ASA/PIX 8.x : Exemple de configuration d'autorisation/blocage des sites FTP utilisant les expressions régulières avec MPF

Contenu

Introduction

Ce document décrit comment configurer les appliances ASA/PIX 8.x de sécurité Cisco qui emploie des expressions régulières avec le cadre de stratégie modulaire (MPF) afin de bloquer ou permettre certains sites de FTP par le nom du serveur.

Conditions préalables

Conditions requises

Ce document suppose que l'appliance de sécurité Cisco est configurée et fonctionne correctement.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- L'appliance de sécurité adaptable de gamme Cisco 5500 (ASA) cette exécute la version de logiciel 8.0(x) et plus tard
- Version 6.x du Cisco Adaptive Security Device Manager (ASDM) pour ASA 8.x

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Aperçu modulaire de cadre de stratégie

MPF fournit un cohérent et une façon flexible pour configurer des caractéristiques de dispositifs de sécurité. Par exemple, vous pouvez employer MPF pour créer une configuration de délai d'attente qui est spécifique à une application TCP particulière, par opposition à une qui s'applique à toutes les applications TCP.

MPF prend en charge ces caractéristiques :

- Normalisation de TCP, limites et délais d'attente de connexion de TCP et UDP, et randomisation de numéro de séquence de TCP
- CSC
- Inspection d'application
- IPS
- QoS a entré le maintien de l'ordre
- QoS a sorti le maintien de l'ordre
- File d'attente prioritaire de QoS

La configuration du MPF se compose de quatre tâches :

1. Identifiez le trafic de la couche 3 et de la couche 4 auquel vous voulez s'appliquer des actions. Référez-vous à identifier le trafic utilisant un pour en savoir plus de class map de la couche 3/4.
2. (Inspection d'application seulement.) Définissez les actions spéciales pour le trafic d'inspection d'application. Référez-vous à configurer des actions spéciales pour le pour en savoir plus d'inspections d'application.
3. Appliquez-vous les actions au trafic de la couche 3 et de la couche 4. Référez-vous à définir des actions utilisant un pour en savoir plus de carte de stratégie de la couche 3/4.
4. Lancez les actions sur une interface. Référez-vous à s'appliquer une stratégie de la couche 3/4 à une interface utilisant un pour en savoir plus de stratégie de service.

Expression régulière

Une expression régulière apparie des chaînes de texte littéralement comme chaîne précise ou en

employant des métacaractères, ainsi vous pouvez apparier de plusieurs variantes d'une chaîne de texte. Vous pouvez employer une expression régulière pour apparier le contenu de certain trafic de l'application. Par exemple, vous pouvez apparier une chaîne d'URL à l'intérieur d'un paquet de HTTP.

Remarque: Employez **Ctrl+V** afin d'échapper à tous les caractères particuliers dans le CLI, tel que des points d'interrogation (?) ou des onglets. Par exemple, type **d [Ctrl+V] g** afin d'écrire **d ? g** dans la configuration.

Afin de créer une expression régulière, utilisez la commande d'**expression régulière**. En outre, la commande d'**expression régulière** peut être utilisée pour différentes caractéristiques qui exigent apparier des textes. Par exemple, vous pouvez configurer des actions spéciales pour l'inspection d'application avec l'utilisation du MPF qui utilise une carte de stratégie d'inspection. Référez-vous au pour en savoir plus de commande de policy-map type inspect.

Dans la carte de stratégie d'inspection, vous pouvez identifier le trafic que vous voulez agir au moment si vous créez un class map d'inspection qui contient un ou plusieurs **commandes match**, ou vous pouvez utiliser des **commandes match** directement dans la carte de stratégie d'inspection. Quelques **commandes match** vous ont permis d'identifier le texte dans un paquet utilisant une expression régulière. Par exemple, vous pouvez des chaînes de match url à l'intérieur des paquets de HTTP. Vous pouvez grouper des expressions régulières dans un class map d'expression régulière. Référez-vous au pour en savoir plus de commande d'expression régulière de type de class-map.

Ce tableau présente les métacaractères qui ont des significations particulières.

Caractère	Description	Notes
.	Point	Correspond à n'importe quel caractère unique. Par exemple, **d.g apparie le** chien, le dag, le dtg, et n'importe quel mot qui contient ces caractères, tels que le doggonnit.
(exp)	Subexpression	Un subexpression isole des caractères des caractères environnants, de sorte que vous puissiez utiliser d'autres métacaractères sur le subexpression. Par exemple, **d (o|**le chien de correspondances **a) g** et le dag, mais **font|**les correspondances **AG** font et AG. Un subexpression peut également être utilisé avec des quantificateurs de répétition pour différencier les caractères signifiés pour la répétition. Par exemple, **ab(xy){3}z** apparie l'abxyxyxyz.
|	Alternance	Apparie l'un ou l'autre d'expression qu'elle sépare. Par exemple, **chien|le cat** apparie le chien ou le cat.
?	Point d'interrogation	Un quantificateur qui indique qu'il y a 0 ou de 1 de l'expression précédente. Par exemple, **lo ? l'expert en logiciel** apparie le LSE ou le perd.

		Remarque: Vous devez écrire **Ctrl+V** et puis le point d'interrogation ou bien la fonction d'aide est appelé.
*	Astérisque	Un quantificateur qui indique qu'il y a de 0, 1, ou un certain nombre d'expression précédente. Par exemple, le **lo*se** apparie le LSE, perdent, lâche, et ainsi de suite.
{x}	Quantificateur de répétition	De la répétition temps exactement x. Par exemple, **ab(xy){3}z** apparie l'abxyxyxyz.
{x,}	Quantificateur minimum de répétition	Temps de la répétition au moins x. Par exemple, **ab(xy){2,}z** apparie l'abxyxyz, abxyxyxyz, et ainsi de suite.
[ABC]	Classe de caractères	Apparie n'importe quel caractère dans les crochets. Par exemple, **[ABC]** apparie a, b, ou C.
[^abc]	Classe de caractères réalisée une inversion	Apparie un caractère unique qui n'est pas contenu dans les crochets. Par exemple, **[^abc]** apparie n'importe quel caractère autre qu'a, b, ou C. **[^A-Z]** apparie n'importe quel caractère unique qui n'est pas une lettre majuscule.
[courant alternatif]	Classe de chaîne de caractère	Apparie n'importe quel caractère dans la plage. **[a-z]** apparie n'importe quelle lettre minuscule. Vous pouvez mélanger des caractères et des plages : **[abcq-z]** apparie a, b, c, q, r, s, t, u, v, W, x, y, z, et ainsi fait **[un-CQ-z]**. Le caractère de tiret (-) est littéral seulement si c'est le bout ou le premier caractère dans les crochets : **[ABC]** ou **[- ABC]**.
""	Guillemets	Conserves traînant ou menant les espaces dans la chaîne. Par exemple, le « **test** » préserve le principal espace quand il recherche une correspondance.
^	Caret	Spécifie le début d'une ligne.
\	Caractère d'échappement	Une fois utilisé avec un métacaractère, apparie un caractère littéral. Par exemple, **\ [**apparie le crochet de carré de gauche.
car	Caractè	Quand le caractère n'est pas un

	re	métacaractère, apparie le caractère littéral.
\ r	Retour chariot	Apparie un retour chariot : 0x0d.
\ n	Saut de ligne	Apparie une nouvelle ligne : 0x0a.
\ t	Onglet	Apparie un onglet : 0x09.
\ f	Chargement de page	Apparie une alimentation papier : 0x0c.
\ xNN	Nombre hexadécimal échappé	Apparie un caractère ASCII qui utilise un hexadécimal qui est exactement deux chiffres.
\ NNN	Nombre octal échappé	Apparie un caractère ASCII car octal qui est exactement trois chiffres. Par exemple, le caractère 040 représente un espace.

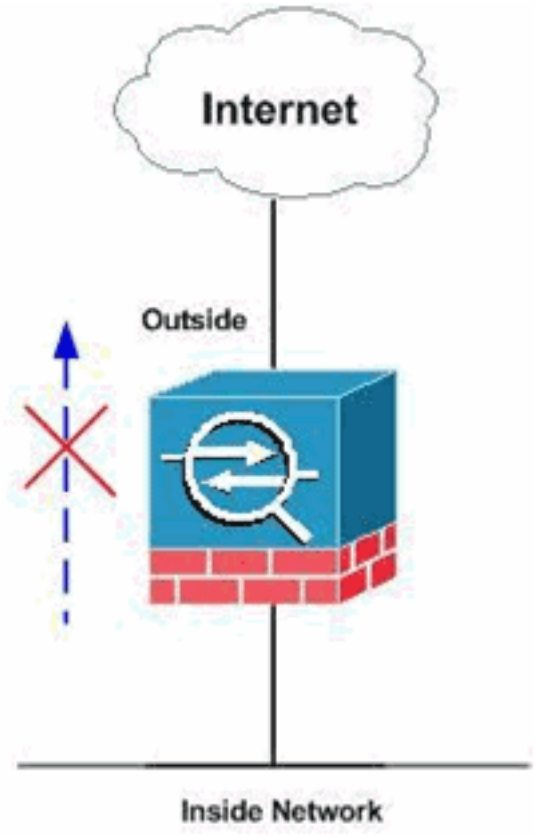
Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque: Des sites sélectionnés de FTP sont permis ou bloqués utilisant des expressions régulières.

Configurations

Ce document utilise les configurations suivantes :

- Configuration de l'interface de ligne de commande ASA
- Configuration 8.x ASA avec ASDM 6.x

Configuration de l'interface de ligne de commande ASA

Configuration de l'interface de ligne de commande 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 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
```

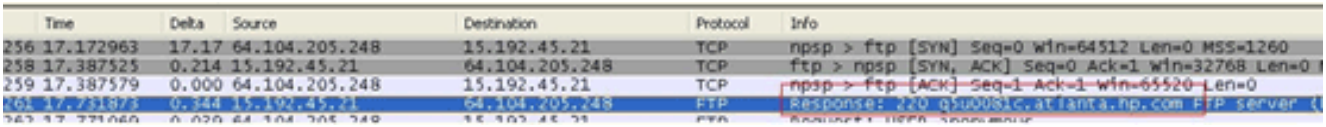
```
telnet timeout 5
ssh scopy enable
ssh timeout 5
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept


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
```

Configuration 8.x ASA avec ASDM 6.x

Terminez-vous ces étapes afin de configurer les expressions régulières et s'appliquer les à MPF afin de bloquer les sites de FTP de particularité :

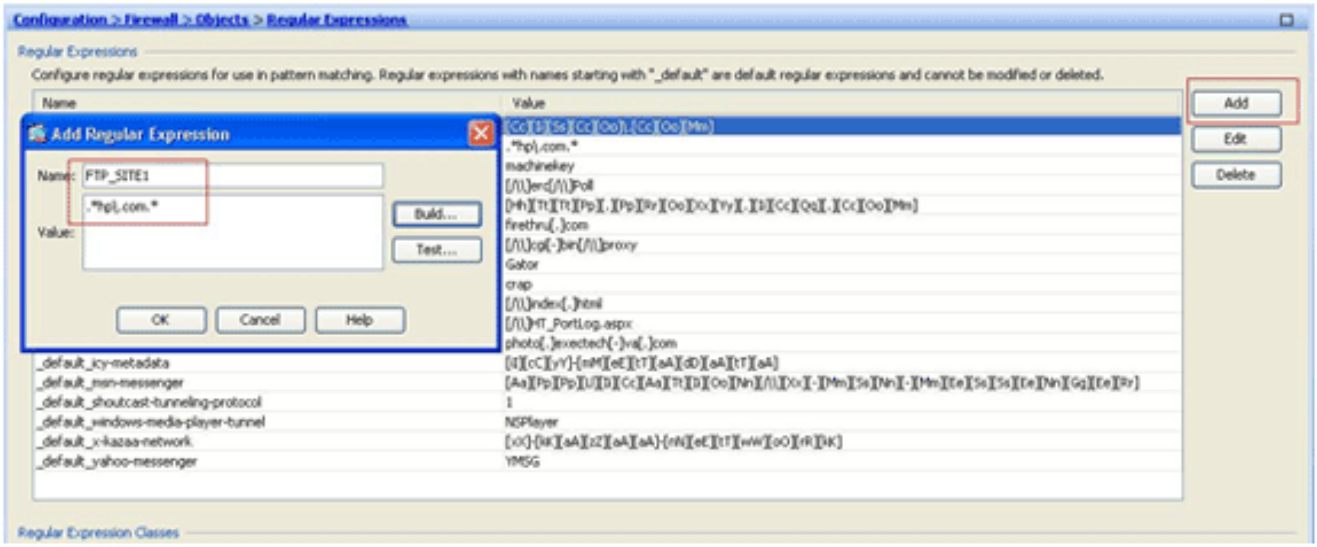
1. **Déterminez le nom serveur ftp.**L'engine d'inspection de FTP peut fournir l'inspection utilisant le critère différent, tel que la commande, le nom du fichier, le type de fichier, le serveur, et le

nom d'utilisateur. Cette procédure utilise le serveur comme critère. L'engine d'inspection de FTP utilise la réponse du serveur 220 envoyée par le site ftp comme valeur de serveur. Cette valeur peut être différente que le nom de domaine utilisé par le site. Cet exemple emploie Wireshark pour capturer des paquets de FTP au site qui est examiné afin d'obtenir la valeur de la réponse 220 pour utilisé dans notre expression régulière dans l'étape 2.

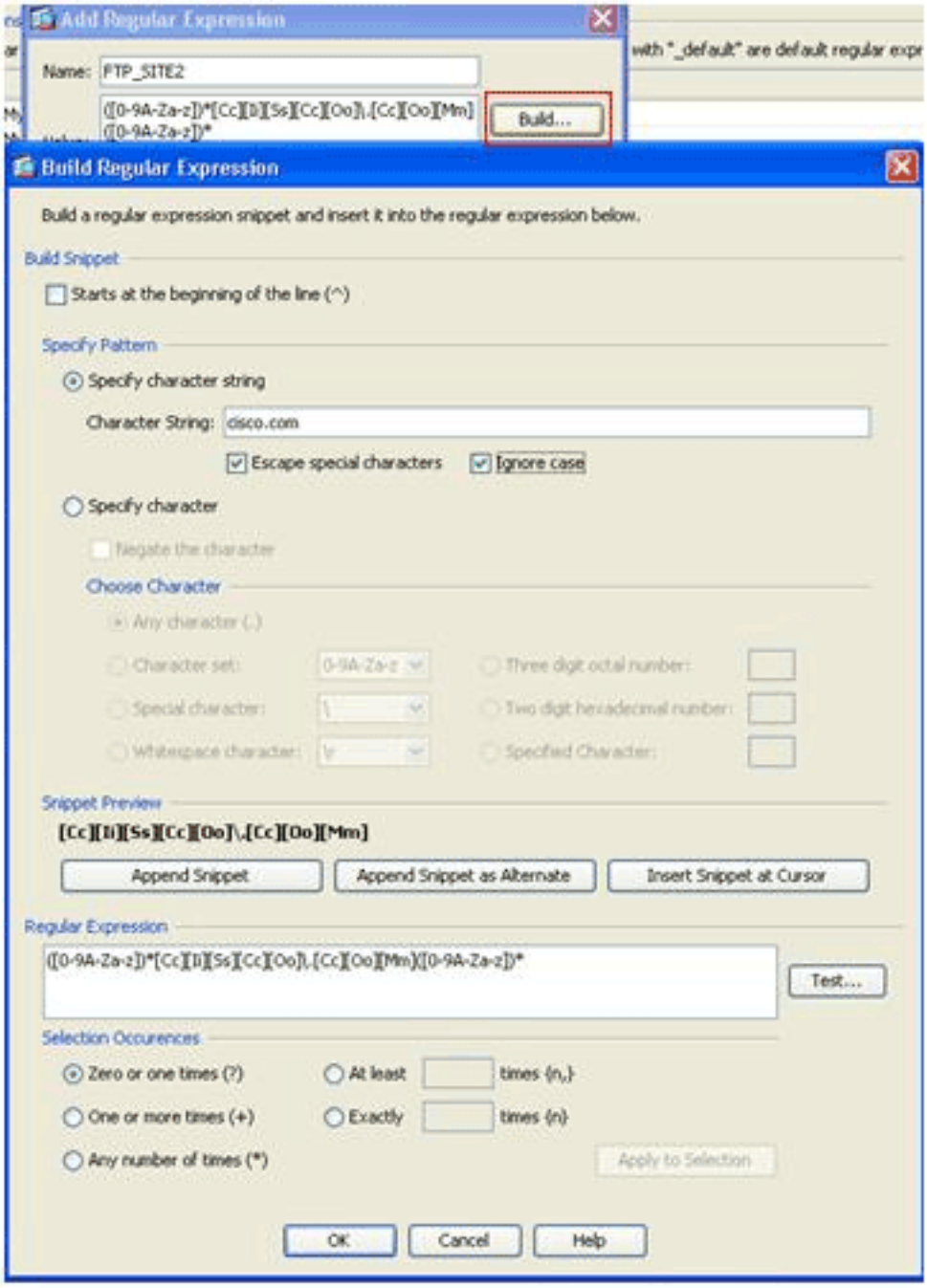


Basé sur la capture la valeur de la réponse 220 pour ftp://hp.com est (par exemple) *q5u0081c.atlanta.hp.com*.

2. **Créez les expressions régulières.**Choisissez la **configuration > le Pare-feu > les objets > les expressions régulières**, et cliquez sur Add sous l'onglet d'expression régulière afin de créer des expressions régulières comme décrit dans cette procédure :Créez une expression régulière, *FTP_SITE1*, afin d'apparier la réponse 220 (comme vu dans la capture de paquet dans Wireshark ou tout autre outil utilisé) reçue du site ftp (par exemple, « . * les puissances en chevaux \ .com.*"), et cliquent sur OK.

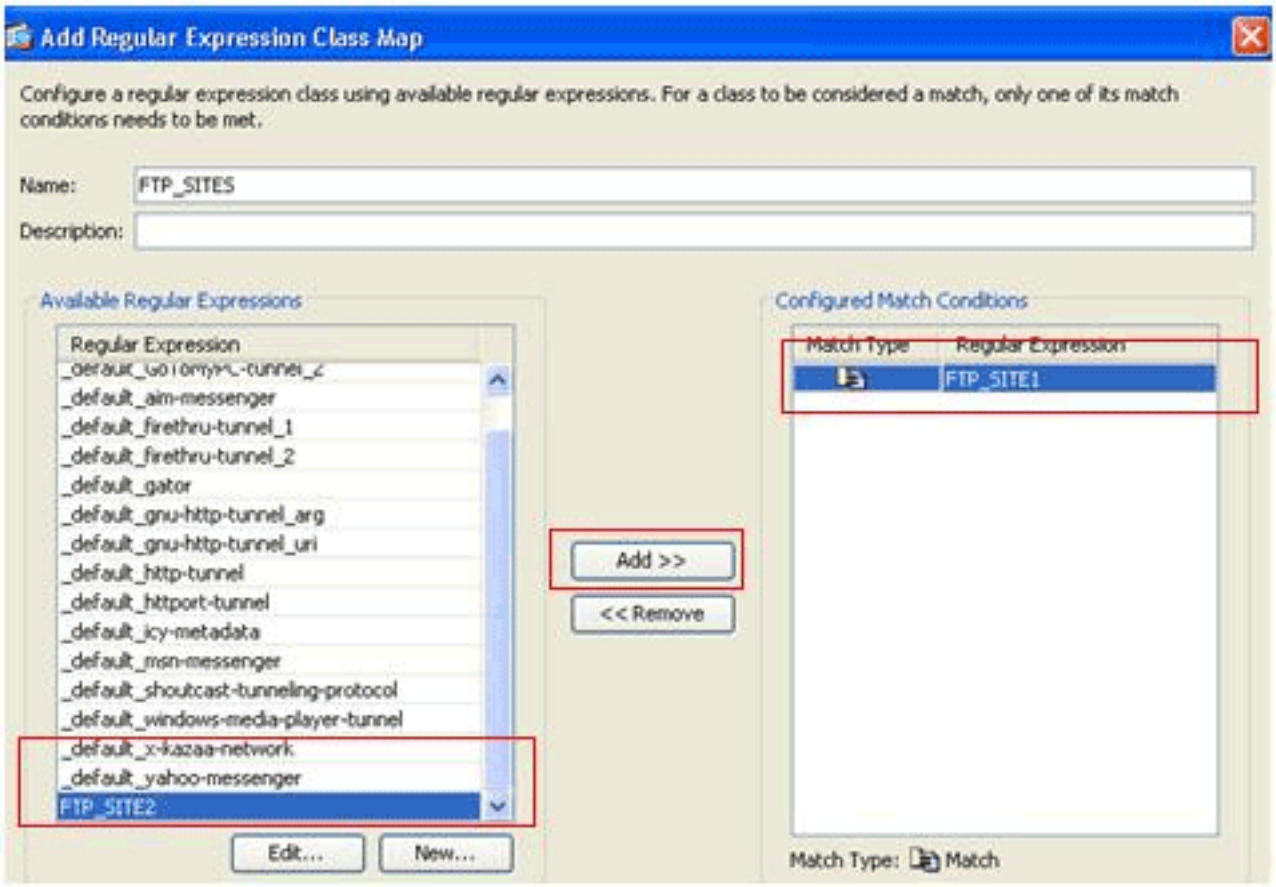


Remarque: Vous pouvez cliquer sur la **construction** pour l'aide sur la façon dont créer des expressions régulières plus

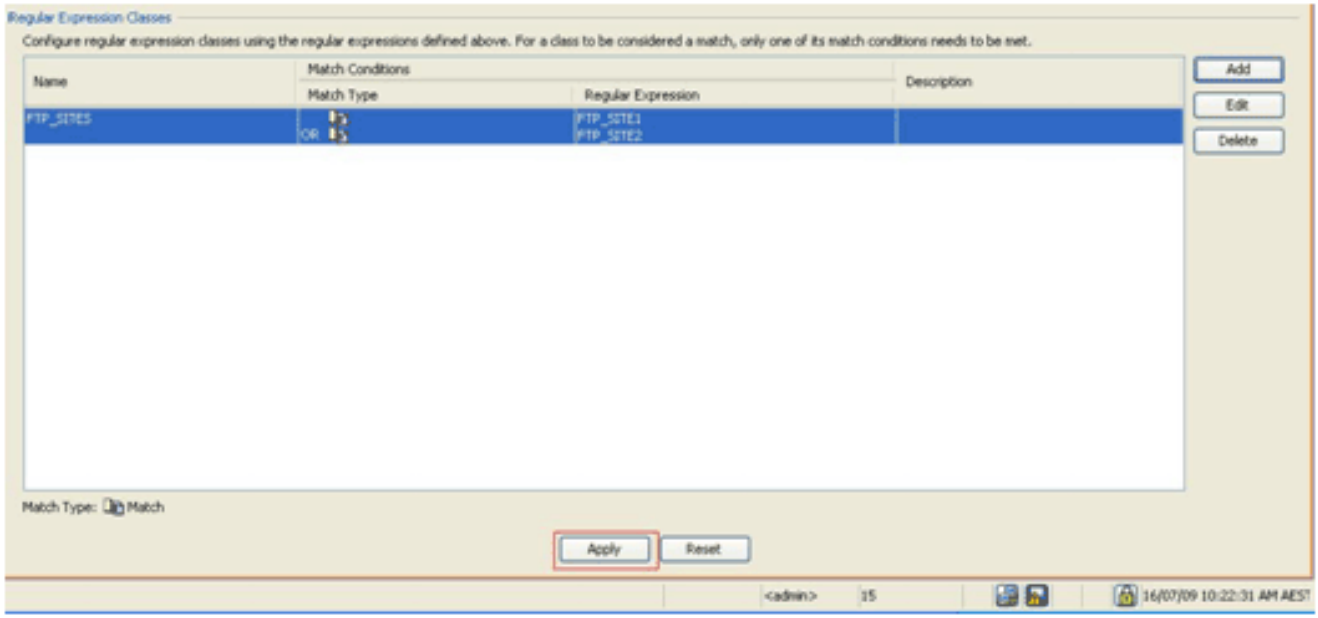


avancées. Une fois que l'expression régulière est créée, cliquez sur Apply.

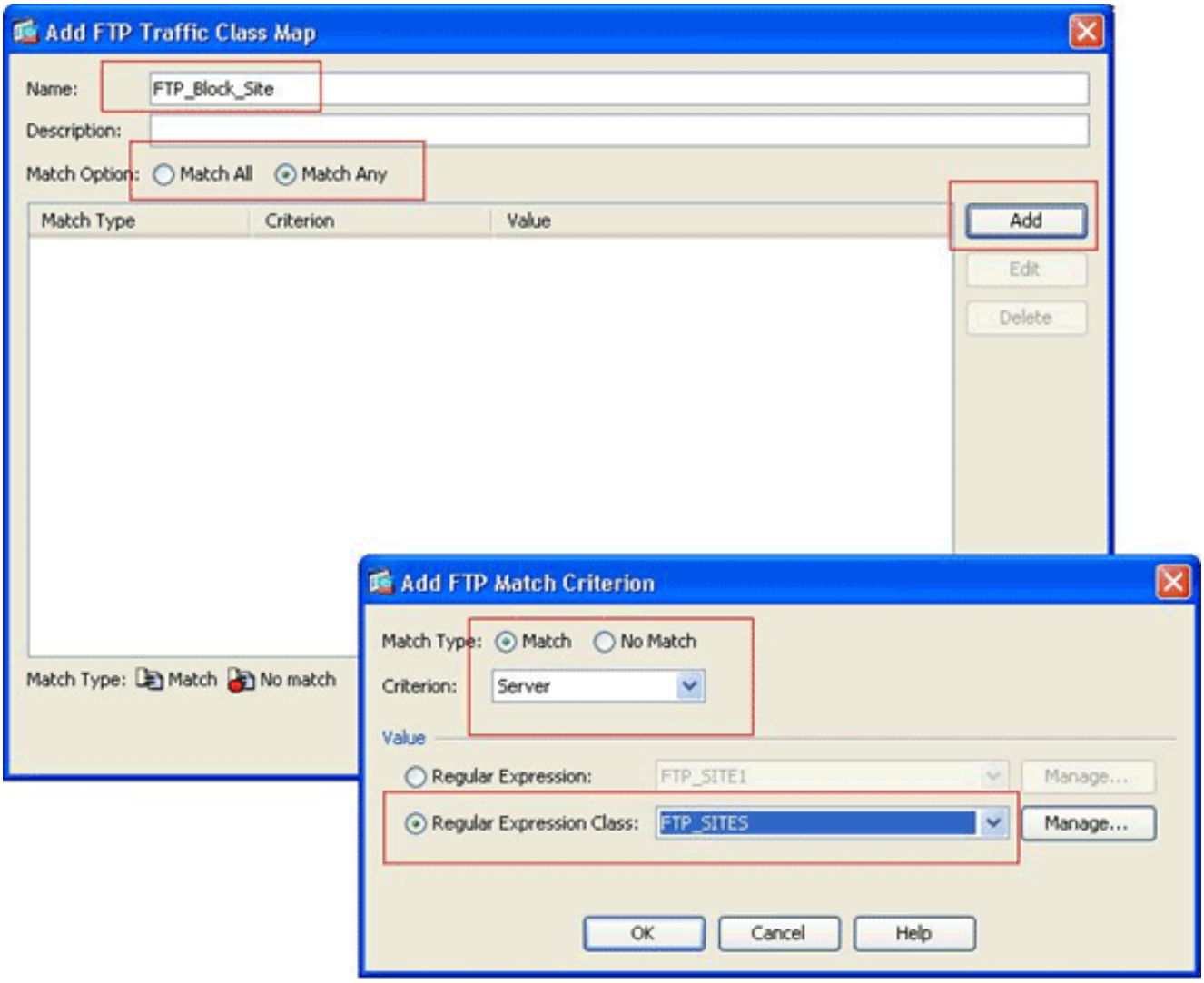
3. **Créez les classes d'expression régulière.**Choisissez la **configuration > le Pare-feu > les objets > les expressions régulières**, et cliquez sur Add sous la section de classes d'expression régulière afin de créer la classe comme décrit dans cette procédure :Créez une classe d'expression régulière, *FTP_SITES*, afin d'apparier les expressions régulières l'unes des *FTP_SITE1* et le *FTP_SITE2*, et cliquez sur
OK.



U
ne fois que le class map est créé, cliquez sur
Apply.

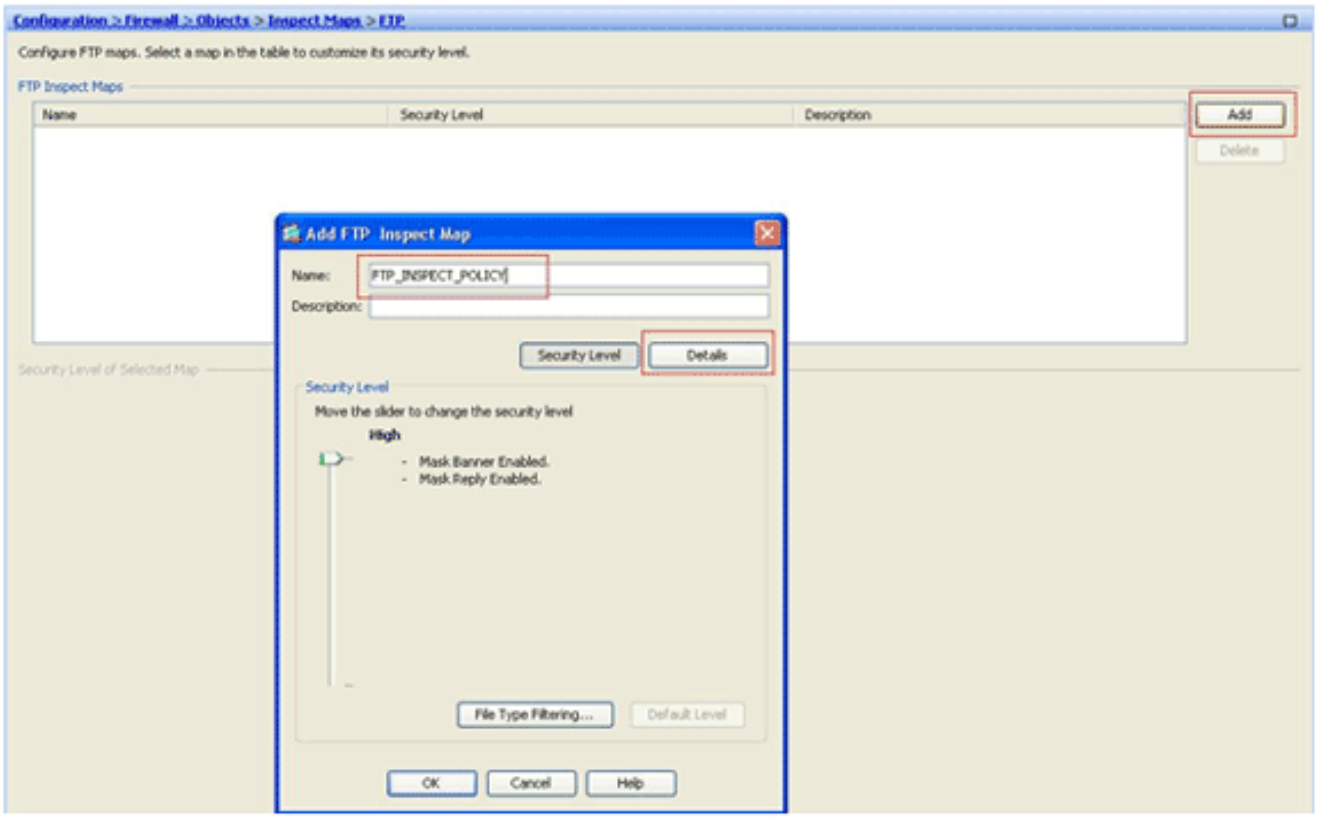


4. **Examinez le trafic identifié avec des class map.**Choisissez la **configuration > le Pare-feu > les objets > les class map > le FTP > ajoutent**, cliquent avec le bouton droit, et choisissent **ajoutent** afin de créer un class map pour examiner le trafic FTP identifié par de diverses expressions régulières comme décrit dans cette procédure :Créez un class map, *FTP_Block_Site*, afin d'apparier la réponse 220 de FTP avec les expressions régulières que vous avez
créées.

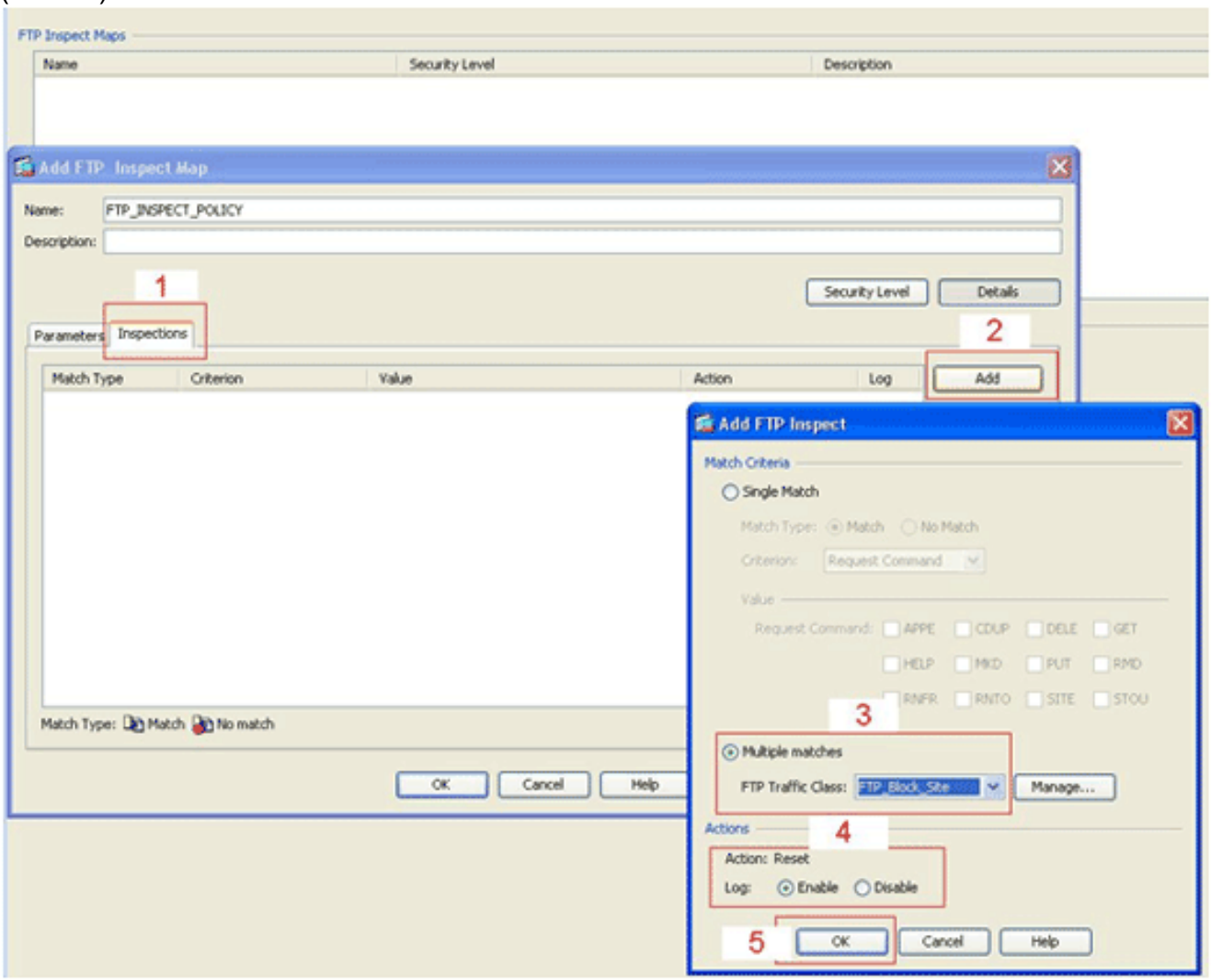


Si vous voulez exclure les sites spécifiés dans l'expression régulière, ne cliquez sur l'**aucune** case d'option de **correspondance**.Dans la section de valeur, choisissez une expression régulière ou une classe d'expression régulière. Pour cette procédure, choisissez la classe qui a été créée plus tôt.Cliquez sur **Apply**.

5. **Placez les actions pour le trafic apparié dans la stratégie d'inspection.**Choisissez la **configuration > le Pare-feu > les objets > examinent des cartes > FTP> ajoutent** afin de créer une stratégie d'inspection, et placent l'action pour le trafic apparié au besoin.

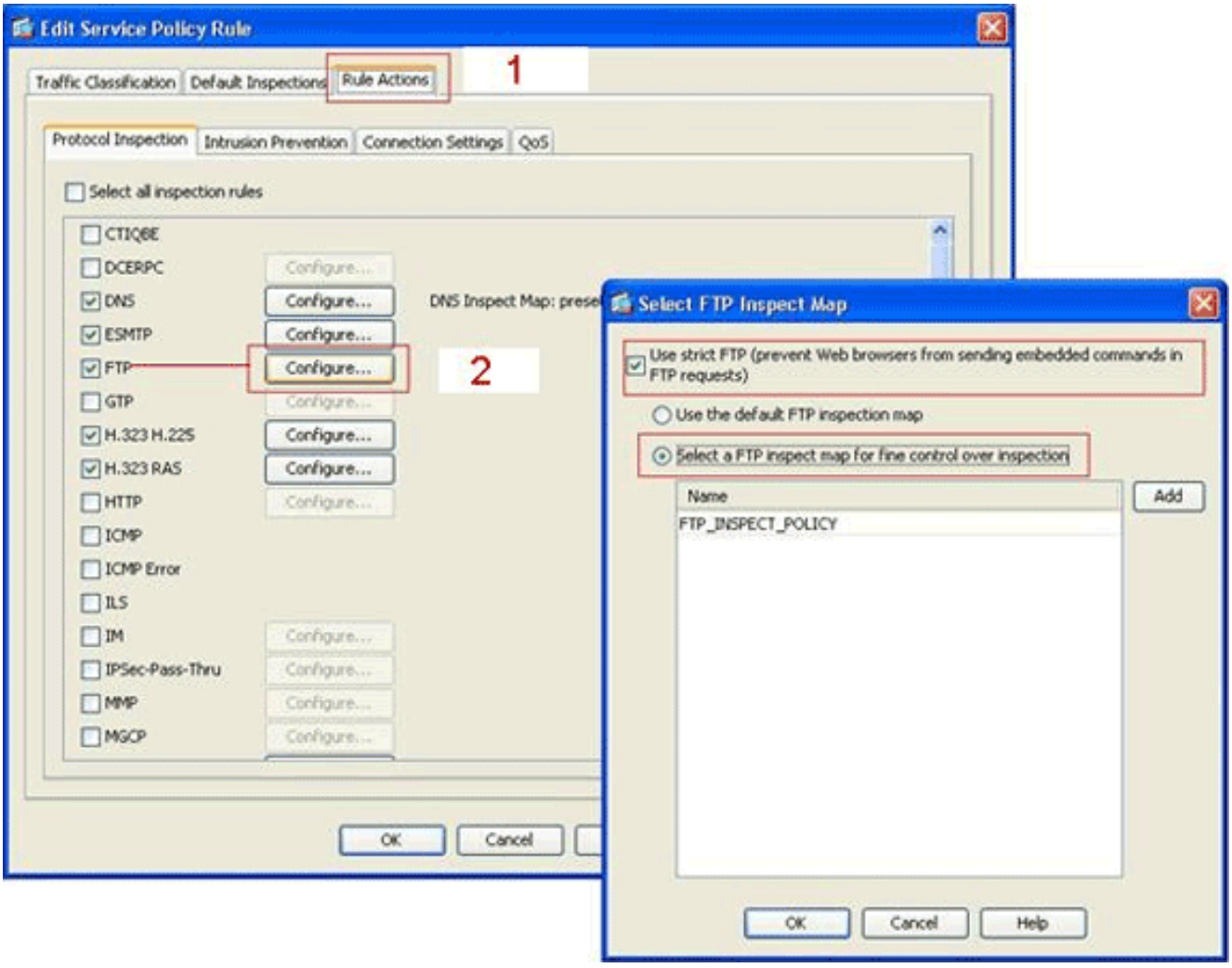


Écrivez le nom et une description pour la stratégie d'inspection. (Par exemple, *FTP_INSPECT_POLICY*.)Cliquez sur **Details**
(Détails).



Cliquez sur les **inspections** tableau (1)Cliquez sur **Add**. (2)Cliquez sur la case d'option de **correspondances de multiple**, et choisissez la classe du trafic de la liste déroulante. (3)Choisissez l'action désirée de remise d'activer ou désactiver. Cet exemple permet à la connexion FTP de remettre à l'état initial pour tous les sites de FTP *n'appariant pas* nos sites spécifiés. (4)Cliquez sur OK, cliquez sur OK de nouveau, et cliquez sur Apply alors. (5)

6. **Appliquez-vous la stratégie de FTP d'inspection à la liste globale d'inspection.**Choisissez les **règles de configuration > de stratégie de Pare-feu > de service**.Du côté droit, sélectionnez la stratégie d'**inspection_default**, et cliquez sur Edit.Selon la règle les actions tabulent (1), cliquent sur le bouton de **configurer** pour le FTP. (2)Dans le FTP choisi examinez la boîte de dialogue de carte, cochez la case **stricte de FTP d'utilisation**, et puis cliquez sur le **FTP examinent la carte pour assurer le contrôle correct de la** case d'option d'**inspection**.La nouvelle stratégie d'inspection de FTP, *FTP_INSPECT_POLICY*, devrait être visible dans la liste.Cliquez sur OK, cliquez sur OK de nouveau, et cliquez sur Apply alors.



Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **expression régulière de show running-config** — Affiche les expressions régulières qui ont été

configurées.

```
ciscoasa#show running-configregex
regex FTP_SITE1 "[Cc][Ii][Ss][Cc][Oo]\.[Cc][Oo][Mm]"
regex FTP_SITE2 ".*hp\.com.*"
```

- **class−map de show running-config** — Affiche les class map qui ont été configurés.

```
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
!
```

- **policy-map type inspect http de show running-config** — Affiche les cartes de stratégie qui examinent le trafic http qui ont été configurés.

```
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
 !
```

- **Policy-map de show running-config** — Affiche tous les configuration de policy-map, aussi bien que configuration de carte de stratégie par défaut.

```
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
!
```

- **service-stratégie de show running-config** — Affiche tous qui exécutent actuellement des configurations de politique de service.

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

Dépanner

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Vous pouvez employer la commande de **show service-policy** afin de vérifier que l'engine d'inspection examine le trafic et correctement les permet ou relâche.

```
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
```

Informations connexes

- ASA/PIX 8.x : Exemple de configuration de blocage de certains sites Web (URL) à l'aide d'expressions régulières avec MPF
- PIX/ASA 7.x et versions ultérieures : Exemple de configuration du blocage du trafic P2P (Peer-to-Peer) et de la messagerie instantanée (IM) à l'aide de MPF
- PIX/ASA 7.x : Exemple de configuration de l'activation des services FTP/TFTP
- Application de l'inspection de protocole de la couche applicative
- Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 – Support
- Cisco Adaptive Security Device Manager (ASDM)
- Dispositifs de sécurité de la gamme Cisco PIX 500 – Support
- Logiciels pare-feu Cisco PIX – Support
- Références de commandes de Logiciels pare-feu Cisco PIX