Security Device Manager: Блочный Трафик P2P на маршрутизаторе Cisco IOS с помощью Примера Конфигурации NBAR

Содержание

Введение

Этот документ описывает, как настроить маршрутизатор Cisco IOS® для блокирования одноранговый (P2P) трафик от внутренней сети до Интернета с помощью Сетевого распознавания приложений (NBAR).

NBAR распознает определенные сетевые протоколы и сетевые приложения, которые используются в вашей сети. Однажды протокол или приложение распознан NBAR, можно использовать Модульный интерфейс командной строки для обеспечения качества обслуживания (MQC) для группировки пакетов, привязанных к тем протоколам или приложениям в классы. Эти классы сгруппированы на основе того, соответствуют ли пакеты определенным критериям.

Для NBAR критерий - совпадает ли пакет с определенным протоколом или приложением, известным NBAR. Использование MQC, сетевого трафика с одним сетевым протоколом (Citrix, например) может быть размещено в один класс трафика, в то время как трафик, который совпадает с другим сетевым протоколом (gnutella, например) может быть

размещен в другой класс трафика. Позже, сетевому трафику в каждом классе можно дать соответствующую обработку QoS при помощи политики трафика (карта политик). Обратитесь Сетевой трафик Классификации Использование раздела NBAR *Руководства по конфигурации Решений для качества сервиса Cisco IOS* для получения дополнительной информации о NBAR.

Предварительные условия

Требования

Перед настройкой NBAR для блокирования трафика P2P, необходимо включить технологию CEF.

Используйте **ip cef** в режиме глобальной конфигурации для включения CEF:

```
Hostname(config)#ip cef
```

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Маршрутизатор Cisco 2801 с Выпуском 12.4 (15) T программного обеспечения Cisco IOS
- Диспетчер устройств защиты CISCO SDM версии 2.5

Примечание: См. Базовую настройку маршрутизатора с помощью SDM, чтобы позволить маршрутизатору быть настроенным SDM.

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

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

Обзор сетевого распознавания приложений (NBAR)

Сетевое распознавание приложений (NBAR) является модулем классификации, который распознает и классифицирует большое разнообразие протоколов и приложений. Когда NBAR распознает и классифицирует протокол или приложение, сеть может быть настроена для применения соответствующего качества обслуживания (QoS) для того приложения или трафика с тем протоколом.

NBAR выполняет эти функции:

- **Идентификация приложений и протоколов (Уровень 4 к Уровню 7)**NBAR может классифицировать приложения, которые используют:Статически назначенный Протокол управления передачей (TCP) и номера порта протокола пользовательских датаграмм

(UDP).IP-протоколы, не основанные на UDP и TCP.Динамично назначенный TCP и Номера порта UDP выполнили согласование во время установки соединения. Проверка трафика потоком требуется для классификации приложений и протоколов. Проверка трафика потоком является способностью обнаружить соединения данных, которые будут классифицированы путем передачи контрольных соединений по порту соединения в режиме передачи данных, где сделаны присвоения.Классификация суб - портов: Классификация HTTP (URL, mime или имена хоста) и трафик Независимой вычислительной архитектуры (ICA) приложений Citrix на основе публикованного имени приложения.Классификация на основе глубокой проверки пакетов и множественных специализированных атрибутов. Классификация Информационных наполнений Протокола RTP основывается на этом алгоритме, в котором пакет классифицирован как RTP на основе множественных атрибутов в заголовке RTP.

- **Обнаружение протокола**Обнаружение протокола является обычно используемой функцией NBAR, которая собирает приложение и статистику протокола (количества пакетов, количества байтов и битовые скорости) для интерфейса. GUI базировался, средства управления могут графически отобразить эту информацию путем опроса статистики SNMP от Информационной базы управления (MIB) PD NBAR. Как с любой сетевой функцией, важно понять производительность и характеристики масштабируемости прежде, чем развернуть функцию в рабочую сеть. На программных платформах метрики, которые рассматривают, являются влиянием загрузки ЦПУ и поддерживаемой скоростью передачи данных, в то время как активирована эта опция. Для настройки NBAR для обнаружения трафика для всех протоколов, которые известны NBAR на определенном интерфейсе, используют **команду ip nbar protocol-discovery** в режиме конфигурации интерфейса или Режиме конфигурирования VLAN. Для отключения обнаружения трафика используйте **команду no ip nbar protocol-discovery**.

Настройте одноранговое (P2P) блокирование трафика

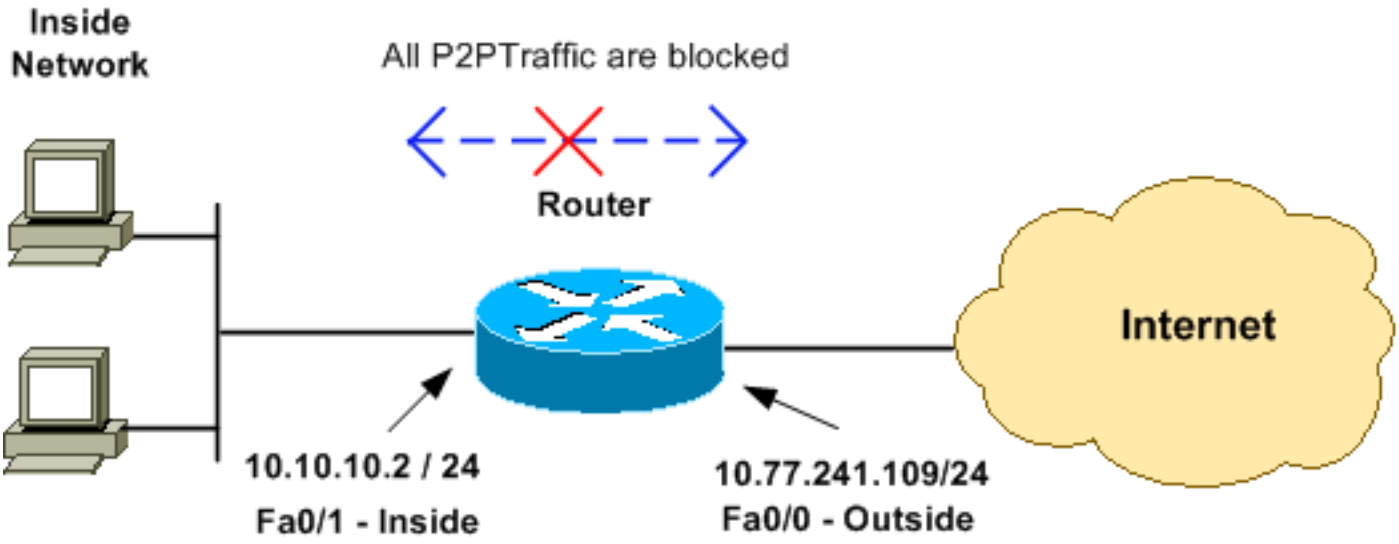
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Некоторый трафик P2P не может быть полностью заблокирован из-за природы его протокола P2P. Эти протоколы P2P динамично изменяют свои подписи для обхода любых механизмов DPI, которые пытаются полностью заблокировать их трафик. Поэтому Cisco рекомендует ограничить пропускную способность вместо того, чтобы полностью блокировать их. (Отрегулируйте пропускную способность для этого трафика. Дайте очень меньше пропускной способности; однако, позвольте соединению пройти.)

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:



Настройка маршрутизатора

Конфигурация для блокирования трафика P2P на маршрутизаторе Cisco IOS

```
R1#show run
Building configuration...

Current configuration : 4543 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
logging buffered 4096
enable secret 5 $1$bKq9$AHOxTgk6d3hcMGn6jTGxs/
!
aaa new-model
!
!
!
!
aaa session-id common
!--- IP CEF should be enabled at first to block P2P
traffic. !--- P2P traffic cannot be blocked when IPC CEF
is disabled. ip cef
!
!--- Configure the user name and password with Privilege
level 15 !--- to get full access when using SDM for
configuring the router. username cisco123 privilege 15
password 7 121A0C0411045D5679
secure boot-image
secure boot-config
archive
 log config
  hidekeys
!
!
!
!--- Configure the class map named p2p to match the P2P
protocols !--- to be blocked with this class map p2p.
```

```
class-map match-any p2p

!--- Mention the P2P protocols to be blocked in order to
block the !--- P2P traffic flow between the required
networks. edonkey, !--- fasttrack, gnutella, kazaa2,
skype are some of the P2P !--- protocols used for P2P
traffic flow. This example !--- blocks these protocols.
match protocol edonkey
 match protocol fasttrack
 match protocol gnutella
 match protocol kazaa2
 match protocol winmx
 match protocol skype

!--- The access list created is now mapped with the
class map P2P !--- to specify the interesting traffic.
match access-group 102
!
!
!--- Here the policy map named SDM-QoS-Policy-2 is
created, and the !--- configured class map p2p is
attached to this policy map. !--- Drop is the command to
block the P2P traffic.

policy-map SDM-QoS-Policy-2
 class p2p
   drop
!
!
!
!--- Below is the basic interface configuration on the
router. interface FastEthernet0/0 ip address
10.77.241.109 255.255.255.192 duplex auto speed auto !
interface FastEthernet0/1 ip address 10.10.10.2
255.255.255.0 !--- The command ip nbar protocol-
discovery enables NBAR !--- protocol discovery on this
interface where the QoS !--- policy configured is being
used.

 ip nbar protocol-discovery
 duplex auto
 speed auto
!--- Use the service-policy command to attach a policy
map to !--- an input interface so that the interface
uses this policy map.

 service-policy input SDM-QoS-Policy-2
!
ip route 10.77.241.0 255.255.255.0 10.10.10.2
ip route 10.77.0.0 255.255.0.0 10.77.241.65
!
!--- Configure the below commands to enable SDM !---
access to the Cisco routers. ip http server
ip http authentication local
no ip http secure-server
!
!--- Configure the access lists and map them to the
configured class map. !--- Here the access list 102 is
mapped to the class map p2p. The access !--- lists are
created for both Incoming and outgoing traffic through
!--- the inside network interface.

access-list 102 remark SDM_ACL Category=256
access-list 102 remark Outgoing Traffic
```

```
access-list 102 permit ip 10.10.10.0 0.0.0.255
10.77.241.0 0.0.0.255
access-list 102 remark Incoming Traffic
access-list 102 permit ip 10.77.241.0 0.0.0.255
10.10.10.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
 password 7 02250C520807082E01165E41
line vty 0 4
 exec-timeout 0 0
 password 7 05080F1C22431F5B4A
 transport input all
!
!
webvpn cef
end
```

Настройте маршрутизатор с SDM

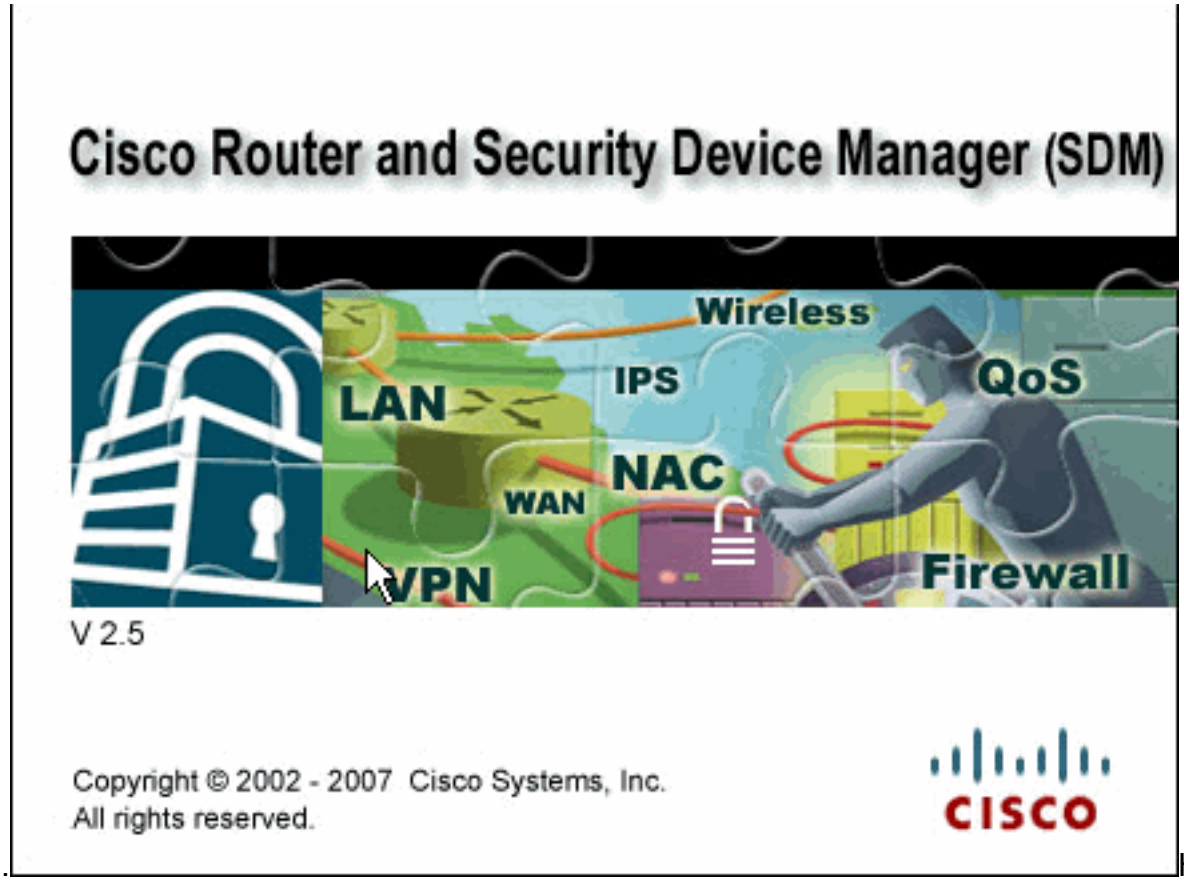
Настройка маршрутизатора с помощью SDM

Выполните эти шаги для настройки блокирования трафика P2P на маршрутизаторе Cisco IOS:

Примечание: Для настройки NBAR для обнаружения трафика для всех протоколов, которые известны NBAR на определенном интерфейсе, команда ip nbar protocol-discovery должна использоваться в режиме конфигурации интерфейса или Режиме конфигурирования VLAN для включения обнаружения трафика. Продолжите SDM-конфигурацию после настройки обнаружения протокола на соответствующем интерфейсе, где используется настроенная политика QoS.

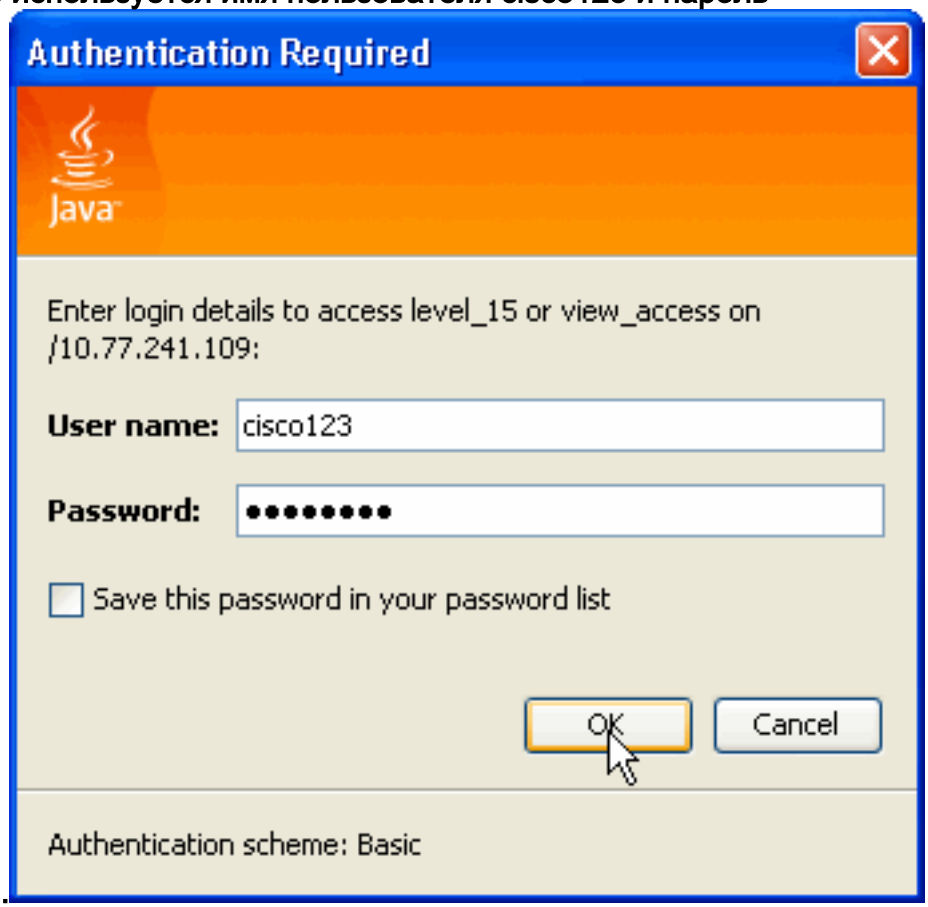
```
Hostname#config t
               Hostname(config)#interface fastEthernet 0/1
               Hostname(config-if)#ip nbar protocol-discovery
               Hostname(config-if)#end
```

1. Откройте браузер и введите IP-адрес маршрутизатора, который был настроен для доступа SDM. Например, **https://*<SDM_Router_IP_Address>***Удостоверьтесь, что авторизовали любые предупреждения, которые ваш браузер дает вам отнесенный подлинности сертификата SSL. По умолчанию имя пользователя и пароль являются пустыми.Маршрутизатор отображает это окно для разрешения загрузки приложения SDM. В данном примере используется приложение, загруженное на локальный компьютер, а не приложение



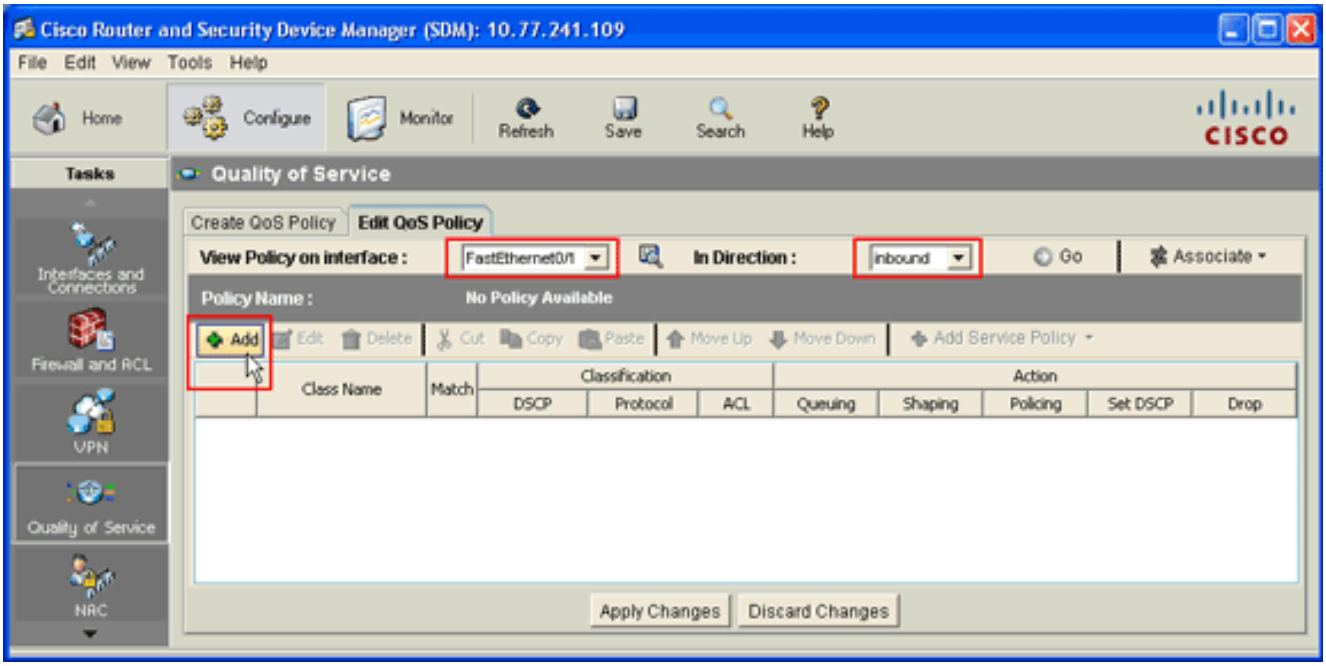
Java.Начнется загрузка SDM.

2. После загрузки SDM Launcher выполните все шаги, сопровождаемые соответствующими подсказками, необходимые для установки приложения и запуска Cisco SDM Launcher.
3. Введите имя пользователя и пароль, если вы задали один, и нажмите **OK.В этом примере используется имя пользователя cisco123 и пароль**



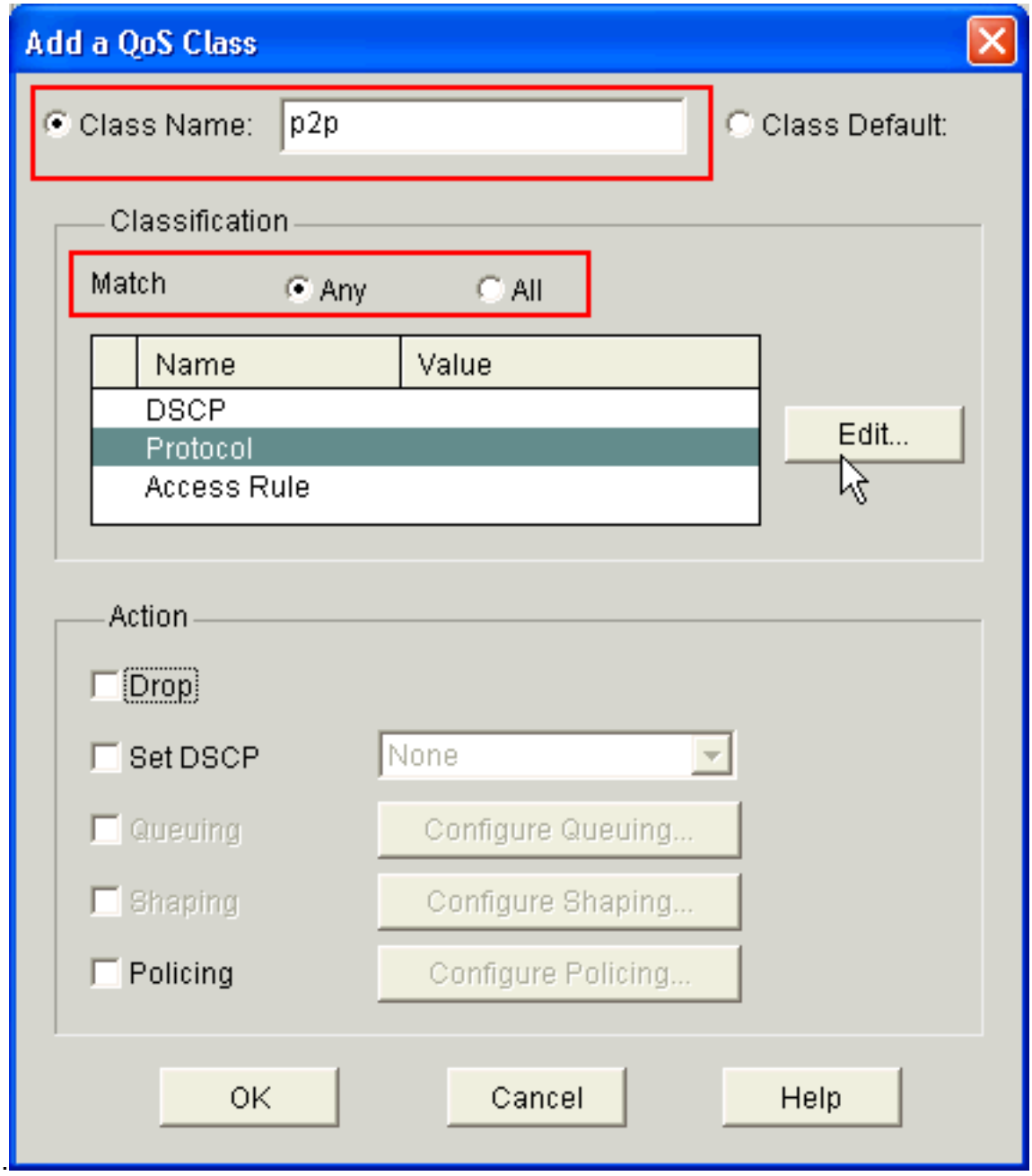
cisco123.

4. Выберите **Configure> Quality of Service** и нажмите вкладку **Edit QoS Policy** на домашней странице
   SDM.



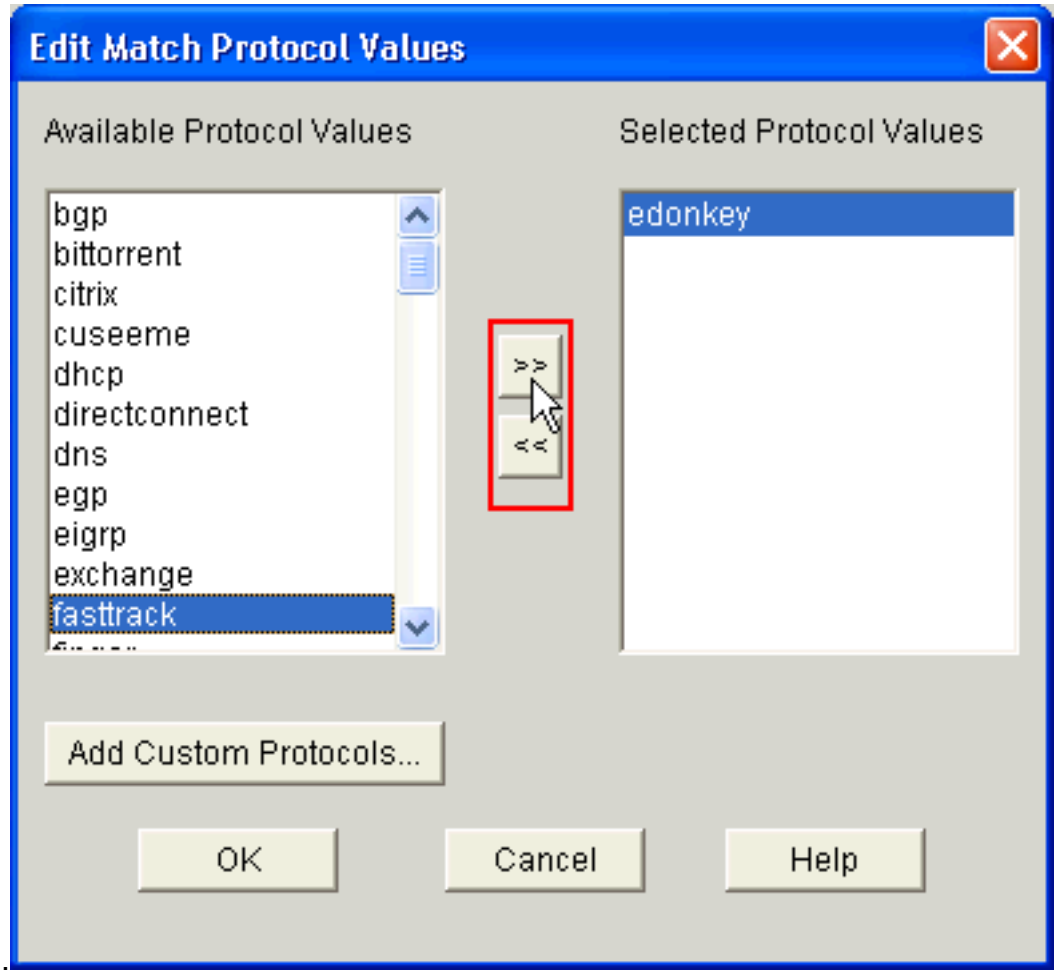
5. От Обзорной Политики по интерфейсному выпадающему списку выберите имя интерфейса, и затем выберите поток направления трафика (или входящий или исходящий) от В выпадающем списке Направления.В данном примере интерфейс является *FastEthernet 0/1*, и направление является *входящим*.
6. **Нажмите Add** для добавления нового класса QoS для интерфейса.Диалоговое окно Add a QoS Class

появляется.

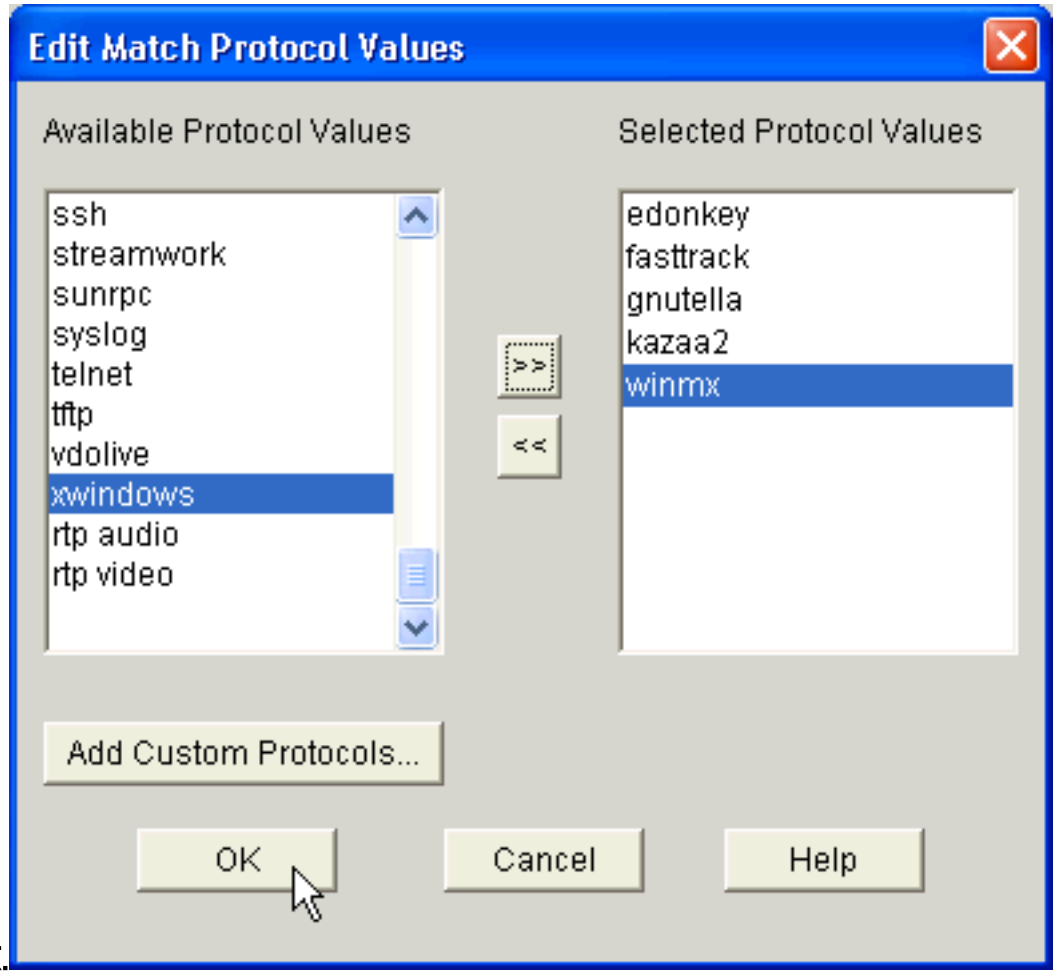


7. Если вы хотите создать новый класс, нажмите кнопку с зависимой фиксацией **Class Name** и введите имя для вашего класса. В противном случае нажмите кнопку с зависимой фиксацией **Class Default**, если вы хотите использовать класс по умолчанию.Данный пример создает новый класс, названный *p2p*.
8. В области Classification нажмите или **Любую** кнопку с зависимой фиксацией или **Всю** кнопку с зависимой фиксацией для опции Match.Данные примеры используют опцию *Any Match*, которая выполняет [команду p2p match-any class-map](#) на маршрутизаторе.
9. Выберите **Protocol** в списке Classifcation и нажмите **Edit** для редактирования параметра протокола.Диалоговое окно Edit Match Protocol Values

появляется.

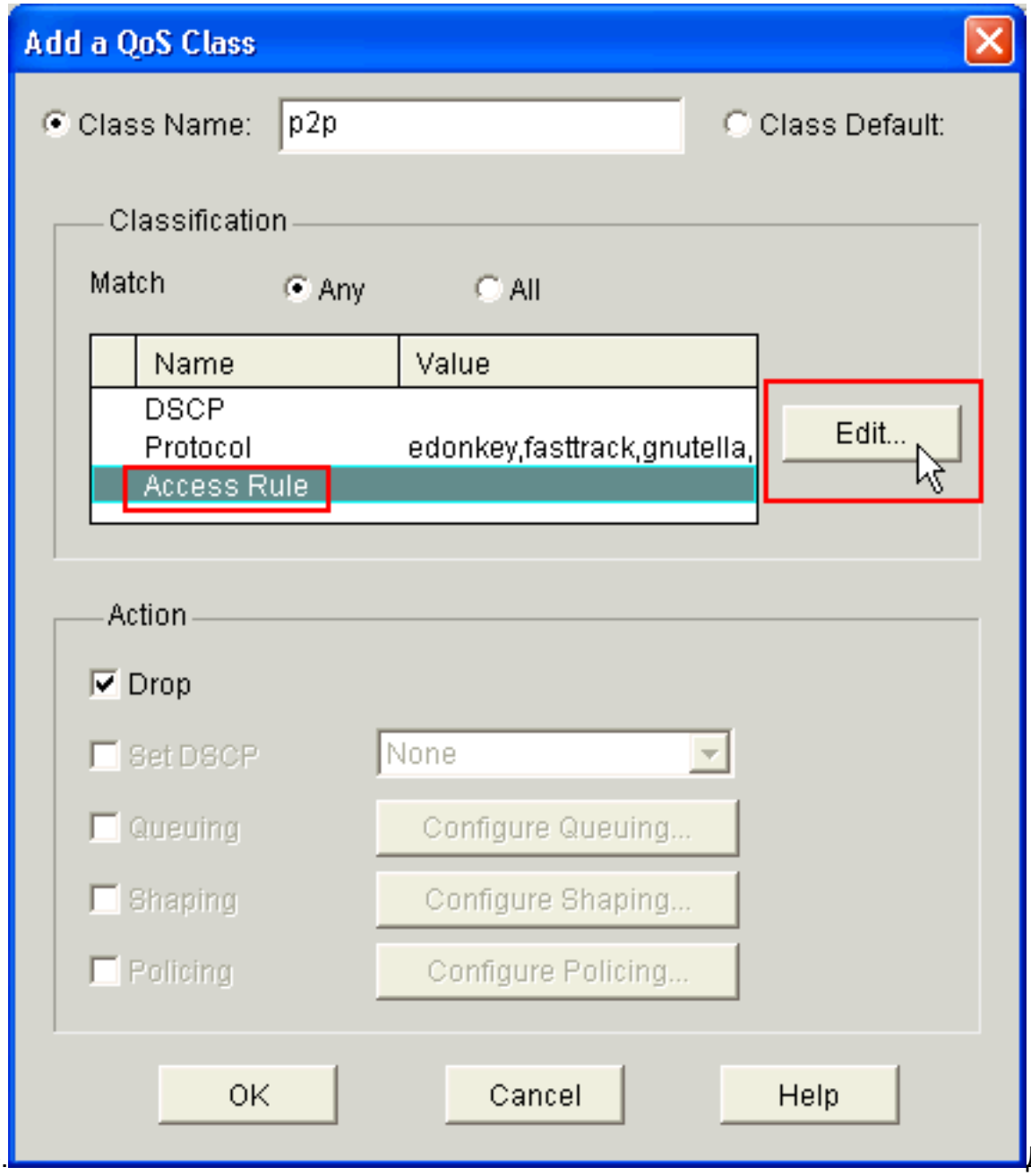


10. Из Доступного списка Значений протокола выберите каждый протокол P2P, который вы хотите заблокировать и нажать правую стрелку (**>>**) кнопка для перемещения каждого протокола в список Значений Выбранного протокола.**Примечание:** Для классификации трафика P2P с NBAR перейдите к Странице загрузки программного обеспечения и загрузите последнее программное обеспечение P2P Protocol Description Language Module (PDLM) и Файлы предварительных сведений. PDLM P2P доступные для скачивания включают WinMx, BitTorrent, Kazaa2, Gnutella, eDonkey, Fasttrack и Napster. В зависимости от вашего IOS вам, возможно, не понадобились бы последние версии PDLM, так как некоторые могли бы быть интегрированы в ваш IOS (например, Fasttrack и Napster). После того, как загруженный, скопируйте PDLM к флэш-памяти маршрутизатора и загрузите их в IOS путем настройки **ip nbar pdlm** *<flash_device>*: *<filename>* **.pdlm**. Выполните **команду show ip nbar pdlm**, чтобы гарантировать, что она была загружена успешно. После того, как загруженный, можно использовать их в операторах match protocol под конфигурацией карты классов.
11. **Нажмите кнопку**

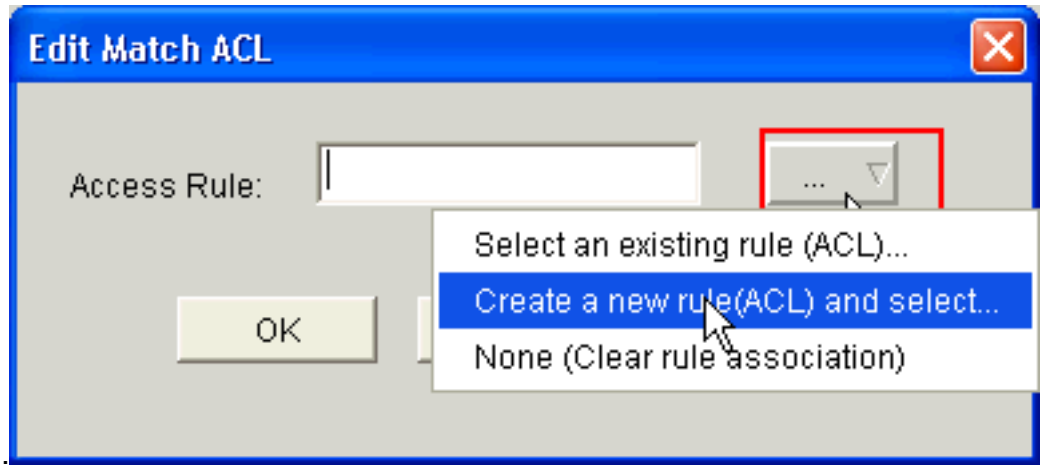


OK.

12. В диалоговом окне Add a QoS Class выберите **Access Rules** из списка Классификации и нажмите **Edit** для создания нового правила доступа. Можно также сопоставить существующее правило доступа с картой классов

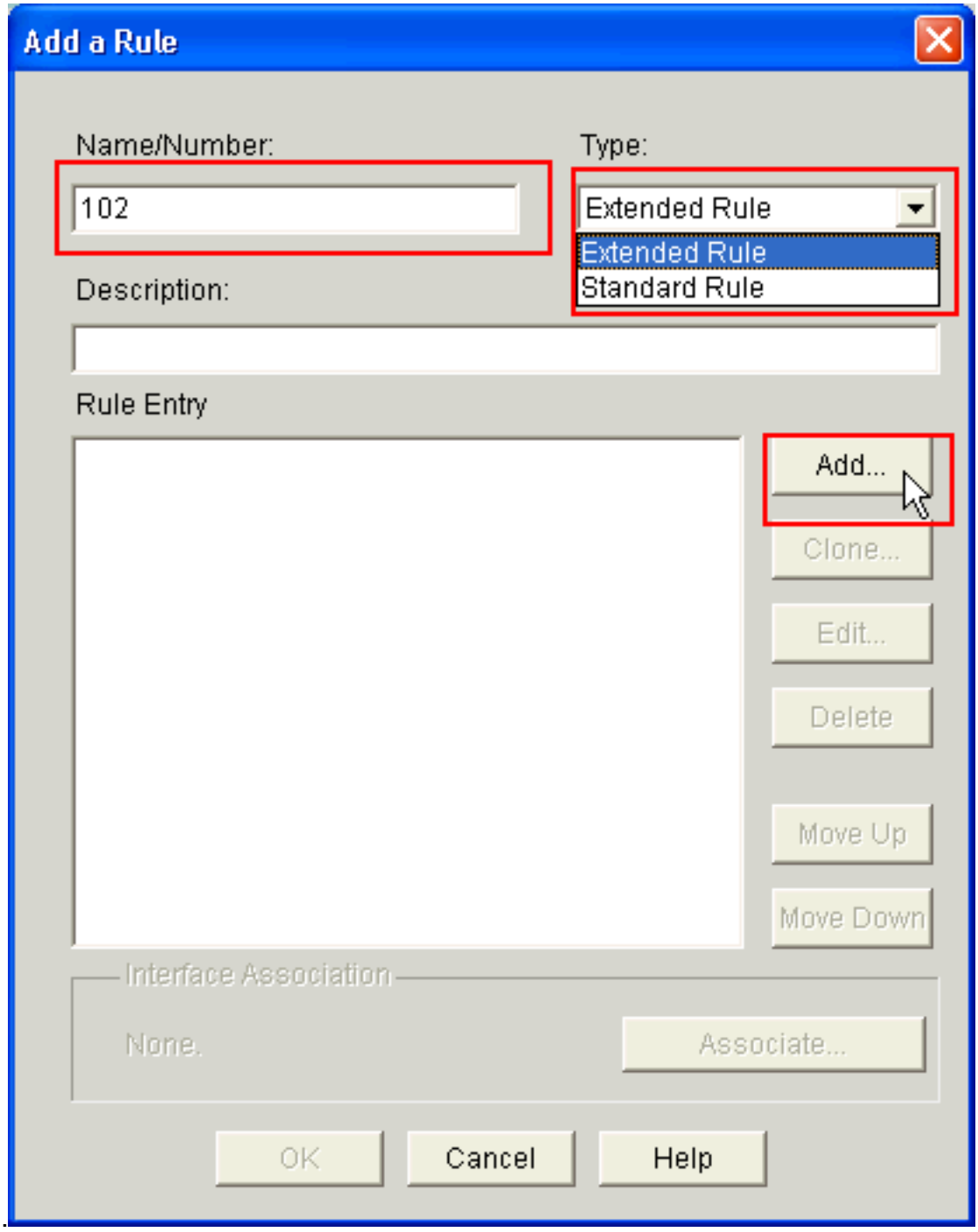


p2p.Диалоговое окно Edit Match ACL появляется.

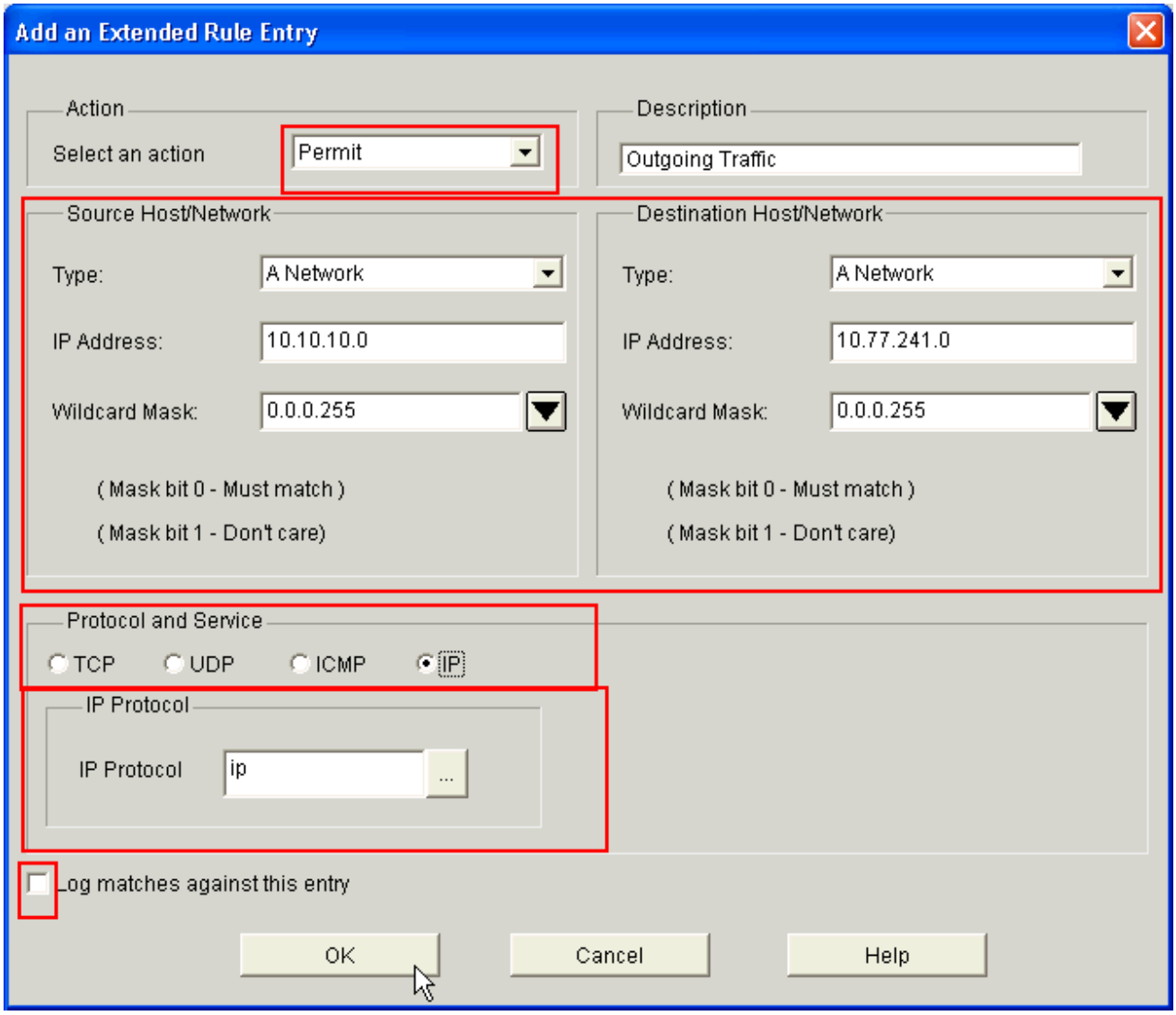


13. Нажмите кнопку Access Rule **(...)** и выберите нужный вариант. Данный пример создает новый ACL.Диалоговое окно Add a Rule

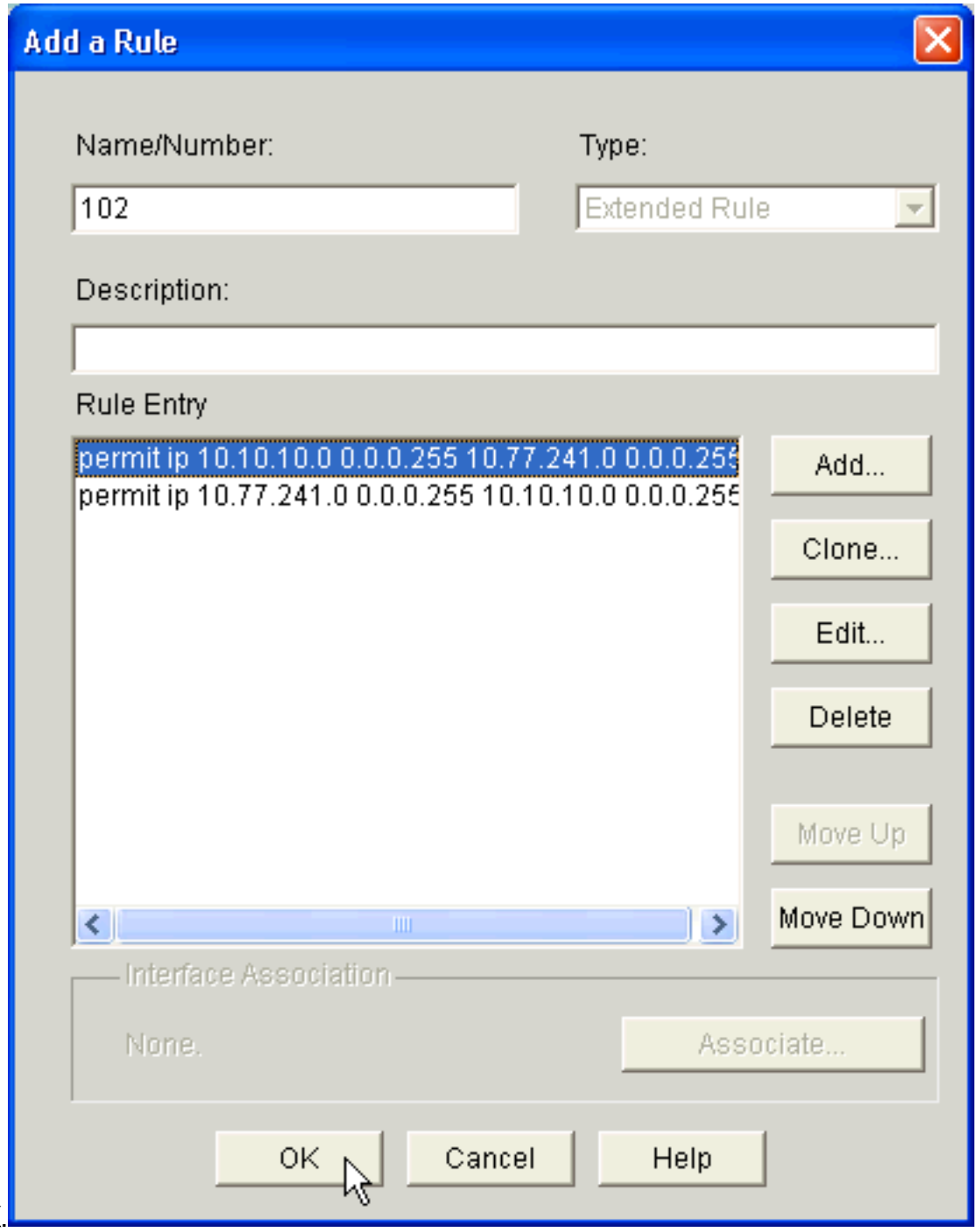
появляется.



14. В диалоговом окне Add a Rule введите имя или количество ACL, который будет создан на Название/Поле номера ACL.
15. От выпадающего списка Типа выберите тип ACL, который будет создан (или *Расширенное Правило* или *Стандартное Правило*).
16. **Нажмите Add** для добавления подробных данных к *ACL 102*.Добавление Расширенной коробки Диалогового окно Создать нового VPN-подключение Правила появляется.

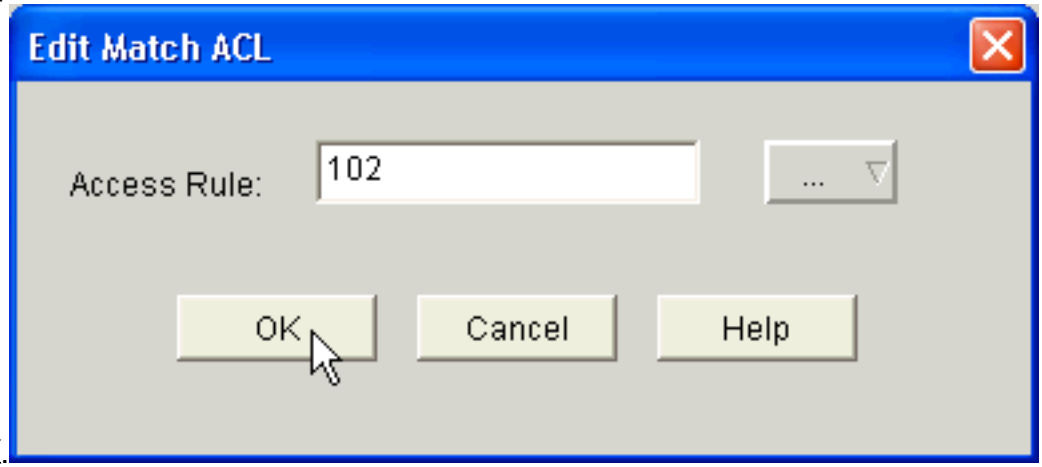


17. В Добавлении Расширенной коробки Диалогового окно Создать нового VPN-подключение Правила выберите действие (любой *Permit or Deny*) от Выбора выпадающий список действия, который указывает, должно ли правило списка прав доступа (ACL) permit or deny трафик между источником и сетями назначения. Это правило для исходящего потока данных от внутренней сети до внешней сети.
18. Введите информацию для источника и сетей назначения в Исходном хосте / Сеть и Адресат / Области сети соответственно.
19. В Протоколе и Области обслуживания, нажмите соответствующую кнопку с зависимой фиксацией. Данный пример использует IP.
20. Если вы хотите регистрировать соответствующие пакеты против этого правила списка прав доступа (ACL), проверьте **Регистрационные Соответствия против этого флажка entry**.
21. **Нажмите кнопку OK.**
22. В диалоговом окне Add a Rule нажмите



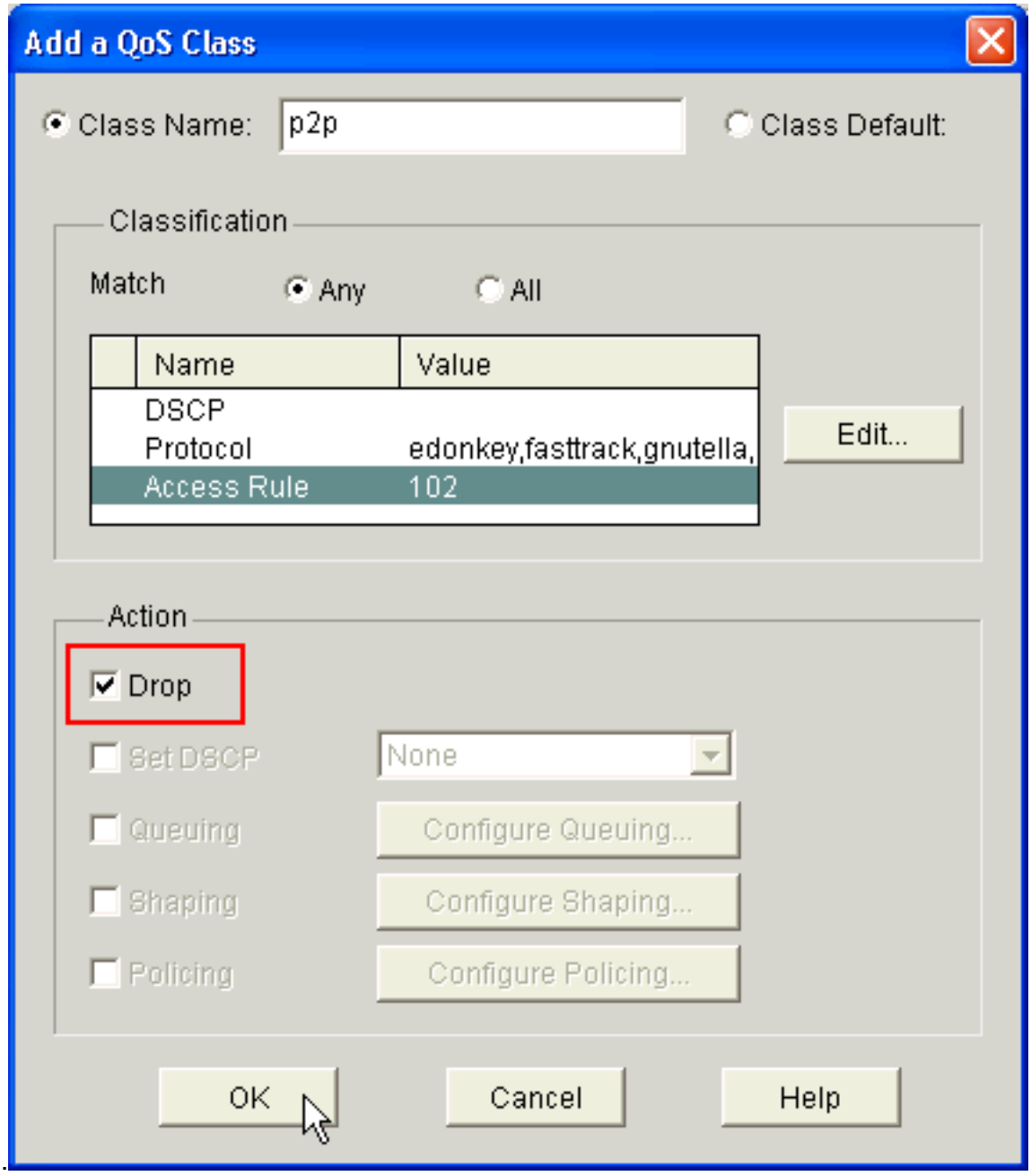
OK.

23. В диалоговом окне Edit Match ACL нажмите



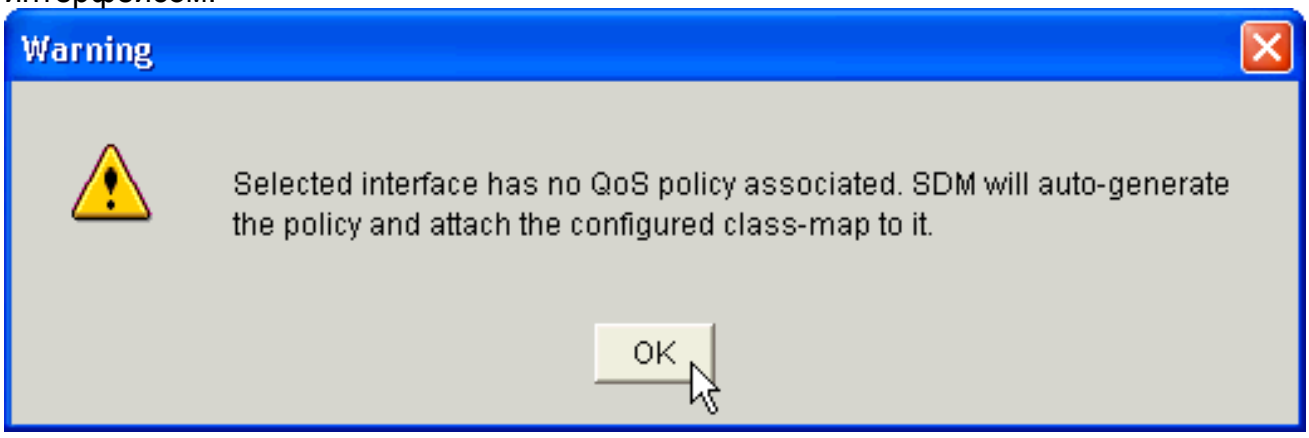
OK.

24. В диалоговом окне Add a QoS Class проверьте флажок **Drop**, чтобы вынудить маршрутизатор заблокировать трафик



P2P.

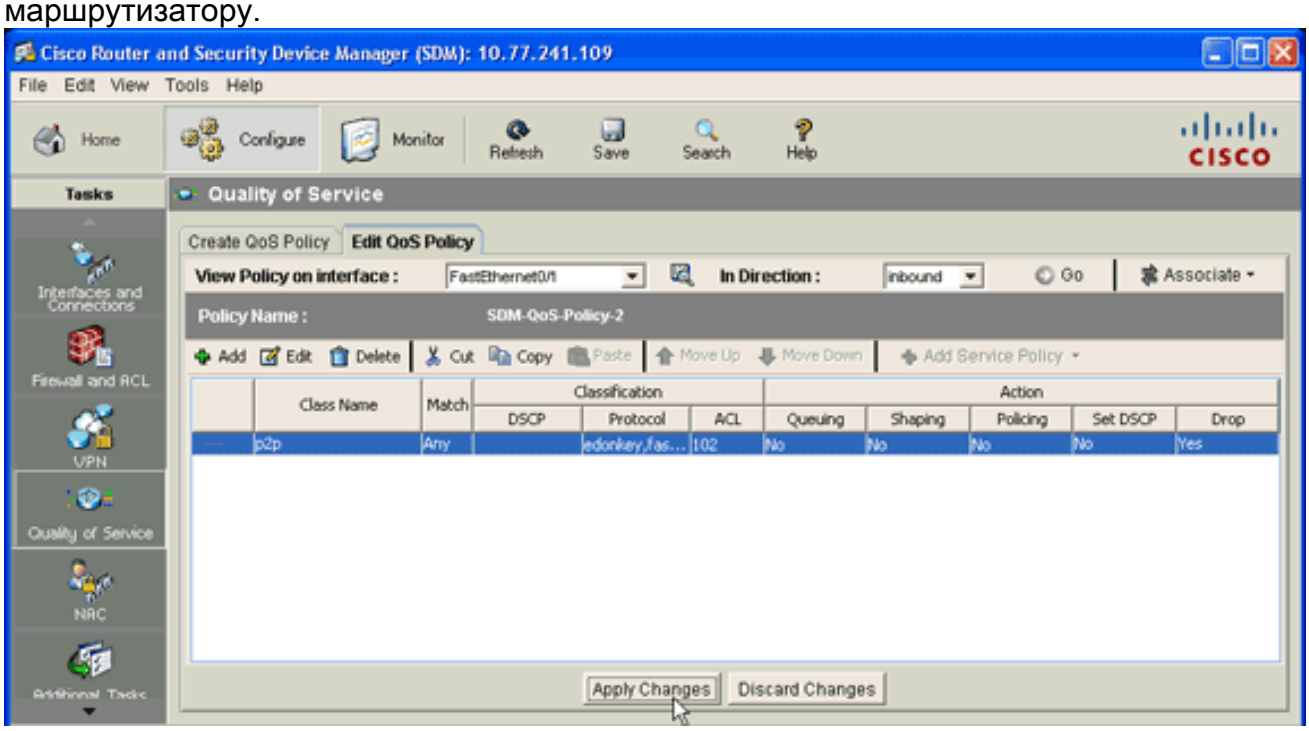
25. **Нажмите кнопку OK.**Следующее предупреждающее сообщение показывают по умолчанию, поскольку никакая политика QoS не сопоставлена с интерфейсом.



SDM автоматически сгенерирует политику QoS и подключит карту настроенного класса к политике. Интерфейс командной строки (CLI), эквивалентный из этого шага SDM-конфигурации:`R1(config)#`**`policy-map SDM-QoS-Policy-2`**
`R1(config-pmap)#`**`class p2p`**
`R1(config-pmap-c)#`**`drop`**

```
R1(config-pmap-c)#end
R1#
```

26. На вкладке Edit QoS Policy нажмите **Apply Changes** для отправки конфигурации маршрутизатору.



Межсетевой экран приложения — мгновенная функция осуществления трафика сообщений в версиях Cisco IOS 12.4 (4) T и позже

Мгновенное осуществление трафика сообщений

Межсетевой экран Приложения — Мгновенная функция Осуществления Трафика сообщений позволяет пользователям определить и принудить политику, которая задает, какие типы трафика пейджера позволены в сеть. Можно управлять множественными средствами рассылки (а именно, AOL, YAHOO и MSN) одновременно, когда настроено в **appfw политике** в соответствии с **приложением im.** Поэтому, следующая дополнительная функциональность может также быть принуждена:

- Конфигурация правил контроля межсетевого экрана
- Глубокая проверка пакетов информационного наполнения (ищущий сервисы, такие как текстовый чат)

Примечание: Функция Осуществления Трафика сообщений Момента межсетевого экрана приложения поддерживается в версиях Cisco IOS 12.4 (4) T и позже.

Правило приложений пейджера

Межсетевой экран приложения использует правило приложений, которое состоит из набора статических подписей, для обнаружения нарушений безопасности. Статическая подпись является набором параметров, которые задают условия протокола, которые нужно соблюдать, прежде чем меры приняты. Эти условия протокола и реакции определены конечным пользователем через CLI для формирования правила приложений.

Межсетевой экран приложения Cisco IOS был улучшен для поддержки мгновенных собственных правил приложений средства рассылки. Таким образом межсетевой экран Cisco IOS может теперь обнаружить и запретить подключения пользователя к серверам пейджера для Пейджера AOL (AIM), Yahoo! Messenger и служб мгновенных сообщений MSN Messenger. Эта функциональность управляет всеми соединениями для поддерживаемых сервисов, включая текст, голос, видео и возможности передачи файла. Эти три ходатайства могут быть индивидуально отклонены или разрешены. Каждый сервис может индивидуально управляться так, чтобы сервис текстового чата был позволен, и голос, передача файла, видео, и другие сервисы ограничены. Эта функциональность увеличивает возможность контроля существующего приложения управлять трафиком приложения пейджера (IM), который был замаскирован как HTTP (сеть) трафик. См. Межсетевой экран Приложения - Мгновенное Осуществление Трафика сообщений для получения дополнительной информации.

Примечание: Если приложение IM заблокировано, соединение перезагружено, и сообщение системного журнала генерируется, как соответствующее.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- show ip nbar pdlm — Для отображения PDLM в использовании NBAR используйте **команду show ip nbar pdlm** в привилегированном режиме EXEC:`Router#`**`show ip nbar pdlm`**

```
The following PDLMs have been loaded:
flash://edonkey.pdlm
flash://fasttrack.pdlm
flash://gnutella.pdlm
flash://kazaa2.pdlm
```

- show ip nbar version — Для отображения информацию о версии программного обеспечения NBAR в Cisco IOS Release или версии PDLM NBAR на маршрутизаторе Cisco IOS, используйте **команду show ip nbar version** в привилегированном режиме EXEC:`R1#`**`show ip nbar version`**

```
NBAR software version:  6

1   base                 Mv: 2
2   ftp                  Mv: 2
3   http                 Mv: 9
4   static               Mv: 6
5   tftp                 Mv: 1
6   exchange             Mv: 1
7   vdolive              Mv: 1
8   sqlnet               Mv: 1
9   rcmd                 Mv: 1
10  netshow              Mv: 1
11  sunrpc               Mv: 2
12  streamwork           Mv: 1
13  citrix               Mv: 10
14  fasttrack            Mv: 2
15  gnutella             Mv: 4
16  kazaa2               Mv: 7
```

```
17  custom-protocols     Mv: 1
18  rtsp                 Mv: 4
19  rtp                  Mv: 5
20  mgcp                 Mv: 2
21  skinny               Mv: 1
22  h323                 Mv: 1
23  sip                  Mv: 1
24  rtcp                 Mv: 2
25  edonkey              Mv: 5
26  winmx                Mv: 3
27  bittorrent           Mv: 4
28  directconnect        Mv: 2
29  skype                Mv: 1


{<No.>}<PDLM name> Mv: <PDLM Version>, {Nv: <NBAR Software Version>; <File name>
}{Iv: <PDLM Interdependency Name>   - <PDLM Interdependency Version>}
```

- show policy-map interface Для отображения пакетной статистики всех классов, которые настроены для всей политики обслуживания или на заданном интерфейсе или на подинтерфейсе или на определенной постоянной виртуальной цепи (PVC) на интерфейсе, используют **команду show policy-map interface** в привилегированном режиме EXEC:`R1#show policy-map interface fastEthernet 0/1`

```
 FastEthernet0/1

  Service-policy input: SDM-QoS-Policy-2

    Class-map: p2p (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol edonkey
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol fasttrack
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol gnutella
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol kazaa2
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol winmx
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: access-group 102
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol skype
        0 packets, 0 bytes
        5 minute rate 0 bps
      drop

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

- **show running-config policy-map** Для отображения всех конфигураций карты политик, а также конфигурации карты политики по умолчанию, используйте **команду show running-config policy-map**:`R1#show running-config policy-map`

```
Building configuration...
```

```
Current configuration : 57 bytes
!
policy-map SDM-QoS-Policy-2
 class p2p
   drop
!
end
```

- **show running-config class-map** — Для отображения информации о конфигурации карты классов используйте **команду show running-config class-map**:`R1#show running-config class-map`

```
Building configuration...

Current configuration : 178 bytes
!
class-map match-any p2p
 match protocol edonkey
 match protocol fasttrack
 match protocol gnutella
 match protocol kazaa2
 match protocol winmx
 match access-group 102
!
end
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **show access-list** — Для отображения accesslist конфигурации, которая работает на маршрутизаторе Cisco IOS, используйте команду **show access-list**:`R1#show access-lists`

```
Extended IP access list 102
    10 permit ip 10.10.10.0 0.0.0.255 10.77.241.0 0.0.0.255
    20 permit ip 10.77.241.0 0.0.0.255 10.10.10.0 0.0.0.255
```

Дополнительные сведения

- Руководство по конфигурации безопасности Cisco IOS, выпуск, с 12.4 поддержкой
- Сетевое распознавание приложений (NBAR)
- Cisco Express Forwarding (CEF)
- Cisco Systems – техническая поддержка и документация