ASA 8.3 und höher: Festlegen des Timeout für SSH/Telnet/HTTP-Verbindungen mithilfe des MPF-Konfigurationsbeispiels

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die Cisco Adaptive Security Appliance (ASA) mit Version 8.3(1) und höher eines Timeouts, das für eine bestimmte Anwendung wie SSH/Telnet/HTTP spezifisch ist, im Gegensatz zu einer Konfiguration, die für alle Anwendungen gilt. In diesem Konfigurationsbeispiel wird das Modular Policy Framework (MPF) verwendet, das mit der Cisco Adaptive Security Appliance (ASA) Version 7.0 eingeführt wurde. Weitere Informationen finden Sie unter Verwenden des modularen Richtlinien-Frameworks.

In dieser Beispielkonfiguration ist die Cisco ASA so konfiguriert, dass die Workstation (10.77.241.129) Telnet/SSH/HTTP an den Remote-Server (10.1.1.1) hinter dem Router anschließen kann. Ein separates Zeitlimit für Verbindungen zum Telnet-/SSH-/HTTP-Datenverkehr wird ebenfalls konfiguriert. Alle anderen TCP-Datenverkehr haben weiterhin den normalen Zeitüberschreitungswert für die Verbindung, der **Timeout conn 1:00:00** zugeordnet ist.

Weitere Informationen finden Sie unter PIX/ASA 7.x und höher/FWSM: Legen Sie ein Timeout für SSH/Telnet/HTTP-Verbindungen mithilfe des MPF-Konfigurationsbeispiels für die gleiche Konfiguration auf der Cisco ASA mit Version 8.2 und früher fest.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ASA Security Appliance Software Version 8.3(1) mit Adaptive Security Device Manager (ASDM) 6.3.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

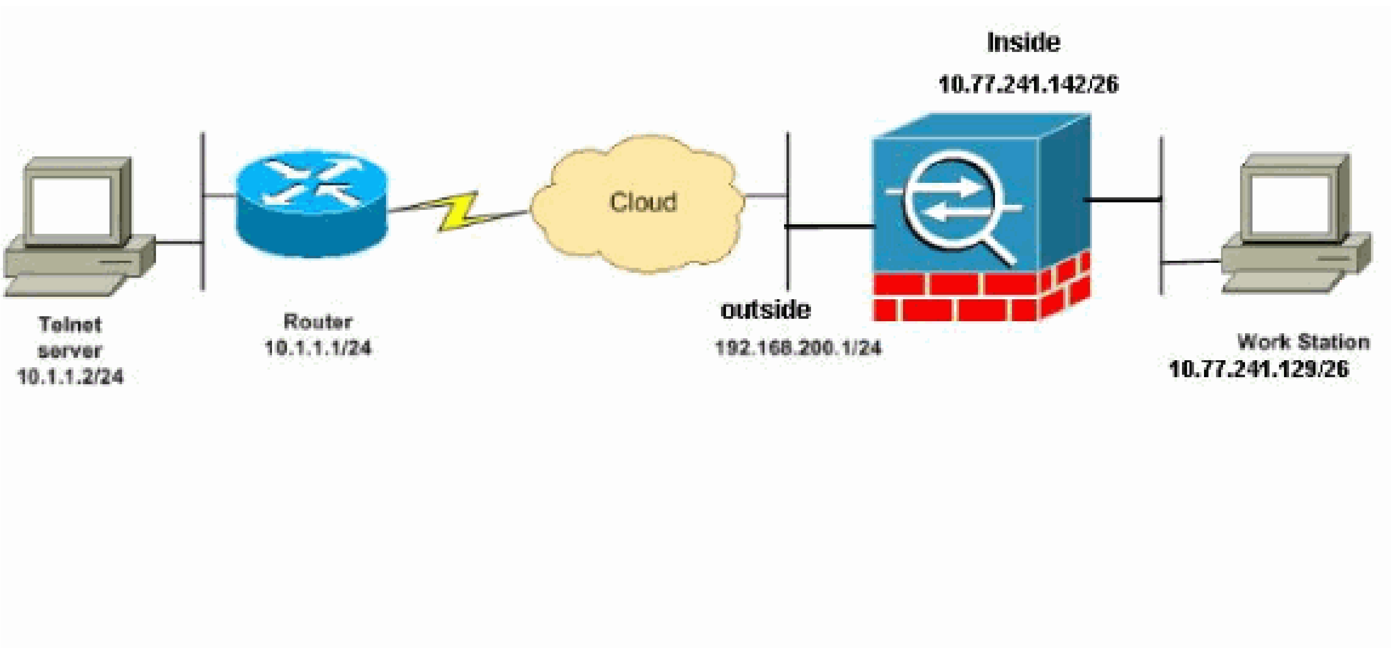
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- CLI-Konfiguration
- ASDM-Konfiguration

Hinweis: Diese CLI- und ASDM-Konfigurationen gelten für das Firewall Service Module (FWSM).

CLI-Konfiguration

ASA 8.3(1)-Konfiguration

```
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.
```

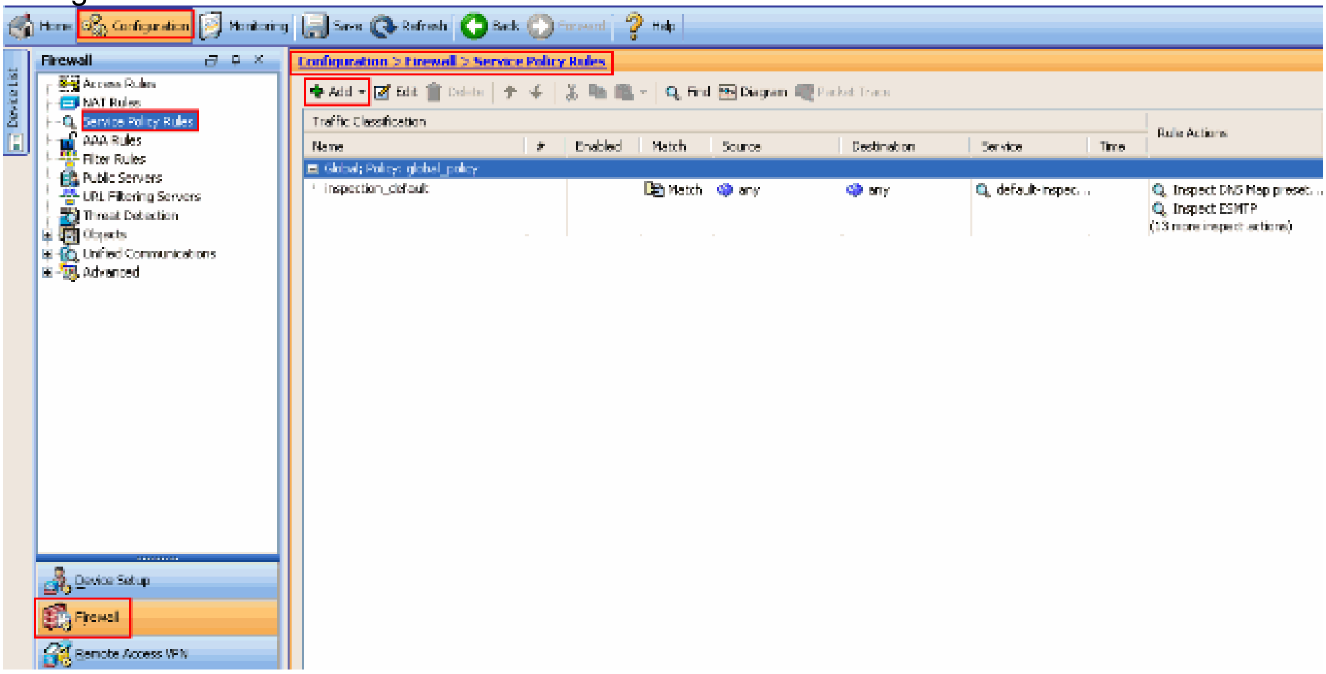
```
!--- You can apply the service-policy command to any
interface that !--- can be defined by the nameif
command.

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

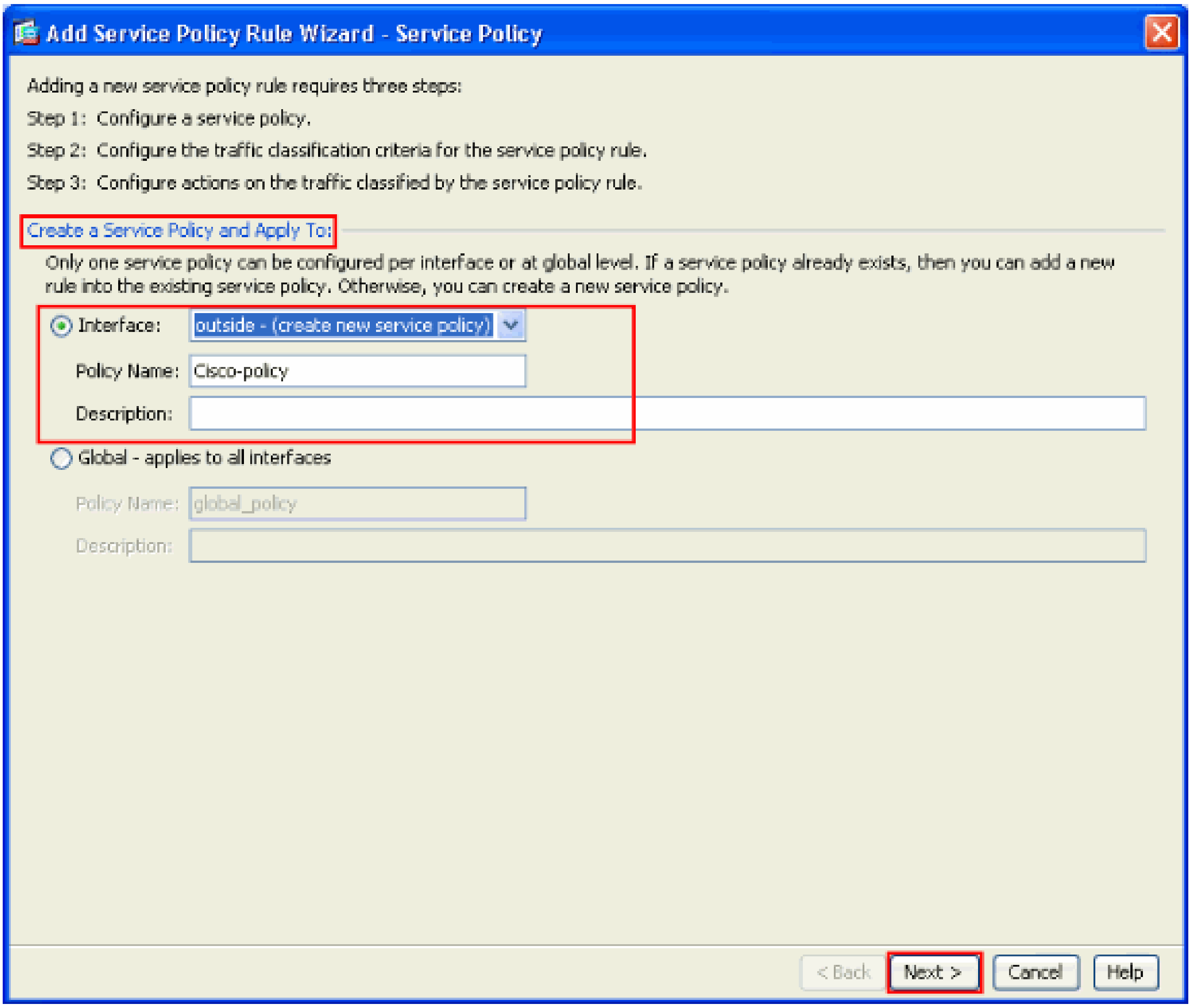
ASDM-Konfiguration

Führen Sie diese Schritte aus, um das Timeout für TCP-Verbindungen für Telnet-, SSH- und HTTP-Datenverkehr mithilfe von ASDM wie gezeigt einzurichten.

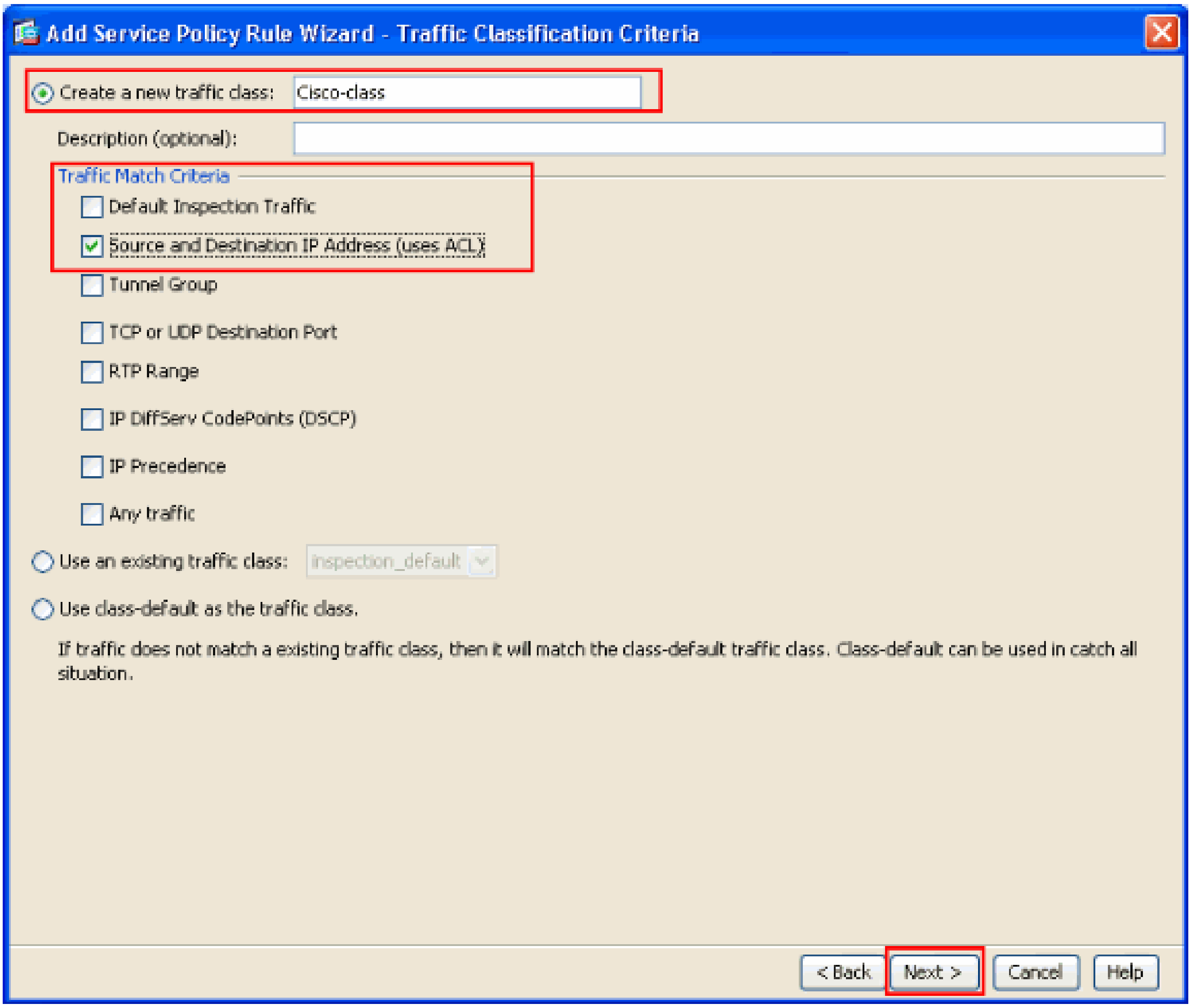
Hinweis: Unter Zulassen von HTTPS-Zugriff für ASDM finden Sie grundlegende Einstellungen, um über ASDM auf PIX/ASA zuzugreifen.

1. Wählen Sie **Konfiguration > Firewall > Service Policy Rules** und klicken Sie auf **Add**, um die Service Policy-Regel wie gezeigt zu konfigurieren.


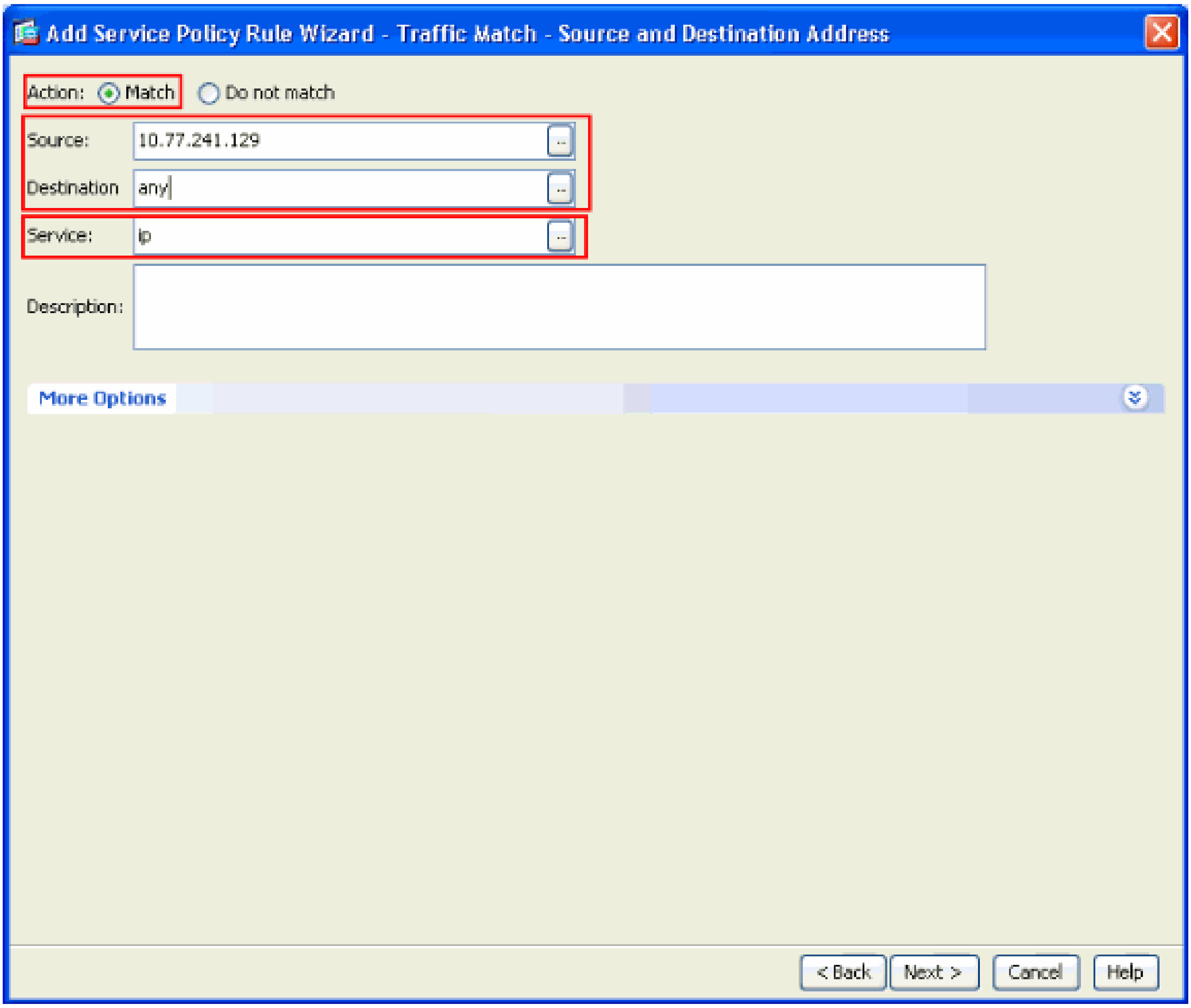
2. Wählen Sie im Fenster **Add Service Policy Wizard - Service Policy (Service-Richtlinie hinzufügen)** das Optionsfeld neben **Interface (Schnittstelle)** im Abschnitt **Create a Service Policy (Servicebichtlinie erstellen) und Apply To (Übernehmen auf) aus**. Wählen Sie nun die gewünschte Schnittstelle aus der Dropdown-Liste aus, und geben Sie einen **Policy Name (Richtliniennamen)** ein. Der in diesem Beispiel verwendete Richtlinienname lautet **Cisco-policy**. Klicken Sie anschließend auf **Weiter**.



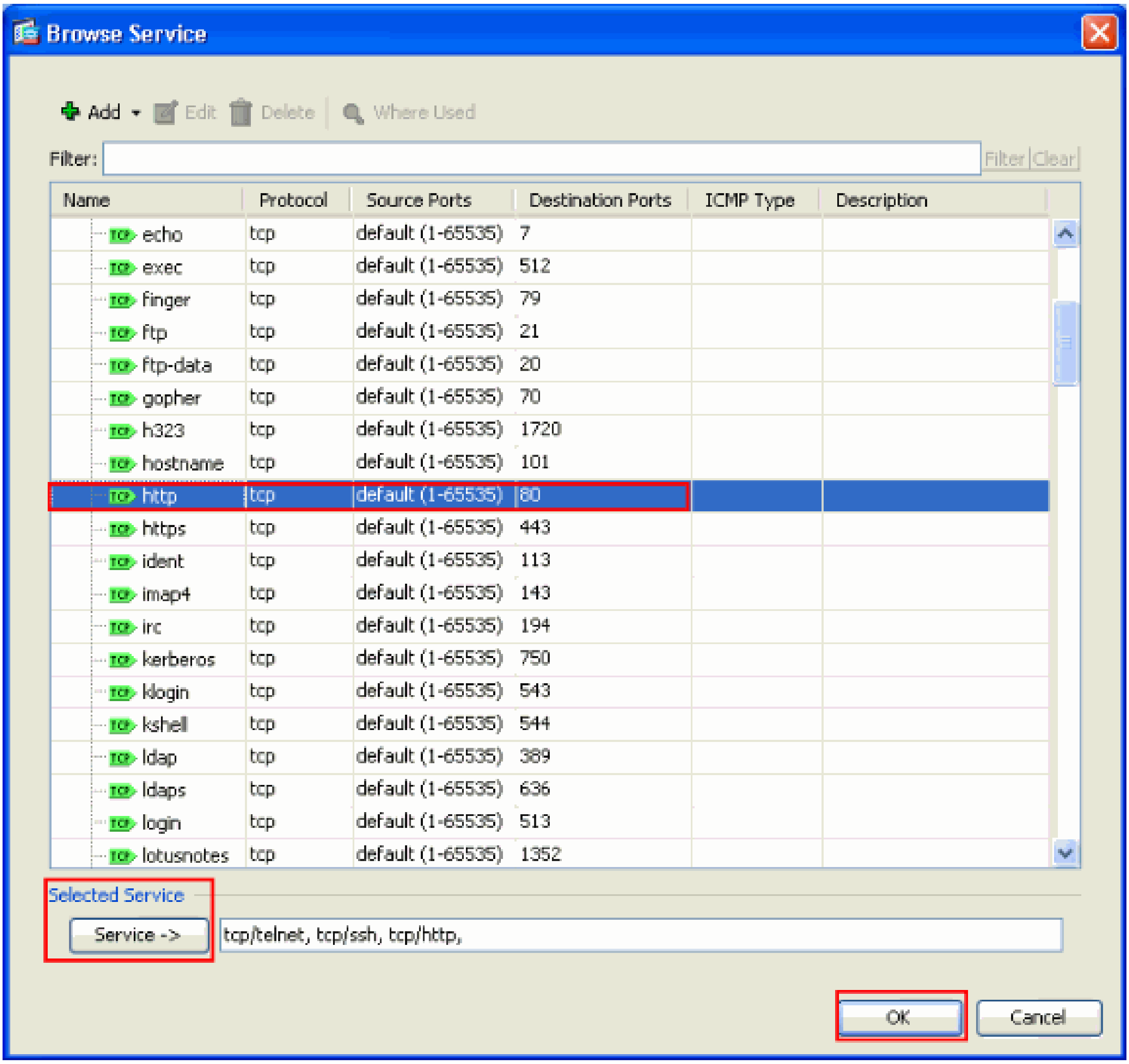
3. Erstellen Sie einen Klassenzuordnungsnamen **Cisco-class**, und aktivieren Sie das **Kontrollkästchen Source and Destination IP address (use ACL)** im Feld Traffic Match Criteria. Klicken Sie anschließend auf **Weiter**.



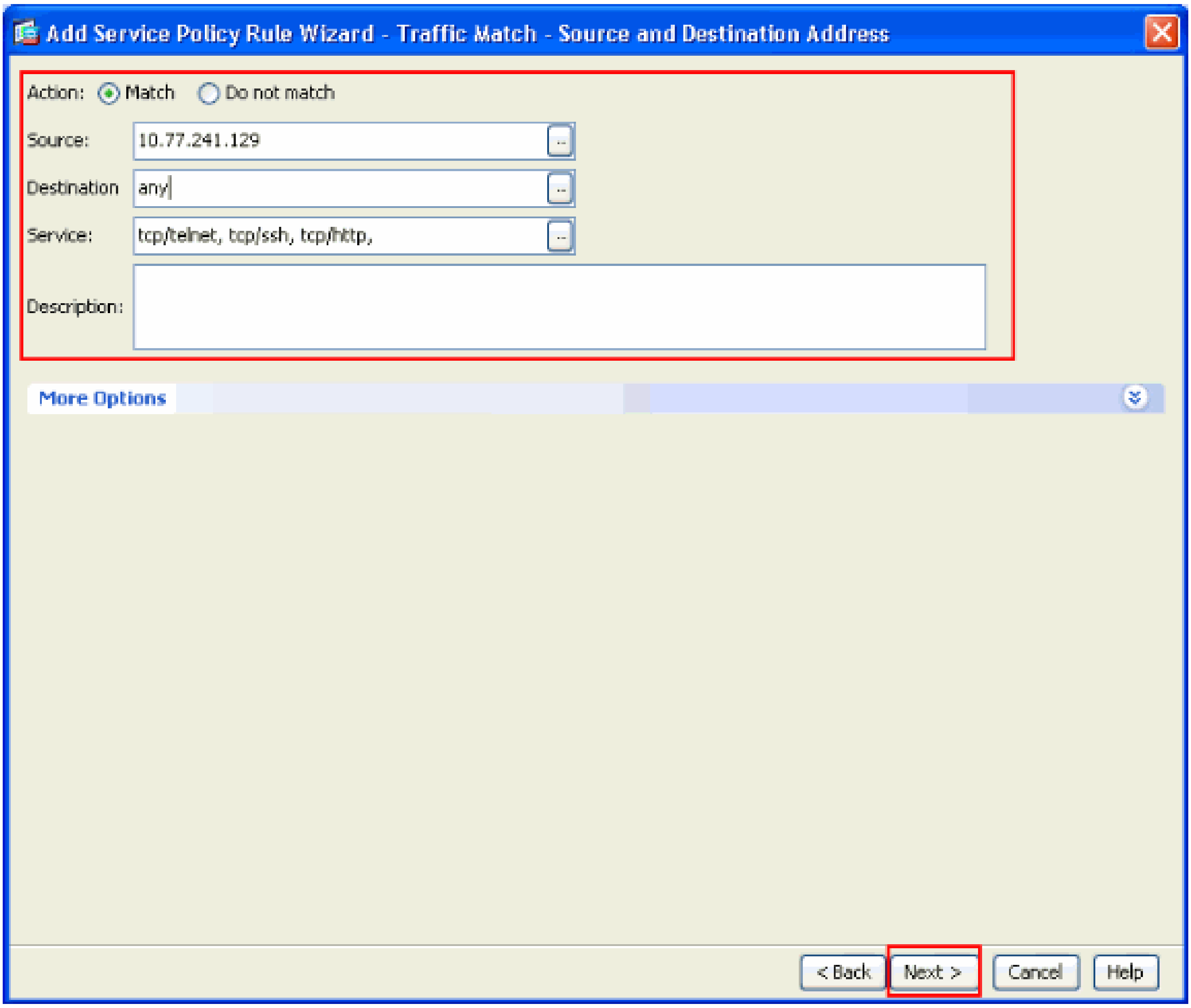
4. Wählen Sie im Fenster **Add Service Policy Rule Wizard (Regelassistent für Hinzufügen von Service-Richtlinien - Datenverkehrszuordnung - Quell- und Zieladresse** das Optionsfeld neben **Match (Übereinstimmung) aus**, und geben Sie dann die Quell- und Zieladresse wie gezeigt an. Klicken Sie auf die Dropdown-Schaltfläche neben **Service**, um die gewünschten Services
auszuwählen.



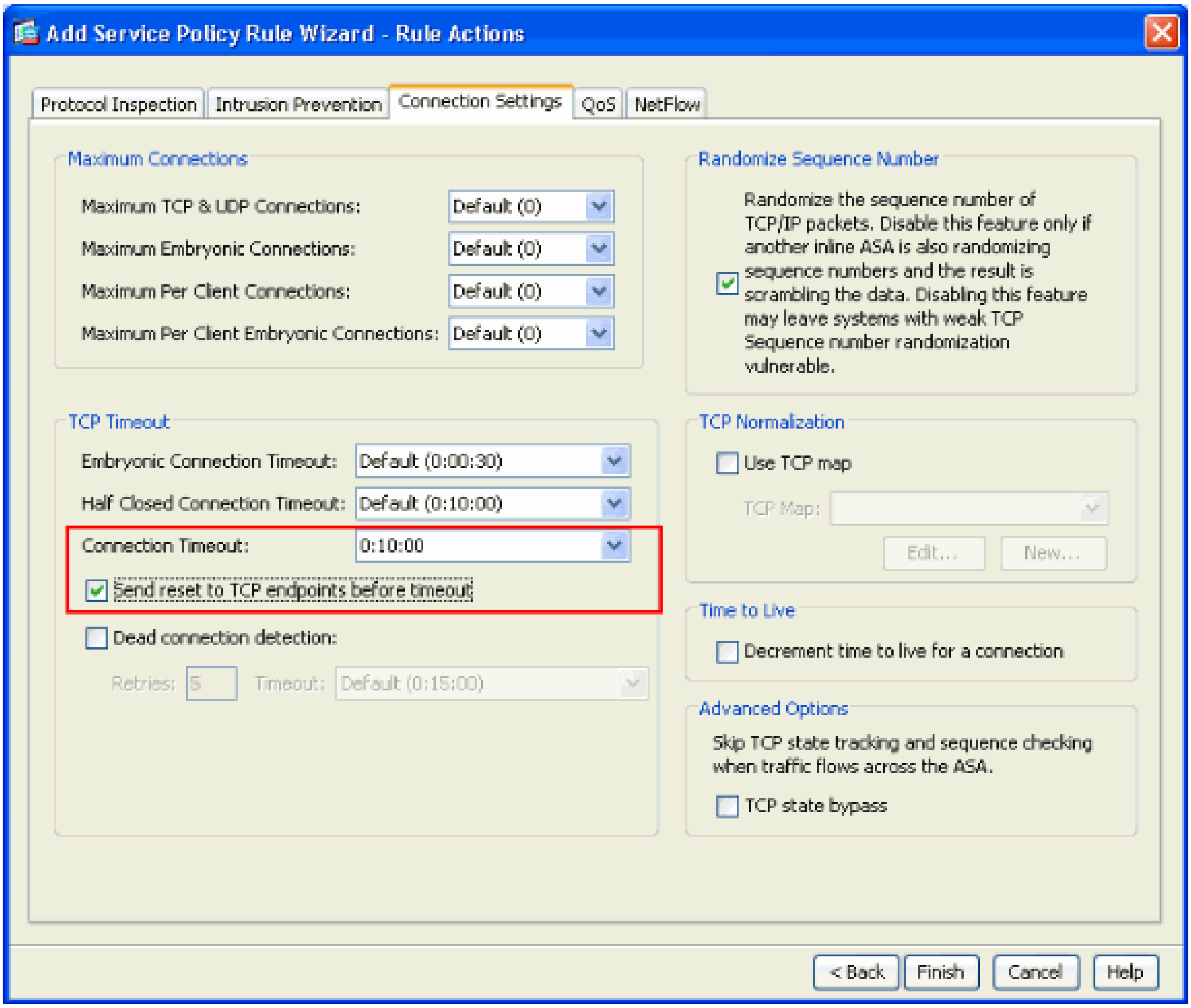
5. Wählen Sie die erforderlichen Services wie **Telnet**, **ssh** und **http aus**. Klicken Sie anschließend auf **OK**.



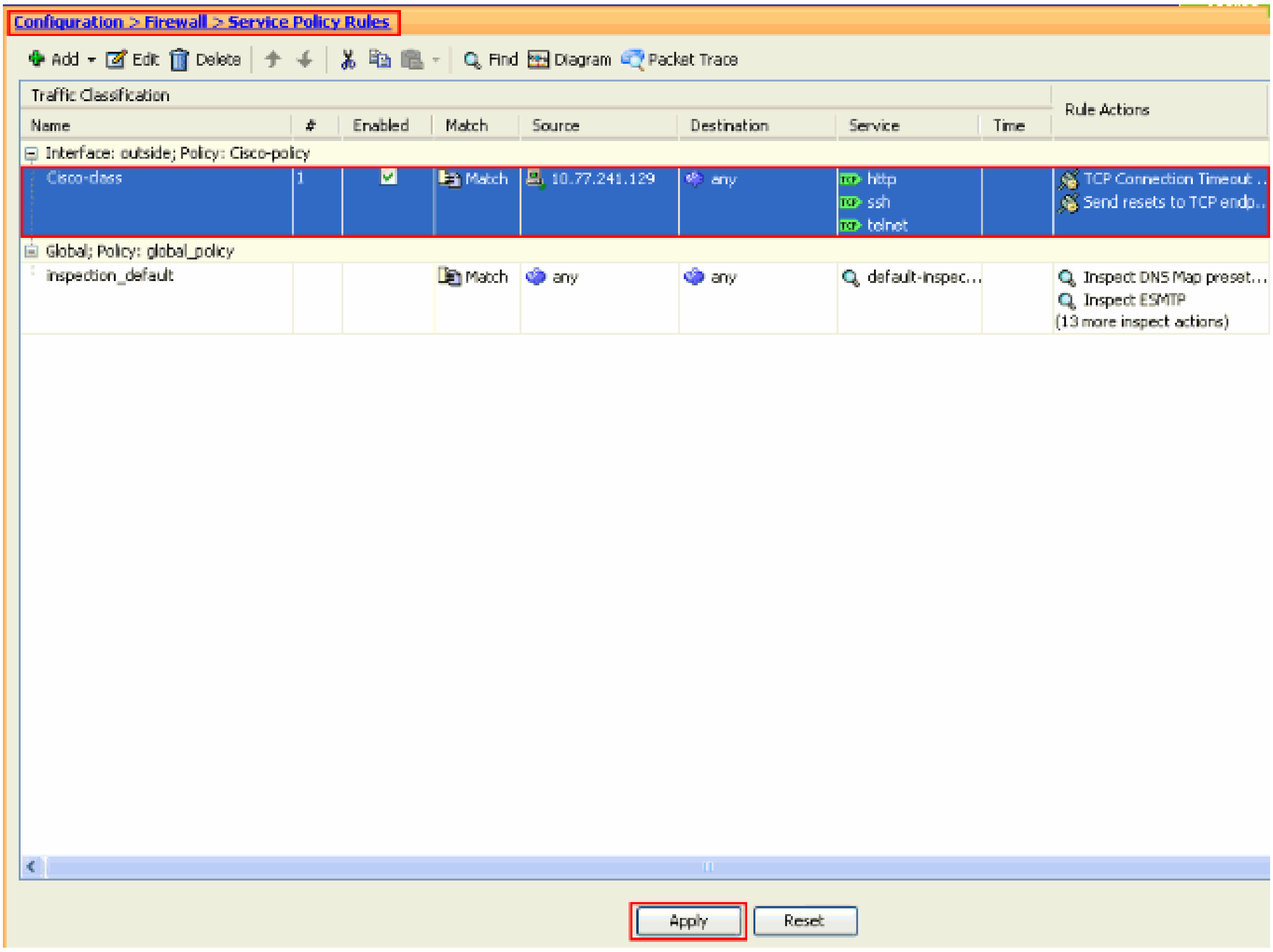
6. **Konfigurieren von Timeouts**. Klicken Sie auf **Weiter**.



7. Wählen Sie **Verbindungseinstellungen aus**, um das TCP-Verbindungs-Timeout auf 10 Minuten einzustellen. Aktivieren Sie außerdem das Kontrollkästchen **Rücksetzen an TCP-Endpunkte senden vor dem Timeout**. Klicken Sie auf **Fertig stellen**.



8. Klicken Sie auf **Apply**, um die Konfiguration auf die Sicherheits-Appliance anzuwenden.Damit ist die Konfiguration abgeschlossen.



Ebryonic-Timeout

Eine embryonale Verbindung ist die Verbindung, die halb offen ist oder z.B. der Drei-Wege-Handshake für sie noch nicht abgeschlossen ist. Es wird als SYN-Timeout auf der ASA definiert. Standardmäßig beträgt der SYN-Timeout auf der ASA 30 Sekunden. So konfigurieren Sie die embryonale Zeitüberschreitung:

```
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
```

Fehlerbehebung

Wenn Sie feststellen, dass das Verbindungszeitüberschreitung nicht mit dem MPF funktioniert, überprüfen Sie die Verbindung zum TCP-Initiieren. Beim Problem kann es sich um eine Umkehr der Quell- und Ziel-IP-Adresse handeln, oder eine falsch konfigurierte IP-Adresse in der Zugriffsliste stimmt nicht mit der in MPF überein, um den neuen Timeout-Wert festzulegen oder das Standard-Timeout für die Anwendung zu ändern. Erstellen Sie einen Zugriffslisteneintrag (Quelle und Ziel) entsprechend der Initiierung der Verbindung, um das Verbindungszeitlimit mit MPF festzulegen.

Zugehörige Informationen

- Cisco Adaptive Security Device Manager
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems