ASA 8.3 이상: Enable FTP/TFTP Services 컨피그레이션 예

목차

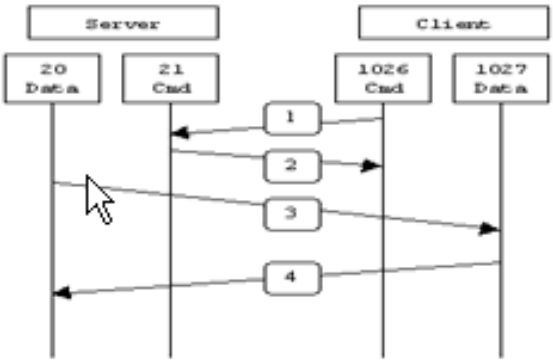
소개

이 문서에서는 네트워크 외부의 사용자가 DMZ 네트워크의 FTP 및 TFTP 서비스에 액세스하는 데 필요한 단계를 설명합니다.

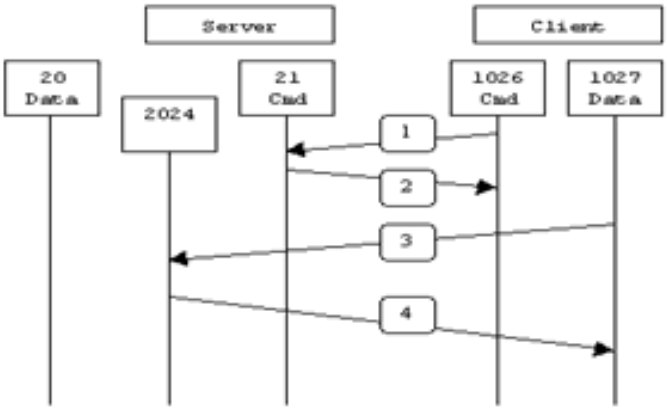
FTP(File Transfer Protocol)

FTP에는 두 가지 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 모드에서 클라이언트는 임의의 비권한 포트(N>1023)에서 FTP 서버의 명령 포트(21)로 연결합니다. 그런 다음 클라이언트가 포트 N+1을 수신하기 시작하고 FTP 명령 포트 N+1을 FTP 서버로 전송합니다. 그런 다음 서버는 로컬 데이터 포트(포트 20)에서 클라이언트의 지정된 데이터 포트에 다시 연결합니다.

패시브 FTP 모드에서 클라이언트는 서버에 대한 두 연결을 모두 시작합니다. 이렇게 하면 서버에서 클라이언트로의 수신 데이터 포트 연결을 필터링하는 방화벽 문제가 해결됩니다. FTP 연결이 열리면 클라이언트는 로컬에서 두 개의 권한이 없는 임의의 포트를 엽니다(N>1023 및 N+1). 첫 번째 포트는 포트 21에서 서버에 연결합니다. 그러나 그런 다음 **port** 명령을 실행하여 서버가 데이터 포트에 다시 연결되도록 하는 대신 클라이언트는 **PASV** 명령을 실행합니다. 그 결과 서버는 권한 없는 임의의 포트(P>1023)를 열고 **포트 P** 명령을 클라이언트로 다시 보냅니다. 그런 다음 클라이언트는 데이터를 전송하기 위해 서버의 포트 N+1에서 포트 P로 연결을 시작합니다. 보안 어플라이언스에서 **inspection** 명령 컨피그레이션이 없으면 내부 사용자의 아웃바운드 FTP는 패시브 모드에서만 작동합니다. 또한 FTP 서버로 향하는 인바운드 외부의 사용자는 액세스가 거부됩니다.

PIX/ASA 7.x 참조: Cisco ASA(Adaptive Security Appliance) 버전 8.2 이하의 동일한 컨피그레이션에 대해 FTP/TFTP Services Configuration Example을 활성화합니다.

TFTP(Trivial File Transfer Protocol)

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

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 필수 인터페이스 간에는 기본적인 통신이 있습니다.
- DMZ 네트워크에 FTP 서버를 구성했습니다.

사용되는 구성 요소

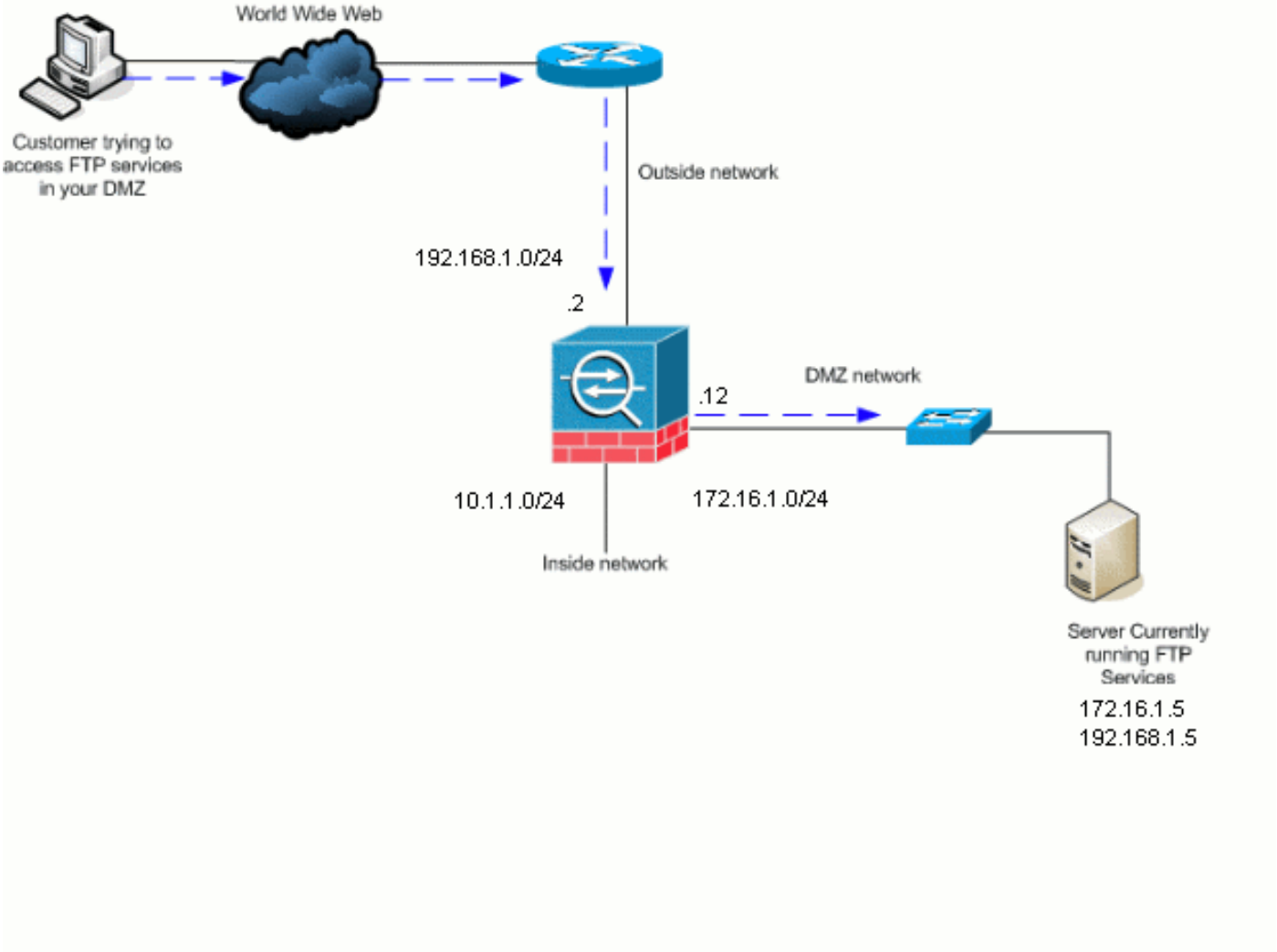
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 8.4(1) 소프트웨어 이미지를 실행하는 ASA 5500 Series Adaptive Security Appliance
- FTP 서비스를 실행하는 Windows 2003 Server
- TFTP 서비스를 실행하는 Windows 2003 Server
- 네트워크 외부에 있는 클라이언트 PC

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

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 실습 환경에서 사용된 RFC 1918 주소입니다.

관련 제품

이 컨피그레이션은 Cisco Adaptive Security Appliance 8.3 이상에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

Security Appliance는 Adaptive Security Algorithm 기능을 통한 애플리케이션 검사를 지원합니다. Security Appliance는 Adaptive Security Algorithm에서 사용하는 스테이트풀 애플리케이션 검사를 통해 방화벽을 통과하는 각 연결을 추적하고 해당 연결이 유효한지 확인합니다. 상태 저장 검사를 통해 방화벽은 연결 상태를 모니터링하여 상태 테이블에 배치할 정보를 컴파일합니다. 관리자가 정의한 규칙 외에도 상태 테이블을 사용하면 필터링 결정은 이전에 방화벽을 통과한 패킷에 의해 설정된 컨텍스트를 기반으로 합니다. 애플리케이션 검사의 구현은 다음 작업으로 구성됩니다.

- 트래픽을 식별합니다.
- 트래픽에 검사를 적용합니다.
- 인터페이스에서 검사를 활성화합니다.

고급 프로토콜 처리

FTP

일부 애플리케이션은 Cisco Security Appliance 애플리케이션 검사 기능을 통해 특별한 처리를 필요로 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 임베디드 주소 지정 정보의 위치를 식별합니다.

내장된 주소 지정 정보를 식별하는 것 외에도 애플리케이션 검사 기능은 세션을 모니터링하여 보조 채널의 포트 번호를 확인합니다. 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 종류의 동작을 나타냅니다.

FTP 프로토콜은 FTP 세션당 2개의 포트를 사용하기 때문에 몇 가지 특별한 처리가 필요합니다. FTP 프로토콜은 데이터 전송을 위해 활성화될 때 두 개의 포트를 사용합니다. 각각 포트 21과 20을 사용하는 컨트롤 채널 및 데이터 채널. 제어 채널을 통해 FTP 세션을 시작하는 사용자는 해당 채널을 통해 모든 데이터 요청을 수행합니다. 그런 다음 FTP 서버가 서버 포트 20에서 사용자 컴퓨터로 포트를 열라는 요청을 시작합니다. FTP는 항상 데이터 채널 통신에 포트 20을 사용합니다. 보안 어플라이언스에서 FTP 검사가 활성화되지 않은 경우 이 요청이 무시되고 FTP 세션은 요청된 데이터를 전송하지 않습니다. 보안 어플라이언스에서 FTP 검사가 활성화된 경우 보안 어플라이언스는 제어 채널을 모니터링하고 데이터 채널 열기 요청을 인식하려고 시도합니다. FTP 프로토콜은 제어 채널 트래픽에 데이터 채널 포트 사양을 포함하므로, Security Appliance가 제어 채널을 통해 데이터 포트 변경을 검사해야 합니다. Security Appliance에서 요청을 인식하면 세션 동안 지속되는 데이터 채널 트래픽에 대한 오프닝을 일시적으로 생성합니다. 이렇게 하면 FTP 검사 기능은 제어 채널을 모니터링하고 데이터 포트 할당을 식별하며 세션 기간 동안 데이터 포트에서 데이터를 교환할 수

있습니다.

보안 어플라이언스는 기본적으로 전역 검사 클래스 맵을 통해 FTP 트래픽에 대한 포트 21 연결을 검사합니다. 또한 보안 어플라이언스는 활성 FTP 세션과 수동 FTP 세션의 차이점도 인식합니다. FTP 세션이 패시브 FTP 데이터 전송을 지원하는 경우 Security Appliance는 inspect **ftp** 명령을 통해 사용자의 데이터 포트 요청을 인식하고 1023보다 큰 새 데이터 포트를 엽니다.

FTP 애플리케이션 검사는 FTP 세션을 검사하고 4가지 작업을 수행합니다.

- 동적 보조 데이터 연결 준비
- FTP 명령-응답 시퀀스 추적
- 감사 추적 생성
- NAT를 사용하여 임베디드 IP 주소를 변환합니다.

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

TFTP

TFTP 검사는 기본적으로 활성화되어 있습니다.

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

필요한 경우 동적 보조 채널 및 PAT 변환은 유효한 RRQ 또는 WRQ의 수신에 할당됩니다. 이 보조 채널은 이후에 파일 전송 또는 오류 알림에 TFTP에서 사용됩니다.

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

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

기본 FTP 애플리케이션 검사 구성

기본적으로 컨피그레이션에는 모든 기본 애플리케이션 검사 트래픽과 일치하는 정책이 포함되어 있으며 모든 인터페이스의 트래픽에 검사를 적용합니다(글로벌 정책). 기본 애플리케이션 검사 트래픽에는 각 프로토콜의 기본 포트에 대한 트래픽이 포함됩니다. 전역 정책을 하나만 적용할 수 있으므로, 예를 들어, 비표준 포트에 검사를 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**.
   ```
   ASA(config)#policy-map global_policy
   ```

2. class inspection_default 명령**을 실행합니다**.
   ```
   ASA(config-pmap)#class inspection_default
   ```

3. inspect FTP **명령을 실행합니다**.
   ```
   ASA(config-pmap-c)#inspect FTP
   ```

inspect FTP strict **명령**을 사용할 수 있는 옵션**이 있습니다**. 이 명령은 웹 브라우저가 FTP 요청에 포함된 명령을 전송하지 못하도록 하여 보호된 네트워크의 보안을 향상시킵니다.인터페이스에서 **strict 옵션을 활성화한** 후 **FTP 검사는** 다음 동작을 적용합니다.보안 어플라이언스에서 새 명령을 허용하려면 먼저 FTP 명령을 승인해야 합니다.Security Appliance는 포함된 명령을 전송하는 연결을 삭제합니다.**227** 및 **PORT** 명령은 오류 문자열에 나타나지 않도록 확인합니다.**경고:** strict 옵션을 사용하면 FTP RFC를 엄격하게 준수하지 않는 FTP 클라이언트가 실패할 수 있습니다. *strict **옵션***의 사용에 대한 자세한 내용은 Using the strict Option을 **참조하십시오**.

컨피그레이션 예

장치 이름 1

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

 ASA Version 8.4(1)
!
hostname ASA
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif Inside
 security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
  security-level 50
  ip address 172.16.1.12 255.255.255.0
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Management0/0
  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
!--- Permit inbound FTP data traffic. access-list 100
extended permit tcp any host 192.168.1.5 eq ftp-data
!
!--- Object groups are created to define the hosts.
object network DMZ
host 172.16.1.5
object network DMZ-out
host 192.168.1.5
```

```
!--- Configure manual NAT nat (DMZ,outside) source
static DMZ DMZ-out
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)#
```

비표준 TCP 포트에서 FTP 프로토콜 검사 구성

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

```
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
```

기본 TFTP 애플리케이션 검사 구성

기본적으로 컨피그레이션에는 모든 기본 애플리케이션 검사 트래픽과 일치하는 정책이 포함되어 있으며 모든 인터페이스의 트래픽에 검사를 적용합니다(글로벌 정책). 기본 애플리케이션 검사 트래픽에는 각 프로토콜의 기본 포트에 대한 트래픽이 포함됩니다. 하나의 전역 정책만 적용할 수 있습니다. 따라서 전역 정책(예: 비표준 포트에 검사를 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.
   ```
   ASA(config)#policy-map global_policy
   ```

2. class inspection_default 명령을 실행합니다.
   ```
   ASA(config-pmap)#class inspection_default
   ```

3. inspect TFTP 명령을 실행합니다.
   ```
   ASA(config-pmap-c)#inspect TFTP
   ```

컨피그레이션 예

장치 이름 1

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

 ASA Version 8.4(1)
!
hostname ASA
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif Inside
 security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
  security-level 50
  ip address 172.16.1.12 255.255.255.0
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Management0/0
  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 DMZ
host 172.16.1.5
object network DMZ-out
host 192.168.1.5
```

```
!--- Configure manual NAT nat (DMZ,outside) source
static DMZ DMZ-out
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 사용합니다. 또한 show service-policy inspect ftp **명령**을 사용해서만 출력을 FTP 검사**로 제한합니다.**

```
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#
```

문제 해결

현재 이 구성에 대해 사용 가능한 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliance

- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems