ASA/PIX 7.X: Disabilita ispezione globale predefinita e Abilita ispezione applicazione non predefinita utilizzando ASDM

Sommario

Introduzione

In questo documento viene descritto come rimuovere il controllo predefinito dai criteri globali per un'applicazione e come abilitare il controllo per un'applicazione non predefinita.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stata usata un'appliance Cisco Adaptive Security Appliance (ASA) con immagine software 7.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 l'appliance di sicurezza PIX con

l'immagine software 7.x.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Criterio globale predefinito

Per impostazione predefinita, la configurazione include un criterio che corrisponde a tutto il traffico di ispezione delle applicazioni predefinito e applica determinate ispezioni al traffico su tutte le interfacce (un criterio globale). Non tutte le ispezioni sono abilitate per impostazione predefinita. È possibile applicare un solo criterio globale. Se si desidera modificare il criterio globale, è necessario modificare il criterio predefinito oppure disattivarlo e applicarne uno nuovo. Un criterio di interfaccia ha la precedenza sul criterio globale.

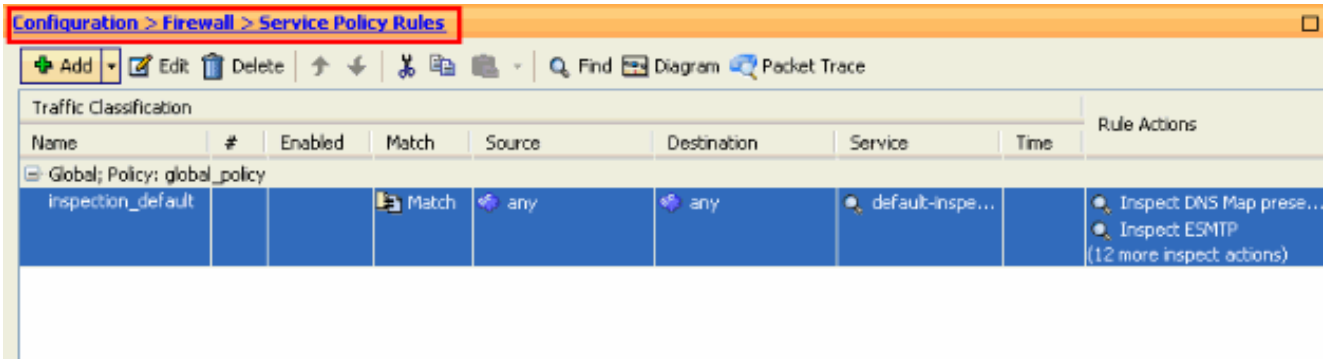
La configurazione predefinita dei criteri include i comandi seguenti:

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
service-policy global_policy global
```

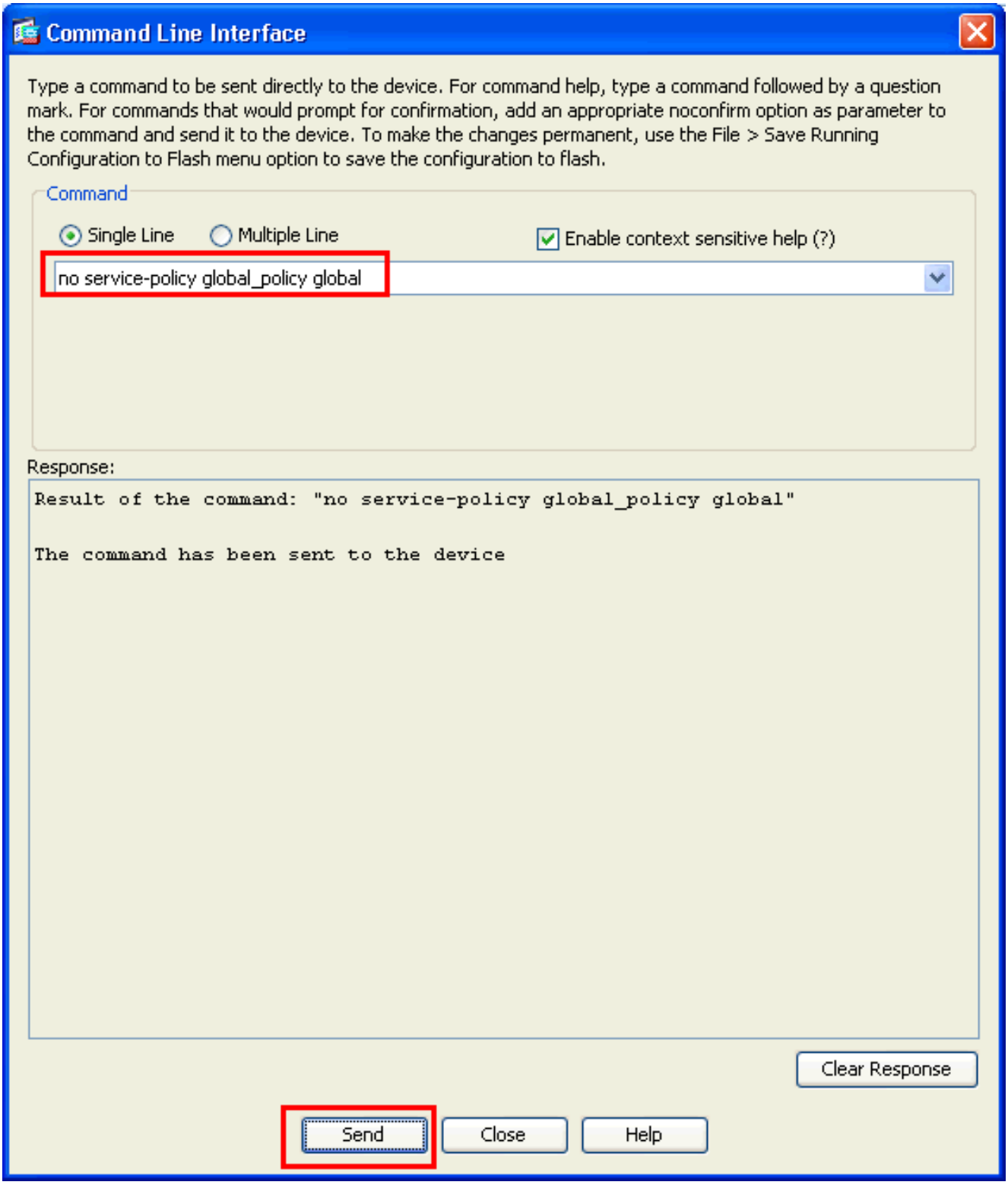
Abilita ispezione applicazione non predefinita

Completare questa procedura per abilitare il controllo delle applicazioni non predefinite sull'appliance Cisco ASA:

1. Accedere ad **ASDM**. Selezionare **Configurazione > Firewall > Regole dei criteri di servizio**.

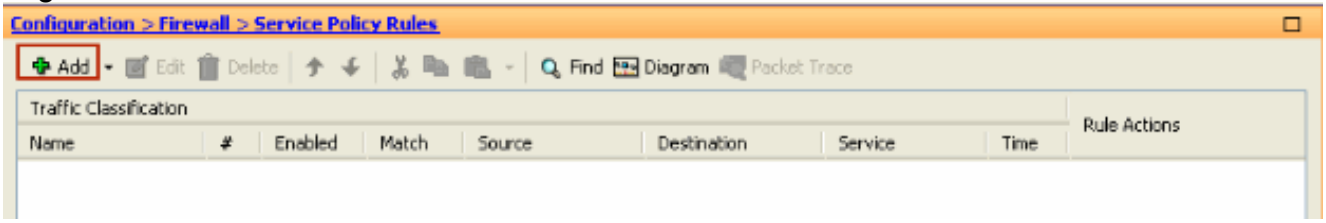


2. Se si desidera mantenere la configurazione per i criteri globali che include la mappa delle classi predefinita e la mappa dei criteri predefinita, ma si desidera rimuovere i criteri a livello globale, passare a **Strumenti > Interfaccia da riga di comando** e utilizzare il comando **globale no service-policy** per rimuovere i criteri a livello globale. Quindi, fare clic su **Send** per applicare il comando all'appliance
ASA.



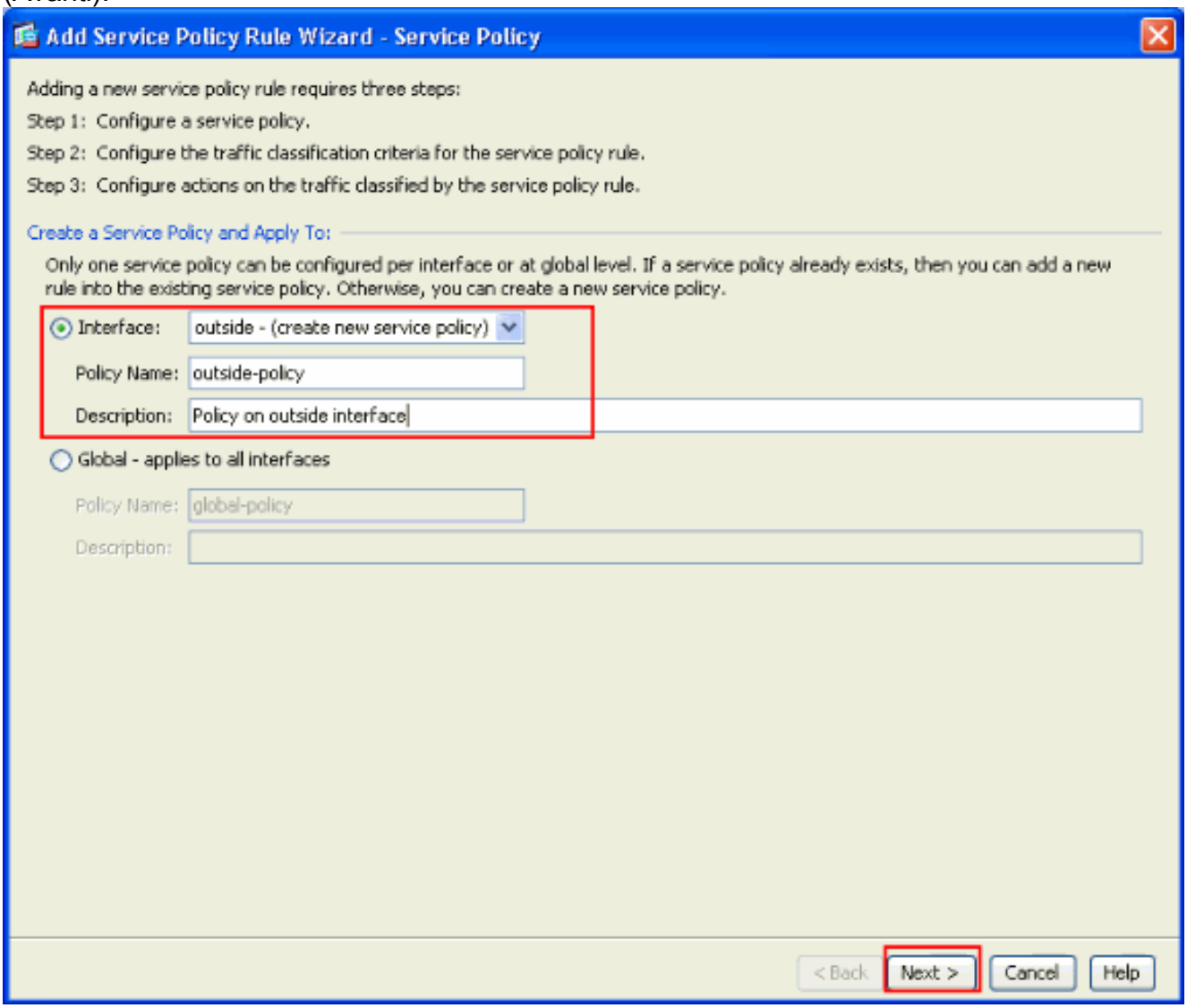
Nota: con questo passaggio, la policy globale diventa invisibile in Adaptive Security Device Manager (ASDM), ma viene visualizzata nella CLI.

3. Per aggiungere un nuovo criterio, fare clic su **Add** (Aggiungi) come mostrato di seguito:

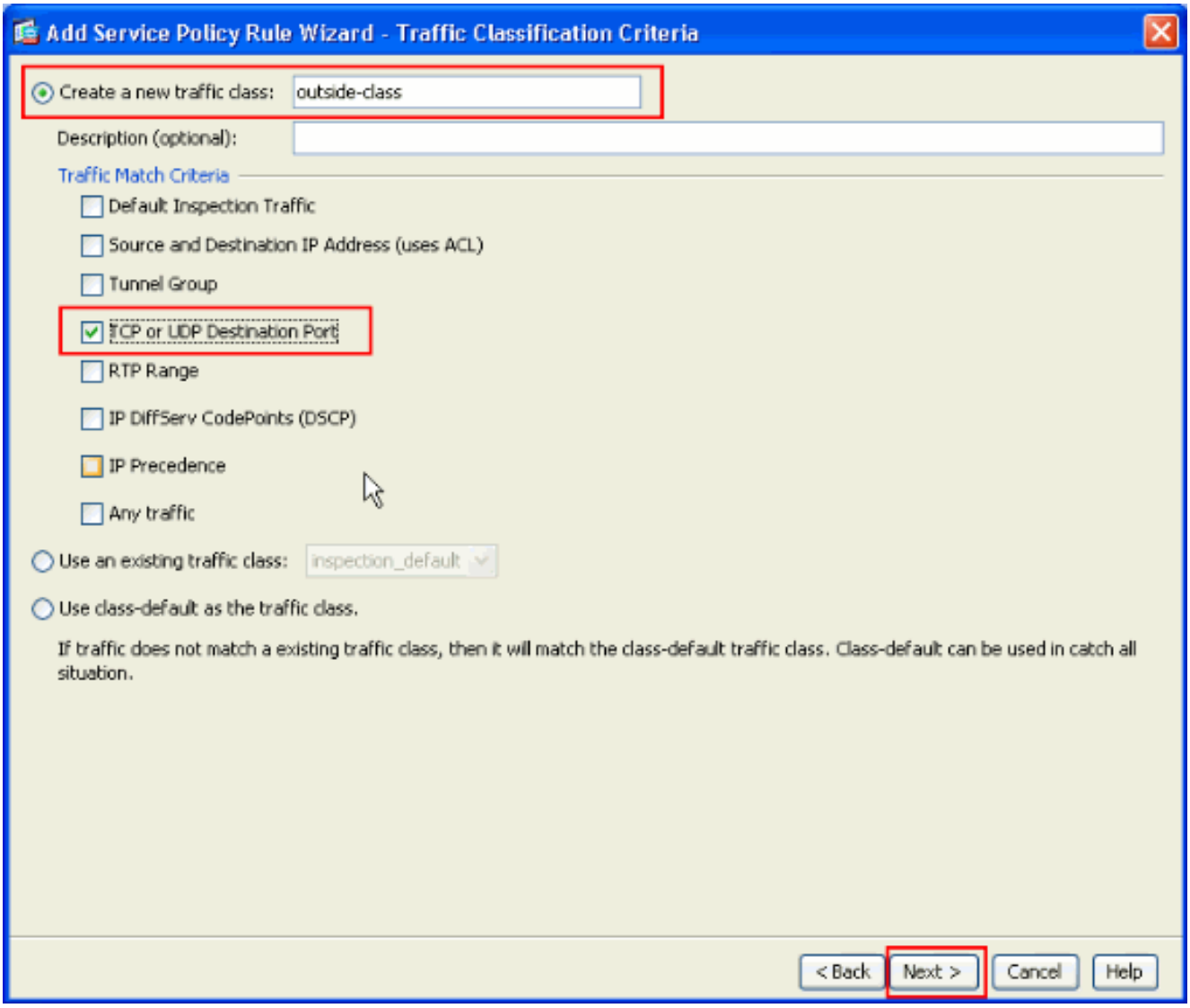


4. Verificare che il pulsante di opzione accanto a **Interfaccia** sia selezionato e scegliere l'interfaccia a cui applicare il criterio dal menu a discesa. Fornire quindi il **Nome criterio** e la

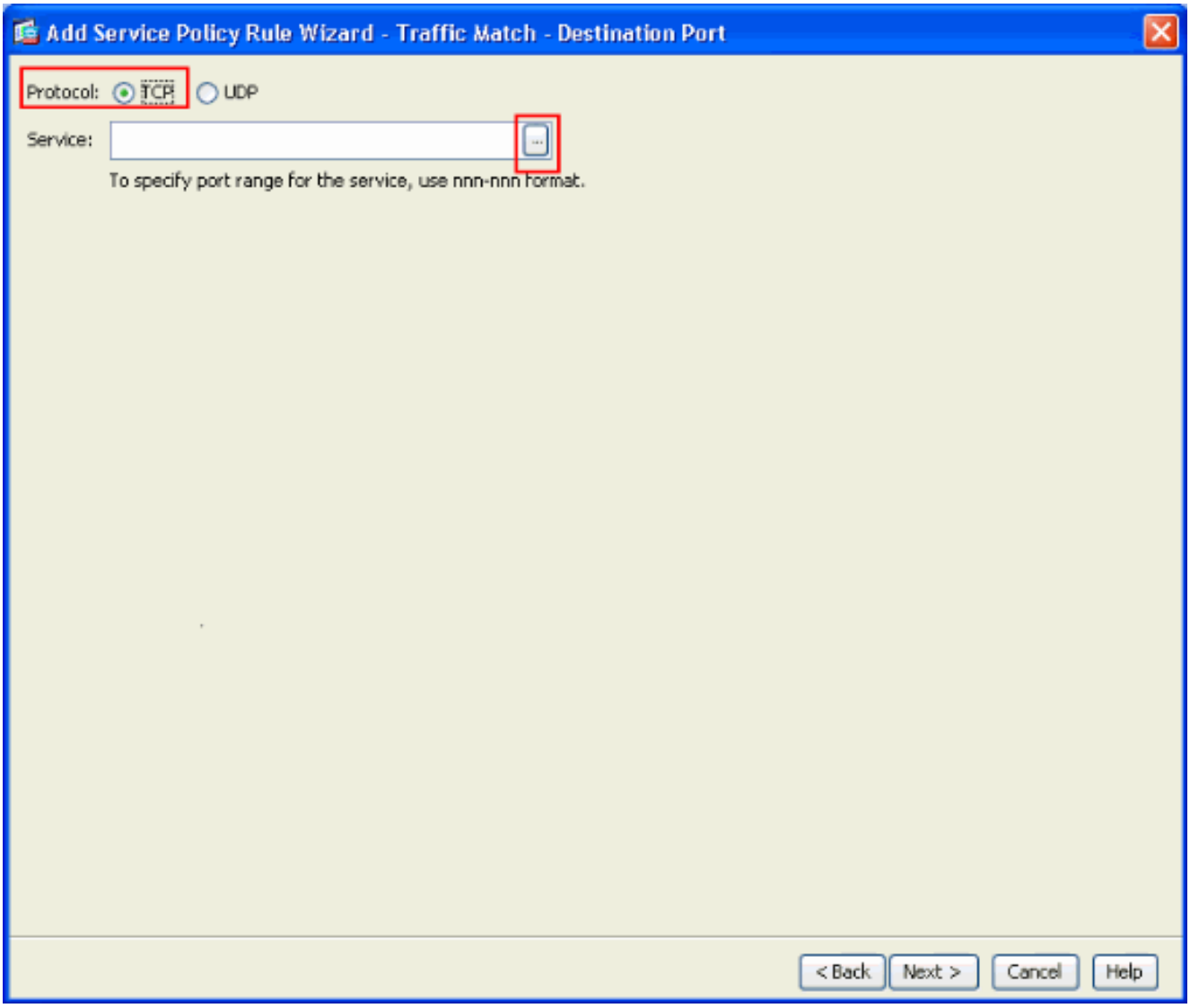
Descrizione. Fare clic su **Next** (Avanti).



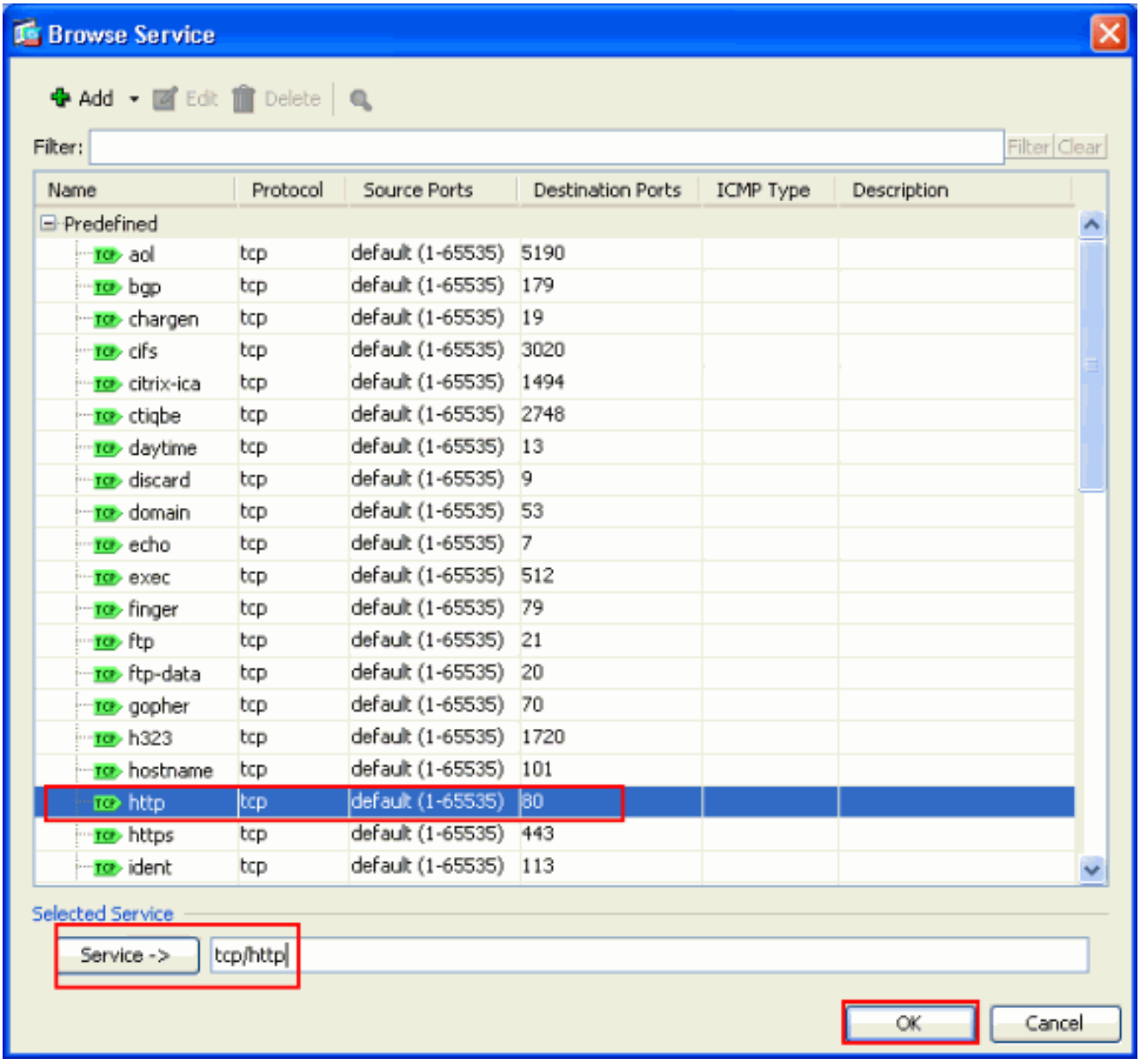
5. Creare una nuova mappa di classe per far corrispondere il traffico **TCP** mentre il traffico **HTTP** rientra in TCP. Fare clic su **Next** (Avanti).



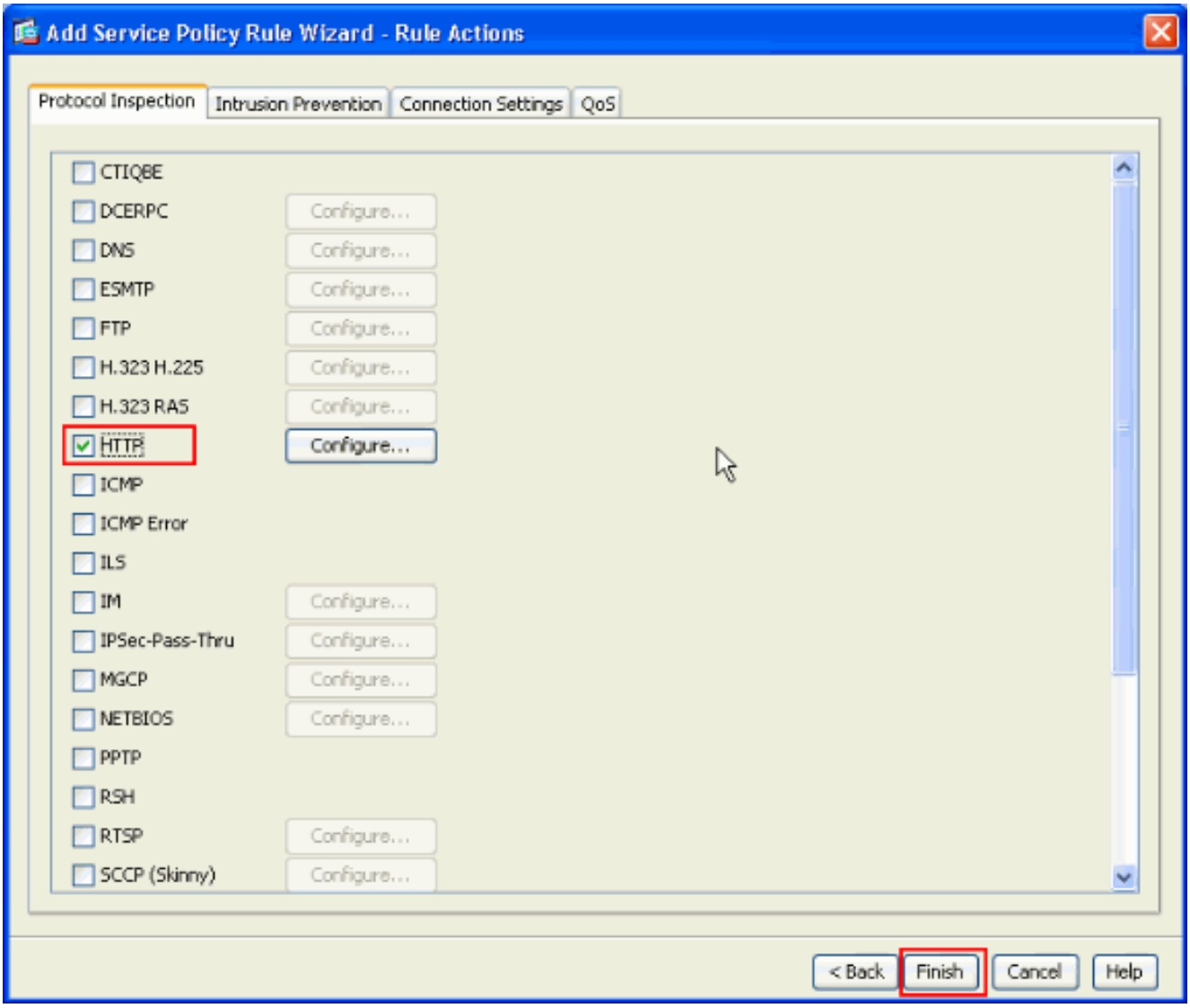
6. Selezionare **TCP** come protocollo.



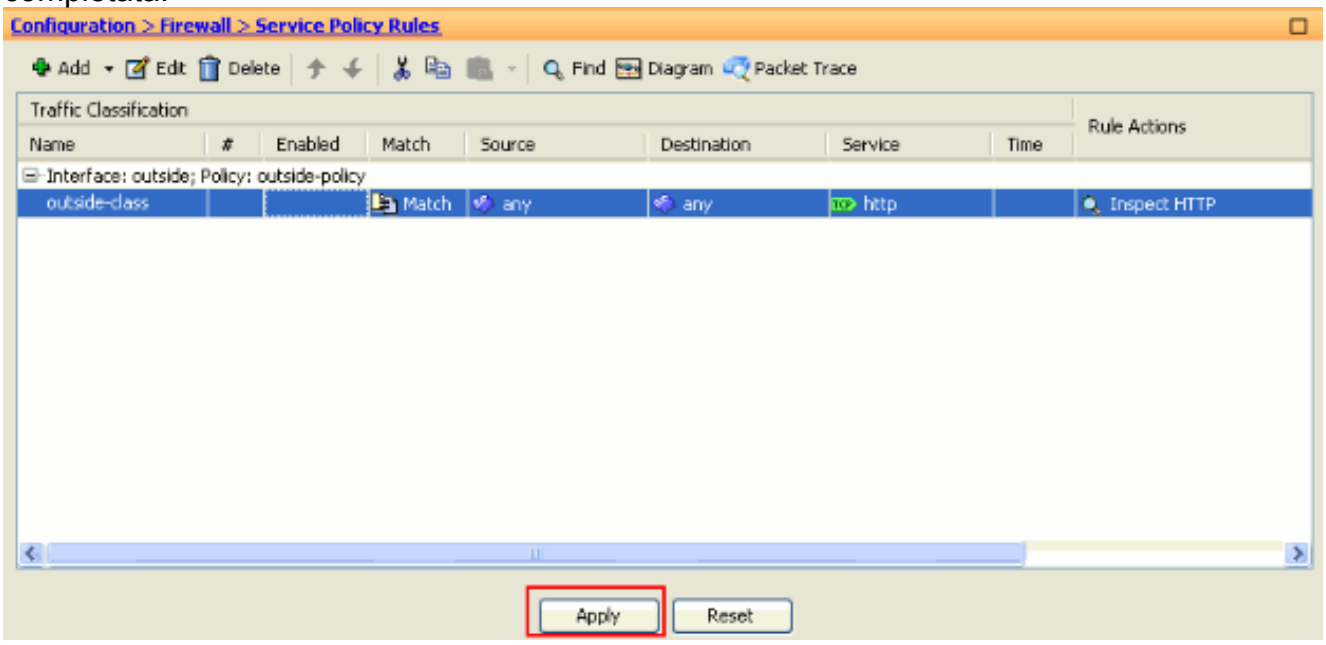
Scegliere **Porta HTTP 80** come servizio e fare clic su **OK**.



7. Scegliere **HTTP** e fare clic su **Fine**.



8. Fare clic su **Apply** (Applica) per inviare le modifiche alla configurazione all'appliance ASA da ASDM. La configurazione è stata completata.



Verifica

Utilizzare i seguenti comandi **show** per verificare la configurazione:

- Utilizzare il comando **show run class-map** per visualizzare le mappe classi configurate.

```
ciscoasa# sh run class-map
!
class-map inspection_default
match default-inspection-traffic
class-map outside-class
match port tcp eq www
!
```

- Utilizzare il comando **show run policy-map** per visualizzare i mapping dei criteri configurati.

```
ciscoasa# sh run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
policy-map outside-policy
 description Policy on outside interface
 class outside-class
  inspect http
!
```

- Utilizzare il comando **show run service-policy** per visualizzare i criteri dei servizi configurati.

```
ciscoasa# sh run service-policy
service-policy outside-policy interface outside
```

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Riferimenti per i comandi di Cisco ASA serie 5500
- Pagina di supporto di Cisco Adaptive Security Device Manager (ASDM)
- Software Cisco PIX Firewall
- RFC (Requests for Comments)
- Cisco PIX serie 500 Security Appliance
- Applicazione dell'ispezione del protocollo a livello di applicazione
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Documentazione e supporto tecnico – Cisco Systems