ASA 8.x والإصدارات الأحدث: إضافة قائمة وصول وأ لوصو ل GUI نيوكت لاثم لالخ نم اهليدعت ASDM

المحتويات

المقدمة

يشرح هذا المستند كيفية إستخدام مدير أجهزة الأمان المعدلة (ASDM) من Cisco للعمل باستخدام قوائم التحكم في الوصول. وهذا يشمل إنشاء قائمة وصول جديدة وكيفية تحرير قائمة وصول موجودة ووظائف أخرى باستخدام قوائم الوصول.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- أجهزة الأمان المعدلة Cisco Adaptive Security Appliance (ASA) مع الإصدار x.8.2
- مدير أجهزة حلول الأمان المعدلة (ASDM) من Cisco مع الإصدار x.6.3

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.

معلومات أساسية

يتم إستخدام قوائم الوصول بشكل أساسي للتحكم في تدفق حركة المرور عبر جدار الحماية. يمكنك السماح بأنواع معينة من حركة المرور باستخدام قوائم الوصول أو رفضها. تحتوي كل قائمة وصول على عدد من إدخالات قائمة الوصول (ACEs) التي تتحكم في تدفق حركة المرور من مصدر معين إلى وجهة معينة. عادة، تكون قائمة الوصول هذه مرتبطة بواجهة لإخطار إتجاه التدفق الذي يجب أن تبحث فيه. يتم تصنيف قوائم الوصول بشكل رئيسي إلى نوعين عريضين.

1. قوائم الوصول الواردة
2. قوائم الوصول الصادرة

تنطبق قوائم الوصول الواردة على حركة المرور التي تدخل هذه الواجهة، وقوائم الوصول الصادرة التي تنطبق على حركة المرور التي تخرج الواجهة. يشير التدوين الوارد/الصادر إلى إتجاه حركة المرور فيما يتعلق بتلك الواجهة ولكنه لا يشير إلى حركة مرور البيانات بين واجهات الأمان الأعلى والأسفل.

لاتصالات TCP و UDP، لا تحتاج إلى قائمة وصول للسماح بحركة المرور العائدة لأن جهاز الأمان يسمح لجميع حركة المرور العائدة للاتصالات الثنائية الإتجاه المؤسسة. بالنسبة للبروتوكولات غير المتصلة مثل ICMP، يقوم جهاز الأمان بإنشاء جلسات عمل أحادية الإتجاه، لذلك تحتاج إما إلى قوائم الوصول لتطبيق قوائم الوصول على واجهات المصدر والوجهة للسماح ل ICMP في كلا الاتجاهين، أو تحتاج إلى تمكين محرك فحص ICMP. يعامل محرك فحص ICMP جلسات ICMP على أنها إتصالات ثنائية الإتجاه.

من الإصدار x.6.3 من ASDM، هناك نوعان من قوائم الوصول يمكنك تكوينها.

1. قواعد الوصول إلى الواجهة
2. قواعد الوصول العالمية

ملاحظة: تشير قاعدة الوصول إلى إدخال قائمة وصول فردية (ACE).

ترتبط قواعد الوصول إلى الواجهة بأي واجهة في وقت إنشائها. بدون ربطها بواجهة، لا يمكنك إنشاؤها. وهذا يختلف عن مثال سطر الأوامر. باستخدام واجهة سطر الأوامر (CLI)، يمكنك أولا إنشاء قائمة الوصول باستخدام الأمر **access list**، ثم ربط قائمة الوصول هذه بواجهة باستخدام الأمر **access-group**. ASDM 6.3 والإصدارات الأحدث، يتم إنشاء قائمة الوصول والارتباط بواجهة كمهمة واحدة. ينطبق هذا على حركة المرور المتدفقة عبر تلك الواجهة المحددة فقط.

قواعد الوصول العمومي غير مرتبطة بأي واجهة. يمكن تكوينها من خلال علامة التبويب "مدير قائمة التحكم في الوصول" في ASDM ويتم تطبيقها على حركة مرور الدخول العالمية. يتم تنفيذها عندما يكون هناك تطابق استنادا إلى المصدر والوجهة ونوع البروتوكول. لا يتم نسخ هذه القواعد نسخا متماثلا على كل واجهة، لذلك فإنها توفر مساحة الذاكرة.

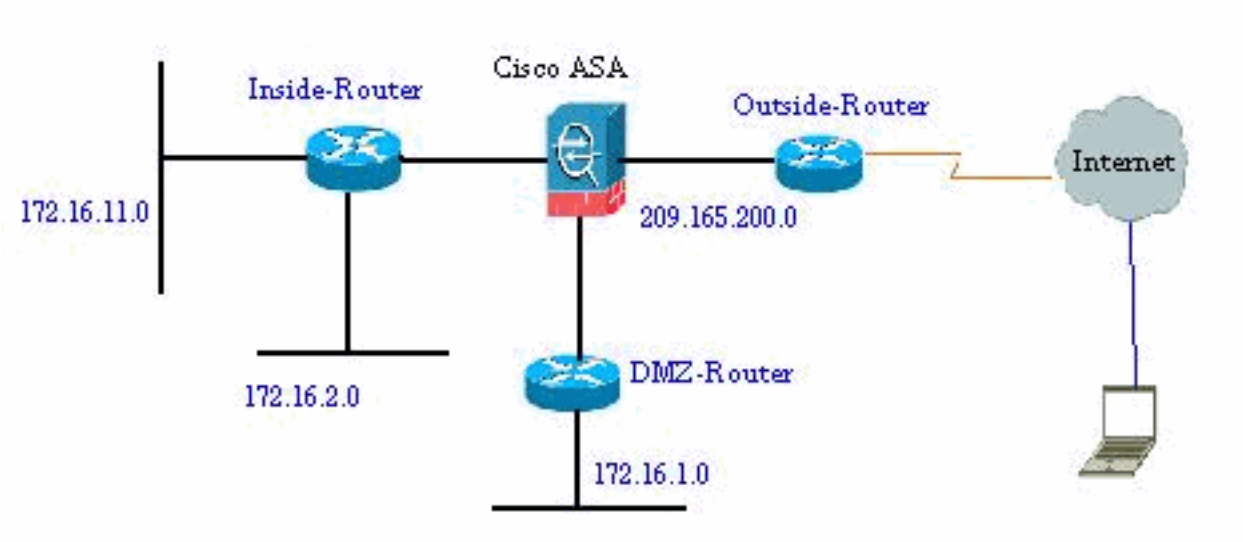
عندما يتم تنفيذ كل من هذه القواعد، تكون لقواعد الوصول إلى الواجهة عادة الأولوية على قواعد الوصول العالمية.

التكوين

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

الرسم التخطيطي للشبكة

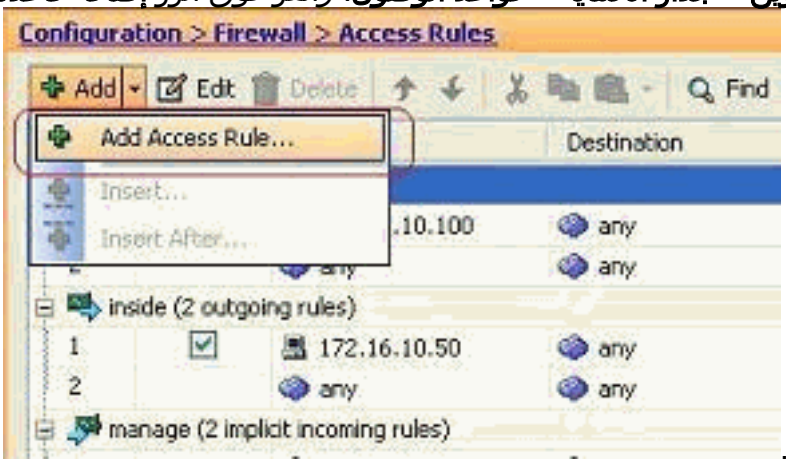
يستخدم هذا المستند إعداد الشبكة التالي:



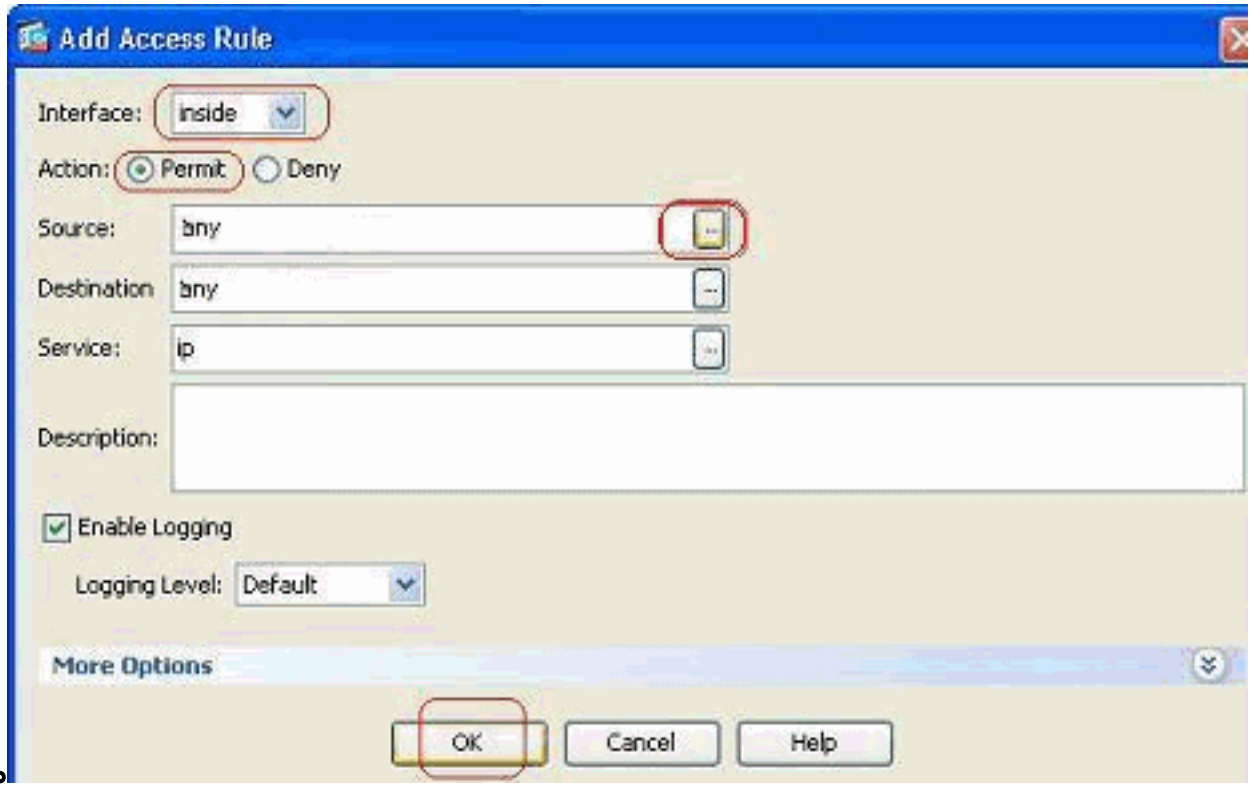
إضافة قائمة وصول جديدة

أكمل الخطوات التالية لإنشاء قائمة وصول جديدة باستخدام ASDM:

1. أختر **تكوين > جدار الحماية > قواعد الوصول**، وانقر فوق الزر **إضافة قاعدة الوصول**.

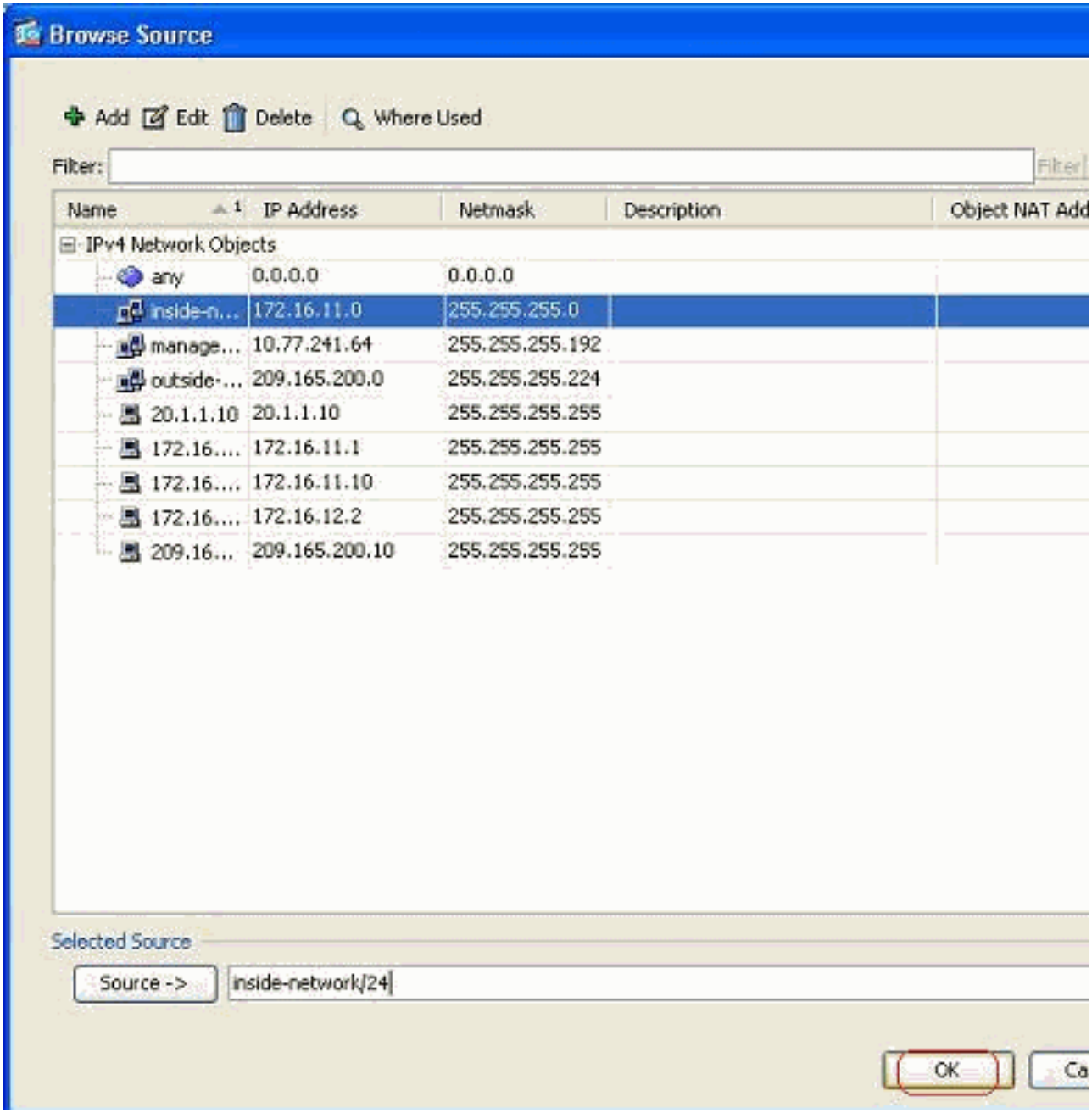


2. أختر الواجهة التي يجب أن ترتبط بها قائمة الوصول هذه، بالإضافة إلى الإجراء الذي سيتم إجراؤه على حركة المرور مثل، السماح/الرفض. ثم انقر على زر **التفاصيل** لتحديد الشبكة المصدر.

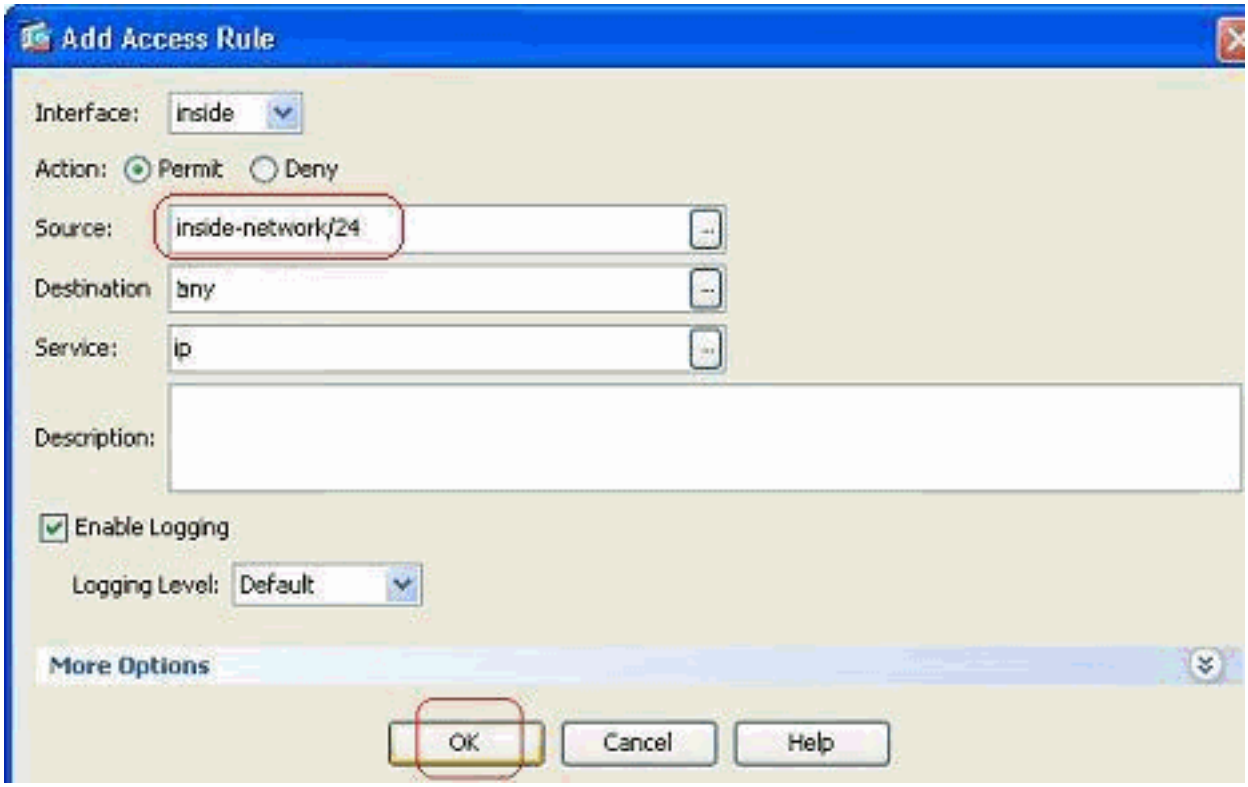


ملاحظة: فيما يلي شرح مختصر للحقول المختلفة المعروضة في هذه النافذة:**الواجهة**—يحدد الواجهة التي ترتبط بها قائمة الوصول هذه.**الإجراء** — يحدد نوع الإجراء للقاعدة الجديدة. هناك خياران متاحان. **السماح** يسمح لجميع حركة المرور المطابقة وكتل **الرفض** لجميع حركة المرور المطابقة.**المصدر**—يحدد هذا الحقل مصدر حركة المرور. يمكن أن يكون هذا أي شيء بين عنوان IP واحد أو شبكة أو عنوان IP للواجهة لجدار الحماية أو مجموعة كائن شبكة. يمكن تحديد هذه العناصر باستخدام زر **التفاصيل**.**غاية** — يعين هذا مجال مصدر الحركة مرور. يمكن أن يكون هذا أي شيء بين عنوان IP واحد أو شبكة أو عنوان IP للواجهة لجدار الحماية أو مجموعة كائن شبكة. يمكن تحديد هذه العناصر باستخدام زر **التفاصيل**.**الخدمة**—يحدد هذا الحقل بروتوكول حركة المرور التي يتم تطبيق قائمة الوصول هذه عليها أو خدمتها. كما يمكنك تحديد مجموعة خدمة تحتوي على مجموعة من البروتوكولات المختلفة.

3. بعد النقر فوق الزر **تفاصيل**، يتم عرض نافذة جديدة تحتوي على كائنات الشبكة الموجودة. حدد **الشبكة الداخلية**، وانقر فوق
موافق.



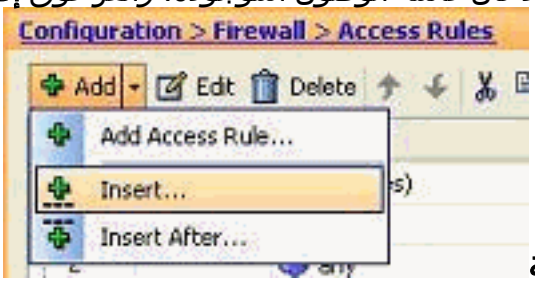
4. يتم إرجاعك إلى نافذة **إضافة قاعدة الوصول**. اكتب **any** في حقل الوجهة. وانقر فوق **موافق** لإكمال تكوين قاعدة
الوصول.



إضافة قاعدة وصول قبل قاعدة موجودة:

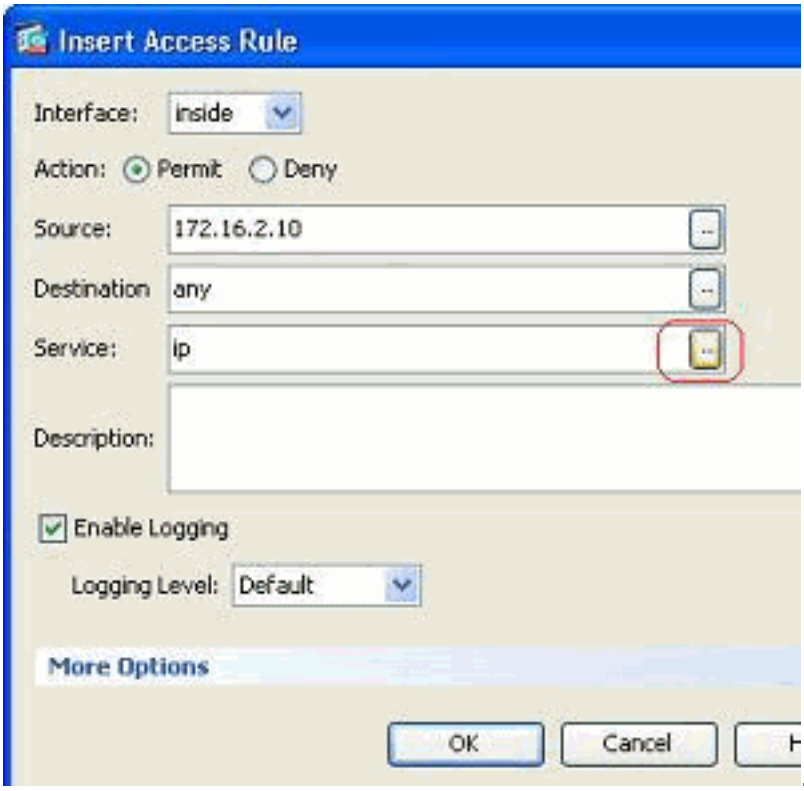
أكمل الخطوات التالية لإضافة قاعدة وصول مباشرة قبل قاعدة وصول موجودة بالفعل:

1. حدد إدخال قائمة الوصول الموجودة، وانقر فوق **إدراج** من القائمة المنسدلة



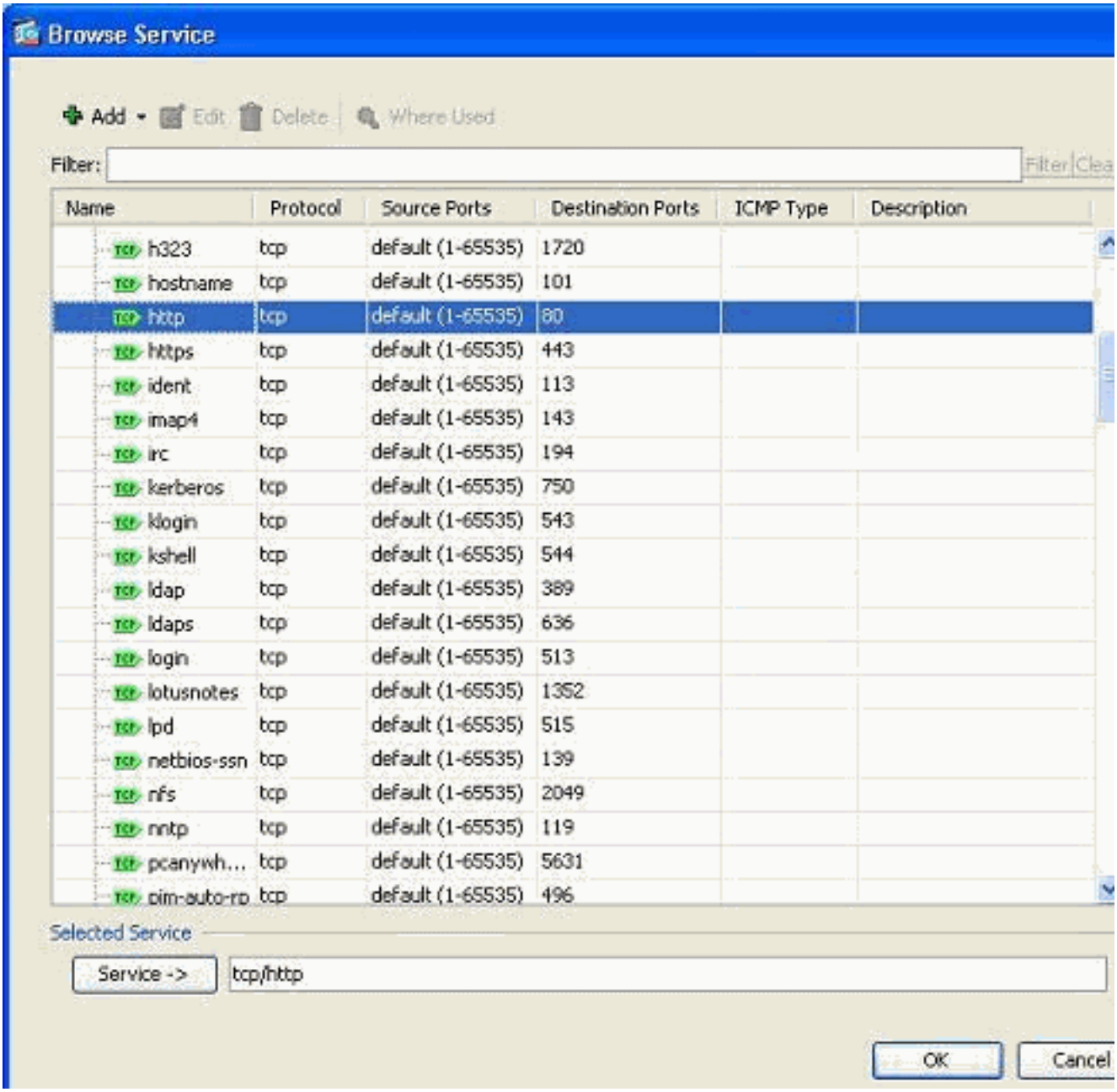
إضافة

2. أختر المصدر والوجهة، وانقر فوق زر **التفاصيل** في حقل الخدمة لاختيار

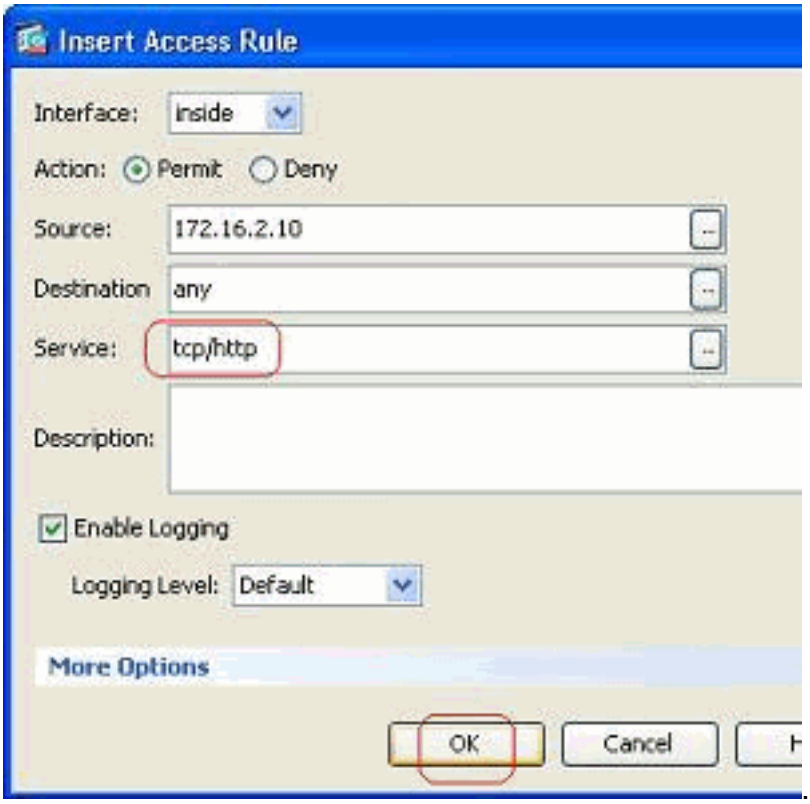


البروتوكول.

3. أخترت HTTP البروتوكول، وطقطقة **ok**.

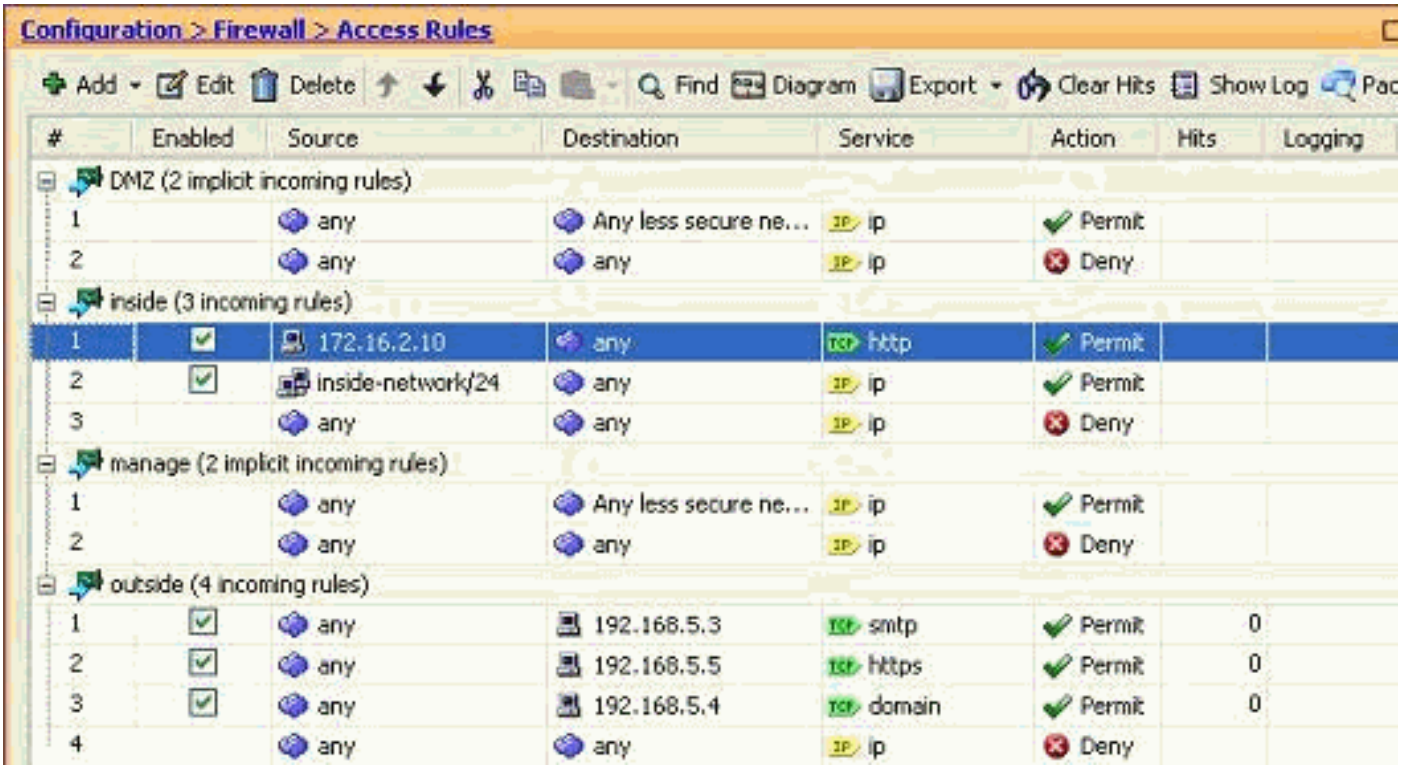


4. يتم إرجاعك إلى نافذة "إدراج قاعدة الوصول". يتم ملء حقل الخدمة **بـ tcp/http** كبروتوكول محدد. انقر فوق **موافق** لإكمال تكوين إدخال قائمة الوصول



الجديدة.

يمكنك الآن ملاحظة قاعدة الوصول الجديدة الموضحة قبل الإدخال الموجود بالفعل للشبكة الداخلية مباشرة.



ملاحظة: ترتيب قواعد الوصول مهم جدا. أثناء معالجة كل حزمة للتصفية، يفحص ASA ما إذا كانت الحزمة تطابق أي من معيار قاعدة الوصول في ترتيب تسلسلي وإذا حدثت تطابق، فإنها تنفذ الإجراء الخاص بقاعدة الوصول تلك. عند مطابقة قاعدة وصول، لا تتم المتابعة إلى المزيد من قواعد الوصول والتحقق منها مرة أخرى.

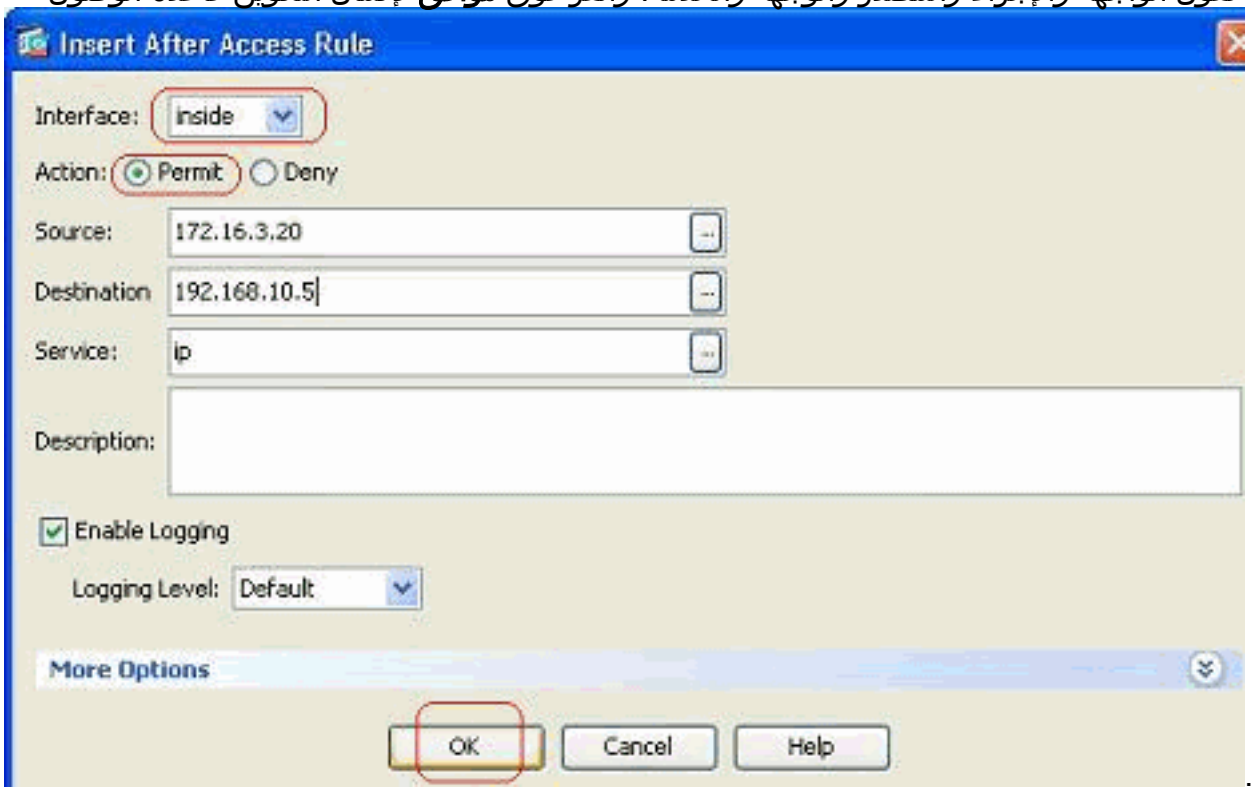
إضافة قاعدة وصول بعد أخرى موجودة:

أكمل هذه الخطوات لإنشاء قاعدة وصول مباشرة بعد قاعدة وصول موجودة بالفعل.

1. حدد قاعدة الوصول التي تحتاج بعد ذلك إلى وجود قاعدة وصول جديدة، واختر **إدراج بعد** من القائمة المنسدلة

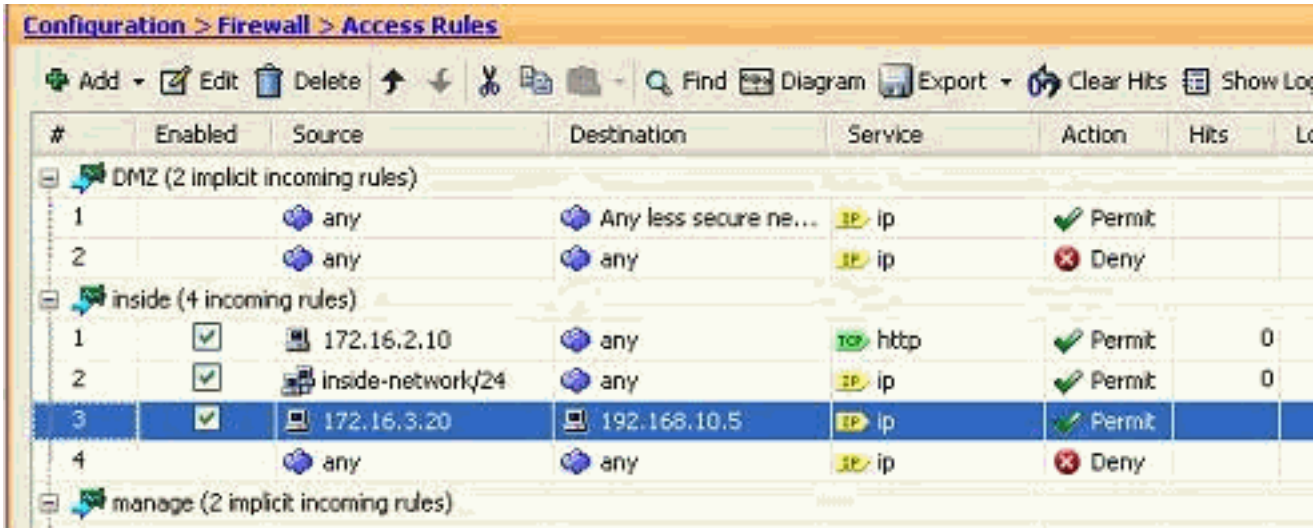
إضافة.

2. حدد حقول الواجهة والإجراء والمصدر والوجهة والخدمة، وانقر فوق **موافق** لإكمال التكوين قاعدة الوصول



هذه.

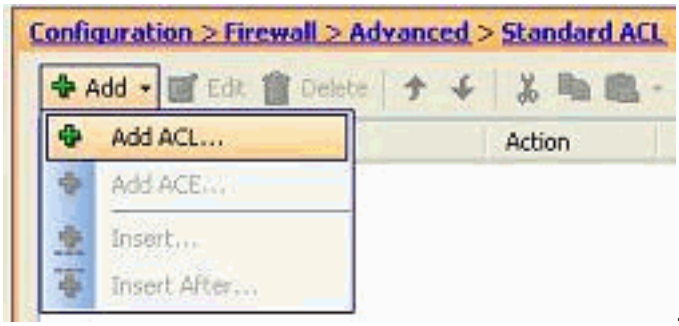
يمكنك عرض قاعدة الوصول التي تم تكوينها حديثا بعد القاعدة التي تم تكوينها بالفعل مباشرة.



إنشاء قائمة وصول قياسية

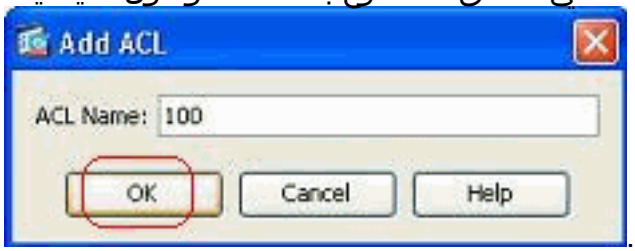
أكمل هذه الخطوات لإنشاء قائمة وصول قياسية باستخدام واجهة المستخدم الرسومية (GUI) ل ASDM.

1. أختر **التكوين > جدار الحماية > متقدم > قائمة التحكم في الوصول القياسية > إضافة**، وانقر فوق **إضافة قائمة**



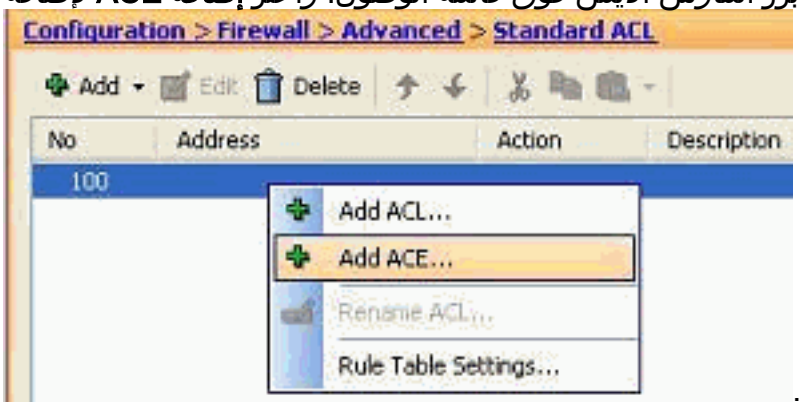
التحكم في الوصول (ACL).

2. امنح رقما في النطاق المسموح به لقائمة الوصول القياسية، وانقر فوق



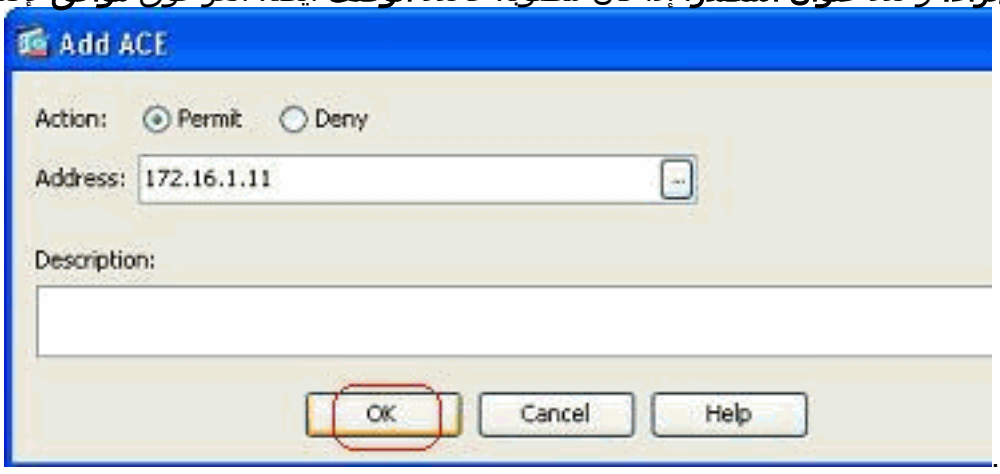
موافق.

3. انقر بزر الماوس الأيمن فوق قائمة الوصول، واختر **إضافة ACE** لإضافة قاعدة وصول إلى قائمة الوصول



هذه.

4. حدد **الإجراء**، وحدد **عنوان المصدر**. إذا كان مطلوبا، فحدد **الوصف** أيضا. انقر فوق **موافق** لإكمال تكوين قاعدة

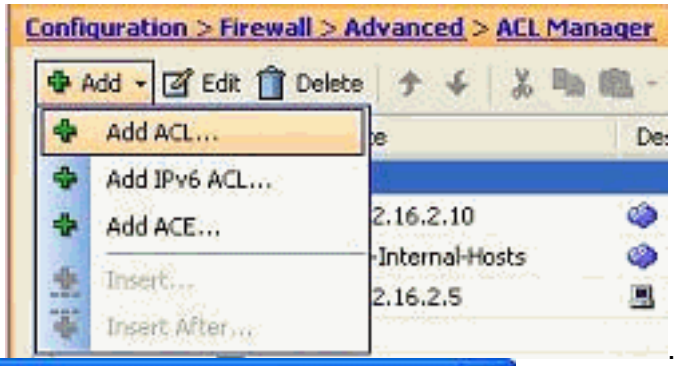


الوصول.

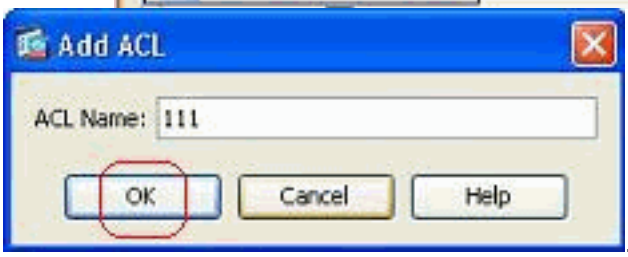
إنشاء قاعدة وصول عمومية

أكمل هذه الخطوات لإنشاء قائمة وصول موسعة تحتوي على قواعد وصول عمومية.

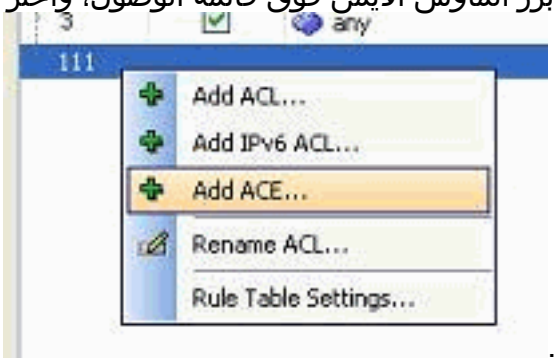
1. أختر **تكوين > جدار حماية > متقدم > إدارة قائمة التحكم في الوصول (ACL) > إضافة**، وانقر فوق **زر إضافة**



قائمة التحكم في الوصول (ACL).

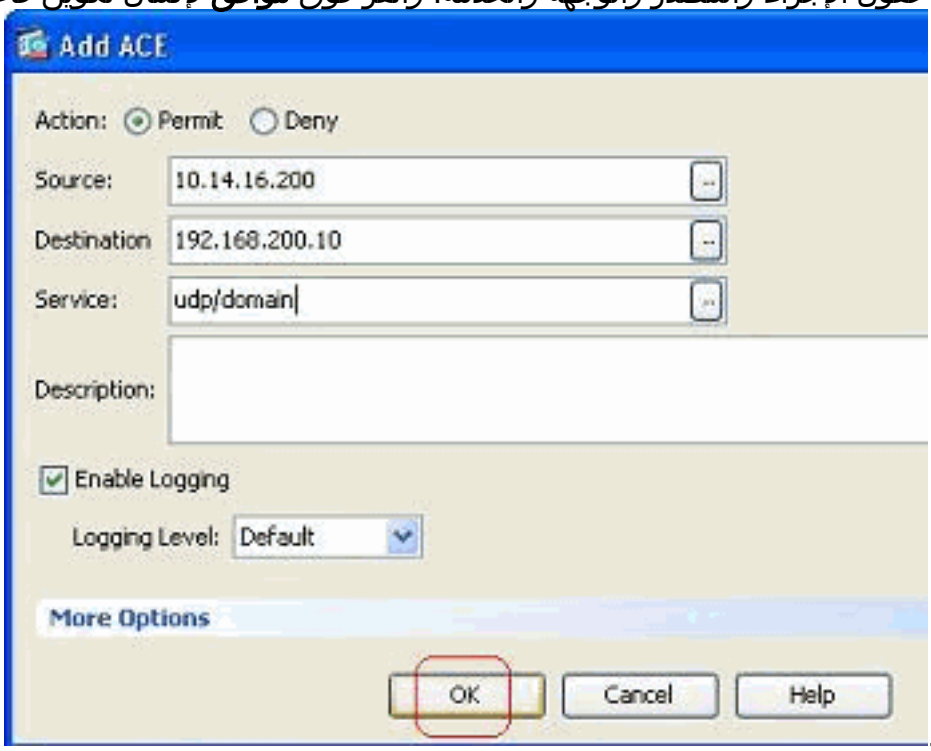


2. حدد اسما لقائمة الوصول، ثم انقر على **موافق**.
3. انقر بزر الماوس الأيمن فوق قائمة الوصول، واختر **إضافة ACE** لإضافة قاعدة وصول إلى قائمة الوصول



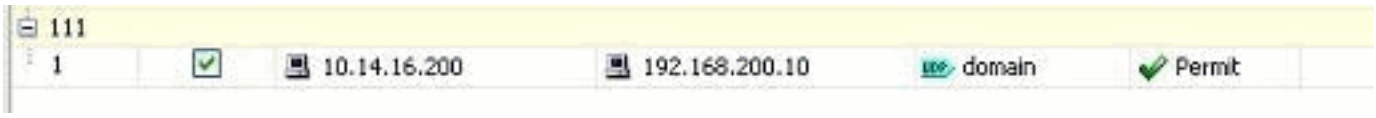
هذه.

4. أكمل حقول الإجراء والمصدر والوجهة والخدمة، وانقر فوق **موافق** لإكمال تكوين قاعدة الوصول



العام.

يمكنك الآن عرض قاعدة الوصول العام، كما هو موضح.



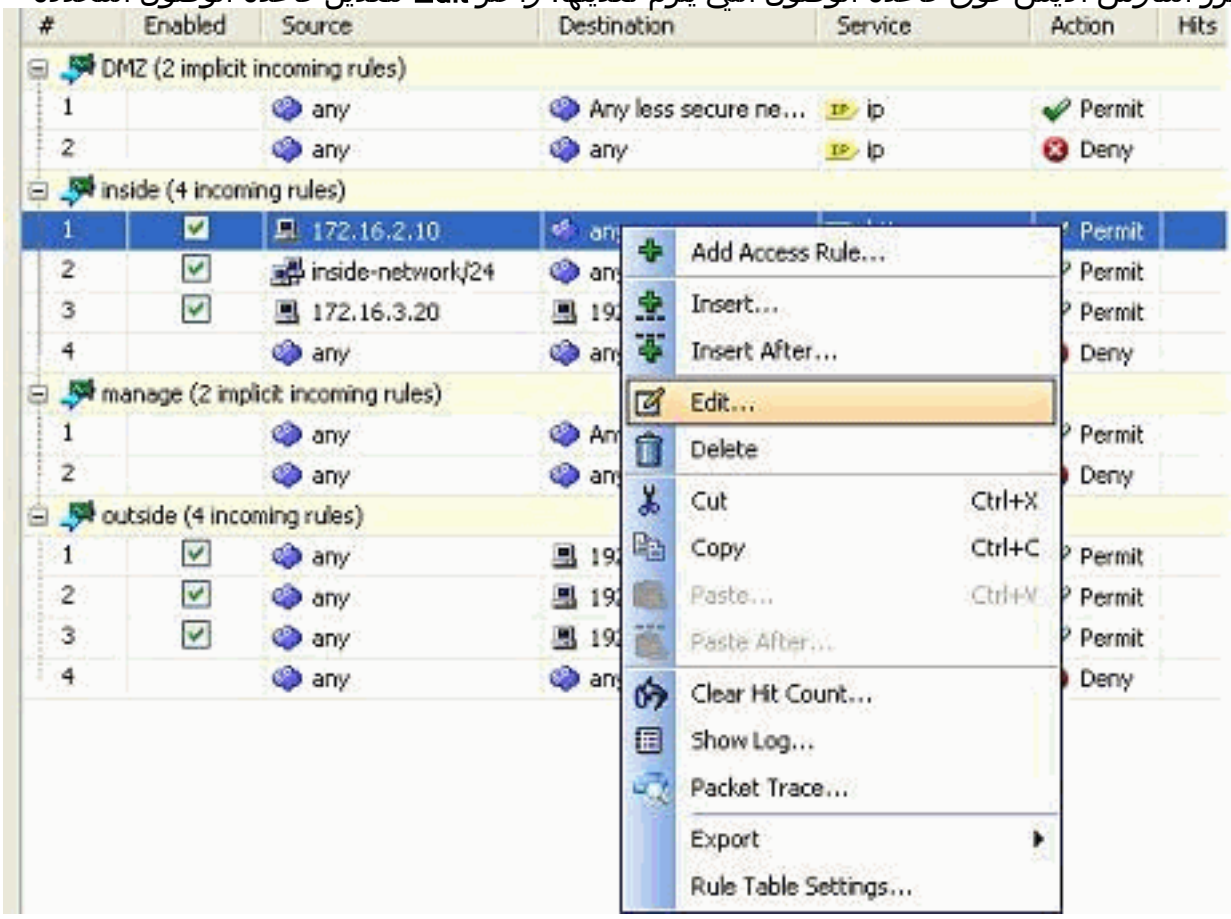
تحرير قائمة وصول موجودة

يناقش هذا القسم كيفية تحرير وصول موجود.

تحرير حقل البروتوكول لإنشاء مجموعة خدمات:

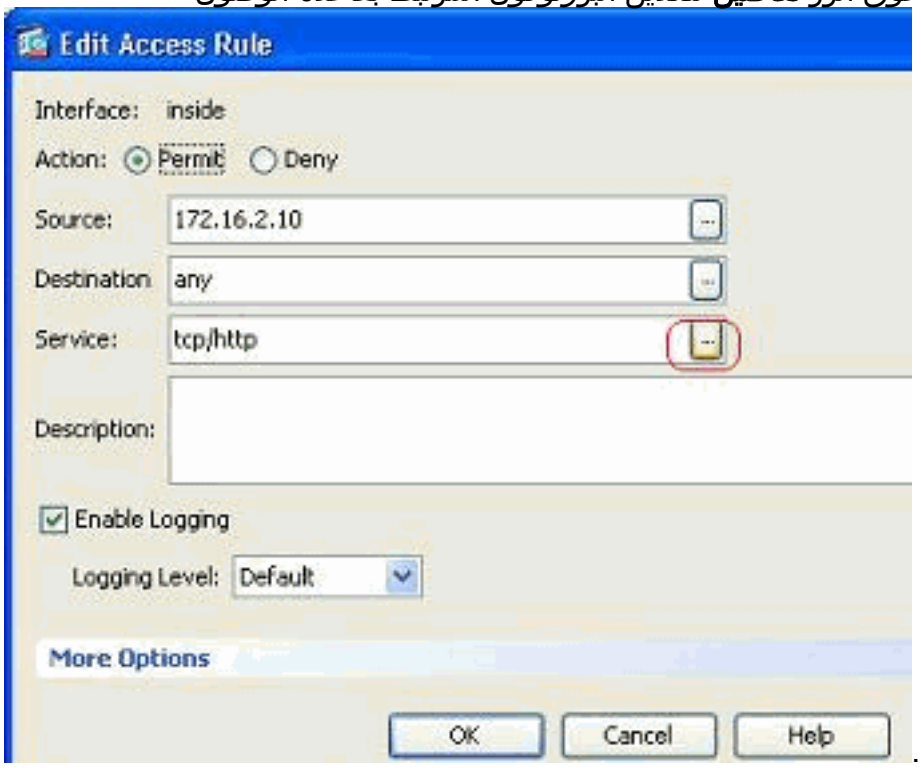
أكمل هذه الخطوات لإنشاء مجموعة خدمات جديدة.

1. انقر بزر الماوس الأيمن فوق قاعدة الوصول التي يلزم تعديلها، واختر **Edit** لتعديل قاعدة الوصول المحددة



هذه.

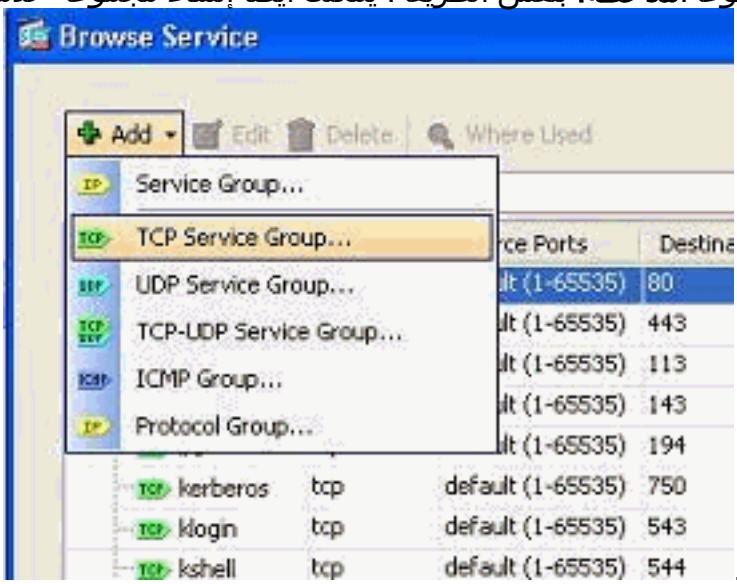
2. انقر فوق الزر **تفاصيل** لتعديل البروتوكول المرتبط بقاعدة الوصول



هذه.

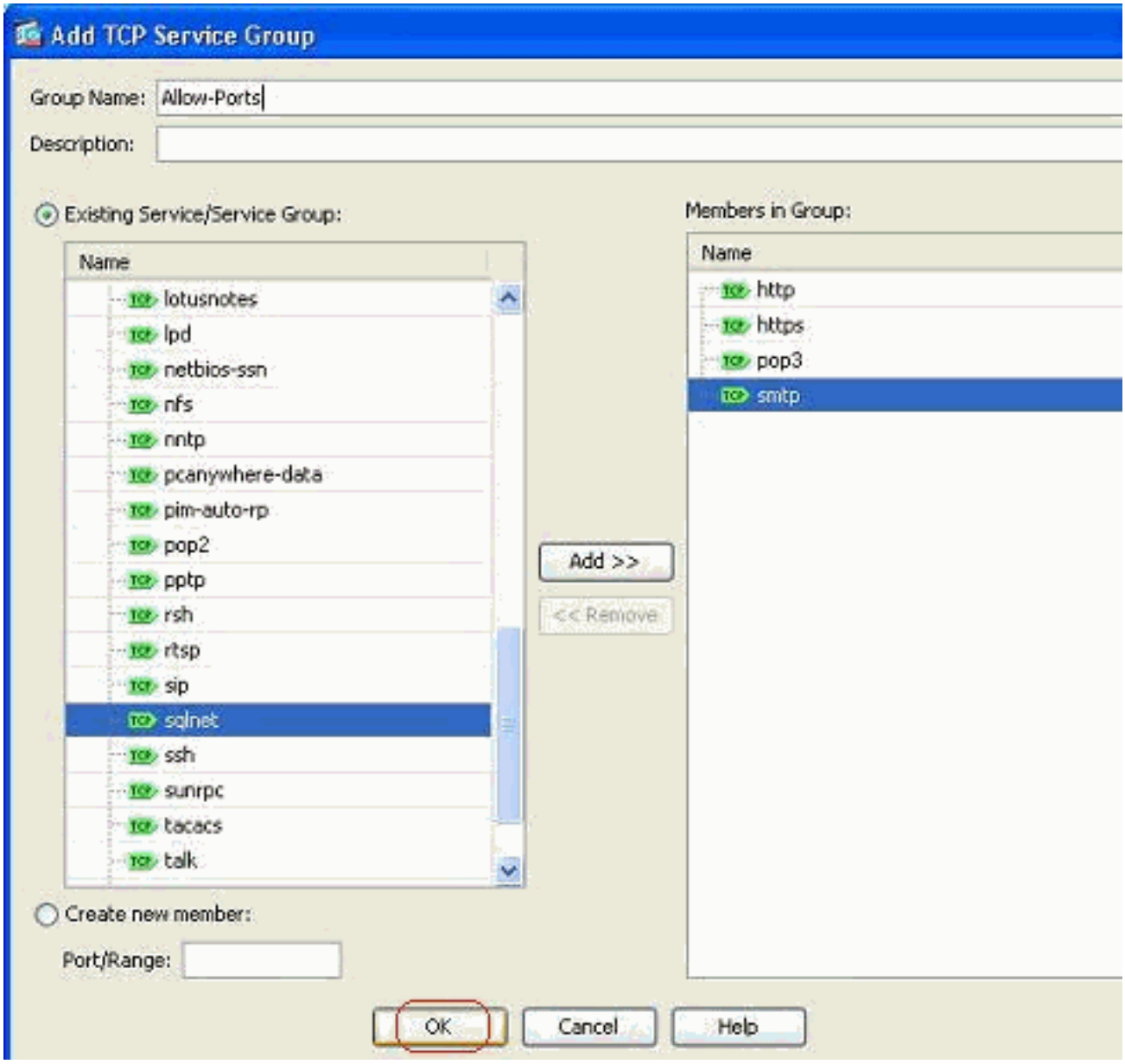
3. يمكنك تحديد أي بروتوكول آخر غير HTTP إذا كان مطلوبا. في حالة وجود بروتوكول واحد فقط ليتم تحديده،

فلا حاجة لإنشاء مجموعة الخدمات. من المفيد إنشاء مجموعة خدمات عند وجود متطلبات لتحديد العديد من البروتوكولات غير المتجاورة التي سيتم مطابقتها بقاعدة الوصول هذه.أخترت **إضافة<TCP خدمة مجموعة** in order to خلقت جديد TCP خدمة مجموعة.**ملاحظة:** بنفس الطريقة، يمكنك أيضا إنشاء مجموعة خدمة UDP

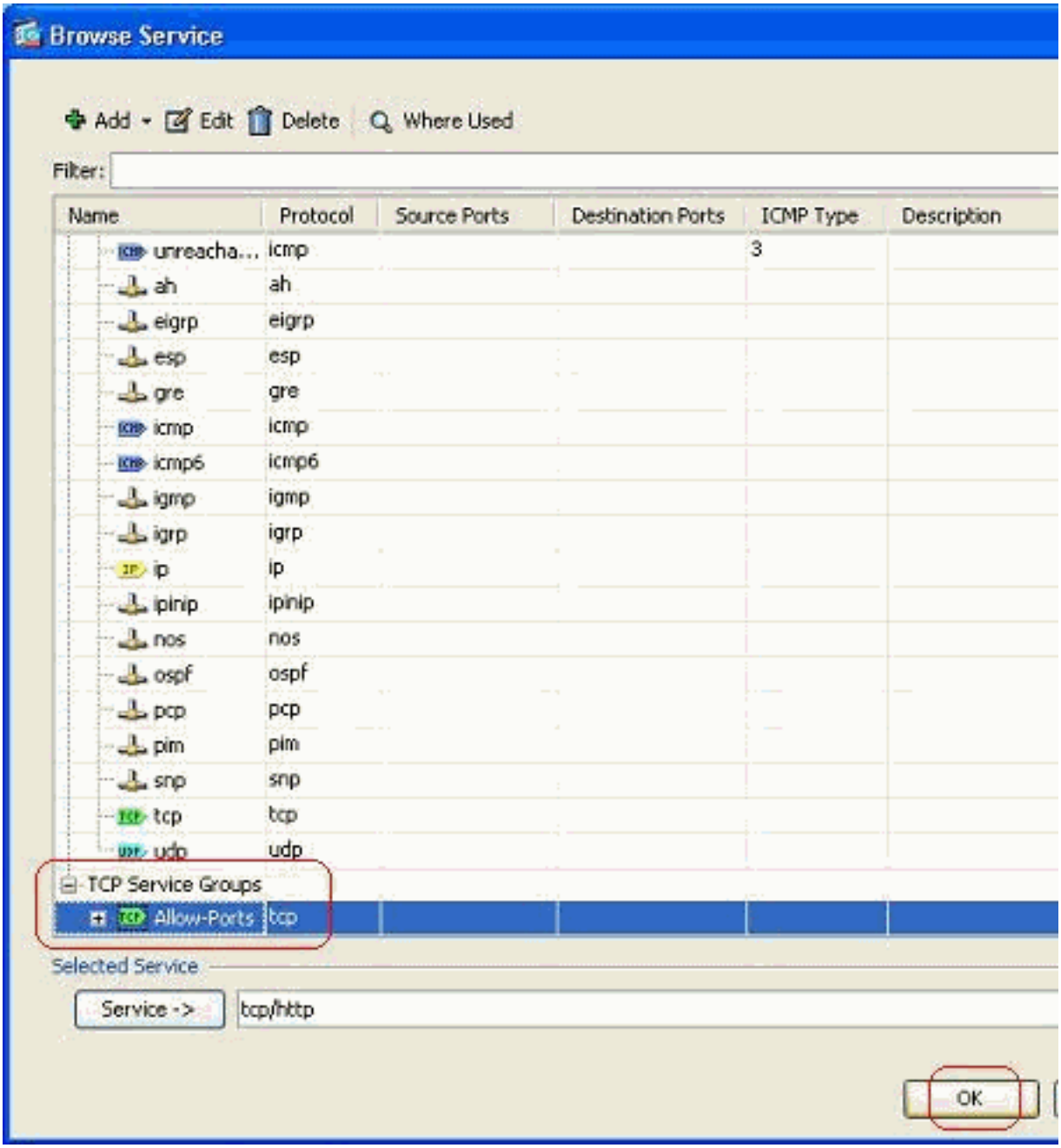


جديدة أو مجموعة ICMP وما إلى ذلك.

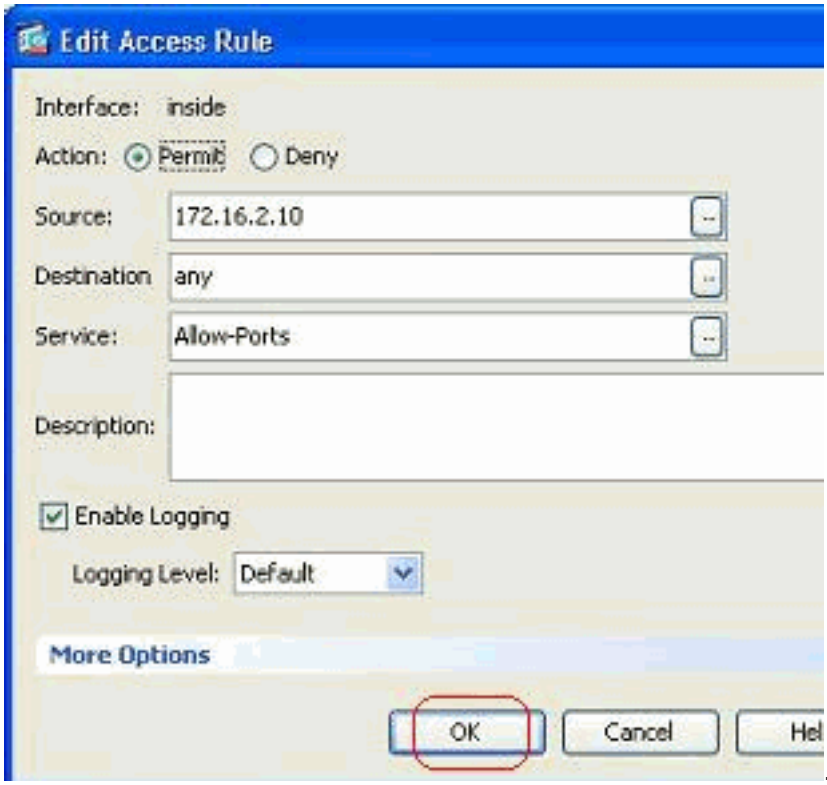
4. حدد اسما لمجموعة الخدمات هذه، وحدد البروتوكول في القائمة الموجودة على الجانب الأيسر، وانقر فوق **إضافة** لنقلهم إلى قائمة الأعضاء في المجموعة الموجودة على الجانب الأيمن. يمكن إضافة العديد من البروتوكولات كأعضاء في مجموعة خدمة وفقا للمتطلبات. تتم إضافة البروتوكولات واحدا تلو الآخر. بعد إضافة جميع الأعضاء، انقر فوق **موافق**.



5. يمكن عرض مجموعة الخدمات التي تم إنشاؤها حديثا ضمن علامة التبويب **مجموعات خدمة TCP**. انقر فوق الزر **موافق** للعودة إلى نافذة "تحرير قاعدة الوصول".

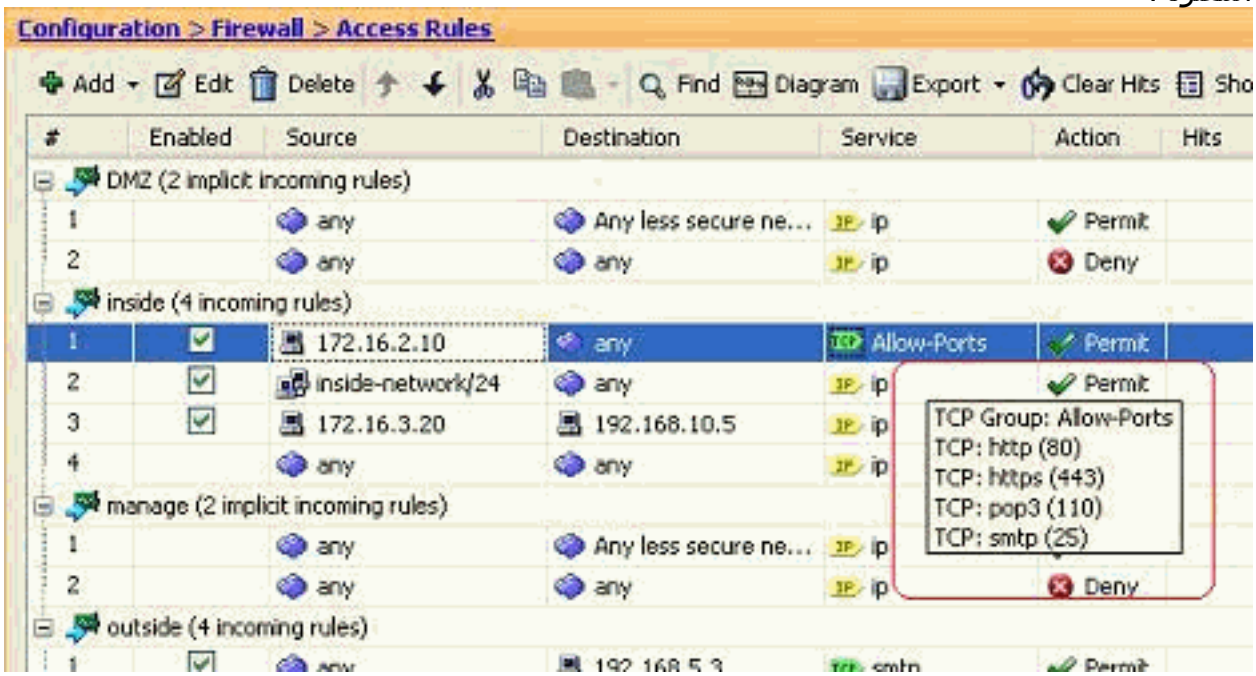


6. يمكنك أن ترى أن حقل الخدمة يتم تعبئته بمجموعة الخدمة التي تم إنشاؤها حديثا. طقطقة ok in order to



أتمت التحرير.

7. قم بتحريك الماوس عبر مجموعة الخدمات المحددة هذه لعرض جميع البروتوكولات المقترنة.

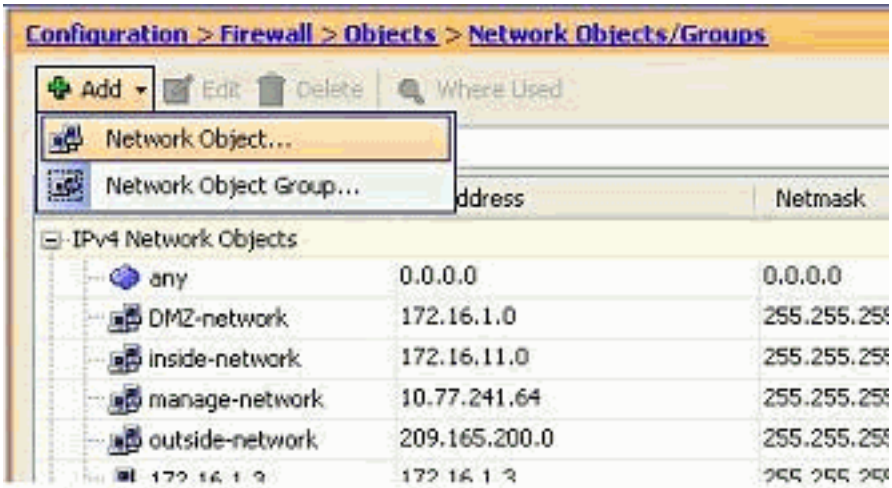


تحرير حقول المصدر/الوجهة لإنشاء مجموعة كائنات الشبكة:

يتم إستخدام مجموعات الكائنات لتبسيط إنشاء قوائم الوصول وصيانتها. عندما تقوم بتجميع كائنات مثل معا، يمكنك إستخدام مجموعة الكائن في ACE واحد بدلا من الحاجة لإدخال ACE لكل كائن بشكل مستقل. قبل أن تقوم بإنشاء مجموعة كائن، تحتاج لإنشاء الكائنات. في مصطلحات ASDM، يسمى الكائن كائن الشبكة وتسمى مجموعة الكائن مجموعة كائن الشبكة.

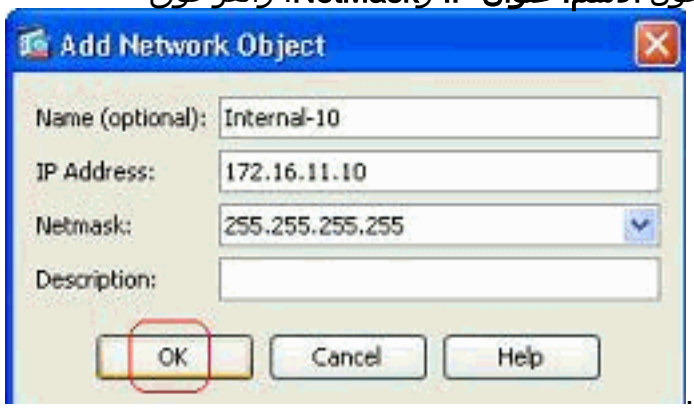
أكمل الخطوات التالية:

1. أختر **تشكيل > جدار حماية > كائنات > كائنات/مجموعات الشبكة > إضافة**، وانقر **كائن الشبكة** لإنشاء كائن شبكة



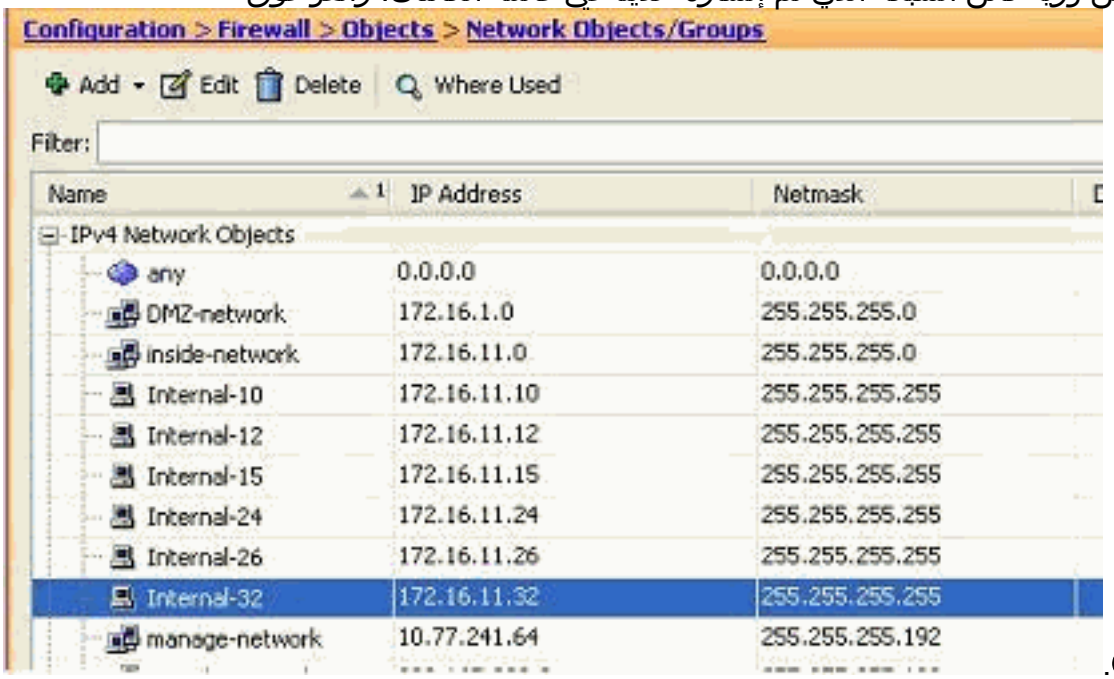
جديد.

2. املأ حقول **الاسم، عنوان IP** و**NetMask**، وانقر فوق



موافق.

3. يمكن رؤية كائن الشبكة الذي تم إنشاؤه حديثا في قائمة الكائنات. وانقر فوق

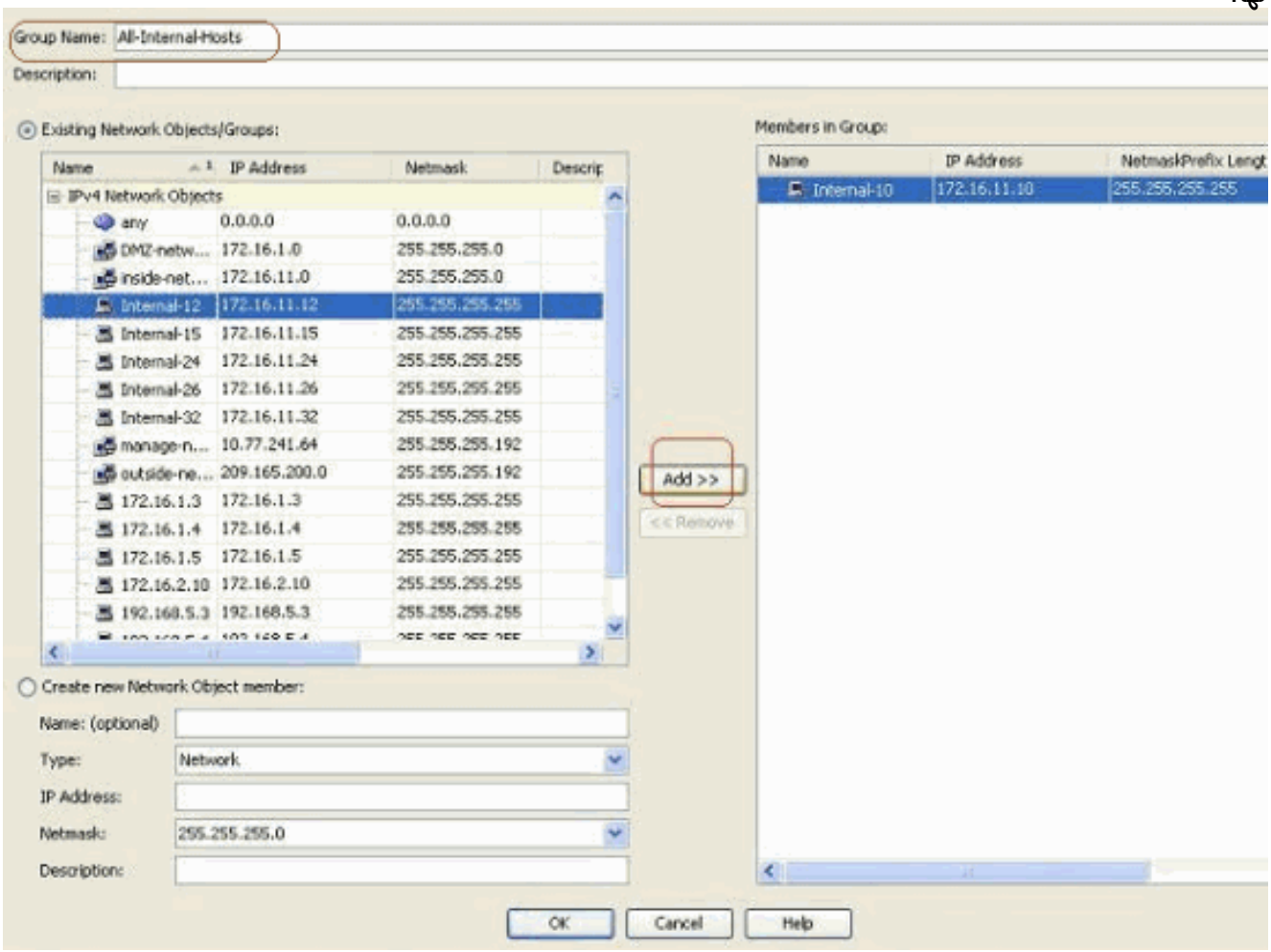


OK.

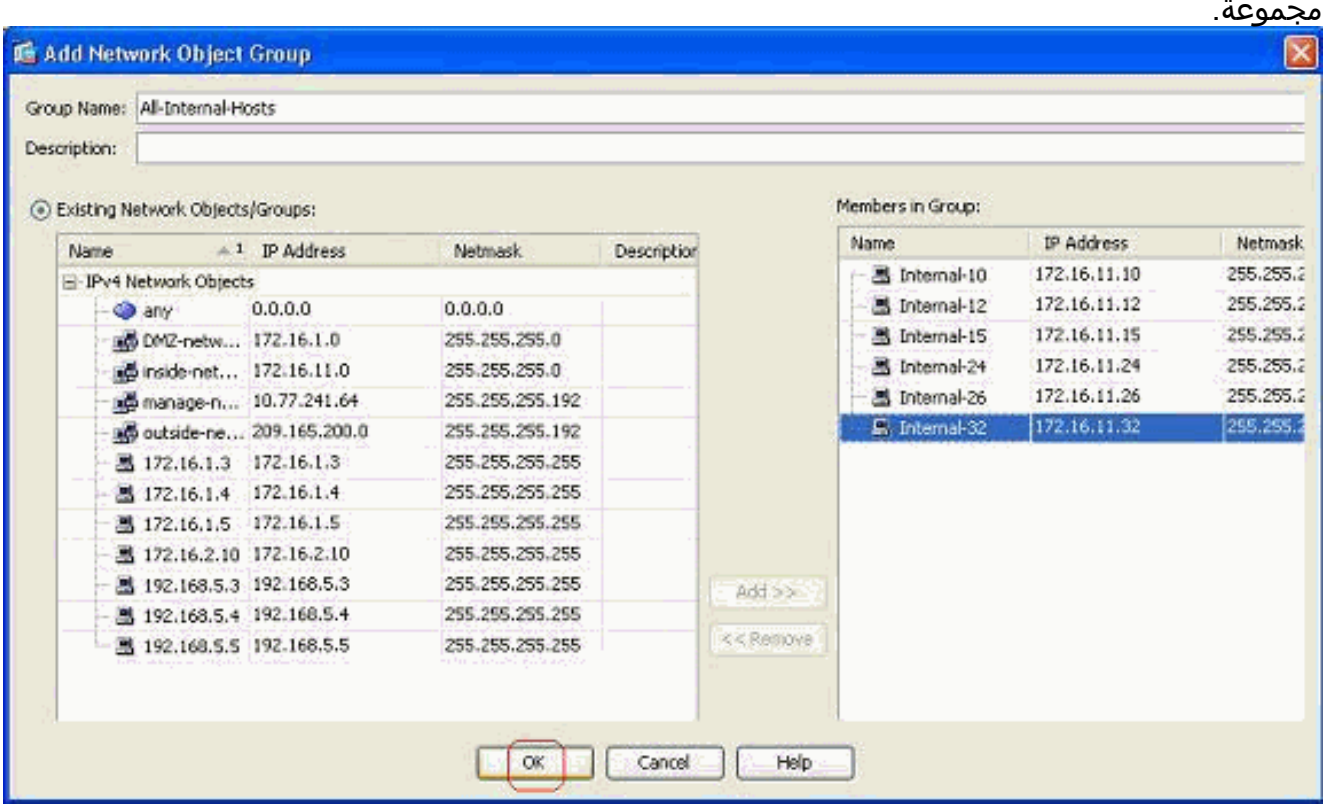
4. أختر **تشكيل > جدار حماية > كائنات > كائنات/مجموعات الشبكة > إضافة**، وانقر **مجموعة كائنات الشبكة** لإنشاء

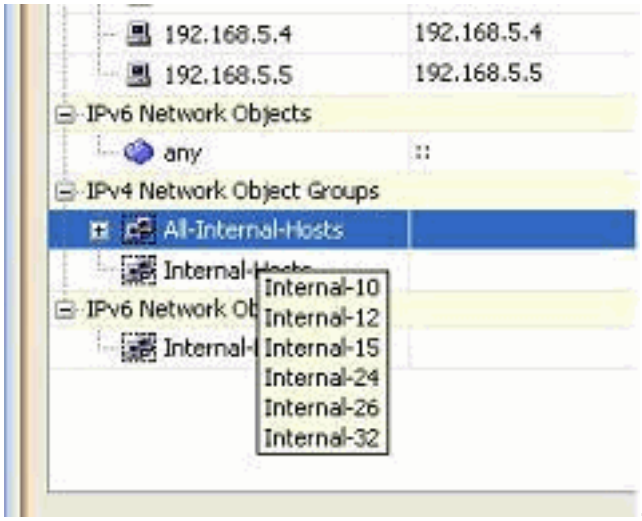
مجموعة كائنات شبكة جديدة.

5. يمكن العثور على القائمة المتوفرة لجميع كائنات الشبكة في الجزء الأيسر من الإطار. حدد كائنات شبكة منفردة، وانقر زر **إضافة** in order to جعلهم أعضاء من مجموعة كائنات الشبكة التي تم إنشاؤها حديثا. يجب تحديد اسم المجموعة في الحقل المخصص
لها.



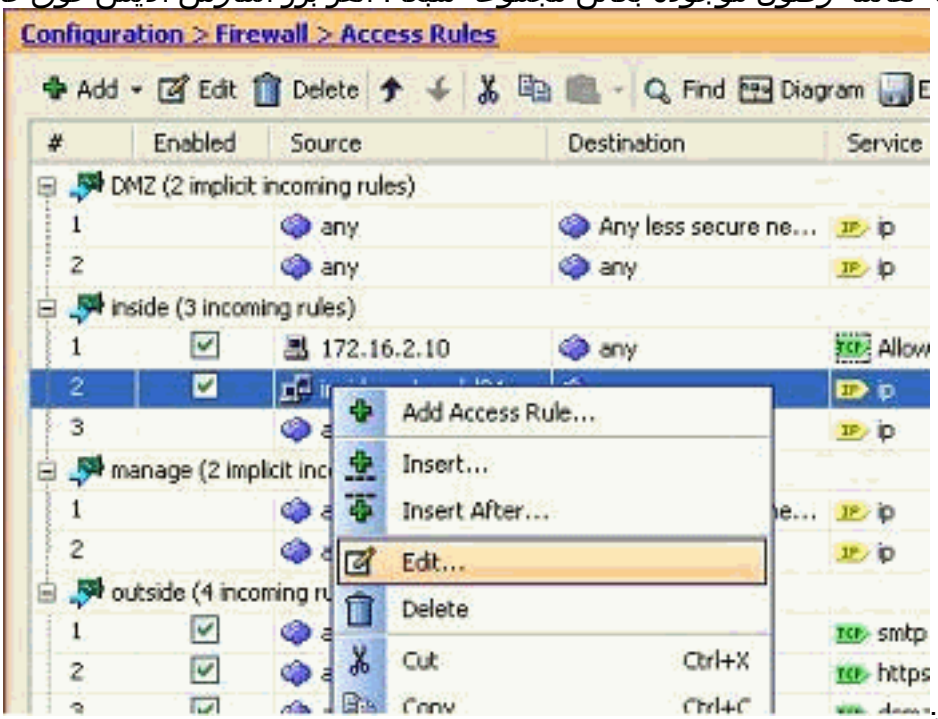
6. طقطقت **ok** بعد أن أنت تضيف كل الأعضاء إلى
مجموعة.





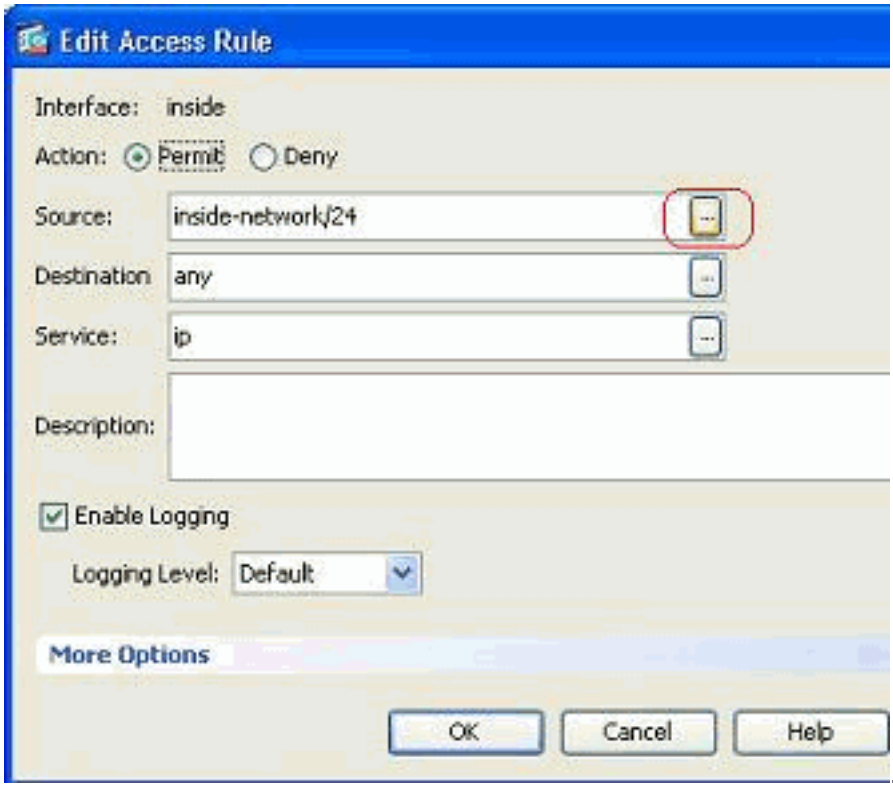
يمكنك الآن عرض مجموعة كائنات الشبكة.

7. لتعديل أي حقل مصدر/وجهة لقائمة وصول موجودة بكائن مجموعة شبكة، انقر بزر الماوس الأيمن فوق قاعدة



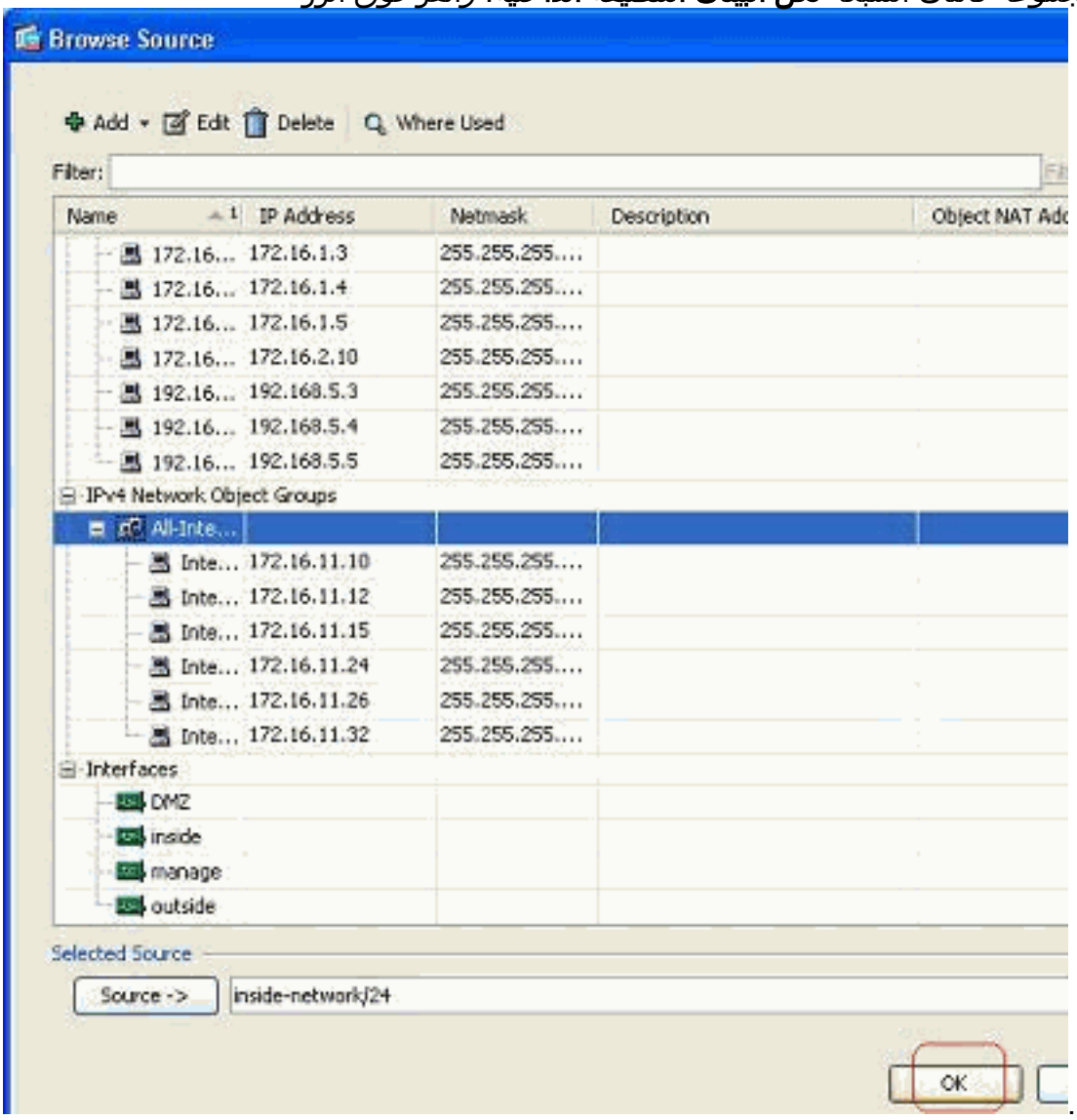
وصول محددة، واختر **تحرير**.

8. تظهر نافذة تحرير قاعدة الوصول. انقر فوق الزر **تفاصيل** في حقل المصدر

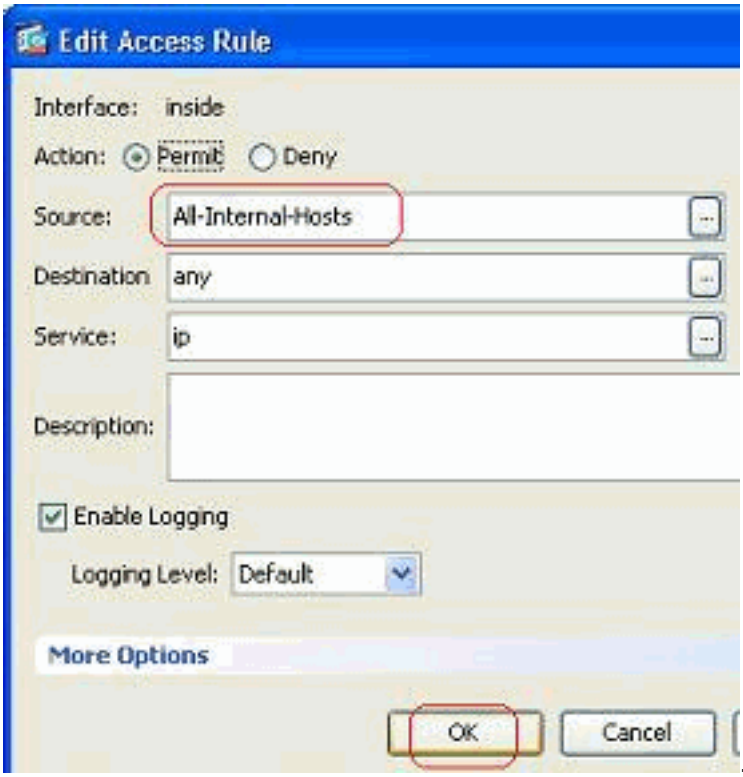


لتعديله.

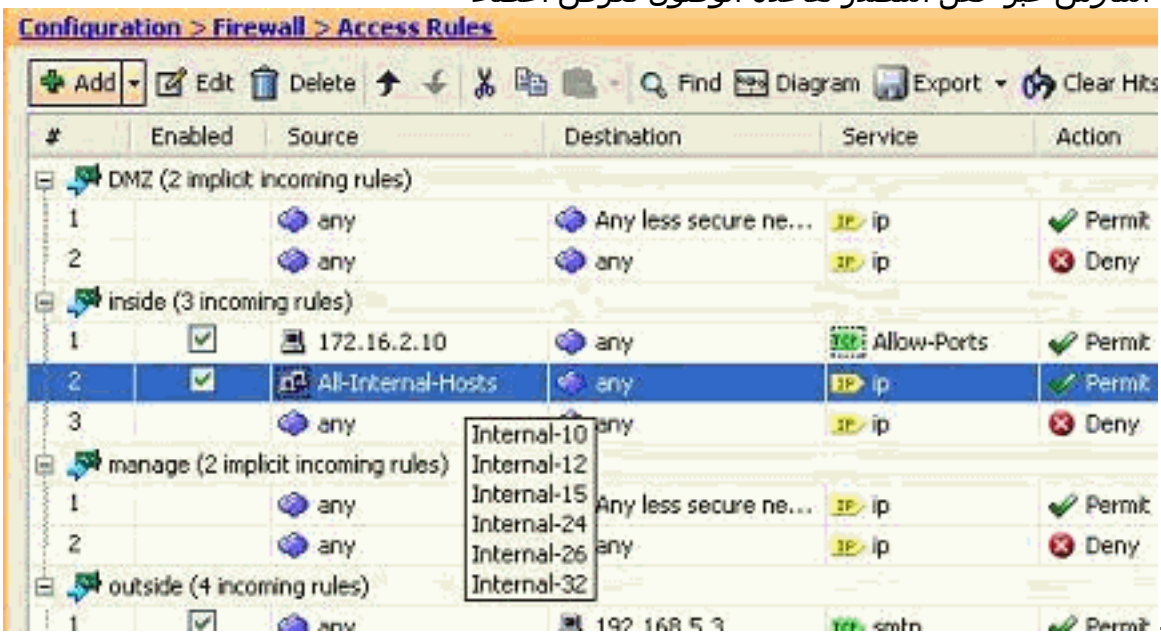
9. حدد مجموعة كائنات الشبكة **لكل البيئات المضيفة الداخلية**، وانقر فوق الزر



موافق.



10. وانقر فوق **OK**.
11. قم بتحريك الماوس عبر حقل المصدر لقاعدة الوصول لعرض أعضاء

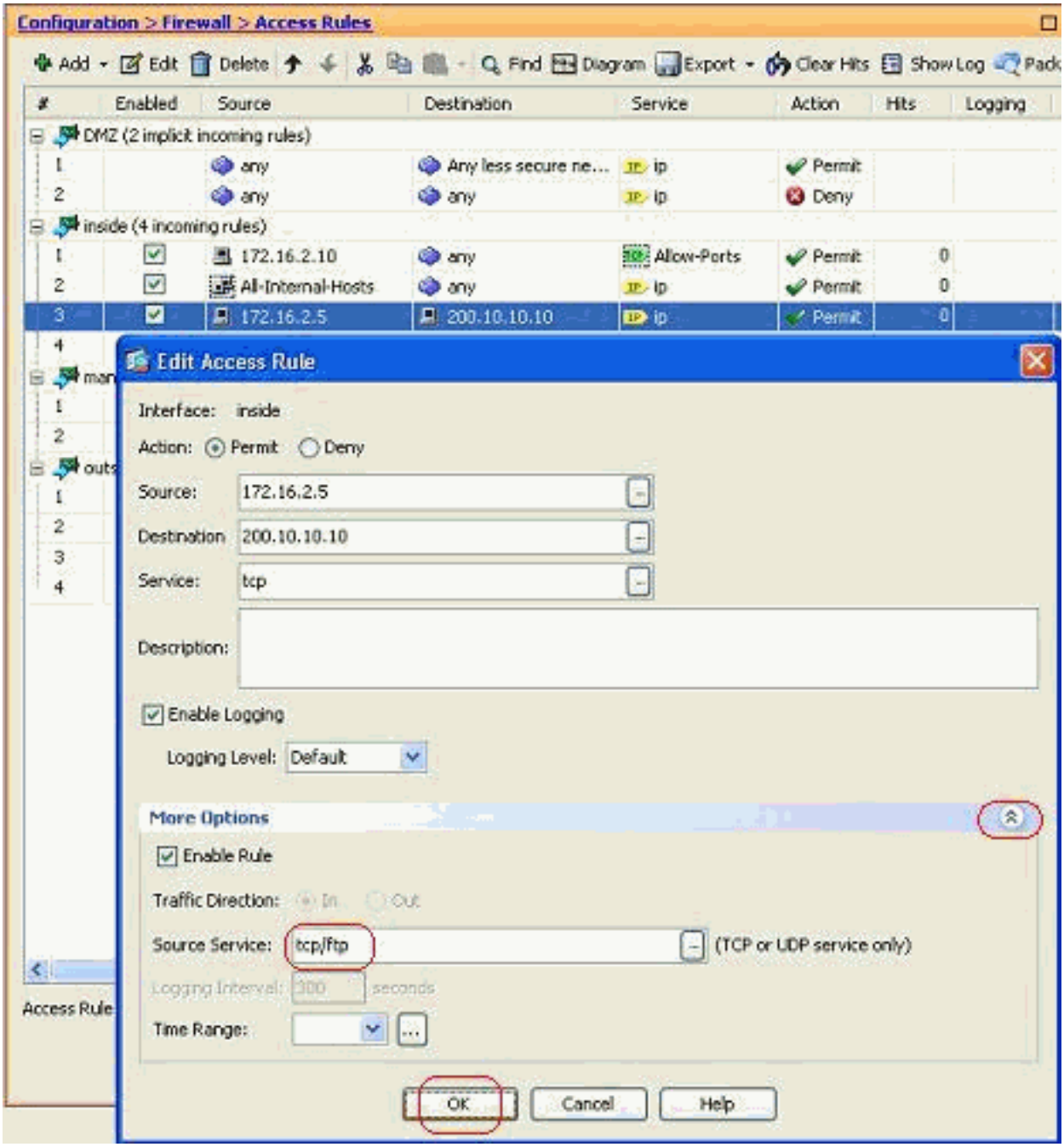


المجموعة.

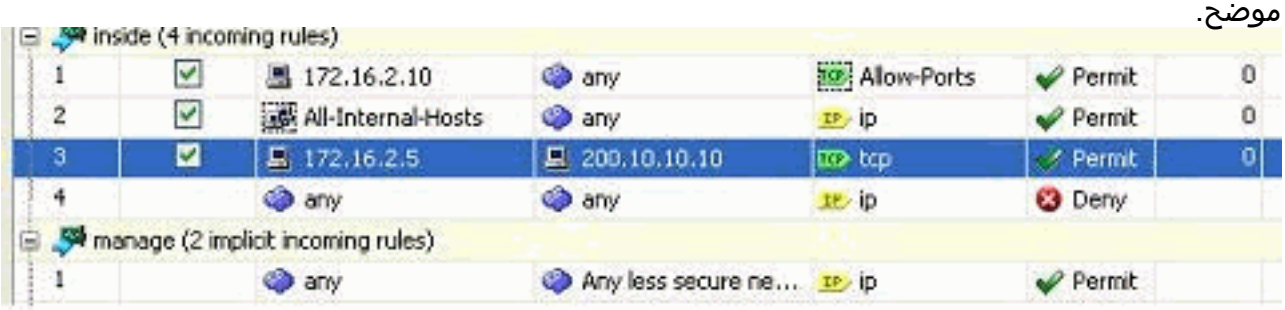
حرر المصدر ميناء:

أكمل هذه الخطوات لتعديل منفذ المصدر لقاعدة وصول.

1. لتعديل منفذ المصدر لقاعدة وصول موجودة، انقر بزر الماوس الأيمن عليه، واختر **تحرير**.تظهر نافذة تحرير قاعدة
الوصول.



2. انقر فوق الزر المنسدل **المزيد من الخيارات** لتعديل حقل "الخدمة المصدر"، ثم انقر فوق **موافق**.يمكنك عرض قاعدة الوصول المعدلة، كما هو موضح.

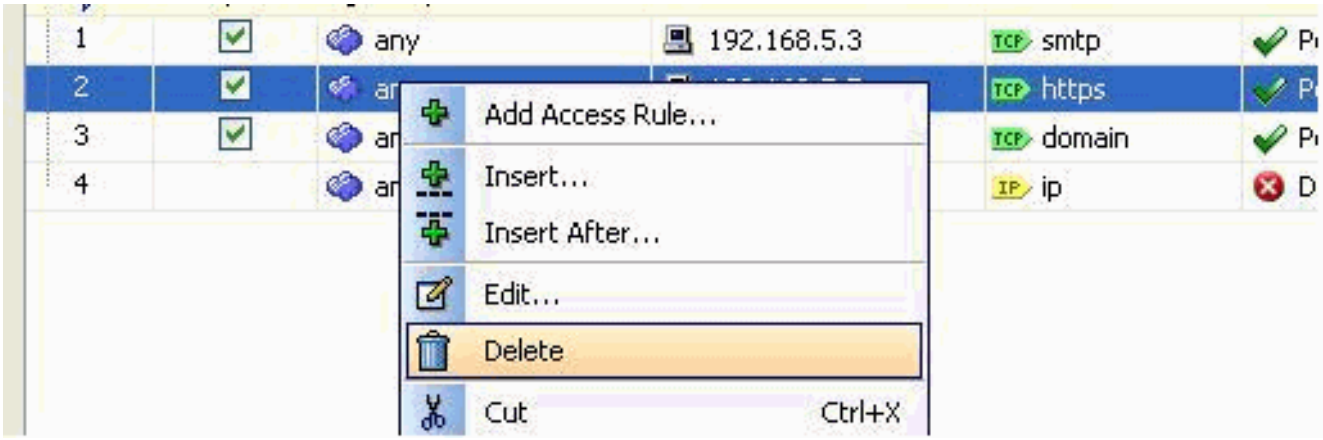


حذف قائمة الوصول

أكمل الخطوات التالية لحذف قائمة وصول:

1. قبل حذف قائمة وصول موجودة، يلزمك حذف إدخالات قائمة الوصول (قواعد الوصول). لا يمكن حذف قائمة الوصول ما لم تقم أولا بحذف جميع قواعد الوصول.انقر بزر الماوس الأيمن فوق قاعدة الوصول المراد حذفها،

واختر
حذف.



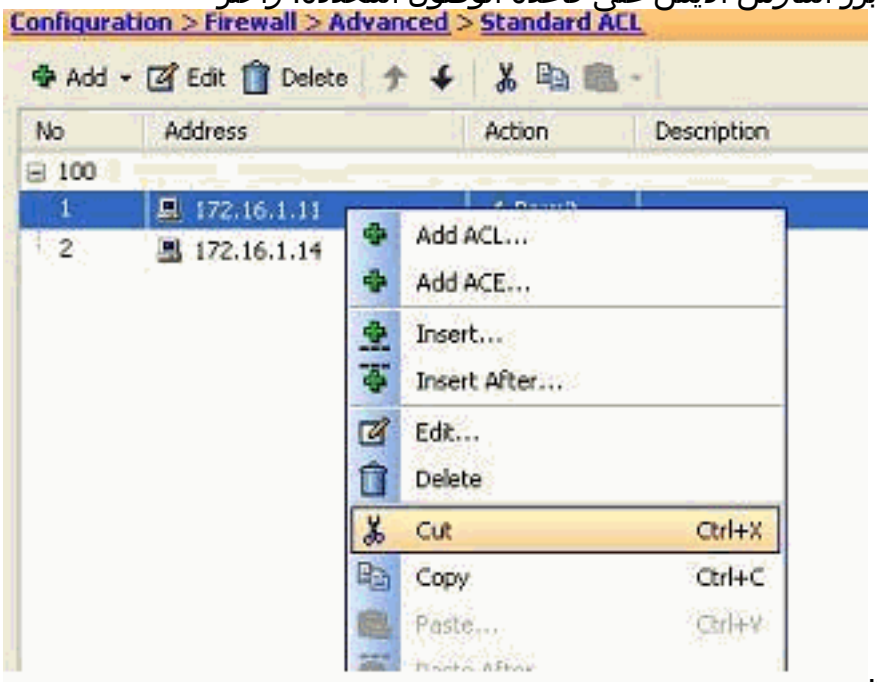
2. أكمل عملية الحذف نفسها على كافة قواعد الوصول الموجودة، ثم حدد قائمة الوصول واختر **حذف** لحذفها.

تصدير قاعدة الوصول

تقوم قواعد الوصول إلى ASDM بربط قائمة الوصول بالواجهة المقابلة بينما يقوم مدير قائمة التحكم في الوصول (ACL) بتعقب جميع قوائم الوصول الموسعة. لا ترتبط قواعد الوصول التي تم إنشاؤها باستخدام إدارة قائمة التحكم في الوصول (ACL) بأي واجهة. يتم إستخدام قوائم الوصول هذه بشكل عام بغرض اعفاء NAT و VPN-Filter والوظائف الأخرى المماثلة في حال عدم وجود اقتران مع الواجهة. يحتوي مدير قائمة التحكم في الوصول (ACL) على جميع الإدخالات الموجودة في قسم **التكوين > جدار الحماية > قواعد الوصول**. بالإضافة إلى ذلك، تحتوي **إدارة قائمة التحكم في الوصول (ACL)** أيضا على قواعد الوصول العالمية غير المقترنة بأي واجهة. يتم تنظيم ASDM بطريقة يمكنك من خلالها تصدير قاعدة وصول من أي قائمة وصول إلى أخرى بسهولة.

على سبيل المثال، إذا كنت بحاجة إلى قاعدة وصول تكون بالفعل جزءا من قاعدة وصول عمومية ليتم ربطها بواجهة، فأنت لا تحتاج إلى تكوينها مرة أخرى. وبدلا من ذلك، يمكنك تنفيذ عملية **قص ولصق** لتحقيق ذلك.

1. انقر بزر الماوس الأيمن على قاعدة الوصول المحددة، واختر
قص.



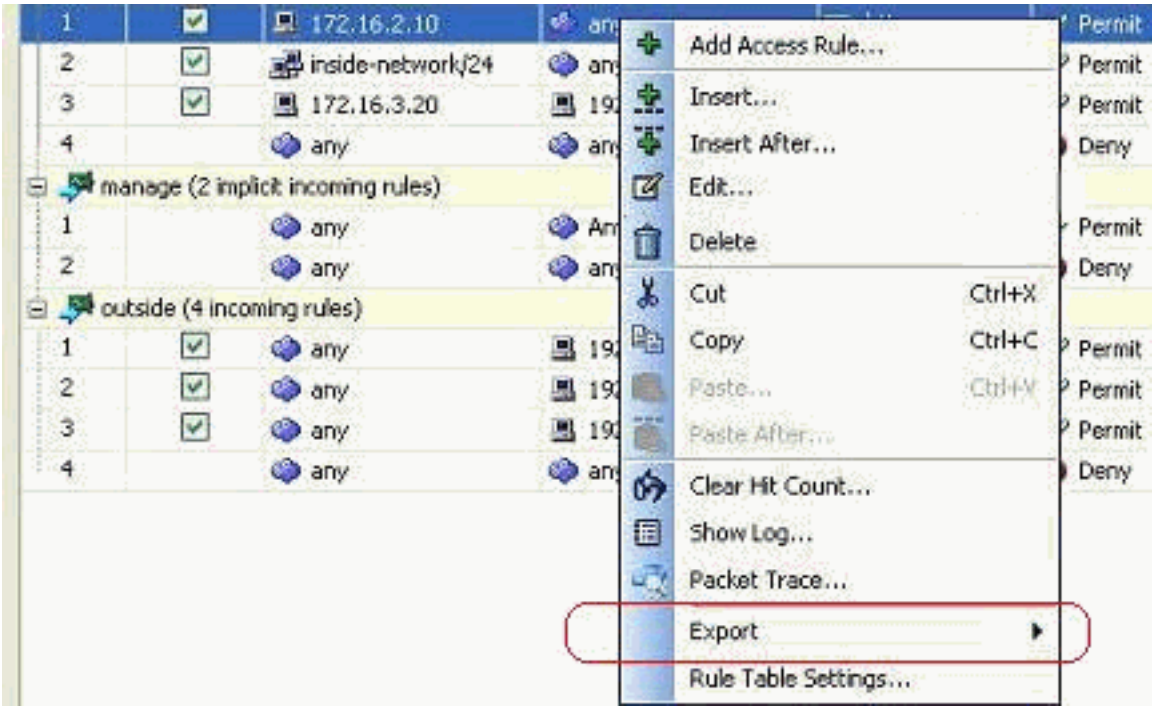
2. حدد قائمة الوصول المطلوبة التي تحتاج إلى إدراج قاعدة الوصول هذه فيها. يمكنك إستخدام **اللصق** في شريط الأدوات لإدراج قاعدة الوصول.

تصدير معلومات قائمة الوصول

يمكنك تصدير معلومات قائمة الوصول إلى ملف آخر. تم دعم تنسيقين لتصدير هذه المعلومات.

1. تنسيق القيمة المفصولة بفاصلة (CSV)
2. تنسيق HTML

انقر بزر الماوس الأيمن فوق أي من قواعد الوصول، واختر **تصدير** لإرسال معلومات قائمة الوصول إلى ملف.



فيما يلي معلومات قائمة الوصول الموضحة بتنسيق HTML.

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
DMZ (2 incoming rules)									
1	True	172.16.1.10	any	ip	Permit		Default		
2		any	any	ip	Deny		Default		Implicit rule
inside (3 incoming rules)									
1	True	172.16.2.10	any	Allow-Ports	Permit	0	Default		
2	True	All-Internal-Hosts	any	ip	Permit	0	Default		
3		any	any	ip	Deny		Default		Implicit rule
manage (2 implicit incoming rules)									
1		any	Any less secure networks	ip	Permit		Default		Implicit rule: Permit all traffic to less secure networks
2		any	any	ip	Deny		Default		Implicit rule
outside (4 incoming rules)									
1	True	any	192.168.5.3	tcp/smtp	Permit	0	Default		
2	True	any	192.168.5.5	tcp/https	Permit	0	Default		
3	True	any	192.168.5.4	tcp/domain	Permit	0	Default		
4		any	any	ip	Deny		Default		Implicit rule

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- أدلة أستكشاف المشكلات وإصلاحها
- أمثلة تكوين ASA والملاحظات التقنية
- 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).