ASA/PIX 7.2: Блокировать определенные веб-сайты (URL) с помощью регулярных выражений в примерах конфигурации MPF

Содержание

Введение

Этот документ описывает, как настроить на устройствах Cisco Security ASA/PIX 7.2 с регулярными выражениями модульную систему политик (MPF), чтобы заблокировать определенные веб-сайты (URL).

Примечание: Эта конфигурация не блокирует все загрузки приложений. Для надежных блоков файла должно использоваться специализированное устройство, таких как Websense, и т.д., или модуль, таких как модуль CSC для ASA.

Фильтрация HTTPS не поддерживается на ASA. ASA не может сделать глубокой проверки пакетов или контроля на основе регулярного выражения для Трафика HTTPS, потому что в HTTPS содержание пакета зашифровано (ssl).

Предварительные условия

Требования

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

Используемые компоненты

- Устройство адаптивной защиты (ASA) серии 5500 Cisco, которое работает под управлением ПО версии 7.2 (2)
- Cisco Adaptive Security Device Manager (ASDM) версия 5.2 (2) для ASA 7.2 (2)

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 Cisco PIX серии 500, который работает под управлением ПО версии 7.2 (2).

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 совпадает с текстовыми строками или буквально как с точной строкой, или с метасимволами, таким образом, можно совпасть со множественными вариантами 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 из всех специальных символов в CLI, таких как вопросительный знак (?) или вкладка. Например, **тип d [Ctrl+V] g** для ввода **d? g** в конфигурации.

Для создания регулярного выражения используйте **команду regex**, которая может использоваться для различных функций, которые требуют текстового соответствия. Например, можно настроить специальные действия для контроля приложения с Модульной Системой политик с картой политики проверки (см. команду inspect типа карты политик). **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 **соответствия** позволяют вам определить текст в пакете с регулярным выражением; например, можно совместить строки URL внутри пакетов HTTP. Можно сгруппировать регулярные выражения в карте класса регулярных выражений (см. команду regex типа class-map).

Таблица 1 перечисляет метасимволы, которые имеют особые значения.

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, **lo*se** совпадает с lse, потеряйте, высвободите и так далее.
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, **ab (xy) {2} z** совпадает с abxyxyz, abxyxyxyz, и так далее.
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].** Тире (-) символ является литеральным, только если это - последний или первый символ в скобках: **[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	То, когда символ не является метасимволом, совпадает с буквенным символом.
\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	Совпадает с ASCII - символом с шестнадцатеричным (точно две цифры).
\NNN	Восьмеричная нумерация	Совпадает с ASCII - символом как восьмеричным (точно три цифры). Например, код 040 соответствует пробелу.

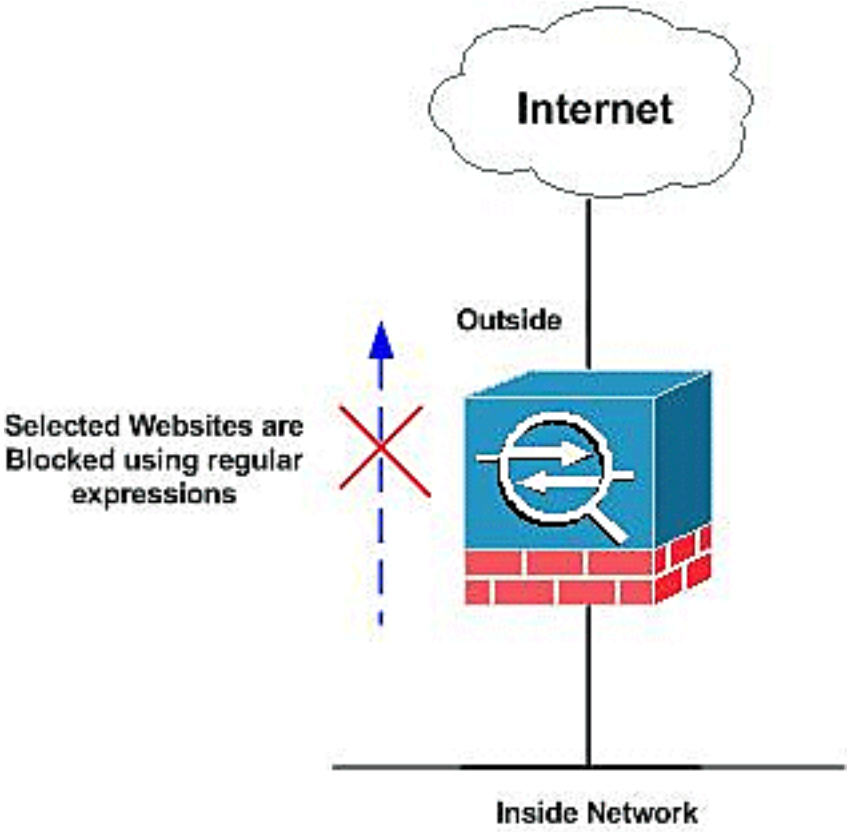
Настройка

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

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:



Конфигурации

Эти конфигурации используются в данном документе:

- Конфигурация ASA в интерфейсе командной строки
- Конфигурация ASA 7.2 (x) с ASDM 5.2

Конфигурация ASA в интерфейсе командной строки

Конфигурация ASA в интерфейсе командной строки

```
ciscoasa#show running-config : Saved : ASA Version
7.2(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
```

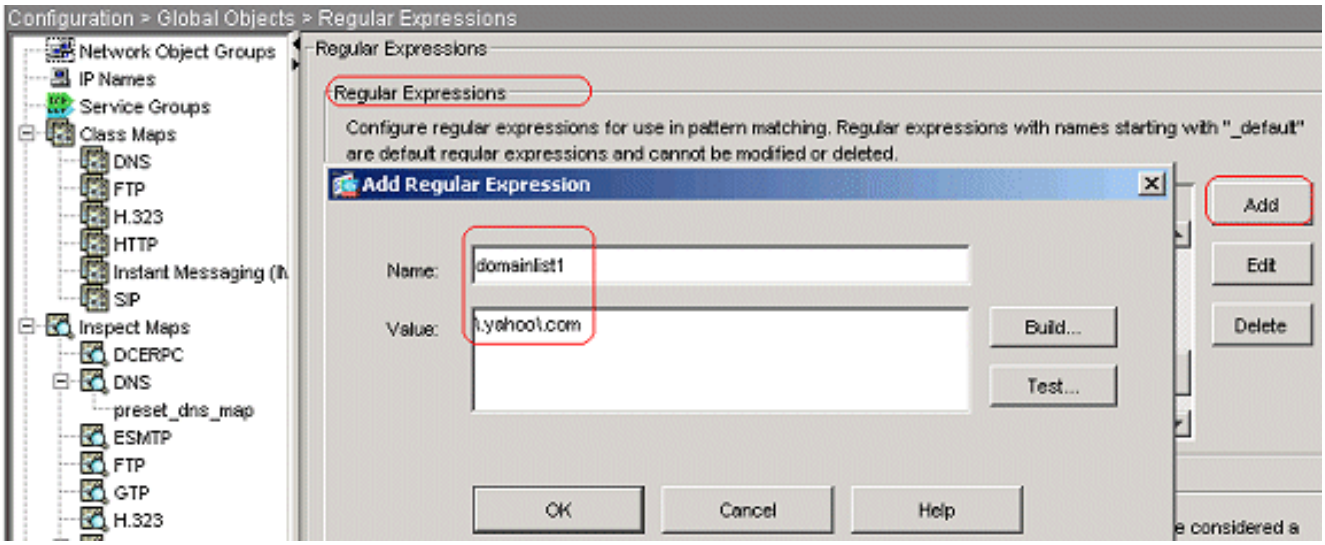
```
used by web browser must be either !--- 1.0 or 1.1 regex
urllist3 ".*\.([Dd][Oo][Cc]|[Xx][Ll][Ss]|[Pp][Pp][Tt])
HTTP/1.[01]" !--- Extensions such as .doc(word),
.xls(ms-excel), .ppt to be captured and provided !---
the http version being used by web browser must be
either 1.0 or 1.1 regex urllist4
".*\.([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 will be blocked prompt
hostname context
Cryptochecksum:e629251a7c37af205c289cf78629fc11 : end
ciscoasa#
```

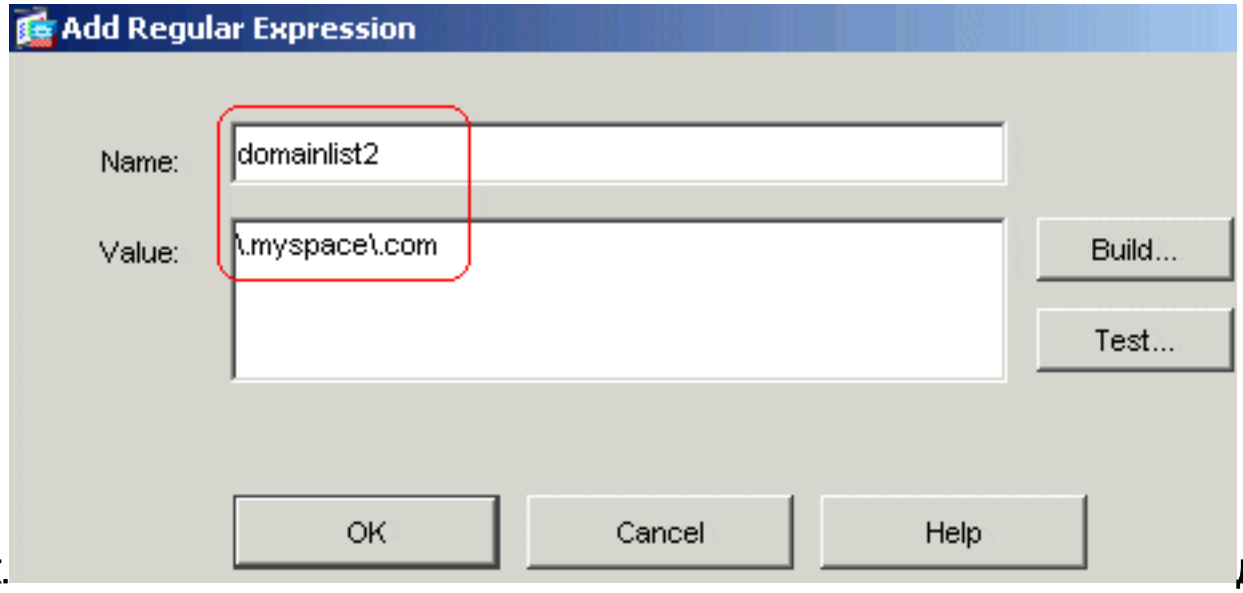
Конфигурация ASA 7.2 (x) с ASDM 5.2

Выполните эти шаги, чтобы настроить регулярные выражения и применить их к MPF для блокирования определенных веб-сайтов:

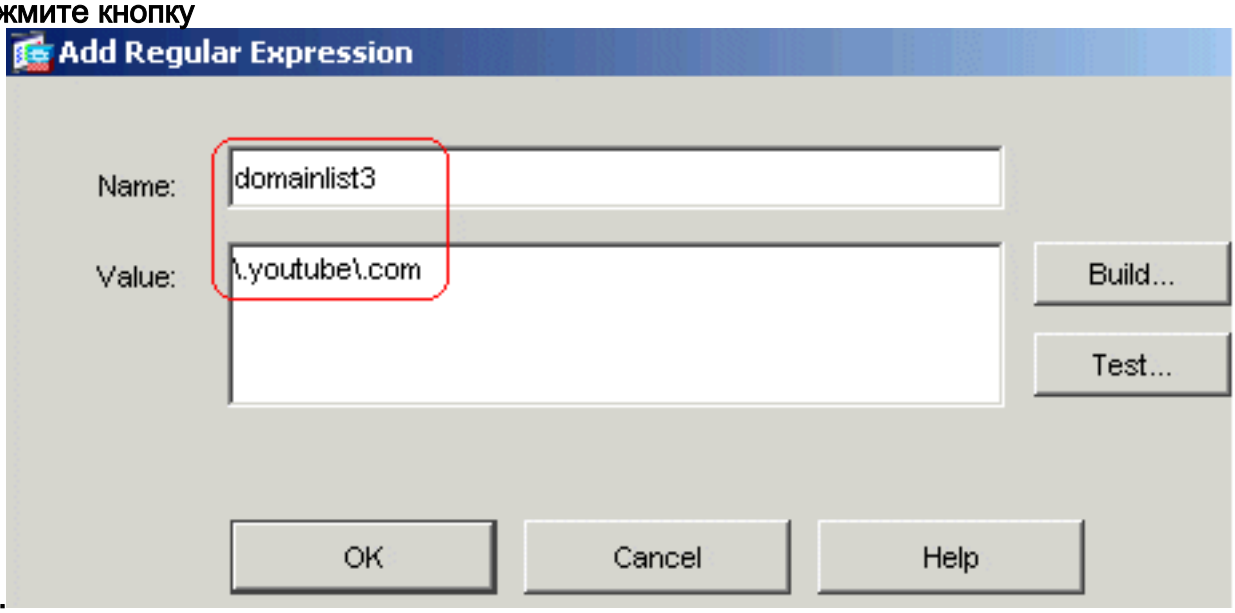
1. **Создание регулярных выражений**Выберите **Configuration> Global Objects> Regular Expressions** и **нажмите Add** под вкладкой Regular Expression для создания регулярных выражений.**Для перехвата имени домена yahoo.com создайте регулярное выражение domainlist1. Нажмите кнопку**
   OK.



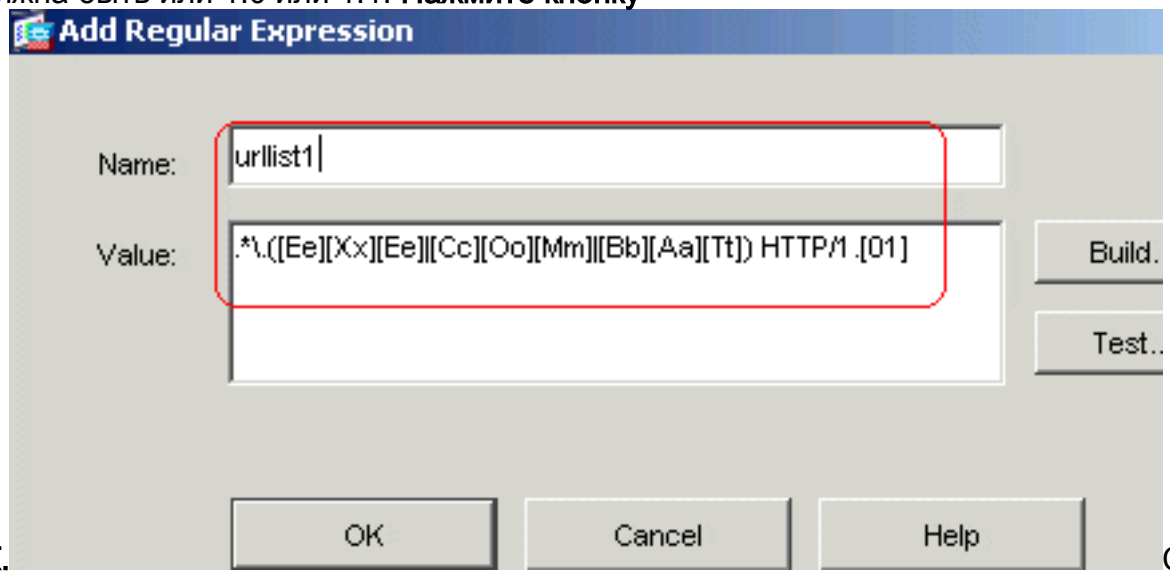
   Для перехвата имени домена myspace.com создайте регулярное выражение domainlist2. Нажмите кнопку



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

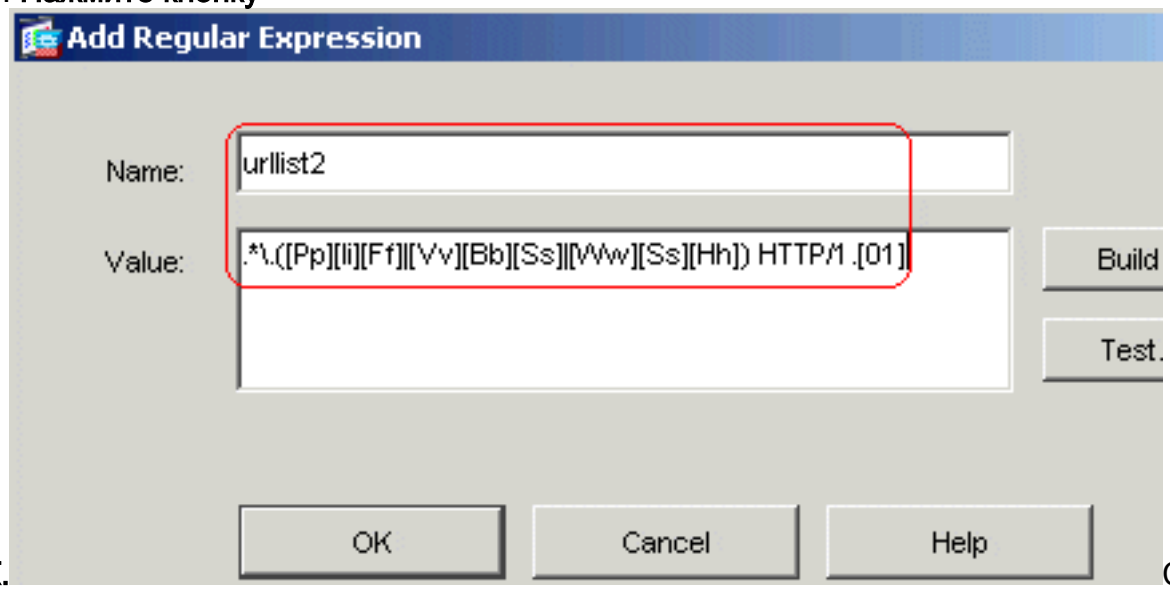


OK. Создайте регулярное выражение **urllist1** для получения расширений файла, таких как **exe**, **com** и **летучая мышь** при условии, что версия http, используемая web-браузером, должна быть или 1.0 или 1.1. **Нажмите кнопку**

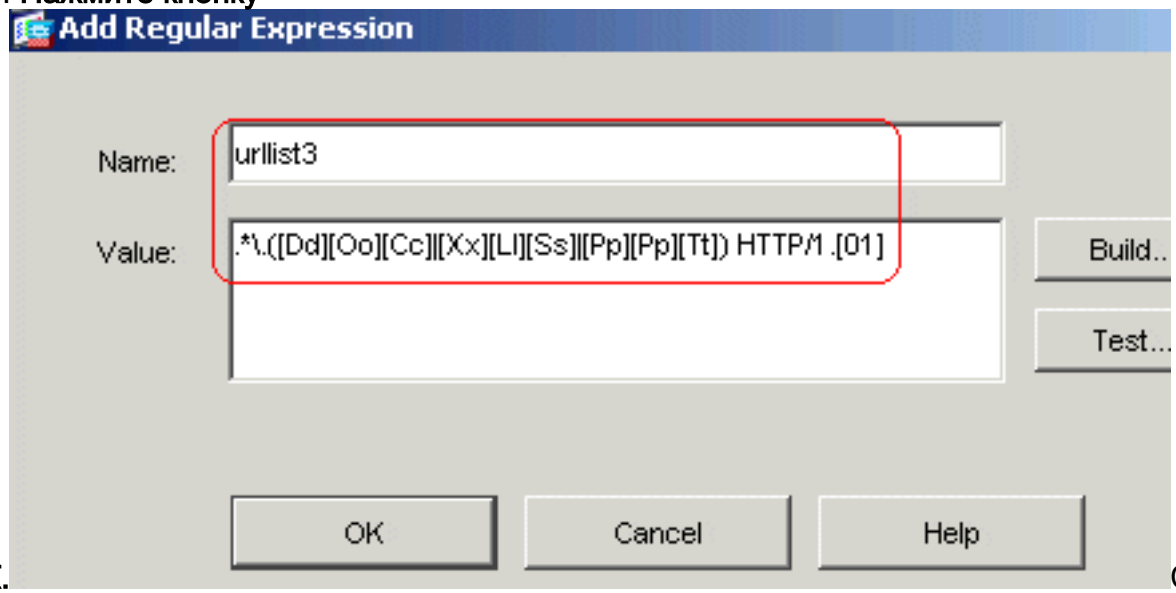


OK. Создайте регулярное выражение **urllist2** для получения расширений файла, таких как **pif**, **vbs**, и **wsh** при условии, что версия HTTP, которая используется web-браузером, или 1.0 или

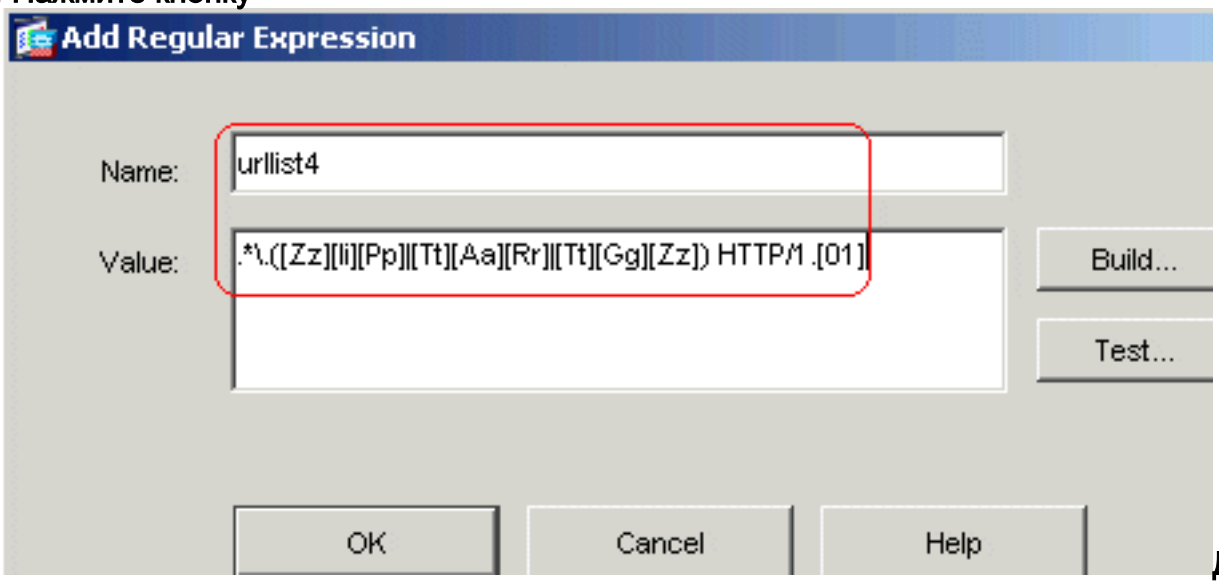
1.1. **Нажмите кнопку**



OK. Создайте регулярное выражение **urllist3** для получения расширений файла, таких как **doc**, **xls**, и **ppt** при условии, что версия HTTP, которая используется web-браузером, или 1.0 или 1.1. **Нажмите кнопку**

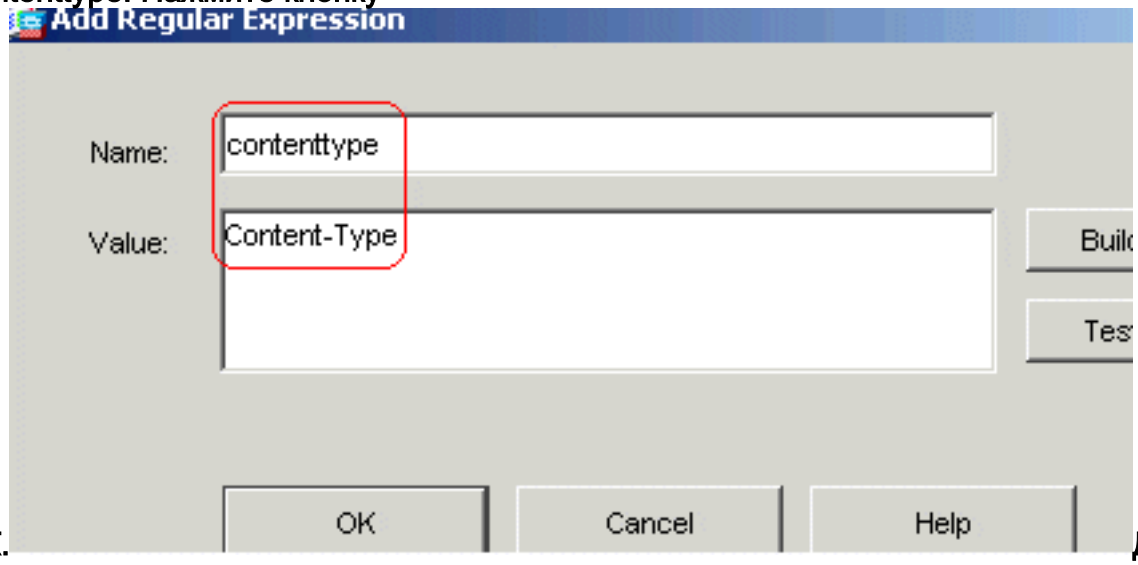


OK. Создайте регулярное выражение **urllist4** для получения расширений файла, таких как **zip**, **tar** и **tgz** при условии, что версия HTTP, которая используется web-браузером, или 1.0 или 1.1. **Нажмите кнопку**

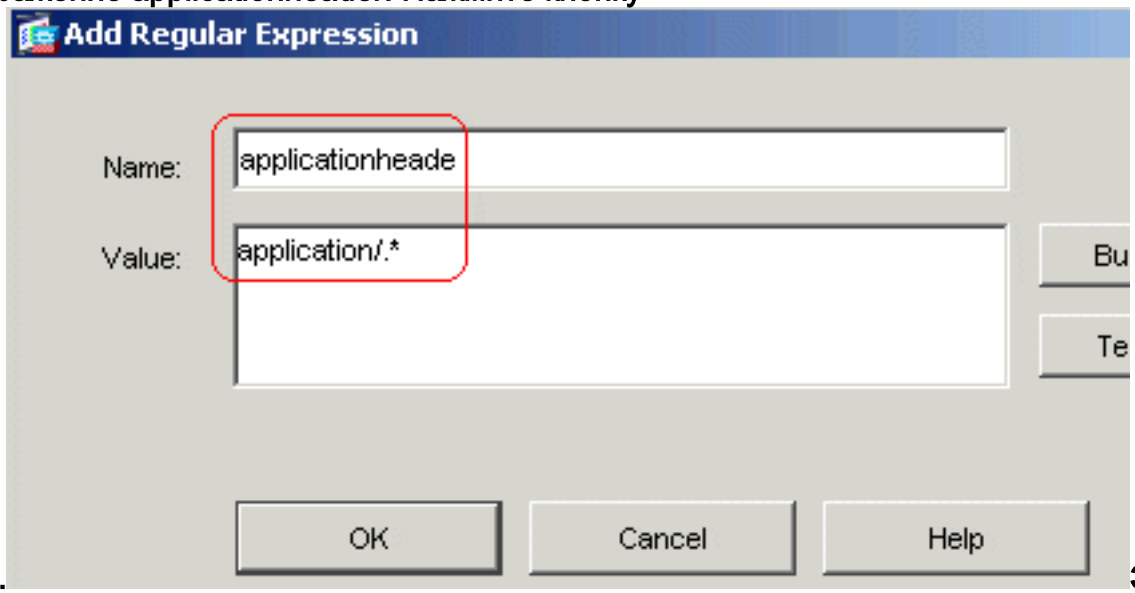


OK. **Дл**

я перехвата идентификатора типа содержимого создайте регулярное выражение contenttype. Нажмите кнопку

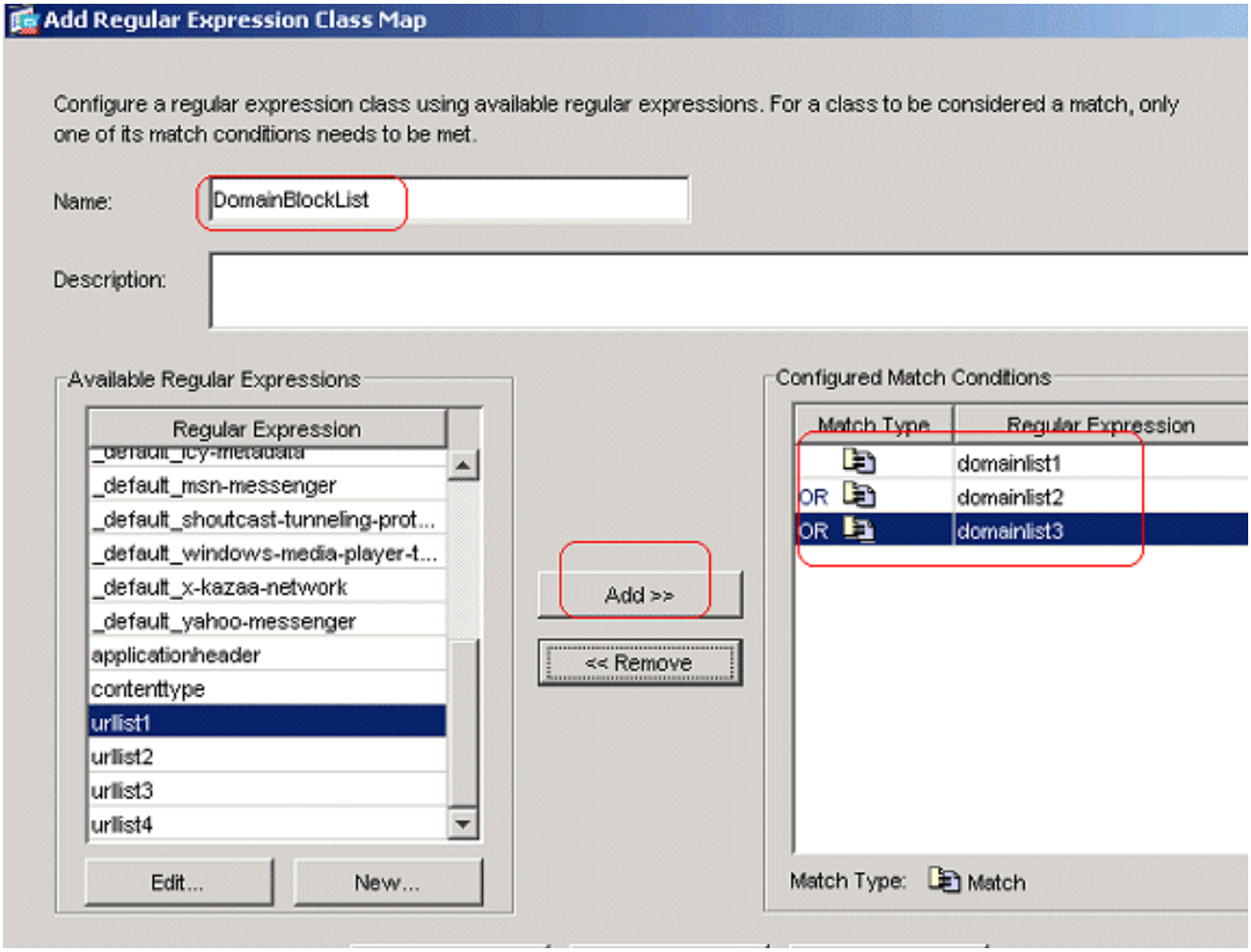


OK. Для перехвата заголовков различных приложений содержимого создайте регулярное выражение applicationheader. Нажмите кнопку

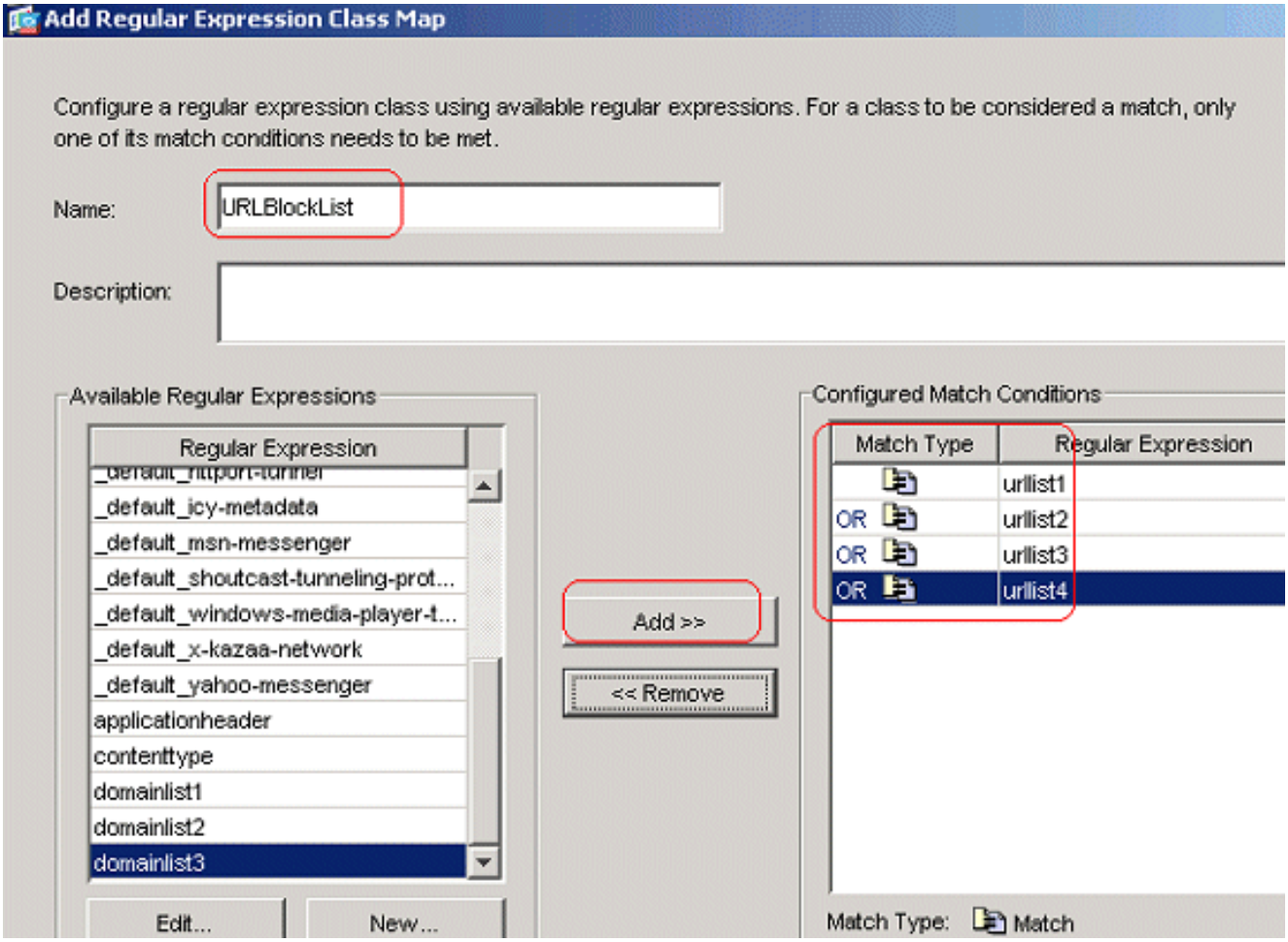


OK. Эквивалентная конфигурация в интерфейсе командной строки

2. Создание классов регулярных выраженийВыберите Configuration> Global Objects> Regular Expressions и нажмите Add под вкладкой Regular Expression Classes для создания различных классов.Для перехвата совпадений с любым из регулярных выражений domainlist1, domainlist2 и domainlist3 создайте класс регулярных выражений DomainBlockList. Нажмите кнопку
OK.

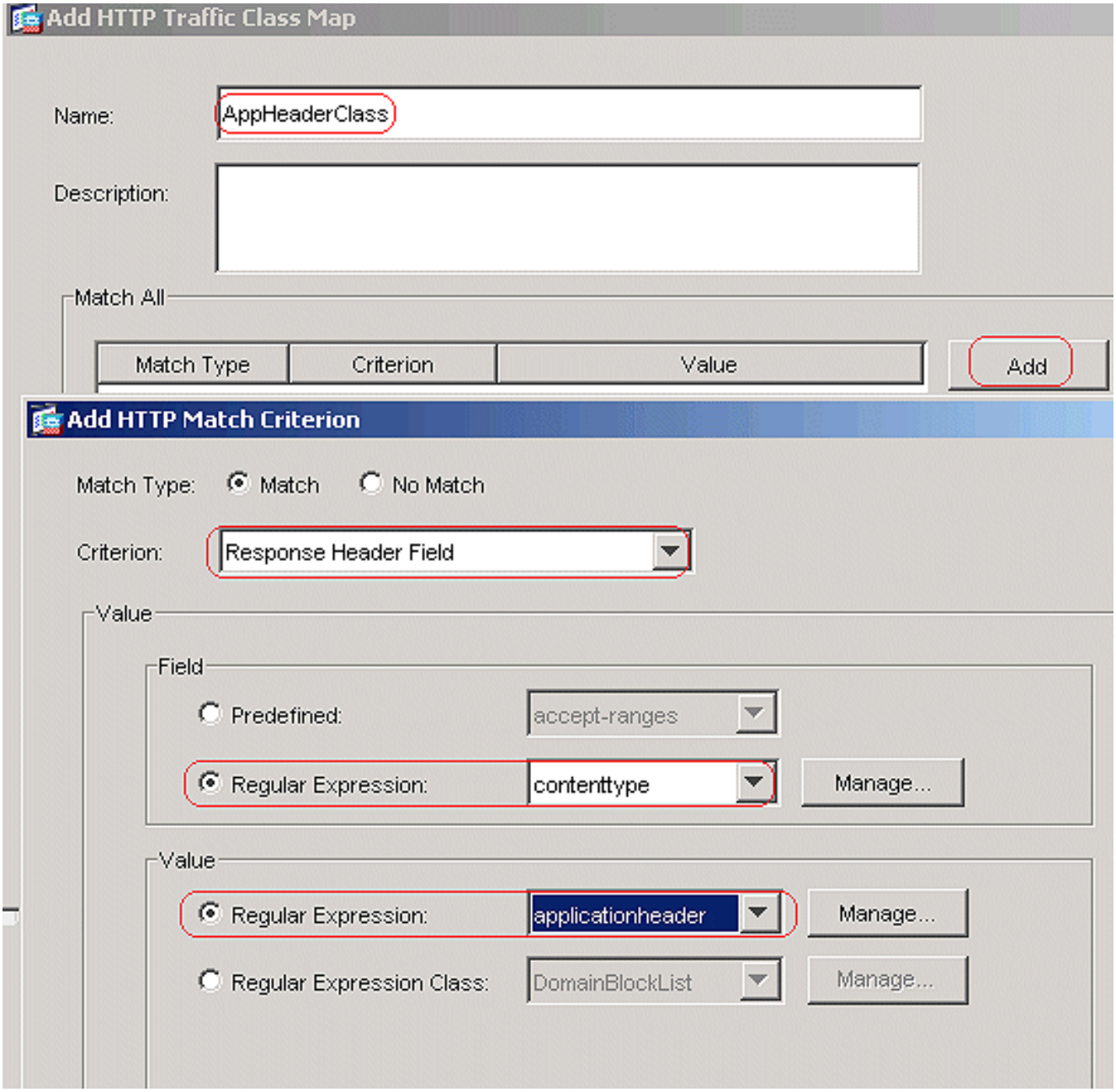


Для перехвата совпадений с любым из регулярных выражений urllist1, urllist2, urllist3 и urllist4 создайте класс регулярных выражений URLBlockList. Нажмите кнопку OK.

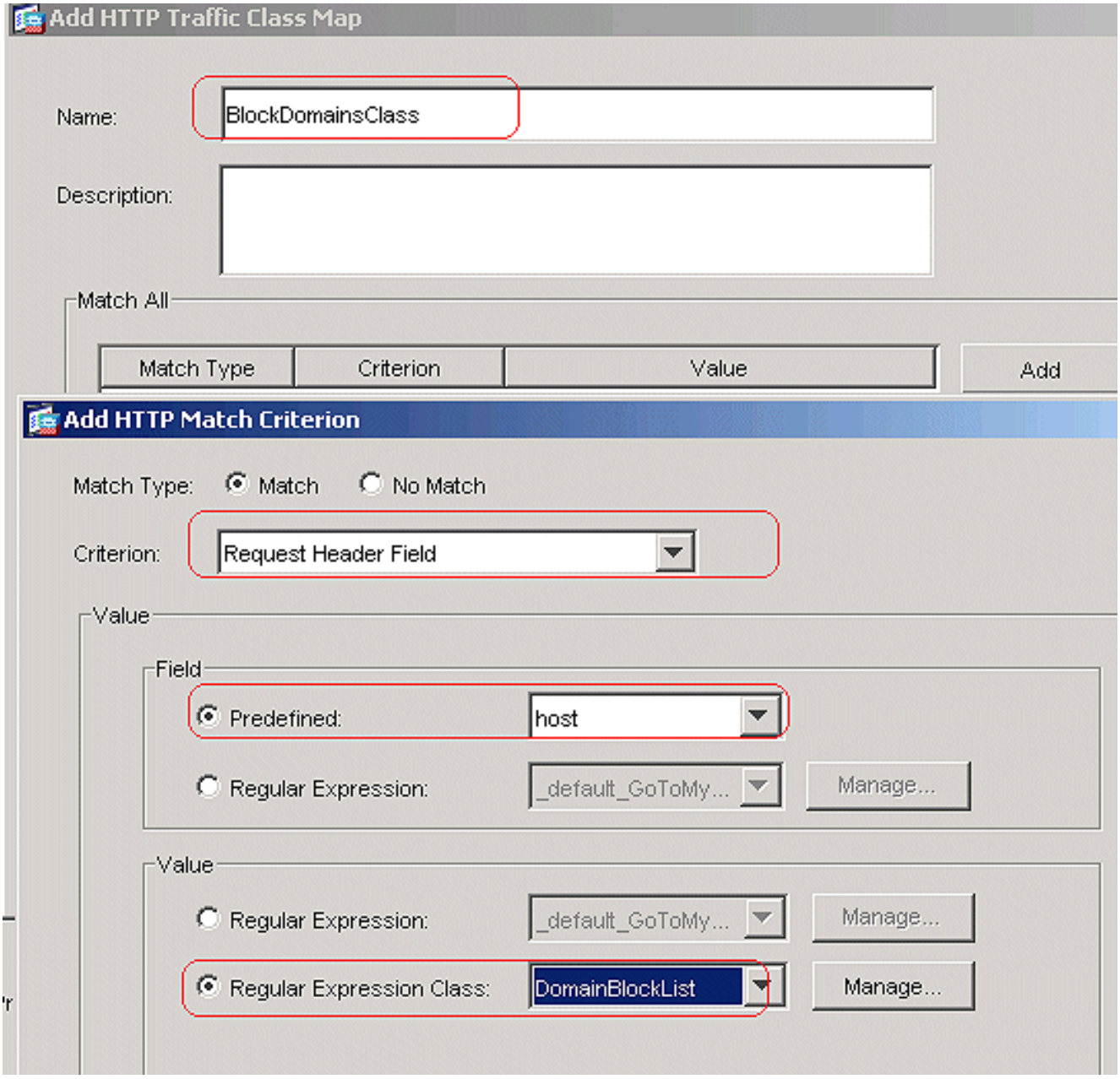


Эквивалентная конфигурация в интерфейсе командной строки

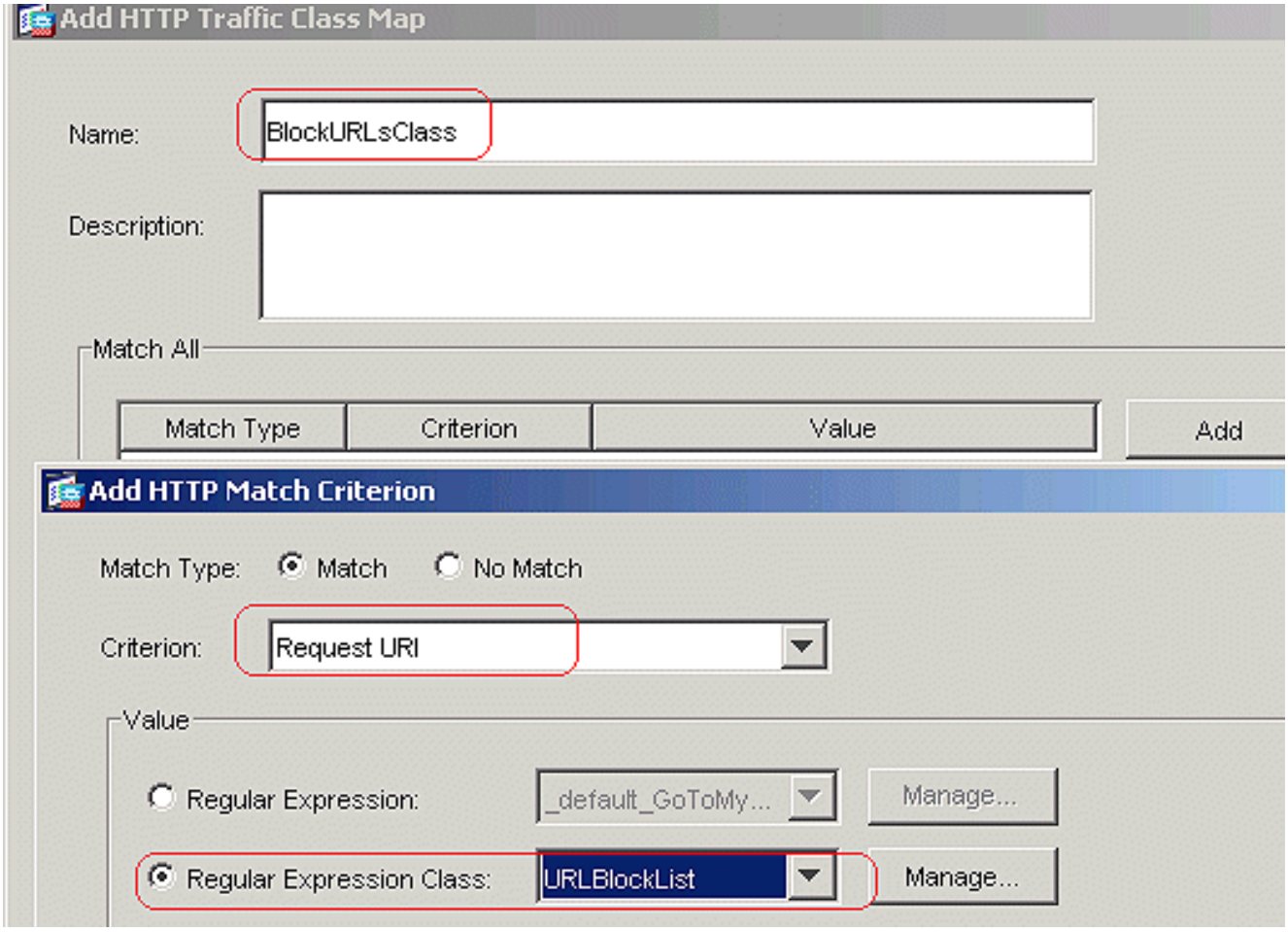
3. **Проверка указанного трафика с помощью карт класса**Выберите **Configuration> Global Objects> Class Maps> HTTP> Add** для создания карты классов для осмотра трафика HTTP, определенного различными регулярными выражениями.Создайте карту классов **AppHeaderClass** для соответствия с заголовком ответа с перехватами регулярного выражения.



Нажмите кнопку OK.Создайте карту классов **BlockDomainsClass** для соответствия с заголовком запроса с перехватами регулярного выражения.

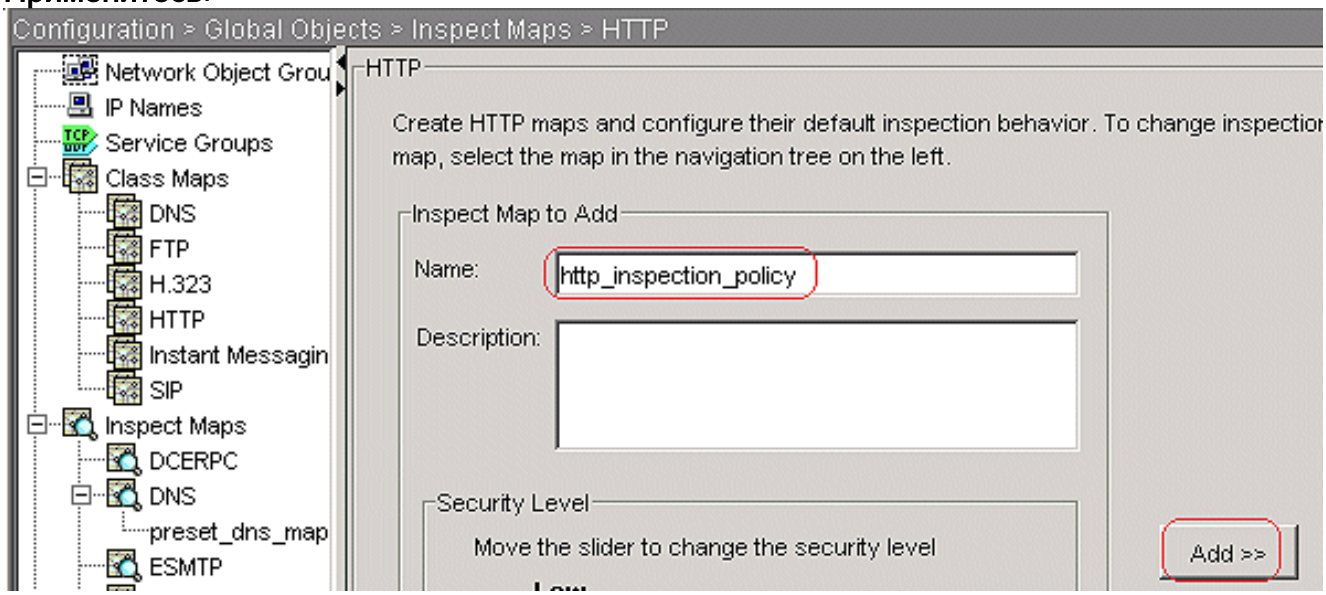


Нажмите кнопку OK.Создайте карту классов **BlockURLsClass** для соответствия с URI запроса с перехватами регулярного
выражения.

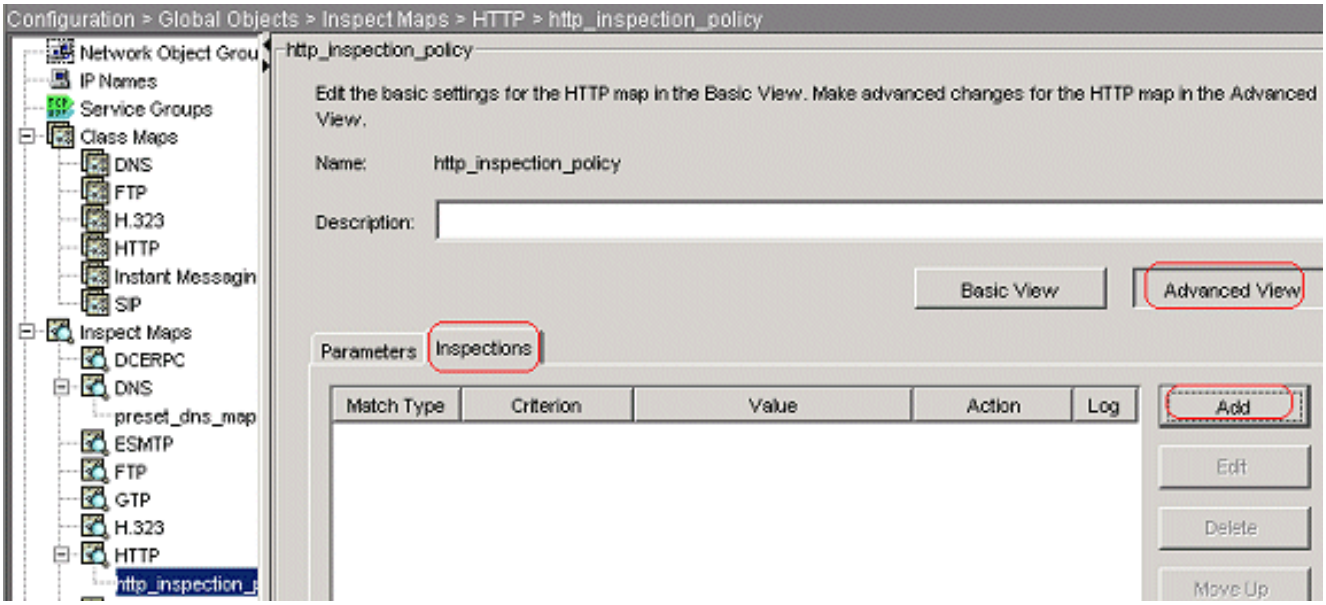


Нажмите кнопку ОК.Эквивалентная конфигурация в интерфейсе командной строки

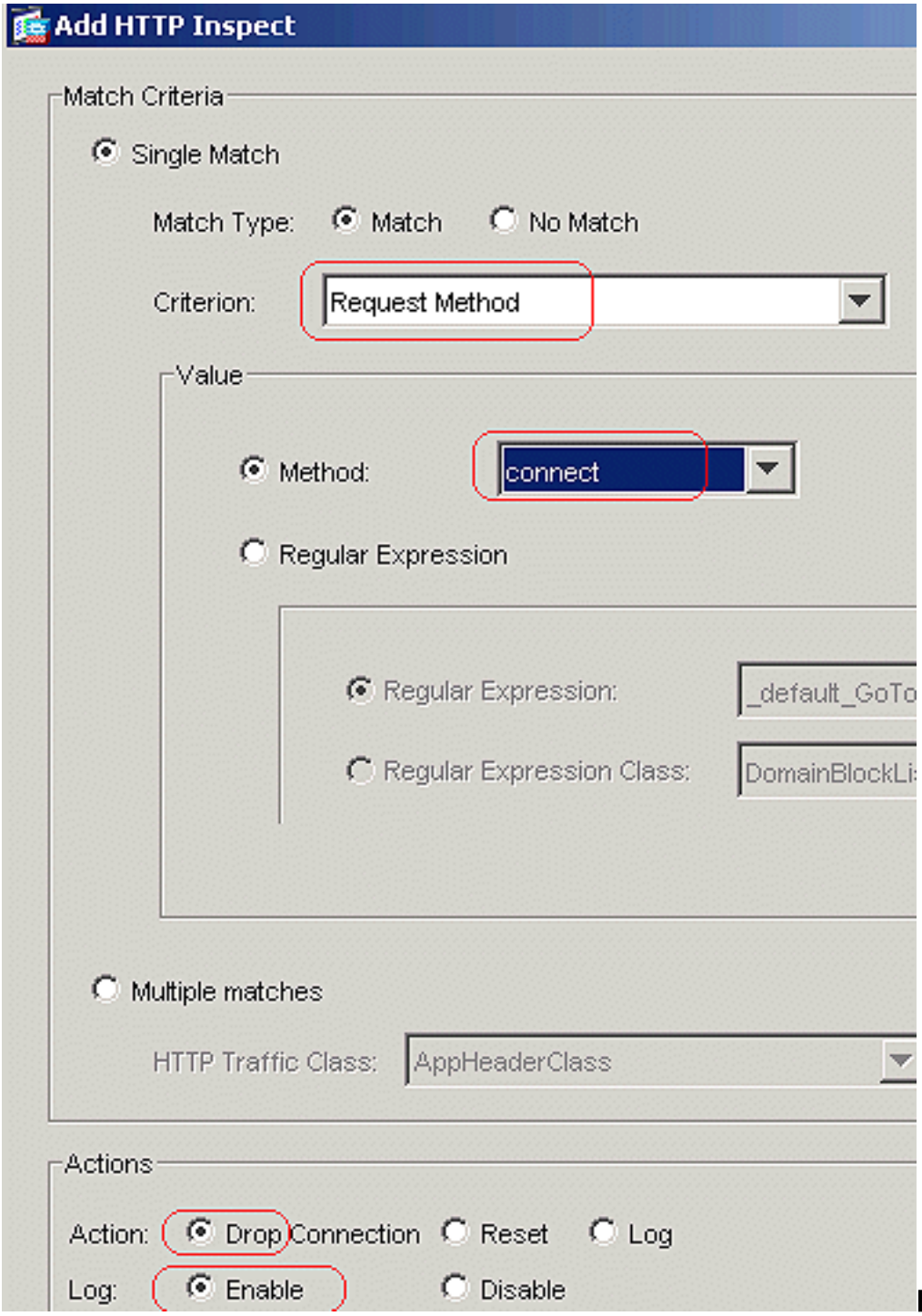
4. **Задание действий для перехваченного трафика в политике анализа**Выберите **Configuration> Global Objects> Inspect Maps> HTTP** для создания **http_inspection_policy** для установки действия для проверяемого трафика. **Нажмите Add** и **Применитесь**.



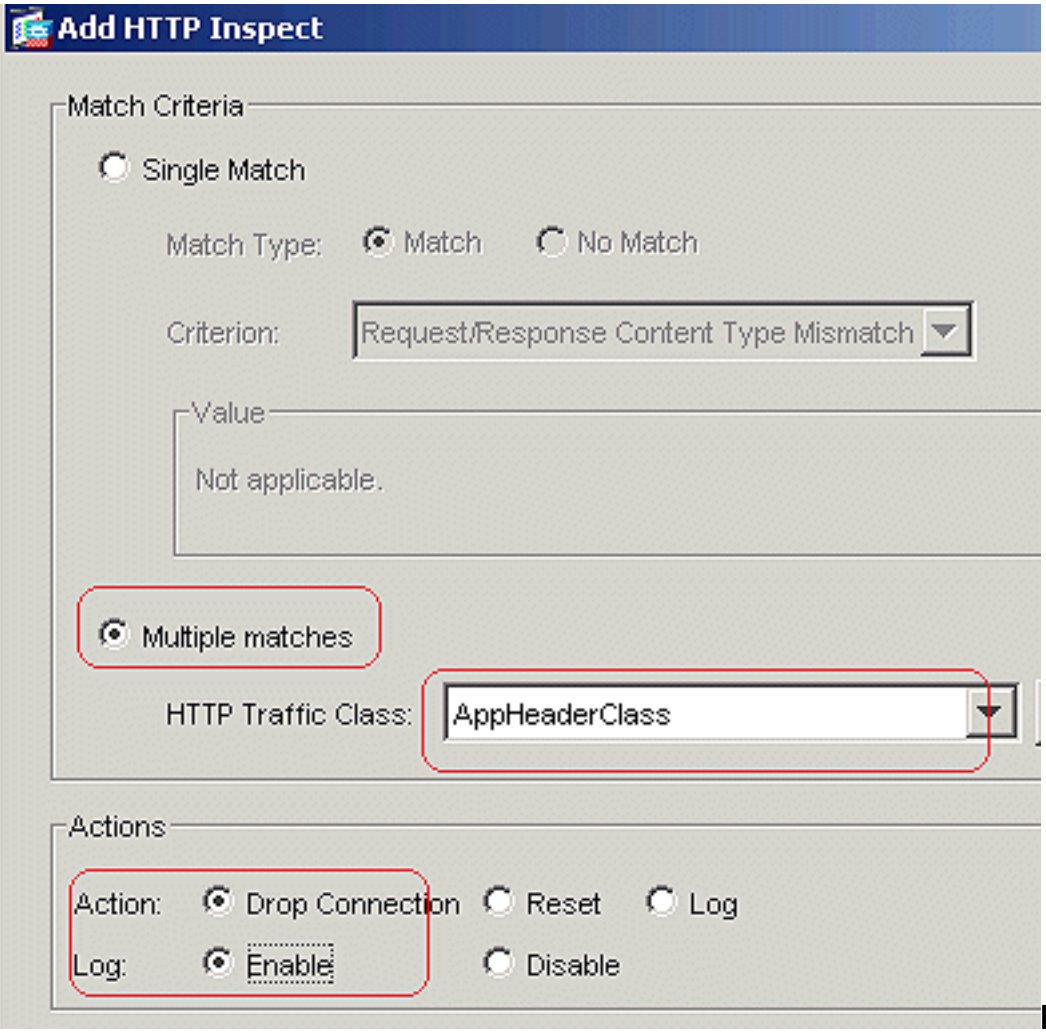
Выберите **Configuration> Global Objects> Inspect Maps> HTTP> http_inspection_policy** и нажмите **Advanced View> Inspections> Add** для установки действий для различных Классов, созданных до сих
пор.



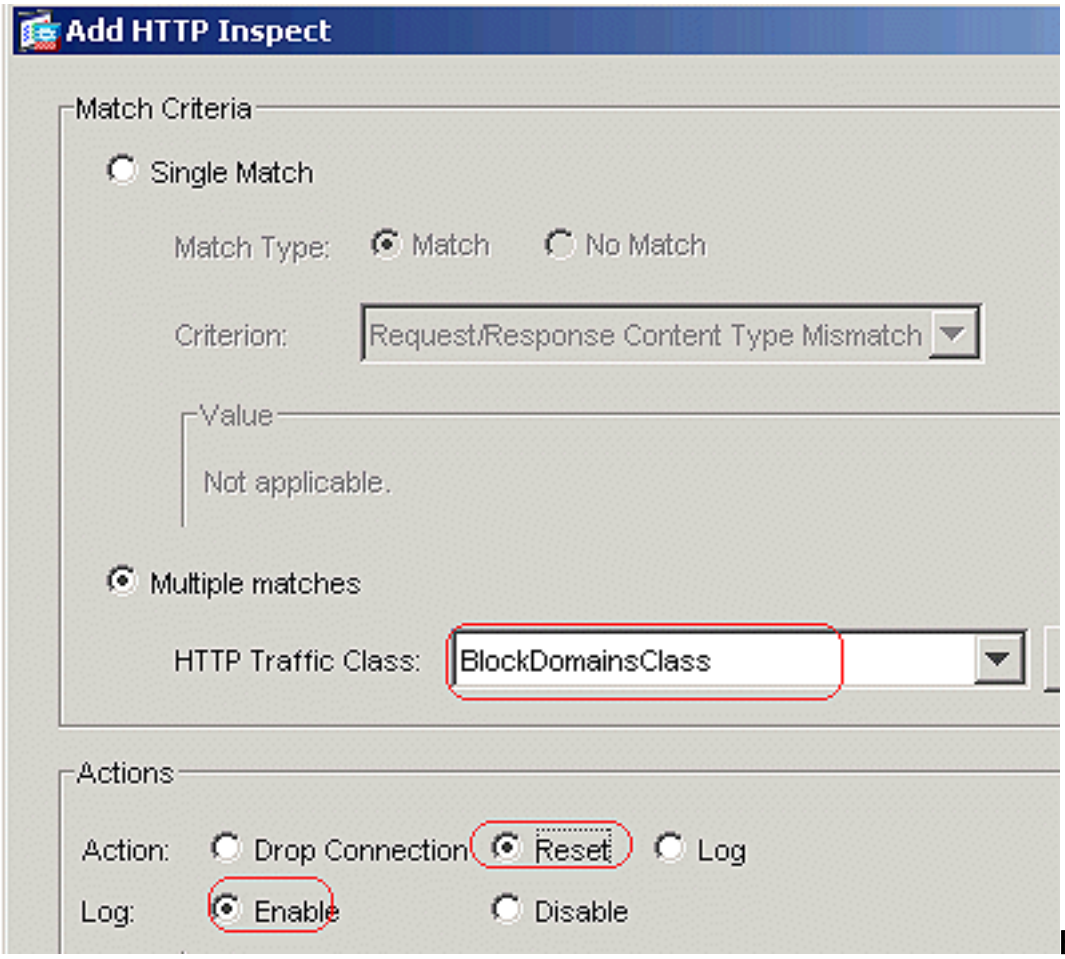
Нажмите кнопку ОК.Установите действие как **Соединение Отбрасывания**; **Включите** регистрацию для Критерия как Метод запроса и Значение как



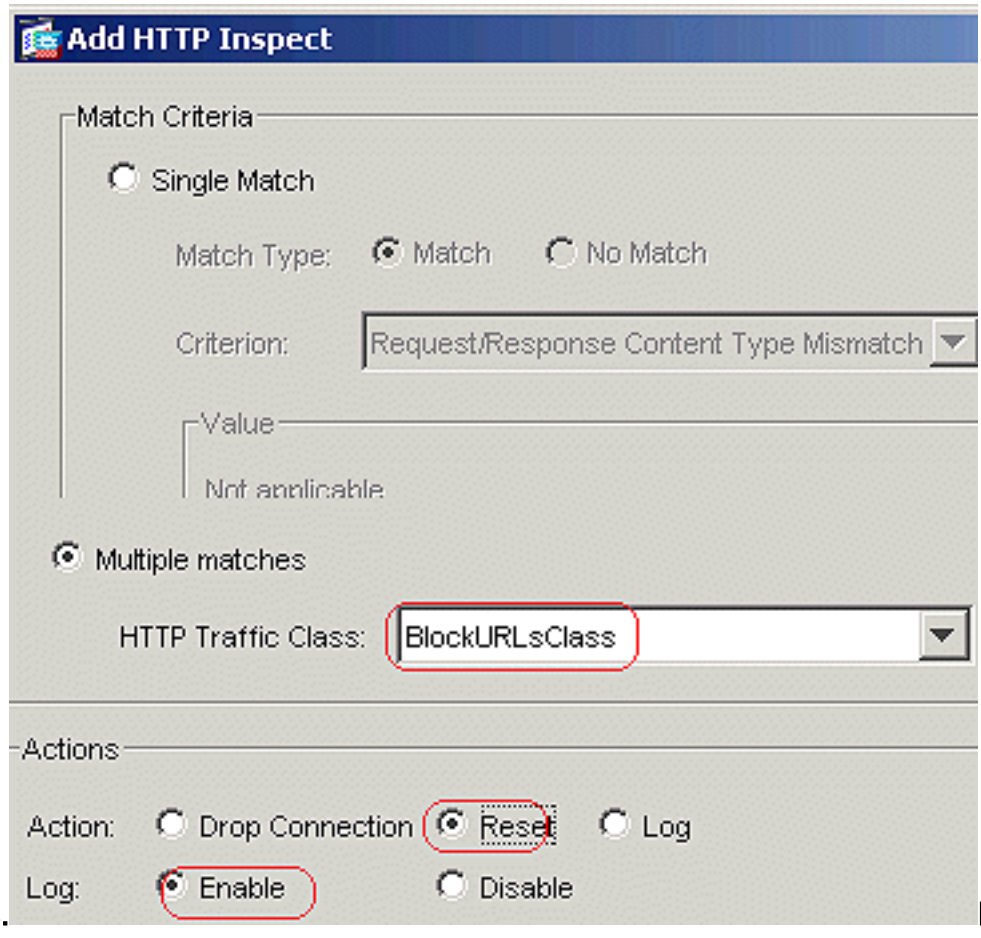
подключение. Нажмите кнопку OK.Установите действие Drop Connection (Разрывать соединение) и включите (Enable) ведение журнала для класса



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

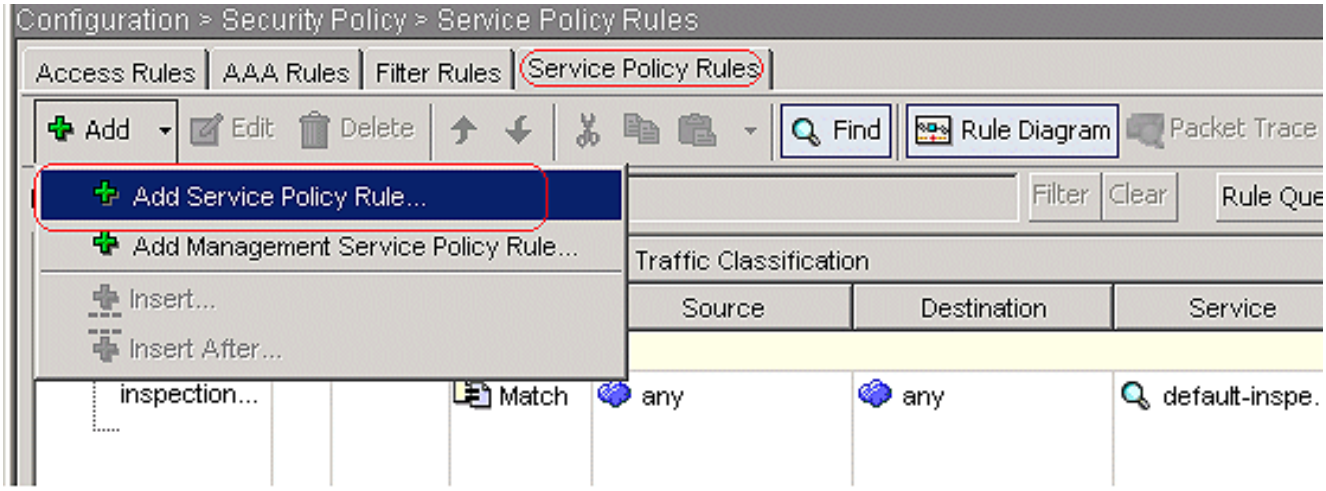


Нажмите кнопку ОК.Установите действие Reset (Выполнять сброс) и включите (Enable) ведение журнала для класса

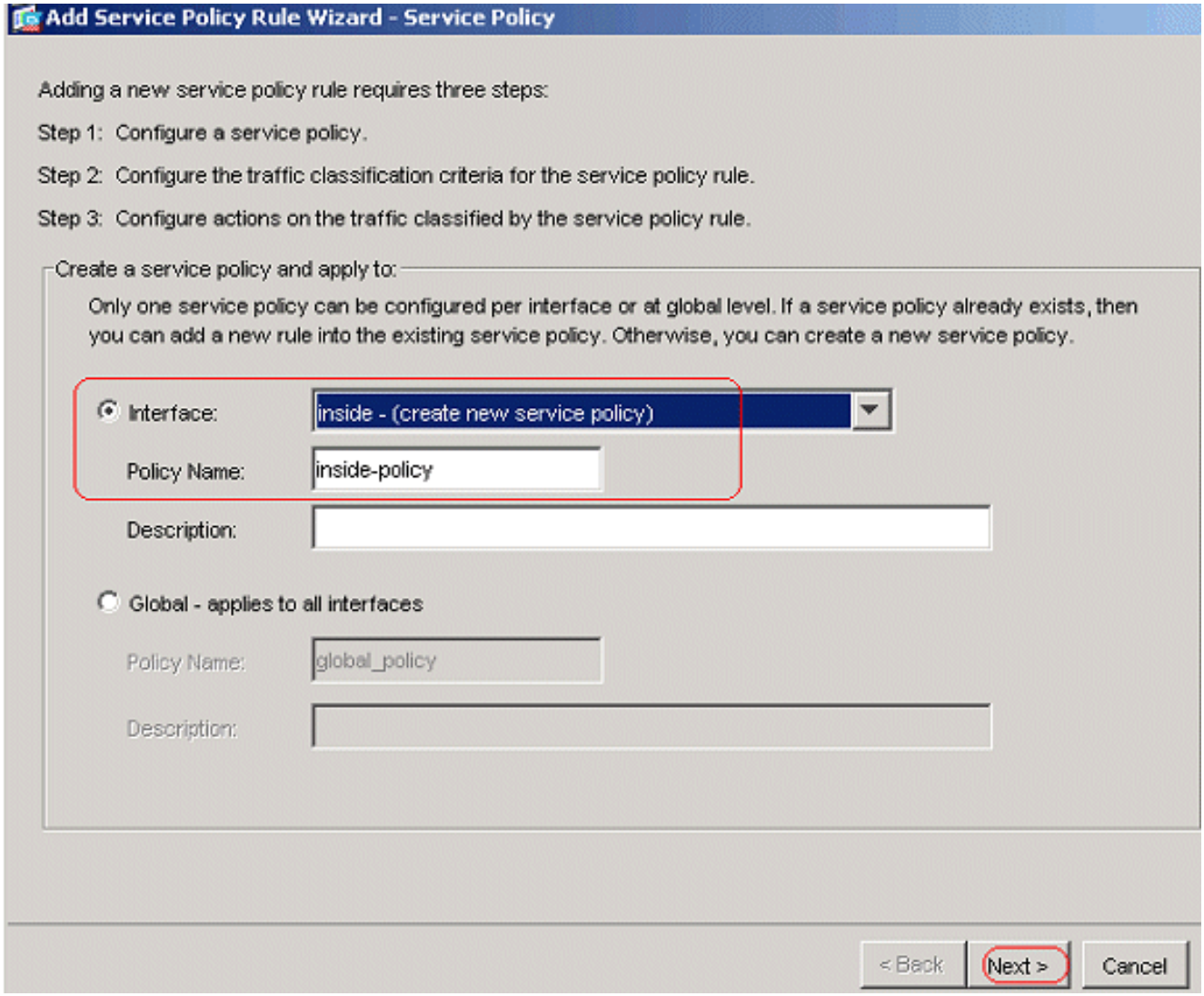


BlockURLsClass. Нажмите кнопку ОК.Щелкните "Применить".Эквивалентная конфигурация в интерфейсе командной строки

5. **Применение политики анализа HTTP для интерфейса**Выберите**> Security Configuration Политика>, Правила Политики обслуживания> Добавляют>, Добавляет Правило Политики обслуживания** под вкладкой Service Policy Rules.

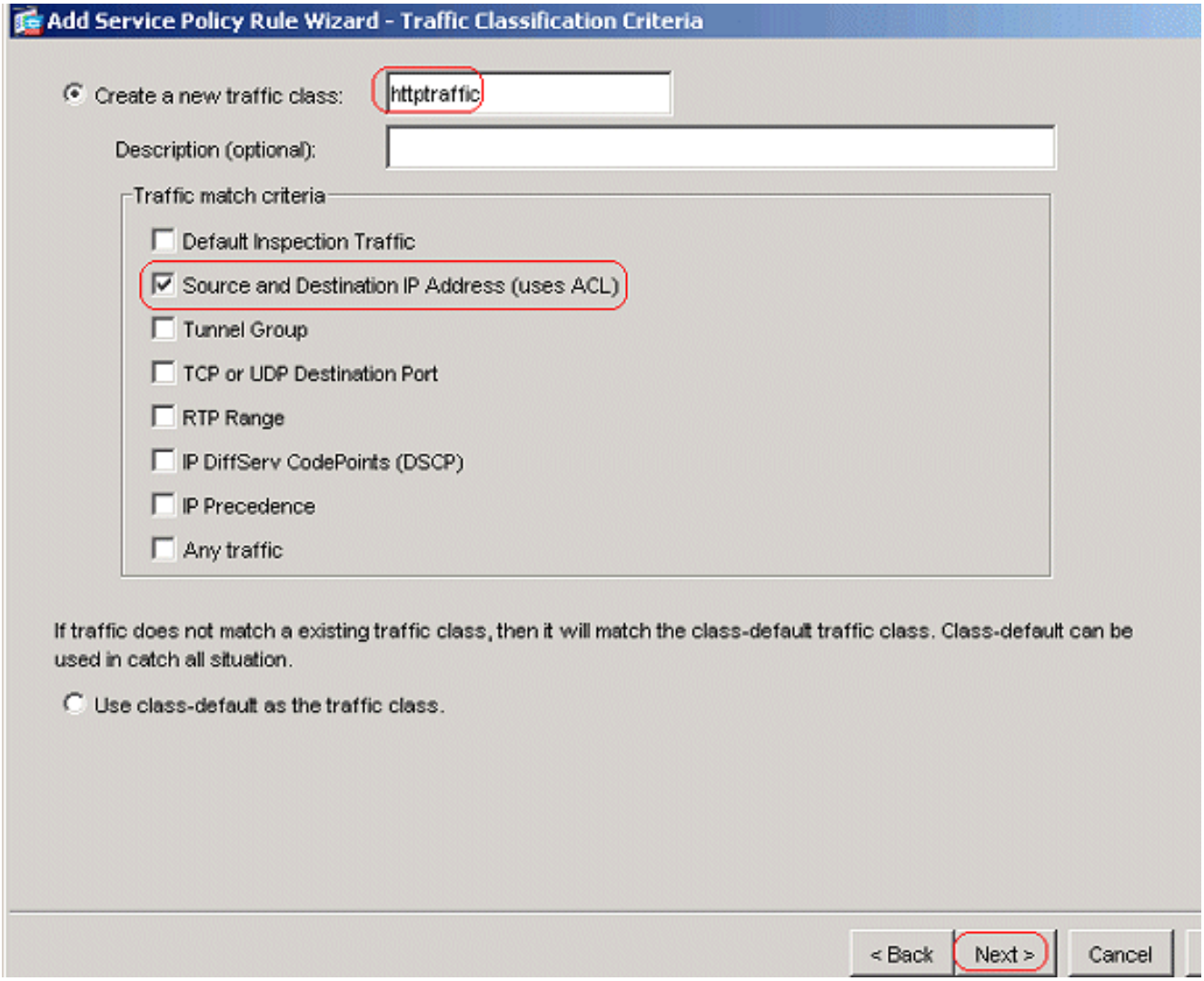


Трафик HTTPВыберите кнопку с зависимой фиксацией **Interface** с **внутренним интерфейсом** от раскрывающегося меню и Названия Политики как **внутренняя политика**. **Нажмите кнопку Next.**

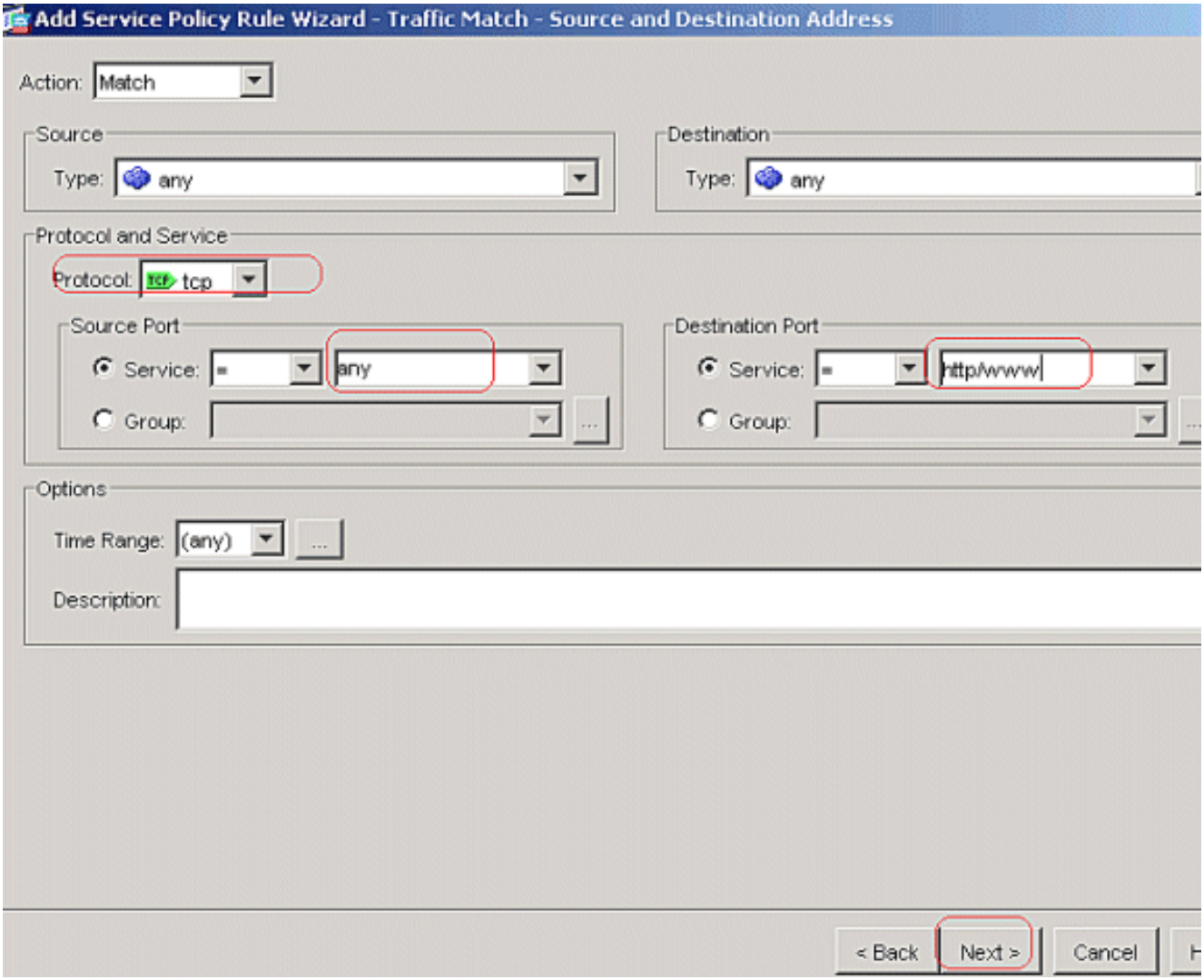


Создайте карту классов httptraffic и отметьте поля Source (Источник) и Destination IP Address (uses ACL) (IP-адрес получателя [с использованием списка ACL]). Нажмите

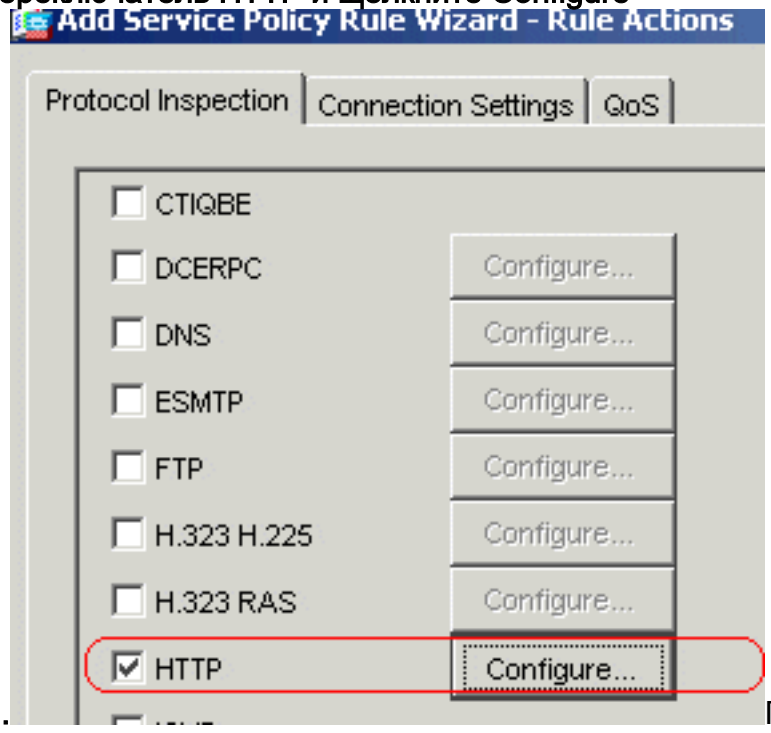
кнопку
Next.



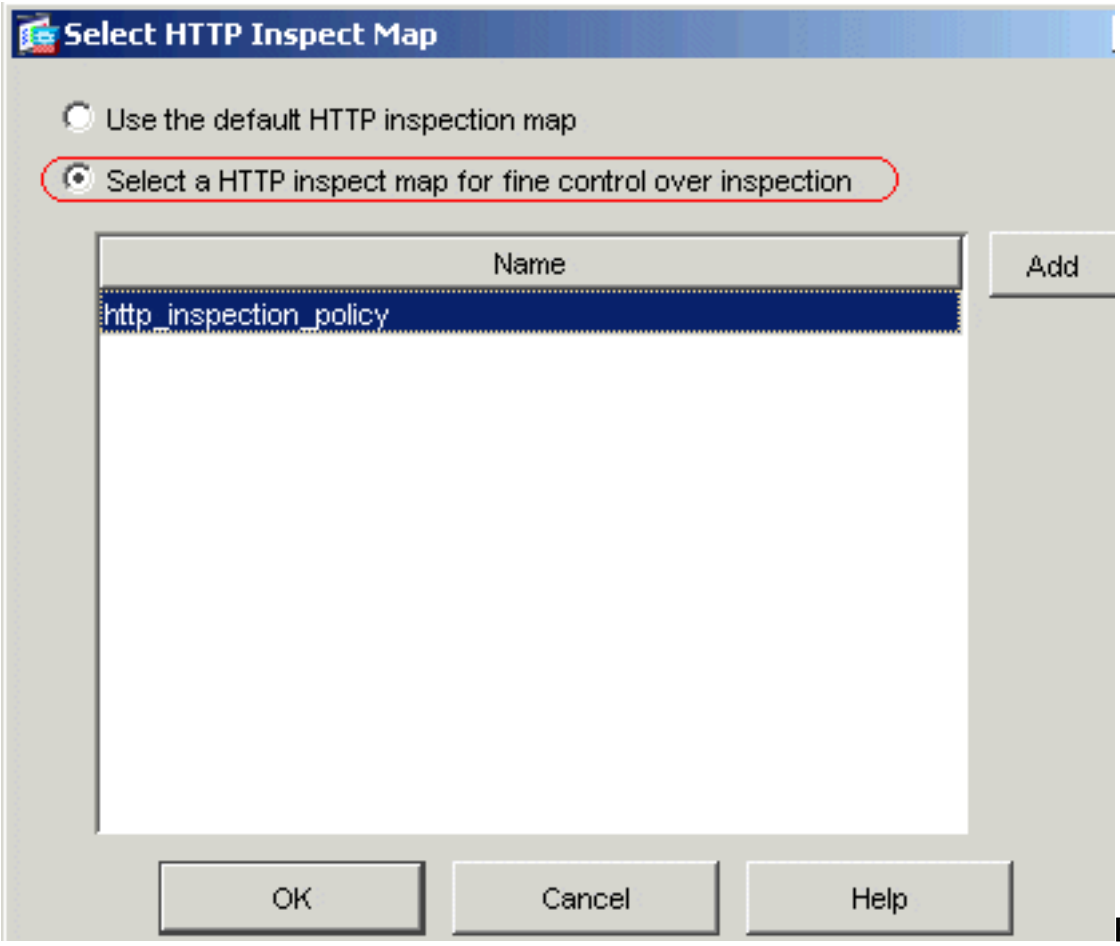
Выберите Source и Destination как **любой** с портом TCP как **HTTP**. **Нажмите кнопку Next.**



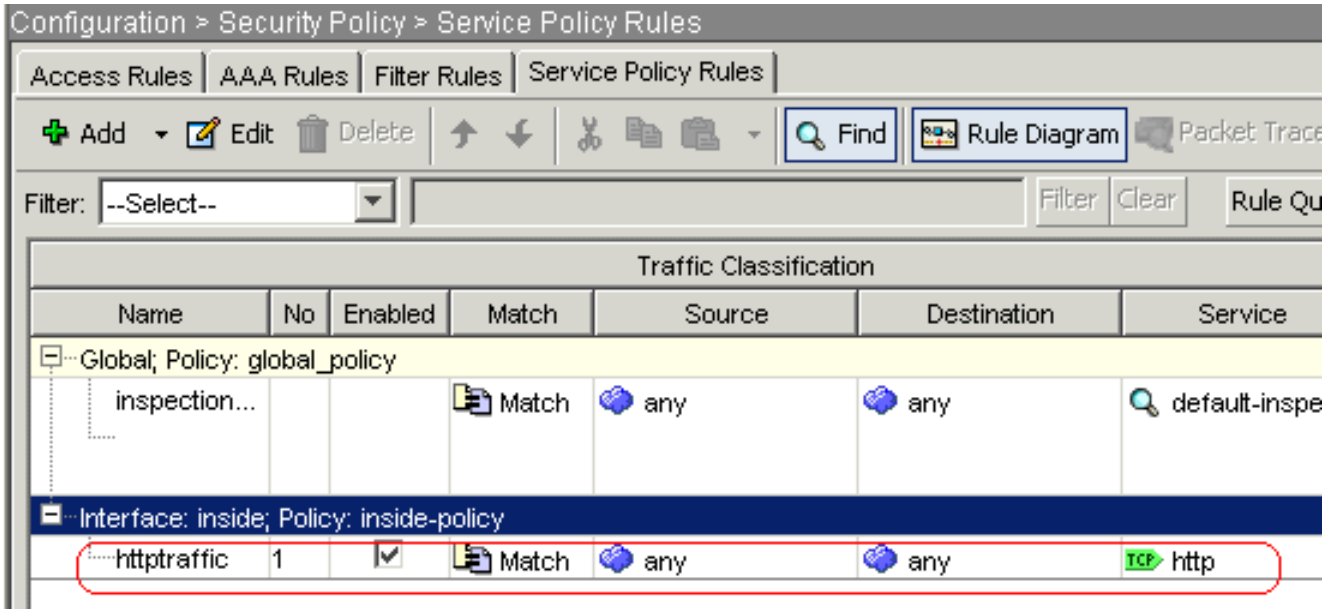
Выберите переключатель HTTP и щелкните Configure



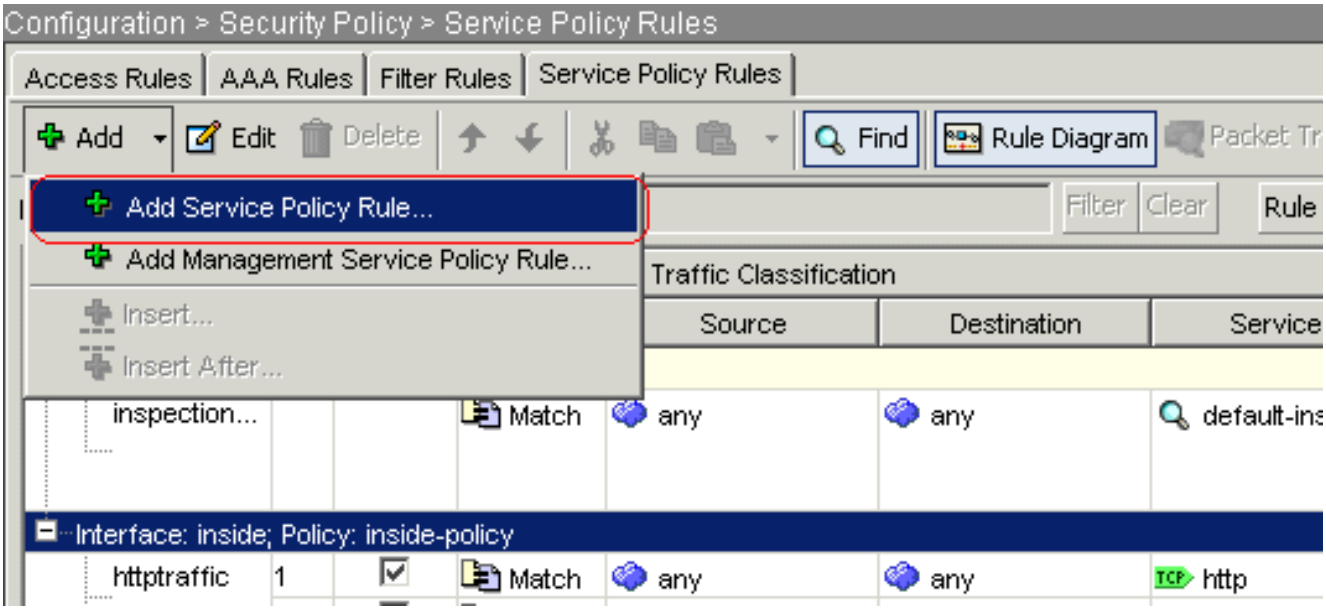
(Настроить). Проверьте кнопку с зависимой фиксацией Select, HTTP осматривает карту для контроля над контролем. Нажмите кнопку



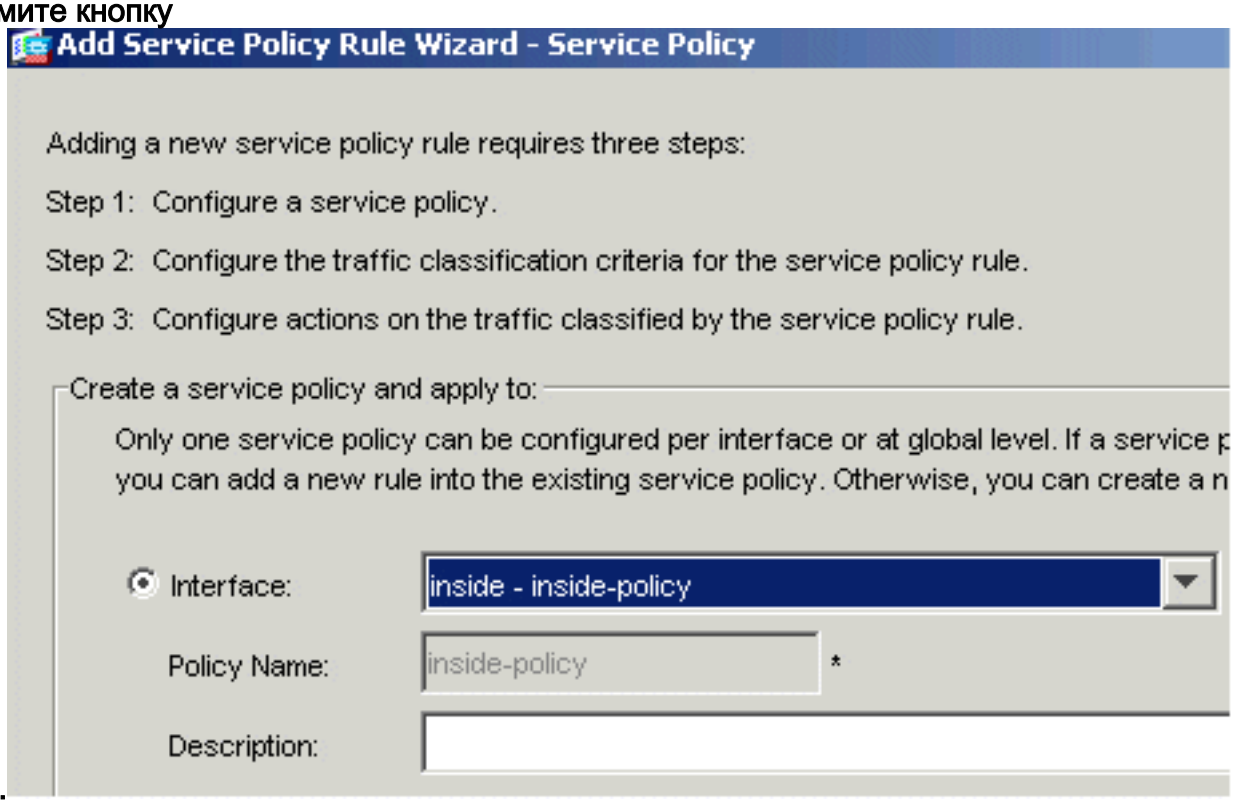
OK. Нажмите кнопку Finish.



Трафик через порт 8080Снова, нажмите Add>, Добавляет Правило Политики обслуживания.

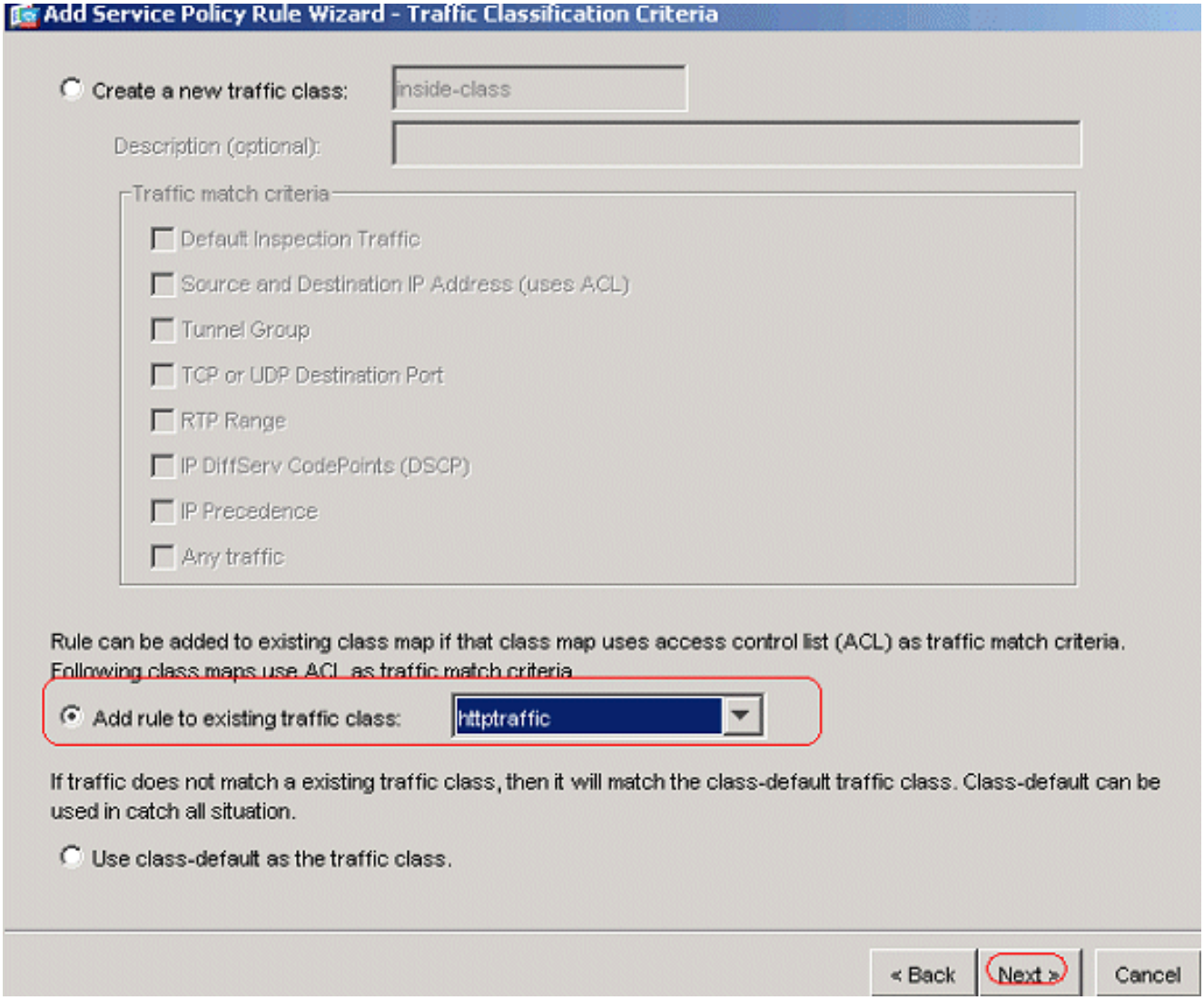


Нажмите кнопку

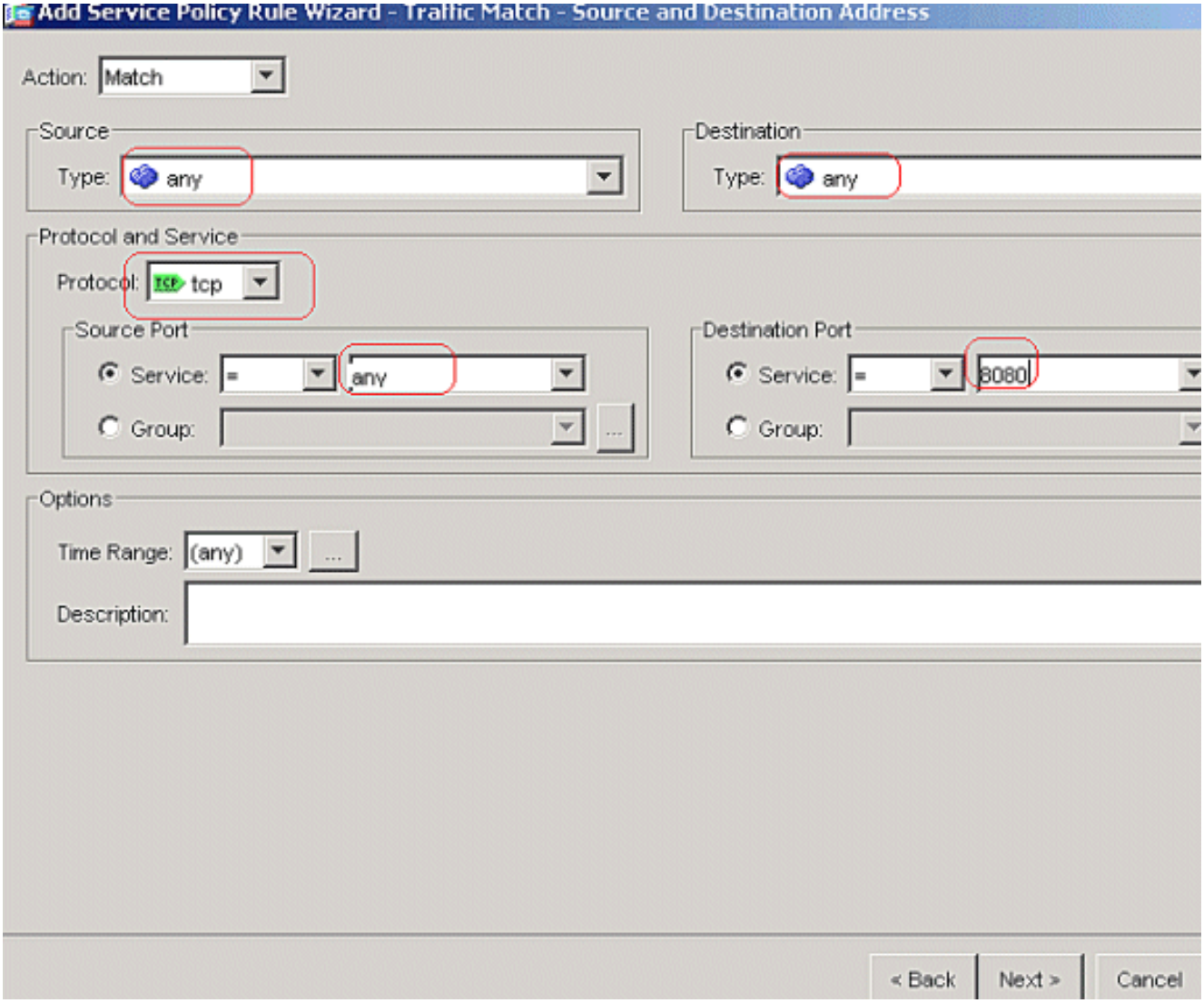


Next.

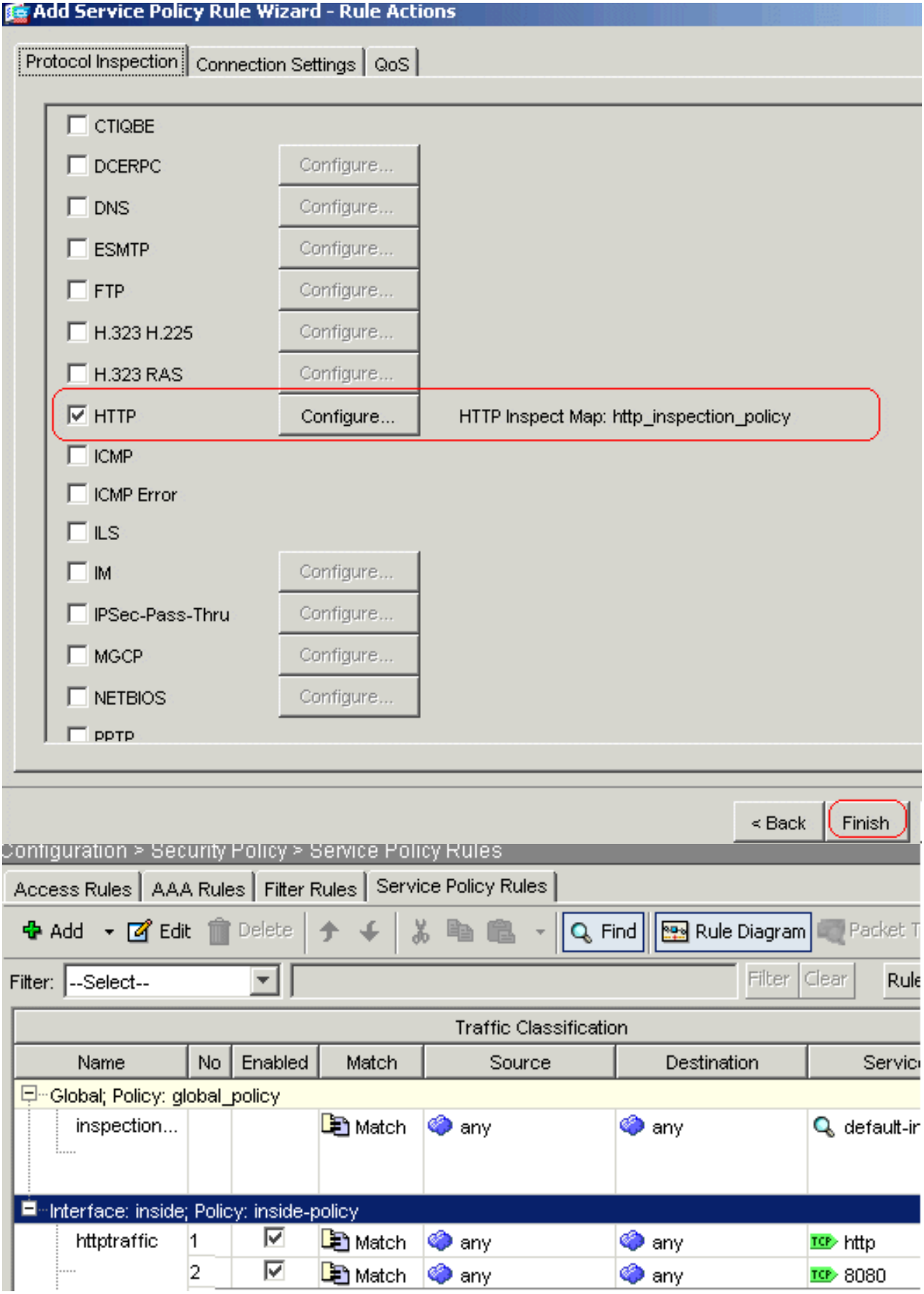
Выберите **правило Add к существующей** кнопке с зависимой фиксацией **класса трафика** и выберите **httptraffic** из раскрывающегося меню. **Нажмите кнопку Next.**



Выберите Source и Destination как **любой** с портом TCP как **8080**. **Нажмите кнопку Next.**



Нажмите кнопку Finish.



Щелкните "Применить".Эквивалентная конфигурация в интерфейсе командной строки

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 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

- Страница поддержки устройств адаптивной защиты Cisco
- Cisco Adaptive Security Device Manager (ASDM) страница технической поддержки
- Страница поддержки маршрутизаторов Cisco PIX серии 500
- Cisco Systems – техническая поддержка и документация