PIX/ASA 7.x e versioni successive/FWSM: Impostazione del timeout della connessione SSH/Telnet/HTTP con l'esempio di configurazione MPF

Sommario

Introduzione

Questo documento offre una configurazione di esempio per PIX 7.1(1) e versioni successive di un timeout specifico per una particolare applicazione come SSH/Telnet/HTTP, a differenza di uno che si applica a tutte le applicazioni. In questo esempio di configurazione viene utilizzata la nuova struttura dei criteri modulare introdotta in PIX 7.0. Per ulteriori informazioni, vedere Utilizzo della struttura dei criteri modulare.

In questa configurazione di esempio, il firewall PIX 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 alla versione ASA 8.3 e successive: Per ulteriori informazioni sulla configurazione identica usando ASDM con Cisco Adaptive Security Appliance (ASA) versione 8.3 e successive, impostare il timeout della connessione SSH/Telnet/HTTP con l'esempio di configurazione MPF.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco PIX/ASA Security Appliance versione 7.1(1) con Adaptive Security Device Manager (ASDM) 5.1.

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.

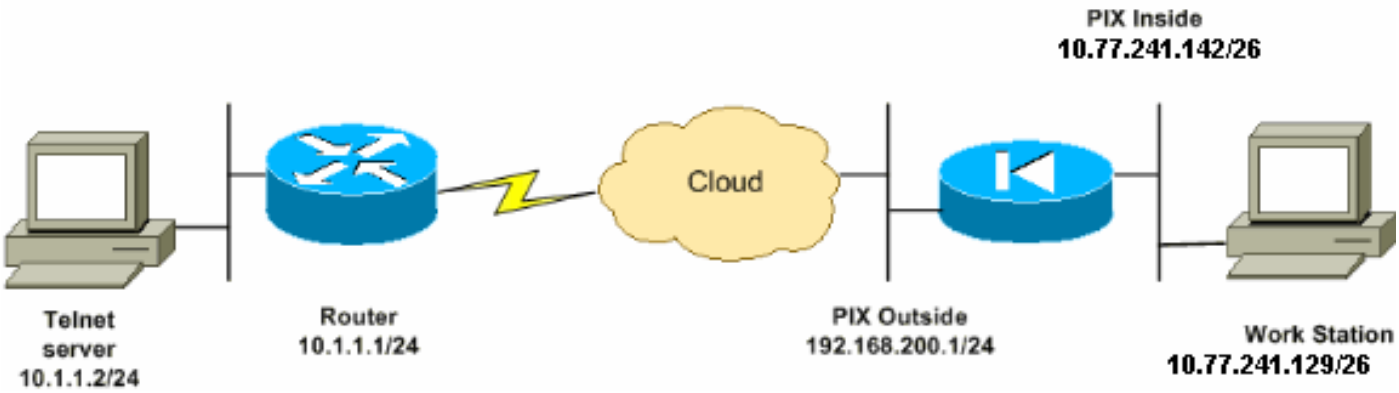
Configurazione

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.

Configurazione

Nel documento viene usata questa configurazione:

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

Configurazione CLI:

Configurazione PIX

```
PIX Version - 7.1(1)
!
hostname PIX
domain-name Cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!


access-list inside_nat0_outbound extended permit ip
10.77.241.128 255.255.255.192 any

!--- Define the traffic that has to be matched in the
class map. !--- Telnet is defined in this example.
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq telnet
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq ssh
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq www
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq telnet
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq ssh
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq www

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
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 telnet 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 telnet
 description telnet
  match access-list outside_mpc_in

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 telnet in the policy
map.


policy-map telnet

!--- Set the connection timeout under the class mode in
which !--- 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 telnet
  set connection timeout tcp 00:10:00 reset
!
!
service-policy global_policy global

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

service-policy telnet interface outside
end
```

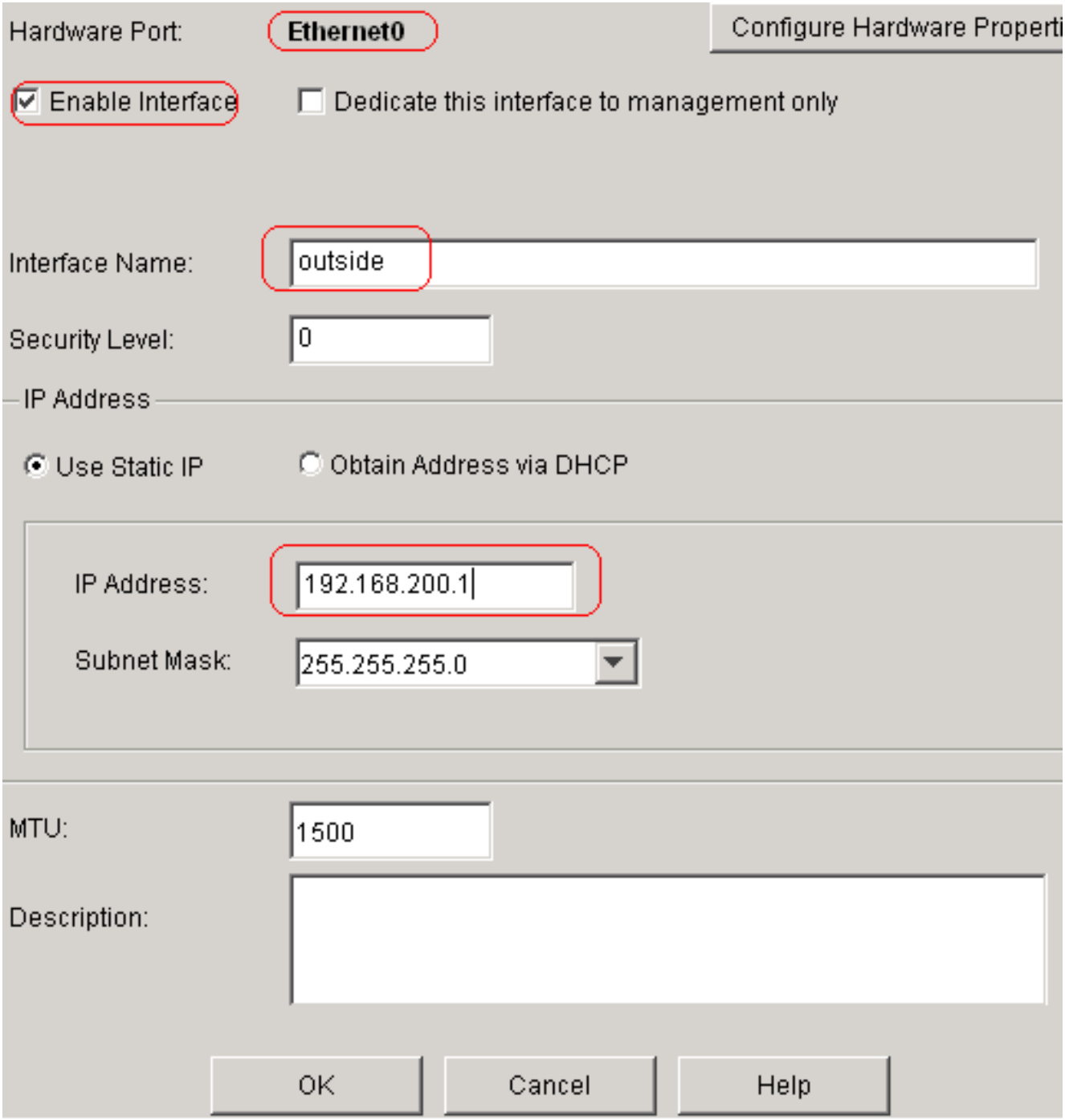
Configurazione ASDM:

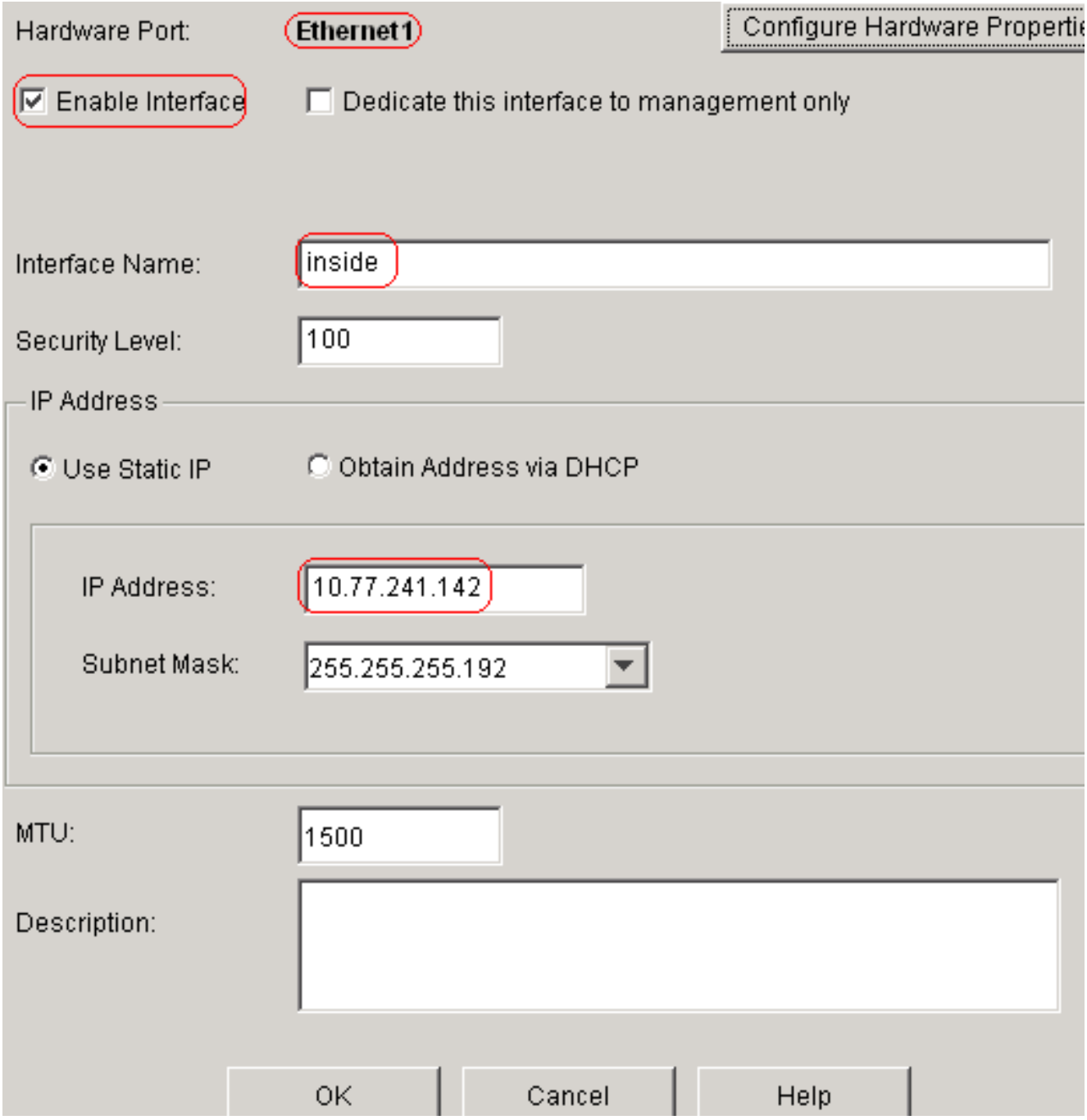
Completare questa procedura per impostare il timeout della connessione TCP per il traffico Telnet

basato sull'elenco degli accessi che utilizza ASDM, come mostrato.

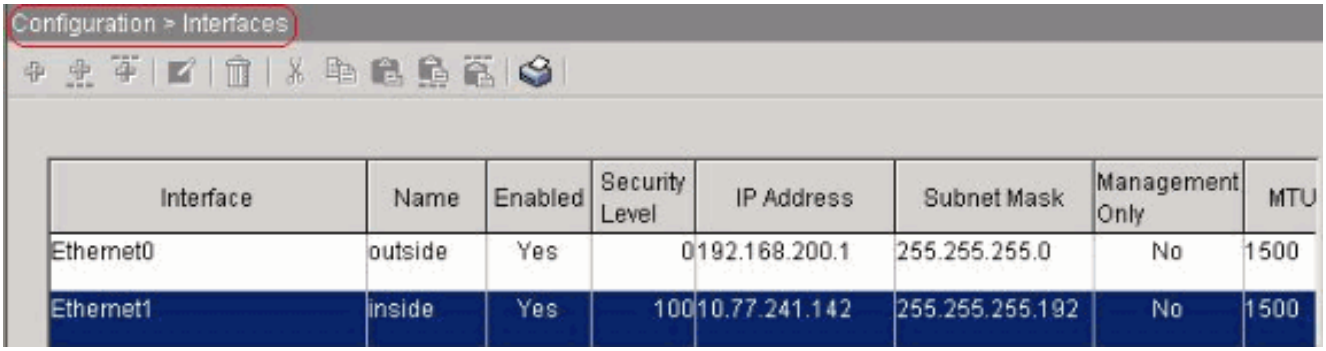
Nota: per accedere a PIX/ASA tramite ASDM, consultare le impostazioni di base di Consenti accesso HTTPS per ASDM.

1. **Configurazione interfacce**Scegliere **Configurazione > Interfacce > Aggiungi** per configurare le interfacce Ethernet0 (esterna) ed Ethernet1 (interna) come mostrato.





Fare clic su
OK.

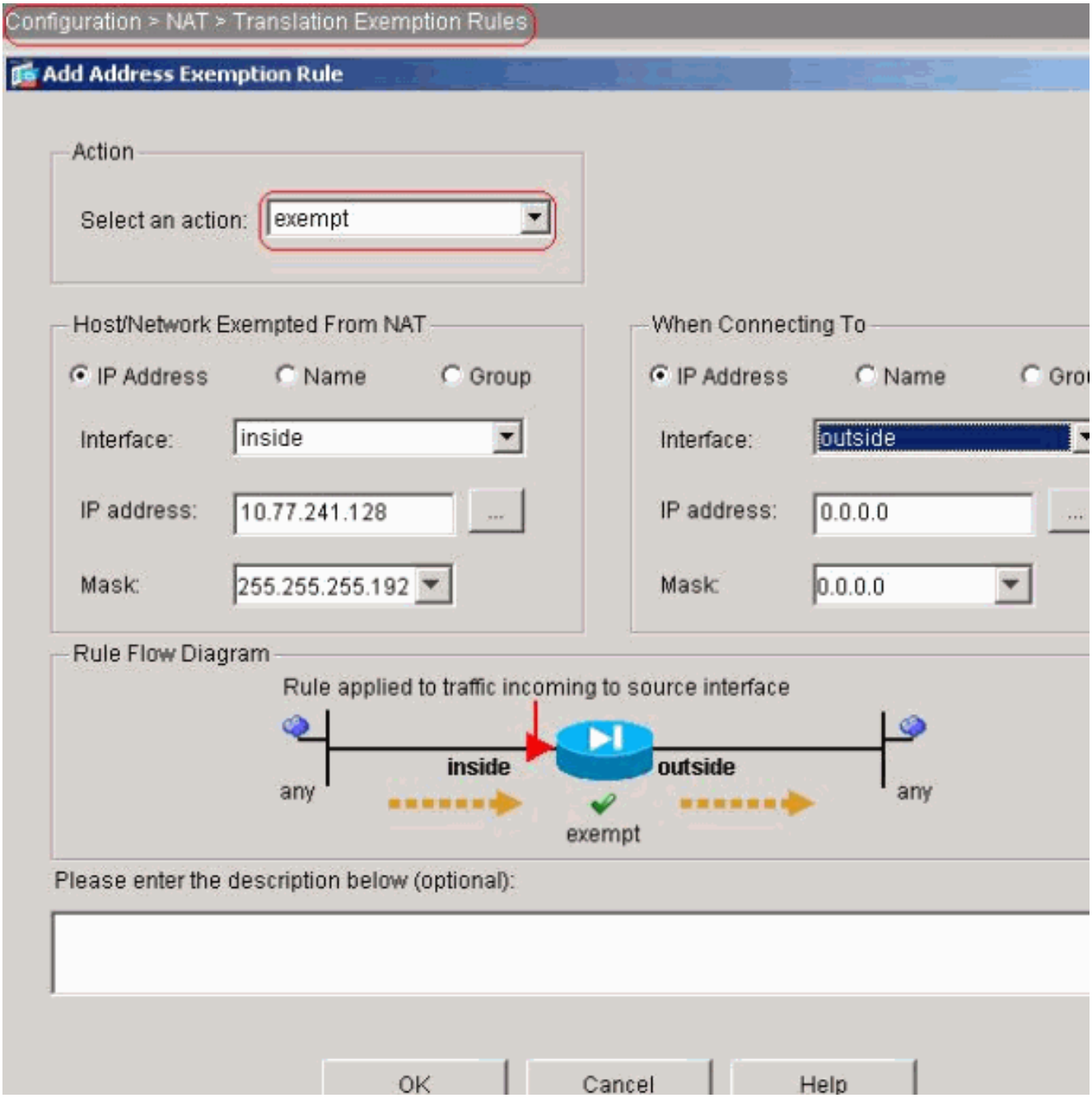


Configurazione CLI equivalente come mostrato:

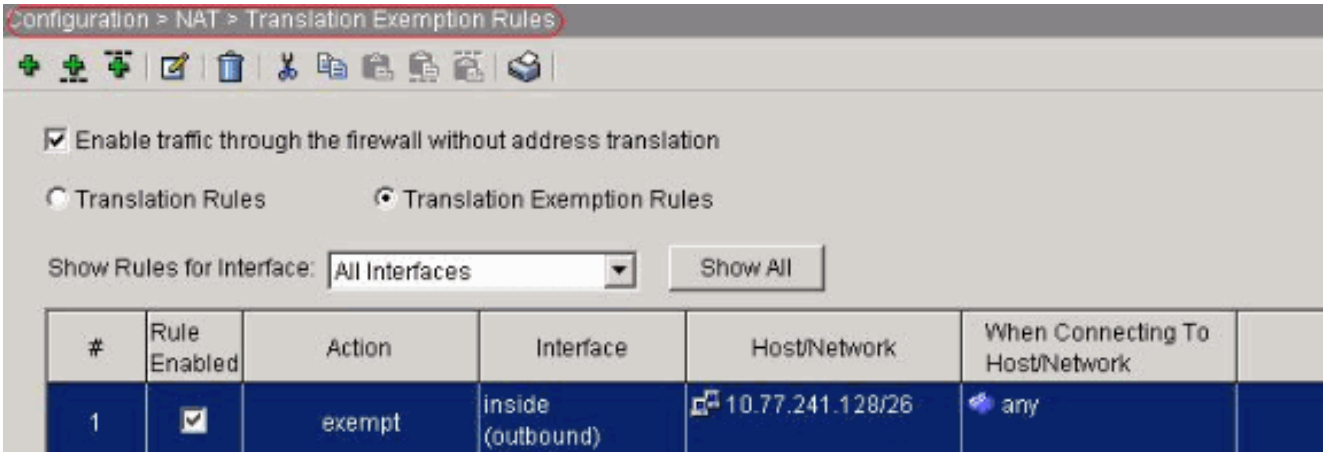
```
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
```

```
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
```

2. **Configura NAT 0**Scegliere **Configurazione > NAT > Regole di esenzione dalla traduzione > Aggiungi** per consentire al traffico proveniente dalla rete 10.77.241.128/26 di accedere a Internet senza alcuna traduzione.



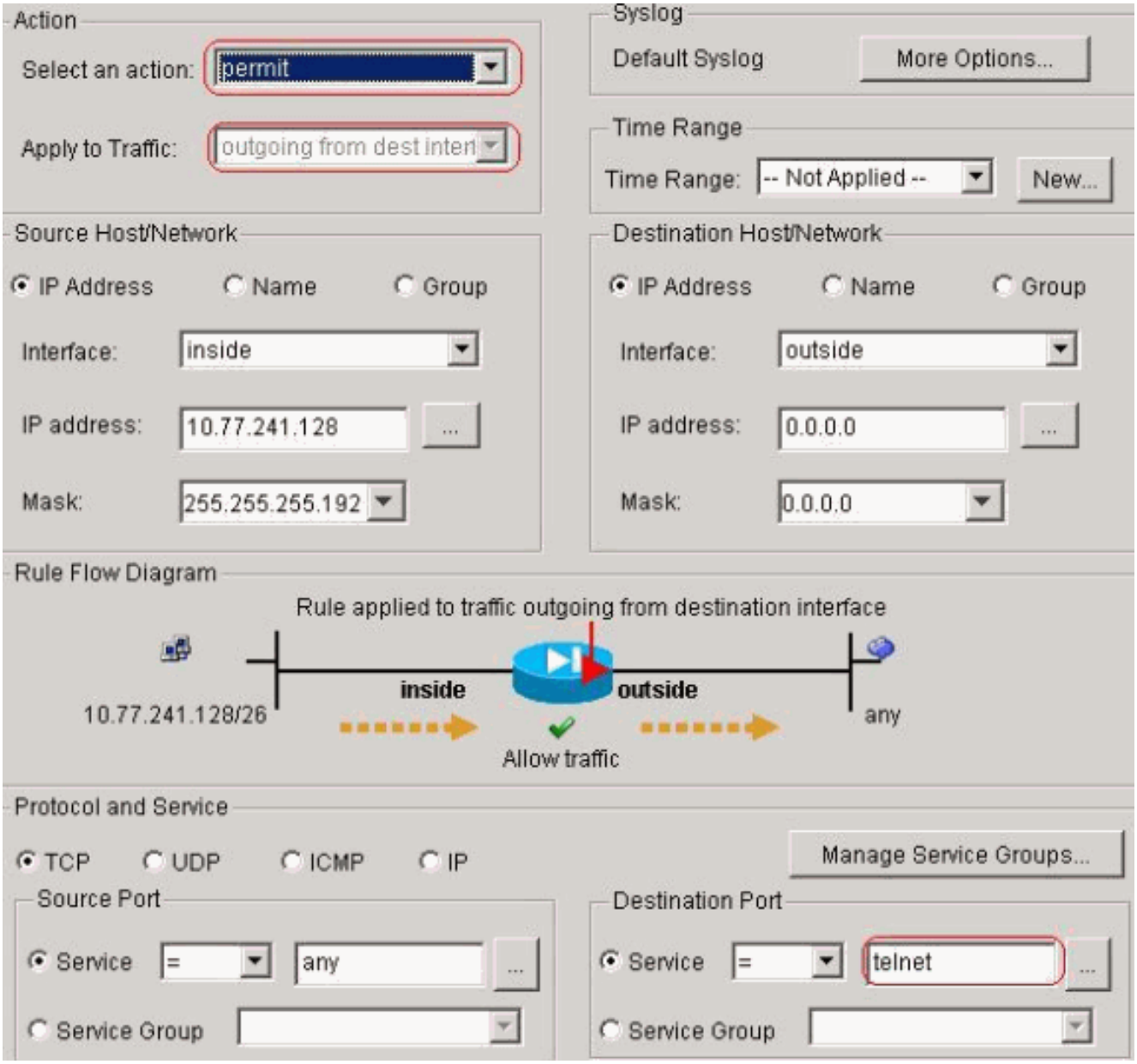
Fare clic su **OK**.



Configurazione CLI equivalente come mostrato:

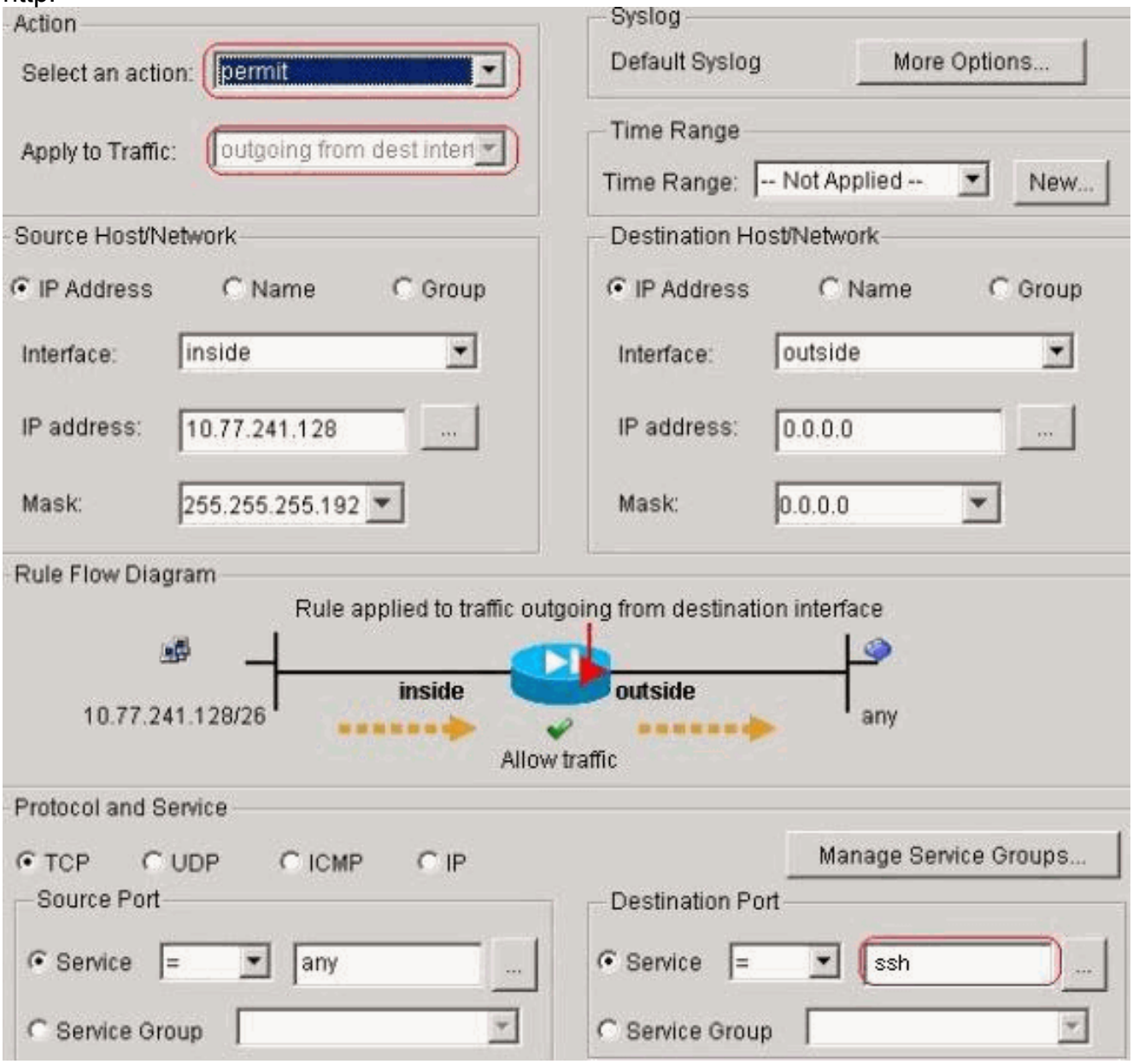
```
access-list inside_nat0_outbound extended permit ip 10.77.241.128 255.255.255.192 any
nat (inside) 0 access-list inside_nat0_outbound
```

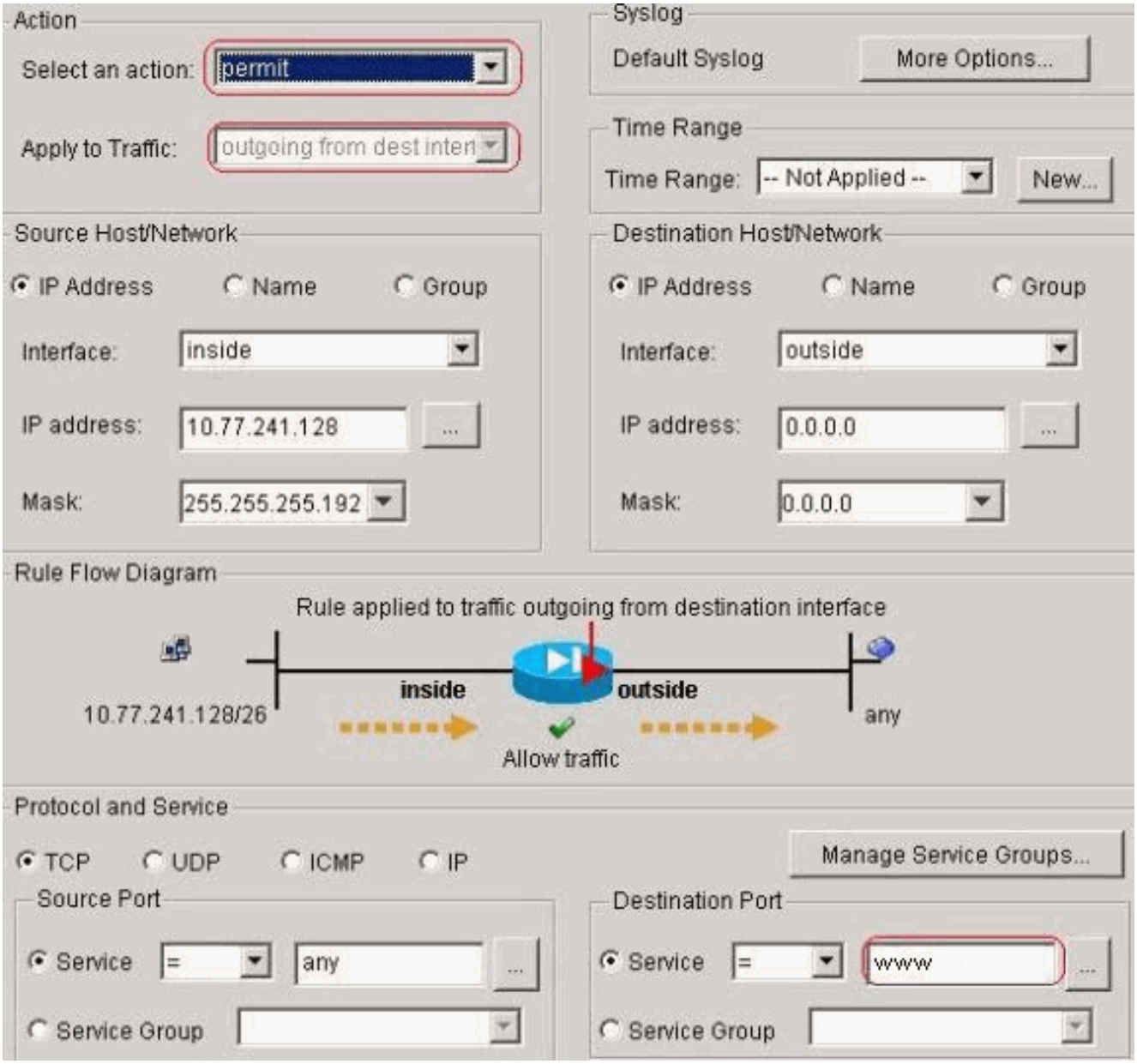
3. **Configurazione degli ACL**Per configurare gli ACL come mostrato, scegliere **Configurazione > Criteri di sicurezza >Regole** di accesso.Fare clic su **Add** (Aggiungi) per configurare un ACL 101 che consenta al traffico Telnet originato dalla rete 10.77.241.128/26 di raggiungere qualsiasi rete di destinazione e applicarlo al traffico in uscita sull'interfaccia esterna.



Fare clic su **OK**. Analogamente, per il traffico ssh e

http:

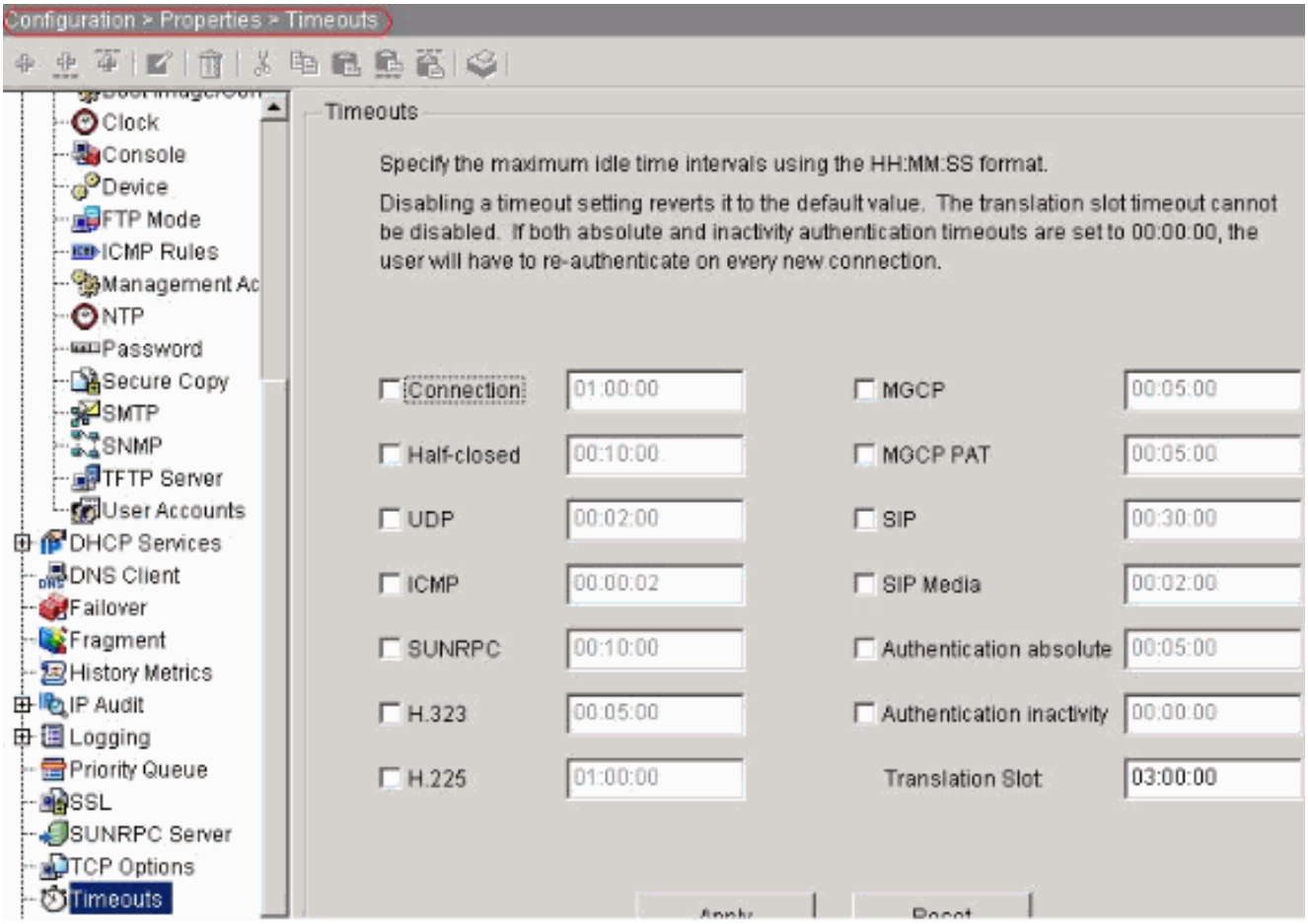

Action
Select an action:
permit
Apply to Traffic:
outgoing from dest inter
Syslog
Default Syslog
More Options...
Time Range
Time Range:
-- Not Applied --
New...
Source Host/Network
IP Address
Name
Group
Interface:
inside
IP address:
10.77.241.128
Mask:
255.255.255.192
Destination Host/Network
IP Address
Name
Group
Interface:
outside
IP address:
0.0.0.0
Mask:
0.0.0.0
Rule Flow Diagram
Rule applied to traffic outgoing from destination interface
10.77.241.128/26
inside
outside
any
Allow traffic
Protocol and Service
TCP
UDP
ICMP
IP
Manage Service Groups...
Source Port
Service
=
any
Service Group
Destination Port
Service
=
ssh
Service Group



Configurazione CLI equivalente come mostrato:

```
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq telnet
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq ssh
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq www
access-group 101 out interface outside
```

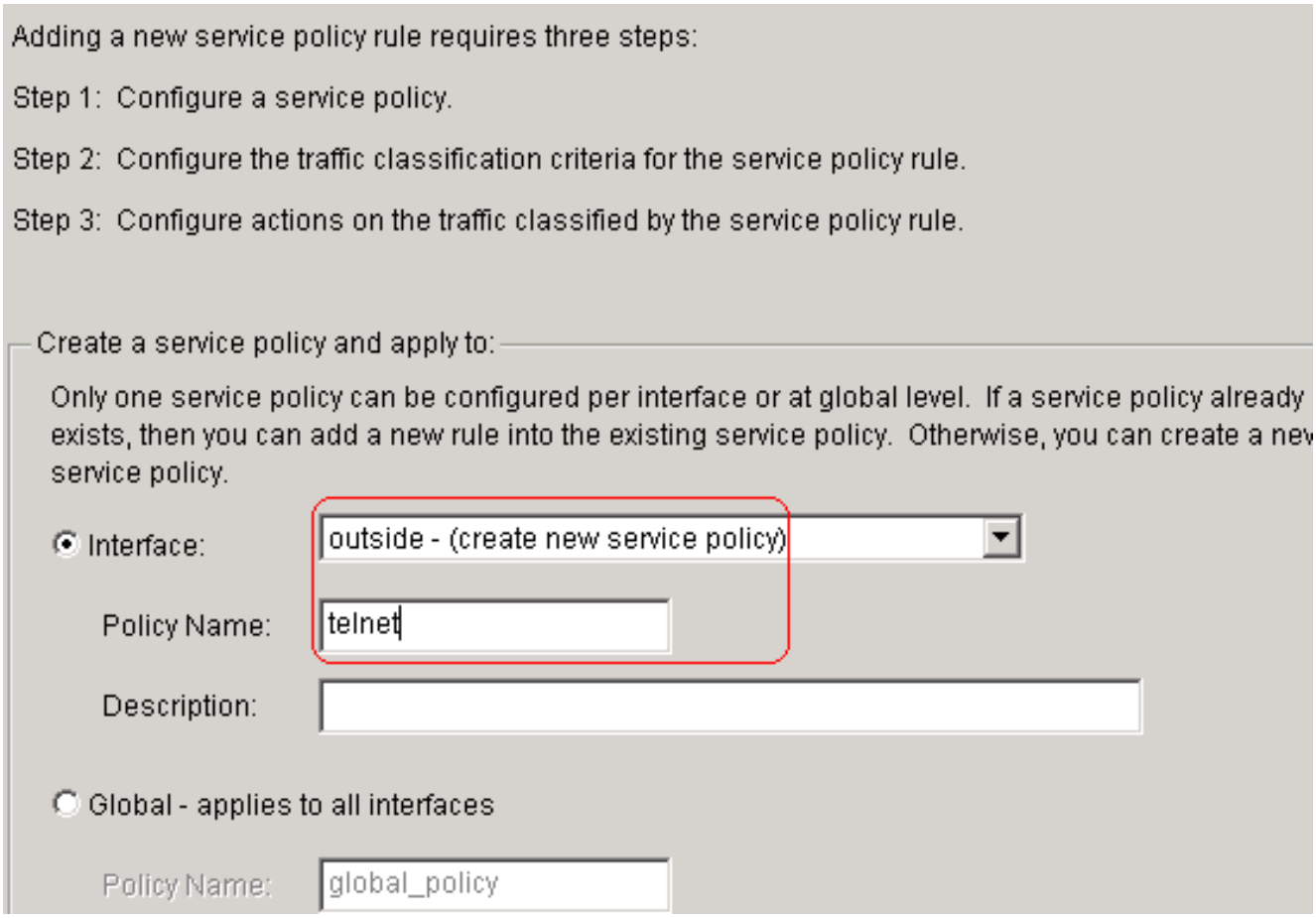
4. **Configura timeout**Per configurare i vari timeout, scegliete **Configurazione > Proprietà > Timeout**. In questo scenario, mantenere il valore predefinito per tutti i timeout.



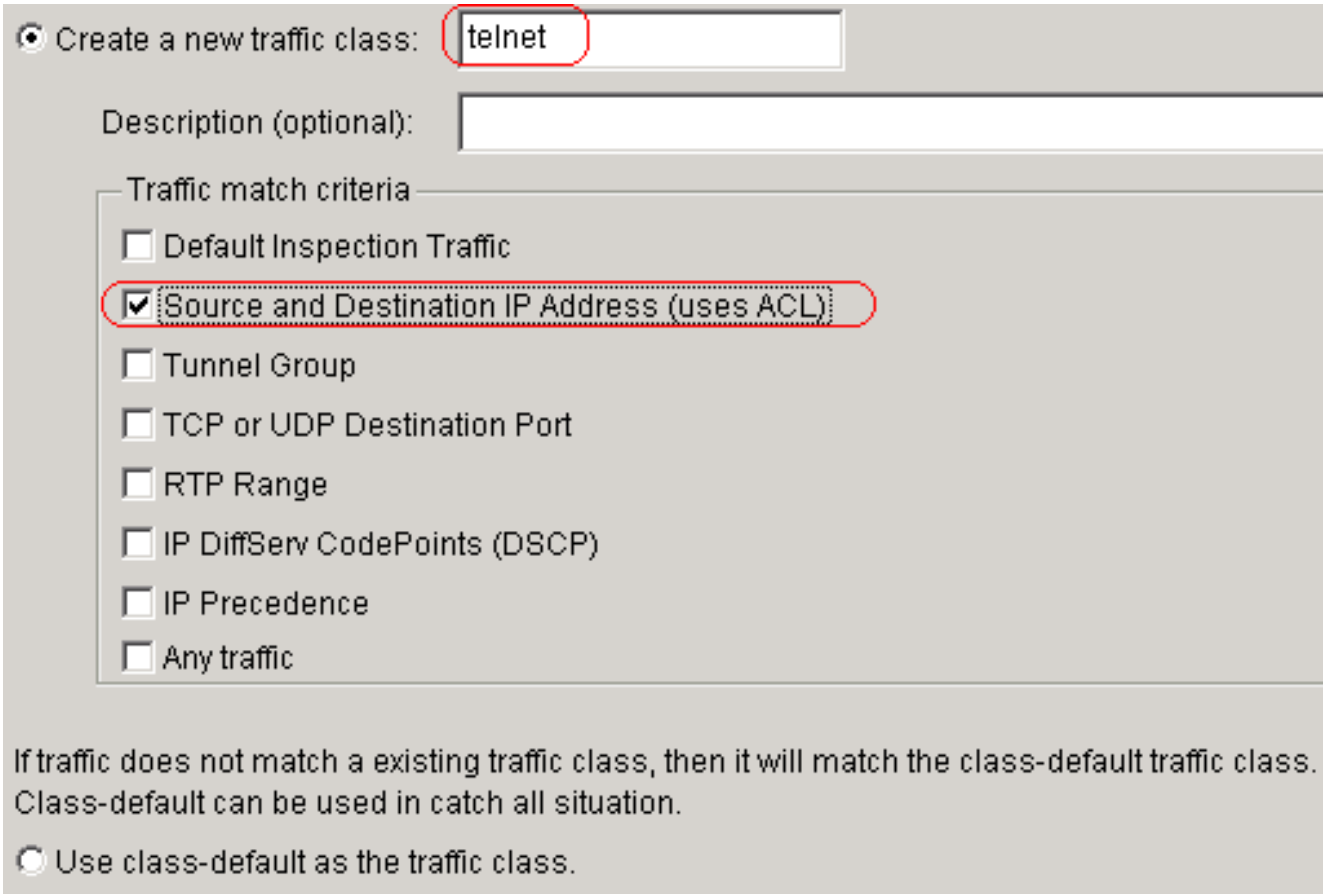
Configurazione CLI equivalente come mostrato:

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
```

5. Configurare **le regole dei criteri di servizio**.Scegliere **Configurazione > Criteri di sicurezza > Regole dei criteri di servizio > Aggiungi** per configurare la mappa della classe, la mappa dei criteri per l'impostazione del timeout della connessione TCP come 10 minuti e applicare i criteri del servizio sull'interfaccia esterna come mostrato.Selezionare il pulsante di opzione **Interface** per scegliere **outside - (create new service policy)**, che deve essere creato, e assegnare **telnet** come nome del
criterio.

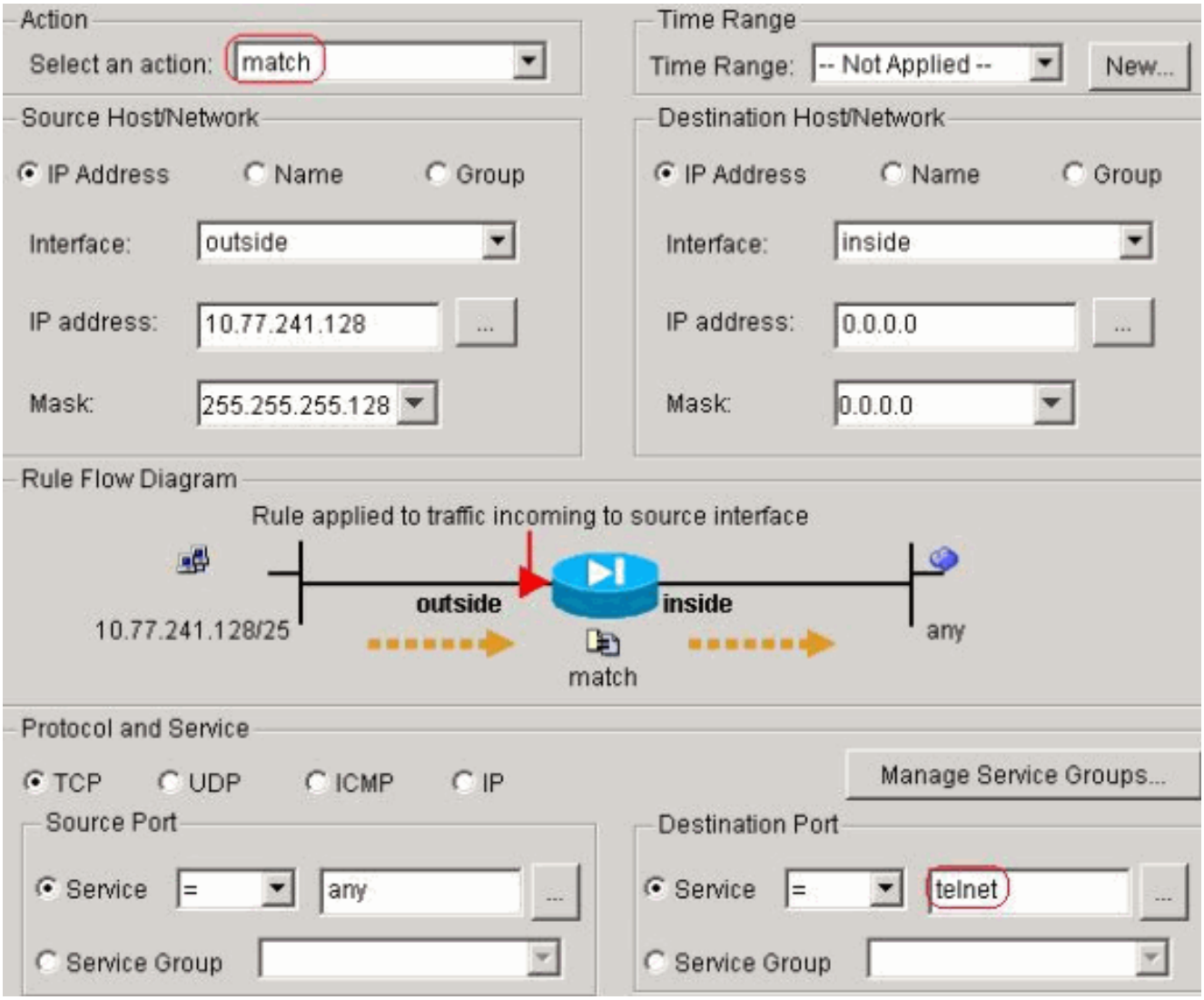


Fare clic su **Next** (Avanti).Creare una mappa di classe con il nome **telnet** e selezionare la casella di controllo **Source and Destination IP address (uses ACL)** nei criteri Traffic match.

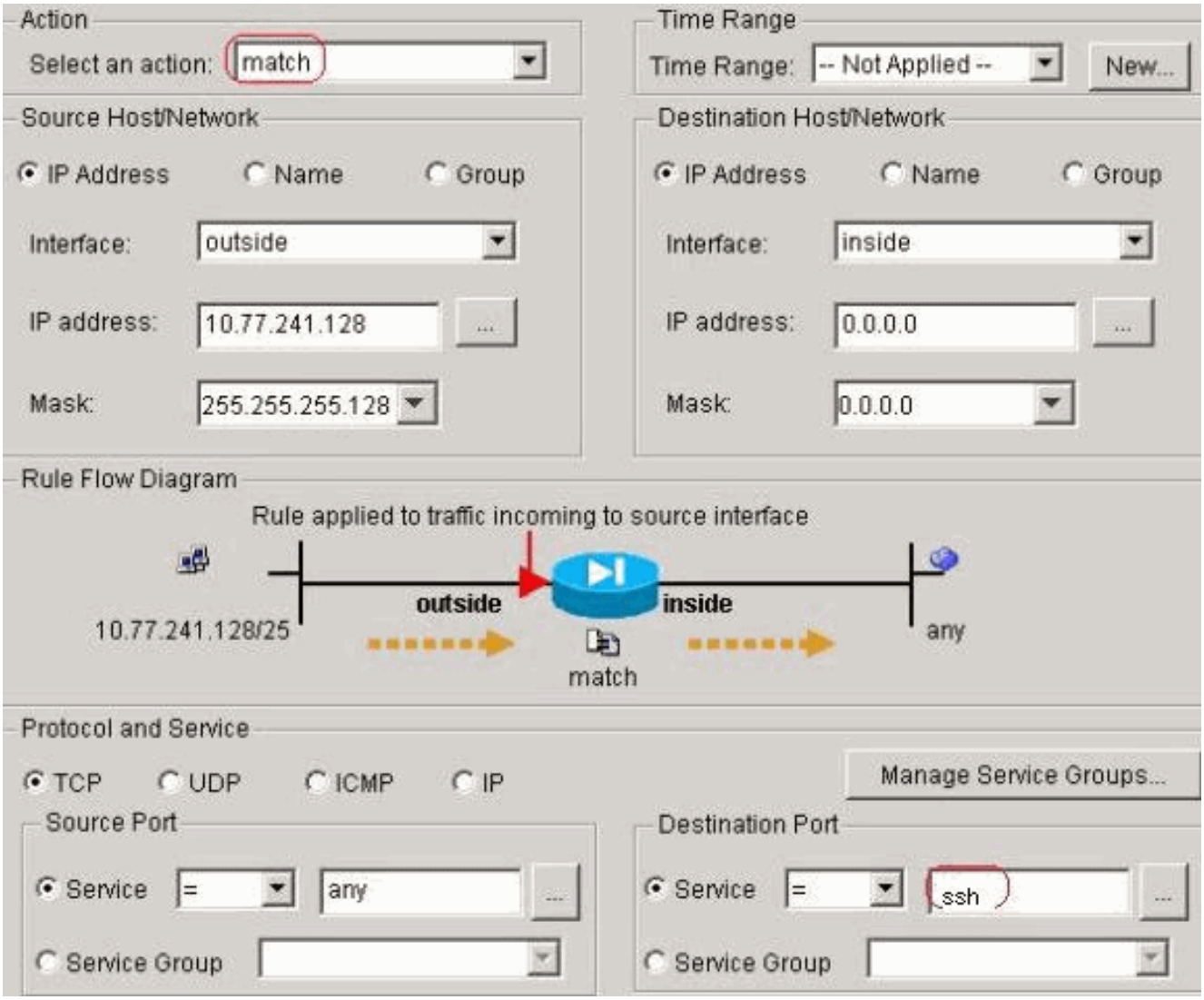


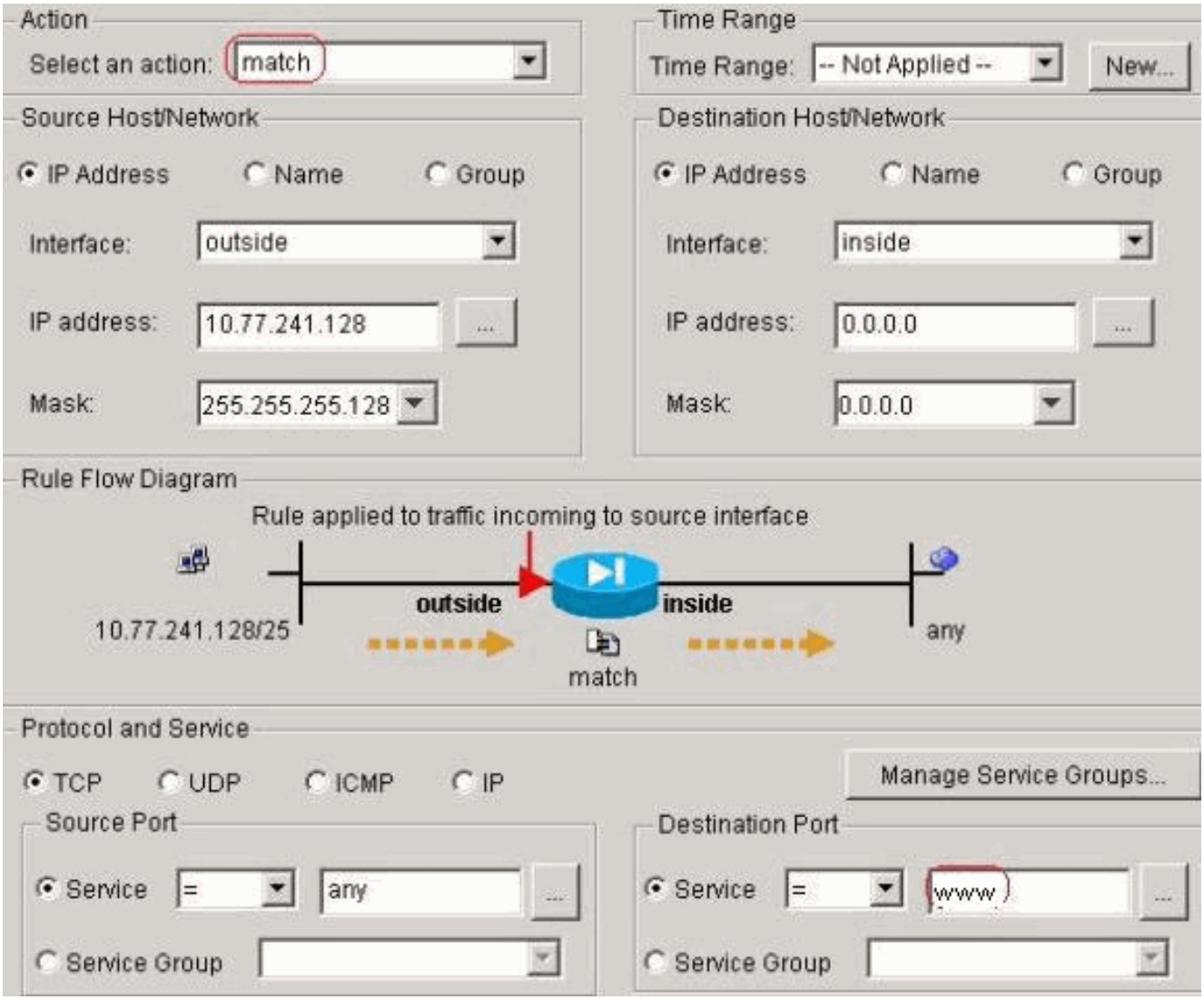
Fare clic su **Next** (Avanti).Creare un ACL in modo che corrisponda al traffico Telnet originato dalla rete 10.77.241.128/26 verso una rete di destinazione e applicarlo alla classe

telnet.

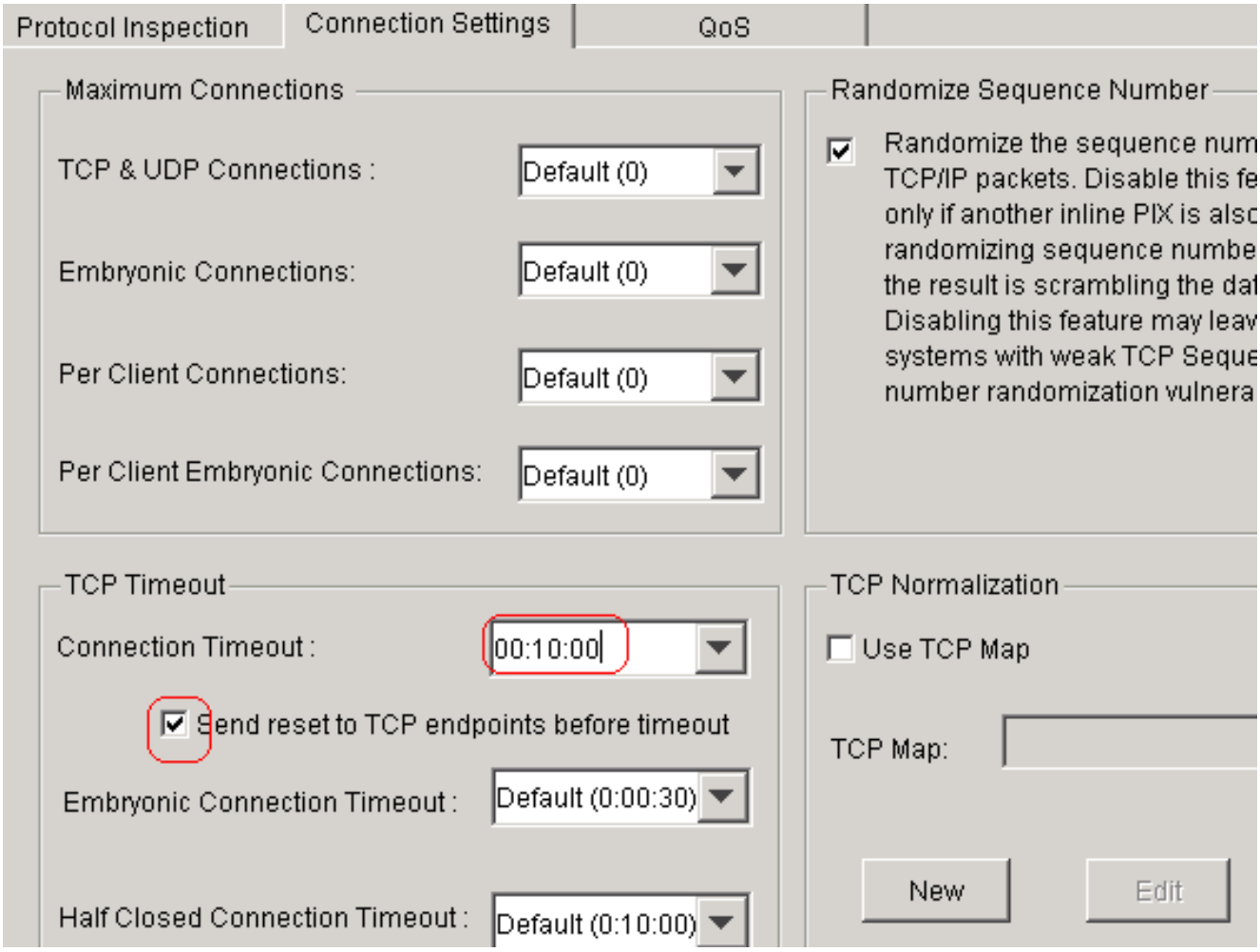


Fare clic su **Next** (Avanti). Analogamente, per il traffico ssh e http:

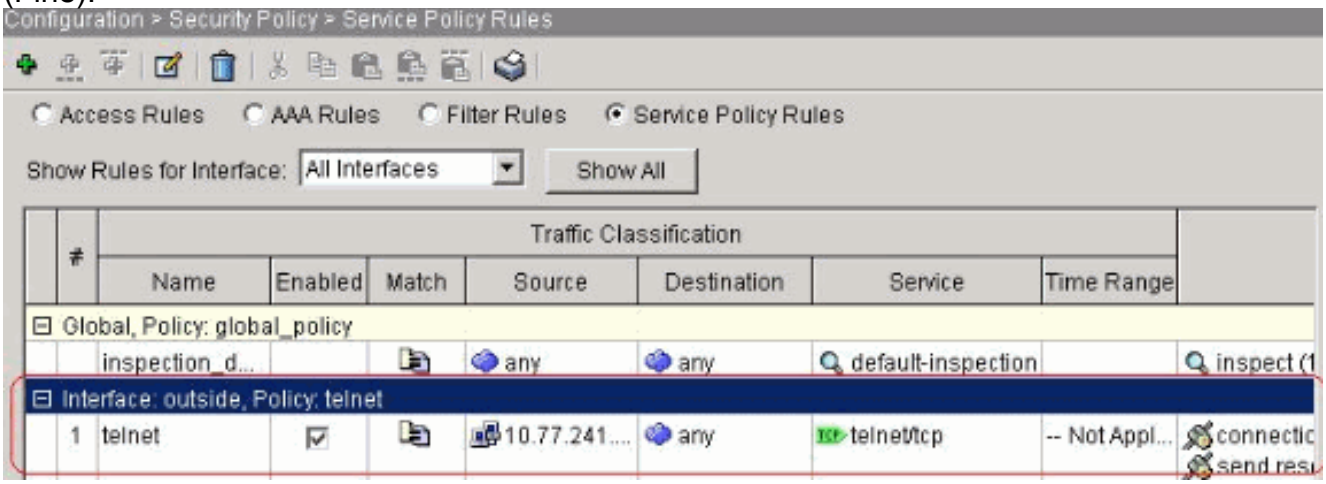

Action
Select an action: match
Time Range
Time Range: -- Not Applied --
New...
Source Host/Network
IP Address
Name
Group
Interface: outside
IP address: 10.77.241.128
Mask: 255.255.255.128
Destination Host/Network
IP Address
Name
Group
Interface: inside
IP address: 0.0.0.0
Mask: 0.0.0.0
Rule Flow Diagram
Rule applied to traffic incoming to source interface
10.77.241.128/25
outside
inside
any
match
Protocol and Service
TCP
UDP
ICMP
IP
Manage Service Groups...
Source Port
Service = any
Service Group
Destination Port
Service = ssh
Service Group



Selezionare **Connection Settings** (Impostazioni di connessione) per impostare il timeout della connessione TCP su 10 minuti, quindi selezionare la casella di controllo **Send reset to TCP endpoints before timeout** (Invia reset agli endpoint TCP prima del timeout).



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



Configurazione CLI equivalente come mostrato:

```
access-list outside_mpc_in extended permit tcp host 10.77.241.129  any eq telnet
access-list outside_mpc_in extended permit tcp host 10.77.241.129 any eq ssh
access-list outside_mpc_in extended permit tcp host 10.77.241.129 any eq www

class-map telnet
 description telnet
  match access-list outside_mpc_in

policy-map telnet
class telnet
  set connection timeout tcp 00:10:00 reset
service-policy telnet interface outside
```

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. In questo modo è possibile 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
```

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**.

Per verificare le configurazioni, usare il comando **show service-policy interface outside**.

```
PIX#show service-policy interface outside

   Interface outside:
    Service-policy: http
     Class-map: http
      Set connection policy:
      Set connection timeout policy:
        tcp 0:05:00 reset
      Inspect: http, packet 80, drop 0, reset-drop 0
```

Per verificare che il traffico specificato corrisponda alle configurazioni dei criteri del servizio, eseguire il comando **show service-policy flow**.

L'output di questo comando mostra un esempio:

```
PIX#show service-policy flow tcp host 10.77.241.129 host 10.1.1.2 eq 23

   Global policy:
  Service-policy: global_policy

Interface outside:
  Service-policy: telnet
    Class-map: telnet
      Match: access-list 101
        Access rule: permit tcp 10.77.241.128 255.255.255.192 any eq telnet
      Action:
        Input flow:  set connection timeout tcp 0:10:00 reset
```

Risoluzione dei problemi

Se il timeout della connessione non funziona con Modular Policy Framework (MPF), controllare la connessione TCP di avvio. Il problema può essere un'inversione dell'indirizzo IP di origine e di destinazione o un indirizzo IP non configurato correttamente nell'elenco degli accessi non corrispondente 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 PIX serie 500 Security Appliance
- Cisco ASA serie 5500 Adaptive Security Appliance
- 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)