ASA 7.x/PIX 6.x 이상: 포트 구성 열기/차단 예

목차

소개

이 문서에서는 보안 어플라이언스에서 http 또는 ftp와 같은 다양한 유형의 트래픽에 대한 포트를 열거나 차단하는 방법에 대한 샘플 컨피그레이션을 제공합니다.

참고: "포트 열기" 및 "포트 허용" 용어는 동일한 의미를 제공합니다. 마찬가지로 "포트 차단" 및 "포트 제한"도 같은 의미를 제공합니다.

사전 요구 사항

요구 사항

이 문서에서는 PIX/ASA가 구성되어 제대로 작동한다고 가정합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 8.2(1)를 실행하는 Cisco 5500 Series ASA(Adaptive Security Appliance)
- Cisco ASDM(Adaptive Security Device Manager) 버전 6.3(5)

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.

관련 제품

이 컨피그레이션은 소프트웨어 버전 6.x 이상에서 Cisco 500 Series PIX Firewall Appliance와 함께 사용할 수도 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

각 인터페이스에는 0(최저)에서 100(최고)까지의 보안 레벨이 있어야 합니다. 예를 들어 내부 호스트 네트워크와 같이 가장 안전한 네트워크를 레벨 100에 할당해야 합니다. 인터넷에 연결된 외부 네트워크는 레벨 0이 될 수 있지만 DMZ와 같은 다른 네트워크는 그 사이에 배치될 수 있습니다. 동일한 보안 레벨에 여러 인터페이스를 할당할 수 있습니다.

기본적으로 모든 포트는 외부 인터페이스(보안 레벨 0)에서 차단되며 모든 포트는 보안 어플라이언스의 내부 인터페이스(보안 레벨 100)에서 열립니다. 이렇게 하면 모든 아웃바운드 트래픽이 컨피그레이션 없이 보안 어플라이언스를 통과할 수 있지만, 보안 어플라이언스의 액세스 목록 및 고정 명령 컨피그레이션에서 인바운드 트래픽을 허용할 수 있습니다.

참고: 일반적으로 모든 포트는 Lower Security Zone에서 Higher Security Zone으로 차단되며, 모든 포트는 Higher Security Zone에서 Lower Security Zone으로 열려 있으므로 인바운드 및 아웃바운드 트래픽 모두에 대해 스테이트풀 검사가 활성화됩니다.

이 섹션은 다음과 같은 하위 섹션으로 구성됩니다.

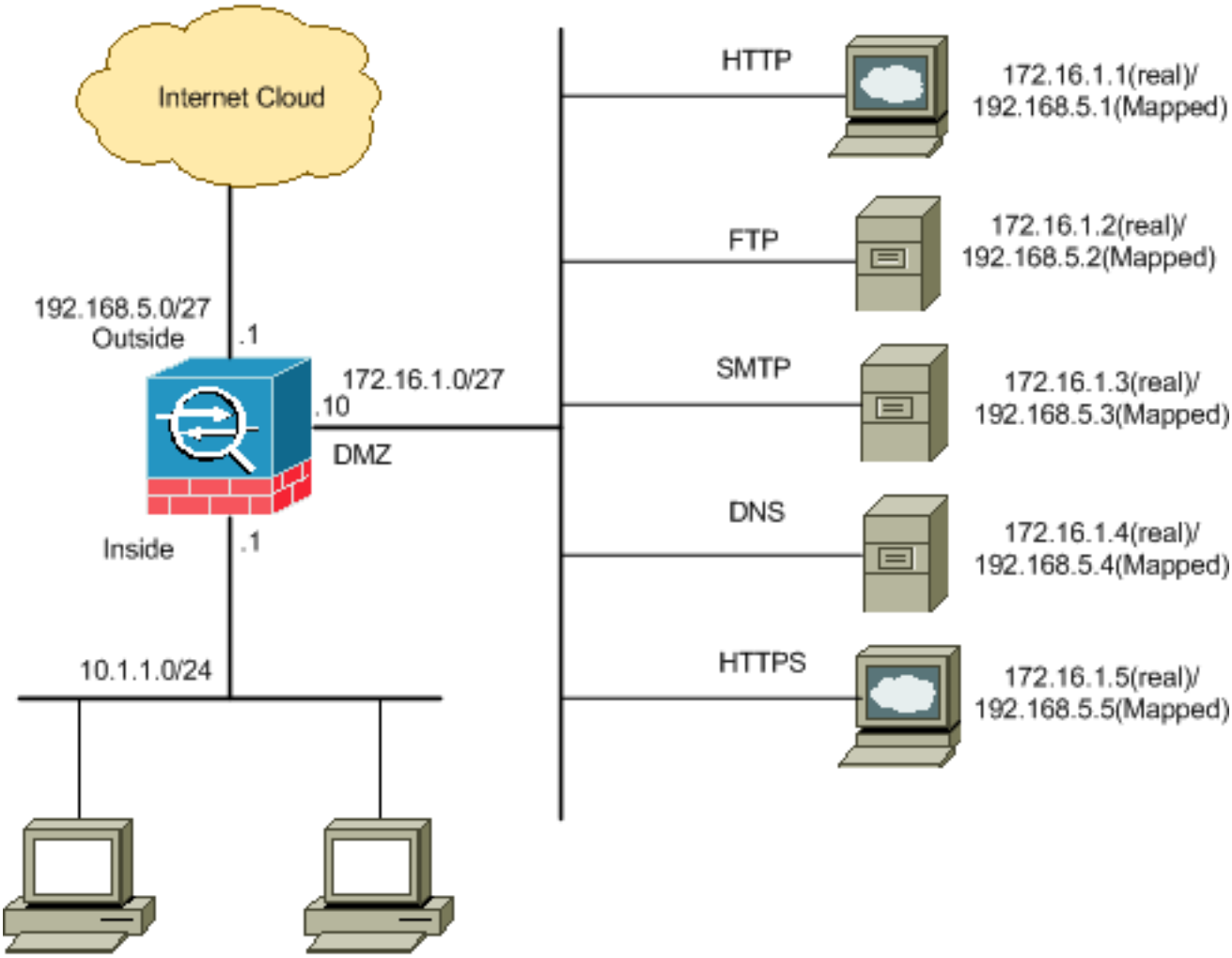
- 네트워크 다이어그램
- 포트 구성 차단
- 포트 구성 열기

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



포트 구성 차단

보안 어플라이언스는 확장 액세스 목록에 의해 명시적으로 차단되지 않는 한 모든 아웃바운드 트래픽을 허용합니다.

액세스 목록은 하나 이상의 액세스 제어 항목으로 구성됩니다. 액세스 목록 유형에 따라 소스 및 목적지 주소, 프로토콜, 포트(TCP 또는 UDP용), ICMP 유형(ICMP용) 또는 이더 유형을 지정할 수 있습니다.

참고: ICMP와 같은 연결 없는 프로토콜의 경우 보안 어플라이언스는 단방향 세션을 설정하므로 두 방향의 ICMP를 허용하려면(소스 및 대상 인터페이스에 대한 액세스 목록 응용 프로그램) 액세스 목록이 필요하거나 ICMP 검사 엔진을 활성화해야 합니다. ICMP 검사 엔진은 ICMP 세션을 양방향 연결로 취급합니다.

일반적으로 내부(상위 보안 영역)에서 DMZ(하위 보안 영역) 또는 외부에 대한 DMZ로 시작되는 트래픽에 적용되는 포트를 차단하려면 다음 단계를 완료하십시오.

1. 지정된 포트 트래픽을 차단하는 방식으로 액세스 제어 목록을 생성합니다.

```
access-list
```

2. 그런 다음 access-list를 access-group 명령으로 바인딩하여 활성화합니다.

```
access-group
```

예:

1. **HTTP 포트 트래픽을 차단합니다.** DMZ 네트워크에 IP 172.16.1.1이 배치된 내부 네트워크 10.1.1.0에 대한 http(웹 서버) 액세스를 차단하려면 다음과 같이 ACL을 생성합니다.

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.1  eq 80
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

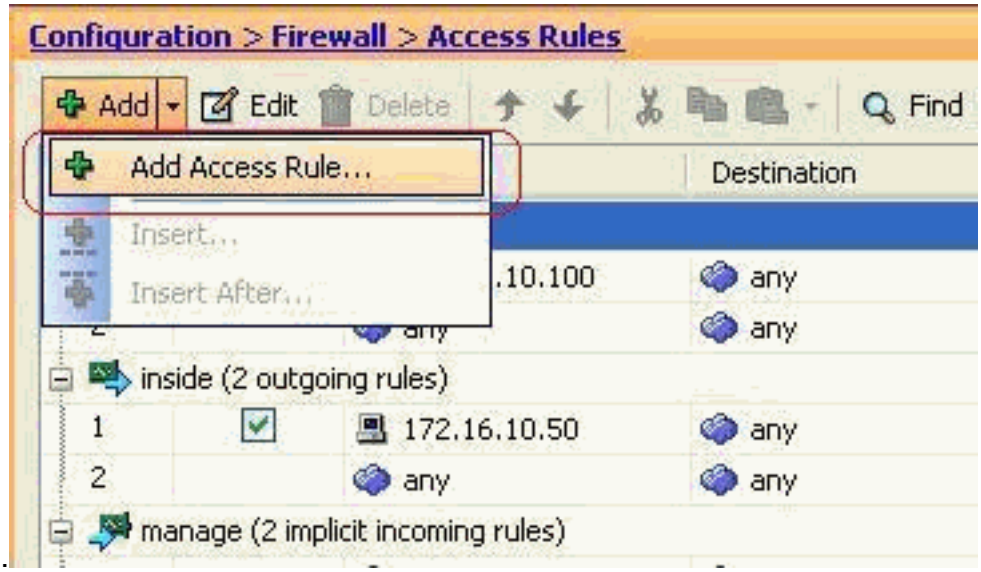
   참고: no와 access list 명령을 차례로 사용하여 포트 차단을 제거합니다.
2. **FTP 포트 트래픽을 차단합니다.** DMZ 네트워크에 IP 172.16.1.2이 배치된 내부 네트워크 10.1.1.0이 FTP(파일 서버)에 대한 액세스를 차단하려면 다음과 같이 ACL을 생성합니다.

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
   host 172.16.1.2  eq 21
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

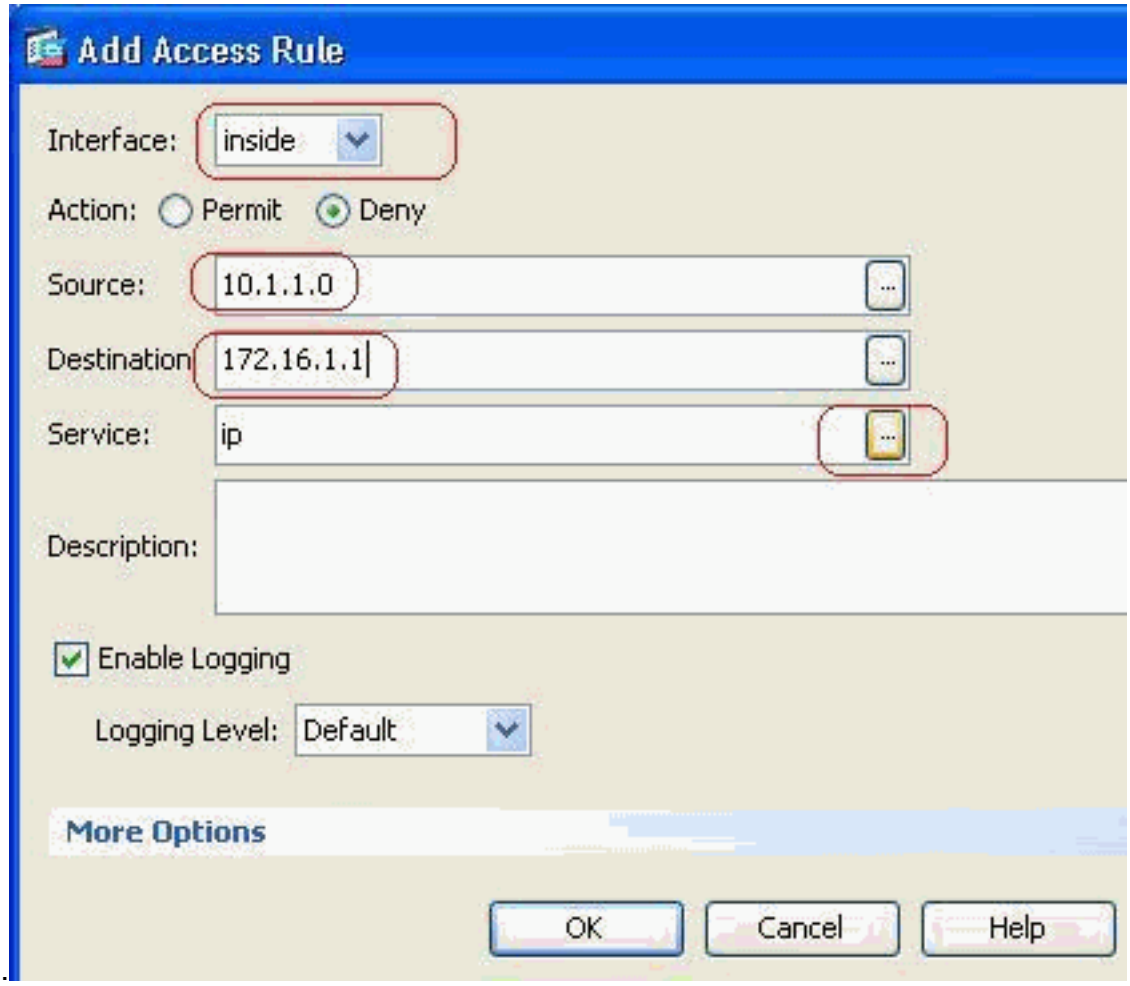
참고: 포트 할당에 대한 자세한 내용은 IANA 포트를 참조하십시오.

이 섹션에서는 ASDM을 통해 이를 수행하는 단계별 컨피그레이션을 설명합니다.

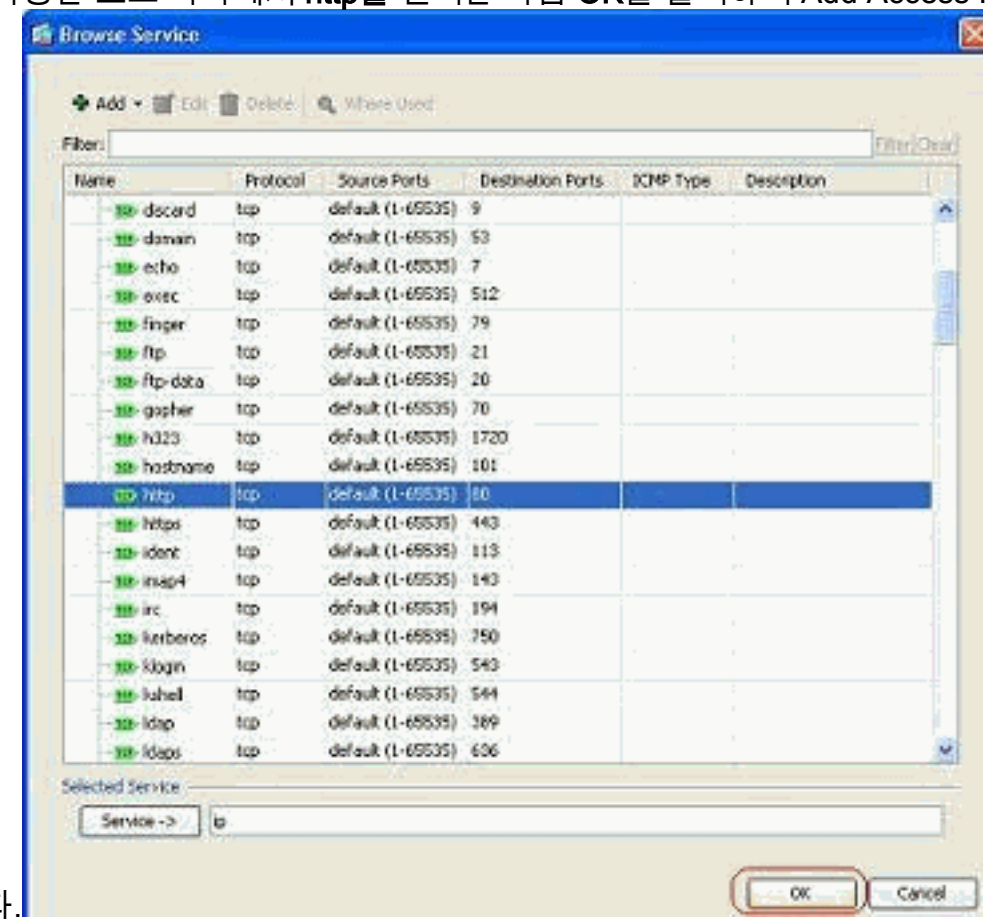
1. Configuration(컨피그레이션) **> Firewall(방화벽) > Access Rules(액세스 규칙)로 이동합니다.** Add **Access Rule**을 클릭하여 access-list를 생성합니다



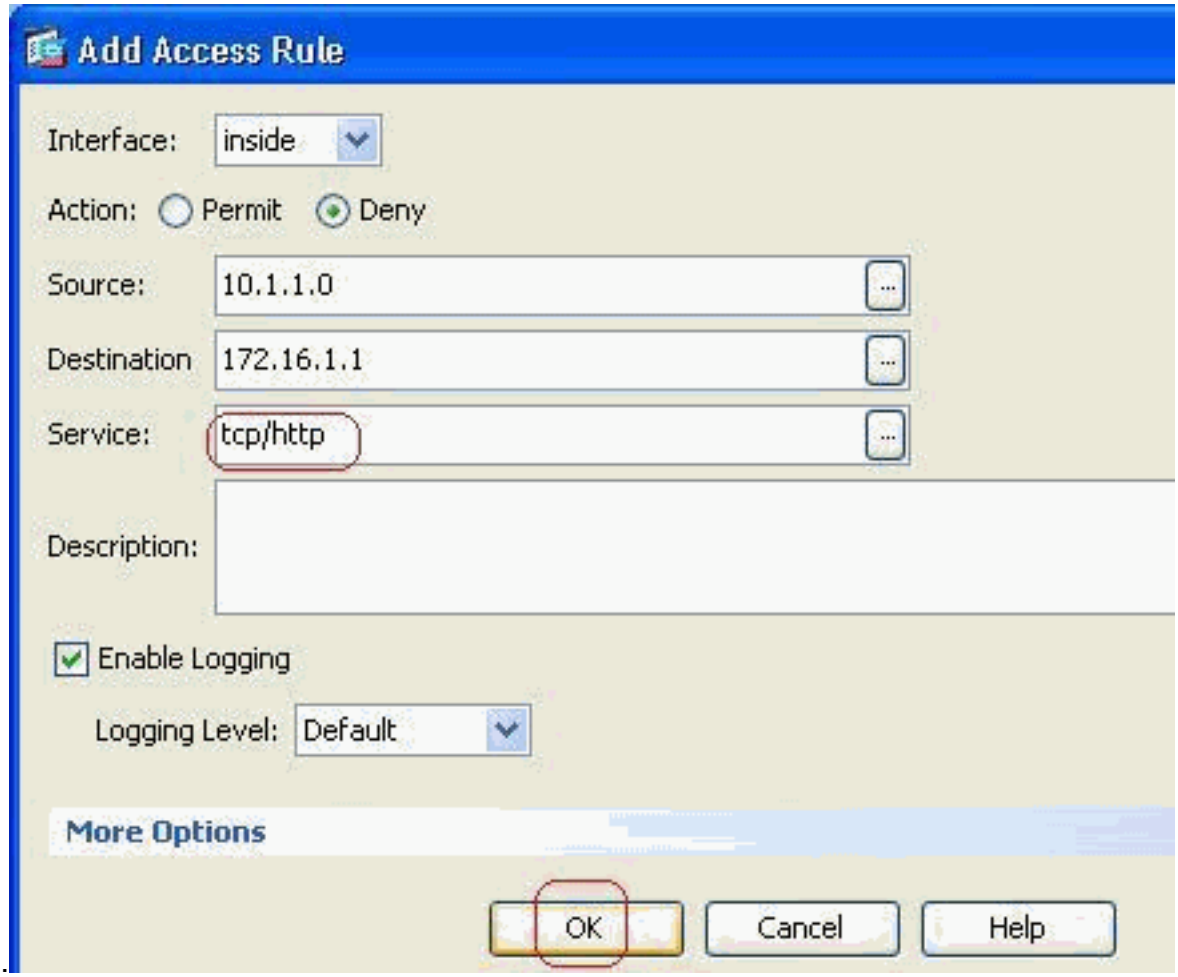
2. 이 액세스 규칙이 연결될 인터페이스와 함께 액세스 규칙의 소스 및 대상 및 작업을 정의합니다. 차단할 특정 포트를 선택하려면 세부 정보를 선택합니다



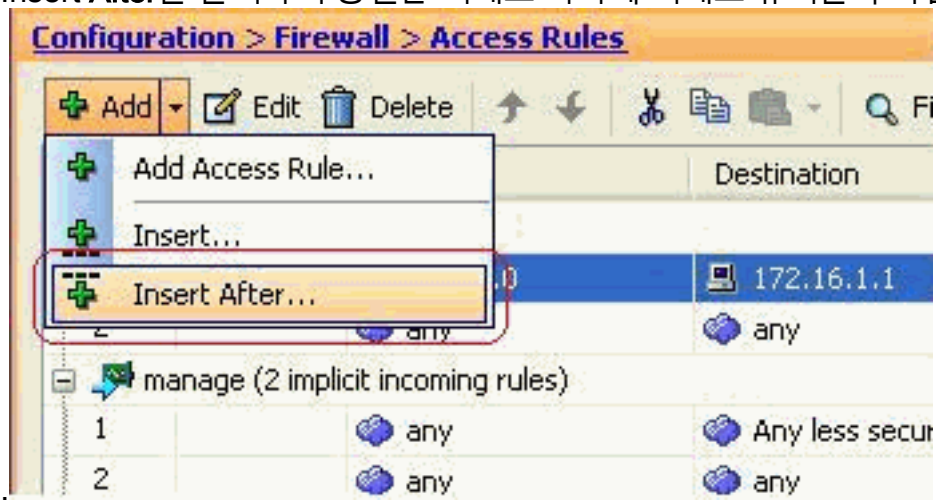
3. 사용 가능한 포트 목록에서 **http**를 선택한 다음 **OK**를 클릭하여 Add Access Rule 창으로 돌아갑니다.



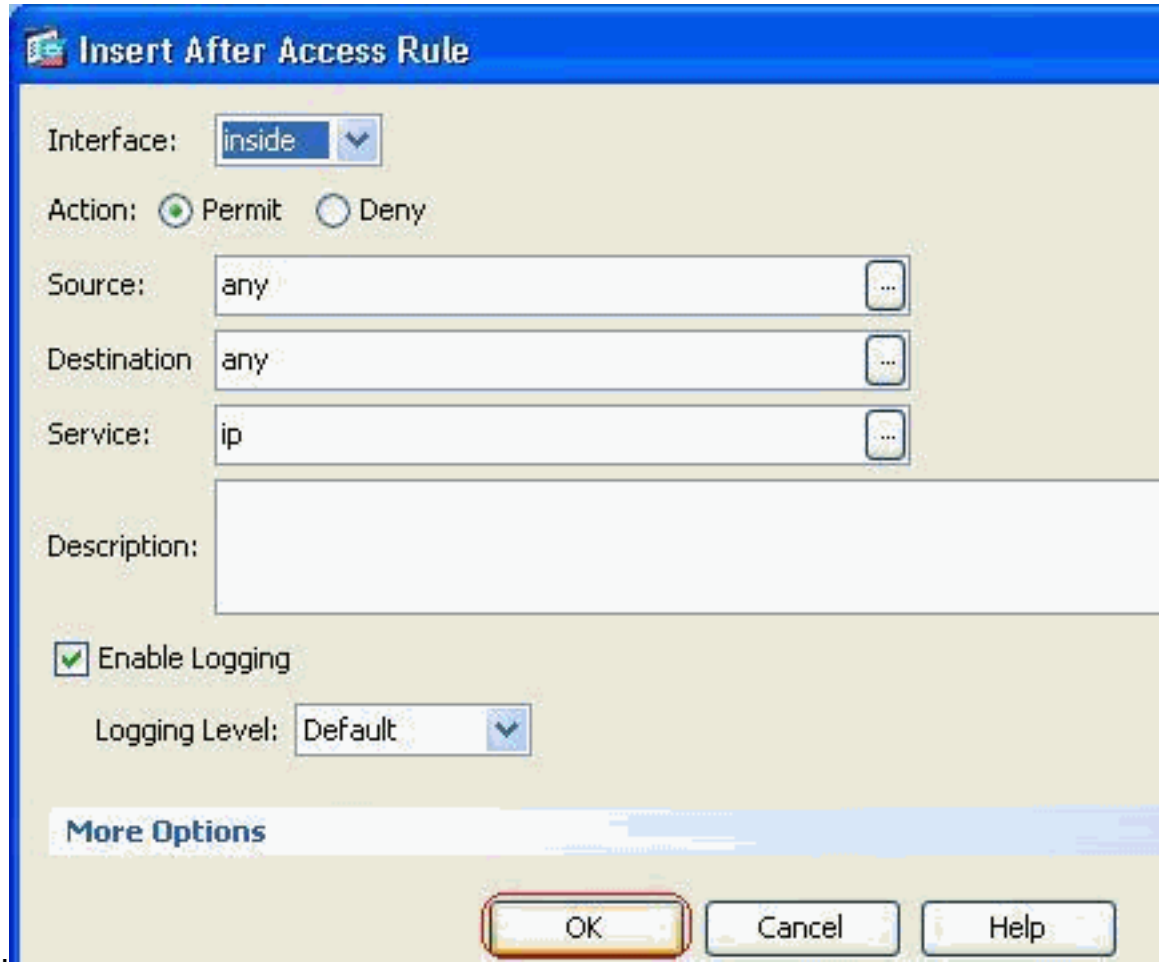
4. OK(**확인**)를 클릭하여 액세스 규칙의 컨피그레이션을 완료합니다



5. Insert **After**를 클릭하여 동일한 액세스 목록에 액세스 규칙을 추가합니다

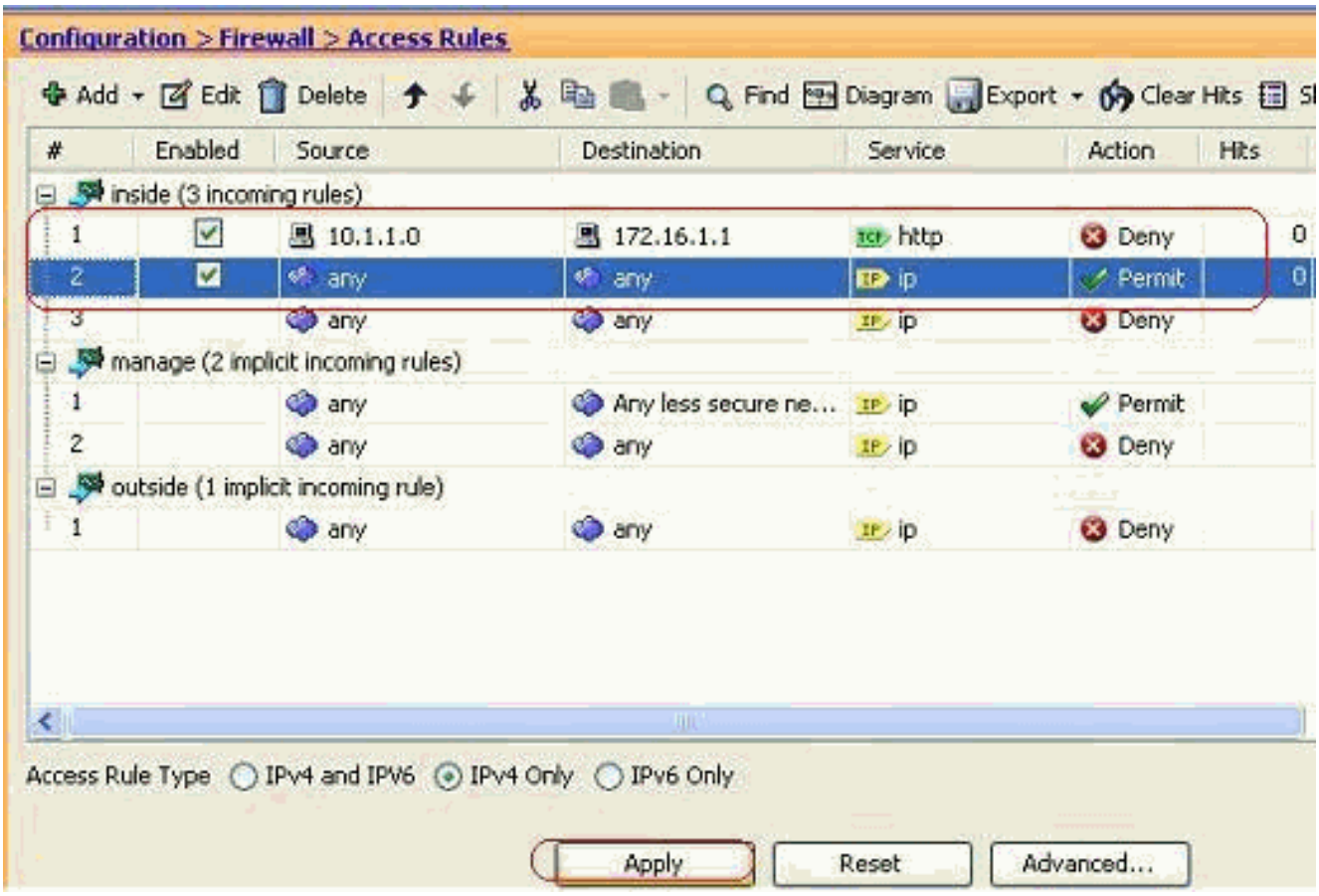


6. "any"에서 "any"로 트래픽을 허용하여 "암시적 거부"를 방지합니다. 그런 다음 **OK**(확인)를 클릭하여 이 액세스 규칙 추가를 완료합니다



7. 구성된 액세스 목록은 Access Rules(액세스 규칙) 탭에서 확인할 수 있습니다. Apply(**적용**)를 클릭하여 이 컨피그레이션을 보안 어플라이언스에 전송합니다

.



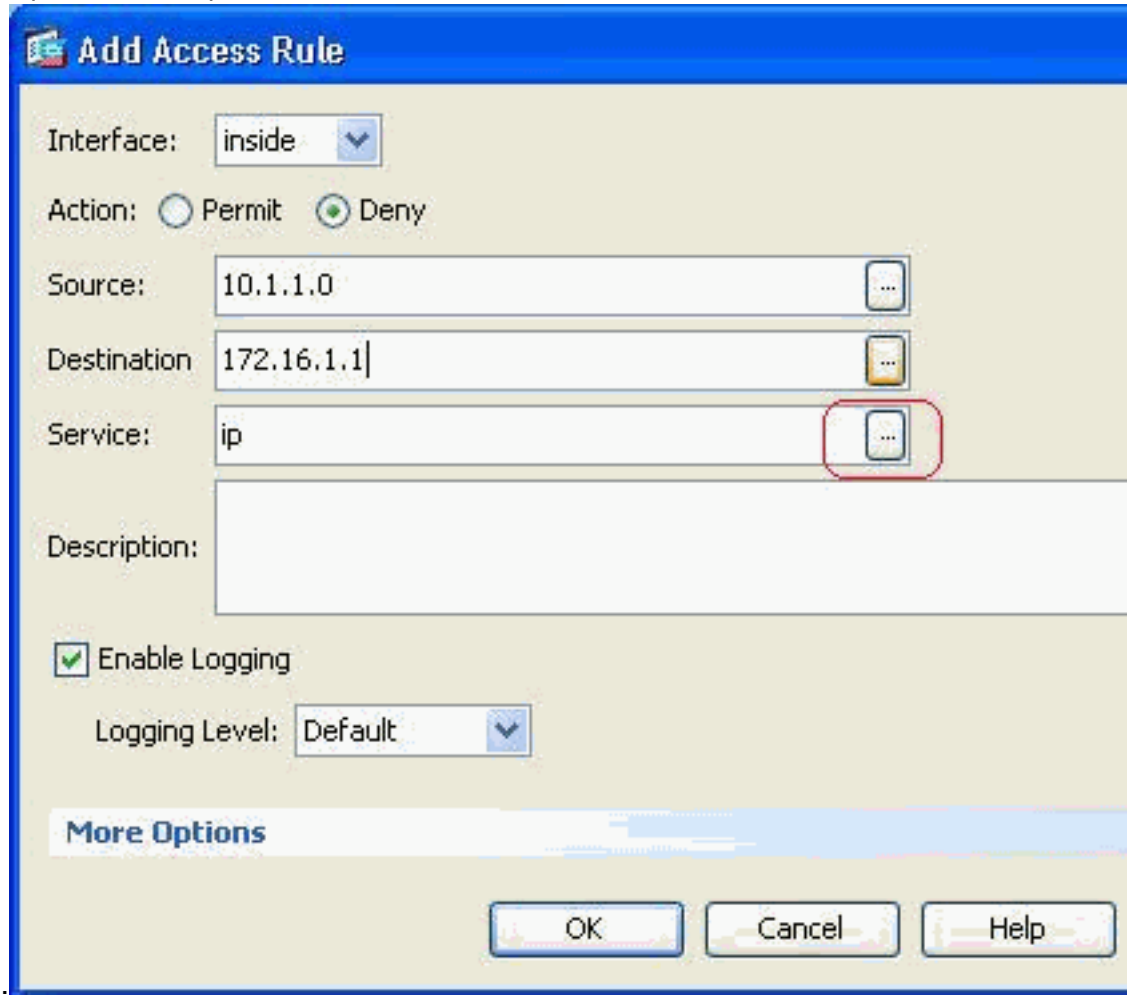
ASDM에서 전송된 컨피그레이션을 통해 ASA의 CLI(Command Line Interface)에서 이 명령

집합이 생성됩니다.

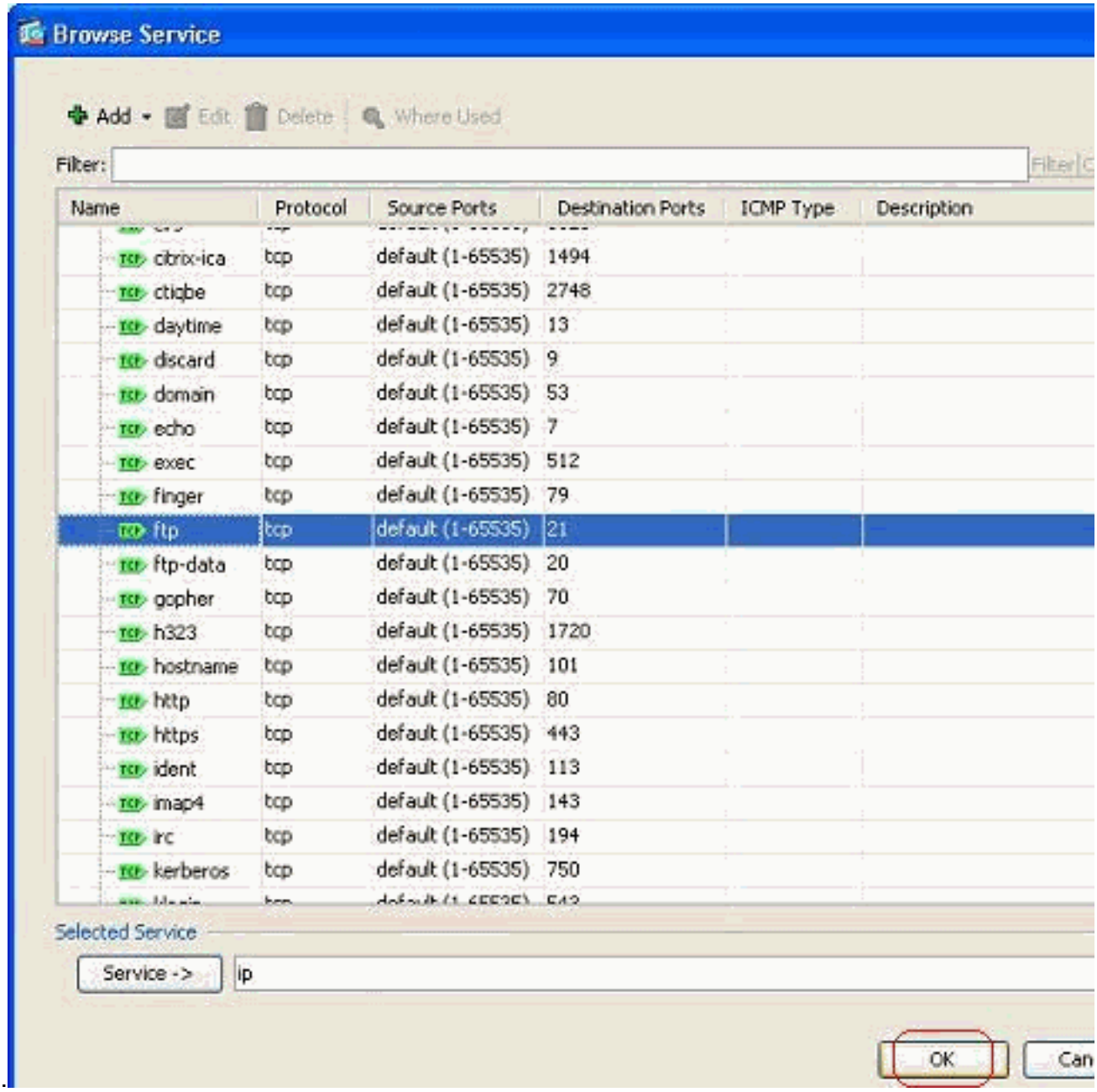
```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

이 단계를 통해 예 1은 ASDM을 통해 수행되어 10.1.1.0 네트워크가 웹 서버 172.16.1.1에 액세스하지 못하도록 차단되었습니다. 예 2도 동일한 방법으로 전체 10.1.1.0 네트워크가 FTP 서버 172.16.1.2에 액세스하지 못하도록 차단할 수 있습니다. 유일한 차이점은 포트를 선택하는 단계입니다.**참고:** 예 2에 대한 이 액세스 규칙 컨피그레이션은 새로운 컨피그레이션으로 간주됩니다.

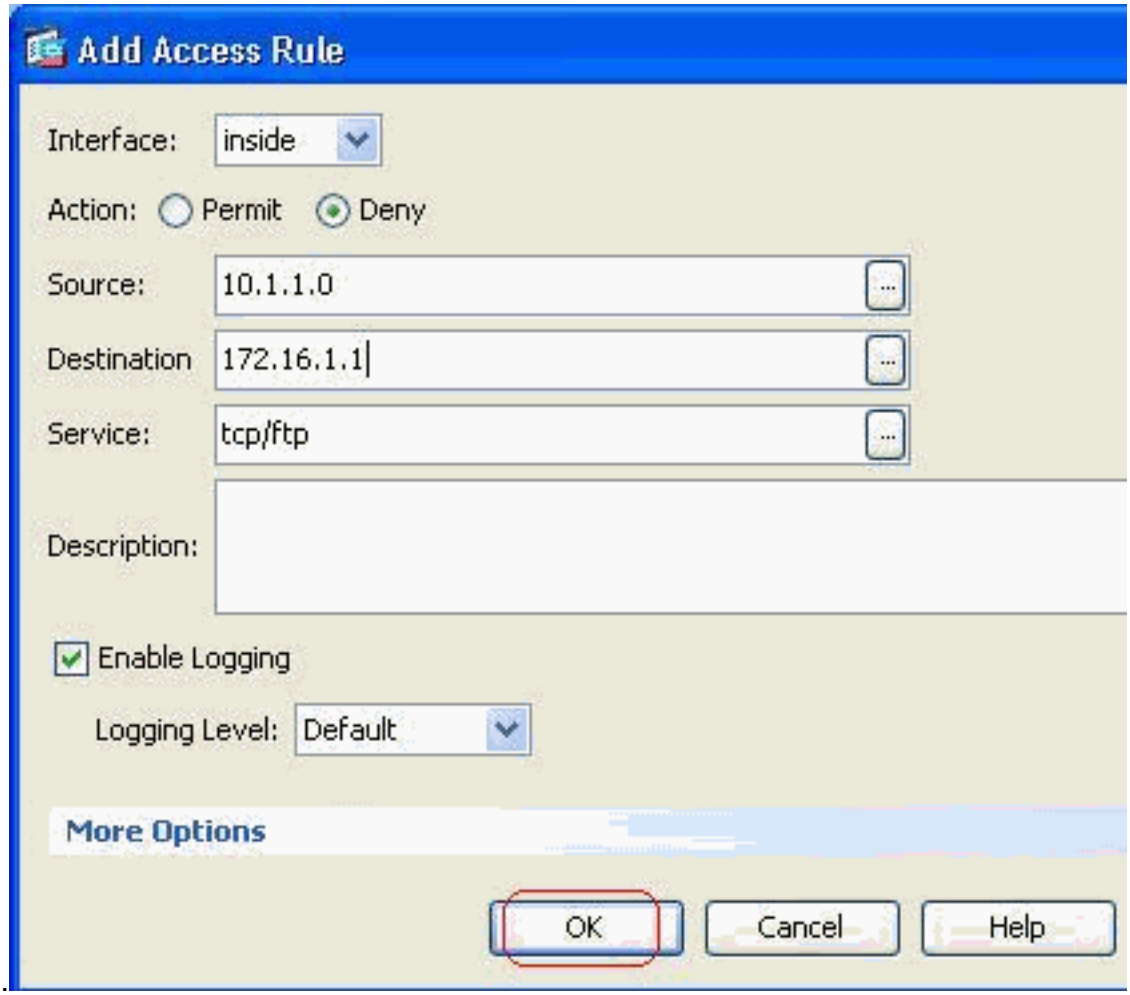
8. FTP 트래픽 차단을 위한 액세스 규칙을 정의한 다음 **Details** 탭을 클릭하여 대상 포트를 선택합니다.



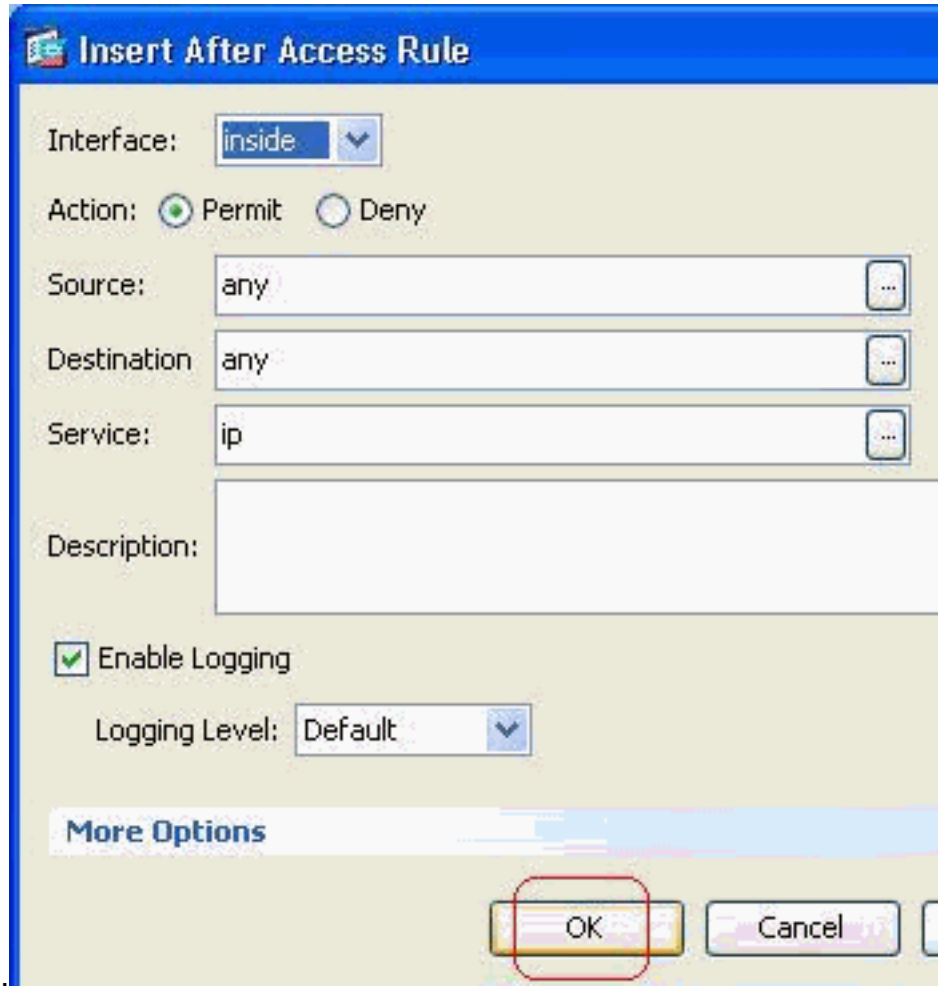
9. **ftp** 포트를 선택하고 **OK**를 클릭하여 Add Access Rule 창으로 돌아갑니다



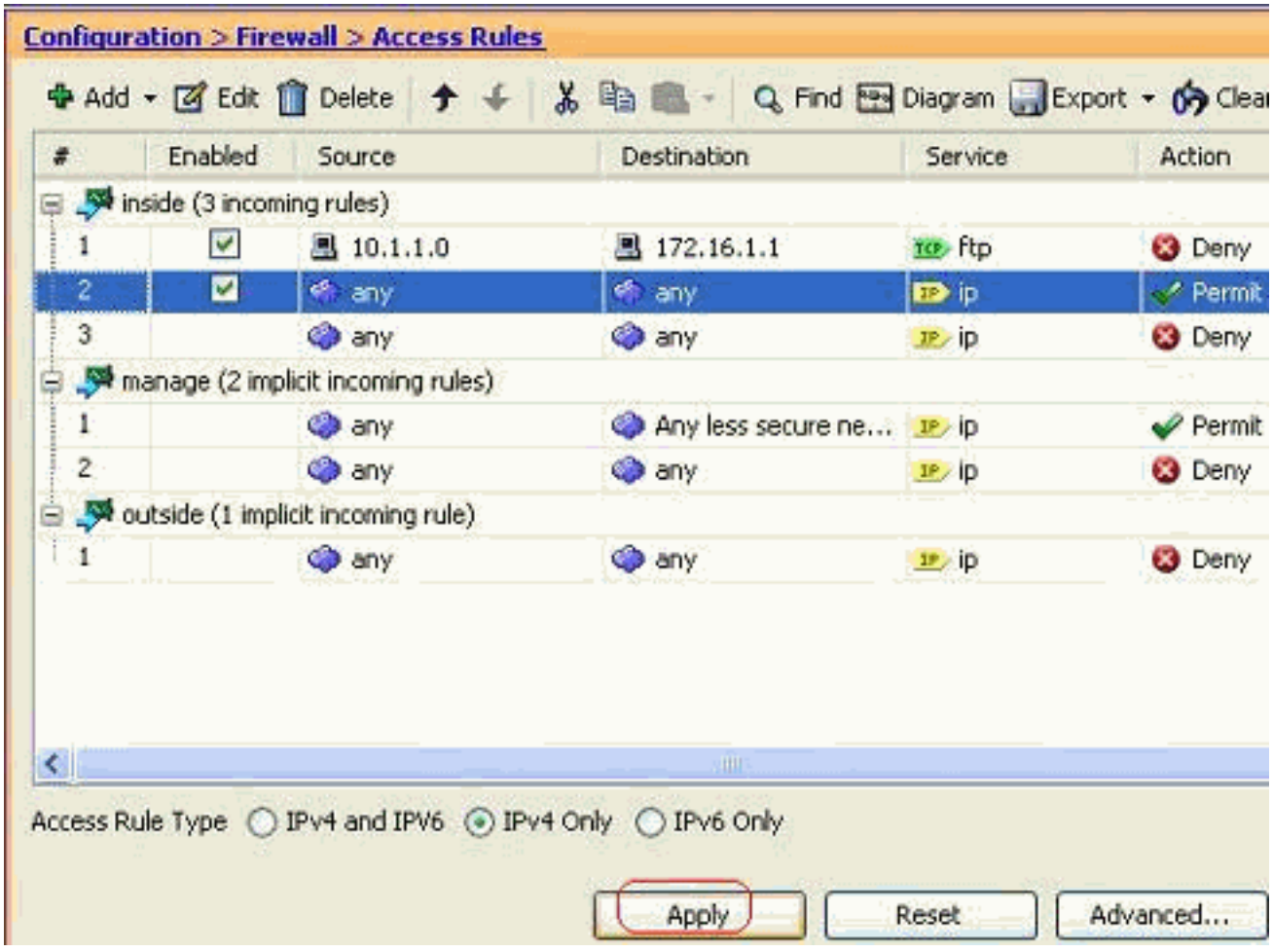
10. OK(**확인**)를 클릭하여 액세스 규칙의 컨피그레이션을 완료합니다



11. 다른 트래픽을 허용하려면 다른 액세스 규칙을 추가합니다. 그렇지 않으면 Implicit Deny 규칙은 이 인터페이스의 모든 트래픽을 차단합니다



12. 전체 액세스 목록 컨피그레이션은 Access Rules(액세스 규칙) 탭 아래에서 이와 같습니다



13. Apply(**적용**)를 클릭하여 컨피그레이션을 ASA로 전송합니다. 동일한 CLI 컨피그레이션은 다음과 같습니다.

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

포트 구성 열기

보안 어플라이언스는 확장 액세스 목록에서 명시적으로 허용하지 않는 한 인바운드 트래픽을 허용하지 않습니다.

외부 호스트가 내부 호스트에 액세스하도록 허용하려면 외부 인터페이스에 인바운드 액세스 목록을 적용할 수 있습니다. 변환된 주소는 외부 네트워크에서 사용할 수 있는 주소이므로 액세스 목록에서 내부 호스트의 변환된 주소를 지정해야 합니다. 하위 보안 영역에서 상위 보안 영역으로 포트를 열려면 다음 단계를 완료하십시오. 예를 들어 외부(하위 보안 영역)에서 내부 인터페이스(상위 보안 영역)로 또는 DMZ에서 내부 인터페이스로 이동하는 트래픽을 허용합니다.

1. 고정 NAT는 실제 주소의 고정 변환을 매핑된 주소로 생성합니다. 이 매핑된 주소는 인터넷에서 호스트하는 주소이며 서버의 실제 주소를 알 필요 없이 DMZ의 애플리케이션 서버에 액세스하는 데 사용할 수 있습니다.

   ```
   static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] |
      access-list access_list_name | interface}
   ```

   자세한 내용은 PIX/ASA에 대한 명령 참조의 Static NAT 섹션을 참조하십시오.
2. 특정 포트 트래픽을 허용하도록 ACL을 생성합니다.

   ```
   access-list
   ```

3. access-list를 **access-group** 명령으로 바인딩하여 활성화합니다.

   ```
   access-group
   ```

예:

1. **SMTP 포트 트래픽을 엽니다.** 외부(인터넷)의 호스트가 DMZ 네트워크에 위치한 메일 서버에 액세스할 수 있도록 포트 **tcp 25**를 엽니다.Static 명령은 외부 주소 192.168.5.3을 실제 DMZ 주소 172.16.1.3에 매핑합니다.

   ```
   ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3
    netmask 255.255.255.255
   ciscoasa(config)#access-list 100 extended permit tcp
    any host 192.168.5.3 eq 25
   ciscoasa(config)#access-group 100 in interface outside
   ```

2. **HTTPS 포트 트래픽을 엽니다.** 외부(인터넷)의 호스트가 DMZ 네트워크에 있는 웹 서버(보안

)에 액세스하도록 허용하려면 포트 **tcp 443**을 엽니다.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
 any host 192.168.5.5  eq 443
ciscoasa(config)#access-group 100 in interface outside
```

3. **DNS 트래픽 허용:** 외부(인터넷)의 호스트가 DMZ 네트워크에 있는 DNS 서버(보안)에 액세스하도록 허용하려면 포트 **udp 53**을 엽니다.

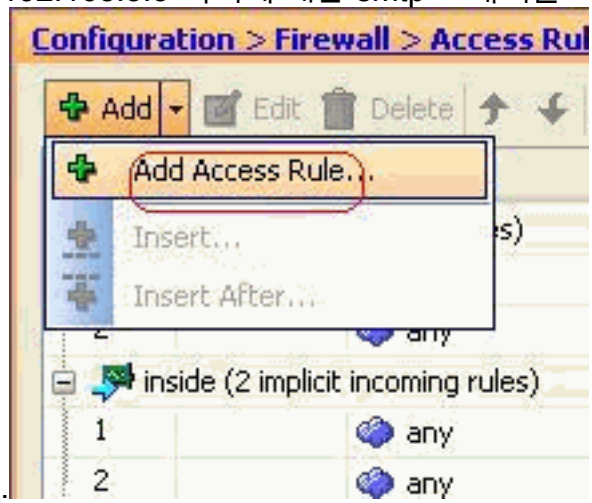
```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4
 netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit udp
 any host 192.168.5.4  eq 53
ciscoasa(config)#access-group 100 in interface outside
```

참고: 포트 할당에 대한 자세한 내용은 IANA 포트를 참조하십시오.

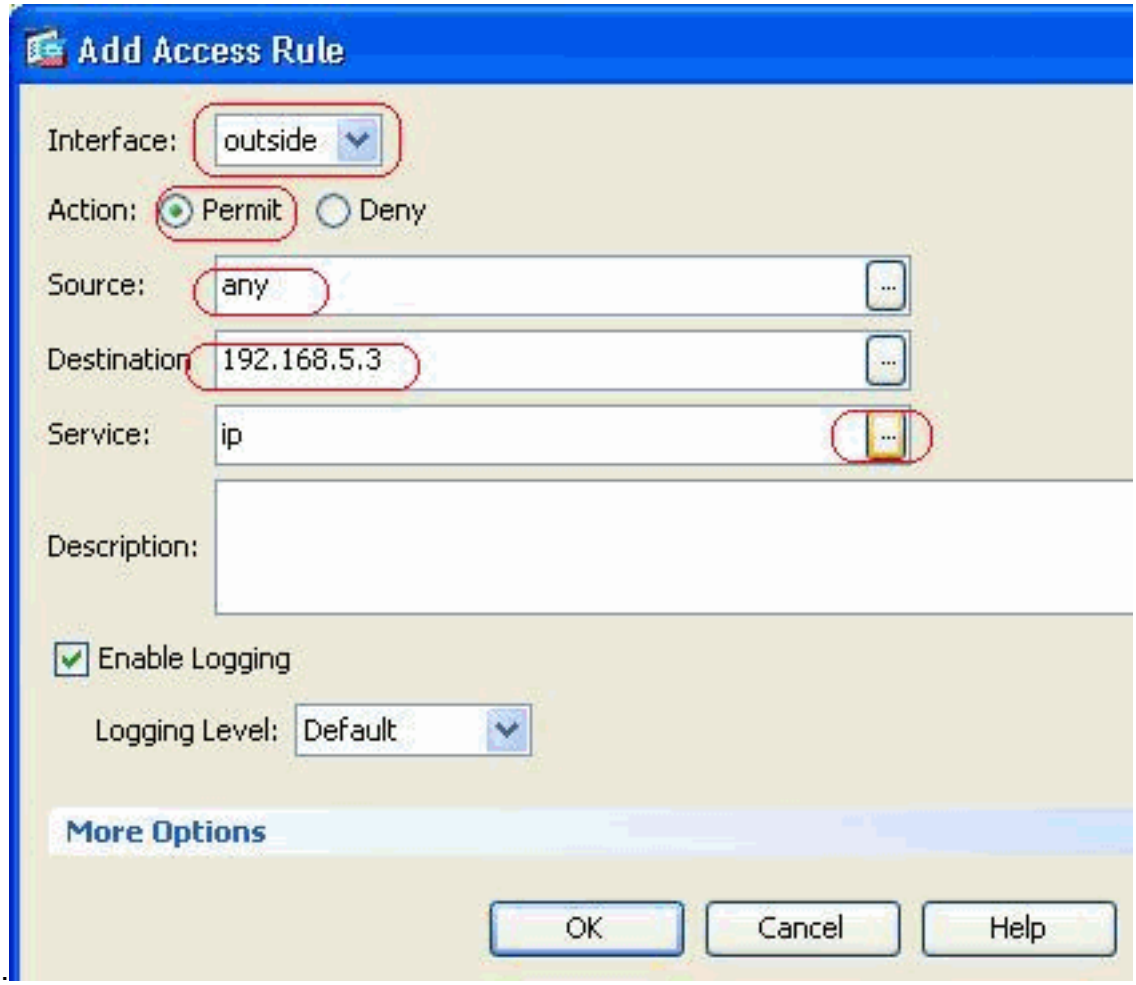
ASDM을 통한 구성

이 섹션에서는 ASDM을 통해 위에서 언급한 작업을 수행하는 단계별 접근 방식을 설명합니다.

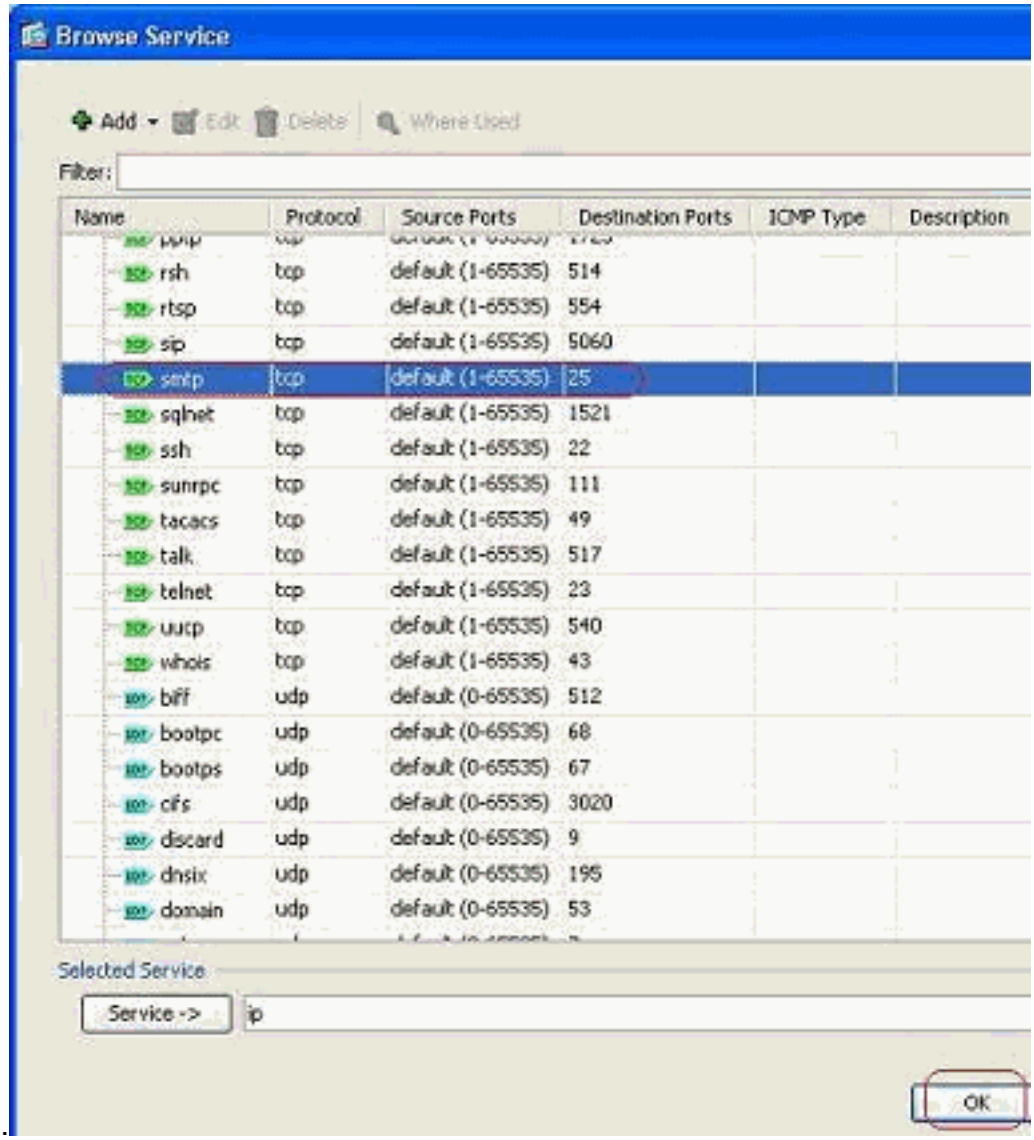
1. 192.168.5.3 서버에 대한 smtp 트래픽을 허용하도록 액세스 규칙을 생성합니다



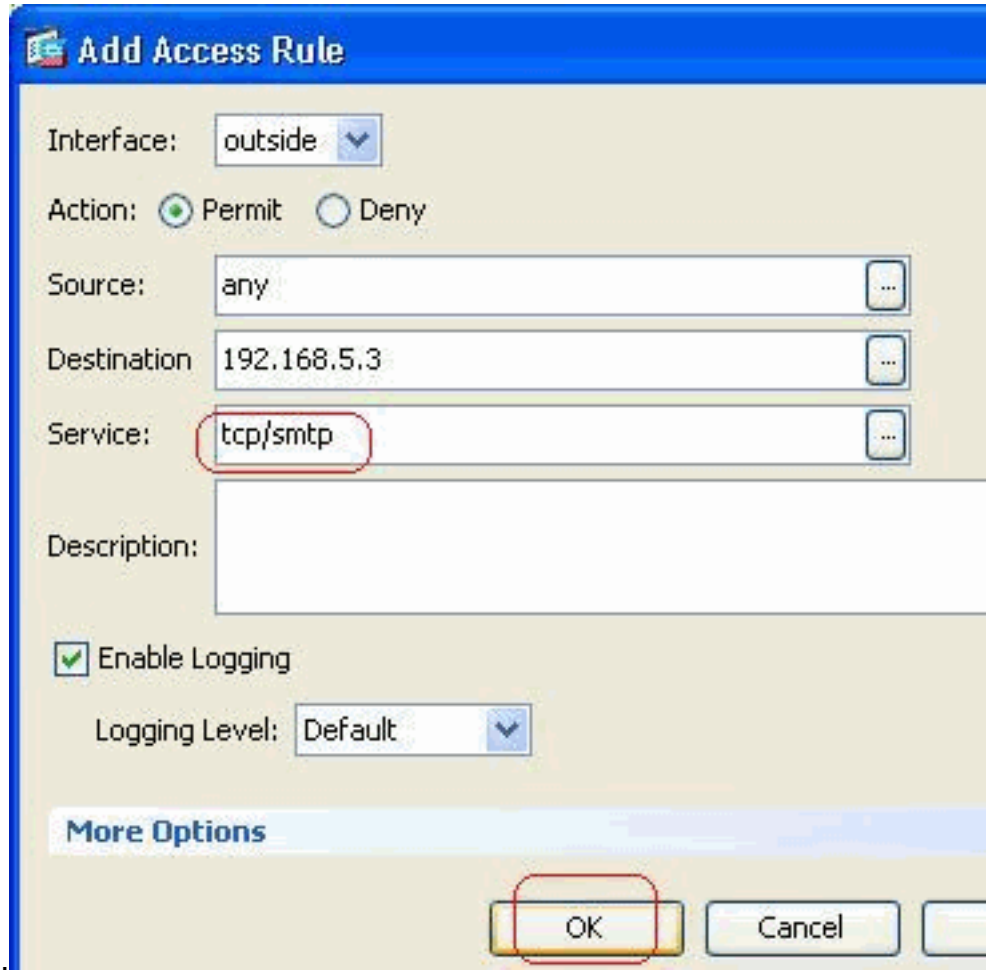
2. 액세스 규칙의 소스 및 목적지와 이 규칙이 바인딩하는 인터페이스를 정의합니다. 또한 작업을 **허용**으로 정의합니다



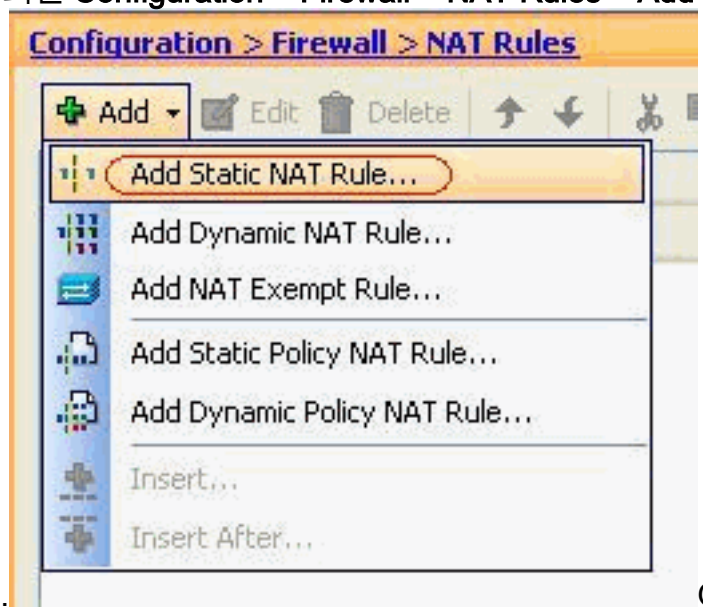
3. SMTP를 포트로 선택한 다음 OK를 클릭합니다



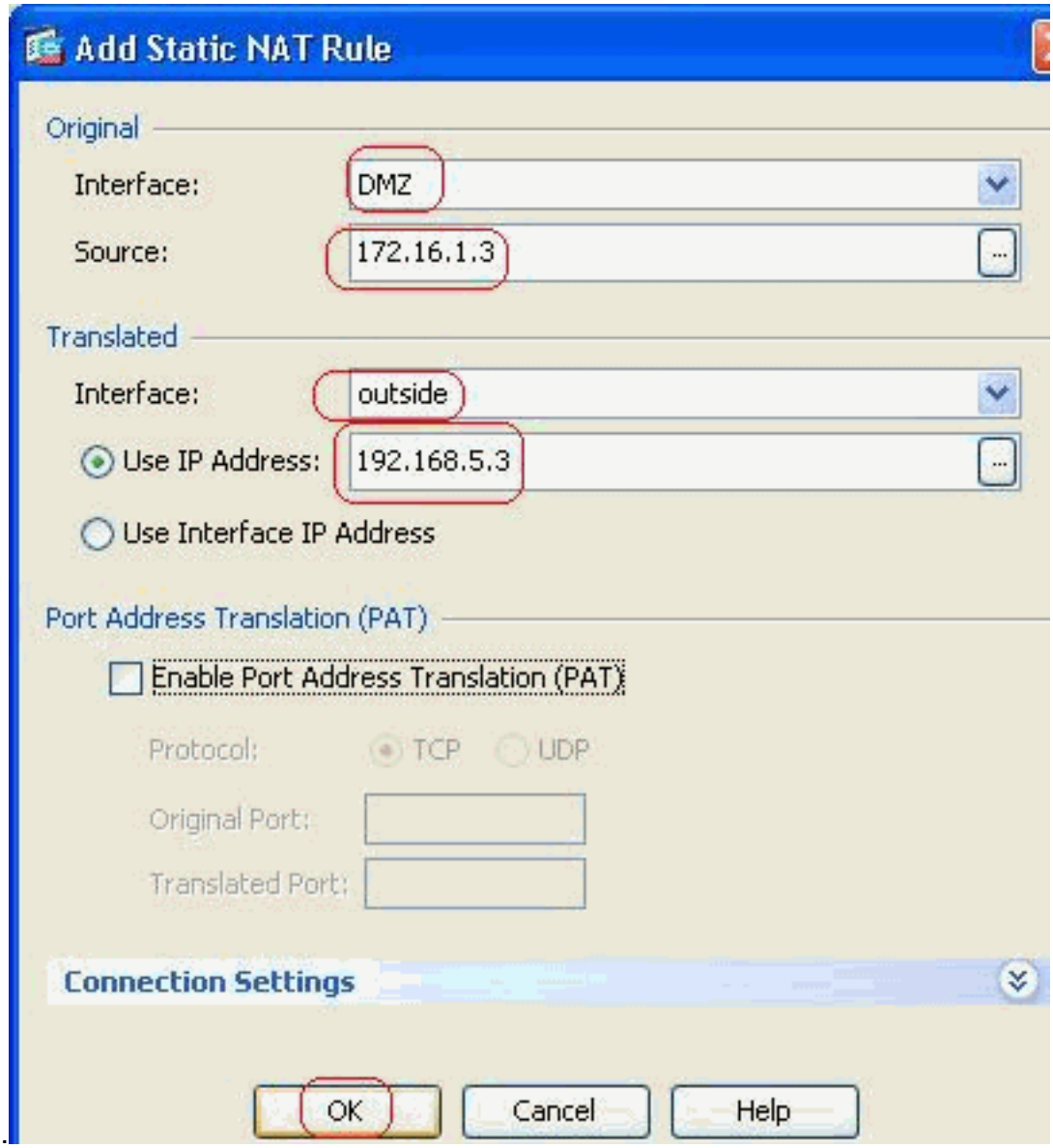
4. OK(**확인**)를 클릭하여 액세스 규칙 구성을 완료합니다



5. 172.16.1.3을 192.168.5.3으로 변환하려면 고정 NAT를 구성합니다.고정 NAT **항목을** 추가하려면 **Configuration > Firewall > NAT Rules > Add Static NAT Rule**으로 이동합니다

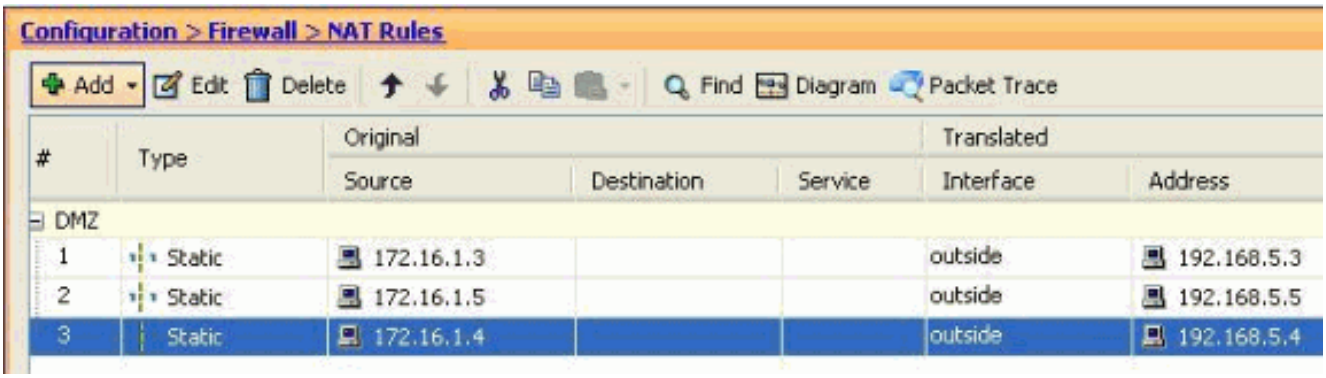


Original Source 및 Translated IP 주소를 관련 인터페이스와 함께 선택한 다음 **OK**를 클릭하여 Static NAT 규칙 구성을 완료합니다



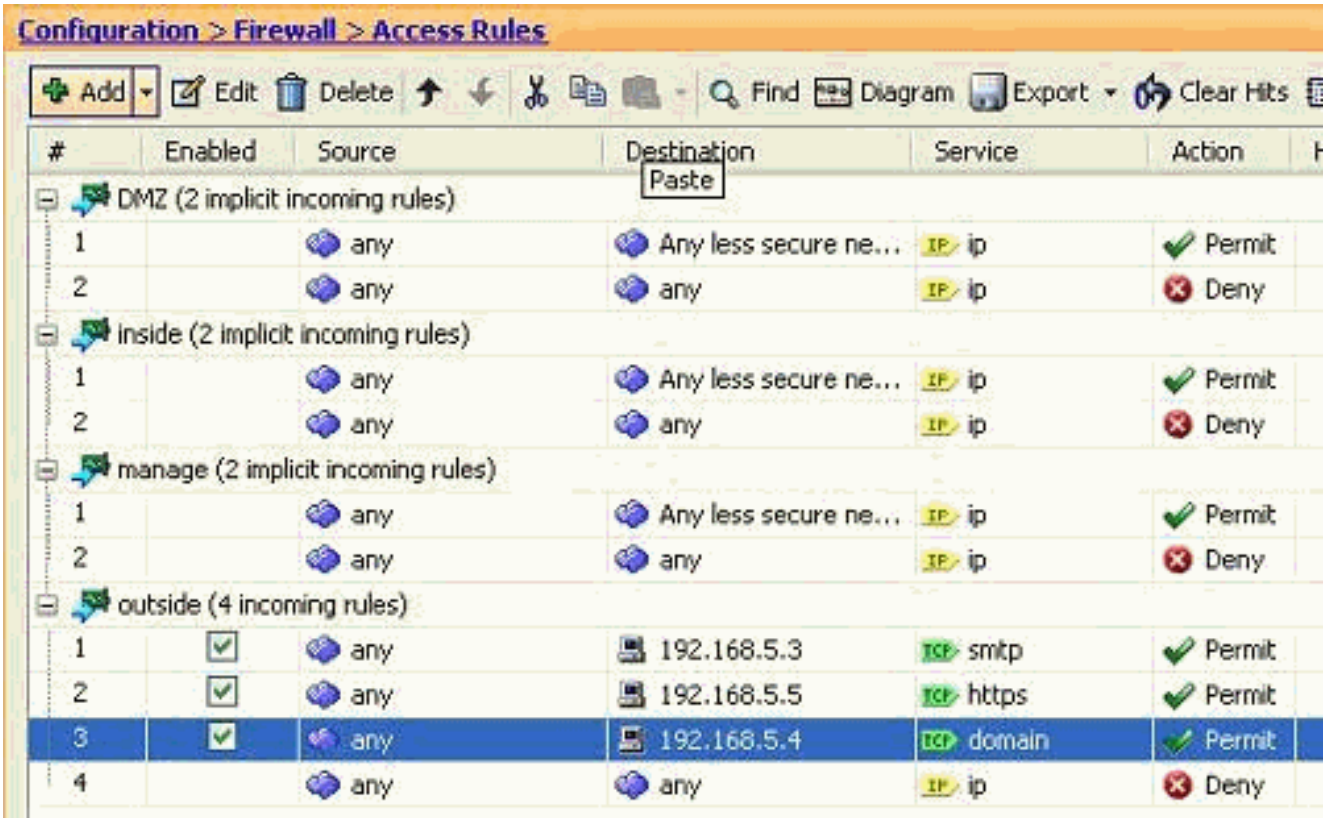
이 이미지는 Example 섹션에 나열된 세 가지 고정 규칙을 모두 보여줍니다

.



이 이미지는 Examples(예) 섹션에 나열된 세 가지 액세스 규칙 모두를 나타냅니다

.



다음을 확인합니다.

다음과 같이 특정 **show** 명령으로 확인할 수 있습니다.

- **show xlate** - 현재 변환 정보를 표시합니다.
- **show access-list**—액세스 정책에 대한 적중 카운터를 표시합니다.
- **show logging** - 버퍼의 로그를 표시합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- PIX/ASA 7.x: 인터페이스 간 통신 활성화/비활성화
- PIX 7.0 및 Adaptive Security Appliance Port Redirection(Forwarding) with nat, global, static, patoral 및 access-list 명령
- PIX에서 nat, global, static, pattern, access-list 명령 및 포트 리디렉션(전달) 사용
- PIX/ASA 7.x: Enable FTP/TFTP Services 컨피그레이션 예
- PIX/ASA 7.x: VoIP(SIP,MGCP,H323,SCCP) 서비스 구성 사용 예
- PIX/ASA 7.x: DMZ 구성의 메일 서버 액세스 예
- 기술 지원 및 문서 – Cisco Systems