FTP/TFTP 서비스 구성: ASA 9.X

목차

소개

이 문서에서는 ASA, ASA FTP/TFTP 검사 컨피그레이션 및 기본 트러블슈팅에 대한 다양한 FTP 및 TFTP 검사 시나리오에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- 필수 인터페이스 간 기본 통신

- DMZ 네트워크에 있는 FTP 서버 구성

사용되는 구성 요소

이 문서에서는 ASA(Adaptive Security Appliance)의 다양한 FTP 및 TFTP 검사 시나리오에 대해 설명하고 ASA FTP/TFTP 검사 컨피그레이션 및 기본적인 트러블슈팅에 대해서도 설명합니다.

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 9.1(5) 소프트웨어 이미지를 실행하는 ASA 5500 또는 ASA 5500-X Series ASA
- 모든 FTP 서버
- 모든 FTP 클라이언트

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

보안 어플라이언스는 Adaptive Security Algorithm 기능을 통해 애플리케이션 검사를 지원합니다.

Adaptive Security Algorithm에서 사용하는 상태 기반 애플리케이션 검사를 통해 Security Appliance는 방화벽을 통과하는 각 연결을 추적하여 유효한지 확인합니다.

방화벽은 상태 기반 검사를 통해 연결 상태를 모니터링하여 상태 테이블에 배치할 정보를 컴파일합니다.

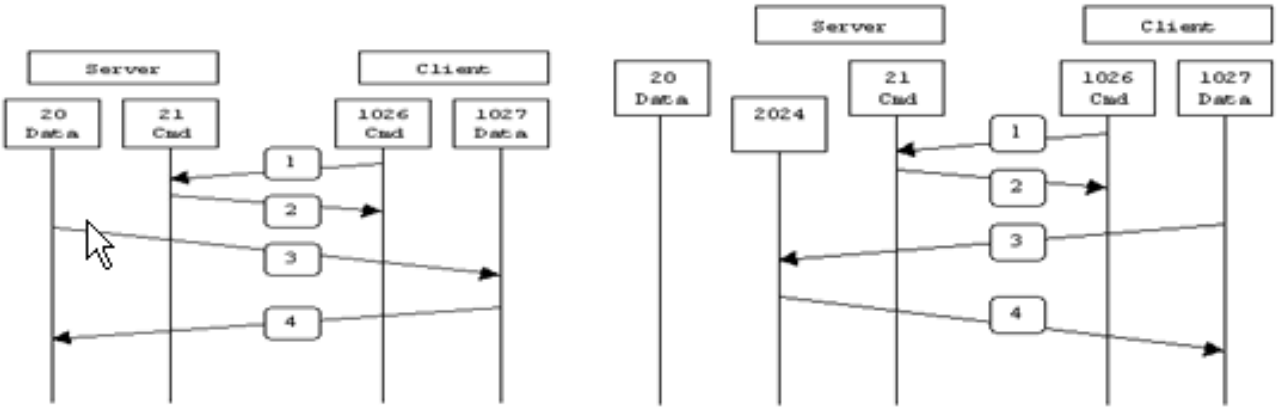
관리자 정의 규칙 외에 상태 테이블을 사용할 경우, 이전에 방화벽을 통과한 패킷에 의해 설정된 컨텍스트를 기반으로 필터링 결정이 이루어집니다.

애플리케이션 검사 구현은 다음 작업으로 구성됩니다.

- 트래픽 식별
- 트래픽에 검사 적용
- 인터페이스에서 검사 활성화

그림과 같이 두 가지 FTP 형식이 있습니다.

- 활성 모드
- 수동 모드



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

활성 FTP

활성 FTP 모드에서는 클라이언트가 임의의 권한 없는 포트(N>1023)에서 FTP 서버의 명령 포트(21)로 연결됩니다. 그런 다음 클라이언트는 포트 N>1023을 수신 대기하기 시작하고 FTP 서버에 FTP 명령 포트 N>1023을 전송합니다. 그런 다음 서버는 로컬 데이터 포트(포트 20)에서 클라이언트의 지정된 데이터 포트에 다시 연결합니다.

수동 FTP

패시브 FTP 모드에서는 클라이언트가 서버에 대한 두 연결을 모두 시작합니다. 그러면 서버에서 클라이언트에 대한 수신 데이터 포트 연결을 필터링하는 방화벽 문제가 해결됩니다. FTP 연결이 열리면 클라이언트는 로컬에서 임의의 권한 없는 포트 2개를 엽니다. 첫 번째 포트는 포트 21의 서버에 접속합니다. 그러나 port 명령을 실행하고 서버가 해당 데이터 포트에 다시 연결하도록 허용하는 대신, 클라이언트는 PASV 명령을 실행합니다. 그 결과 서버는 임의의 권한 없는 포트를 열고(P>1023) port P 명령을 클라이언트로 다시 전송합니다. 그런 다음 클라이언트는 서버의 포트 N>1023에서 포트 P로의 연결을 시작하여 데이터를 전송합니다. 보안 어플라이언스에서 inspection 명령 컨피그레이션이 없으면 아웃바운드로 향하는 내부 사용자의 FTP는 패시브 모드에서만 작동합니다. 또한 FTP 서버로 향하는 인바운드 이외의 사용자는 액세스가 거부됩니다.

TFTP

RFC 1350에 설명된 대로, TFTP는 TFTP 서버와 클라이언트 간에 파일을 읽고 쓰기 위한 간단한 프로토콜입니다. TFTP는 UDP 포트 69를 사용합니다.

고급 프로토콜 처리

FTP 검사가 필요한 이유는 무엇입니까?

일부 애플리케이션은 Cisco Security Appliance 애플리케이션 검사 기능을 사용하여 특별히 처리해야 합니다. 이러한 유형의 애플리케이션은 일반적으로 사용자 데이터 패킷에 IP 주소 지정 정보를 포함하거나 동적으로 할당된 포트에서 보조 채널을 엽니다. 애플리케이션 검사 기능은 NAT(Network Address Translation)와 함께 작동하여 포함된 주소 정보의 위치를 식별하는 데 도움이 됩니다.

애플리케이션 검사 기능은 내장된 주소 지정 정보의 식별 외에도 세션을 모니터링하여 보조 채널에 대한 포트 번호를 결정합니다. 많은 프로토콜이 보조 TCP 또는 UDP 포트를 열어 성능을 향상시킵니다. 잘 알려진 포트의 초기 세션은 동적으로 할당된 포트 번호를 협상하는 데 사용됩니다.

애플리케이션 검사 기능은 이러한 세션을 모니터링하고, 동적 포트 할당을 식별하며, 특정 세션 동안 이러한 포트에서 데이터 교환을 허용합니다. 멀티미디어 및 FTP 애플리케이션은 이러한 동작을 나타냅니다.

보안 어플라이언스에서 FTP 검사가 활성화되지 않은 경우 이 요청은 취소되며 FTP 세션은 요청된 데이터를 전송하지 않습니다.

FTP 검사가 ASA에서 활성화된 경우 ASA는 제어 채널을 모니터링하고 데이터 채널 열기 요청을 인식하려고 시도합니다. FTP 프로토콜은 데이터 채널 포트 사양을 제어 채널 트래픽에 포함하므로 Security Appliance가 제어 채널에서 데이터 포트 변경을 검사해야 합니다.

ASA는 요청을 인식하면 세션 동안 지속되는 데이터 채널 트래픽에 대한 개방을 일시적으로 생성합니다. 이러한 방식으로, FTP 검사 기능은 제어 채널을 모니터링하고, 데이터 포트 할당을 식별하며, 세션의 길이에 대해 데이터 포트에서 데이터를 교환할 수 있게 한다.

ASA는 전역 검사 클래스 맵을 통해 기본적으로 포트 21 연결에서 FTP 트래픽을 검사합니다. 보안 어플라이언스는 액티브 및 패시브 FTP 세션의 차이도 인식합니다.

FTP 세션이 패시브 FTP 데이터 전송을 지원하는 경우, ASA는 inspect ftp 명령을 통해 사용자의 데이터 포트 요청을 인식하고 1023보다 큰 새 데이터 포트를 엽니다.

inspect ftp 명령 검사는 FTP 세션을 검사하고 네 가지 작업을 수행합니다.

- 동적 보조 데이터 연결 준비
- FTP 명령-응답 시퀀스 추적
- 감사 추적 생성
- NAT를 사용하여 포함된 IP 주소 변환

FTP 애플리케이션 검사는 FTP 데이터 전송을 위한 보조 채널을 준비합니다. 채널은 파일 업로드, 파일 다운로드 또는 디렉토리 나열 이벤트에 대한 응답으로 할당되며 사전 협상되어야 합니다. 포트는 PORT 또는 PASV(227) 명령을 통해 협상됩니다.

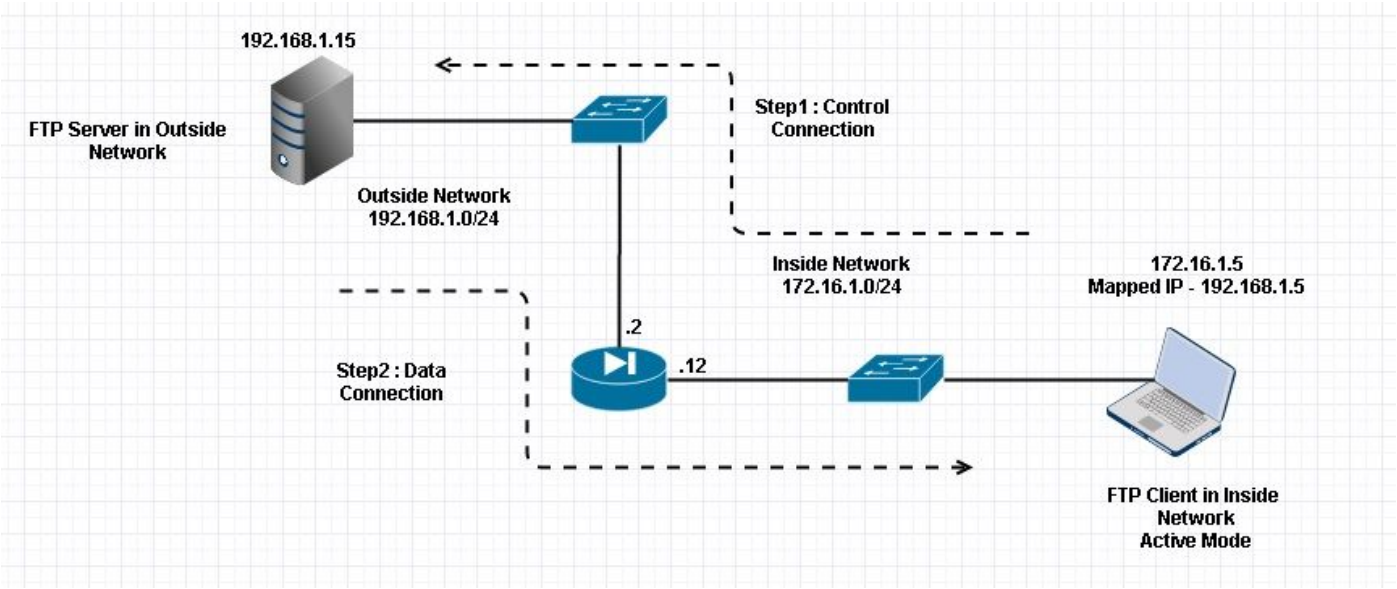
설정

참고: 모든 네트워크 시나리오는 ASA에서 FTP 검사가 활성화된 상태에서 설명합니다.

시나리오 1. 활성 모드에 대해 구성된 FTP 클라이언트

ASA의 내부 네트워크에 연결된 클라이언트 및 외부 네트워크의 서버.

네트워크 다이어그램



참고: 이 컨피그레이션에서 사용되는 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.

이 이미지에 표시된 것처럼, 사용된 네트워크 설정에는 IP 172.16.1.5를 사용하는 내부 네트워크에 클라이언트와 함께 ASA가 있습니다. 서버가 IP 192.168.1.15의 외부 네트워크에 있습니다. 클라이언트는 외부 네트워크에 매핑된 IP 192.168.1.5를 가지고 있습니다.

FTP 검사에서 Dynamic Port Channel(동적 포트 채널)이 열리므로 외부 인터페이스에서 액세스 목록을 허용할 필요가 없습니다.

컨피그레이션 예시:

<#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)#
```

다음을 확인합니다.

연결

<#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

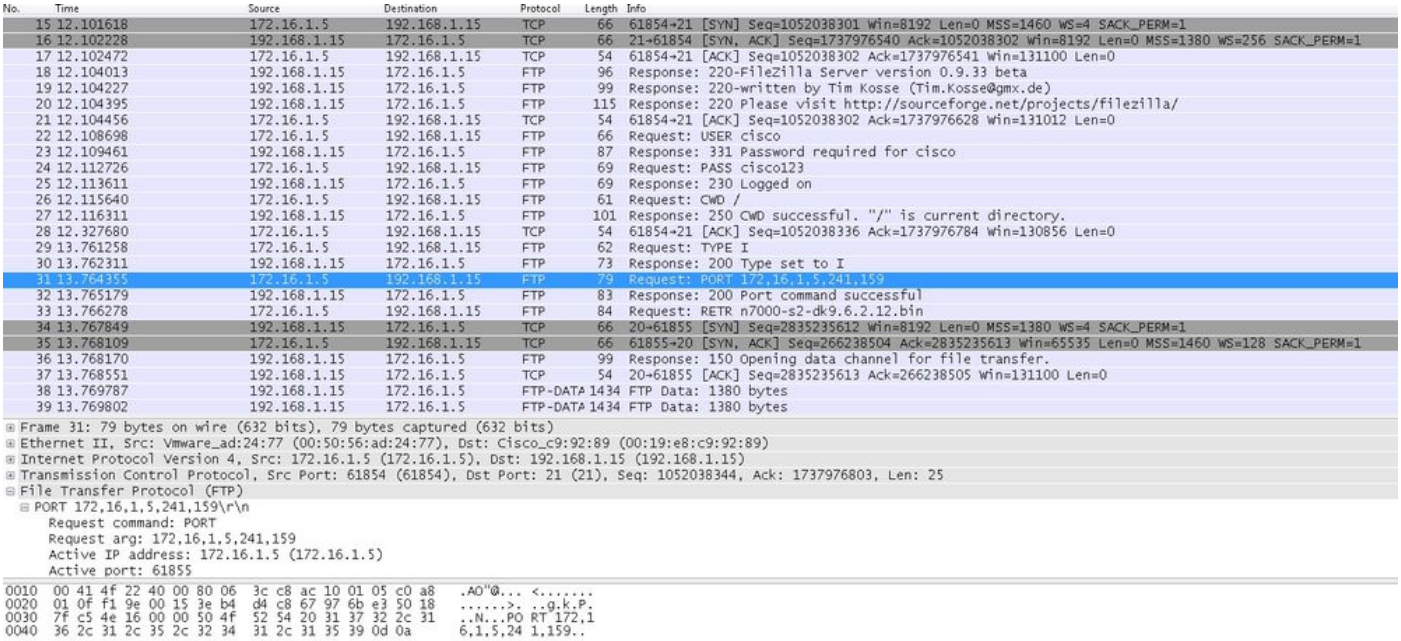
```
 TCP Outside
```

192.168.1.15:21 inside 172.16.1.5:61854

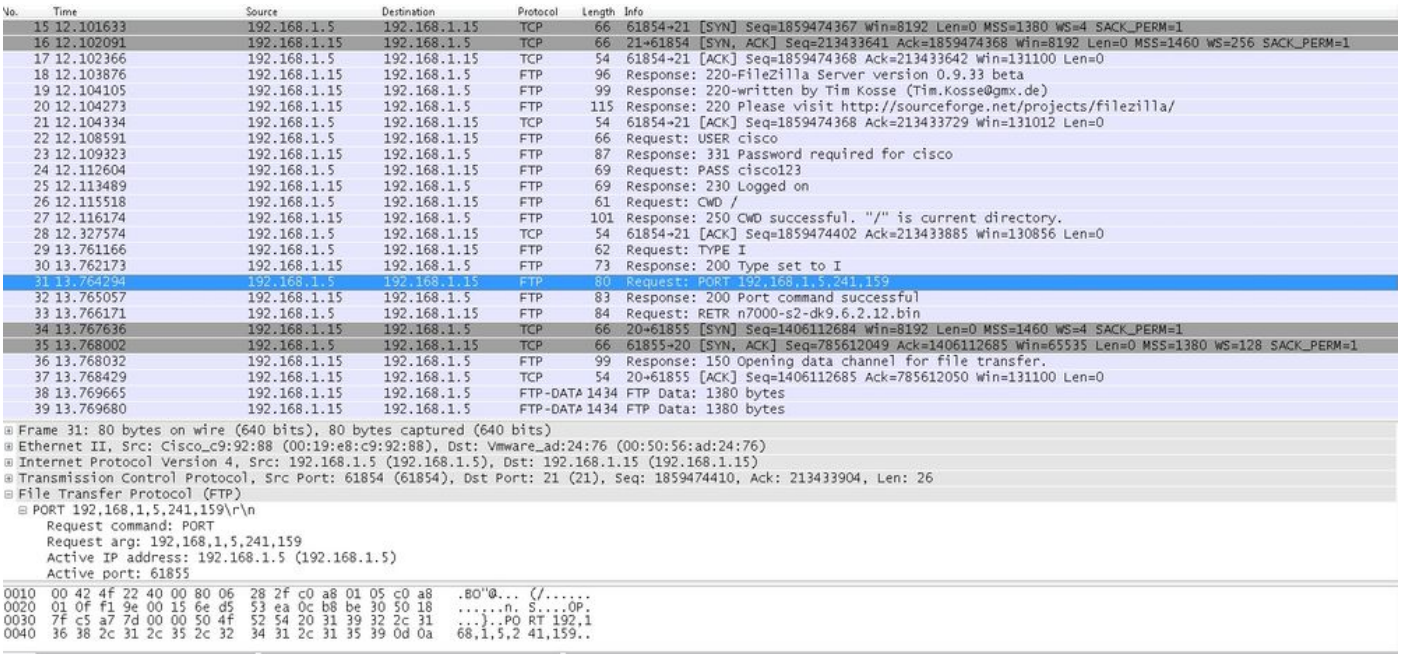
```
, idle 0:00:00, bytes 434, flags UIO
```

여기서 Inside의 클라이언트는 소스 포트 61854과 목적지 포트 21에 대한 연결을 시작합니다. 그런 다음 클라이언트는 6튜플 값과 함께 Port 명령을 전송합니다. 그러면 서버가 소스 포트 20과의 보조/데이터 연결을 시작하고 이 캡처 후에 언급된 단계를 통해 대상 포트가 계산됩니다.

이 이미지에 표시된 내부 인터페이스를 캡처합니다.



이 이미지에 표시된 대로 외부 인터페이스를 캡처합니다.



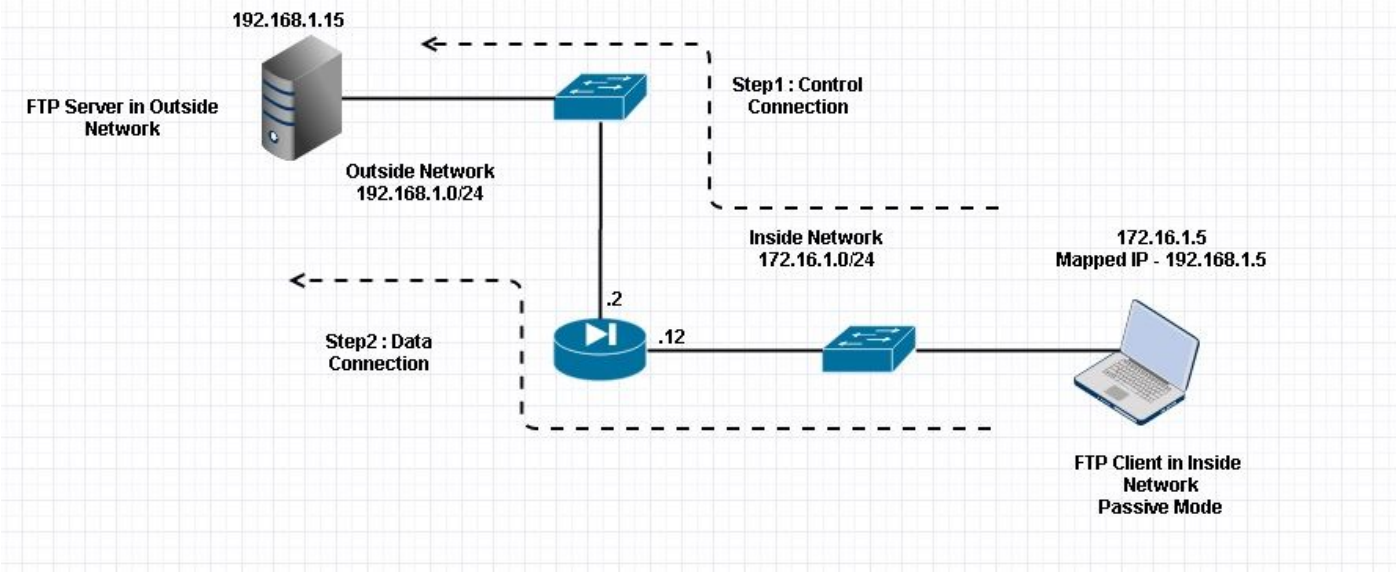
포트 값은 6개 중 마지막 2개를 사용하여 계산됩니다. 왼쪽 4튜플은 IP 주소이고 2튜플은 포트용입니다. 이 그림에서 볼 수 있듯이 IP 주소는 192.168.1.5이고 241*256 + 159 = 61855입니다.

Capture(캡처)는 FTP 검사가 활성화된 경우 Port Commands(포트 명령)의 값이 변경되었음을 보여줍니다. Inside Interface Capture는 IP의 실제 값을 보여주며 Client for Server가 데이터 채널용 클라이언트에 연결하기 위해 보낸 포트를 보여주고 Outside Interface Capture는 매핑된 주소를 보여줍니다.

시나리오 2. 수동 모드로 구성된 FTP 클라이언트

ASA의 내부 네트워크에 있는 클라이언트 및 외부 네트워크에 있는 서버

네트워크 다이어그램



연결

<#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

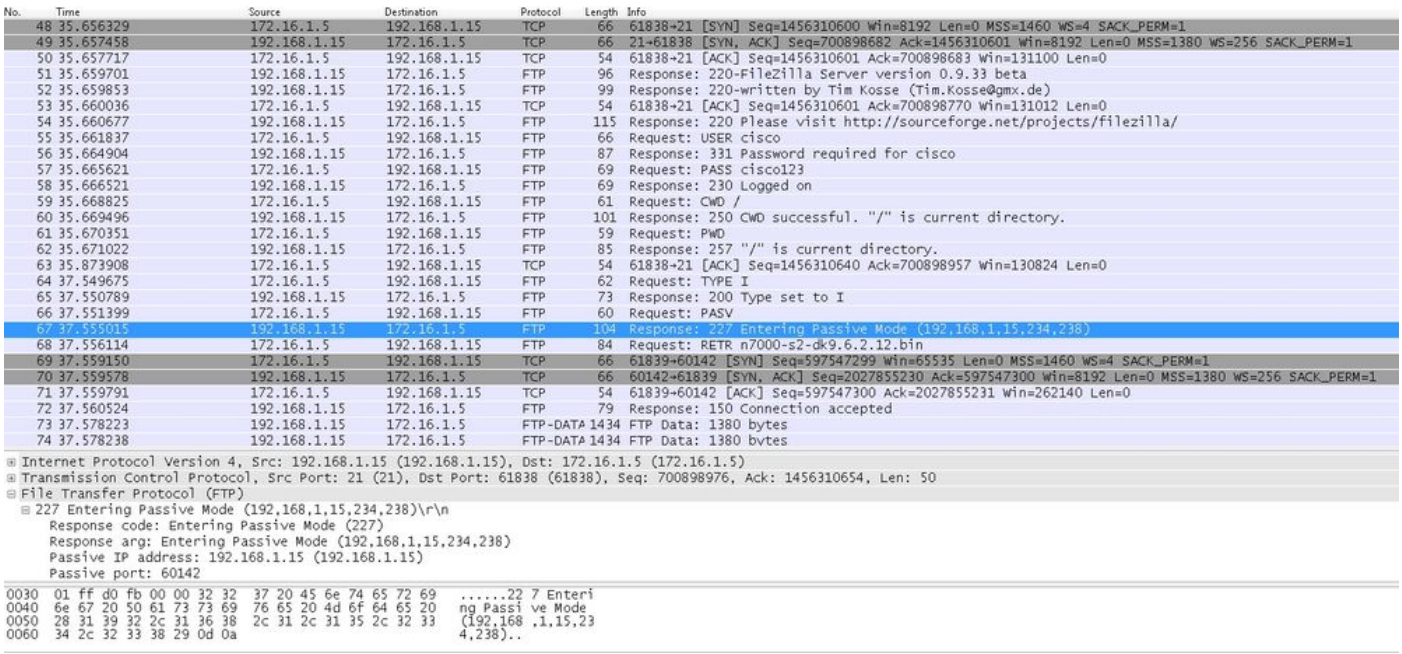
192.168.1.15:21 inside 172.16.1.5:61838

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

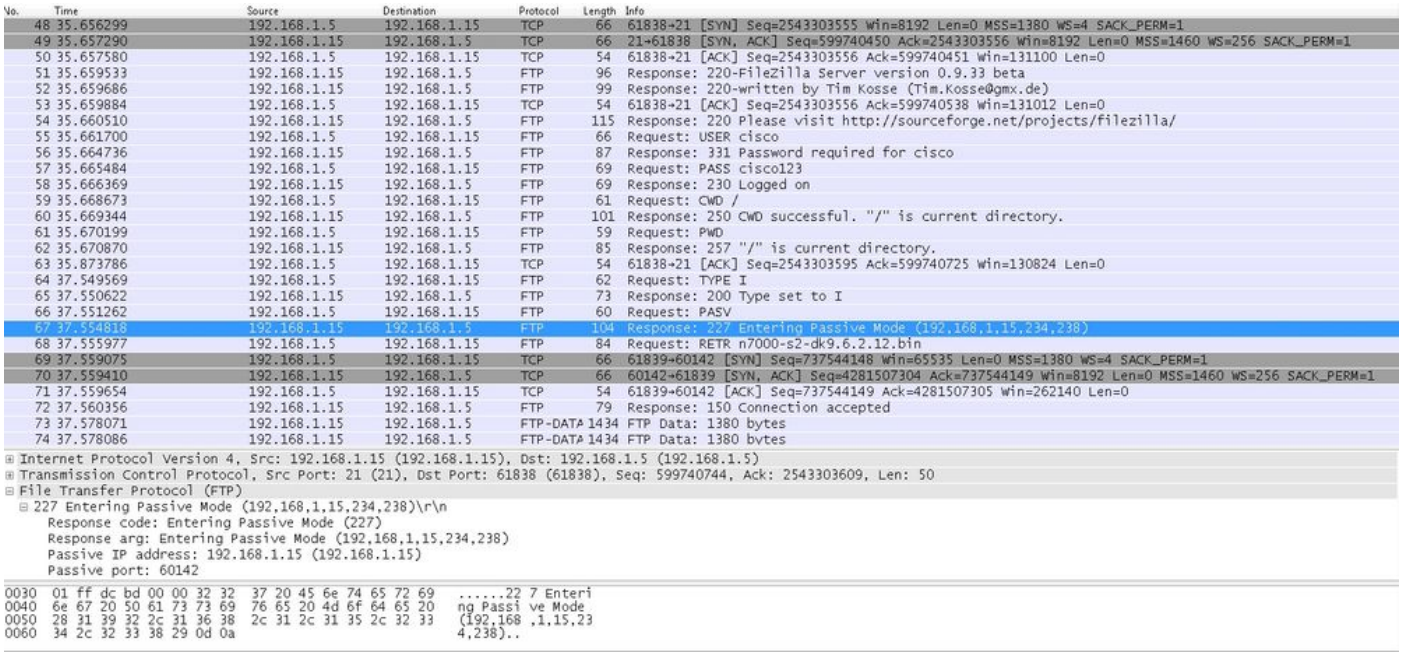
여기서 내부 클라이언트는 소스 포트 61838 목적지 포트 21과의 연결을 시작합니다. 패시브 FTP이

므로 클라이언트는 두 연결을 모두 시작합니다. 따라서 클라이언트가 PASV 명령을 전송하면 서버는 6 튜플 값으로 응답하고 클라이언트는 데이터 연결을 위해 해당 소켓에 연결합니다.

이 이미지에 표시된 내부 인터페이스를 캡처합니다.



이 이미지에 표시된 대로 외부 인터페이스를 캡처합니다.



포트에 대한 계산은 동일하게 유지됩니다.

앞에서 언급한 것처럼 FTP 검사가 활성화된 경우 ASA는 포함된 IP 값을 다시 씁니다. 또한 데이터 연결을 위해 동적 포트 채널을 엽니다.

다음과 같은 경우 연결 세부 정보입니다. FTP 검사 사용 안 함

연결:

<#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 검사가 없으면 포트 명령을 다시 보내기만 시도하지만, 외부에서 Original IP가 NAT되지 않은 PORT를 수신하므로 응답이 없습니다. 덤프에서도 같은 현상이 나타났습니다.

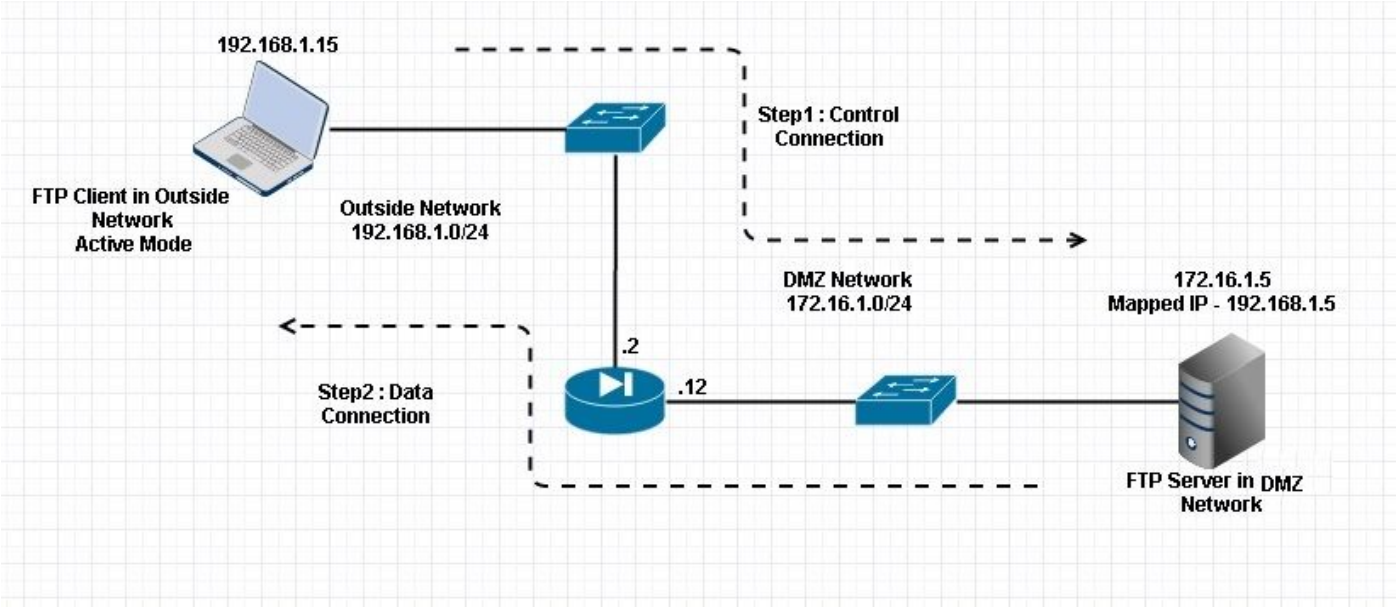
컨피그레이션 터미널 모드에서는 fixup protocol ftp 21 명령이 없으면 FTP 검사를 비활성화할 수 있습니다.

FTP 검사가 없으면 클라이언트가 Inside에 있을 때 PASV 명령만 작동합니다. Inside에서 오는 포트 명령이 없고, 이 두 연결은 모두 Inside에서 시작됩니다.

시나리오 3. 활성 모드에 대해 구성된 FTP 클라이언트

ASA의 외부 네트워크에 있는 클라이언트 및 DMZ 네트워크에 있는 서버

네트워크 다이어그램



설정:

<#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)#
```

다음을 확인합니다.

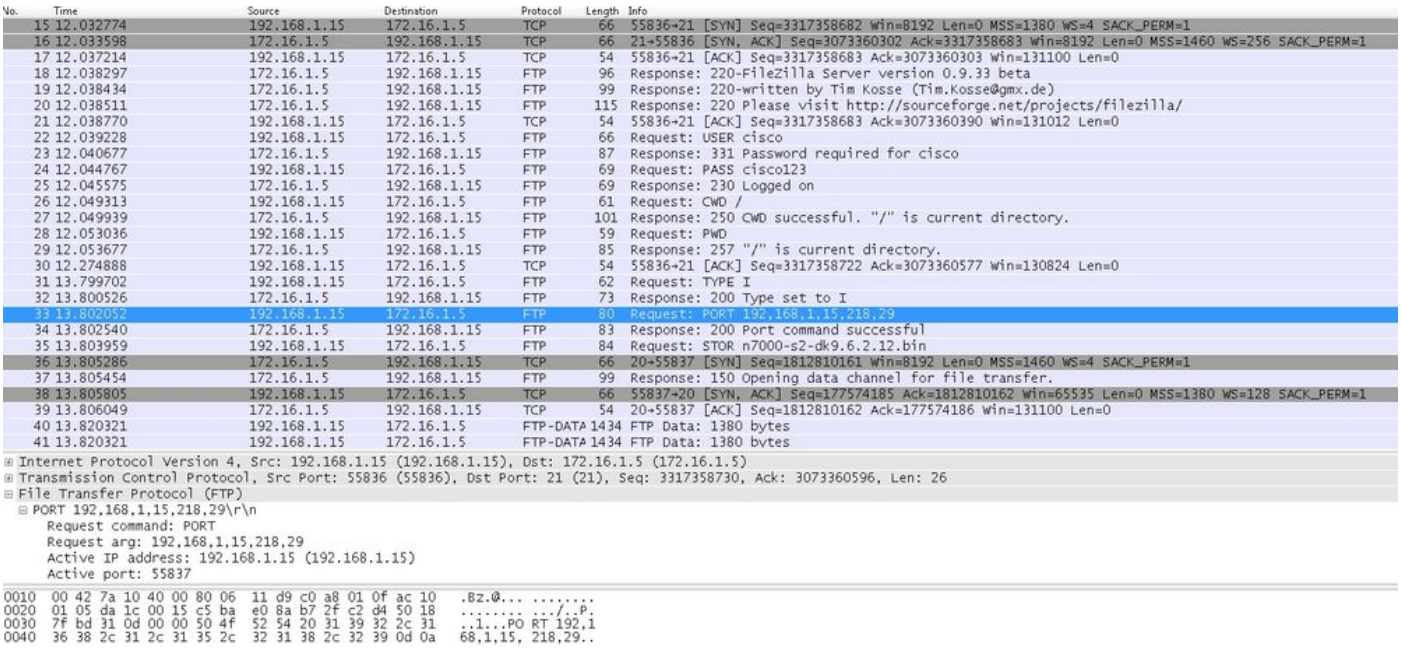
연결:

<#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
```

이 이미지에 표시된 대로 DMZ 인터페이스를 캡처합니다.

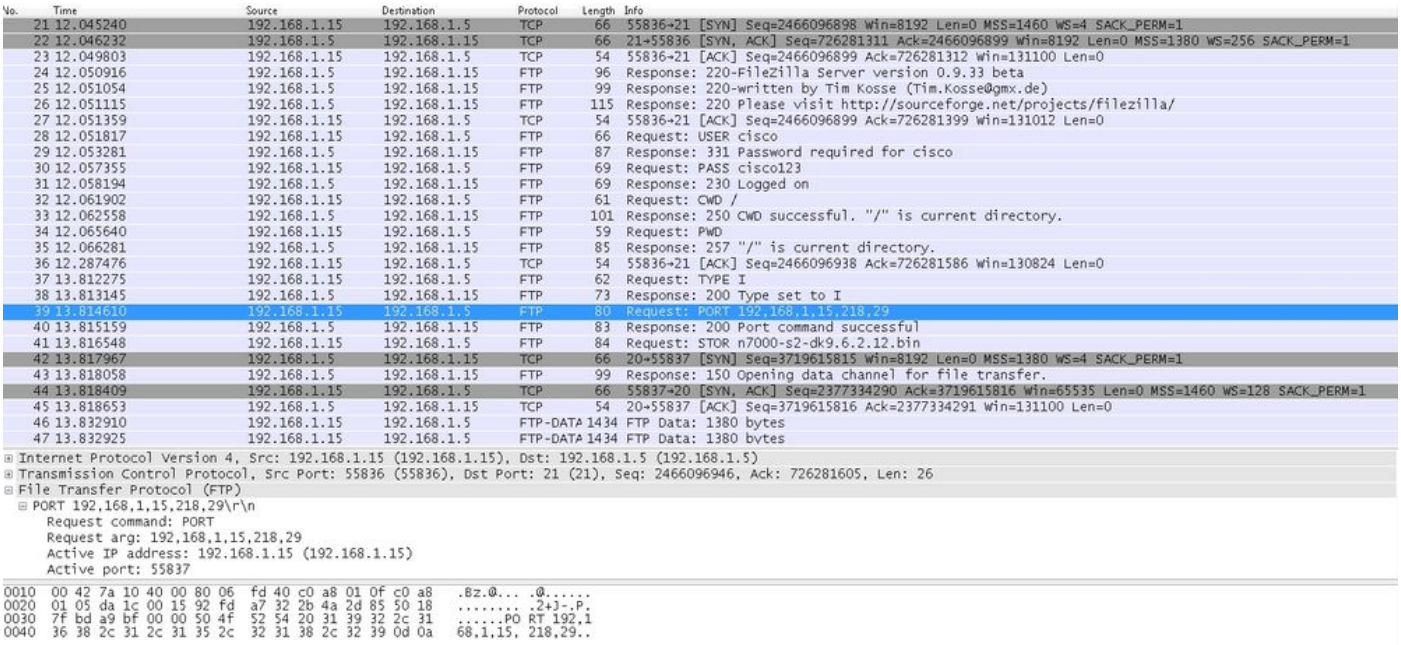


No.	Time	Source	Destination	Protocol	Length	Info
15	12.032774	192.168.1.15	172.16.1.5	TCP	66	55836→21 [SYN] Seq=3317358682 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
16	12.033598	172.16.1.5	192.168.1.15	TCP	66	21→55836 [SYN, ACK] Seq=3073360302 Ack=3317358683 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
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..
```

이 이미지에 표시된 대로 외부 인터페이스를 캡처합니다.

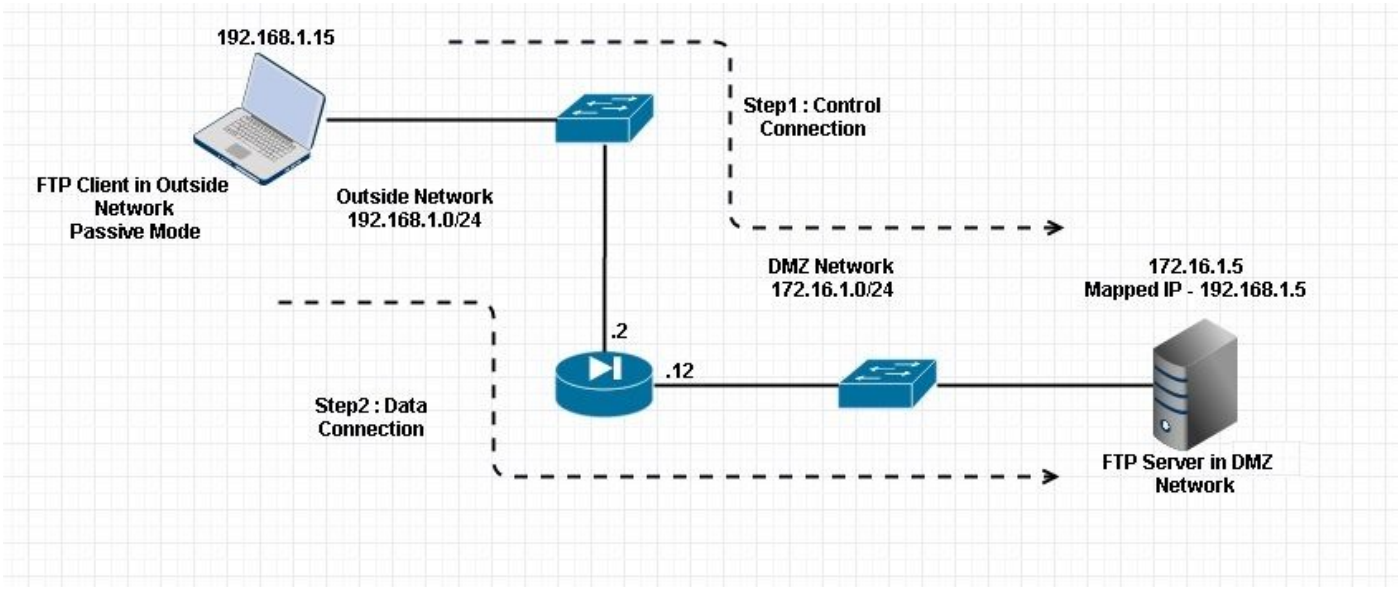


여기서 클라이언트는 액티브 모드 클라이언트 192.168.1.15를 실행하고 포트 21의 DMZ에 있는 서버에 대한 연결을 시작합니다. 그런 다음 클라이언트는 6튜플 값이 포함된 port 명령을 서버에 전송하여 해당 동적 포트에 연결합니다. 그런 다음 서버는 소스 포트와의 데이터 연결을 20으로 시작합니다.

시나리오 4. 수동 모드를 실행하는 FTP 클라이언트

ASA의 외부 네트워크에 있는 클라이언트 및 DMZ 네트워크에 있는 서버

네트워크 다이어그램



연결


```
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
```

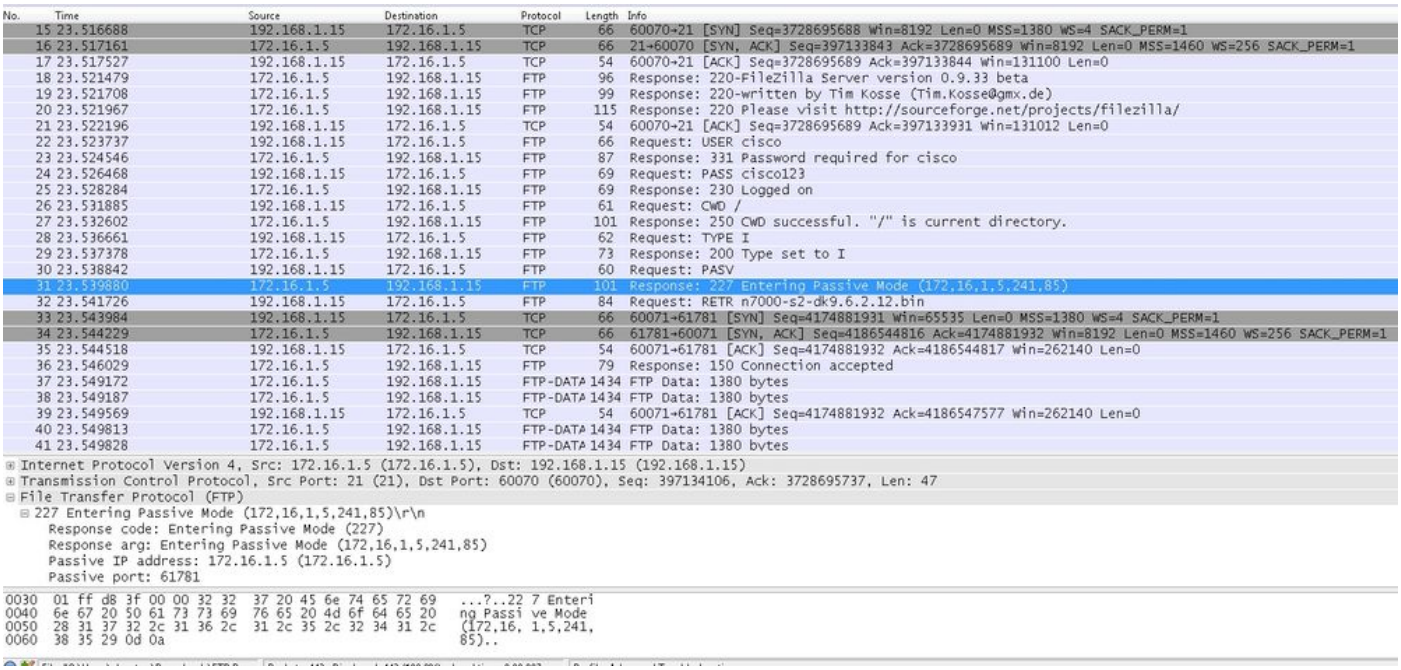
<--- Dynamic channel Open

```
TCP
```

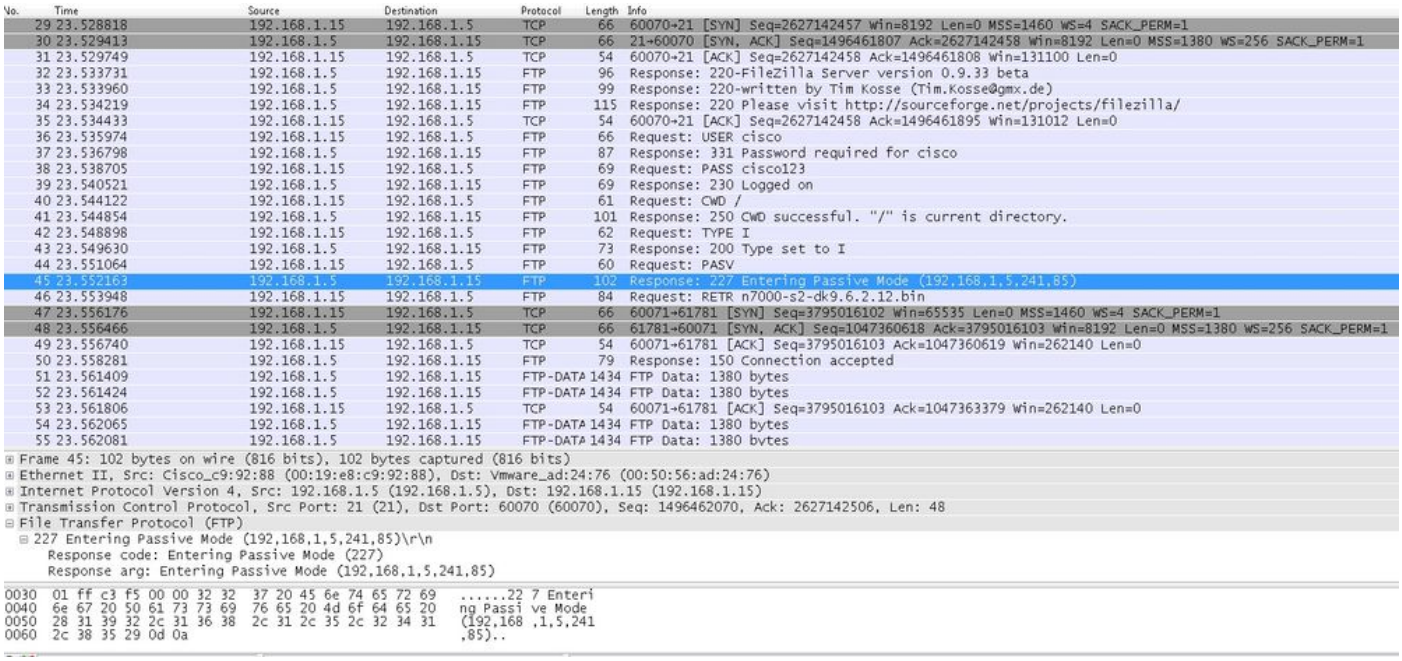
Outside 192.168.1.15:60070 DMZ 172.16.1.5:21

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

이 이미지에 표시된 대로 DMZ 인터페이스를 캡처합니다.



이 이미지에 표시된 대로 외부 인터페이스를 캡처합니다.



기본 FTP 애플리케이션 검사 구성

기본적으로 컨피그레이션에는 모든 기본 애플리케이션 검사 트래픽과 일치하는 정책이 포함되어 있으며 모든 인터페이스의 트래픽에 검사가 적용됩니다(글로벌 정책). 기본 애플리케이션 검사 트래픽에는 각 프로토콜의 기본 포트에 대한 트래픽이 포함됩니다.

글로벌 정책은 하나만 적용할 수 있으므로, 예를 들어 검사를 비표준 포트에 적용하거나 기본적으로 활성화되지 않은 검사를 추가하려면 기본 정책을 수정하거나 비활성화하고 새 정책을 적용해야 합니다. 모든 기본 포트 목록은 기본 검사 정책을 참조하십시오.

1. policy-map global_policy 명령을 실행합니다.

```
<#root>

 ASA(config)#

policy-map global_policy
```

2. class inspection_default 명령을 실행합니다.

```
<#root>

 ASA(config-pmap)#

class inspection_default
```

3. inspect FTP 명령을 실행합니다.

<#root>

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

4. inspect FTP strict 명령을 사용할 수 있는 옵션이 있습니다. 이 명령은 웹 브라우저가 FTP 요청에 포함된 명령을 전송하지 못하도록 하여 보호된 네트워크의 보안을 강화합니다.

   인터페이스에서 strict 옵션을 활성화하면 FTP 검사는 다음 동작을 적용합니다.

   - FTP 명령이 승인되어야 보안 어플라이언스에서 새 명령을 허용합니다.
   - Security Appliance는 내장된 명령을 전송하는 연결을 삭제합니다
   - 227 및 PORT 명령은 오류 문자열에 표시되지 않는지 확인합니다

   경고: strict 옵션을 사용하면 FTP RFC를 엄격하게 준수하지 않는 FTP 클라이언트가 실패할 수 있습니다. strict 옵션 사용에 대한 자세한 내용은 strict 옵션 사용을 참조하십시오.

비표준 TCP 포트에서 FTP 프로토콜 검사 구성

다음 컨피그레이션 라인으로 비표준 TCP 포트에 대한 FTP 프로토콜 검사를 구성할 수 있습니다 (XXXX를 새 포트 번호로 대체).

<#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
```

다음을 확인합니다.

컨피그레이션을 성공적으로 수행하려면 show service-policy 명령을 실행합니다. 또한 show service-policy inspect ftp 명령을 실행하여 출력을 FTP 검사로 제한합니다.

<#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 검사는 기본적으로 사용됩니다.

보안 어플라이언스는 TFTP 트래픽을 검사하고 필요한 경우 동적으로 연결 및 변환을 생성하여 TFTP 클라이언트와 서버 간의 파일 전송을 허용합니다. 특히 검사 엔진은 TFTP RRQ(읽기 요청), WRQ(쓰기 요청) 및 ERROR(오류 알림)를 검사합니다.

필요한 경우 유효한 RRQ 또는 WRQ를 수신할 때 동적 보조 채널 및 PAT 변환이 할당됩니다. 이 보조 채널은 이후에 TFTP에서 파일 전송 또는 오류 알림에 사용됩니다.

TFTP 서버만 보조 채널을 통해 트래픽을 시작할 수 있으며, TFTP 클라이언트와 서버 사이에는 불완전한 보조 채널이 하나만 존재할 수 있습니다. 서버에서 오류 알림을 보내면 보조 채널이 닫힙니다.

고정 PAT를 사용하여 TFTP 트래픽을 리디렉션하는 경우 TFTP 검사를 활성화해야 합니다.

기본 TFTP 애플리케이션 검사 구성

기본적으로 컨피그레이션에는 모든 기본 애플리케이션 검사 트래픽과 일치하는 정책이 포함되어 있으며 모든 인터페이스의 트래픽에 검사가 적용됩니다(글로벌 정책). 기본 애플리케이션 검사 트래픽에는 각 프로토콜의 기본 포트에 대한 트래픽이 포함됩니다.

하나의 전역 정책만 적용할 수 있습니다. 따라서 글로벌 정책을 변경하려면(예: 검사를 비표준 포트에 적용하거나 기본적으로 활성화되지 않은 검사를 추가하려면) 기본 정책을 수정하거나 비활성화하고 새 정책을 적용해야 합니다. 모든 기본 포트 목록은 기본 검사 정책을 참조하십시오.

1. policy-map global_policy 명령을 실행합니다.

<#root>

ASA(config)#

policy-map global_policy

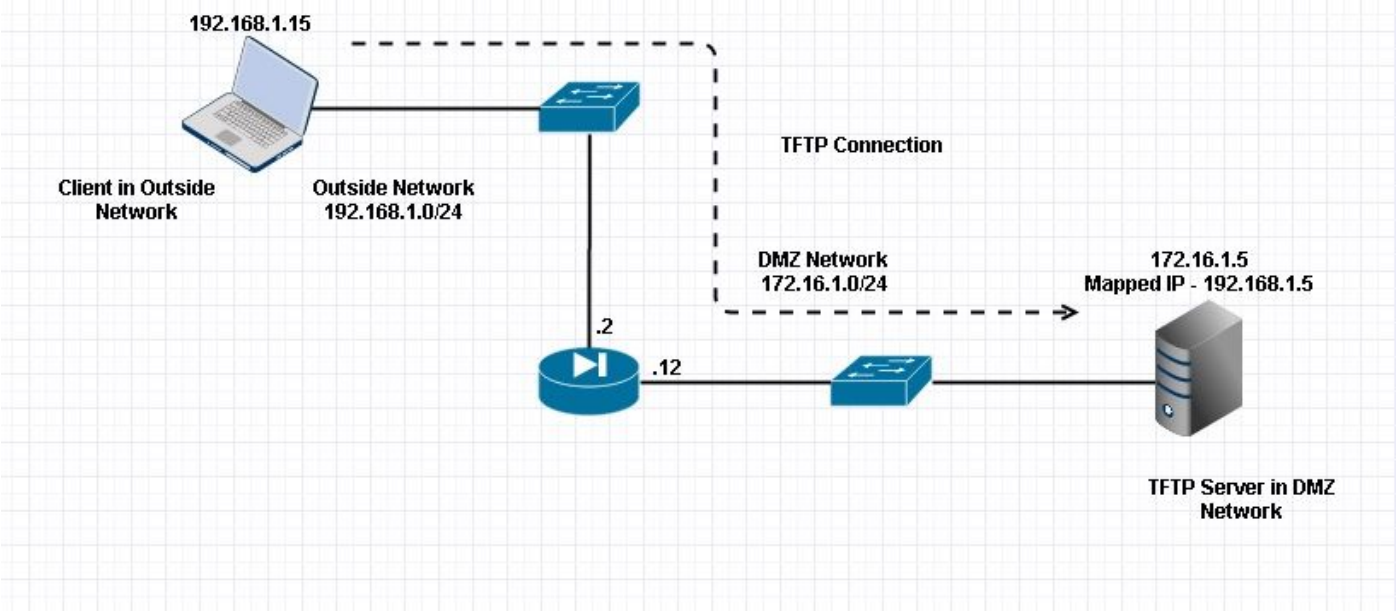
2. class inspection_default 명령을 실행합니다.

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

3. inspect TFTP 명령을 실행합니다.

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

네트워크 다이어그램



여기서 클라이언트는 외부 네트워크에 구성되어 있습니다. TFTP 서버는 DMZ 네트워크에 배치됩니다. 서버는 외부 서브넷에 있는 IP 192.168.1.5에 매핑됩니다.

컨피그레이션 예시:

```
<#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)#
```

다음을 확인합니다.

컨피그레이션을 성공적으로 수행하려면 show service-policy 명령을 실행합니다. 또한 show service-policy inspect tftp 명령을 실행하여 출력을 TFTP 검사로 제한합니다.

<#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#
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

패킷 추적기

내부 네트워크의 클라이언트

<#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
```

외부 네트워크의 클라이언트

<#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
```

패킷 추적기 모두에서 볼 수 있듯이, 트래픽은 해당 NAT 문 및 FTP 검사 정책에 도달합니다. 또한 필요한 인터페이스도 남겨 둡니다.

트러블슈팅 중에 ASA 인그레스 및 이그레스 인터페이스를 캡처하여 ASA Embedded IP 주소 재쓰기가 제대로 작동하는지 확인하고 ASA에서 동적 포트가 허용되는지 연결을 확인할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.