ASA/PIX 7.x: Отключите глобальный контроль по умолчанию и включите контролю приложения ня по умолчанию Использование ASDM

Содержание

Введение

В этом документе описано удаление анализа по умолчанию из глобальной политики для приложения и включение анализа для приложения не по умолчанию.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на устройстве адаптивной защиты Cisco (ASA), который выполняется 7.x образ программного обеспечения.

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.

Родственные продукты

Эта конфигурация может также использоваться с Устройством безопасности PIX, которое выполняется 7.x образ программного обеспечения.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов 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.).)

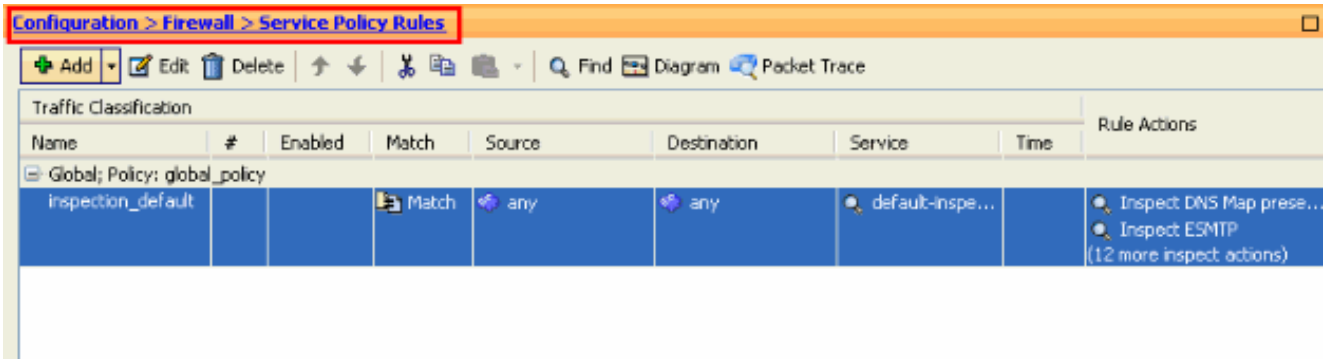
Конфигурация политики по умолчанию содержит следующие команды:

```
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
```

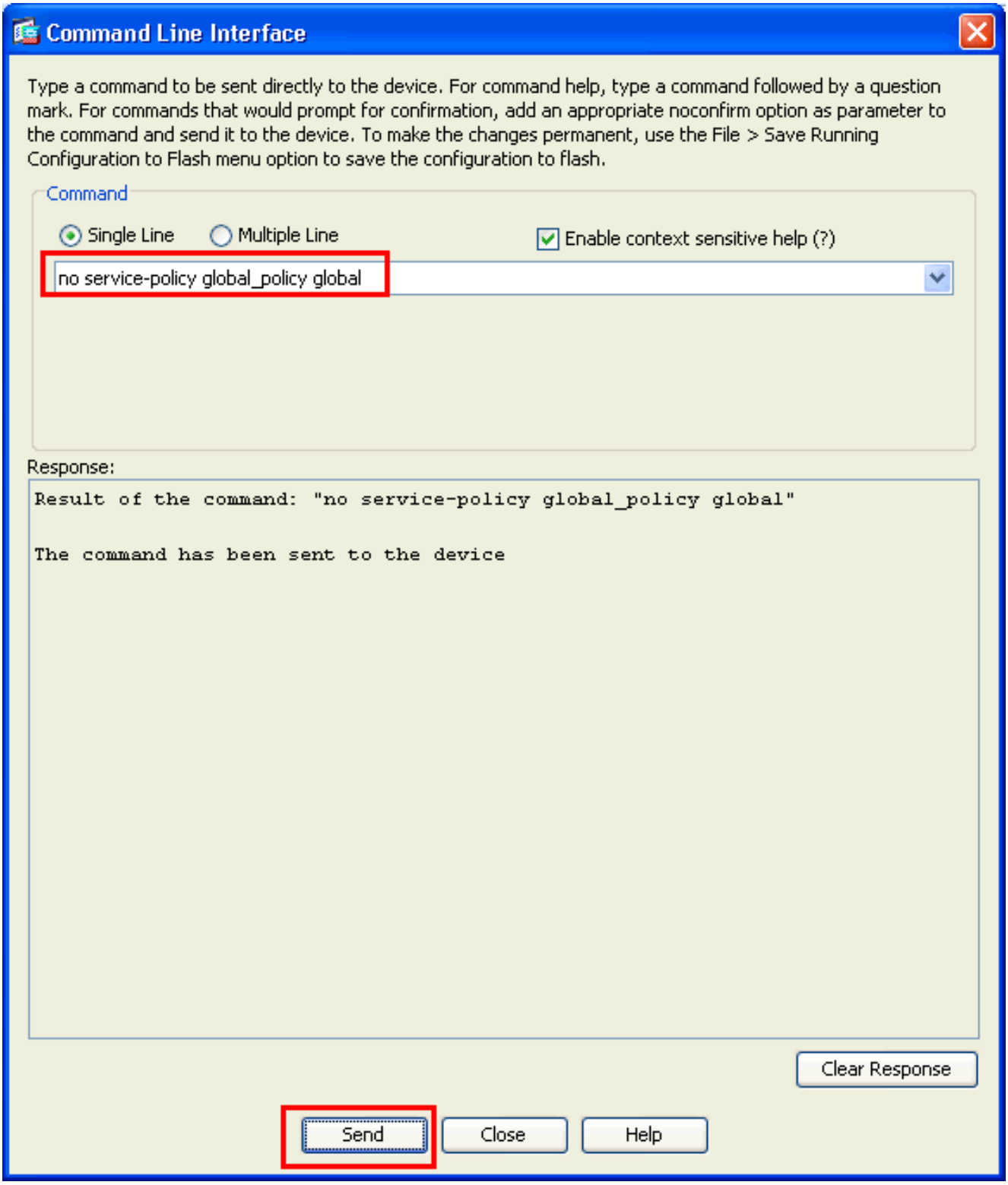
Включите контроль приложения ня по умолчанию

Завершите эту процедуру для включения Контроля приложения Ня по умолчанию на Cisco ASA:

1. Вход в систему к **ASDM**. Перейдите **к Конфигурации> Межсетевой экран> Правила Политики обслуживания**.

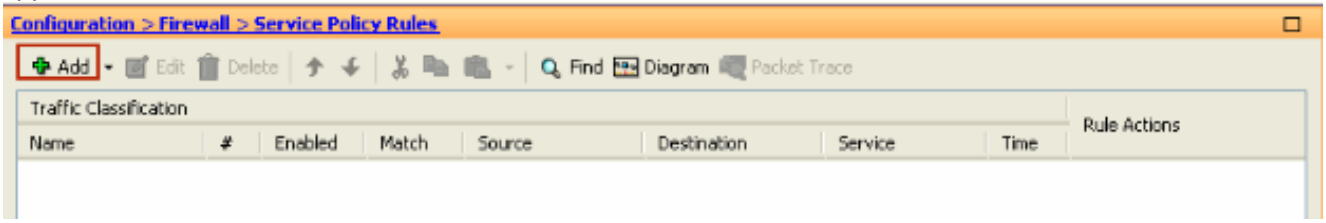


2. Если вы хотите поддержать Конфигурацию для Глобальной политики, которая включает Class-map По умолчанию и Policy-map По умолчанию, но хотят удалить политику глобально, перейти **к Программным средствам> Интерфейс командной строки** и использовать **команду no service-policy global-policy global** для удаления политики глобально. Затем нажмите **Send**, таким образом, команда применена к ASA.



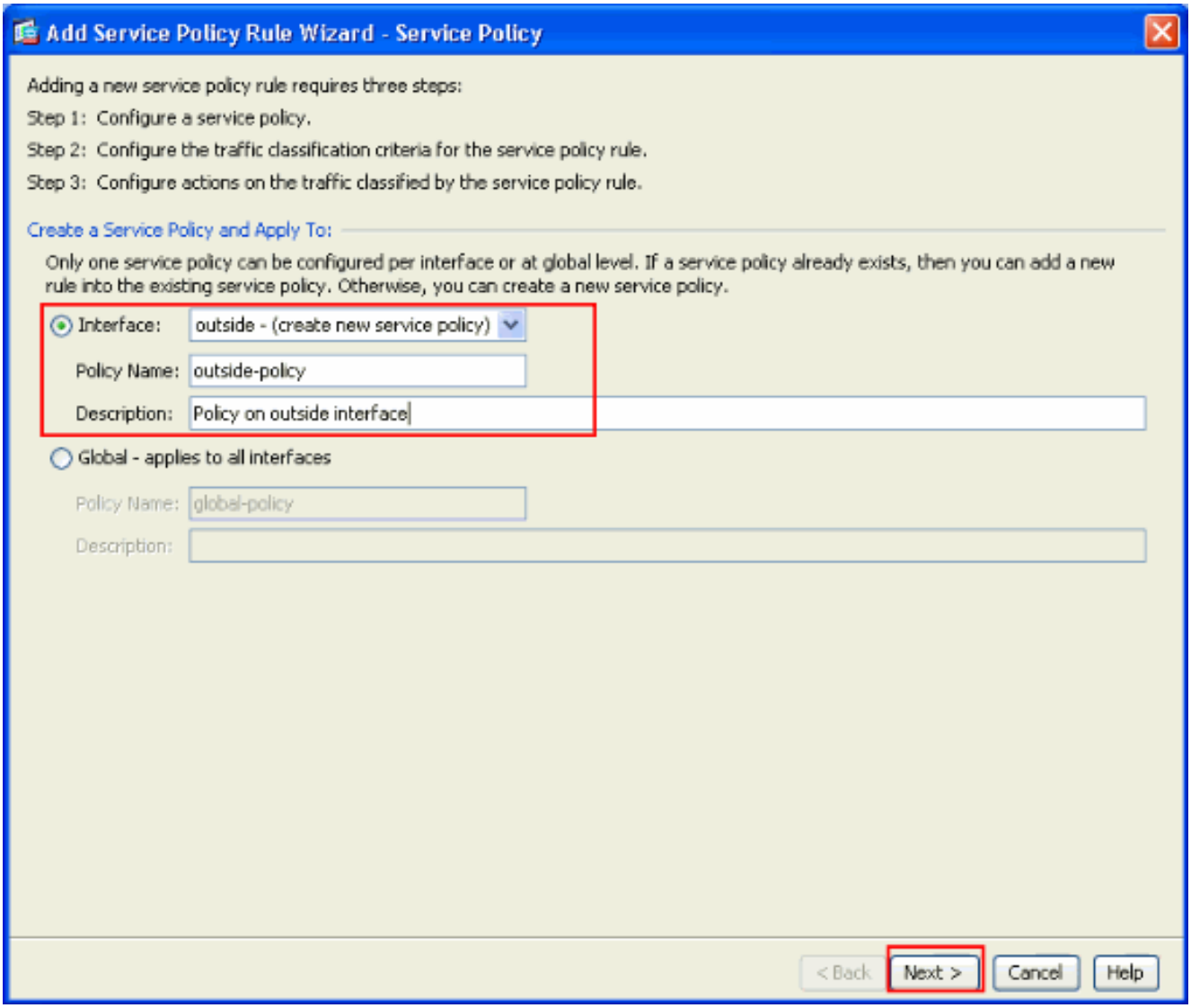
Примечание: С этим шагом Глобальная политика становится невидимой в Менеджере устройств адаптивной безопасности (ASDM) (ASDM), но показана в CLI.

3. **Нажмите Add** для добавления новой политики как показано здесь:

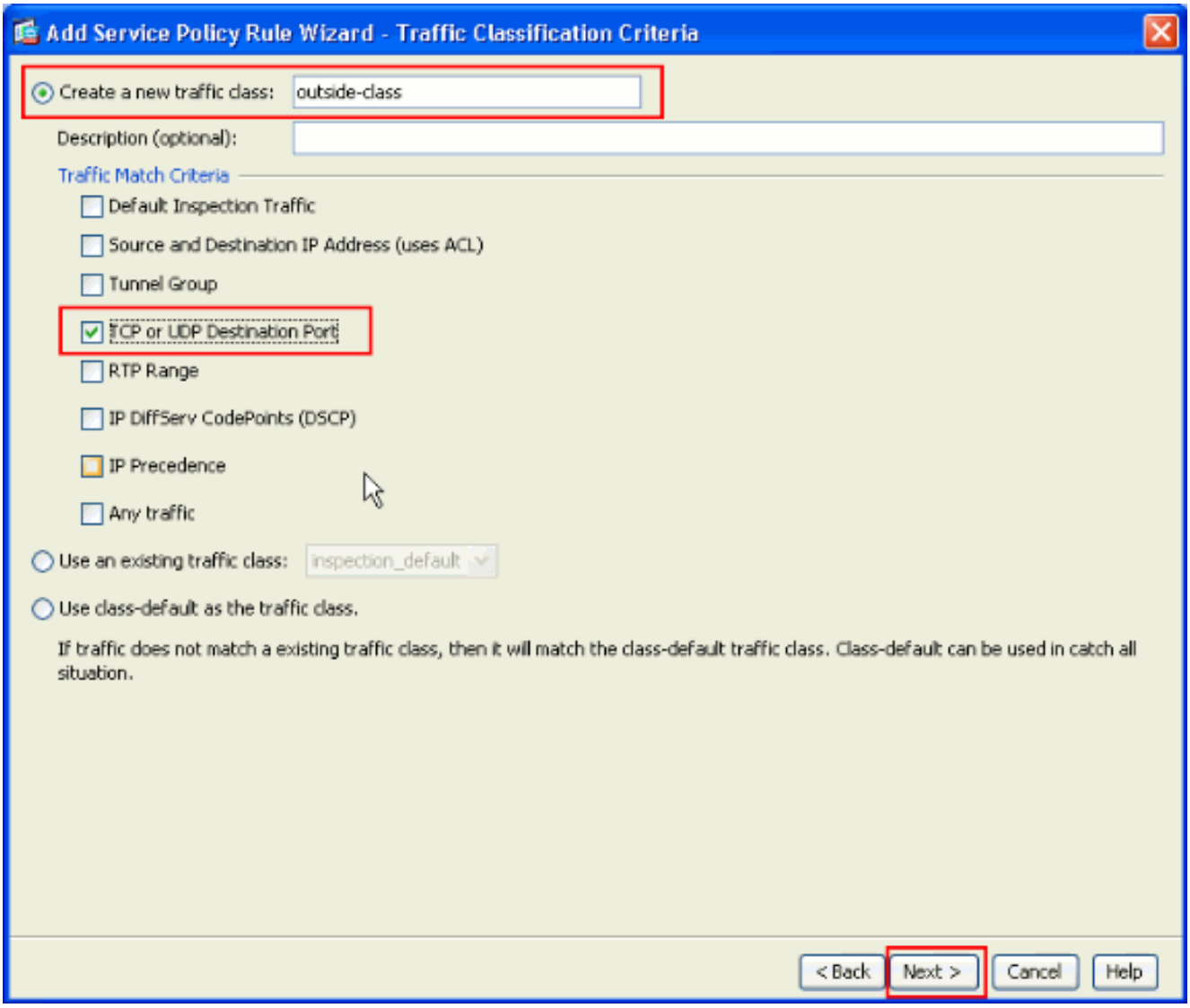


4. Удостоверьтесь, что кнопка с зависимой фиксацией, следующая за **Интерфейсом**, проверена, и выберите интерфейс, вы хотите применить политику от раскрывающегося

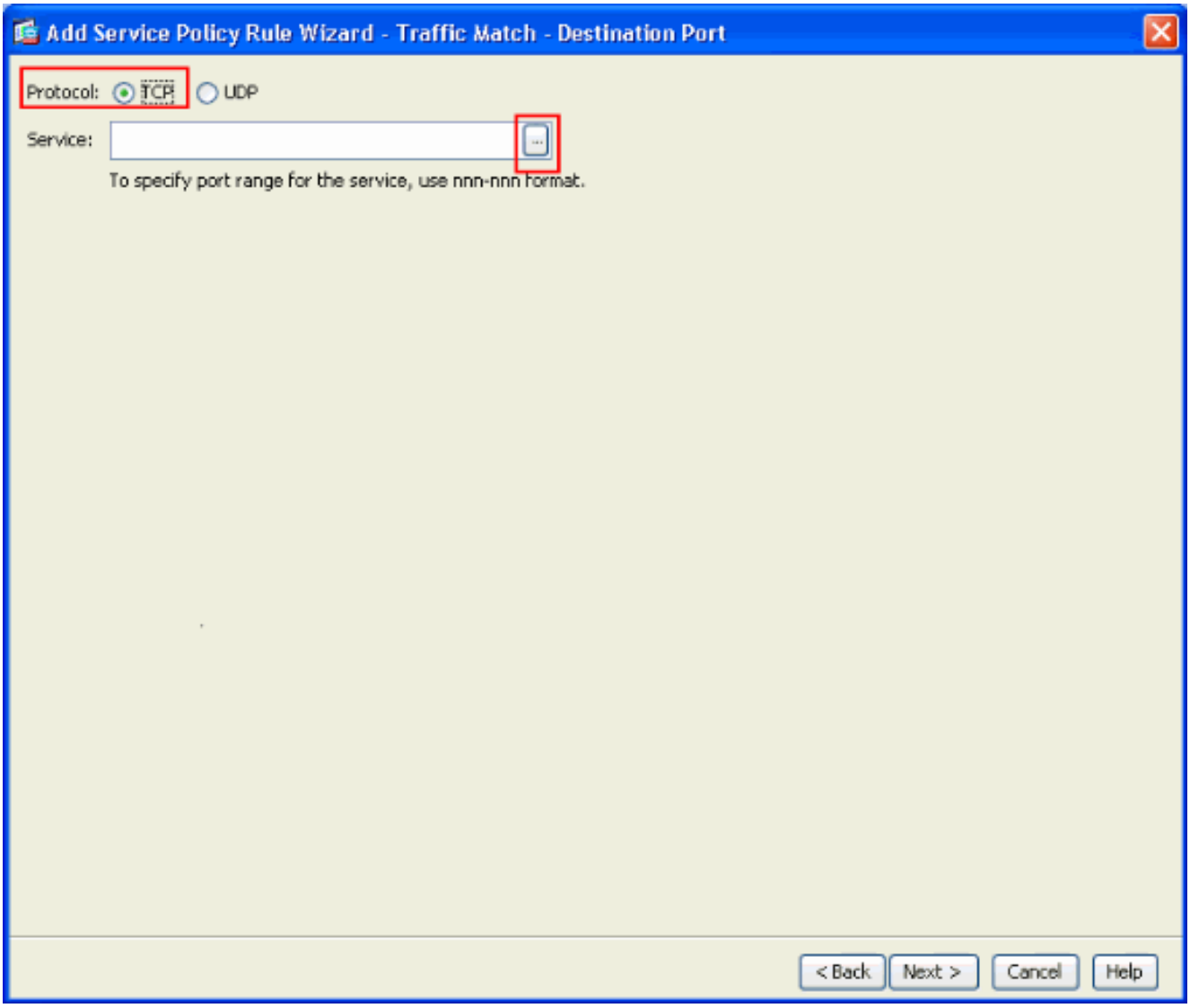
меню. Затем предоставьте **Название Политики** и **Описание**. **Нажмите кнопку Next.**



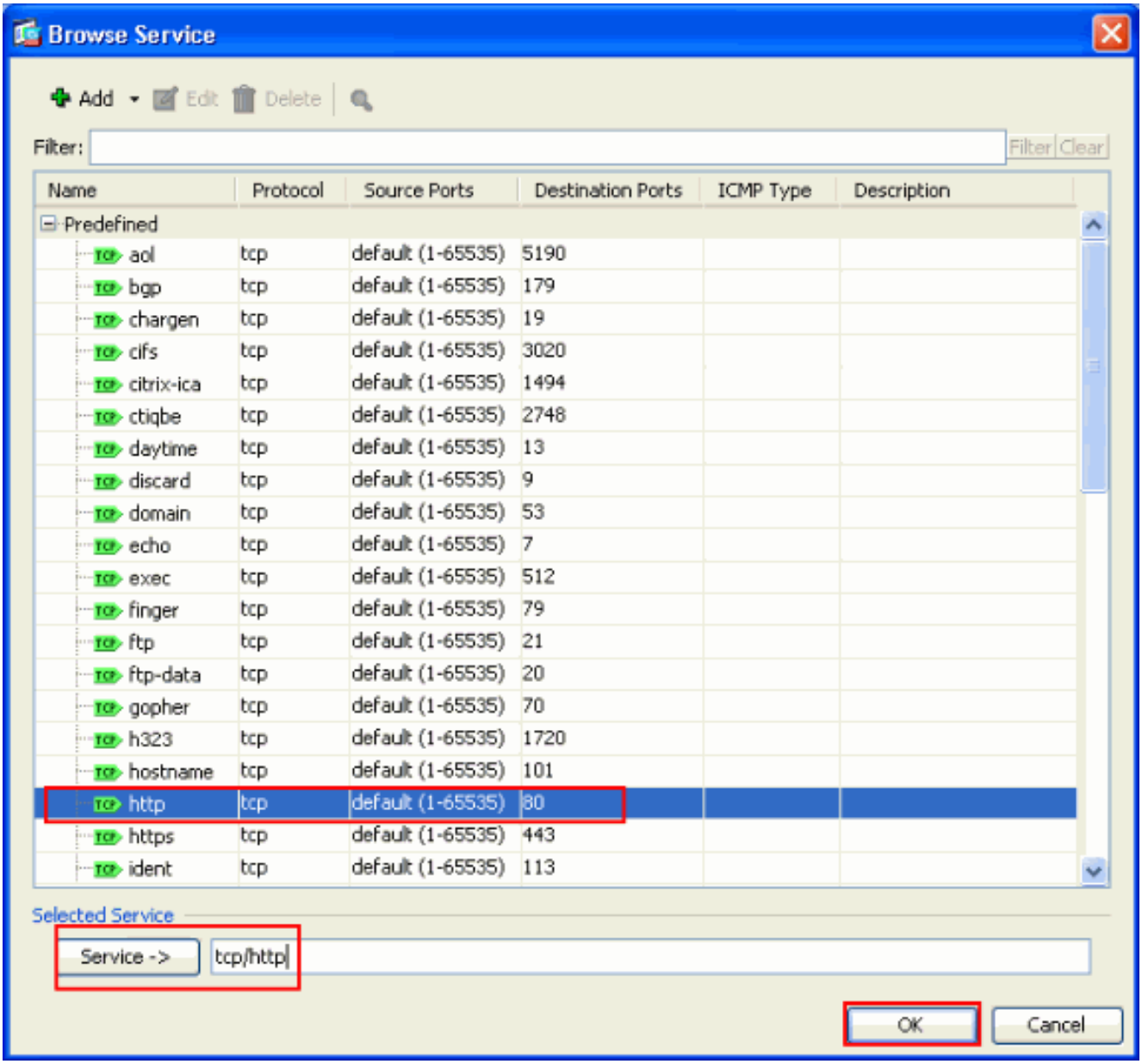
5. Создайте новый class-map для соответствия **с Трафиком TCP**, поскольку **HTTP** подпадает под TCP. **Нажмите кнопку Next.**



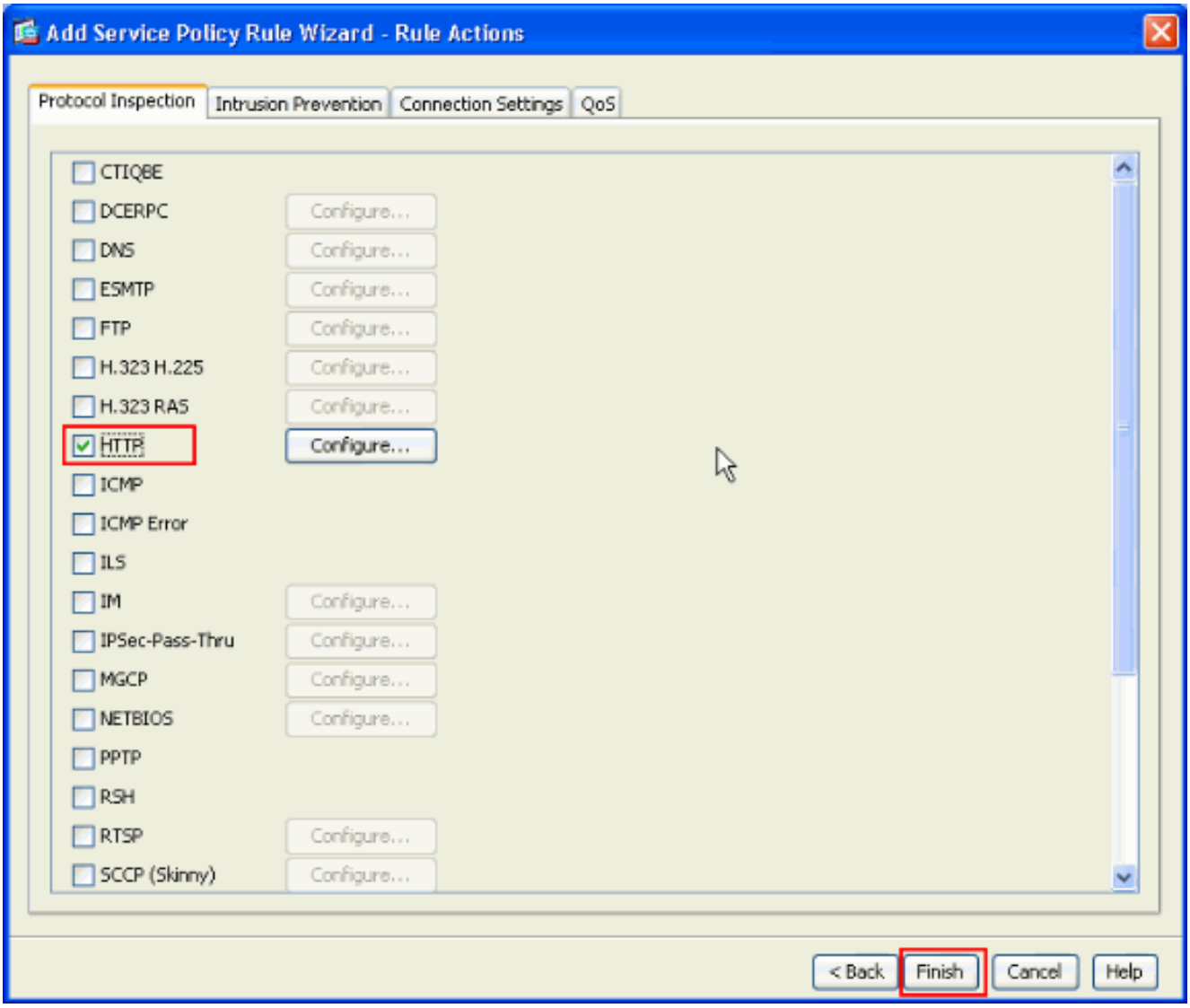
6. Выберите **TCP** в качестве протокола.



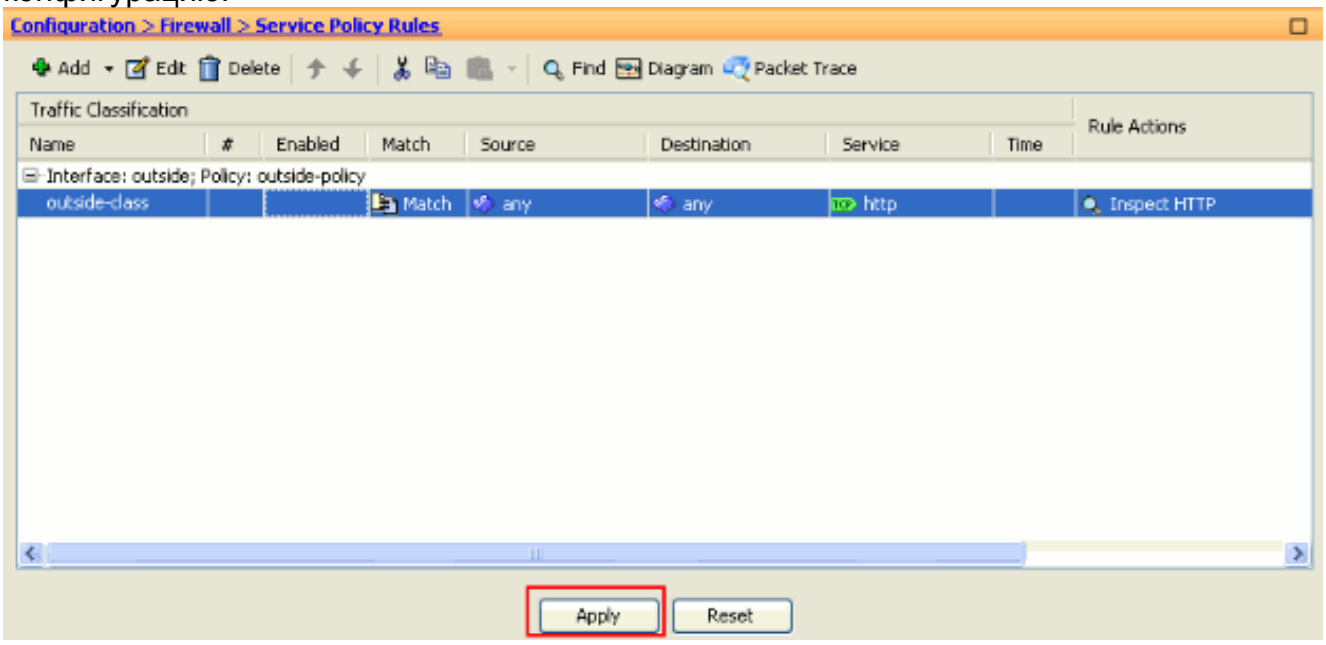
Выберите **порт HTTP 80** в качестве Сервиса и нажмите **OK**.



7. Выберите **HTTP** и нажмите **Finish**.



8. Нажмите **Apply** для передачи этих изменений конфигурации к ASA от ASDM. Это завершает конфигурацию.



Проверка

Для проверки конфигурации используйте следующие команды show:

- Используйте **команду show run class-map** для просмотра настроенных карт классов.
```
ciscoasa# sh run class-map
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class match port tcp eq www !
```
- Используйте **команду show run policy-map** для просмотра настроенных карт политик.
```
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 !
```
- Используйте **команду show run service-policy** для просмотра настроенной политики обслуживания.
```
ciscoasa# sh run service-policy
service-policy outside-policy interface outside
```

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Справочники по командам серии 5500 Cisco ASA
- Cisco Adaptive Security Device Manager (ASDM) страница технической поддержки
- Cisco PIX Firewall Software
- Запросы комментариев (RFC)
- Cisco PIX 500 Series Security Appliances
- Применение анализа протоколов прикладного уровня
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Cisco Systems – техническая поддержка и документация