ASA/PIX 8.x: Reserve/locais do bloco FTP usando expressões regulares com exemplo da configuração MPF

Índice

Introdução

Este documento descreve como configurar os dispositivos ASA/PIX 8.x do Cisco Security que usa expressões regulares com estrutura de política modular (MPF) a fim obstruir ou permitir determinados locais FTP pelo nome do servidor.

Pré-requisitos

Requisitos

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

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- 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.

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 o tráfego da camada 3 e da camada 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 ao tráfego da camada 3 e da camada 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 pontos de interrogação (?) ou abas. Por exemplo, datilografe o **[Ctrl+V] g d** a fim incorporar **d? g na** configuração.

A fim criar uma expressão regular, use o comando do **regex**. Além, o comando do **regex** 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 do MPF 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.

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.
carvão animal	Caractere	Quando o caráter não é um metacharacter, combina o caráter literal.
\ r	Tecla semelhante a tecla	Combina uma tecla semelhante a tecla ENTER: 0x0d.

	ENTER	
\ 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.

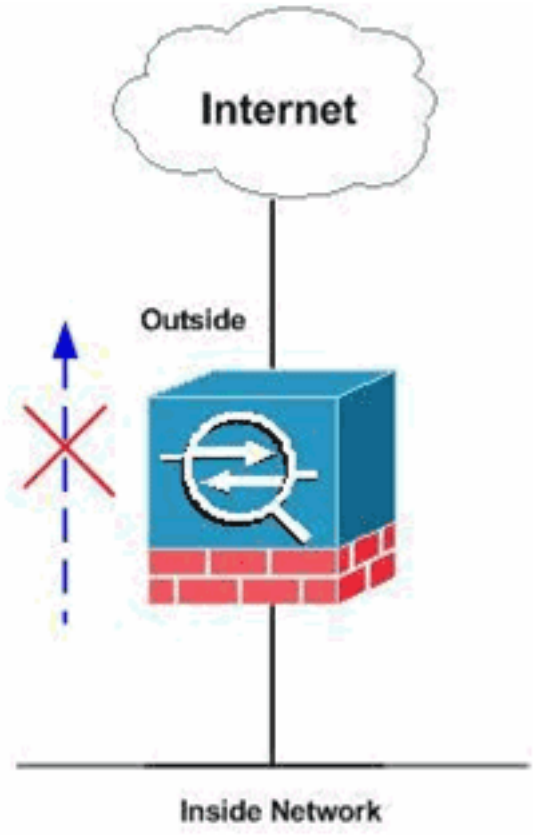
Configurar

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:



Nota: Os locais selecionados FTP são permitidos ou obstruídos usando expressões regulares.

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 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 g1u0103c.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
```

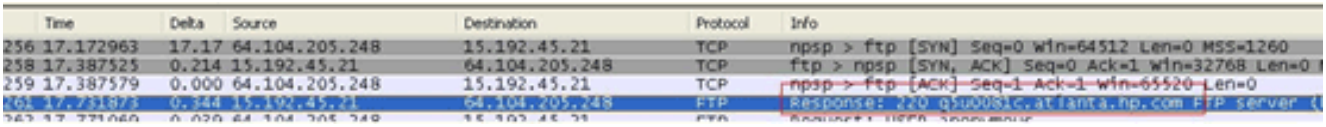
```
connection will be denied if !--- there is no match on
any one line). boot system disk0:/asa804-k8.bin ftp mode
passive pager lines 24 logging enable logging timestamp
logging buffered debugging mtu outside 1500 mtu inside
1500 no failover icmp unreachable rate-limit 1 burst-
size 1 asdm image disk0:/asdm-61557.bin 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 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 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
```

Configuração 8.x ASA com ASDM 6.x

Termine estas etapas a fim configurar as expressões regulares e aplicá-las ao MPF a fim obstruir os locais específicos FTP:

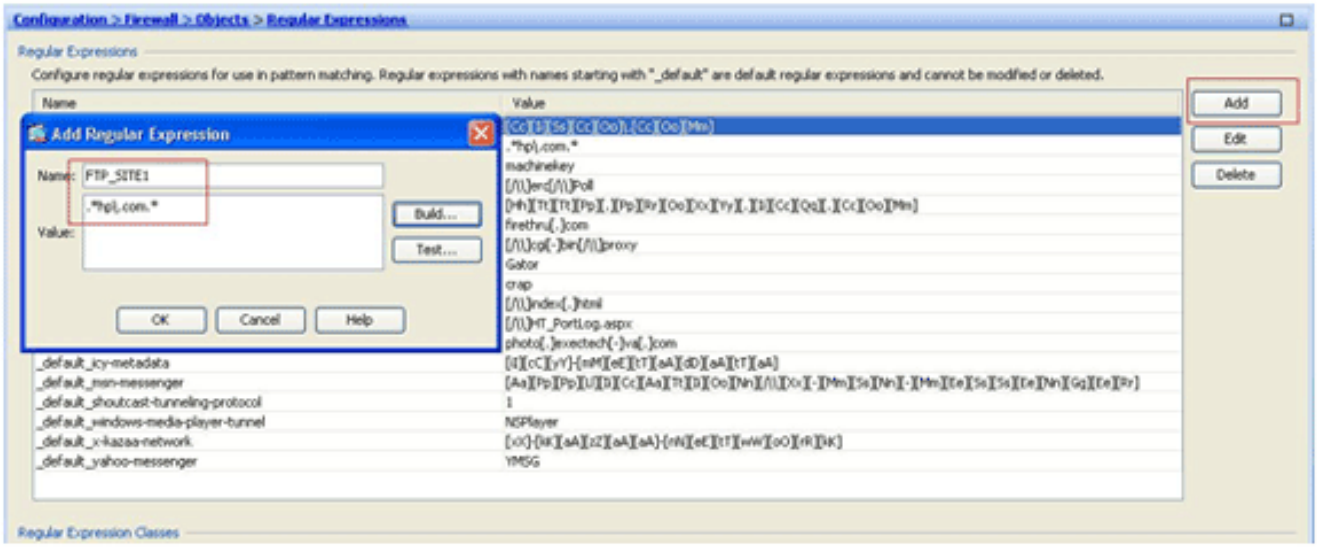
1. **Determine o nome do servidor FTP.**O motor da inspeção FTP pode fornecer a inspeção usando o critério diferente, tal como o comando, o nome de arquivo, o tipo de arquivo, o server, e o nome de usuário. Este procedimento usa o server como o critério. O motor da inspeção FTP usa a resposta do server 220 enviada pelo ftp site como o valor do server.

Este valor pode ser diferente do que o Domain Name usado pelo local. Este exemplo usa Wireshark para capturar pacotes de FTP ao local que é inspecionado a fim obter o valor da resposta 220 para usado em nossa expressão regular em etapa
2.

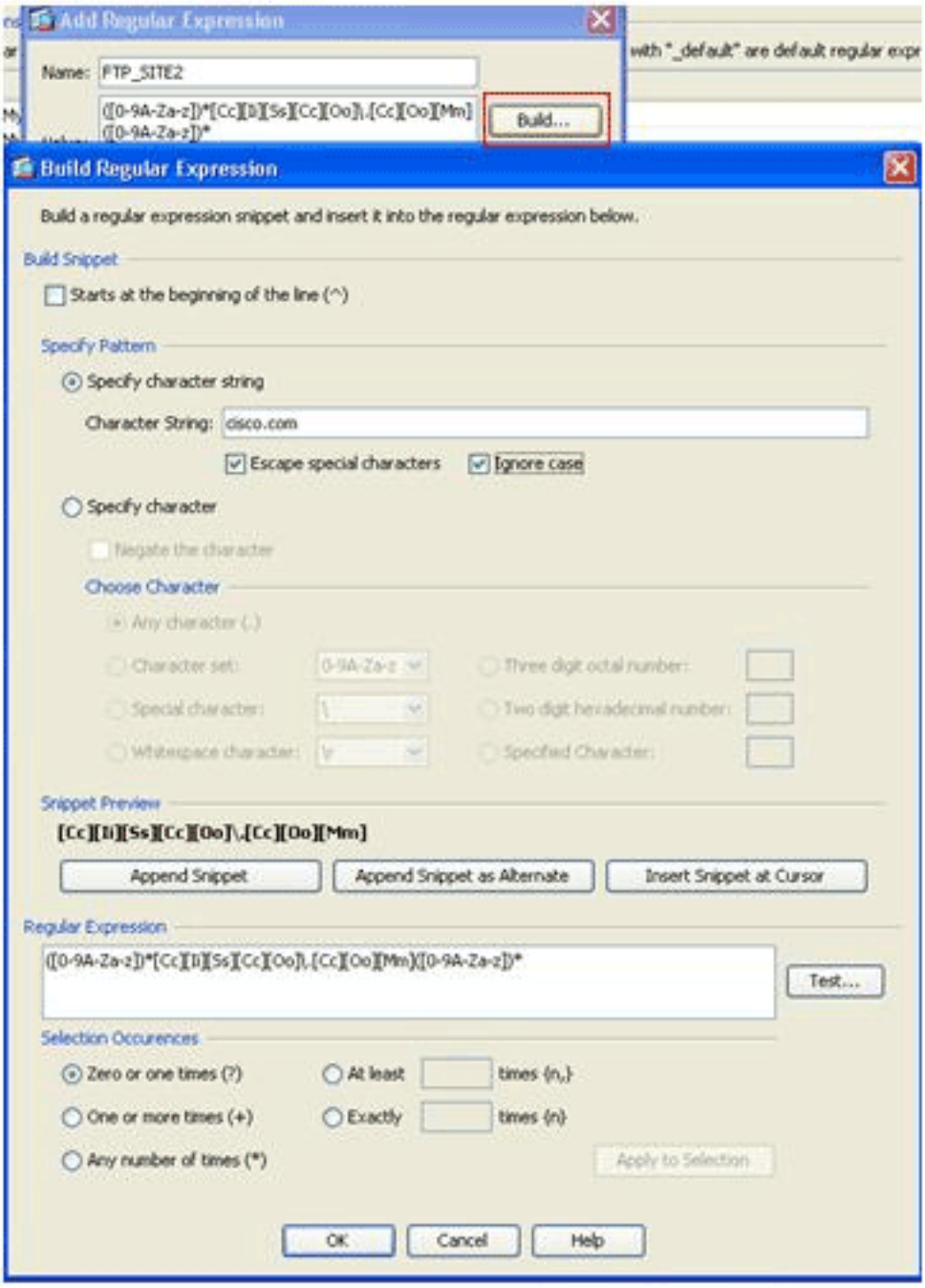


Baseado na captação o valor da resposta 220 para ftp://hp.com é (por exemplo) *q5u0081c.atlanta.hp.com*.

2. **Crie expressões regulares.**Escolha a **configuração > o Firewall > os objetos > as expressões regulares**, e o clique **adiciona** sob a aba da expressão regular a fim criar expressões regulares como descrito neste procedimento:Crie uma expressão regular, *FTP_SITE1*, a fim combinar a resposta 220 (como visto na captura de pacote de informação em Wireshark ou em alguma outra ferramenta usada) recebida do ftp site (por exemplo, “. * cavalos-força \ .com.*"), e **APROVAÇÃO do**
clique.

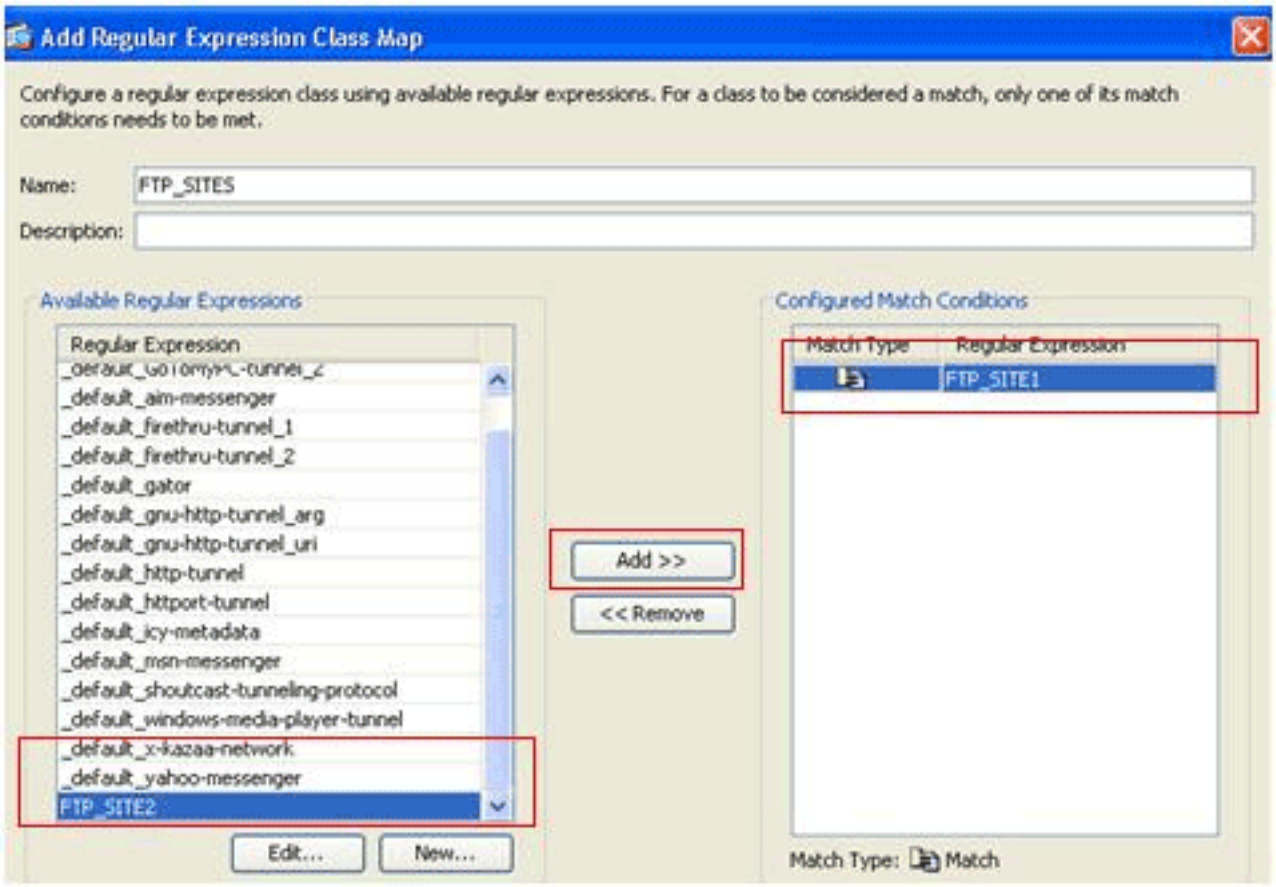


Nota: Você pode clicar a **construção** para a ajuda em como criar umas expressões regulares

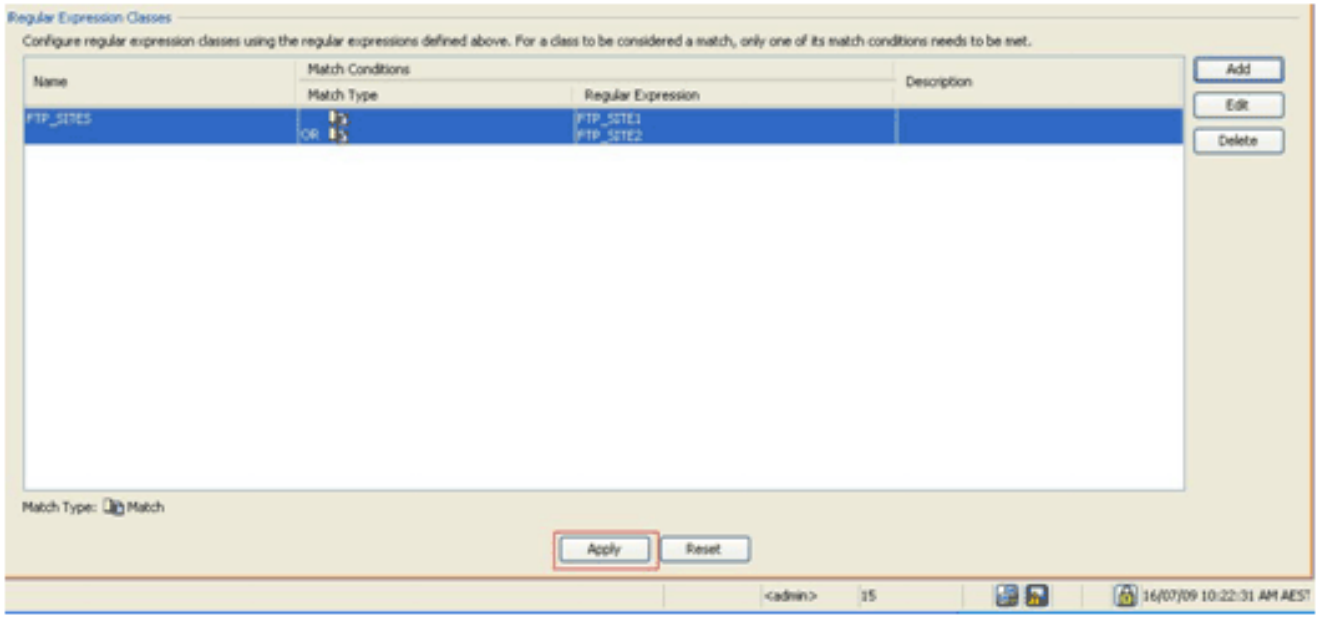


mais avançadas. Uma vez que a expressão regular é criada, o clique **aplica-se.**

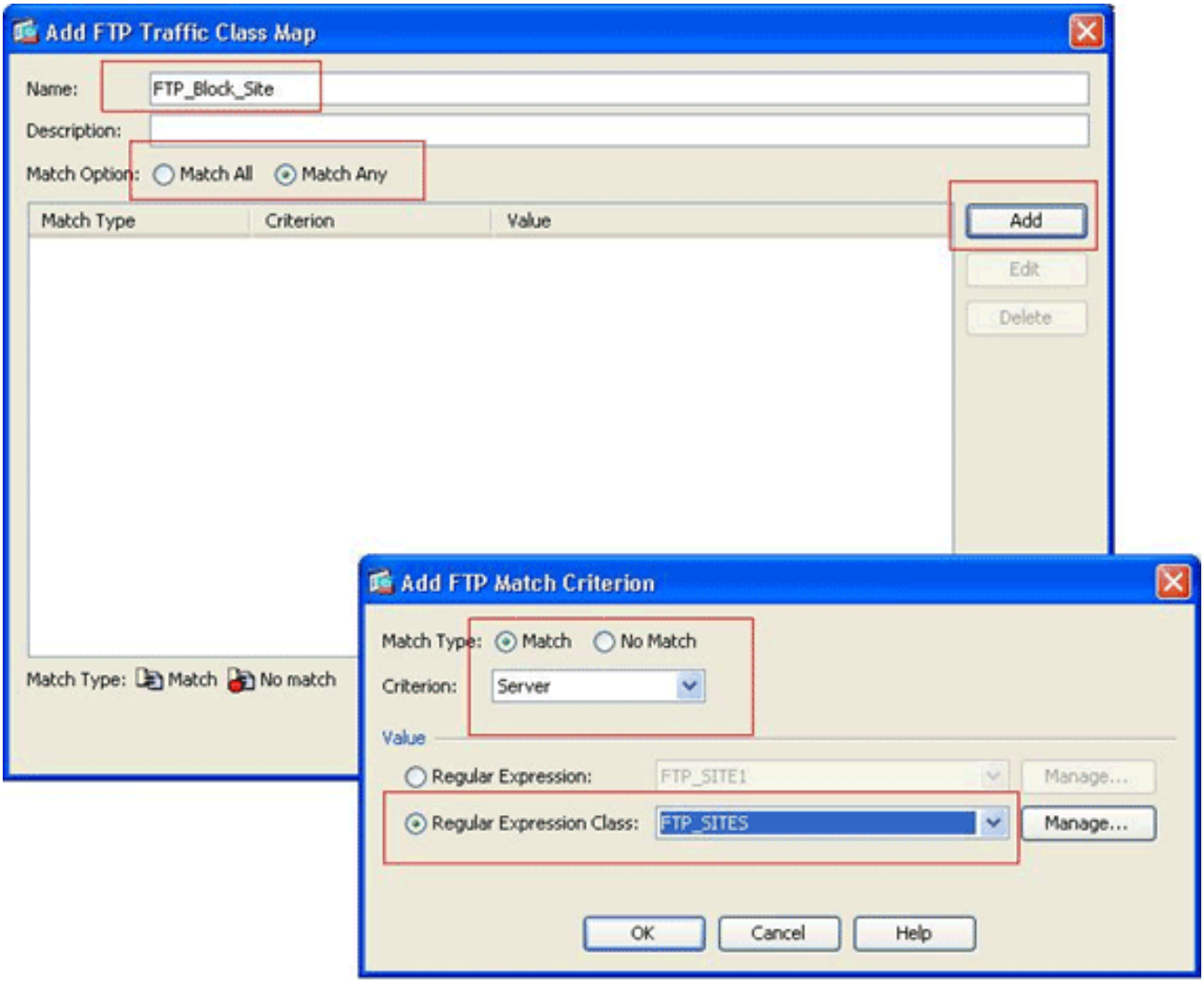
3. **Crie classes da expressão regular.**Escolha a **configuração > o Firewall > os objetos > as expressões regulares**, e o clique **adiciona** sob a seção das classes da expressão regular a fim criar a classe como descrito neste procedimento:Crie uma classe da expressão regular, *FTP_SITES*, a fim combinar algumas das expressões regulares *FTP_SITE1* e *FTP_SITE2*, e clique a **APROVAÇÃO**.



U ma vez que o mapa da classe é criado, o clique **aplica-se**.

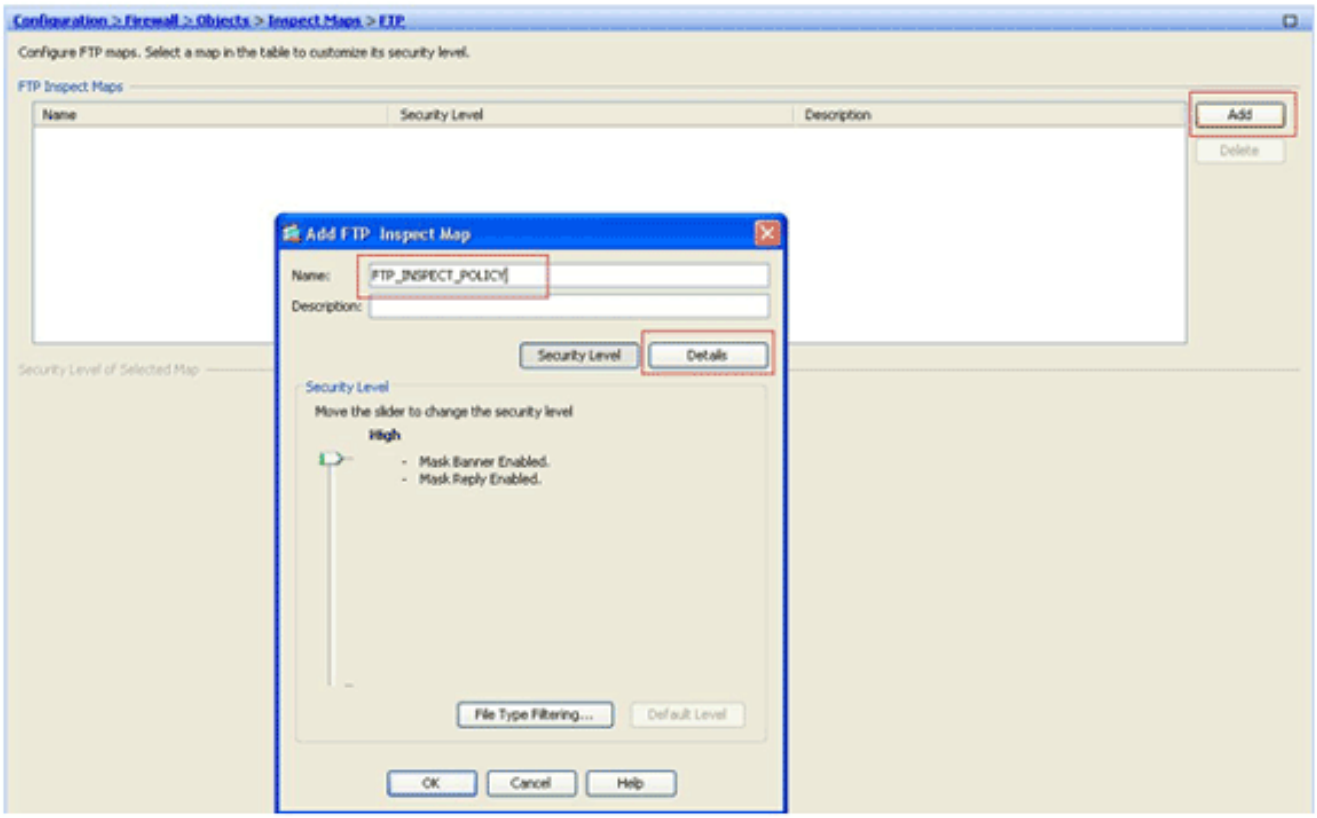


4. **Inspecione o tráfego identificado com mapas da classe.**Escolha a **configuração > o Firewall > os objetos > a classe traça > > Add FTP**, clicam com o botão direito, e escolhem **adicionam** a fim criar um mapa da classe para inspecionar o tráfego FTP identificado por várias expressões regulares como descrito neste procedimento:Crie um mapa da classe, *FTP_Block_Site*, a fim combinar a resposta 220 FTP com as expressões regulares que você criou.

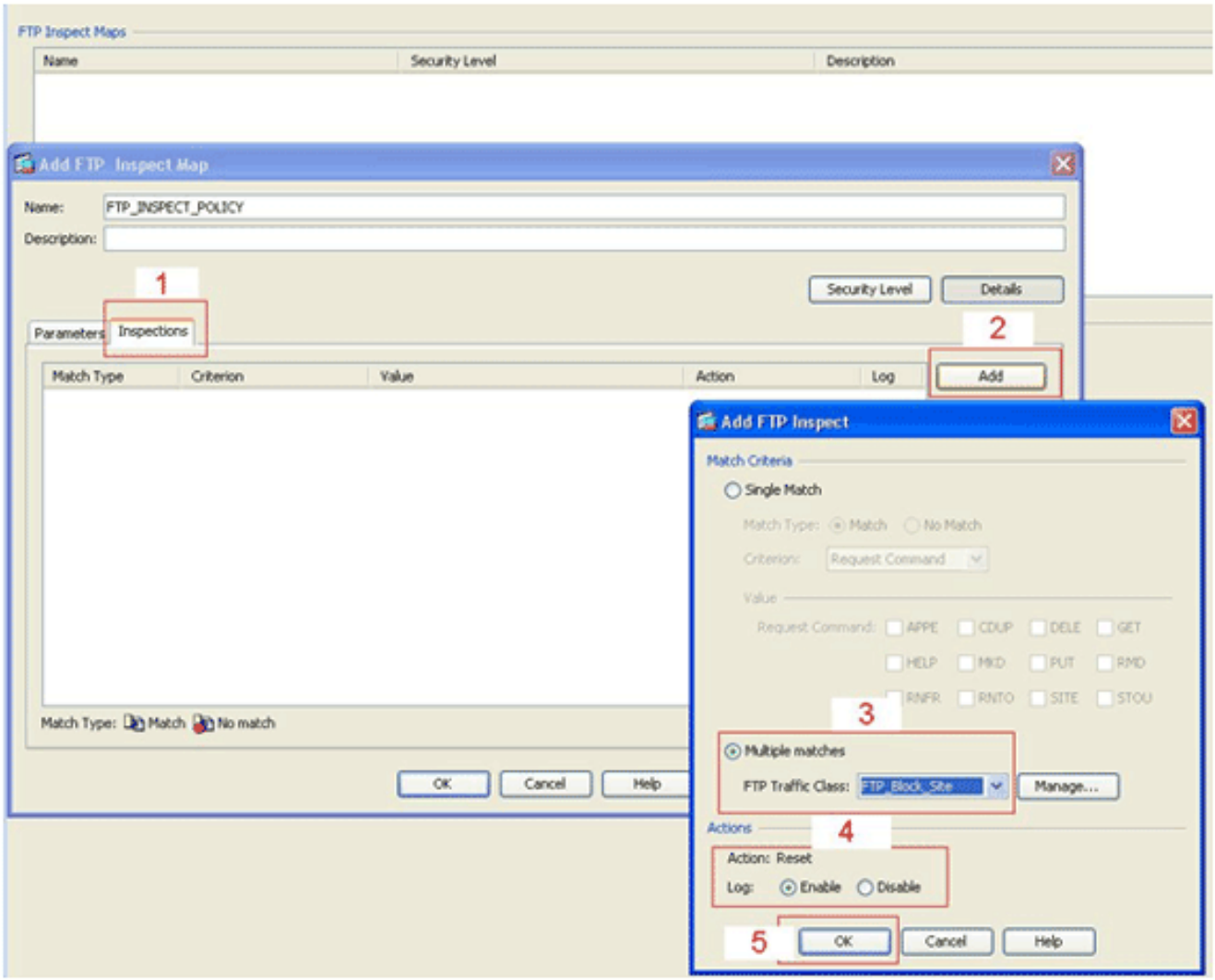


Se você quer excluir os locais especificados na expressão regular, não clique **nenhum** botão de rádio do **fósforo**.Na seção do valor, escolha uma expressão regular ou uma classe da expressão regular. Para este procedimento, escolha a classe que foi criada mais cedo.Clique em Apply.

5. **Ajuste as ações para o tráfego combinado na política da inspeção.**Escolha a **configuração > o Firewall > os objetos > inspecionam mapas > FTP> adicionam** a fim criar uma política da inspeção, e ajustam a ação para o tráfego combinado como necessário.

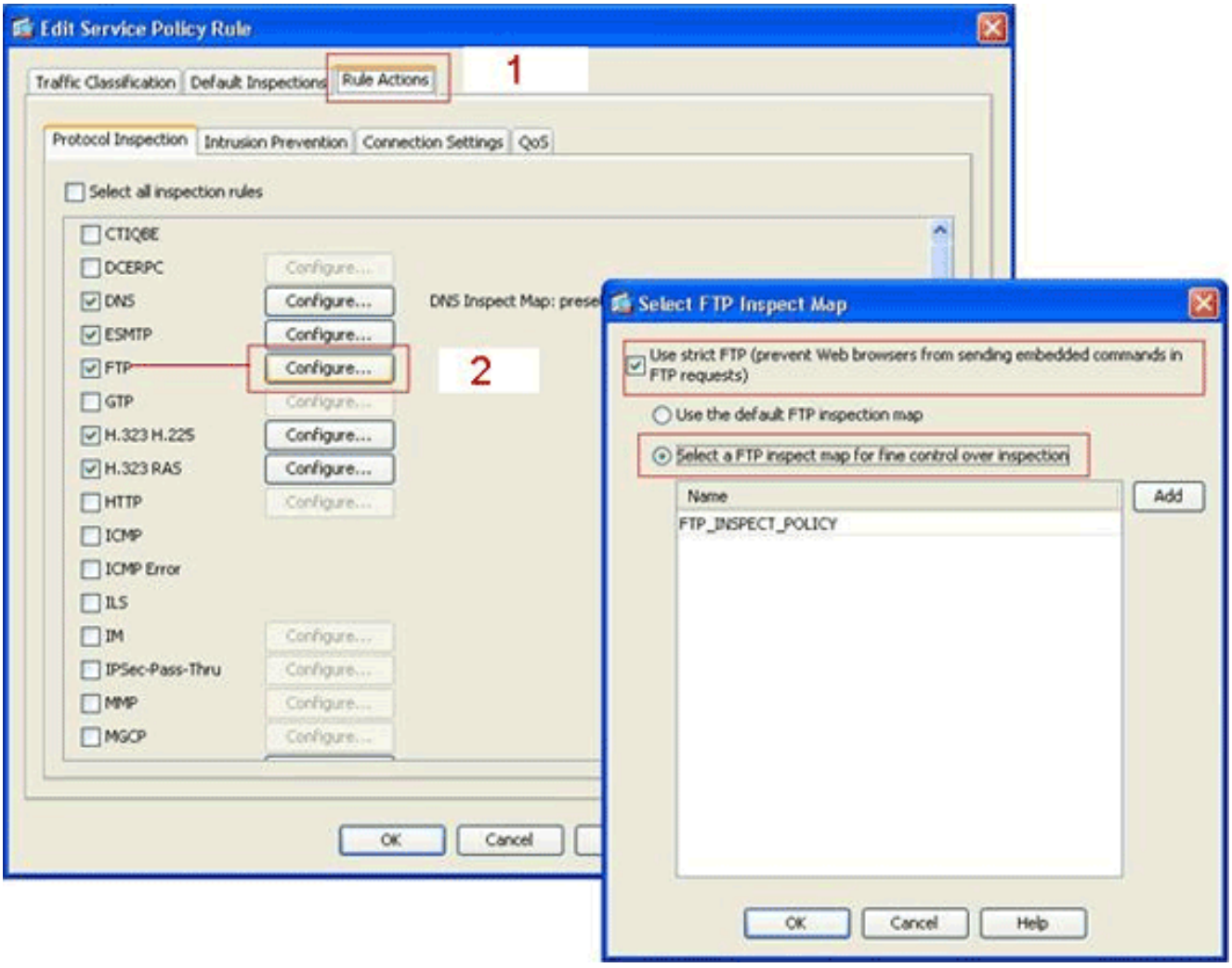


Incorpore o nome e uma descrição para a política da inspeção. (Por exemplo, *FTP_INSPECT_POLICY*.)Clique em **Details**.



Clique a aba das **inspeções**. (1)Clique em Add. (2)Clique o botão de rádio dos **fósforos do múltiplo**, e escolha a classe de tráfego da lista de drop-down. (3)Escolha a ação desejada da restauração permitir ou desabilitar. Este exemplo permite a conexão de FTP de restaurar para todos os locais FTP que *não combinam* nossos locais especificados. (4)Clique a **APROVAÇÃO**, clique a **APROVAÇÃO** outra vez, e clique-a então **aplicam-se**. (5)

6. **Aplique a política da inspeção FTP à lista global da inspeção.**Escolha **regras da configuração > do Firewall > da política de serviços**.No lado direito, selecione a política do **inspection_default**, e o clique **edita**.Sob as ações da regra catalogue (1), clicam o **botão Configure Button** para o FTP. (2)No FTP seleto inspecione a caixa de diálogo do mapa, verifique a caixa de verificação **restrita do uso FTP**, e clique então o **FTP inspecionam o mapa para o controle fino sobre o** botão de rádio da **inspeção**.A política nova da inspeção FTP, *FTP_INSPECT_POLICY*, deve ser visível na lista.Clique a **APROVAÇÃO**, clique a **APROVAÇÃO** outra vez, e clique-a então **aplicam-se**.



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 FTP_SITE1 "[Cc][Ii][Ss][Cc][Oo]\.[Cc][Oo][Mm]" regex FTP_SITE2 ".*hp\.com.*"`

- **mostre o class−map da executar-configuração** — Mostra os mapas da classe que foram configurados.`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 !`
- **o tipo do mapa de política da executar-configuração da mostra inspeciona o HTTP** — Mostra os mapas da política que inspecionam o tráfego de HTTP que foi configurado.`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 !`
- **Mostre o mapa de política da executar-configuração** — Indica todas as configurações de mapa de política, assim como configuração de mapa da política padrão.
`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 !`
- **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`

Troubleshooting

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

Você pode usar o **comando service-policy da mostra** a fim verificar que o motor da inspeção inspeciona o tráfego e corretamente os permite ou deixa cair.

```
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
```

Informações Relacionadas

- ASA/PIX 8.x: Determinados Web site do bloco (URL) que usam expressões regulares com exemplo da configuração MPF
- PIX/ASA 7.x e mais tarde: Obstrua o tráfego peer-to-peer (P2P) e das mensagens instantâneas (IM) usando o exemplo da configuração MPF
- PIX/ASA 7.x: Exemplo de Configuração de Habilitação de Serviços de FTP/TFTP
- Aplicando a inspeção do protocolo de camada do aplicativo
- Dispositivos de segurança adaptáveis Cisco ASA série 5500 – Apoio
- Cisco Adaptive Security Device Manager (ASDM)
- Dispositivos de segurança Cisco PIX série 500 – Apoio

- Software do firewall Cisco PIX – Apoio
- Referências de comandos do Software do firewall Cisco PIX
- Suporte Técnico e Documentação - Cisco Systems