ASA/PIX 8.x: FTP-sites toestaan/blokkeren met behulp van reguliere expressies met behulp van MPF-configuratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco security applicaties ASA/PIX 8.x kunt configureren die gebruik maakt van reguliere expressies met Modular Policy Framework (MPF) om bepaalde FTP-sites door servernaam te blokkeren of toestaan.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de Cisco security applicatie is geconfigureerd en goed werkt.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5500 Series adaptieve security applicatie (ASA) die de softwareversie 8.0(x) en hoger

uitvoeren
- Cisco Adaptieve Security Devices Manager (ASDM) versie 6.x voor ASA 8.x

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Overzicht van het beleidskader

MPF biedt een consistente en flexibele manier om de functies van security applicaties te configureren. U kunt bijvoorbeeld MPF gebruiken om een tijdelijke configuratie te maken die specifiek is voor een bepaalde TCP-toepassing, in tegenstelling tot een configuratie die van toepassing is op alle TCP-toepassingen.

MPF ondersteunt deze functies:

- TCP-normalisatie, TCP- en UDP-verbindingslimieten en -onderbreking, en TCP-sequentienummer-randomisatie
- CSC
- Toepassingscontrole
- IPS
- QoS-input-toezicht
- QoS-uitvoertoezicht
- QoS-prioriteitswachtrij

De samenstelling van het MPF bestaat uit vier taken:

1. Identificeer Layer 3 en Layer 4 verkeer waarop u acties wilt toepassen. Raadpleeg het Identificeren van verkeer met een Layer 3/4 Class Map voor meer informatie.
2. (Uitsluitend op de toepassing controleren.) Bijzondere maatregelen vaststellen voor toepassingsinspectieverkeer. Zie Speciale acties voor Toepassingsinspecties configureren voor meer informatie.
3. Pas acties op Layer 3 en Layer 4 verkeer toe. Raadpleeg Handelingen definiëren met een Layer 3/4 beleidskaart voor meer informatie.
4. Activeert de acties op een interface. Raadpleeg het gedeelte Layer 3/4-beleid toepassen op een interface met een servicebeleid voor meer informatie.

Normale expressie

Een reguliere expressie komt overeen met tekstreorden letterlijk als een exacte string of met het gebruik van metacharacters, zodat je meerdere varianten van een tekststring kunt vergelijken. U kunt gebruikmaken van een reguliere expressie om de inhoud van een bepaald toepassingsverkeer aan te passen. Bijvoorbeeld, je kunt een URL string in een HTTP pakje

matchen.

Opmerking: Gebruik **Ctrl+V** om alle speciale tekens in de CLI te verwijderen, zoals vraagtekens (?) of tabbladen. Bijvoorbeeld, type **d[Ctrl+V]g** om **d?g** in de configuratie in te voeren.

Gebruik de opdracht **regex** om een reguliere expressie te maken. Bovendien kan de **regex**-opdracht worden gebruikt voor verschillende functies waarvoor tekst moet worden aangepast. U kunt bijvoorbeeld speciale acties voor Application Visibility and Control instellen met behulp van het MPF dat gebruik maakt van een kaart met inspectiebeleid. Raadpleeg de opdracht **voor** inspectie van het **beleid-kaarttype** voor meer informatie.

In de kaart van het inspectiebeleid, kunt u het verkeer identificeren waarop u wilt reageren als u een kaart van de inspectieklasse maakt die één of meer **overeenkomende** opdrachten bevat, of u kunt **wedstrijdopdrachten** rechtstreeks in de kaart van het inspectiebeleid gebruiken. Sommige **overeenkomende** opdrachten laten u tekst in een pakje identificeren met behulp van een reguliere expressie. Bijvoorbeeld, kunt u URL koorden in HTTP pakketten aanpassen. U kunt reguliere expressies groeperen in een class map met reguliere expressies. Raadpleeg de opdracht **class-map type regex** voor meer informatie.

In deze tabel worden de metacharacters weergegeven met speciale betekenis.

karakter	Beschrijving	Opmerkingen
.	punt	Overeenkomsten met één teken. Bijvoorbeeld komt **d.g** overeen met hond, dag, dtg, en elk woord dat die tekens bevat, zoals hondengonnit.
(nl.)	Subexpressie	Een compressie scheidt tekens van omliggende tekens, zodat u andere tekens op de onderdrukking kunt gebruiken. **d(o|a)g** bijvoorbeeld komt overeen met hond en dag, maar **do|ag** overeenkomsten doen en ag. Er kan ook een compressie worden gebruikt met herkende kwantificeringen om een onderscheid te maken tussen de tekens die bij een herhaling moeten worden gebruikt. Bijvoorbeeld, **ab (xy) {3} z** past abxyz aan.
|	Alternatie	Overeenkomsten van een van beide expressies die het scheidt. Bijvoorbeeld **hond |cat** komt overeen met hond of kat.
?	vraagteken	Een kwanfier die aangeeft dat er 0 of 1 van de vorige expressie is. Bijvoorbeeld, **zie?** Zie overeenkomsten verloren of verliezen. **Opmerking:** U moet **Ctrl+V** invoeren en vervolgens het vraagteken of anders wordt de Help-functie opgeroepen.

*	Asterisk	Een kwanfier die aangeeft dat er 0, 1 of een willekeurig aantal van de vorige expressie is. Bijvoorbeeld, **zie*se** overeenkomsten minder, verliezen, los, etc.
{x}	Herhaal kwantificator	Doe precies x keer. Bijvoorbeeld, **ab (xy) {3} z** past abxyz aan.
{x,}	Minimale herhalingskwantificering	Herhaal dit minstens x keer. Bijvoorbeeld, **ab (xy) {2,} z** past bij abxyz, abxyxyz, enz.
[abc]	Tekenklasse	Overeenkomt een teken in de haakjes. Bijvoorbeeld komt **[abc]** overeen met a, b of c.
[^abc]	Negatieve tekenklasse	Overeenkomsten met één teken dat niet tussen de haakjes zit. Bijvoorbeeld, **[^abc]** komt een ander teken aan dan a, b of c. **[^A-Z]** komt overeen met elk teken dat geen hoofdletter is.
[a-c]	Tekenklasse	Overeenkomst met elk teken in het bereik. **[a-z]** komt overeen met elke kleine letter. U kunt tekens en bereik samenvoegen: **[abcq-z]** komt overeen met a, b, c, q, r, s, t, u, v, w, x, y, z, en **[a-cq-z]**. Het streepje (-) teken is alleen letterlijk als het laatste of het eerste teken in de haakjes is: **[abc-]** of **[-abc]**.
""	Quotentietekens	Houdt het tekenen of uitlopen van spaties in de string vast. Bijvoorbeeld, "**test**" behoudt de toonaangevende ruimte wanneer deze op een match zoekt.
^ ^ ^	kleding	Specificeert het begin van een regel.
\	Escape-teken	Bij gebruik met een metacharacter komt een letterlijk teken overeen. Bijvoorbeeld **\[** komt overeen met de linkerkant van de beugel.
klusje	karakter	Wanneer het teken geen metacharacter is, past het letterlijke teken aan.
\r	wagenoord	Overeenkomsten met een vervoersterugkeer: 0x0d.
\n	Nieuws	Overeenkomt een nieuwe regel: 0x0a.
\t	Tab	Overeenkomsten van een tabblad: 0x09.
\f	Formulier	Overeenkomsten met een formulierfeed: 0x0c.

\xNN	Escaped hexadecimaal nummer	Overeenkomst een ASCII-teken dat een hexadecimaal gebruikt dat exact twee cijfers bevat.
\NNN	Verbroken octaal nummer	Overeenkomst een ASCII-teken als octal dat exact drie cijfers bevat. Het teken 040 vertegenwoordigt bijvoorbeeld een ruimte.

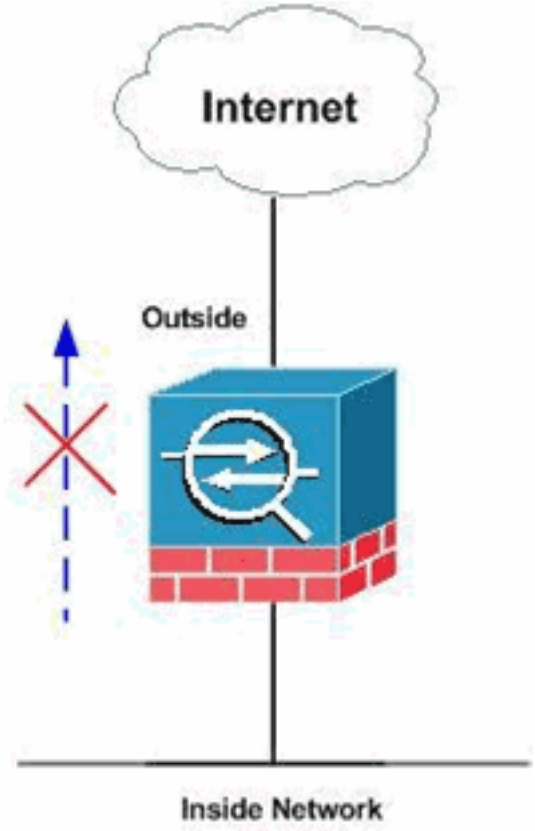
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: Geselecteerde FTP-sites zijn toegestaan of geblokkeerd via reguliere expressies.

Configuraties

Dit document gebruikt deze configuraties:

- ASA CLI-configuratie
- ASA-configuratie 8.x met ASDM 6.x

ASA CLI-configuratie

ASA CLI-configuratie

```
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
```

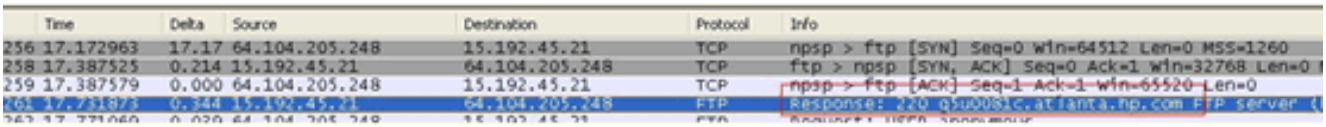
```
! Policy map created in order to define the actions !---
such as drop, reset, or log. policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect h323 h225 inspect h323 ras inspect netbios
inspect rsh inspect rtsp inspect skinny inspect esmtp
inspect sqlnet inspect sunrpc 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
```

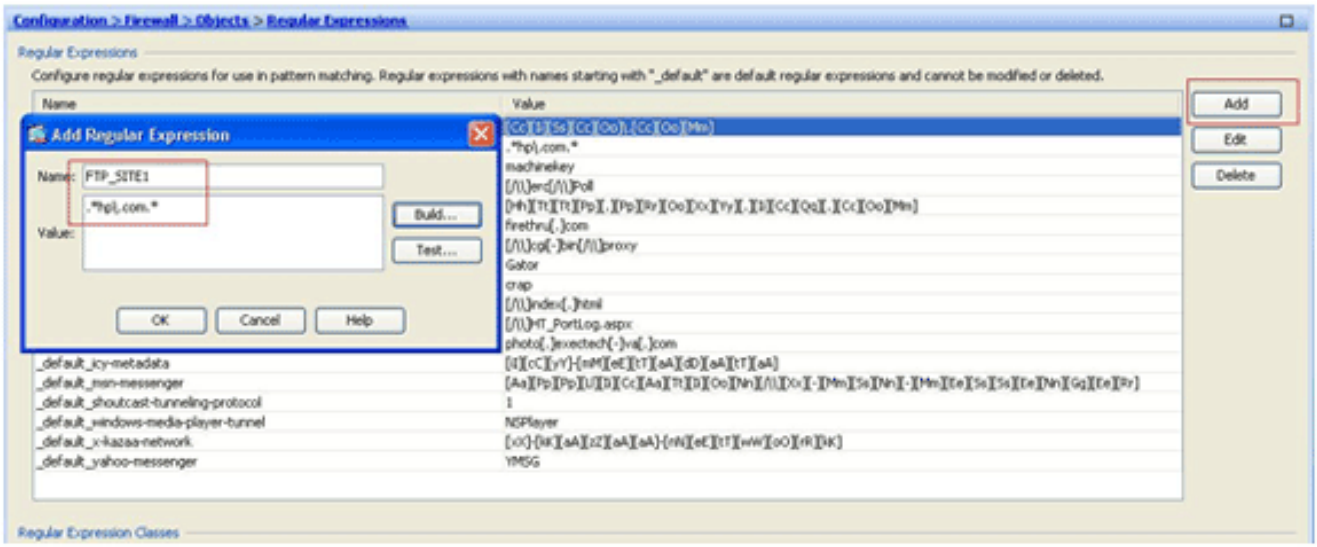
ASA-configuratie 8.x met ASDM 6.x

Voltooi deze stappen om de reguliere expressies te configureren en ze op MPF toe te passen om de specifieke FTP-sites te blokkeren:

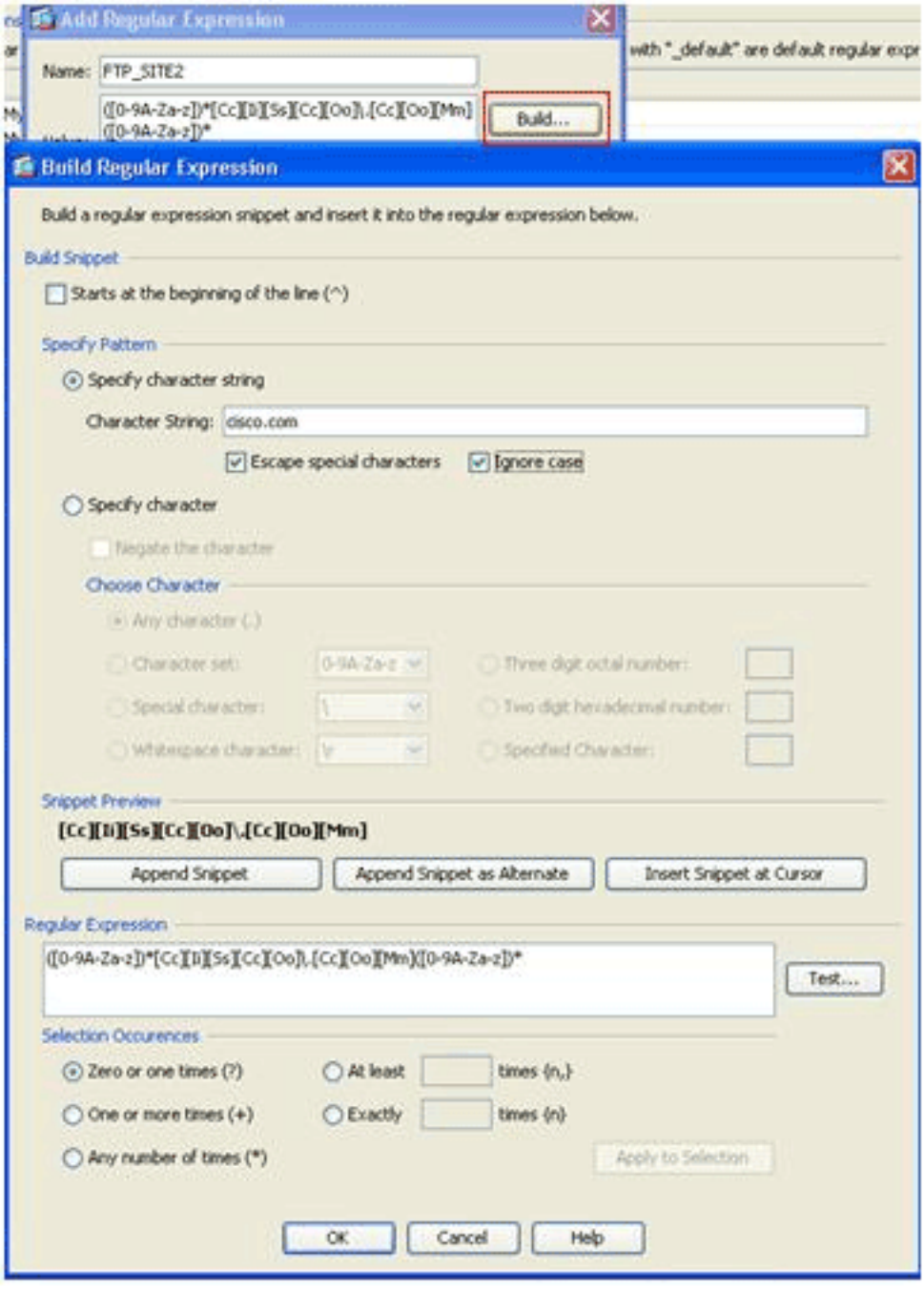
1. **Bepaal de naam van de FTP-server.**De FTP-inspectiemachine kan inspectie bieden aan de hand van verschillende criteria, zoals opdracht, bestandsnaam, bestandstype, server en gebruikersnaam. Deze procedure gebruikt de server als criterium. De FTP-inspectiemotor gebruikt de server 220 respons die door de FTP-site wordt verstuurd als de serverwaarde. Deze waarde kan verschillen met de domeinnaam die door de site wordt gebruikt. Dit voorbeeld gebruikt Wireshark om FTP-pakketten op de website te vangen die wordt geïnspecteerd om de respons 220 waarde te krijgen voor gebruik in onze reguliere expressie in stap
   2.



   Gebaseerd op de opname is de responswaarde 220 voor ftp://hp.com (bijvoorbeeld) *q5u0081c.atlanta.hp.com*.
2. **Reguliere expressies maken.**Kies **Configuration > Firewall > Objects > Reguliere expressies** en klik op **Add** onder het tabblad Reguliere expressie om reguliere expressies te maken zoals in deze procedure wordt beschreven:Maak een reguliere expressie, *FTP_SITE1*, zodat deze overeenkomt met de respons 220 (zoals weergegeven in de pakketvastlegging in Wireshark of enig ander gebruikt gereedschap) die ontvangen is van de ftp site (bijvoorbeeld ".* hp\.com.*") en klik op
   OK.



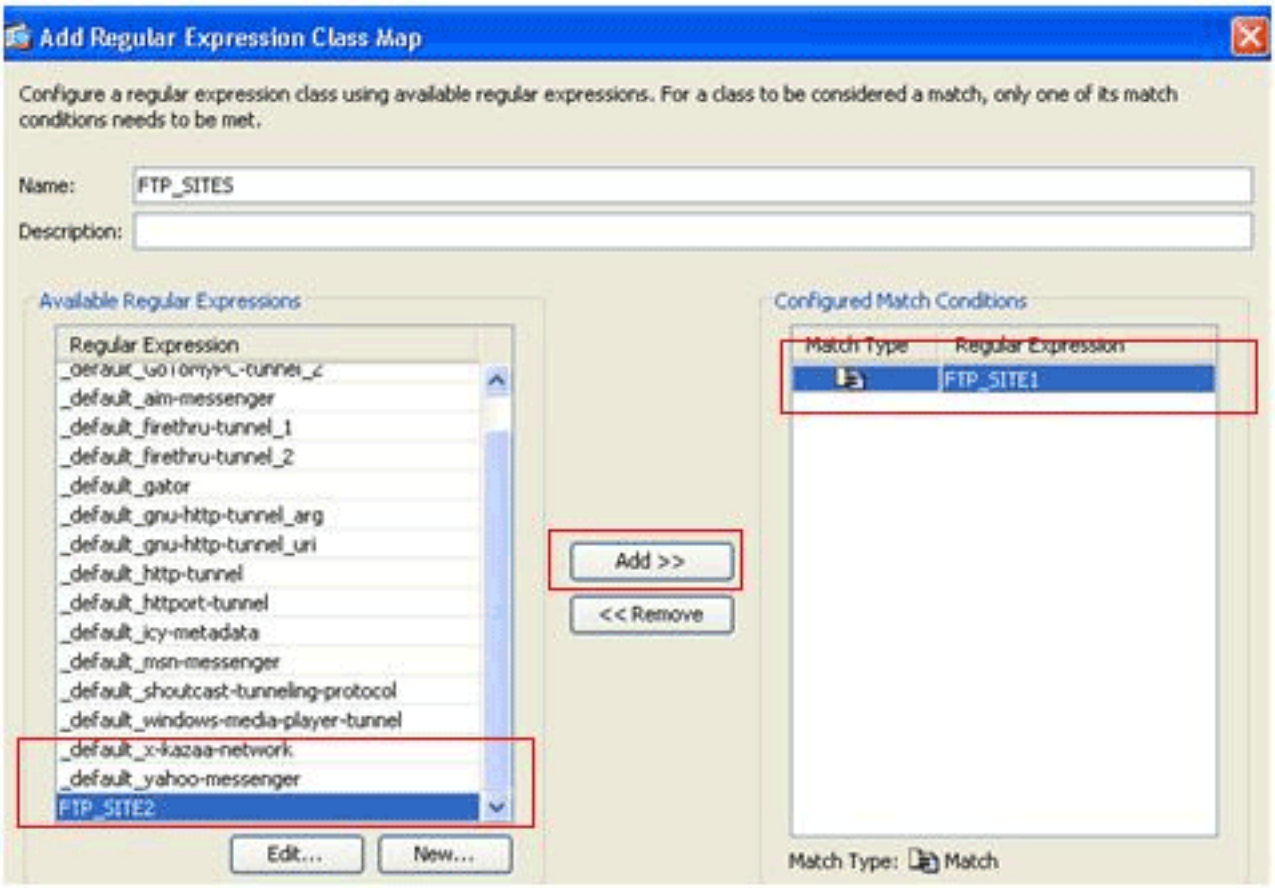
Opmerking: U kunt op **Build** for help klikken om geavanceerde reguliere expressies te



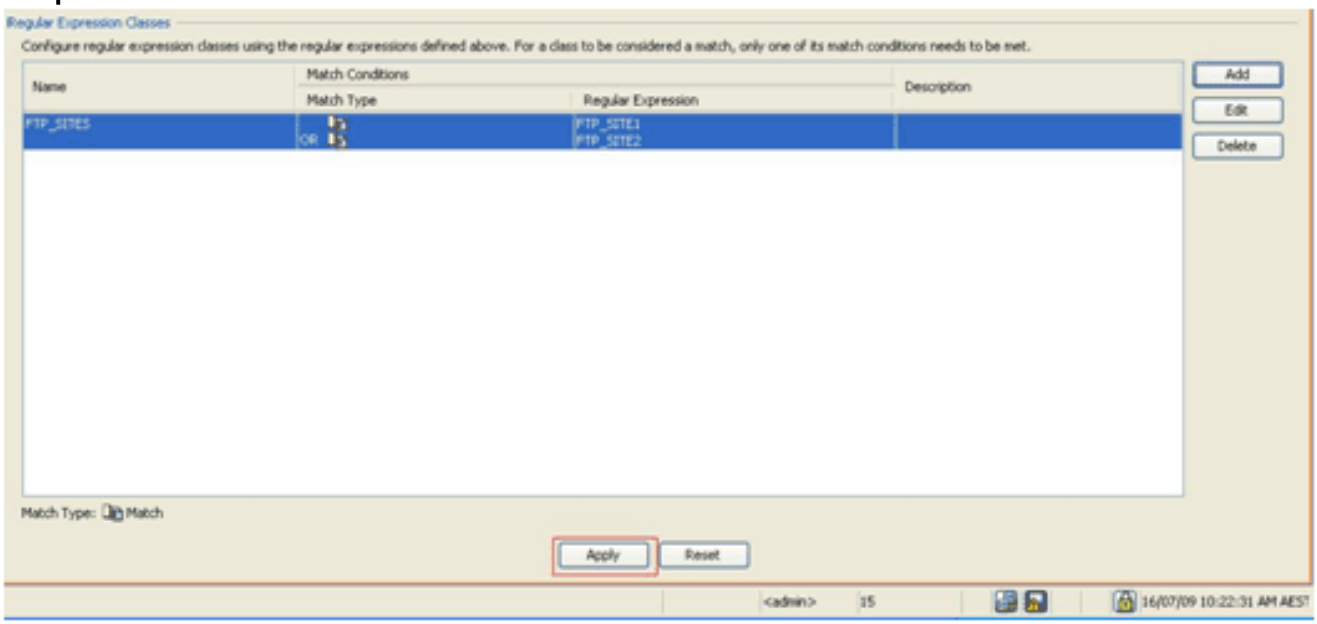
maken. Klik op **Toepassen** als de reguliere expressie is gemaakt.

3. **Maak reguliere expressieklasse.**Kies **Configuration > Firewall > Objects > Reguliere**

expressies en klik op **Add** onder de sectie Reguliere expressie class om de klasse te maken zoals in deze procedure wordt beschreven:Maak een reguliere expressieklasse, *FTP_SITES*, om een van de reguliere expressies *FTP_SITE1* en *FTP_SITE2* aan te passen, en klik op **OK**.

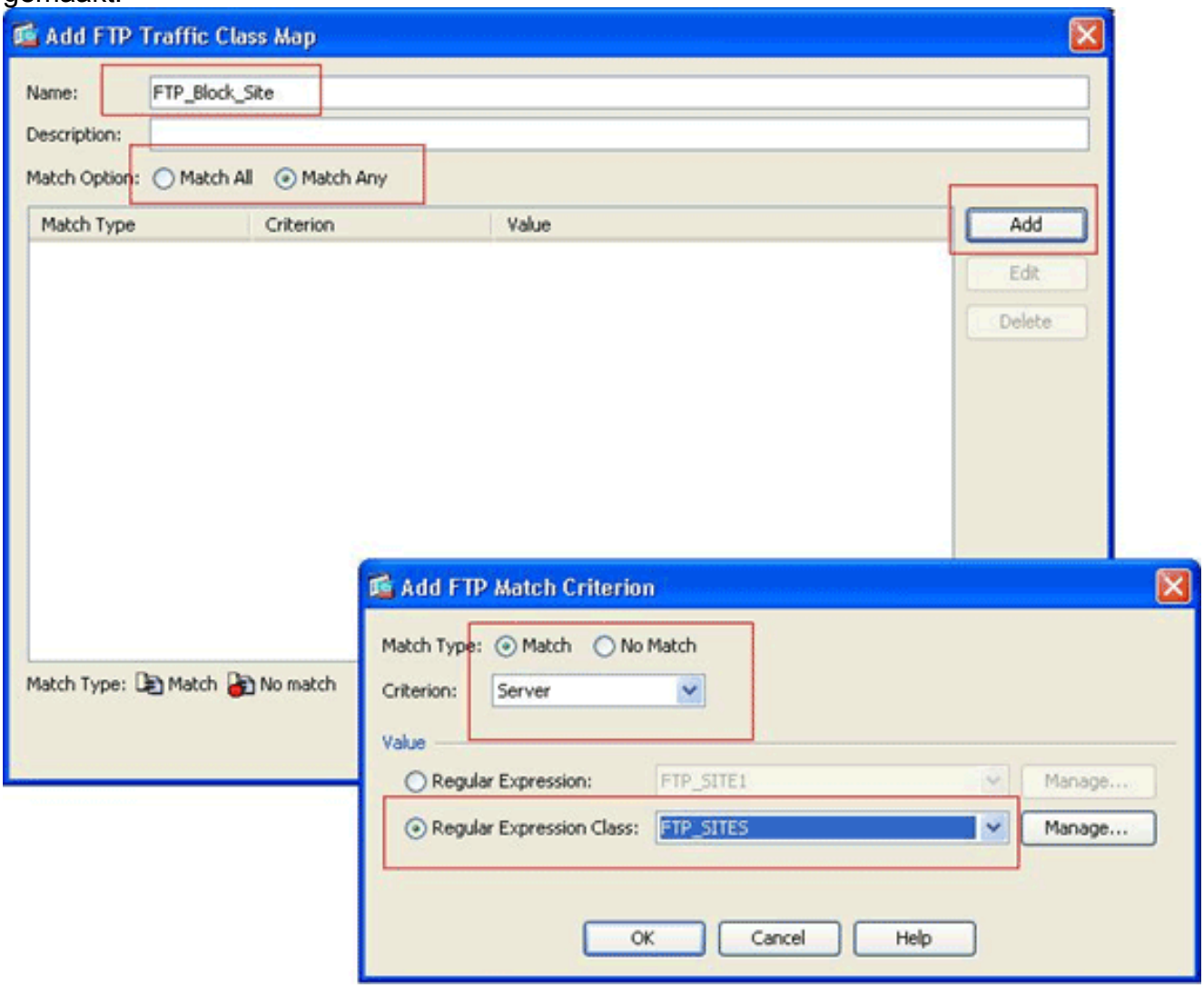


Z odra de class map is aangemaakt, klikt u op **Toepassen**.



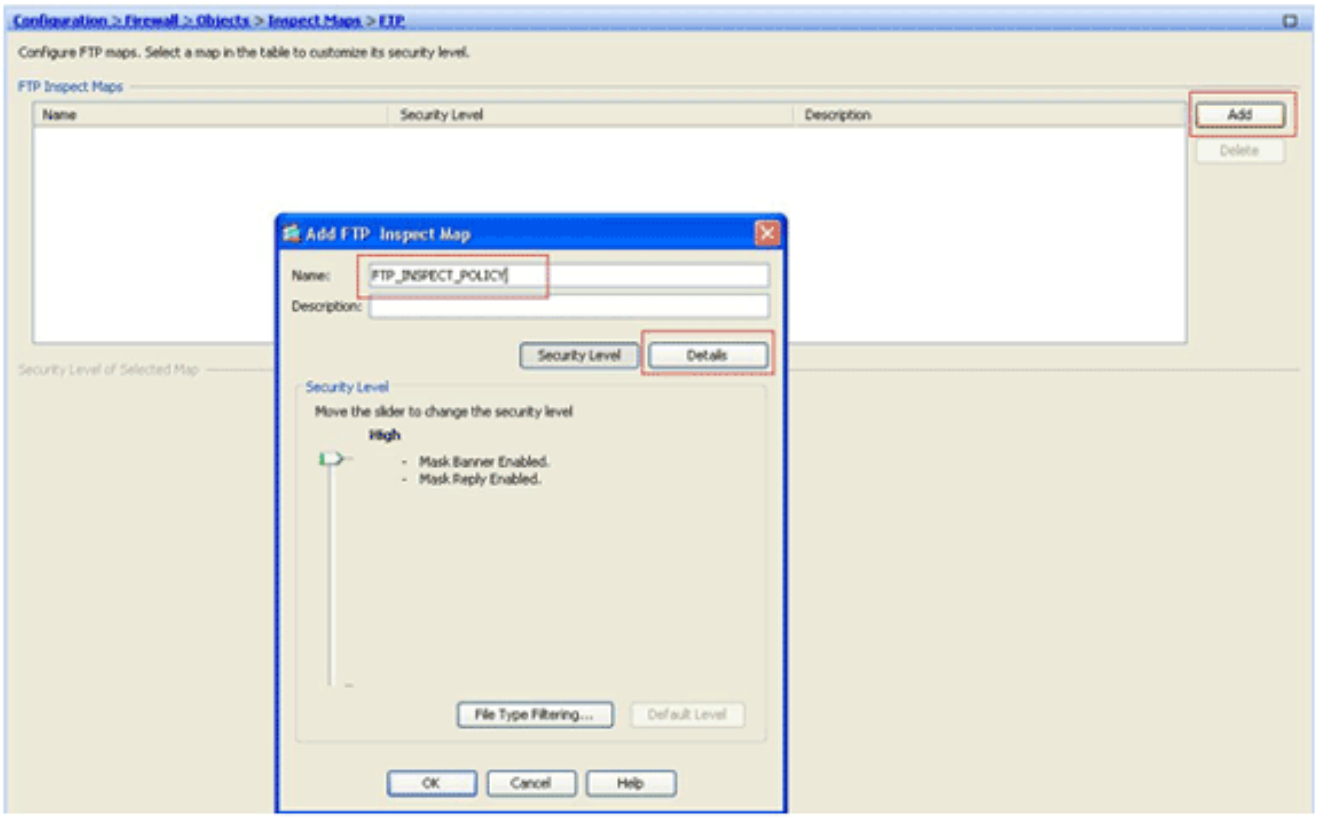
4. **Controleer het geïdentificeerde verkeer met klassenkaarten.**Kies **Configuration > Firewall > Objects > Class Maps > FTP > Add**, klik met de rechtermuisknop en kies **Add** om een class map te maken om het FTP-verkeer te inspecteren dat door verschillende reguliere expressies is geïdentificeerd zoals in deze procedure beschreven:Maak een class map, *FTP_Block_Site*, om de FTP respons 220 aan te passen aan de reguliere expressies die u hebt

gemaakt.

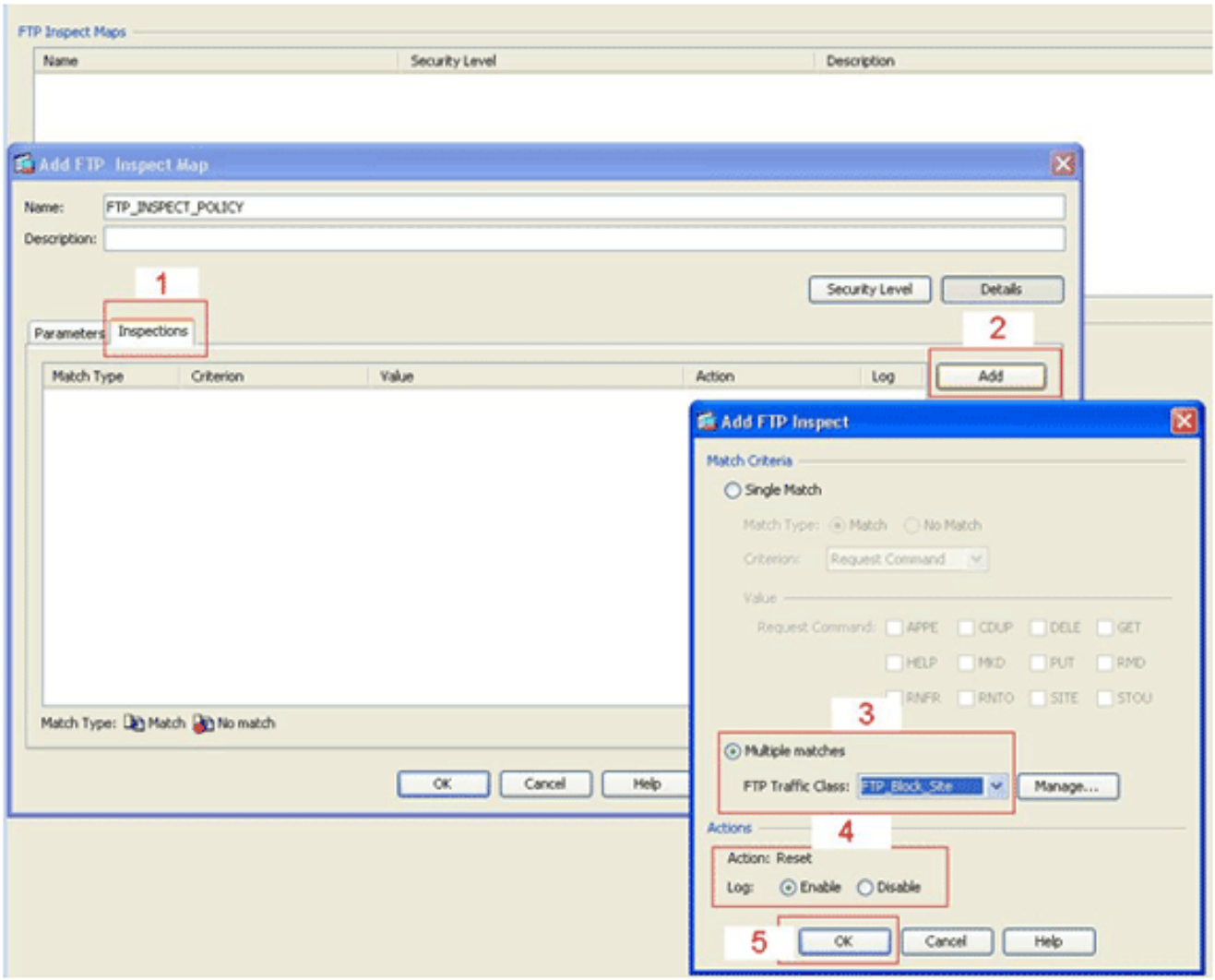


Als u de sites wilt uitsluiten die in de reguliere expressie zijn gespecificeerd, klikt u op het radioknop **Geen overeenstemming**.Selecteer in het gedeelte Waarde een reguliere expressie of een klasse met reguliere expressies. Kies voor deze procedure de class die eerder is gemaakt.Klik op **Toepassen**.

5. **Stel in het inspectiebeleid de maatregelen vast voor het gecompenseerde verkeer.**Kies **Configuration > Firewall > Objects > Inspect Maps > FTP> Add** om een inspectiebeleid te creëren en stel de actie voor het gematchte verkeer in zoals vereist.

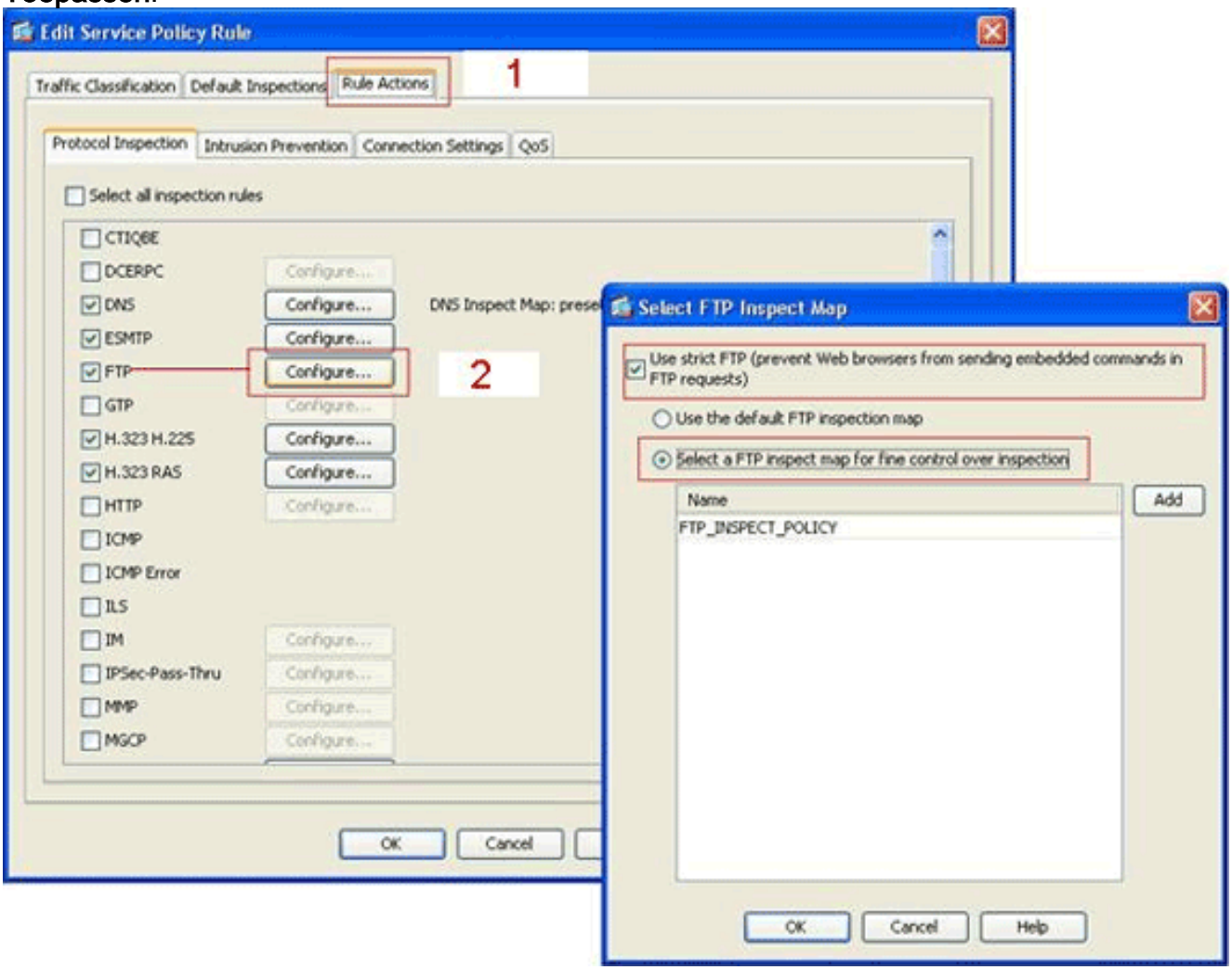


Voer de naam en een beschrijving van het inspectiebeleid in. (Bijvoorbeeld *FTP_INSPECT_POLICY*.)Klik op **Details.**



Klik op het tabblad **Inspecties**. (1)Klik op **Toevoegen**. (2)Klik op de radioknop **Meerdere overeenkomsten** en kies de verkeersklasse in de vervolgkeuzelijst. (3)Kies de gewenste resetactie om in te schakelen of uit te schakelen. Dit voorbeeld maakt het mogelijk om de FTP-verbinding te resetten voor alle FTP-sites *die* niet *overeenkomen* met onze opgegeven sites. (4)Klik op **OK**, klik nogmaals op **OK** en klik vervolgens op **Toepassen**. (5)

6. **Pas het beleid van het inspectiepatroon op de globale controlelijst toe.**Kies **Configuration > Firewall > Service Policy rules**.Aan de rechterkant selecteert u het **inspectie_default** beleid en vervolgens klikt u op **Bewerken**.Klik onder het tabblad Action (1) op de knop **Configureren** voor FTP. (2)In het dialoogvenster Map selecteren als FTP-inspectie controleert u het vakje **FTP** gebruiken en vervolgens klikt u op de **map FTP-inspectie om de** radioknop **van de inspectie te controleren**.Het nieuwe FTP inspectie beleid, *FTP_INSPECT_POLICY*, moet in de lijst zichtbaar zijn.Klik op **OK**, klik nogmaals op **OK** en klik vervolgens op **Toepassen**.



Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **tonen in werking stellen-in werking stellen regex**-Toont de regelmatige expressies die zijn gevormd.

```
ciscoasa#show running-configregex
```

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

- **tonen in werking stellen-in werking stellen-enig klembord**-toont de class kaarten die zijn gevormd.

```
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
!
```

- **toon in werking stellen-in werking stellen politiek-kaart type inspectie http**-Toont de beleidskaarten die het HTTP verkeer inspecteren dat is gevormd.

```
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
 !
```

- **Toon in werking stellen-in werking stellen-enig beleid-kaart**-Toont alle beleidskaartconfiguraties, zowel als de standaardbeleidskaartconfiguratie.

```
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
!
```

- **toon in werking stellen-wijk service-beleid**-Toont alle momenteel in werking zijnde de dienstbeleidsconfiguraties.

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

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

U kunt de opdracht **showservice-beleid** gebruiken om te controleren of de inspectiemachine het verkeer inspecteert en het verkeer op de juiste manier toestaat of laat vallen.

```
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
```

Gerelateerde informatie

- ASA/PIX 8.x: Blokkeer bepaalde websites (URL's) met behulp van reguliere expressies met behulp van een MPF-configuratievoorbeeld
- PIX/ASA 7.x en later: Blokkeer het peer-to-peer (P2P) en Instant Messaging (IM) verkeer met behulp van MPF-configuratievoorbeeld
- PIX/ASA 7.x: Configuratievoorbeeld van FTP/TFTP-services inschakelen
- Toepassend Application Layer Protocol-inspectie
- Cisco ASA 5500 Series adaptieve security applicaties - ondersteuning
- Cisco Adaptieve Security Devices Manager (ASDM)
- Cisco PIX 500 Series security applicaties - ondersteuning
- Cisco PIX-firewallsoftware - ondersteuning
- Cisco PIX-firewall-softwarefuncties