

ASA/PIX 8.x: Ciertos sitios web del bloque (URL) usando las expresiones normales con el ejemplo de la configuración MPF

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[Antecedentes](#)

[Descripción modular del Marco de políticas](#)

[Expresión normal](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración CLI ASA](#)

[Configuración 8.x ASA con el ASDM 6.x](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo configurar Cisco Security Appliances ASA/PIX 8.x que utilizan expresiones normales con el Marco de políticas modular (MPF) para bloquear ciertos sitios Web (URL).

Nota: Esta configuración no bloquea todas las descargas de la aplicación. Para el archivo confiable que bloquea, un dispositivo dedicado tal como serie S de Ironport o un módulo tal como el módulo del CSC para el ASA debe ser utilizado.

Nota: La filtración HTTPS no se soporta en el ASA. El ASA no puede hacer la inspección de paquetes profunda o examen basado en la expresión normal para el tráfico HTTPS, porque en el HTTPS, el contenido del paquete se cifra (SSL).

[prerrequisitos](#)

[Requisitos](#)

Este documento asume que el dispositivo del Cisco Security está configurado y trabaja correctamente.

Componentes Utilizados

- El dispositivo de seguridad adaptante de las Cisco 5500 Series (ASA) ese funciona con la versión de software 8.0(x) y posterior
- Versión 6.x del Cisco Adaptive Security Device Manager (ASDM) para ASA 8.x

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con las Cisco 500 Series PIX que funciona con la versión de software 8.0(x) y posterior.

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Descripción modular del Marco de políticas

El MPF proporciona un constante y una manera flexible configurar las características del dispositivo de seguridad. Por ejemplo, usted puede utilizar el MPF para crear una configuración del descanso que sea específica a una aplicación TCP determinada, en comparación con una que se aplique a todas las aplicaciones TCP.

El MPF soporta estas características:

- Normalización TCP, TCP y límites y descansos de la conexión UDP, y distribución aleatoria del número de secuencia TCP
- CSC
- Inspección de la aplicación
- IPS
- Políticas de entrada de QoS
- Policing de la salida de QoS
- Prioridad de Calidad de servicio (QoS) cola

La configuración del MPF consiste en cuatro tareas:

1. Identifique la capa 3 y el tráfico 4 al cual usted quiere aplicar las acciones. Refiera a [identificar el tráfico usando un mapa de la clase de la capa 3/4](#) para más información.
2. (Inspección de la aplicación solamente) defina las acciones especiales para el tráfico de la Inspección de la aplicación. Refiera a [configurar las acciones especiales para las](#)

[Inspecciones de la aplicación](#) para más información.

3. Aplique las acciones a la capa 3 y el tráfico 4. Refiera a [definir las acciones usando una correspondencia de políticas de la capa 3/4](#) para más información.
4. Active las acciones en una interfaz. Refiera a [aplicar una directiva de la capa 3/4 a una interfaz usando una política de servicio](#) para más información.

Expresión normal

Una expresión normal hace juego las cadenas de texto literalmente como cadena exacta, o por el uso de los metacharacters así que usted puede hacer juego las variantes múltiples de una cadena de texto. Usted puede utilizar una expresión normal para hacer juego el contenido de cierto tráfico de aplicación; por ejemplo, usted puede hacer juego una cadena URL dentro de un paquete HTTP.

Nota: ¿Utilice **Ctrl+V** para escapar todos los caracteres especiales en el CLI, tal como signo de interrogación (?) o un cuadro por ejemplo, **[Ctrl+V]** del tipo **d?** ¿**g** para ingresar **d? g** en la configuración.

Para la creación de una expresión normal, utilice el comando del **regex**, que se puede utilizar para las diversas características que requieren corresponder con del texto. Por ejemplo, usted puede configurar las acciones especiales para la Inspección de la aplicación con el uso del Marco de políticas modular que utiliza una correspondencia de políticas del examen. Refiera al [comando inspect del tipo de la correspondencia de políticas](#) para más información. En la correspondencia de políticas del examen, usted puede identificar el tráfico que usted quiere actuar sobre si usted crea una correspondencia de la clase del examen que contenga uno o más **comandos match** o usted puede utilizar los **comandos match** directamente en la correspondencia de políticas del examen. Algunos **comandos match** le dejaron identificar el texto en un paquete usando una expresión normal; por ejemplo, usted puede hacer juego las cadenas URL dentro de los paquetes HTTP. Usted puede agrupar las expresiones normales en una correspondencia de la clase de la expresión normal. Refiera al comando del [regex del tipo del clase-mapa](#) para más información.

Esta [tabla](#) enumera los metacharacters que tienen significados especiales.

Carácter	Descripción	Notas
.	Punto	Coincide con cualquier carácter único. Por ejemplo, d.g hace juego el perro, el dag, el dtg, y cualquier palabra que contenga esos caracteres, tales como doggonnit.
(exp)	Subexpresión	Un subexpresión segrega los caracteres de los caracteres circundantes, de modo que usted pueda utilizar otros metacharacters en el subexpresión. Por ejemplo, d(o)el perro de las coincidencias a) g y el dag, pero hacen las coincidencias AG hacen y AG. Un subexpresión se puede también utilizar con los cuantificadores de la repetición para distinguir los caracteres significados para la repetición. Por ejemplo, ab(xy){3}z hace

		juego el abxyxyz.
	Alternancia	Hace juego cualquier expresión que se separa. Por ejemplo, perro el gato hace juego el perro o el gato.
¿?	Signo de interrogación	Un cuantificador que indica que hay 0 o 1 de la expresión anterior. ¿Por ejemplo, lo? el SE hace juego el lse o pierde. Nota: Usted debe ingresar Ctrl+V y entonces se invoca el signo de interrogación o bien la función de ayuda.
*	Asterisco	Un cuantificador que indica que hay 0, 1 o cualquier número de la expresión anterior. Por ejemplo, el lo*se hace juego el lse, pierde, flexible, y así sucesivamente.
{x}	Relance el cuantificador	Relance exactamente los tiempos x. Por ejemplo, ab(xy){3}z hace juego el abxyxyz.
{x,}	Cuantificador mínimo de la repetición	Relance por lo menos los tiempos x. Por ejemplo, ab(xy){2,}z hace juego el abxyz, abxyxyz, y así sucesivamente.
[abc]	Clase de carácter	Hace juego cualquier carácter en los corchetes. Por ejemplo, el [abc] hace juego a, b, o la C.
[^abc]	Clase de carácter negada	Hace juego un solo carácter que no se contenga dentro de los corchetes. Por ejemplo, el [^abc] hace juego cualquier carácter con excepción de a, b, o el [^A-Z] . C. hace juego cualquier solo carácter que no sea una letra mayúscula.
[a-c]	Clase del rango del carácter	Hace juego cualquier carácter en el rango. el [a-z] hace juego cualquier letra minúscula. Usted puede mezclar los caracteres y los rangos: el [abcq-z] hace juego a, b, c, q, r, s, t, u, v, w, x, y, z, y así que hace el [a-cq-z] . El carácter de la rociada (-) es literal solamente si es el último o el primer carácter dentro de los corchetes: [abc-] o [-abc] .
""	Comillas	Cotos que arrastran o que llevan los espacios en la cadena. Por ejemplo, la "prueba" preserva el espacio principal cuando busca una coincidencia.
^	Signo de intercal	Especifica el principio de una línea

	acción	
\	Carácter de escape	Cuando está utilizado con un metacaracter, hace juego un carácter literal. Por ejemplo, \ [hace juego los corchetes izquierdos.
char	Carácter	Cuando el carácter no es un metacaracter, hace juego el carácter literal.
\r	Retorno de carro	Hace juego un retorno de carro 0x0d
\n	Newline	Hace juego una línea nueva 0x0a
\t	Lengüeta	Hace juego una lengüeta 0x09
\f	Formfeed	Hace juego una alimentación de forma 0x0c
\xNN	Número hexadecimal escapado	Hace juego un carácter ASCII que utilice un hexadecimal que sea exactamente dos dígitos
\NNN	Número octal escapado	Hace juego un carácter ASCII pues octal que sea exactamente tres dígitos. Por ejemplo, el carácter 040 representa un espacio.

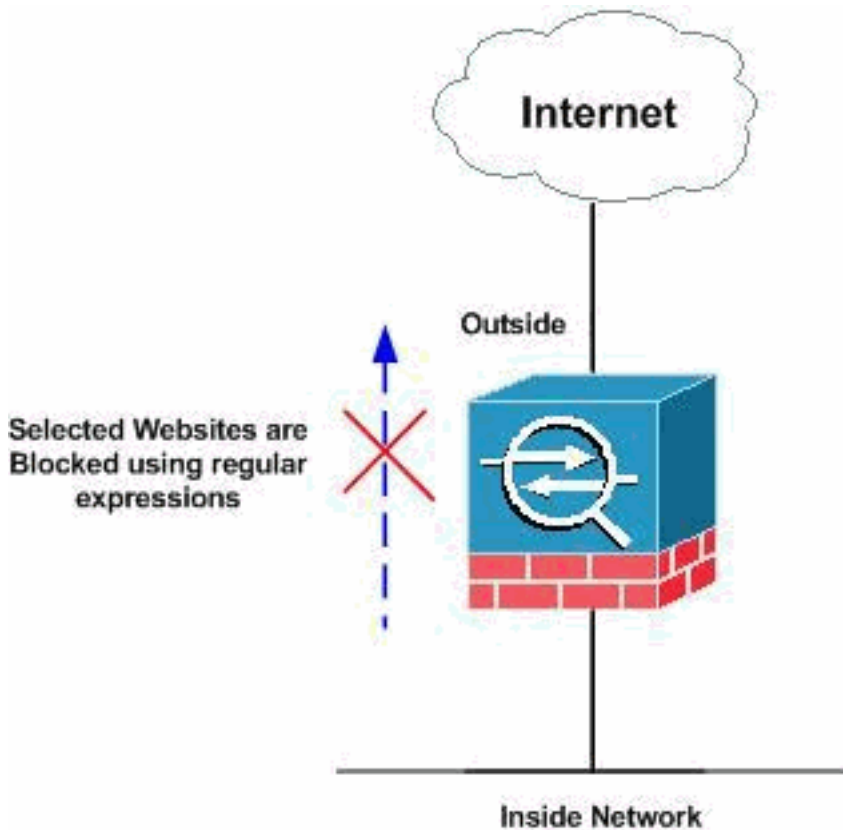
[Configurar](#)

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

[Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- [Configuración CLI ASA](#)
- [Configuración 8.x ASA con el ASDM 6.x](#)

Configuración CLI ASA

Configuración CLI ASA

```

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

```

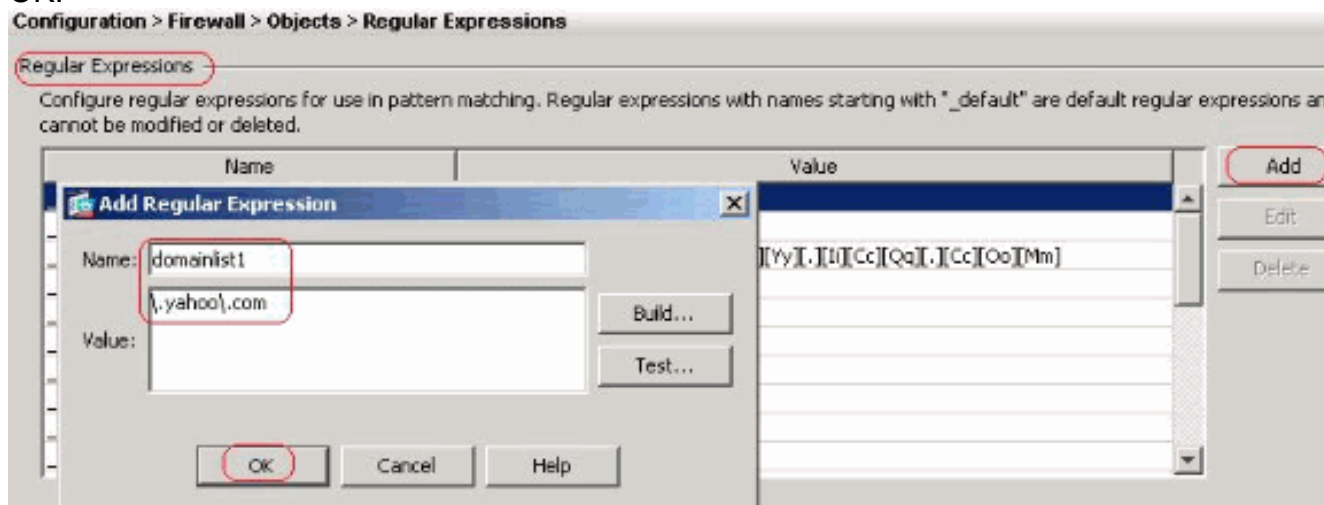
log !--- Define the actions such as drop, reset or log
!--- in the inspection policy map. policy-map
global policy class inspection default inspect dns
preset dns map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect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

```

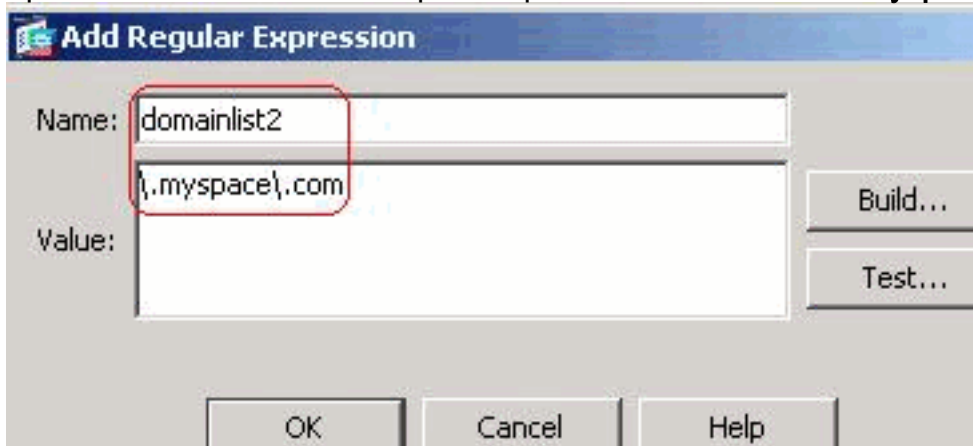
Configuración 8.x ASA con el ASDM 6.x

Complete estos pasos para configurar las expresiones normales y aplicarlas en el MPF para bloquear los sitios web específicos como se muestra.

1. Cree las expresiones normales Elija la configuración > Firewall> se opone > las expresiones normales y el teclado agrega bajo expresión normal de la lengüeta para crear las expresiones normales como se muestra. Cree una expresión normal **domainlist1** para capturar el Domain Name **yahoo.com**. Haga clic en OK.



Cree una expresión normal **domainlist2** para capturar el Domain Name **myspace.com**. Haga



clic en OK.

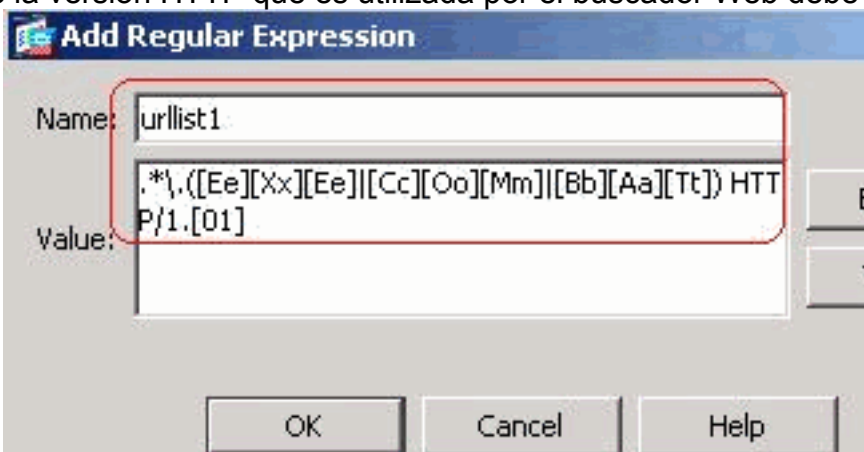
Cree una expresión normal **domainlist3** para capturar el Domain Name **youtube.com**. Haga clic en



OK.

Cree una expresión

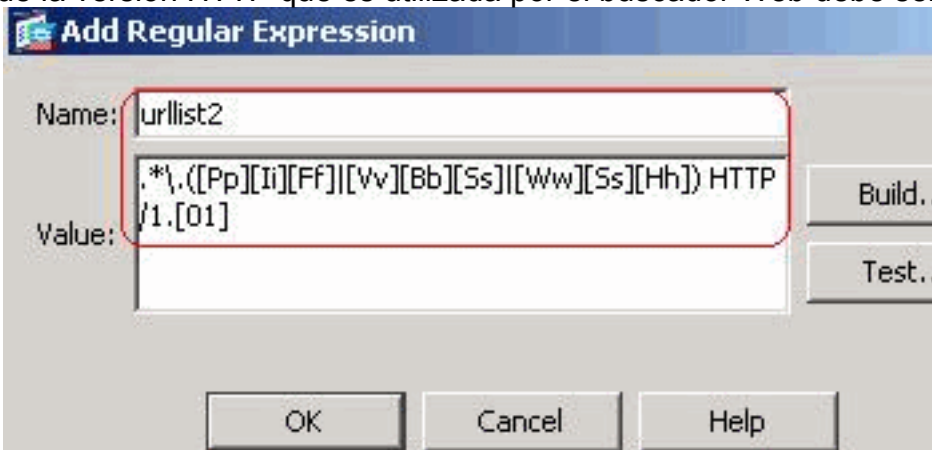
normal **urllist1** para capturar las extensiones de archivo tales como **exe**, **COM** y **palo** a condición de que la versión HTTP que es utilizada por el buscador Web debe ser 1.0 o 1.1.



Haga clic en OK.

Cree una

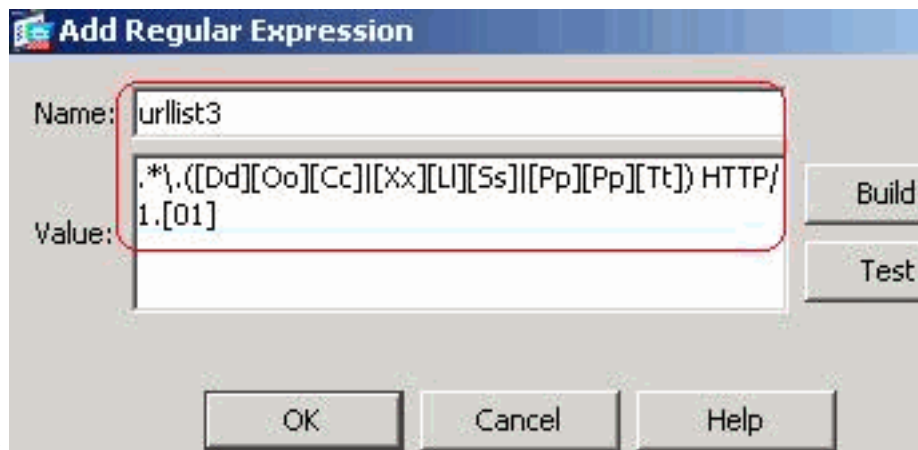
expresión normal **urllist2** para capturar las extensiones de archivo tales como **pif**, **vbs** y **wsh** a condición de que la versión HTTP que es utilizada por el buscador Web debe ser 1.0 o 1.1.



Haga clic en OK.

Cree una

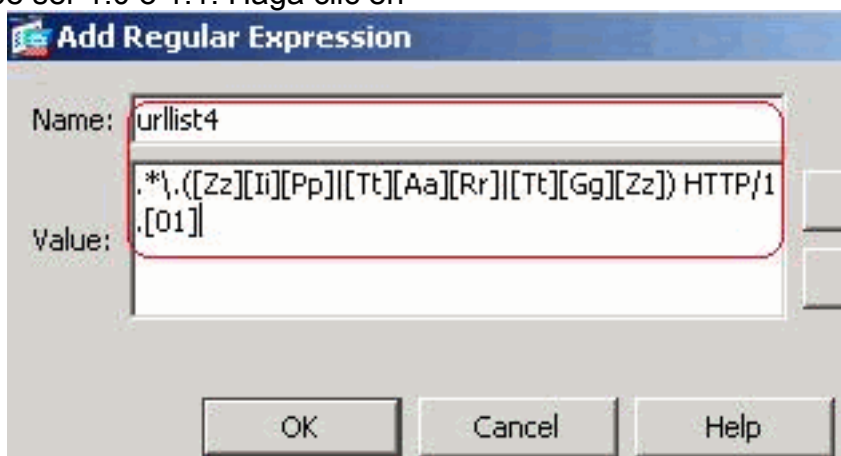
expresión normal **urllist3** para capturar las extensiones de archivo tales como **doc.**, **xls** y **ppt** a condición de que la versión HTTP que es utilizada por el buscador Web debe ser 1.0 o 1.1.



Haga clic en OK.

Cree una

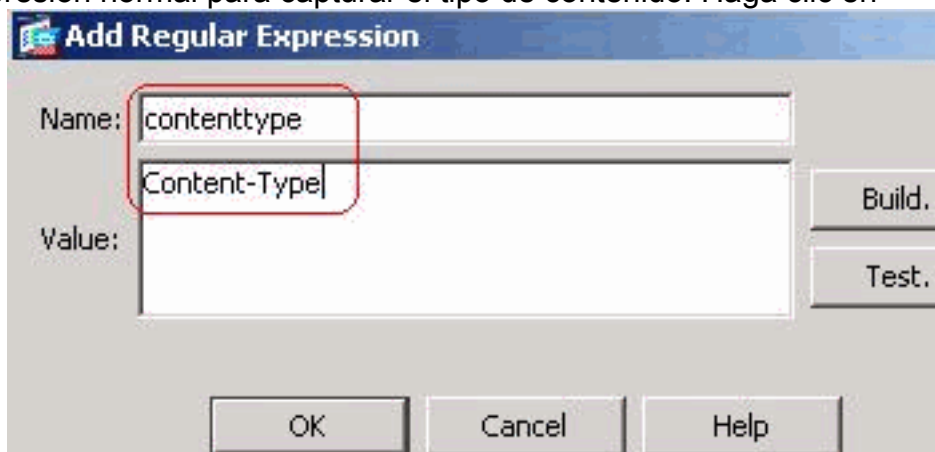
expresión normal **urllist4** para capturar las extensiones de archivo tales como **cremallera**, **alquitrán** y **tgz** a condición de que la versión HTTP que es utilizada por el buscador Web debe ser 1.0 o 1.1. Haga clic en



OK.

Cree un **contenttype** de la

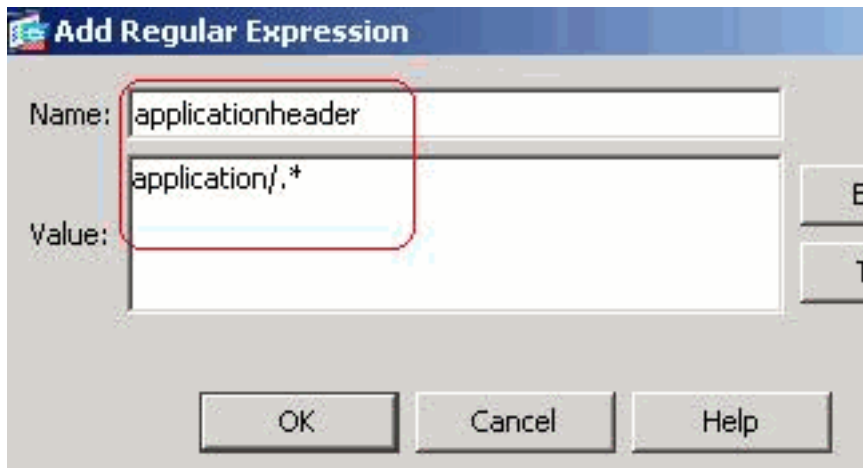
expresión normal para capturar el tipo de contenido. Haga clic en



OK.

Cree un

applicationheader de la expresión normal para capturar la diversa encabezado de la aplicación. Haga clic en

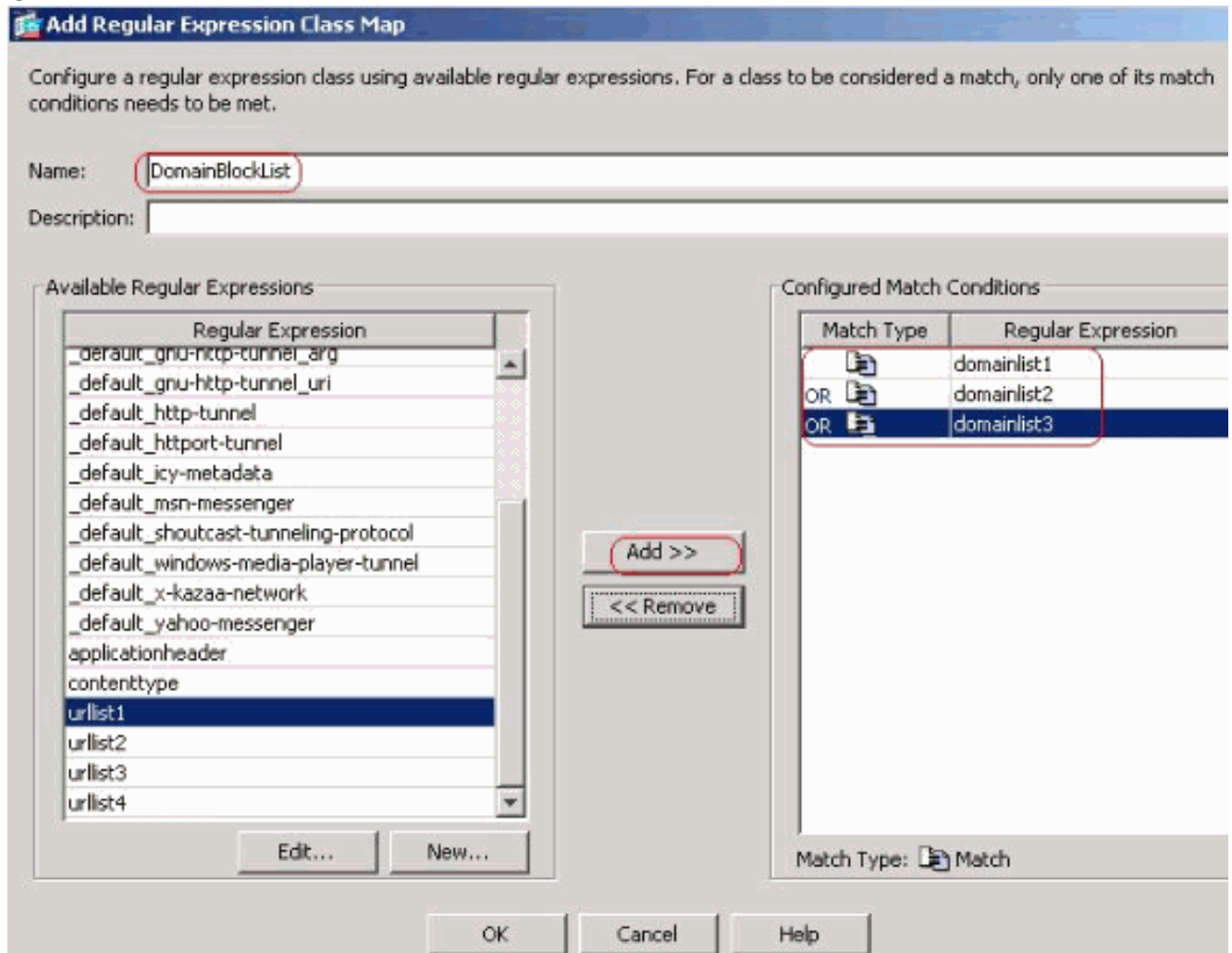


OK.

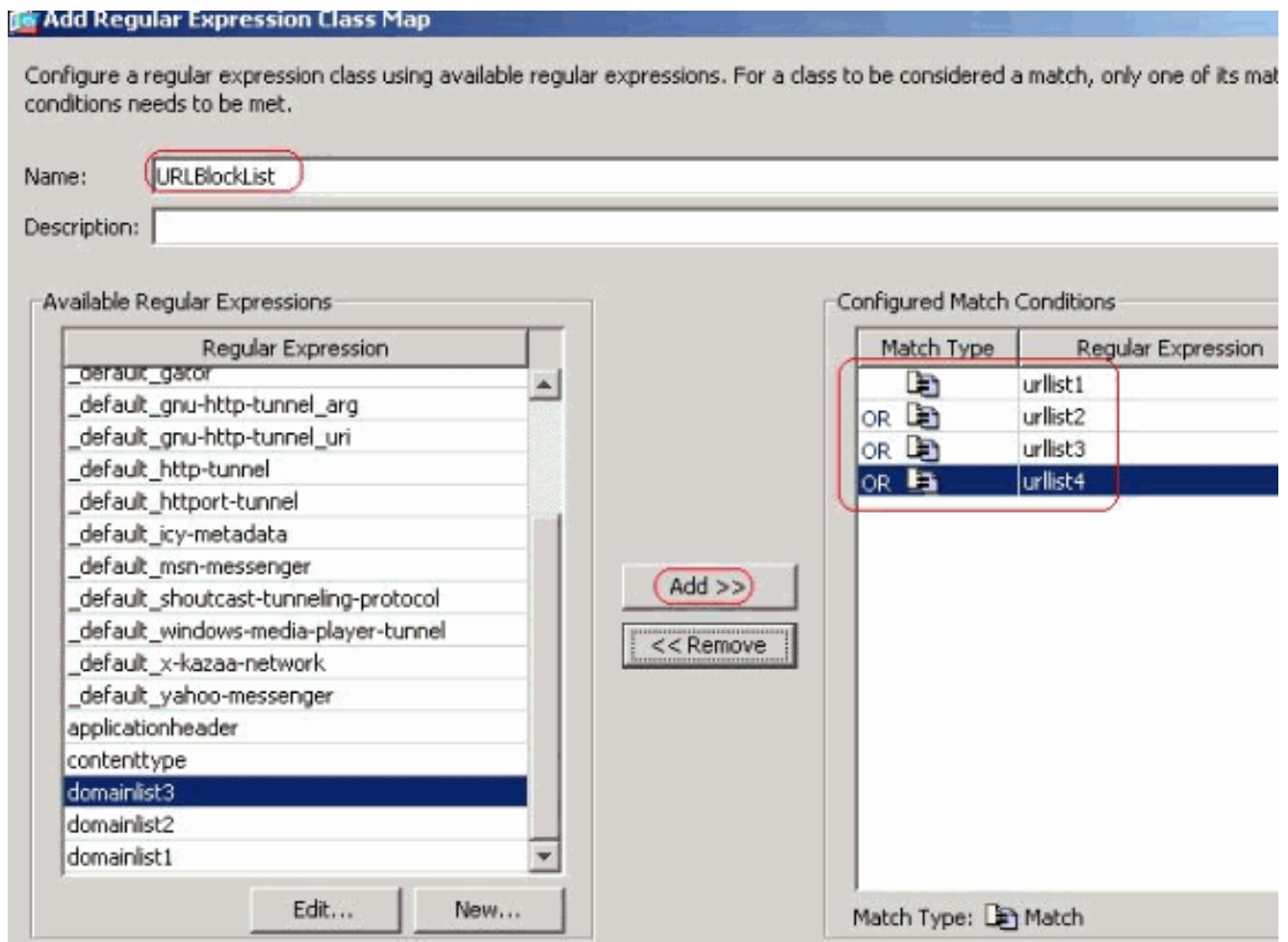
Configuración CLI

equivalente

2. Cree las clases de la expresión normal Elija la configuración > el Firewall > los objetos > las expresiones normales y el tecleo agrega bajo clases de la expresión normal de la lengüeta para crear las diversas clases como se muestra. Cree una clase **DomainBlockList** de la expresión normal para hacer juego las expresiones normales unas de los domainlist1, domainlist2 y domainlist3. Haga clic en OK.

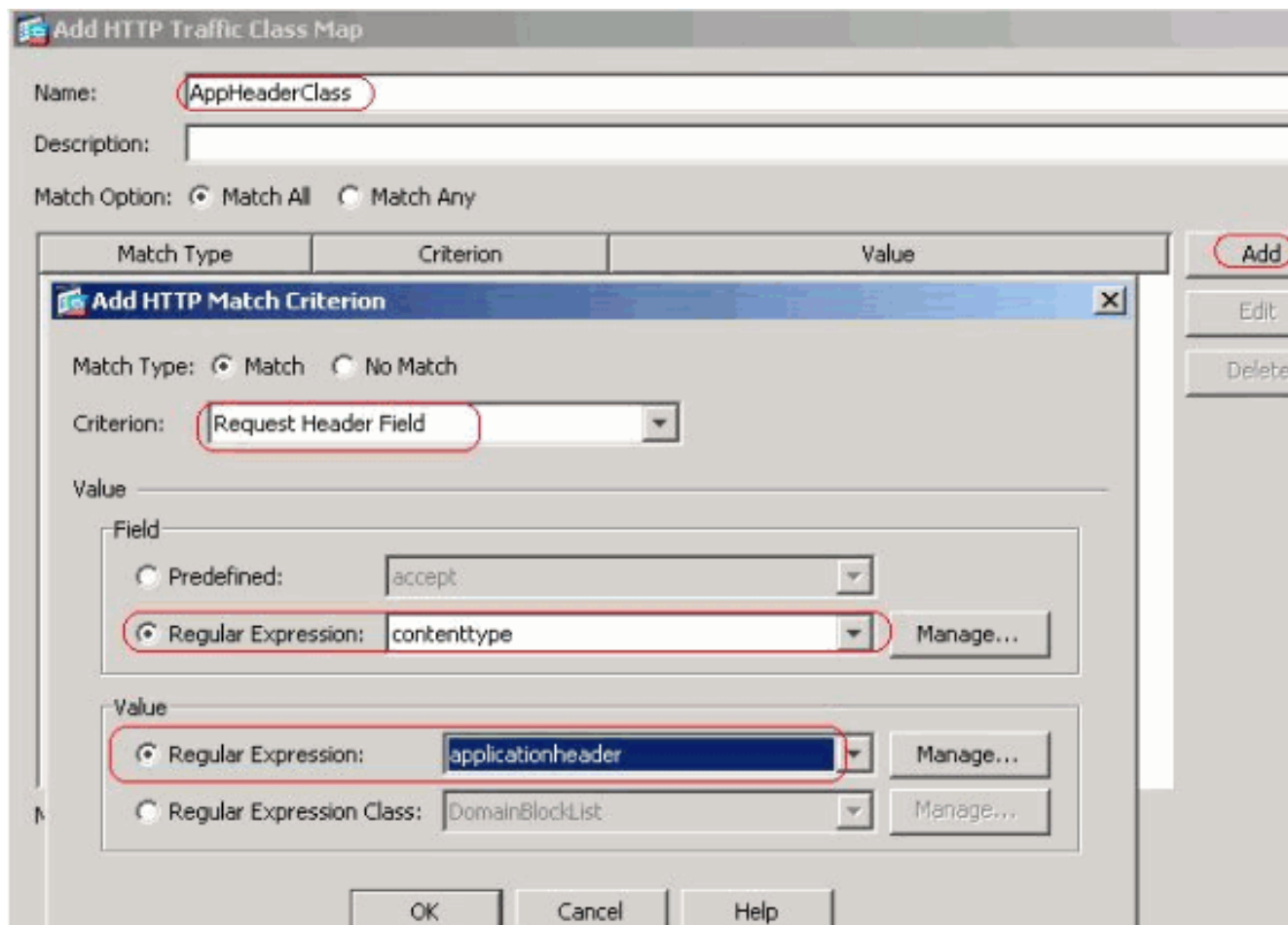


Cree una clase **URLBlockList** de la expresión normal para hacer juego las expresiones normales unas de los urlist1, urlist2, urlist3 y urlist4. Haga clic en OK.

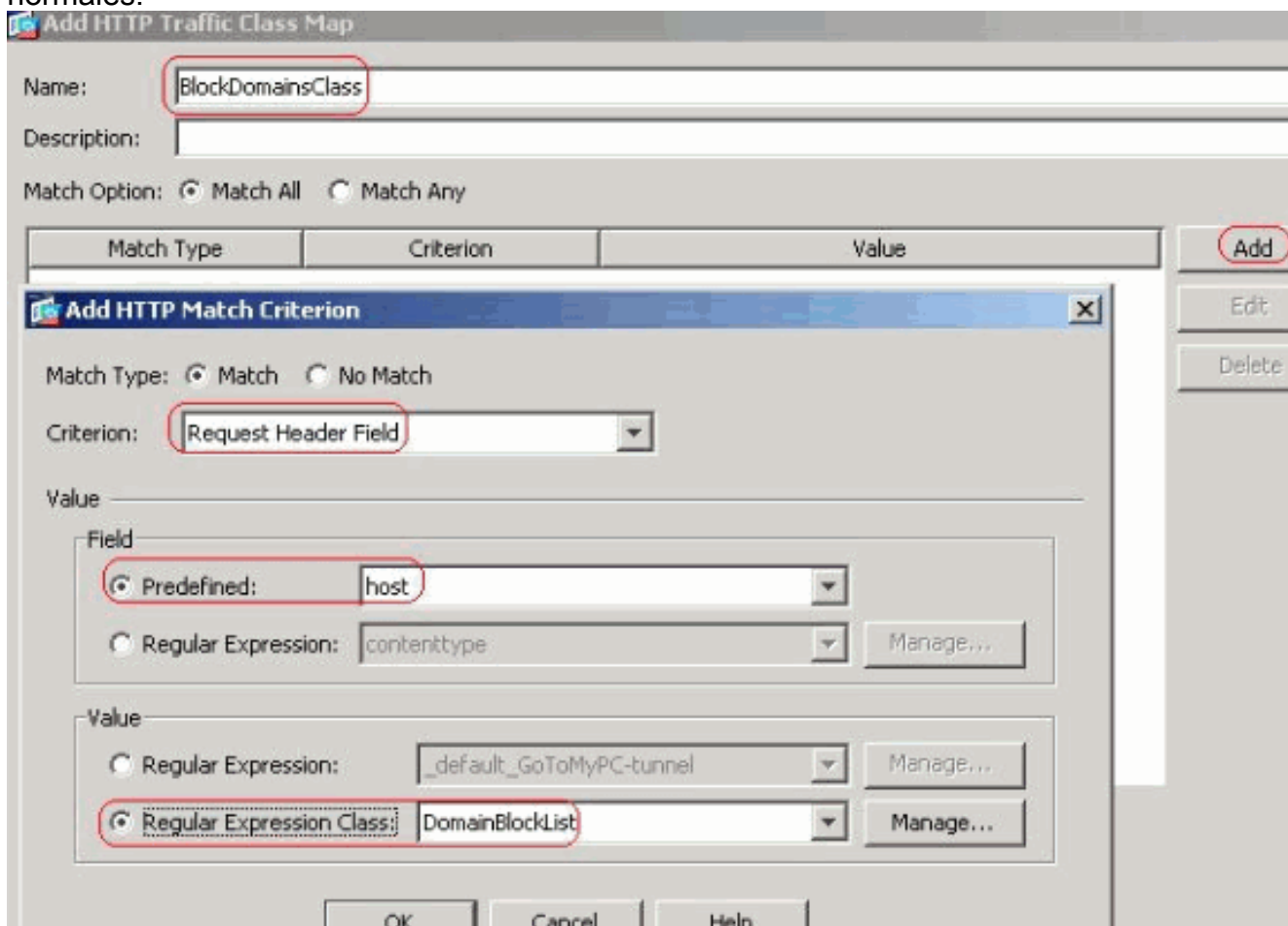


Configuración CLI equivalente

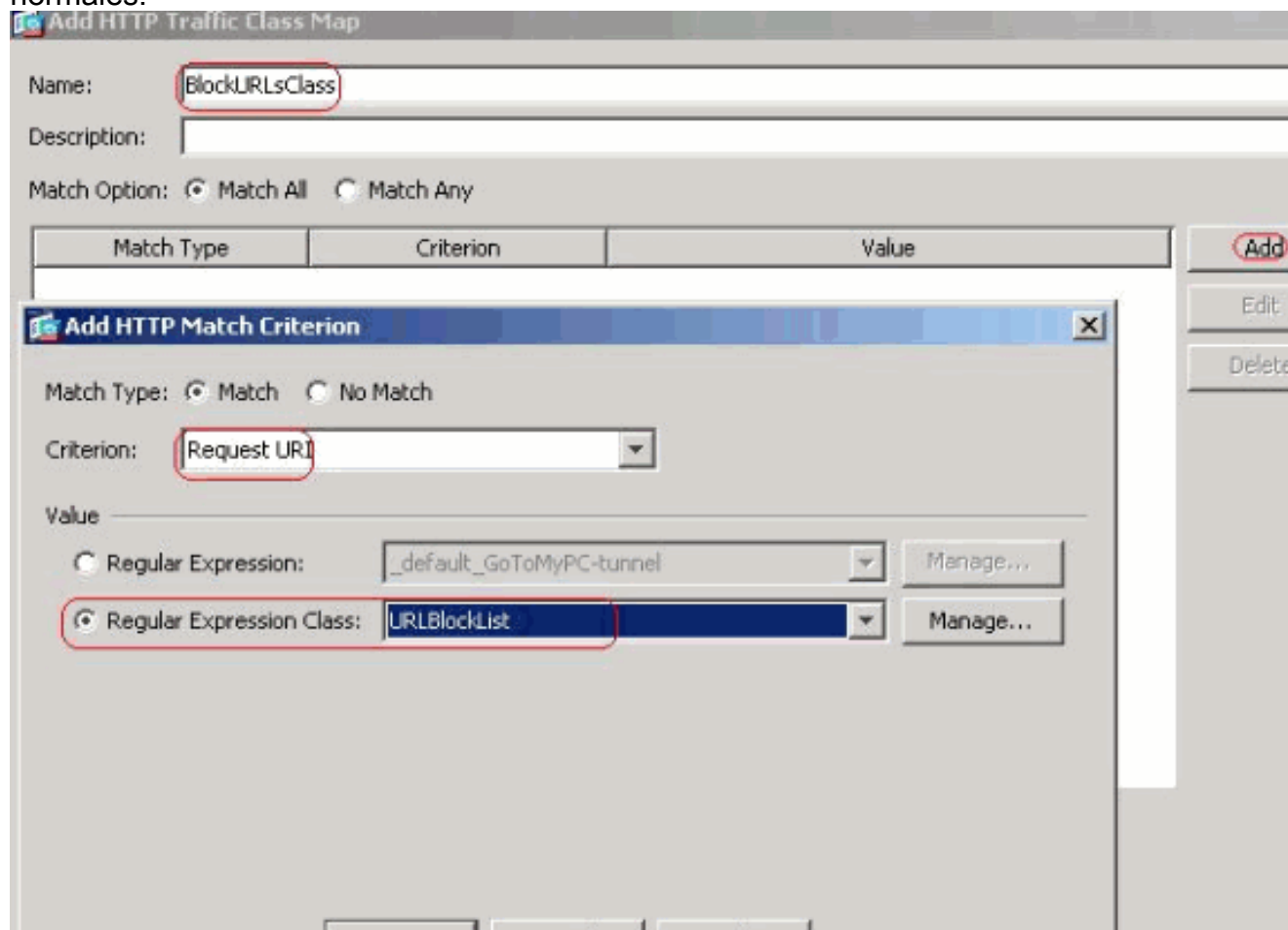
3. Examine el tráfico identificado con las correspondencias de la clase Elija la configuración > el Firewall > los objetos > la clase asocia > HTTP > Add para crear una correspondencia de la clase para examinar el tráfico HTTP identificado por las diversas expresiones normales como se muestra. Cree una correspondencia **AppHeaderClass** de la clase para hacer juego el encabezado de respuesta con las capturas de las expresiones normales.



Haga clic en OK (Aceptar). Cree una correspondencia **BlockDomainsClass** de la clase para hacer juego la encabezado de petición con las capturas de las expresiones normales.

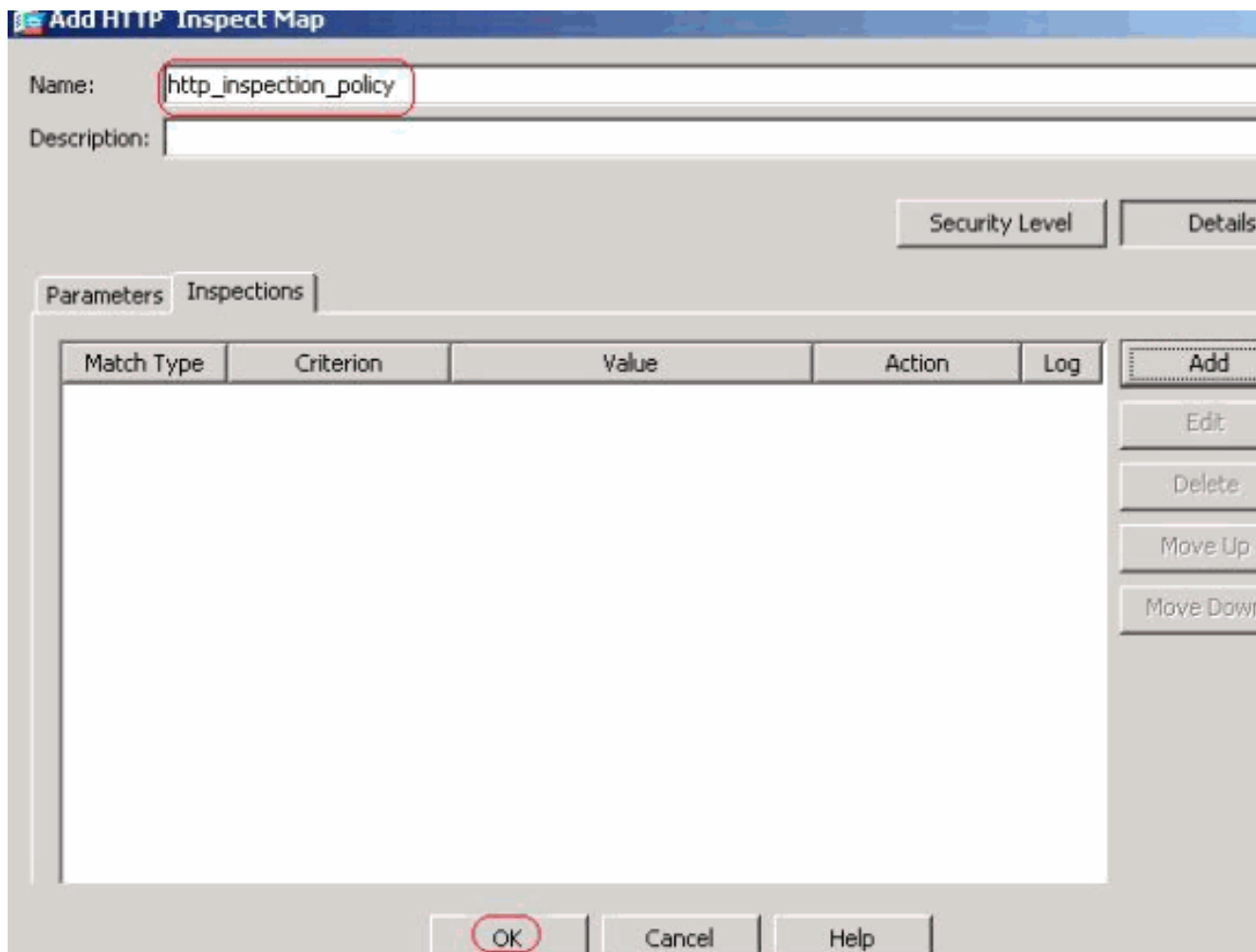


Haga clic en OK. Cree una correspondencia **BlockURLsClass** de la clase para hacer juego el uri de la petición con las capturas de las expresiones normales.

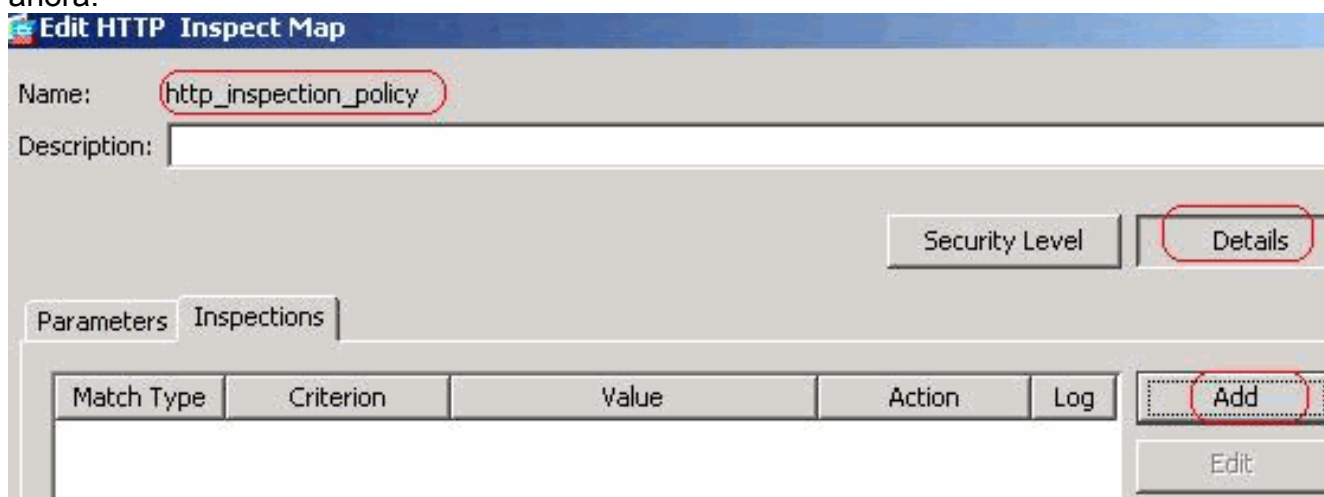


Haga clic en OK. Configuración CLI equivalente

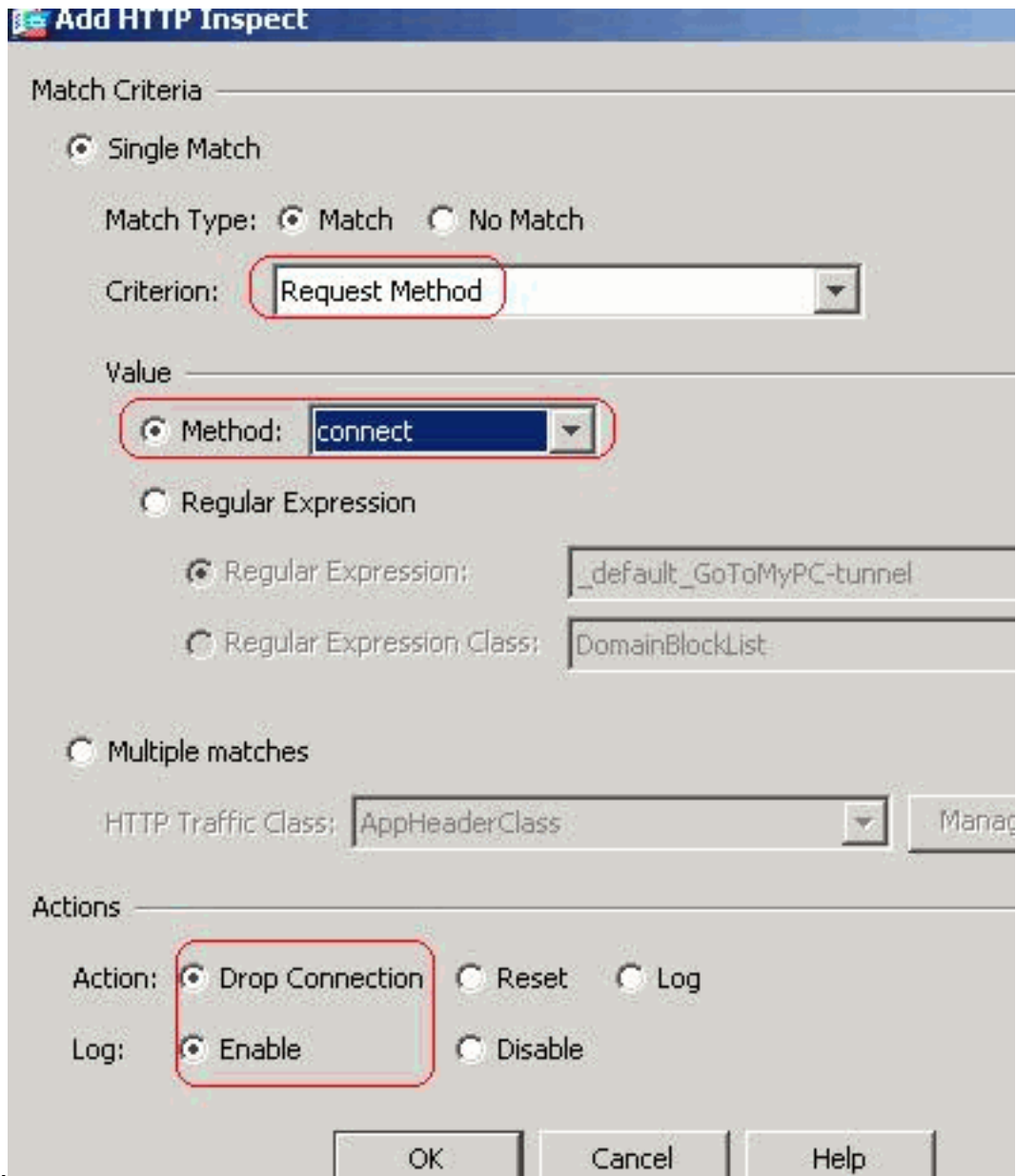
4. Fije las acciones para el tráfico correspondido con en la directiva del examen Elija la configuración > el Firewall > los objetos > examinan las correspondencias > el HTTP para crear un `http_inspection_policy` para fijar la acción para el tráfico correspondido con como se muestra. Haga clic en OK.



Elija la configuración > el Firewall > los objetos > examinan las correspondencias > el HTTP > el `http_inspection_policy` (tecleo doble) y hacen clic los detalles > Add para fijar las acciones para las diversas clases creadas hasta ahora.



Fije la acción como **conexión del descenso** y habilite el registro para el criterio como el método y valor de la petición como



conectan.

Haga clic en OK (Aceptar). Fije la acción como **conexión del descenso** y **habilite el registro** para la clase

Add HTTP Inspect

Match Criteria

Single Match

Match Type: Match No Match

Criterion: Request/Response Content Type Mismatch

Value: Not applicable.

Multiple matches

HTTP Traffic Class: AppHeaderClass

Actions

Action: Drop Connection Reset Log

Log: Enable Disable

OK Cancel Help

AppHeaderClass.

aga clic en OK. Fije la acción como **restauración** y **habilite el registro** para la clase

Add HTTP Inspect

Match Criteria

Single Match

Match Type: Match No Match

Criterion: Request/Response Content Type Mismatch

Value: Not applicable.

Multiple matches

HTTP Traffic Class: BlockDomainsClass

Actions

Action: Drop Connection Reset Log

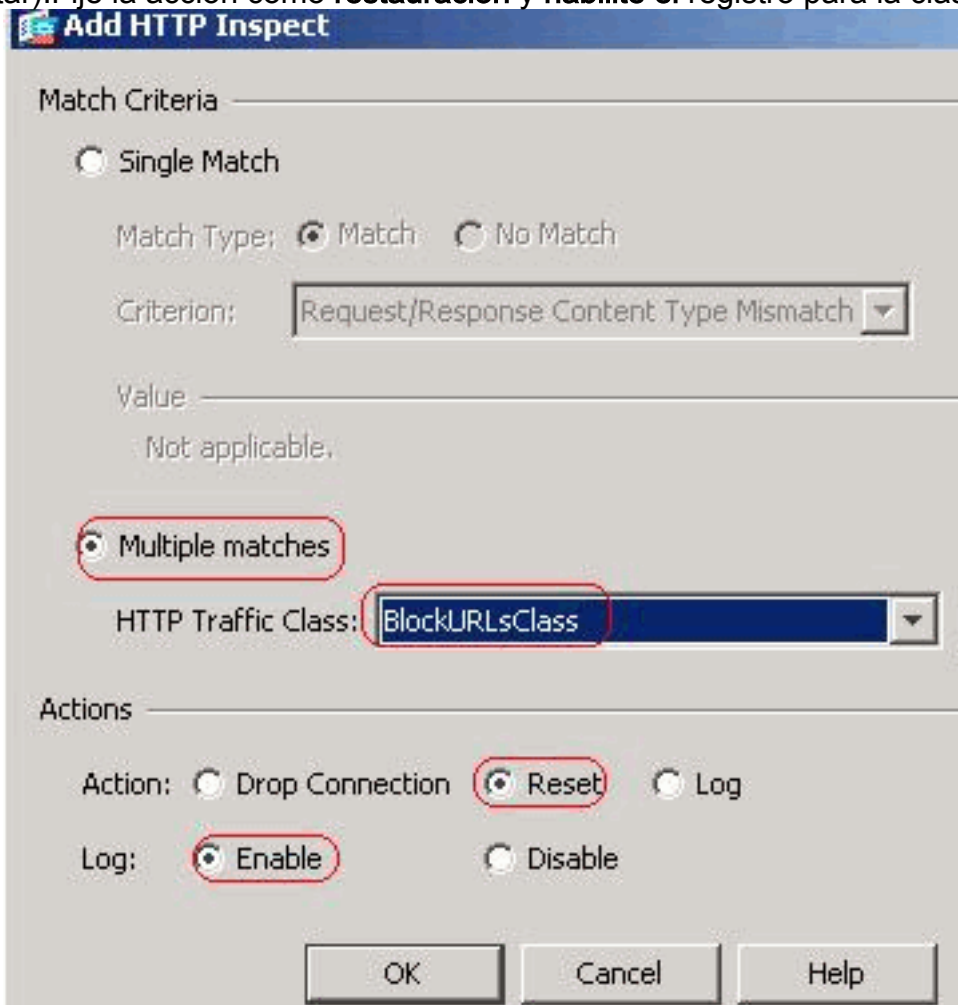
Log: Enable Disable

OK Cancel Help

BlockDomainsClass.

Haga

clic en OK (Aceptar). Fije la acción como **restauración** y **habilite el registro** para la clase

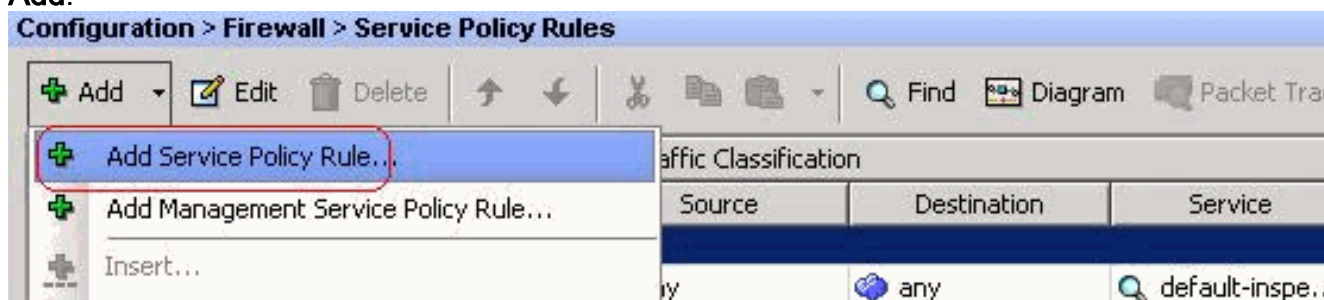


BlockURLsClass.

Haga clic en OK.

Haga clic en Apply (Aplicar). Configuración CLI equivalente

5. Aplique la directiva HTTP del examen a la interfaz. Elija la regla de la configuración > de la política de servicio de las reglas del Firewall > de la política de servicio > Add > Add.



Tráfico HTTP Elija el botón de radio de la **interfaz** con la interfaz interior del nombre del menú desplegable y de la directiva como dentro-**directiva**. Haga clic en Next (Siguiente).

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:

Cree una correspondencia de la clase **httptraffic** y marque el **IP Address de origen y de destino (aplicaciones ACL)**. Haga clic en **Next (Siguiente)**.

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.

Elija la fuente y el destino tan con el servicio como el TCP-UDP/el HTTP. Haga clic en Next (Siguiete).

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

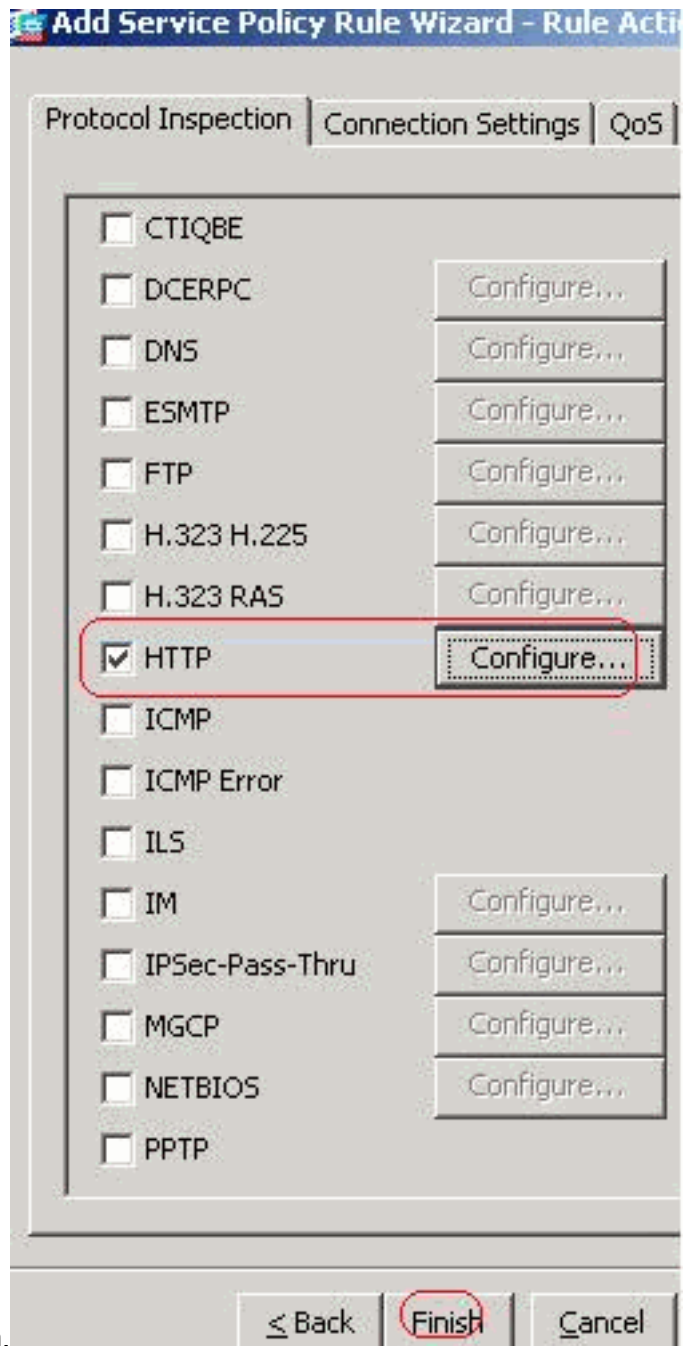
Enable Rule

Source Service: (TCP or UDP service only)

Time Range:

≤ Back **Next >**

Marque el botón de radio **HTTP** y haga clic la



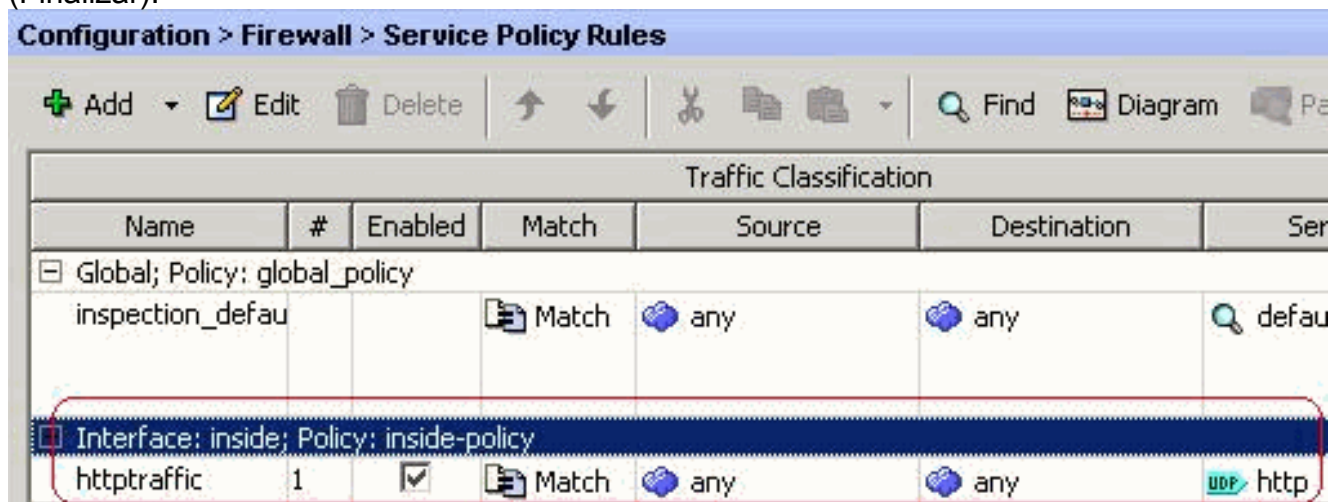
configuración.

seleccionan un HTTP examinan la correspondencia para saber si hay el control sobre el examen como se muestra. Haga clic en

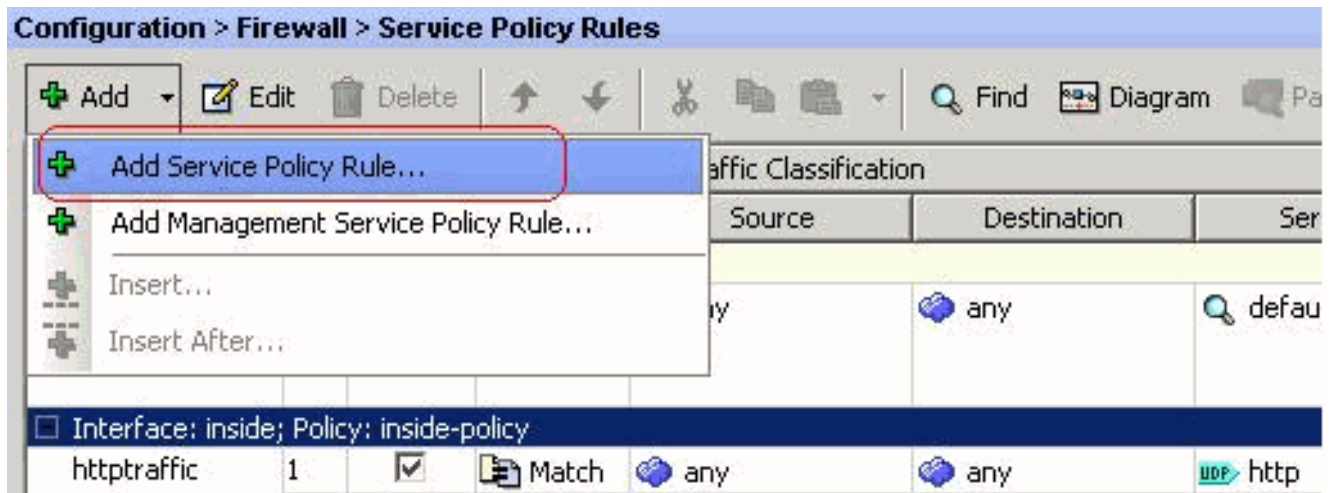
Marque el botón de radio



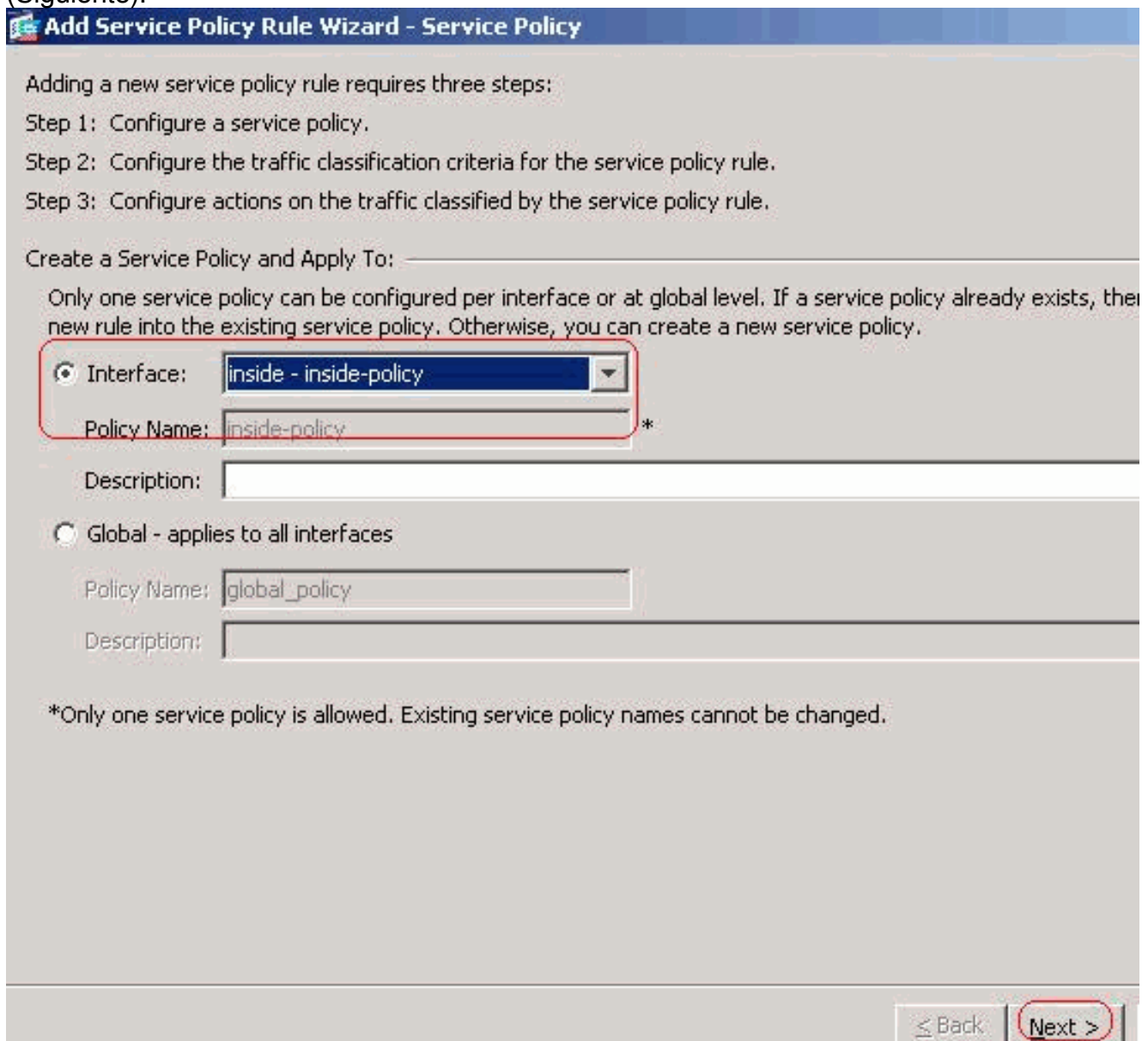
OK. Haga clic en Finish (Finalizar).



Tráfico del puerto 8080Una vez más elija **agregar > Add** la regla de la política de servicio.



Haga clic en Next (Siguiente).



Elija el botón de radio **agregar la regla a la clase de tráfico existente** y eligen **httptraffic** del menú desplegable. Haga clic en Next (Siguiente).

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.

Elija la fuente y el destino como ningunos con **tcp/8080**. Haga clic en Next (Siguiete).

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: ...

Haga clic en Finish
(Finalizar).

Add Service Policy Rule Wizard - Rule Actions

 The Rule Actions are applied to all the rules grouped in the Traffic Match.

Protocol Inspection | Connection Settings | QoS

- CTIQBE
- DCERPC Configure...
- DNS Configure...
- ESMTTP Configure...
- FTP Configure...
- H.323 H.225 Configure...
- H.323 RAS Configure...
- HTTP Configure... HTTP Inspect Map: http_inspection_policy
- ICMP
- ICMP Error
- ILS
- IM Configure...
- IPSec-Pass-Thru Configure...
- MGCP Configure...
- NETBIOS Configure...

< Back | **Finish** | Cancel

Configuration > Firewall > Service Policy Rules

+ Add | Edit | Delete | ↑ ↓ | ✂ | Diagram | Pa

Traffic Classification						
Name	#	Enabled	Match	Source	Destination	Serv
[-] Global; Policy: global_policy						
inspection_defau			Match	any	any	default
[-] Interface: inside; Policy: inside-policy						
httptraffic	1	<input checked="" type="checkbox"/>	Match	any	any	UDP http
	2	<input checked="" type="checkbox"/>	Match	any	any	TCP 8080

Haga clic en Apply (Aplicar). Configuración CLI equivalente

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **muestre el regex de los ejecutar-config** — Muestra las expresiones normales se han

```
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#
```

- **muestre el clase-mapa de los ejecutar-config** — Muestra las correspondencias de la clase se

```
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#
```

- **el tipo del directiva-mapa de los ejecutar-config de la demostración examina el HTTP** —

Muestra las correspondencias de políticas que examina el tráfico HTTP se ha 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#
```

- **muestre el directiva-mapa de los ejecutar-config** — Visualiza todas las configuraciones de correspondencia de políticas así como la configuración de correspondencia de políticas

```
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#
```

- **muestre la servicio-directiva de los ejecutar-config** — Visualiza todas las configuraciones de la política de servicio actualmente que se ejecutan

```
ciscoasa#show running-config service-policy
service-policy global_policy global service-policy inside-policy interface inside
```

- **muestre la lista de acceso de los ejecutar-config** — Visualiza la configuración de la lista de

```
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](#)

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Nota: Consulte [Información Importante sobre Comandos de Debug](#) antes de usar un comando debug.

- **HTTP del debug** — Muestra los mensajes del debug para el tráfico HTTP

Información Relacionada

- [Soporte del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500](#)
- [Soporte del Cisco Adaptive Security Device Manager \(ASDM\)](#)
- [Soporte del Cisco PIX 500 Series Security Appliances](#)
- [Cisco PIX Firewall Software](#)
- [Referencias de Comandos de Cisco Secure PIX Firewall](#)
- [Avisos de campos de productos de seguridad \(incluido PIX\)](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)