ASA 8.3 e versioni successive - Configurazione dell'ispezione con ASDM

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per Cisco Adaptive Security Appliance (ASA) con le versioni 8.3(1) e successive istruzioni su come rimuovere l'ispezione predefinita dai criteri globali di un'applicazione e su come abilitare l'ispezione per un'applicazione non predefinita utilizzando Adaptive Security Device Manager (ASDM).

Per ulteriori informazioni, fare riferimento al documento PIX/ASA 7.X: Disabilitare l'ispezione globale predefinita e abilitare l'ispezione delle applicazioni non predefinita 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 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.

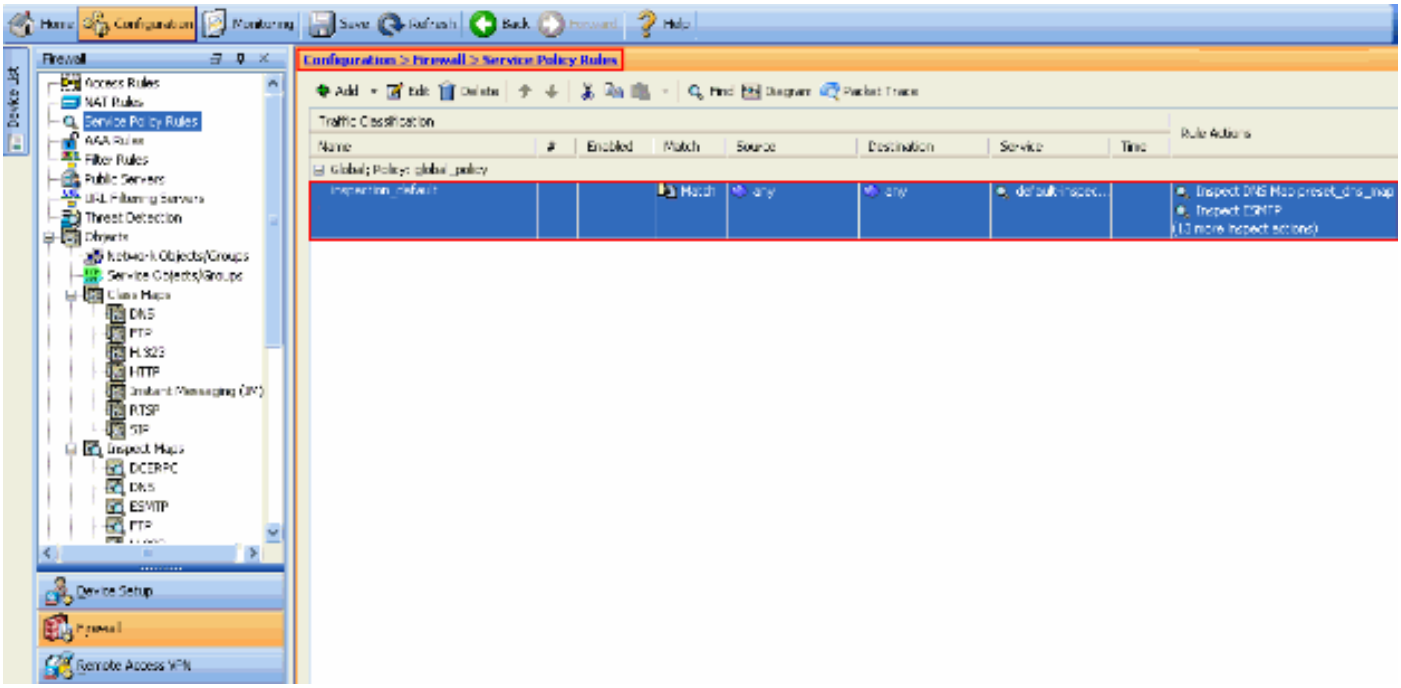
Convenzioni

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

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.

In ASDM, scegliere **Configurazione > Firewall > Regole criteri servizio** per visualizzare il criterio globale predefinito con l'ispezione dell'applicazione predefinita, come mostrato di seguito:

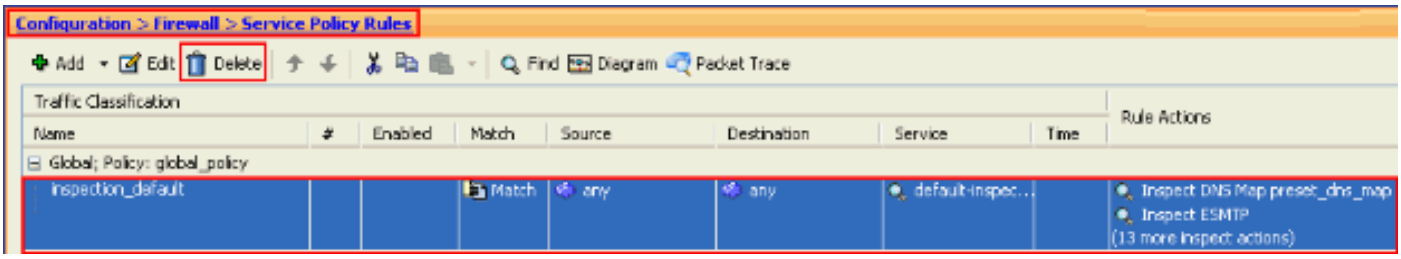


La configurazione predefinita dei criteri include i comandi seguenti:

```
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
```

Se è necessario disabilitare il criterio globale, utilizzare il comando **no service-policy global_policy global_policy**. Per eliminare il criterio globale utilizzando ASDM, scegliere **Configurazione > Firewall > Regole dei criteri di servizio**. Selezionare quindi il criterio globale e fare clic su **Elimina**.



Nota: quando si elimina il criterio del servizio con ASDM, vengono eliminati anche i mapping dei criteri e delle classi associati. Tuttavia, se il criterio del servizio viene eliminato utilizzando CLI, solo il criterio del servizio viene rimosso dall'interfaccia. La mappa delle classi e la mappa dei criteri rimangono invariate.

Disabilita ispezione globale predefinita per un'applicazione

Per disabilitare l'ispezione globale per un'applicazione, utilizzare la versione *no* del comando **inspect**.

Ad esempio, per rimuovere l'ispezione globale dell'applicazione FTP su cui l'accessorio di sicurezza è in ascolto, usare il comando **no inspect ftp** in modalità di configurazione classe.

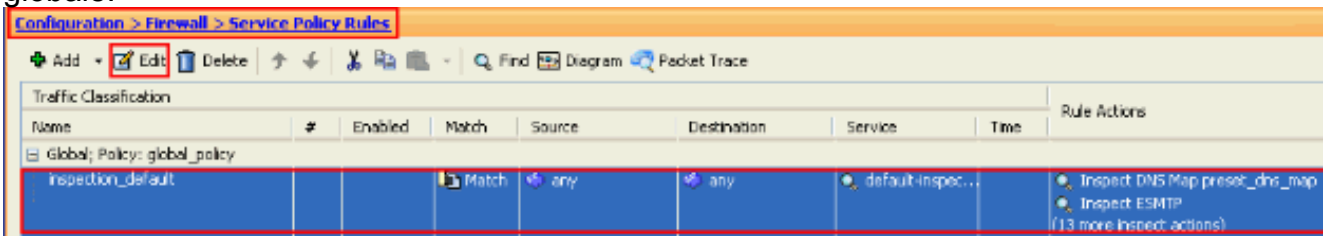
La modalità di configurazione delle classi è accessibile dalla modalità di configurazione della mappa dei criteri. Per rimuovere la configurazione, usare la forma *no* del comando.

```
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#no inspect ftp
```

Per disabilitare l'ispezione globale per FTP con ASDM, attenersi alla seguente procedura:

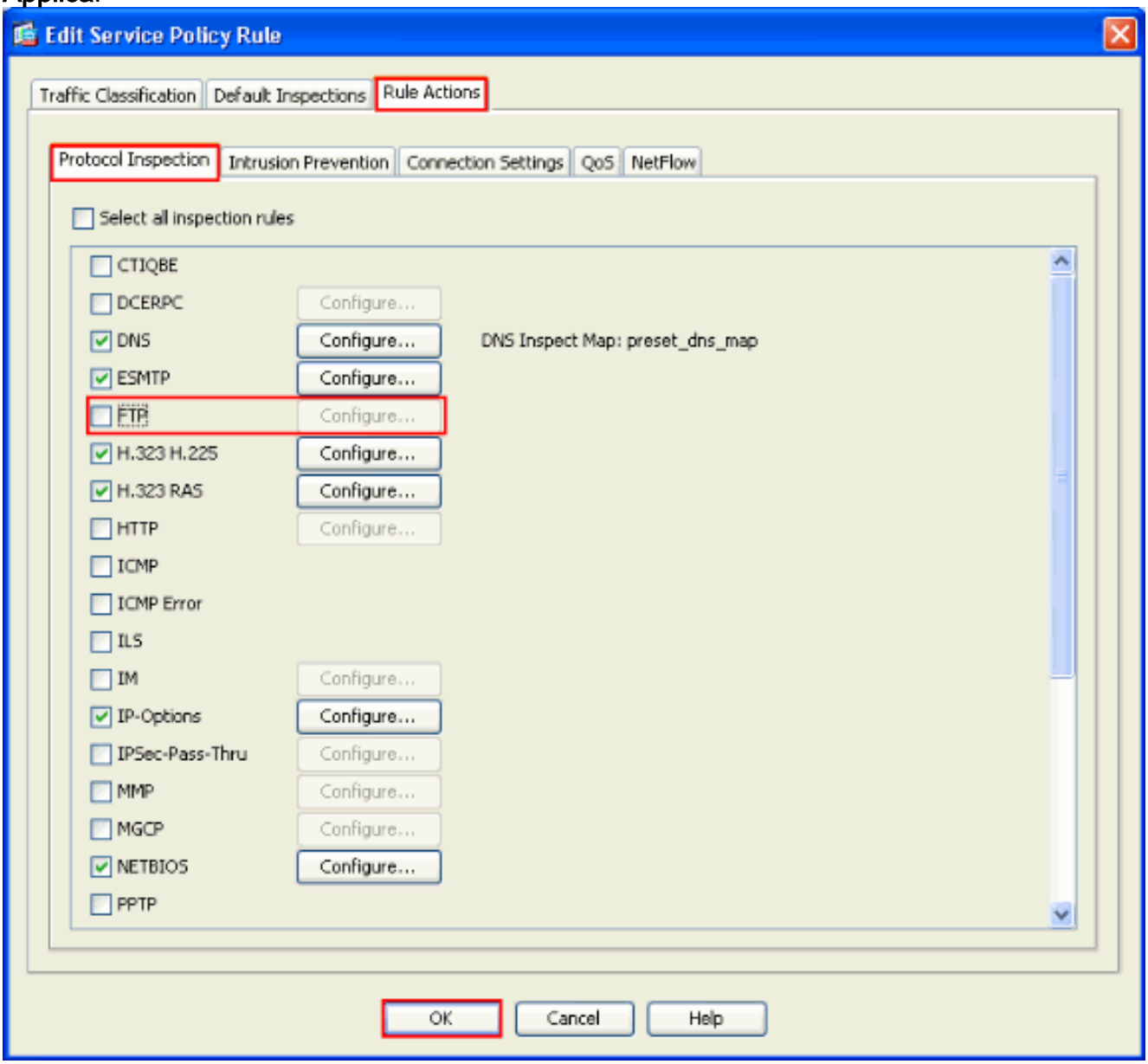
Nota: per accedere a PIX/ASA tramite ASDM, consultare le impostazioni di base di Consenti accesso HTTPS per ASDM.

1. Scegliere **Configurazione > Firewall > Regole criteri servizio** e selezionare il criterio globale predefinito. Fare quindi clic su **Modifica** per modificare il criterio di ispezione globale.



2. Nella finestra Modifica regola dei criteri per i servizi scegliere **Ispezione protocollo** nella

scheda **Azioni regola**. Verificare che la casella di controllo **FTP** sia deselezionata. In questo modo l'ispezione FTP viene disattivata come mostrato nell'immagine seguente. Fare quindi clic su **OK** e su **Applica**.



Nota: per ulteriori informazioni sull'ispezione FTP, consultare il documento PIX/ASA 7.x: Abilita esempio di configurazione dei servizi FTP/TFTP.

Abilita ispezione per applicazione non predefinita

L'ispezione HTTP avanzata è disabilitata per impostazione predefinita. Per abilitare l'ispezione HTTP in global_policy, utilizzare il comando **inspect http** in class_inspection_default.

Nell'esempio, qualsiasi connessione HTTP (traffico TCP sulla porta 80) che entra nell'appliance di sicurezza attraverso un'interfaccia qualsiasi viene classificata per l'ispezione HTTP. *Poiché il criterio è globale, l'ispezione viene eseguita solo quando il traffico entra in ciascuna interfaccia*.

```
ASA(config)# policy-map global_policy
ASA(config-pmap)#  class inspection_default
ASA(config-pmap-c)# inspect http
ASA2(config-pmap-c)# exit
```

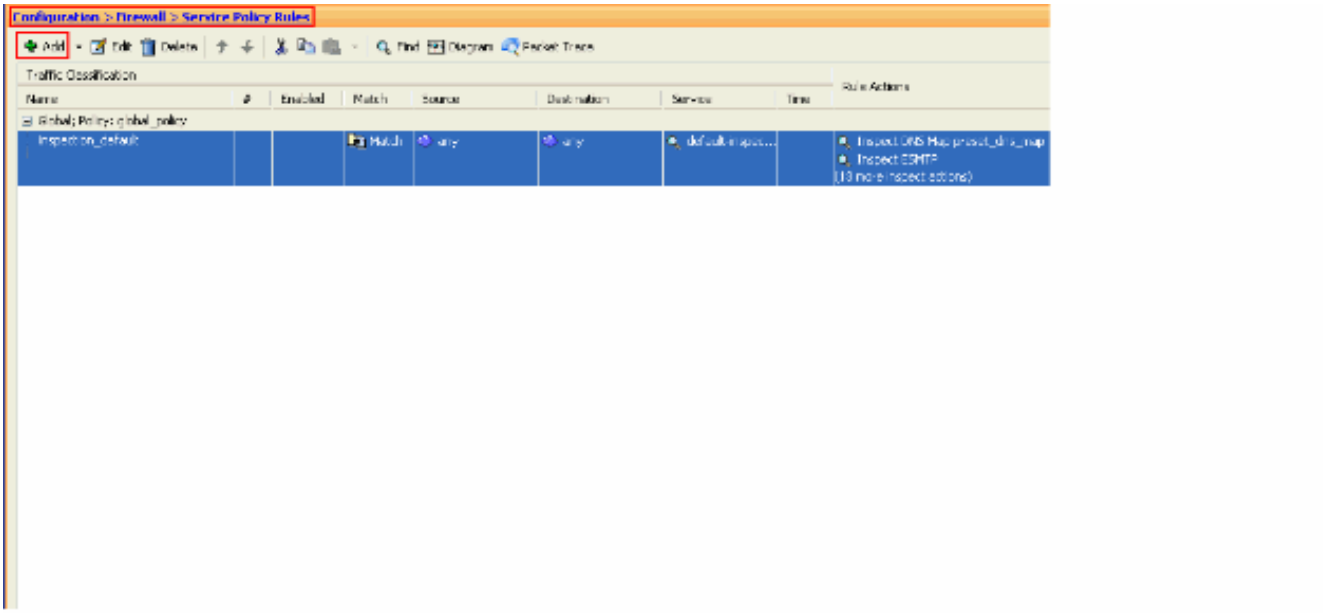
```
ASA2(config-pmap)# exit
ASA2(config)#service-policy global_policy global
```

Nell'esempio, tutte le connessioni HTTP (traffico TCP sulla porta 80) che entrano o escono dall'appliance di sicurezza attraverso l'*interfaccia esterna vengono classificate per l'ispezione HTTP*.

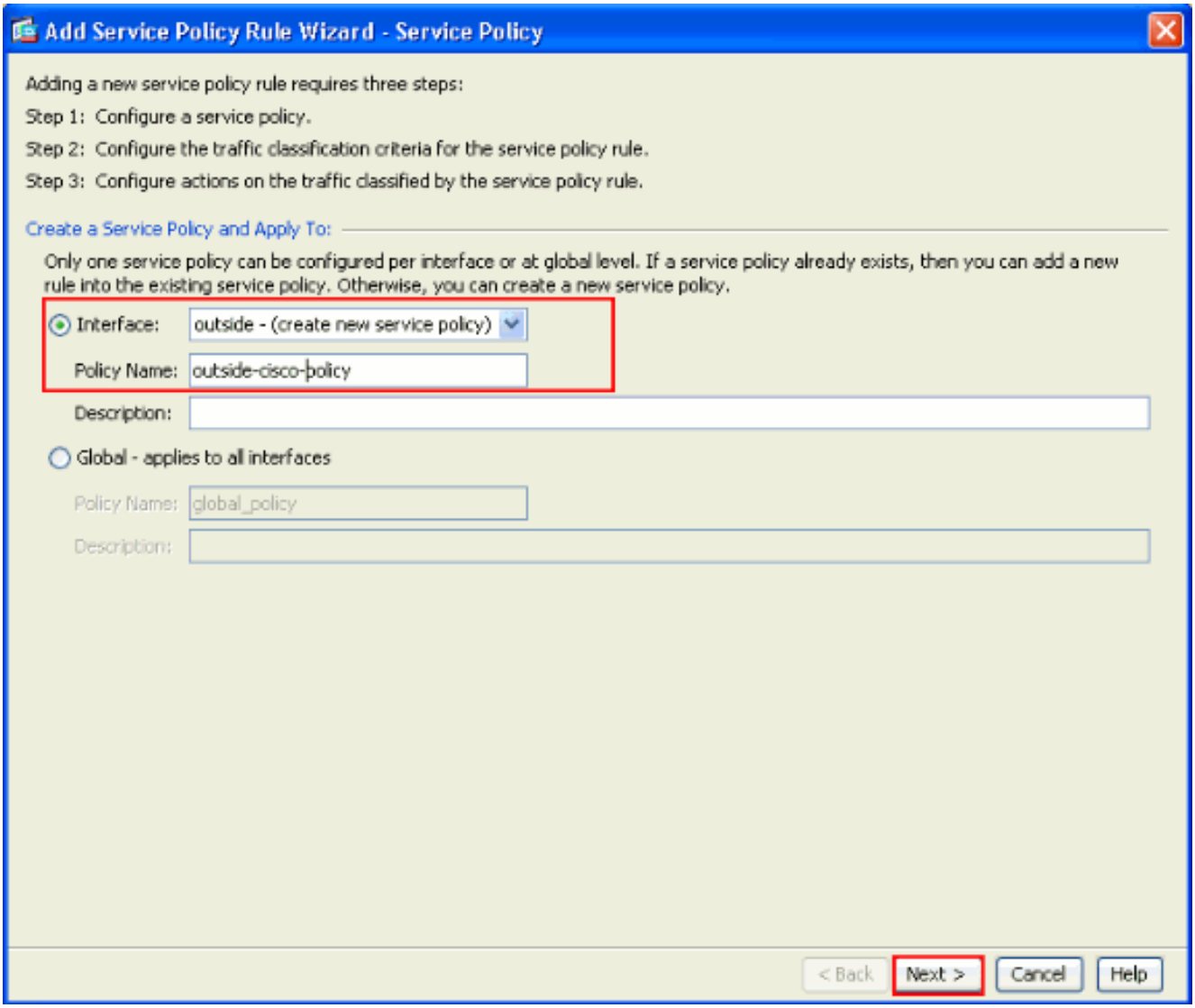
```
ASA(config)#class-map outside-class
ASA(config-cmap)#match port tcp eq www
ASA(config)#policy-map outside-cisco-policy
ASA(config-pmap)#class outside-class
ASA(config-pmap-c)#inspect http
ASA(config)#service-policy outside-cisco-policy interface outside
```

Per configurare l'esempio precedente utilizzando ASDM, attenersi alla seguente procedura:

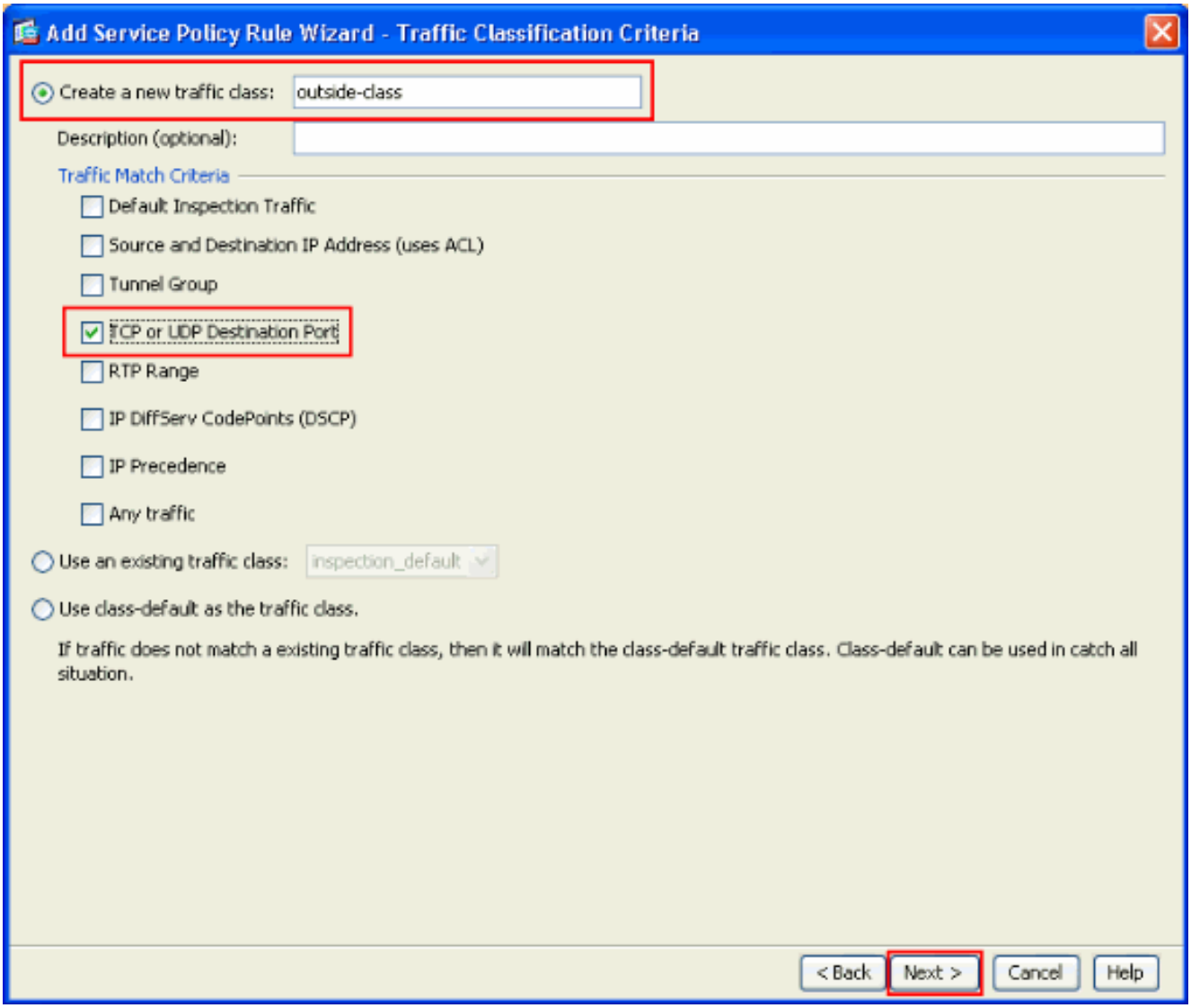
1. Scegliere **Configurazione > Firewall > Regole dei criteri di servizio** e fare clic su **Aggiungi** per aggiungere un nuovo criterio di servizio:



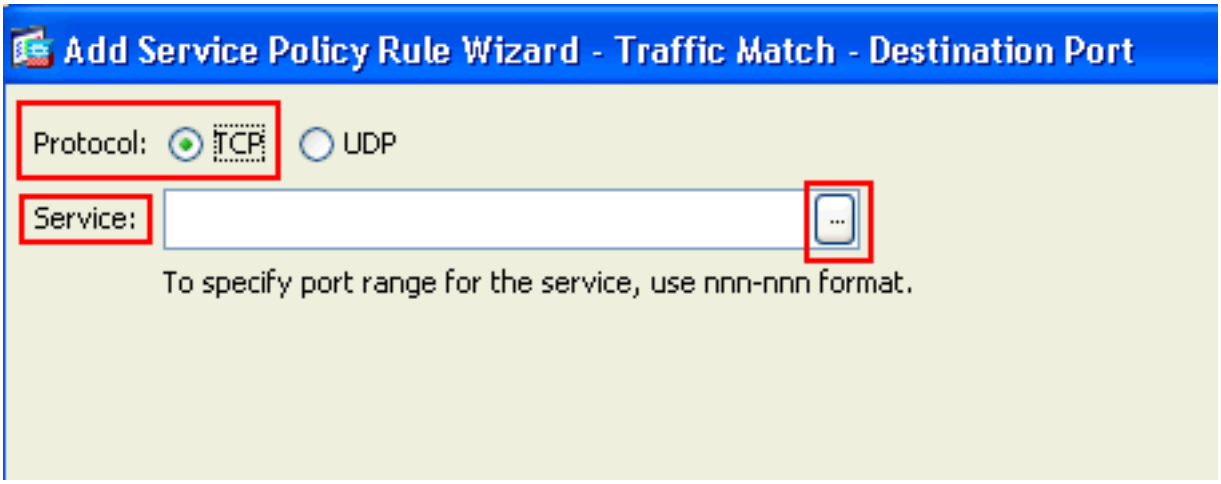
2. Nella finestra Aggiunta guidata regola dei criteri di servizio - Criteri di servizio scegliere il pulsante di opzione accanto a **Interfaccia**. In questo modo il criterio viene applicato a un'interfaccia specifica, ovvero l'interfaccia **esterna** di questo esempio. Specificare un nome di criterio **esterno a cisco-policy** in questo esempio. Fare clic su **Next** (Avanti).



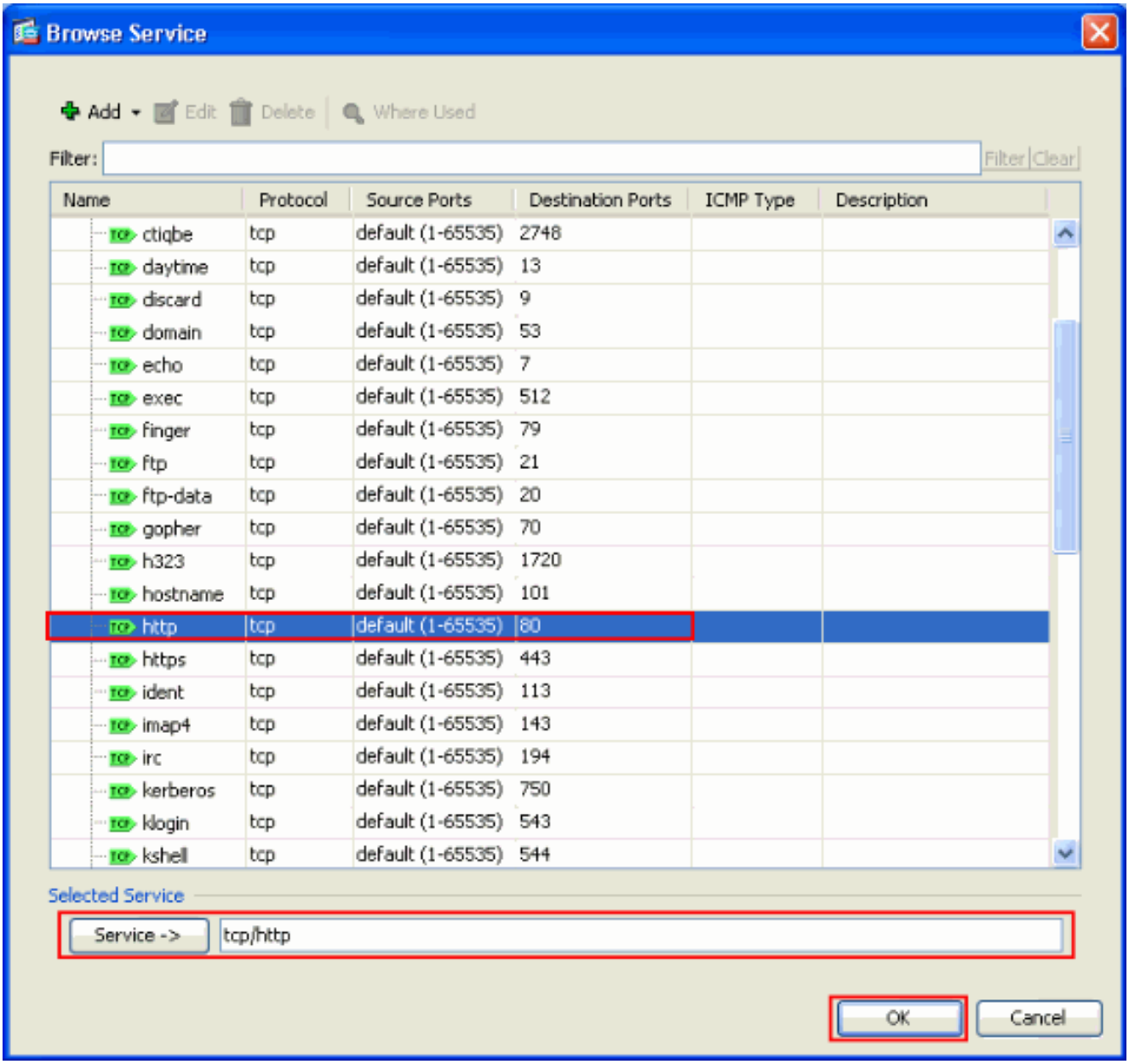
3. Nella finestra Criteri di classificazione traffico della procedura guidata Aggiungi regola dei criteri servizio specificare il nome della nuova classe di traffico. Il nome utilizzato in questo esempio è **outside-class**. Verificare che la casella di controllo accanto a **Porta di destinazione TCP o UDP** sia selezionata e fare clic su **Avanti**.



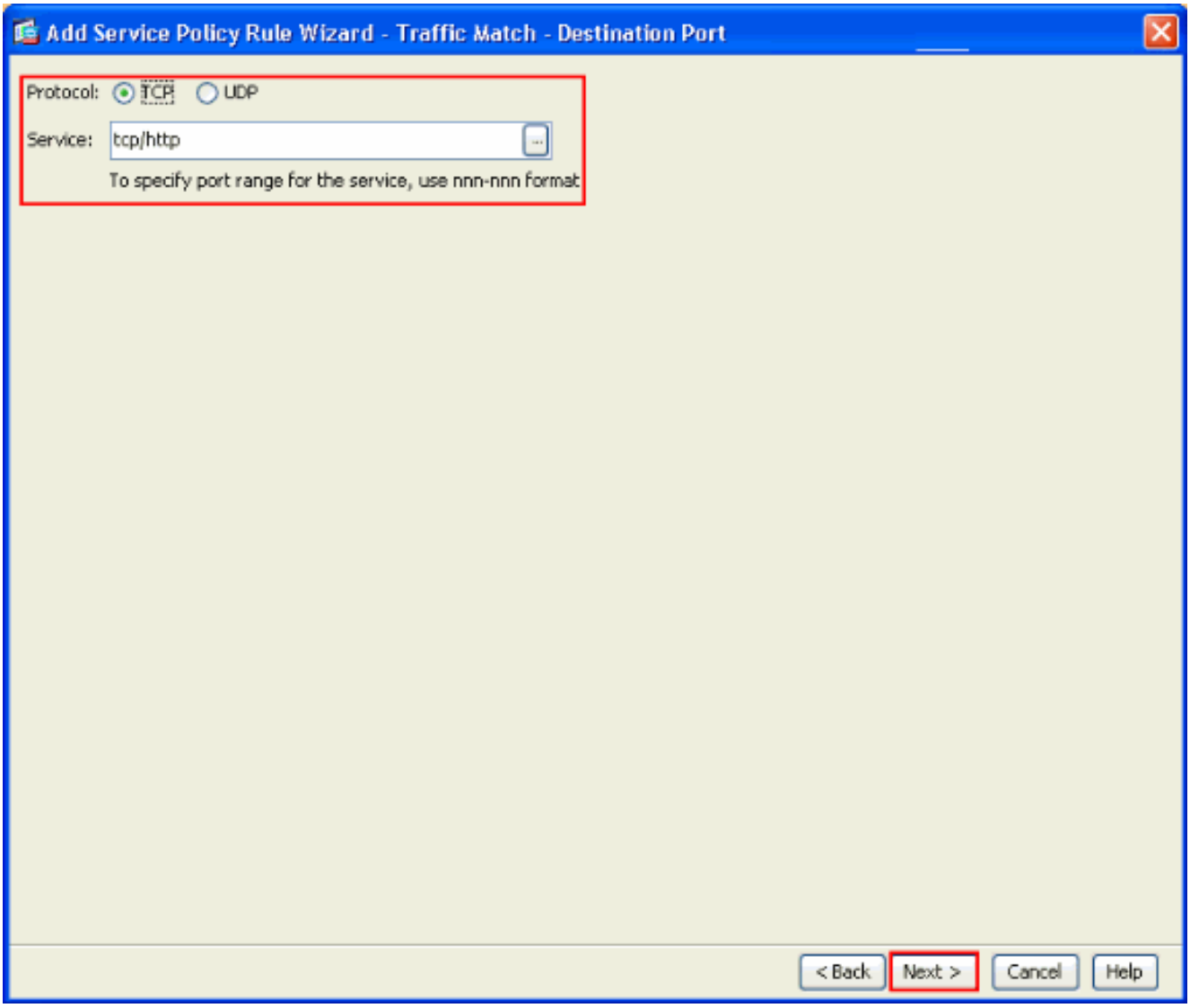
4. Nella finestra Aggiunta guidata regola dei criteri del servizio - Corrispondenza traffico - Porta di destinazione, scegliere il pulsante di opzione accanto a **TCP** nella sezione **Protocollo**. Quindi, fare clic sul pulsante accanto a **Servizio** per scegliere il servizio richiesto.



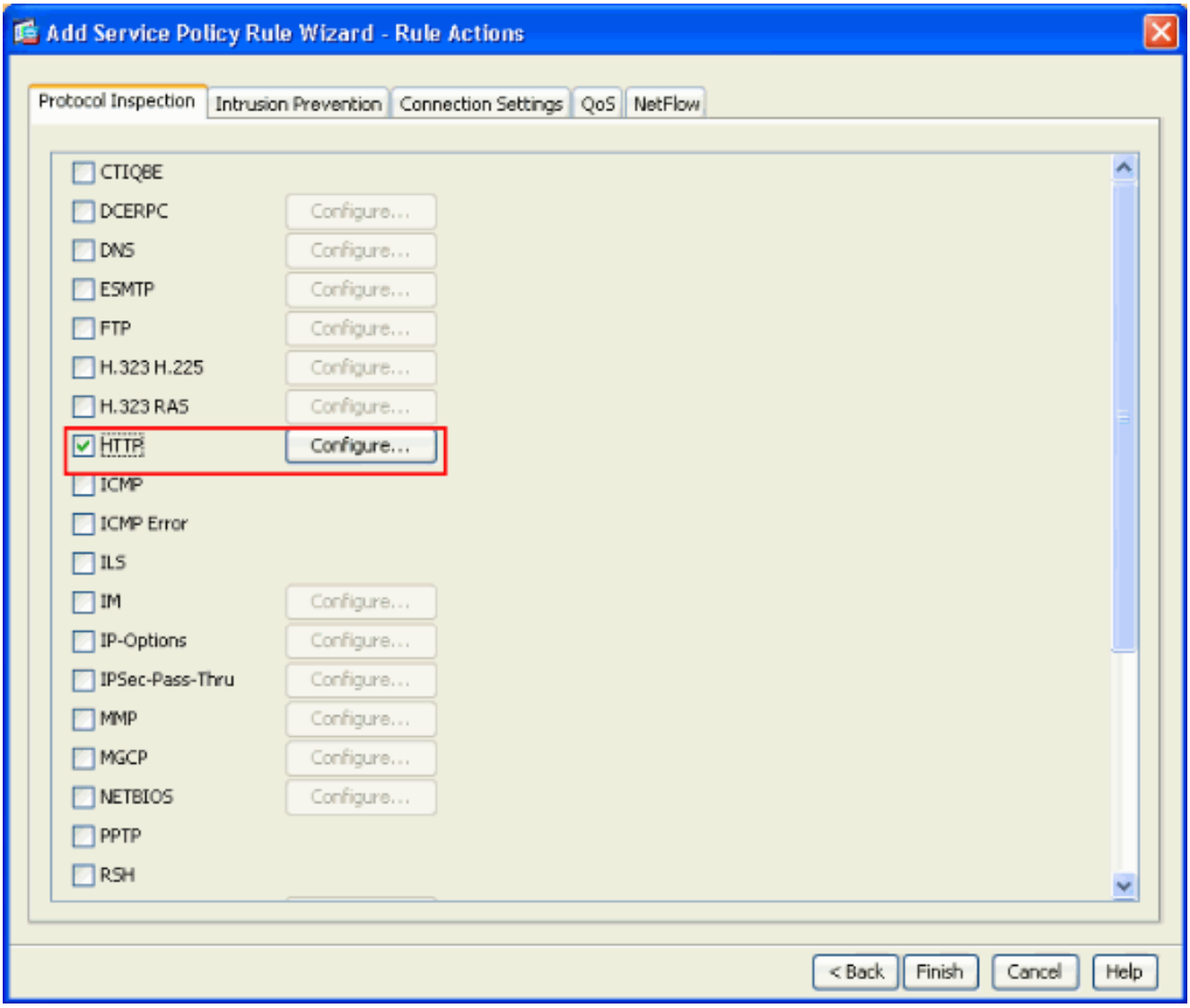
5. Nella finestra Sfoglia servizio, scegliere **HTTP** come servizio. Quindi fare clic su **OK**.



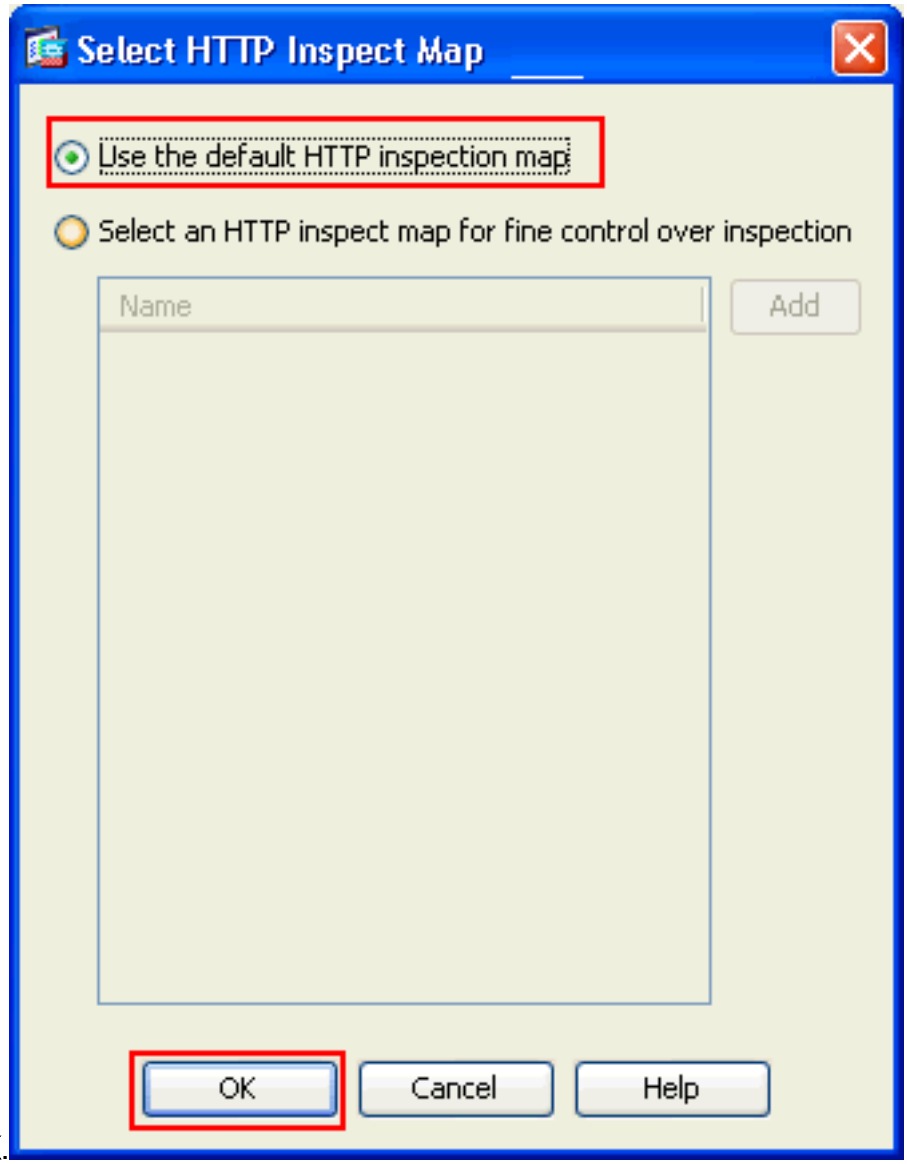
6. Dalla finestra Aggiunta guidata regola dei criteri del servizio - Corrispondenza traffico - Porta di destinazione è possibile verificare che il **servizio** scelto è **tcp/http**. Fare clic su **Next** (Avanti).



7. Nella finestra Aggiunta guidata regole dei criteri del servizio - Azioni regola selezionare la casella di controllo **HTTP**. Quindi, fare clic su **Configure** (Configura) accanto a **HTTP**.

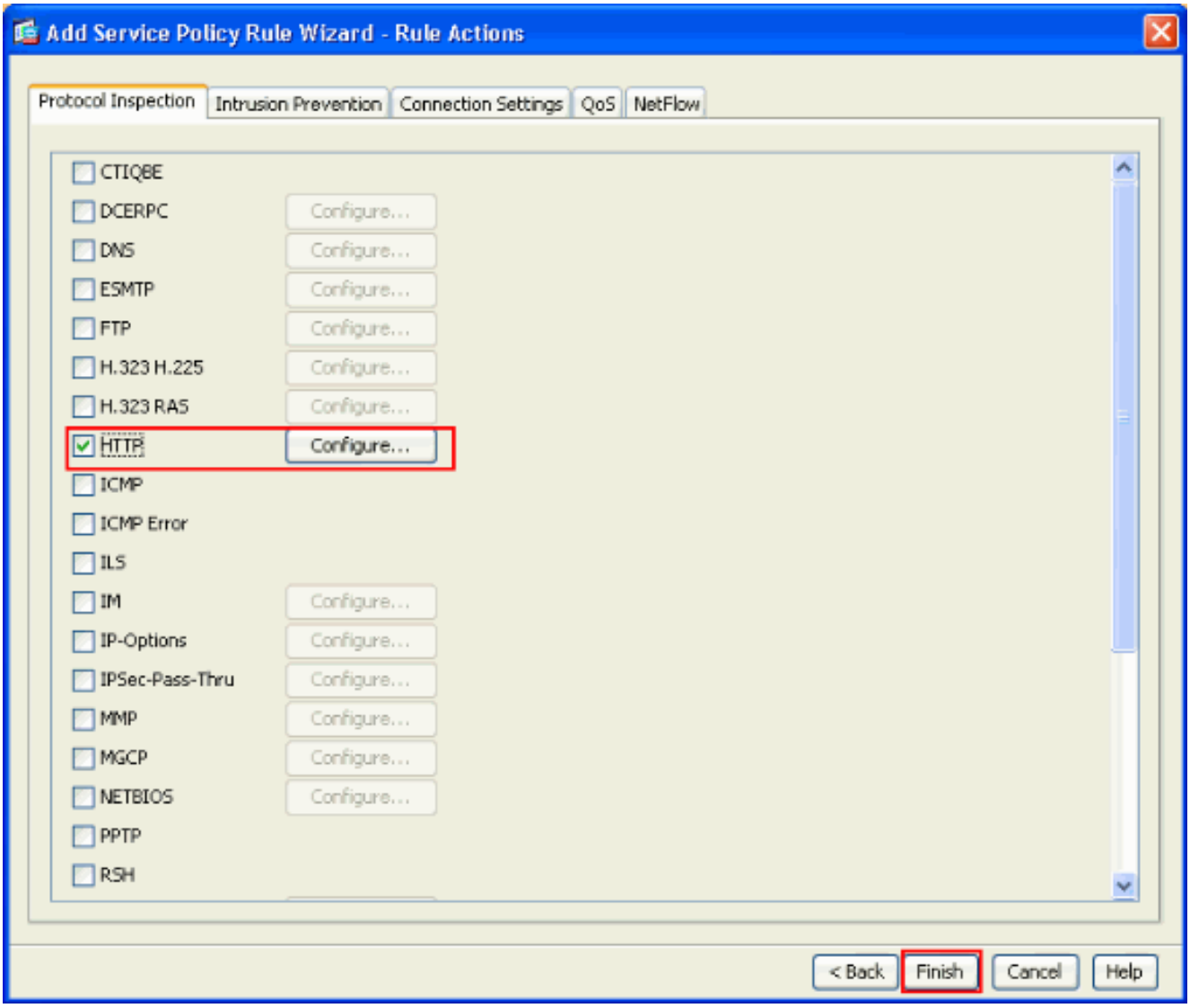


8. Nella finestra Seleziona mappa ispezione HTTP, selezionare il pulsante di opzione accanto a **Usa la mappa di ispezione HTTP predefinita**. In questo esempio viene utilizzata l'ispezione HTTP predefinita. Quindi fare clic su

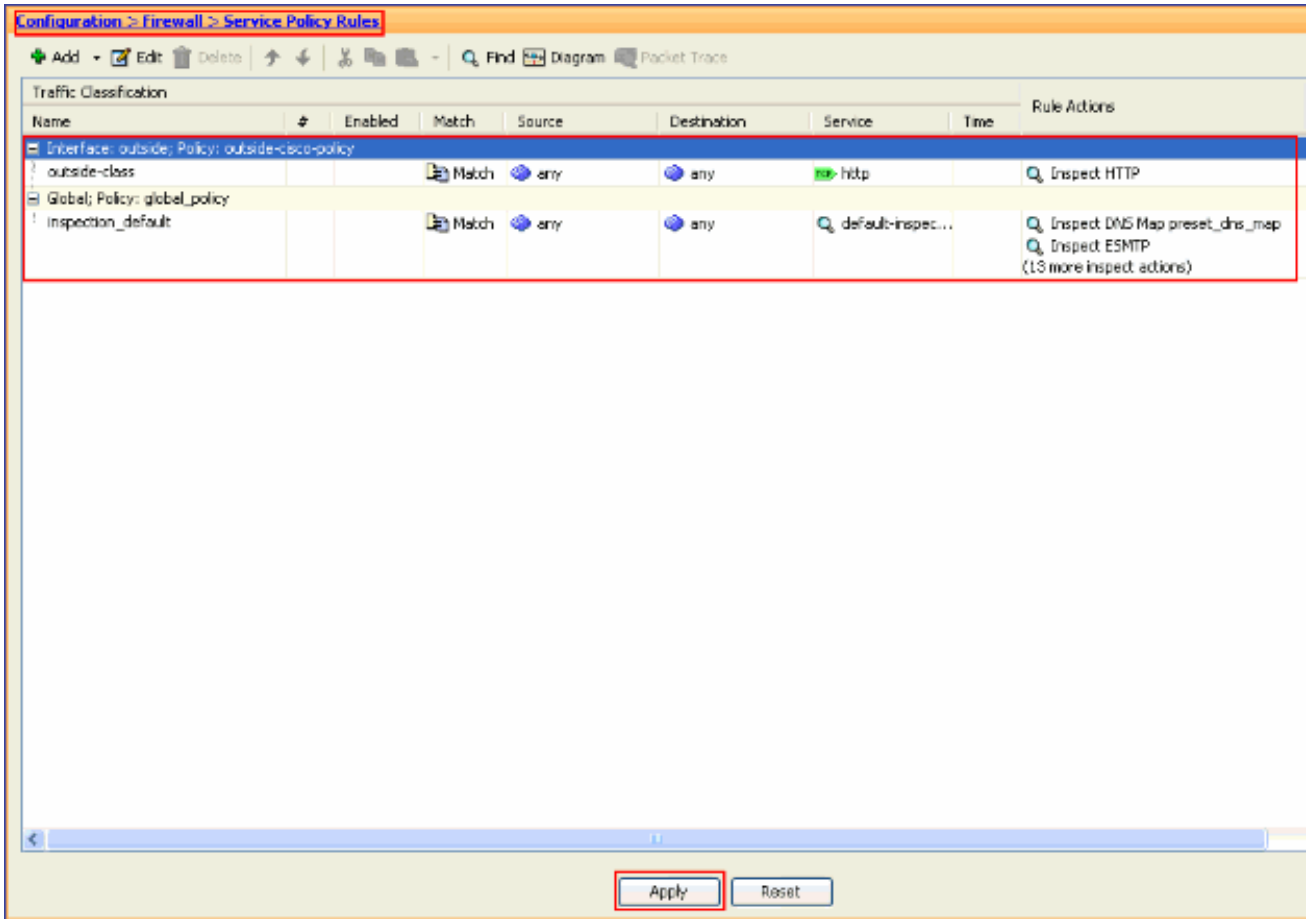


OK.

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



10. In **Configurazione > Firewall > Regole dei criteri di servizio** vengono visualizzati i criteri di servizio appena configurati **esternamente a cisco-policy** (per ispezionare il protocollo HTTP) insieme ai criteri di servizio predefiniti già presenti sull'accessorio. Per applicare la configurazione all'appliance Cisco ASA, fare clic su **Apply**.



Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Cisco Adaptive Security Device Manager
- RFC (Requests for Comments)
- Applicazione dell'ispezione del protocollo a livello di applicazione
- Documentazione e supporto tecnico – Cisco Systems