ASA/PIX 8.x: esempio di blocco di determinati siti Web (URL) tramite espressioni regolari con configurazione MPF

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Security Appliance ASA/PIX 8.x che usa espressioni regolari con Modular Policy Framework (MPF) per bloccare alcuni siti Web (URL).

Nota: questa configurazione non blocca tutti i download di applicazioni. Per un blocco affidabile dei file, è necessario usare un accessorio dedicato come Ironport serie S o un modulo come il modulo CSC per l'appliance ASA.

Nota: 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 8.0(x) e successive
- Cisco Adaptive Security Device Manager (ASDM) versione 6.x per ASA 8.x

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 8.0(x) e successive.

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 applicabile 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 è costituita da 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 consente di trovare le stringhe di testo letteralmente come una stringa esatta oppure tramite l'utilizzo di metacaratteri, in modo che sia possibile trovare più varianti di una stringa di testo. È possibile utilizzare un'espressione regolare per indicare 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 il punto interrogativo (?) o una tabulazione. Ad esempio, digitare d[Ctrl+V]?g per immettere d?g nella configurazione.

Per la creazione di un'espressione regolare, utilizzare il comando regex, che può essere utilizzato per varie caratteristiche che richiedono la corrispondenza del testo. È ad esempio possibile configurare azioni speciali per l'ispezione delle applicazioni utilizzando la struttura dei criteri modulare che utilizza una mappa dei criteri di ispezione. Per ulteriori informazioni, fare riferimento al comando policy map type inspect. 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 match consentono di identificare il testo in un pacchetto utilizzando 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. Per ulteriori informazioni, fare riferimento al comando class-map type regex.

In questa tabella vengono elencati 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 a una delle espressioni che separa. Ad esempio, cane|gatto corrisponde a cane o gatto.
?	Punto interrogativo	Un 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 un numero qualsiasi. 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 anche [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	Se 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	Corrisponde a una scheda 0x09
\f	Alimentatore	Corrisponde a un feed di moduli 0x0c
\xNN	Numero esadecimale con escape	Trova/sostituisce un carattere ASCII che utilizza un carattere esadecimale costituito esattamente da due cifre
\NNN	Numero ottale scappato	Trova/sostituisce un carattere ASCII come ottale che è costituito esattamente da tre cifre. Ad esempio, il carattere 040 rappresenta uno spazio.

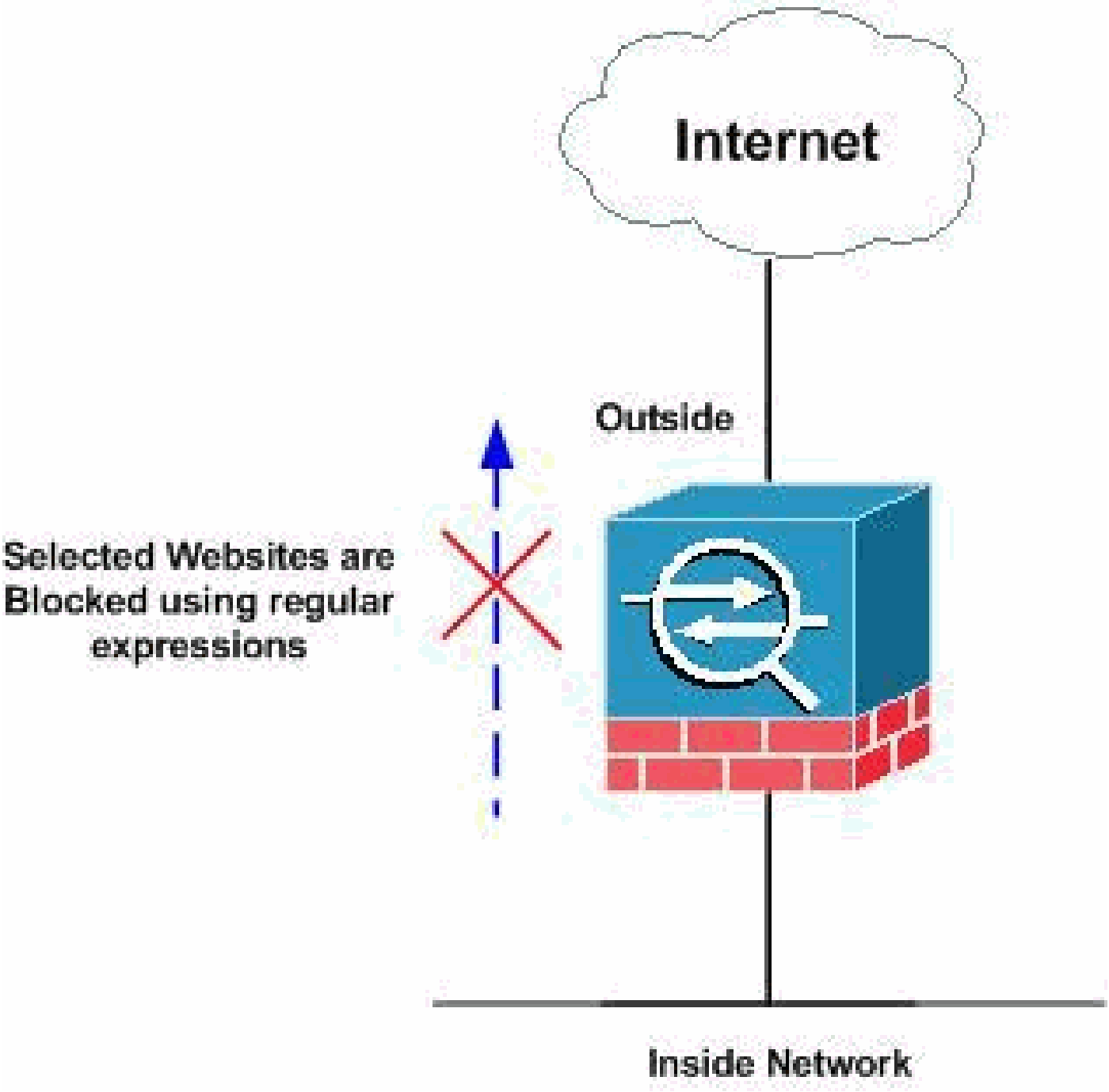
Configurazione

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

Il documento usa la seguente configurazione di rete:



Configurazioni

In questo documento vengono usate le seguenti configurazioni:

- Configurazione ASA CLI
- ASA Configuration 8.x con ASDM 6.x

Configurazione ASA CLI

Configurazione ASA CLI
<#root>

```
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

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

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 ver
```

```
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


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 !


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 th


!
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#
```

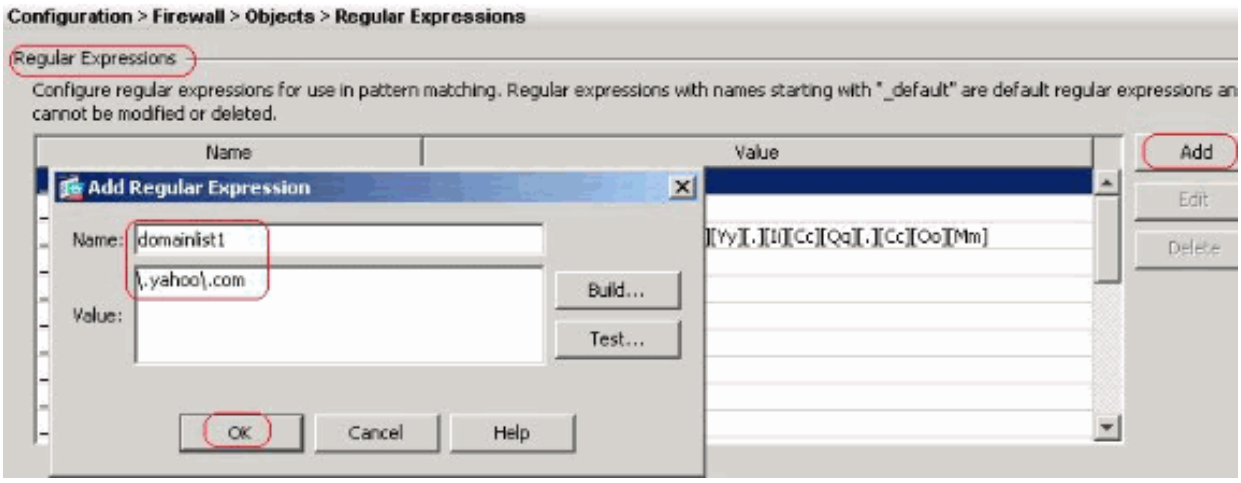
ASA Configuration 8.x con ASDM 6.x

Completare questi passaggi per configurare le espressioni regolari e applicarle in MPF per bloccare i siti Web specifici come mostrato.

1. Crea espressioni regolari

   Scegliere Configurazione > Firewall > Oggetti > Espressioni regolari e fare clic su Aggiungi nella scheda Espressione regolare per creare le espressioni regolari come mostrato.

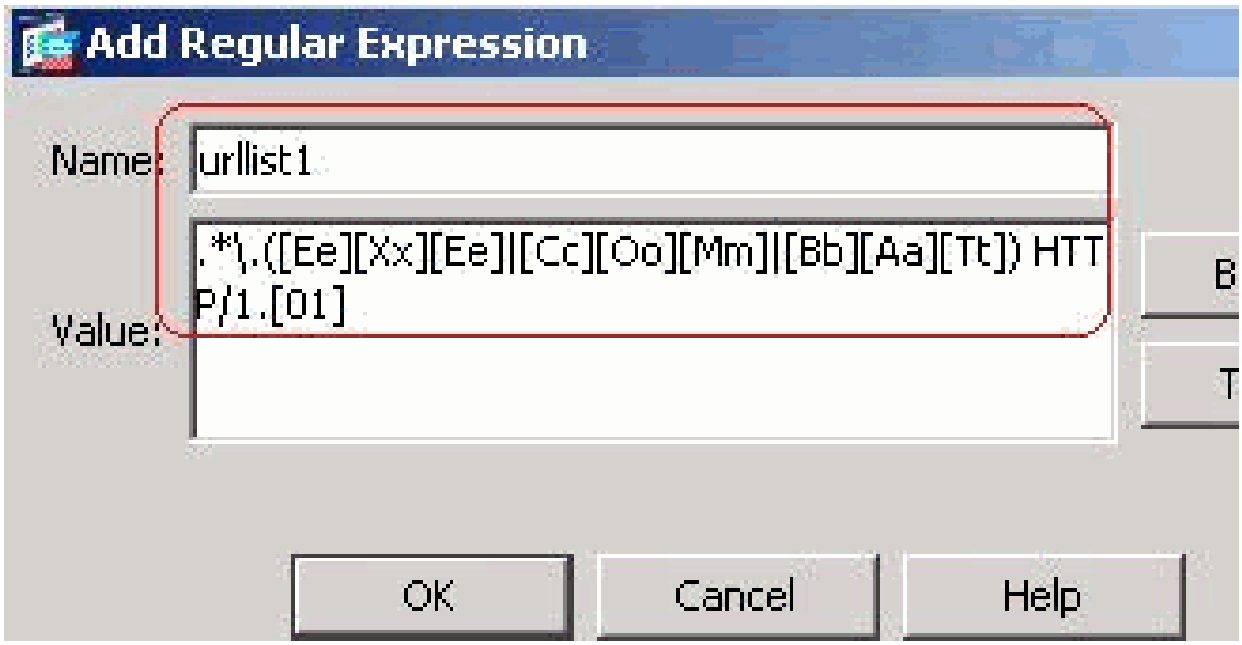
   a. Creare un'espressione regolare domainlist1 per acquisire il nome di dominio yahoo.com. Fare clic su OK.



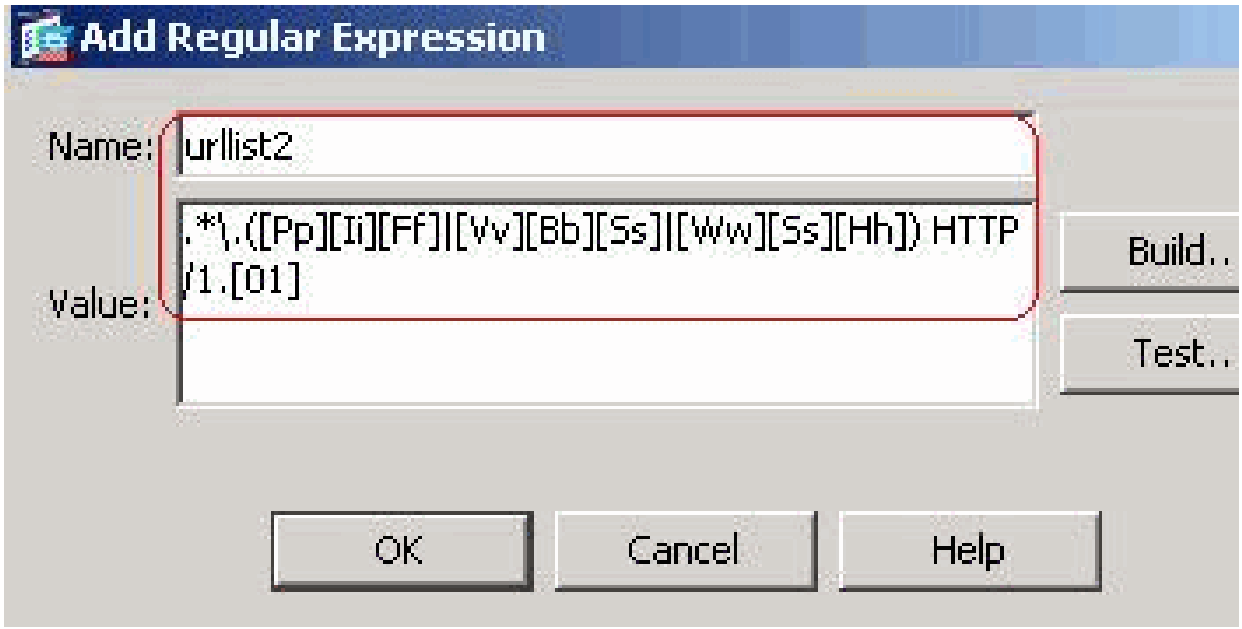
   b. Creare un'espressione regolare domainlist2 per acquisire il nome di dominio myspace.com. Fare clic su OK.

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

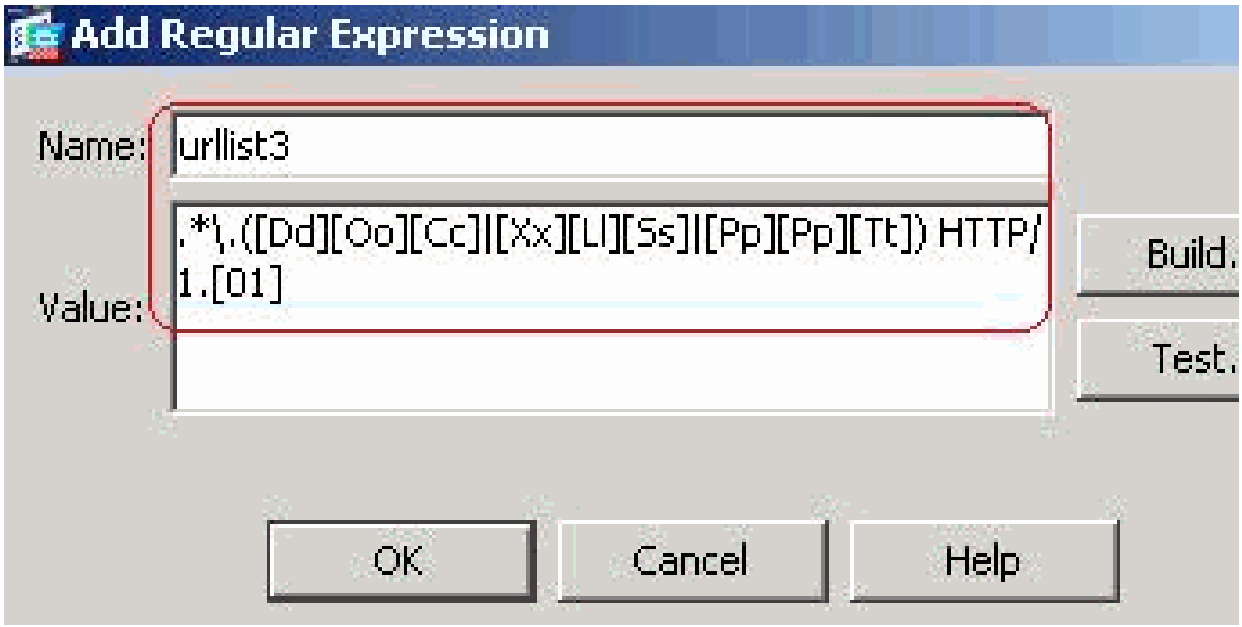
d. Creare un'espressione regolare urllist1 per acquisire le estensioni di file exe, com e bat purché la versione http utilizzata dal browser Web sia 1.0 o 1.1. Fare clic su OK.



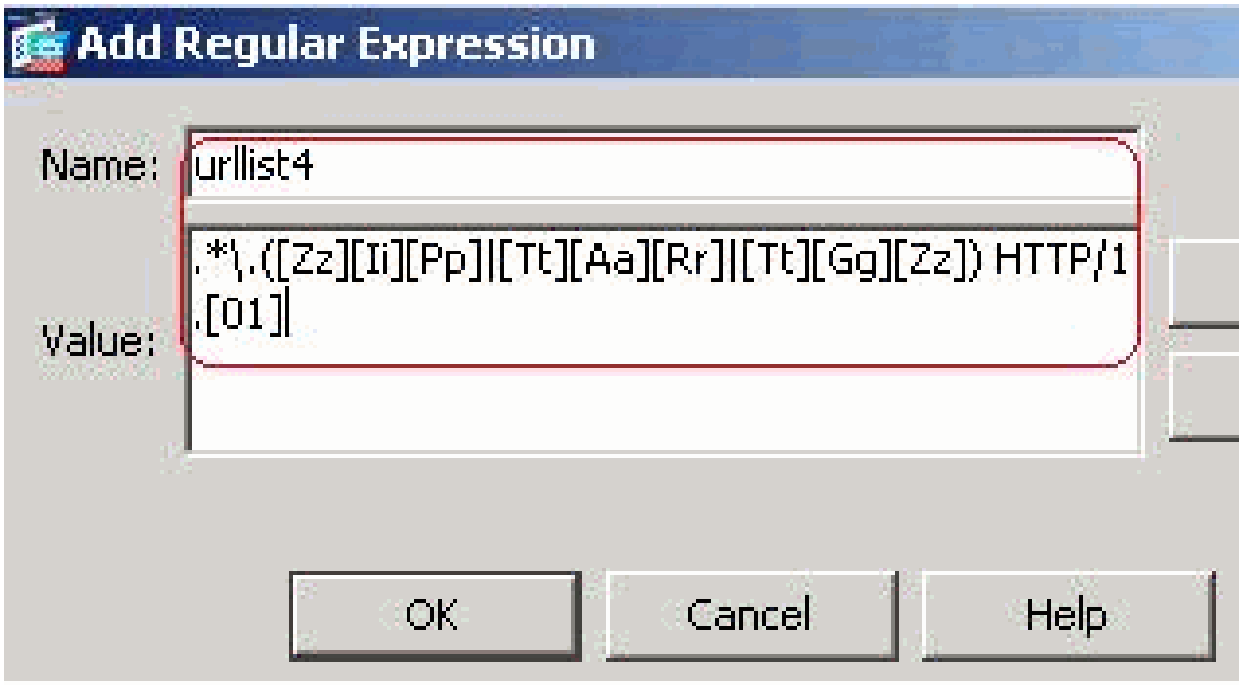
e. Creare un'espressione regolare urllist2 per acquisire le estensioni di file pif, vbs e wsh a condizione che la versione http utilizzata dal browser Web sia 1.0 o 1.1. Fare clic su OK.



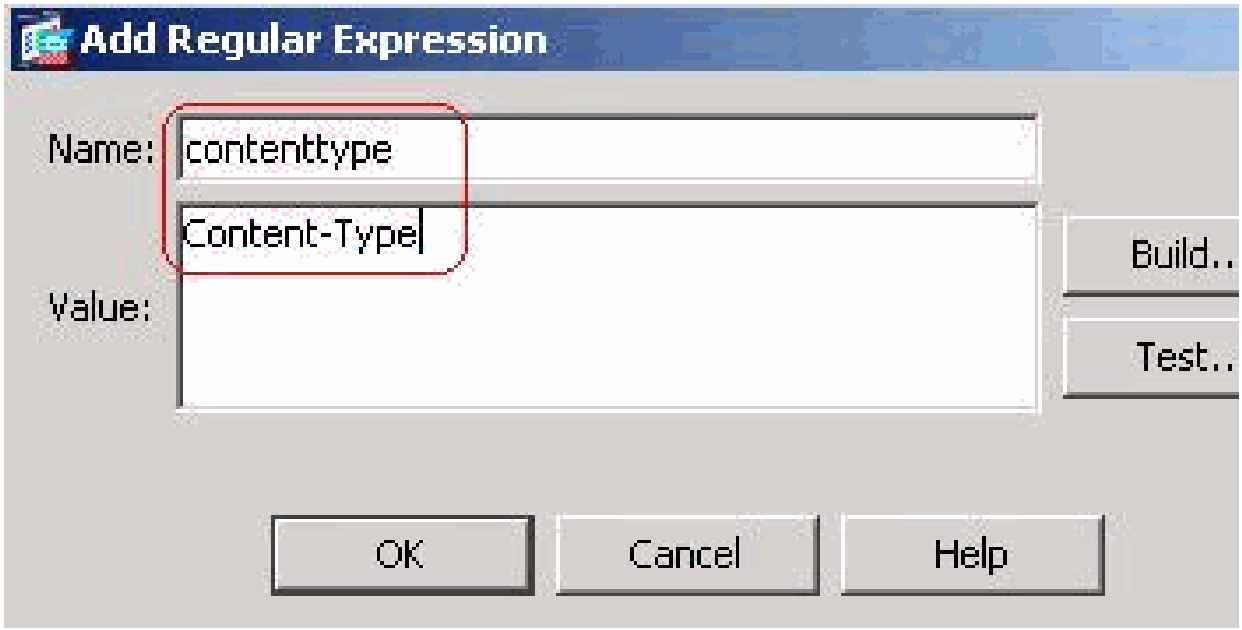
f. Creare un'espressione regolare urllist3 per acquisire le estensioni di file doc, xls e ppt a condizione che la versione http utilizzata dal browser Web sia 1.0 o 1.1. Fare clic su OK.



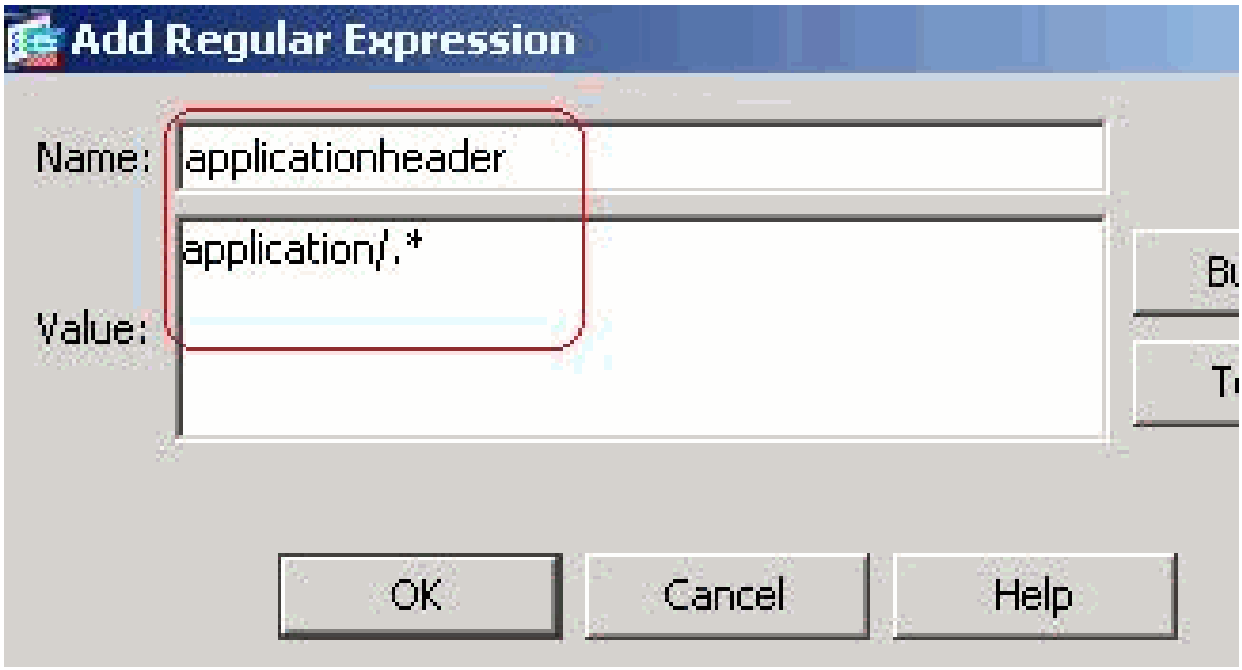
g. Creare un'espressione regolare urllist4 per acquisire le estensioni di file zip, tar e tgz a condizione che la versione http utilizzata dal browser Web sia 1.0 o 1.1. Fare clic su OK.



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



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



Configurazione CLI equivalente

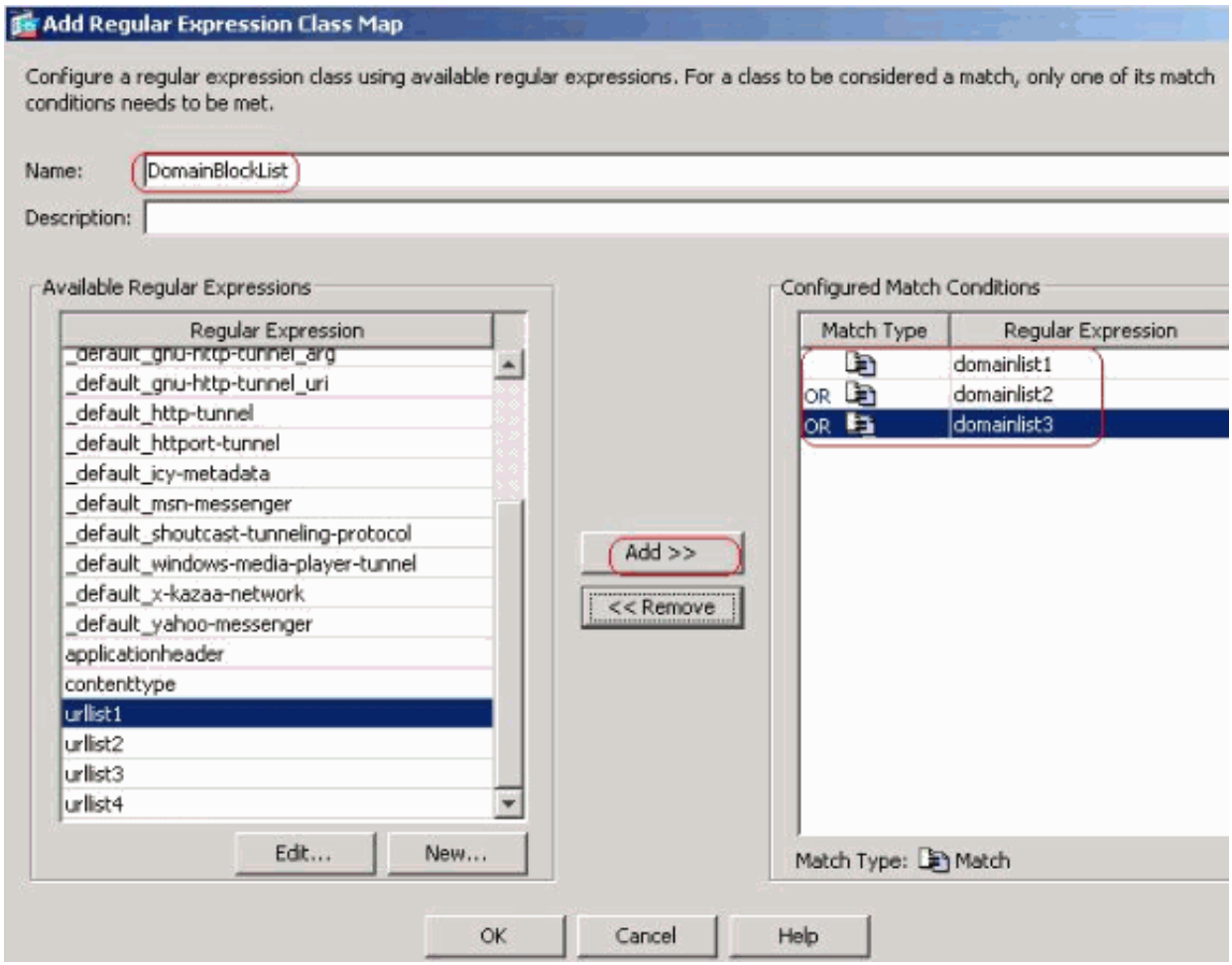
Configurazione ASA CLI
<#root> ciscoasa# **configure terminal** ciscoasa(config)# **regex urllist1** ".*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt])$ ciscoasa(config)# **regex urllist2** ".*\.([Pp][Ii][Ff]|[Vv][Bb][Ss]|[Ww][Ss][Hh])$ ciscoasa(config)# **regex urllist3** ".*\.([Dd][Oo][Cc]|[Xx][Ll][Ss]|[Pp][Pp][Tt])$ ciscoasa(config)# **regex urllist4** ".*\.([Zz][Ii][Pp]|[Tt][Aa][Rr]|[Tt][Gg][Zz])$ ciscoasa(config)# **regex domainlist1** "\.yahoo\.com" ciscoasa(config)# **regex domainlist2** "\.myspace\.com"

```
ciscoasa(config)#

regex domainlist3

 "\.youtube\.com"
ciscoasa(config)#

regex contenttype

 "Content-Type"
ciscoasa(config)#

regex applicationheader

 "application/.*"
```

2. Crea classi di espressioni regolari

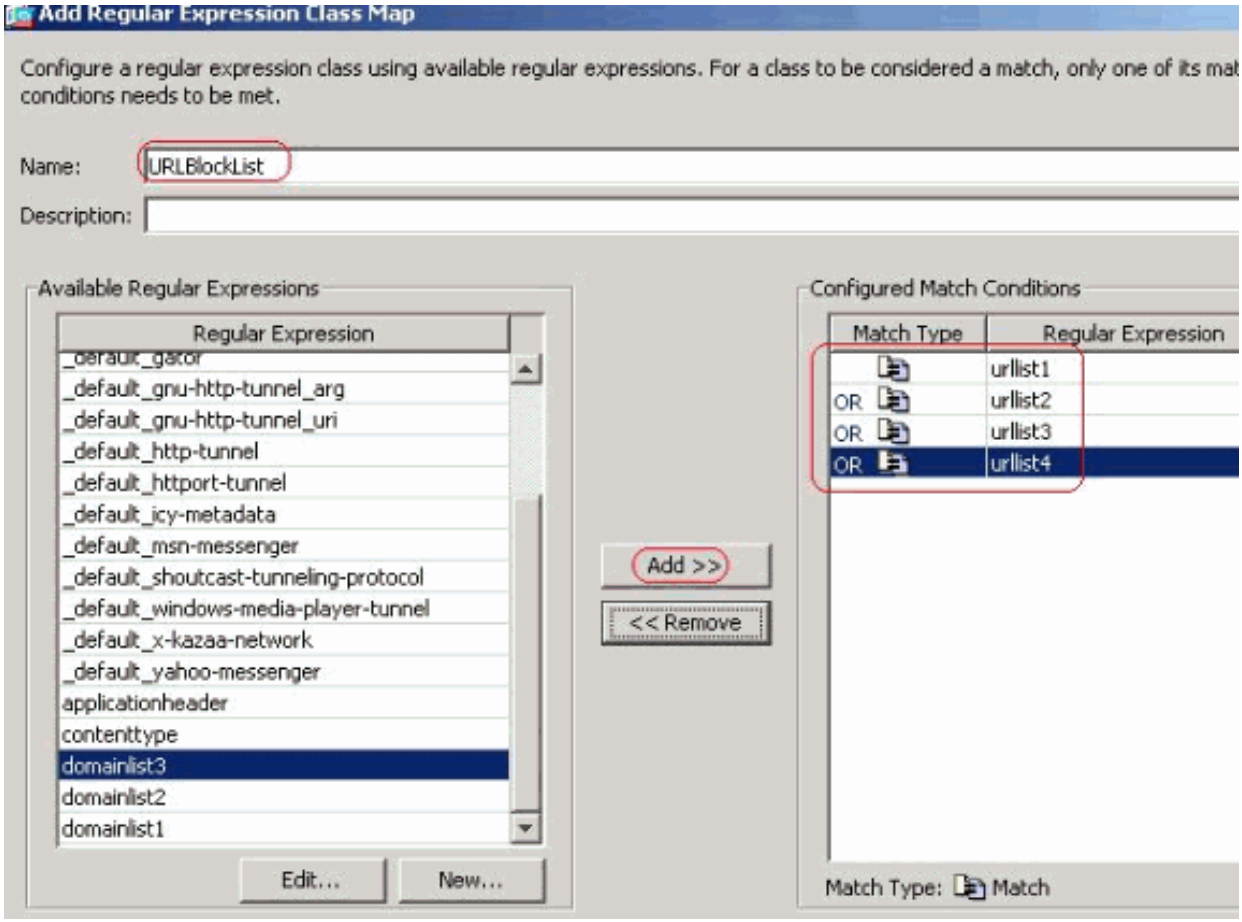
   Scegliere Configurazione > Firewall > Oggetti > Espressioni regolari e fare clic su Aggiungi nella scheda Classi di espressioni regolari per creare le varie classi come mostrato.

   a. Creare una classe di espressione regolare DomainBlockList in modo che corrisponda a una qualsiasi delle espressioni regolari domainlist1, domainlist2 e domainlist3. Fare clic su OK.



   b. 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

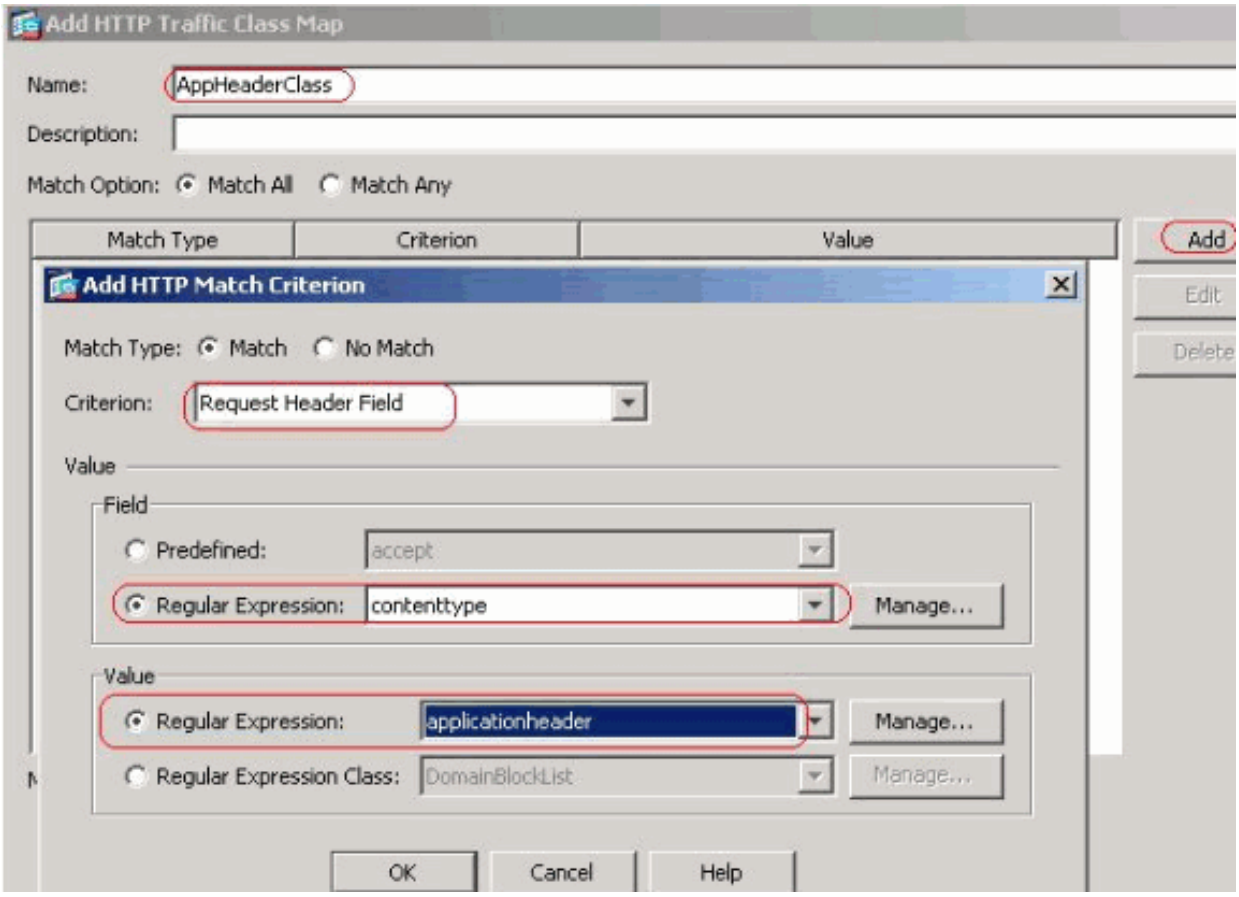
Configurazione ASA CLI
<#root> ciscoasa# **configure terminal** ciscoasa(config)# **class-map type inspect http match-all BlockDomainsClass** ciscoasa(config-cmap)# **match request header host regex class DomainBlockList** ciscoasa(config-cmap)# **exit** ciscoasa(config)# **class-map type regex match-any URLBlockList** ciscoasa(config-cmap)# **match regex urllist1**

```
ciscoasa(config-cmap)#
match regex urllist2
ciscoasa(config-cmap)#
match regex urllist3
ciscoasa(config-cmap)#
match regex urllist4
ciscoasa(config-cmap)#
exit
```

3. Ispezionare il traffico identificato con le mappe di classe

   Scegliere Configurazione > Firewall > Oggetti > Mappe classi > HTTP > Aggiungi per creare una mappa di classe per ispezionare il traffico HTTP identificato dalle varie espressioni regolari, come mostrato.

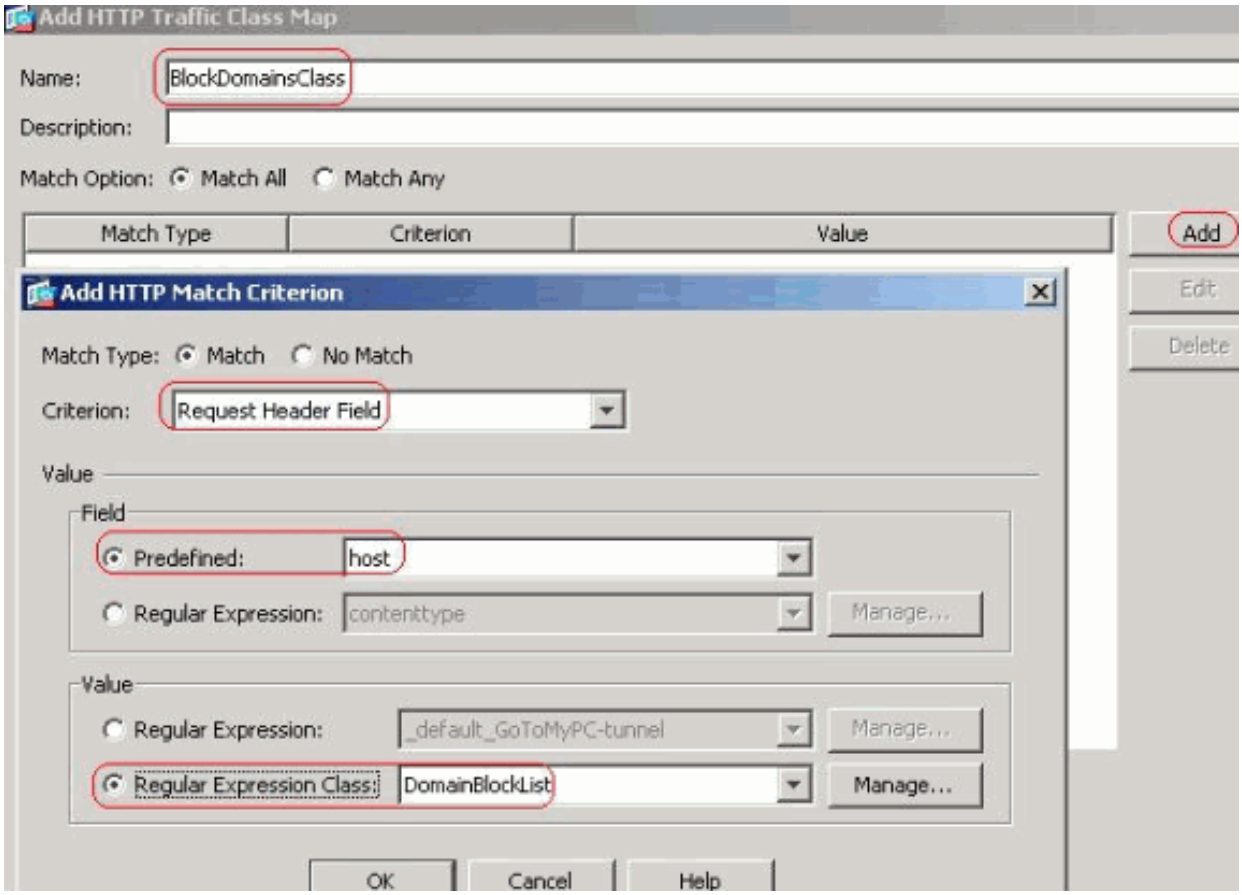
   a. Creare una mappa di classe AppHeaderClass per far corrispondere l'intestazione della risposta alle acquisizioni di espressioni regolari.



   Fare clic su OK.

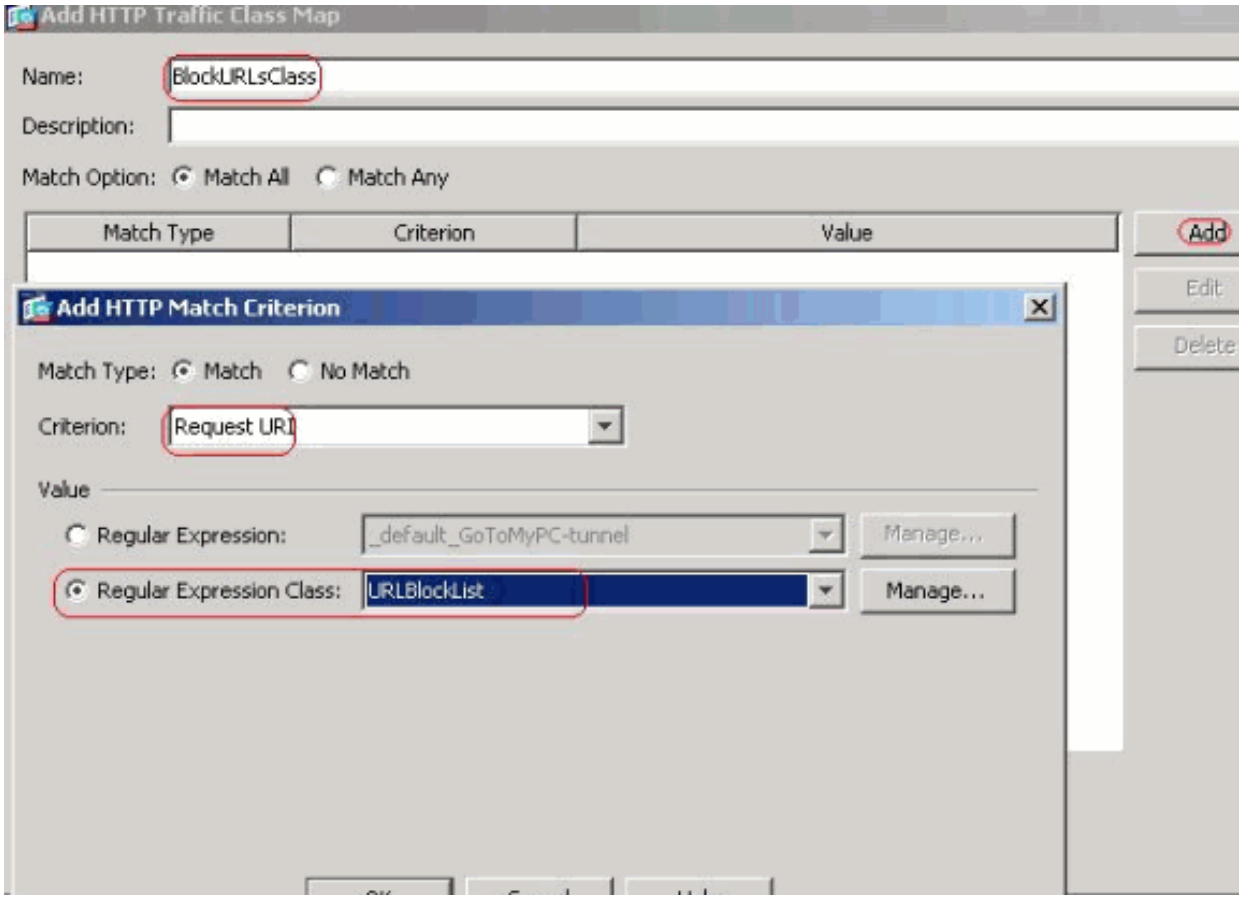
   b. Creare una mappa di classe BlockDomainsClass per far corrispondere l'intestazione

della richiesta con le acquisizioni di espressioni regolari.



Fare clic su OK.

c. Creare una mappa di classe BlockURLsClass in modo che corrisponda all'URI della richiesta con le acquisizioni di espressioni regolari.



Fare clic su OK.

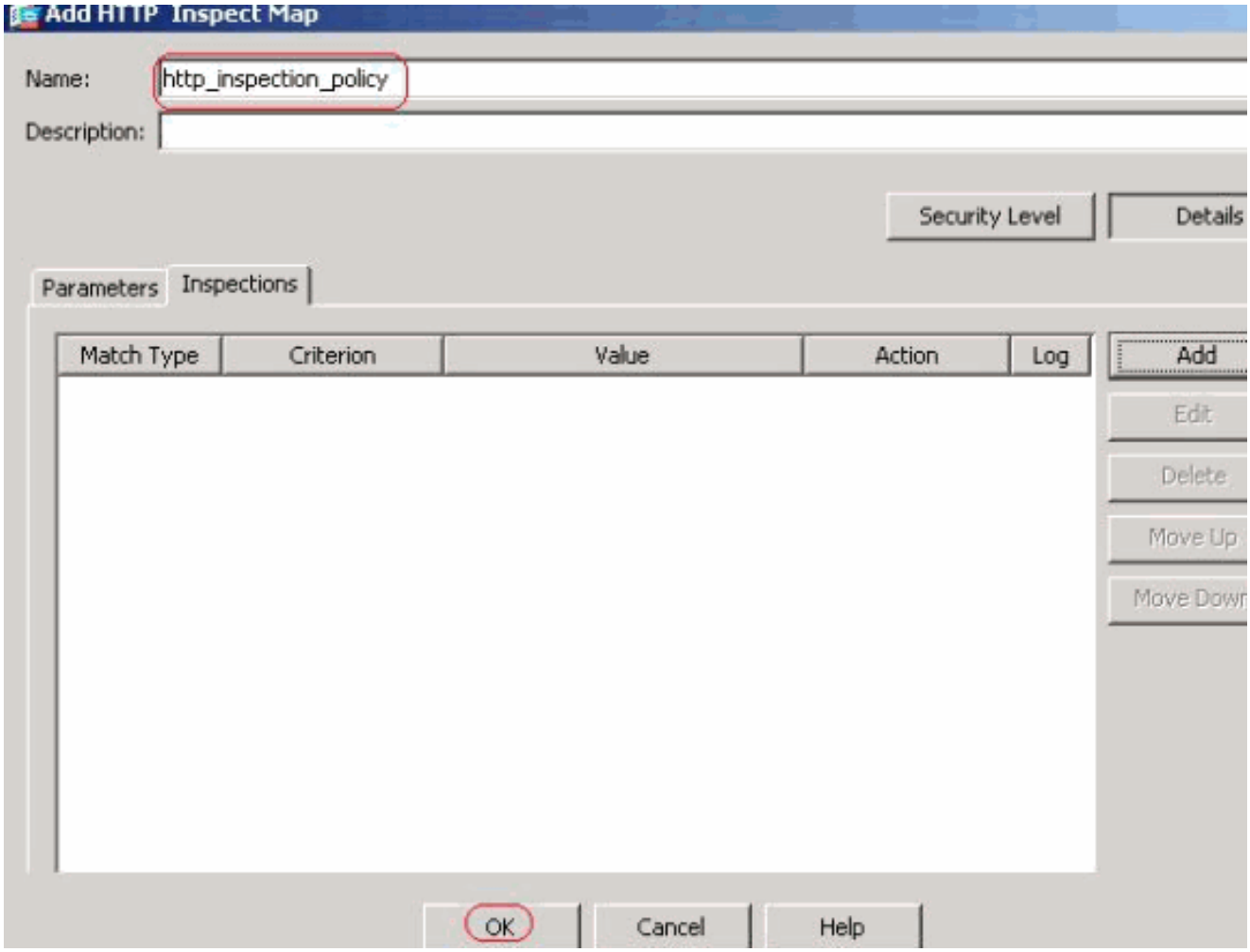
Configurazione CLI equivalente

Configurazione ASA CLI
<#root> ciscoasa# **configure terminal** ciscoasa(config)# **class-map type inspect http match-all AppHeaderClass** ciscoasa(config-cmap)# **match response header regex contenttype regex applicationheader** ciscoasa(config-cmap)# **exit** ciscoasa(config)# **class-map type inspect http match-all BlockDomainsClass** ciscoasa(config-cmap)# **match request header host regex class DomainBlockList**

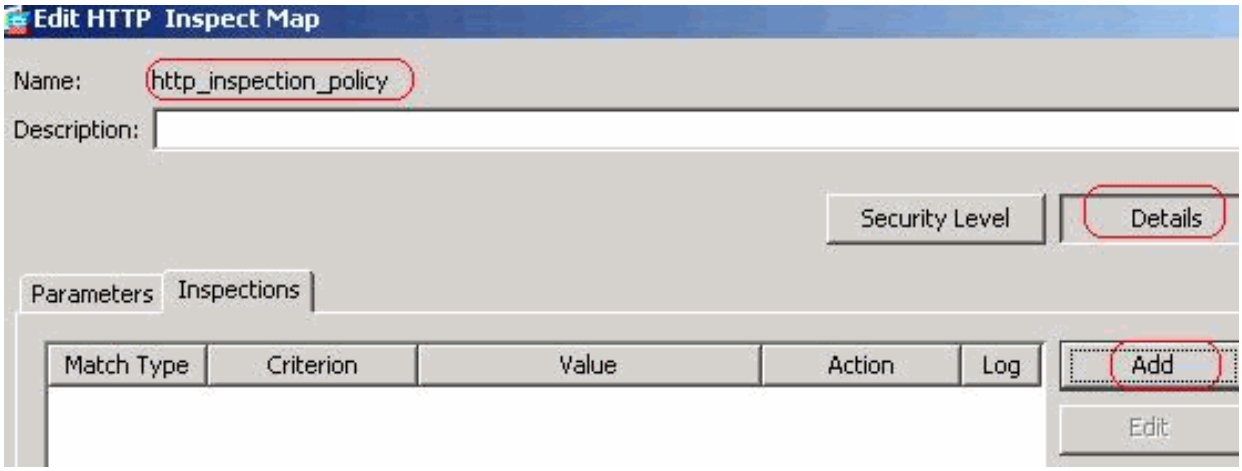
```
ciscoasa(config-cmap)#
exit
ciscoasa(config)#
class-map type inspect http match-all BlockURLsClass
ciscoasa(config-cmap)#
match request uri regex class URLBlockList
ciscoasa(config-cmap)#
exit
```

4. Impostare le azioni per il traffico corrispondente nei criteri di ispezione

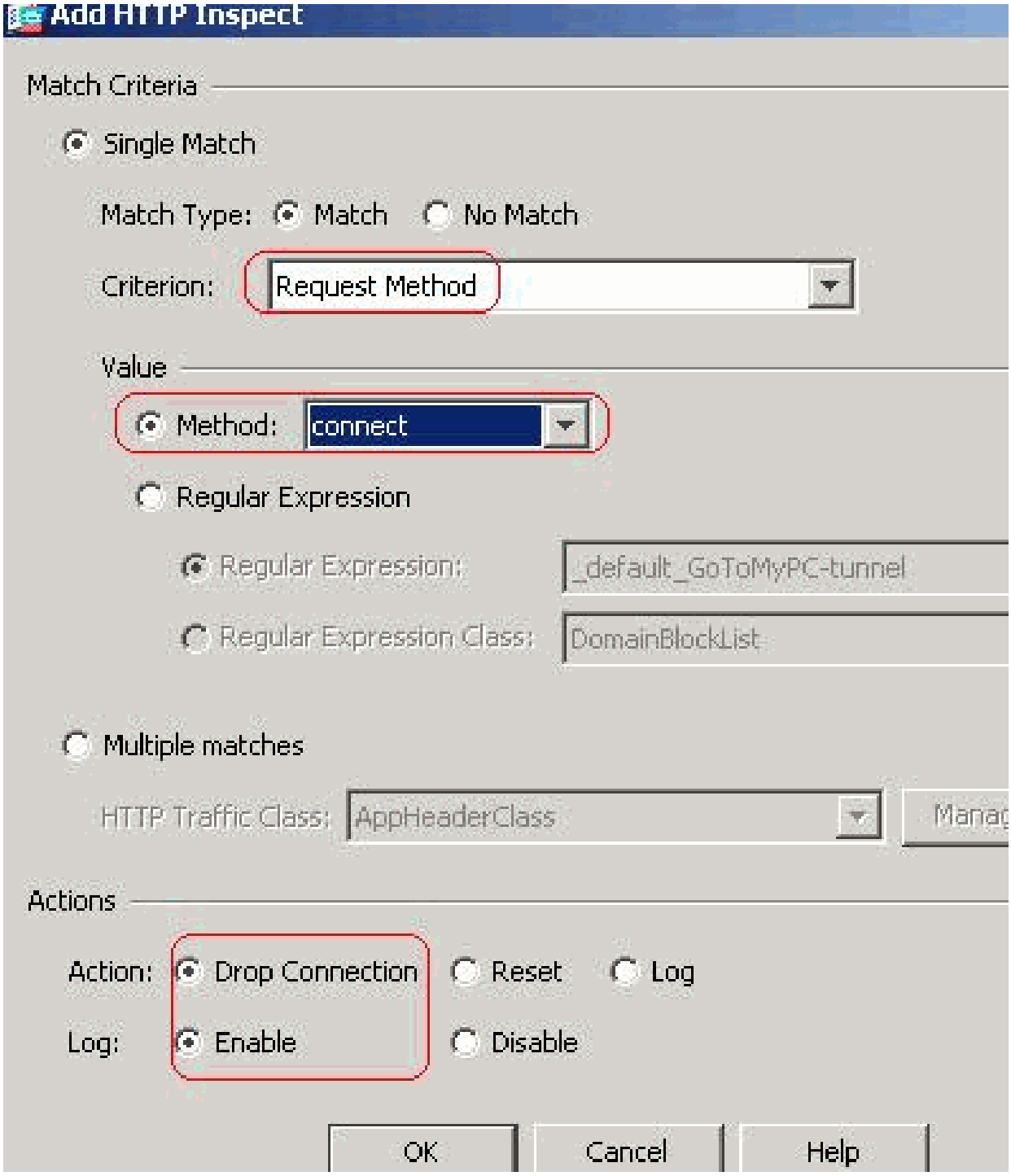
   Scegliere Configurazione > Firewall > Oggetti > Ispeziona mappe > HTTP per creare un criterio http_inspection_policy per impostare l'azione per il traffico corrispondente, come mostrato. Fare clic su OK.



   a. Scegliere Configurazione > Firewall > Oggetti > Ispeziona mappe > HTTP > http_survey_policy (fare doppio clic) e fare clic su Dettagli > Aggiungi per impostare le azioni per le varie classi create finora.

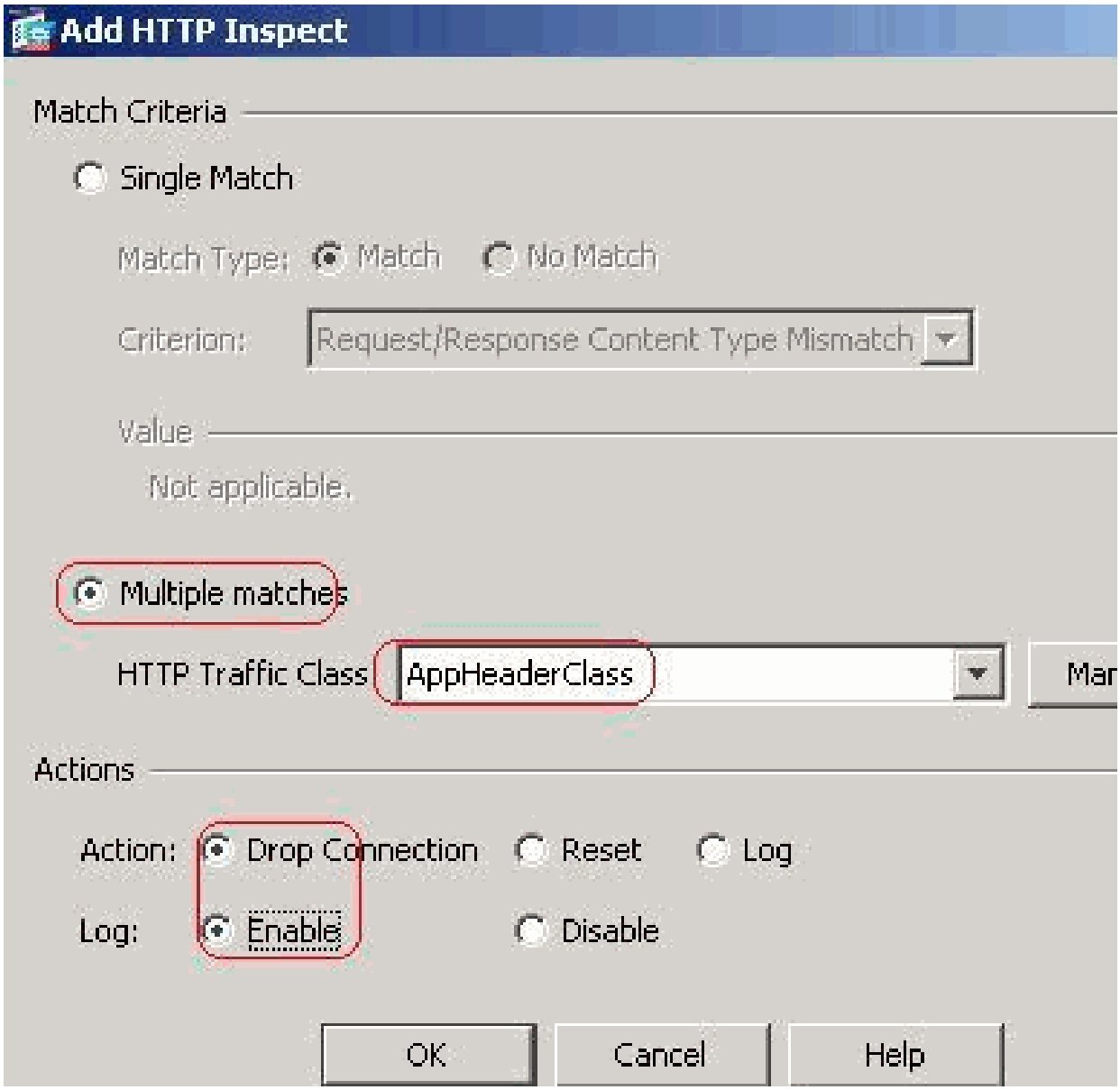


b. Impostare l'azione come Elimina connessione e Abilitare la registrazione per il criterio come metodo di richiesta e Valore come connessione.



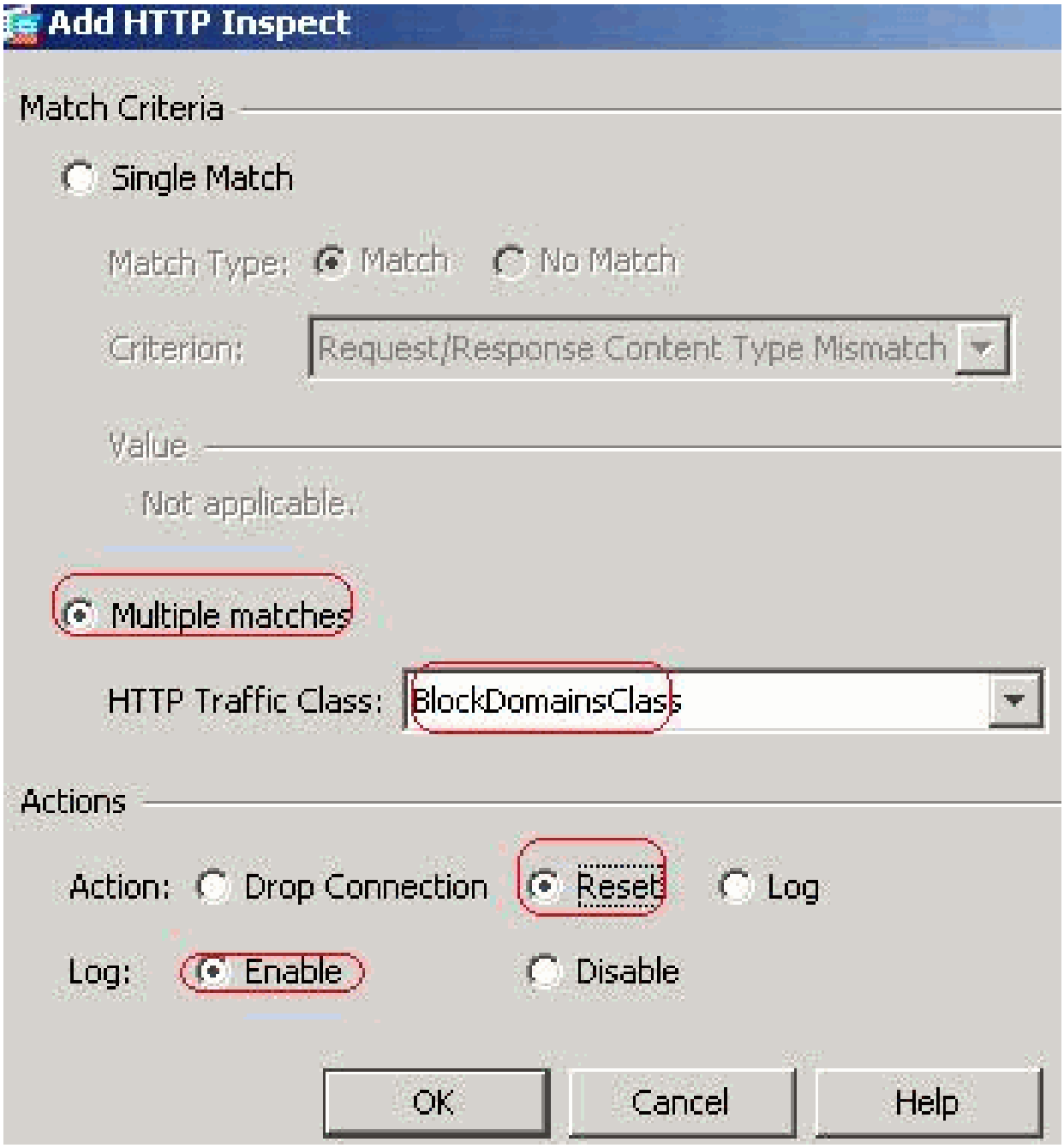
Fare clic su OK.

c. Impostare l'azione come Elimina connessione e Abilitare la registrazione per la classe AppHeaderClass.



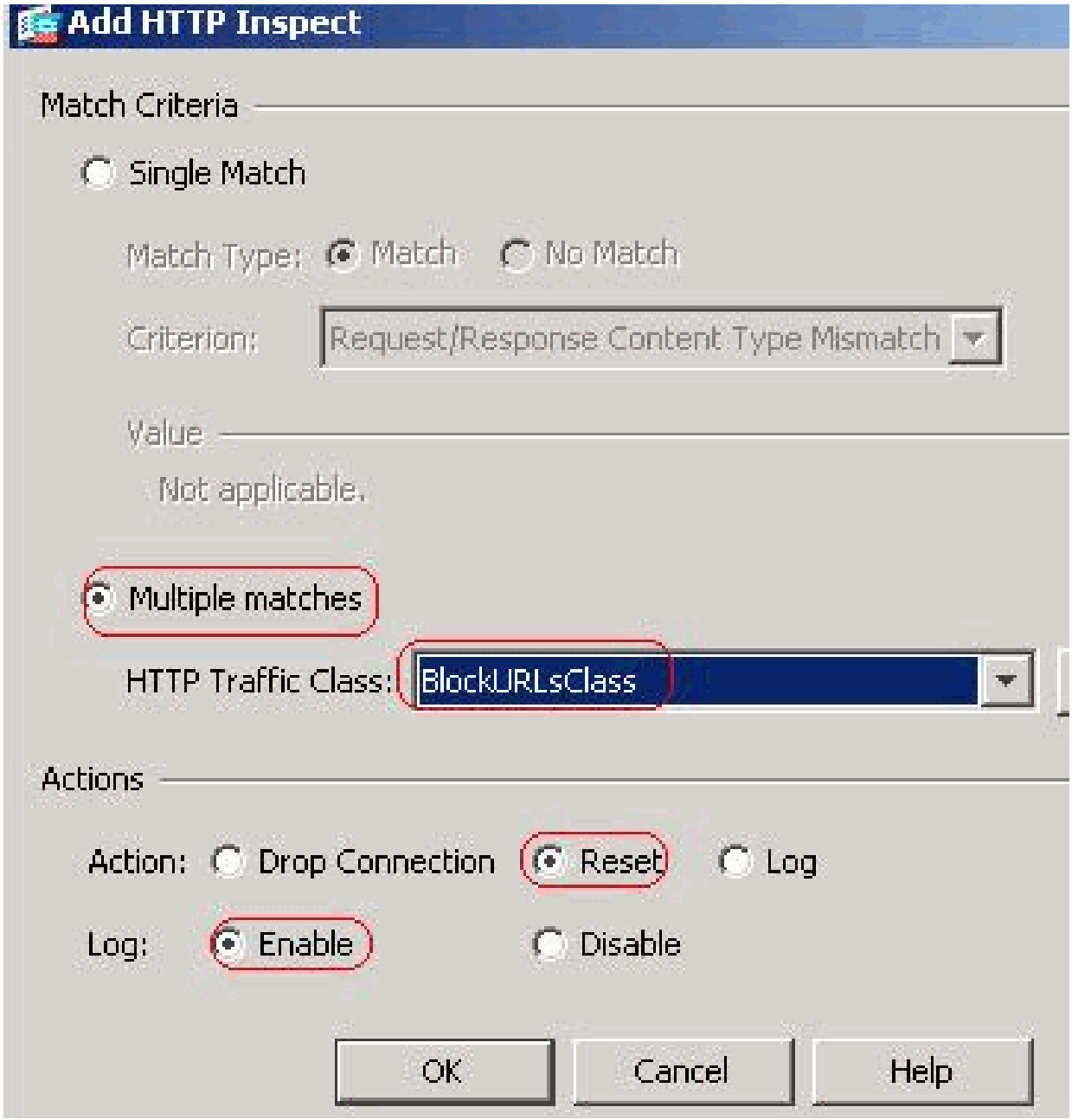
Fare clic su OK.

d. Impostare l'azione come Reset e Enable per la classe BlockDomainsClass.



Fare clic su OK.

e. Impostare l'azione su Reset e Enable per la classe BlockURLsClass.



Fare clic su OK.

Fare clic su Apply (Applica).

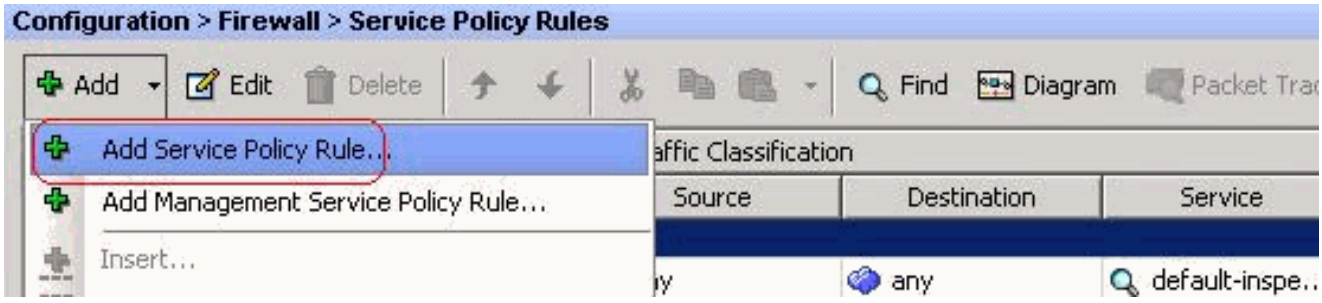
Configurazione CLI equivalente

Configurazione ASA CLI
<#root> ciscoasa# **configure terminal** ciscoasa(config)# **policy-map type inspect http http_inspection_policy**

```
ciscoasa(config-pmap)#
parameters
ciscoasa(config-pmap-p)#
match request method connect
ciscoasa(config-pmap-c)#
drop-connection log
ciscoasa(config-pmap-c)#
class AppHeaderClass
ciscoasa(config-pmap-c)#
drop-connection log
ciscoasa(config-pmap-c)#
class BlockDomainsClass
ciscoasa(config-pmap-c)#
reset log
ciscoasa(config-pmap-c)#
class BlockURLsClass
ciscoasa(config-pmap-c)#
reset log
ciscoasa(config-pmap-c)#
exit
ciscoasa(config-pmap)#
exit
```

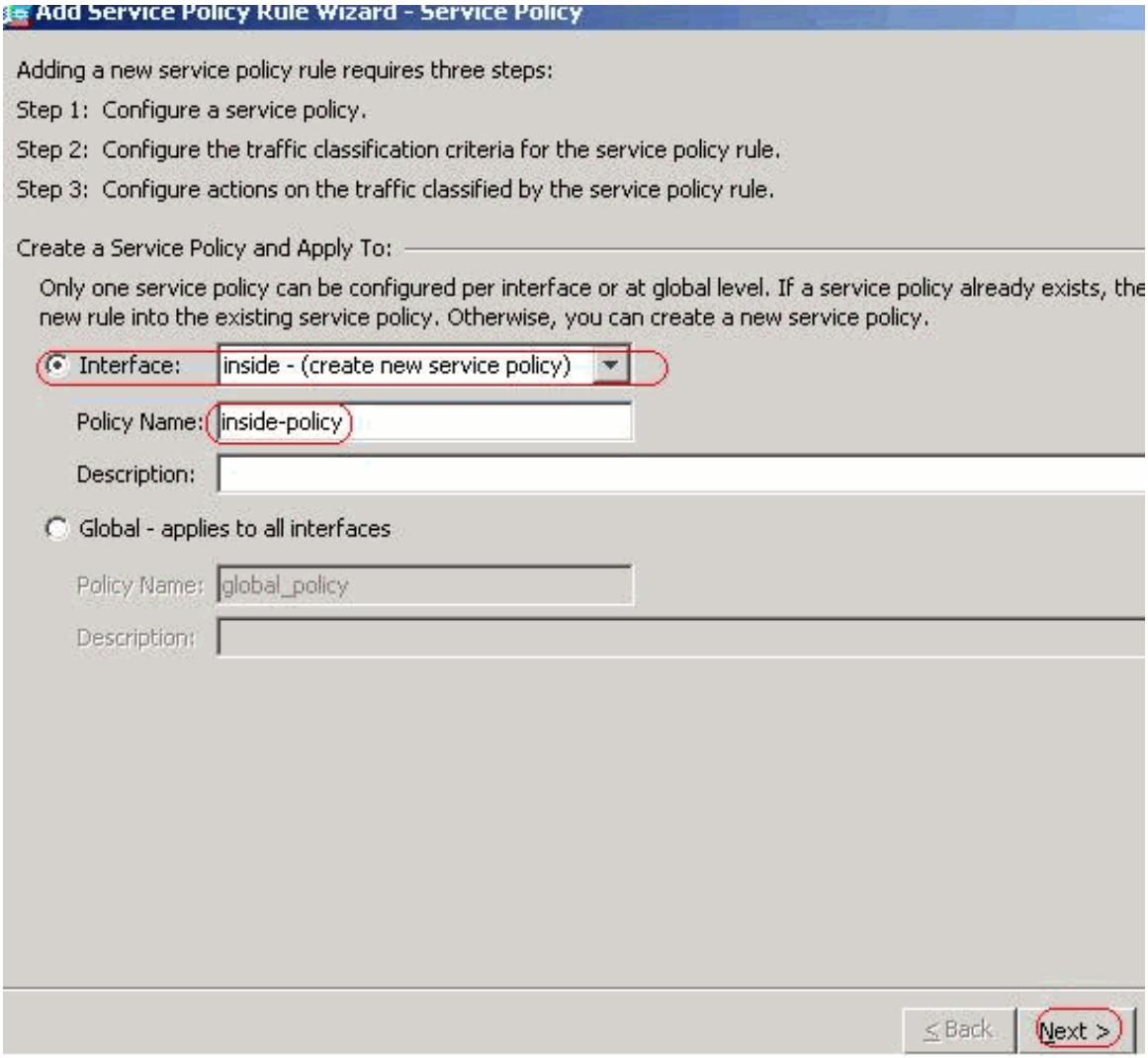
5. Applica il criterio http di ispezione all'interfaccia

   Scegliere Configurazione > Firewall > Regole dei criteri di servizio > Aggiungi > Aggiungi regola dei criteri di servizio.

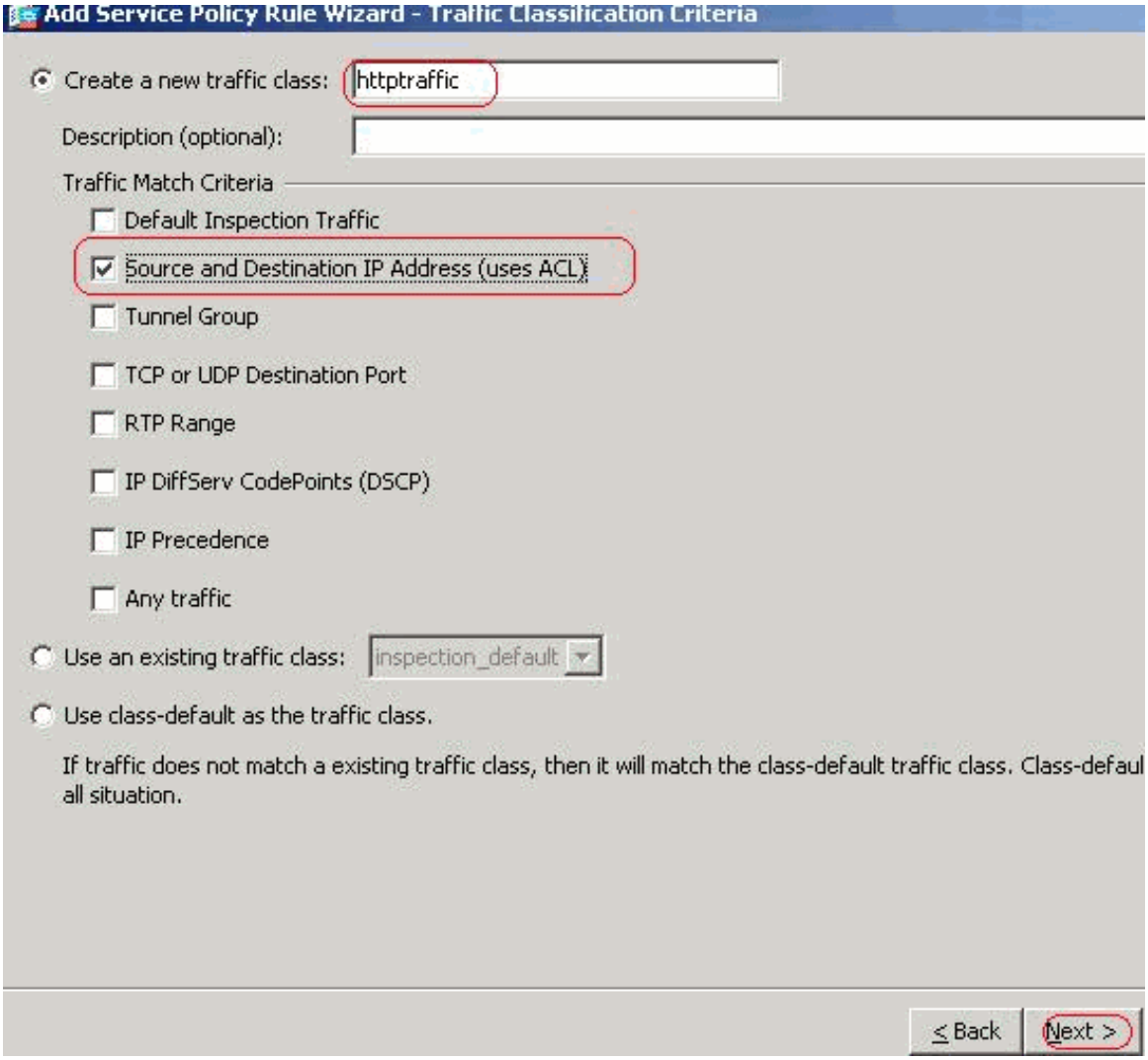


   a. Traffico HTTP

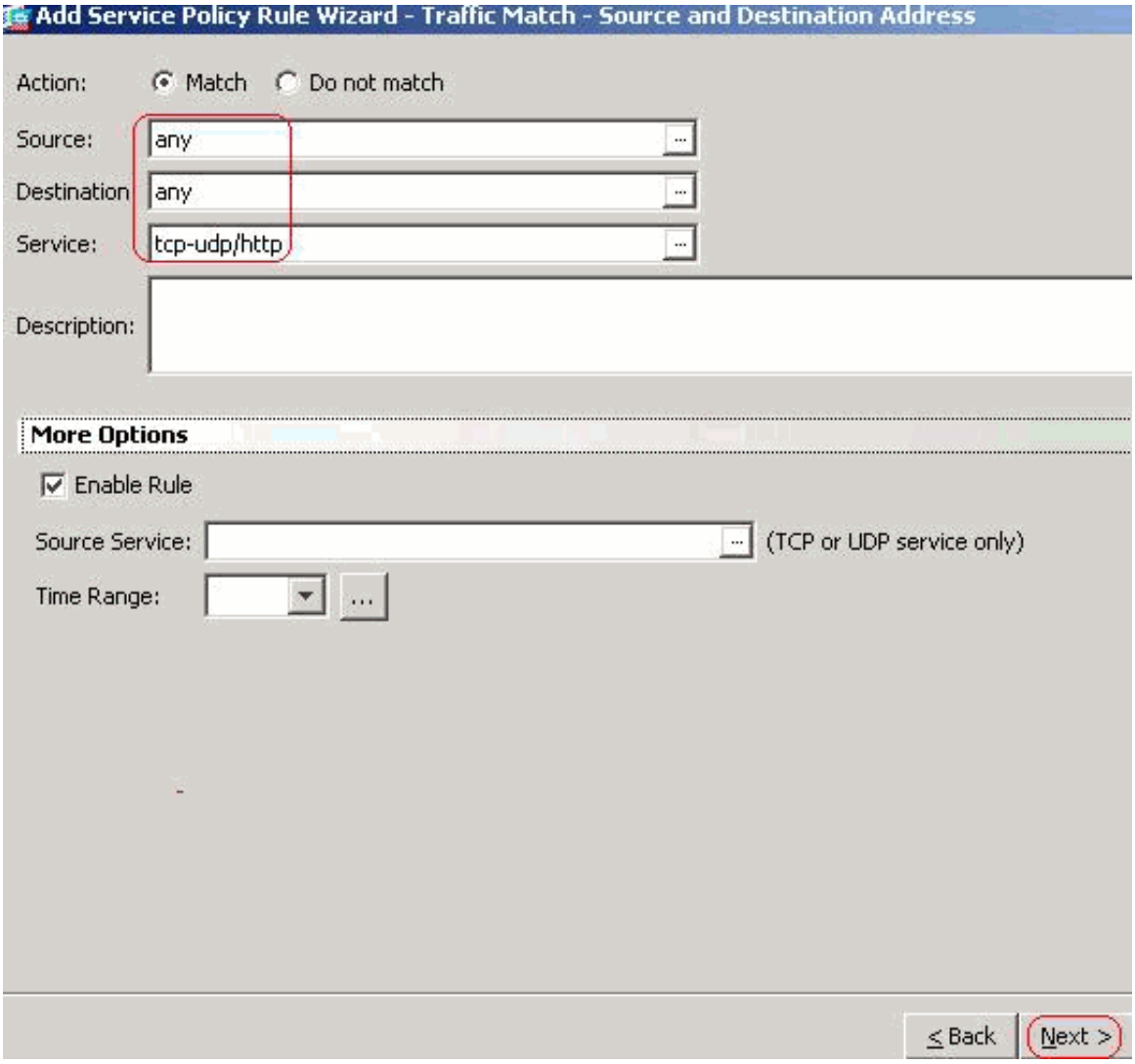
a. Scegliere il pulsante di opzione Interfaccia con interfaccia interna dal menu a discesa e Nome criterio come criterio interno. Fare clic su Next (Avanti).



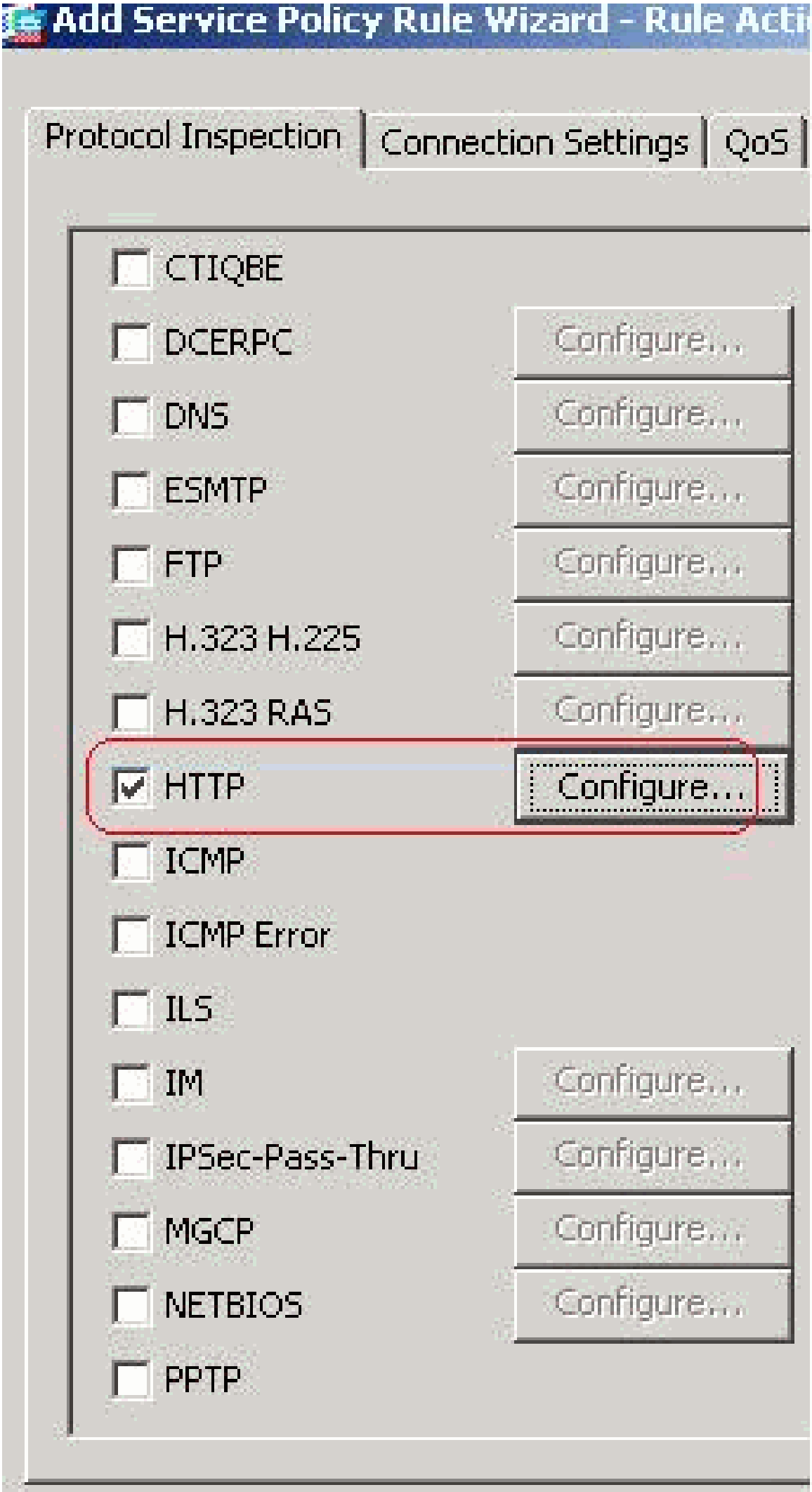
b. Creare una mappa di classe per il traffico http e controllare l'indirizzo IP di origine e di destinazione (utilizza l'ACL). Fare clic su Next (Avanti).



c. Scegliere Origine e Destinazione come qualsiasi con servizio come tcp-udp/http. Fare clic su Next (Avanti).



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


Add Service Policy Rule Wizard - Rule Acti
Protocol Inspection
Connection Settings
QoS
CTIQBE
DCERPC
DNS
ESMTP
FTP
H.323 H.225
H.323 RAS
HTTP
ICMP
ICMP Error
ILS
IM
IPSec-Pass-Thru
MGCP
NETBIOS
PPTP
Configure...
Configure...
Configure...
Configure...
Configure...
Configure...
Configure...
Configure...
Configure...
Configure...
Configure...

```
<#root>
ciscoasa#
configure terminal
ciscoasa(config)#
access-list inside_mpc extended permit tcp any any eq www

ciscoasa(config)#
access-list inside_mpc extended permit tcp any any eq 8080
ciscoasa(config)#
class-map httptraffic
ciscoasa(config-cmap)#
match access-list inside_mpc
ciscoasa(config-cmap)#
exit
ciscoasa(config)#
policy-map inside-policy
ciscoasa(config-pmap)#
class httptraffic
ciscoasa(config-pmap-c)#
inspect http http_inspection_policy
ciscoasa(config-pmap-c)#
exit
ciscoasa(config-pmap)#
exit
ciscoasa(config)#
service-policy inside-policy interface inside
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

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

- show running-config regex: visualizza le espressioni regolari configurate.

<#root>

```
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

<#root>

```
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

<#root>

```
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 relativa configurazione predefinita.

<#root>

```
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.

```
<#root>

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.

```
<#root>

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

In questa sezione vengono fornite informazioni utili per risolvere i problemi di 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

- Cisco ASA serie 5500 Adaptive Security Appliance Support
- Supporto Cisco Adaptive Security Device Manager (ASDM)
- Cisco PIX serie 500 Security Appliance Support
- Software Cisco PIX Firewall

- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).