ASA 8.3 e mais atrasado: Ajuste o timeout de conexão SSH/Telnet/HTTP usando o exemplo da configuração MPF

Índice

Introdução

Este documento fornece uma configuração de exemplo para o Cisco Adaptive Security Appliance (ASA) com versão 8.3(1) ou posterior de um tempo limite que é específico para alguma aplicação em particular, como SSH/Telnet/HTTP, diferente de um que se aplica a toda aplicações. Este exemplo de configuração usa a estrutura de política modular (MPF) que foi introduzida na versão 7.0 adaptável da ferramenta de segurança de Cisco (ASA). Refira a utilização da estrutura de política modular para mais informação.

Nesta configuração de exemplo, Cisco ASA é configurado para permitir a estação de trabalho (10.77.241.129) a Telnet/SSH/HTTP ao servidor remoto (10.1.1.1) atrás do roteador. Um intervalo de conexão separada ao tráfego Telnet/SSH/HTTP é configurado igualmente. Todo tráfego TCP restante continua a ter o valor de timeout da conexão normal associado com a **conexão 1:00:00 do intervalo**.

Refira PIX/ASA 7.x e later/FWSM: Ajuste o timeout de conexão SSH/Telnet/HTTP usando o exemplo da configuração MPF para a mesma configuração em Cisco ASA com versões 8.2 e anterior.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão de software da ferramenta de segurança de Cisco ASA 8.3(1) com Security Device Manager adaptável (ASDM) 6.3.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

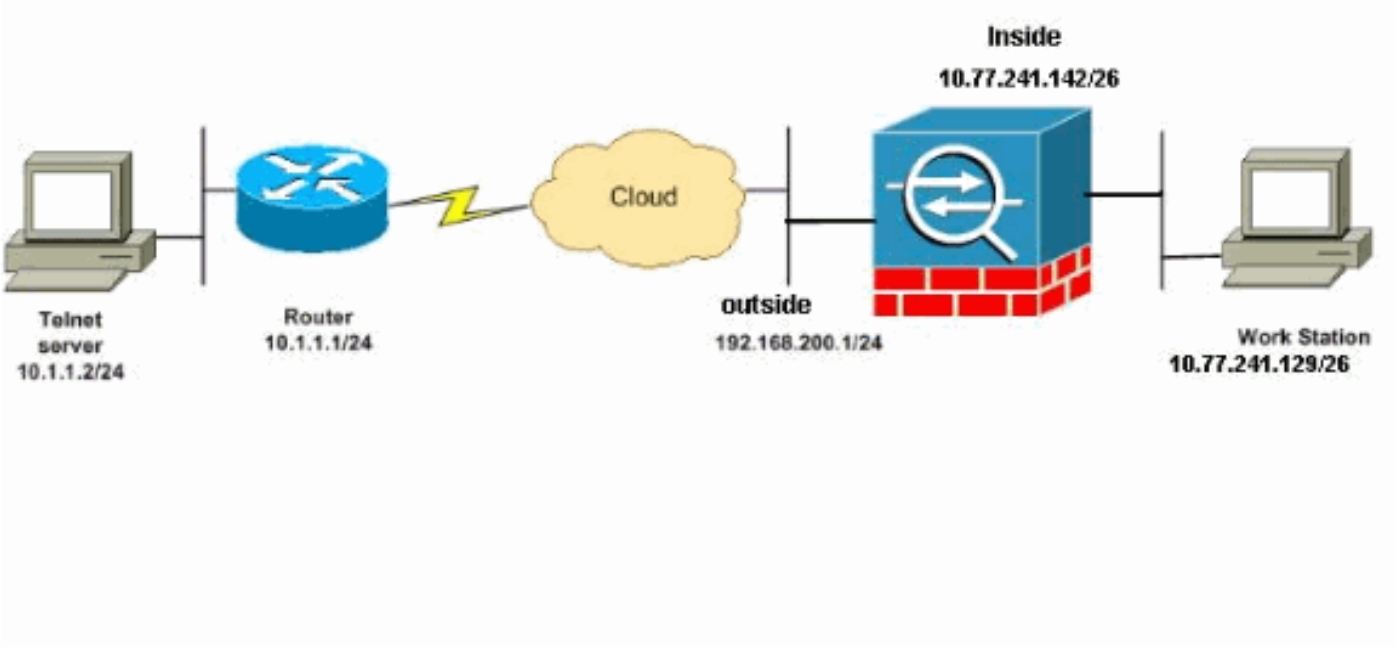
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918, que foram usados em um ambiente de laboratório.

Configurações

Este documento utiliza as seguintes configurações:

- Configuração de CLI
- Configuração ASDM

Nota: Este o CLI e as configurações ASDM são aplicáveis ao módulo firewall service (FWSM).

Configuração de CLI

Configuração 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-
```

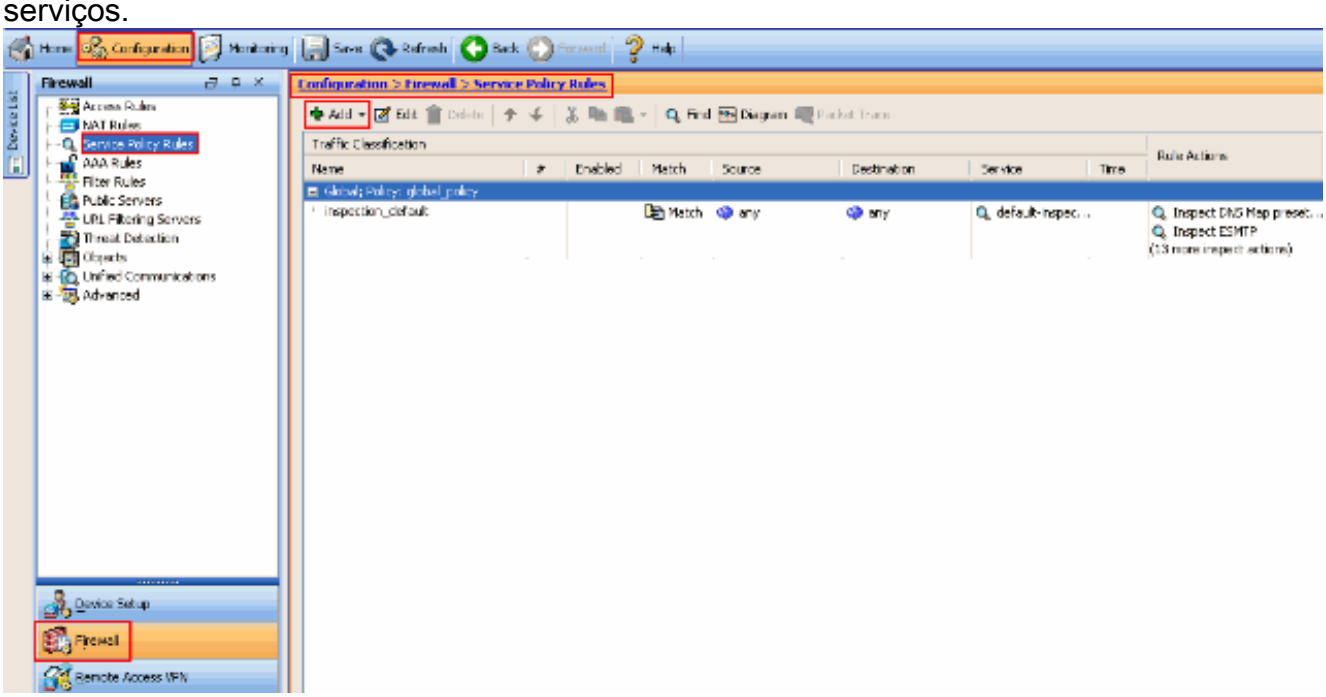
```
map Cisco-class match access-list outside_mpc class-map
inspection_default match default-inspection-traffic ! !
policy-map global_policy class inspection_default
inspect dns maximum-length 512 inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect 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
```

Configuração ASDM

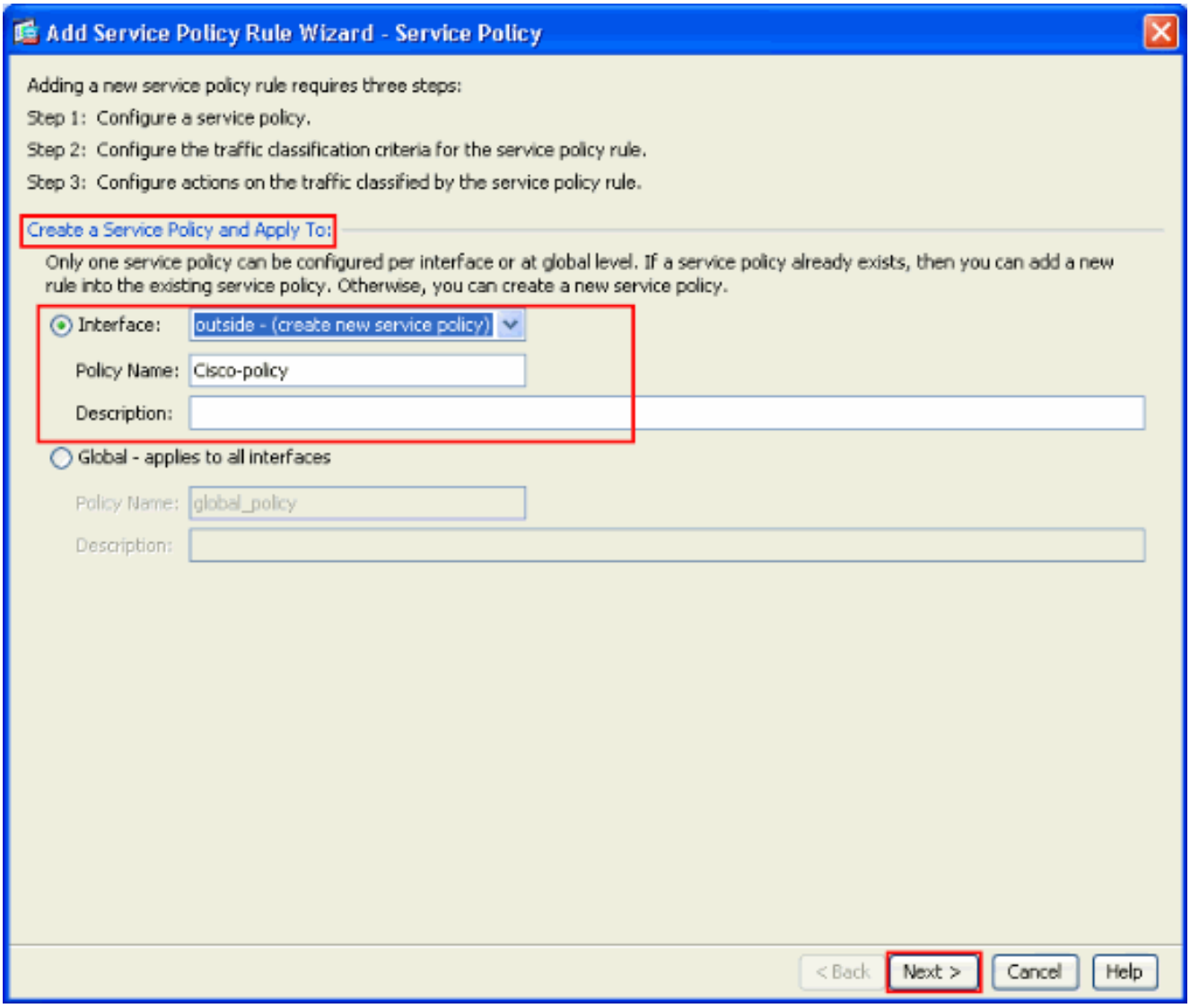
Termine estas etapas a fim estabelecer o intervalo de conexão de TCP para o telnet, o SSH e o tráfego de HTTP usando o ASDM como mostrado.

Nota: Refira permitir que o acesso HTTPS para o ASDM para configurações básicas a fim alcançar o PIX/ASA com o ASDM.

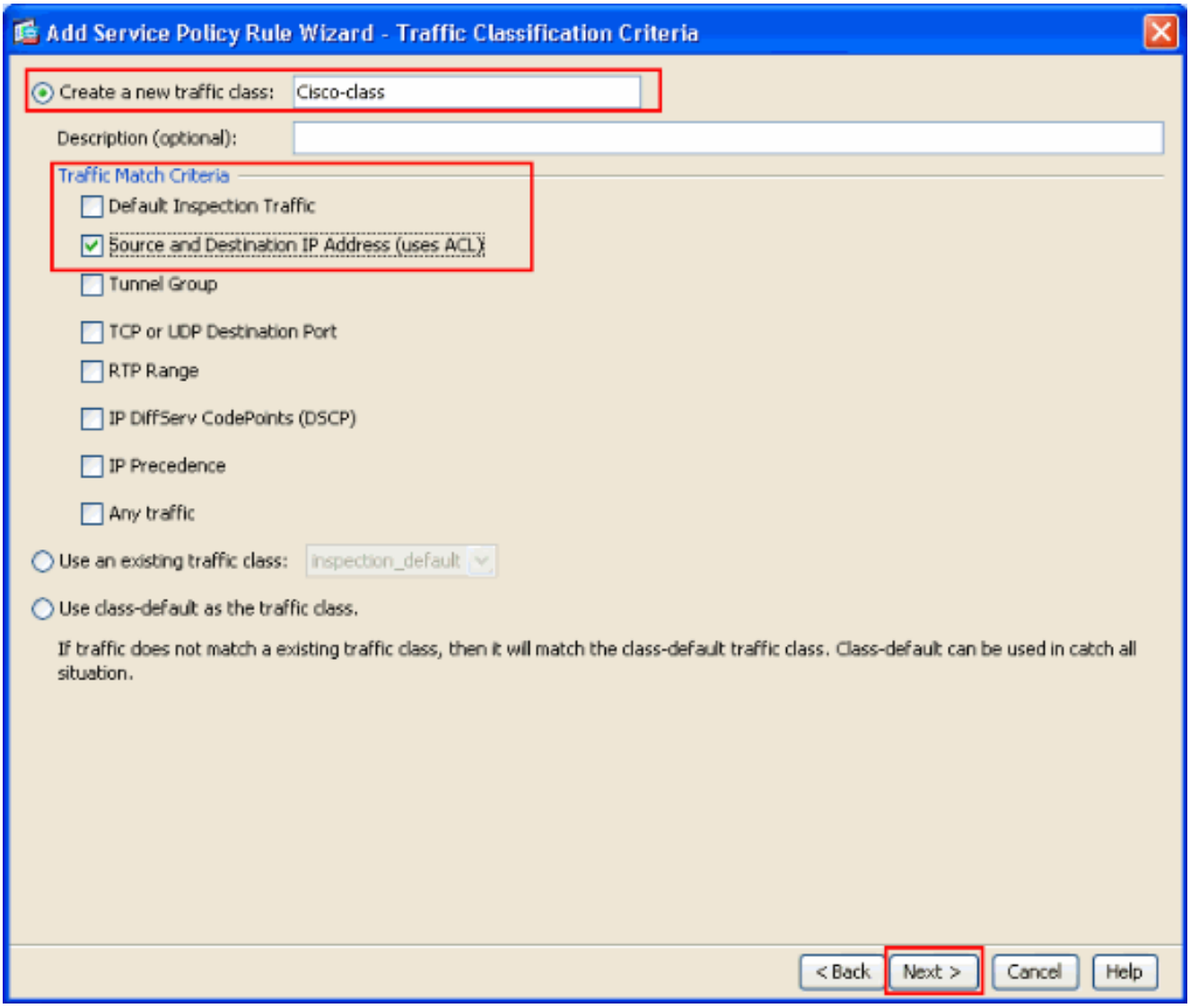
1. Escolha **regras da configuração > do Firewall > da política de serviços** e o clique **adiciona** a fim configurar como mostrado a regra da política de serviços.



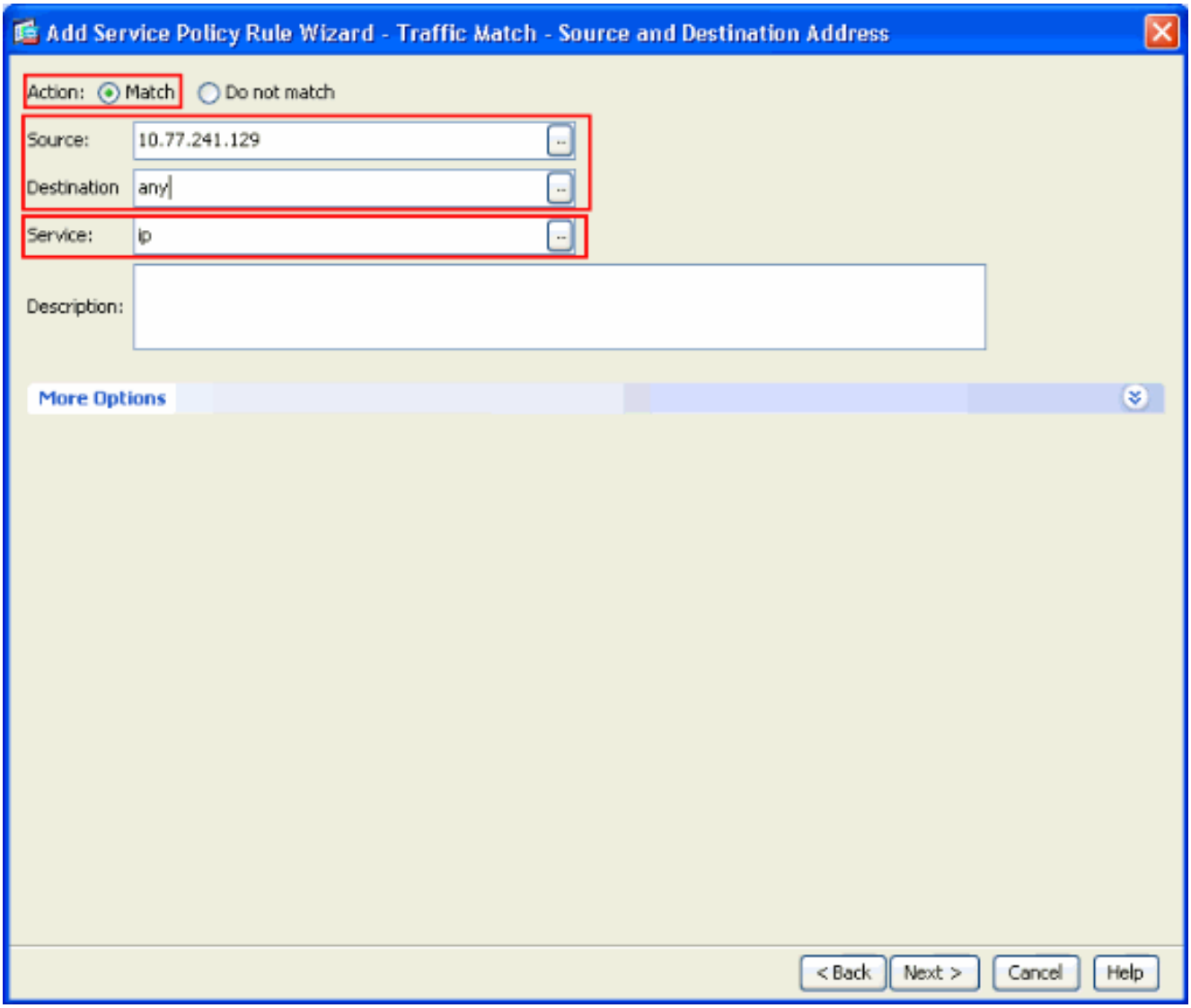
2. **Do assistente da regra da política de serviços adicionar -** O indicador da **política de serviços**, escolhe o botão de rádio ao lado da **relação** sob a **criação uma política de serviços e aplica-se** para secionar. Agora escolha a interface desejada da lista de drop-down e forneça um **nome da política**. O nome da política usado neste exemplo é Cisco-**política**. Então, clique **em seguida**.



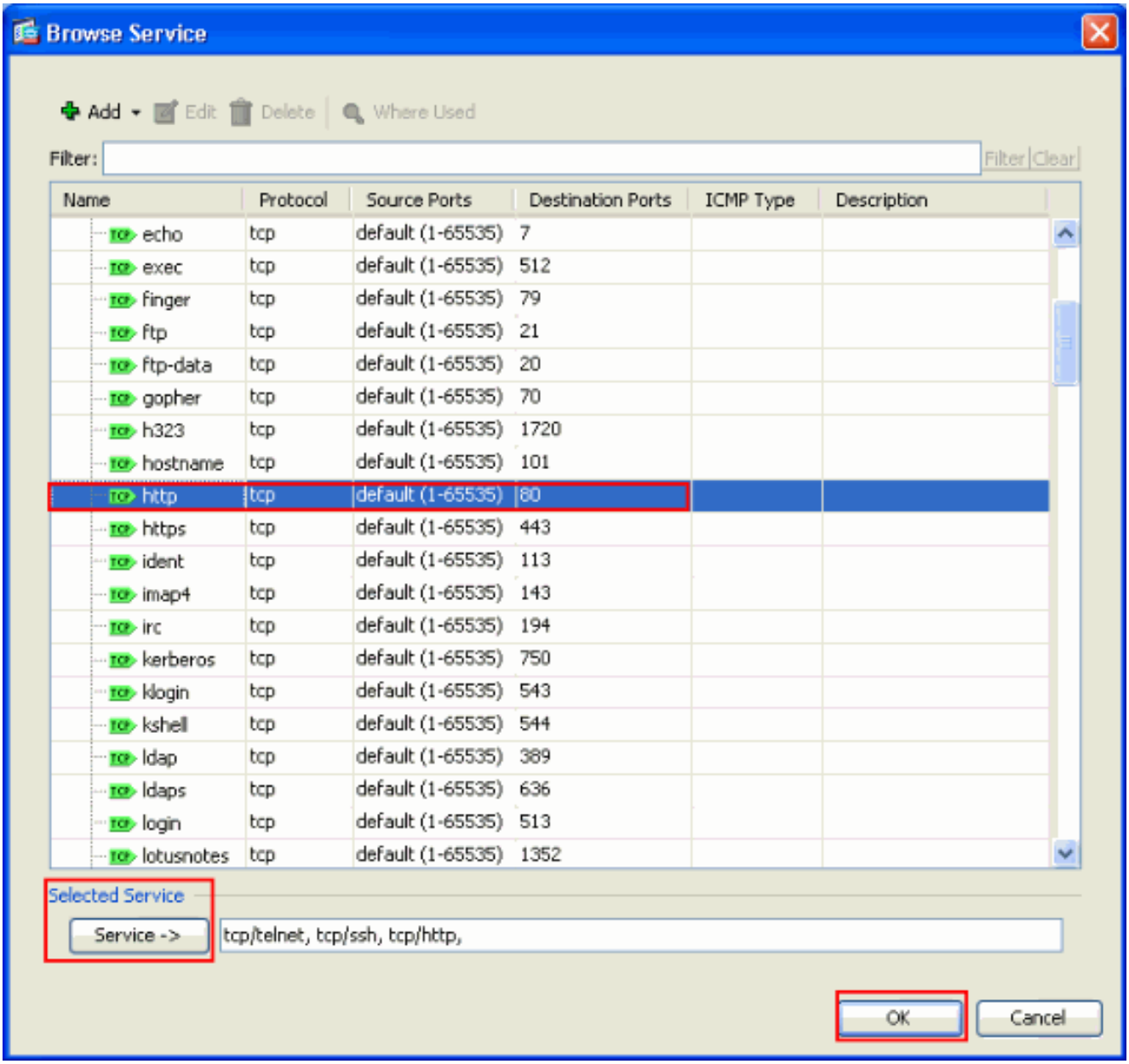
3. Crie uma Cisco-**classe do** nome de mapa da classe e verifique a caixa de verificação do **endereço IP de origem e de destino (usos ACL) nos** critérios de verificação de repetição de dados do tráfego. Então, clique **em seguida**.



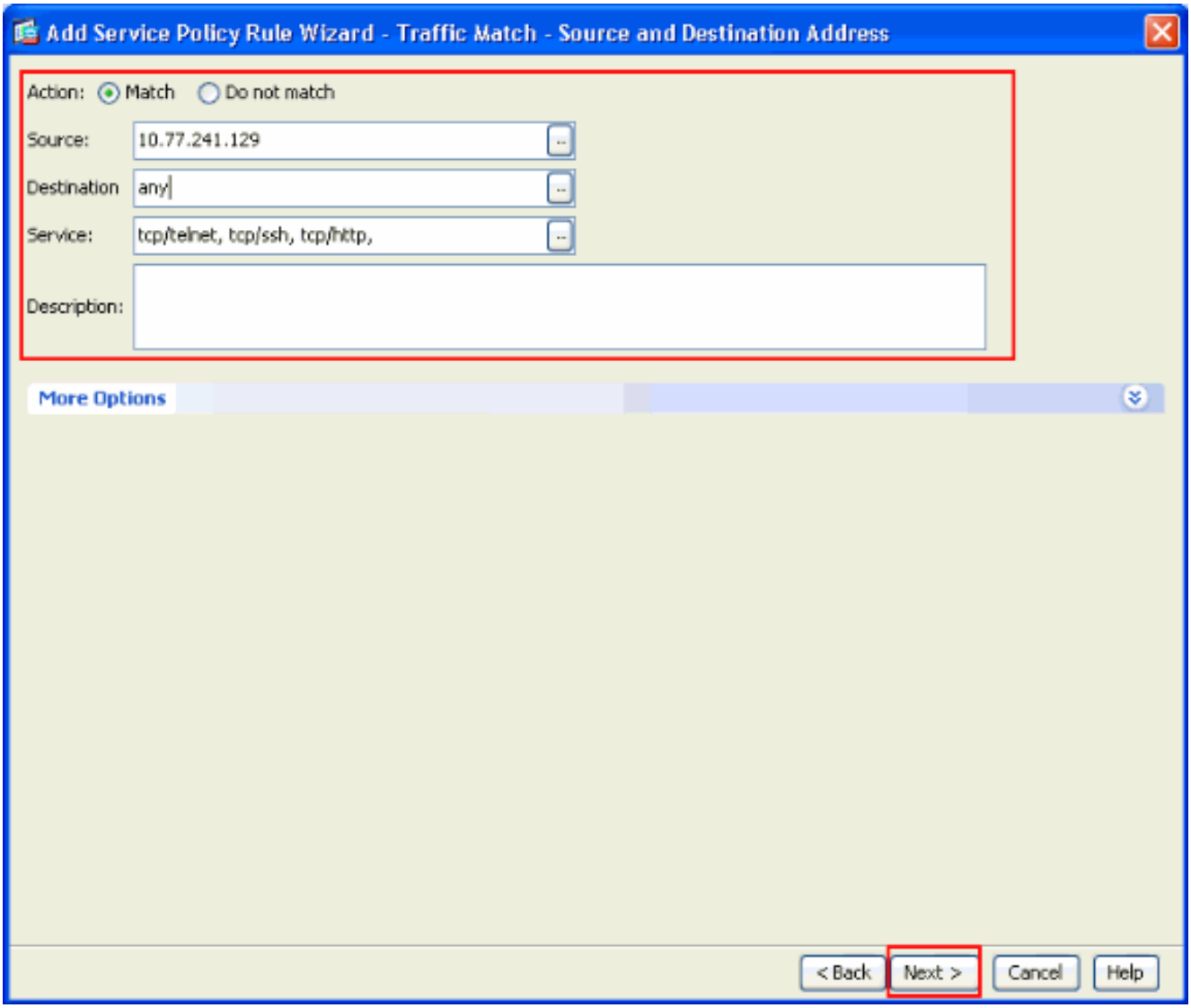
4. **Do assistente da regra da política de serviços adicionar - Fósforo do tráfego - A fonte e a janela de endereço de Destnation**, escolhem o botão de rádio ao lado do **fósforo** e fornecem então a fonte e o endereço de destino como mostrado. Clique o botão da gota-para baixo ao lado do **serviço** para escolher os serviços
requerido.



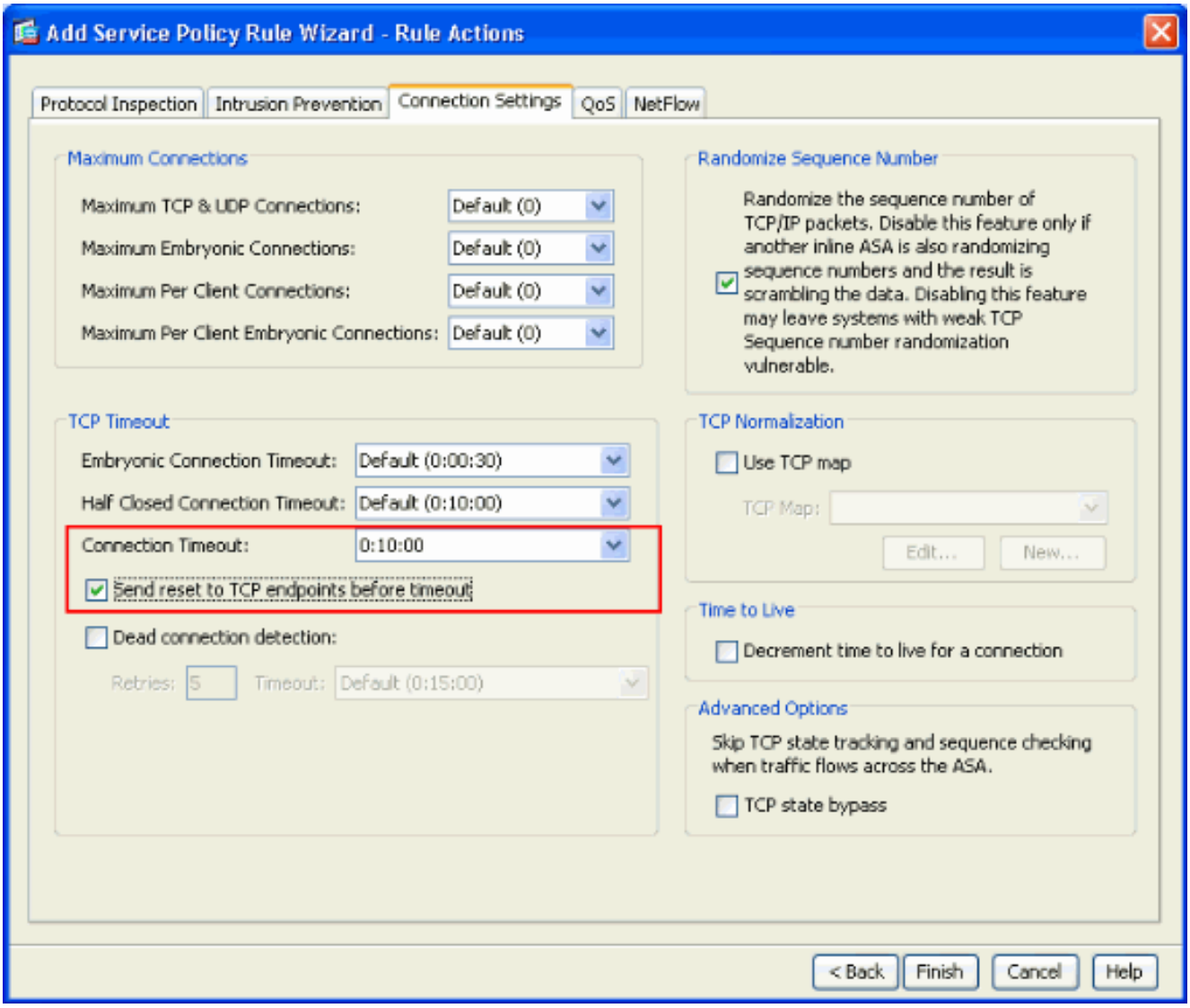
5. Selecione os serviços requerido tais como o **telnet**, o **ssh** e o **HTTP**. Então, **APROVAÇÃO do** clique.



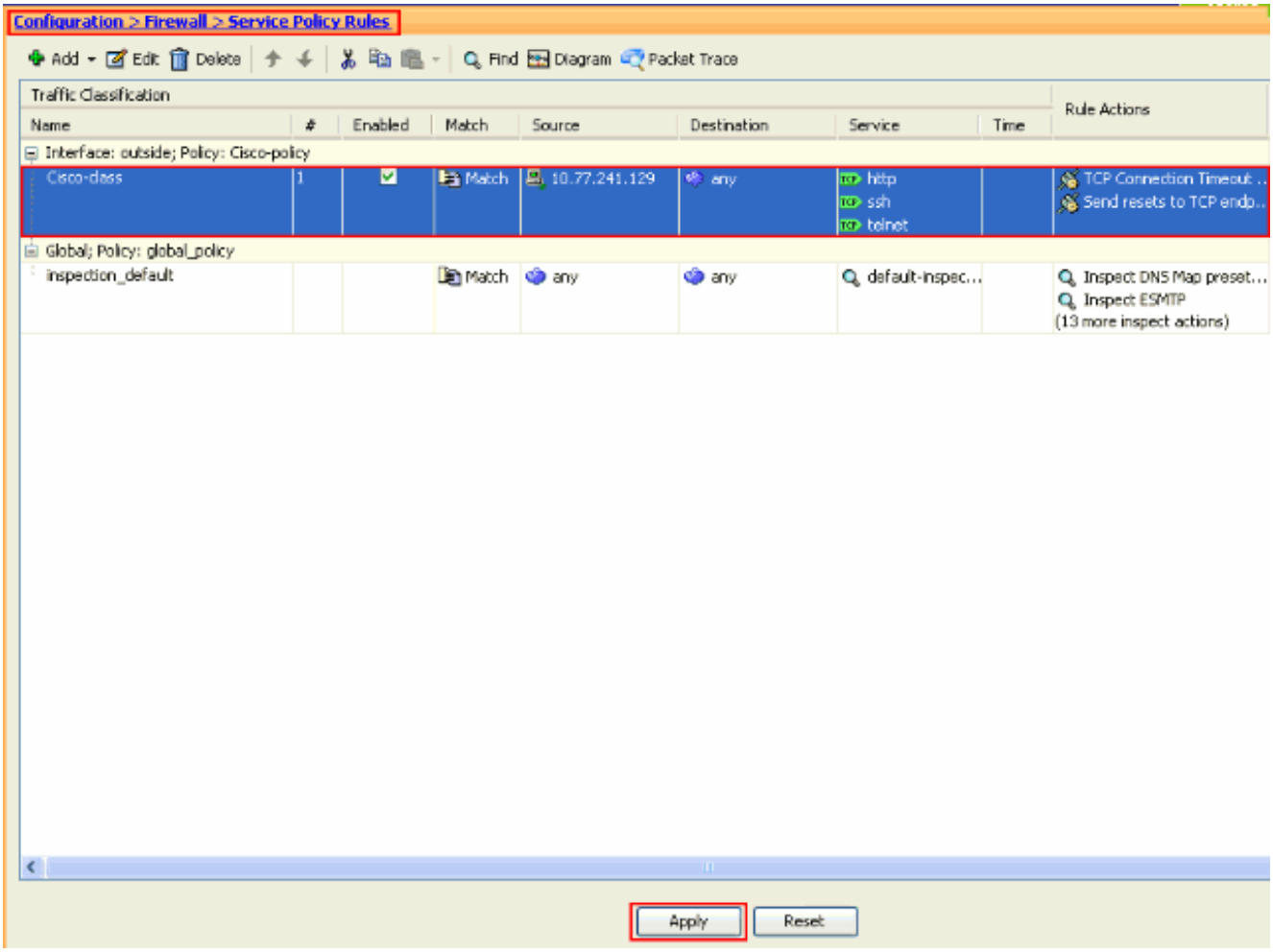
6. **Configurar intervalos**. Clique em Next.



7. Escolha **configurações de conexão** a fim estabelecer o intervalo de conexão de TCP como os minutos 10. Também, verifique a **emissão restaurada aos pontos finais de TCP antes da** caixa de verificação do **intervalo**. Clique em
Finish.



8. O clique **aplica-se** a fim aplicar a configuração à ferramenta de segurança.Isto termina a configuração.



Intervalo de Ebryonic

Uma conexão embriônica é a conexão que é meia abre ou, por exemplo, o cumprimento de três vias não foi terminado para ele. É definido como o Intervalo de SYN no ASA. À revelia, o Intervalo de SYN no ASA é 30 segundos. Isto é como configurar o intervalo embrionário:

```
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
```

Troubleshooting

Se você encontra que o timeout de conexão não trabalha com o MPF, a seguir verifique a conexão da iniciação TCP. A edição pode ser uma reversão do endereço IP de origem e de destino, ou um endereço IP de Um ou Mais Servidores Cisco ICM NT desconfigurado na lista de acessos não combina no MPF para ajustar o valor de timeout novo ou para mudar o timeout padrão para o aplicativo. Crie uma entrada de lista de acesso (fonte e destino) de acordo com a iniciação de conexão a fim ajustar o timeout de conexão com MPF.

Informações Relacionadas

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems