

ASA/PIX 8.x: Determinados Web site do bloco (URL) que usam expressões regulares com exemplo da configuração MPF

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Convenções](#)

[Informações de Apoio](#)

[Vista geral modular da estrutura de política](#)

[Expressão regular](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração do ASA via CLI](#)

[Configuração 8.x ASA com ASDM 6.x](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve como configurar os Cisco Security Appliances ASA/PIX 8.x 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 o arquivo seguro que obstrui, um dispositivo dedicado tal como a série S de Ironport ou um módulo tal como o módulo CSC para o ASA devem ser usados.

Nota: A filtração HTTPS não é apoiada no ASA. O ASA não pode fazer a inspeção de pacote de informação profunda ou inspeção 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 (ASA) essa executa a versão de software 8.0(x) e mais atrasada
- Versão 6.x do Cisco Adaptive Security Device Manager (ASDM) para ASA 8.x

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 8.0(x) e mais atrasado.

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 literalmente como uma corda exata, ou pelo uso dos 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** a fim escapar todos os caracteres especiais no CLI, tal como o ponto de interrogação (?) ou uma aba. Por exemplo, datilografe o **[Ctrl+V] d? g** a fim incorporar **d? g** na configuração.

Para a criação de 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 o uso da estrutura de política modular que usa um mapa de política da inspeção. Refira o [tipo comando inspect do mapa de política](#) para mais informação. 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 usando 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. Refira o [tipo comando do mapa de classe do regex](#) para mais informação.

Esta [tabela](#) alista os metacharacters que têm significados especiais.

Caractere	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 caracteres, tais como o doggonnit.
(exp)	Subexpression	Um subexpression segrega caracteres dos caracteres circunvizinhos, de modo que você possa usar outros metacharacters no subexpression. Por exemplo, d(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 caracteres significados para a repetição. Por exemplo, ab(xy){3}z combina o abxyxyxyz.
	Alterna	Combina uma ou outra expressão que

	ção	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 carácter	Combina todo o carácter nos suportes. Por exemplo, o [abc] combina a, b, ou C.
[^abc]	Classe de carácter negada	Combina um único carácter que não seja contido dentro dos suportes. Por exemplo, o [^abc] combina todo o carácter a não ser a, b, ou o [^A-Z] C. combina qualquer único carácter que não for uma letra maiúscula.
[a-c]	Classe da escala do carácter	Combina todo o carácter na escala. o [a-z] combina toda a letra minúscula. Você pode misturar caracteres 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 carácter do traço (-) é literal somente se é o último ou o primeiro carácter 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 carácter literal. Por exemplo, \ [combina o suporte quadrado esquerdo.

carvão animal	Caractere	Quando o caráter não é um 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 que use um hexadecimal que seja exatamente dois dígitos
\NNN	Número octal escapado	Combina um caractere ASCII porque octal que seja exatamente três dígitos. Por exemplo, o caráter 040 representa um espaço.

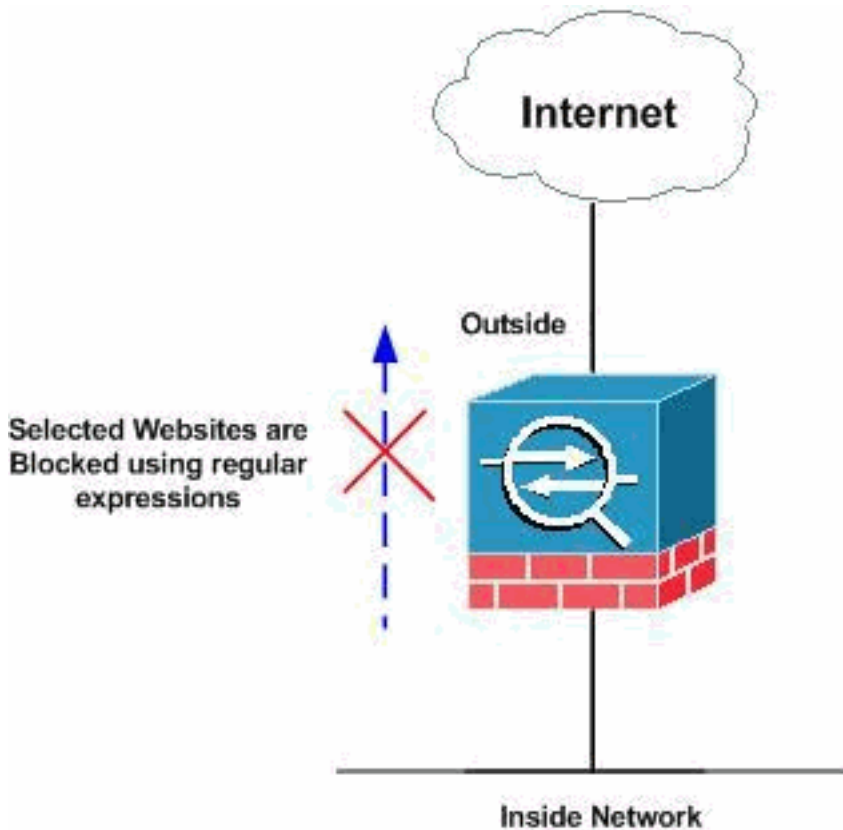
[Configurar](#)

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 8.x ASA com ASDM 6.x](#)

Configuração do ASA via CLI

Configuração do ASA via CLI

```

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

```

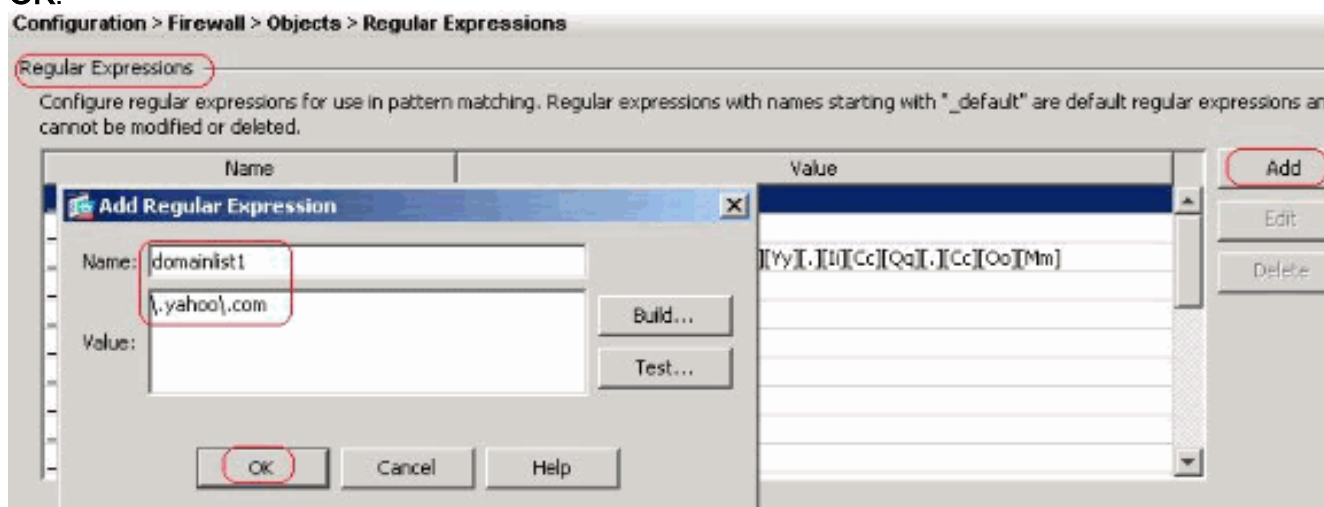
log !--- Define the actions such as drop, reset or log
!--- in the inspection policy map. policy-map
global policy class inspection default inspect dns
preset dns map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
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#

```

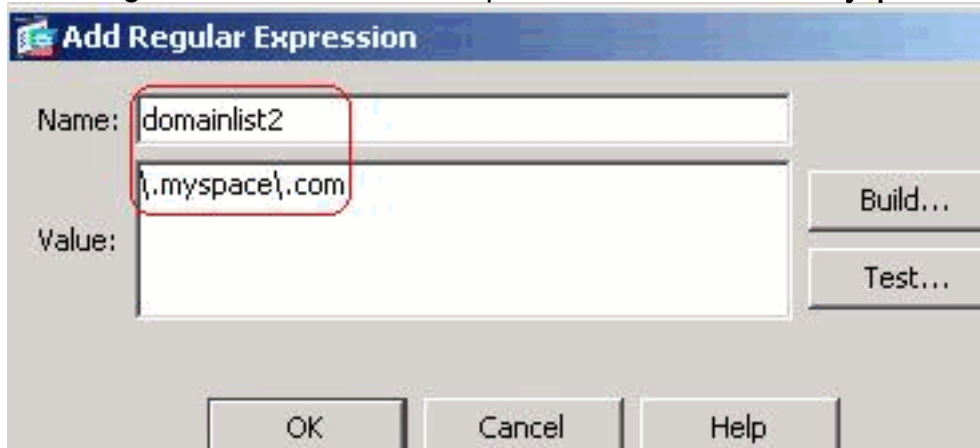
Configuração 8.x ASA com ASDM 6.x

Termine estas etapas a fim configurar as expressões regulares e aplicá-las no MPF para obstruir como mostrado os Web site específicos.

1. Crie expressões regulares Escolha a configuração > o Firewall> objeto > expressões regulares e o clique adiciona sob a expressão regular da aba a fim criar como mostrado 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**.



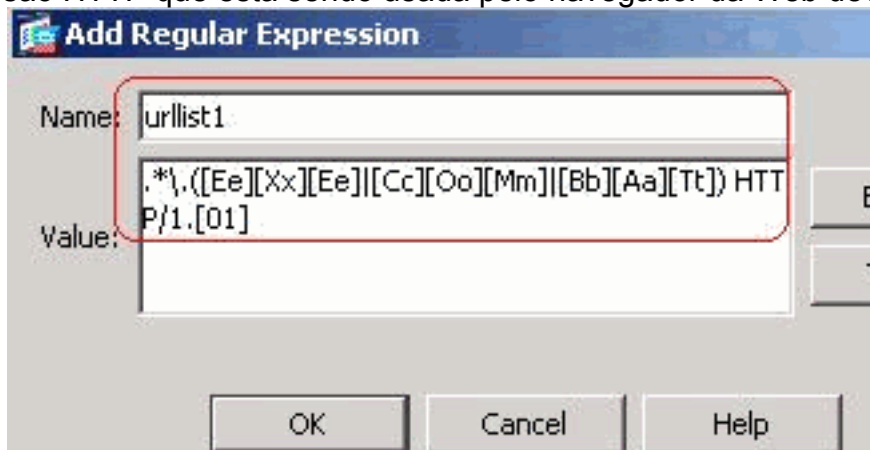
Clique em **OK**.

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



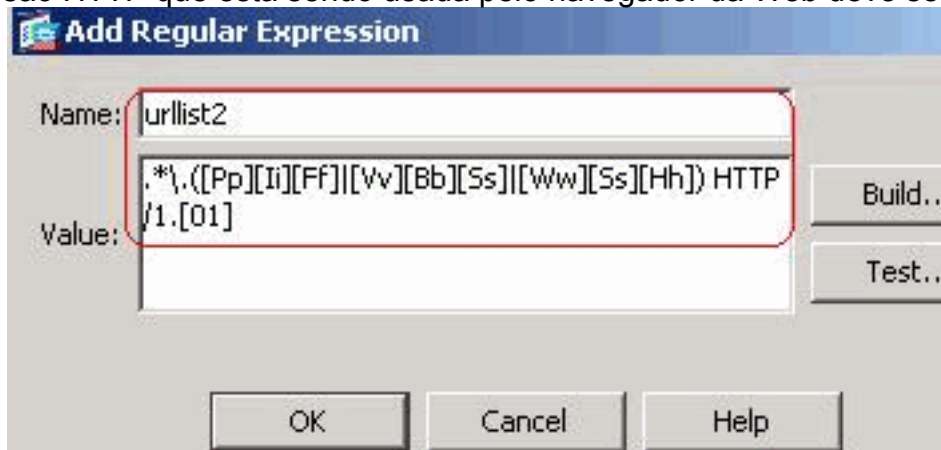
OK.

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 que está sendo usada pelo navegador da Web deve ser 1.0 ou



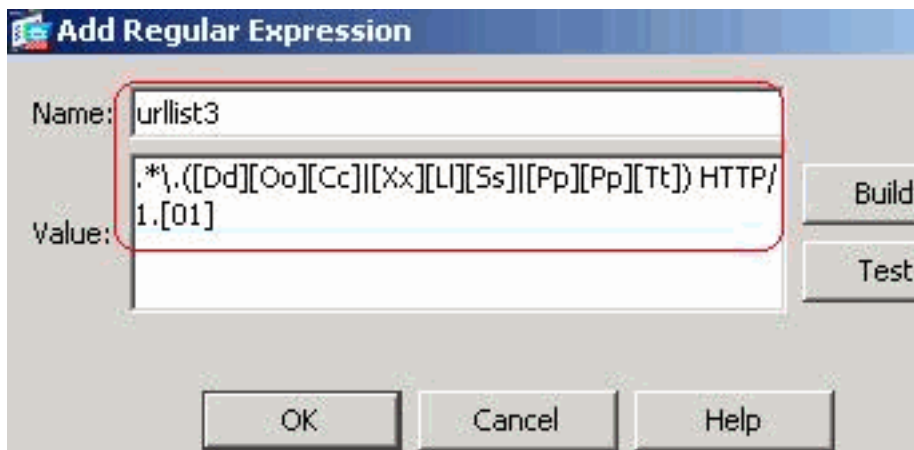
1.1. Clique em OK.

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 sendo usada pelo navegador da Web deve ser 1.0 ou

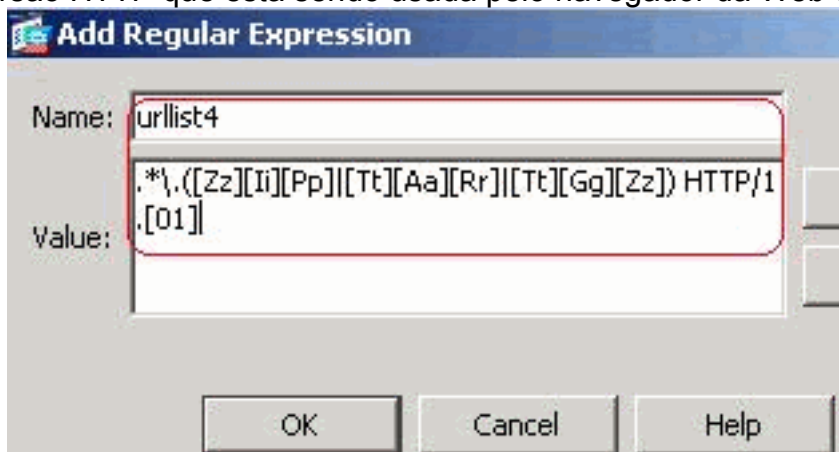


1.1. Clique em OK.

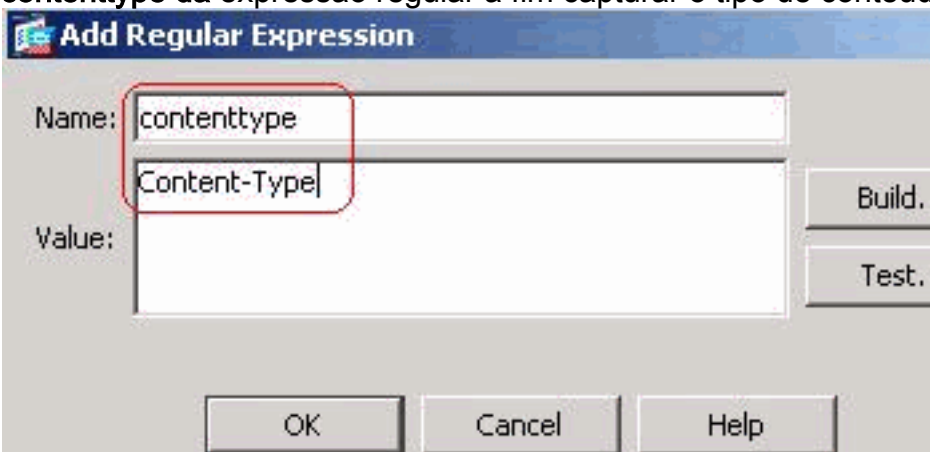
Crie uma expressão regular **urllist3** a fim capturar as extensões de arquivo tais como o **doc**, os **xls** e o **ppt** contanto que a versão HTTP que está sendo usada pelo navegador da Web deve ser 1.0 ou 1.1. Clique em



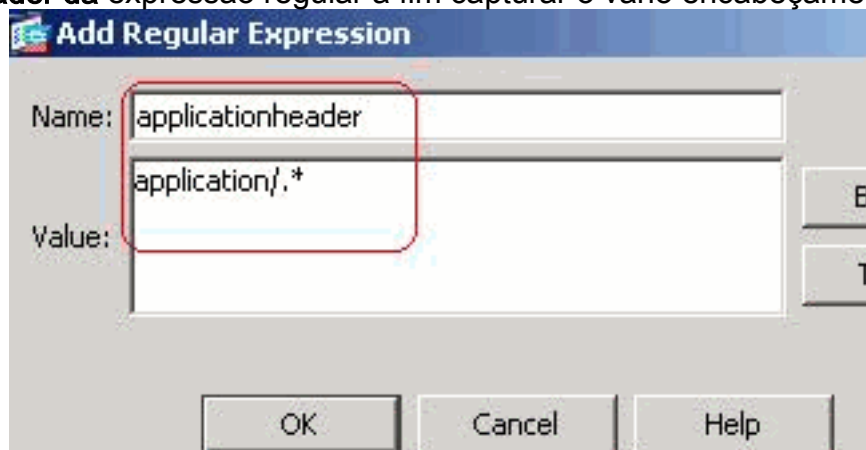
OK. Crie uma expressão regular **urllist4** a fim capturar as extensões de arquivo tais como o **fecho de correr**, o **alcatrão** e o **tgz** contanto que a versão HTTP que está sendo usada pelo navegador da Web deve ser



1.0 ou 1.1. Clique em **OK**. Crie um **contenttype** da expressão regular a fim capturar o tipo de conteúdo. Clique em



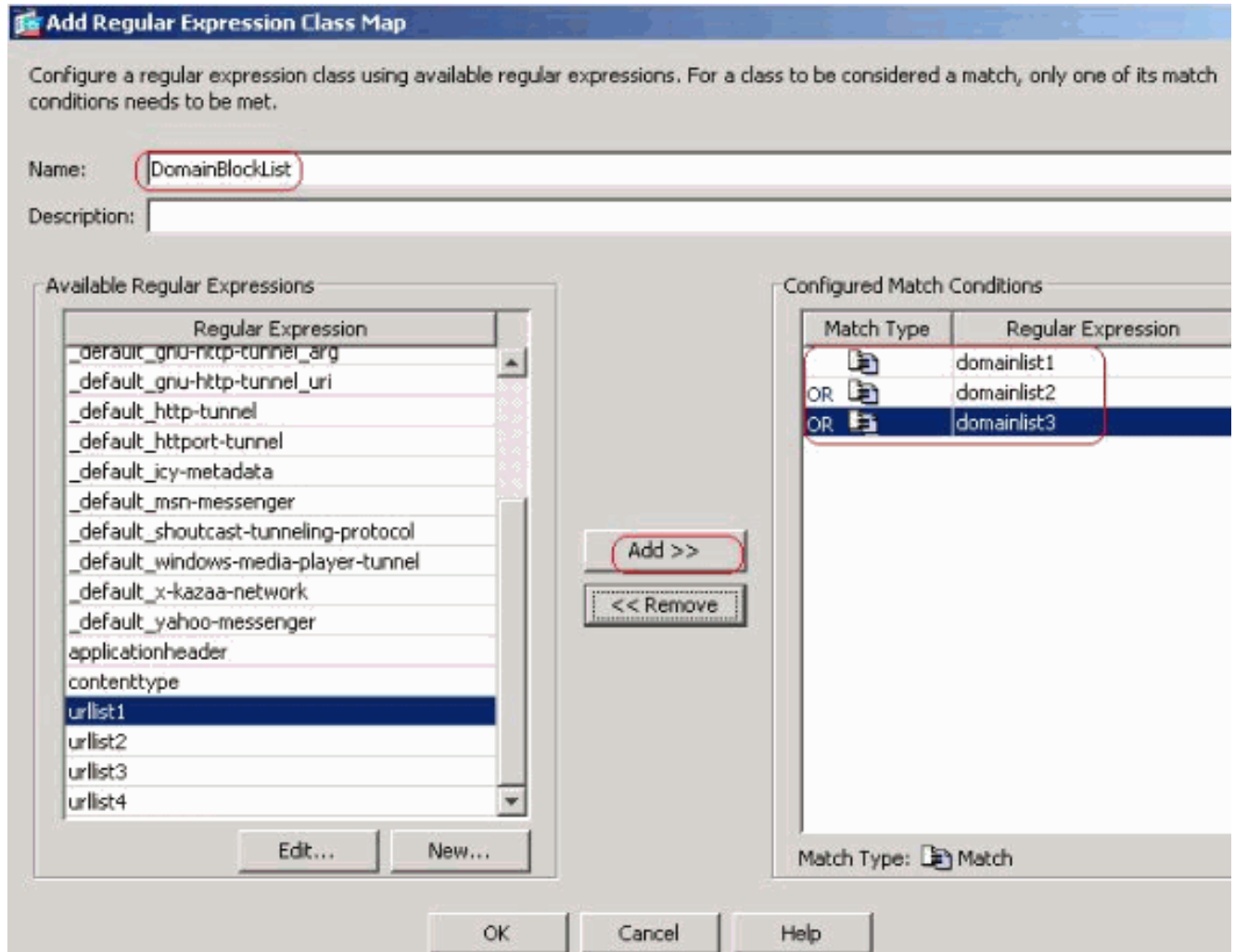
OK. Crie um **applicationheader** da expressão regular a fim capturar o vários encabeçamento do aplicativo.



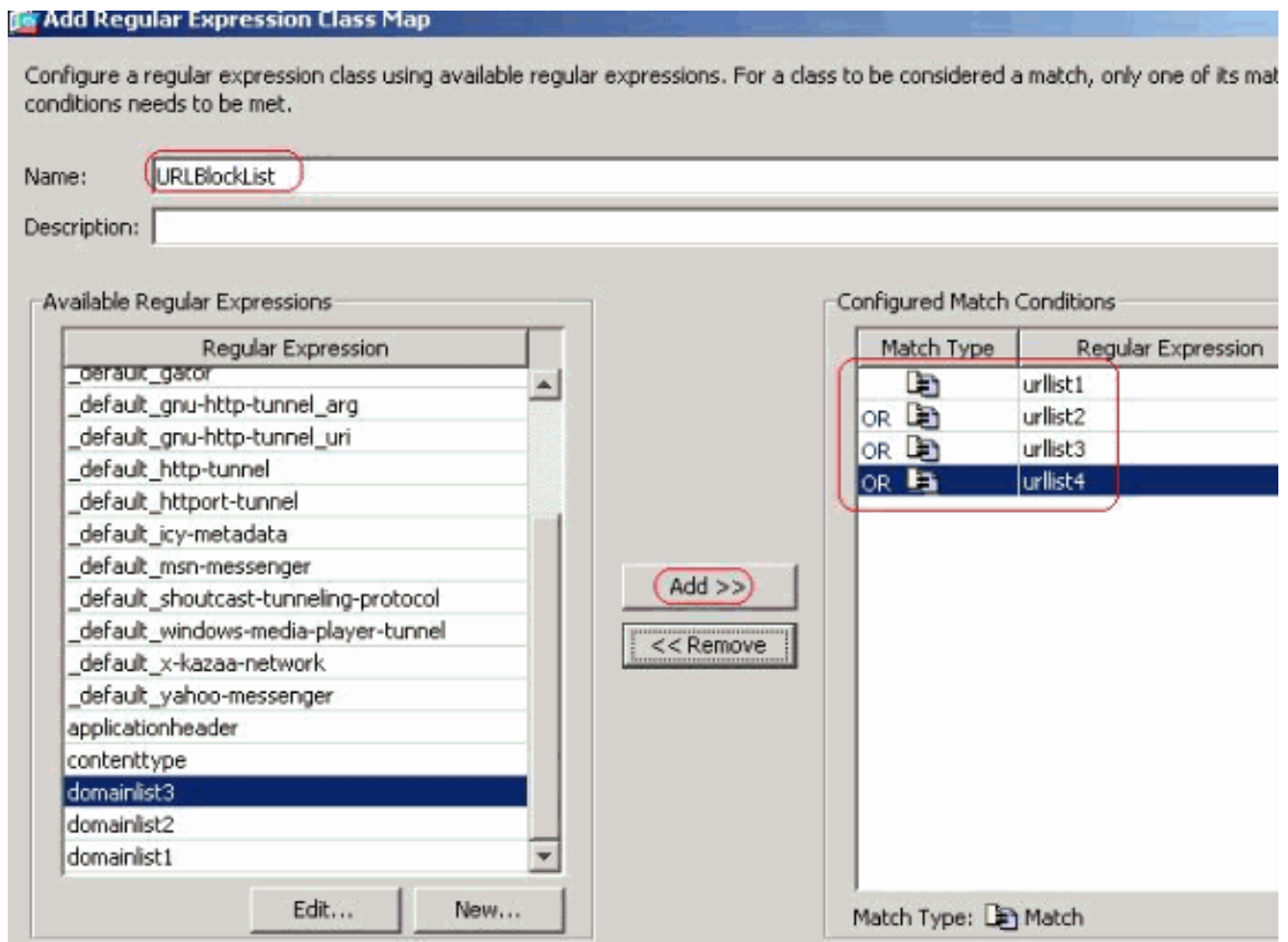
Clique em **OK**. Configuração de

CLI equivalente

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

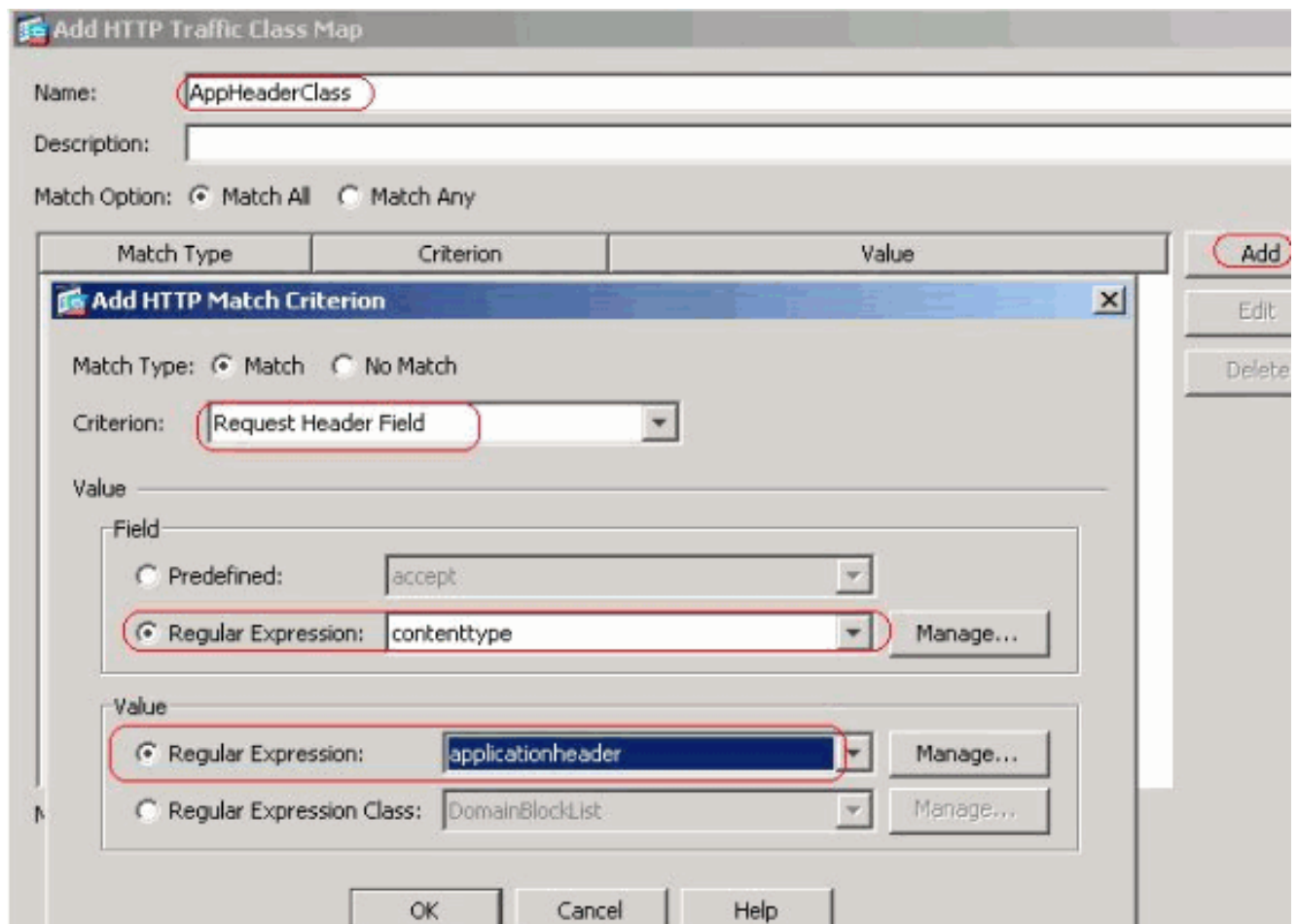


Crie uma classe **URLBlockList** da expressão regular a fim combinar algumas das expressões regulares urlist1, urlist2, urlist3 e urlist4. Clique em **OK**.

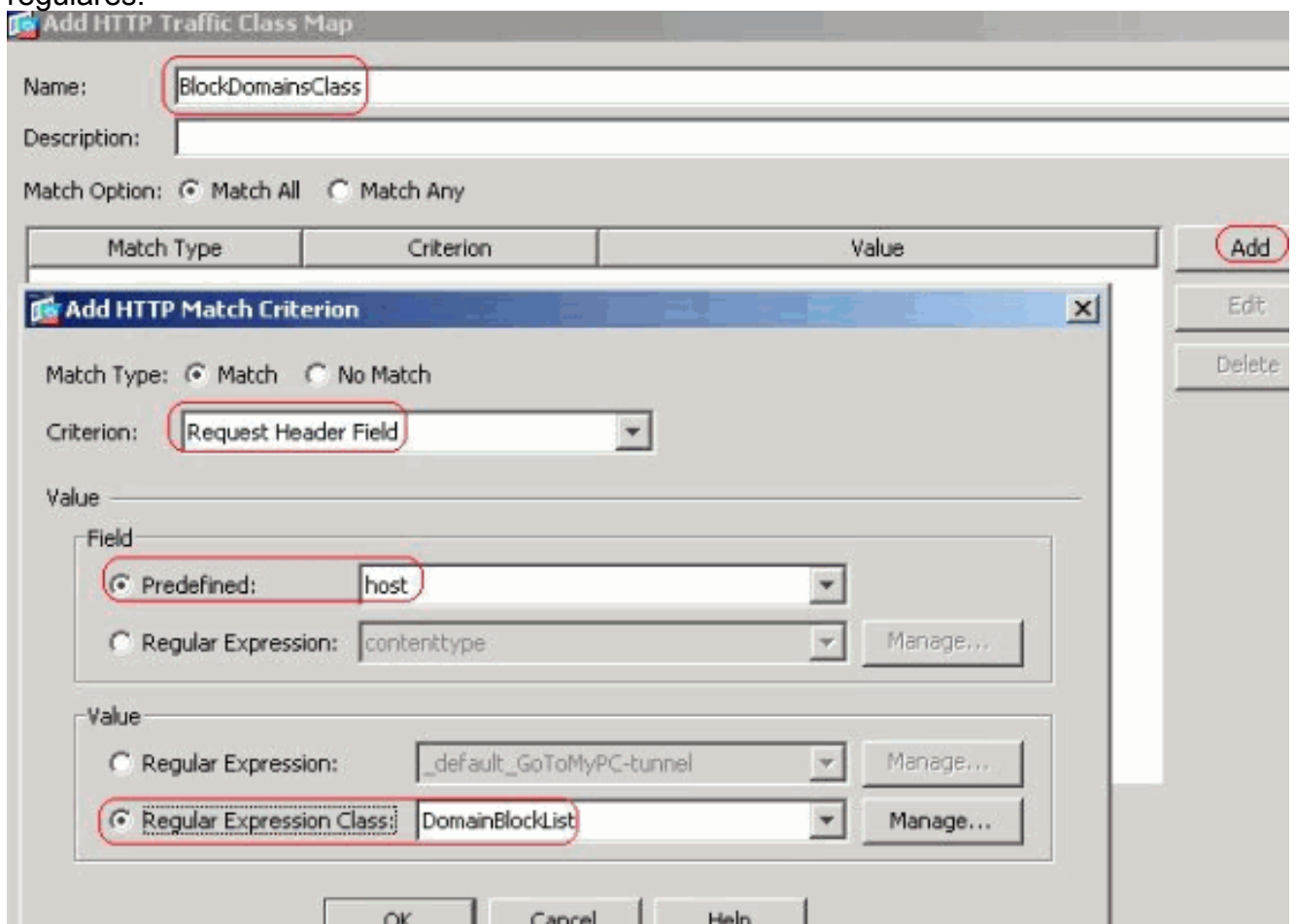


Configuração de CLI equivalente

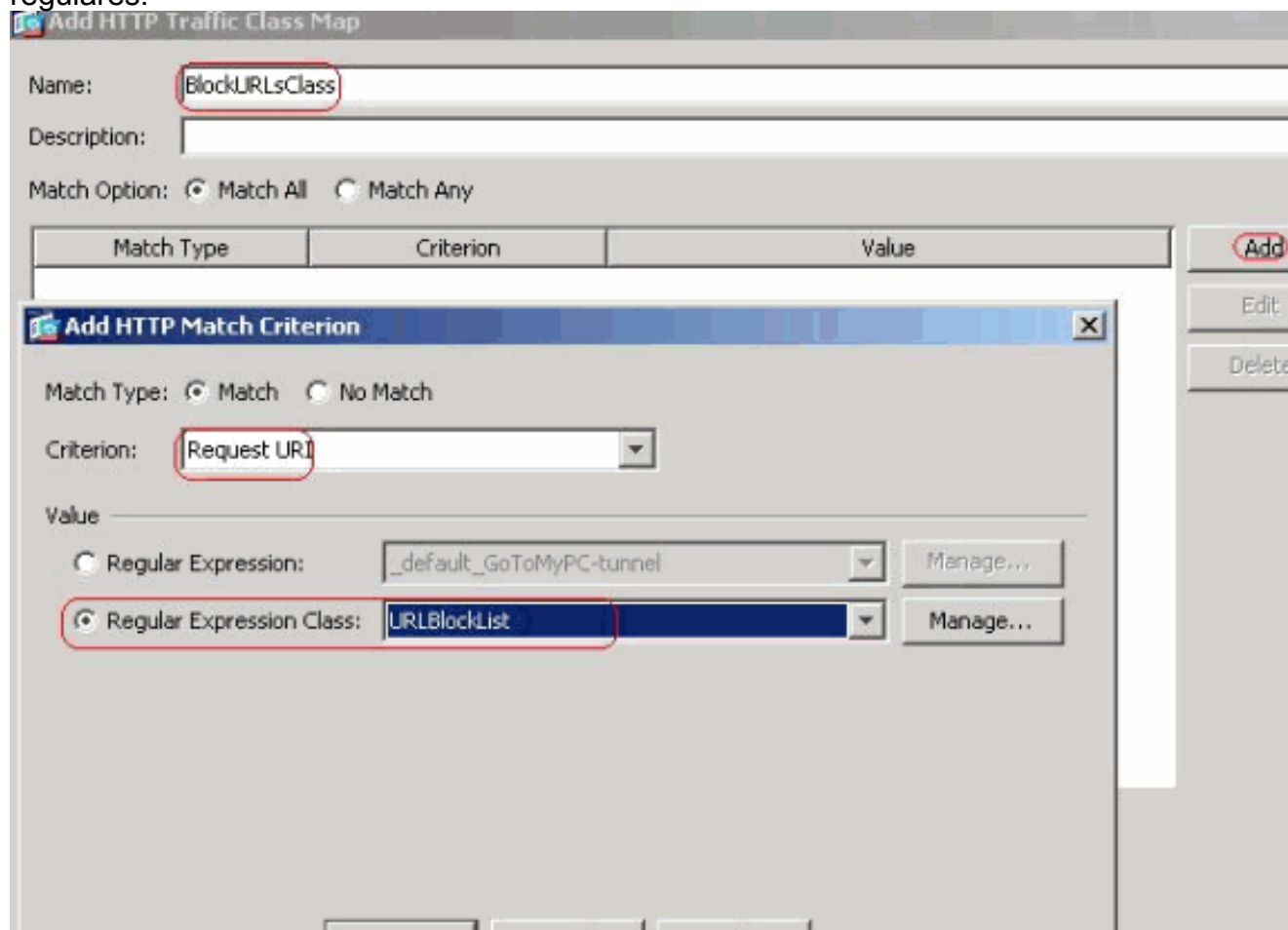
3. Inspeção o tráfego identificado com mapas da classe Escolha a configuração > o Firewall > os objetos > a classe traça > > Add HTTP a fim criar um mapa da classe para inspecionar o tráfego HTTP identificado por várias expressões regulares como mostradas. Crie um mapa **AppHeaderClass** da classe a fim combinar o cabeçalho da resposta com as captações das expressões regulares.



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

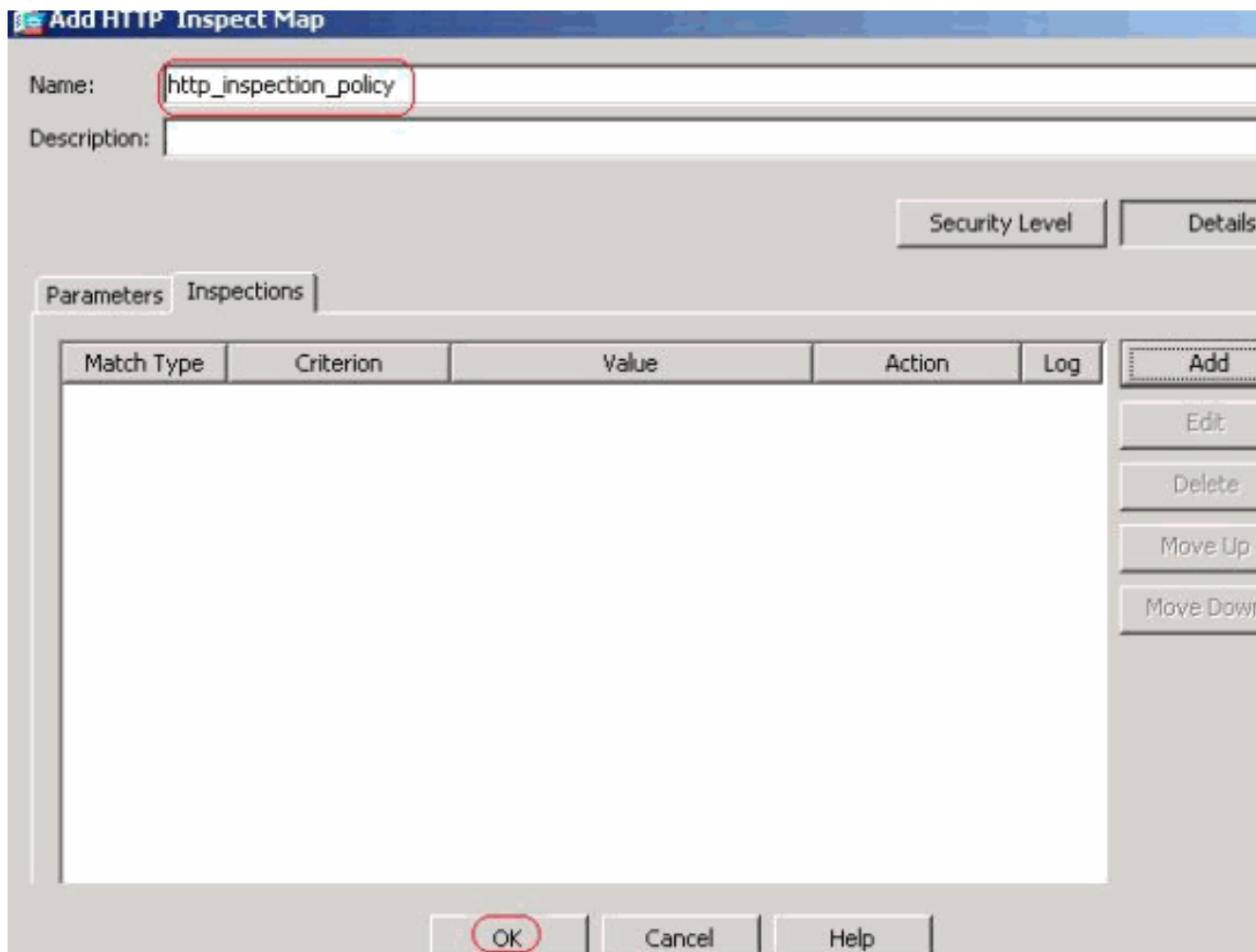


Clique em **OK**. Crie um mapa **BlockURLsClass** da classe a fim combinar o uri do pedido com as captações das expressões regulares.

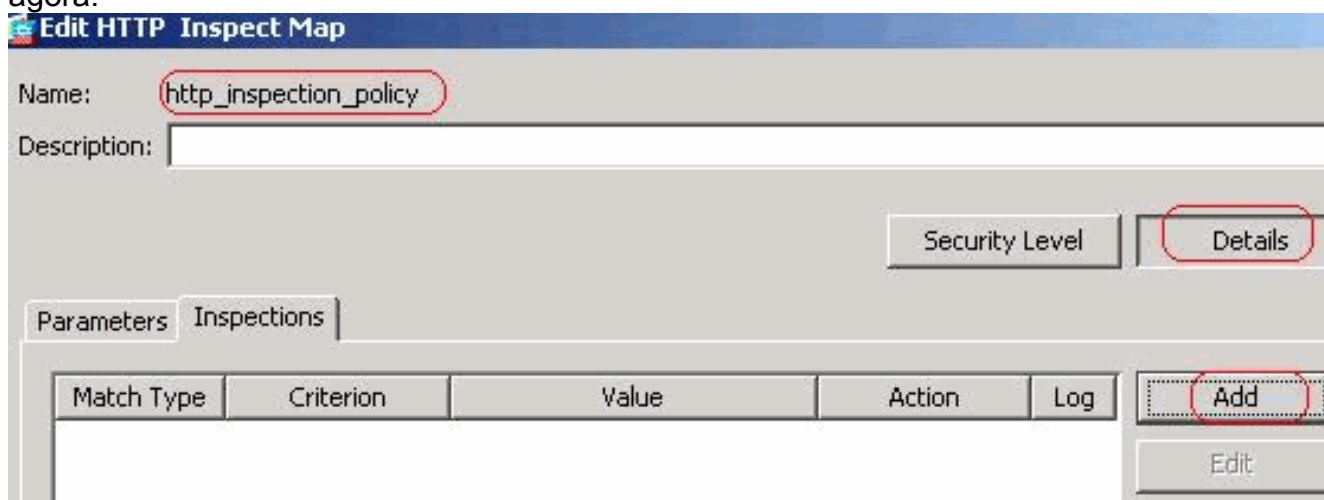


Clique em **OK**. Configuração de CLI equivalente

4. Ajuste as ações para o tráfego combinado na política da inspeção Escolha a configuração > o Firewall > os objetos > inspecionam mapas > HTTP a fim criar um `http_inspection_policy` para ajustar como mostrado a ação para o tráfego combinado. Clique em **OK**.



Escolha a configuração > o Firewall > os objetos > inspecionam mapas > HTTP > **http_inspection_policy** (dobre o clique) e clicam o > **Add dos detalhes** a fim ajustar as ações para as várias classes criadas até agora.



Ajuste a ação como a **conexão da gota** e **permita o registro** para o critério como o método do pedido e valor como

Add HTTP Inspect

Match Criteria

Single Match

Match Type: Match No Match

Criterion:

Value

Method:

Regular Expression

Regular Expression:

Regular Expression Class:

Multiple matches

HTTP Traffic Class:

Actions

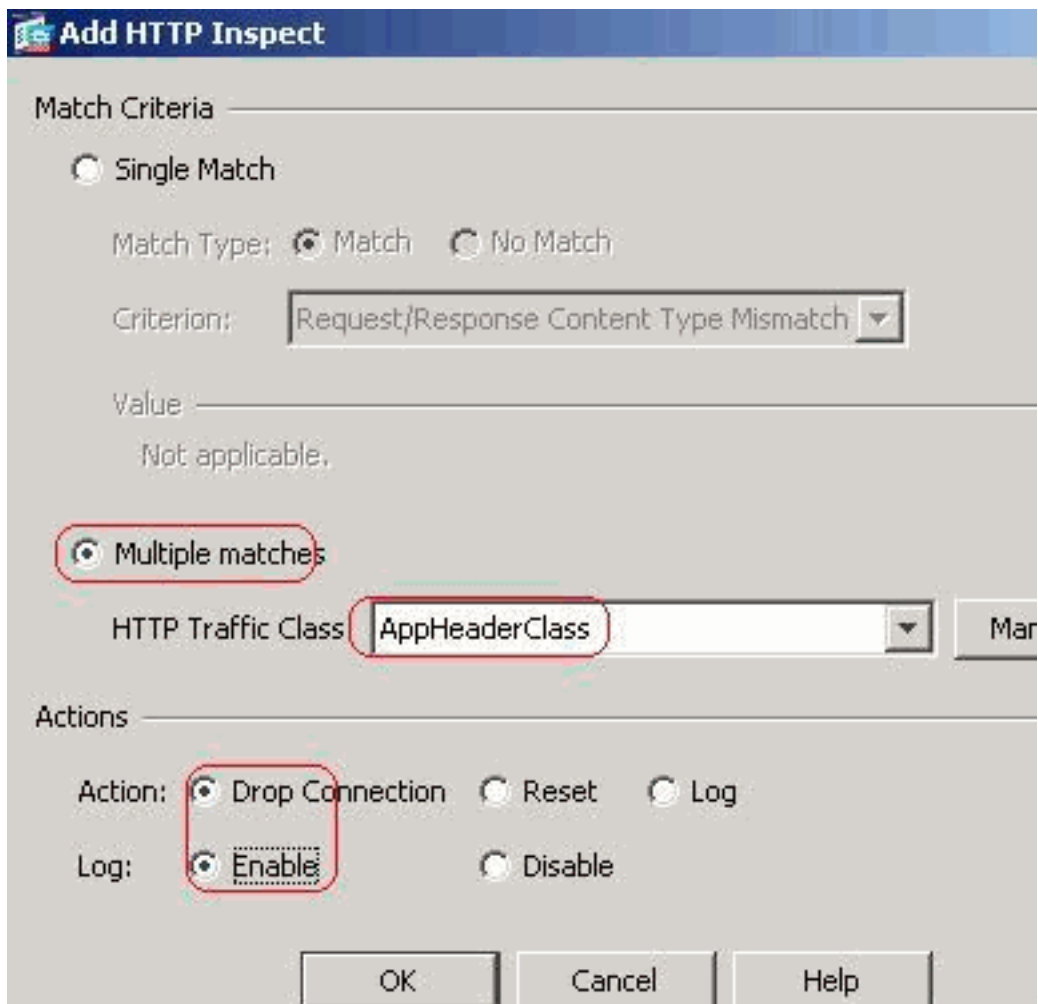
Action: Drop Connection Reset Log

Log: Enable Disable

conectam.

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

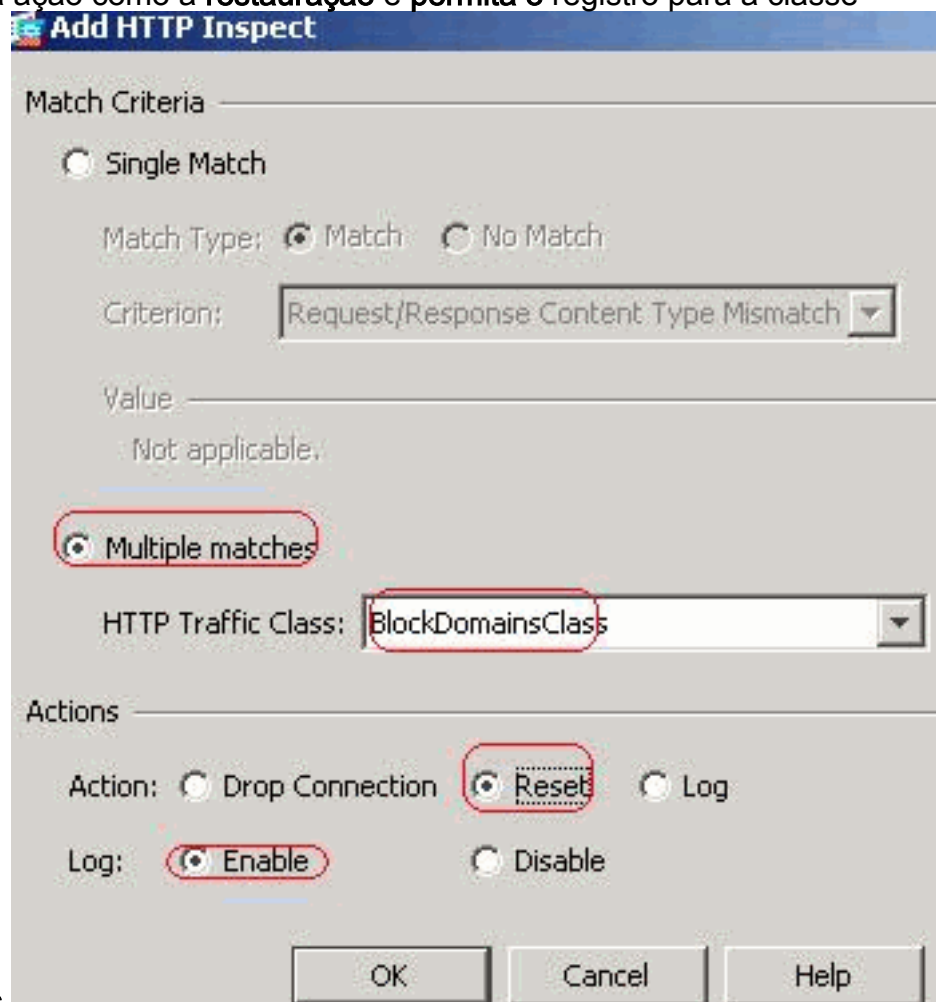
Clique



AppHeaderClass.

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

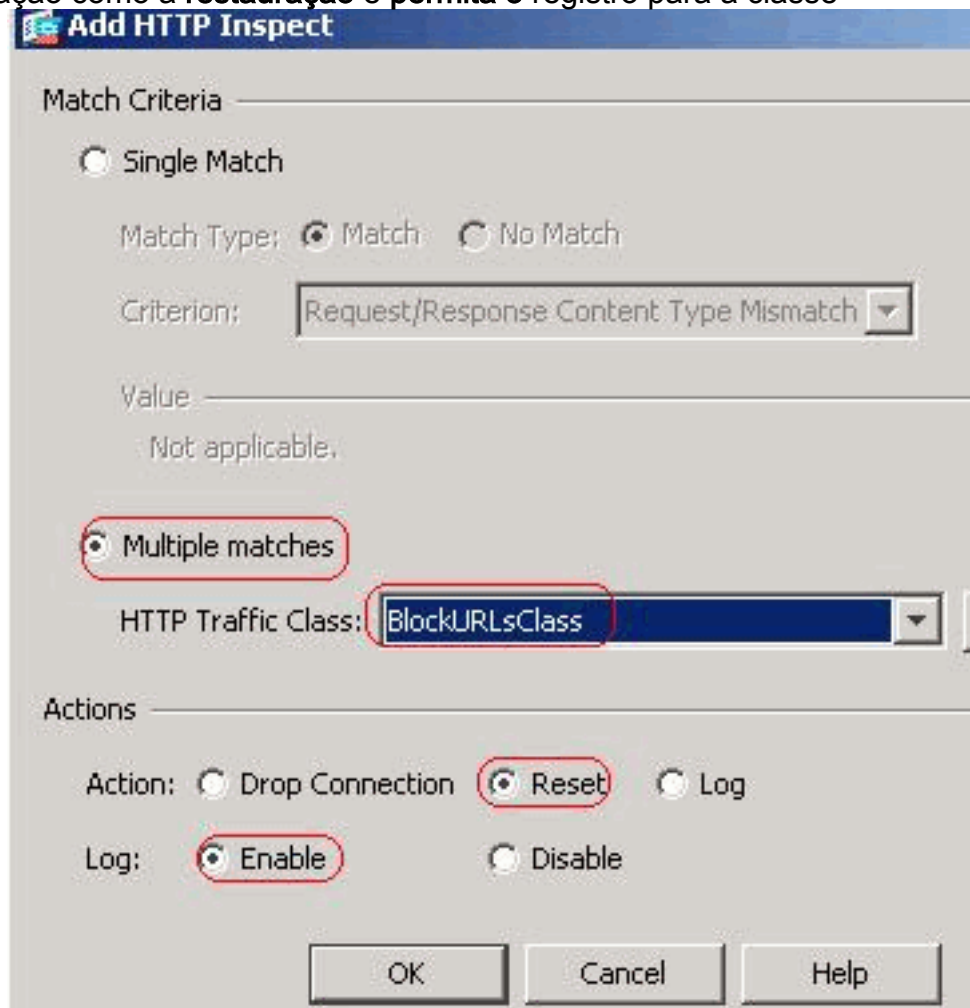
Cli



BlockDomainsClass.

Clique

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

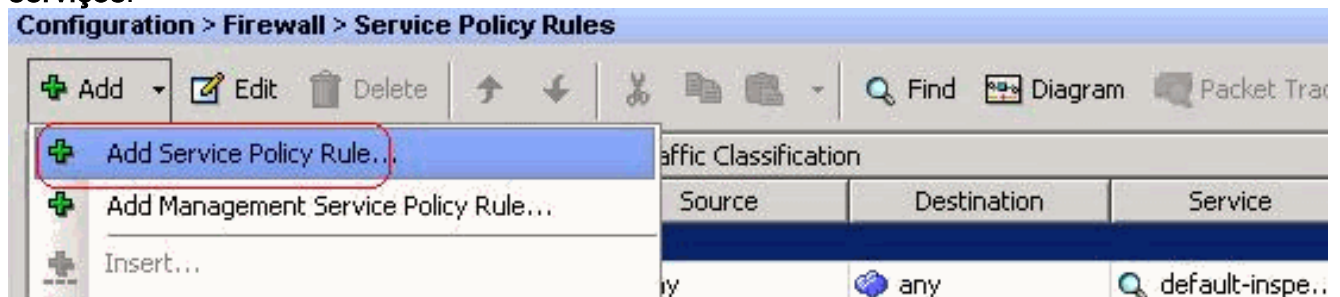


BlockURLsClass.

Clique

em OK. Clique em Apply. Configuração de CLI equivalente

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



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

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To: _____

Only one service policy can be configured per interface or at global level. If a service policy already exists, the new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface: ▼

Policy Name:

Description:

Global - applies to all interfaces

Policy Name:

Description:

< Back

Next >

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

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

Default Inspection Traffic

Source and Destination IP Address (uses ACL)

Tunnel Group

TCP or UDP Destination Port

RTP Range

IP DiffServ CodePoints (DSCP)

IP Precedence

Any traffic

Use an existing traffic class:

Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default all situation.

Escolha a fonte e o destino tão com serviço quanto o TCP-UDP/HTTP. Clique em Next.

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: Match Do not match

Source: any

Destination: any

Service: tcp-udp/http

Description:

More Options

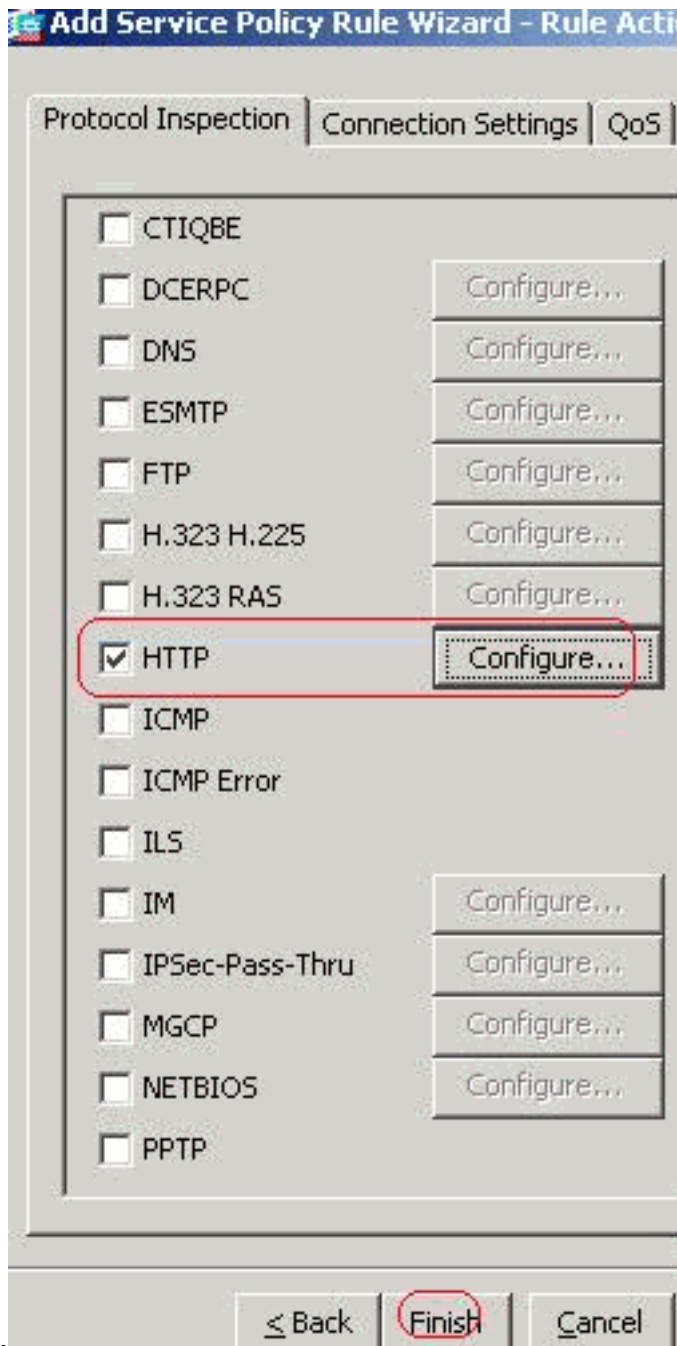
Enable Rule

Source Service: (TCP or UDP service only)

Time Range:

≤ Back **Next >**

Verifique o botão de rádio **HTTP** e o clique

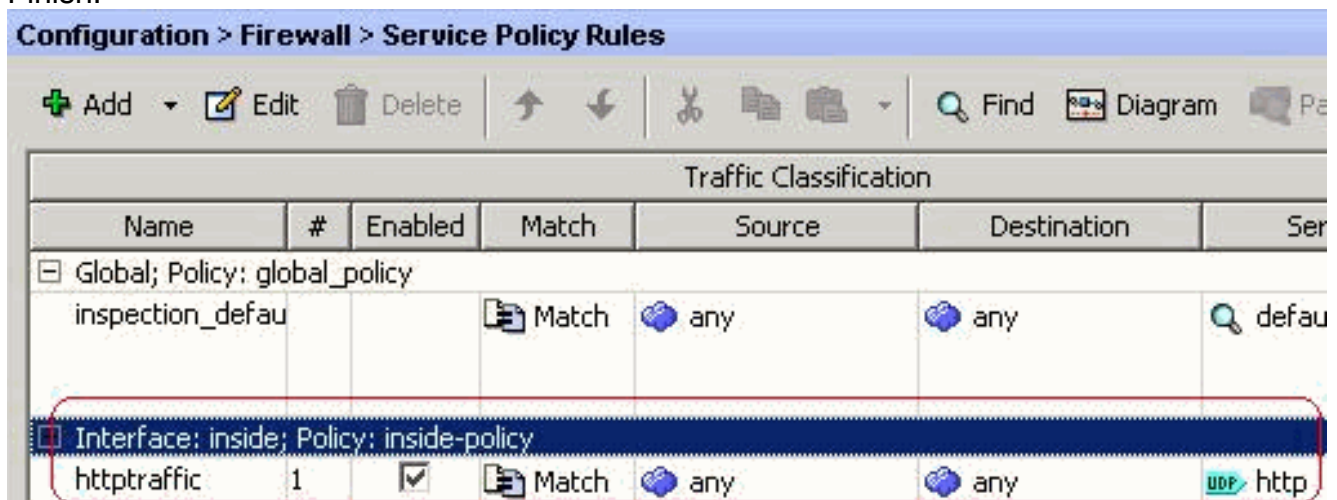


configura. Verifique o botão de rádio selecionam um HTTP inspecionam o mapa para o controle sobre a inspeção como

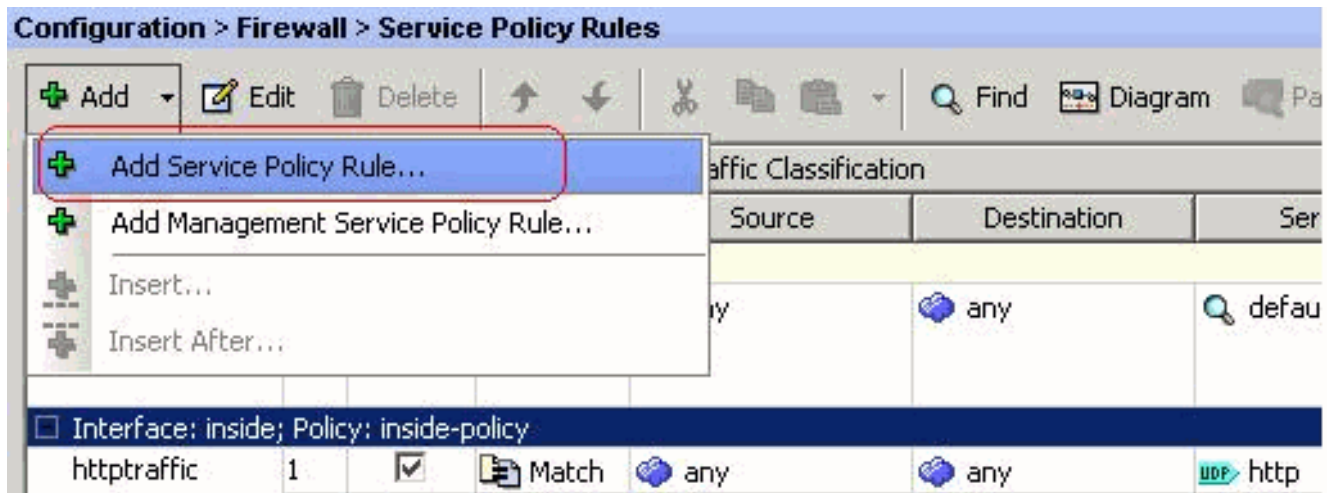


mostrado. Clique em **OK**.

Clique em Finish.

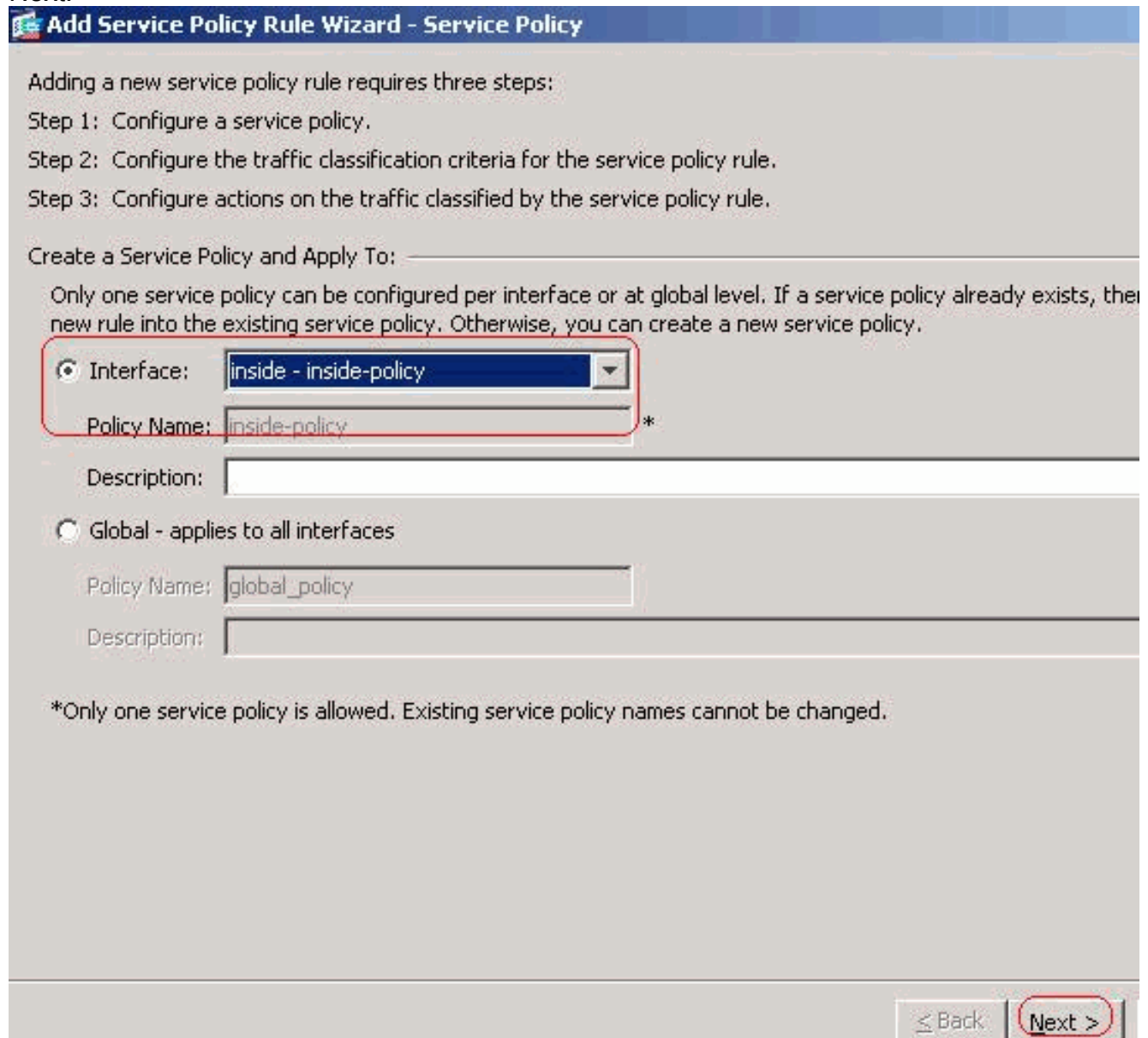


Tráfego da porta 8080 Além disso, escolha **adicionam a regra da política de serviços do > Add.**



Clique em

Next.



Escolha o botão de rádio **adicionam a regra a classe de tráfego existente** e escolhem

httptraffic do menu de gota para baixo. Clique em

Next.

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

Add rule to existing traffic class:

Rule can be added to an existing class map if that class map uses access control list (ACL) as its traffic match

Use an existing traffic class:

Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default all situation.

Escolha a fonte e o destino como alguns com **tcp/8080**. Clique em Next.

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: Match Do not match

Source: ...

Destination: ...

Service: ...

Description:

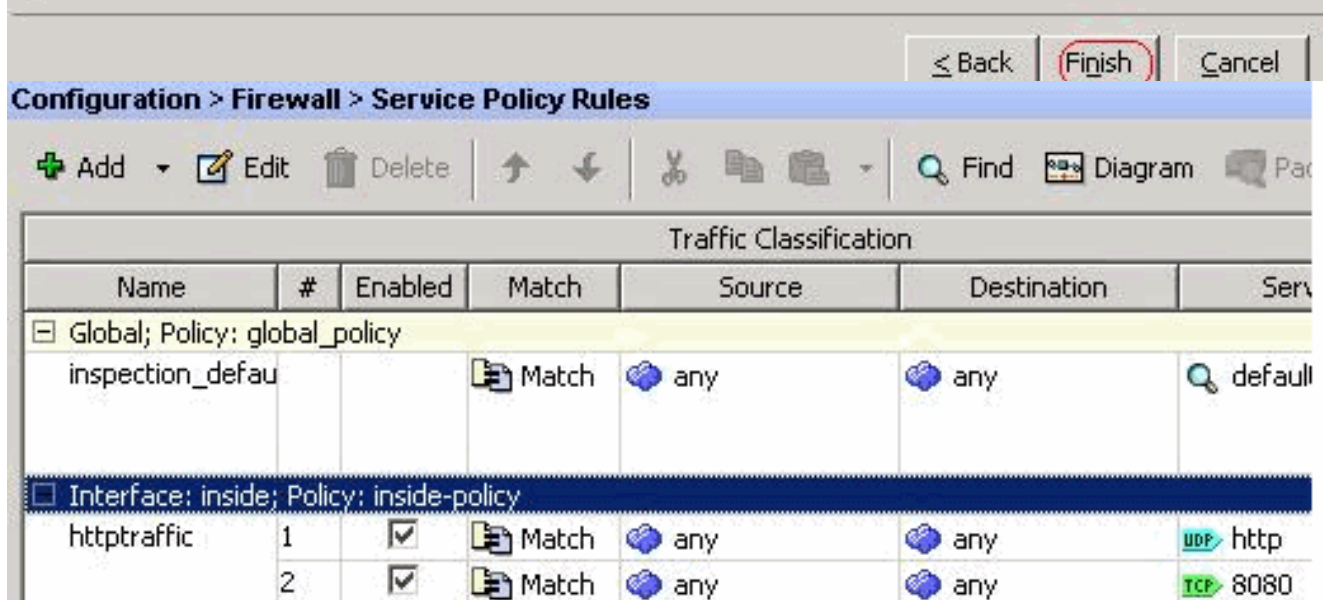
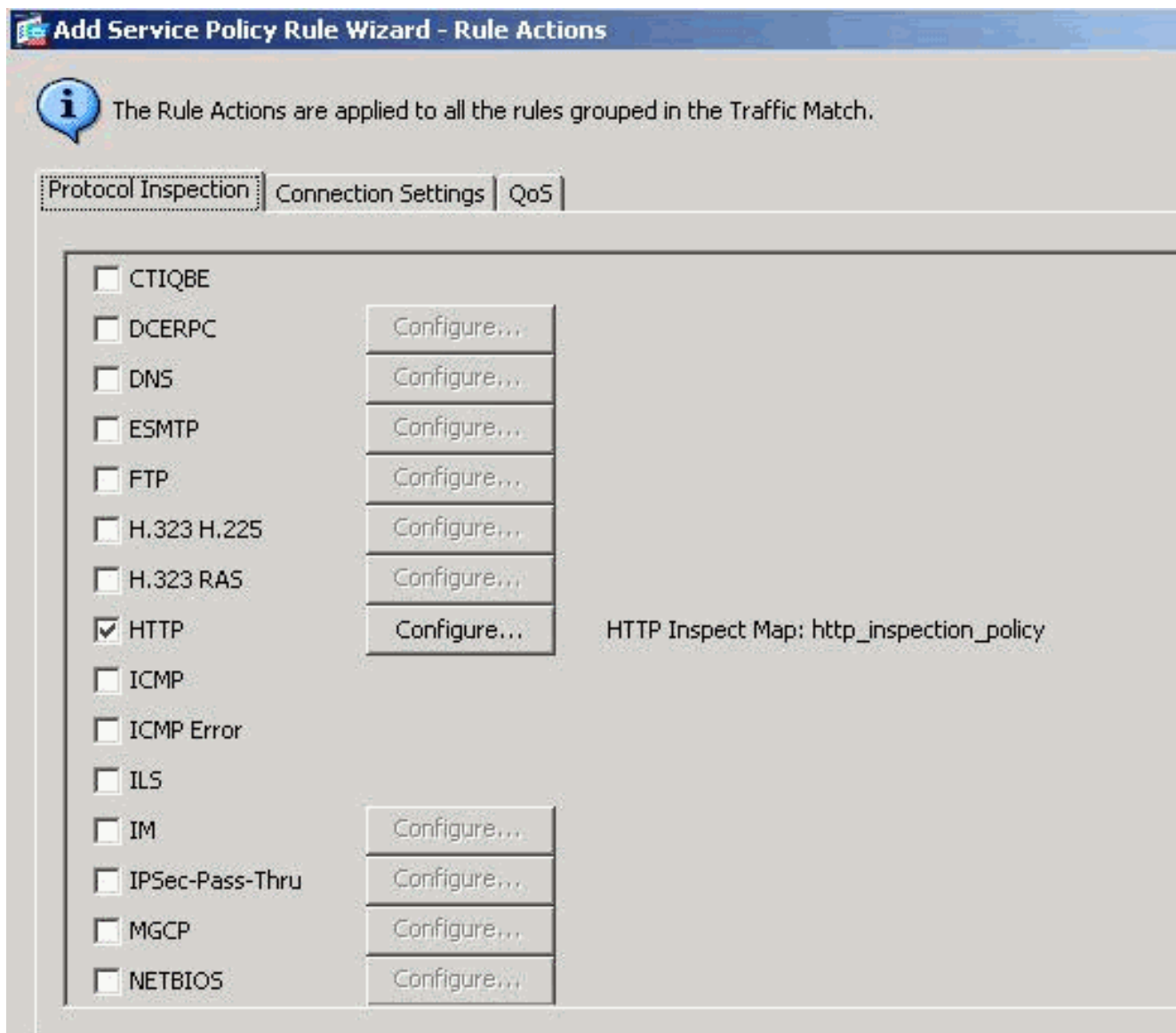
More Options

Enable Rule

Source Service: ... (TCP or UDP service only)

Time Range: ...

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

- [Apoio do Dispositivos de segurança adaptáveis Cisco ASA série 5500](#)
- [Apoio do Cisco Adaptive Security Device Manager \(ASDM\)](#)
- [Apoio do Dispositivos de segurança Cisco PIX série 500](#)
- [Cisco PIX Firewall Software](#)
- [Referências do comando Cisco Secure PIX Firewall](#)
- [Avisos de campo de produto de segurança \(incluindo PIX\)](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)