PIX/ASA 7.x: إعادة توجيه المنفذ (إعادة التوجيه) باستخدام أوامر NAT و Global و Static و Access-list

المحتويات

المقدمة

لزيادة الأمان إلى الحد الأقصى عند تنفيذ جهاز أمان Cisco PIX الإصدار 7.0، من المهم فهم كيفية مرور الحزم بين واجهات الأمان الأعلى وواجهات الأمان الأقل عند إستخدام أوامر **access-list**، **static**، global، nat، nat-control وaccess-groups. يشرح هذا المستند الاختلافات بين هذه الأوامر وكيفية تكوين ميزات إعادة توجيه المنفذ (إعادة التوجيه) وميزة ترجمة عنوان الشبكة (NAT) الخارجية في إصدار برنامج PIX 7.x، مع إستخدام واجهة سطر الأوامر أو مدير أجهزة الأمان القابل للتكيف (ASDM).

ملاحظة: قد تظهر بعض الخيارات في ASDM 5.2 والإصدارات الأحدث مختلفة عن الخيارات الموجودة في ASDM 5.1. راجع وثائق ASDM للحصول على مزيد من المعلومات.

المتطلبات الأساسية

المتطلبات

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:

- برنامج جهاز الأمان Cisco PIX 500 Series Security Appliance Software، الإصدار 7.0 والإصدارات الأحدث
- ASDM الإصدار x.5 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.

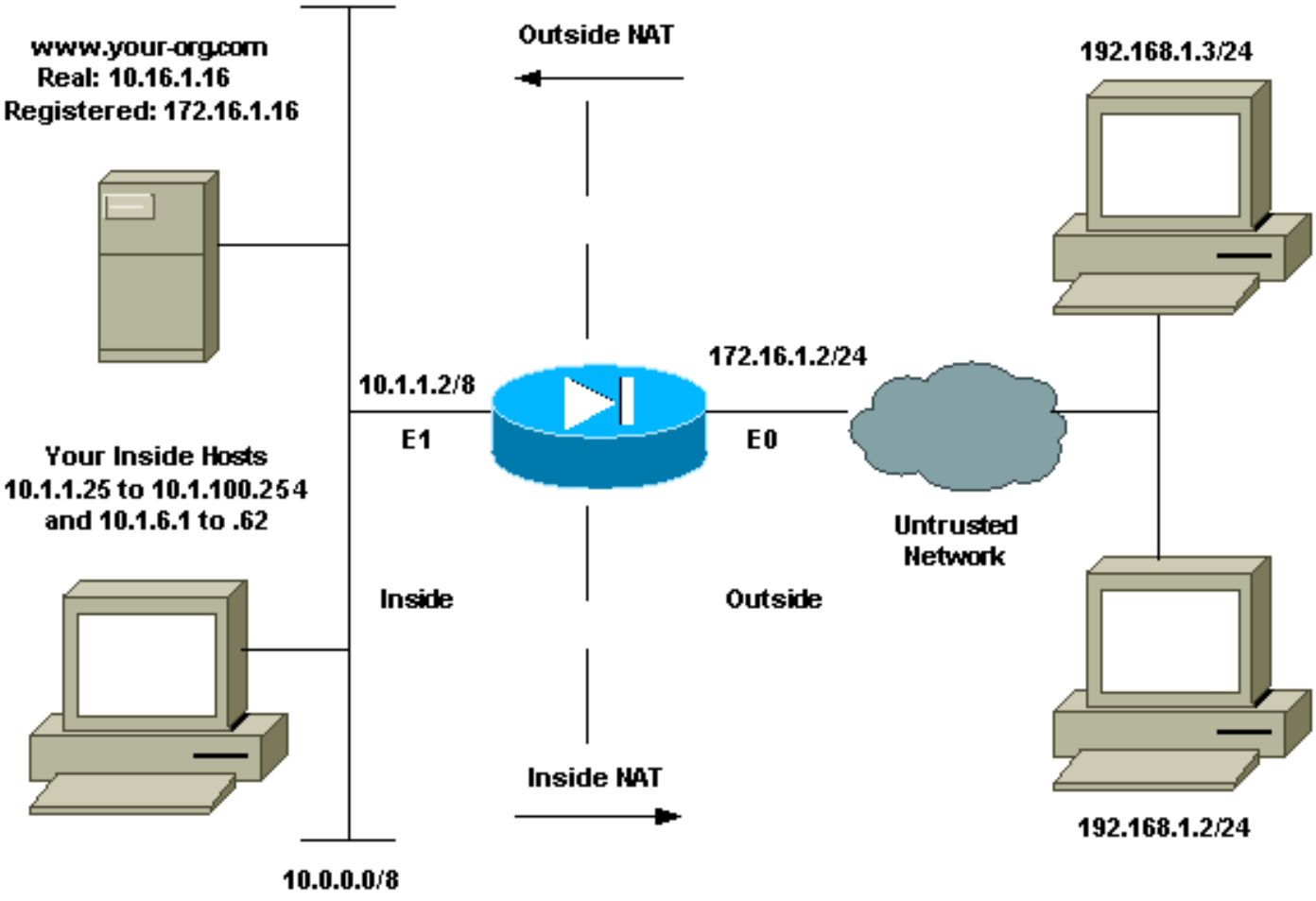
المنتجات ذات الصلة

يمكنك أيضا 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.

الرسم التخطيطي للشبكة



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.

التهيئة الأولية

أسماء الواجهة هي:

- **قارن إثرنيت 0**—namelf خارجي
- **واجهة إيثرنت 1**—namelf داخل

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

السماح بالوصول الصادر

يصف الوصول الصادر الاتصالات من واجهة مستوى أمان أعلى إلى واجهة مستوى أمان أقل. وهذا يشمل الاتصالات من الداخل إلى الخارج، ومن الداخل إلى المناطق المجردة من السلاح (المنطقة المجردة من السلاح)، والمنطقة المجردة من السلاح إلى الخارج. كما يمكن أن يتضمن ذلك إتصالات من DMZ إلى آخر، طالما كانت واجهة مصدر الاتصال تحتوي على مستوى أمان أعلى من الوجهة. راجع التكوين "مستوى الأمان" على واجهات PIX لتأكيد ذلك.

يوضح هذا المثال مستوى الأمان وتكوين اسم الواجهة:

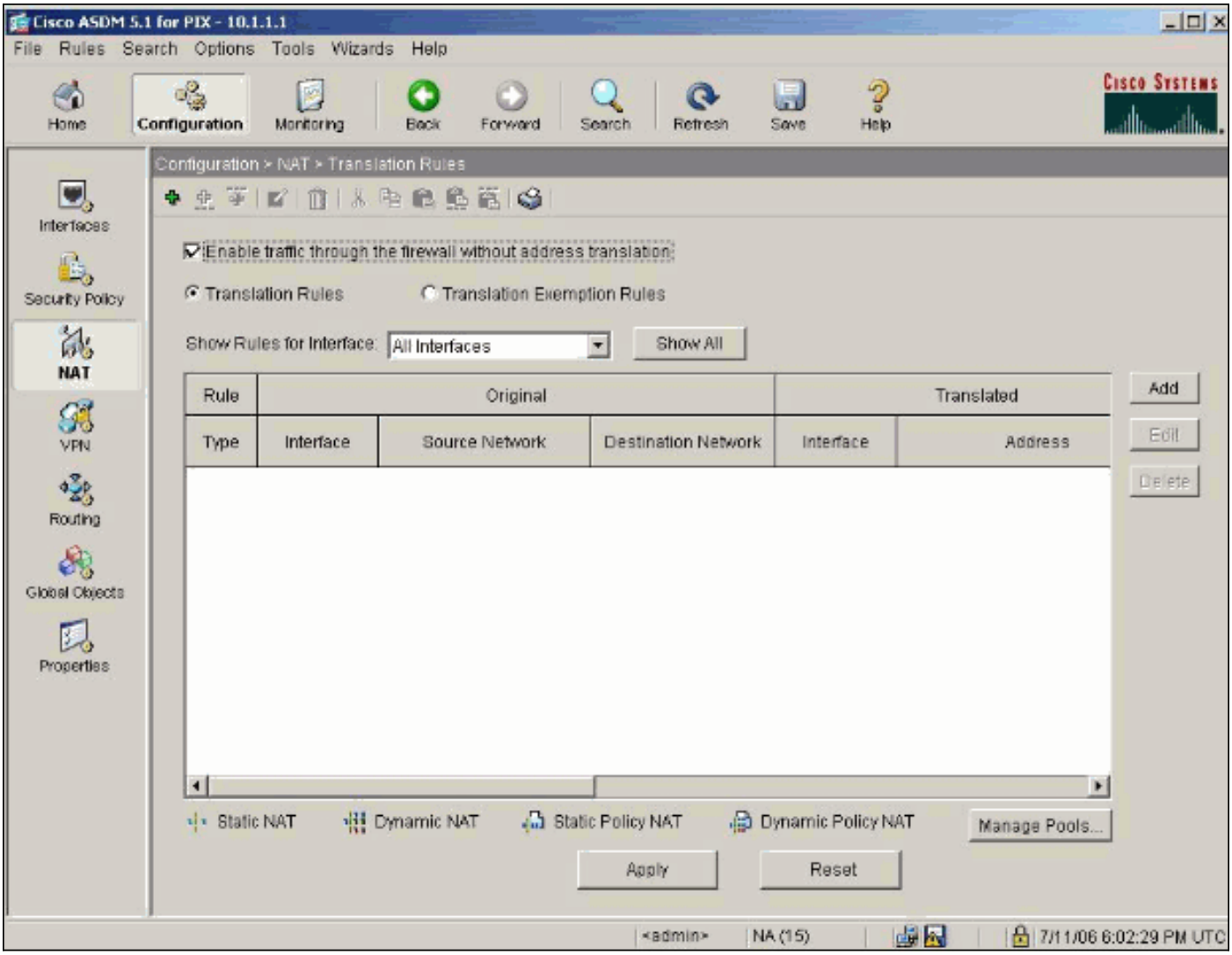
```
pix(config)#interface ethernet 0
pix(config-if)#security-level 0
pix(config-if)#nameif outside
pix(config-if)#exit
```

يقدم PIX 7.0 الأمر **nat-control**. أنت يستطيع استعملت ال **nat-control** أمر في تشكيل أسلوب in order to عينت إن NAT يكون يتطلب ل إتصالات خارجية. مع تمكين التحكم ب NAT، يلزم تكوين قواعد NAT للسماح بحركة المرور الصادرة، كما هو الحال مع الإصدارات السابقة من برنامج PIX. إذا كان التحكم في NAT معطلا (**لا nat-control**)، فيمكن للمضيفين الداخليين الاتصال بالشبكات الخارجية دون تكوين قاعدة NAT. مهما، إن يتلقى أنت داخل مضيف أن لا يتلقى عنوان عام، أنت بعد تحتاج أن يشكل nat ل أن مضيف.

لتكوين التحكم في NAT باستخدام ASDM، حدد علامة التبويب تكوين من نافذة ASDM الرئيسية واختر **NAT** من قائمة الميزات.

تمكين حركة المرور عبر جدار الحماية دون ترجمة: تم إدخال هذا الخيار في الإصدار 7.0(1) من PIX. عندما يكون هذا الخيار محددا، لا يتم إصدار أمر **nat-control** في التكوين. يعني هذا الأمر أنه لا يلزم إجراء أي ترجمة للإجتياز عبر جدار الحماية. عادة ما يتم التحقق من هذا الخيار فقط عندما يكون للمضيفين الداخليين عناوين IP عامة أو أن مخطط الشبكة لا يتطلب ترجمة المضيفين الداخليين إلى أي عنوان IP.

إذا كان للمضيفين الداخليين عناوين IP خاصة، فيجب إلغاء تحديد هذا الخيار بحيث يمكن للمضيفين الداخليين أن يترجموا إلى عنوان IP عام ويدخلوا الإنترنت.



هناك إثنان سياسة أن يكون مطلوب in order to سمحت وصول خارج مع nat تحكم. الأولى هي طريقة الترجمة. هذا يستطيع كنت ترجمة ساكن إستاتيكي مع الإستعمالمن **ساكن إستاتيكي** أمر، أو ترجمة حركية مع الإستعمالمن **nat/global** قاعدة. لا يكون هذا مطلوبا إذا كان التحكم في NAT معطلا وكان لدى المضيفين الداخليين عناوين عامة.

الشرط الآخر للوصول الصادر (والذي ينطبق على ما إذا كان التحكم في الوصول إلى الشبكة (NAT) ممكنا أو معطلا)، هو إذا كانت هناك قائمة تحكم في الوصول (ACL) موجودة. إذا كانت قائمة التحكم في الوصول (ACL) موجودة، فيجب عليها السماح بوصول المضيف المصدر إلى المضيف الوجهة باستخدام البروتوكول والمنفذ المحددين. بشكل افتراضي، لا توجد قيود وصول على الاتصالات الصادرة من خلال PIX. هذا يعني أنه إذا لم توجد قائمة تحكم في الوصول (ACL) تم تكوينها لواجهة المصدر، فسيتم السماح بالاتصال الصادر بشكل افتراضي إذا كان هناك طريقة ترجمة تم تكوينها.

السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام NAT

يوفر هذا التكوين لجميع الأجهزة المضيفة على الشبكة الفرعية 24/10.1.6.0 الوصول إلى الخارج. ومن أجل تحقيق ذلك، أستخدم الأوامر **nat** و**global** كما يوضح هذا الإجراء.

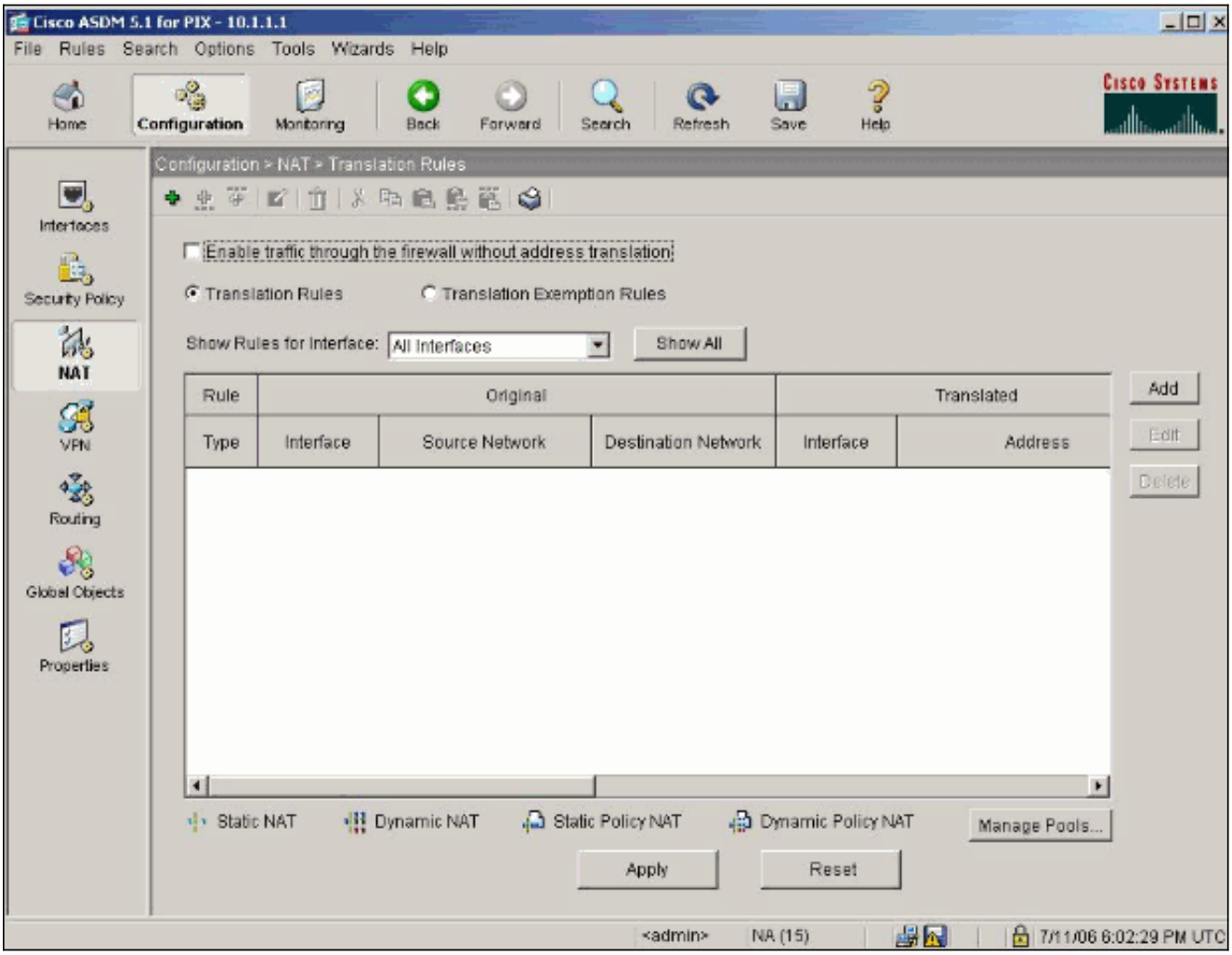
1. قم بتحديد المجموعة الداخلية التي تريد تضمينها ل NAT.

```
nat (inside) 1 10.1.6.0 255.255.255.0
```

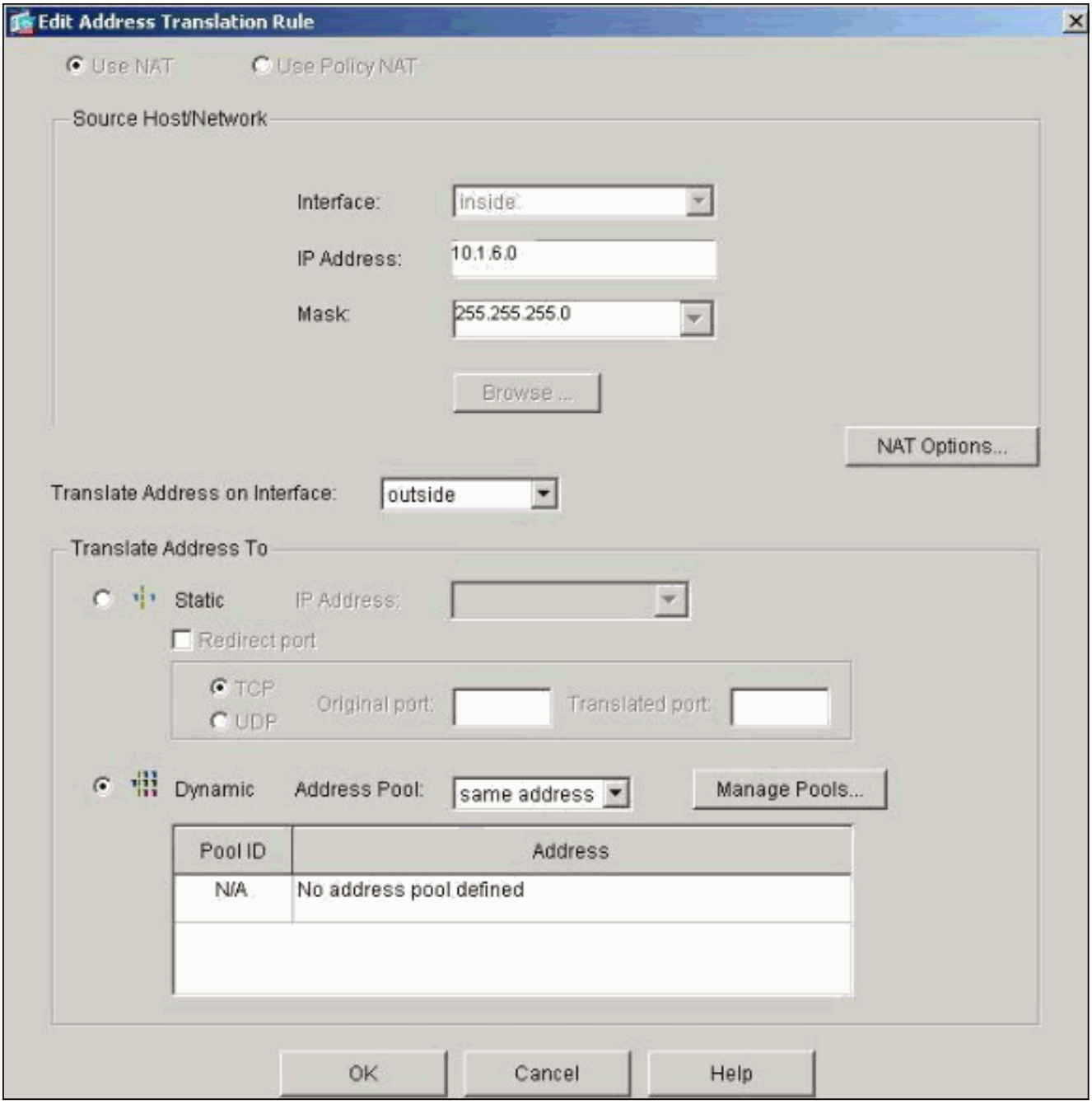
2. عينت بركة العنوان على القارن خارجي إلى أي المضيف يعين في ال nat بيان يكون ترجمت.

```
global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0
```

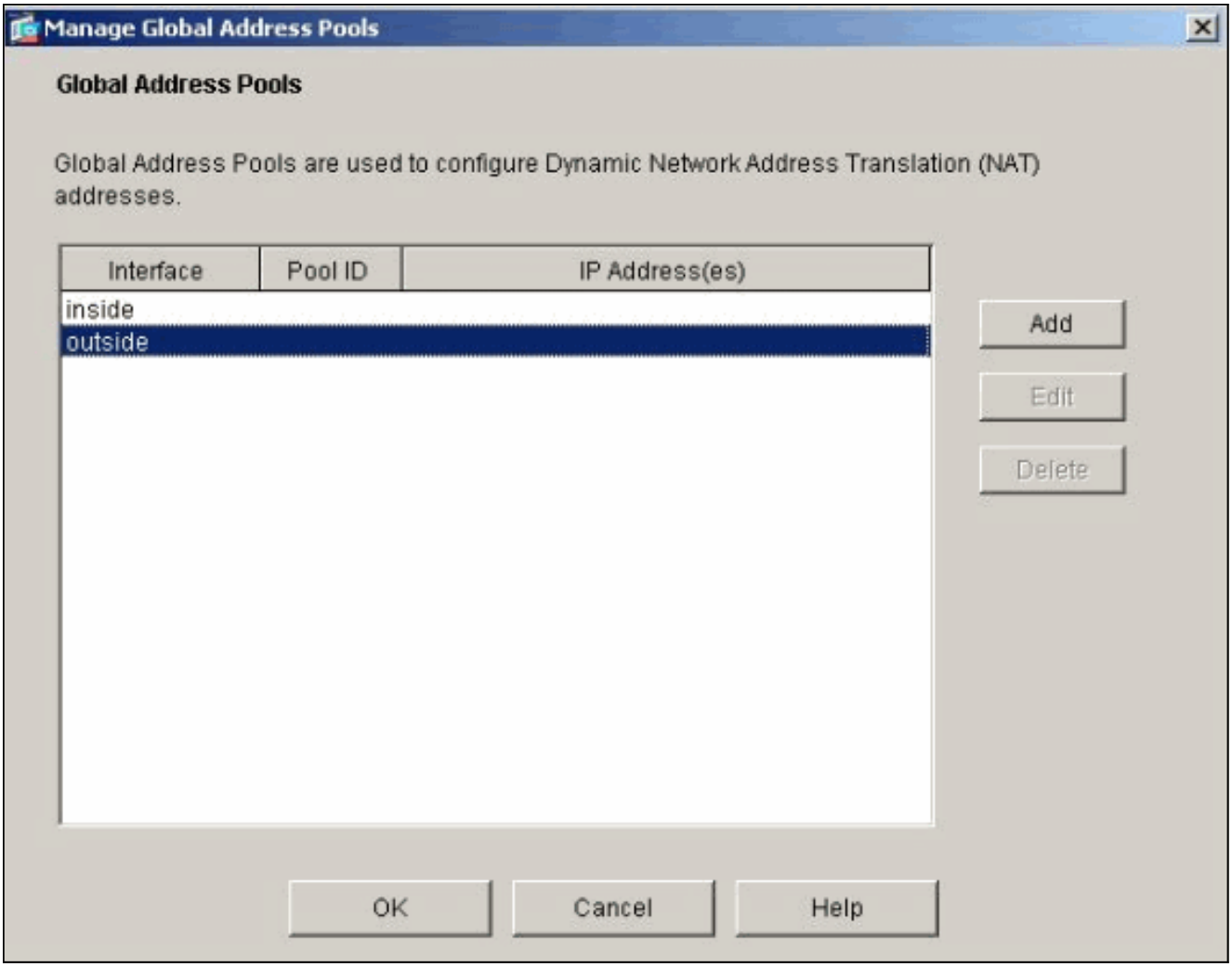
3. أستخدم ASDM من أجل إنشاء تجمع العناوين العام الخاص بك. أخترت **تشكيل>سمة>nat** وألغت **تدقيق يمكن حركة مرور خلال جدار الحماية دون عنوان ترجمة**. ثم انقر فوق **إضافة** لتكوين قاعدة NAT.



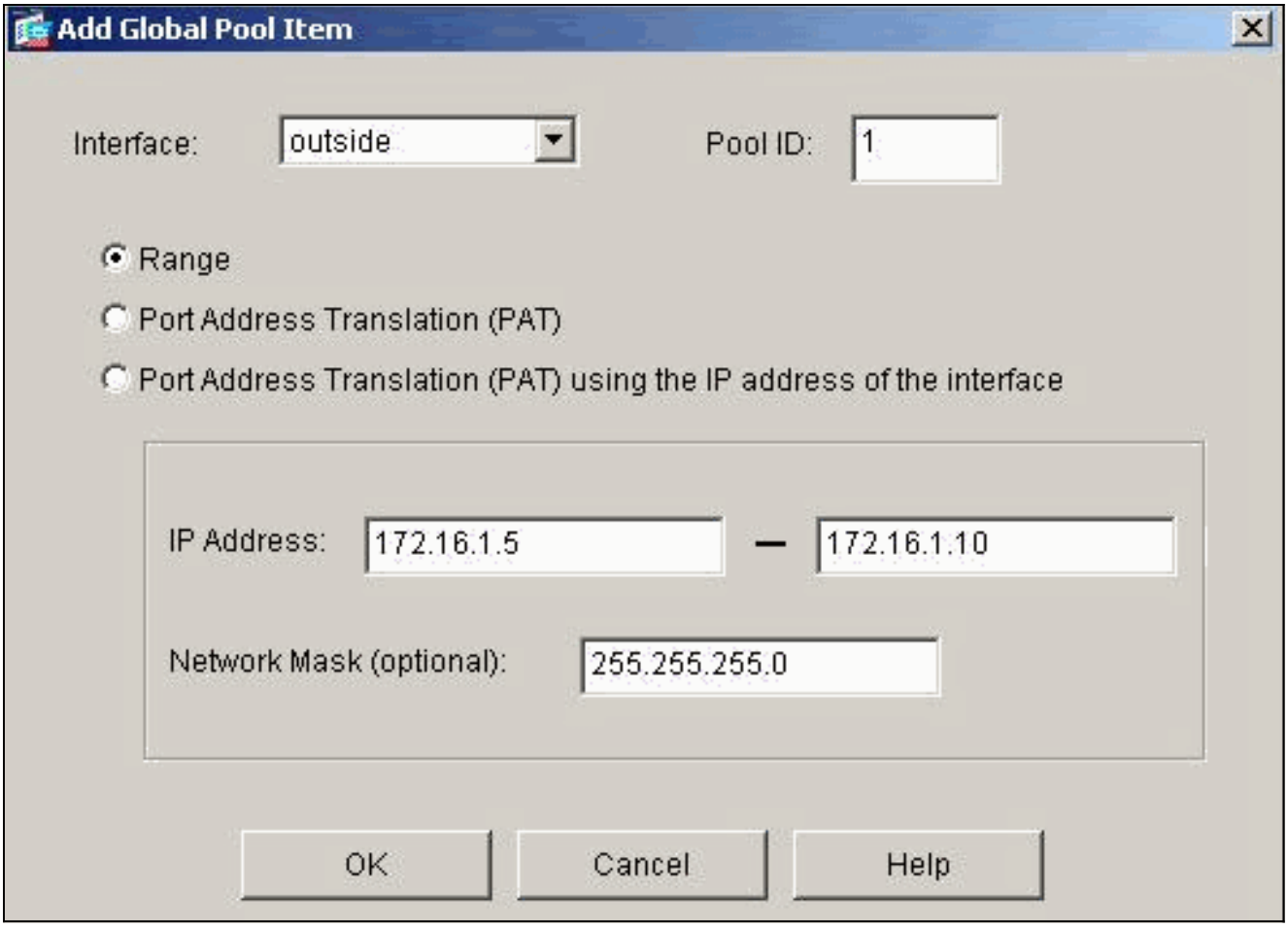
4. طقطقة **يدير بركة** in order to عينت ال nat بركة عنوان.



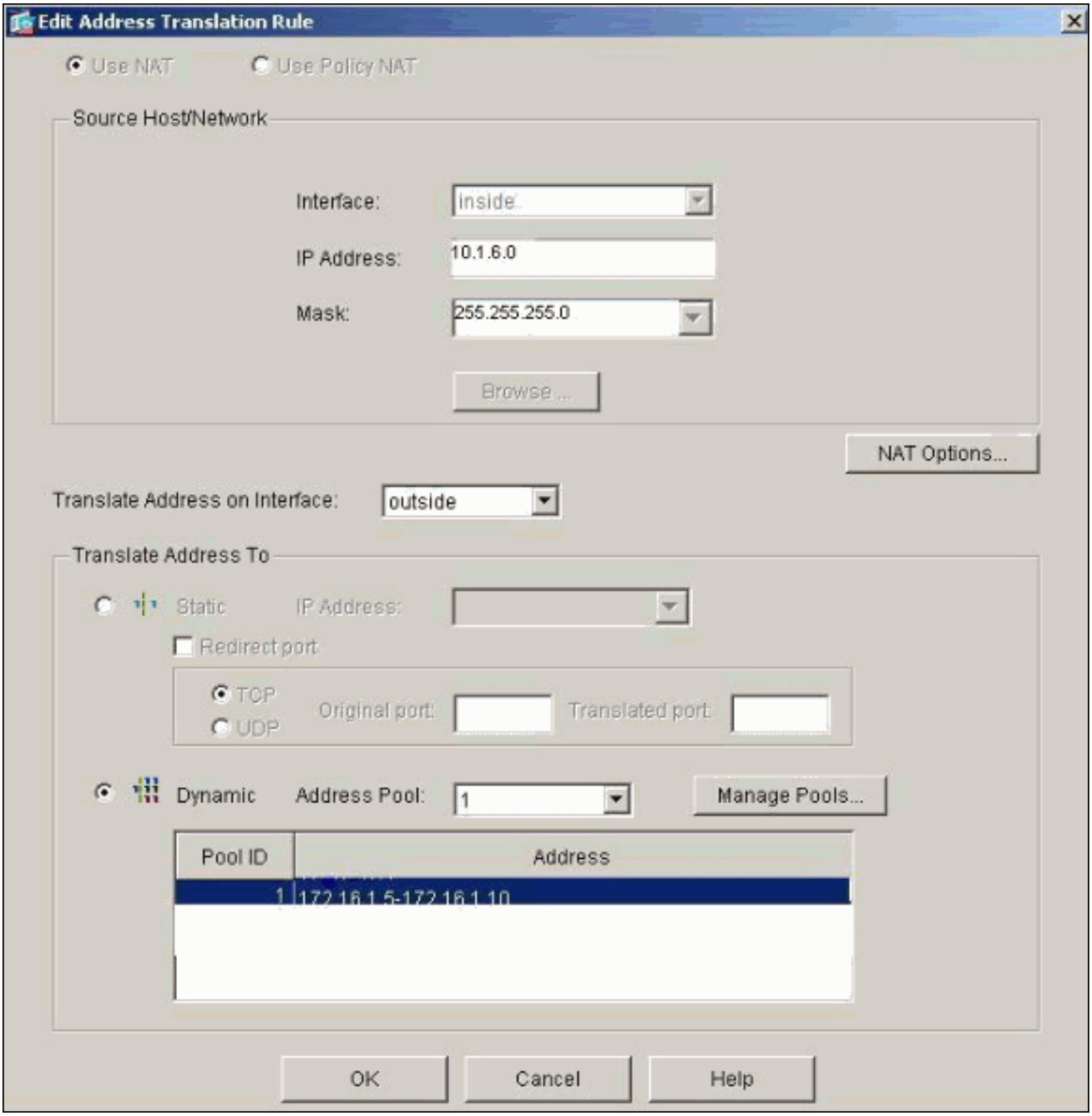
5. أختر **خارجي > إضافة**، واختر نطاق لتحديد تجمع من العناوين.



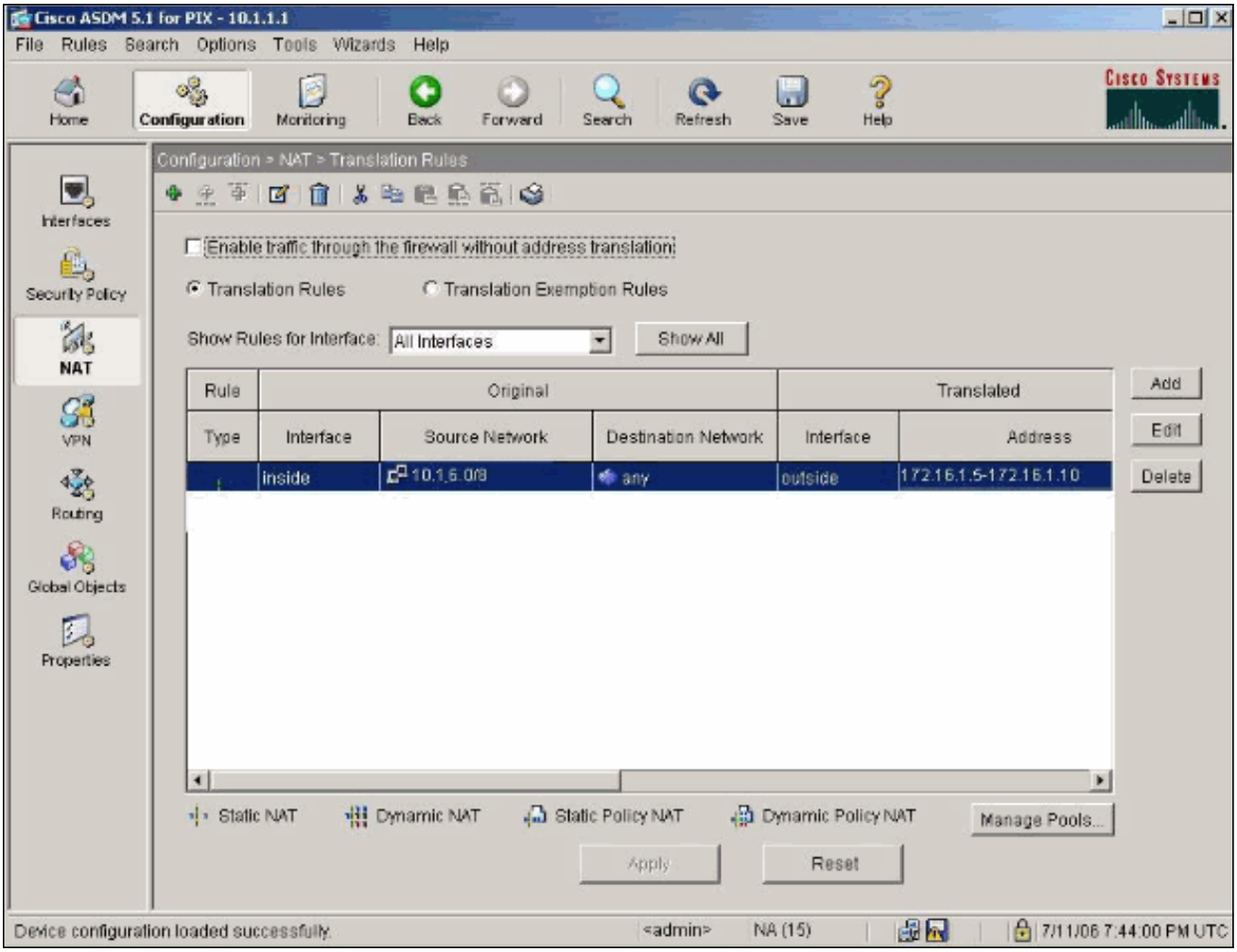
6. أدخل نطاق العناوين الخاص بك، وأدخل معرف تجمع، ثم انقر فوق **موافق**.



7. أخترت **تشكيل>سمة>nat>ترجمة قاعدة** in order to خلقت الترجمة قاعدة.
8. أخترت **داخلي** كمصدر قارن، ودخلت العنوان أنت تريد أن nat.
9. لترجمة العنوان على الواجهة، حدد **خارجي**، واختر **ديناميكي**، وحدد تجمع العناوين الذي قمت بتكوينه للتو.
10. وانقر فوق
OK.



11. يظهر الترجمة في الترجمة قاعدة في **تشكيل > سمة > nat > ترجمة قاعدة**.



يمكن للمضيفين الموجودين في الداخل الوصول إلى الشبكات الخارجية الآن. عندما يبدأ المضيفون من الداخل توصيل إلى الخارج، فإنهم يترجمون إلى عنوان من التجمع العالمي. يتم تعيين العناوين من التجمع العالمي على أساس الأولوية التي تأتي أولا وتترجم، وتبدأ بأدنى عنوان في التجمع. على سبيل المثال، إذا كان المضيف 10.1.6.25 هو أول المضيف الذي يبدأ اتصالا بالخارج، فإنه يستلم العنوان 172.16.1.5. المضيف التالي يستلم 172.16.1.6، وهكذا. هذه ليست ترجمة ثابتة، وتنتهي أزمنة الترجمة بعد فترة من عدم النشاط كما هو محدد بواسطة الأمر **timeout xlate hh:mm:ss**. إن يكون هناك كثير داخل مضيف من هناك عنوان في البركة، العنوان نهائي في البركة استعملت لترجمة عنوان أيسر (ضرب).

السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام ضرب

إن يريد أنت داخل مضيف أن يشارك عنوان عام وحيد للترجمة، استعملت ضرب. إن يعين **العبارة شامل** واحد عنوان، أن عنوان يكون أيسر ترجمت. يسمح ال PIX بترجمة منفذ واحد لكل واجهة وأن الترجمة تدعم ما يصل إلى 65.535 كائن نشط إلى العنوان العمومي الواحد. أتمت هذا steps in order to سمحت داخلي مضيف منفذ إلى شبكة خارجي مع الإستعمالمن ضرب.

1. قم بتحديد المجموعة الداخلية التي تريد تضمينها في عملية ضرب (عندما تستخدم 0 0، فإنك تحدد كل البيئات المضيفة الداخلية.)

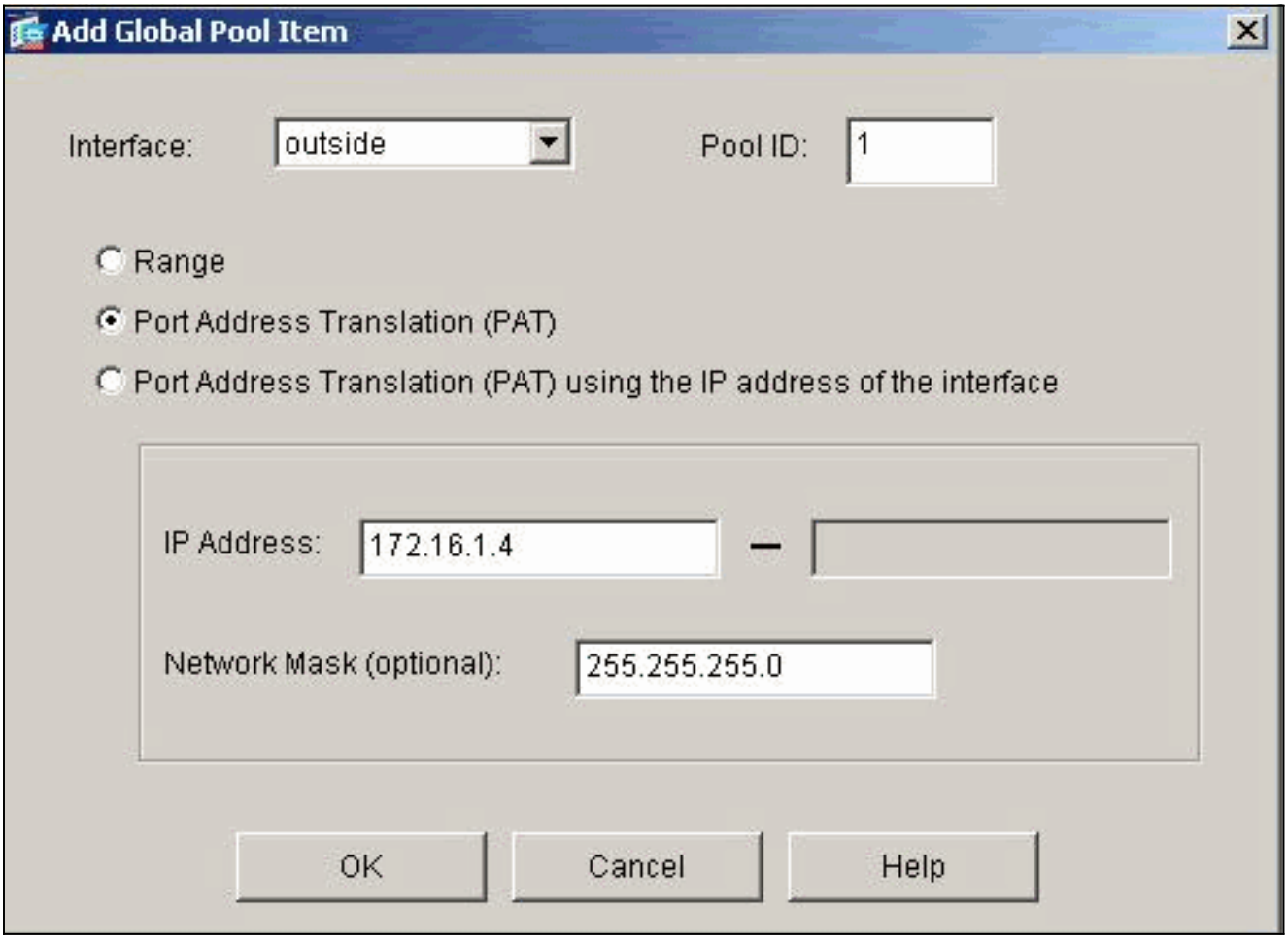
```
nat (inside) 1 10.1.6.0 255.255.255.0
```

2. حدد العنوان العمومي الذي تريد إستخدامه ل PAT. يمكن أن يكون هذا عنوان الواجهة.

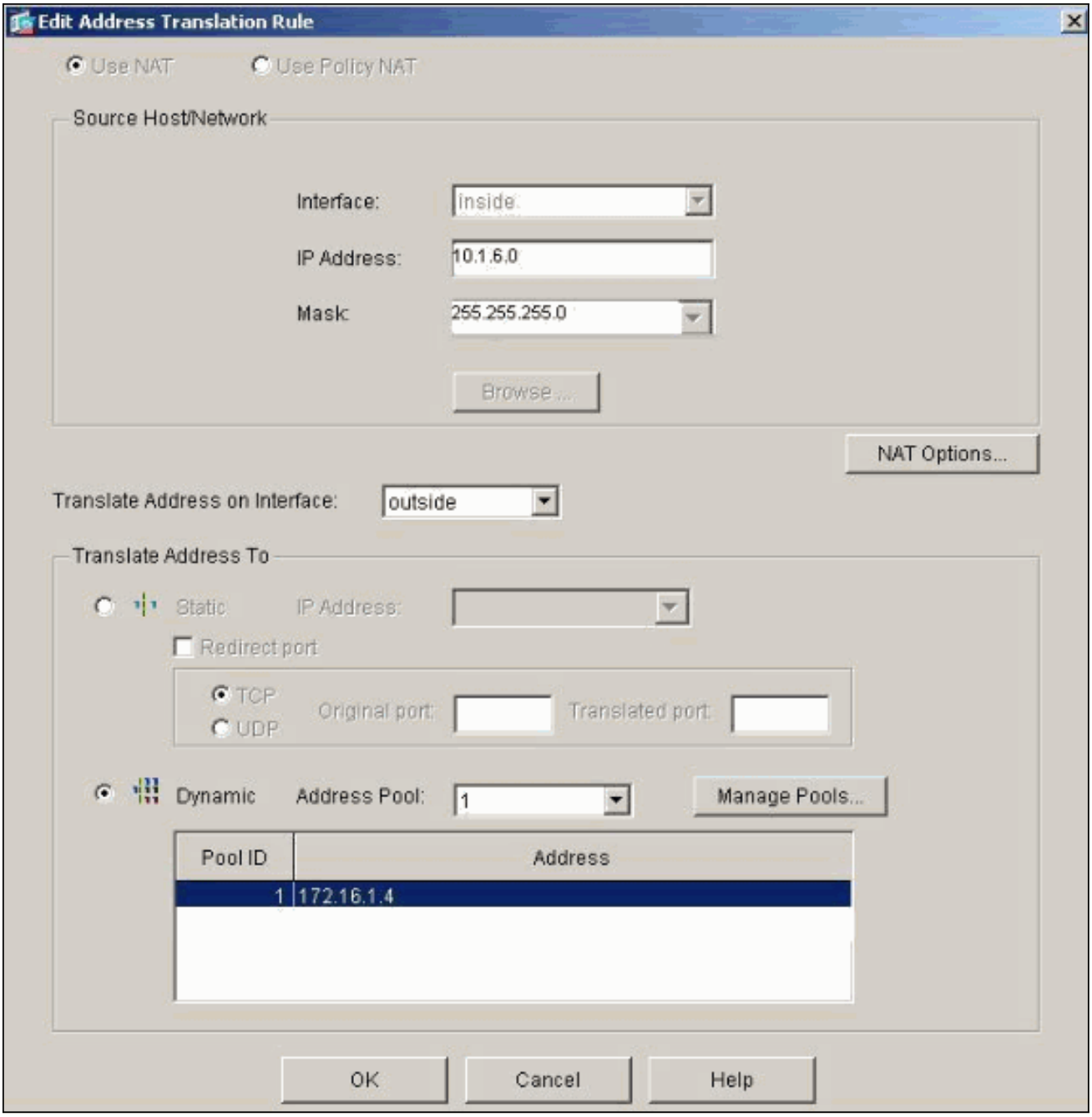
```
global (outside) 1 172.16.1.4 netmask 255.255.255.0
```

3. في ASDM، أخترت **تشكيل>سمة>nat** وألغت **تحديد يمكن حركة مرور خلال جدار الحماية دون عنوان ترجمة**.
4. طقطقة **يضيف** in order to شكلت ال nat قاعدة.
5. أخترت **يدير بركة** in order to شكلت ك ضرب عنوان.

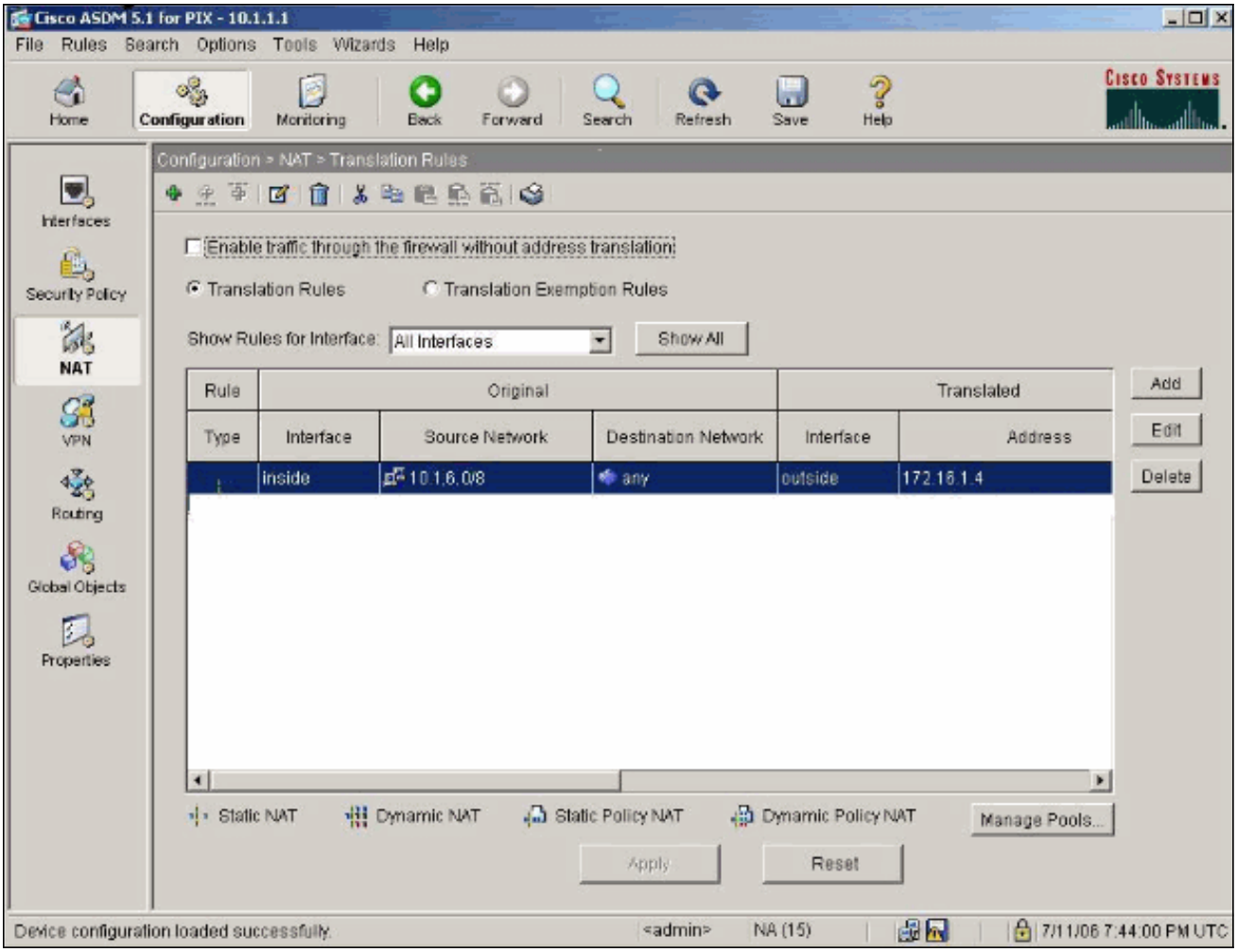
6. أخترت **خارجي>يضيف** وطقطقة **أيسر عنوان ترجمة (ضرب)** in order to شكلت عنوان وحيد لضرب.
7. دخلت عنوان، بركة id، وطقطقة
.ok



8. أخترت **تشكيل>سمة>nat>ترجمة قاعدة** in order to خلقت الترجمة قاعدة.
9. انتقيت **داخلي** كمصدر قارن، ودخلت العنوان أنت تريد أن nat.
10. لترجمة العنوان على الواجهة، حدد **خارج**، واختر **ديناميكي**، وحدد تجمع العناوين الذي قمت بتكوينه للتو. وانقر فوق
.OK



11. يظهر الترجمة في الترجمة قاعدة في **تشكيل > سمة > nat > ترجمة قاعدة**.



هناك بعض الأشياء التي يجب أخذها بعين الإعتبار عند إستخدام عملية ضرب.

- لا يمكن أن تكون عناوين IP التي تحددها ل PAT في تجمع عناوين عمومي آخر.
- لا تعمل PAT مع تطبيقات H.323، خوادم أسماء التخزين المؤقت، وبروتوكول الاتصال النفقي من نقطة إلى نقطة (PPTP). تعمل PAT مع خدمة اسم المجال (DNS)، و FTP و FTP السلبي، و HTTP، والبريد، واستدعاء الإجراء البعيد (RPC)، و rshell، و telnet، وتصفية عنوان URL، و traceroute الصادر.
- لا تستخدم ضرب عندما تحتاج أن يركض تطبيق وسائط متعددة من خلال جدار الحماية. قد تتعارض تطبيقات الوسائط المتعددة مع تعيينات المنافذ التي توفرها تقنية PAT.
- في برنامج PIX الإصدار 4.2(2)، لا تعمل ميزة PAT مع حزم بيانات IP التي تصل بالترتيب العكسي. يعمل برنامج PIX الإصدار 4.2(3) على تصحيح هذه المشكلة.
- تتطلب عناوين IP في تجمع العناوين العامة المحددة باستخدام الأمر **العام** إدخالات DNS عكسية لضمان إمكانية الوصول إلى جميع عناوين الشبكة الخارجية من خلال PIX. لإنشاء تعيينات DNS عكسية، أستخدم سجل مؤشر DNS (PTR) في ملف تعيين عنوان إلى اسم لكل عنوان عام. بدون إدخالات PTR، يمكن أن تواجه المواقع إمكانية اتصال بطيئة أو متقطعة بالإنترنت، كما تتعطل طلبات FTP باستمرار.على سبيل المثال، إذا كان عنوان IP العمومي هو 192.168.1.3 واسم المجال لجهاز أمان PIX هو pix.caguana.com، فإن سجل PTR هو:

```
in-addr.arpa. IN PTR.3.1.1.175
                pix3.caguana.com
in-addr.arpa. IN PTR.4.1.1.175
                .pix4.caguana.com & so on
```

تقييد الوصول إلى الشبكات الخارجية للمضيفين الداخليين

إذا كان هناك أسلوب ترجمة صالح معرف للمضيف المصدر، ولم يتم تحديد قائمة تحكم في الوصول (ACL) لواجهة PIX المصدر، فسيتم السماح بالاتصال الصادر بشكل افتراضي. ومع ذلك، في بعض الحالات، من الضروري تقييد الوصول الصادر استنادا إلى المصدر و/أو الوجهة و/أو البروتوكول و/أو المنفذ. ومن أجل تحقيق ذلك، قم بتكوين قائمة تحكم في الوصول باستخدام الأمر **access-list** وتطبيقها على واجهة PIX لمصدر الاتصال باستخدام الأمر **access-**

group. يمكنك تطبيق قوائم التحكم في الوصول (ACL) الخاصة ببروتوكول PIX 7.0 في كلا الاتجاهين الوارد والصادر. هذا الإجراء هو مثال على السماح بوصول HTTP الصادر لشبكة فرعية واحدة، ولكنه يرفض جميع الأجهزة المضيفة الأخرى وصول HTTP إلى الخارج، مع السماح لجميع حركة مرور IP الأخرى للجميع.

1. تحديد قائمة التحكم في الوصول (ACL).

```
access-list acl_outbound permit tcp 10.1.6.0 255.255.255.0 any eq www
access-list acl_outbound deny tcp any any eq www
access-list acl_outbound permit ip any any
```

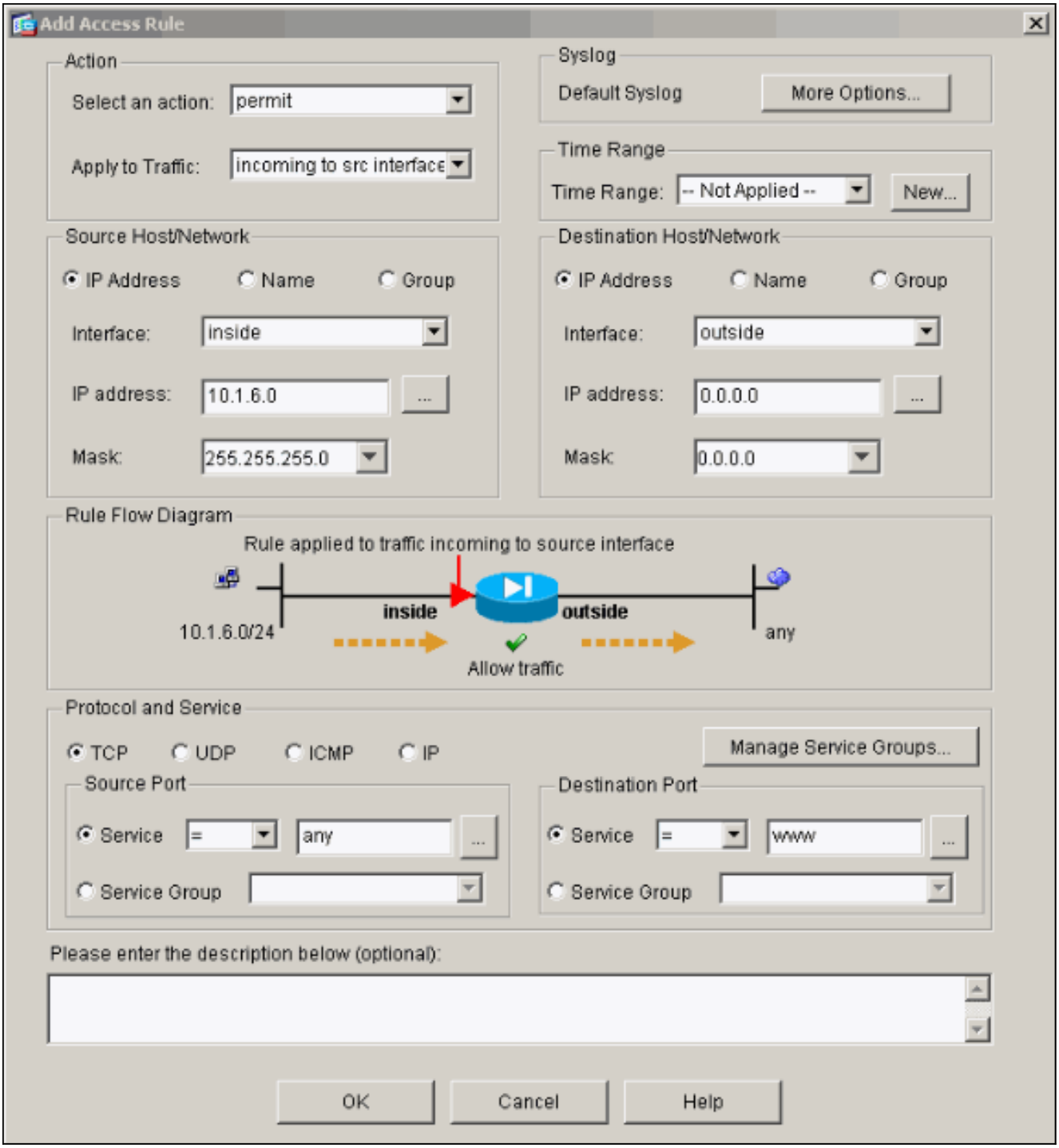
ملاحظة: تختلف قوائم التحكم في الوصول (ACL) للبنية الأساسية (PIX) عن قوائم التحكم في الوصول (ACL) على موجهات Cisco IOS® في أن لا يستخدم PIX قناع حرف بدل مثل Cisco IOS. إنه يستخدم قناع شبكة فرعية عادي في تعريف قائمة التحكم في الوصول (ACL). كما هو الحال مع موجهات Cisco IOS، تحتوي قائمة التحكم في الوصول (ACL) ل PIX على "رفض الكل" ضمني في نهاية قائمة التحكم في الوصول (ACL).**ملاحظة:** سيتم إلحاق إدخالات قائمة الوصول الجديدة بنهاية إدخالات التحكم في الوصول (ACEs) الموجودة. إذا كنت بحاجة إلى إدخال تحكم في الوصول (ACE) محدد تمت معالجته أولا، فيمكنك إستخدام الكلمة الأساسية في قائمة الوصول. هذا مثال على ملخص الأوامر:

```
access-list acl_outbound line 1 extended permit tcp host 10.1.10.225 any
```

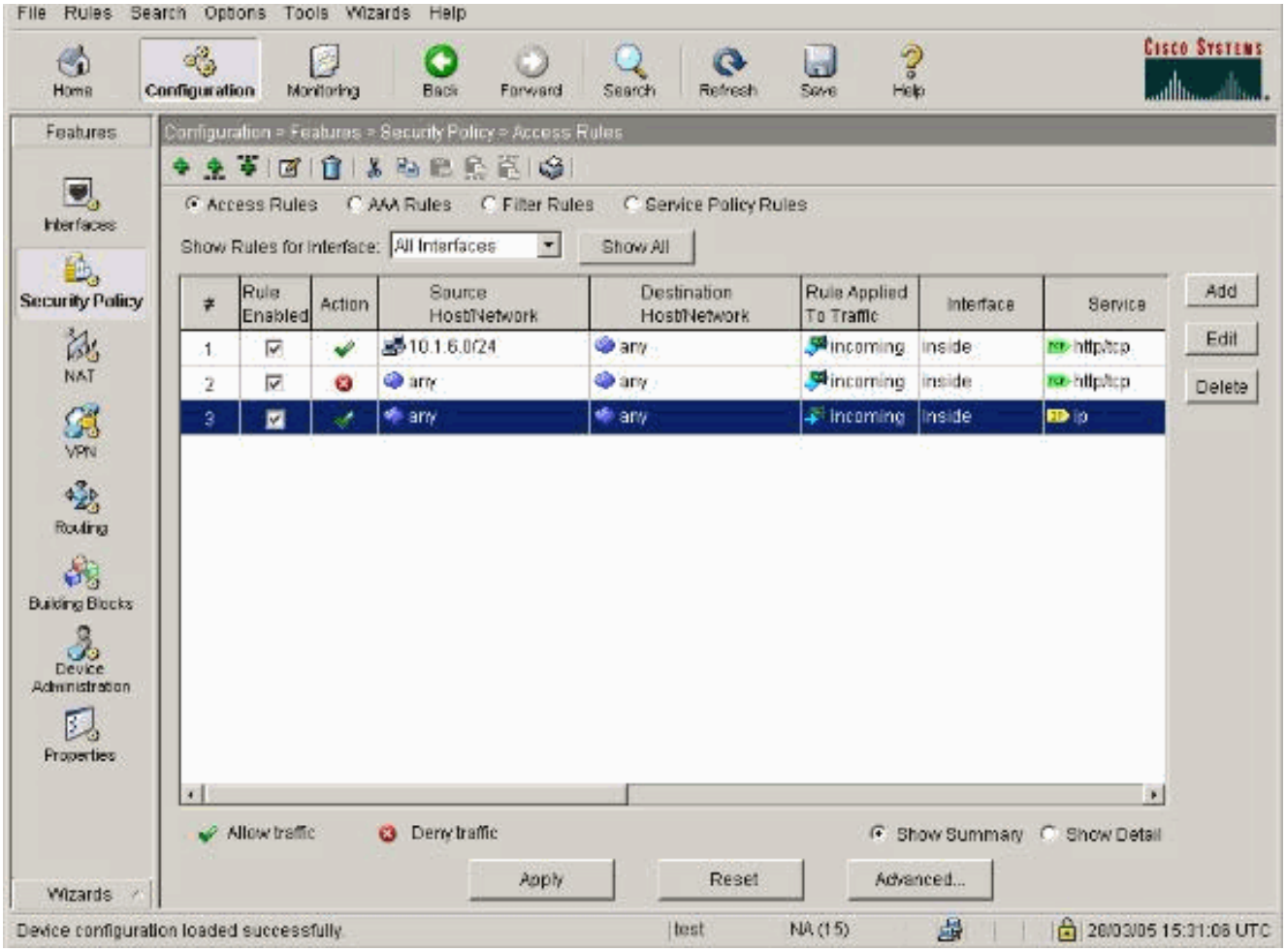
2. تطبيق قائمة التحكم في الوصول (ACL) على الواجهة الداخلية.

```
access-group acl_outbound in interface inside
```

3. أستخدم ASDM لتكوين إدخال قائمة الوصول الأول في الخطوة 1 للسماح لحركة مرور HTTP من 24/10.1.6.0. أختر **التكوين > الميزات > سياسة الأمان > قواعد الوصول**.
4. طقطقة **يضيف**، دخلت المعلومة كما يبدي هذا نافذة، وطقطقة **ok**.



5. بمجرد إدخال إدخالات قائمة الوصول الثلاثة، أختر **تكوين > ميزة > سياسة الأمان > قواعد الوصول** لعرض هذه القواعد.



السماح للمضيفين غير الموثوق بهم بالوصول إلى الأجهزة المضيفة على شبكتك الموثوق بها

تحتاج معظم المؤسسات إلى السماح للمضيفين غير الموثوق بهم بالوصول إلى الموارد الموجودة في شبكتهم الموثوق بها. المثال الشائع هو خادم ويب داخلي. بشكل افتراضي، يرفض PIX الاتصالات من البيئات المضيفة الخارجية إلى البيئات المضيفة الداخلية. in order to سمحت هذا توصيل في nat تحكم أسلوب، استعملت **ال ساكن إستاتيكي** أمر، مع **access-list** و**access-group**. إن nat أعجزت تحكم يكون، فقط **ال access-list** و**access-group** أمر ضروري، إن ما من ترجمة أنجزت.

تطبيق قوائم التحكم في الوصول (ACL) على الواجهات باستخدام الأمر **access-group**. يربط هذا الأمر قائمة التحكم في الوصول (ACL) بالواجهة لفحص حركة المرور التي تتدفق في إتجاه معين.

على النقيض من الأوامر **nat** و**global** التي تسمح بمضيف خارجي، **ساكن إستاتيكي** يخلق أمر ترجمة ثنائية الإتجاه التي تسمح لمضيفين من الداخل والخارج بالدخول إذا قمت بإضافة قوائم التحكم في الوصول المناسبة/المجموعات.

في أمثلة تكوين PAT الموضحة في هذا المستند، إذا حاول مضيف خارجي الاتصال بالعنوان العام، يمكن إستخدامه من قبل آلاف البيئات المضيفة الداخلية. يقوم الأمر **الثابت** بإنشاء تخطيط من واحد إلى واحد. يحدد الأمر **access-list** نوع الاتصال المسموح به للمضيف الداخلي ويتم طلبه دائما عندما يتصل مضيف أمان أقل بمضيف أمان أعلى. يستند الأمر **access-list** إلى كل من المنفذ والبروتوكول ويمكن أن يكون متساهلا للغاية أو مقيدا للغاية بناء على ما يريد مسؤول النظام تحقيقه.

يوضح الرسم التخطيطي للشبكة في هذا المستند إستخدام هذه الأوامر لتكوين PIX للسماح لأي مضيفين غير موثوق بهم بالاتصال بخادم الويب الداخلي، والسماح للمضيف غير الموثوق به بالوصول إلى خدمة FTP على نفس الجهاز.

إستخدام قوائم التحكم في الوصول (ACL) على PIX الإصدار 7.0 والإصدارات الأحدث

أكمل الخطوات التالية لبرنامج PIX الإصدار 7.0 والإصدارات الأحدث باستخدام قوائم التحكم في الوصول (ACL).

1. إن NAT مكنت تحكم يكون، عينت عنوان ترجمة ساكن إستاتيكي لداخل ويب نادل إلى عنوان خارجي/عام.

```
static (inside, outside)  172.16.1.16 10.16.1.16
```

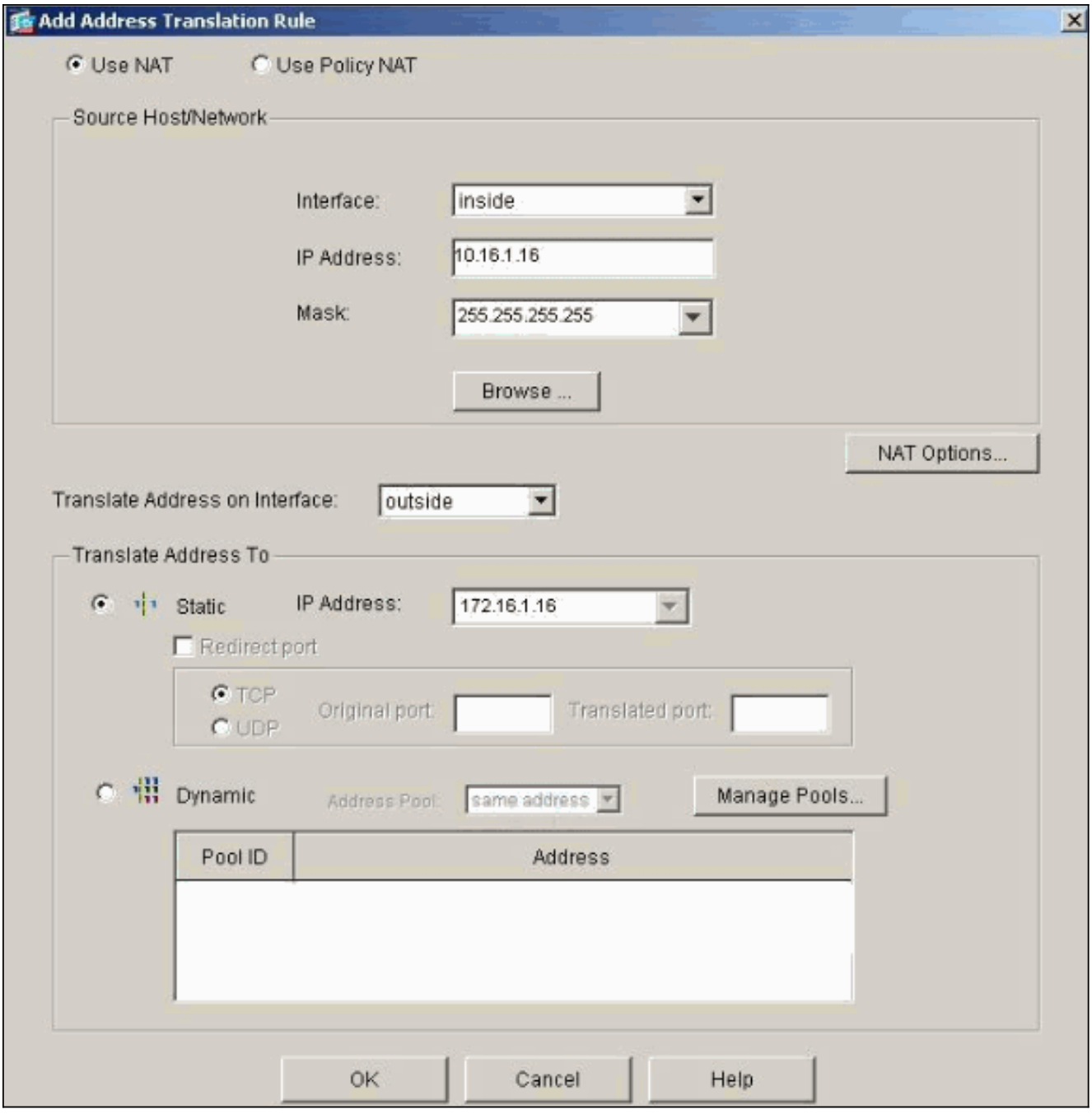
2. حدد البيئات المضيفة التي يمكنها الاتصال على أي المنافذ إلى خادم الويب/FTP لديك.

```
access-list 101 permit tcp any host  172.16.1.16 eq www
access-list 101 permit tcp host  192.168.1.1 host  172.16.1.16 eq ftp
```

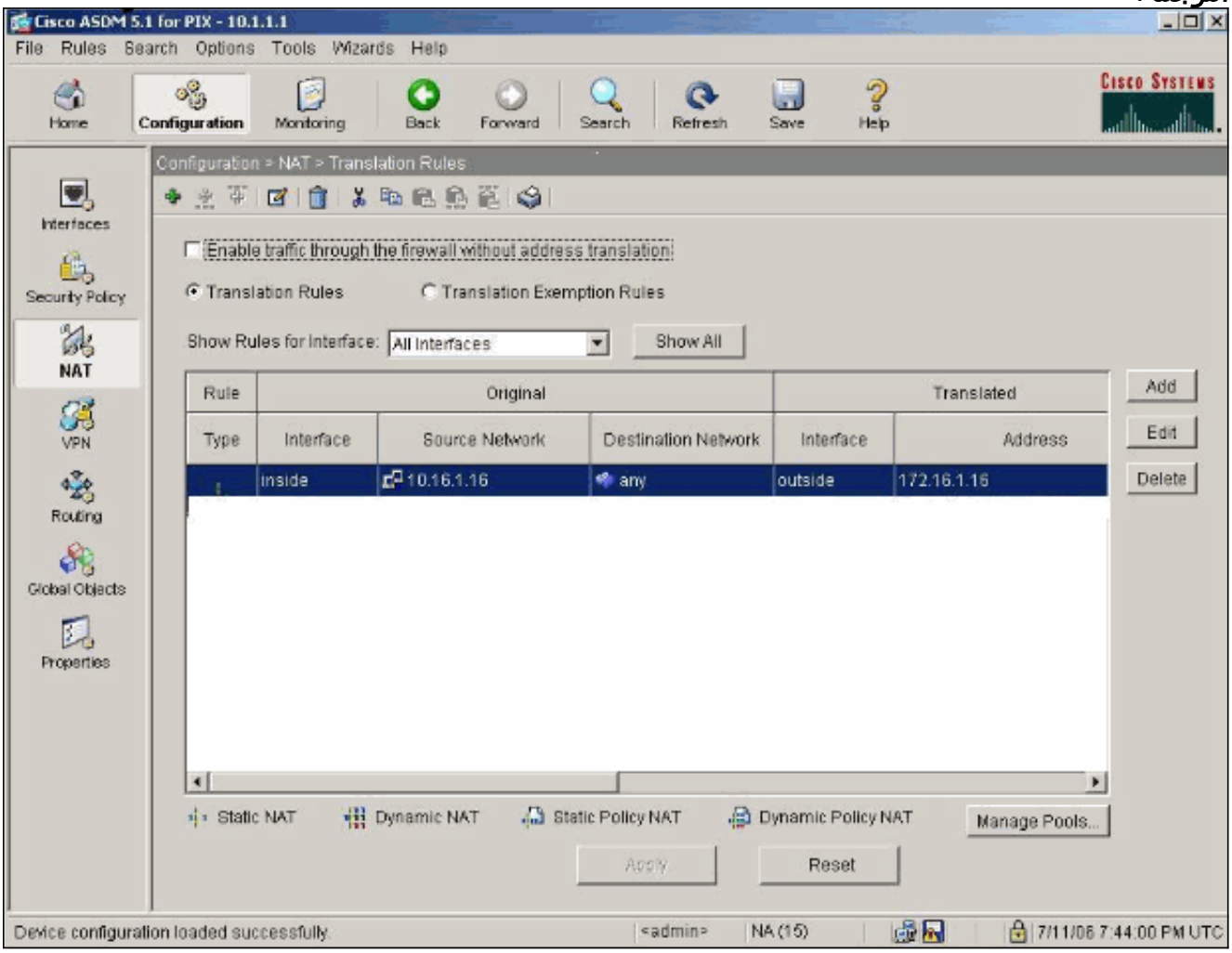
3. تطبيق قائمة التحكم في الوصول (ACL) على الواجهة الخارجية.

```
access-group 101 in interface outside
```

4. أخترت **تشكيل>سمة>nat** وطقطقة **يضيف** in order to خلقت هذا ترجمة ساكن إستاتيكي مع الإستعمالمن ASDM.
5. حدد **داخلي** كواجهة مصدر، وأدخل العنوان الداخلي الذي تريد إنشاء ترجمة ثابتة له.
6. أخترت **ساكن إستاتيكي** ودخلت العنوان خارجي أنت تريد أن يترجم إلى في العنوان مجال. وانقر فوق **OK**.



7. تظهر الترجمة في قواعد الترجمة عندما تختار **تشكيل > ميزات > nat > قواعد الترجمة**.



8. أستخدم إجراء تقييد وصول الأجهزة المضيفة الداخلية إلى الشبكات الخارجية لإدخال إدخالات **قائمة الوصول**.**ملاحظة:** كن حذرا عند تنفيذ هذه الأوامر. إذا قمت بتنفيذ الأمر **access-list 101 allowed ip any**، فيمكن لأي مضيف على الشبكة غير الموثوق بها الوصول إلى أي مضيف على الشبكة الموثوق بها باستخدام IP طالما كانت هناك ترجمة نشطة.

تعطيل NAT للمضيفين/الشبكات المحددة

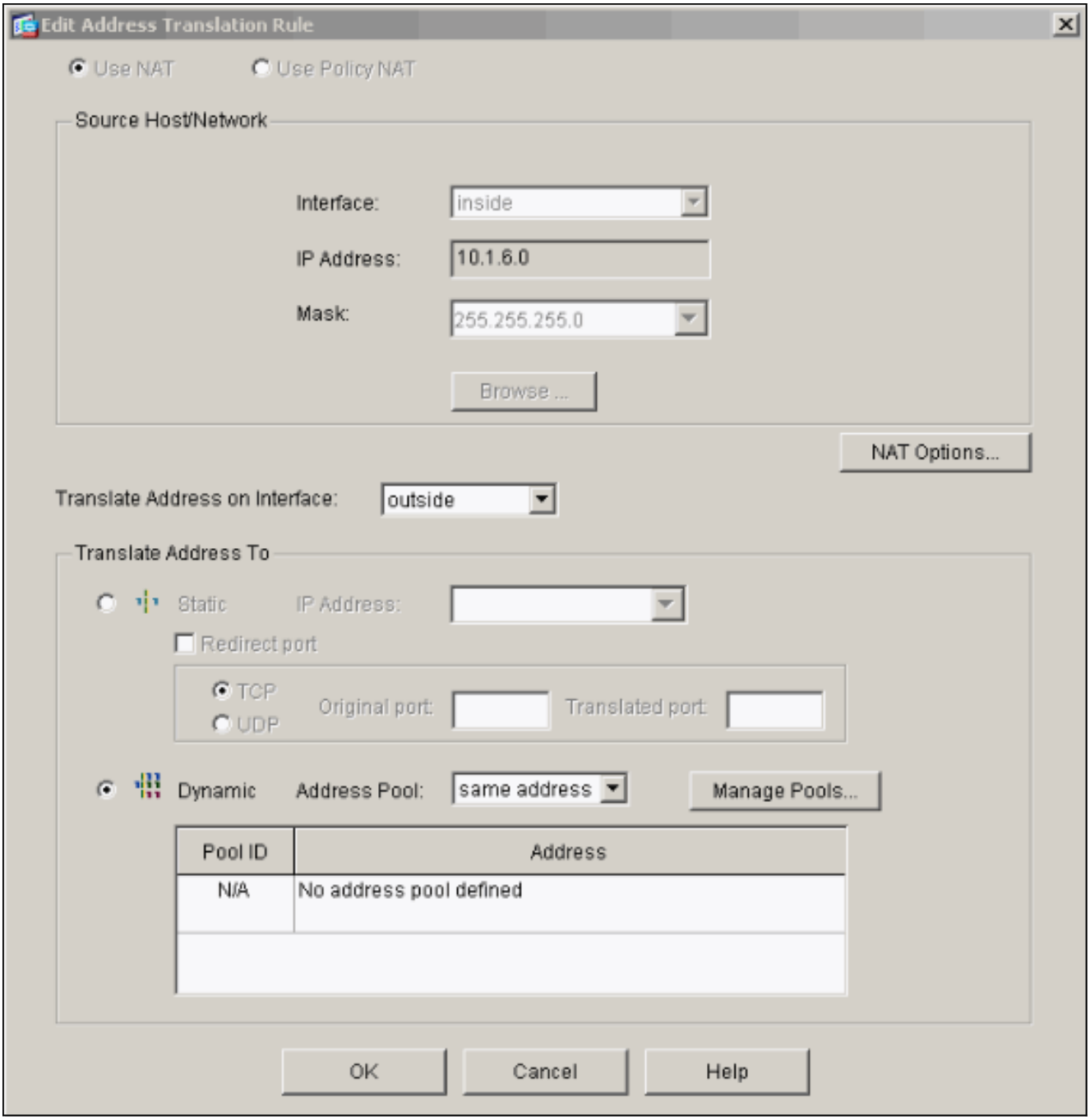
إن يستعمل أنت nat تحكم ويتلقى بعض عنوان عام على الشبكة داخلي، وأنت تريد أن هذا خاص مضيف داخلي أن يذهب إلى الخارج دون ترجمة، أنت يستطيع أعجزت NAT لتلك مضيف، مع **nat 0** أو **ساكن إستاتيكي** أمر.

هذا مثال من ال **nat** أمر:

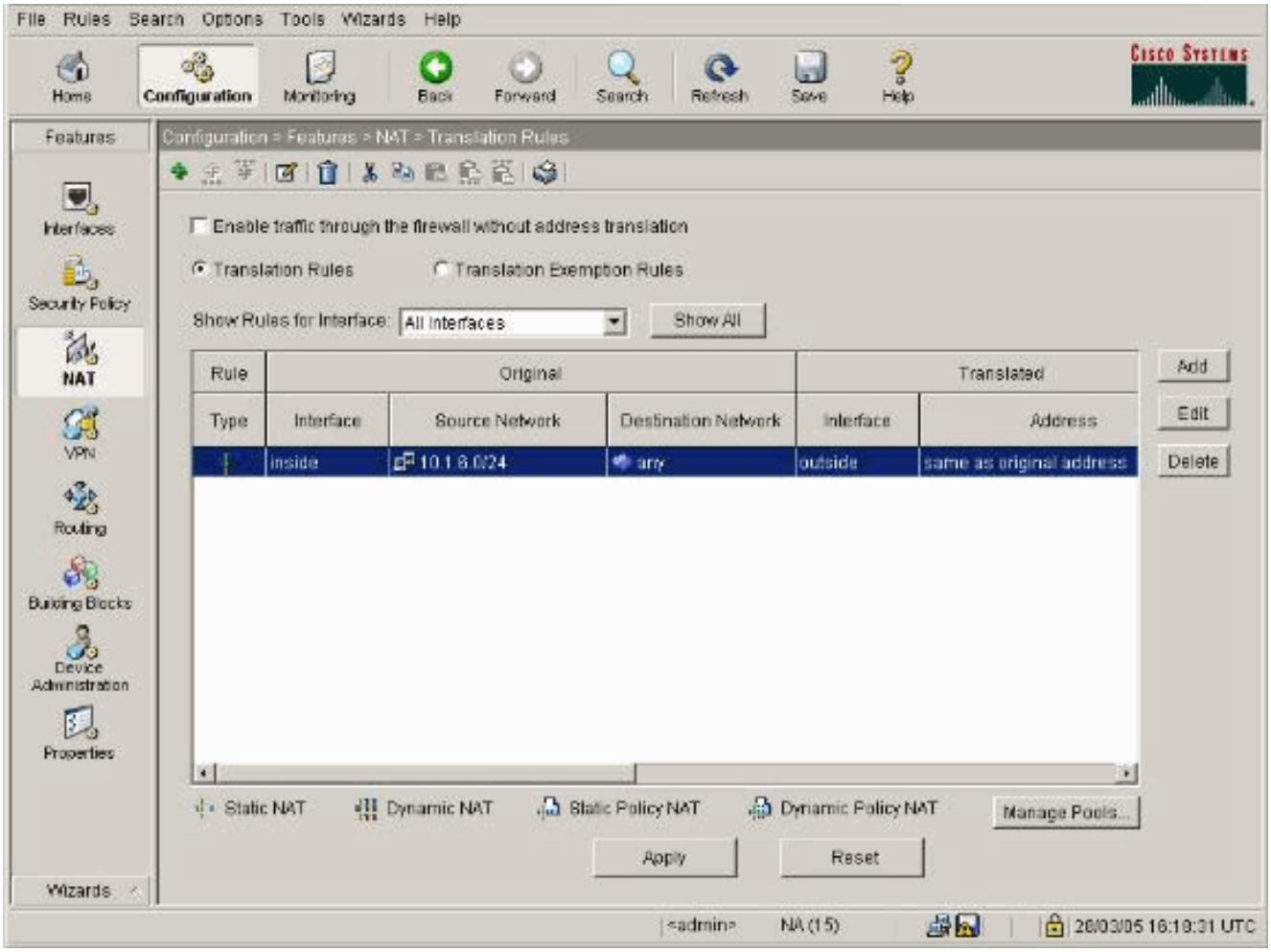
```
nat (inside) 0 10.1.6.0 255.255.255.0
```

أتمت هذا steps in order to أعجزت NAT لمضيفين/شبكات خاص مع الإستعمالمن ASDM.

1. أخترت **تشكيل > سمة>nat** وطقطقة **يضيف**.
2. أخترت **داخلي** كمصدر قارن، ودخلت العنوان داخلي/شبكة ل أي أنت تريد أن يخلق ترجمة ساكن إستاتيكي.
3. أختر **ديناميكي** وحدد نفس العنوان لتجمع العناوين. وانقر فوق **OK**.



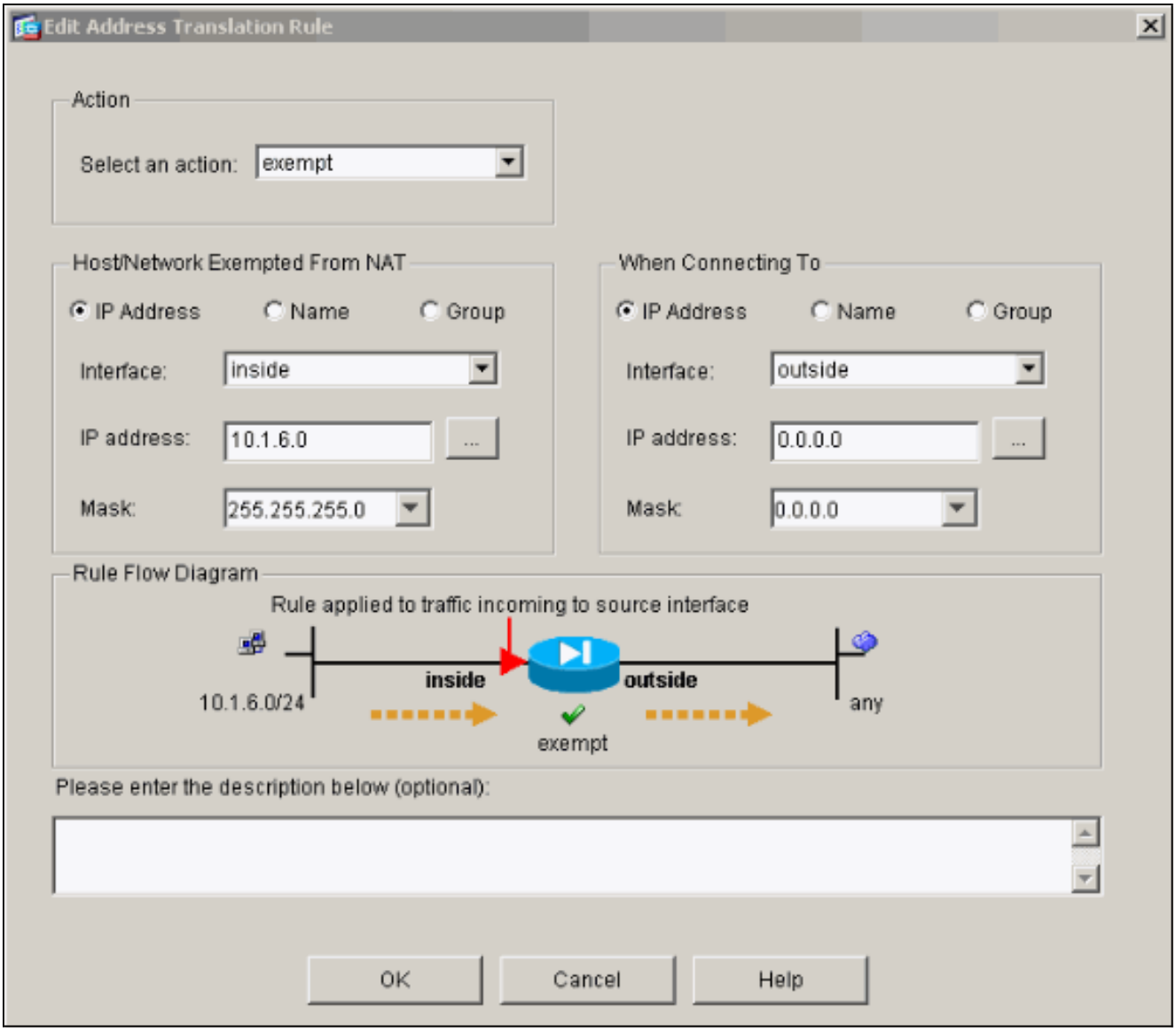
4. تظهر القاعدة الجديدة في قواعد الترجمة عندما تختار **تشكيل > ميزات > nat > قواعد الترجمة**.



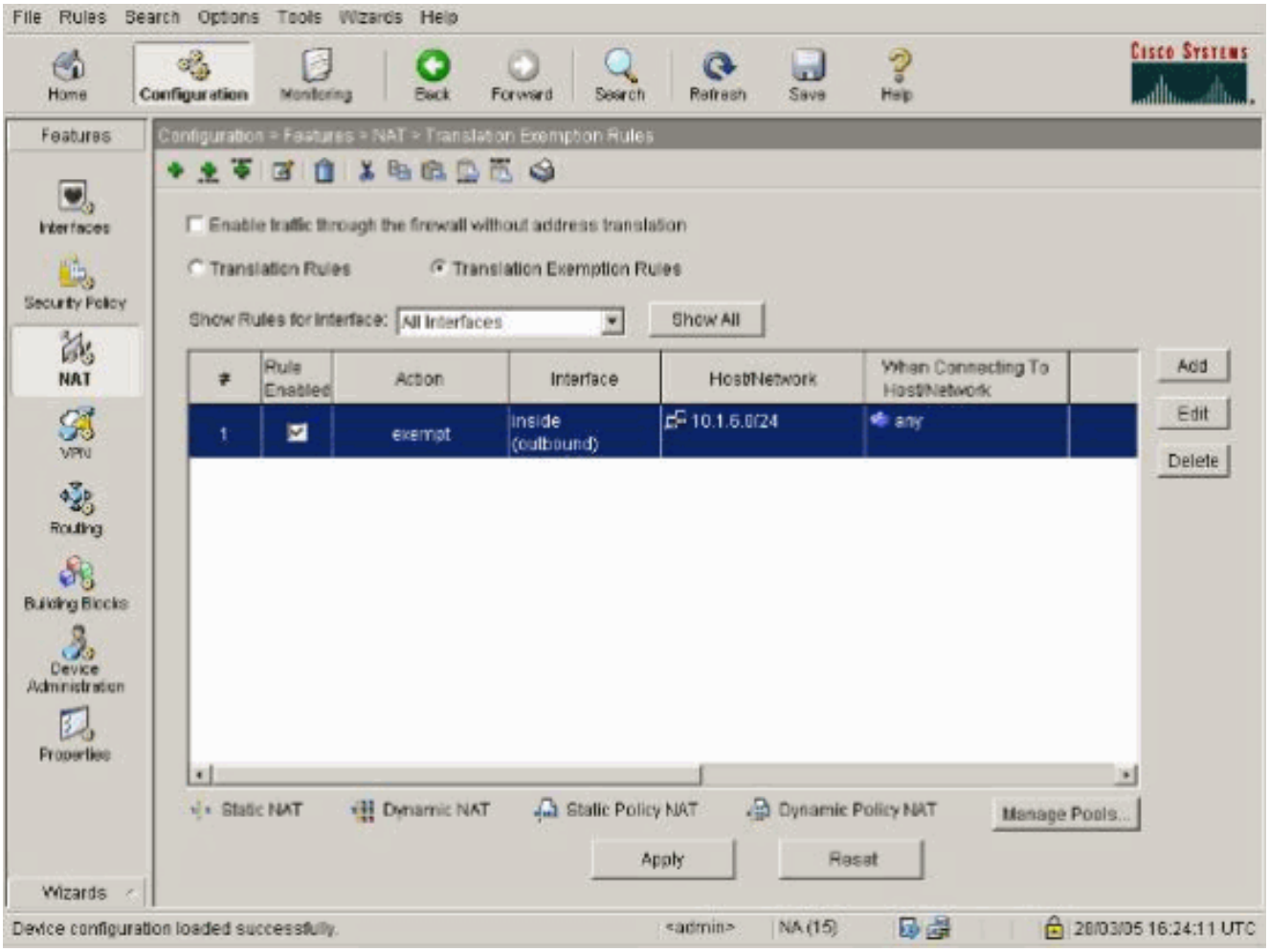
5. إذا كنت تستخدم قوائم التحكم في الوصول (ACL)، والتي تتيح تحكم أكثر دقة في حركة المرور التي يجب ألا ترجمها (استنادا إلى المصدر/الوجهة)، فاستخدم هذه الأوامر.

```
access-list 103 permit ip 10.1.6.0 255.255.255.0 any
nat (inside) 0 access-list 103
```

6. استعملت ASDM واخترت **تشكيل > سمة > nat > ترجمة قاعدة**.
7. أخترت **ترجمة إستثناء قاعدة** وطقطقة **يضيف**.يوضح هذا المثال كيفية إعفاء حركة المرور من شبكة 24/10.1.6.0 إلى أي مكان من الترجمة.



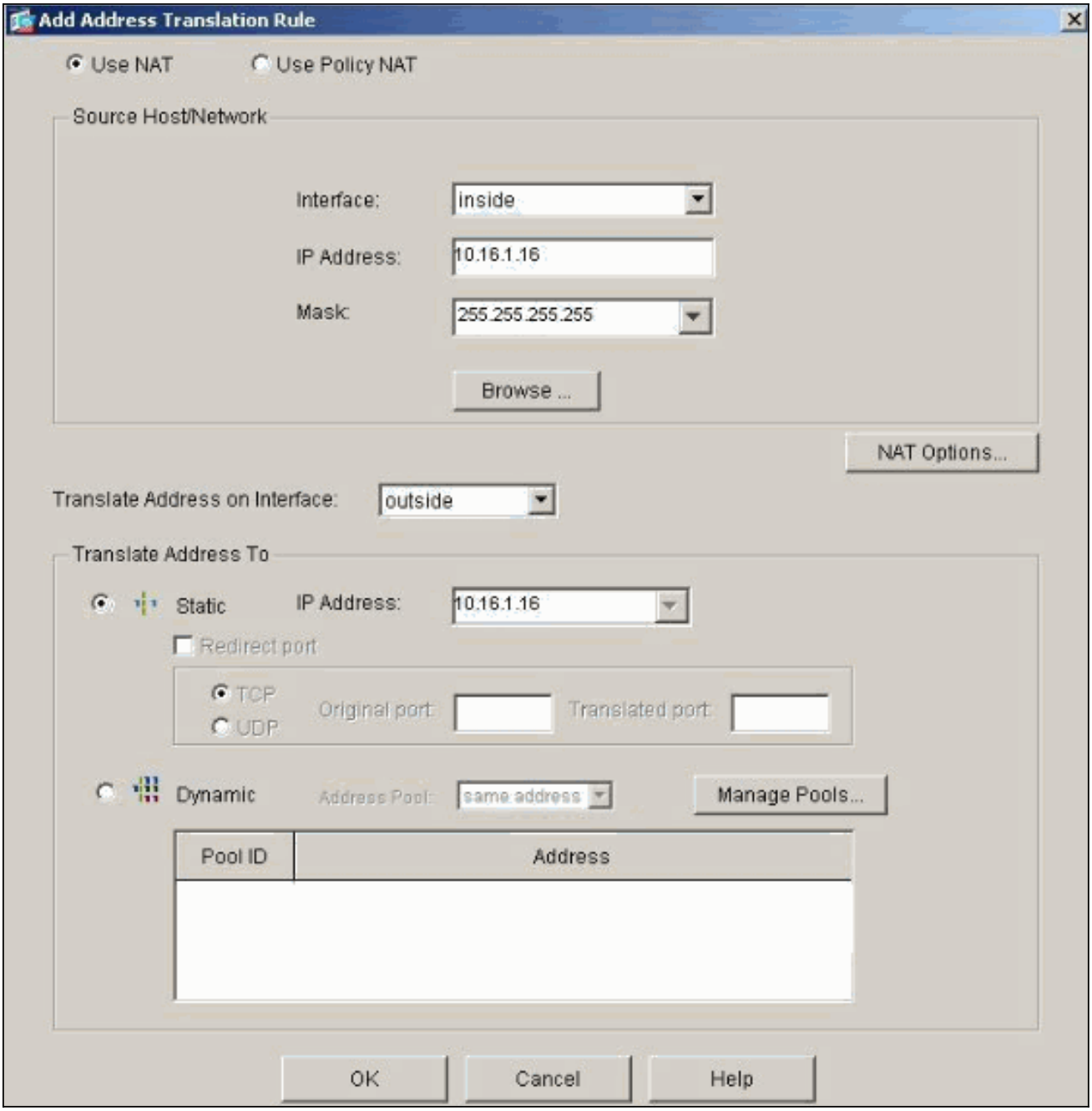
8. أخترت **تشكيل>سمة>nat>ترجمة إستثناء قاعدة** in order to عرضت القاعدة جديد.



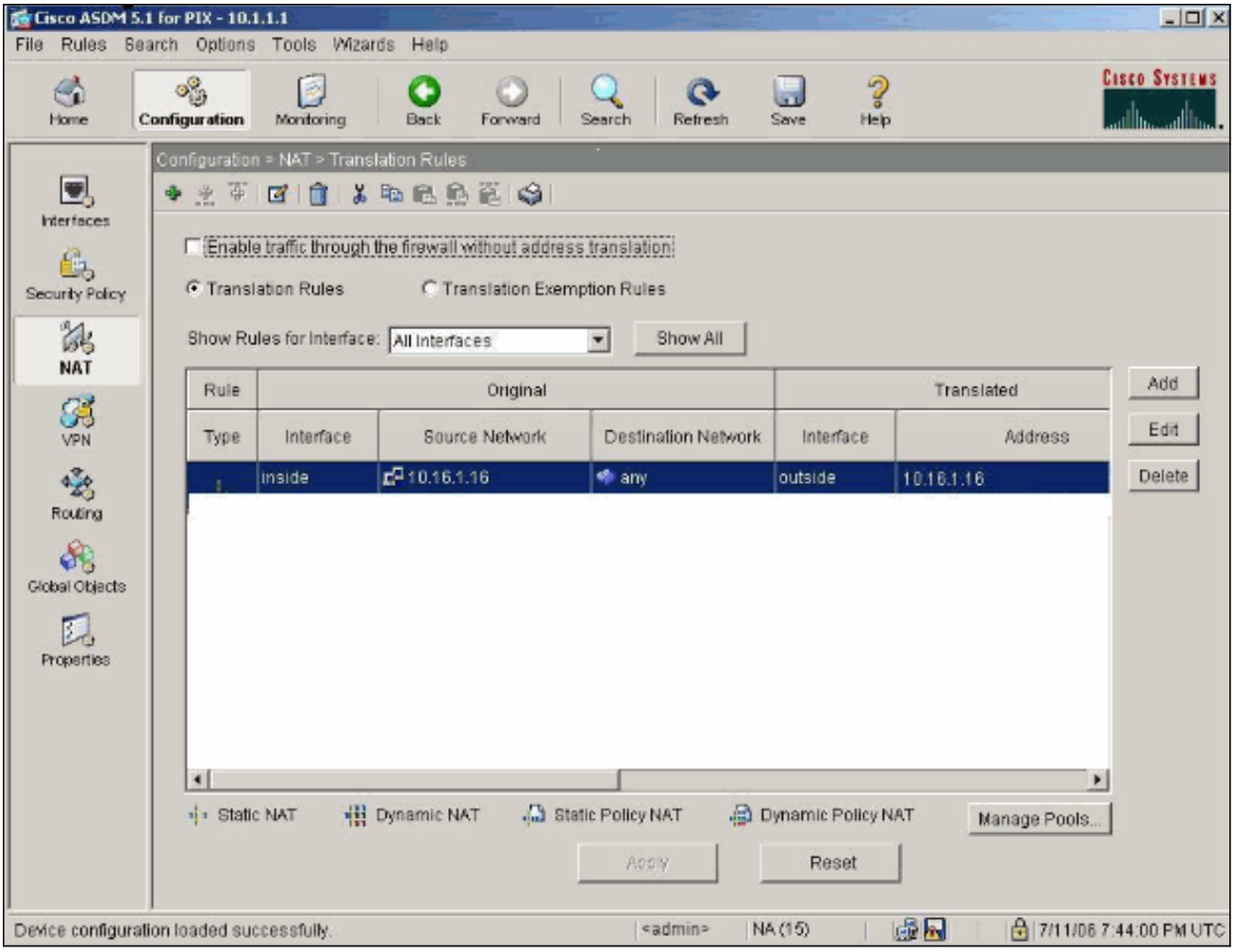
9. يتغير الأمر **الثابت** لخادم الويب كما يوضح هذا المثال.

```
static (inside, outside) 10.16.1.16 10.16.1.16
```

10. من ASDM، أختر **تشكيل > ميزات > nat > قواعد الترجمة**.
11. حدد **قواعد الترجمة** وانقر **إضافة**. أدخل معلومات عنوان المصدر، وحدد **ساكن إستاتيكي**. دخلت ال نفسه عنوان
مجال.



12. تظهر الترجمة في قواعد الترجمة عندما تختار **تشكيل > ميزات > nat > قواعد الترجمة**.



13. إذا كنت تستخدم قوائم التحكم في الوصول (ACL)، فاستخدم هذه الأوامر.

```
access-list 102 permit tcp any host 10.16.1.16 eq www
access-group 102 in interface outside
```

راجع قسم تقييد وصول الأجهزة المضيفة الداخلية إلى الشبكات الخارجية في هذا المستند للحصول على معلومات إضافية حول تكوين قوائم التحكم في الوصول (ACL) في ASDM.لاحظ الفرق بين عندما تستخدم **nat 0** عندما تحدد الشبكة/القناع في مقابل عندما تستخدم قائمة التحكم في الوصول (ACL) التي تستخدم شبكة/قناع يسمح ببدء الاتصالات من الداخل فقط. يسمح إستخدام قوائم التحكم في الوصول باستخدام **nat 0** ببدء الاتصالات بواسطة حركة المرور الواردة أو الصادرة. يجب أن تكون واجهات PIX في شبكات فرعية مختلفة لتجنب مشاكل إمكانية الوصول.

إعادة توجيه المنفذ (إعادة التوجيه) باستخدام الحالات

في PIX 6.0، تمت إضافة ميزة إعادة توجيه المنفذ (إعادة التوجيه) للسماح للمستخدمين الخارجيين بالاتصال بعنوان/منفذ IP معين والسماح ل PIX بإعادة توجيه حركة مرور البيانات إلى الخادم/المنفذ الداخلي المناسب. تم تعديل الأمر **الثابت**. ال يشارك عنوان يستطيع كنت عنوان فريد، مشترك خارج عنوان، أو يشارك مع القارن خارجي. تتوفر هذه الميزة في PIX 7. 0.

ملاحظة: نظرا لقيود المساحة، يتم عرض الأوامر على سطرين.

```
static [(internal_if_name, external_if_name)] {global_ip|interface}local_ip [netmask mask]
[[[[max_conns [emb_limit [norandomseq
```

```
static [(internal_if_name, external_if_name)] {tcp|udp} {global_ip|interface} global_port
[[[local_ip local_port [netmask mask] [max_conns [emb_limit [norandomseq
```

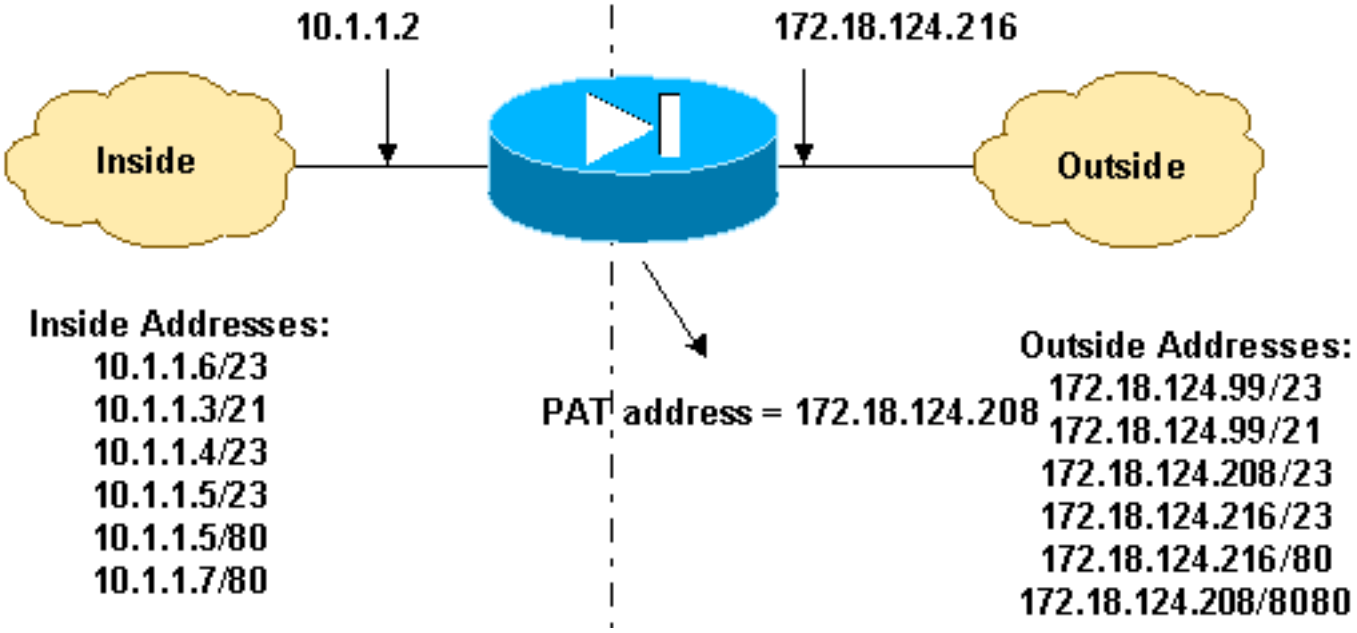
ملاحظة: إذا كان NAT الثابت يستخدم عنوان IP الخارجي (global_ip) للترجمة، فقد يؤدي ذلك إلى ترجمة. لذلك، استعملت الكلمة المفتاح **قارن** بدلا من العنوان في الترجمة ساكن إستاتيكي.

هذا أيسر redirection (برمجية) في هذا شبكة مثال:

- يقوم المستخدمون الخارجيون بتوجيه طلبات برنامج Telnet إلى عنوان IP الفريد 172.18.124.99، والذي يقوم PIX بإعادة توجيهه إلى 10.1.1.6.
- يقوم المستخدمون الخارجيون بتوجيه طلبات FTP إلى عنوان IP الفريد 172.18.124.99، والذي يقوم PIX بإعادة توجيهه إلى 10.1.1.3.
- يوجه المستخدمون الخارجيون طلبات برنامج Telnet إلى عنوان PAT 172.18.124.208، الذي يعيد PIX توجيهه إلى 10.1.1.4.
- يوجه المستخدمون الخارجيون طلب Telnet إلى PIX خارج عنوان IP 172.18.124.216، والذي يقوم PIX بإعادة توجيهه إلى 10.1.1.5.
- يقوم المستخدمون الخارجيون بتوجيه طلب HTTP إلى PIX خارج عنوان IP 172.18.124.216، والذي يقوم PIX بإعادة توجيهه إلى 10.1.1.5.
- يوجه المستخدمون الخارجيون طلب منفذ HTTP 8080 إلى عنوان PAT 172.18.124.208، والذي يقوم PIX بإعادة توجيهه إلى 10.1.1.7 منفذ 80.

يمنع هذا المثال أيضا وصول بعض المستخدمين من الداخل إلى الخارج باستخدام قائمة التحكم في الوصول ((ACL 100. هذه الخطوة إختيارية. يتم السماح بحركة المرور الصادرة دون وجود قائمة التحكم في الوصول (ACL).

الرسم التخطيطي للشبكة - إعادة توجيه المنفذ (إعادة التوجيه)



تكوين PIX الجزئي - إعادة توجيه المنفذ

يوضح هذا التكوين الجزئي إستخدام إعادة توجيه المنفذ الثابت (إعادة التوجيه). راجع الرسم التخطيطي لشبكة إعادة توجيه المنفذ (إعادة التوجيه).

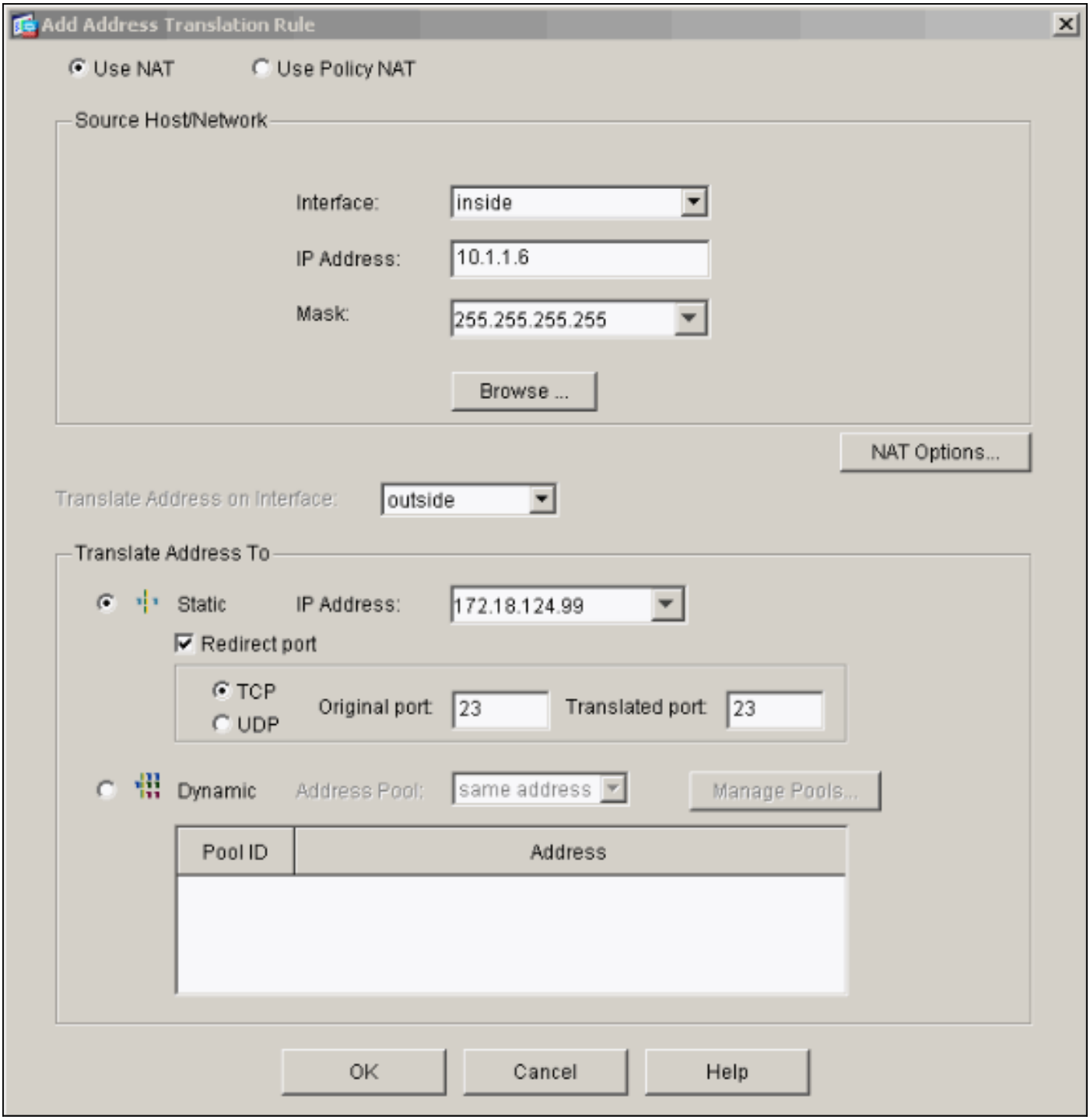
تكوين PIX 7.x جزئي - إعادة توجيه المنفذ (إعادة التوجيه)
fixup protocol ftp 21 *Use of an outbound ACL is optional.* access-list 100 *---!* permit tcp 10.1.1.0 255.255.255.128 any eq www access-

```
list 100 deny tcp any any eq www access-list 100 permit
  tcp 10.0.0.0 255.0.0.0 any access-list 100 permit udp
10.0.0.0 255.0.0.0 host 172.18.124.100 eq domain access-
   list 101 permit tcp any host 172.18.124.99 eq telnet
access-list 101 permit tcp any host 172.18.124.99 eq ftp
  access-list 101 permit tcp any host 172.18.124.208 eq
            telnet access-list 101 permit tcp any host
 172.18.124.216 eq telnet access-list 101 permit tcp any
  host 172.18.124.216 eq www access-list 101 permit tcp
    any host 172.18.124.208 eq 8080 interface Ethernet0
            nameif outside security-level 0 ip address
     172.18.124.216 255.255.255.0 ! interface Ethernet1
   nameif inside security-level 100 ip address 10.1.1.2
  255.255.255.0 ! global (outside) 1 172.18.124.208 nat
 (inside) 1 0.0.0.0 0.0.0.0 0 0 static (inside,outside)
       tcp 172.18.124.99 telnet 10.1.1.6 telnet netmask
        255.255.255.255 0 0 static (inside,outside) tcp
172.18.124.99 ftp 10.1.1.3 ftp netmask 255.255.255.255 0
    0 static (inside,outside) tcp 172.18.124.208 telnet
     10.1.1.4 telnet netmask 255.255.255.255 0 0 static
  (inside,outside) tcp interface telnet 10.1.1.5 telnet
 netmask 255.255.255.255 0 0 static (inside,outside) tcp
  interface www 10.1.1.5 www netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 8080 10.1.1.7
 www netmask 255.255.255.255 0 0 !--- Use of an outbound
   ACL is optional. access-group 100 in interface inside
                    access-group 101 in interface outside
```

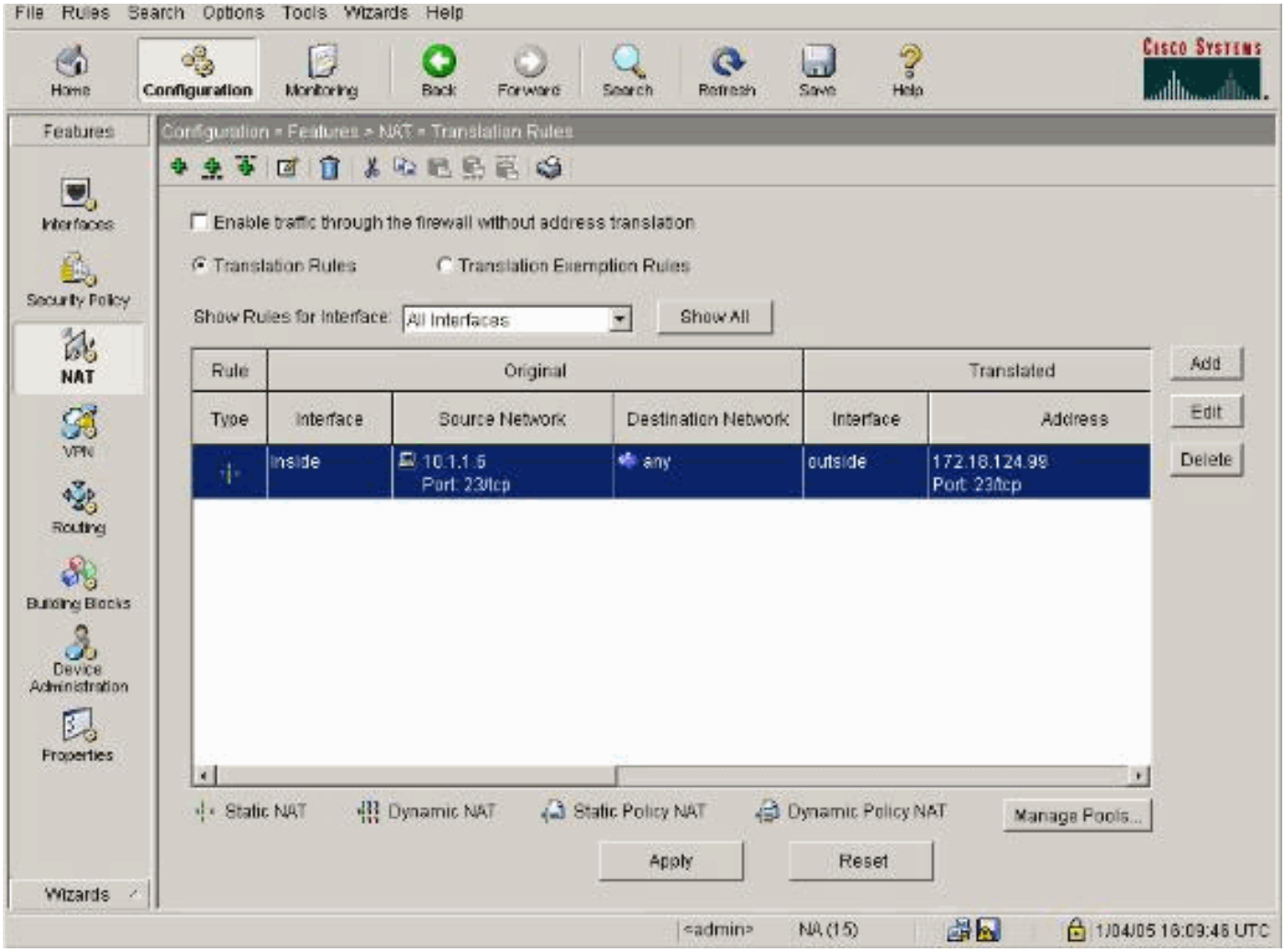
ملاحظة: إذا تم تكوين PIX/ASA باستخدام الأمر yarp **sysopt noproxy الخارجي**، فإنه لا يسمح لجدار الحماية بتنفيذ ترجمات البروكسي والثابت nat في PIX/ASA. لحل هذه المشكلة، قم بإزالة الأمر yarp **sysopt noproxy** خارجي في تكوين PIX/ASA ثم قم بتحديث إدخالات ARP باستخدام ARP مجاني. هذا يسمح ساكن إستاتيكي nat مدخل أن يعمل جيدا.

هذا الإجراء هو مثال على كيفية تكوين إعادة توجيه المنفذ (إعادة التوجيه) الذي يسمح للمستخدمين الخارجيين بتوجيه طلبات Telnet إلى عنوان IP فريد 172.18.124.99، والذي يقوم PIX بإعادة توجيهه إلى 10.1.1.6.

1. استعملت ASDM واخترت **تشكيل > سمة > nat > ترجمة قاعدة**.
2. حدد **قواعد الترجمة** وانقر **إضافة**.
3. للمضيف المصدر/الشبكة، أدخل المعلومات لعنوان IP الداخلي.
4. لترجمة العنوان إلى، حدد **ساكن إستاتيكي**، دخلت العنوان خارجي وفحصت **يعيد ميناء**.
5. دخلت ال pre-ترجمة السابقة وما بعد ترجمة معلومات أيسر (هذا مثال يحافظ ميناء 23). وانقر فوق **OK**.



تظهر الترجمة في قواعد الترجمة عندما تختار **تشكيل > ميزات > nat > قواعد الترجمة**.



الحد من جلسة TCP/UDP باستخدام ثابت

إن يريد أنت أن يقصر ال TCP أو UDP جلسة إلى النادل داخلي وضع في PIX/ASA، بعد ذلك استعملت **الساكن إستاتيكي** أمر.

تحديد الحد الأقصى لعدد إتصالات TCP و UDP المتزامنة للشبكة الفرعية بأكملها. الإعداد الافتراضي هو 0، مما يعني إتصالات غير محدودة (يتم إغلاق الاتصالات الخاملة بعد مهلة الخمول المحددة بواسطة الأمر **timeout conn**.). لا ينطبق هذا الخيار على خارج NAT. يتعقب جهاز الأمان الاتصالات فقط من واجهة أمان أعلى إلى واجهة أمان أقل.

إن الحد من عدد الاتصالات الجنينية يحميك من هجوم رفض الخدمة (DoS). يستخدم جهاز الأمان الحد الجنيني لتشغيل اعتراض TCP، والذي يحمي الأنظمة الداخلية من هجوم رفض الخدمة (DoS) الذي يتم تنفيذه عن طريق إغراق واجهة مع حزم TCP syn. الاتصال الجنيني هو طلب اتصال لم يتم إنهاء المصافحة الضرورية بين المصدر والوجهة. لا ينطبق هذا الخيار على خارج NAT. تنطبق ميزة اعتراض بروتوكول TCP فقط على البيئات المضيفة أو الخوادم الموجودة على مستوى أمان أعلى. إذا قمت بضبط الحد الجنيني ل خارج NAT، فإن الحد الجنيني يتم تجاهله.

على سبيل المثال:

```
ASA(config)#static (inside,outside) tcp 10.1.1.1 www 10.2.2.2 www tcp 500 100
The maximum number of simultaneous tcp connections the local IP !--- hosts are to allow is ---!
500, default is 0 which means unlimited !--- connections. Idle connections are closed after the
time specified !--- by the timeout conn command !--- The maximum number of embryonic connections
.per host is 100
```

PIX-3-201002٪: إتصالات كثيرة جدا على {global_address} {static|xlate}! بريد إلكتروني

هذه رسالة متعلقة بالاتصال. يتم تسجيل هذه الرسالة عند تجاوز الحد الأقصى لعدد الاتصالات بالعنوان الثابت المحدد. المتغير الإلكتروني هو الحد الأقصى لعدد الاتصالات والمنافذ الجنينية هو الحد الأقصى لعدد الاتصالات المسموح بها للثابت أو الأخير.

الإجراء الموصى به هو إستخدام الأمر **show static** للتحقق من الحد المفروض على الاتصالات بعنوان ثابت. الحد قابل للتكوين.

ASA-3-201011٪: تجاوز حد الاتصال 1000/1000 للحزمة الواردة من 2393/10.1.26.51 إلى 135/10.0.86.155 على الواجهة الخارجية

هذا خطأ رسالة إلى cisco بق CSCsg52106 id (سجل زبون فقط). راجع هذا الخطأ للحصول على مزيد من المعلومات.

قائمة الوصول المستندة إلى الوقت

لا يقيد إنشاء نطاق زمني الوصول إلى الجهاز. يحدد الأمر **time-range** النطاق الزمني فقط. بعد تحديد نطاق زمني، يمكنك إرفاقه بقواعد حركة المرور أو إجراء.

لتنفيذ قائمة تحكم في الوصول (ACL) المستندة إلى الوقت، أستخدم الأمر **time-range** لتحديد أوقات محددة من اليوم والأسبوع. ثم أستخدم الأمر **with access-list extended time-range** لربط النطاق الزمني بقوائم التحكم في الوصول (ACL).

يعتمد النطاق الزمني على ساعة النظام الخاصة بجهاز الأمان. ومع ذلك، تعمل الميزة بشكل أفضل مع مزامنة NTP.

بعد إنشاء نطاق زمني وإدخال وضع تكوين النطاق الزمني، يمكنك تحديد معلمات النطاق الزمني باستخدام الأوامر **المطلق** والدوري. لاسترجاع الإعدادات الافتراضية للكلمات الأساسية المطلقة والدورية **للأمر time-range**، أستخدم الأمر **الافتراضي** في وضع تكوين النطاق الزمني.

لتنفيذ قائمة تحكم في الوصول (ACL) المستندة إلى الوقت، أستخدم الأمر **time-range** لتحديد أوقات محددة من اليوم والأسبوع. ثم أستخدم الأمر **with access-list extended** لربط النطاق الزمني بقوائم التحكم في الوصول (ACL). يربط المثال التالي قائمة تحكم في الوصول (ACL) المسماة "Sales" بنطاق زمني مسمى "New York Minute":

يقوم هذا المثال بإنشاء نطاق زمني باسم "دقيقة نيويورك" ويدخل وضع تكوين النطاق الزمني:

```
hostname(config)#time-range New_York_Minute
hostname(config-time-range)#periodic weekdays 07:00 to 19:00
hostname(config)#access-list Sales line 1 extended deny ip any any time-range New_York_Minute
hostname(config)#access-group Sales in interface inside
```

المعلومات التي سيتم جمعها إذا قمت بفتح حالة دعم فني

إذا كنت لا تزال بحاجة إلى مساعدة وتريد فتح حالة باستخدام دعم Cisco التقني، فتأكد من تضمين هذه المعلومات لاستكشاف أخطاء جهاز أمان PIX وإصلاحها.
• وصف المشكلة وتفاصيل المخطط ذات الصلة. • الخطوات التي أستخدمتها لاستكشاف الأخطاء وإصلاحها قبل فتح الحالة.

- مخرجات من الأمر **show tech-support**.
- إخراج من الأمر **show log** بعد تشغيل الأمر **logging buffered debugging**، أو التقاط وحدة التحكم التي توضح المشكلة (إذا كانت متاحة).

قم بإرفاق البيانات المجمعة بالحالة الخاصة بك بتنسيق نص عادي غير مضغوط (.txt). يمكنك إرفاق معلومات إلى حالتك في أداة طلب خدمة TAC (العملاء المسجلون فقط). إذا تعذر عليك الوصول إلى أداة طلب خدمة TAC (العملاء المسجلون فقط)، فيمكنك إرسال المعلومات في مرفق بريد إلكتروني إلى attach@cisco.com مع وجود رقم الحالة في سطر موضوع رسالتك.

معلومات ذات صلة

- صفحة دعم جهاز أمان PIX
- مراجع أوامر PIX
- 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).