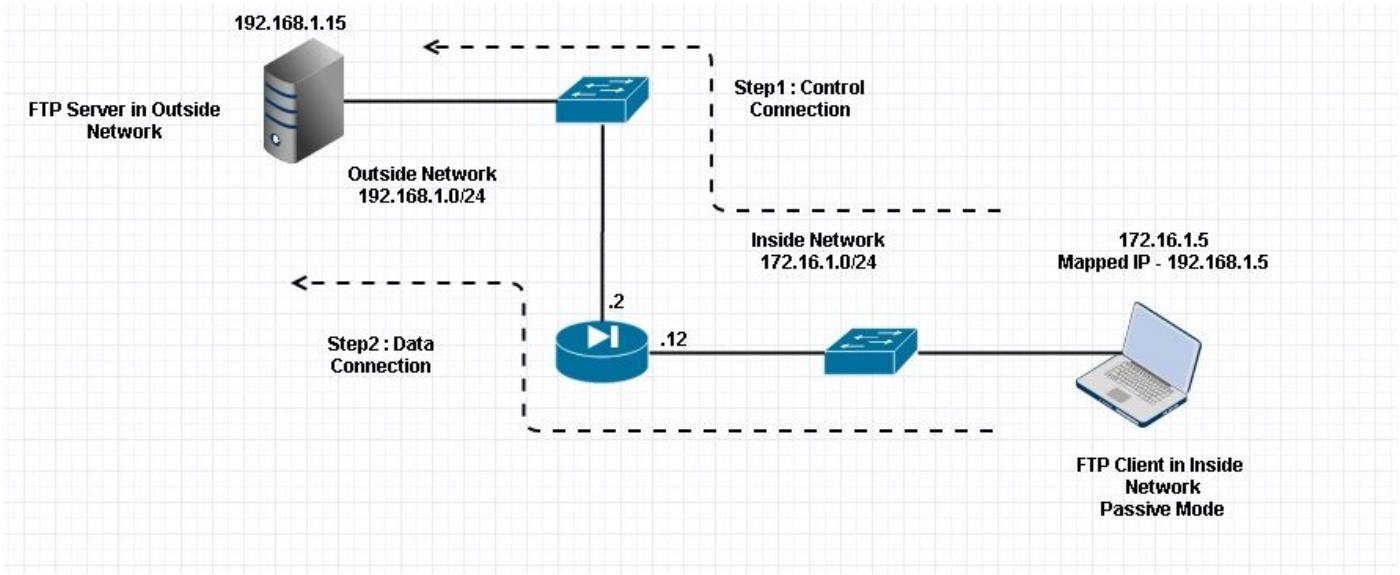
ポートの値は、6 タプルのうちの最後の 2 つを使用して計算されます。左の 4 タプルは IP アドレスであり、2 つのタプルがポート用です。次の図のように、IP アドレスは 192.168.1.5 であり、241 * 256 + 159 = 61855 となります。

上記のキャプチャには、FTP インスペクションが有効になると、ポート コマンドで使用する値が変更されることが示されています。「内部インターフェイスのキャプチャ」には、IP の実際の値と、サーバ用クライアントがデータ チャネル用クライアントに接続するために送信したポートが示されています。「外部インターフェイスのキャプチャ」には、マッピングされたアドレスが示されています。

シナリオ 2.パッシブモードに設定されたFTPクライアント

クライアントは ASA の内部ネットワークに配置され、サーバは外部ネットワークに配置されます。

ネットワーク図



Connection

<#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.

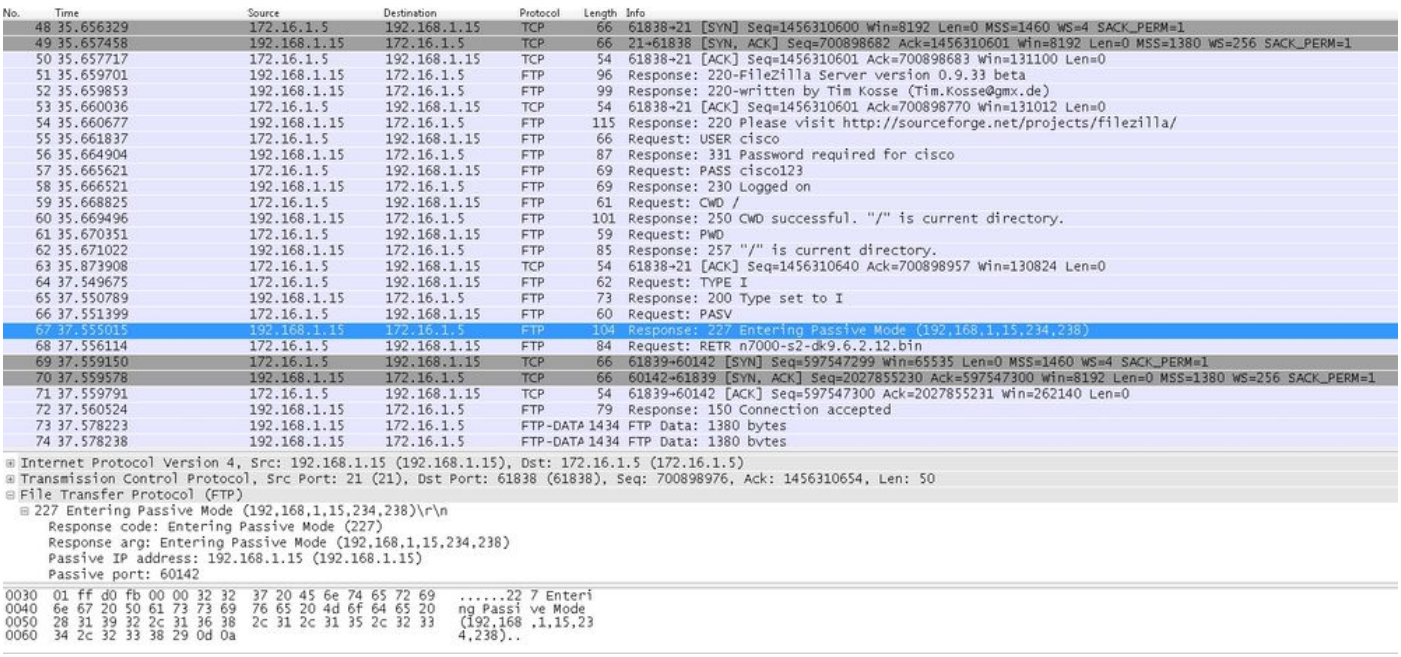
```
TCP Outside
```

192.168.1.15:21 inside 172.16.1.5:61838

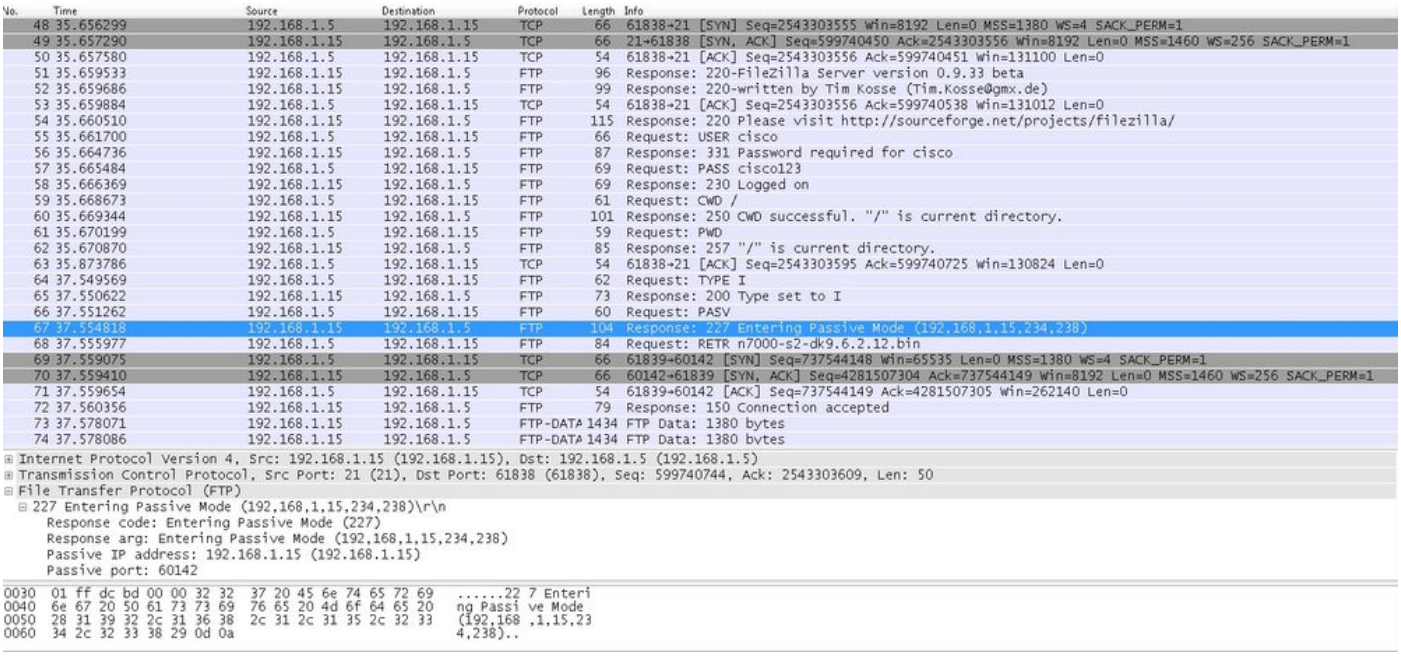
```
, idle 0:00:00, bytes 451, flags UIO
```

内部ネットワークに位置するクライアントが、送信元ポート 61838 と宛先ポート 21 で接続を開始します。これはパッシブ FTP であるため、クライアントが両方向の接続を開始します。そのため、クライアントが PASV コマンドを送信した後、サーバが自身の 6 タプル値で応答すると、クライアントはそのデータ接続用ソケットに接続します。

次の図のように、内部インターフェイスをキャプチャします。



次の図のように、外部インターフェイスをキャプチャします。



No.	Time	Source	Destination	Protocol	Length	Info
48	35.656299	192.168.1.5	192.168.1.15	TCP	66	61838→21 [SYN] Seq=2543303555 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
49	35.657290	192.168.1.15	192.168.1.5	TCP	66	21→61838 [SYN, ACK] Seq=599740450 Ack=2543303556 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
50	35.657580	192.168.1.5	192.168.1.15	TCP	54	61838→21 [ACK] Seq=2543303556 Ack=599740451 Win=131100 Len=0
51	35.659533	192.168.1.15	192.168.1.5	FTP	96	Response: 220-FileZilla Server version 0.9.33 beta
52	35.659686	192.168.1.15	192.168.1.5	FTP	99	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
53	35.659884	192.168.1.5	192.168.1.15	TCP	54	61838→21 [ACK] Seq=2543303556 Ack=599740538 Win=131012 Len=0
54	35.660510	192.168.1.15	192.168.1.5	FTP	115	Response: 220 Please visit http://sourceforge.net/projects/filezilla/
55	35.661700	192.168.1.5	192.168.1.15	FTP	66	Request: USER cisco
56	35.664736	192.168.1.15	192.168.1.5	FTP	87	Response: 331 Password required for cisco
57	35.665484	192.168.1.5	192.168.1.15	FTP	69	Request: PASS cisco123
58	35.666369	192.168.1.15	192.168.1.5	FTP	69	Response: 230 Logged on
59	35.668673	192.168.1.5	192.168.1.15	FTP	61	Request: CWD /
60	35.669344	192.168.1.15	192.168.1.5	FTP	101	Response: 250 CWD successful. "/" is current directory.
61	35.670199	192.168.1.5	192.168.1.15	FTP	59	Request: PWD
62	35.670870	192.168.1.15	192.168.1.5	FTP	85	Response: 257 "/" is current directory.
63	35.873786	192.168.1.5	192.168.1.15	TCP	54	61838→21 [ACK] Seq=2543303595 Ack=599740725 Win=130824 Len=0
64	37.549569	192.168.1.5	192.168.1.15	FTP	62	Request: TYPE I
65	37.550622	192.168.1.15	192.168.1.5	FTP	73	Response: 200 Type set to I
66	37.551262	192.168.1.5	192.168.1.15	FTP	60	Request: PASV
67	37.554818	192.168.1.15	192.168.1.5	FTP	104	Response: 227 Entering Passive Mode (192,168,1,15,234,238)
68	37.555977	192.168.1.5	192.168.1.15	FTP	84	Request: RETR n7000-s2-dk9.6.2.12.bin
69	37.559075	192.168.1.5	192.168.1.15	TCP	66	61839→60142 [SYN] Seq=737544148 Win=65535 Len=0 MSS=1380 WS=4 SACK_PERM=1
70	37.559410	192.168.1.15	192.168.1.5	TCP	66	60142→61839 [SYN, ACK] Seq=4281507304 Ack=737544149 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
71	37.559654	192.168.1.5	192.168.1.15	TCP	54	61839→60142 [ACK] Seq=737544149 Ack=4281507305 Win=262140 Len=0
72	37.560356	192.168.1.15	192.168.1.5	FTP	79	Response: 150 Connection accepted
73	37.578071	192.168.1.15	192.168.1.5	FTP-DATA	1434	FTP Data: 1380 bytes
74	37.578086	192.168.1.15	192.168.1.5	FTP-DATA	1434	FTP Data: 1380 bytes

```
⊞ Internet Protocol Version 4, Src: 192.168.1.15 (192.168.1.15), Dst: 192.168.1.5 (192.168.1.5)
⊞ Transmission Control Protocol, Src Port: 21 (21), Dst Port: 61838 (61838), Seq: 599740744, Ack: 2543303609, Len: 50
⊟ File Transfer Protocol (FTP)
  ⊟ 227 Entering Passive Mode (192,168,1,15,234,238)\r\n
      Response code: Entering Passive Mode (227)
      Response arg: Entering Passive Mode (192,168,1,15,234,238)
      Passive IP address: 192.168.1.15 (192.168.1.15)
      Passive port: 60142
```

```
0030  01 ff dc bd 00 00 32 32  37 20 45 6e 74 65 72 69   ......22 7 Enteri
0040  6e 67 20 50 61 73 73 69  76 65 20 4d 6f 64 65 20   ng Passi ve Mode
0050  28 31 39 32 2c 31 36 38  2c 31 2c 31 35 2c 32 33   (192,168 ,1,15,23
0060  34 2c 32 33 38 29 0d 0a                           4,238)..
```

ポートの計算方法は変わりません。

前述のとおり、FTP インスペクションが有効になっていると、ASA は埋め込み IP 値を書き換えます。また、データ接続用にダイナミックポートチャネルが開きます。

接続の詳細を次に示します。 FTPインスペクションが無効

Connection:

<#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
```

FTP インスペクションを行わない場合、ASA は port コマンドの送信を繰り返し再試行しても応答はありません。外部で受信するのは、NAT が適用された IP ではなく、元の IP のポートであるためです。同じことがダンプに示されています。

FTP インスペクションを無効にするには、コンフィギュレーション ターミナル モードで no fixup

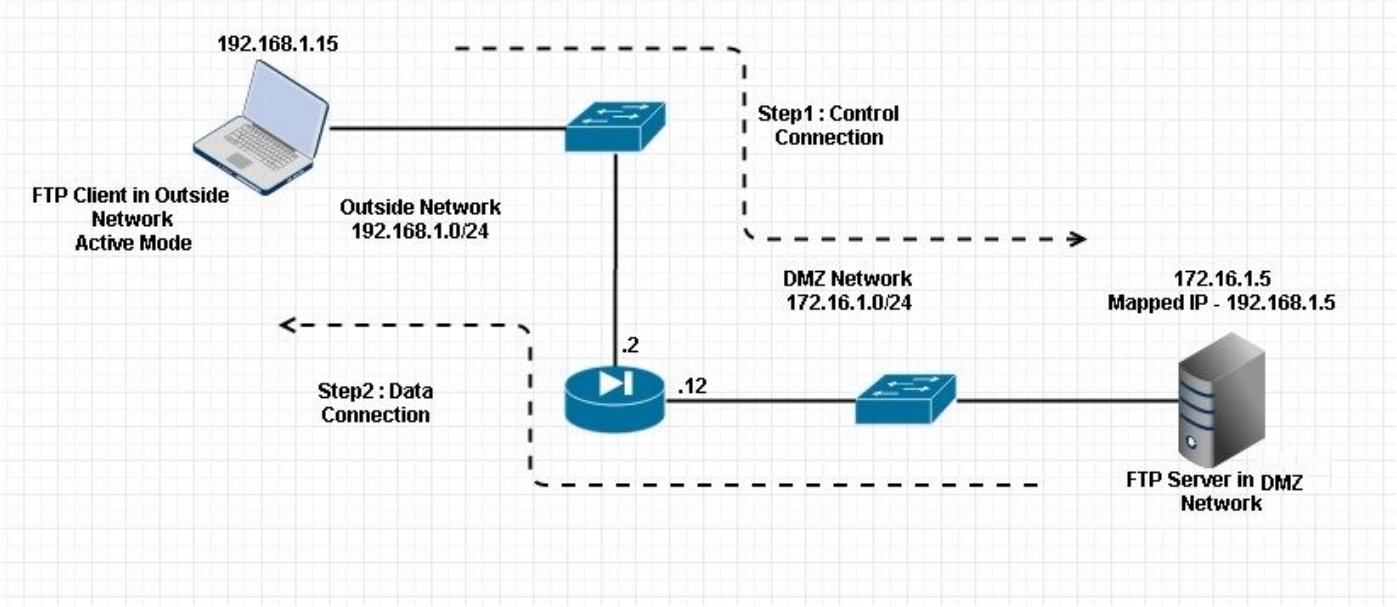
protocol ftp 21 コマンドを使用します。

FTP インスペクションを使用しない場合、クライアントが内部ネットワークに位置していないと、PASV コマンドは機能しません。両方向の接続は内部から開始されるのに、埋め込むべき port コマンドが内部から送信されないためです。

シナリオ 3.アクティブ モードに設定された FTP クライアント

クライアントは ASA の外部ネットワークに配置され、サーバは DMZ ネットワークに配置されます。

ネットワーク図



設定：

<#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)#
```

確認

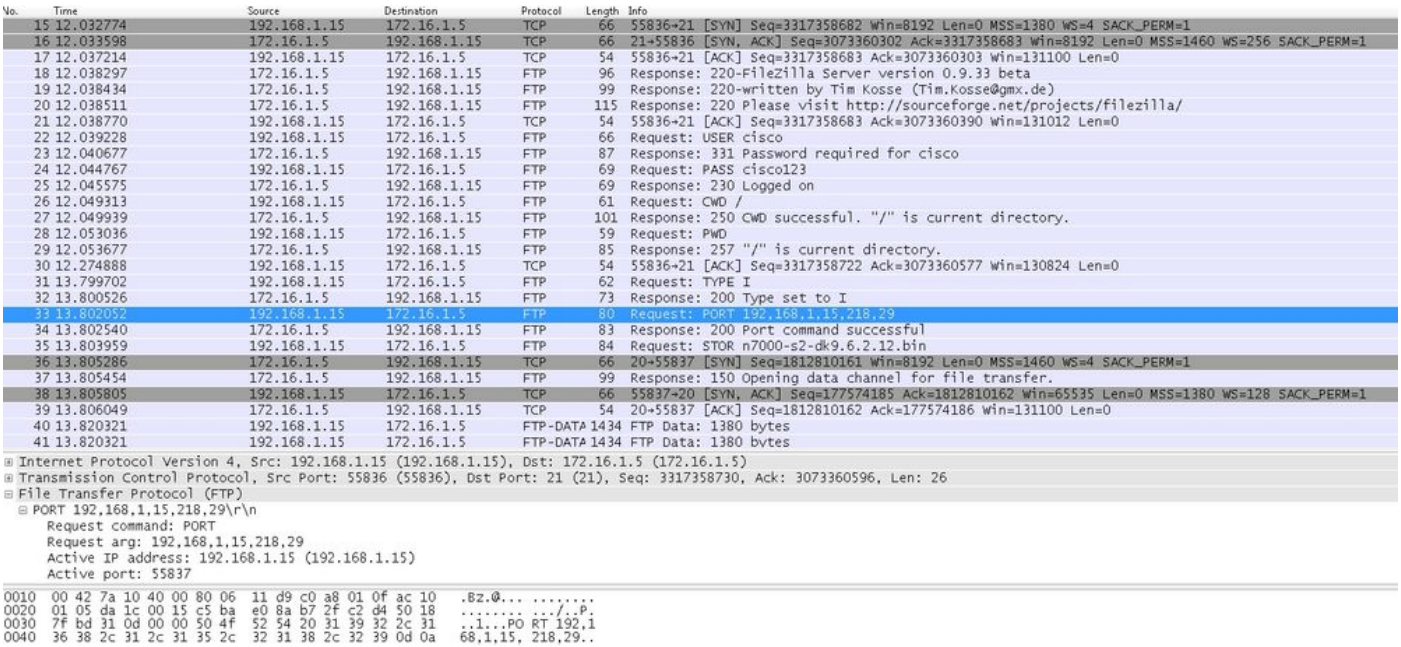
Connection:

<#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
```

次の図のように、DMZ インターフェイスをキャプチャします。

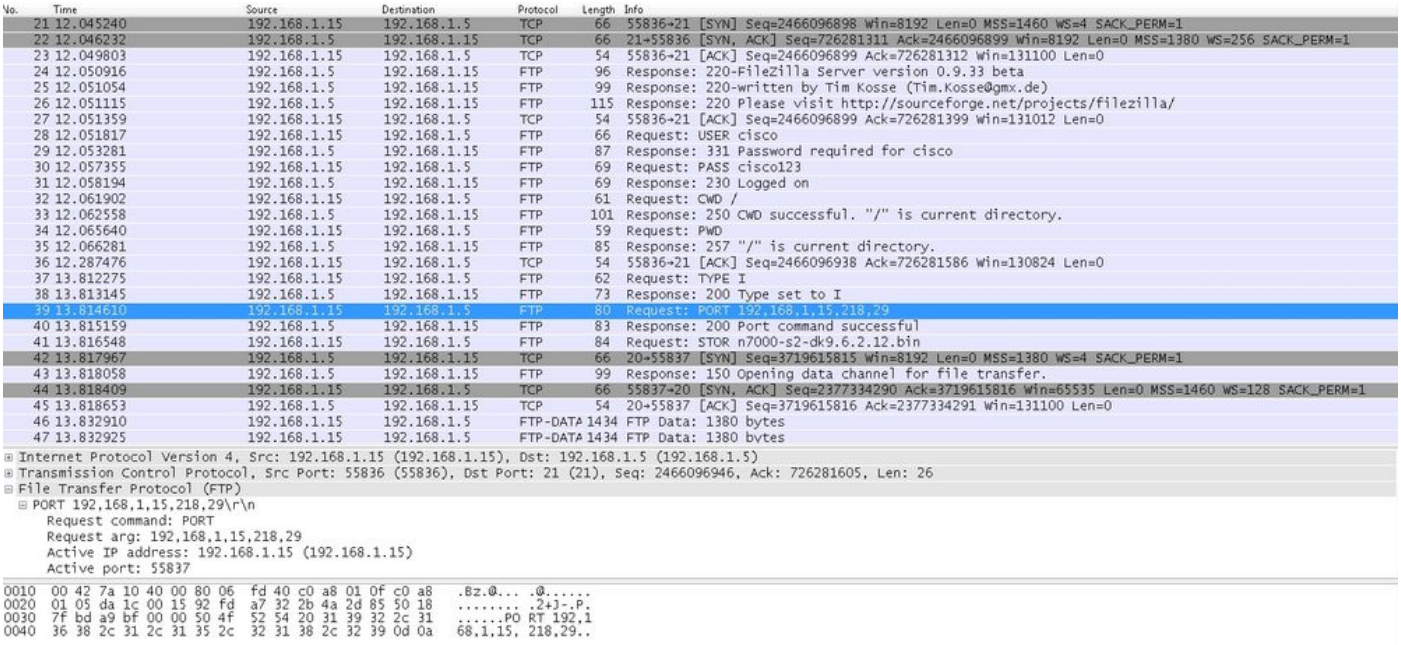


No.	Time	Source	Destination	Protocol	Length	Info
15	12.032774	192.168.1.15	172.16.1.5	TCP	66	55836→21 [SYN] Seq=3317358682 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
16	12.033598	172.16.1.5	192.168.1.15	TCP	66	21→55836 [SYN, ACK] Seq=3073360302 Ack=3317358683 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
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   .Bz.@... ........
0020  01 05 da 1c 00 15 c5 ba  e0 8a b7 2f c2 d4 50 18   ........ .../..P.
0030  7f bd 31 0d 00 00 50 4f  52 54 20 31 39 32 2c 31   ..1...PO RT 192,1
0040  36 38 2c 31 2c 31 35 2c  32 31 38 2c 32 39 0d 0a   68,1,15, 218,29..
```

次の図のように、外部インターフェイスをキャプチャします。



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
```

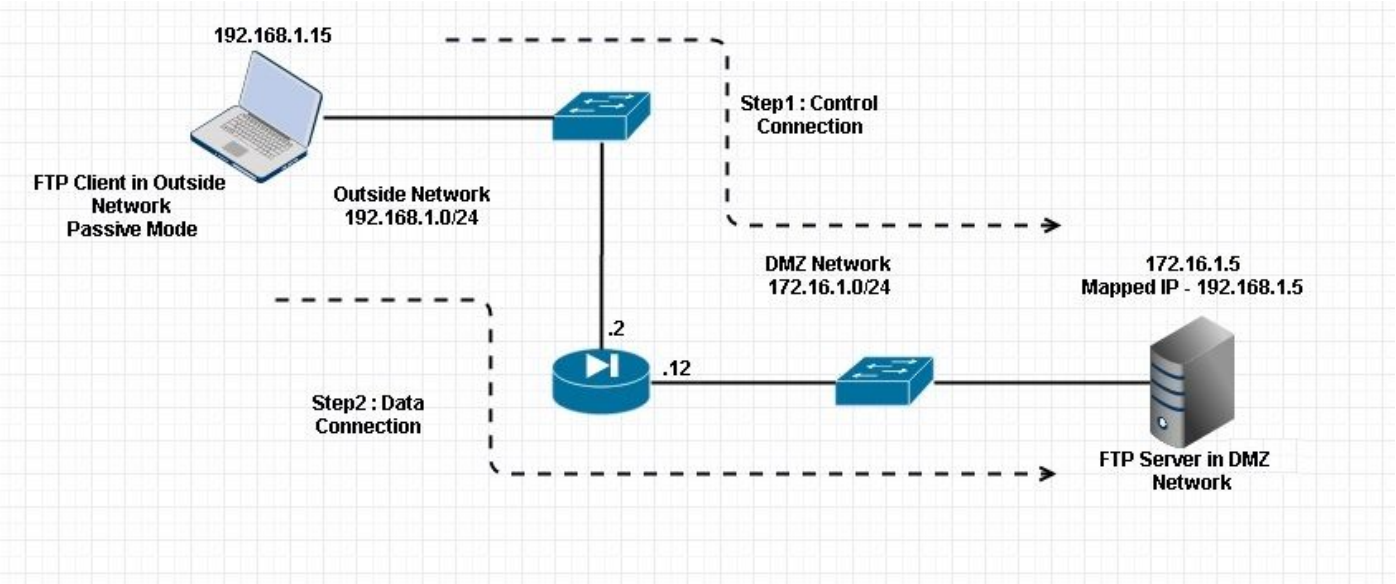
```
0010  00 42 7a 10 40 00 80 06  fd 40 c0 a8 01 0f c0 a8   .Bz.@... .@......
0020  01 05 da 1c 00 15 92 fd  a7 32 2b 4a 2d 85 50 18   ........ .2+J-.P.
0030  7f bd a9 bf 00 00 50 4f  52 54 20 31 39 32 2c 31   ......PO RT 192,1
0040  36 38 2c 31 2c 31 35 2c  32 31 38 2c 32 39 0d 0a   68,1,15, 218,29..
```

アクティブモードのクライアント 192.168.1.15 として稼働しているクライアントが、DMZ 内のサーバとの接続をポート 21 で開始します。続いて、クライアントは、6 タプル値を設定した port コマンドをサーバに送信し、サーバはそのダイナミック ポートに接続します。すると、サーバは送信元ポート 20 でデータ接続を開始します。

シナリオ 4.パッシブ モードで稼働する FTP クライアント

クライアントは ASA の外部ネットワークに配置され、サーバは DMZ ネットワークに配置されます。

ネットワーク図



Connection

<#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

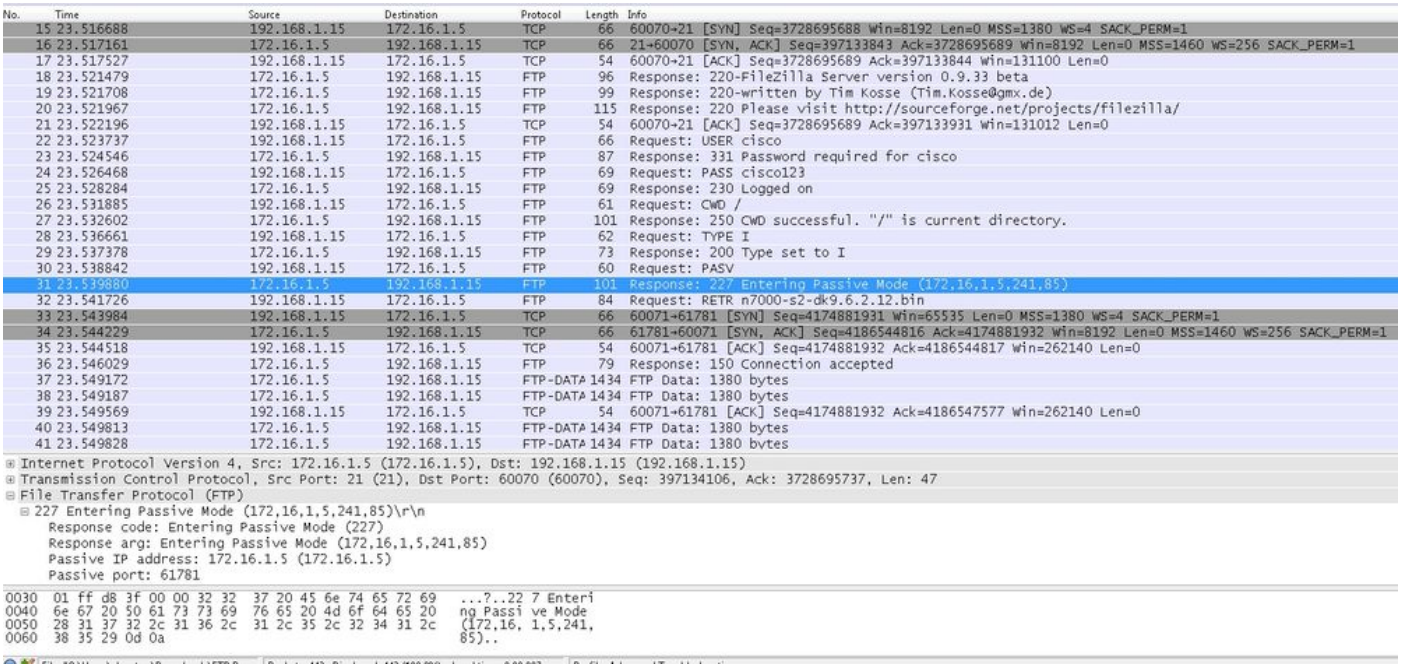
<--- Dynamic channel Open

TCP

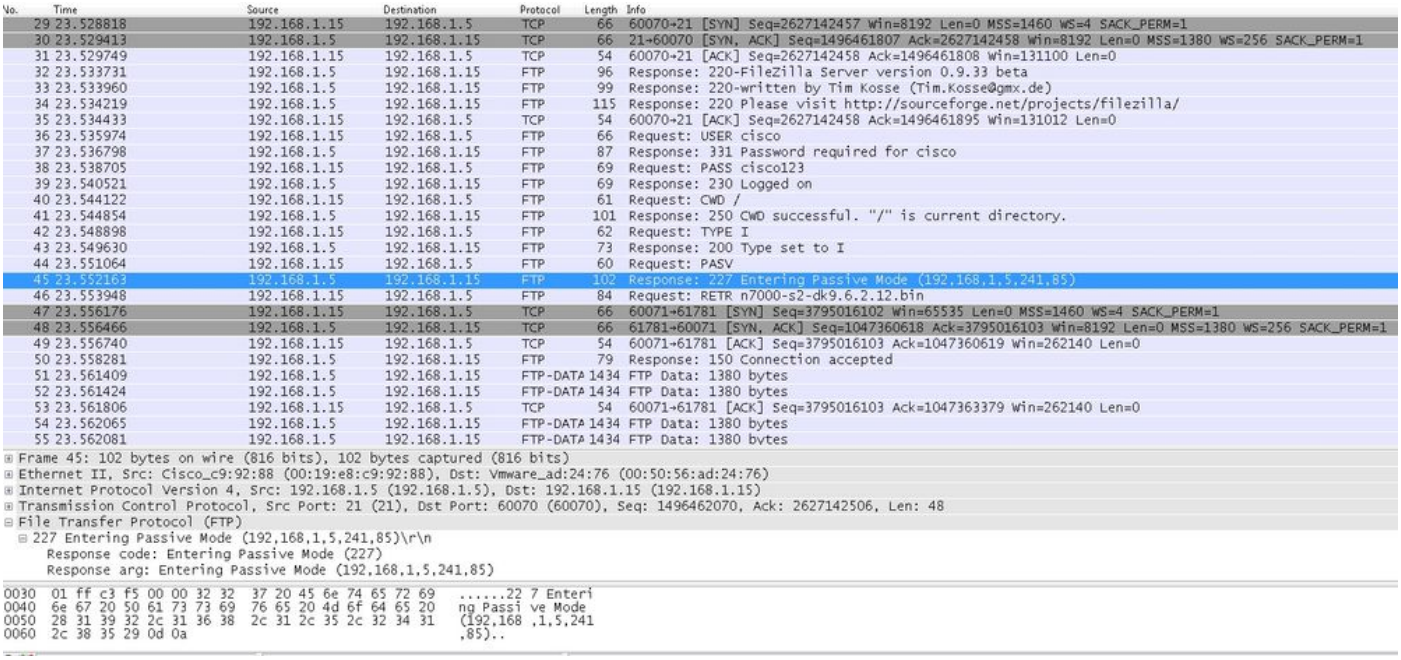
Outside 192.168.1.15:60070 DMZ 172.16.1.5:21

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

次の図のように、DMZ インターフェイスをキャプチャします。



次の図のように、外部インターフェイスをキャプチャします。



基本的な FTP アプリケーション インスペクションの設定

デフォルトでは、デフォルトのアプリケーション インスペクション トラフィックをすべて照合する 1 つのポリシー (グローバル ポリシー) が設定に含まれており、これによりすべてのインターフェイス上のトラフィックにインスペクションが適用されます。デフォルトのアプリケーション インスペクション トラフィックには、各プロトコルのデフォルトのポートに対するトラフィックが含まれています。

適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合、たとえば、非標準ポートにインスペクションを適用したり、デフォルトでは有効にならないインスペクションを追加したりする場合は、デフォルトのポリシーを編集するか、またはデフォルトのポリシーを無効にしてから新しいポリシーを適用する必要があります。すべてのデフォルトのポー

トのリストについては、デフォルトのインスペクション ポリシーを参照してください。

1. policy-map global_policy コマンドを実行します。

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

2. class inspection_default コマンドを実行します。

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

3. inspect FTP コマンドを実行します。

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

4. inspect FTP strict コマンドを使用するオプションが用意されてます。このコマンドでは、FTP 要求に埋め込まれたコマンドの Web ブラウザによる送信を回避することで、保護されたネットワークのセキュリティが向上します。

   インターフェイス上で strict オプションを有効にすると、FTP インスペクションによって次の動作が適用されます。

   - FTP コマンドの確認応答がなければ、セキュリティ アプライアンスは新しいコマンドを許可しません。
   - セキュリティ アプライアンスは、埋め込みコマンドを送信する接続をドロップします。
   - 227 コマンドと PORT コマンドがチェックされ、これらがエラー文字列に表示されていないことが確認されます。

> ⚠ 警告:strictオプションを使用すると、FTP RFCに厳密に準拠していないFTPクライアントで障害が発生する可能性があります。strict オプションの使用についての詳細は、strict オプションの使用を参照してください。

標準外 TCP ポートでの FTP プロトコル インスペクションの設定

次の設定を使用して、標準外 TCP ポートで FTP プロトコル インスペクションを設定できます（ XXXX を新規のポート番号で置き換えてください ）。

<#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
```

確認

設定が正常に行われたことを確認するには、show service-policy コマンドを実行します。また、show service-policy inspect ftp コマンドを実行して、出力を FTP 検査のみに制限します。

<#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

TFTP インスペクションはデフォルトで有効になっています。

セキュリティ アプライアンスによって TFTP トラフィックが検査され、必要に応じて TFTP クライアントとサーバの間でのファイル転送を許可するために、動的に接続および変換が作成されま

す。具体的には、インスペクション エンジンによって TFTP 読み取り要求（RRQ）、書き込み要求（WRQ）、およびエラー通知（ERROR）が検査されます。

動的なセカンダリ チャネルと PAT 変換は、必要に応じて有効な RRQ または WRQ の受信時に割り当てられます。その後、このセカンダリ チャネルはファイル転送または エラー通知のために TFTP によって使用されます。

セカンダリ チャネルを介したトラフィックを開始することができるのは TFTP サーバだけであり、TFTP クライアントとサーバの間に不完全なセカンダリ チャネルが最大で 1 つだけ存在できます。サーバからのエラー通知によって、セカンダリ チャネルが閉じられます。

TFTP トラフィックをリダイレクトするためにスタティック PAT が使用される場合は、TFTP インスペクションを有効にする必要があります。

基本的な TFTP アプリケーション インスペクションの設定

デフォルトでは、デフォルトのアプリケーション インスペクション トラフィックをすべて照合する 1 つのポリシー（グローバル ポリシー）が設定に含まれており、これによりすべてのインターフェイス上のトラフィックにインスペクションが適用されます。デフォルトのアプリケーション インスペクション トラフィックには、各プロトコルのデフォルトのポートに対するトラフィックが含まれています。

適用できるグローバル ポリシーは 1 つだけです。そのため、グローバル ポリシーを変更する場合、たとえば、非標準ポートにインスペクションを適用したり、デフォルトでは有効にならないインスペクションを追加したりする場合は、デフォルトのポリシーを編集するか、またはデフォルトのポリシーを無効にしてから新しいポリシーを適用する必要があります。すべてのデフォルトのポートのリストについては、デフォルトのインスペクション ポリシーを参照してください。

1. policy-map global_policy コマンドを実行します。

```
<#root>

 ASA(config)#

policy-map global_policy
```

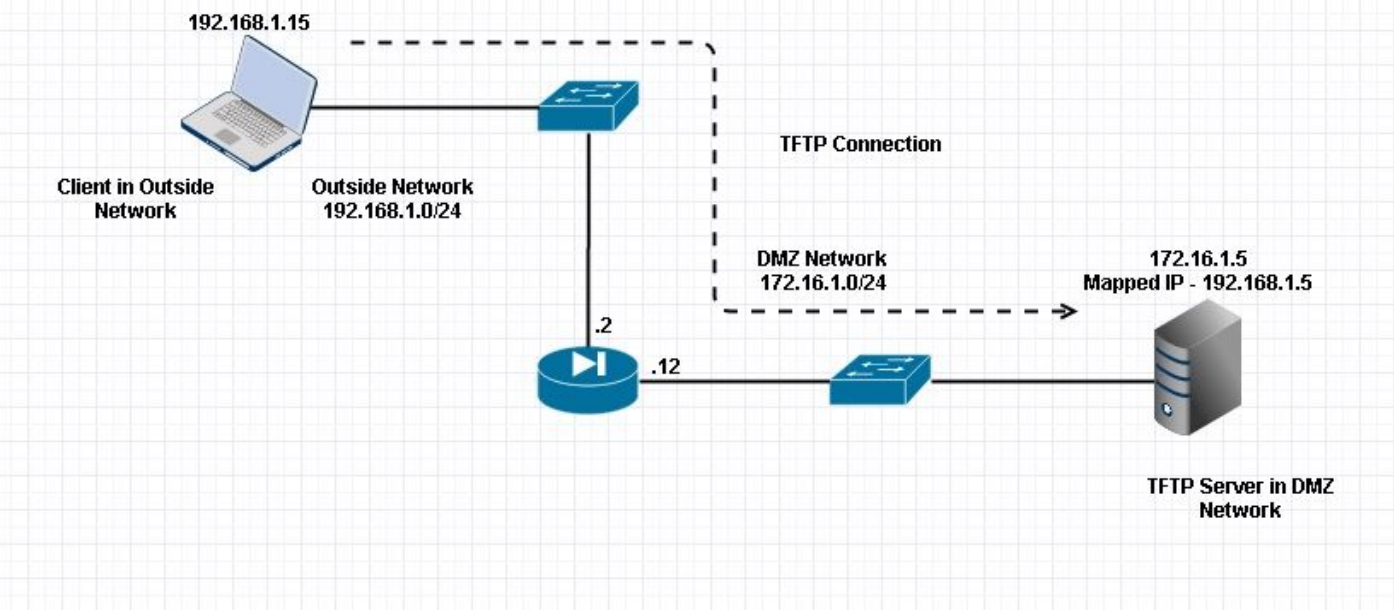
2. class inspection_default コマンドを実行します。

```
<#root>

 ASA(config-pmap)#

class inspection_default
```

3. inspect FTP コマンドを実行します。

```
<#root>

 ASA(config-pmap-c)#

inspect TFTP
```

ネットワーク図



以下に、外部ネットワークでのクライアントの設定を示します。TFTP サーバは DMZ ネットワーク内にあります。サーバは、外部サブネット内の IP 192.168.1.5 にマッピングされます。

設定例：

```
<#root>

 ASA(config)#

show running-config
```

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

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

 !--- Output is suppressed.


 !--- Permit inbound TFTP traffic.


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

!

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


object network obj-172.16.1.5
 host 172.16.1.5


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


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



access-group 100 in interface outside


class-map inspection_default

match default-inspection-traffic

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

policy-map global_policy
```

```
 class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc


inspect tftp


 inspect sip
 inspect xdmcp
!

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

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

確認

設定が正常に行われたことを確認するには、show service-policy コマンドを実行します。また、show service-policy inspect tftp コマンドを実行して、出力を TFTP 検査のみに制限します。

```
<#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#
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

パケット トレーサ

内部ネットワークにあるクライアント

<#root>

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

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

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

Phase: 5
Type: INSPECT

Subtype: inspect-ftp

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

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

object network obj-172.16.1.5

nat (inside,outside) static 192.168.1.5

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

Phase: 7
Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

object network obj-172.16.1.5

nat (inside,outside) static 192.168.1.5

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

----Omitted----

Result:
input-interface:

inside

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

Outside

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

外部ネットワークにあるクライアント

<#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
```

両方のパケットトレーサに示されているように、トラフィックにはそれぞれの NAT ステートメントと FTP 検査ポリシーが適用されています。また、トラフィックはそれぞれに必要なインターフェイスから送信されています。

トラブルシューティングの際は、ASA の入力インターフェイスと出力インターフェイスをキャプチャして、ASA 組み込み IP アドレスの書き換えが正常に行われているかどうかを確認し、接続をチェックして、ダイナミックポートが ASA で許可されているかどうかを確認してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。