ASA 8.3 y posterior: Fije el tiempo de espera de la conexión SSH/Telnet/HTTP usando el ejemplo de la configuración MPF

Contenido

Introducción

Este documento proporciona una configuración de ejemplo de Cisco Adaptive Security Appliance (ASA) con la versión 8.3(1) y posteriores de un tiempo de espera que es específico de una determinada aplicación como SSH/Telnet/HTTP, en comparación con uno que se aplica a todas las aplicaciones. Este ejemplo de configuración utiliza el Marco de políticas modular (MPF) que fue introducido en la versión 7.0 adaptante del dispositivo de seguridad de Cisco (ASA). Refiérase usando el Marco de políticas modular para más información.

En esta configuración de muestra, Cisco ASA se configura para permitir el puesto de trabajo (10.77.241.129) a Telnet/SSH/HTTP al servidor remoto (10.1.1.1) detrás del router. Un descanso de otra conexión al tráfico Telnet/SSH/HTTP también se configura. Todo el otro tráfico TCP continúa teniendo el valor de agotamiento del tiempo de la conexión normal asociado a la **conexión de tiempo de espera 1:00:00**.

Refiera al PIX/ASA 7.x y later/FWSM: Fije el tiempo de espera de la conexión SSH/Telnet/HTTP usando el ejemplo de la configuración MPF para la misma configuración en Cisco ASA con las versiones 8.2 y anterior.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en la versión de software del dispositivo de seguridad de Cisco ASA 8.3(1) con el Administrador de dispositivos de seguridad adaptante (ASDM) 6.3.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

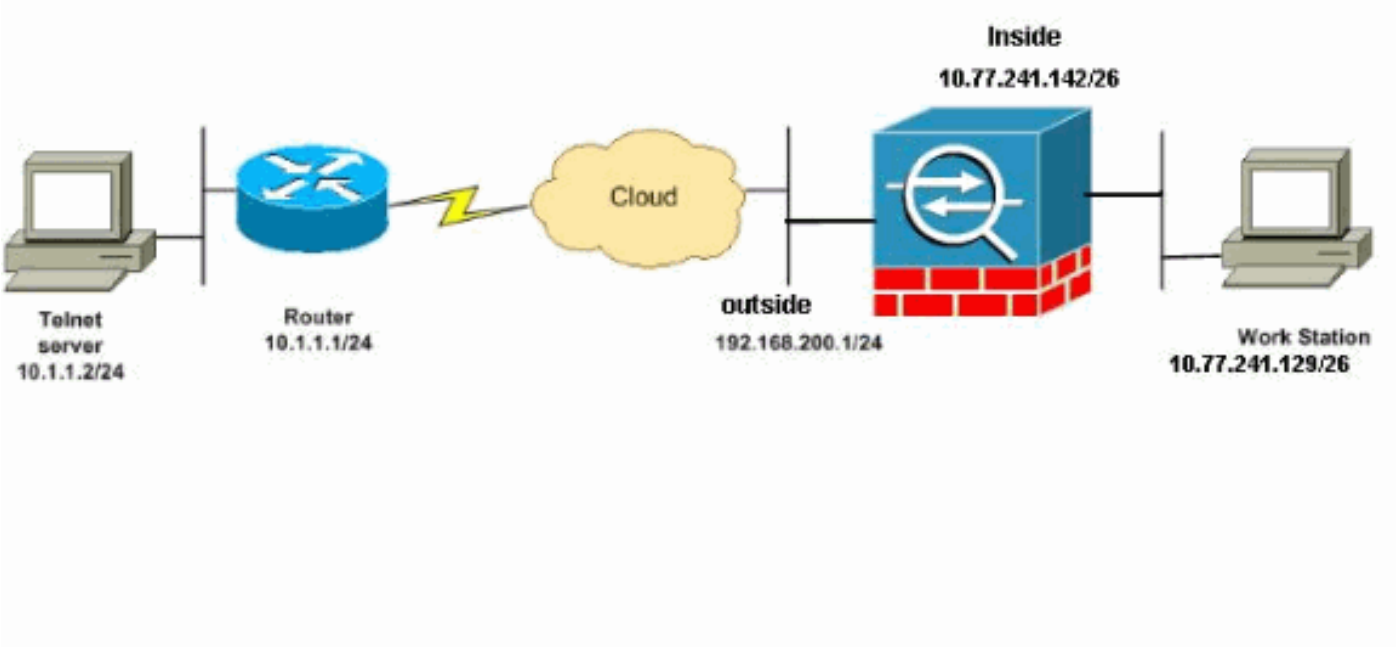
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son los direccionamientos del RFC 1918, que se han utilizado en un ambiente de laboratorio.

Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración de CLI
- Configuración de ASDM

Nota: Este el CLI y las Configuraciones de ASDM son aplicables al módulo firewall service (FWSM).

Configuración de CLI

Configuración 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. !---
```

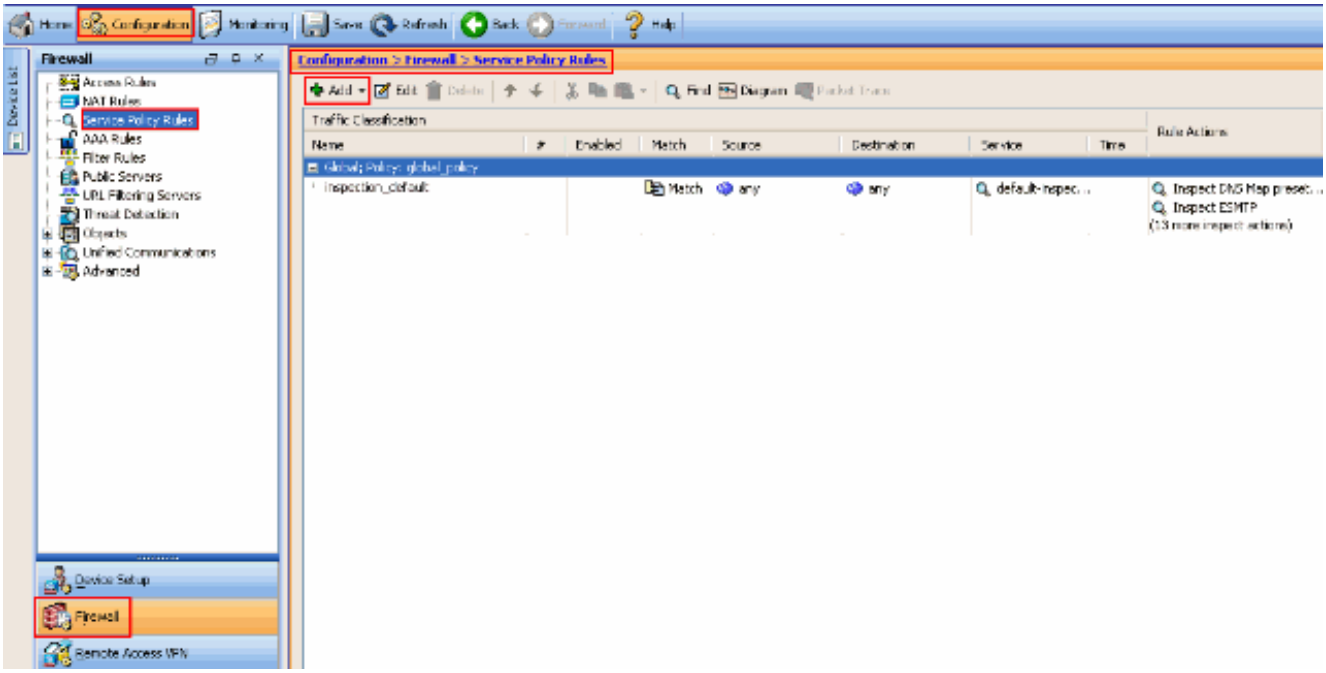
```
Assign the parameters to be matched by class map. class-
map Cisco-class match access-list outside_mpc class-map
inspection_default match default-inspection-traffic ! !
policy-map global_policy class inspection_default
inspect dns maximum-length 512 inspect ftp inspect h323
h225 inspect h323 ras 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
```

Configuración de ASDM

Complete estos pasos para configurar el descanso de conexión TCP para Telnet, SSH y el tráfico HTTP usando el ASDM como se muestra.

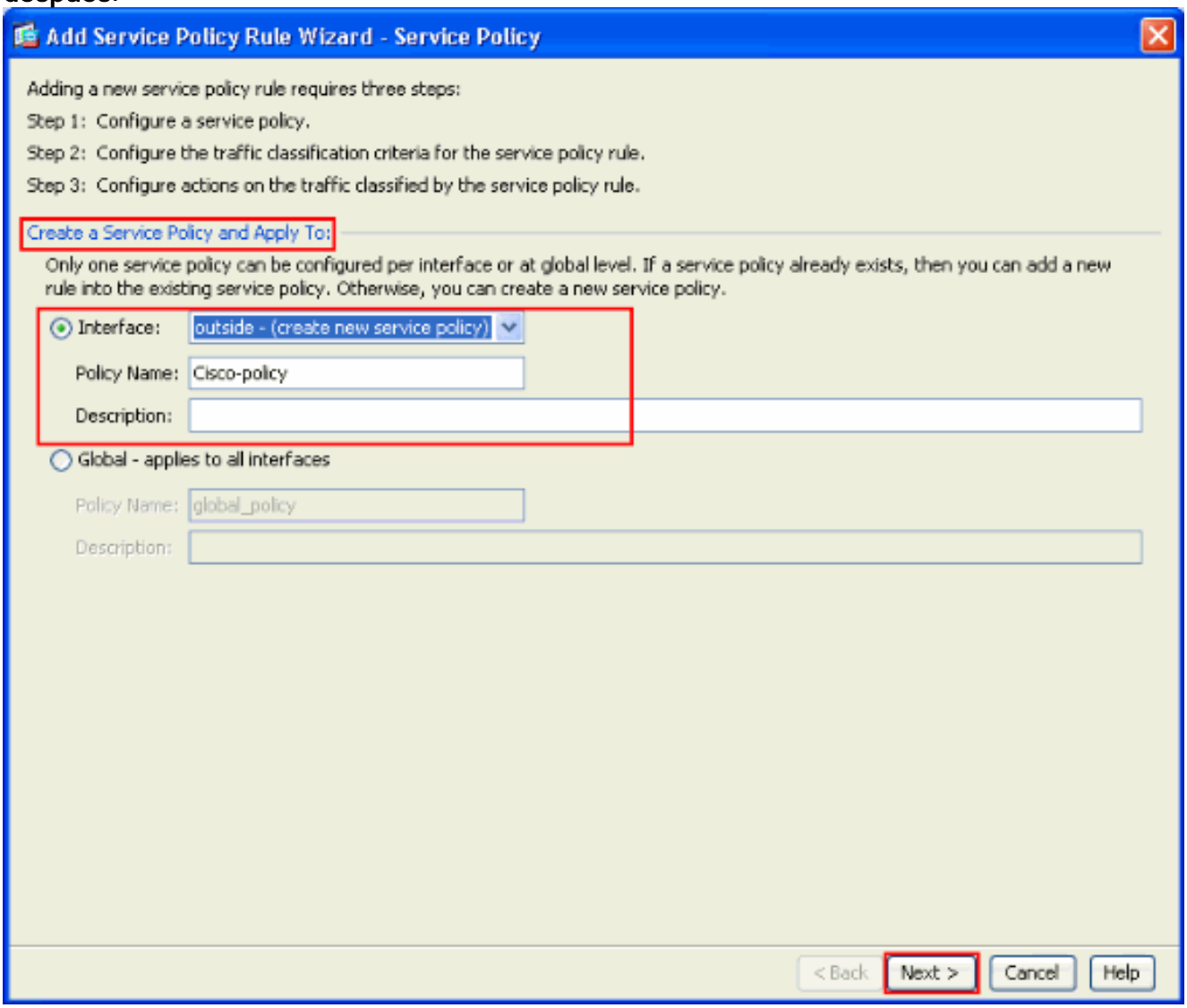
Nota: Refiera a permitir que el acceso HTTPS para el ASDM para las configuraciones básicas para acceder el PIX/ASA con el ASDM.

1. Elija las **reglas de la configuración > del Firewall > de la política de servicio** y el tecleo **agrega** para configurar la regla de la política de servicio como se muestra.

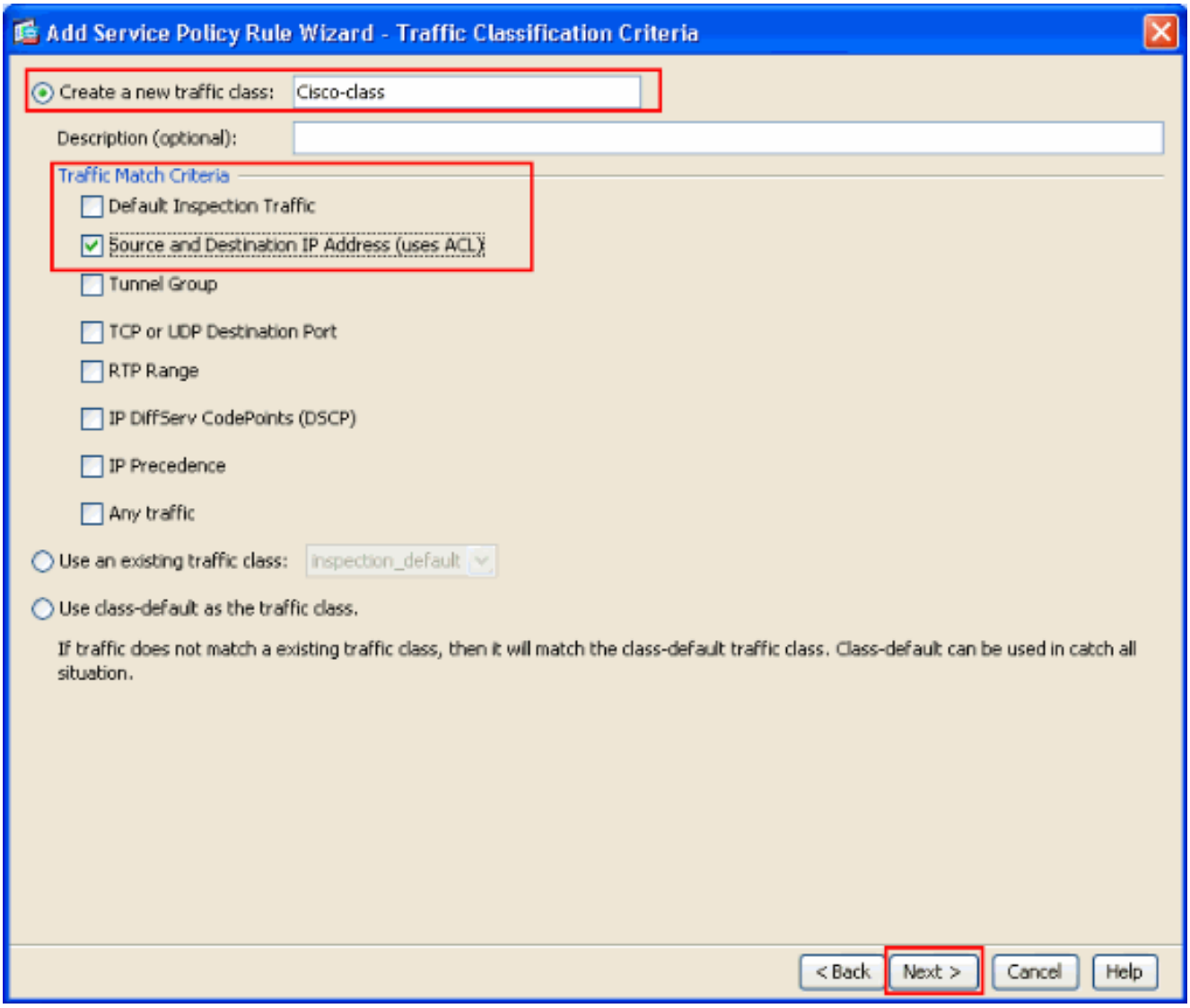


2. **Del Asisitente de la regla de la política de servicio del agregar -** La ventana de la **política de servicio**, elige el botón de radio al lado de la **interfaz** bajo **crear una política de servicio y se aplica** para seccionar. Ahora elija la interfaz deseada de la lista desplegable y proporcione un **nombre de la directiva**. El nombre de la directiva usado en este ejemplo es Cisco-

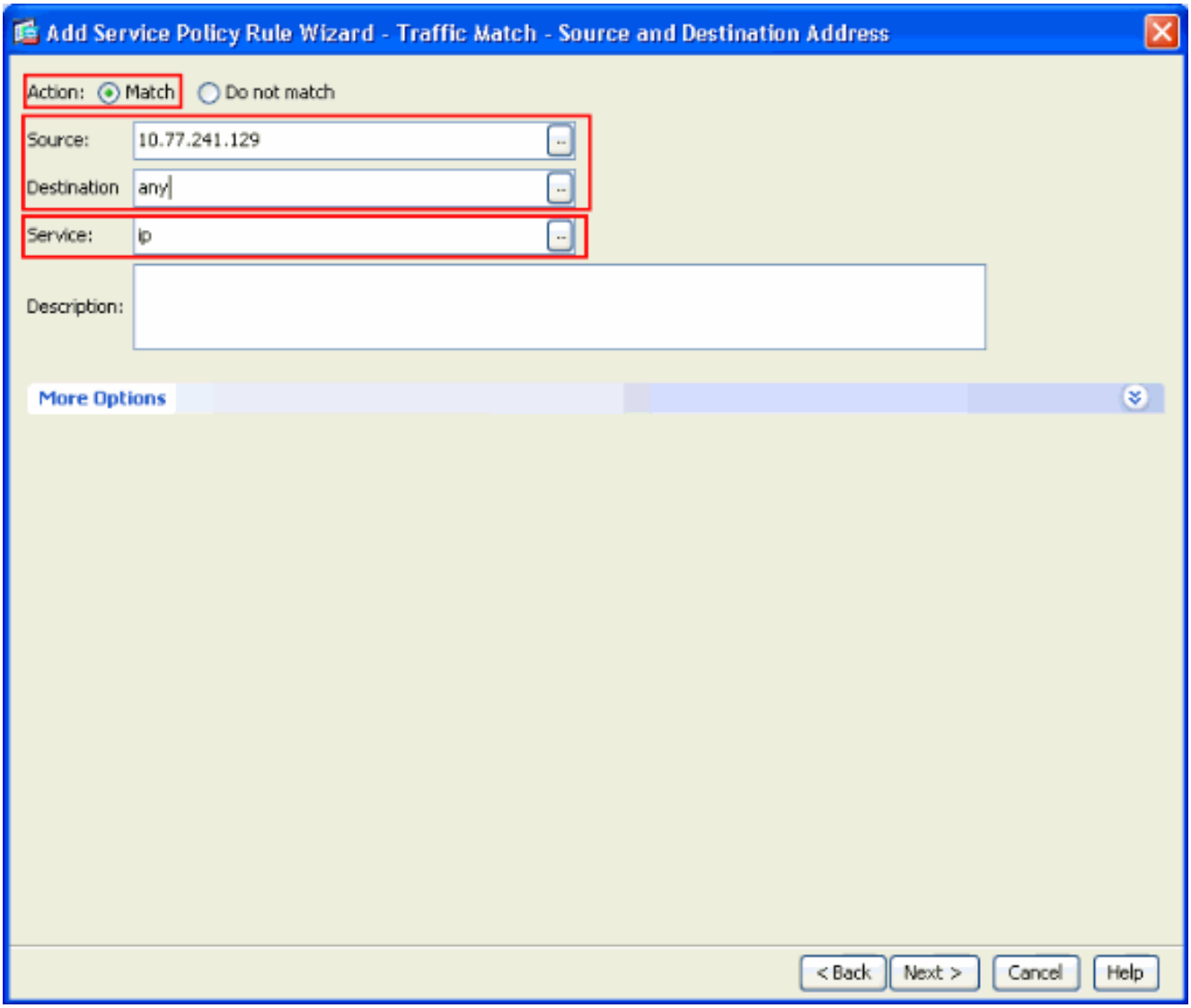
directiva. Entonces, haga clic **después**.



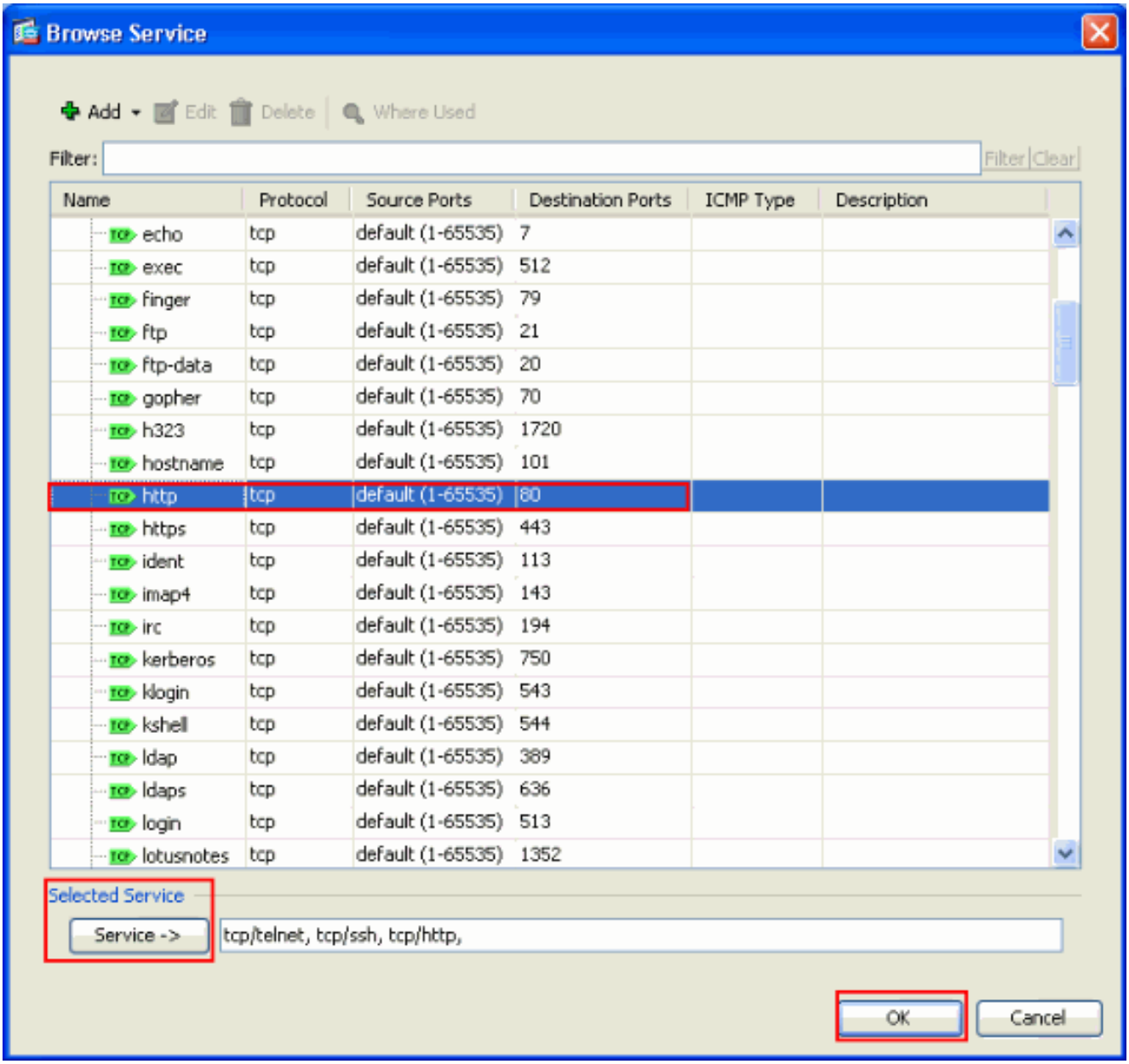
3. Cree una Cisco-**clase del** nombre de asignación de la clase y marque la casilla de verificación del **IP Address de origen y de destino (aplicaciones ACL)** en los criterios de concordancia del tráfico. Entonces, haga clic **después**.



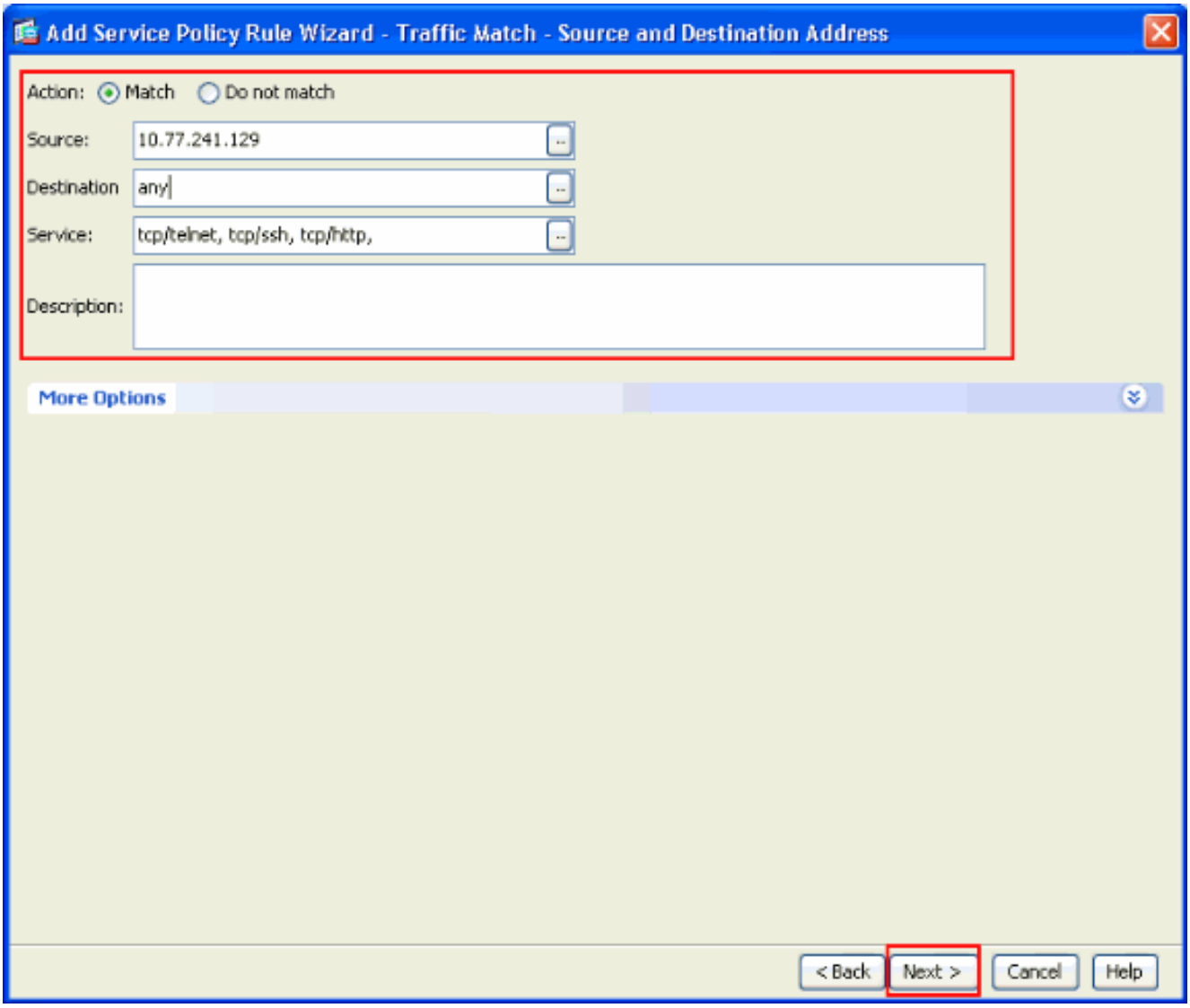
4. **Del Asisitente de la regla de la política de servicio del agregar - Coincidencia del tráfico - La fuente y la ventana de dirección de Destnation**, eligen el botón de radio al lado de la **coincidencia** y después proporcionan la fuente y a la dirección destino como se muestra. Haga clic el botón del descenso-abajo al lado del **servicio** para elegir los servicios solicitados.



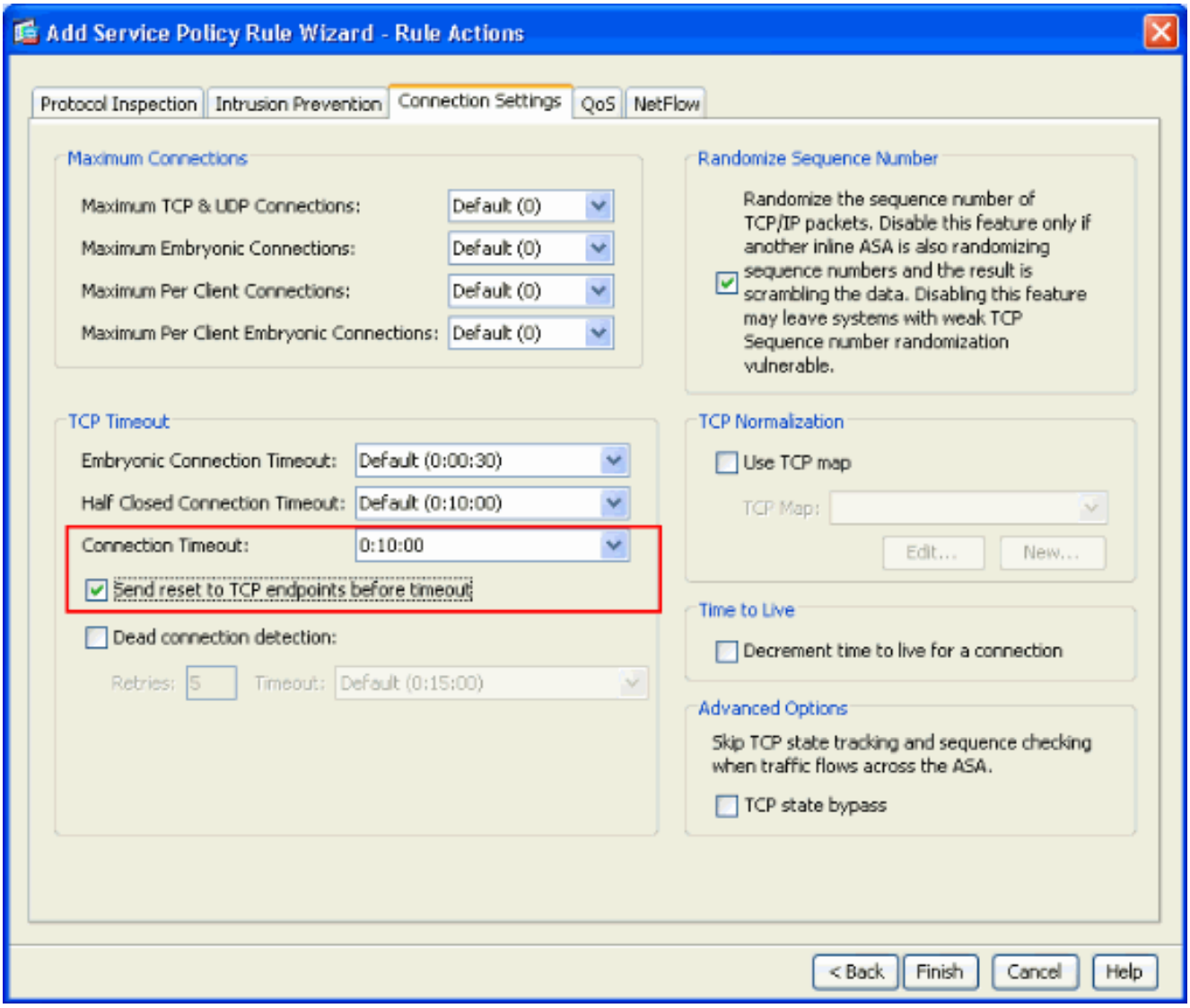
5. Seleccione los servicios solicitados tales como **telnet**, **ssh** y **HTTP**. Entonces, **AUTORIZACIÓN del**
tecleo.



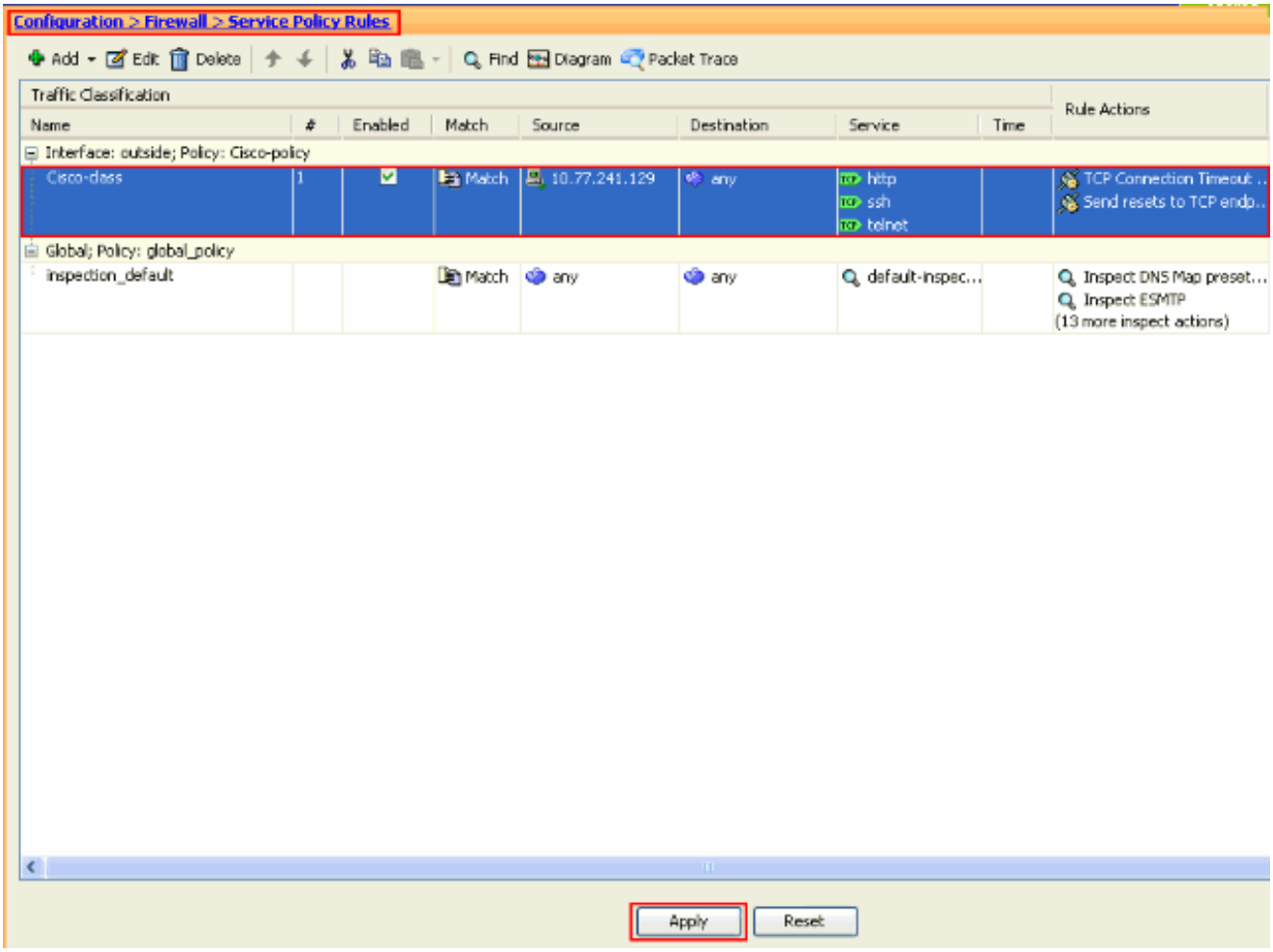
6. **Descansos de la configuración**. Haga clic en Next (Siguiente).



7. Elija las **configuraciones de la conexión** para configurar el descanso de conexión TCP como 10 minutos. También, marque el **envío reajustado a los Puntos finales de TCP antes de la** casilla de verificación del **descanso**. Haga clic en Finish (Finalizar).



8. El tecleo **se aplica** para aplicar la configuración al dispositivo de seguridad.Esto completa la configuración.



Descanso de Ebryonic

Una conexión embrionaria es la conexión que es media se abre o, por ejemplo, la entrada en contacto de tres vías no se ha completado para ella. Se define como tiempo de espera SYN en el ASA. Por abandono, el tiempo de espera SYN en el ASA es 30 segundos. Éste es cómo configurar el descanso embrionario:

```
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

Si usted encuentra que el tiempo de espera de la conexión no trabaja con el MPF, después marque la conexión del lanzamiento TCP. El problema puede ser una revocación del IP Address de origen y de destino, o una dirección IP mal configurado en la lista de acceso no hace juego en el MPF para fijar el nuevo valor de agotamiento del tiempo o para cambiar el tiempo de espera predeterminado para la aplicación. Cree una entrada de lista de acceso (fuente y destino) de acuerdo con el lanzamiento de conexión para fijar el tiempo de espera de la conexión con el MPF.

Información Relacionada

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems