مجموعات تفويض أوامر ACS Shell على مثال تكوين IOS و ASA/PIX/FWSM

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين مجموعات تفويض طبقة الأمان في خادم التحكم في الوصول الآمن (ACS) من Cisco لعملاء AAA، مثل موجهات أو محولات Cisco IOS® وأجهزة الأمان من Cisco (ASA/PIX/FWSM) باستخدام TACACS+ كبروتوكول التفويض.

ملاحظة: لا يدعم ACS Express تفويض الأوامر.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أنه قد تم تعيين التكوينات الأساسية في كل من عملاء AAA و ACS.

في ACS، أختر **تكوين الواجهة > الخيارات المتقدمة**، وتأكد أن خانة الاختيار **سمات TACACS+/RADIUS لكل مستخدم** محددة.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى خادم التحكم في الوصول الآمن (ACS) من Cisco الذي يشغل الإصدار 3.3 من البرنامج والإصدارات الأحدث.

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.

مجموعات تفويض الأوامر

توفر مجموعات تفويض الأوامر آلية مركزية للتحكم في تفويض كل أمر يتم إصداره على أي جهاز شبكة معين. تعزز هذه الميزة إلى حد كبير قابلية التطوير والإدارة المطلوبة لتعيين قيود التفويض.

في ACS، تتضمن مجموعات تفويض الأوامر الافتراضية مجموعات تفويض أوامر Shell ومجموعات تفويض أوامر PIX. يمكن لتطبيقات إدارة أجهزة Cisco، مثل مركز إدارة CiscoWorks لجدران الحماية، توجيه ACS لدعم أنواع مجموعات تفويض الأوامر الإضافية.

ملاحظة: تتطلب مجموعات تفويض أوامر PIX أن يقوم طلب تفويض أوامر TACACS+ بتعريف الخدمة على أنها *pixshell*. تحقق من تنفيذ هذه الخدمة في إصدار PIX OS الذي تستخدمه جدران الحماية؛ وإذا لم يتم ذلك، أستخدم مجموعات "تفويض أوامر Shell" لتنفيذ تفويض الأوامر لأجهزة PIX. راجع تكوين مجموعة تفويض أوامر Shell لمجموعة مستخدمين للحصول على مزيد من المعلومات.

ملاحظة: لم يتم تنفيذ خدمة Pixshell حتى الإصدار 6.3 من PIX OS.

ملاحظة: لا تسمح أجهزة أمان Cisco (ASA/PIX) حاليا بوضع المستخدم مباشرة في وضع التمكين أثناء تسجيل الدخول. يجب أن يدخل المستخدم يدويا في وضع التمكين.

ولتوفير مزيد من التحكم في جلسات عمل برنامج Telnet الإدارية المستضافة من قبل الجهاز، يمكن لجهاز الشبكة الذي يستخدم TACACS+ طلب التفويض لكل سطر أوامر قبل تنفيذه. يمكنك تحديد مجموعة من الأوامر المسموح بها أو المرفوضة للتنفيذ بواسطة مستخدم معين على جهاز معين. عزز ACS هذه الإمكانية أكثر مع هذه الخصائص:

- **مجموعات تفويض الأوامر المسماة التي يمكن إعادة إستخدامها**— دون الإشارة مباشرة إلى أي مستخدم أو مجموعة مستخدمين، يمكنك إنشاء مجموعة مسماة من تراخيص الأوامر. يمكنك تعريف العديد من مجموعات تفويض الأوامر التي تحدد ملفات تخصيص وصول مختلفة. على سبيل المثال:يمكن أن تسمح مجموعة تفويض أوامر *مكتب المساعدة* بالوصول إلى أوامر الاستعراض عالية المستوى، مثل **show run**، ورفض أي أوامر تكوين.يمكن أن تحتوي مجموعة تفويض أوامر *مهندسي الشبكة* على قائمة محدودة من الأوامر المسموح بها لأي مهندس شبكة في المؤسسة.يمكن أن تسمح مجموعة تفويض أوامر *مهندسي الشبكة المحلية* لجميع الأوامر (تتضمن أوامر تكوين عنوان IP).
- **تحبب التكوين الدقيق**—يمكنك إنشاء اقترانات بين مجموعات تفويض الأوامر المسماة ومجموعات أجهزة الشبكة (NDGs). وبالتالي، يمكنك تحديد توصيفات وصول مختلفة للمستخدمين حسب أجهزة الشبكة التي يمكنهم الوصول إليها. يمكنك إقران مجموعة تفويض الأوامر المسماة نفسها بأكثر من NDG واستخدامها لأكثر من مجموعة مستخدمين واحدة. يعمل مصدر المحتوى الإضافي على تعزيز تكامل البيانات. يتم الاحتفاظ بمجموعات تخويل الأوامر المسماة في قاعدة البيانات الداخلية ل ACS. يمكنك إستخدام ميزات "النسخ الاحتياطي والاستعادة ل ACS" لإجراء نسخ إحتياطي لها واستعادتها. يمكنك أيضا نسخ مجموعات تفويض الأوامر إلى ACS

الثانوي مع بيانات التكوين الأخرى.
بالنسبة لأنواع مجموعة تفويض الأوامر التي تدعم تطبيقات إدارة أجهزة Cisco، تكون الميزات متشابهة عند إستخدام مجموعات تفويض الأوامر. يمكنك تطبيق مجموعات تخويل الأوامر على مجموعات ACS التي تحتوي على مستخدمين لتطبيق إدارة الأجهزة لفرض التخويل الخاص بامتيازات مختلفة في تطبيق إدارة الأجهزة. يمكن أن تتطابق مجموعات ACS مع أدوار مختلفة داخل تطبيق إدارة الأجهزة، ويمكنك تطبيق مجموعات تفويض أوامر مختلفة على كل مجموعة، حسب ما هو قابل للتطبيق.

يحتوي ACS على ثلاث مراحل متتالية لتصفية تفويض الأوامر. يتم تقييم كل طلب تفويض أوامر بالترتيب الوارد في القائمة:

1. **مطابقة الأوامر** — يحدد ACS ما إذا كان الأمر الذي تتم معالجته يطابق أمرا مدرجا في مجموعة تفويض الأوامر. إذا لم تتم مطابقة الأمر، يتم تحديد تفويض الأوامر من خلال إعداد أوامر غير متطابقة: *السماح* أو *الرفض*. وإلا، إذا تمت مطابقة الأمر، يستمر التقييم.
2. **مطابقة الوسيطة** — يحدد ACS ما إذا كانت وسيطات الأمر المعروضة تطابق وسيطات الأمر المدرجة في مجموعة تفويض الأوامر.إذا لم تتطابق أي وسيطة، يتم تحديد تفويض الأوامر من خلال تمكين خيار السماح بالوسائط غير المتطابقة. إذا كان مسموحا بالحجج غير المتطابقة، يتم تخويل الأمر وينتهي التقييم، وإلا، فإن الأمر غير مصرح به وينتهي التقييم.وفي حالة تطابق جميع الحجج، يستمر التقييم.
3. **نهج الوسيطة**—بمجرد أن يحدد ACS أن الوسيطات الموجودة في الأمر تطابق الوسيطات الموجودة في مجموعة تفويض الأوامر، يحدد ACS ما إذا كان كل وسيطة أمر مسموح بها بشكل صريح أم لا. إذا تم السماح بشكل صريح بجميع الوسيطات، فإن ACS يمنح تفويض الأوامر. إذا لم يكن مسموحا بأية وسيطات، يرفض ACS تفويض الأوامر.

إضافة مجموعة تخويل أمر Shell

يتضمن هذا القسم السيناريوهات التي تصف كيفية إضافة مجموعة تفويض أوامر:

- السيناريو 1: امتياز الوصول للقراءة والكتابة أو الوصول الكامل
- السيناريو 2: امتياز الوصول للقراءة فقط
- السيناريو 3: امتياز الوصول المقيد

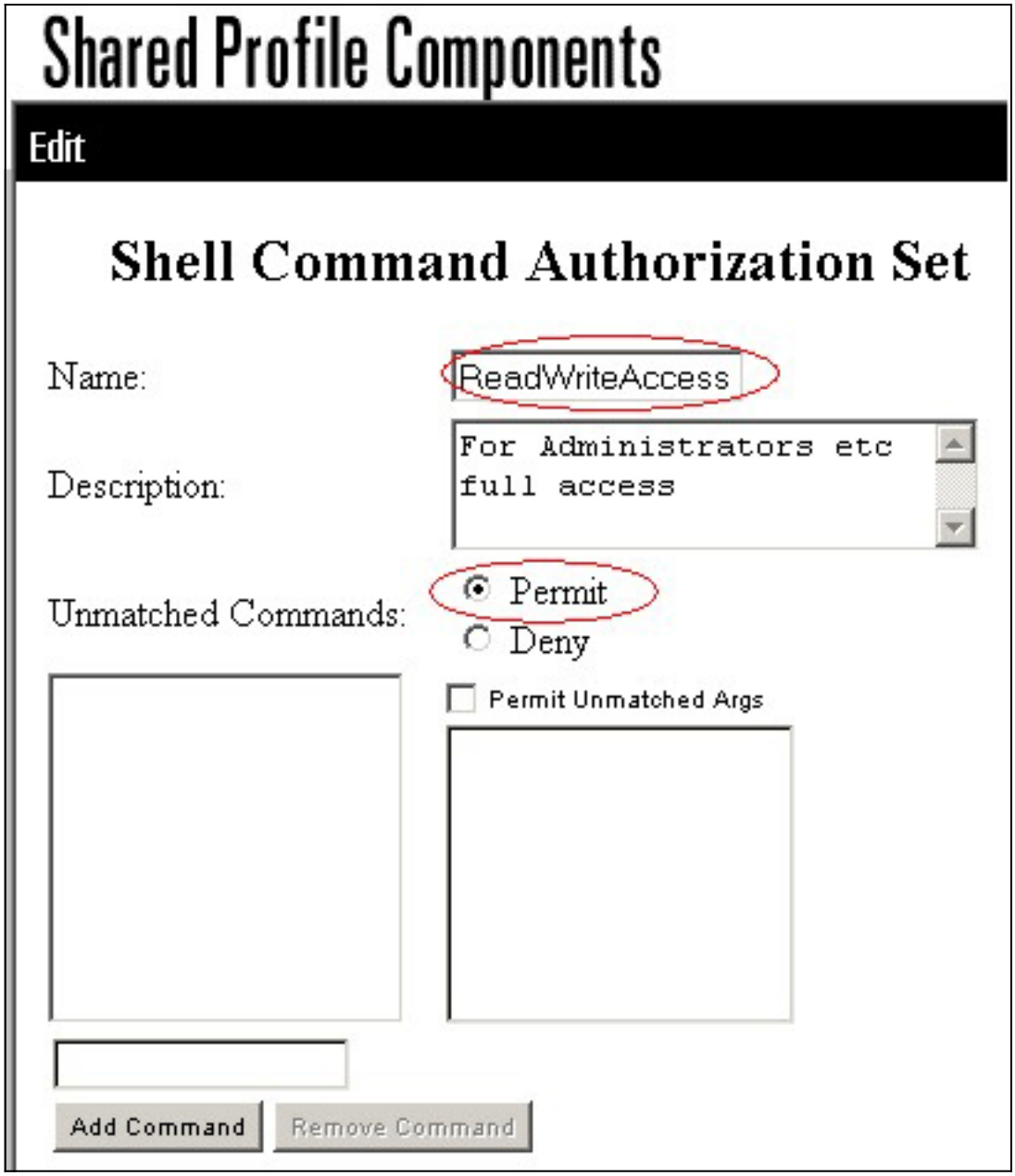
ملاحظة: راجع قسم إضافة مجموعة تفويض الأوامر" في دليل المستخدم ل Cisco Secure Access Control Server 4.1 للحصول على مزيد من المعلومات حول كيفية إنشاء مجموعات تفويض الأوامر. ارجع إلى تحرير مجموعة تفويض الأوامر وحذف مجموعة تفويض الأوامر للحصول على مزيد من المعلومات حول كيفية تحرير مجموعات تفويض الأوامر وحذفها.

السيناريو 1: امتياز الوصول للقراءة والكتابة أو الوصول الكامل

في هذه السيناريوهات، يتم منح المستخدمين حق الوصول للقراءة والكتابة (أو بالكامل).

في منطقة مجموعة تخويل أمر الهيكل من نافذة مكونات التوصيف المشترك، قم بتكوين الإعدادات التالية:

1. في حقل "الاسم"، أدخل **ReadWriteAccess** كاسم مجموعة تفويض الأوامر.
2. في حقل الوصف، أدخل وصفا لمجموعة تفويض الأوامر.
3. انقر زر **السماح** للراديو، ثم انقر **تسليم**.

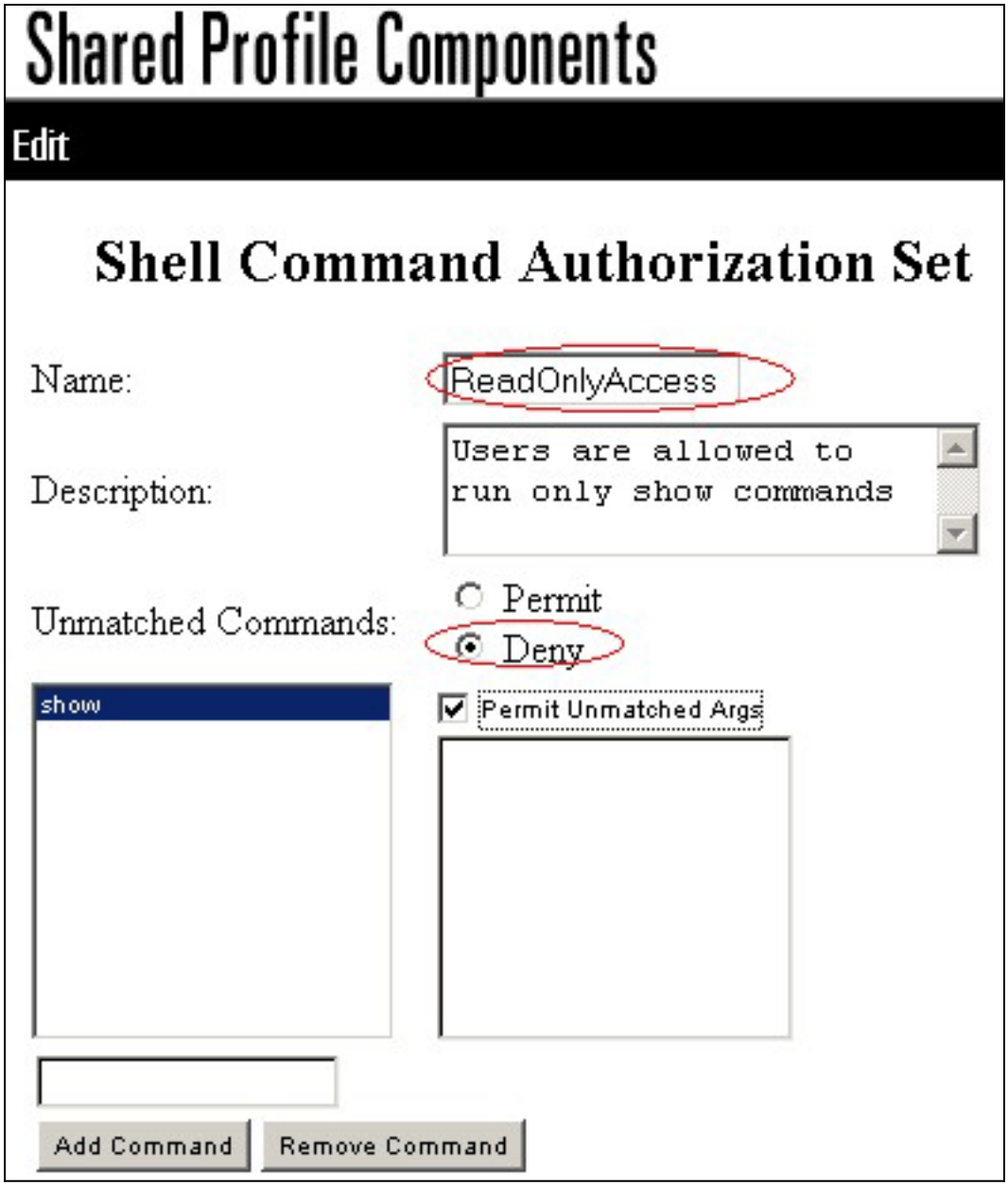


السيناريو 2: امتياز الوصول للقراءة فقط

في هذه السيناريوهات، يمكن للمستخدمين إستخدام أوامر **show** فقط.

في منطقة مجموعة تخويل أمر الهيكل من نافذة مكونات التوصيف المشترك، قم بتكوين الإعدادات التالية:

1. في حقل "الاسم"، أدخل **ReadOnlyAccess** كاسم لمجموعة تفويض الأوامر.
2. في حقل الوصف، أدخل وصفا لمجموعة تفويض الأوامر.
3. انقر على زر **رفض** الراديو.
4. أدخل الأمر **show** في الحقل أعلى زر أمر الإضافة، ثم انقر **أمر إضافة**.
5. حدد خانة الاختيار **السماح للروابط غير المتطابقة**، وانقر **إرسال**.

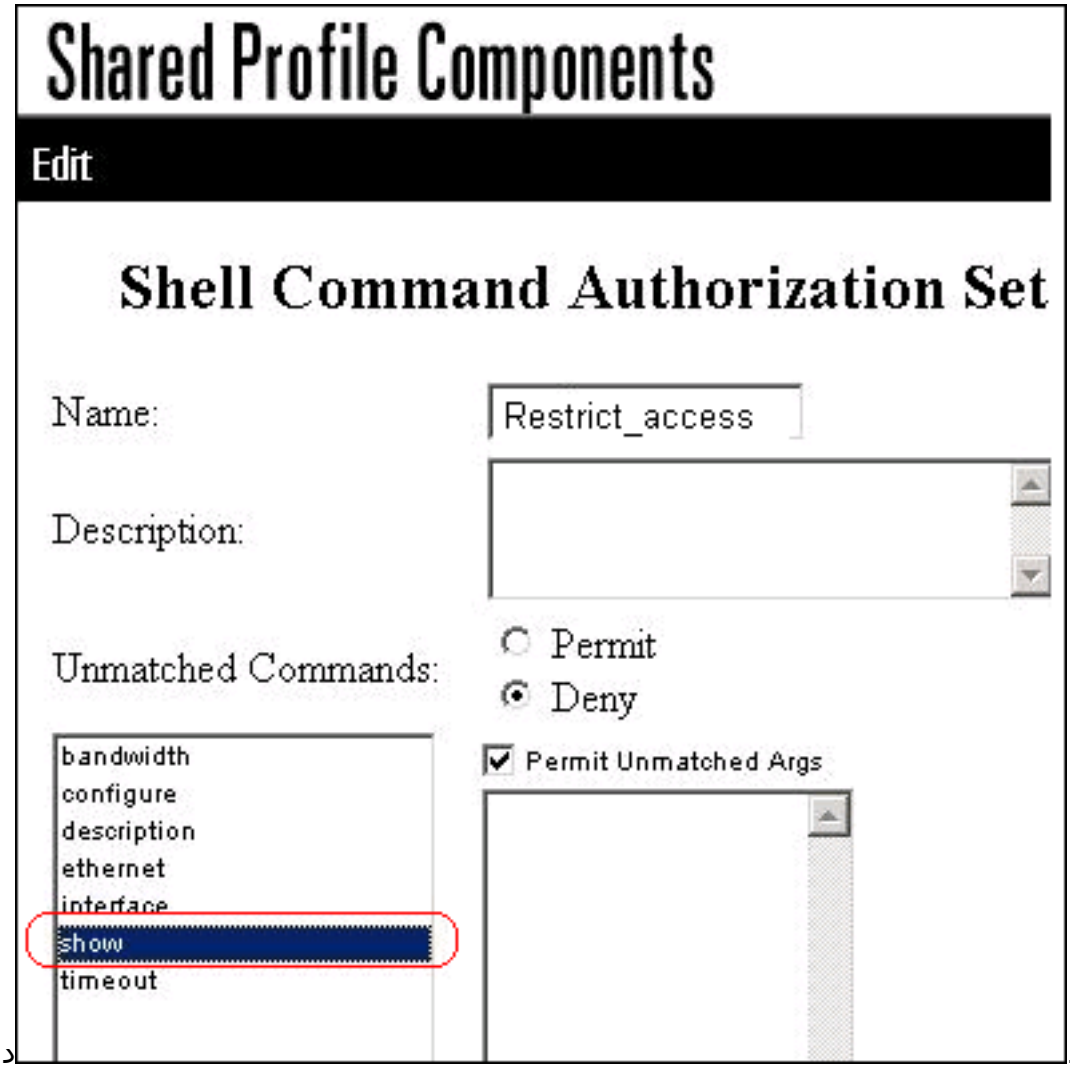


السيناريو 3: امتياز الوصول المقيد

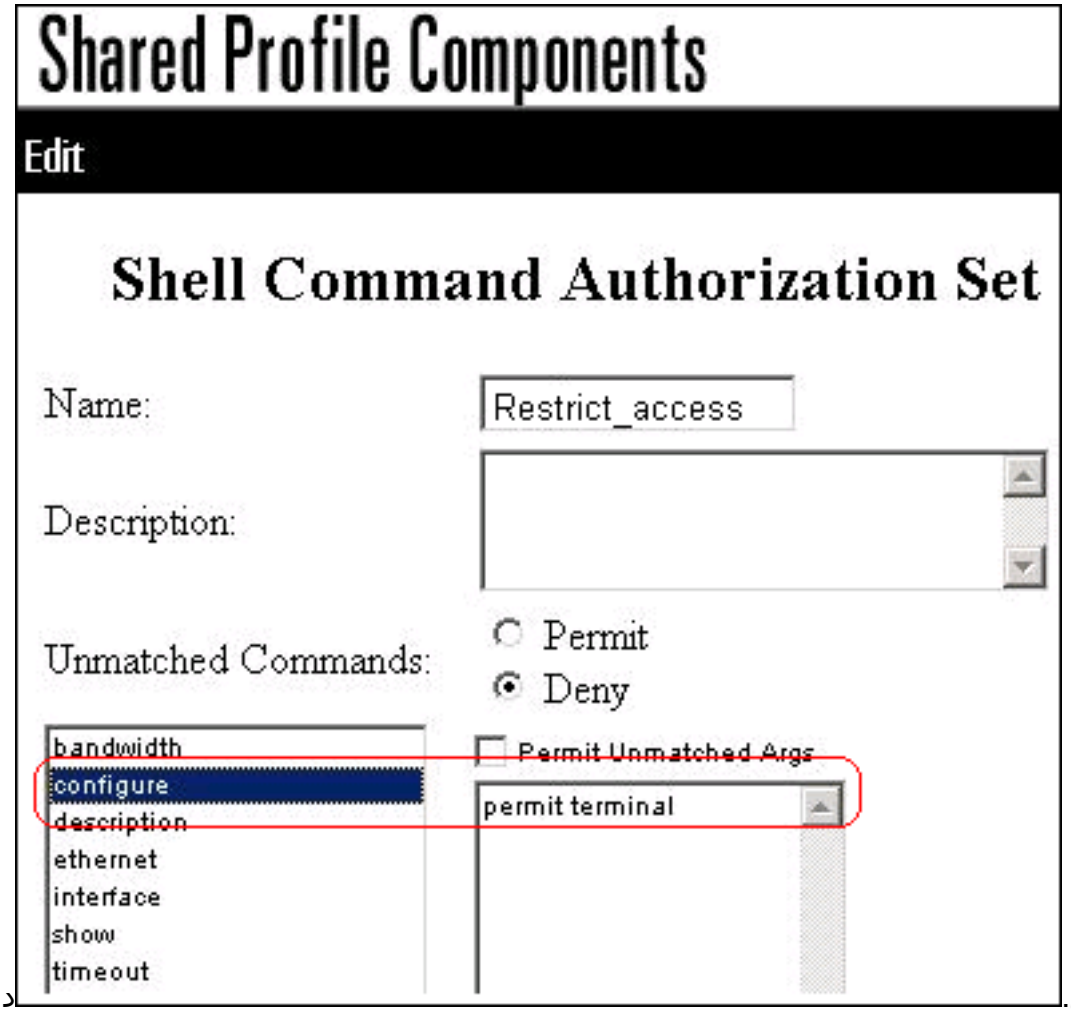
في هذا السيناريو، يمكن للمستخدمين إستخدام الأوامر الانتقائية.

في منطقة مجموعة تخويل أمر الهيكل من نافذة مكونات التوصيف المشترك، قم بتكوين الإعدادات التالية:

1. في حقل "الاسم"، أدخل **Restrict_access** كاسم لمجموعة تفويض الأوامر.
2. انقر على زر **رفض** الراديو.
3. أدخل الأوامر التي تريد السماح بها على عملاء AAA.في الحقل الموجود أعلى زر أمر الإضافة، أدخل الأمر **show**، وانقر **أمر**

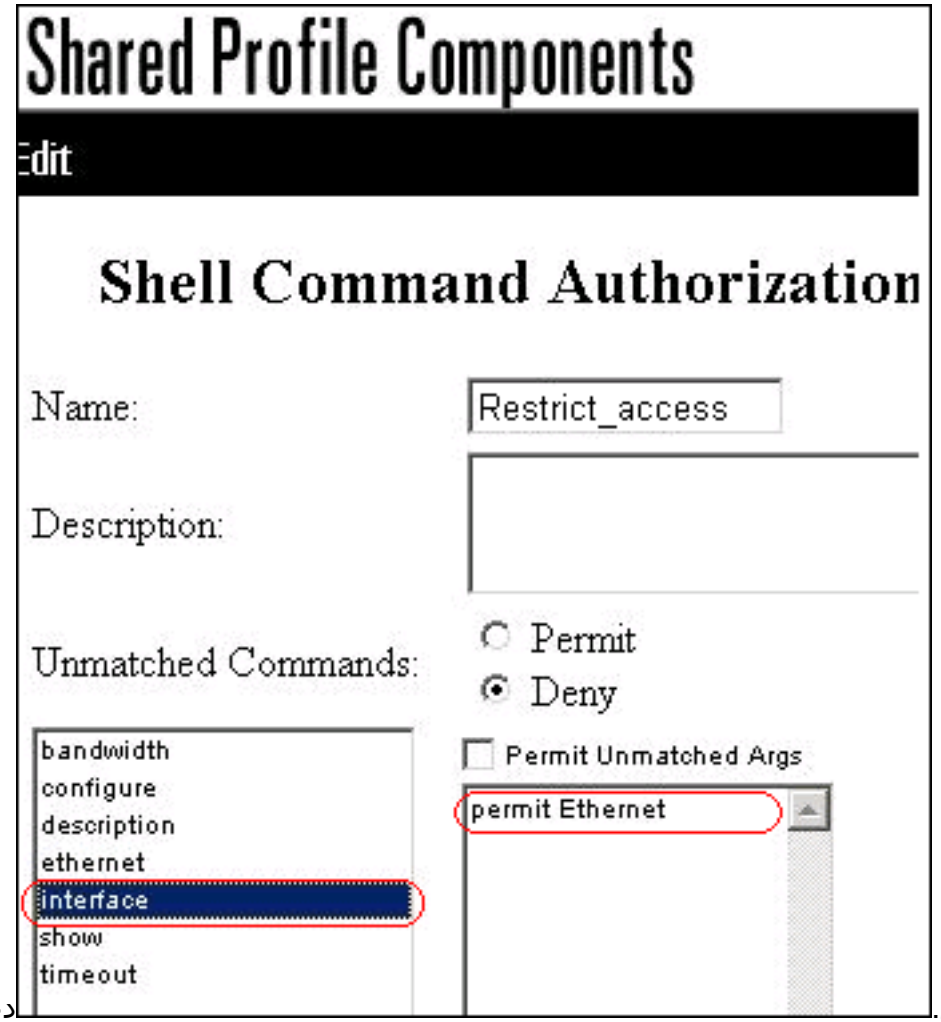


دخلت **ال** **إضافة**. configure أمر، وطقطقة **يضيف أمر**.حدد الأمر configure، وأدخل **وحدة السماح الطرفية** في الحقل إلى



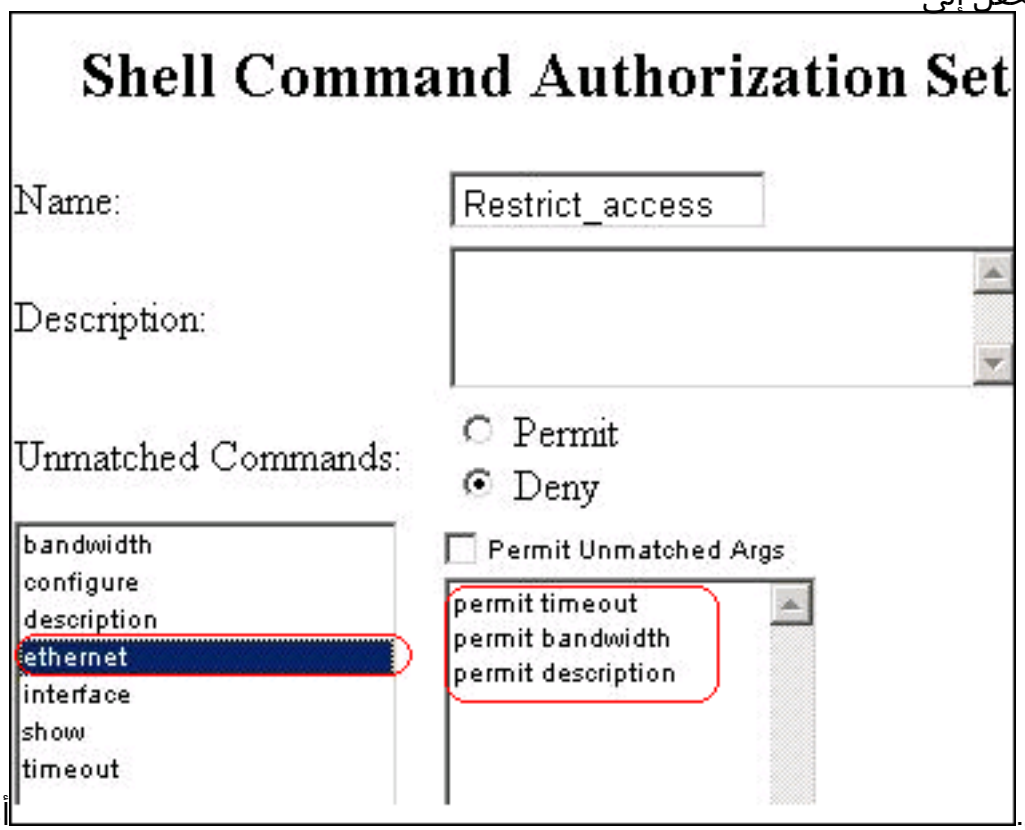
دخلت **القارن** اليمين.

أمر، وطقطقة **يضيف أمر**.حدد أمر **الواجهة**، وأدخل **السماح بالإيثرنت** في الحقل إلى



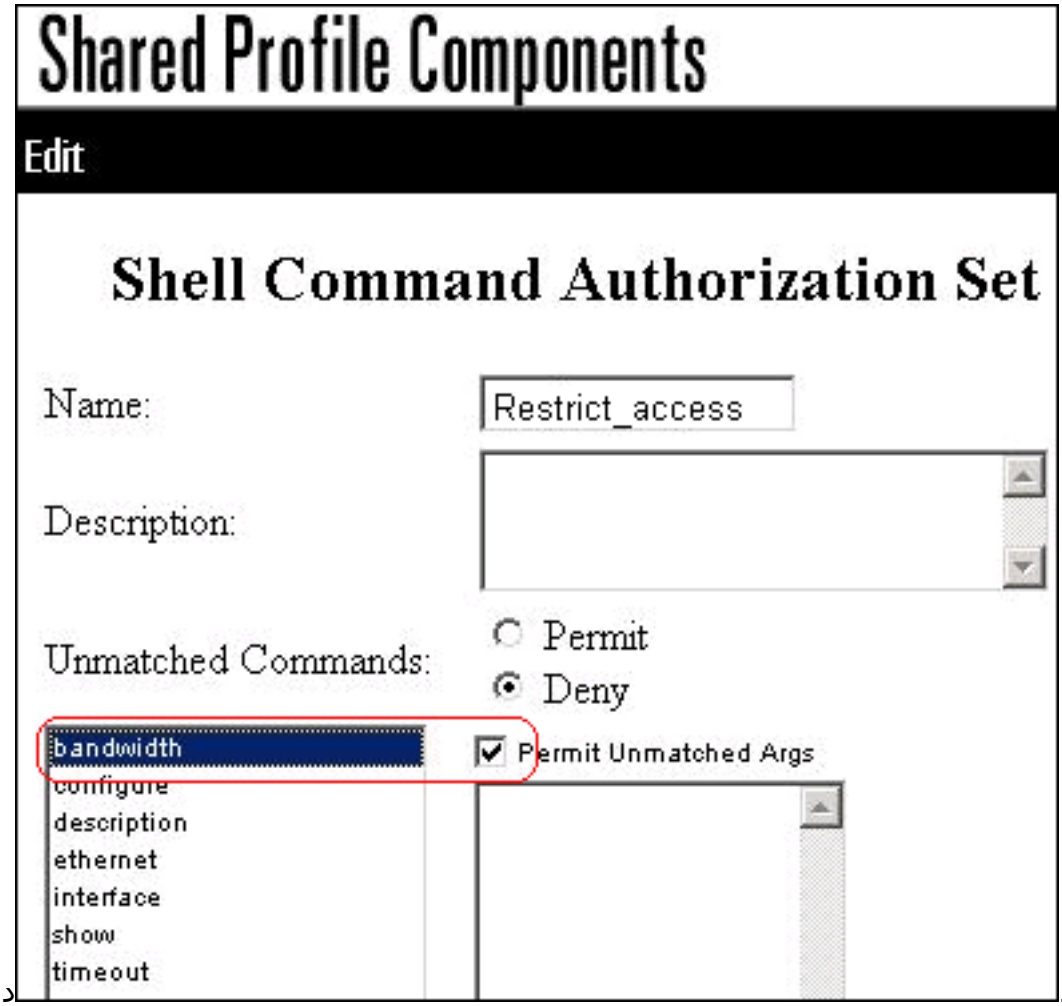
دخلت **الإثرنيت** أمر، اليمين.

وطقطقة **يضيف أمر**.حدد أمر **الواجهة**، وأدخل **مهلة السماح**، و**السماح بعرض النطاق الترددي**، و**وصف الترخيص** في الحقل إلى

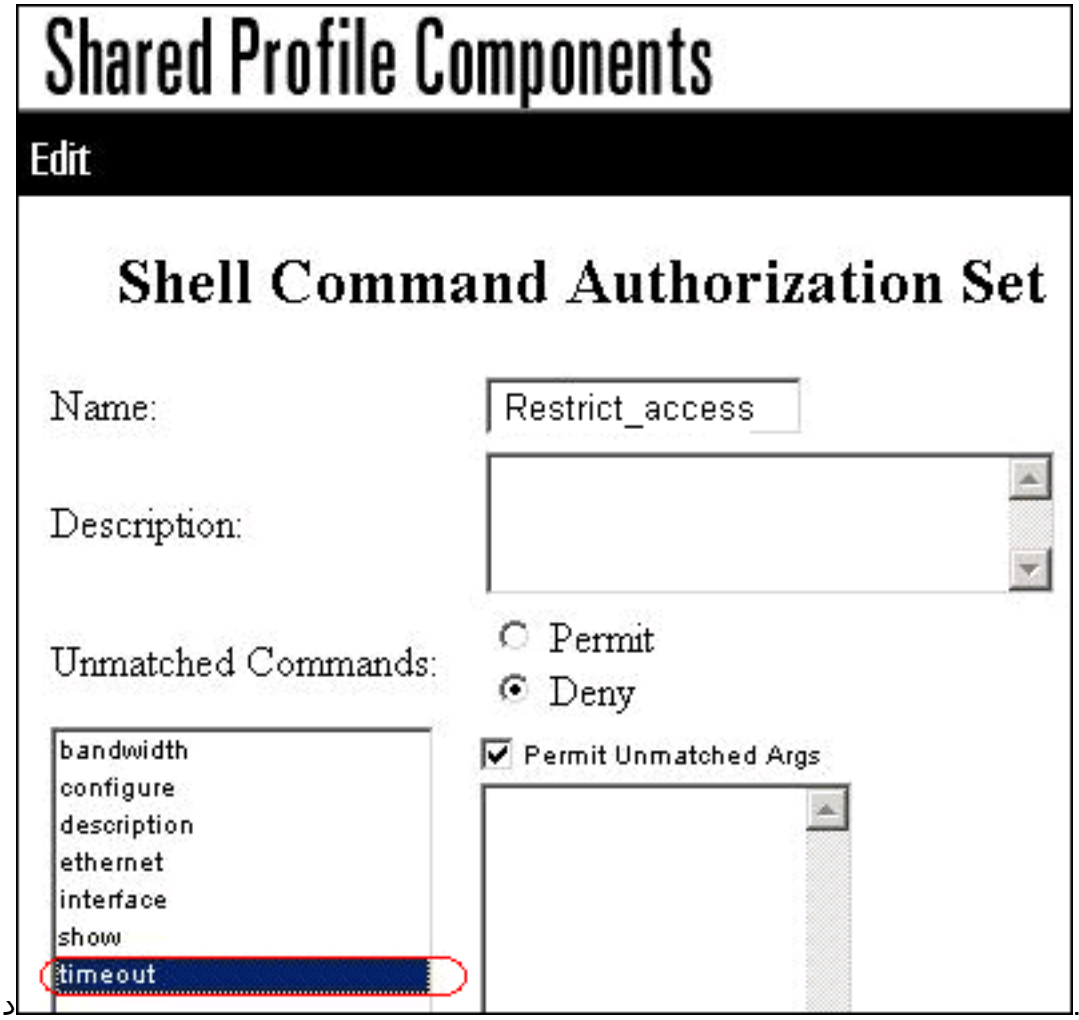


أدخل الأمر اليمين.

bandwidth، وانقر **فوق أمر**

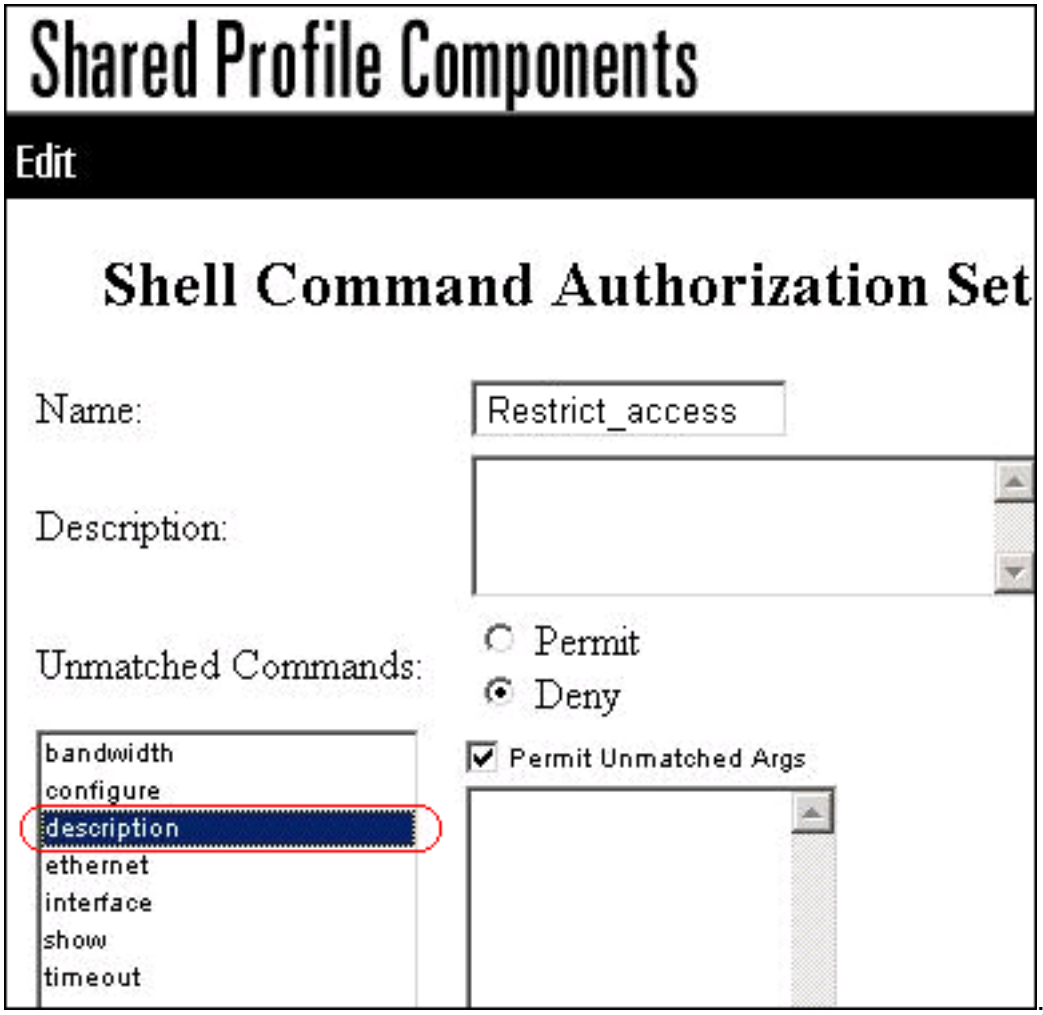


إضافة. دخلت **التعطيل** أمر، وطقطقة **يضيف**



أمر.

دخلت **الوصف** أمر، وطقطقة **يضيف**



أمر.

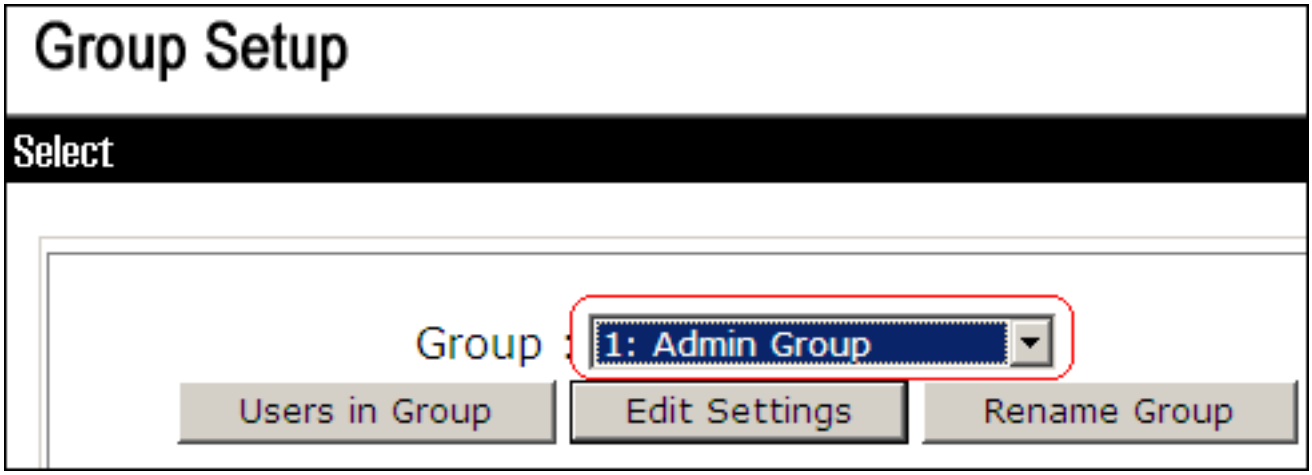
4. انقر على **إرسال**.

إقران مجموعة تفويض أمر Shell بمجموعة المستخدمين

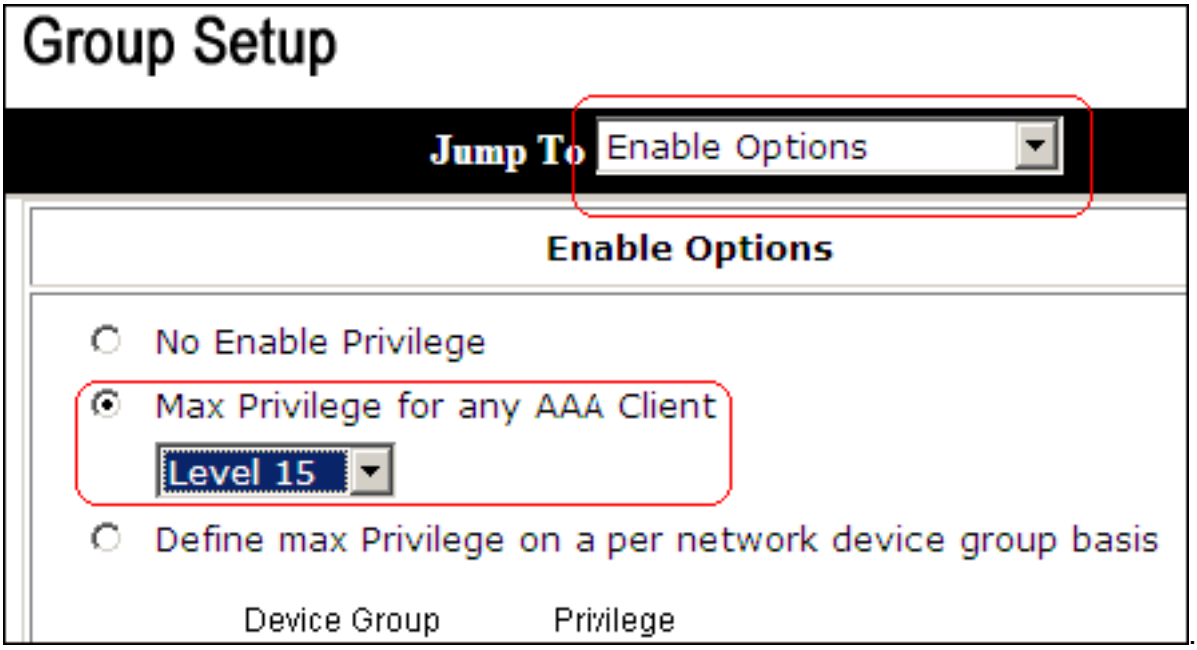
راجع قسم تكوين مجموعة تفويض أوامر Shell لمجموعة مستخدمين في دليل المستخدم لخادم التحكم في الوصول الآمن من Cisco 4.1 للحصول على مزيد من المعلومات حول كيفية تكوين تكوين مجموعة تفويض أوامر Shell لمجموعات المستخدمين.

إقران مجموعة تفويض أمر Shell (وصول ReadWrite) بمجموعة المستخدمين (مجموعة المسؤولين)

1. في نافذة ACS، انقر على **إعداد المجموعة**، واختر **مجموعة المسؤول** من القائمة المنسدلة للمجموعة.

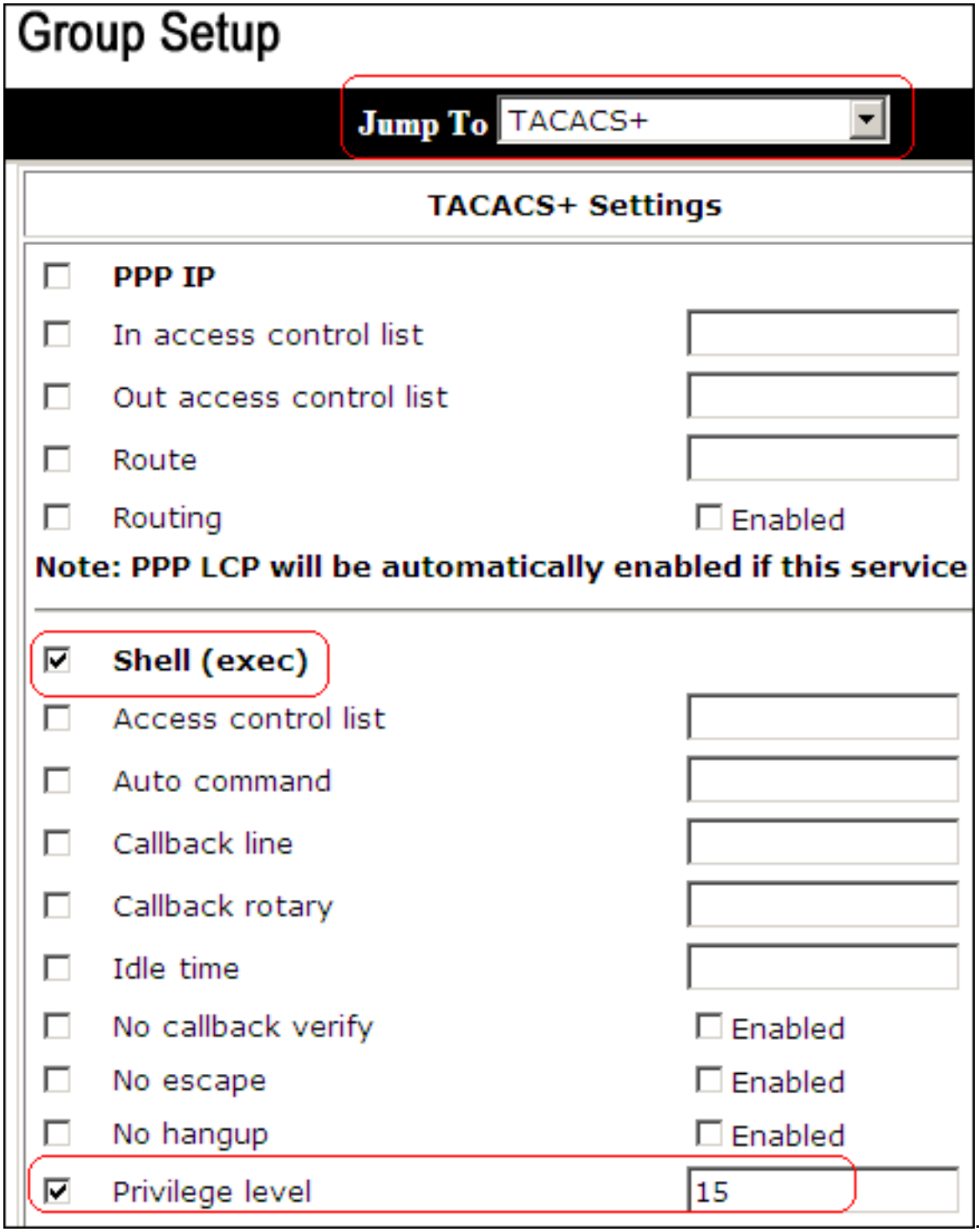


2. طقطقة **يحرر عملية إعداد**.
3. من القائمة المنسدلة قفز إلى، أختر **تمكين الخيارات**.
4. في منطقة "تمكين الخيارات"، انقر فوق **الحد الأقصى للامتياز لأي** زر راديو **عميل AAA**، واختر **المستوى 15** من القائمة



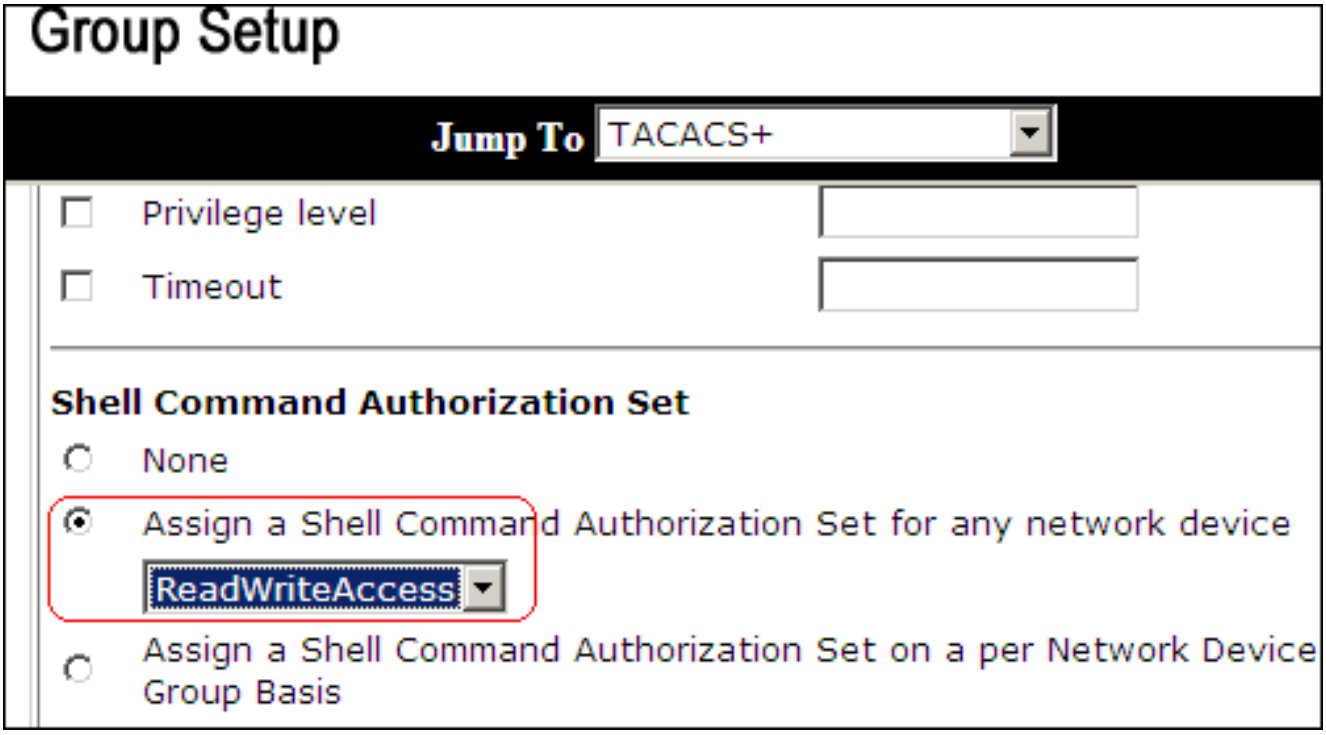
المنسدلة.

5. من القائمة الانتقال إلى القائمة المنسدلة، أختر **TACACS+**.
6. في منطقة إعدادات TACACS+، حدد خانة الاختيار **طبقة (exec)**، وحدد خانة الاختيار **مستوى الامتياز**، وأدخل **15** في حقل مستوى



الامتياز.

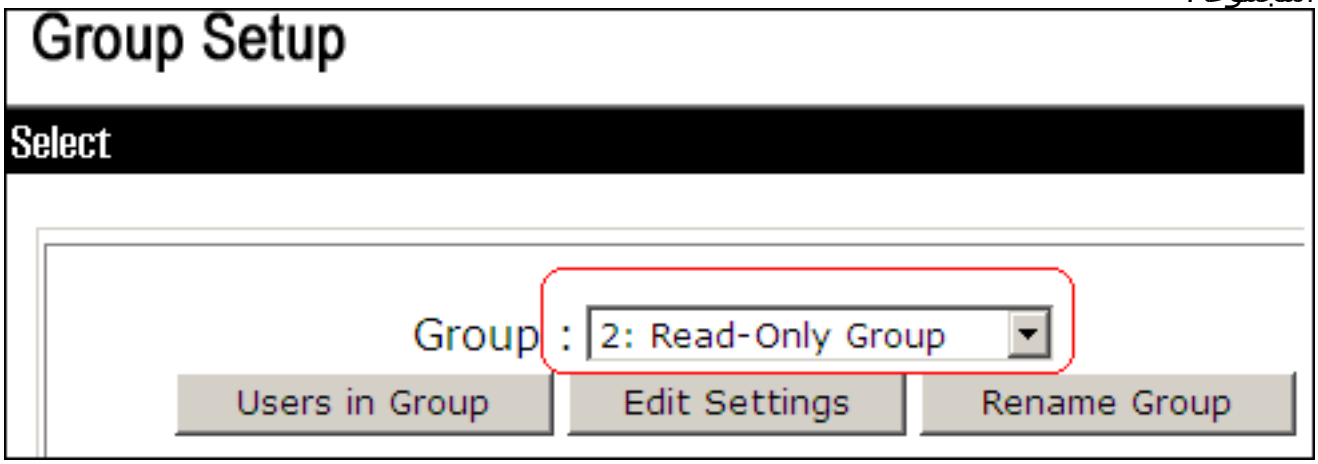
7. في منطقة مجموعة تفويض أوامر Shell، انقر فوق **مجموعة تفويض أوامر Shell لأي** زر لاسلكي **بجهاز الشبكة**، **واختر** ReadWriteAccess من القائمة المنسدلة.



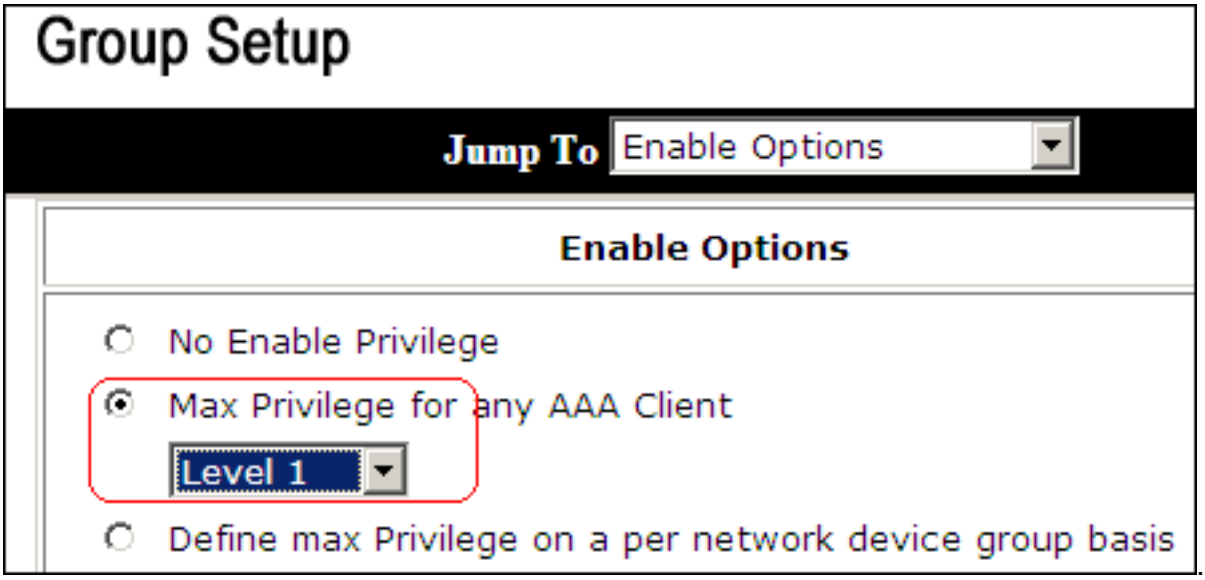
8. انقر على **إرسال**

إقران مجموعة تفويض أمر Shell (وصول ReadOnly) بمجموعة المستخدمين (مجموعة للقراءة فقط)

1. في نافذة ACS، انقر فوق **إعداد المجموعة**، واختر **مجموعة للقراءة فقط** من القائمة المنسدلة المجموعة.

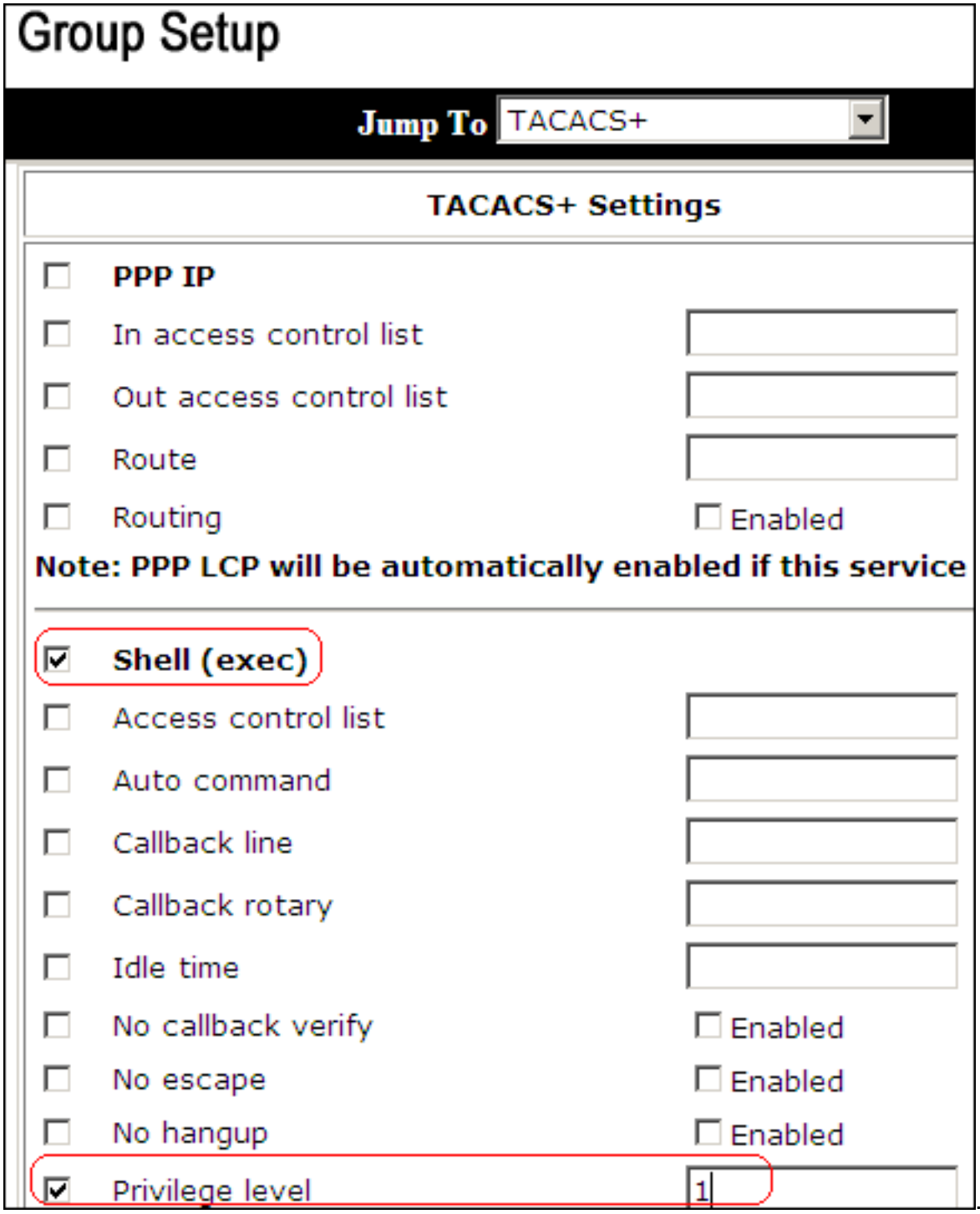


2. طقطقة **يحرر عملية إعداد**.
3. من القائمة المنسدلة قفز إلى، أختر **تمكين الخيارات**.
4. في منطقة "تمكين الخيارات"، انقر فوق **الحد الأقصى للامتياز لأي** زر راديو **عميل AAA**، واختر **المستوى 1** من القائمة



المنسدلة.

5. في منطقة إعدادات TACACS+، حدد خانة الاختيار **طبقة (exec)**، وحدد خانة الاختيار **مستوى الامتياز**، وأدخل 1 في حقل مستوى



الامتياز.

6. في منطقة "مجموعة تفويض أوامر Shell"، انقر فوق **مجموعة تفويض أوامر Shell لأي** زر لاسلكي **بجهاز الشبكة**، واختر **ReadOnlyAccess** من القائمة

المنسدلة.

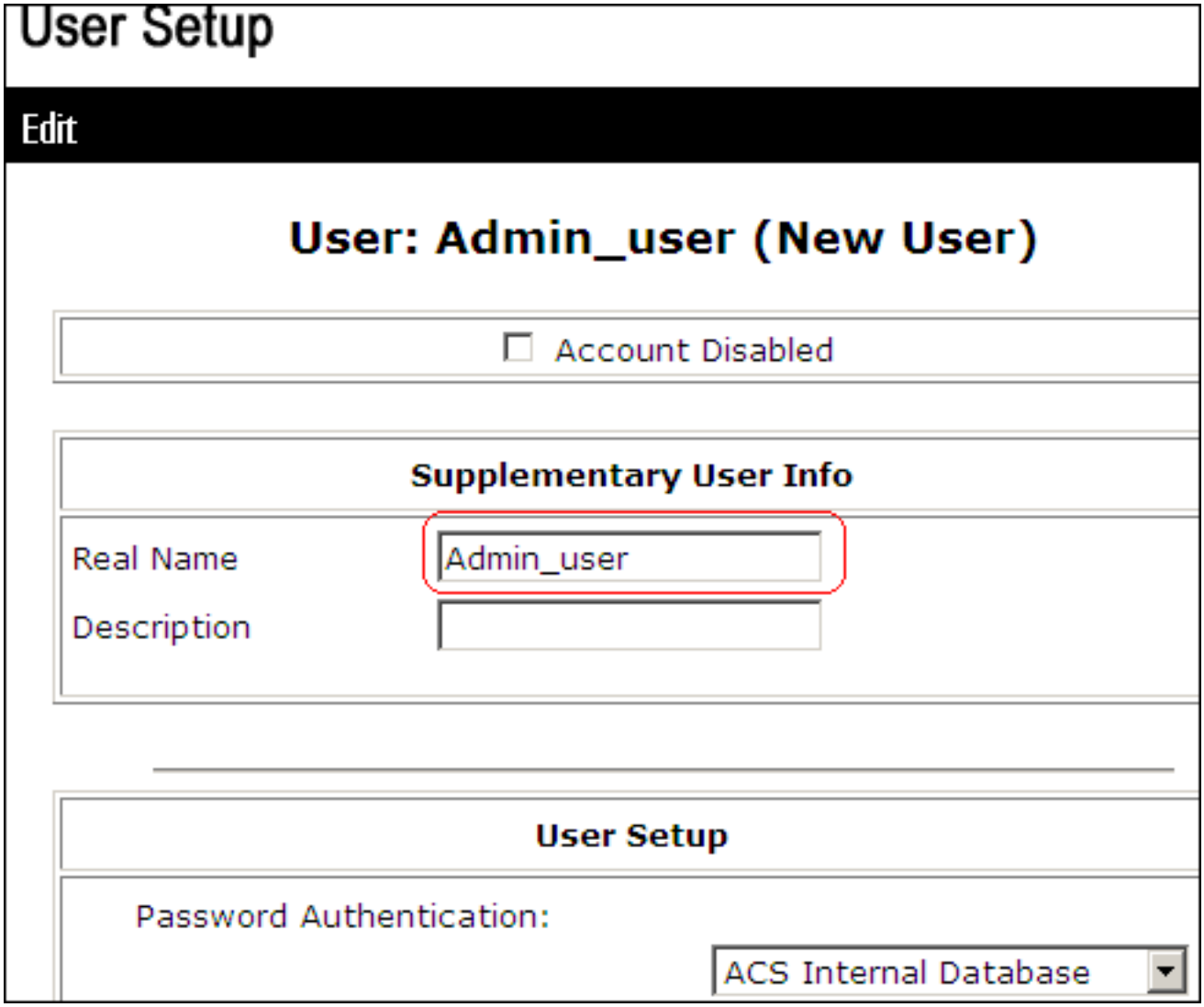
7. انقر على **إرسال**

إقران مجموعة تفويض أمر Shell (RESTRICT_ACCESS) بالمستخدم

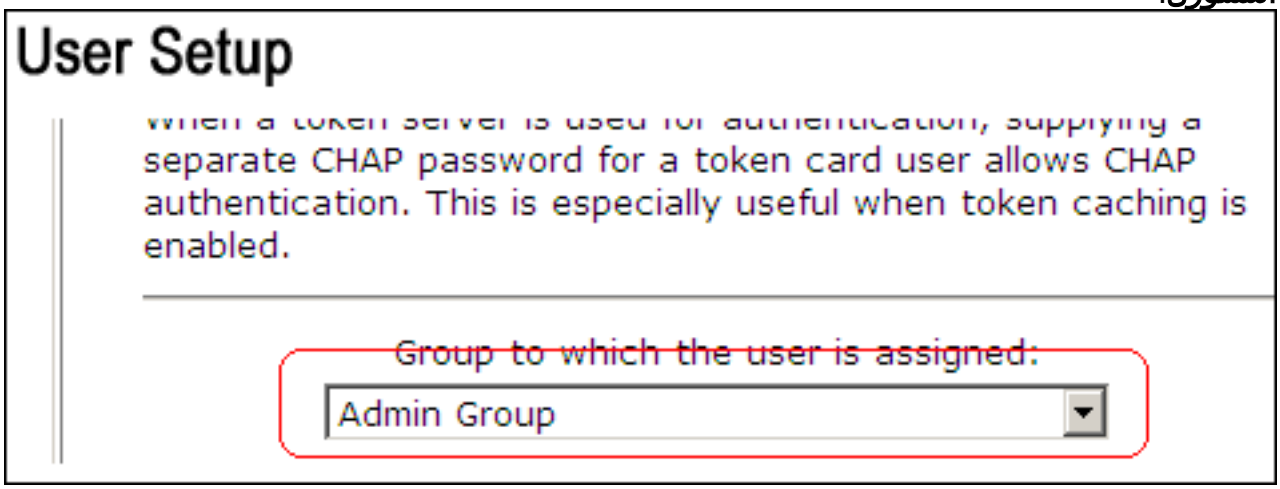
راجع مجموعة تفويض أوامر Shell الخاصة بقسم مستخدم في دليل المستخدم لخادم التحكم في الوصول الآمن من Cisco 4.1 للحصول على مزيد من المعلومات حول كيفية تكوين تكوين مجموعة تفويض أوامر Shell للمستخدمين.

ملاحظة: تتجاوز الإعدادات على مستوى المستخدم الإعدادات على مستوى المجموعة في ACS، مما يعني أنه إذا كان لدى المستخدم مجموعة تفويض أوامر shell في الإعدادات على مستوى المستخدم، فإنها تتجاوز الإعدادات على مستوى المجموعة.

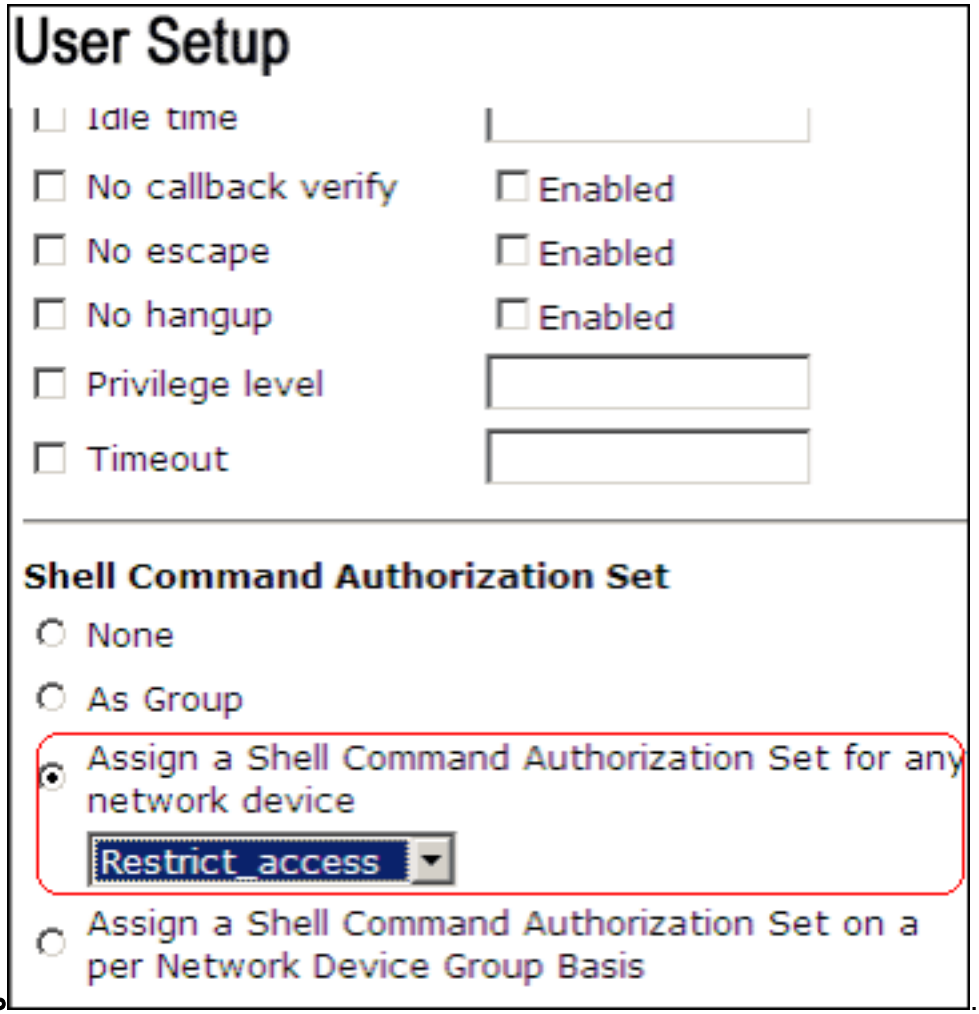
1. انقر فوق **إعداد المستخدم > إضافة/تحرير** لإنشاء مستخدم جديد باسم *admin_user* ليكون جزءا من مجموعة الإدارة.



2. من المجموعة التي يتم تعيين قائمة منسدلة لها للمستخدم، أختر **مجموعة المسؤول**.



3. في منطقة مجموعة تفويض أوامر Shell، انقر فوق **مجموعة تفويض أوامر Shell لأي** زر لاسلكي **لجهاز الشبكة**، واختر **Restrict_Access** من القائمة المنسدلة.**ملاحظة:** في هذا السيناريو، يعد هذا المستخدم جزءا من "مجموعة الإدارة". مجموعة تفويض طبقة *Restrict_access* قابلة للتطبيق؛ مجموعة تفويض طبقة *ReadWrite Access* غير قابلة



للتطبيق. **ملاحظة:** في قسم (Cisco TACACS+) من منطقة تكوين الواجهة، تأكد من تحديد خيار **طبقة (exec)** في عمود المستخدم.

تكوين موجه IOS

بالإضافة إلى تكوين الإعداد المسبق الخاص بك، يلزم وجود هذه الأوامر على موجه IOS أو المحول من أجل تنفيذ تفويض الأوامر من خلال خادم ACS:

```
aaa new-model
aaa authorization config-commands
aaa authorization commands 0 default  group tacacs+ local
aaa authorization commands 1 default  group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
tacacs-server host 10.1.1.1
tacacs-server key cisco123
```

تكوين ASA/PIX/FWSM

بالإضافة إلى التكوين المسبق الخاص بك، يلزم وجود هذه الأوامر على ASA/PIX/FWSM من أجل تنفيذ تفويض الأوامر من خلال خادم ACS:

```
+aaa-server authserver protocol tacacs
aaa-server authserver host 10.1.1.1
aaa authorization command authserver
```

ملاحظة: لا يمكن إستخدام بروتوكول RADIUS لتقييد وصول المستخدم إلى ASDM لأغراض للقراءة فقط. ونظرا لأن حزم RADIUS تحتوي على المصادقة والتخويل في نفس الوقت، فإن جميع المستخدمين الذين تتم مصادقتهم

في خادم RADIUS لديهم مستوى امتياز قدره 15. يمكنك تحقيق ذلك من خلال TACACS باستخدام تنفيذ مجموعات تفويض الأوامر.

ملاحظة: يستغرق ASA/PIX/FWSM وقتا طويلا لتنفيذ كل أمر تمت كتابته حتى إذا كان ACS غير متوفر لتنفيذ تفويض الأوامر. إذا لم يتوفر ACS وكان ASA لديه تفويض الأوامر الذي تم تكوينه، سيظل ASA يطلب تفويض الأوامر لكل أمر.

استكشاف الأخطاء وإصلاحها

خطأ: فشل تفويض الأوامر

المشكلة

بعد تسجيل الدخول إلى جدار الحماية من خلال تسجيل TACACS، لا تعمل الأوامر. عند إدخال أمر، يتم تلقي هذا الخطأ: .

الحل

أتمت هذا steps in order to حللت هذا إصدار:

1. تأكد من إستخدام اسم المستخدم الصحيح ومن تعيين كافة الامتيازات المطلوبة للمستخدم.
2. إذا كان اسم المستخدم والامتيازات صحيحة، فتحقق من أن ASA لديه اتصال مع ACS وأن ACS نشط.

ملاحظة: يمكن أن يحدث هذا الخطأ أيضا إذا قام المسؤول بتكوين تفويض الأوامر بشكل خاطئ للمستخدمين المحليين، بالإضافة إلى TACACS. في هذه الحالة، أنجزت كلمة إستعادة in order to حللت الإصدار.

معلومات ذات صلة

- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)
- صفحة دعم خادم التحكم في الوصول الآمن من Cisco
- 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).