ASA 8. 3 и позже: Пример настройки времени ожидания соединения SSH/Telnet/HTTP с использованием MPF

Содержание

Введение

В этом документе приводится пример настройки устройства адаптивной защиты Cisco (ASA) с ПО версии 8.3(1) или выше для задания времени ожидания индивидуально для конкретного приложения, такого как SSH/Telnet/HTTP, вместо единой настройки для всех приложений. Этот пример конфигурации использует Модульную систему политик (MPF), которая была представлена в устройстве адаптивной защиты Cisco (ASA) версия 7.0. См. Использование Модульной Системы политик для получения дополнительной информации.

В этом примере конфигурации Cisco ASA настроен для разрешения рабочей станции (10.77.241.129) Telnet/SSH/HTTP к удаленному серверу (10.1.1.1) позади маршрутизатора. Таймаут отдельного подключения к TELNET/SSH/ТРАФИКУ HTTP также настроен. Весь другой Трафик TCP продолжает привязывать значение таймаута обычного подключения к **1:00:00 времени ожидания соединения**.

См. PIX/ASA 7.x и позже / FWSM: Подайте Таймаут SSH/TELNET/СОЕДИНЕНИЯ HTTP с помощью Примера Конфигурации MPF 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 Менеджером устройств адаптивной безопасности (ASDM) (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.

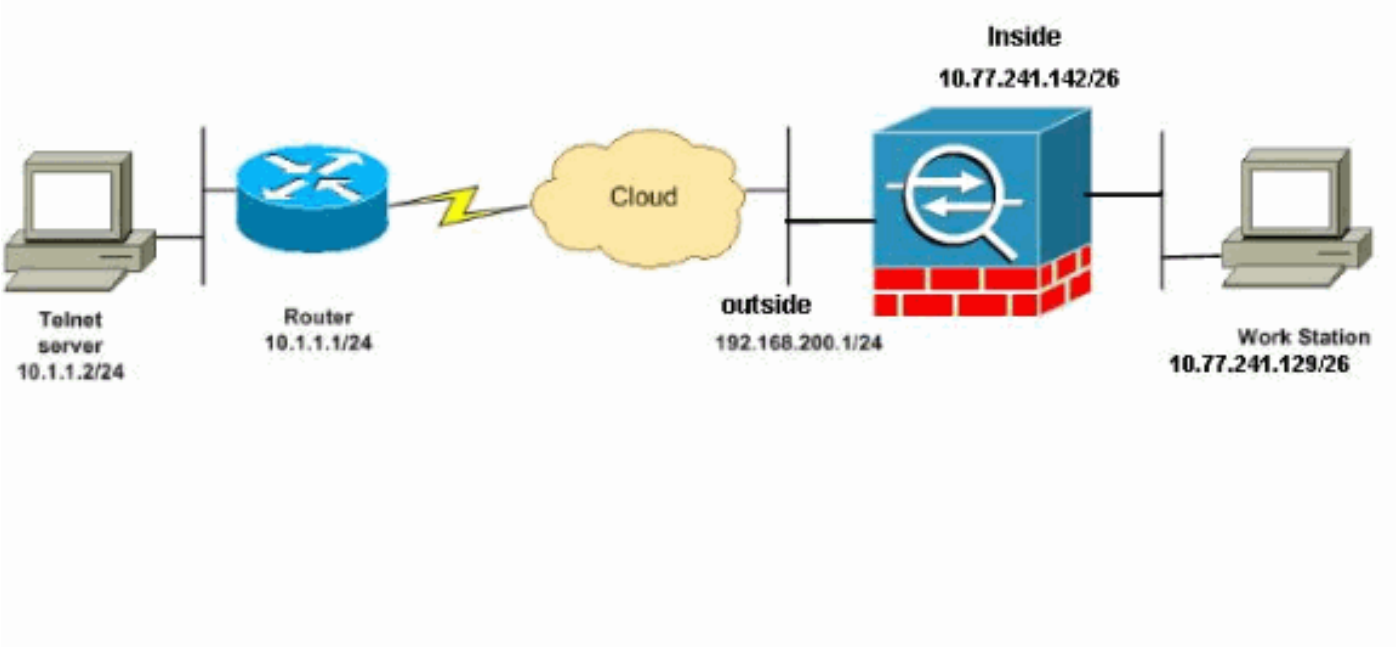
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Конфигурации

Эти конфигурации используются в данном документе:

- Конфигурация интерфейса командой строки CLI
- Настройка посредством ASDM

Примечание: Они CLI и конфигурации ASDM применимы к Модулю Сервиса межсетевого экрана (FWSM).

Конфигурация интерфейса командой строки CLI

ASA 8. 3 (1) конфигурация

```
ASA Version 8.3(1)
!
hostname ASA
domain-name nantes-port.fr
enable password S39lgaewi/JM5WyY level 3 encrypted
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 1mZfSd48bl0UdPgP encrypted
no names

dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
ip address 10.77.241.142 255.255.255.0


boot system disk0:/asa831-k8.bin
ftp mode passive
dns domain-lookup outside

!--- Creates an object called DM_INLINE_TCP_1. This
defines the traffic !--- that has to be matched in the
class map. object-group service DM_INLINE_TCP_1 tcp
port-object eq www port-object eq ssh port-object eq
telnet access-list outside_mpc extended permit tcp host
10.77.241.129 any object-group DM_INLINE_TCP_1 pager
lines 24 mtu inside 1500 mtu outside 1500 no failover no
asdm history enable arp timeout 14400 nat (inside) 0
access-list inside_nat0_outbound access-group 101 in
interface outside route outside 0.0.0.0 0.0.0.0
192.168.200.2 1 timeout xlate 3:00:00 !--- The default
connection timeout value of one hour is applicable to !-
-- all other TCP applications. timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute timeout tcp-proxy-
reassembly 0:01:00 no snmp-server location no snmp-
server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart telnet timeout
5 ssh timeout 5 console timeout 0 ! !--- Define the
class map Cisco-class in order !--- to classify
Telnet/ssh/http traffic when you use Modular Policy
Framework !--- to configure a security feature. !---
```

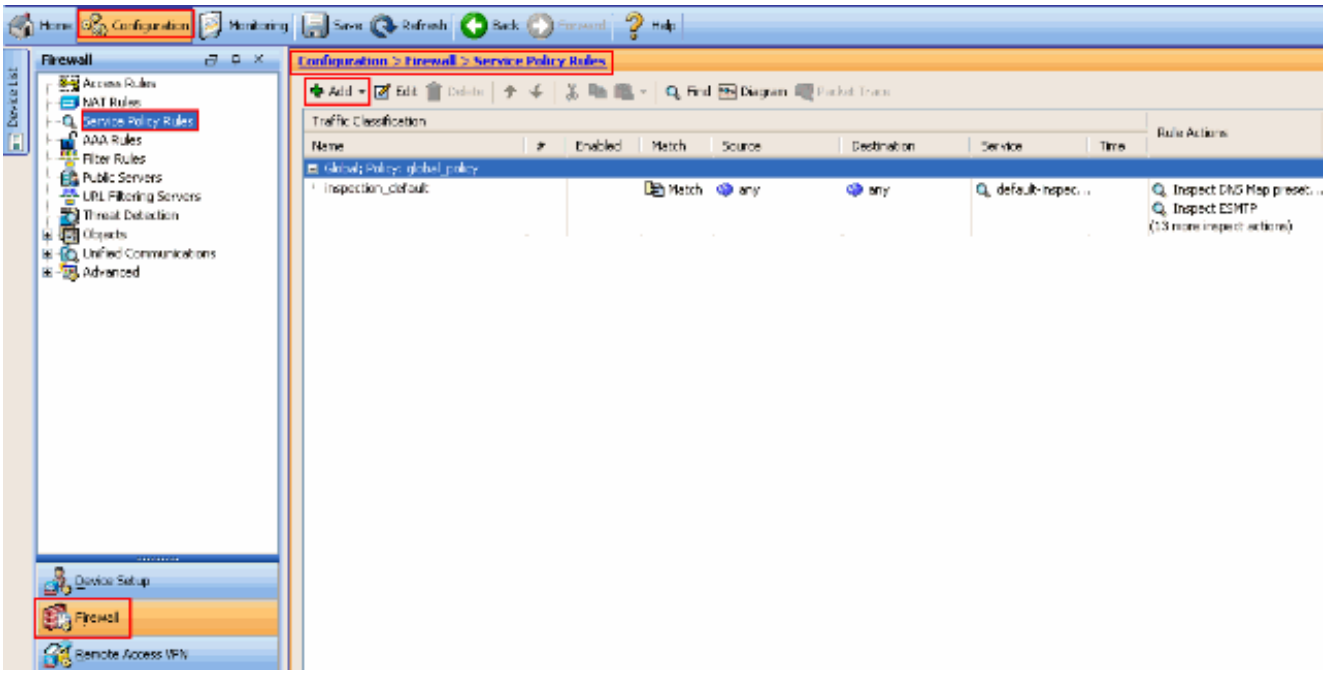
```
Assign the parameters to be matched by class map. class-
map Cisco-class match access-list outside_mpc class-map
inspection_default match default-inspection-traffic ! !
policy-map global_policy class inspection_default
inspect dns maximum-length 512 inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect sqlnet
inspect sunrpc inspect tftp inspect sip inspect xdmcp !-
-- Use the pre-defined class map Cisco-class in the
policy map. policy-map Cisco-policy !--- Set the
connection timeout under the class mode where !--- the
idle TCP (Telnet/ssh/http) connection is disconnected.
!--- There is a set value of ten minutes in this
example. !--- The minimum possible value is five
minutes. class Cisco-class set connection timeout idle
0:10:00 reset ! ! service-policy global_policy global !-
-- Apply the policy-map Cisco-policy on the interface.
!--- You can apply the service-policy command to any
interface that !--- can be defined by the nameif
command. service-policy Cisco-policy interface outside
end
```

Настройка посредством ASDM

Выполните эти шаги для устанавливания таймаута TCP - подключения для Telnet, SSH и трафика HTTP с помощью ASDM как показано.

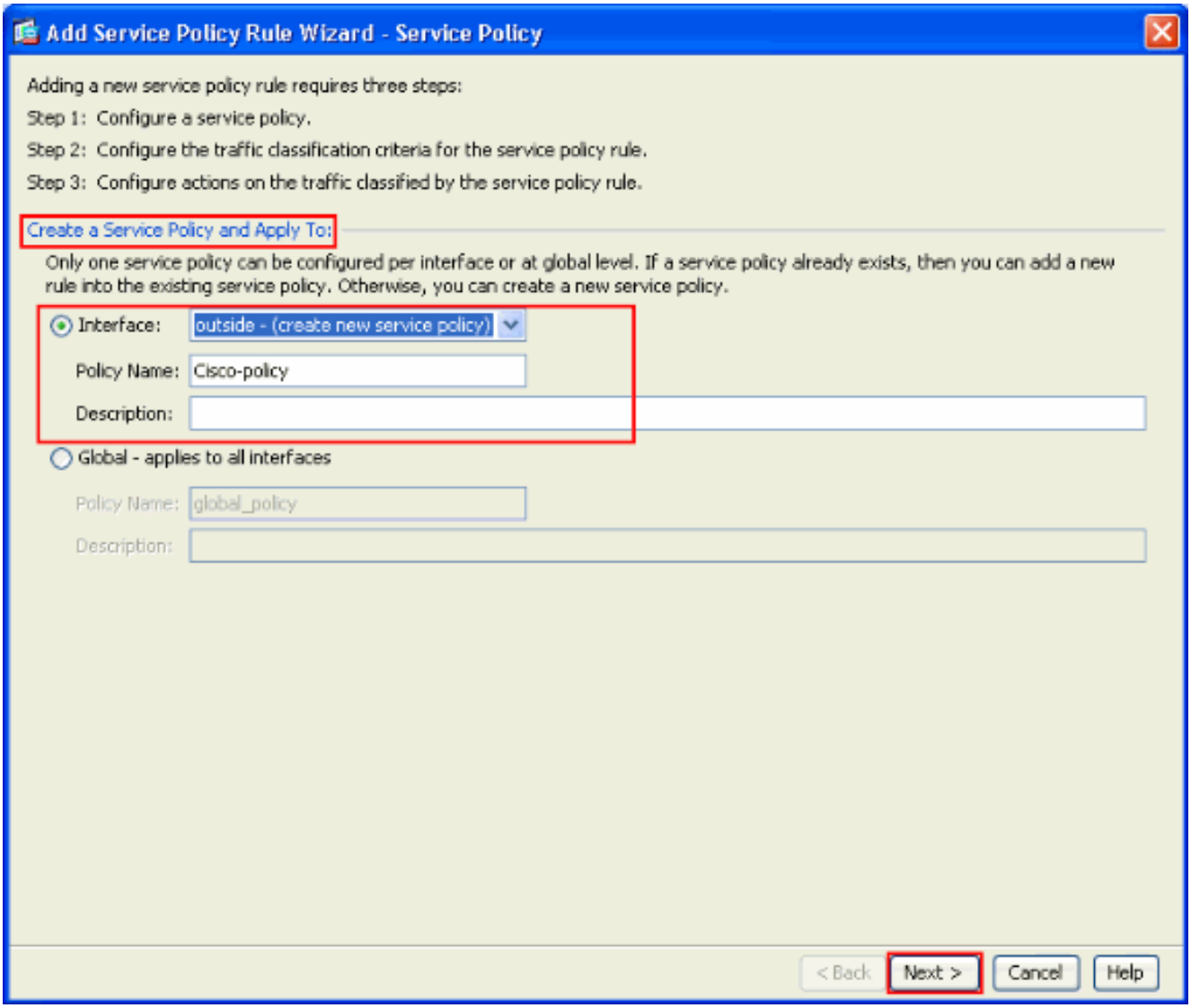
Примечание: См. документ Разрешение HTTPS-доступа для ASDM для базовых параметров для доступа к PIX/ASA через ASDM.

1. Выберите **Configuration> Firewall> Service Policy Rules** и **нажмите Add** для настройки правила Политики обслуживания как показано.

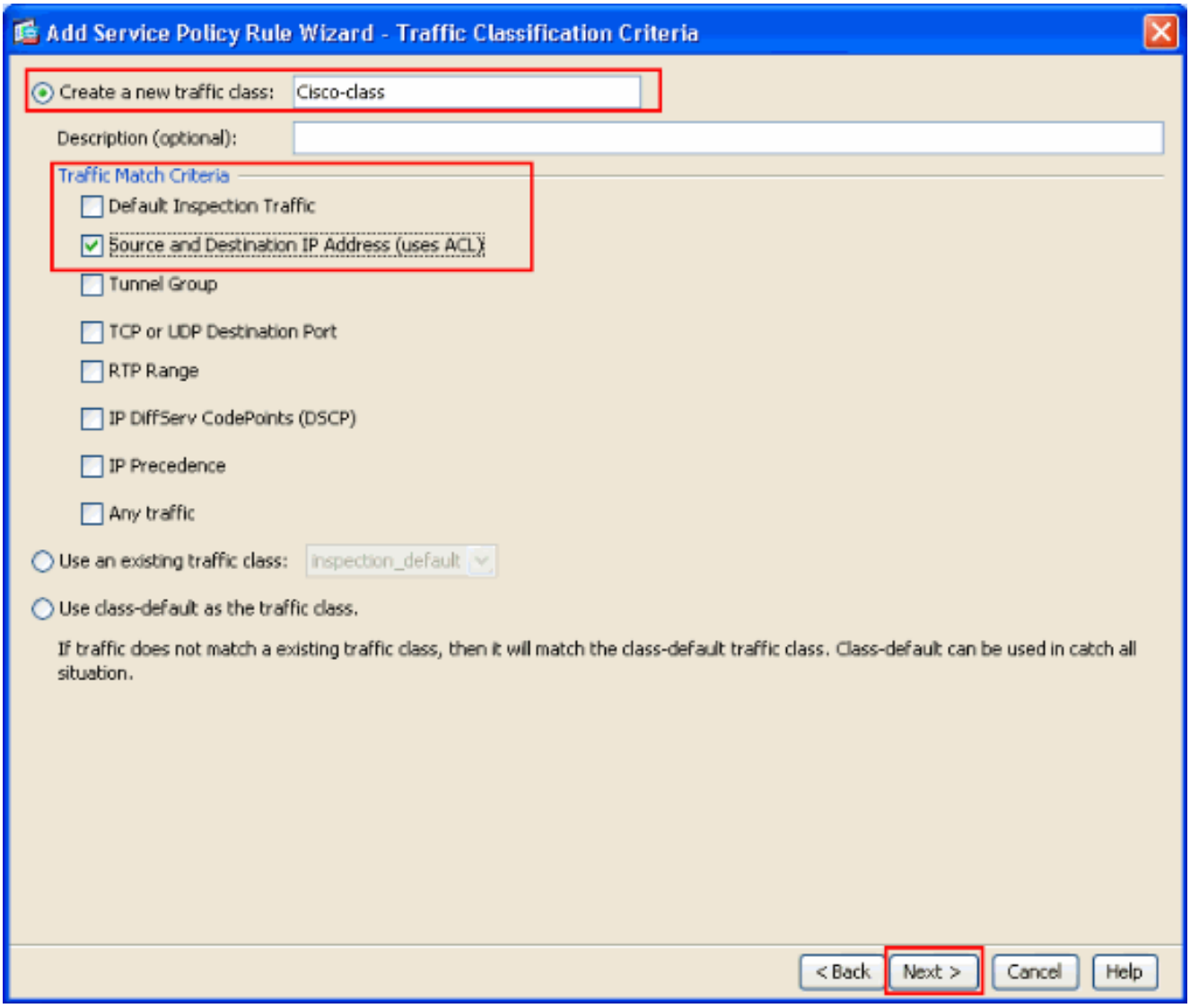


2. От **добавьте сервис политика управляют мастером - сервисное Окно политики**, выбирают кнопку с зависимой фиксацией затем, чтобы **Взаимодействовать** при **Создавании Политики обслуживания и Примениться к** разделу. Теперь выберите необходимый интерфейс из выпадающего списка и предоставьте **Название Политики**.

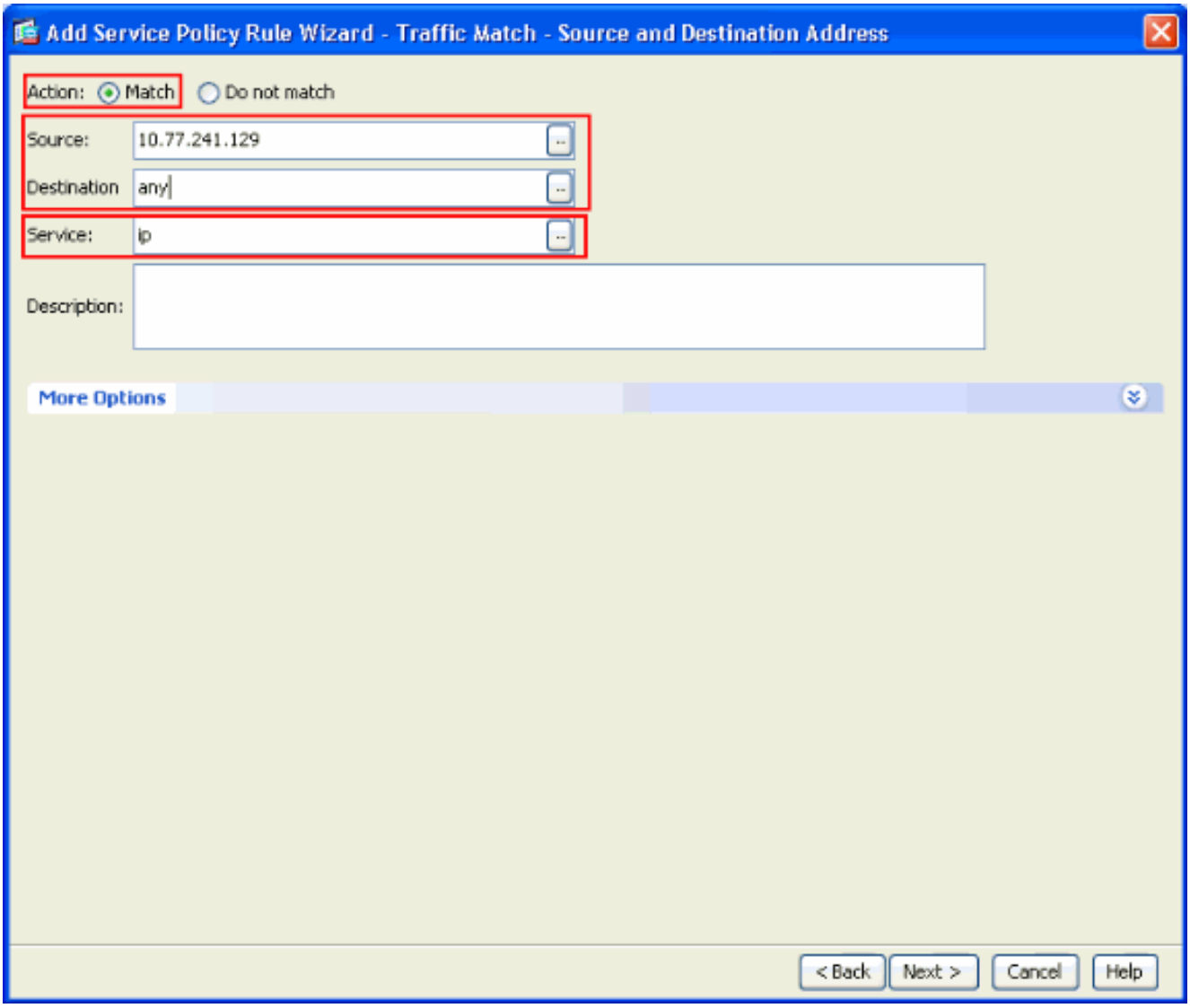
Название политики, используемое в данном примере, является **политикой Cisco**. **Нажмите кнопку**
Next.



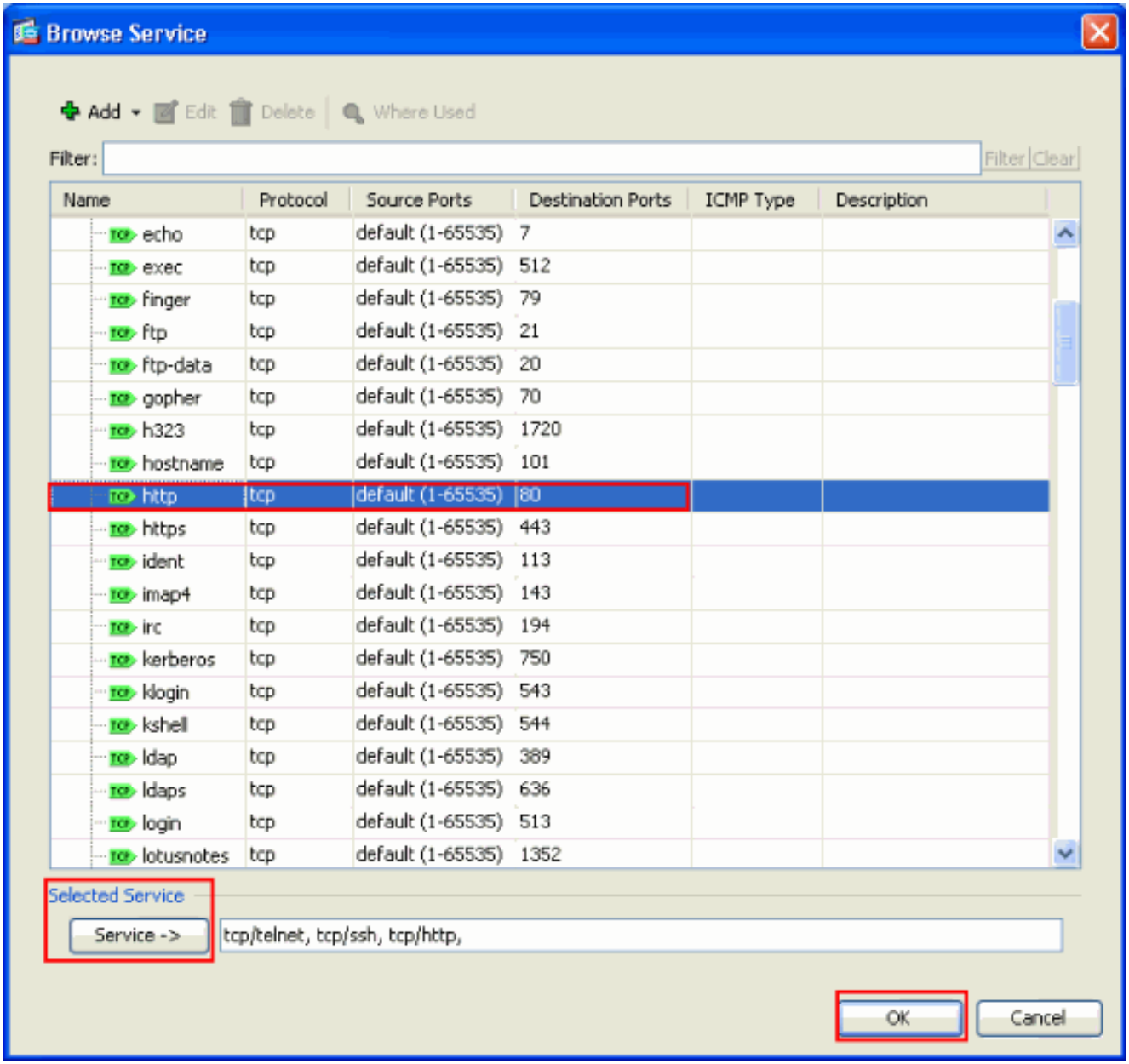
3. Создайте **класс Cisco** названия карты классов и проверьте **IP - адрес источника и получателя (ACL использования)** флажок в Условиях соответствия Трафика. **Нажмите кнопку**
Next.



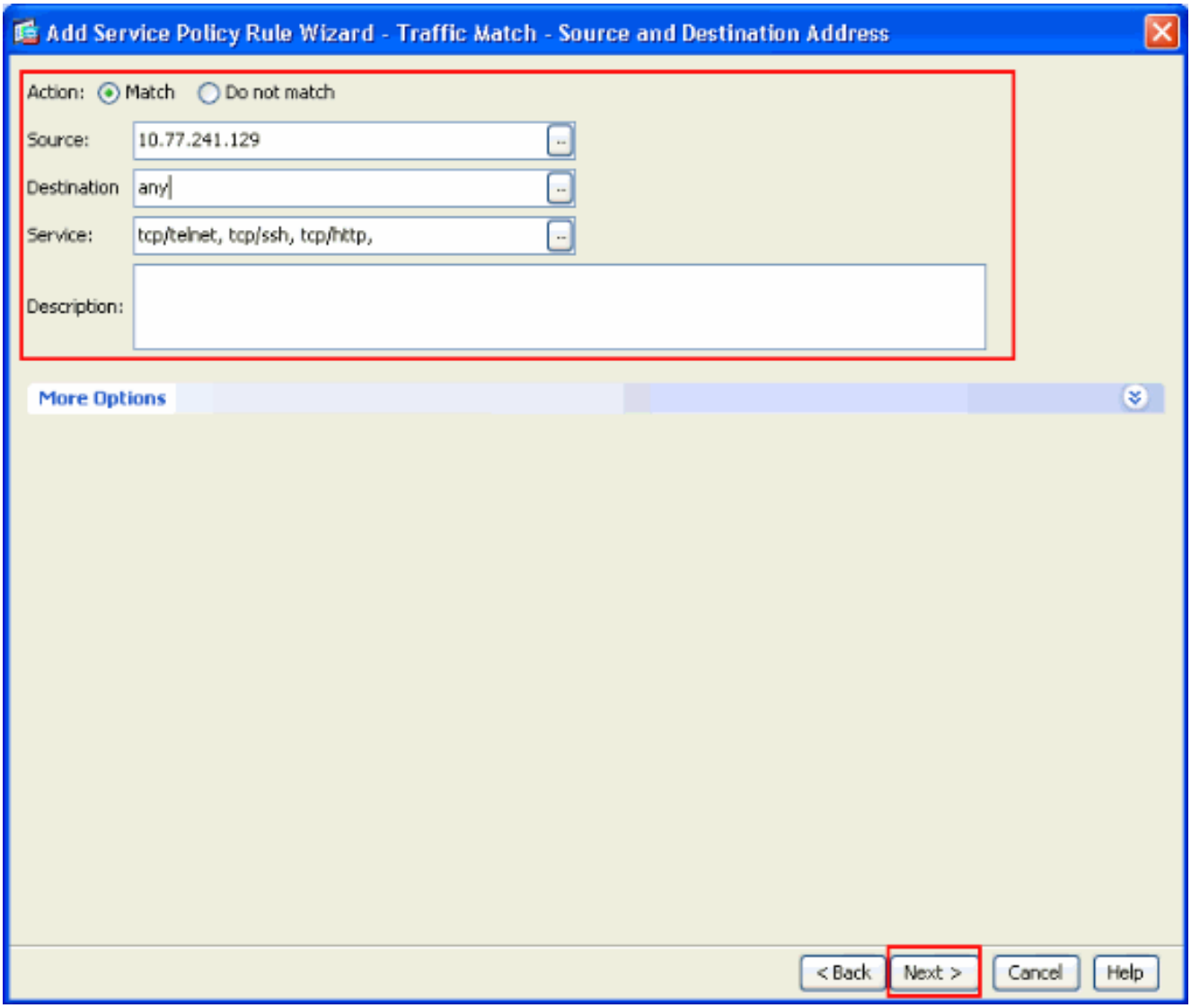
4. От **Добавить Мастера Правила Политики обслуживания - Соответствия Трафика - Источник и Окно адреса Destnation**, выберите кнопку с зависимой фиксацией, следующую за **Соответствием**, и затем предоставьте источник и адрес назначения (DA) как показано. Нажмите кнопку раскрытия списка, следующую за **Сервисом** для выбора требуемых
сервисов.



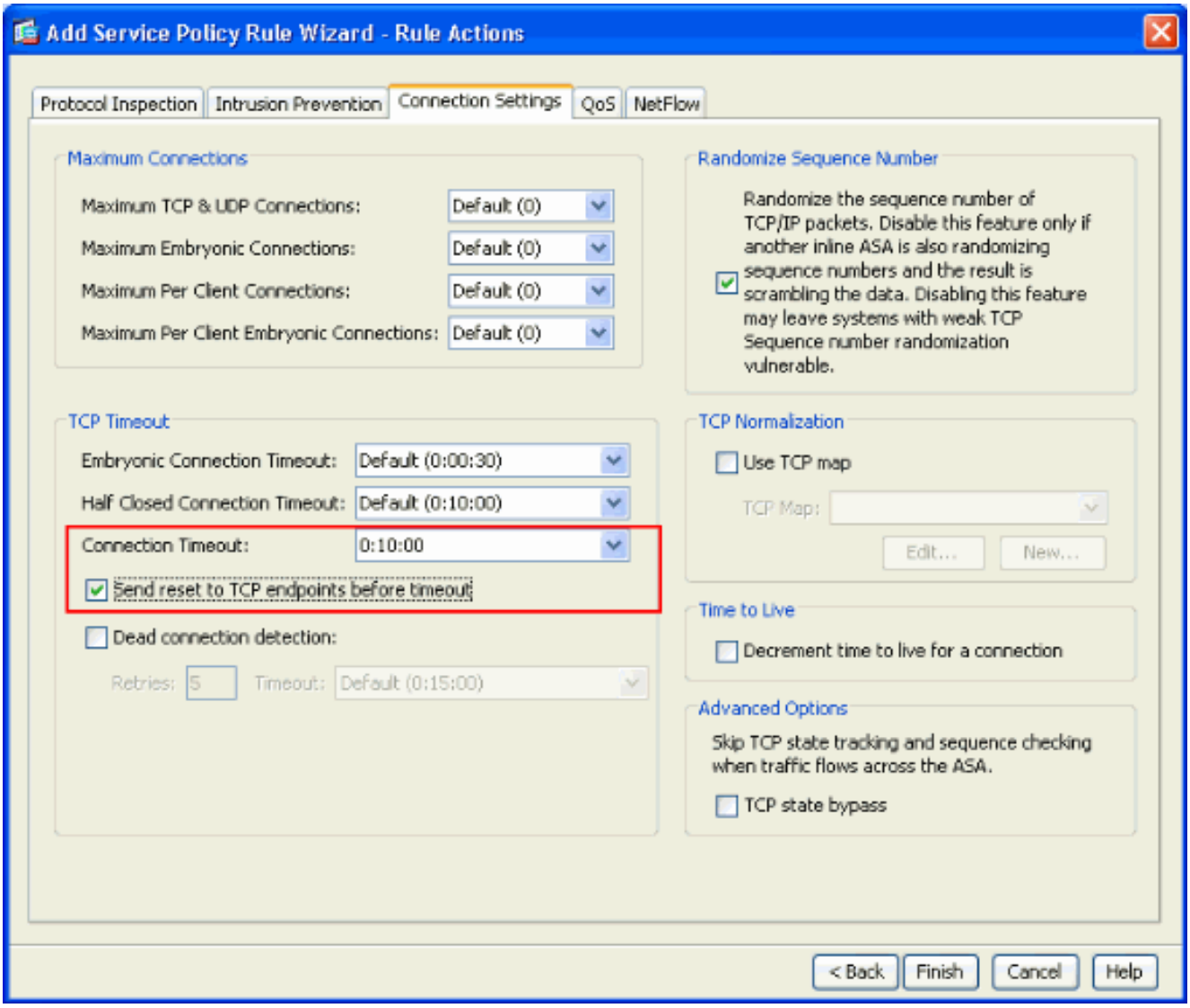
5. Выберите требуемые сервисы, такие как **telnet**, **ssh** и **http**. **Затем нажмите кнопку ОК.**



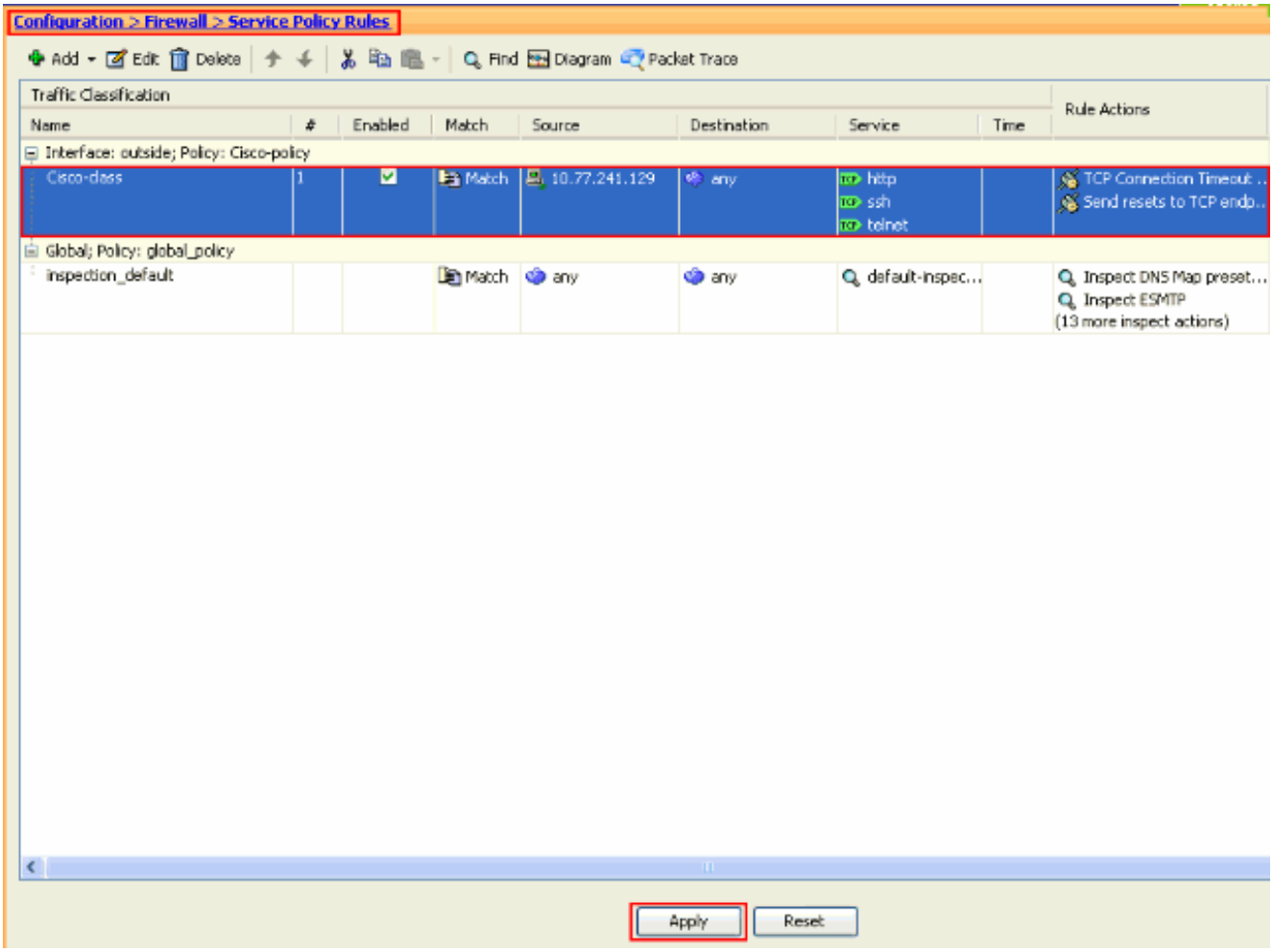
6. Настройте таймауты. Нажмите кнопку Next.



7. Выберите **Connection Settings** для устанавливания Таймаута TCP - подключения как 10 минут. Кроме того, проверьте **сброс Передачи к оконечным точкам TCP перед** флажком **таймаута**. **Нажмите кнопку**
Finish.



8. Нажмите **Apply** для применения конфигурации к Устройству безопасности.Это завершает
конфигурацию.



Таймаут Ebryonic

Неустановившееся соединение является соединением, которое полуоткрыто или, например, трехэтапное установление связи не было завершено для него. Это определено как время ожидания SYN на ASA. По умолчанию время ожидания SYN на ASA составляет 30 секунд. Это - то, как настроить Начальный Таймаут:

```
access-list emb_map extended permit tcp any any

class-map emb_map
match access-list emb_map

policy-map global_policy
class emb_map
set connection timeout embryonic 0:02:00

service-policy global_policy global
```

Устранение неполадок

Если вы находите, что время ожидания соединения не работает с MPF, то проверьте соединение инициирования TCP. Проблема может быть реверсированием IP - адреса источника и получателя, или IP-адрес неверна настроенного в списке доступа не совпадает в MPF, чтобы установить новое значение таймаута или изменить время ожидания по умолчанию для приложения. Создайте запись списка доступа (источник и назначение) в соответствии с инициированием соединения для установки времени ожидания соединения с MPF.

Дополнительные сведения

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