

Konfigurieren der FTP-/TFTP-Dienste: ASA 9.x

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Erweiterte Protokollbehandlung](#)

[Konfiguration](#)

[Szenario 1. Für aktiven Modus konfigurierter FTP-Client](#)

[Netzwerkdiagramm](#)

[Szenario 2. Für passiven Modus konfigurierter FTP-Client](#)

[Netzwerkdiagramm](#)

[Szenario 3. Für aktiven Modus konfigurierter FTP-Client](#)

[Netzwerkdiagramm](#)

[Szenario 4. Passiver FTP-Client-Modus](#)

[Netzwerkdiagramm](#)

[Konfigurieren der grundlegenden FTP-Anwendungsinspektion](#)

[FTP-Protokollüberprüfung für nicht standardmäßigen TCP-Port konfigurieren](#)

[Überprüfung](#)

[TFTP](#)

[Konfigurieren der grundlegenden TFTP-Anwendungsprüfung](#)

[Netzwerkdiagramm](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Client im internen Netzwerk](#)

[Client in externem Netzwerk](#)

Einleitung

In diesem Dokument werden die verschiedenen FTP- und TFTP-Prüfszenarien für die ASA-, ASA-FTP-/TFTP-Prüfkonfiguration und die grundlegende Fehlerbehebung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Grundlegende Kommunikation zwischen den erforderlichen Schnittstellen
- Konfiguration des FTP-Servers im DMZ-Netzwerk

Verwendete Komponenten

In diesem Dokument werden verschiedene FTP- und TFTP-Prüfszenarien für die Adaptive Security Appliance (ASA) beschrieben. Außerdem werden die ASA-FTP-/TFTP-Prüfkonfiguration und grundlegende Fehlerbehebungsfunktionen behandelt.

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ASA der Serie 5500 oder ASA 5500-X, die das Software-Image von 9.1(5) ausführt
- Jeder FTP-Server
- Beliebiger FTP-Client

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die Sicherheits-Appliance unterstützt die Anwendungsinspektion mithilfe der Funktion Adaptive Security Algorithm.

Durch die Stateful-Anwendungsinspektion, die vom Adaptive Security Algorithm verwendet wird, verfolgt die Security Appliance jede Verbindung, die die Firewall passiert, und stellt sicher, dass sie gültig ist.

Die Firewall überwacht mittels Stateful Inspection auch den Status der Verbindung, um Informationen für die Platzierung in einer Statustabelle zu kompilieren.

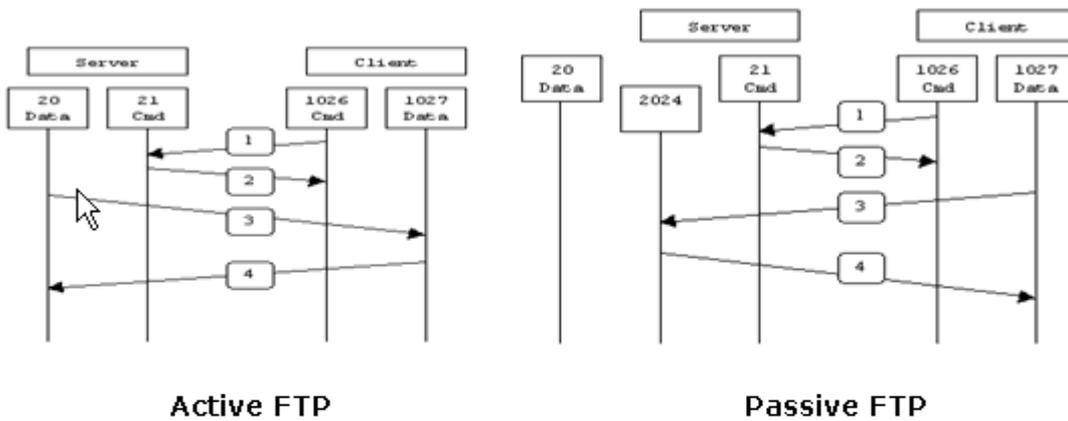
Bei Verwendung der Statustabelle und der vom Administrator definierten Regeln basieren die Filterungsentscheidungen auf Kontext, der durch Pakete erstellt wird, die zuvor durch die Firewall geleitet wurden.

Die Durchführung von Anwendungsinspektionen umfasst folgende Maßnahmen:

- Identifizieren des Datenverkehrs
- Traffic-Inspektionen durchführen
- Aktivieren von Inspektionen an einer Schnittstelle

Es gibt zwei Formen von FTP, wie im Bild dargestellt.

- Aktiver Modus
- Passiver Modus



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

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

Aktives FTP

Im aktiven FTP-Modus stellt der Client über einen zufälligen nicht privilegierten Port ($N > 1023$) eine Verbindung mit dem Befehlsport (21) des FTP-Servers her. Dann beginnt der Client, Port $N > 1023$ abzuhören und sendet den FTP-Befehlsport $N > 1023$ an den FTP-Server. Der Server stellt dann über seinen lokalen Datenport, Port 20, eine Verbindung zu den angegebenen Daten-Ports des Clients her.

Passives FTP

Im Modus für passives FTP initiiert der Client beide Verbindungen zum Server, wodurch das Problem einer Firewall gelöst wird, die die eingehende Datenportverbindung zum Client vom Server filtert. Wenn eine FTP-Verbindung geöffnet wird, öffnet der Client zwei zufällige nicht privilegierte Ports lokal. Der erste Port verbindet den Server mit Port 21. Anstatt jedoch einen **Port**-Befehl auszuführen und dem Server zu erlauben, sich wieder mit seinem Daten-Port zu verbinden, gibt der Client den **PASV**-Befehl aus. Dies hat zur Folge, dass der Server dann einen zufälligen unprivilegierten Port öffnet ($P > 1023$) und den Befehl **Port P** zurück an den Client sendet. Der Client initiiert dann die Verbindung von Port $N > 1023$ zu Port P auf dem Server, um Daten zu übertragen. Ohne die **Prüfbefehlskonfiguration** auf der Sicherheits-Appliance funktioniert FTP von internen Benutzern mit ausgehendem Port nur im passiven Modus. Außerdem wird Benutzern, die sich außerhalb des FTP-Servers befinden, der Zugriff verweigert.

TFTP

TFTP, wie in [RFC 1350](#) beschrieben, ist ein einfaches Protokoll zum Lesen und Schreiben von Dateien zwischen einem TFTP-Server und einem Client. TFTP verwendet den UDP-Port 69.

Erweiterte Protokollbehandlung

Warum benötigen Sie eine FTP-Überprüfung?

Für einige Anwendungen ist eine spezielle Behandlung durch die Anwendungsinspektionsfunktion der Cisco Security Appliance erforderlich. Diese Arten von Anwendungen betten IP-Adressierungsinformationen in das Benutzerdatenpaket ein oder öffnen sekundäre Kanäle an dynamisch

zugewiesenen Ports. Die Anwendungsinspektionsfunktion arbeitet mit Network Address Translation (NAT) zusammen, um den Speicherort der eingebetteten Adressinformationen zu identifizieren.

Neben der Identifizierung eingebetteter Adressinformationen überwacht die Anwendungsinspektionsfunktion Sitzungen, um die Portnummern für sekundäre Kanäle zu ermitteln. Viele Protokolle öffnen sekundäre TCP- oder UDP-Ports, um die Leistung zu verbessern. Die erste Sitzung auf einem bekannten Port wird verwendet, um dynamisch zugewiesene Portnummern auszuhandeln.

Die Anwendungsinspektionsfunktion überwacht diese Sitzungen, identifiziert die dynamischen Portzuweisungen und ermöglicht den Datenaustausch an diesen Ports für die Dauer der jeweiligen Sitzungen. Multimedia- und FTP-Anwendungen verhalten sich ähnlich.

Wenn die FTP-Überprüfung auf der Sicherheits-Appliance nicht aktiviert wurde, wird diese Anforderung verworfen, und die FTP-Sitzungen übertragen keine angeforderten Daten.

Wenn die FTP-Überprüfung auf dem ASA-Gerät aktiviert ist, überwacht das ASA-Gerät den Steuerungskanal und versucht, eine Anforderung zum Öffnen des Datenkanals zu erkennen. Das FTP-Protokoll bettet die Datenkanal-Portspezifikationen in den Steuerungskanal-Datenverkehr ein. Die Security Appliance muss den Steuerungskanal daraufhin überprüfen, ob Datenport-Änderungen vorliegen.

Sobald die ASA eine Anforderung erkennt, erstellt sie vorübergehend eine Öffnung für den Datenverkehr auf dem Datenkanal, die über die gesamte Lebensdauer der Sitzung andauert. Auf diese Weise überwacht die FTP-Prüffunktion den Steuerkanal, identifiziert eine Datenport-Zuordnung und ermöglicht den Datenaustausch auf dem Datenport über die Dauer der Sitzung.

ASA überprüft standardmäßig Port-21-Verbindungen über die Global-Inspection Class-Map auf FTP-Datenverkehr. Die Sicherheits-Appliance erkennt außerdem den Unterschied zwischen einer aktiven und einer passiven FTP-Sitzung.

Wenn die FTP-Sitzungen eine passive FTP-Datenübertragung unterstützen, erkennt die ASA über den Befehl **inspect ftp** die Datenportanforderung des Benutzers und öffnet einen neuen Datenport, der größer als 1023 ist.

Die **inspect ftp**-Befehlsüberprüfung überprüft FTP-Sitzungen und führt vier Aufgaben aus:

- Bereitet eine dynamische sekundäre Datenverbindung vor
- Verfolgt die FTP-Befehlsantwortsequenz
- Generiert einen Prüfpfad
- Wandelt die eingebettete IP-Adresse mithilfe von NAT um

Die FTP-Anwendungsinspektion bereitet sekundäre Kanäle für die FTP-Datenübertragung vor. Die Kanäle werden als Reaktion auf einen Datei-Upload, einen Datei-Download oder ein Verzeichnisauflistungsereignis zugewiesen und müssen vorab ausgehandelt werden. Der Port wird über die Befehle **PORT** oder **PASV** (227) ausgehandelt.

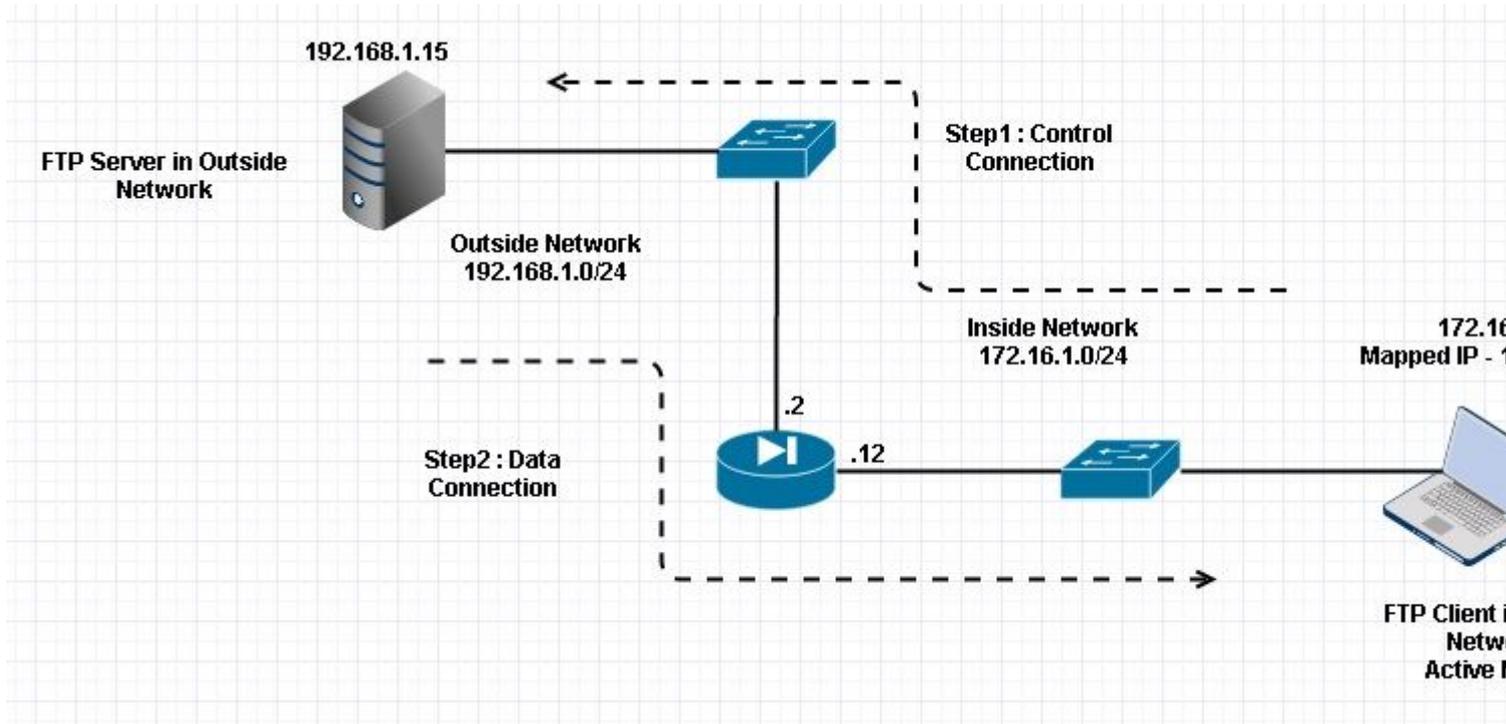
Konfiguration

Hinweis: Alle Netzwerkszenarien werden erläutert, indem die FTP-Prüfung auf der ASA aktiviert ist.

Szenario 1. Für aktiven Modus konfigurierter FTP-Client

Mit dem internen Netzwerk der ASA verbundener Client und Server im externen Netzwerk.

Netzwerkdiagramm



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht legal routbar.

Wie in diesem Bild gezeigt, verfügt die verwendete Netzwerkkonfiguration über die ASA mit Client im internen Netzwerk mit IP 172.16.1.5. Server befindet sich im externen Netzwerk mit IP 192.168.1.15. Dem Client wurde im externen Netzwerk die IP 192.168.1.5 zugeordnet.

Es ist nicht erforderlich, eine Zugriffsliste für die externe Schnittstelle zuzulassen, da die FTP-Überprüfung den dynamischen Port-Channel öffnet.

Konfigurationsbeispiel:

```
<#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)#
```

Überprüfung

Verbindung

```
<#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
```

Hier initiiert der Client in Inside die Verbindung mit Quellport 61854 zum Zielport 21. Der Client sendet dann den **Port**-Befehl mit 6 Tupelwerten. Der Server wiederum initiiert die Sekundär-/Datenverbindung mit dem Quell-Port 20, und der Ziel-Port wird anhand der nach diesen Erfassungen genannten Schritte berechnet.

Capture Inside Interface (Interne Schnittstelle erfassen), wie in diesem Bild dargestellt.

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	.AD"@... <.....
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..

Erfassen Sie die externe Schnittstelle, wie in diesem Bild dargestellt.

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..

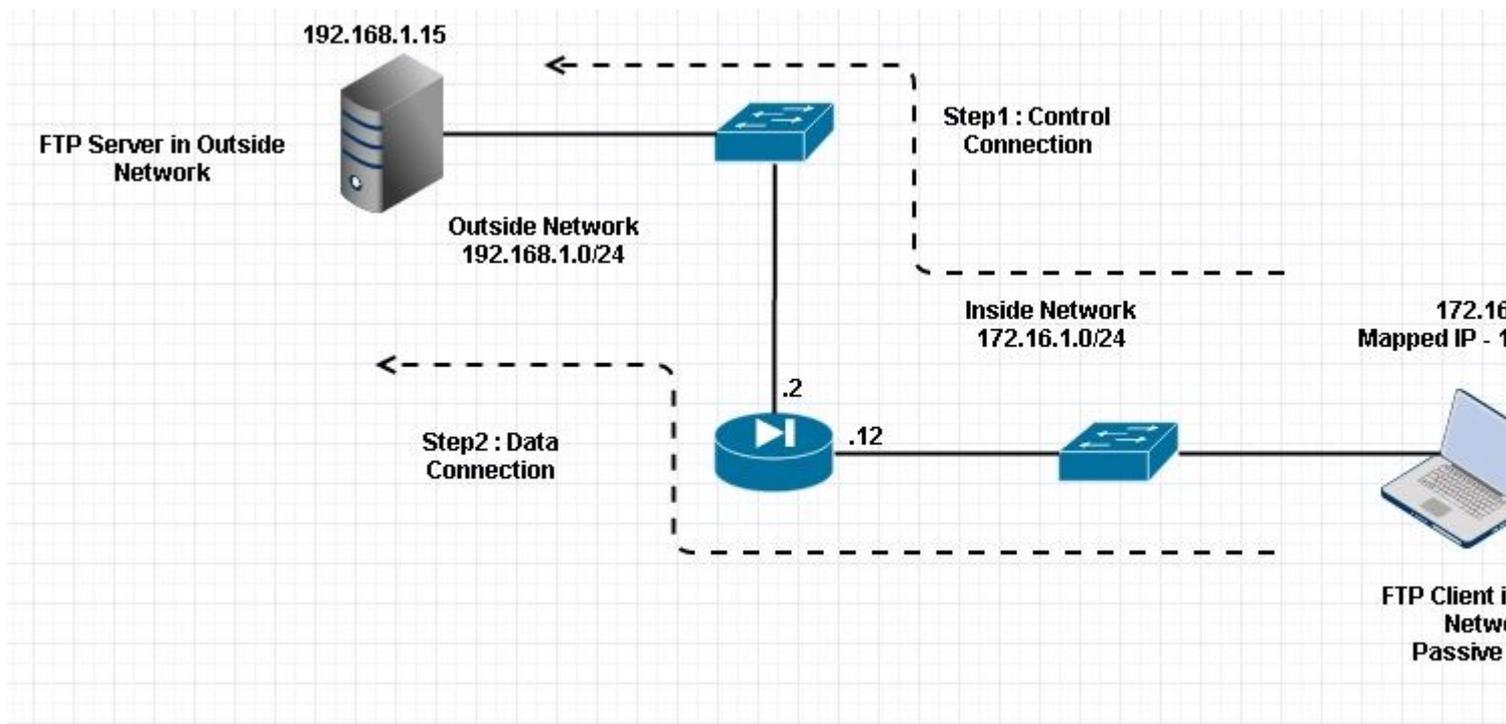
Der Port-Wert wird mit den letzten zwei von sechs Tupeln berechnet. Links 4 Tupel sind IP-Adresse und 2 Tupel sind für Port. Wie in diesem Bild gezeigt, ist die IP-Adresse 192.168.1.5 und $241 * 256 + 159 = 61855$.

Capture zeigt außerdem, dass die Werte mit Port-Befehlen geändert werden, wenn die FTP-Prüfung aktiviert ist. Die Erfassung der internen Schnittstelle zeigt den tatsächlichen IP-Wert an, und der Port, der von Client für Server gesendet wurde, um eine Verbindung mit dem Client für den Datenkanal herzustellen, und die Erfassung der externen Schnittstelle zeigt die zugeordnete Adresse an.

Szenario 2. Für passiven Modus konfigurierter FTP-Client

Client im internen Netzwerk der ASA und Server im externen Netzwerk.

Netzwerkdiagramm



Verbindung

```
<#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

Hier initiiert der Client im Inneren eine Verbindung mit Quellport 61838 und Zielport 21. Da es sich um ein passives FTP handelt, initiiert der Client beide Verbindungen. Nachdem der Client den **PASV**-Befehl gesendet hat, antwortet der Server mit seinem 6-Tupelwert, und der Client stellt eine Verbindung mit diesem Socket für die Datenverbindung her.

Capture Inside Interface (Interne Schnittstelle erfassen), wie in diesem Bild dargestellt.

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=8192 Len=0 MSS=1460
50	35.657717	172.16.1.5	192.168.1.15	TCP	54	61838+21 [ACK] Seq=1456310601 Ack=700898683 win=1310
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/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=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=1460
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=1460
71	37.559791	172.16.1.5	192.168.1.15	TCP	54	61839+60142 [ACK] Seq=597547300 Ack=2027855231 win=284
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)..

Erfassen Sie die externe Schnittstelle, wie in diesem Bild dargestellt.

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=1310
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=1310
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=1308
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=260
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)..

```

Die Berechnung für die Ports bleibt unverändert.

Wie bereits erwähnt, schreibt die ASA die eingebetteten IP-Werte neu, wenn die FTP-Überprüfung aktiviert ist. Außerdem wird ein dynamischer Port-Channel für die Datenverbindung geöffnet.

Dies sind die Verbindungsdetails, wenn **FTP-Überprüfung ist deaktiviert**

Verbindung:

```
<#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

```

Ohne FTP-Inspektion, Es versucht nur, **Port-Befehl** immer und immer wieder senden, aber es gibt keine

Antwort, da außen den PORT mit Original-IP nicht NATTed ein empfängt. Dasselbe wurde in der Deponie gezeigt.

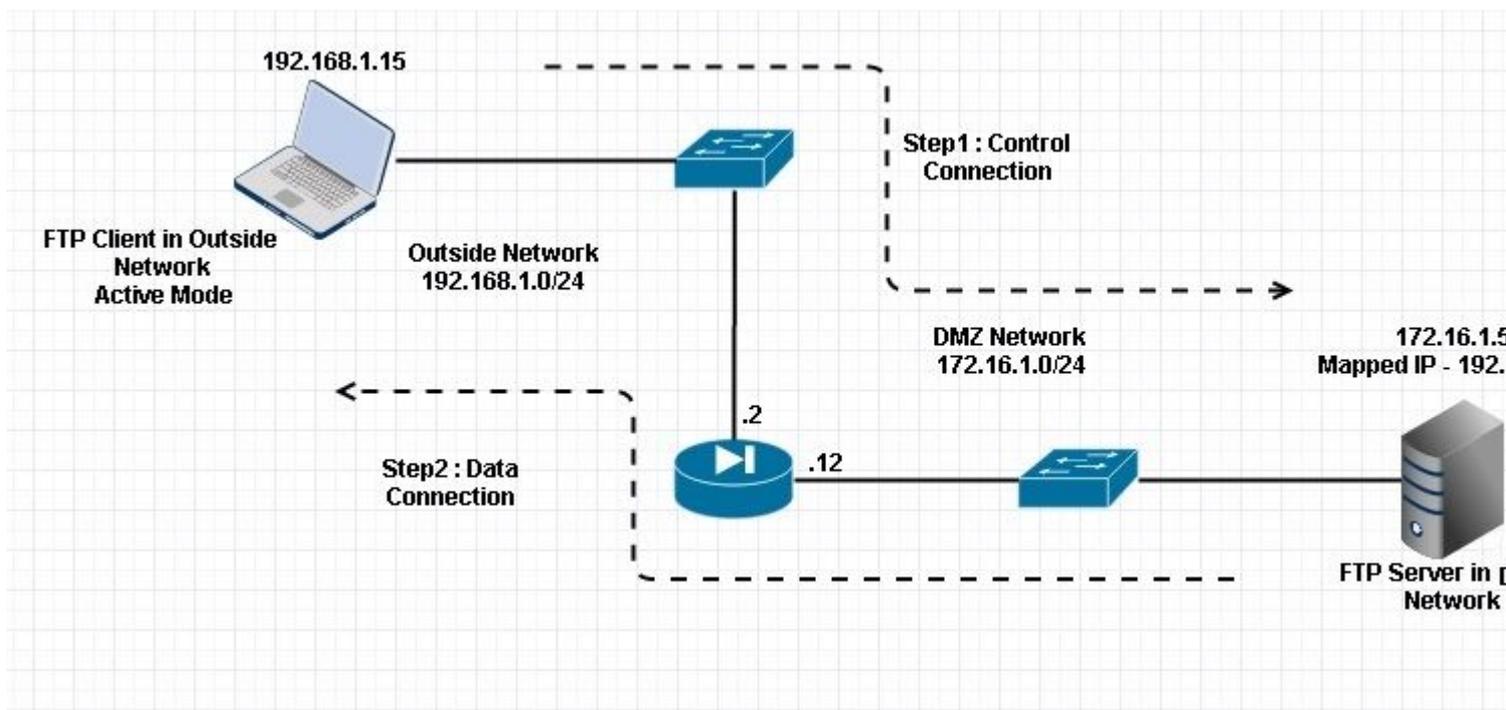
Die FTP-Überprüfung kann deaktiviert werden, wenn im Konfigurationsendgerätemodus **kein FTP 21-** Befehl für das **Fixup-Protokoll** ausgeführt wird.

Ohne FTP-Inspektion funktioniert nur der **PASV**-Befehl, wenn sich der Client im Inneren befindet, da kein **Port**-Befehl von innen kommt, der eingebettet werden muss, und beide Verbindungen von innen initiiert werden.

Szenario 3. Für aktiven Modus konfigurierter FTP-Client

Client außerhalb des Netzwerks der ASA und Server im DMZ-Netzwerk.

Netzwerkdiagramm



Konfiguration:

```
<#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)#
```

Überprüfung

Verbindung:

```
<#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 22595694, flags UI

<--- Dynamic Port channel

Erfassen Sie die DMZ-Schnittstelle wie in diesem Bild dargestellt.

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=131
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/pr
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 directo
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=130
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=131
39	13.806049	172.16.1.5	192.168.1.15	TCP	54	20+55837 [ACK] Seq=1812810162 Ack=177574186 Win=131
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 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..

Erfassen Sie die externe Schnittstelle, wie in diesem Bild dargestellt.

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	55837→20 [SYN, ACK] Seq=2377334290 Ack=3719615816 Win=8192 Len=0 MSS=1380
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 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..

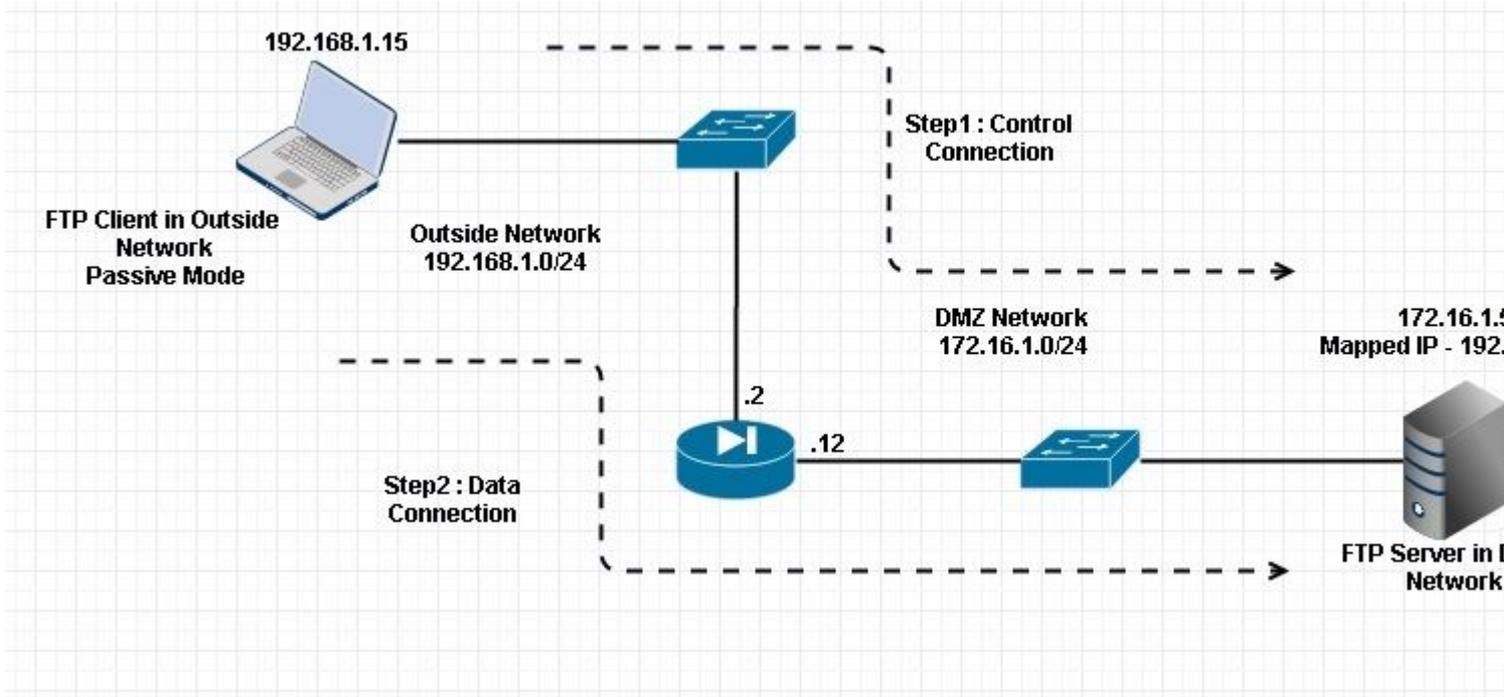
```

Der Client führt hier den Active Mode-Client 192.168.1.15 aus und initiiert die Verbindung zum Server in der DMZ auf Port 21. Der Client sendet dann **den Port**-Befehl mit sechs Tupelwerten an den Server, um eine Verbindung zu diesem spezifischen dynamischen Port herzustellen. Der Server initiiert dann die Datenverbindung mit dem Quellport als 20.

Szenario 4. Passiver FTP-Client-Modus

Client außerhalb des Netzwerks der ASA und Server im DMZ-Netzwerk.

Netzwerkdiagramm



Verbindung

<#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
```

Erfassen Sie die DMZ-Schnittstelle wie in diesem Bild dargestellt.

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)..

Erfassen Sie die externe Schnittstelle, wie in diesem Bild dargestellt.

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=65535 Len=0 MSS=1460
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=65535 Len=0 MSS=1460
49	23.556740	192.168.1.15	192.168.1.5	TCP	54	60071→61781 [ACK] Seq=3795016103 Ack=1047360619 Win=65535 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=65535 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

[E] Frame 45: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
 [E] Ethernet II, Src: Cisco_c9:92:88 (00:19:e8:c9:92:88), Dst: Vmware_ad:24:76 (00:50:56:ad:24:76)
 [E] Internet Protocol Version 4, Src: 192.168.1.5 (192.168.1.5), Dst: 192.168.1.15 (192.168.1.15)
 [E] Transmission Control Protocol, Src Port: 21 (21), Dst Port: 60070 (60070), Seq: 1496462070, Ack: 2627142506, Len: 48
 [E] File Transfer Protocol (FTP)
 [E] 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)..
  
```

Konfigurieren der grundlegenden FTP-Anwendungsinspektion

Standardmäßig enthält die Konfiguration eine Richtlinie, die mit dem gesamten standardmäßigen Anwendungsinspektionsverkehr übereinstimmt und die Inspektion auf den Datenverkehr an allen Schnittstellen anwendet (eine globale Richtlinie). Der standardmäßige Anwendungsinspektionsverkehr beinhaltet Datenverkehr zu den Standardports für jedes Protokoll.

Sie können nur eine globale Richtlinie anwenden. Wenn Sie also die globale Richtlinie ändern möchten, z. B. Inspektionen auf nicht standardmäßige Ports anwenden oder Inspektionen hinzufügen möchten, die nicht standardmäßig aktiviert sind, müssen Sie die Standardrichtlinie entweder bearbeiten oder deaktivieren und eine neue anwenden. Eine Liste aller Standard-Ports finden Sie unter [Standard-Inspektionsrichtlinie](#).

1. Führen Sie den Befehl `policy-map global_policy` aus.

```

<#root>

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

2. Führen Sie den Befehl `class inspection_default` aus.

```

<#root>
  
```

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

3. Führen Sie den Befehl **inspect FTP** aus.

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

4. Es gibt eine Option, den Befehl **inspect FTP strict** zu verwenden. Dieser Befehl erhöht die Sicherheit geschützter Netzwerke, indem verhindert wird, dass ein Webbrowser eingebettete Befehle in FTP-Anforderungen sendet.

Nachdem Sie die Option "**strict**" für eine Schnittstelle aktiviert haben, erzwingt die FTP-Überprüfung folgendes Verhalten:

- Ein FTP-Befehl muss bestätigt werden, bevor die Security Appliance einen neuen Befehl zulässt.
- Die Sicherheits-Appliance bricht eine Verbindung ab, die eingebettete Befehle sendet
- Die Befehle **227** und **PORT** werden überprüft, um sicherzustellen, dass sie nicht in einer Fehlerzeichenfolge angezeigt werden.

Warnung: Die Verwendung der **strikten** Option führt möglicherweise zum Ausfall von FTP-Clients, die nicht streng mit FTP-RFCs konform sind. Weitere Informationen zur Verwendung **der strikten** Option finden Sie unter [Using the strict Option](#).

FTP-Protokollüberprüfung für nicht standardmäßigen TCP-Port konfigurieren

Sie können die FTP-Protokollüberprüfung für nicht standardmäßige TCP-Ports mithilfe der folgenden Konfigurationszeilen konfigurieren (XXXX durch die neue Portnummer ersetzen):

```
<#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
```

Überprüfung

Um sicherzustellen, dass die Konfiguration erfolgreich durchgeführt wurde, führen Sie den Befehl **show service-policy** aus. Begrenzen Sie außerdem die Ausgabe auf die FTP-Überprüfung, indem Sie den Befehl **show service-policy inspect ftp** ausführen.

```
<#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

Die TFTP-Überprüfung ist standardmäßig aktiviert.

Die Sicherheits-Appliance prüft den TFTP-Datenverkehr und erstellt bei Bedarf dynamisch Verbindungen und Übersetzungen, um die Dateiübertragung zwischen einem TFTP-Client und -Server zu ermöglichen. Die Prüfungs-Engine überprüft insbesondere TFTP-Leseanforderungen (RRQ), Schreibanforderungen (WRQ) und Fehlerbenachrichtigungen (ERROR).

Ein dynamischer Sekundärkanal und ggf. eine PAT-Übersetzung werden bei einem Empfang eines gültigen RRQ oder WRQ zugeordnet. Dieser sekundäre Kanal wird anschließend vom TFTP für die Dateiübertragung oder die Fehlerbenachrichtigung verwendet.

Nur der TFTP-Server kann den Datenverkehr über den sekundären Kanal initiieren, und es kann maximal ein unvollständiger sekundärer Kanal zwischen dem TFTP-Client und dem Server vorhanden sein. Der sekundäre Kanal wird durch eine Fehlermeldung des Servers geschlossen.

Die TFTP-Prüfung muss aktiviert werden, wenn die statische PAT zum Umleiten des TFTP-Datenverkehrs verwendet wird.

Konfigurieren der grundlegenden TFTP-Anwendungsprüfung

Standardmäßig enthält die Konfiguration eine Richtlinie, die mit dem gesamten standardmäßigen Anwendungsinspektionsverkehr übereinstimmt und die Inspektion auf den Datenverkehr an allen Schnittstellen anwendet (eine globale Richtlinie). Der standardmäßige Anwendungsinspektionsverkehr beinhaltet Datenverkehr zu den Standardports für jedes Protokoll.

Sie können nur eine globale Richtlinie anwenden. Wenn Sie also die globale Richtlinie ändern möchten, z. B. Inspektionen auf nicht standardmäßige Ports anwenden oder Inspektionen hinzufügen möchten, die standardmäßig nicht aktiviert sind, müssen Sie die Standardrichtlinie entweder bearbeiten oder deaktivieren und eine neue anwenden. Eine Liste aller Standard-Ports finden Sie unter [Standard-Inspektionsrichtlinie](#).

1. Führen Sie den Befehl **policy-map global_policy** aus.

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

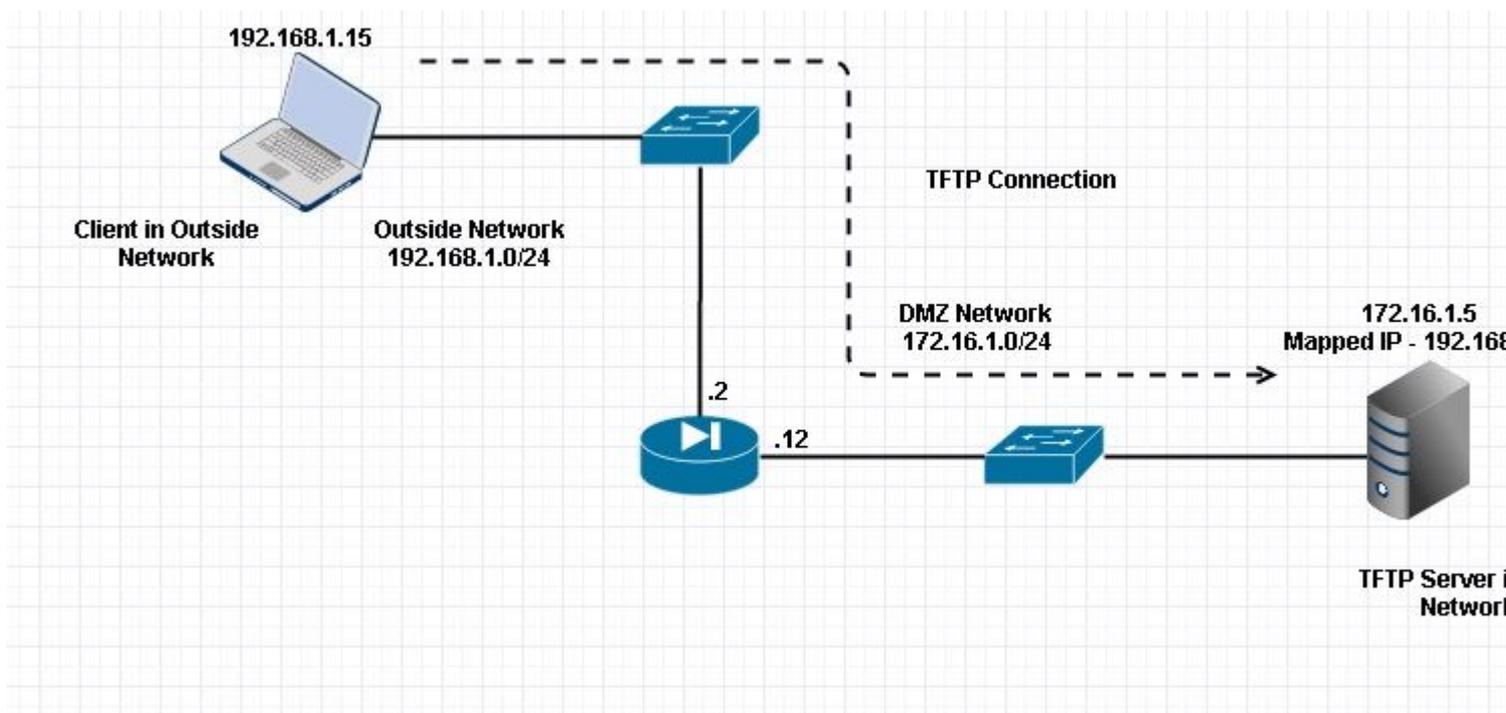
2. Führen Sie den Befehl **class inspection_default** aus.

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

3. Führen Sie den Befehl **inspect TFTP** aus.

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

Netzwerkdiagramm



Hier ist der Client in Außerhalb des Netzwerks konfiguriert. Der TFTP-Server wird im DMZ-Netzwerk platziert. Der Server ist der IP 192.168.1.5 zugeordnet, die sich im externen Subnetz befindet.

Konfigurationsbeispiel:

```
<#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)#

```

Überprüfung

Um sicherzustellen, dass die Konfiguration erfolgreich durchgeführt wurde, führen Sie den Befehl **show service-policy** aus. Beschränken Sie die Ausgabe außerdem auf die TFTP-Überprüfung, indem Sie den

Befehl **show service-policy inspect tftp** ausführen.

<#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#
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Packet Tracer

Client im internen Netzwerk

<#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 in externem Netzwerk

<#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
```

Wie in beiden Paket-Tracern zu sehen, trifft der Datenverkehr auf die jeweiligen NAT-Anweisungen und die FTP-Prüfungsrichtlinie. Sie verlassen auch die erforderliche Schnittstelle.

Während der Fehlerbehebung können Sie versuchen, die ASA-Eingangs- und -Ausgangsschnittstellen zu erfassen und festzustellen, ob das Umschreiben der integrierten ASA-IP-Adresse ordnungsgemäß funktioniert. Außerdem können Sie überprüfen, ob die Verbindung mit dem dynamischen Port auf der ASA

zulässig ist.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.