PAT و NAT تانايب :FWSM و PIX/ASA 7.x

المحتويات

المقدمة

يزود هذا وثيقة مثال من أساسي شبكة عنوان ترجمة (NAT) وميناء عنوان ترجمة (PAT) تشكيل على ال cisco PIX/ASA أمن أداة. يتم توفير مخططات مبسطة للشبكة. ارجع إلى وثائق PIX/ASA للحصول على إصدار برنامج PIX/ASA لديك للحصول على معلومات تفصيلية.

راجع إستخدام أوامر NAT و global و static و channel و access-list و إعادة توجيه المنفذ (Forwarding) على PIX لمعرفة المزيد حول NAT وglobal و **static** و**channels** وaccess-list وإعادة توجيه المنفذ (إعادة التوجيه) على PIX 5.x والإصدارات الأحدث.

راجع إستخدام عبارات NAT و PAT على جدار حماية Cisco PIX الآمن لمعرفة المزيد حول أمثلة تكوينات NAT الأساسية و PAT على جدار حماية Cisco PIX الآمن.

أحلت ل كثير معلومة على تشكيل nat في ASA صيغة 8.3 ومتأخر، معلومة حول NAT.

ملاحظة: NAT في الوضع الشفاف مدعوم من PIX/ASA الإصدار x.8. أحلت nat في أسلوب شفاف ل كثير معلومة.

المتطلبات الأساسية

المتطلبات

يجب أن يكون قراء هذا المستند على دراية بجهاز الأمان Cisco PIX/ASA.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 7.0 من برنامج جهاز الأمان Cisco PIX 500 Series Security Appliance والإصدارات الأحدث.

ملاحظة: تمت إعادة تصنيف هذا المستند باستخدام PIX/ASA الإصدار x.8.

ملاحظة: تنطبق الأوامر المستخدمة في هذا المستند على الوحدة النمطية لخدمة جدار الحماية (FWSM).

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.

أمر التحكم في الشبكة (NAT)

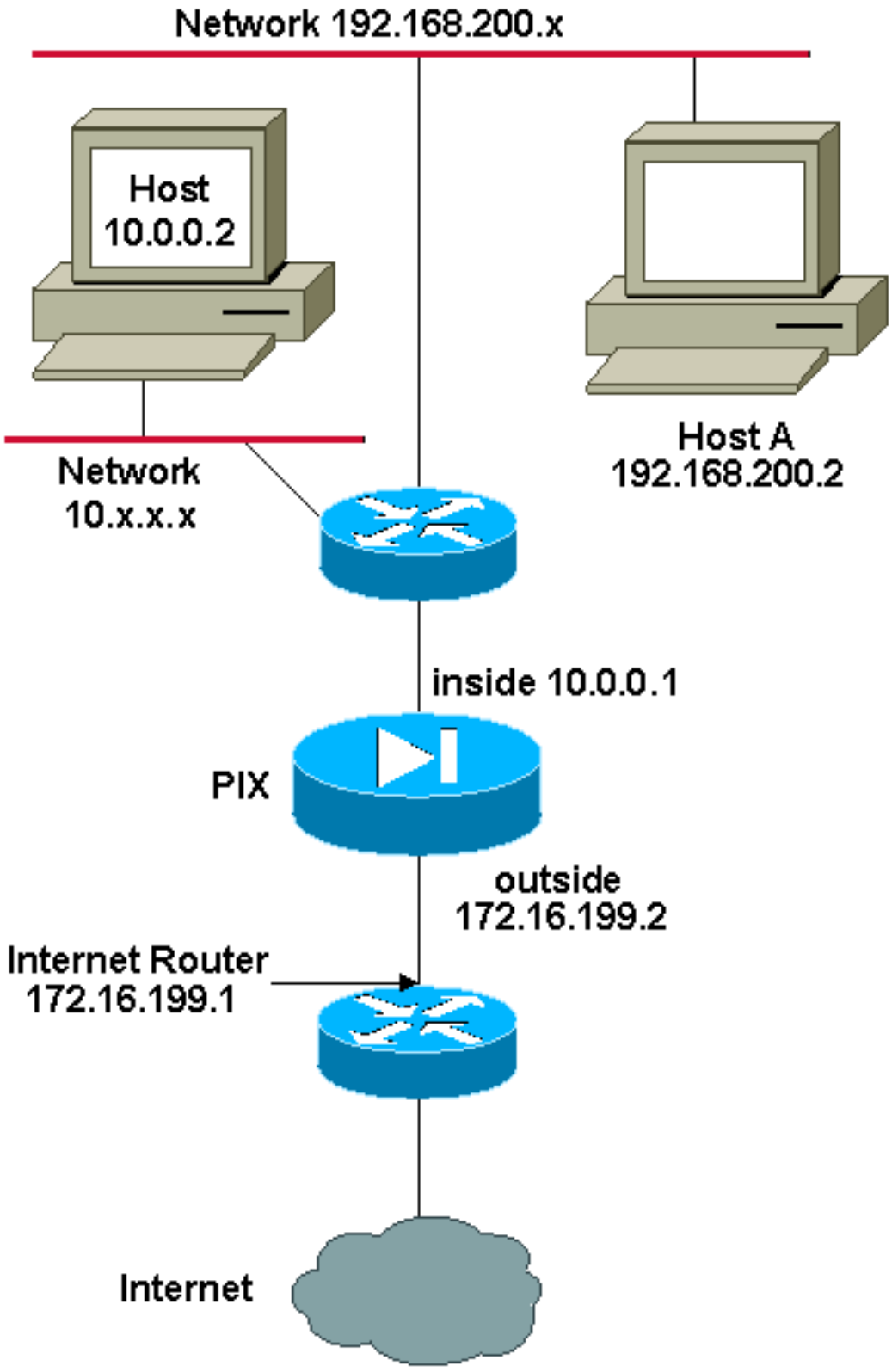
يحدد الأمر **nat-control** على PIX/ASA أن كل حركة مرور عبر جدار الحماية يجب أن يكون لها إدخال ترجمة محدد (بيان **nat** مع عبارة **global** متطابقة أو عبارة **ثابتة**) لحركة المرور تلك التي تمر عبر جدار الحماية. يضمن الأمر **nat-control** أن سلوك الترجمة هو نفس إصدارات جدار حماية PIX السابقة على الإصدار 7.0. يكون التكوين الافتراضي ل PIX/ASA الإصدار 7.0 والإصدارات الأحدث هو مواصفات الأمر **no nat-control**. باستخدام الإصدار 7.0 من PIX/ASA والإصدارات الأحدث، يمكنك تغيير هذا السلوك عند إصدار الأمر **nat-control**.

مع تعطيل **التحكم في nat**، يقوم PIX/ASA بإعادة توجيه الحزم من واجهة أمان أعلى إلى واجهة أخرى أقل دون إدخال ترجمة محدد في التكوين. لتمرير حركة المرور من واجهة أمان أقل إلى واجهة أمان أعلى، أستخدم قوائم الوصول للسماح بحركة المرور. وبعد ذلك يقوم PIX/ASA بإعادة توجيه حركة المرور. يركز هذا المستند على سلوك جهاز الأمان PIX/ASA مع تمكين **عنصر التحكم في nat**.

ملاحظة: إذا كنت ترغب في إزالة عبارة التحكم في الشبكة (NAT) في PIX/ASA أو تعطيلها، فأنت بحاجة إلى إزالة جميع عبارات NAT من جهاز الأمان. بشكل عام، تحتاج إلى إزالة NAT قبل إيقاف تشغيل عنصر تحكم NAT. يجب إعادة تكوين عبارة NAT في PIX/ASA للعمل كما هو متوقع.

عبارات متعددة ل NAT مع 0 NAT

الرسم التخطيطي للشبكة



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

في هذا المثال، يوفر ISP مدير الشبكة بنطاق من العناوين من 172.16.199.1 إلى 172.16.199.63. يقرر مدير الشبكة تخصيص 172.16.199.1 للواجهة الداخلية على موجه الإنترنت و 172.16.199.2 للواجهة الخارجية ل PIX/ASA.

كان لمسؤول الشبكة عنوان من الفئة C معين للشبكة، 24/192.168.200.0، ولديه بعض محطات العمل التي تستخدم هذه العناوين للوصول إلى الإنترنت. لا يجب أن تكون محطات العمل هذه مترجمة. ومع ذلك، يتم تعيين عناوين لمحطات العمل الجديدة في شبكة 8/10.0.0.0، وتحتاج إلى ترجمتها.

in order to احتويت هذا شبكة تصميم، الشبكة مدير ينبغي استعملت إثنان nat عبارة وواحد شامل بركة في ال PIX/ASA تشكيل بما أن هذا إنتاج يبدي:

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 192.168.200.0 255.255.255.0 0 0

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

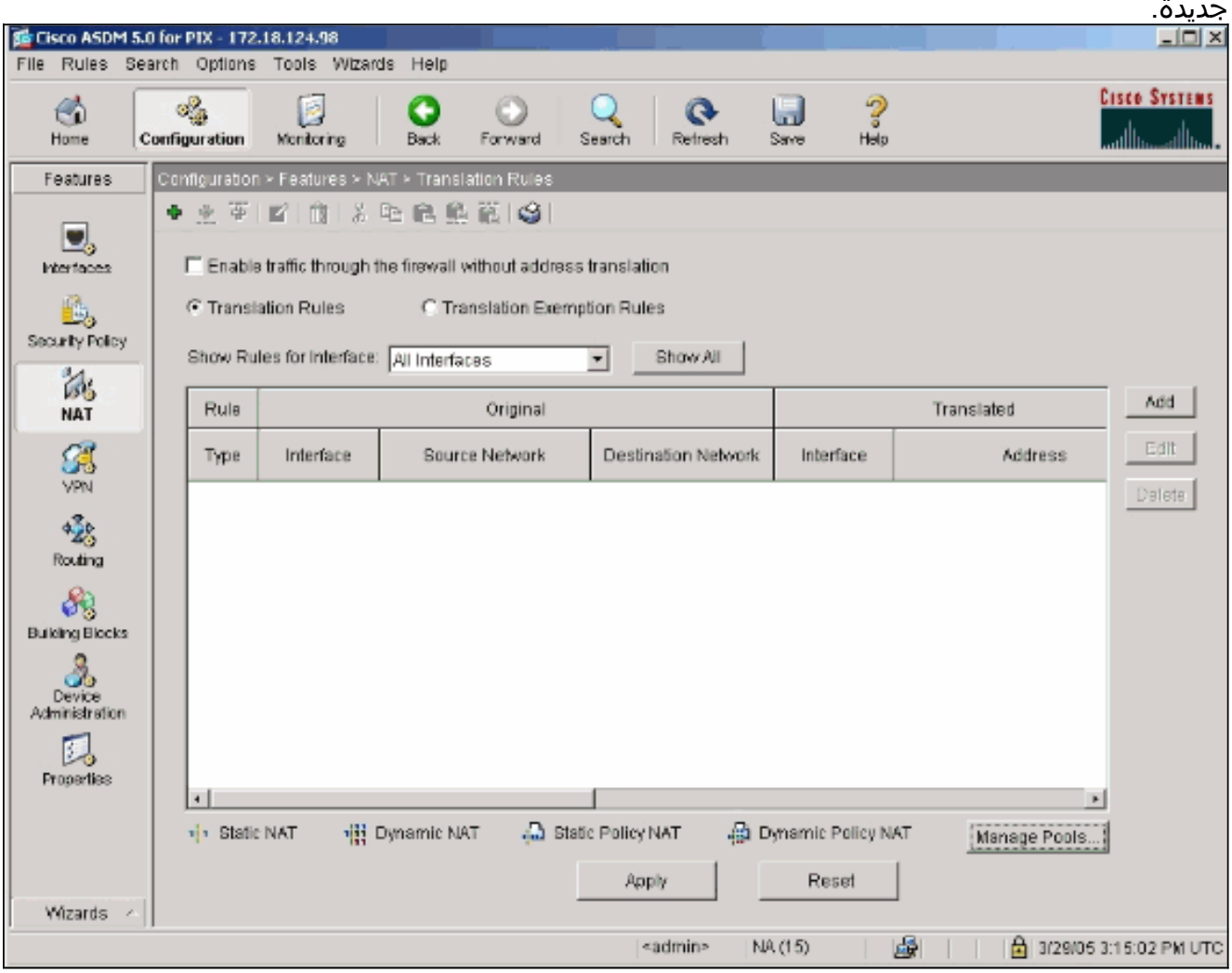
لا يترجم هذا تشكيل عنوان المصدر لأي حركة مرور صادرة من الشبكة 24/192.168.200.0. وهو يترجم عنوان مصدر في شبكة 8/10.0.0.0 إلى عنوان من النطاق 172.16.199.3 إلى 172.16.199.62.

توفر هذه الخطوات شرحا لكيفية تطبيق هذا التكوين نفسه باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM).

ملاحظة: قم بإجراء جميع تغييرات التكوين من خلال واجهة سطر الأوامر (CLI) أو إدارة قاعدة بيانات المحول (ASDM). يتسبب إستخدام كل من CLI و ASDM لتغييرات التكوين في سلوك غير منتظم للغاية فيما يتعلق بما يتم تطبيقه من قبل ASDM. هذا ليس خطأ، ولكنه يحدث بسبب كيفية عمل ASDM.

ملاحظة: عند فتح ASDM، فإنه يستورد التكوين الحالي من PIX/ASA ويعمل من هذا التكوين عند إجراء التغييرات وتطبيقها. إذا تم إجراء تغيير على PIX/ASA أثناء فتح جلسة عمل ASDM، فلن يعمل ASDM بعد ذلك مع ما "يعتقد" أنه التكوين الحالي ل PIX/ASA. تأكد من إغلاق أي جلسات عمل ASDM إذا قمت بتغييرات التكوين عبر CLI (واجهة سطر الأوامر). افتح ASDM مرة أخرى عندما تريد العمل عبر واجهة المستخدم الرسومية.

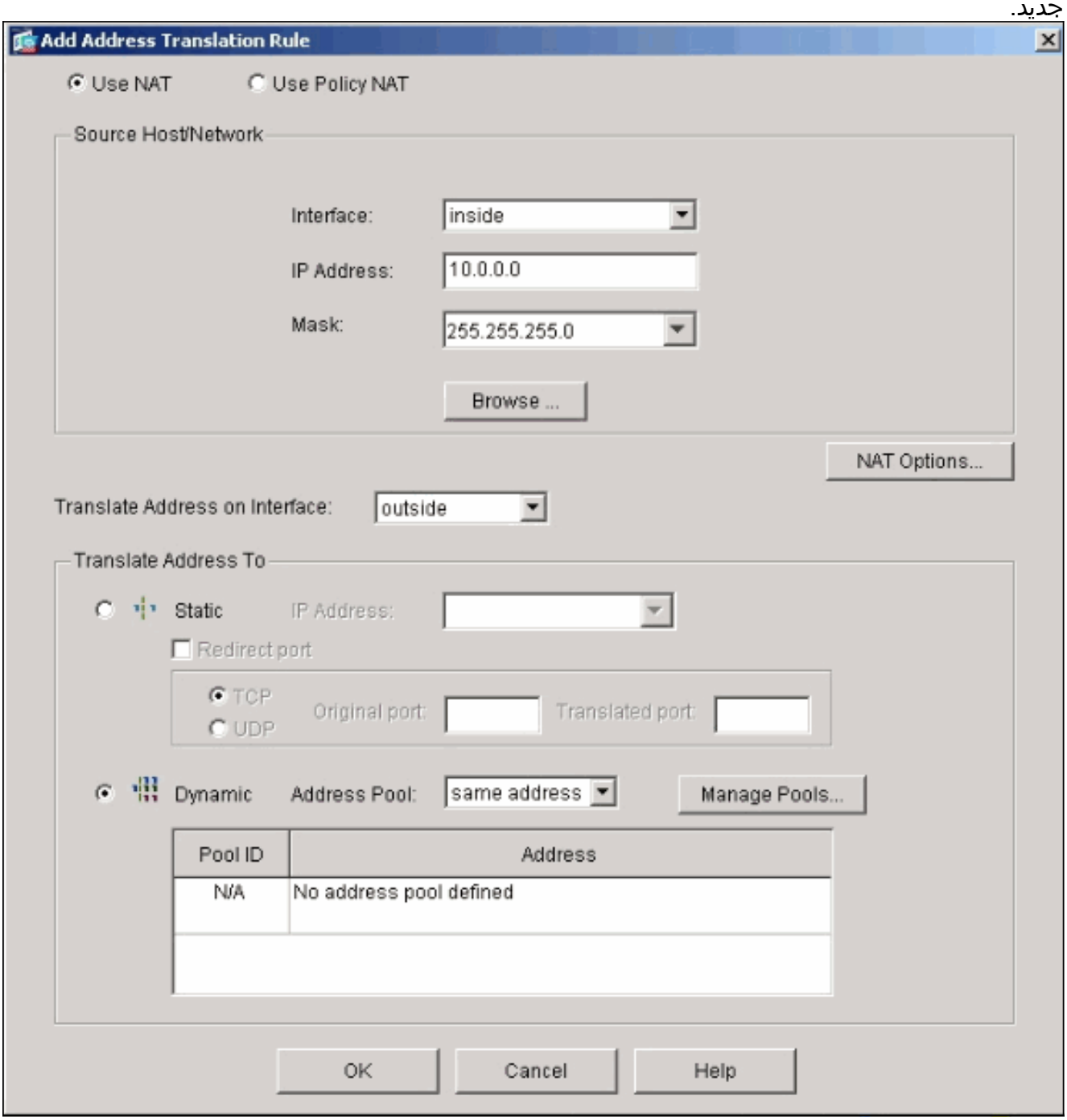
1. قم بتشغيل ASDM، وتصفح إلى علامة التبويب التكوين، وانقر فوق **NAT**.
2. انقر فوق **إضافة** لإنشاء قاعدة جديدة.



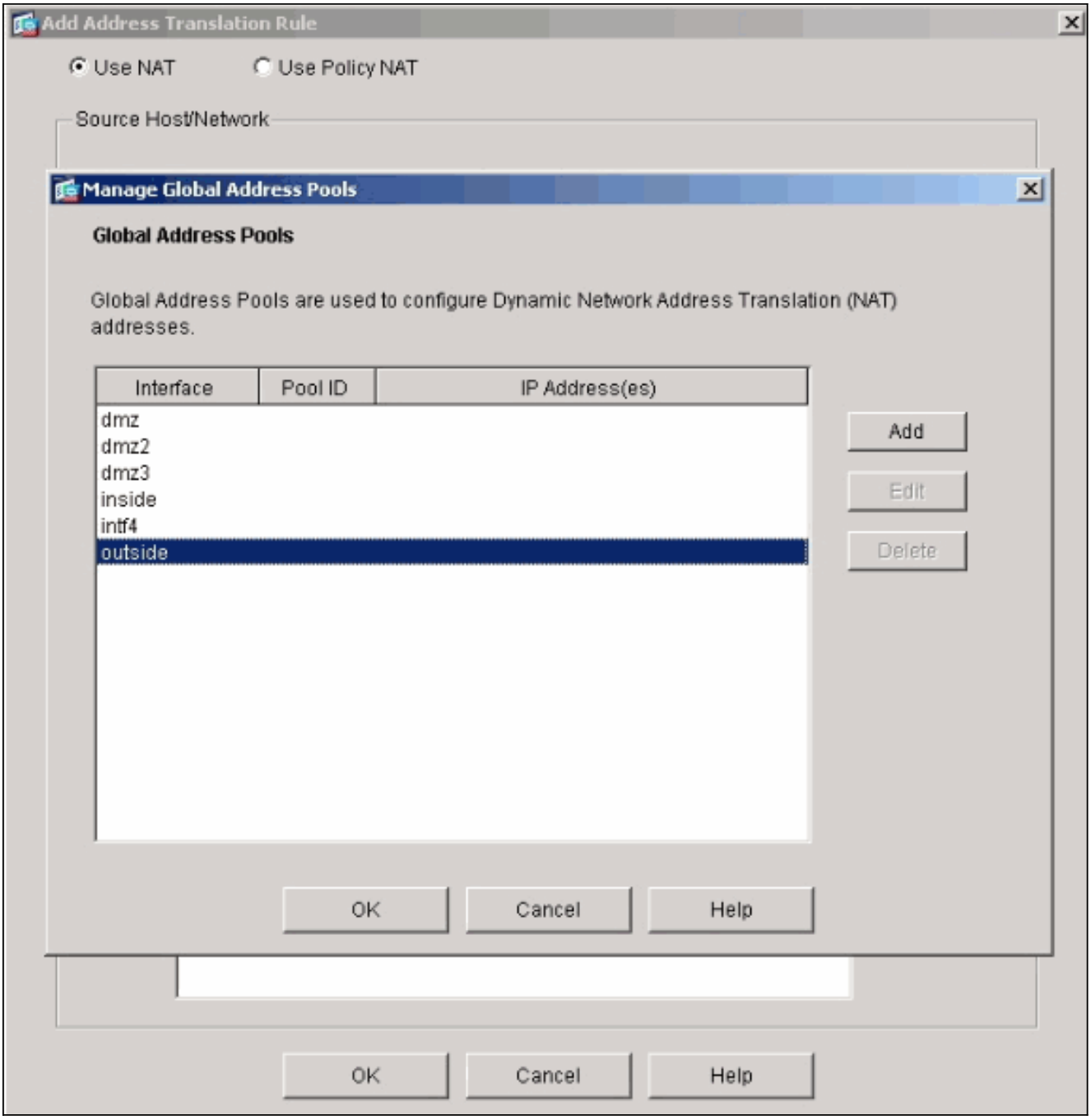
يظهر نافذة جديد أن يسمح المستعمل أن يغير NAT خيار ل هذا nat مدخل. على هذا المثال، قم بتنفيذ NAT

على الحزم التي تصل إلى الواجهة الداخلية التي يتم الحصول عليها من شبكة 24/10.0.0.0 المحددة.يترجم ال PIX/ASA هذا ربط إلى حركي ip بركة على القارن خارجي. عقب يدخل أنت المعلومة أن يصف أي حركة مرور إلى nat، عينت تجمع من عنوان ل ال يترجم حركة مرور.

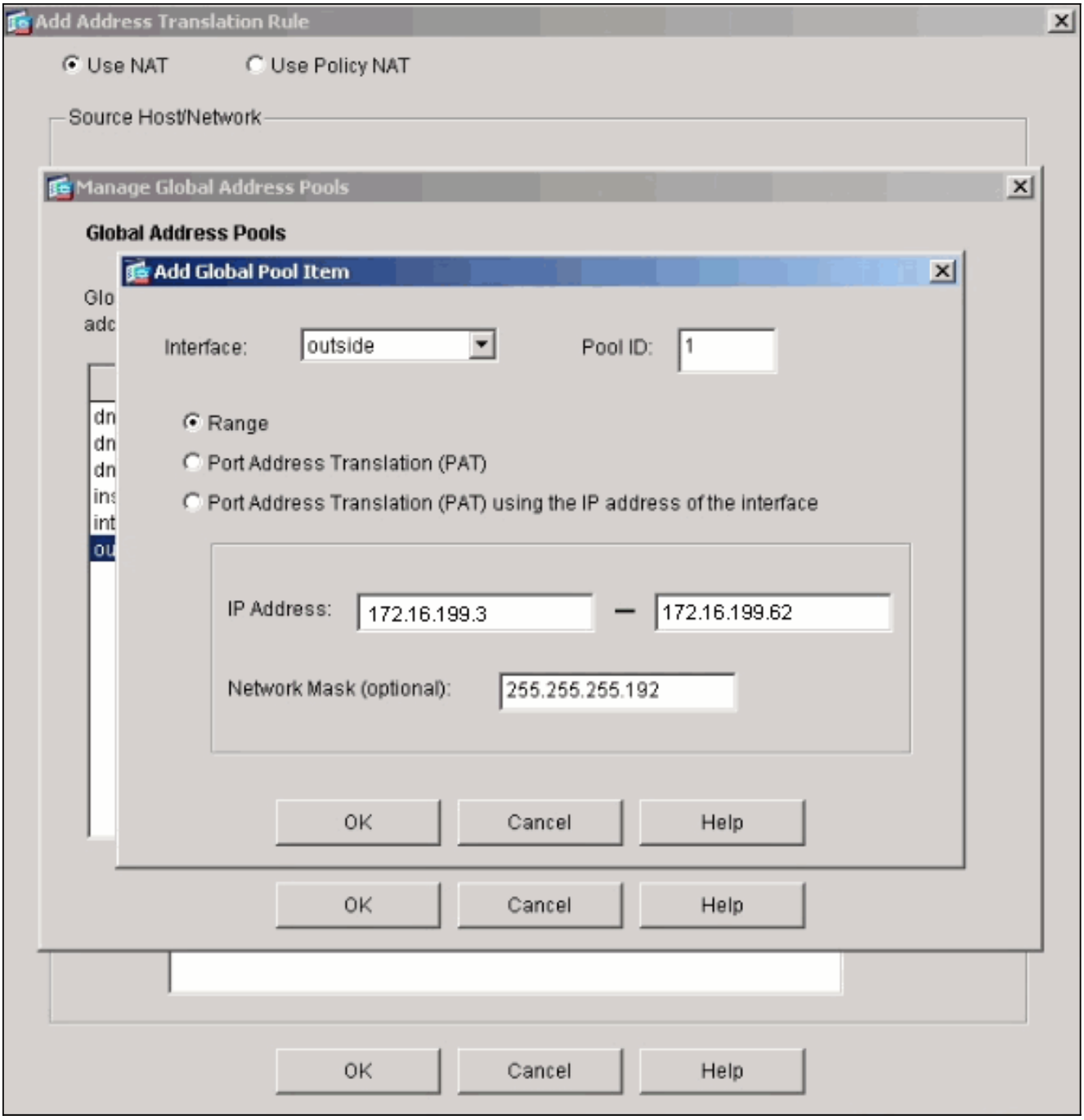
3. انقر فوق **إدارة تجمعات** لإضافة تجمع IP جديد.



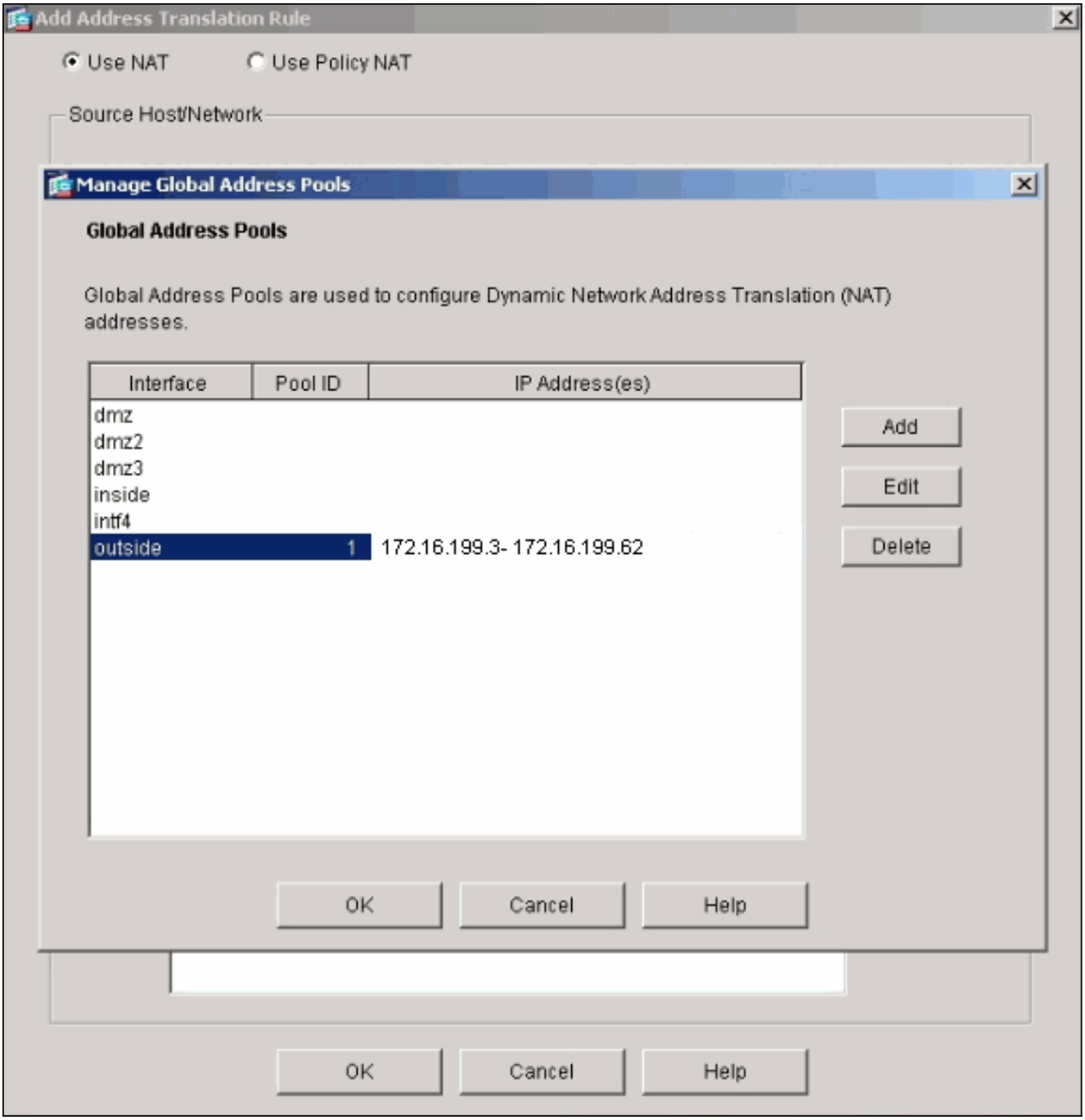
4. أخترت **خارجي**، وطقطقة **يضيف**.



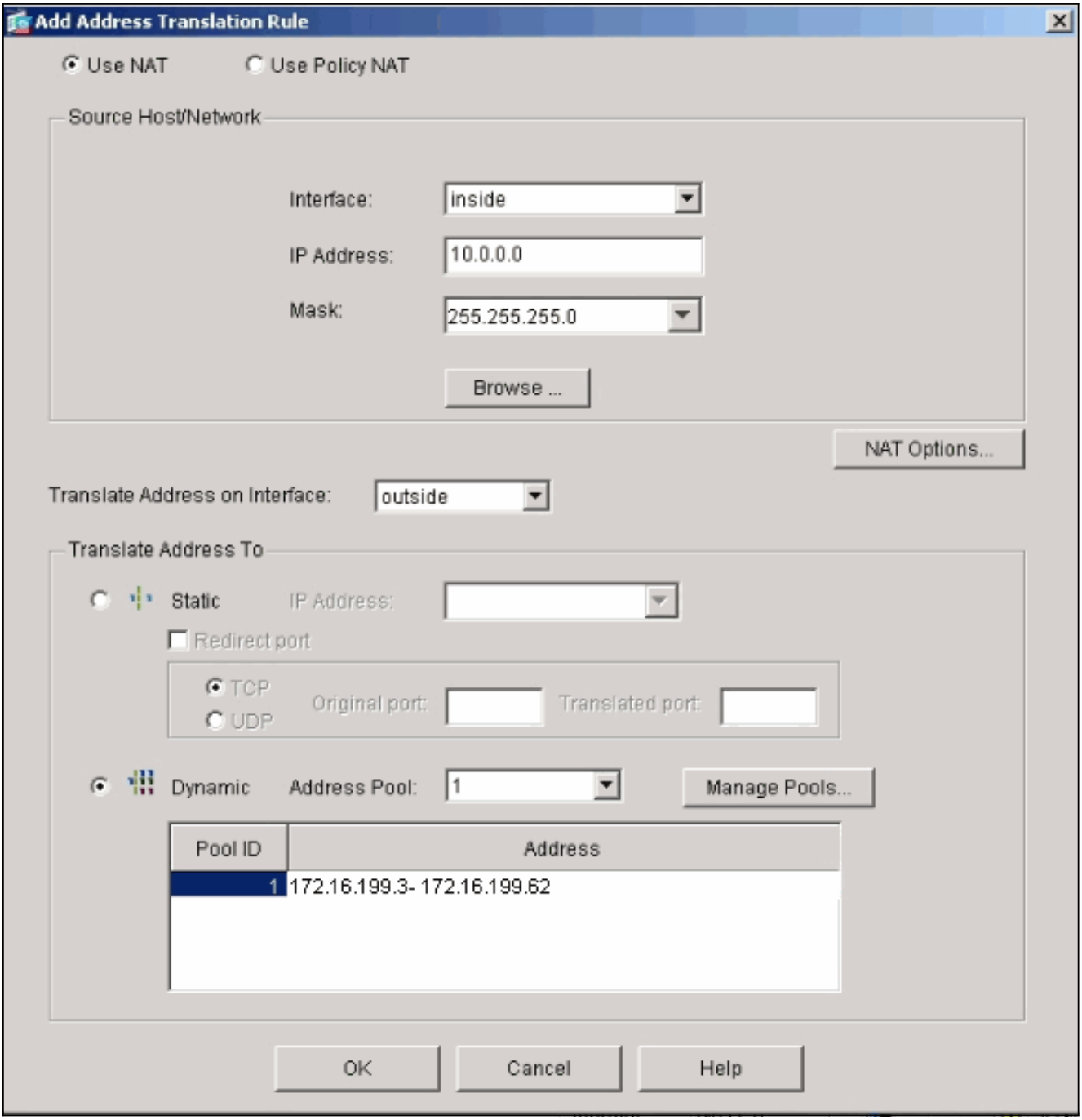
5. حدد نطاق IP للتجمع، وأعط التجمع رقم معرف عدد صحيح فريد.



6. قم بإدخال القيم المناسبة، وانقر **موافق**.يتم تحديد التجمع الجديد للواجهة الخارجية.

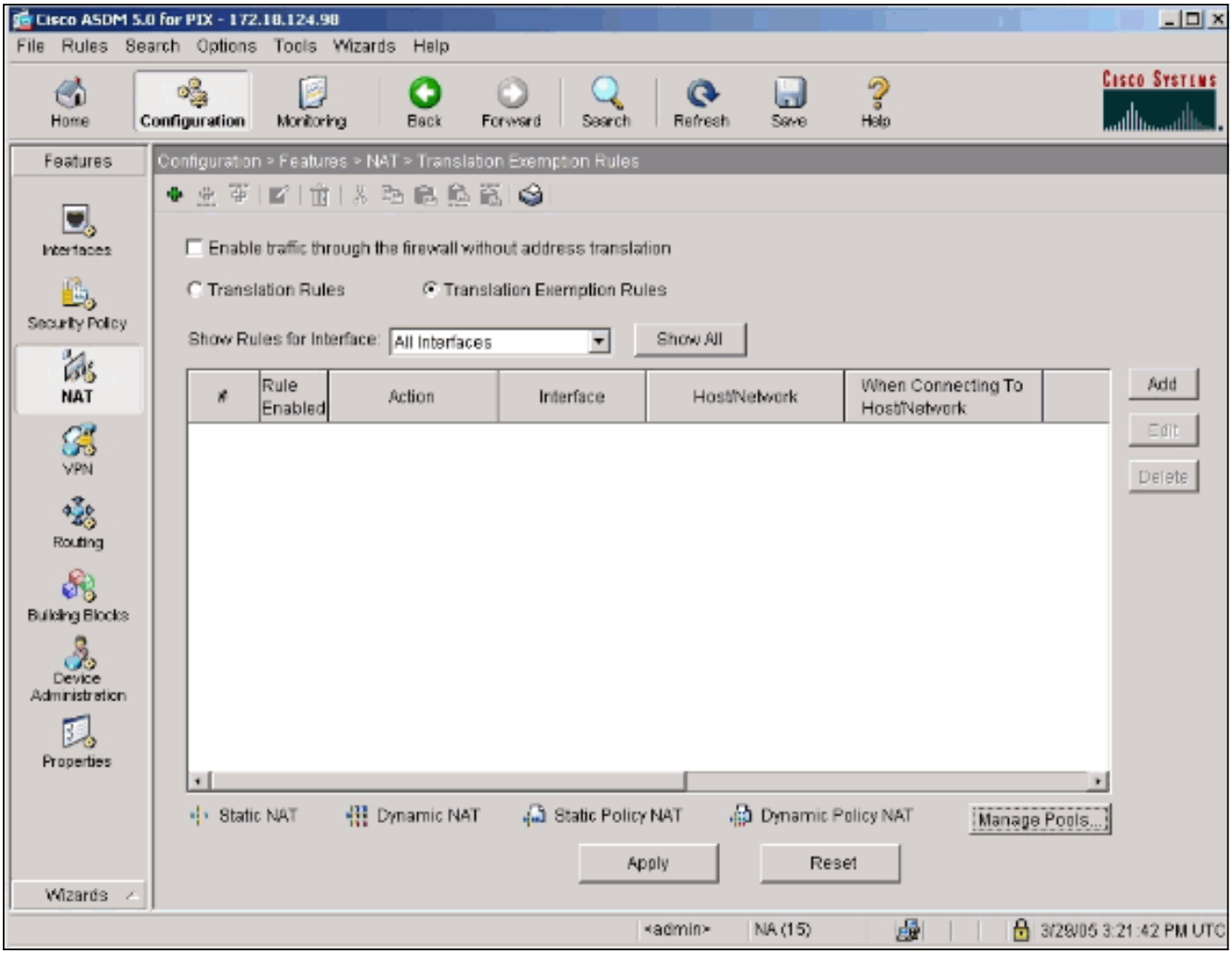


7. بعد تحديد التجمع، انقر فوق **موافق** للعودة إلى نافذة تكوين قاعدة nat.تأكد من إختيار التجمع الصحيح الذي قمت بإنشائه الآن ضمن القائمة المنسدلة لتجمع العناوين.

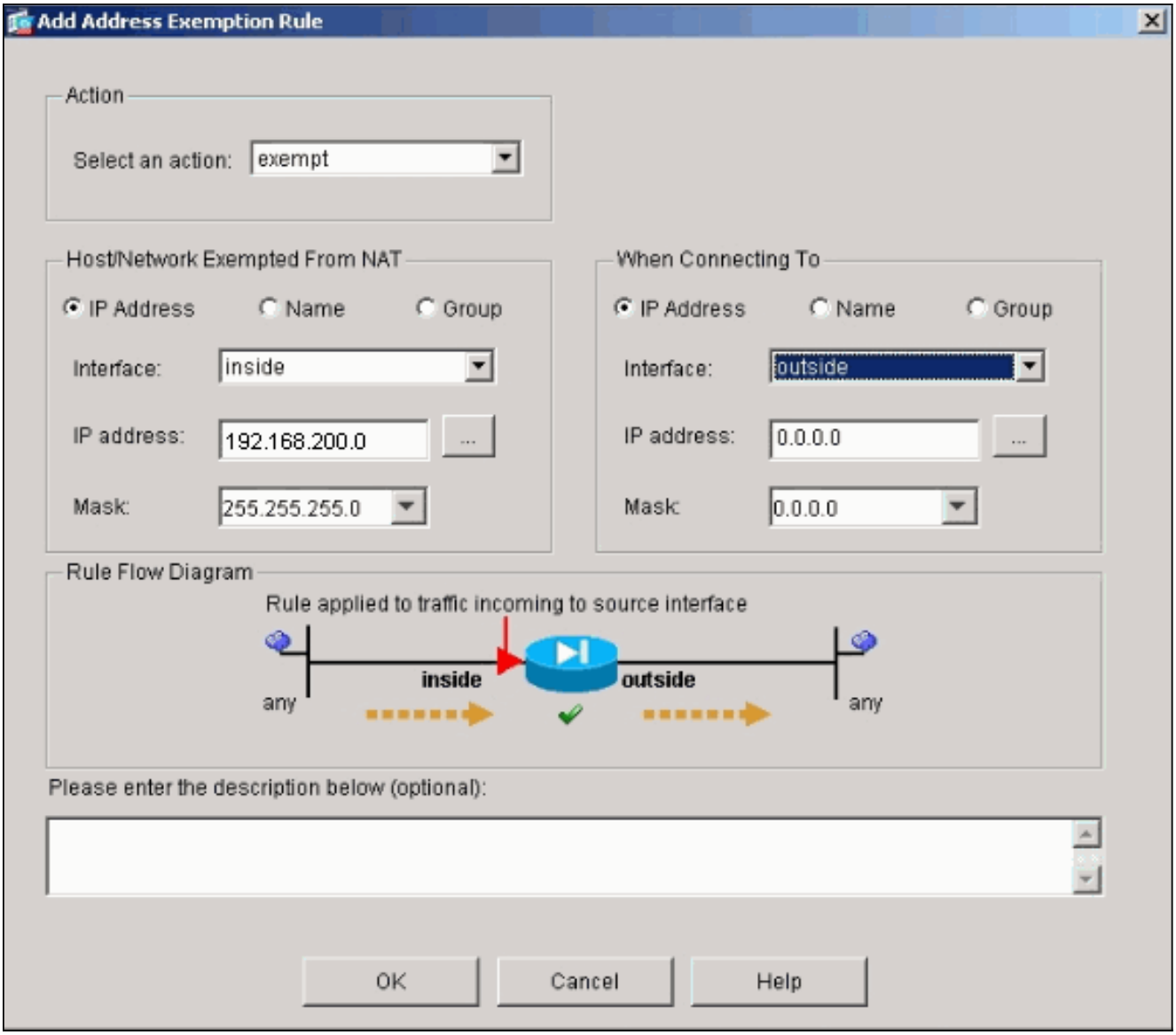


أنت الآن خلقت ترجمة nat من خلال الأمان أداة. مهما، أنت بعد تحتاج أن يخلق ال nat مدخل أن يعين ما حركة مرور لا إلى NAT.

8. انقر فوق **قواعد إستثناء الترجمة** الموجودة في أعلى الإطار، ثم انقر فوق **إضافة** لإنشاء قاعدة جديدة.



9. أخترت *القارن داخلي* كمصدر، وعينت **ال 24/192.168.200.0** subnet. أترك قيم "عند التوصيل" كالقيم الافتراضية.



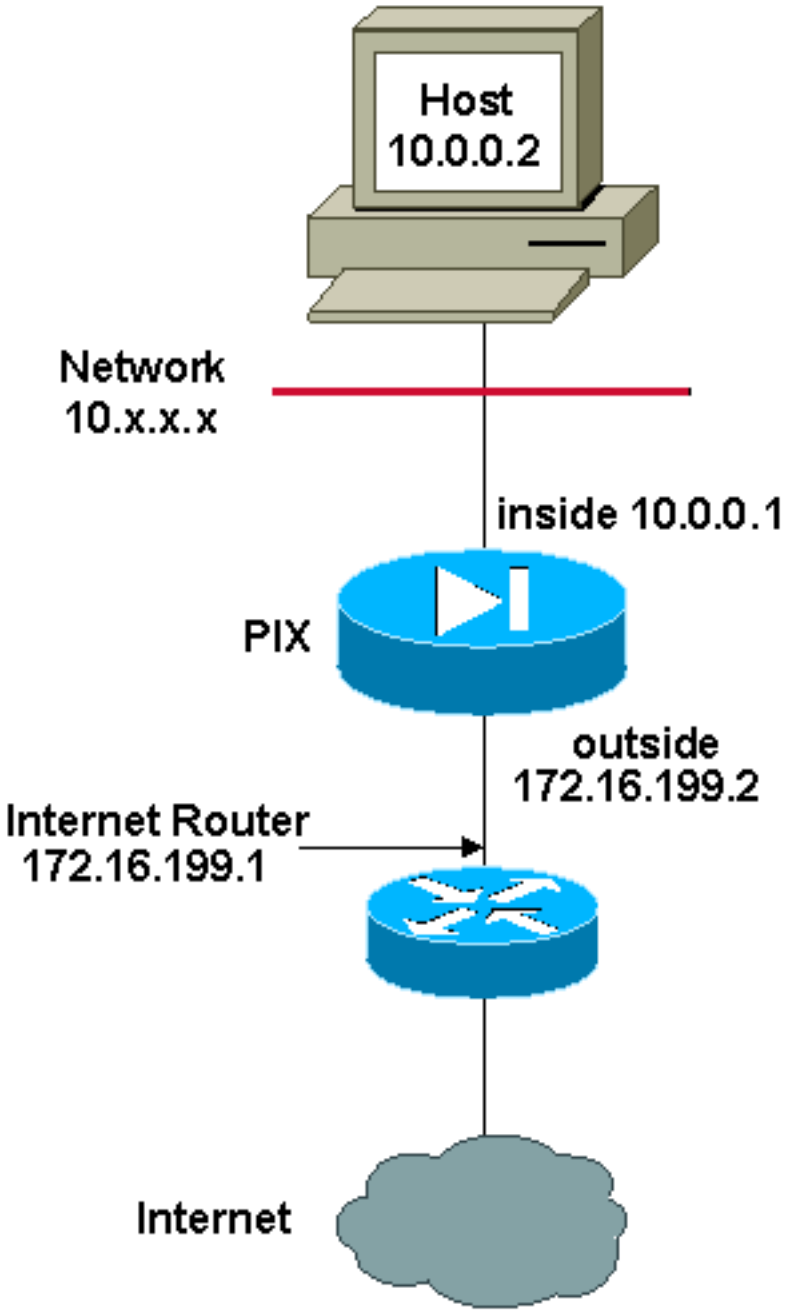
يتم الآن تحديد قواعد NAT.

10. انقر فوق **تطبيق** لتطبيق التغييرات على التكوين الجاري تشغيله الحالي لجهاز الأمان.يوضح هذا الإخراج الإضافات الفعلية التي يتم تطبيقها على تكوين PIX/ASA. تختلف قليلا عن الأوامر التي تم إدخالها من الطريقة اليدوية، لكنها متساوية.

```
access-list inside_nat0_outbound extended permit
ip 192.168.200.0 255.255.255.0 any

global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 10.0.0.0 255.255.255.0
```

تجمعات عمومية متعددة

الرسم التخطيطي للشبكة



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

في هذا المثال، يحتوي مدير الشبكة على نوعين من عناوين IP التي تسجل على الإنترنت. يجب على مدير الشبكة تحويل جميع العناوين الداخلية الموجودة في نطاق 8/10.0.0.0 إلى عناوين مسجلة. نطاقات عناوين IP التي يجب أن يستخدمها مدير الشبكة هي 172.16.199.1 إلى 172.16.199.62 و 192.168.150.1 إلى 192.168.150.254.
يمكن لمدير الشبكة القيام بذلك باستخدام:

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

global (outside) 1 192.168.150.1-192.168.150.254 netmask 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

في NAT حركي، العبارة الأكثر تحديدا هي التي تأخذ أسبقية عندما يستعمل أنت ال نفسه قارن على شامل.

```
nat (inside) 1 10.0.0.0 255.0.0.0
nat (inside) 2 10.1.0.0 255.255.0.0
```

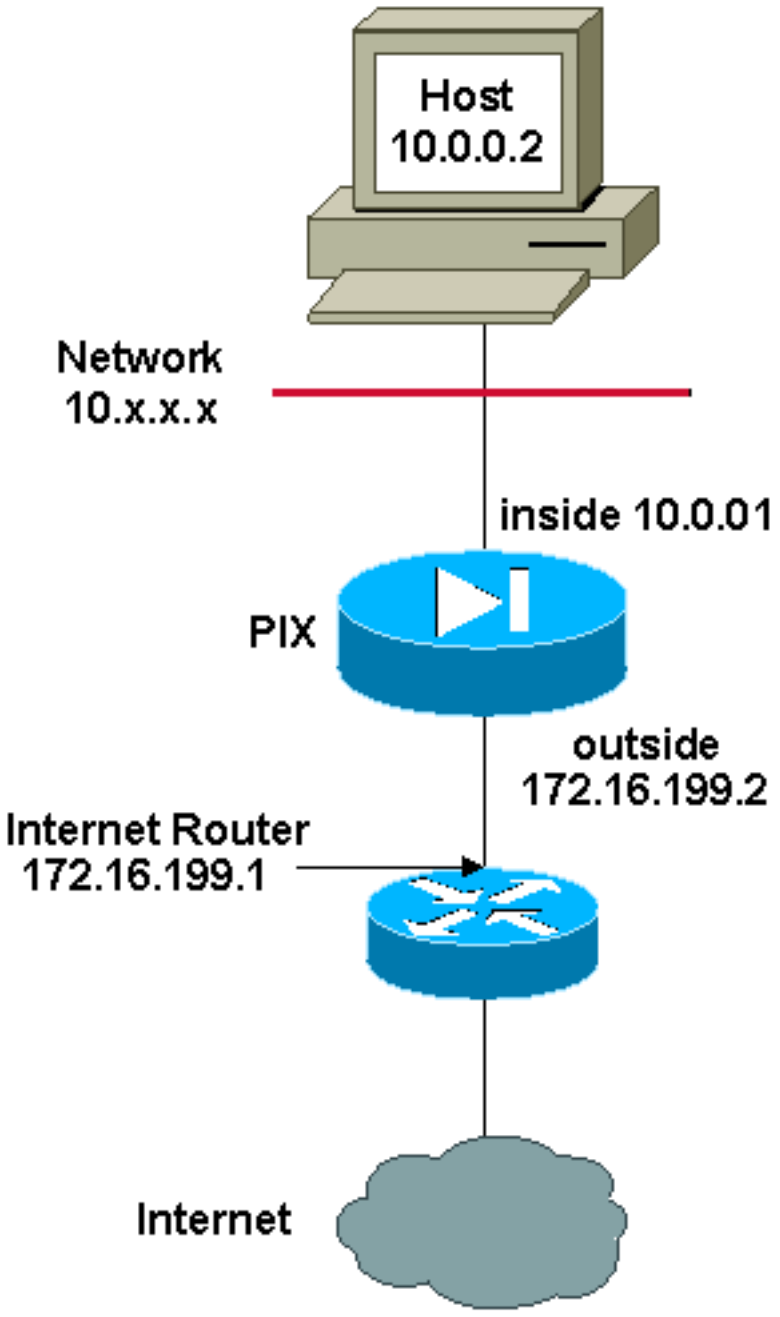
```
global (outside) 1 172.16.1.1
global (outside) 2 192.168.1.1
```

إذا كانت الشبكة الداخلية لديك على هيئة 10.1.0.0، فإن NAT Global 2 له الأسبقية على 1 لأنه أكثر تحديدا للترجمة.

ملاحظة: يتم إستخدام مخطط عنونة حرف بدل في عبارة NAT. يطلب هذا البيان من PIX/ASA ترجمة أي عنوان مصدر داخلي عند خروجه إلى الإنترنت. يمكن أن يكون العنوان في هذا الأمر أكثر تحديدا إذا كان مطلوبا.

خلط NAT و PAT العالمية

الرسم التخطيطي للشبكة



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

في هذا المثال، يوفر ISP لمدير الشبكة مجموعة من العناوين من 172.16.199.1 إلى 172.16.199.63 لاستخدام الشركة. يقرر مدير الشبكة إستخدام 172.16.199.1 للواجهة الداخلية على موجه الإنترنت و 172.16.199.2 للواجهة

الخارجية على PIX/ASA. يتبقى لديك 172.16.199.3 إلى 172.16.199.62 للاستخدام لتجمع NAT. ومع ذلك، فمدير الشبكة يعرف أنه يمكن أن يكون هناك في أي وقت أكثر من ستين شخصا يحاولون الخروج من تطبيق PIX/ASA. لذلك، يقرر مدير الشبكة أن يأخذ 172.16.199.62 ويجعل منه عنوان PAT بحيث يمكن للعديد من المستخدمين مشاركة عنوان واحد في نفس الوقت.

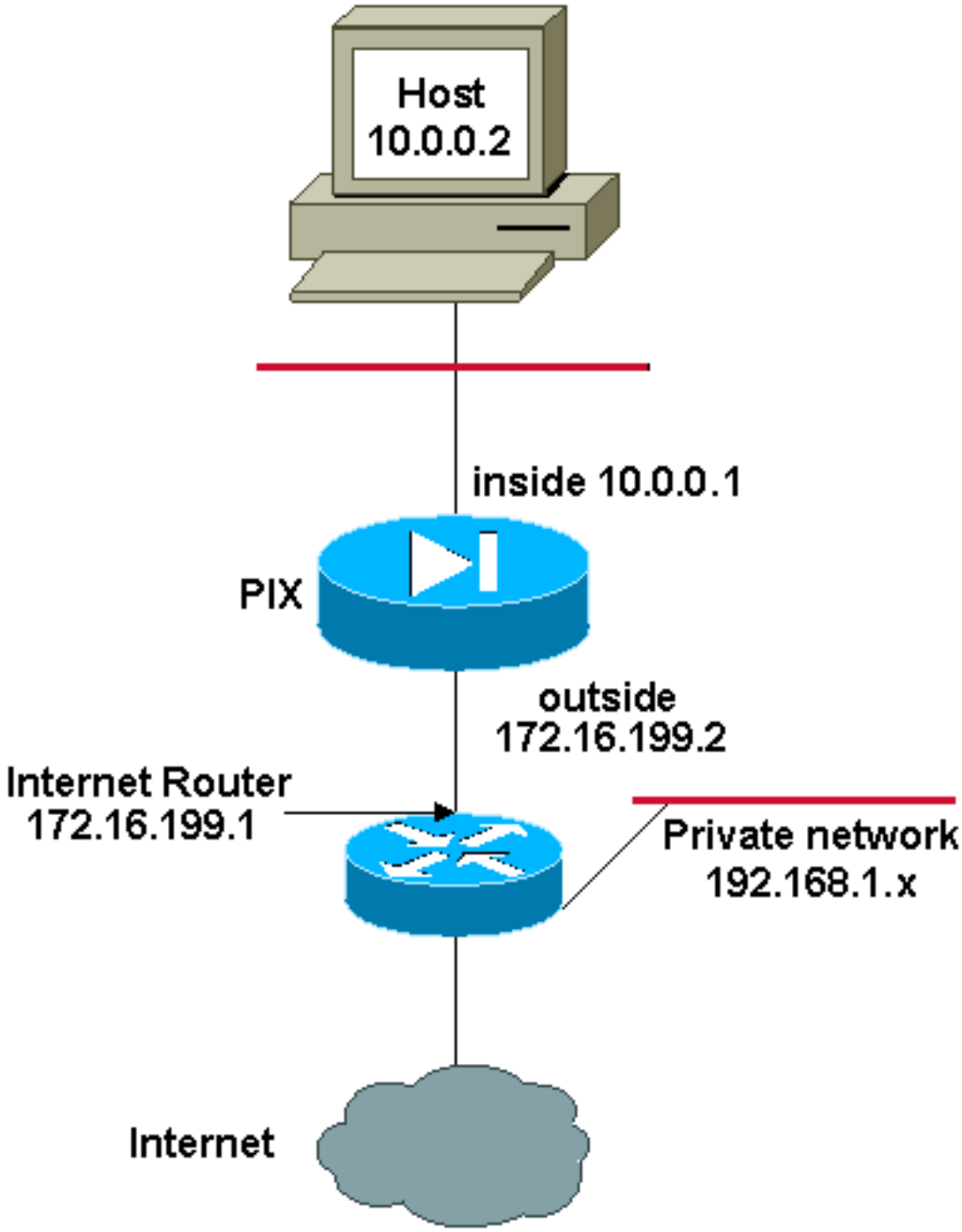
```
global (outside) 1 172.16.199.3-172.16.199.61 netmask 255.255.255.192

global (outside) 1 172.16.199.62 netmask 255.255.255.192

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

ترشد هذه الأوامر PIX/ASA لترجمة عنوان المصدر إلى 172.16.199.3 حتى 172.16.199.61 لأول 59 مستخدما داخليا عبروا PIX/ASA. بعد استنفاد هذه العناوين، يترجم PIX بعد ذلك جميع عناوين المصدر التالية إلى 172.16.199.62 حتى يصبح أحد العناوين في تجمع NAT حرا.

ملاحظة: يتم إستخدام مخطط عنونة حرف بدل في عبارة NAT. يطلب هذا البيان من PIX/ASA ترجمة أي عنوان مصدر داخلي عند خروجه إلى الإنترنت. يمكن أن يكون العنوان في هذا الأمر أكثر تحديدا إذا أردت.

عبارات متعددة ل NAT مع قائمة الوصول 0 NAT

الرسم التخطيطي للشبكة



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

في هذا المثال، يوفر ISP مدير الشبكة بنطاق من العناوين من 172.16.199.1 إلى 172.16.199.63. يقرر مدير الشبكة تخصيص 172.16.199.1 للواجهة الداخلية على موجه الإنترنت و 172.16.199.2 للواجهة الخارجية ل PIX/ASA.

ومع ذلك، في هذا السيناريو، يتم طرح مقطع آخر من شبكة LAN الخاصة خارج موجه الإنترنت. يفضل مدير الشبكة عدم هدر العناوين من التجمع العالمي عندما يتحدث المضيفون في هاتين الشبكتين مع بعضهم البعض. لا يزال مدير الشبكة بحاجة إلى ترجمة عنوان المصدر لجميع المستخدمين الداخليين (8/10.0.0.0) عند خروجهم إلى الإنترنت.

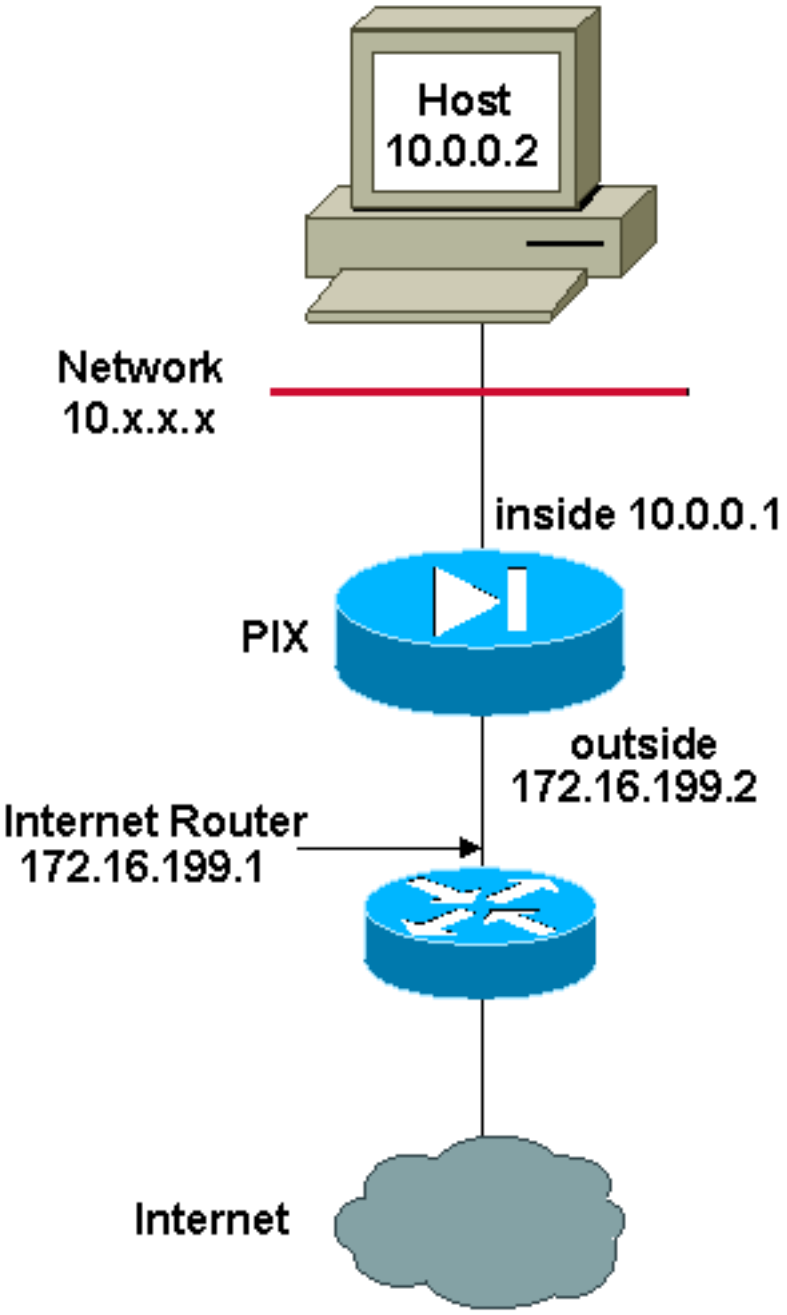
```
access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0

global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 access-list 101
```

```
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```
لا يترجم هذا تشكيل هذا عنوان أن مع مصدر عنوان 8/10.0.0.0 وغاية عنوان 24/192.168.1.0. وهو يترجم عنوان المصدر من أي حركة مرور تبدأ من داخل شبكة 8/10.0.0.0 وتكون موجهة إلى أي مكان آخر غير 24/192.168.1.0 إلى عنوان من النطاق 172.16.199.3 إلى 172.16.199.62.

إن يتلقى أنت الإنتاج من **كتابة terminal** أمر من ك cisco أداة، أنت يستطيع استعملت الإنتاج مترجم أداة (يسجل زبون فقط).

إستخدام سياسة NAT

الرسم التخطيطي للشبكة



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

عندما يستعمل أنت منفذ قائمة مع ال **nat** أمر ل أي nat id آخر غير 0، بعد ذلك أنت يمكن سياسة nat.

ملاحظة: أدخلت السياسة NAT في الإصدار 6-3-2.

يسمح سياسة nat أنت أن يعين حركة مرور محلي لعنوان ترجمة عندما أنت تعين المصدر وغاية عنوان (أو ميناء) في قائمة منفذ. يستعمل NAT عادي مصدر عنوان/ميناء فقط، حيث السياسة nat يستعمل على حد سواء مصدر وغاية عنوان/ميناء.

ملاحظة: جميع أنواع NAT لدعم سياسة دعم NAT باستثناء إستثناء nat. (**nat 0 access list**) NAT يستعمل إستثناء قائمة تحكم منفذ in order to عينت العنوان محلي، غير أن يختلف من سياسة nat في أن الميناء لا يعتبر.

مع سياسة nat، أنت يستطيع خلقت يتعدد nat أو جمل ساكن إستاتيكي أن يعين ال نفسه عنوان محلي بما أن المصدر/ميناء وغاية/ميناء خليط فريد لكل جملة. أنت يستطيع بعد ذلك طابقت عنوان مختلف إلى كل مصدر/ميناء وغاية/ميناء زوج.

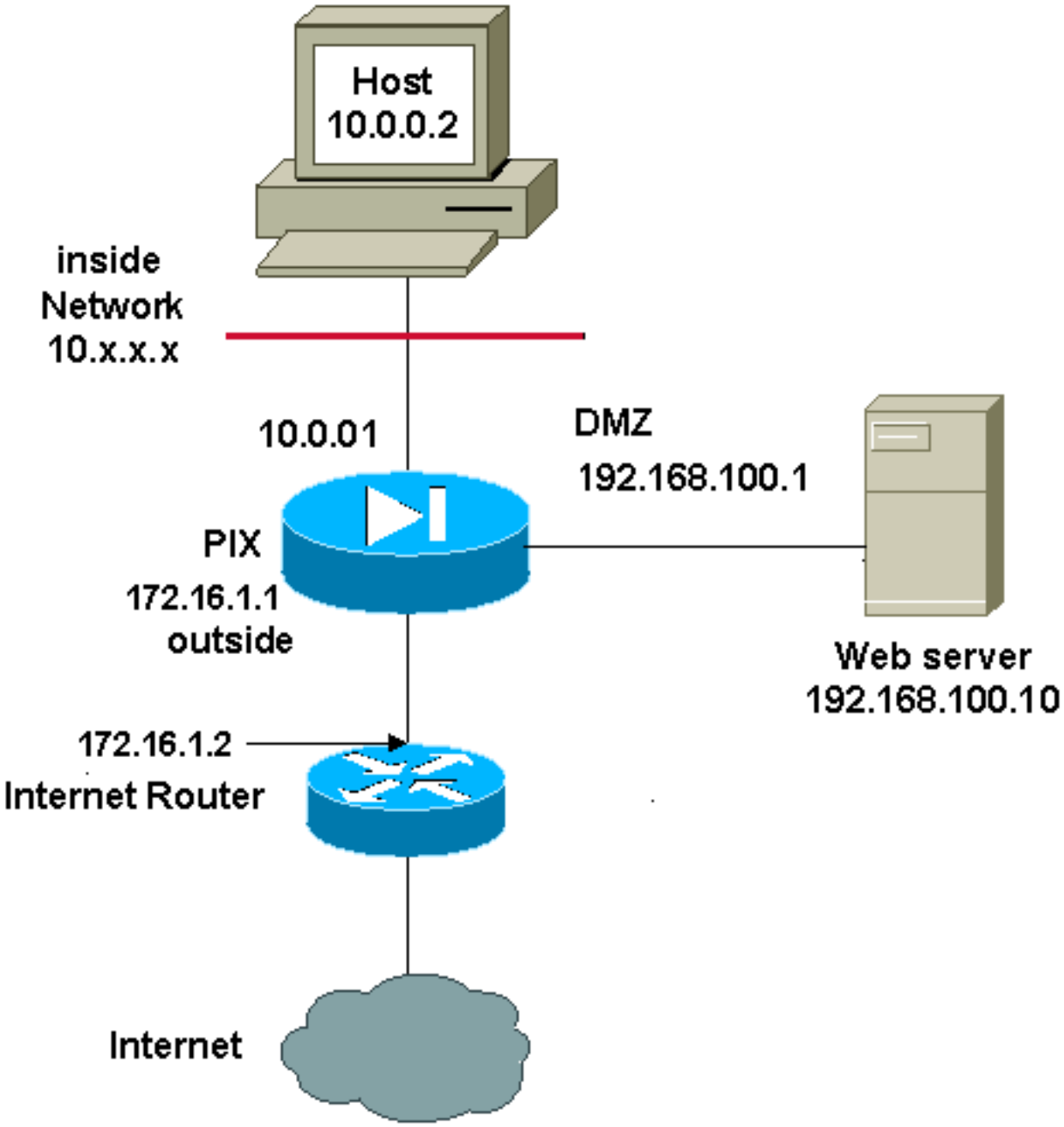
في هذا المثال، يوفر مدير الشبكة الوصول إلى عنوان IP للوجهة 192.168.201.11 للمنفذ 80 (الويب) والمنفذ 23 (Telnet)، ولكن يجب إستخدام عنواني IP مختلفين كعنوان مصدر. يتم إستخدام عنوان IP 172.16.199.3 كعنوان مصدر للويب. يتم إستخدام عنوان IP 172.16.199.4 ل Telnet، ويجب أن يقوم بتحويل جميع العناوين الداخلية، الموجودة في نطاق 8/10.0.0.0. يمكن لمدير الشبكة القيام بذلك باستخدام:

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
eq 80 255.255.255.255

access-list TELNET permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
eq 23 255.255.255.255

nat (inside) 1 access-list WEB

nat (inside) 2 access-list TELNET

global (outside) 1 172.16.199.3 netmask 255.255.255.192

global (outside) 2 172.16.199.4 netmask 255.255.255.192
```

أنت يستطيع استعملت إنتاج مترجم أداة (يسجل زبون فقط) in order to عرضت ممكن إصدار ونقطة معينة.

NAT الثابت

الرسم التخطيطي للشبكة



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

تشكيل ساكن إستاتيكي nat يخلق تخطيط واحد إلى واحد ويترجم عنوان خاص إلى عنوان آخر. يقوم هذا النوع من التكوين بإنشاء إدخال دائم في جدول NAT طالما كان التكوين موجودا ويمكن الأجهزة المضيفة الداخلية والخارجية من بدء اتصال. وهذا مفيد في الغالب للمضيفين الذين يقدمون خدمات التطبيقات مثل البريد والويب و FTP وغيرها. في هذا المثال، تم تكوين عبارات NAT الثابتة للسماح للمستخدمين على الداخل والمستخدمين على الخارج بالوصول إلى خادم الويب على DMZ.

يوضح هذا الإخراج كيفية إنشاء جملة ثابتة. لاحظ ترتيب عناوين IP المعينة والحقيقية.

```
static (real_interface,mapped_interface) mapped_ip real_ip netmask mask
```

فيما يلي الترجمة الثابتة التي تم إنشاؤها لمنح المستخدمين على الواجهة الداخلية حق الوصول إلى الخادم على DMZ. هو يخلق تخطيط بين عنوان في الداخل وعنوان الخادم على ال DMZ. ويمكن للمستخدمين الموجودين بالداخل الوصول إلى الخادم الموجود على المنطقة المنزوعة السلاح من خلال العنوان الداخلي.

```
static (DMZ,inside) 10.0.0.10 192.168.100.10 netmask 255.255.255.255
```

هنا الترجمة ساكن إستاتيكي يخلق أن يعطي مستعمل على القارن خارجي منفذ إلى الخادم على ال DMZ. هو يخلق تخطيط بين عنوان على الخارج وعنوان الخادم على ال DMZ. ويمكن للمستخدمين في الخارج الوصول إلى الخادم على المنطقة المجردة من السلاح من خلال العنوان الخارجي.

```
static (DMZ,outside) 172.16.1.5 192.168.100.10 netmask 255.255.255.255
```

ملاحظة: نظرا لأن الواجهة الخارجية تحتوي على مستوى أمان أقل من DMZ، يجب أيضا إنشاء قائمة وصول للسماح للمستخدمين الموجودين على الوصول الخارجي إلى الخادم على DMZ. يجب أن تمنح قائمة الوصول المستخدمين حق الوصول إلى **العنوان المعين** في الترجمة الثابتة. يوصى بأن تكون قائمة الوصول هذه محددة قدر الإمكان. في هذه الحالة، يسمح لأي مضيف بالوصول إلى المنافذ 80 (www/http) و 443 (https) فقط على خادم الويب.

```
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq www
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq https
```

ويجب بعد ذلك تطبيق قائمة الوصول على الواجهة الخارجية.

```
access-group OUTSIDE in interface outside
```

ارجع إلى access-list extended وaccess-group للحصول على مزيد من المعلومات حول أوامر **access-list** و**access-group**.

كيفية تجاوز NAT

يوضح هذا القسم كيفية تجاوز NAT. أنت أمكن أردت أن يتجاوز NAT عندما أنت يمكن nat تحكم. أنت يستطيع استعملت هوية nat، هوية ساكن إستاتيكي nat، أو nat إعفاء in order to تجاوزت NAT.

تكوين NAT للهوية

يترجم هوية nat العنوان حقيقي إلى ال نفسه عنوان. يمكن فقط للمضيفين "المترجمين" إنشاء ترجمات NAT، ويتم السماح بحركة المرور المستجيبة مرة أخرى.

ملاحظة: إذا قمت بتغيير تكوين NAT، ولا تريد الانتظار حتى تنتهي الترجمات الموجودة قبل إستخدام معلومات NAT الجديدة، فأنت تستخدم الأمر **clear xlate** لمسح جدول الترجمة. ومع ذلك، يتم قطع اتصال كافة الاتصالات الحالية التي تستخدم الترجمات عند مسح جدول الترجمة.

دخلت in order to شكلت هوية nat، هذا أمر:

```
hostname(config)#nat (real_interface) 0 real_ip
mask [dns] [outside] [norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp]
[udp_max_conns
```

مثلا، دخلت in order to استعملت هوية nat لداخل 24/10.1.1.0 شبكة، هذا أمر:

```
hostname(config)#nat (inside) 0 10.1.1.0
255.255.255.0
```

راجع Cisco Security Appliance Command Reference، الإصدار 7.2 للحصول على مزيد من المعلومات حول الأمر **nat**.

تكوين NAT للهوية الثابتة

هوية ساكن إستاتيكي nat يترجم العنوان حقيقي إلى ال نفسه عنوان. تكون الترجمة نشطة دائما، ويمكن لكل من "translate" والمضيفين البعيدين إنشاء إتصالات. NAT للهوية الثابتة يتيح لك إستخدام NAT عادي أو nat للسياسة. السياسة nat يسمح أنت عينت الحقيقي والوجهة عنوان عندما يعين العنوان حقيقي أن يترجم (راجع إستعمال سياسة nat قسم ل كثير معلومة حول سياسة nat). على سبيل المثال، يمكنك إستخدام هوية ثابتة للسياسة NAT لعنوان داخلي عندما يصل إلى الواجهة الخارجية والوجهة هي الخادم A، ولكن أستخدم ترجمة عادية عند الوصول إلى الخادم الخارجي B.

ملاحظة: إذا قمت بإزالة أمر ساكن إستاتيكي، فلن تتأثر الاتصالات الحالية التي تستخدم الترجمة. لإزالة هذه الاتصالات، أدخل الأمر clear local-host. لا يمكنك مسح الترجمات الثابتة من جدول الترجمة باستخدام الأمر **clear xlate**؛ يجب عليك إزالة الأمر الثابت بدلا من ذلك. يمكن إزالة الترجمات الديناميكية فقط التي تم إنشاؤها بواسطة الأمر nat والأمر العام باستخدام الأمر clear xlate.

لتكوين هوية ثابتة للنهج NAT، أدخل هذا الأمر:

```
hostname(config)#static
[real_interface,mapped_interface) real_ip access-list acl_id [dns)
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

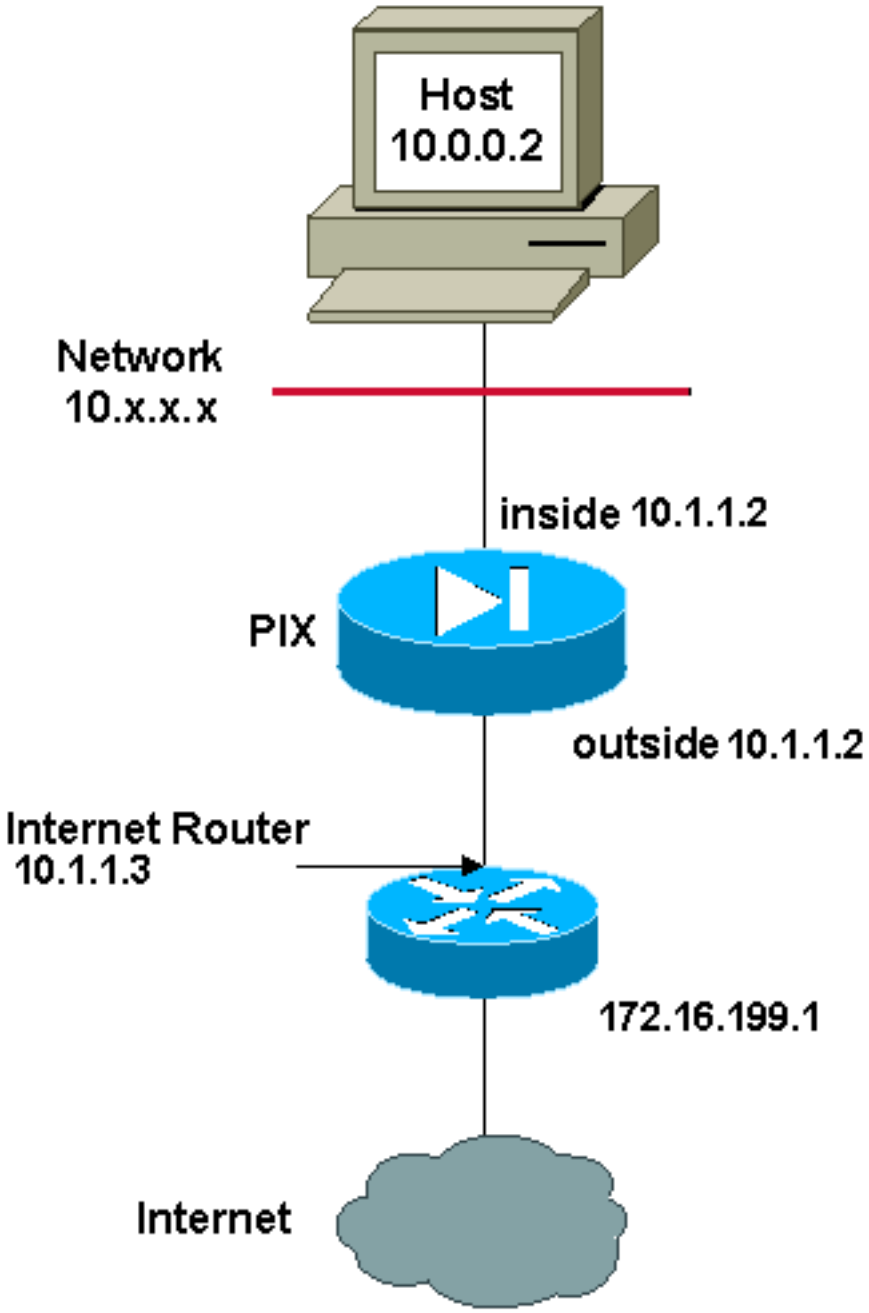
أستخدم الأمر **access-list extended** لإنشاء قائمة الوصول الموسعة. يجب أن تتضمن قائمة الوصول هذه إدخالات التحكم في الوصول (ACEs) المسموح بها فقط. تأكد من تطابق عنوان المصدر في قائمة الوصول مع real_ip في هذا الأمر. لا يعتبر Policy NAT الكلمات الأساسية غير النشطة أو المدى الزمني؛ تعتبر جميع إدخالات التحكم في الوصول (ACE) نشطة لتكوين NAT للنهج. راجع قسم إستخدام سياسة nat للحصول على مزيد من المعلومات.

دخلت in order to شكلت عادي ساكن إستاتيكي هوية NAT، هذا أمر:

```
hostname(config)#static
[real_interface,mapped_interface) real_ip real_ip [netmask mask] [dns)
norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp]
[udp_max_conns
```

حدد عنوان IP نفسه لكل من وسيطات real_ip.

الرسم التخطيطي للشبكة



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

على سبيل المثال، يستخدم هذا الأمر NAT للهوية الثابتة لعنوان IP داخلي (10.1.1.2) عند الوصول إليه من الخارج:

```
hostname(config)#static (inside,outside) 10.1.1.2
                 netmask 255.255.255.255 10.1.1.2
```

راجع مرجع أمر جهاز الأمان من Cisco، الإصدار 7.2 للحصول على مزيد من المعلومات حول الأمر **الثابت**.

يستعمل هذا أمر هوية ساكن إستاتيكي nat لعنوان خارجي (172.16.199.1) عندما ينفذ من الداخل:

```
hostname(config)#static (outside,inside) 172.16.199.1
                 netmask 255.255.255.255 172.16.199.1
```

يقوم هذا الأمر بتعيين شبكة فرعية بأكملها بشكل ثابت:

```
hostname(config)#static (inside,dmz) 10.1.1.2 10.1.1.2
netmask 255.255.255.0
```

هذا ساكن إستاتيكي هوية سياسة nat يبدي عنوان حقيقي وحيد أن يستعمل هوية nat عندما ينفذ واحد غاية عنوان و ترجمة عندما ينفذ آخر:

```
hostname(config)#access-list NET1 permit ip host
255.255.255.224 172.16.199.0 10.1.1.3
```

```
hostname(config)#access-list NET2 permit ip host
255.255.255.224 172.16.199.224 10.1.1.3
```

```
hostname(config)#static (inside,outside) 10.1.1.3
access-list NET1
```

```
hostname(config)#static (inside,outside) 172.16.199.1
access-list NET2
```

ملاحظة: للحصول على مزيد من المعلومات حول الأمر **الثابت**، ارجع إلى مرجع أمر جهاز الأمان القابل للتكيف ASA 5580 من Cisco، الإصدار 8.1.

ملاحظة: للحصول على مزيد من المعلومات حول قوائم الوصول، ارجع إلى دليل تكوين سطر أوامر جهاز الأمان القابل للتكيف ASA 5580 من Cisco، الإصدار 8.1.

تكوين إستثناء NAT

يعفي إستثناء NAT العناوين من الترجمة ويسمح لكل من الأجهزة المضيفة الحقيقية والبعيدة بإنشاء الاتصالات. NAT يسمح أنت عينت الحقيقي وغاية عنوان عندما يعين الحركة مرور حقيقي أن يعفي (مماثل إلى سياسة nat)، لذلك أنت تتلقى تحكم أكبر يستعمل إعفاء nat من هوية nat. ومع ذلك، وعلى عكس النهج NAT، لا يعتبر إستثناء NAT المنافذ في قائمة الوصول. استعملت هوية ساكن إستاتيكي nat أن يعتبر ميناء في الوصول قائمة ميلان إلى جانب.

ملاحظة: إذا قمت بإزالة تكوين إستثناء NAT، فلن تتأثر الاتصالات الموجودة التي تستخدم إستثناء NAT. لإزالة هذه الاتصالات، أدخل الأمر clear local-host.

دخلت in order to شكلت nat إعفاء، هذا أمر:

```
hostname(config)#nat (real_interface) 0 access-list
[acl_name [outside
```

قم بإنشاء قائمة الوصول الموسعة باستخدام الأمر access-list extended . يمكن أن تتضمن قائمة الوصول هذه كلا من وحدات ACE المسموح بها ووحدات ACE المرفوضة. لا تحدد المنافذ الحقيقية والوجهة في قائمة الوصول؛ لا يأخذ إستثناء NAT في الاعتبار المنافذ. لا يعتبر إستثناء NAT أيضا الكلمات الأساسية غير النشطة أو المدى الزمني؛ وتعتبر جميع إدخالات التحكم في الوصول (ACE) نشطة لتكوين إعفاء NAT.

بشكل افتراضي، يعفي هذا الأمر حركة المرور من الداخل إلى الخارج. إن يريد أنت حركة مرور من الخارج إلى الداخل أن يتجاوز NAT، بعد ذلك أضفت إضافي **nat** أمر ودخلت خارج أن يعين ال nat مثيل بما أن خارج NAT. أنت أمكن أردت أن يستعمل خارجي nat إعفاء إن يشكل أنت حركي nat للقارن خارجي وتريد أن يعفي آخر حركة مرور.

على سبيل المثال، لإعفاء شبكة داخلية عند الوصول إلى أي عنوان وجهة، أدخل هذا الأمر:

```
hostname(config)#access-list EXEMPT permit ip 10.1.1.0
                                              any 255.255.255.0


hostname(config)# nat (inside) 0 access-list
                                              EXEMPT
```

دخلت in order to استعملت حركي خارج NAT لشبكة DMZ، وأعفت آخر DMZ شبكة، هذا أمر:

```
hostname(config)#nat (dmz) 1 10.1.1.0 255.255.255.0
                                              outside dns


hostname(config)#global (inside) 1
                                              10.1.1.2


hostname(config)#access-list EXEMPT permit ip 10.1.1.0
                                              any 255.255.255.0


hostname(config)#nat (dmz) 0 access-list
                                              EXEMPT
```

دخلت in order to أعفيت عنوان داخلي عندما ينفذ إثنان مختلف غاية عنوان، هذا أمر:

```
hostname(config)#access-list NET1 permit ip 10.1.1.0
                                      255.255.255.224 172.16.199.0 255.255.255.0


hostname(config)#access-list NET1 permit ip 10.1.1.0
                                    255.255.255.224 172.16.199.224 255.255.255.0


hostname(config)#nat (inside) 0 access-list NET1
```

التحقق من الصحة

حركة المرور التي تتدفق من خلال جهاز الأمان تخضع على الأرجح ل NAT. ارجع إلى PIX/ASA: مراقبة مشاكل الأداء واستكشاف أخطائها وإصلاحها للتحقق من الترجمات المستخدمة على جهاز الأمان.

يعرض الأمر **show xlate count** عدد الترجمات الحالي والأقصى عدد من خلال PIX. الترجمة هو تخطيط لعنوان داخلي إلى عنوان خارجي ويمكن أن يكون تخطيط من واحد إلى واحد، مثل NAT، أو تخطيط من عدة إلى واحد، مثل PAT. هذا الأمر هو مجموعة فرعية من الأمر **show xlate** ، والذي ينتج كل ترجمة من خلال PIX. يعرض إخراج الأمر الترجمات "قيد الاستخدام"، التي تشير إلى عدد الترجمات النشطة في PIX عند إصدار الأمر؛ يشير "الأكثر إستخداما" إلى الحد الأقصى للترجمات التي تم رؤيتها على PIX منذ تشغيله.

استكشاف الأخطاء وإصلاحها

خطأ إستلمت رسالة عندما يضيف ضرب ساكن إستاتيكي للميناء 443

المشكلة

أنت تستلم هذا خطأ رسالة عندما أنت تضيف ضرب ساكن إستاتيكي لميناء 443:

```
TCP 443 192.168.1.87 443 netmask 255.255.255.255 tcp 0 udp 0  ( )  []

443

:
```

الحل

تحدث رسالة الخطأ هذه عندما يتم تشغيل ASDM أو WebVPN على منفذ 443. لحل هذه المشكلة، قم بتسجيل الدخول إلى جدار الحماية، وإكمال إحدى الخطوات التالية:

- دخلت in order to غيرت ال ASDM ميناء إلى أي شيء غير 443، هذا أمر:
```
ASA(config)#no http server enable
ASA(config)#http server enable 8080
```

- لتغيير منفذ WebVPN إلى أي شيء آخر غير 443، قم بتشغيل الأوامر التالية:
```
ASA(config)#webvpn
ASA(config-webvpn)#enable outside
ASA(config-webvpn)#port 65010
```

عقب يركض أنت هذا أمر، أنت سوفت كنت يمكن أن يضيف nat/ضرب على ميناء 443 إلى آخر نادل. عندما تحاول إستخدام ASDM لإدارة ASA في المستقبل، حدد المنفذ الجديد على أنه 8080.

خطأ: تعارض عنوان معين مع ثابت موجود

المشكلة

أنت تستلم هذا خطأ عندما أنت تضيف عبارة ساكن إستاتيكي على ال ASA:

:

الحل

تحقق من عدم وجود إدخال بالفعل للمصدر الثابت الذي تريد إضافته.

معلومات ذات صلة

- صفحة دعم PIX
- مراجع أوامر PIX
- صفحة دعم ASA
- مراجع أوامر ASA
- 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).