PIX/ASA 7.x والإصدارات الأحدث: توصيل شبكات داخلية متعددة بمثال تكوين الإنترنت

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
المنتجات ذات الصلة
الاصطلاحات
التكوين
معلومات أساسية
الرسم التخطيطي للشبكة
التكوينات
تكوين PIX باستخدام ASDM
تكوين PIX باستخدام CLI
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
أوامر استكشاف الأخطاء وإصلاحها
إجراء استكشاف الأخطاء وإصلاحها
تعذر الوصول إلى مواقع الويب بالاسم
معلومات ذات صلة

المقدمة

يقدم هذا المستند نموذجا لتكوين جهاز أمان PIX/ASA الإصدار x.7 والإصدارات الأحدث مع شبكات داخلية متعددة متصلة بالإنترنت (أو شبكة خارجية) باستخدام واجهة سطر الأوامر (CLI) أو مدير أجهزة الأمان القابل للتكيف ((ASDM 5.x والإصدارات الأحدث.

ارجع إلى إنشاء الاتصال واستكشاف أخطائه وإصلاحها من خلال جهاز أمان Cisco للحصول على معلومات حول كيفية إنشاء الاتصال واستكشاف أخطائه وإصلاحها من خلال PIX/ASA.

راجع إستخدام أوامر NAT و global و static و channel و access-list وإعادة توجيه المنفذ (إعادة التوجيه) على PIX للحصول على معلومات حول أوامر PIX العامة.

ملاحظة: يمكن أن تظهر بعض الخيارات في إصدارات ASDM الأخرى بشكل مختلف عن الخيارات الموجودة في ASDM 5.1. راجع وثائق ASDM للحصول على مزيد من المعلومات.

المتطلبات الأساسية

المتطلبات

عند إضافة أكثر من شبكة داخلية خلف جدار حماية PIX، تذكر هذه النقاط:

- لا يدعم PIX العنونة الثانوية.
- يجب إستخدام موجه خلف PIX لتحقيق التوجيه بين الشبكة الموجودة والشبكة التي تمت إضافتها حديثا.
- يجب أن تشير العبارة الافتراضية لجميع البيئات المضيفة إلى الموجه الداخلي.
- إضافة مسار افتراضي على الموجه الداخلي الذي يشير إلى PIX.
- قم بمسح ذاكرة التخزين المؤقت لبروتوكول تحليل العنوان (ARP) على الموجه الداخلي.

ارجع إلى السماح بوصول HTTPS ل ASDM للسماح بتكوين الجهاز بواسطة ASDM.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز أمان PIX 515E مع إصدار برنامج 7.1
- ASDM 5.1
- cisco مسحاج تخديد مع cisco ios ® برمجية إطلاق T(7)12.3

ملاحظة: تمت إعادة تصنيف هذا المستند باستخدام برنامج PIX/ASA الإصدار x.8 وبرنامج Cisco IOS الإصدار 12.4.

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.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco ASA الإصدار x.7 والإصدارات الأحدث.

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.

مخططات عنونة IP المستخدمة في هذا التكوين غير قابلة للتوجيه من الناحية القانونية على الإنترنت. وهي عناوين RFC 1918 التي تم استخدامها في بيئة مختبرية.

معلومات أساسية

في هذا السيناريو، هناك ثلاث شبكات داخلية (24/10.1.1.0 و 24/10.2.1.0 و 24/10.3.1.0) سيتم توصيلها بالإنترنت (أو شبكة خارجية) من خلال PIX. يتم توصيل الشبكات الداخلية بالواجهة الداخلية ل PIX. يتم اتصال الإنترنت من خلال موجه يتم توصيله بالواجهة الخارجية ل PIX. يحتوي PIX على عنوان IP 172.16.1.1/24.

يتم إستخدام المسارات الثابتة لتوجيه الحزم من الشبكات الداخلية إلى الإنترنت والعكس. بدلا من إستخدام المسارات الثابتة، يمكنك أيضا إستخدام بروتوكول توجيه ديناميكي مثل بروتوكول معلومات التوجيه (RIP) أو فتح أقصر مسار أولا (OSPF).

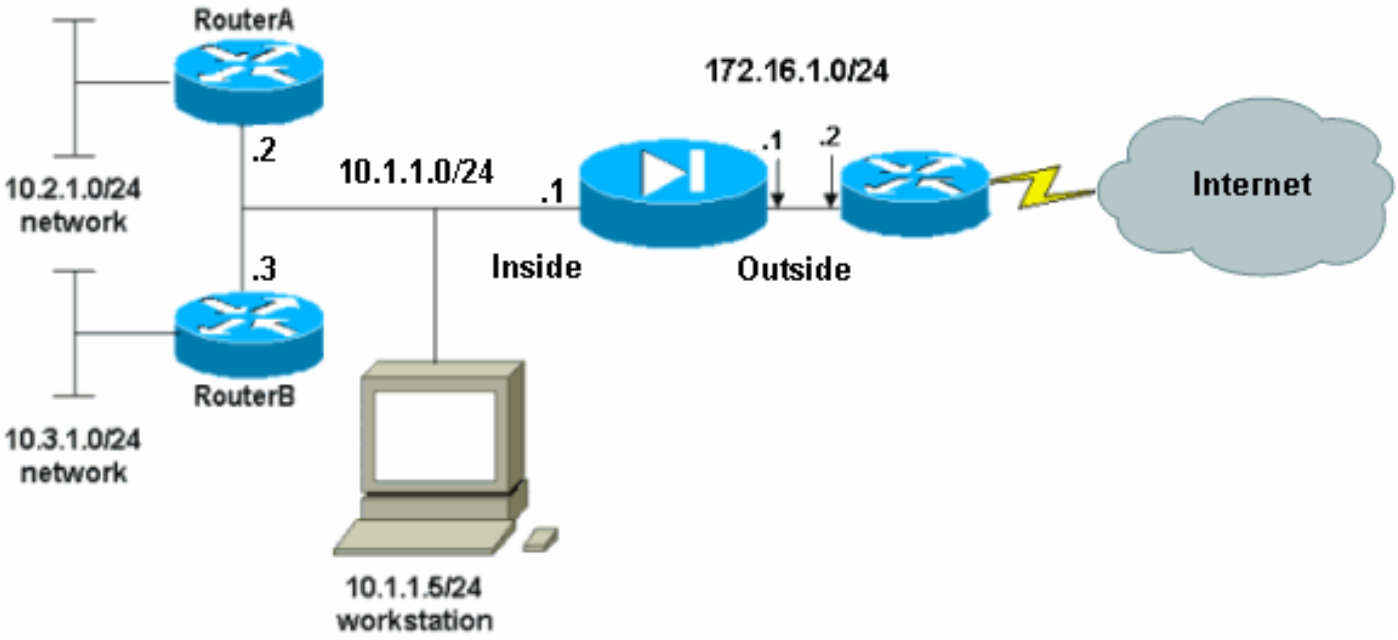
تتصل الأجهزة المضيفة الداخلية بالإنترنت عن طريق ترجمة الشبكات الداخلية على PIX باستخدام NAT الديناميكي (مجموعة عناوين IP - 172.16.1.5 إلى 172.16.1.10). إذا تم استنفاد تجمع عناوين IP، سيقوم PIX بتعليم (باستخدام عنوان IP 172.16.1.4) الأجهزة المضيفة الداخلية للوصول إلى الإنترنت.

راجع عبارات PIX/ASA 7.x NAT و PAT للحصول على مزيد من المعلومات حول NAT/PAT.

ملاحظة: إذا كان NAT الثابت يستخدم عنوان IP الخارجي (global_ip) للترجمة، فقد يؤدي ذلك إلى ترجمة. لذلك، استعملت الكلمة المفتاح قارن بدلا من العنوان في الترجمة ساكن إستاتيكي.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تشير العبارة الافتراضية للمضيفين على الشبكة 10.1.1.0 إلى الموجه A. تتم إضافة مسار افتراضي على RouterB يشير إلى RouterA. يحتوي الموجه A على مسار افتراضي يشير إلى واجهة PIX الداخلية.

التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين الموجه A
- تكوين RouterB
- تكوين جهاز أمان PIX 7.1تكوين PIX باستخدام ASDMتكوين واجهة سطر الأوامر (CLI) عبر جهاز أمان PIX

تكوين الموجه A

```
RouterA#show running-config
...Building configuration

Current configuration : 1151 bytes
!
```

```
version 12.4
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!

interface Ethernet2/0
ip address 10.2.1.1 255.255.255.0
half-duplex
!

interface Ethernet2/1
ip address 10.1.1.2 255.255.255.0
half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
!
!
line con 0
line aux 0
line vty 0 4
!
end
#RouterA
```

تكوين RouterB

```
RouterB#show running-config
...Building configuration
Current configuration : 1132 bytes
!
version 12.4
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterB
!

interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
speed auto
!

interface Ethernet1/0
ip address 10.3.1.1 255.255.255.0
half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
control-plane
!
!
line con 0
```

```
line aux 0
line vty 0 4
!
end
#RouterB
```

إذا كنت ترغب في إستخدام ASDM لتكوين جهاز أمان PIX، ولكن لم تقم بتمهيد الجهاز، أكمل الخطوات التالية:

1. وحدة تحكم في PIX.
2. من تكوين ممسوح، أستخدم المطالبات التفاعلية لتمكين ASDM لإدارة PIX من محطة العمل 10.1.1.5.

تكوين جهاز أمان PIX 7.1

```
  Pre-configure Firewall now through interactive prompts
                                          [yes]? yes
                                  :[Firewall Mode [Routed
        Enable password [<use current password>]: cisco
                          ?[Allow password recovery [yes
                                       :(Clock (UTC
                                    :[Year [2005
                                    :[Month [Mar
                                       :[Day [15
                               Time [05:40:35]: 14:45:00
                               Inside IP address: 10.1.1.1
                      Inside network mask: 255.255.255.0
                                    Host name: OZ-PIX
                                 Domain name: cisco.com
    IP address of host running Device Manager: 10.1.1.5

              :The following configuration will be used
                         Enable password: cisco
                     Allow password recovery: yes
                Clock (UTC): 14:45:00 Mar 15 2005
                        Firewall Mode: Routed
                  Inside IP address: 10.1.1.1
              Inside network mask: 255.255.255.0
                           Host name: OZ-PIX
                       Domain name: cisco.com
    IP address of host running Device Manager:
                                          10.1.1.5

         Use this configuration and write to flash? yes
INFO: Security level for "inside" set to 100 by
                                          .default
     Cryptochecksum: a0bff9bb aa3d815f c9fd269a
                                          3f67fef5

                           bytes copied in 0.880 secs 965
  INFO: converting 'fixup protocol dns maximum-
                               length 512' to MPF commands
INFO: converting 'fixup protocol ftp 21' to MPF
                                          commands
     INFO: converting 'fixup protocol h323_h225
                                    1720' to MPF commands
INFO: converting 'fixup protocol h323_ras 1718-
                                    1719' to MPF commands
  INFO: converting 'fixup protocol netbios 137-
                                     138' to MPF commands
   INFO: converting 'fixup protocol rsh 514' to
                                          MPF commands
  INFO: converting 'fixup protocol rtsp 554' to
```

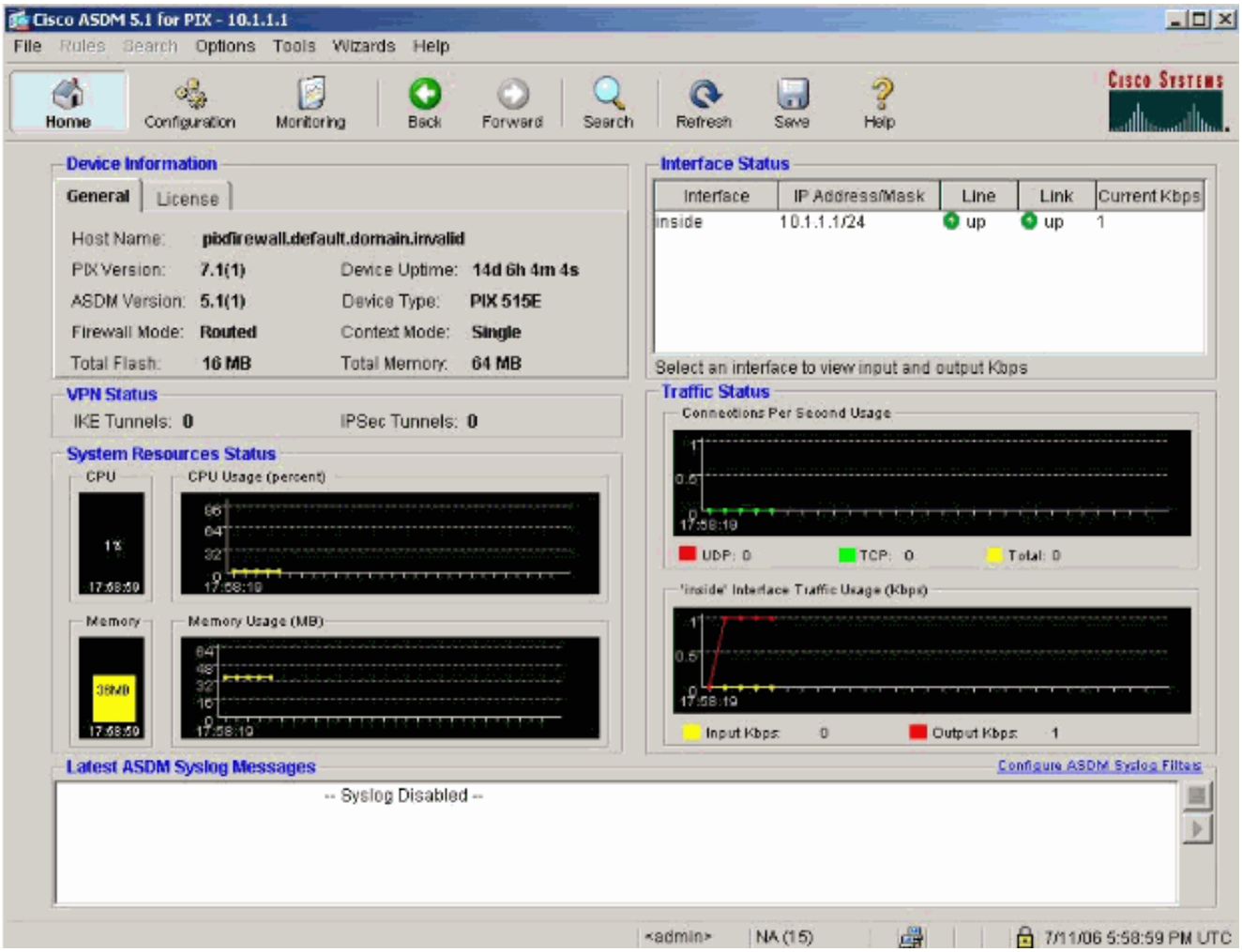
```
                                                    MPF commands
 INFO: converting 'fixup protocol sip 5060' to
                                                    MPF commands
 INFO: converting 'fixup protocol skinny 2000'
                                                 to MPF commands
  INFO: converting 'fixup protocol smtp 25' to
                                                    MPF commands
 INFO: converting 'fixup protocol sqlnet 1521'
                                                 to MPF commands
   INFO: converting 'fixup protocol sunrpc_udp
                                              111' to MPF commands
  INFO: converting 'fixup protocol tftp 69' to
                                                    MPF commands
INFO: converting 'fixup protocol sip udp 5060'
                                                 to MPF commands
INFO: converting 'fixup protocol xdmcp 177' to
                                                    MPF commands

     .Type help or '?' for a list of available commands
                                                 <OZ-PIX
```

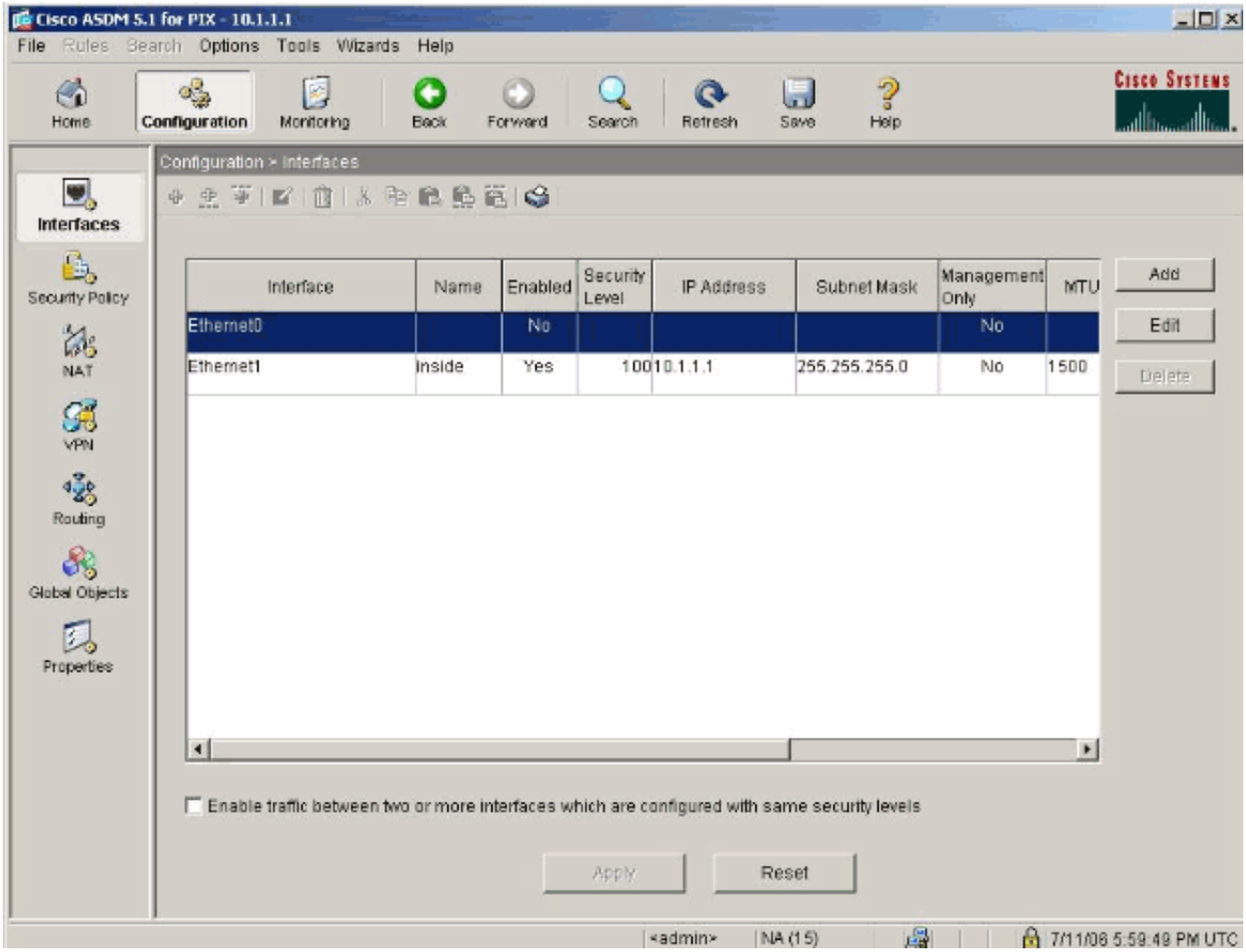
تكوين PIX باستخدام ASDM

أتمت هذا steps in order to شكلت عبر ال ASDM GUI:

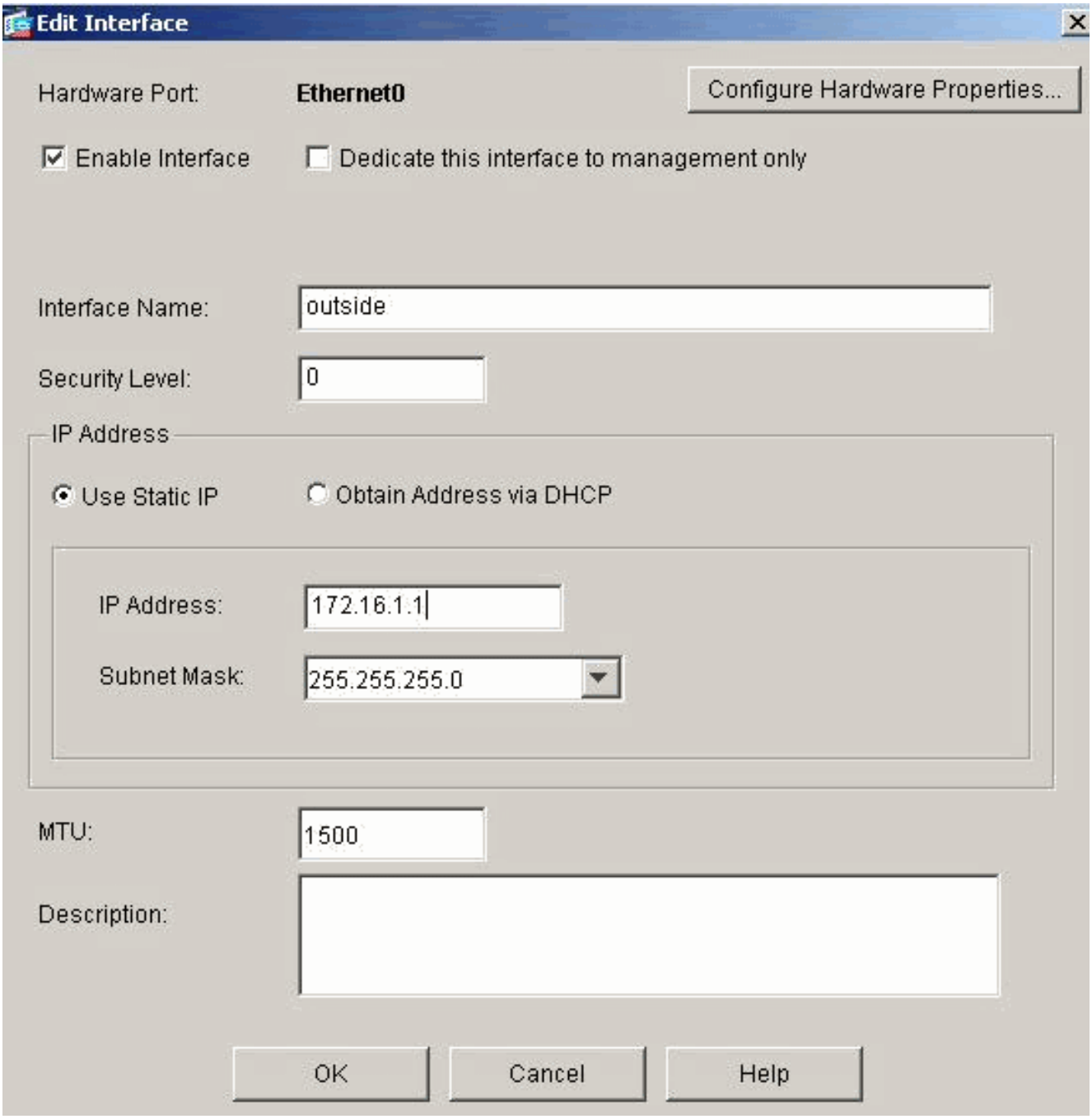
1. من محطة العمل 10.1.1.5، افتح مستعرض ويب لاستخدام ADSM (في هذا المثال، https://10.1.1.1).
2. طقطقة **نعم** على مطالبات الشهادة.
3. قم بتسجيل الدخول باستخدام كلمة مرور enable ، كما تم تكوينها مسبقا.
4. إذا كانت هذه هي المرة الأولى التي يتم فيها تشغيل ASDM على الكمبيوتر الشخصي، يوعز إليك باستخدام مشغل ASDM أو ASDM كتطبيق Java. في هذا المثال، يتم تحديد مشغل ASDM وتثبيته.
5. انتقل إلى نافذة ASDM الرئيسية وانقر فوق **تكوين**.



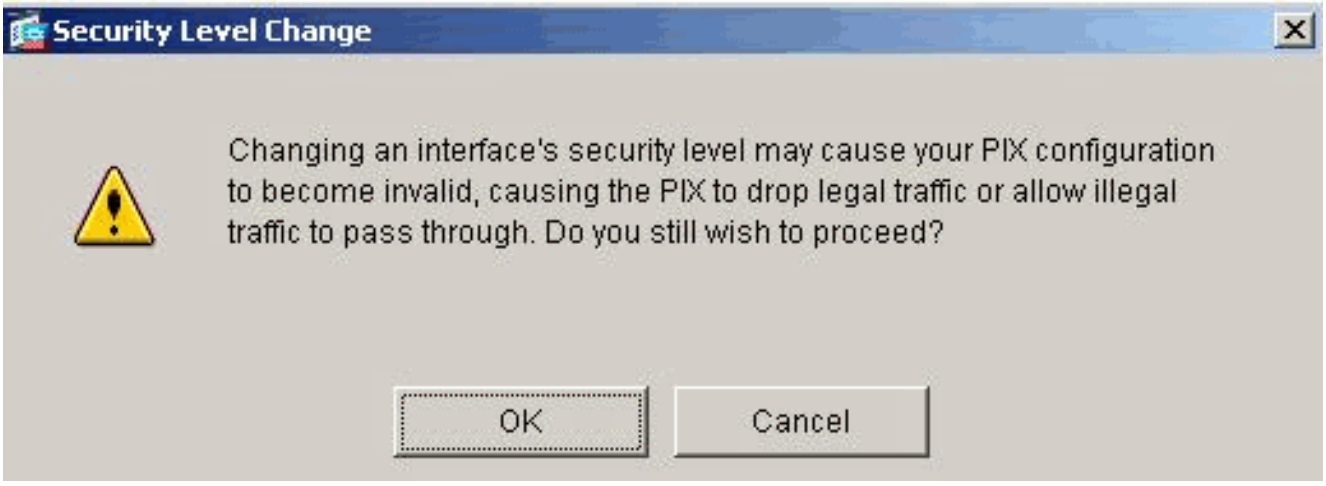
6. أخترت **قارن>يحرر** in order to شكلت القارن خارجي.



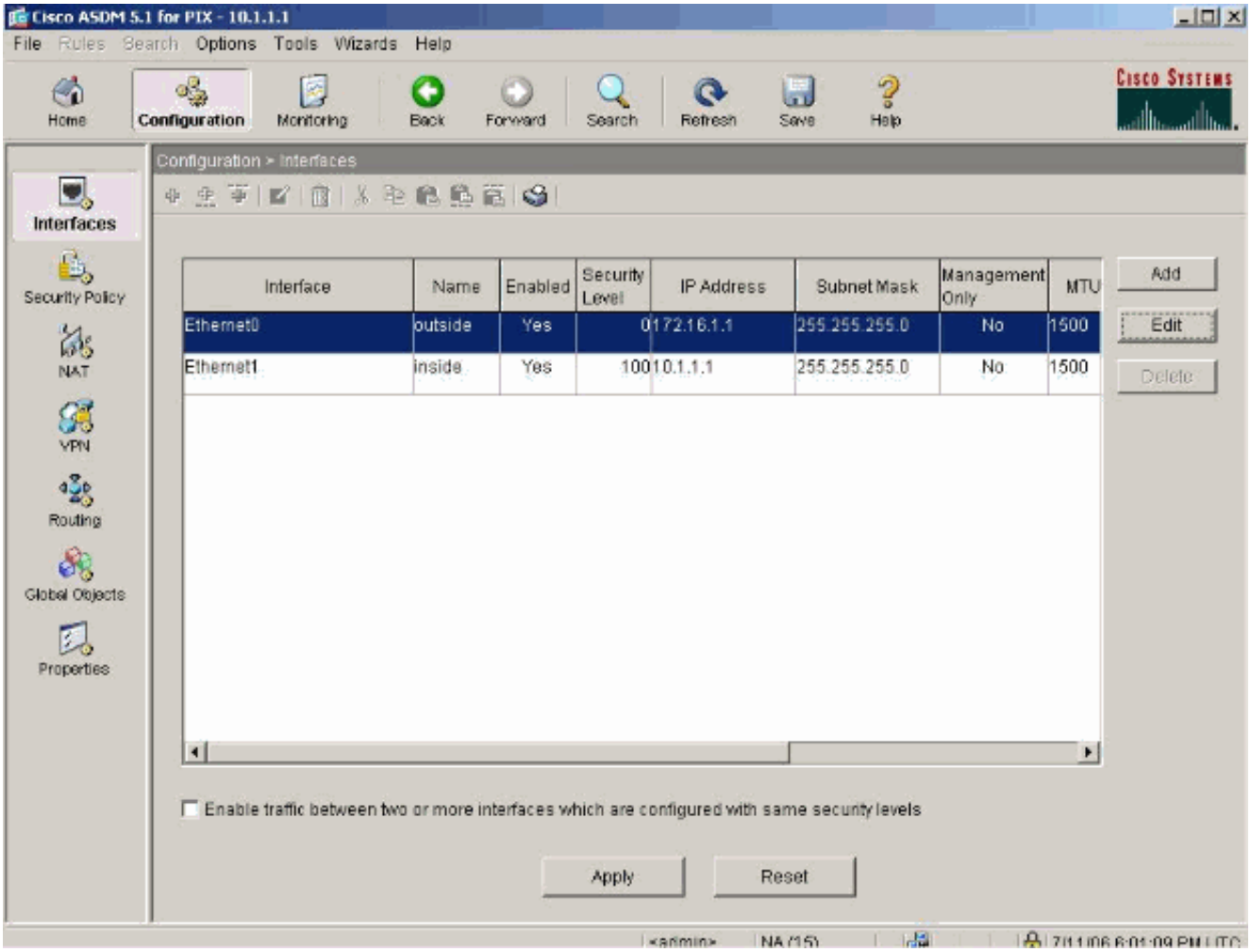
7. أدخل تفاصيل الواجهة وانقر فوق **موافق** عند انتهائك.



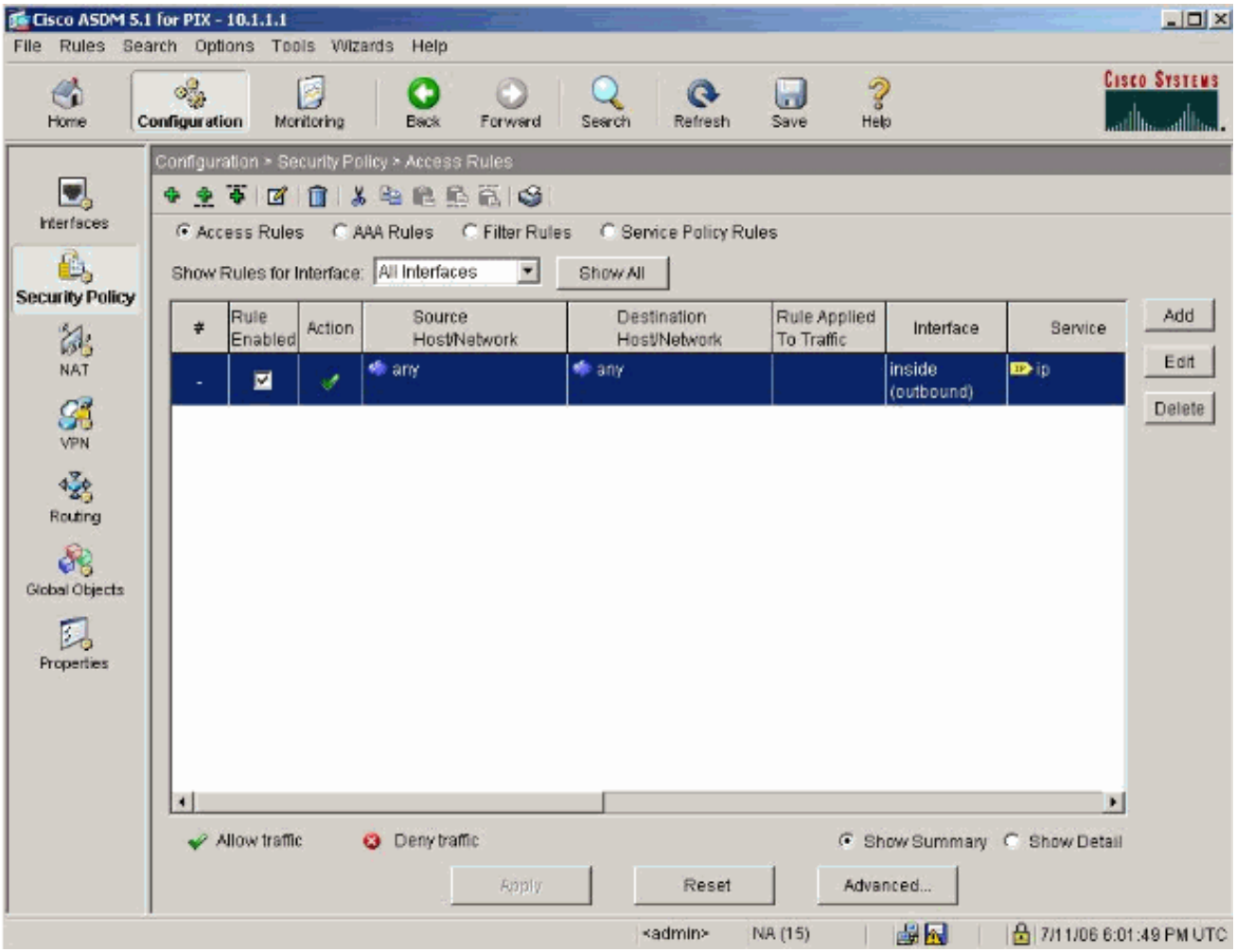
8. انقر فوق **موافق** في شاشة تغيير مستوى الأمان.



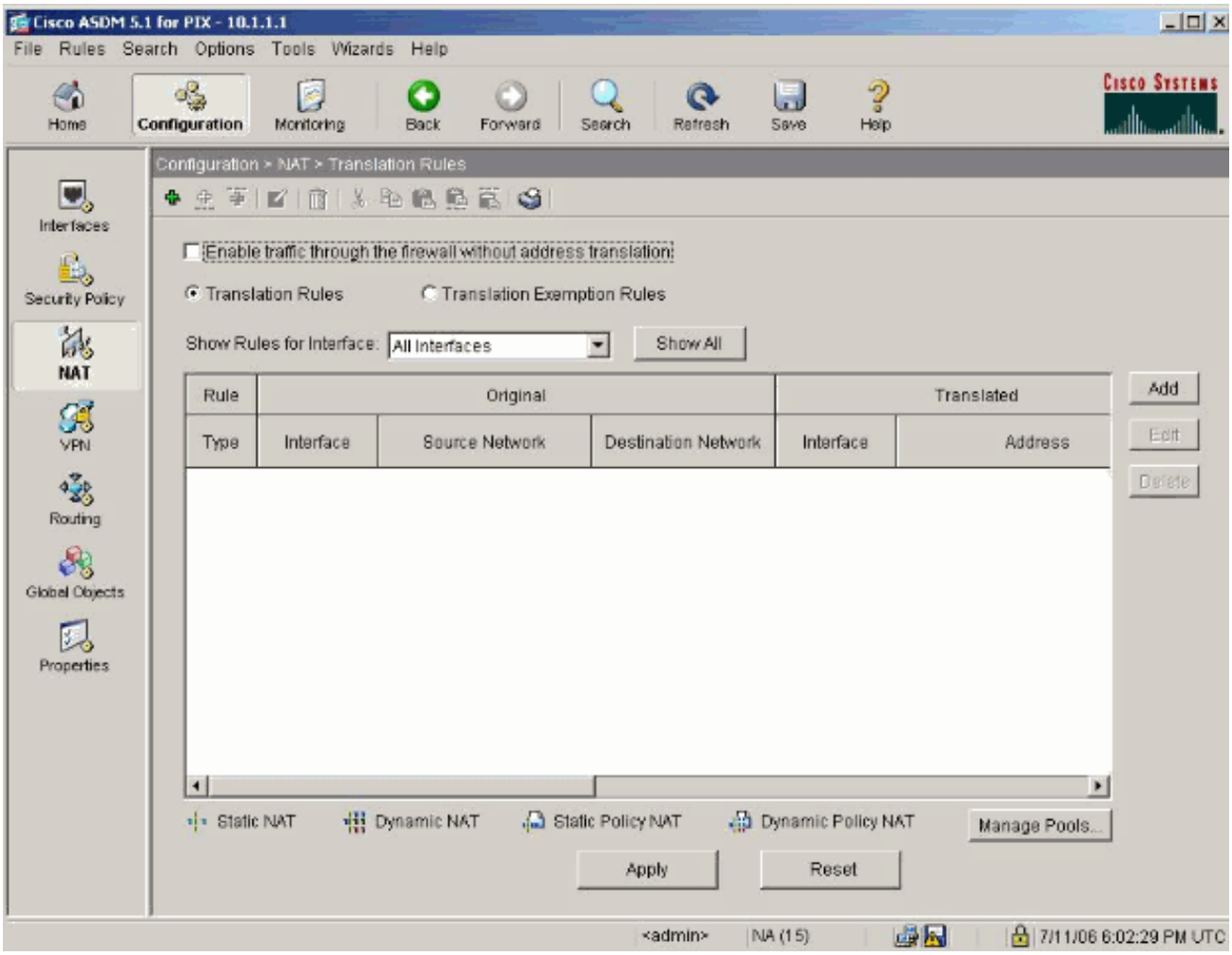
9. طقطقة **يطبق** أن يقبل القارن تشكيل. كما يتم دفع التهيئة إلى تطبيق PIX.



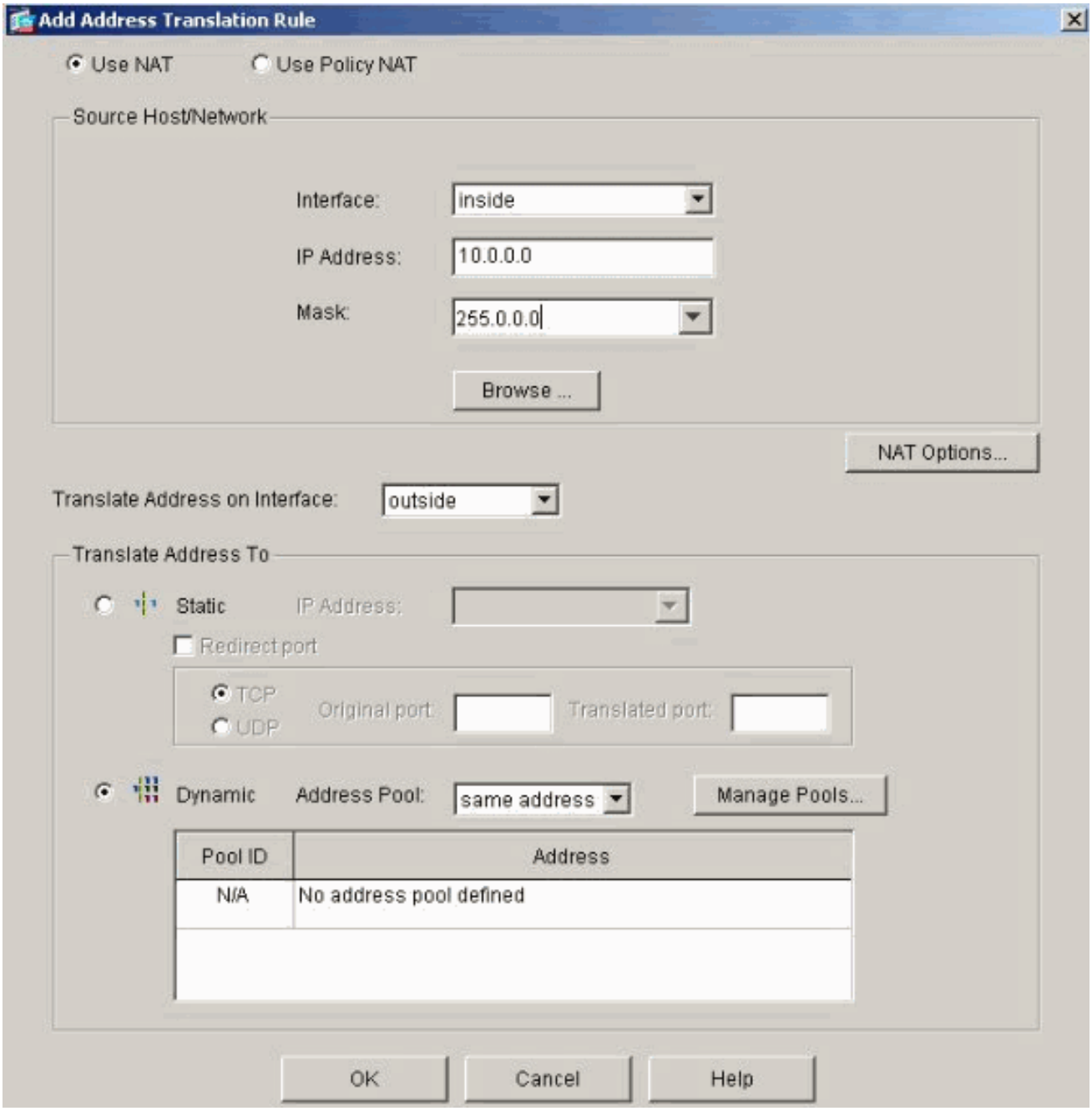
10. أختر **نهج الأمان** في علامة التبويب "الميزات" لمراجعة قاعدة نهج الأمان المستخدمة. في هذا المثال، يتم إستخدام القاعدة الداخلية
الافتراضية.



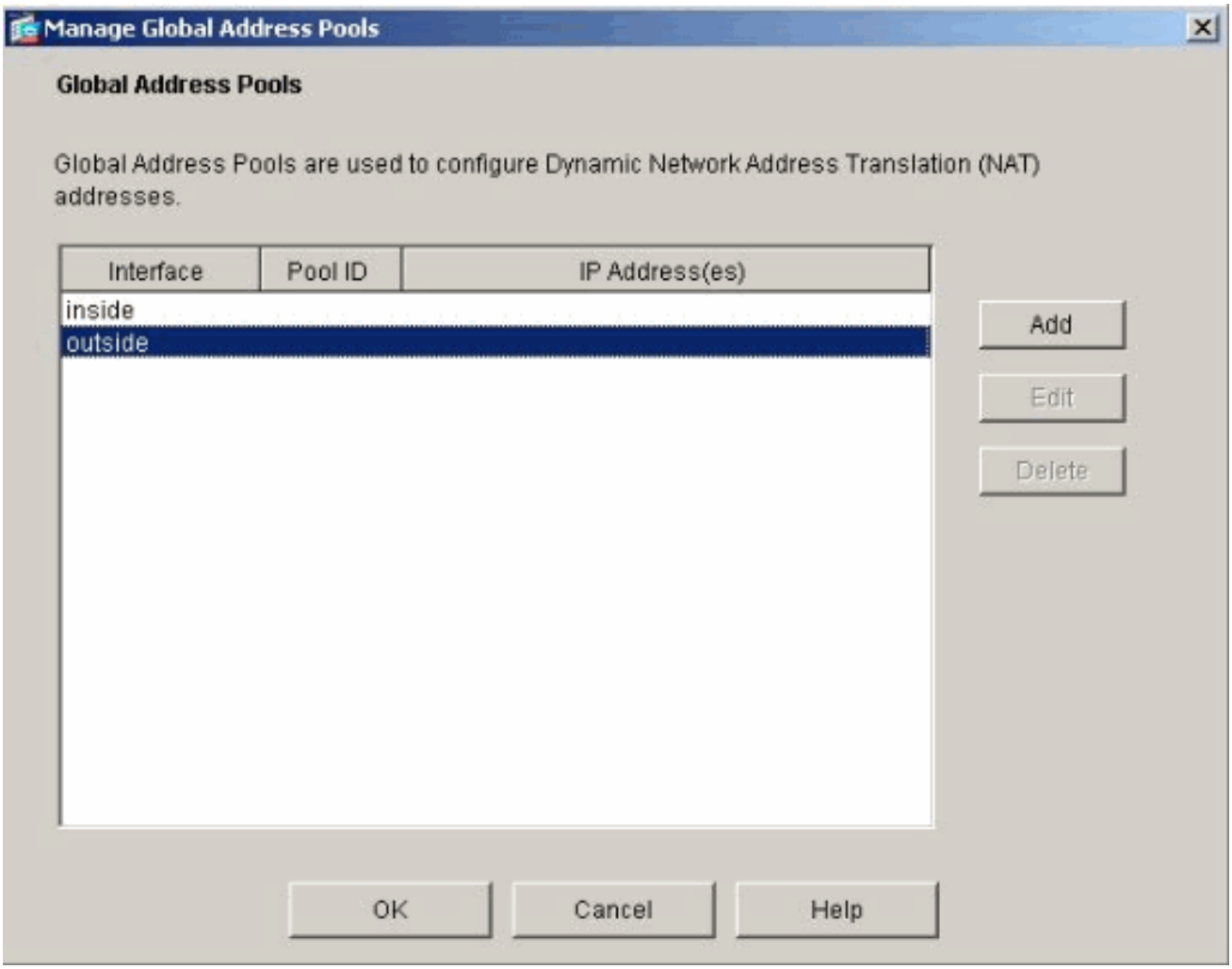
11. في هذا مثال، استعملت nat. قم بإلغاء تحديد خانة الاختيار **تمكين حركة مرور البيانات من خلال جدار الحماية بدون ترجمة العنوان** وانقر فوق **إضافة** لتكوين قاعدة NAT.



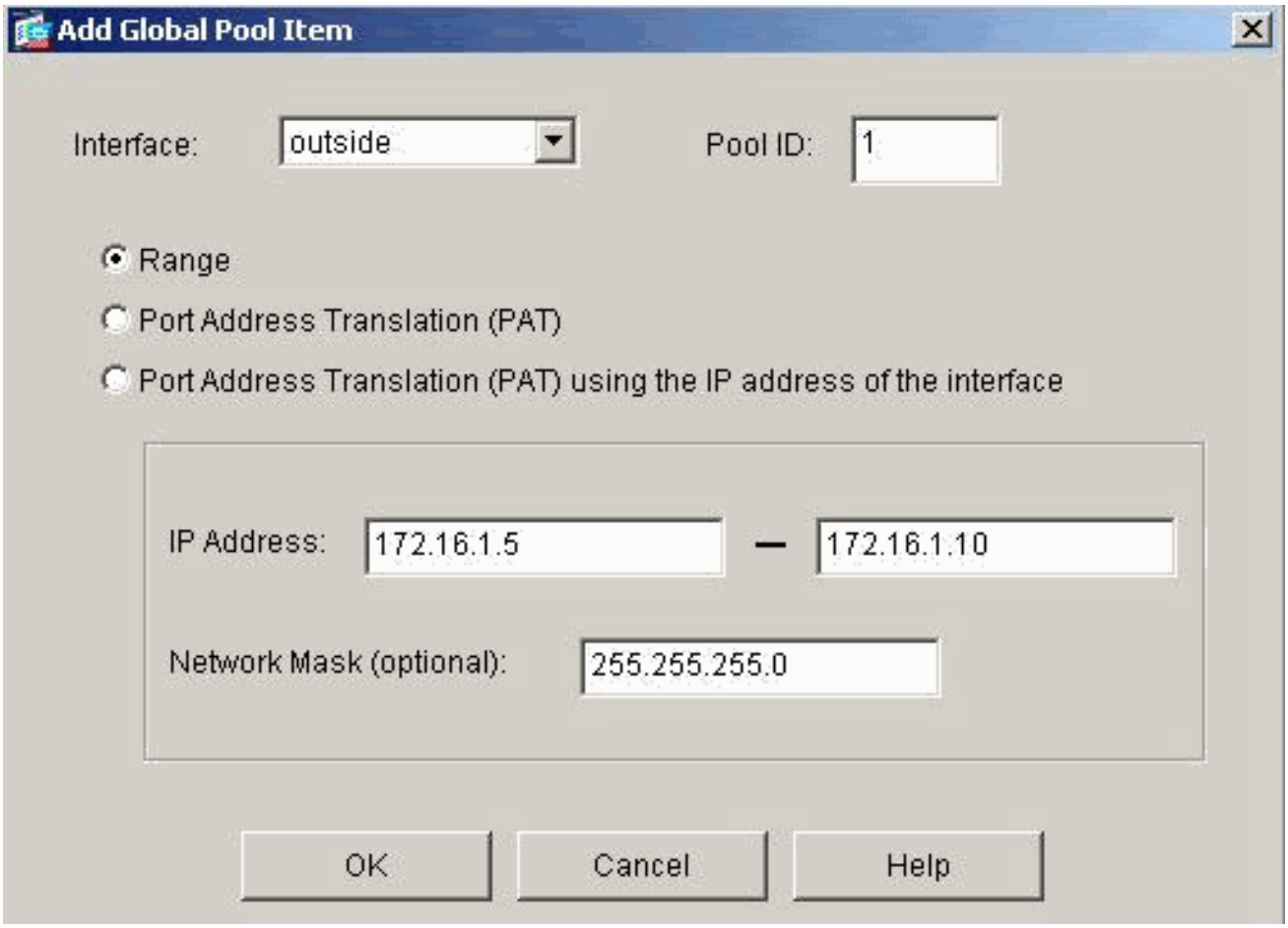
12. قم بتكوين الشبكة المصدر. في هذا المثال، يتم إستخدام 10.0.0.0 لعنوان IP، ويتم إستخدام 255.0.0.0 للقناع.طقطقة **يدير بركة** in order to عينت ال nat بركة عنوان.



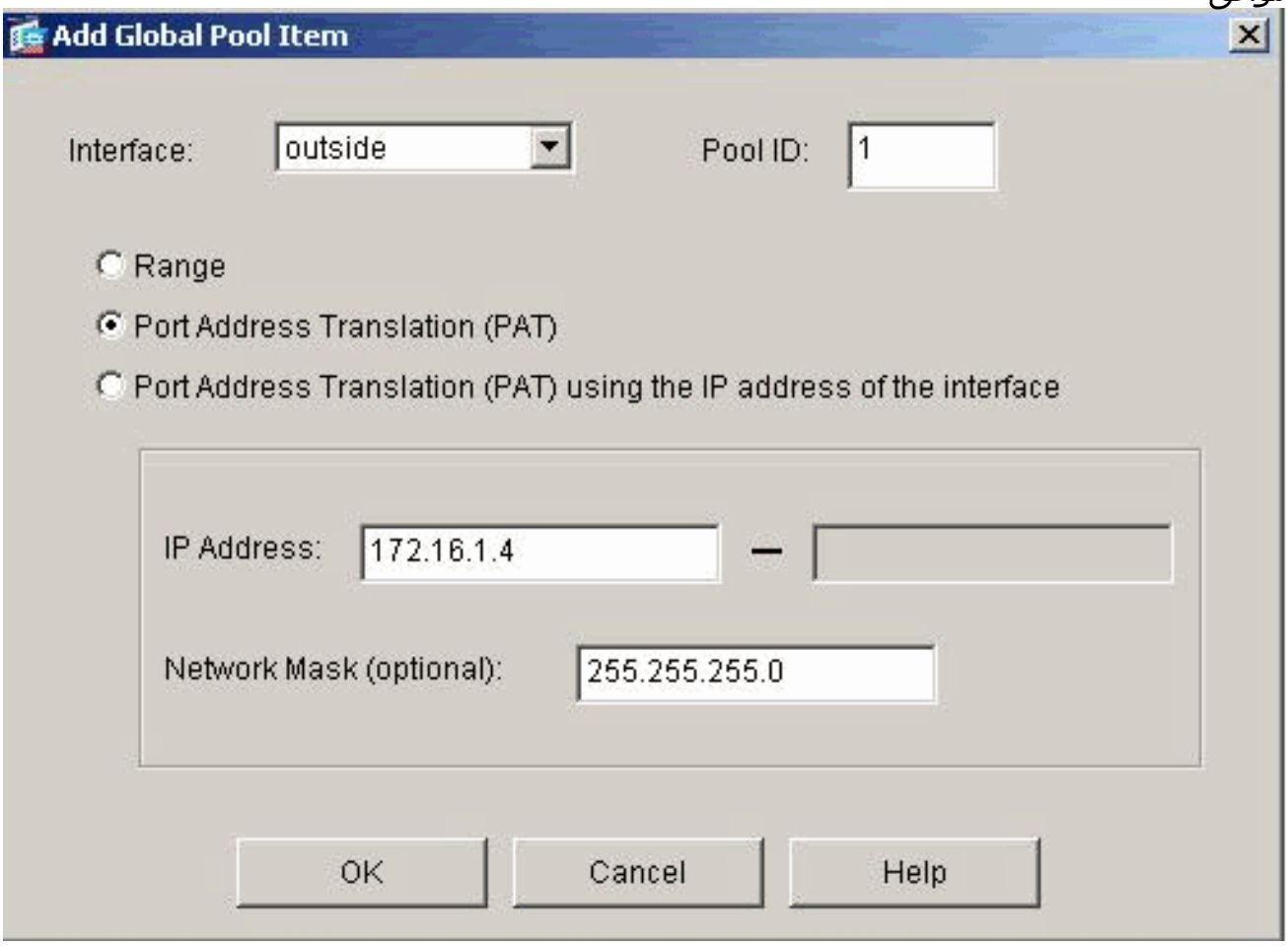
13. حدد الواجهة الخارجية وانقر **إضافة**.



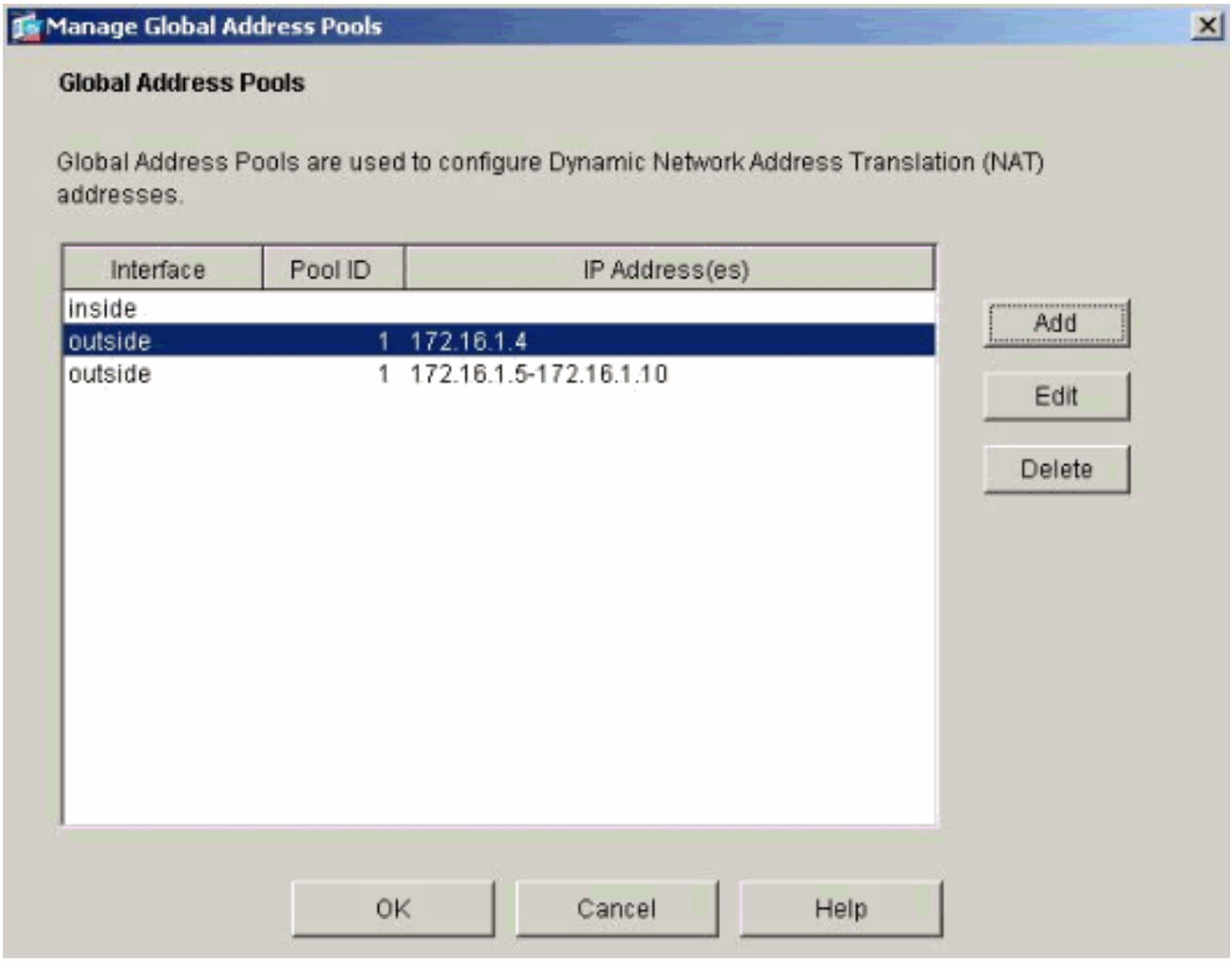
14. في هذا مثال، مدى و ضرب عنوان بركة شكلت. شكلت النطاق nat بركة عنوان وطقطقة **ok**.



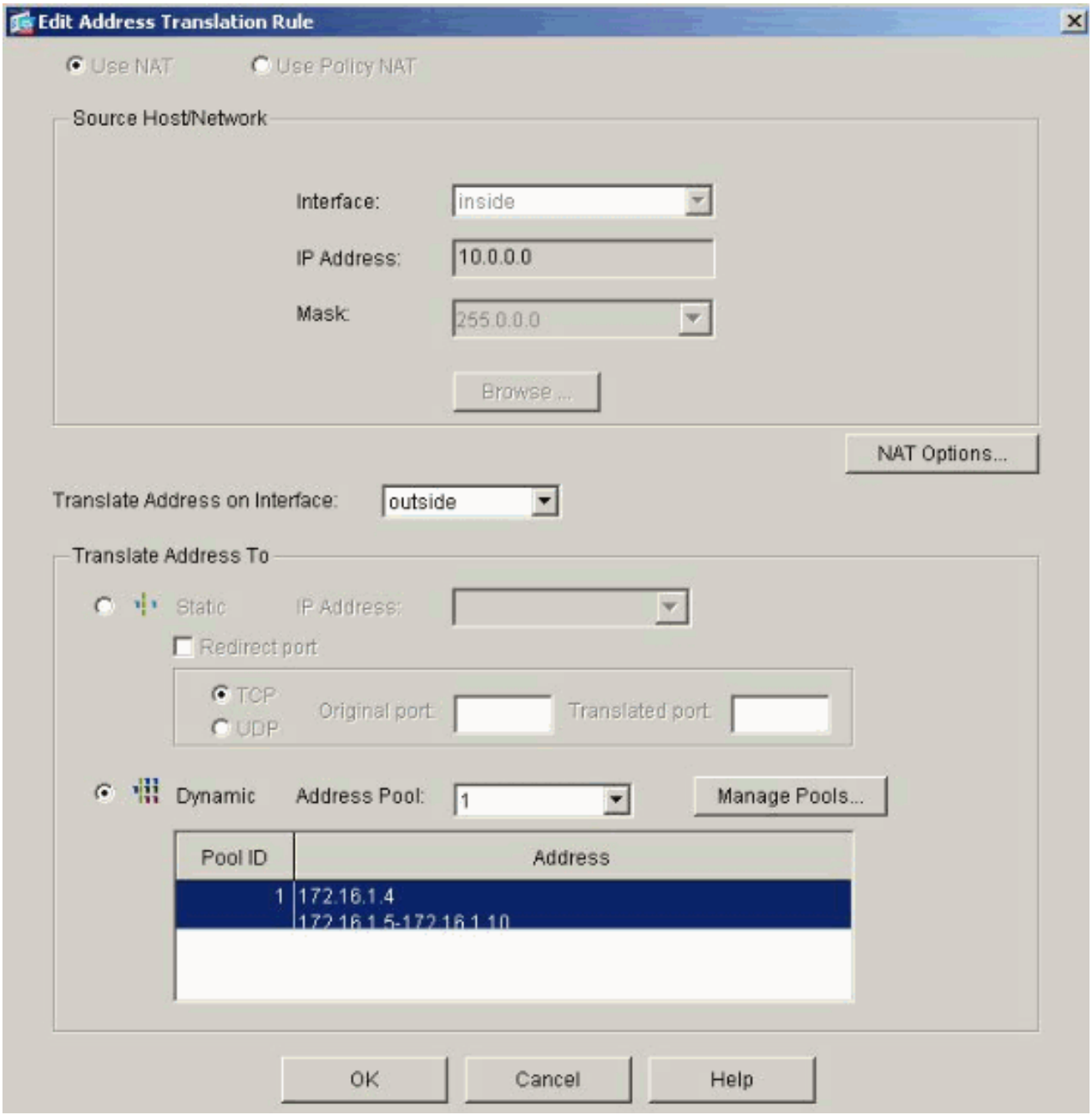
15. أخترت القارن خارجي في خطوة 13 in order to شكلت ال ضرب عنوان. ثم انقر فوق موافق



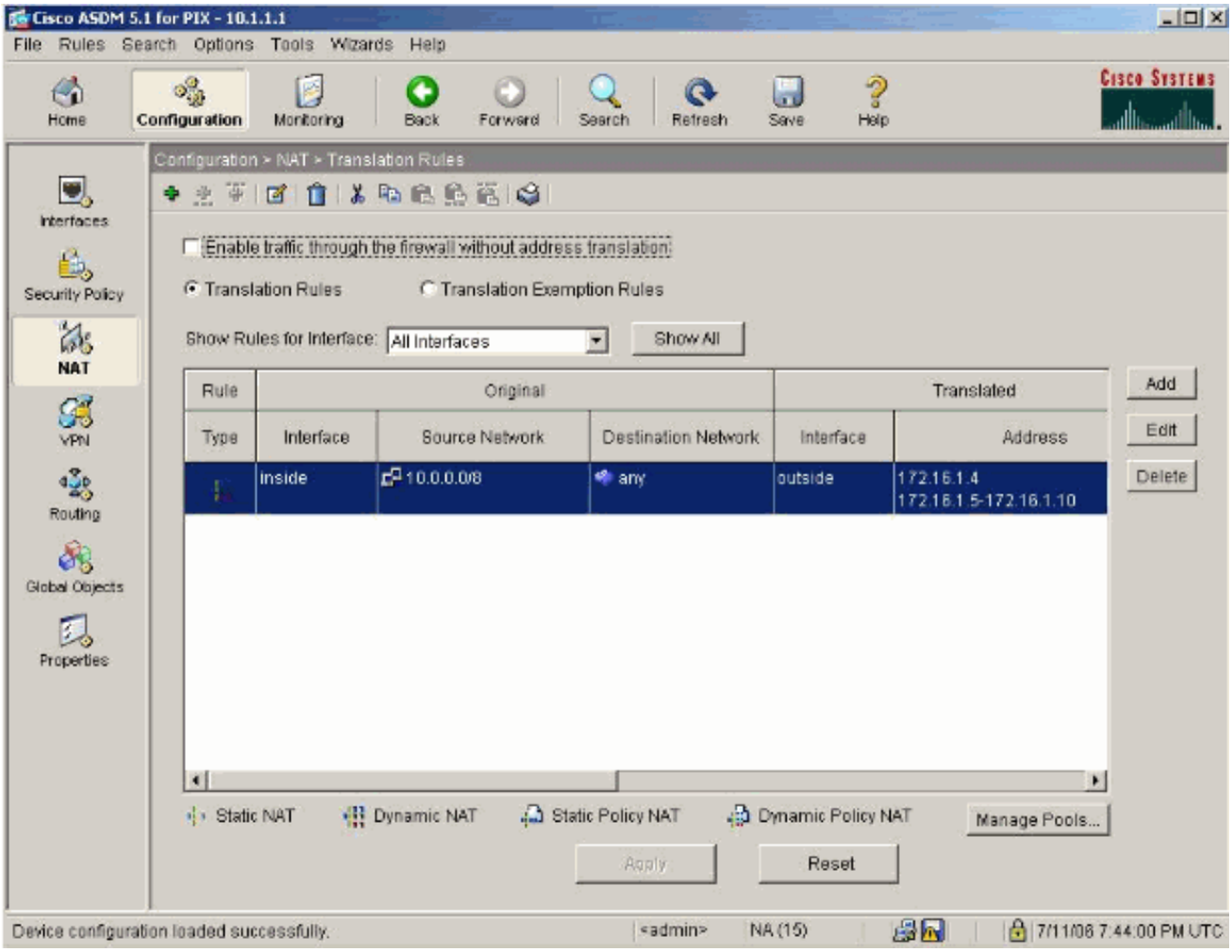
طقطقة in order to **ok**
تابعت.



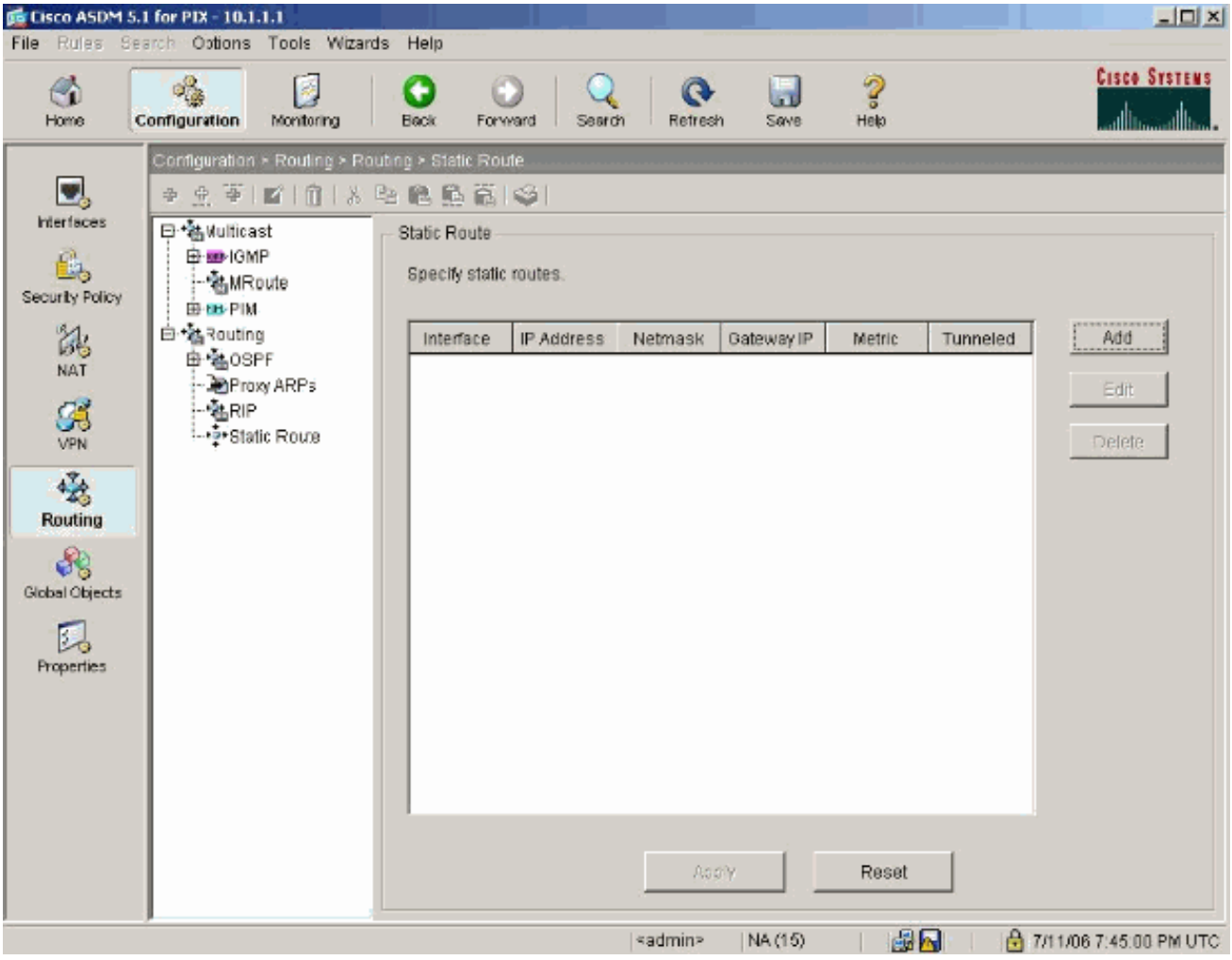
16. في نافذة "تحرير قاعدة ترجمة العنوان"، حدد معرف التجمع الذي سيتم إستخدامه بواسطة الشبكة المصدر التي تم تكوينها. وانقر فوق
.OK



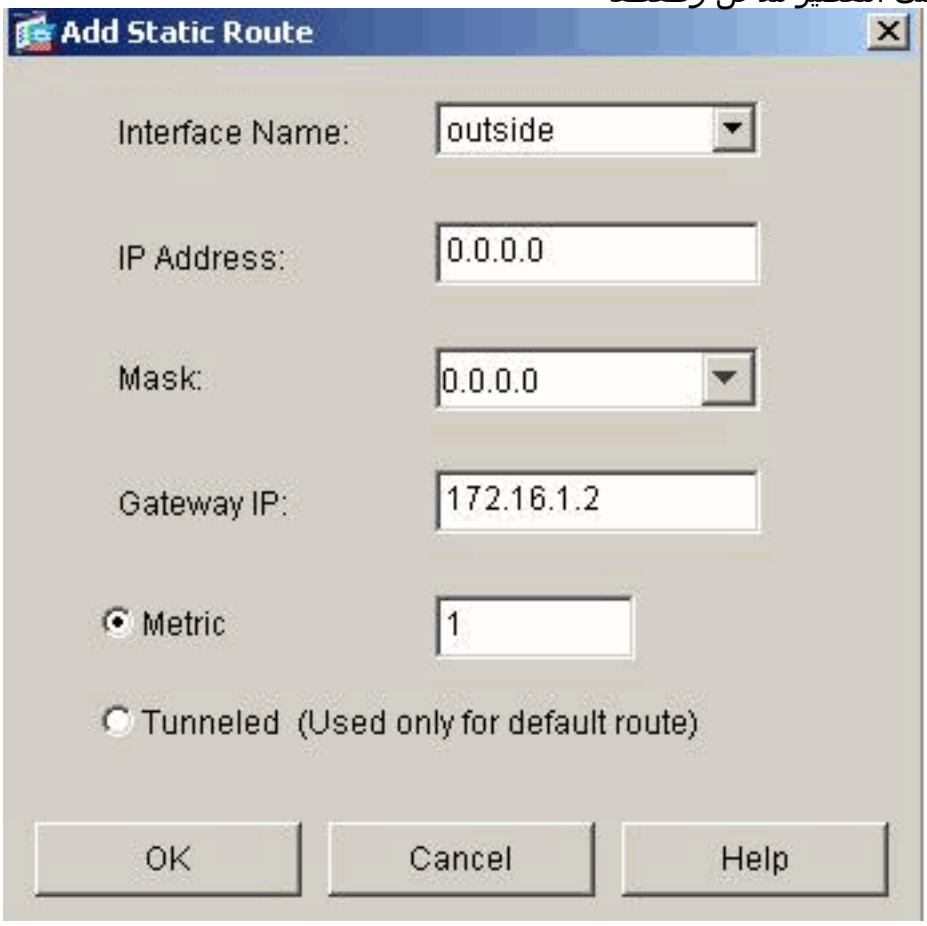
17. طقطقة **يطبق** in order to دفعت ال يشكل nat قاعدة إلى ال PIX.



18. في هذا المثال، يتم إستخدام المسارات الثابتة. طقطقة **يوجه**، يختار **ساكن إستاتيكي** ممر وطقطقة **يضيف**.

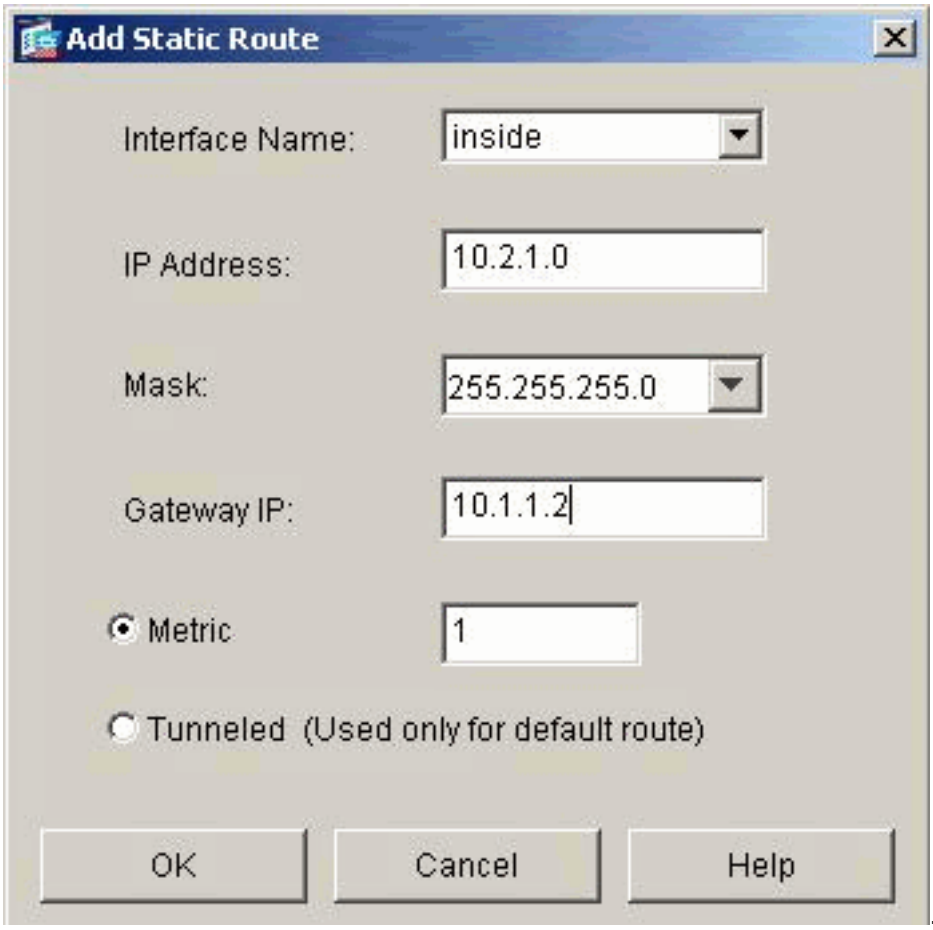


19. شكلت التقصير مدخل وطقطقة



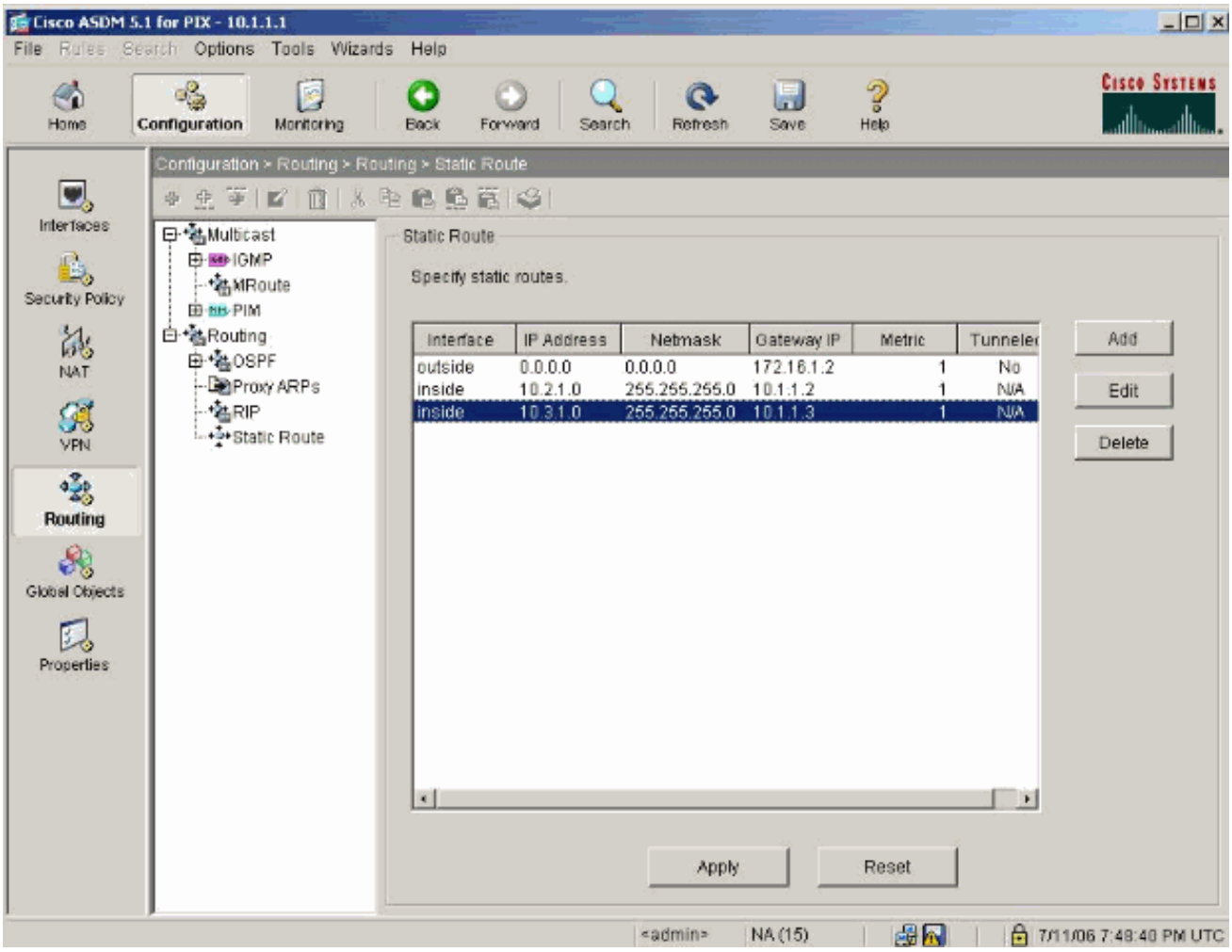
ok.

20. انقر على **إضافة** وأضف المسارات إلى الشبكات



الداخلية.

21. تأكد من تكوين المسارات الصحيحة وانقر فوق **تطبيق**.



تكوين PIX باستخدام CLI

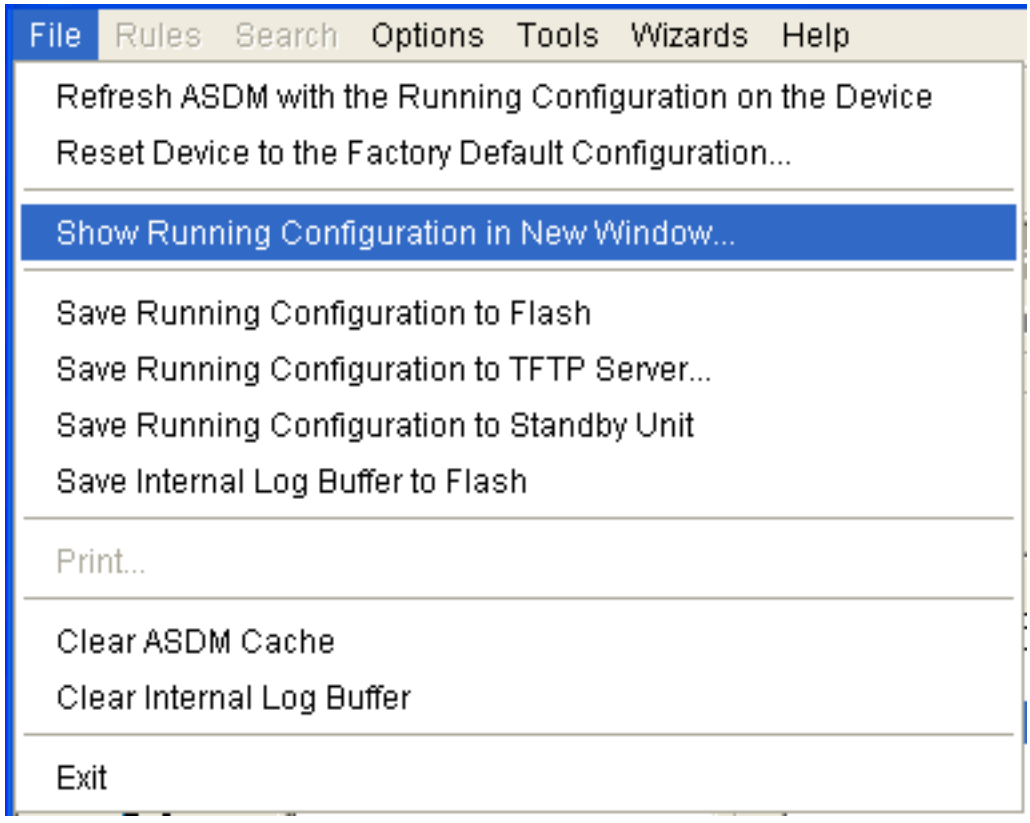
اكتمل الآن التكوين عبر واجهة المستخدم الرسومية (GUI) ل ASDM.

يمكنك رؤية هذا التكوين من خلال CLI (واجهة سطر الأوامر):

واجهة سطر الأوامر (CLI) الخاصة بجهاز أمان PIX
pixfirewall(config)#**write terminal** PIX Version 7.0(0)102 names ! **interface Ethernet0** **nameif outside** **security-level 0** **ip address 172.16.1.1 255.255.255.0** ! **interface Ethernet1** **nameif inside** **security-level 100** **ip address 10.1.1.1 255.255.255.0** *Assign name and IP address to the interfaces* enable *---!* password 2KFQnbNIdI.2KYOU encrypted passwd 2KFQnbNIdI.2KYOU encrypted asdm image flash:/asdmfile.50073 no asdm history enable arp timeout 14400 **nat-control** *Enforce a strict NAT for all the traffic through ---!* *the Security appliance* **global (outside) 1 172.16.1.5-**

```
                                    172.16.1.10 netmask 255.255.255.0
    Define a pool of global addresses 172.16.1.5 to ---!
172.16.1.10 with !--- NAT ID 1 to be used for NAT global
                    (outside) 1 172.16.1.4 netmask 255.255.255.0
Define a single IP address 172.16.1.4 with NAT ID 1 ---!
    to be used for PAT nat (inside) 1 10.0.0.0 255.0.0.0
 Define the inside networks with same NAT ID 1 used ---!
     in the global command for NAT route inside 10.3.1.0
                                    255.255.255.0 10.1.1.3 1
          route inside 10.2.1.0 255.255.255.0 10.1.1.2 1
    Configure static routes for routing the packets ---!
      towards the internal network route outside 0.0.0.0
                                    0.0.0.0 172.16.1.2 1
     Configure static route for routing the packets ---!
towards the Internet (or External network) timeout xlate
    3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
   0:02:00 icmp 0:00:02 sunrpc 0:10:00 h323 0:05:00 h225
       1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00
   sip_media 0:02:00 timeout uauth 0:05:00 absolute http
                                    server enable
 Enable the HTTP server on PIX for ASDM access http ---!
                                    10.1.1.5 255.255.255.255 inside
 Enable HTTP access from host 10.1.1.5 to configure ---!
       PIX using ASDM (GUI) ! !--- Output suppressed ! !
  Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5 : end
```

أخترت **مبرد>عرض تشكيل جار في نافذة جديد** in order to شاهدت ال CLI تشكيل في ASDM.



التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

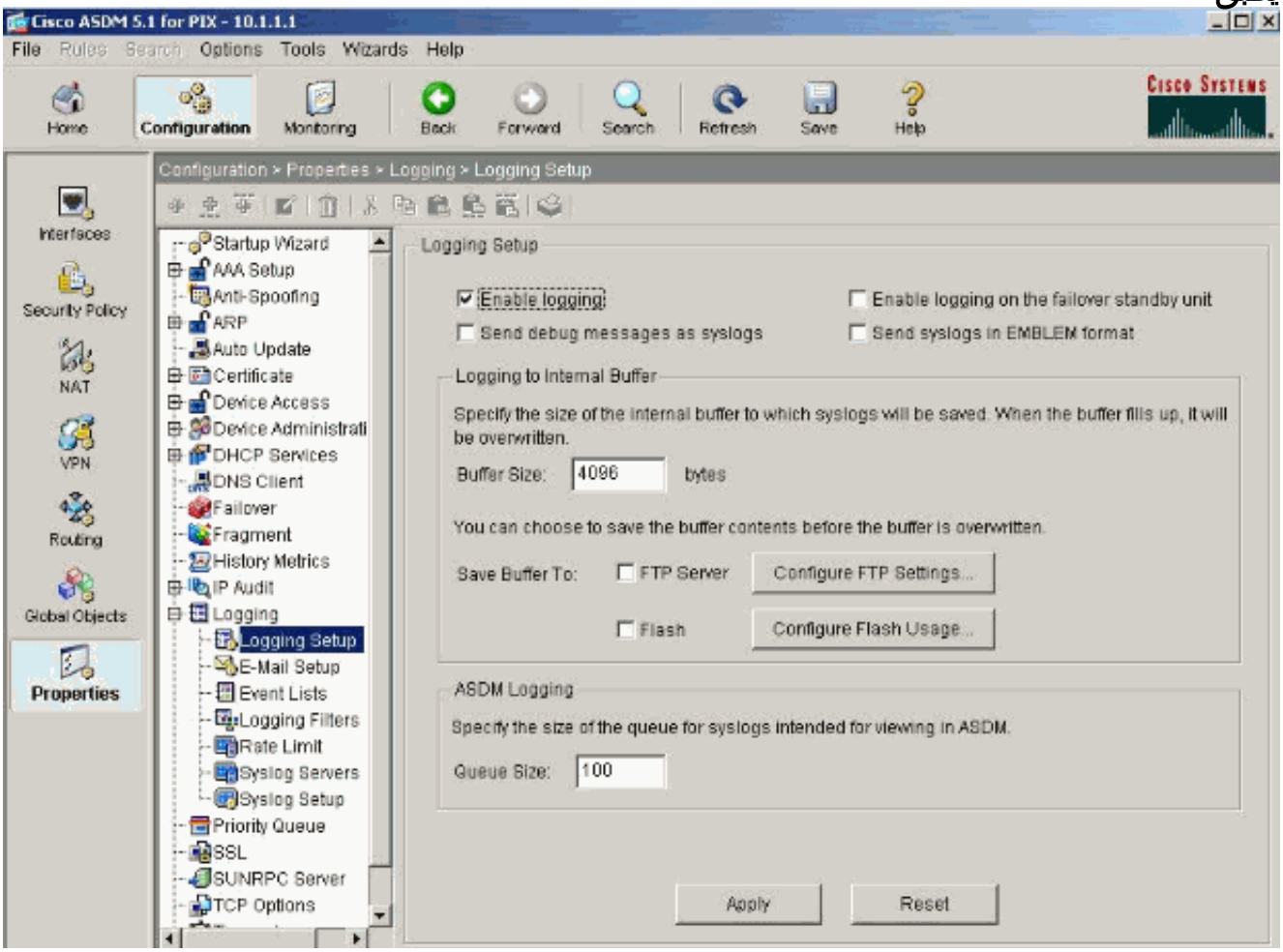
ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- **debug icmp trace**— يعرض ما إذا كانت طلبات ICMP من الأجهزة المضيفة تصل إلى PIX. لتشغيل تصحيح الأخطاء هذا، يلزمك إضافة أمر **access-list** للسماح ب ICMP في التكوين الخاص بك.
- **تصحيح أخطاء مخزن التسجيل المؤقت**— يعرض الاتصالات التي تم إنشاؤها ورفض إرسالها إلى الأجهزة المضيفة التي تمر عبر PIX. يتم تخزين المعلومات في المخزن المؤقت لسجل PIX ويمكنك رؤية الإخراج باستخدام الأمر **show log**.

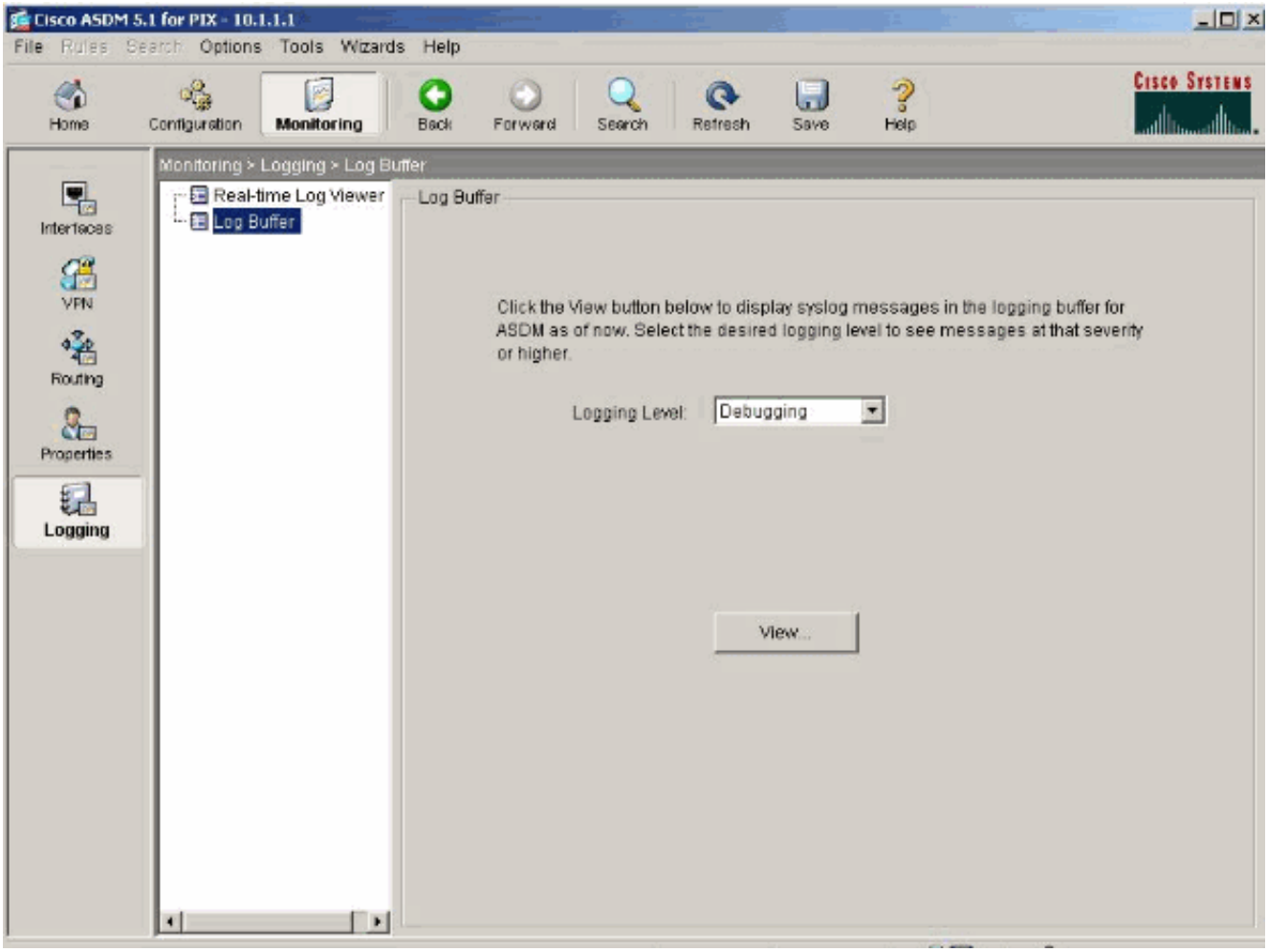
إجراء استكشاف الأخطاء وإصلاحها

يمكن إستخدام ASDM لتمكين التسجيل، وأيضا لعرض السجلات:

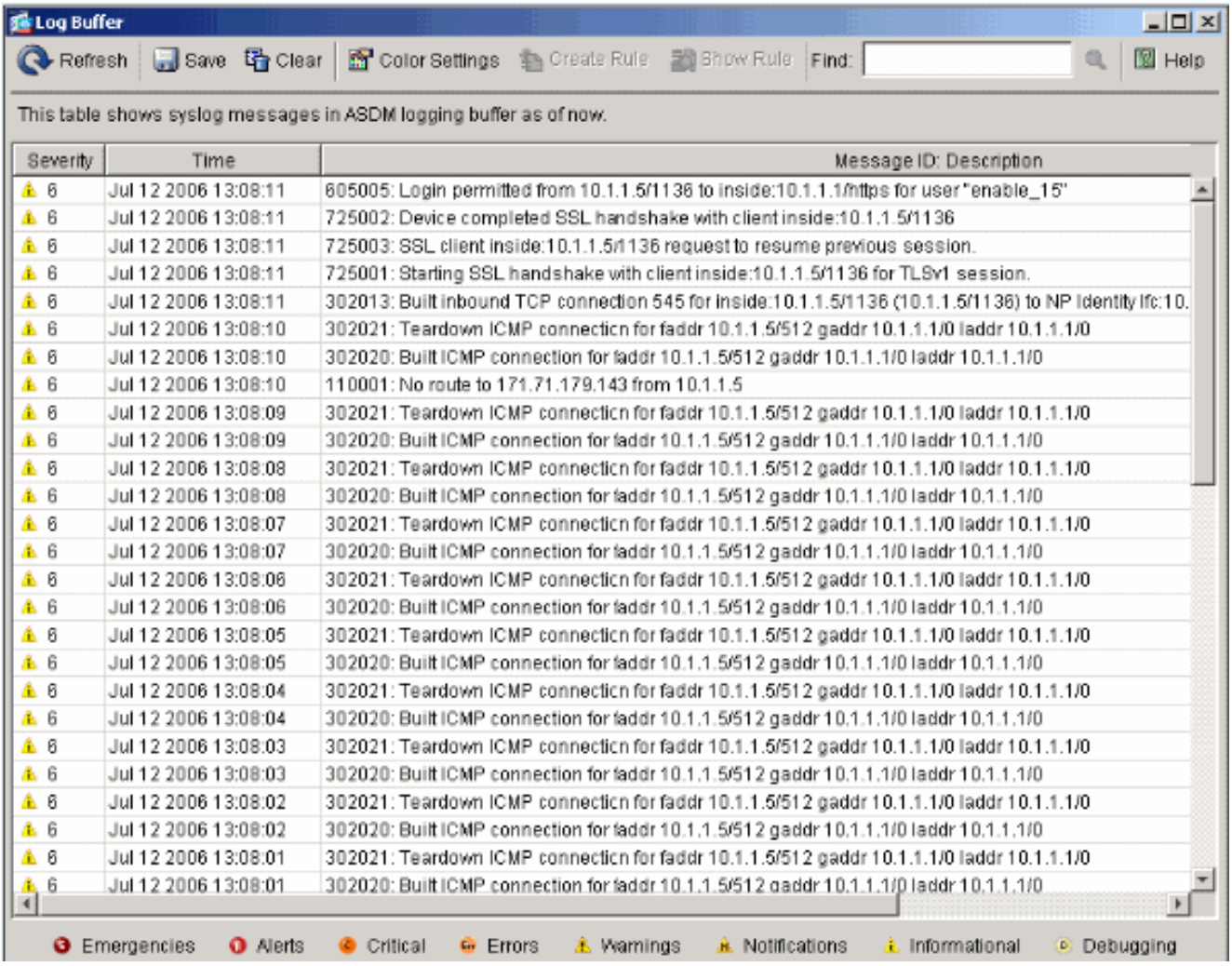
1. أخترت **تشكيل > خصائص > تسجيل > تسجيل إعداد**، **يمكن تسجيل**، وطقطقة **يطبق**.



2. أختر **المراقبة > التسجيل > المخزن المؤقت للسجل > مستوى التسجيل** واختر **المخزن المؤقت للتسجيل** من القائمة المنسدلة. انقر فوق **عرض**.



3. هنا مثال من السجل مخزن مؤقت:



تعذر الوصول إلى مواقع الويب بالاسم

في بعض السيناريوهات، لا يمكن للشبكات الداخلية الوصول إلى مواقع الإنترنت باستخدام الاسم (يعمل مع عنوان IP في مستعرض الويب. هذا إصدار شائع وعادة ما يحدث إذا لم يتم تعريف خادم DNS، وخاصة في الحالات التي يكون PIX/ASA فيها هو خادم DHCP. كما يمكن أن يحدث ذلك في الحالات التي يتعذر فيها على PIX/ASA دفع خادم DNS أو إذا لم يكن خادم DNS قابلا للوصول إليه.

معلومات ذات صلة

- أجهزة الأمان Cisco PIX 500 Series Security Appliances
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- مدير أجهزة حلول الأمان المعدلة من Cisco
- أستكشاف أخطاء مدير أجهزة حلول الأمان المعدلة (ASDM) وإصلاحها والتنبيهات من Cisco
- 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).