ASA 8.3 이상 - ASDM을 사용하여 검사 구성

목차

소개

이 문서에서는 애플리케이션에 대한 전역 정책에서 기본 검사를 제거하는 방법 및 ASDM(Adaptive Security Device Manager)을 사용하여 기본 이외의 애플리케이션에 대한 검사를 활성화하는 방법에 대해 버전 8.3(1) 이상의 Cisco ASA(Adaptive Security Appliance)에 대한 샘플 컨피그레이션을 제공합니다.

PIX/ASA 7.X 참조: 버전 8.2 이하의 Cisco ASA에서 동일한 컨피그레이션에 대해 Default Global Inspection을 비활성화하고 Enable Non-Default Application Inspection을 활성화합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 ASDM 6.3이 포함된 Cisco ASA Security Appliance Software 버전 8.3(1)을 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.

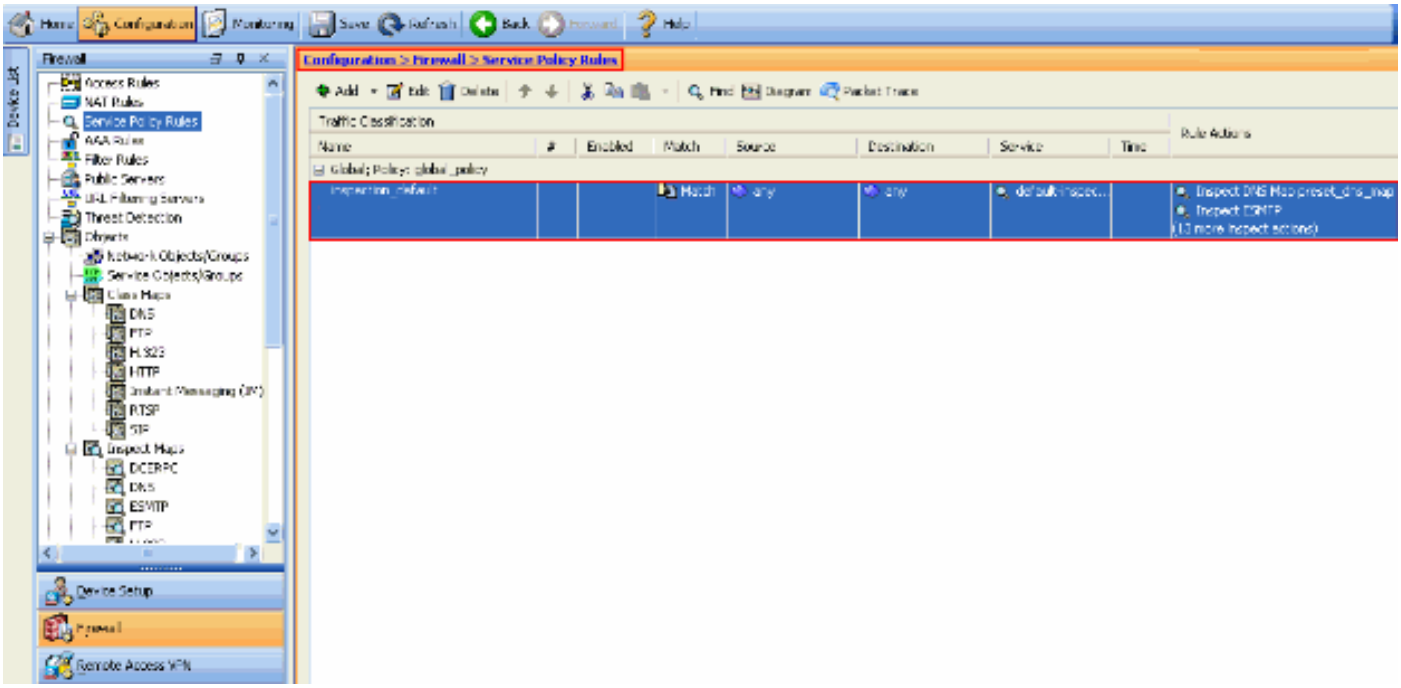
표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

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.)

ASDM에서 Configuration(컨피그레이션) **> Firewall(방화벽) > Service Policy Rules(서비스 정책 규칙)**를 선택하여 기본 애플리케이션 검사가 있는 기본 전역 정책을 다음과 같이 확인합니다.

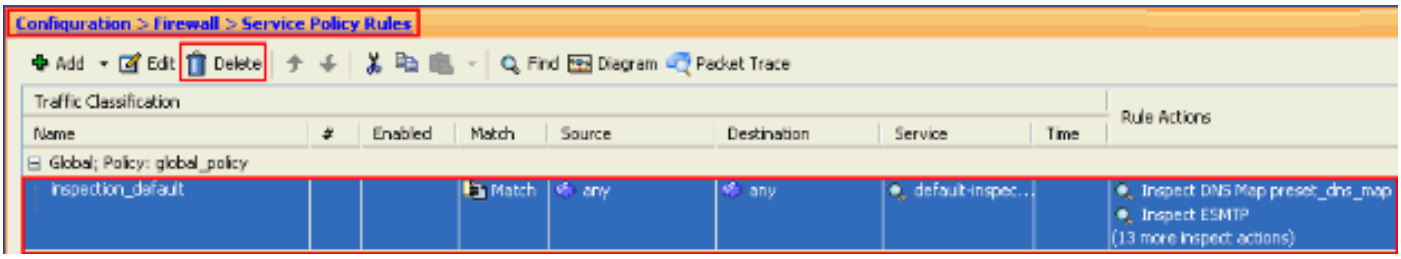


기본 정책 컨피그레이션에는 다음 명령이 포함됩니다.

```
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
```

전역 정책을 비활성화해야 하는 경우 **no service-policy global_policy 전역** 명령을 사용합니다.

ASDM을 사용하여 전역 정책을 삭제하려면 Configuration(컨피그레이션) **> Firewall(방화벽) > Service Policy Rules(서비스 정책 규칙)를 선택합니다**. 그런 다음 전역 정책을 선택하고 Delete(**삭제**)를 클릭합니다.



참고: ASDM을 사용하여 서비스 정책을 삭제하면 관련 정책 및 클래스 맵이 삭제됩니다. 그러나 CLI를 사용하여 서비스 정책을 삭제하면 서비스 정책만 인터페이스에서 제거됩니다. 클래스 맵 및 정책 맵은 변경되지 않습니다.

응용 프로그램에 대한 기본 전역 검사 비활성화

응용 프로그램에 대한 전역 검사를 비활성화하려면 inspect 명령의 *no* 버전을 사용합니다.

예를 들어, 보안 어플라이언스가 수신 대기하는 FTP 애플리케이션에 대한 전역 검사를 제거하려면 클래스 컨피그레이션 모드에서 **no inspect ftp** 명령을 사용합니다.

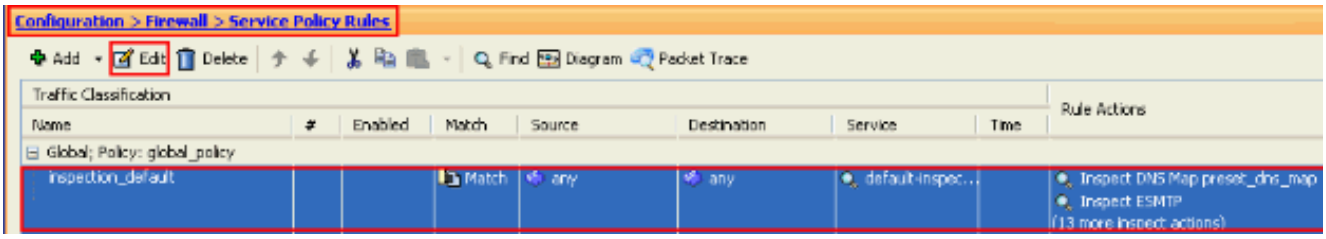
클래스 컨피그레이션 모드는 정책 맵 컨피그레이션 모드에서 액세스할 수 있습니다. 컨피그레이션을 제거하려면 이 명령의 *no* 형식을 사용합니다.

```
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#no inspect ftp
```

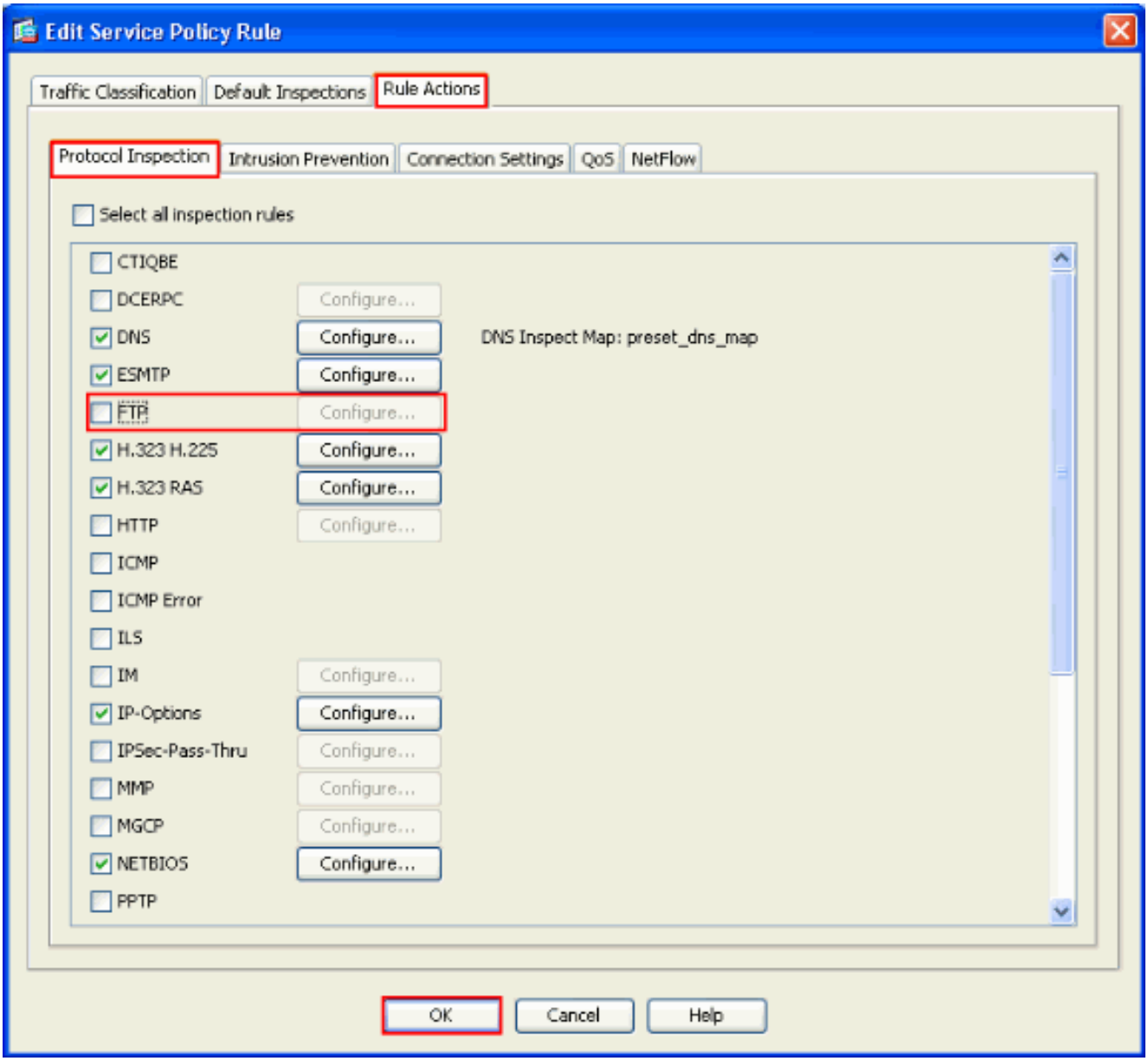
ASDM을 사용하여 FTP에 대한 전역 검사를 비활성화하려면 다음 단계를 완료하십시오.

참고: ASDM을 통해 PIX/ASA에 액세스하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

1. Configuration **> Firewall > Service Policy Rules**를 선택하고 기본 전역 정책을 선택합니다. 그런 다음 **Edit(편집)**를 클릭하여 전역 검사 정책을 편집합니다



2. Edit Service Policy Rule(서비스 정책 규칙 수정) 창의 Rule Actions(**규칙 작업**) 탭 아래에 **Protocol Inspection(프로토콜 검사)을** 선택합니다. **FTP** 확인란이 선택되지 않았는지 확인합니다. 그러면 다음 이미지에 표시된 대로 FTP 검사가 비활성화됩니다. 그런 다음 **확인**을 클릭하고 **적용 을 클릭합니다**



참고: FTP 검사에 대한 자세한 내용은 PIX/ASA 7.x: FTP/TFTP 서비스 컨피그레이션 예를 활성화합니다.

기본 응용 프로그램이 아닌 응용 프로그램에 대한 검사 사용

고급 HTTP 검사는 기본적으로 비활성화되어 있습니다. global_policy에서 HTTP 검사를 활성화하려면 class inspection_default 아래에서 **inspect http** 명령을 사용합니다.

이 예에서는 모든 인터페이스를 통해 보안 어플라이언스에 들어가는 모든 HTTP 연결(포트 80의 TCP 트래픽)이 HTTP 검사를 위해 분류됩니다. *정책은 전역 정책이므로 트래픽이 각 인터페이스에 들어갈 때만 검사가 발생합니다.*

```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

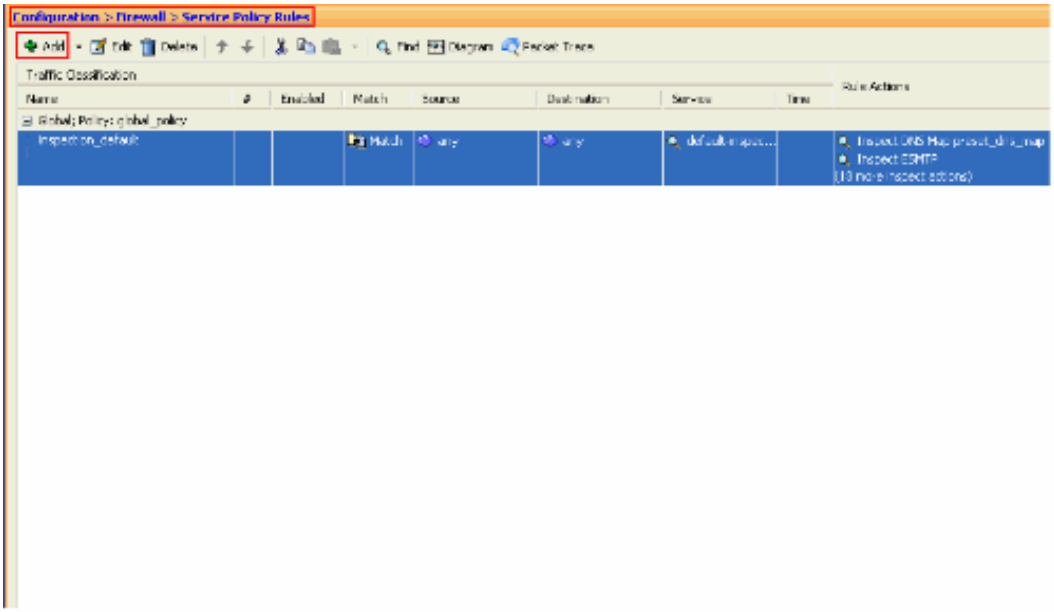
이 예에서는 *외부 인터페이스*를 통해 보안 어플라이언스를 드나드는 HTTP 연결(포트 80의 TCP 트래픽)이 *HTTP 검사를 위해 분류됩니다.*

```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

ASDM을 사용하여 위의 예를 구성하려면 다음 단계를 수행합니다.

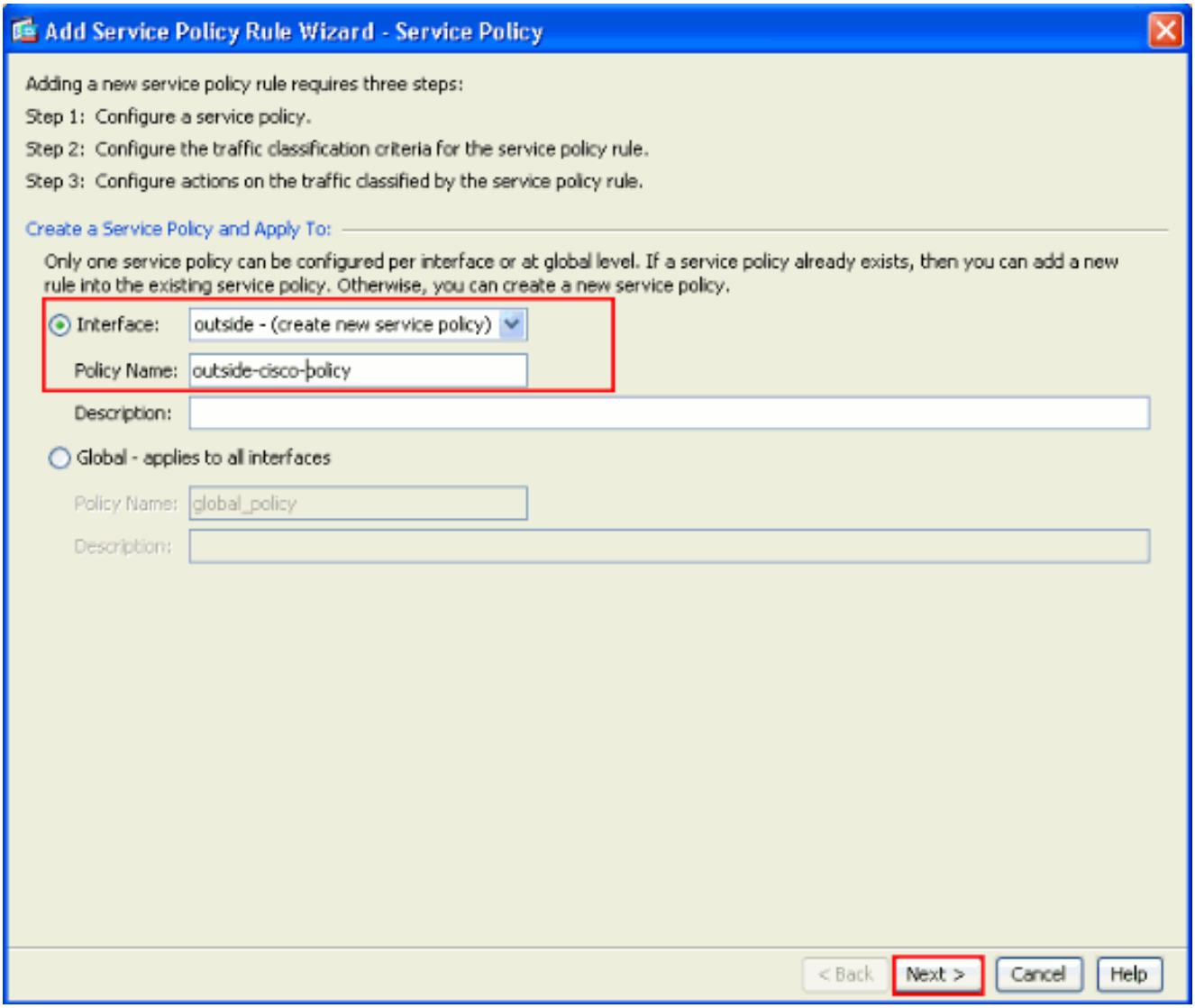
1. Configuration(**컨피그레이션**) > **Firewall(방화벽)** > **Service Policy Rules(서비스 정책 규칙)**를 선택하고 **Add(추가)**를 클릭하여 새 서비스 정책을 추가합니다

.



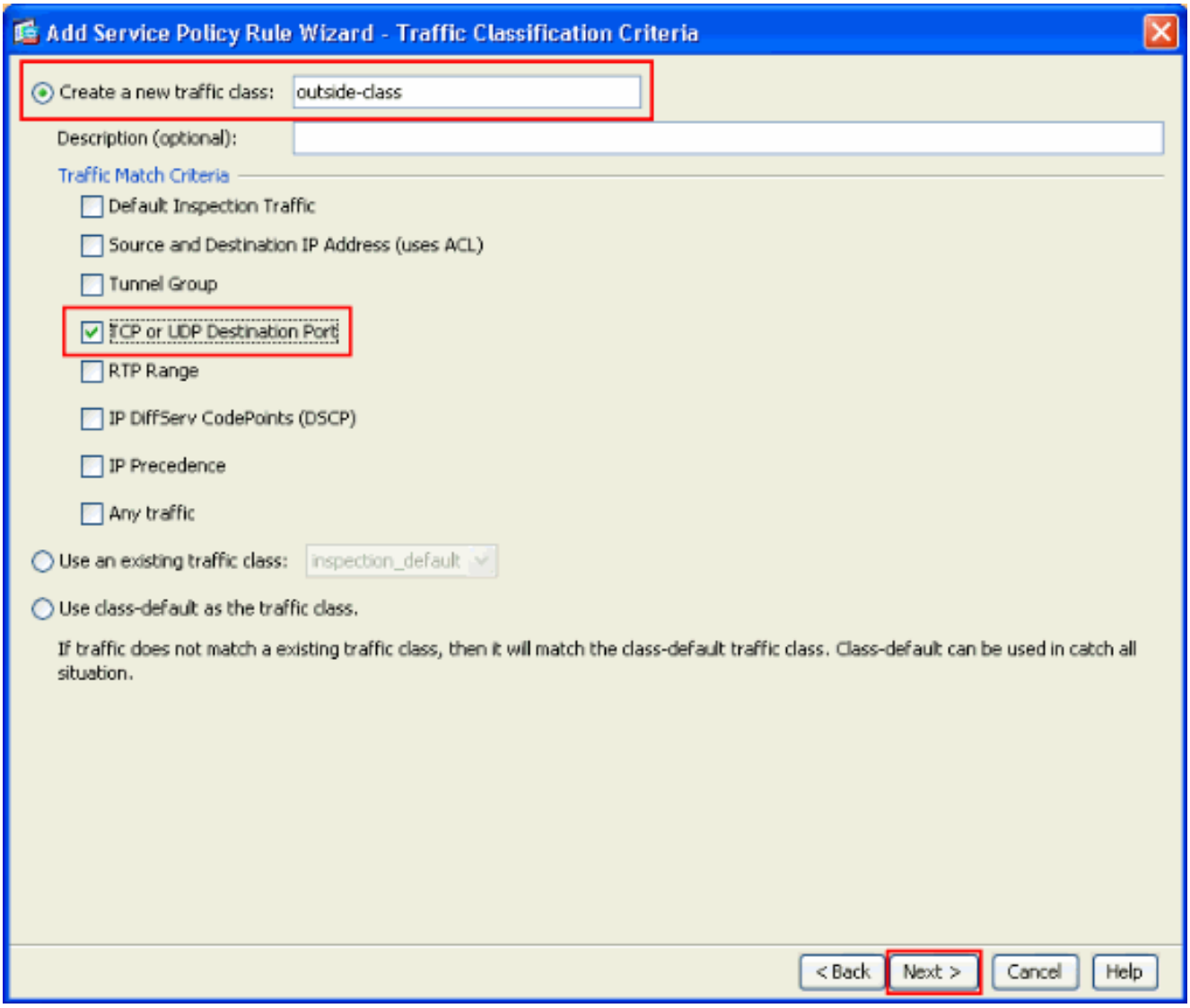
2. Add Service Policy Rule Wizard - Service Policy(서비스 정책 추가 마법사 - 서비스 정책) 창에서 **Interface** 옆의 라디오 버튼을 선택합니다. 이렇게 하면 특정 인터페이스에 생성된 정책이 적용됩니다. 이 인터페이스는 **외부** 인터페이스입니다. 이 예에서 **outside-cisco-policy**인 정책 이름을 입력합니다. Next(**다음**)**를 클릭합니다**

.

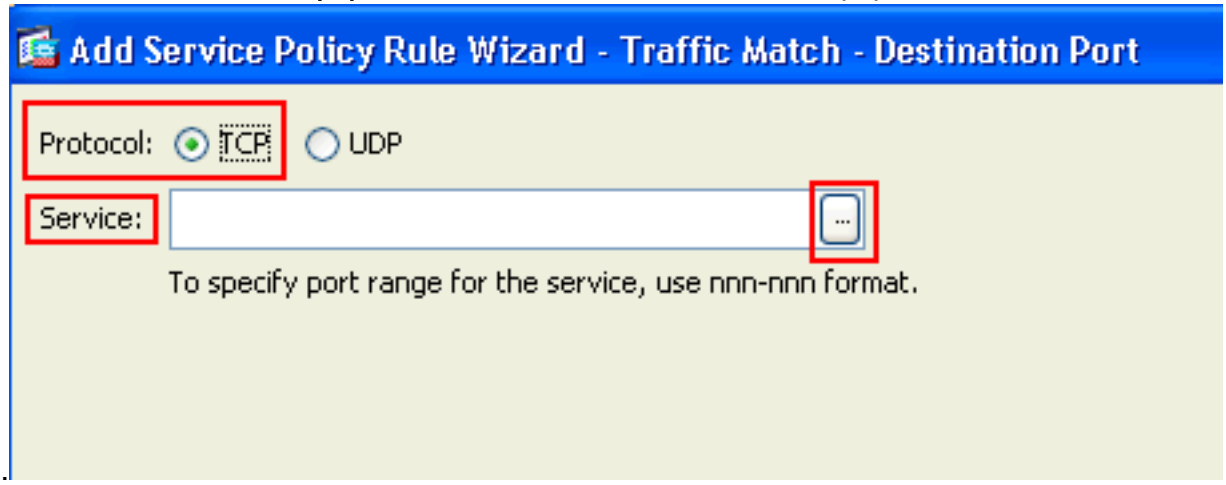


3. Add Service Policy Rule Wizard - Traffic Classification Criteria 창에서 새 트래픽 클래스 이름을 제공합니다. 이 예에서 사용되는 이름은 **outside-class입니다**. **TCP 또는 UDP Destination Port** 옆의 확인란이 선택되었는지 확인하고 **Next**(다음)를 클릭합니다

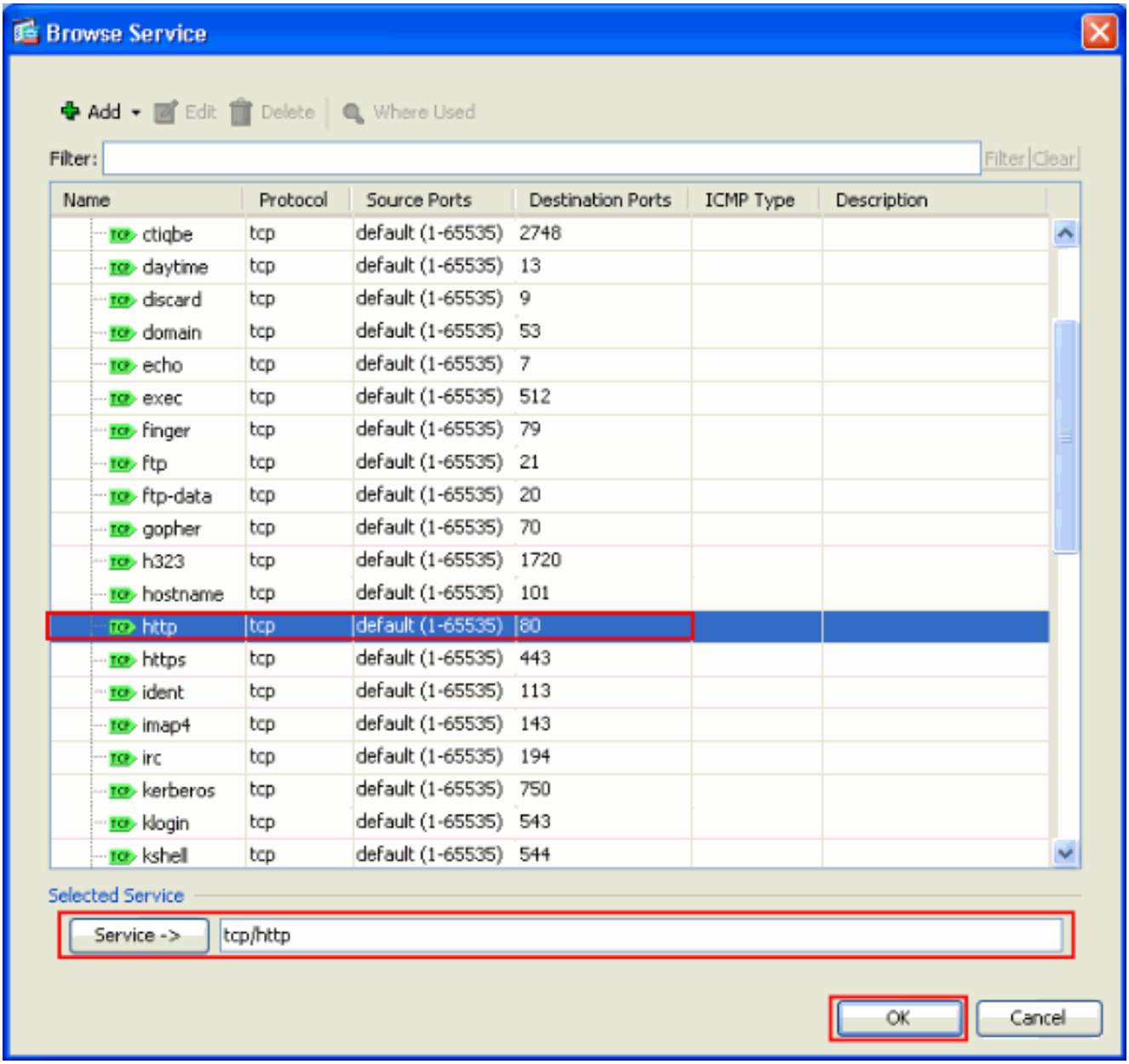
.



4. Add Service Policy Rule Wizard - Traffic Match - Destination Port(서비스 정책 규칙 추가 마법사 - 트래픽 매치 - 대상 포트) 창에서 Protocol(프로토콜) 섹션에서 **TCP** 옆의 라디오 버튼을 선택합니다. 그런 다음 **서비스** 옆의 버튼을 클릭하여 필요한 서비스를 선택합니다

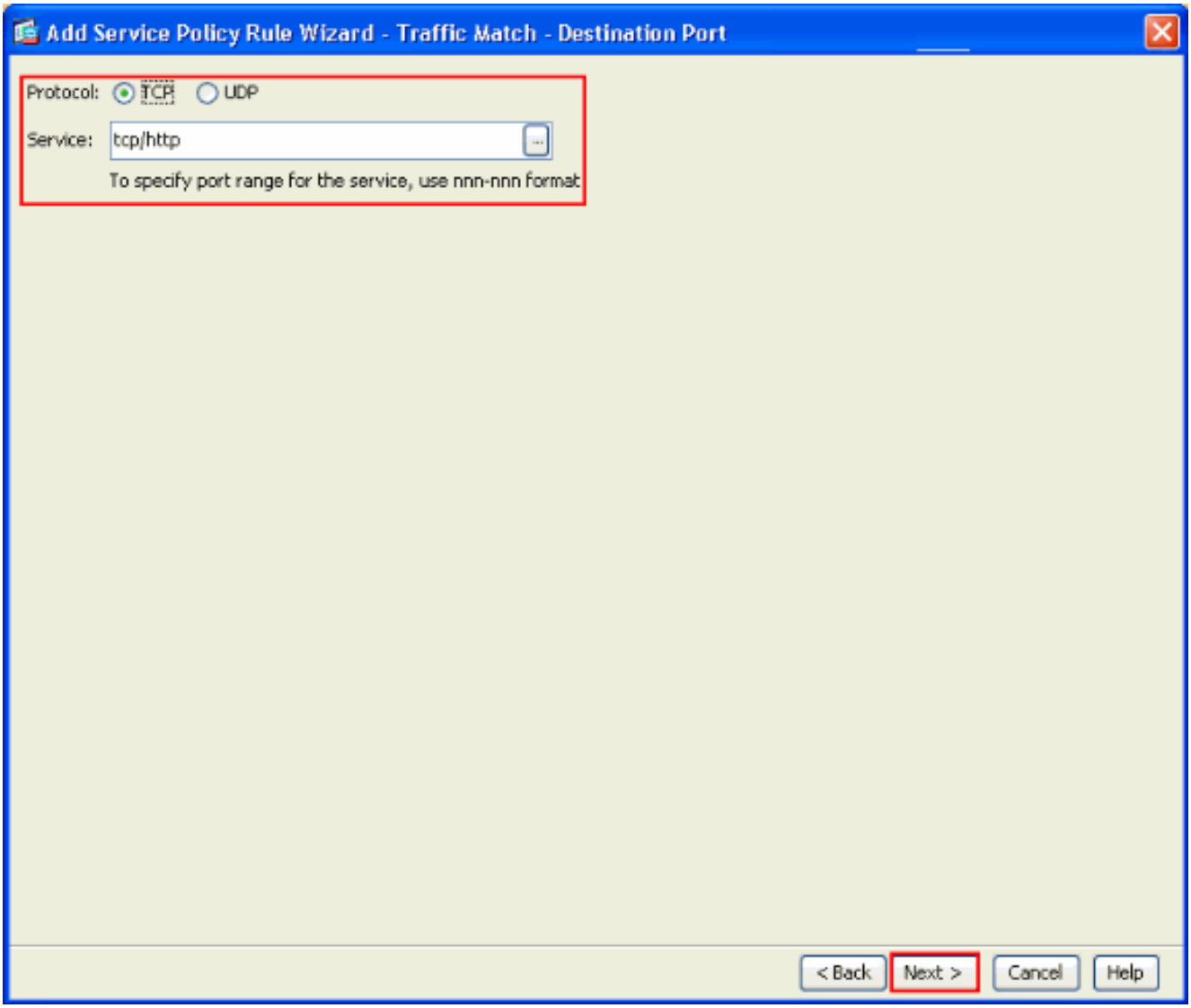


5. Browse Service(서비스 찾아보기) 창에서 **HTTP**를 서비스로 선택합니다. 그런 다음 **확인**을 클릭합니다

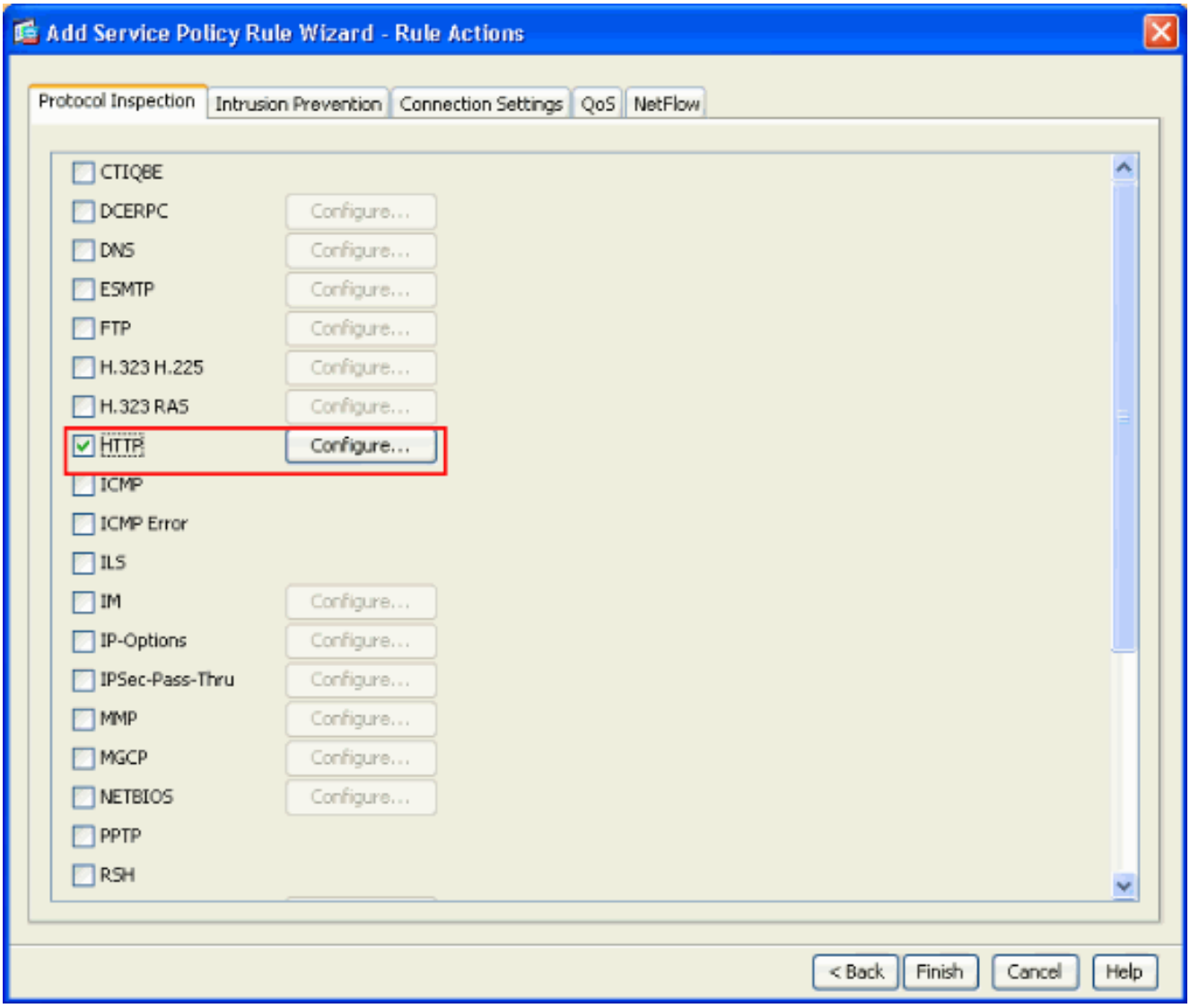


6. Add Service Policy Rule Wizard - Traffic Match - Destination Port(서비스 정책 규칙 추가 마법사 - 트래픽 일치 - 대상 포트) 창에서 선택한 **서비스**가 **tcp/http**임을 확인할 수 있습니다. Next(**다음)를 클릭합니다**

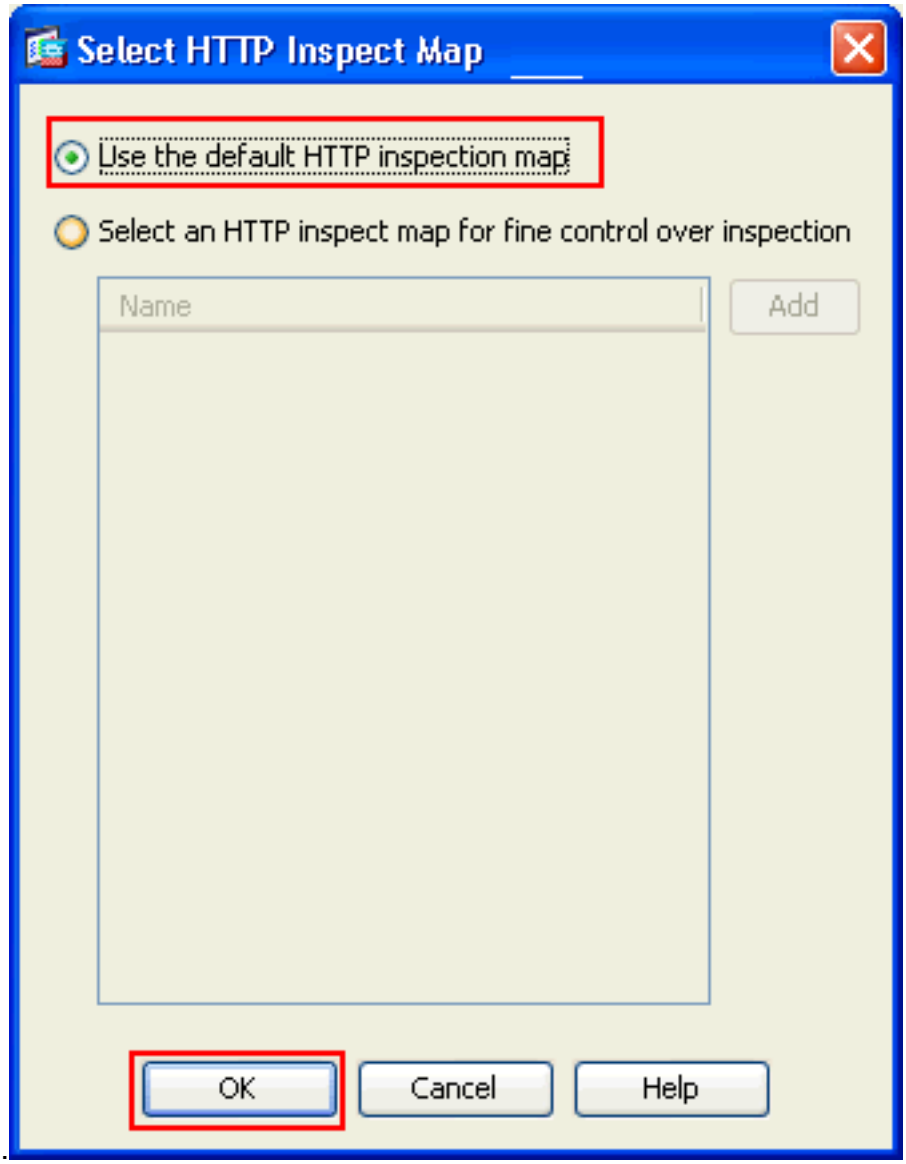
.



7. Add Service Policy Rule Wizard - Rule Actions(서비스 정책 규칙 추가 마법사 - 규칙 작업) 창에서 **HTTP** 옆의 확인란을 선택합니다. 그런 다음 **HTTP 옆에 있는 Configure**를 클릭합니다 .

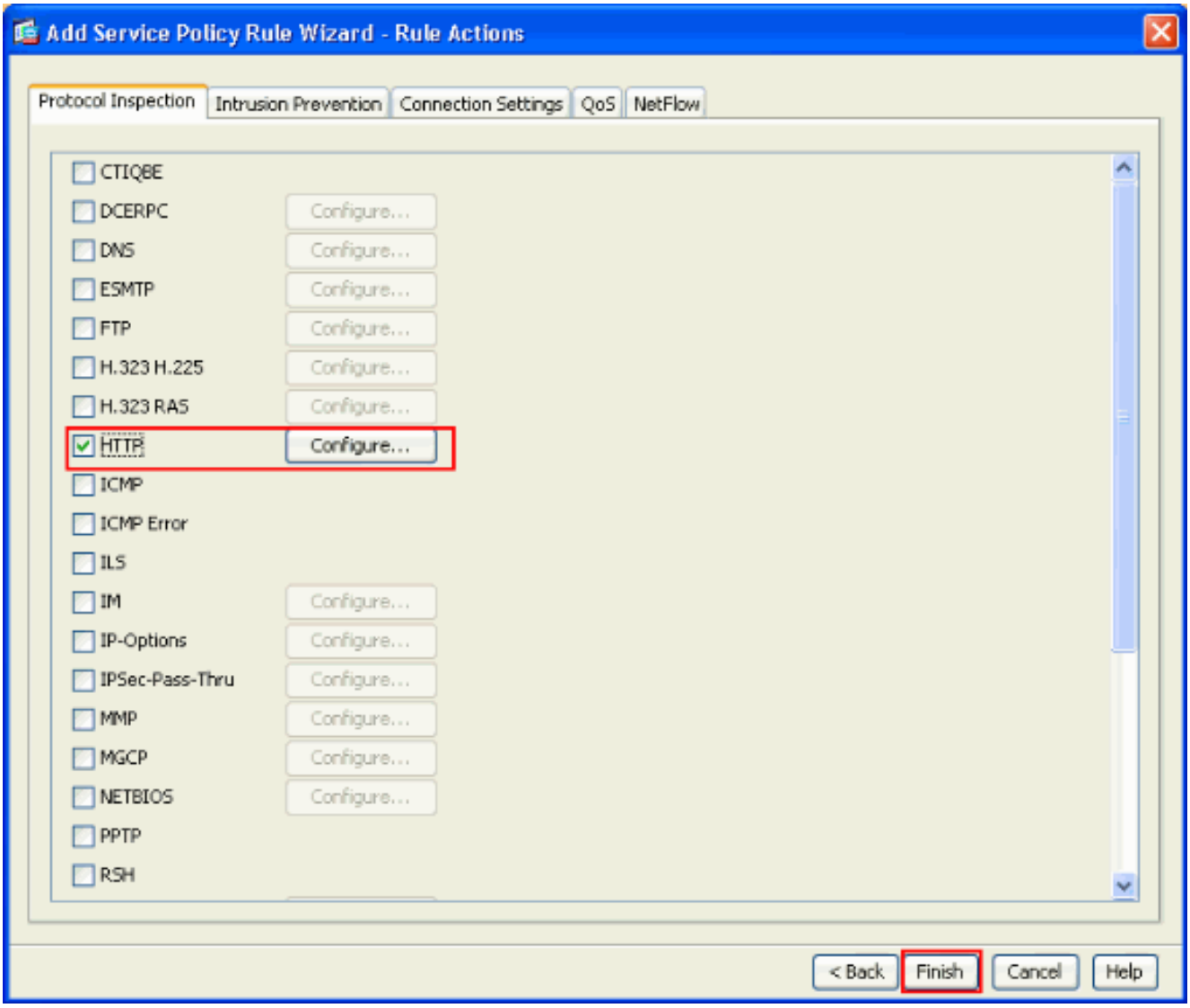


8. Select HTTP Inspect Map(HTTP 검사 맵 선택) 창에서 Use the Default **HTTP inspection map(기본 HTTP 검사 맵 사용)** 옆의 라디오 버튼**을 선택합니다**. 이 예에서는 기본 HTTP 검사가 사용됩니다. 그런 다음 **확인**을 클릭합니다


Select HTTP Inspect Map
Use the default HTTP inspection map
Select an HTTP inspect map for fine control over inspection
Name
Add
OK
Cancel
Help

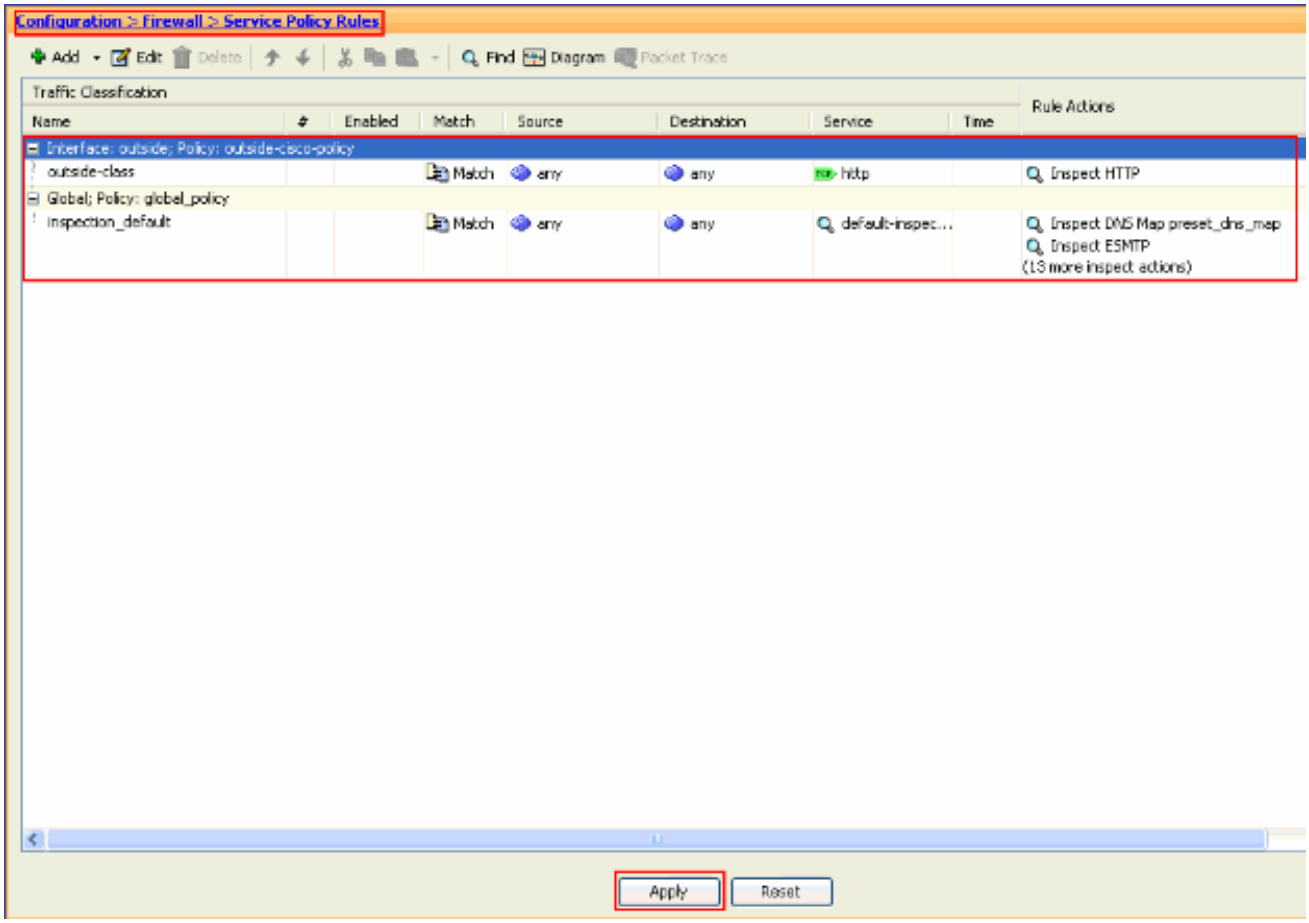
9. 마침을 클릭합니다

.



10. Configuration(**컨피그레이션) > Firewall(방화벽) > Service Policy Rules(서비스 정책 규칙**)에서 새로 구성된 서비스 정책 **outside-cisco-policy**(HTTP 검사를 위해)가 어플라이언스에 이미 있는 기본 서비스 정책과 함께 표시됩니다. Cisco ASA에 컨피그레이션을 적용하려면 Apply를 클릭합니다

.



관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- Cisco Adaptive Security Device Manager
- RFC(Request for Comments)
- 애플리케이션 레이어 프로토콜 검사 적용
- 기술 지원 및 문서 – Cisco Systems