

# ASA/PIX 8.x: Permita/los sitios FTP del bloque usando las expresiones normales con el ejemplo de la configuración MPF

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[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 utiliza expresiones normales con el Marco de Políticas Modular (MPF) para bloquear o permitir ciertos sitios FTP por nombre de servidor.

## **[prerrequisitos](#)**

### **[Requisitos](#)**

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

### **[Componentes Utilizados](#)**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 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.

## 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 el tráfico de la capa 3 y de la capa 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 al tráfico de la capa 3 y de la capa 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 signos de interrogación (?) o lenguetas. ¿Por ejemplo, teclee el **[Ctrl+V] g d** para ingresar **d? g** en la configuración.

Para crear una expresión normal, utilice el comando del **regex**. Además, el comando del **regex** 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 MPF que utiliza una correspondencia de políticas del examen. Refiera al [comando inspect del tipo del directiva-mapa](#) 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, <b>d.g</b> 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, <b>d(o)el</b> perro de las coincidencias <b>a) g</b> y el dag, pero <b>hacen</b> las coincidencias <b>AG</b> 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, <b>ab(xy){3}z</b> hace juego el abxyxyxyz.
	Alternancia	Hace juego cualquier expresión que se separa. Por ejemplo, <b>perro el gato</b> 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, <b>lo?</b> el SE hace juego el lse o pierde. <b>Nota:</b> Usted debe ingresar <b>Ctrl+V</b> 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 <b>lo*se</b> hace juego el lse, pierde, flexible, y así sucesivamente.
{x}	Relance el cuantificador	Relance exactamente los tiempos x. Por ejemplo, <b>ab(xy){3}z</b> hace juego el abxyxyxyz.
{x,}	Cuantificador mínimo de la repetición	Relance por lo menos los tiempos x. Por ejemplo, <b>ab(xy){2,}z</b> hace juego el abxyxyz, abxyxyxyz, y así sucesivamente.
[abc]	Clase de carácter	Hace juego cualquier carácter en los corchetes. Por ejemplo, el <b>[abc]</b> 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 <b>[^abc]</b> hace juego cualquier carácter con excepción de a, b, o el <b>[^A-Z]</b> 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. <b>el [a-z]</b> hace juego cualquier letra minúscula. Usted puede mezclar los caracteres y los rangos: <b>el [abcq-z]</b> hace juego a, b, c, q, r, s, t, u, v, w, x, y, z, y así que hace el <b>[a-cq-z]</b> . El carácter de la rociada (-) es literal solamente si es el último o el primer carácter dentro de los corchetes: <b>[abc-]</b> o <b>[-abc]</b> .
""	Comillas	Cotos que arrastran o que llevan los espacios en la cadena. Por ejemplo, la <b>"prueba"</b> preserva el espacio principal cuando busca una coincidencia.
^	Signo de intercalación	Especifica el principio de una línea.
\	Carácter de escape	Cuando está utilizado con un metacaracter, hace juego un carácter literal. Por ejemplo, <b>\ [</b> hace juego los corchetes izquierdos.
cha r	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.

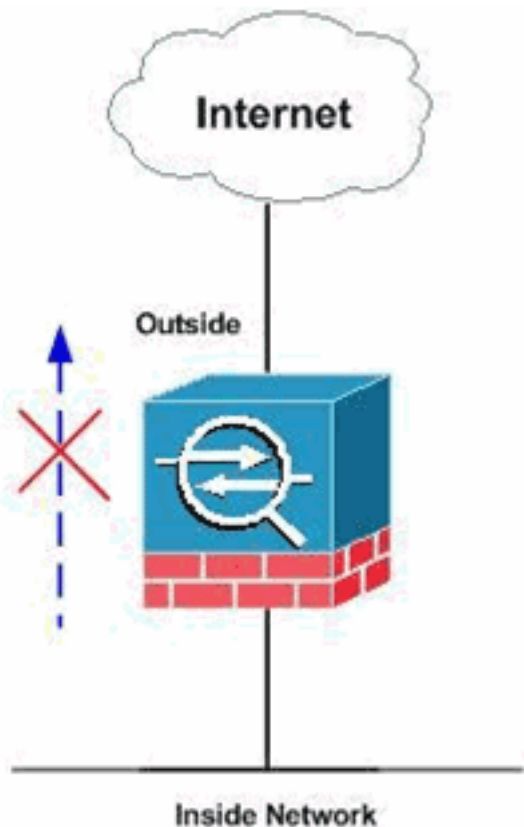
## [Configurar](#)

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

**Nota:** Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

## [Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:



**Nota:** Los sitios FTP seleccionados se permiten o se bloquean usando las expresiones normales.

## 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 run : Saved : ASA Version 8.0(4) !
hostname ciscoasa domain-name cisco.com enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted names ! interface GigabitEthernet0/0 nameif
outside security-level 0 ip address 10.66.79.86
255.255.255.224 ! interface GigabitEthernet0/1 nameif
inside security-level 100 ip address 10.238.26.129
255.255.255.248 ! interface Management0/0 shutdown no
nameif no security-level no ip address !!-- Write
regular expression (regex) to match the FTP site you
want !!-- to access. NOTE: The regular expression
written below must match !!-- the response 220 received
from the server. This can be different !!-- than the URL
entered into the browser. For example, !!-- FTP
Response: 220 q1u0103c.austin.hp.com regex FTP SITE1
"([0-9A-Za-z])*[Hh][Pp]\.[Cc][Oo][Mm]" regex FTP SITE2
"([0-9A-Za-z])* CISCO SYSTEMS ([0-9A-Za-z])*" !!-- NOTE:
The regular expression will be checked against every
line !!-- in the Response 220 statement (which means if
the FTP server !!-- responds with multiple lines, the
```

```

connection will be denied if !--- there is no match on
any one line). boot system disk0:/asa804-k8.bin ftp mode
passive pager lines 24 logging enable logging timestamp
logging buffered debugging mtu outside 1500 mtu inside
1500 no failover icmp unreachable rate-limit 1 burst-
size 1 asdm image disk0:/asdm-61557.bin no asdm history
enable arp timeout 14400 global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0
0.0.0.0 10.66.79.65 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 mqcpc
0:05:00 mqcpc-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 sip-provisional-media 0:02:00 uauth 0:05:00
absolute dynamic-access-policy-record DfltAccessPolicy
http server enable http 0.0.0.0 0.0.0.0 inside http
0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-
server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart telnet timeout
5 ssh scopy enable ssh timeout 5 console timeout 0
management-access inside threat-detection basic-threat
threat-detection statistics access-list no threat-
detection statistics tcp-intercept class-map type regex
match-any FTP SITES match regex FTP SITE1 match regex
FTP SITE2 ! Class map created in order to match the
server names ! of FTP sites to be blocked by regex.
class-map type inspect ftp match-all FTP class map match
not server regex class FTP SITES ! Write an FTP inspect
class map and match based on server !--- names, user
name, FTP commands, and so on. Note that this !---
example allows the sites specified with the regex
command !--- since it uses the match not command. If you
need to block !--- specific FTP sites, use the match
command without the not option. class-map
inspection default match default-inspection-traffic
policy-map type inspect dns preset dns map parameters
message-length maximum 512 policy-map type inspect ftp
FTP INSPECT POLICY parameters class FTP class map reset
log ! Policy map created in order to define the actions
!--- such as drop, reset, or log. policy-map
global policy class inspection default inspect dns
preset dns map 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 inspect icmp inspect ftp
strict FTP INSPECT POLICY !--- The FTP inspection is
specified with strict option !--- followed by the name
of policy. service-policy global policy global prompt
hostname context
Cryptochecksum:40cefb1189e8c9492ed7129c7577c477 : end

```

## Configuración 8.x ASA con el ASDM 6.x

Complete estos pasos para configurar las expresiones normales y aplicarlas al MPF para bloquear los sitios FTP específicos:

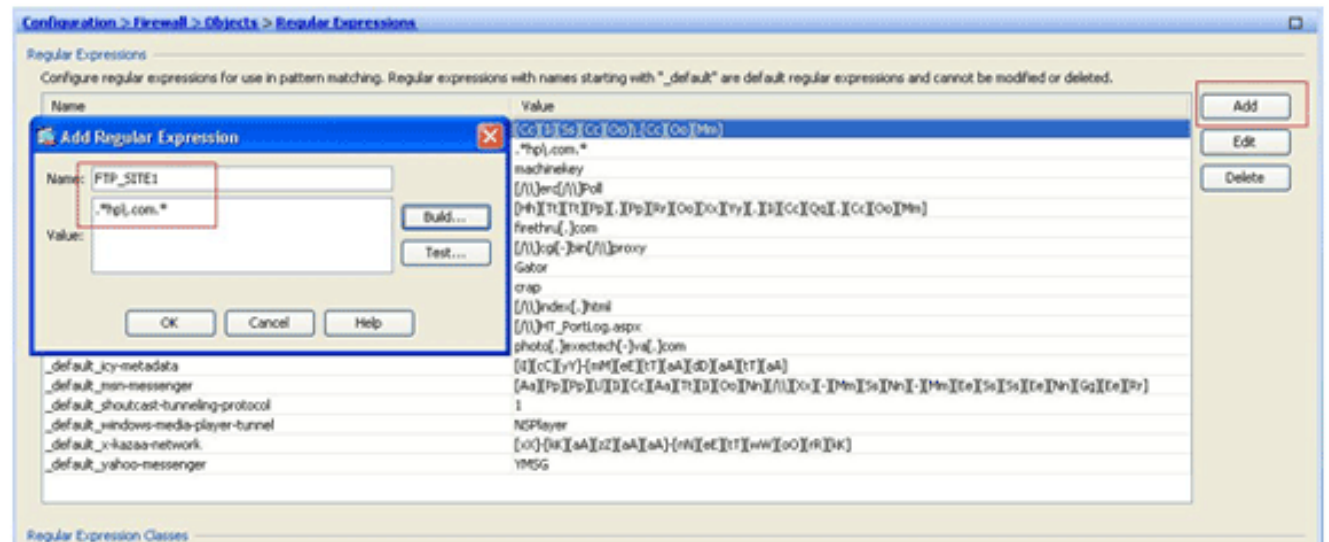
1. **Determine el nombre del servidor FTP.** El motor del examen FTP puede proporcionar el examen usando diverso criterio, tal como comando, nombre del archivo, tipo de archivo, servidor, y Nombre de usuario. Este procedimiento utiliza el servidor como criterio. El motor del examen FTP utiliza la respuesta del servidor 220 enviada por el sitio FTP como el valor

del servidor. Este valor puede ser diferente que el Domain Name usado por el sitio. Este ejemplo utiliza Wireshark para capturar los paquetes FTP al sitio que se examina para conseguir el valor de la respuesta 220 para utilizado en nuestra expresión normal en el paso 2.

Time	Delta	Source	Destination	Protocol	Info
256	17.172963	17.17.64.104.205.248	15.192.45.21	TCP	npss > ftp [SYN] Seq=0 win=64512 Len=0 MSS=1260
258	17.387525	0.214 15.192.45.21	64.104.205.248	TCP	ftp > npss [SYN, ACK] Seq=0 Ack=1 win=32768 Len=0
259	17.387579	0.000 64.104.205.248	15.192.45.21	TCP	npss > ftp [ACK] Seq=1 Ack=1 win=65520 Len=0
261	17.731871	0.344 15.192.45.21	64.104.205.248	FTP	Response: 220 q5u0081c.atlanta.hp.com FTP server (

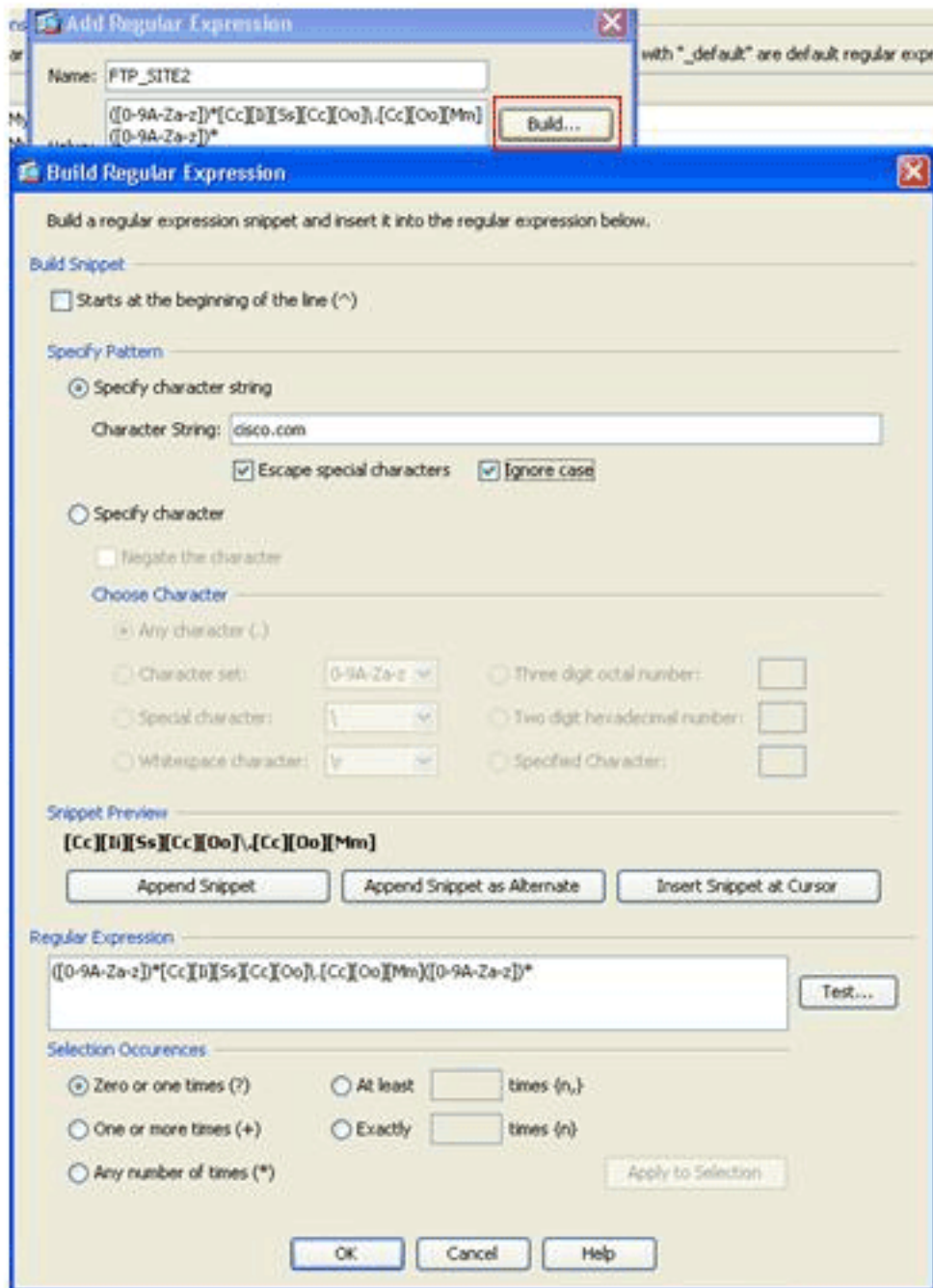
De acuerdo con la captura el valor de la respuesta 220 para ftp://hp.com es (por ejemplo) *q5u0081c.atlanta.hp.com*.

2. Cree las expresiones normales. Elija la configuración > el Firewall > los objetos > las expresiones normales, y el tecleo **agrega** bajo lengüeta de la expresión normal para crear las expresiones normales según lo descrito en este procedimiento: Cree una expresión normal, *FTP\_SITE1*, para hacer juego la respuesta 220 (como se ve en la captura de paquetes en Wireshark o cualquier otra herramienta usada) recibida del ftp site (por ejemplo, “. \* caballos de fuerza \ .com.\*”), y **AUTORIZACIÓN** del tecleo.



**Nota:** Usted puede hacer clic la **estructura** para la ayuda en cómo crear expresiones normales más



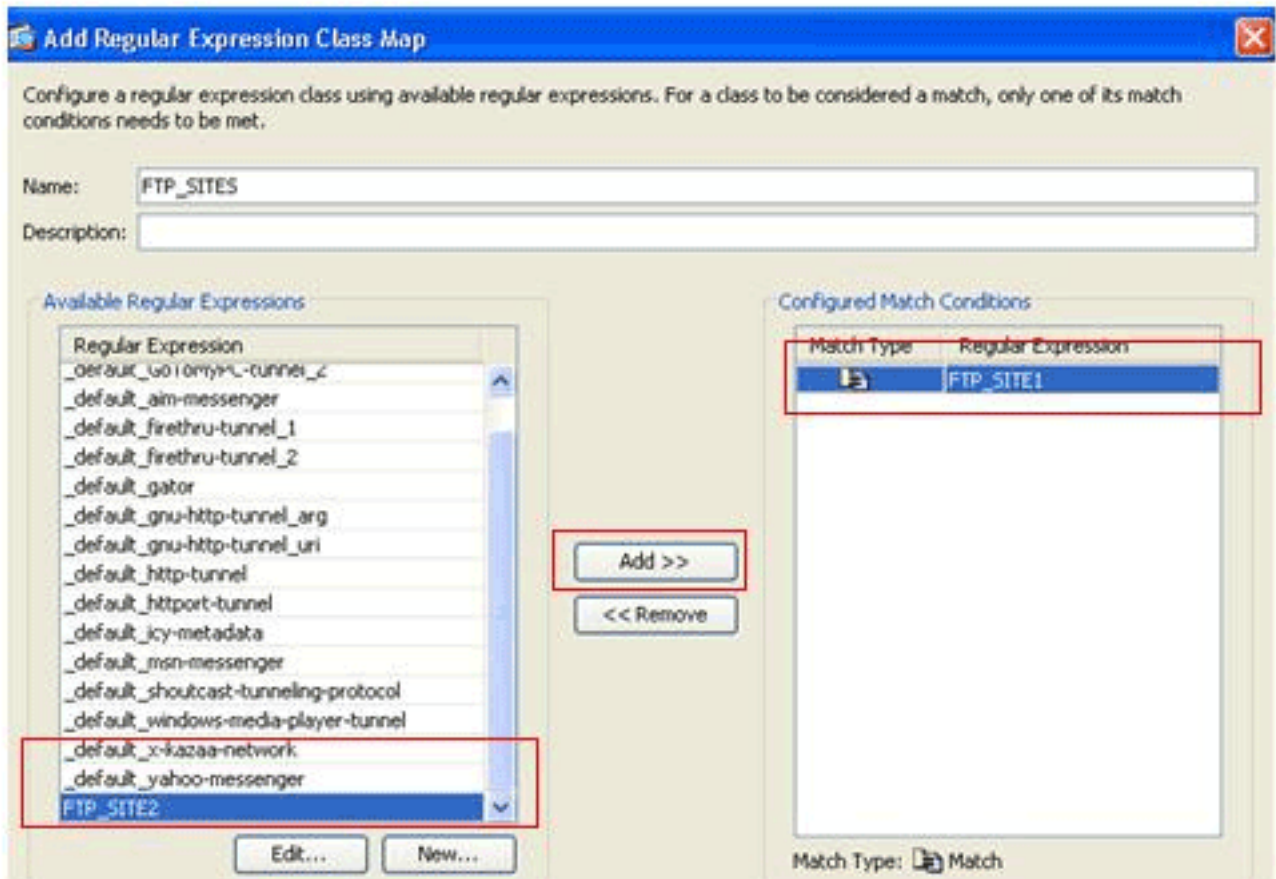


avanzadas.

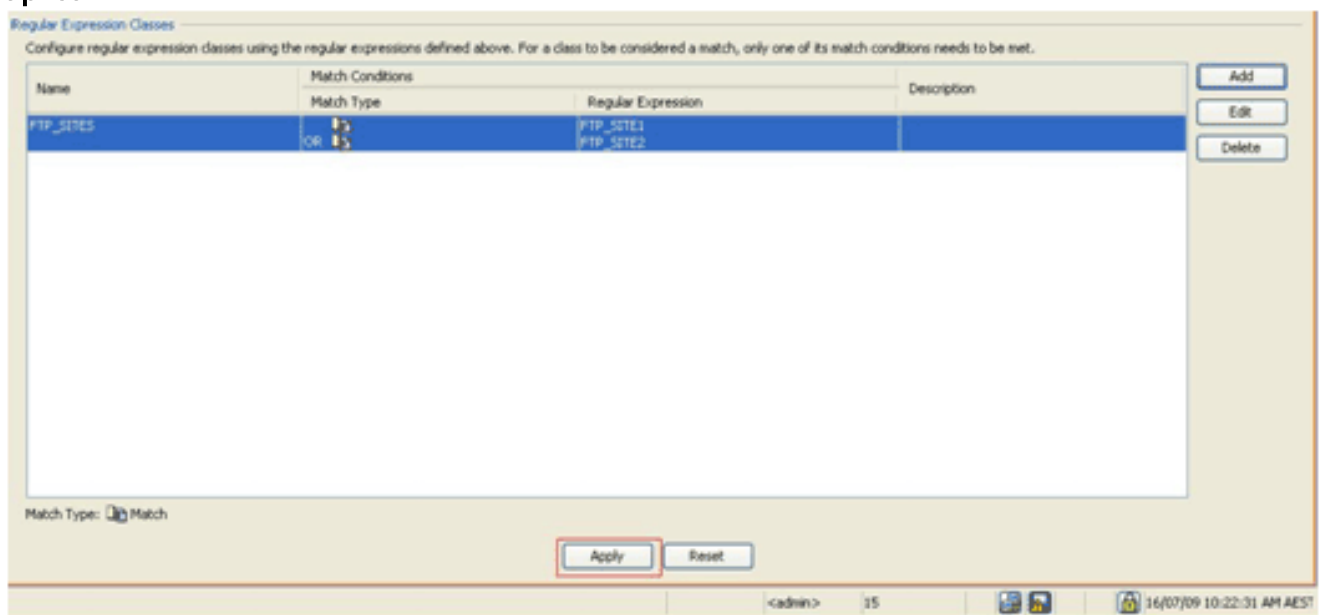
Una vez

que se crea la expresión normal, el teclado se aplica.

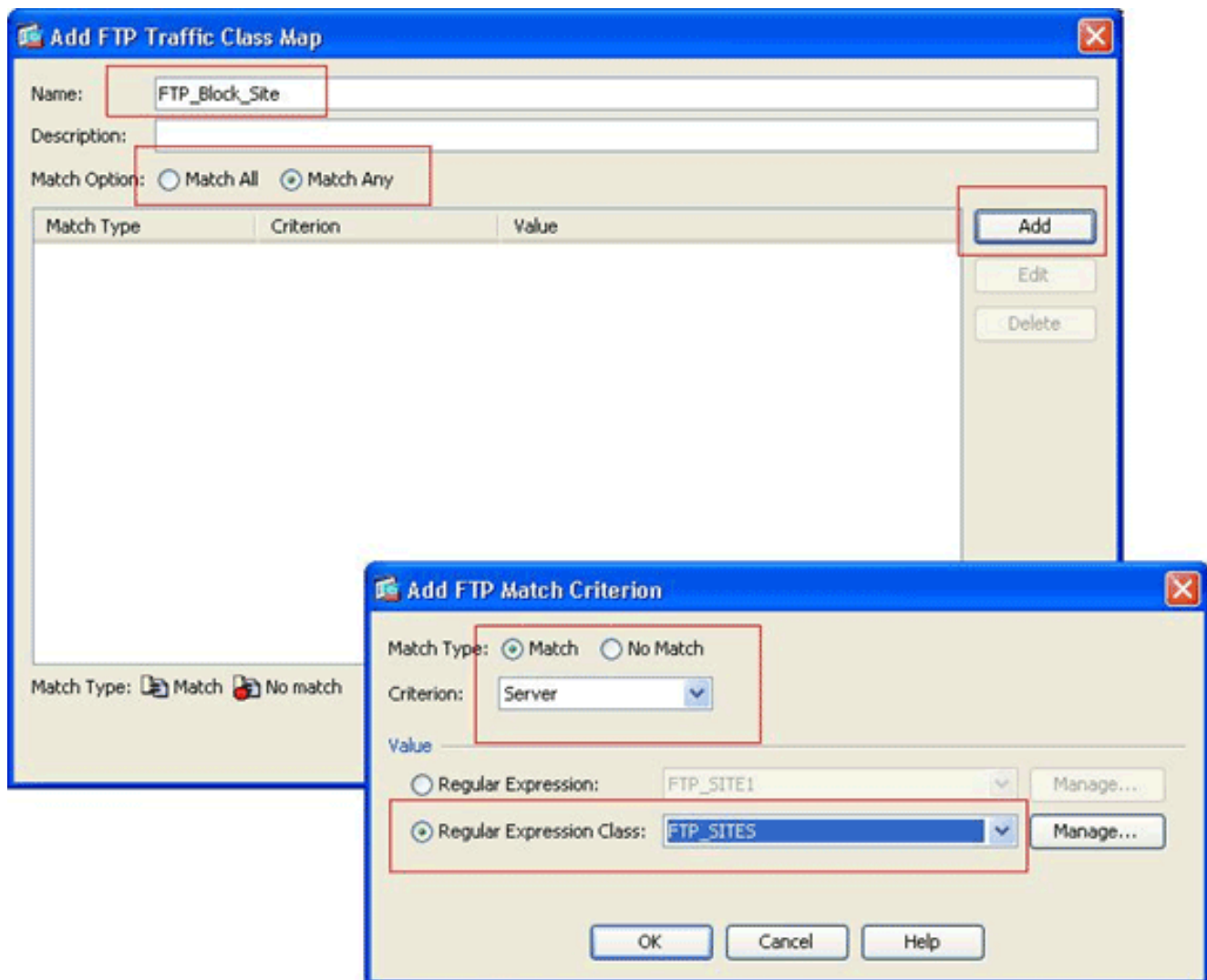
3. Cree las clases de la expresión normal. Elija la configuración > el Firewall > los objetos > las expresiones normales, y el teclado agrega bajo sección de las clases de la expresión normal para crear la clase según lo descrito en este procedimiento: Cree una clase de la expresión normal, *FTP\_SITES*, para hacer juego las expresiones normales unas de los *FTP\_SITE1* y *FTP\_SITE2*, y haga clic la AUTORIZACIÓN.



na vez que se crea la correspondencia de la clase, el teclado se aplica.

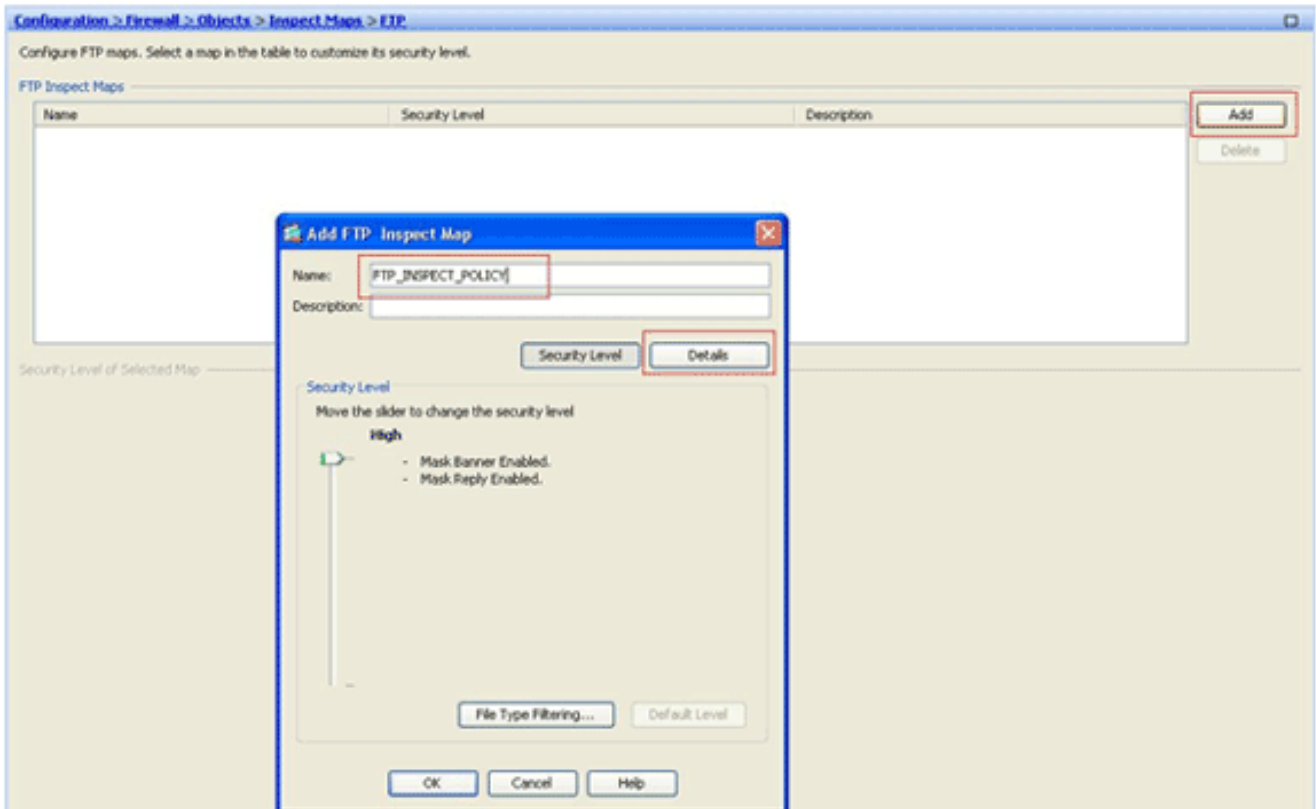


- Examine el tráfico identificado con las correspondencias de la clase. Elija la configuración > el Firewall > los objetos > la clase asocia > FTP > agregan, hacen clic con el botón derecho del ratón, y eligen **agregan** para crear una correspondencia de la clase para examinar el tráfico FTP identificado por las diversas expresiones normales según lo descrito en este procedimiento: Cree una correspondencia de la clase, *FTP\_Block\_Site*, para hacer juego la respuesta 220 FTP con las expresiones normales que usted creó.

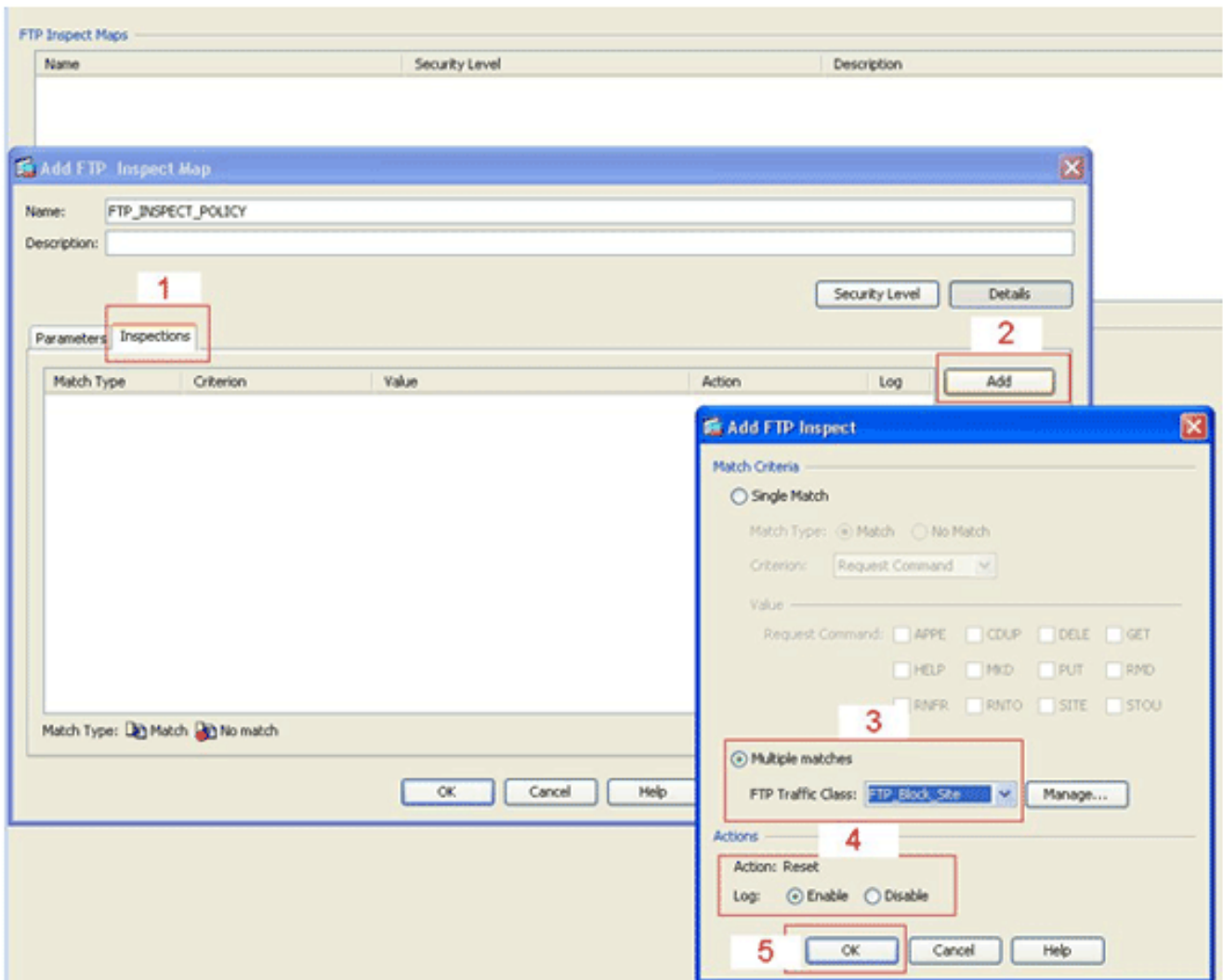


Si usted quiere excluir los sitios especificados en la expresión normal, no haga clic el **ningún** botón de radio de la **coincidencia**. En la sección del valor, elija una expresión normal o una clase de la expresión normal. Para este procedimiento, elija la clase que fue creada anterior. Haga clic en Apply (Aplicar).

5. Fije las acciones para el tráfico correspondido con en la directiva del examen. Elija la configuración > el Firewall > los objetos > examinan las correspondencias > el FTP > agregan para crear una directiva del examen, y fijan la acción para el tráfico correspondido con como sea necesario.

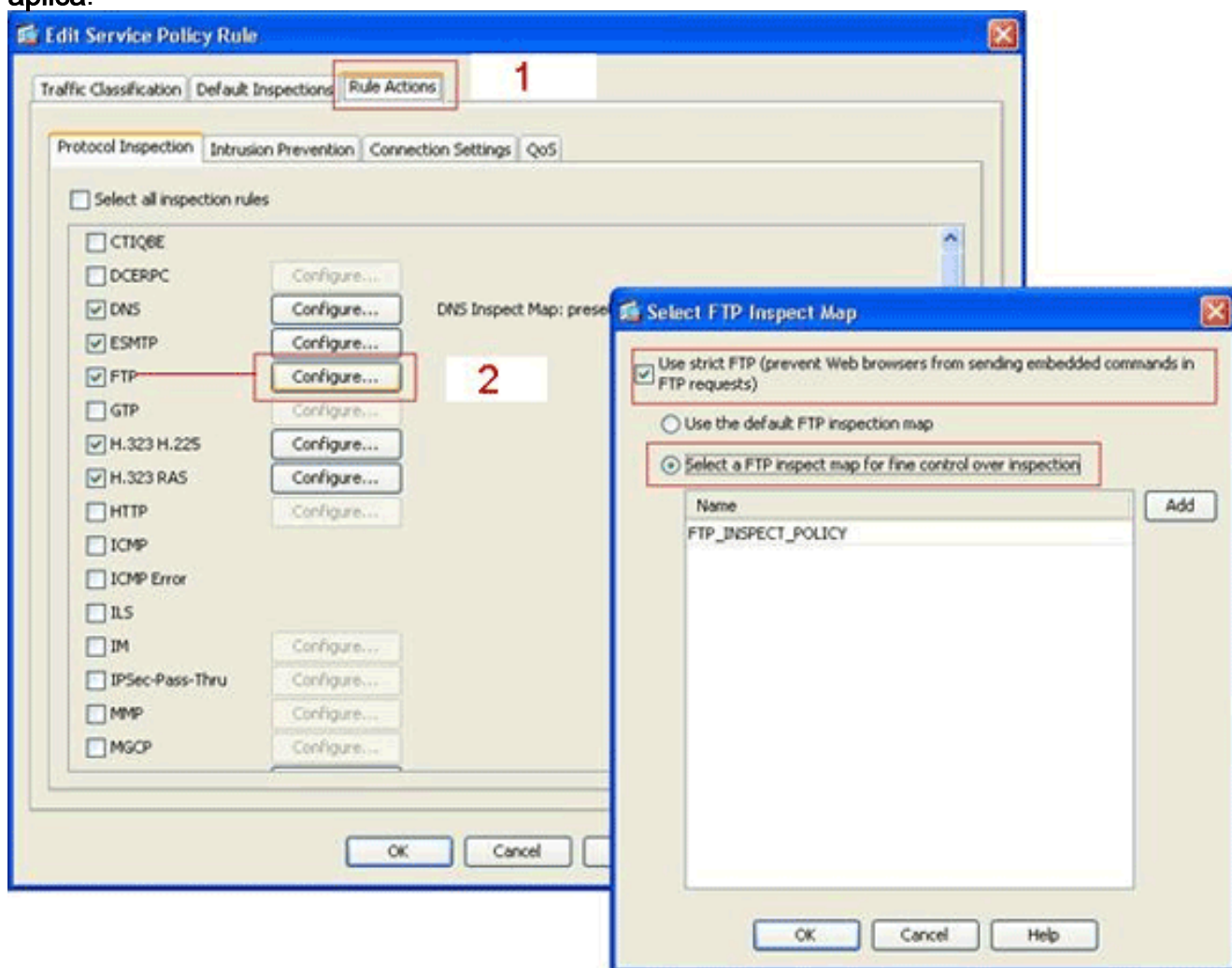


Ingrese el nombre y una descripción para la directiva del examen. (Por ejemplo, *FTP\_INSPECT\_POLICY*.) Haga clic en **Details**.



Haga clic los **exámenes** cuadro (1)Haga clic en Add (Agregar). (2)Haga clic el botón de radio **múltiple de las coincidencias**, y elija la clase de tráfico de la lista desplegable. (3)Elija la acción deseada de la restauración para habilitar o para inhabilitar. Este ejemplo habilita la restauración de la conexión FTP para todos los sitios FTP *que no corresponden con* nuestros sitios especificados. (4)El Haga Click en OK, **AUTORIZACIÓN** del tecleo otra vez, y entonces hace clic **se aplica**. (5)

6. **Aplice la directiva del examen FTP a la lista global del examen.** Elija las **reglas de la configuración > del Firewall > de la política de servicio.** En el lado derecho, seleccione la directiva del **inspection\_default**, y el tecleo **edita**. Bajo acciones de la regla tabule (1), hacen clic el **botón Configure Button** para el FTP. (2)En el FTP selecto examine el cuadro de diálogo del mapa, marque la casilla de verificación **estricta del uso FTP**, y después haga clic el **FTP examinan la correspondencia para saber si hay el control fino sobre el botón de radio del examen.** La nueva directiva del examen FTP, **FTP\_INSPECT\_POLICY**, debe ser visible en la lista. El Haga Click en OK, **AUTORIZACIÓN** del tecleo otra vez, y entonces hace clic **se aplica**.



## Verificación

Use esta sección para confirmar que su configuración funciona 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 configurado que.  

```
ciscoasa#show running-config regex regex FTP_SITE1 "[Cc][Ii][Ss][Cc][Oo]\.[Cc][Oo][Mm]" regex FTP_SITE2 ".*hp\.com.*"
```
- **muestre el class-map de los ejecutar-config** — Muestra las correspondencias de la clase se han configurado que.  

```
ciscoasa#show running-config class-map class-map type regex match-any FTP_SITES match regex FTP_SITE1 match regex FTP_SITE2 class-map type inspect ftp match-all FTP_Block_Site match not server regex class FTP_SITES class-map inspection_default match default-inspection-traffic !
```
- **el tipo del directiva-mapa de los ejecutar-config de la demostración examina el HTTP** — Muestra las correspondencias de políticas que examinan el tráfico HTTP se ha configurado que.  

```
ciscoasa#show running-config policy-map type inspect ftp ! policy-map type inspect ftp FTP_INSPECT_POLICY parameters mask-banner mask-syst-reply class FTP_Block_Site reset log !
```
- **Muestre el directiva-mapa de los ejecutar-config** — Visualiza todas las configuraciones de correspondencia de políticas, así como la configuración de asignación de la política predeterminada.  

```
ciscoasa#show running-config policy-map ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map type inspect ftp FTP_INSPECT_POLICY parameters mask-banner mask-syst-reply class FTP_Block_Site reset log policy-map global_policy class inspection_default inspect dns preset_dns_map 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 inspect ftp strict FTP_INSPECT_POLICY !
```
- **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
```

## Troubleshooting

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

Usted puede utilizar el **comando service-policy de la demostración** para verificar que el motor del examen examina el tráfico y correctamente los permite o cae.

```
ciscoasa#show service-policy Global policy: Service-policy: global_policy Class-map: inspection_default Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0 Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0 Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0 Inspect: netbios, packet 0, drop 0, reset-drop 0 Inspect: rsh, packet 0, drop 0, reset-drop 0 Inspect: rtsp, packet 0, drop 0, reset-drop 0 Inspect: skinny , packet 0, drop 0, reset-drop 0 Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0 Inspect: sqlnet, packet 0, drop 0, reset-drop 0 Inspect: sunrpc, packet 0, drop 0, reset-drop 0 Inspect: tftp, packet 0, drop 0, reset-drop 0 Inspect: sip , packet 0, drop 0, reset-drop 0 Inspect: xdmcp, packet 0, drop 0, reset-drop 0 Inspect: ftp strict FTP_INSPECT_POLICY, packet 40, drop 0, reset-drop 2
```

## Información Relacionada

- [ASA/PIX 8.x: Ciertos sitios web del bloque \(URL\) usando las expresiones normales con el ejemplo de la configuración MPF](#)
- [PIX/ASA 7.x y posteriores: Bloquee el tráfico del peer a peer \(P2P\) y de la Mensajería inmediata \(IM\) usando el ejemplo de la configuración MPF](#)
- [PIX/ASA 7.x: El permiso FTP/TFTP mantiene el ejemplo de configuración](#)
- [Aplicación del examen del Application Layer Protocol](#)
- [Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 – Soporte](#)

- [Cisco Adaptive Security Device Manager \(ASDM\)](#)
- [Dispositivos de seguridad Cisco PIX de la serie 500 – Soporte](#)
- [Software Cisco PIX Firewall – Soporte](#)
- [Referencias de comandos del Software Cisco PIX Firewall](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)