ASA 8.X 이상:ASDM GUI 컨피그레이션 예를 통해 액세스 목록 추가 또는 수정

목차

소개

이 문서에서는 액세스 제어 목록과 함께 작업하기 위해 Cisco ASDM(Adaptive Security Device Manager)을 사용하는 방법에 대해 설명합니다.여기에는 새 액세스 목록 생성, 기존 액세스 목록 수정 방법 및 액세스 목록을 사용한 기타 기능이 포함됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA(Adaptive Security Appliance) 버전 8.2.X

- Cisco ASDM(Adaptive Security Device Manager) 버전 6.3.X

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

액세스 목록은 주로 방화벽을 통과하는 트래픽 흐름을 제어하는 데 사용됩니다.액세스 목록을 사용하여 특정 유형의 트래픽을 허용하거나 거부할 수 있습니다.모든 액세스 목록에는 특정 소스에서 특정 대상으로의 트래픽 흐름을 제어하는 여러 ACE(Access List Entry)가 포함되어 있습니다.일반적으로 이 액세스 목록은 인터페이스가 확인해야 하는 플로우의 방향을 알리기 위해 인터페이스에 바인딩됩니다.액세스 목록은 주로 두 가지 광범위한 유형으로 분류됩니다.

1. 인바운드 액세스 목록
2. 아웃바운드 액세스 목록

인바운드 액세스 목록은 해당 인터페이스로 들어가는 트래픽에 적용되며, 아웃바운드 액세스 목록은 인터페이스를 나가는 트래픽에 적용됩니다.인바운드/아웃바운드 표기법은 해당 인터페이스의 관점에서 트래픽의 방향을 의미하지만 상위 및 하위 보안 인터페이스 간의 트래픽 이동은 의미하지 않습니다.

TCP 및 UDP 연결의 경우 보안 어플라이언스는 설정된 양방향 연결에 대해 모든 반환 트래픽을 허용하므로 반환 트래픽을 허용하는 액세스 목록이 필요하지 않습니다.ICMP와 같은 연결 없는 프로토콜의 경우 보안 어플라이언스는 단방향 세션을 설정하므로, 양방향으로 ICMP를 허용하려면 소스 및 대상 인터페이스에 액세스 목록을 적용하려면 액세스 목록이 필요하거나 ICMP 검사 엔진을 활성화해야 합니다.ICMP 검사 엔진은 ICMP 세션을 양방향 연결로 취급합니다.

ASDM 버전 6.3.X에서는 두 가지 유형의 액세스 목록을 구성할 수 있습니다.

1. 인터페이스 액세스 규칙
2. 전역 액세스 규칙

참고: 액세스 규칙은 ACE(개별 액세스 목록 항목)를 참조합니다.

인터페이스 액세스 규칙은 생성 시 모든 인터페이스에 바인딩됩니다.인터페이스에 바인딩하지 않으면 생성할 수 없습니다.이는 명령줄 예와 다릅니다.CLI를 사용하여 먼저 **access list** 명령으로 액세스 목록을 생성한 다음 access-group 명령을 사용하여 이 액세스 목록을 인터페이스에 **바인딩합니다**.ASDM 6.3 이상에서는 액세스 목록이 생성되어 하나의 작업으로 인터페이스에 바인딩됩니다.이는 특정 인터페이스를 통과하는 트래픽에만 적용됩니다.

전역 액세스 규칙은 어떤 인터페이스도 바인딩되지 않습니다.ASDM의 ACL Manager 탭을 통해 구성할 수 있으며 전역 인그레스 트래픽에 적용됩니다.소스, 대상 및 프로토콜 유형을 기반으로 일치하는 항목이 있을 때 구현됩니다.이러한 규칙은 각 인터페이스에서 복제되지 않으므로 메모리 공간을 절약합니다.

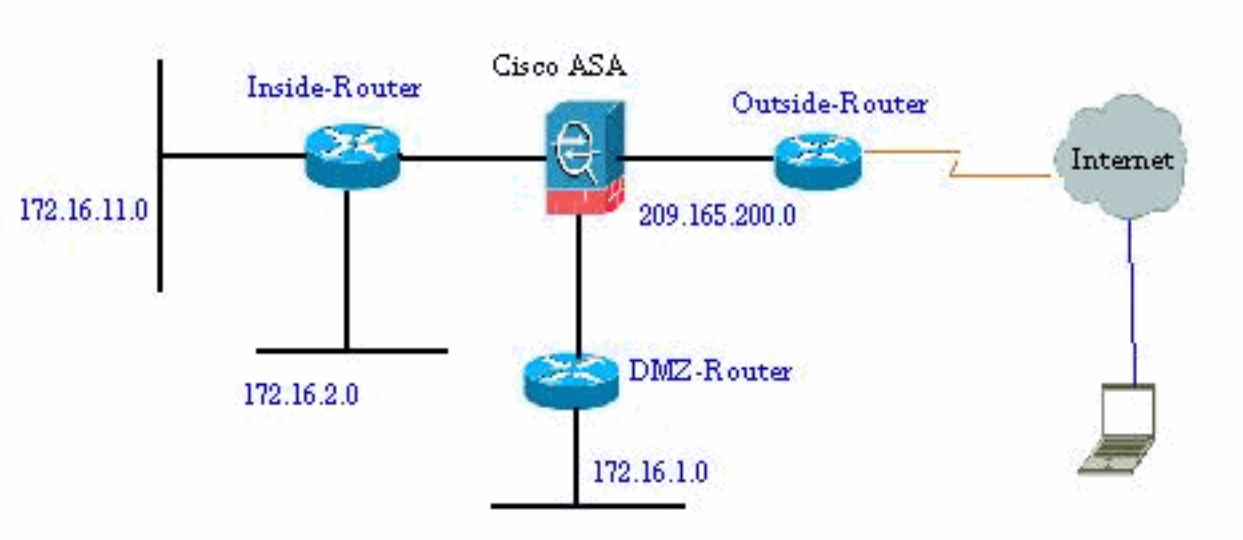
이러한 두 규칙을 모두 구현할 경우 일반적으로 인터페이스 액세스 규칙이 전역 액세스 규칙보다 우선합니다.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

네트워크 다이어그램

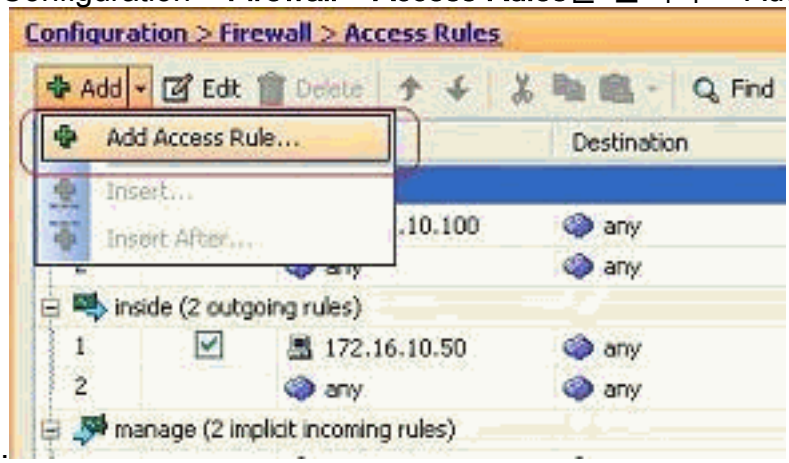
이 문서에서는 다음 네트워크 설정을 사용합니다.



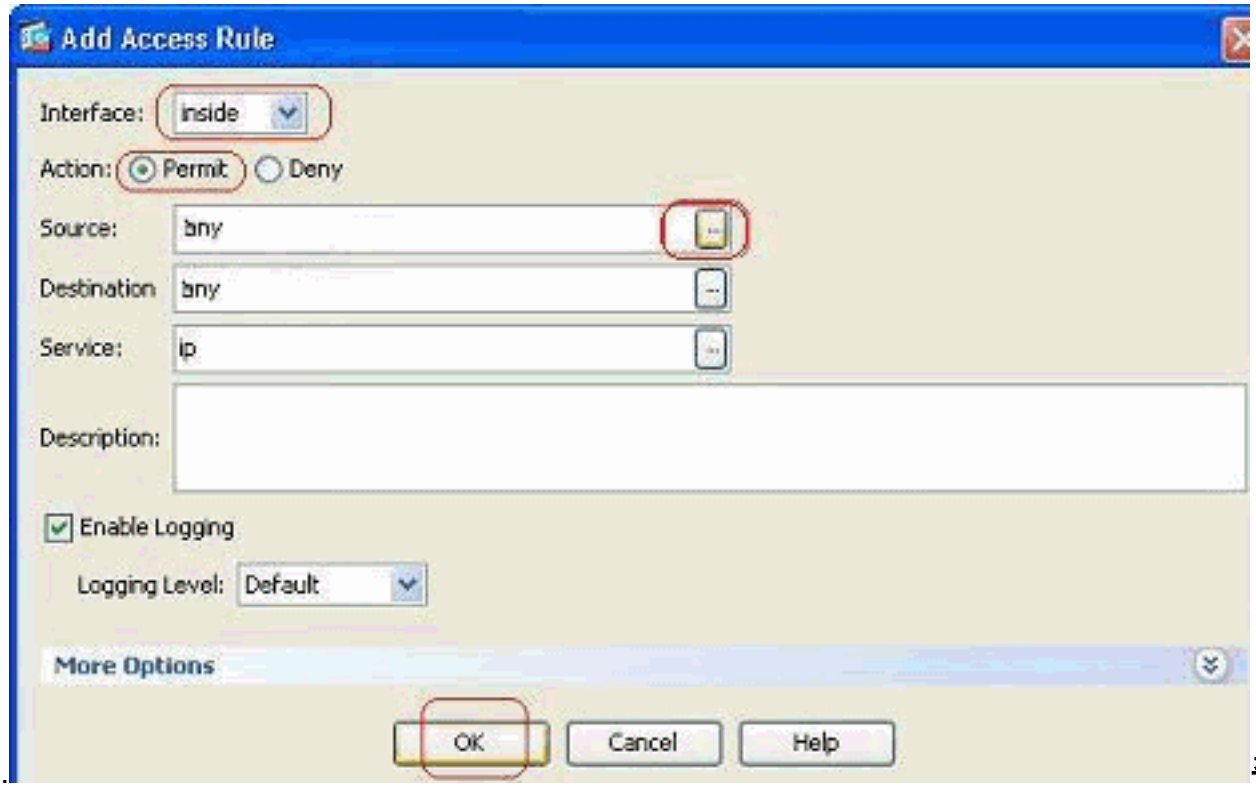
새 액세스 목록 추가

ASDM을 사용하여 새 액세스 목록을 생성하려면 다음 단계를 완료합니다.

1. Configuration **> Firewall > Access Rules**를 선택하고 Add **Access Rule** 버튼을 클릭합니다

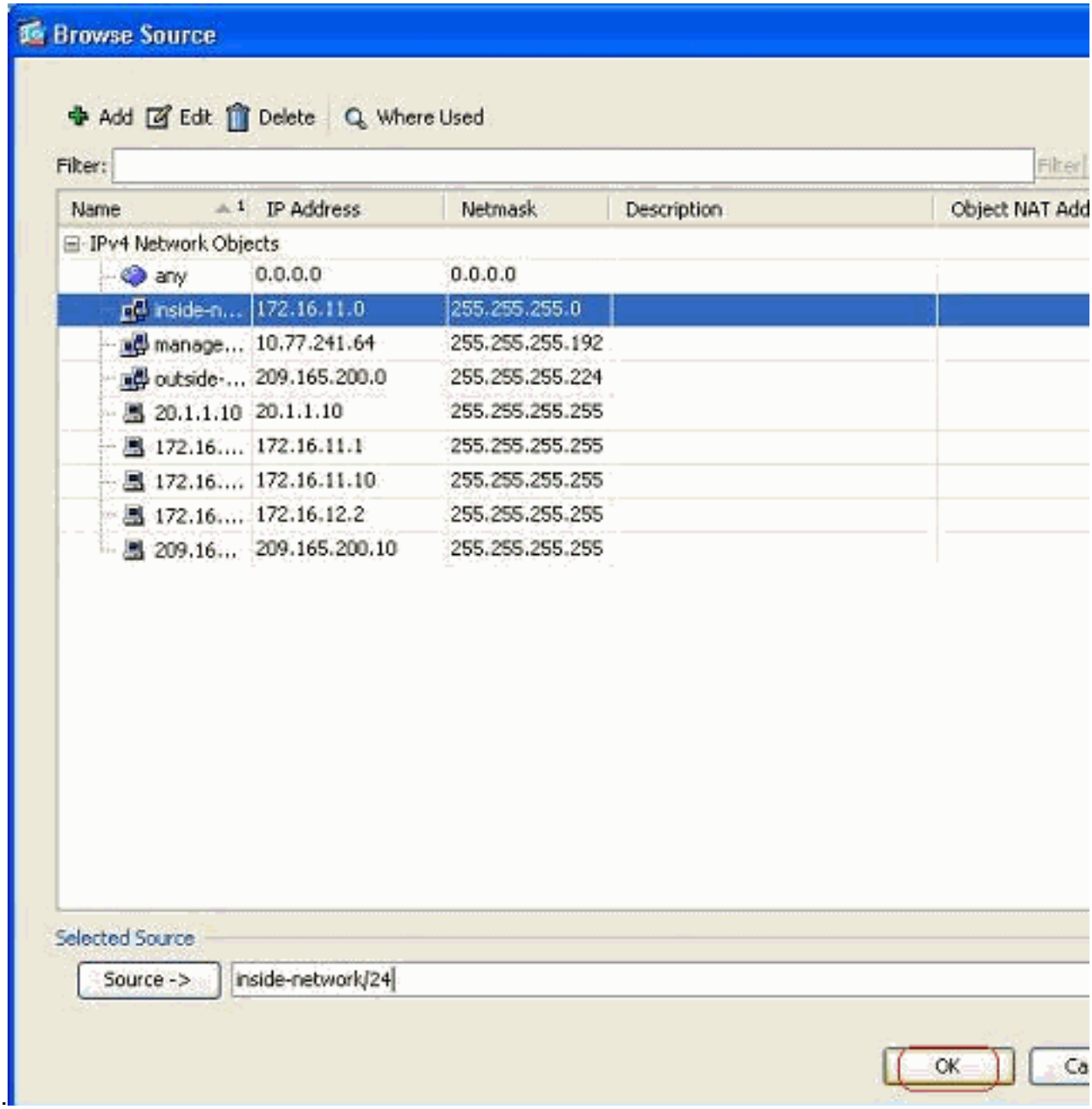


2. 트래픽에서 수행할 작업과 함께 이 액세스 목록이 바인딩되어야 하는 인터페이스(예: 허용/거부)를 선택합니다.그런 다음 **Details** 버튼을 클릭하여 소스 네트워크를 선택합니다

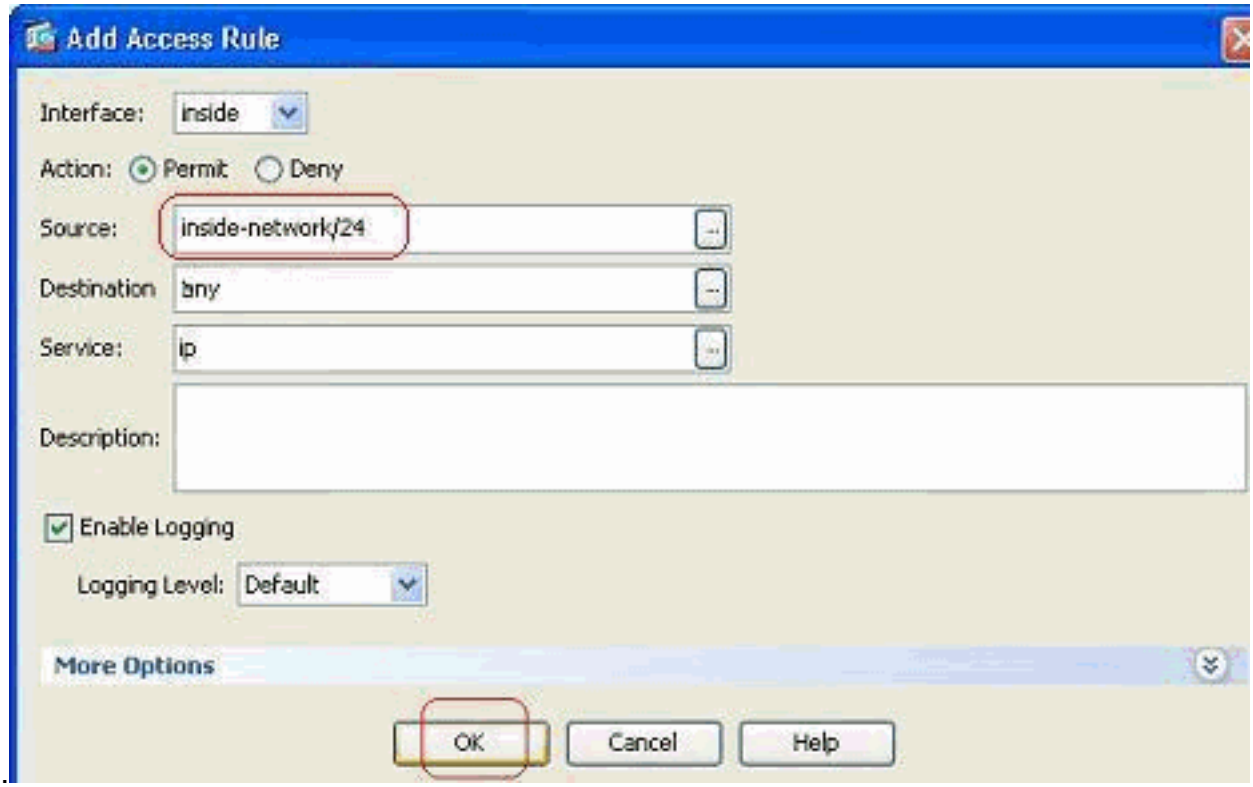


주: 이 창에 표시되는 여러 필드에 대한 간단한 설명은 다음과 같습니다.**Interface**(인터페이스) - 이 액세스 목록이 바인딩된 인터페이스를 결정합니다.**Action** - 새 규칙의 작업 유형을 결정합니다.두 가지 옵션을 사용할 수 있습니다.**Permit(허용)**은 일치하는 모든 트래픽을 허용하며 Deny는 일치하는 모든 트래픽을 차단합니다.**Source**(소스) - 이 필드는 트래픽의 소스를 지정합니다.이는 단일 IP 주소, 네트워크, 방화벽의 인터페이스 IP 주소 또는 네트워크 객체 그룹 중 무엇이든 될 수 있습니다.이러한 옵션은 **Details** 버튼으로 선택할 수 있습니다.**Destination**(대상) - 이 필드는 트래픽의 소스를 지정합니다.이는 단일 IP 주소, 네트워크, 방화벽의 인터페이스 IP 주소 또는 네트워크 객체 그룹 중 무엇이든 될 수 있습니다.이러한 옵션은 **Details** 버튼으로 선택할 수 있습니다.**Service**(서비스) - 이 필드는 이 액세스 목록이 적용되는 트래픽의 프로토콜 또는 서비스를 결정합니다.다른 프로토콜 집합을 포함하는 서비스 그룹을 정의할 수도 있습니다.

3. **세부 정보** 버튼을 클릭하면 기존 네트워크 객체가 포함된 새 창이 표시됩니다.**내부 네트워크**를 **선택하고 확인**을 클릭합니다



4. Add Access **Rule** 창으로 돌아갑니다.Destination 필드에 any를 입력합니다.OK(**확인**)를 클릭하여 액세스 규칙의 컨피그레이션을 완료합니다

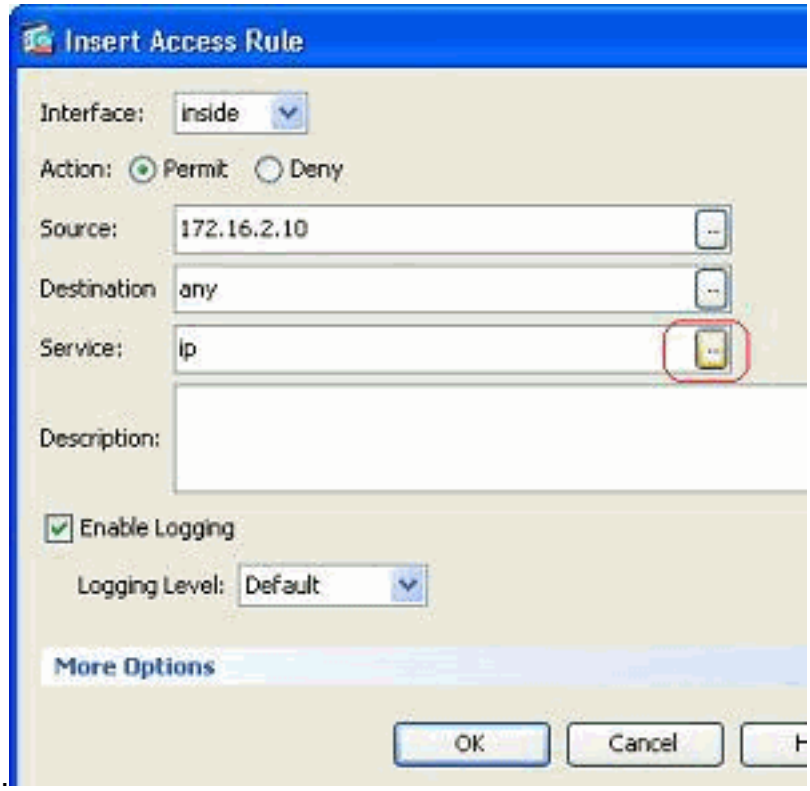


기존 규칙 앞에 액세스 규칙을 추가합니다.

기존 액세스 규칙 바로 전에 액세스 규칙을 추가하려면 다음 단계를 완료하십시오.

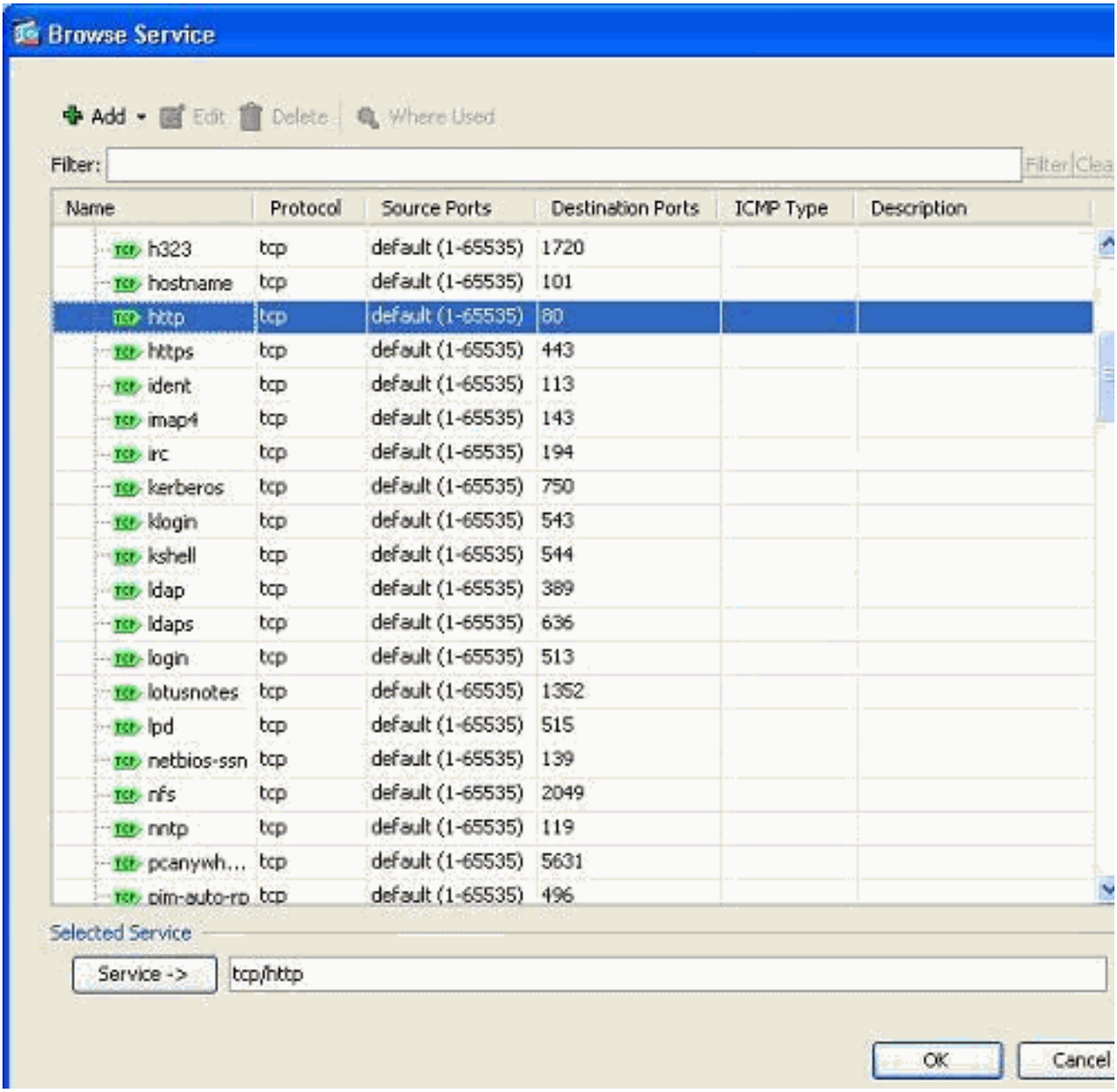
1. 기존 액세스 목록 항목을 선택하고 **Add** 드롭다운 메뉴에서 **Insert**를 클릭합니다

2. Source(소스) 및 Destination(대상)을 선택하고 Service(서비스) 필드의 **Details(세부사항)** 버튼을 클릭하여 Protocol(프로토콜)을 선택합니다



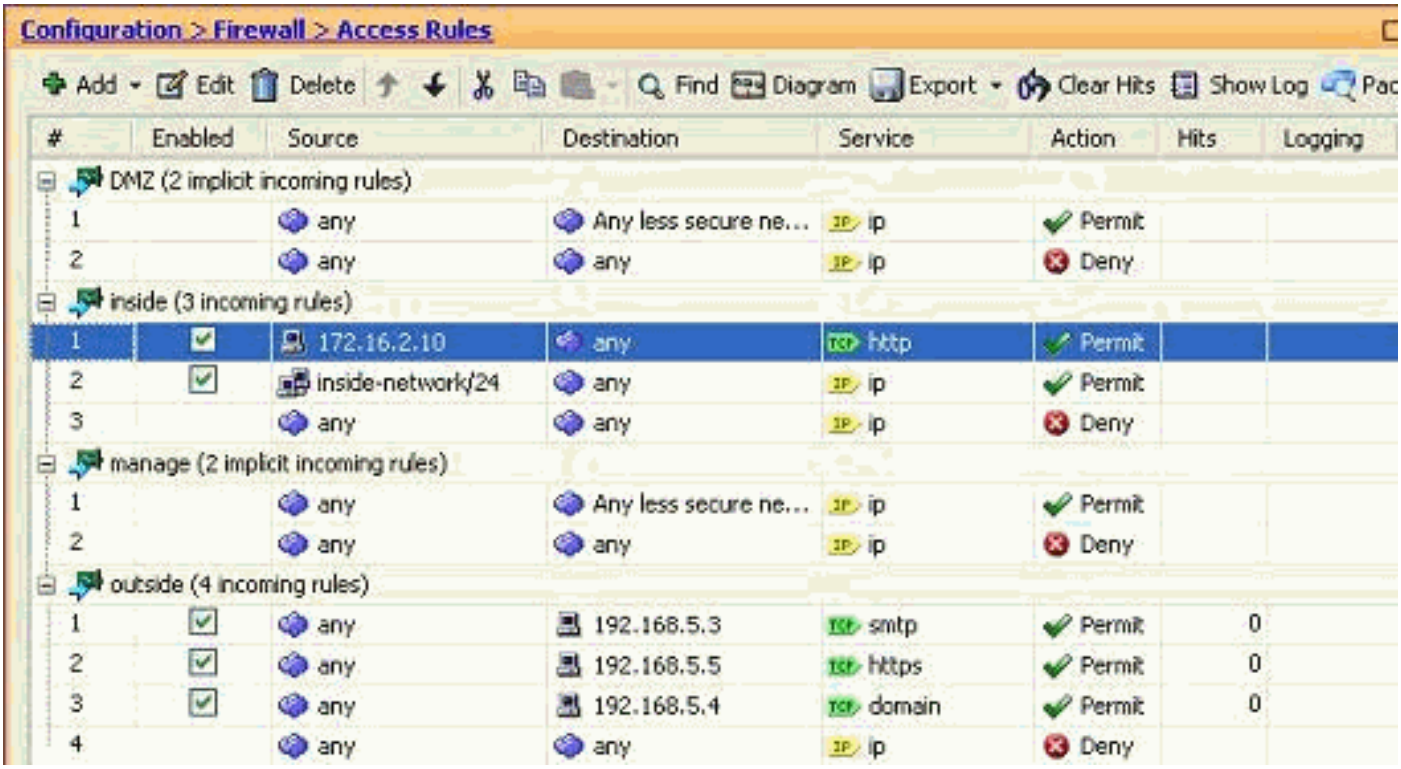
3. 프로토콜을 HTTP를 선택하고 OK를 **클릭합니다**

.



4. 액세스 규칙 삽입 창으로 돌아갑니다.Service(서비스) 필드는 **tcp/http**로 선택된 프로토콜로 채워집니다.새 액세스 목록 항목의 컨피그레이션을 완료하려면 확인을 클릭합니다

이제 Inside-Network에 대한 기존 항목 바로 앞에 표시되는 새 액세스 규칙을 관찰할 수 있습니다.



참고: 액세스 규칙의 순서는 매우 중요합니다.필터링할 각 패킷을 처리하는 동안 ASA는 패킷이 순차적 순서로 액세스 규칙 기준과 일치하는지 검사하고, 일치하는 경우 해당 액세스 규칙의 작업을 구현합니다.액세스 규칙이 일치하면 추가 액세스 규칙으로 진행되지 않고 다시 확인합니다.

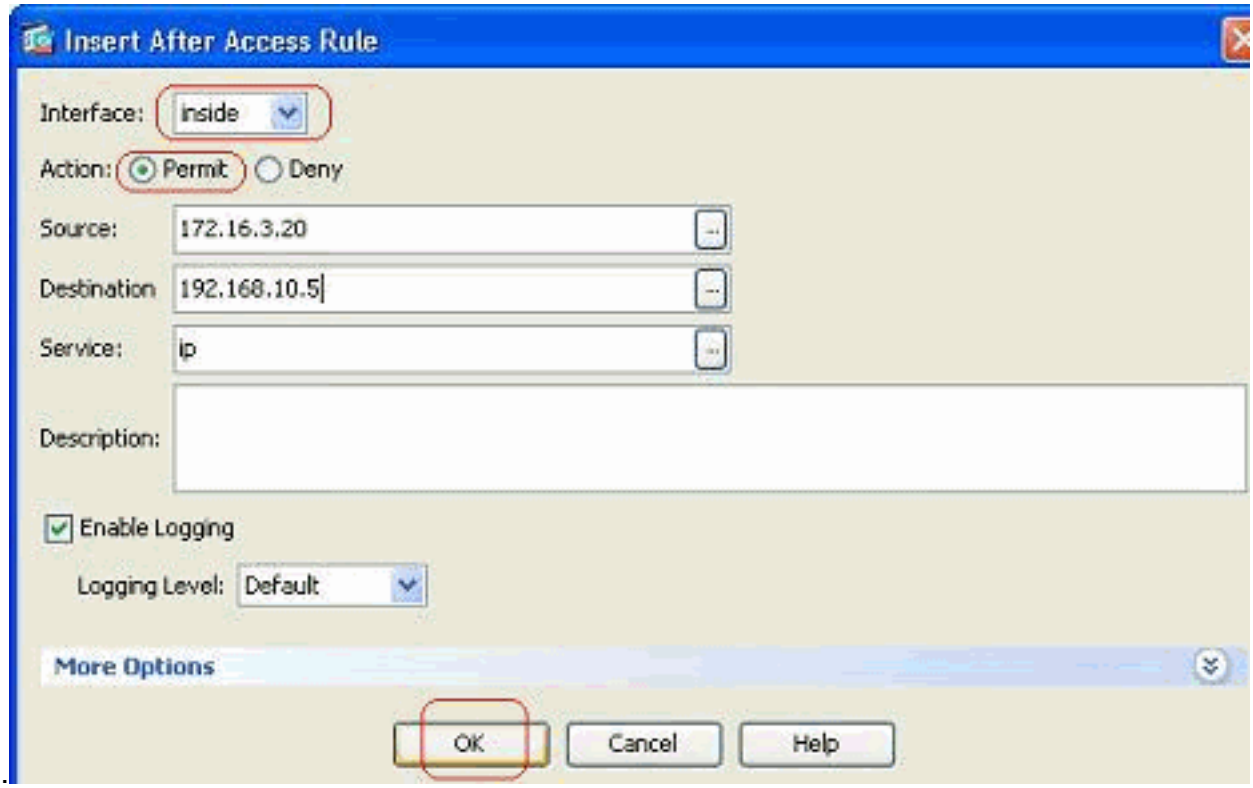
기존 규칙 뒤에 액세스 규칙 추가:

기존 액세스 규칙 바로 다음에 액세스 규칙을 생성하려면 다음 단계를 완료합니다.

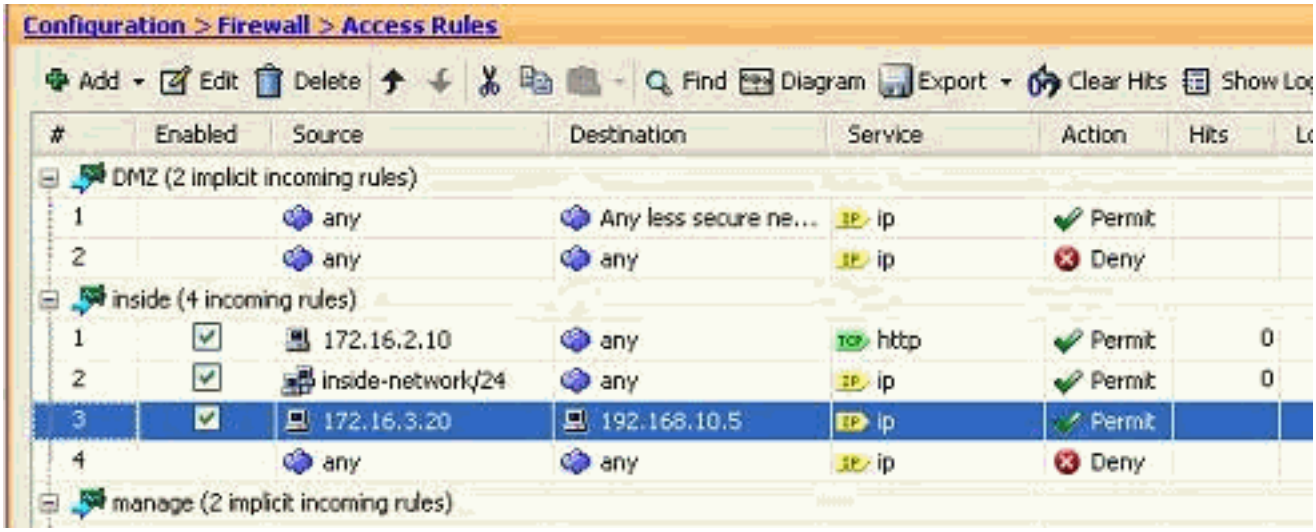
1. 새 액세스 규칙을 가져야 하는 액세스 규칙을 선택하고 Add 드롭다운 메뉴에서 Insert After를

선택합니다.

2. Interface, Action, Source, Destination 및 Service 필드를 지정하고 **OK**를 클릭하여 이 액세스 규칙의 컨피그레이션을 완료합니다



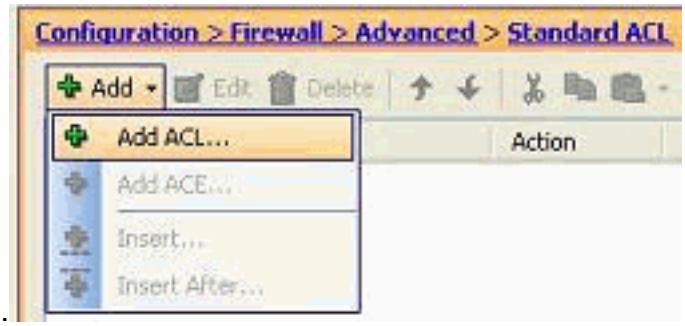
새로 구성된 액세스 규칙이 이미 구성된 액세스 규칙 바로 뒤에 있는지 확인할 수 있습니다.



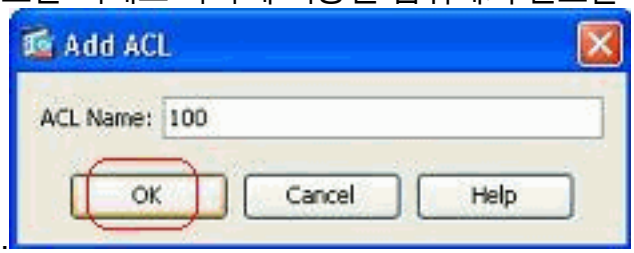
표준 액세스 목록 생성

ASDM GUI를 사용하여 표준 액세스 목록을 생성하려면 다음 단계를 완료합니다.

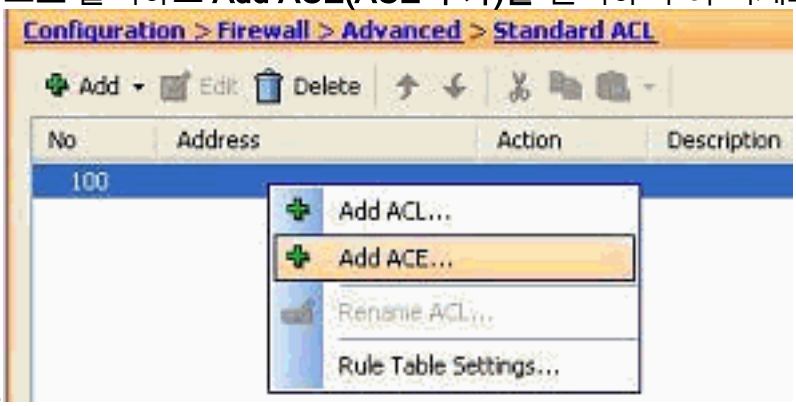
1. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > **Advanced(고급)** > **Standard ACL(표준 ACL)** > **Add(추가)를 선택하고 Add ACL(ACL 추가)**을 클릭합니다



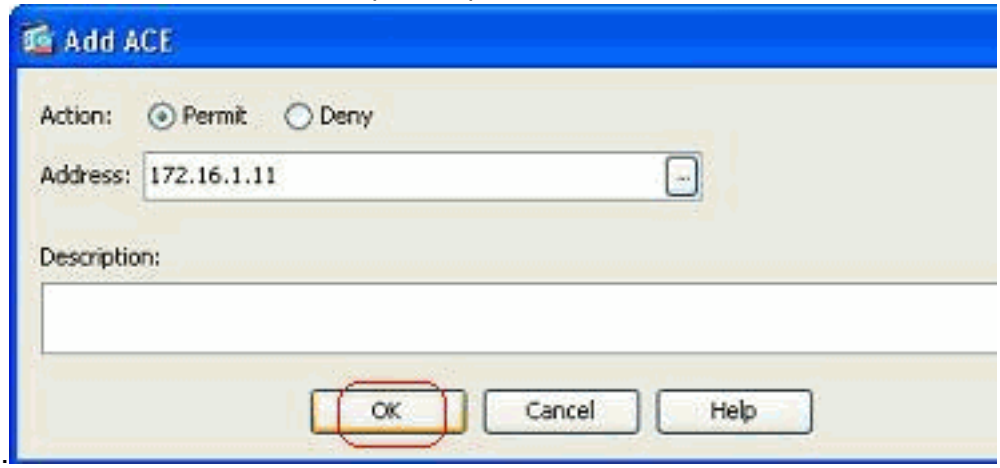
2. 표준 액세스 목록에 허용된 범위에서 번호를 지정하고 **확인**을 클릭합니다



3. 액세스 목록을 마우스 오른쪽 버튼으로 클릭하고 **Add ACE(ACE 추가)를** 선택하여 이 액세스 목록에 액세스 규칙을 추가합니다.



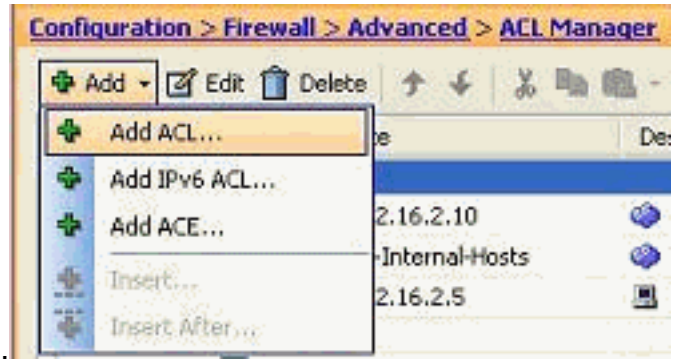
4. Action(작업)을 선택하고 **Source 주소**를 **지정합니다**.필요한 경우 **설명**도 지정합니다.OK**를** 클릭하여 액세스 규칙의 컨피그레이션을 완료합니다



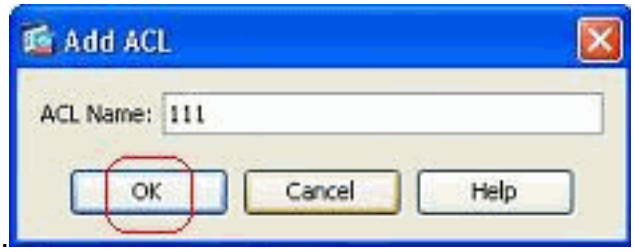
전역 액세스 규칙 생성

전역 액세스 규칙이 포함된 확장 액세스 목록을 생성하려면 다음 단계를 완료합니다.

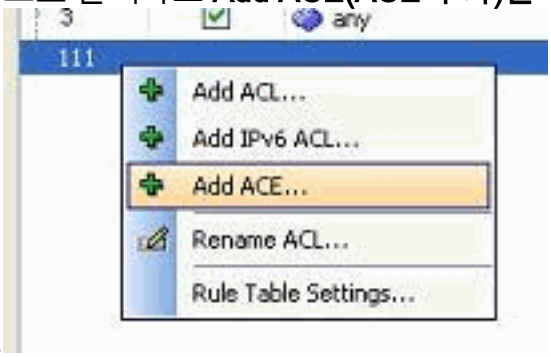
1. Configuration(**컨피그레이션**) > Firewall(**방화벽**) > Advanced(**고급**) > ACL Manager(**ACL 관리자**) > Add(**추가**)**를** 선택하고 **Add ACL(ACL 추가)** 버튼**을** 클릭합니다



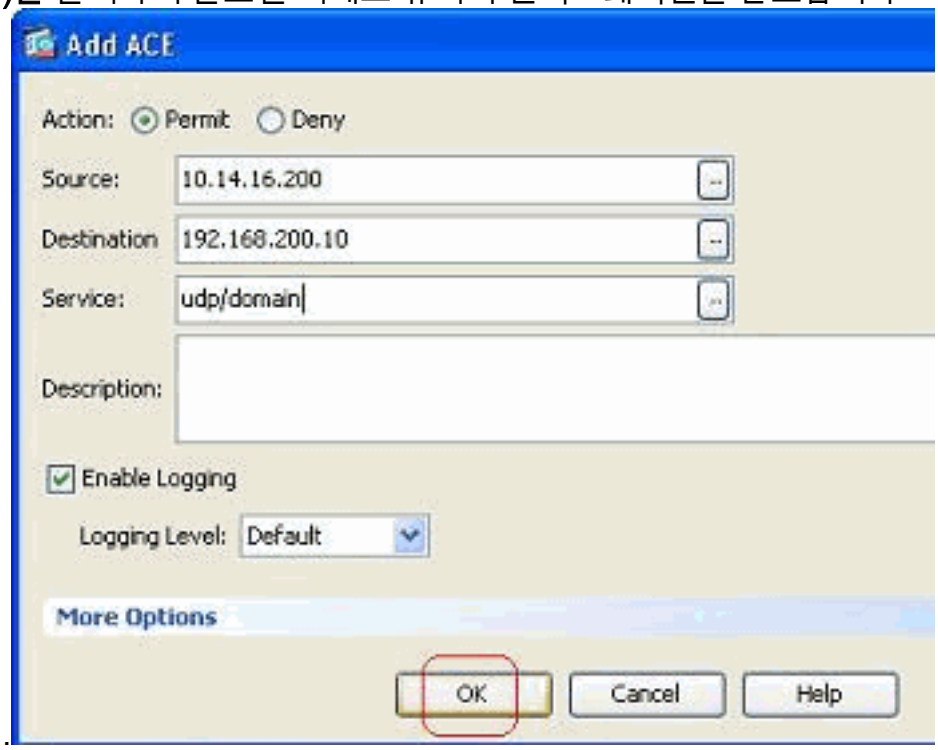
2. 액세스 목록의 이름을 지정하고 확인을 **클릭합니다**



3. 액세스 목록을 마우스 오른쪽 버튼으로 클릭하고 **Add ACE(ACE 추가)를** 선택하여 이 액세스 목록에 액세스 규칙을 추가합니다.



4. Action(작업), Source(소스), Destination(대상) 및 Service(서비스) 필드를 완성하고 **OK(확인)를** 클릭하여 글로벌 액세스 규칙의 컨피그레이션을 완료합니다



이제 표시된 대로 전역 액세스 규칙을 볼 수 있습니다.

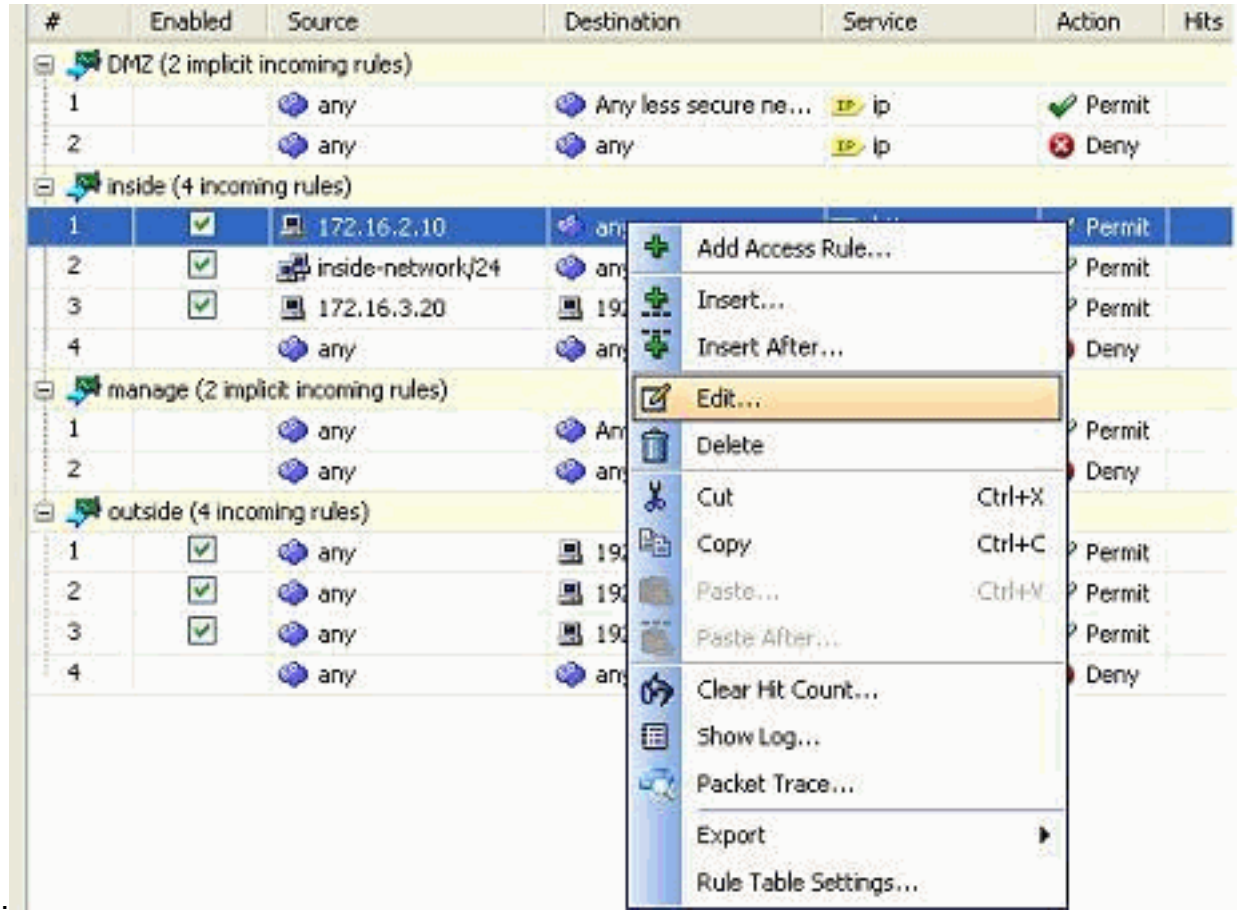
기존 액세스 목록 편집

이 섹션에서는 기존 액세스를 수정하는 방법에 대해 설명합니다.

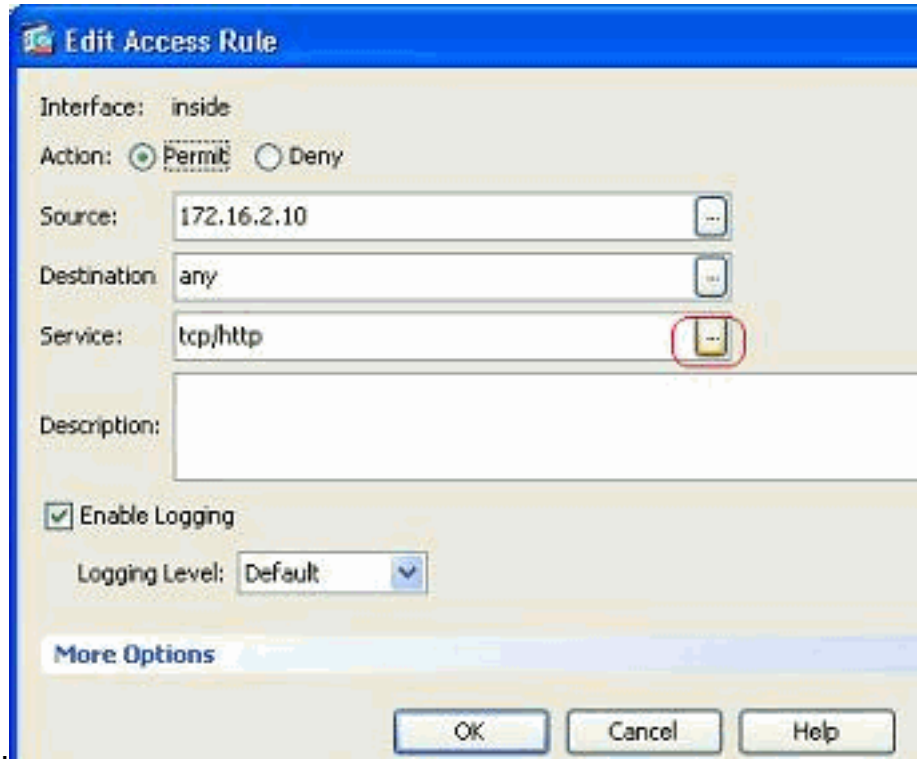
Protocol 필드를 편집하여 서비스 그룹을 생성합니다.

새 서비스 그룹을 생성하려면 다음 단계를 완료합니다.

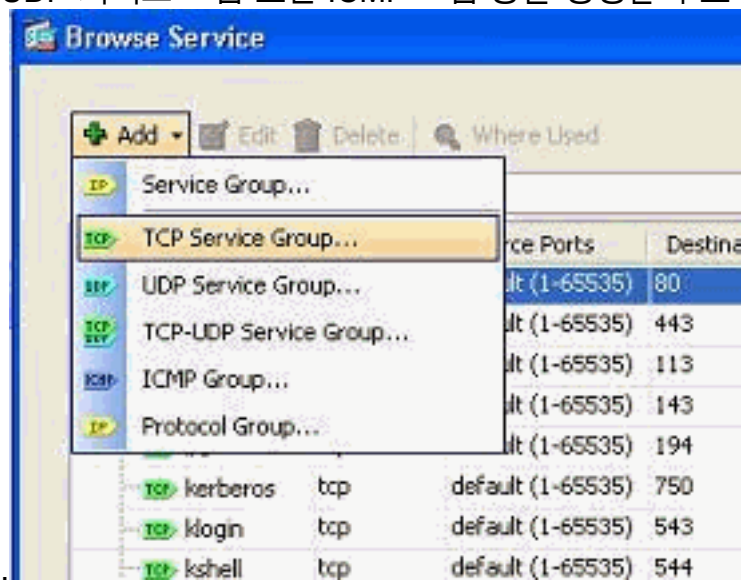
1. 수정해야 하는 액세스 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Edit**(수정)를 선택하여 특정 액세스 규칙을 수정합니다



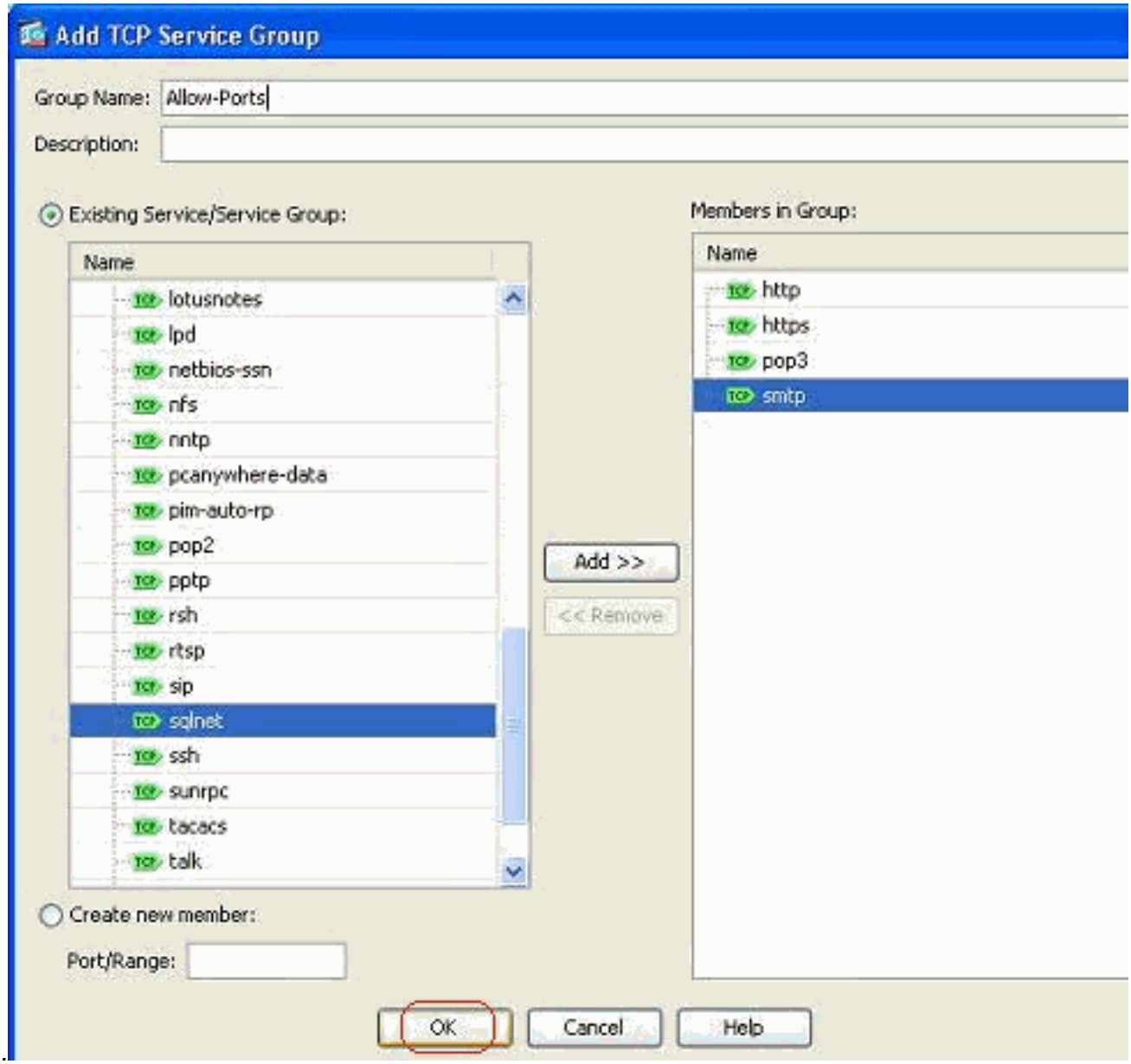
2. 이 액세스 규칙과 연결된 프로토콜을 수정하려면 Details(세부사항) 버튼을 클릭합니다



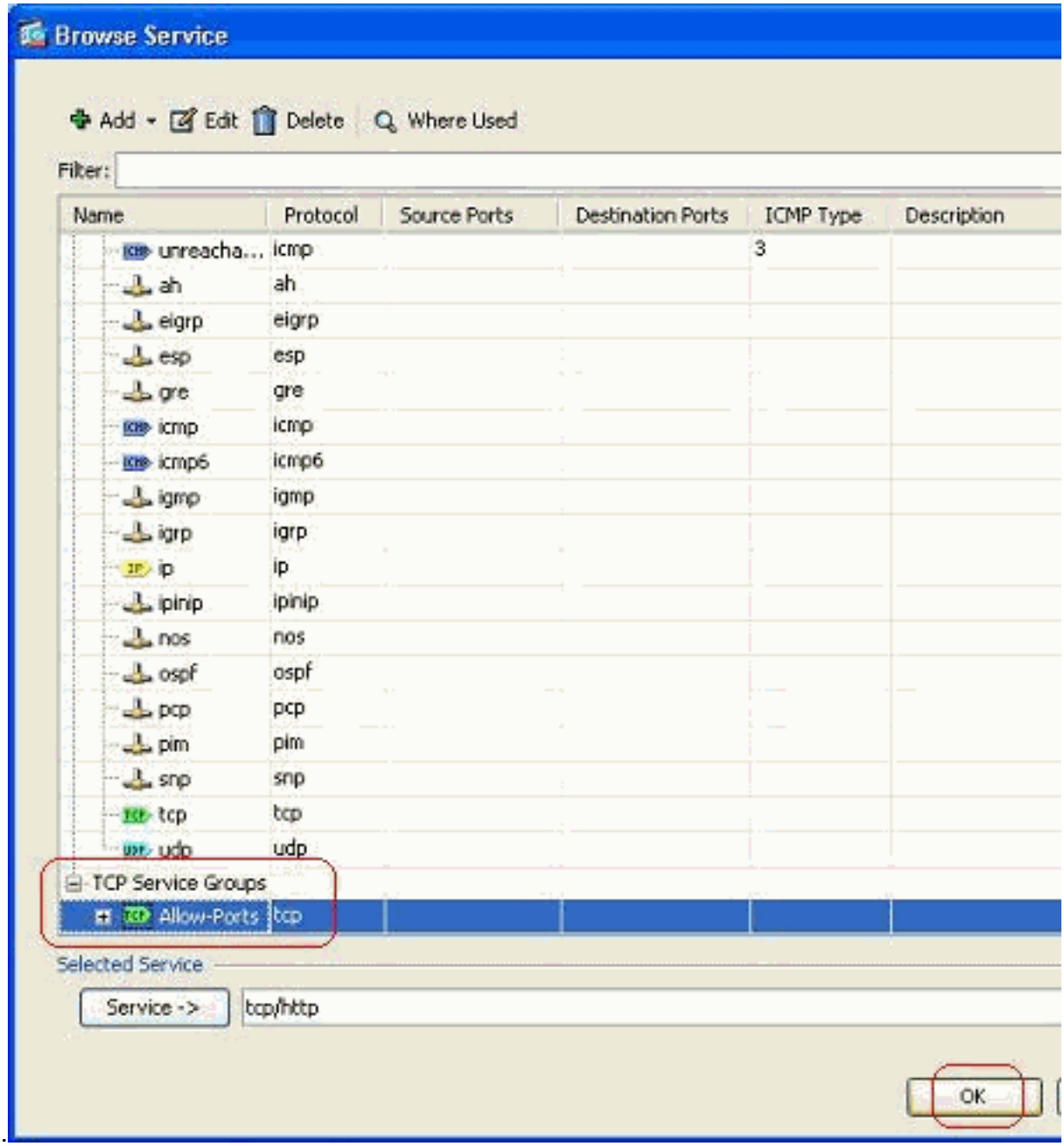
3. 필요한 경우 HTTP 이외의 프로토콜을 선택할 수 있습니다.단일 프로토콜만 선택할 경우 서비스 그룹을 생성할 필요가 없습니다.이 액세스 규칙과 매칭할 인접하지 않은 여러 프로토콜을 식별해야 하는 요구 사항이 있는 경우 서비스 그룹을 생성하는 것이 좋습니다.새 TCP 서비스 그룹**을** 생성하려면 Add**(추가) > TCP 서비스 그룹**을 선택합니다.**참고:** 동일한 방식으로 새 UDP 서비스 그룹 또는 ICMP 그룹 등을 생성할 수도 있습니다



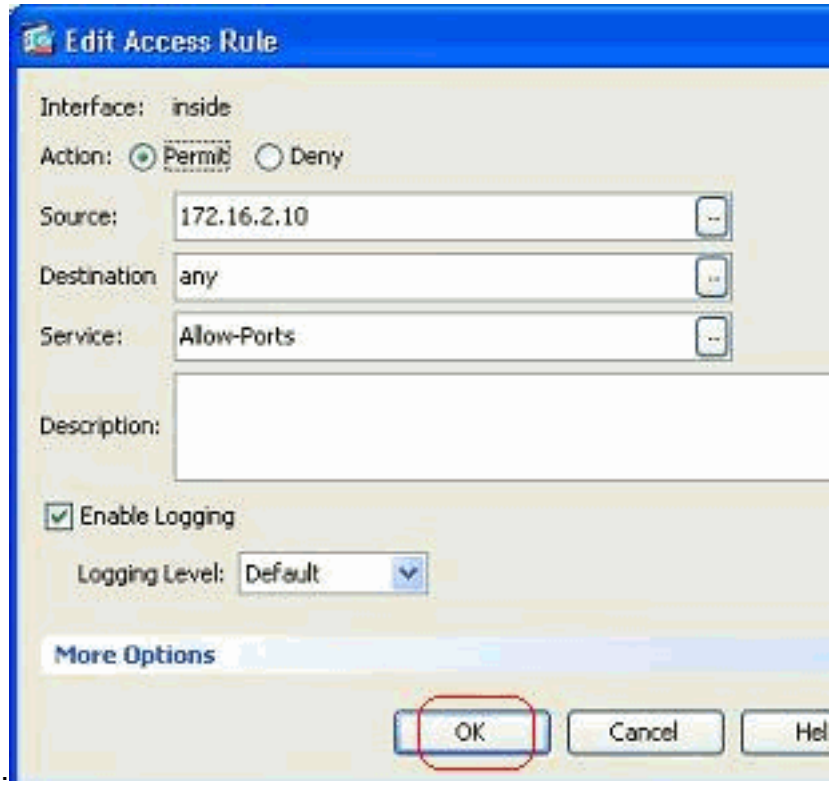
4. 이 서비스 그룹의 이름을 지정하고 왼쪽 메뉴에서 프로토콜을 선택한 다음 **추가를** 클릭하여 오른쪽 그룹의 구성원 메뉴로 이동합니다.요구 사항에 따라 여러 프로토콜을 서비스 그룹의 멤버로 추가할 수 있습니다.프로토콜은 하나씩 추가됩니다.모든 구성원이 추가된 후 **확인**을 클릭합니다



5. 새로 생성된 서비스 그룹은 탭 **TCP 서비스 그룹** 아래에서 볼 수 있습니다.OK 버튼을 클릭하여 Edit Access Rule 창으로 돌아갑니다

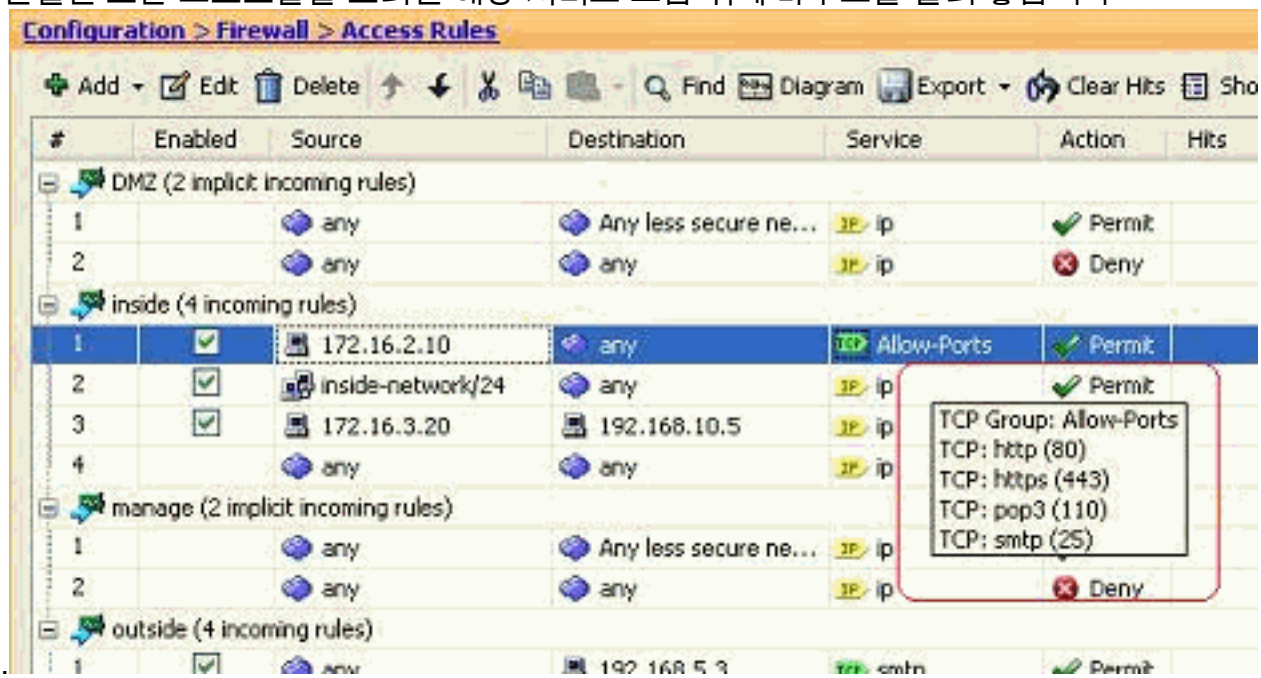


6. 서비스 필드가 새로 생성된 서비스 그룹으로 채워져 있음을 확인할 수 있습니다.OK(**확인**)를



클릭하여 편집을 완료합니다.

7. 연결된 모든 프로토콜을 보려면 해당 서비스 그룹 위에 마우스를 올려 놓습니다

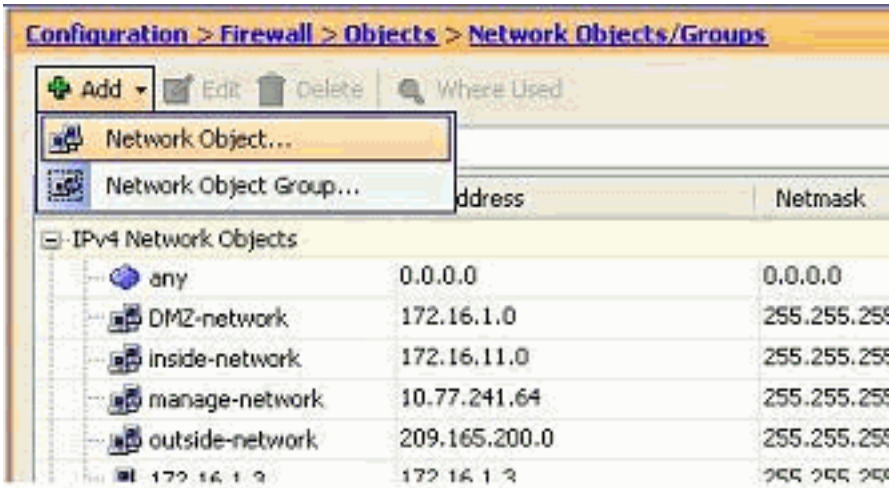


Source/Destination 필드를 편집하여 네트워크 객체 그룹을 생성합니다.

객체 그룹은 액세스 목록의 생성 및 유지 관리를 간소화하는 데 사용됩니다.유사 객체를 함께 그룹화할 때 각 객체에 대해 ACE를 별도로 입력하지 않고 단일 ACE에서 객체 그룹을 사용할 수 있습니다.객체 그룹을 생성하기 전에 객체를 생성해야 합니다.ASDM 용어에서 객체는 네트워크 객체라고 하고 객체 그룹을 네트워크 객체 그룹이라고 합니다.

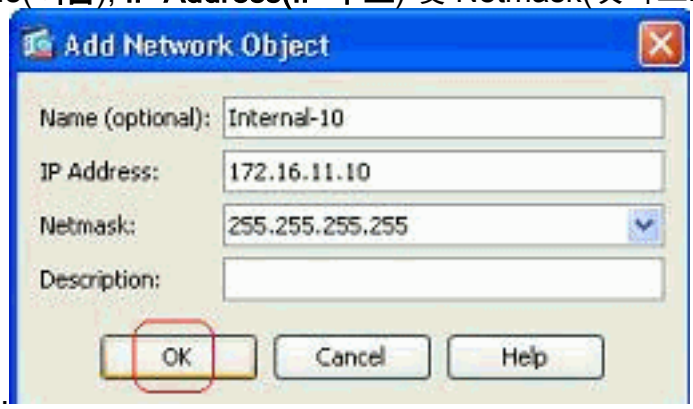
다음 단계를 완료하십시오.

1. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > **Objects(개체)** > **Network Objects/Groups(네트워크 개체/그룹)** > **Add(추가)**를 선택하고 **Network Object(네트워크 개체)**를 클릭하여 새 네트워크 개체를 만듭니다

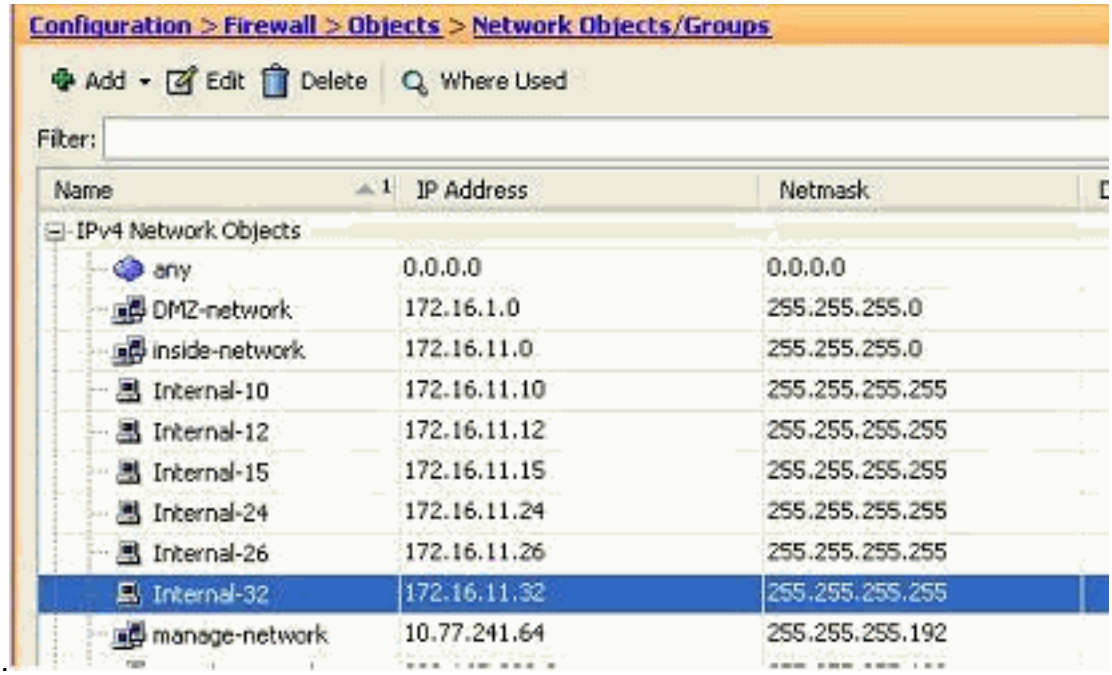


.

2. Name(**이름**), **IP Address(IP 주소)** 및 Netmask(넷마스크) **필드**를 입력하고 **OK(확인)**를 클릭합니다.



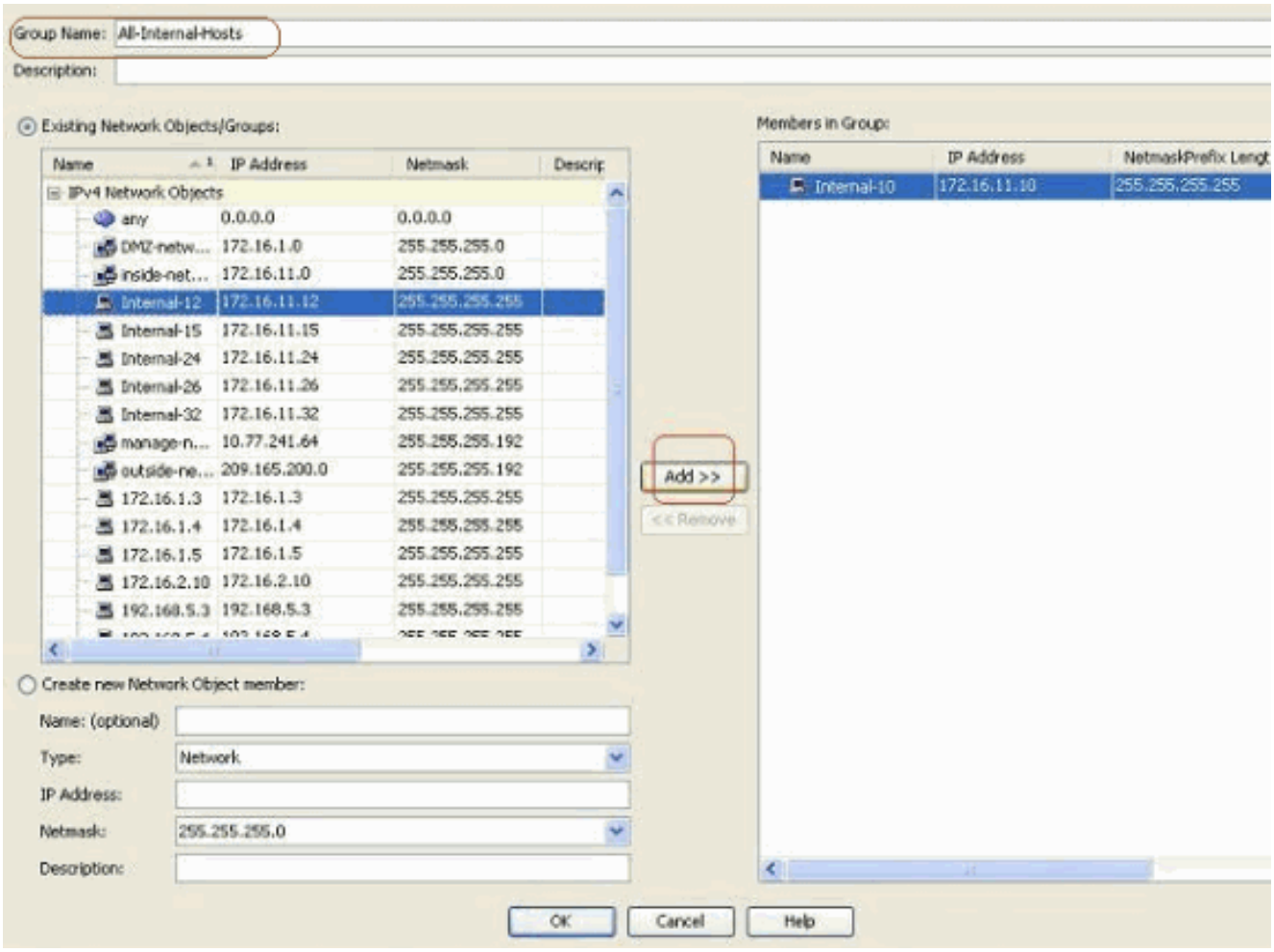
3. 새로 생성된 네트워크 객체는 객체 목록에서 확인할 수 있습니다.**확인**을 **클릭합니다**



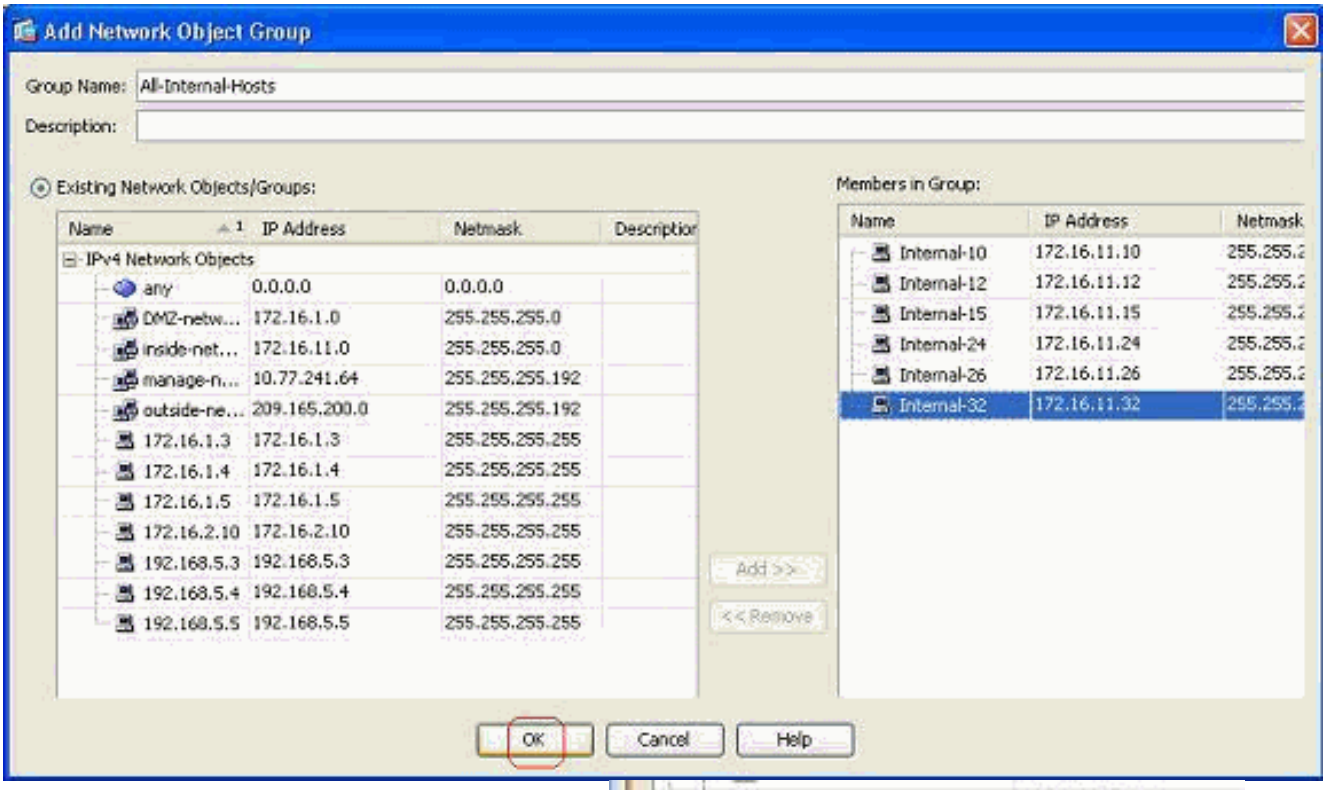
.

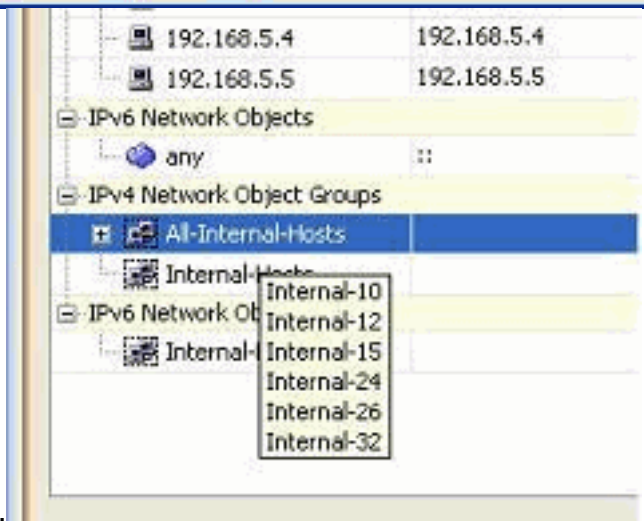
4. Configuration(**컨피그레이션**) **> Firewall(방화벽) > Objects(개체) > Network Objects/Groups(네트워크 개체/그룹) > Add(추가)**를 선택하고 **Network Object Group(네트워크 개체 그룹)**을 클릭하여 새 네트워크 개체 그룹을 만듭니다

5. 모든 네트워크 객체의 사용 가능한 목록은 창의 왼쪽 창에서 확인할 수 있습니다.개별 네트워크 객체를 선택하고 **Add** 버튼을 클릭하여 새로 생성된 네트워크 객체 그룹의 멤버로 만듭니다.그룹 이름은 할당된 필드에 지정해야 합니다



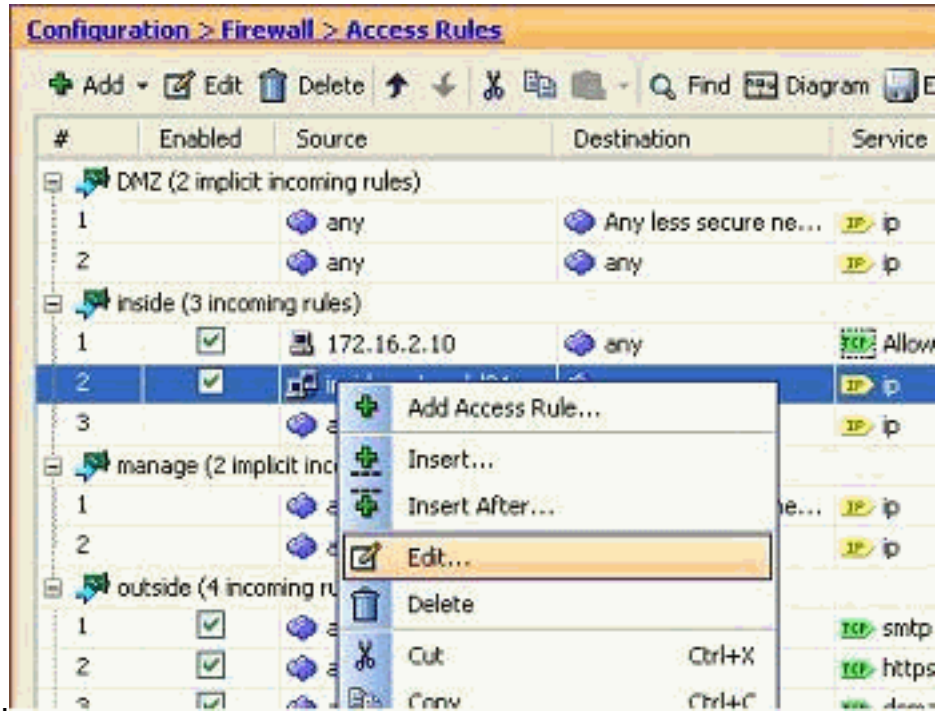
6. 그룹의 모든 구성원을 추가한 후 **확인**을 클릭합니다



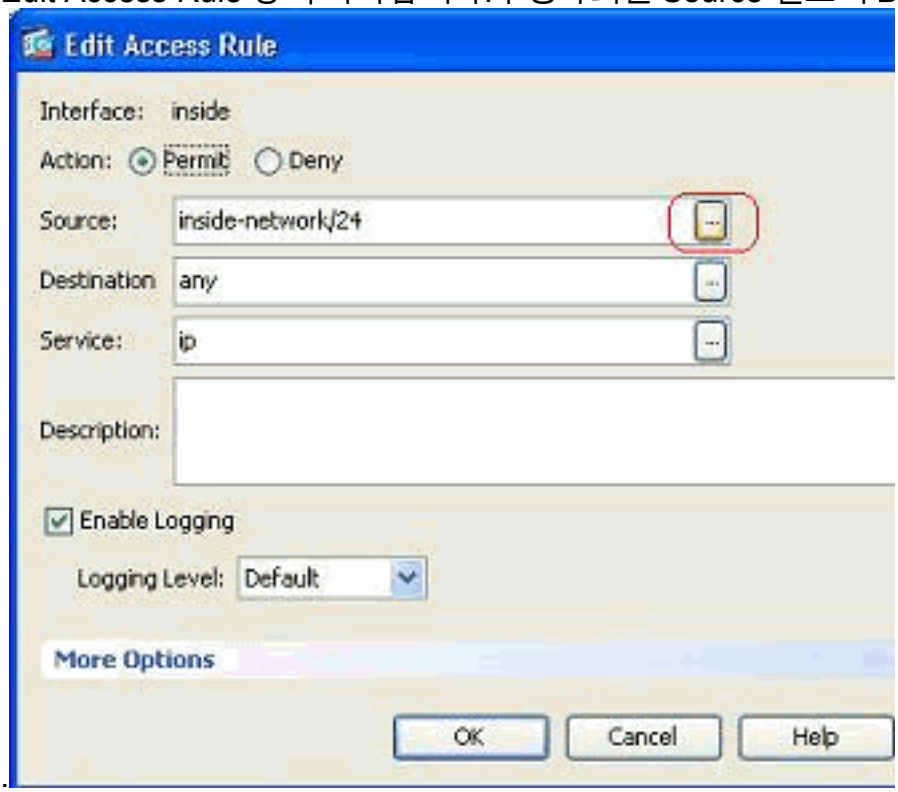


이제 네트워크 객체 그룹을 볼 수 있습니다.

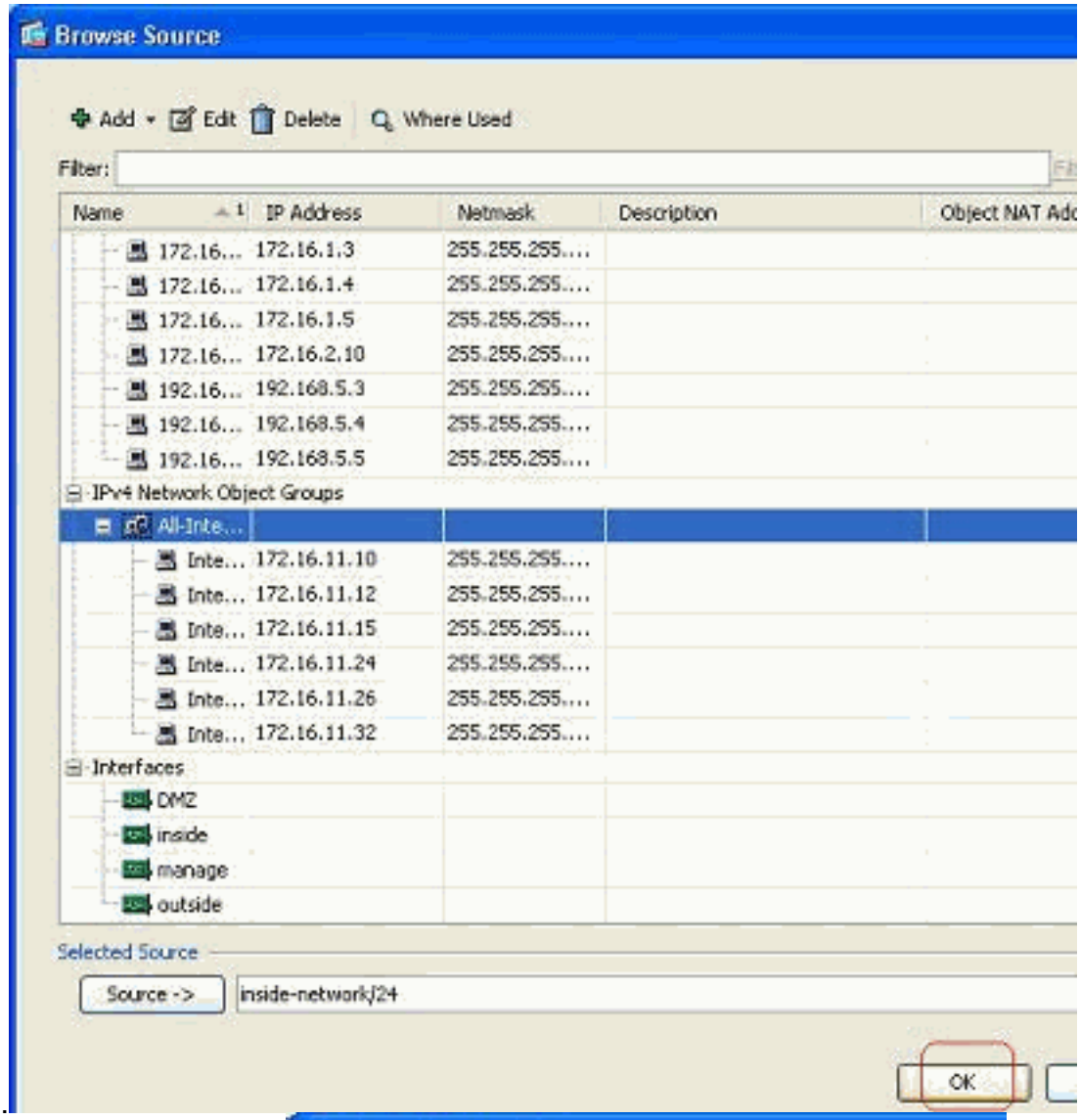
7. 네트워크 그룹 객체를 사용하여 기존 액세스 목록의 소스/대상 필드를 수정하려면 특정 액세스 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Edit**를 선택합니다

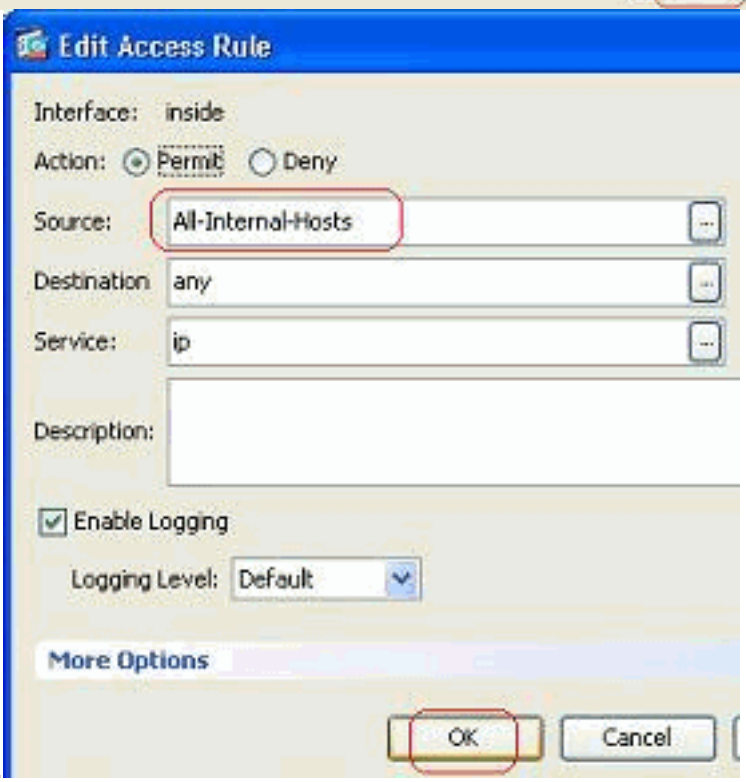


8. Edit Access Rule 창이 나타납니다.수정하려면 Source 필드의 **Details** 버튼을 클릭합니다

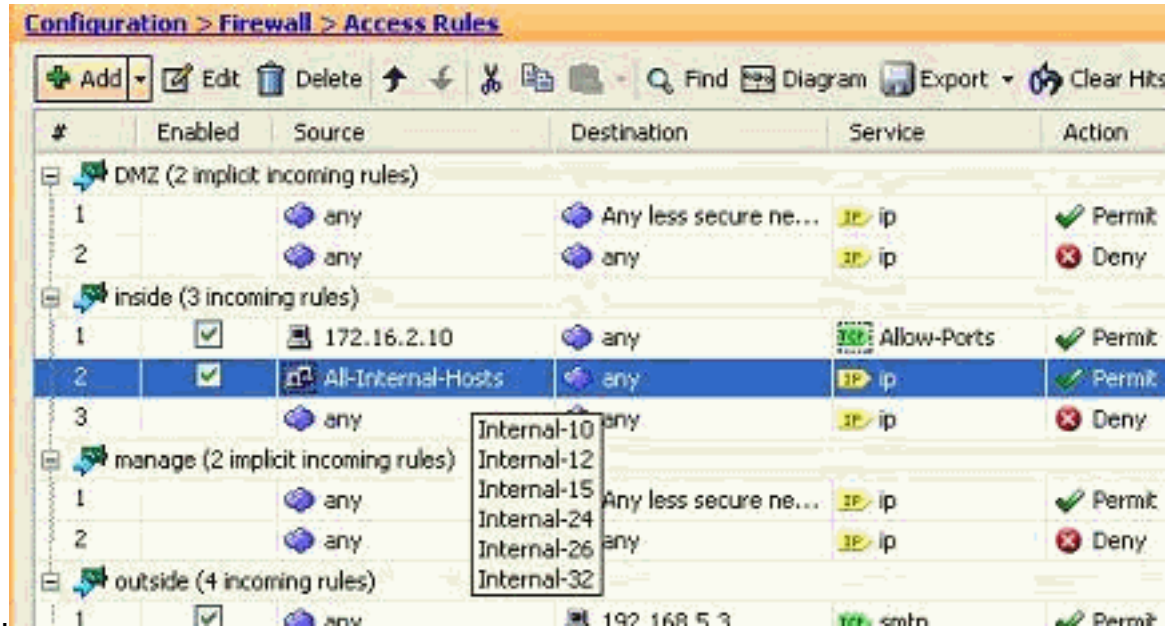


9. All-**Internal-Hosts** 네트워크 객체 그룹을 선택하고 **OK** 버튼을 클릭합니다





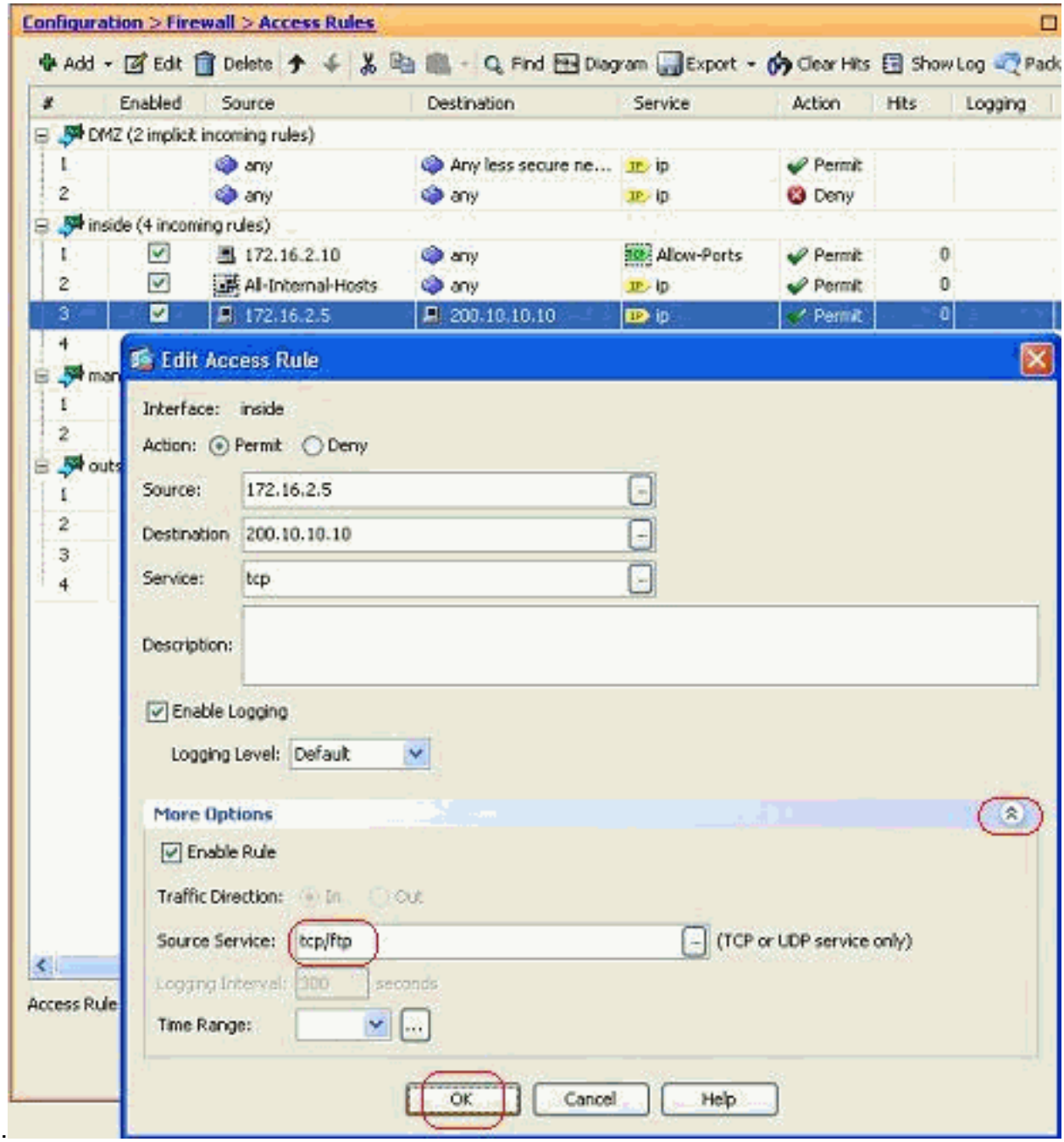
10. **확인**을 **클릭합니다**.
11. 그룹의 멤버를 보려면 액세스 규칙의 Source(소스) 필드 위에 마우스를 올려 놓습니다



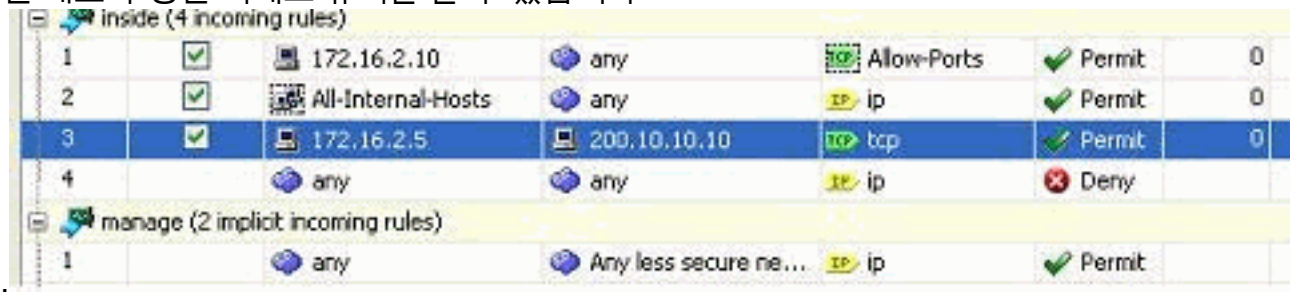
소스 포트 편집:

액세스 규칙의 소스 포트를 수정하려면 다음 단계를 완료하십시오.

1. 기존 액세스 규칙의 소스 포트를 수정하려면 해당 포트를 마우스 오른쪽 버튼으로 클릭하고 Edit(수정)를 **선택합니다**.Edit Access Rule 창이 나타납니다



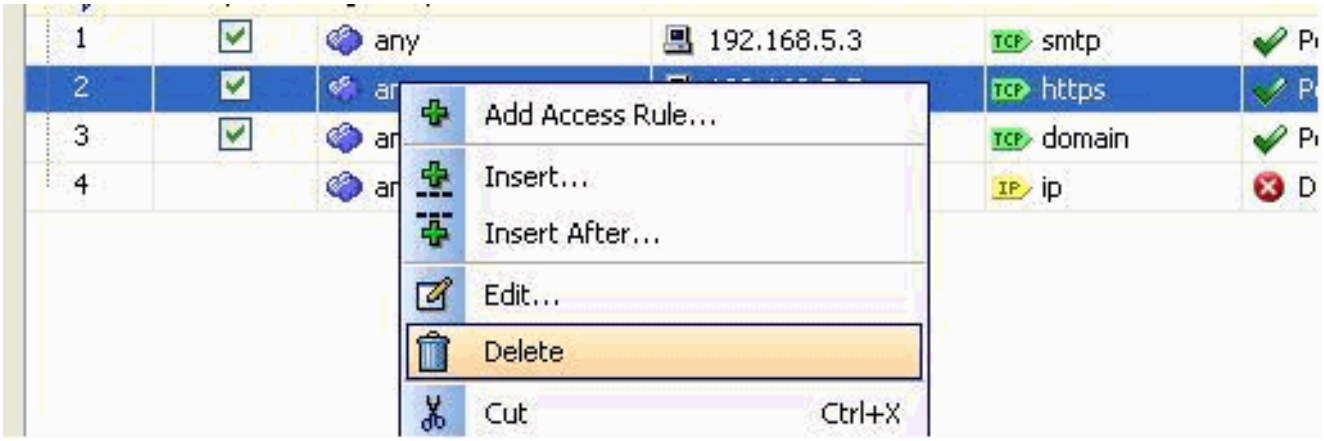
2. 소스 서비스 필드를 수정하려면 **추가 옵션** 드롭다운 버튼을 클릭하고 **확인**을 클릭합니다.표시된 대로 수정된 액세스 규칙을 볼 수 있습니다



액세스 목록 삭제

액세스 목록을 삭제하려면 다음 단계를 완료하십시오.

1. 기존 액세스 목록을 삭제하기 전에 액세스 목록 항목(액세스 규칙)을 삭제해야 합니다. 먼저 모든 액세스 규칙을 삭제해야 액세스 목록을 삭제할 수 있습니다.삭제할 액세스 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Delete**(삭제)를 선택합니다



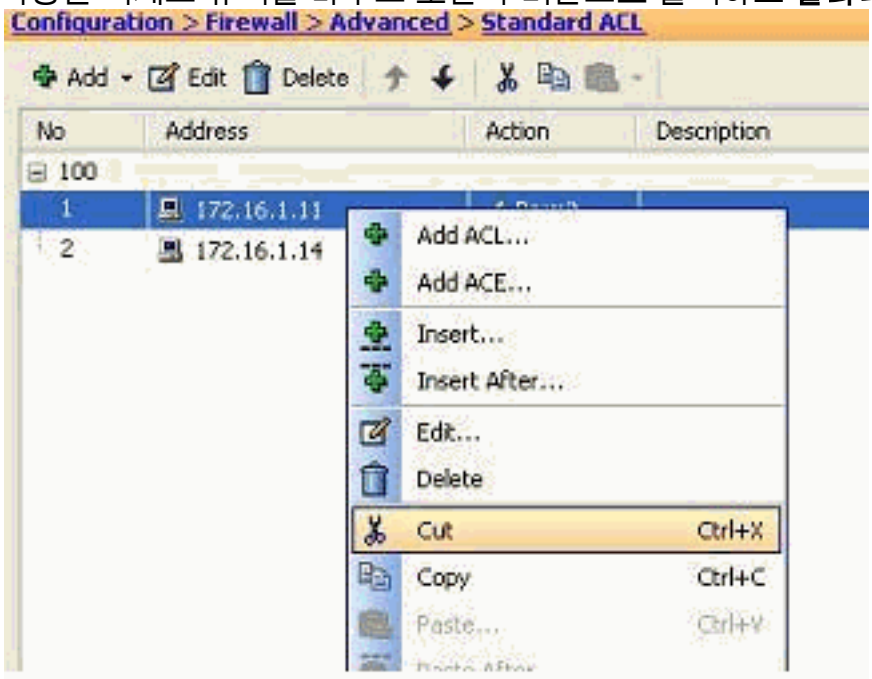
2. 모든 기존 액세스 규칙에서 동일한 Delete(삭제) 작업을 완료한 다음 액세스 목록을 선택하고 **Delete(삭제)**를 선택하여 삭제합니다.

액세스 규칙 내보내기

ASDM 액세스 규칙은 액세스 목록을 각 인터페이스와 바인딩하는 반면 ACL Manager는 모든 확장 액세스 목록을 추적합니다.ACL Manager로 생성된 액세스 규칙은 어떤 인터페이스도 바인딩하지 않습니다.이러한 액세스 목록은 일반적으로 NAT-Exempt, VPN-Filter 및 인터페이스와 연결되지 않은 유사한 기타 기능에 사용됩니다.ACL Manager에는 Configuration(컨피그레이션) **> Firewall(방화벽) > Access Rules(액세스 규칙)** 섹션에 있는 모든 항목**이** 포함됩니다.또한 **ACL 관리자**는 어떤 인터페이스도 연결되지 않은 전역 액세스 규칙을 포함합니다.ASDM은 액세스 목록에서 다른 액세스 목록으로 쉽게 액세스 규칙을 내보낼 수 있는 방식으로 구성됩니다.

예를 들어, 이미 전역 액세스 규칙의 일부인 액세스 규칙이 인터페이스에 연결되어야 하는 경우 다시 구성할 필요가 없습니다.대신 **잘라내기** 및 붙여넣기 **작업을** 수행하여 이를 수행할 수 있습니다.

1. 지정된 액세스 규칙을 마우스 오른쪽 버튼으로 클릭하고 **잘라내기**를 선택합니다



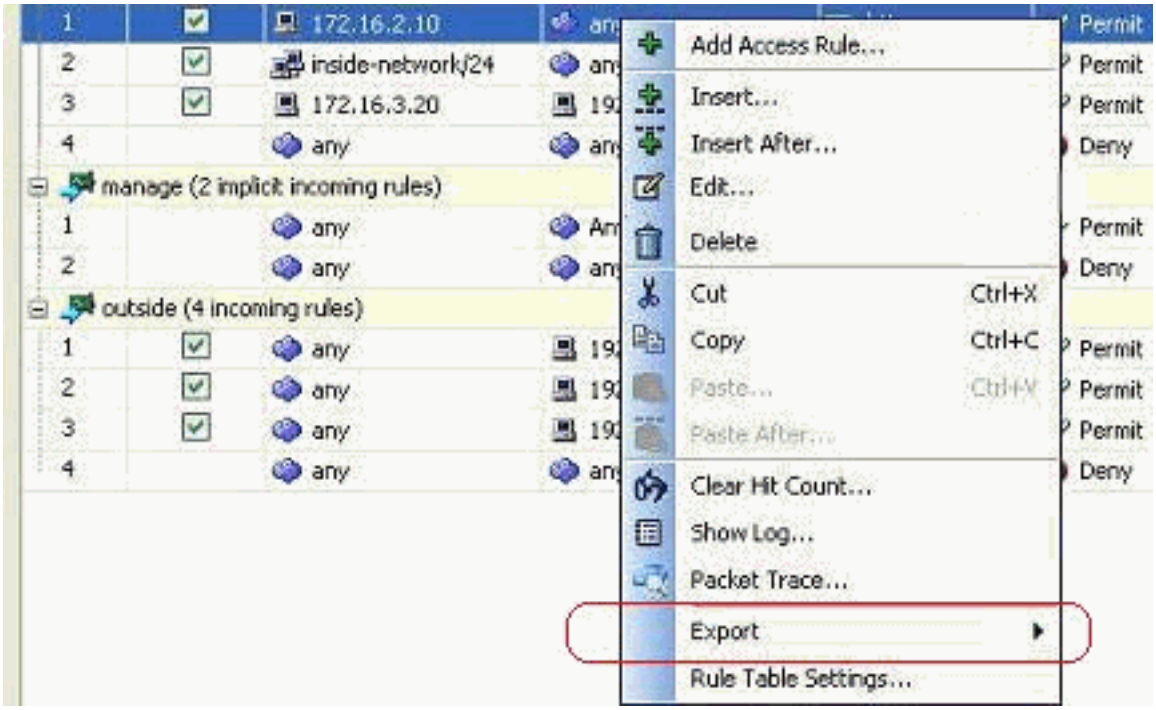
2. 이 액세스 규칙을 삽입해야 하는 필수 액세스 목록을 선택합니다.도구 모음에서 붙여넣기를 사용하여 액세스 규칙을 삽입할 수 있습니다.

액세스 목록 정보 내보내기

액세스 목록 정보를 다른 파일로 내보낼 수 있습니다.이 정보를 내보내려면 두 가지 형식이 지원됩니다.

1. 쉼표로 구분된 값(CSV) 형식
2. HTML 형식

액세스 규칙 중 하나를 마우스 오른쪽 버튼으로 클릭하고 **Export(내보내기)**를 선택하여 액세스 목록 정보를 파일로 전송합니다.



다음은 HTML 형식으로 표시되는 액세스 목록 정보입니다.

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
DMZ (2 incoming rules)									
1	True	172.16.1.10	any	ip	Permit		Default		
2		any	any	ip	Deny		Default		Implicit rule
inside (3 incoming rules)									
1	True	172.16.2.10	any	Allow-Ports	Permit	0	Default		
2	True	All-Internal-Hosts	any	ip	Permit	0	Default		
3		any	any	ip	Deny		Default		Implicit rule
manage (2 implicit incoming rules)									
1		any	Any less secure networks	ip	Permit		Default		Implicit rule: Permit all traffic to less secure networks
2		any	any	ip	Deny		Default		Implicit rule
outside (4 incoming rules)									
1	True	any	192.168.5.3	tcp/smtp	Permit	0	Default		
2	True	any	192.168.5.5	tcp/https	Permit	0	Default		
3	True	any	192.168.5.4	tcp/domain	Permit	0	Default		
4		any	any	ip	Deny		Default		Implicit rule

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

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

관련 정보

- ASDM 컨피그레이션 예 및 TechNotes
- ASA 컨피그레이션 예 및 Technotes
- 기술 지원 및 문서 – Cisco Systems