ASA/PIX 7.X:기본 전역 검사 비활성화 및 ASDM을 사용하여 기본이 아닌 애플리케이션 검사 활성화

목차

소개

이 문서에서는 응용 프로그램에 대한 전역 정책에서 기본 검사를 제거하는 방법 및 기본값이 아닌 응용 프로그램에 대해 검사를 활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 7.x 소프트웨어 이미지를 실행하는 Cisco ASA(Adaptive Security Appliance)를 기반으로 합니다.

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 7.x 소프트웨어 이미지를 실행하는 PIX Security Appliance와 함께 사용할 수도 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

기본 전역 정책

기본적으로 컨피그레이션에는 모든 기본 애플리케이션 검사 트래픽과 일치하는 정책이 포함되어 있으며 모든 인터페이스의 트래픽에 특정 검사를 적용합니다(글로벌 정책). 기본적으로 모든 검사가 활성화되어 있는 것은 아닙니다.하나의 전역 정책만 적용할 수 있습니다.전역 정책을 변경하려면 기본 정책을 수정하거나 비활성화하고 새 정책을 적용해야 합니다.(인터페이스 정책은 전역 정책을 재정의합니다.)

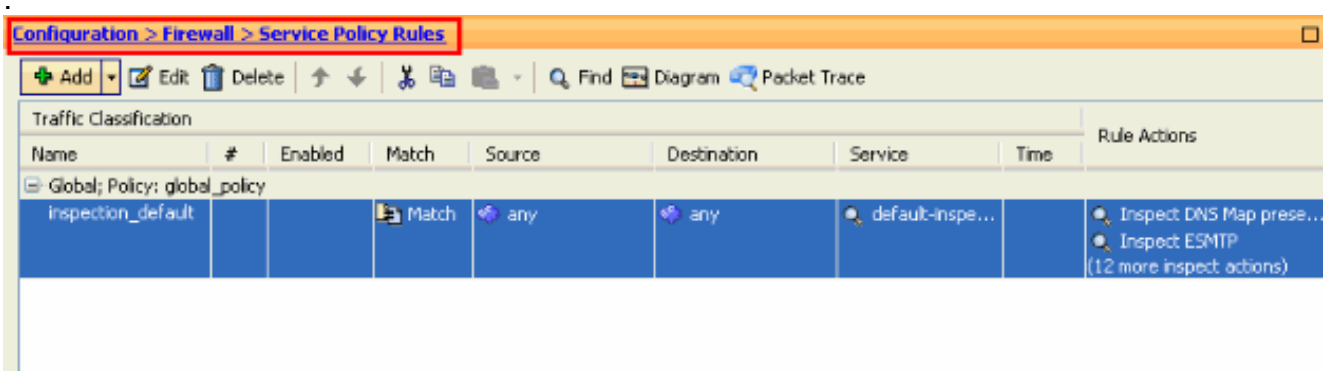
기본 정책 컨피그레이션에는 다음 명령이 포함됩니다.

```
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 rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
service-policy global_policy global
```

기본 애플리케이션 검사 사용

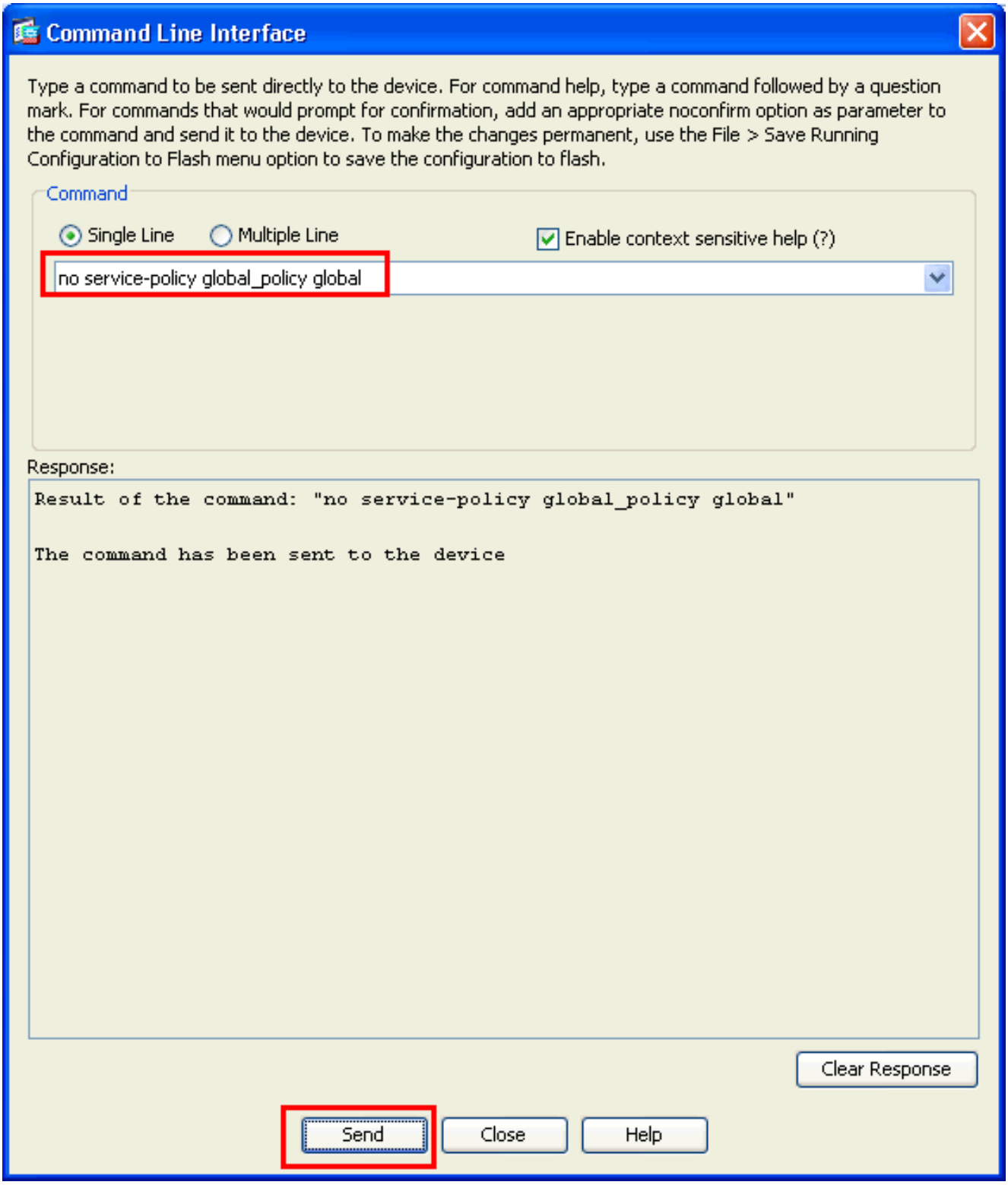
Cisco ASA에서 기본이 아닌 애플리케이션 검사를 활성화하려면 다음 절차를 완료합니다.

1. ASDM에 **로그인합니다**.Configuration(컨피그레이션) **> Firewall(방화벽) > Service Policy Rules(서비스 정책 규칙)로 이동합니다**



2. Default Class-map 및 Default Policy-map을 포함하는 전역 정책에 대한 컨피그레이션을 유지하지만 정책을 전역적으로 제거하려면 **Tools > Command Line Interface**로 이동하여 **no service-policy global-policy 전역** 명령을 사용하여 정책을 전역적으로 제거합니다.그런 다음 **Send**를 클릭하여 명령이 ASA에 적용되도록 합니다

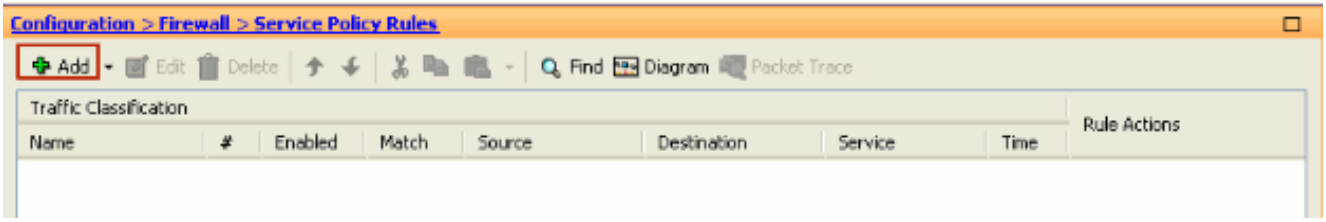
.



참고: 이 단계에서는 ASDM(Adaptive Security Device Manager)에서 전역 정책이 표시되지 않지만 CLI에 표시됩니다.

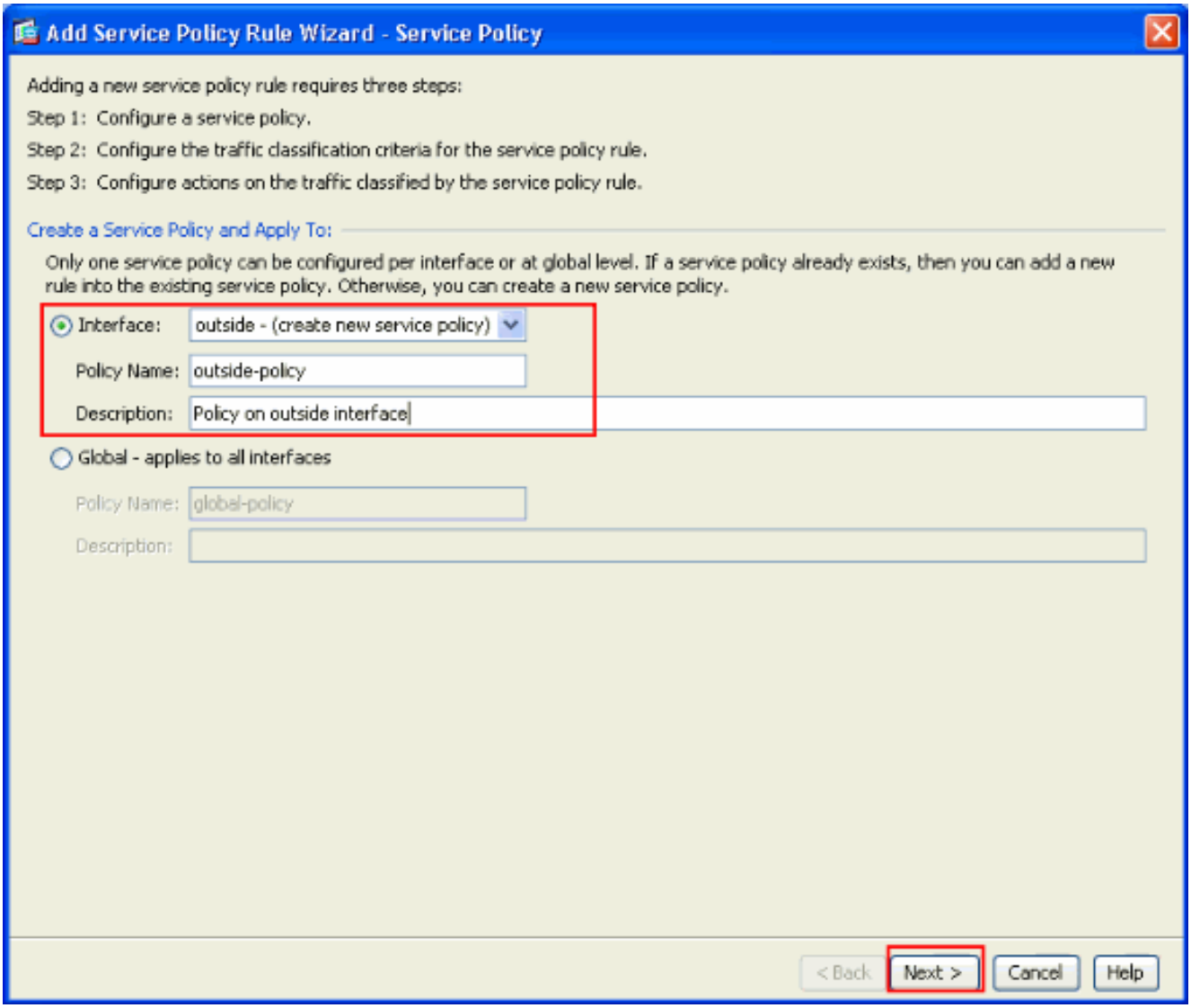
3. Add(**추가**)를 클릭하여 다음과 같이 새 정책을 추가합니다

.



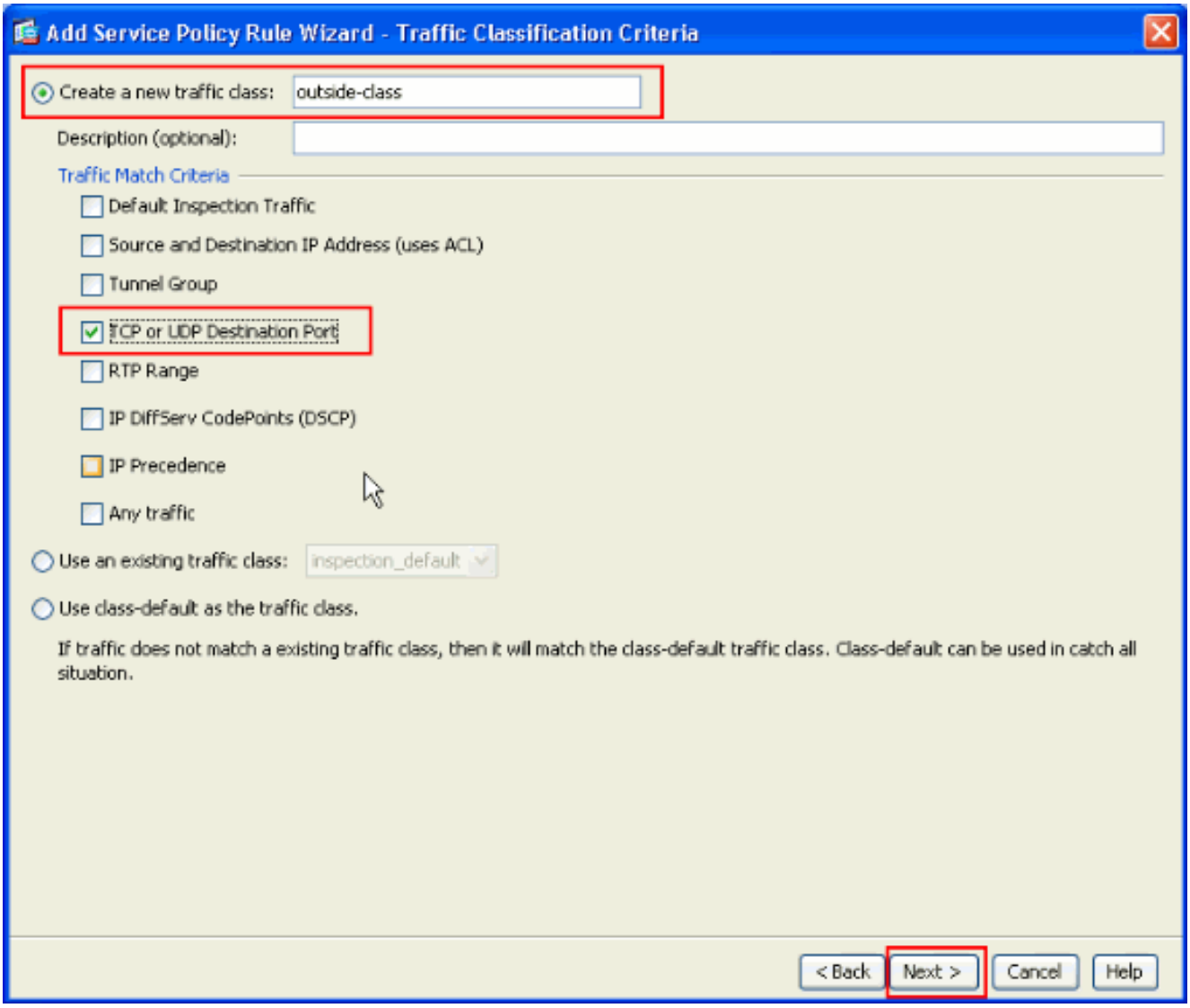
4. **Interface** 옆의 라디오 버튼이 선택되어 있는지 확인하고 드롭다운 메뉴에서 정책을 적용할 인터페이스를 선택합니다.그런 다음 **정책 이름**과 **설명**을 **입력합니다**.Next(**다음**)**를 클릭합니다**

.



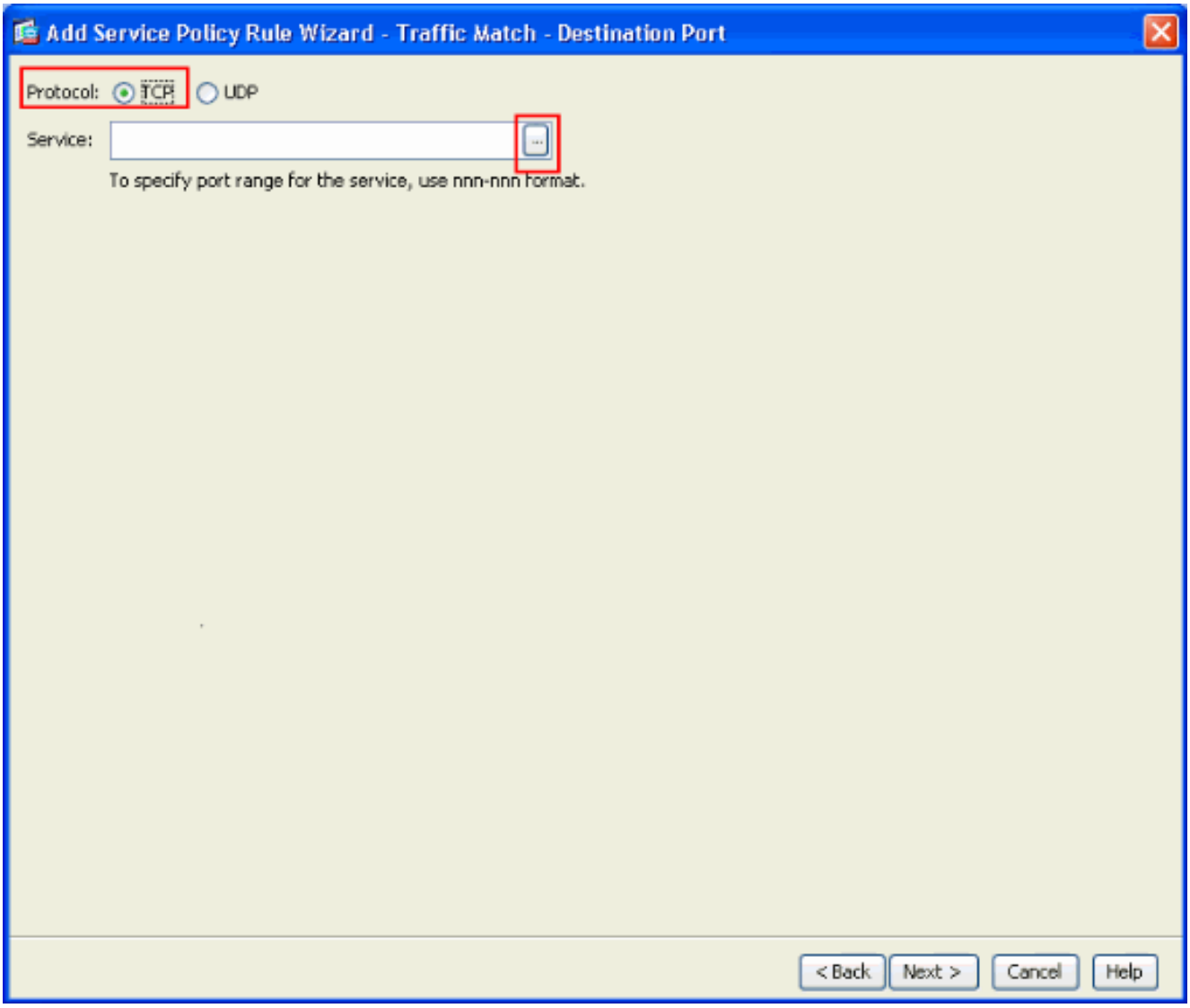
5. **HTTP**가 TCP에 속하는 **TCP** 트래픽과 매칭할 새 클래스 맵을 만듭니다.Next(**다음**)**를 클릭합니다**

.



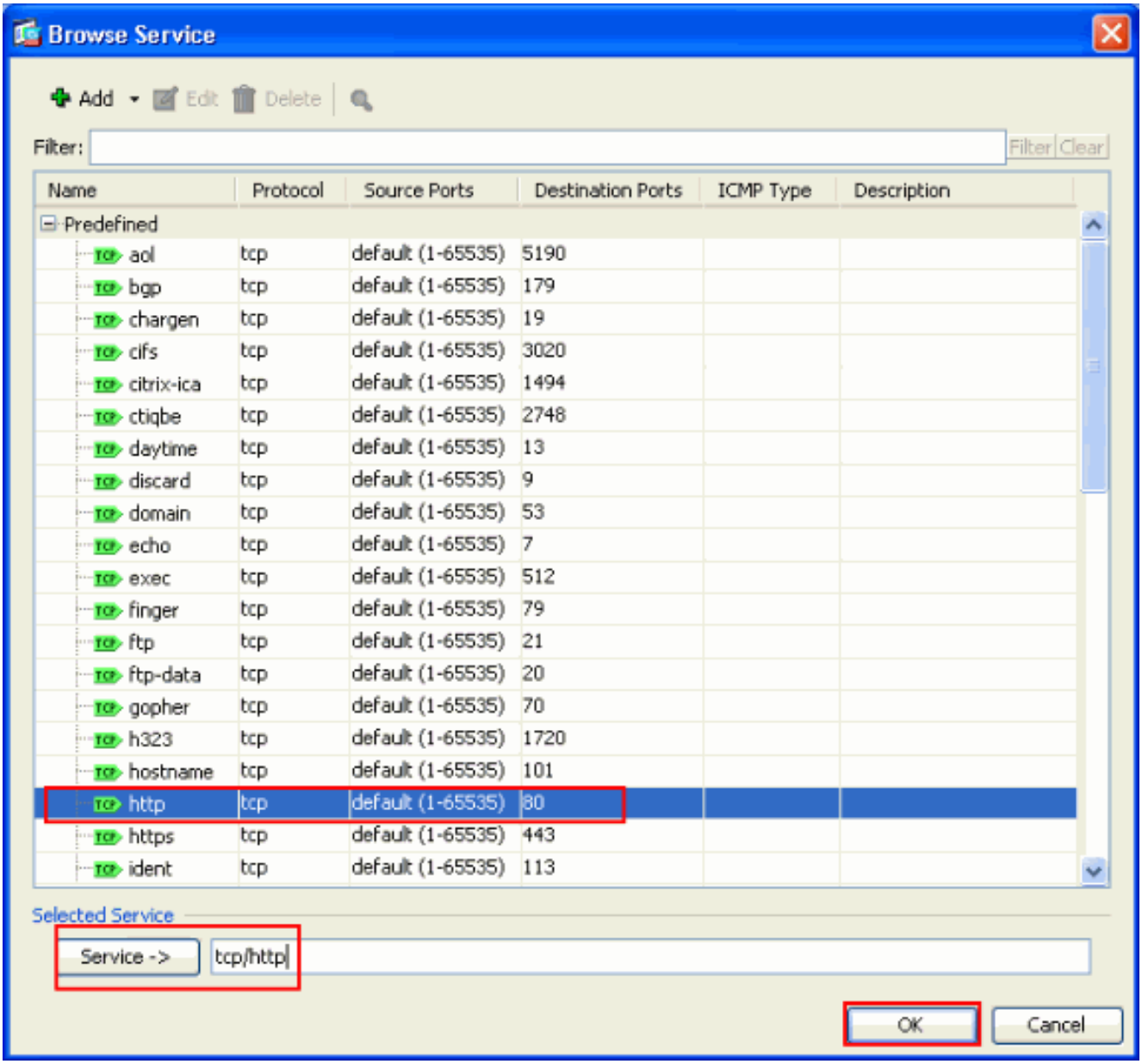
6. TCP를 프로토콜로 선택합니다

.



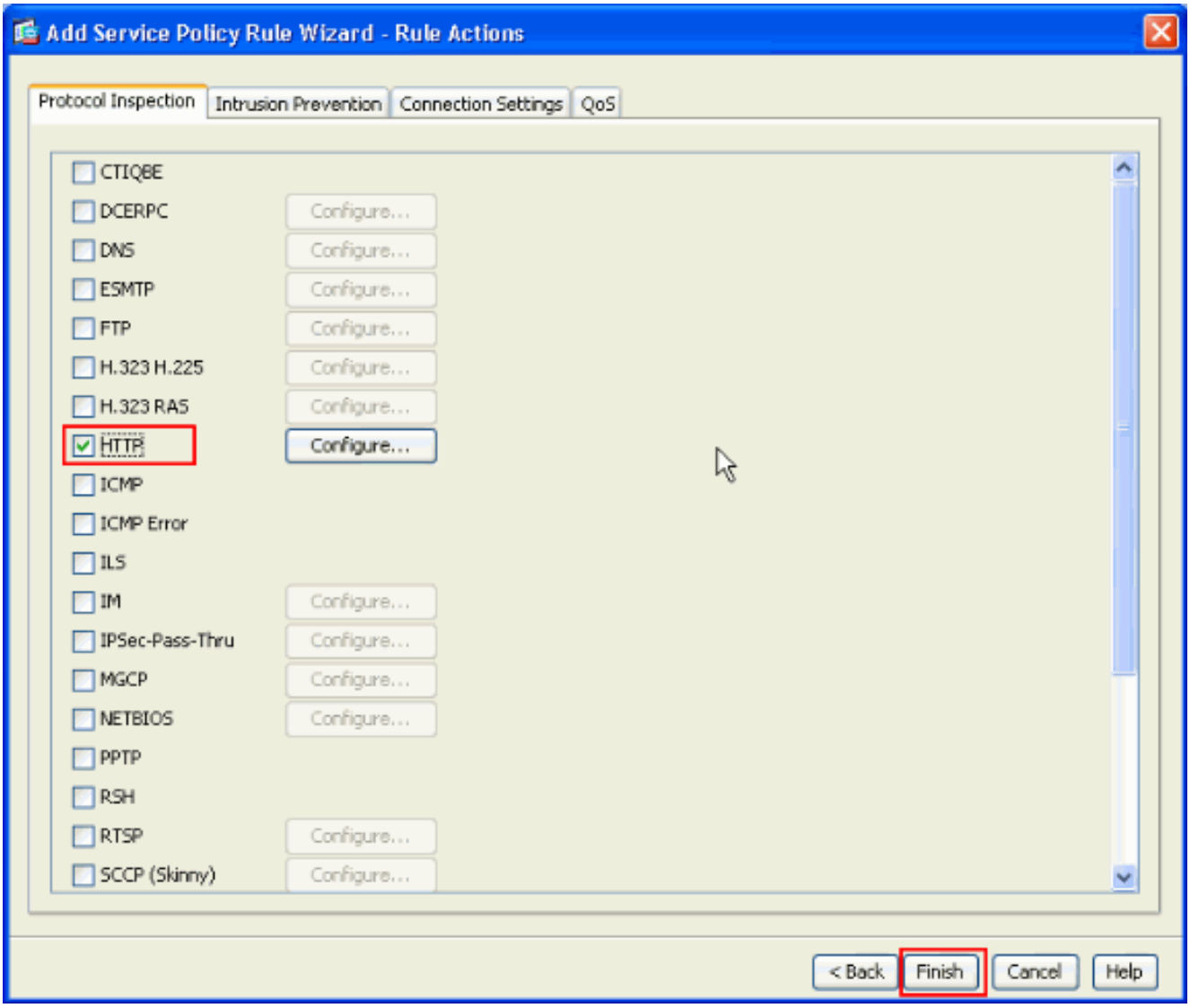
HTTP **포트 80을** 서비스로 선택하고 **OK**를 클릭합니다

.



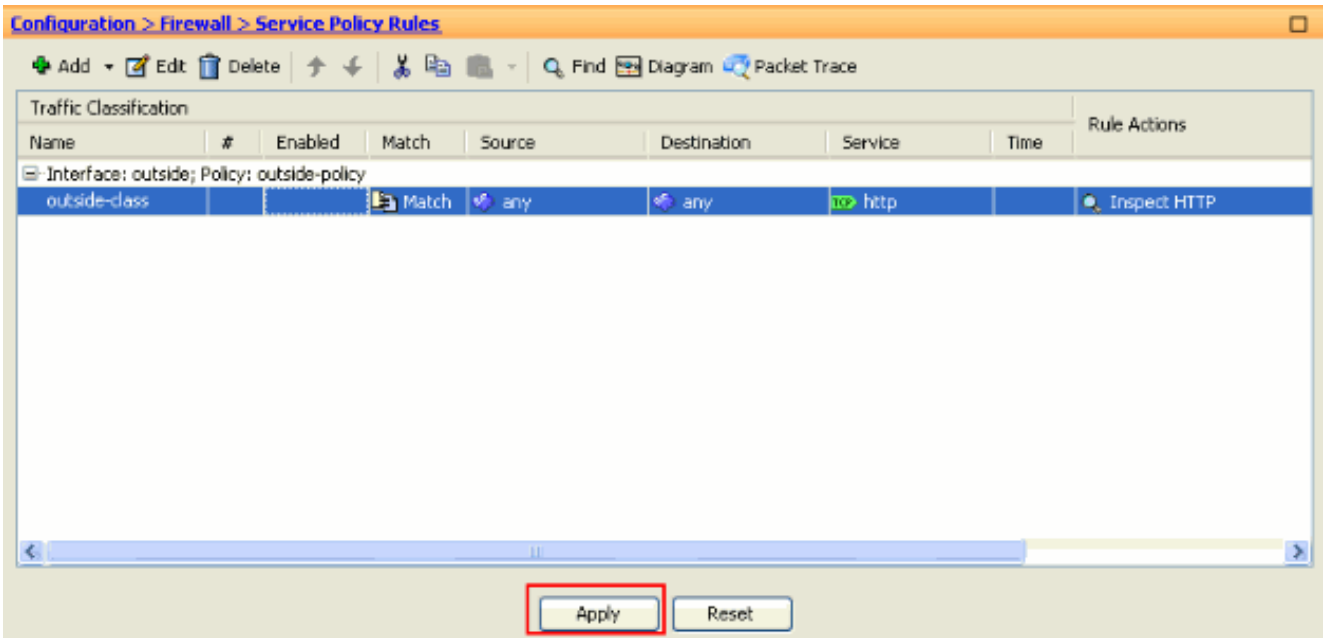
7. **HTTP**를 **선택하고** Finish(**마침**)를 클릭합니다

.



8. Apply(**적용**)를 클릭하여 ASDM에서 ASA로 컨피그레이션 변경 사항을 전송합니다.이렇게 하면 컨피그레이션이 완료됩니다

.



다음을 확인합니다.

다음 **show** 명령을 사용하여 컨피그레이션을 확인합니다.

- 구성된 **클래스 맵을** 보려면 show run class-map 명령을 사용합니다.
```
ciscoasa# sh run class-map
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class
match port tcp eq www
!
```
- 구성된 **정책 맵을** 보려면 show run policy-map 명령을 사용합니다.
```
ciscoasa# sh run policy-map
!
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 rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
policy-map outside-policy
 description Policy on outside interface
 class outside-class
  inspect http
!
```
- 구성된 서비스 정책을 보려면 **show run service-policy** 명령을 사용합니다.
```
ciscoasa# sh run service-policy
service-policy outside-policy interface outside
```

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco ASA 5500 Series 명령 참조
- Cisco ASDM(Adaptive Security Device Manager) 지원 페이지
- Cisco PIX 방화벽 소프트웨어
- RFC(Request for Comments)
- Cisco PIX 500 Series 보안 어플라이언스
- 애플리케이션 레이어 프로토콜 검사 적용
- Cisco Secure PIX Firewall 명령 참조
- 기술 지원 및 문서 – Cisco Systems