# ASA 8. 3 и Позже: Отключите Глобальный Контроль По умолчанию и Включите Контроль приложения Ня по умолчанию с помощью ASDM

## Содержание



## Введение

Этот документ предоставляет пример конфигурации для устройства адаптивной защиты Cisco (ASA) с версиями 8.3 (1) и позже как удалить контроль по умолчанию из глобальной политики для приложения и как включить контроль для приложения ня по умолчанию с помощью Менеджера устройств адаптивной безопасности (ASDM) (ASDM).

Подробное описание настройки сети VPN на базе IPSec между двумя узлами в устройстве защиты Cisco с версией ПО 7.x см. в документе PIX/ASA 7.x: Отключите Глобальный Контроль По умолчанию и Включите Контроль приложения Ня по умолчанию для одинаковой конфигурации на Cisco ASA с версиями 8.2 и ранее.

## Предварительные условия

### Требования

Для этого документа отсутствуют особые требования.

### Используемые компоненты

Сведения в этом документе основываются на Версии программного обеспечения 8.3 (1) Устройства безопасности Cisco ASA с ASDM 6.3.

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

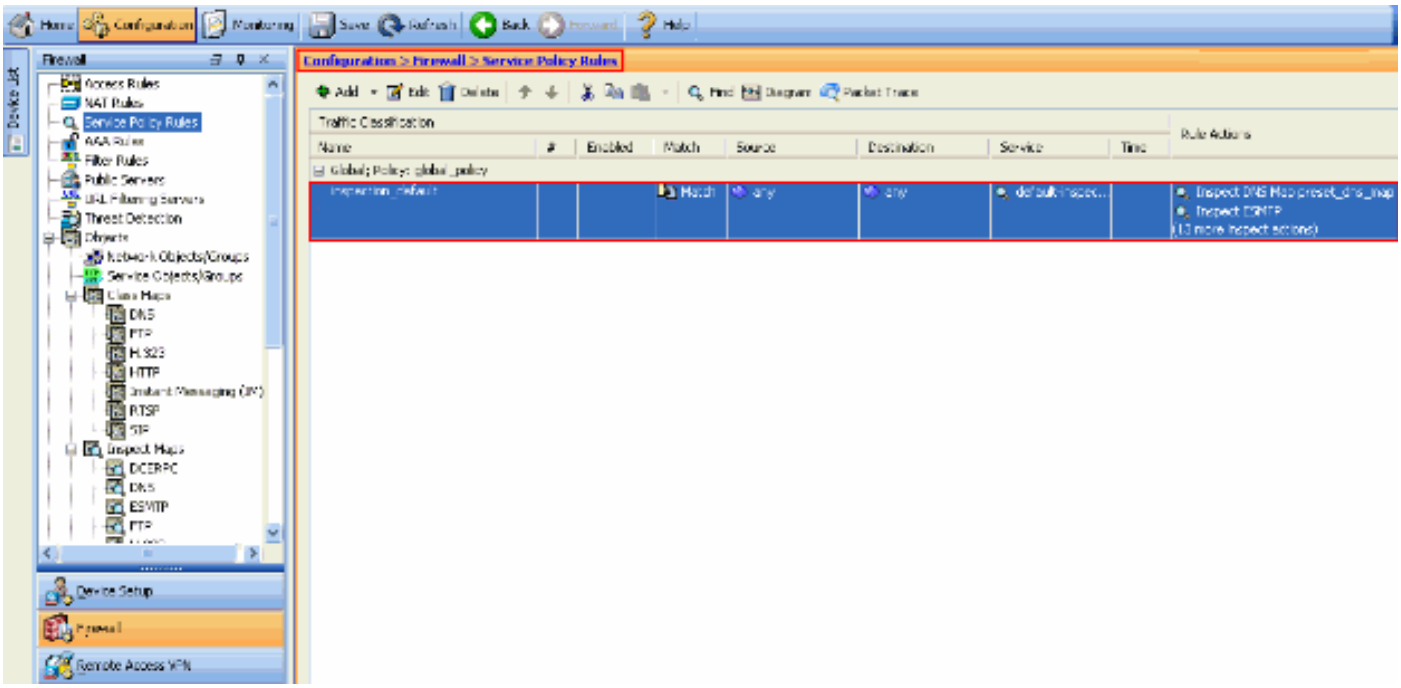
## Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

# Глобальная политика по умолчанию

По умолчанию в конфигурацию включается политика, соотносящая весь трафик проверок приложений, заданных по умолчанию, и применяющая определенные виды анализа для трафика на всех интерфейсах (глобальная политика). По умолчанию включены не все виды анализа. Применять можно только одну глобальную политику. Чтобы изменить глобальную политику, необходимо либо отредактировать политику по умолчанию, либо отключить ее и ввести в действие новую политику. (Политика интерфейса заменяет собой глобальную политику.).)

В ASDM выберите **Configuration> Firewall> Service Policy Rules** для просмотра глобальной политики по умолчанию, которая имеет контроль приложения по умолчанию как показано здесь:

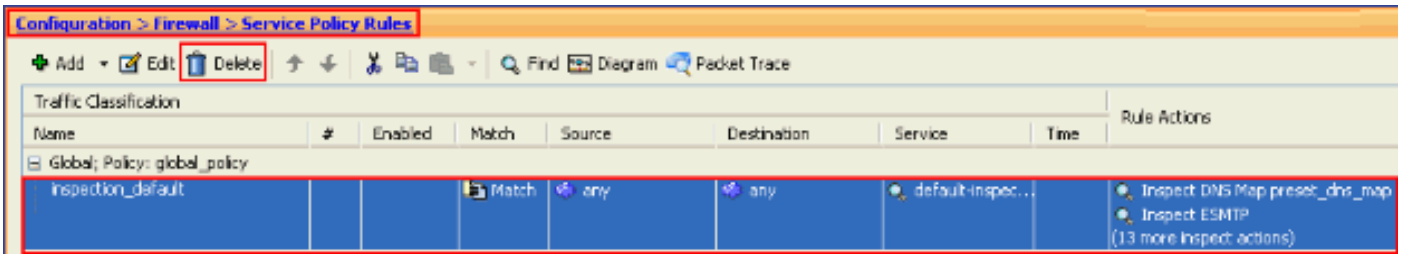



Конфигурация политики по умолчанию содержит следующие команды:

```
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
```

Если необходимо отключить глобальную политику, используйте **команду no service-policy global_policy global**. Для удаления глобальной политики с помощью ASDM, выбирают **Configuration> Firewall> Service Policy Rules**. Затем выберите глобальную политику и нажмите **Delete**.




**Примечание:** При удалении политики обслуживания с ASDM связанная политика и карты классов удалены. Однако, если политика обслуживания удалена с помощью CLI, только политика обслуживания удалена из интерфейса. Карта классов и карта политик остаются неизменными.

## Отключение глобального анализа по умолчанию для приложения

*Чтобы отключить глобальный анализ для приложения, используйте команду inspect с модификатором no.*

**Например, чтобы удалить глобальный анализ для приложения FTP, прослушиваемого устройством защиты, используйте команду no inspect ftp в режиме настройки класса.**

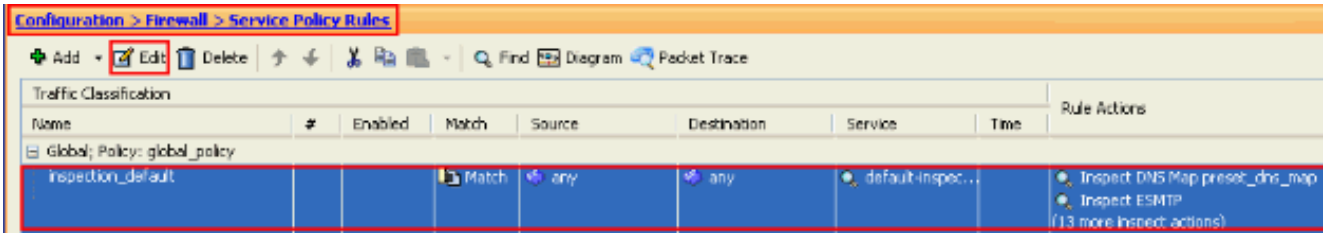
Режим настройки класса доступен из режима настройки карты политик. *Для удаления конфигурации используйте команду с модификатором no.*

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

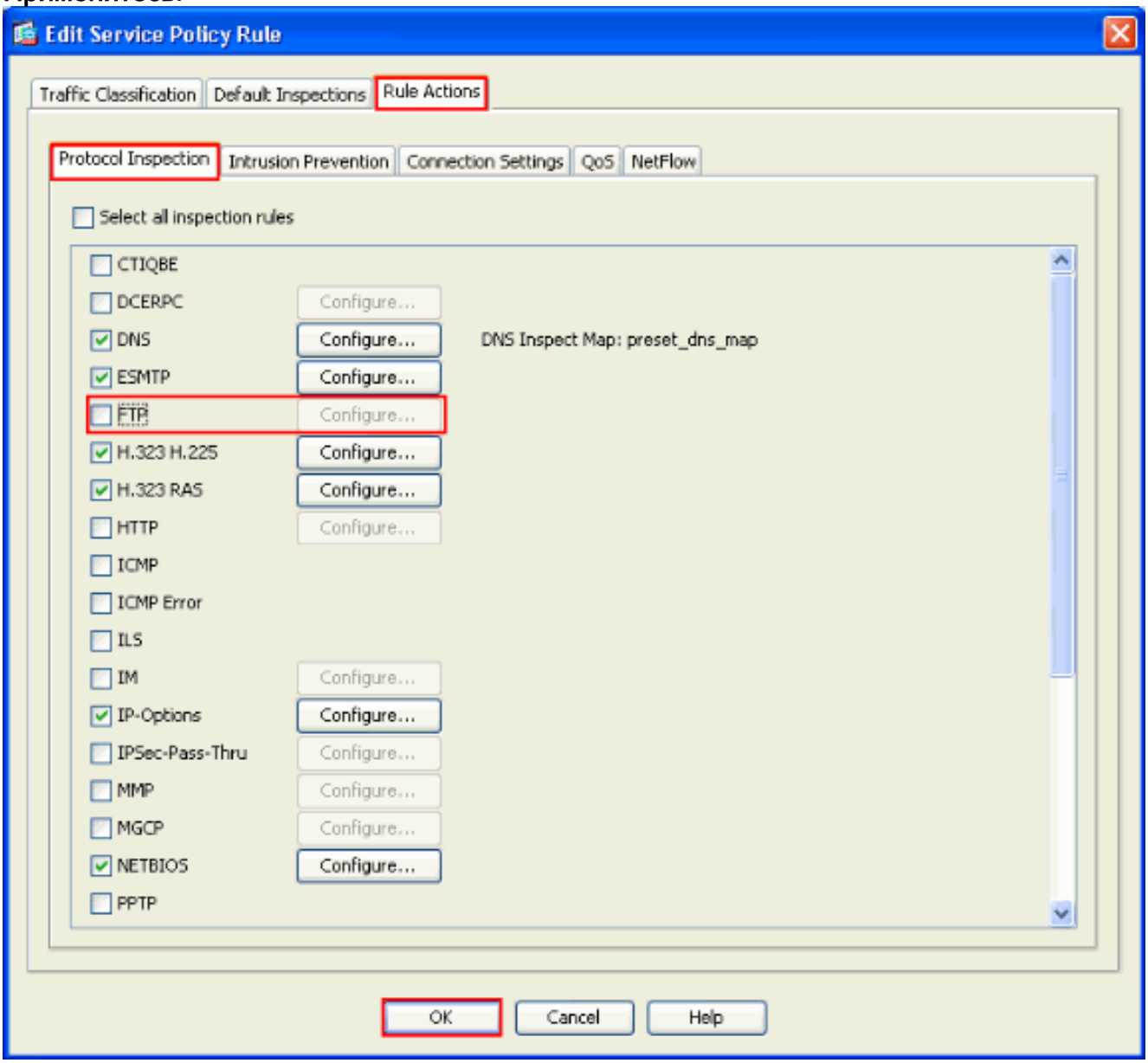
Для отключения глобального контроля для FTP с помощью ASDM выполните эти шаги:

**Примечание:** См. документ Разрешение HTTPS-доступа для ASDM для базовых параметров для доступа к PIX/ASA через ASDM.

1. Выберите **Configuration> Firewall> Service Policy Rules** и выберите глобальную политику по умолчанию. Затем нажмите **Edit** для редактирования глобальной политики проверки.




2. Из окна Edit Service Policy Rule выберите **Protocol Inspection** под вкладкой **Rule Actions**. Удостоверьтесь, что неконтролируем флажок **FTP**. Это отключает контроль FTP как показано в следующем образе. Затем нажмите **OK** и затем **Применитесь**.




**Примечание:** Для получения дополнительной информации о контроле FTP обратитесь к PIX/ASA 7. x: Пример настройки служб FTP/TFTP.

## Включение анализа для приложений, отличных от приложения по умолчанию

Расширенный анализ HTTP по умолчанию отключен. Для включения Проверки HTTP в global_policy используйте **команду inspect http** под классом inspection_default.

В этом примере любое подключение по протоколу HTTP (трафик TCP на порту 80), входящее на устройство защиты через любой интерфейс, классифицируется для анализа

HTTP. *Поскольку политика является глобальной, то анализ действует только при вхождении трафика на каждый интерфейс.*

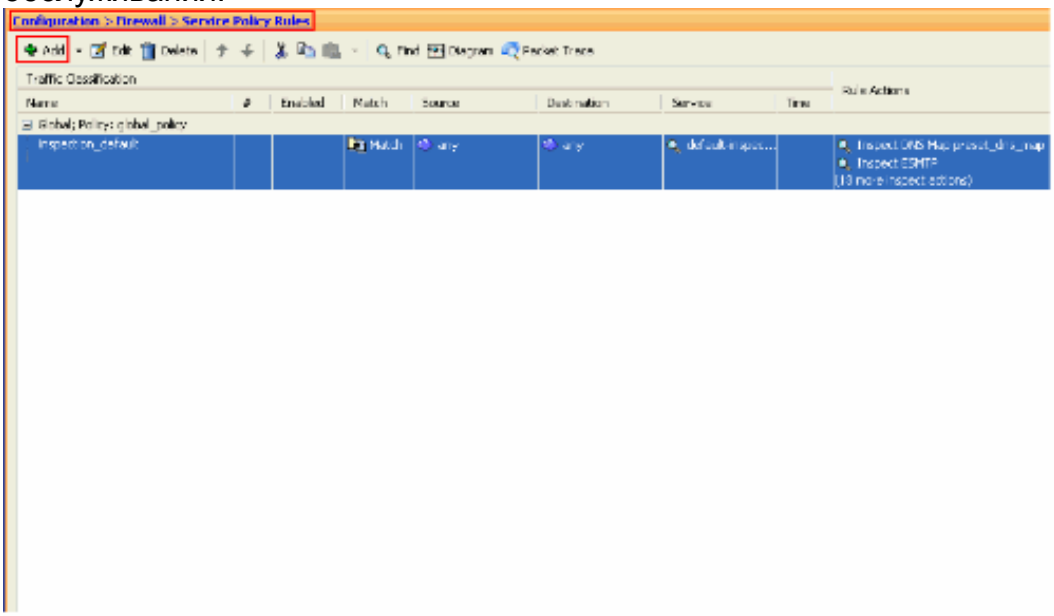
```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

*В этом примере любое подключение по протоколу HTTP (трафик TCP на порту 80), входящее на устройство защиты или выходящее из него через внешний интерфейс, классифицируется для анализа HTTP.*

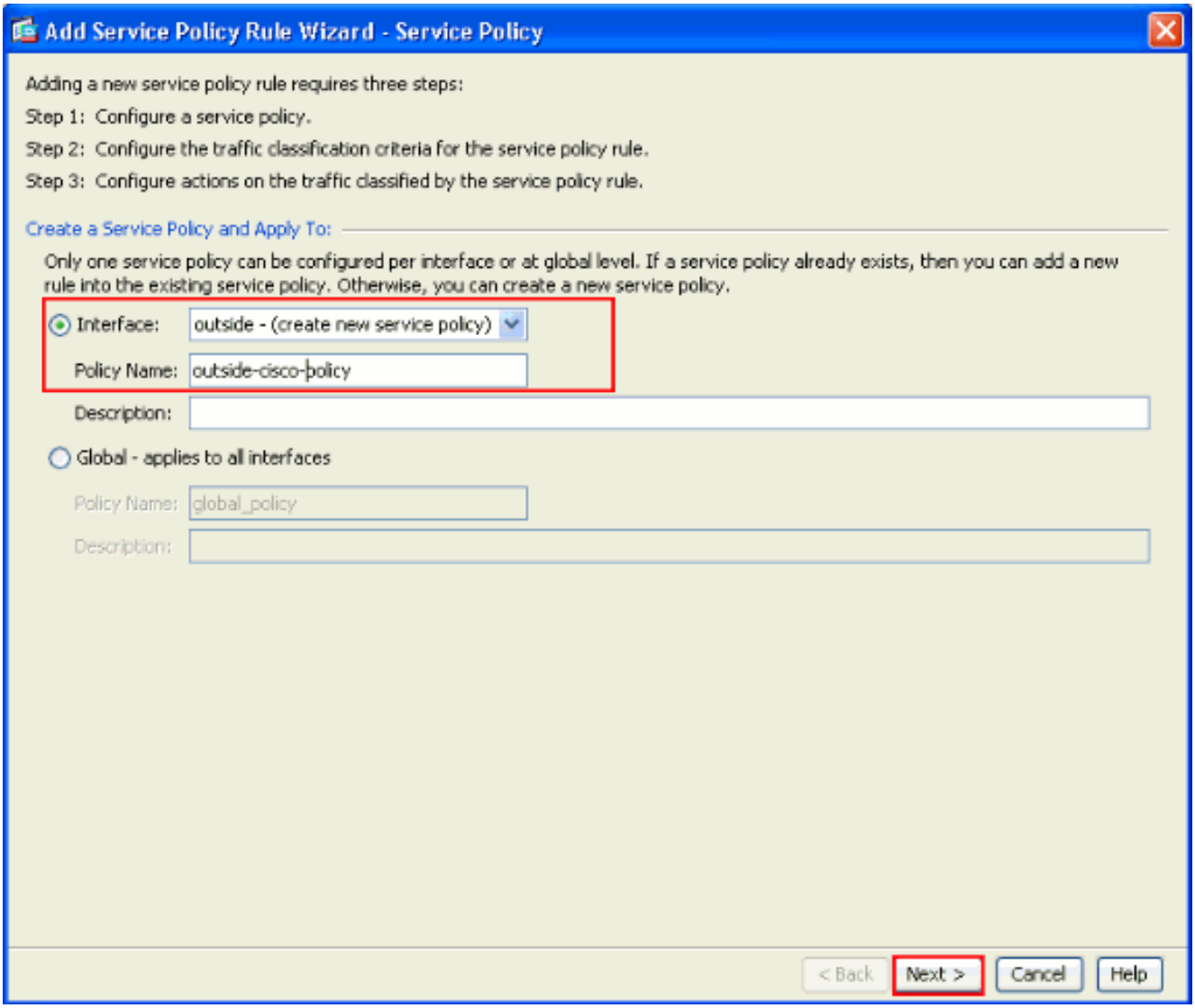
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

Выполните эти шаги для настройки вышеупомянутого примера с помощью ASDM:

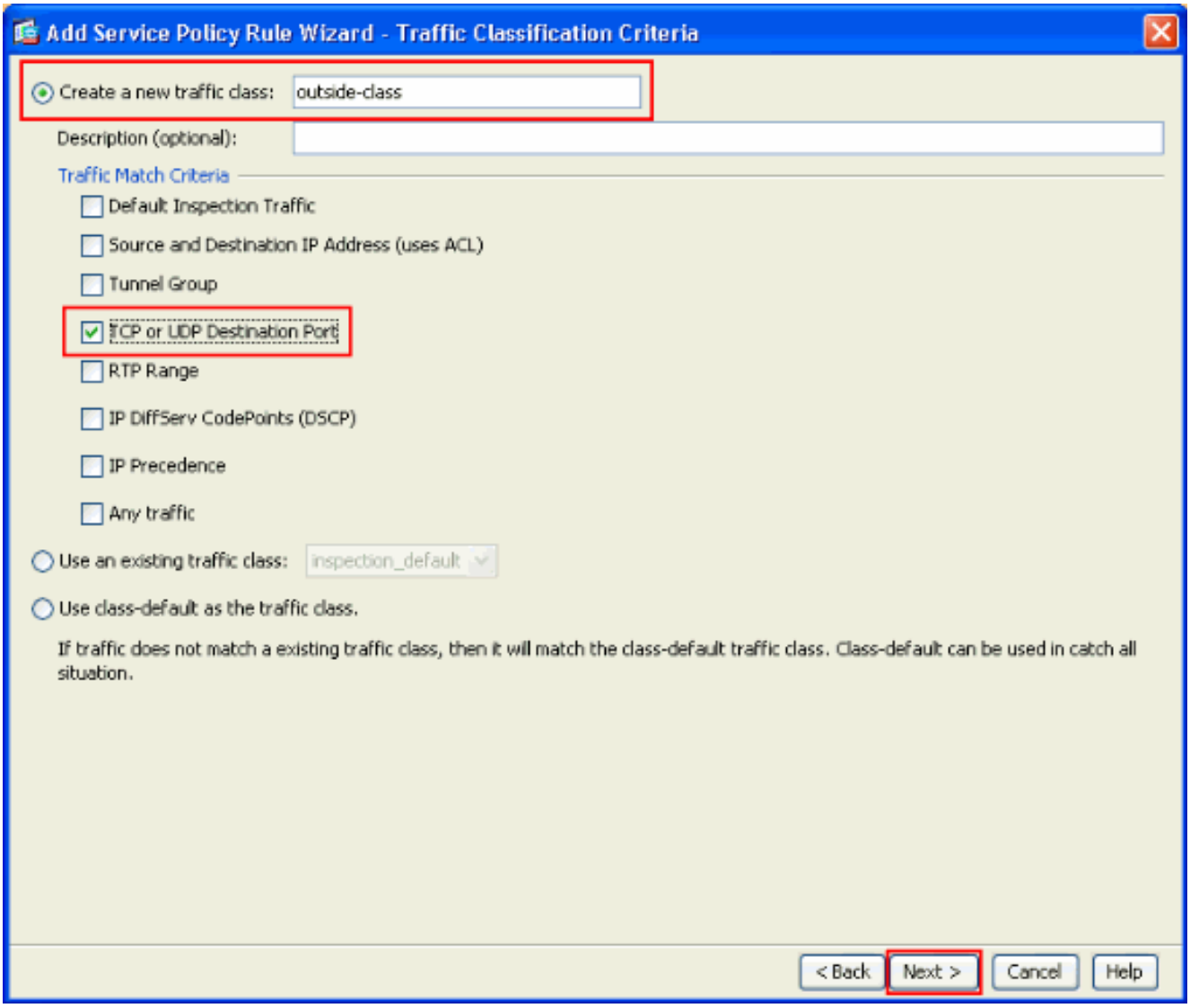
1. Выберите **Configuration> Firewall> Service Policy Rules** и **нажмите Add** для добавления новой политики обслуживания:



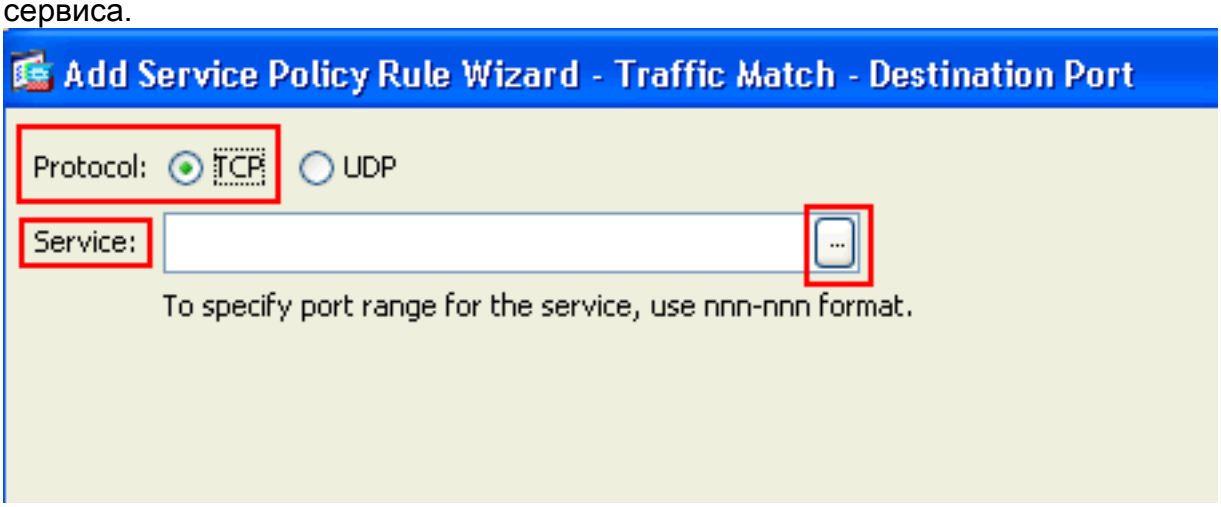
2. От добавьте сервис политика управляют мастером - сервисное Окно политики, выбирают кнопку с зависимой фиксацией, следующую за **Интерфейсом**. Это применяет политику, созданную к определенному интерфейсу, который является **Внешним интерфейсом** в данном примере. Предоставьте название политики, которое является **внешней политикой Cisco** в данном примере. **Нажмите кнопку Next.**



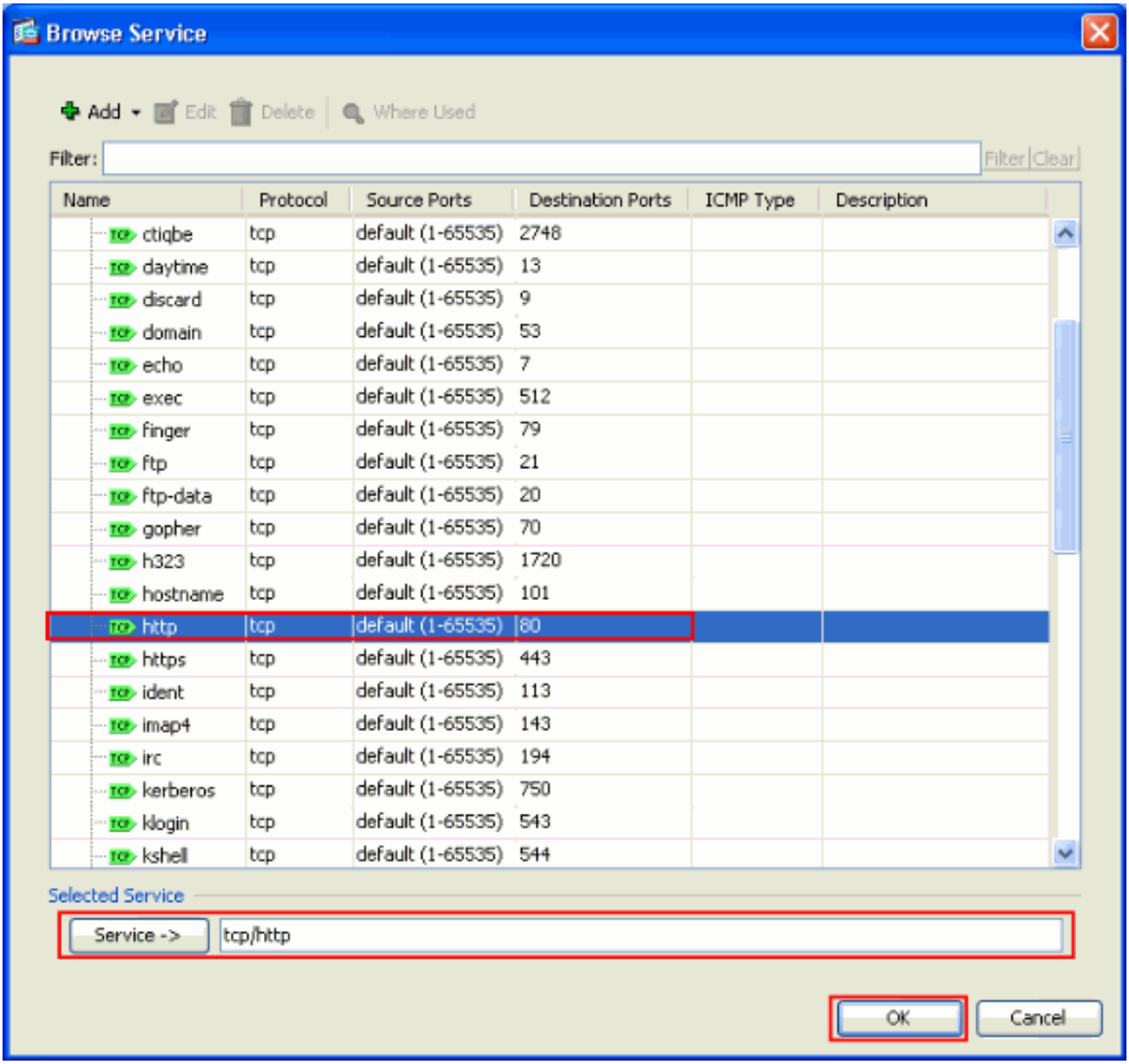

3. От добавьте сервис политика управляет мастером - окно критерии классификации трафиков, предоставляет новое название класса трафика. Название, используемое в данном примере, является **внешним классом**. Гарантируйте, что флажок, следующий за **TCP или портом Получателя UDP**, проверен, и нажмите **Next**.



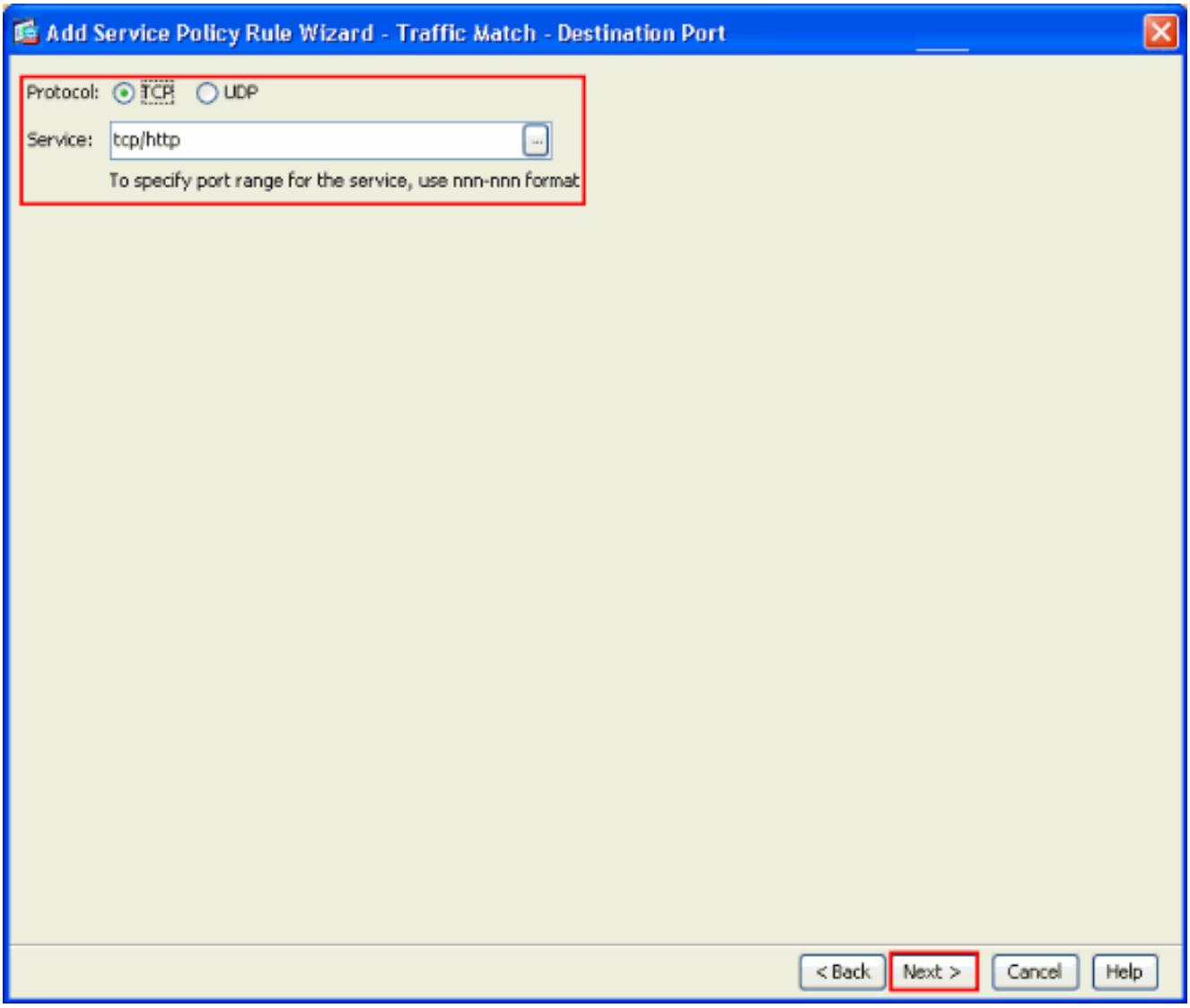

4. От Добавить Мастера Правила Политики обслуживания - Соответствия Трафика - окно Destination Port, выберите кнопку с зависимой фиксацией, следующую за **TCP** под **Разделом протокола**. Затем нажмите кнопку, следующую за **Сервисом** для выбора требуемого
сервиса.



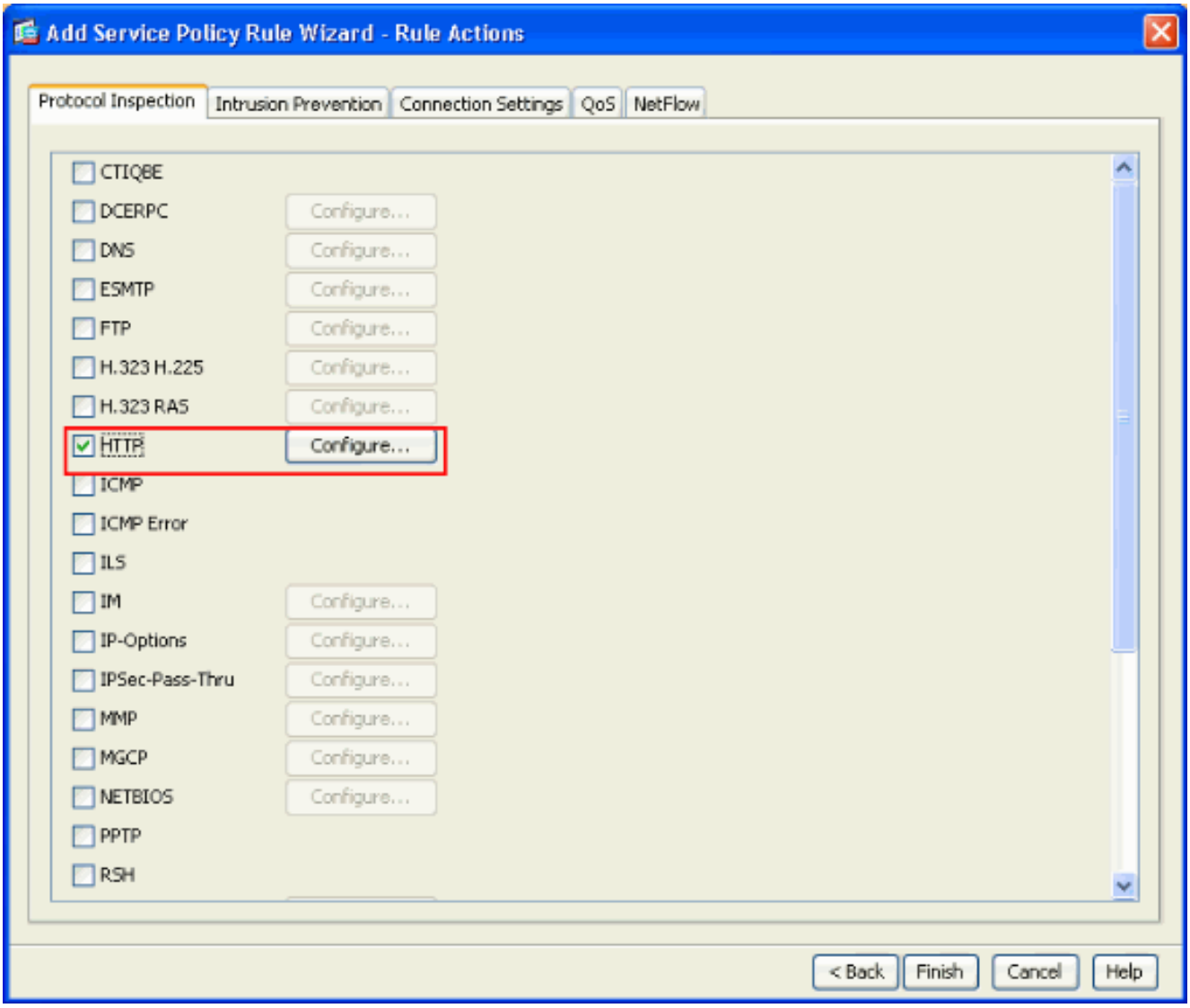

5. Из окна Browse Service выберите **HTTP** в качестве сервиса. **Затем нажмите кнопку ОК.**



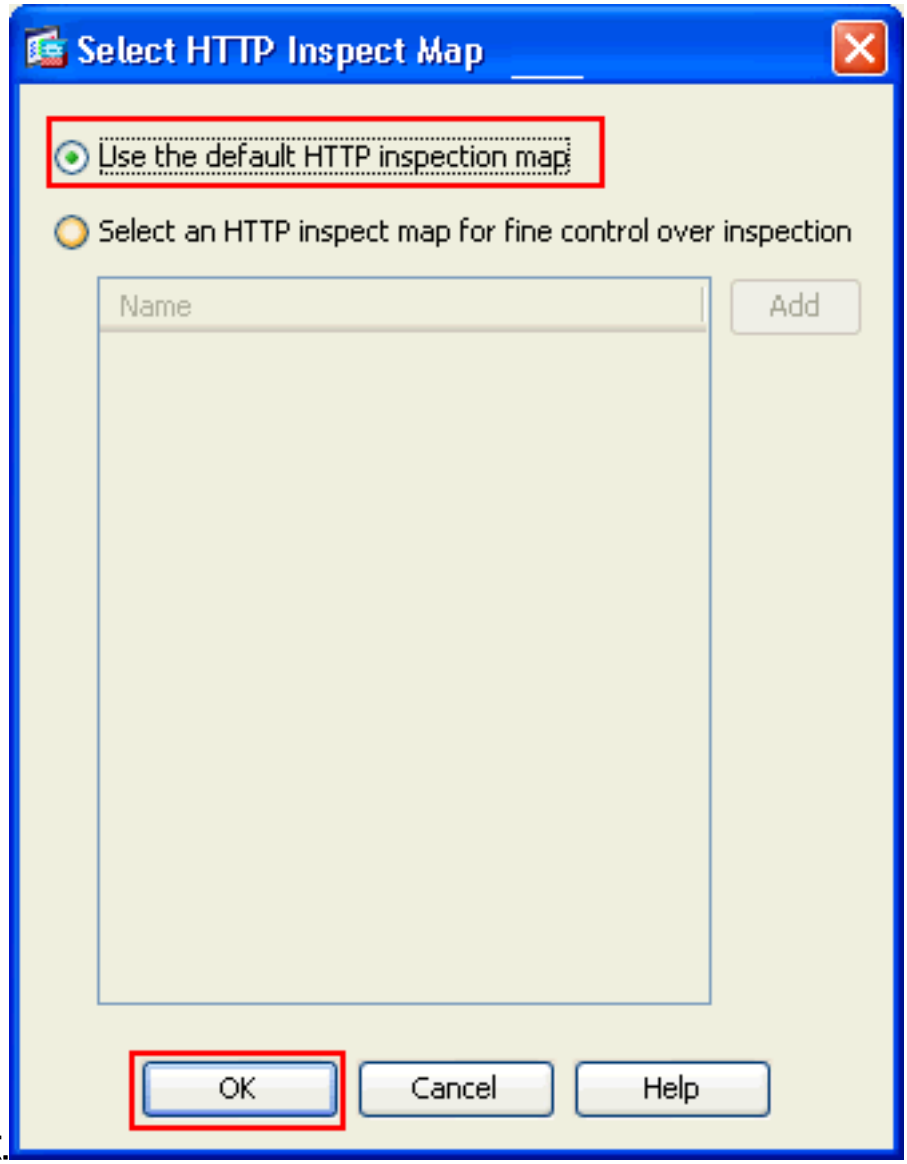

6. От Добавить Мастера Правила Политики обслуживания - Соответствия Трафика - окно Destination Port, вы видите, что выбранный **Сервис** является **tcp/http**. **Нажмите кнопку Next.**




7. От добавьте сервис политика управляет мастером - окно действия правила, проверяет флажок, следующий за **HTTP**. Затем нажмите **Configure**, следующий за **HTTP**.

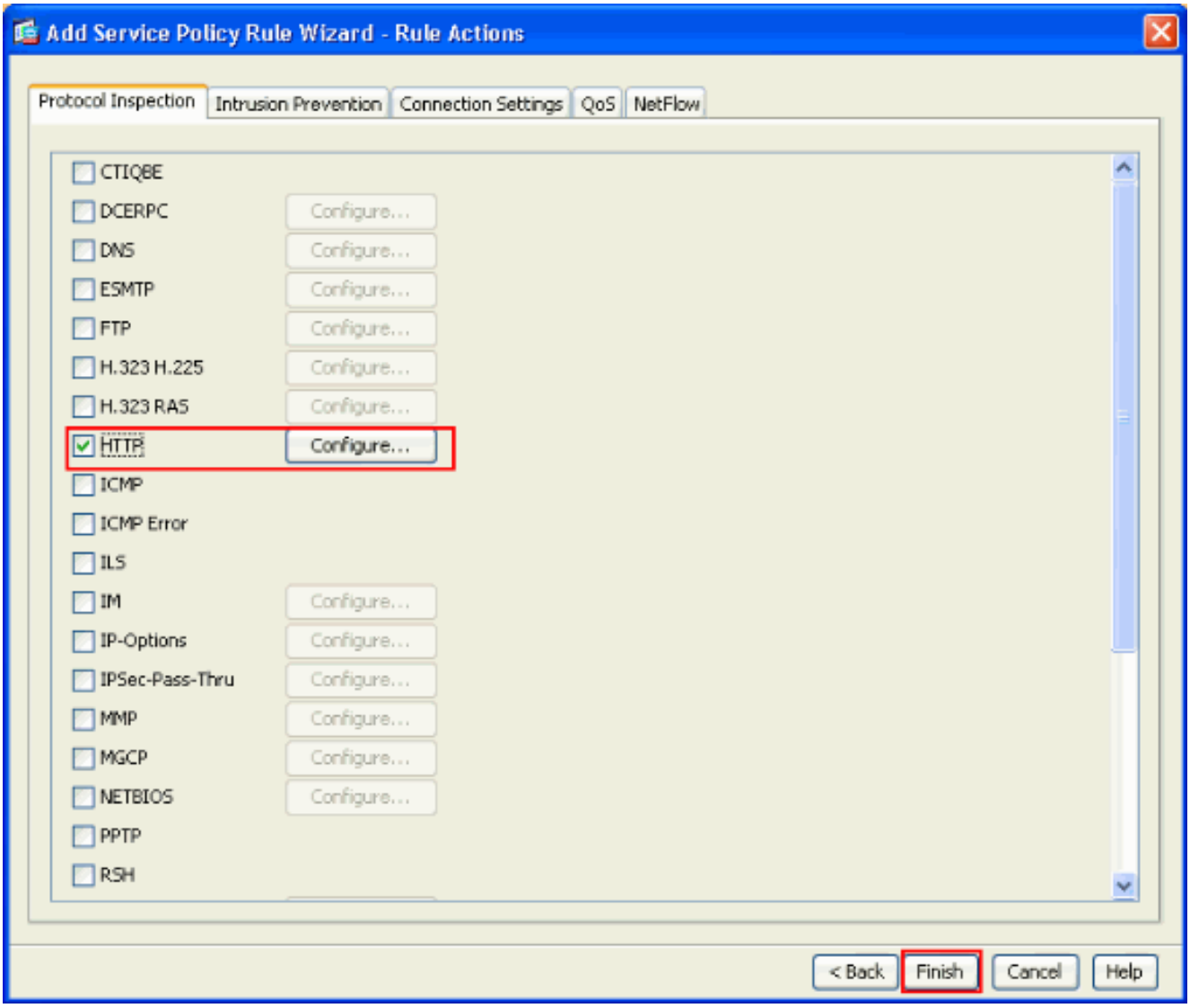



8. Из окна Select HTTP Inspect Map проверьте кнопку с зависимой фиксацией затем для **Использования карты Проверки HTTP По умолчанию**. Проверка HTTP по умолчанию используется в данном примере. **Затем нажмите кнопку**

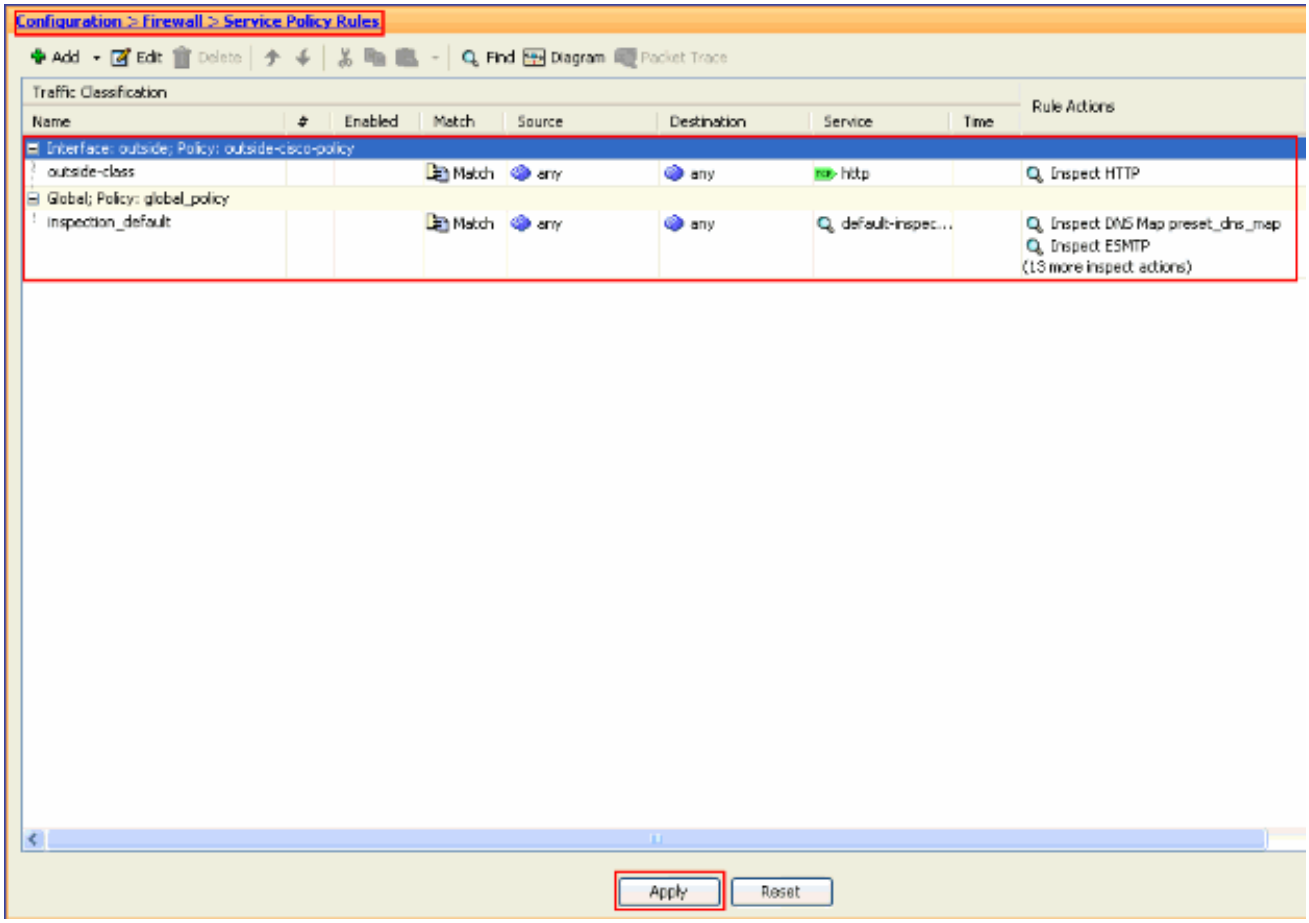



OK.

9. Нажмите кнопку Finish.




10. Под **Конфигурацией> Межсетевой экран> Правила Политики обслуживания**, вы будете видеть, что недавно настроенная **внешняя политика Cisco** Политики обслуживания (для осмотра HTTP) наряду с политикой сервиса по умолчанию уже представляет на устройстве. Нажмите **Apply** для применения конфигурации к Cisco ASA.




## Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Диспетчер адаптивных устройств защиты Cisco (Cisco Adaptive Security Device Manager)
- Запросы комментариев (RFC)
- Применение анализа протоколов прикладного уровня
- Cisco Systems – техническая поддержка и документация