ASA/PIX 8.x: FTP-Sites mit regulären Ausdrücken mit MPF-Konfigurationsbeispiel zulassen/blockieren

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Cisco Security Appliances ASA/PIX 8.x konfigurieren, die reguläre Ausdrücke mit Modular Policy Framework (MPF) verwenden, um bestimmte FTP-Sites über den Servernamen zu blockieren oder zuzulassen.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass die Cisco Security Appliance konfiguriert ist und ordnungsgemäß funktioniert.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance (ASA) der Serie 5500 mit Softwareversion 8.0(x) und höher
- Cisco Adaptive Security Device Manager (ASDM) Version 6.x für ASA 8.x

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Übersicht über das modulare Richtlinien-Framework

MPF bietet eine konsistente und flexible Möglichkeit zur Konfiguration von Security Appliance-Funktionen. Beispielsweise können Sie mit MPF eine Timeout-Konfiguration erstellen, die für eine bestimmte TCP-Anwendung spezifisch ist, im Gegensatz zu einer Konfiguration, die für alle TCP-Anwendungen gilt.

MPF unterstützt folgende Funktionen:

- TCP-Normalisierung, TCP- und UDP-Verbindungsbeschränkungen und -Timeouts sowie Randomisierung der TCP-Sequenznummern
- CSC
- Anwendungsinspektion
- IPS
- QoS-Eingangsüberwachung
- QoS-Output-Policing
- QoS-Prioritätswarteschlange

Die MPF-Konfiguration umfasst vier Aufgaben:

1. Identifizieren Sie den Layer-3- und Layer-4-Datenverkehr, auf den Sie Aktionen anwenden möchten. Weitere Informationen finden Sie unter Identifizieren von Datenverkehr mithilfe einer Layer-3/4-Klassenzuordnung.
2. (Nur Anwendungsinspektion) Definieren spezieller Aktionen für Anwendungsinspektionsdatenverkehr. Weitere Informationen finden Sie unter Konfigurieren von Sonderaktionen für Anwendungsinspektionen.
3. Wenden Sie Aktionen auf den Layer-3- und Layer-4-Datenverkehr an. Weitere Informationen finden Sie unter Definieren von Aktionen mithilfe einer Layer-3/4-Richtlinienzuordnung.
4. Aktivieren Sie die Aktionen auf einer Schnittstelle. Weitere Informationen finden Sie unter Anwenden einer Layer-3/4-Richtlinie auf eine Schnittstelle mithilfe einer Dienstrichtlinie.

Regulärer Ausdruck

Ein regulärer Ausdruck ordnet Textzeichenfolgen entweder wörtlich als exakte Zeichenfolge oder mithilfe von Metazeichen zu, sodass Sie mehrere Varianten einer Zeichenfolge zuordnen können.

Sie können einen regulären Ausdruck verwenden, um den Inhalt des bestimmten Anwendungsdatenverkehrs abzugleichen. Beispielsweise können Sie eine URL-Zeichenfolge innerhalb eines HTTP-Pakets zuordnen.

Hinweis: Verwenden Sie **Strg+V**, um alle Sonderzeichen in der CLI zu entfernen, z. B. Fragezeichen (?) oder Registerkarten. Geben Sie z. B. **d[Strg+V]g ein**, um **d?g** in die Konfiguration einzugeben.

Um einen regulären Ausdruck zu erstellen, verwenden Sie den Befehl **regex**. Darüber hinaus kann der Befehl **regex** für verschiedene Funktionen verwendet werden, die eine Textzählung erfordern. Sie können z. B. spezielle Aktionen für die Anwendungsinspektion konfigurieren, indem Sie die MPF verwenden, die eine Inspektionsrichtlinienzuordnung verwendet. Weitere Informationen finden Sie im Befehl **policy-map type inspect (Richtlinienzuordnung)**.

In der Richtlinienzuordnung für die Inspektionsrichtlinien können Sie den Datenverkehr identifizieren, für den Sie handeln möchten, wenn Sie eine Klassenzuordnung für die Inspektion erstellen, die mindestens einen **Übereinstimmungsbefehl** enthält, oder Sie können **Übereinstimmungsbefehle** direkt in der Richtlinienzuordnung für die Inspektion verwenden. Mit einigen **Übereinstimmungsbefehlen** können Sie Text in einem Paket mithilfe eines regulären Ausdrucks identifizieren. Beispielsweise können Sie URL-Zeichenfolgen in HTTP-Paketen zuordnen. Sie können reguläre Ausdrücke in einer Klassenzuordnung für reguläre Ausdrücke gruppieren. Weitere Informationen finden Sie im Befehl **class-map type regex**.

In dieser Tabelle sind die Metazeichen mit speziellen Bedeutungen aufgeführt.

Zeichen	Beschreibung	Hinweise
.	Punkt	Entspricht einem beliebigen Zeichen. Beispielsweise stimmt **d.g** mit Hund, Dag, dtg und jedem Wort überein, das diese Zeichen enthält, z. B. dogonnit.
(exp)	Unterdrückung	Ein Teilausdruck trennt Zeichen von umgebenden Zeichen, sodass Sie für den Unterausdruck andere Metazeichen verwenden können. So gleicht **d(o|a)g** Hund und Dag, aber **do|ag** Übereinstimmungen tun und ag. Ein Teilausdruck kann auch mit Wiederholquantifizierern verwendet werden, um die für Wiederholungen bestimmten Zeichen zu unterscheiden. Beispielsweise entspricht **ab(xy){3}z** Abxyxyxyz.
\| | Alternative | Entspricht einem Ausdruck, den er trennt. So passt **dog\|cat** Hund oder Katze. |
? | Fragezeichen | Ein Quantifizierer, der angibt, dass 0 oder 1 des vorherigen Ausdrucks vorhanden ist. Zum Beispiel **lo?se** |

		Matches verlieren oder verlieren. **Hinweis:** Sie müssen **Strg+V** eingeben und dann das Fragezeichen eingeben. Andernfalls wird die Hilfefunktion aufgerufen.
*	Asterisk	Ein Quantifizierer, der angibt, dass 0, 1 oder eine beliebige Zahl des vorherigen Ausdrucks vorhanden ist. Zum Beispiel **lo*se** gleicht weniger, verlieren, locker usw. aus.
{x}	Quantifizierer wiederholen	Wiederholen Sie die Schritte genau x mal. Beispielsweise entspricht **ab(xy){3}z** Abxyxyxyz.
{x,}	Mindestwiederholquantifizierer	Wiederholen Sie diese Schritte mindestens x. Zum Beispiel entsprechen **ab(xy){2,}z** Abxyz, Abxyxyxyxyxyz usw.
[abc]	Character-Klasse	Entspricht einem beliebigen Zeichen in den Klammern. Zum Beispiel **[abc]** stimmt mit a, b oder c überein.
[^abc]	Negative Zeichenklasse	Entspricht einem einzelnen Zeichen, das nicht in Klammern enthalten ist. Beispielsweise **[^abc]** stimmt mit einem beliebigen Zeichen außer a, b oder c überein. **[^A-Z]** Entspricht einem beliebigen Zeichen, das kein Großbuchstabe ist.
[a-c]	Zeichenbereichsklasse	Entspricht einem beliebigen Zeichen im Bereich. **[a-z]** stimmt mit jedem Kleinbuchstaben überein. Sie können Zeichen und Bereiche mischen: **[abcq-z]** stimmt mit a, b, c, q, r, s, t, u, v, w, x, y, z überein, und dasselbe gilt für **[a-cq-z]**. Das Bindestrich (-)-Zeichen ist nur dann literal, wenn es sich um das letzte oder das erste Zeichen in den Klammern handelt: **[abc-]** oder **[-abc]**.
""	Anführungszeichen	Bewahrt nachfolgende oder führende Leerzeichen in der Zeichenfolge. Beispielsweise behält **" test"** bei der Suche nach einer Übereinstimmung das führende Leerzeichen bei.
^	Sorgfalt	Gibt den Beginn einer Zeile an.
\	Escape-Zeichen	Bei Verwendung mit einem Metazeichen wird einem literalen

		Zeichen entsprochen. Beispiel: **\[** stimmt mit der linken quadratischen Klammer überein.
Char	Zeichen	Wenn das Zeichen kein Metazeichen ist, entspricht es dem literalen Zeichen.
\r	Frachtrücksendung	Entspricht einem Wagenrücklauf: 0x0d.
\n	Netzkabel	Entspricht einem neuen Posten: 0x0a.
\t	Registerkarte	Ordnet eine Registerkarte zu: 0 x 09.
\f	Vorspeise	Entspricht einem Formularvorschub: 0x0c.
\xNN	Hexadezimalzahl mit Escapezeichen	Entspricht einem ASCII-Zeichen, das ein Hexadezimalzeichen mit genau zwei Ziffern verwendet.
\NNN	Escaped Oktalnummer	Entspricht einem ASCII-Zeichen einem Oktal, das genau drei Ziffern umfasst. Beispielsweise stellt das Zeichen 040 ein Leerzeichen dar.

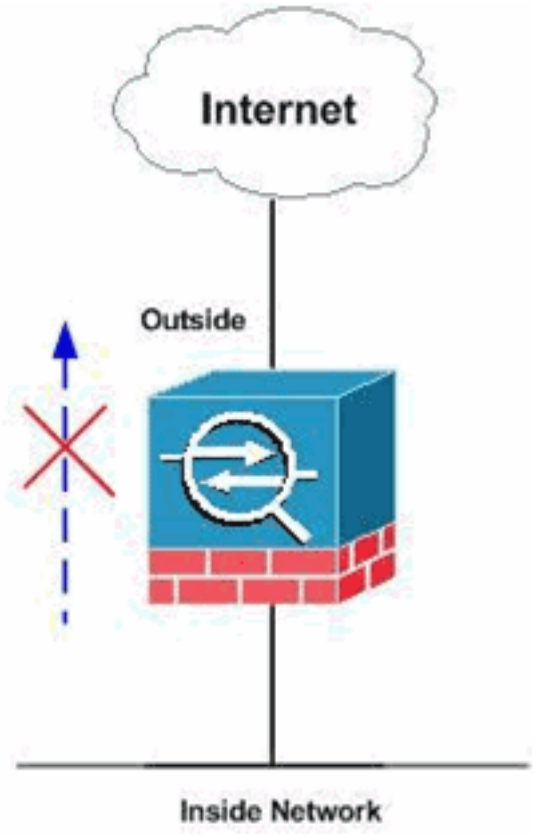
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Ausgewählte FTP-Sites sind mit regulären Ausdrücken zulässig oder blockiert.

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- ASA CLI-Konfiguration
- ASA-Konfiguration 8.x mit ASDM 6.x

ASA CLI-Konfiguration

ASA CLI-Konfiguration

```
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
```

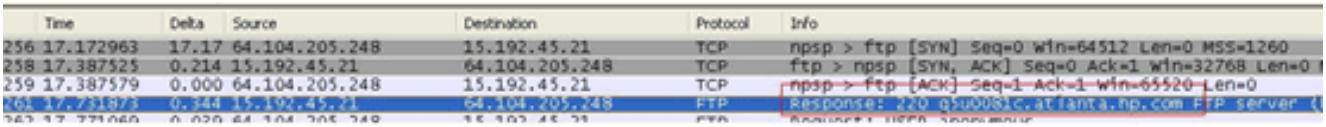
```
telnet timeout 5
ssh scopy enable
ssh timeout 5
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept


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-Konfiguration 8.x mit ASDM 6.x

Gehen Sie wie folgt vor, um die regulären Ausdrücke zu konfigurieren und sie auf MPF anzuwenden, um die spezifischen FTP-Sites zu blockieren:

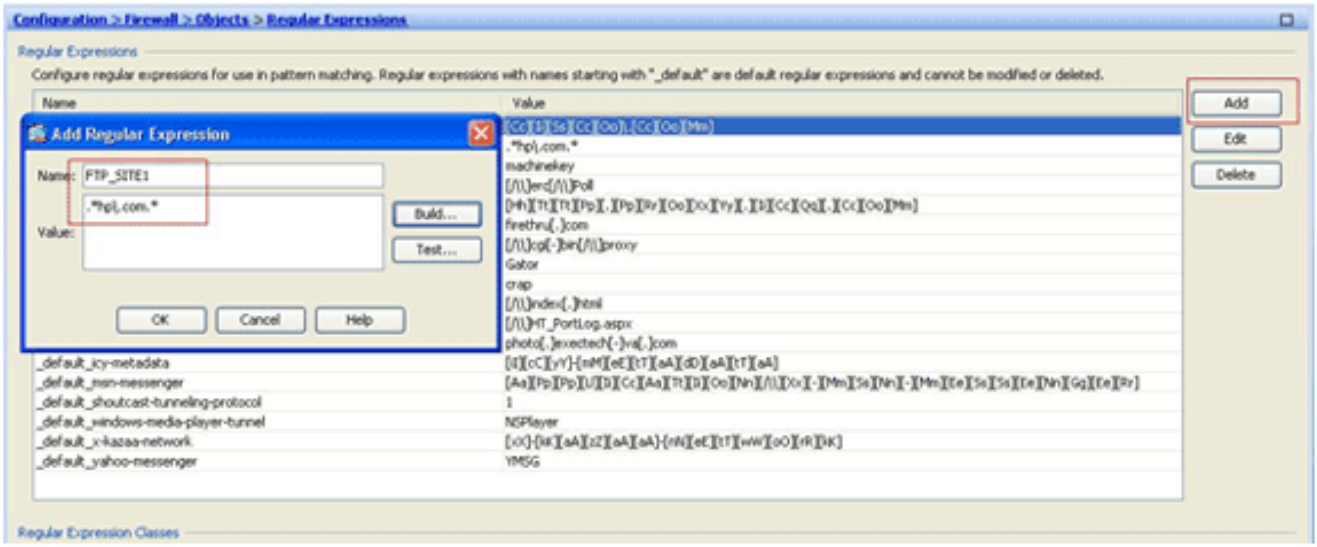
1. **Bestimmen Sie den Namen des FTP-Servers.**Die FTP Inspection Engine kann Prüfungen anhand unterschiedlicher Kriterien wie Befehl, Dateiname, Dateityp, Server und Benutzername durchführen. Bei diesem Verfahren wird der Server als Kriterium

herangezogen. Die FTP Inspection Engine verwendet die Server 220-Antwort, die von der FTP-Site als Serverwert gesendet wurde. Dieser Wert kann sich vom Domänennamen der Site unterscheiden. In diesem Beispiel wird Wireshark verwendet, um FTP-Pakete an die Website zu erfassen, die überprüft werden, um den Wert response 220 für den in Schritt 2 verwendeten regulären Ausdruck
abzurufen.

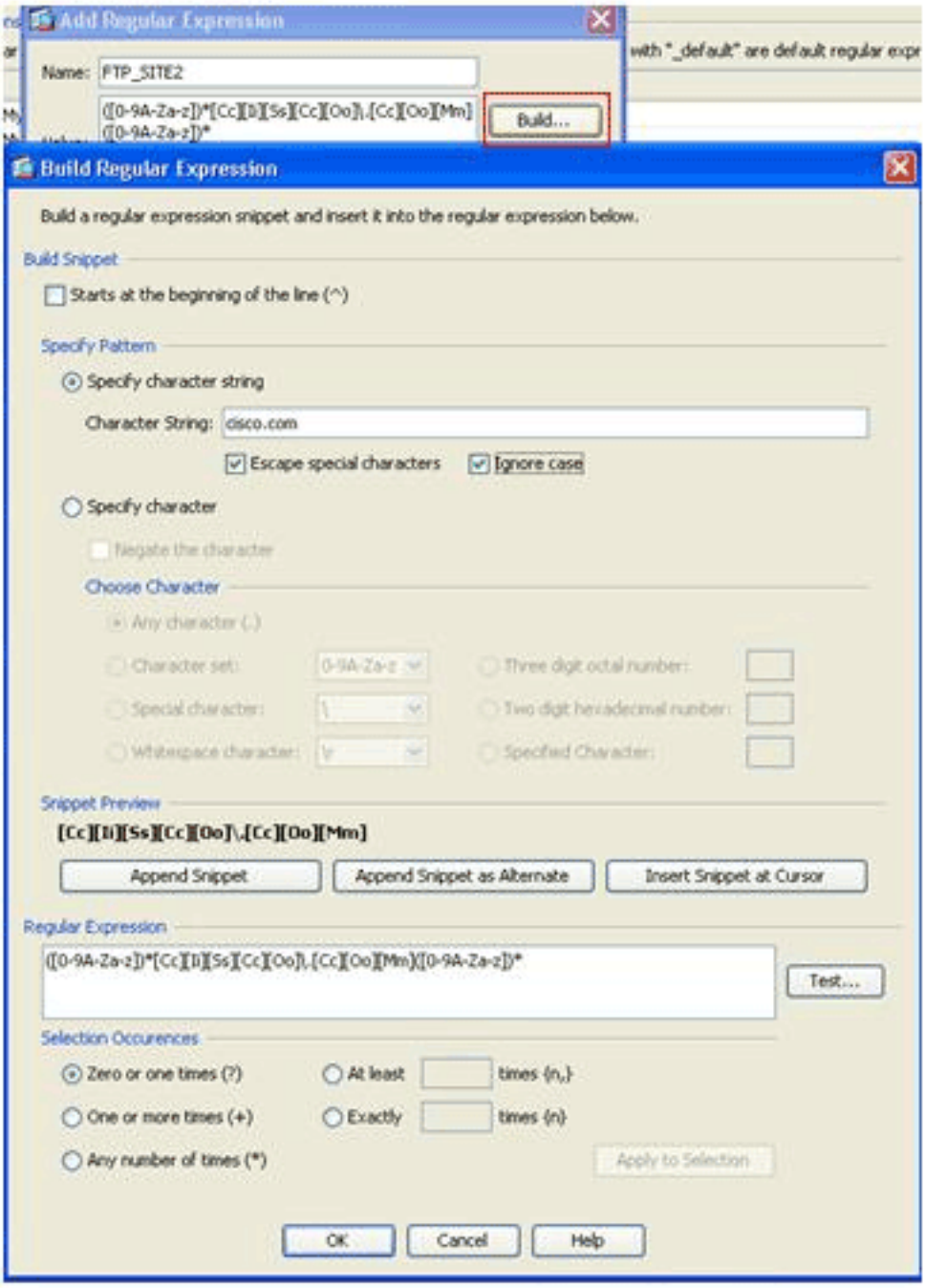


Basierend auf der Erfassung lautet der Wert für die Antwort 220 für ftp://hp.com (z. B.) *q5u0081c.atlanta.hp.com*.

2. **Erstellen Sie reguläre Ausdrücke.**Wählen Sie **Konfiguration > Firewall > Objekte > Reguläre Ausdrücke**, und klicken Sie unter der Registerkarte Regulärer Ausdruck auf **Hinzufügen**, um reguläre Ausdrücke wie in diesem Verfahren beschrieben zu erstellen:Erstellen Sie einen regulären Ausdruck, *FTP_SITE1*, um die Antwort 220 (wie in der Paketerfassung in Wireshark oder einem anderen verwendeten Tool dargestellt) zu erreichen, die Sie von der FTP-Site erhalten haben (z. B. ".* hp\.com.*"), und klicken Sie auf
OK.

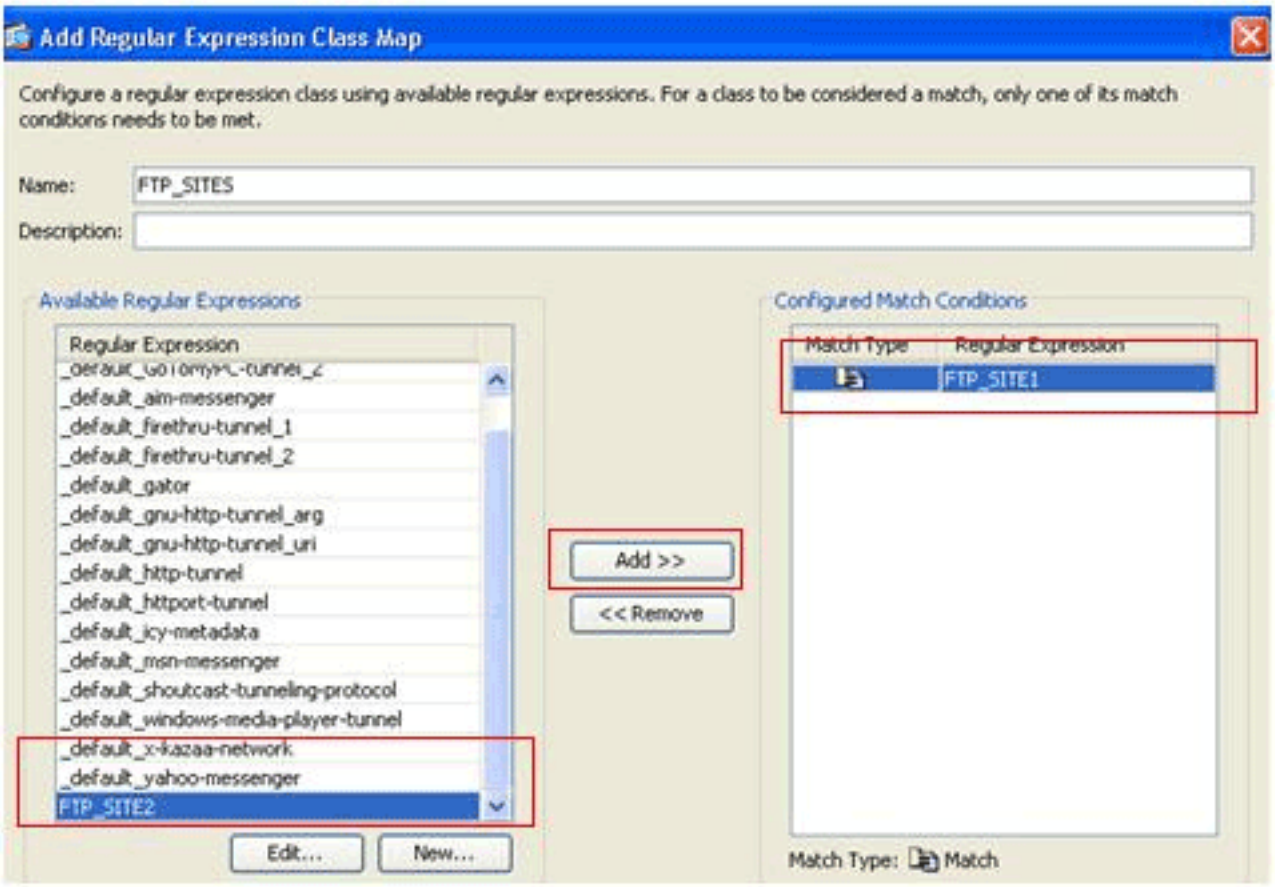


Hinweis: Sie können auf **Erstellen** klicken, um Hilfe zum Erstellen von erweiterten regulären Ausdrücken zu

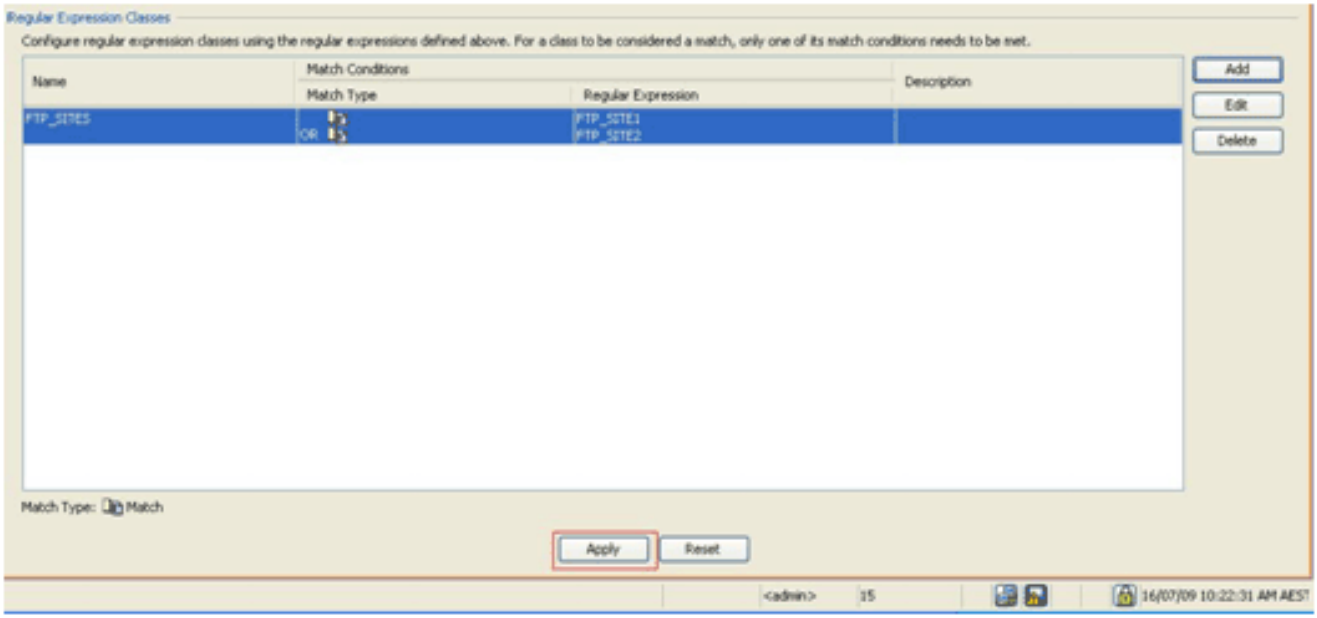


erhalten. Nachdem der reguläre Ausdruck erstellt wurde, klicken Sie auf **Übernehmen.**

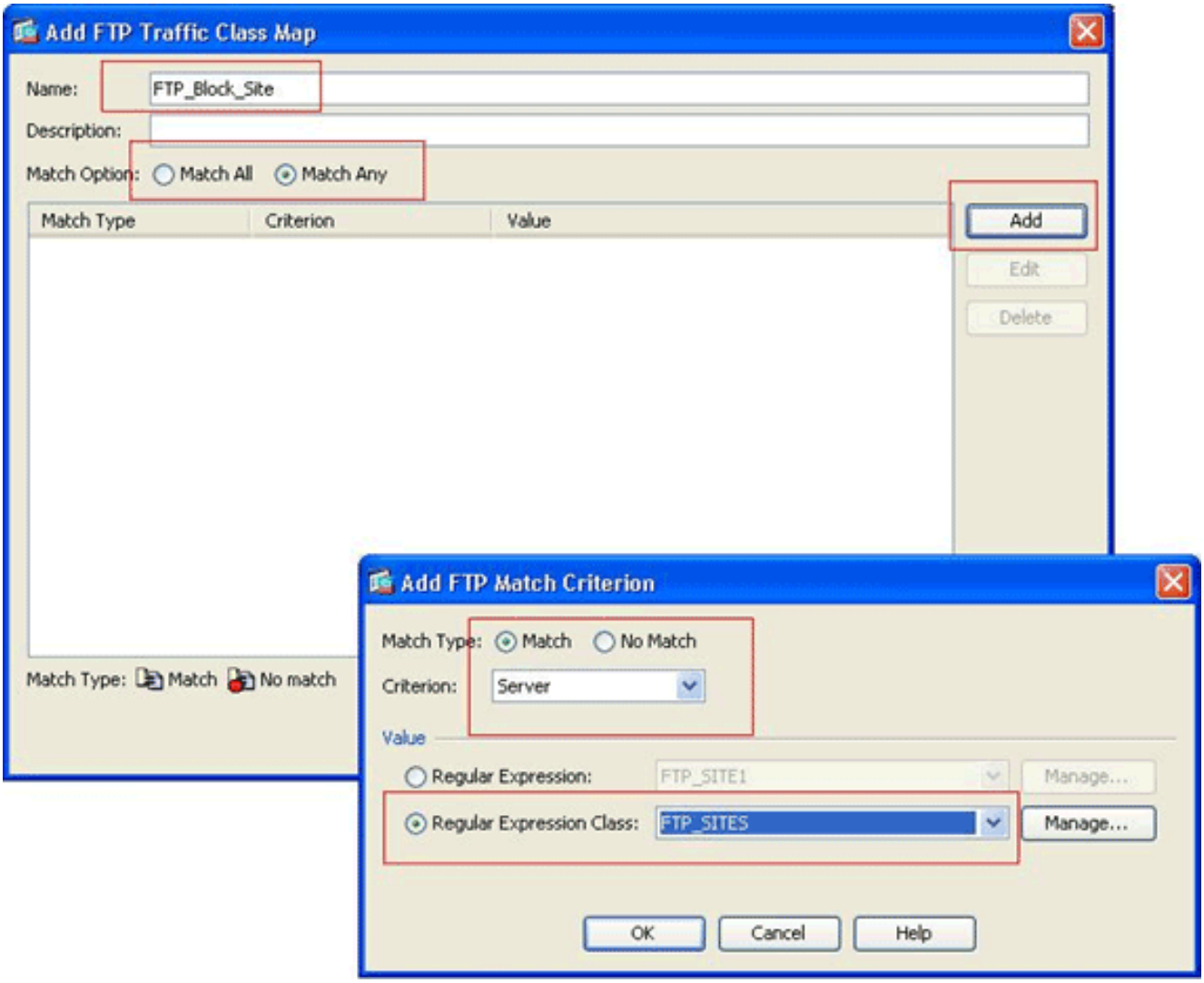
3. **Erstellen von Klassen für reguläre Ausdrücke.**Wählen Sie **Konfiguration > Firewall > Objekte > Reguläre Ausdrücke**, und klicken Sie im Abschnitt Klassen regulärer Ausdrücke auf **Hinzufügen**, um die in diesem Verfahren beschriebene Klasse zu erstellen:Erstellen Sie eine Klasse für reguläre Ausdrücke, *FTP_SITES*, um einen der regulären Ausdrücke *FTP_SITE1* und *FTP_SITE2* abzustimmen, und klicken Sie auf **OK**.



Wenn die Klassenzuordnung erstellt wurde, klicken Sie auf **Übernehmen**.

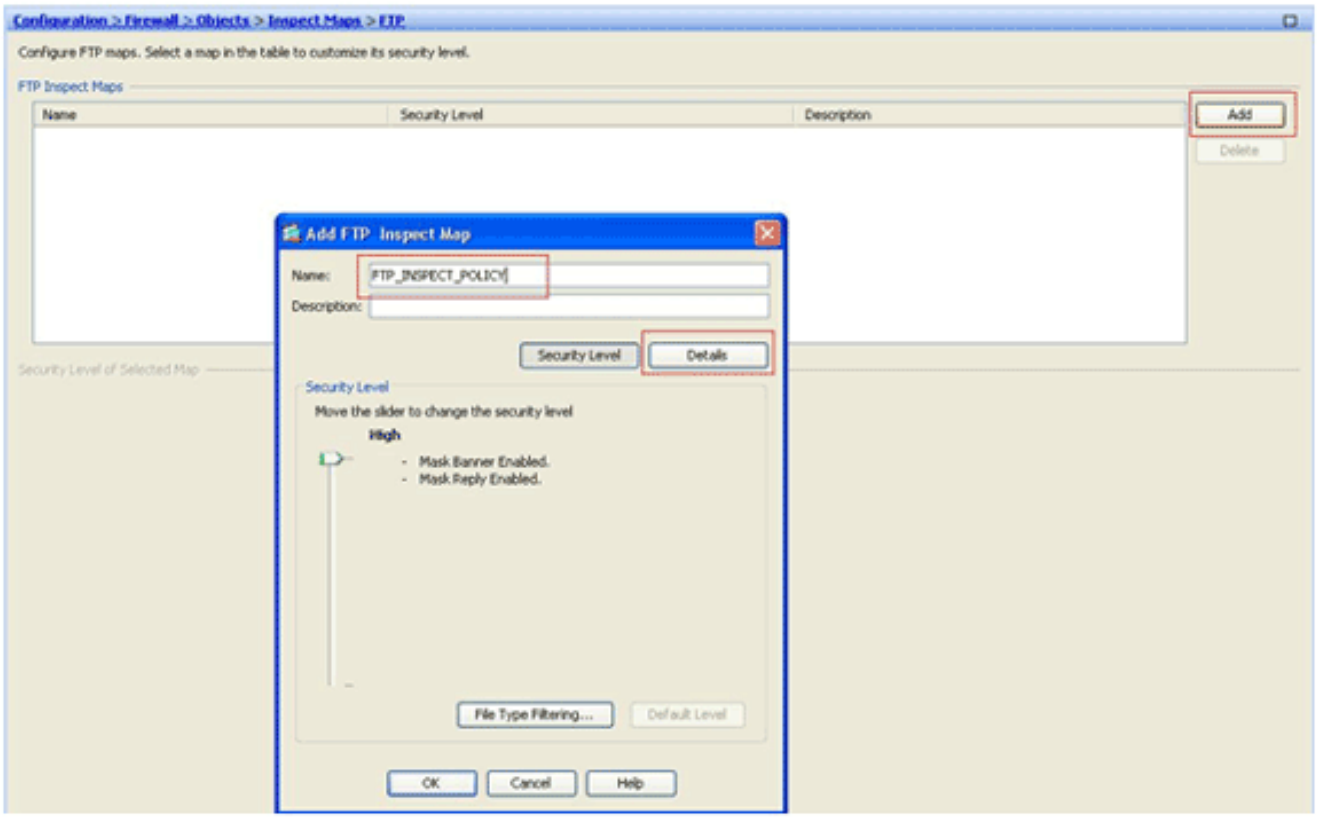


4. **Überprüfen Sie den identifizierten Datenverkehr mit Klassenzuordnungen.**Wählen Sie **Configuration > Firewall > Objects > Class Maps > FTP > Add**, klicken Sie mit der rechten Maustaste, und wählen Sie **Add** aus, um eine Klassenzuordnung zu erstellen, um den FTP-Datenverkehr zu überprüfen, der durch verschiedene reguläre Ausdrücke wie in diesem Verfahren beschrieben identifiziert wurde:Erstellen Sie eine Klassenzuordnung, *FTP_Block_Site*, um die FTP-Antwort 220 mit den von Ihnen erstellten regulären Ausdrücken abzugleichen.

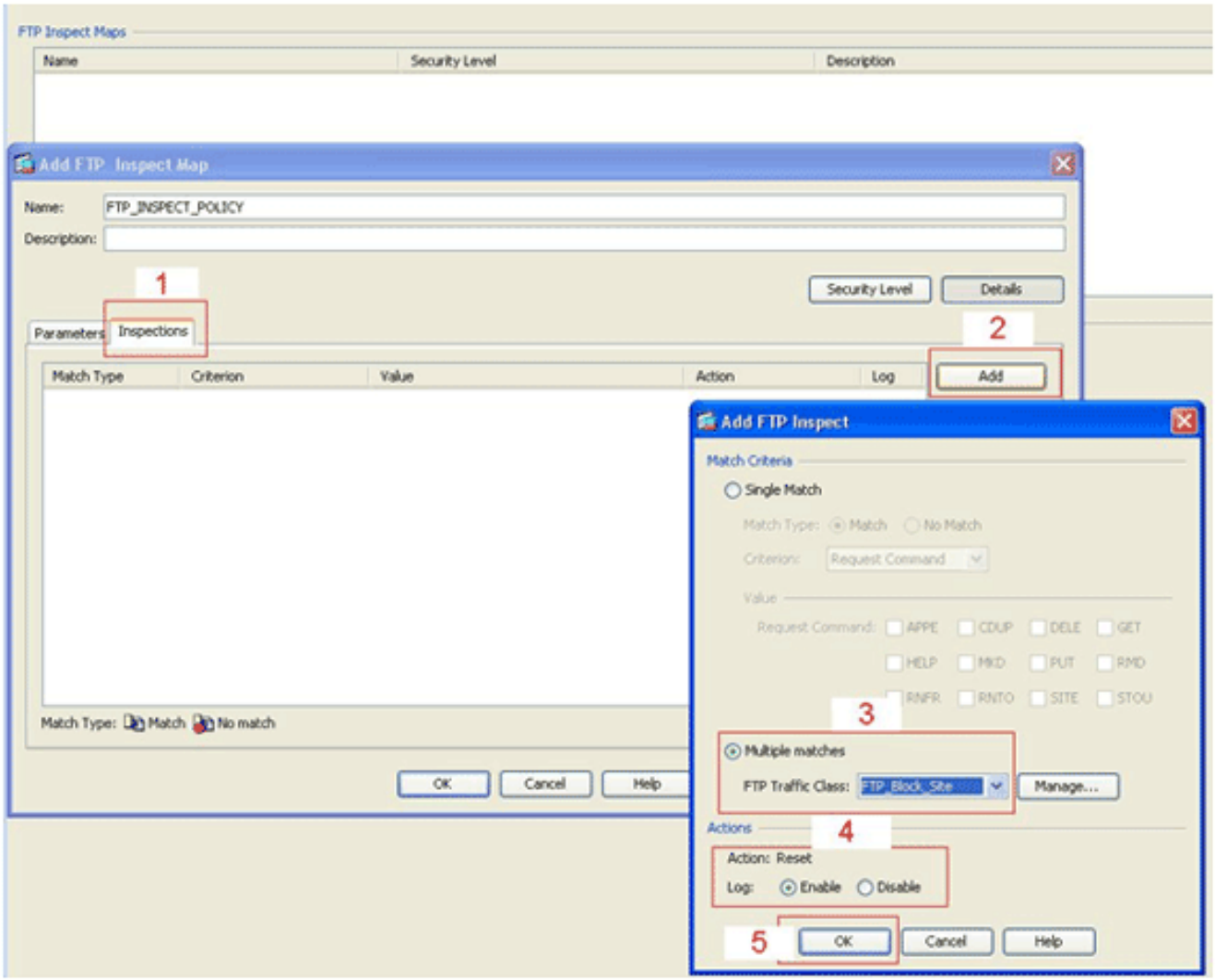


Wenn Sie die im regulären Ausdruck angegebenen Sites ausschließen möchten, klicken Sie auf das Optionsfeld **Keine Übereinstimmung**.Wählen Sie im Abschnitt Wert entweder einen regulären Ausdruck oder eine Klasse für reguläre Ausdrücke aus. Wählen Sie für diese Prozedur die Klasse aus, die zuvor erstellt wurde.Klicken Sie auf **Übernehmen**.

5. **Legen Sie die Aktionen für den zugeordneten Datenverkehr in der Überprüfungsrichtlinie fest.**Wählen Sie **Configuration > Firewall > Objects > Inspect Maps > FTP> Add (Konfiguration > Firewall > Objekte > Inspection Maps > FTP> Add** aus, um eine Überprüfungsrichtlinie zu erstellen, und legen Sie die Aktion für den zugeordneten Datenverkehr bei Bedarf
fest.

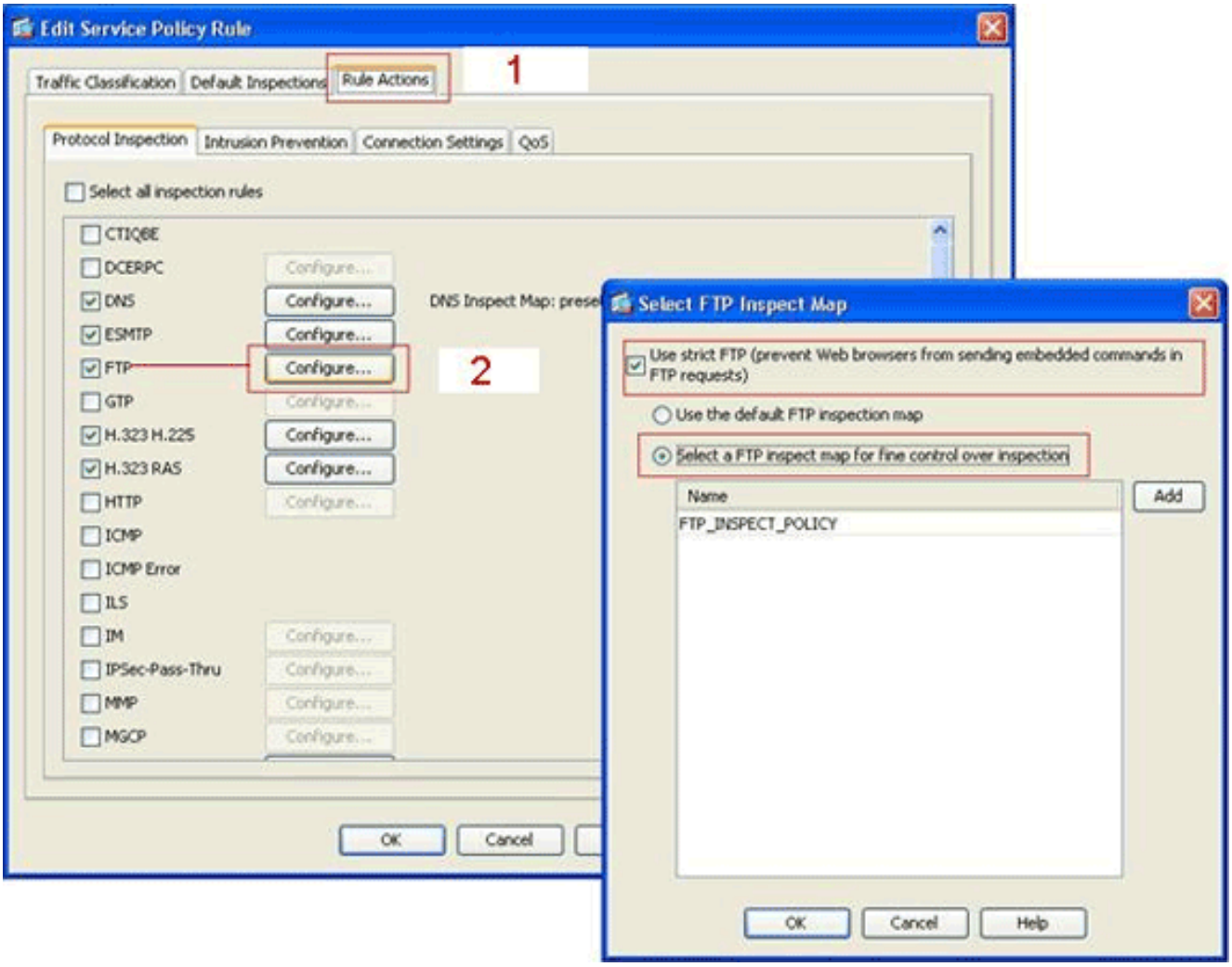


Geben Sie den Namen und eine Beschreibung für die Überprüfungsrichtlinie ein. (Beispiel: *FTP_INSPECT_POLICY*.)Klicken Sie auf **Details.**



Klicken Sie auf die Registerkarte **Inspektionen**. Absatz 1Klicken Sie auf **Hinzufügen**. Absatz 2Klicken Sie auf das Optionsfeld **Mehrere Übereinstimmungen**, und wählen Sie die Verkehrsklasse aus der Dropdown-Liste aus. Absatz 3Wählen Sie die gewünschte Reset-Aktion aus, um die Funktion zu aktivieren oder zu deaktivieren. In diesem Beispiel wird die Rücksetzung der FTP-Verbindung für alle FTP-Sites aktiviert, die *nicht mit* unseren angegebenen Sites *übereinstimmen*. (4)Klicken Sie auf **OK**, klicken Sie erneut **auf OK** und klicken Sie anschließend auf **Übernehmen**. 5.

6. **Wenden Sie die Inspection-FTP-Richtlinie auf die globale Inspektionsliste an.**Wählen Sie **Konfiguration > Firewall > Service Policy Rules aus**.Wählen Sie auf der rechten Seite die **Inspection_default-**Richtlinie aus, und klicken Sie auf **Bearbeiten**.Klicken Sie auf der Registerkarte Regelaktionen (1) auf die Schaltfläche **Konfigurieren** für FTP. Absatz 2Aktivieren Sie im Dialogfeld Select FTP Inspect Map (FTP-Inspektionszuordnung auswählen) das Kontrollkästchen **Use strict FTP (Strenge FTP-**Prüfung **verwenden**), und klicken Sie dann auf die **FTP-Inspektionszuordnung, um die Kontrolle über das** Optionsfeld **Überprüfung** zu **überprüfen**.Die neue FTP-Überwachungsrichtlinie, *FTP_INSPECT_POLICY*, sollte in der Liste angezeigt werden.Klicken Sie auf **OK**, klicken Sie erneut **auf OK** und klicken Sie anschließend auf **Übernehmen**.



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show running-config regex**: Zeigt die konfigurierten regulären Ausdrücke an.

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

- **show running-config class-map**: Zeigt die konfigurierten Klassenzuordnungen.

```
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
!
```

- **show running-config policy-map type inspect http**: Zeigt die Richtlinienzuordnungen an, die den konfigurierten HTTP-Datenverkehr überprüfen.

```
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
 !
```

- **Show running-config policy-map** (**Richtlinienzuordnung anzeigen**): Zeigt alle Richtlinienzuordnungskonfigurationen sowie die Standardzuordnungskonfiguration an.

```
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
!
```

- **show running-config service-policy**: Zeigt alle aktuell ausgeführten

Servicerichtlinienkonfigurationen an.

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

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Sie können den Befehl **show service-policy** verwenden, um zu überprüfen, ob die Prüfungs-Engine den Datenverkehr überprüft und ihn korrekt zulässt oder verwirft.

```
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
```

Zugehörige Informationen

- ASA/PIX 8.x: Sperren bestimmter Websites (URLs) mithilfe von regulären Ausdrücken mit MPF-Konfigurationsbeispiel
- PIX/ASA 7.x und höher: Blockieren des Peer-to-Peer- (P2P) und Instant Messaging-Datenverkehrs (IM) mithilfe des MPF-Konfigurationsbeispiels
- PIX/ASA 7.x: Beispiel für die Konfiguration von FTP- und TFTP-Services aktivieren
- Anwenden der Protokollüberprüfung auf Anwendungsebene
- Cisco Adaptive Security Appliances der Serie ASA 5500 - Unterstützung
- Cisco Adaptive Security Device Manager (ASDM)
- Cisco PIX Security Appliances der Serie 500 - Support
- Cisco PIX Firewall-Software - Support
- Cisco PIX Firewall-Software - Befehlsreferenzen