ASA 8.3及更高版本：使用MPF配置設定SSH/Telnet/HTTP連線超時示例

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[設定](#)
[網路圖表](#)
[組態](#)
[Ebryonic超時](#)
[疑難排解](#)
[相關資訊](#)

簡介

本文檔提供了思科自適應安全裝置(ASA)的示例配置，該配置包含特定應用（如SSH/Telnet/HTTP）的超時版本8.3(1)及更高版本，而不是適用於所有應用的超時版本。此配置示例使用思科自適應安全裝置(ASA)版本7.0中引入的模組化策略框架(MPF)。有關詳細資訊，請參閱使用模組化策略框架。

在此示例配置中，Cisco ASA配置為允許工作站(10.77.241.129)通過Telnet/SSH/HTTP連線到路由器後面的遠端伺服器(10.1.1.1)。還配置了Telnet/SSH/HTTP流量的單獨連線超時。所有其他TCP流量繼續具有與**timeout conn 1:00:00關聯的正常連線超時值**。

請參閱PIX/ASA 7.x及更高版本/FWSM:使用MPF配置示例設定SSH/Telnet/HTTP連線超時，適用於版本8.2及更低版本的Cisco ASA上的相同配置。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於採用自適應安全裝置管理器(ASDM)6.3的Cisco ASA安全裝置軟體版本8.3(1)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

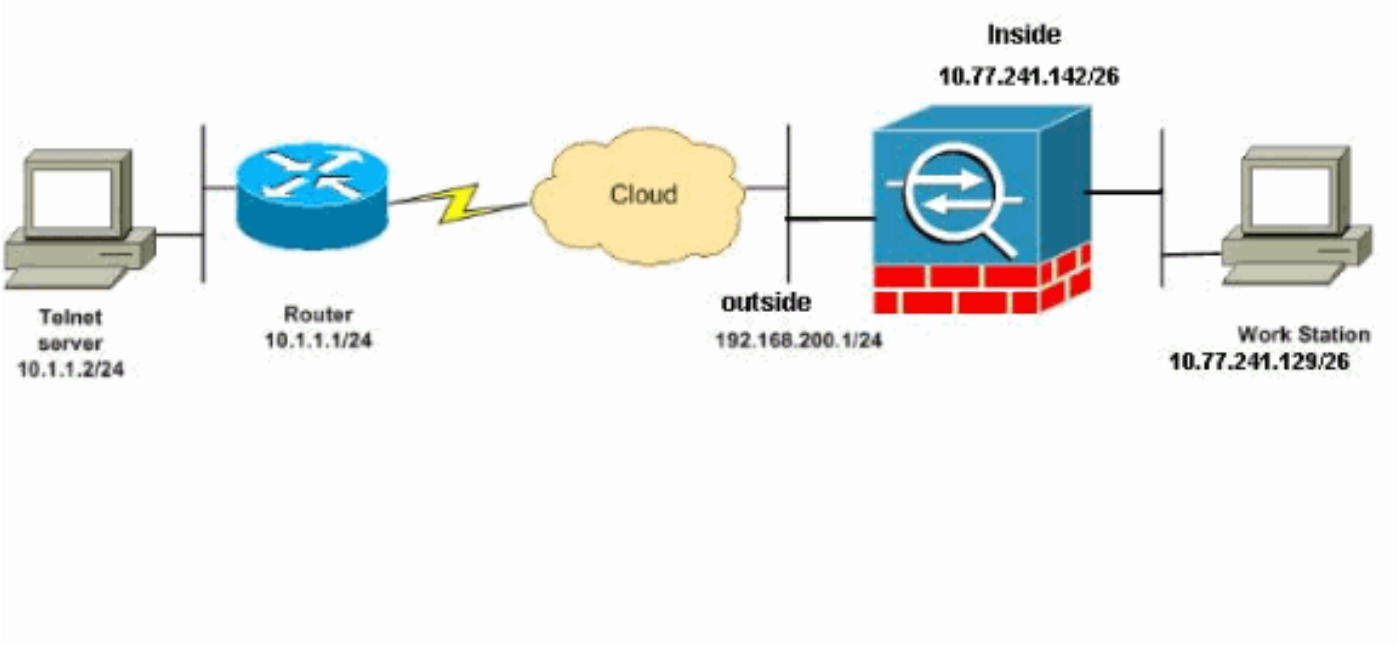
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用 Command Lookup Tool(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是RFC 1918地址，已在實驗室環境中使用。

組態

本檔案會使用以下設定：

- CLI組態
- ASDM配置

注意：這些CLI和ASDM配置適用於防火牆服務模組(FWSM)。

CLI組態

ASA 8.3(1)配置
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
```

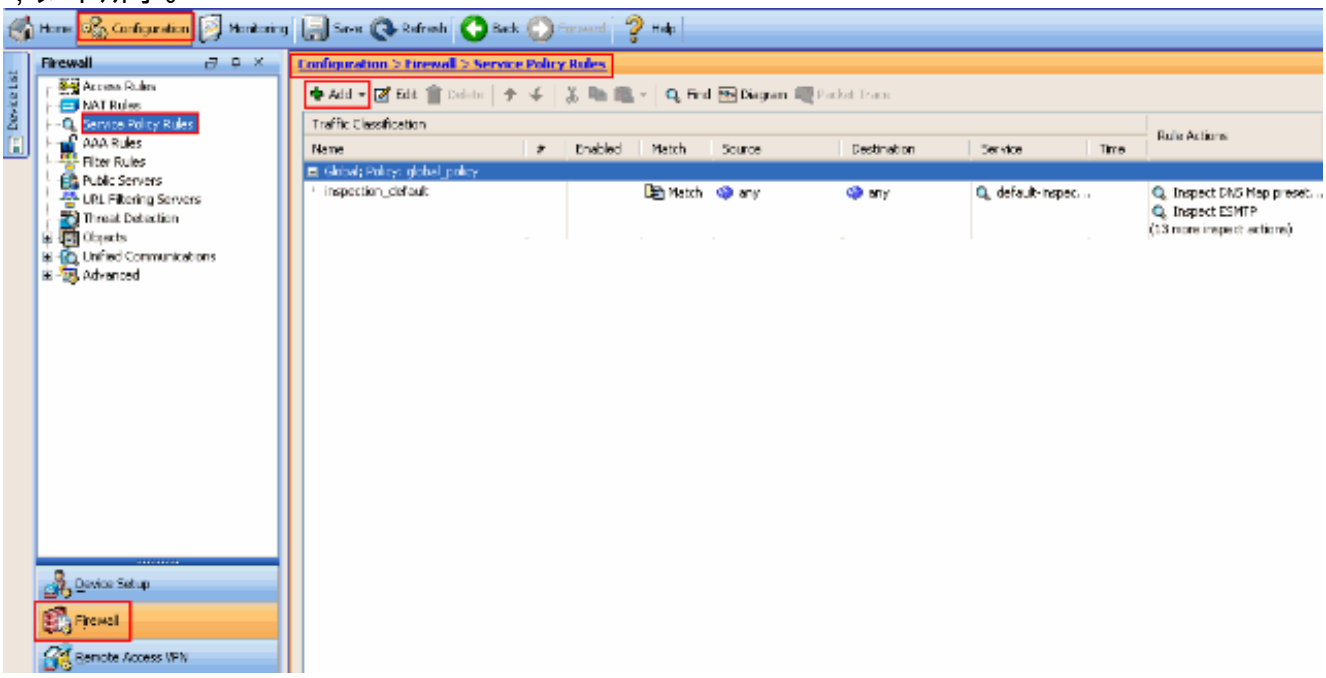
```
!

!--- 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配置

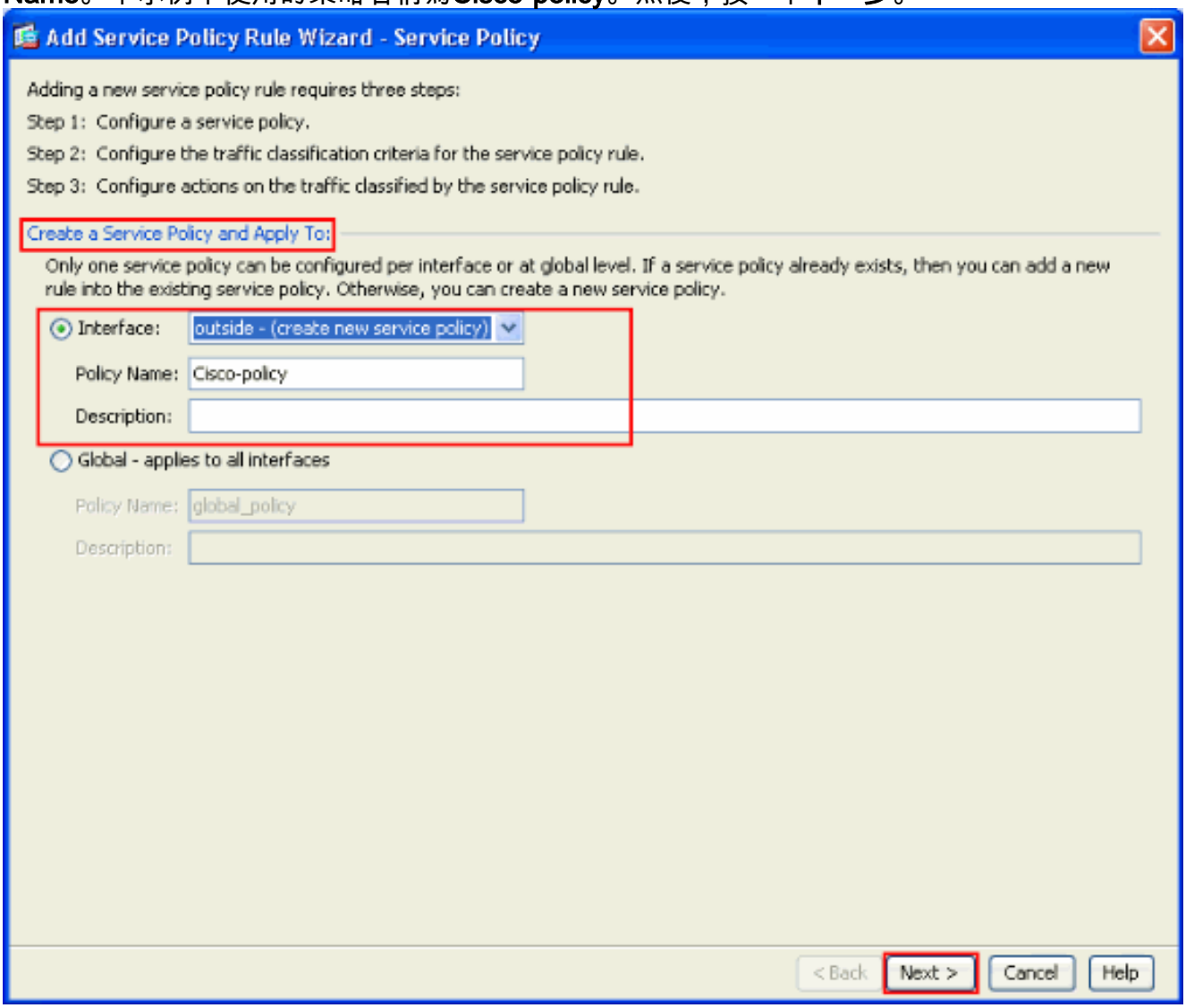
完成以下步驟，以便使用ASDM為Telnet、SSH和HTTP流量設定TCP連線超時，如下所示。

注意：請參閱允許ASDM的HTTPS訪問以瞭解基本設定，以便通過ASDM訪問PIX/ASA。

1. 選擇**Configuration > Firewall > Service Policy Rules**，然後按一下**Add**以配置服務策略規則，如下所示。

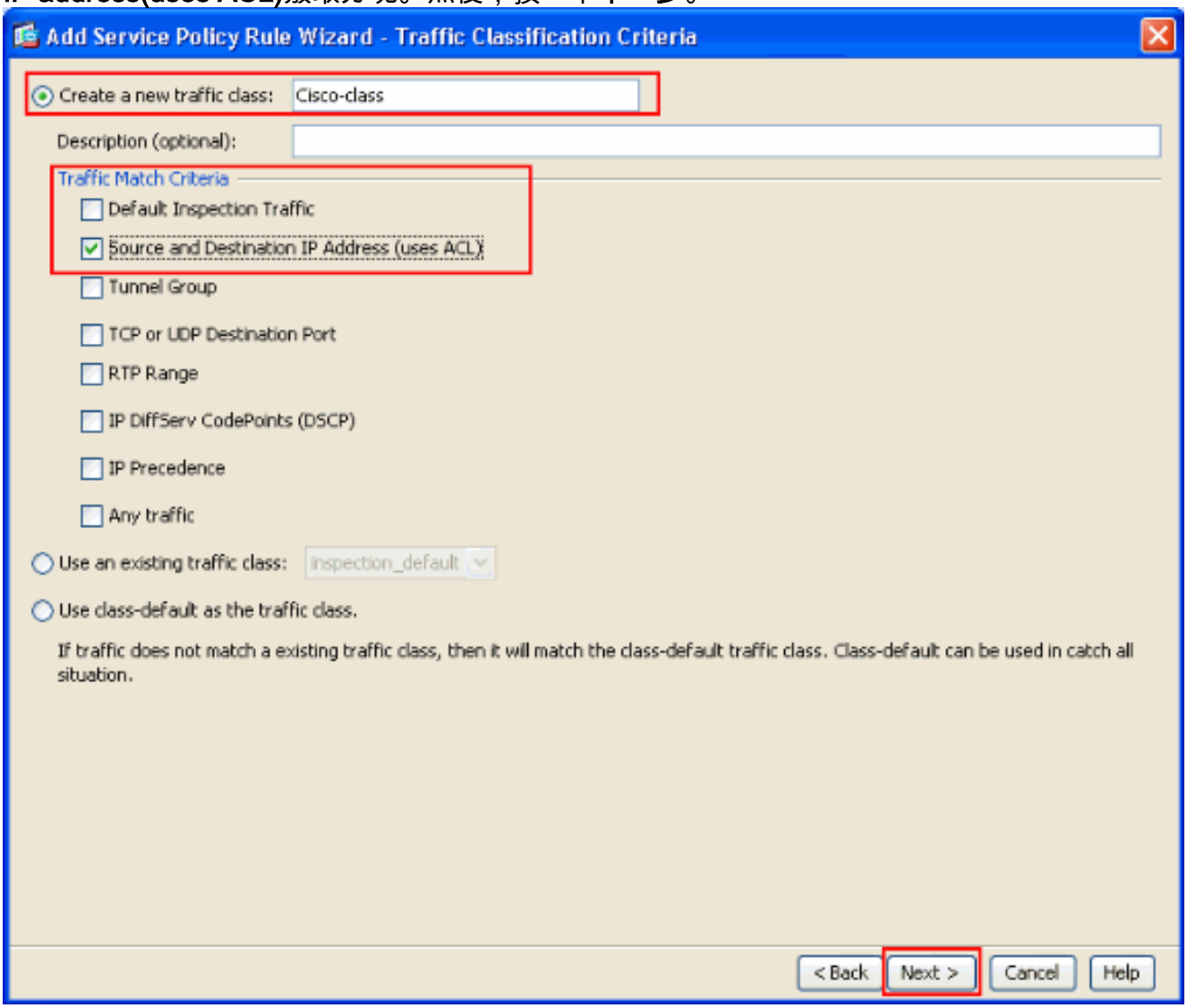


2. 在**Add Service Policy Rule Wizard - Service Policy**視窗中，選擇**Create a Service Policy and Apply To**部分下**Interface**旁邊的單選按鈕。現在，從下拉選單中選擇所需的介面並提供**Policy Name**。本示例中使用的策略名稱為**Cisco-policy**。然後，按一下**下一步**。

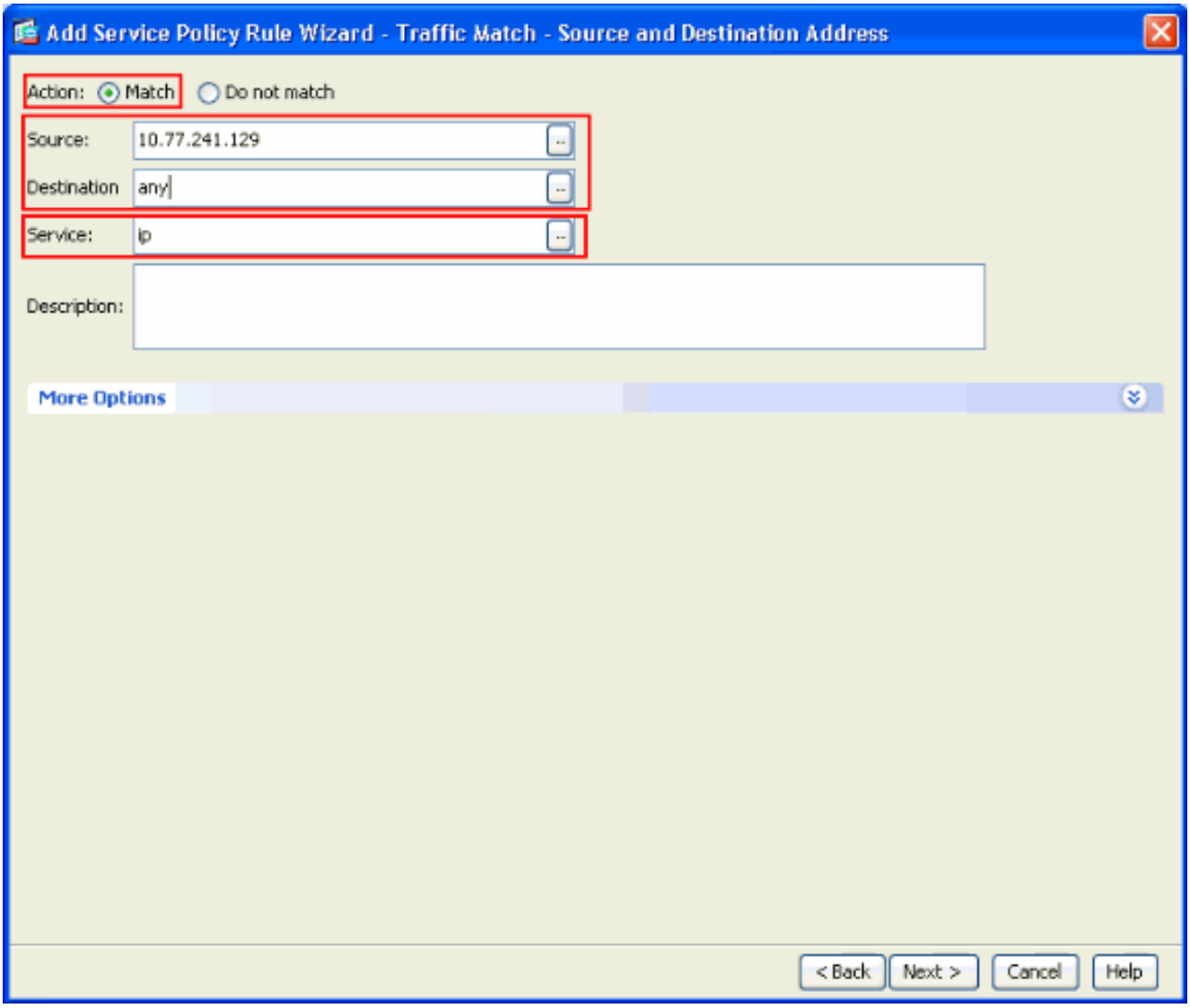


3. 建立一個類對映名稱**Cisco-class**，然後選中Traffic Match Criteria中的**Source and Destination**

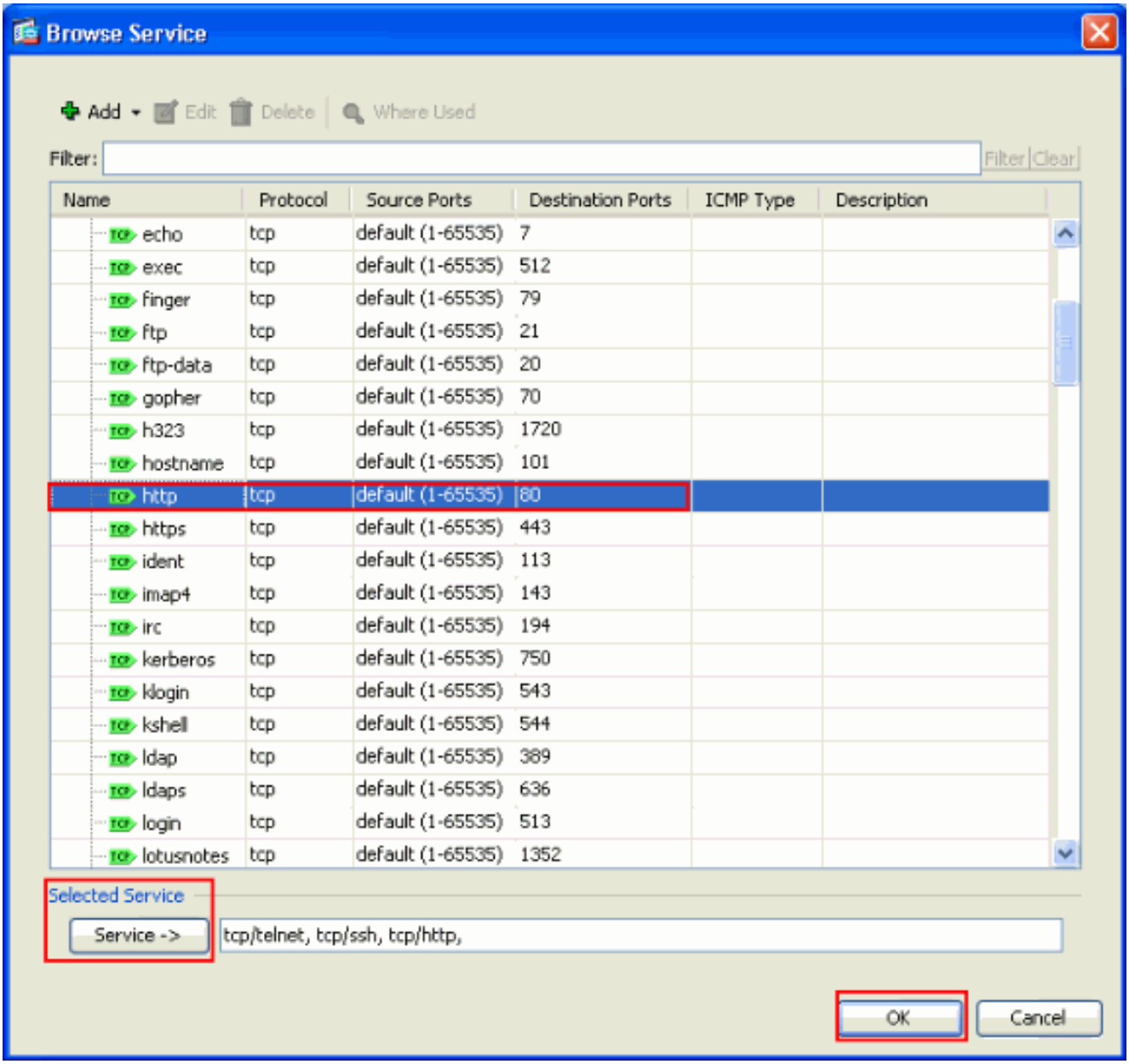
IP address(uses ACL)覈取方塊。然後，按一下**下一步**。



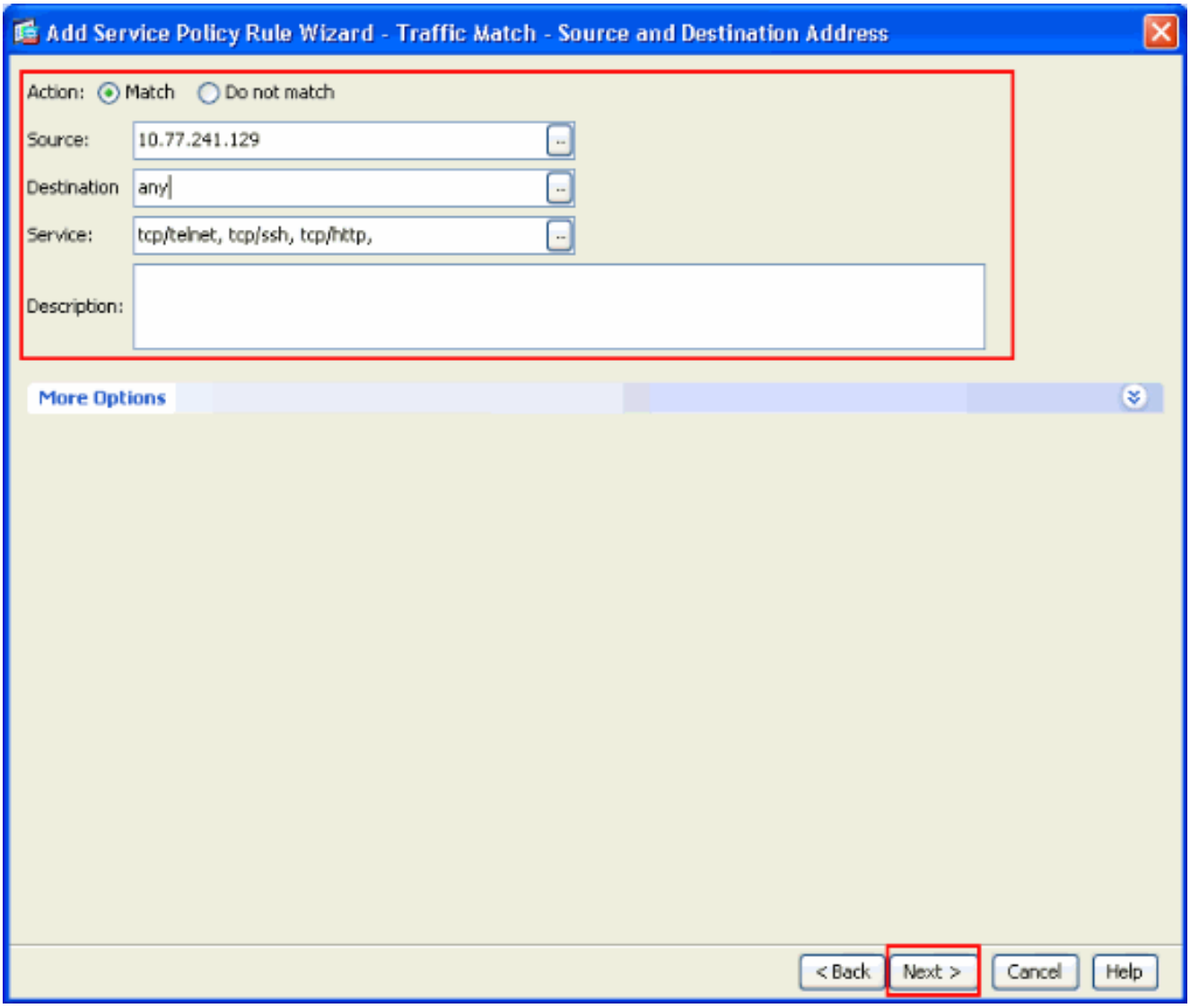
4. 在**Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address**視窗中，選擇**Match**旁邊的單選按鈕，然後提供源和目標地址，如下所示。點選**服務**旁邊的下拉按鈕以選擇所需的服務。



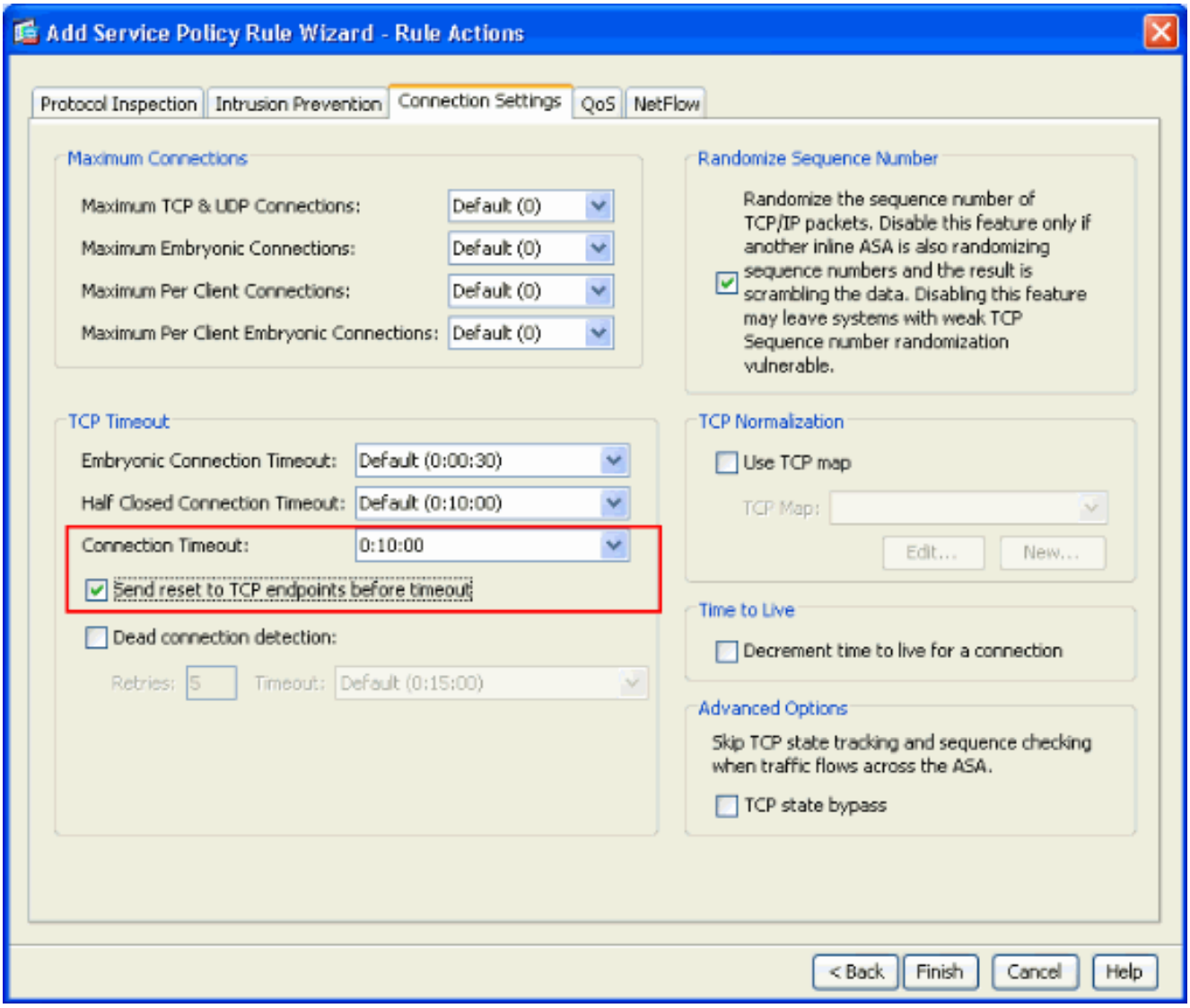
5. 選擇所需的服務，例如**telnet**、**ssh**和**http**。然後，按一下**OK**。



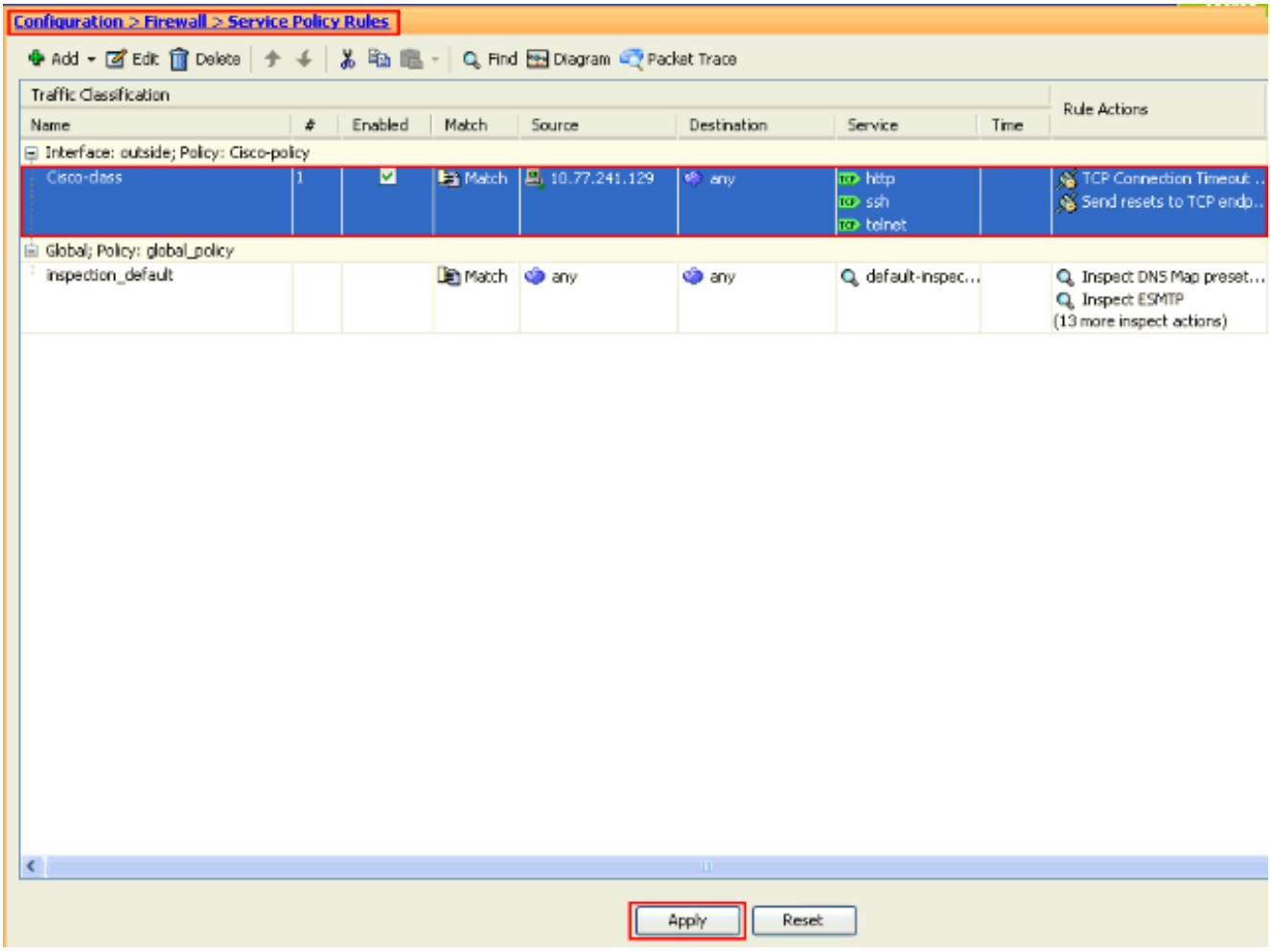
6. **配置超時。**按「**Next**」（下一步）。



7. 選擇Connection Settings以將TCP連線超時設定為10分鐘。此外，選中Send reset to TCP endpoints before timeout覈取方塊。按一下「Finish」（結束）。



8. 按一下「Apply」將組態套用到安全裝置。這樣即可完成配置。



Ebryonic超時

早期連線是半開連線，或者例如尚未完成三次握手。定義為ASA上的SYN超時。預設情況下，ASA上的SYN超時為30秒。以下是配置Embryonic Timeout的方式：

```
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
```

疑難排解

如果您發現連線超時在MPF中不起作用，請檢查TCP啟動連線。問題可能是源和目標IP地址顛倒，或者訪問清單中配置的IP地址在MPF中不匹配，以設定新的超時值或更改應用程式的預設超時。根據連線發起建立訪問清單條目（源和目標），以便使用MPF設定連線超時。

相關資訊

- 思科調適型資安裝置管理員

- Cisco ASA 5500系列調適型安全裝置
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems