ASA/PIX 7.2: Sperren bestimmter Websites (URLs) mithilfe von regulären Ausdrücken mit MPF-Konfigurationsbeispielen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Cisco Security Appliances ASA/PIX 7.2 mit regulären Ausdrücken mit modularem Richtlinien-Framework (MPF) konfigurieren, um bestimmte Websites (URLs) zu blockieren.

Hinweis: Diese Konfiguration blockiert nicht alle Anwendungs-Downloads. Für zuverlässige Dateiblöcke muss eine dedizierte Appliance, wie Websense usw., oder ein Modul, wie das CSC-Modul für die ASA, verwendet werden.

HTTPS-Filterung wird auf ASA nicht unterstützt. ASA kann keine Deep Packet Inspection oder Inspektion auf der Grundlage von regulären Ausdrücken für HTTPS-Datenverkehr durchführen, da der Inhalt des Pakets 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 7.2(2)
- Cisco Adaptive Security Device Manager (ASDM) Version 5.2(2) für ASA 7.2(2)

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 Software Version 7.2(2) 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 mit 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.

Um einen regulären Ausdruck zu erstellen, verwenden Sie den Befehl **regex**, der für verschiedene Features verwendet werden kann, die eine Textzuordnung erfordern. Sie können z. B. spezielle Aktionen für die Anwendungsinspektion mit dem modularen Richtlinien-Framework mit einer Inspektionsrichtlinienzuordnung konfigurieren (siehe Befehl Policy Map Type inspect). 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 mit einem regulären Ausdruck identifizieren. Sie können beispielsweise URL-Zeichenfolgen in HTTP-Paketen zuordnen. Sie können reguläre Ausdrücke in einer Klassenzuordnung für reguläre Ausdrücke gruppieren (siehe Befehl class-map type regex).

In Tabelle 1 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** Übereinstimmungen mit weniger, lose, lose usw.
{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. Beispielsweise 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 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 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 ein Zeichen kein Metazeichen ist, entspricht es dem literalen Zeichen.
\r	Frachtrücksendung	Entspricht einem Wagenrücklauf 0x0d.
\n	Netzkabel	Entspricht einer neuen Zeile 0x0a.
\t	Registerkarte	Entspricht einer Registerkarte 0x09.
\f	Vorspeise	Entspricht einem Formular-Feed 0x0c.
\xNN	Hexadezimalzahl mit Escapezeichen	Ordnet ein ASCII-Zeichen dem Hexadezimalzeichen zu (genau zwei Ziffern).
\NNN	Escaped Oktalnummer	Entspricht einem ASCII-Zeichen als Oktal (genau drei Ziffern). Beispielsweise stellt das Zeichen 040 ein Leerzeichen dar.

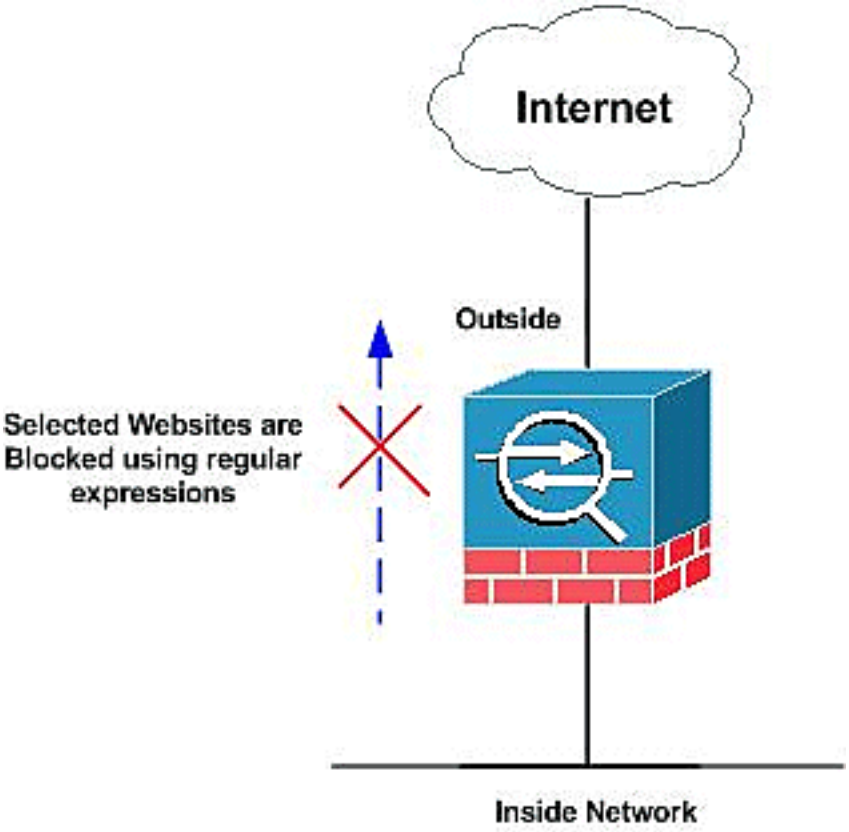
Konfigurieren

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 7.2(x) mit ASDM 5.2

ASA CLI-Konfiguration

ASA CLI-Konfiguration

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(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
```

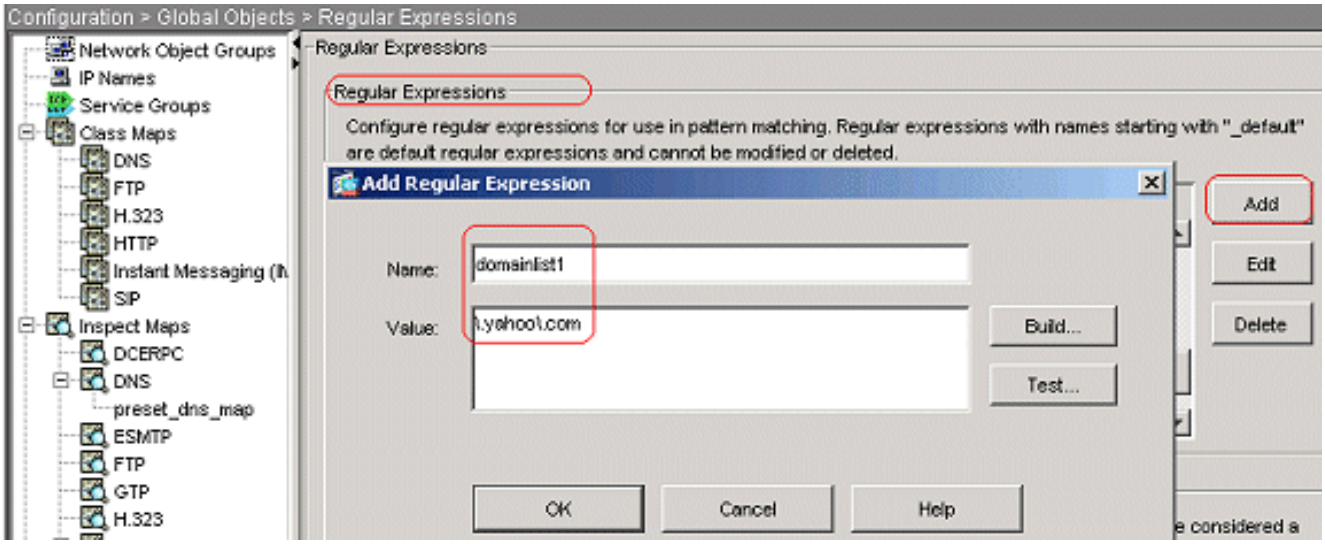
```
asdm history enable arp timeout 14400 route DMZ 0.0.0.0
0.0.0.0 10.77.241.129 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00
sip_media 0:02:00 sip-invite 0:03:00 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
esmtp 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 will be blocked prompt hostname context
Cryptochecksum:e629251a7c37af205c289cf78629fc11 : end
ciscoasa#
```

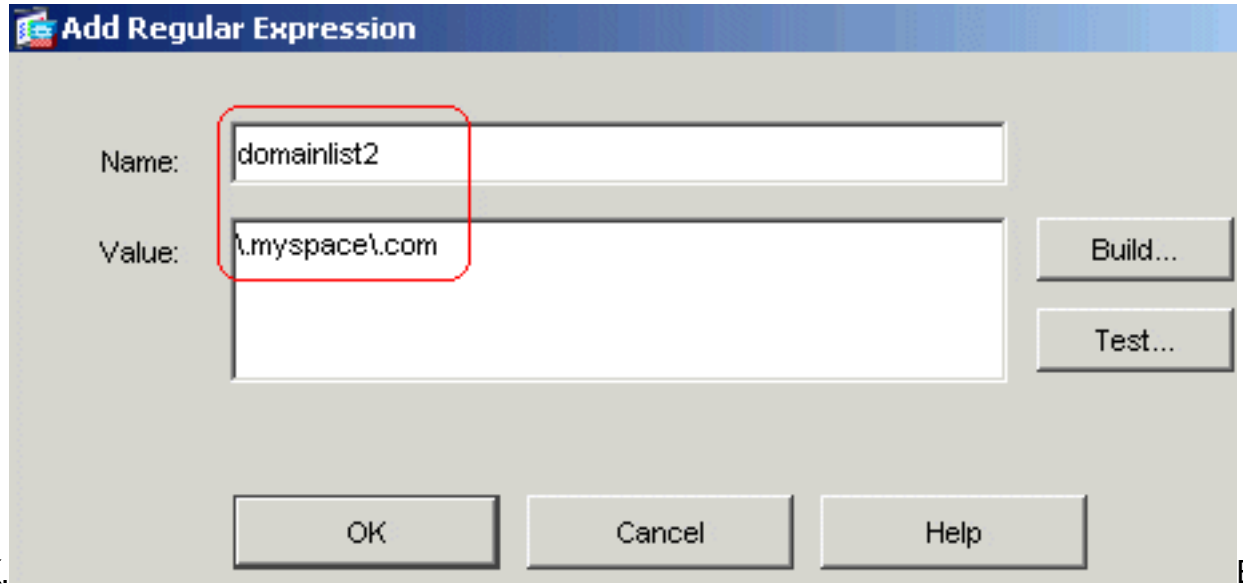
ASA-Konfiguration 7.2(x) mit ASDM 5.2

Gehen Sie wie folgt vor, um reguläre Ausdrücke zu konfigurieren und sie auf MPF anzuwenden, um bestimmte Websites zu blockieren:

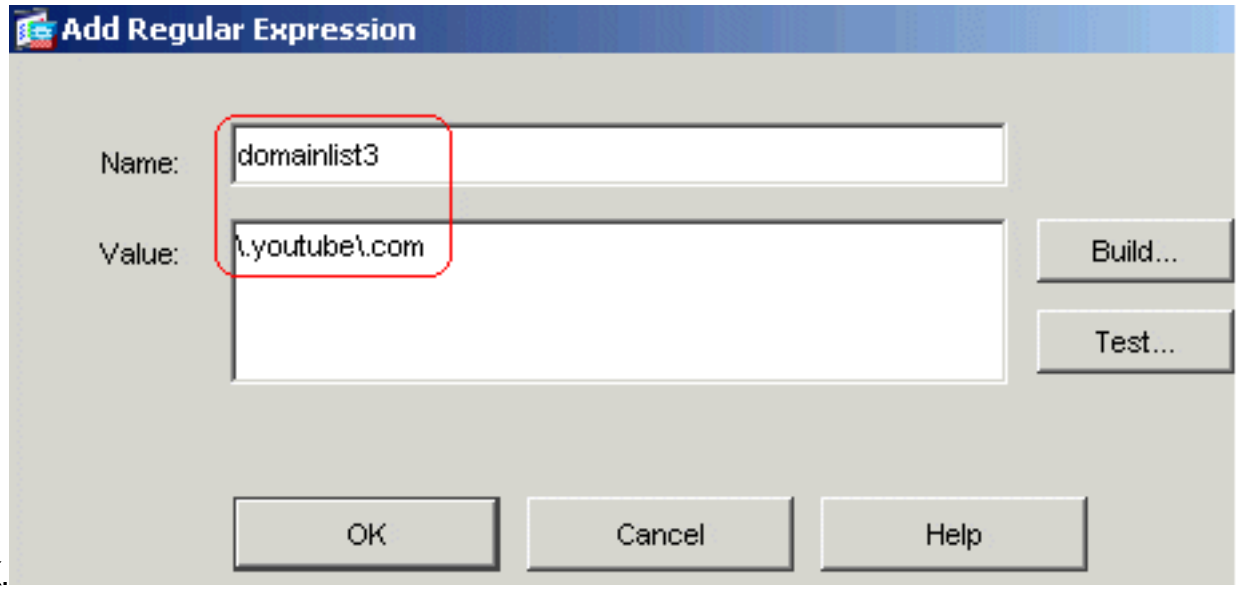
1. **Erstellen regulärer Ausdrücke**Wählen Sie **Konfiguration > Globale Objekte > Reguläre Ausdrücke** aus, und klicken Sie unter der Registerkarte Regulärer Ausdruck auf **Hinzufügen**, um reguläre Ausdrücke zu erstellen.Erstellen Sie eine **domainlist1 für** reguläre Ausdrücke, um den Domänennamen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



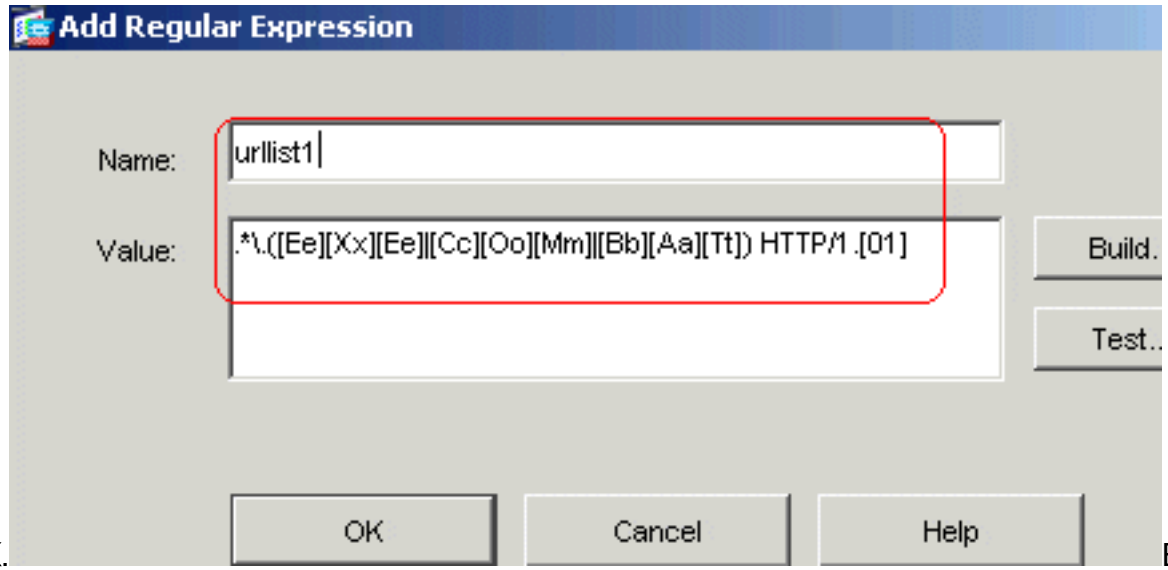
Erstellen Sie einen regulären Ausdruck **domainlist2**, um den Domänennamen **myspace.com** zu erfassen. Klicken Sie auf



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

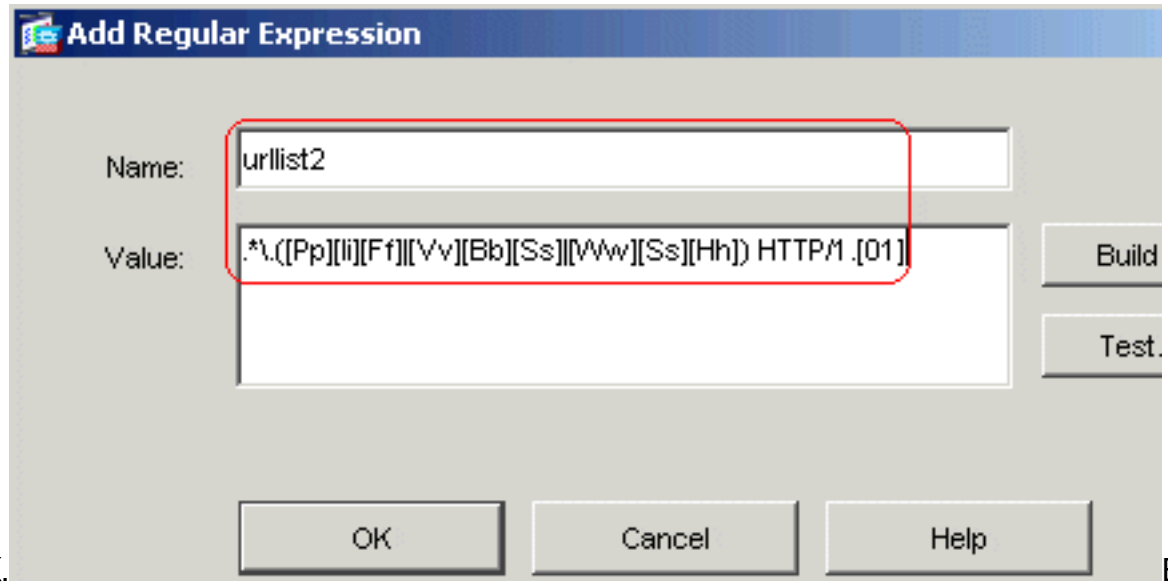


OK. Erstellen Sie einen regulären Ausdruck **urllist1**, um Dateierweiterungen wie **exe**, **com** und **bat** zu erfassen, sofern die vom Webbrowser verwendete HTTP-Version entweder 1.0 oder 1.1 sein muss. Klicken Sie auf

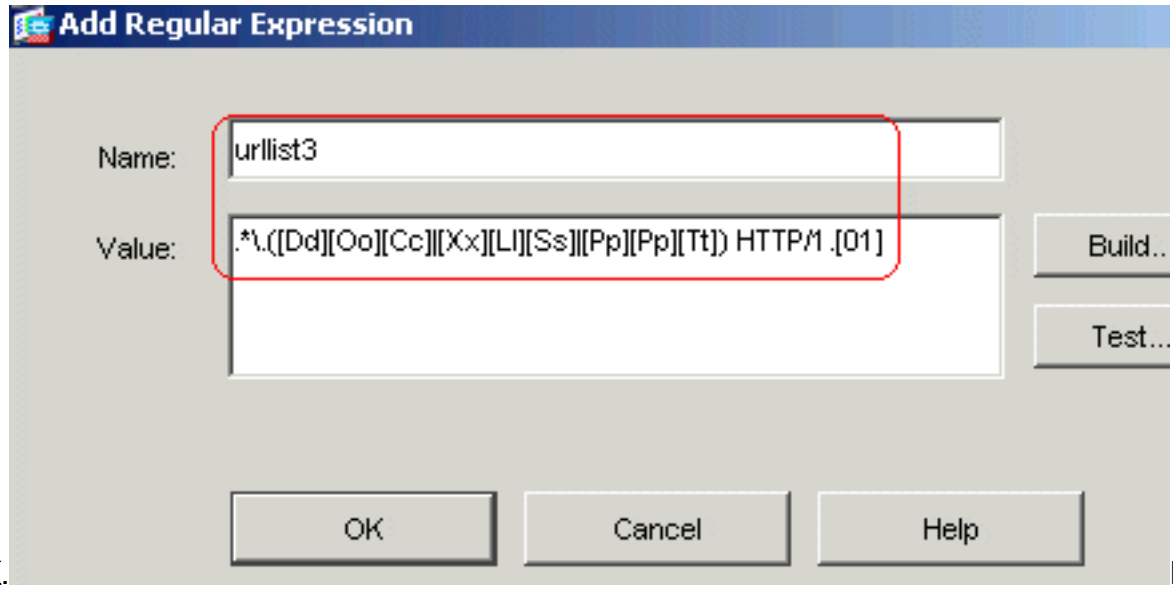


OK. Erstellen Sie einen regulären Ausdruck **urllist2**, um die Dateierweiterungen wie **pif**, **vbs** und **wsh** zu erfassen, sofern die vom Webbrowser verwendete HTTP-Version entweder 1.0 oder 1.1 ist.

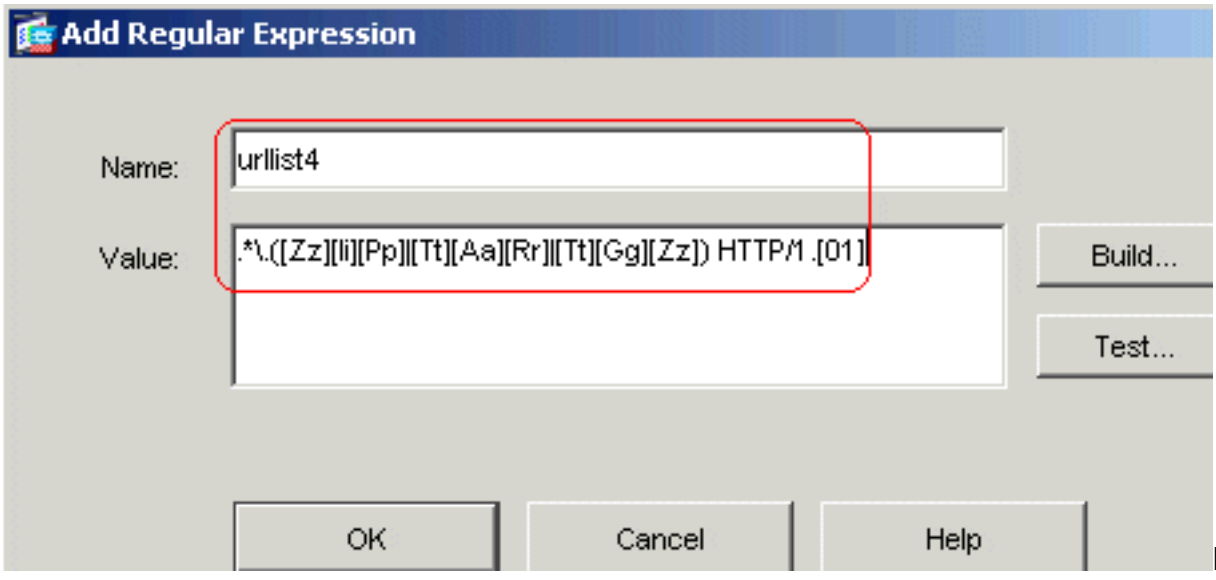
Klicken Sie auf



OK. Erstellen Sie eine **URLlist3 für** reguläre Ausdrücke, um Dateierweiterungen wie **doc**, **xls** und **ppt** zu erfassen, sofern die HTTP-Version, die vom Webbrowser verwendet wird, entweder 1.0 oder 1.1 ist. Klicken Sie auf

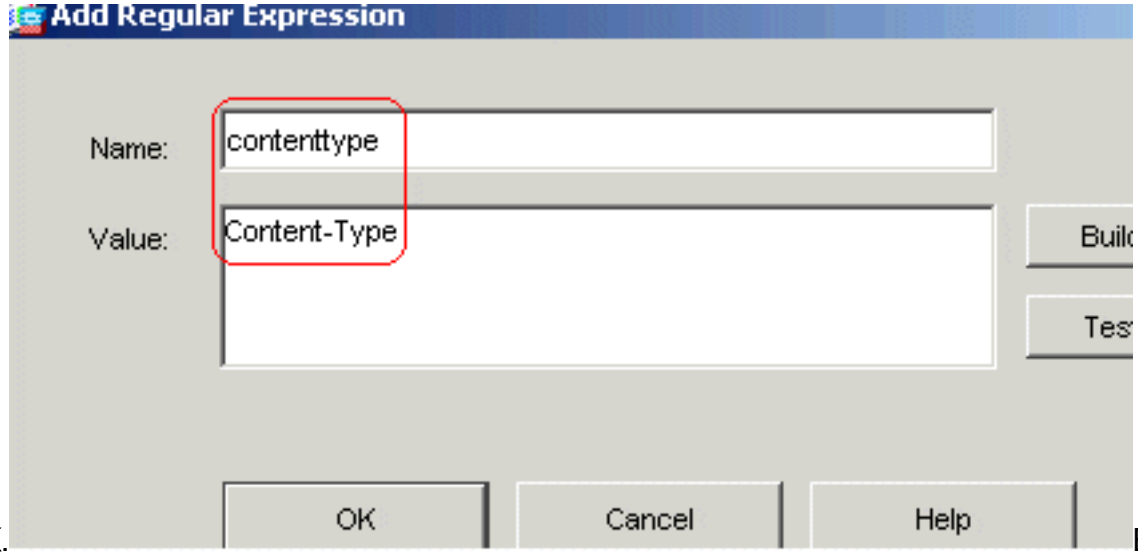


OK. Erstellen Sie eine **URLlist4** für reguläre Ausdrücke, um Dateierweiterungen wie **zip**, **tar** und **tgz** zu erfassen, sofern die HTTP-Version, die vom Webbrowser verwendet wird, entweder 1.0 oder 1.1 ist. Klicken Sie auf

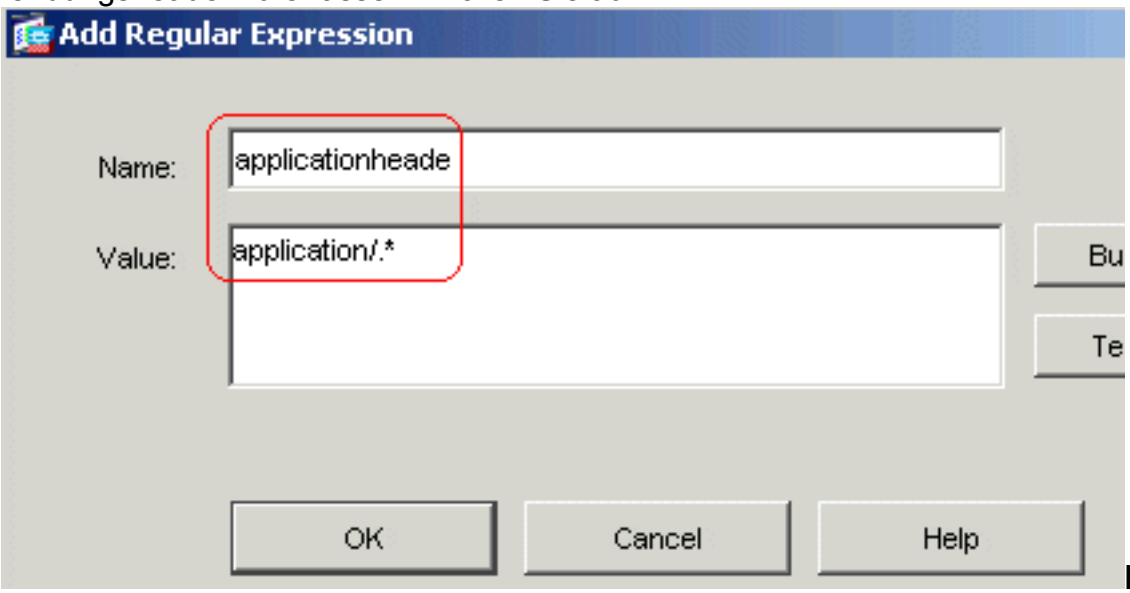


OK. Ers

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

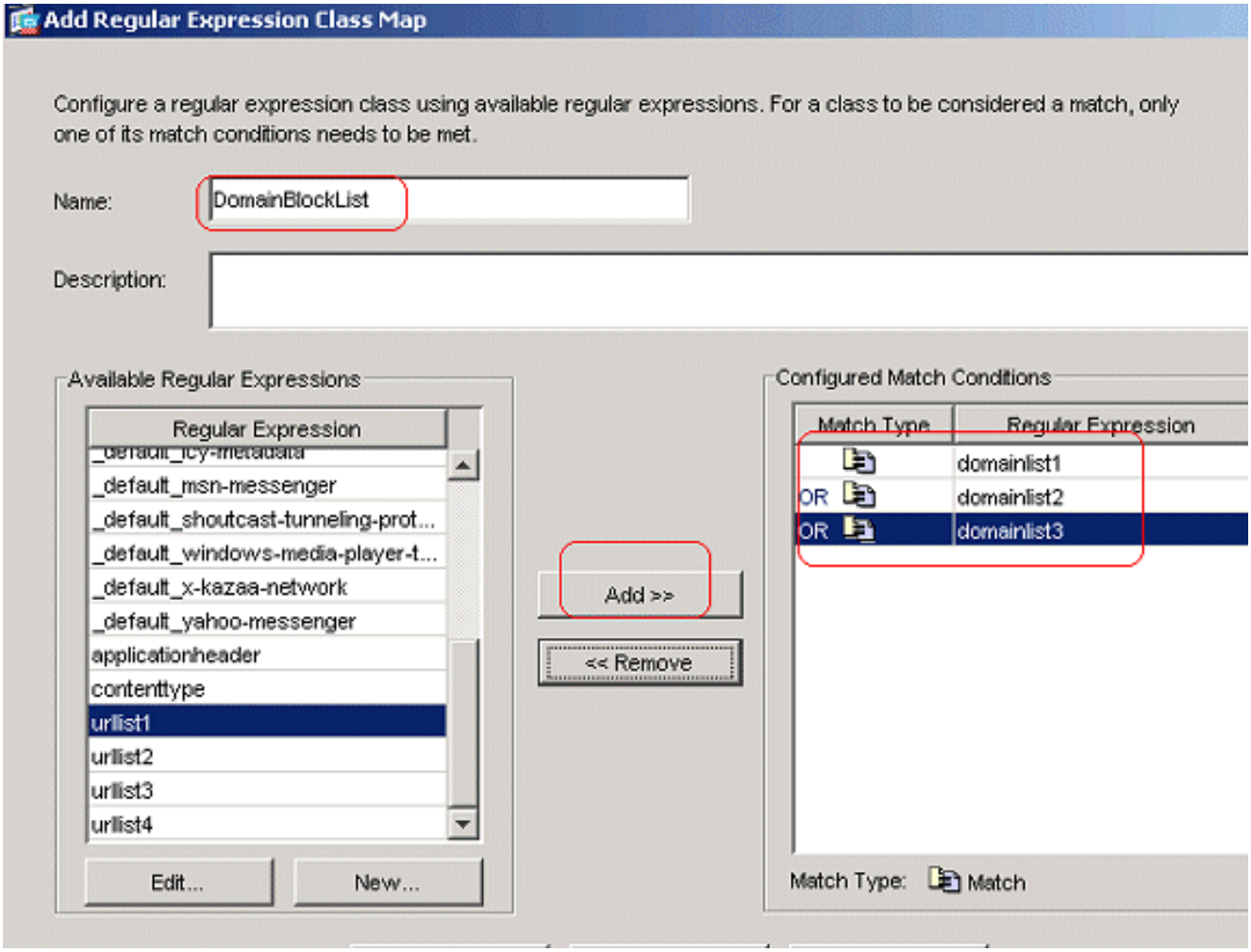


OK. Erstellen Sie einen **Anwendungsheader für** reguläre Ausdrücke, um die verschiedenen Anwendungsheader zu erfassen. Klicken Sie auf

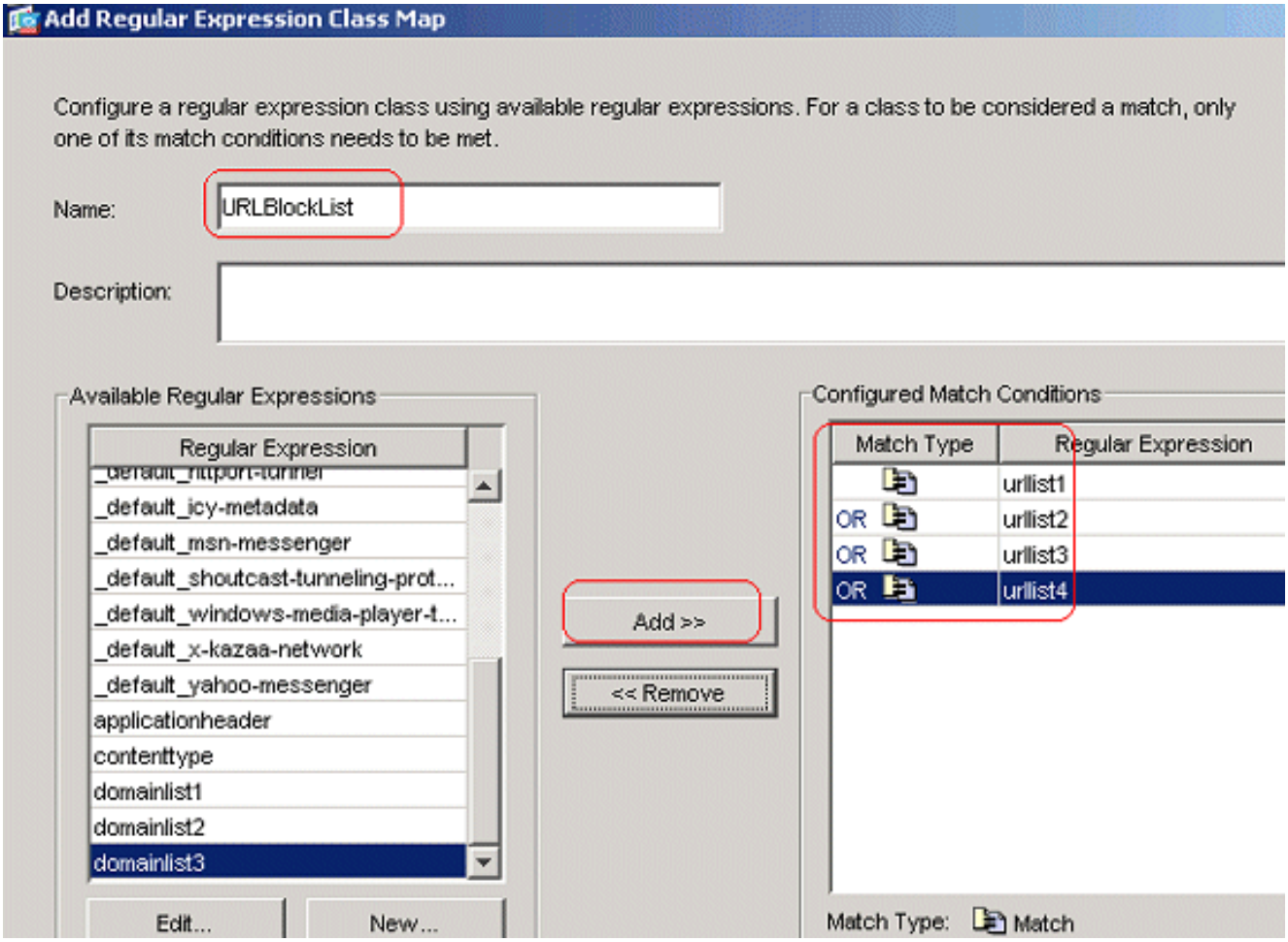


OK. **Entsprechende CLI-Konfiguration**

2. **Erstellen von Klassen regulärer Ausdrücke**Wählen Sie **Konfiguration > Globale Objekte > Reguläre Ausdrücke**, und klicken Sie auf **Hinzufügen** unter der Registerkarte **Klassen für reguläre Ausdrücke**, um die verschiedenen Klassen zu erstellen.Erstellen Sie eine Klasse für reguläre Ausdrücke **DomainBlockList**, um einen der regulären Ausdrücke zu übernehmen: domainlist1, domainlist2 und domainlist3. Klicken Sie auf **OK**.

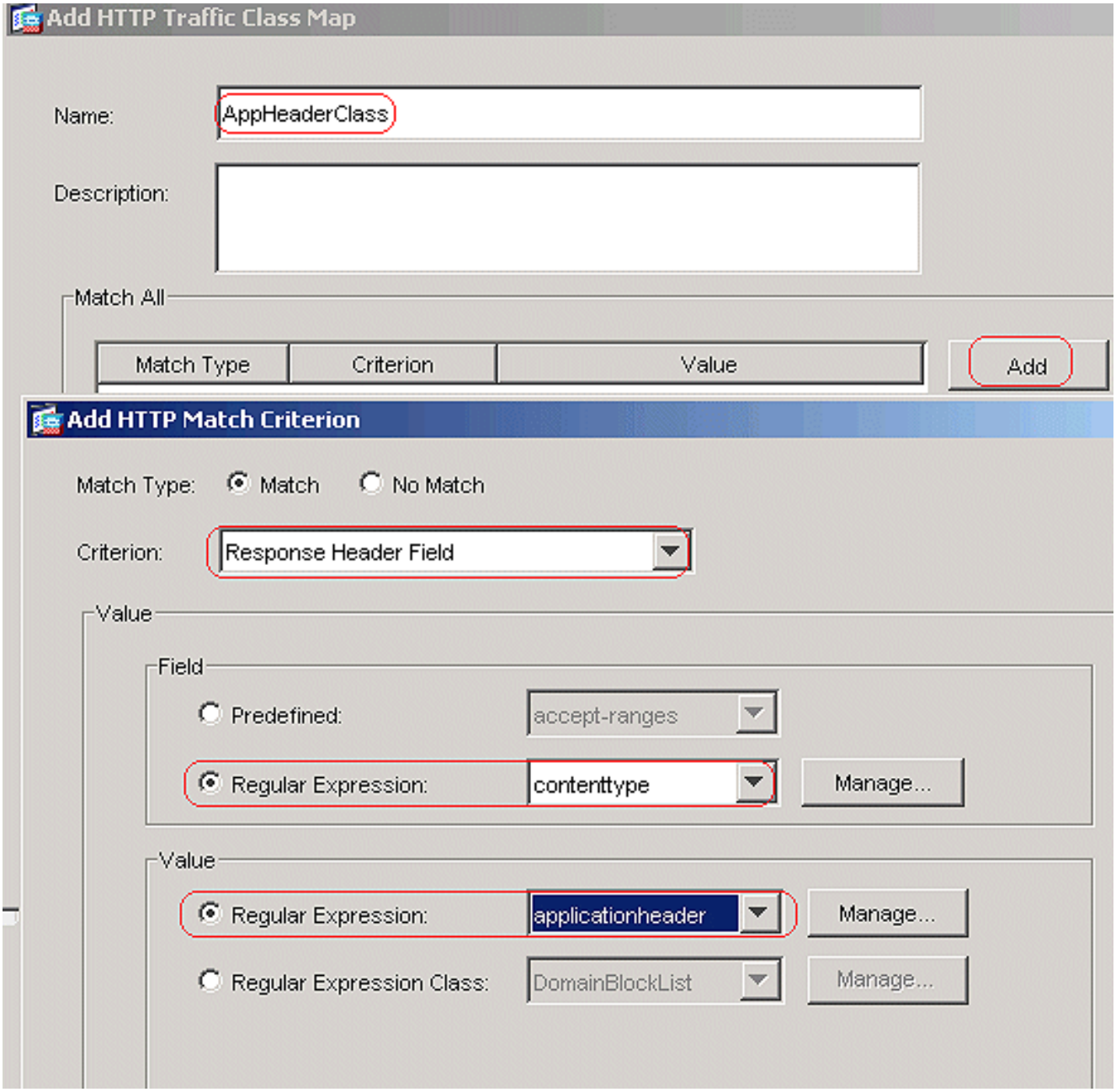


Erstellen Sie eine **URLBlockList für** reguläre Ausdrücke, um einen der regulären Ausdrücke zuzuordnen: urllist1, urllist2, urllist3 und urllist4. Klicken Sie auf **OK**.

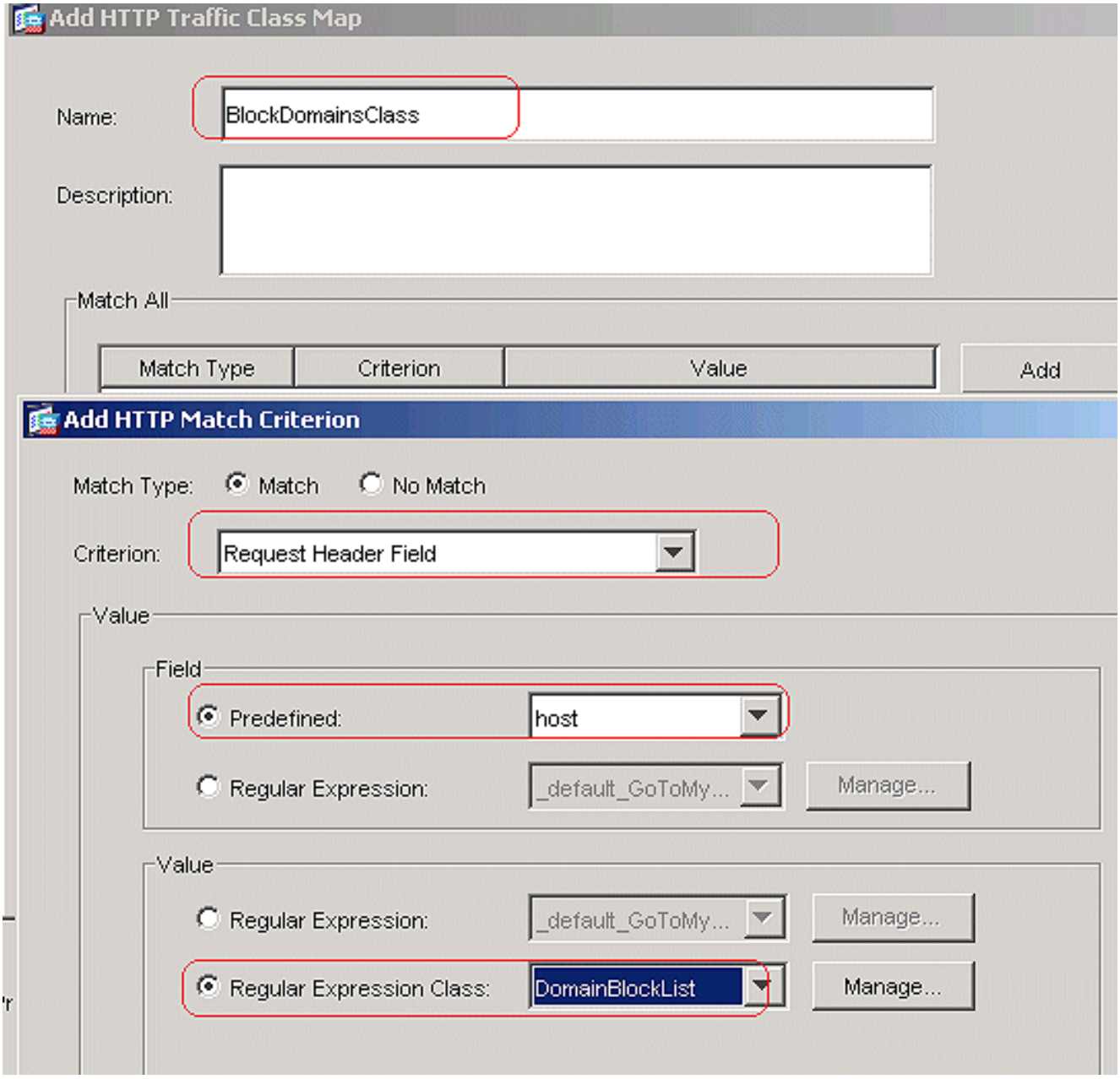


Entsprechende CLI-Konfiguration

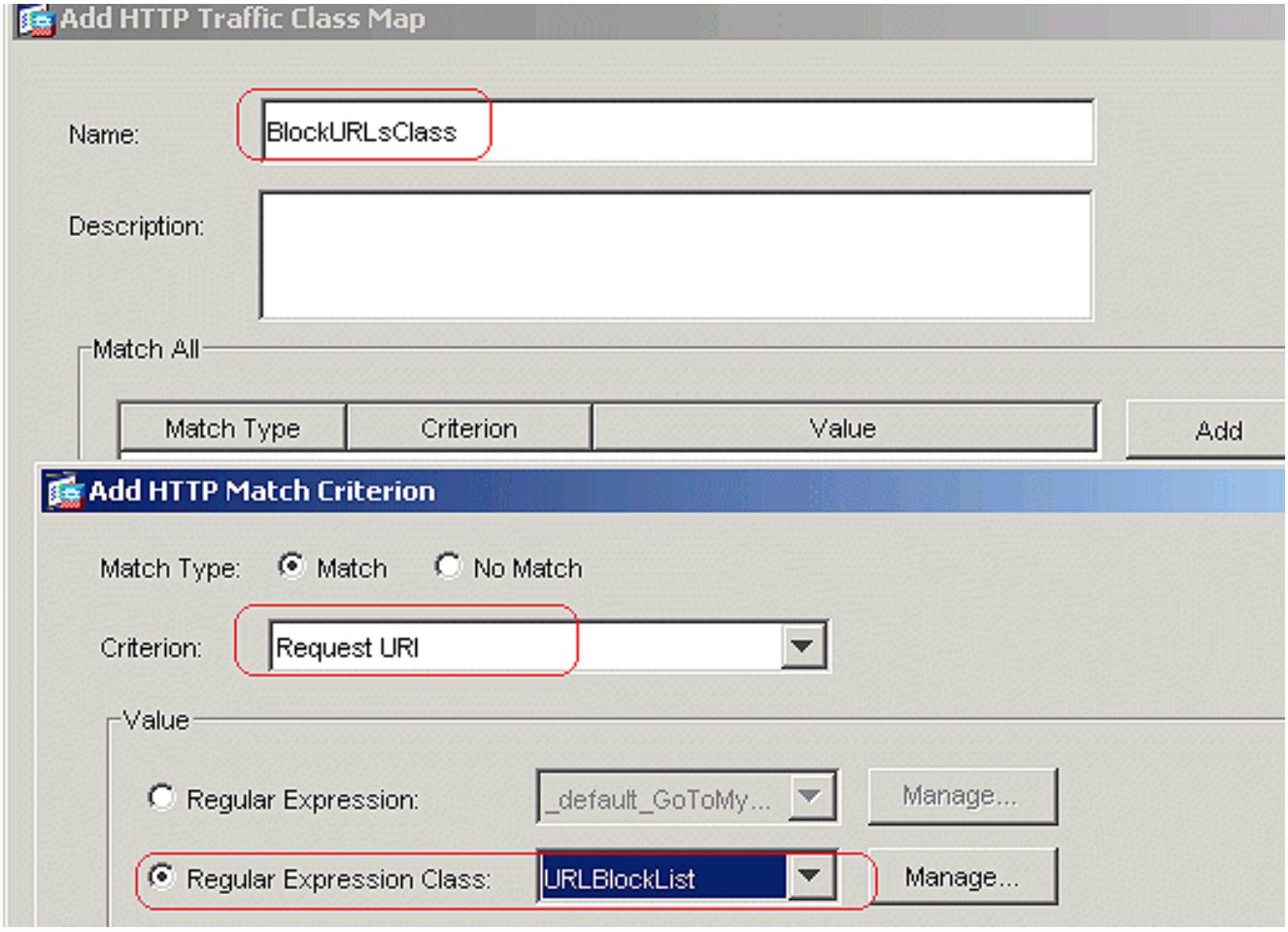
3. **Identifizierten Datenverkehr mit Klassenzuordnungen untersuchen**Wählen Sie **Configuration > Global Objects > Class Maps > HTTP > Add** aus, um eine Klassenzuordnung zum Überprüfen des HTTP-Datenverkehrs zu erstellen, der durch verschiedene reguläre Ausdrücke identifiziert wurde.Erstellen Sie eine Klassenzuordnung **AppHeaderClass**, um den Response-Header mit der Erfassung regulärer Ausdrücke abzustimmen.



Klicken Sie auf **OK**.Erstellen Sie eine Klassenzuordnung **BlockDomainsClass**, um den Anforderungsheader mit der Erfassung regulärer Ausdrücke abzustimmen.

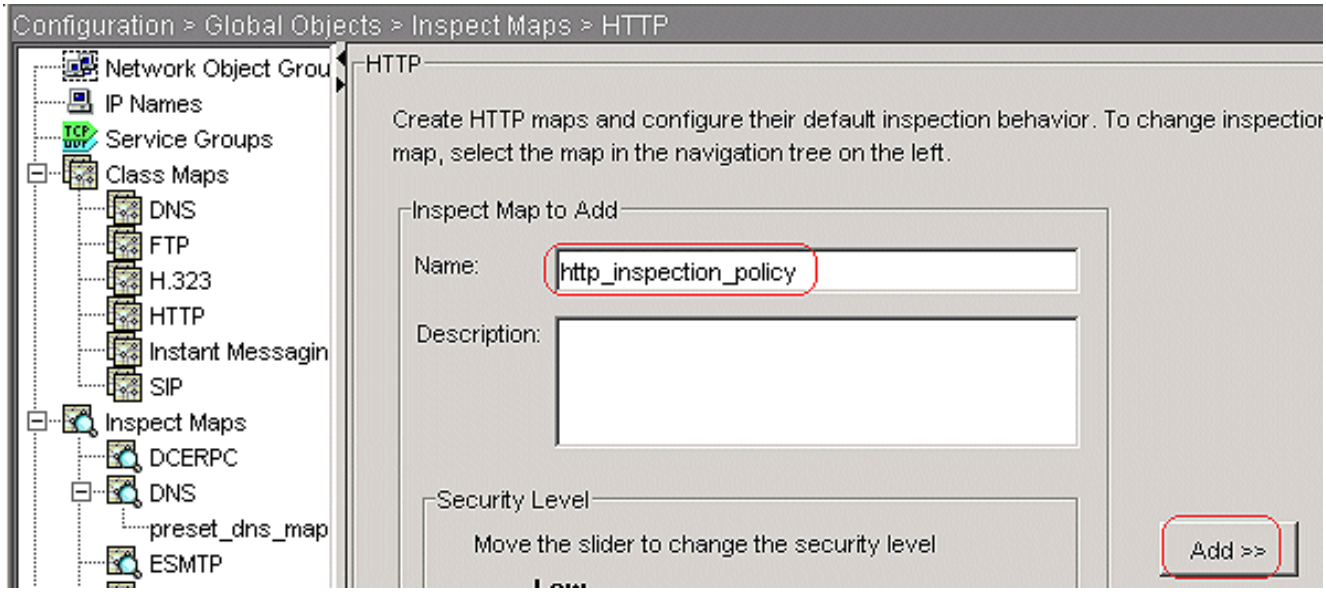


Klicken Sie auf **OK**.Erstellen Sie eine Klassenzuordnung **BlockURLsClass**, um den Anforderungs-URI mit der Erfassung regulärer Ausdrücke abzustimmen.

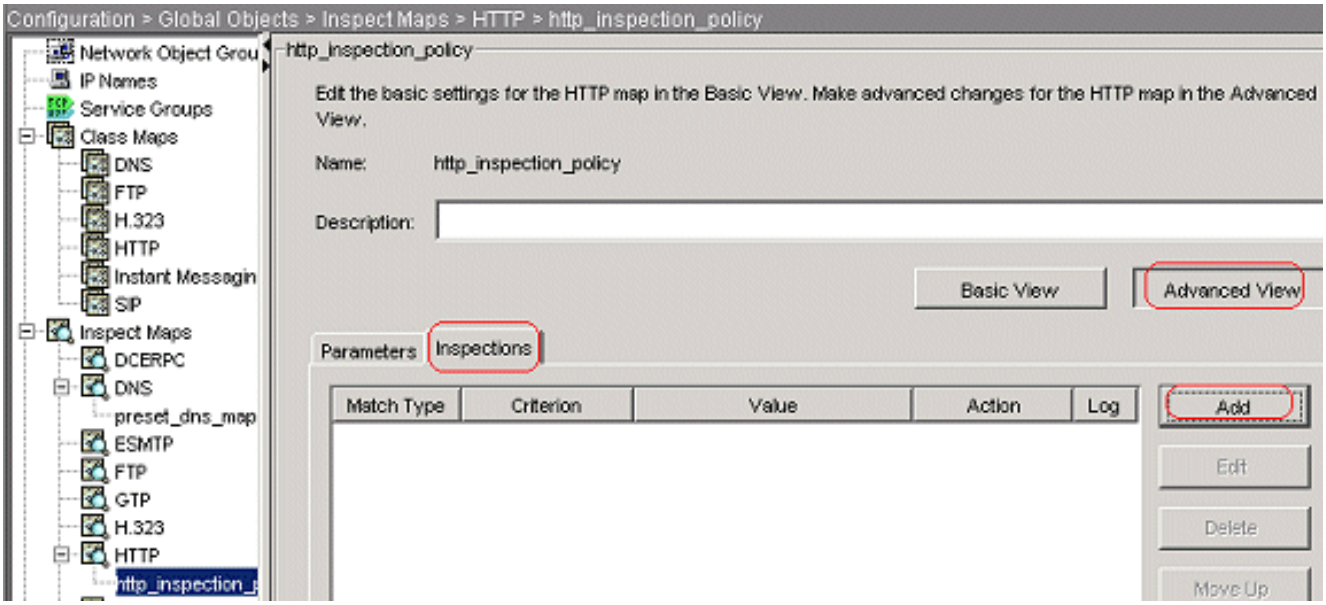


Klicken Sie auf **OK**.**Entsprechende CLI-Konfiguration**

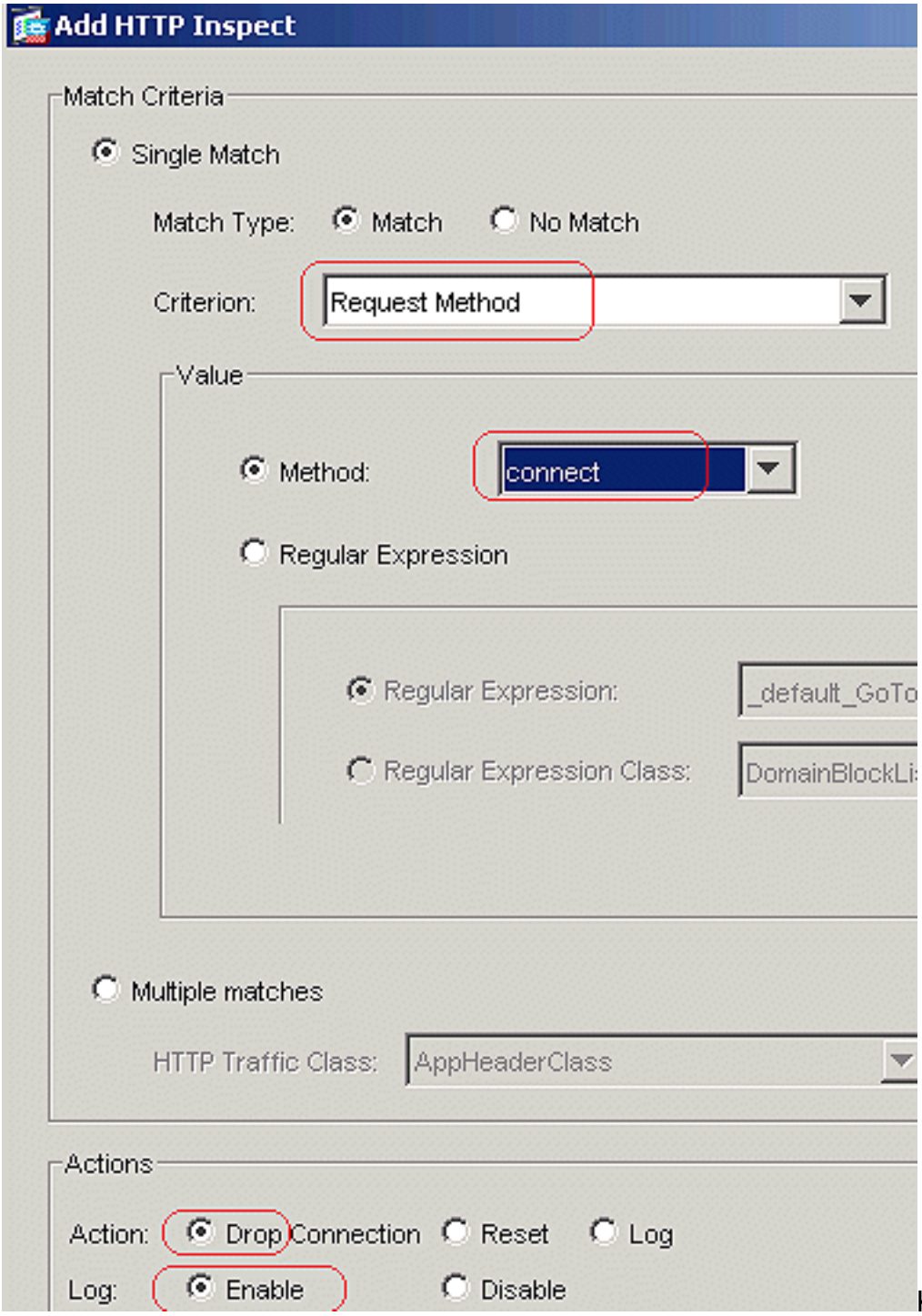
4. **Festlegen der Aktionen für den abgeglichenen Datenverkehr in der Überprüfungsrichtlinie**Wählen Sie **Configuration > Global Objects > Inspect Maps > HTTP**, um eine **http_Inspection_policy** zu erstellen, um die Aktion für den zugeordneten Datenverkehr festzulegen. Klicken Sie auf **Hinzufügen** und **Übernehmen**.



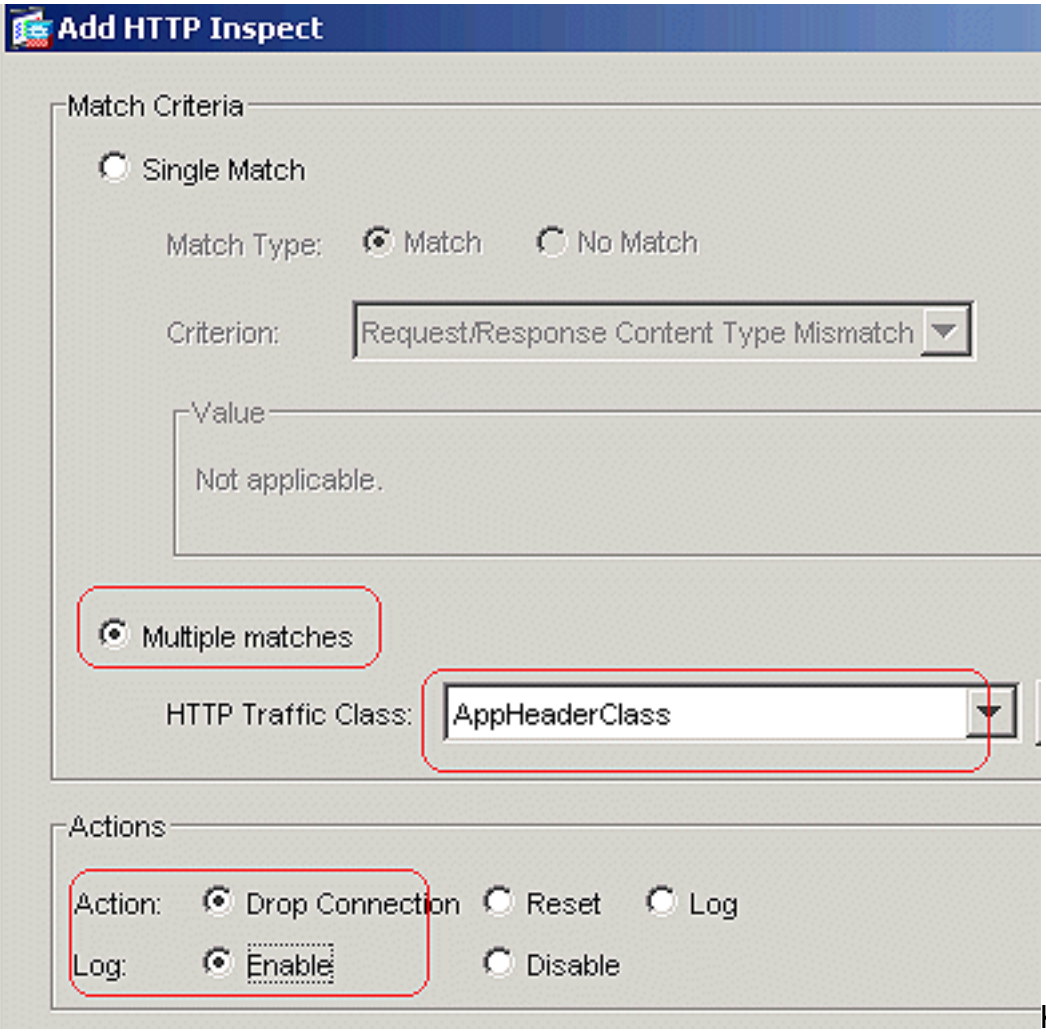
Wählen Sie **Configuration > Global Objects > Inspect Maps > HTTP > http_Inspection_policy** und klicken Sie auf **Advanced View > Inspections > Add**, um die Aktionen für die verschiedenen bisher erstellten Klassen festzulegen.



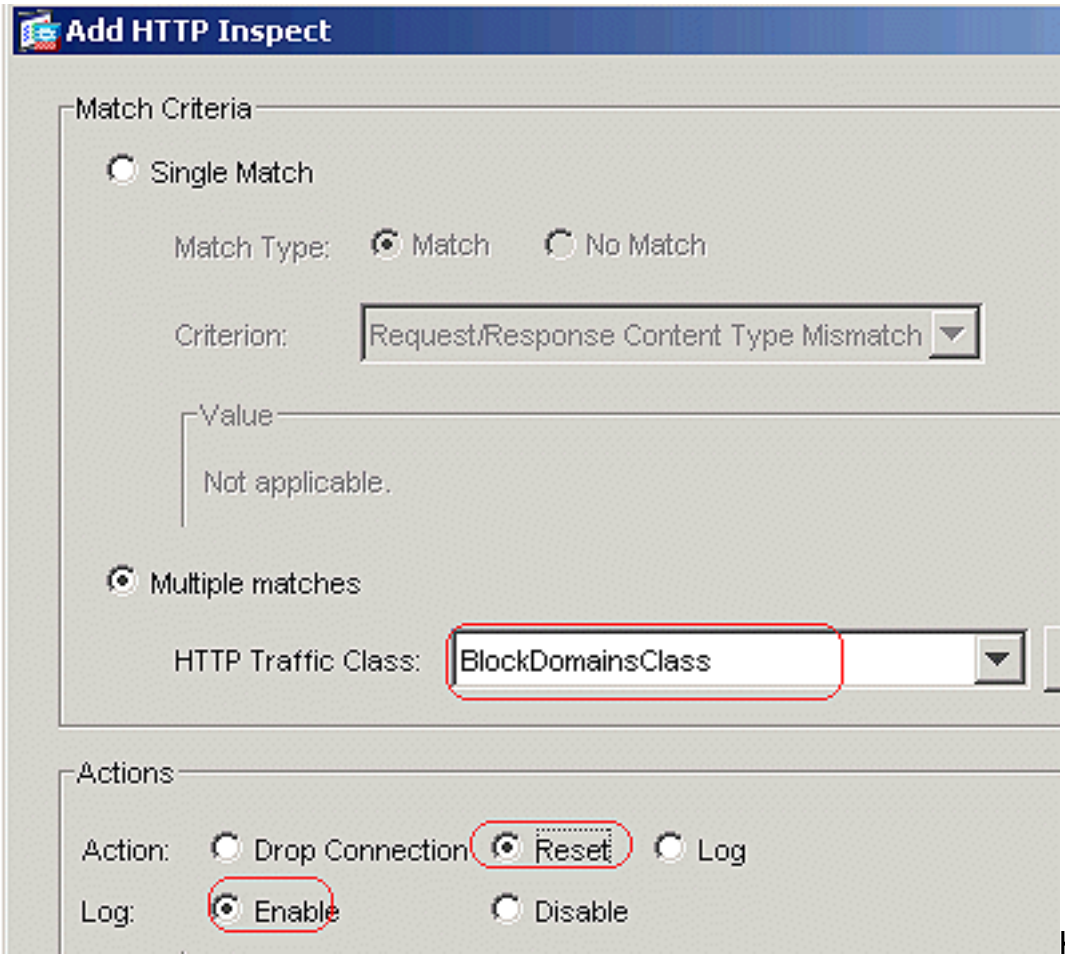
Klicken Sie auf **OK**.Legen Sie die Aktion als **Drop Connection** fest. **Aktivieren Sie** die Protokollierung für das Kriterium als Request Method und Value as



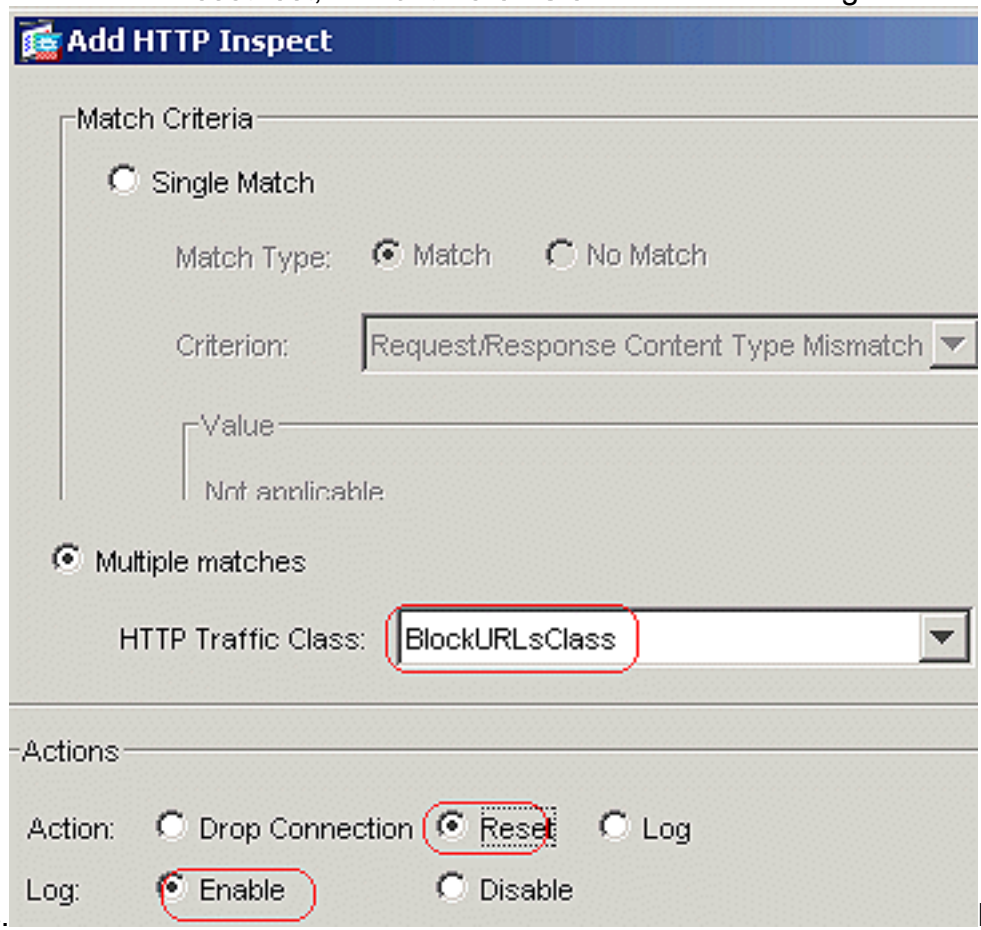
connect. Klicken Sie auf **OK**.Legen Sie die Aktion als **Drop Connection fest**, und **aktivieren Sie** die Protokollierung für die Klasse



AppHeaderClass.K licken Sie auf **OK**.Legen Sie die Aktion als **Reset fest**, und **aktivieren Sie** die Protokollierung für die Klasse **BlockDomainsClass**.



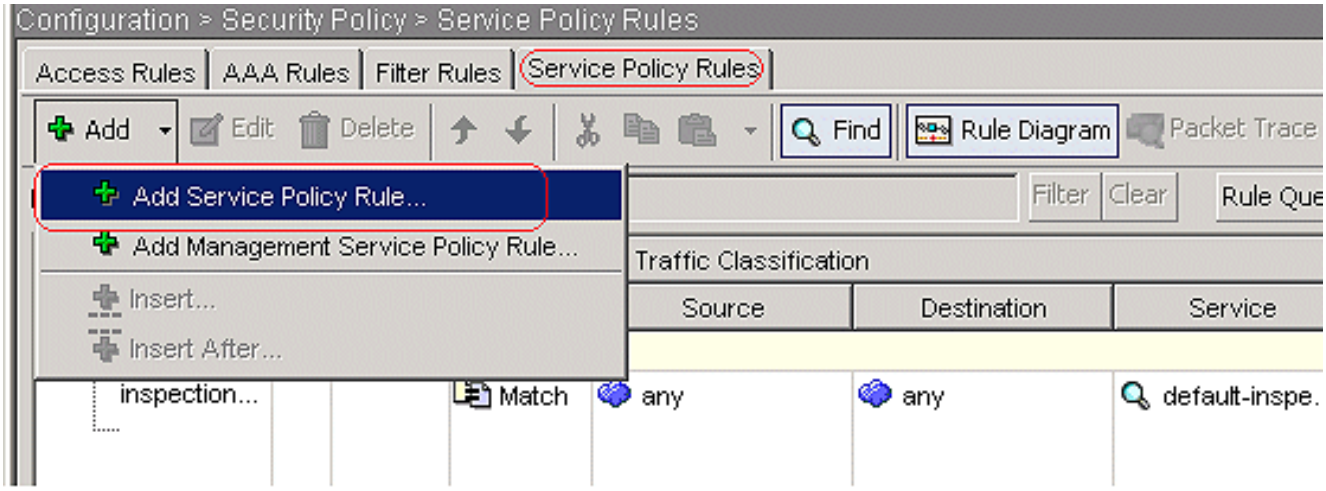
Klicken Sie auf **OK**.Legen Sie die Aktion als **Reset fest**, und **aktivieren Sie** die Protokollierung für die Klasse



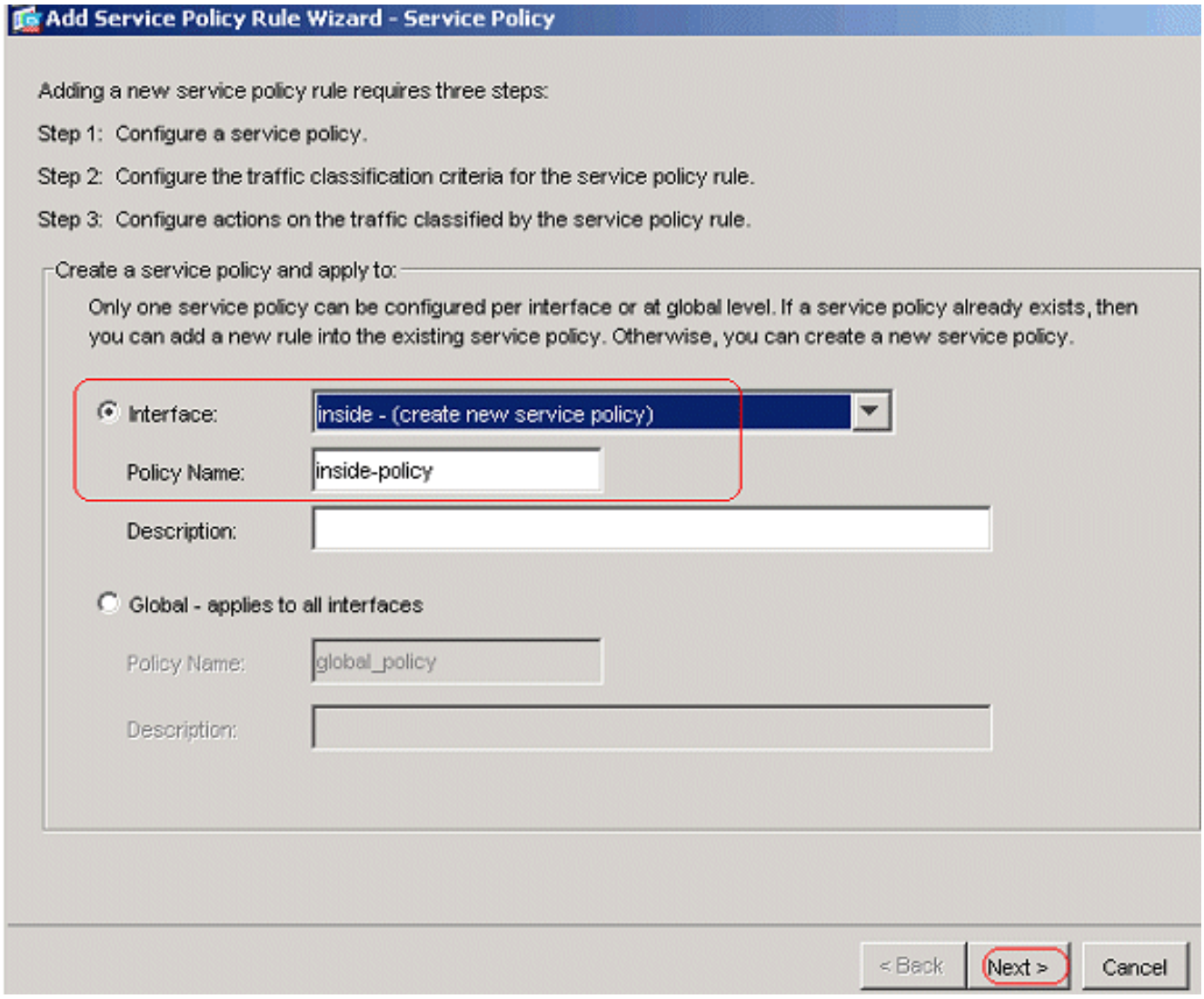
BlockURLsClass. Klicken Sie auf **OK**.Klicken Sie auf **Übernehmen**.**Entsprechende CLI-Konfiguration**

5. **Wenden Sie die Inspection-http-Richtlinie auf die Schnittstelle an.**Wählen Sie auf der Registerkarte "Service Policy Rules" (Servicebestimmungen) **Configuration > Security Policy**

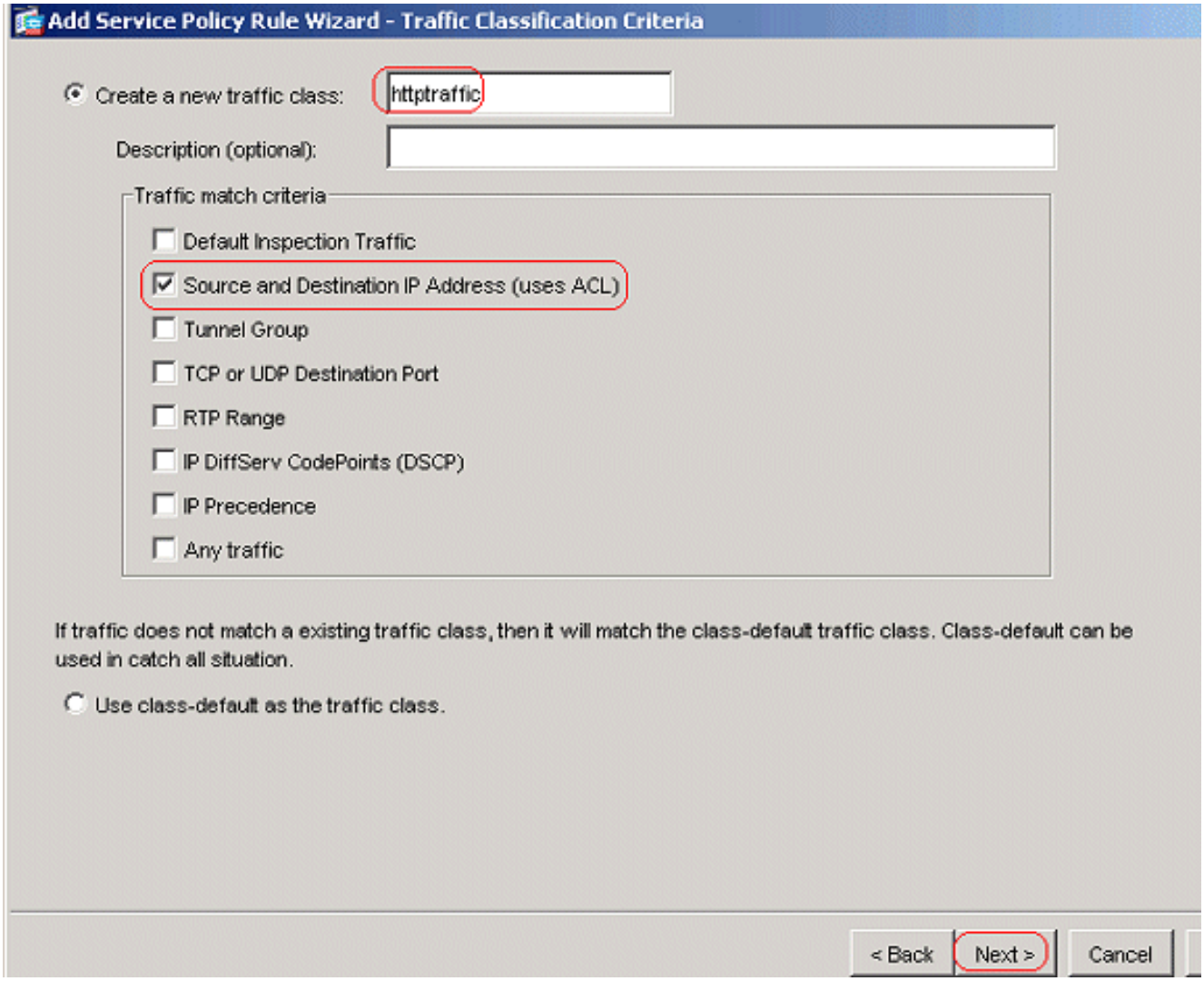
> Service Policy Rules > Add > Add Service Policy Rule (Konfiguration > Sicherheitsrichtlinie > Service-Richtlinien > Hinzufügen > Service Policy-Regel hinzufügen aus.



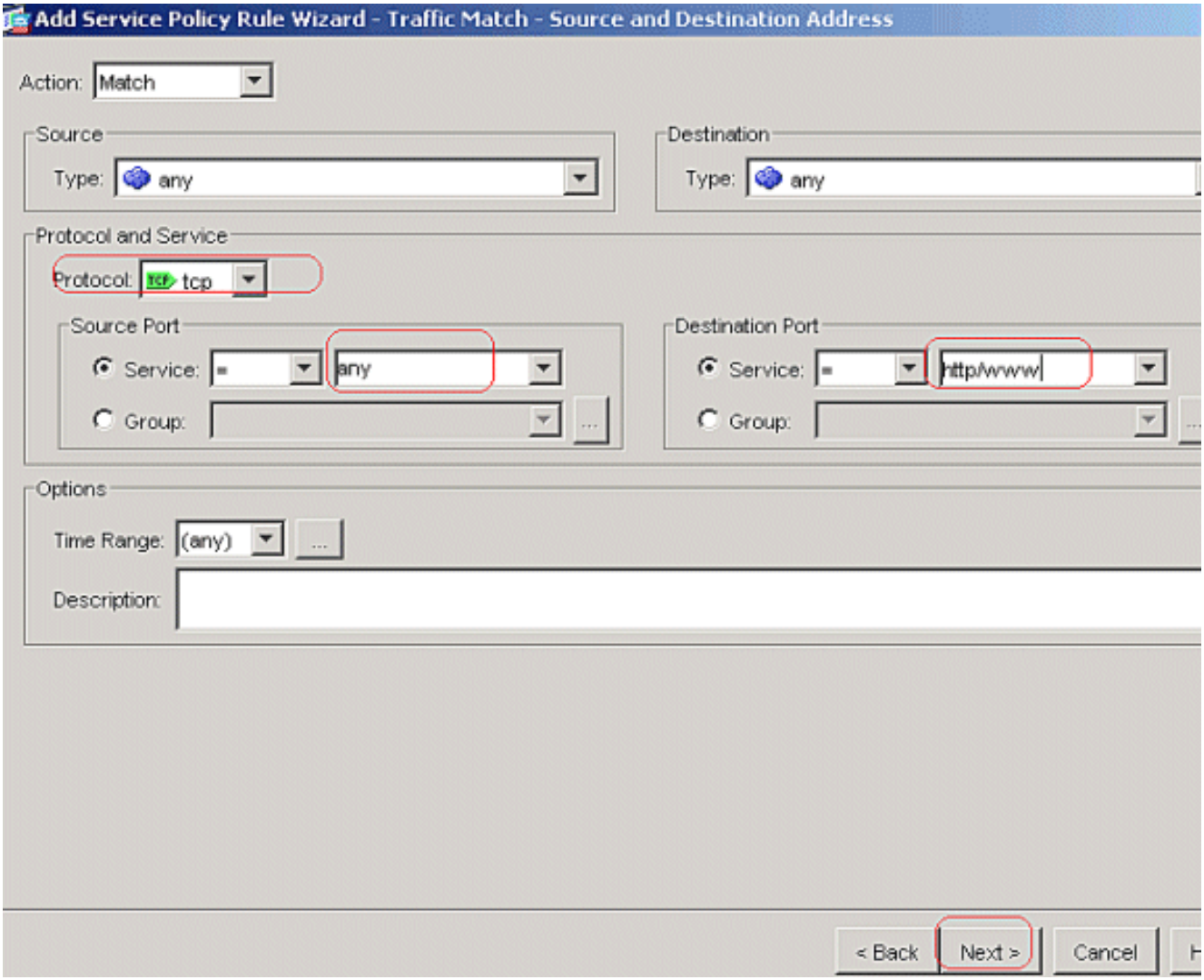
HTTP-DatenverkehrWählen Sie im Dropdown-Menü das Optionsfeld **Interface (Schnittstelle)** mit der **internen** Schnittstelle aus, und geben Sie den Richtliniennamen als **Insider-Richtlinie an**. Klicken Sie auf **Weiter**.



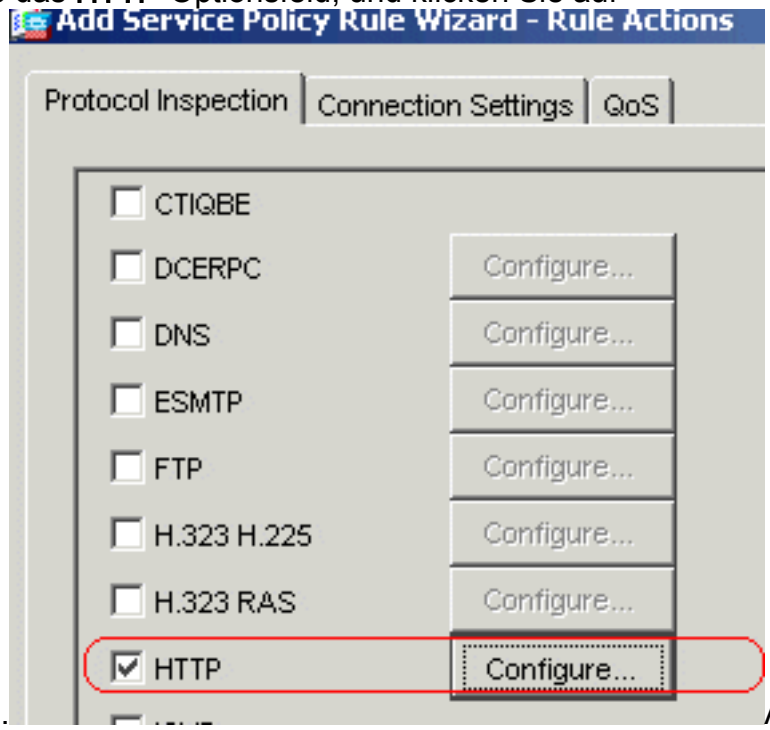
Erstellen Sie eine Klassenzuordnung **httptraffic**, und überprüfen Sie die **Quell- und Ziel-IP-Adresse (verwendet ACL)**. Klicken Sie auf **Weiter**.



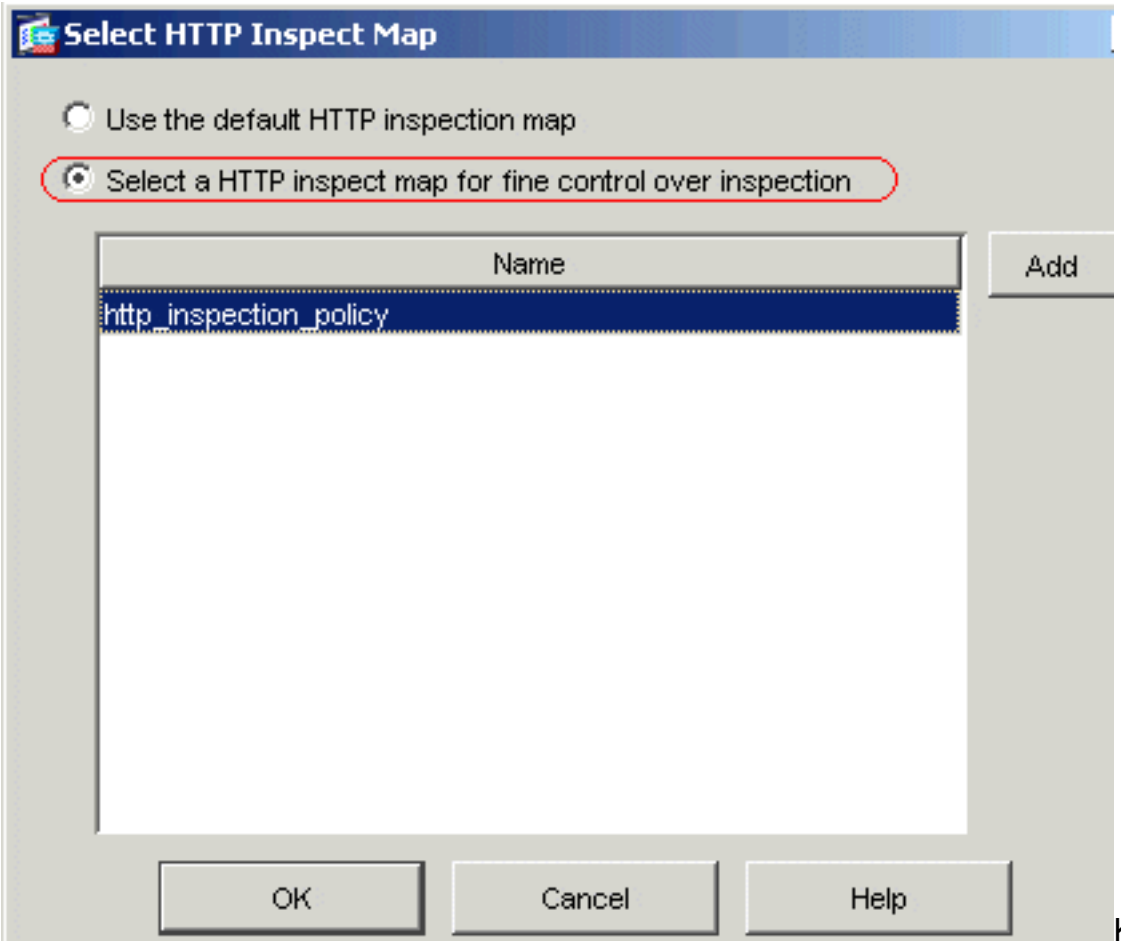
Wählen Sie Source und Destination (Quelle und Ziel) wie **jeder** mit dem TCP-Port als **HTTP aus**. Klicken Sie auf
Weiter.



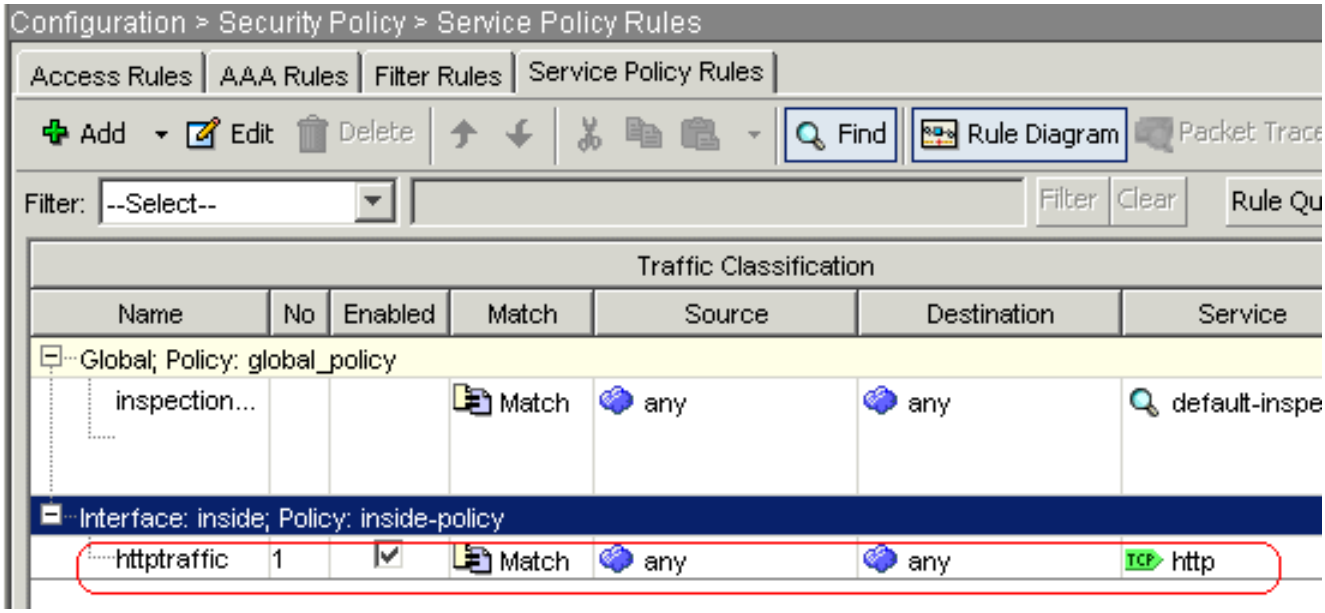
Aktivieren Sie das **HTTP-**Optionsfeld, und klicken Sie auf



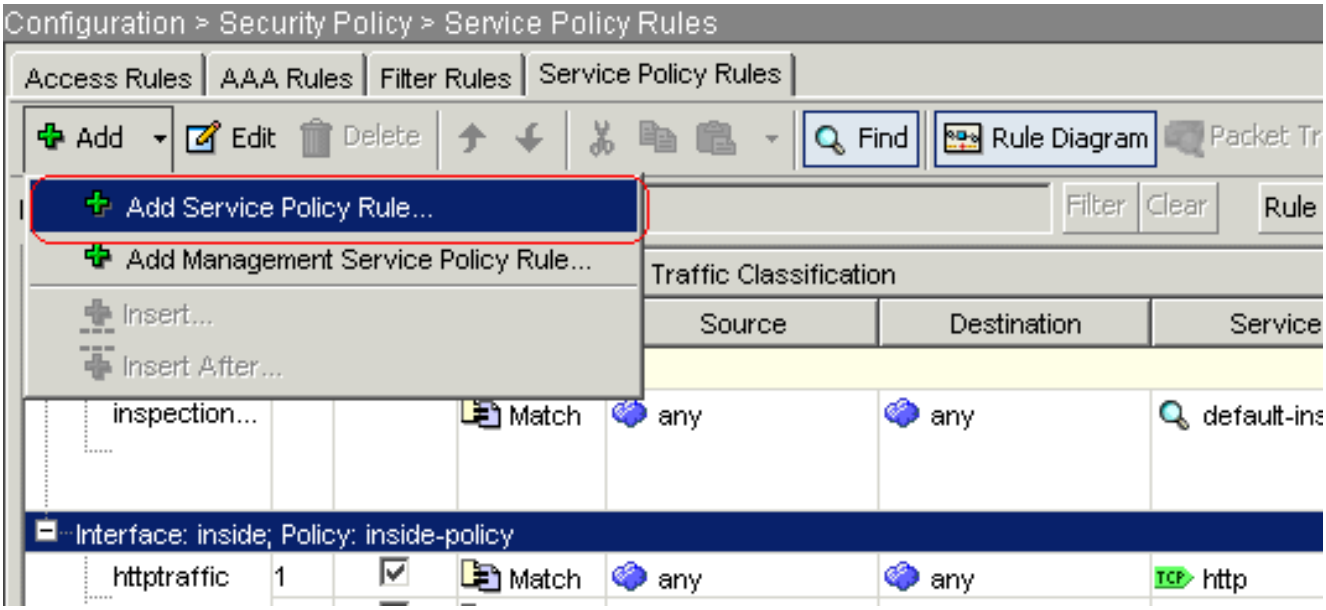
Konfigurieren. Aktivieren Sie das Optionsfeld **Wählen Sie eine HTTP-Inspektionszuordnung für das Steuerelement über Inspektion aus**. Klicken Sie auf



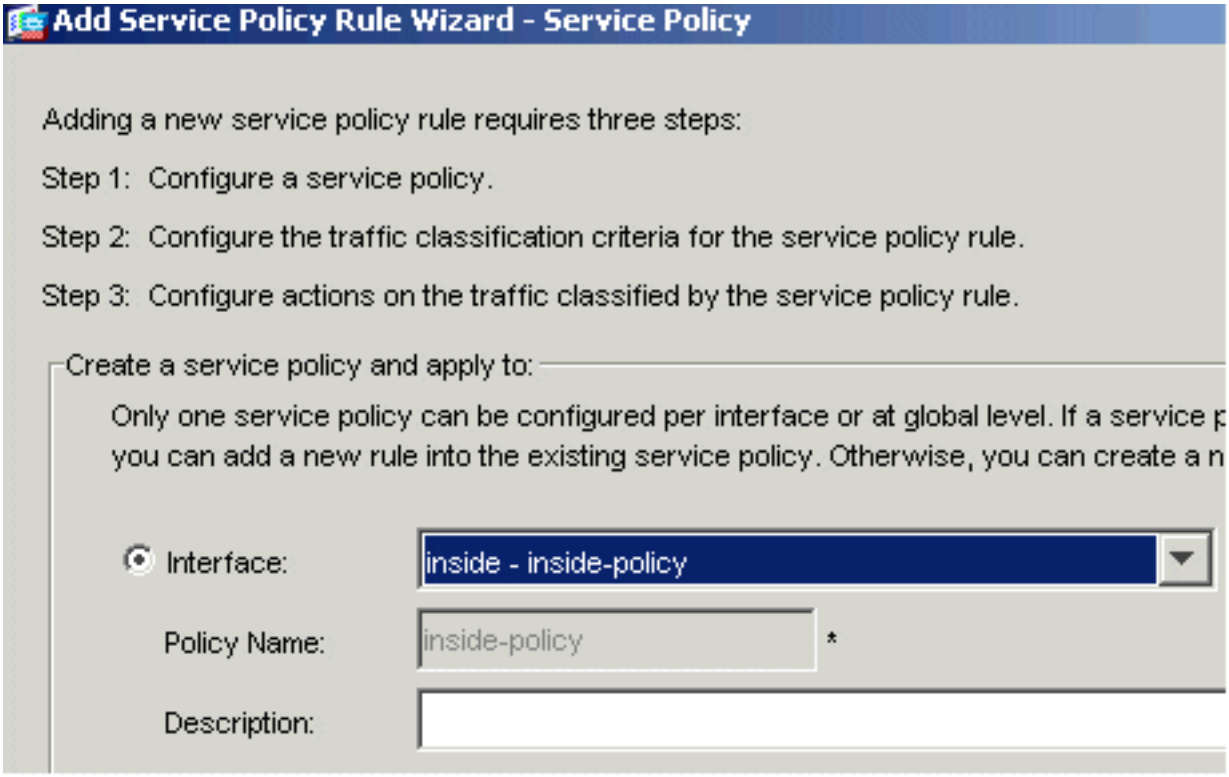
OK. Klicken Sie auf **Fertig stellen**.



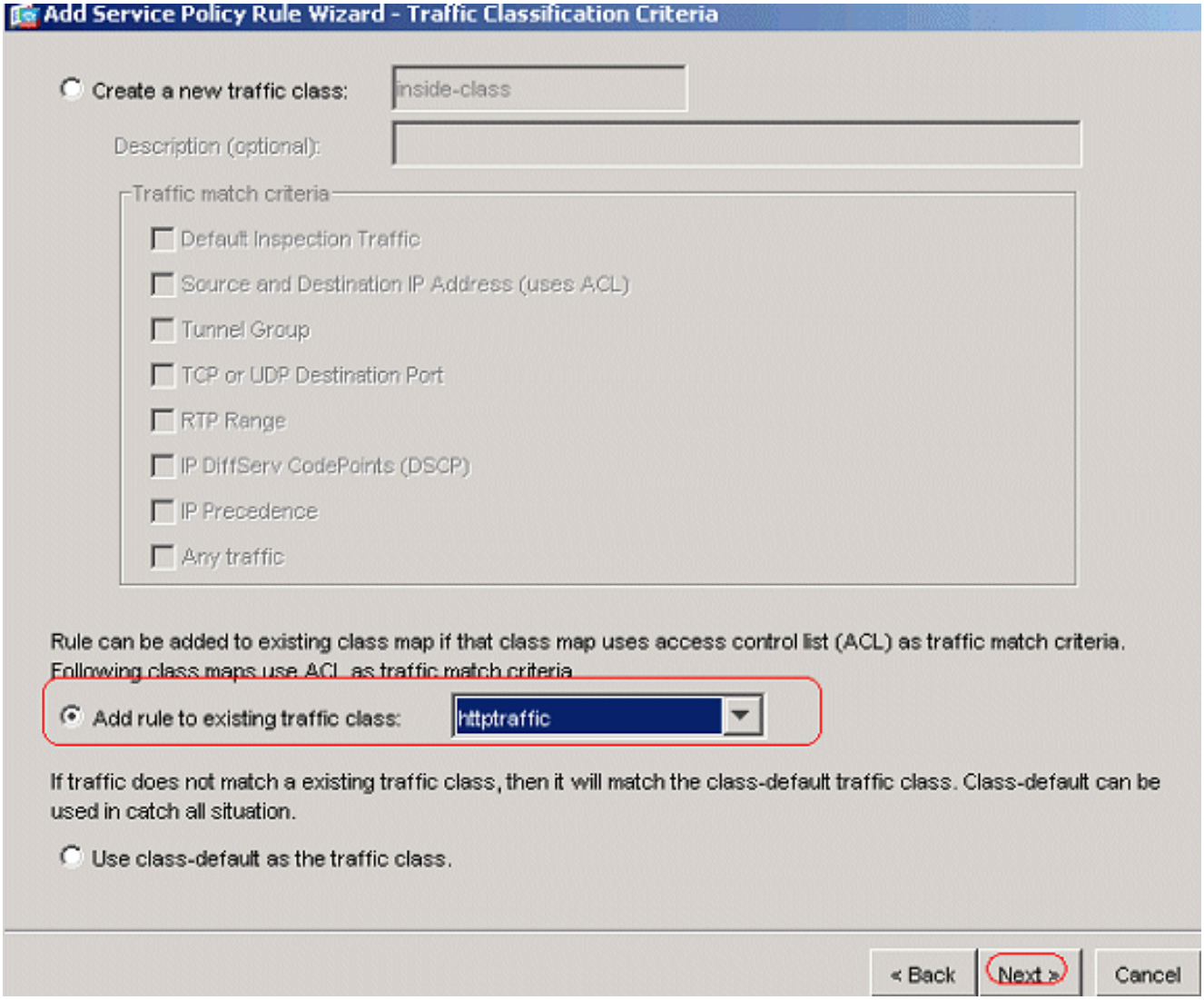
Datenverkehr über Port 8080 Klicken Sie erneut auf **Hinzufügen > Service Policy Rule (Servicebeschreibungsregel hinzufügen)**.



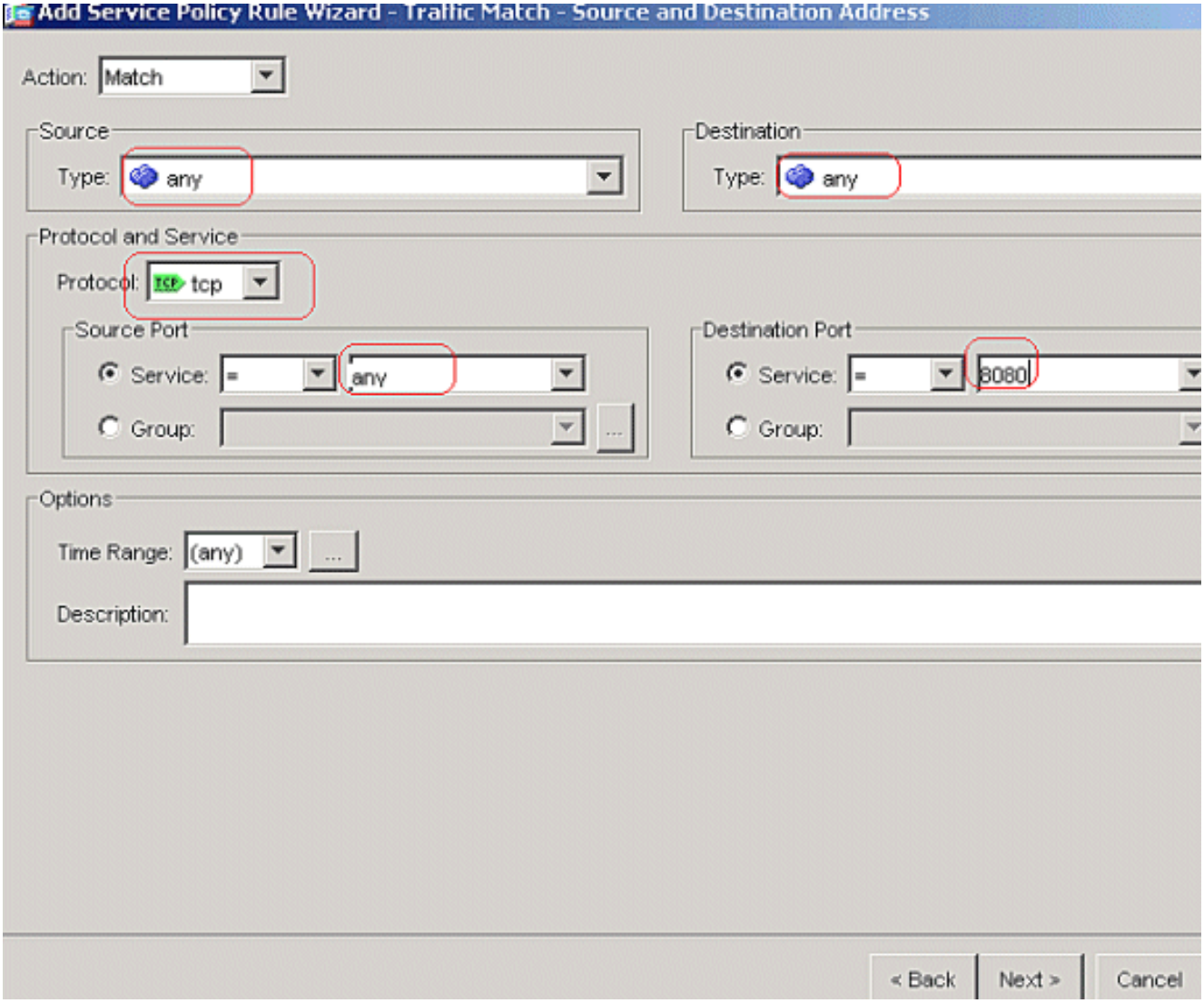
Klicken Sie auf **Weiter**.



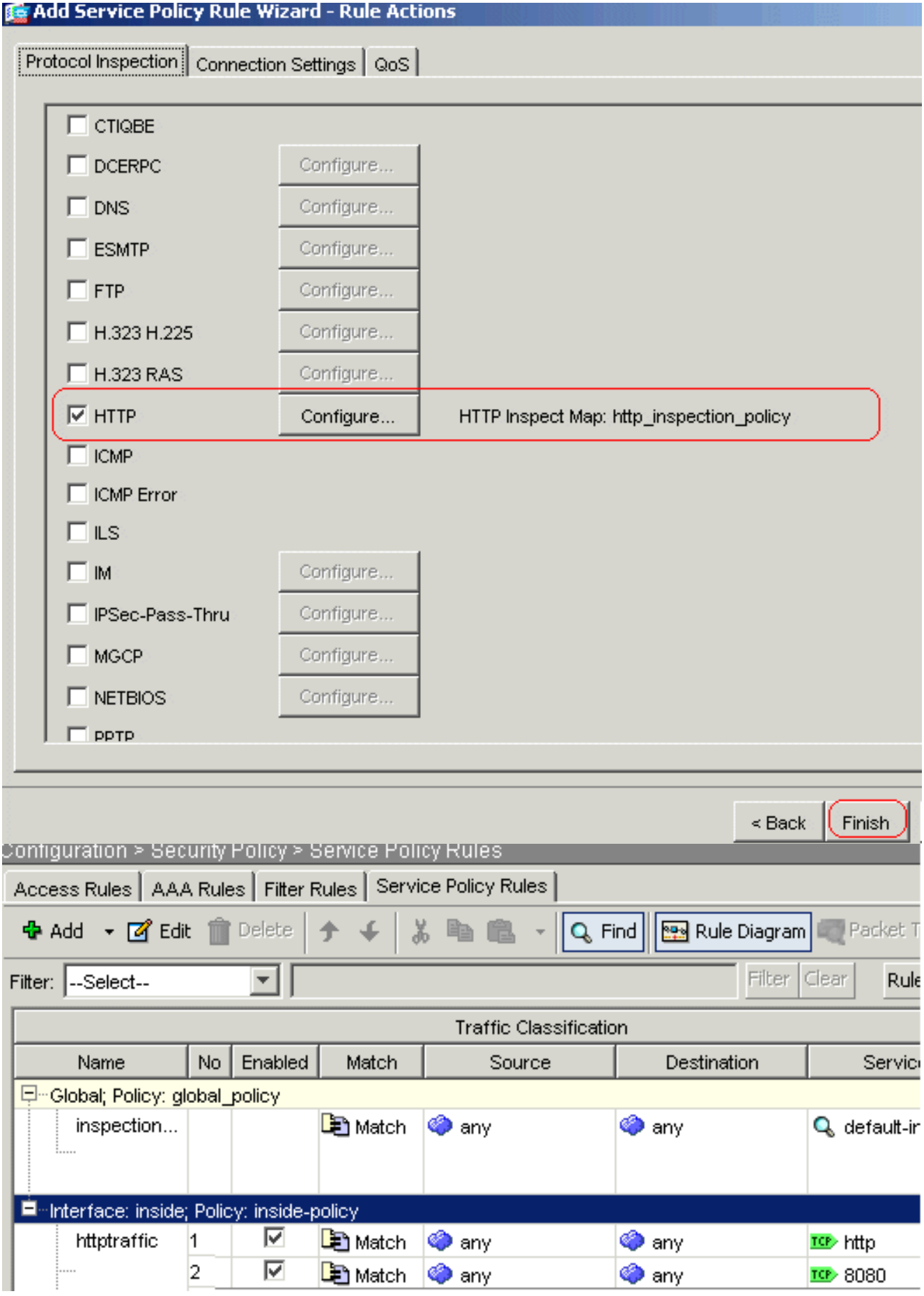
Wählen Sie das Optionsfeld **Regel zu vorhandener Datenverkehrsklasse hinzufügen**, und wählen Sie im Dropdown-Menü die Option **httptraffic** aus. Klicken Sie auf **Weiter**.



Wählen Sie die Quelle und das Ziel wie **alle** mit dem TCP-Port **8080 aus**. Klicken Sie auf **Weiter**.



Klicken Sie auf **Fertig stellen**.



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 Debugmeldungen für HTTP-Datenverkehr an.

Zugehörige Informationen

- Support-Seite für Cisco Adaptive Security Appliance
- Support-Seite für Cisco Adaptive Security Device Manager (ASDM)
- Support-Seite für Cisco PIX der Serie 500
- Technischer Support und Dokumentation - Cisco Systems