

ASA/PIX 8.x: Sperren bestimmter Websites (URLs) mithilfe von regulären Ausdrücken mit MPF-Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Zugehörige Produkte](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Übersicht über das modulare Richtlinien-Framework](#)

[Regulärer Ausdruck](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[ASA CLI-Konfiguration](#)

[ASA-Konfiguration 8.x mit ASDM 6.x](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

In diesem Dokument wird beschrieben, wie Sie die Cisco Security Appliances ASA/PIX 8.x konfigurieren, die reguläre Ausdrücke mit modularem Richtlinien-Framework (MPF) verwenden, um bestimmte Websites (URLs) zu blockieren.

Hinweis: Diese Konfiguration blockiert nicht alle Anwendungs-Downloads. Für eine zuverlässige Dateiblockierung sollte eine dedizierte Appliance wie die Ironport S-Serie oder ein Modul wie das CSC-Modul für die ASA verwendet werden.

Hinweis: HTTPS-Filterung wird auf ASA nicht unterstützt. Die ASA kann keine Deep Packet Inspection oder Inspektion auf der Grundlage von regulären Ausdrücken für HTTPS-Datenverkehr durchführen, da der Paketinhalt in HTTPS verschlüsselt (SSL) ist.

[Voraussetzungen](#)

[Anforderungen](#)

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

Verwendete Komponenten

- 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.

Zugehörige Produkte

Diese Konfiguration kann auch mit dem Cisco PIX der Serie 500 verwendet werden, auf dem die Softwareversion 8.0(x) und höher ausgeführt wird.

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) Legen Sie besondere Aktionen für Anwendungsinspektionsverkehr fest. 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 von bestimmten Anwendungsdatenverkehr abzugleichen. Beispielsweise können Sie eine URL-Zeichenfolge in einem HTTP-Paket zuordnen.

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

Verwenden Sie zum Erstellen eines regulären Ausdrucks den Befehl **regex**, der für verschiedene Features verwendet werden kann, die eine Textzuordnung erfordern. Sie können z. B. spezielle Aktionen für die Anwendungsinspektion konfigurieren, indem Sie das modulare Richtlinien-Framework verwenden, das eine Überwachungsrichtlinienzuordnung verwendet. Weitere Informationen finden Sie im **Befehl** zur Richtlinienzuordnung. In der Richtlinienzuordnung für die Inspektionsrichtlinie 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. Sie können beispielsweise 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](#).

Diese [Tabelle](#) listet die Metazeichen auf, die besondere Bedeutungen haben.

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. So behält beispielsweise der "Test" beim Suchen nach einer Übereinstimmung das führende Leerzeichen bei.
^	Sorgfalt	Gibt den Anfang 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 einem Register 0x09 zu
\f	Vorspeise	Entspricht einem Formular-Feed 0x0c
\xN	Hexadezimalzahl mit Escapezeichen	Entspricht einem ASCII-Zeichen, das ein Hexadezimalzeichen mit genau zwei Ziffern verwendet
\N	Escaped Oktalnummer	Entspricht einem ASCII-Zeichen einem Oktal, das genau drei Ziffern umfasst. Beispielsweise stellt das Zeichen 040 ein Leerzeichen dar.

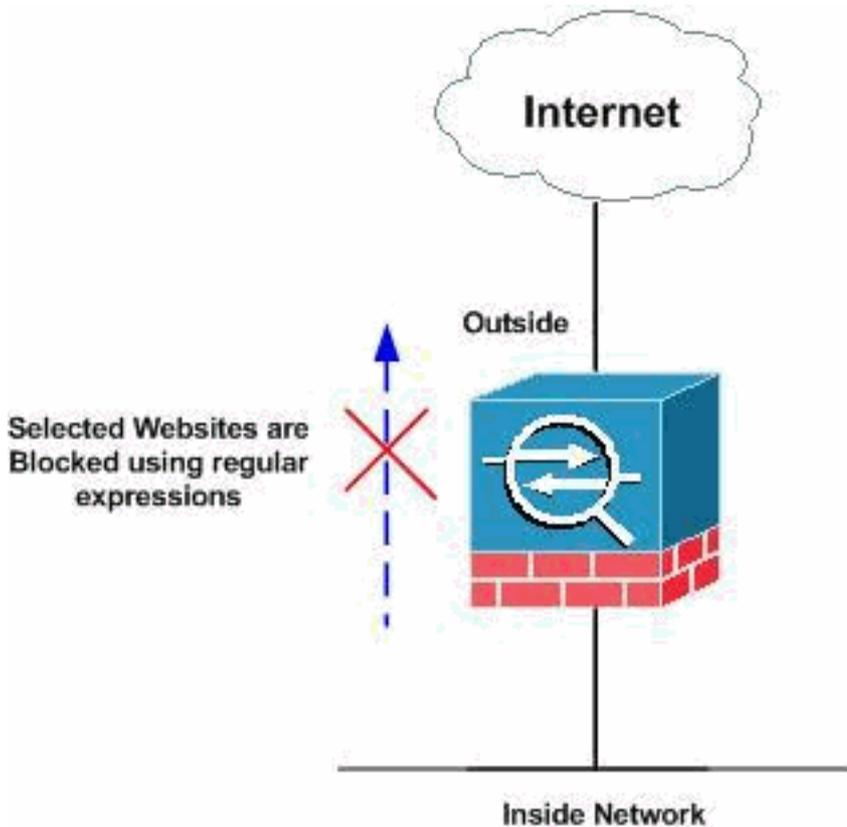
Konfigurieren

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:



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 running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 192.168.1.5 255.255.255.0
!
interface Ethernet0/2
```

```

nameif DMZ
security-level 90
ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted

regex urllist1
".*\.( [Ee] [Xx] [Ee] | [Cc] [Oo] [Mm] | [Bb] [Aa] [Tt] )
HTTP/1.[01]"

!--- Extensions such as .exe, .com, .bat to be captured
and !--- provided the http version being used by web
browser must be either 1.0 or 1.1 regex urllist2
".*\.( [Pp] [Ii] [Ff] | [Vv] [Bb] [Ss] | [Ww] [Ss] [Hh] )
HTTP/1.[01]"

!--- Extensions such as .pif, .vbs, .wsh to be captured
!--- and provided the http version being used by web
browser must be either !--- 1.0 or 1.1 regex urllist3
".*\.( [Dd] [Oo] [Cc] | [Xx] [Ll] [Ss] | [Pp] [Pp] [Tt] )
HTTP/1.[01]"

!--- Extensions such as .doc(word), .xls(ms-excel), .ppt
to be captured and provided !--- the http version being
used by web browser must be either 1.0 or 1.1 regex
urllist4 ".*\.( [Zz] [Ii] [Pp] | [Tt] [Aa] [Rr] | [Tt] [Gg] [Zz] )
HTTP/1.[01]"

!--- Extensions such as .zip, .tar, .tgz to be captured
and provided !--- the http version being used by web
browser must be either 1.0 or 1.1 regex domainlist1
"\.yahoo\.com"
regex domainlist2 "\.myspace\.com"
regex domainlist3 "\.youtube\.com"

!--- Captures the URLs with domain name like yahoo.com,
!--- youtube.com and myspace.com regex contenttype
"Content-Type"
regex applicationheader "application/*"

!--- Captures the application header and type of !---
content in order for analysis boot system disk0:/asa802-
k8.bin ftp mode passive dns server-group DefaultDNS
domain-name default.domain.invalid access-list
inside_mpc extended permit tcp any any eq www

access-list inside_mpc extended permit tcp any any eq
8080

!--- Filters the http and port 8080 !--- traffic in
order to block the specific traffic with regular !---
expressions pager lines 24 mtu inside 1500 mtu outside
1500 mtu DMZ 1500 no failover icmp unreachable rate-

```

```

limit 1 burst-size 1 asdm image disk0:/asdm-602.bin no
asdm history enable arp timeout 14400 route DMZ 0.0.0.0
0.0.0.0 10.77.241.129 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 uauth 0:05:00 absolute dynamic-access-
policy-record DfltAccessPolicy http server enable http
0.0.0.0 0.0.0.0 DMZ no snmp-server location no snmp-
server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart no crypto
isakmp nat-traversal telnet timeout 5 ssh timeout 5
console timeout 0 threat-detection basic-threat threat-
detection statistics access-list ! class-map type regex
match-any DomainBlockList
  match regex domainlist1
  match regex domainlist2
  match regex domainlist3

!--- Class map created in order to match the domain
names !--- to be blocked class-map type inspect http
match-all BlockDomainsClass
  match request header host regex class DomainBlockList

!--- Inspect the identified traffic by class !---
"DomainBlockList". class-map type regex match-any
URLBlockList
  match regex urllist1
  match regex urllist2
  match regex urllist3
  match regex urllist4

!--- Class map created in order to match the URLs !---
to be blocked class-map inspection_default match
default-inspection-traffic class-map type inspect http
match-all AppHeaderClass
  match response header regex contenttype regex
applicationheader

!--- Inspect the captured traffic by regular !---
expressions "content-type" and "applicationheader".
class-map httptraffic
  match access-list inside_mpc

!--- Class map created in order to match the !---
filtered traffic by ACL class-map type inspect http
match-all BlockURLsClass
  match request uri regex class URLBlockList
!

!--- Inspect the identified traffic by class !---
"URLBlockList". ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map type inspect http http_inspection_policy
parameters
  protocol-violation action drop-connection
class AppHeaderClass
  drop-connection log
match request method connect
  drop-connection log
class BlockDomainsClass
  reset log
class BlockURLsClass
  reset log

```

```

!--- Define the actions such as drop, reset or log !---
in the inspection policy map. policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtplib inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp policy-map inside-policy
class httptraffic
inspect http http_inspection_policy

!--- Map the inspection policy map to the class !---
"httptraffic" under the policy map created for the !---
inside network traffic. ! service-policy global_policy
global service-policy inside-policy interface inside

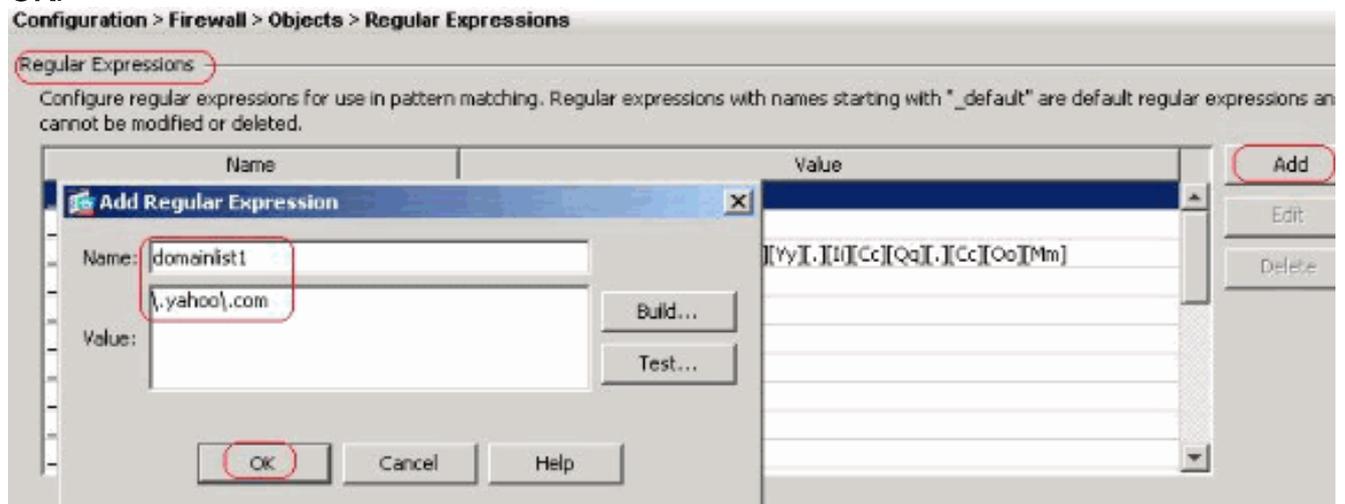
!--- Apply the policy to the interface inside where the
websites are blocked. prompt hostname context
Cryptochecksum:e629251a7c37af205c289cf78629fc11 : end
ciscoasa#

```

ASA-Konfiguration 8.x mit ASDM 6.x

Führen Sie diese Schritte aus, um die regulären Ausdrücke zu konfigurieren und sie in MPF anzuwenden, um die entsprechenden Websites wie gezeigt zu blockieren.

1. **Erstellen regulärer Ausdrücke** Wählen Sie **Konfiguration > Firewall > Objekte > Reguläre Ausdrücke** und klicken Sie unter der Registerkarte **Regulärer Ausdruck** auf **Hinzufügen**, um reguläre Ausdrücke wie gezeigt zu erstellen. Erstellen Sie eine **domainlist1** für reguläre Ausdrücke, um den Domännennamen **yahoo.com** zu erfassen. Klicken Sie auf **OK**.



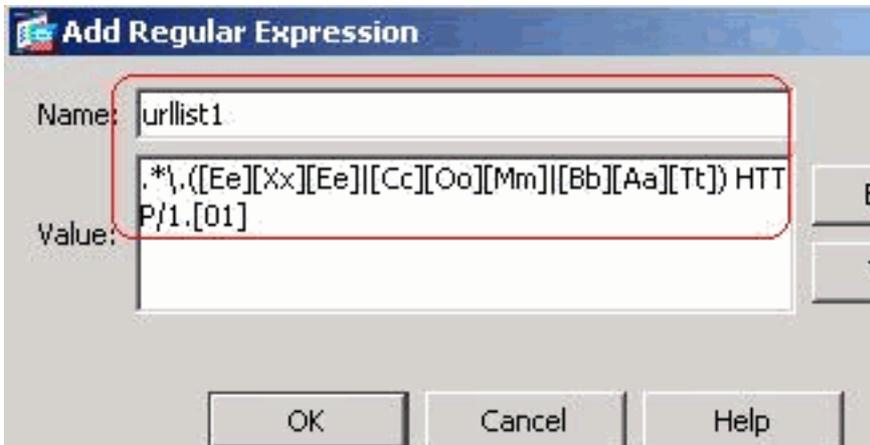
Erstellen Sie einen regulären Ausdruck **domainlist2**, um den Domännennamen **myspace.com** zu erfassen. Klicken Sie auf



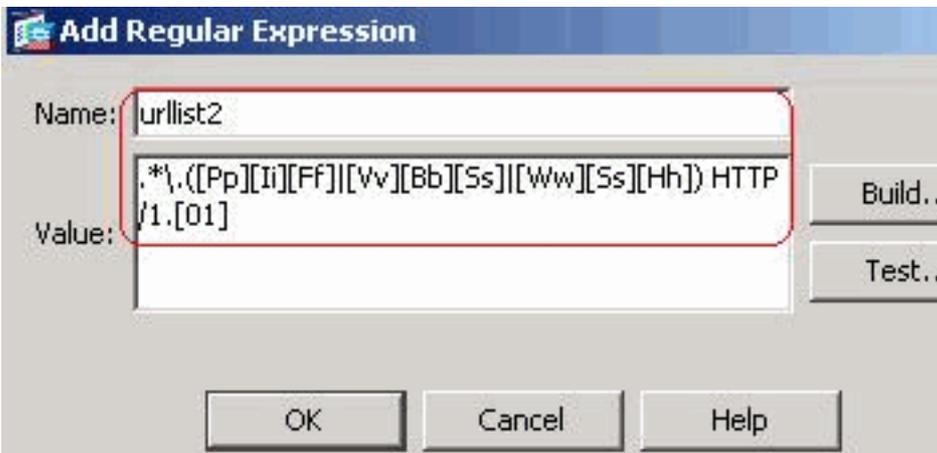
OK. Erstellen Sie einen regulären Ausdruck **domainlist3**, um den Domännennamen **youtube.com** zu erfassen. Klicken



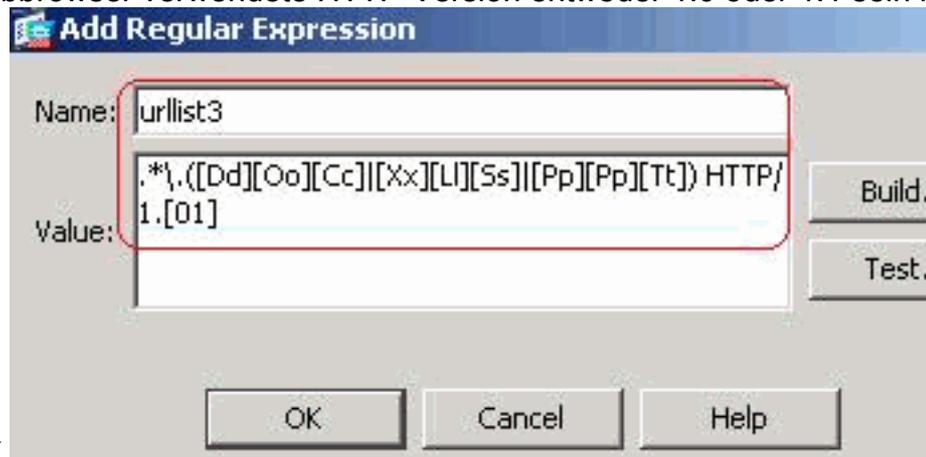
Sie auf OK. Erstellen Sie einen regulären Ausdruck **urllist1**, um Dateierweiterungen wie **exe**, **com** und **bat** zu erfassen, sofern die vom Webbrowser verwendete HTTP-Version entweder 1.0 oder 1.1 sein muss. Klicken



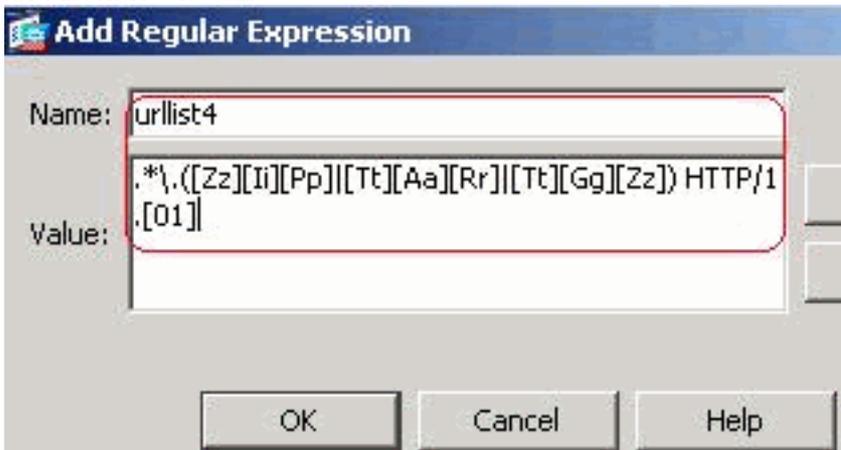
Sie auf OK. Erstellen Sie einen regulären Ausdruck **urllist2**, um Dateierweiterungen wie **pif**, **vbs** und **wsh** zu erfassen, vorausgesetzt, die vom Webbrowser verwendete HTTP-Version muss entweder 1.0 oder 1.1 sein. Klicken Sie auf



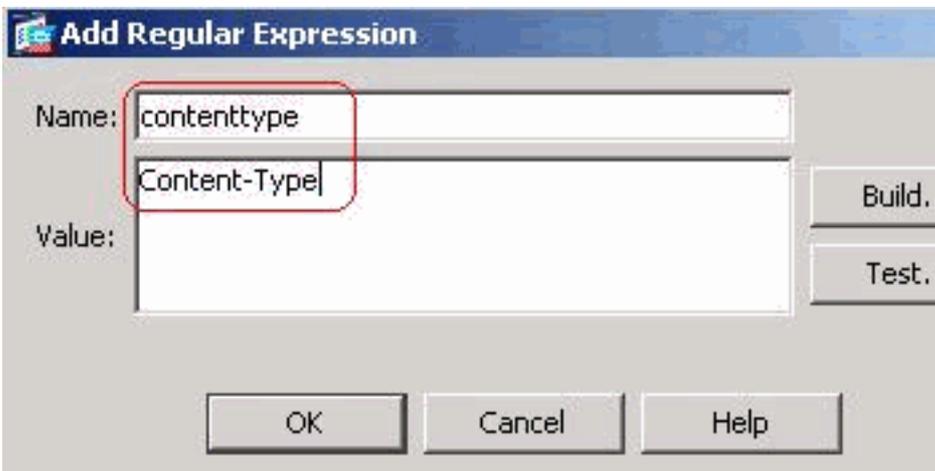
OK. Erstellen Sie eine **URLlist3** für reguläre Ausdrücke, um Dateierweiterungen wie **doc**, **xls** und **ppt** zu erfassen, sofern die vom Webbrowser verwendete HTTP-Version entweder 1.0 oder 1.1 sein muss.



Klicken Sie auf **OK**. Erstellen Sie eine **URLlist4** für reguläre Ausdrücke, um Dateierweiterungen wie **zip**, **tar** und **tgz** zu erfassen, sofern die vom Webbrowser verwendete HTTP-Version entweder 1.0 oder 1.1 sein muss. Klicken Sie auf



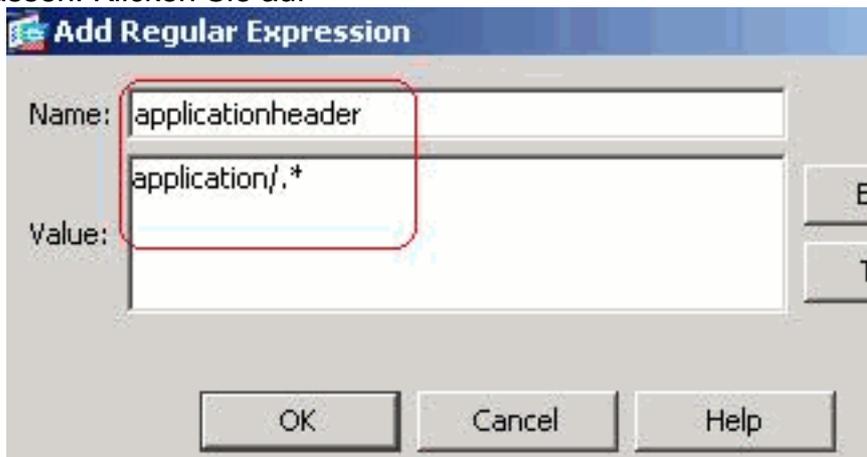
OK. Erstellen Sie einen **Inhaltstyp** für reguläre Ausdrücke, um den Inhaltstyp zu erfassen. Klicken Sie auf



OK.

Erstellen Sie einen

Anwendungsheader für reguläre Ausdrücke, um die verschiedenen Anwendungsheader zu erfassen. Klicken Sie auf

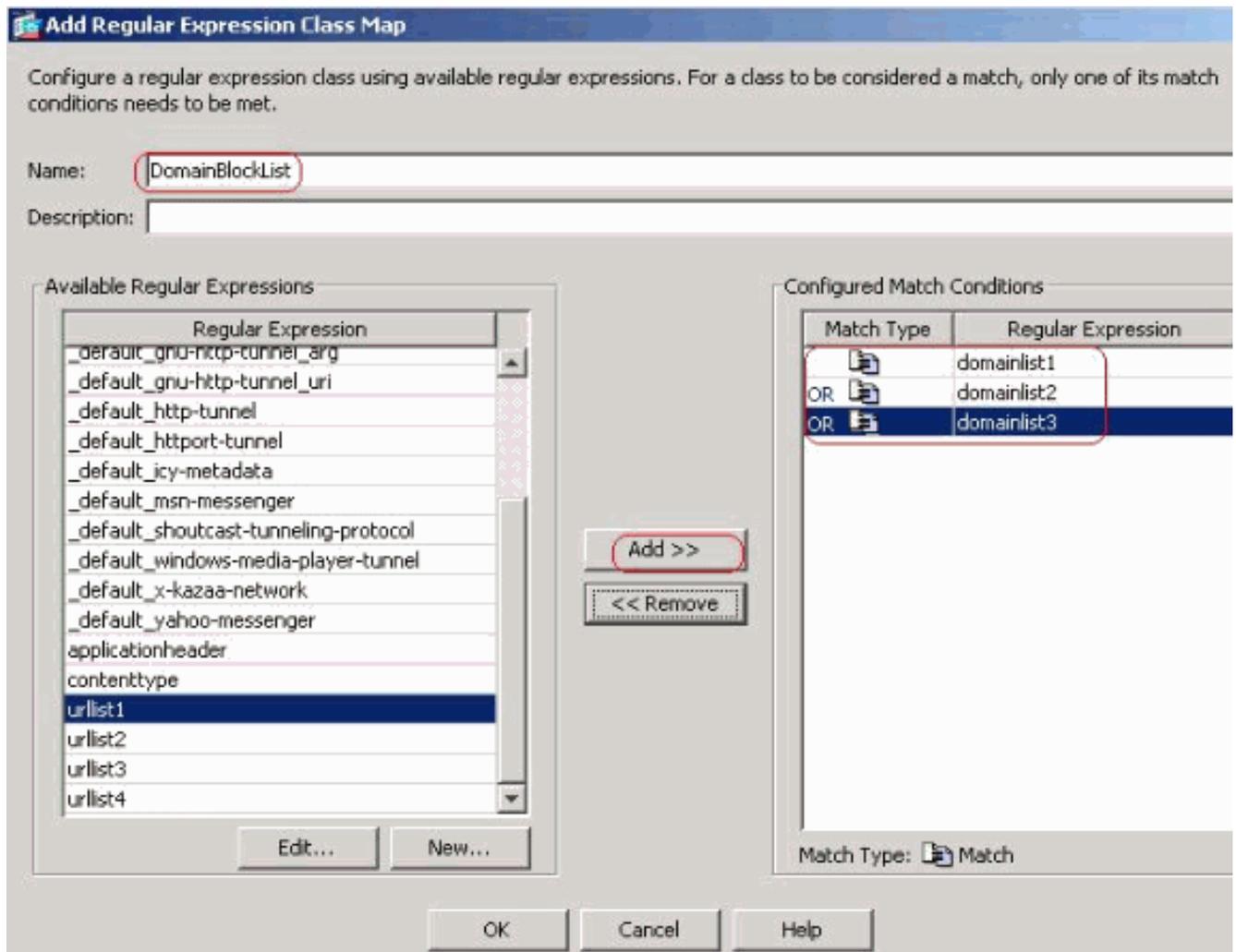


OK.

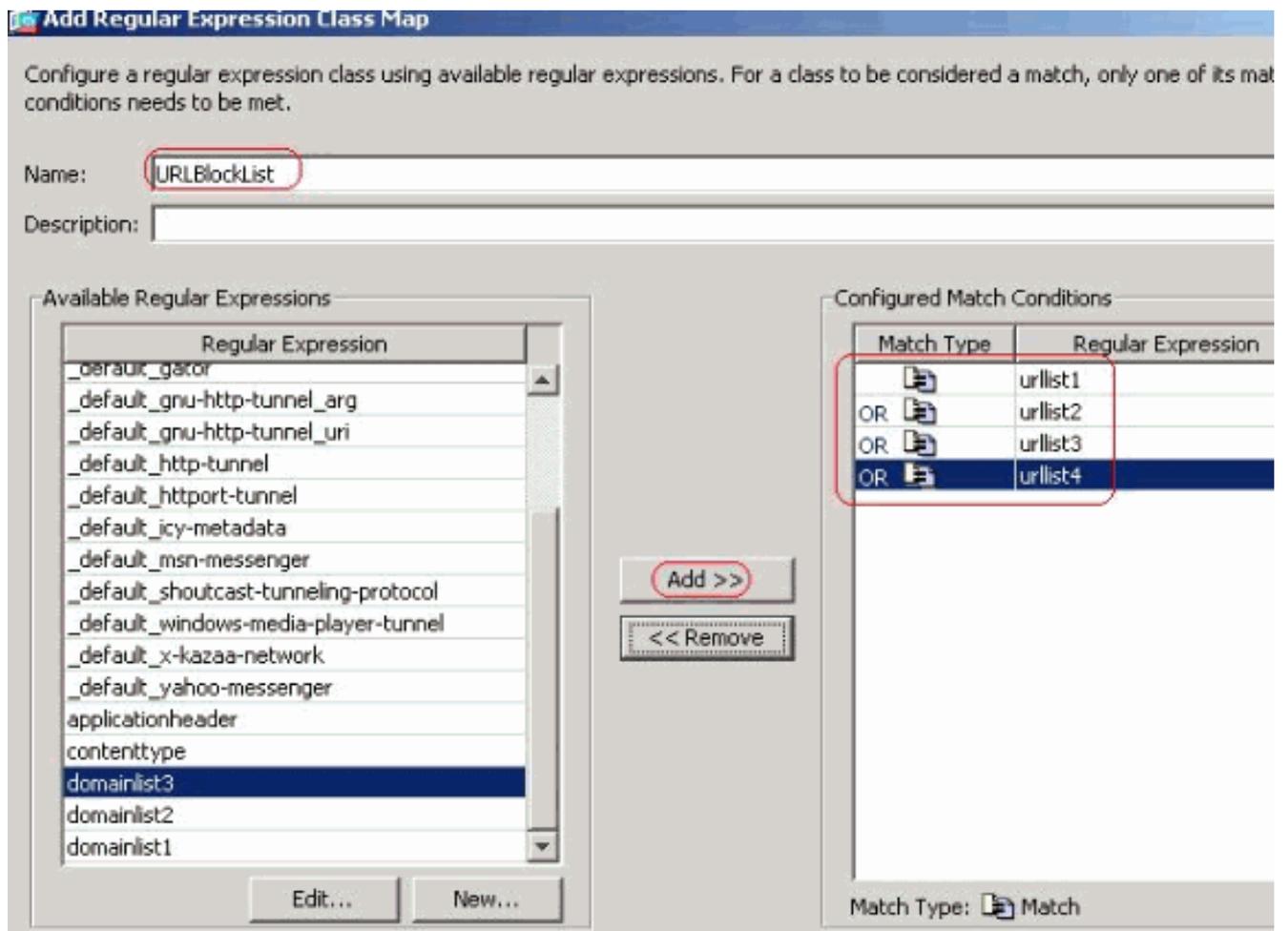
Entsprechende CLI-

Konfiguration

2. **Erstellen von Klassen regulärer Ausdrücke** Wählen Sie **Konfiguration > Firewall > Objekte > Reguläre Ausdrücke** und klicken Sie unter der Registerkarte **Klassen regulärer Ausdrücke** auf **Hinzufügen**, um die verschiedenen Klassen wie gezeigt zu erstellen. Erstellen Sie eine **DomainBlockList**-Klasse für reguläre Ausdrücke, um mit einem der regulären Ausdrücke domainlist1, domainlist2 und domainlist3 übereinstimmen zu können. Klicken Sie auf **OK**.

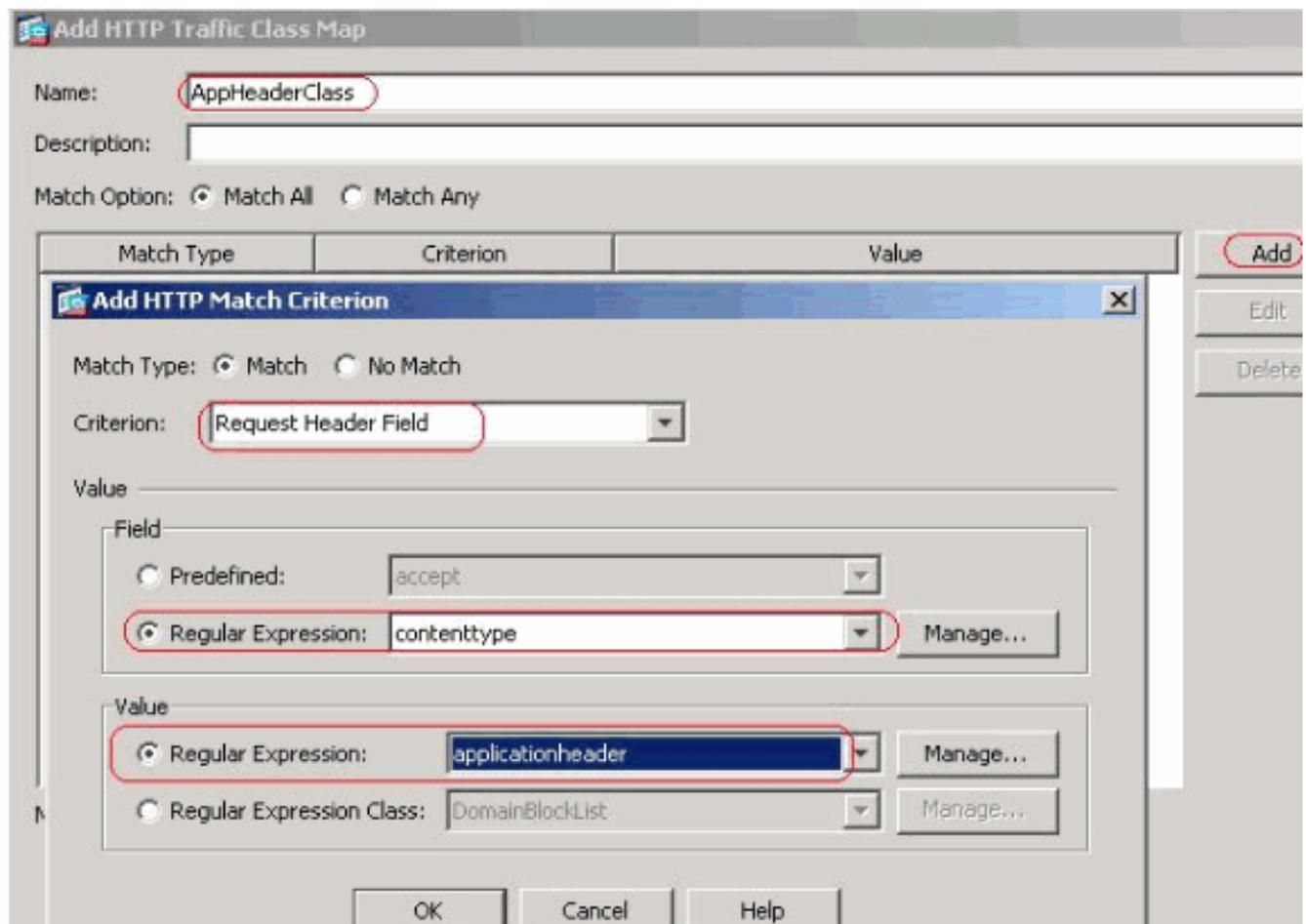


Erstellen Sie eine **URLBlockList** für reguläre Ausdrücke, um die regulären Ausdrücke urllist1, urllist2, urllist3 und urllist4 abzugleichen. Klicken Sie auf **OK**.

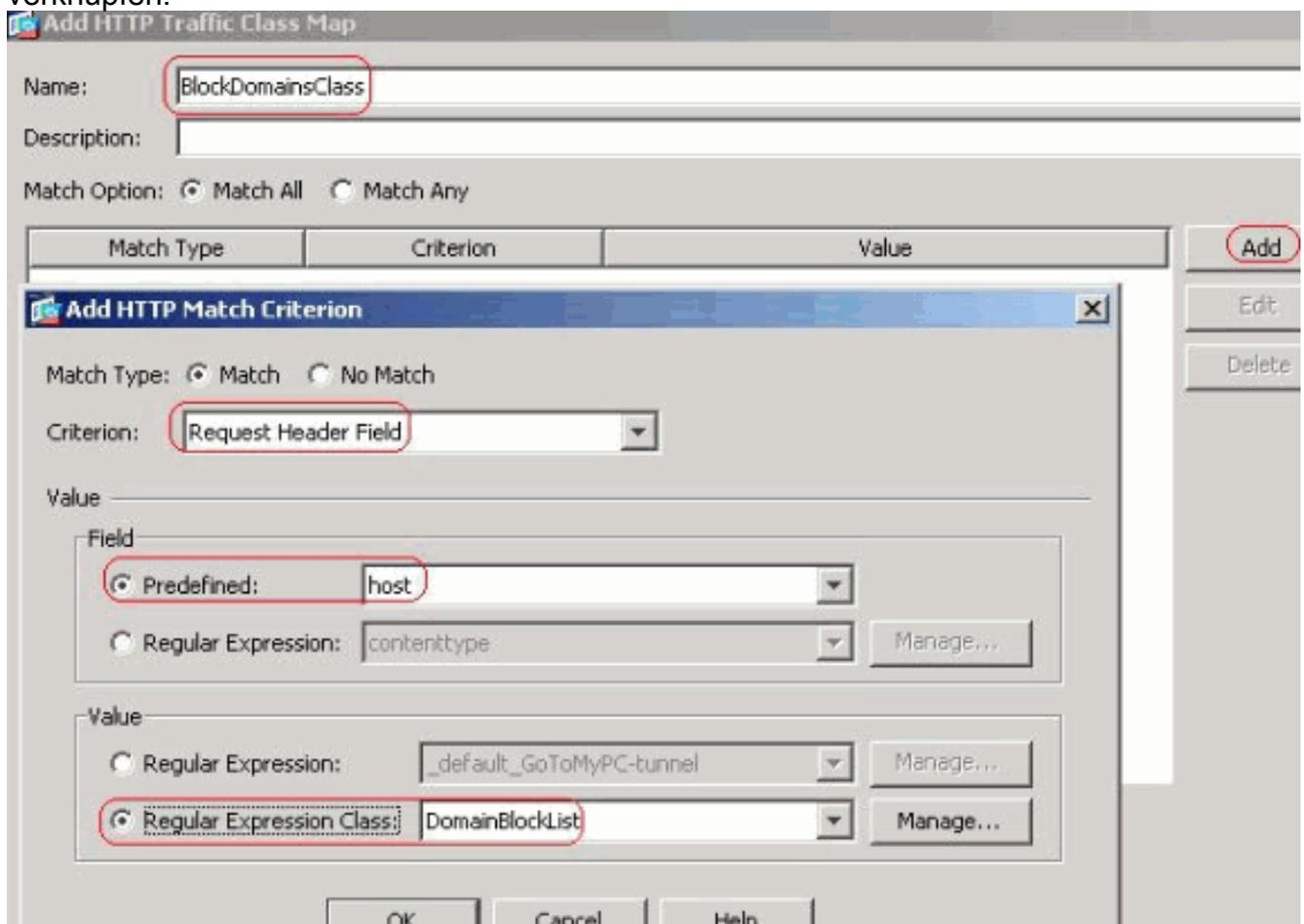


Entsprechende CLI-Konfiguration

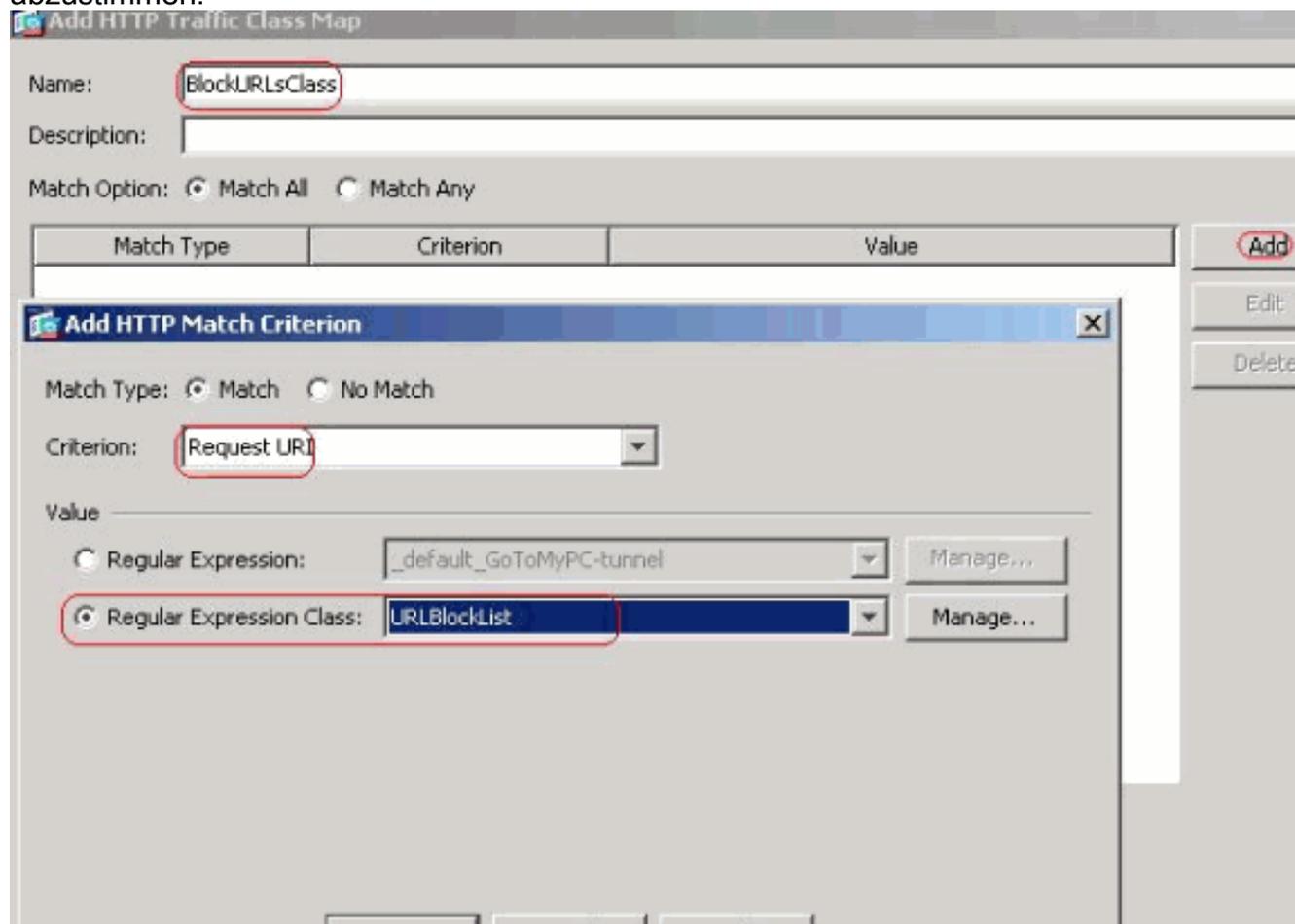
3. Identifizierten Datenverkehr mit Klassenzuordnungen untersuchen Wählen Sie **Configuration > Firewall > Objects > Class Maps > HTTP > Add**, um eine Klassenzuordnung zu erstellen, um den HTTP-Datenverkehr zu überprüfen, der durch verschiedene reguläre Ausdrücke wie dargestellt identifiziert wird. Erstellen Sie eine Klassenzuordnung **AppHeaderClass**, um den Antwortheader mit regulären Ausdrücken zu verknüpfen.



Klicken Sie auf **OK** erstellen Sie eine Klassenzuordnung **BlockDomainsClass**, um den Anforderungsheader mit regulären Ausdrücken zu verknüpfen.

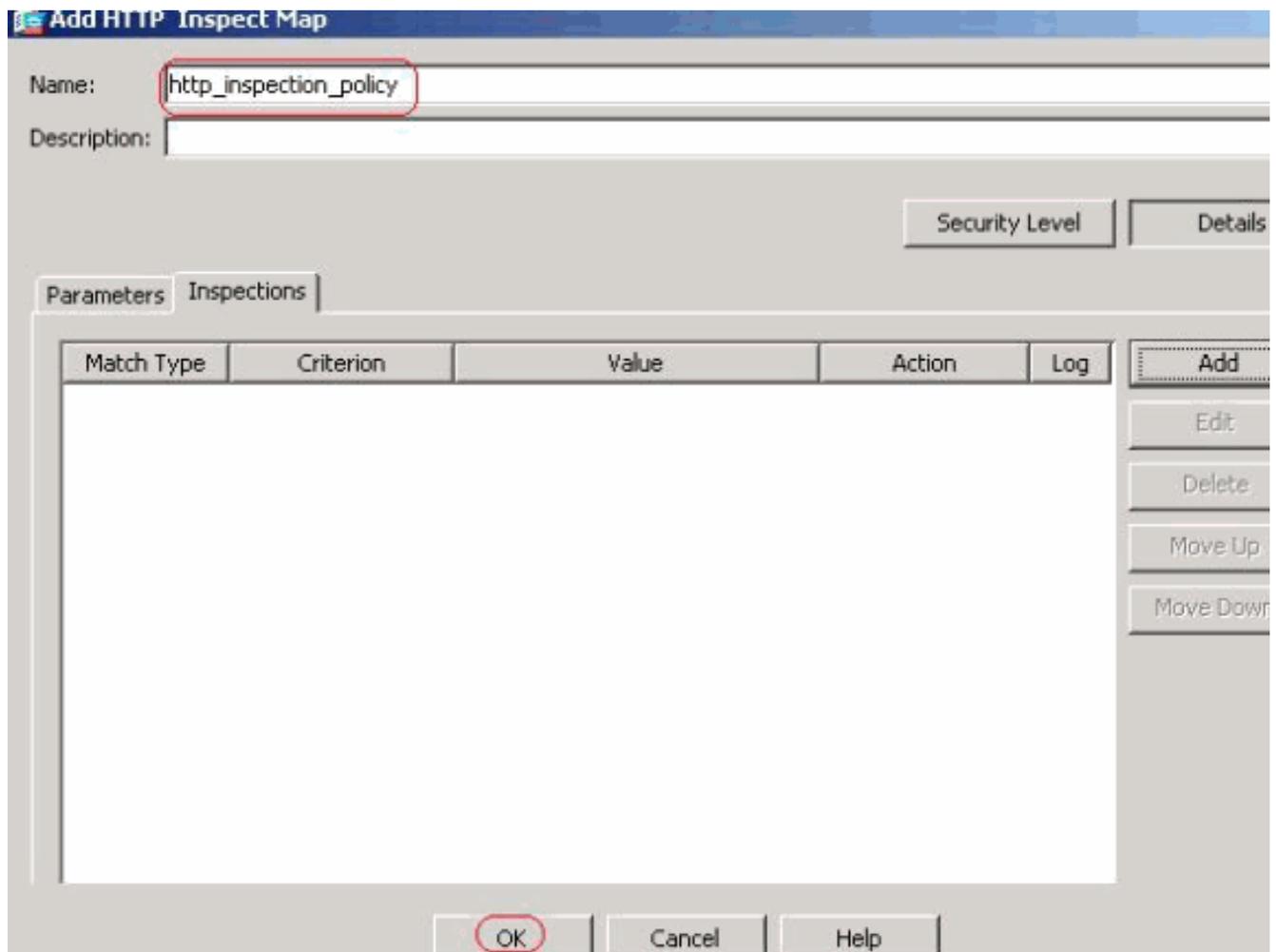


Klicken Sie auf **OK**. Erstellen Sie eine Klassenzuordnung **BlockURLsClass**, um das Anforderungs-uri mit der Erfassung regulärer Ausdrücke abzustimmen.

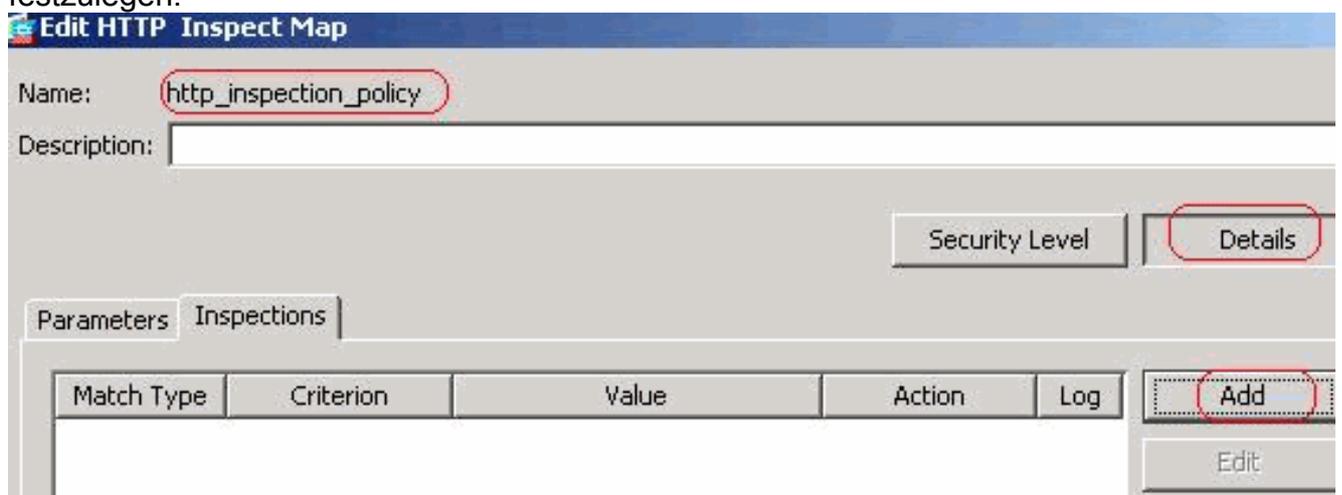


Klicken Sie auf **OK**. Entsprechende CLI-Konfiguration

4. Festlegen der Aktionen für den abgeglichenen Datenverkehr in der Überprüfungsrichtlinie Wählen Sie **Configuration > Firewall > Objects > Inspect Maps > HTTP** aus, um eine **http_inspection_policy** zu erstellen, um die Aktion für den zugeordneten Datenverkehr wie gezeigt festzulegen. Klicken Sie auf **OK**.



Wählen Sie **Configuration > Firewall > Objects > Inspect Maps > HTTP > http_Inspection_policy** (doppelklicken Sie auf) und klicken Sie auf **Details > Add**, um die Aktionen für die verschiedenen bisher erstellten Klassen festzulegen.



Legen Sie die Aktion als **Drop Connection** fest, und **aktivieren Sie** die Protokollierung für das Kriterium als Request Method und Value as

Add HTTP Inspect

Match Criteria

Single Match

Match Type: Match No Match

Criterion:

Value

Method:

Regular Expression

Regular Expression:

Regular Expression Class:

Multiple matches

HTTP Traffic Class:

Actions

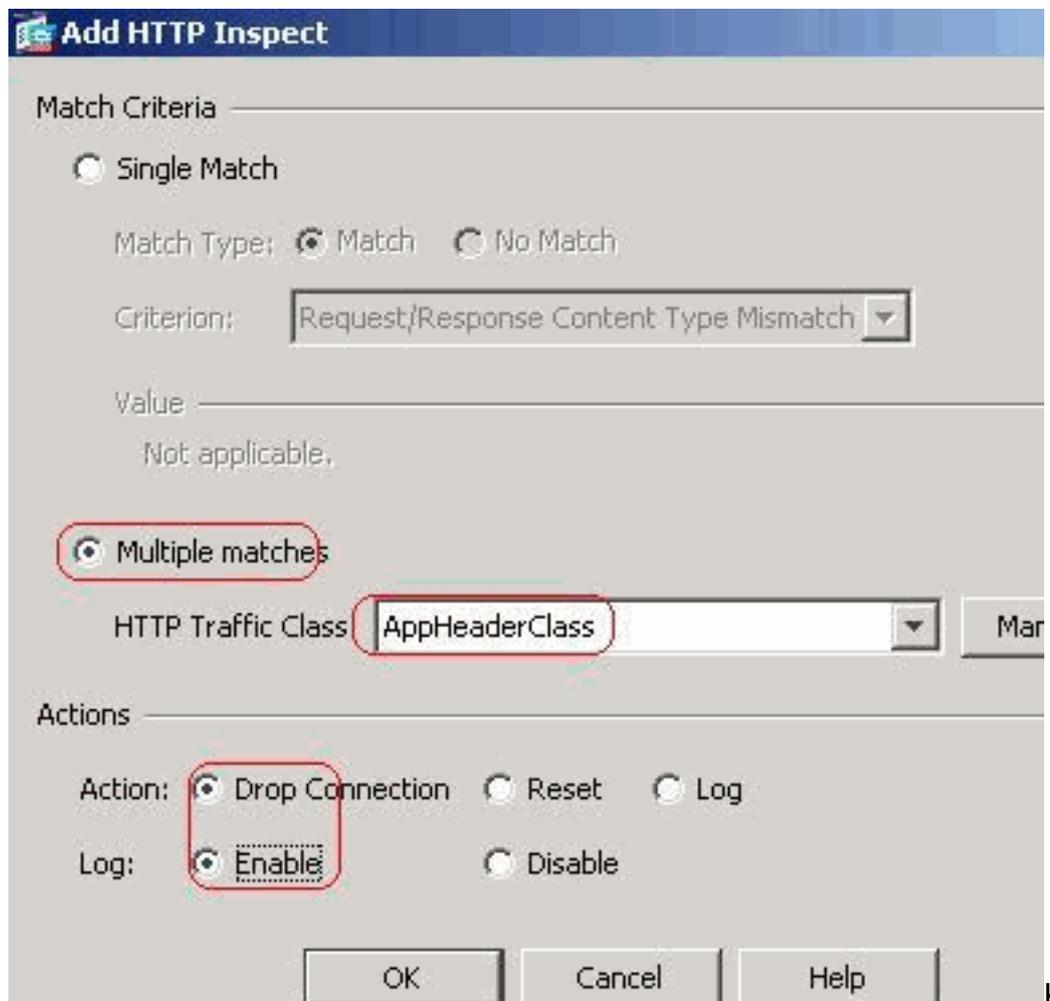
Action: Drop Connection Reset Log

Log: Enable Disable

connect.

Klicken

Sie auf **OK** Legen Sie die Aktion als **Drop Connection** fest, und **aktivieren Sie** die Protokollierung für die Klasse



AppHeaderClass.

cken Sie auf **OK**. Legen Sie die Aktion auf **Reset** und **Enable** die Protokollierung für die Klasse **BlockDomainsClass**

Kli

Add HTTP Inspect

Match Criteria

Single Match

Match Type: Match No Match

Criterion: Request/Response Content Type Mismatch

Value: Not applicable.

Multiple matches

HTTP Traffic Class: BlockDomainsClass

Actions

Action: Drop Connection Reset Log

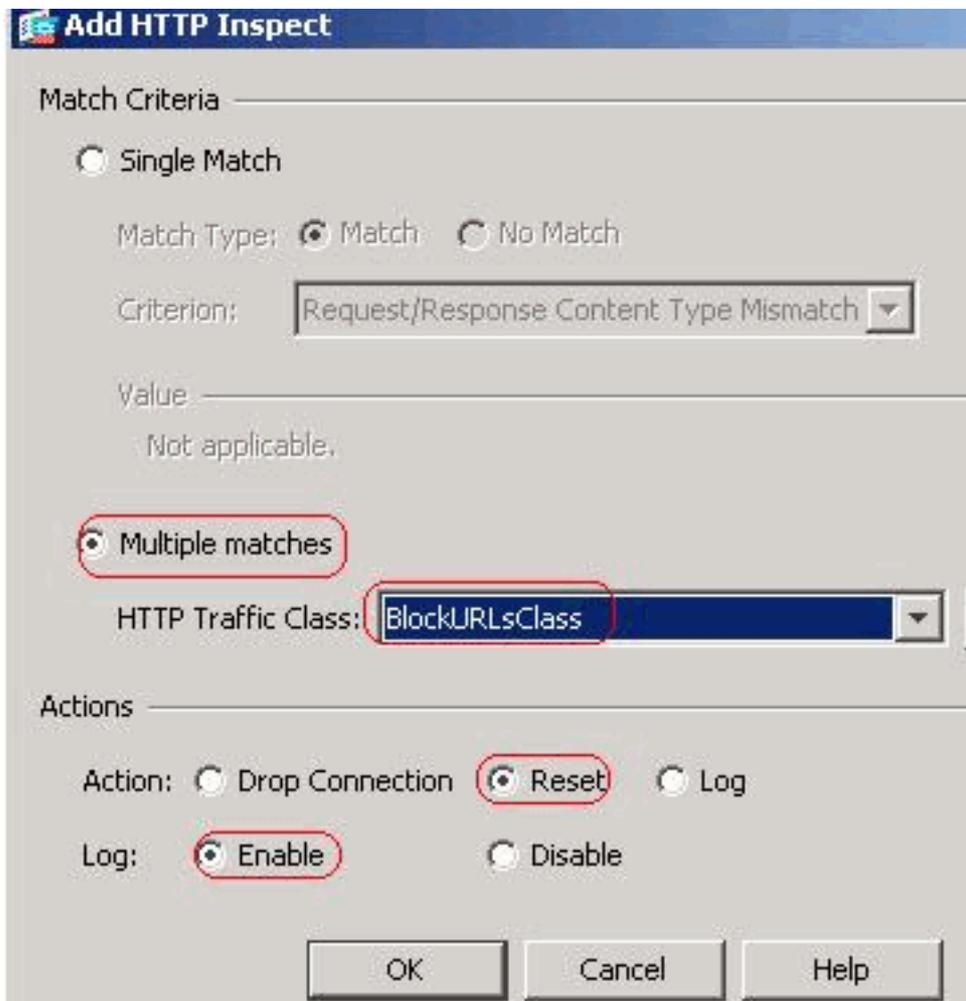
Log: Enable Disable

OK Cancel Help

fest.

OK Legen Sie die Aktion als **Reset** und **Enable** die Protokollierung für die Klasse **BlockURLsClass**

Klicken Sie auf



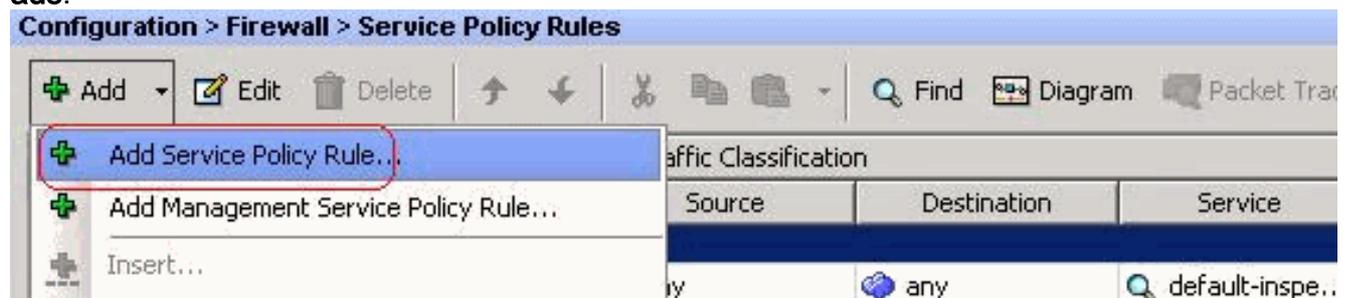
fest.

Klicken Sie auf

OK. Klicken Sie auf **Übernehmen**. Entsprechende CLI-Konfiguration

- Wenden Sie die Inspection-http-Richtlinie auf die Schnittstelle an. Wählen Sie **Configuration > Firewall > Service Policy Rules > Add > Add Service Policy Rule** (Konfiguration > Firewall > Service-Richtlinienregeln hinzufügen)

aus.



HTTP-Datenverkehr Wählen Sie im Dropdown-Menü die Optionsschaltfläche **Interface** (Schnittstelle) mit interner Schnittstelle aus, und wählen Sie Policy Name (Richtlinienname) als **Insider-Richtlinie** aus. Klicken Sie auf **Weiter**.

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To: _____

Only one service policy can be configured per interface or at global level. If a service policy already exists, the new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface: ▼

Policy Name:

Description:

Global - applies to all interfaces

Policy Name:

Description:

≤ Back

Next >

Erstellen Sie eine Klassenzuordnung **httptraffic**, und überprüfen Sie die **Quell-** und **Ziel-IP-Adresse (verwendet ACL)**. Klicken Sie auf **Weiter**.

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

Use an existing traffic class:

Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default all situation.

Wählen Sie "Source" (Quelle) und "Destination" (Ziel) wie bei "Service" als **tcp-udp/http** aus.
Klicken Sie auf **Weiter**.

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: Match Do not match

Source: any

Destination: any

Service: tcp-udp/http

Description:

More Options

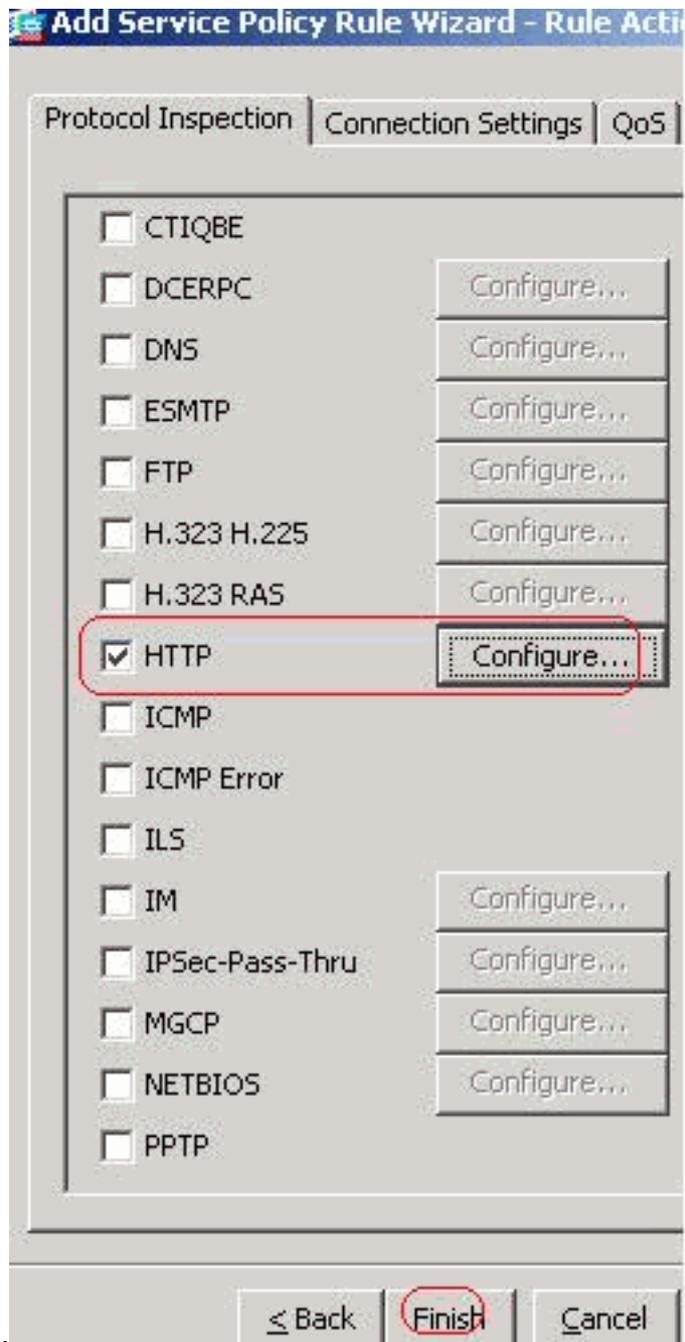
Enable Rule

Source Service: (TCP or UDP service only)

Time Range:

≤ Back **Next >**

Aktivieren Sie das **HTTP**-Optionsfeld, und klicken Sie auf



Konfigurieren.

Wählen Sie eine HTTP-Inspektionszuordnung für das Steuerelement über Inspektion wie

Aktivieren Sie das Optionsfeld

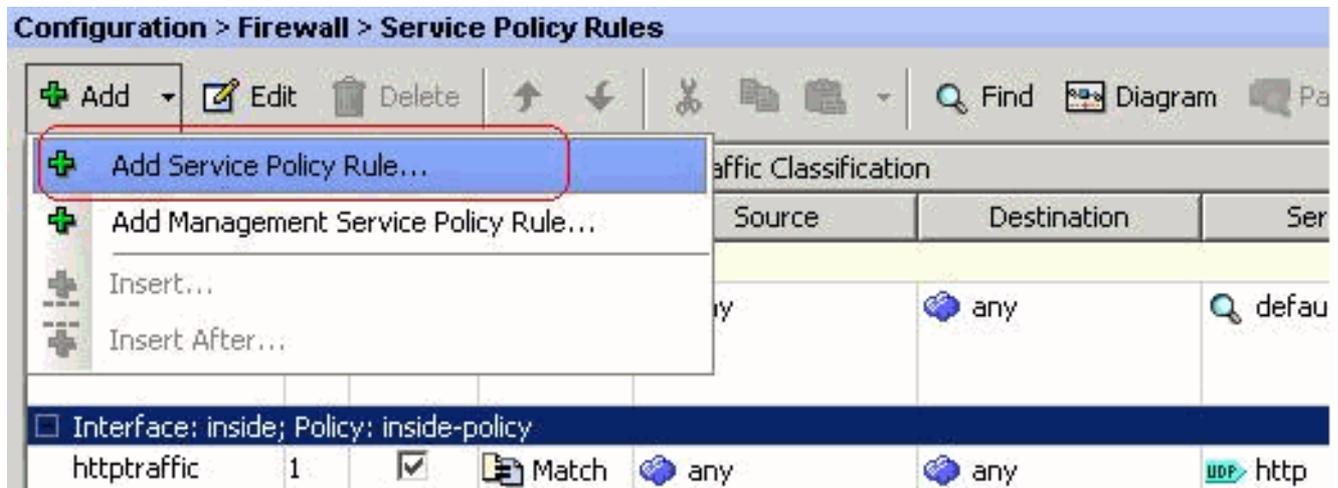


gezeigt aus. Klicken Sie auf OK.
auf **Fertig**
stellen.

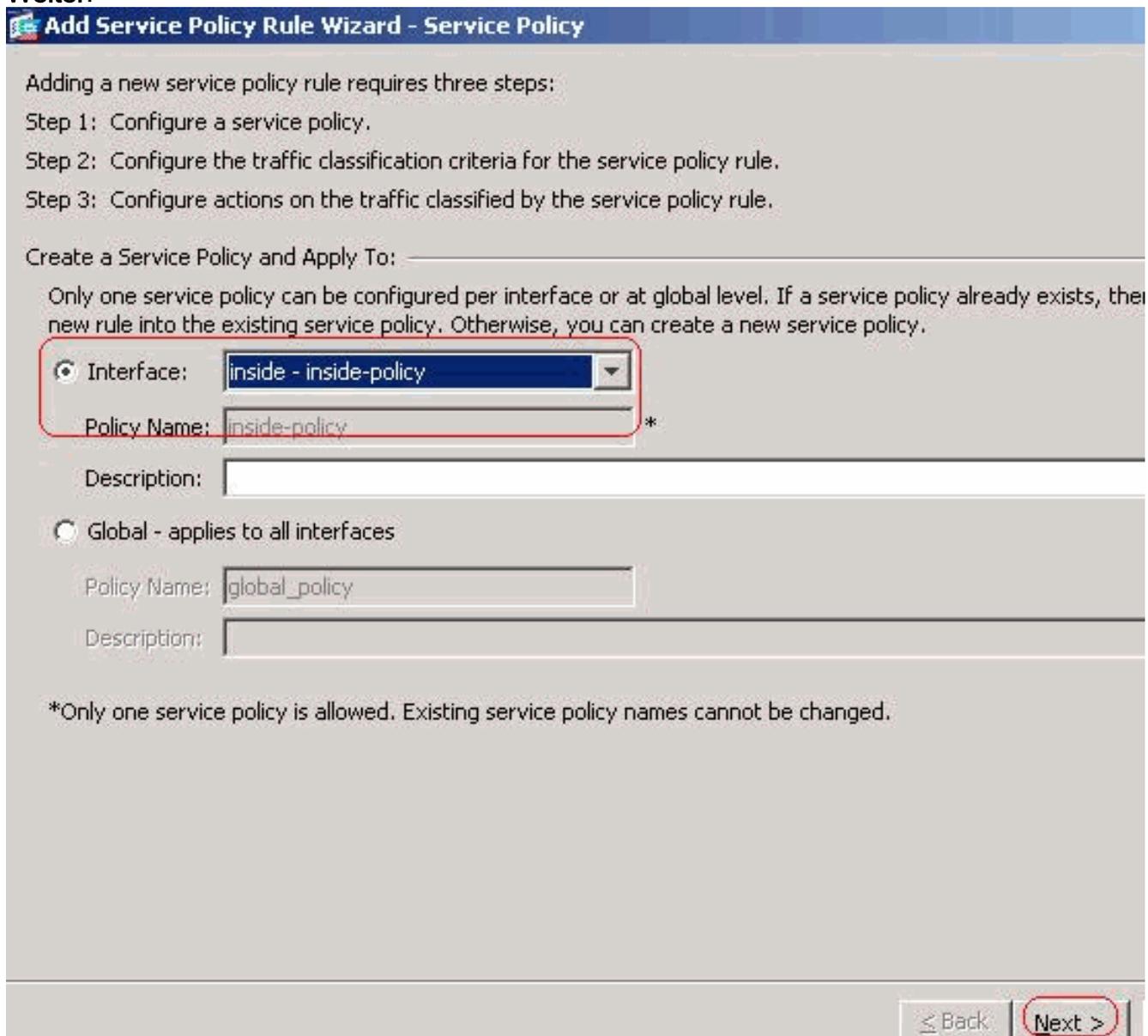
Klicken Sie



Datenverkehr über Port 8080
Wählen Sie erneut **Hinzufügen > Service Policy Rule**
(Servicenichtlinie
hinzufügen).



Klicken Sie auf
Weiter.



Wählen Sie das Optionsfeld **Regel zur vorhandenen Datenverkehrs-kategorie hinzufügen** aus, und wählen Sie im Dropdown-Menü die Option **HTTPS** aus. Klicken Sie auf **Weiter.**

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

Add rule to existing traffic class:

Rule can be added to an existing class map if that class map uses access control list (ACL) as its traffic match

Use an existing traffic class:

Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default all situation.

Wählen Sie mit **tcp/8080** als Quelle und Ziel aus. Klicken Sie auf **Weiter**.

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: Match Do not match

Source: ...

Destination: ...

Service: ...

Description:

More Options

Enable Rule

Source Service: ... (TCP or UDP service only)

Time Range: ...

Klicken Sie auf **Fertig stellen**.

Add Service Policy Rule Wizard - Rule Actions



The Rule Actions are applied to all the rules grouped in the Traffic Match.

Protocol Inspection | Connection Settings | QoS

- CTIQBE
- DCERPC Configure...
- DNS Configure...
- ESMTTP Configure...
- FTP Configure...
- H.323 H.225 Configure...
- H.323 RAS Configure...
- HTTP Configure... HTTP Inspect Map: http_inspection_policy
- ICMP
- ICMP Error
- ILS
- IM Configure...
- IPSec-Pass-Thru Configure...
- MGCP Configure...
- NETBIOS Configure...

≤ Back | **Finish** | Cancel

Configuration > Firewall > Service Policy Rules

+ Add | Edit | Delete | ↑ ↓ | ✂ | Diagram | Pa

Traffic Classification						
Name	#	Enabled	Match	Source	Destination	Serv
Global; Policy: global_policy						
inspection_defau			Match	any	any	default
Interface: inside; Policy: inside-policy						
httptraffic	1	<input checked="" type="checkbox"/>	Match	any	any	UDP http
	2	<input checked="" type="checkbox"/>	Match	any	any	TCP 8080

Klicken Sie auf **Übernehmen**. Entsprechende CLI-Konfiguration

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-config regex
regex urllist1 ".*\.[Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt] HTTP/1.[01]"
regex urllist2 ".*\.[Pp][Ii][Ff]|[Vv][Bb][Ss]|[Ww][Ss][Hh] HTTP/1.[01]"
regex urllist3 ".*\.[Dd][Oo][Cc]|[Xx][Ll][Ss]|[Pp][Pp][Tt] HTTP/1.[01]"
regex urllist4 ".*\.[Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz] HTTP/1.[01]"
regex domainlist1 "\.yahoo\.com"
regex domainlist2 "\.myspace\.com"
regex domainlist3 "\.youtube\.com"
regex contenttype "Content-Type"
regex applicationheader "application/*"
ciscoasa#
```

- **show running-config class-map** - Zeigt die konfigurierten Klassenzuordnungen an

```
ciscoasa#show running-config class-map
!
class-map type regex match-any DomainBlockList
  match regex domainlist1
  match regex domainlist2
  match regex domainlist3
class-map type inspect http match-all BlockDomainsClass
  match request header host regex class DomainBlockList
class-map type regex match-any URLBlockList
  match regex urllist1
  match regex urllist2
  match regex urllist3
  match regex urllist4
class-map inspection_default
  match default-inspection-traffic
class-map type inspect http match-all AppHeaderClass
  match response header regex contenttype regex applicationheader
class-map httptraffic
  match access-list inside_mpc
class-map type inspect http match-all BlockURLsClass
  match request uri regex class URLBlockList
!
ciscoasa#
```

- **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 http
!
policy-map type inspect http http_inspection_policy
  parameters
    protocol-violation action drop-connection
  class AppHeaderClass
    drop-connection log
  match request method connect
    drop-connection log
  class BlockDomainsClass
    reset log
  class BlockURLsClass
    reset log
!
ciscoasa#
```

- **show running-config policy-map**: Zeigt alle Richtlinienzuordnungskonfigurationen sowie die Standard-Richtlinienzuordnungskonfiguration an.

```
ciscoasa#show running-config policy-map
!
policy-map type inspect dns preset_dns_map
```

```

parameters
  message-length maximum 512
policy-map type inspect http http_inspection_policy
parameters
  protocol-violation action drop-connection
class AppHeaderClass
  drop-connection log
match request method connect
  drop-connection log
class BlockDomainsClass
  reset log
class BlockURLsClass
  reset log
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  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
policy-map inside-policy
class httptraffic
  inspect http http_inspection_policy
!
ciscoasa#

```

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

```

ciscoasa#show running-config service-policy
service-policy global_policy global
service-policy inside-policy interface inside

```

- **show running-config access-list:** Zeigt die Zugriffslistenkonfiguration an, die auf der Sicherheits-Appliance ausgeführt wird.

```

ciscoasa#show running-config access-list
access-list inside_mpc extended permit tcp any any eq www

access-list inside_mpc extended permit tcp any any eq 8080
ciscoasa#

```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Hinweis: Beachten Sie [vor der](#) Verwendung von **Debug**-Befehlen die [Informationen](#) zu [Debug-Befehlen](#).

- **debug http:** Zeigt die Debug-Meldungen für HTTP-Datenverkehr an

Zugehörige Informationen

- [Unterstützung von Cisco Adaptive Security Appliances der Serie ASA 5500](#)
- [Unterstützung von Cisco Adaptive Security Device Manager \(ASDM\)](#)
- [Unterstützung von Cisco PIX Security Appliances der Serie 500](#)
- [Cisco PIX Firewall-Software](#)
- [Cisco Secure PIX Firewall - Befehlsreferenzen](#)
- [Problemhinweise zu Sicherheitsprodukten \(einschließlich PIX\)](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)