ASA/PIX 8.x: Блокировать определенные веб-сайты (URL) с помощью регулярных выражений в примере конфигурации MPF

Содержание

Введение

В настоящем документе описывается настройка защитных устройств Cisco ASA/PIX 8.x с применением регулярных выражений и системы модульных политик (Modular Policy Framework, MPF) для блокировки/разрешения определенных web-сайтов (URL-адресов).

Примечание: Эта конфигурация не блокирует все загрузки приложений. Для надежного блокирования файлов нужно использовать либо отдельное устройство, например Ironport серии S, либо модуль, например модуль CSC для ASA.

Примечание: Фильтрация HTTPS не поддерживается на ASA. В случае HTTPS устройство ASA не имеет возможности выполнять глубокий анализ пакетов или анализ трафика на основе регулярных выражений, поскольку в трафике HTTPS содержимое пакетов шифруется (SSL).

Предварительные условия

Требования

В данном документе предполагается, что устройство защиты Cisco корректно настроено и работает нормально.

Используемые компоненты

- Устройство адаптивной защиты Cisco серии 5500 (ASA), на котором установлена версия ПО 8.0(x) или более поздняя
- Cisco Adaptive Security Device Manager (ASDM) версии 6.x для ASA 8.x

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

Рассматриваемая конфигурация также может использоваться для устройств Cisco PIX серии 500, работающих под управлением ПО версии 8.0(x) или более поздней версии.

Условные обозначения

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

Общие сведения

Обзор модульной системы политик

Модульная система политик (MPF) обеспечивает гибкий способ настройки параметров устройств защиты. Например, MPF можно использовать для создания конфигурации с ограничением по времени, которая является специфичной для определенного TCP-приложения, в отличие от конфигураций, применимых ко всем TCP-приложениям.

MPF поддерживает функции, перечисленные ниже:

- Нормализация TCP, ограничение числа и продолжительности TCP- и UDP-подключений, а также рандомизация порядкового номера TCP
- CSC
- Контроль трафика на прикладном уровне
- IPS
- Входной контроль QoS
- Выходной контроль QoS
- Очередь с приоритетом QoS

Настройка MPF включает следующие 4 задачи:

1. Определение трафика уровней 3 и 4, для которого требуется применить действия. Подробную информацию см. в документе Определение трафика с использованием

карты классов уровней 3/4.

2. (Только при анализе трафика приложений) Определение специальных действий, необходимых для анализа трафика на прикладном уровне. Подробную информацию см. в документе Задание специальных действий для анализа трафика на прикладном уровне.
3. Применение действий к трафику 3-го и 4-го уровней. Подробную информацию см. в документе Определение действий с использованием карты политик уровней 3/4.
4. Активация действий на интерфейсе. Подробную информацию см. в документе Применение политики уровня 3/4 к интерфейсу с использованием служебной политики.

Регулярные выражения

Регулярное выражение либо точно соответствует текстовой строке, либо допускает использование метасимволов, позволяя совмещать различные варианты текстовой строки. Регулярные выражения можно использовать для выявления трафика определенных приложений, например, с их помощью можно распознавать строку URL-адреса в пакете HTTP.

Примечание: Используйте **Ctrl+V** для выхода изо всех специальных символов в CLI, таких как вопросительный знак (?) или вкладка. **Например, используйте комбинацию d[Ctrl+V]g, чтобы ввести в конфигурацию d?g.**

Для создания регулярного выражения используется команда regex, применяемая в различных функциях, требующих сравнения текста. Например, можно задать специальные действия для контроля приложения с использованием MPF и карты политик анализа. **Для получения подробной информации см. команду policy-map type inspect. На карте политик анализа можно задать трафик, используемый при создании карты классов анализа, которая содержит одну или несколько команд match. Можно также использовать команды match непосредственно в карте политик анализа. Некоторые команды match позволяют идентифицировать текст в пакете HTTP, используя регулярное выражение.** Можно группировать регулярные выражения в соответствующую карту класса. **Для получения подробной информации см. команду class-map type regex.**

Следующая таблица содержит список метасимволов, имеющих специальное значение.

Символ	Описание	Примечания
.	Точка	Соответствует любому одиночному символу. **Например, выражению d.g соответствуют слова dog, dag, dtg, а также любое слово, содержащее эти символы, например doggonnit.**
(exp)	Вложенное выражение	Вложенное выражение отделяет символы от окружающего текста, позволяя использовать внутри скобок другие метасимволы. **Например, выражению d(o|a)g соответствуют слова dog и dag, в то время как выражению do|ag соответствуют do и ag.** Вложенные выражения могут также

		использоваться с кванторами повторения для указания числа повторяющихся знаков. **Например, выражению ab(xy){3}z удовлетворяет последовательность abxyxyxyz.**
|	Дизъюнкция	Соответствует любому из разделенных им выражений. **Например, выражению dog|cat удовлетворяет как слово dog, так и слово cat.**
?	Вопросительный знак	Квантор, указывающий, что предшествующее ему выражение может встречаться 0 или 1 раз. **Например, выражению lo?se соответствуют строки lse и lose. Примечание:** Необходимо ввести **Ctrl+V**, и затем вопросительный знак или иначе функция справки вызваны.
*	Звездочка	Квантор, указывающий, что предшествующее ему выражение может встречаться 0, 1 или произвольное число раз. **Например, выражению lo*se соответствуют строки lse, lose, loose и т. д.**
x	Квантор повторения	Повторяет символы ровно x раз. **Например, выражению ab(xy){3}z удовлетворяет последовательность abxyxyxyz.**
x	Квантор минимального повторения	Повторяет символы не менее x раз. **Например, выражению ab(xy){2,}z удовлетворяют последовательности abxyxyz, abxyxyxyz и т. д.**
A B C	Класс символа	Соответствует любому символу в квадратных скобках. **Например, выражению [abc] удовлетворяют символы a, b и c.**
[^abc]	Отрицание класса символа	Соответствует одному символу, не содержащемуся в квадратных скобках. **Например, выражению [^abc] удовлетворяет любой из знаков, кроме a, b и c. [^A-Z] соответствует любому одиночному знаку, который не является латинской буквой в верхнем регистре.**
[a-c]	Класс диапазона символов	Соответствует любому символу в определенном диапазоне. **[a-z] соответствует любой букве в**

		нижнем регистре. Символы и диапазоны можно сочетать: **[abcq-z] соответствует знакам a, b, c, q, r, s, t, u, v, w, x, y, z, как и выражение [a-cq-z].** Внутри квадратных скобок знак тире (-) воспринимается как таковой только в том случае, если он стоит первым или последним: **[abc-] или [-abc].**
""	Кавычки	Позволяют указать пробелы в начале или конце строк. **Например, выражение " test" обрабатывается с учетом стоящего в начале пробела.**
^	Вставка	Указывает, что выражение должно начинаться с начала строки
\	Обратная косая черта	В сочетании с метасимволом указывает, что последний должен восприниматься как обычный символ. **Например, выражению \[соответствует открывающая квадратная скобка.**
char	Символ	Если знак не является метасимволом, он воспринимается как обычный символ.
\r	Возврат каретки	Соответствует символу возврату каретки (0x0d)
\n	Новая строка	Соответствует символу перевода строки (0x0a)
T	Вкладка	Соответствует табулятору (0x09)
_____ F	Новая страница	Соответствует символу новой страницы (0x0c)
\xNN	Шестнадцатеричная нумерация	Соответствует символу ASCII с указанным кодом в шестнадцатеричном виде (код должен содержать строго две цифры)
\NNN	Восьмеричная нумерация	Соответствует символу ASCII с указанным кодом в восьмеричном виде (код должен содержать строго три цифры). Например, код 040 соответствует пробелу.

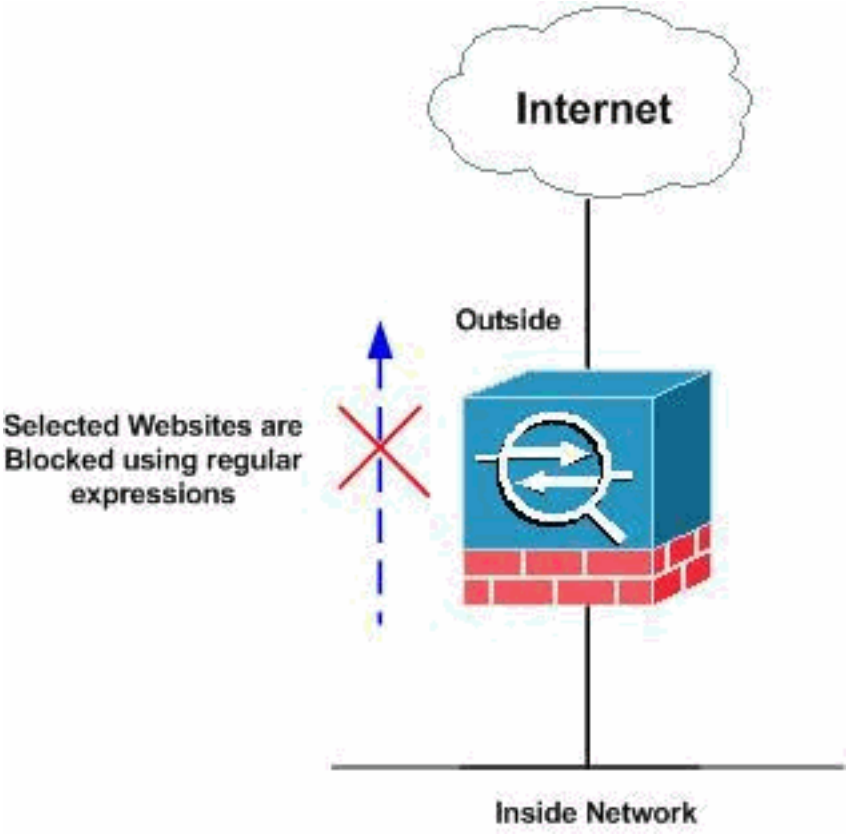
Настройка

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:



Конфигурации

Эти конфигурации используются в данном документе:

- Конфигурация ASA в интерфейсе командной строки
- Конфигурация ASA 8.x с ASDM 6.x

Конфигурация ASA в интерфейсе командной строки

Конфигурация ASA в интерфейсе командной строки

```
ciscoasa#show running-config : Saved : ASA Version
8.0(2) ! hostname ciscoasa domain-name
default.domain.invalid enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.5 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 90 ip address
10.77.241.142 255.255.255.192 ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
regex urllist1
".*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt])
HTTP/1.[01]" !--- Extensions such as .exe, .com, .bat to
be captured and !--- provided the http version being
used by web browser must be either 1.0 or 1.1 regex
urllist2 ".*\.([Pp][Ii][Ff]|[Vv][Bb][Ss]|[Ww][Ss][Hh])
```

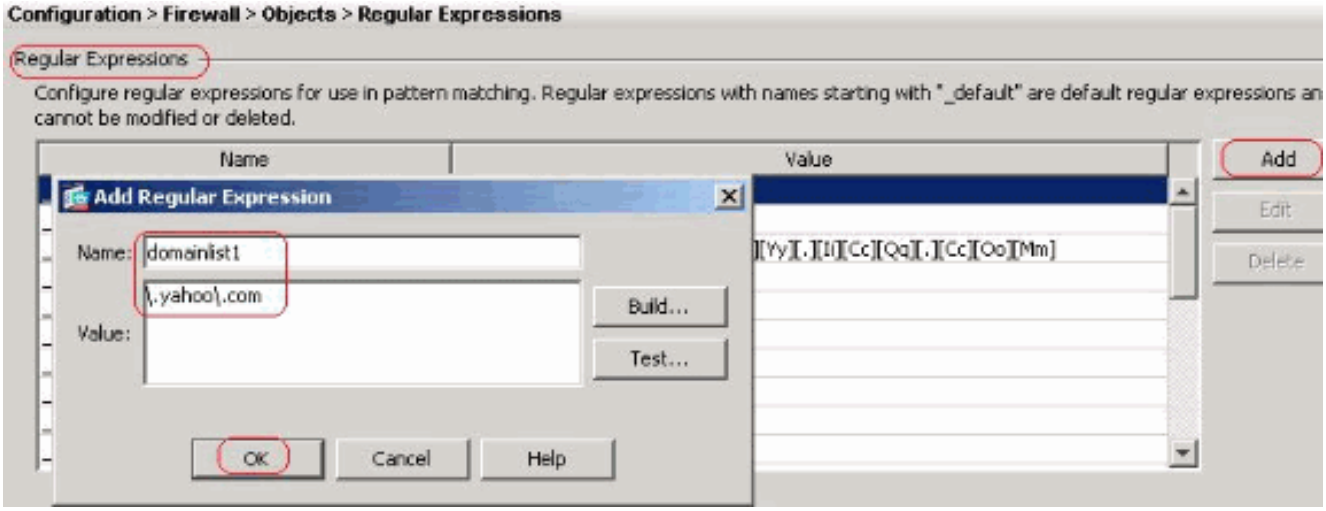
```
HTTP/1.[01]" !--- Extensions such as .pif, .vbs, .wsh to be captured !--- and provided the http version being used by web browser must be either !--- 1.0 or 1.1 regex urllist3 ".*\.([Dd][Oo][Cc]|[Xx][Ll][Ss]|[Pp][Pp][Tt]) HTTP/1.[01]" !--- Extensions such as .doc(word), .xls(ms-excel), .ppt to be captured and provided !--- the http version being used by web browser must be either 1.0 or 1.1 regex urllist4 ".*\.([Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz]) HTTP/1.[01]" !--- Extensions such as .zip, .tar, .tgz to be captured and provided !--- the http version being used by web browser must be either 1.0 or 1.1 regex domainlist1 "\.yahoo\.com" regex domainlist2 "\.myspace\.com" regex domainlist3 "\.youtube\.com" !--- Captures the URLs with domain name like yahoo.com, !--- youtube.com and myspace.com regex contenttype "Content-Type" regex applicationheader "application/.*" !--- Captures the application header and type of !--- content in order for analysis boot system disk0:/asa802-k8.bin ftp mode passive dns server-group DefaultDNS domain-name default.domain.invalid access-list inside_mpc extended permit tcp any any eq www access-list inside_mpc extended permit tcp any any eq 8080 !--- Filters the http and port 8080 !--- traffic in order to block the specific traffic with regular !--- expressions pager lines 24 mtu inside 1500 mtu outside 1500 mtu DMZ 1500 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400 route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1 timeout xlate 3:00:00 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 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0 DMZ no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart no crypto isakmp nat-traversal telnet timeout 5 ssh timeout 5 console timeout 0 threat-detection basic-threat threat-detection statistics access-list ! class-map type regex match-any DomainBlockList match regex domainlist1 match regex domainlist2 match regex domainlist3 !--- Class map created in order to match the domain names !--- to be blocked class-map type inspect http match-all BlockDomainsClass match request header host regex class DomainBlockList !--- Inspect the identified traffic by class !--- "DomainBlockList". class-map type regex match-any URLBlockList match regex urllist1 match regex urllist2 match regex urllist3 match regex urllist4 !--- Class map created in order to match the URLs !--- to be blocked class-map inspection_default match default-inspection-traffic class-map type inspect http match-all AppHeaderClass match response header regex contenttype regex applicationheader !--- Inspect the captured traffic by regular !--- expressions "content-type" and "applicationheader". class-map httptraffic match access-list inside_mpc !--- Class map created in order to match the !--- filtered traffic by ACL class-map type inspect http match-all BlockURLsClass match request uri regex class URLBlockList ! !--- Inspect the identified traffic by class !--- "URLBlockList". ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512
```

```
policy-map type inspect http http_inspection_policy
parameters protocol-violation action drop-connection
class AppHeaderClass drop-connection log match request
method connect drop-connection log class
BlockDomainsClass reset log class BlockURLsClass reset
log !--- Define the actions such as drop, reset or log
!--- in the inspection policy map. policy-map
global_policy class inspection_default inspect dns
preset_dns_map 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 policy-map
inside-policy class httptraffic inspect http
http_inspection_policy !--- Map the inspection policy
map to the class !--- "httptraffic" under the policy map
created for the !--- inside network traffic. ! service-
policy global_policy global service-policy inside-policy
interface inside !--- Apply the policy to the interface
inside where the websites are blocked. prompt hostname
context Cryptochecksum:e629251a7c37af205c289cf78629fc11
: end ciscoasa#
```

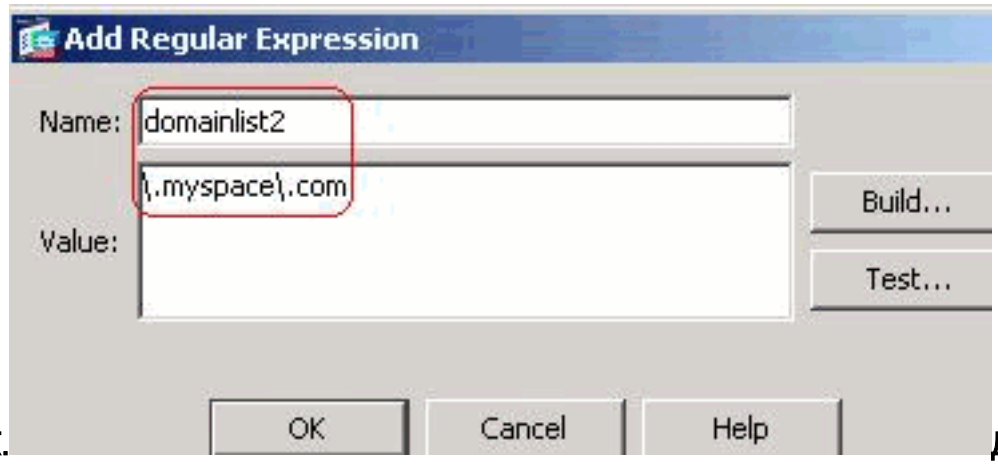
Конфигурация ASA 8.x с ASDM 6.x

Чтобы задать регулярные выражения и применить их к MPF для блокирования определенных web-сайтов, выполните следующие шаги.

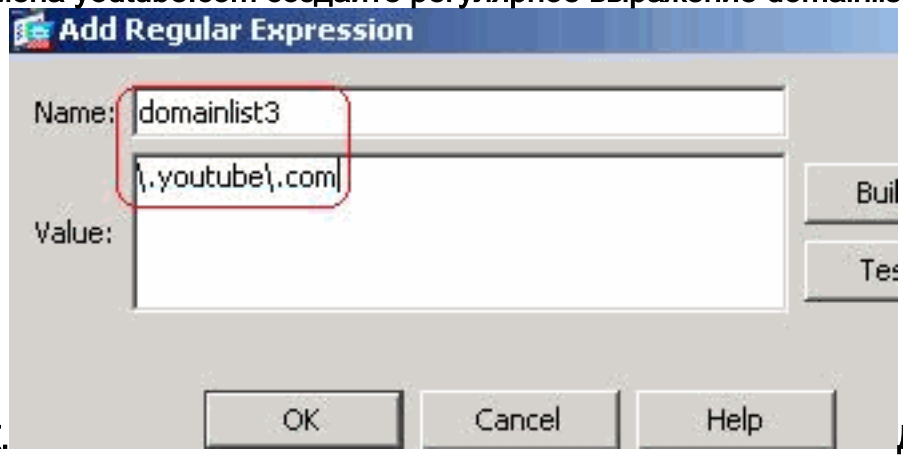
1. **Создание регулярных выраженийДля создания регулярного выражения на основе показанных примеров выберите Configuration > Firewall > Objects > Regular Expressions (Конфигурация > Межсетевой экран > Объекты > Регулярные выражения) и нажмите Add (Добавить) на вкладке Regular Expression.Для перехвата имени домена yahoo.com создайте регулярное выражение domainlist1. Нажмите кнопку ОК.**



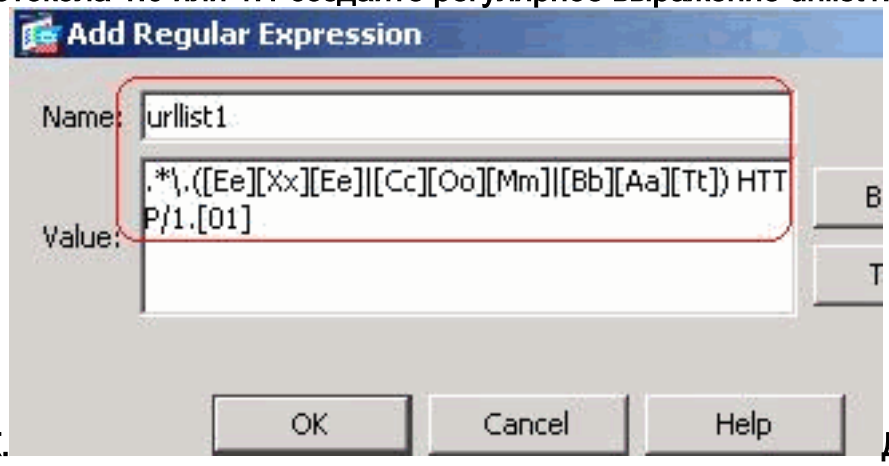
Для перехвата имени домена myspace.com создайте регулярное выражение domainlist2. Нажмите кнопку



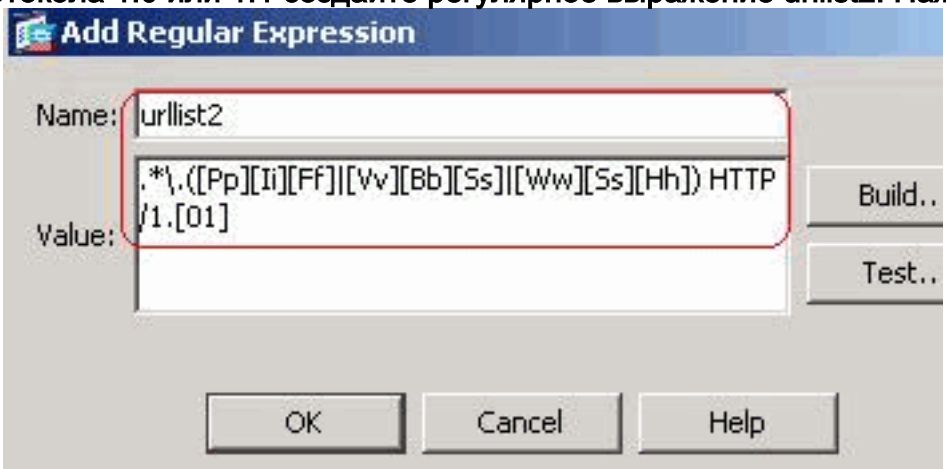
OK. Для перехвата имени домена youtube.com создайте регулярное выражение domainlist1. Нажмите



кнопку OK. Для перехвата расширений файлов exe, com и bat при условии использования web-браузером версии протокола 1.0 или 1.1 создайте регулярное выражение urllist1. Нажмите кнопку

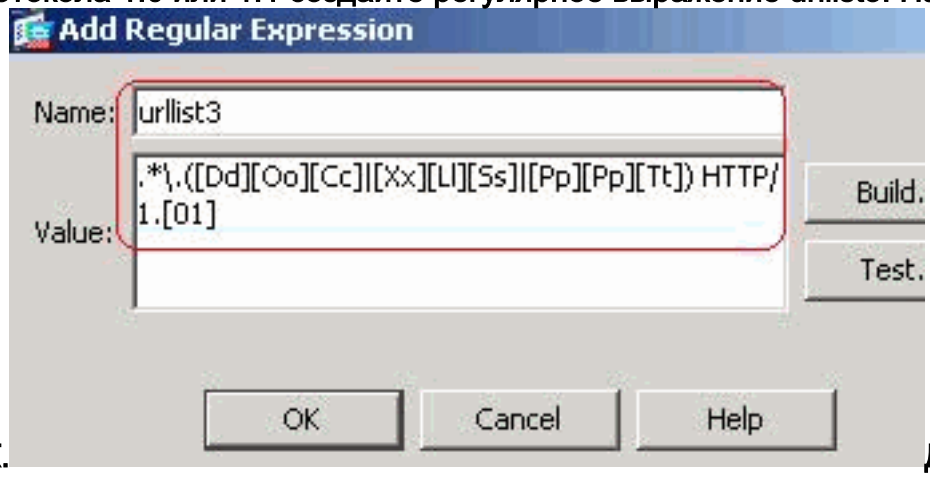


OK. Для перехвата расширений файлов pif, vbs и wsh при условии использования web-браузером версии протокола 1.0 или 1.1 создайте регулярное выражение urllist2. Нажмите кнопку

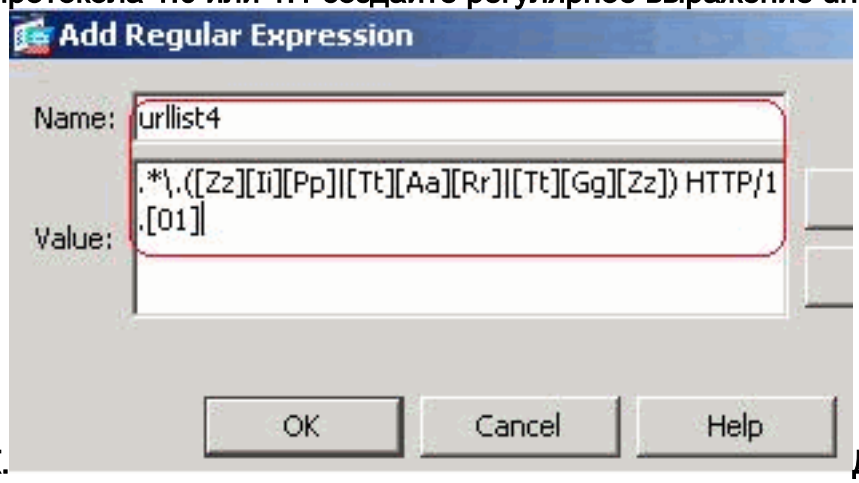


OK. Для перехвата

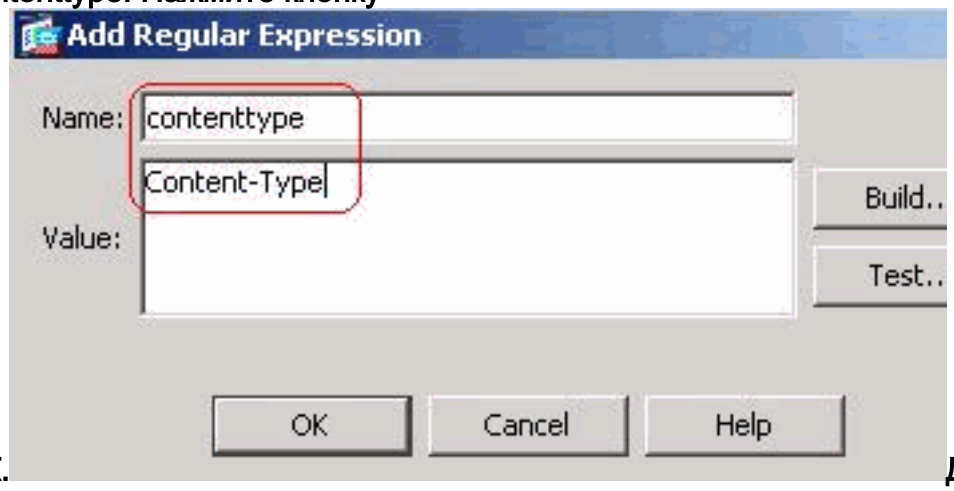
расширений файлов doc, xls и ppt при условии использования web-браузером версии протокола 1.0 или 1.1 создайте регулярное выражение urllist3. Нажмите кнопку



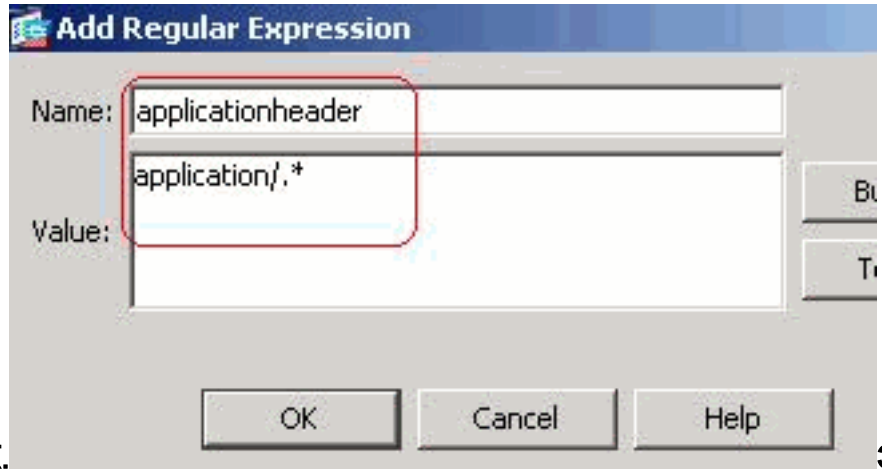
OK. Для перехвата расширений файлов (например, zip, tar и tgz) при условии использования web-браузером версии протокола 1.0 или 1.1 создайте регулярное выражение urllist4.



Нажмите кнопку OK. Для перехвата идентификатора типа содержимого создайте регулярное выражение contenttype. Нажмите кнопку

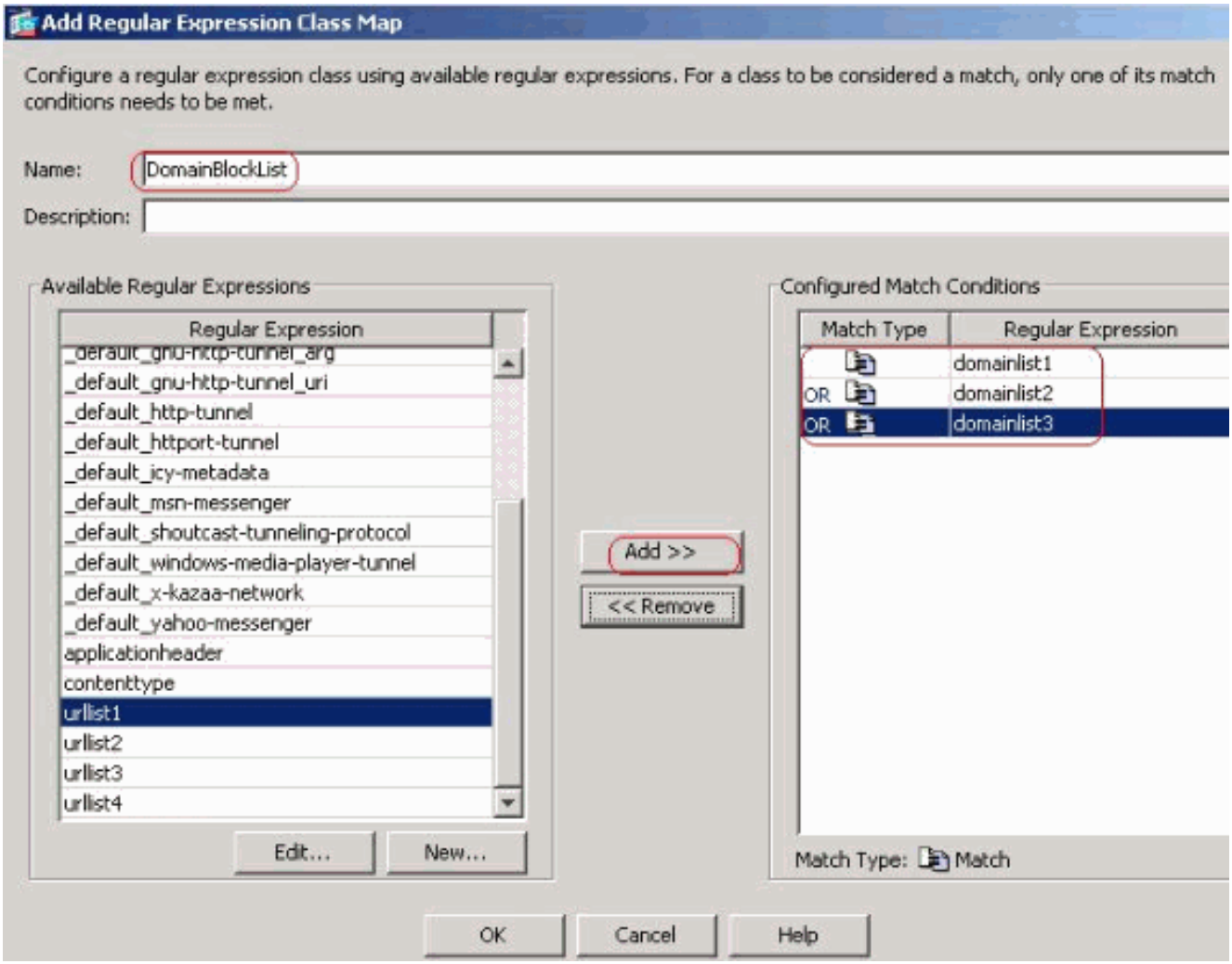


OK. Для перехвата заголовков различных приложений содержимого создайте регулярное выражение applicationheader. Нажмите кнопку

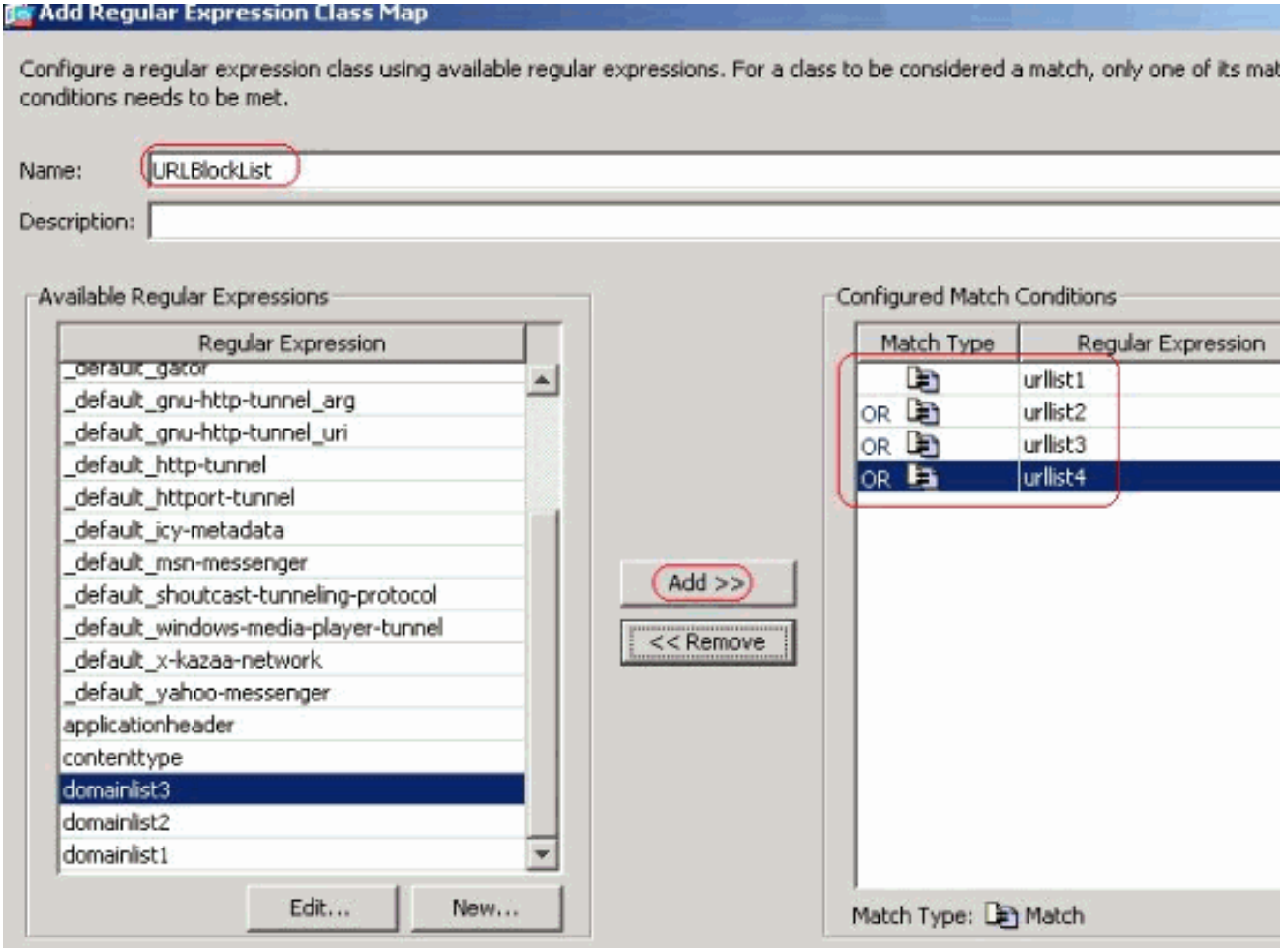


OK. Эквивалентная конфигурация в интерфейсе командной строки

2. Создание классов регулярных выраженийДля создания различных показанных классов выберите Configuration > Firewall > Objects > Regular Expressions (Конфигурация > Межсетевой экран > Объекты > Регулярные выражения) и нажмите Add (Добавить) на вкладке Regular Expression Classes.Для перехвата совпадений с любым из регулярных выражений domainlist1, domainlist2 и domainlist3 создайте класс регулярных выражений DomainBlockList. Нажмите кнопку
OK.

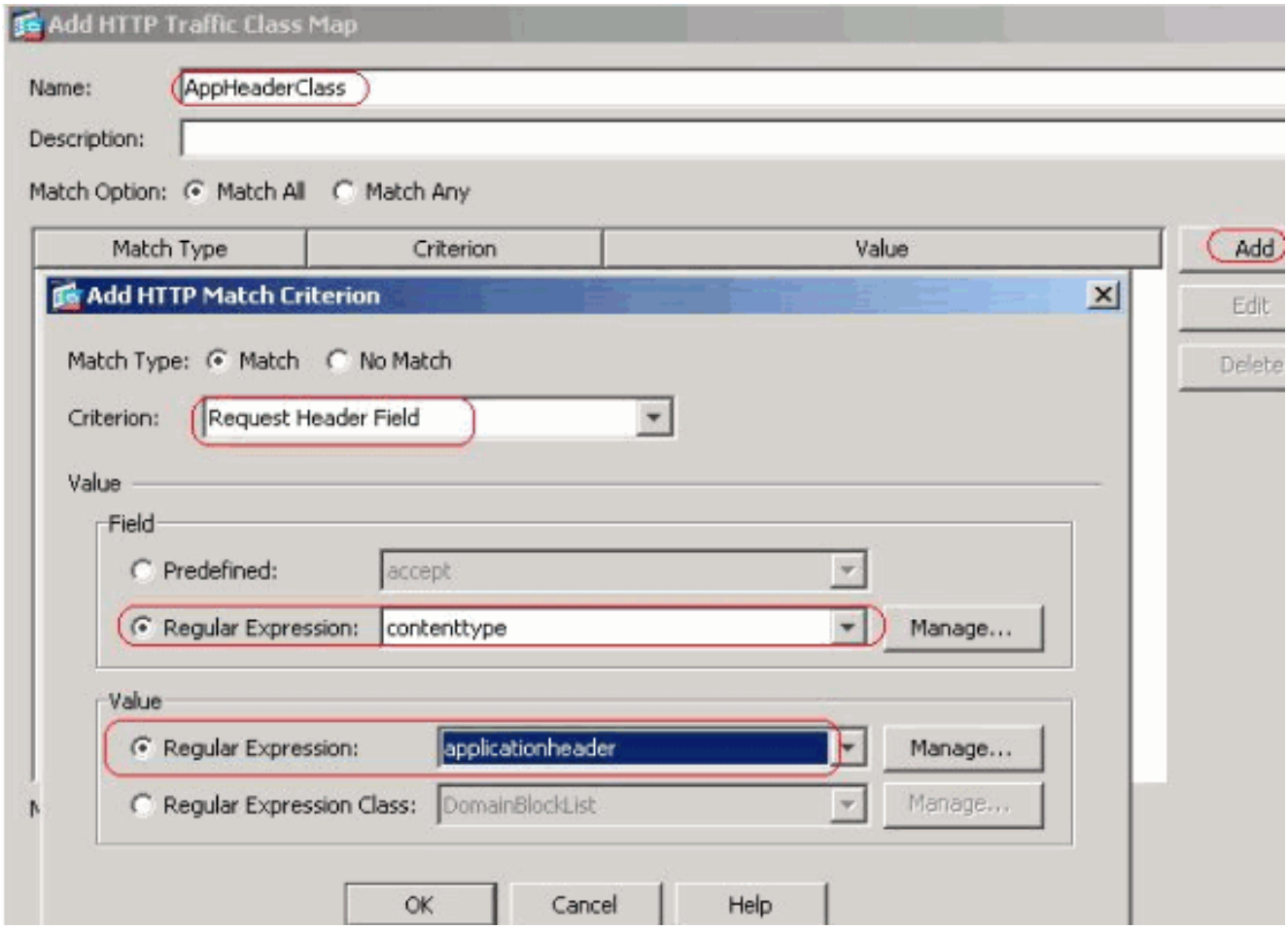


Для перехвата совпадений с любым из регулярных выражений urllist1, urllist2, urllist3 и urllist4 создайте класс регулярных выражений URLBlockList. Нажмите кнопку
OK.

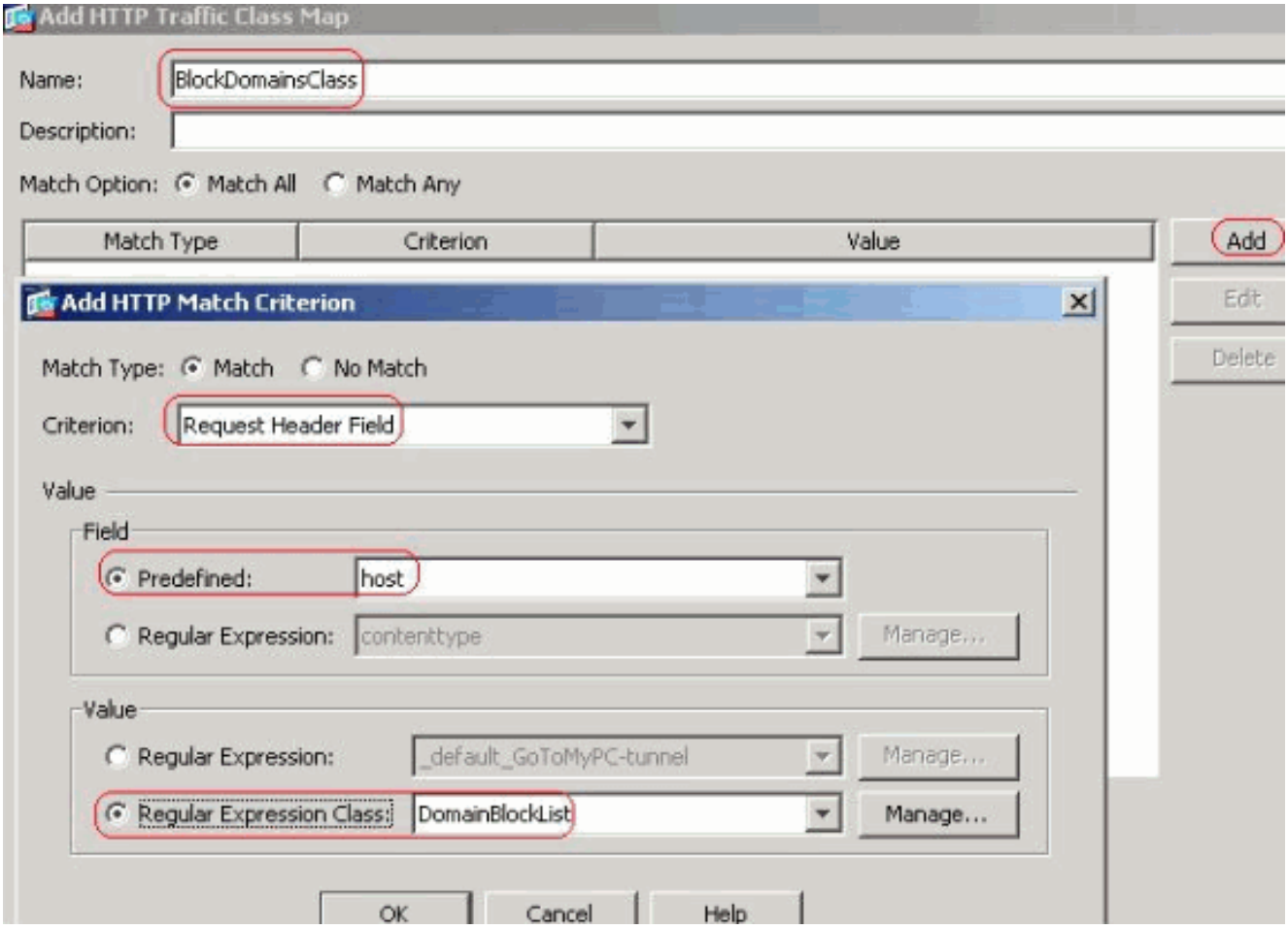


Эквивалентная конфигурация в интерфейсе командной строки

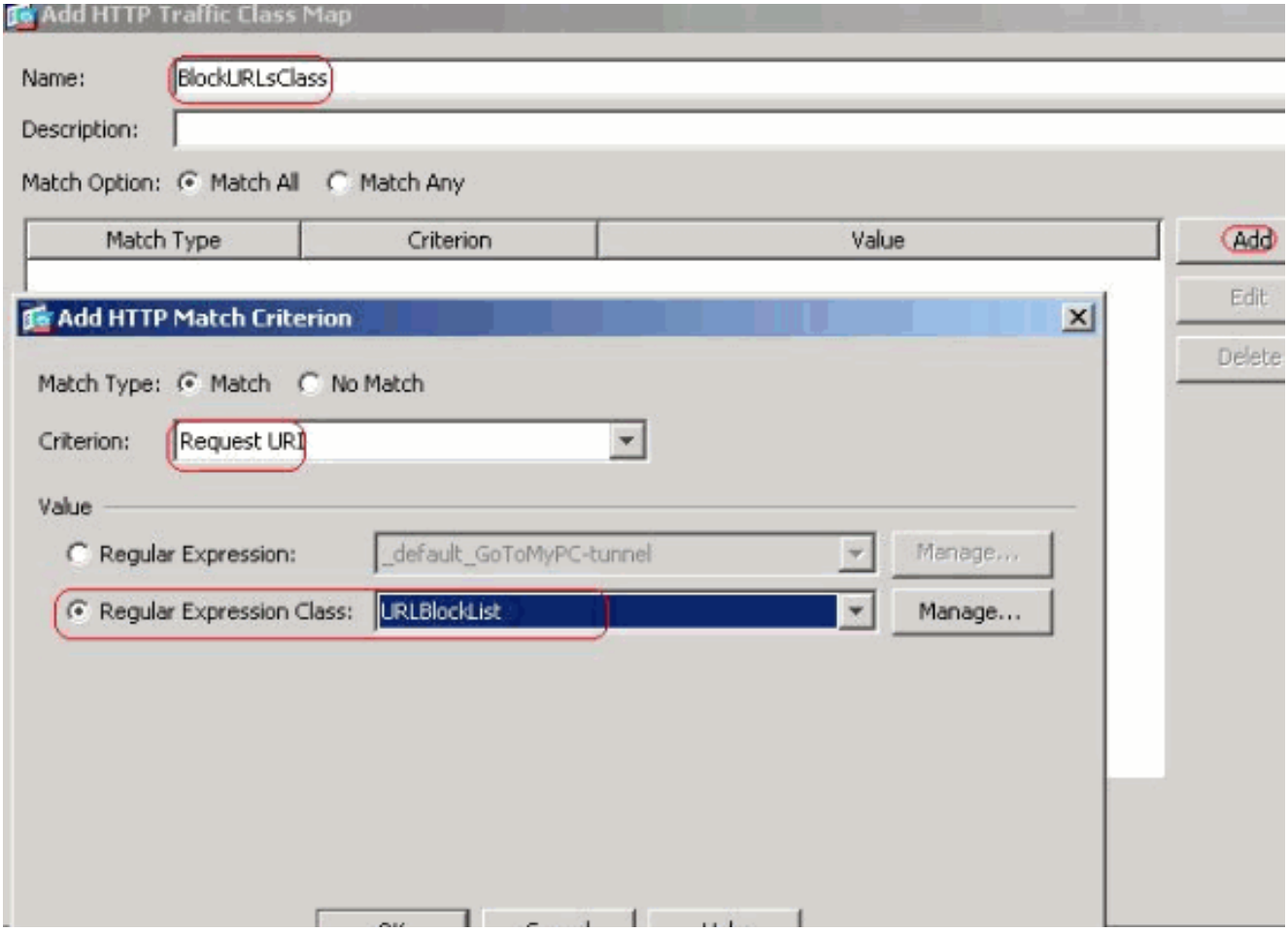
3. Проверка указанного трафика с помощью карт классаДля анализа трафика HTTP, соответствующего различным регулярным выражениям из приведенных примеров, выберите Configuration > Firewall > Objects > Class Maps > HTTP > Add (Конфигурация > Межсетевой экран > Объекты > Карты классов > HTTP > Добавить).Для обработки заголовка отклика, перехваченного на основе регулярных выражений, создайте карту классов
BlockDomainsClass.



Нажмите кнопку ОКДля обработки заголовка запроса, перехваченного на основе регулярных выражений, создайте карту классов BlockDomainsClass.

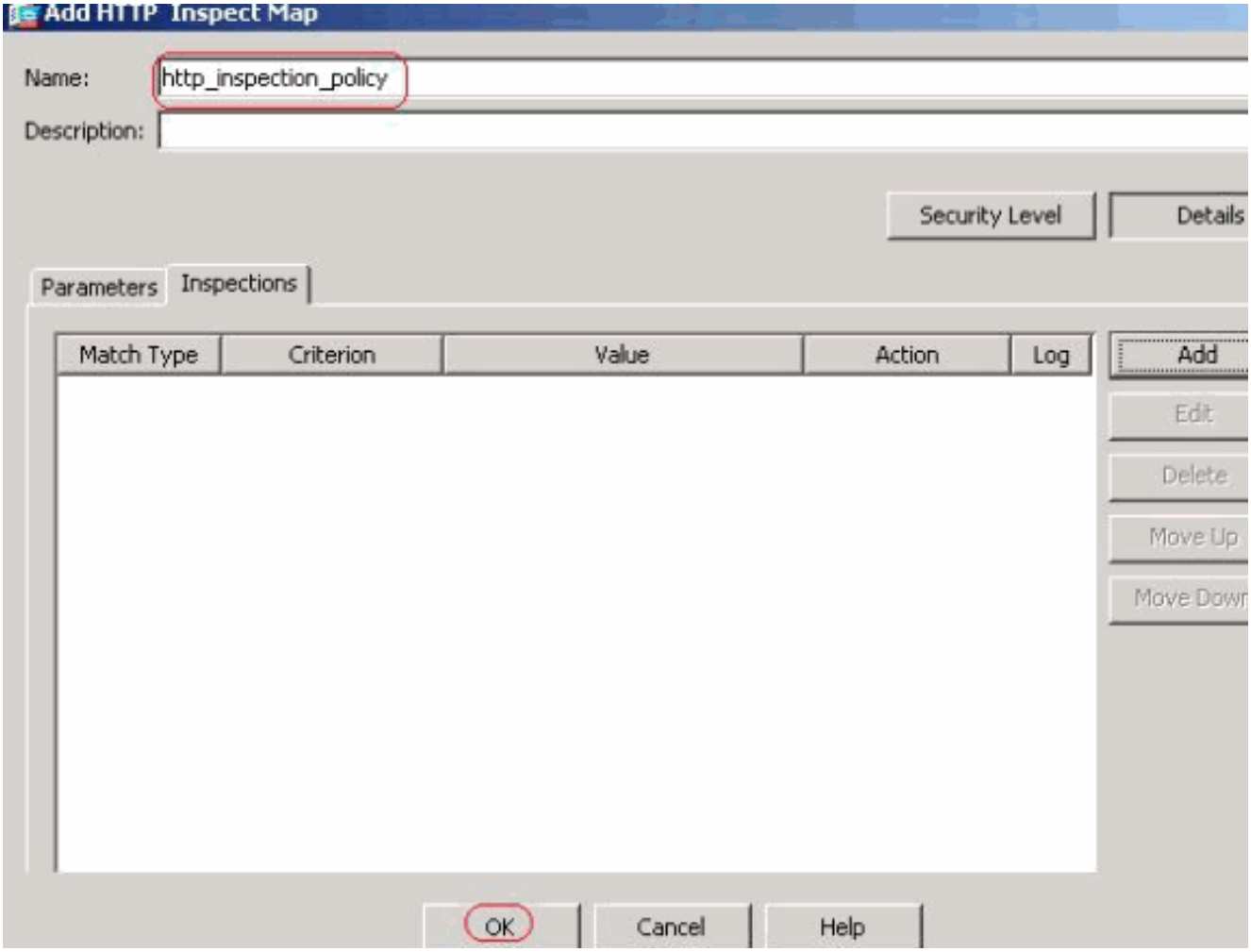


Нажмите кнопку OK.Для обработки URL-адреса запроса, перехваченного на основе регулярных выражений, создайте карту классов BlockURLsClass.

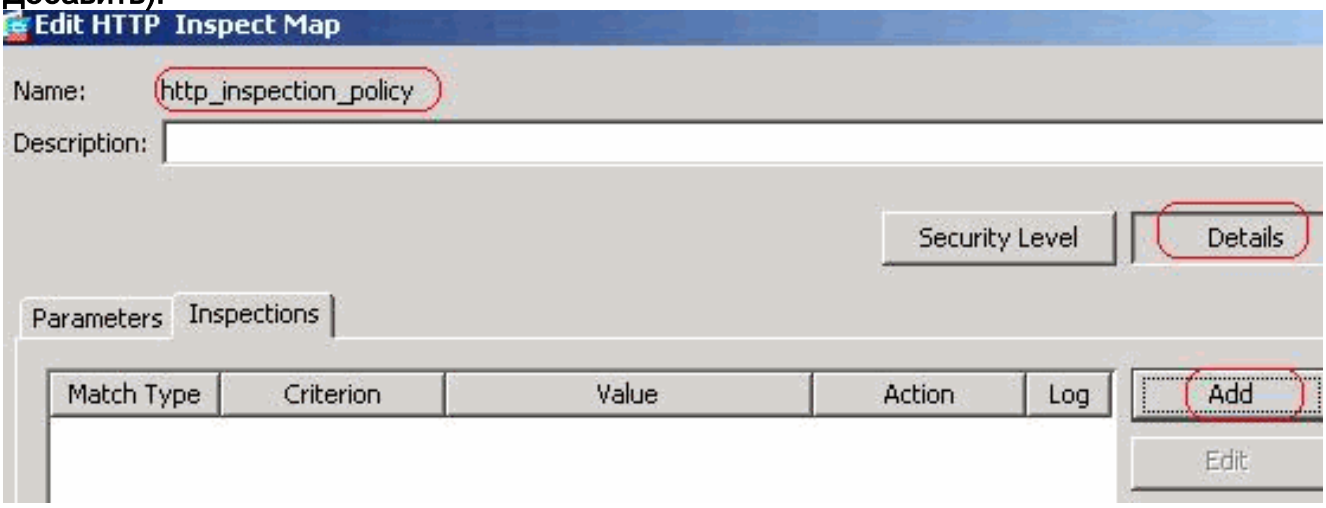


Нажмите кнопку OK.Эквивалентная конфигурация в интерфейсе командной строки

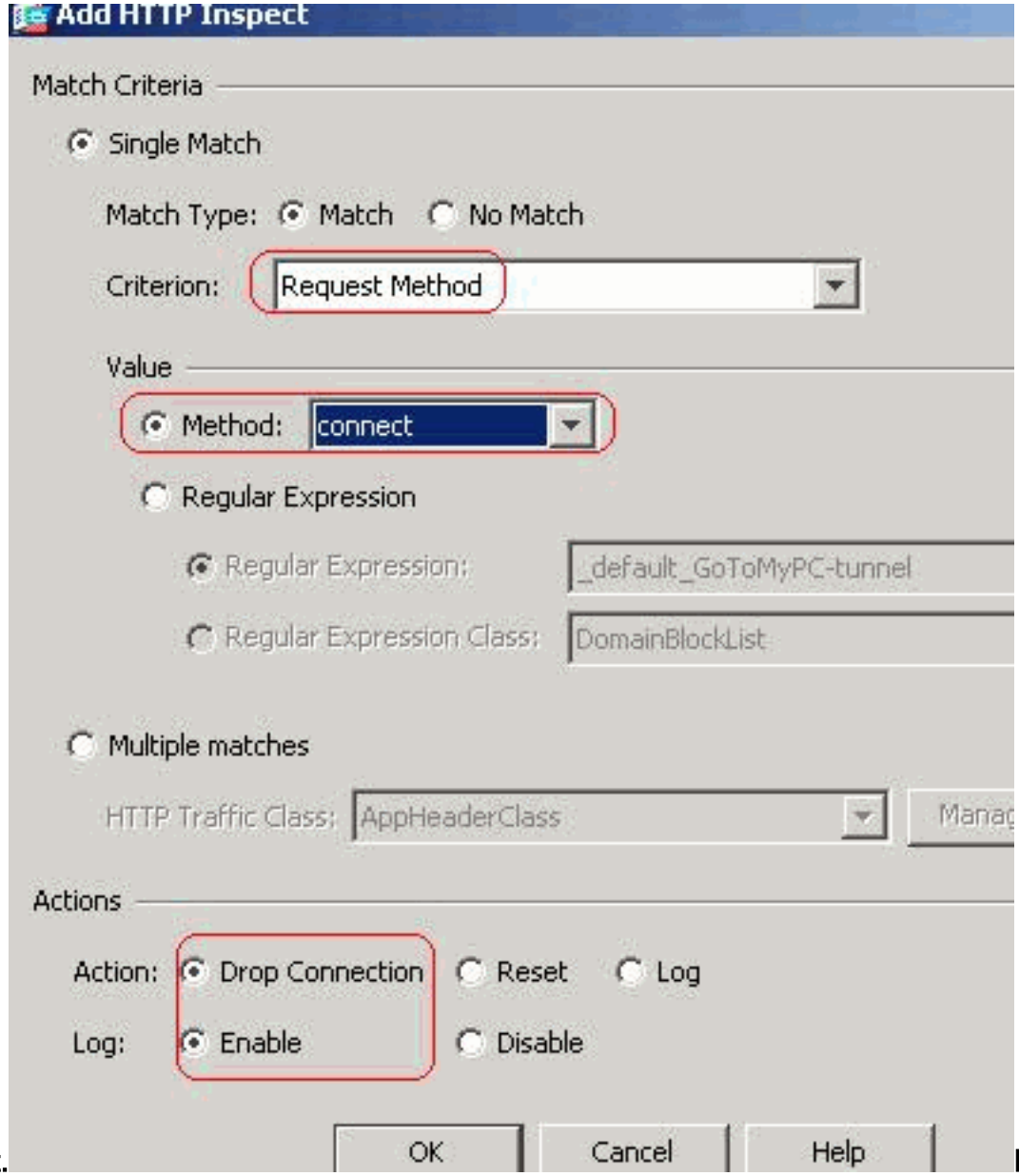
4. Задание действий для перехваченного трафика в политике анализаЧтобы создать политику http_inspection_policy, определяющую действия для перехваченного трафика. выберите Configuration > Firewall > Objects > Inspect Maps > HTTP (Конфигурация > Межсетевой экран > Объекты > Карты анализа > HTTP). Нажмите кнопку OK.



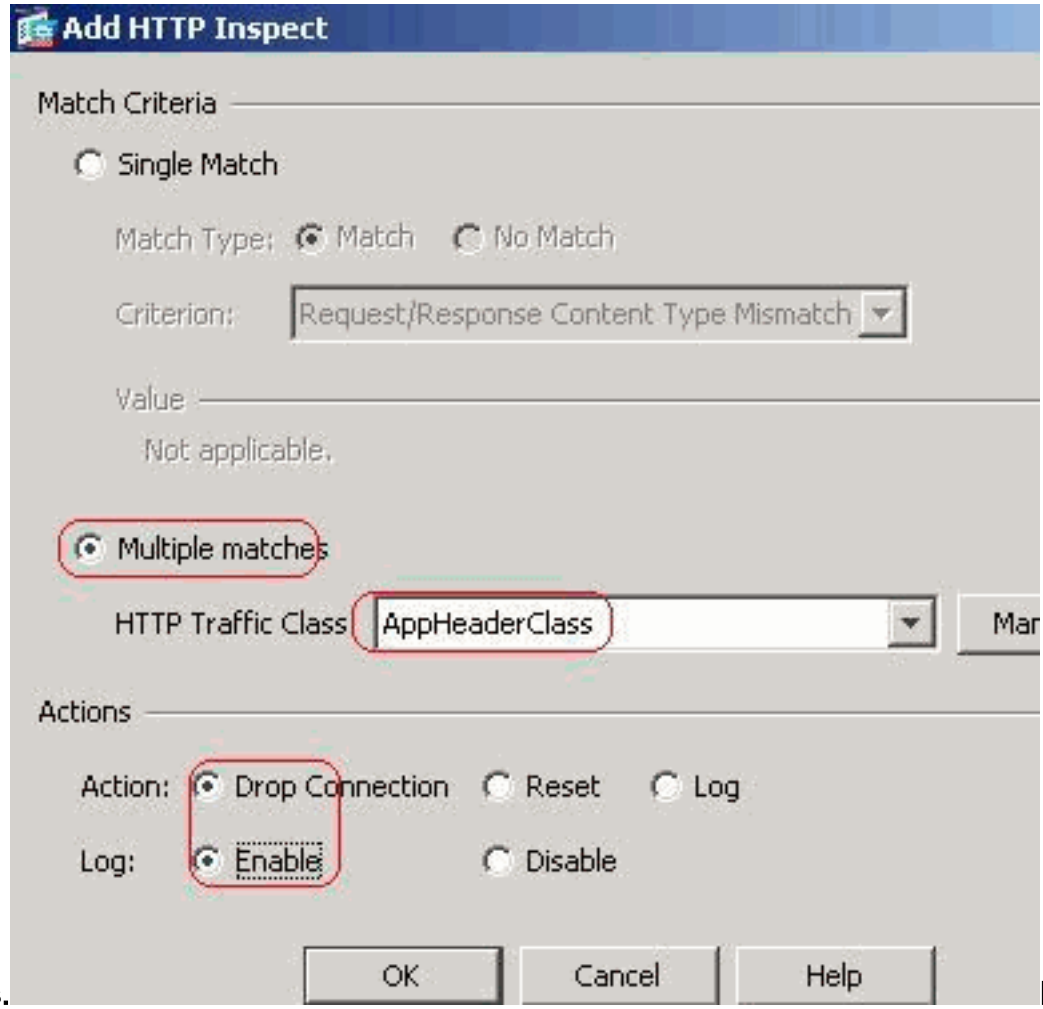
Чтобы задать действия для созданных ранее классов, выберите Configuration > Firewall > Objects > Inspect Maps > HTTP > http_inspection_policy (щелкните дважды), затем щелкните Details > Add (Сведения > Добавить).



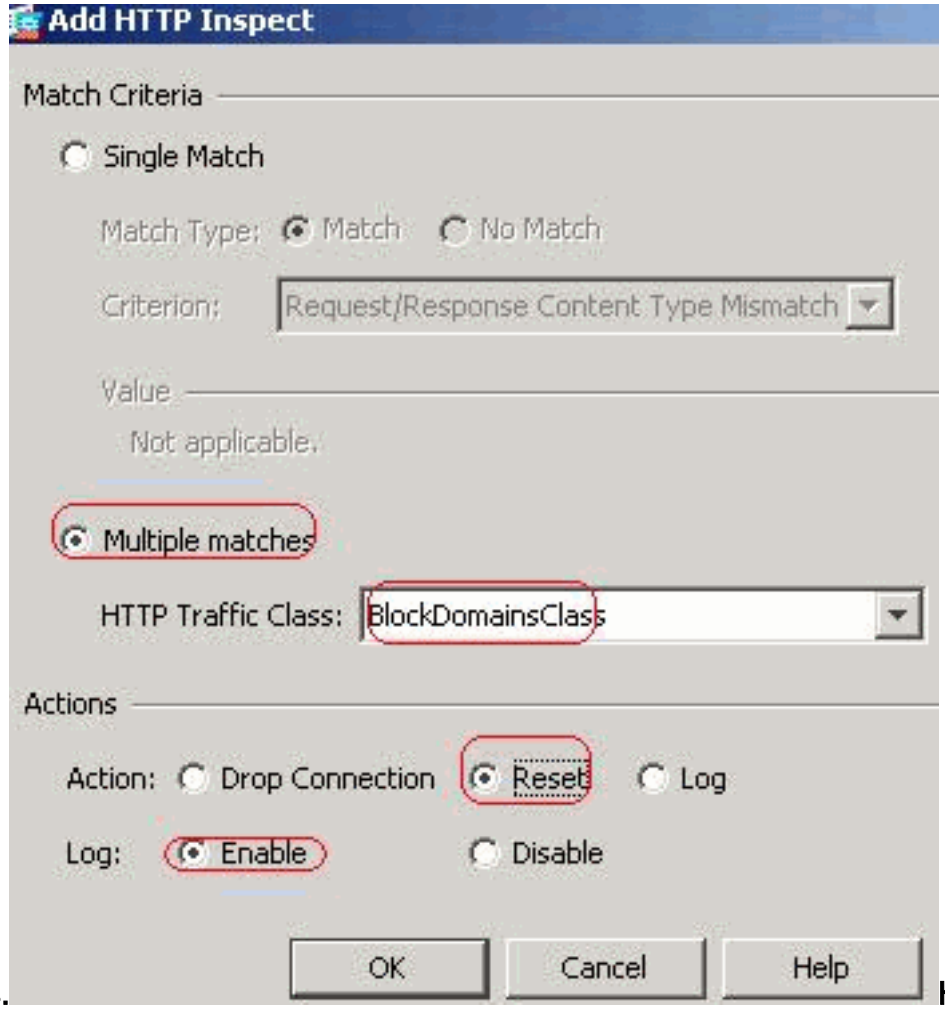
Задайте действие (например, Drop Connection – разорвать соединение) и включите (Enable) ведение журналов по критерию (Criterion) метода запроса (Request Method) и значению (Value)



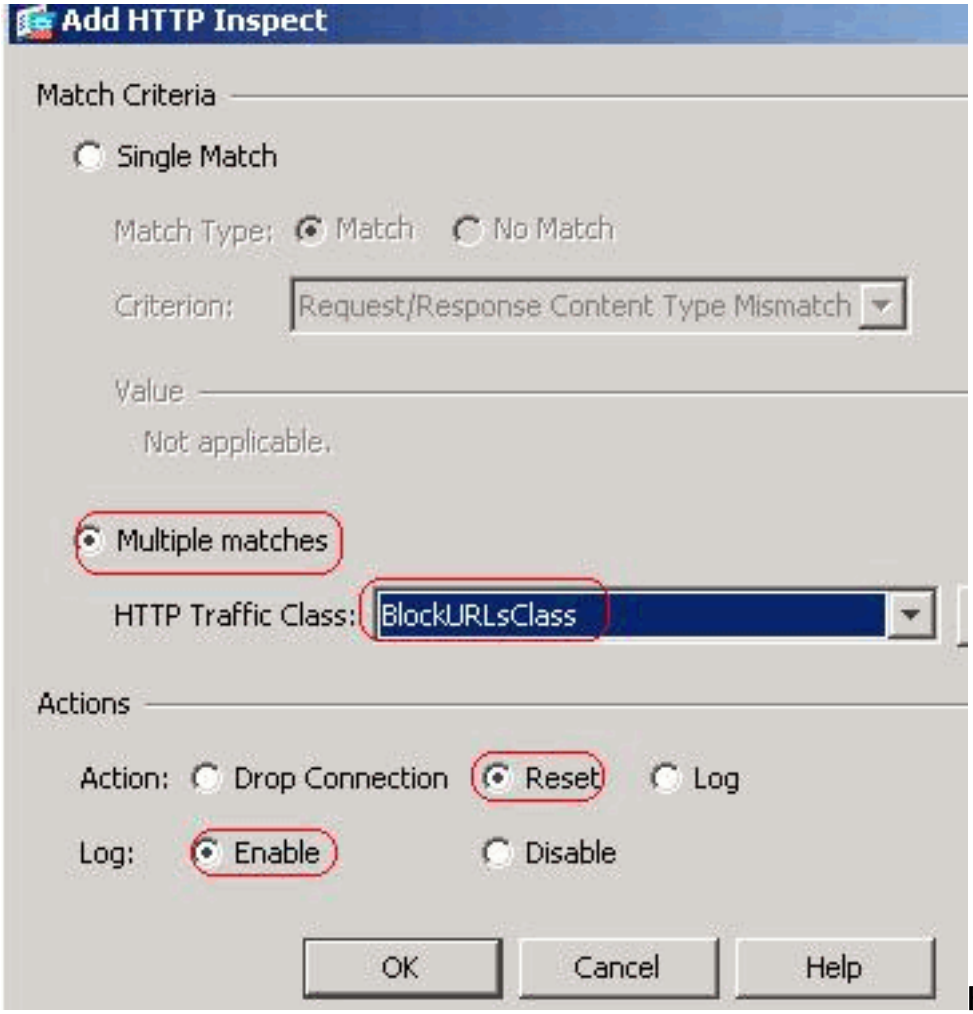
connect. Нажмите кнопку ОКУстановите действие Drop Connection (Разрывать соединение) и включите (Enable) ведение журнала для класса



AppHeaderClass. Нажмите кнопку OK.Установите действие Reset (Выполнять сброс) и включите (Enable) ведение журнала для класса

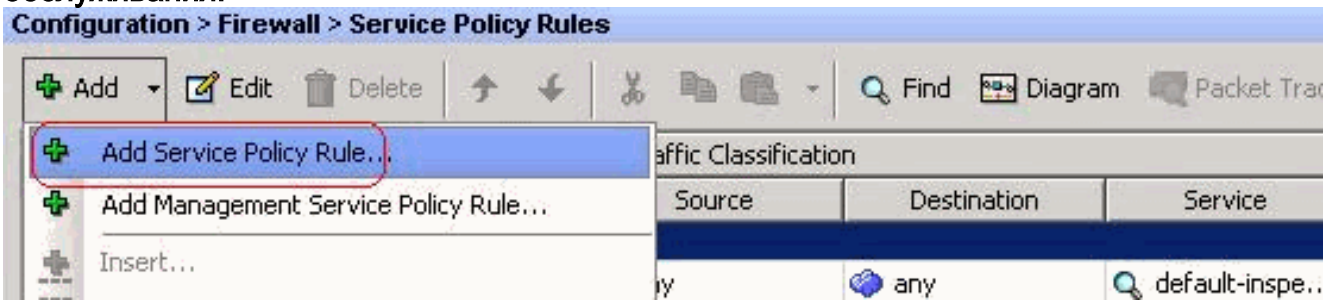


BlockDomainsClass. Нажмите кнопку ОКУстановите действие Reset (Выполнять сброс) и включите (Enable) ведение журнала для класса

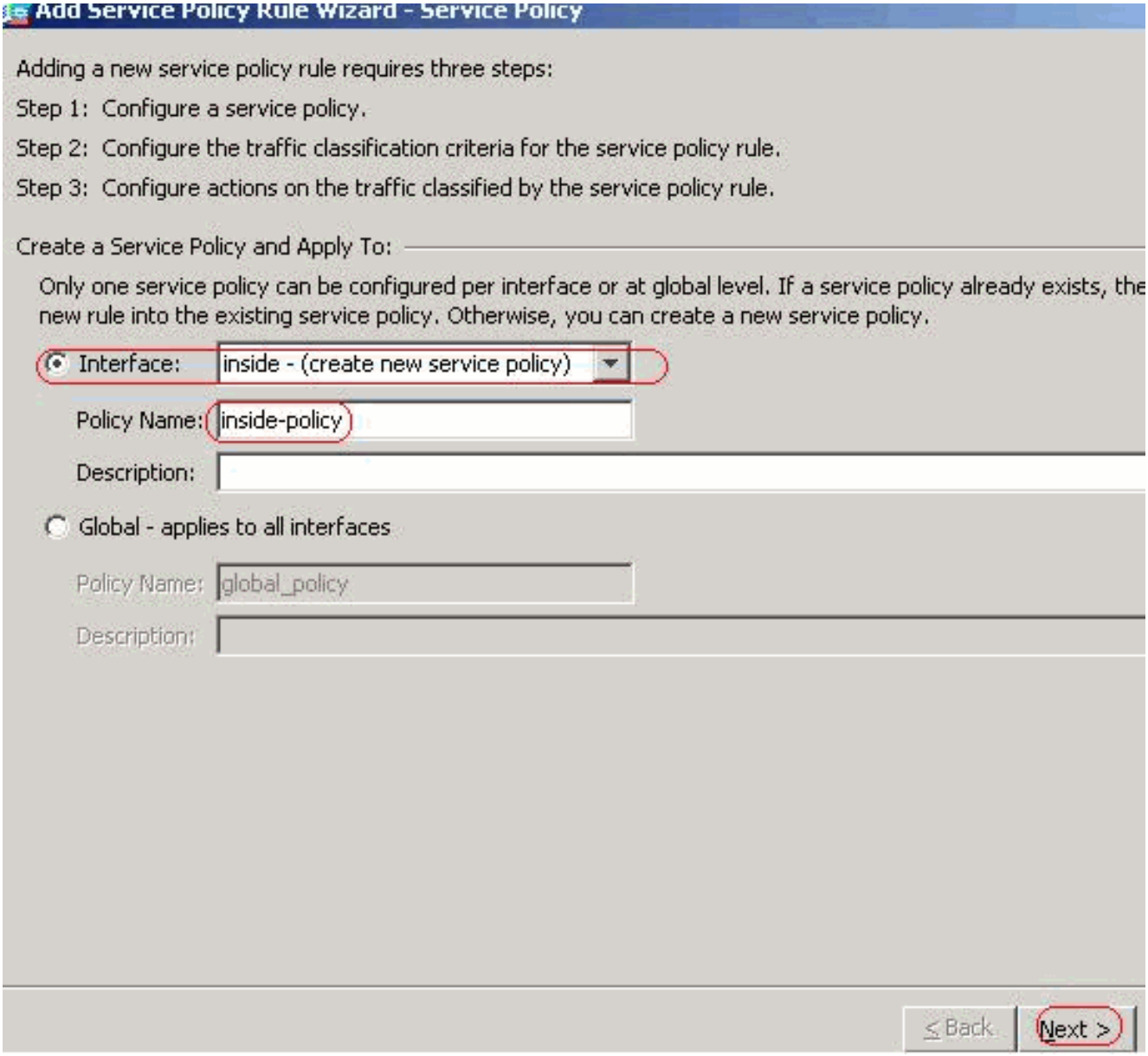


BlockURLsClass. Нажмите кнопку OK.Щелкните "Применить".Эквивалентная конфигурация в интерфейсе командной строки

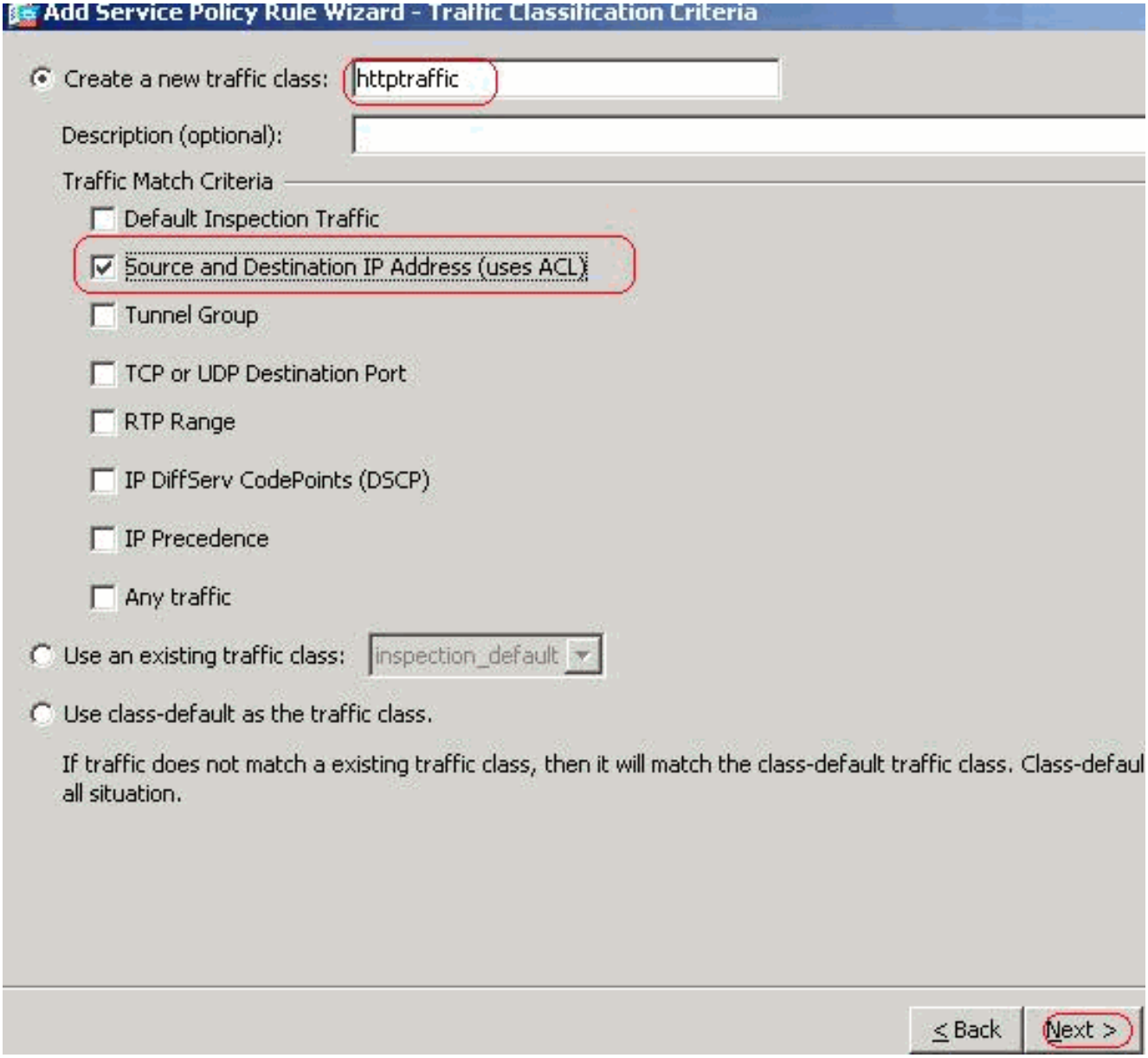
5. Применение политики анализа HTTP для интерфейсаВыберите Configuration > Firewall > Service Policy Rules > Add > Add Service Policy Rule (Конфигурация > Межсетевой экран > Правила политик обслуживания > Добавить > Добавить правило политики обслуживания.



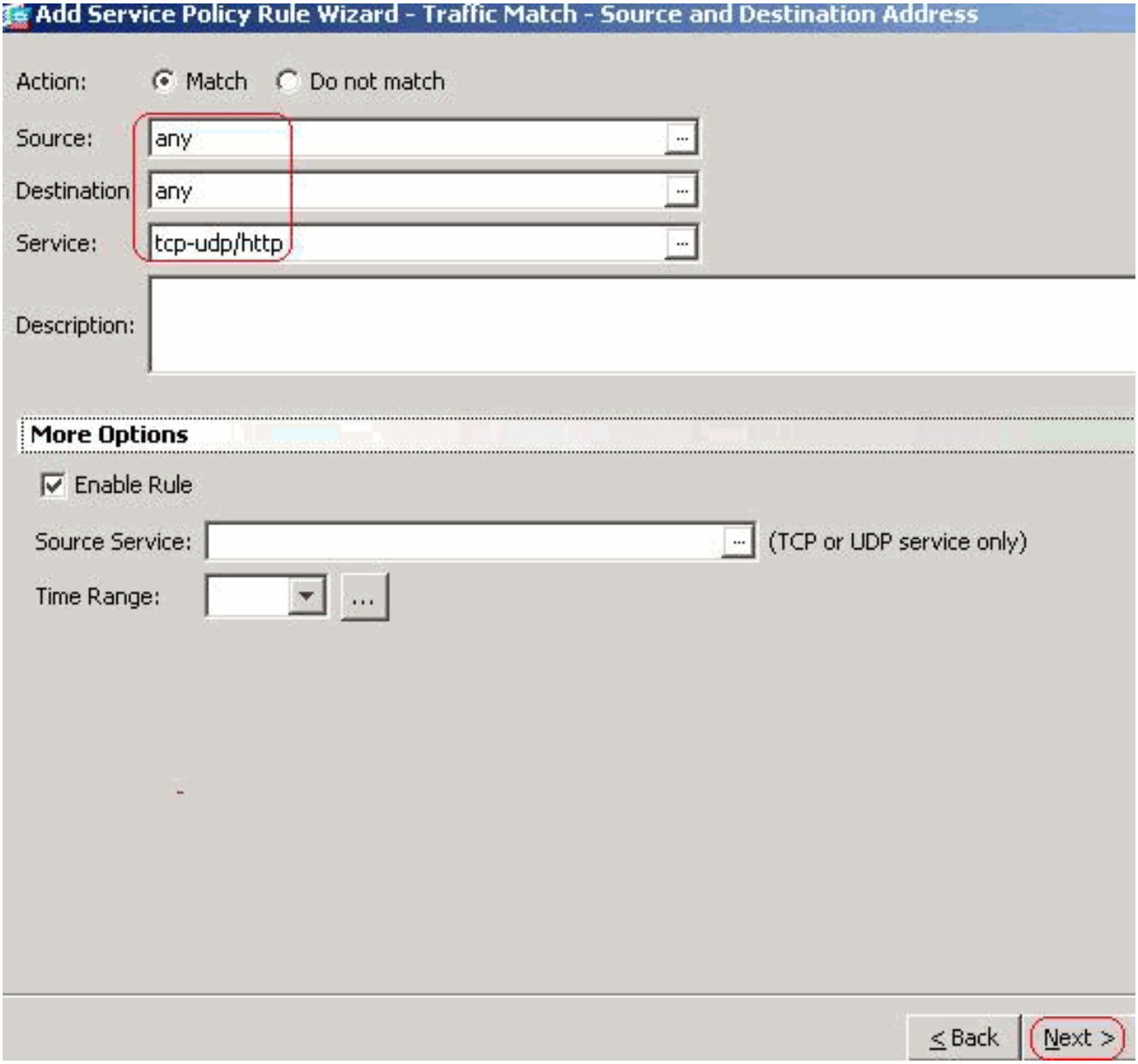
Трафик HTTPB раскрывающемся меню выберите переключатель Interface (Интерфейс), соответствующий внутреннему интерфейсу, и укажите название политики (Policy Name) inside-policy. Нажмите кнопку
Next.



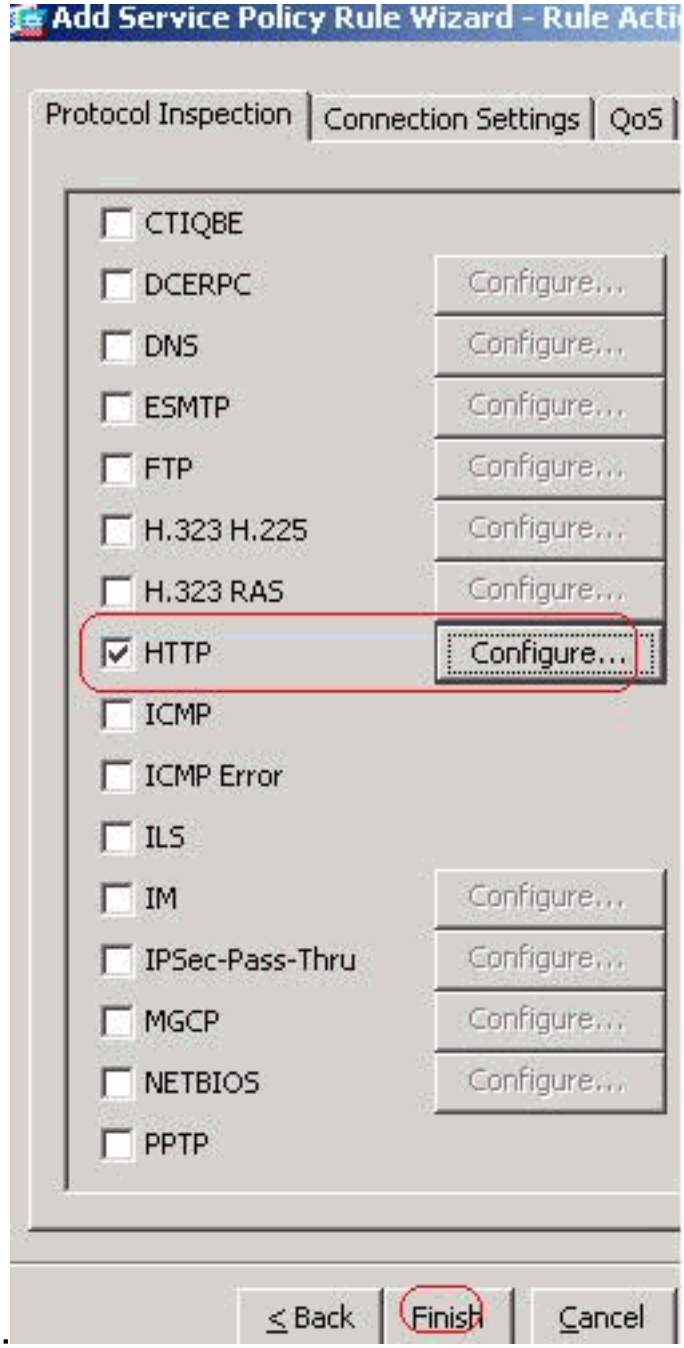
Создайте карту классов httptraffic и отметьте поля Source (Источник) и Destination IP Address (uses ACL) (IP-адрес получателя [с использованием списка ACL]). Нажмите кнопку
Next.



В полях Source (Источник) и Destination (Получатель) укажите «any» (любой) и выберите службу tcp-udp/http. Нажмите кнопку Next.

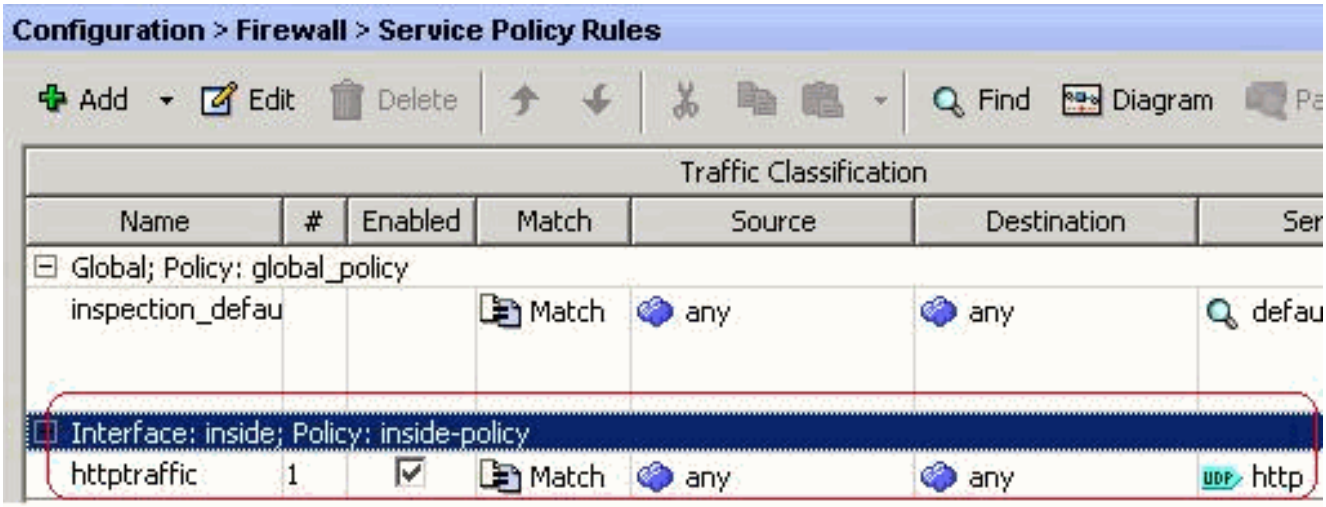


Выберите переключатель HTTP и щелкните Configure

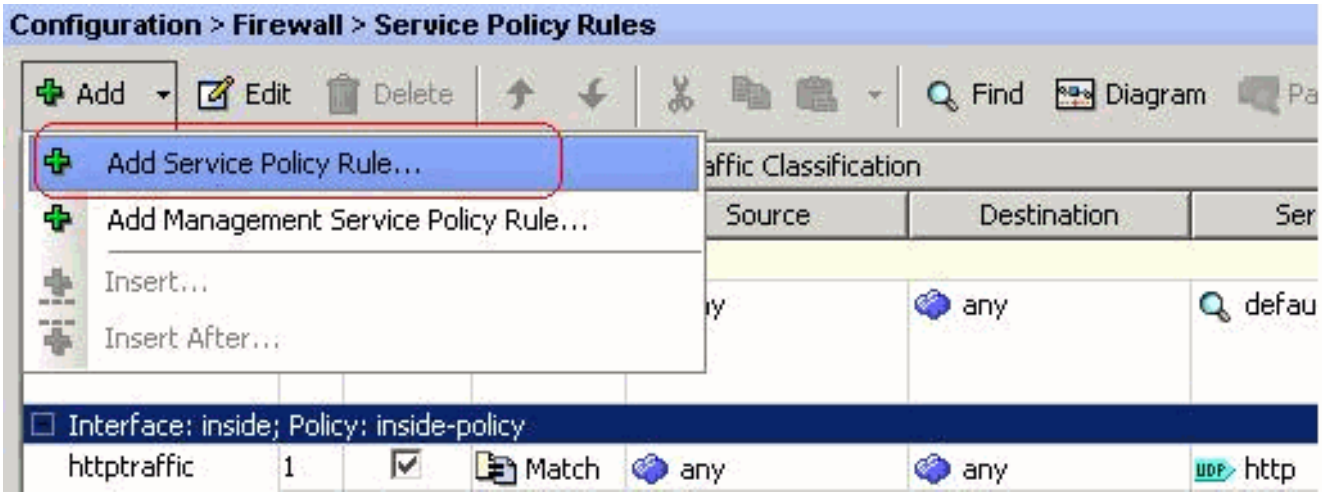


(Настроить). Выберите переключатель Select a HTTP inspect map for the control over inspection (Выбрать для управления анализом карту анализа HTTP), как показано в примере. Нажмите кнопку

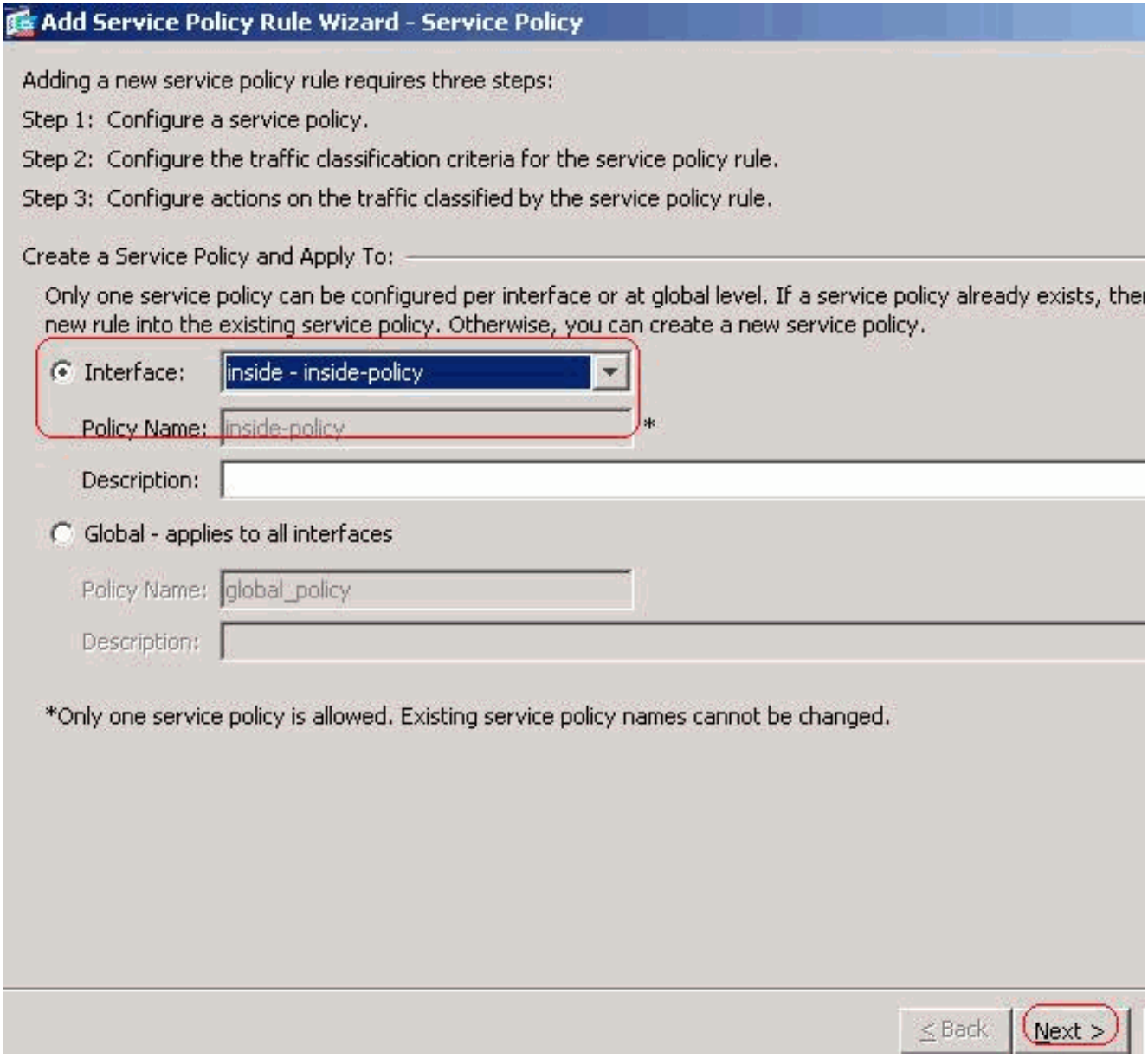
OK.Нажмите кнопку Finish.



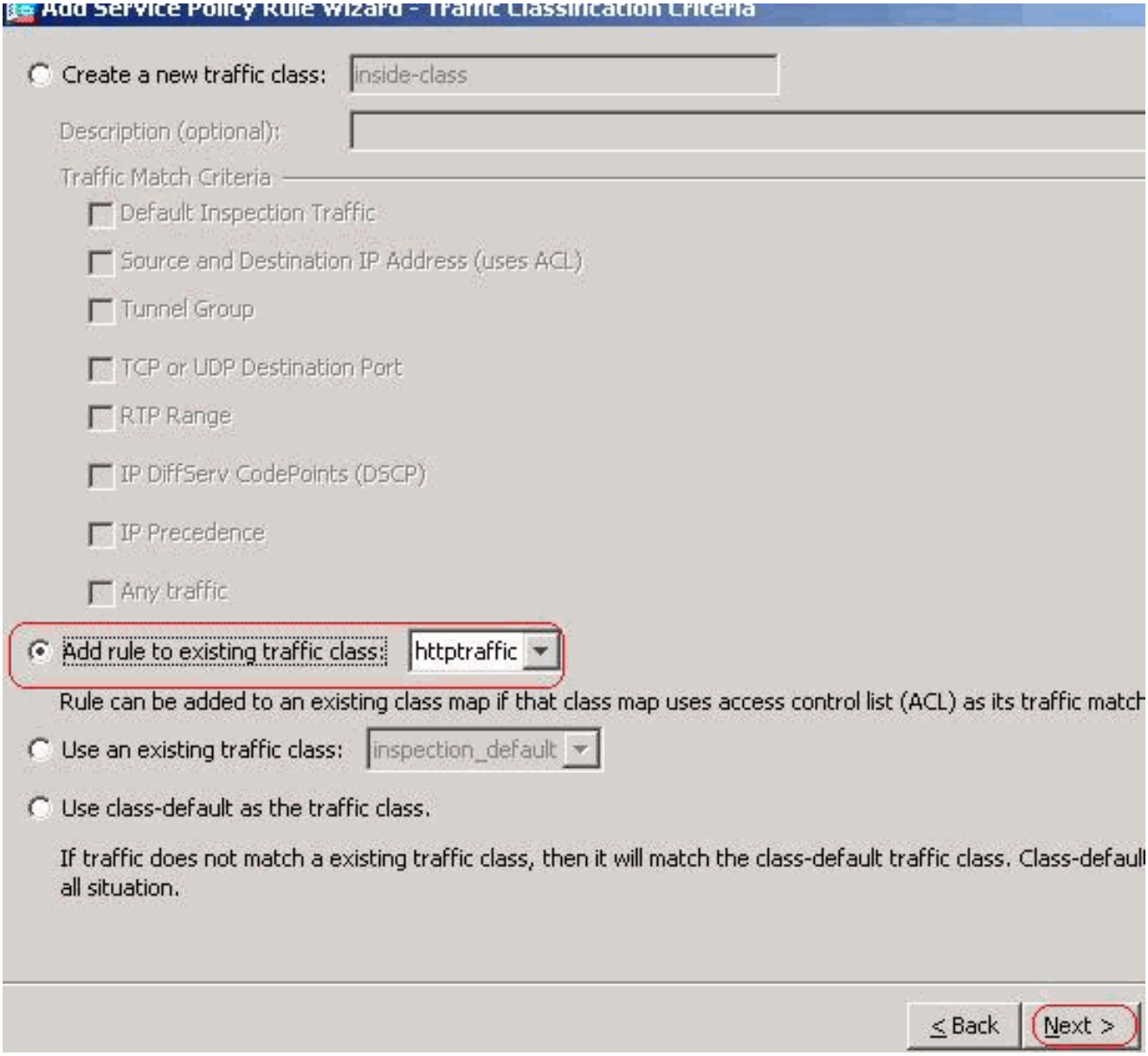
Трафик через порт 8080Снова выберите Add > Add Service Policy Rule (Добавить > Добавить правило политики обслуживания).



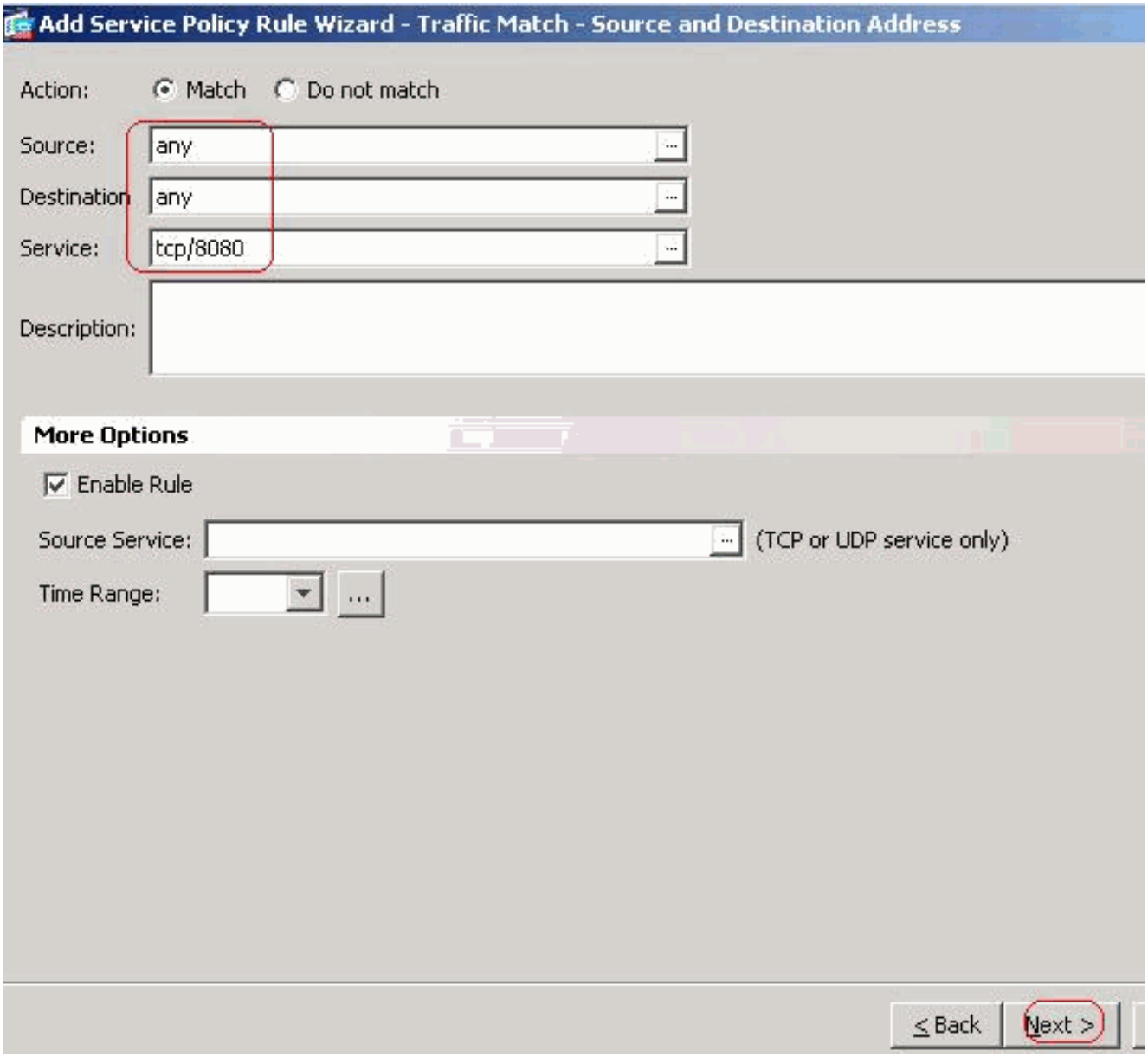
Нажмите кнопку
Next.



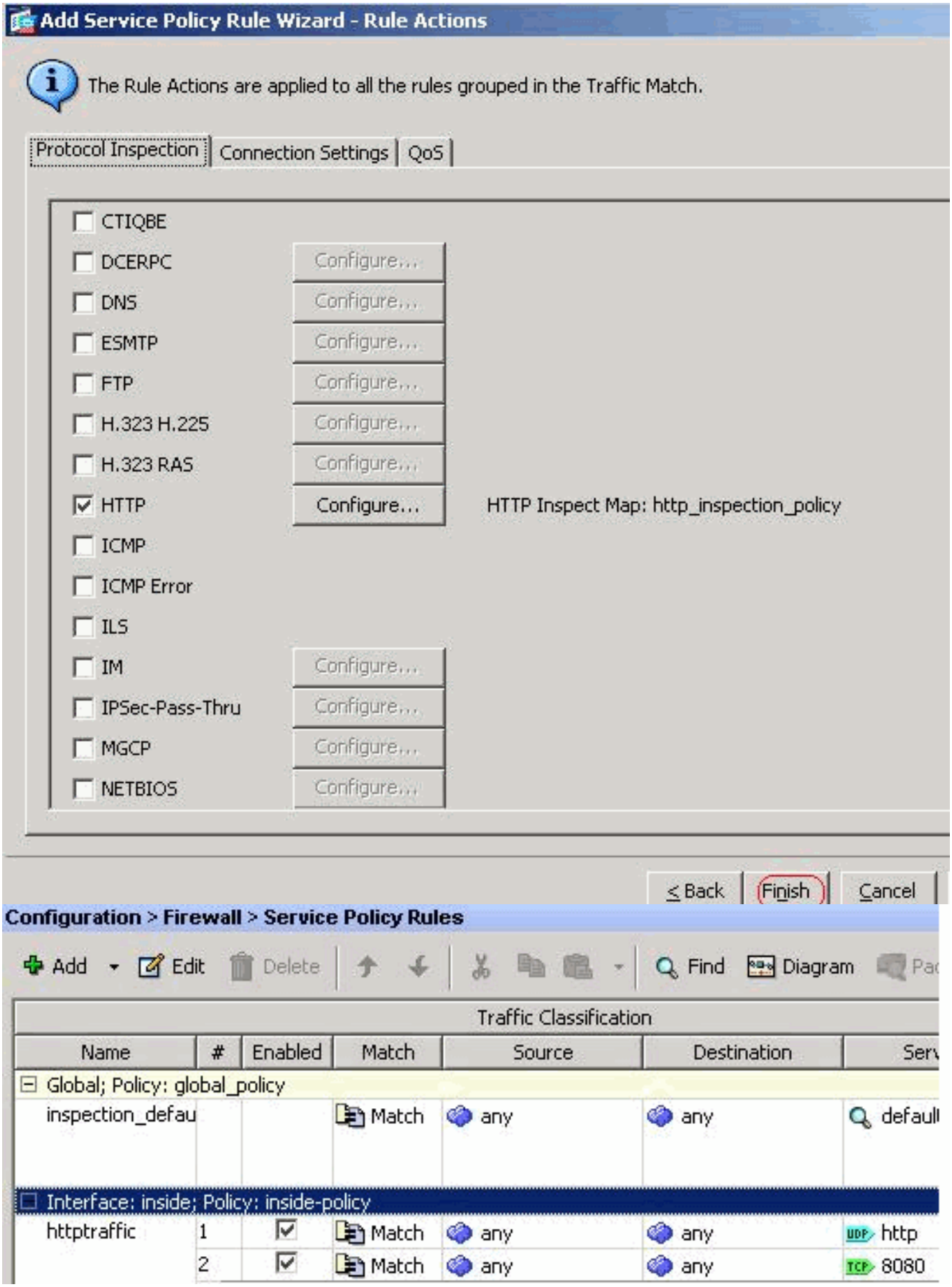
Выберите переключатель Add rule to existing traffic class (Добавить правило к существующему классу трафика) и в раскрывающемся меню укажите httptraffic.
Нажмите кнопку
Next.



В полях Source (Источник) и Destination (Получатель) укажите «any» (любой) с номером порта tcp/8080. Нажмите кнопку
Next.



Нажмите кнопку
Finish.



Щелкните "Применить".Эквивалентная конфигурация в интерфейсе командной строки

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей

конфигурации.

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

- **show running-config regex — данная команда показывает созданные конфигурации регулярных выражений**
```
ciscoasa#show running-config regex regex urllist1 ".*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt]) HTTP/1.[01]" regex urllist2 ".*\.([Pp][Ii][Ff]|[Vv][Bb][Ss]|[Ww][Ss][Hh]) HTTP/1.[01]" regex urllist3 ".*\.([Dd][Oo][Cc]|[Xx][Ll][Ss]|[Pp][Pp][Tt]) HTTP/1.[01]" regex urllist4 ".*\.([Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz]) HTTP/1.[01]" regex domainlist1 "\.yahoo\.com" regex domainlist2 "\.myspace\.com" regex domainlist3 "\.youtube\.com" regex contenttype "Content-Type" regex applicationheader "application/.*" ciscoasa#
```
- **show running-config class−map– данная команда показывает созданные конфигурации карт классов**
```
ciscoasa#show running-config class-map ! class-map type regex match-any DomainBlockList match regex domainlist1 match regex domainlist2 match regex domainlist3 class-map type inspect http match-all BlockDomainsClass match request header host regex class DomainBlockList class-map type regex match-any URLBlockList match regex urllist1 match regex urllist2 match regex urllist3 match regex urllist4 class-map inspection_default match default-inspection-traffic class-map type inspect http match-all AppHeaderClass match response header regex contenttype regex applicationheader class-map httptraffic match access-list inside_mpc class-map type inspect http match-all BlockURLsClass match request uri regex class URLBlockList ! ciscoasa#
```
- **show running-config policy-map type inspect http – данная команда показывает созданные конфигурации карт политик для проверки трафика HTTP**
```
ciscoasa#show running-config policy-map type inspect http ! policy-map type inspect http http_inspection_policy parameters protocol-violation action drop-connection class AppHeaderClass drop-connection log match request method connect drop-connection log class BlockDomainsClass reset log class BlockURLsClass reset log ! ciscoasa#
```
- **show running-config policy-map – данная команда показывает все конфигурации карт политик, а также конфигурации карт политик по умолчанию**
```
ciscoasa#show running-config policy-map ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map type inspect http http_inspection_policy parameters protocol-violation action drop-connection class AppHeaderClass drop-connection log match request method connect drop-connection log class BlockDomainsClass reset log class BlockURLsClass reset log policy-map global_policy class inspection_default inspect dns preset_dns_map 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 policy-map inside-policy class httptraffic inspect http http_inspection_policy ! ciscoasa#
```
- **show running-config service-policy — показывает все конфигурации политик обслуживания, действующие в данный момент**
```
ciscoasa#show running-config service-policy service-policy global_policy global service-policy inside-policy interface inside
```
- **show running-config access-list – данная команда показывает конфигурацию списков контроля доступа, действующую в устройстве защиты**
```
ciscoasa#show running-config access-list access-list inside_mpc extended permit tcp any any eq www access-list inside_mpc extended permit tcp any any eq 8080 ciscoasa#
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

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

- debug http — данная команда показывает отладочные сообщения для трафика HTTP

Дополнительные сведения

- Поддержка устройств адаптивной защиты Cisco ASA серии 5500
- Поддержка Диспетчера устройств адаптивной защиты Cisco (ASDM)
- Поддержка Cisco PIX 500 Series Security Appliances
- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация