ASA 8.3 والإصدارات الأحدث: تفويض RADIUS (ACS 5.x) للوصول إلى VPN باستخدام قائمة التحكم في الوصول (ACL) القابلة للتنزيل ASDM مع CLI ومثال تكوين

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين جهاز الأمان لمصادقة المستخدمين للوصول إلى الشبكة. ونظرا لأنه يمكنك تمكين تفويضات RADIUS ضمنيا، فإن هذا المستند لا يحتوي على معلومات حول تكوين تفويض RADIUS على جهاز الأمان. وهو يوفر معلومات حول كيفية معالجة جهاز الأمان لمعلومات قائمة الوصول التي يتم تلقيها من خوادم RADIUS.

يمكنك تكوين خادم RADIUS لتنزيل قائمة الوصول إلى جهاز الأمان أو اسم قائمة الوصول في وقت المصادقة. يسمح للمستخدم فقط بما هو مسموح به في قائمة الوصول الخاصة

بالمستخدم.

قوائم الوصول القابلة للتنزيل هي أكثر الوسائل قابلية للتطوير عند إستخدام خادم Cisco لتوفير قوائم الوصول المناسبة لكل مستخدم. التحكم في الوصول الآمن (ACS). لمزيد من المعلومات حول ميزات قائمة الوصول القابلة للتنزيل و Cisco Secure ACS، ارجع إلى تكوين خادم RADIUS لإرسال قوائم التحكم في الوصول القابلة للتنزيل وقوائم التحكم في الوصول إلى IP القابلة للتنزيل.

ارجع إلى ASA/PIX 8.x: تفويض RADIUS (ACS) للوصول إلى الشبكة باستخدام قائمة التحكم في الوصول (ACL) القابلة للتنزيل مع CLI ومثال تكوين ASDM للتكوين المتطابق على Cisco ASA مع الإصدارات 8.2 والإصدارات الأقدم.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن جهاز الأمان القابل للتكيف (ASA) قيد التشغيل الكامل وتم تكوينه للسماح لمديري أجهزة الأمان المعدلة (ASDM) أو CLI من Cisco بإجراء تغييرات التكوين.

ملاحظة: ارجع إلى السماح بوصول HTTPS إلى ASDM للسماح بتكوين الجهاز عن بعد بواسطة ASDM أو Secure Shell (SSH).

المكونات المستخدمة

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

- برنامج ASA الإصدار 8.3 من Cisco والإصدارات الأحدث
- Cisco ASDM، الإصدار 6.3 والإصدارات الأحدث
- عميل شبكة VPN من Cisco الإصدار 5.x والإصدارات الأحدث
- Cisco Secure ACS 5.x

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.

الاصطلاحات

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

معلومات أساسية

يمكنك إستخدام قوائم التحكم في الوصول إلى IP القابلة للتنزيل لإنشاء مجموعات من

تعريفات قائمة التحكم في الوصول (ACL) التي يمكنك تطبيقها على العديد من المستخدمين أو مجموعات المستخدمين. تسمى هذه المجموعات من تعريفات قائمة التحكم بالوصول (ACL) محتويات قائمة التحكم بالوصول (ACL).

تعمل قوائم التحكم في الوصول (ACL) إلى IP القابلة للتنزيل بهذه الطريقة:

1. عندما يمنح ACS للمستخدم حق الوصول إلى الشبكة، فإن ACS يحدد ما إذا كانت قائمة التحكم في الوصول إلى IP قابلة للتنزيل يتم تعيينها إلى ملف تعريف التخويل في قسم النتائج.

2. إذا حدد ACS قائمة تحكم في الوصول إلى IP قابلة للتنزيل تم تعيينها إلى ملف تعريف التخويل، فإن ACS يرسل سمة (جزء من جلسة عمل المستخدم، في حزمة قبول الوصول إلى RADIUS) تحدد قائمة التحكم في الوصول إلى ACL المسماة، وإصدار قائمة التحكم في الوصول (ACL) المسماة.

3. إذا رد عميل AAA بأنه لا يحتوي على الإصدار الحالي من قائمة التحكم في الوصول (ACL) في ذاكرة التخزين المؤقت الخاصة به (أي أن قائمة التحكم في الوصول جديدة أو محدثة) إلى (جديدة أو محدثة)، فإن ACS يرسل قائمة التحكم في الوصول (ACL) المسماة.

قوائم التحكم في الوصول إلى IP القابلة للتنزيل هي بديل لتكوين قوائم التحكم في الوصول (ACL) في سمة RADIUS Cisco-AV-pair [26/9/1] لكل مستخدم أو مجموعة مستخدم. يمكنك إنشاء قائمة تحكم في الوصول (ACL) إلى IP قابلة للتنزيل مرة واحدة، ومنحها اسما، ثم تعيين قائمة التحكم في الوصول إلى IP القابلة للتنزيل إلى أي ملف تعريف تفويض إذا قمت بإرجاع اسمه. تكون هذه الطريقة أكثر فعالية من إذا قمت بتكوين سمة RADIUS Cisco-av-pair لتوصيف التخويل.

عندما تدخل تعريفات قائمة التحكم في الوصول (ACL) في واجهة ويب ACS، لا تستخدم أمر قائمة التحكم في الوصول (ACL) القياسية والأسماء لعميل AAA الذي تنوي تطبيق قائمة التحكم في الوصول (ACL) إلى IP القابلة للتنزيل عليه. تتضمن تعريفات قائمة التحكم في الوصول (ACL) التي تدخلها في ACS أمر واحد أو أكثر من أوامر قائمة التحكم في الوصول (ACL) على سطر منفصل. يجب أن يكون كل أمر قائمة تحكم في الوصول (ACL).

في ACS، يمكنك تحديد العديد من قوائم التحكم في الوصول إلى IP القابلة للتنزيل، واستخدامها في ملفات تعريف التخويل المختلفة. استنادا إلى الشروط الواردة في قواعد تفويض خدمة الوصول، يمكنك إرسال ملفات تعريف تفويض تحتوي على قوائم التحكم في الوصول إلى IP القابلة للتنزيل إلى عملاء AAA مختلفين.

في (ACL) عالوة على ذلك، يمكنك تغيير ترتيب محتويات قائمة التحكم في الوصول (ACL) إلى IP قابلة للتنزيل. يقوم ACS بفحص محتويات قائمة تحكم في الوصول (ACL) إلى IP قابلة للتنزيل وتنزيل أول محتوى لقائمة التحكم في الوصول (ACL)، بدءا من أعلى الجدول. عند تعيين الترتيب، يمكنك التأكد من كفاءة النظام إذا قمت بوضع محتويات قائمة التحكم في الوصول (ACL) الأكثر قابلية للتطبيق على نحو أعلى في القائمة.

من أجل إستخدام قائمة تحكم في الوصول (ACL) إلى IP قابلة للتنزيل على عميل AAA، يجب أن يلتزم عميل AAA بالقواعد التالية:

- إستخدام RADIUS للمصادقة
- دعم قوائم التحكم في الوصول (ACL) إلى IP القابلة للتنزيل

هذه أمثلة على أجهزة Cisco التي تدعم قوائم التحكم في الوصول إلى IP القابلة للتنزيل:

- ASA
- أجهزة Cisco التي تشغل IOS، الإصدار 12.3(8)T والإصدارات الأحدث

هذا مثال على التنسيق الذي يجب عليك إستخدامه لإدخال قوائم التحكم في الوصول (ACL) إلى مربع تعريفات قائمة التحكم في الوصول (ACL):

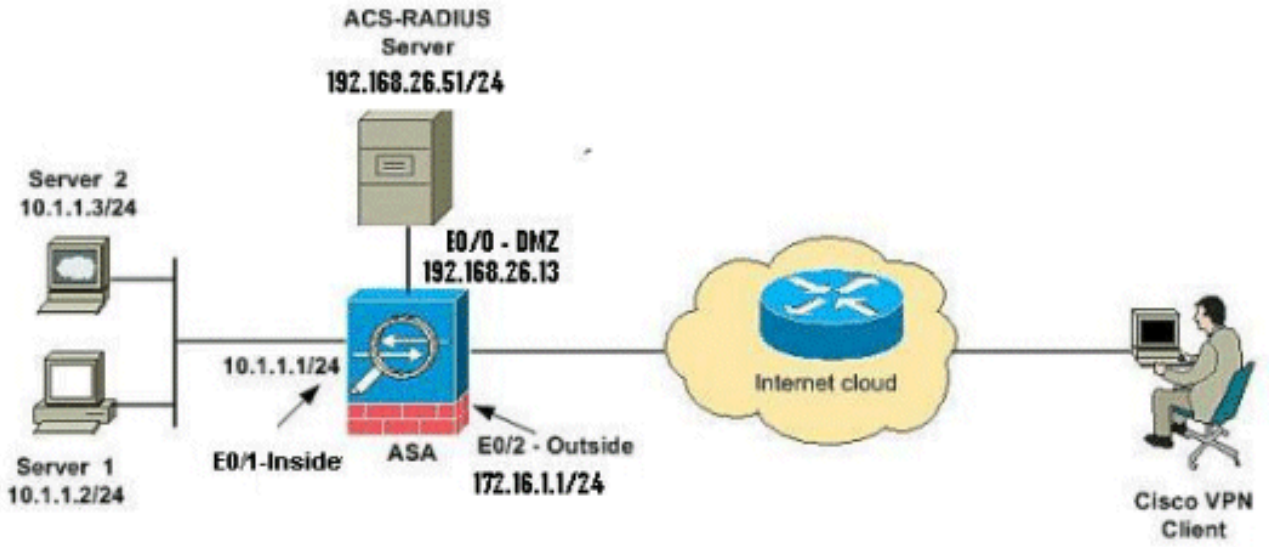
```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

التكوين

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



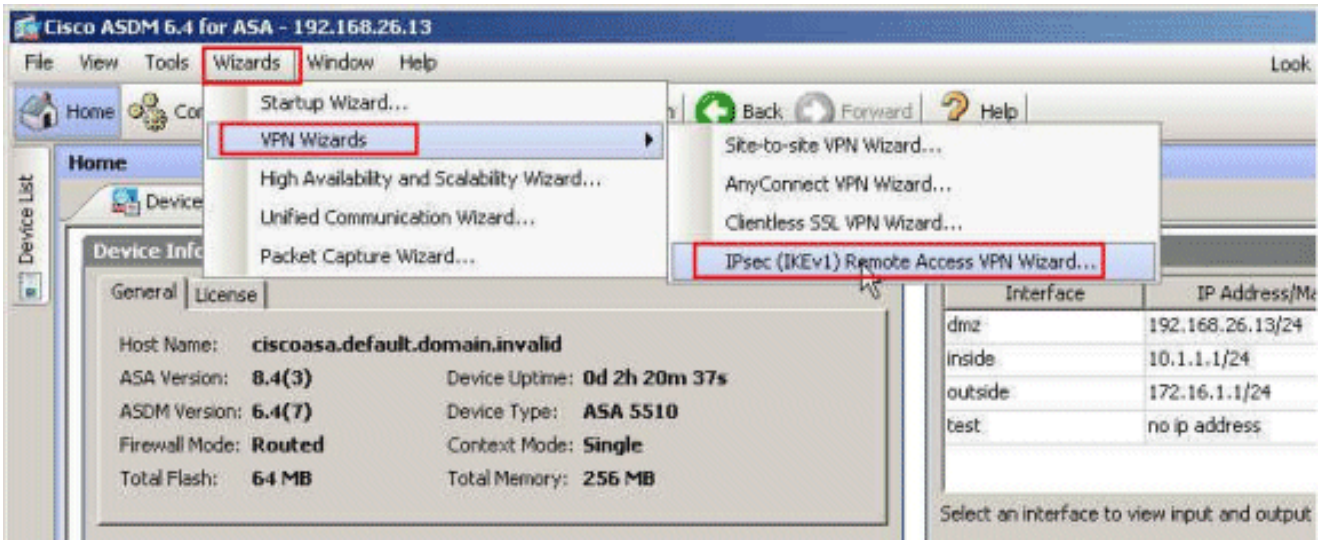
ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت.
هم rfc 1918 عنوان أي كان استعملت في مختبر بيئة.

تكوين شبكة VPN للوصول عن بعد (IPsec)

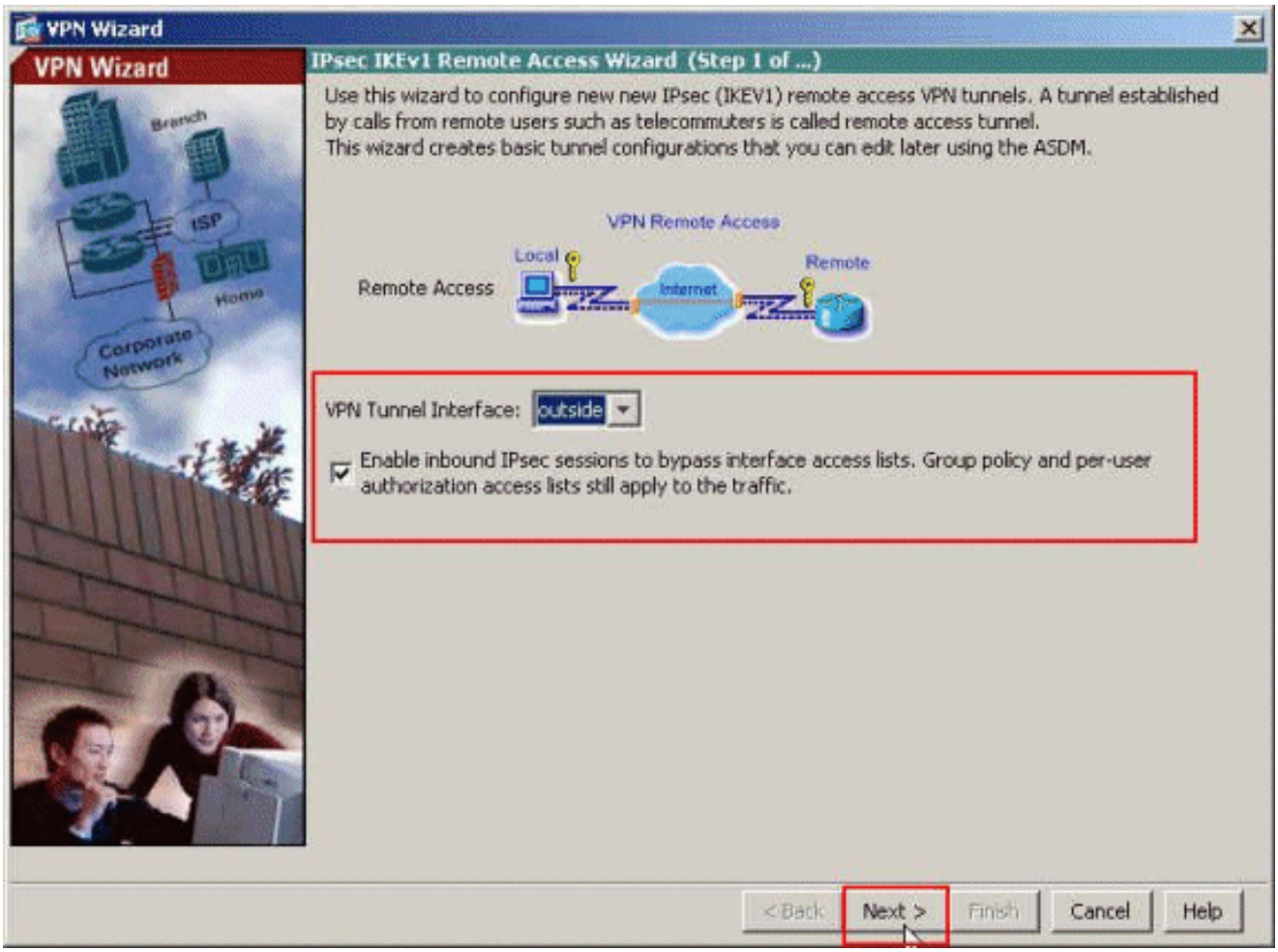
إجراء ASDM

أتمت هذا steps in order to شكلت الوصول عن بعد VPN:

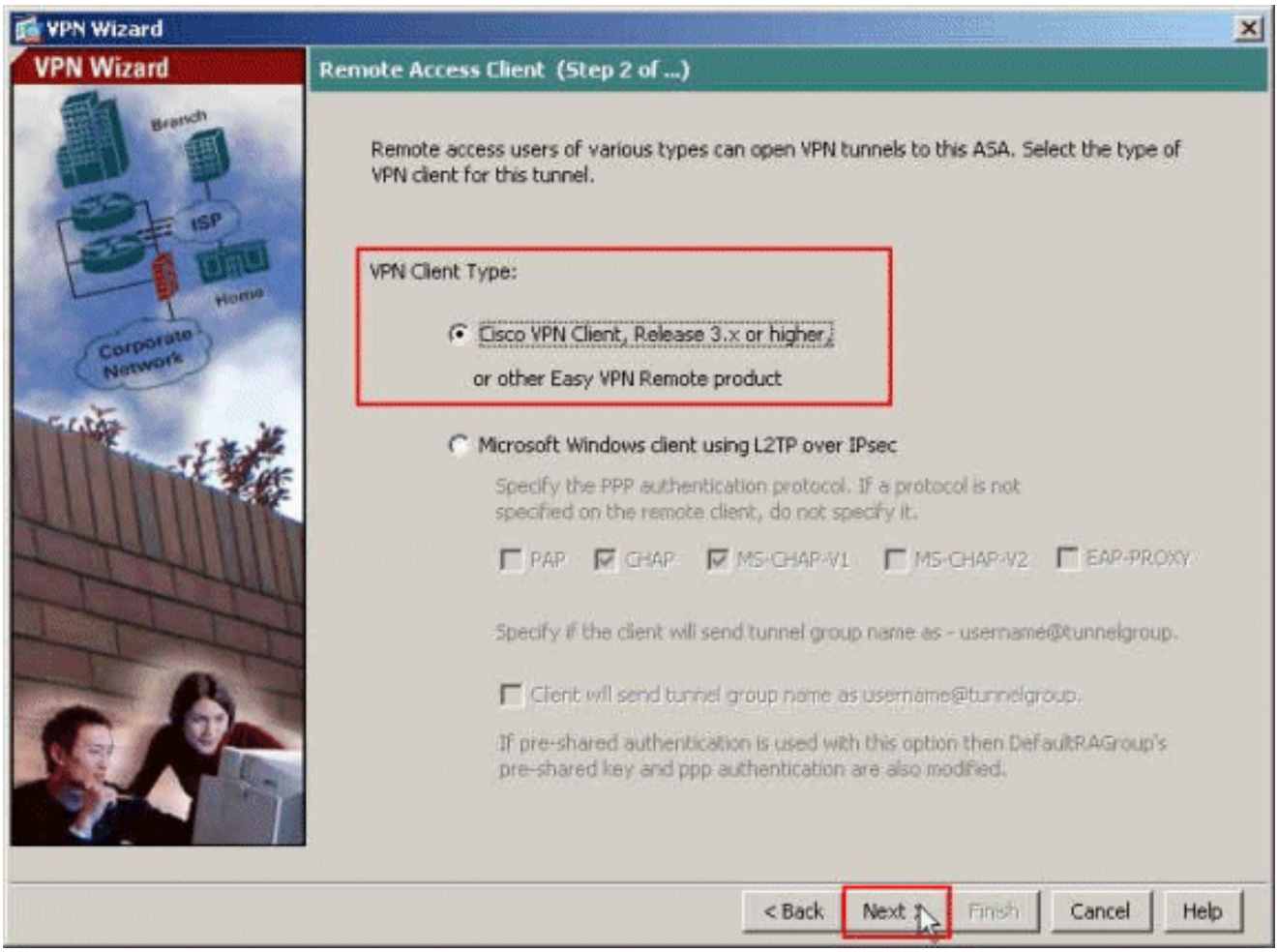
1. حدد المعالجات > معالجات VPN > IPsec (IKEv1) معالج VPN للوصول عن بعد من الإطار الرئيسي.



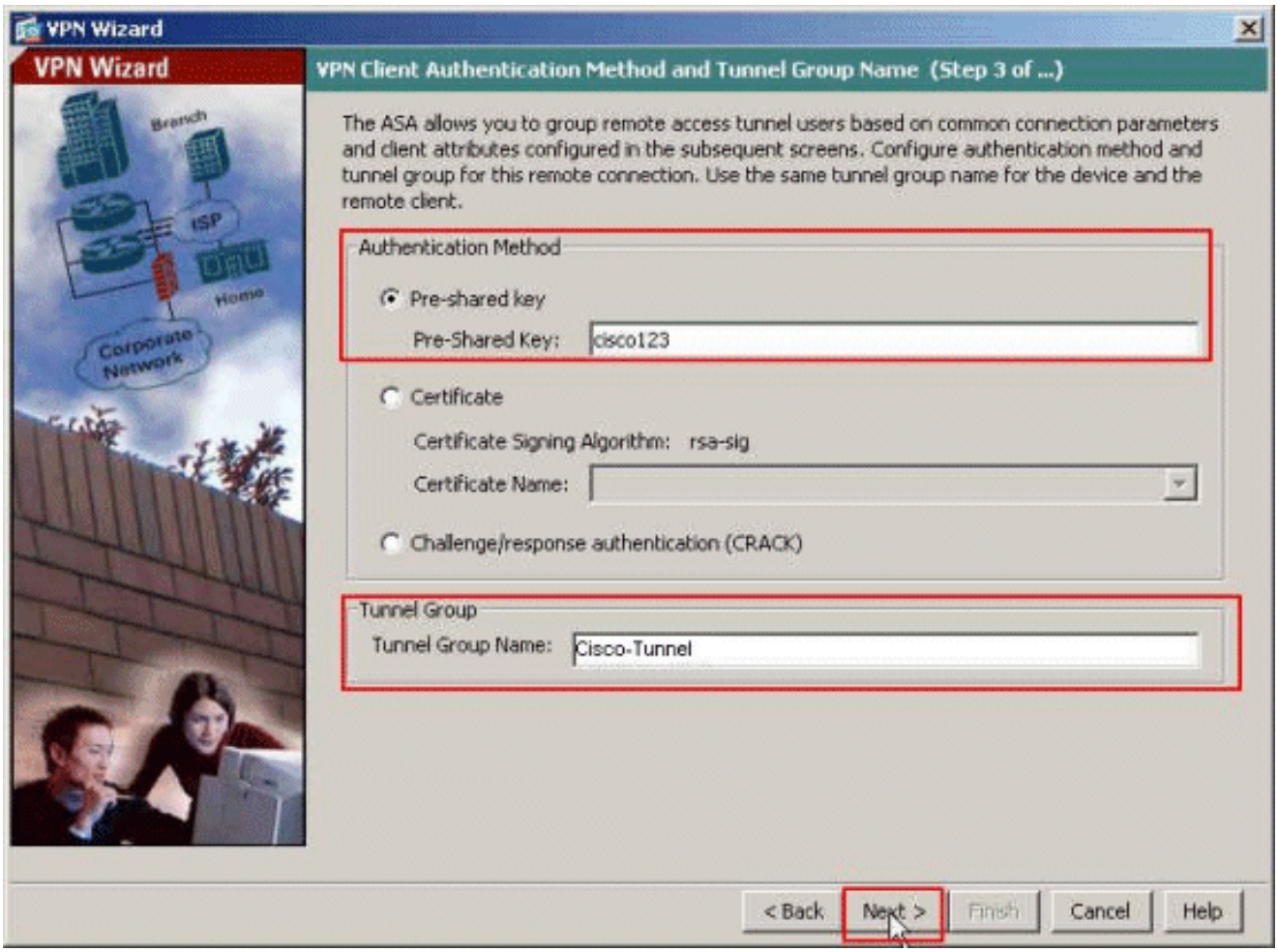
2. حدد واجهة نفق VPN كما هو مطلوب (خارجي، في هذا المثال)، وتأكد أيضا من تحديد خانة الاختيار المجاورة ل تمكين جلسات عمل IPsec الواردة لتجاوز قوائم الوصول إلى الواجهة.



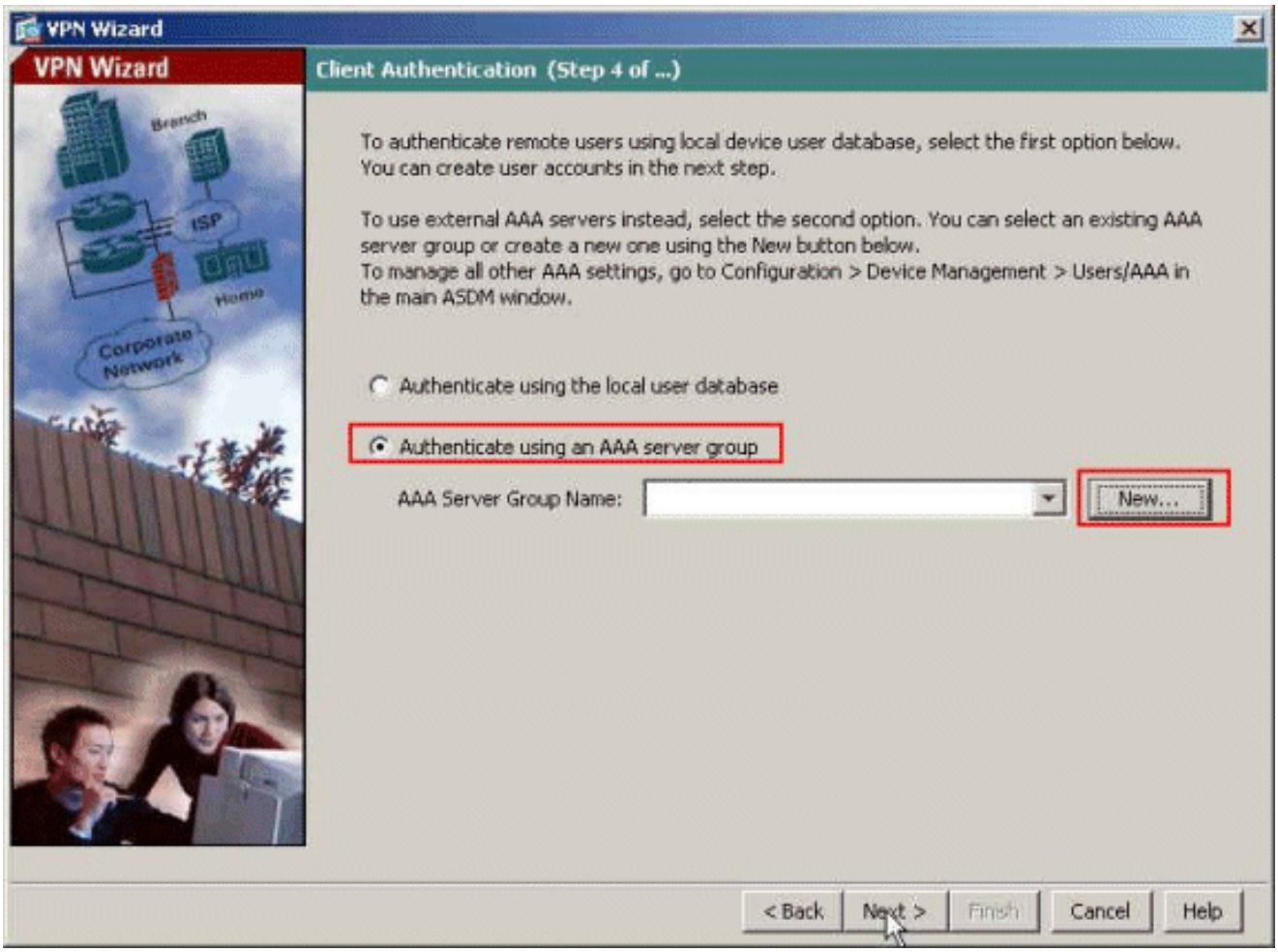
3. انقر فوق Next. إطلاق 3.x أو أعلى. أخترت ال VPN زبون نوع بما أن cisco VPN زبون، (التالي).



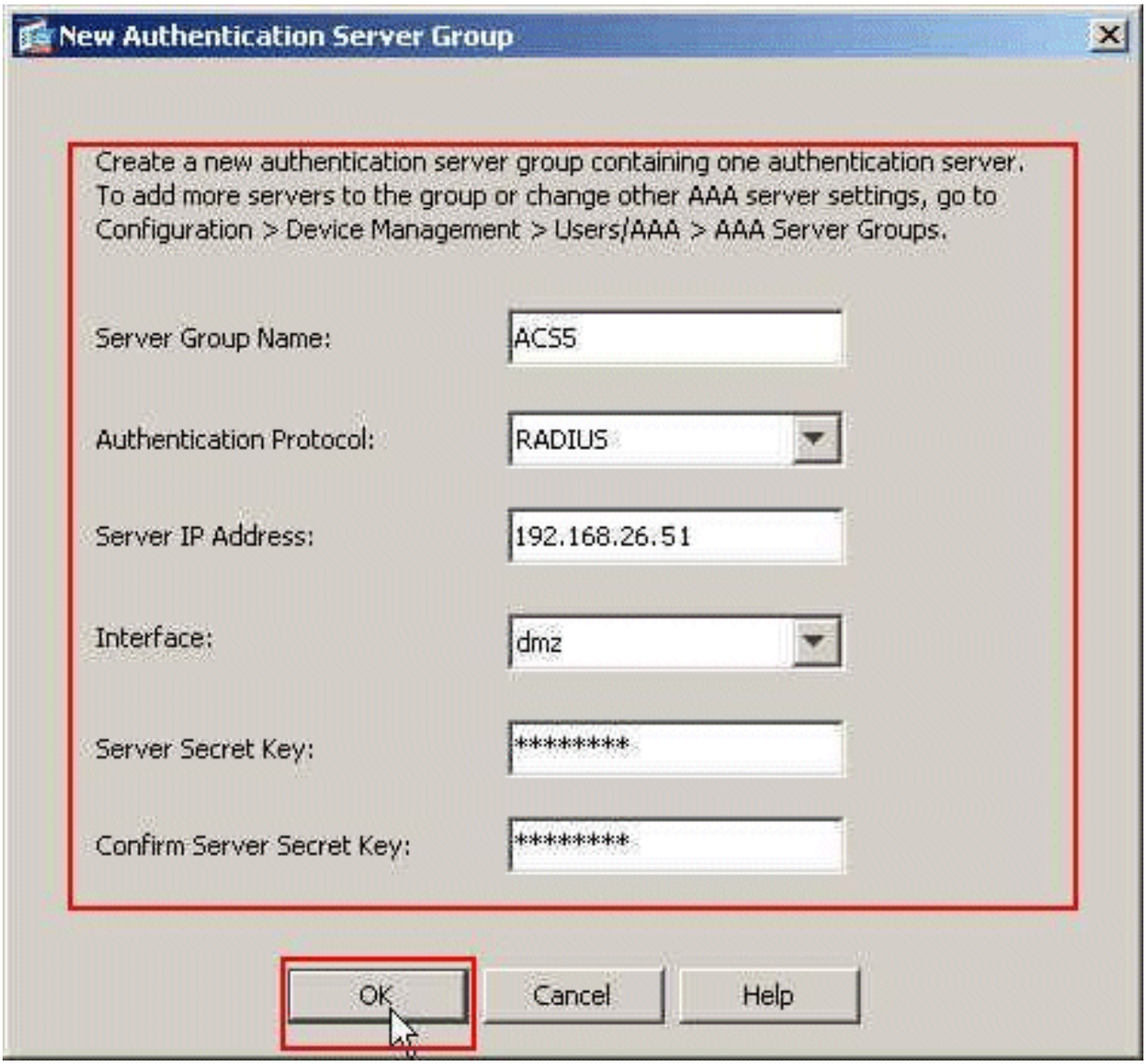
4. أختر أسلوب المصادقة ووفر معلومات المصادقة. طريقة المصادقة المستخدمة هنا هي مفاتيح مشترك مسبقا. قم أيضا بتوفير اسم مجموعة النفق في المساحة المتوفرة. اسم مجموعة النفق المستخدم هو Cisco123 والمفاتيح المشترك مسبقا المستخدم هنا هو Cisco-Tunnel. انقر فوق Next (التالي).



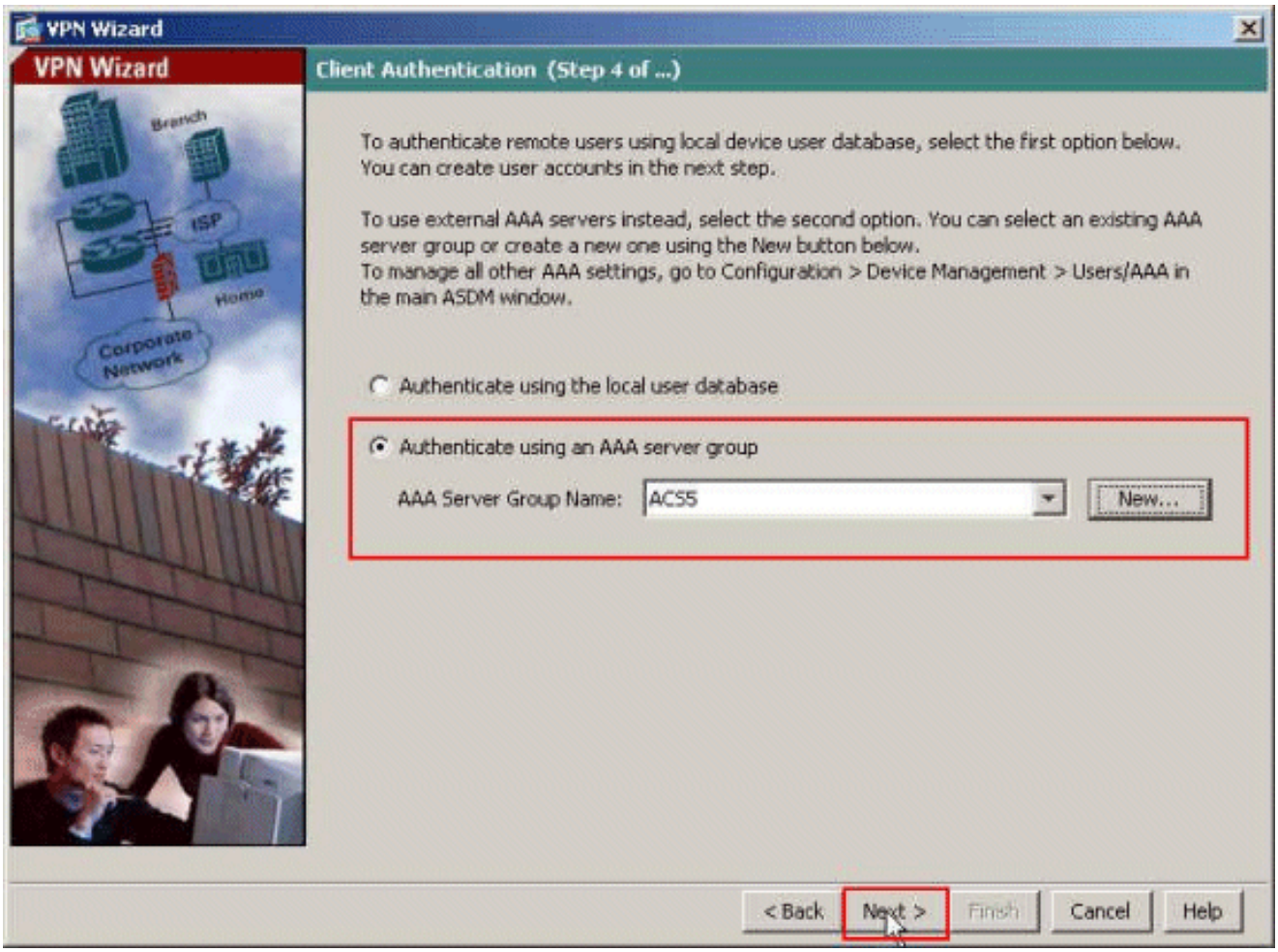
5. أختر ما إذا كنت تريد مصادقة المستخدمين عن بعد إلى قاعدة بيانات المستخدم المحلية أو إلى مجموعة خوادم AAA خارجية. هنا، نختار المصادقة باستخدام مجموعة خوادم AAA. انقر فوق جديد بجوار حقل اسم مجموعة خوادم AAA لإنشاء اسم مجموعة خوادم AAA جديد.



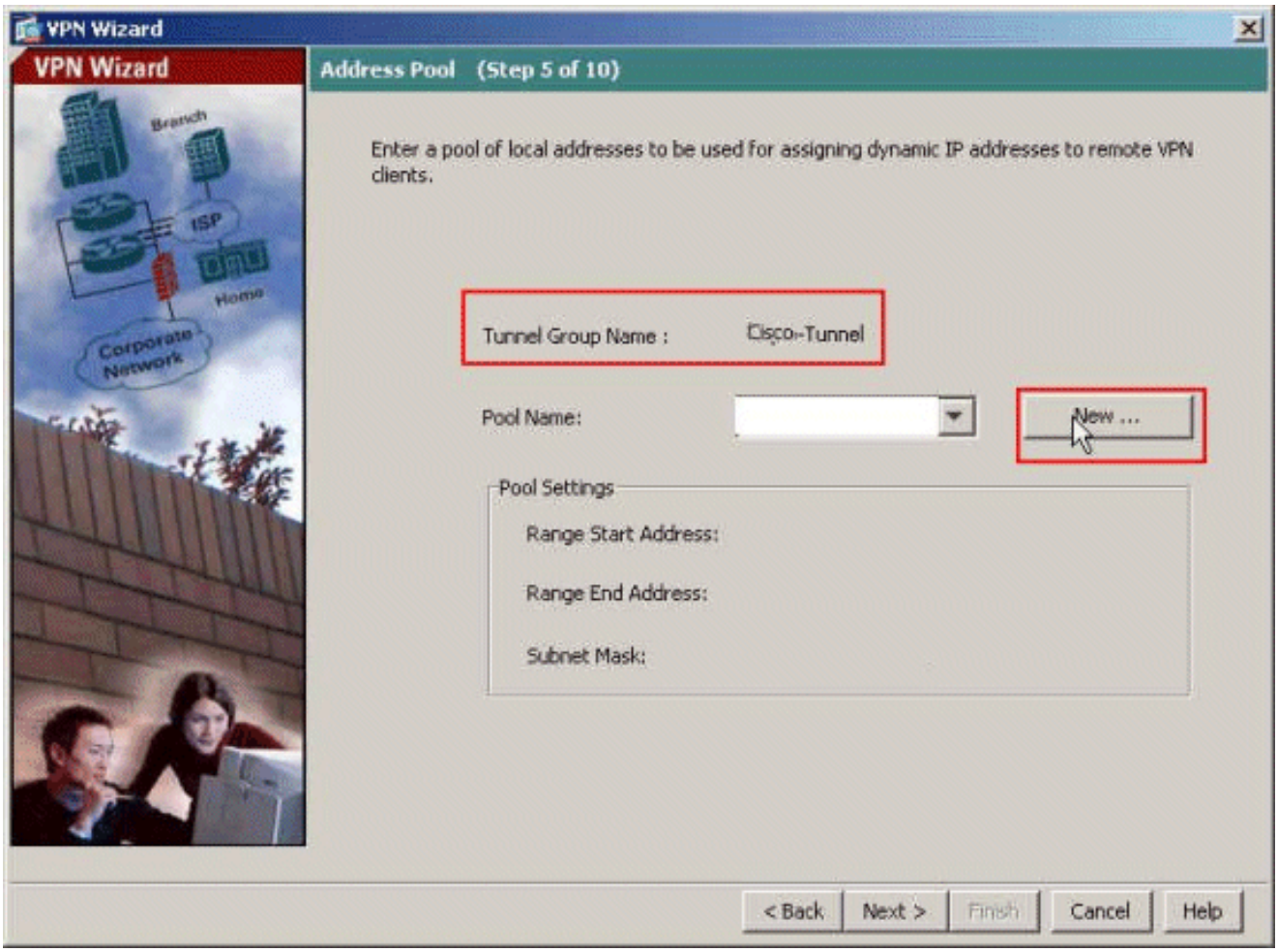
6. قم بتوفير اسم مجموعة الخادم وبروتوكول المصادقة وعنوان IP للخادم واسم الواجهة ومفتاح سر الخادم في المساحات المقابلة المتوفرة، وانقر موافق.



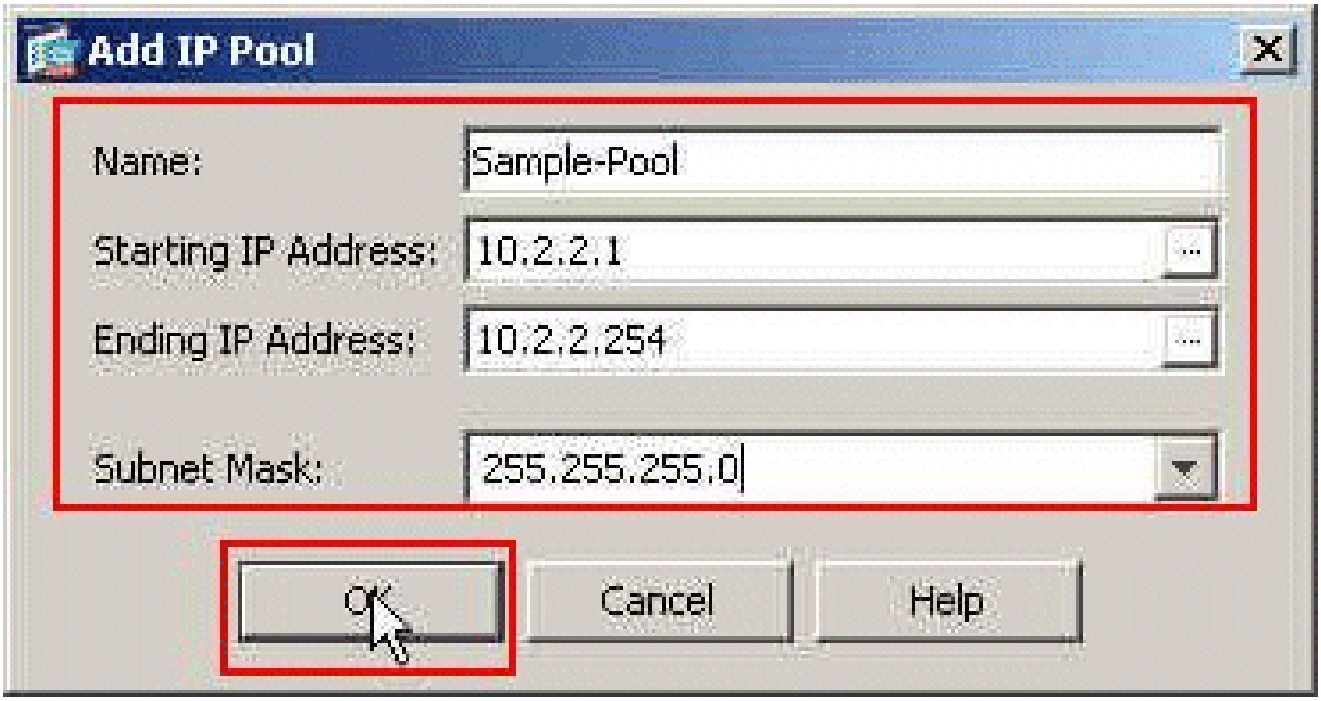
7. انقر فوق Next (التالي).



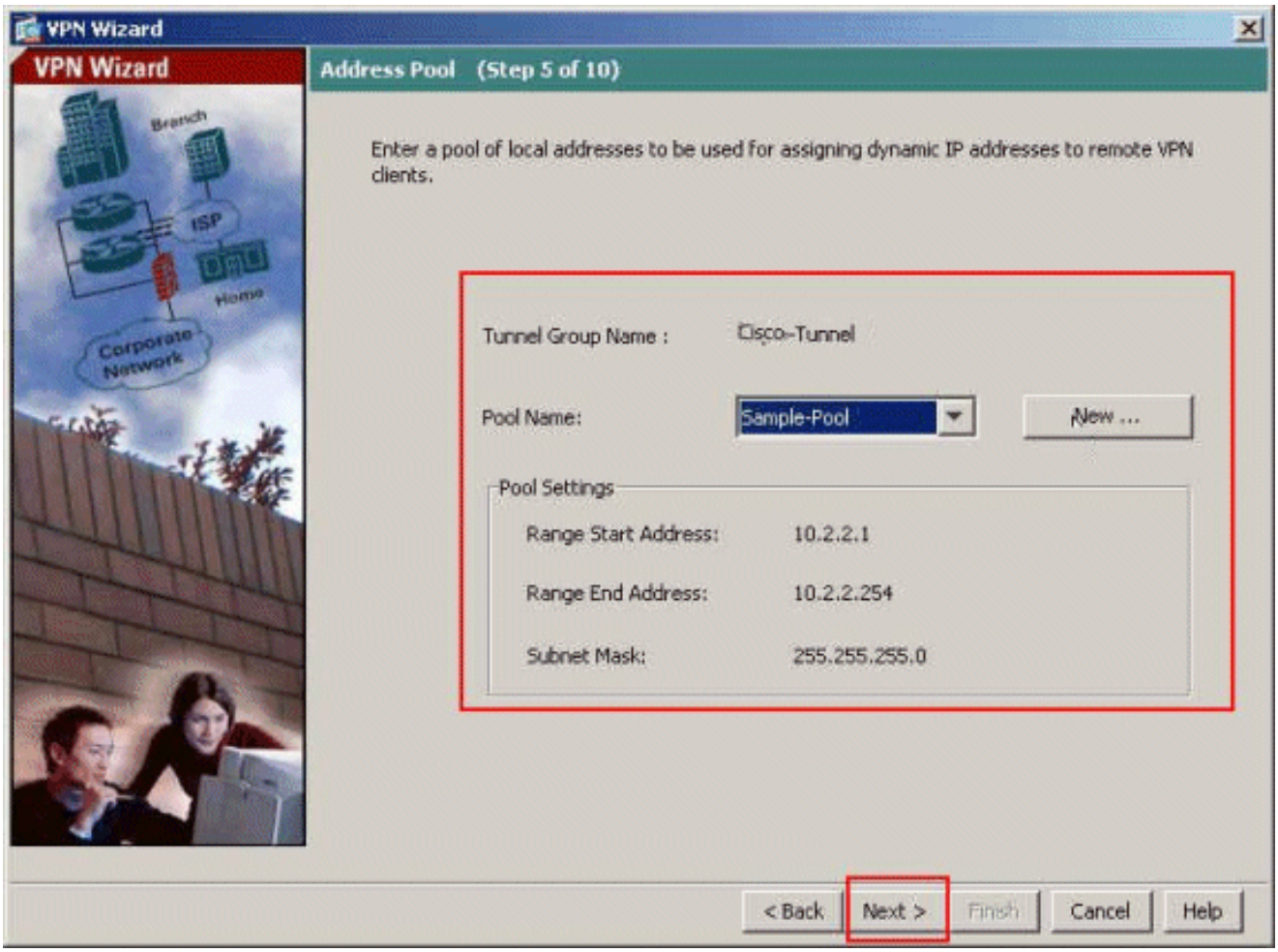
حدد مجموعة من العناوين المحلية ليتم تعيينها ديناميكيا لعملاء شبكات VPN8. البعيدة عند إتصالها. طقطقت جديد in order to خلقت جديد برك من عنوان محلي.



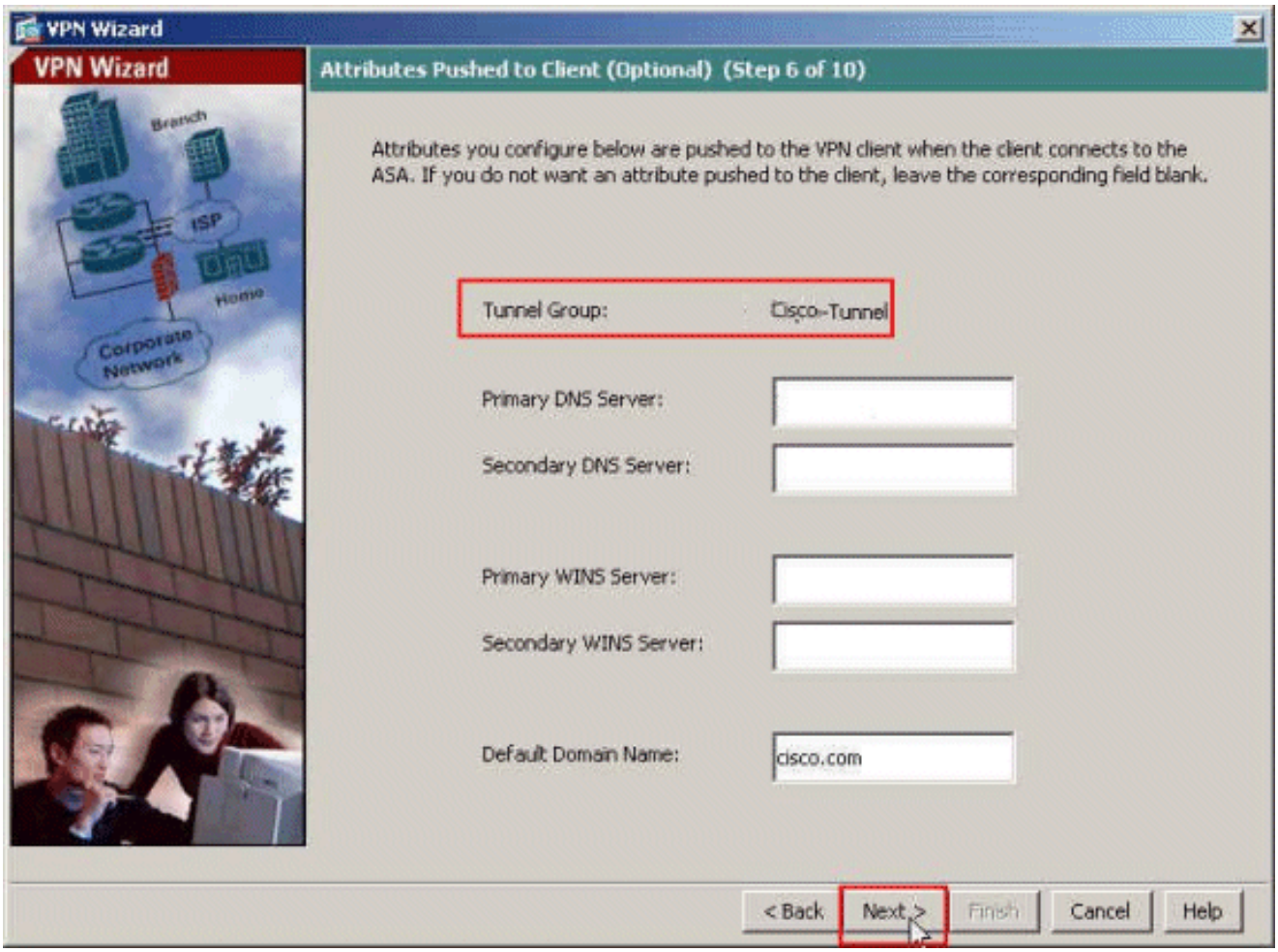
9. في نافذة إضافة تجمع IP، قم بتوفير اسم التجمع، وبدء عنوان IP، وإنهاء عنوان IP، وقناع الشبكة الفرعية. وانقر فوق OK.



10. حدد اسم التجمع من القائمة المنسدلة، وانقر التالي. اسم التجمع لهذا المثال هو نموذج تجمع الذي تم إنشاؤه في الخطوة 9.



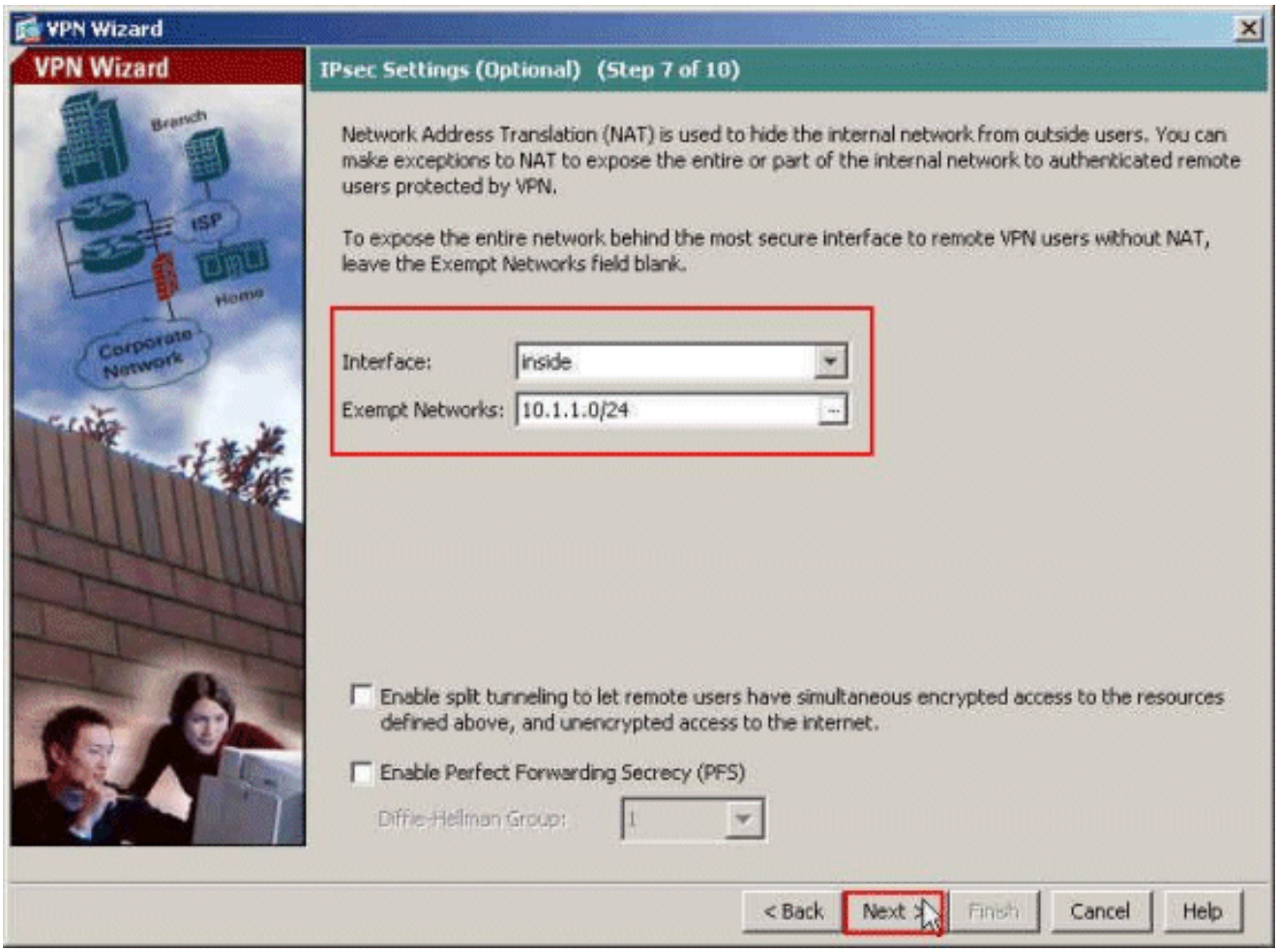
11. إختياري: حدد معلومات خادم DNS و WINS واسم مجال افتراضي ليتم دفعه إلى عملاء VPN البعيدة.



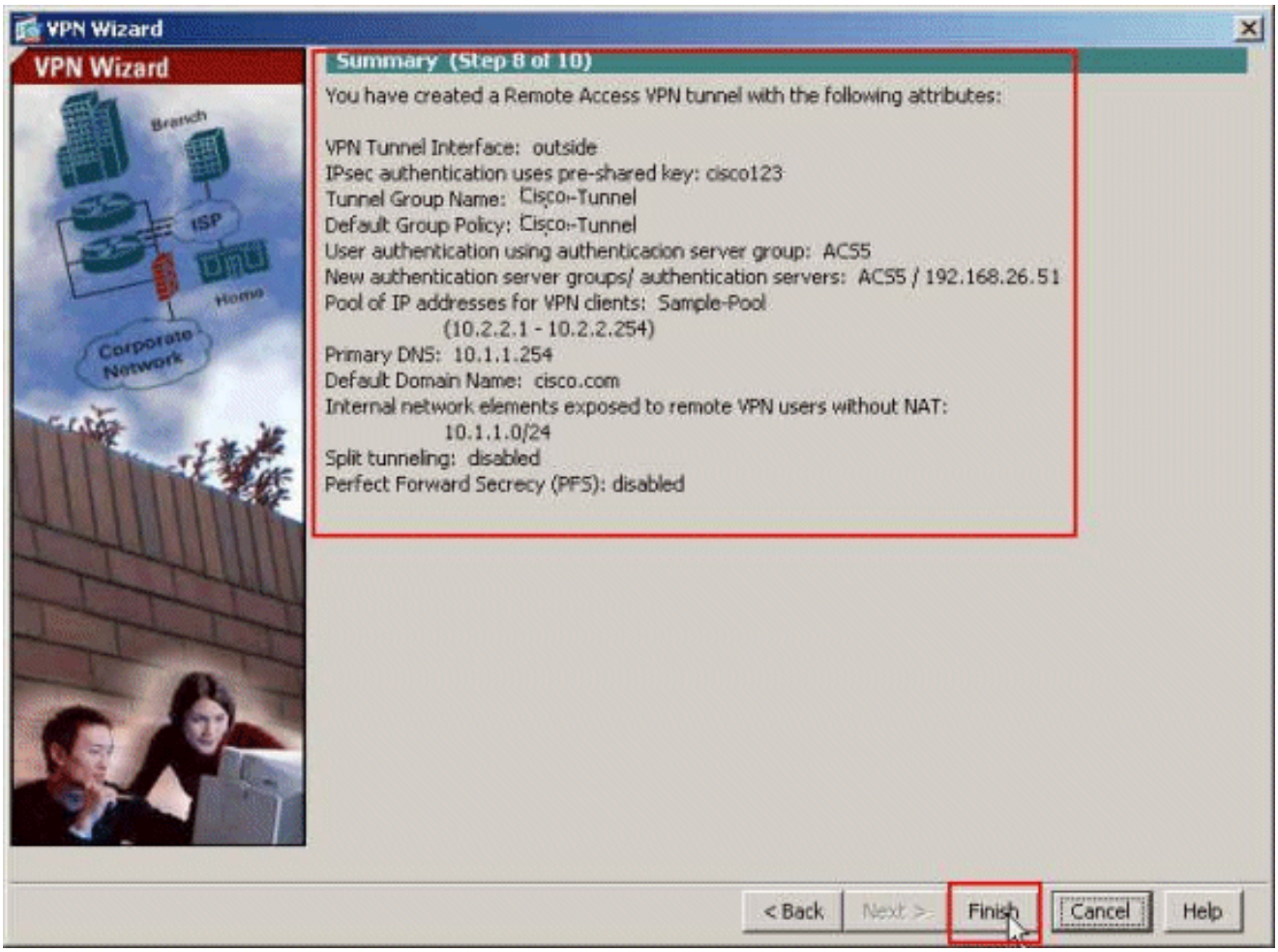
12. حدد أي البيانات المضيفة الداخلية أو الشبكات، إن وجدت، يجب أن يتم تعريفها لمستخدمي شبكات VPN البعيدة. طقطقت بعد ذلك بعد توفير القارن إسم والشبكات أن يكون استثنيت في الاستثناء شبكة مجال.

إن يترك أنت هذا قائمة فارغ، وه يسمح بعيد VPN مستعمل أن ينفذ الكامل داخل شبكة من ال ASA.

أنت يستطيع أيضا مكنت انقسام tunneling على هذا نافذة. يقوم الاتصال النفقي المنقسم بتشفير حركة مرور البيانات إلى المواد المحددة مسبقا في هذا الإجراء وتوفير وصول غير مشفر إلى الإنترنت بشكل عام من خلال عدم إنشاء قنوات لحركة مرور البيانات هذه. إن ال يمكن انقسام tunneling يكون، كل حركة مرور من بعيد VPN مستعمل أنفاق إلى ال ASA. يمكن أن يشكل ذلك نطاقا ترددي عريضا جدا ومعالجا مكثفا، وذلك بناء على عملية التهيئة لديك.



13. تعرض هذه النافذة ملخصا للإجراءات التي اتخذتها. انقر فوق إنهاء إذا كنت راضيا عن التكوين الخاص بك.



تكوين ASA باستخدام CLI

هذا هو تكوين CLI:

يتم ت

```
!--- Create the AAA server group "ACS5" and speci

!--- PHASE 2 CONFIGURATION ---! !---
```

```
!--- PHASE 1 CONFIGURATION ---! !--- This configuration uses ISAKMP policies defined with all the perm
```

```
                                                                    !--- Associate
```

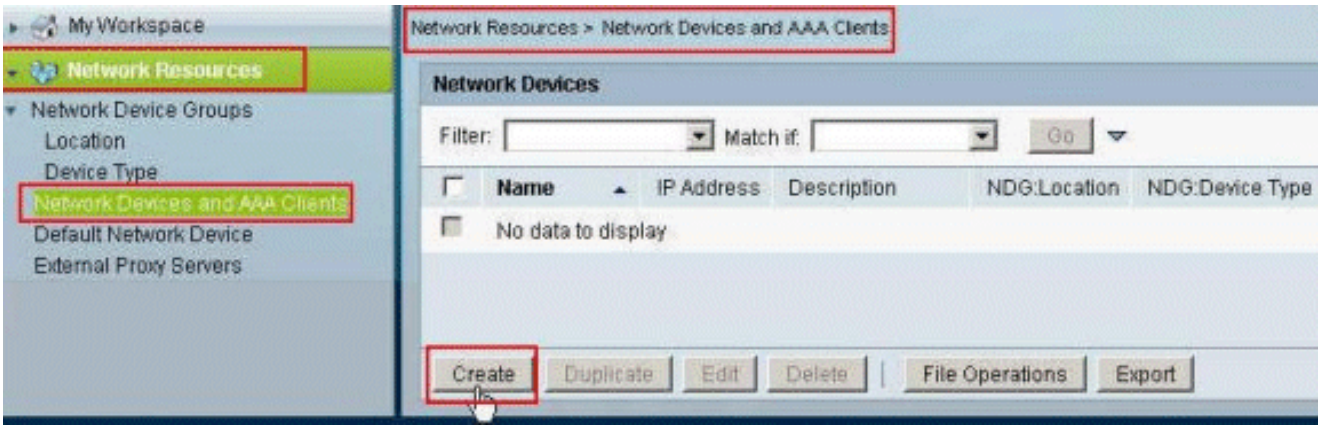
تكوين ACS لقائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم الفردي

يمكنك تكوين قوائم الوصول القابلة للتنزيل على Cisco Secure ACS 5.x كائنات أذونات مسماة ثم تعيينه إلى ملف تعريف التفويض الذي سيتم إختياره في قسم النتائج من قاعدة في خدمة الوصول.

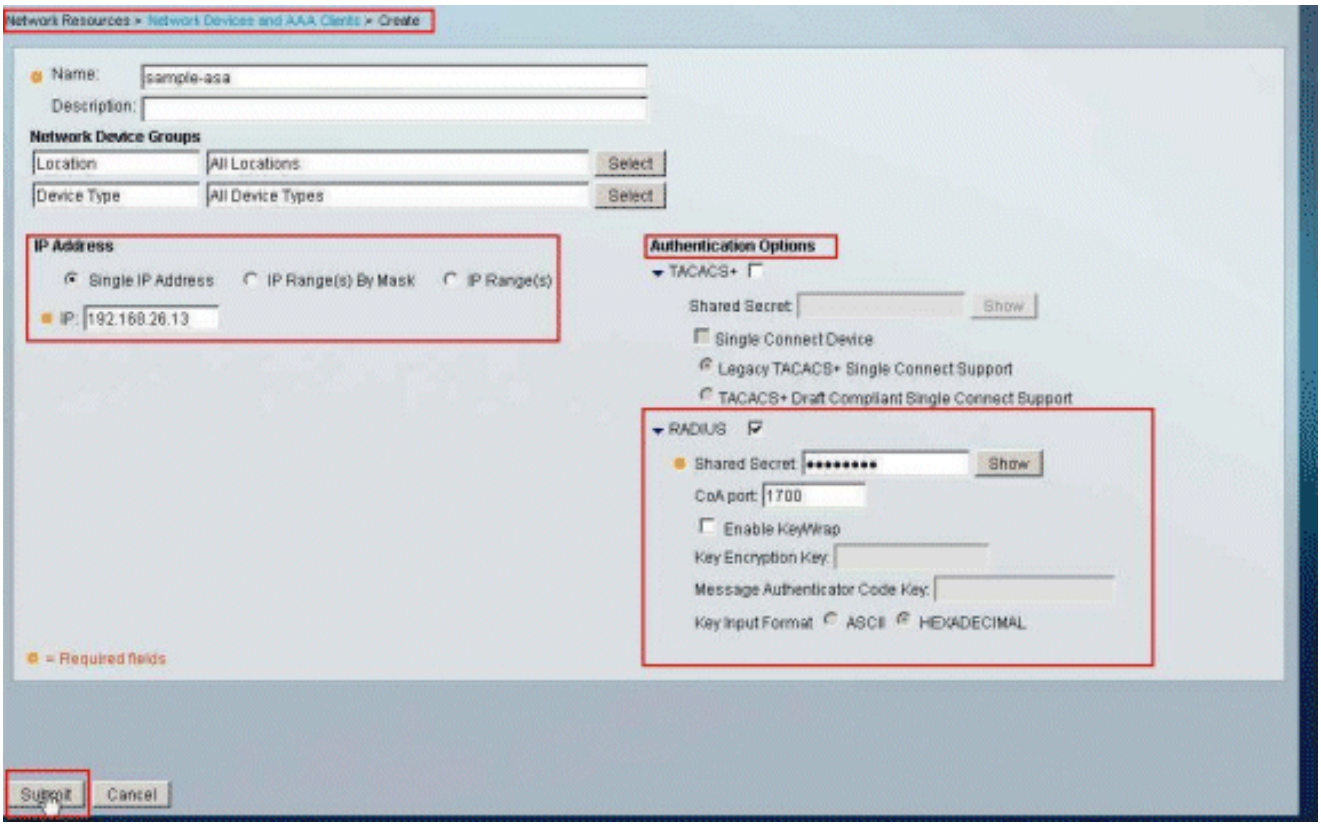
في هذا المثال، تتم مصادقة مستخدم شبكة VPN ل IPsec بنجاح، ويرسل خادم RADIUS قائمة وصول قابلة للتنزيل إلى جهاز الأمان. يمكن للمستخدم "cisco" الوصول إلى خادم (ACL)، 10.1.1.2 فقط ويرفض جميع الوصول الآخر. للتحقق من قائمة التحكم في الوصول القابلة للتنزيل للمستخدم/المجموعة قائمة التحكم في الوصول (ACL) راجع قسم.

أتمت هذا steps in order to شكلت RADIUS بزبون في cisco أمن ACS 5.x:

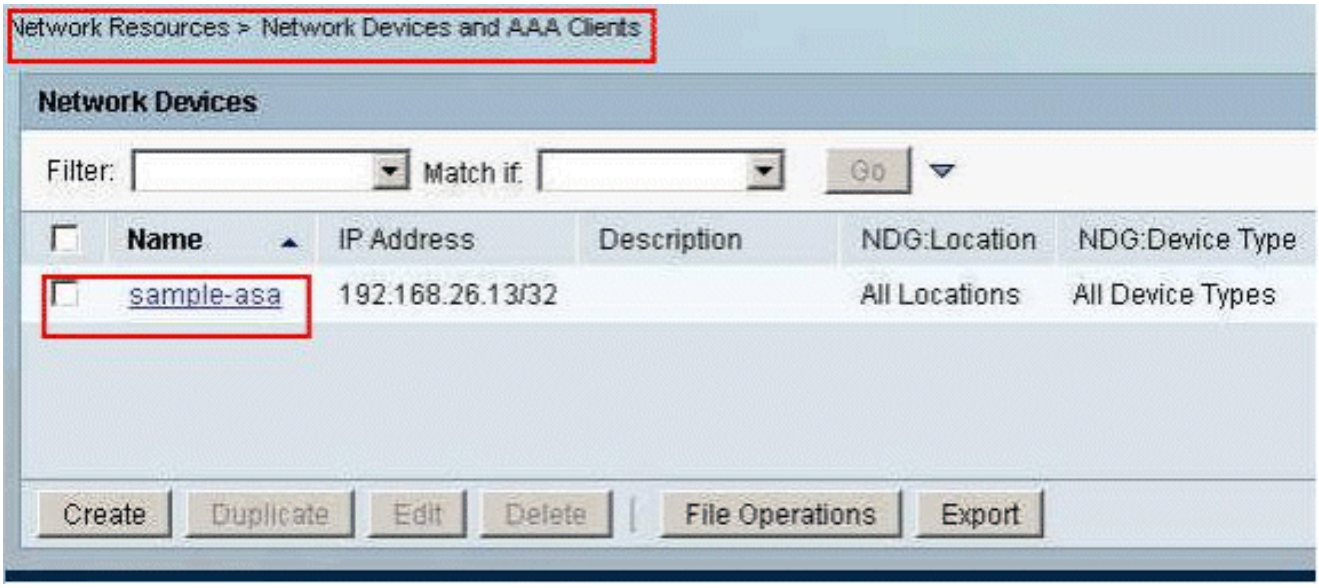
1. أخترت شبكة مورد>شبكة أداة و AAA بزبون، وطقطقة يخلق in order to أضفت مدخل ل الـ ASA في الـ RADIUS نادل قاعدة معطيات.



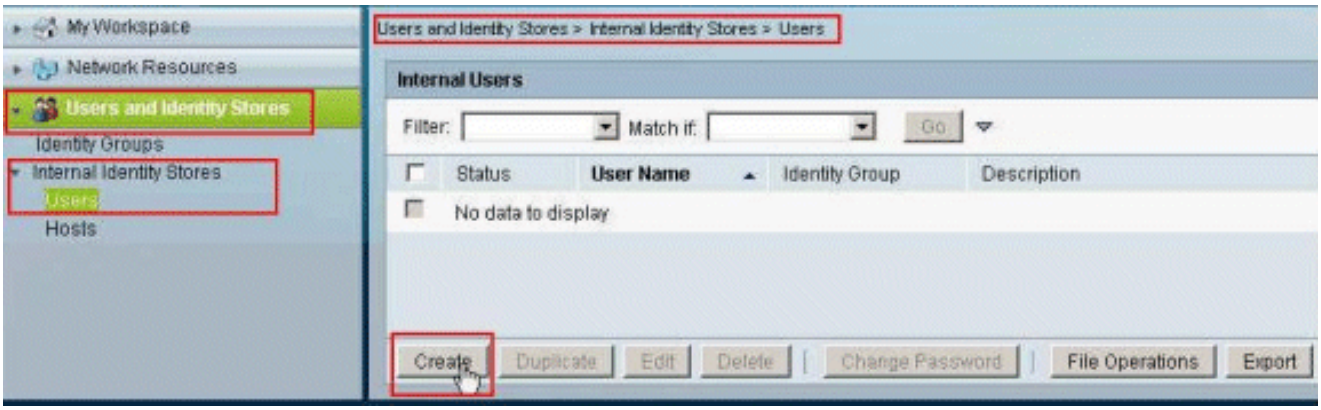
2. دخلت اسم محلي مهم ل الـ ASA (عينة-asa، في هذا مثال)، بعد ذلك دخلت 192.168.26.132. في العنوان مجال. أخترت RADIUS في المصادقة خيار قسم ب يفحص الـ RADIUS. دقيق صندوق وأدخل Cisco123 ل الـ يشارك سر مجال. انقر على إرسال.



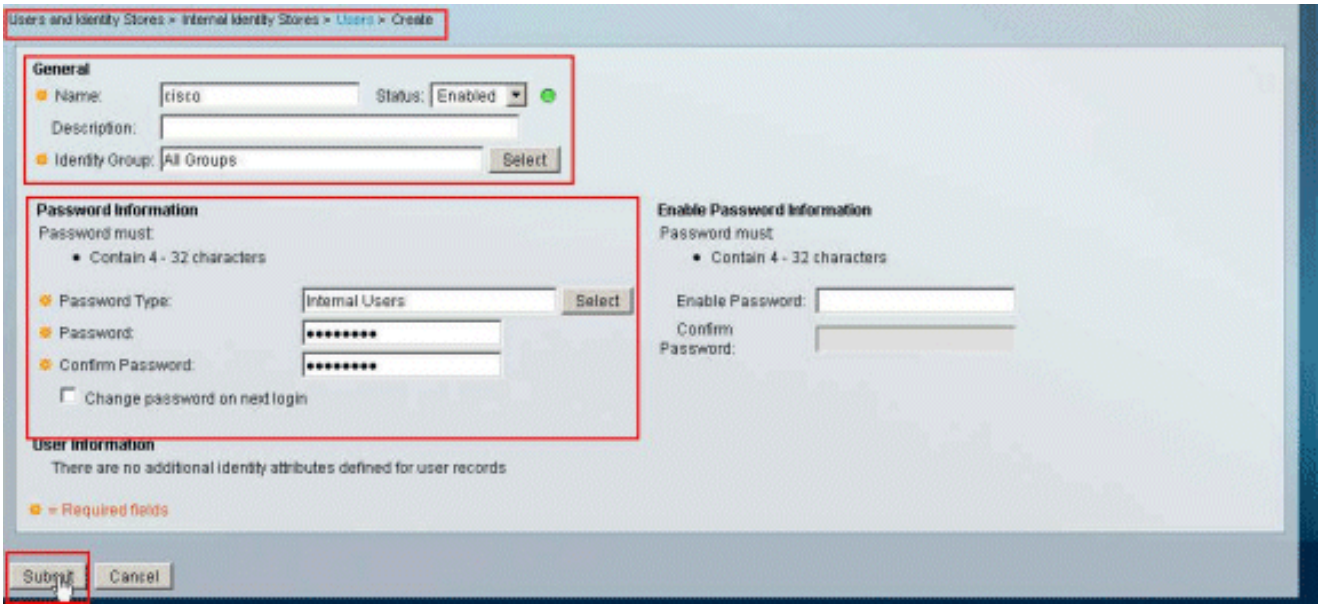
3. تتم إضافة ASA بنجاح إلى قاعدة بيانات خادم RADIUS (ACS).



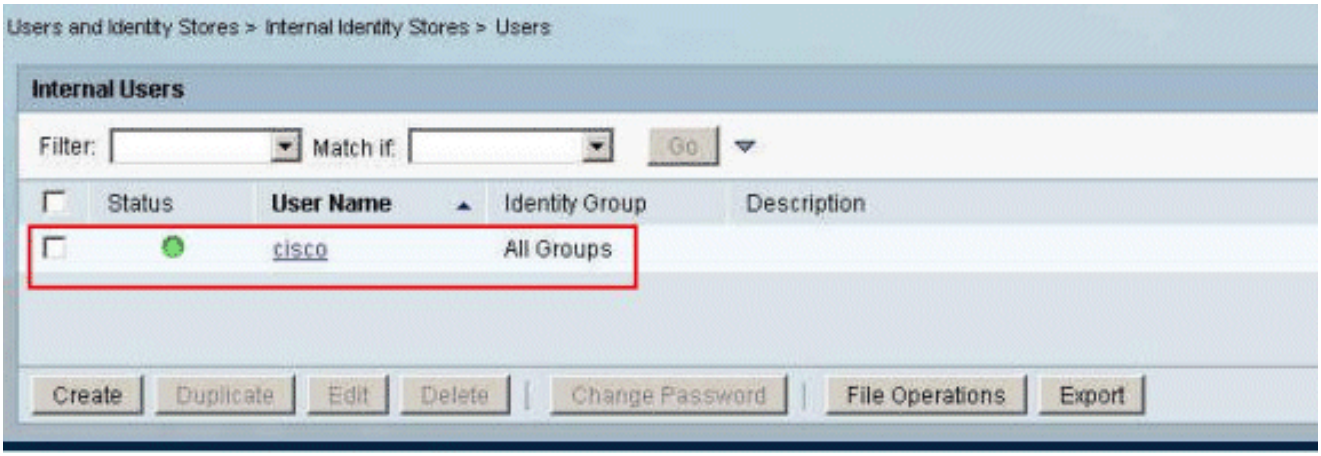
4. أخترت مستعمل ومخازن هويةدخلي هوية يخزنمستعمل، وطقطقة يخلق in order to خلقت مستعمل في القاعدة معطيات محلي من ال ACS ل VPN صحة هوية.



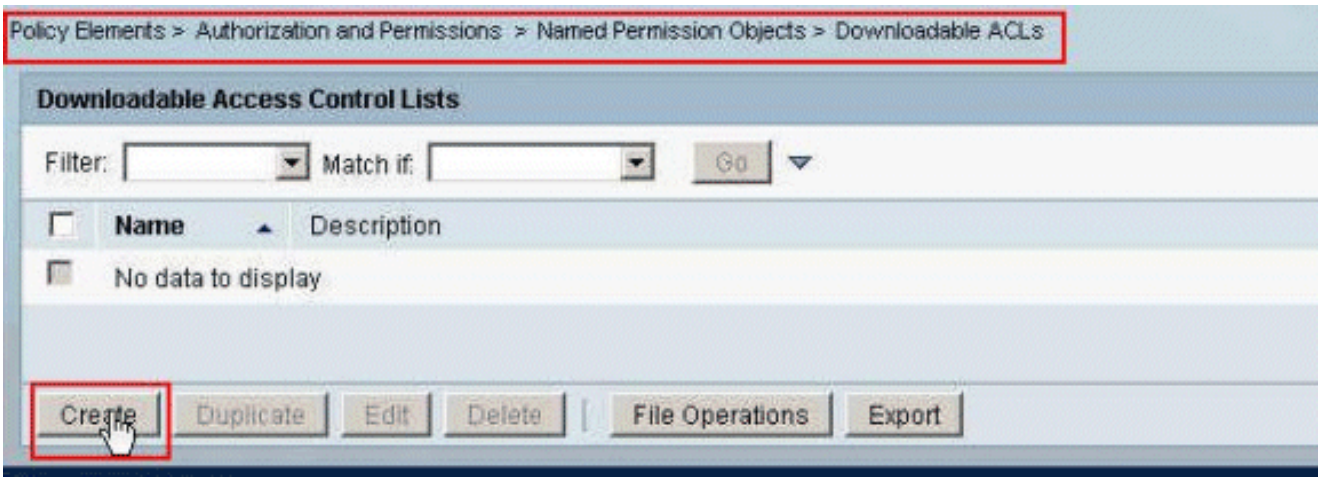
5. أدخل اسم المستخدم Cisco. حدد نوع كلمة المرور كمستخدمين داخليين، وأدخل كلمة المرور (Cisco123، في هذا المثال). قم بتأكيد كلمة المرور، وانقر إرسال.



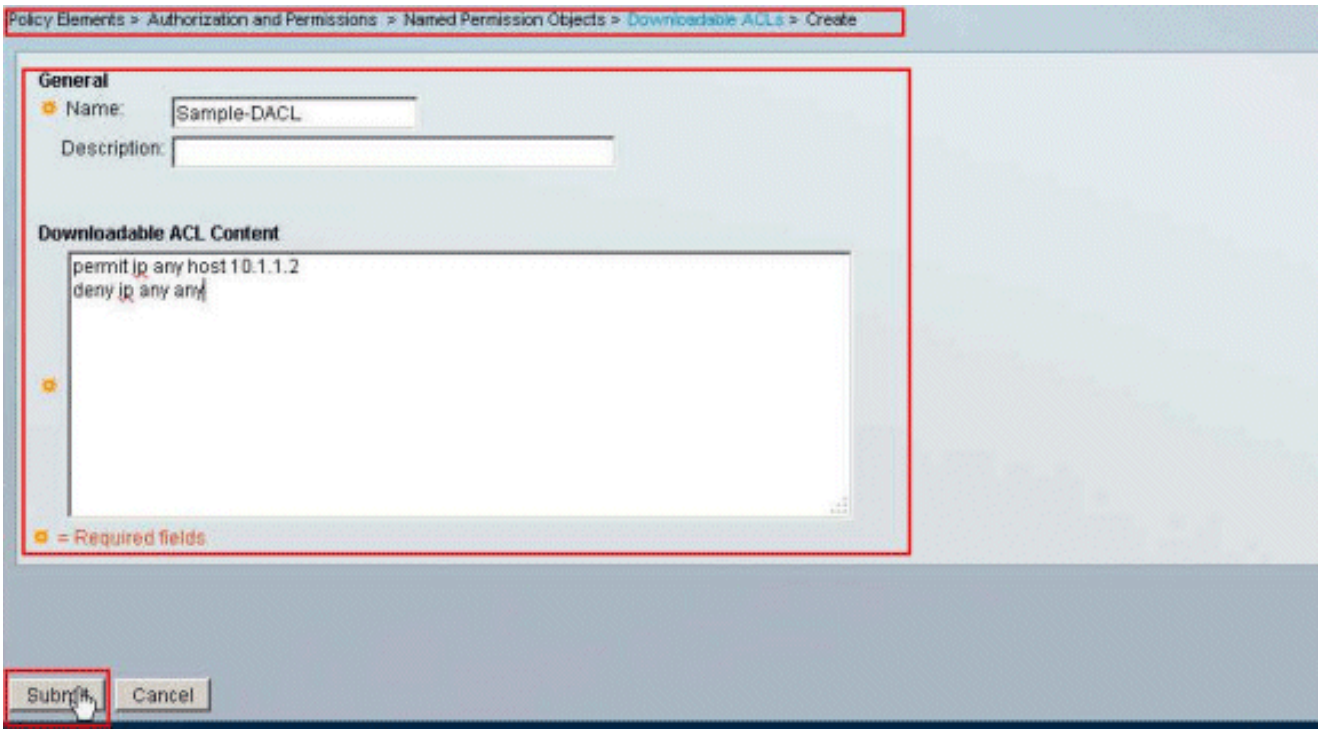
6. تم إنشاء المستخدم cisco بنجاح.



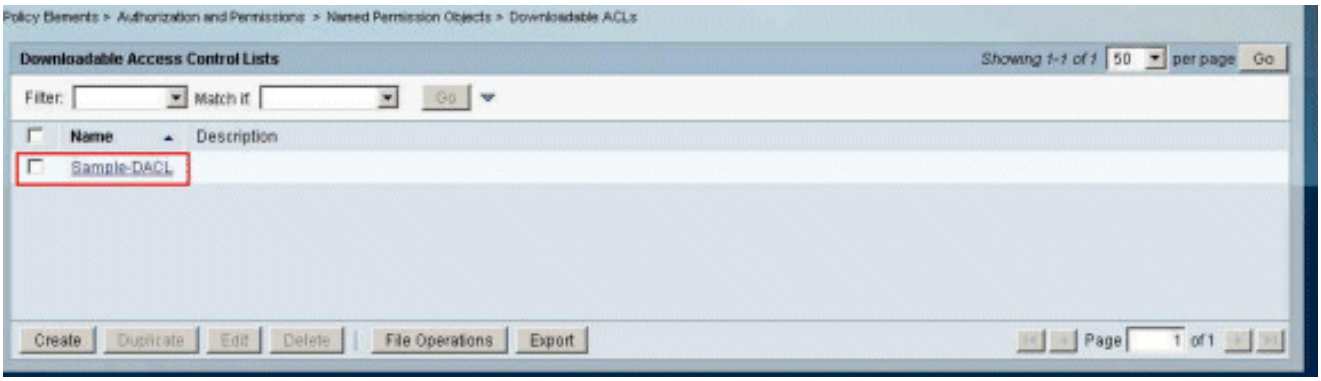
7. لإنشاء قائمة تحكم في الوصول (ACL) قابلة للتنزيل، أختر عناصر النهج > قوائم التحكم في الوصول (ACL) > كائنات الأذونات المسماة > التفويض والأذونات > القابلة للتنزيل، وانقر فوق إنشاء.



8. توفير اسم قائمة التحكم في الوصول (ACL) القابلة للتنزيل، بالإضافة إلى محتوى قائمة التحكم في الوصول (ACL). انقر على إرسال.

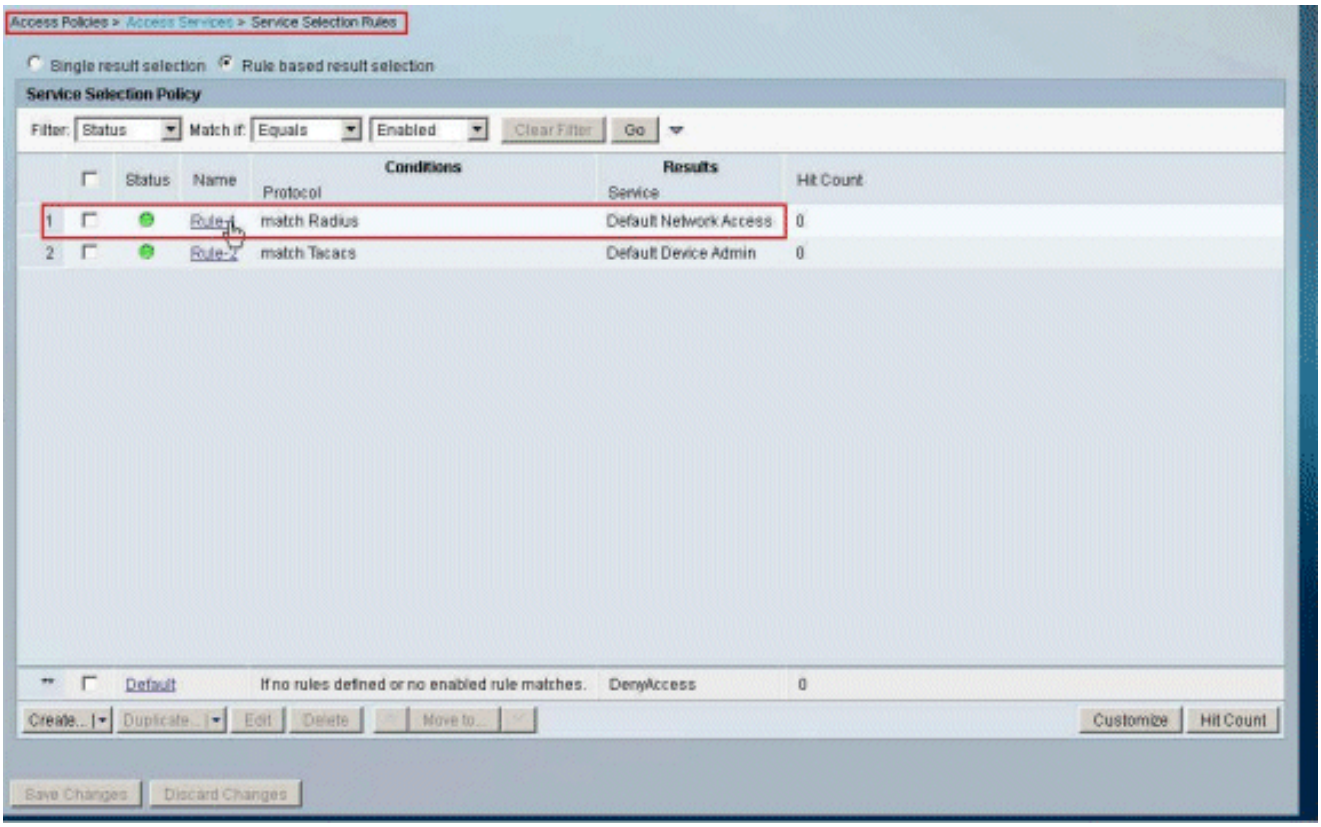


9. يتم إنشاء قائمة التحكم في الوصول (ACL) القابلة للتنزيل نموذج DACL بنجاح.

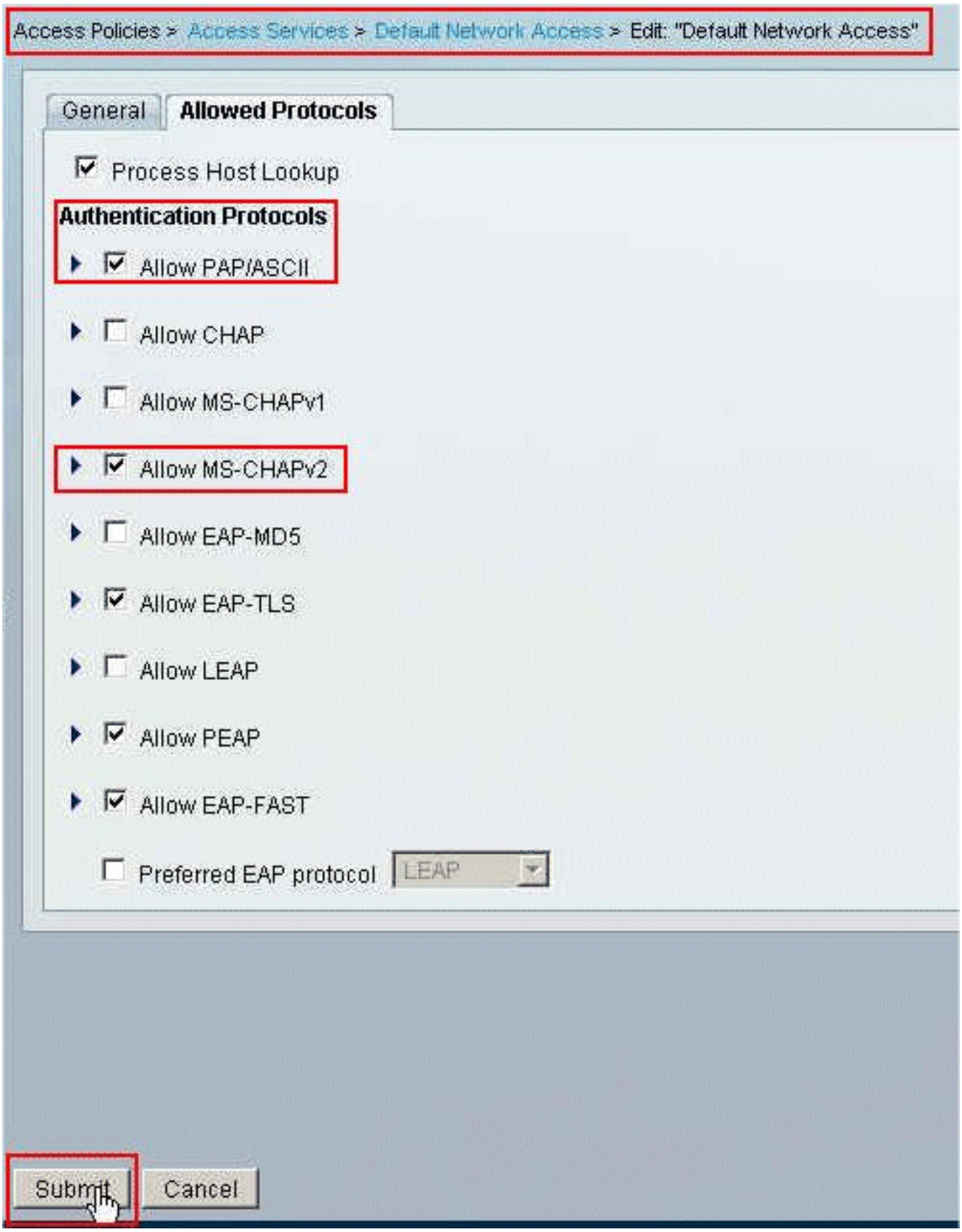


10. أخترت in order to شكلت Access-Policy for VPN صحة هوية، منفذ سياسة>منفذ خدمات>خدمة>خدمة تحديد قاعدة، وحددت أي خدمة خدمة تخدم إلى بروتوكول RADIUS. في هذا

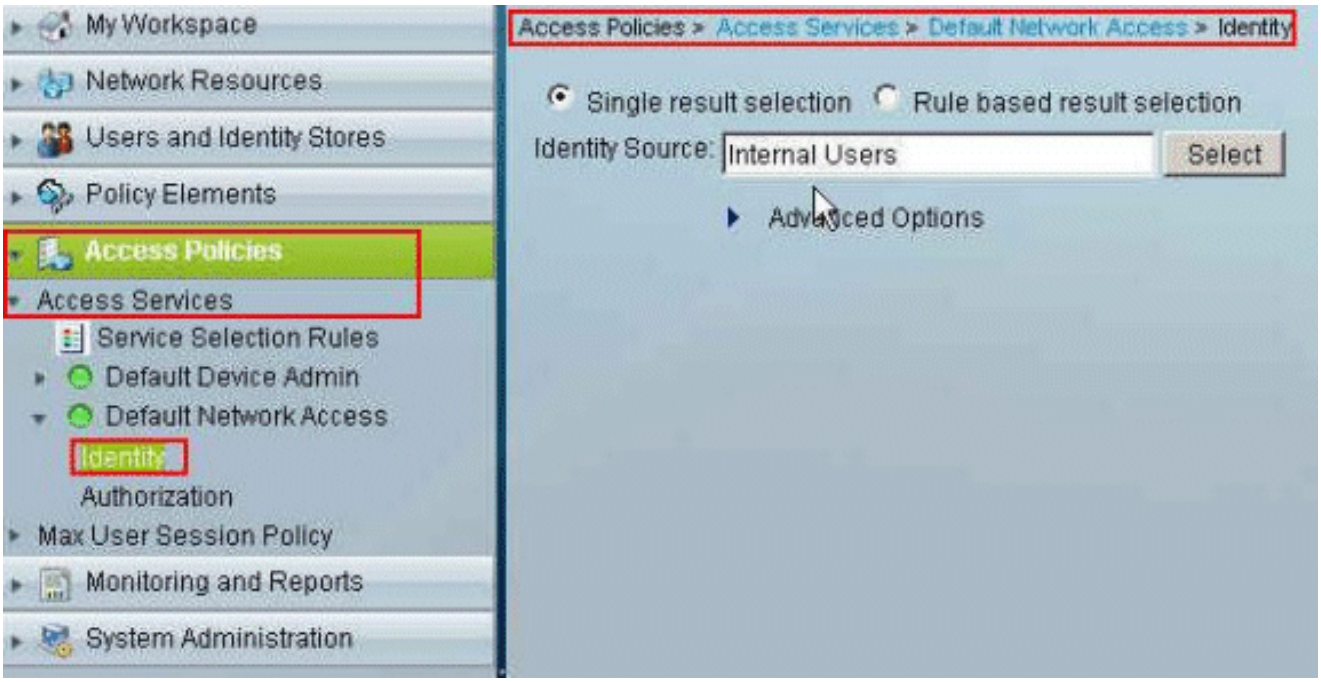
المثال، تتطابق القاعدة 1 مع RADIUS، وسيلبي الوصول إلى الشبكة الافتراضي طلب RADIUS.



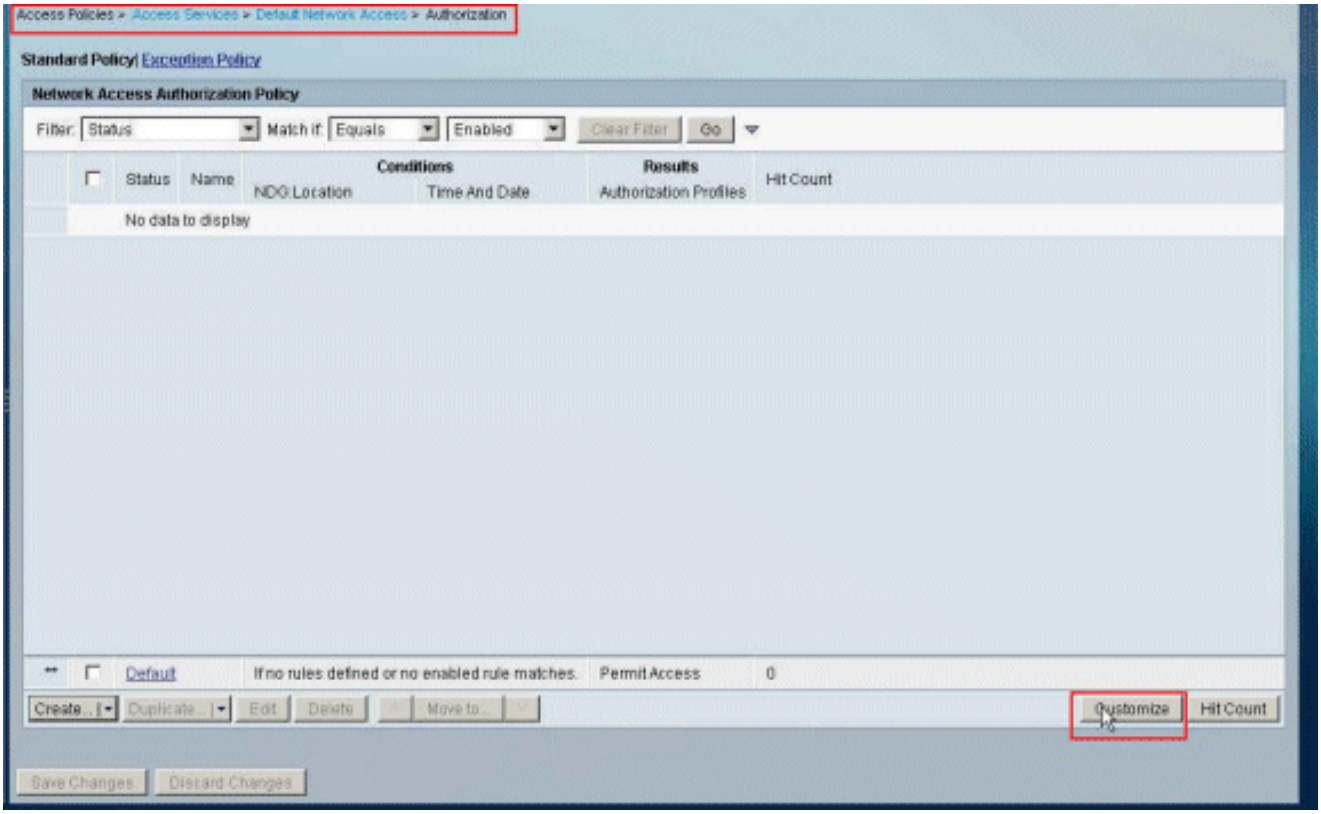
11. أختر خدمة الوصول المحددة من الخطوة 10. في هذا المثال، يتم إستخدام الوصول الافتراضي إلى الشبكة. أختر علامة التبويب البروتوكولات المسموح بها، وتأكد من تحديد السماح ب PAP/ASCII والسماح ب MS-CHAPv2. انقر فوق إرسال.



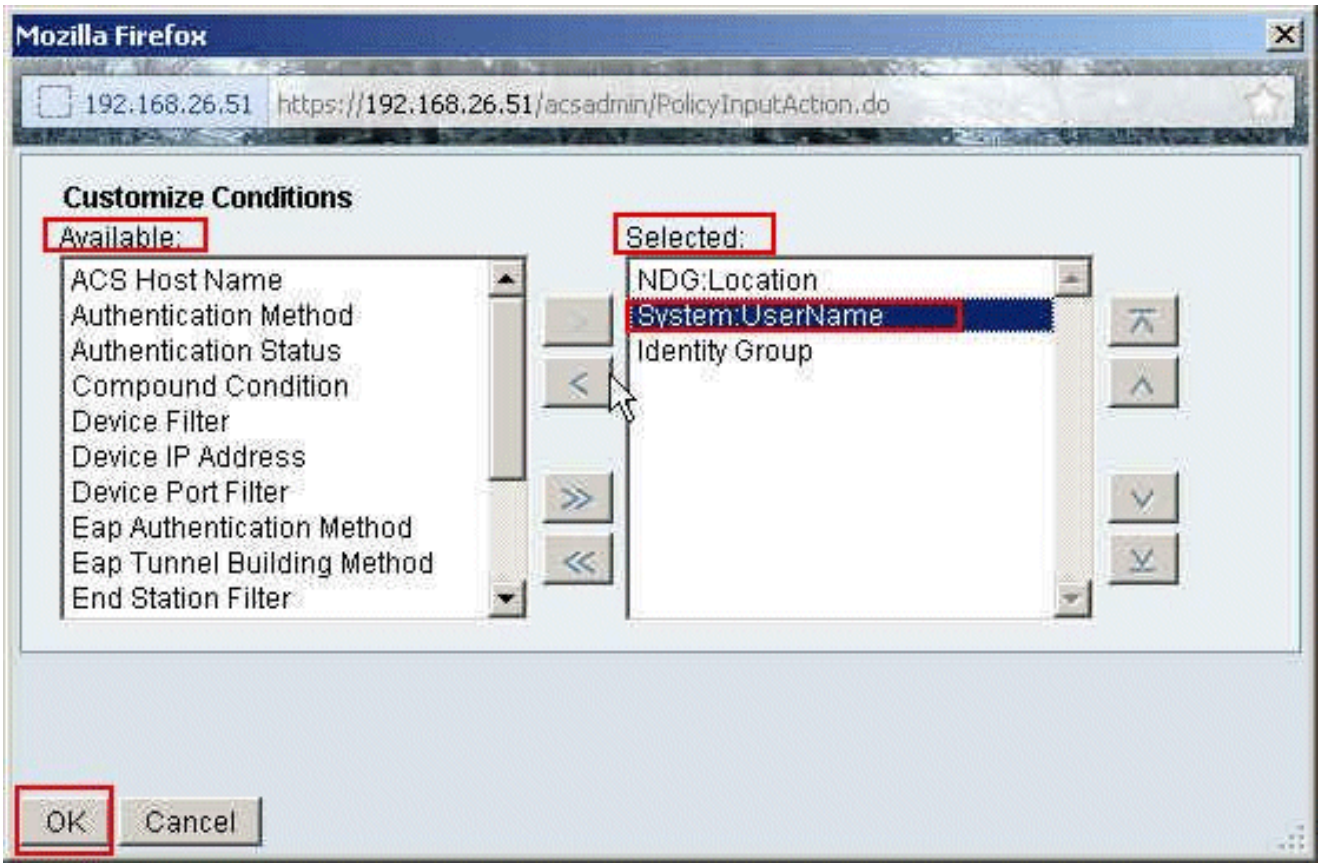
12. انقر فوق قسم الهوية في خدمات Access، وتأكد من تحديد المستخدمين الداخليين كمصدر هوية. في هذا المثال، أخذنا الوصول الافتراضي للشبكة.



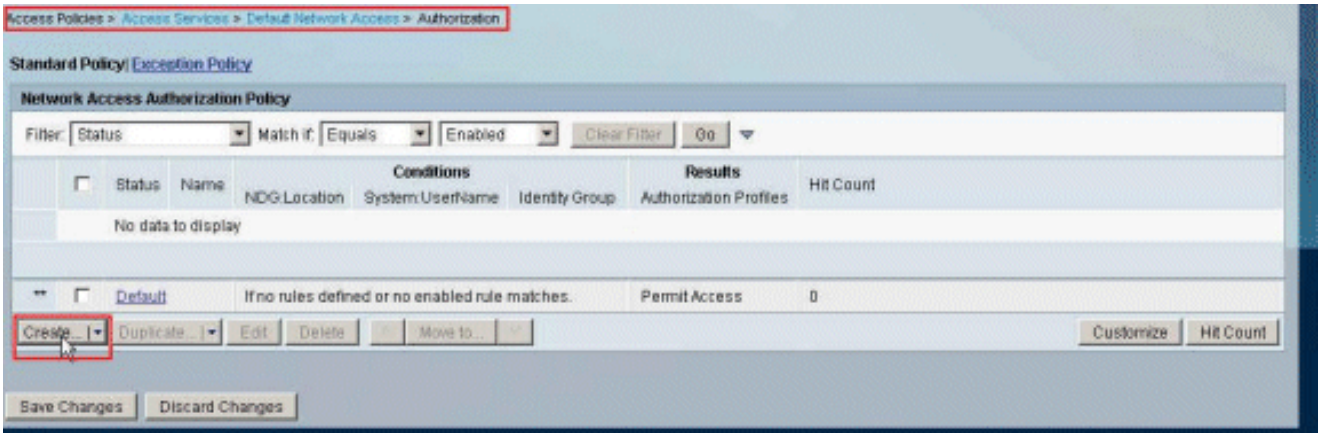
13. أختر سياسات الوصول > خدمات الوصول > الوصول الافتراضي للشبكة > التفويض، وانقر فوق تخصيص.



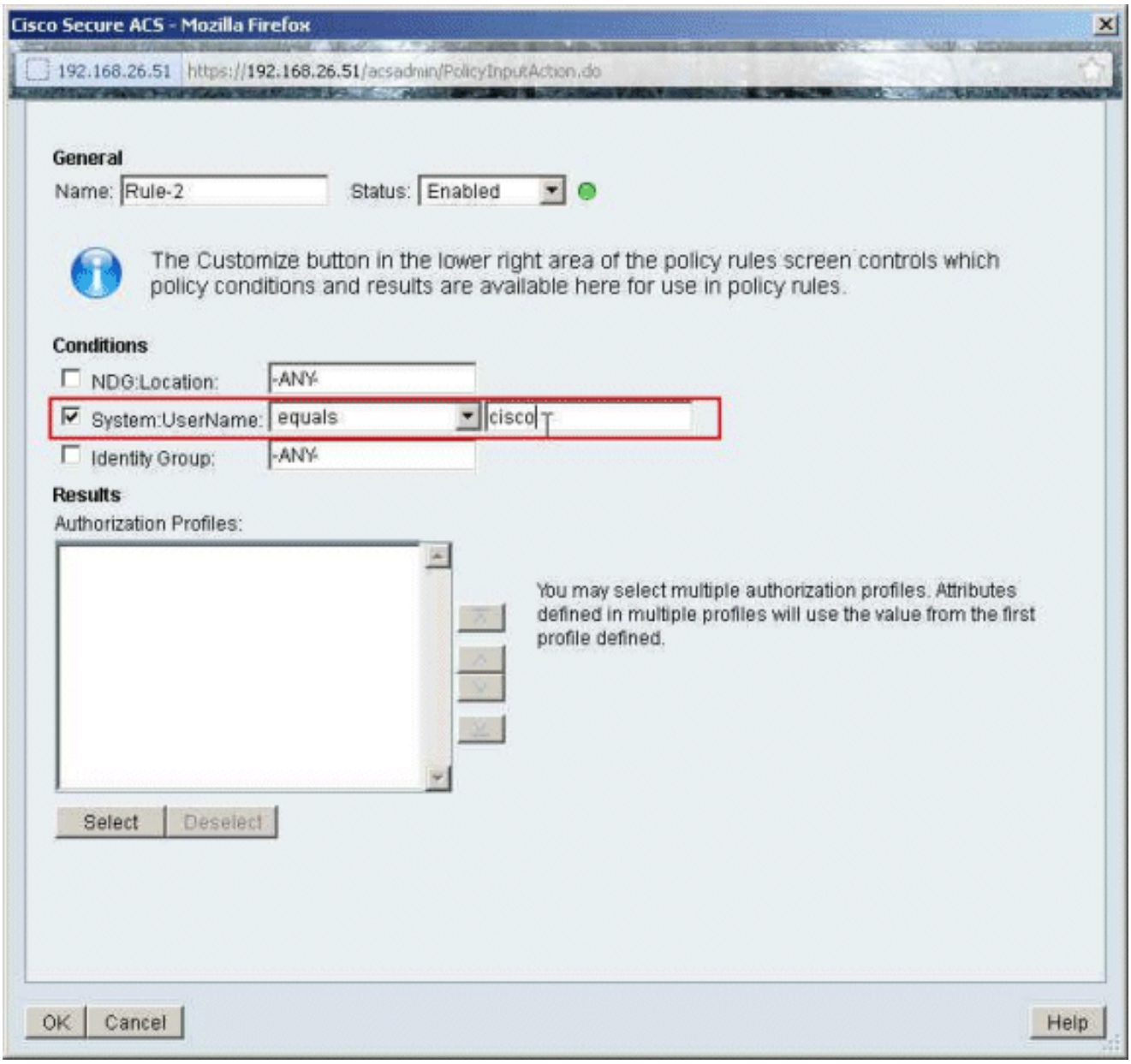
14. نقل System:UserName من العمود المتوفر إلىالعمود المحدد، وانقر فوق OK.



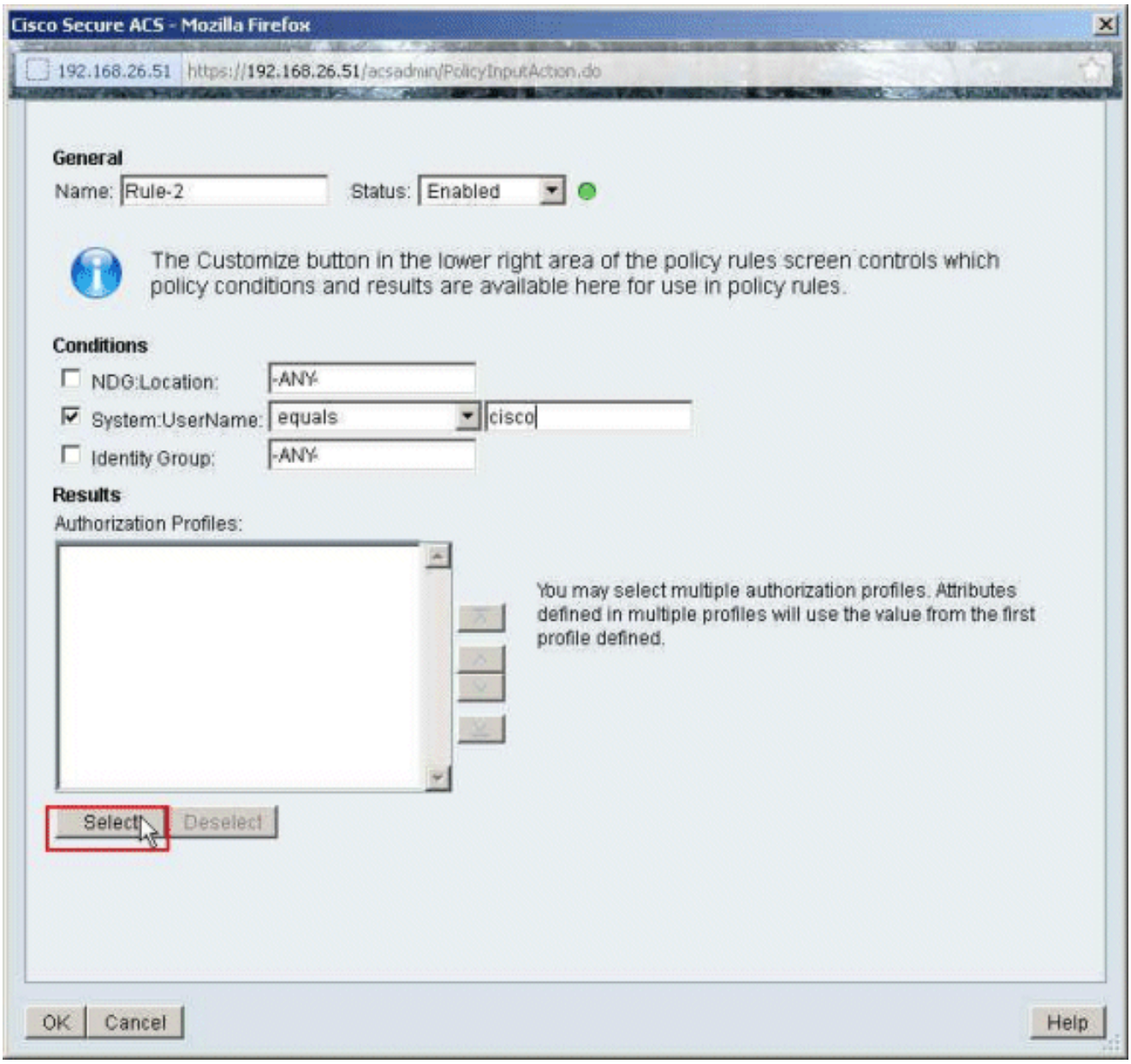
15. انقر فوق إنشاء لإنشاء قاعدة جديدة.



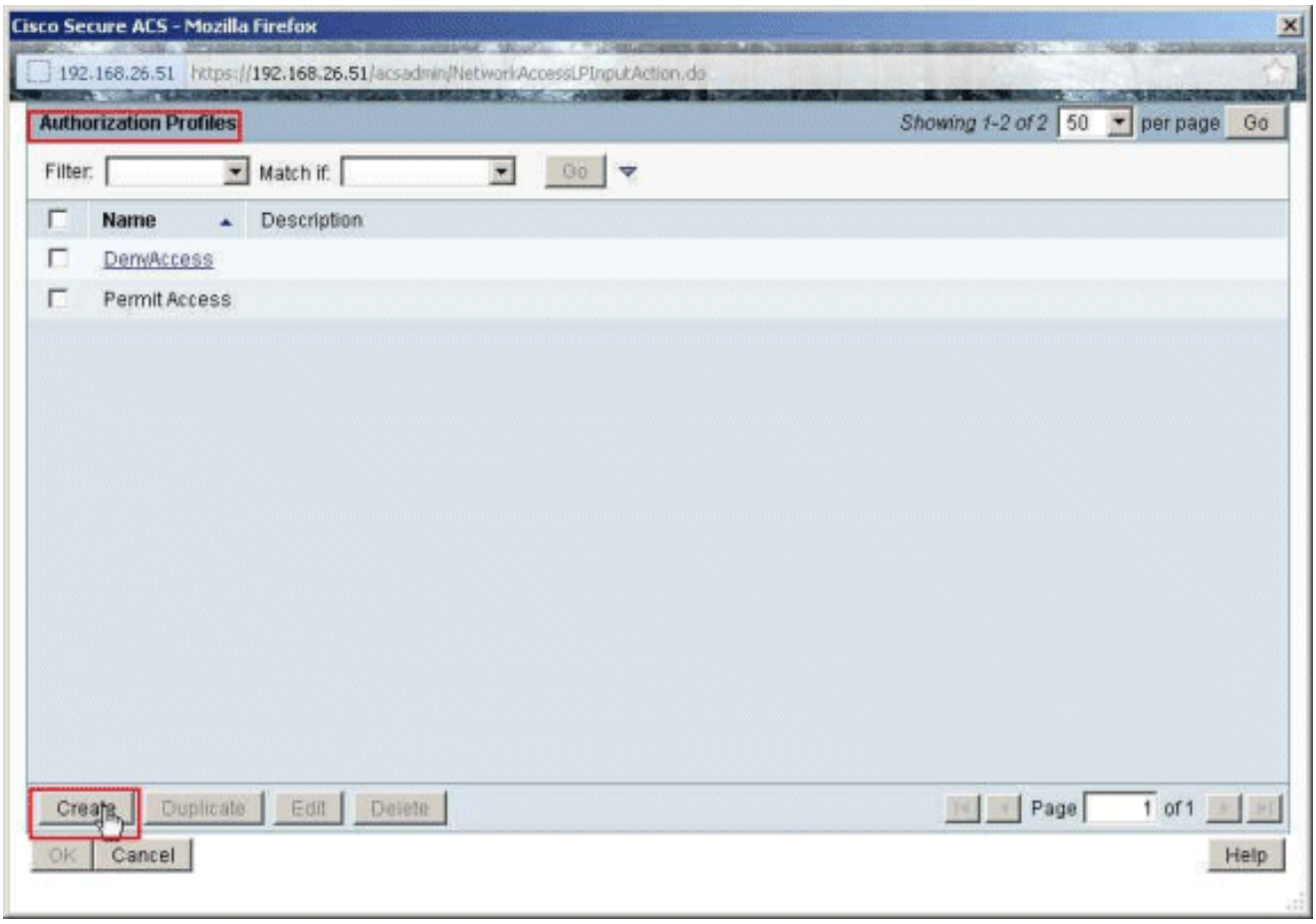
16. تأكد من تحديد خانة الاختيار المجاورة لـ System:UserName، واختر يساوي من القائمة المنسدلة، وأدخل اسم المستخدم Cisco.



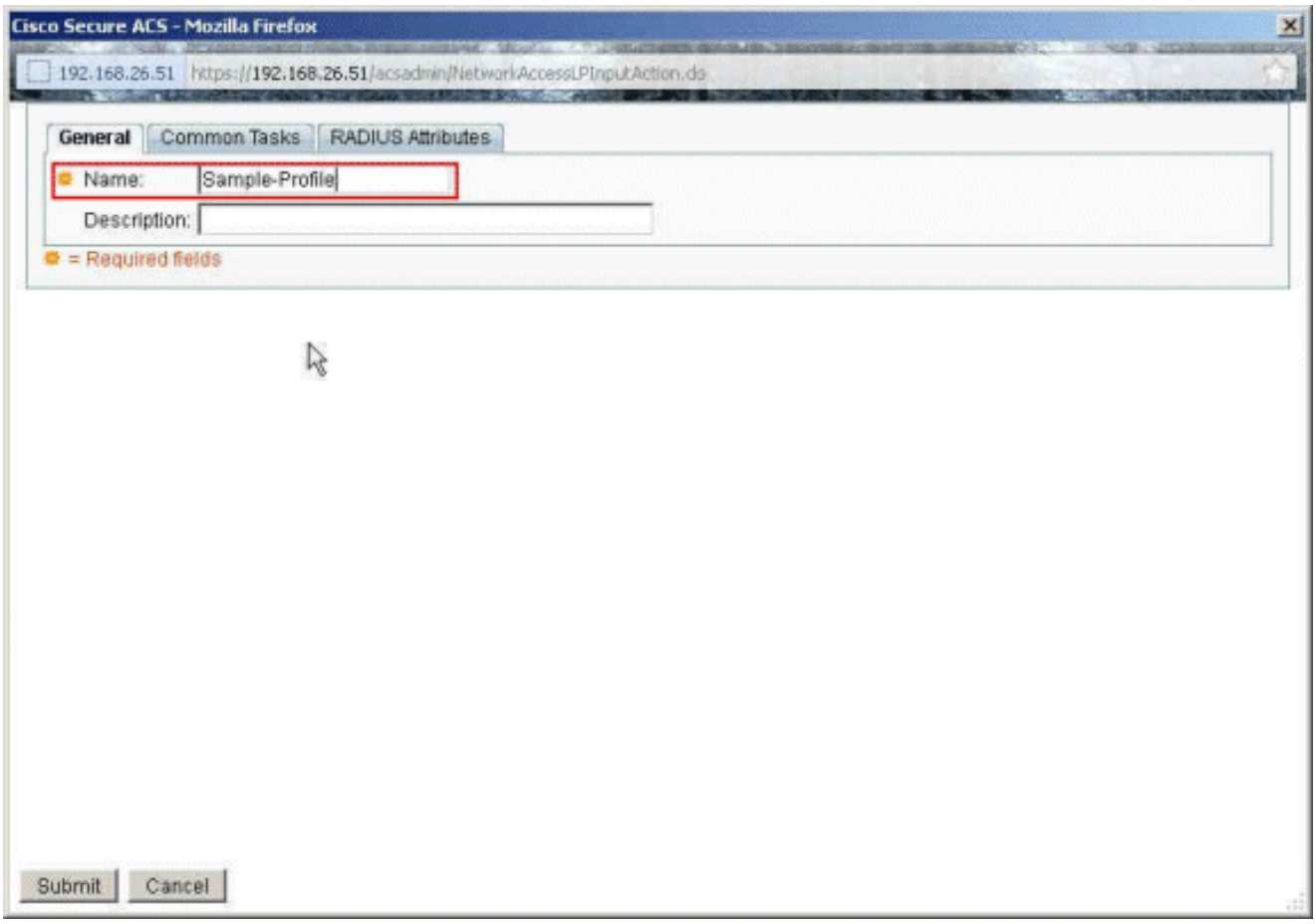
17. انقر فوق تحديد.



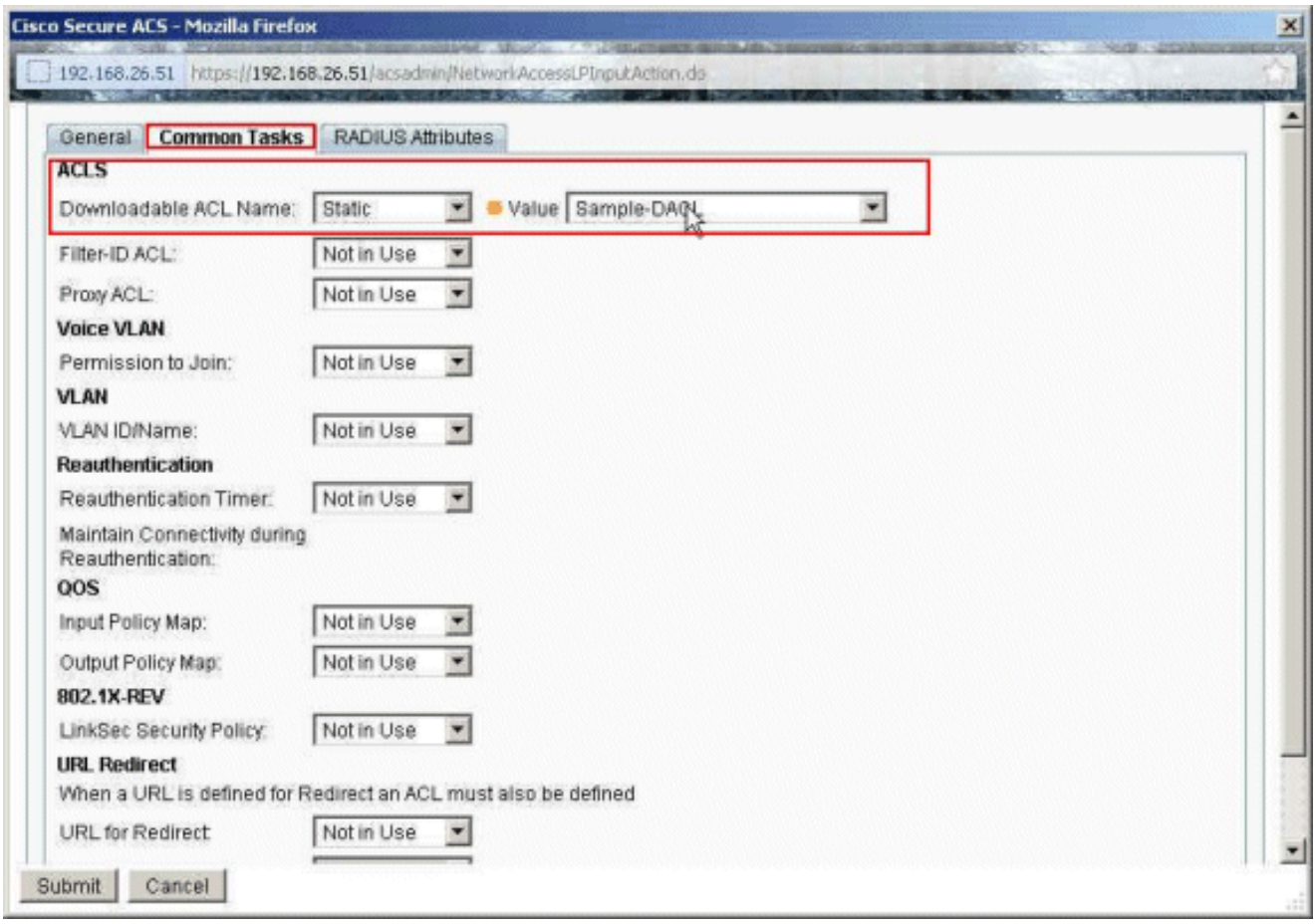
18. انقر على إنشاء لإنشاء ملف تعريف تخويل جديد.



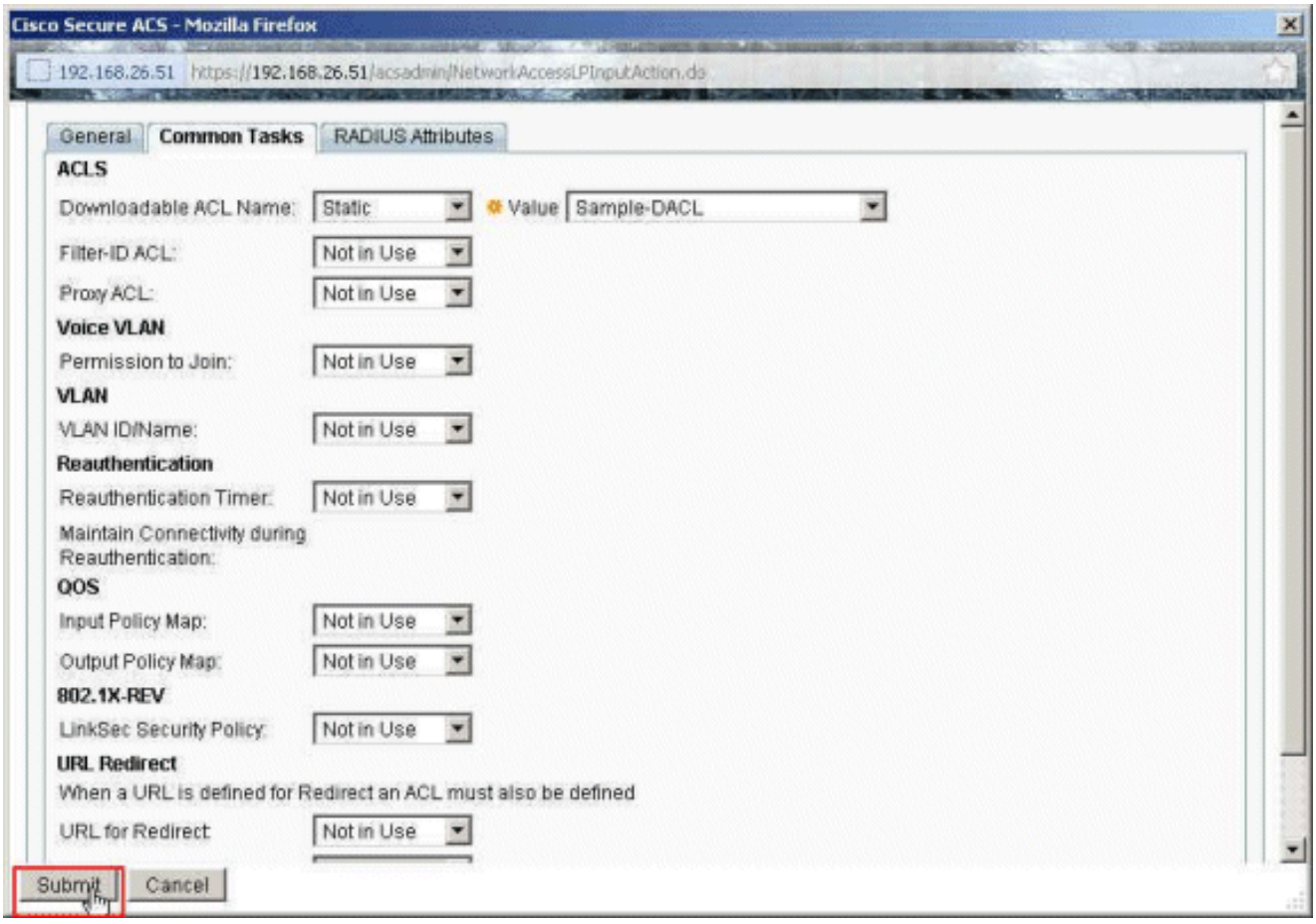
19. قم بتوفير اسم لملف تعريف التخويل. يتم إستخدام نموذج ملف التعريف في هذا المثال.



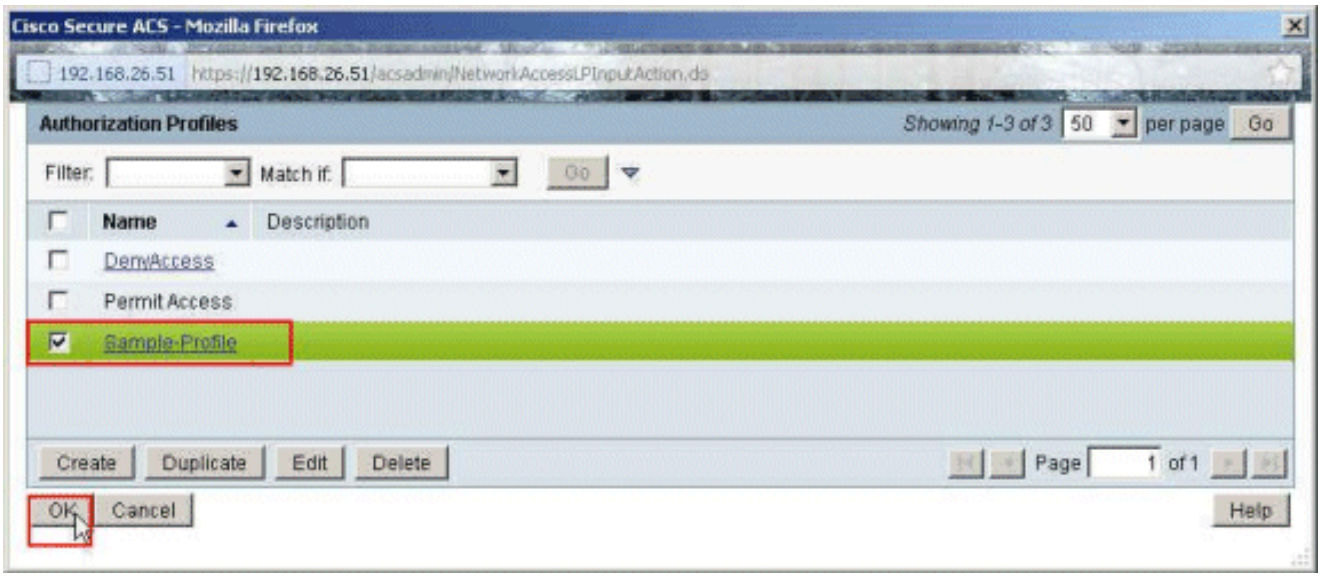
20. أختر علامة التبويب مهام مشتركة، وحدد ثابت من القائمة المنسدلة لاسم قائمة التحكم في الوصول (ACL) القابل للتنزيل. أختر DACL الذي تم إنشاؤه حديثا (نموذج - DACL) من القائمة المنسدلة للقيمة.



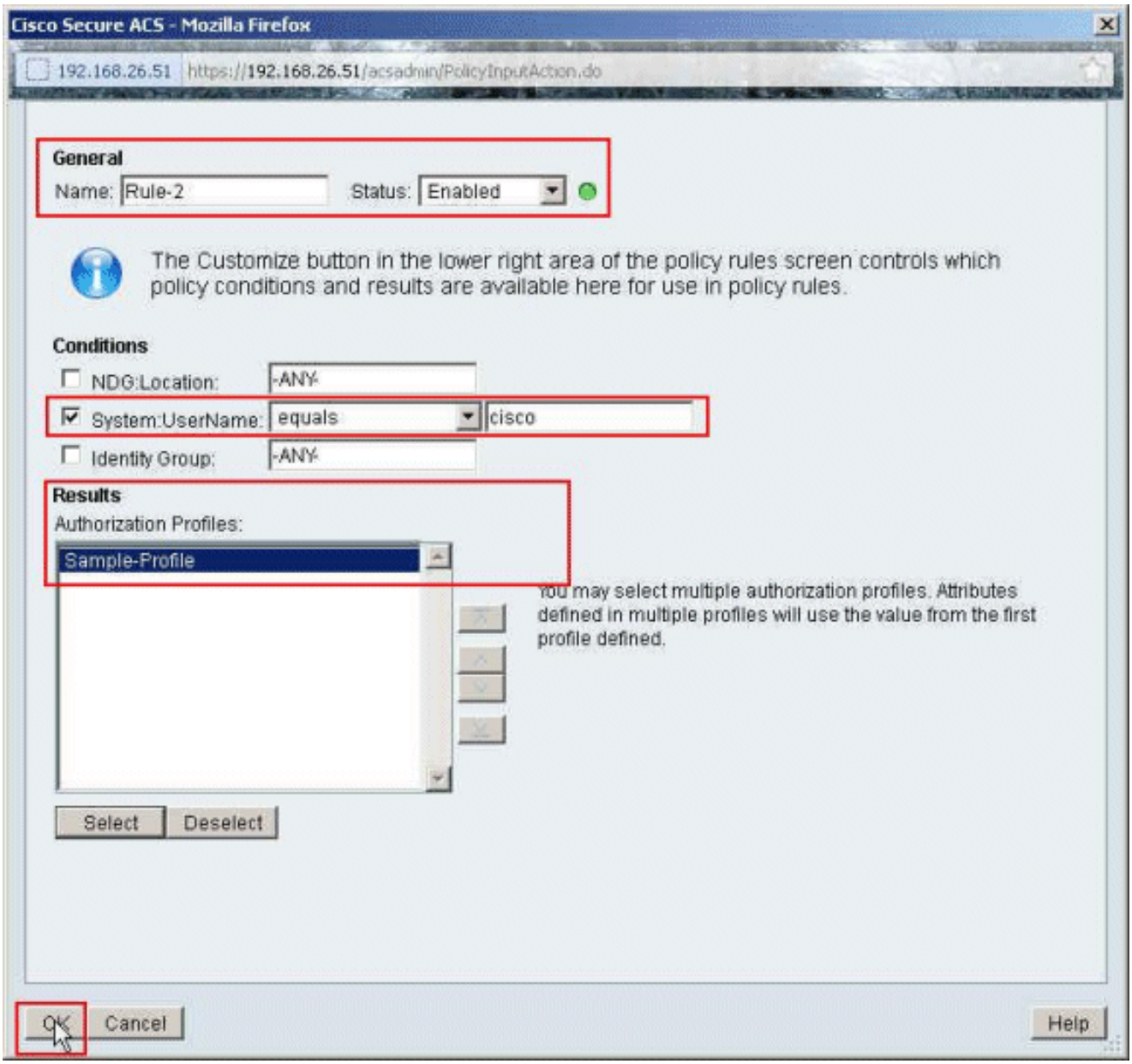
21. انقر على إرسال.



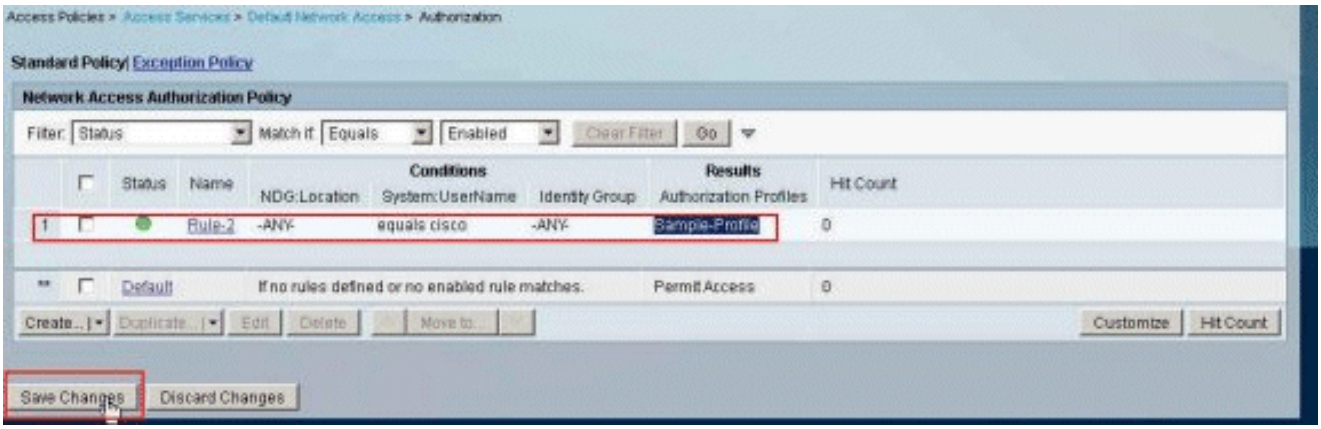
22. تأكد من أن خانة الاختيار المجاورة لنموذج ملف التعريف (ملف تعريف التخويل الذي تم إنشاؤه حديثا) محددة، وانقر موافق.



23. بمجرد التحقق من تحديد نموذج التوصيف الذي تم إنشاؤه حديثا في حقل توصيفات التخويل، انقر على موافق.



تحقق من إنشاء القاعدة الجديدة (القاعدة-2) باستخدام System:UserName يساوي24. شروط Cisco وSample-Profile كنتيجة لذلك. انقر فوق حفظ التغييرات. تم إنشاء القاعدة 2 بنجاح.



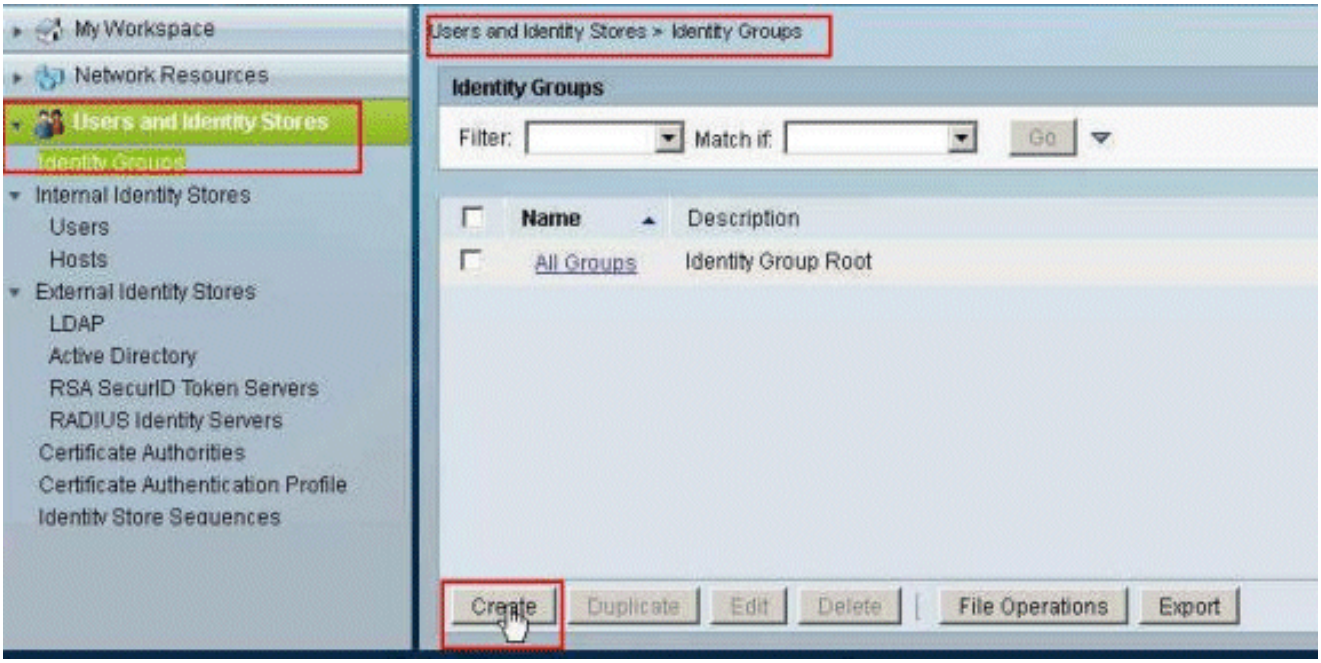
تكوين ACS لقائمة التحكم في الوصول (ACL) القابلة للتنزيل للمجموعة

أكمل الخطوات من 1 إلى 12 من تكوين ACS لقائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم الفردي وأجرى هذه الخطوات لتكوين قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمجموعة في Cisco ACS الآمن.

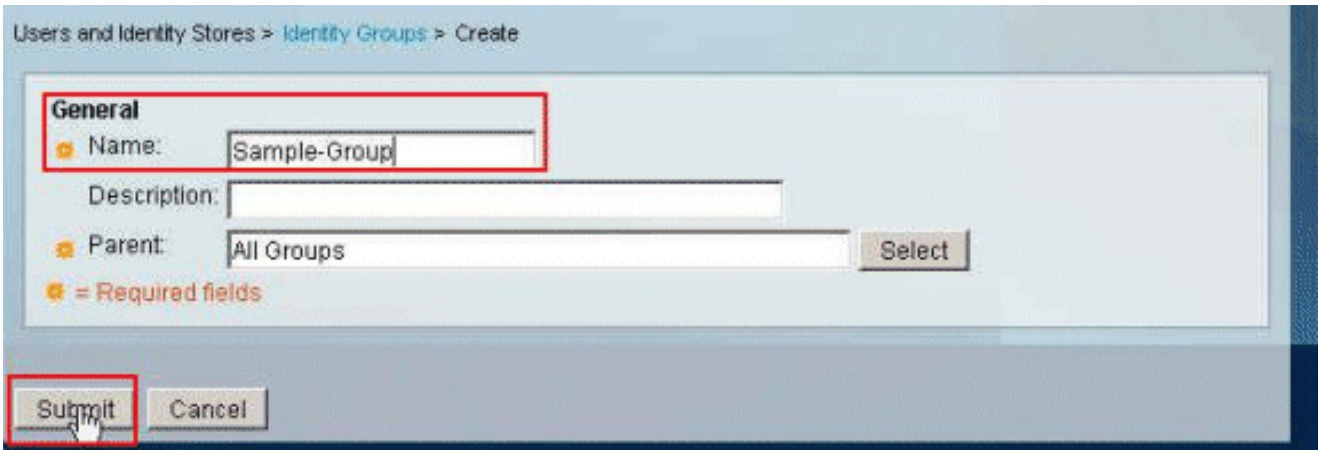
في هذا المثال، ينتمي مستخدم IPsec VPN "cisco" إلى مجموعة العينة.

يقوم مستخدم مجموعة العينة Cisco بالمصادقة بنجاح، ويرسل خادم RADIUS قائمة وصول قابلة للتنزيل إلى جهاز الأمان. يمكن للمستخدم "cisco" الوصول إلى خادم 10.1.1.2 فقط ويرفض جميع الوصول الآخر. للتحقق من قائمة التحكم في الوصول (ACL)، ارجع إلى قسم قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم/المجموعة.

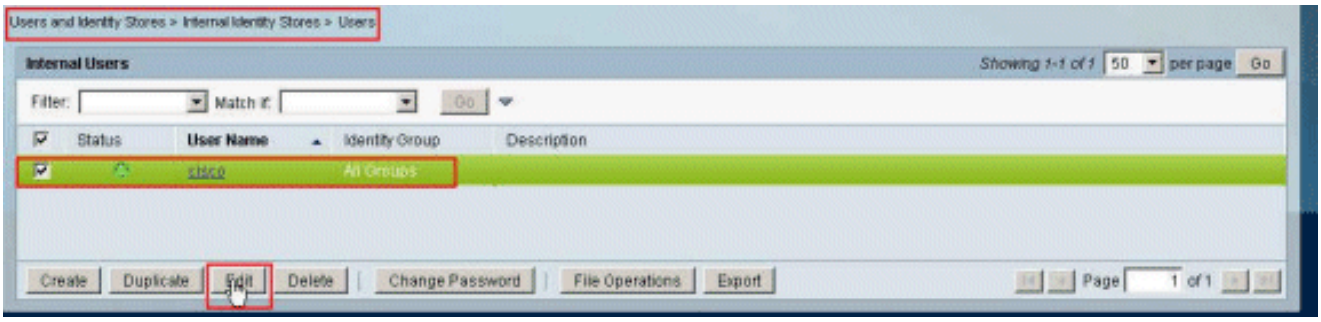
1. في شريط التنقل، انقر فوق المستخدمين ومخازن الهوية > مجموعات الهوية، وانقر فوق إنشاء لإنشاء مجموعة جديدة.



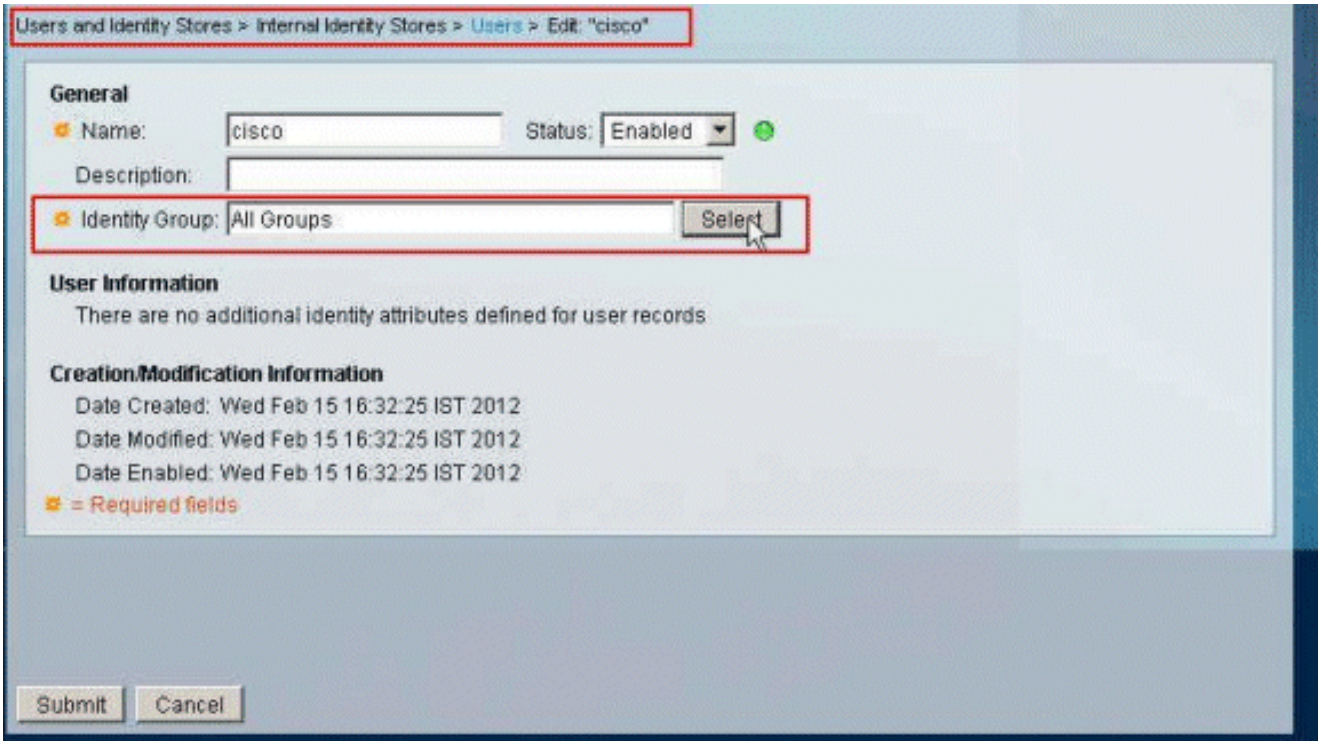
2. قم بتوفير اسم مجموعة (نموذج مجموعة)، وانقر إرسال.



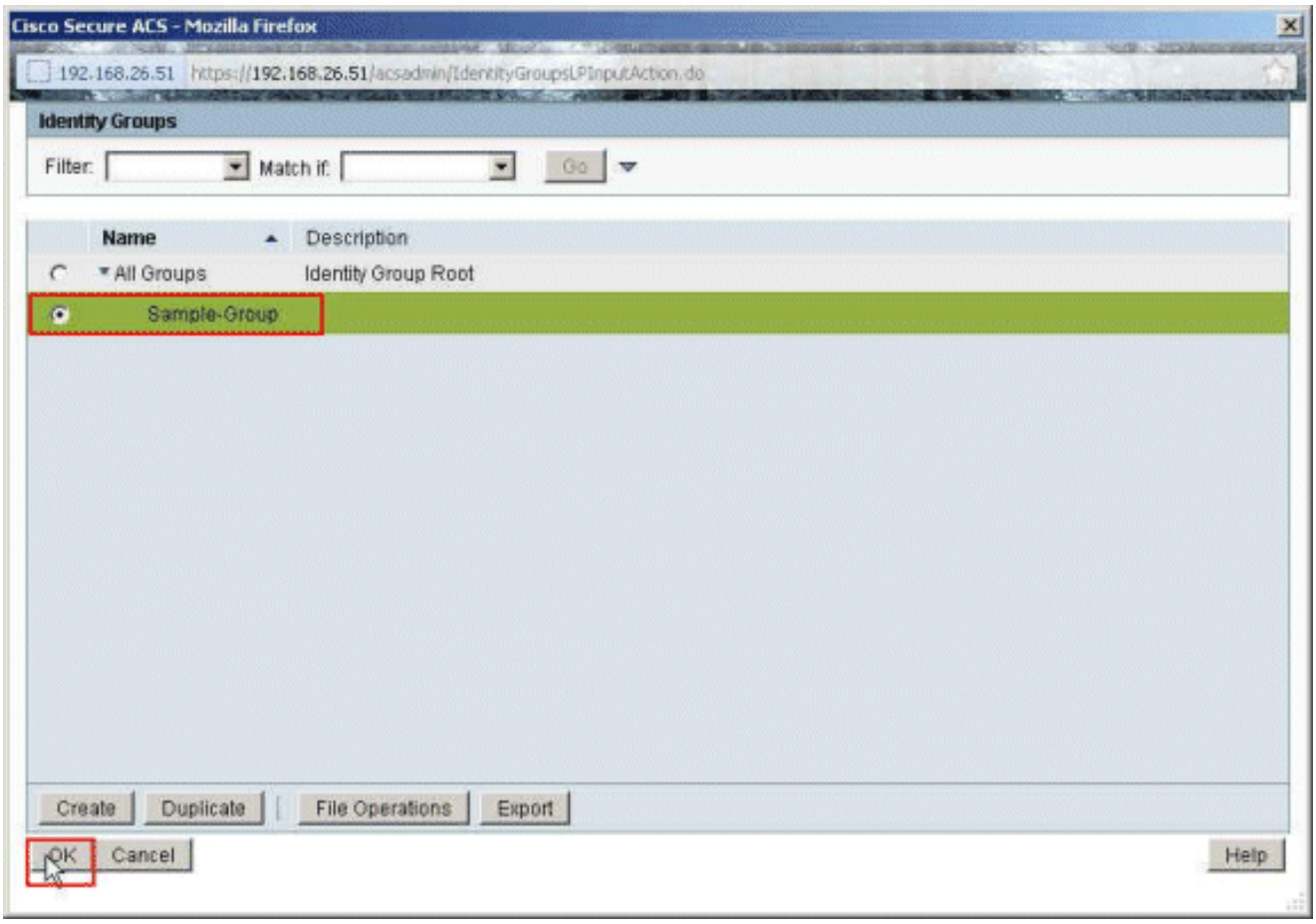
3. أختر مخازن هوية المستخدم>مخازن الهوية الداخلية>المستخدمين، وحدد المستخدم Cisco. انقر فوق تحرير لتغيير عضوية المجموعة لهذا المستخدم.



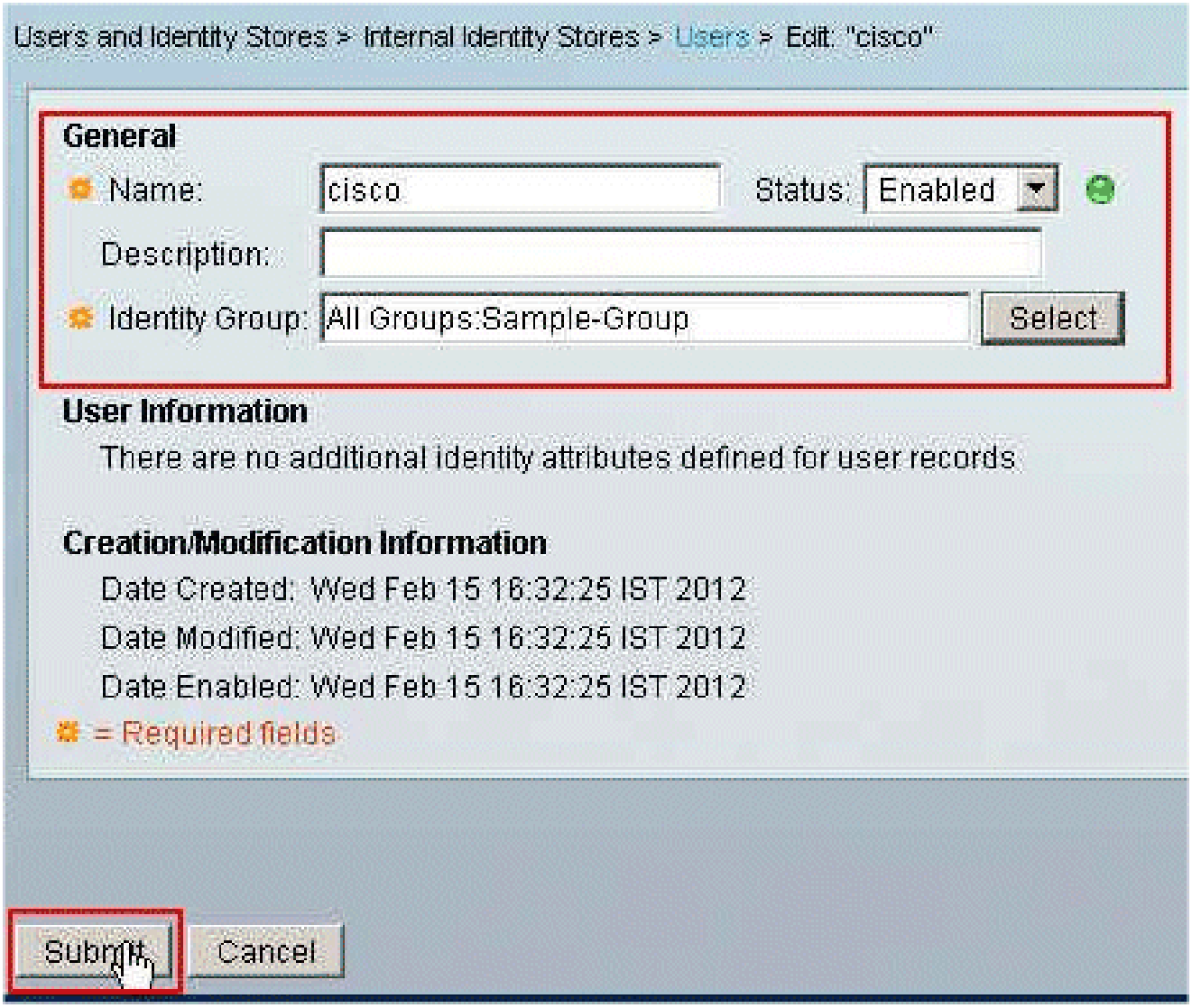
4. انقر فوق تحديد بجوار مجموعة الهوية.



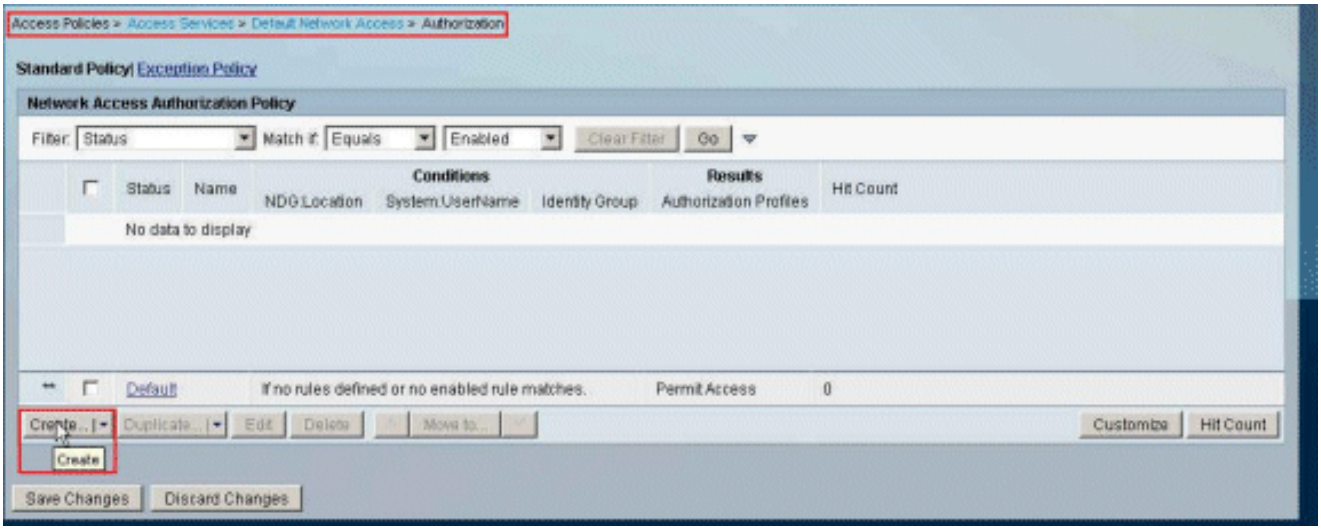
5. حدد المجموعة التي تم إنشاؤها حديثا (والتي هي مجموعة العينة)، وانقر موافق.



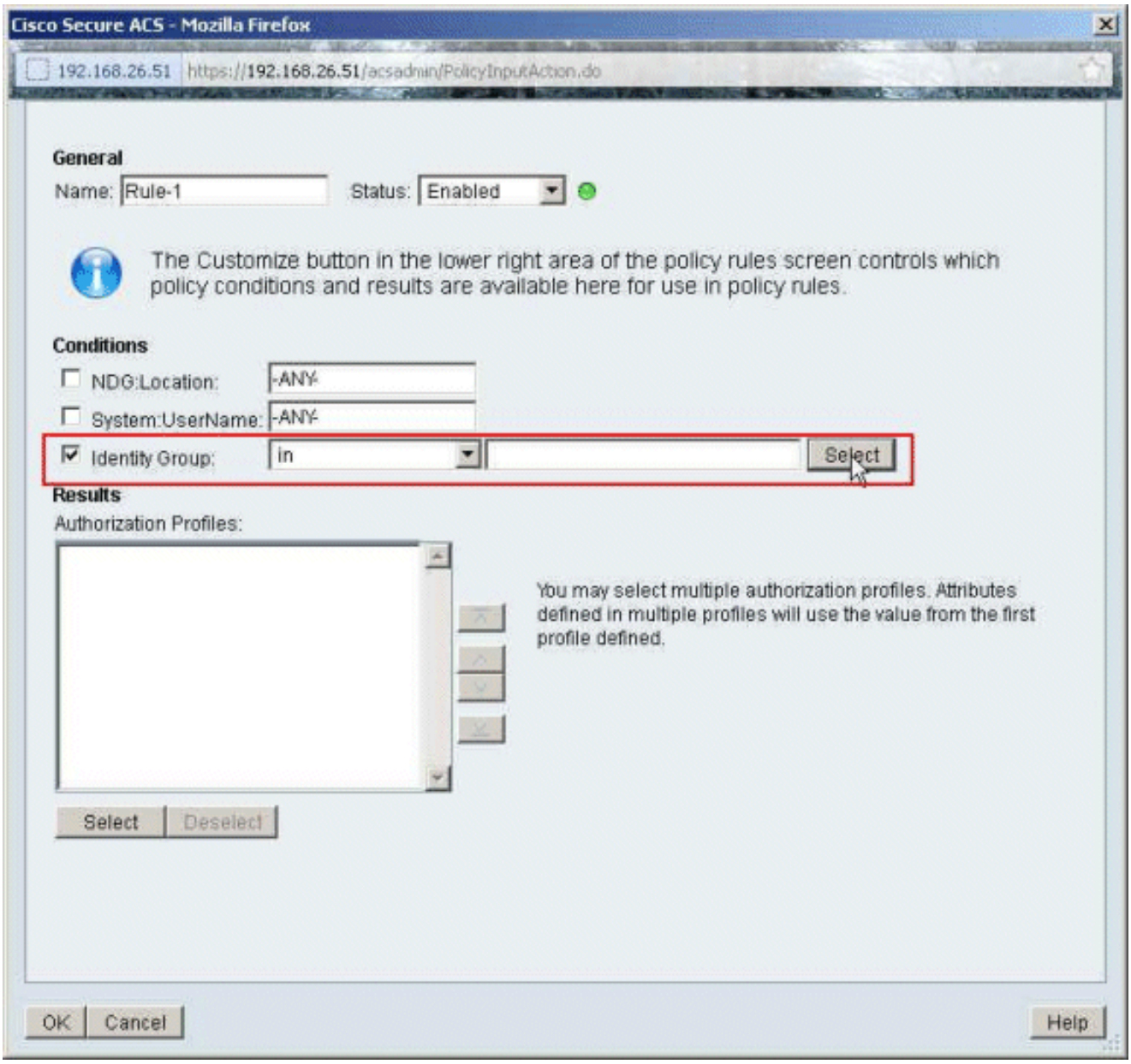
6. انقر على إرسال.



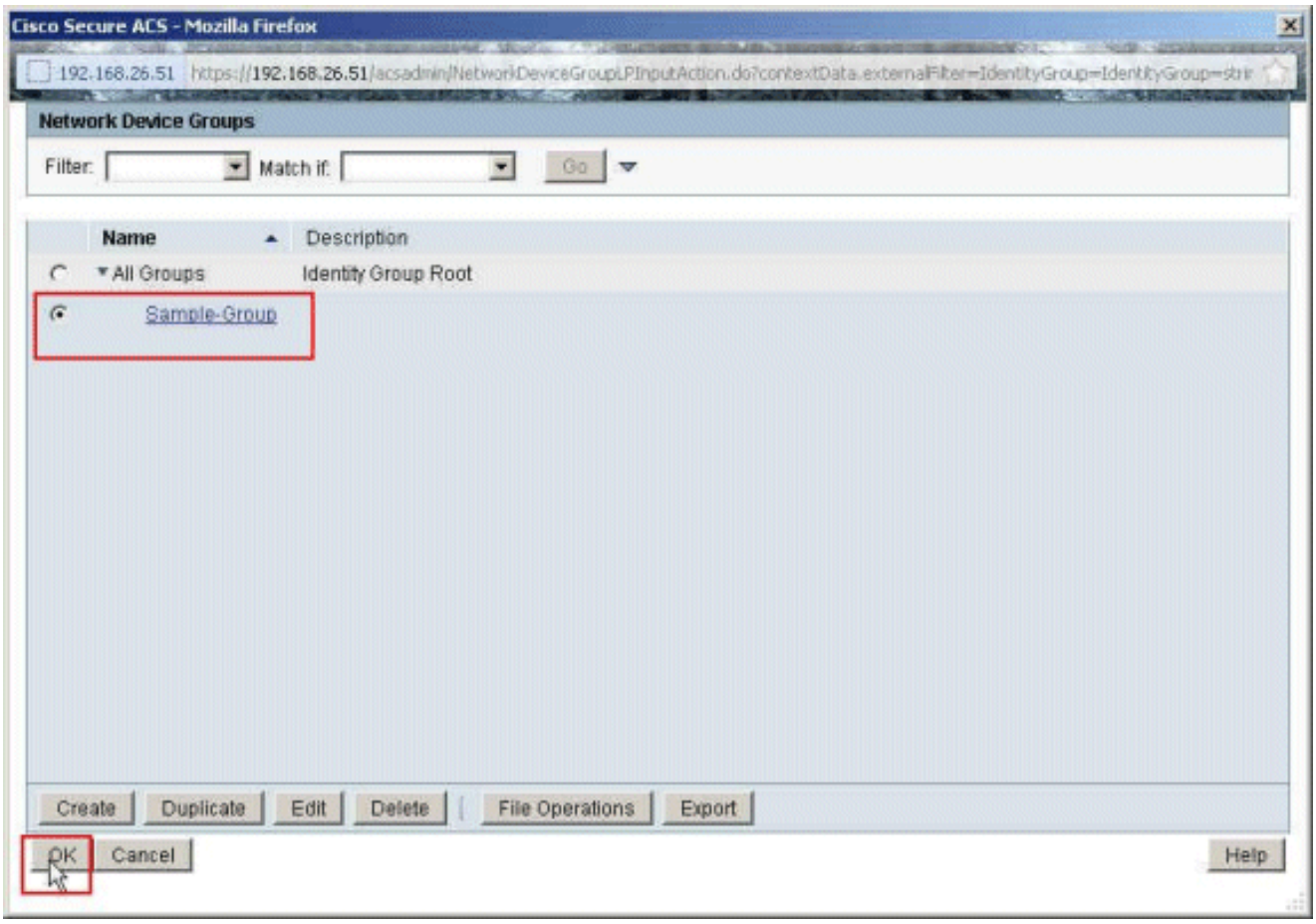
7. أختر سياسات الوصول > خدمات الوصول>الوصول الافتراضي إلى الشبكة التفويض، وانقر فوق إنشاء لإنشاء قاعدة جديدة.



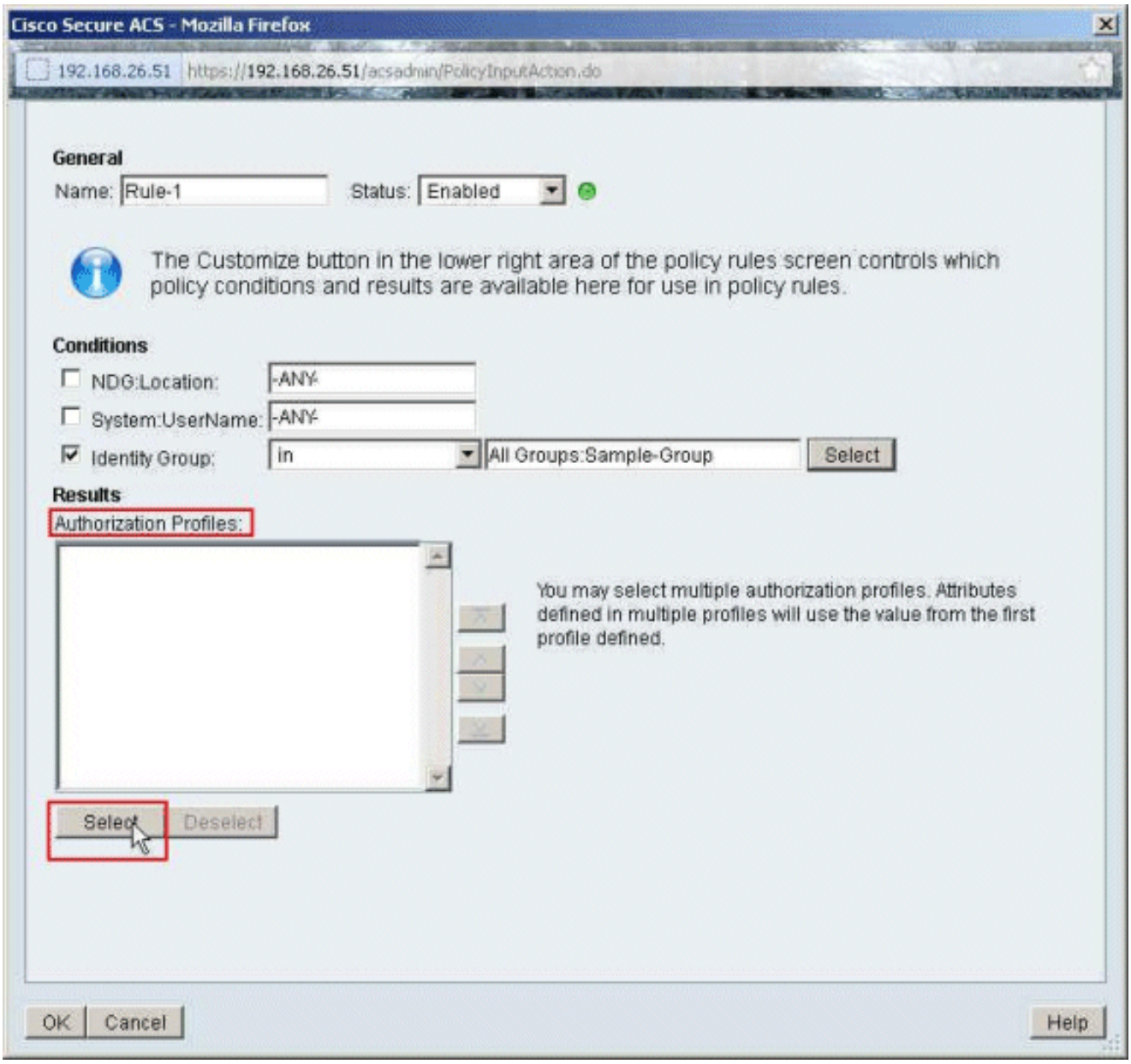
8. تأكد من أن خانة الاختيار المجاورة لمجموعة الهوية محددة، وانقر تحديد.



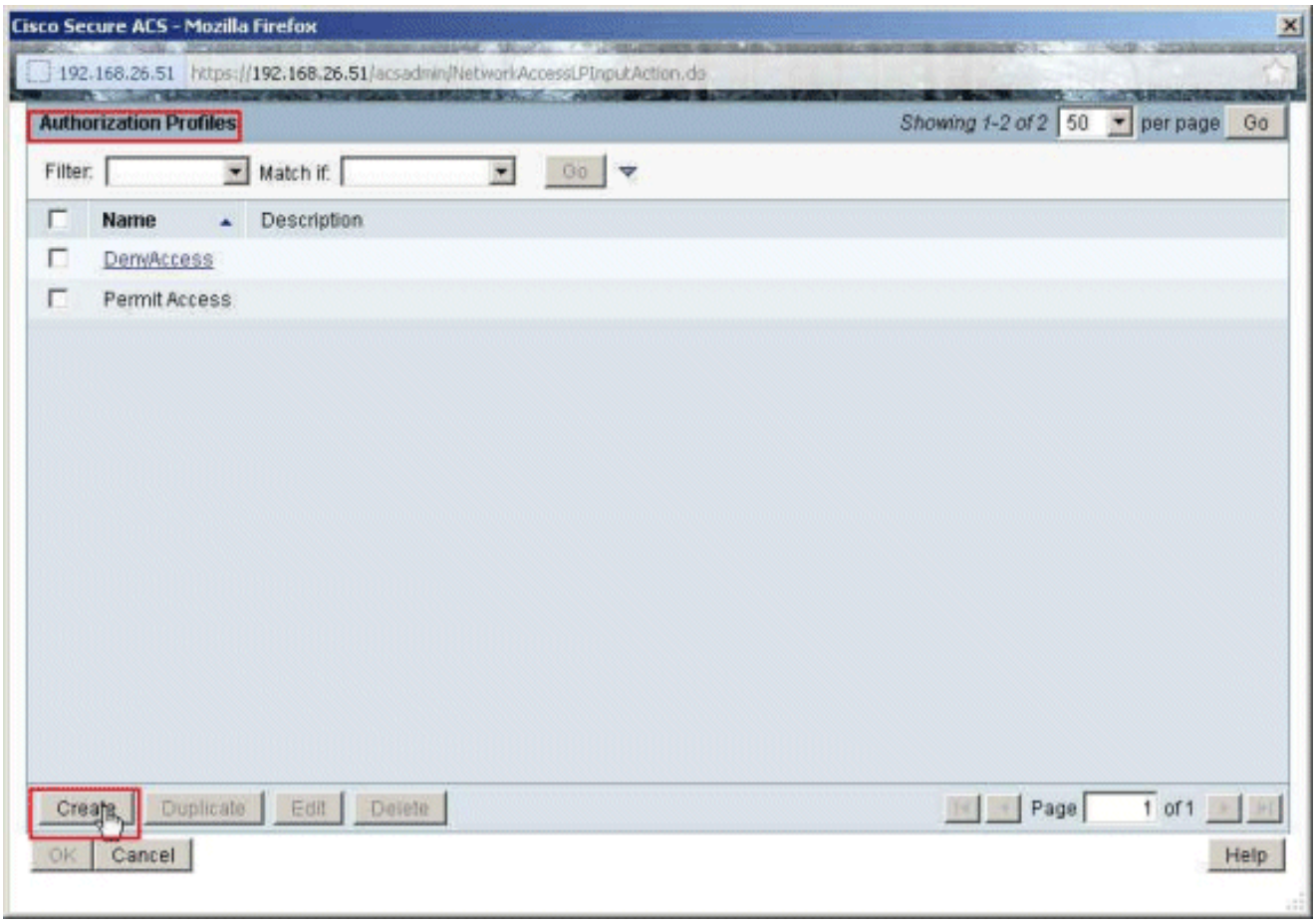
أخترت عينة مجموعة، وطقطقة ok.9.



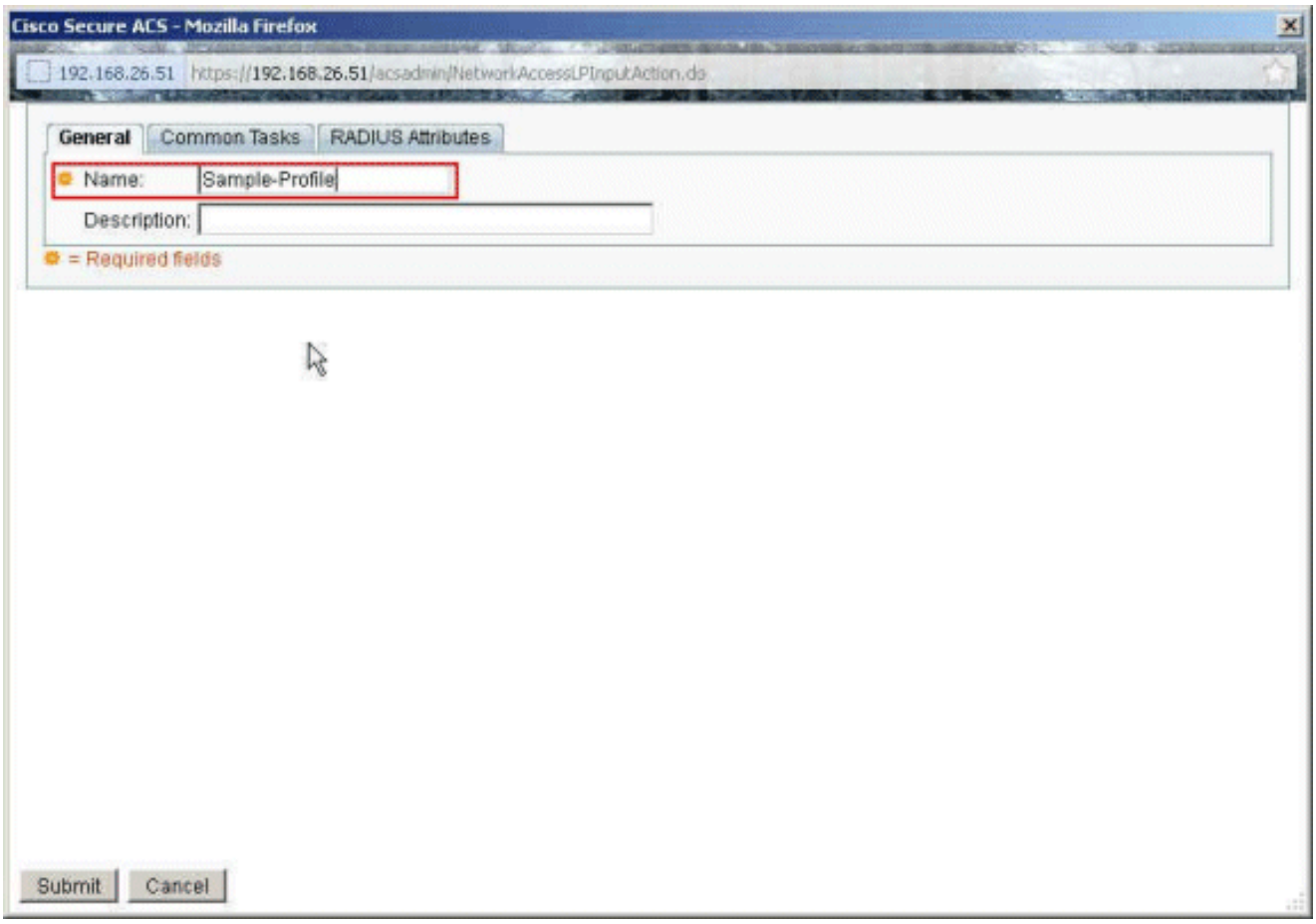
10. انقر علی تحدید ، في قسم توصيفات التخويل.



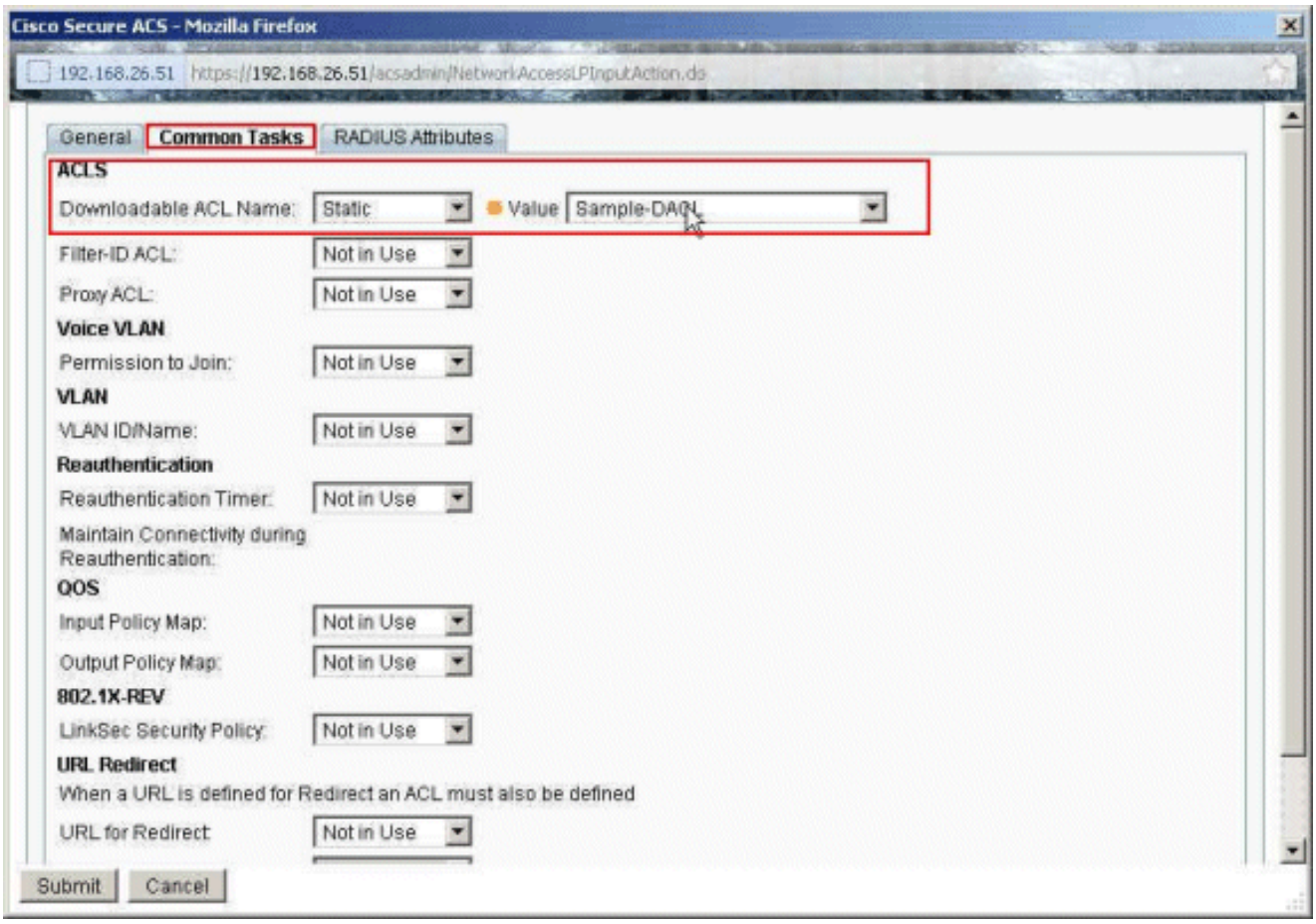
11. انقر على إنشاء لإنشاء ملف تعريف تخويل جديد.



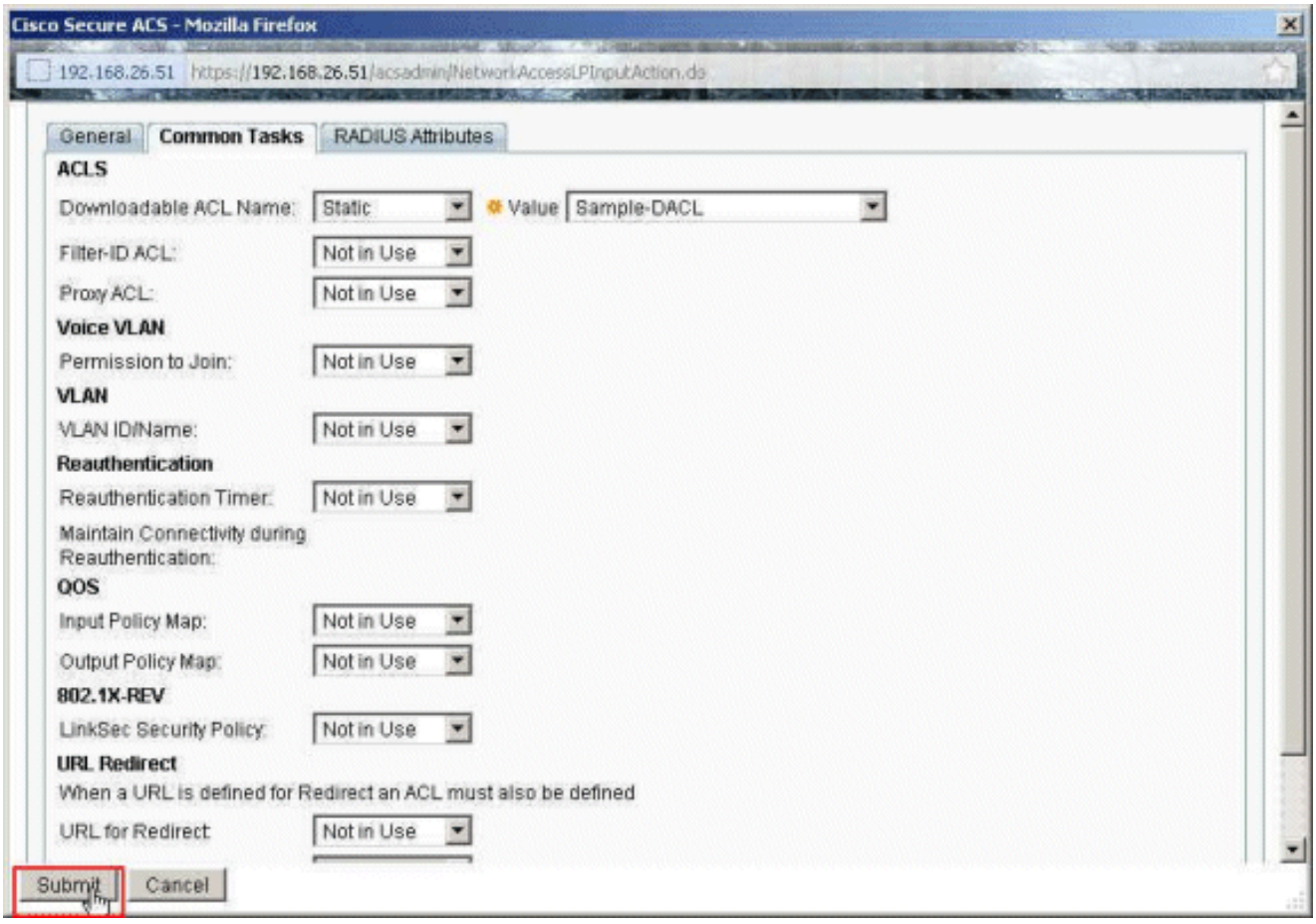
12. قم بتوفير اسم لملف تعريف التخويل. ملف التعريف هو الاسم المستخدم في هذا المثال.



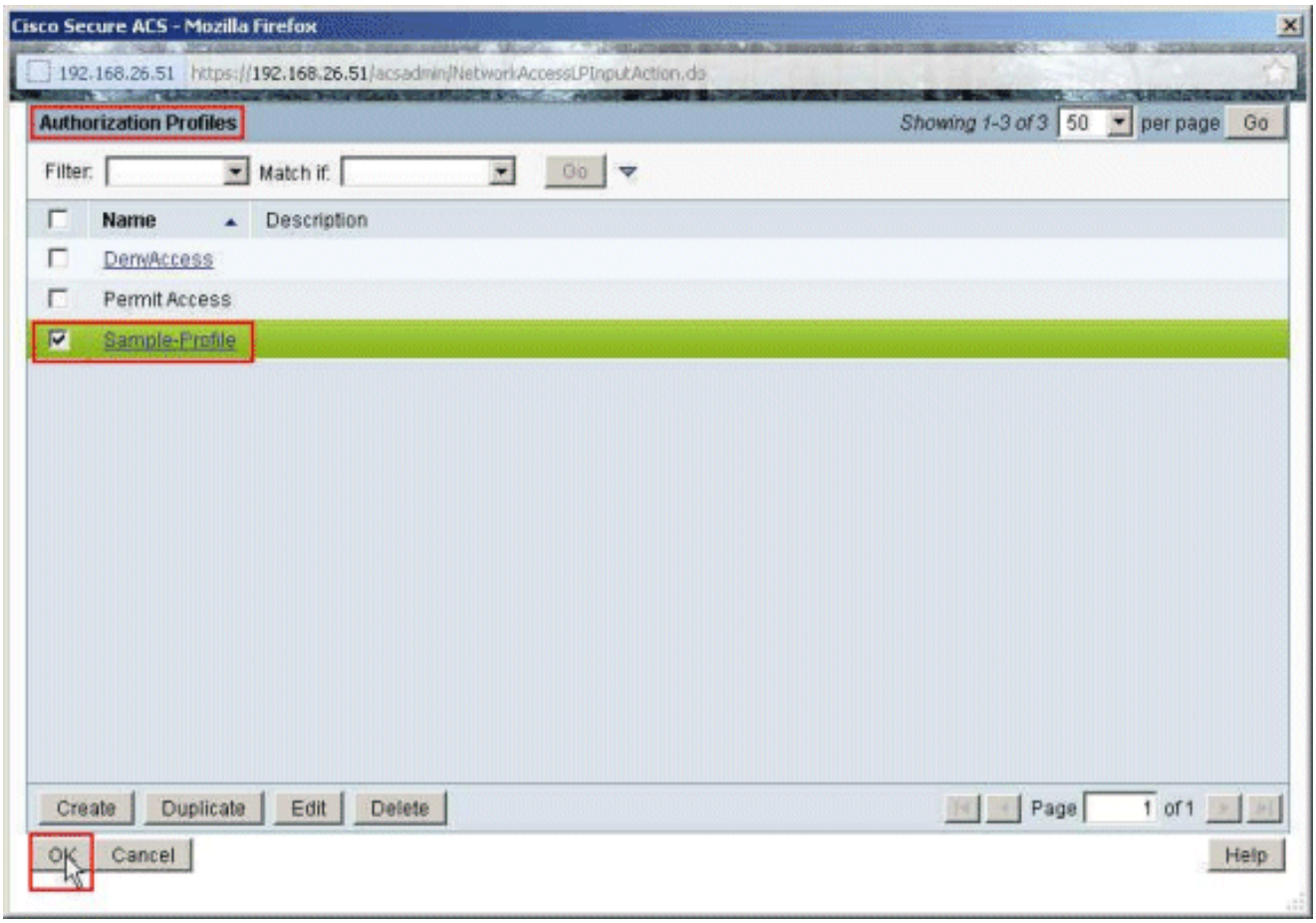
13. أختر علامة التبويب مهام مشتركة، وحدد ثابت من القائمة المنسدلة لاسم قائمة التحكم في الوصول (ACL) القابل للتنزيل. أختر DACL الذي تم إنشاؤه حديثا (نموذج - DACL) من القائمة المنسدلة "القيمة".



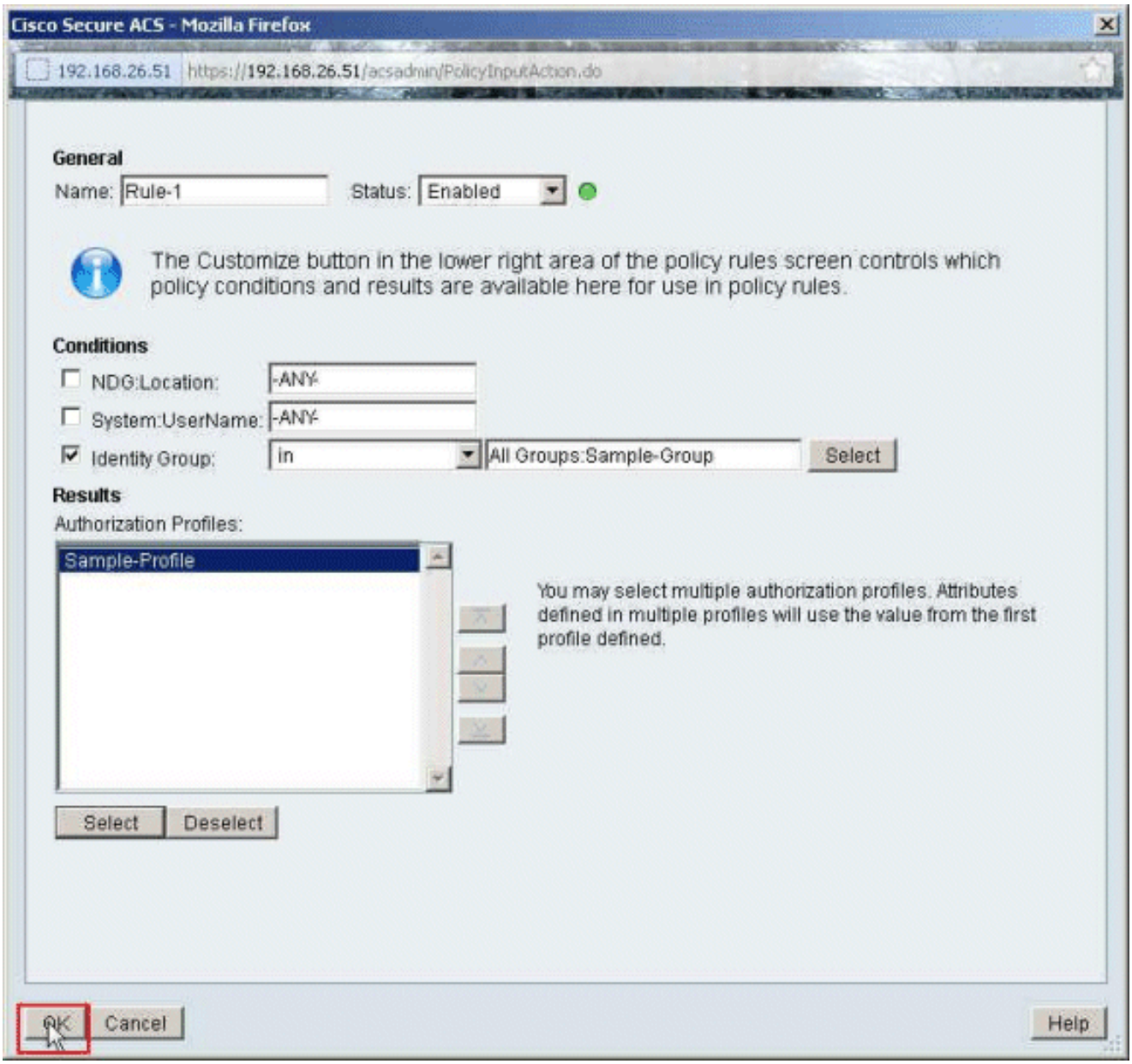
14. انقر على إرسال.



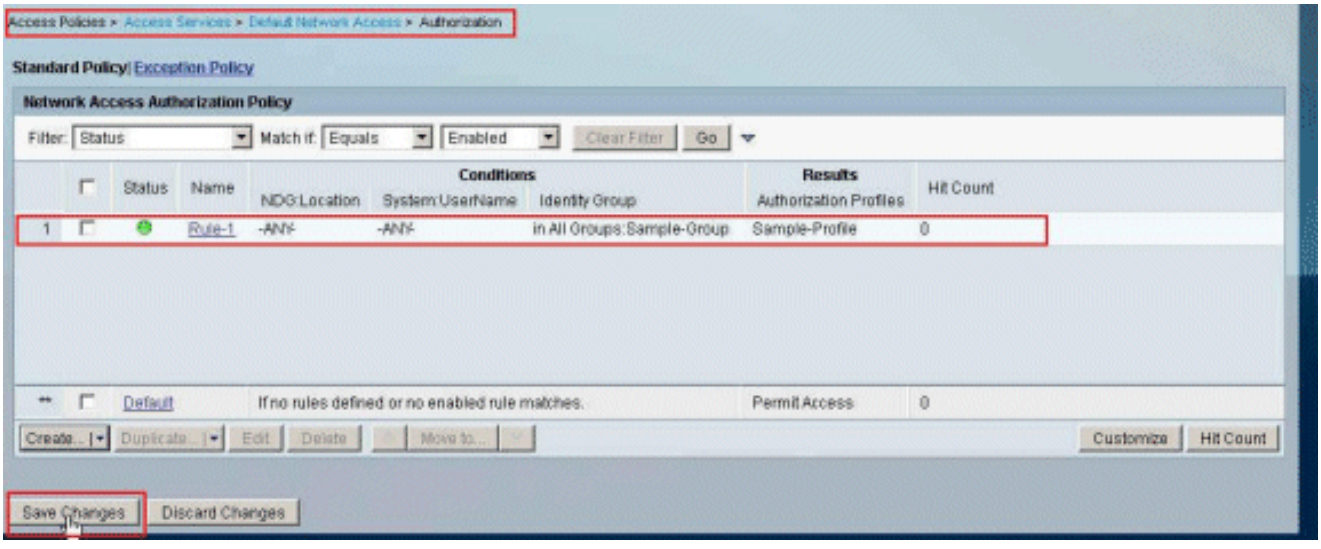
15. أختر نموذج ملف تعريف التخويل الذي تم إنشاؤه مسبقا، وانقر فوق موافق.



16. انقر فوق OK.



17. تحقق من إنشاء القاعدة 1 مع المجموعة العينة الخاصة بهوية المجموعة كشرط ونموذج ملف التعريف كنتيجة لذلك. انقر فوق حفظ التغييرات.

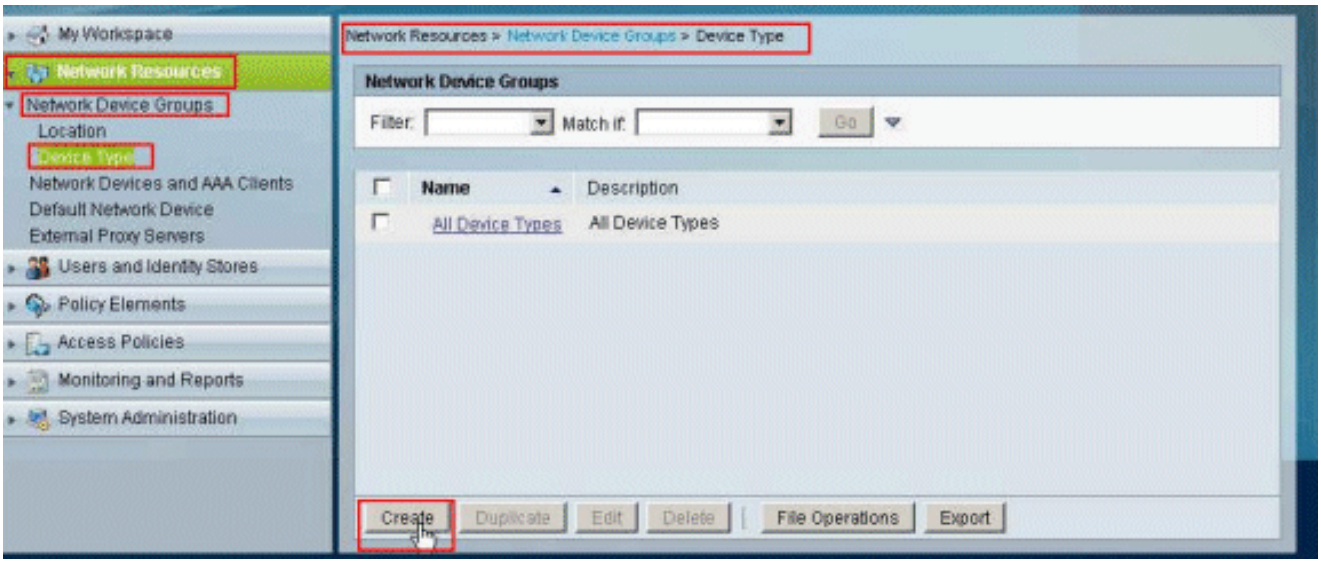


تكوين ACS لقائمة التحكم في الوصول (ACL) القابلة للتنزيل لمجموعة أجهزة الشبكة

أكمل الخطوات من 1 إلى 12 من تكوين ACS لقائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم الفردي وأجرى هذه الخطوات لتكوين قائمة التحكم في الوصول (ACL) القابلة للتنزيل لمجموعة أجهزة الشبكة في Cisco Secure ACS.

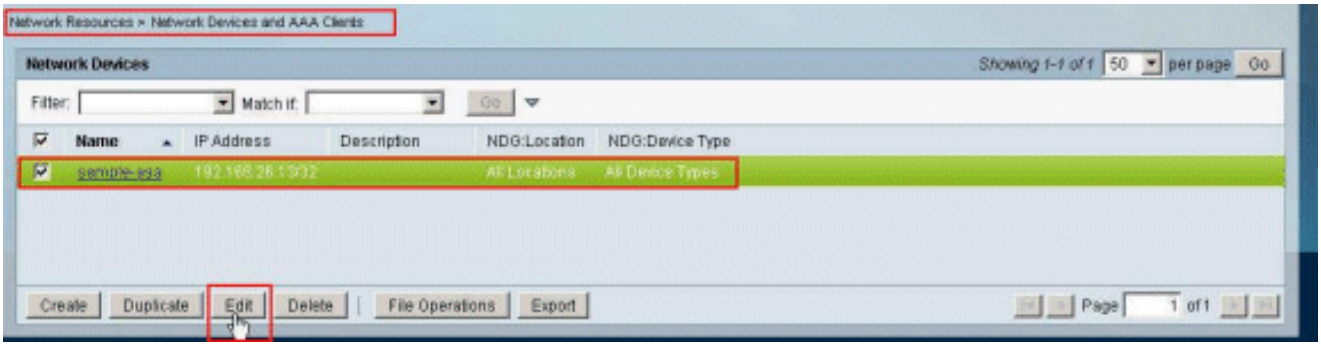
في هذا المثال، يتمتع عميل RADIUS (ASA) إلى بوابات VPN الخاصة بمجموعة أجهزة الشبكة. يتم بنجاح إرسال طلب مصادقة VPN الوارد من ASA للمستخدم "Cisco"، ويرسل "cisco" الوصول إلى خادم RADIUS قائمة وصول قابلة للتنزيل إلى جهاز الأمان. يمكن للمستخدم "cisco" الوصول إلى خادم 10.1.1.2 فقط ويرفض جميع الوصول الآخر. للتحقق من قائمة التحكم في الوصول القابلة للتنزيل (ACL)، ارجع إلى قسم قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم/المجموعة.

1. أخترت شبكة مورد>شبكة أداة مجموعة>أداة نوع، وطقطقة يخلقin order to خلقت شبكة أداة مجموعة جديد.

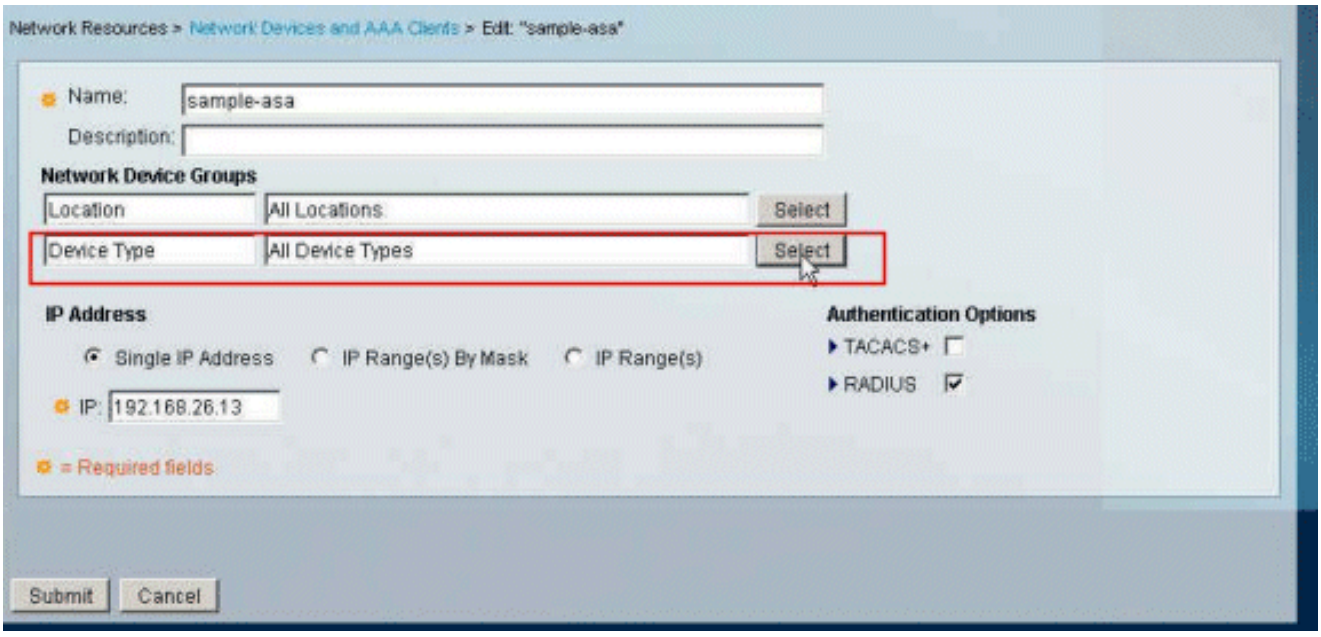


2. قم بتوفير اسم مجموعة أجهزة الشبكة (بوابات VPN في هذا المثال)، وانقر فوق إرسال.

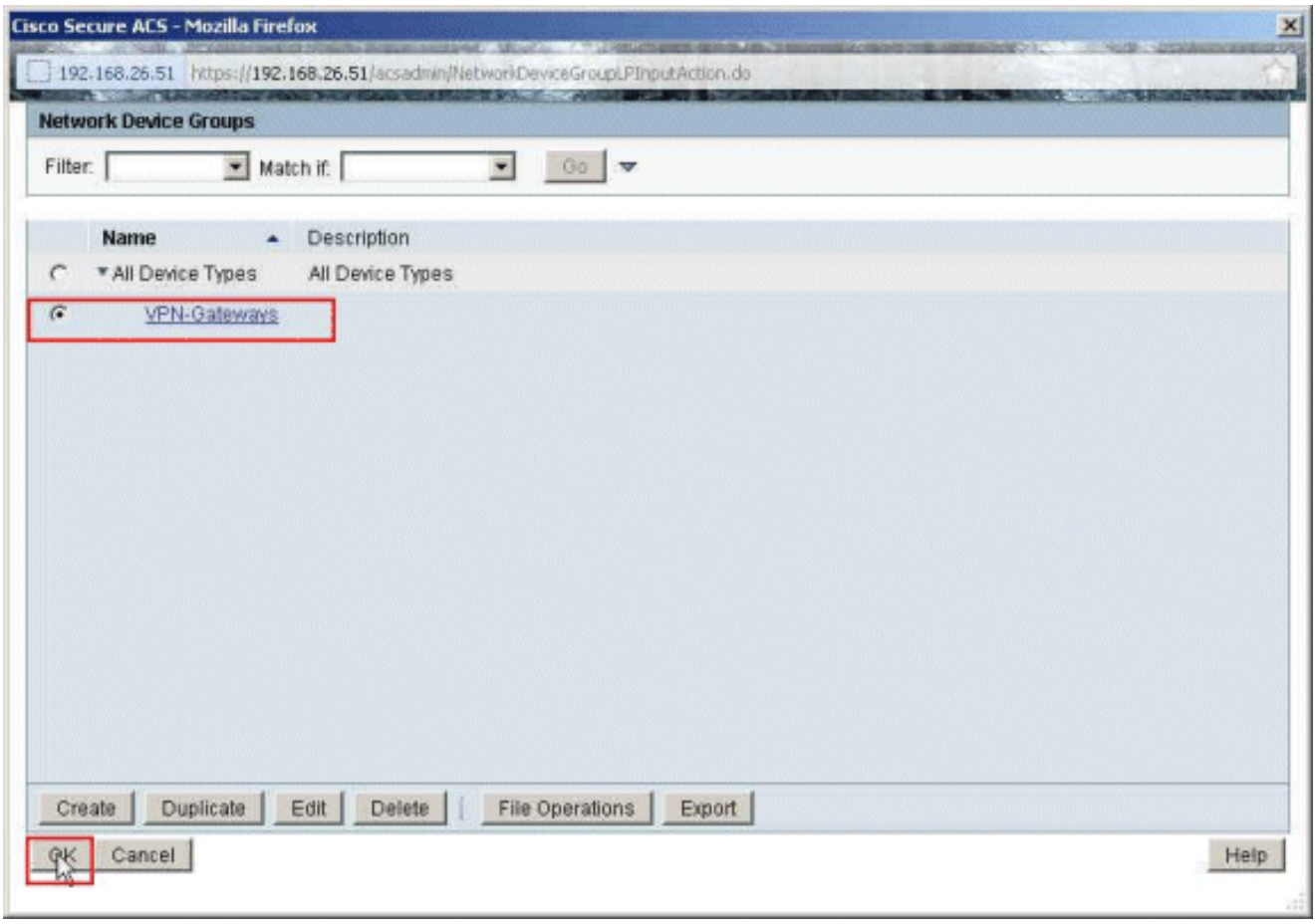
3. أختر موارد الشبكة>أجهزة الشبكة وعملاء AAA، وحدد عميل RADIUS Sample-asa الذي تم إنشاؤه سابقا. طقطقة يحرر in order to غيرت الشبكة أداة مجموعة عضوية من هذا RADIUS زبون (ASA).



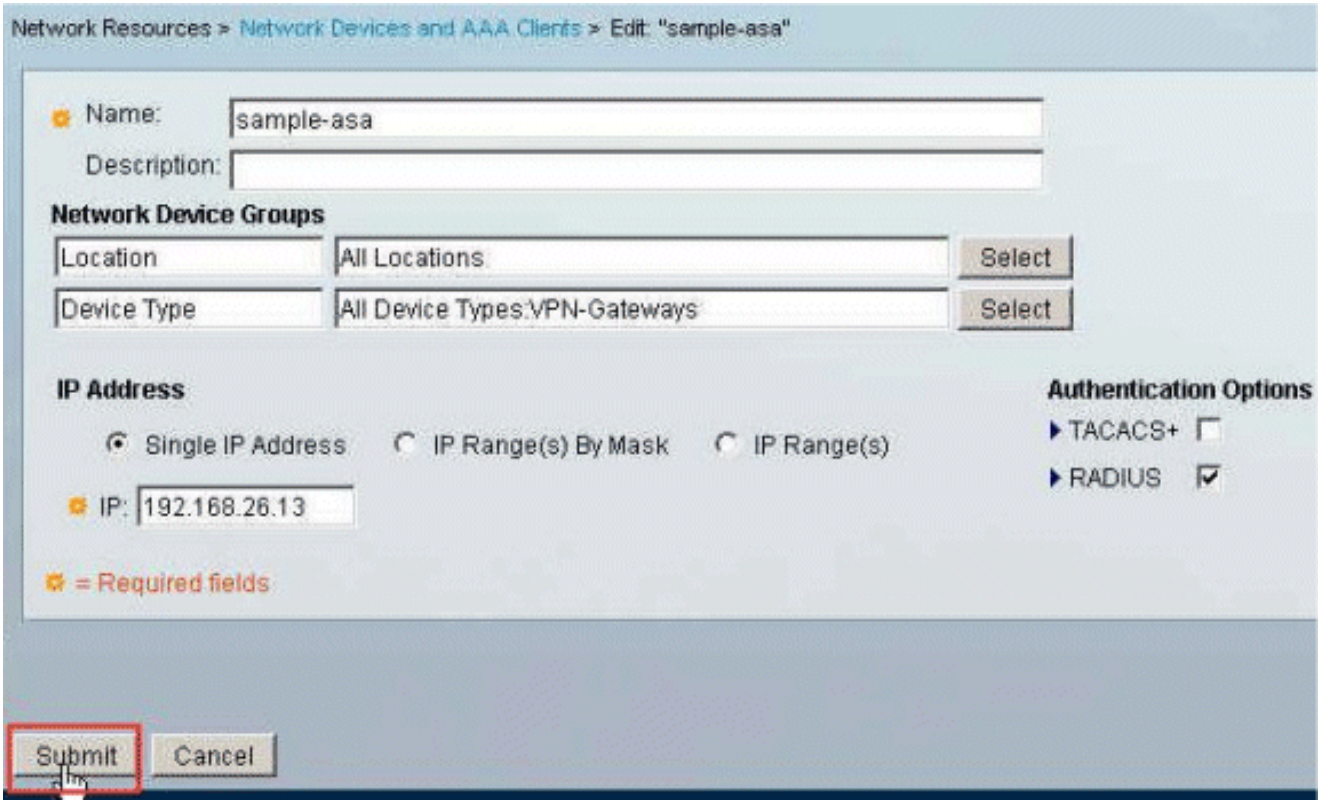
4. انقر فوق تحديد بجوار نوع الجهاز.



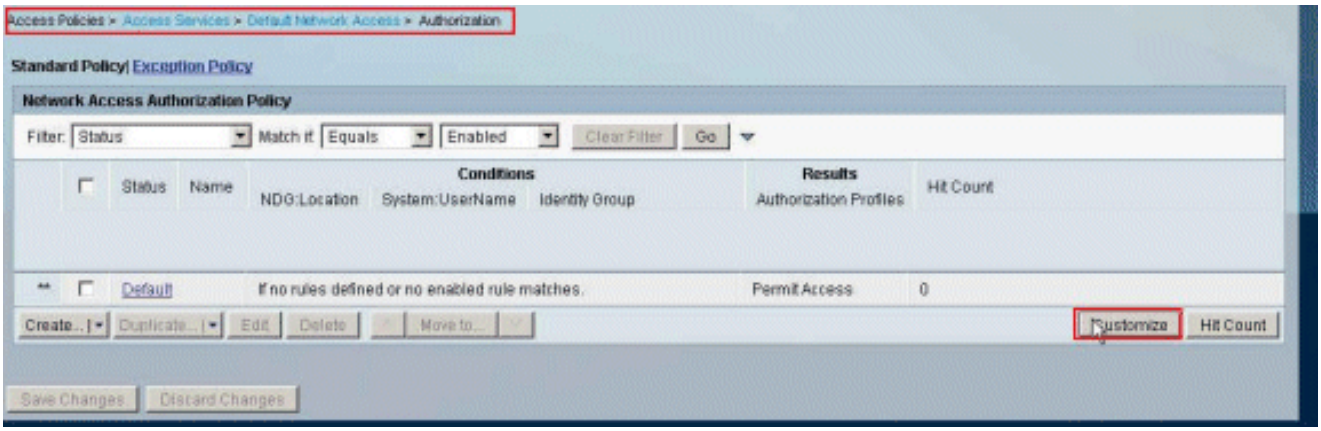
5. حدد مجموعة أجهزة الشبكة التي تم إنشاؤها حديثا (والتي هي بوابات VPN)، وانقر فوق موافق.



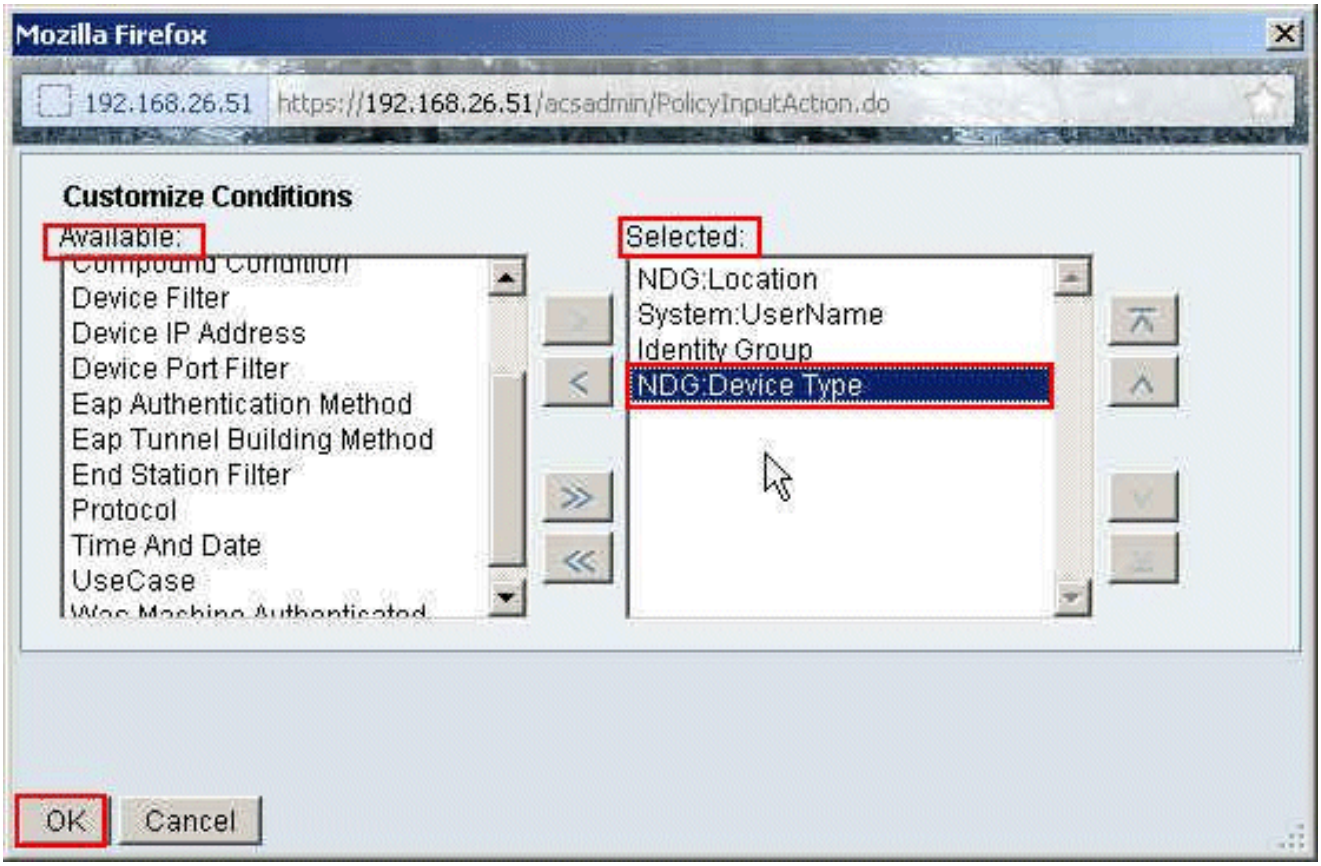
6. انقر على إرسال.



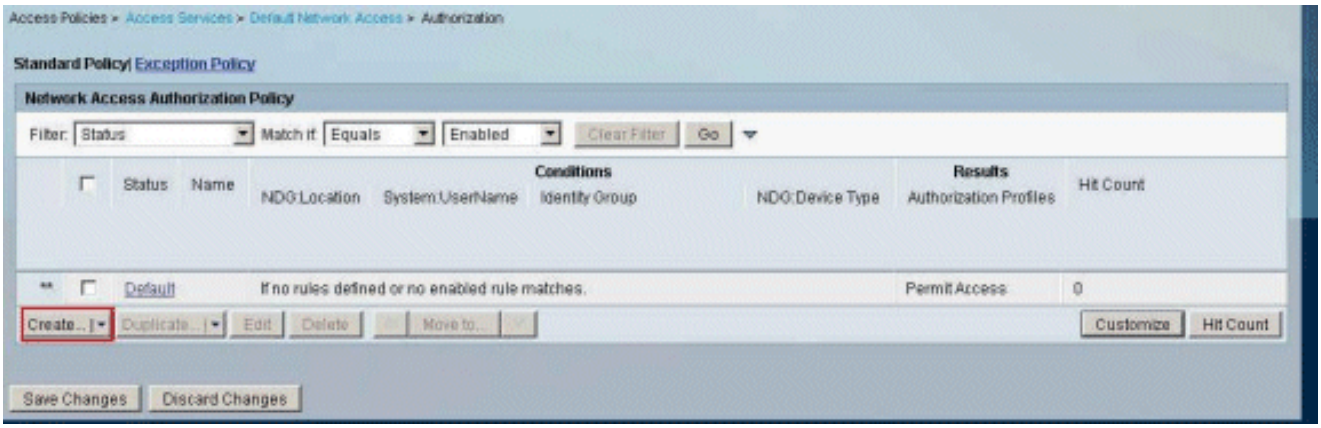
7. أختر سياسات الوصول > خدمات الوصول > الوصول الافتراضي للشبكة > التفويض، وانقر فوق تخصيص.



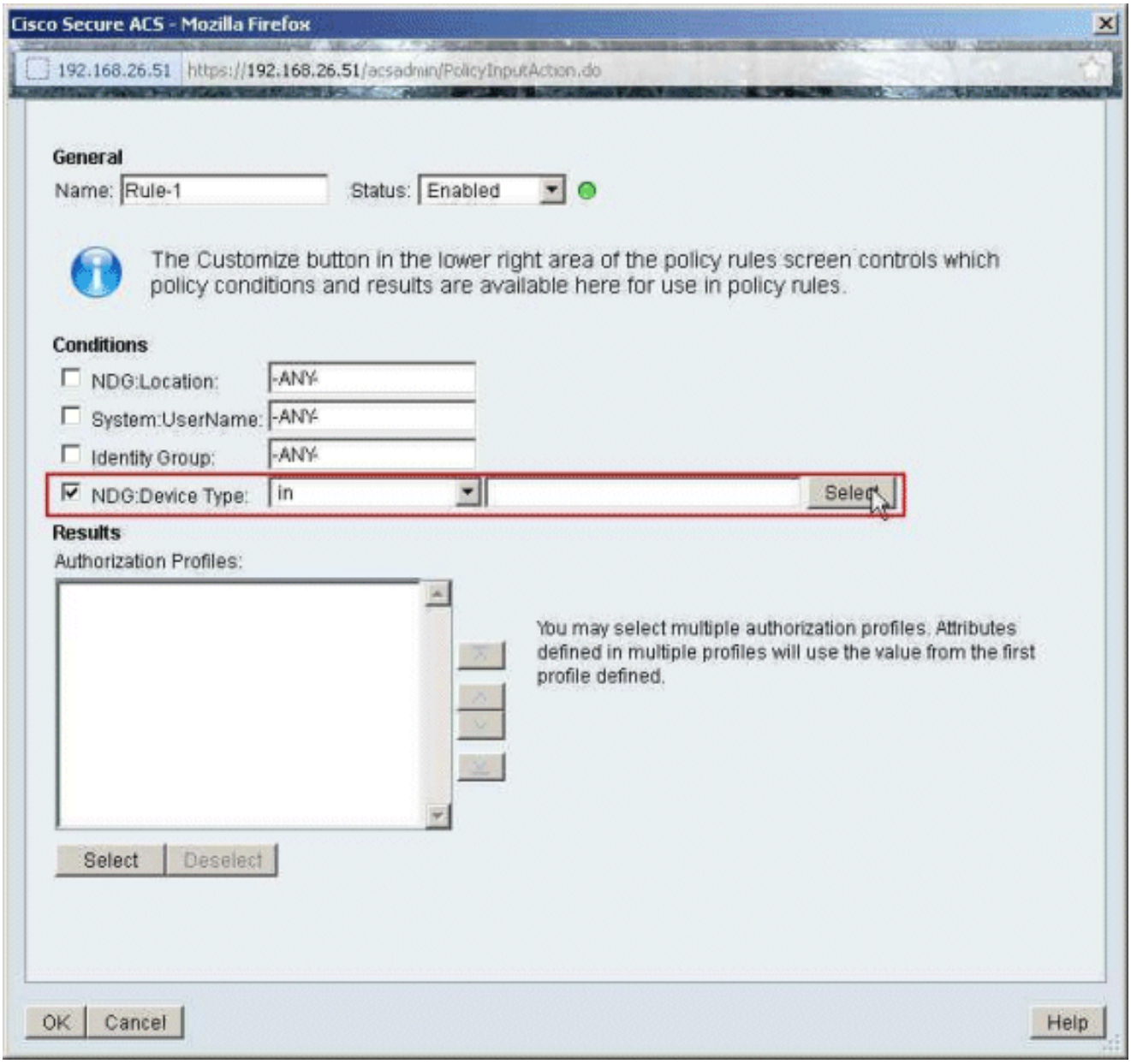
8. انقل NDG:نوع الجهاز من القسم متوفر إلى القسم المحدد، وانقر فوق موافق.



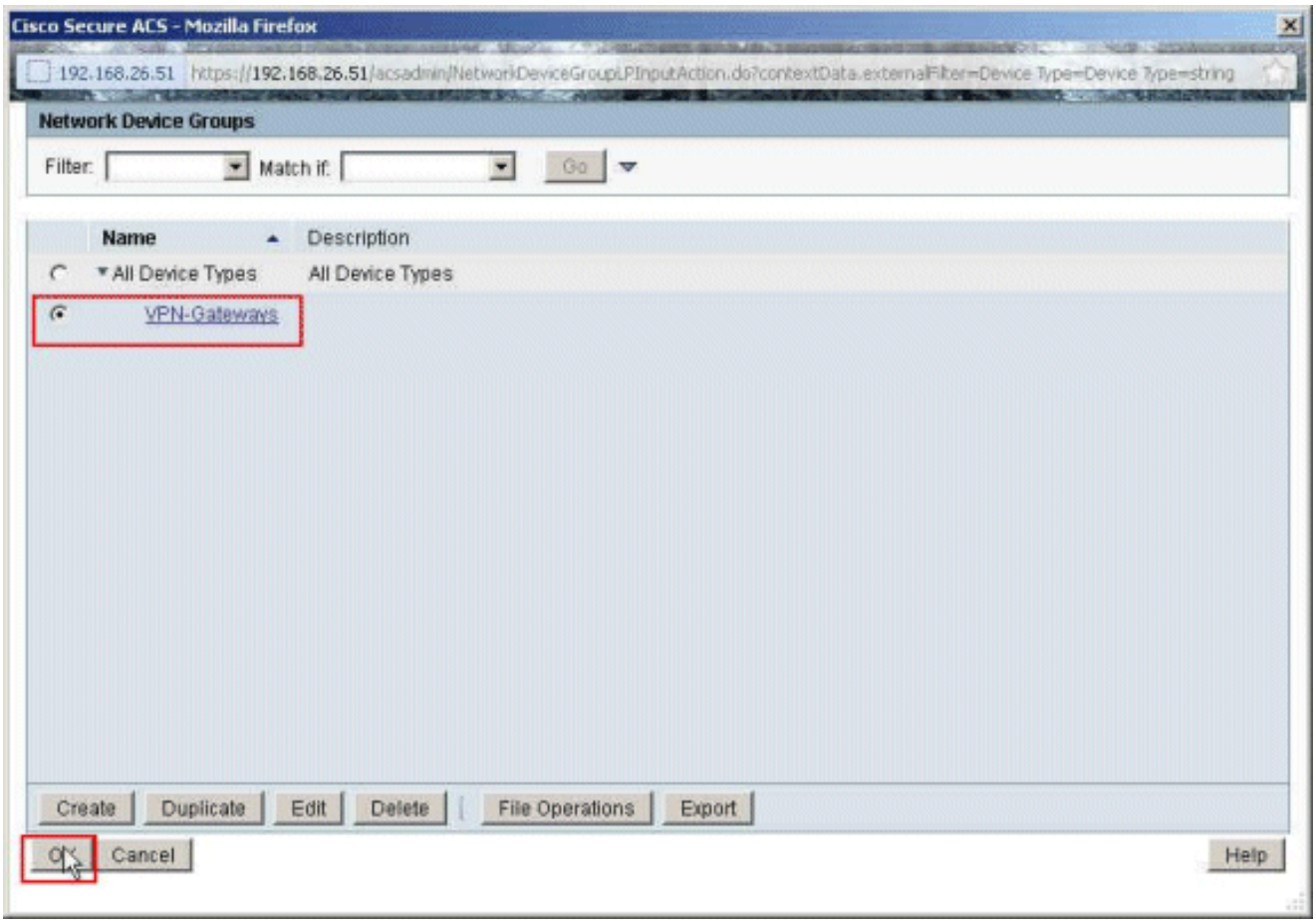
9. انقر فوق إنشاء لإنشاء قاعدة جديدة.



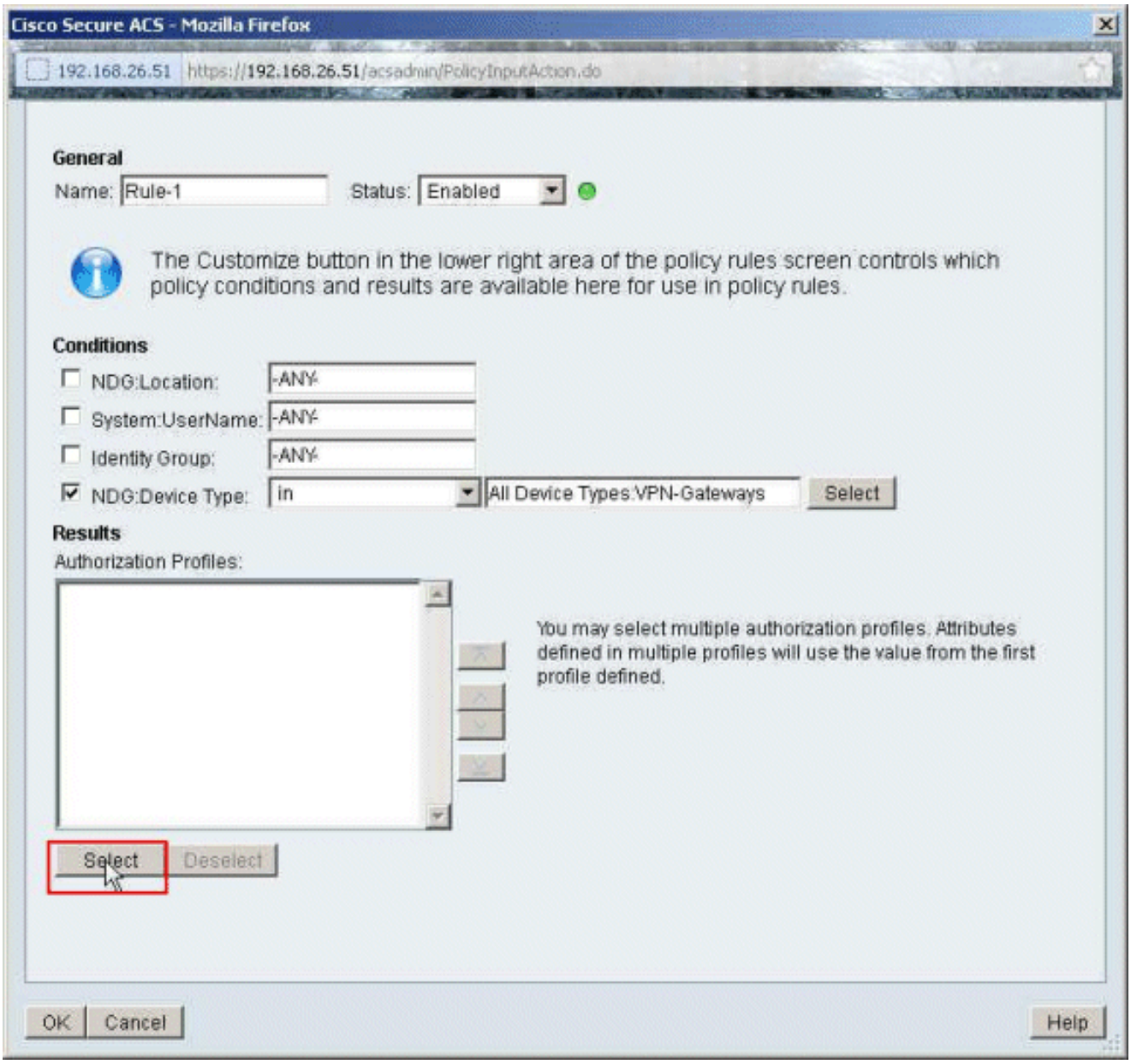
10. تأكد من أن خانة الاختيار المجاورة ل NDG:Device Type محددة واختر in من القائمة المنسدلة. انقر فوق تحديد.



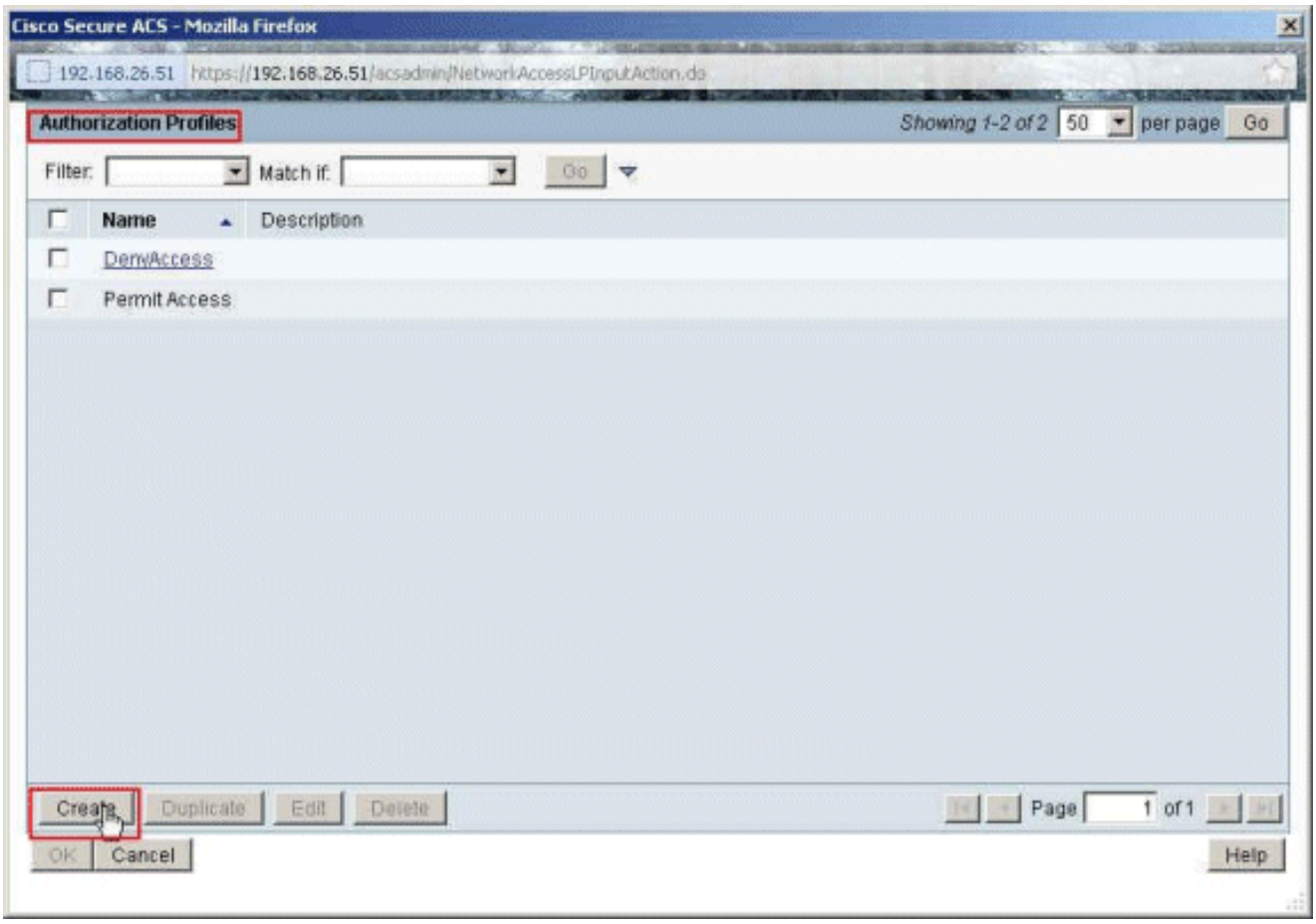
11. أختر الشبكة أداة مجموعة VPN-Gateways يخلق سابقا، وطقطقة ok.



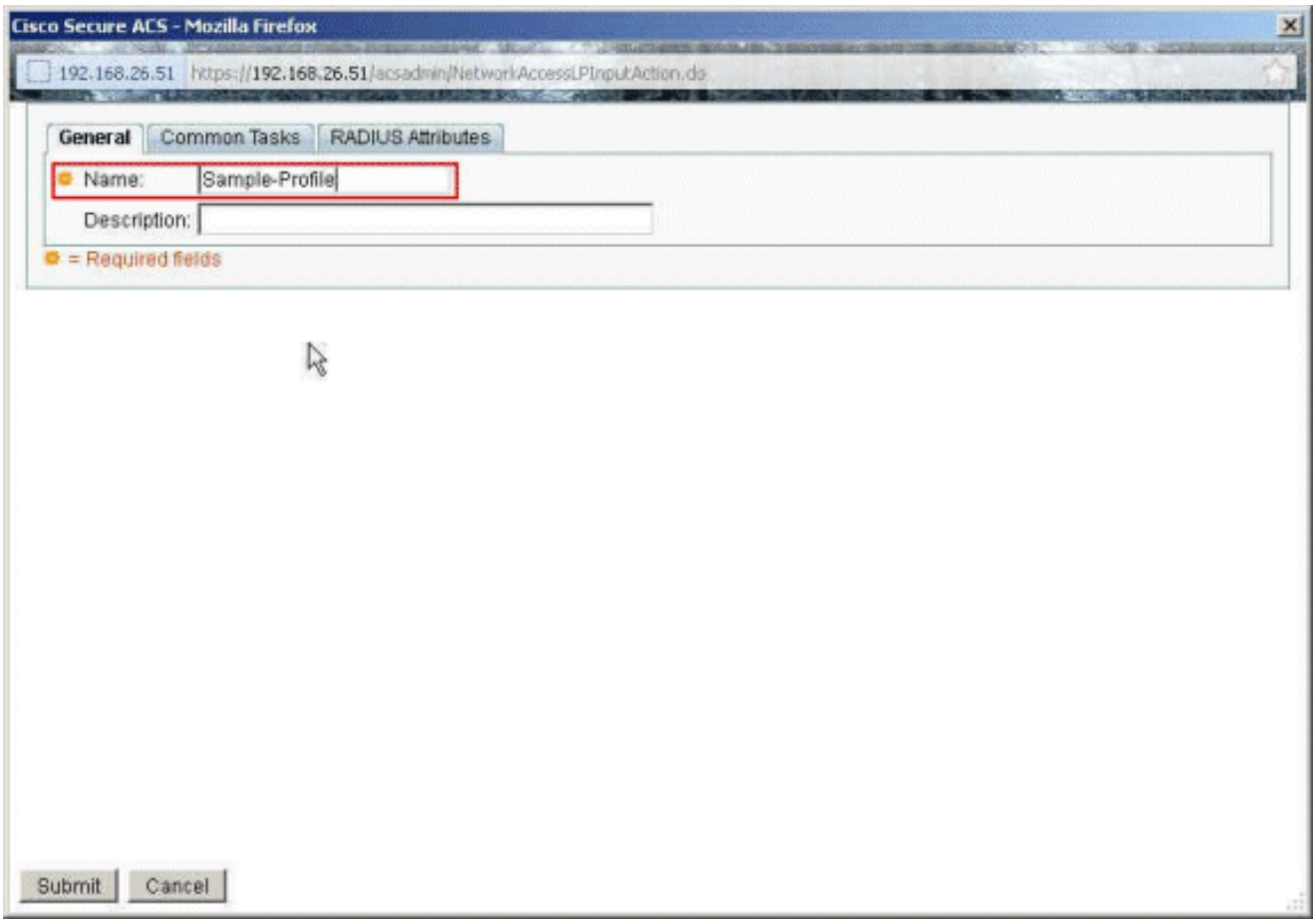
12. انقر فوق تحديد.



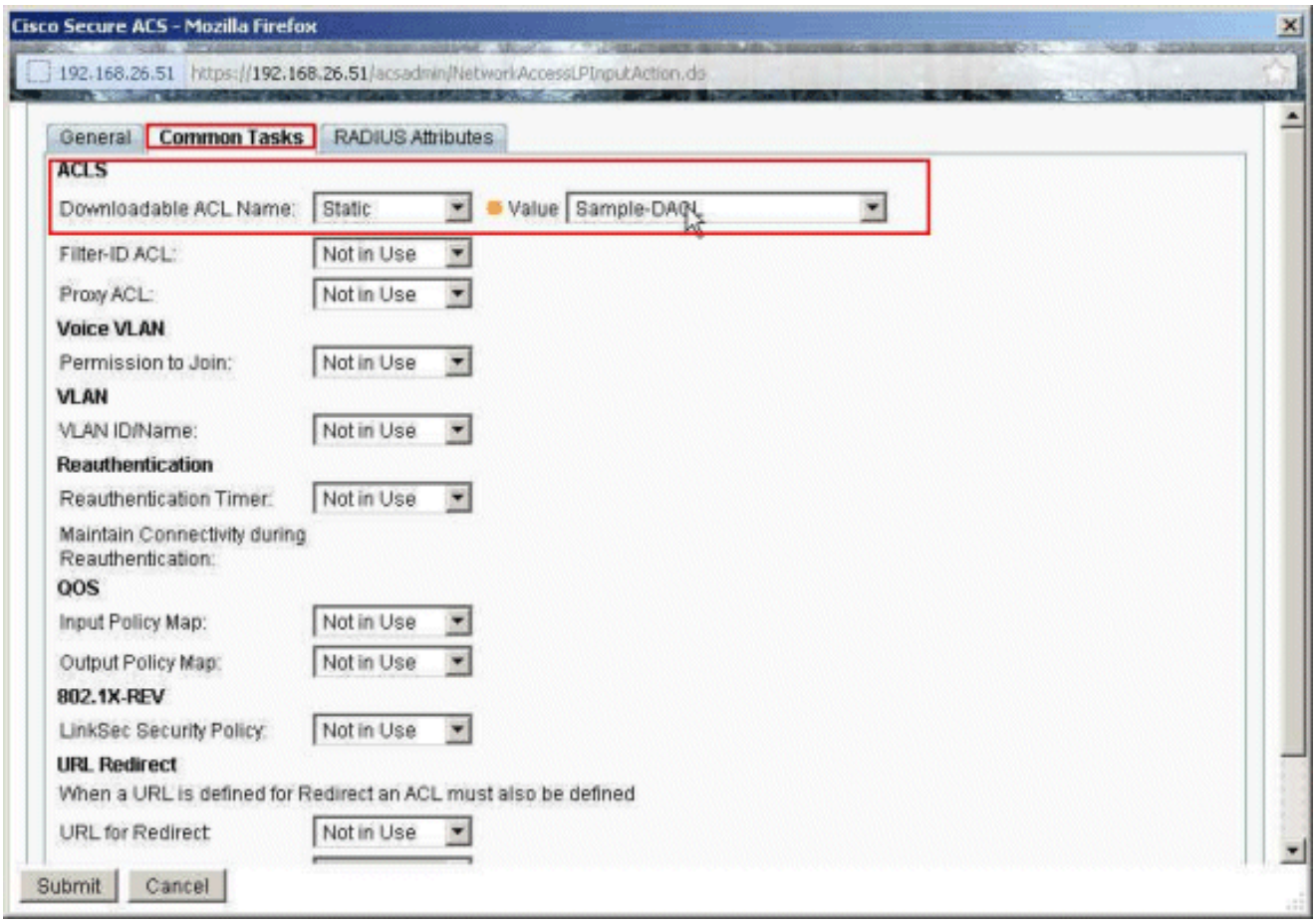
13. انقر على إنشاء لإنشاء ملف تعريف تخويل جديد.



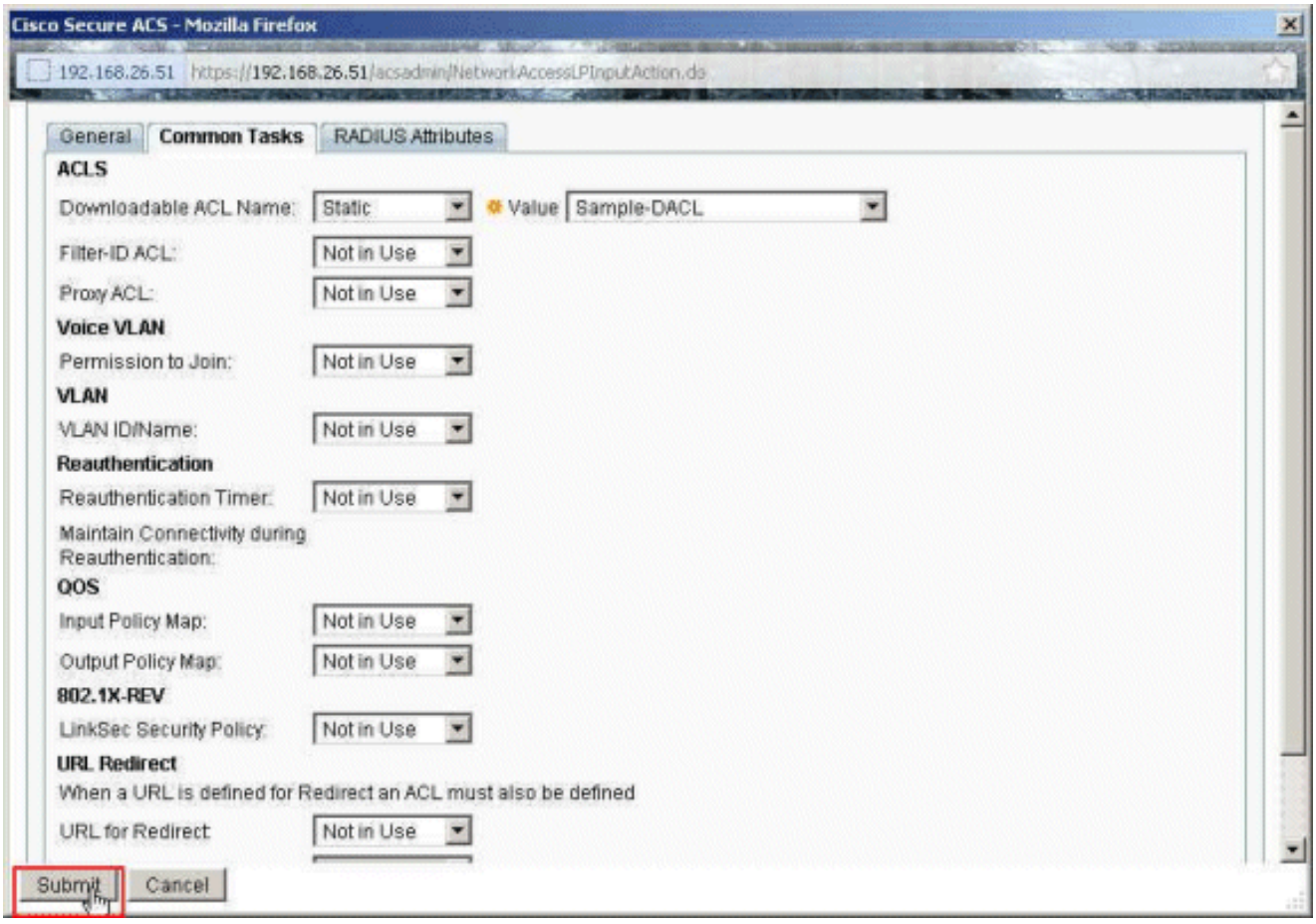
14. قم بتوفير اسم لملف تعريف التخويل. ملف التعريف هو الاسم المستخدم في هذا المثال.



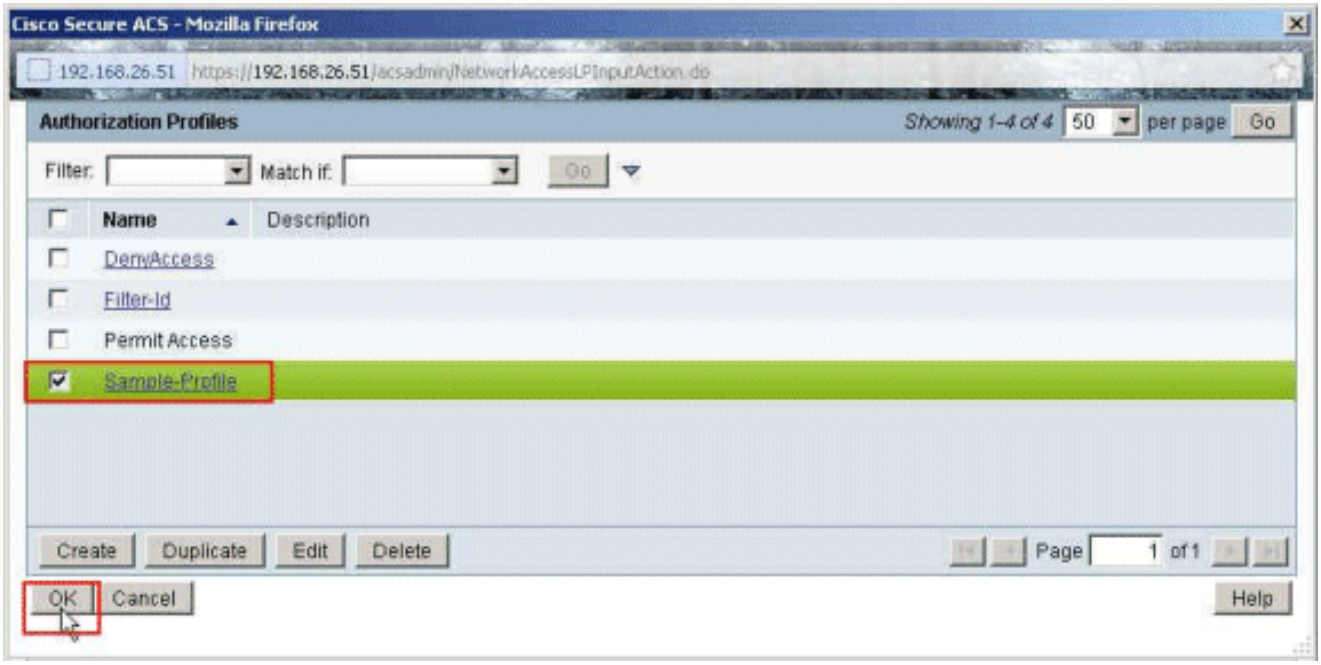
15. أختر علامة التبويب مهام مشتركة، وحدد ثابت من القائمة المنسدلة لاسم قائمة التحكم في الوصول (ACL) القابل للتنزيل. أختر DACL الذي تم إنشاؤه حديثا (نموذج DACL) من القائمة المنسدلة للقيمة.



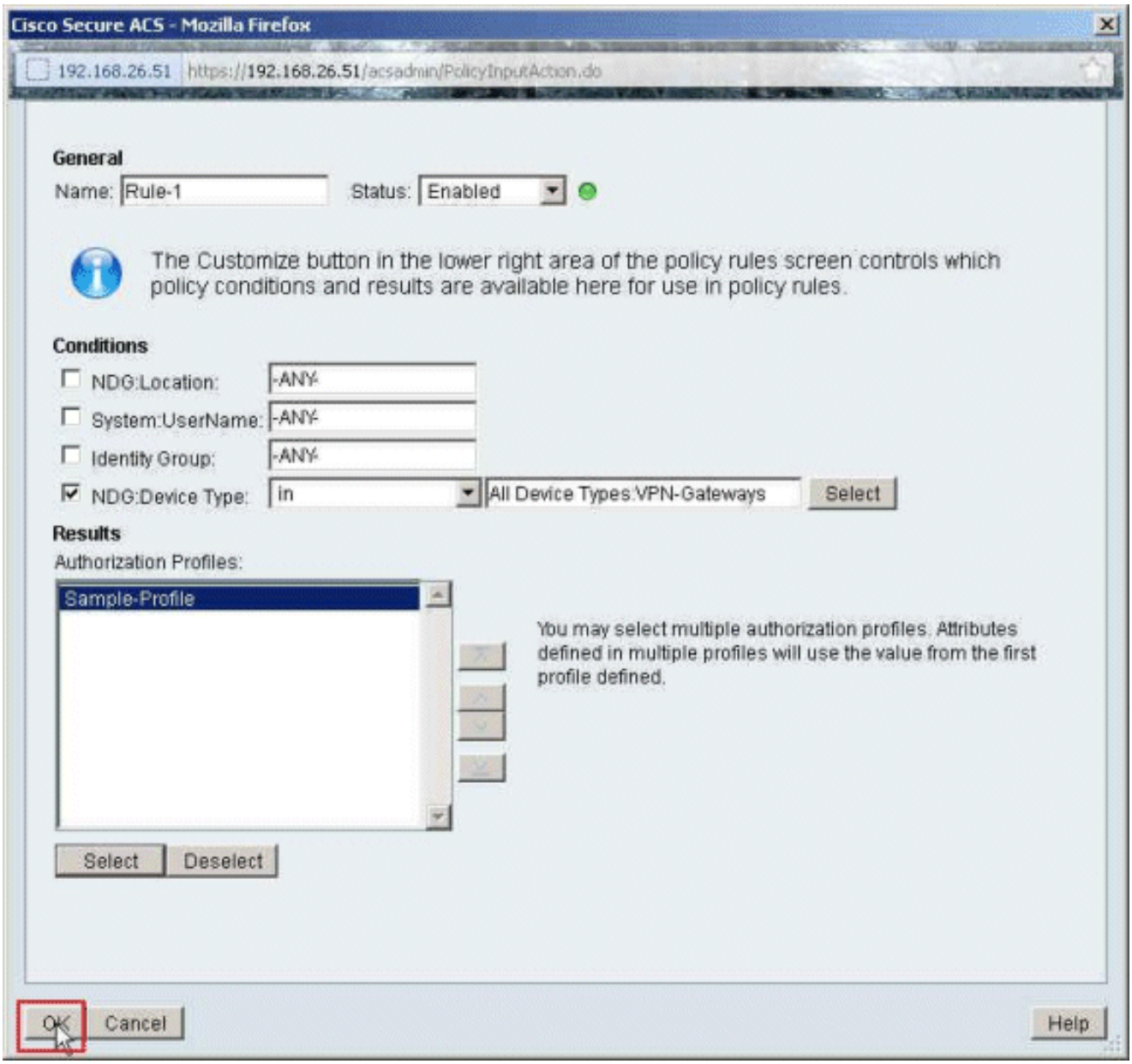
16. انقر على إرسال.



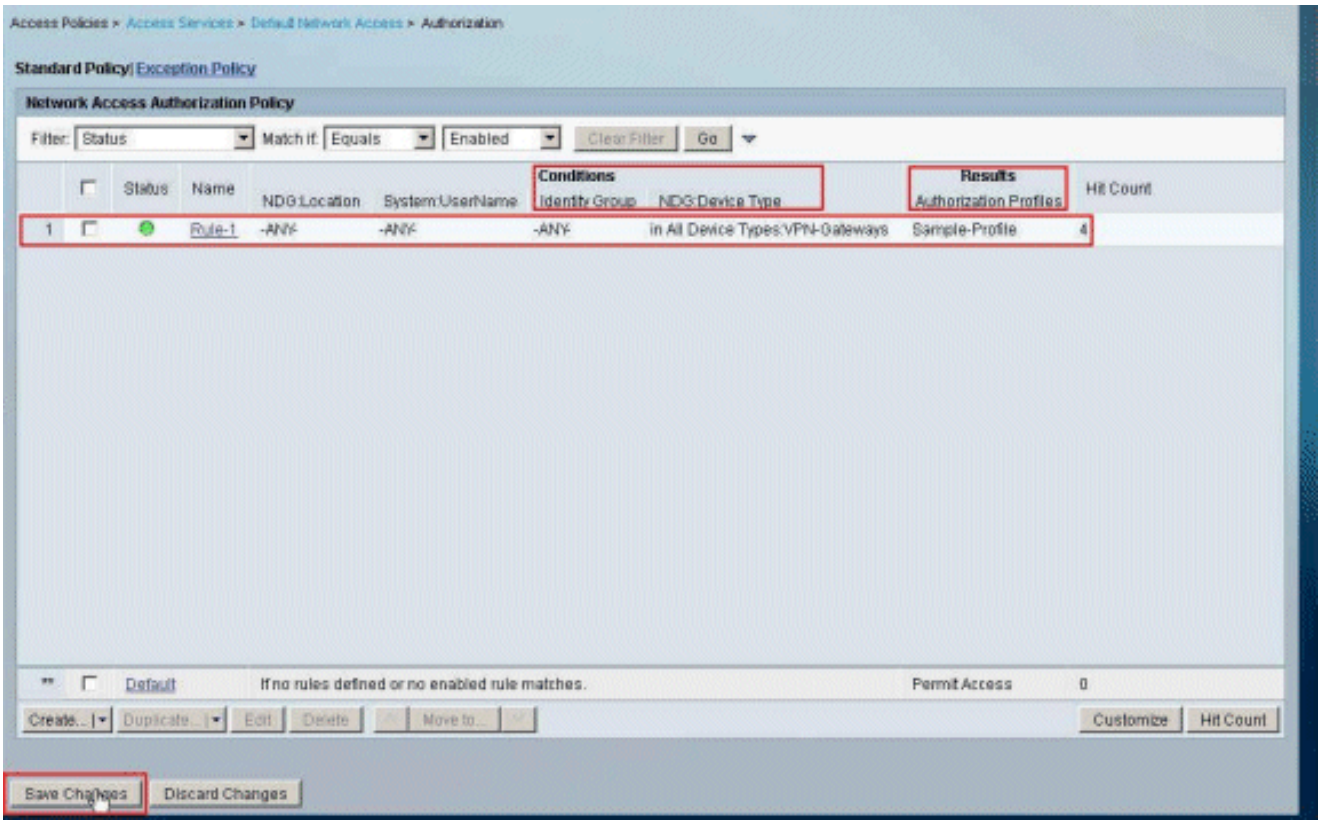
17. حدد نموذج ملف التعريف الذي تم إنشاؤه سابقا، وانقر موافق.



18. وانقر فوق OK.



19. تحقق من إنشاء القاعدة 1- باستخدام عبارات VPN كحالة NDG:نوع الجهاز، ومن نتيجة ذلك نموذج ملف التعريف. انقر فوق حفظ التغييرات.



تكوين إعدادات IETF RADIUS لمجموعة مستخدمين

لتنزيل اسم لقائمة وصول قمت بإنشائها بالفعل على جهاز الأمان من خادم RADIUS عند مصادقة المستخدم، قم بتكوين السمة IETF RADIUS filter-id (السمة رقم 11):

```
<#root>

filter-id=acl_name
```

يقوم مستخدم مجموعة العينة بمصادقة Cisco بنجاح، ويقوم خادم RADIUS بتنزيل اسم قائمة التحكم في الوصول (جديد) لقائمة وصول قمت بإنشائها بالفعل على جهاز الأمان. يمكن للمستخدم "cisco" الوصول إلى جميع الأجهزة الموجودة داخل شبكة ASA باستثناء خادم 10.1.1.2. للتحقق من قائمة التحكم في الوصول (ACL)، راجع قسم قائمة التحكم في الوصول إلى معرفة التصفية.

وفقا للمثال، تم تكوين قائمة التحكم في الوصول (ACL) المسماة جديدة للتصفية في ASA:

```
<#root>

access-list new extended deny ip any host 10.1.1.2
access-list new extended permit ip any any
```

تظهر هذه المعلمات فقط عندما تكون صحيحة. لقد قمت بتكوين:

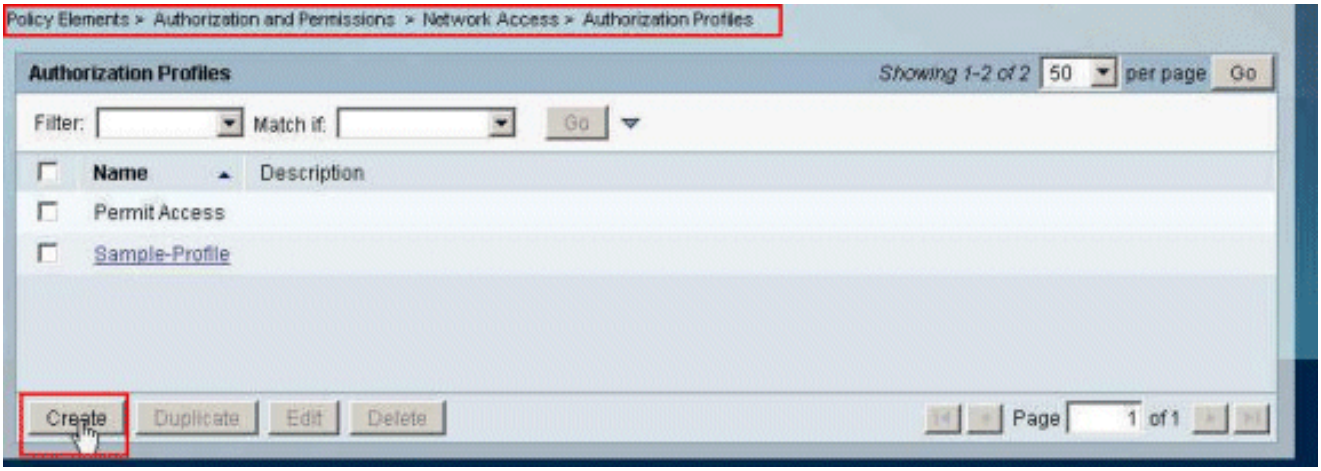
- تكوين الشبكة في RADIUS وتوكولات أحد برو استخدام عميل AAA
- تم تحديد ملف تعريف تفويض بعامل تصفية معرف RADIUS (IETF) ضمن قسم النتائج من القاعدة في خدمة الوصول.

تم إرسال سمات RADIUS كملف تعريف لكل مستخدم من ACS إلى عميل AAA الطالب.

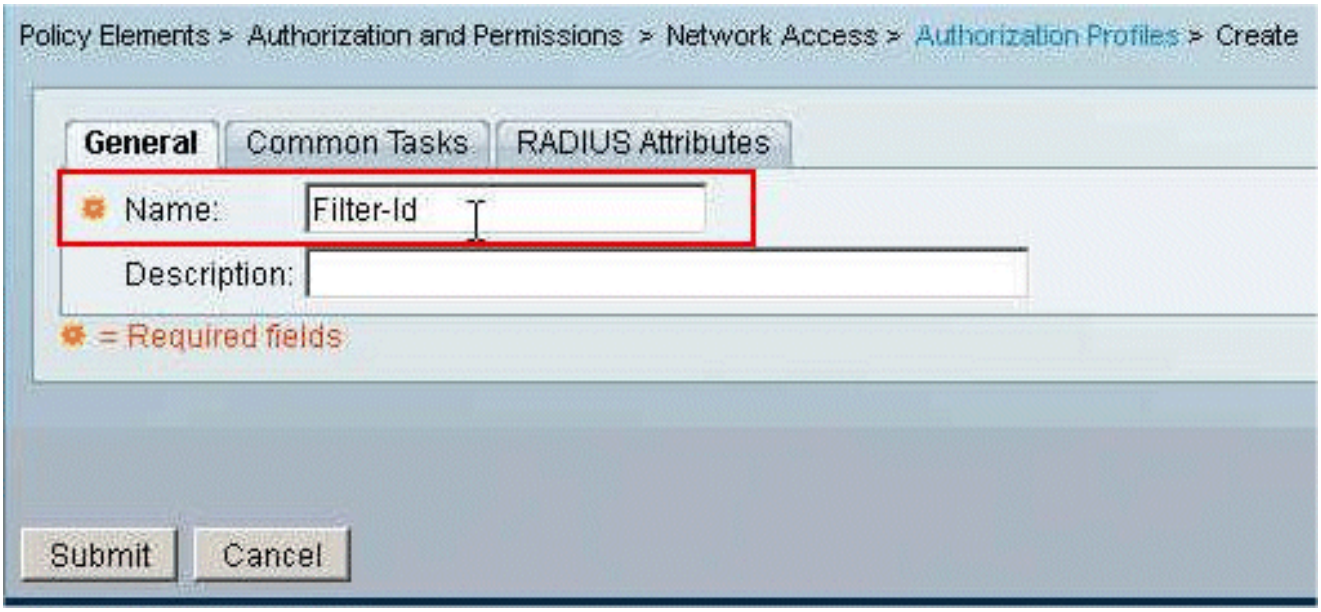
تكوين ACS لقائمة التحكم بالوصول (ACL) نم 12 إلى 10 و 6 إلى 1 من أكمل الخطوات من 6 إلى 1 من تكوين ACS القابلة للتنزيل للمستخدم الفردي، متبوعة بالخطوات من هذه الخطوات في اذا القسم القابلة للتنزيل للمجموعة، وأقم قائمة التحكم في الوصول القابلة للتنزيل للمجموعة لتكوين معرف التصفية في Cisco ACS الآمن.

لتكوين إعدادات سمة IETF RADIUS لتطبيقها كما هو الحال في توصيف التخويل، نفذ الخطوات التالية:

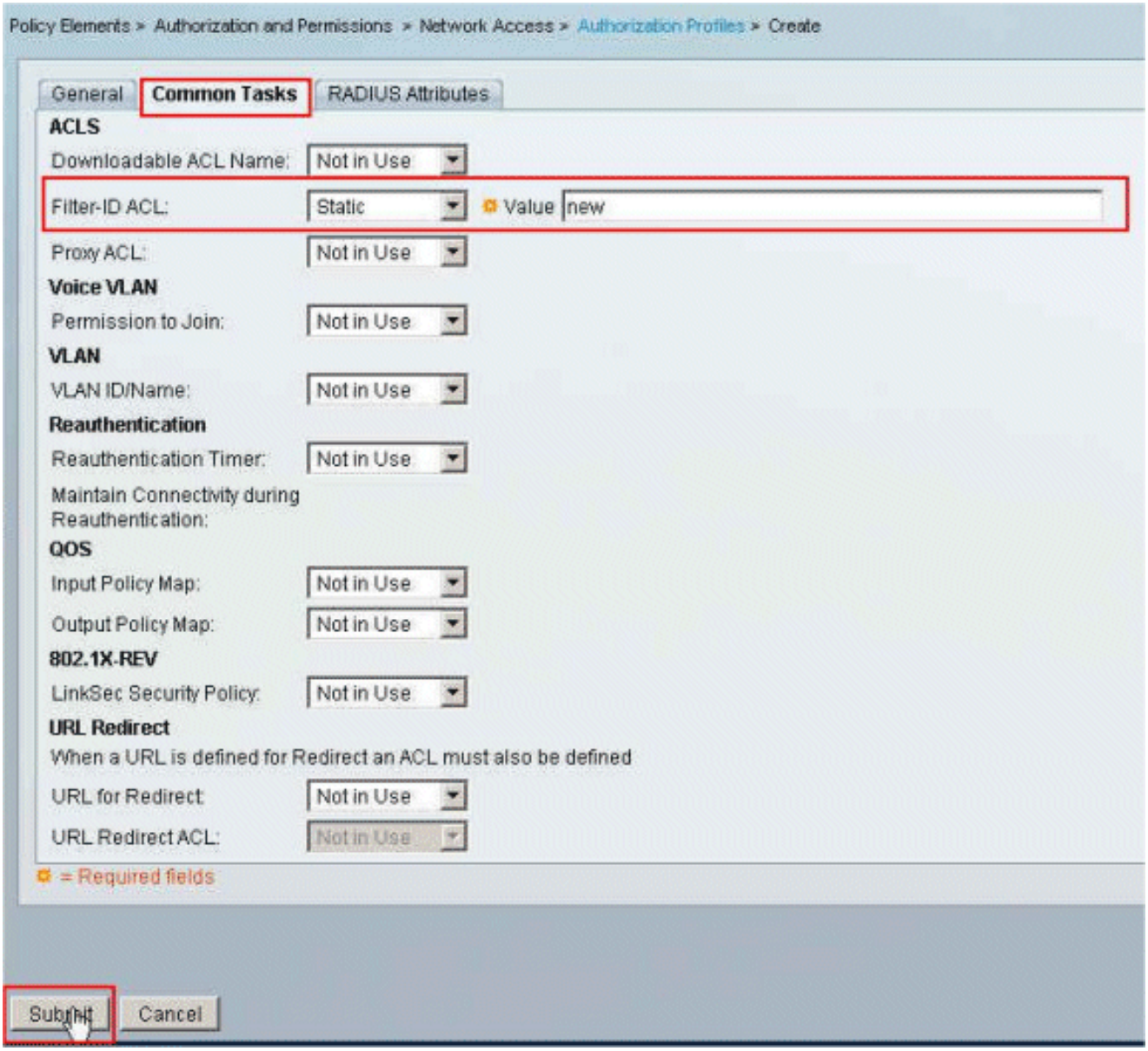
1. أختر عناصر النهج > التفويض والأذونات>الوصول إلى الشبكة>ملفات تعريف التفويض، وانقر فوق إنشاء لإنشاء ملف تعريف تفويض جديد.



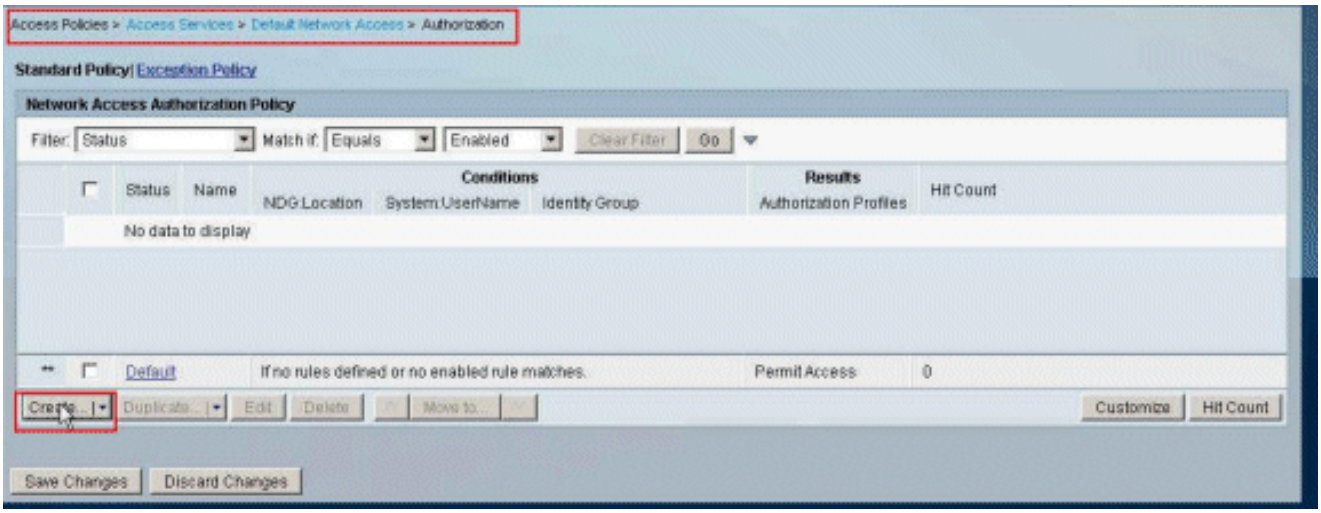
2. قم بتوفير اسم لملف تعريف التخويل. معرف عامل التصفية هو اسم ملف تعريف التخويل الذي تم إختياره في هذا المثال للبساطة.



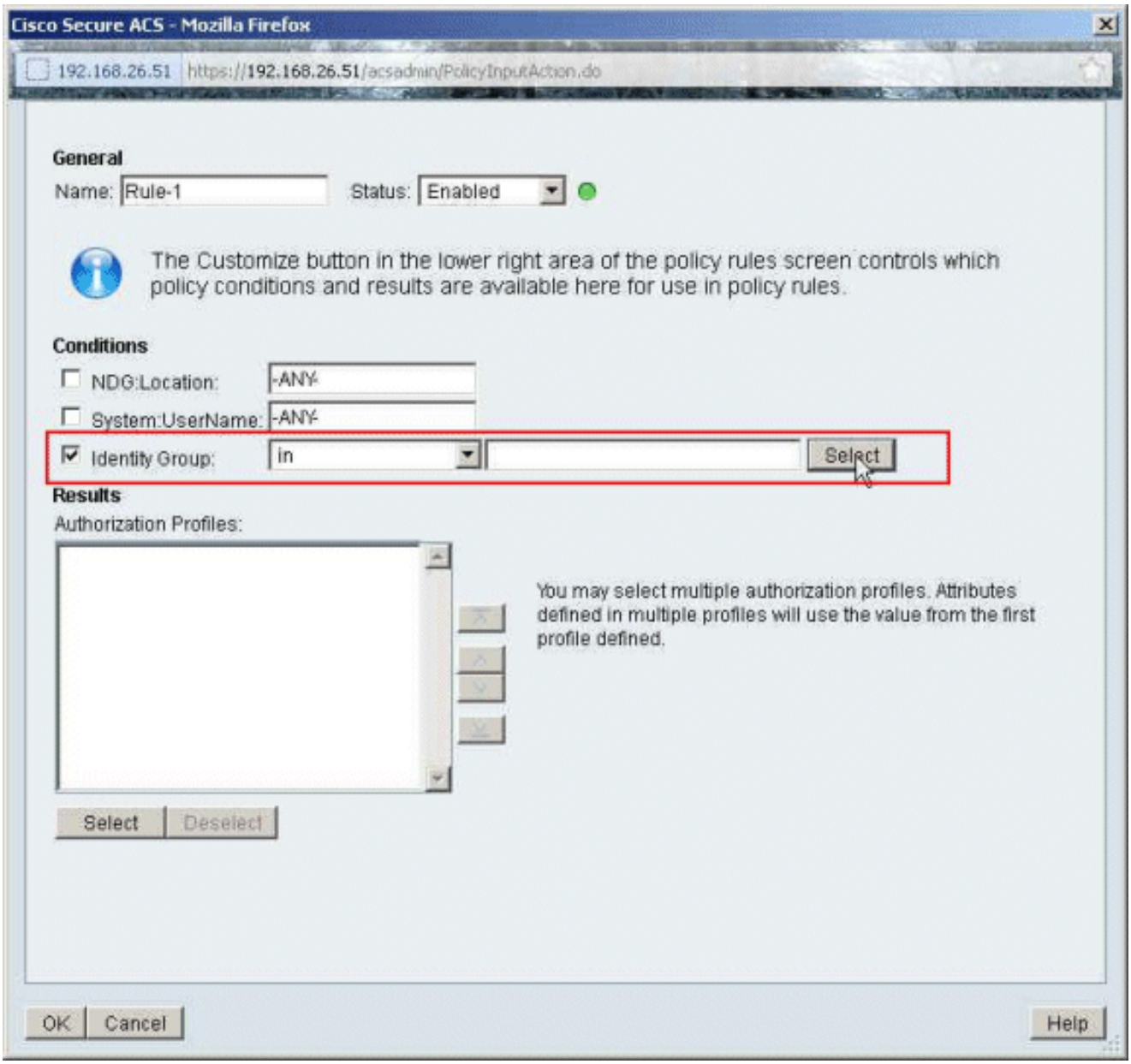
3. انقر فوق علامة التبويب مهام مشتركة، واختر ثابتة من القائمة المنسدلة ل قائمة التحكم في الوصول (ACL) الخاصة بمعرف التصفية. أدخل اسم قائمة الوصول جديدا في حقل القيمة، وانقر فوق إرسال.



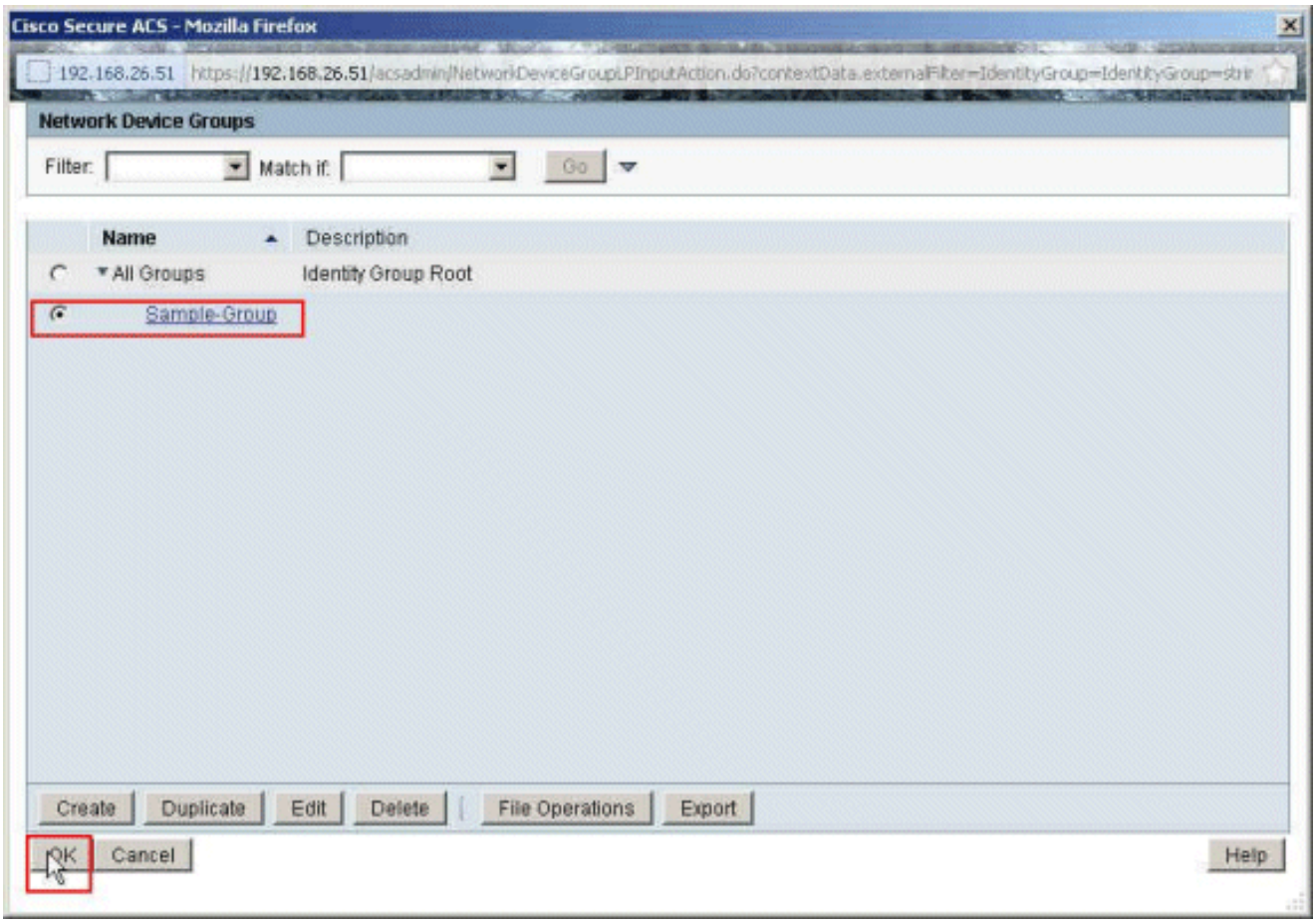
4. أختر سياسات الوصول > خدمات الوصول>الوصول الافتراضي إلى الشبكة > التفويض، وانقر فوق إنشاء لإنشاء قاعدة جديدة.



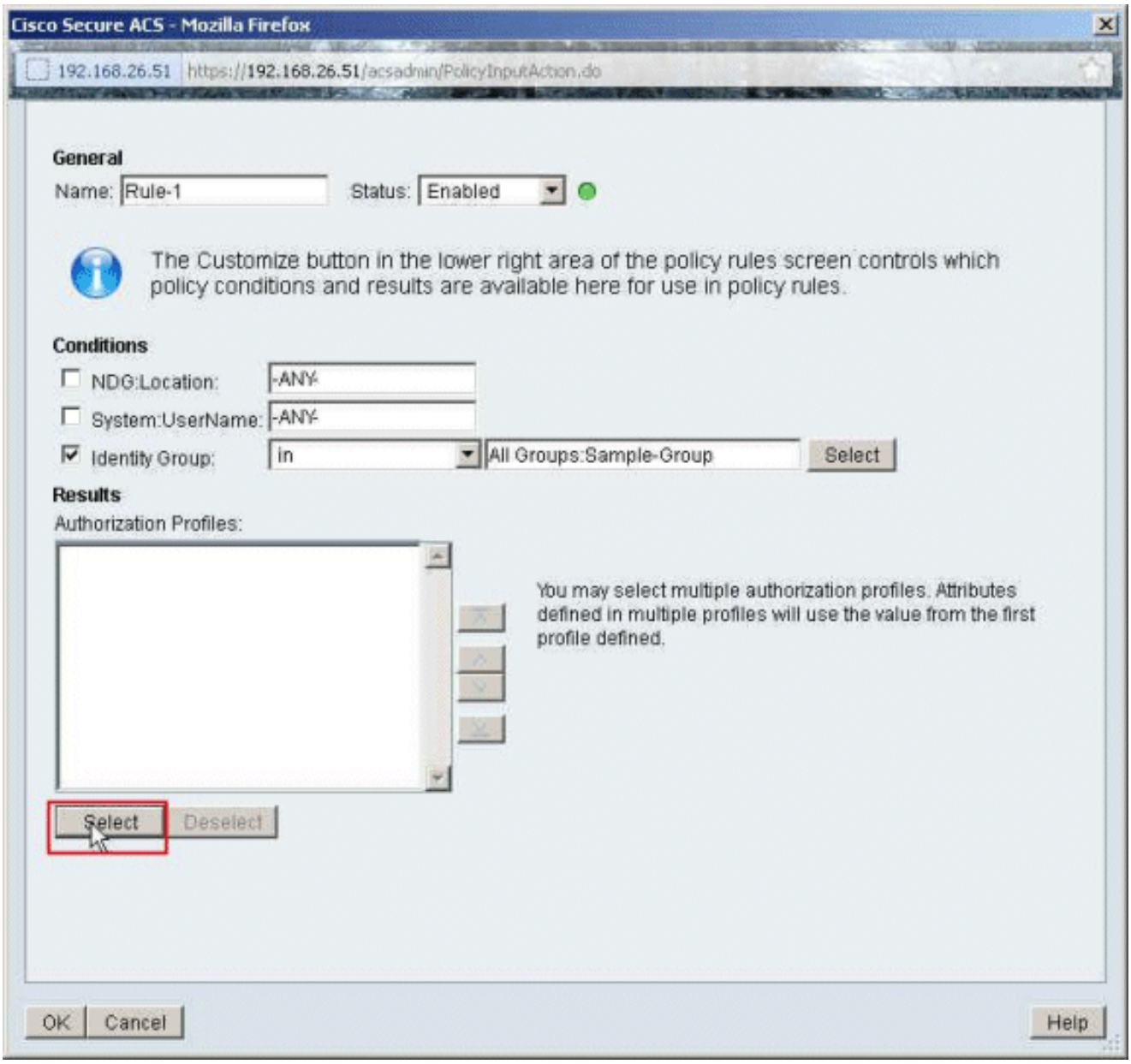
5. تأكد من أن خانة الاختيار المجاورة لمجموعة الهوية محددة، وانقر تحديد.



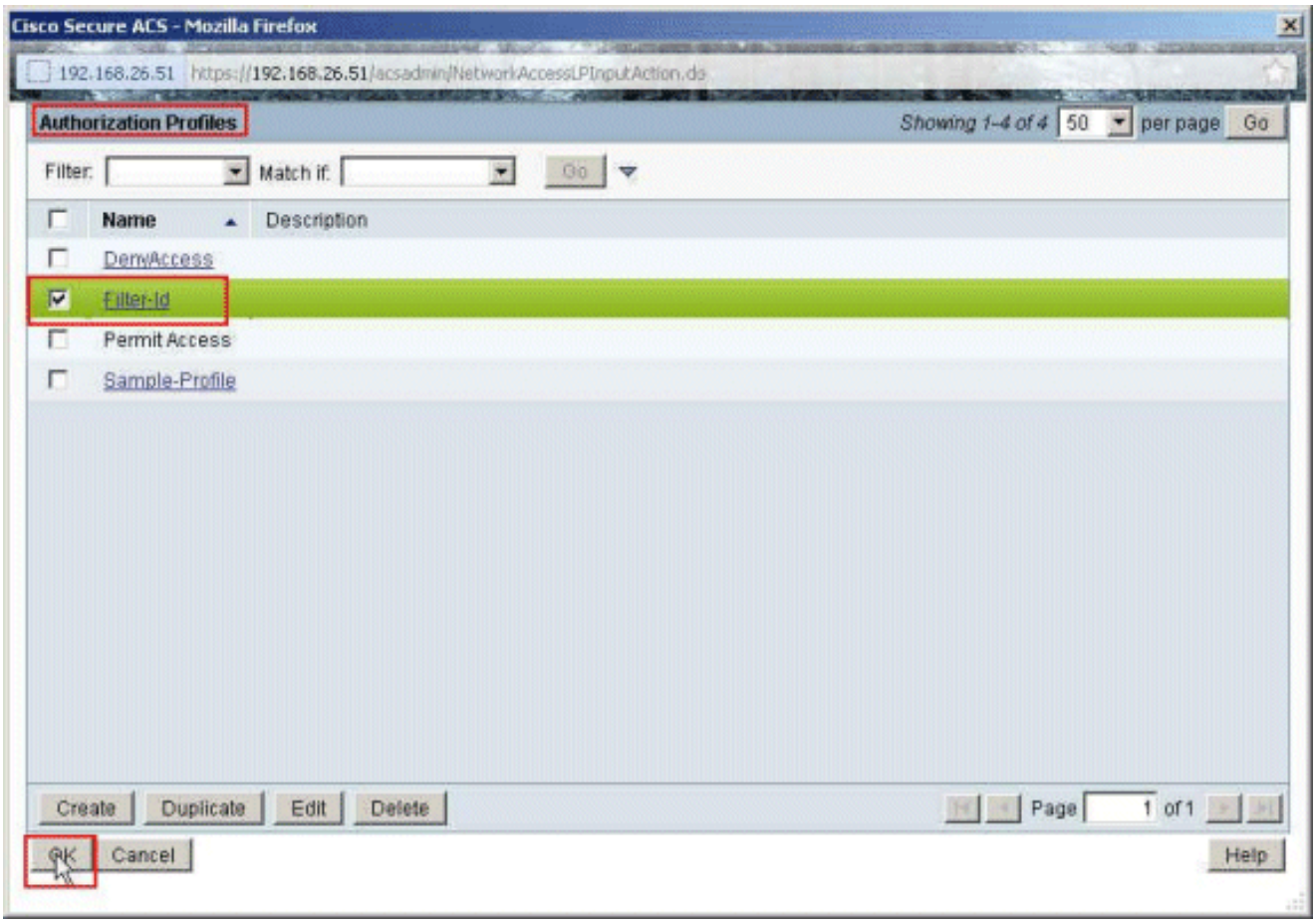
6. أخترت عينة مجموعة، وطقطقة ok.



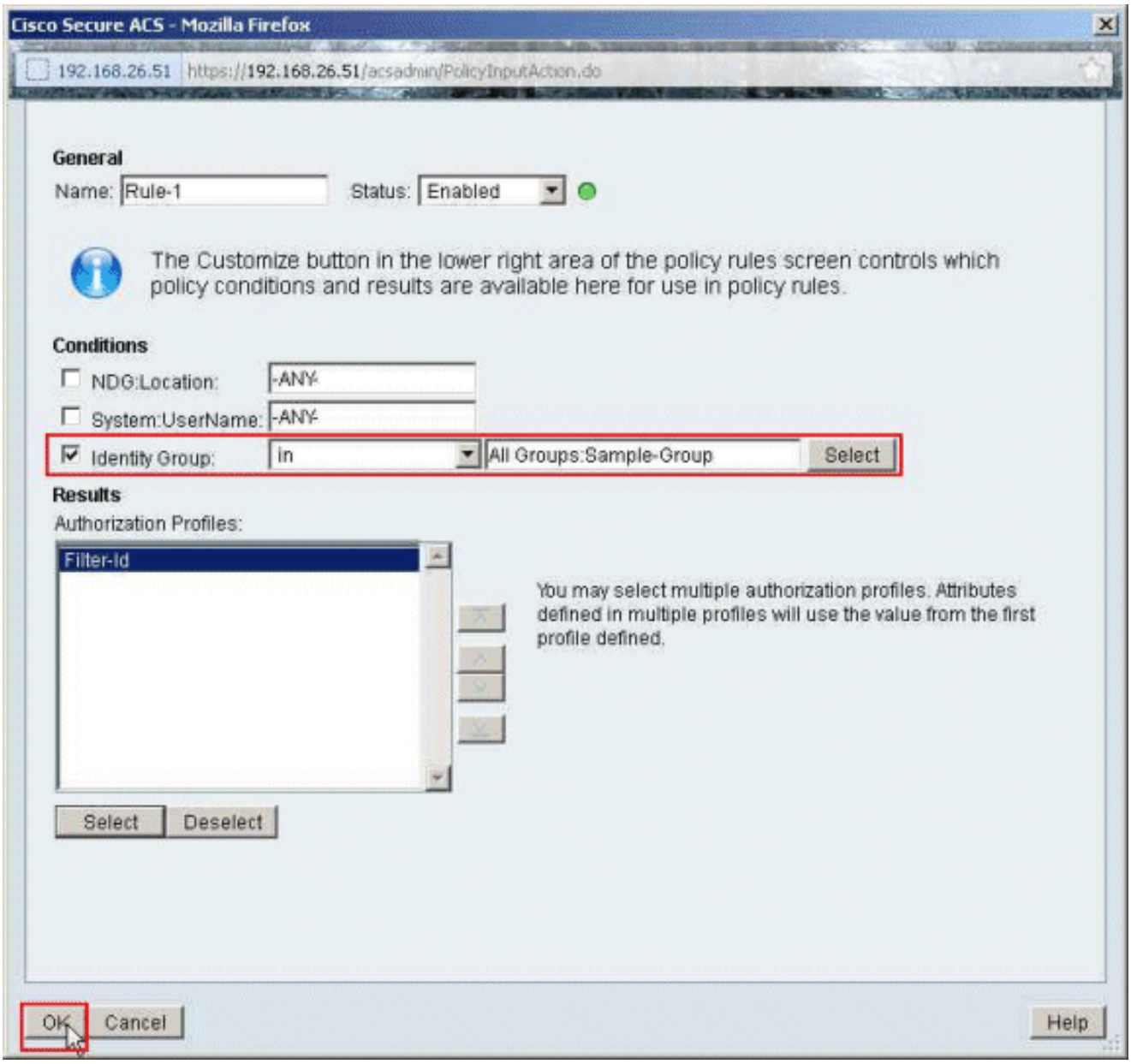
7. انقر على تحديد في قسم توصيفات التخويل.



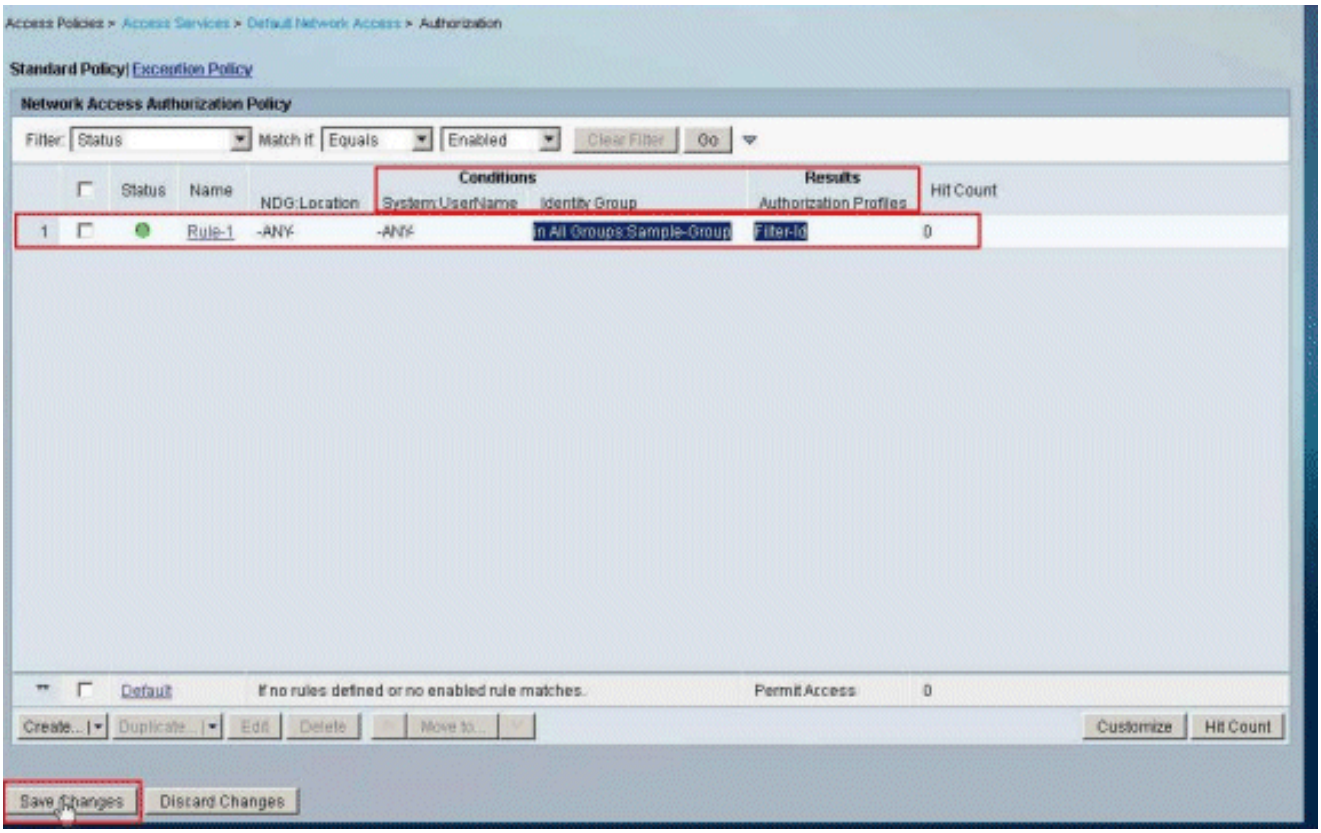
8. أختر معرف عامل تصفية ملف تعريف التخويل الذي تم إنشاؤه مسبقا، وانقر فوق موافق.


Cisco Secure ACS - Mozilla Firefox
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.do
Authorization Profiles
Showing 1-4 of 4 50 per page Go
Filter: Match if: Go
Name Description
DenyAccess
Filter-Id
Permit Access
Sample-Profile
Create Duplicate Edit Delete
Page 1 of 1
OK Cancel
Help

9. انقر فوق OK.



تحقق من إنشاء القاعدة-1 باستخدام مجموعة عينات هوية المجموعة كشرط وfilter-id10. نتيجة لذلك. انقر فوق حفظ التغييرات.



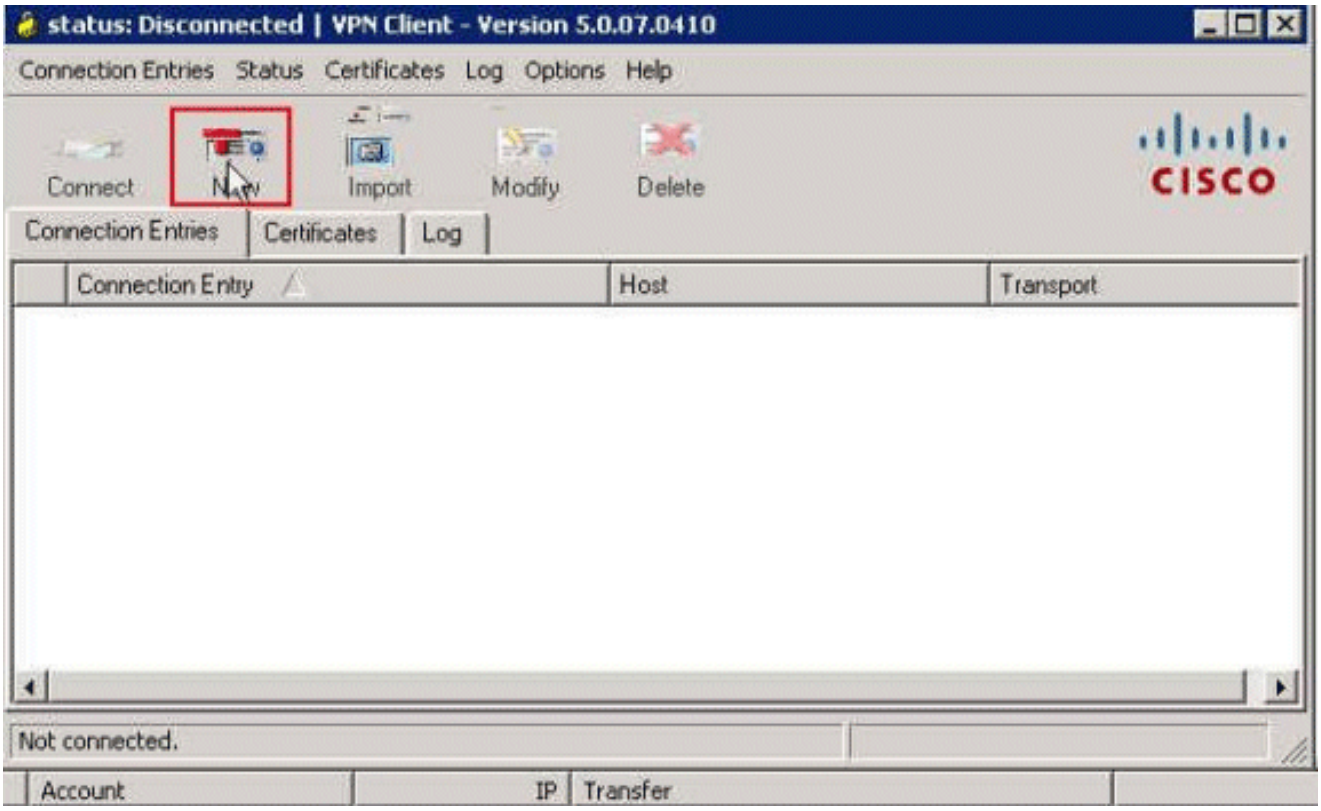
تكوين عميل شبكة VPN من Cisco

قم بالاتصال ب Cisco ASA باستخدام عميل Cisco VPN للتحقق من تكوين ASA بنجاح.

أكمل الخطوات التالية:

1. أخترت بداية>برنامج>cisco نظام VPN زبون>VPN زبون.

2. طقطقت جديد in order to أطلقت ال create جديد VPN توصيل مدخل نافذة



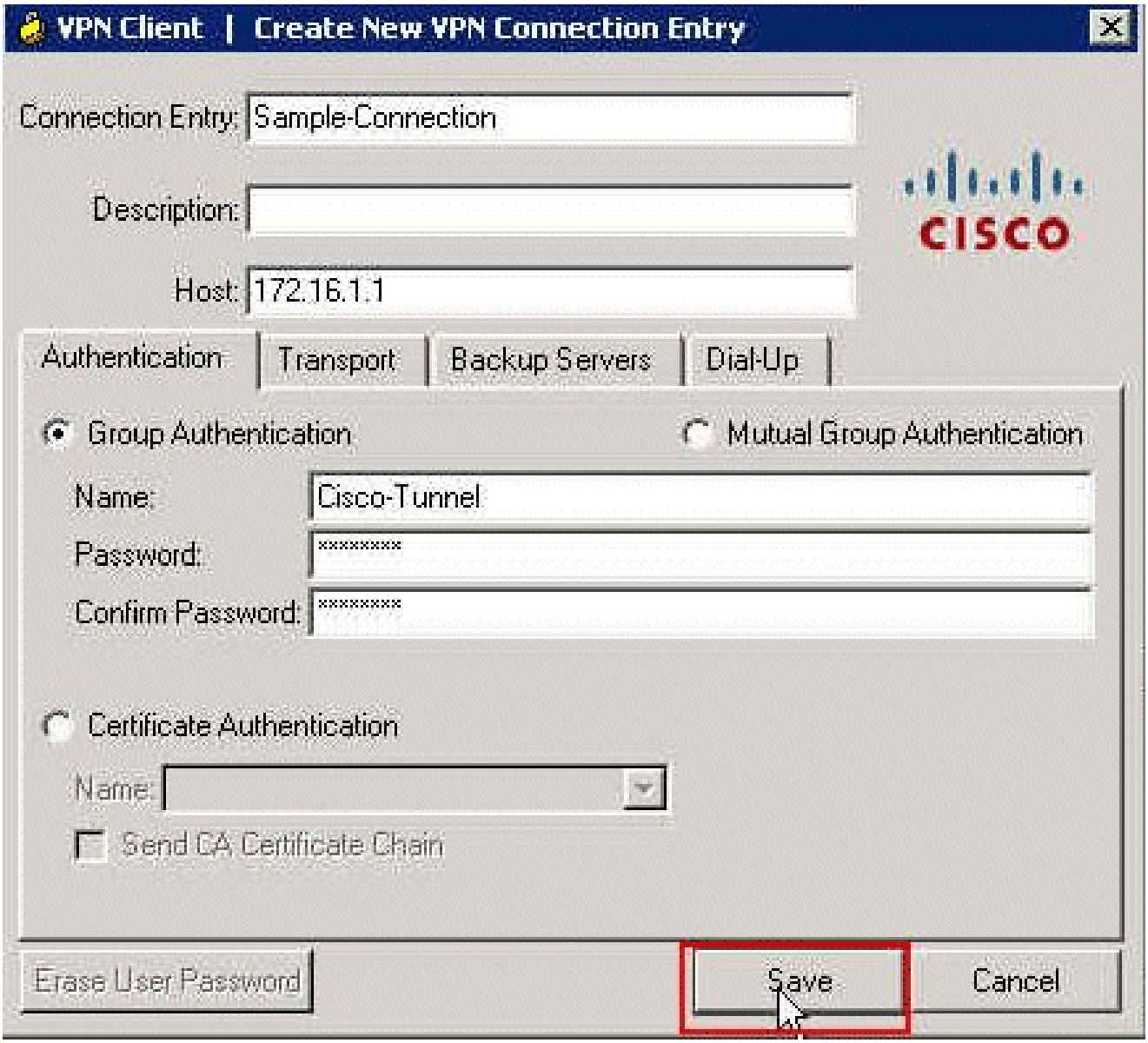
3. المألفة تفاصيل إتصالك الجديد:

a. أدخل اسم "إدخال الاتصال" مع وصف

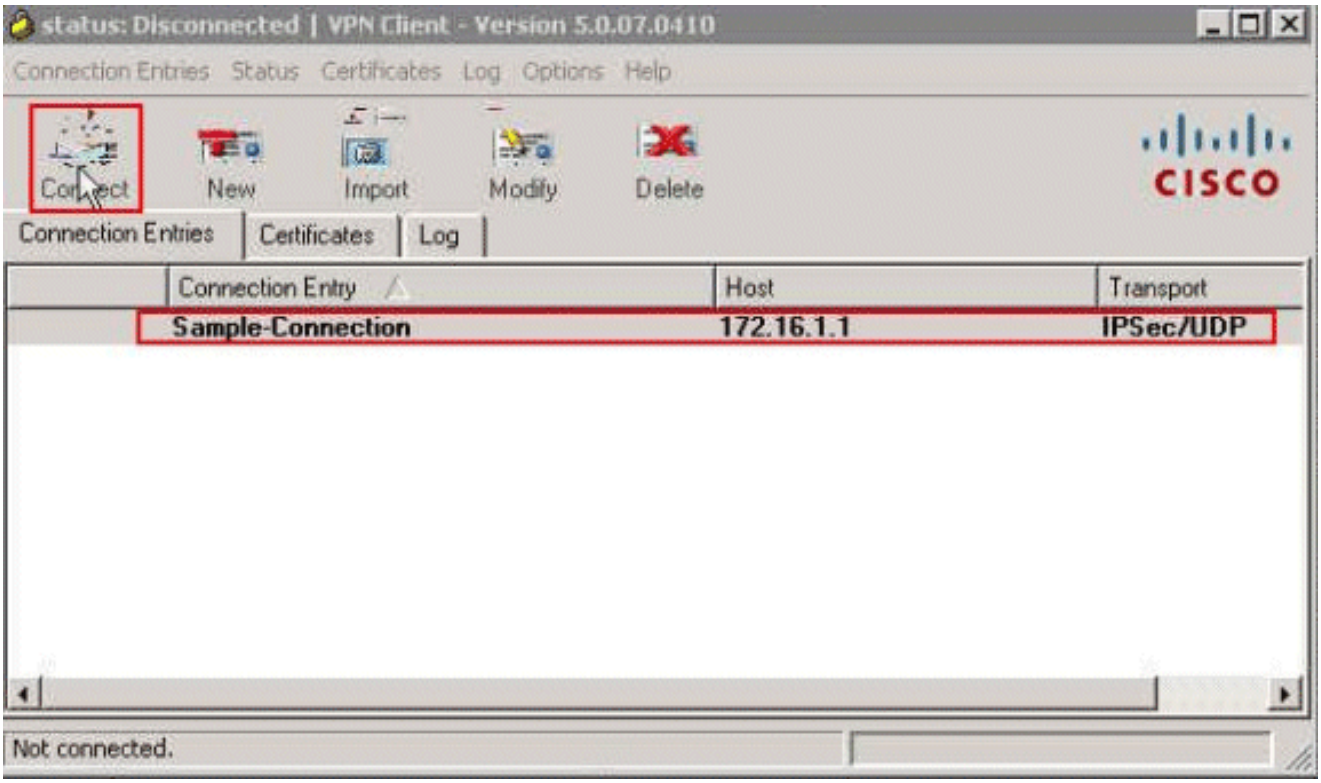
b. دخلت العنوان خارجي من ال ASA في المضيف صندوق

c. أدخل اسم مجموعة نفق VPN (Cisco-Tunnel) وكلمة المرور (مفتاح مشترك مسبقا Cisco123) كما تم تكوينها في ASA.

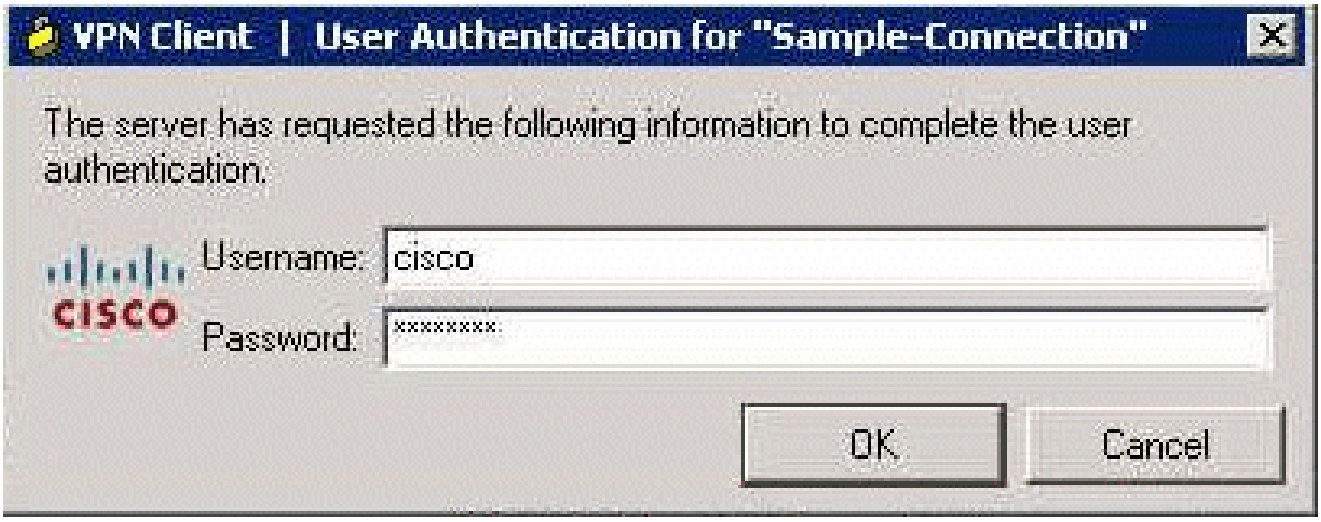
d. انقر فوق حفظ



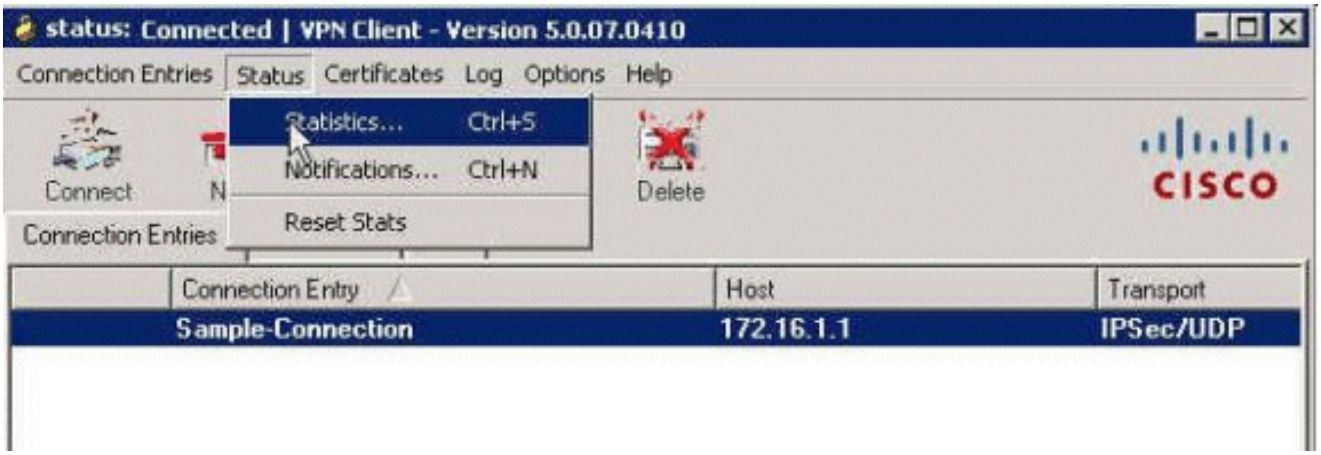
4. انقر فوق الاتصال الذي تريد إستخدامه، ثم انقر فوق الاتصال من الإطار الرئيسي لعميل شبكة VPN.



5. دخلت عندما حث، ال username cisco وكلمة cisco123 كما شكلت في ال ASA للمصادقة، وطقطقة ok in order to ربطت إلى الشبكة بعيد.



6. بمجرد تأسيس الاتصال بنجاح، أختر إحصائيات من قائمة الحالة للتحقق من تفاصيل النفق.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

إظهار أوامر التشفير

- show crypto isakmp sa - يعرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.

```
<#root>

ciscoasa#

sh crypto isakmp sa


IKEv1 SAs:

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.16.1.50
Type    : user              Role    : responder
Rekey   : no                State   : AM_ACTIVE
ciscoasa#
```

- show crypto ipSec - يعرض الإعدادات المستخدمة من قبل SAs الحالية.

```
<#root>

ciscoasa#

sh crypto ipsec sa

interface: outside
Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr:
```

```
                                                                    172.16.1.1

                local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0)
                               current_peer: 172.16.1.50, username: cisco
                                      dynamic allocated peer ip: 10.2.2.1

                        #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
                #pkts decaps: 333, #pkts decrypt: 333, #pkts verify: 333
                               #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly:
                                                                      0
                                          #send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.1.50/0
                        path mtu 1500, ipsec overhead 74, media mtu 1500
                                     current outbound spi: 9A06E834
                                     current inbound spi : FA372121

                                                    inbound esp sas:
                                               spi: 0xFA372121 (4197916961)
                                transform: esp-aes esp-sha-hmac no compression
                                            in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 16384, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
                                sa timing: remaining key lifetime (sec): 28678
                                                    IV size: 16 bytes
                                             replay detection support: Y
                                                    Anti replay bitmap:
                                                 0xFFFFFFFF 0xFFFFFFFF
                                                    outbound esp sas:
                                               spi: 0x9A06E834 (2584143924)
                                transform: esp-aes esp-sha-hmac no compression
                                            in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 16384, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP
                                sa timing: remaining key lifetime (sec): 28678
                                                    IV size: 16 bytes
                                             replay detection support: Y
                                                    Anti replay bitmap:
                                                 0x00000000 0x00000001
```

قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم/المجموعة

تحقق من قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم Cisco. يتم تنزيل قوائم التحكم في الوصول (ACL) من CSACS.

```
<#root>

ciscoasa#

sh access-list

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
                                                    alert-interval 300
                               access-list OUTIN; 1 elements; name hash: 0x683c318c
access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
```

```
access-list #ACSACL#-IP-Sample-DACL-4f3b9117; 2 elements; name hash: 0x3c878038
                                                                    (dynamic)
access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 1 extended permit ip any host
                                                    10.1.1.2 (hitcnt=0) 0x5e896ac3
   access-list #ACSACL#-IP-Sample-DACL-4f3b9117 line 2 extended deny ip any any
                                                        (hitcnt=130) 0x19b3b8f5
```

قائمة التحكم في الوصول (ACL) لمعرف عامل التصفية

تم تطبيق [011] Filter-ID على المجموعة - Sample-Group، وتتم تصفية مستخدمي المجموعة قائمة التحكم في الوصول (ACL) (الجديدة) المحددة في ASA. وفقا لقائمة التحكم في الوصول (ACL)

```
<#root>

ciscoasa#

sh access-list

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
                                                    alert-interval 300
                                access-list OUTIN; 1 elements; name hash: 0x683c318c
            access-list OUTIN line 1 extended permit icmp any any (hitcnt=1) 0x2ba5809c
                                access-list new; 2 elements; name hash: 0xa39433d3

          access-list new line 1 extended permit ip any host 10.1.1.2 (hitcnt=4)
                                                                    0x58a3ea12
          access-list new line 2 extended deny ip any any (hitcnt=27) 0x61f918cd
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها. يتم أيضا عرض إخراج تصحيح الأخطاء للعينة.

ملاحظة: للحصول على مزيد من المعلومات حول أستكشاف أخطاء شبكة VPN الخاصة ب IPsec وإصلاحها، ارجع إلى [حلول لأستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) وإصلاحها](#) للوصول عن بعد و L2L.

مسح الاقترانات الأمنية

عند أستكشاف الأخطاء وإصلاحها، تأكد من مسح حالات SA الموجودة بعد إجراء تغييرات. في الوضع ذي الامتيازات ل PIX، أستخدم الأوامر التالية:

- مسح [crypto] ipSec sa - يحذف شبكات IPsec النشطة. تشفير الكلمة الأساسية الإختياري.
- مسح [crypto] isakmp sa - يحذف شبكات IKE النشطة. تشفير الكلمة الأساسية الإختياري.

اوامر استكشاف الأخطاء وإصلاحها

مجرتم ةادأ مدختسا .show رماوأ ضعب (طقف نيلجسملاءالمعلل) جراخلا مجرتم ةادأ معدت .show رمألا جَرخُم ليلحت ضرعل (OIT) جراخإلا

.debug رماوأ مادختسإ لبق ةحيحصتلا رماوأ لوح ةمهم تامولعم ىلإ عجرا :ةظحالم

2. debug crypto ipSec 7 - يعرض مفاوضات IPsec للمرحلة
1. debug crypto isakmp 7 - يعرض مفاوضات ISAKMP للمرحلة

معلومات ذات صلة

- Cisco من ASA 5500 Series في التكوين للمقارنة الأمان أجهزة دعم صفحة
- Cisco ASA 5500 Series Adaptive Security Appliances المعدلة الأمان أجهزة أوامر مراجع Command References
- Cisco من المعدلة الأمان أجهزة حلول إدارة
- IKE بروتوكولات/IPsec مفاوضة دعم صفحة
- Cisco من VPN شبكة عميل دعم صفحة
- Cisco من الوصول في التحكم أنظمة من
- طلبات التعليقات (RFCs)
- Cisco Systems - المستندات والدعم التقني

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).