PIX/ASA (الإصدار 7.x والإصدارات الأحدث) نفق IPsec VPN مع مثال تكوين ترجمة عنوان الشبكة

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
المنتجات ذات الصلة
التكوين
الرسم التخطيطي للشبكة
التكوينات
تكوين جهاز أمان PIX وقائمة الوصول
تكوين جهاز أمان PIX و MPF (إطار عمل السياسات النمطي)
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
أوامر أستكشاف الأخطاء وإصلاحها ل IPsec للموجه
التخلص من الرابطات الأمنية
أوامر أستكشاف الأخطاء وإصلاحها ل PIX
معلومات ذات صلة

المقدمة

يوضح هذا التكوين العينة نفق VPN ل IPsec من خلال جدار حماية يقوم بتنفيذ ترجمة عنوان الشبكة (NAT). **لا يعمل هذا التكوين مع ترجمة عنوان المنفذ (PAT) إذا كنت تستخدم إصدارات برنامج Cisco IOS® التي تسبق الإصدار ولا تتضمن 12.2(13)T.** يمكن إستخدام هذا النوع من التكوين لنقل بيانات IP عبر النفق. لا يمكن إستخدام هذا التكوين لتشفير حركة المرور التي لا تمر عبر جدار حماية، مثل تحديثات التوجيه أو IPX. يعد الاتصال النفقي للتوجيه العام (GRE) خيارا أكثر ملاءمة. في هذا المثال، تعد موجهات Cisco 2621 و 3660 نقاط النهاية لنفق IPsec التي تنضم إلى شبكتين خاصتين، مع قنوات أو قوائم التحكم في الوصول (ACLs) على PIX فيما بينها للسماح بحركة مرور IPsec.

ملاحظة: NAT هي ترجمة العنوان من فرد إلى آخر، ولا ينبغي الخلط بينها وبين PAT، وهي ترجمة عديدة (داخل جدار الحماية) إلى واحد. أحلت ل كثير معلومة على عملية NAT وتكوينه، بتحرى nat عملية و أساسي nat بتحرى أو كيف يعمل NAT.

ملاحظة: قد لا يعمل IPsec مع PAT بشكل صحيح لأن جهاز نقطة نهاية النفق الخارجي لا يمكنه معالجة أنفاق متعددة من عنوان IP واحد. اتصل بموردك لتحديد ما إذا كانت أجهزة نقطة نهاية النفق تعمل مع PAT أم لا. in cisco ios برمجية إطلاق 12.2(13)T وفيما بعد، ال nat شفافية سمة يستطيع كنت استعملت ل ضرب. لمزيد من التفاصيل، ارجع إلى شفافية IPSec NAT. راجع دعم IPSec ESP من خلال NAT لمعرفة المزيد حول هذه الميزات في

برنامج Cisco IOS الإصدار 12.2(13)T والإصدارات الأحدث.

ملاحظة: قبل فتح حالة باستخدام دعم Cisco الفني، ارجع إلى الأسئلة المتكررة NAT، والتي تحتوي على العديد من الإجابات على الأسئلة الشائعة.

راجع تكوين نفق IPSec من خلال جدار حماية باستخدام NAT للحصول على مزيد من المعلومات حول كيفية تكوين نفق IPsec من خلال جدار الحماية باستخدام NAT على الإصدار x.6 من PIX والإصدارات الأقدم.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج IOS الإصدار T.12.0.7 من Cisco (حتى لا يتضمن برنامج Cisco IOS الإصدار 12.2(13)T)للحصول على إصدارات أحدث، ارجع إلى شفافية IPSec nat.
- موجّه Cisco 2621
- موجّه Cisco 3660
- جهاز الأمان Cisco PIX 500 Series Security Appliance الذي يشغل الإصدار x.7 والإصدارات الأحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة 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.

المنتجات ذات الصلة

كما يمكن إستخدام هذا المستند مع جهاز الأمان القابل للتكيف (ASA) من السلسلة Cisco 5500 مع إصدار البرنامج x.7 والإصدارات الأحدث.

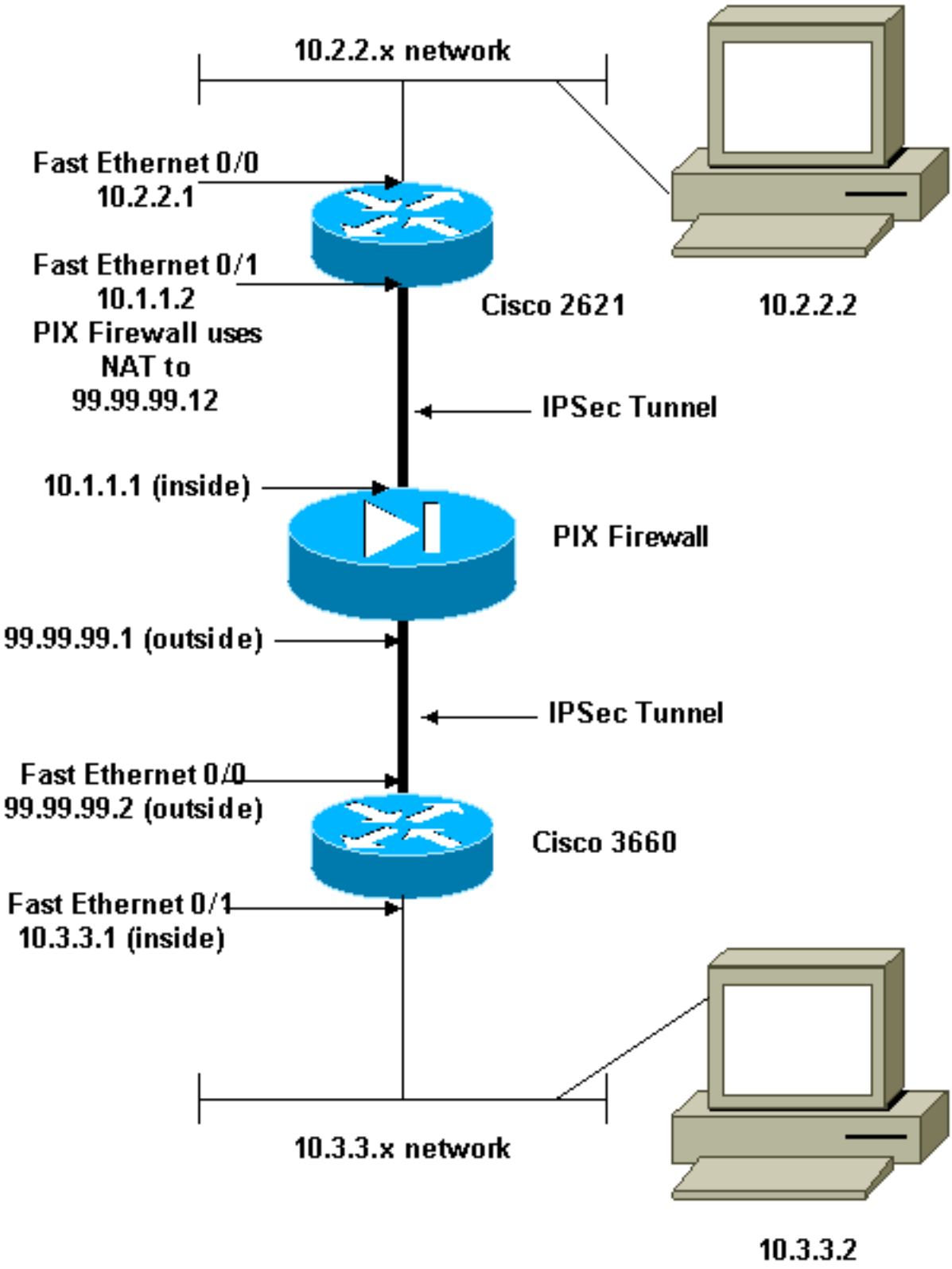
التكوين

يقدم لك هذا القسم المعلومات التي يمكنك إستخدامها لتكوين الميزات التي يصفها هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر التي يستخدمها هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- تكوين Cisco 2621
- تكوين Cisco 3660
- تكوين جهاز أمان PIX وقائمة الوصولتكوين واجهة المستخدم الرسومية (ASDM) لبرنامج Advanced Security Managerتكوين واجهة سطر الأوامر (CLI)
- تكوين جهاز أمان PIX و MPF (إطار عمل السياسات النمطي)

Cisco 2621

```
:Current configuration
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-2621
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
isdn voice-call-failure 0
cns event-service server
!
The IKE policy. crypto isakmp policy 10 ---!
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 99.99.99.2
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/1

IPsec policy.  crypto map mymap 10 ipsec-isakmp ---!
 set peer 99.99.99.2
 set transform-set myset

Include the private-network-to-private-network ---!
traffic !--- in the encryption process. match address
101
!
controller T1 1/0
!
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto

Apply to the interface. crypto map mymap ---!
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
no ip http server

Include the private-network-to-private-network ---!
traffic !--- in the encryption process. access-list 101
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
line con 0
 transport input none
line aux 0
line vty 0 4
!
```

```
no scheduler allocate
end
```

Cisco 3660

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-3660
!
ip subnet-zero
!
cns event-service server
!

The IKE policy. crypto isakmp policy 10 ---!
hash md5
authentication pre-share
crypto isakmp key cisco123 address 99.99.99.12
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/0

The IPsec policy. crypto map mymap 10 ipsec-isakmp ---!
set peer 99.99.99.12
set transform-set myset

Include the private-network-to-private-network ---!
traffic !--- in the encryption process.  match address
101
!
interface FastEthernet0/0
ip address 99.99.99.2 255.255.255.0
no ip directed-broadcast
ip nat outside
duplex auto
speed auto

Apply to the interface. crypto map mymap ---!
!
interface FastEthernet0/1
ip address 10.3.3.1 255.255.255.0
no ip directed-broadcast
ip nat inside
duplex auto
speed auto
!
interface Ethernet3/0
no ip address
no ip directed-broadcast
shutdown
!
interface Serial3/0
no ip address
no ip directed-broadcast
no ip mroute-cache
shutdown
!
interface Ethernet3/1
no ip address
```

```
                                no ip directed-broadcast
                                    interface Ethernet4/0
                                           no ip address
                                no ip directed-broadcast
                                             shutdown
                                                   !
                                   interface TokenRing4/0
                                           no ip address
                                no ip directed-broadcast
                                             shutdown
                                           ring-speed 16
                                                   !

The pool from which inside hosts translate to !--- ---!
  the globally unique 99.99.99.0/24 network. ip nat pool
   OUTSIDE 99.99.99.70 99.99.99.80 netmask 255.255.255.0

Except the private network from the NAT process. ip ---!
          nat inside source route-map nonat pool OUTSIDE
                                           ip classless
                        ip route 0.0.0.0 0.0.0.0 99.99.99.1
                                        no ip http server
                                                   !

    Include the private-network-to-private-network ---!
 traffic !--- in the encryption process. access-list 101
        permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
      access-list 101 deny   ip 10.3.3.0 0.0.0.255 any

   Except the private network from the NAT process. ---!
   access-list 110 deny   ip 10.3.3.0 0.0.0.255 10.2.2.0
                                                0.0.0.255
      access-list 110 permit ip 10.3.3.0 0.0.0.255 any
                                 route-map nonat permit 10
                                     match ip address 110
                                                   !
                                          line con 0
                                    transport input none
                                          line aux 0
                                        line vty 0 4
                                                   !
                                                 end
```

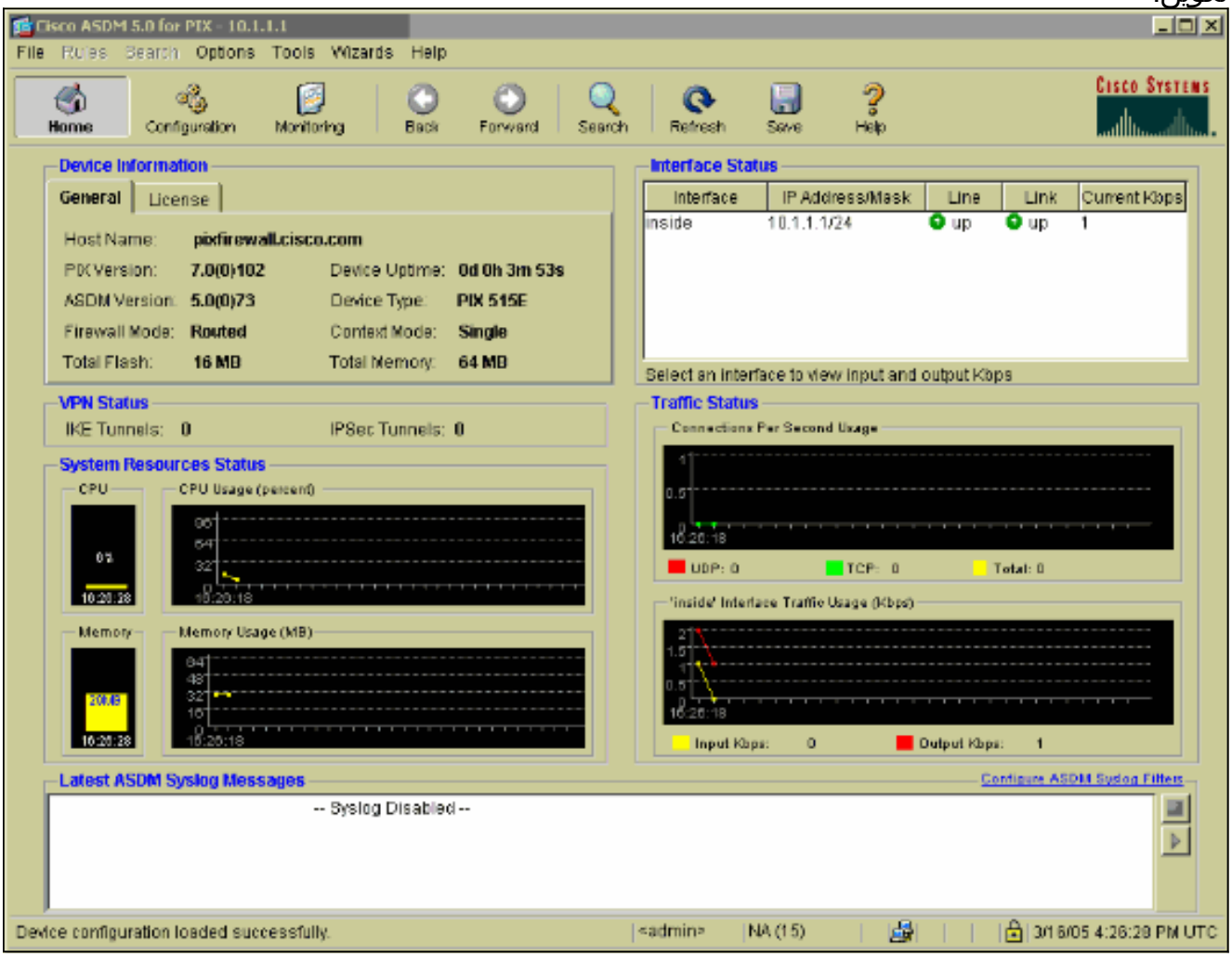
تكوين جهاز أمان PIX وقائمة الوصول

تكوين ASDM 5.0

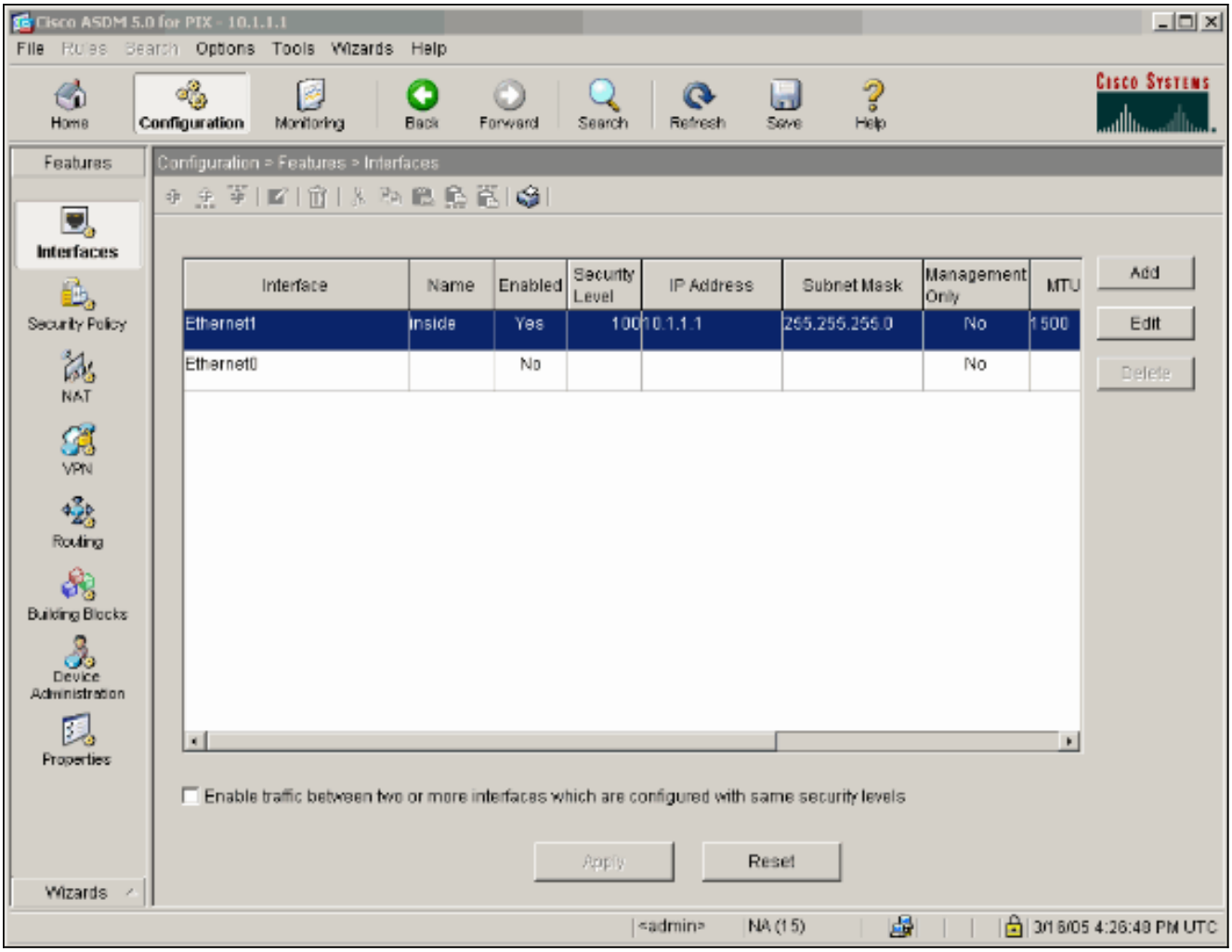
أكمل هذه الخطوات لتكوين جدار حماية PIX الإصدار 7.0 باستخدام ASDM.

1. وحدة تحكم في PIX. من تكوين ممسوح، أستخدم موجهات الأوامر التفاعلية لتمكين **واجهة المستخدم الرسومية (GUI) لمدير الأمان المتقدم (ASDM)** لإدارة PIX من محطة العمل 10.1.1.3.
2. من محطة العمل 10.1.1.3، افتح مستعرض ويب واستخدم ADSM (في هذا المثال، https://10.1.1.1).
3. أختر **نعم** على مطالبات الشهادة والدخول باستخدام كلمة مرور enable كما تم تكوينها في تكوين واجهة سطر أوامر ASDM لجدار حماية PIX.
4. إذا كانت هذه هي المرة الأولى التي يتم فيها تشغيل ASDM على الكمبيوتر الشخصي، فإنها تطالبك ما إذا كنت تستخدم مشغل ASDM، أو تستخدم ASDM كتطبيق Java.في هذا المثال، يتم تحديد مشغل ASDM وتثبيت هذه المطالبات.
5. انتقل إلى نافذة ASDM Home وحدد علامة التبويب

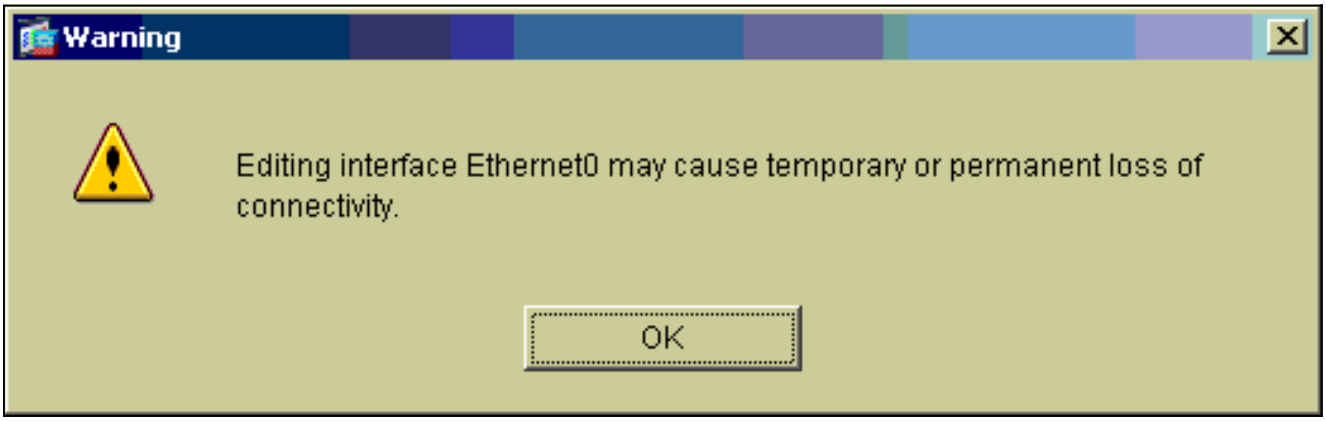
تكوين.



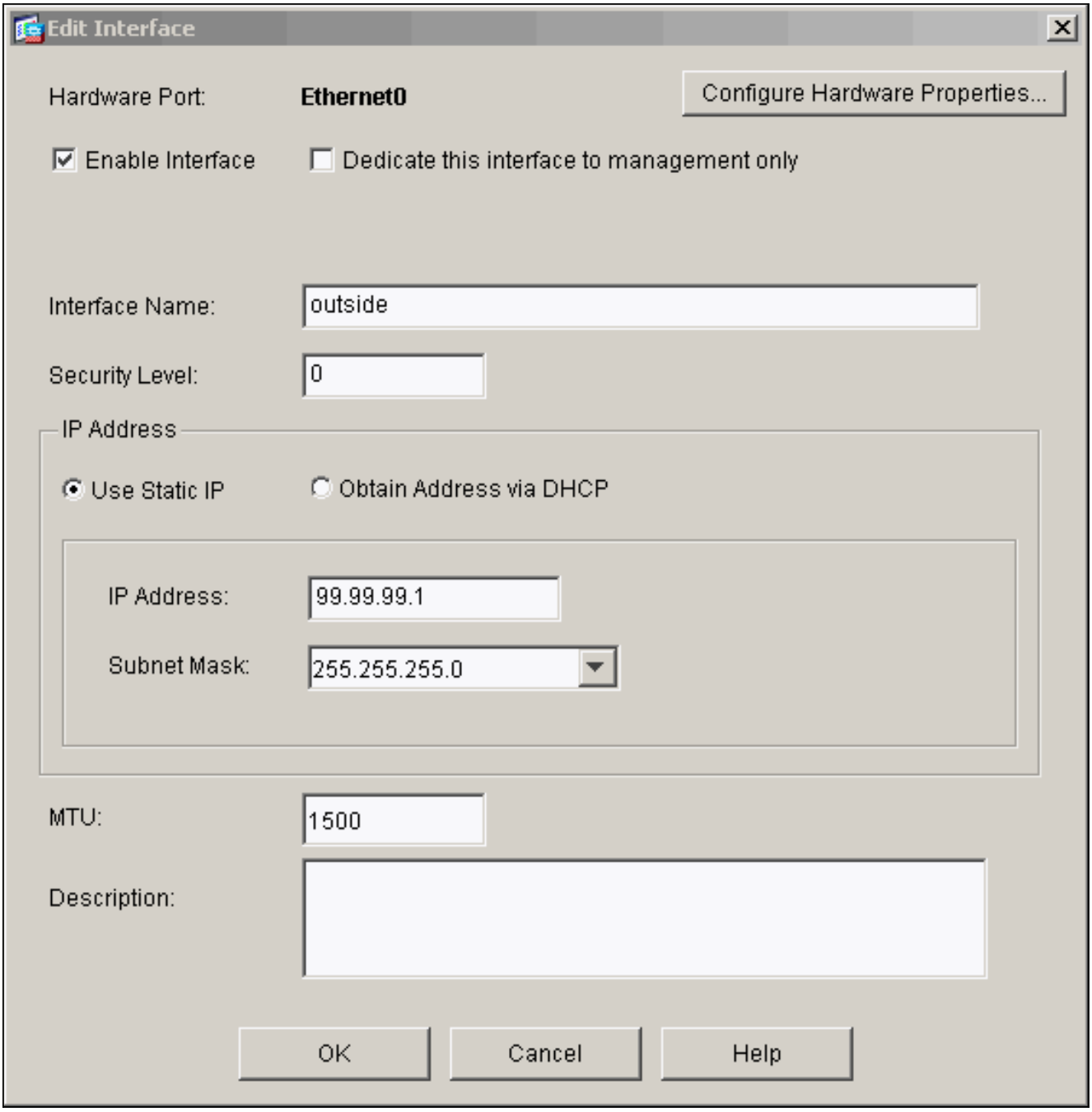
6. ركزت **الإثرنيت 0 قارن** وطقطقة **حررت** in order to شكلت القارن خارجي.



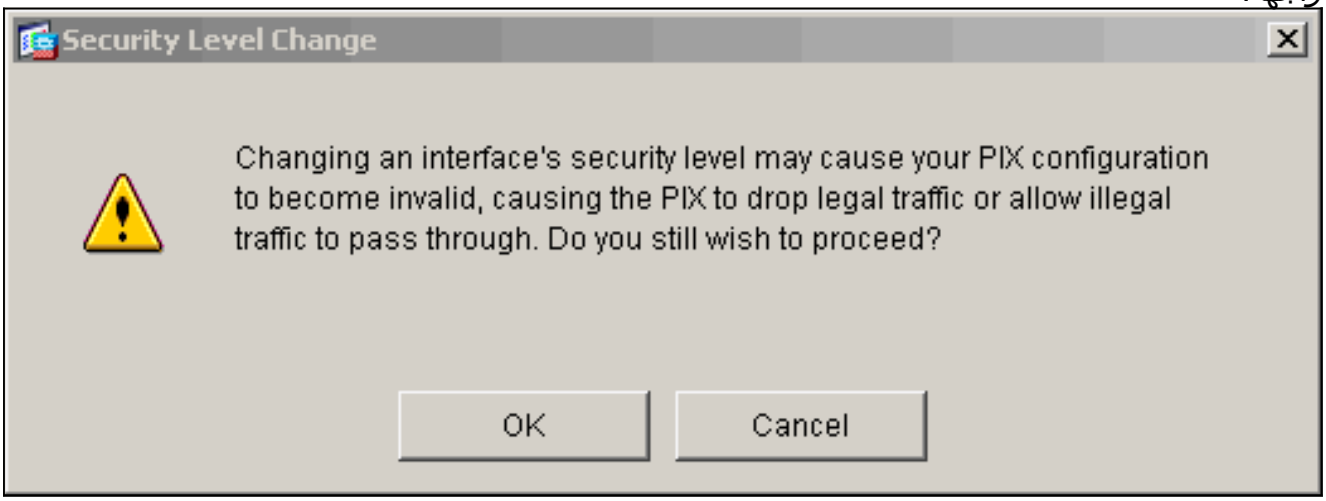
7. طقطقة **ok** في ال edit قارن رسالة
حث.



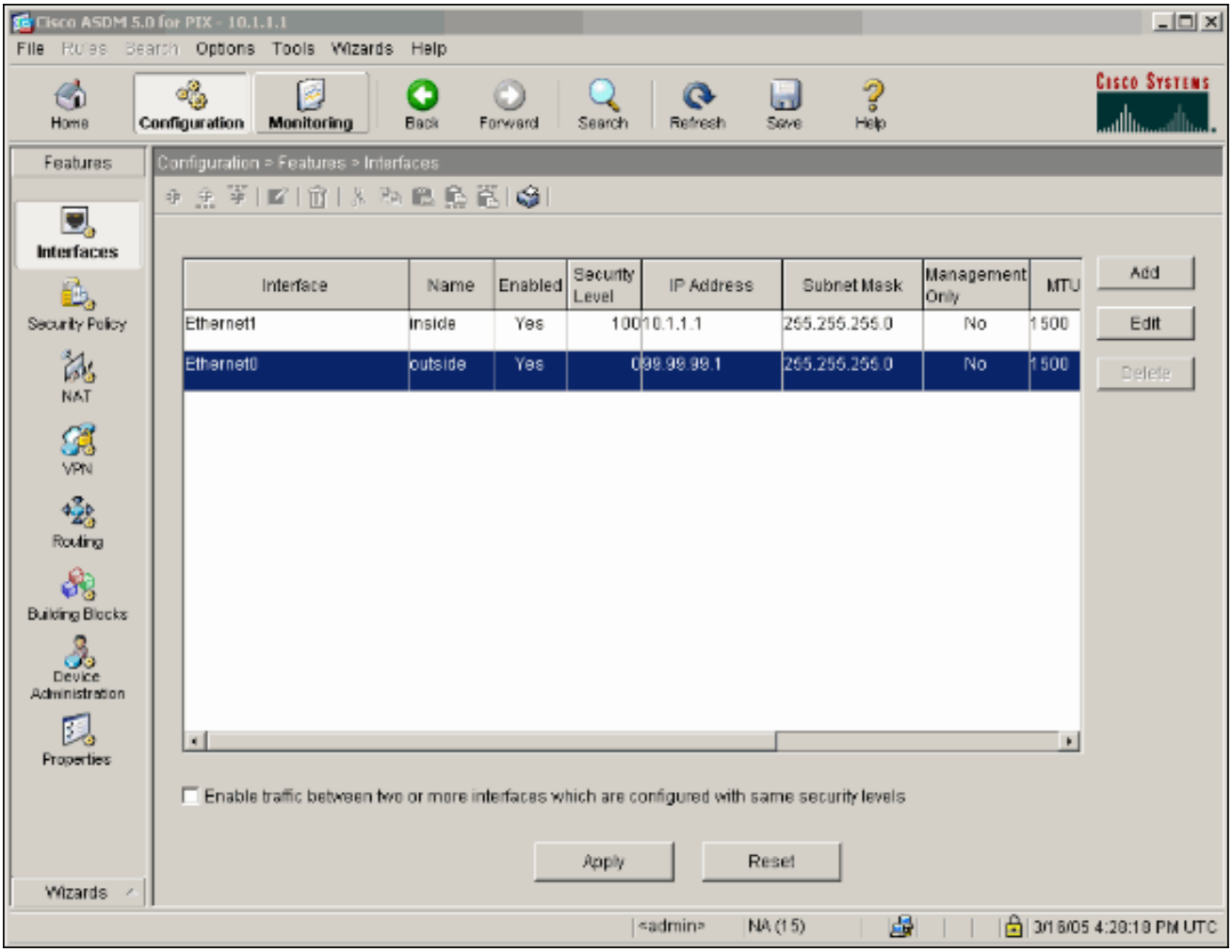
8. أدخل تفاصيل الواجهة وانقر فوق **موافق** عند
انتهائك.



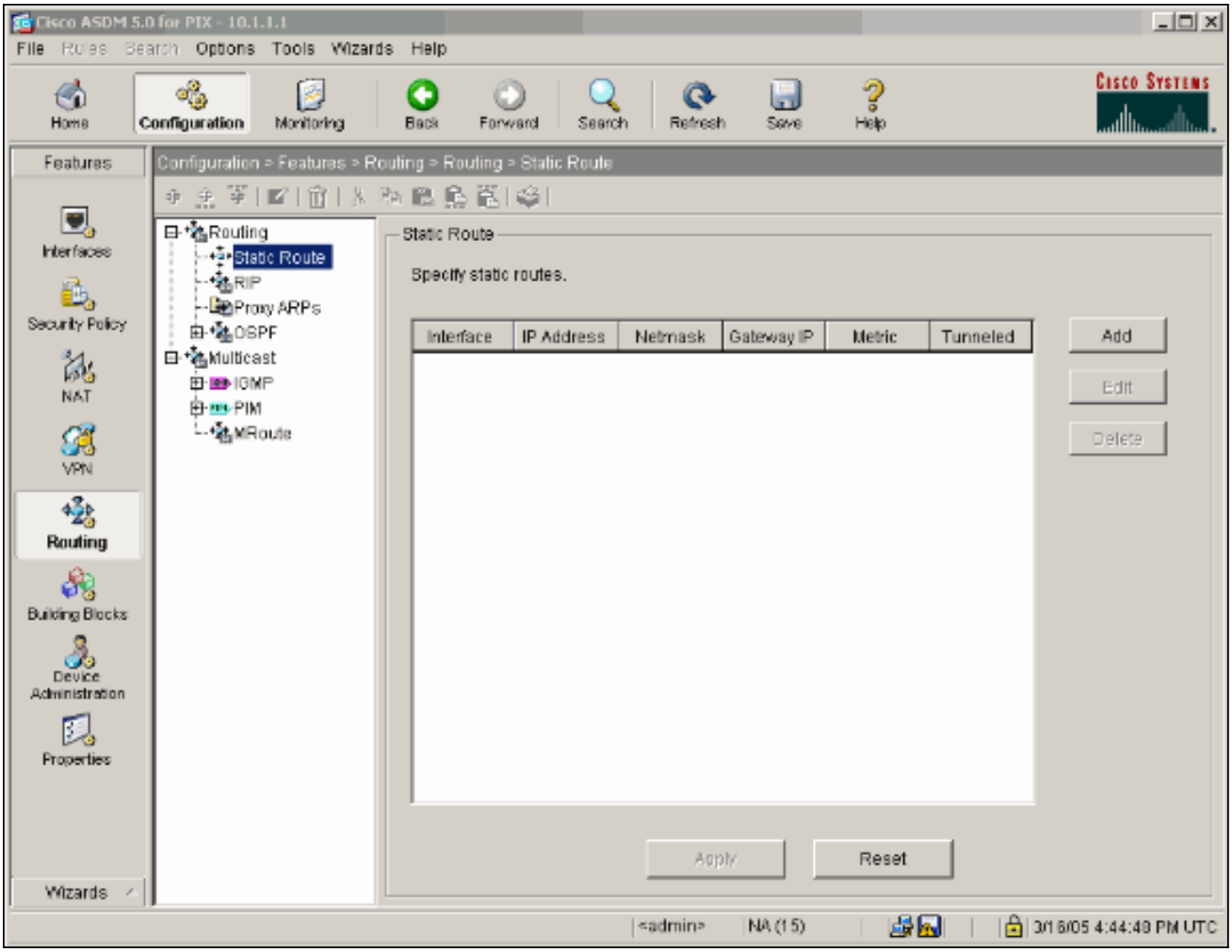
9. انقر فوق **موافق** في موجه الأمر تغيير واجهة.



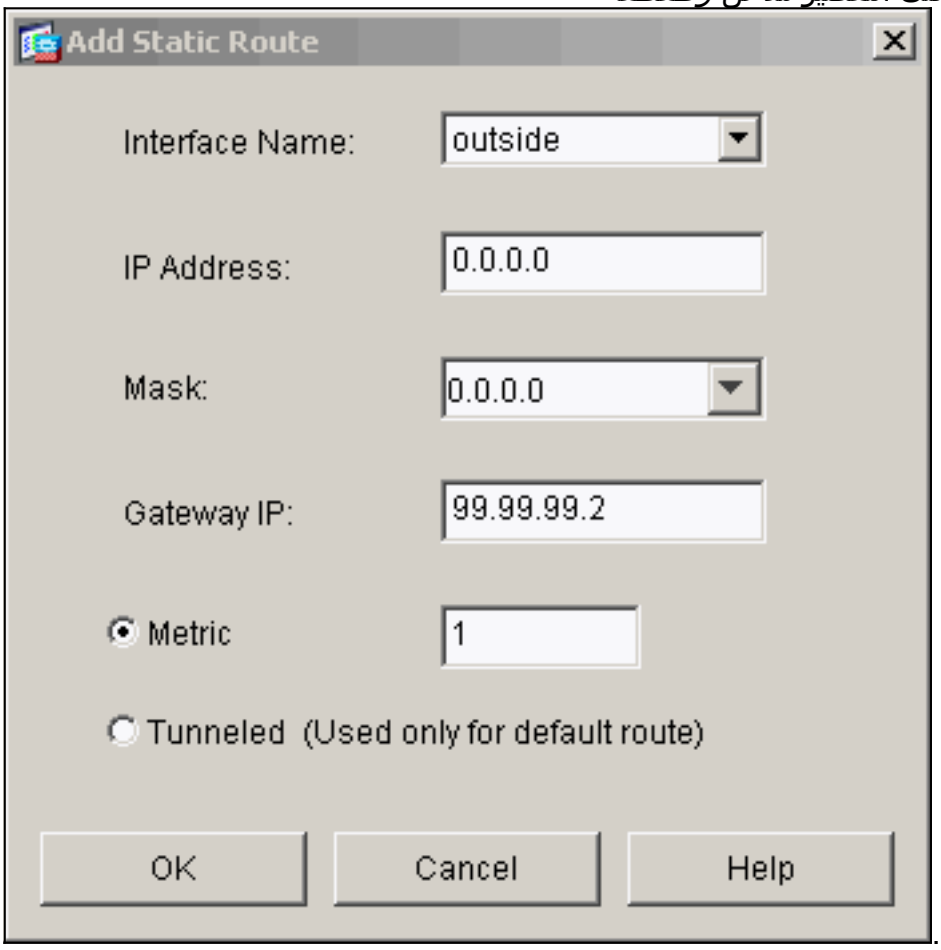
10. طقطقة **يطبق** in order to قبلت القارن تشكيل. كما يتم دفع التهيئة إلى تطبيق PIX. يستخدم هذا المثال مسارات ثابتة.



11. انقر على **توجيه** ضمن علامة التبويب الميزات، قم بتمييز **المسار الثابت**، وانقر فوق **إضافة**.

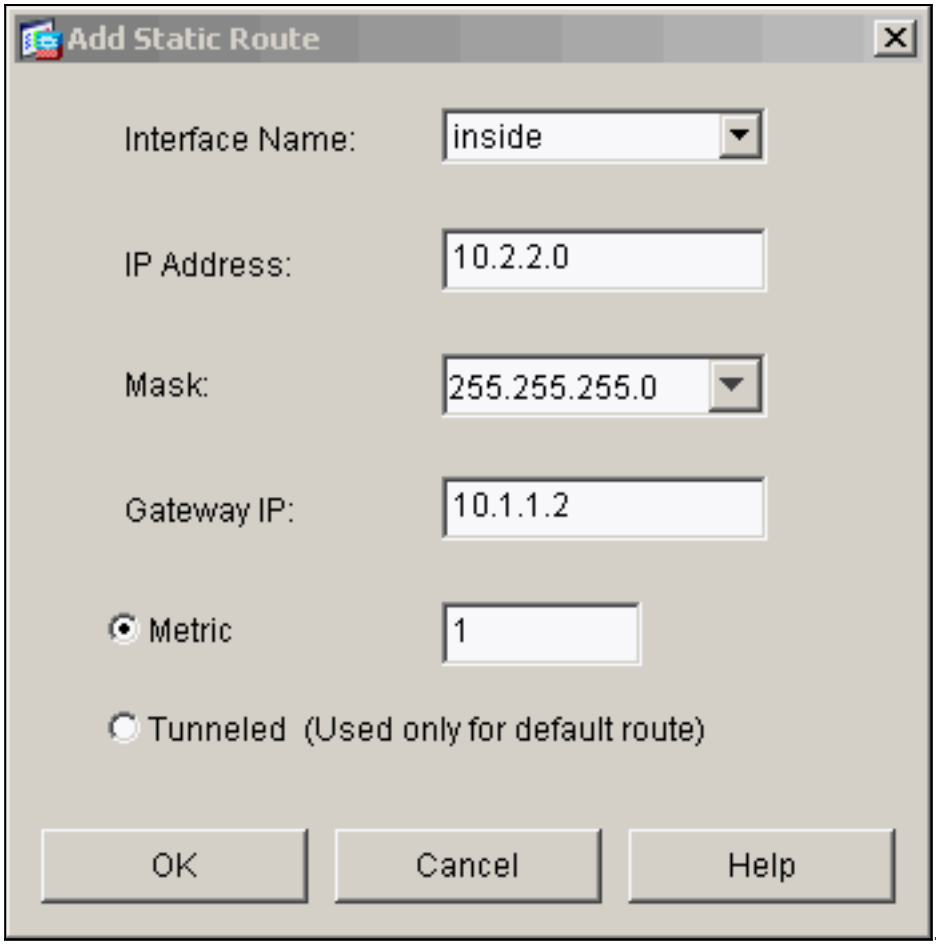


12. شكلت التقصير مدخل وطقطقة



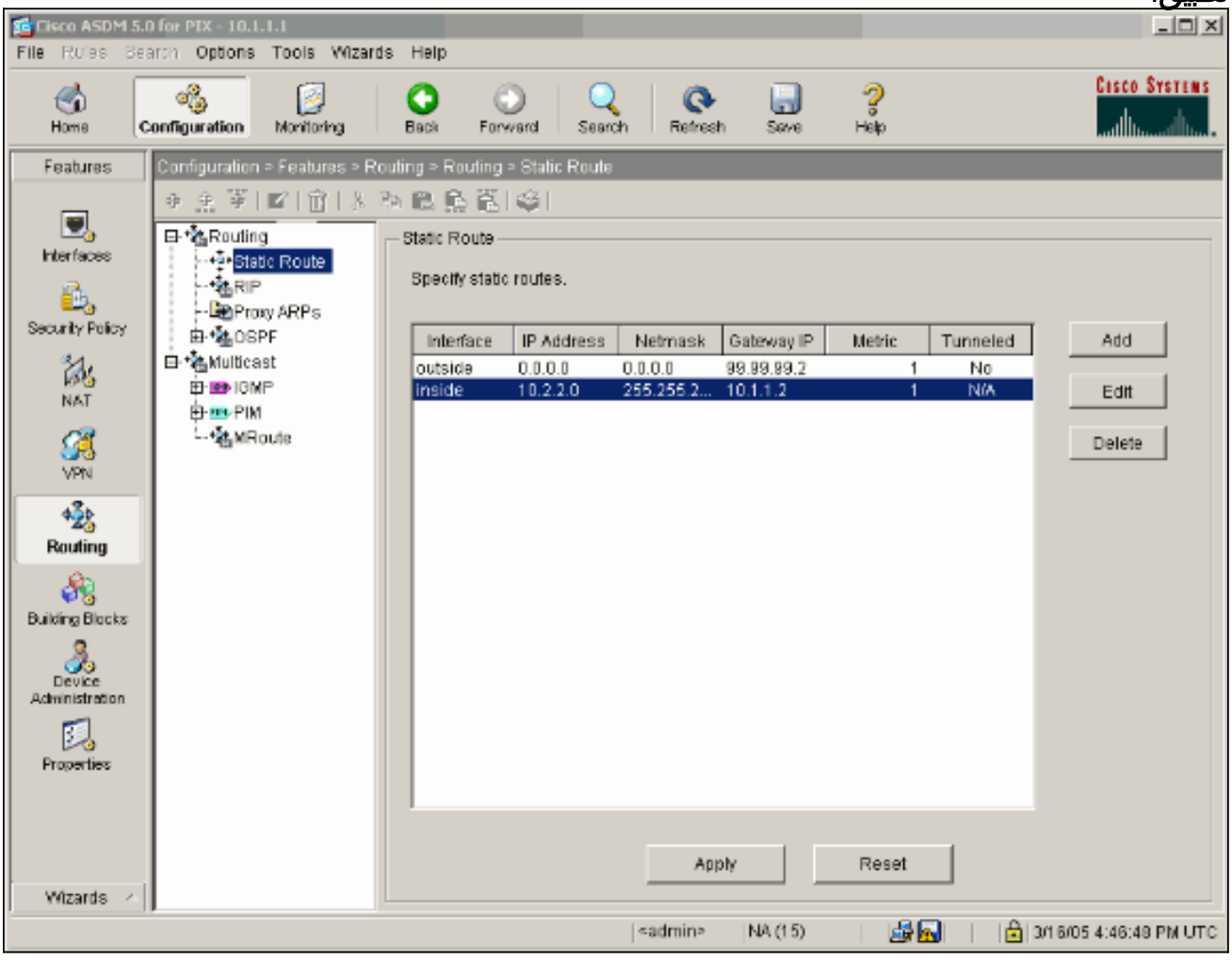
.ok

13. انقر على **إضافة** المسارات وإضافتها إلى الشبكات

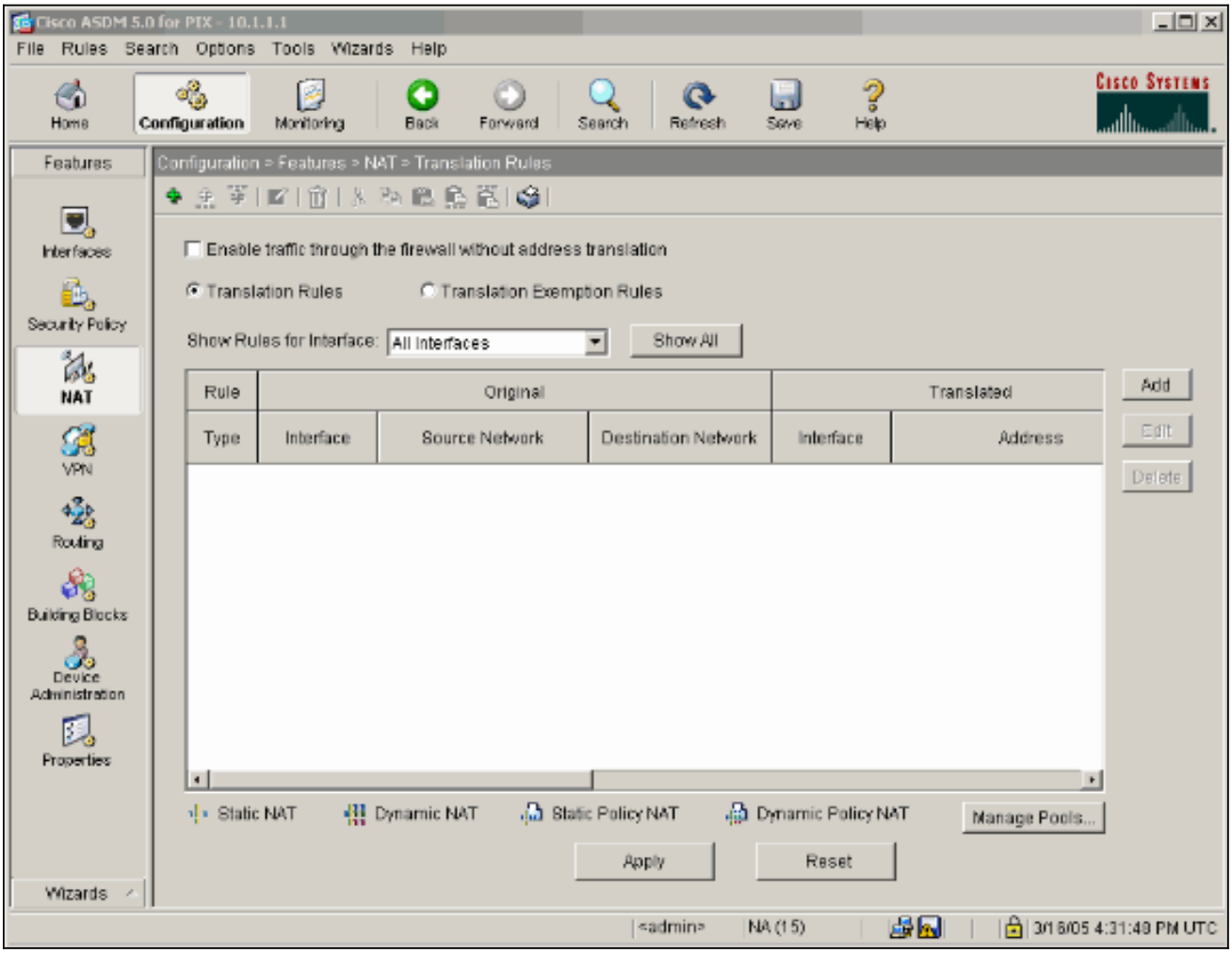


الداخلية.

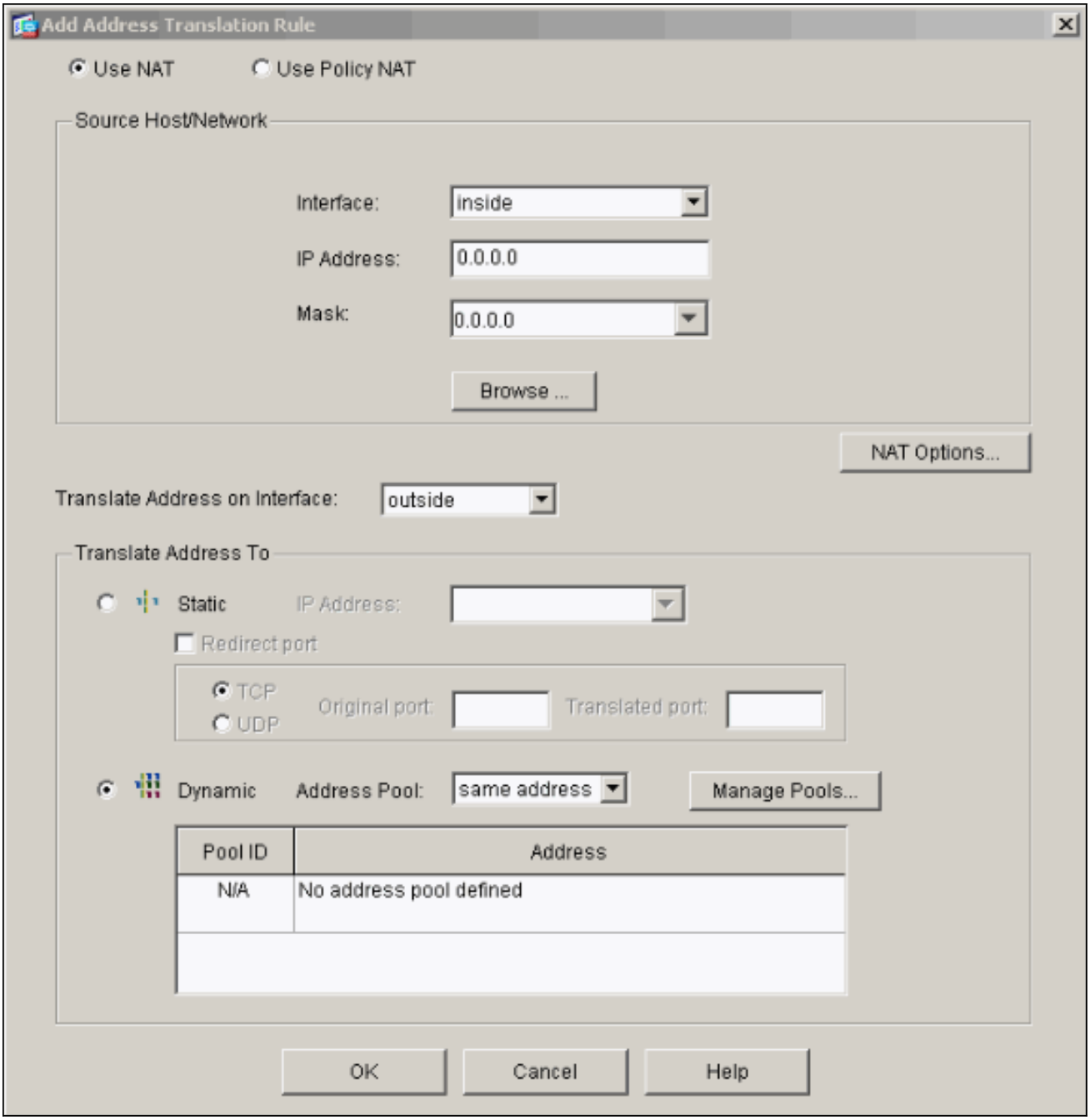
14. تأكد من تكوين المسارات الصحيحة وانقر فوق **تطبيق**.



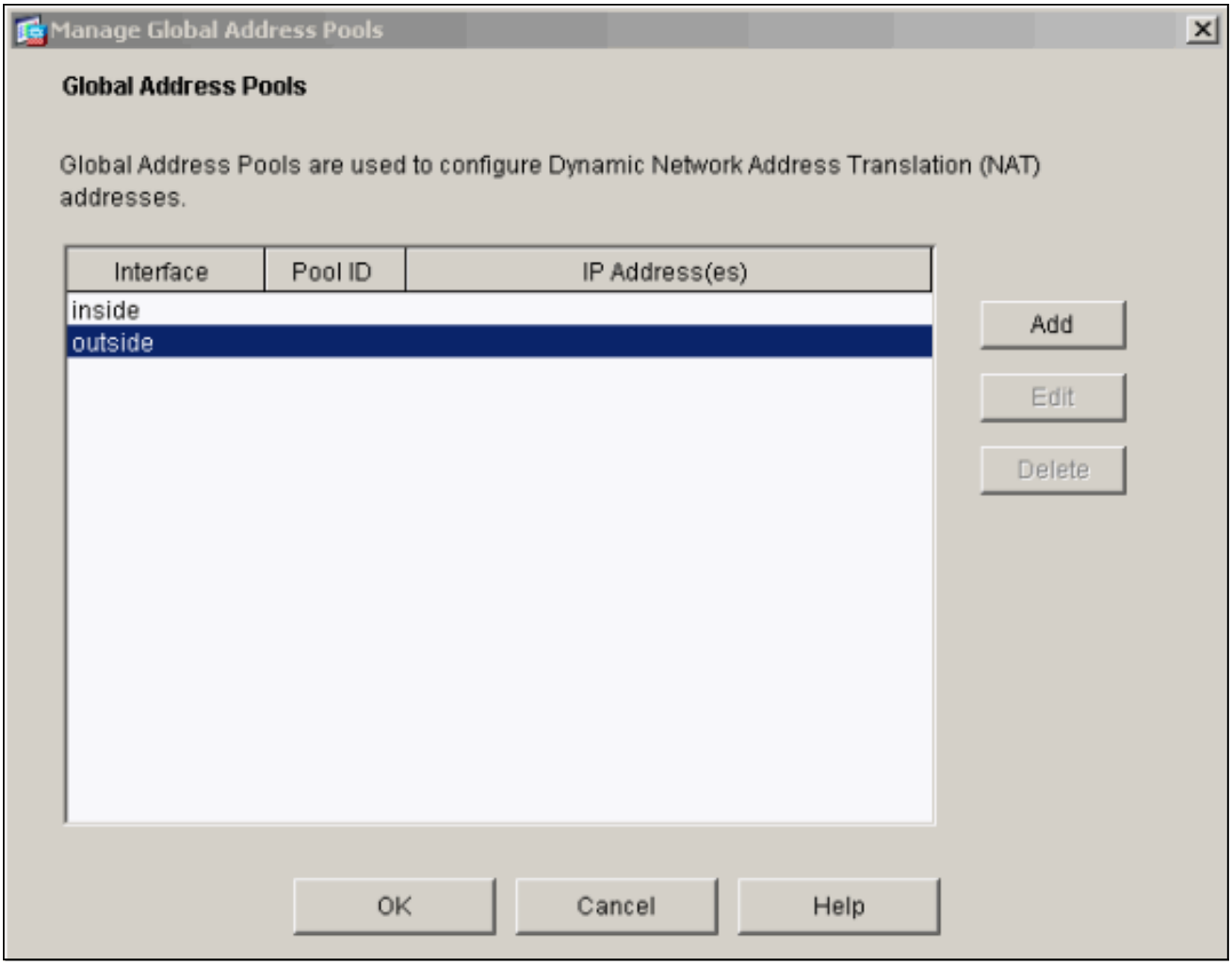
15. في هذا مثال، استعملت nat. أزلت ال تدقيق على صندوق ل **يمكن حركة مرور خلال جدار الحماية دون عنوان ترجمة** وطقطقة **يضيف** in order to شكلت ال nat قاعدة.



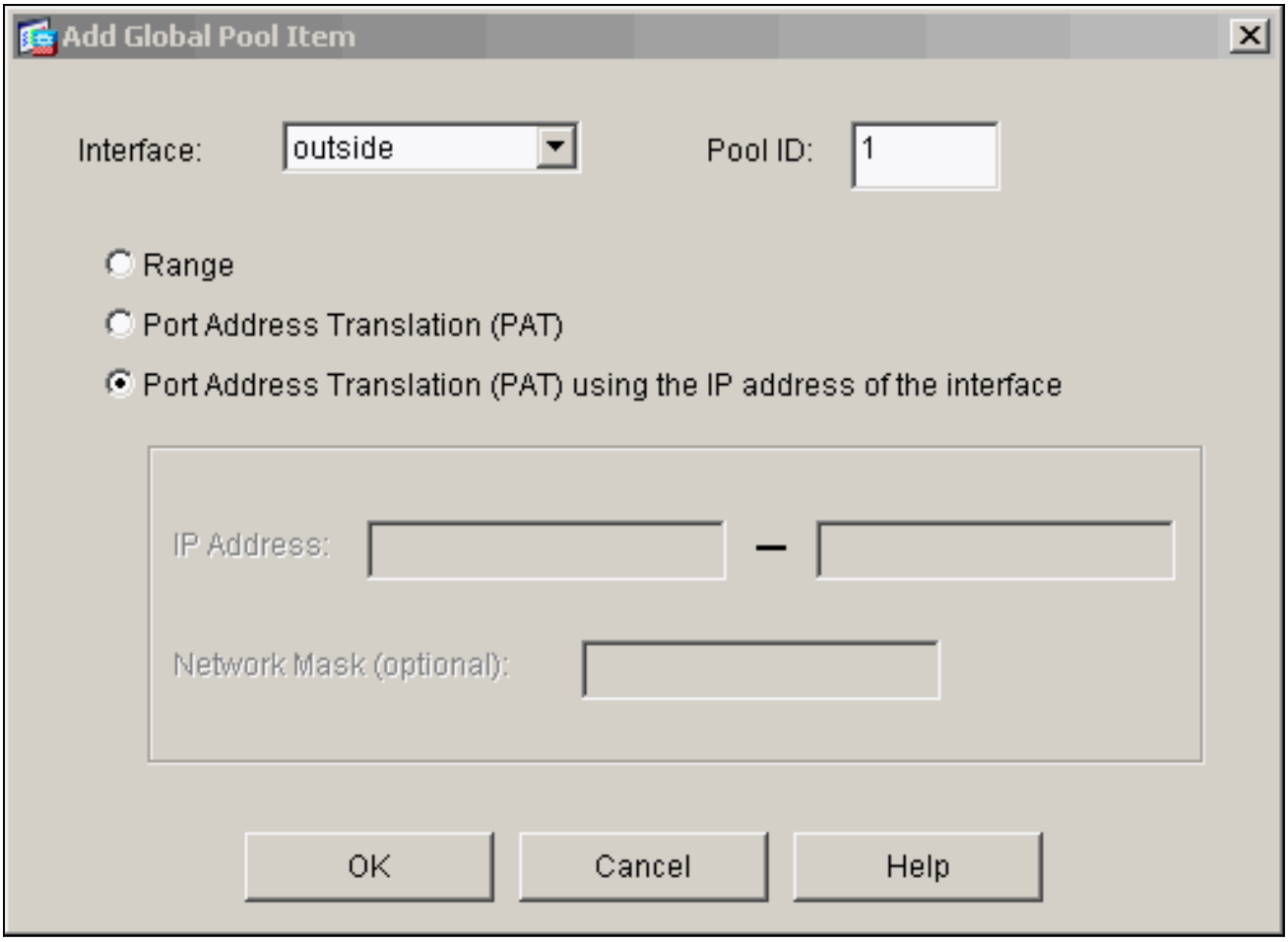
16. قم بتكوين الشبكة المصدر (هذا المثال يتضمن أي). بعد ذلك انقر فوق **إدارة التجمعات** لتحديد ضرب.



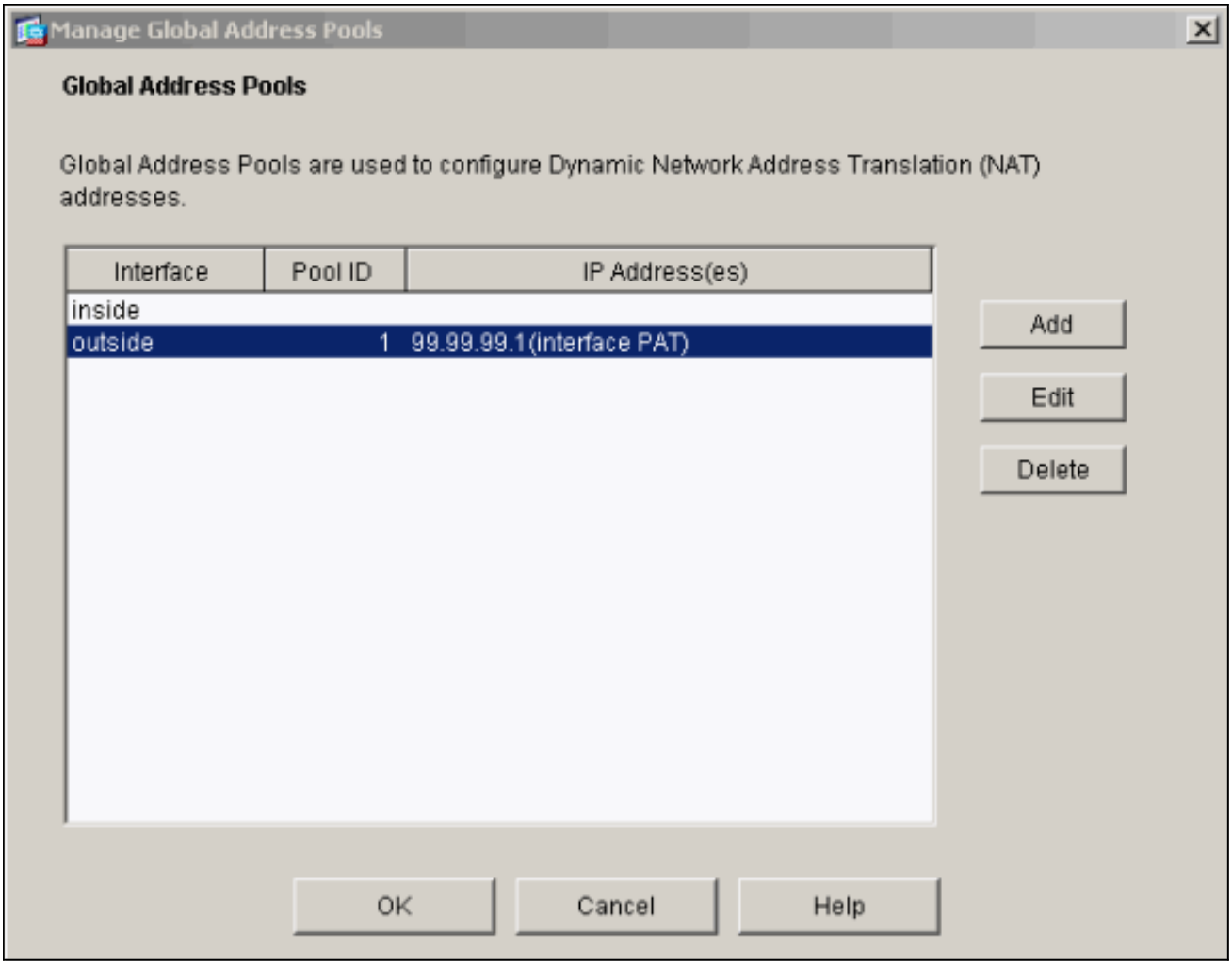
17. حدد الواجهة **الخارجية** وانقر فوق **إضافة**.



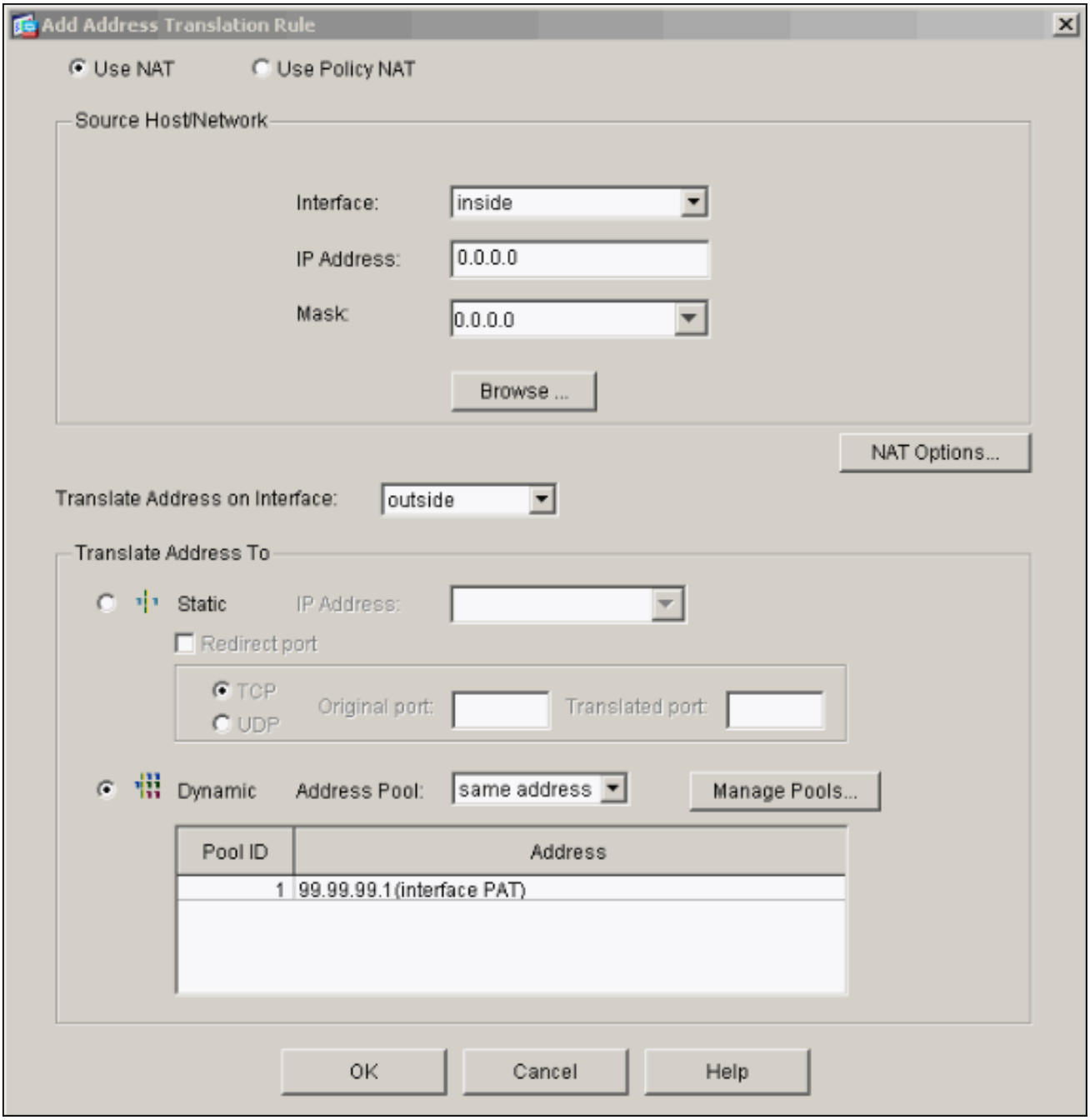
يستعمل هذا مثال ضرب يستعمل العنوان من القارن.



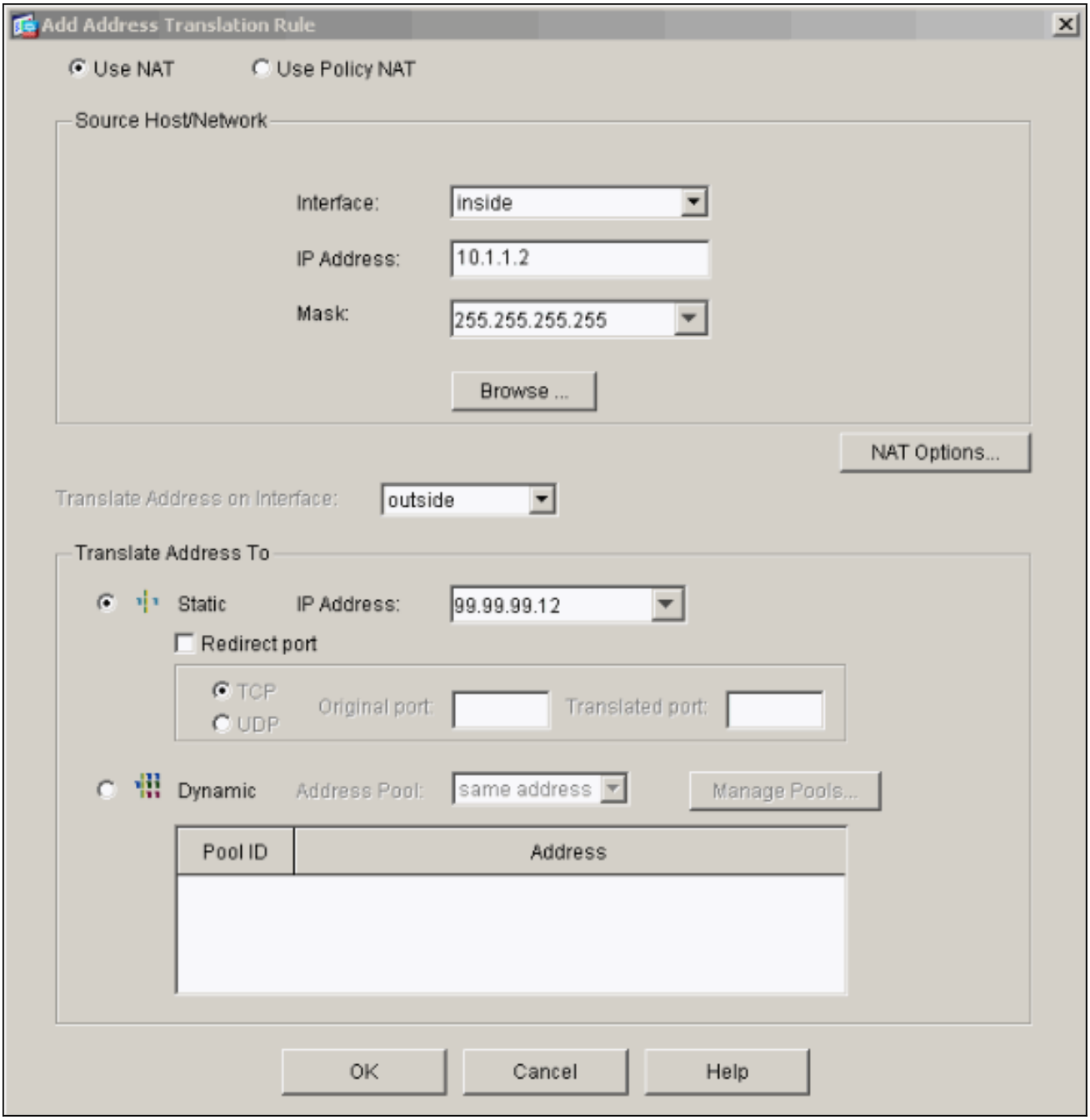
18. طقطقت **ok** عندما ال ضرب يكون شكلت.



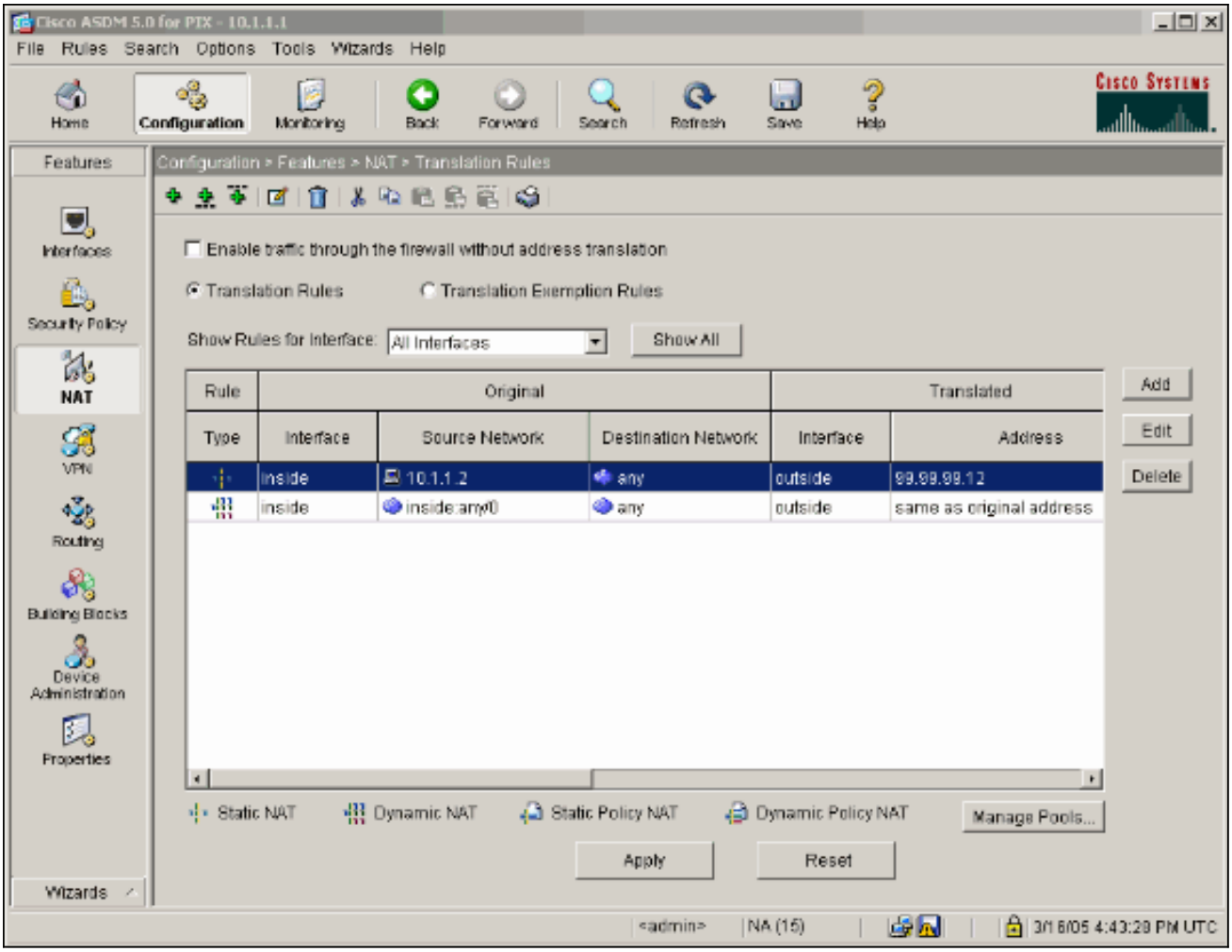
19. طقطقة **يضيف** in order to شكلت الترجمة ساكن إستاتيكي.



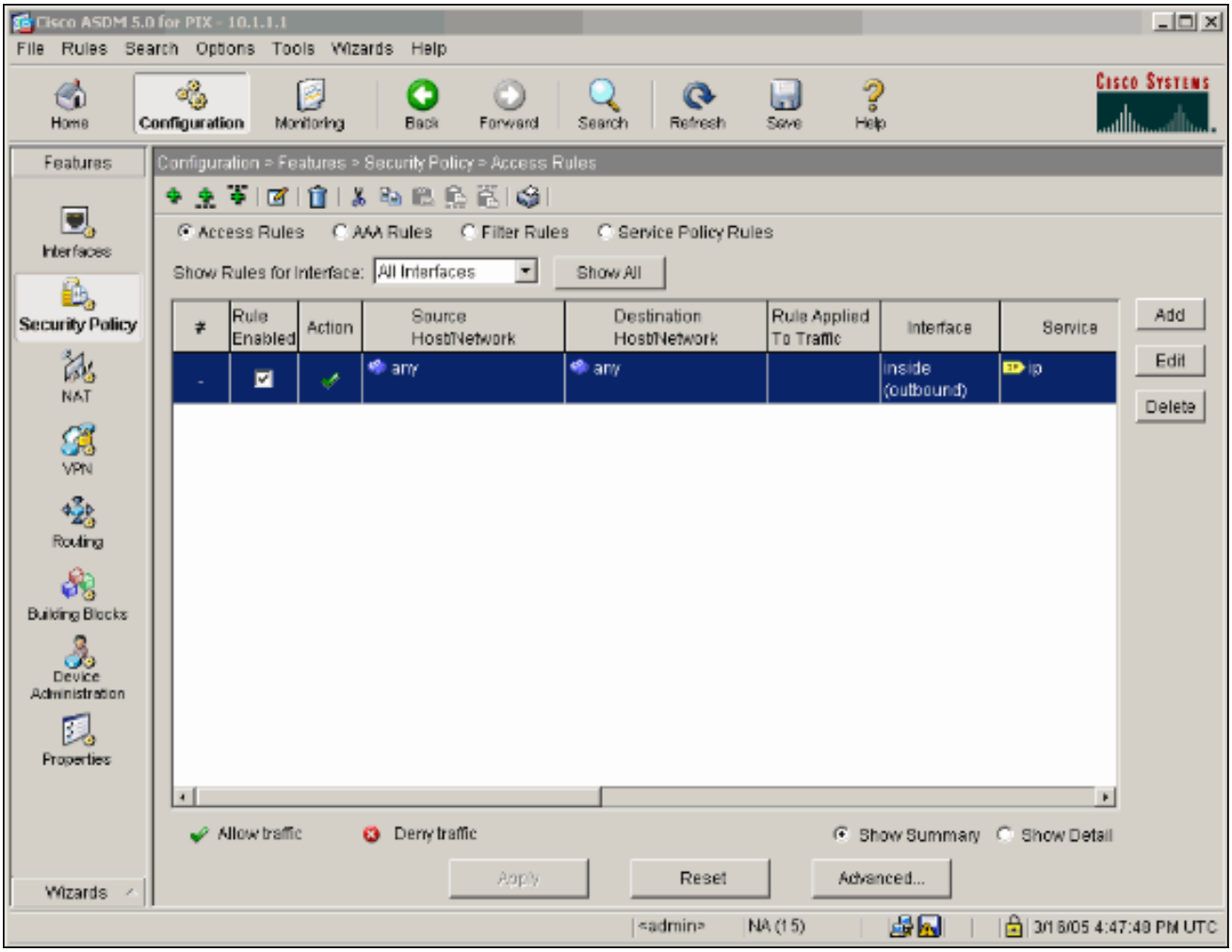
20. حدد داخل على الواجهة المنسدلة، ثم أدخل عنوان IP **10.1.1.2**، قناع الشبكة الفرعية **255.255.255.255**، واختر ثابت وفي نوع حقل عنوان IP خارج العنوان 99.99.99.12. انقر فوق موافق عند الانتهاء.



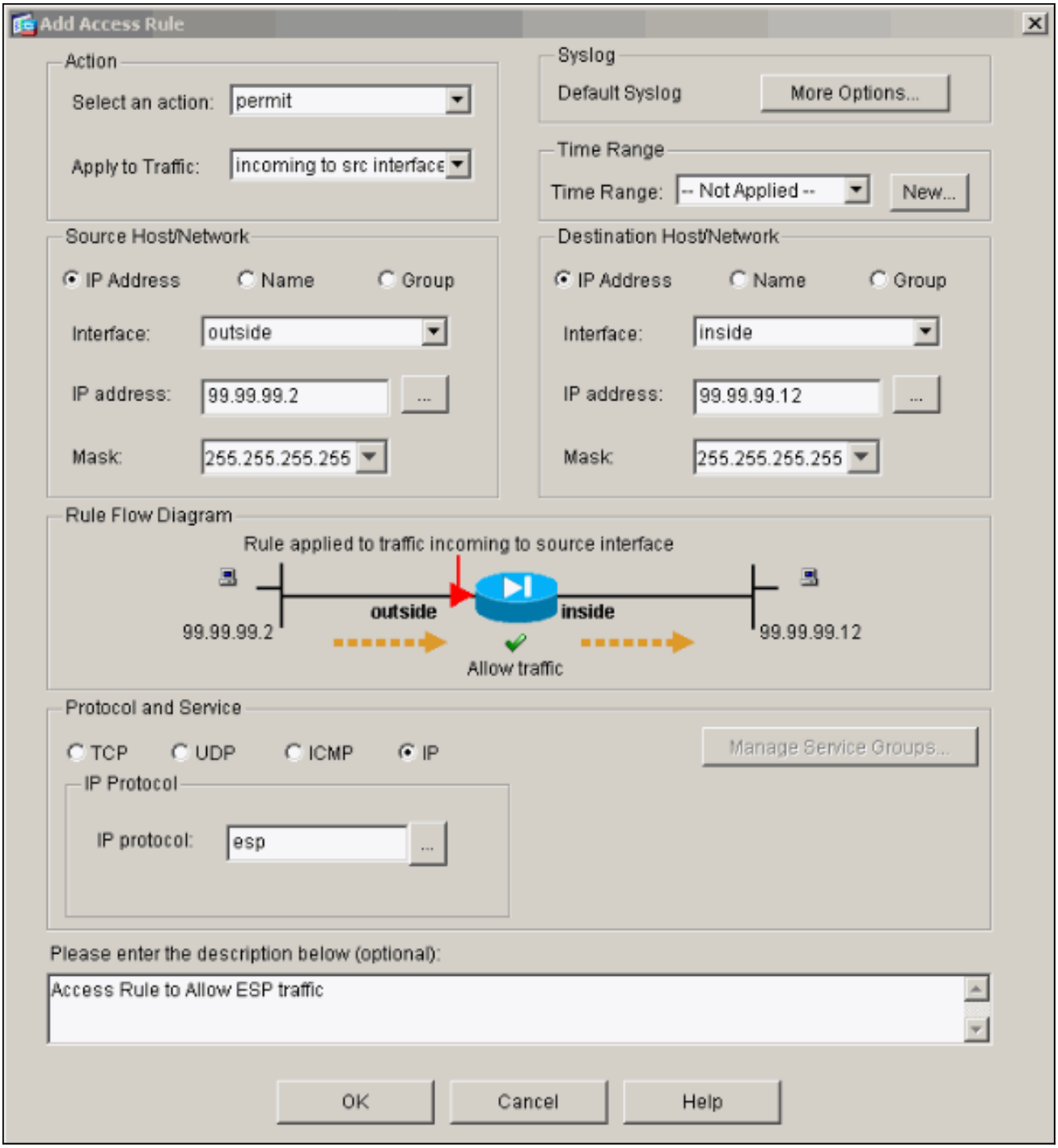
21. طقطقة **يطبق** أن يقبل القارن تشكيل. كما يتم دفع التهيئة إلى تطبيق PIX.



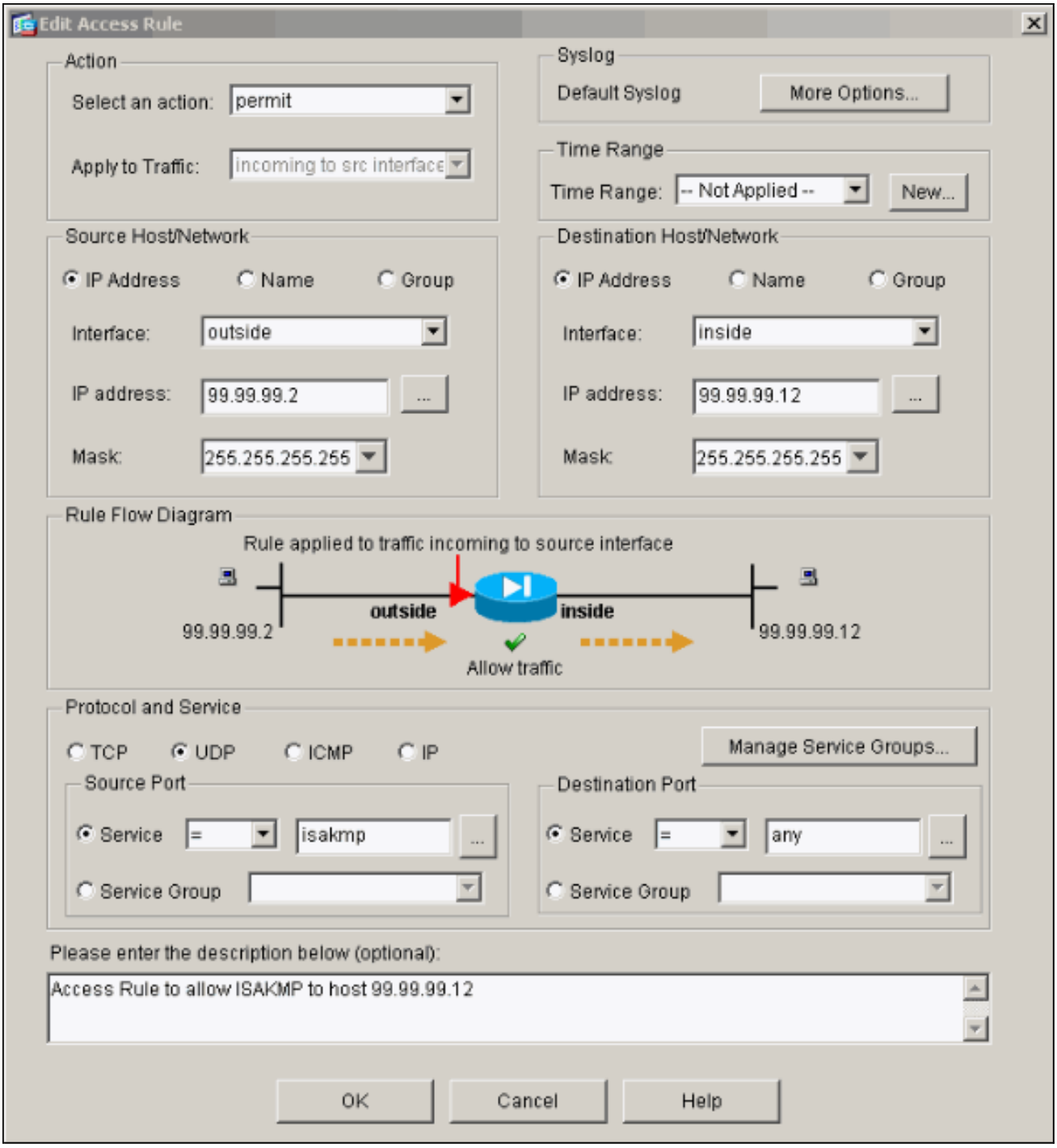
22. حدد **نهج الأمان** ضمن علامة التبويب الميزات لتكوين قاعدة نهج الأمان.



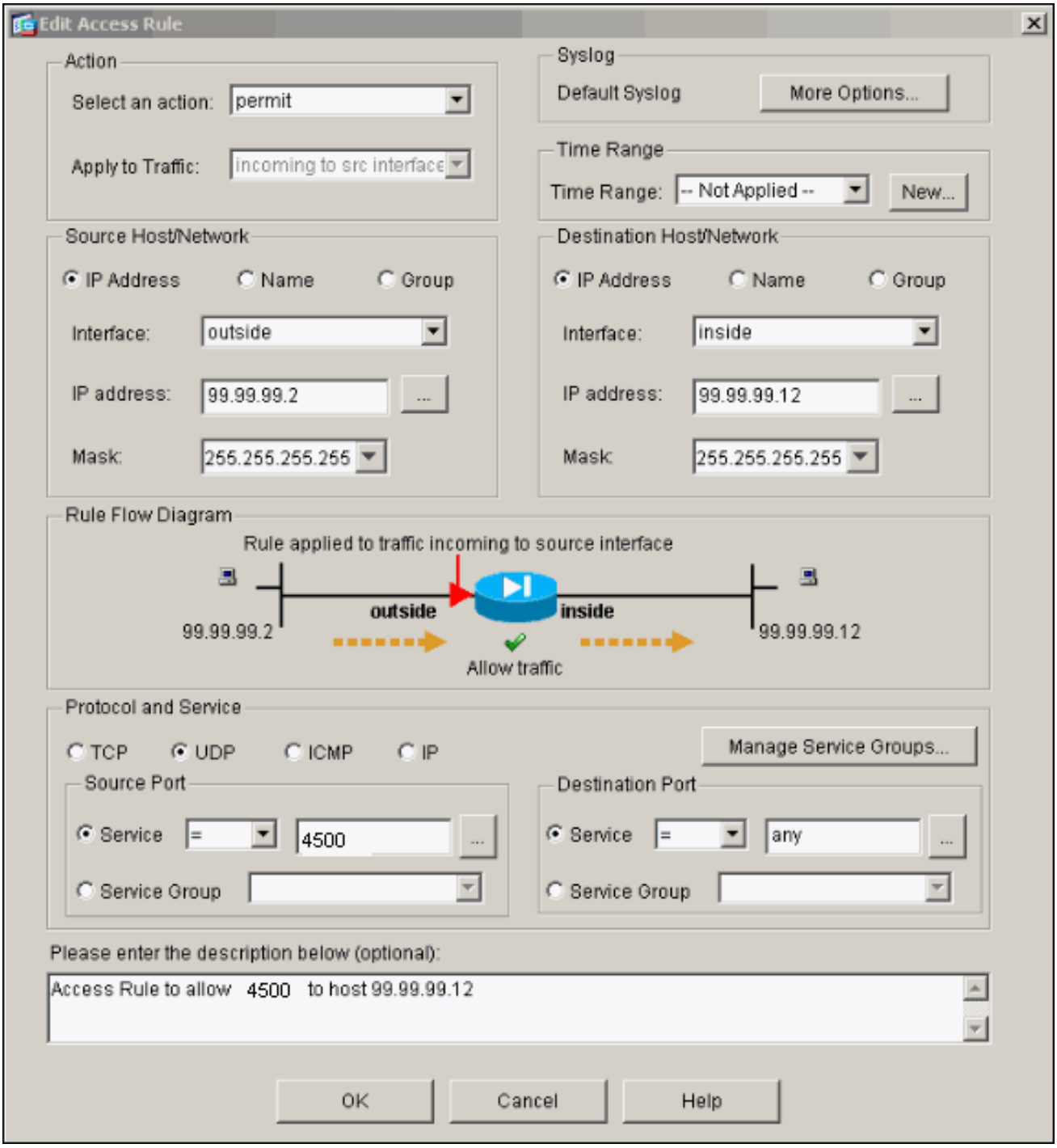
23. انقر فوق **إضافة** للسماح بحركة مرور ESP وانقر فوق **موافق** للمتابعة.



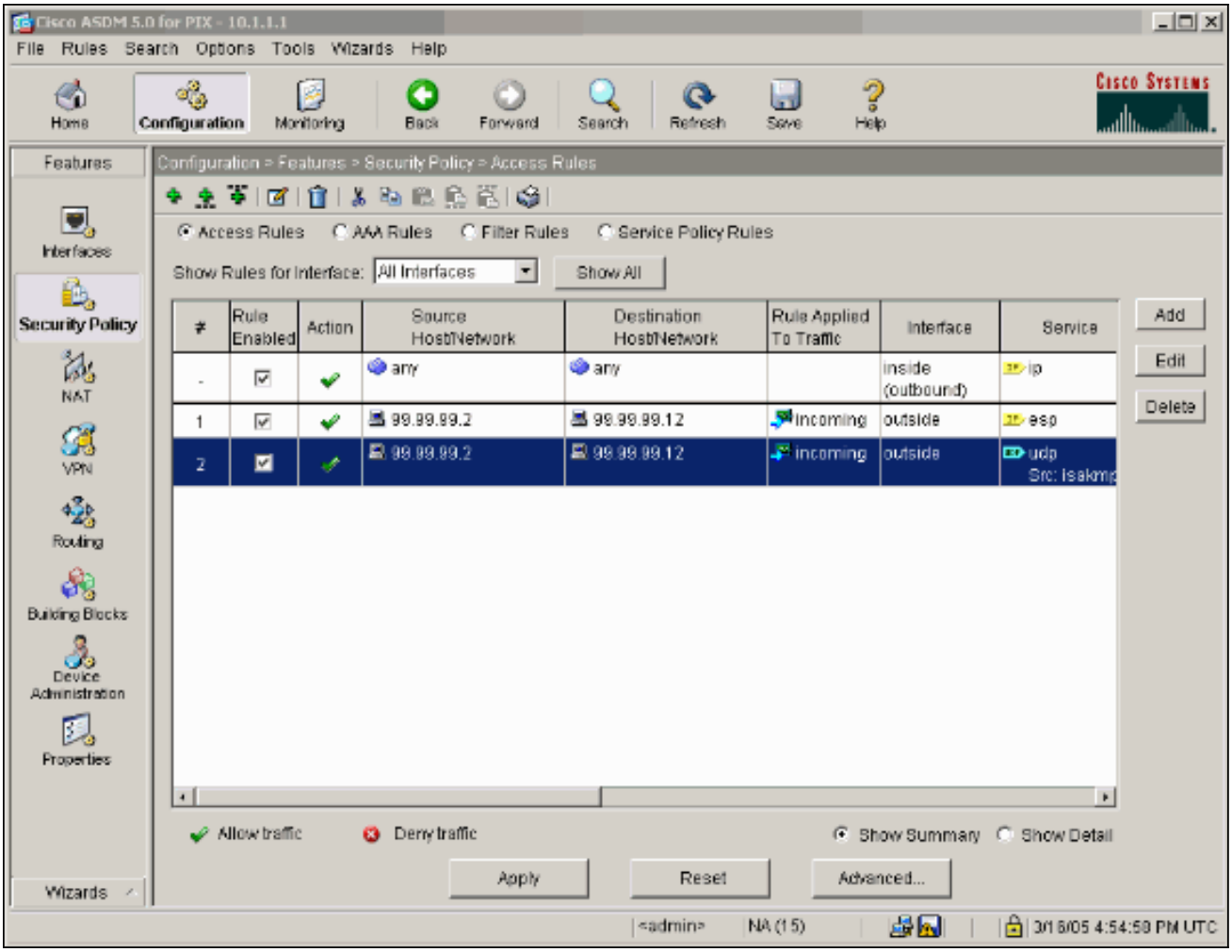
24. انقر فوق **إضافة** للسماح بحركة مرور ISAKMP وانقر فوق **موافق** للمتابعة.



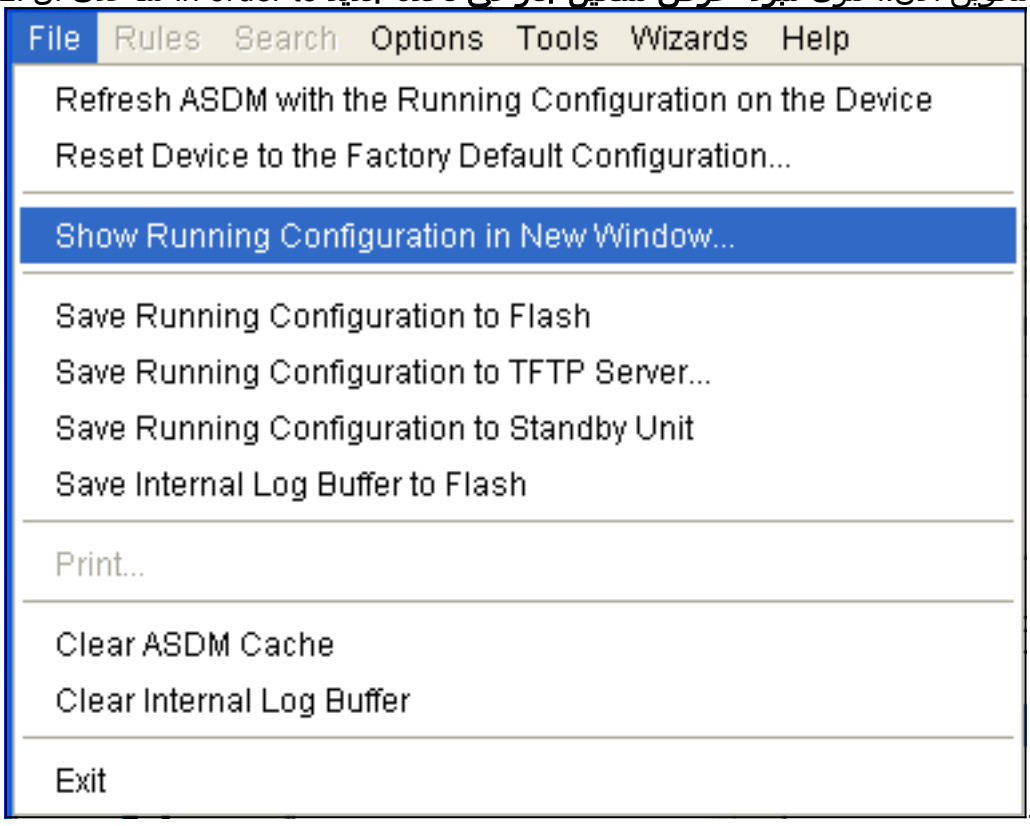
25. طقطقة **يضيف** in order to سمحت UDP ميناء 4500 حركة مرور ل NAT-T وطقطقة to in order **ok** باشرت.



26. طقطقة **يطبق** in order to قبلت القارن تشكيل. كما يتم دفع التهيئة إلى تطبيق PIX.



27. اكتمل التكوين الآن.أخترت **مبرد>عرض تشكيل جار في نافذة جديد** in order to شاهدت ال CLI



تشكيل.

[تكوين جدار حماية PIX]

جدار حماية PIX

```
pixfirewall# show run
Saved :
:
PIX Version 7.0(0)102
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 99.99.99.1 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
ftp mode passive

access-list outside_access_in remark Access Rule to
Allow ESP traffic
access-list outside_access_in
extended permit esp host 99.99.99.2 host
99.99.99.12

access-list outside_access_in
remark Access Rule to allow ISAKMP to host
99.99.99.12
access-list outside_access_in
extended permit udp host 99.99.99.2 eq
isakmp host 99.99.99.12


access-list outside_access_in
remark Access Rule to allow port 4500 (NAT-
T) to host 99.99.99.12
access-list outside_access_in
extended permit udp host 99.99.99.2
eq 4500 host 99.99.99.12
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
monitor-interface inside
monitor-interface outside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 0 0.0.0.0 0.0.0.0
static (inside,outside) 99.99.99.12 10.1.1.2 netmask
255.255.255.255
access-group outside_access_in in interface outside
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
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
                                  sip 0:30:00 sip_media 0:02:00 0:05:00
                                         timeout uauth 0:05:00 absolute
                                                  http server enable
                                   http 10.1.1.3 255.255.255.255 inside
                                               no snmp-server location
                                                no snmp-server contact
                                          snmp-server enable traps snmp
                                                       telnet timeout 5
                                                          ssh timeout 5
                                                     console timeout 0
                                                                     !
                                           class-map inspection_default
                                        match default-inspection-traffic
                                                                     !
                                                                     !
                                      policy-map asa_global_fw_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
                                                                     !
                                    service-policy asa_global_fw_policy global
                                  Cryptochecksum:0a12956036ce4e7a97f351cde61fba7e
                                                              end :
```

تكوين جهاز أمان PIX و MPF (إطار عمل السياسات النمطي)

بدلا من قائمة الوصول، أستخدم الأمر **فحص ipSec-pass-thru** في MPF(إطار عمل السياسة النمطية) لتمرير حركة مرور IPsec من خلال أجهزة أمان PIX/ASA.

تم تكوين هذا الفحص لفتح ثقوب لحركة مرور ESP. يتم السماح بجميع تدفقات بيانات ESP عند وجود تدفق للأمام، ولا يوجد حد على الحد الأقصى لعدد الاتصالات التي يمكن السماح بها. غير مسموح ب AH. تم تعيين المهلة الافتراضية في وضع الخمول لتدفقات بيانات ESP بشكل افتراضي على 10 دقائق. يمكن تطبيق هذا الفحص في جميع المواقع التي يمكن تطبيق عمليات فحص أخرى عليها، والتي تتضمن أوضاع الأوامر من حيث الفئة والمطابقة. يوفر فحص التطبيق IPSec Pass Through إجتياز مناسب لحركة مرور ESP (بروتوكول IP رقم 50) المرتبطة باتصال منفذ IKE UDP رقم 500. كما يتجنب تكوين قائمة الوصول الطويلة للسماح بحركة مرور ESP ويوفر الأمان أيضا مع إتصالات المهلة والحد الأقصى. أستخدم الأوامر **class-map** و**policy-map** و**service-policy** لتحديد فئة حركة مرور البيانات، لتطبيق أمر الفحص على الفئة، وتطبيق السياسة على واجهة واحدة أو أكثر. عند تمكينها، يسمح الأمر **inspection ipsEC-pass-thru** بحركة مرور ESP غير المحدودة بمهلة 10 دقائق، والتي تكون غير قابلة للتكوين. يسمح بحركة المرور NAT وغير NAT.

```
hostname(config)#access-list test-udp-acl extended permit udp any any eq 500
hostname(config)#class-map test-udp-class
hostname(config-cmap)#match access-list test-udp-acl
hostname(config)#policy-map test-udp-policy
```

```
hostname(config-pmap)#class test-udp-class
hostname(config-pmap-c)#inspect ipsec-pass-thru
hostname(config)#service-policy test-udp-policy interface outside
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- **show crypto ips sa**—يعرض اقترانات أمان المرحلة 2.
- **show crypto isakmp sa**—يعرض اقترانات أمان المرحلة 1.
- **show crypto engine connections active** — يعرض الحزم المشفرة وغير المشفرة.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر أستكشاف الأخطاء وإصلاحها ل IPsec للموجه

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

- **debug crypto engine**—يعرض حركة مرور البيانات التي يتم تشفيرها.
- **debug crypto ipSec**—يعرض مفاوضات IPsec للمرحلة 2.
- **debug crypto isakmp**—يعرض مفاوضات بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) للمرحلة الأولى.

التخلص من الرابطات الأمنية

- **مسح التشفير isakmp**—يعمل على مسح اقترانات أمان تبادل مفتاح الإنترنت (IKE).
- **مسح اقترانات** أمان IPsec **للتشفير**.

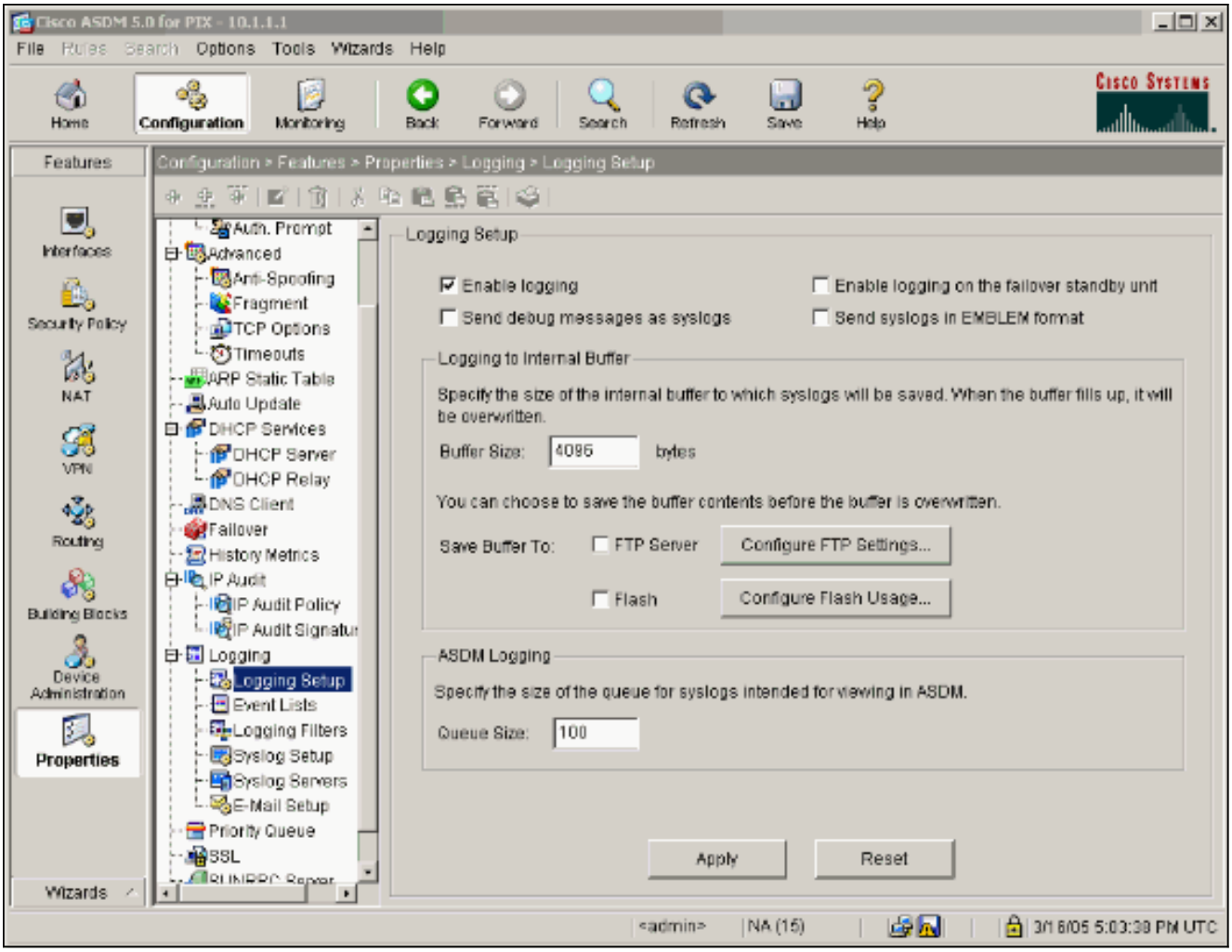
أوامر أستكشاف الأخطاء وإصلاحها ل PIX

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

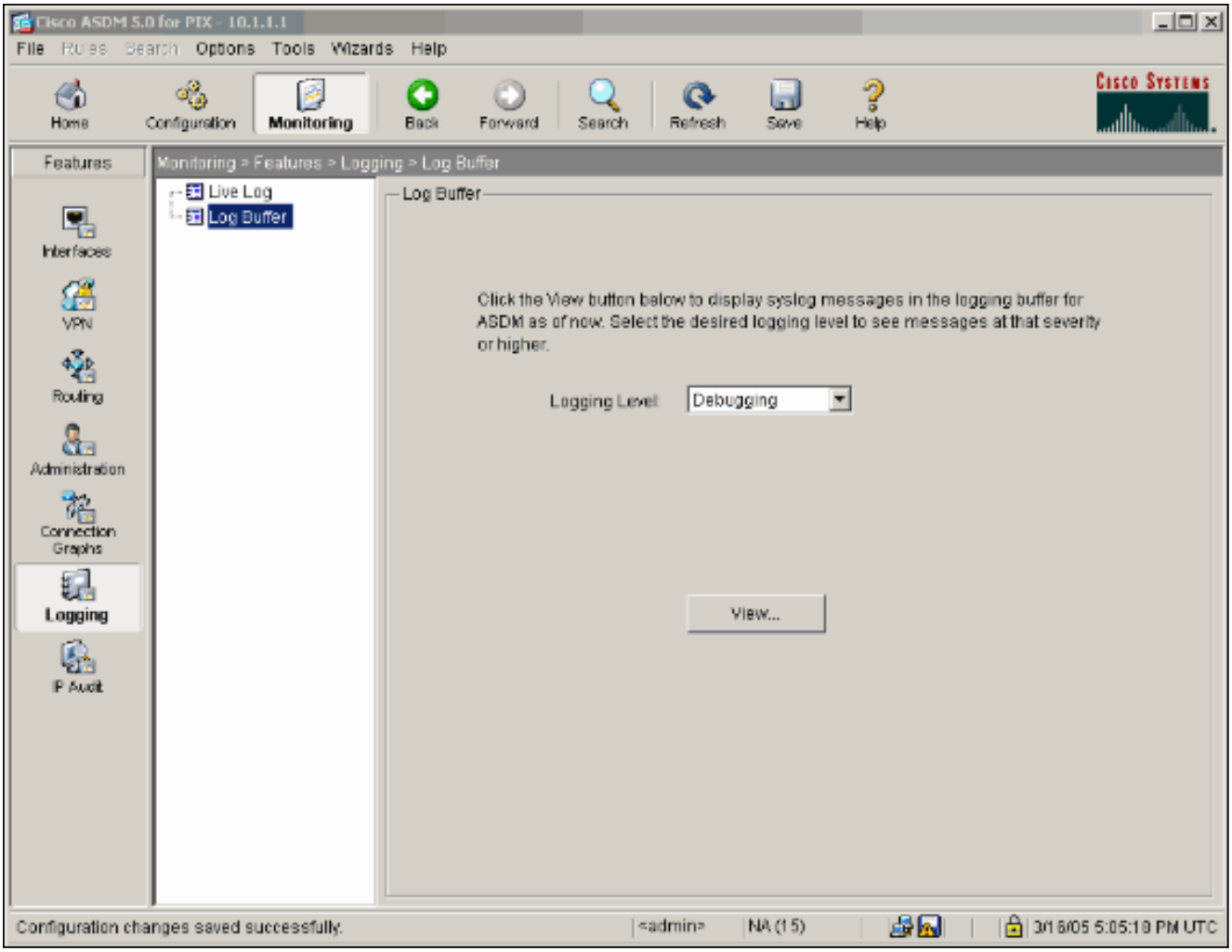
ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إصدار أوامر **debug**.

- **تصحيح أخطاء مخزن التسجيل المؤقت**— يعرض الاتصالات التي يتم إنشاؤها ويتم رفضها للمضيفين الذين يمرون عبر PIX. يتم تخزين المعلومات في المخزن المؤقت لسجل PIX ويمكن رؤية الإخراج باستخدام الأمر **show log**.
- يمكن إستخدام ASDM لتمكين التسجيل وأيضا لعرض السجلات كما هو موضح في هذه الخطوات.

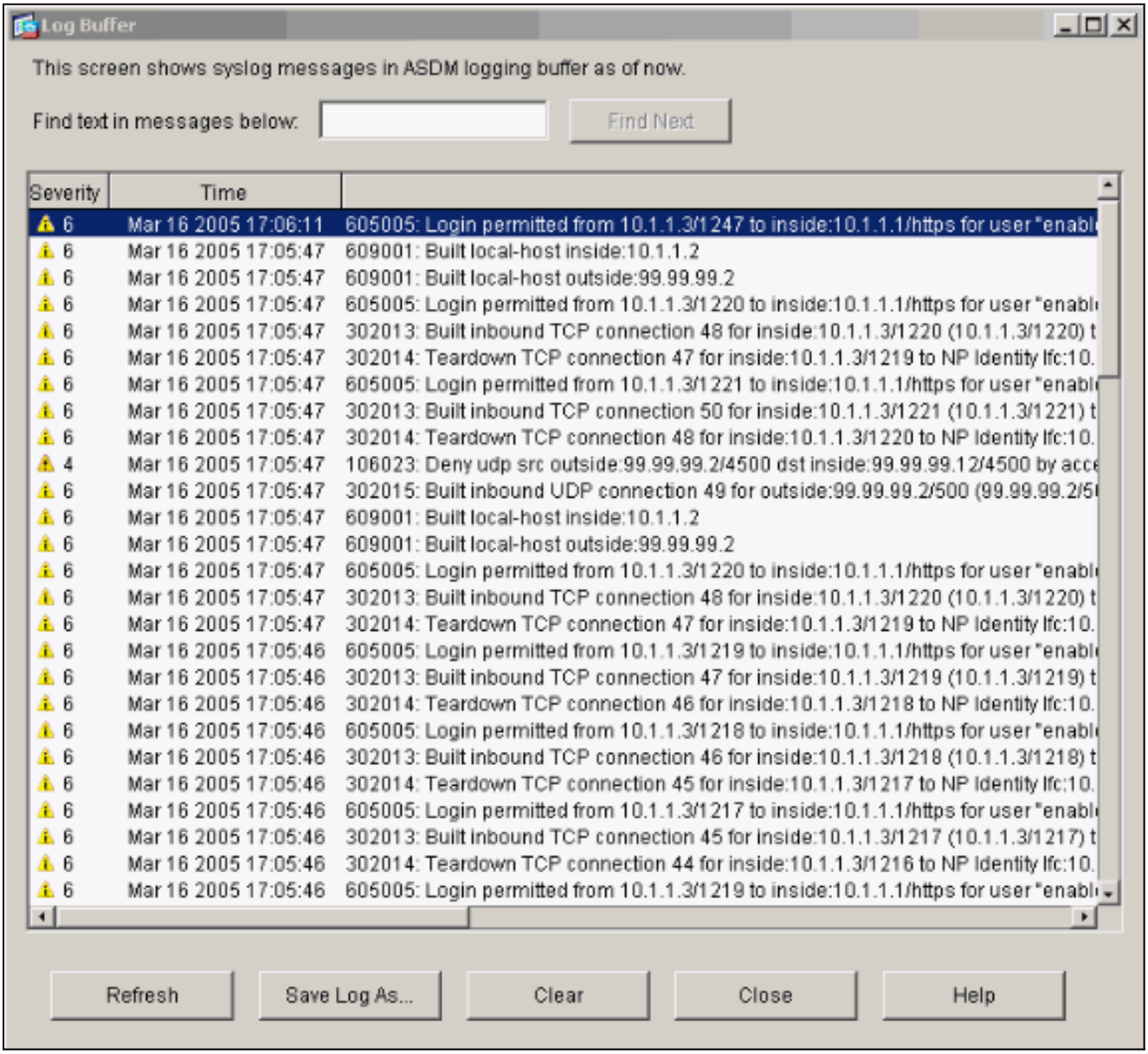
1. أختر **تكوين > خصائص > تسجيل > إعداد التسجيل > تمكين التسجيل** ثم انقر فوق **تطبيق**.



2. أختر **مراقبة > تسجيل > مخزن السجل المؤقت > على مستوى التسجيل > مخزن التسجيل المؤقت**، ثم انقر فوق
عرض.



هذا مثال على المخزن المؤقت
للسجل.



معلومات ذات صلة

- صفحة دعم مفاوضة IPsec/بروتوكولات IKE
- صفحة دعم PIX
- مراجع أوامر PIX
- صفحة دعم ترجمة عناوين الشبكة (NAT)
- 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).