ASA 8.3 والإصدارات الأحدث: ضبط مهلة اتصال SSH/Telnet/HTTP باستخدام مثال تكوين MPF

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين جهاز الأمان القابل للتكيف (ASA) من Cisco مع الإصدار 8.3(1) والإصدارات الأحدث من مهلة تكون محددة لتطبيق معين مثل SSH/Telnet/HTTP، بدلا من واحد ينطبق على جميع التطبيقات. يستخدم مثال التكوين هذا إطار عمل السياسة النمطية (MPF) الذي تم تقديمه في جهاز الأمان القابل للتكيف (ASA) من Cisco، الإصدار 7.0. راجع إستخدام إطار عمل السياسة النمطية للحصول على مزيد من المعلومات.

في هذا التكوين النموذجي، يتم تكوين Cisco ASA للسماح لمحطة العمل (10.77.241.129) ب Telnet/SSH/HTTP بالخادم البعيد (10.1.1.1) خلف الموجه. كما تم تكوين مهلة اتصال منفصلة لحركة مرور بيانات Telnet/SSH/HTTP. تستمر جميع حركات مرور TCP الأخرى في الحصول على قيمة انتهاء مهلة الاتصال العادية المقترنة **بمهلة conn 1:00:00**.

ارجع إلى PIX/ASA 7.x والإصدارات الأحدث/FWSM: تعيين مهلة اتصال SSH/Telnet/HTTP باستخدام مثال تكوين MPF لنفس التكوين على Cisco ASA مع الإصدارات 8.2 والإصدارات الأقدم.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج جهاز الأمان Cisco ASA Security Appliance، الإصدار 8.3(1) مع Adaptive Security Device Manager (ASDM) 6.3.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

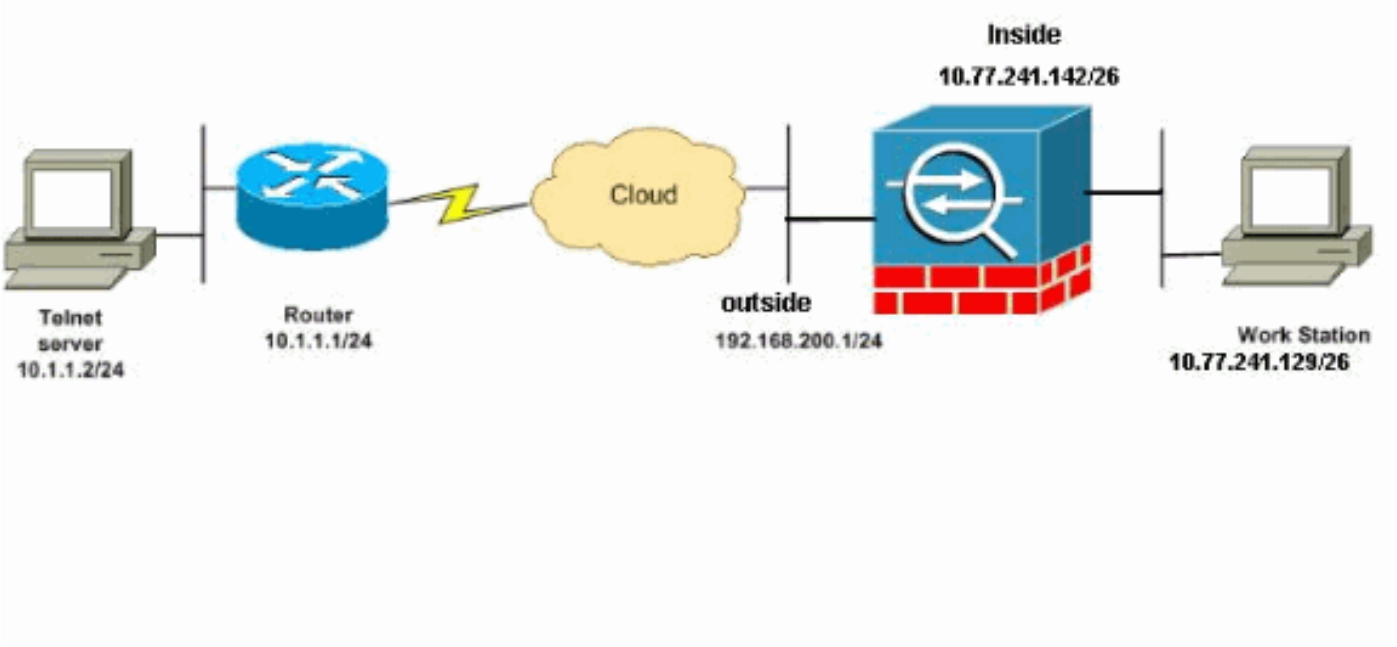
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان، أي يتلقى يكون استعملت في مختبر بيئة.

التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين واجهة سطر الأوامر (CLI)
- تكوين ASDM

ملاحظة: تنطبق تكوينات CLI و ASDM هذه على الوحدة النمطية لخدمة جدار الحماية (FWSM).

تكوين واجهة سطر الأوامر (CLI)

تكوين 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
```

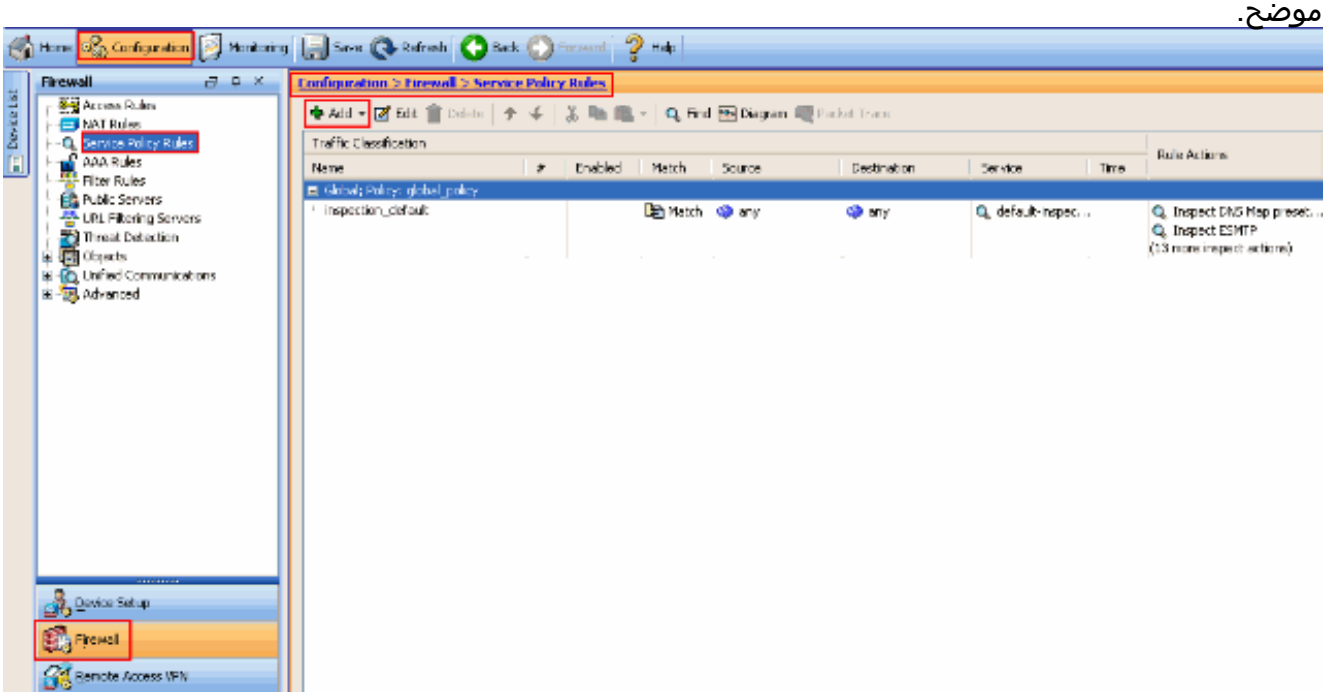
```
                                                linkdown coldstart
                                                  telnet timeout 5
                                                     ssh timeout 5
                                                console timeout 0
                                                                !


  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
```

[تكوين ASDM](#)

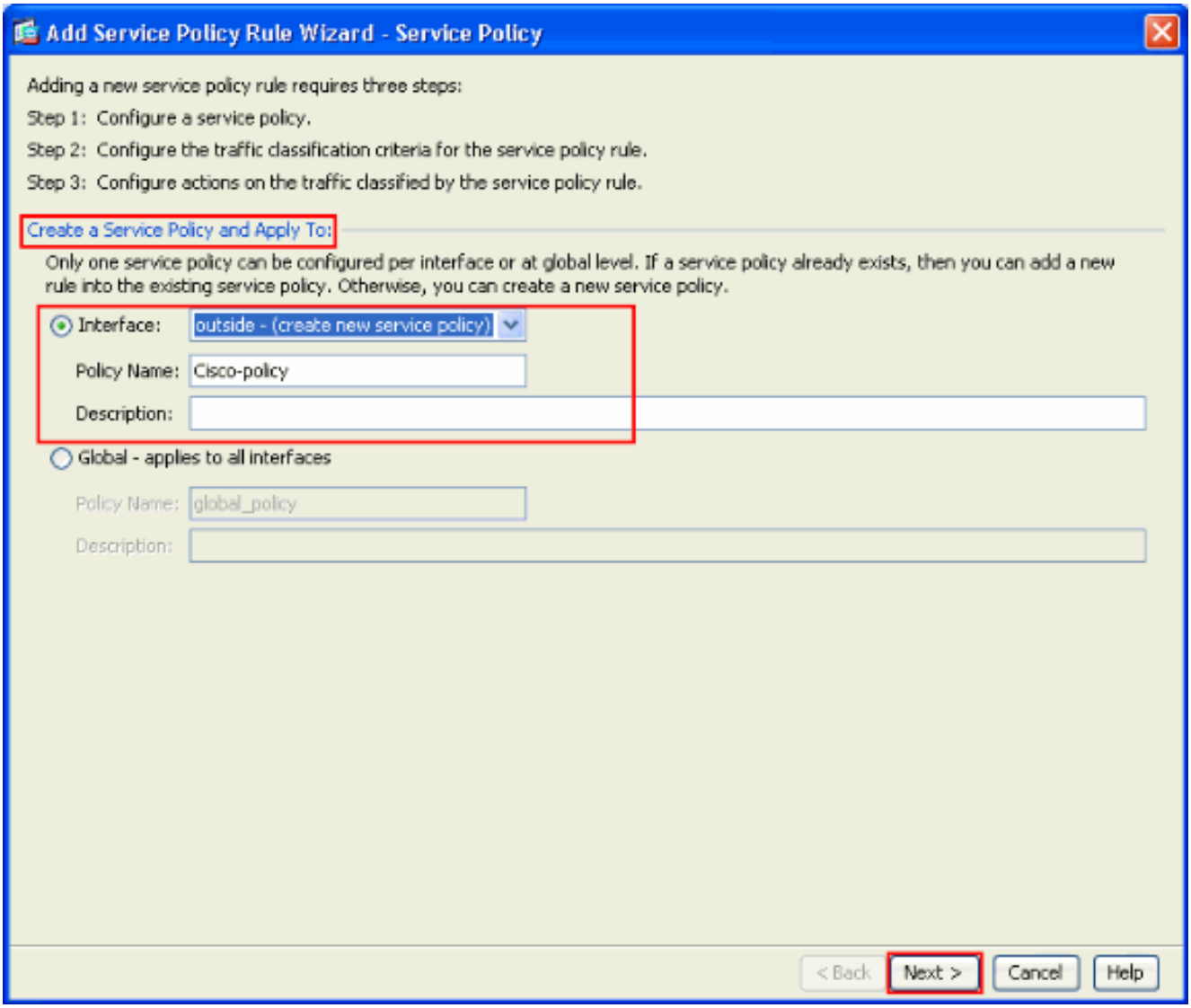
أكمل هذه الخطوات لإعداد مهلة اتصال TCP لحركة مرور Telnet و SSH و HTTP باستخدام ASDM كما هو موضح.

ملاحظة: راجع السماح بوصول HTTPS ل ASDM للإعدادات الأساسية للوصول إلى PIX/ASA من خلال ASDM.

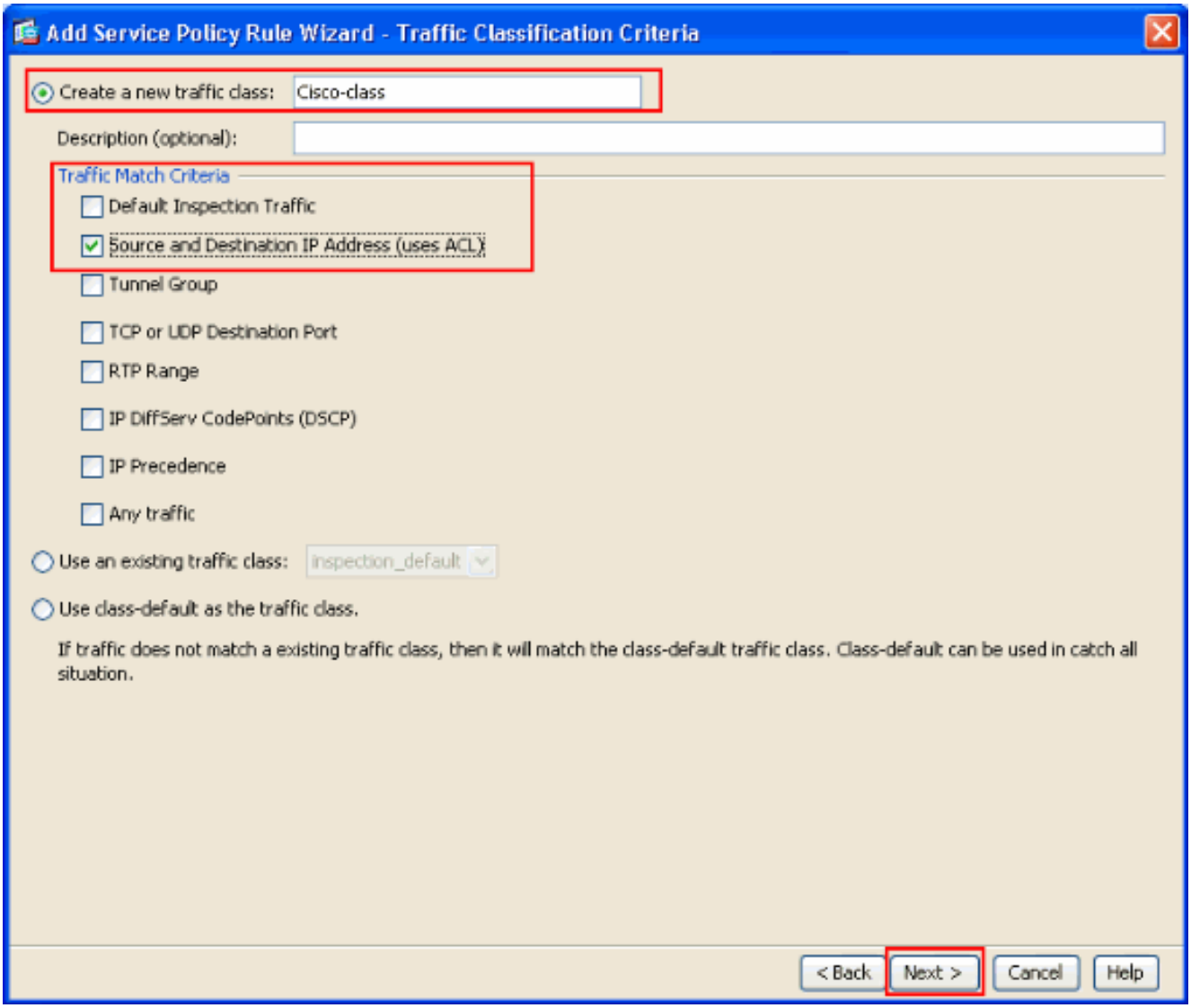
1. أخترت **تشكيل>جدار حماية>خدمة سياسة قاعدة** وطقطقة **يضيف** in order to شكلت الخدمة سياسة قاعدة كما هو
موضح.



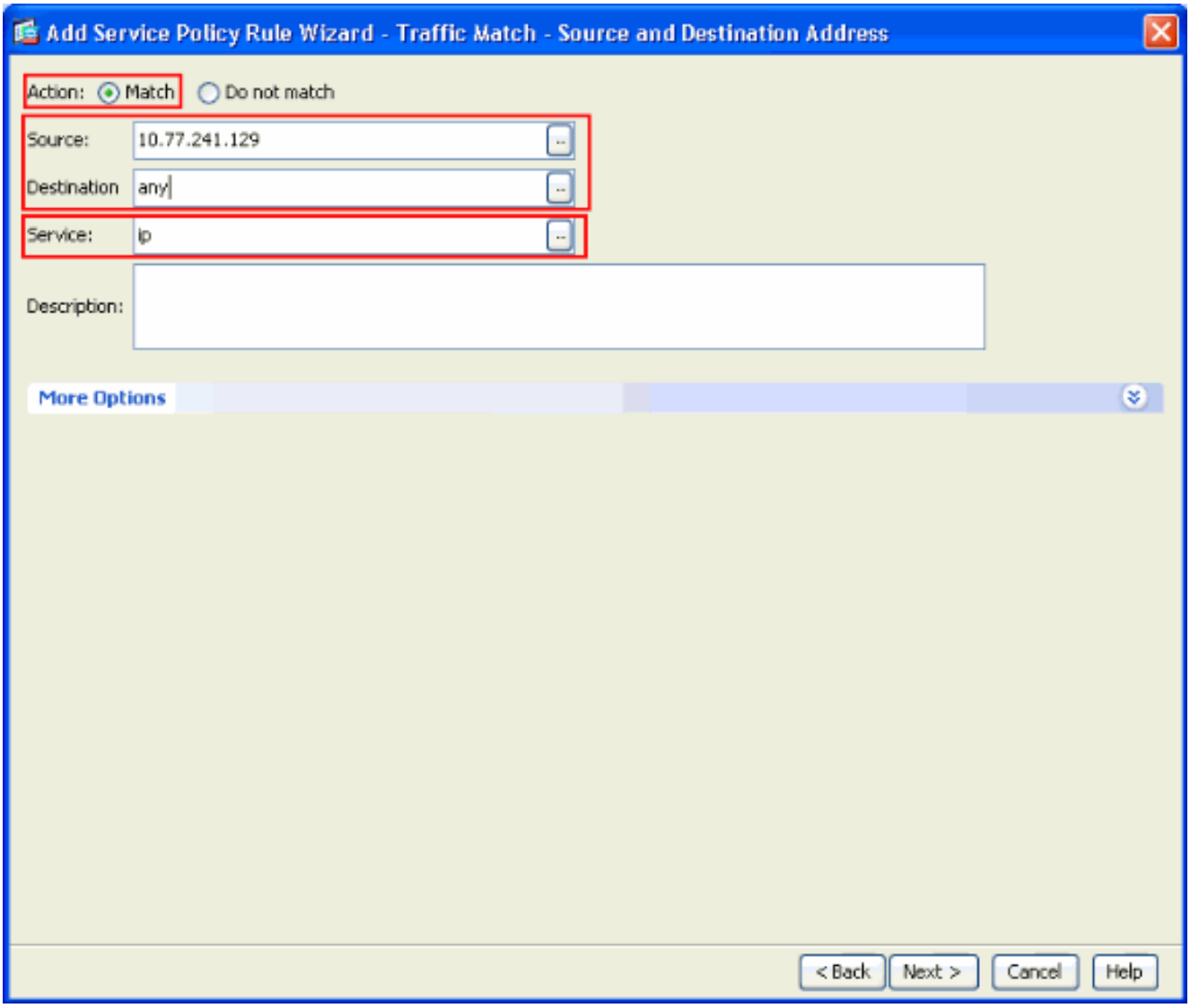
2. من **معالج "إضافة قاعدة سياسة الخدمة" -** إطار **نهج الخدمة**، أختر الزر "إختيار" الموجود بجوار **الواجهة** ضمن المقطع **إنشاء نهج خدمة والتطبيق على**. أختر الآن الواجهة المطلوبة من القائمة المنسدلة وقم بتوفير **اسم نهج**. اسم النهج المستخدم في هذا المثال هو **Cisco-policy**. ثم انقر فوق
التالي.



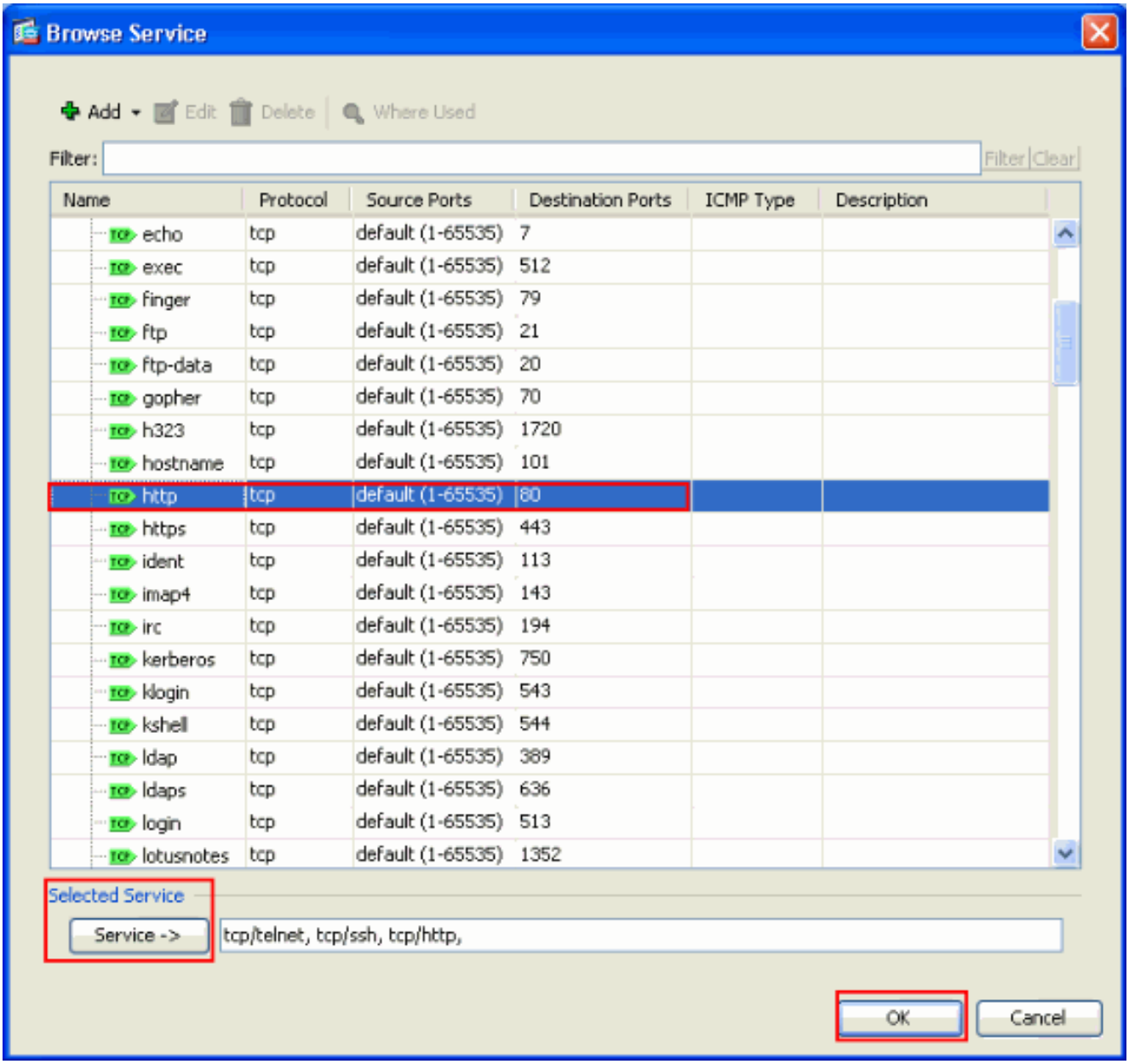
3. قم بإنشاء اسم خريطة فئة **Cisco-class** وحدد **عنوان IP للمصدر والوجهة (يستخدم قائمة التحكم في الوصول (ACL)** خانة الاختيار في معايير مطابقة حركة المرور. ثم انقر فوق **التالي**.



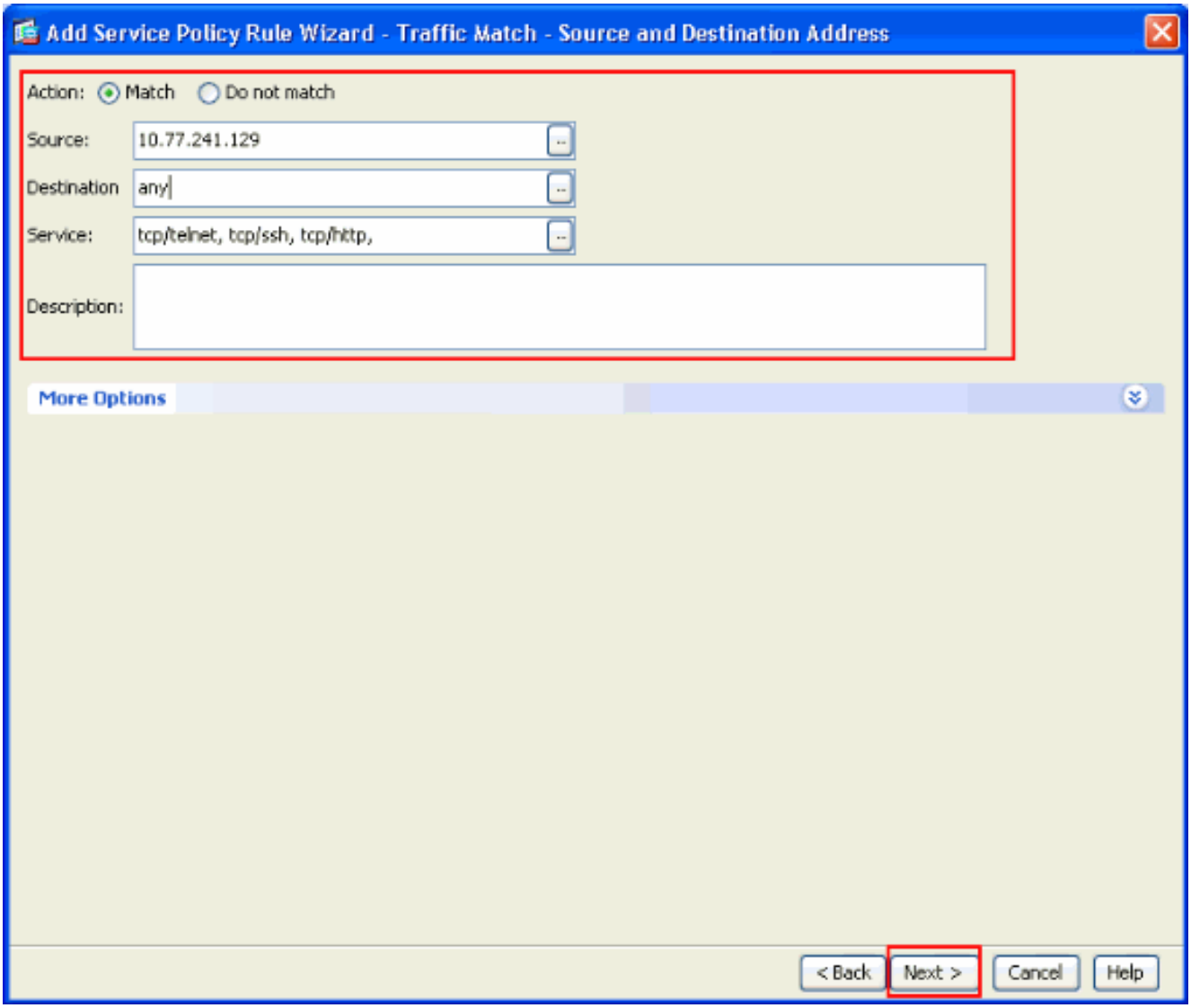
4. من معالج **إضافة قاعدة سياسة الخدمة - مطابقة حركة المرور - نافذة مصدر وعنوان مصدر**، أختر زر الخيار المجاور **للمطابقة** ثم قم بتوفير عنوان المصدر والوجهة كما هو موضح. انقر فوق الزر المنسدل الموجود بجوار **الخدمة** لاختيار الخدمات المطلوبة.



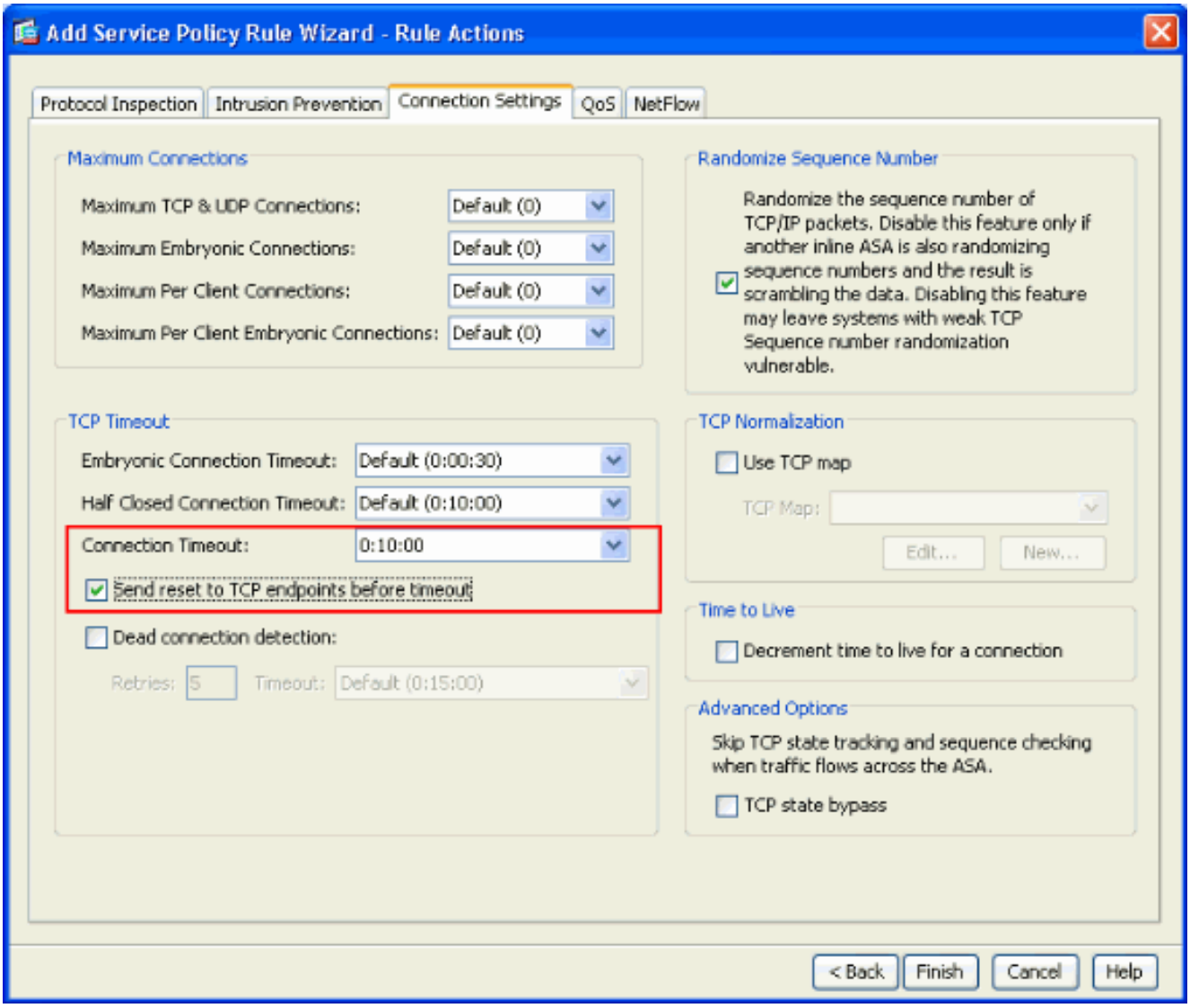
5. حدد الخدمات المطلوبة مثل **Telnet** و**SSH** و**http**. ثم انقر فوق **OK**.



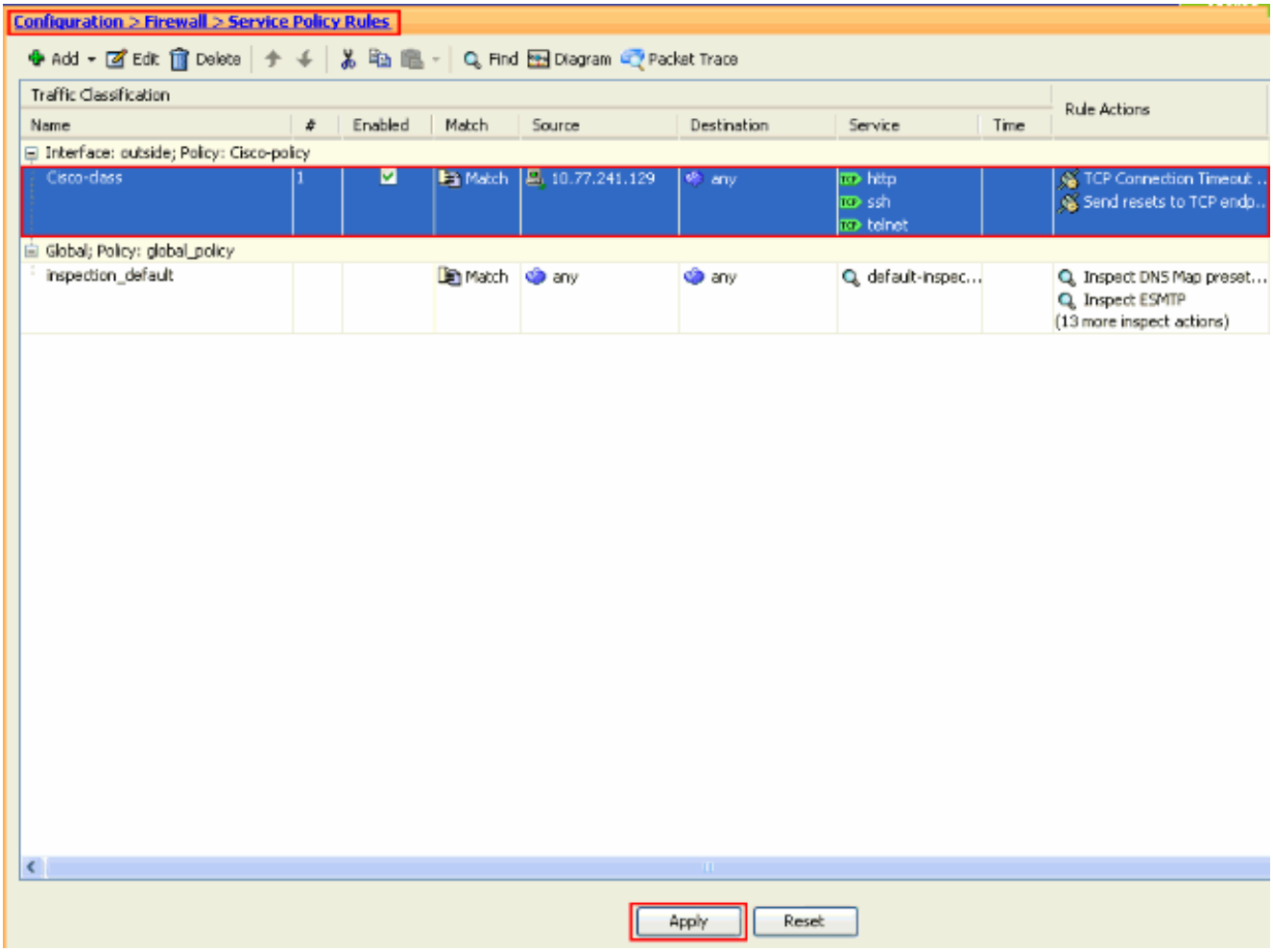
6. **تكوين حالات انتهاء المهلة الزمنية**. انقر فوق **Next (التالي)**.



7. أخترت **توصيل عملية إعداد** in order to setup ال TCP توصيل مهلة 10 دقيقة. تحقق أيضا من خانة الاختيار **إعادة تعيين الإرسال إلى نقاط نهاية TCP قبل المهلة**. انقر فوق **إنهاء**.



8. انقر فوق **تطبيق** لتطبيق التكوين على جهاز الأمان.يؤدي هذا إلى اكتمال التكوين.



مهلة إبريونية

الاتصال الجنيني هو اتصال نصف مفتوح أو، على سبيل المثال، لم تكتمل المصافحة الثلاثية له. يتم تعريفه على أنه مهلة SYN على ASA. افتراضيا، ال syn مهلة على ال ASA 30 ثاني. هذه هي كيفية تكوين المهلة الجنينية:

```
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
```

استكشاف الأخطاء وإصلاحها

إذا وجدت أن مهلة الاتصال لا تعمل مع MPF، فتحقق من اتصال بدء TCP. يمكن أن تكون المشكلة عكس عنوان IP للمصدر والوجهة، أو أن عنوان IP الذي تم تكوينه بشكل غير صحيح في قائمة الوصول لا يتطابق مع MPF لتعيين قيمة المهلة الجديدة أو لتغيير المهلة الافتراضية للتطبيق. قم بإنشاء إدخال قائمة وصول (المصدر والوجهة) وفقا لبدء الاتصال لتعيين مهلة الاتصال باستخدام MPF.

معلومات ذات صلة

- مدير أجهزة حلول الأمان المعدلة من Cisco
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- طلبات التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).