ASA 8.3 e versioni successive: Impostazione del timeout della connessione SSH/Telnet/HTTP con l'esempio di configurazione MPF

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per Cisco Adaptive Security Appliance (ASA) con versione 8.3(1) e successive con un timeout specifico di una particolare applicazione, ad esempio SSH/Telnet/HTTP, rispetto a una configurazione applicabile a tutte le applicazioni. In questo esempio di configurazione viene utilizzato il Modular Policy Framework (MPF) introdotto in Cisco Adaptive Security Appliance (ASA) versione 7.0. Per ulteriori informazioni, vedere Utilizzo del Modular Policy Framework.

In questa configurazione di esempio, Cisco ASA è configurato in modo da consentire alla workstation (10.77.241.129) di connettersi al server remoto (10.1.1.1) dietro il router in modalità Telnet/SSH/HTTP. È inoltre configurato un timeout di connessione separato per il traffico Telnet/SSH/HTTP. A tutto il resto del traffico TCP continua a essere associato un valore di timeout della connessione normale con valore **conn 1:00:00**.

Fare riferimento a PIX/ASA 7.x e versioni successive/FWSM: Impostare il timeout della connessione SSH/Telnet/HTTP utilizzando l'esempio di configurazione MPF per la stessa configurazione sull'appliance Cisco ASA con le versioni 8.2 e precedenti.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco ASA Security Appliance versione 8.3(1) con Adaptive Security Device Manager (ASDM) 6.3.

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.

Convenzioni

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

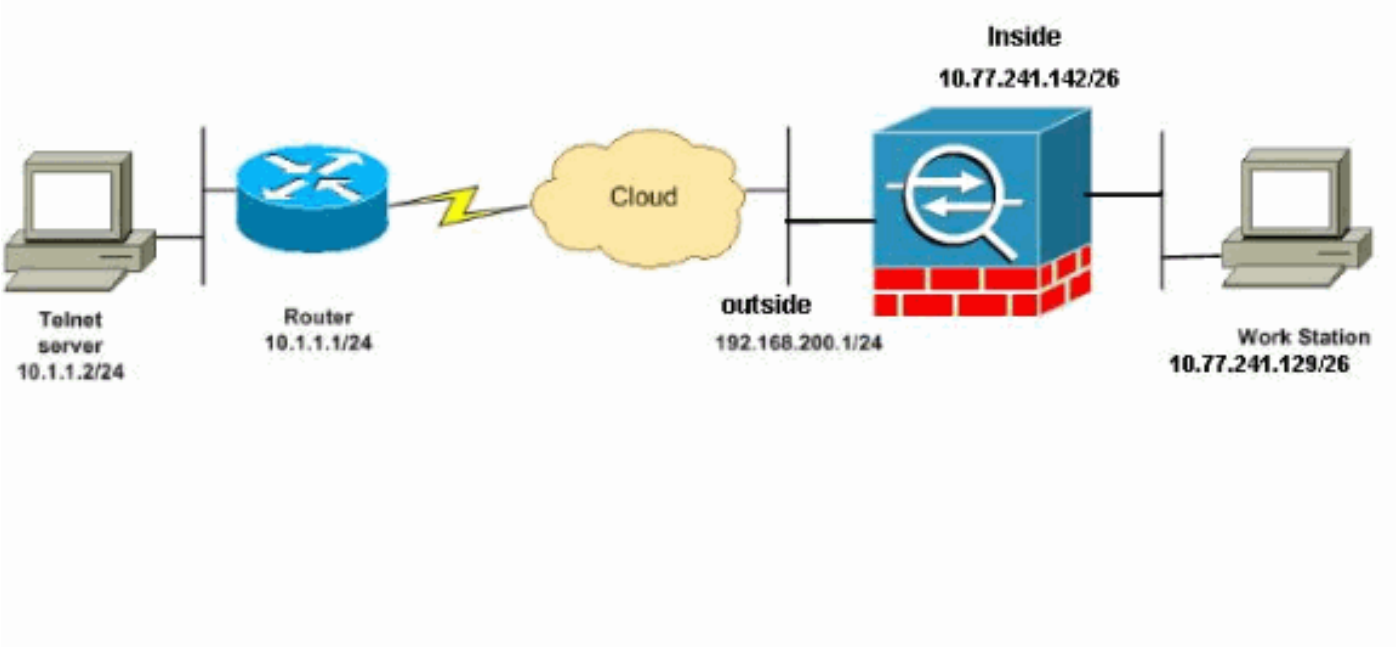
Configurazione

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:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Configurazioni

Nel documento vengono usate queste configurazioni:

- Configurazione CLI
- Configurazione ASDM

Nota: queste configurazioni CLI e ASDM sono applicabili al modulo FWSM (Firewall Service Module).

Configurazione CLI

Configurazione ASA 8.3(1)

```
ASA Version 8.3(1)
!
hostname ASA
domain-name nantes-port.fr
enable password S39lgaewi/JM5WyY level 3 encrypted
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 1mZfSd48bl0UdPgP encrypted
no names

dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
ip address 10.77.241.142 255.255.255.0


boot system disk0:/asa831-k8.bin
ftp mode passive
dns domain-lookup outside

!--- Creates an object called DM_INLINE_TCP_1. This
defines the traffic !--- that has to be matched in the
class map. object-group service DM_INLINE_TCP_1 tcp
 port-object eq www
 port-object eq ssh
 port-object eq telnet

access-list outside_mpc extended permit tcp host
10.77.241.129 any object-group DM_INLINE_TCP_1


pager lines 24
mtu inside 1500
mtu outside 1500
no failover
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
access-group 101 in interface outside

route outside 0.0.0.0 0.0.0.0 192.168.200.2 1
timeout xlate 3:00:00
```

```
!--- The default connection timeout value of one hour is
applicable to !--- all other TCP applications. 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
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!

!--- Define the class map Cisco-class in order !--- to
classify Telnet/ssh/http traffic when you use Modular
Policy Framework !--- to configure a security feature.
!--- Assign the parameters to be matched by class map.


class-map Cisco-class
 match access-list outside_mpc

class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  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

!--- Use the pre-defined class map Cisco-class in the
policy map.


policy-map Cisco-policy

!--- Set the connection timeout under the class mode
where !--- the idle TCP (Telnet/ssh/http) connection is
disconnected. !--- There is a set value of ten minutes
in this example. !--- The minimum possible value is five
minutes. class Cisco-class
  set connection timeout idle 0:10:00 reset
!
!
service-policy global_policy global
```

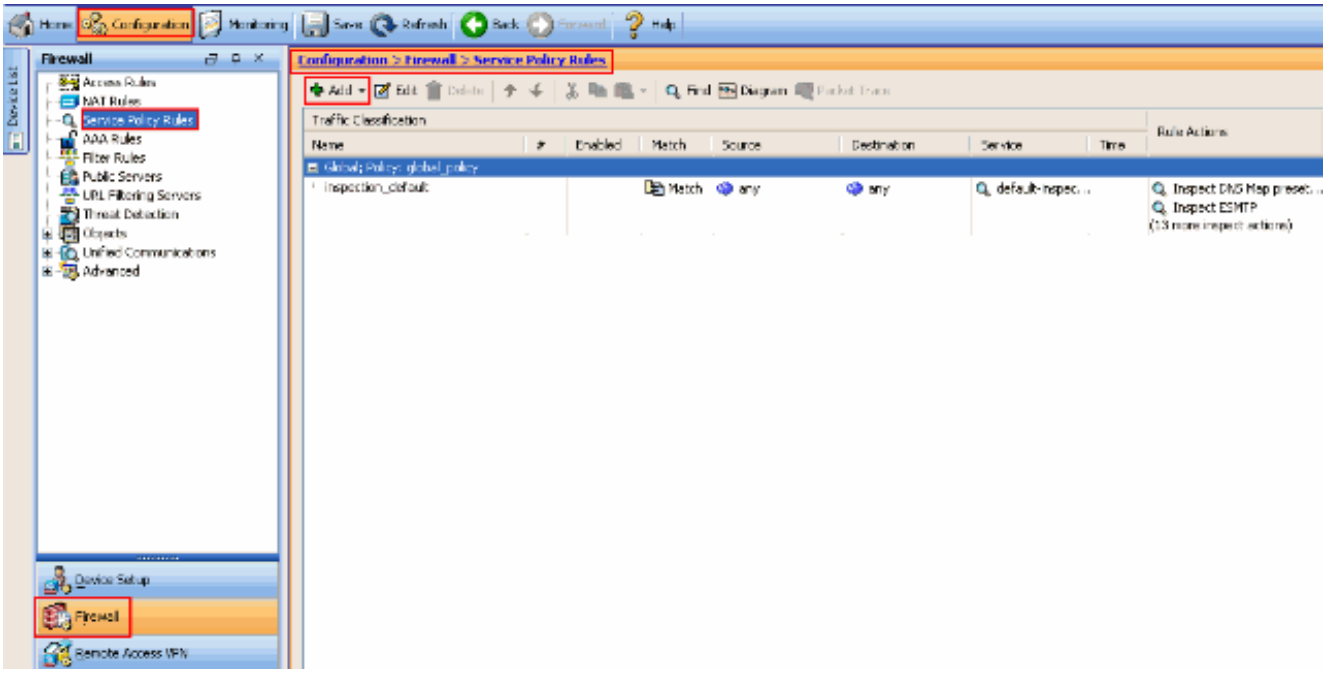
```
!--- Apply the policy-map Cisco-policy on the interface.
!--- You can apply the service-policy command to any
interface that !--- can be defined by the nameif
command.

service-policy Cisco-policy interface outside
end
```

Configurazione ASDM

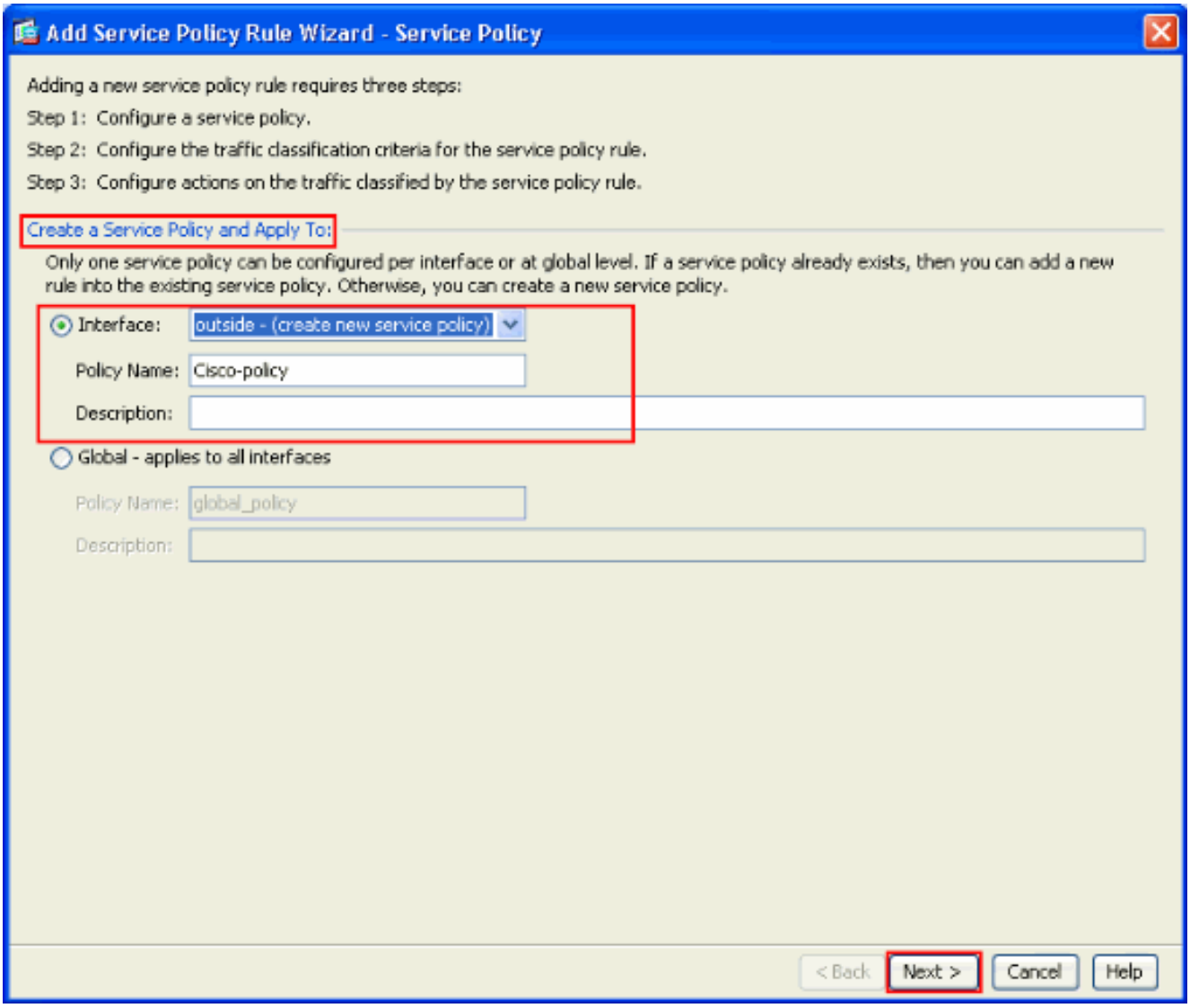
Completare questa procedura per impostare il timeout della connessione TCP per il traffico Telnet, SSH e HTTP tramite ASDM, come mostrato.

Nota: per accedere a PIX/ASA tramite ASDM, consultare le impostazioni di base di Consenti accesso HTTPS per ASDM.

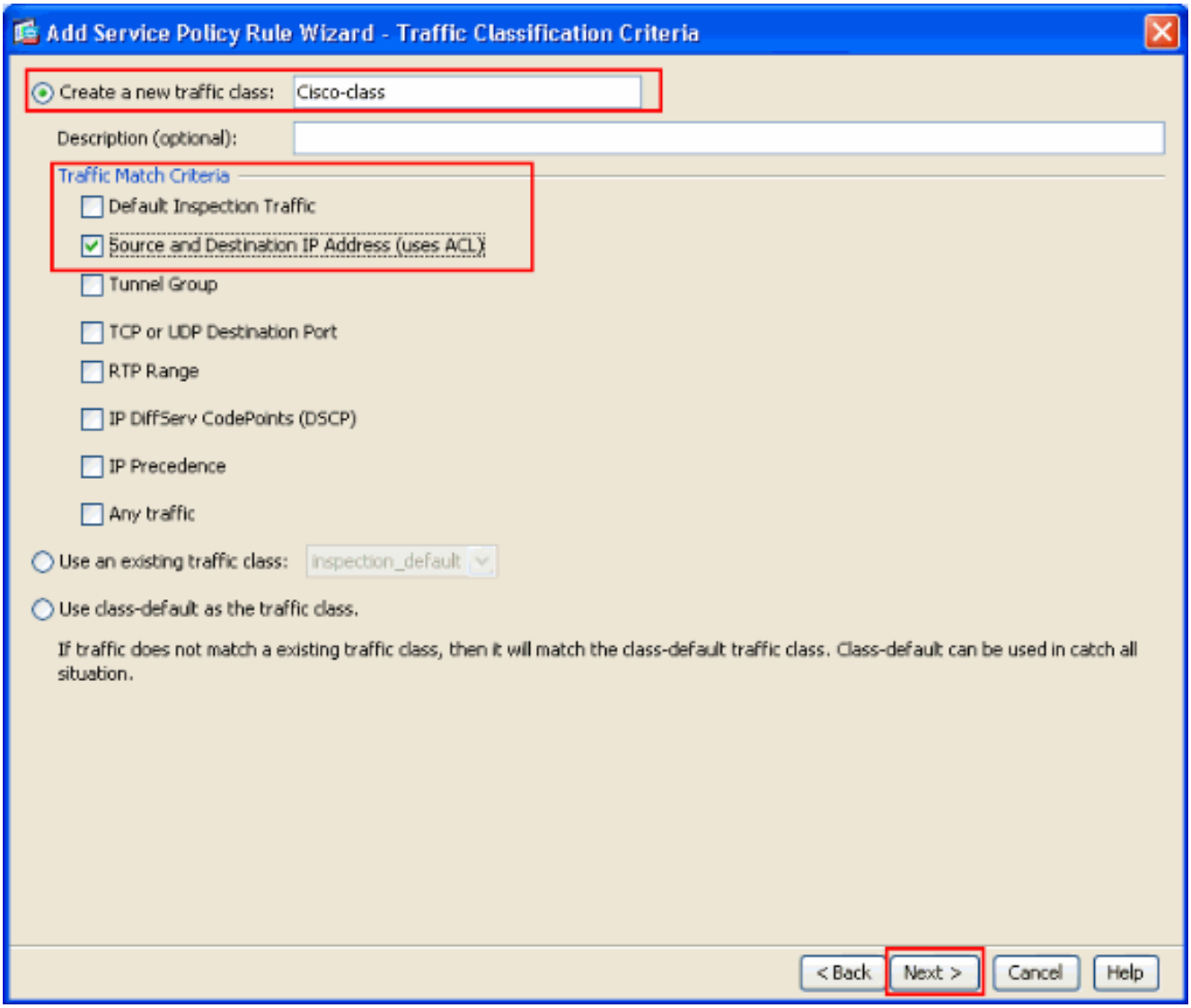
1. Scegliere **Configurazione > Firewall > Regole criteri di servizio** e fare clic su **Aggiungi** per configurare la regola dei criteri di servizio come mostrato.



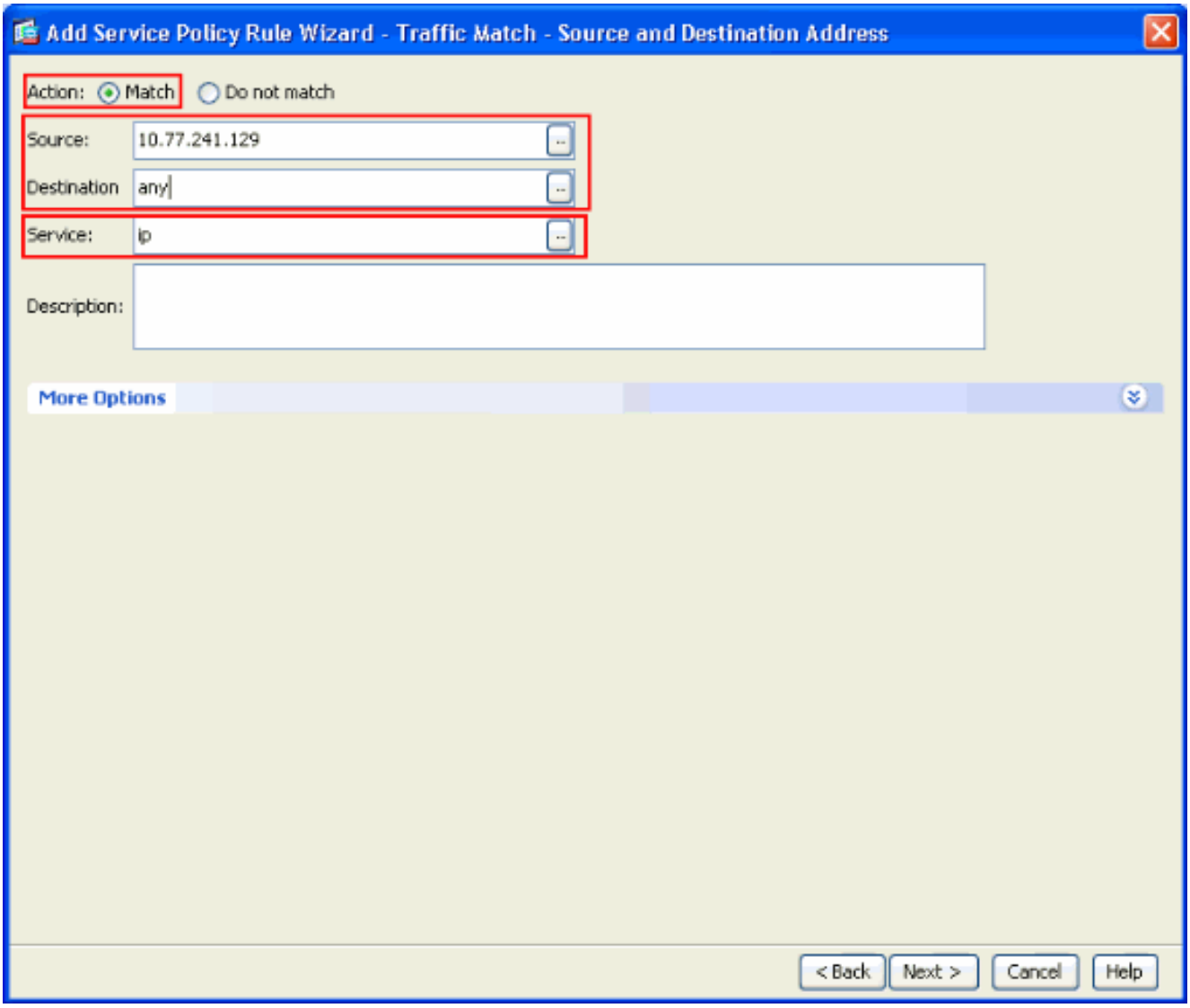
2. Nella sezione **Creazione guidata regole dei criteri del servizio -** Criteri del servizio scegliere il pulsante di opzione accanto a **Interfaccia** nella finestra **Crea criteri del servizio e applica a**. Selezionare l'interfaccia desiderata dall'elenco a discesa e specificare il **nome** del **criterio**. Il nome del criterio utilizzato in questo esempio è **Cisco-policy**. Fare quindi clic su **Avanti**.



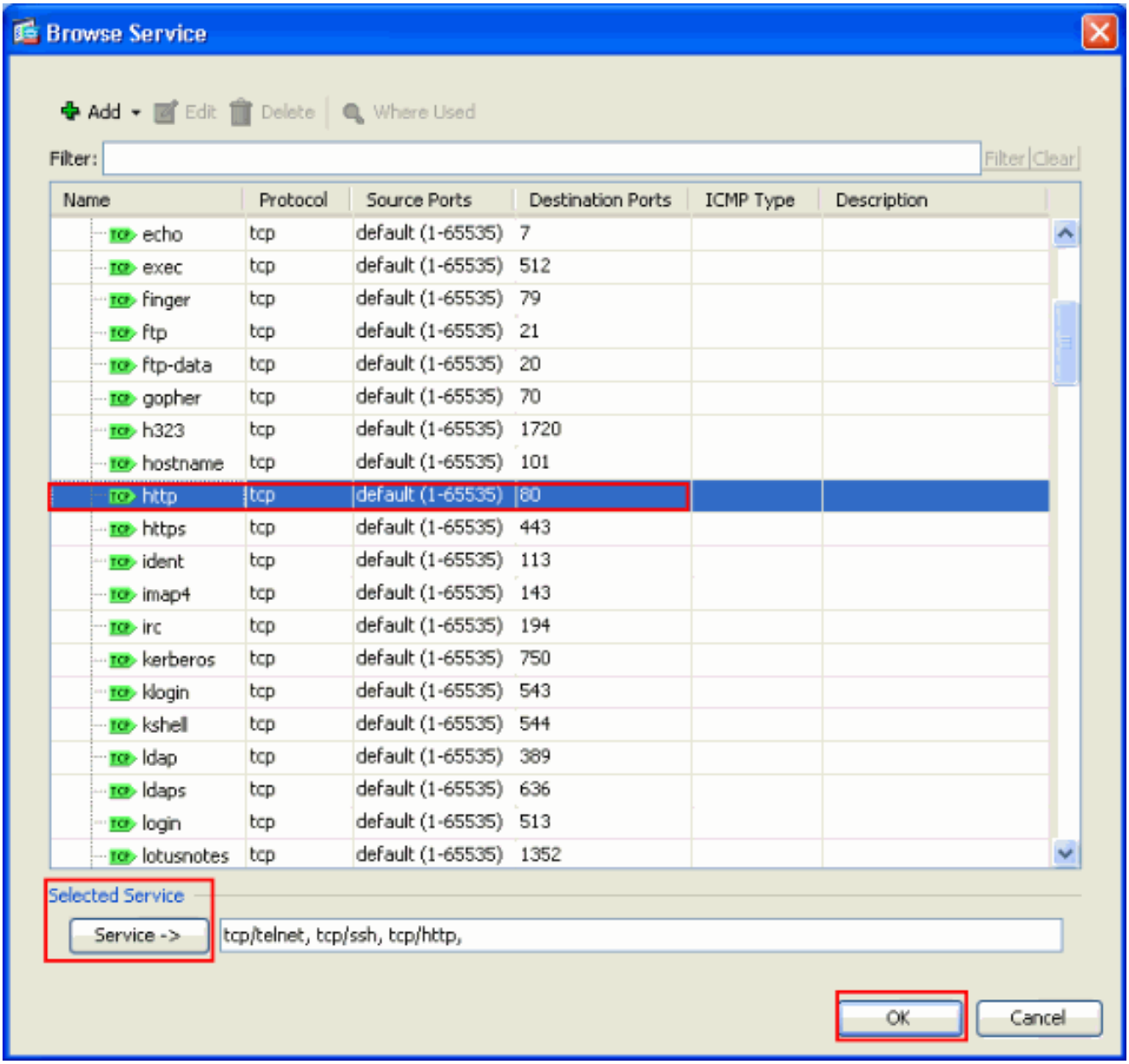
3. Creare una mappa delle classi con il nome **Cisco-class** e selezionare la casella di controllo **Source and Destination IP address (uses ACL)** in Traffic Match Criteria (Criteri di corrispondenza traffico). Fare quindi clic su **Avanti**.



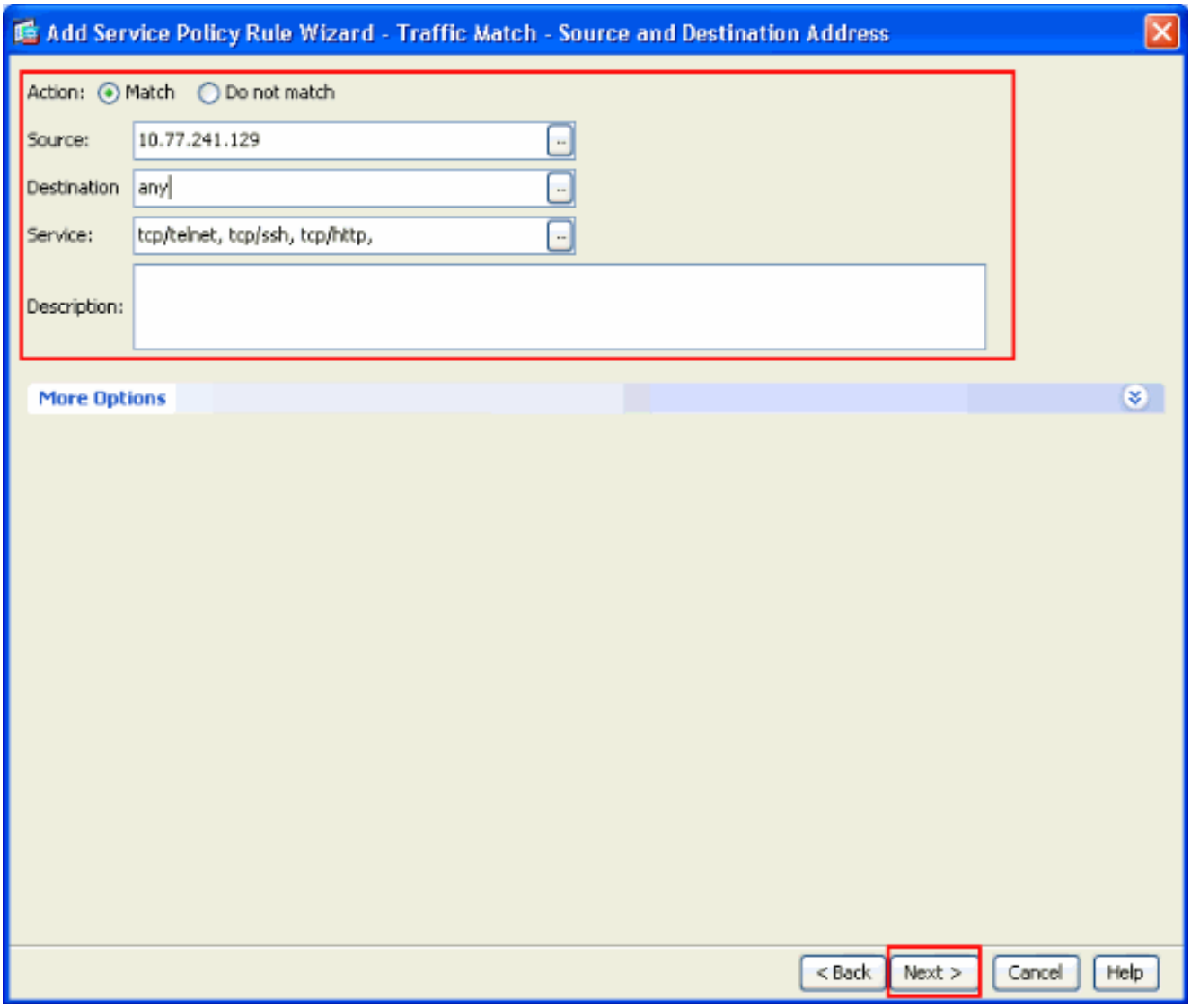
4. Nella finestra **Aggiunta guidata regola dei criteri del servizio - Corrispondenza traffico - Indirizzo di origine e di destinazione**, scegliere il pulsante di opzione accanto a **Corrispondenza** e quindi fornire l'indirizzo di origine e di destinazione come mostrato. Fare clic sul pulsante a discesa accanto a **Servizio** per scegliere i servizi richiesti.



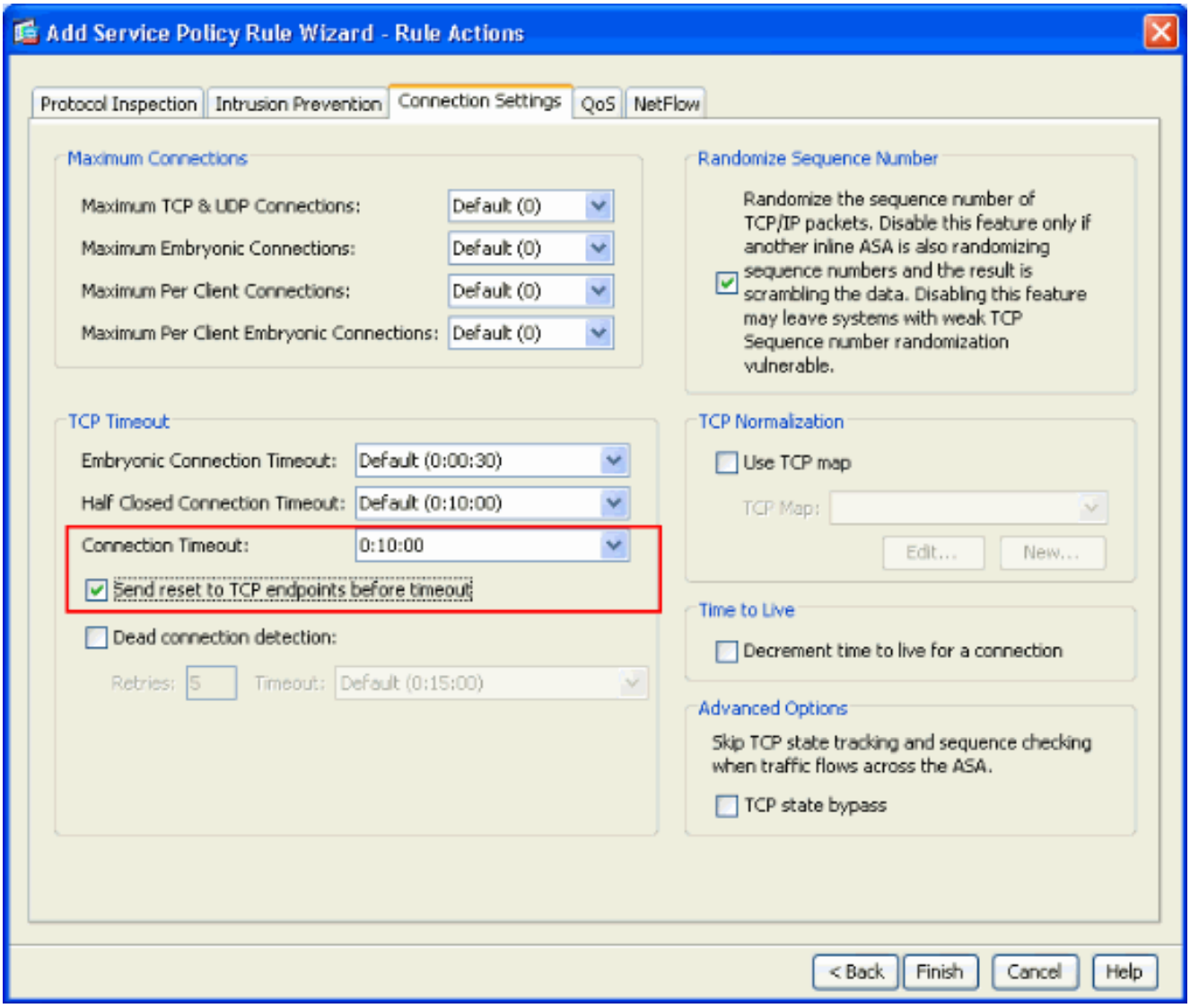
5. Selezionare i servizi richiesti, ad esempio **telnet**, **ssh** e **http**. Quindi fare clic su **OK**.



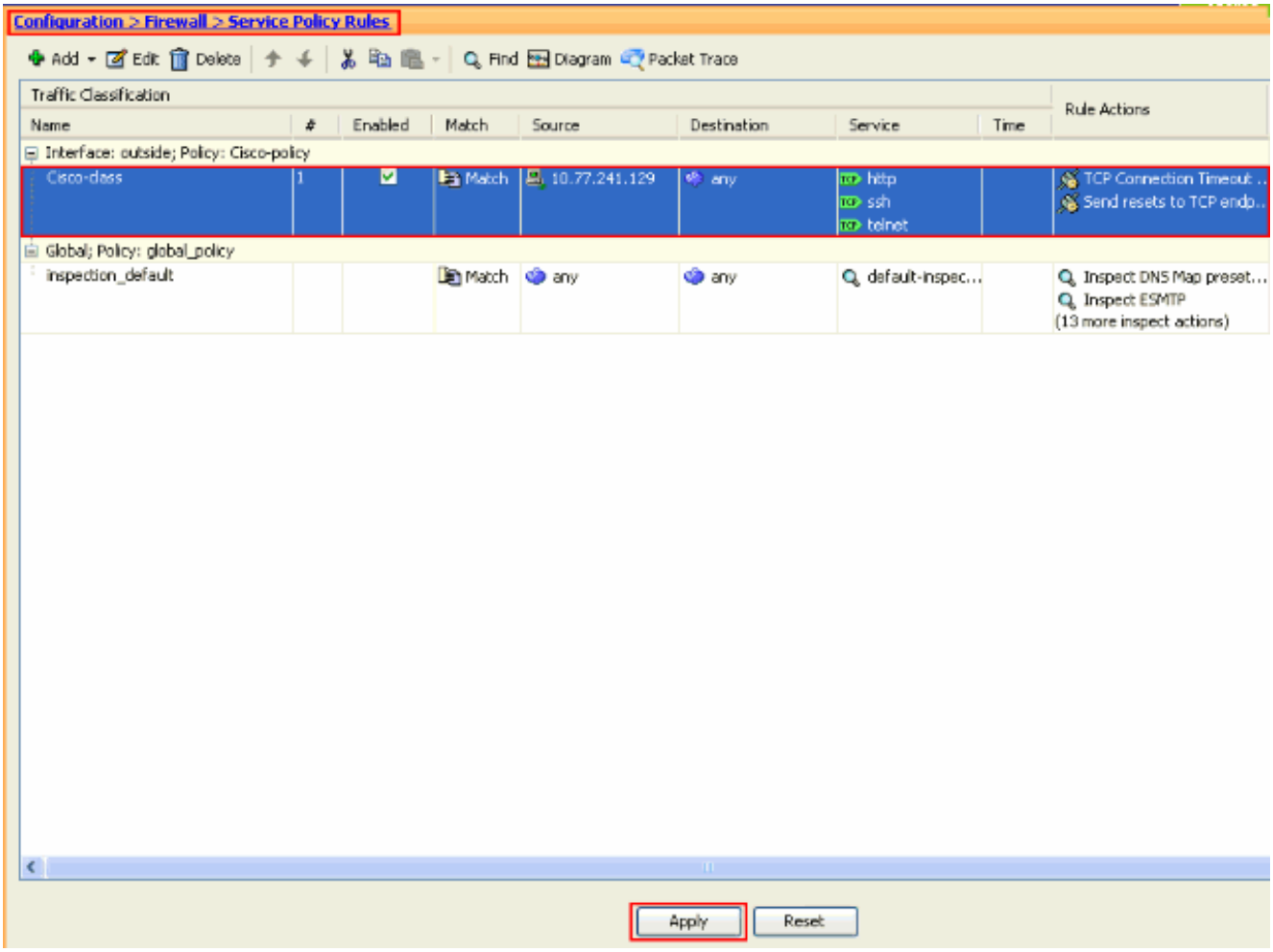
6. **Configurare i timeout**. Fare clic su **Next** (Avanti).



7. Scegliere **Impostazioni connessione** per impostare il timeout della connessione TCP su 10 minuti. Inoltre, selezionare la casella di controllo **Invia ripristino agli endpoint TCP prima del timeout**. Fare clic su **Finish**
(Fine).



8. Per applicare la configurazione all'appliance di sicurezza, fare clic su **Apply** (Applica).La configurazione è stata
completata.



Timeout Ebraico

Una connessione embrionale è la connessione semichiusa o, ad esempio, l'handshake a tre vie non è stato completato. Il timeout è definito come SYN sull'appliance ASA. Per impostazione predefinita, il timeout SYN sull'appliance ASA è 30 secondi. Di seguito viene riportata la procedura per configurare il timeout embrio:

```
access-list emb_map extended permit tcp any any

class-map emb_map
match access-list emb_map

policy-map global_policy
class emb_map
set connection timeout embryonic 0:02:00

service-policy global_policy global
```

Risoluzione dei problemi

Se il timeout della connessione non funziona con MPF, controllare la connessione TCP di avvio. Il problema può essere un'inversione dell'indirizzo IP di origine e di destinazione oppure un indirizzo IP non configurato correttamente nell'elenco degli accessi non corrisponde nell'MPF per impostare il nuovo valore di timeout o per modificare il timeout predefinito per l'applicazione. Creare una voce dell'elenco degli accessi (origine e destinazione) in base all'avvio della connessione per impostare il timeout della connessione con MPF.

Informazioni correlate

- Cisco Adaptive Security Device Manager
- Cisco ASA serie 5500 Adaptive Security Appliance
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems