PIX/ASA 7.x والإصدارات الأحدث/FWSM: تعيين مهلة اتصال SSH/Telnet/HTTP باستخدام مثال تكوين MPF

المحتويات

المقدمة

يقدم هذه المستند عينة تكوين لـ PIX 7.1(1) والإصدارات الأحدث من المهلة التي تكون محددة لتطبيق معين مثل SSH/Telnet/HTTP، مقارنة بالتكوين الذي ينطبق على جميع التطبيقات. يستخدم مثال التكوين هذا إطار العمل الجديد للسياسة النمطية الذي تم تقديمه في PIX 7.0. راجع استخدام إطار عمل السياسة النمطية للحصول على مزيد من المعلومات.

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

ارجع إلى ASA 8.3 والإصدارات الأحدث: تعيين مهلة اتصال SSH/Telnet/HTTP باستخدام مثال تكوين MPF للحصول على مزيد من المعلومات حول التكوين المتطابق باستخدام ASDM مع جدار الحماية القابل للتكيف (ASA) من Cisco الإصدار 8.3 والإصدارات الأحدث.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى برنامج جدار الأمان Cisco PIX/ASA Security Appliance، الإصدار 7.1(1) مع Adaptive Security Device Manager (ASDM) 5.1.

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذه 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.

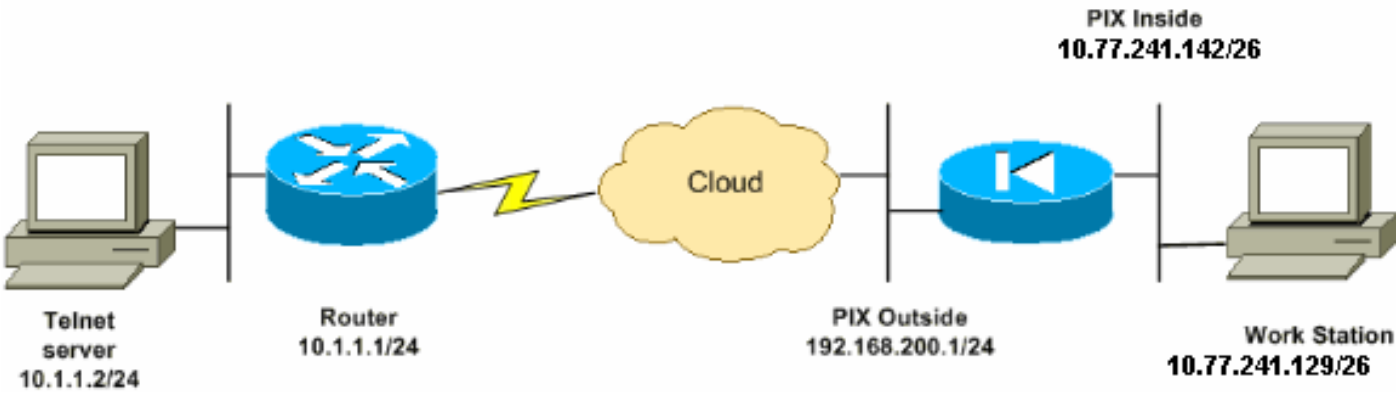
التكوين

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

التكوين

يستعمل هذا وثيقة هذا تشكيل:

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

CLI تشكيل:

تكوين PIX
PIX Version - 7.1(1) ! hostname PIX domain-name Cisco.com

```
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!


access-list inside_nat0_outbound extended permit ip
10.77.241.128 255.255.255.192 any

!--- Define the traffic that has to be matched in the
class map. !--- Telnet is defined in this example.
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq telnet
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq ssh
access-list outside_mpc_in extended permit tcp host
10.77.241.129 any eq www
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq telnet
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq ssh
access-list 101 extended permit tcp 10.77.241.128
255.255.255.192 any eq www

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
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 telnet in order !--- to
classify Telnet/ssh/http traffic when you use Modular
```

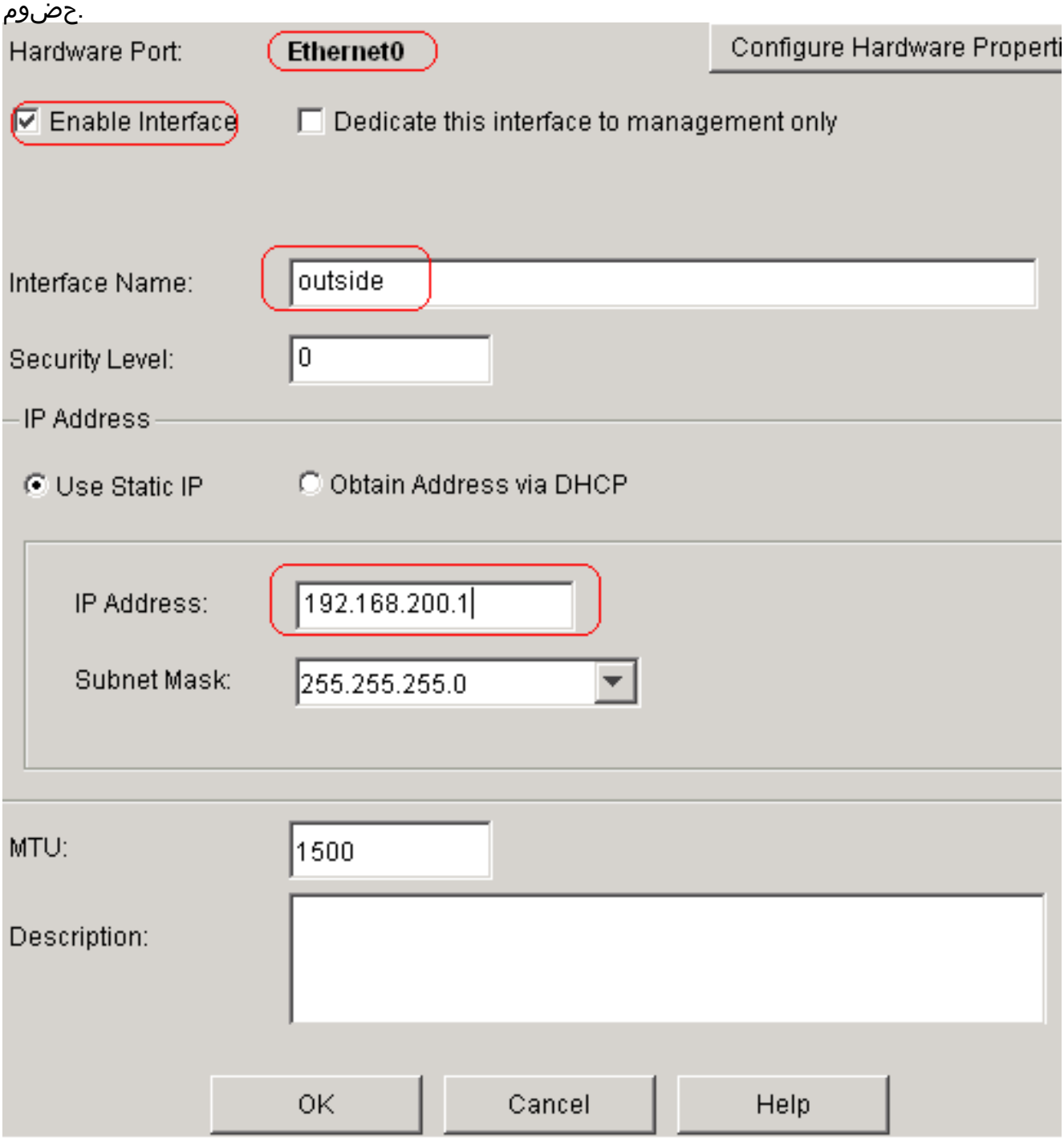
```
Policy Framework !--- to configure a security feature.
!--- Assign the parameters to be matched by class map.


class-map telnet
 description telnet
  match access-list outside_mpc_in

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 telnet in the policy
map.


policy-map telnet

!--- Set the connection timeout under the class mode in
which !--- 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 telnet
  set connection timeout tcp 00:10:00 reset
!
!
service-policy global_policy global

!--- Apply the policy-map telnet on the interface. !---
You can apply the service-policy command to any
interface that !--- can be defined by the nameif
command.

service-policy telnet interface outside
end
```

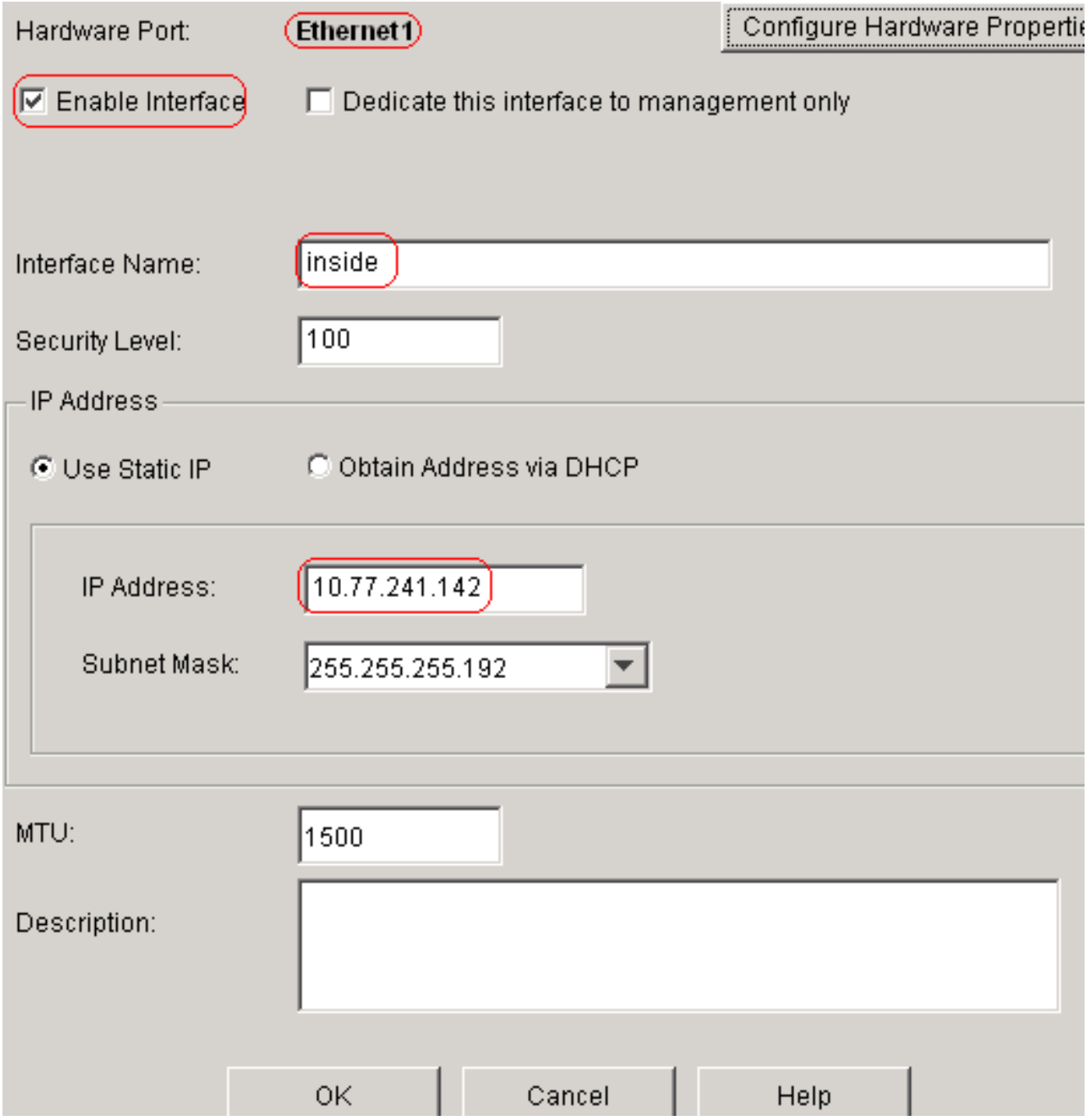
تكوين ASDM:

أكمل هذه الخطوات لإعداد مهلة اتصال TCP لحركة مرور بيانات Telnet استنادا إلى قائمة الوصول التي تستخدم ASDM كما هو موضح.

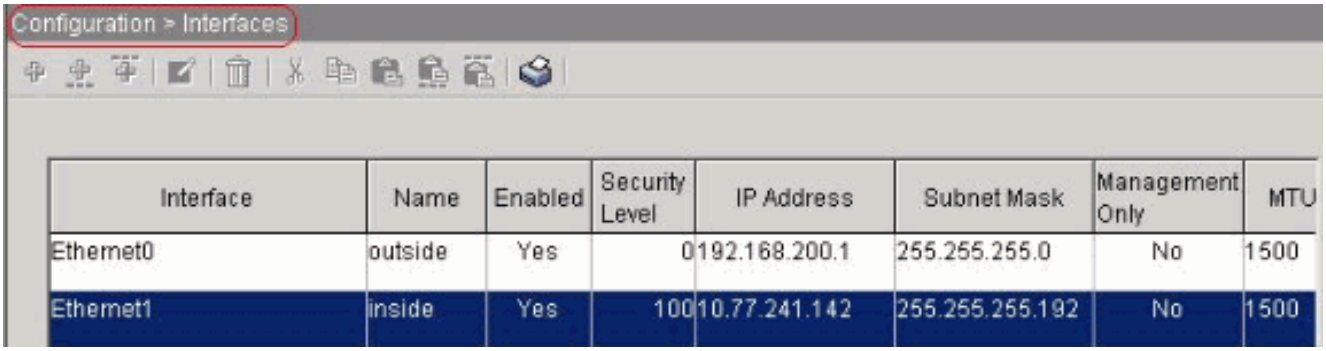
ملاحظة: راجع السماح بوصول HTTPS لـ ASDM للإعدادات الأساسية للوصول إلى PIX/ASA من خلال ASDM.

1. **تكوين الواجهات**أخترت **تشكيل حرانحيضيف** in order to شكلت القارن إثرنيت0 (خارج) و إثرنيت 1 (داخل) كما هو موضح.





وانقر فوق
OK.

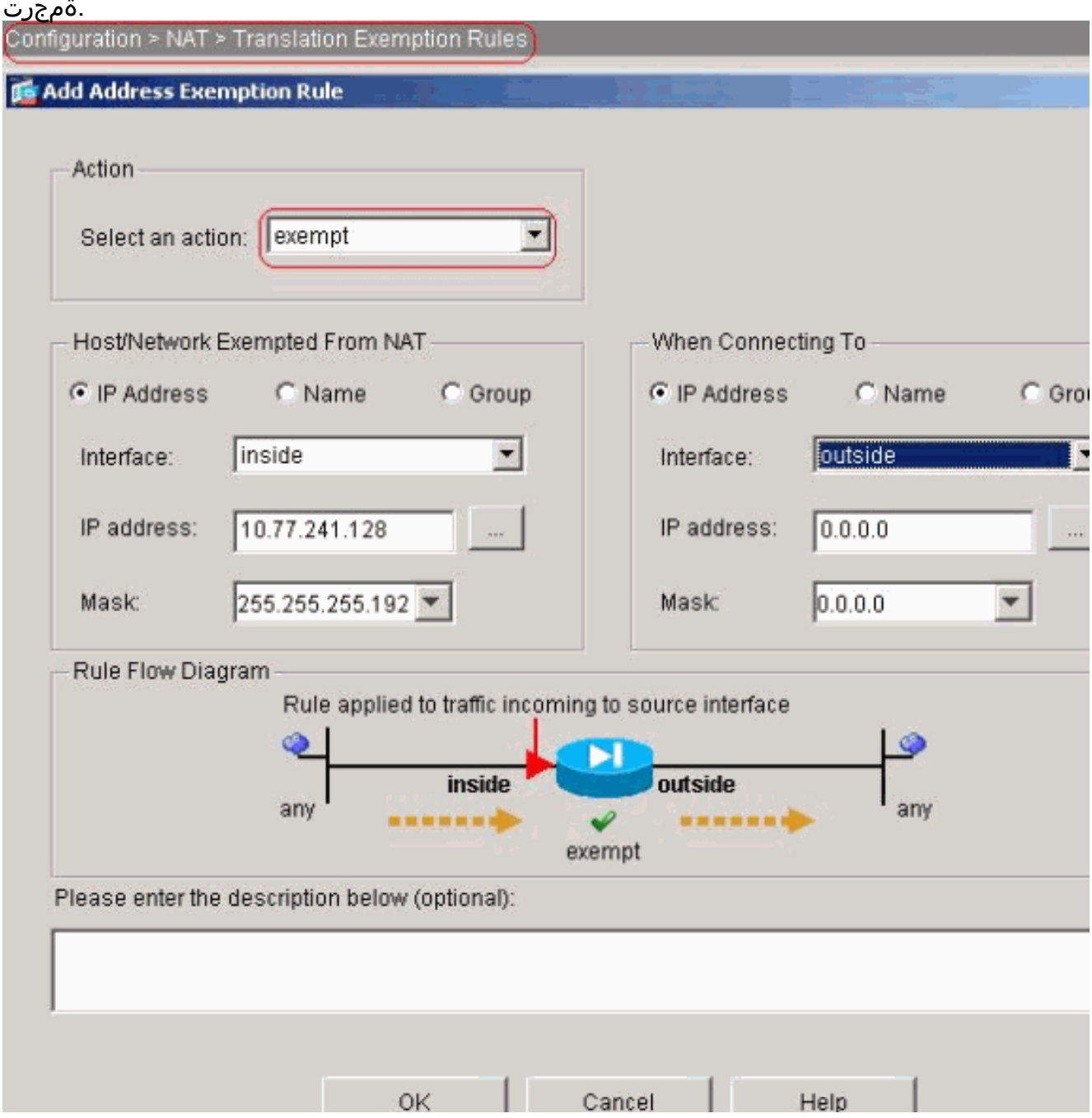


تكوين CLI المكافئ كما هو موضح:

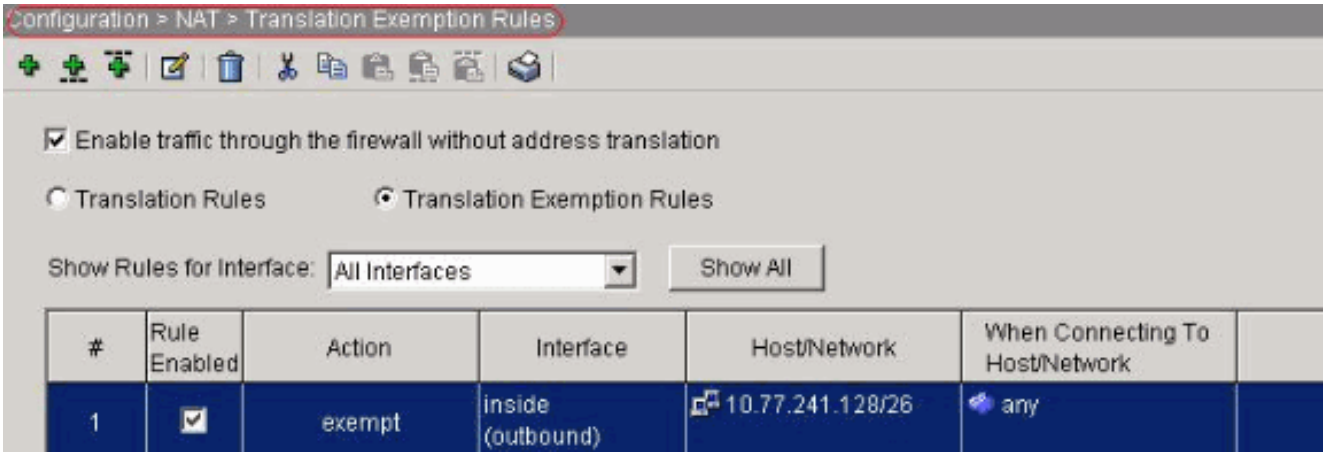
```
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.200.1 255.255.255.0
!
interface Ethernet1
```

```
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
```

2. **تكوين NAT 0**أخترت **تشكيل>nat>ترجمة إستثناء قاعدة>يضيف** in order to سمحت الحركة مرور من الشبكة 10.77.241.128/26 أن ينفذ الإنترنت دون أي ترجمة.



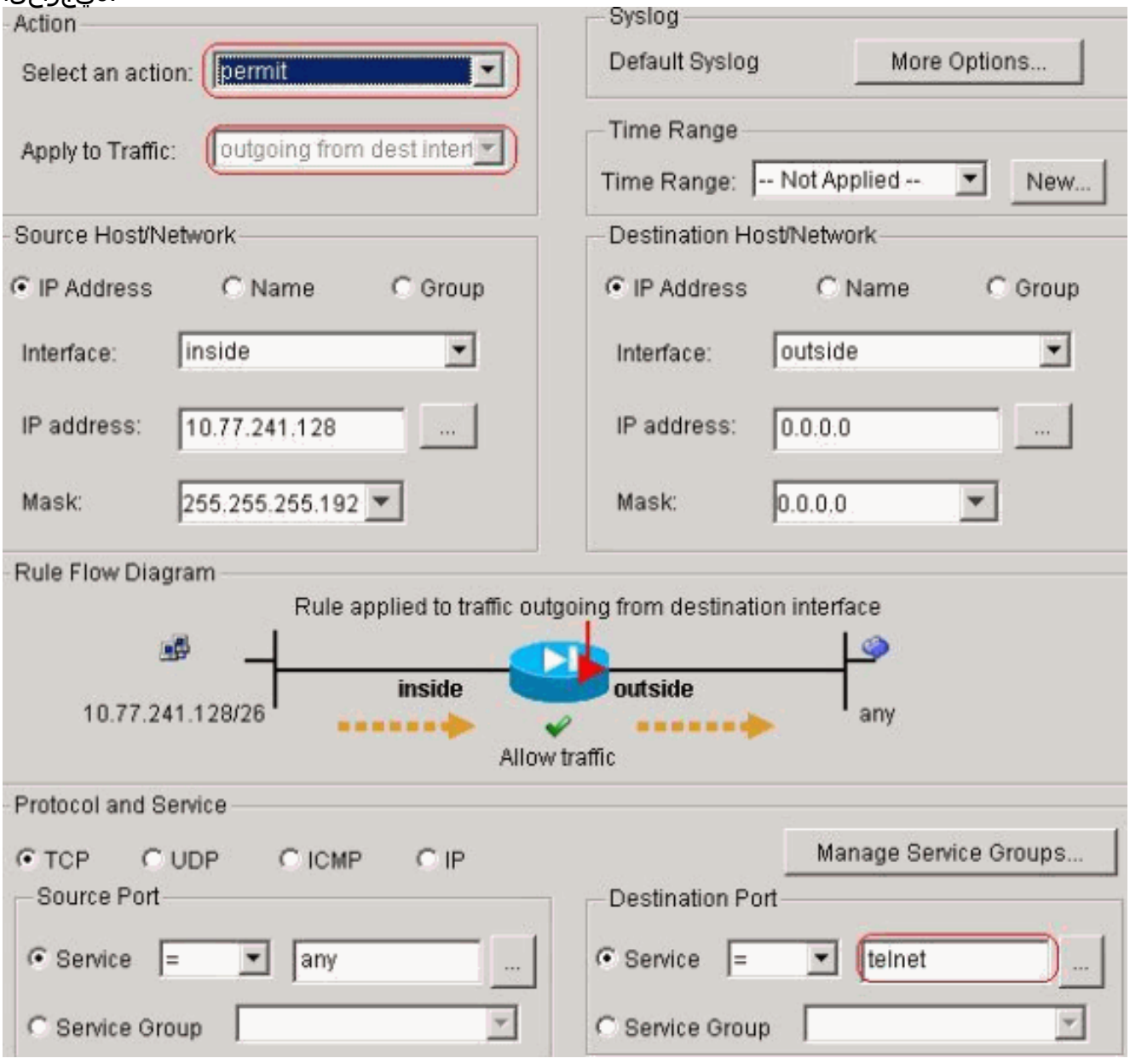
وانقر فوق **OK**.



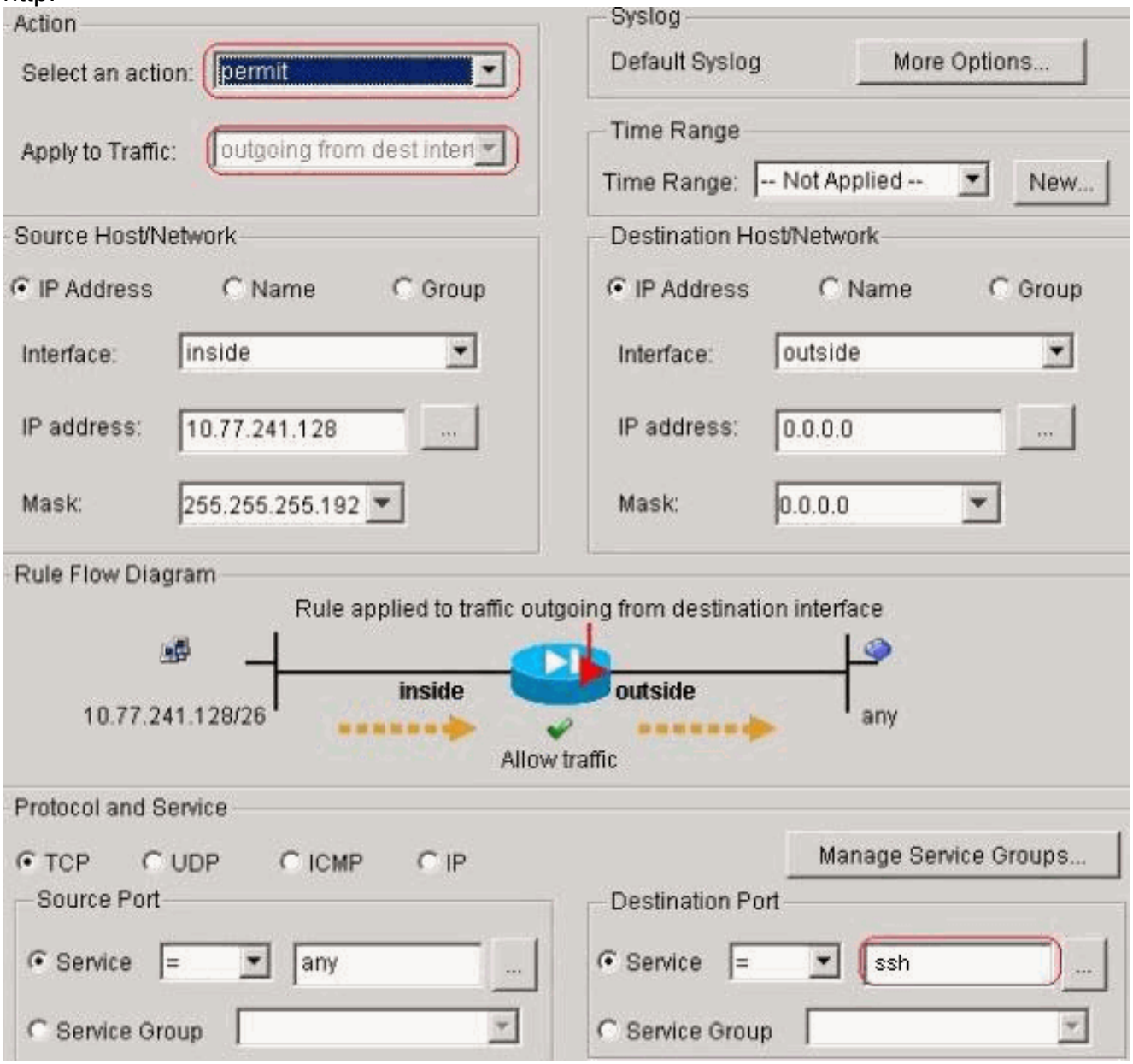
تكوين CLI المكافئ كما هو موضح:

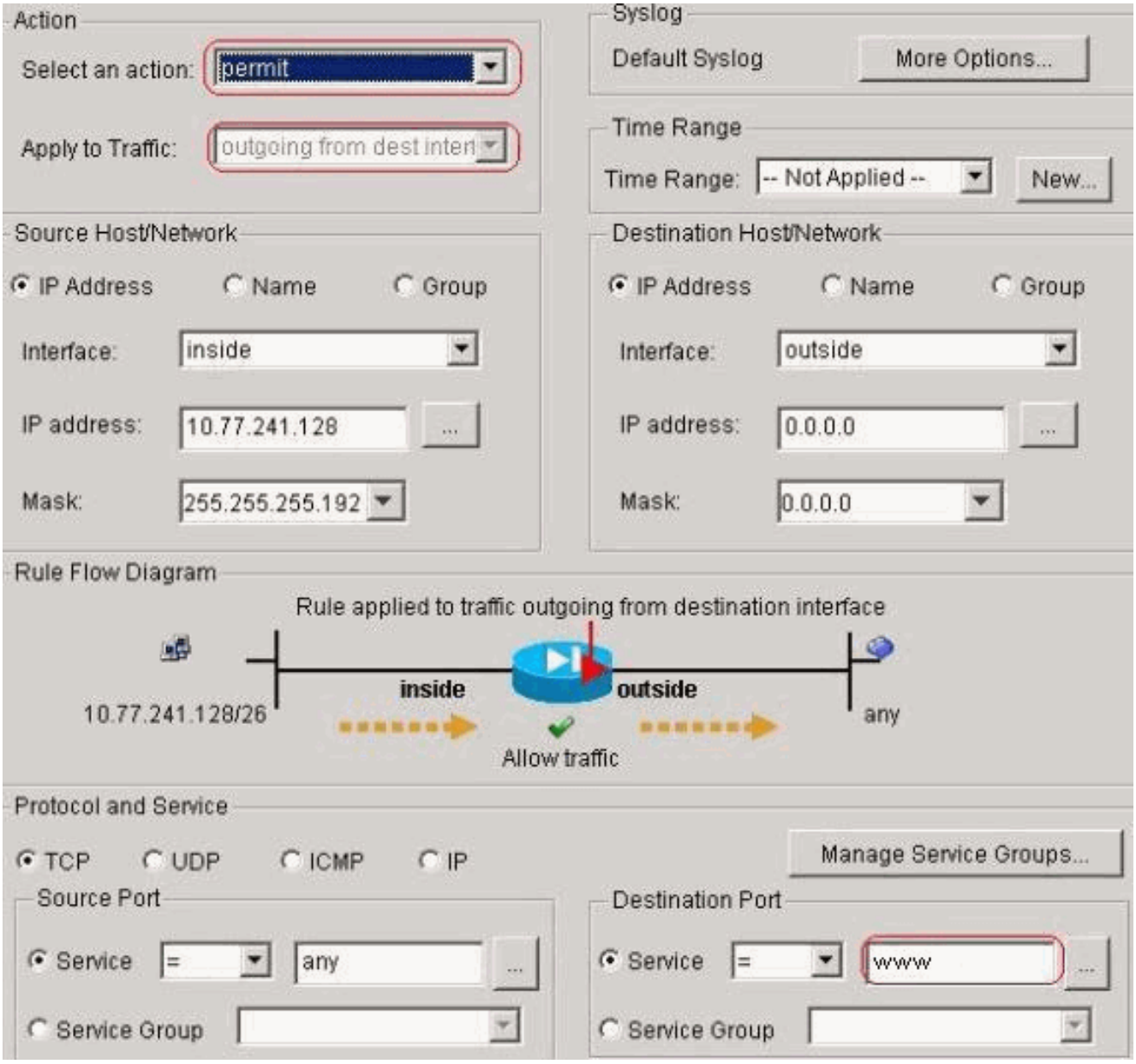
```
access-list inside_nat0_outbound extended permit ip 10.77.241.128 255.255.255.192 any
nat (inside) 0 access-list inside_nat0_outbound
```

3. **تكوين قواعد التحكم في الوصول إلى ACL**أختر **تكوين > سياسة الأمان >قواعد الوصول** لتكوين قواعد التحكم في الوصول (ACL) كما هو موضح.انقر فوق **إضافة** لتكوين قاعدة التحكم في الوصول (ACL) 101 التي تسمح بإنشاء حركة مرور Telnet من الشبكة 10.77.241.128/26 إلى أي شبكة وجهة وتطبيقها على حركة المرور الصادرة على الواجهة الخارجية.



وانقر فوق OK. وبالمثل لحركة مرور SSH و
http:

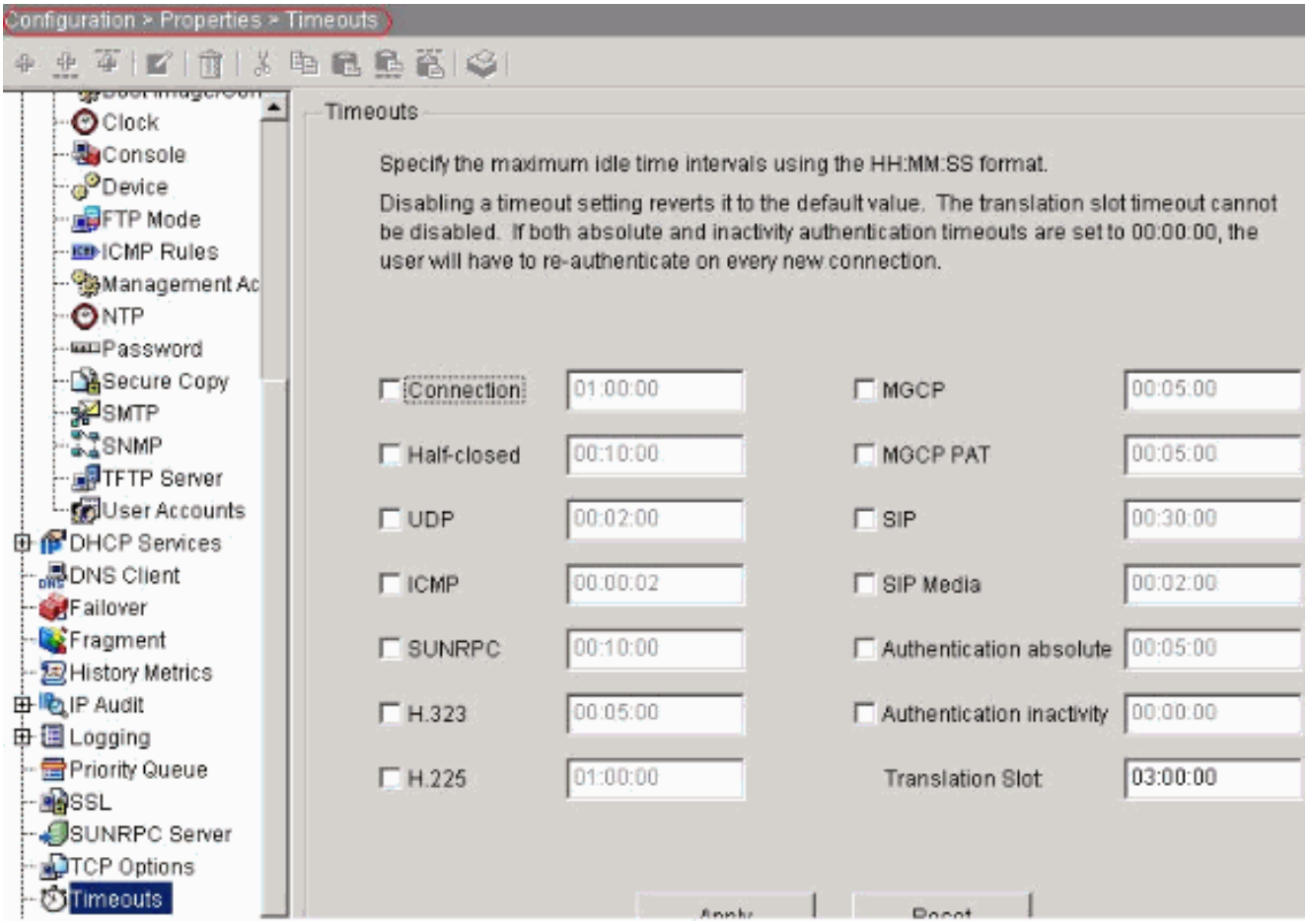




تكوين CLI المكافئ كما هو موضح:

```
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq telnet
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq ssh
access-list 101 extended permit tcp 10.77.241.128 255.255.255.192 any eq www
access-group 101 out interface outside
```

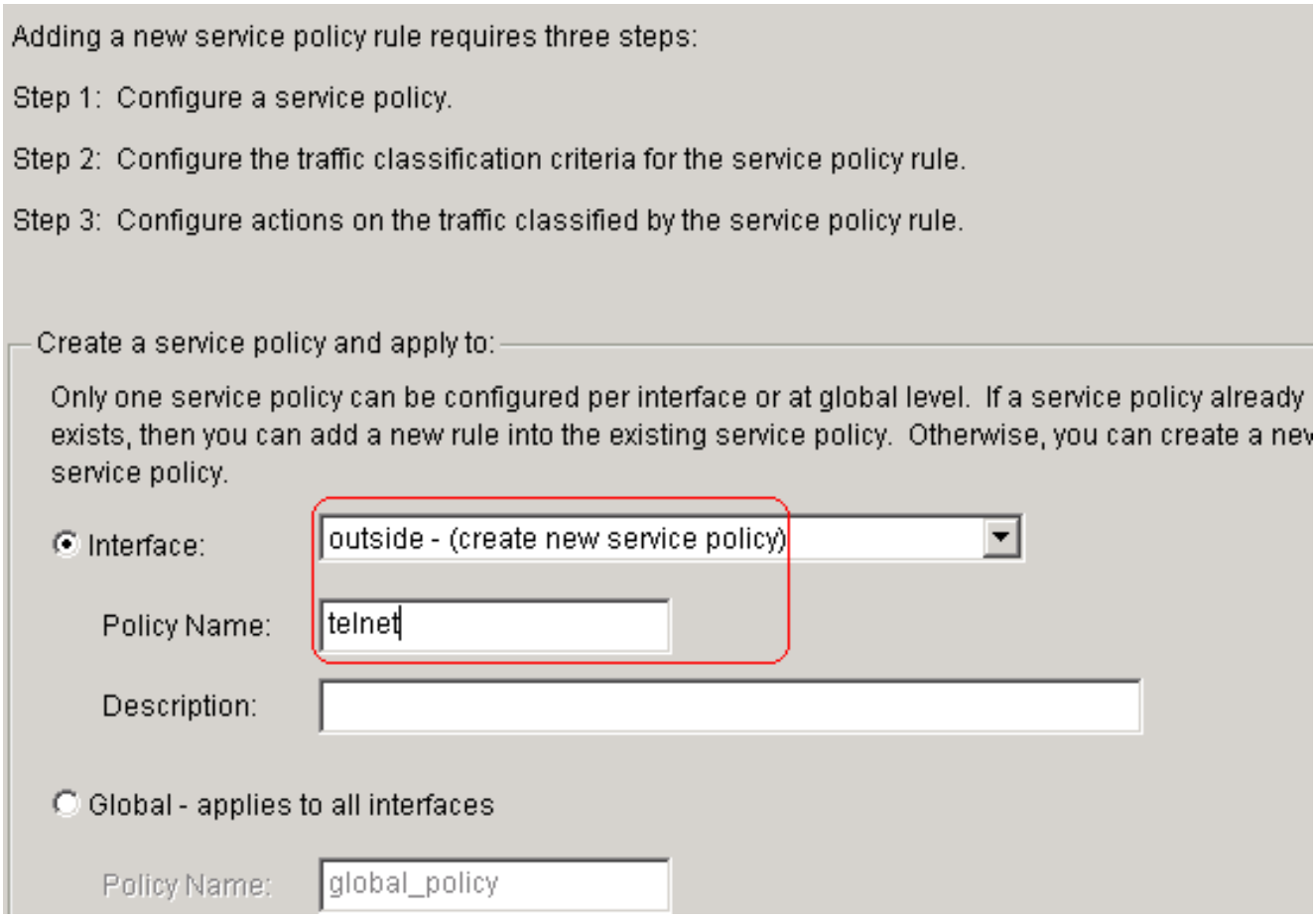
4. **تكوين حالات انتهاء المهلة**أخترت **تشكيل>خصائص>وقت** in order to شكلت المختلف وقت. في هذه السيناريو، احتفظ بالقيمة الافتراضية لجميع حالات انتهاء المهلة.



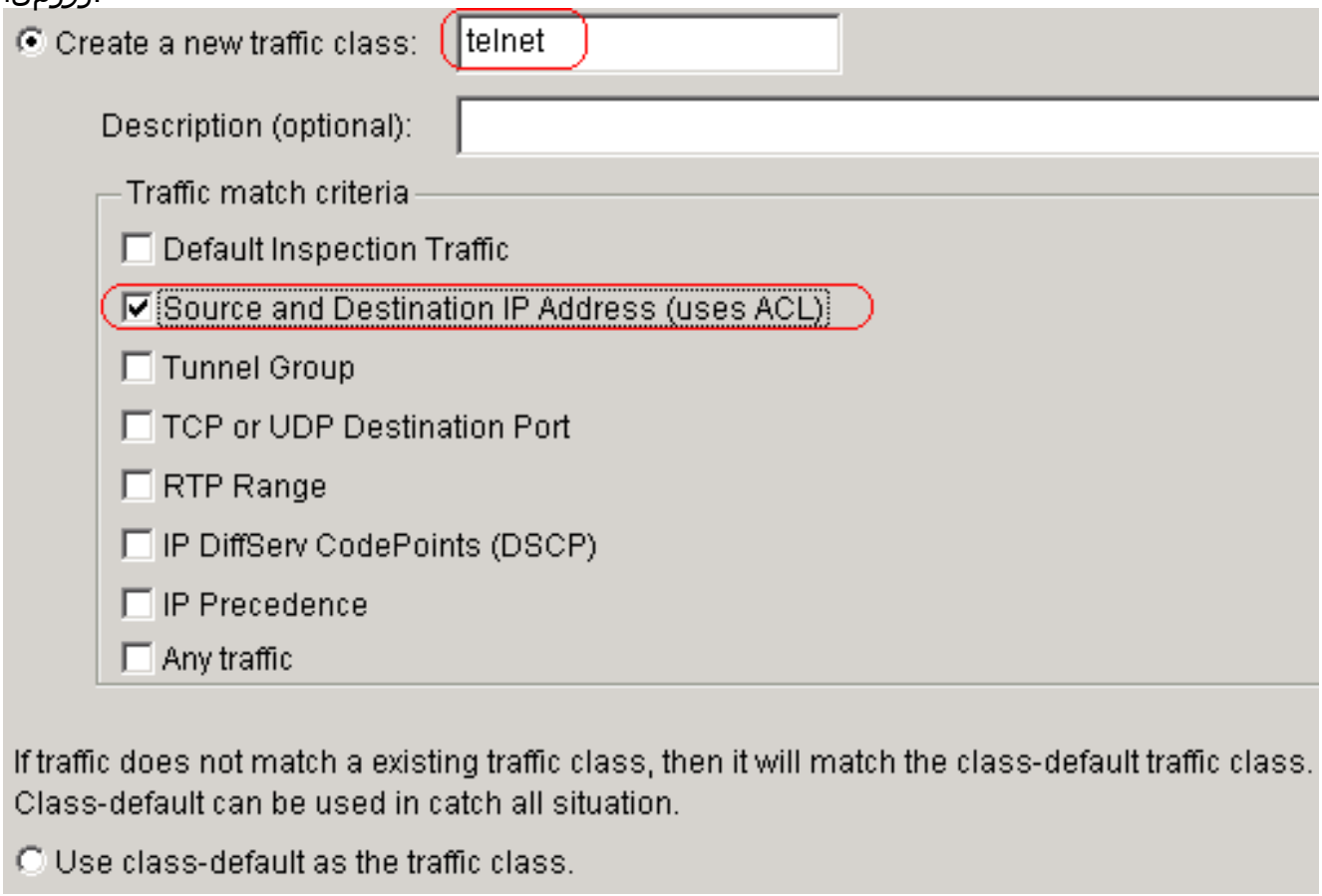
تكوين CLI المكافئ كما هو موضح:

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
```

5. تكوين **قواعد سياسة الخدمة**.أختر **تكوين > سياسة الأمان > قواعد سياسة الخدمة > إضافة** لتكوين خريطة الفئة، ومخطط السياسة لإعداد مهلة اتصال TCP ك10 دقائق، وتطبيق سياسة الخدمة على الواجهة الخارجية كما هو موضح.أخترت **القرين** لاسلكي in order to أخترت **خارجي - (ليخلق خدمة سياسة جديد)**، أي أن يكون خلقت، وعينت **telnet** كالسياسة
إسم.

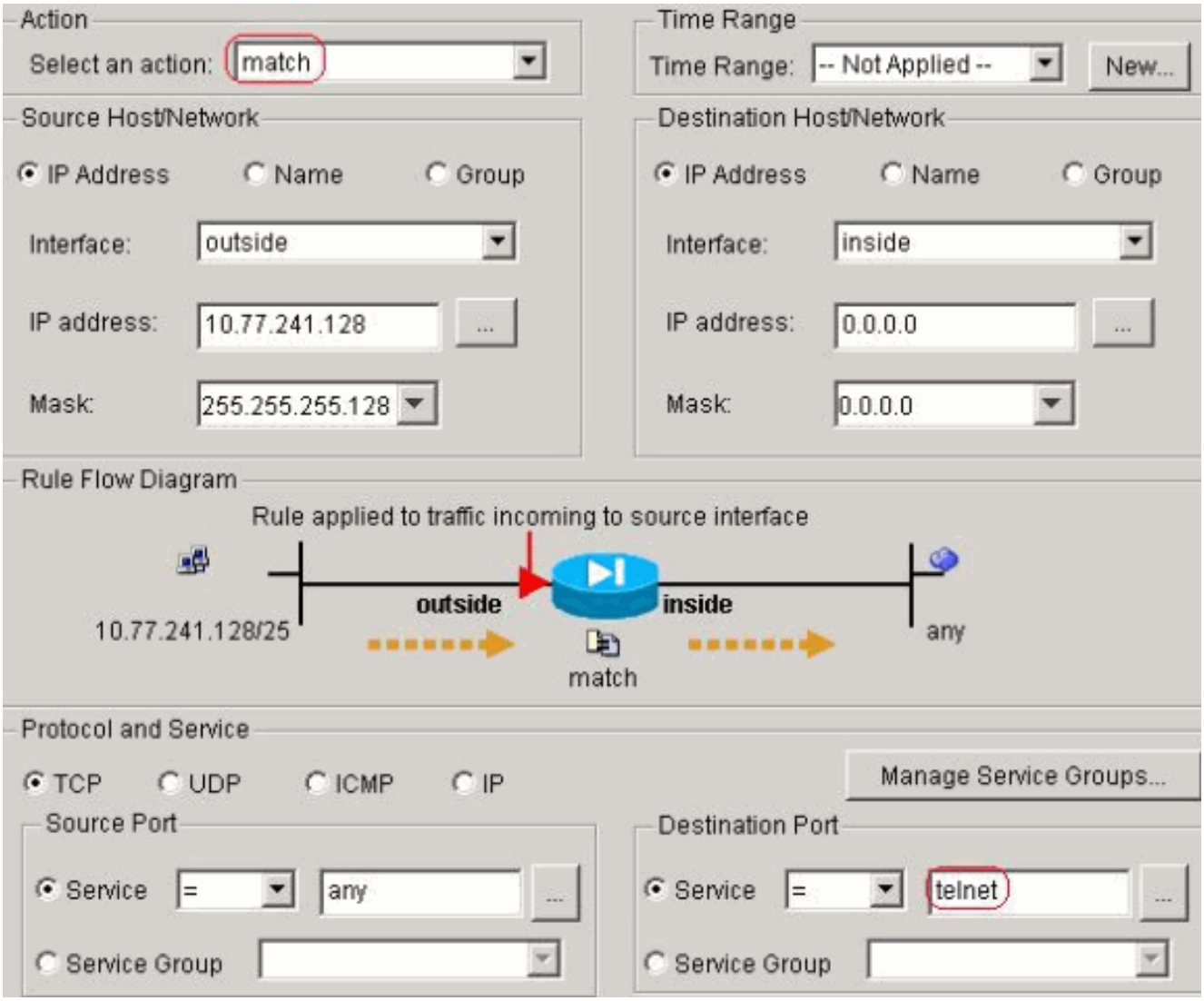


انقر فوق **Next (التالي)**.قم بإنشاء اسم خريطة الفئة **telnet** واختر **عنوان IP للمصدر والوجهة (يستخدم قائمة التحكم في الوصول (ACL)** خانة الاختيار في معايير مطابقة حركة
المرور.

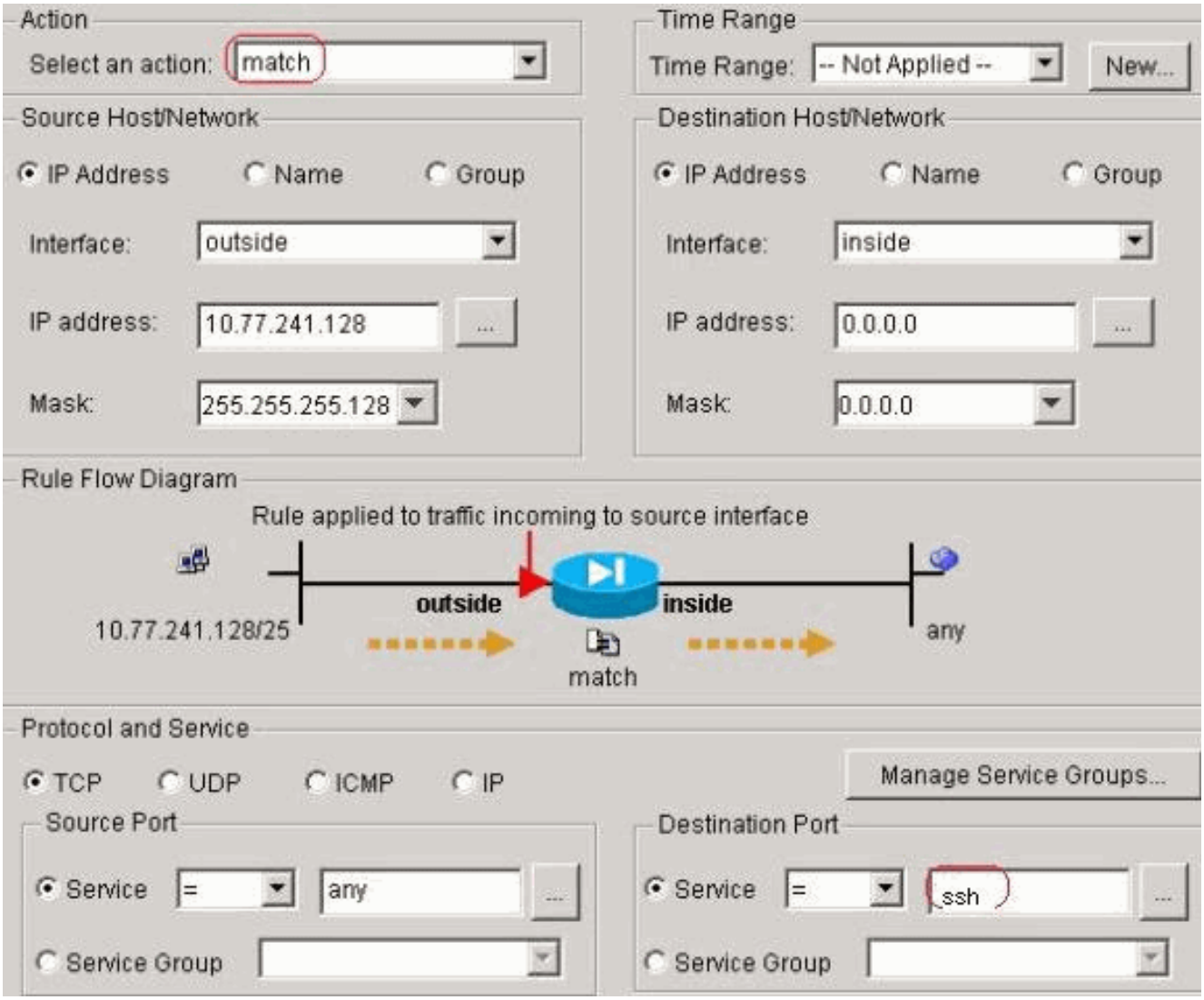


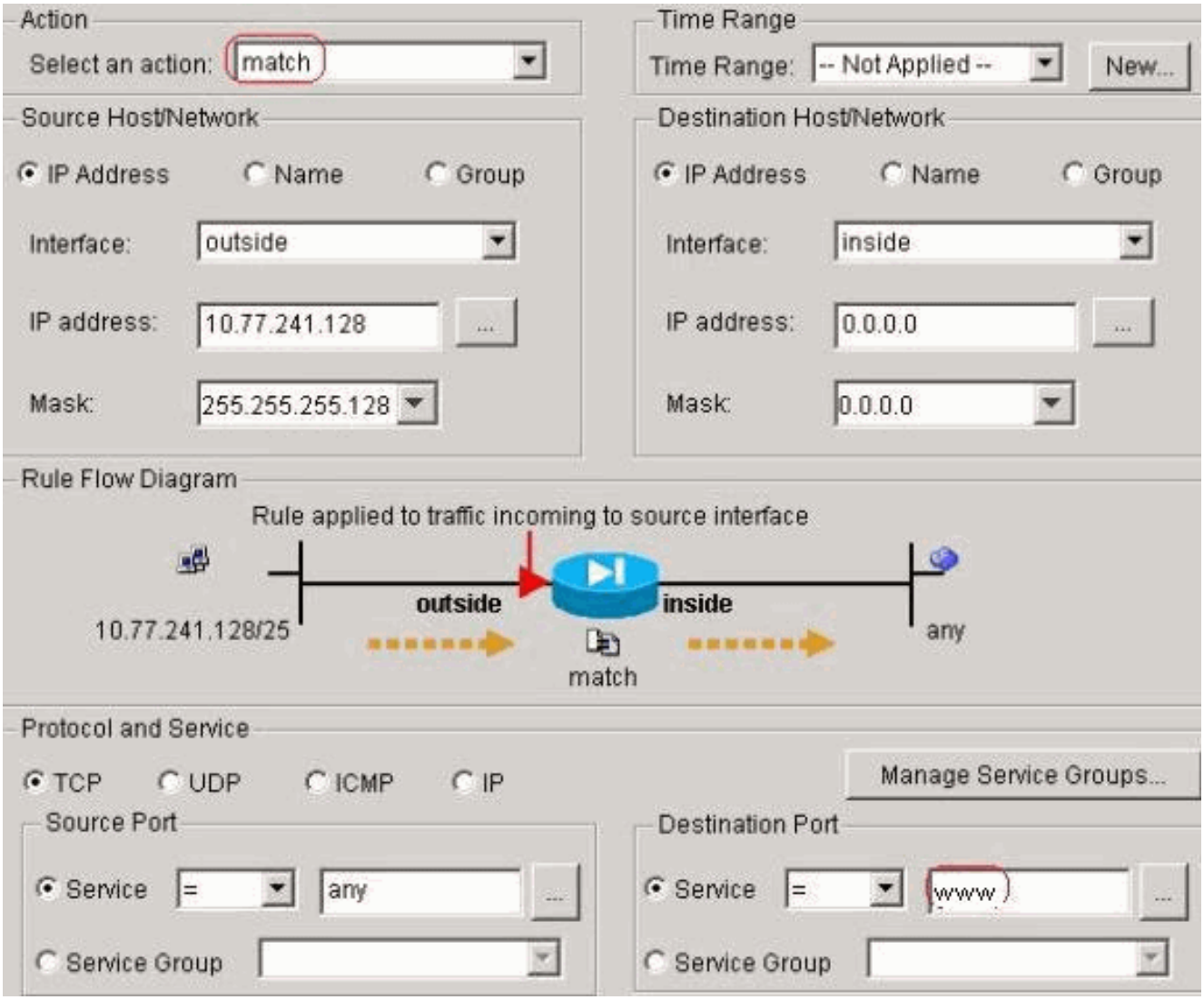
انقر فوق **Next (التالي)**.قم بإنشاء قائمة تحكم في الوصول (ACL) لمطابقة حركة

مرور Telnet التي تم إنشاؤها من الشبكة 10.77.241.128/26 إلى أي شبكة وجهة
وتطبيقها على الفئة
Telnet.

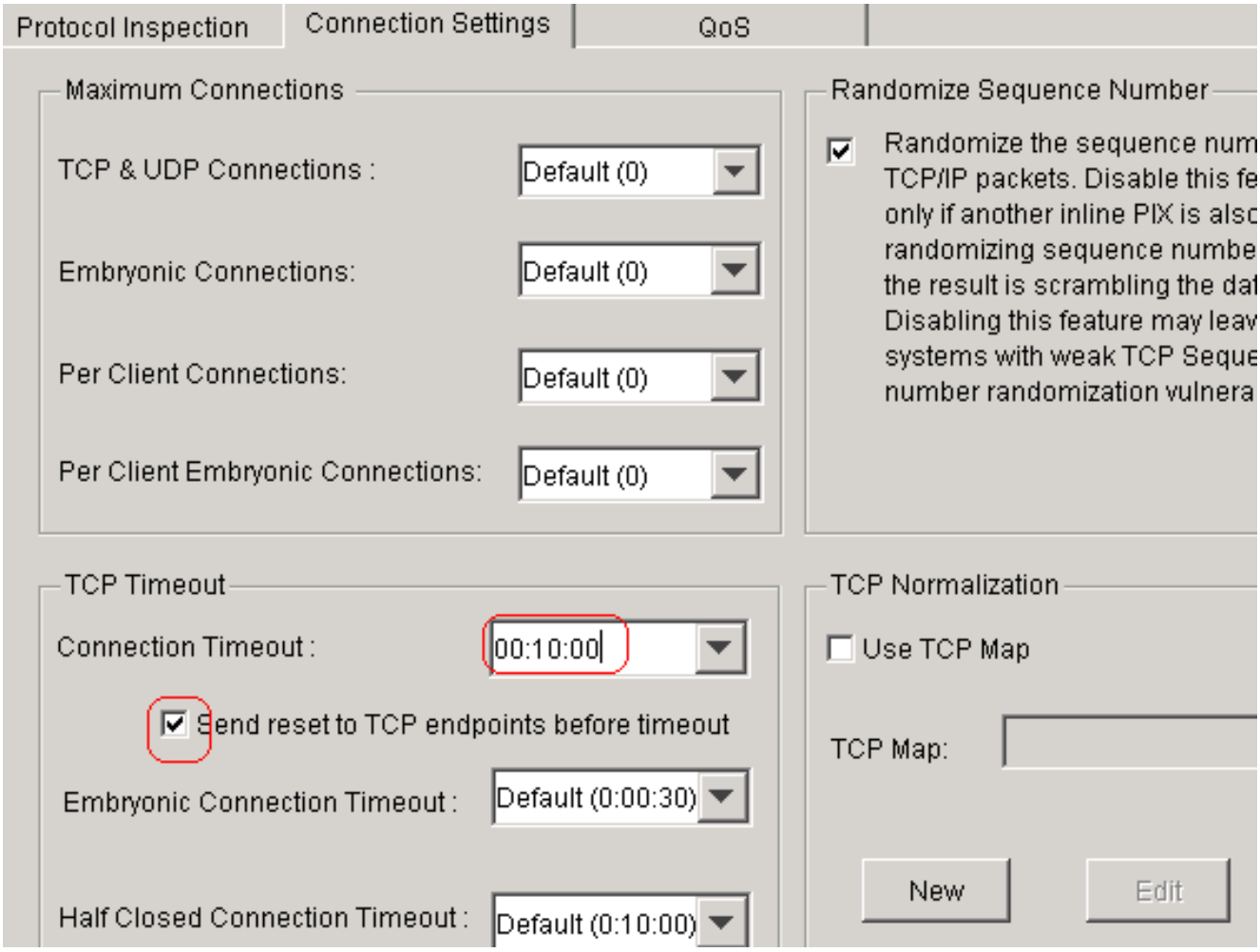


انقر فوق **Next (التالي)**. وبالمثل لحركة مرور SSH و
http:

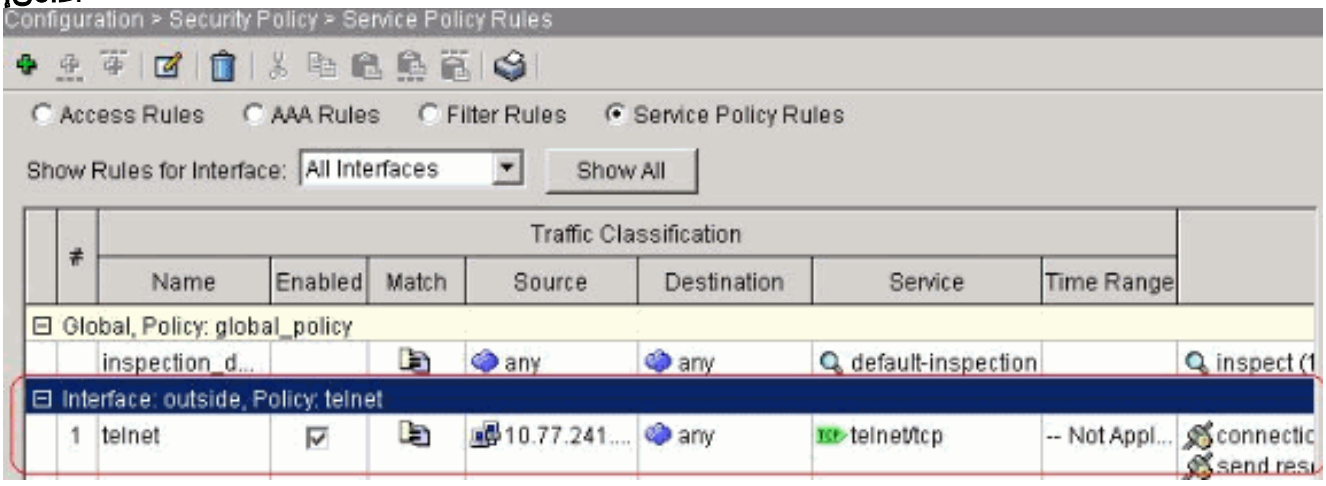

Action
Select an action: match
Time Range
Time Range: -- Not Applied --
New...
Source Host/Network
IP Address
Name
Group
Interface: outside
IP address: 10.77.241.128
Mask: 255.255.255.128
Destination Host/Network
IP Address
Name
Group
Interface: inside
IP address: 0.0.0.0
Mask: 0.0.0.0
Rule Flow Diagram
Rule applied to traffic incoming to source interface
10.77.241.128/25
outside
inside
any
match
Protocol and Service
TCP
UDP
ICMP
IP
Manage Service Groups...
Source Port
Service = any
Service Group
Destination Port
Service = ssh
Service Group



أختر **إعدادات الاتصال** لإعداد مهلة اتصال TCP ك10 دقائق، واختر أيضا خانة الاختيار **إرسال إعادة التعيين إلى نقاط نهاية TCP قبل المهلة**.



انقر فوق
انعام.



تكوين CLI المكافئ كما هو موضح:

```
access-list outside_mpc_in extended permit tcp host 10.77.241.129  any eq telnet
access-list outside_mpc_in extended permit tcp host 10.77.241.129 any eq ssh
access-list outside_mpc_in extended permit tcp host 10.77.241.129 any eq www

class-map telnet
 description telnet
  match access-list outside_mpc_in

policy-map telnet
class telnet
  set connection timeout tcp 00:10:00 reset
service-policy telnet interface outside
```

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؛ وبشكل افتراضي تكون مهلة SYN على ASA 30 ثانية. هذه هي الطريقة لتكوين 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
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاء المسجلين فقط) بعض أوامر show. استعملت ال OIT in order to شاهدت تحليل من **عرض** أمر إنتاج.

قم بإصدار الأمر **show service-policy interface** خارج النظام للتحقق من التكوينات الخاصة بك.

```
PIX#show service-policy interface outside

   Interface outside:
    Service-policy: http
     Class-map: http
      Set connection policy:
      Set connection timeout policy:
        tcp 0:05:00 reset
      Inspect: http, packet 80, drop 0, reset-drop 0
```

قم بإصدار الأمر show service-policy flow للتحقق من تطابق حركة المرور المحددة مع تكوينات سياسة الخدمة.

تعرض مخرجات الأمر هذه مثال:

```
PIX#show service-policy flow tcp host 10.77.241.129 host 10.1.1.2 eq 23

   Global policy:
  Service-policy: global_policy

Interface outside:
  Service-policy: telnet
    Class-map: telnet
      Match: access-list 101
        Access rule: permit tcp 10.77.241.128 255.255.255.192 any eq telnet
      Action:
        Input flow:  set connection timeout tcp 0:10:00 reset
```

استكشاف الأخطاء وإصلاحها

إذا وجدت أن مهلة الاتصال لا تعمل مع "إطار عمل السياسات النمطية" (MPF)، فتحقق من اتصال بدء بروتوكول TCP. يمكن أن تكون المشكلة عكس عنوان IP للمصدر والوجهة أو عنوان IP مكون بشكل غير صحيح في قائمة الوصول التي تطابق مع MPF لتعيين قيمة المهلة الجديدة أو لتغيير المهلة الافتراضية للتطبيق. قم بإنشاء إدخال قائمة وصول (المصدر والوجهة) وقم بدء الاتصال لتعيين مهلة الاتصال باستخدام MPF.

معلومات ذات صلة

- أجهزة الأمان Cisco PIX 500 Series Security Appliances
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)

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).