

# (هيجوتل اءءاع) ذفنملا هيجوت اءاع: ASA 8.2 Access-Static و Global و NAT رماوا مادختساب ASDM مادختساب list

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [الرسم التخطيطي للشبكة](#)
- [السماح بالوصول الصادر](#)
- [السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام NAT](#)
- [السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام PAT](#)
- [تقييد الوصول إلى الشبكات الخارجية للمضيفين الداخليين](#)
- [السماح بحركة المرور بين الواجهات ذات مستوى الأمان نفسه](#)
- [السماح للمضيفين غير الموثوق بهم بالوصول إلى الأجهزة المضيفة على شبكتك الموثوق بها](#)
- [تعطيل NAT للمضيفين/الشبكات المحددة](#)
- [إعادة توجيه المنفذ \(إعادة توجيه\) باستخدام الحالات](#)
- [الحد من جلسة TCP/UDP باستخدام ثابت](#)
- [قائمة الوصول المستندة إلى الوقت](#)
- [معلومات ذات صلة](#)

## 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

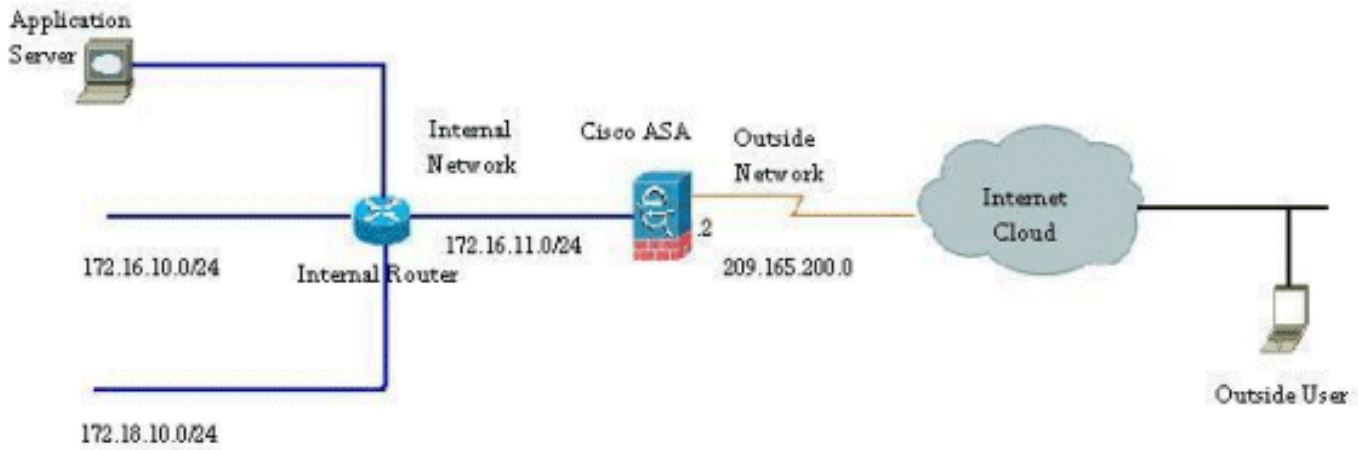
**ملاحظة:** يعمل هذا التكوين بشكل جيد من برنامج Cisco ASA الإصدار 8.0 إلى 8.2 فقط، نظرا لعدم وجود تغييرات رئيسية في وظيفة NAT.

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

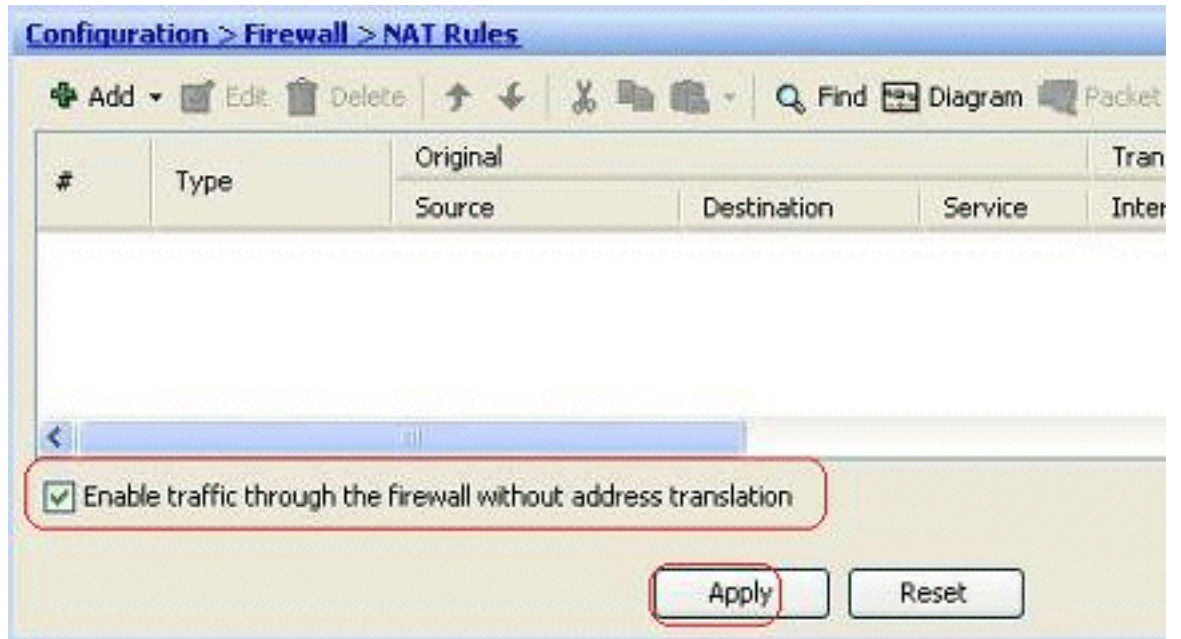


مخططات عنوانة IP المستخدمة في هذا التكوين غير قابلة للتوجيه من الناحية القانونية على الإنترنت. وهي عناوين RFC 1918 التي تم استخدامها في بيئة مختبرية.

## 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 اتصالات 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.

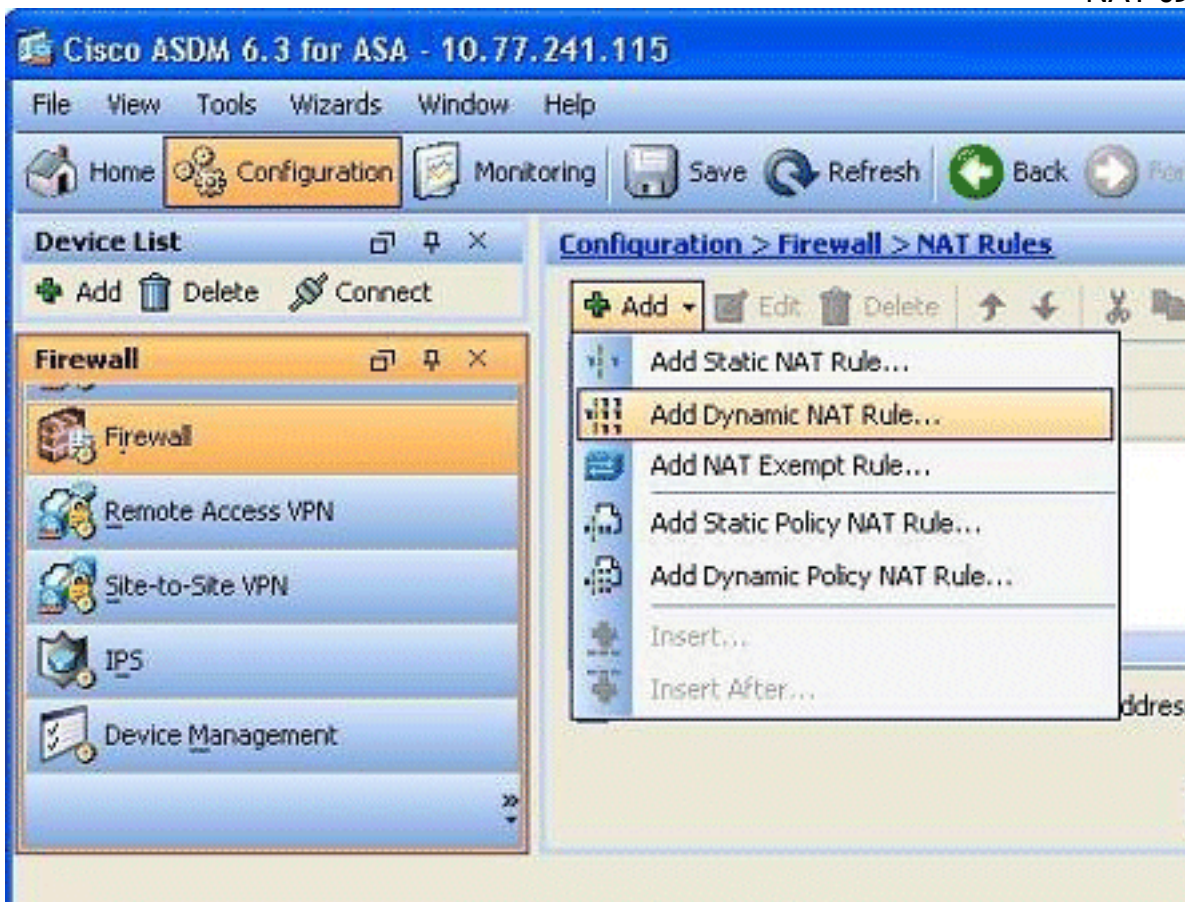


## السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام NAT

أنت تستطيع 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 اختر خيار إضافة قاعدة NAT الديناميكية لتكوين قاعدة NAT



الديناميكية.

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

يستعمل ال تفاصيل زر في المصدر  
مجال.

**Add Dynamic NAT Rule**

Original

Interface:

Source:

Translated

Select a global pool for dynamic translation.

Pool ID	Interface	Addresses Pool
0	(outbound)	Same as original address (identity)
0	(inbound)	Same as original address (identity)

Connection Settings

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

**Browse Source**

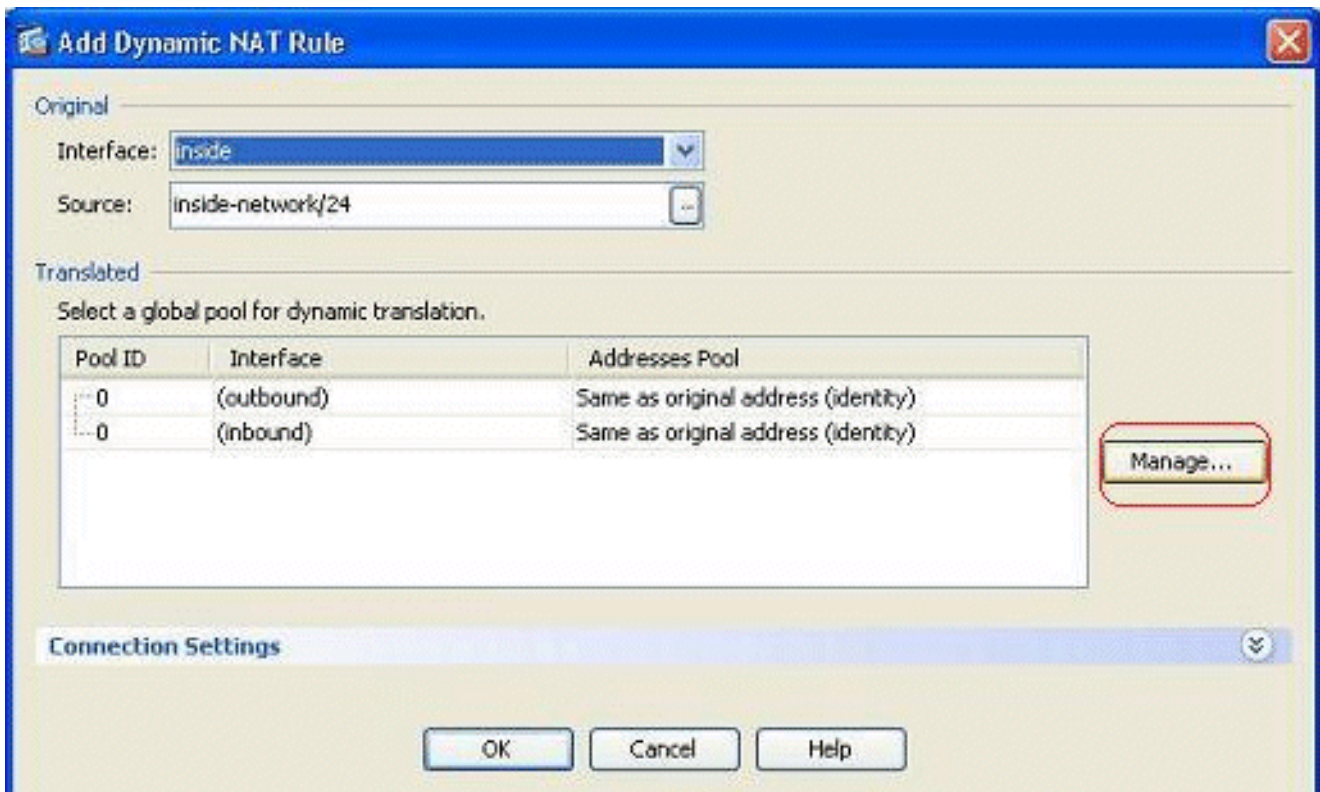
Filter:

Name	IP Address	Netmask	Description	Object NAT Add
IPv4 Network Objects				
any	0.0.0.0	0.0.0.0		
inside-n...	172.16.11.0	255.255.255.0		
manage...	10.77.241.64	255.255.255.192		
outside-...	209.165.200.0	255.255.255.224		
20.1.1.10	20.1.1.10	255.255.255.255		
172.16....	172.16.11.1	255.255.255.255		
172.16....	172.16.11.10	255.255.255.255		
172.16....	172.16.12.2	255.255.255.255		
209.16...	209.165.200.10	255.255.255.255		

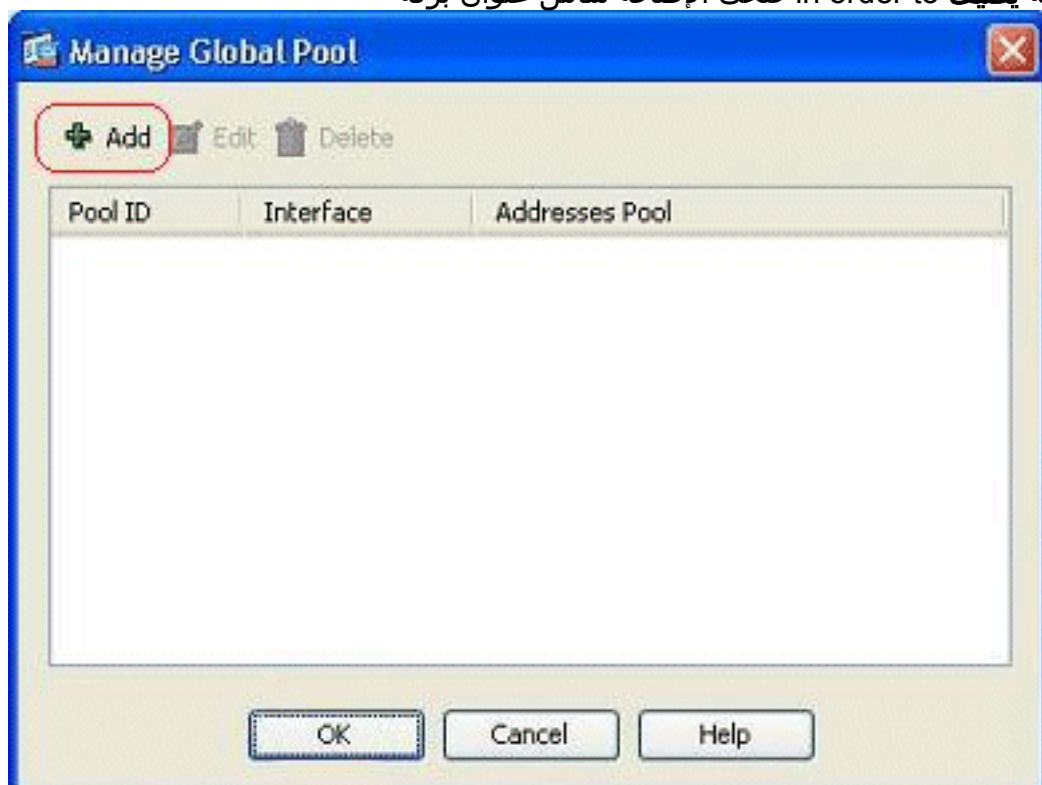
Selected Source

Source ->

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

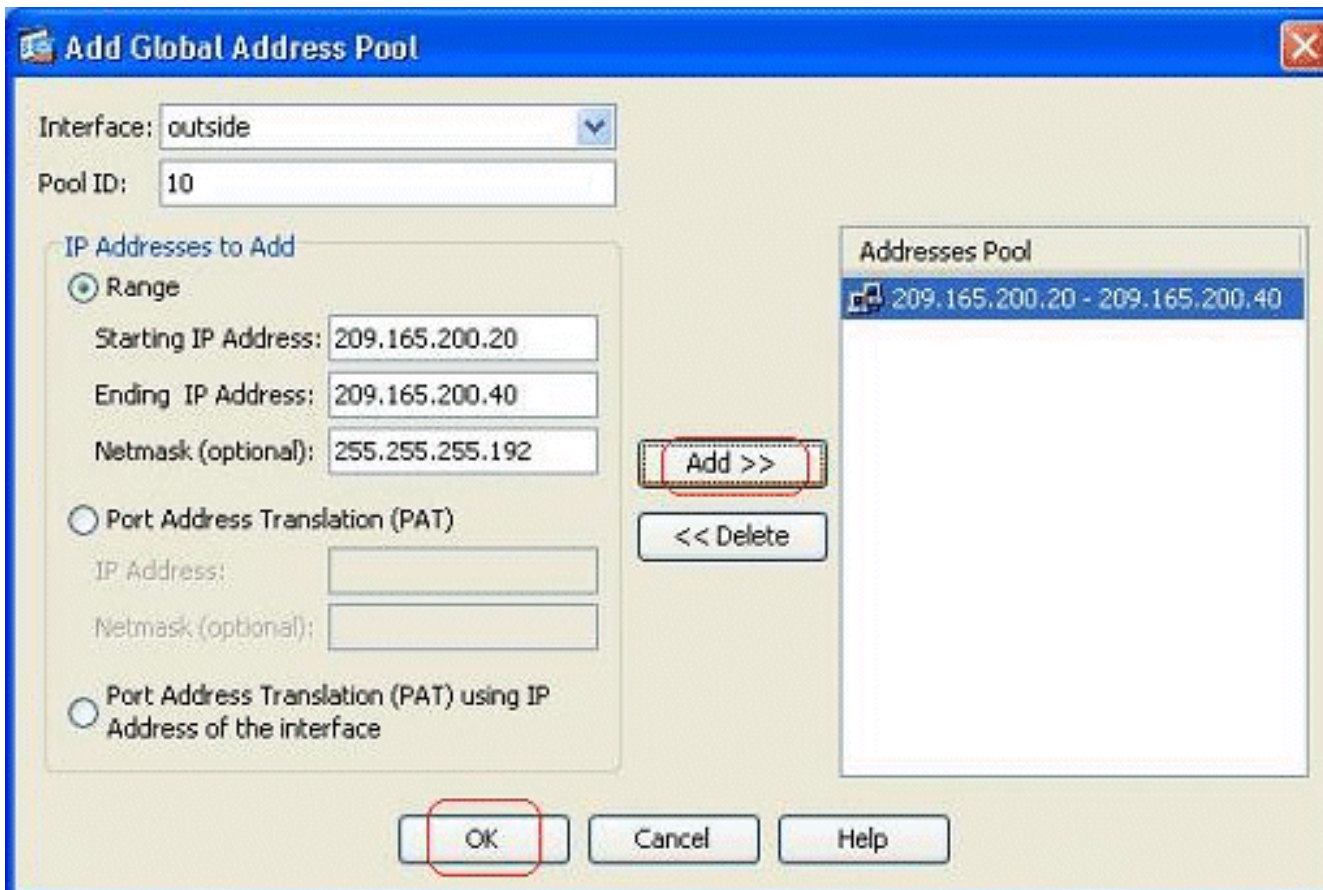


5. طقطقة يضيف in order to فتحت الإضافة شامل عنوان بركة

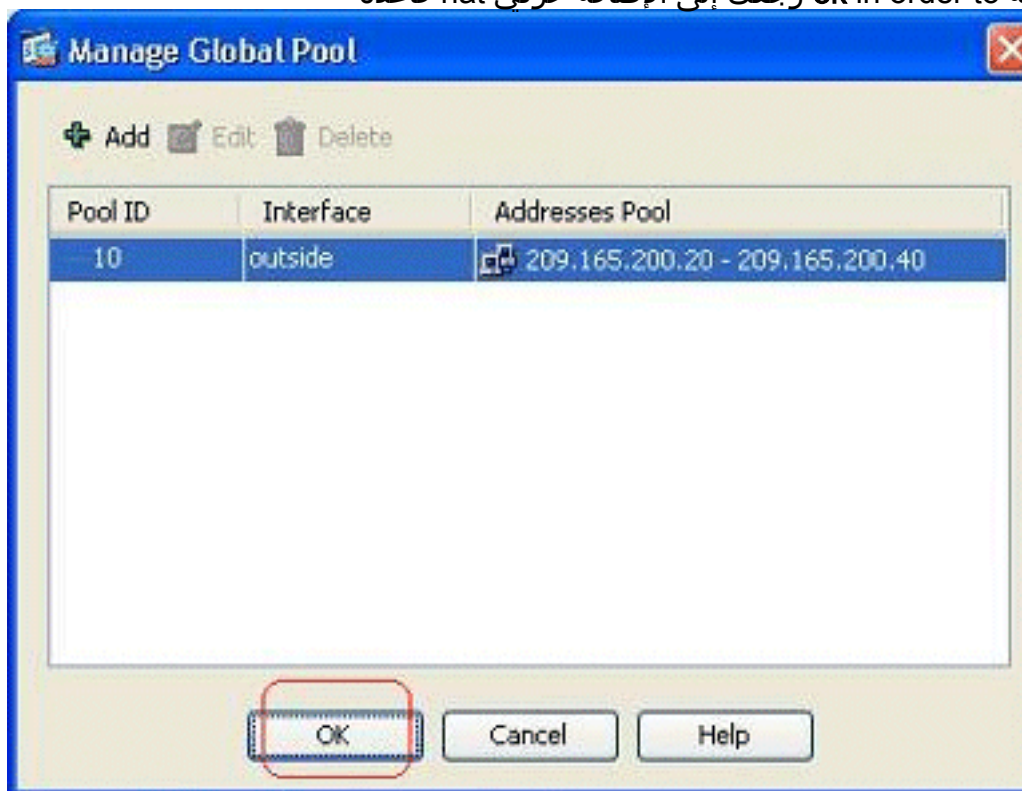


نافذة.

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 ok in order to رجعت إلى الإدارة بركة شامل نافذة.

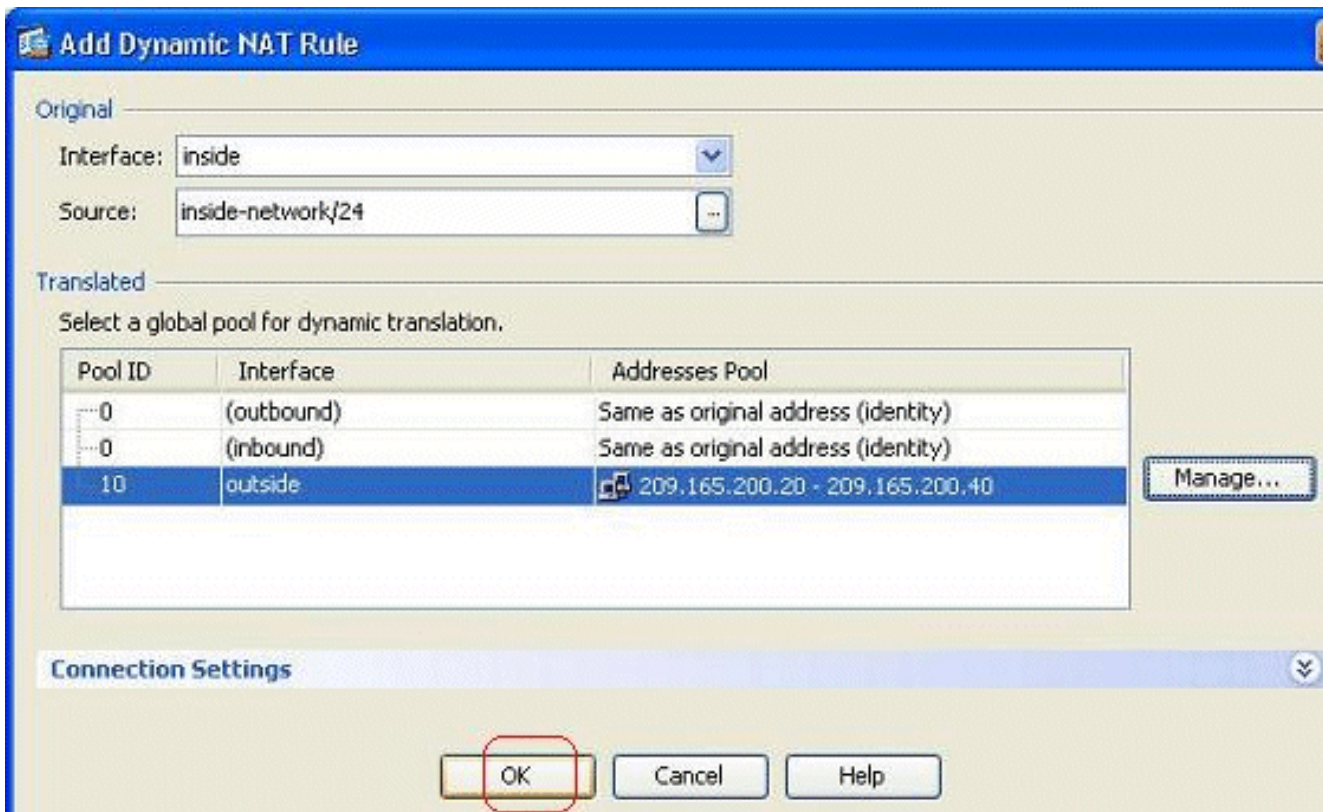


7. طقطقة إلى الإضافة حركي قاعدة nat ok in order to رجعت

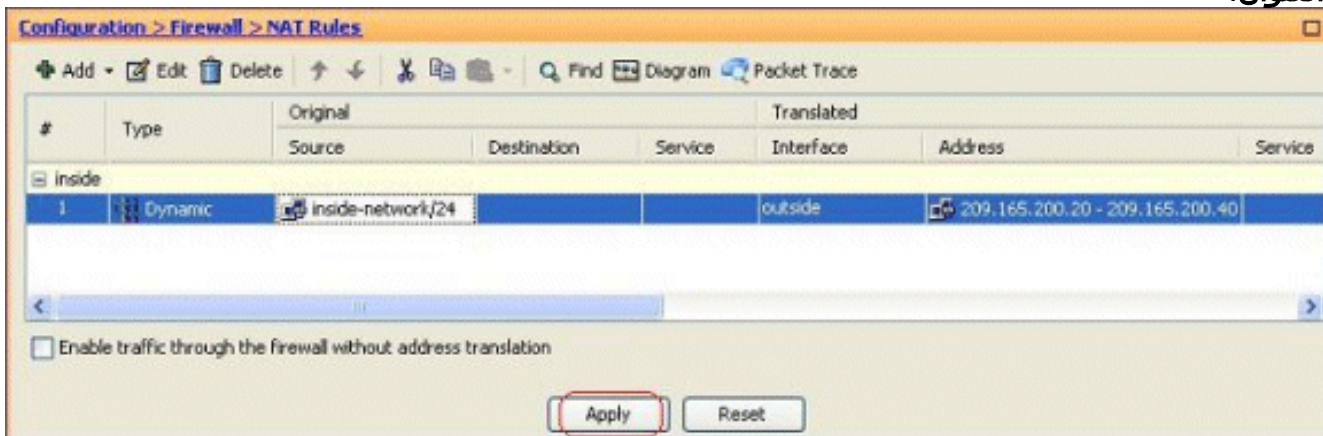


نافذة.

8. طقطقة ok in order to أتمت الحركي قاعدة nat 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، سيتم ترجمة الأجهزة المضيفة في شبكة 172.16.11.0 إلى أي عنوان IP من تجمع NAT، 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 تستطيع حاولت طبقت ضرب أو أنت تستطيع حاولت أن يحرر العنوان موجود بركة أن يمدده.

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

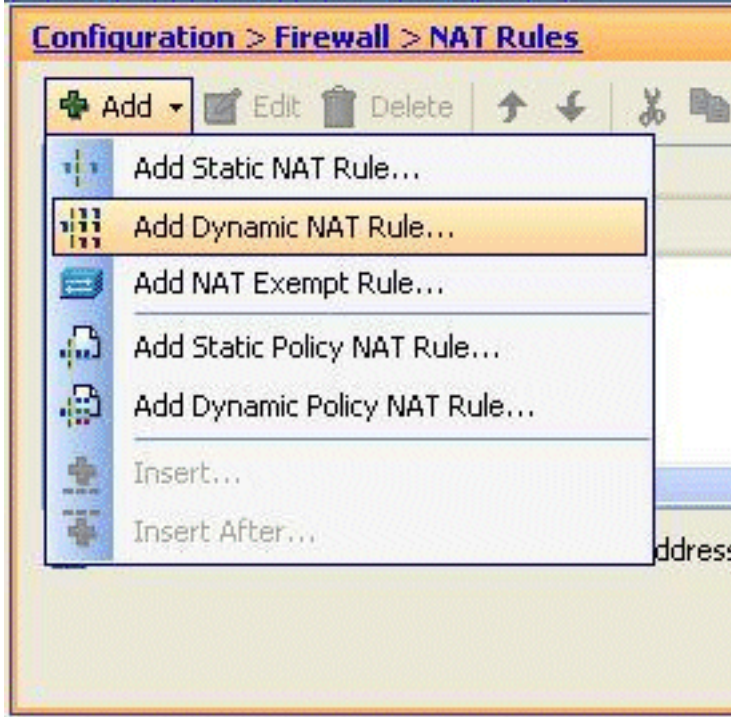


## السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام PAT

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.

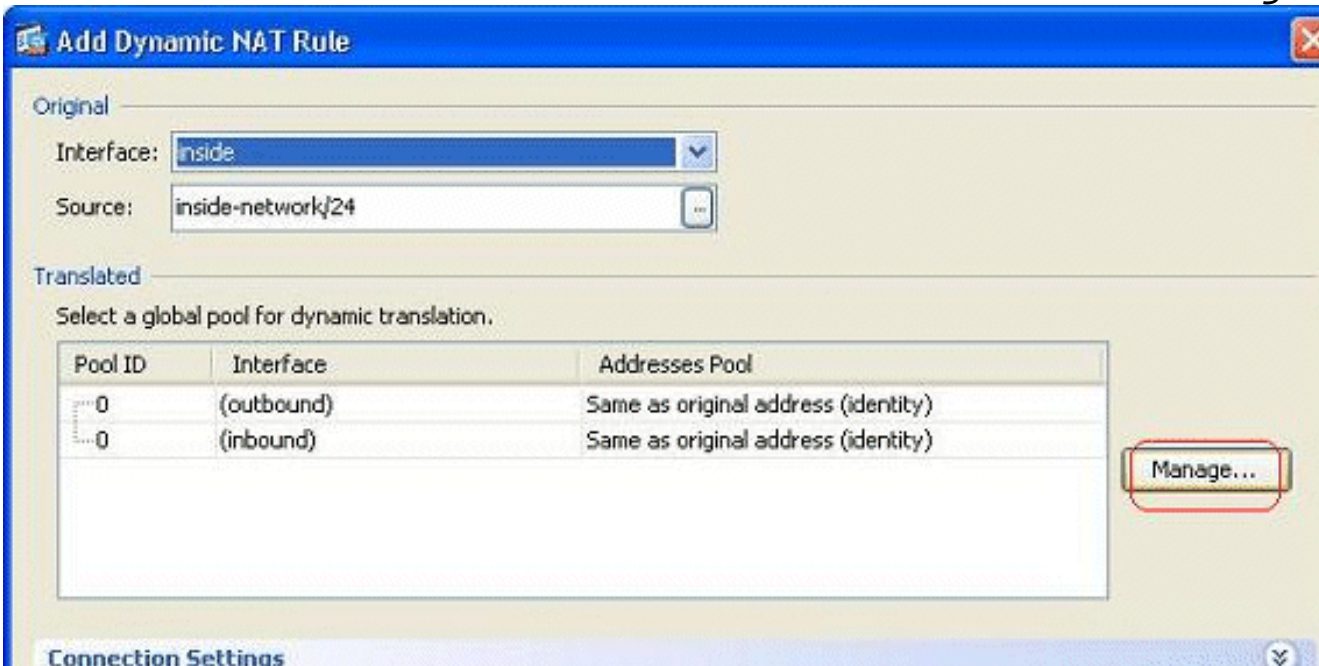
أتمت هذا steps in order to سمحت داخلي مضيف منفذ إلى شبكة خارجي مع ضرب:

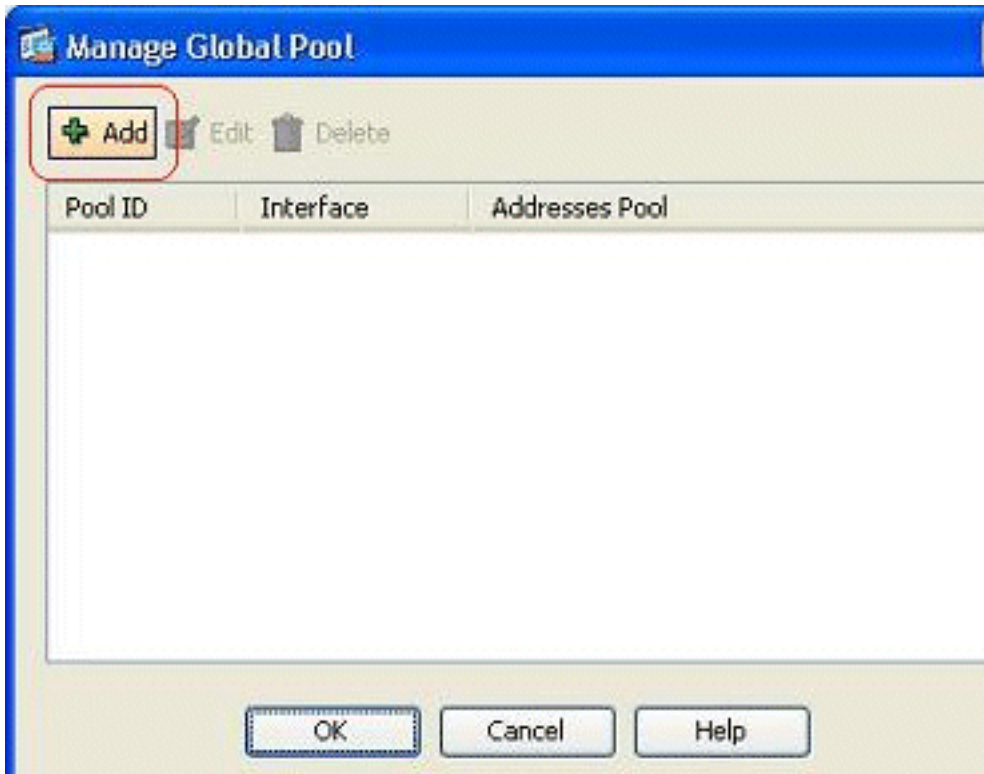
1. انتقل إلى التكوين < جدار الحماية> قواعد NAT، انقر إضافة، ثم اختر خيار إضافة قاعدة NAT الديناميكية



لتكوين قاعدة NAT الديناميكية.

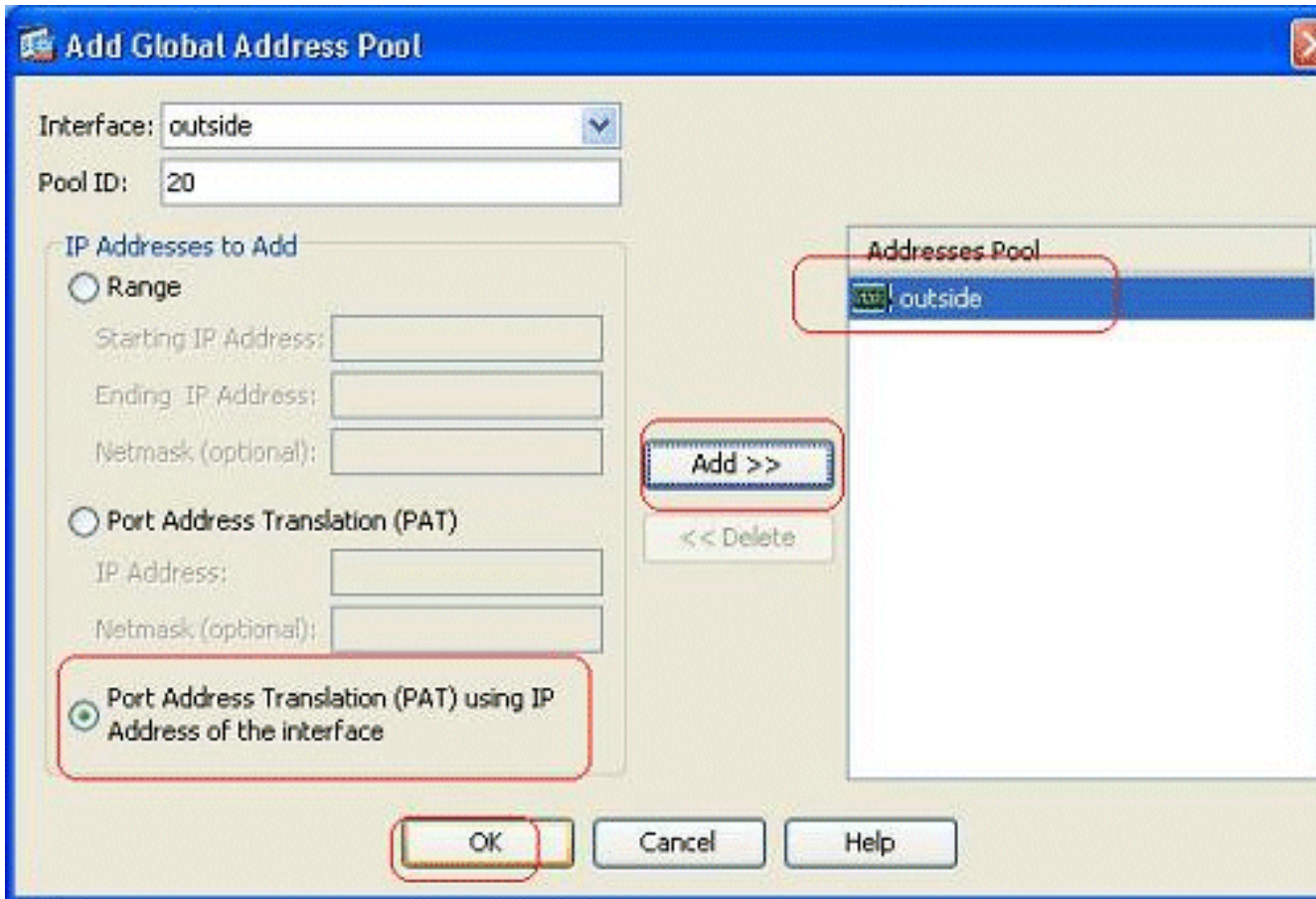
2. أخترت الاسم من القارن إلى أي المضيف حقيقي يكون ربطت. أخترت العنوان حقيقي من المضيف/شبكة يستعمل ال تفاصيل زر في المصدر مجال، واخترت داخل شبكة. قطعة يدير in order to عينت ال يترجم عنوان معلومة.



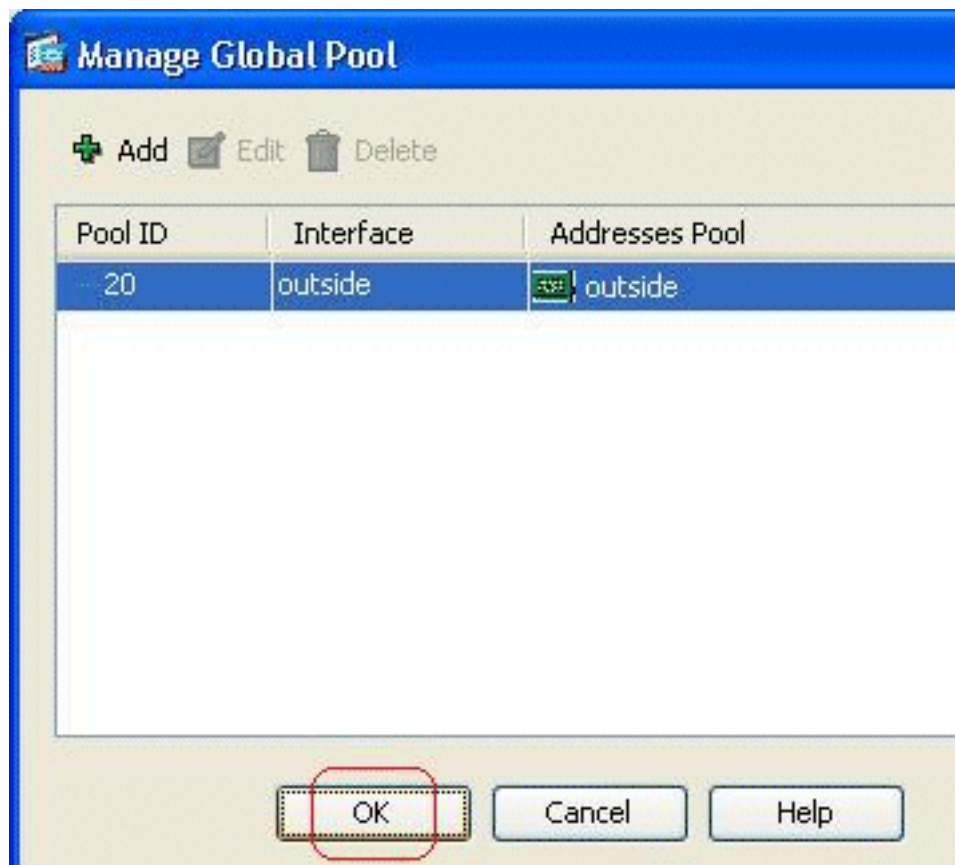


3. انقر فوق إضافة (Add).

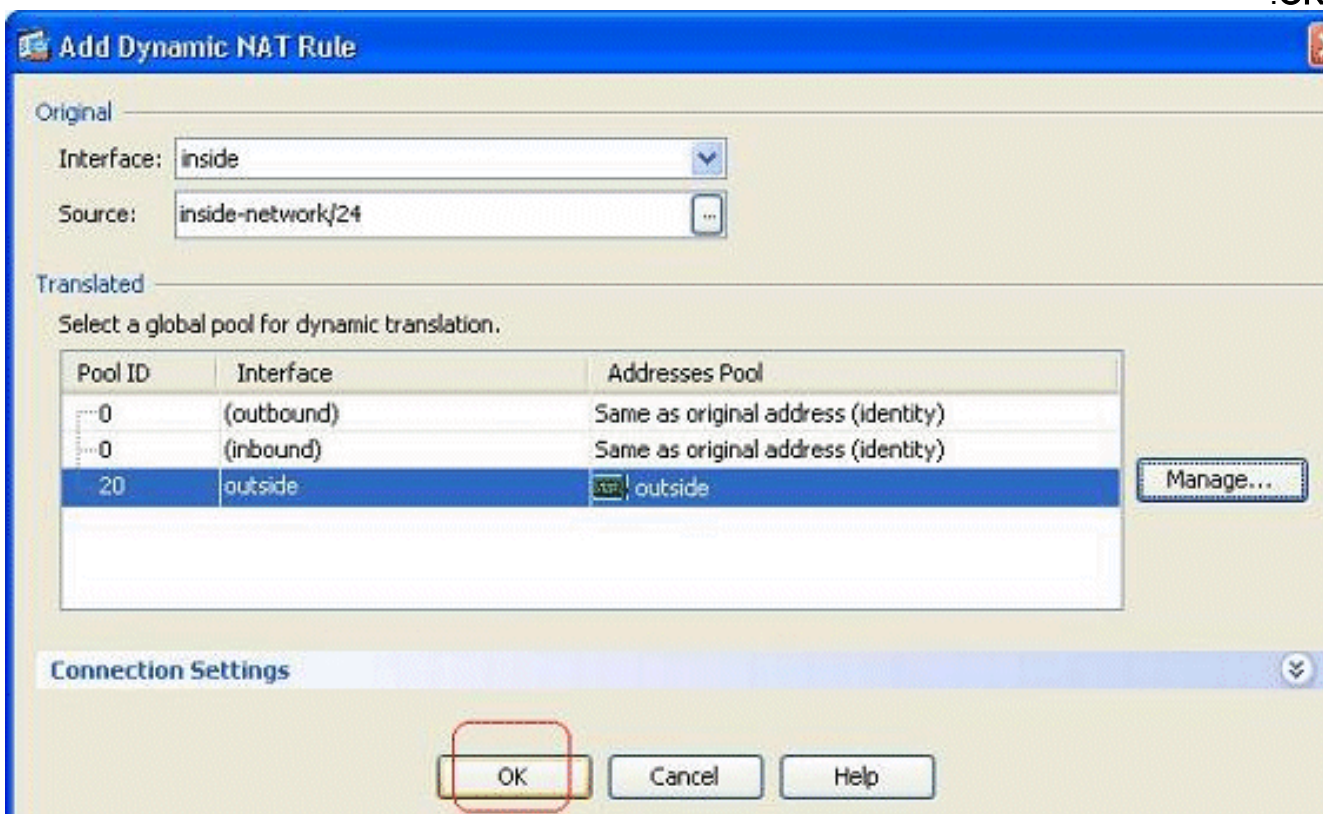
4. أخترت الأيسر عنوان ترجمة (ضرب) يستعمل عنوان من القارن خيار، وطققة يضيف in order to أضفت هو إلى العنوان بركة. لا تنس تعيين معرف فريد لتجمع عناوين NAT هذا.



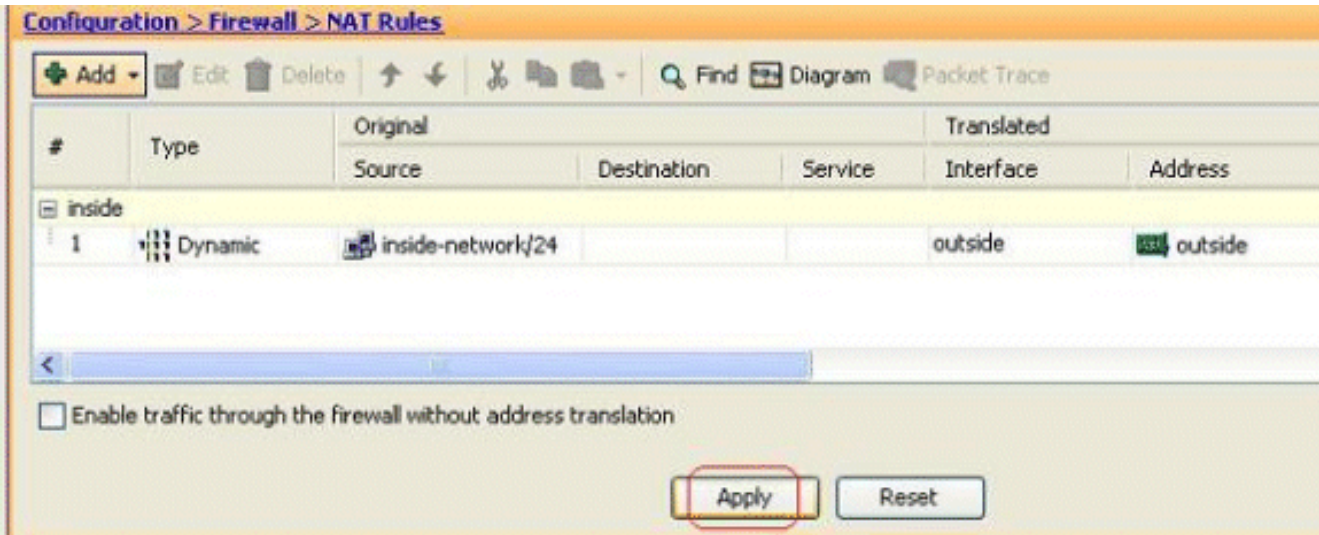
5. كما هو موضح هنا هو تجمع العناوين الذي تم تكوينه مع الواجهة الخارجية كعنوان متاح فقط في هذا التجمع. طقطقة ok in order to رجعت إلى الإضافة حركي nat قاعدة



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
```

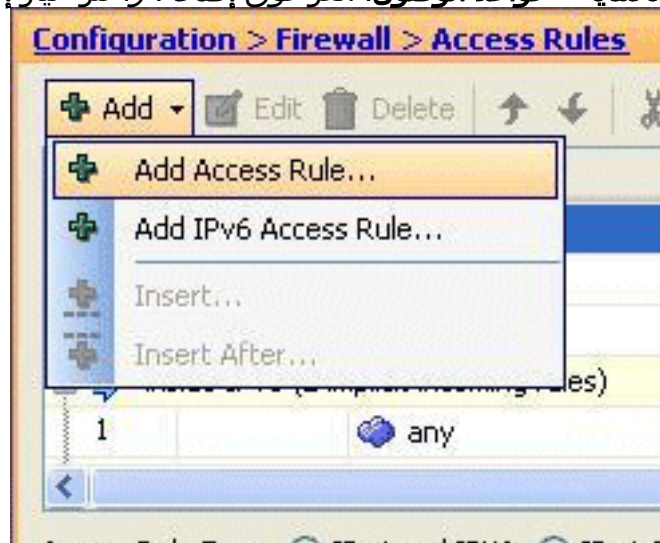
## تقييد الوصول إلى الشبكات الخارجية للمضيفين الداخليين

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، استخدم 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.

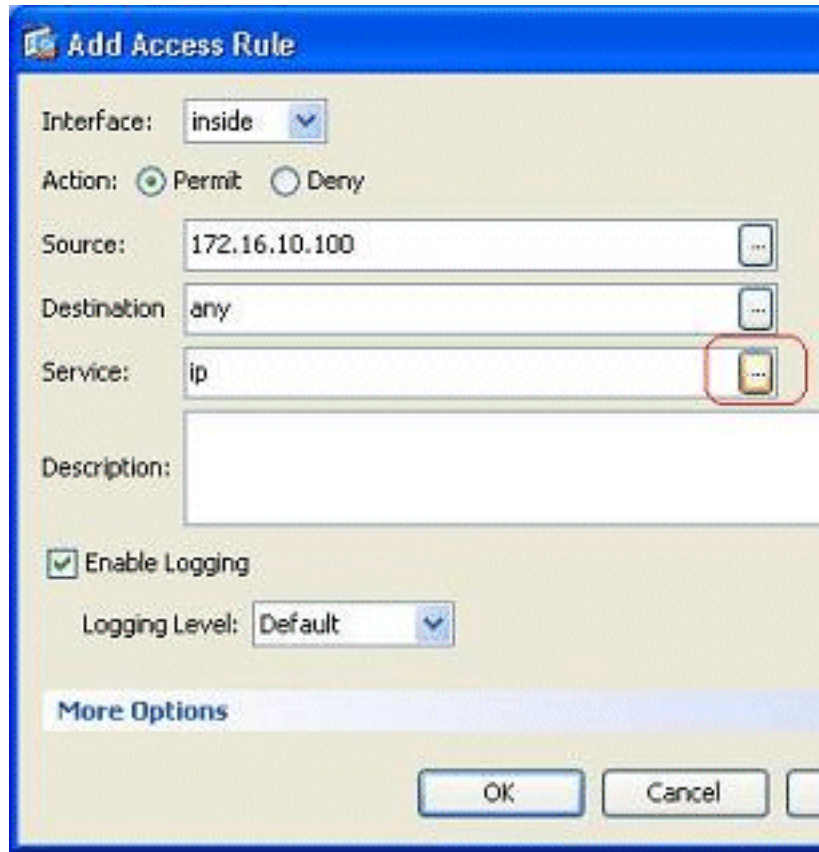
أكمل الخطوات التالية:

1. انتقل إلى التكوين < جدار الحماية > قواعد الوصول، انقر فوق إضافة، واختر خيار إضافة قاعدة الوصول لإنشاء



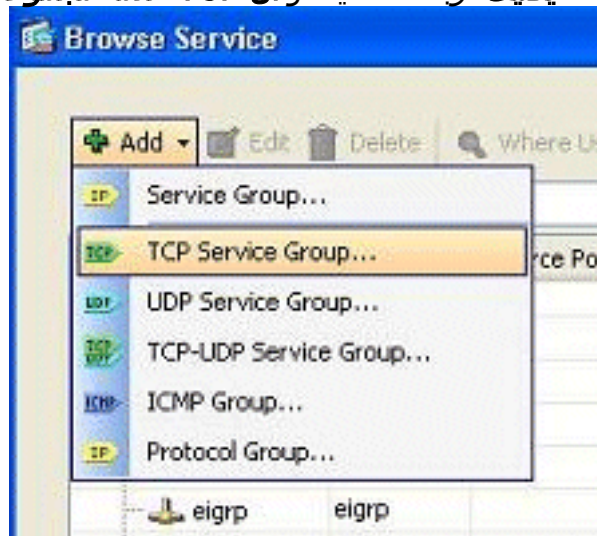
إدخال قائمة وصول جديد.

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



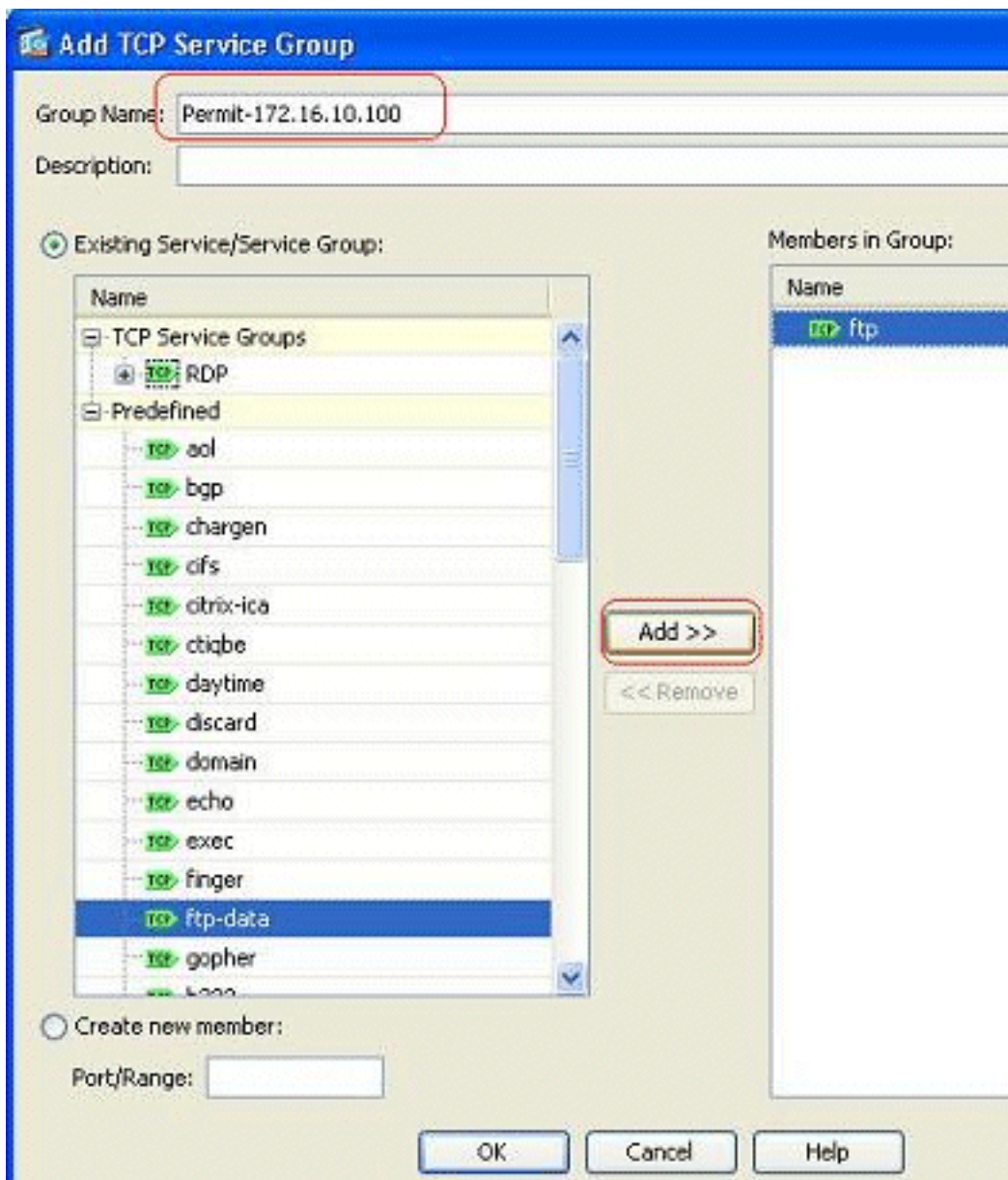
ميناء.

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

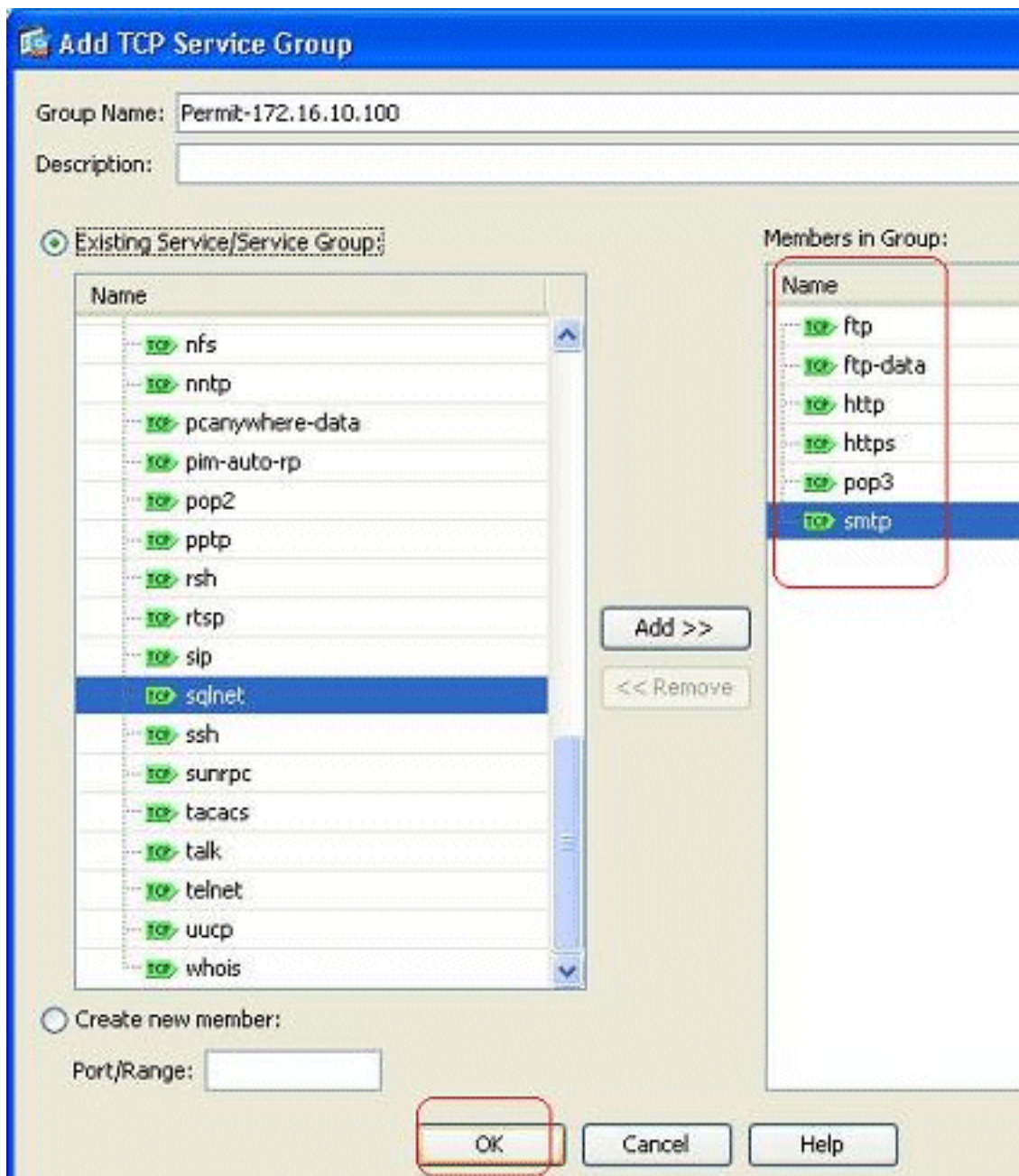


خيار.

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

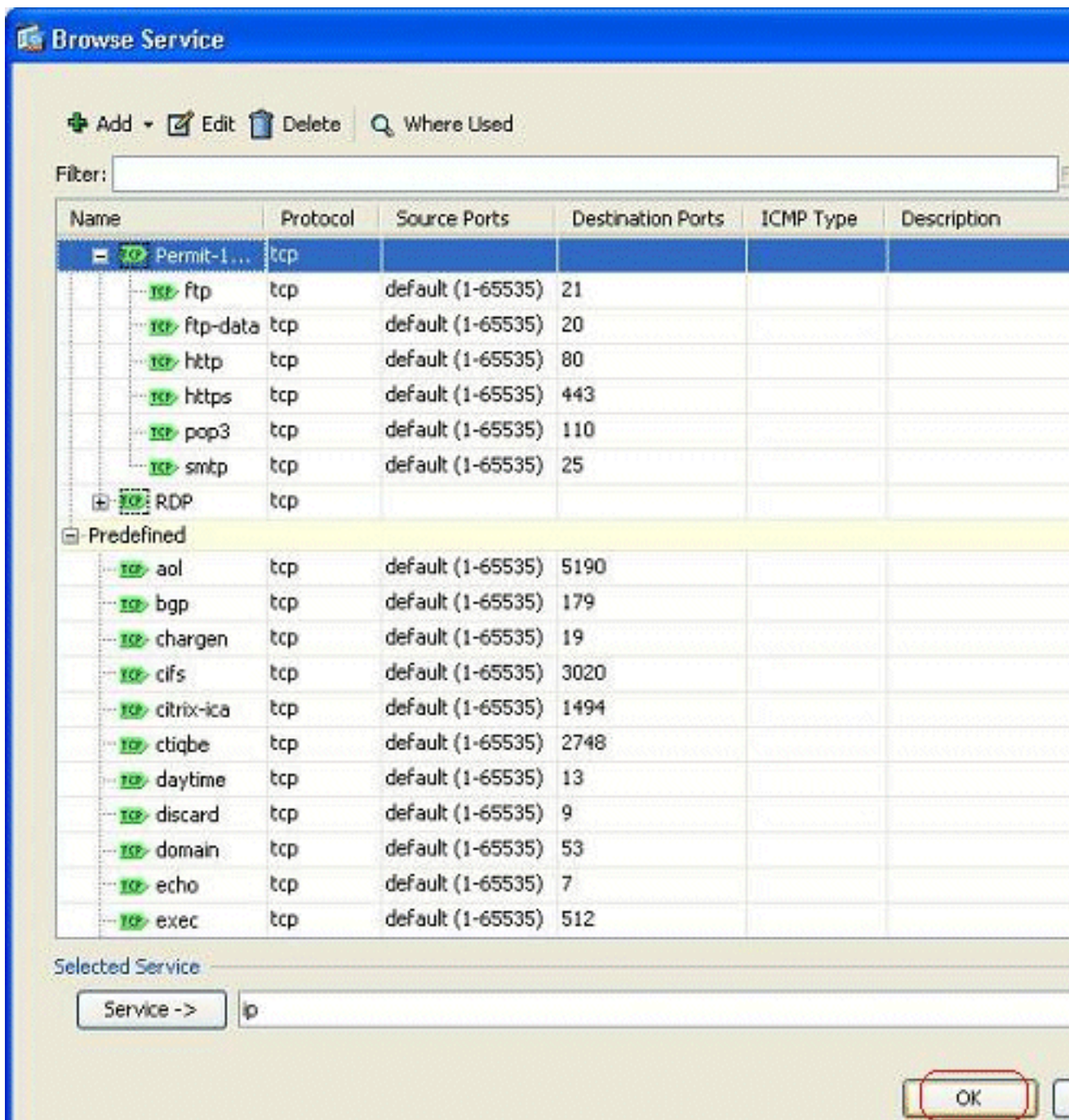


في مجموعة مجال.  
5. يجب أن ترى جميع المنافذ المحددة في الحقل الأيمن. طقطقة ok in order to أتمت الخدمة ميناء يحدد



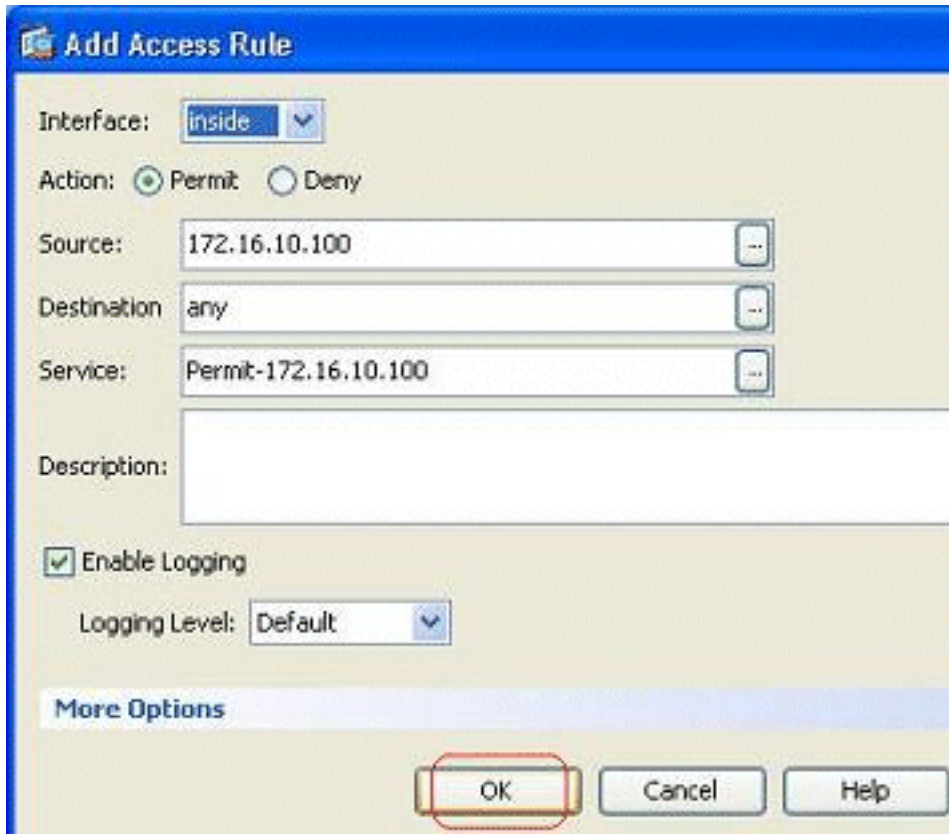
عملية.

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



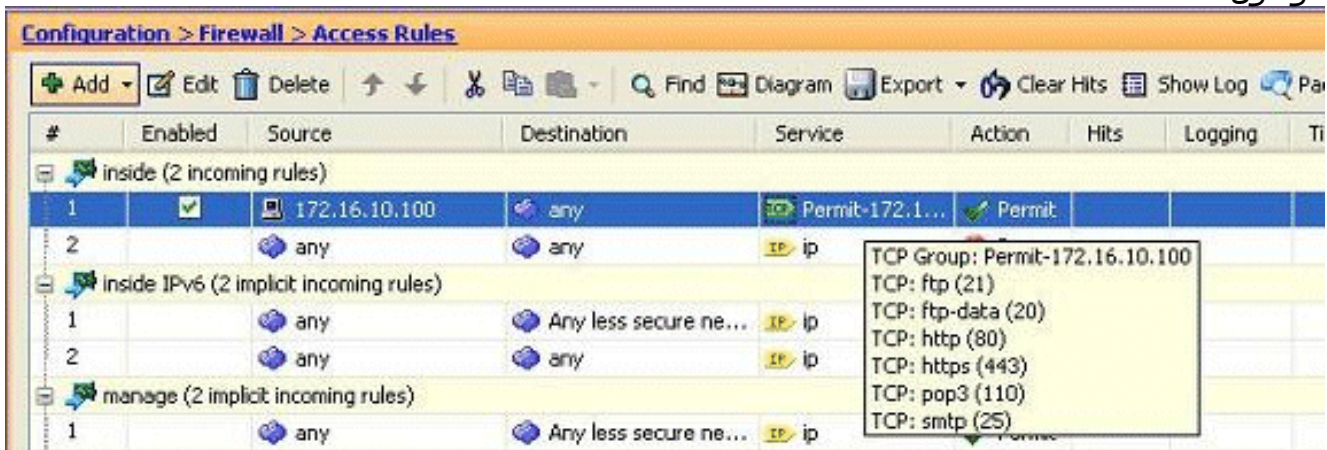
7. طقطقة ok in order to أتمت



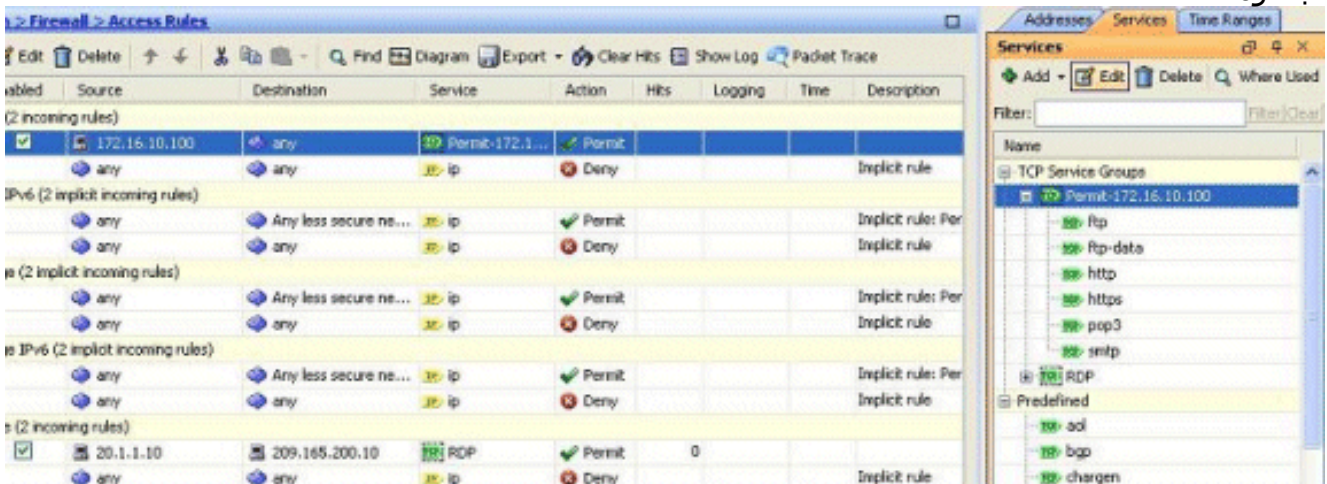


التشكيل.

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

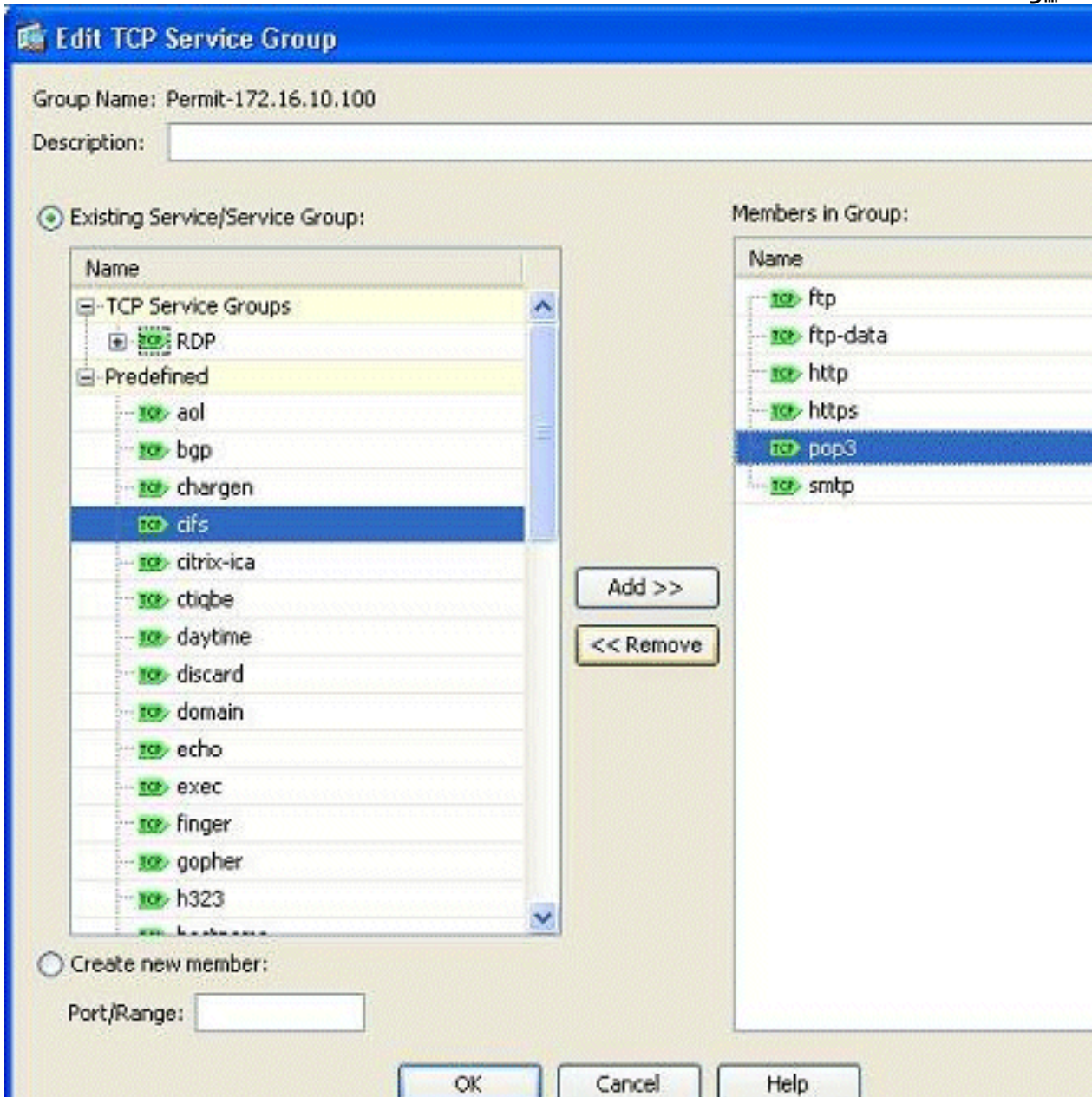


9. لسهولة الاستخدام، يمكنك أيضا تحرير مجموعة خدمة TCP مباشرة على الجزء الأيمن في علامة التبويب خدمات. انقر فوق تحرير لتعديل مجموعة الخدمات هذه مباشرة.

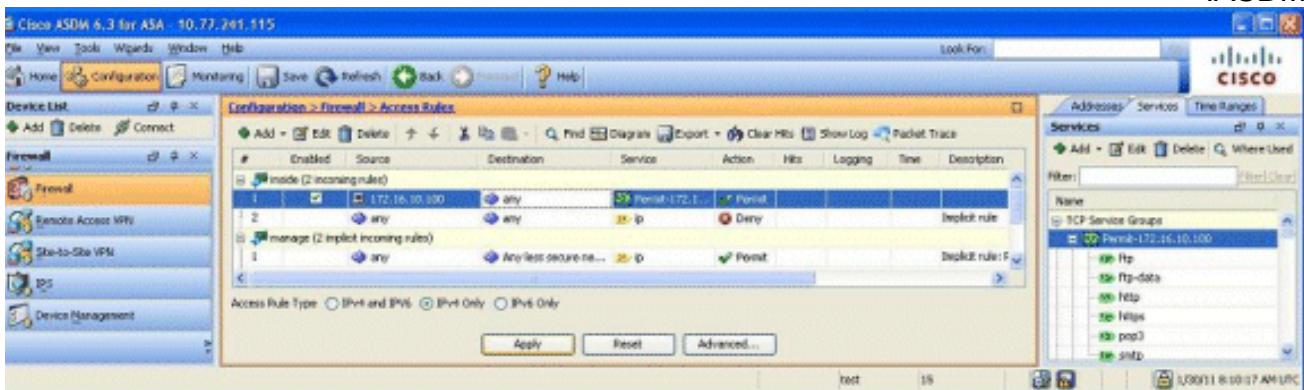


10. يعيد التوجيه مرة أخرى إلى نافذة تحرير مجموعة خدمة TCP. قم بإجراء التعديلات استنادا إلى متطلباتك،

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.

Configuration > Device Setup > Interfaces

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Redundancy
Ethernet0/0	outside	Yes	0	209.165.200.2	255.255.255.192	No
Ethernet0/1	inside	Yes	100	172.16.11.10	255.255.255.0	No
Ethernet0/2	manage	Yes	90	10.77.241.115	255.255.255.192	No
Ethernet0/3		No				No

Enable traffic between two or more interfaces which are configured with same security levels

Enable traffic between two or more hosts connected to the same interface

Apply Reset

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.

Configuration > Device Setup > Interfaces

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Redun
Ethernet0/0	outside	Yes	0	209.165.200.2	255.255.255.192	No
Ethernet0/1	inside	Yes	100	172.16.11.10	255.255.255.0	No
Ethernet0/2	manage	Yes	90	10.77.241.115	255.255.255.192	No
Ethernet0/3		No				No

Enable traffic between two or more interfaces which are configured with same security levels  
 Enable traffic between two or more hosts connected to the same interface

Apply Reset

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:

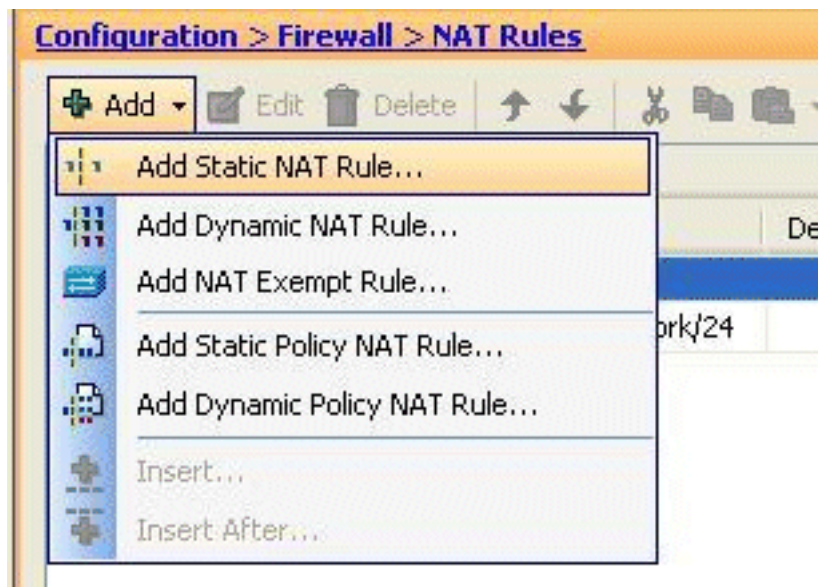
```
access-list 101 permit TCP any host 209.165.200.5
```

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.

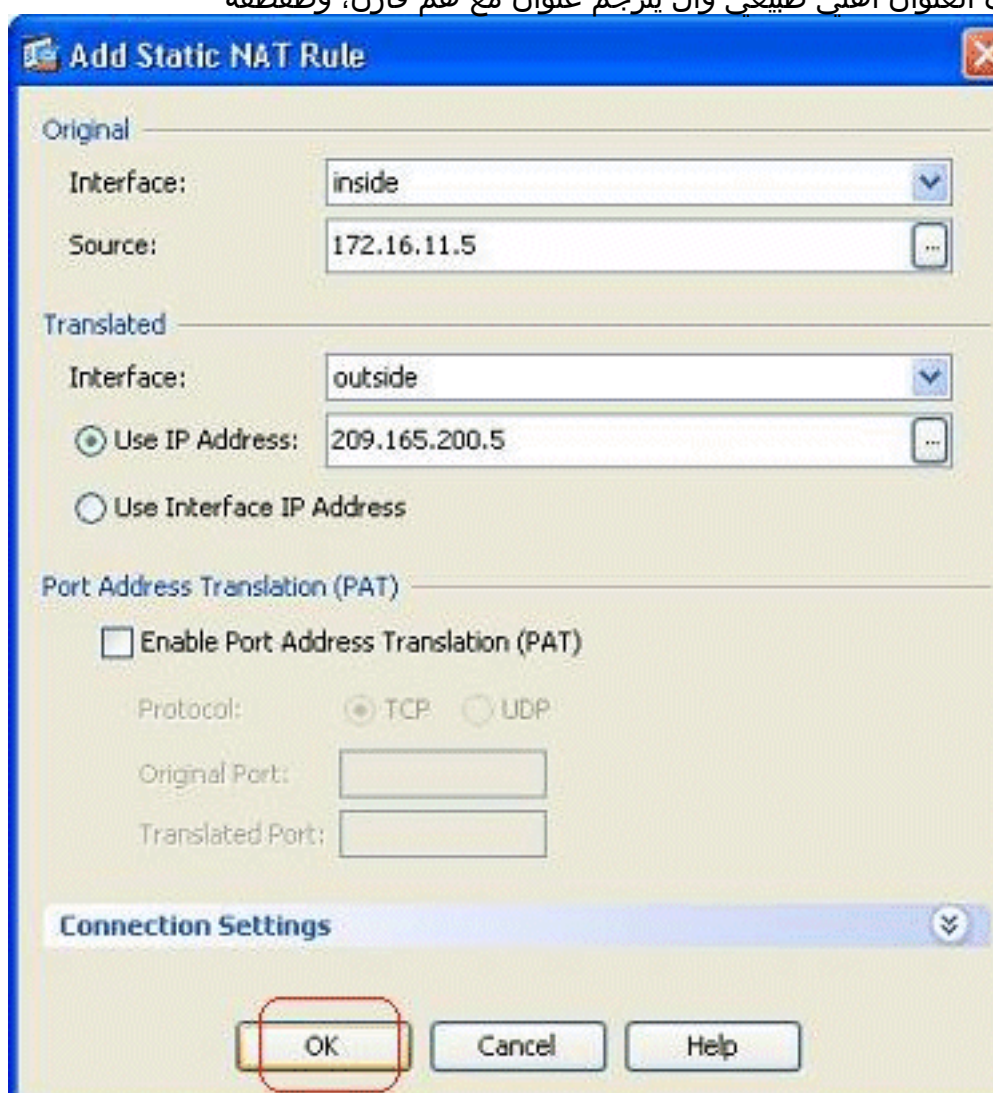
أتمت هذا steps in order to شكلت الساكن إستاتيكي nat:

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



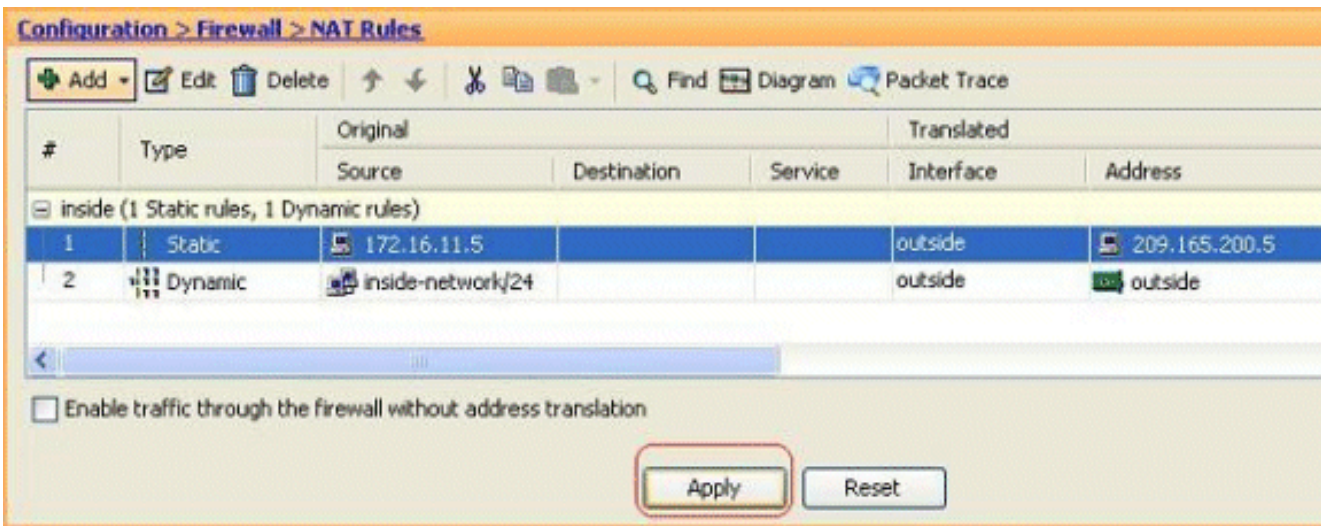
الثابتة.

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



.ok

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



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

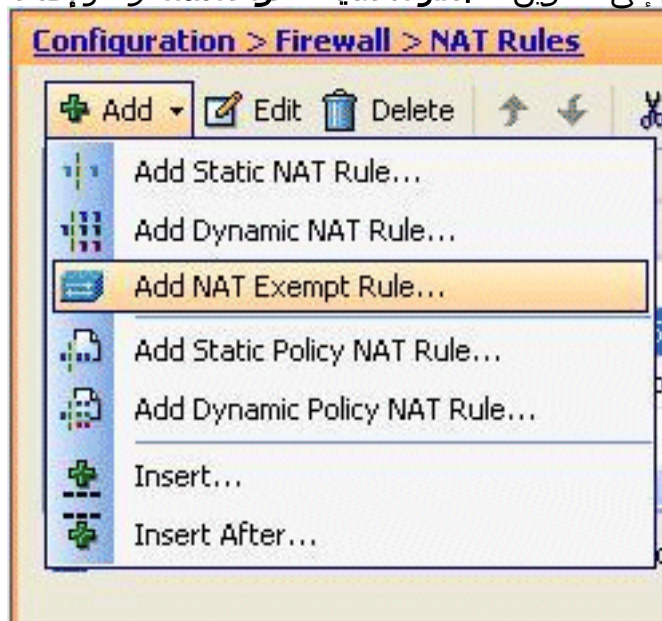
```
static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255
```

## 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 والبعيدون على حد سواء ببدء الاتصالات.

أكمل الخطوات التالية:

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



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

ملاحظة: عند إختيار خيار

الخطوة.

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. قطعة يطبق in order to أرسلت التشكيل إلى ال .ASA

#	Type	Original			Translated
		Source	Destination	Service	Interface
inside (1 Exempt rules, 1 Static rules, 1 Dynamic rules)					
1	Exempt	172.18.10.0	any		(outbound)
2	Static	172.16.11.5			outside
3	Dynamic	inside-network/24			outside

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 الإنجاه تم تغييره إلى  
الوارد.

#	Type	Original			Translated
		Source	Destination	Service	Interface
inside (1 Exempt rules, 1 Static rules, 1 Dynamic rules)					
1	Exempt	172.18.10.0	any		(inbound)
2	Static	172.16.11.5			outside
3	Dynamic	inside-network/24			outside

قطعة 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. دعوات 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
```

!  
!  
!

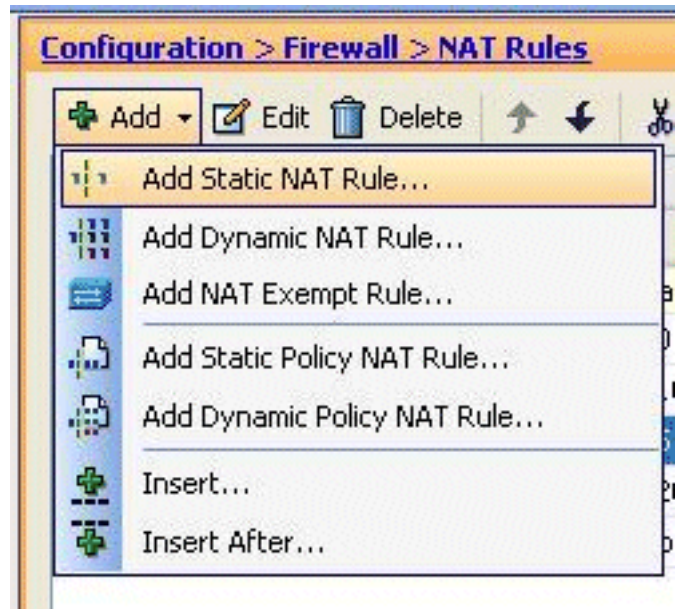
## إعادة توجيه المنفذ (إعادة توجيه) باستخدام الحالات

إعادة توجيه المنفذ أو إعادة توجيه المنفذ هي ميزة مفيدة حيث يحاول المستخدمون الخارجيون الوصول إلى خادم داخلي على منفذ معين. in order to تمت 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:

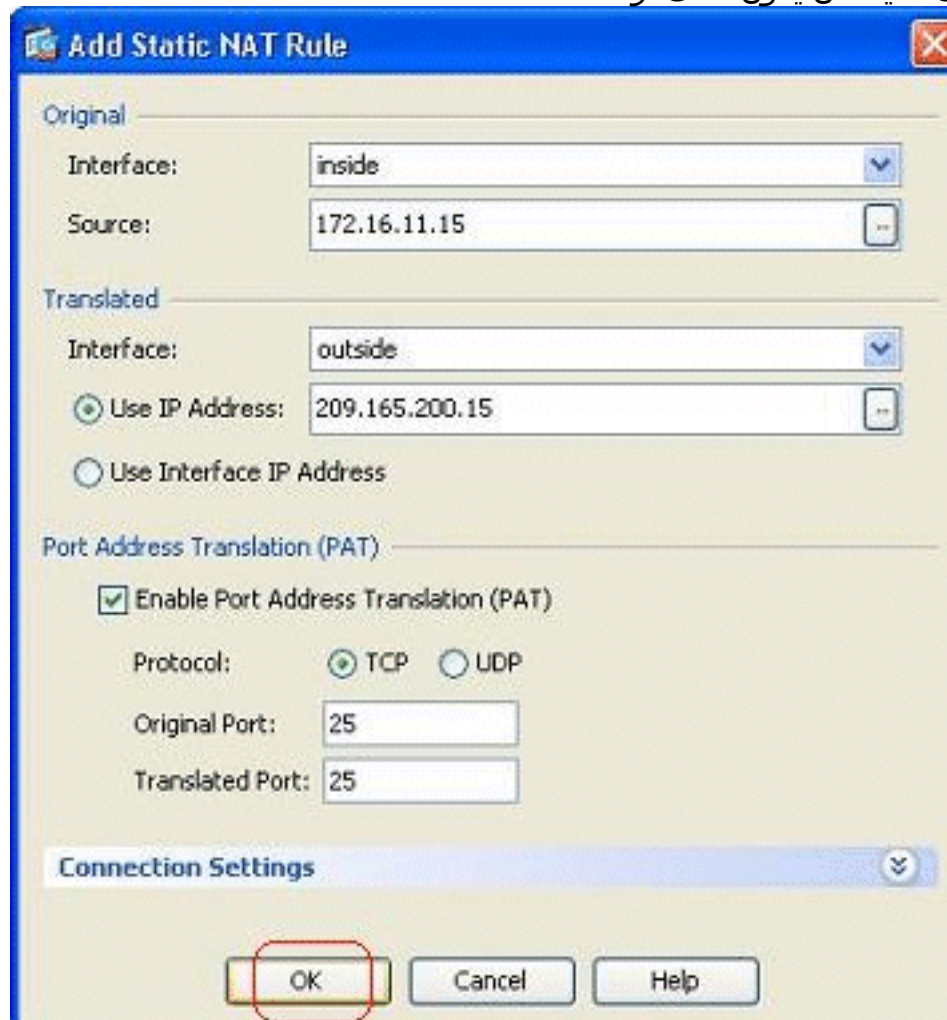
1. ترجمة خادم البريد الداخلي، 172.16.11.15 على المنفذ 25، إلى عنوان IP العام، 209.165.200.15 في المنفذ 25.
  2. السماح بالوصول إلى خادم البريد العام، 209.165.200.15 على المنفذ 25.
- عندما يحاول المستخدم الخارجي الوصول إلى الخادم، 209.165.200.15 في المنفذ 25، ستم إعادة توجيه حركة مرور البيانات هذه إلى خادم البريد الداخلي، 172.16.11.15 في المنفذ 25.

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



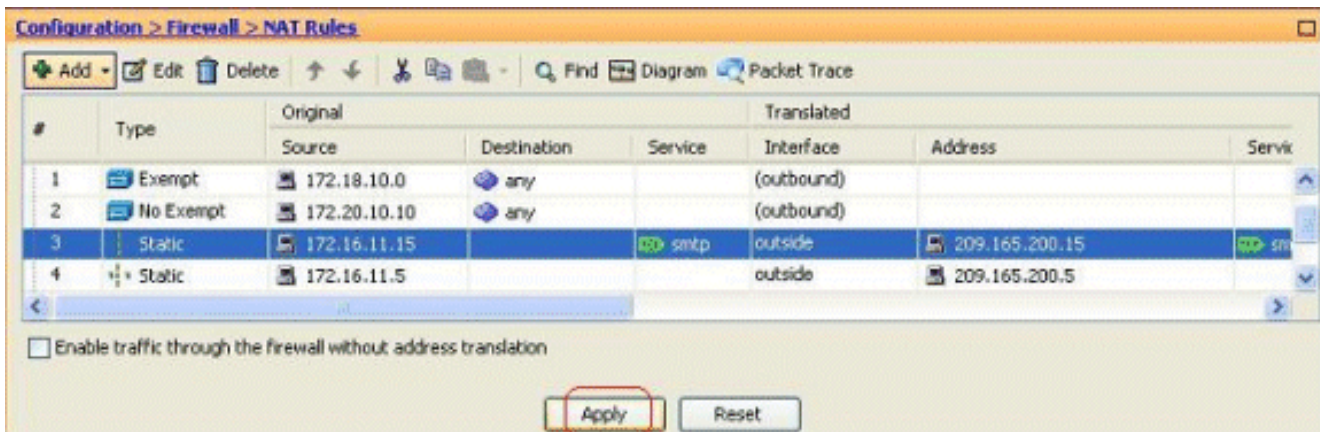
الثابتة.

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



.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

#	Type	Original Source	Original Destination	Original Service	Translated Interface	Translated Address	Translated Service	Action
1	any	any	Any less secure ne...	IP ip				Permit
2	any	any	any	IP ip				Deny
outside (3 incoming rules)								
1	✓	20.1.1.10	209.165.200.10	TCP RDP				Permit
2	✓	any	209.165.200.15	TCP smtp-access				Permit
3	any	any	any	IP ip				Deny

TCP Group: smtp-access  
TCP: smtp (25)

ملاحظة: تأكد من استخدام مضيفين محددین بدلاً من استخدام أي كلمة أساسية في مصدر قاعدة الوصول.

## الحد من جلسة TCP/UDP باستخدام ثابت

يمكنك تحديد الحد الأقصى لعدد اتصالات TCP/UDP باستخدام القاعدة الثابتة. يمكنك أيضاً تحديد الحد الأقصى لعدد الاتصالات الجينية. الاتصال الجيني 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

### Edit Static NAT Rule

**Original**

Interface: inside

Source: 172.16.11.15

**Translated**

Interface: outside

Use IP Address: 209.165.200.15

Use Interface IP Address

**Port Address Translation (PAT)**

Enable Port Address Translation (PAT)

Protocol:  TCP  UDP

Original Port: smtp

Translated Port: smtp

**Connection Settings**

Translate the DNS replies that match the translation rule

Randomize sequence number

Maximum TCP Connections: 100

Maximum UDP Connections: 0

Maximum Embryonic Connections: 50

OK Cancel Help

الثابتة.

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

Original			Translated		
Source	Destination	Service	Interface	Address	Service
Static rules, 1 Dynamic rules)					
172.18.10.0	any		(outbound)		
172.20.10.10	any		(outbound)		
172.16.11.15		smtp	outside	209.165.200.15	smtp

Options				
DNS Rewrite	Max TCP Connections	Embryonic Limit	Max UDP Connections	Randomize Sequer
<input type="checkbox"/>	100	50	Unlimited	<input checked="" type="checkbox"/>

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 استناداً 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 أيضاً 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

**Add Access Rule**

Interface:

Action:  Permit  Deny

Source:

Destination:

Service:

Description:

Enable Logging

Logging Level:

**More Options**

Enable Rule

Traffic Direction:  In  Out

Source Service:

Logging Interval:  seconds

Time Range:

OK Cancel Help

الزميني.

**Browse Time Range**

Add  Edit  Delete

Name	Start Time	End Time	Recurrir

2. انقر فوق إضافة لإنشاء نطاق زميني جديد.

3. قم بتحديد اسم النطاق الزمني، وحدد وقت البدء ووقت الانتهاء. وانقر فوق OK.

**Add Time Range**

Time Range Name:

Start Time

Start now

Start at

Month:  Day:  Year:

Hour:  Minute:

End Time

Never end

End at (inclusive)

Month:  Day:  Year:

Hour:  Minute:

Recurring Time Ranges

You can further constrain the active time of this range by specifying recurring ranges. The recurring time ranges will be active within the start and stop time specified.

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

**Browse Time Range**

Name	Start Time	End Time	Recurring Entries
Res...	14:00 05 Fe...	16:30 06 F...	

الوصول".

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

هذه. وفقاً لتكوين قاعدة الوصول هذه، تم منع المستخدم في 172.16.10.50 من استخدام 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.



**Edit Time Range**

Time Range Name: Restrict-Usage

**Start Time**

Start now

Start at

Month: February Day: 05 Year: 2011

Hour: 00 Minute: 00

**End Time**

Never end

End at (Inclusive)

Month: March Day: 06 Year: 2011

Hour: 00 Minute: 30

**Recurring Time Ranges**

You can further constrain the active time of this range by specifying recurring ranges. The recurring time ranges will be active within the start and stop time specified.

7. حدد الإعدادات بناء على متطلباتك، وانقر موافق

**Add Recurring Time Range**

Specify days of the week and times on which this recurring range will be active

For example, use this option when you want the time range to be active every Monday through Thursday, from 8:00 through 16:59, only.

**Days of the Week**

Every day

Weekdays

Weekends

On these days of the week:

Mon  Tue  Wed  Thu  Fri  Sat  Sun

**Daily Start Time**

Hour: 15 Minute: 00

**Daily End Time (Inclusive)**

Hour: 21 Minute: 00

Specify a weekly interval when this recurring range will be active

For example, use this option when you want the time range to be active continuously from Monday at 8:00 through Friday at 16:59.

**Weekly Interval**

From: Monday Hour: 00 Minute: 00

From: Friday Hour: 23 Minute: 59

للاكمال.

8. اضغط ok في order رجعت إلى المدى الزمني نافذة.

**Edit Time Range**

Time Range Name: Restrict-Usage

Start Time

Start now

Start at

Month: February Day: 05 Year: 2011

Hour: 00 Minute: 00

End Time

Never end

End at (inclusive)

Month: March Day: 06 Year: 2011

Hour: 00 Minute: 30

Recurring Time Ranges

You can further constrain the active time of this range by specifying recurring ranges. The recurring time ranges will be active within the start and stop time specified.

weekdays 15:00 through 20:00

Buttons: Add, Edit, Delete, OK, Cancel, Help

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](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل