ASA/PIX 7.2: Bloccare determinati siti Web (URL) utilizzando espressioni regolari con esempi di configurazione MPF

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Security Appliance ASA/PIX 7.2 con espressioni regolari con Modular Policy Framework (MPF) per bloccare alcuni siti Web (URL).

Nota: questa configurazione non blocca tutti i download di applicazioni. Per i blocchi di file affidabili, è necessario usare un accessorio dedicato, ad esempio Websense, ecc., o un modulo, come il modulo CSC per l'appliance ASA.

Il filtro HTTPS non è supportato sull'appliance ASA. L'ASA non può eseguire l'ispezione o l'ispezione approfondita dei pacchetti in base all'espressione regolare per il traffico HTTPS perché, in HTTPS, il contenuto del pacchetto è crittografato (ssl).

Prerequisiti

Requisiti

in questo documento si presume che Cisco Security Appliance sia configurato e funzioni correttamente.

Componenti usati

- Cisco serie 5500 Adaptive Security Appliance (ASA) con software versione 7.2(2)
- Cisco Adaptive Security Device Manager (ASDM) versione 5.2(2) per ASA 7.2(2)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con i Cisco serie 500 PIX con software versione 7.2(2).

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Panoramica del framework di criteri modulari

MPF offre un modo coerente e flessibile per configurare le funzionalità delle appliance di sicurezza. Ad esempio, è possibile utilizzare MPF per creare una configurazione di timeout specifica per una particolare applicazione TCP, a differenza di una configurazione che si applica a tutte le applicazioni TCP.

MPF supporta le seguenti funzionalità:

- normalizzazione TCP, limiti e timeout delle connessioni TCP e UDP e randomizzazione dei numeri di sequenza TCP
- CSC
- Ispezione delle applicazioni
- IPS
- Policy di input QoS
- Policy di output QoS
- Coda priorità QoS

La configurazione dell'MPF prevede quattro attività:

1. Identificare il traffico di layer 3 e 4 a cui si desidera applicare le azioni. per ulteriori informazioni, fare riferimento a Identificazione del traffico con una mappa delle classi del layer 3/4.
2. (Solo ispezione delle applicazioni) Definire azioni speciali per il traffico di ispezione delle applicazioni. per ulteriori informazioni, fare riferimento a Configurazione delle azioni speciali

per le ispezioni delle applicazioni.
3. Applicare azioni al traffico di layer 3 e 4. per ulteriori informazioni, fare riferimento a Definizione delle azioni mediante una mappa dei criteri di layer 3/4.
4. Attivare le azioni su un'interfaccia. Per ulteriori informazioni, fare riferimento a Applicazione di un criterio di layer 3/4 a un'interfaccia tramite un criterio di servizio.

Espressione regolare

Un'espressione regolare corrisponde alle stringhe di testo letteralmente come una stringa esatta o con metacaratteri, pertanto è possibile trovare più varianti di una stringa di testo. È possibile utilizzare un'espressione regolare per far corrispondere il contenuto di un determinato traffico dell'applicazione; ad esempio, è possibile trovare una stringa URL all'interno di un pacchetto HTTP.

Nota: utilizzare **Ctrl+V** per eseguire l'escape di tutti i caratteri speciali nella CLI, ad esempio un punto interrogativo (?) o una tabulazione. Ad esempio, digitare **d[Ctrl+V]g** per immettere **d?g** nella configurazione.

Per creare un'espressione regolare, utilizzare il comando **regex**, che può essere utilizzato per varie caratteristiche che richiedono la corrispondenza del testo. Ad esempio, è possibile configurare azioni speciali per l'ispezione delle applicazioni con Modular Policy Framework con una mappa dei criteri di ispezione (vedere il comando type inspect della mappa dei criteri). Nella mappa dei criteri di ispezione è possibile identificare il traffico su cui si desidera intervenire se si crea una mappa della classe di ispezione contenente uno o più comandi di **corrispondenza** oppure è possibile utilizzare i comandi di **corrispondenza** direttamente nella mappa dei criteri di ispezione. Alcuni comandi di **corrispondenza** consentono di identificare il testo in un pacchetto con un'espressione regolare; ad esempio, è possibile trovare le stringhe URL all'interno dei pacchetti HTTP. È possibile raggruppare le espressioni regolari in una mappa di classe delle espressioni regolari (vedere il comando class-map type regex).

La Tabella 1 elenca i metacaratteri con significati speciali.

Carattere	Descrizione	Note
.	Punto	Corrisponde a qualsiasi carattere singolo. Ad esempio, **d.g** corrisponde a dog, dag, dtg e a qualsiasi parola che contenga tali caratteri, ad esempio doggonnit.
(espr)	Sottoespressione	Una sottoespressione separa i caratteri dai caratteri circostanti, in modo che sia possibile utilizzare altri metacaratteri nella sottoespressione. Ad esempio, **d(o|a)g** corrisponde a cane e cane, mentre **do|ag** corrisponde a do e ag. Una sottoespressione può essere utilizzata anche con i quantificatori di ripetizione per differenziare i caratteri destinati alla ripetizione. Ad esempio, **ab(xy){3}z** corrisponde ad abxyxyxyxyz.

|	Alternanza	Corrisponde all'espressione che separa. Ad esempio, **cane|gatto** corrisponde a cane o gatto.
?	Punto interrogativo	Quantificatore che indica che l'espressione precedente contiene 0 o 1. Ad esempio, **lo?se** corrisponde a lse o lose. **Nota: è** necessario immettere **Ctrl+V**, quindi il punto interrogativo, altrimenti viene richiamata la funzione della guida.
*	Asterisco	Un quantificatore che indica che l'espressione precedente contiene 0, 1 o qualsiasi numero. Ad esempio, **lo*se** corrisponde a lse, lose, loose e così via.
{x}	Ripeti quantificatore	Ripetere esattamente x volte. Ad esempio, **ab(xy){3}z** corrisponde ad abxyxyxyxyz.
{x}	Quantificatore a ripetizione minimo	Ripetere almeno x volte. Ad esempio, **ab(xy){2,}z** corrisponde ad abxyxyz, abxyxyxyxyz e così via.
[abc]	Classe Character	Corrisponde a qualsiasi carattere tra parentesi. Ad esempio, **[abc]** corrisponde a, b o c.
[^abc]	Classe di caratteri negata	Corrisponde a un singolo carattere non contenuto tra parentesi. Ad esempio, **[^abc]** corrisponde a qualsiasi carattere diverso da a, b o c. **[^A-Z]** corrisponde a qualsiasi carattere singolo diverso da una lettera maiuscola.
[a-c]	Classe intervallo caratteri	Trova tutti i caratteri compresi nell'intervallo. **[a-z]** corrisponde a qualsiasi lettera minuscola. È possibile combinare caratteri e intervalli: **[abcq-z]** corrisponde a, b, c, q, r, s, t, u, v, w, x, y, z e così **[a-cq-z]**. Il carattere trattino (-) è letterale solo se è l'ultimo o il primo carattere tra parentesi: **[abc-]** o **[-abc]**.
""	Virgolette	Mantiene gli spazi finali o iniziali nella stringa. Ad esempio, **" test"** mantiene lo spazio iniziale quando cerca una corrispondenza.
^	Accento circonflesso	Specifica l'inizio di una riga.
\	Carattere di escape	Se utilizzato con un metacarattere, corrisponde a un carattere letterale. Ad esempio, **\[** corrisponde alla parentesi quadra sinistra.

carattere	Carattere	Quando un carattere non è un metacarattere, corrisponde al carattere letterale.
\r	Ritorno a capo	Corrisponde a un ritorno a capo 0x0d.
\n	Nuova riga	Corrisponde a una nuova riga 0x0a.
\t	Tabulazione	Trova/sostituisce una tabulazione 0x09.
\f	Alimentazione	Corrisponde a un feed di moduli 0x0c.
\xNN	Numero esadecimale con escape	Trova/sostituisce un carattere ASCII con un carattere esadecimale (esattamente due cifre).
\NNN	Numero ottale scappato	Corrisponde a un carattere ASCII come ottale (esattamente tre cifre). Ad esempio, il carattere 040 rappresenta uno spazio.

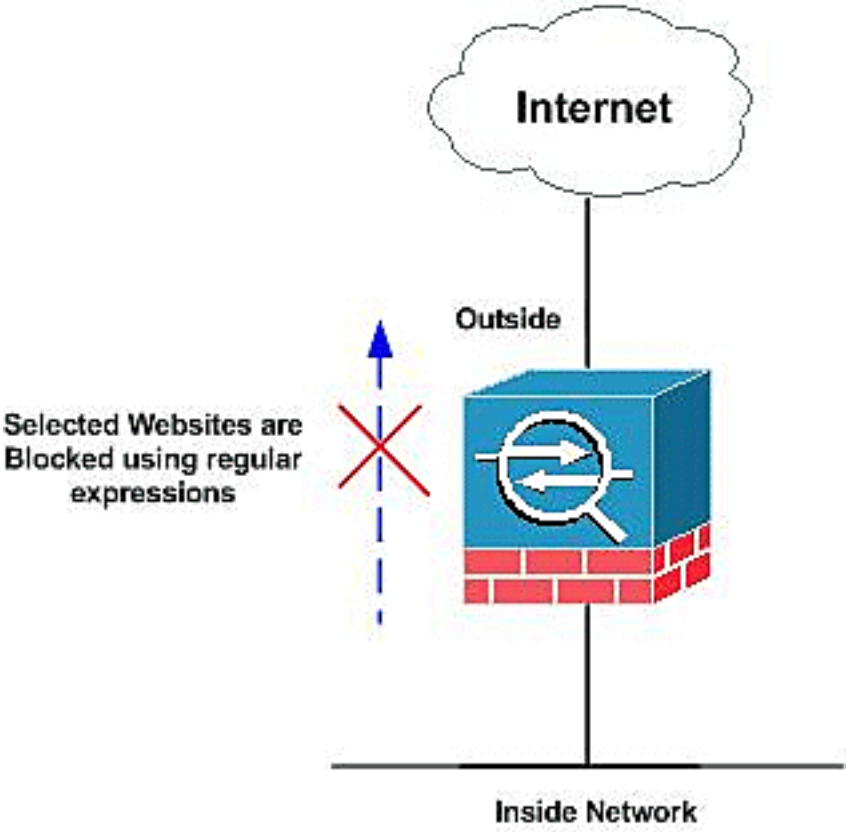
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- Configurazione ASA CLI
- Configurazione ASA 7.2(x) con ASDM 5.2

Configurazione ASA CLI

Configurazione ASA CLI

```
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
```

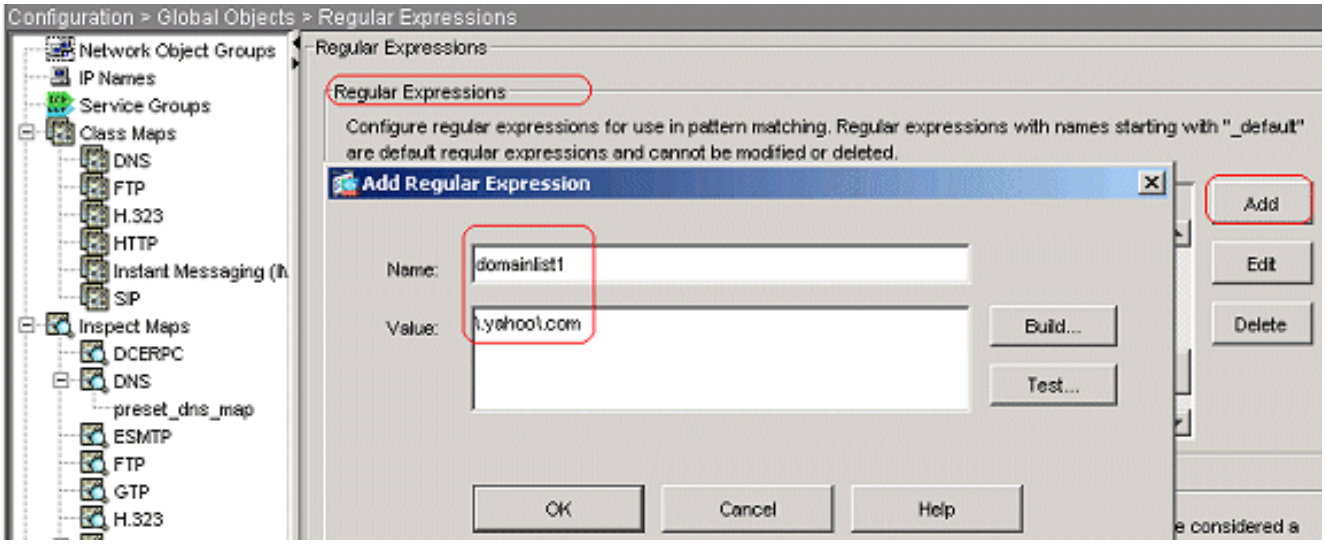
```
asdm history enable arp timeout 14400 route DMZ 0.0.0.0
0.0.0.0 10.77.241.129 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00
sip_media 0:02:00 sip-invite 0:03:00 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#
```

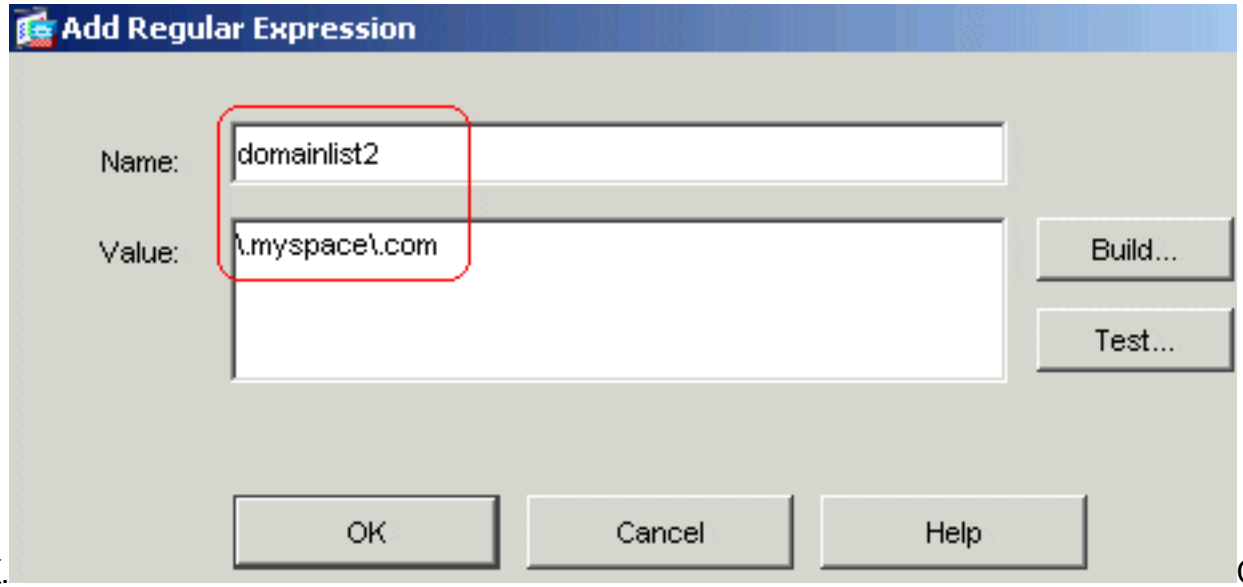
Configurazione ASA 7.2(x) con ASDM 5.2

Completare questi passaggi per configurare le espressioni regolari e applicarle a MPF per bloccare i siti Web specifici:

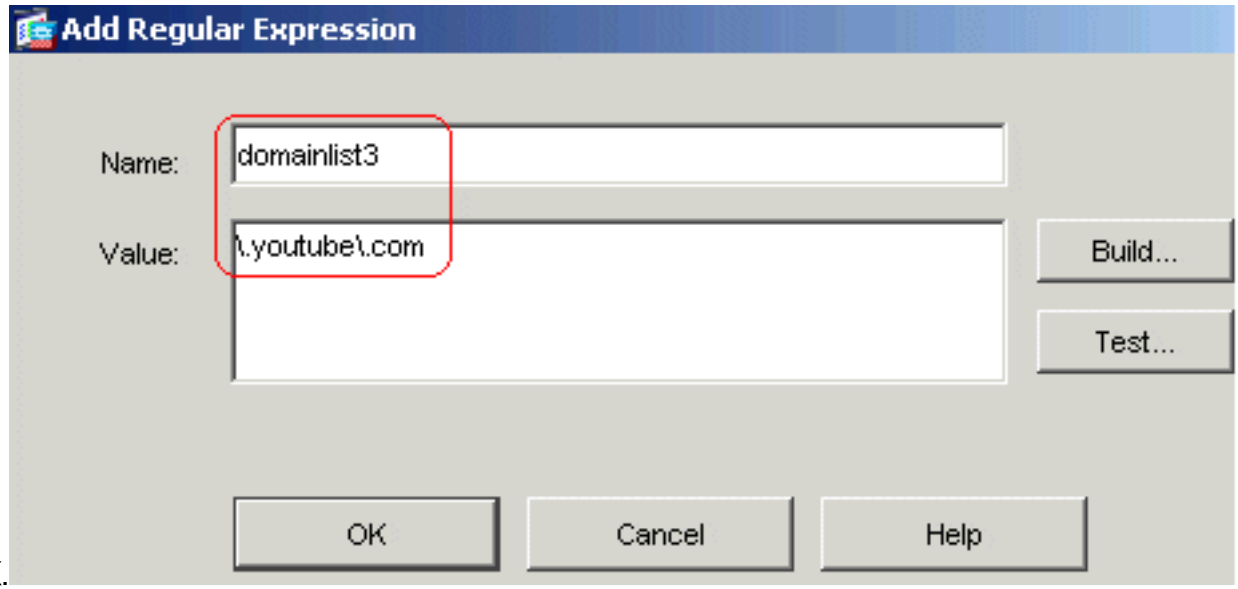
1. **Crea espressioni regolari**Per creare espressioni regolari, scegliete **Configurazione > Oggetti globali > Espressioni regolari** e fate clic su **Aggiungi** nella scheda Espressione regolare.Creare un'espressione regolare **domainlist1** per acquisire il nome di dominio **yahoo.com**. Fare clic su
OK.



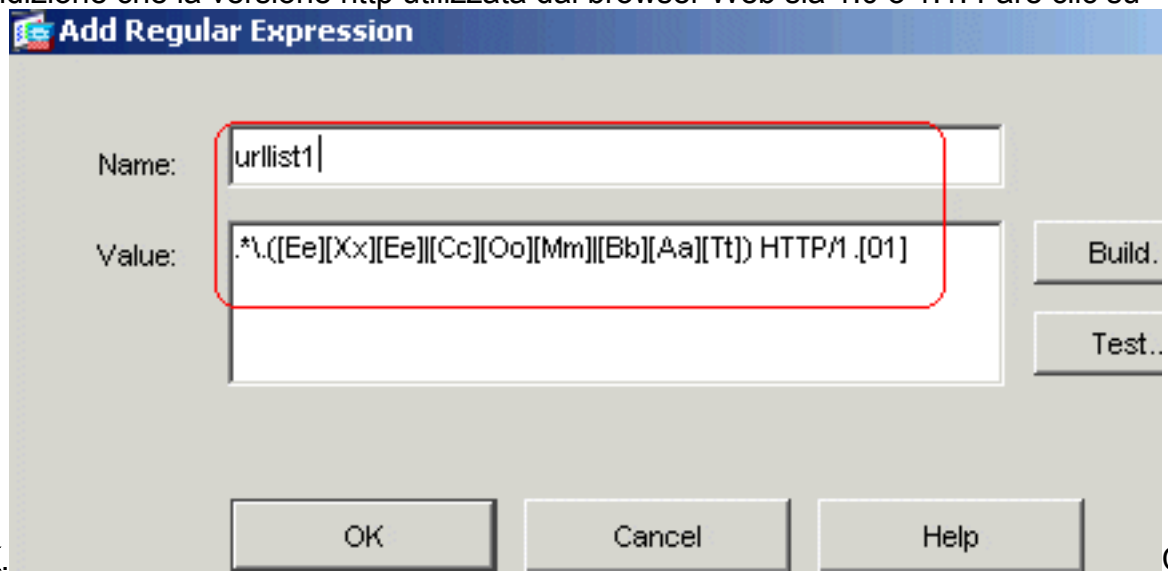
Creare un'espressione regolare **domainlist2** per acquisire il nome di dominio **myspace.com**. Fare clic su



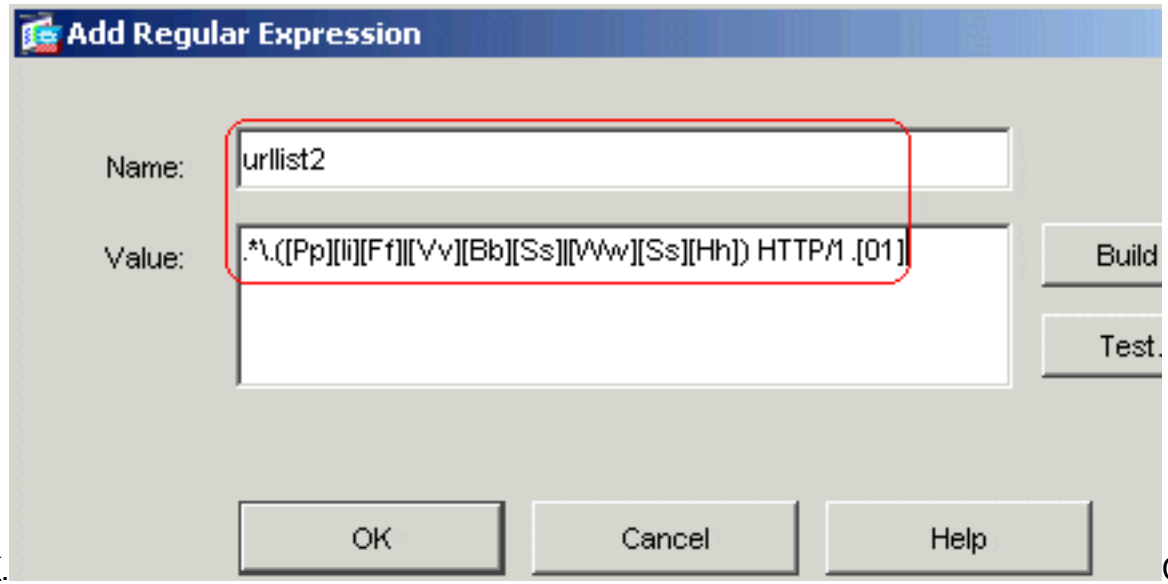
OK. Creare un'espressione regolare **domainlist3** per acquisire il nome di dominio **youtube.com**. Fare clic su



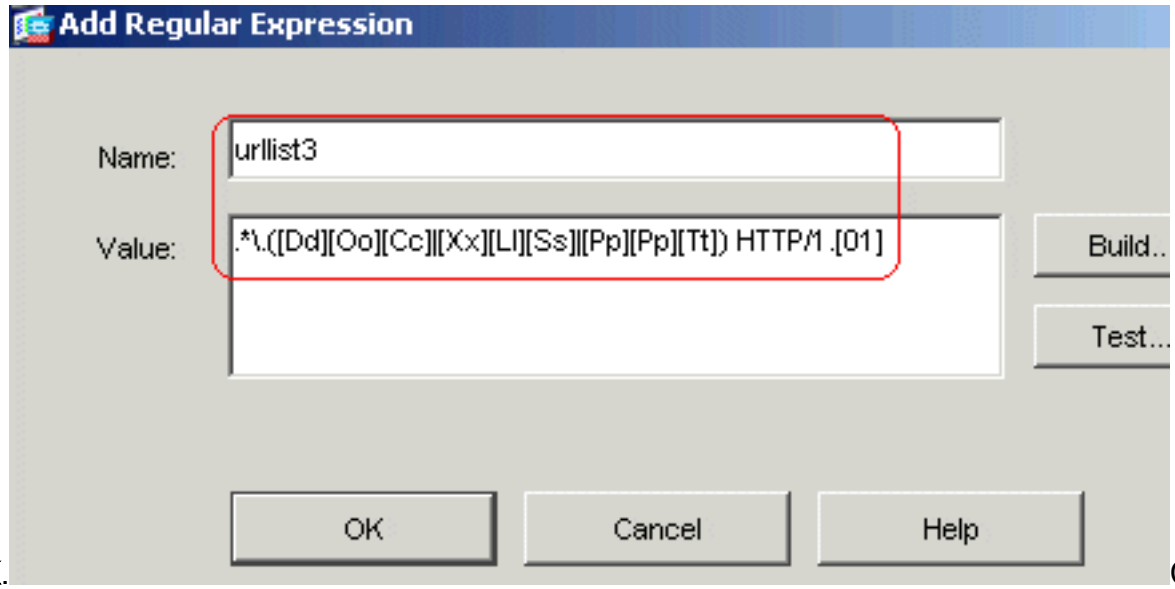
OK. Creare un'espressione regolare urllist1 per acquisire le estensioni di file **exe**, **com** e **bat** a condizione che la versione http utilizzata dal browser Web sia 1.0 o 1.1. Fare clic su



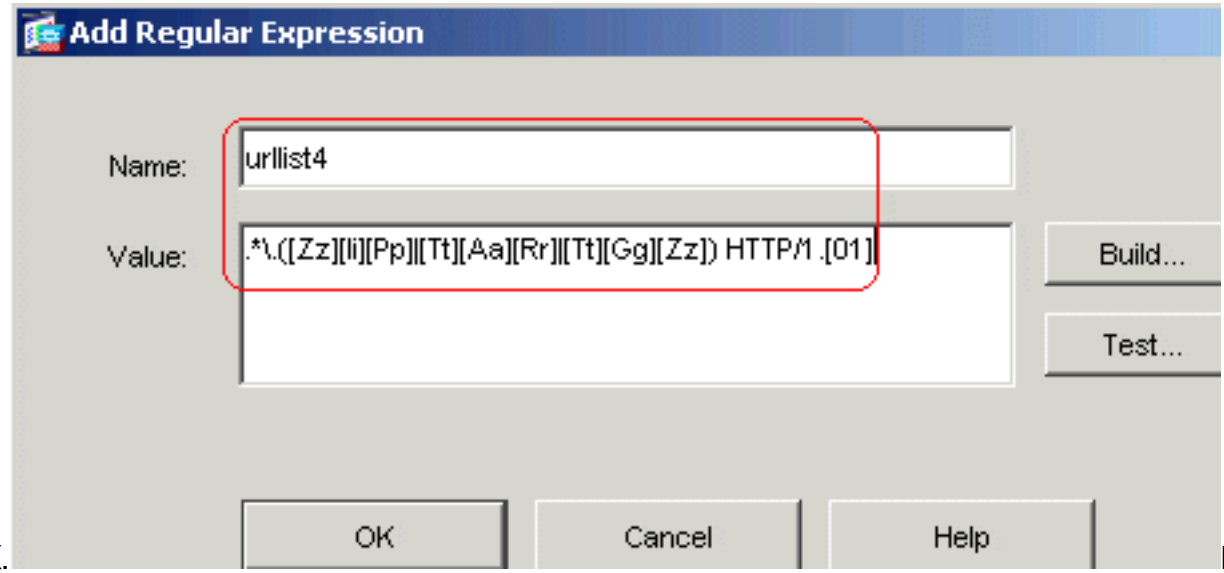
OK. Creare un'espressione regolare urllist2 per acquisire le estensioni di file, ad esempio **pif**, **vbs** e **wsh** a condizione che la versione HTTP utilizzata dal browser Web sia 1.0 o 1.1. Fare clic su



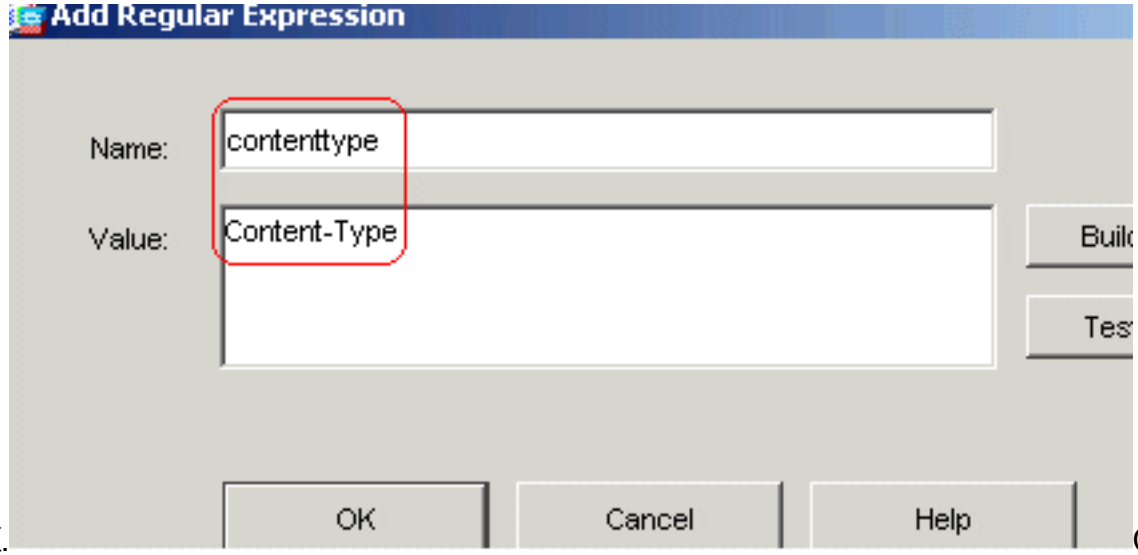
OK. Creare un'espressione regolare urllist3 per acquisire le estensioni di file, ad esempio **doc**, **xls** e **ppt** a condizione che la versione HTTP utilizzata dal browser Web sia 1.0 o 1.1. Fare clic su



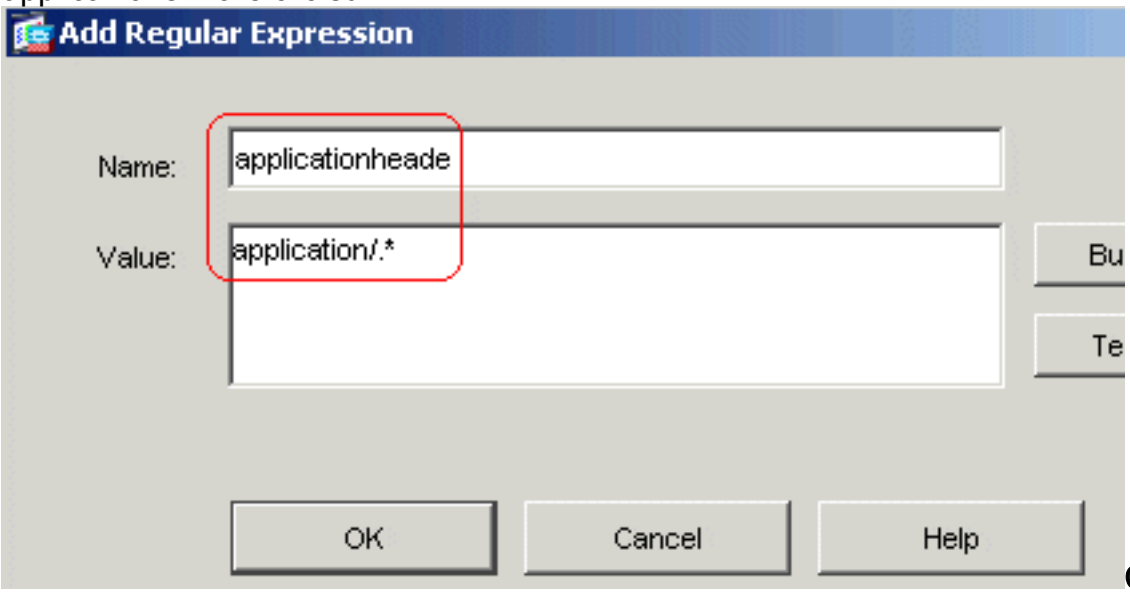
OK. Creare un'espressione regolare urllist4 per acquisire le estensioni di file, ad esempio **zip**, **tar** e **tgz** a condizione che la versione HTTP utilizzata dal browser Web sia 1.0 o 1.1. Fare clic su



OK. Per acquisire un **tipo di contenuto,** creare un'espressione regolare contenttype. Fare clic su



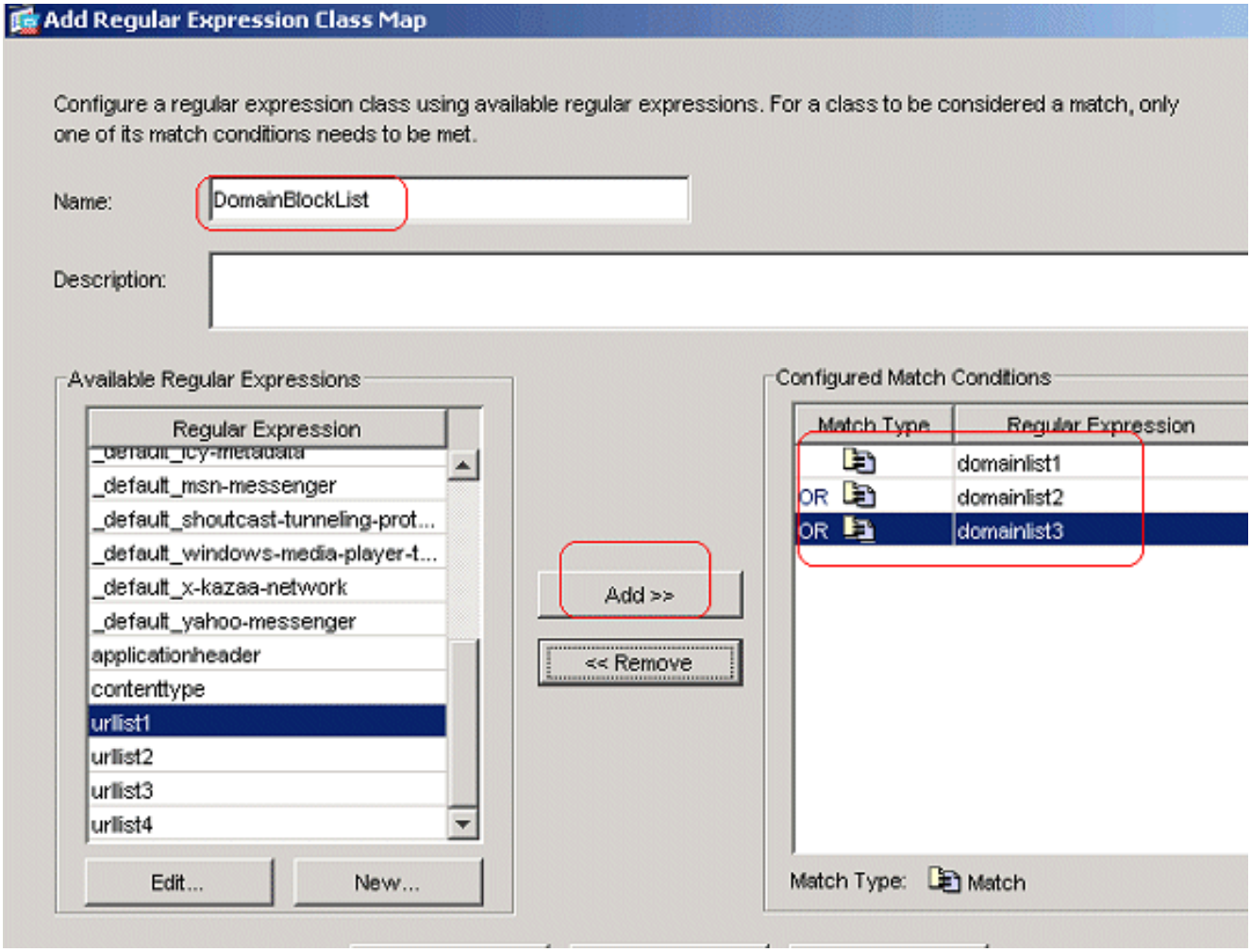
OK. Creare un'espressione regolare **applicationheader** per acquisire le varie intestazioni dell'applicazione. Fare clic su



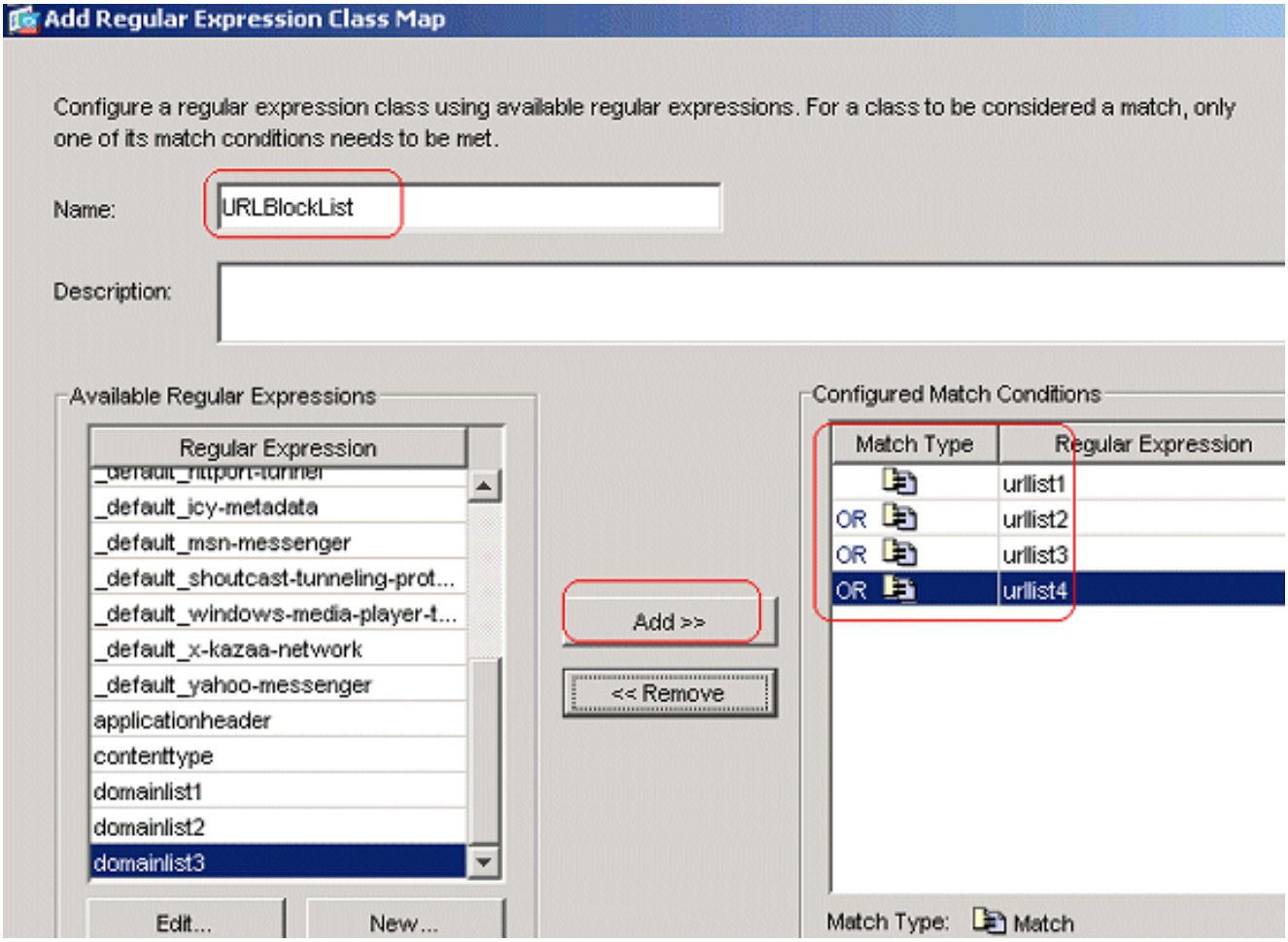
OK.

Configurazione CLI equivalente

2. **Crea classi di espressioni regolari**Per creare le varie classi, scegliere **Configurazione > Oggetti globali > Espressioni regolari**, quindi fare clic su **Aggiungi** nella scheda **Classi di espressioni regolari**.Creare una classe di espressioni regolari **DomainBlockList** in modo che corrisponda a una qualsiasi delle espressioni regolari: domainlist1, domainlist2 e domainlist3. Fare clic su
OK.

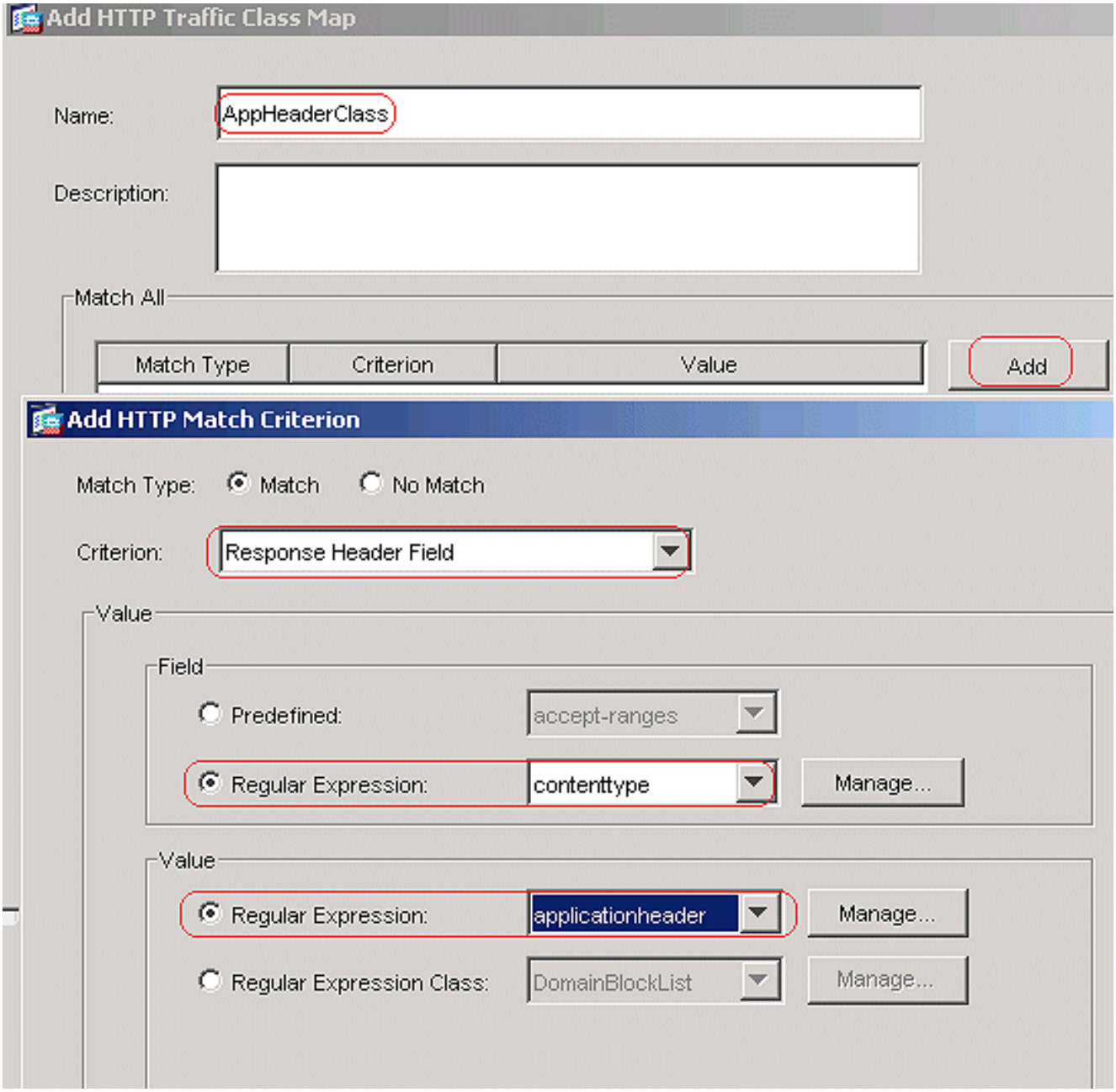


Creare una classe di espressioni regolari **URLBlockList** in modo che corrisponda a una qualsiasi delle espressioni regolari: urllist1, urllist2, urllist3 e urllist4. Fare clic su **OK**.

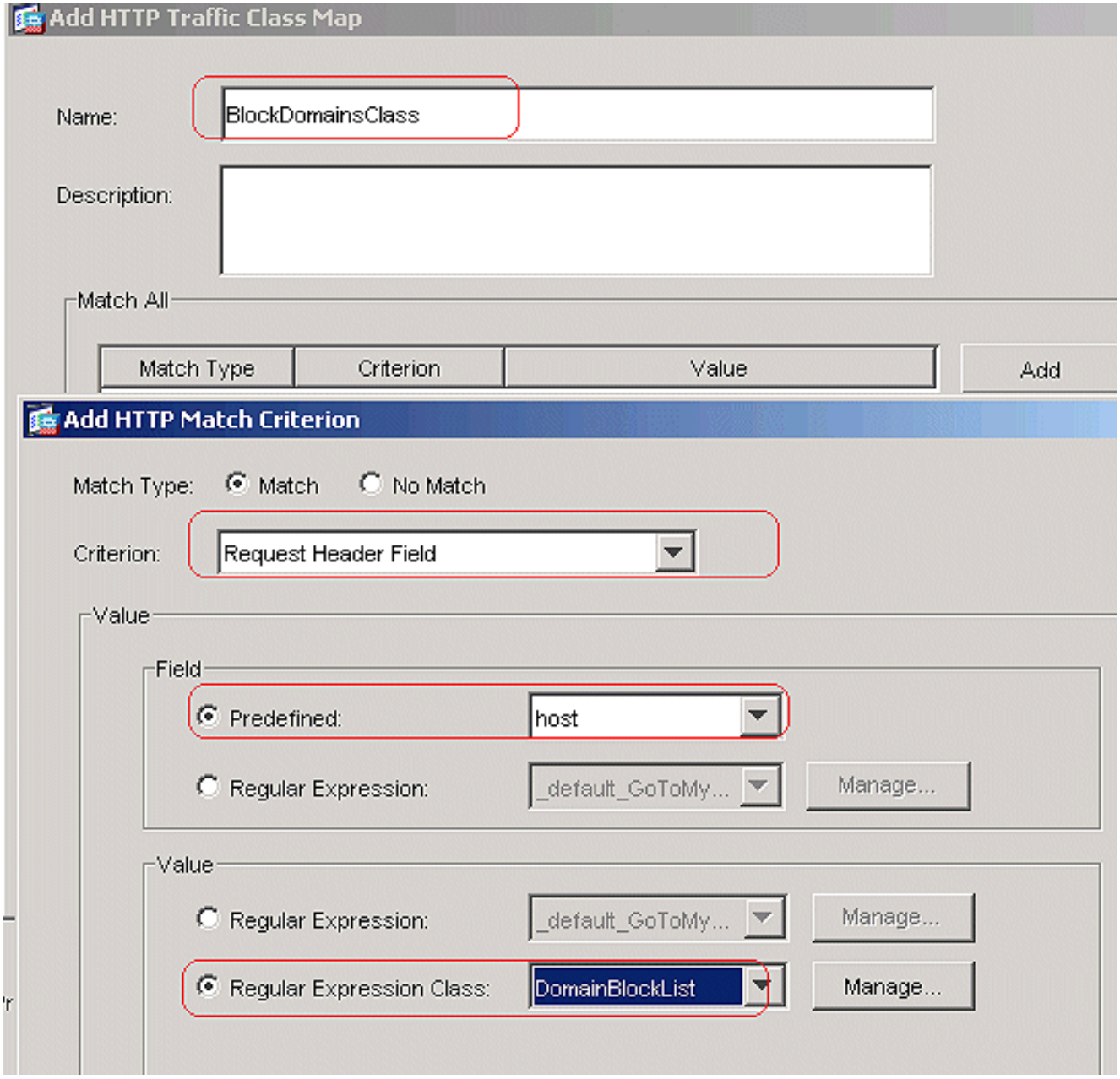


Configurazione CLI equivalente

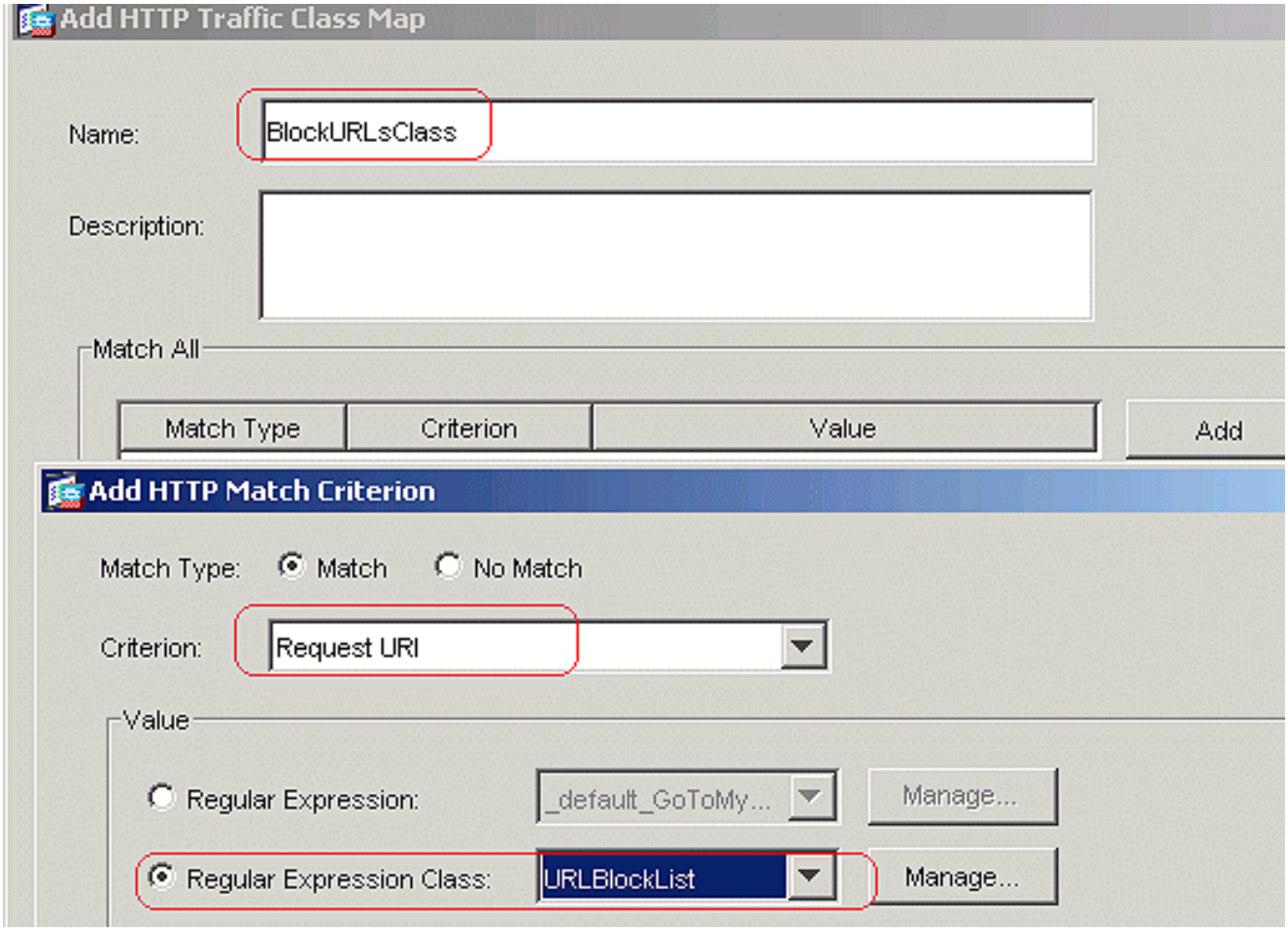
3. **Ispezionare il traffico identificato con le mappe classi**Scegliere **Configurazione > Oggetti globali > Mappe classi > HTTP > Aggiungi** per creare una mappa di classe per ispezionare il traffico HTTP identificato da varie espressioni regolari.Creare una mappa di classe **AppHeaderClass** in modo che corrisponda all'intestazione della risposta con acquisizioni di espressioni
regolari.



Fare clic su **OK**.Creare una mappa di classe **BlockDomainsClass** in modo che corrisponda all'intestazione della richiesta con acquisizioni di espressioni regolari.

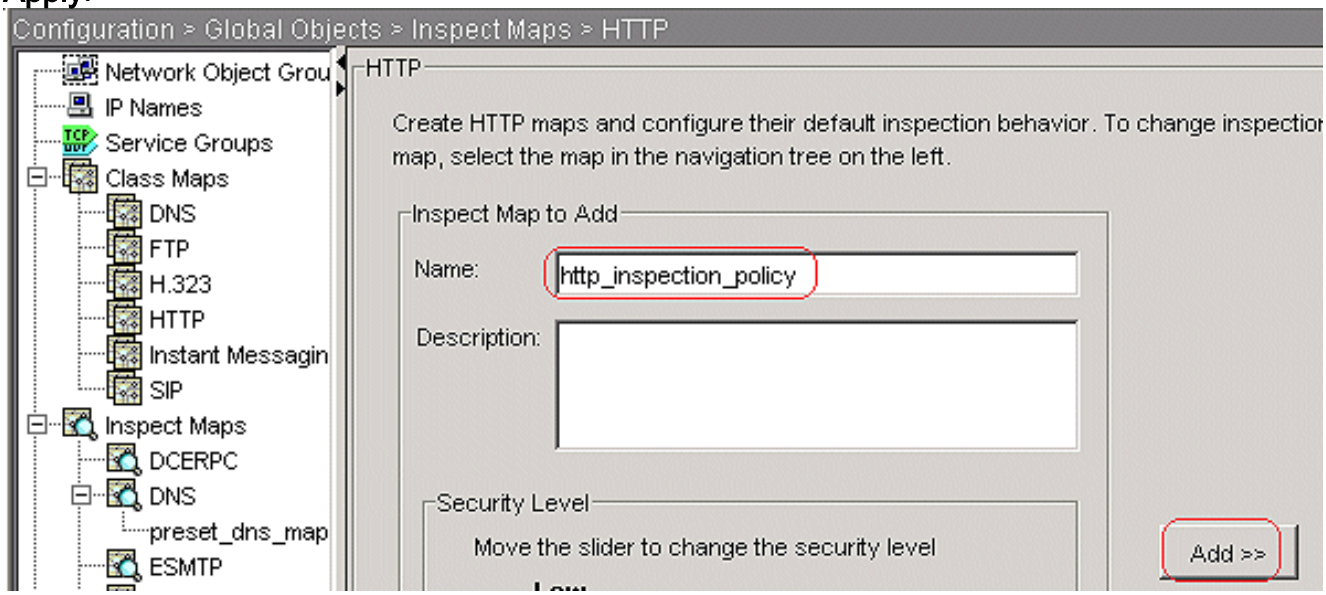


Fare clic su **OK**.Creare una mappa di classe **BlockURLsClass** in modo che corrisponda all'URI della richiesta con acquisizioni di espressioni regolari.

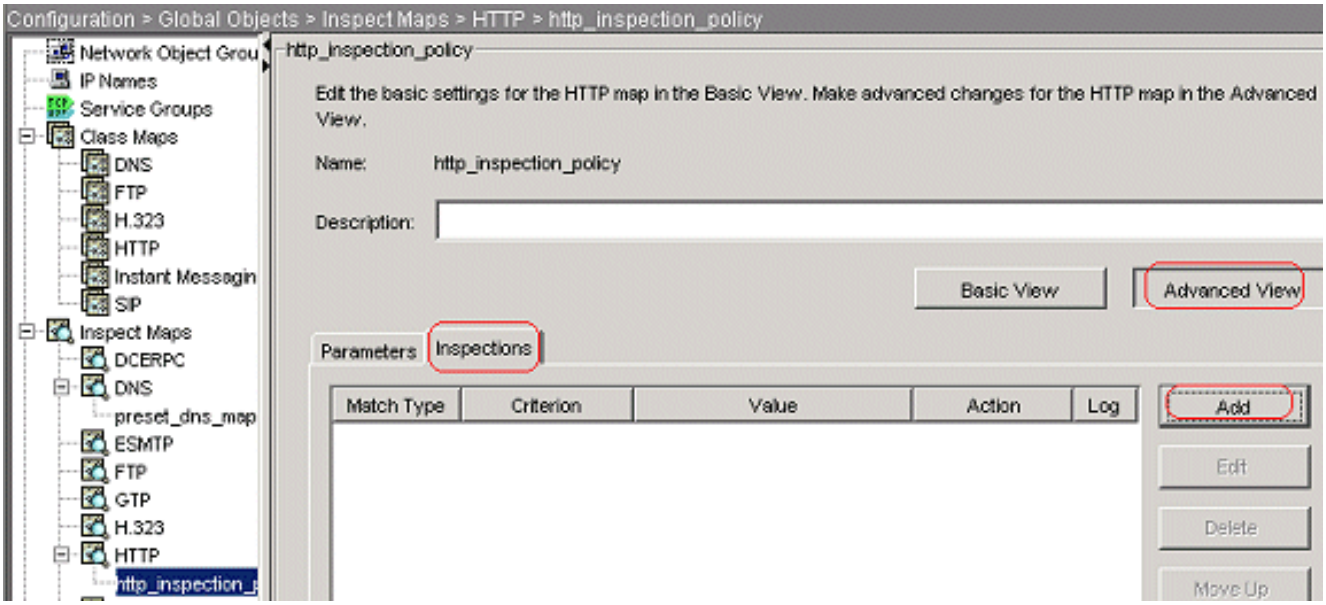


Fare clic su **OK**.**Configurazione CLI equivalente**

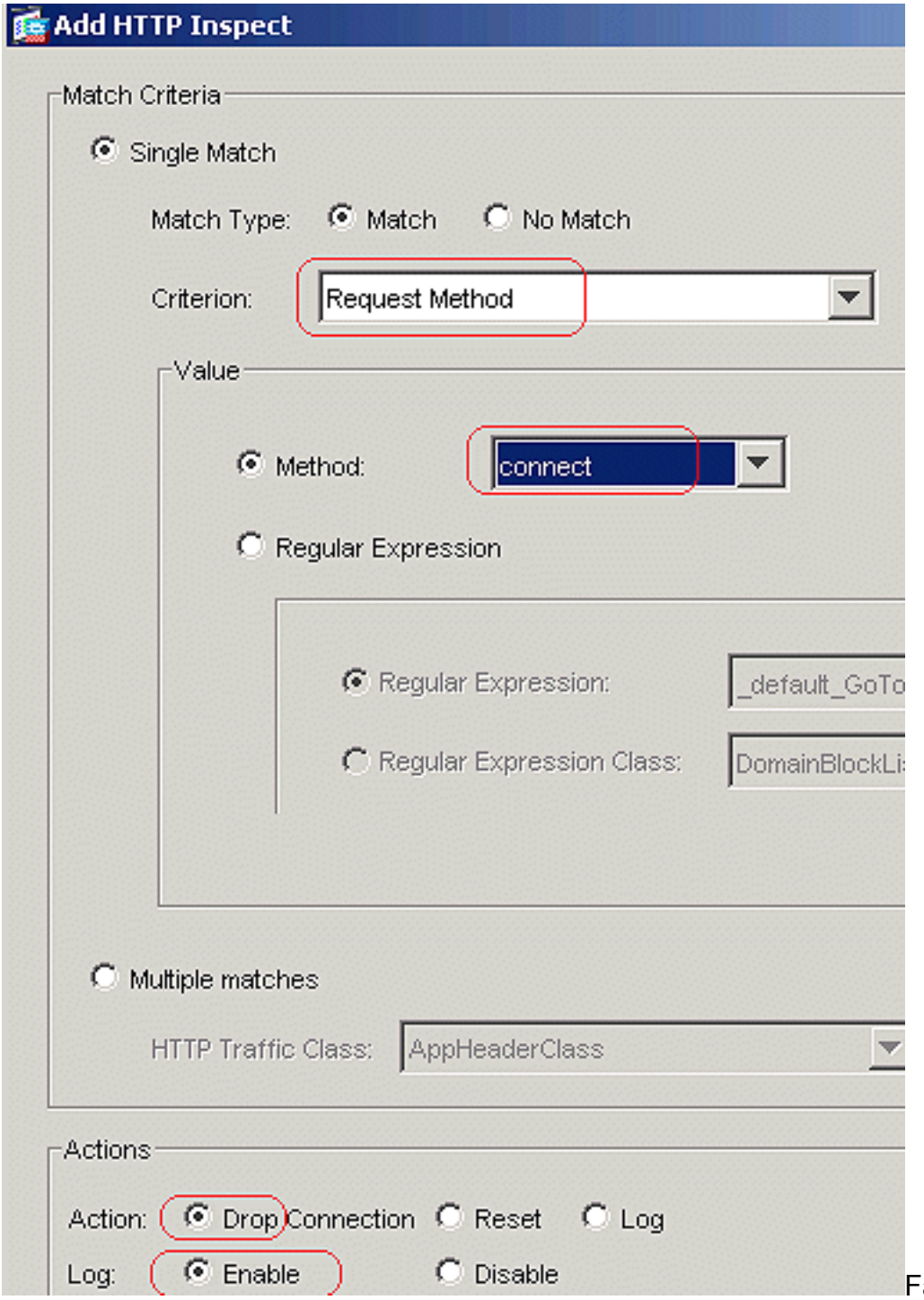
4. **Impostare le azioni per il traffico corrispondente nei criteri di ispezione**Per creare un **http_inspection_policy** per impostare l'azione per il traffico corrispondente, scegliere **Configurazione > Oggetti globali > Ispeziona mappe > HTTP**. Fare clic su **Add** and **Apply**.



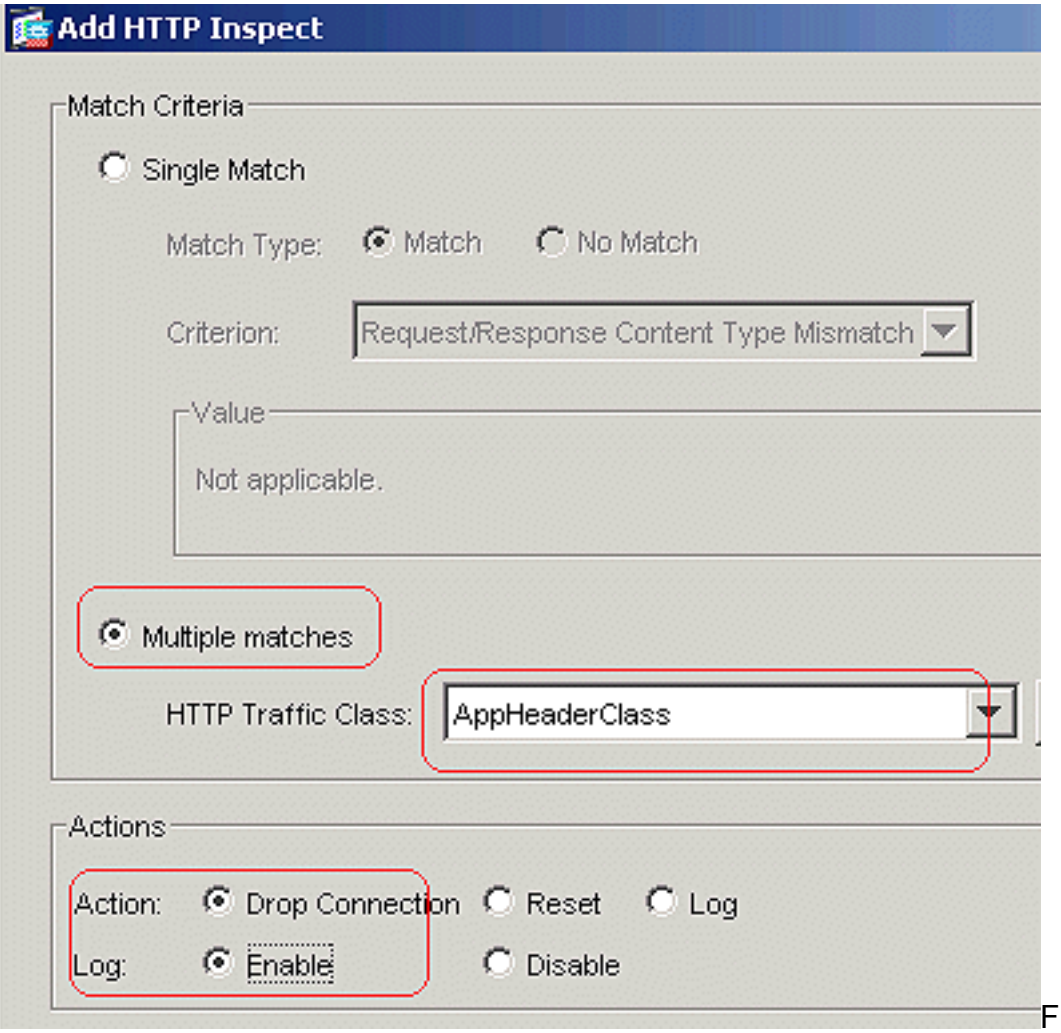
Scegliere **Configurazione > Oggetti globali > Ispezione mappe > HTTP > http_survey_policy** e fare clic su **Visualizzazione avanzata > Ispezioni > Aggiungi** per impostare le azioni per le varie classi create
finora.



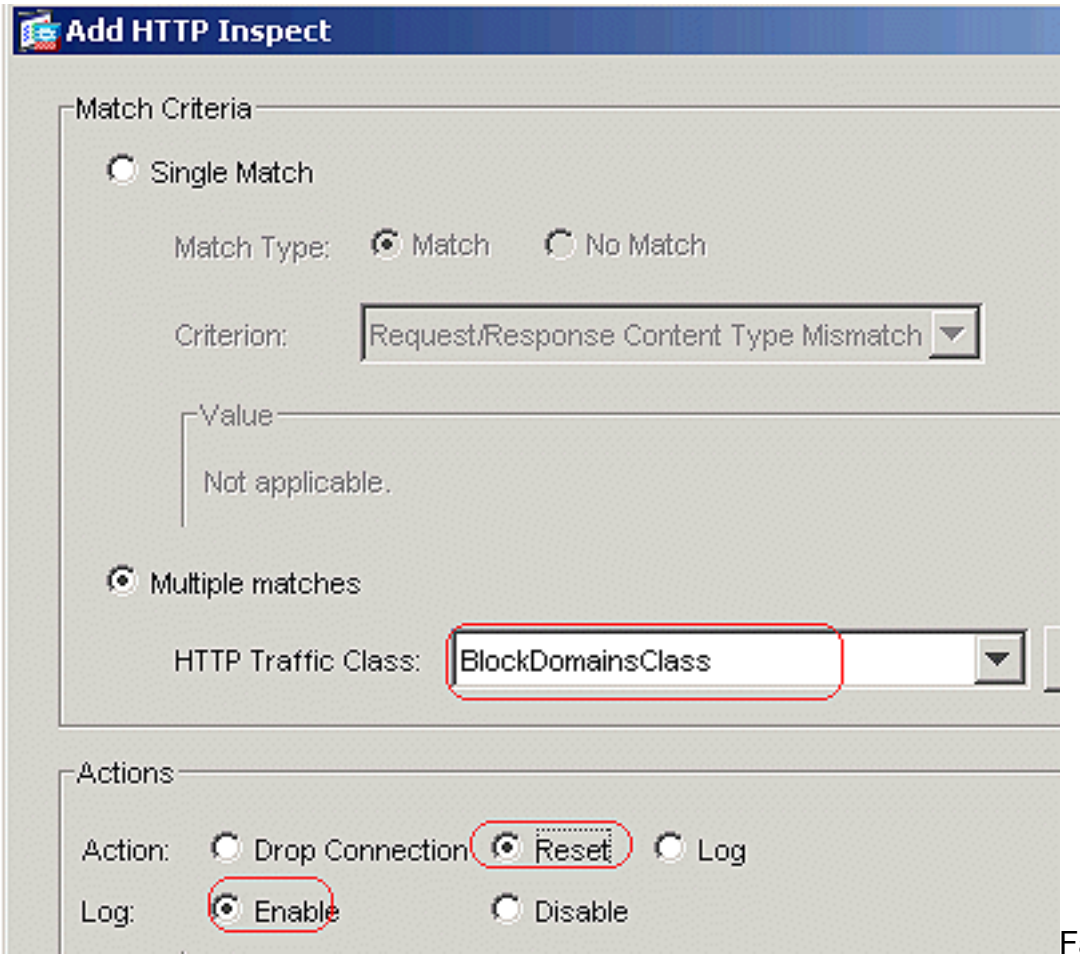
Fare clic su **OK**.Impostare l'azione come **Elimina connessione**; **Abilitare** la registrazione per il criterio come metodo di richiesta e il valore come



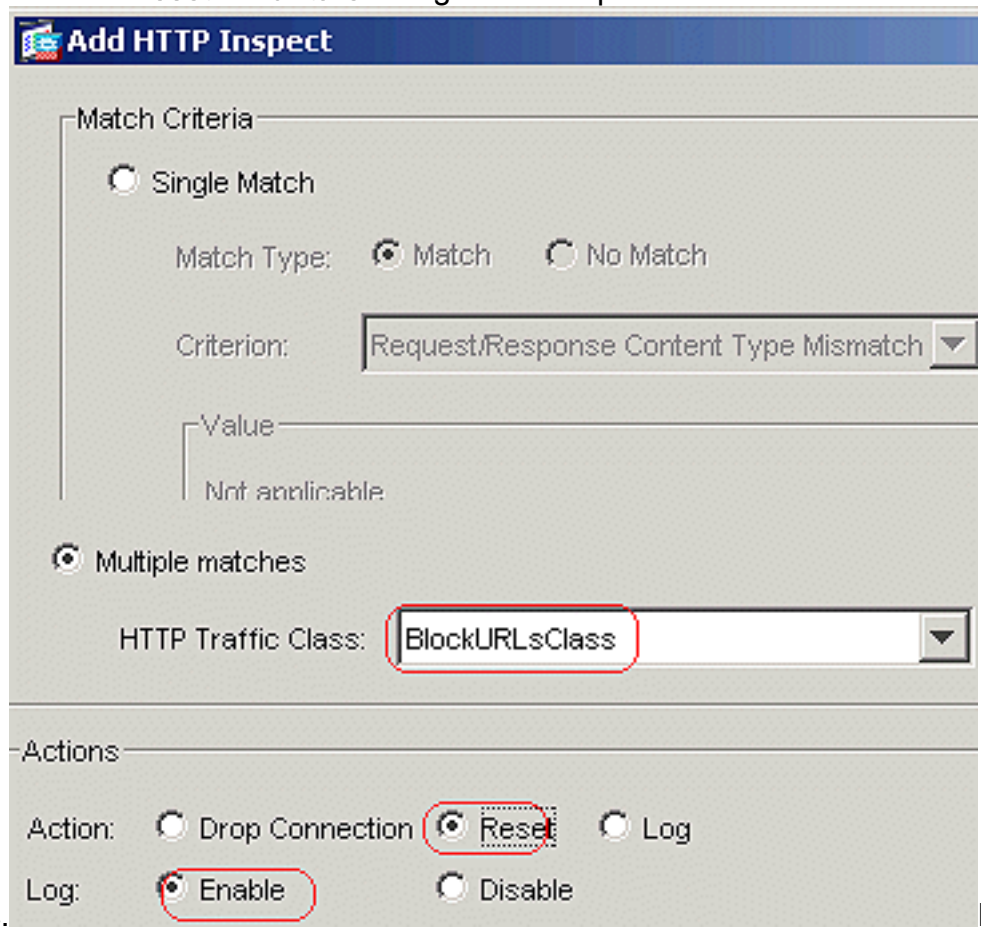
connessione. Fare clic su **OK**.Impostare l'azione come **Elimina connessione** e **Abilitare** la registrazione per la classe



AppHeaderClass.F are clic su **OK**.Impostare l'azione come **Reset** e **Abilitare** la registrazione per la classe **BlockDomainsClass**.



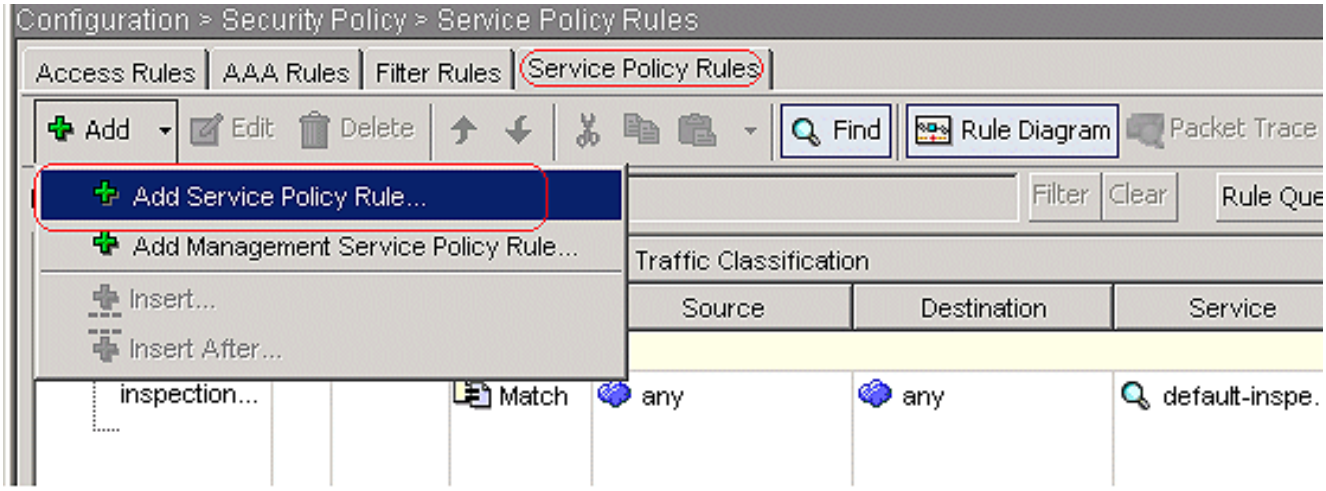
Fare clic su **OK**.Impostare l'azione su **Reset** e **Abilitare** la registrazione per la classe



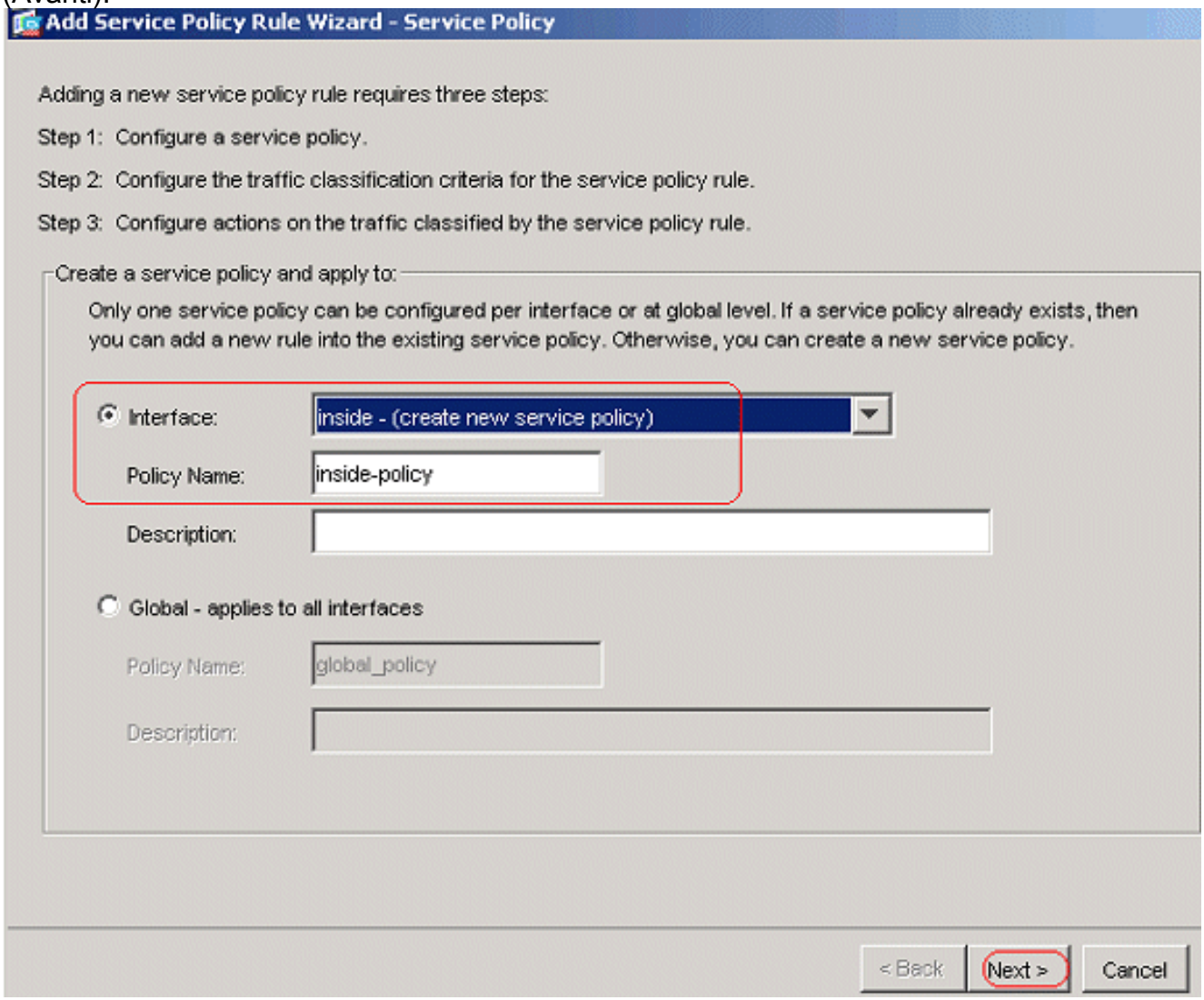
BlockURLsClass. Fare clic su **OK**.Fare clic su **Apply** (Applica).**Configurazione CLI equivalente**

5. **Applica il criterio http di ispezione all'interfaccia**Scegliere **Configurazione > Criteri di sicurezza > Regole dei criteri di servizio > Aggiungi > Aggiungi regola dei criteri di servizio**

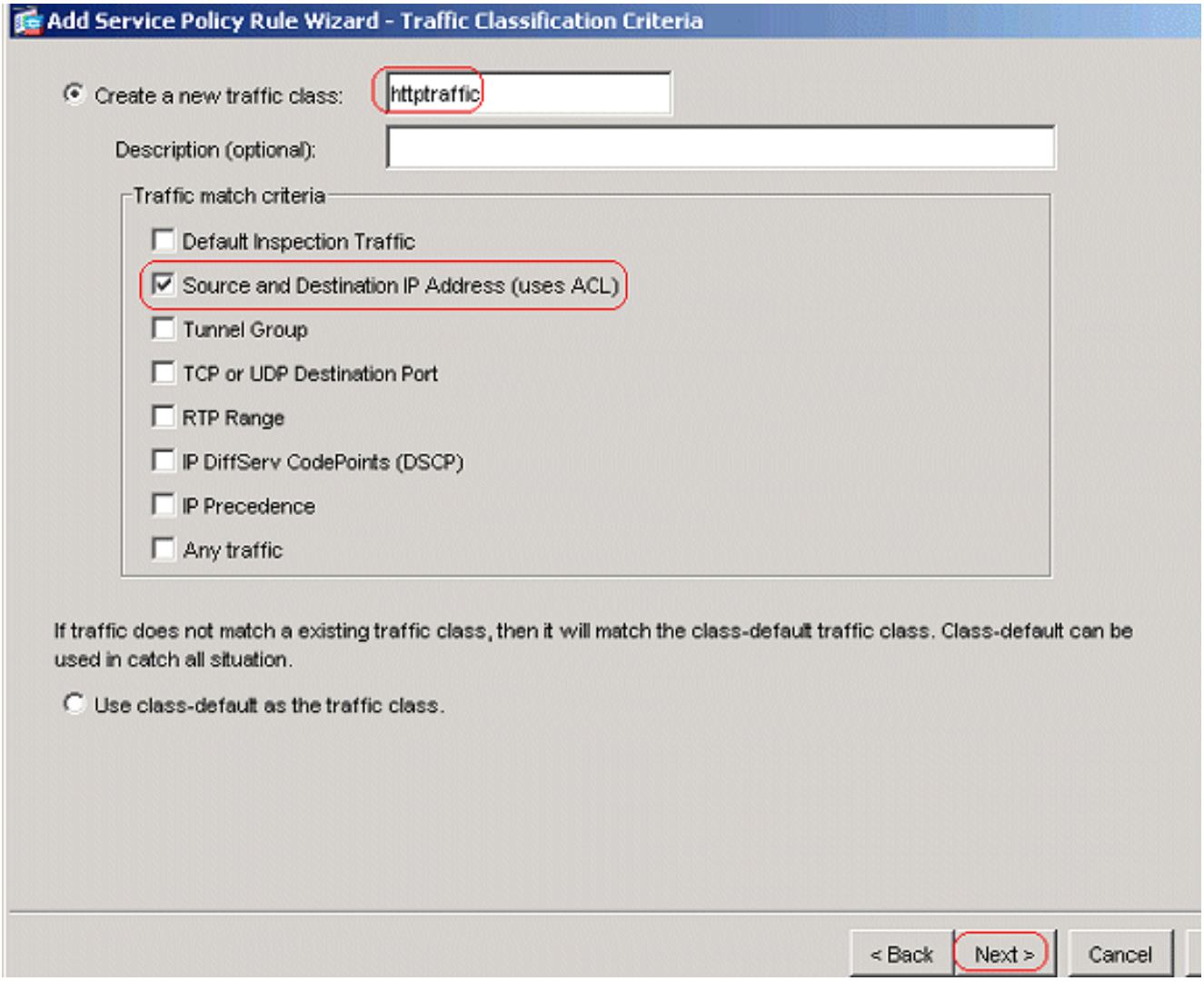
nella scheda Regole dei criteri di servizio.



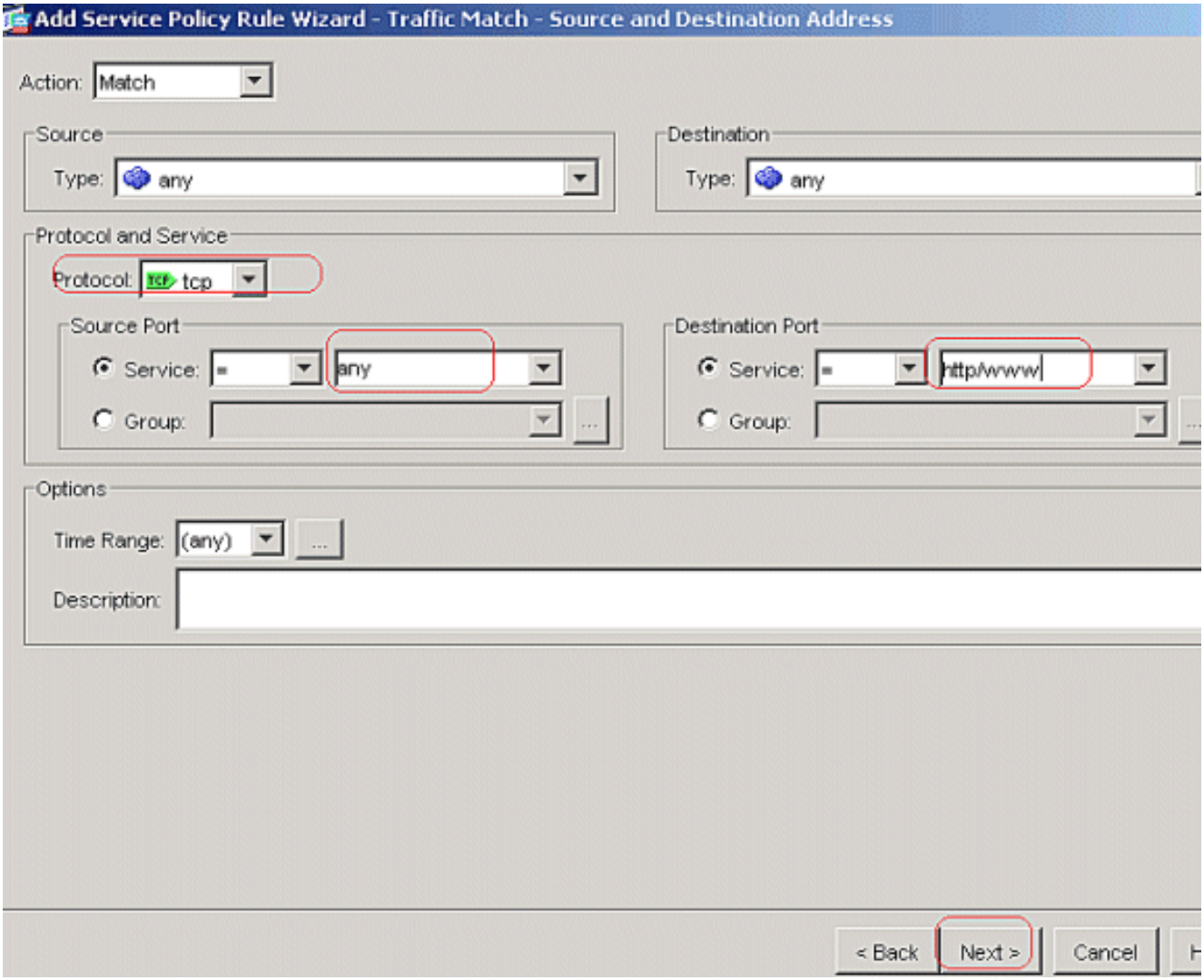
Traffico HTTP Selezionare il pulsante di opzione **Interface** (Interfaccia) con l'interfaccia **interna** dal menu a discesa e impostare Policy Name (Nome criterio) come **inside-policy**. Fare clic su **Next** (Avanti).



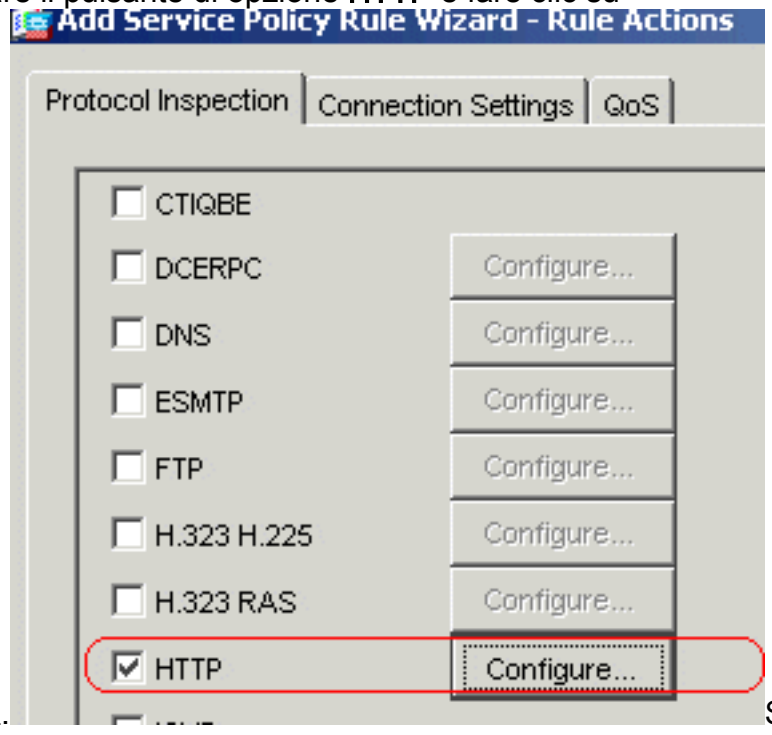
Creare una mappa di classe per il **traffico http** e controllare l'**indirizzo IP di origine e di destinazione (utilizza l'ACL)**. Fare clic su **Next** (Avanti).



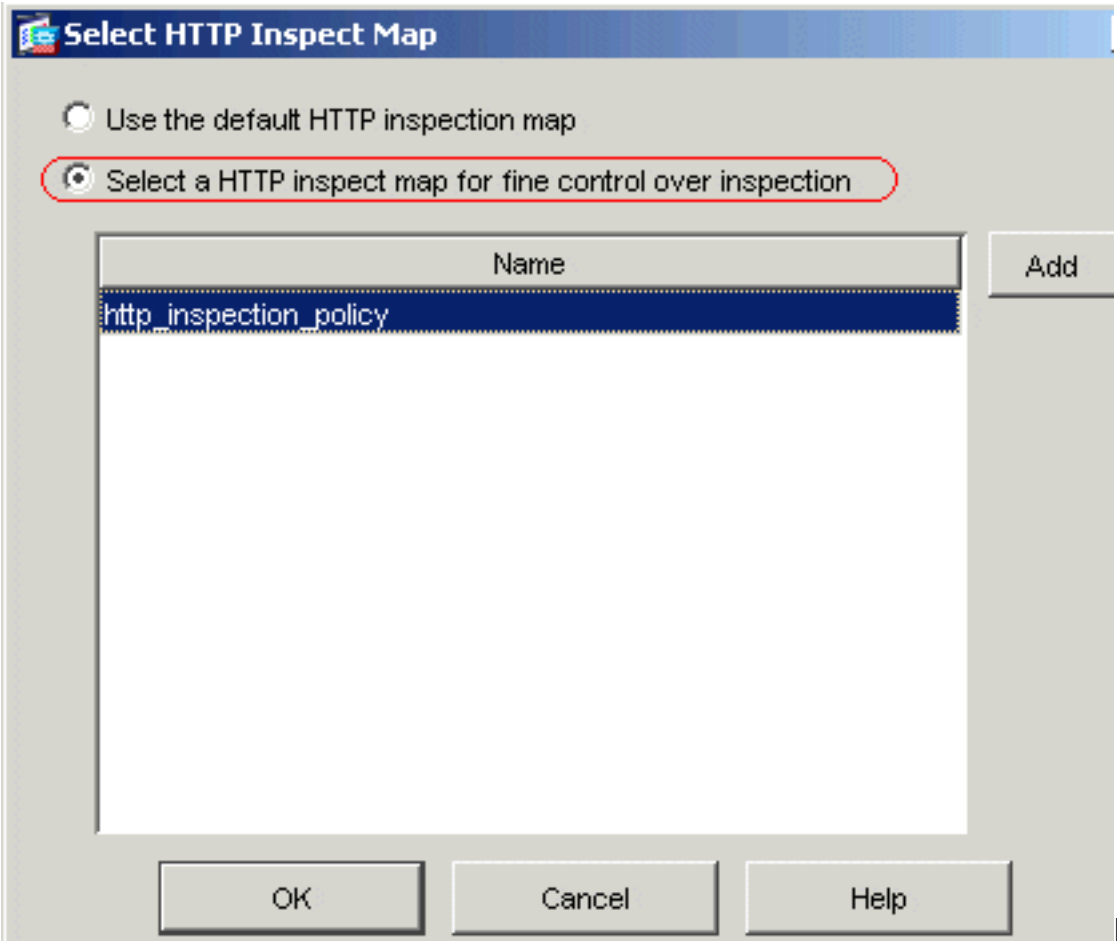
Selezionare Origine e Destinazione come **qualsiasi** con la porta TCP come **HTTP**. Fare clic su **Next**
(Avanti).



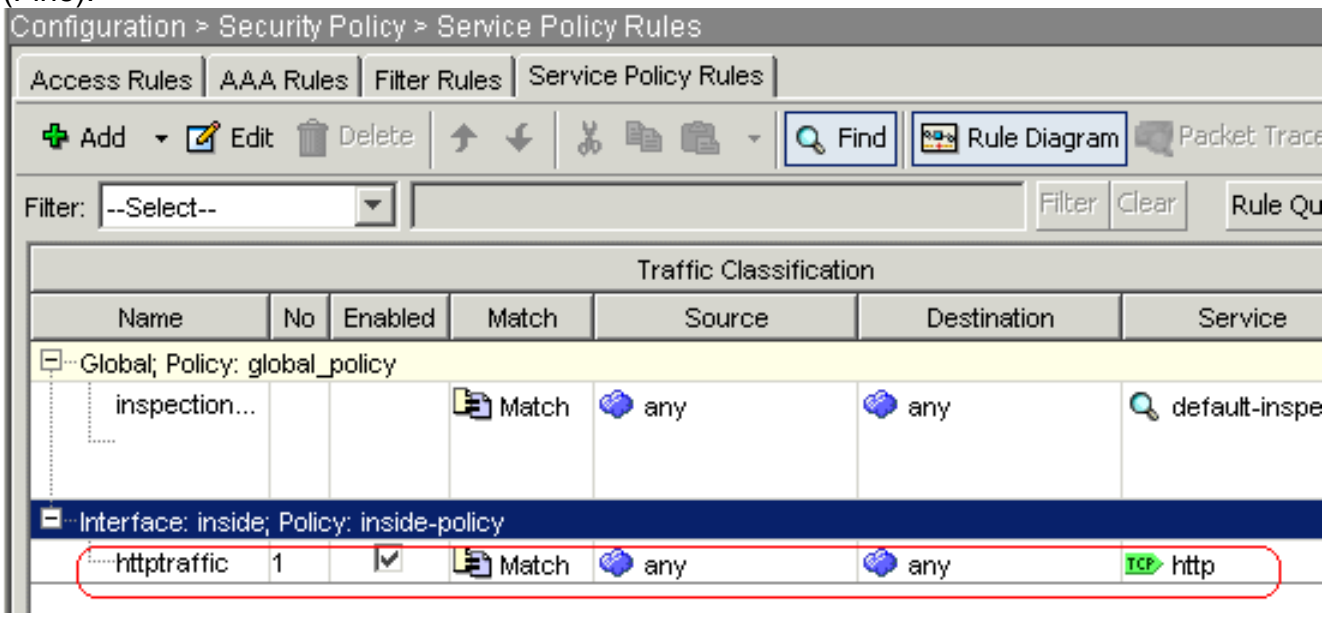
Selezionare il pulsante di opzione **HTTP** e fare clic su **Configura**.



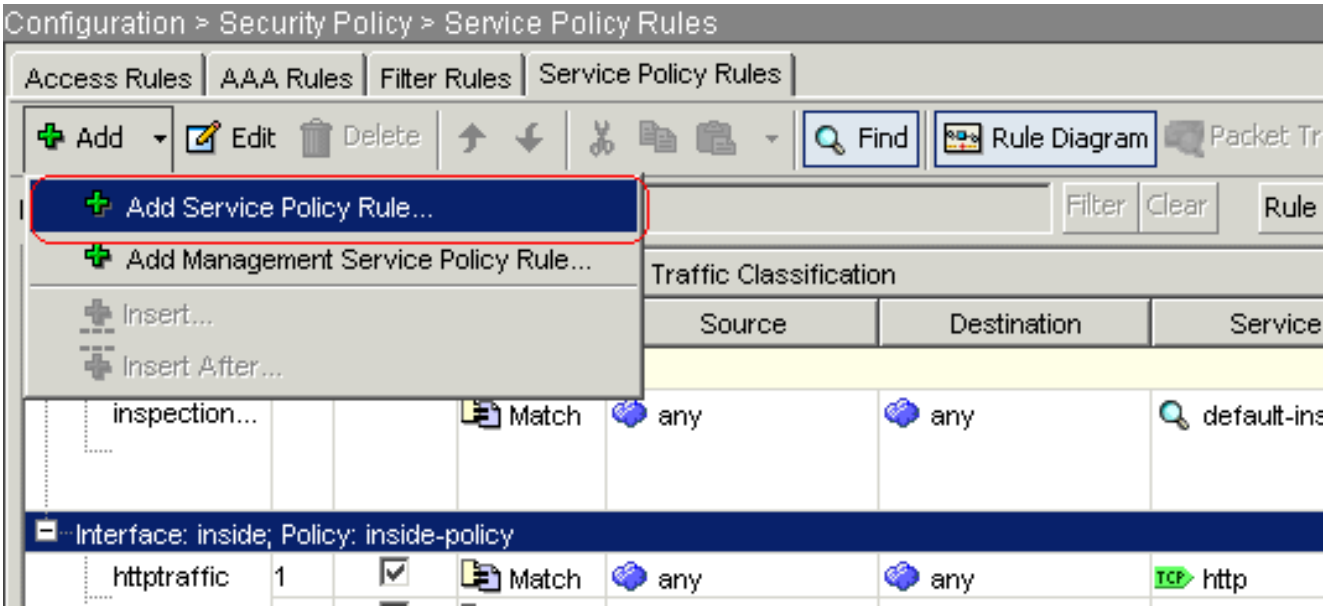
Selezionare il pulsante di opzione **Selezionare una mappa di ispezione HTTP per il controllo sull'ispezione**. Fare clic su



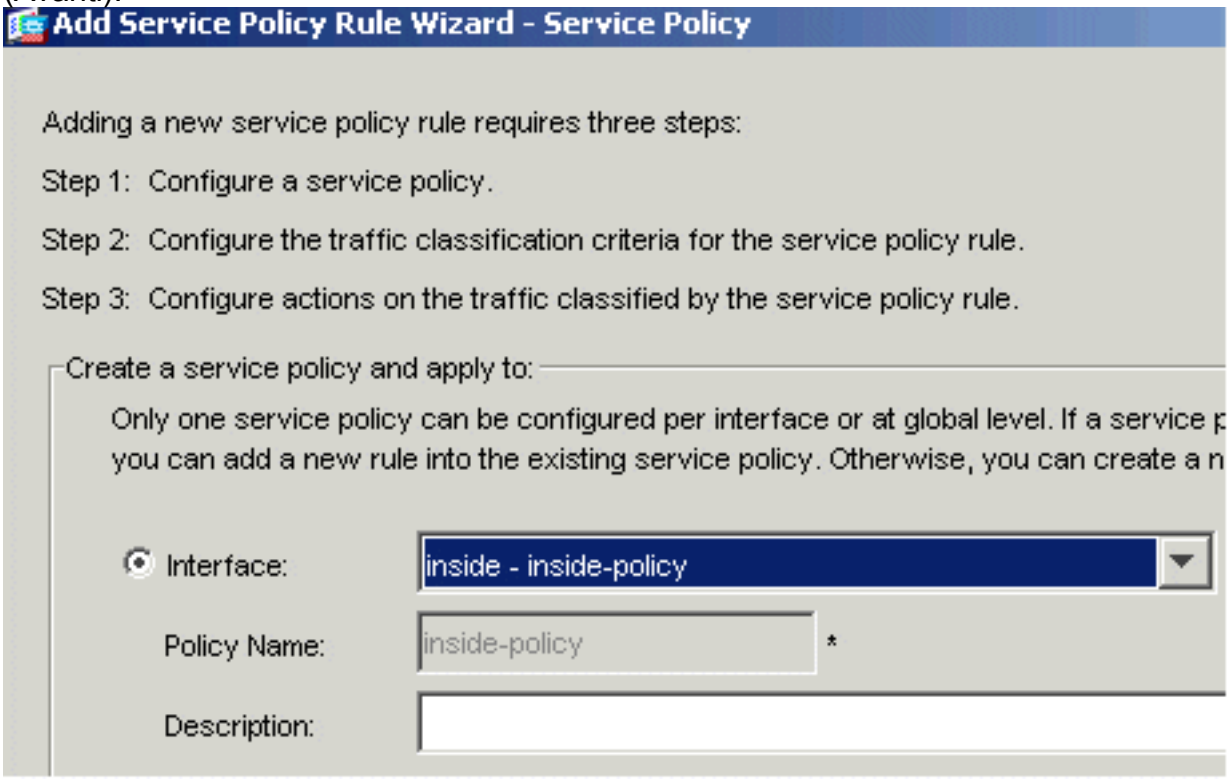
OK. Fare clic su **Finish** (Fine).



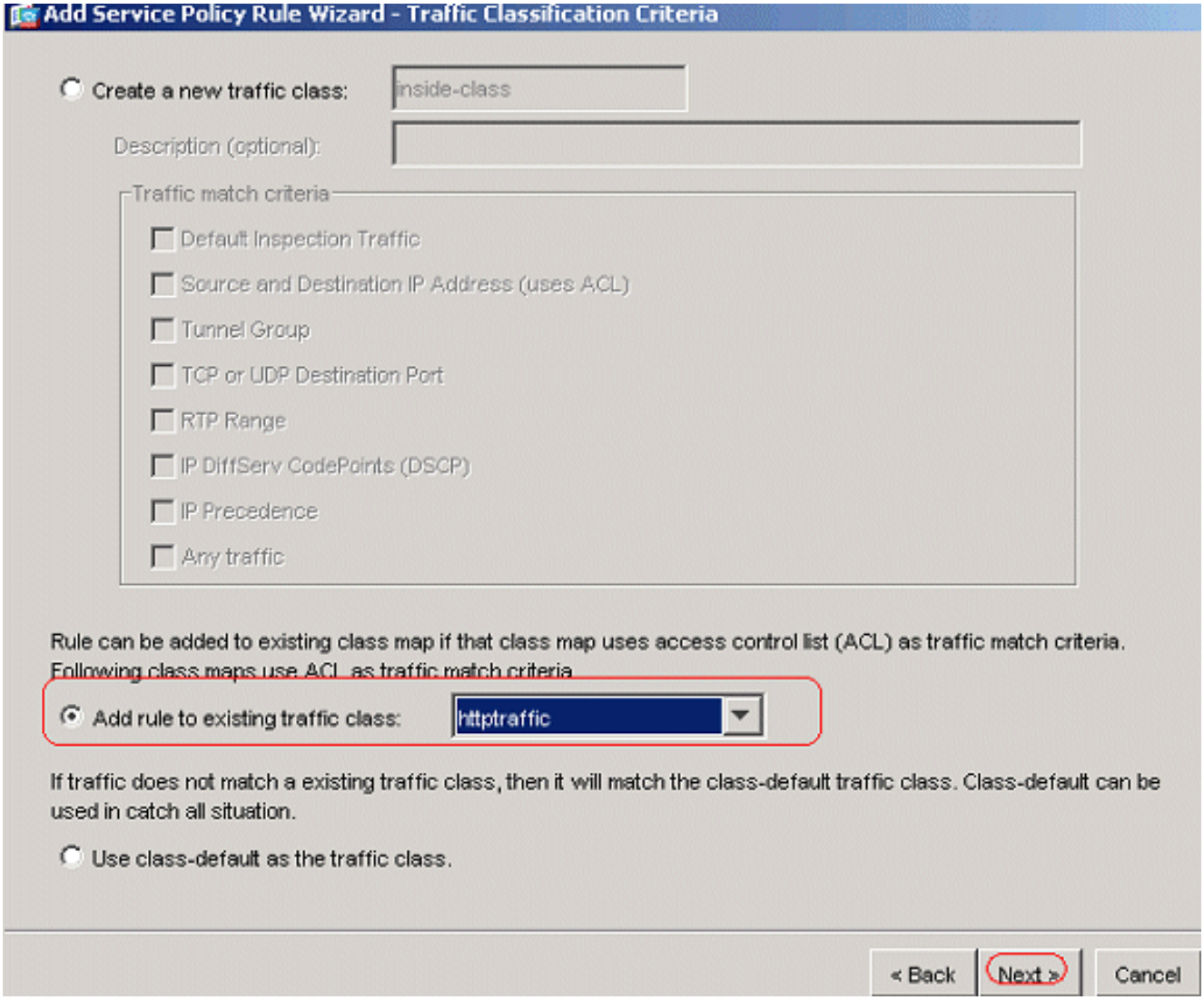
Traffico porta 8080 Fare nuovamente clic su **Aggiungi > Aggiungi regola dei criteri del servizio**.



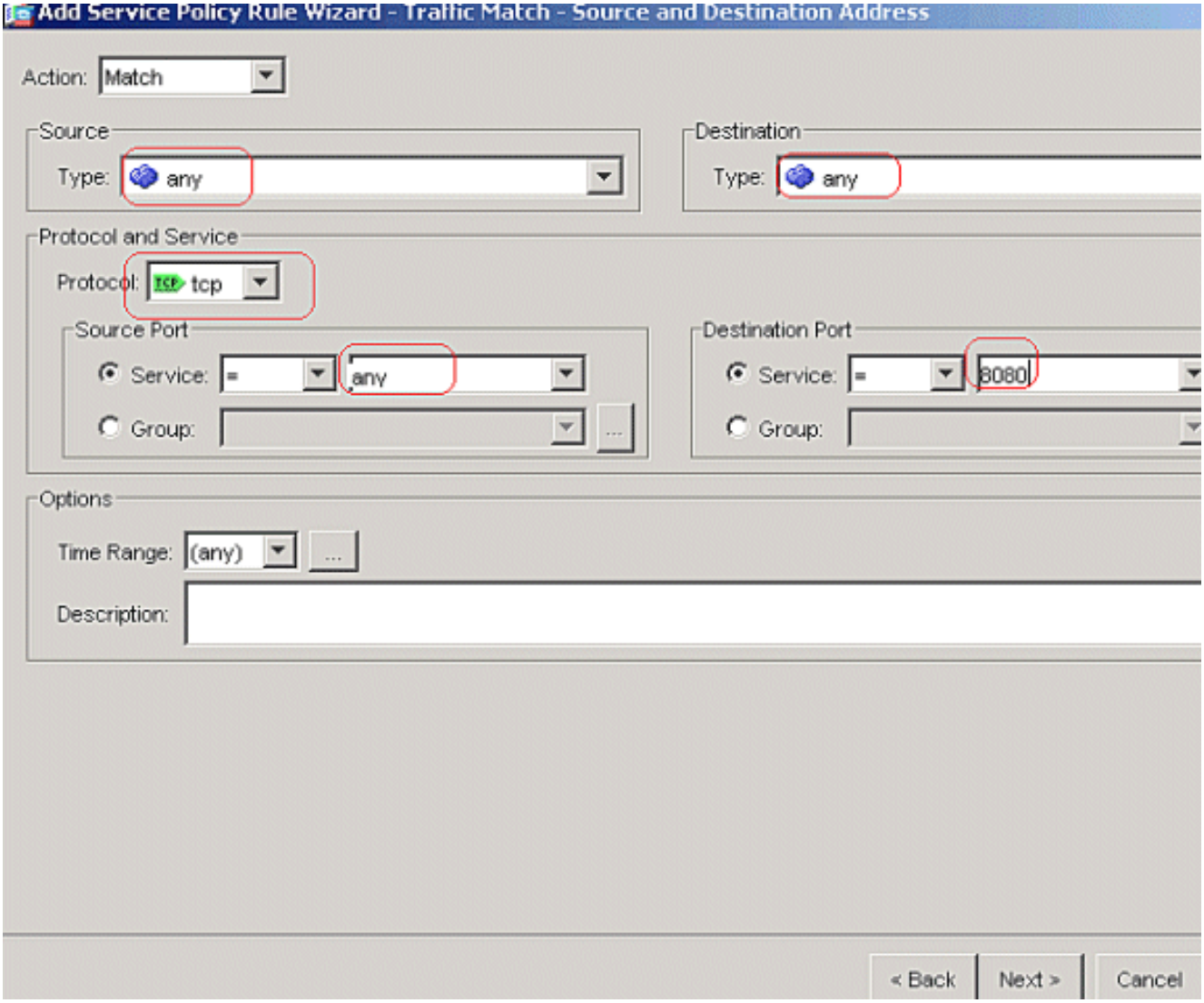
Fare clic su **Next** (Avanti).



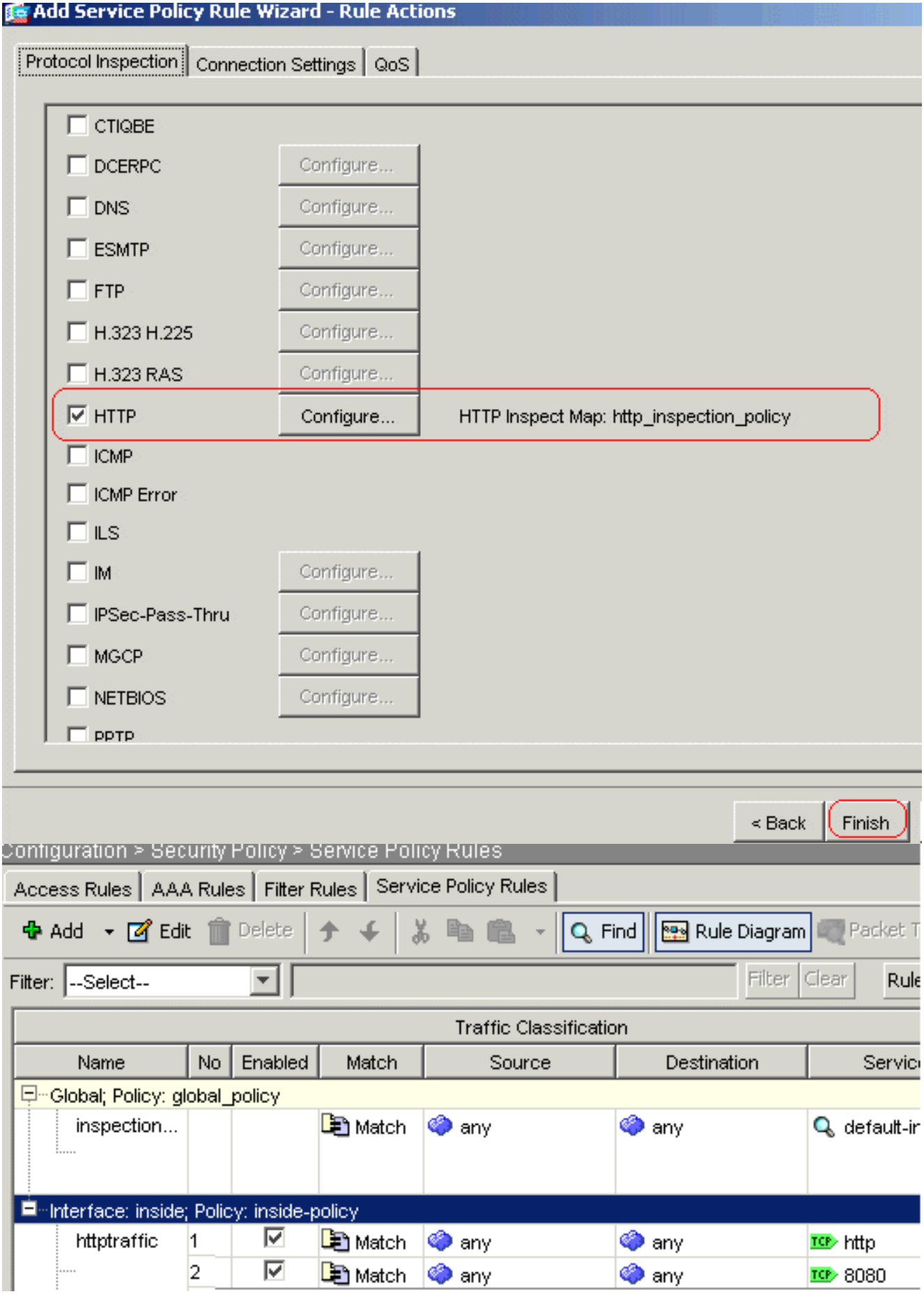
Selezionare il pulsante di opzione **Add rule to existing traffic class**, quindi scegliere **httptraffic** dal menu a discesa. Fare clic su **Next** (Avanti).



Selezionare l'origine e la destinazione come **qualsiasi** con la porta TCP **8080**. Fare clic su **Next**
(Avanti).



Fare clic su **Finish** (Fine).



Fare clic su **Apply** (Applica).**Configurazione CLI equivalente**

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show running-config regex**: visualizza le espressioni regolari configurate
```
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**: visualizza le mappe di classe configurate
```
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**: visualizza le mappe dei criteri che controllano il traffico http configurato
```
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**: visualizza tutte le configurazioni della mappa dei criteri e la configurazione predefinita della mappa dei criteri.
```
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**: visualizza tutte le configurazioni dei criteri del servizio attualmente in esecuzione.

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

- **show running-config access-list**: visualizza la configurazione dell'elenco degli accessi in esecuzione sull'appliance di sicurezza.

```
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#
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug http**: visualizza i messaggi di debug per il traffico HTTP.

Informazioni correlate

- Pagina di supporto di Cisco Adaptive Security Appliance
- Pagina di supporto di Cisco Adaptive Security Device Manager (ASDM)
- Cisco serie 500 PIX Support Page
- Documentazione e supporto tecnico – Cisco Systems