ASA 7.x/PIX 6.x أو على: فتح/حظر مثال تكوين المنافذ

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين كيفية فتح المنافذ أو حظرها للنوع المتعدد من حركة المرور، مثل http أو ftp، في جهاز الأمان.

ملاحظة ان مصطلحي "فتح الميناء" و"السماح بالمنفذ" يلقيان نفس المعنى. وبالمثل، فإن "إغلاق الميناء" و"تقييد الميناء" هما أيضا لهما نفس المعنى.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أنه قد تم تكوين PIX/ASA وأنه يعمل بشكل صحيح.

المكونات المستخدمة

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

- جهاز الأمان القابل للتكيف (ASA) من Cisco 5500 Series الذي يشغل الإصدار 8.2(1)
- Cisco Adaptive Security Device Manager (ASDM)، الإصدار 6.3(5)

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

المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز جدار حماية Cisco 500 Series PIX باستخدام إصدار البرنامج x.6 والإصدارات الأحدث.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

التكوين

يجب أن يكون لكل واجهة مستوى أمان من 0 (الأقل) إلى 100 (الأعلى). على سبيل المثال، يجب عليك تعيين الشبكة الأكثر أمانا، مثل شبكة المضيف الداخلية، للمستوى 100. بينما يمكن أن تكون الشبكة الخارجية المتصلة بالإنترنت من المستوى 0، يمكن وضع الشبكات الأخرى، مثل DMZ، في الوسط. يمكنك تخصيص واجهات متعددة لنفس مستوى الأمان.

بشكل افتراضي، يتم حظر جميع المنافذ على الواجهة الخارجية (مستوى الأمان 0)، وتكون جميع المنافذ مفتوحة على الواجهة الداخلية (مستوى الأمان 100) من جهاز الأمان. بهذه الطريقة، يمكن أن تمر جميع حركة المرور الصادرة عبر جهاز الأمان دون أي تكوين، ولكن يمكن السماح بحركة المرور الواردة بواسطة تكوين قائمة الوصول والأوامر الثابتة في جهاز الأمان.

ملاحظة: بوجه عام، يتم حظر جميع المنافذ من منطقة الأمان الأدنى إلى منطقة الأمان الأعلى، وتكون جميع المنافذ مفتوحة من منطقة الأمان الأعلى إلى منطقة الأمان الأدنى شريطة تمكين الفحص الذي يحدد الحالة لحركة المرور الواردة والصادرة على حد سواء.

يتكون هذا القسم من الأقسام الفرعية كما هو موضح:

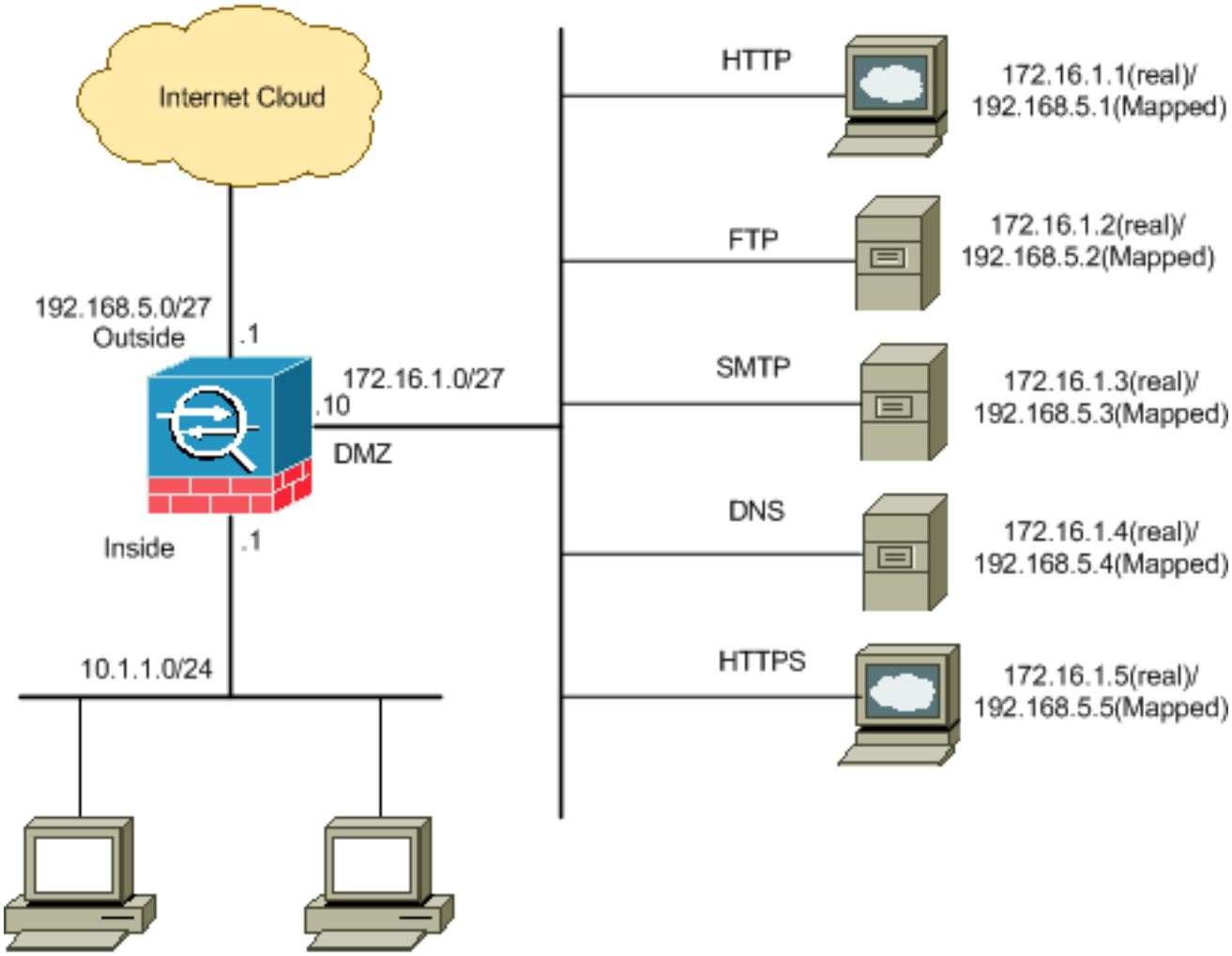
- الرسم التخطيطي للشبكة
- حظر تكوين المنافذ
- فتح تكوين المنافذ

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



حظر تكوين المنافذ

يسمح جهاز الأمان بأية حركة مرور صادرة ما لم يتم منعها بشكل صريح بواسطة قائمة الوصول الموسعة.

تتكون قائمة الوصول من إدخال أو أكثر من إدخالات التحكم في الوصول. بناء على نوع قائمة الوصول، يمكنك تحديد عناوين المصدر والوجهة، أو البروتوكول، أو المنافذ (ل TCP أو UDP)، أو نوع ICMP (ل ICMP)، أو EtherType.

ملاحظة: بالنسبة للبروتوكولات غير المتصلة، مثل ICMP، يقوم جهاز الأمان بإنشاء جلسات عمل أحادية الإتجاه، لذلك تحتاج إما إلى قوائم الوصول للسماح ICMP في كلا الاتجاهين (من خلال تطبيق قوائم الوصول إلى واجهات المصدر والوجهة)، أو تحتاج إلى تمكين محرك فحص ICMP. يعامل محرك فحص ICMP جلسات ICMP على أنها إتصالات ثنائية الإتجاه.

أتمت هذا steps in order to منعت الميناء، أي عادة يطبق إلى حركة مرور أن ينشأ من الداخل (منطقة أمن أعلى) إلى DMZ (منطقة أمن أدنى) أو DMZ إلى الخارج.

1. قم بإنشاء قائمة التحكم في الوصول بطريقة يمكنك من خلالها حظر حركة مرور المنفذ المحددة.

```
access-list
```

2. ثم قم بربط قائمة الوصول باستخدام الأمر **access-group** لكي تكون نشطة.

الأمثلة:

1. **حظر حركة مرور منفذ HTTP:** لحظر الشبكة الداخلية 10.1.1.0 من الوصول إلى HTTP (خادم الويب) باستخدام IP 172.16.1.1 الموضوع في شبكة DMZ، قم بإنشاء قائمة تحكم في الوصول (ACL) كما هو موضح:

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
                                        host 172.16.1.1  eq 80
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

ملاحظة: أستخدم أوامر no المتبوعة بقائمة الوصول لإزالة حظر المنفذ.

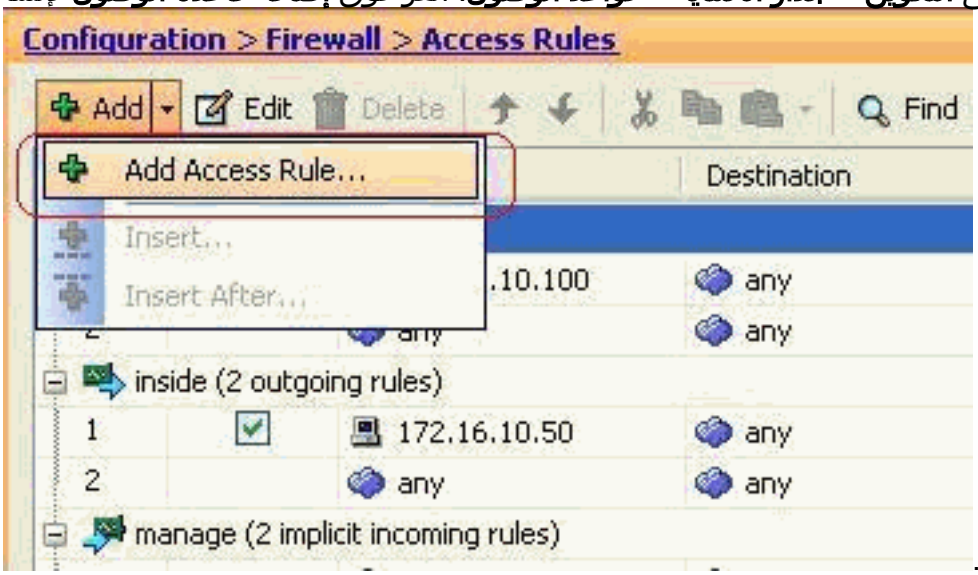
2. **حظر حركة مرور منفذ FTP:** لحظر الشبكة الداخلية 10.1.1.0 من الوصول إلى FTP (خادم الملفات) مع وضع IP 172.16.1.2 في الشبكة DMZ، قم بإنشاء قائمة تحكم في الوصول (ACL) كما هو موضح:

```
ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0
                                        host 172.16.1.2  eq 21
ciscoasa(config)#access-list 100 extended permit ip any any
ciscoasa(config)#access-group 100 in interface inside
```

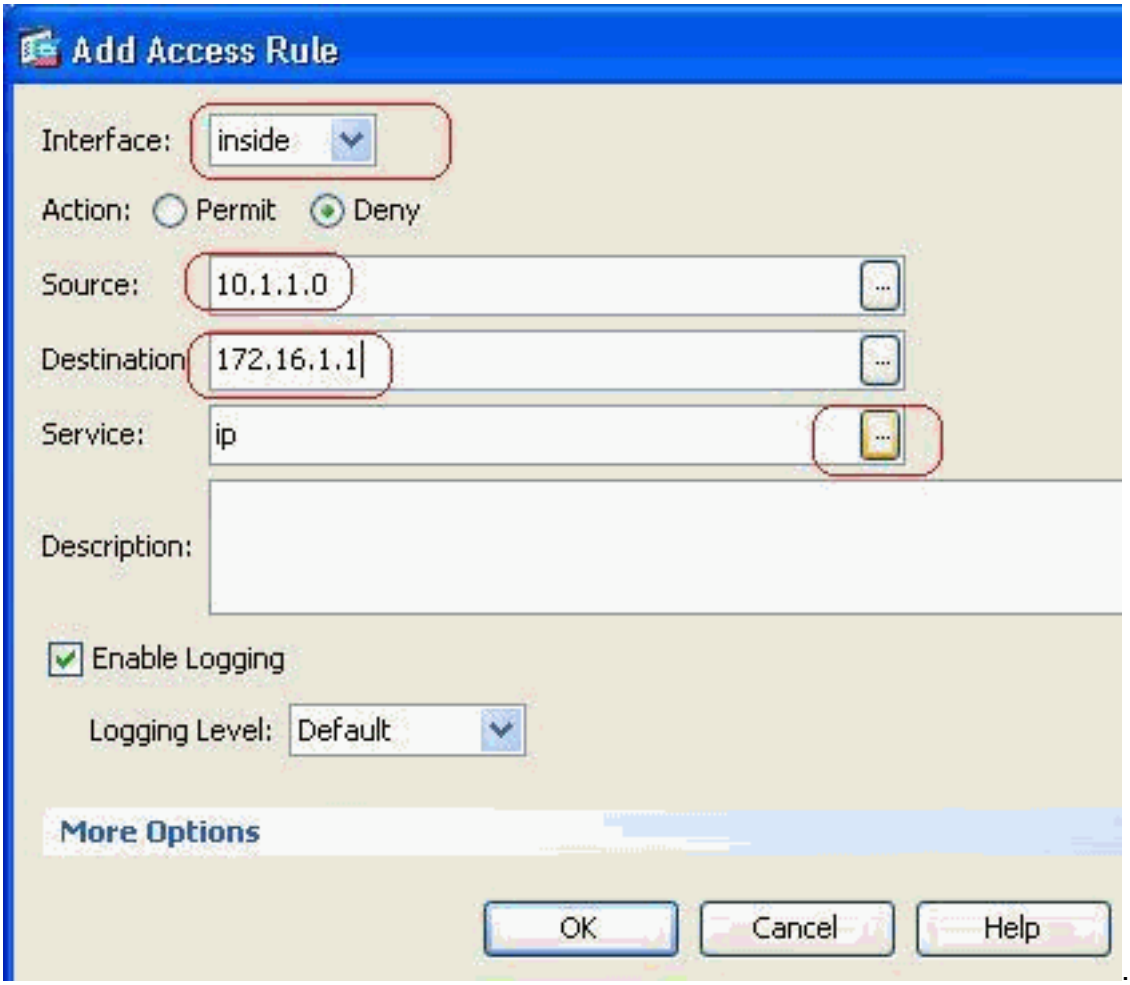
ملاحظة: ارجع إلى منافذ ANA لمعرفة المزيد من المعلومات حول تعيينات المنافذ.

يتم عرض التكوين خطوة بخطوة لتنفيذ هذا الإجراء من خلال ASDM في هذا القسم.

1. انتقل إلى **التكوين > جدار الحماية > قواعد الوصول**. انقر فوق **إضافة قاعدة الوصول** لإنشاء قائمة الوصول.

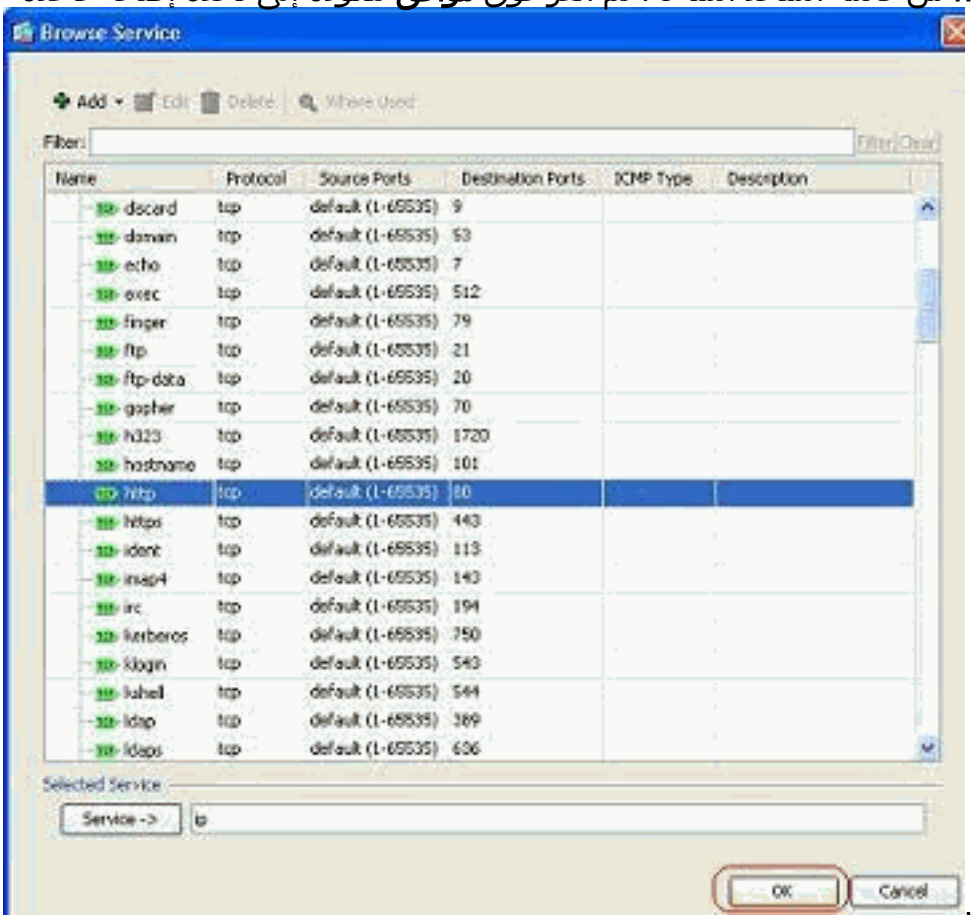


2. حدد المصدر والوجهة والإجراء الخاص بقاعدة الوصول مع الواجهة التي سيتم إقران قاعدة الوصول هذه بها. حدد التفاصيل لاختيار المنفذ المحدد الذي تريد



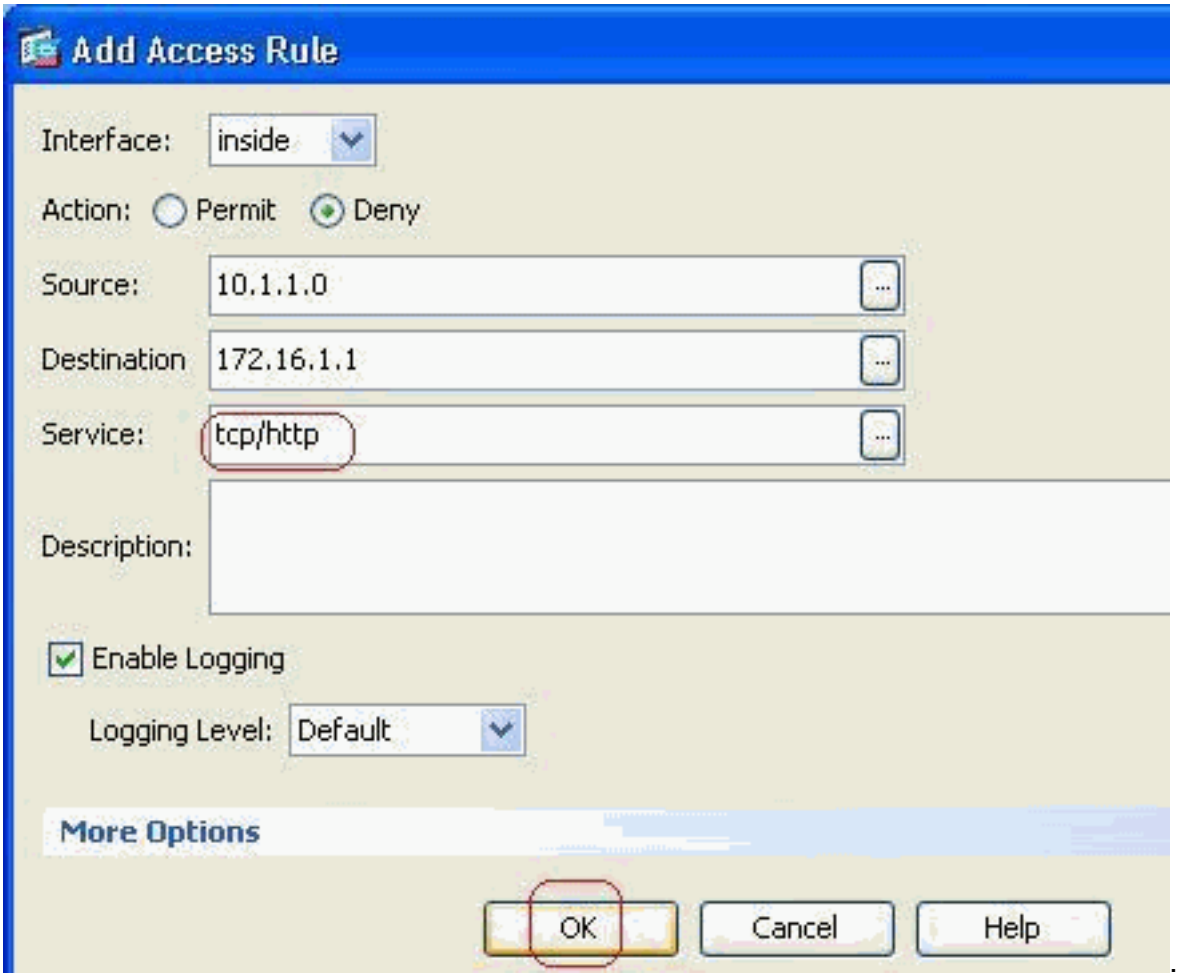
حظره.

3. أختر **http** من قائمة المنافذ المتاحة، ثم انقر فوق **موافق** للعودة إلى نافذة إضافة قاعدة



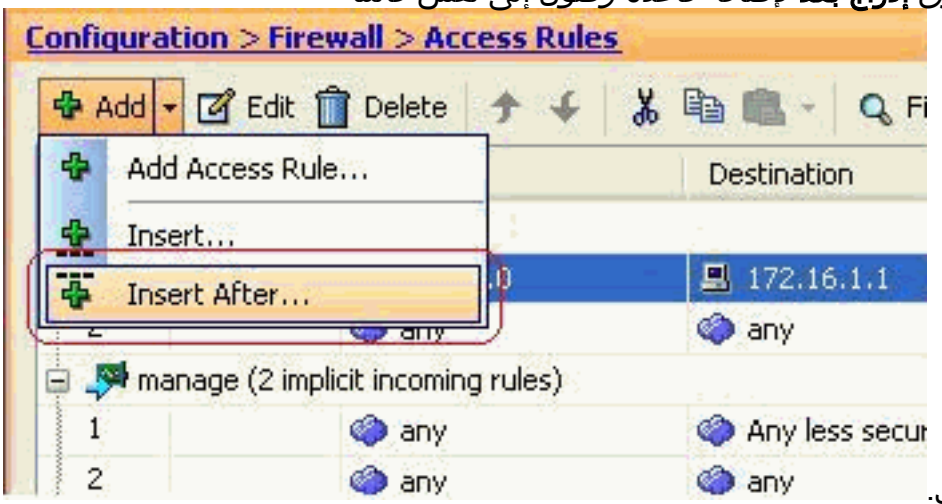
الوصول.

4. انقر فوق **موافق** لإكمال تكوين قاعدة



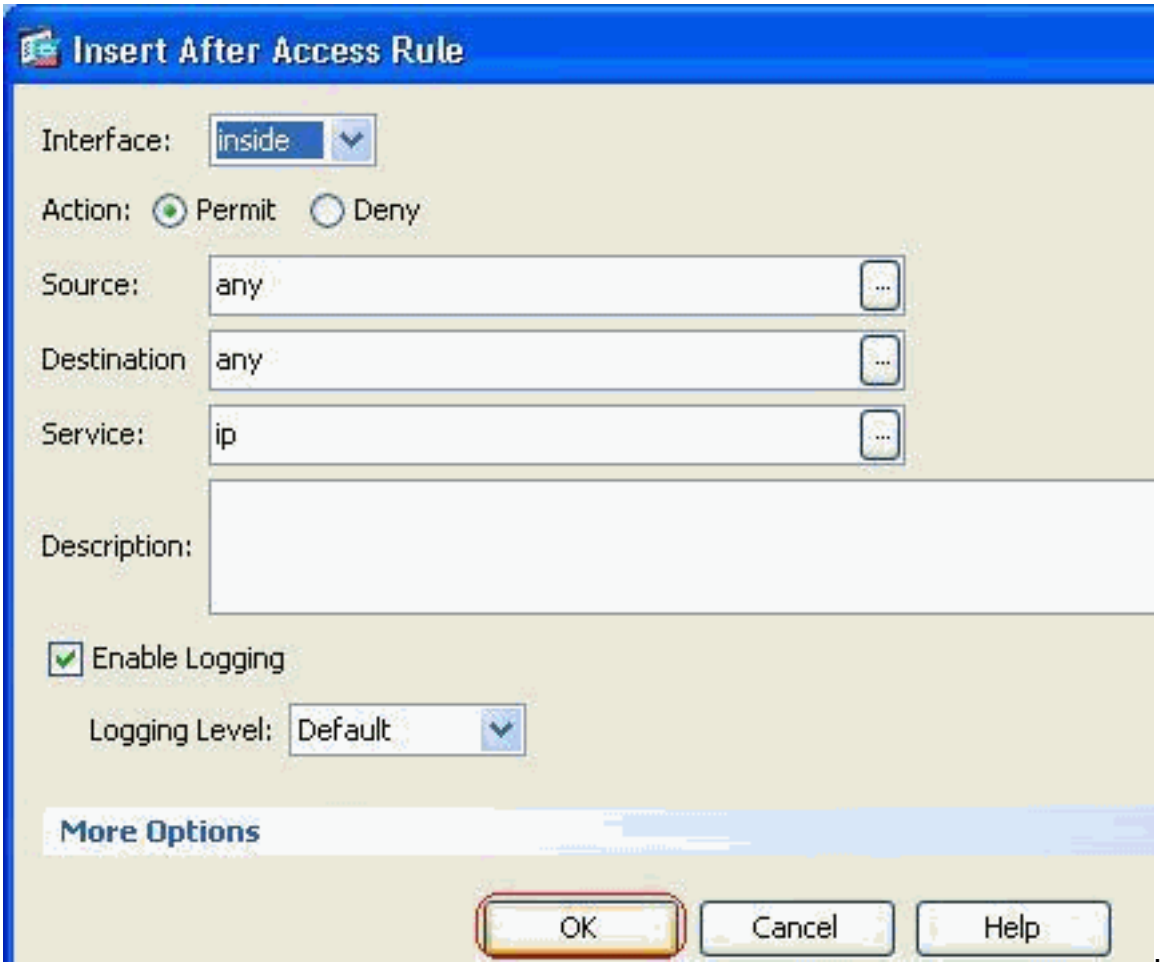
الوصول.

5. انقر فوق **إدراج بعد** لإضافة قاعدة وصول إلى نفس قائمة



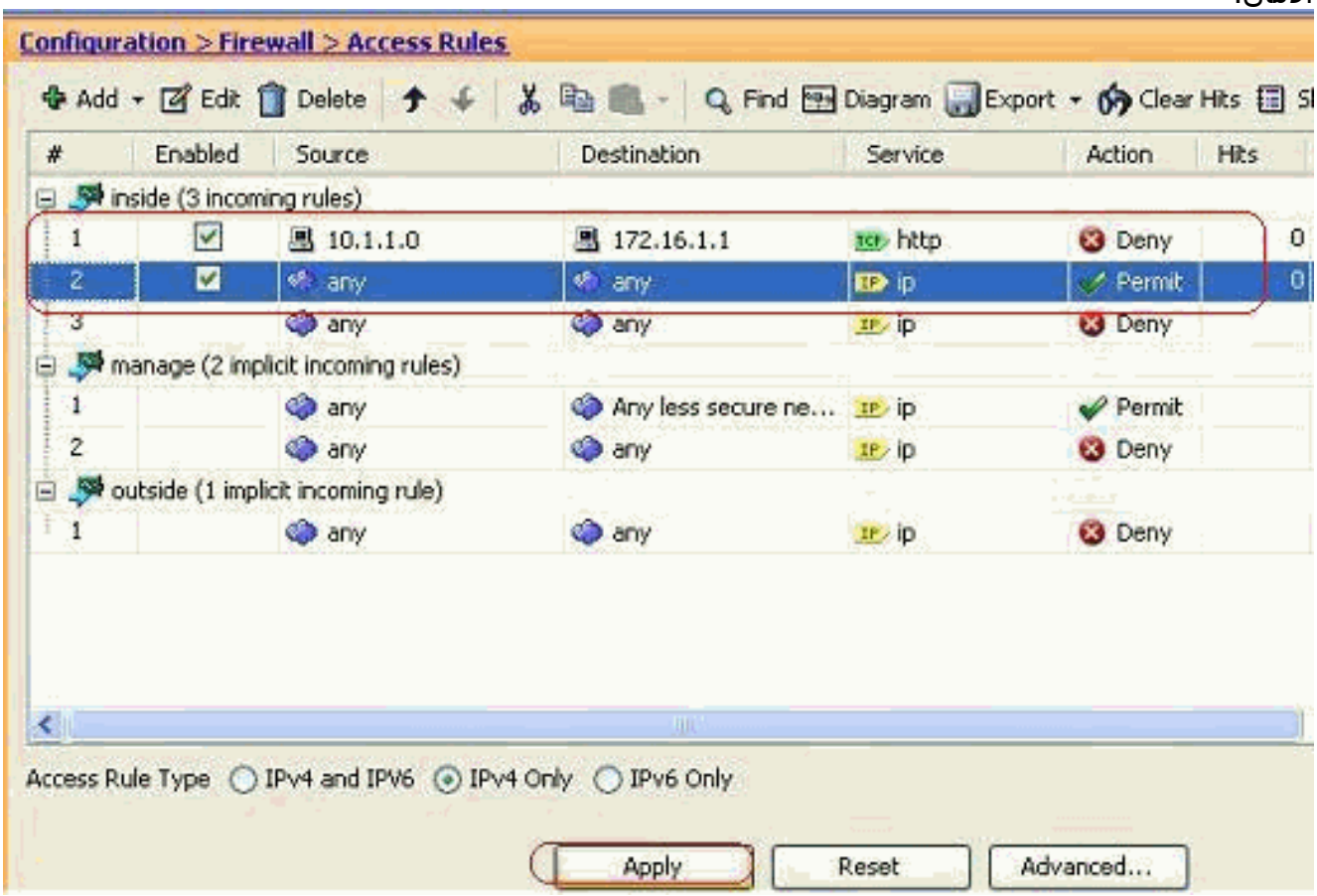
الوصول.

6. السماح بحركة المرور من "أي" إلى "أي" لمنع "الرفض الضمني". ثم انقر فوق **موافق** لإكمال إضافة قاعدة



الوصول هذه.

7. يمكن الاطلاع على قائمة الوصول التي تم تكوينها في علامة التبويب قواعد الوصول. انقر فوق **تطبيق** لإرسال هذا التكوين إلى جهاز الأمان.

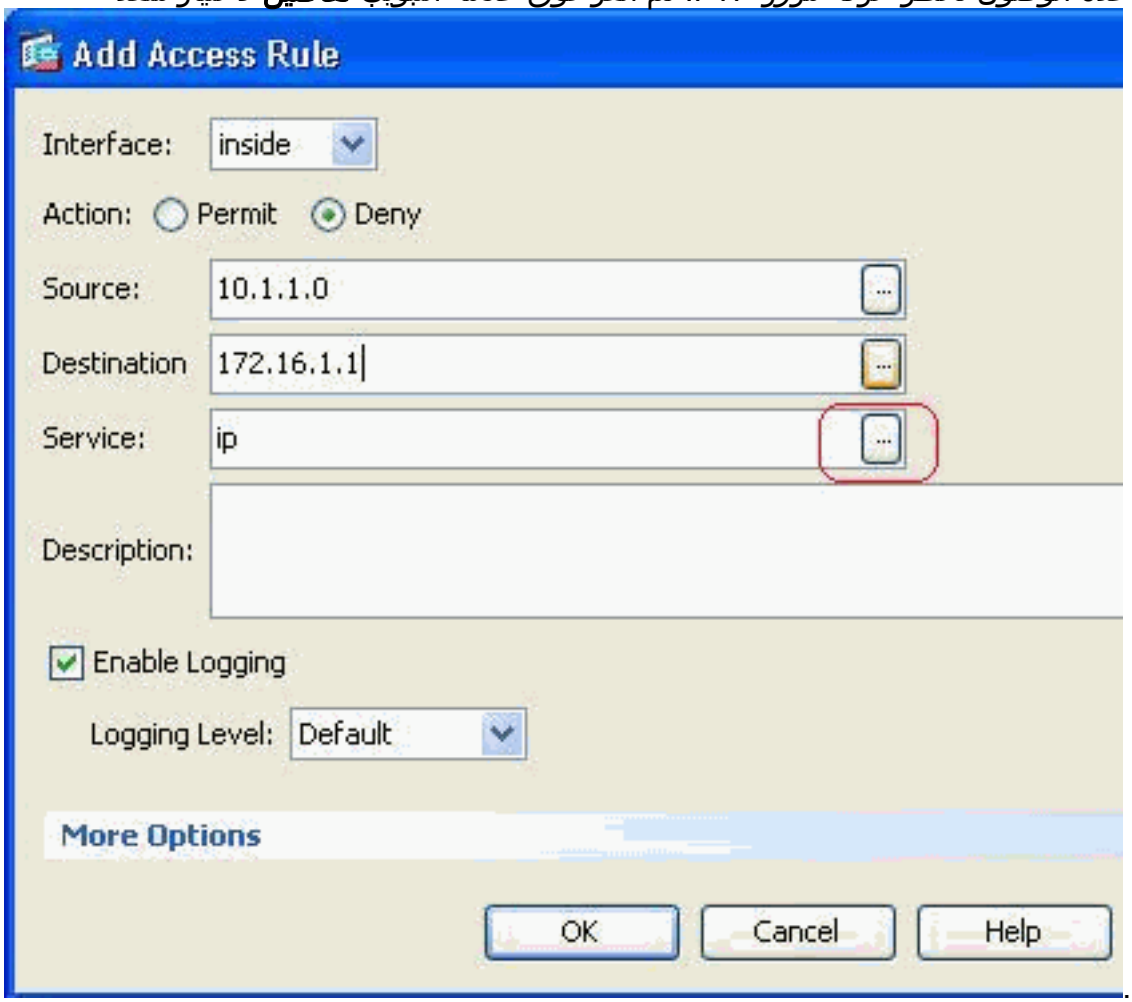


التشكيل يرسل من ال ASDM ينتج في هذا مجموعة الأمر على الأمر خط قارن (CLI) من ال ASA.

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

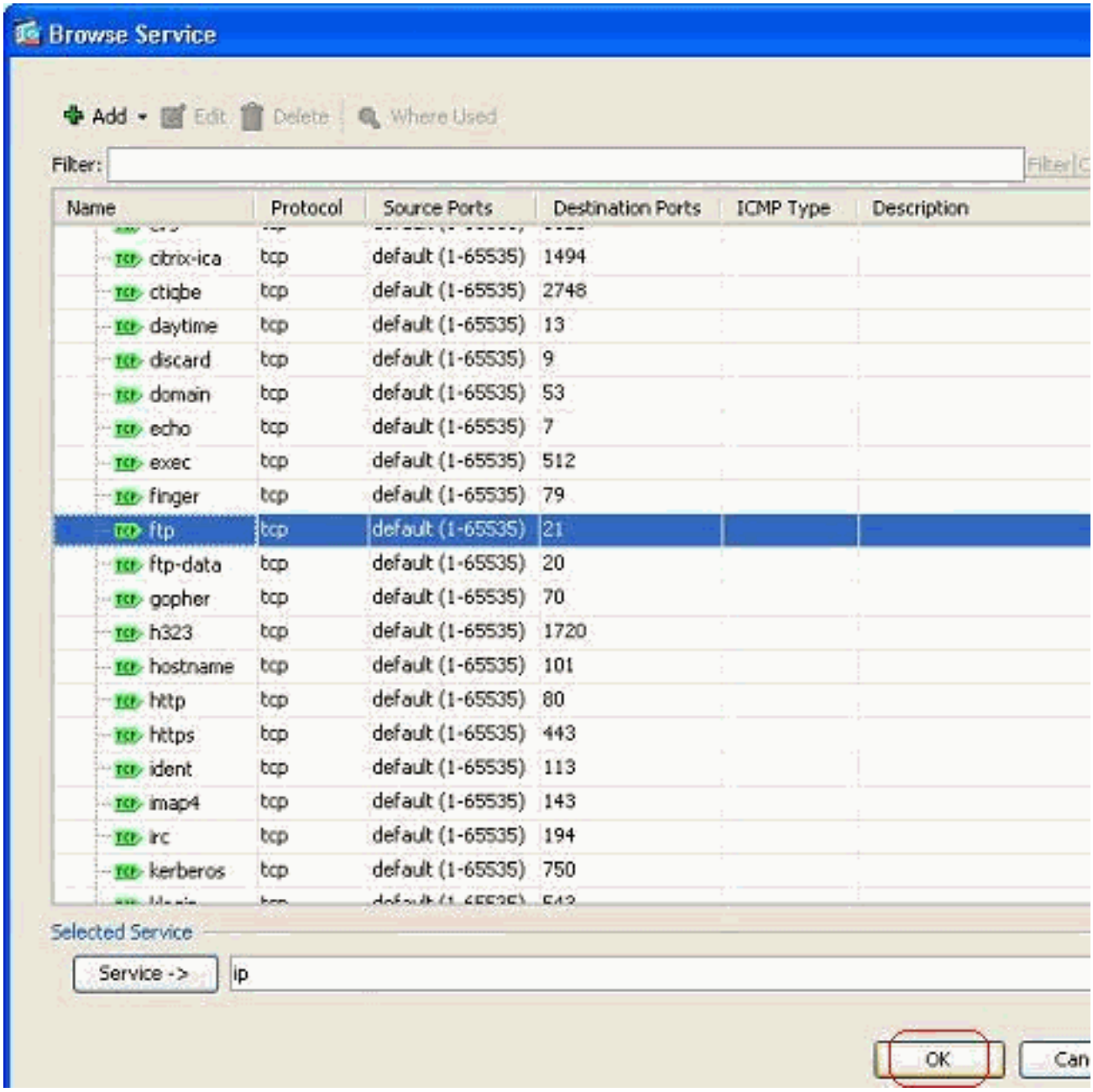
من خلال هذه الخطوات، تم تنفيذ المثال 1 من خلال ASDM لمنع شبكة 10.1.1.0 من الوصول إلى خادم الويب، الإصدار 172.16.1.1. كما يمكن تحقيق المثال 2 بنفس الطريقة لمنع شبكة 10.1.1.0 بالكامل من الوصول إلى خادم FTP، الإصدار 172.16.1.2. سيكون الاختلاف الوحيد في نقطة إختيار المنفذ.**ملاحظة:** يفترض أن يكون تكوين قاعدة الوصول هذه، على سبيل المثال 2، تكوينا جديدا.

8. حدد قاعدة الوصول لحظر حركة مرور FTP، ثم انقر فوق علامة التبويب **تفاصيل** لاختيار منفذ

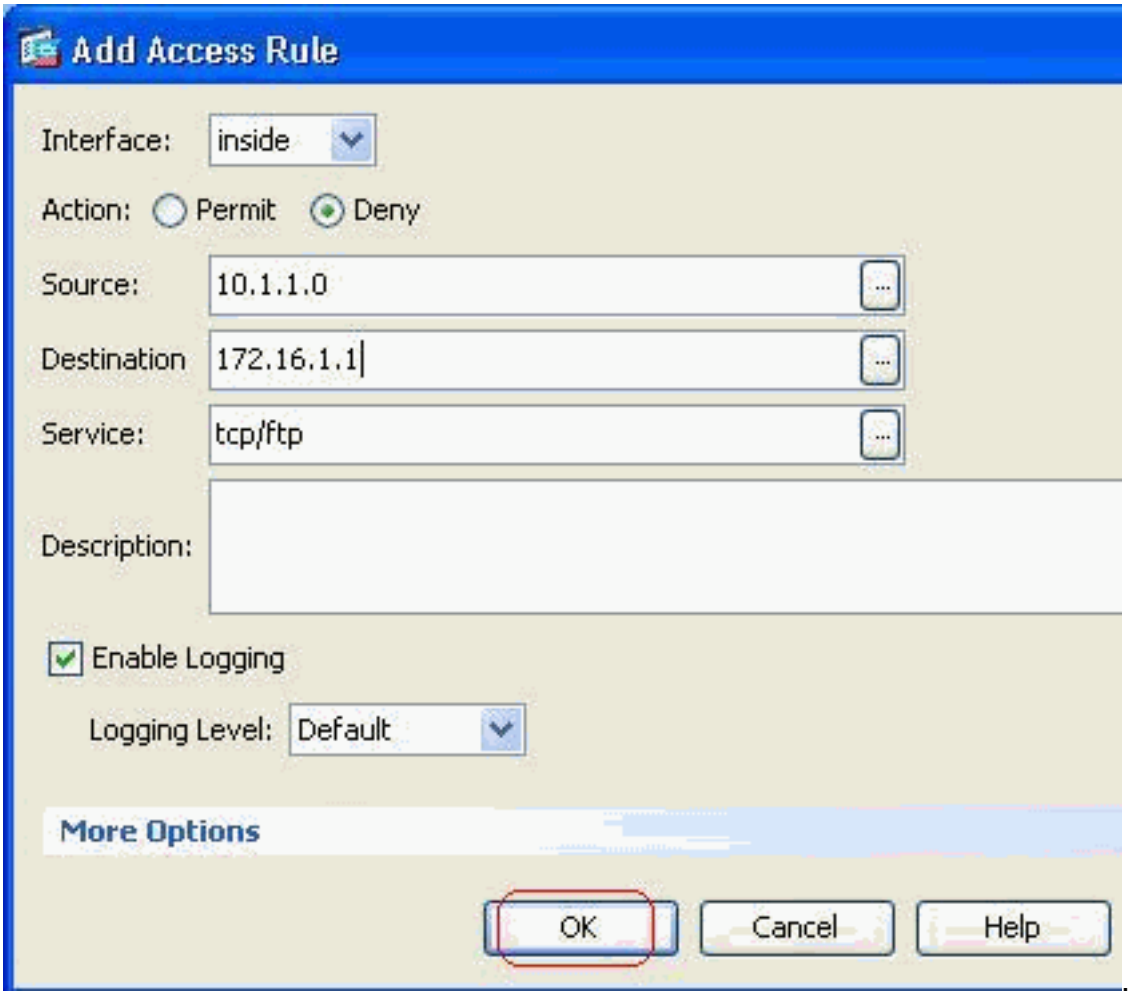


الوجهة.

9. أختر منفذ **FTP** وانقر فوق **موافق** للعودة إلى نافذة إضافة قاعدة الوصول.

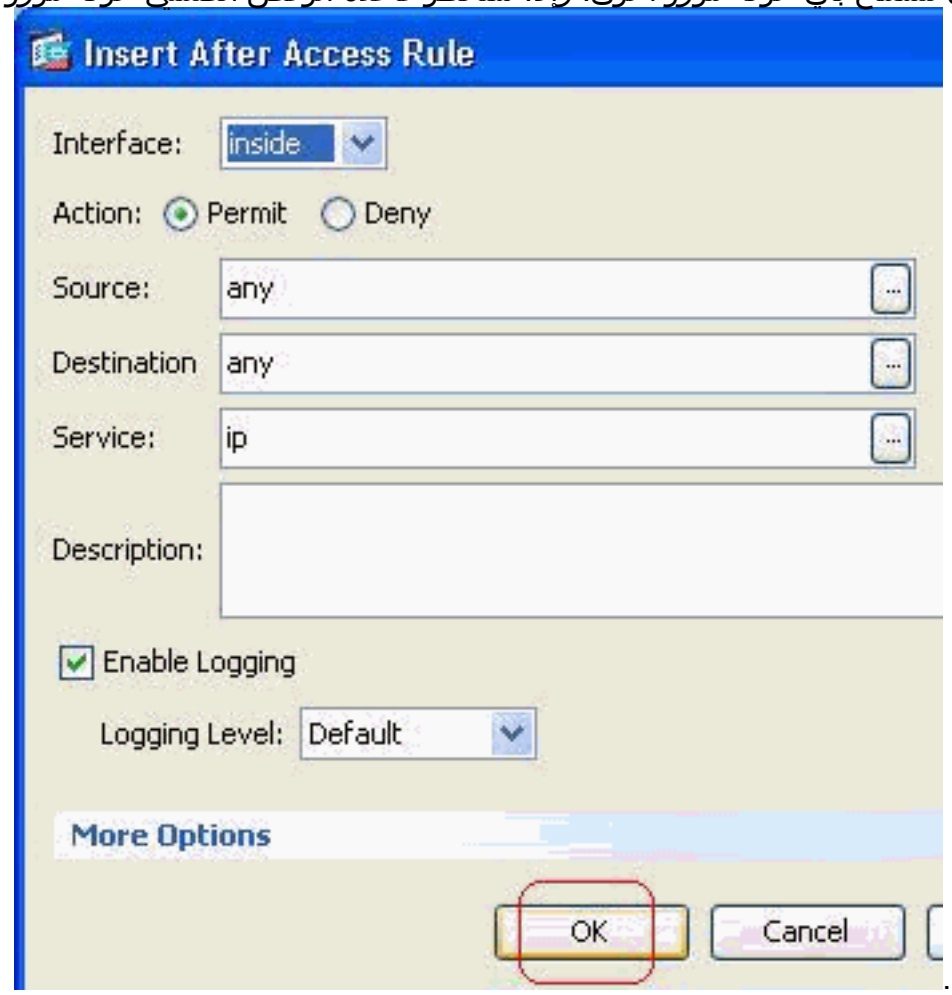


10. انقر فوق **موافق** لإكمال تكوين قاعدة



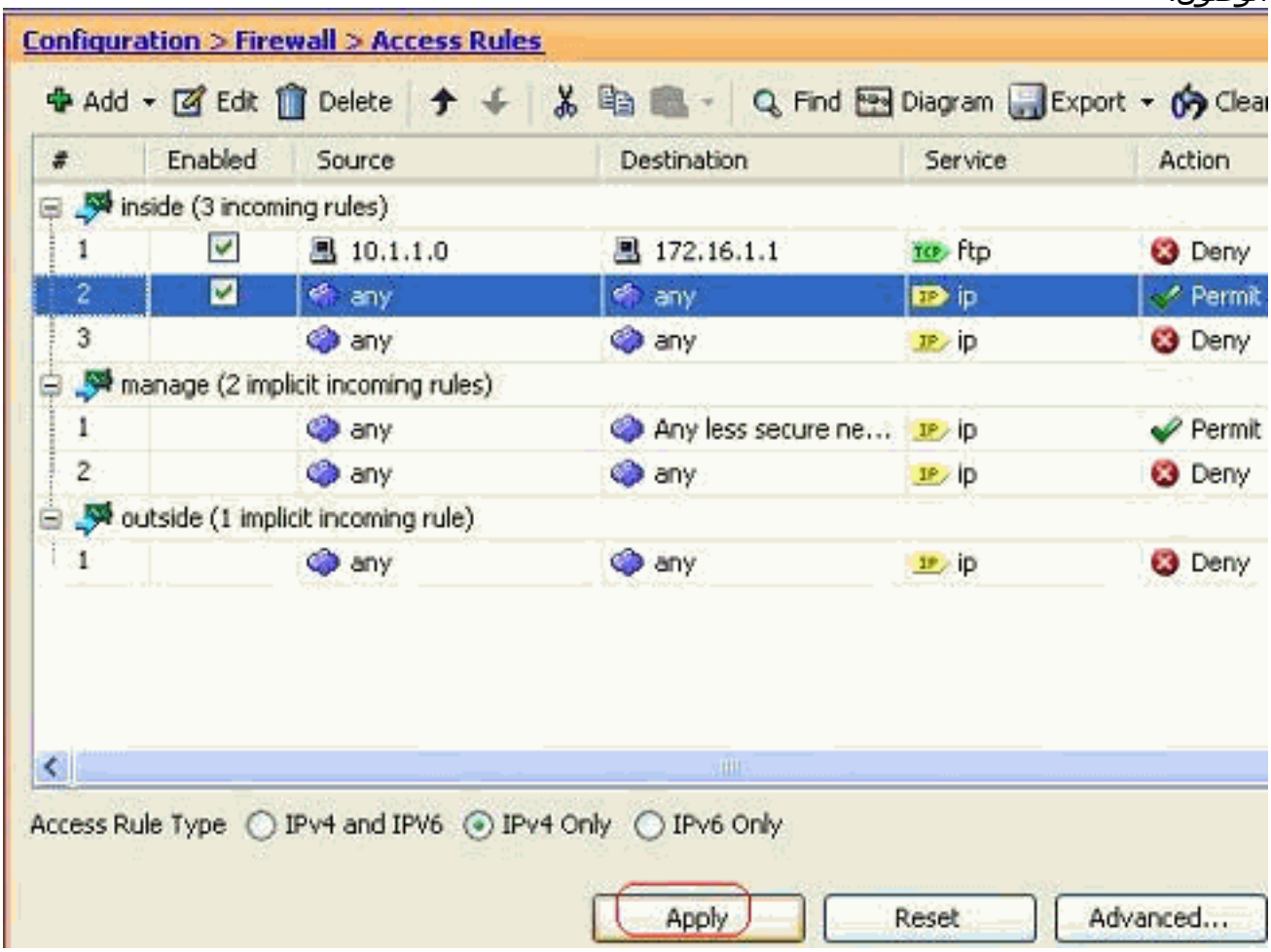
الوصول.

11. أضف قاعدة وصول أخرى للسماح بأي حركة مرور أخرى. وإلا، ستحظر قاعدة الرفض الضمني حركة مرور



البيانات على هذه الواجهة.

12. يبدو تكوين قائمة الوصول الكاملة بهذا الشكل تحت علامة التبويب قواعد الوصول.



13. طقطقة **يطبق** أن يرسل التشكيل إلى ال ASA. يبدو تكوين CLI المكافئ كما يلي:

```
access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp
access-list inside_access_in extended permit ip any any
access-group inside_access_in in interface inside
```

فتح تكوين المنافذ

لا يسمح جهاز الأمان بأي حركة مرور واردة ما لم تكن مسموح بها بشكل صريح من قبل قائمة الوصول الموسعة.

إذا كنت ترغب في السماح لمضيف خارجي بالوصول إلى مضيف داخلي، فيمكنك تطبيق قائمة وصول واردة على الواجهة الخارجية. أنت تحتاج أن يعين العنوان يترجم من المضيف داخلي في قائمة الوصول لأن العنوان يترجم العنوان أن يستطيع كنت استعملت على الشبكة الخارجية. أكمل هذه الخطوات لفتح المنافذ من منطقة الأمان الأدنى إلى منطقة الأمان الأعلى. على سبيل المثال، السماح بحركة المرور من الخارج (منطقة الأمان الأقل) إلى الواجهة الداخلية (منطقة الأمان الأعلى) أو DMZ إلى الواجهة الداخلية.

1. nat ساكن إستاتيكي يخلق ترجمة ثابتة من عنوان حقيقي إلى عنوان يخطط. هذا العنوان المعين هو عنوان يستضيف على الإنترنت ويمكن إستخدامه للوصول إلى خادم التطبيق على DMZ بدون الحاجة إلى معرفة العنوان الحقيقي للخادم.

```
| [static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask
                {access-list access_list_name | interface
```

أحلت الساكن إستاتيكي nat قسم من الأمر مرجع ل PIX/ASA in order to علمت كثير معلومة.

2. قم بإنشاء قائمة تحكم في الوصول (ACL) للسماح بحركة مرور المنفذ المحددة.

```
access-list
```

3. قم بربط قائمة الوصول باستخدام الأمر **access-group** لكي تكون نشطة.

access-group

الأمثلة:

افتح حركة مرور منفذ SMTP: افتح المنفذ **TCP 25** للسماح للمضيفين من الخارج (الإنترنت) بالوصول إلى خادم البريد الموجود في شبكة DMZ.يقوم الأمر **الثابت** بتعيين العنوان الخارجي 192.168.5.3 إلى عنوان DMZ الحقيقي 172.16.1.3.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3
                                        netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
                                      any host 192.168.5.3 eq 25
ciscoasa(config)#access-group 100 in interface outside
```

2. **افتح حركة مرور منفذ HTTPS:** افتح المنفذ **tcp 443** للسماح للمضيفين من الخارج (الإنترنت) بالوصول إلى خادم الويب (الآمن) الموضوع في شبكة DMZ.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
                                        netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
                                    any host 192.168.5.5  eq 443
ciscoasa(config)#access-group 100 in interface outside
```

3. **السماح بحركة مرور DNS:** افتح المنفذ **UDP 53** للسماح للمضيفين من الخارج (الإنترنت) بالوصول إلى خادم DNS (آمن) الموضوع في شبكة DMZ.

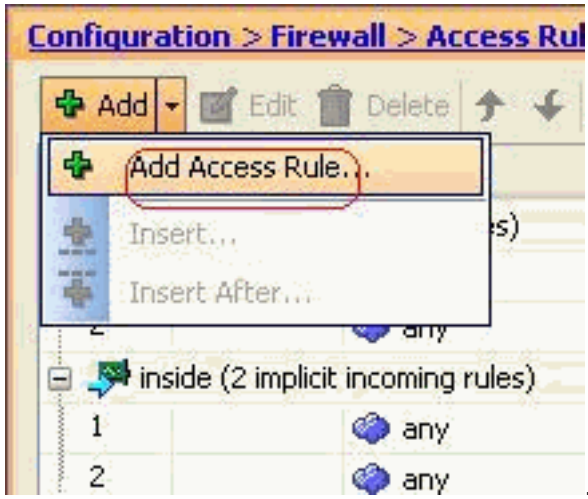
```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4
                                        netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit udp
                                      any host 192.168.5.4  eq 53
ciscoasa(config)#access-group 100 in interface outside
```

ملاحظة: ارجع إلى منافذ ANA لمعرفة المزيد من المعلومات حول تعيينات المنافذ.

التكوين من خلال ASDM

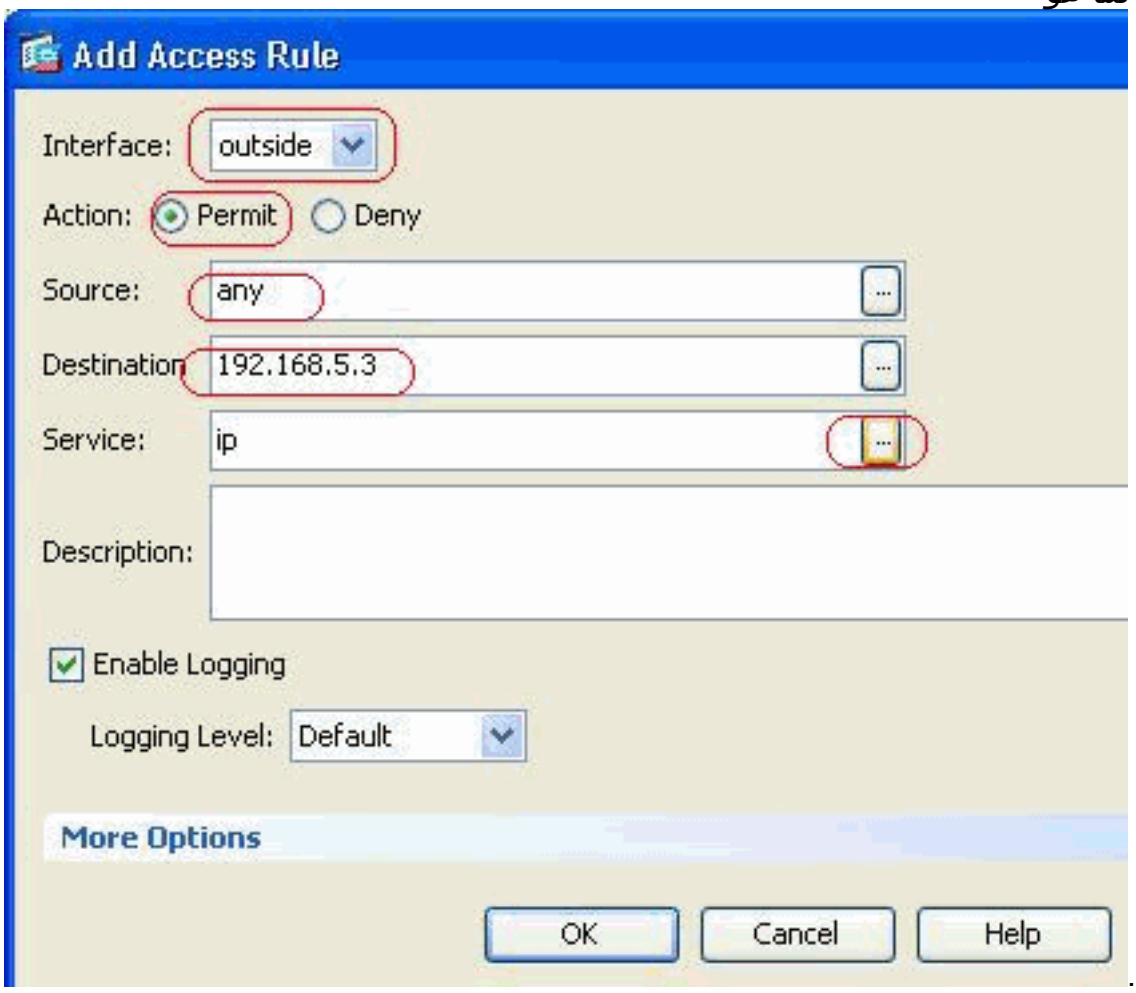
ويرد في هذا القسم نهج مفصل خطوة بخطوة لأداء المهام المذكورة أعلاه من خلال إدارة قاعدة بيانات الإدارة.

1. قم بإنشاء قاعدة الوصول للسماح بحركة مرور SMTP إلى الخادم



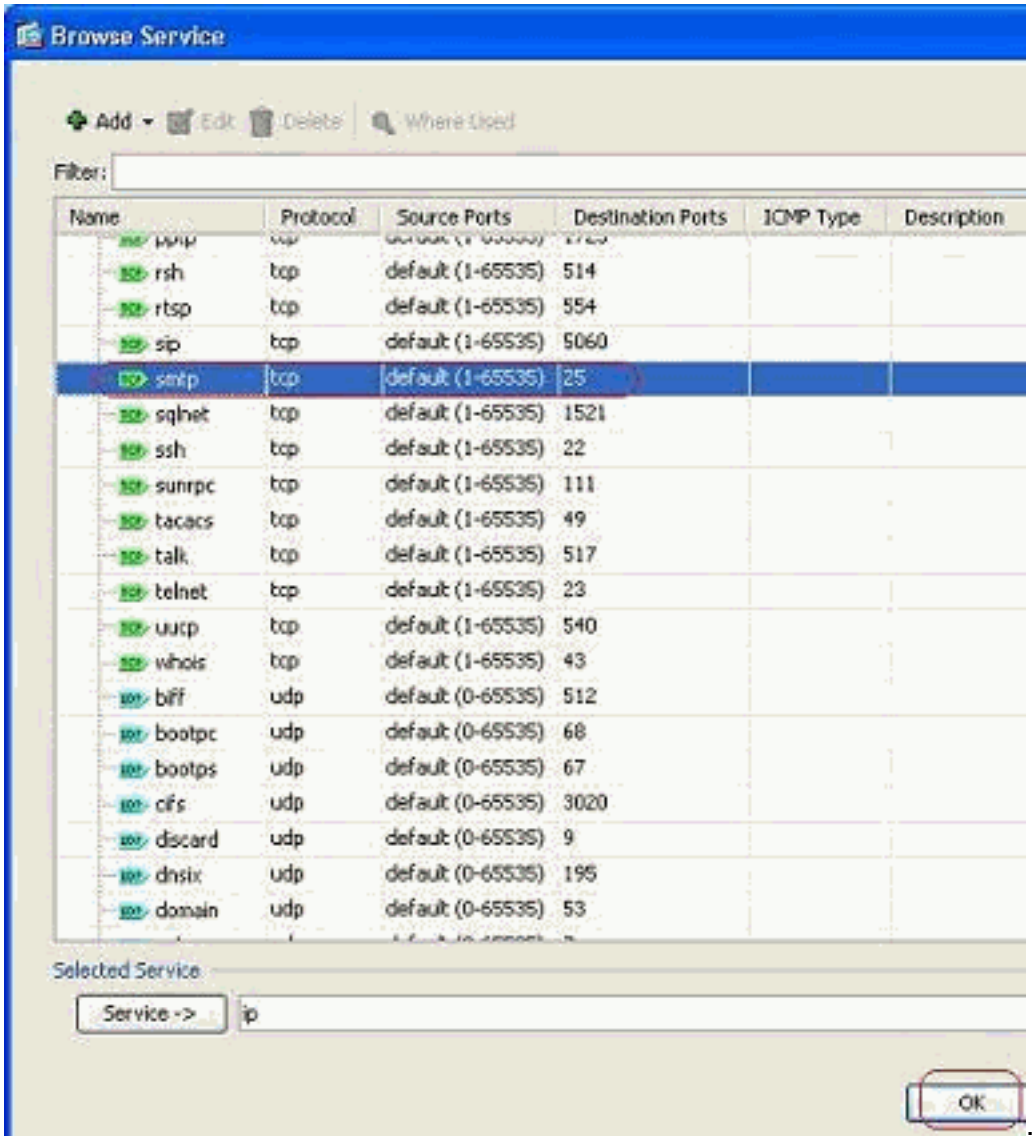
192.168.5.3.

2. قم بتحديد مصدر قاعدة الوصول والوجهة الخاصة بها، والواجهة التي ترتبط بها هذه القاعدة. قم أيضا بتعريف الإجراء كما هو



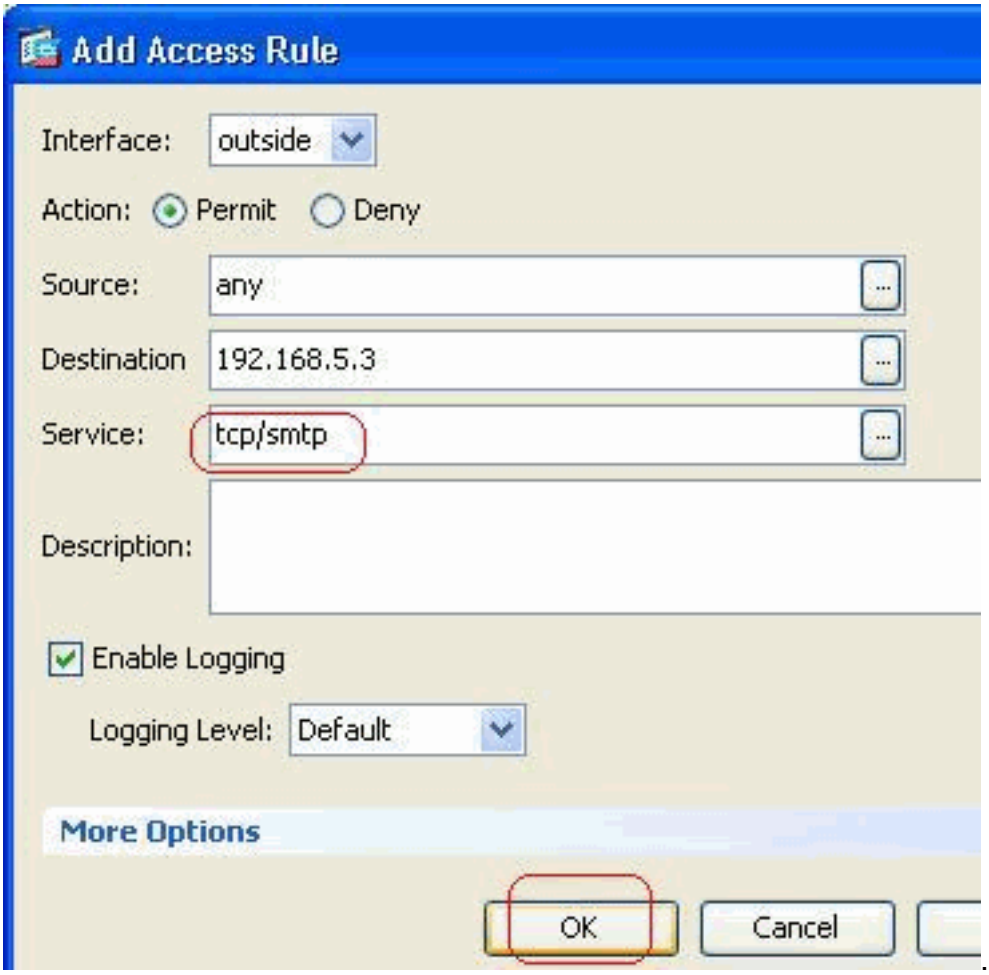
مسموح.

3. أخترت **SMTP** كالميناء، بعد ذلك طقطقت



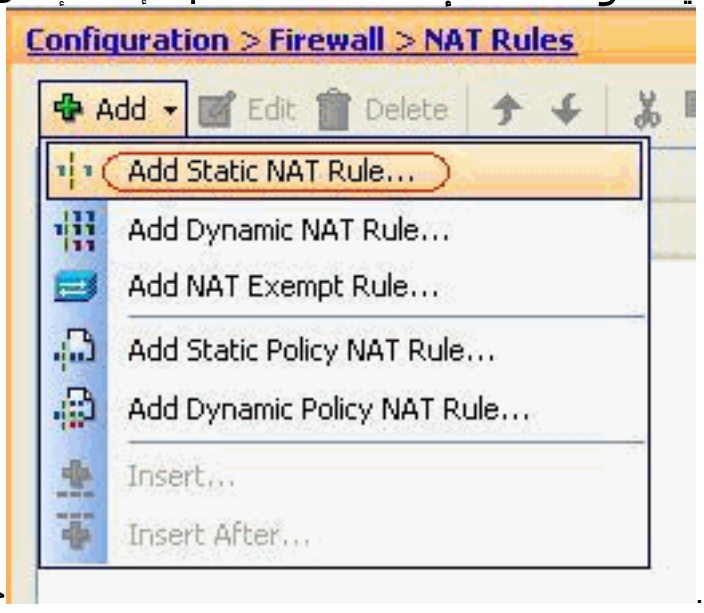
.ok

4. انقر فوق **موافق** لإكمال تكوين قاعدة

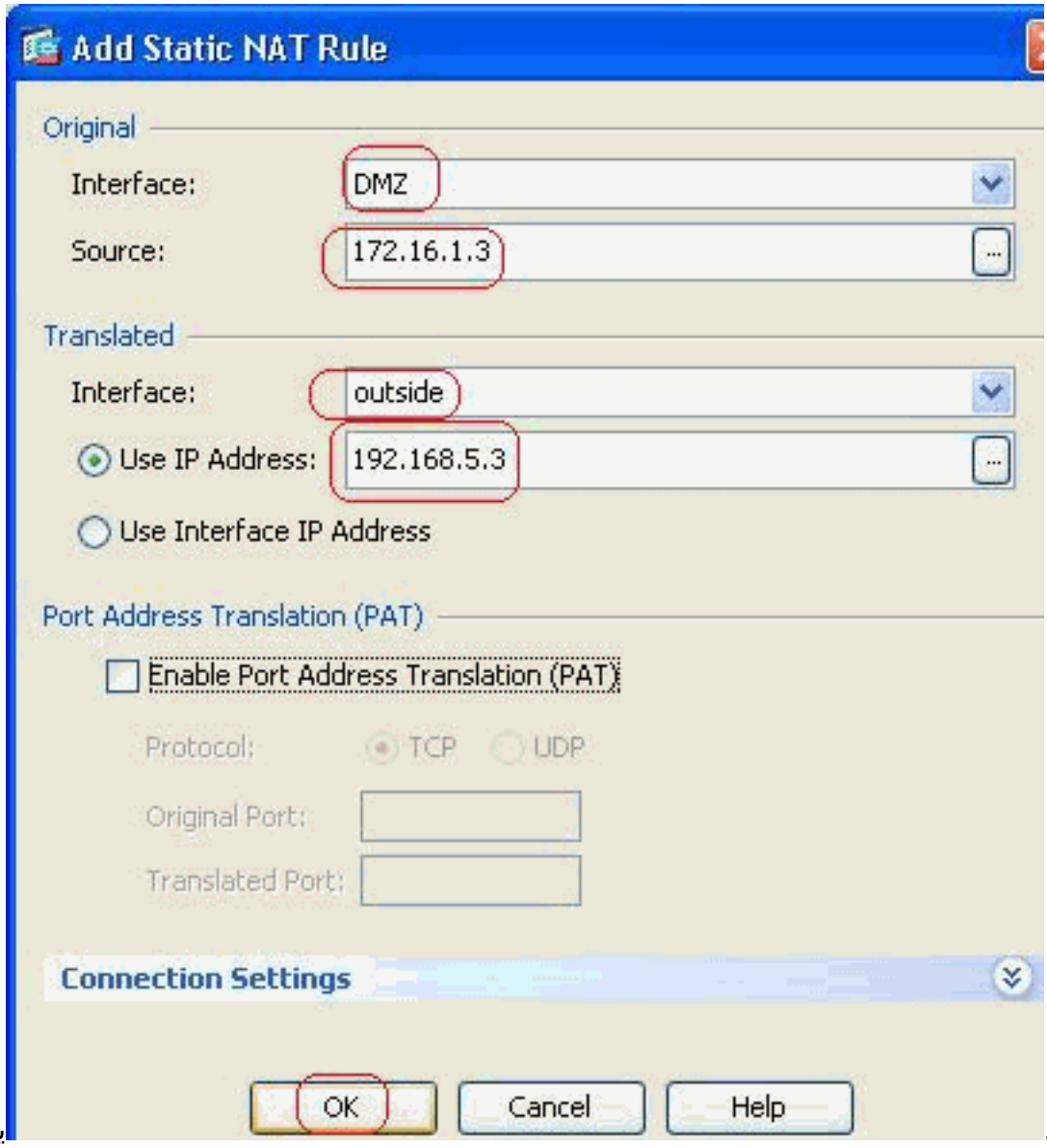


الوصول.

5. شكلت الساكن إستاتيكي nat in order to ترجمت ال 172.16.1.3 إلى 192.168.5.3انتقل إلى **التكوين > جدار الحماية > قواعد NAT > إضافة قاعدة NAT ثابتة** لإضافة إدخال NAT

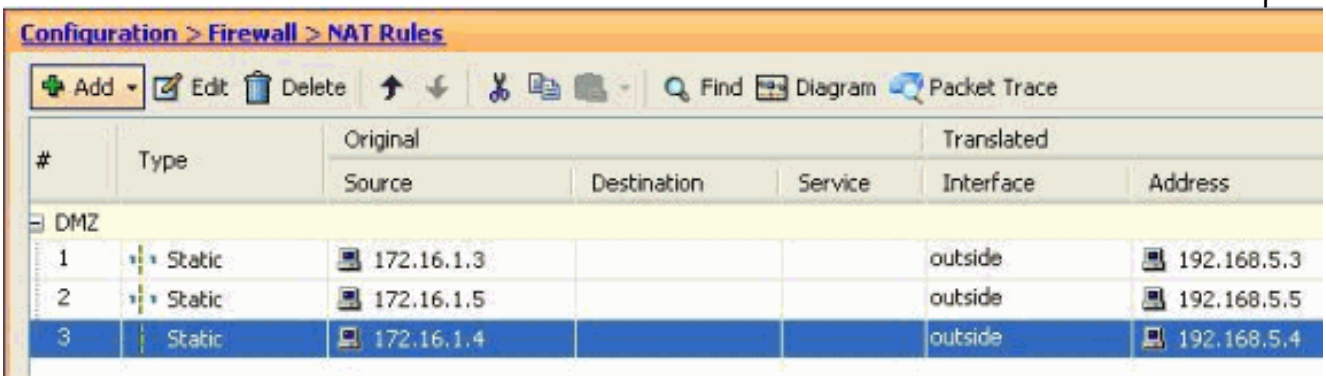


ثابت. حدد المصدر الأصلي وعنوان IP المترجم مع الواجهات المرتبطة به، ثم انقر **موافق** لإنهاء تكوين قاعدة NAT

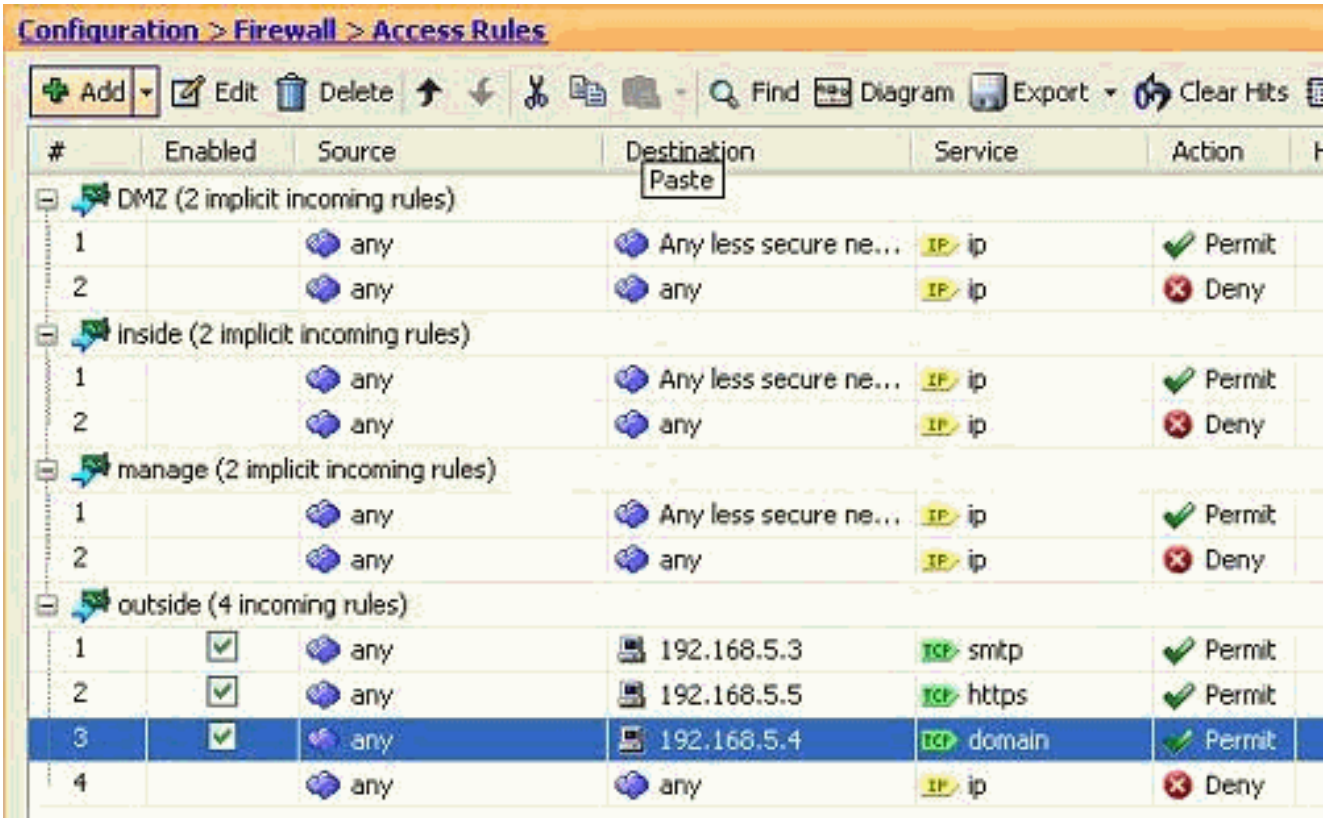


يصف هذا الثابتة.

صورة كل القواعد الثابتة الثلاثة التي تم سردها في الأمثلة قسم:



تصف هذه الصورة قواعد الوصول الثلاثة جميعها المدرجة في قسم الأمثلة:



التحقق من الصحة

يمكنك التحقق باستخدام بعض أوامر **show**، كما هو موضح:

- **show xlate**—عرض معلومات الترجمة الحالية
- **show access-list**—show hit counters لنهج الوصول
- **show logging** — عرض السجلات في المخزن المؤقت.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- PIX/ASA 7.x: تمكين/تعطيل الاتصال بين الواجهات
- PIX 7.0 وإعادة توجيه المنفذ (إعادة توجيه) جهاز الأمان القابل للتكيف مع أوامر NAT و global و static و access-list و channel
- إستخدام أوامر nat و global و static و channel و access-list وإعادة توجيه المنفذ (إعادة التوجيه) على PIX
- PIX/ASA 7.x: تمكين مثال تكوين خدمات FTP/TFTP
- PIX/ASA 7.x: تمكين مثال تكوين خدمات VoIP (SIP و MGCP و H323 و SCCP)
- PIX/ASA 7.x: الوصول إلى خادم البريد على مثال تكوين DMZ
- 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).