ASA/PIX 7.2: Determinados Web site do bloco (URL) que usam expressões regulares com exemplos da configuração MPF

Índice

Introdução

Este documento descreve como configurar os Cisco Security Appliances ASA/PIX 7.2 que usam Expressões Regulares com Estrutura de Política Modular (MPF) para bloquear determinados sites da Web (URL).

Nota: Esta configuração não obstrui todas as transferências do aplicativo. Para blocos de arquivo seguros, um dispositivo dedicado, tal como Websense, etc., ou o módulo, tal como o módulo CSC para o ASA, deve ser usado.

A filtração HTTPS não é apoiada no ASA. O ASA não pode fazer a inspeção de pacote de informação ou a inspeção profunda baseada na expressão regular para o tráfego HTTPS porque, no HTTPS, o índice do pacote é cifrado (SSL).

Pré-requisitos

Requisitos

Este documento supõe que o dispositivo do Cisco Security está configurado e trabalha corretamente.

Componentes Utilizados

- A ferramenta de segurança adaptável do Cisco 5500 Series (o ASA) essa executa a versão de software 7.2(2)
- Versão 5.2(2) do Cisco Adaptive Security Device Manager (ASDM) para o ASA 7.2(2)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração pode igualmente ser usada com o Cisco 500 Series PIX que executa a versão de software 7.2(2).

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Vista geral modular da estrutura de política

O MPF fornece um consistente e uma maneira flexível para configurar características da ferramenta de segurança. Por exemplo, você pode usar o MPF para criar uma configuração do intervalo que seja específica a um aplicativo de TCP/IP particular, ao contrário de um que se aplica a todos os aplicativos de TCP/IP.

O MPF apoia estas características:

- Normalização TCP, TCP e limites e intervalos da conexão de UDP, e de número de sequência TCP randomization
- CSC
- Inspeção de aplicativo
- IPS
- Vigilância de entrada de QoS
- QoS output o policiamento
- Fila de prioridade de QoS

A configuração do MPF consiste em quatro tarefas:

1. Identifique a camada 3 e o tráfego 4 a que você quer aplicar ações. Refira a identificação do tráfego usando um mapa da classe da camada 3/4 para mais informação.
2. (Inspeção de aplicativo somente) defina ações especiais para o tráfego da inspeção de aplicativo. Refira configurar ações especiais para inspeções de aplicativo para mais

informação.
3. Aplique ações à camada 3 e o tráfego 4. Refira a definição de ações usando um mapa de política da camada 3/4 para mais informação.
4. Ative as ações em uma relação. Refira a aplicação de uma política da camada 3/4 a uma relação usando uma política de serviços para mais informação.

Expressão regular

Uma expressão regular combina sequências de caracteres de texto ou literalmente enquanto uma corda exata, ou com metacharacters, assim que você pode combinar variações múltiplas de uma sequência de caracteres de texto. Você pode usar uma expressão regular para combinar o índice de determinado tráfego de aplicativo; por exemplo, você pode combinar uma série de URL dentro de um pacote de HTTP.

Nota: Use **Ctrl+V** para escapar todos os caracteres especiais no CLI, tal como um ponto de interrogação (?) ou a aba. Por exemplo, datilografe o **[Ctrl+V] g d** para incorporar **d? g na** configuração.

A fim criar uma expressão regular, use o comando do **regex**, que pode ser usado para as várias características que exigem a harmonização do texto. Por exemplo, você pode configurar ações especiais para a inspeção de aplicativo com estrutura de política modular com um mapa de política da inspeção (veja o tipo comando inspect do mapa de política). No mapa de política da inspeção, você pode identificar o tráfego que você quer atuar em cima se você cria um mapa da classe da inspeção que contenha uns ou vários **comandos match**, ou você pode usar **comandos match** diretamente no mapa de política da inspeção. Alguns **comandos match** deixaram-no identificar o texto em um pacote com uma expressão regular; por exemplo, você pode combinar séries de URL dentro dos pacotes de HTTP. Você pode agrupar expressões regulares em um mapa da classe da expressão regular (veja o tipo comando do mapa de classe do regex).

A tabela 1 alista os metacharacters que têm significados especiais.

Caracter e	Descrição	Notas
.	Ponto	Combina todo caractere único. Por exemplo, **d.g combina o** cão, o dag, o dtg, e a toda a palavra que contiver aqueles caráteres, tais como o doggonnit.
(exp)	Subexpression	Um subexpression segrega caráteres dos caráteres circunvizinhos, de modo que você possa usar outros metacharacters no subexpression. Por exemplo, **d (o|o** cão dos fósforos **a) g** e o dag, mas **fazem|**os fósforos **AG** fazem e AG. Um subexpression pode igualmente ser usado com quantifiers da repetição para diferenciar os caráteres significados para a repetição. Por exemplo, **ab(xy){3}z** combina o abxyxyxyz.
|	Alternação	Combina uma ou outra expressão que separa. Por exemplo, **cão|o gato** combina

		o cão ou o gato.
?	Ponto de interrogação	Um quantifier que indique que há 0 ou 1 da expressão anterior. Por exemplo, **lo? o SE** combina o lse ou perde-o. **Nota:** Você deve incorporar **Ctrl+V** e então o ponto de interrogação ou então a função de ajuda são invocados.
*	Asterisco	Um quantifier que indique que há 0, 1 ou todo o número da expressão anterior. Por exemplo, o **lo*se** combina o lse, perde, fraco, e assim por diante.
{x}	Repita o quantifier	Repita exatamente tempos x. Por exemplo, **ab(xy){3}z** combina o abxyxyxyz.
{x,}	Quantifier mínimo da repetição	Repita pelo menos tempos x. Por exemplo, **ab(xy){2,}z** combina o abxyxyz, abxyxyxyz, e assim por diante.
[abc]	Classe de caráter	Combina todo o caráter nos suportes. Por exemplo, o **[abc]** combina a, b, ou C.
[^abc]	Classe de caráter negada	Combina um único caráter que não seja contido dentro dos suportes. Por exemplo, o **[^abc]** combina todo o caráter a não ser a, b, ou o **[^A-Z]** C. combina qualquer único caráter que não for uma letra maiúscula.
[a-c]	Classe da escala do caráter	Combina todo o caráter na escala. **o [a-z]** combina toda a letra minúscula. Você pode misturar caráteres e escalas: **o [abcq-z]** combina a, b, c, q, r, s, t, u, v, w, x, y, z, e assim que faz o **[a-cq-z]**. O caráter do traço (-) é literal somente se é o último ou o primeiro caráter dentro dos suportes: **[abc-]** ou **[-abc]**.
""	Cotação - marcas	Conservas que arrastam ou que conduzem espaços na corda. Por exemplo, o **"teste"** preserva o espaço principal quando procura um fósforo.
^	Sinal de intercalação	Especifica o começo de uma linha.
\	Caractere de escape	Quando usado com um metacharacter, combina um caráter literal. Por exemplo, **\[**combina o suporte quadrado esquerdo.
carv	Caract	Quando um caráter não é um

ão animal	ere	metacharacter, combina o caráter literal.
\ **r**	Tecla semelhante a tecla ENTER	Combina uma tecla semelhante a tecla ENTER 0x0d.
\ **n**	Newline	Combina uma nova linha 0x0a.
\ **t**	Aba	Combina uma aba 0x09.
\ **f**	Formfeed	Combina uma alimentação de formulário 0x0c.
\ xNN	Número hexadecimal escapado	Combina um caractere ASCII com o hexadecimal (exatamente dois dígitos).
\ NNN	Número octal escapado	Combina um caractere ASCII como octal (exatamente três dígitos). Por exemplo, o caráter 040 representa um espaço.

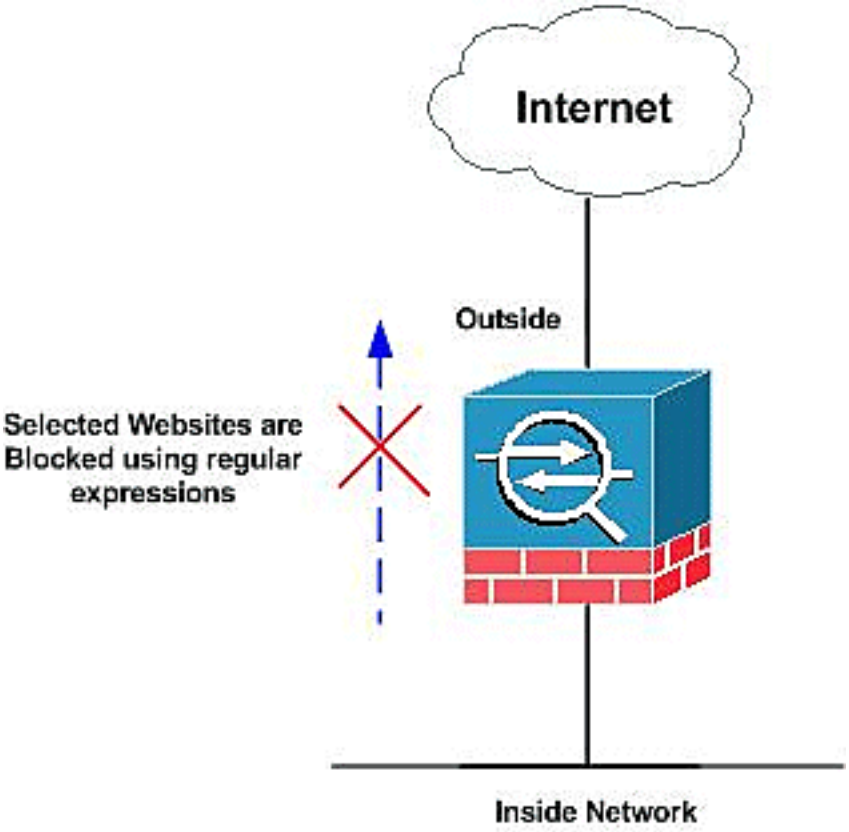
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- Configuração do ASA via CLI
- Configuração ASA 7.2(x) com ASDM 5.2

Configuração do ASA via CLI

Configuração do ASA via CLI

```
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),
```

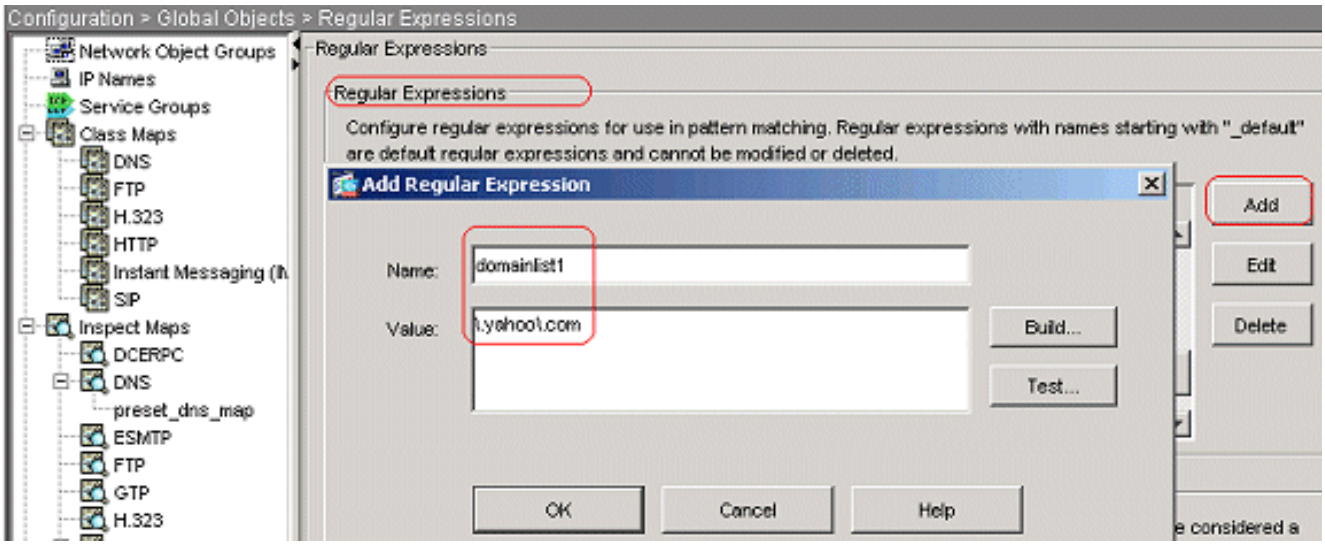
.xls(ms-excel), .ppt to be captured and provided !--- the http version being used by web browser must be either 1.0 or 1.1 **regex urllist4 ".*\.([Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz]) HTTP/1.[01]"** *!--- Extensions such as .zip, .tar, .tgz to be captured and provided !--- the http version being used 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#
```

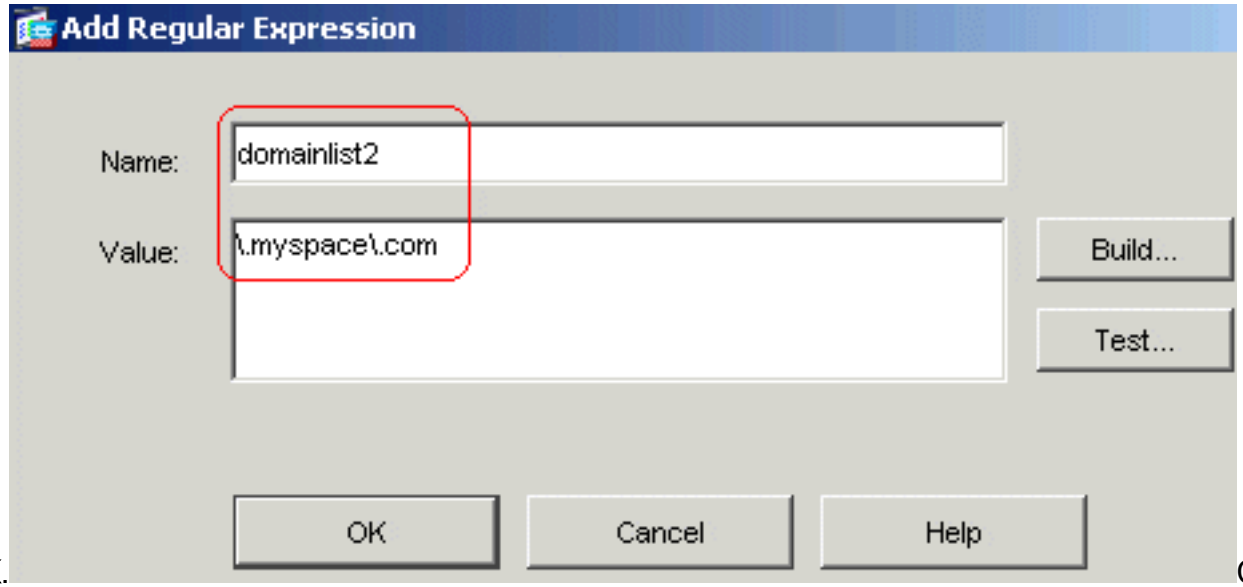
Configuração ASA 7.2(x) com ASDM 5.2

Termine estas etapas a fim configurar as expressões regulares e aplicá-las ao MPF para obstruir os Web site específicos:

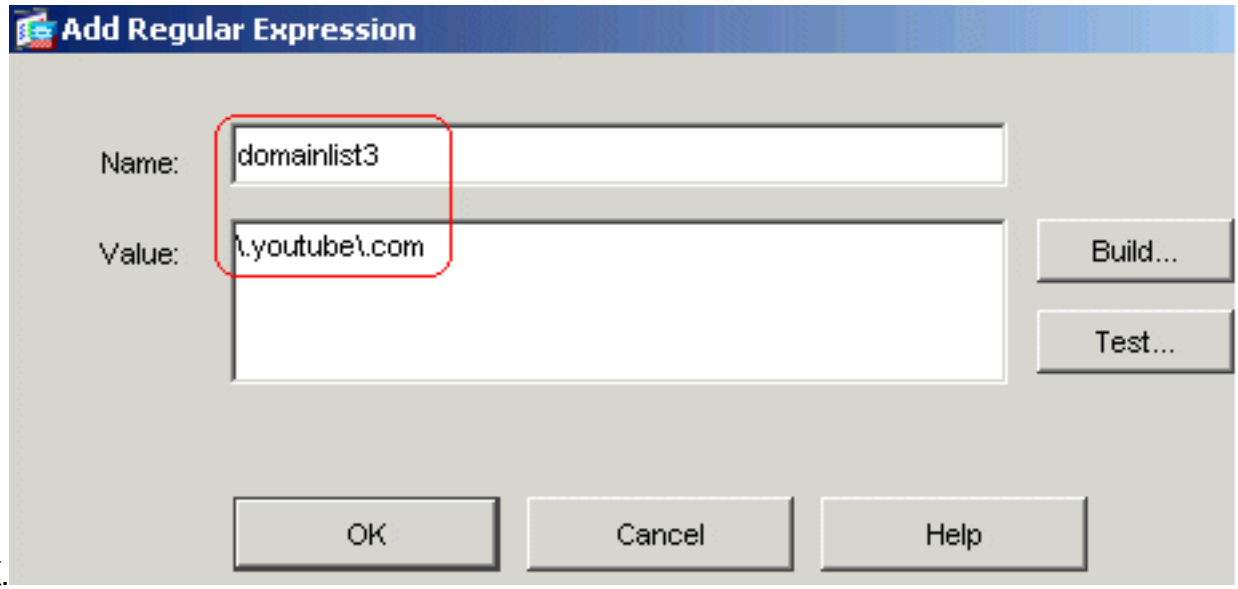
1. **Crie expressões regulares**Escolha a **configuração > objetos > expressões regulares globais** e o clique **adiciona** sob a aba da expressão regular a fim criar expressões regulares.Crie uma expressão regular **domainlist1** a fim capturar o Domain Name **yahoo.com**. Clique em **OK**.



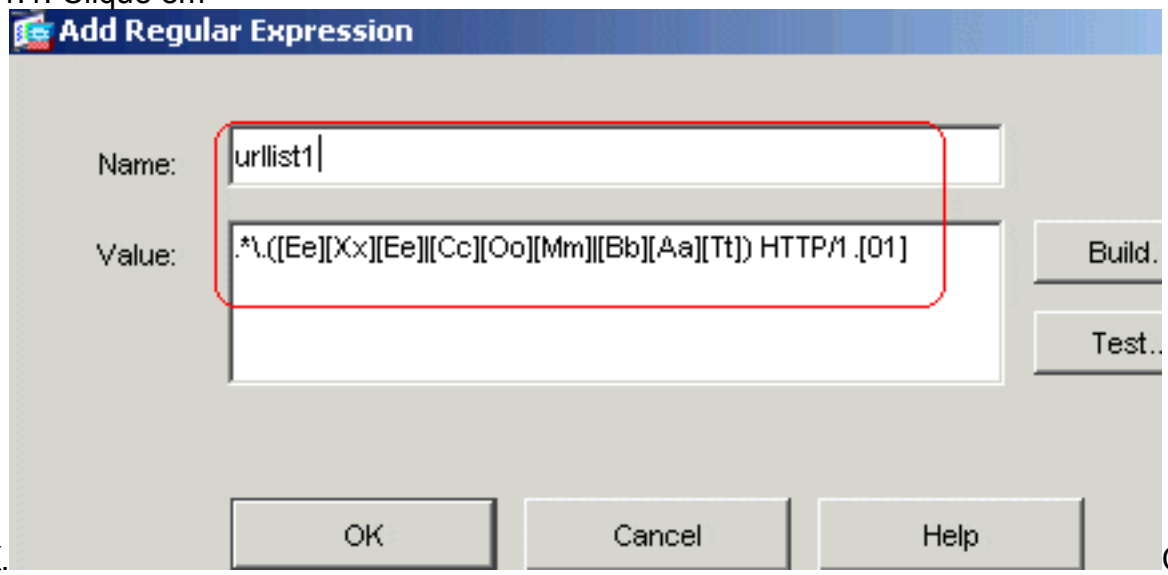
Crie uma expressão regular **domainlist2** a fim capturar o Domain Name **myspace.com**. Clique em



OK. Crie uma expressão regular **domainlist3** a fim capturar o Domain Name **youtube.com**. Clique em

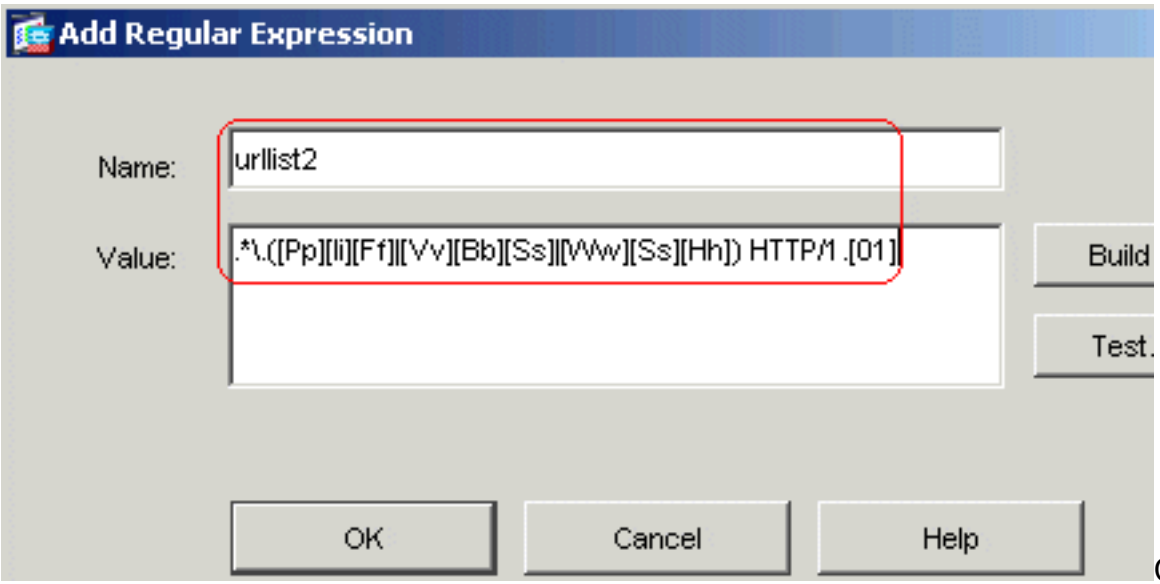


OK. Crie uma expressão regular **urllist1** a fim capturar as extensões de arquivo tais como o **exe**, a **COM**, e o **bastão** contanto que a versão HTTP usada pelo navegador da Web deve ser 1.0 ou 1.1. Clique em

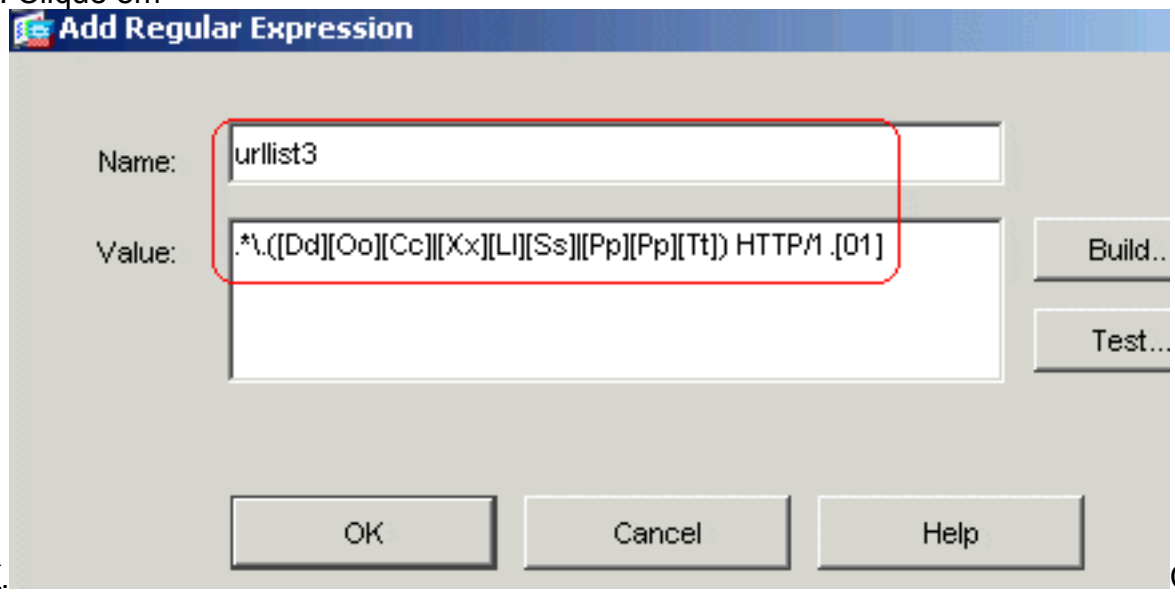


OK. Crie uma expressão regular **urllist2** a fim capturar as extensões de arquivo, tais como **pif**, **vbs**, e **wsh** contanto que a versão HTTP que está usada pelo navegador da Web é 1.0 ou 1.1.

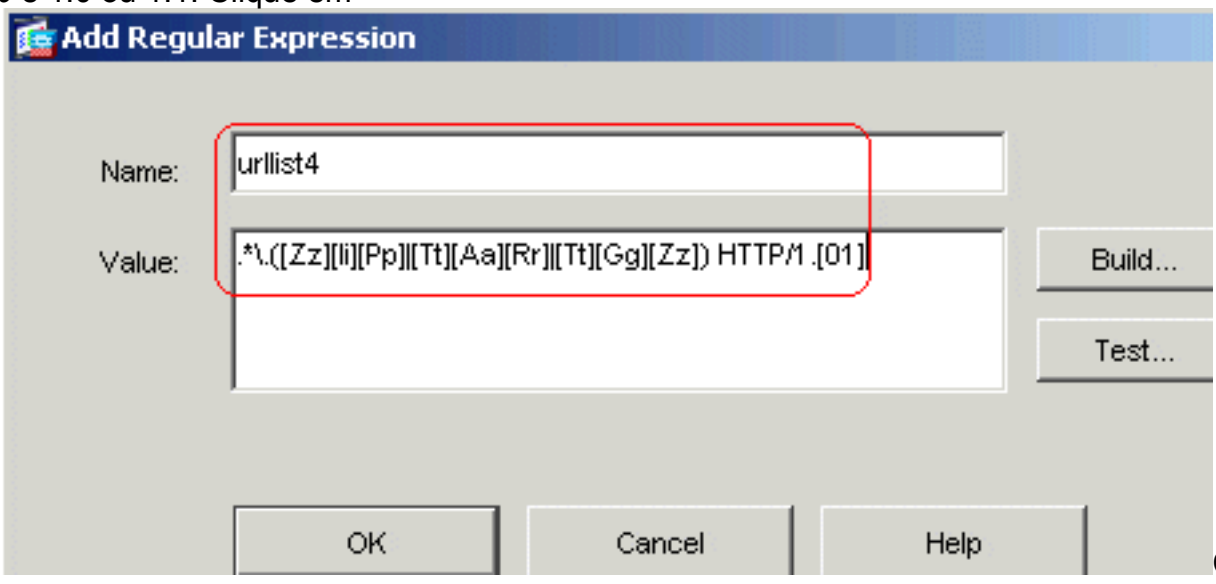
Clique em



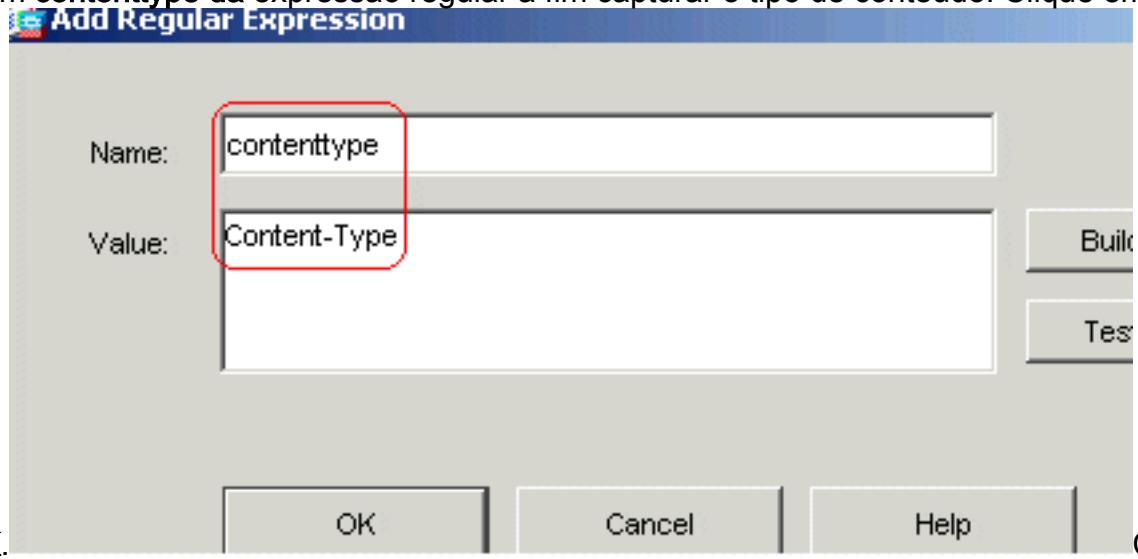
OK. Crie uma expressão regular **urllist3** a fim capturar as extensões de arquivo, tais como o **doc**, os **xls**, e o **ppt** contanto que a versão HTTP que está usada pelo navegador da Web é 1.0 ou 1.1. Clique em

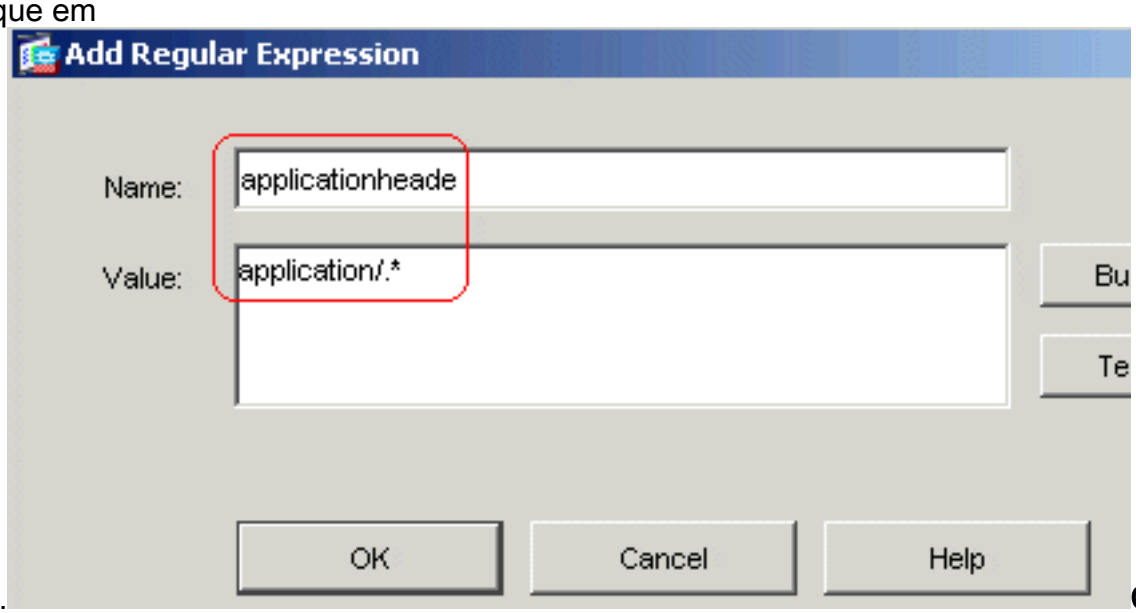


OK. Crie uma expressão regular **urllist4** a fim capturar as extensões de arquivo, tais como o **fecho de correr**, o **alcatrão**, e o **tgz** contanto que a versão HTTP que está usada pelo navegador da Web é 1.0 ou 1.1. Clique em



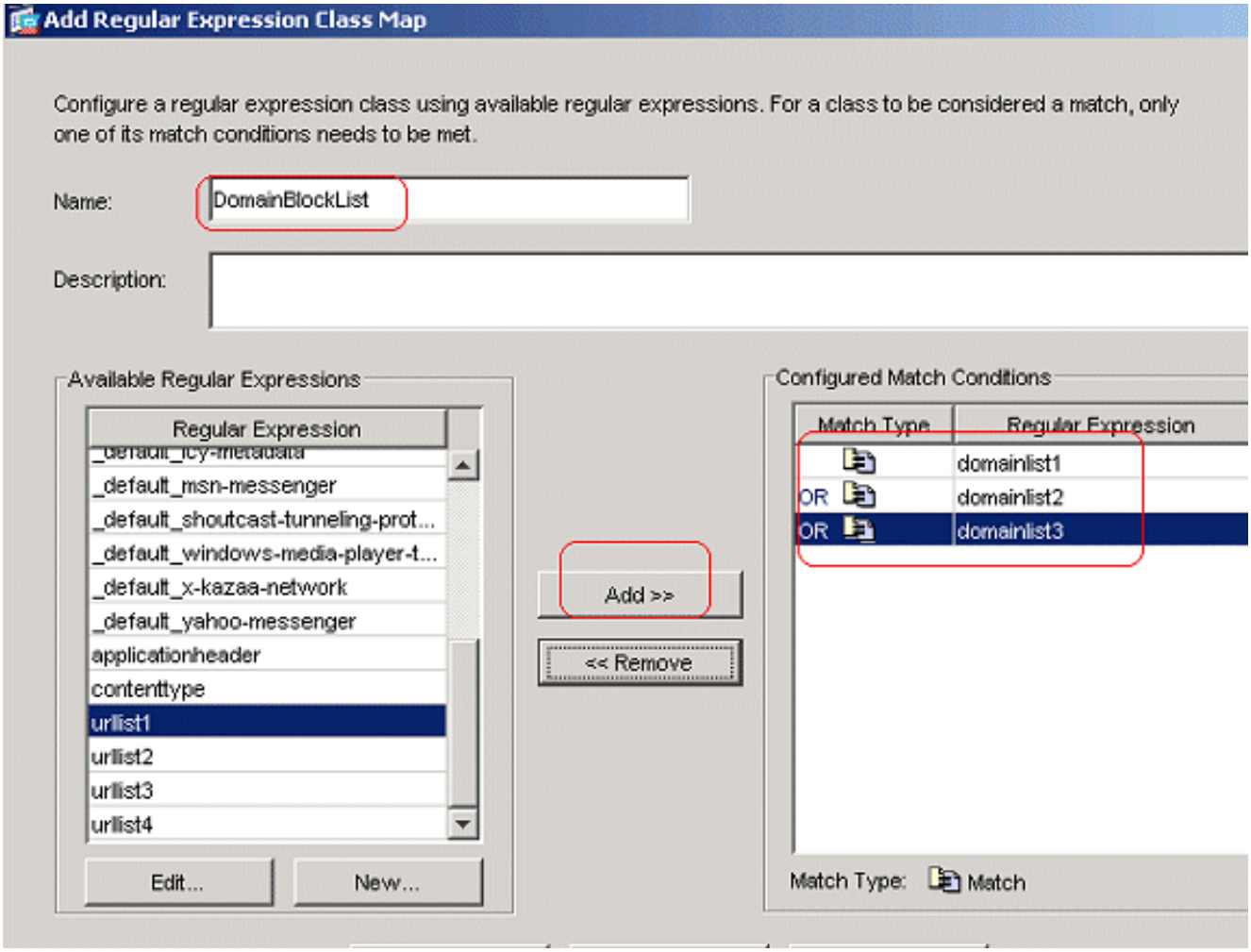
OK. Cri

e um **contenttype da** expressão regular a fim capturar o tipo de conteúdo. Clique em


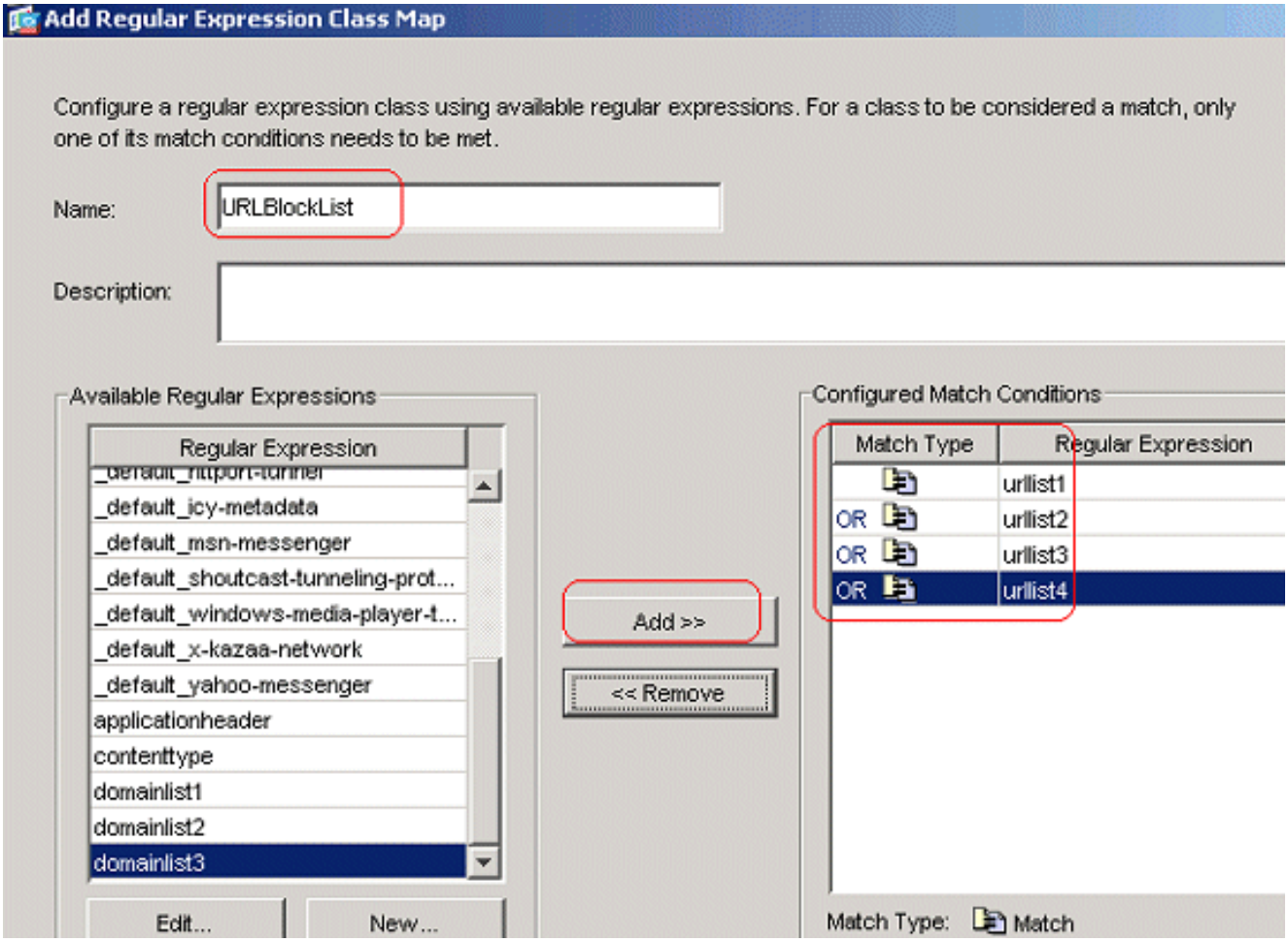
OK. Crie um **applicationheader da** expressão regular a fim capturar o vário encabeçamento do aplicativo. Clique em


OK. **Configuração de CLI equivalente**

2. **Crie classes da expressão regular**Escolha a **configuração > objetos > expressões regulares globais**, e o clique **adiciona** sob a aba das **classes da expressão regular** a fim criar as várias classes.Crie uma classe **DomainBlockList da** expressão regular a fim combinar algumas das expressões regulares: domainlist1, domainlist2, e domainlist3. Clique em **OK**.

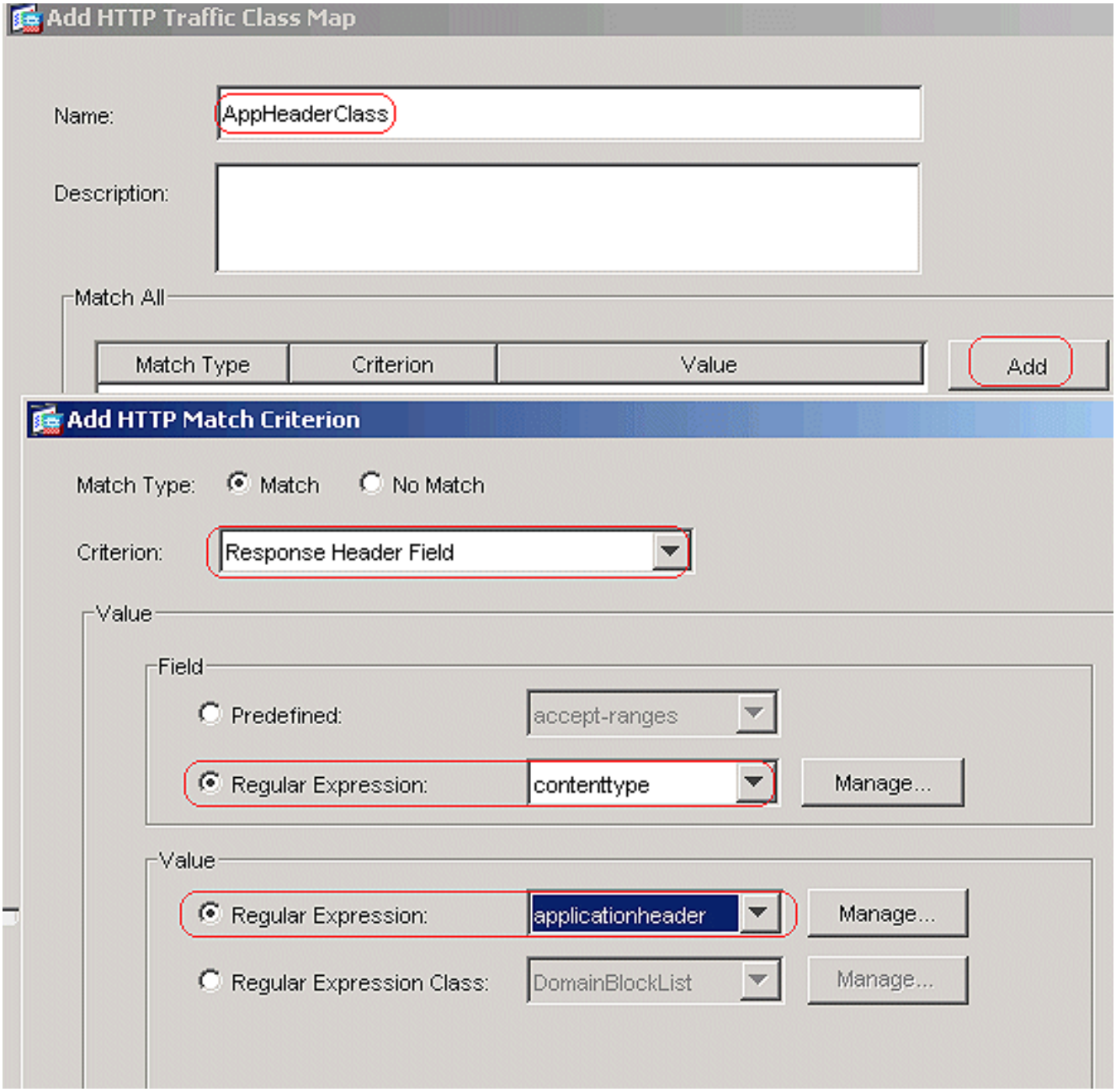


Crie uma classe **URLBlockList da** expressão regular a fim combinar algumas das expressões regulares: urllist1, urllist2, urllist3, e urllist4. Clique em **OK**.

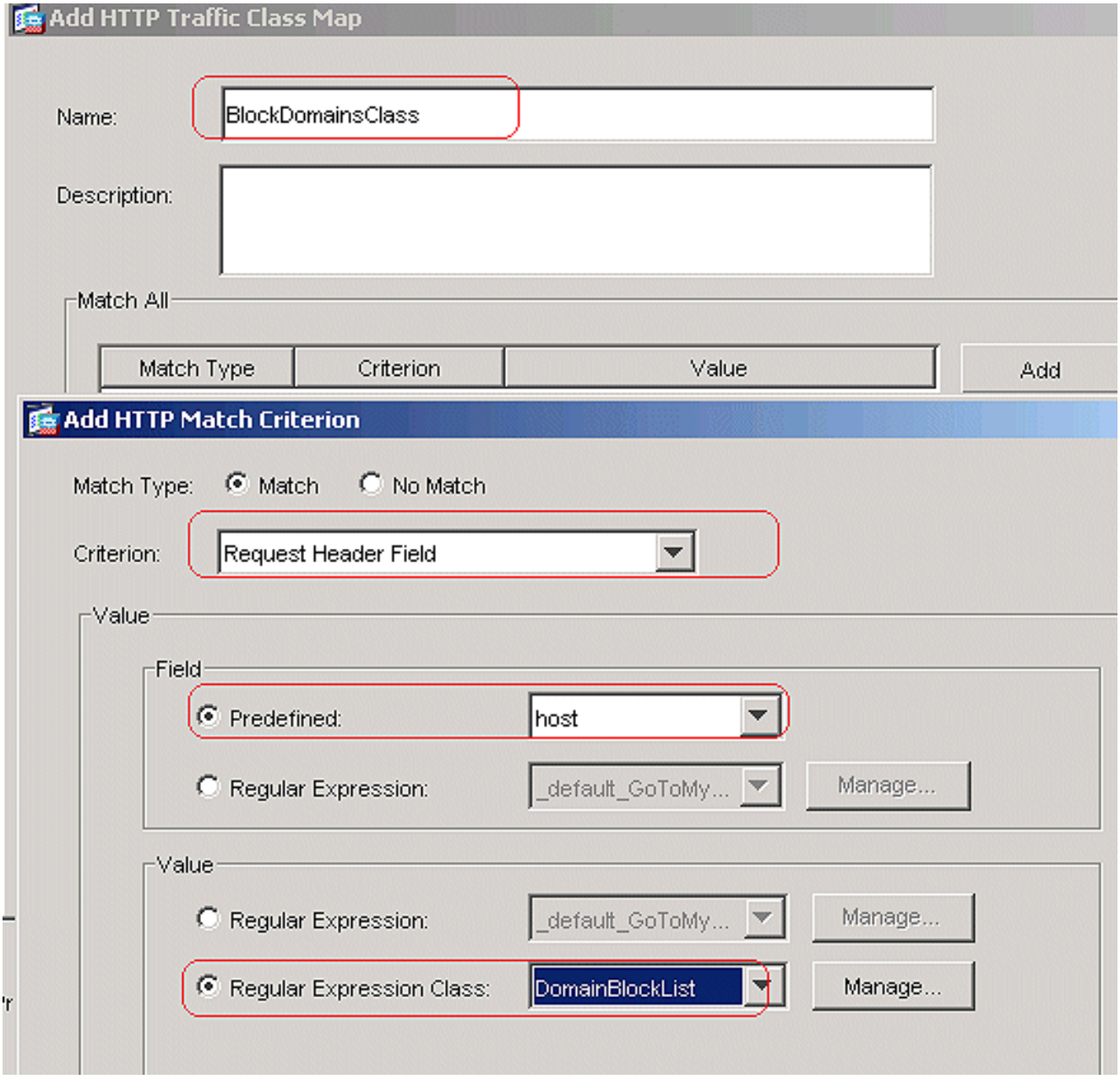


Configuração de CLI equivalente

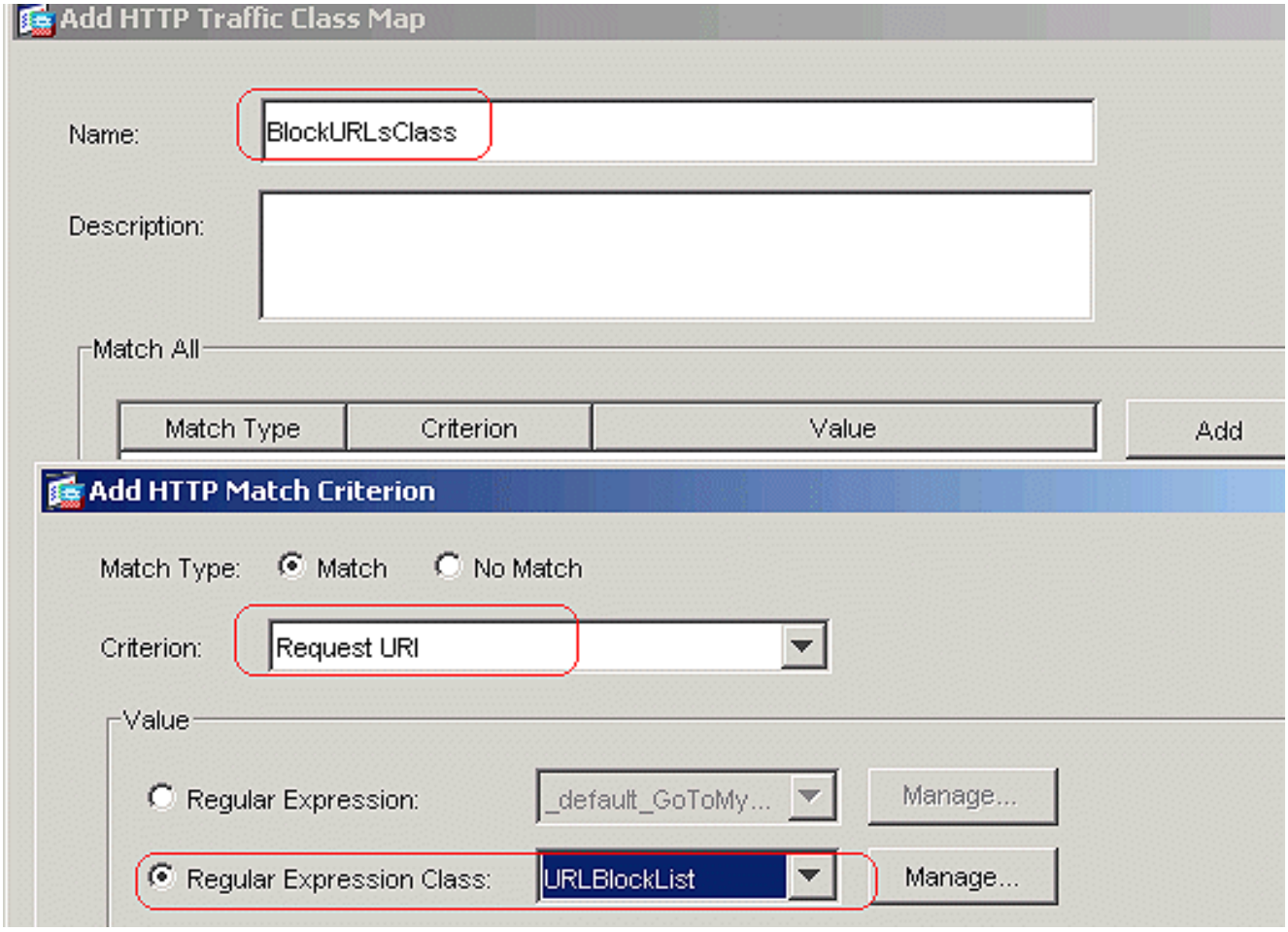
3. **Inspecione o tráfego identificado com mapas da classe**Escolha a **configuração > objetos > classe globais traça > > Add HTTP** a fim criar um mapa da classe para inspecionar o tráfego de HTTP identificado por várias expressões regulares.Crie um mapa **AppHeaderClass da** classe a fim combinar o cabeçalho da resposta com as captações da expressão regular.



Clique em **OK**.Crie um mapa **BlockDomainsClass da** classe a fim combinar o encabeçamento de pedido com as captações da expressão regular.

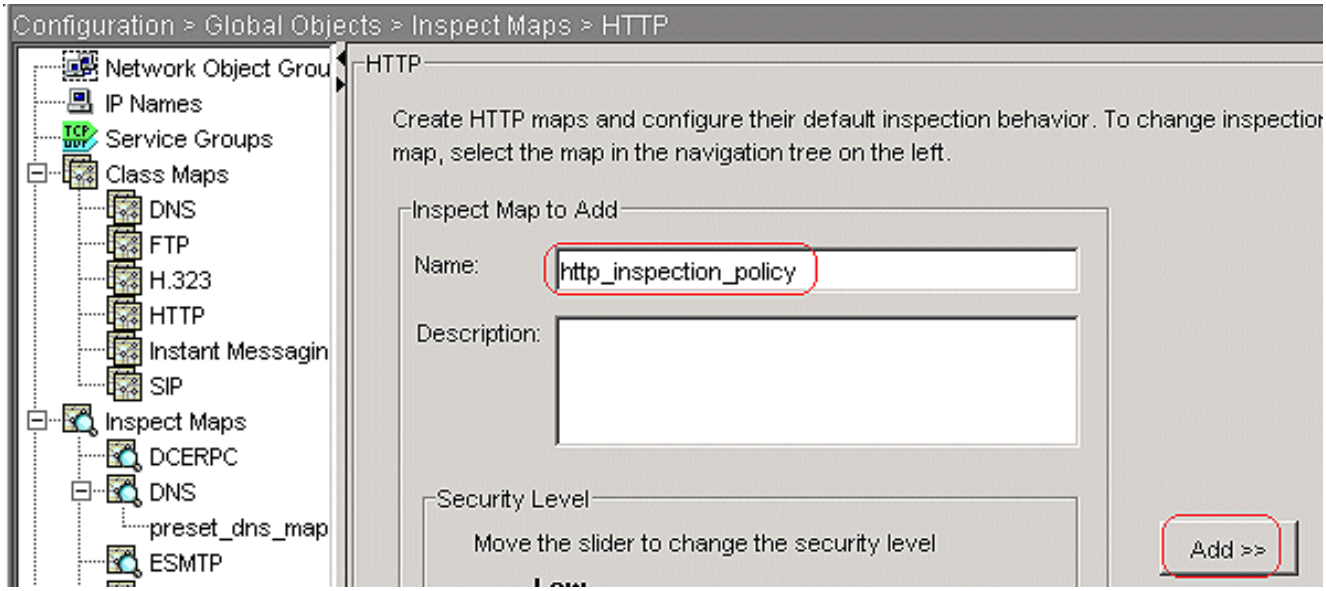


Clique em **OK**.Crie um mapa **BlockURLsClass da** classe a fim combinar o pedido URI com as captações da expressão
regular.

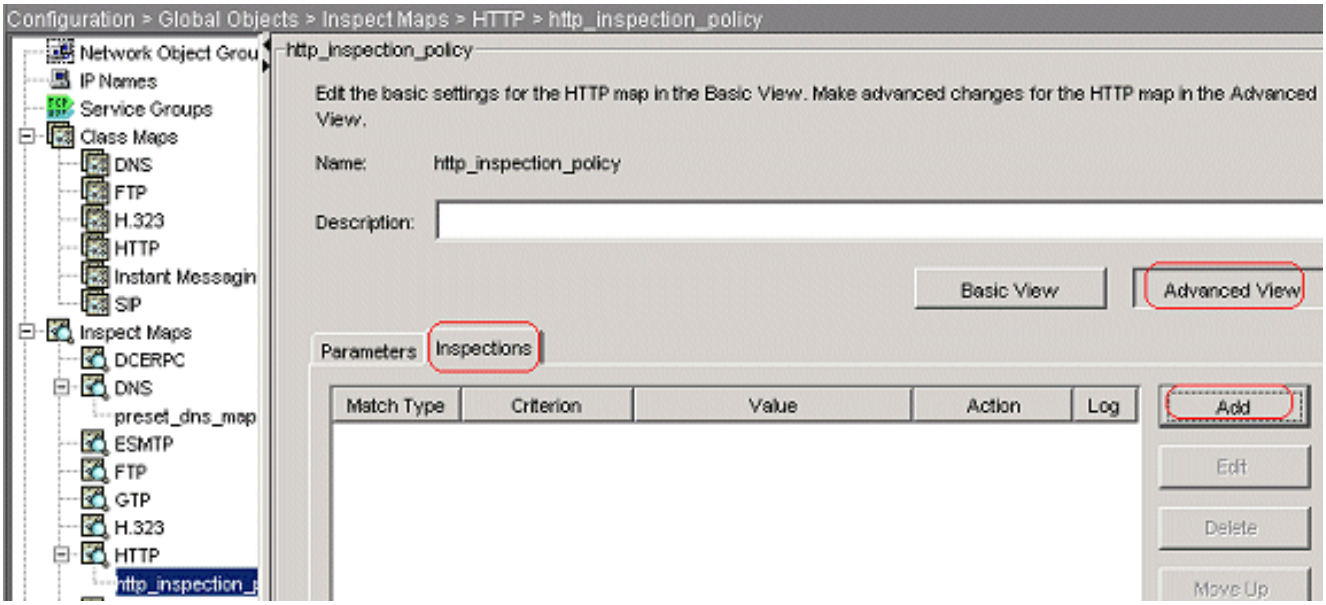


Clique em **OK.Configuração de CLI equivalente**

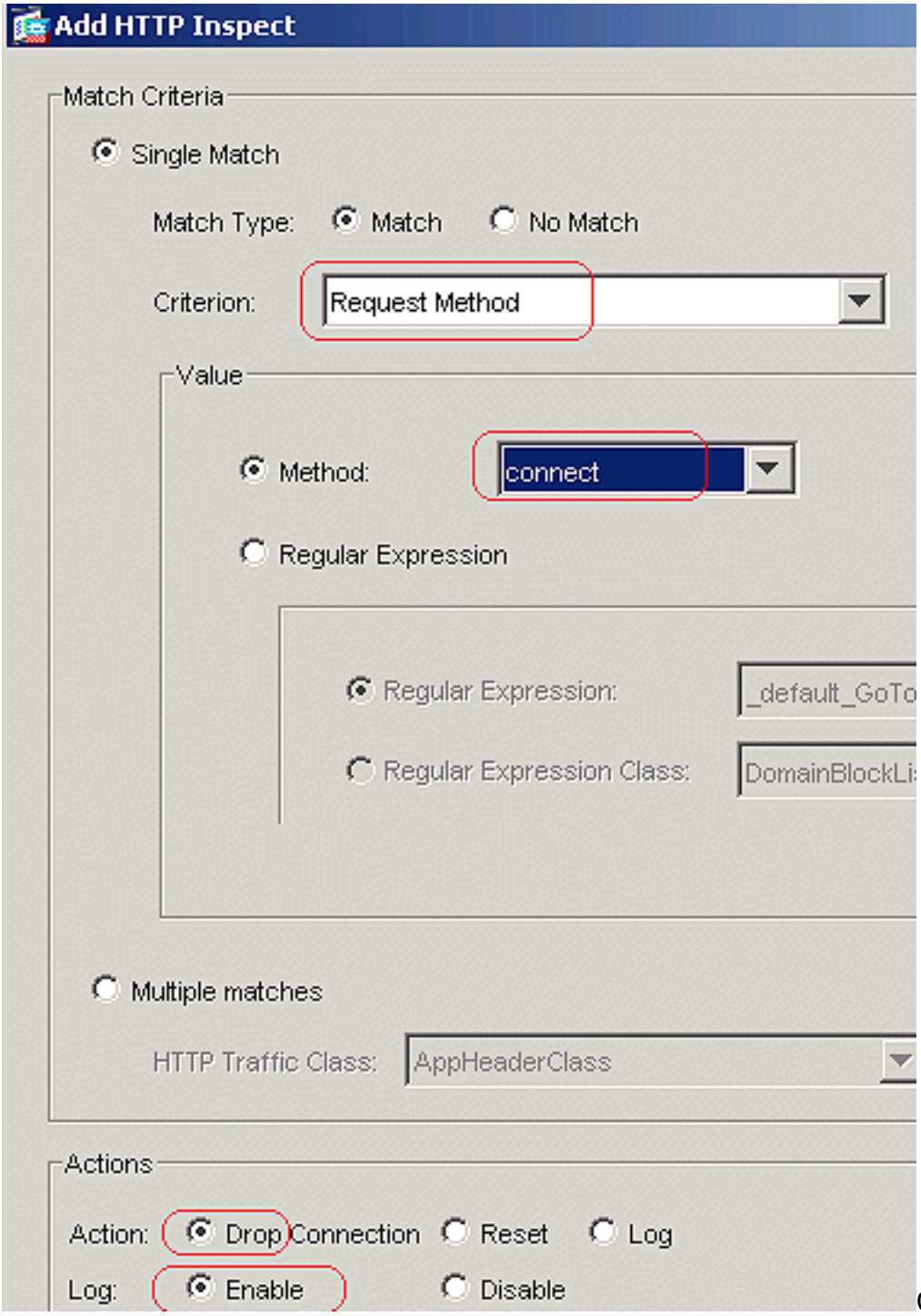
4. **Ajuste as ações para o tráfego combinado na política da inspeção**Escolha a **configuração > objetos globais > inspecionam mapas > HTTP** a fim criar um **http_inspection_policy** para ajustar a ação para o tráfego combinado. O clique **adiciona** e **aplica-se**.



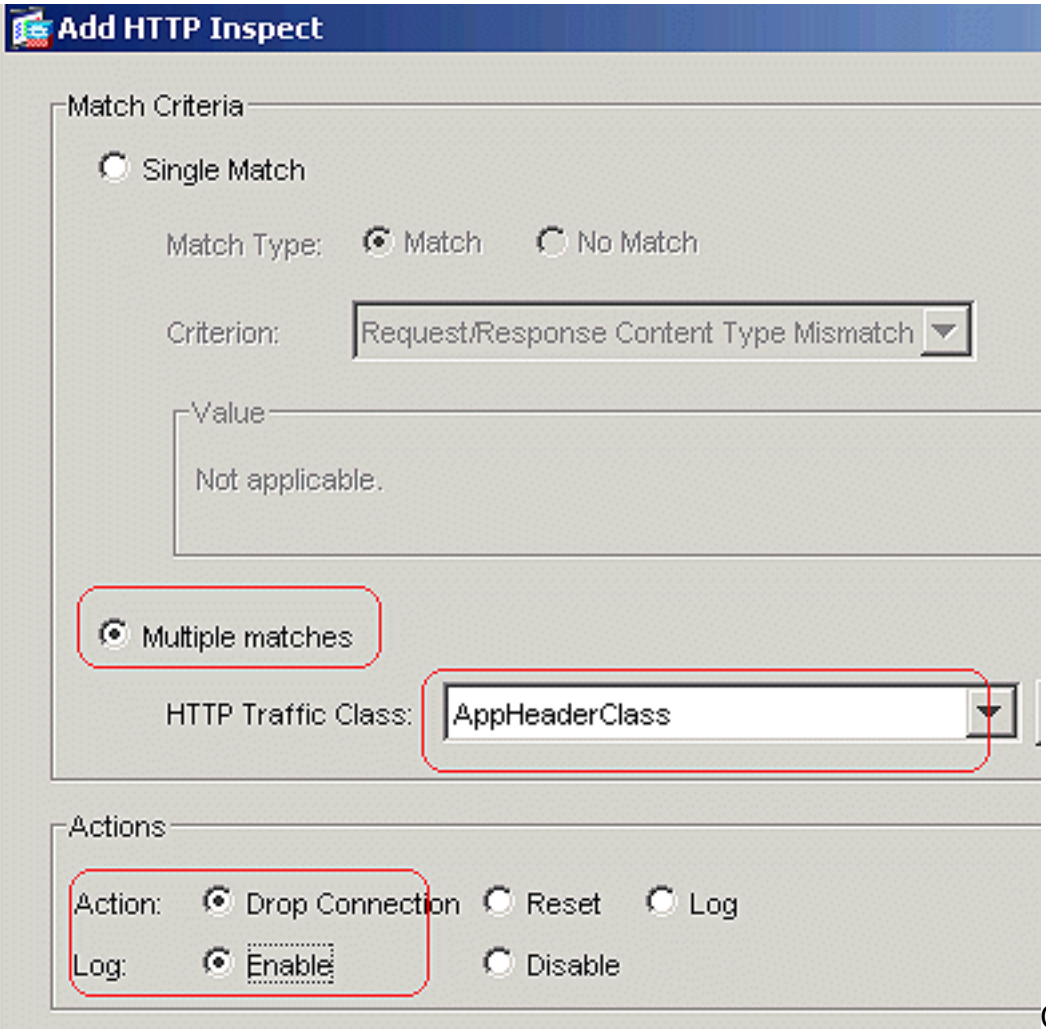
Escolha a **configuração > objetos globais > inspecionam mapas > HTTP > http_inspection_policy** e clicam o **> Add da vista avançada > das inspeções** a fim ajustar as ações para as várias classes criadas até
agora.



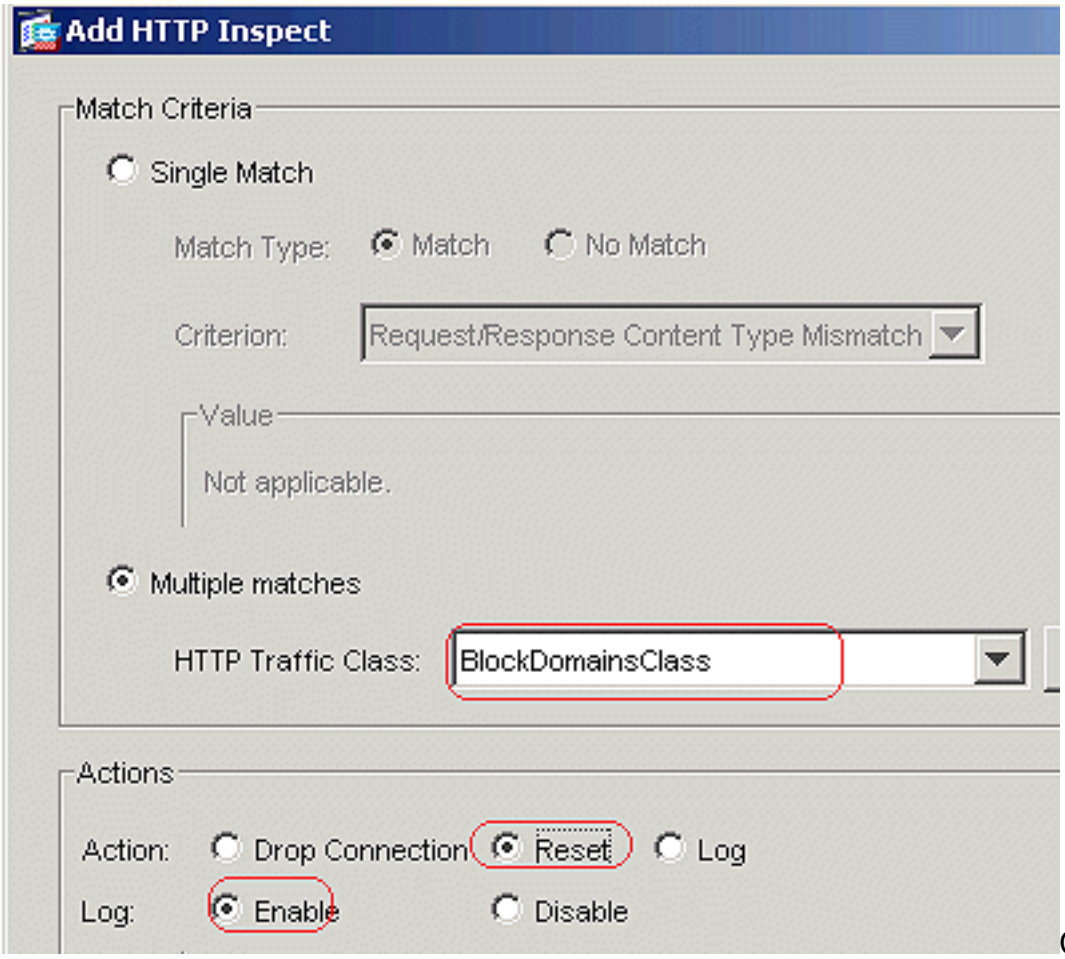
Clique em **OK**.Ajuste a ação como a **conexão da gota**; **Permita o** registro para o critério como o método do pedido e valor como



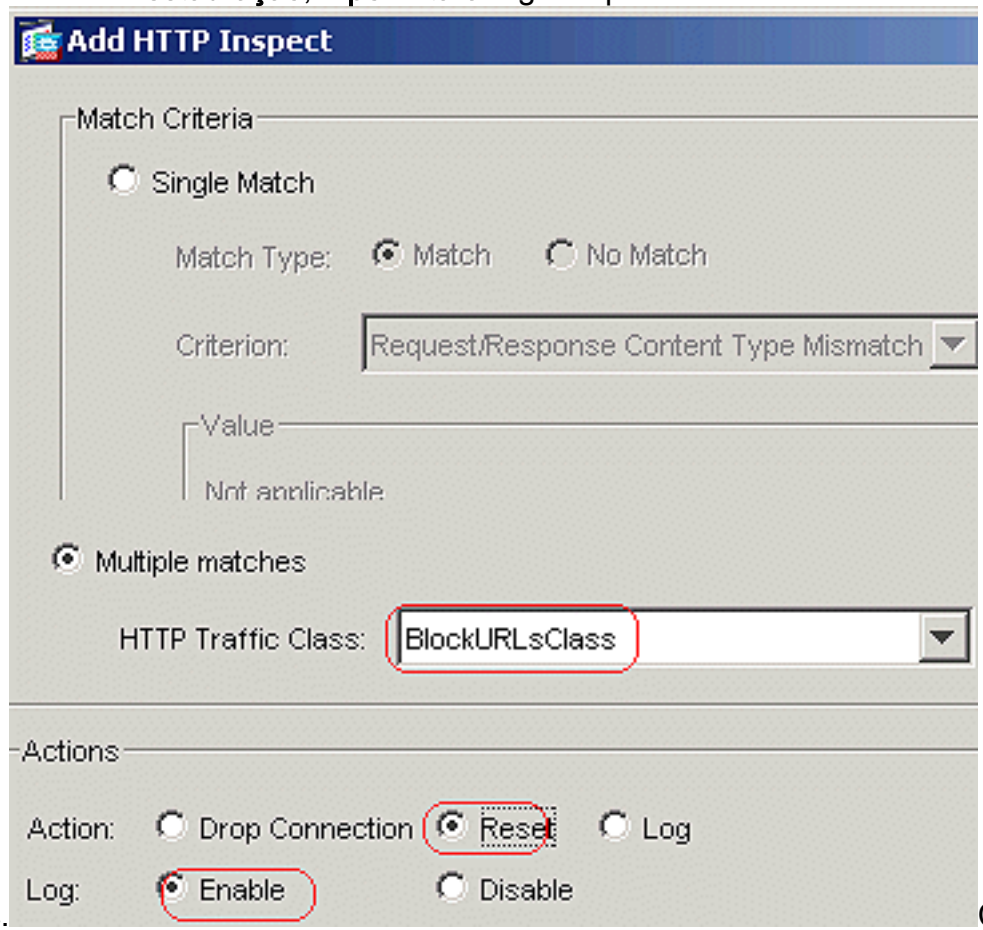
conectam. Clique em **OK**.Ajuste a ação como a **conexão da gota**, e **permita o** registro para a classe



AppHeaderClass. Clique em **OK**.Ajuste a ação como a **restauração**, e **permita o** registro para a classe **BlockDomainsClass**.



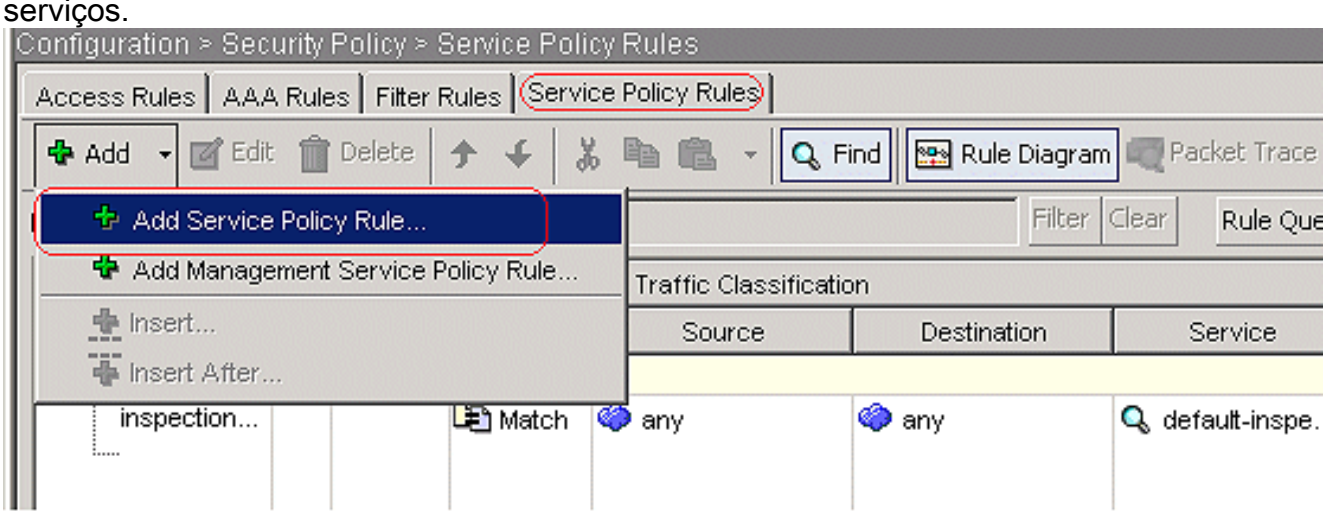
Clique em **OK**.Ajuste a ação como a **restauração**, e **permita o** registro para a classe



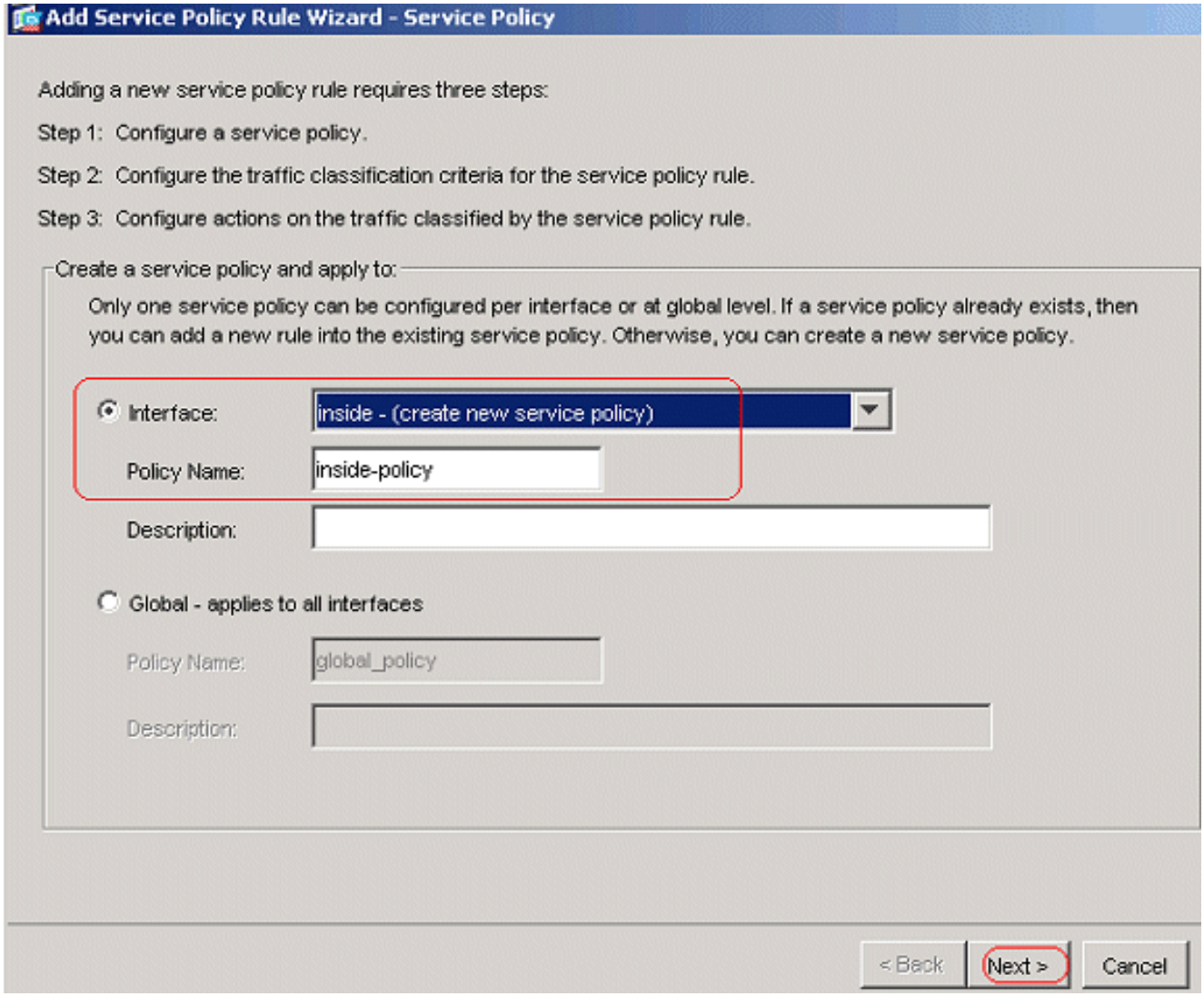
BlockURLsClass. Clique em **OK**.Clique em Apply.**Configuração de CLI equivalente**

5. **Aplique a política HTTP da inspeção à relação**Escolha a **regra da política de serviços do > Add do > Add das regras da política > da política de serviços do > segurança da**

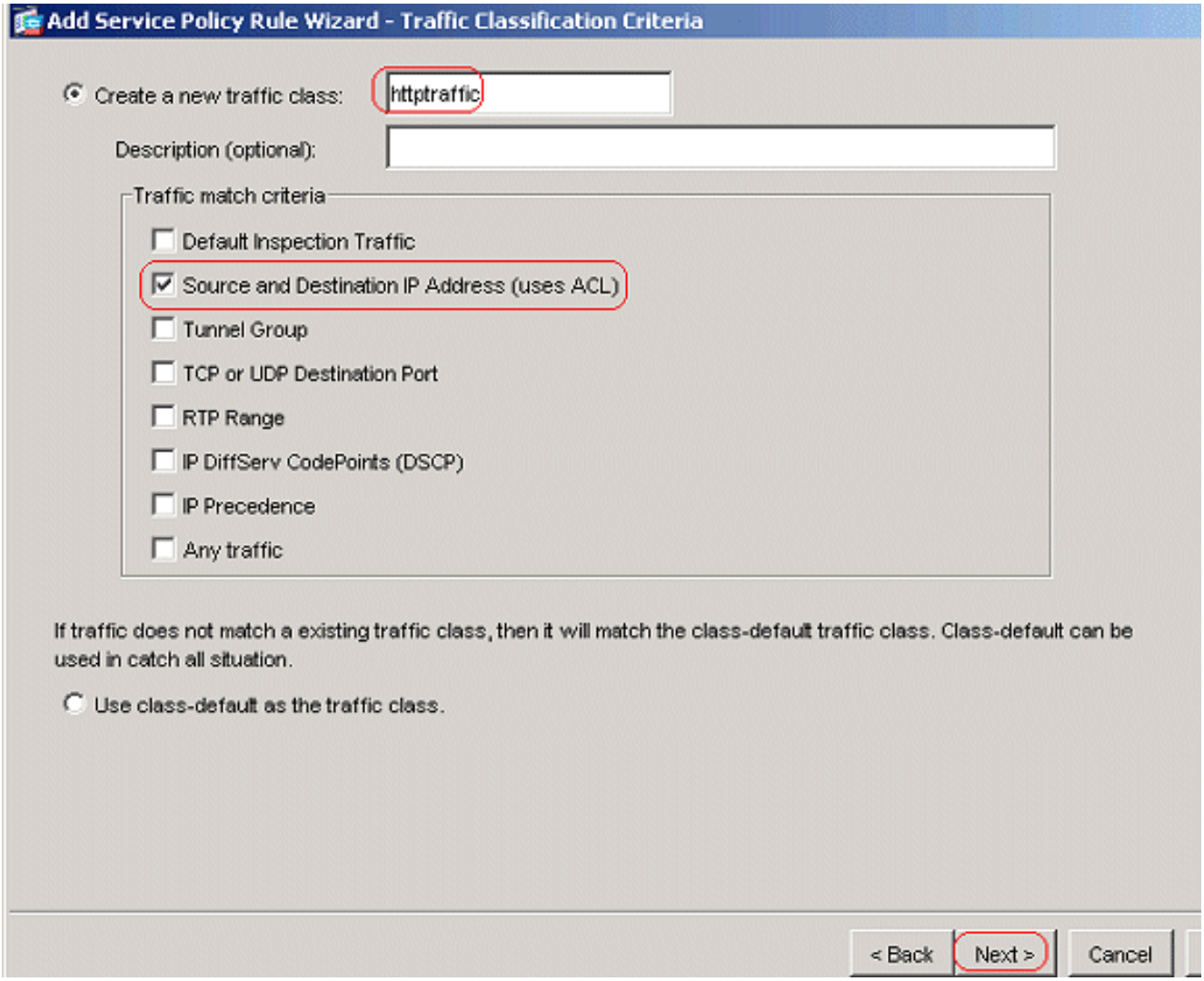
configuração sob a aba das regras da política de serviços.



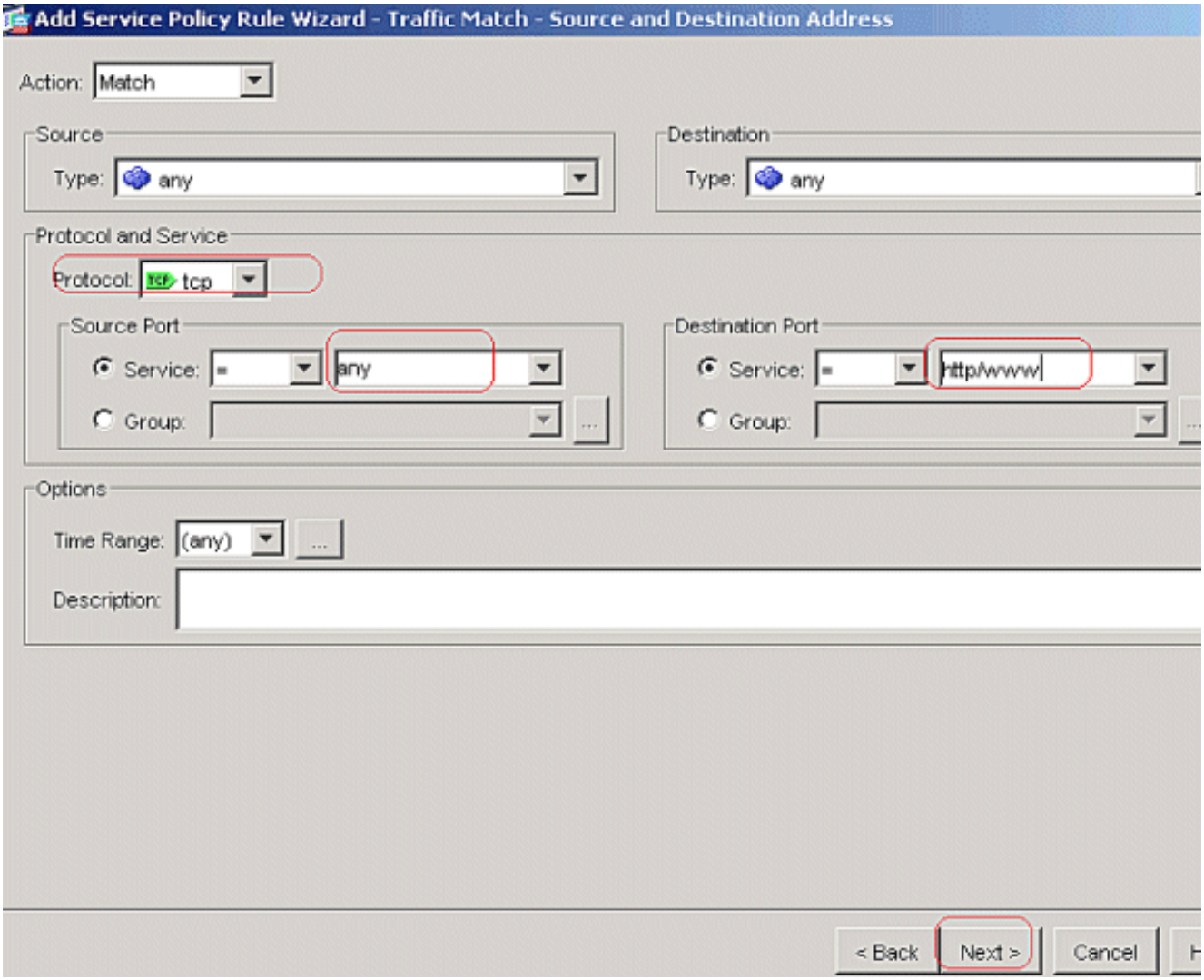
Tráfego de HTTP Escolha o botão de rádio da **relação** com a **interface interna do** menu suspenso e do nome da política como a dentro-**política**. Clique em Next.



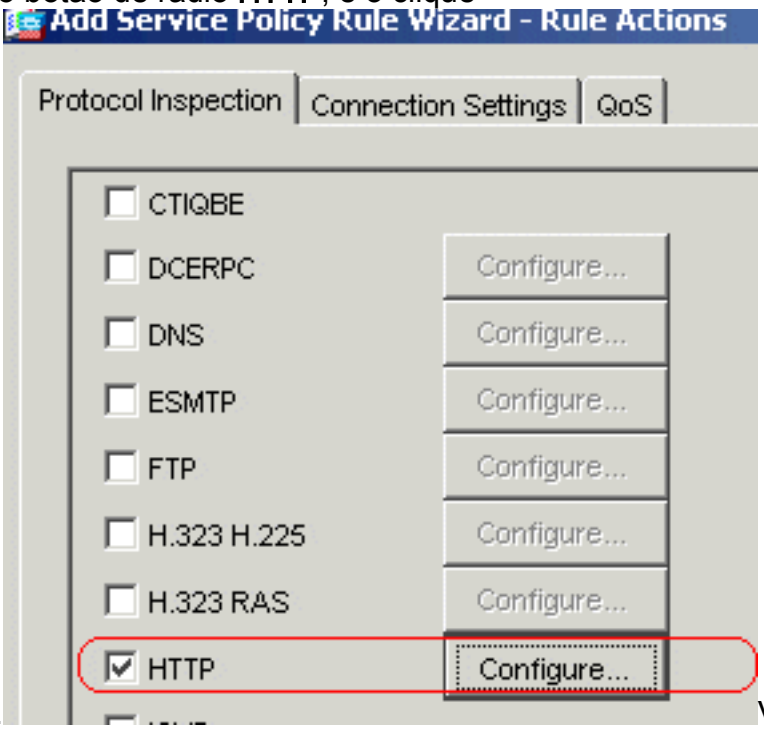
Crie um mapa da classe **httptraffic**, e verifique o **endereço IP de origem e de destino (usos ACL)**. Clique em Next.



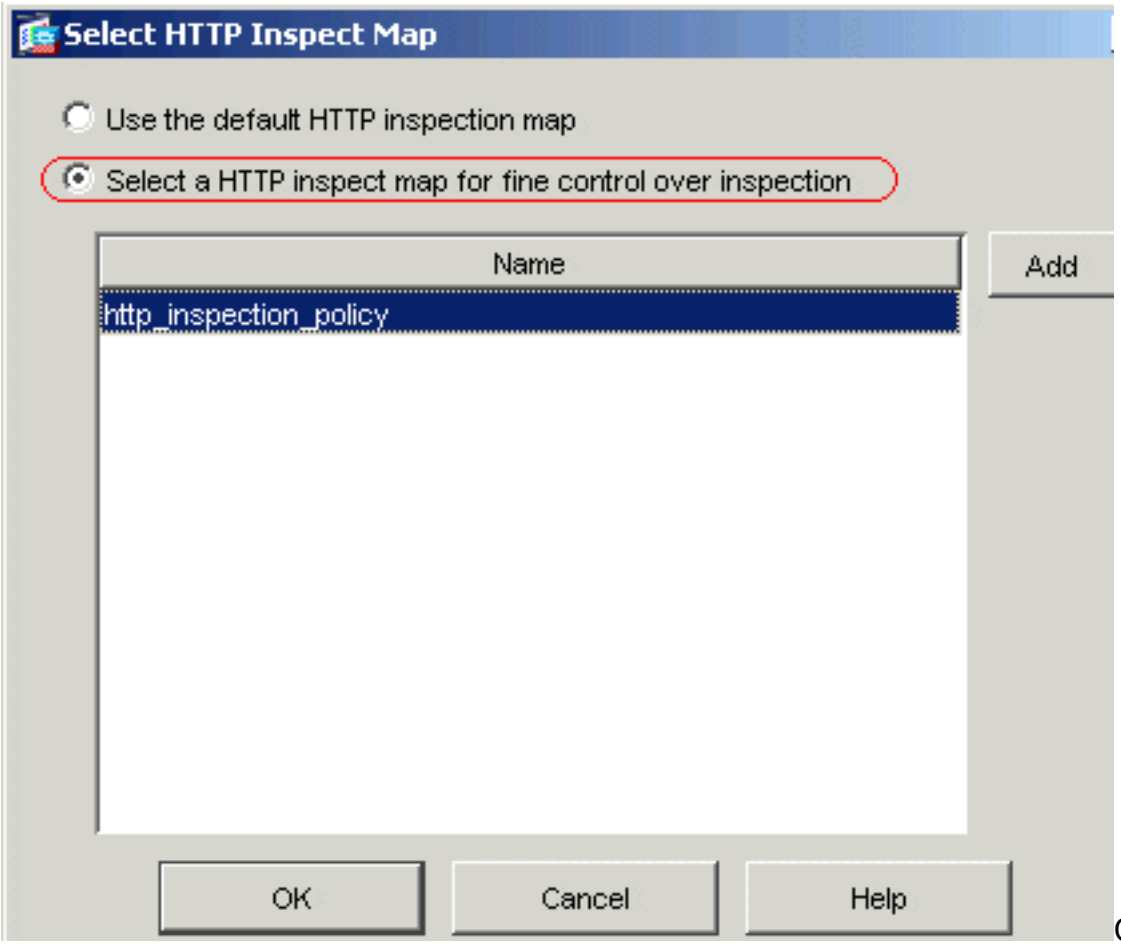
Escolha a fonte e o destino tão com a porta TCP quanto o **HTTP**. Clique em Next.



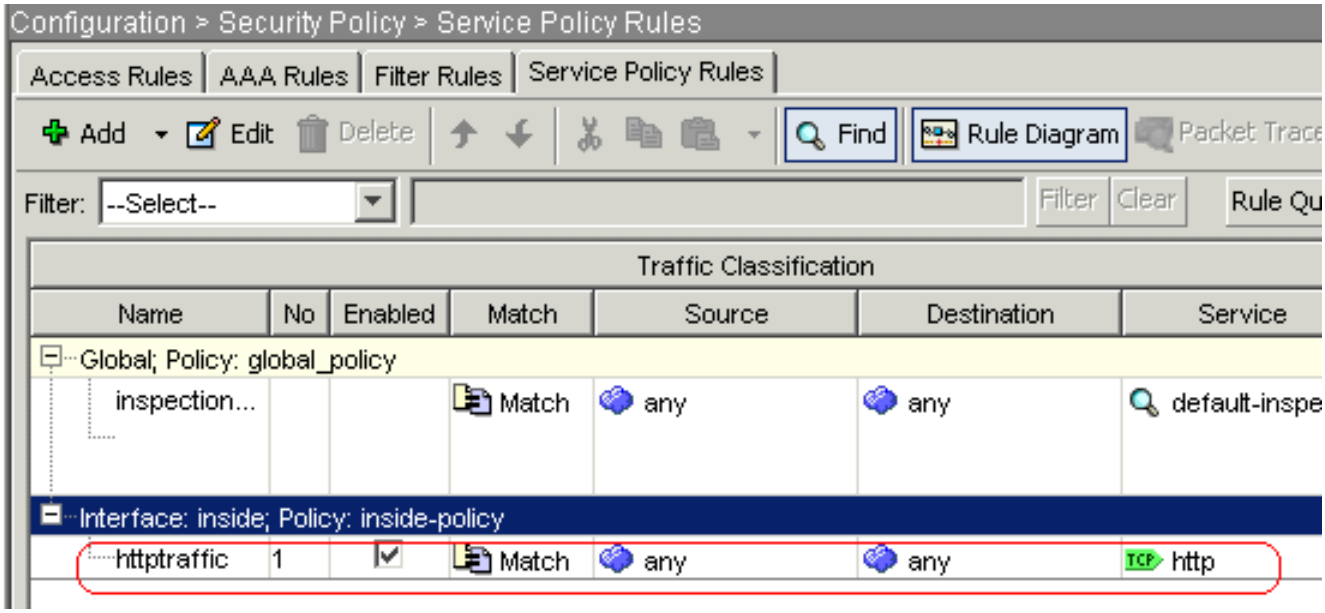
Verifique o botão de rádio **HTTP**, e o clique **configura**.



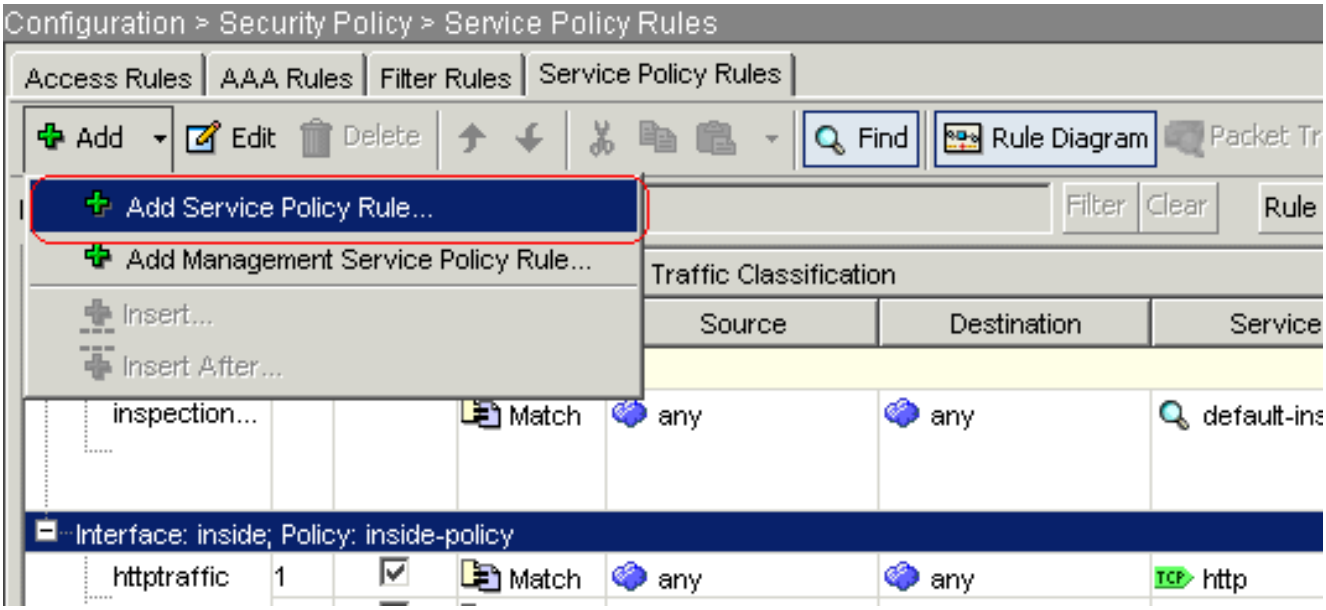
Verifique o botão de rádio **selecionam um HTTP inspecionam o mapa para o controle sobre a inspeção**. Clique em



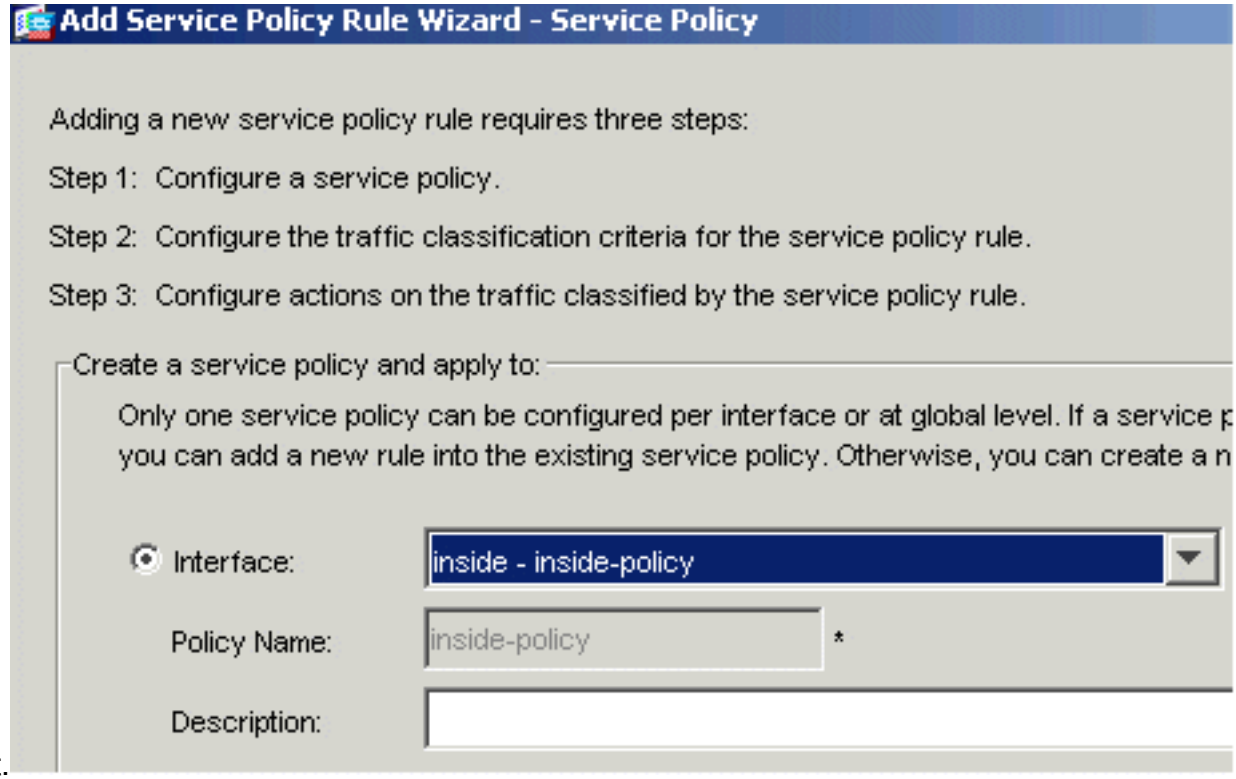
OK. Clique em Finish.



Tráfego da porta 8080 Além disso, o clique **adiciona a regra da política de serviços do > Add**.

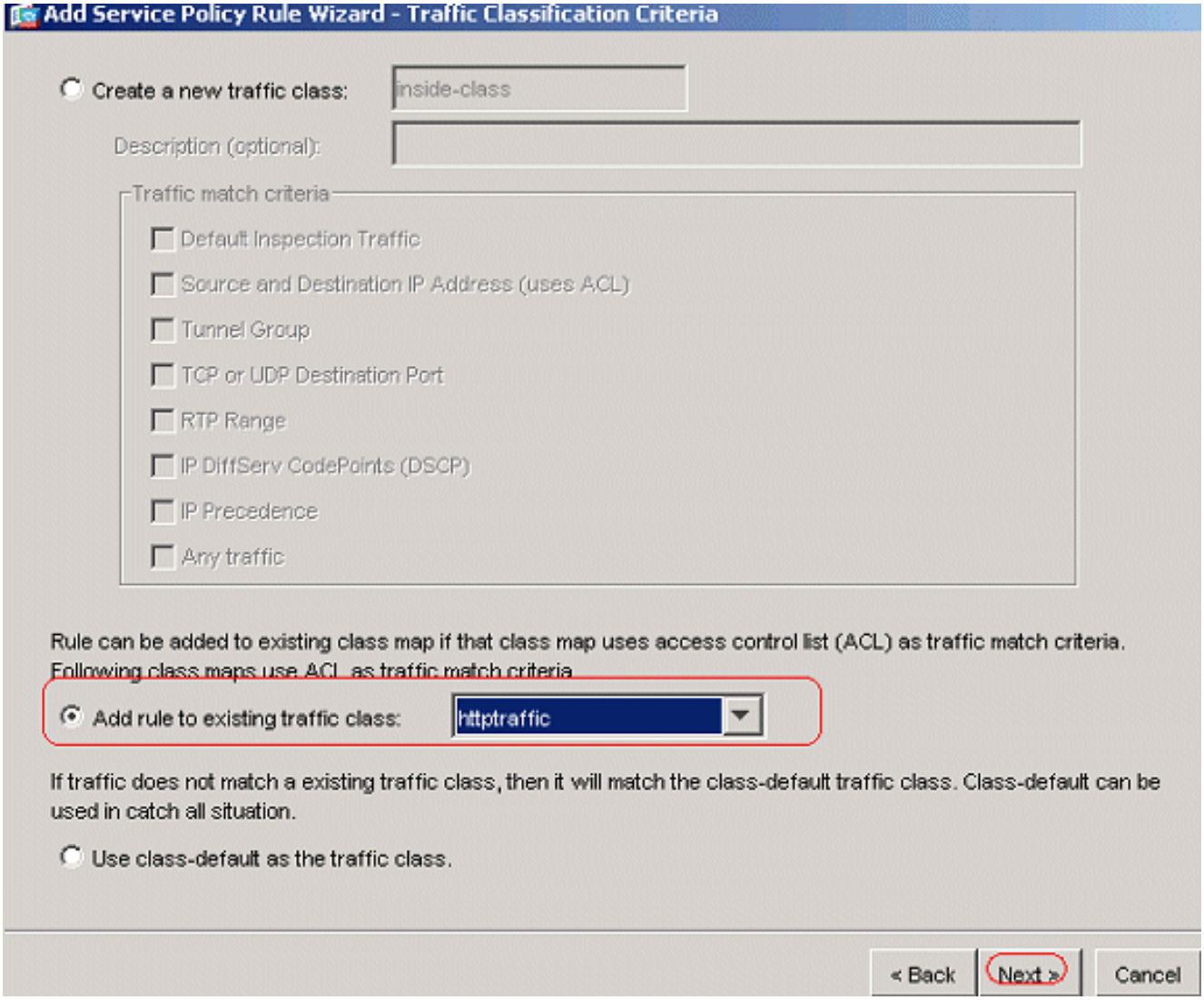


Clique em

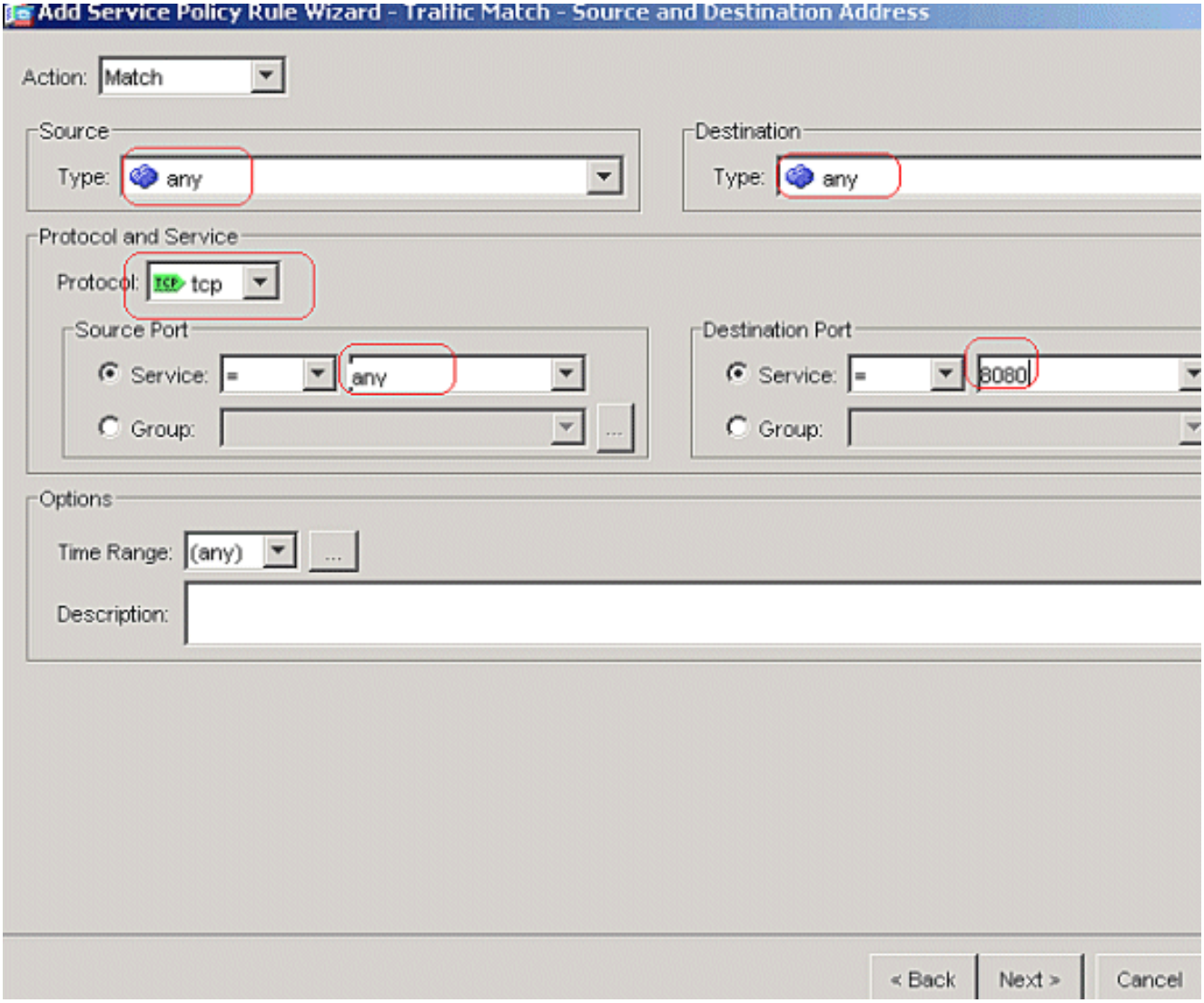


Next.

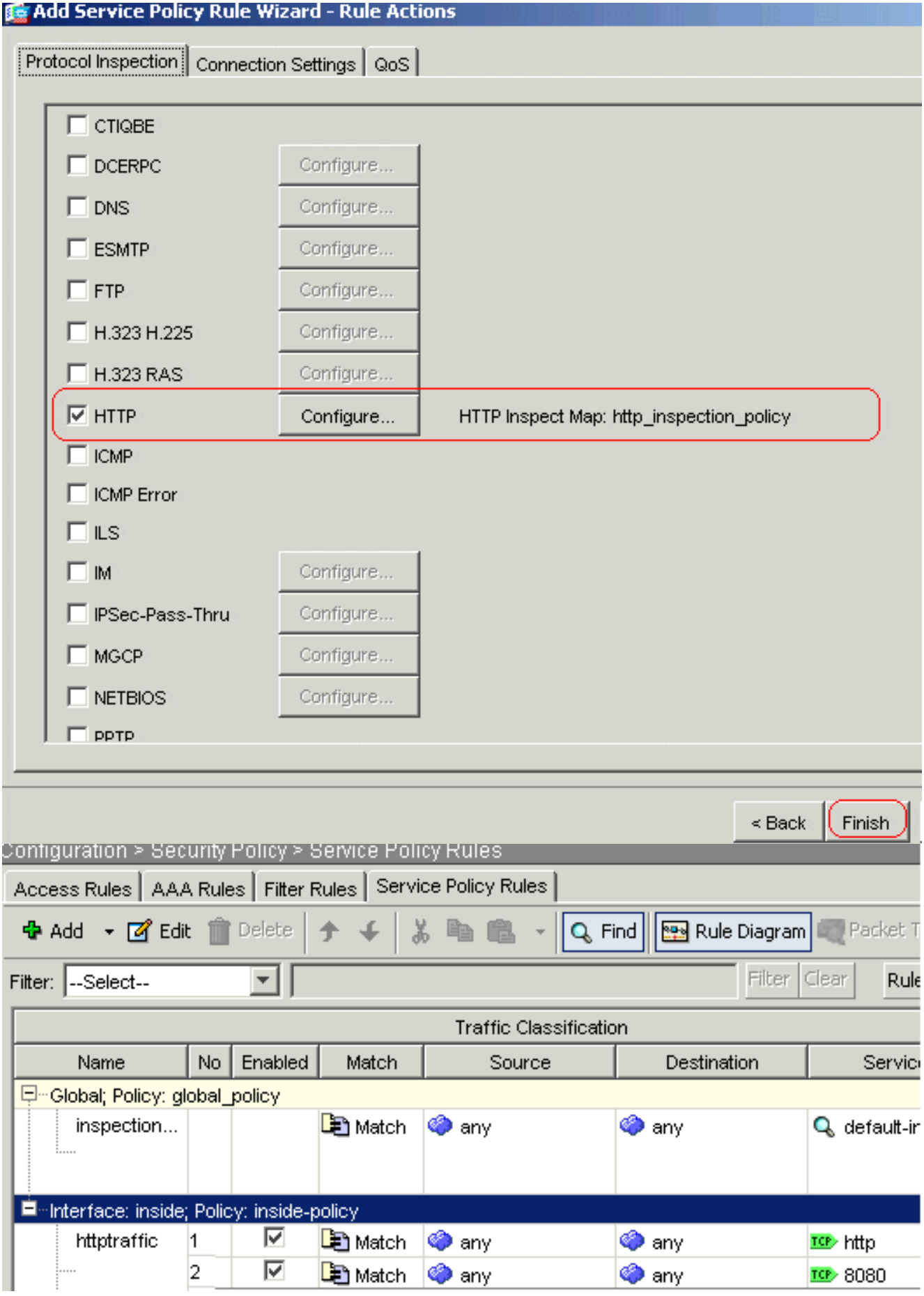
Escolha a **regra adicionar a** botão de rádio **existente da classe de tráfego**, e escolha **httptraffic do** menu suspenso. Clique em
Next.



Escolha a fonte e o destino tão com a porta TCP quanto **8080**. Clique em Next.



Clique em
Finish.



Clique em Apply.**Configuração de CLI equivalente**

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre o regex da executar-configuração** — Mostra as expressões regulares que foram configuradas`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#`
- **mostre o mapa de classe da executar-configuração** — Mostra os mapas da classe que foram configurados`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#`
- **o tipo do mapa de política da executar-configuração da mostra inspeciona o HTTP** — Mostra os mapas da política que inspeciona o tráfego HTTP que foi configurado`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#`
- **mostre o mapa de política da executar-configuração** — Indica todas as configurações de mapa de política assim como configuração de mapa de política do padrão`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#`
- **mostre a serviço-política da executar-configuração** — Indica todas as configurações atualmente sendo executado da política de serviços`ciscoasa#show running-config service-policy service-policy global_policy global service-policy inside-policy interface inside`
- **mostre a lista de acesso da executar-configuração** — Indica a configuração de lista de acesso que é executado na ferramenta de segurança`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#`

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **debugar o HTTP** — Mostra as mensagens debugar para o tráfego de HTTP.

Informações Relacionadas

- Página de suporte adaptável da ferramenta de segurança de Cisco
- Página de suporte do Cisco Adaptive Security Device Manager (ASDM)
- Página do suporte de PIX do Cisco 500 Series
- Suporte Técnico e Documentação - Cisco Systems