ASA 8.2: إعادة توجيه المنفذ (إعادة التوجيه) باستخدام أوامر NAT و Global و Static و Access-list باستخدام ASDM

المحتويات

المقدمة

يوضح هذا المستند كيفية عمل إعادة توجيه المنفذ على جهاز الأمان القابل للتكيف (ASA) من Cisco باستخدام ASDM. وهو يتناول التحكم في الوصول لحركة المرور من خلال ASA وكيفية عمل قواعد الترجمة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- نظرة عامة على NAT
- PIX/ASA 7.x: إعادة توجيه المنفذ

المكونات المستخدمة

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

- Cisco 5500 Series ASA، الإصدار 8.2
- Cisco ASDM، الإصدار 6.3

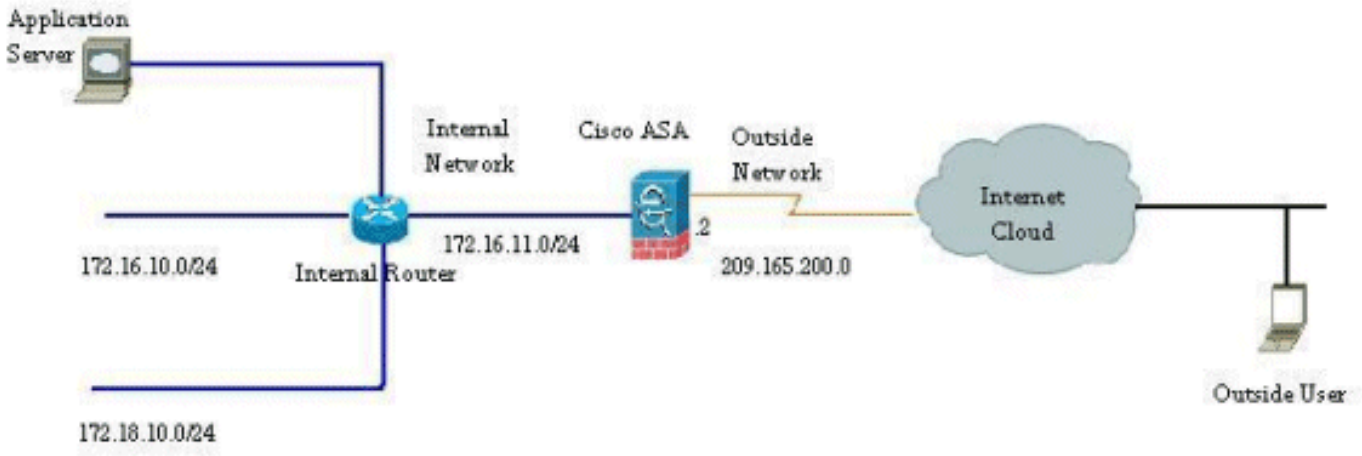
ملاحظة: يعمل هذا التكوين بشكل جيد من برنامج Cisco ASA الإصدار 8.0 إلى 8.2 فقط، نظرا لعدم وجود تغييرات رئيسية في وظيفة NAT.

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.

الرسم التخطيطي للشبكة

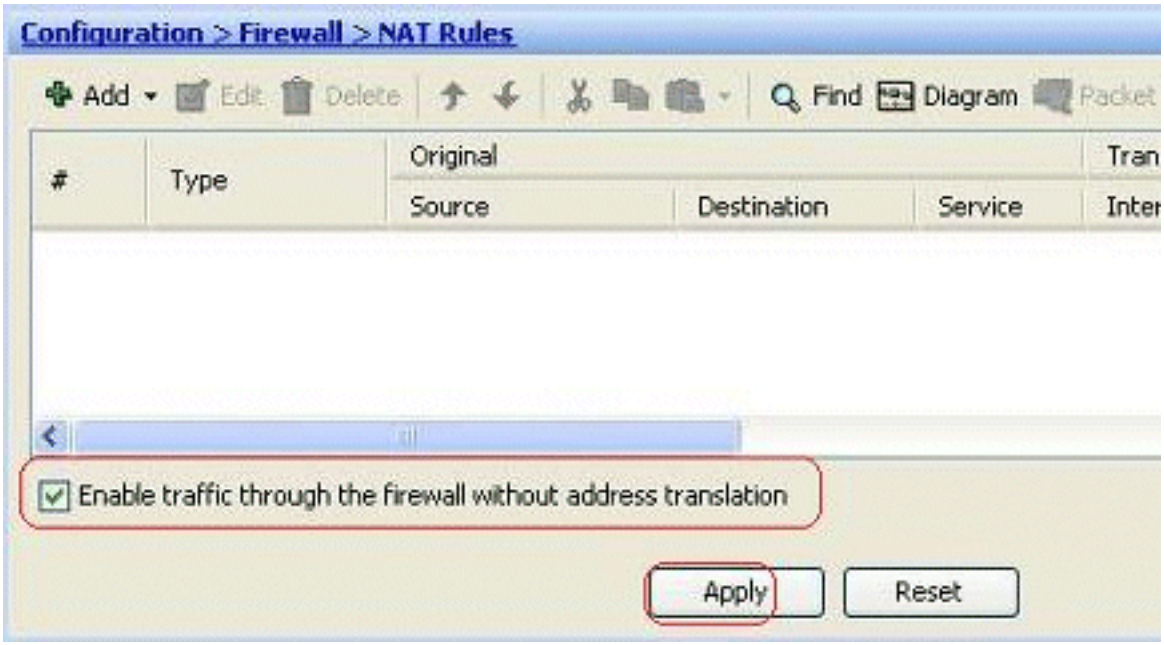


مخططات عنونة IP المستخدمة في هذا التكوين غير قابلة للتوجيه من الناحية القانونية على الإنترنت. وهي عناوين RFC 1918 التي تم استخدامها في بيئة مختبرية.

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.

لا يمكن لأي اتصال المرور عبر جهاز الأمان دون تكوين قاعدة ترجمة. ويطلق على هذه الميزة عنصر تحكم nat . توضح الصورة الموضحة هنا كيفية تعطيل هذا الإجراء من خلال ASDM للسماح بالاتصالات عبر ASA دون أي ترجمة للعنوان. ومع ذلك، إذا كان لديك أي قاعدة ترجمة تم تكوينها، فإن تعطيل هذه الميزة لا يظل صالحا لجميع حركات المرور وستحتاج إلى إستثناء الشبكات بشكل صريح من ترجمة العنوان.

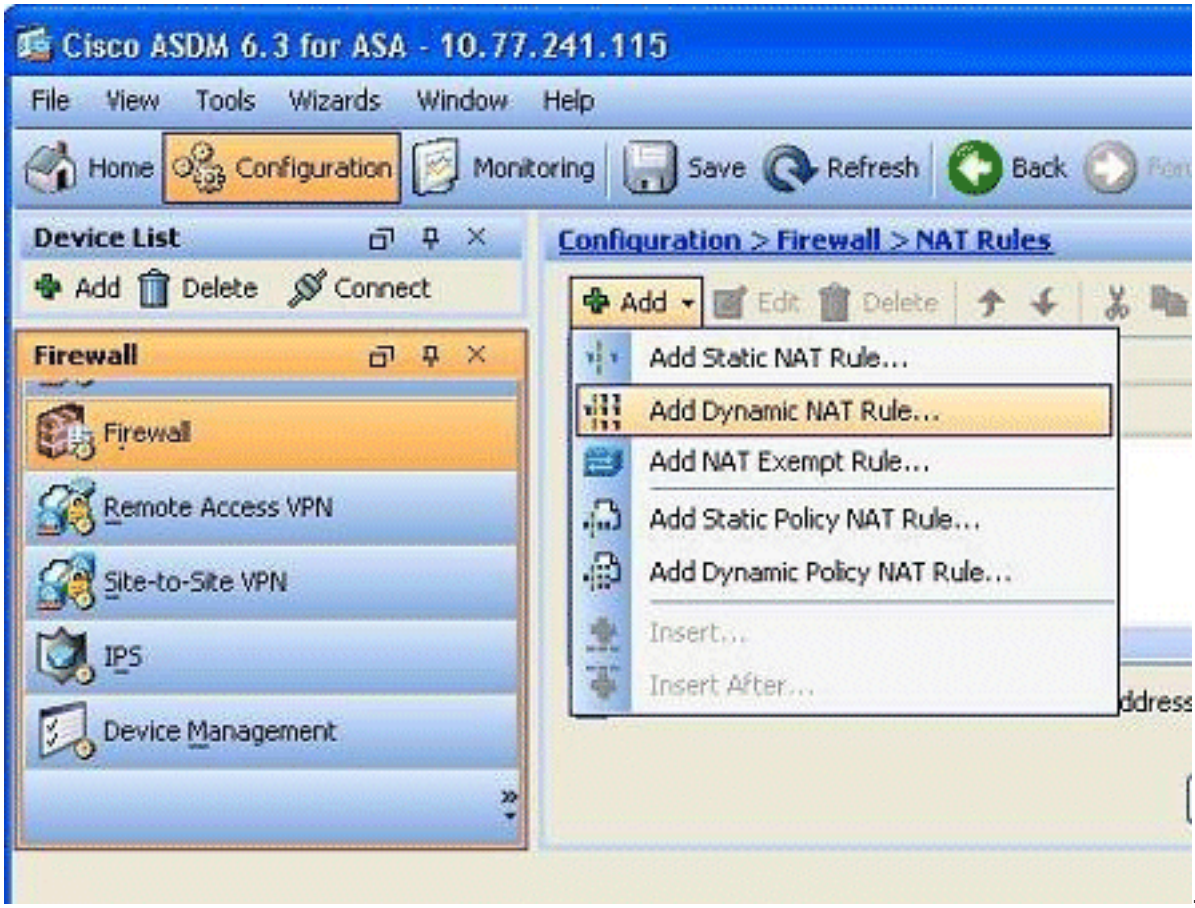


السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام NAT

أنت يستطيع سمحت مجموعة من الداخل مضيف/شبكة أن ينفذ العالم خارجي ب يشكل الحركي nat قاعدة. ومن أجل تحقيق ذلك، يلزمك تحديد العنوان الحقيقي للمضيفين/الشبكات التي سيتم منحها حق الوصول ومن ثم يتعين تعيينها إلى تجمع من عناوين IP المترجمة.

أتمت هذا steps in order to سمحت داخلي مضيف منفذ إلى شبكة خارجية مع NAT:

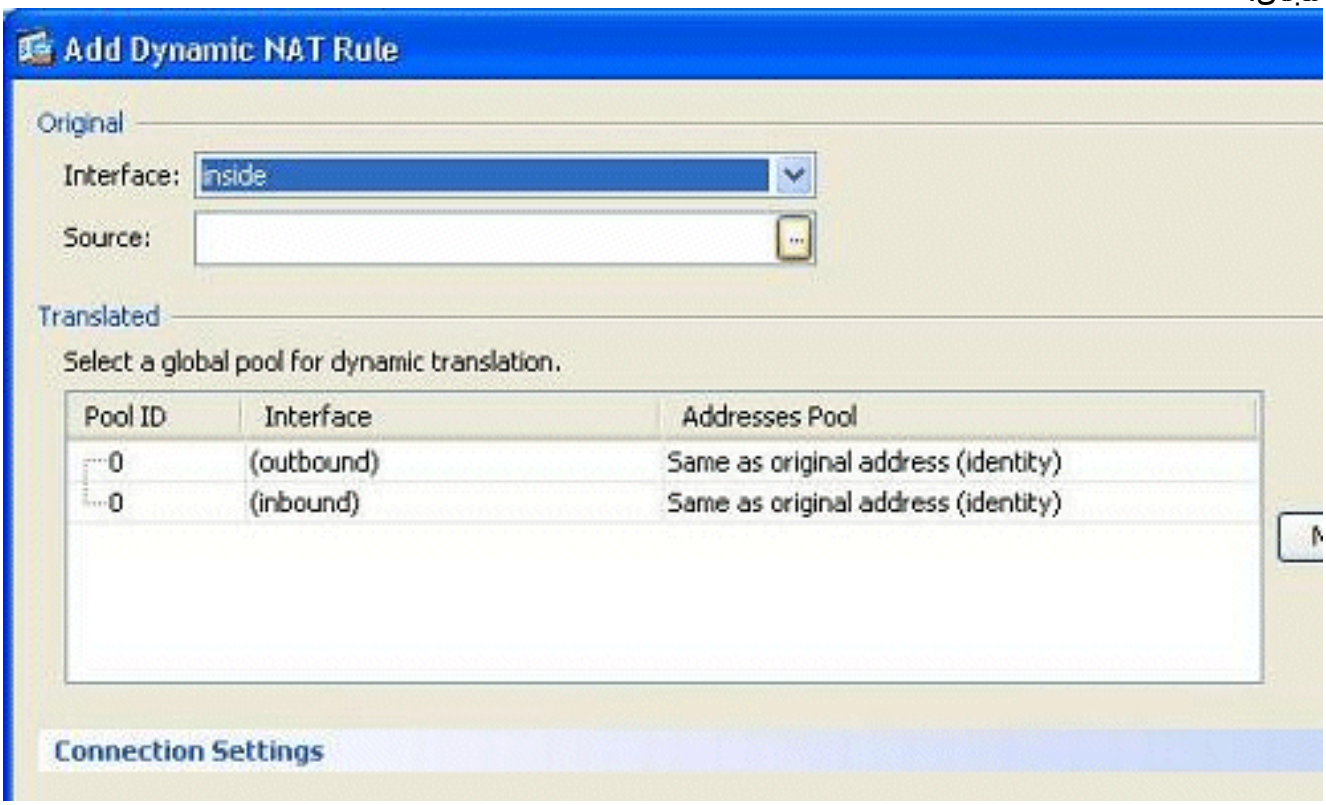
1. انتقل إلى التكوين > **جدار الحماية>قواعد NAT**، انقر **إضافة**، ثم أختر **خيار إضافة قاعدة NAT الديناميكية** لتكوين قاعدة NAT



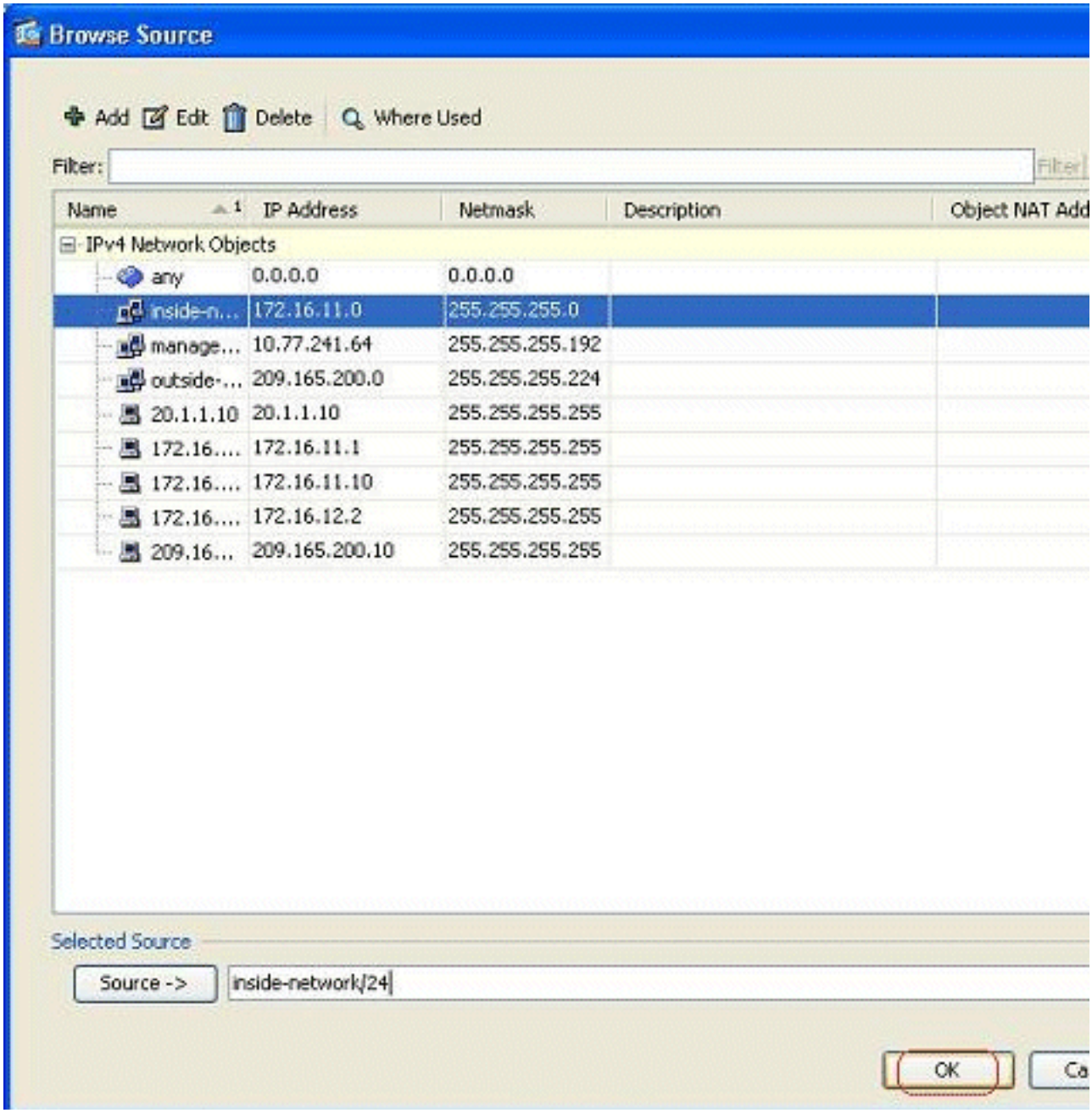
الديناميكية.

2. أخترت الإسم من القارن إلى أي المضيف حقيقي يكون ربطت. أخترت العنوان حقيقي من المضيف/شبكة

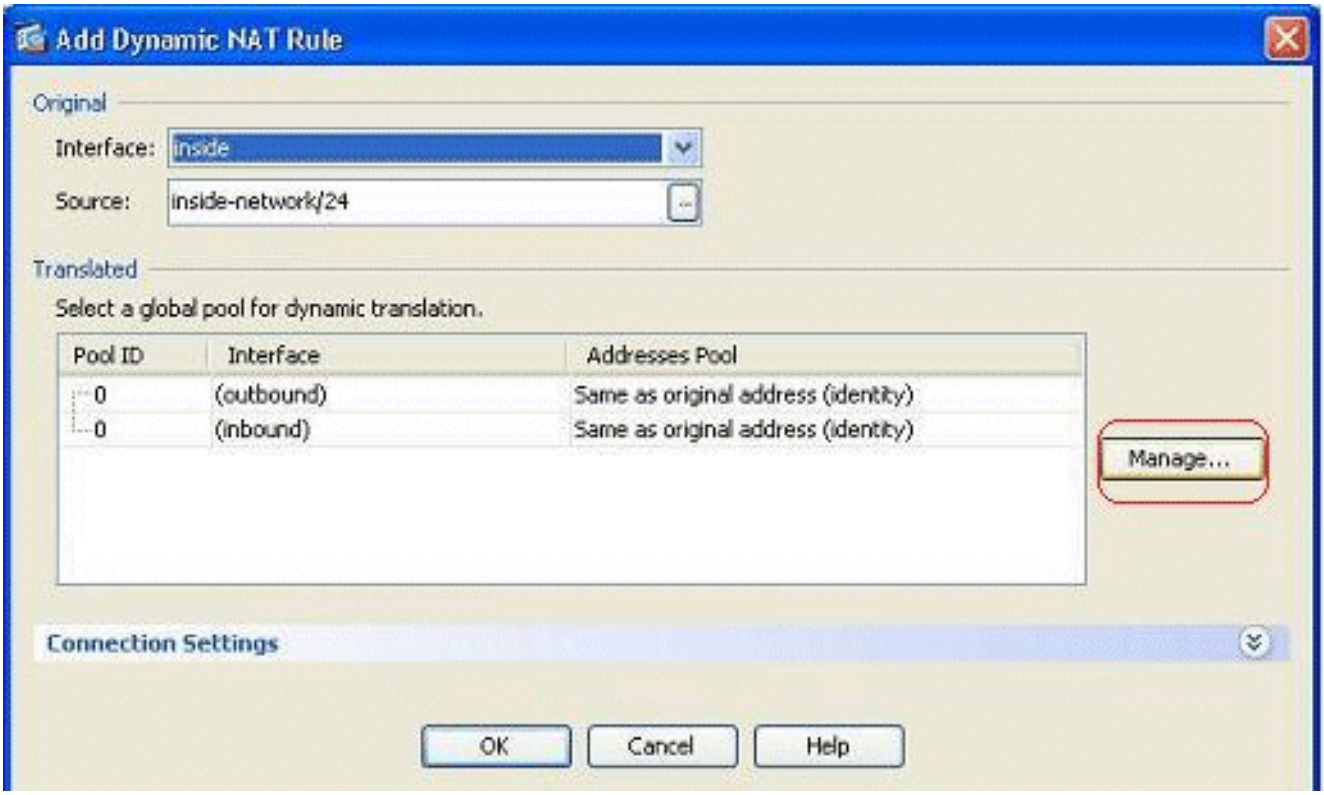
يستعمل ال **تفاصيل** زر في **المصدر**
مجال.



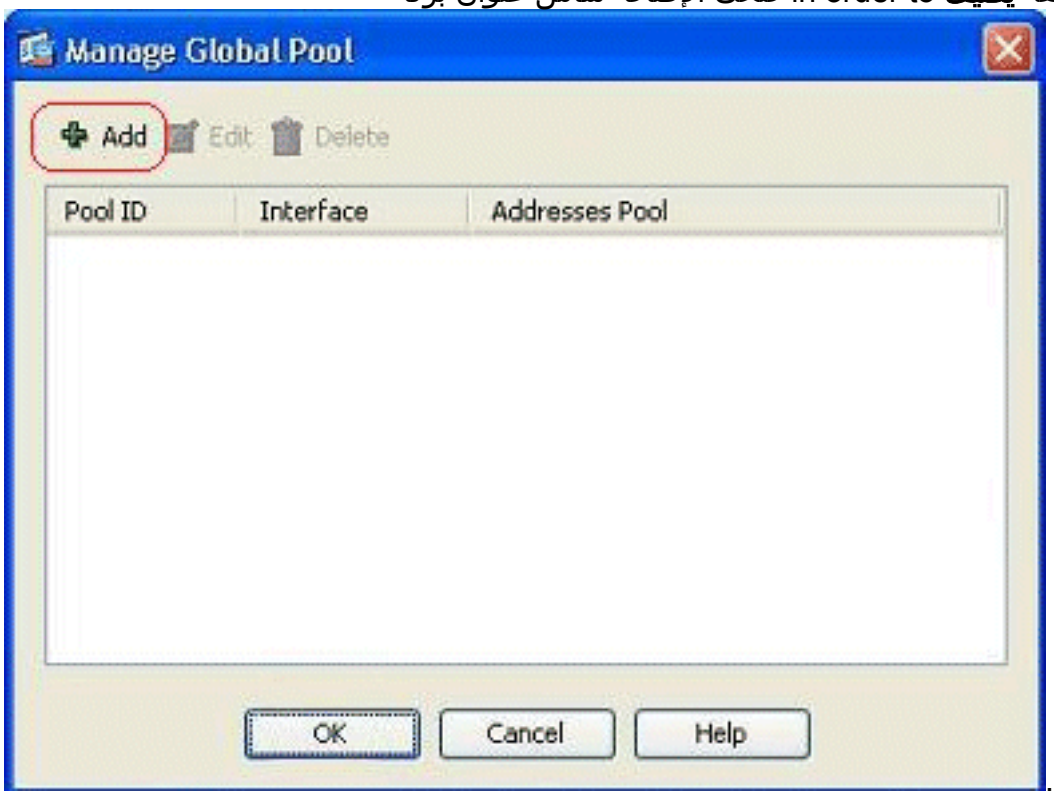
3. في هذا المثال، تم تحديد *الشبكة الداخلية* بالكامل. انقر فوق **موافق** لإكمال التحديد.



4. انقر فوق **إدارة** لتحديد تجمع عناوين IP التي سيتم تعيين الشبكة الحقيقية لها.

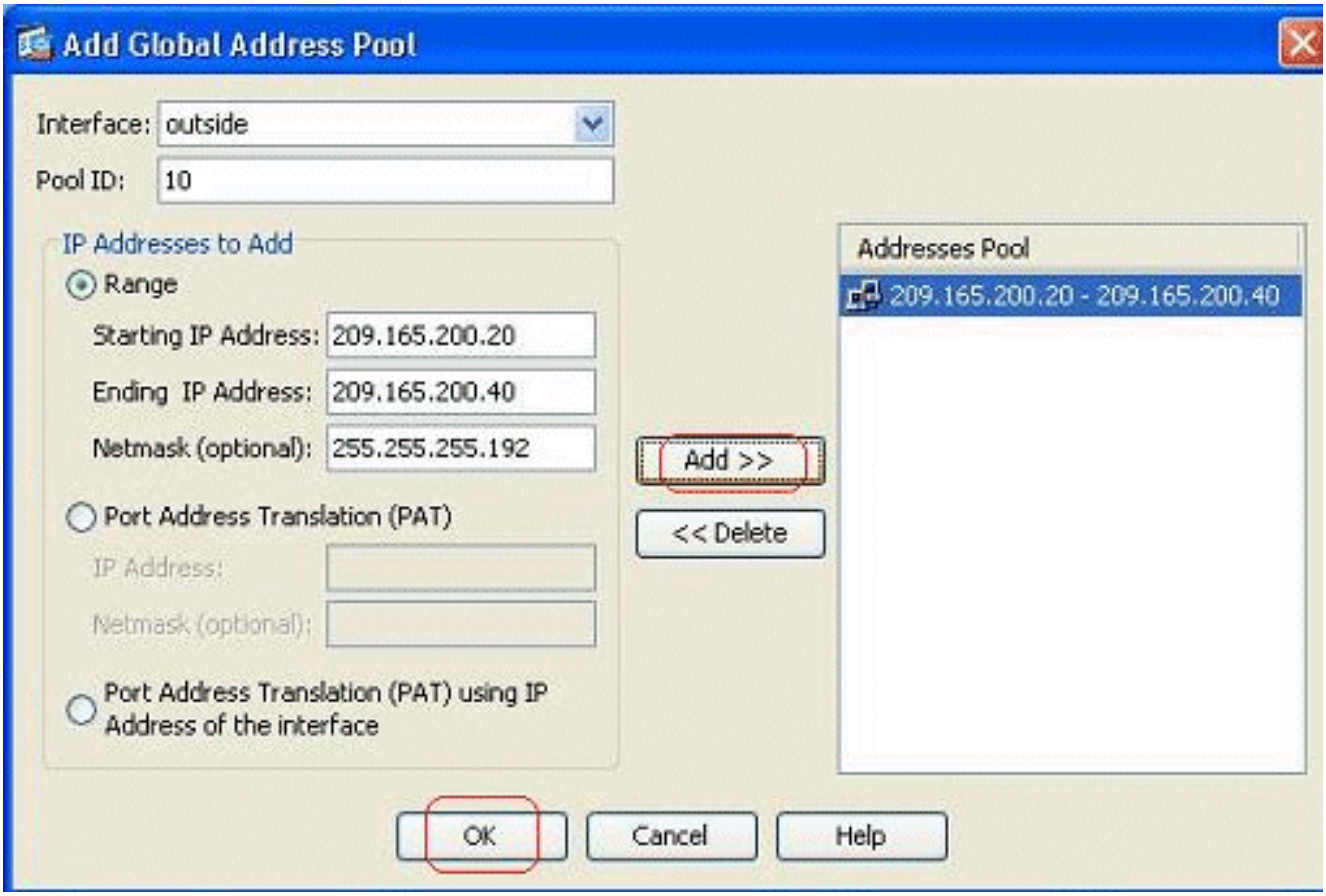


5. طقطقة **يضيف** in order to فتحت الإضافة شامل عنوان بركة

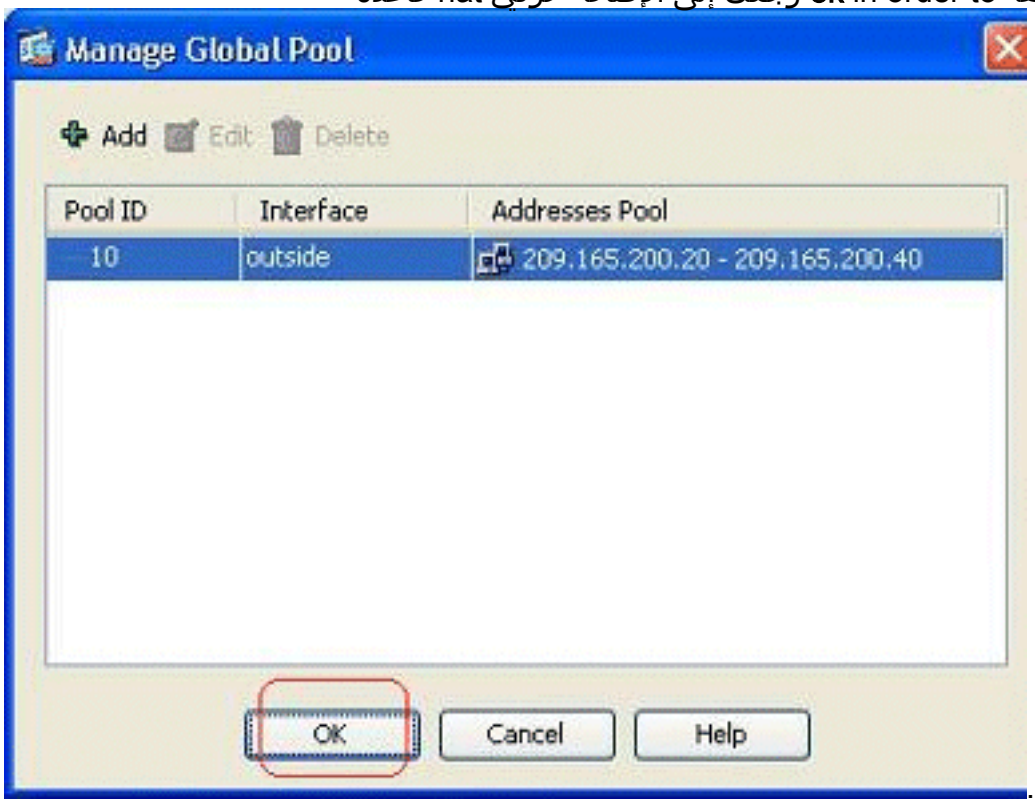


نافذة.

6. أخترت **النطاق** خيار وعينت البداية والنهاية عنوان مع المخرج قارن. عينت أيضا، فريد بركة id وطقطقة **يضيف** in order to أضفت هذا إلى العنوان بركة. طقطقة in order to **ok** رجعت إلى الإدارة بركة شامل نافذة.

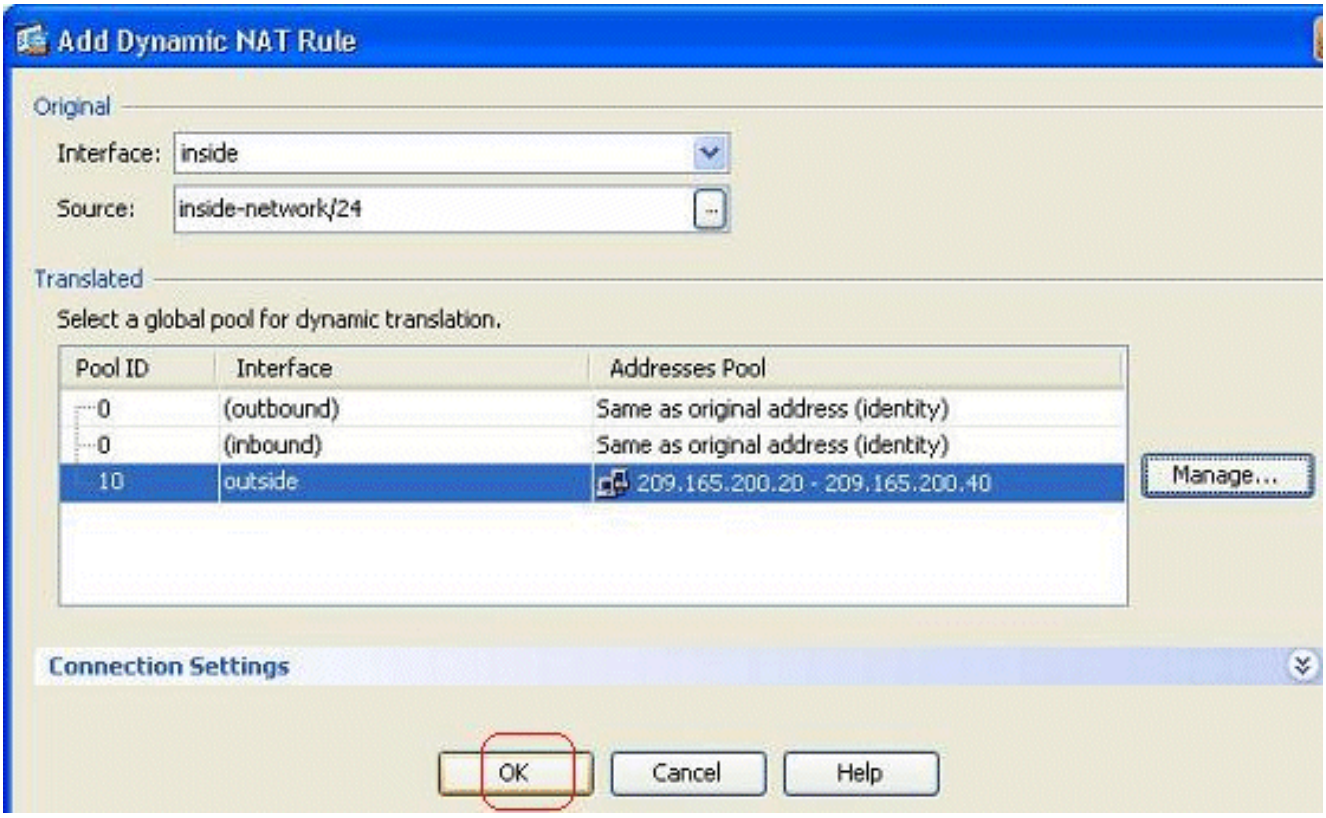


7. طقطقة **ok** in order to رجعت إلى الإضافة حركي nat قاعدة

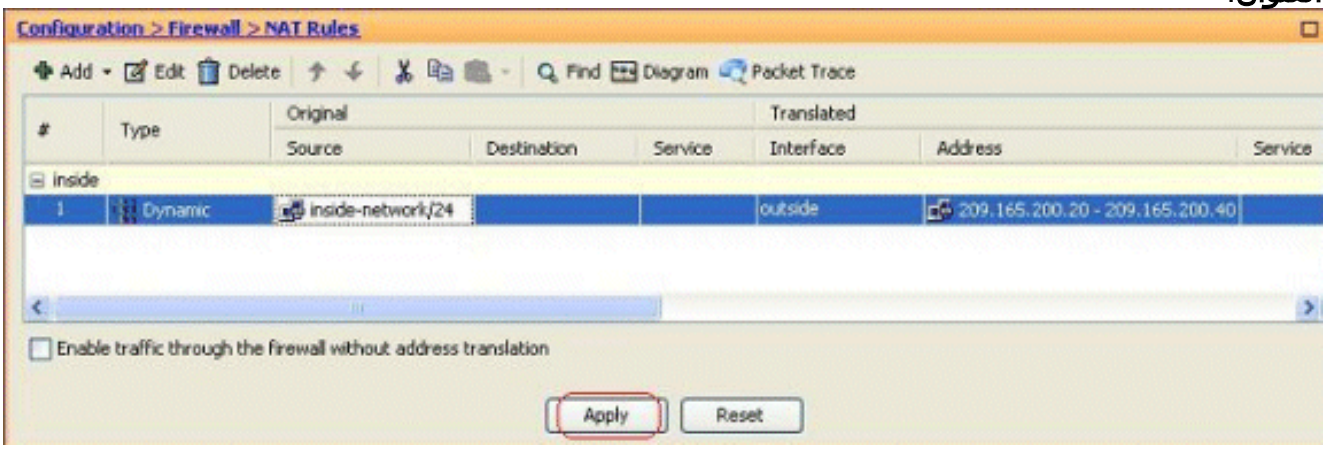


نافذة.

8. طقطقة **ok** in order to أتمت الحركي nat قاعدة تشكيل.



9. انقر فوق **تطبيق** لتفعيل التغييرات.**ملاحظة:** لا يتم تحديد خيار **تمكين حركة مرور البيانات عبر جدار الحماية بدون ترجمة العنوان**.



هذا هو إخراج واجهة سطر الأوامر (CLI) المكافئ لتكوين ASDM هذا:

```
nat-control
global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192
nat (inside) 10 172.16.11.0 255.255.255.0
```

وفقا لهذا التكوين، ستتم ترجمة الأجهزة المضيفة في شبكة 172.16.11.0 إلى أي عنوان IP من تجمع NAT، 209.165.200.20-209.165.200.40. هنا، معرف تجمع NAT مهم جدا. أنت يستطيع عينت ال نفسه nat بركة إلى آخر داخلي/dmz شبكة. إذا كان التجمع الذي تم تعيينه يحتوي على عناوين أقل من المجموعة الحقيقية، يمكن أن تنفذ العناوين إذا كان مقدار حركة المرور أكثر من المتوقع. بالنتيجة، أنت يستطيع حاولت طبقت ضرب أو أنت يستطيع حاولت أن يحرر العنوان موجود بركة أن يمدده.

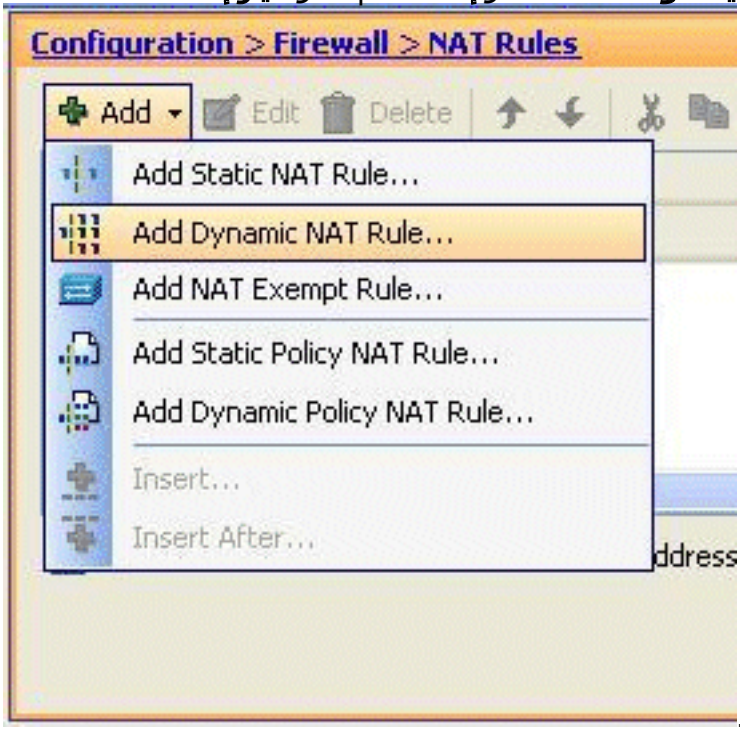
ملاحظة: أثناء إجراء أي تعديل على قاعدة الترجمة الموجودة، لاحظ أنك تحتاج إلى إستخدام الأمر clear xlate لتفعيل هذه التعديلات. وإلا، فسيظل الاتصال الموجود السابق موجودا في جدول الاتصال حتى ينتهي. توخى الحذر عند إستخدام الأمر **clear xlate**، لأنه ينهي الاتصالات الموجودة على الفور.

السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام PAT

إن يريد أنت داخل مضيف أن يشارك عنوان عام وحيد للترجمة، استعملت ضرب. إن **العالمي** يعين بيان واحد عنوان، أن عنوان يكون ميناء يترجم. يسمح ال ASA واحد ميناء ترجمة لكل قارن وأن ترجمة يساند ما يصل إلى 65،535 **نشط** كائن إلى العنوان شامل وحيد.

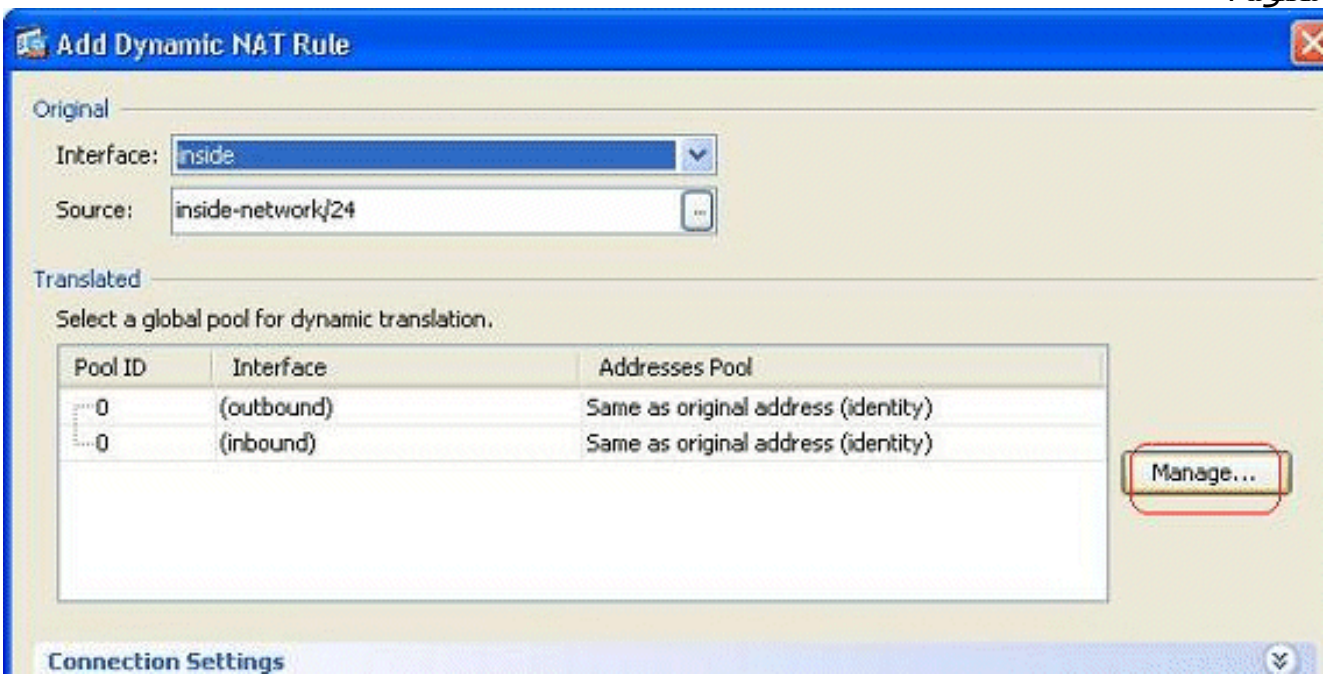
أتمت هذا steps in order to سمحت داخلي مضيف منفذ إلى شبكة خارجي مع ضرب:

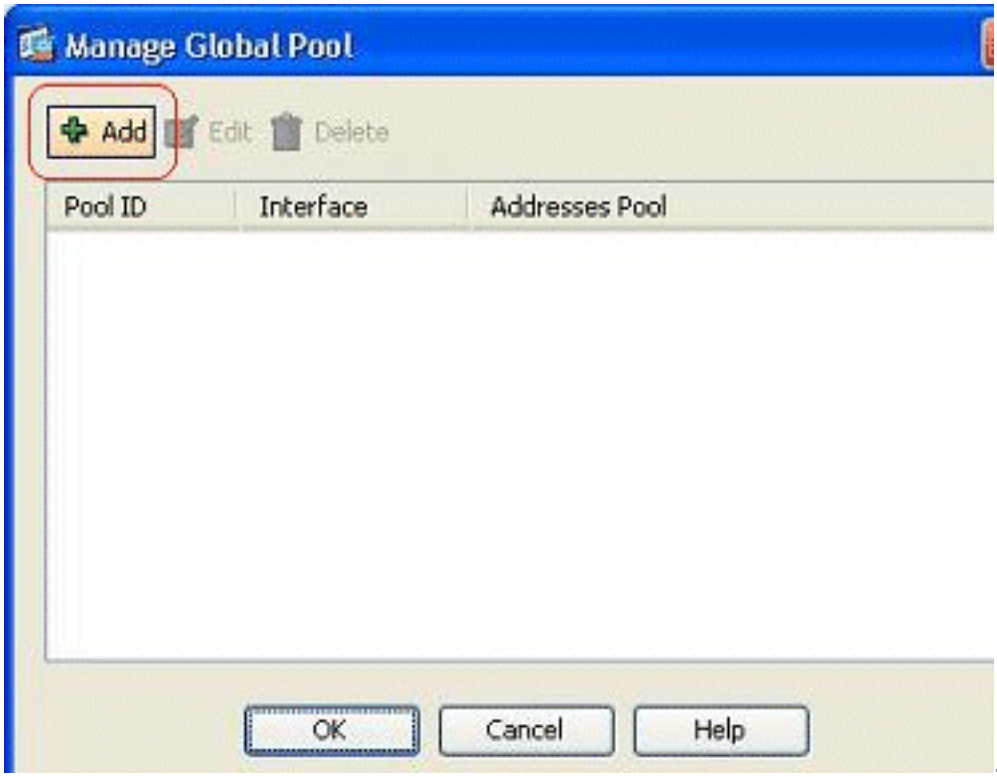
1. انتقل إلى التكوين > **جدار الحماية>قواعد NAT**، انقر **إضافة**، ثم أختر **خيار إضافة قاعدة NAT الديناميكية**



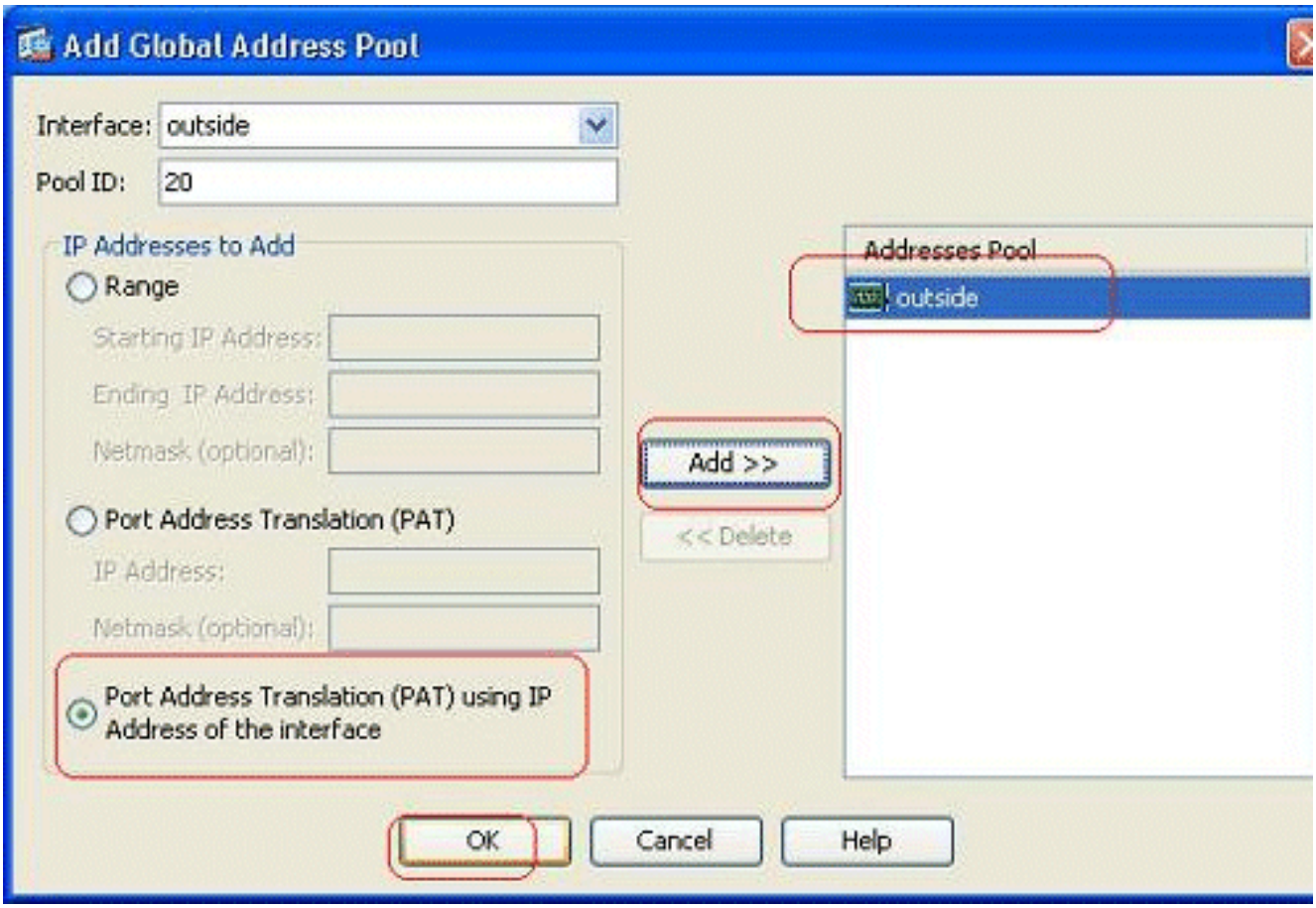
لتكوين قاعدة NAT الديناميكية.

2. أخترت الإسم من القارن إلى أي المضيف حقيقي يكون ربطت. أخترت العنوان حقيقي من المضيف/شبكة يستعمل ال **تفاصيل** زر في **المصدر** مجال، واخترت **داخل شبكة**. طقطقة **يدير** in order to عينت ال يترجم عنوان
معلومة.

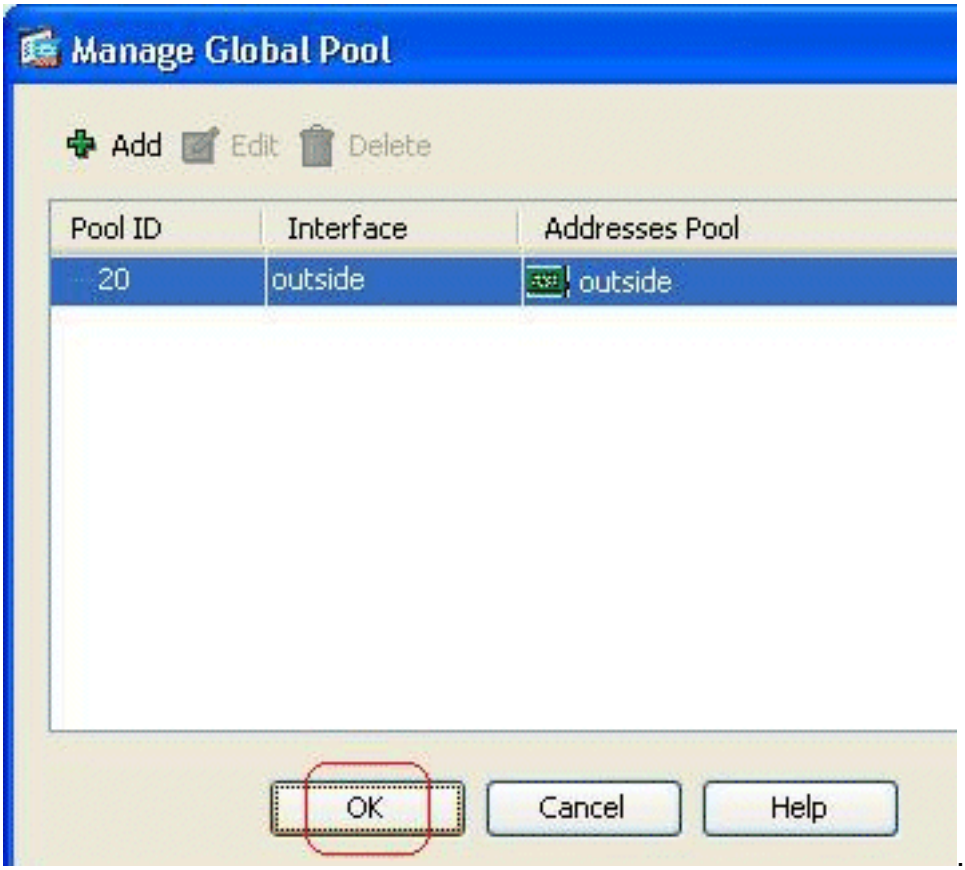




3. انقر فوق **إضافة (Add)**.
4. أخترت **الأيسر عنوان ترجمة (ضرب) يستعمل عنوان من القارن** خيار، وطقطقة **يضيف** in order to أضفت هو إلى العنوان بركة. لا تنس تعيين معرف فريد لتجمع عناوين NAT هذا.

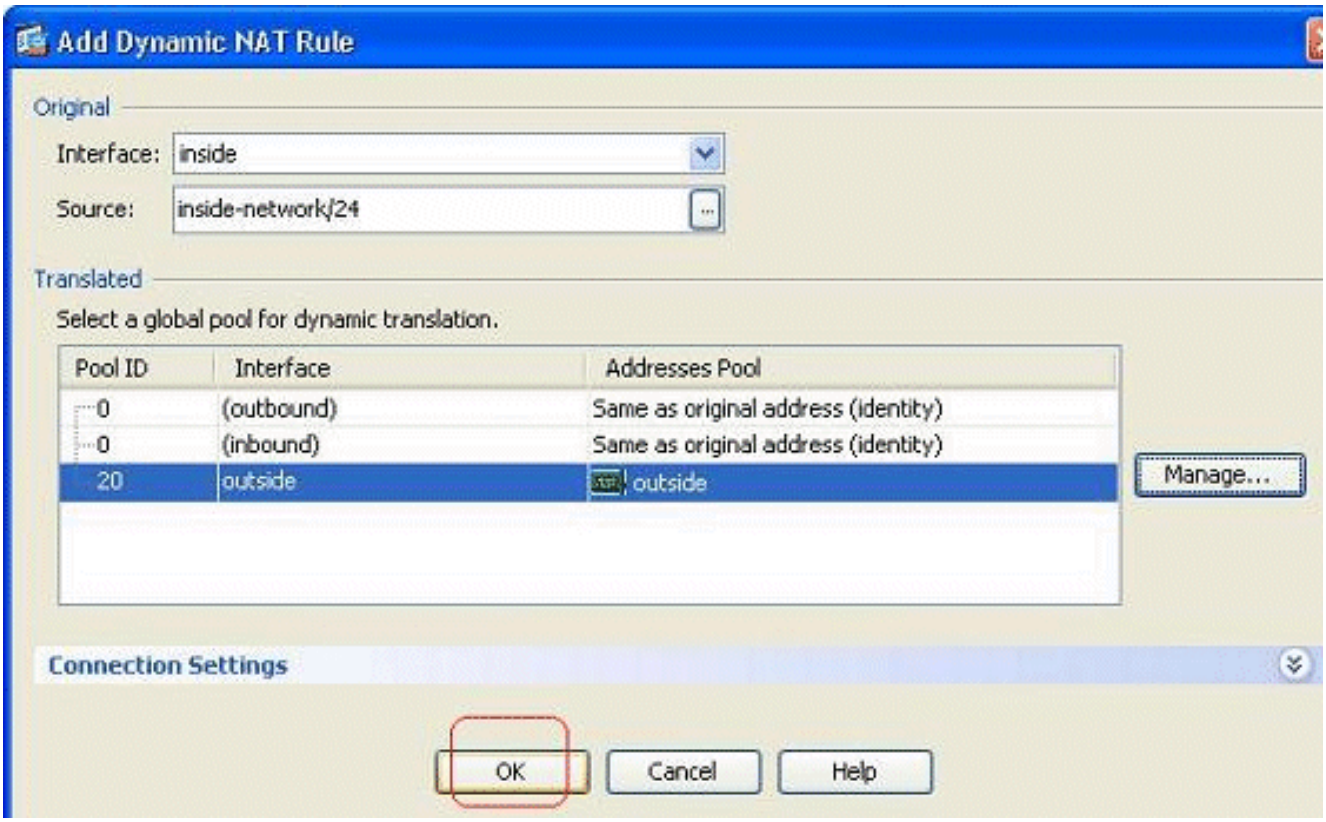


5. كما هو موضح هنا هو تجمع العناوين الذي تم تكوينه مع الواجهة الخارجية كعنوان متاح فقط في هذا التجمع. طقطقة in order to **ok** رجعت إلى الإضافة حركي nat قاعدة

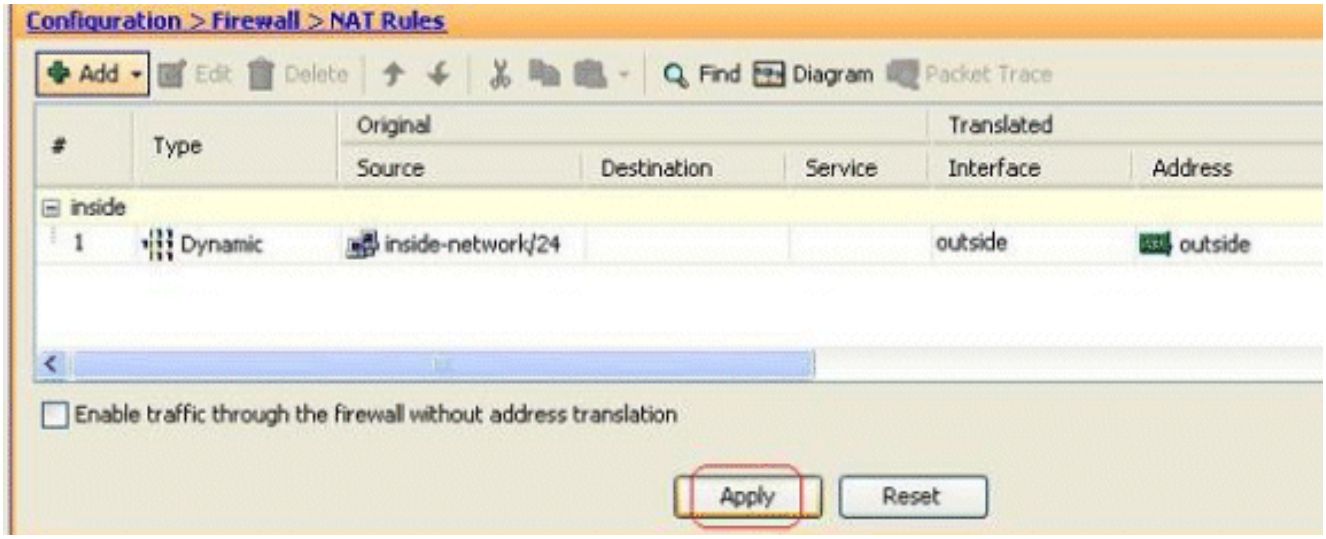


نافذة.

6. وانقر فوق
OK.



7. تظهر قاعدة NAT الديناميكية التي تم تكوينها هنا في جزء التكوين > جدار الحماية > قواعد
.nat



هذا هو مخرج CLI المكافئ لتكوين PAT هذا:

```
global (outside) 20 interface
nat (inside) 20 172.16.11.0 255.255.255.0
```

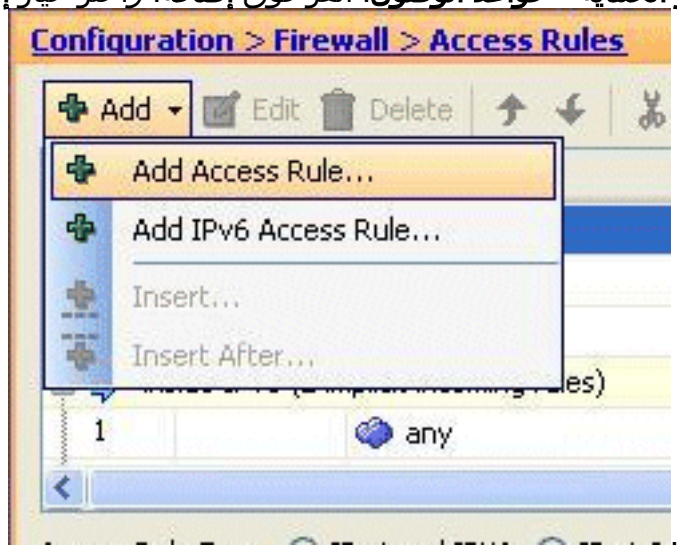
تقييد الوصول إلى الشبكات الخارجية للمضيفين الداخليين

عندما لا يتم تحديد قواعد وصول، يمكن للمستخدمين من واجهة أمان أعلى الوصول إلى أي موارد مقترنة بواجهة أمان أقل. لتقييد وصول مستخدمين معينين إلى موارد معينة، أستخدم قواعد الوصول في ASDM. يوضح هذا المثال كيفية السماح لمستخدم واحد بالوصول إلى الموارد الخارجية (باستخدام FTP و SMTP و POP3 و HTTPS و WWW) وتقييد جميع المستخدمين الآخرين من الوصول إلى الموارد الخارجية.

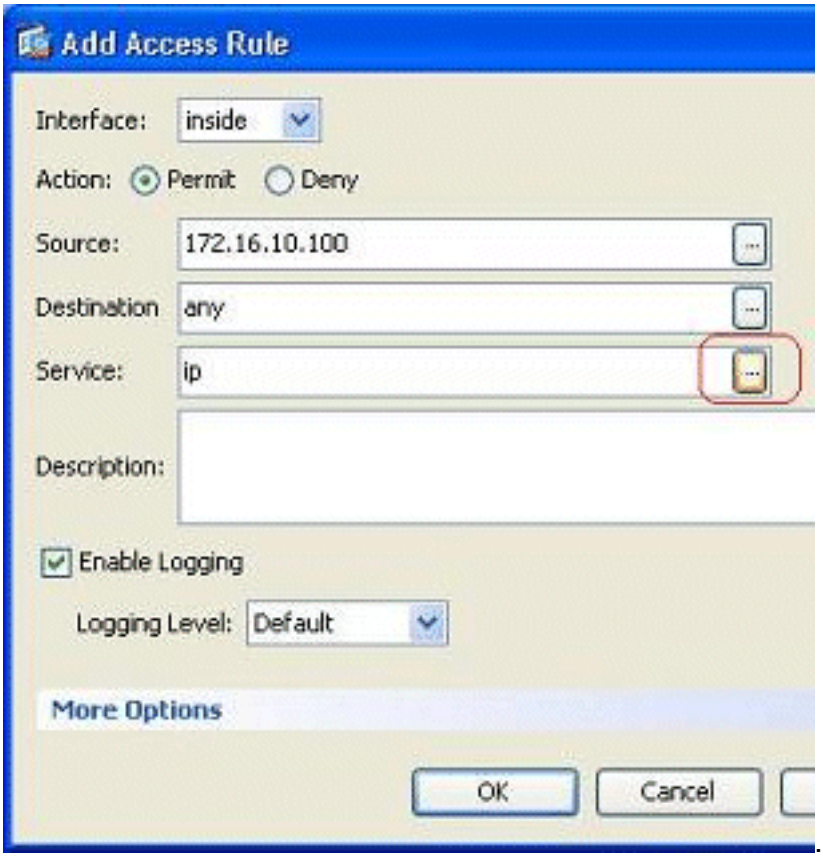
ملاحظة: ستكون هناك قاعدة "رفض ضمني" في نهاية كل قائمة وصول.

أكمل الخطوات التالية:

1. انتقل إلى التكوين > **جدار الحماية** > **قواعد الوصول**، انقر فوق **إضافة**، واختر خيار **إضافة قاعدة الوصول** لإنشاء إدخال قائمة وصول جديد.

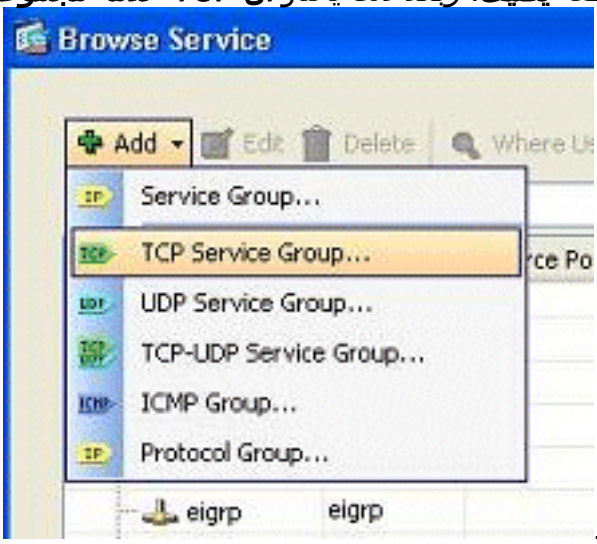


2. أخترت المصدر عنوان أن يكون سمحت في **المصدر** مجال. أخترت **any** كغاية، **داخلي** كالقارن، **يسمح** كالإجراء. أخيرا، طقطقت **ال details** زر في الخدمة مجال in order to خلقت TCP خدمة مجموعة ل ال يتطلب



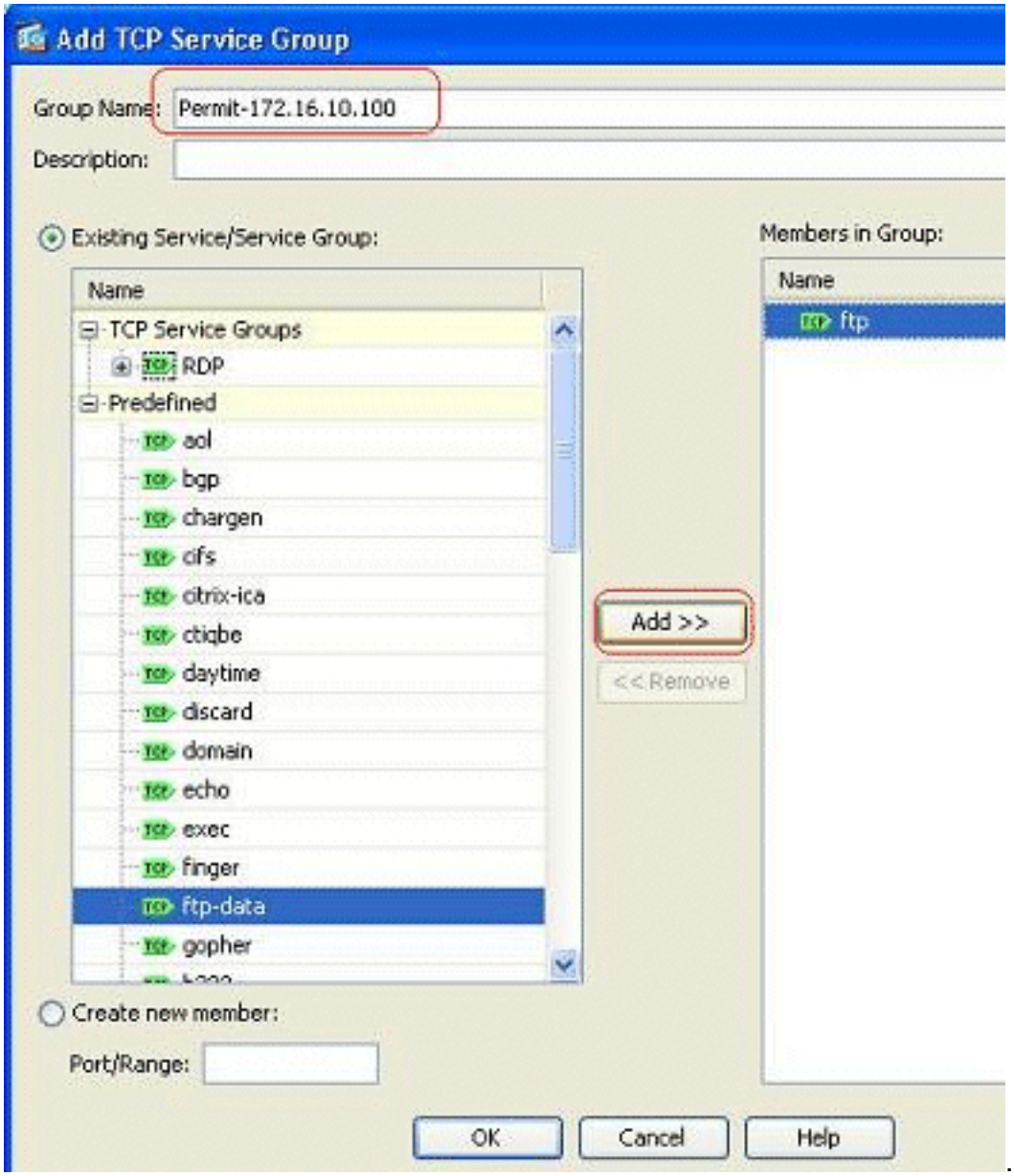
ميناء.

3. طقطقة **يضيف**، وبعد ذلك يختار **ال TCP خدمة مجموعة**



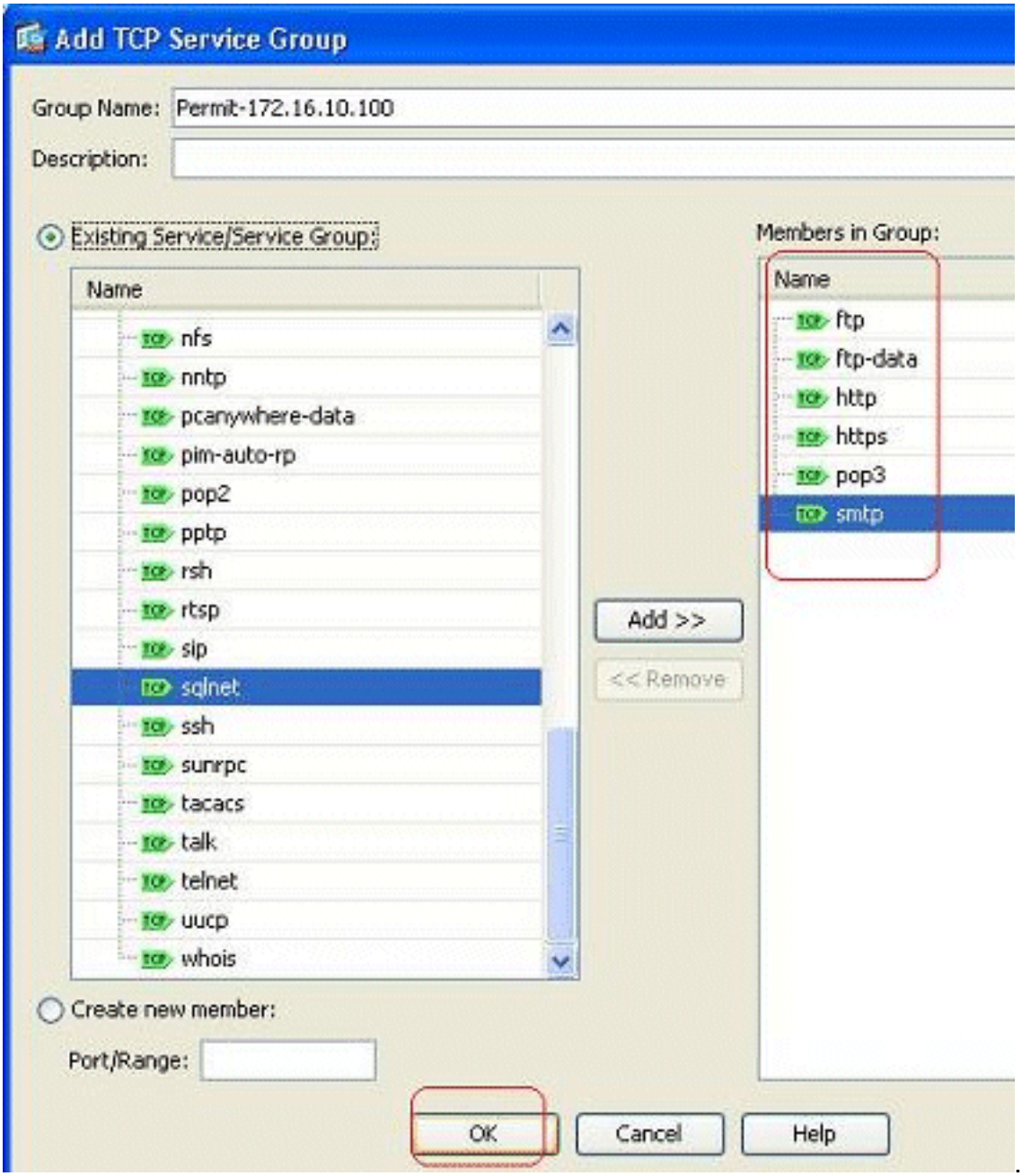
خيار.

4. أدخل اسما لهذه المجموعة. أخترت كل من ال يتطلب ميناء، وطقطقة **يضيف** in order to نقلتهم إلى الأعضاء



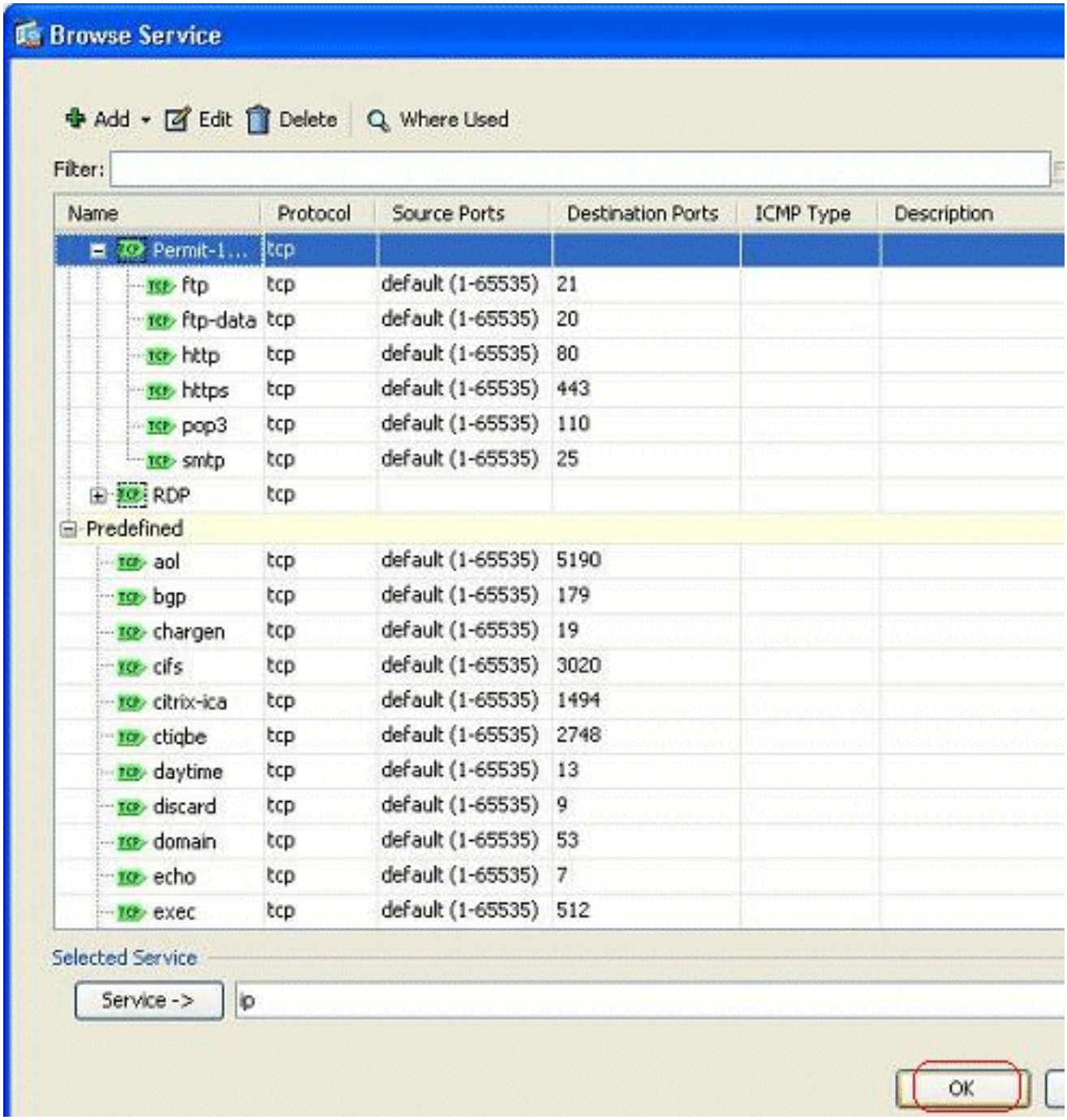
في مجموعة مجال.

5. يجب أن ترى جميع المنافذ المحددة في الحقل الأيمن. طقطقة ok in order to أتمت الخدمة ميناء يحدد

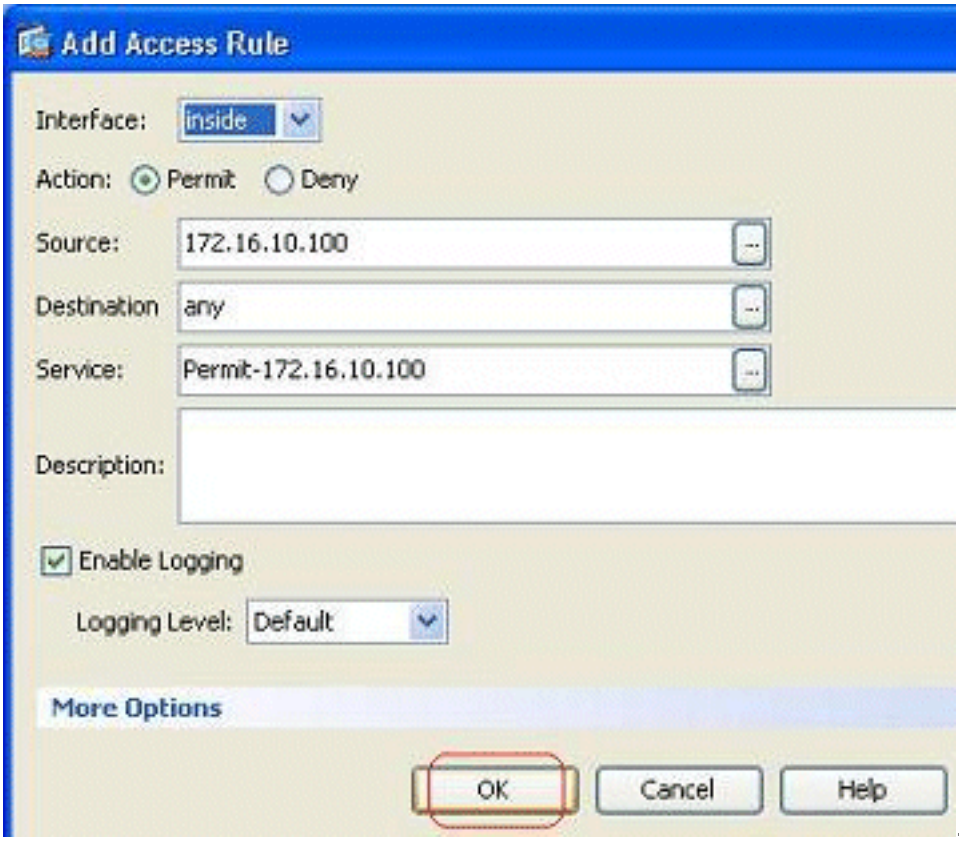


عملية.

6. يمكنك رؤية مجموعة خدمة TCP التي تم تكوينها هنا. وانقر فوق **OK**.

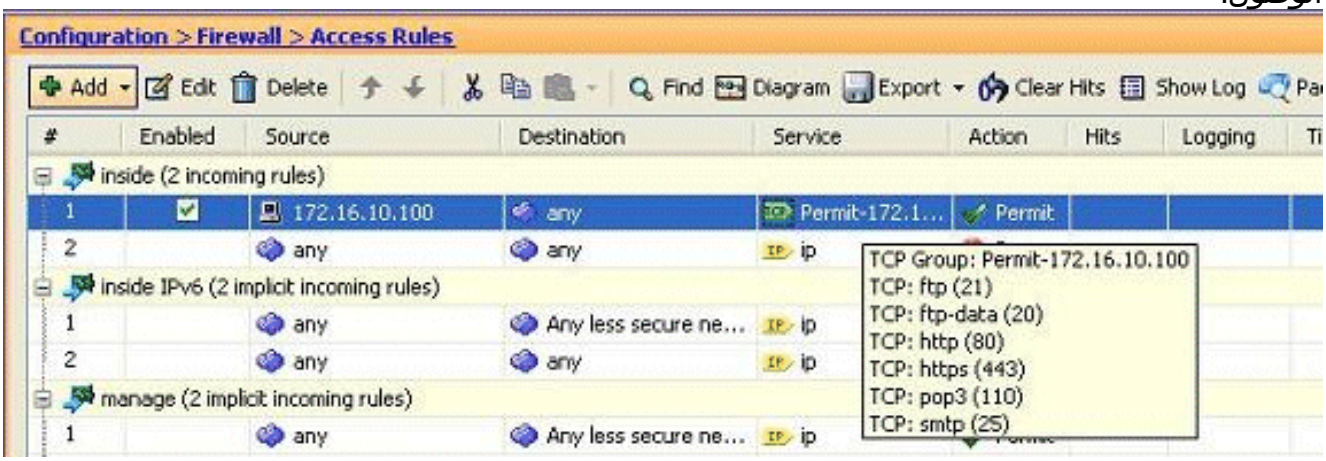


7. طقطقة in order to أتمت **ok**

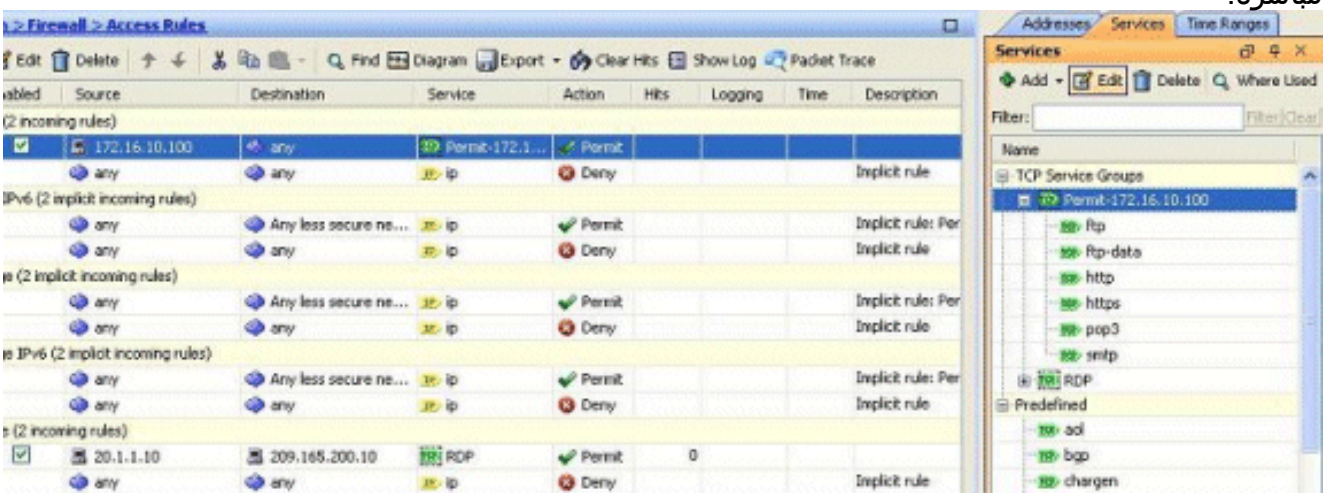


التشكيل.

8. يمكن ملاحظة قاعدة الوصول التي تم تكوينها أسفل الواجهة **الداخلية** في جزء التكوين > جدار الحماية > قواعد الوصول.

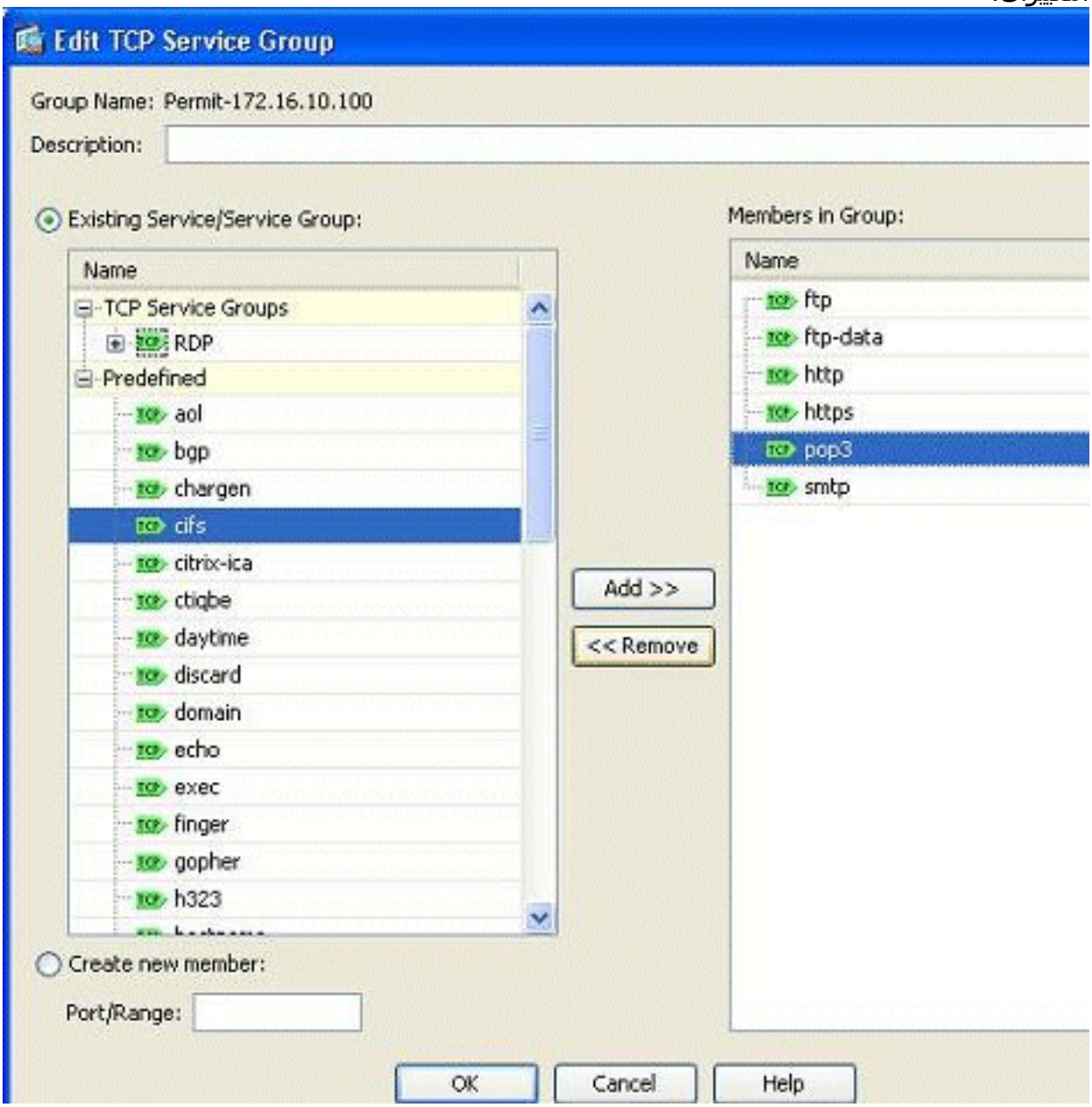


9. لسهولة الاستخدام، يمكنك أيضا تحرير مجموعة خدمة TCP مباشرة على الجزء الأيمن في علامة التبويب **خدمات**. انقر فوق **تحرير** لتعديل مجموعة الخدمات هذه مباشرة.

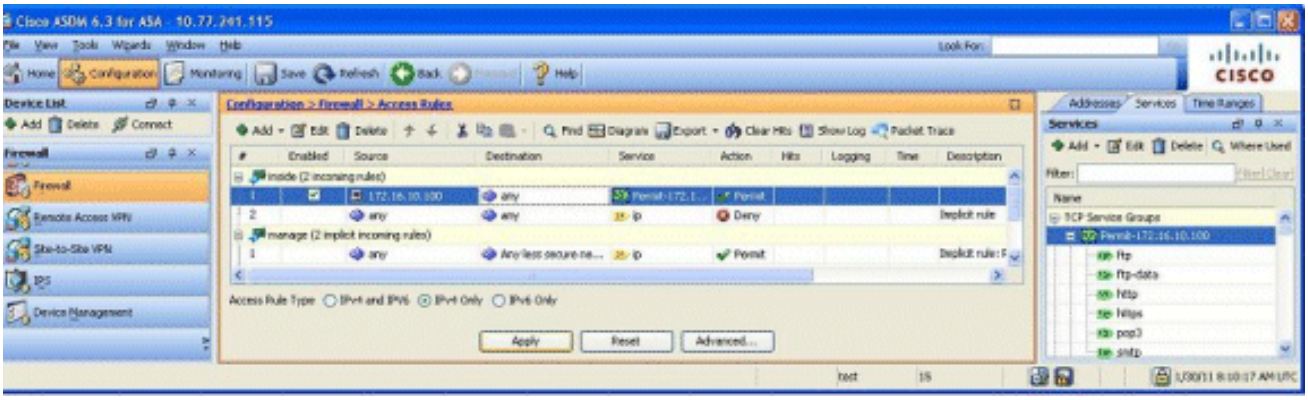


10. يعيد التوجيه مرة أخرى إلى نافذة تحرير مجموعة خدمة TCP. قم بإجراء التعديلات استنادا إلى متطلباتك،

وانقر فوق **موافق** لحفظ
التغييرات.



11. فيما يلي عرض كامل ل
ASDM:



هذا هو تكوين CLI المكافئ:

```
object-group service Permit-172.16.10.100 TCP
```

```
 port-object eq ftp
 port-object eq ftp-data
 port-object eq www
 port-object eq https
 port-object eq pop3
 port-object eq smtp
!
access-list inside_access_in extended permit TCP host 172.16.10.100 any
 object-group Permit-172.16.10.100
!
access-group inside_access_in in interface inside
!
```

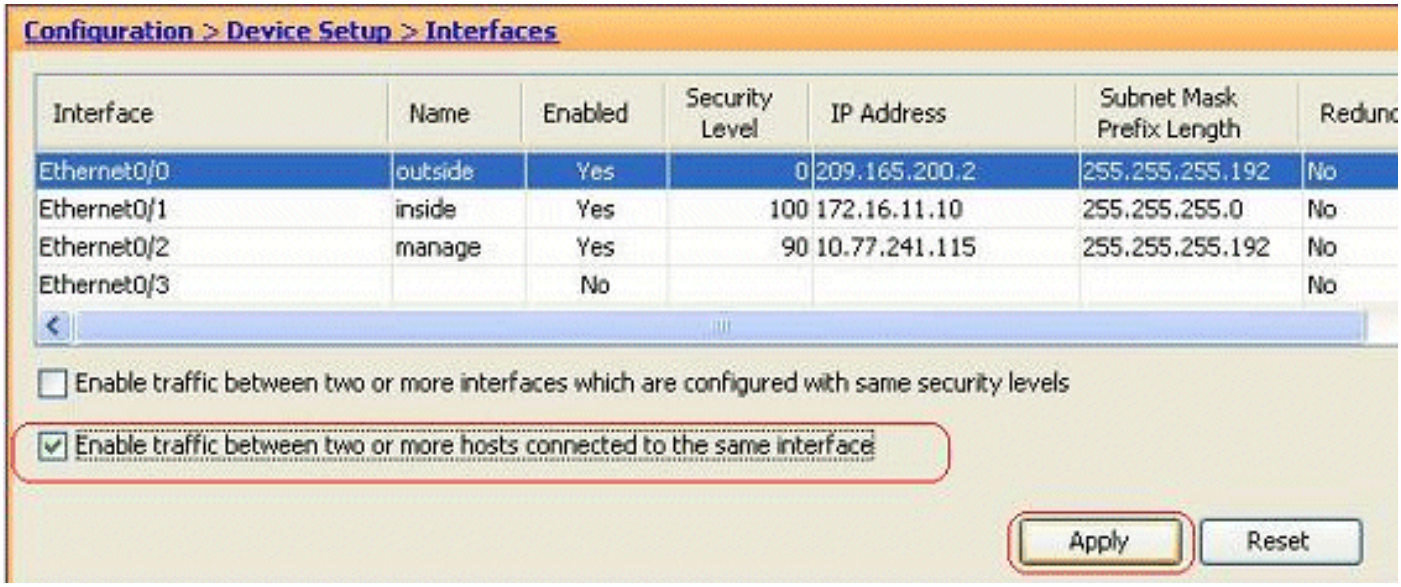
للحصول على معلومات كاملة حول تنفيذ التحكم في الوصول، ارجع إلى إضافة قائمة وصول أو تعديلها من خلال واجهة المستخدم الرسومية (GUI) ل ASDM.

السماح بحركة المرور بين الواجهات ذات مستوى الأمان نفسه

يوضح هذا القسم كيفية تمكين حركة المرور داخل الواجهات التي تحتوي على نفس مستويات الأمان.

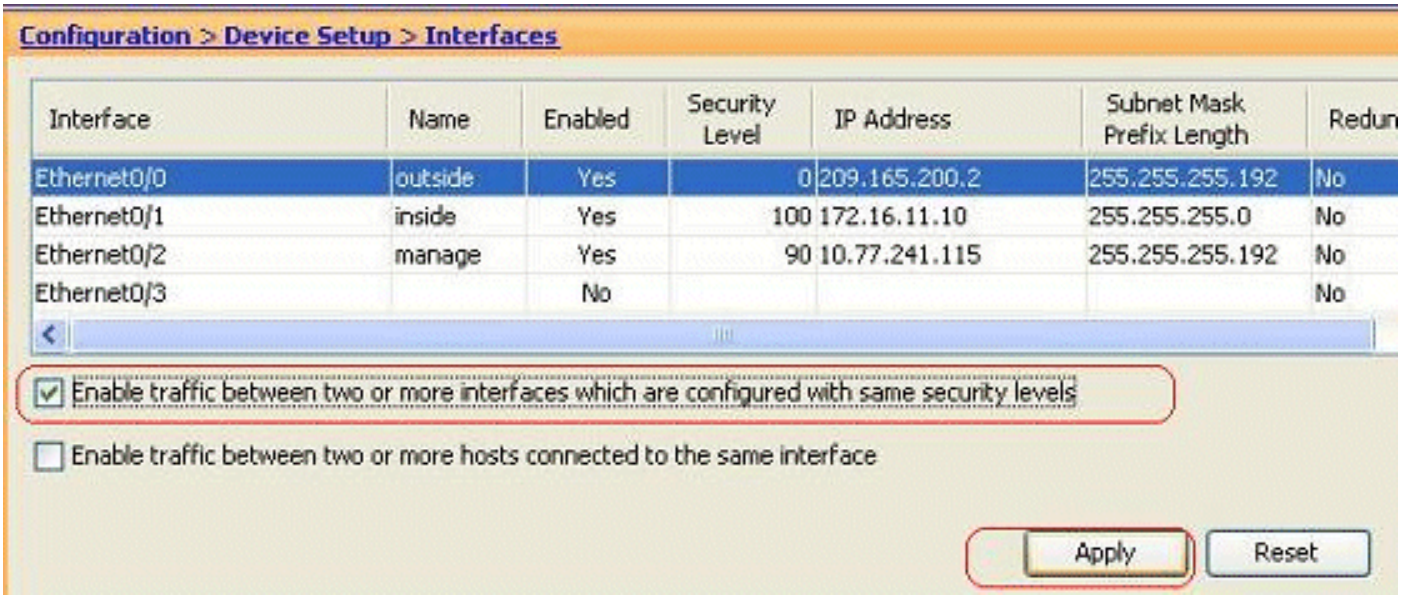
تصف هذه التعليمات كيفية تمكين الاتصال بين الواجهات.

هذا سيكون مفيد ل VPN حركة مرور أن يدخل قارن، غير أن بعد ذلك وجهت خارج ال نفسه قارن. قد تكون حركة مرور VPN غير مشفرة في هذه الحالة، أو قد يتم إعادة تشفيرها لاتصال VPN آخر. انتقل إلى **التكوين>إعداد الجهاز > الواجهات**، واختر **تمكين حركة مرور البيانات بين جهازين مضيفين أو أكثر متصلين بنفس خيار الواجهة**.



تصف هذه التعليمات كيفية تمكين الاتصال بين الواجهة.

وهذا مفيد للسماح بالتواصل بين الواجهات ذات مستويات الأمان المتساوية. انتقل إلى **التكوين>إعداد الجهاز > الواجهات**، واختر **تمكين حركة مرور البيانات بين واجهات أو أكثر تم تكوينها باستخدام خيار مستويات الأمان نفسها**.



هذا ال يماثل CLI ل كلا من هذا عملية إعداد:

```
same-security-traffic permit intra-interface
same-security-traffic permit inter-interface
```

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

يمكن تحقيق ذلك من خلال تطبيق ترجمة ثابتة ل NAT وقاعدة وصول للسماح لهذه الأجهزة المضيفة. أنت تحتاج إلى تكوين هذا كلما رغب مستخدم خارجي في الوصول إلى أي خادم موجود في شبكتك الداخلية. سيكون للخادم الموجود في الشبكة الداخلية عنوان IP خاص غير قابل للتوجيه على الإنترنت. ونتيجة لذلك، يلزمك ترجمة عنوان IP الخاص هذا إلى عنوان IP عام من خلال قاعدة NAT ثابتة. افترض أن لديك خادما داخليا (172.16.11.5). in order to جعلت هذا عمل، أنت تحتاج أن يترجم هذا نادل خاص نادل ip إلى عام ip. يوضح هذا المثال كيفية تنفيذ NAT الثابت ثنائي الإتجاه لترجمة 172.16.11.5 إلى 209.165.200.5.

لا يتم عرض القسم الخاص بالسماح للمستخدم الخارجي بالوصول إلى خادم ويب هذا من خلال تنفيذ قاعدة وصول هنا. يتم عرض مقتطف CLI موجز هنا للفهم الخاص بك:

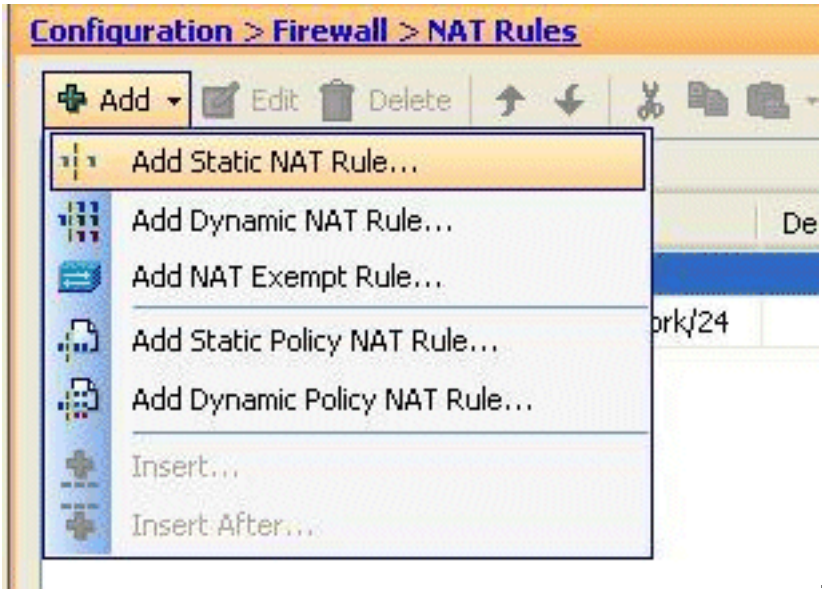
```
access-list 101 permit TCP any host 209.165.200.5
```

لمزيد من المعلومات، ارجع إلى إضافة قائمة وصول أو تعديلها من خلال واجهة المستخدم الرسومية (GUI) ل ASDM.

ملاحظة: يسمح تحديد الكلمة الأساسية "any" لأي مستخدم من العالم الخارجي بالوصول إلى هذا الخادم. أيضا، إذا لم يتم تحديده لأي منافذ خدمة، يمكن الوصول إلى الخادم على أي منفذ خدمة حيث يظل هذا المنفذ مفتوحا. توخ الحذر عند التنفيذ، وينصح بتقييد الإذن إلى المستخدم الخارجي الفردي وأيضا إلى المنفذ المطلوب على الخادم.

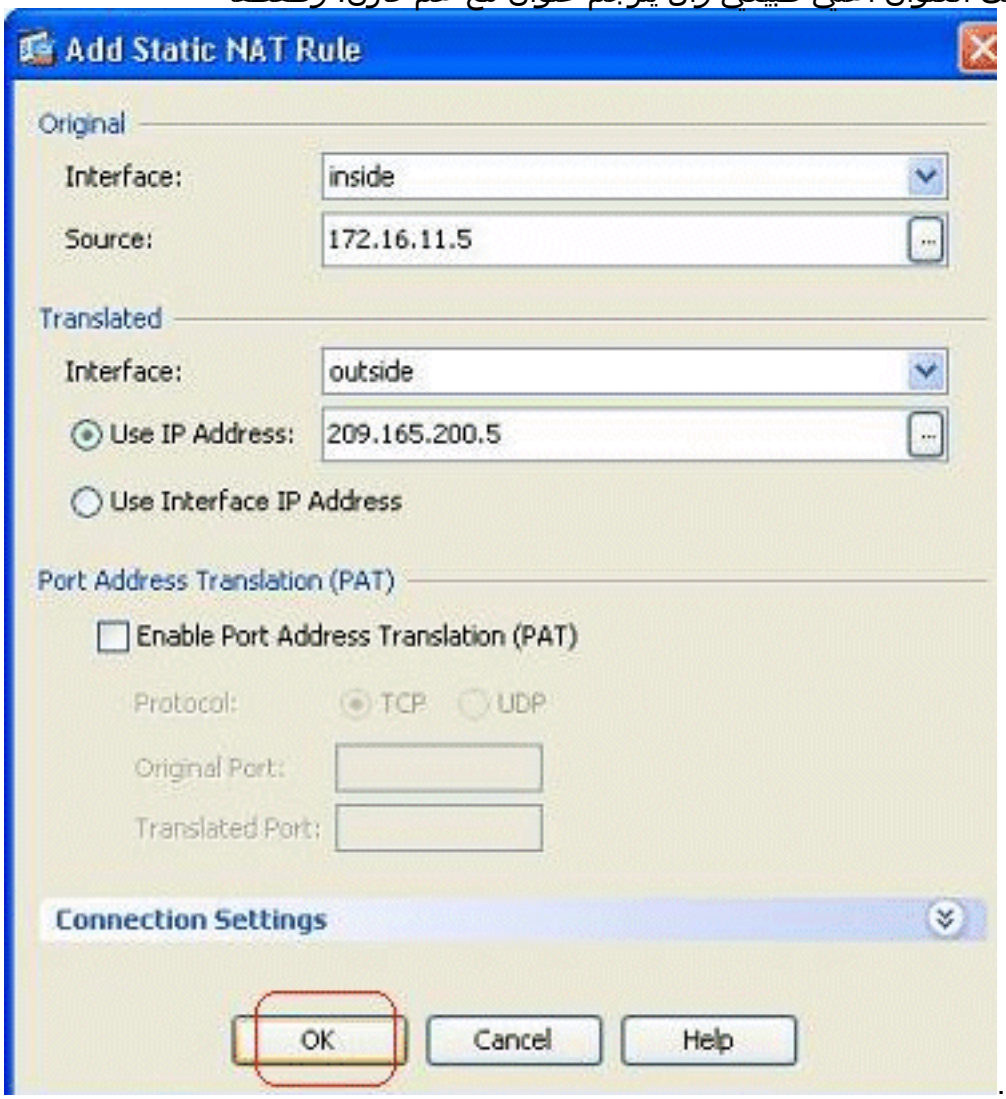
أتمت هذا steps in order to شكلت الساكن إستاتيكي nat:

1. انتقل إلى التكوين > **جدار الحماية>قواعد NAT**، وانقر **إضافة**، واختر إضافة قاعدة NAT



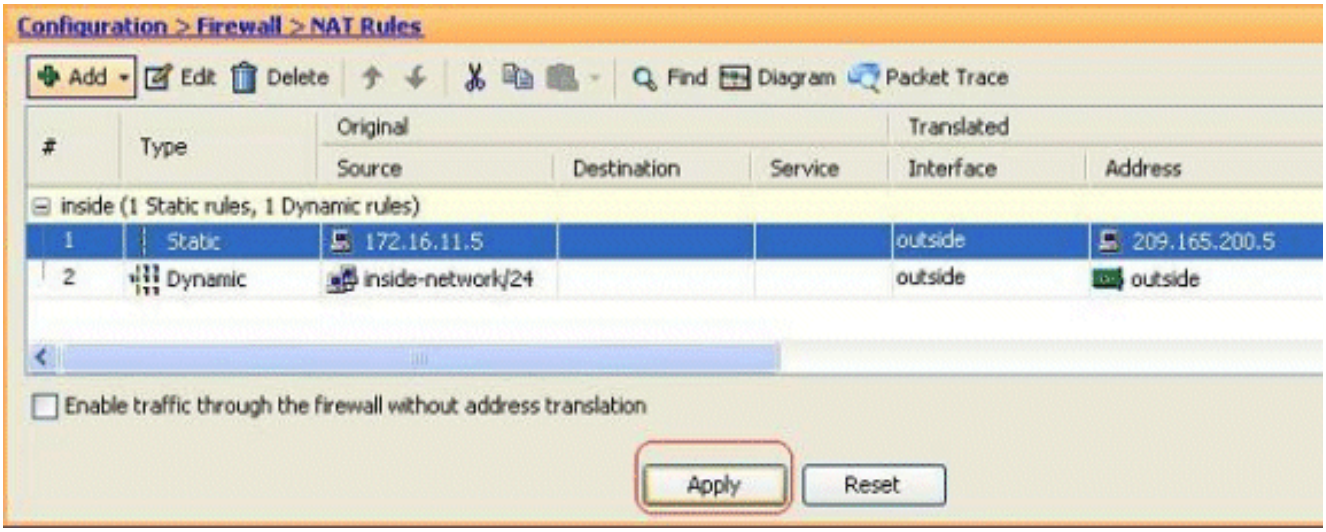
الثابتة.

2. عينت العنوان أهلي طبيعي وال يترجم عنوان مع هم قارن، وطقطقة



ok.

3. أنت يستطيع رأيت ال يشكل ساكن إستاتيكي nat مدخل هنا. طقطقة **يطبق** in order to أرسلت هذا إلى ال ASA.



هذا مثال موجز على واجهة سطر الأوامر (CLI) لتكوين ASDM هذا:

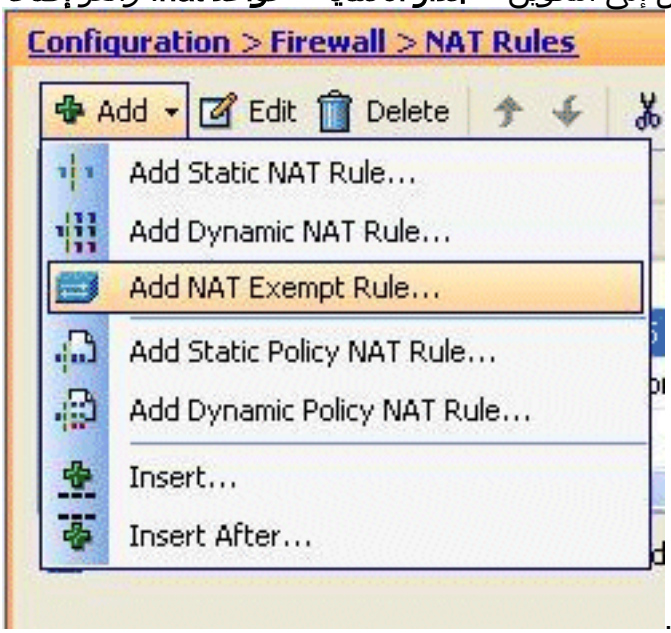
```
!
static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255
!
```

تعطيل NAT للمضيفين/الشبكات المحددة

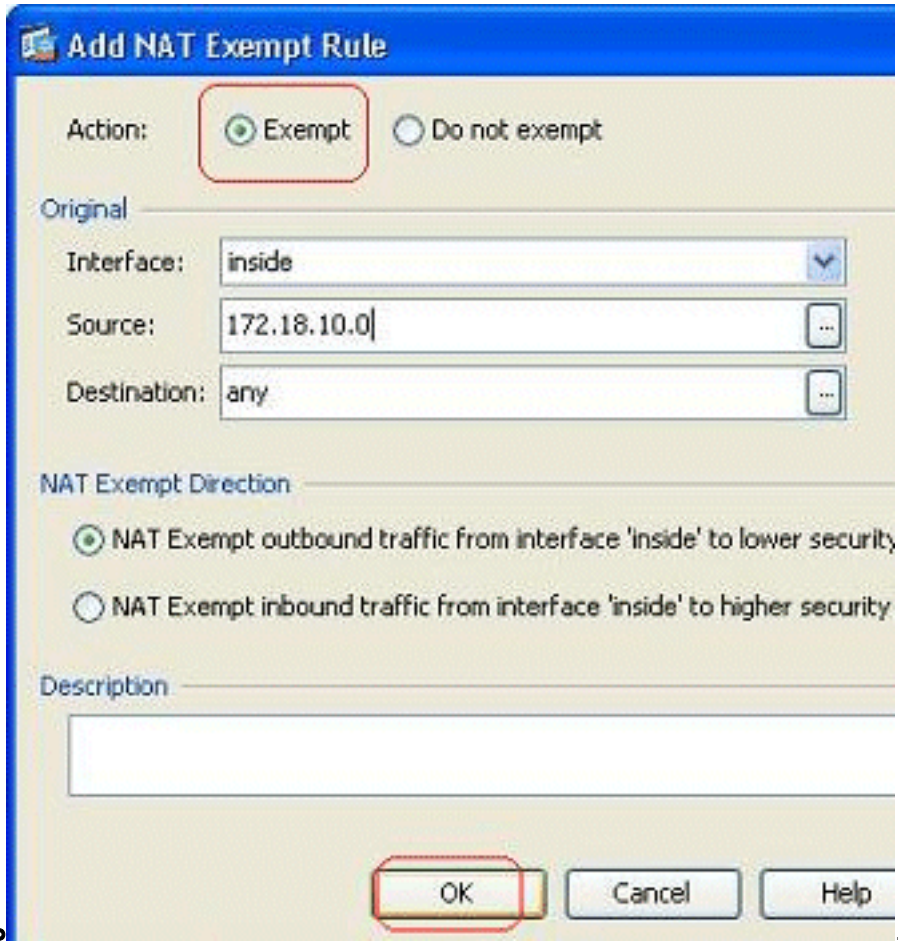
عندما تحتاج إلى إستثناء مضيفين أو شبكات معينة من NAT، أضف قاعدة إستثناء NAT لتعطيل ترجمة العنوان. وهذا يسمح للمضيفين المترجمين والبعيدين على حد سواء ببدء الاتصالات.

أكمل الخطوات التالية:

1. انتقل إلى التكوين > **جدار الحماية** > **قواعد nat**، وانقر **إضافة**، واختر إضافة قاعدة إستثناء nat.

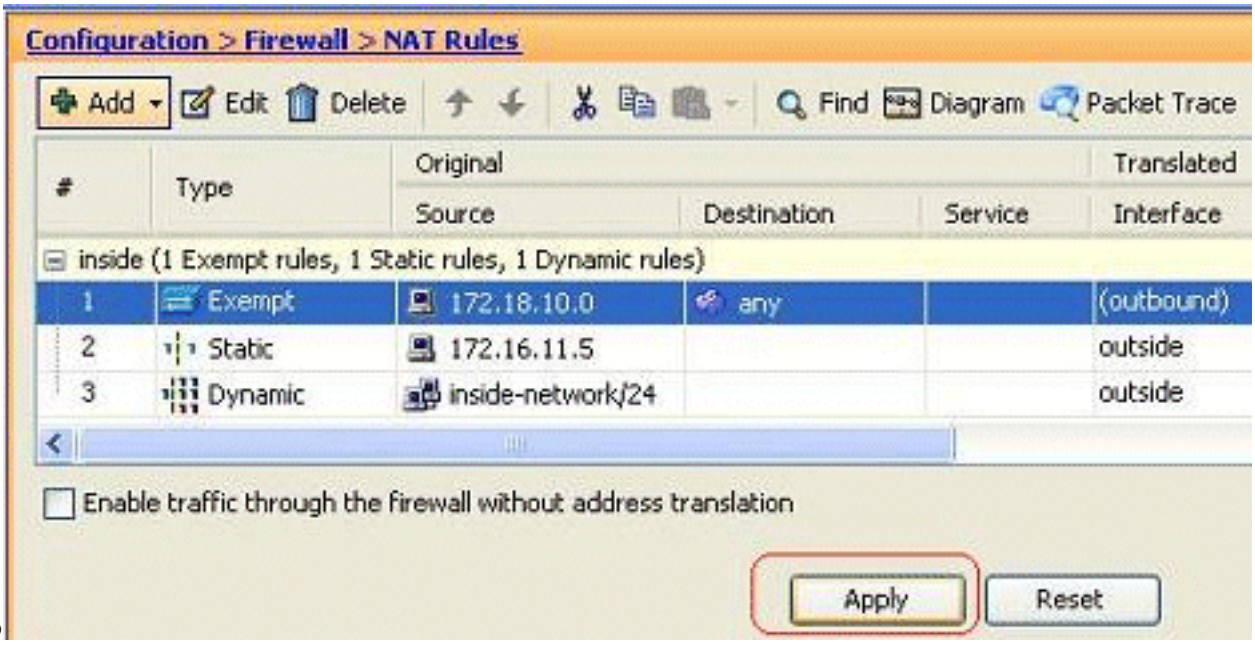


2. هنا، تم إستثناء الشبكة الداخلية 172.18.10.0 من ترجمة العنوان. تأكد من تحديد خيار **الاستثناء**. إتجاه إستثناء NAT له خياران:حركة المرور الصادرة إلى واجهات الأمان الأقلحركة المرور الواردة إلى واجهات الأمان العلياالخيار الافتراضي هو لحركة المرور الصادرة. طقطقة **ok** in order to أتمت



ملاحظة: عند إختيار خيار **عدم الاستثناء**، لن يتم إعفاء ذلك المضيف المعين من NAT وستتم إضافة قاعدة وصول منفصلة باستخدام الكلمة الأساسية "deny". يفيد ذلك في تجنب الأجهزة المضيفة المحددة من إستثناء NAT حيث أن الشبكة الفرعية الكاملة، باستثناء هذه الأجهزة المضيفة، ستكون معفاة من NAT.

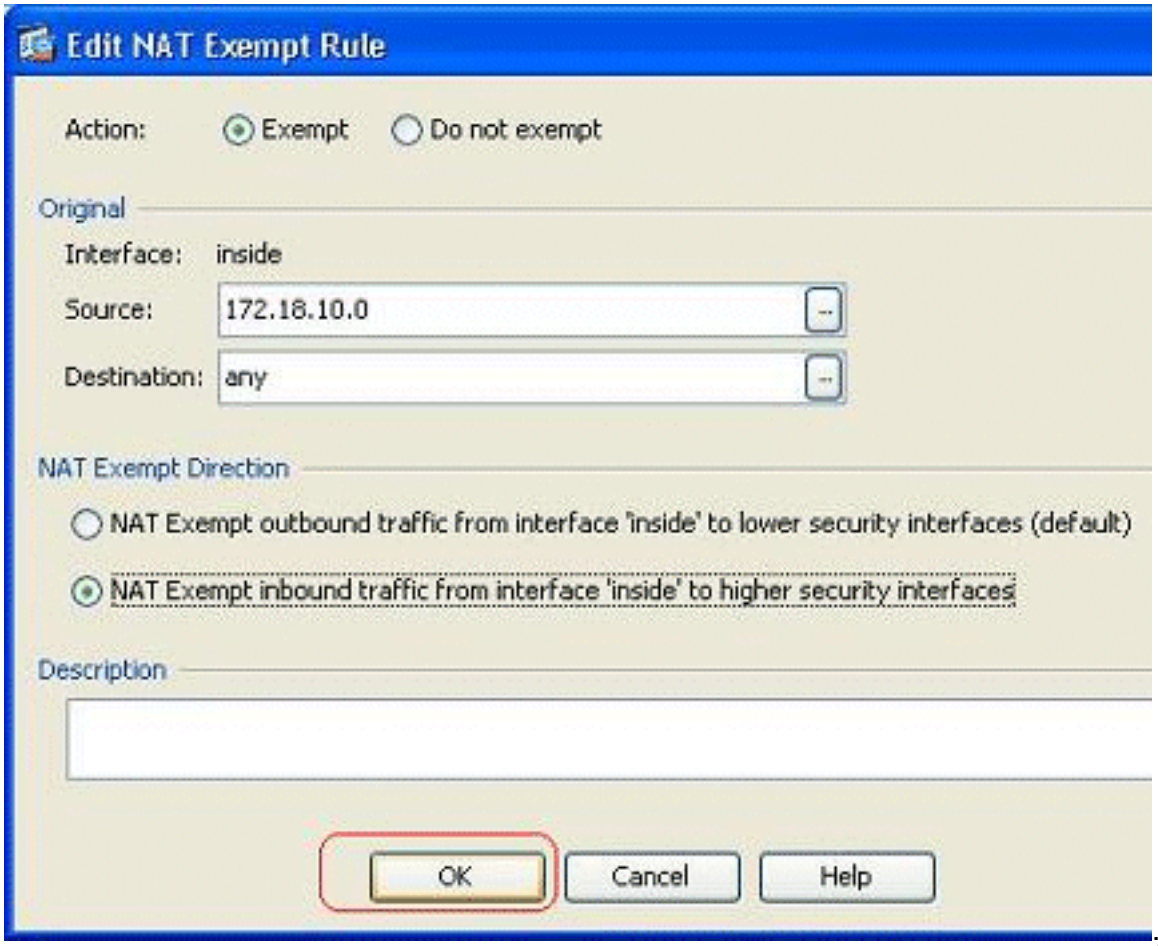
3. يمكنك رؤية قاعدة إستثناء NAT للاتجاه الصادر هنا. طقطقة **يطبق** in order to أرسلت التشكيل إلى ال ASA.



هذا هو مخرج واجهة سطر الأوامر (CLI) المكافئ للمرجع الخاص بك:

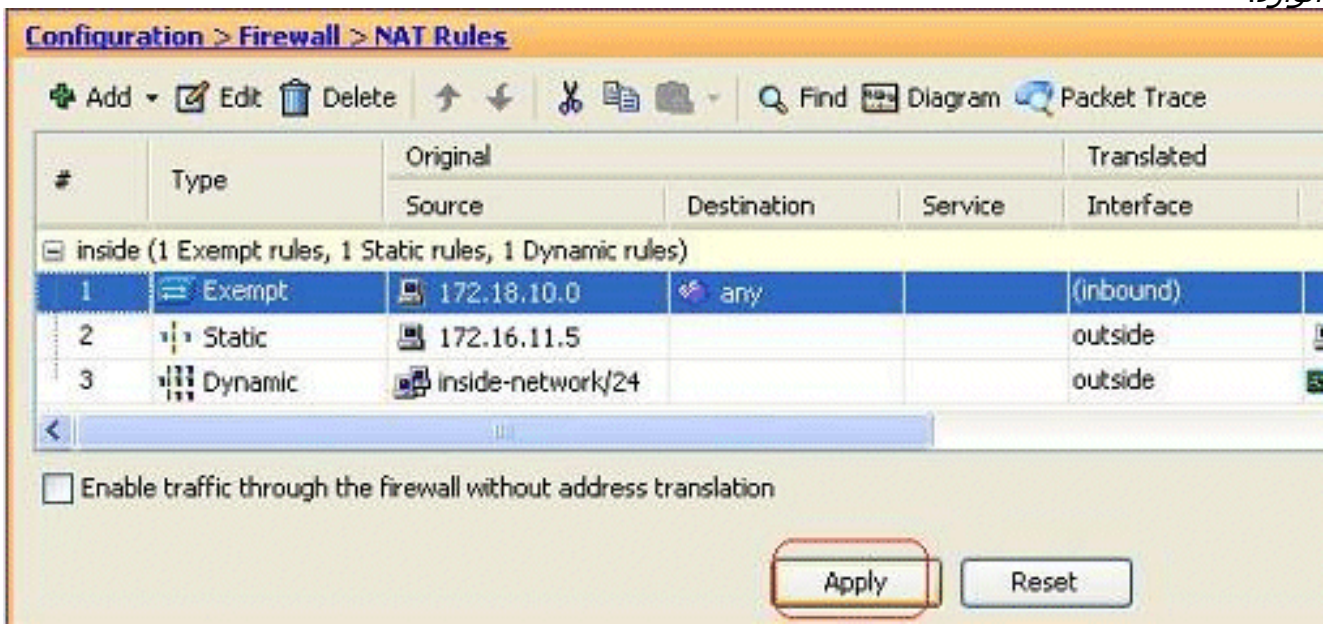
```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound
```

4. هنا يمكنك رؤية كيفية تحرير قاعدة إستثناء NAT لاتجاهها. انقر فوق **موافق**" لكي يسري هذا



الخيار.

5. يمكنك الآن أن ترى أن الإتجاه تم تغييره إلى *الوارد*.

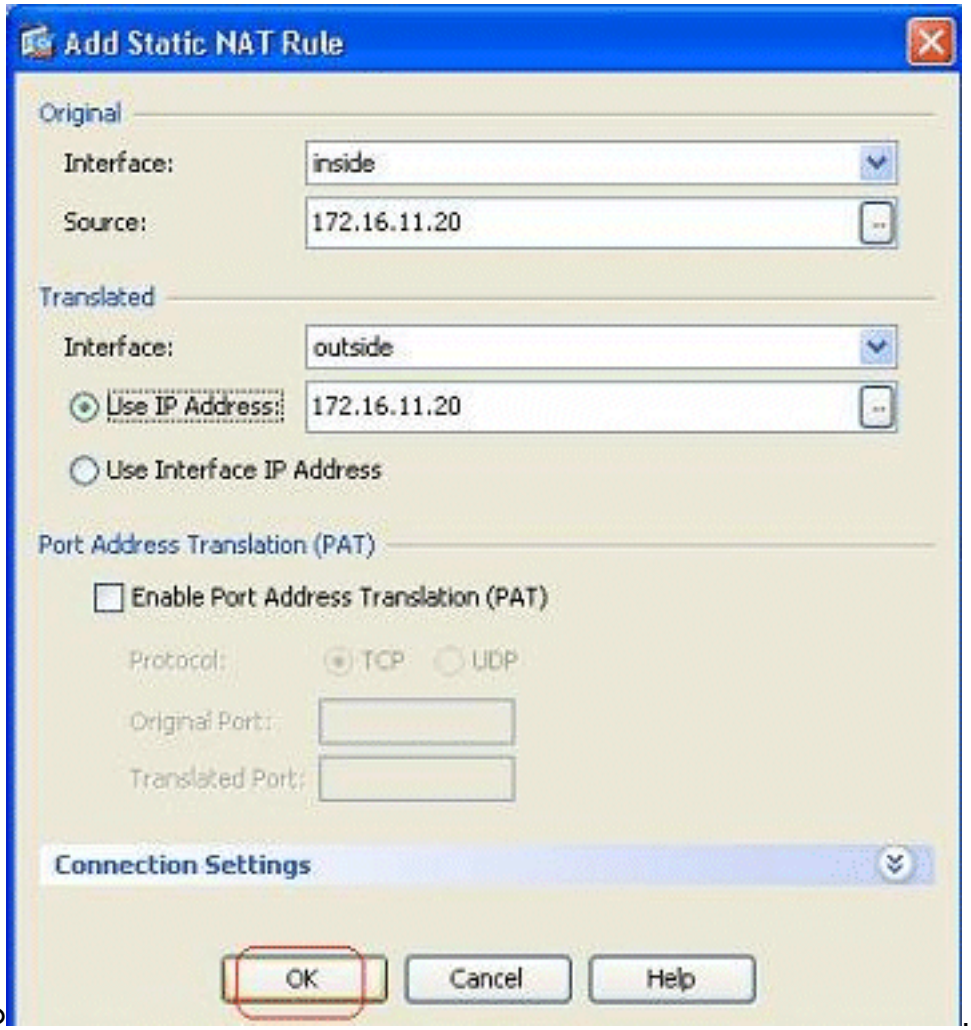


طقطقة **يطبق** in order to أرسلت هذا CLI إنتاج إلى ال ASA:

```
access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound outside
```

ملاحظة: من هذا، يمكنك أن ترى أنه تمت إضافة كلمة أساسية جديدة (خارج) إلى نهاية الأمر **nat 0**. دعات هذا سمة **خارجي nat**.

6. آخر طريق أن يعجز nat من خلال تنفيذ هوية nat. هوية nat يترجم مضيف إلى ال نفسه عنوان. هنا مثال ساكن إستاتيكي عادي NAT، حيث المضيف (172.16.11.20) ترجمت إلى ال نفسه عنوان عندما هو يكون



هذا هو نفذت من الخارج.
مخرج واجهة سطر الأوامر (CLI) المكافئ:

```
!
static (inside,outside) 172.16.11.20 172.16.11.20 netmask 255.255.255.255
!
```

إعادة توجيه المنفذ (إعادة توجيه) باستخدام الحالات

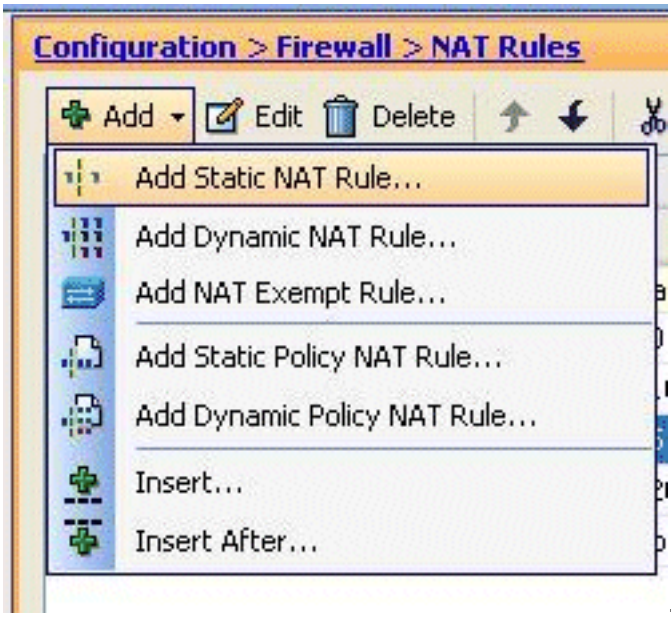
إعادة توجيه المنفذ أو إعادة توجيه المنفذ هي ميزة مفيدة حيث يحاول المستخدمون الخارجيون الوصول إلى خادم داخلي على منفذ معين. in order to أتمت هذا، ال داخلي، يتلقى عنوان خاص، يكون ترجمت إلى عنوان عام أي بدوره يسمح منفذ للميناء خاص.

في هذا المثال، يريد المستخدم الخارجي الوصول إلى خادم 209.165.200.15، SMTP على المنفذ 25. ويتحقق ذلك في خطوتين:

1. ترجمة خادم البريد الداخلي، 172.16.11.15 على المنفذ 25، إلى عنوان IP العام، 209.165.200.15 في المنفذ 25.
2. السماح بالوصول إلى خادم البريد العام، 209.165.200.15 على المنفذ 25.

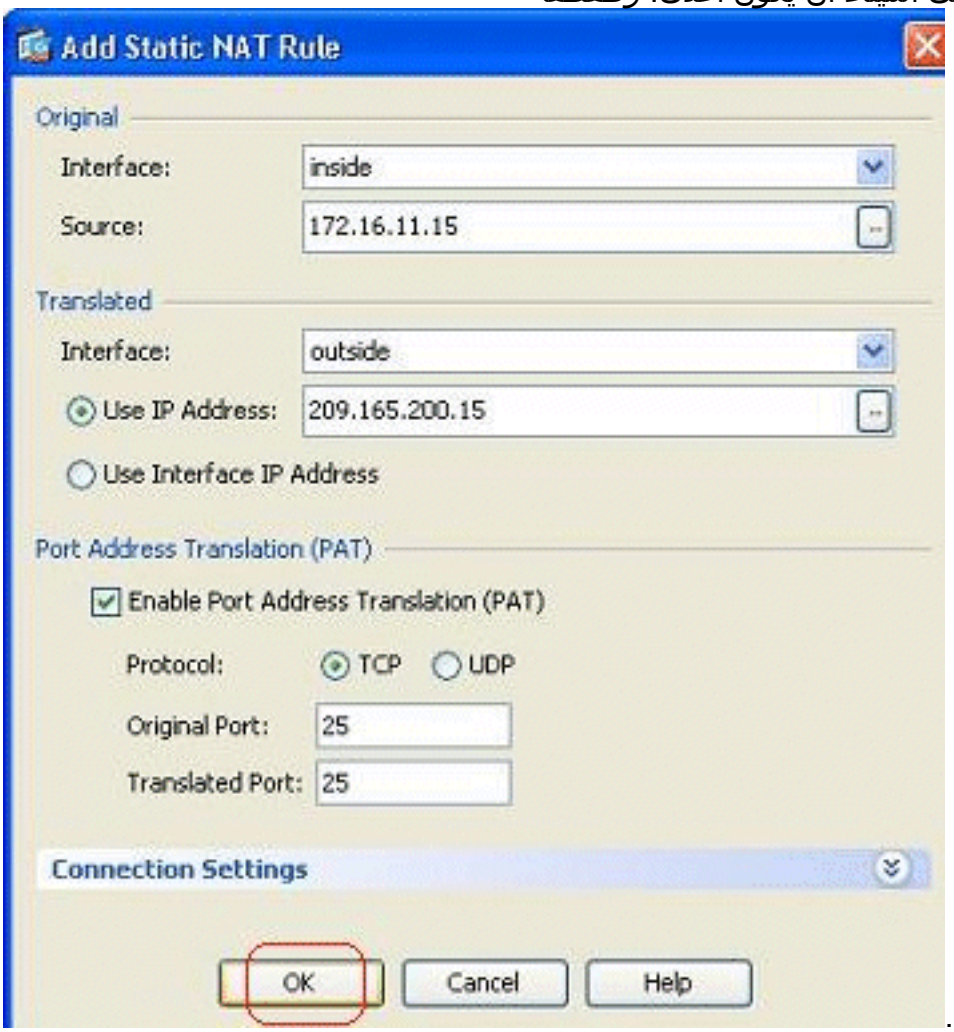
عندما يحاول المستخدم الخارجي الوصول إلى الخادم، 209.165.200.15 في المنفذ 25، ستتم إعادة توجيه حركة مرور البيانات هذه إلى خادم البريد الداخلي، 172.16.11 15 في المنفذ 25.

1. انتقل إلى التكوين > **جدار الحماية>قواعد NAT**، وانقر **إضافة**، واختر إضافة قاعدة NAT



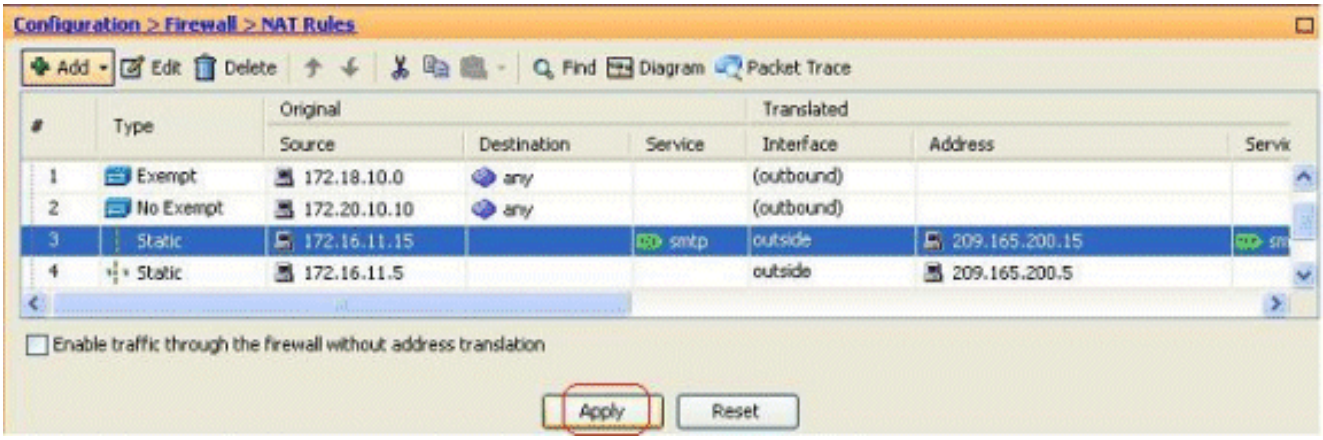
الثابتة.

2. حدد المصدر الأصلي وعنوان IP المترجم مع الواجهات المرتبطة بها. أخترت **يمكن أيسر عنوان ترجمة (ضرب)**، عينت الميناء أن يكون أعدت، وطقطقة



ok.

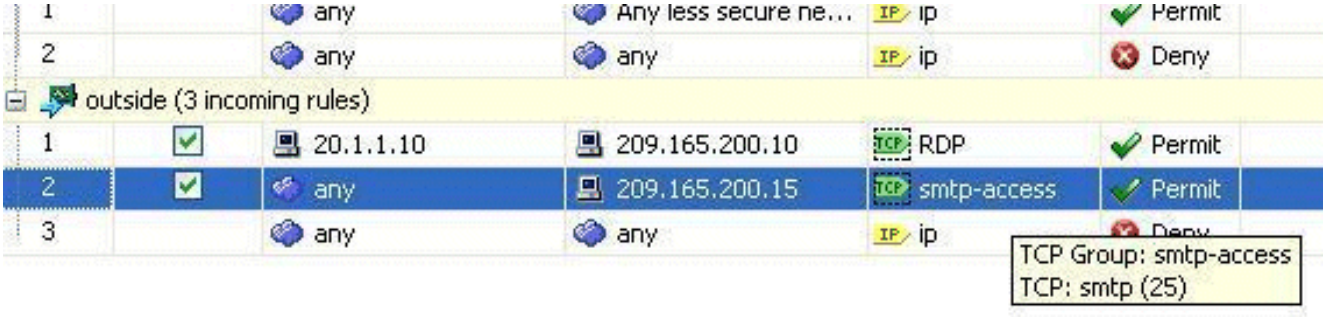
3. يرى قاعدة PAT الثابتة التي تم تكوينها هنا:



هذا هو مخرج واجهة سطر الأوامر (CLI) المكافئ:

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
                                                    255.255.255.255
!
```

4. هذه هي قاعدة الوصول التي تسمح للمستخدم الخارجي بالوصول إلى خادم SMTP العام على 209.165.200.15:



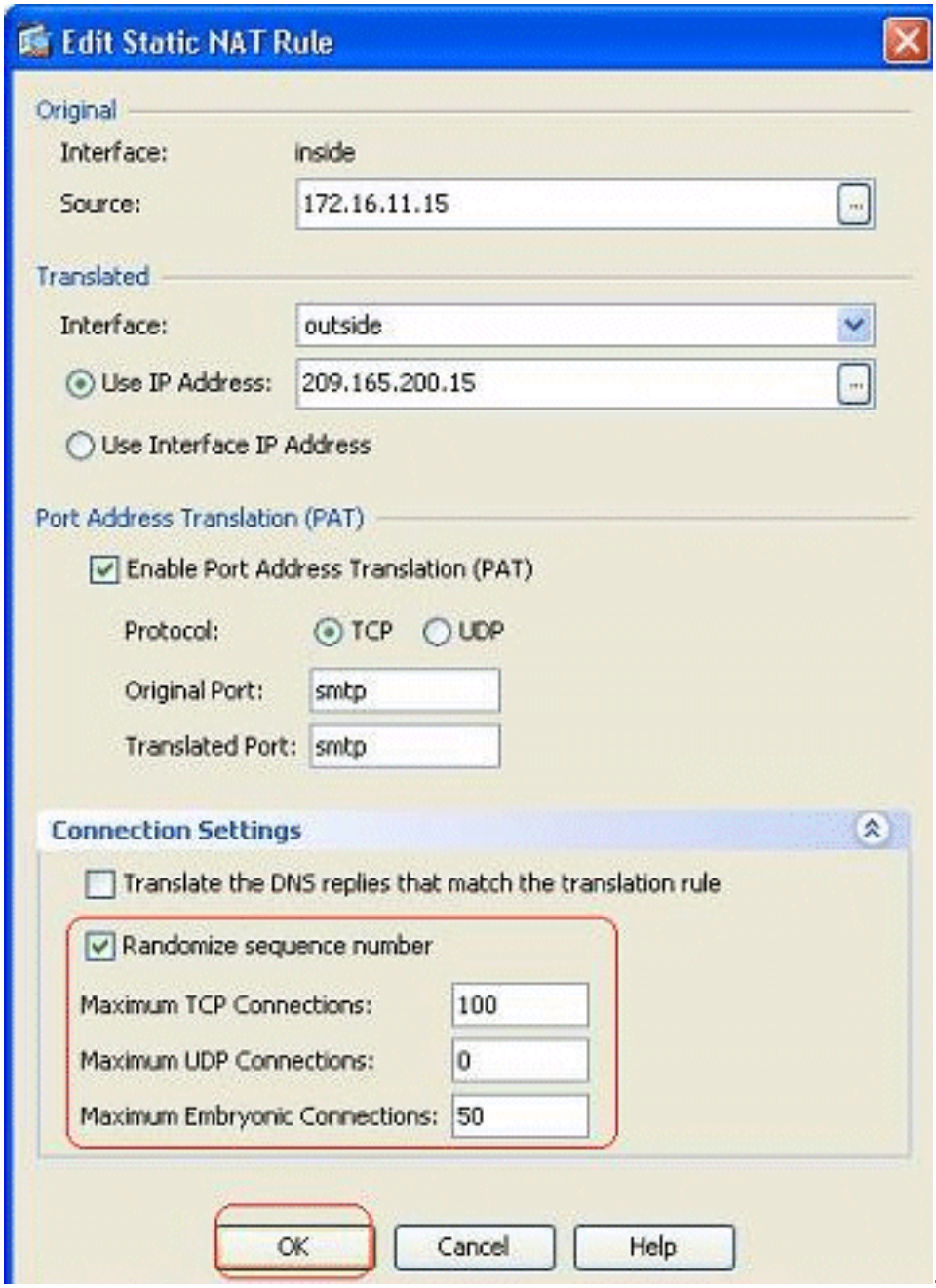
ملاحظة: تأكد من إستخدام مضيفين محددين بدلا من إستخدام **أي** كلمة أساسية في مصدر قاعدة الوصول.

الحد من جلسة TCP/UDP باستخدام ثابت

يمكنك تحديد الحد الأقصى لعدد إتصالات TCP/UDP باستخدام القاعدة الثابتة. يمكنك أيضا تحديد الحد الأقصى لعدد الاتصالات الجنينية. الاتصال الجنيني هو اتصال في حالة نصف مفتوحة. وسيؤثر عدد أكبر من هذه العوامل على أداء نظام المحاسبة المستقل. وسيؤدي الحد من هذه الاتصالات إلى منع هجمات معينة مثل DoS و SYN إلى حد ما. للحصول على تخفيف كامل، يلزمك تحديد السياسة في إطار عمل ميزة "حماية مستوى الإدارة (MPF)"، والتي تتجاوز نطاق هذا المستند. للحصول على معلومات إضافية حول هذا الموضوع، ارجع إلى التخفيف من هجمات الشبكة.

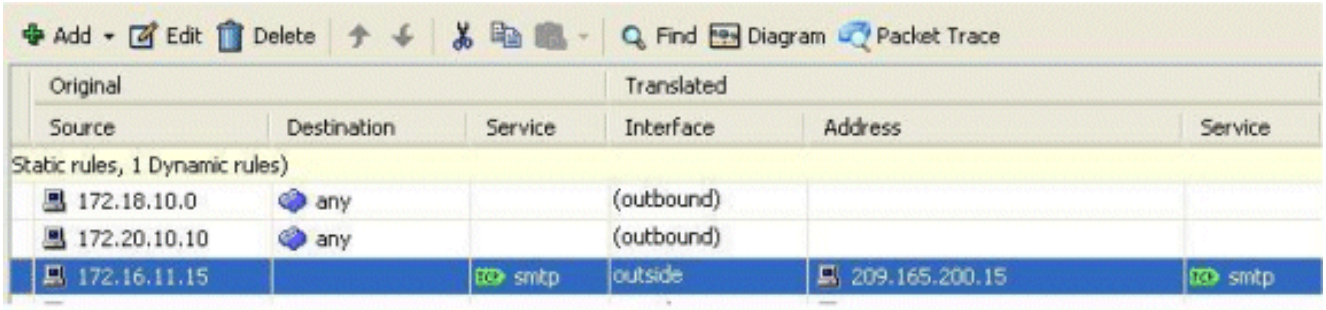
أكمل الخطوات التالية:

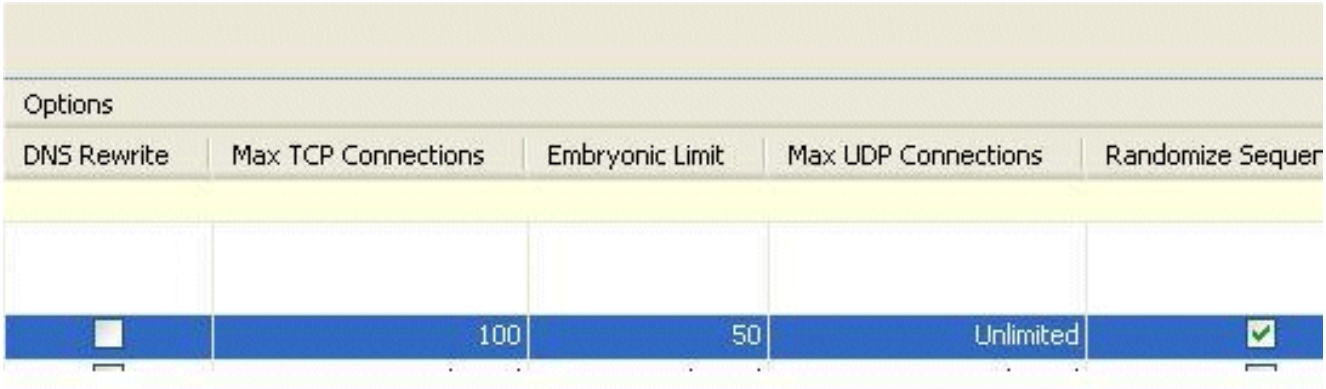
1. انقر فوق علامة التبويب **إعدادات الاتصال**، وحدد القيم الخاصة بالحد الأقصى للاتصالات لهذه الترجمة



الثابتة.

2. تظهر هذه الصور حدود الاتصال لهذه الترجمة الثابتة المحددة:





هذا هو مخرج واجهة سطر الأوامر (CLI) المكافئ:

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
                                                TCP 100 50 255.255.255.255
!
```

قائمة الوصول المستندة إلى الوقت

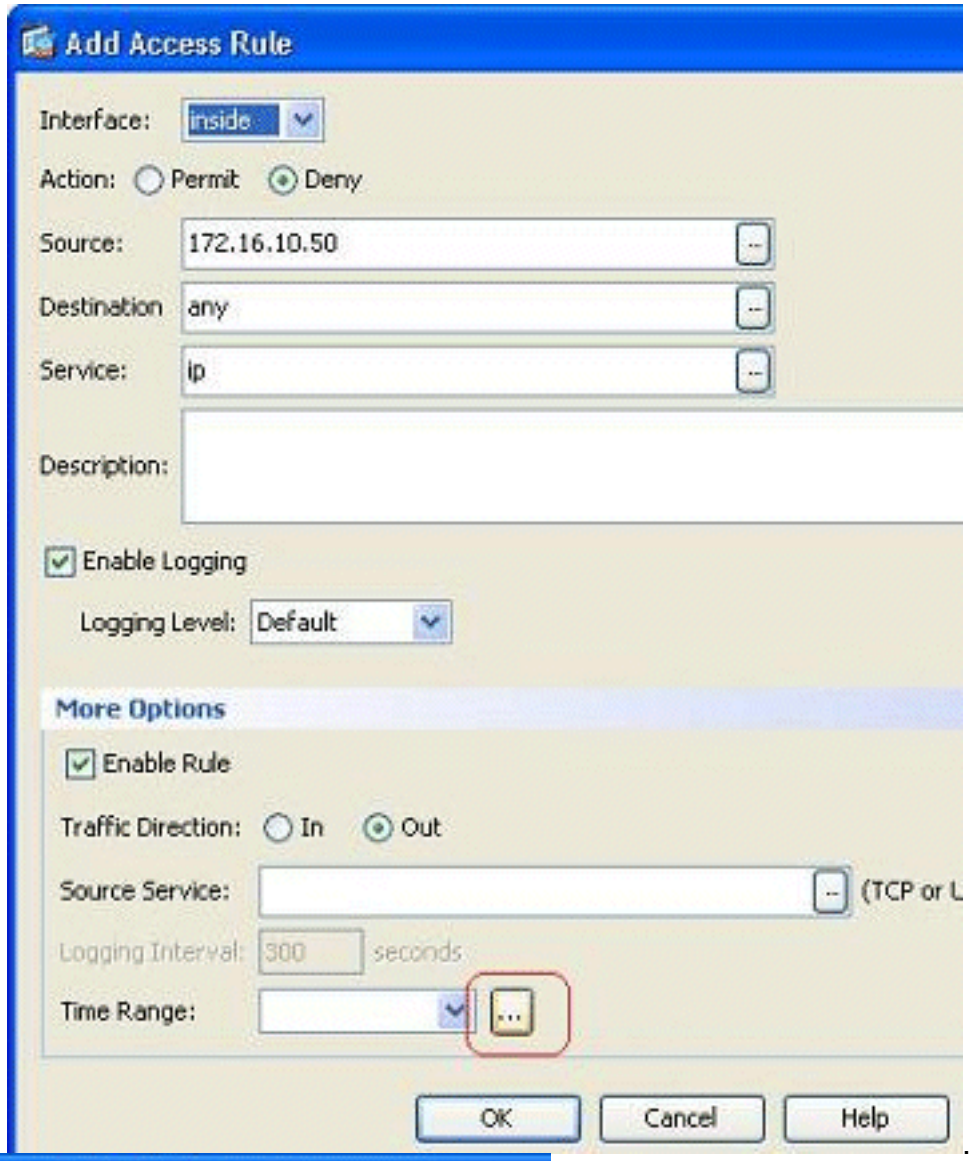
يتعامل هذا القسم مع تنفيذ قوائم الوصول المستندة إلى الوقت باستخدام ASDM. يمكن تطبيق قواعد الوصول استنادا إلى الوقت. لتنفيذ هذا الإجراء، يلزمك تحديد نطاق زمني يحدد التوقيتات حسب اليوم/الأسبوع/الشهر/السنة. بعد ذلك، تحتاج إلى ربط هذا النطاق الزمني بقاعدة الوصول المطلوبة. يمكن تعريف النطاق الزمني بطريقتين:

1. مطلق - يحدد الفترة الزمنية مع وقت البدء ووقت الانتهاء.
2. دوري - يعرف أيضا باسم متكرر. تعريف الفترة الزمنية التي تحدث على فترات زمنية محددة.

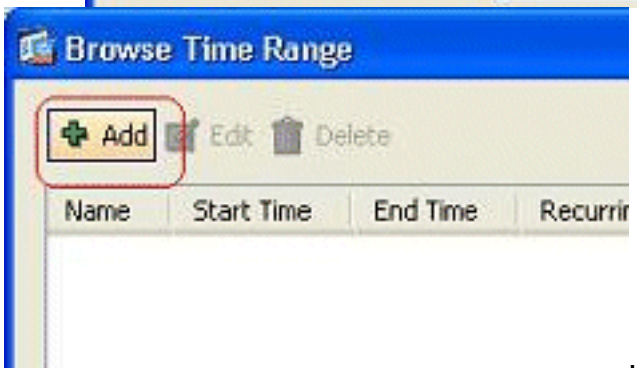
ملاحظة: قبل تكوين النطاق الزمني، تأكد من تكوين ASA بإعدادات التاريخ/الوقت الصحيحة لأن هذه الميزة تستخدم إعدادات ساعة النظام للتنفيذ. سيؤدي مزامنة ASA مع خادم NTP إلى نتائج أفضل بكثير.

أتمت هذا steps in order to شكلت هذا سمة من خلال ASDM:

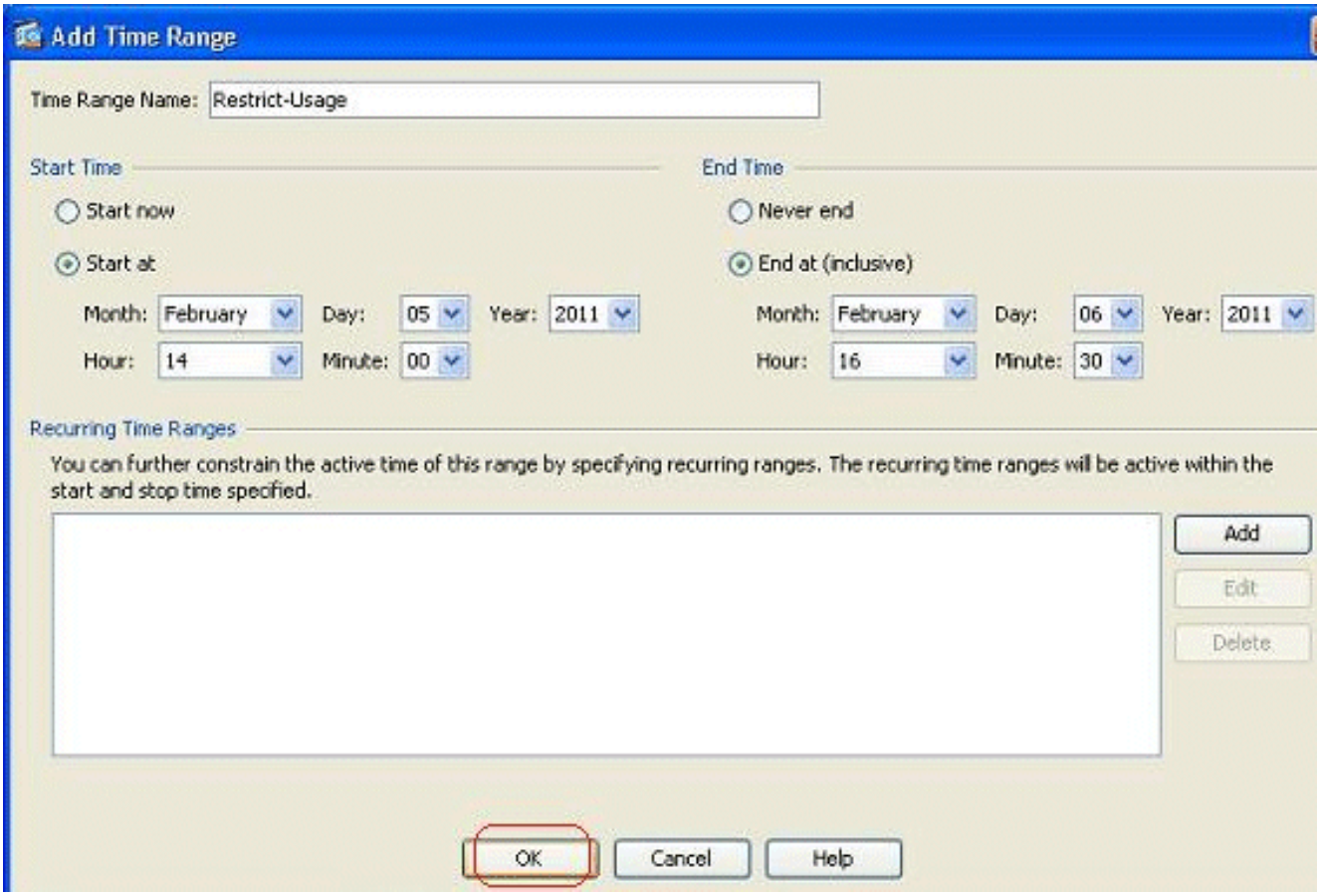
1. أثناء تحديد قاعدة الوصول، انقر فوق زر **التفاصيل** في حقل النطاق



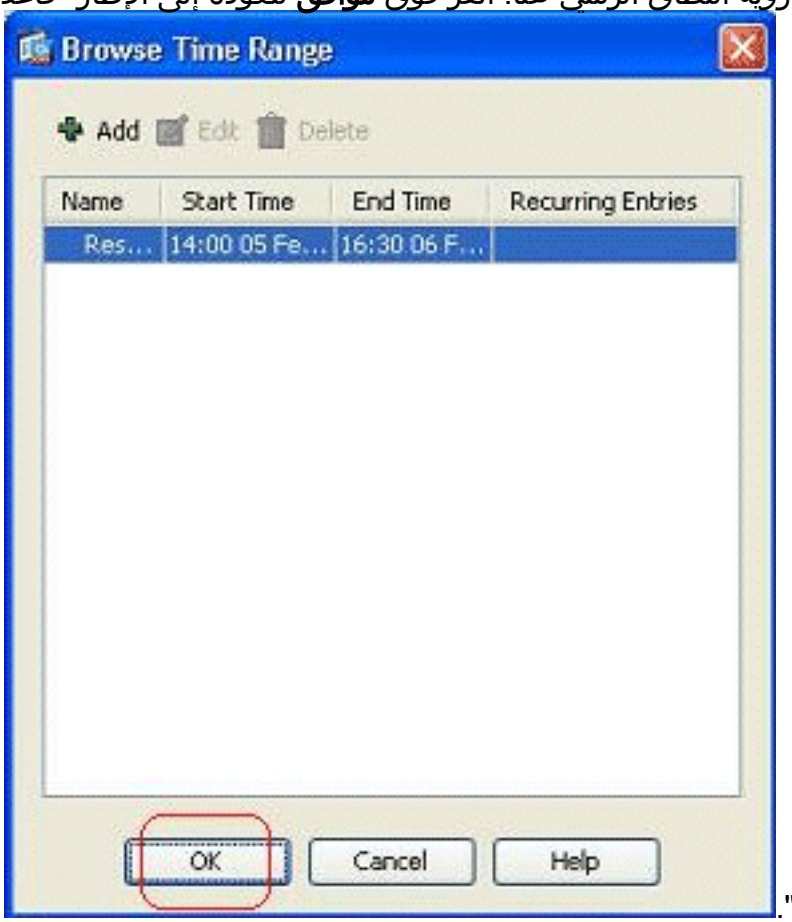
الزمني.



2. انقر فوق **إضافة** لإنشاء نطاق زمني جديد.
3. قم بتحديد اسم النطاق الزمني، وحدد وقت البدء ووقت الانتهاء. وانقر فوق OK.

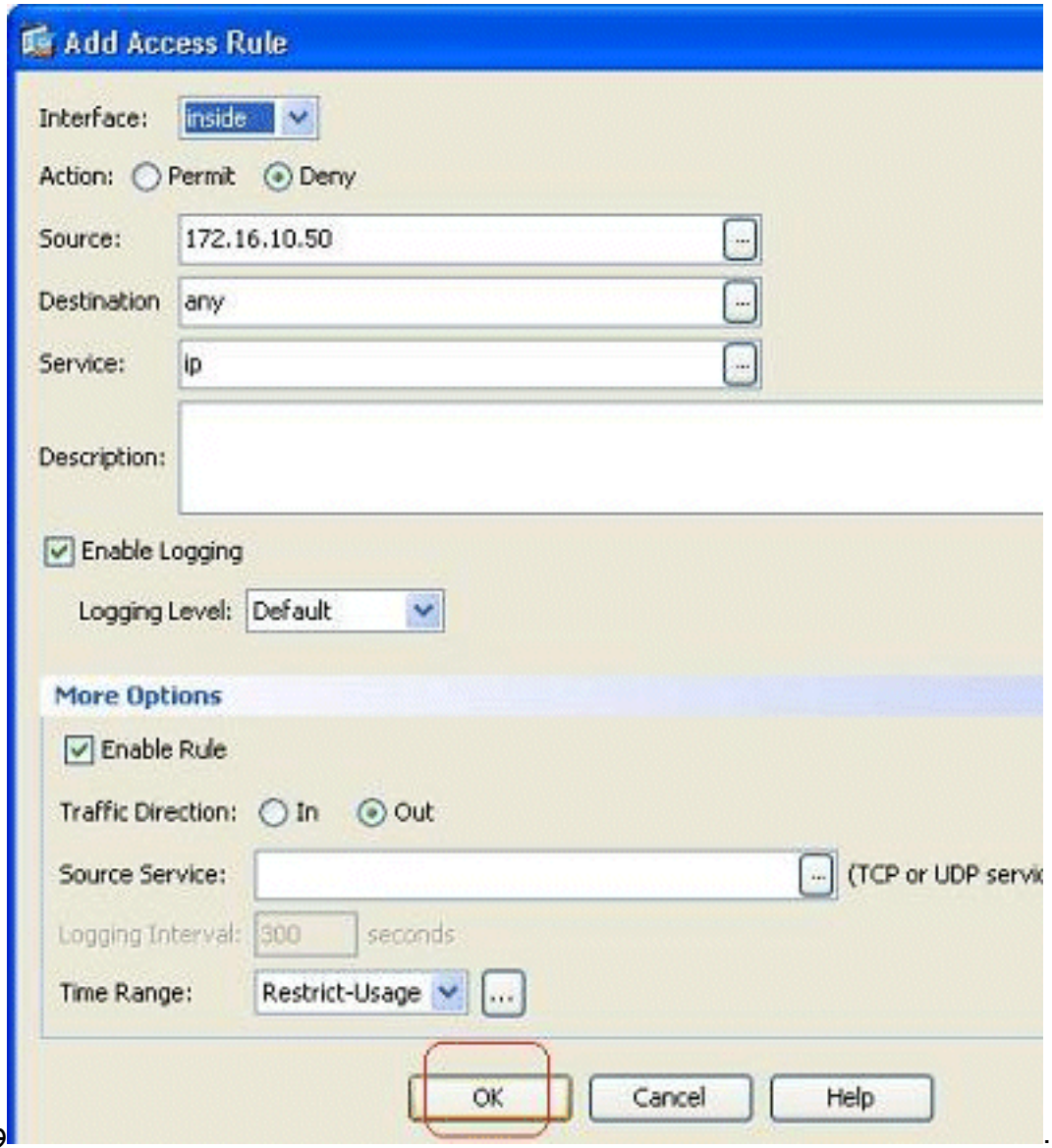


4. يمكنكم رؤية النطاق الزمني هنا. انقر فوق **موافق** للعودة إلى الإطار "قاعدة إضافة



الوصول".

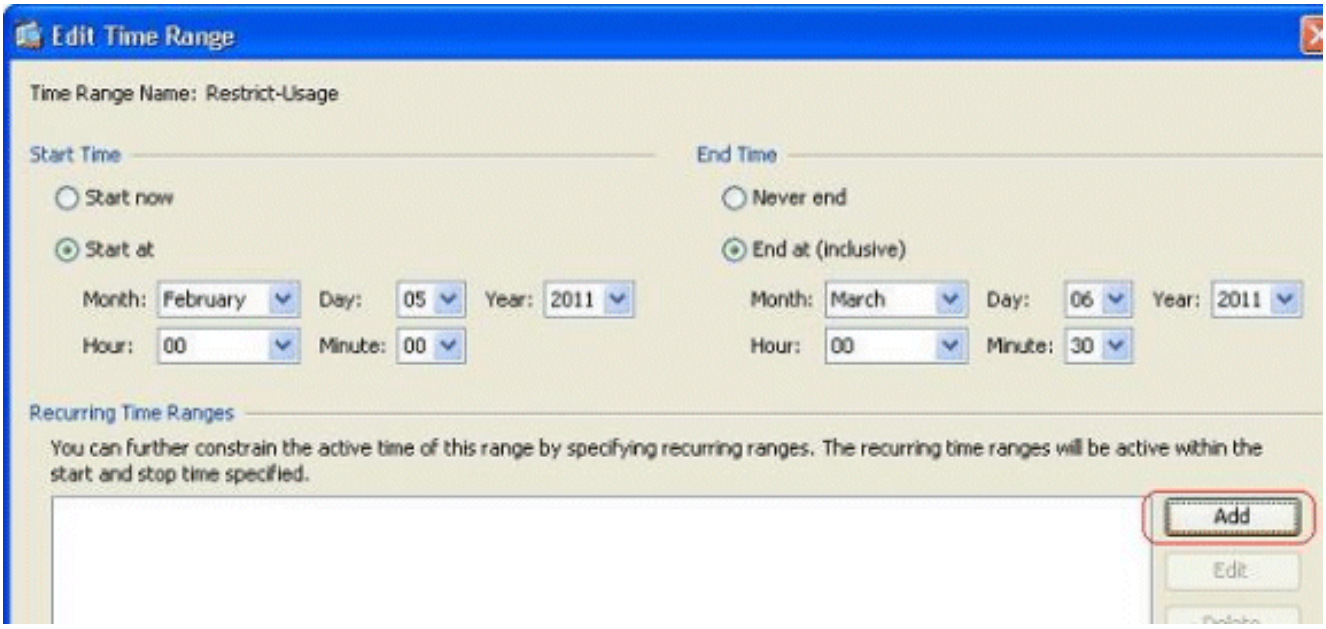
5. يمكنك الآن أن ترى أن نطاق وقت تقييد الاستخدام قد تم ربطه بقاعدة الوصول



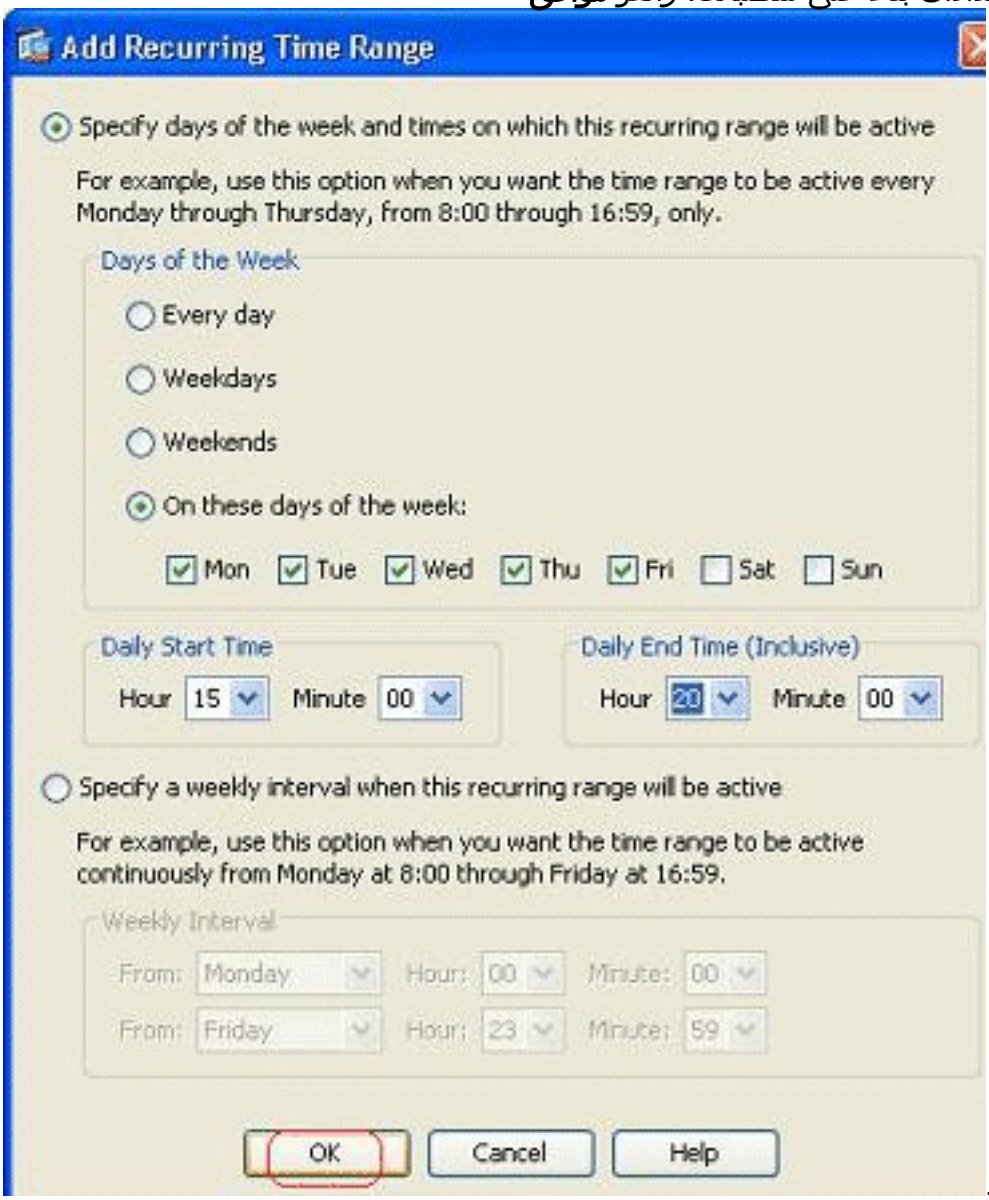
وفقا لتكوين هذه. قاعدة الوصول هذه، تم منع المستخدم في 172.16.10.50 من إستخدام أي موارد من الساعة 2011/5/05 إلى الساعة 2011/16/06 الساعة 17/4.30. هذا هو مخرج واجهة سطر الأوامر (CLI) المكافئ:

```
time-range Restrict-Usage
absolute start 14:00 05 February 2011 end 16:30 06 February 2011
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

6. فيما يلي مثال على كيفية تحديد نطاق زمني متكرر. انقر فوق **إضافة** لتحديد نطاق زمني متكرر.

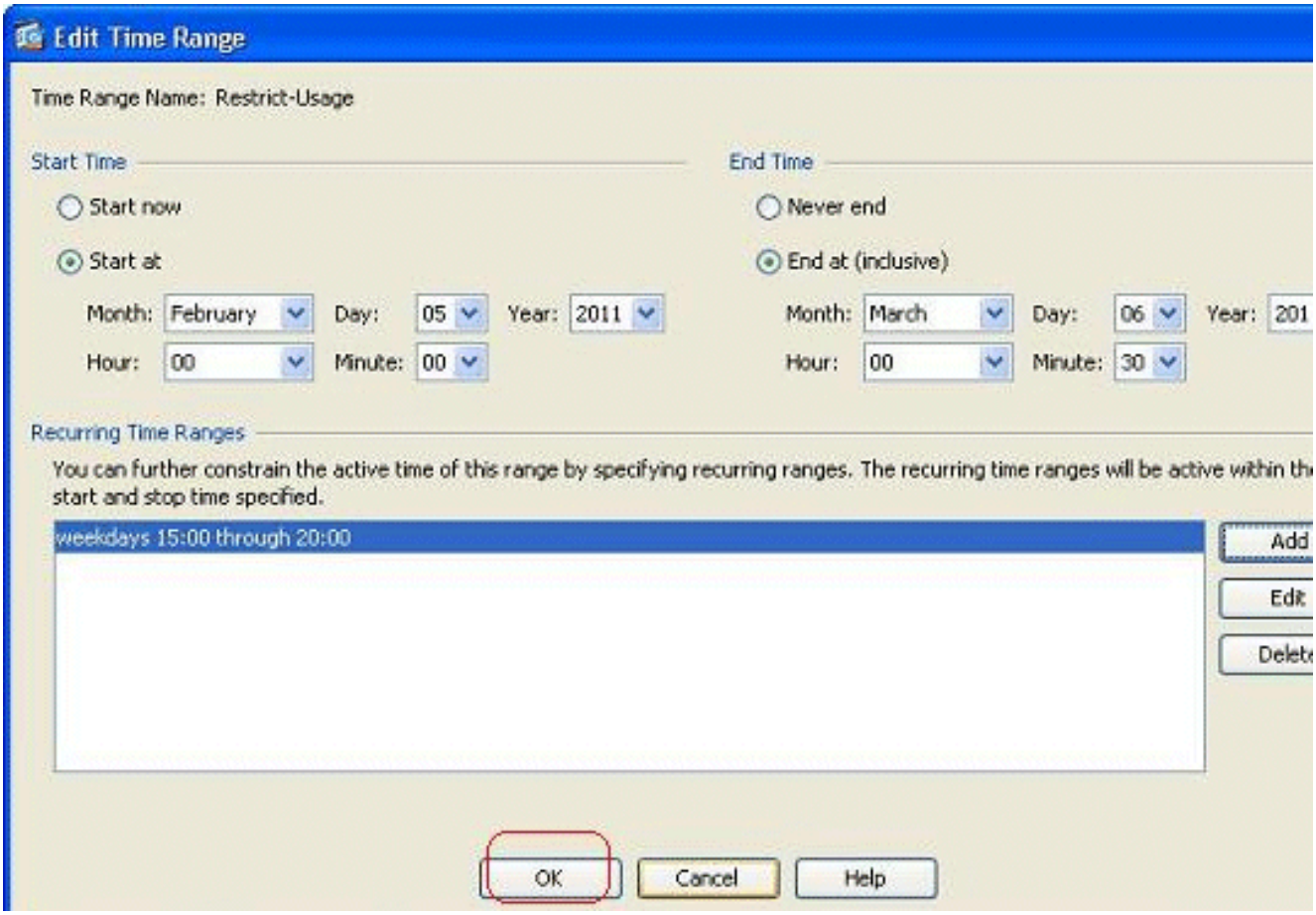


7. حدد الإعدادات بناء على متطلباتك، وانقر **موافق**



للاكتمال.

8. طقطقة in order to **ok** رجعت إلى المدى الزمني نافذة.



وفقا لهذا التكوين، تم منع المستخدم في 172.16.10.50 من الوصول إلى أي موارد من الساعة 3 مساء إلى 8 مساء في جميع أيام الأسبوع باستثناء يومي السبت والأحد.

```
!
time-range Restrict-Usage
absolute start 00:00 05 February 2011 end 00:30 06 March 2011
periodic weekdays 15:00 to 20:00
!
access-list inside_access_out extended deny ip host 172.16.10.50 any
time-range Restrict-Usage
!
access-group inside_access_out in interface inside
```

ملاحظة: إذا كان للأمر **بالنطاق الزمني** قيم مطلقة ودورية محددة، فسيتم تقييم الأوامر **الدورية** فقط بعد الوصول إلى وقت البدء المطلق، ولا يتم تقييمها أكثر بعد الوصول إلى وقت النهاية المطلقة.

معلومات ذات صلة

- صفحة وثائق Cisco ASA
- 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).