تقنية القفل والمفتاح: قوائم الوصول الديناميكية

المحتويات

المقدمة

يسمح لك الوصول القفل والمفتاح بإعداد قوائم وصول ديناميكية تمنح الوصول لكل مستخدم إلى مضيف مصدر/وجهة محدد من خلال عملية مصادقة المستخدم. يتم السماح بوصول المستخدم من خلال جدار حماية Cisco IOS® بشكل ديناميكي، دون أي تضحيات في قيود الأمان.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. في هذه الحالة، كانت بيئة المختبر تتألف من موجه 2620 يشغل برنامج Cisco IOS® الإصدار 12.3(1). بدأت جميع الأجهزة المُستخدمة 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.

اعتبارات الانتحال

يسمح الوصول القفل والمفتاح لحدث خارجي بوضع فتح في جدار حماية Cisco IOS. بعد وجود هذا الفتح، يكون الموجه عرضة لانتحال عنوان المصدر. لمنع ذلك، قم بتوفير دعم التشفير باستخدام تشفير IP مع المصادقة أو التشفير.

الانتحال مشكلة في جميع قوائم الوصول الموجودة. لا يعالج الوصول إلى تقنية القفل والمفتاح هذه المشكلة.

نظرا لأن الوصول عبر تقنية القفل والمفتاح يقدم مسارا محتملا من خلال جدار حماية الشبكة، فأنت بحاجة إلى إعتبار الوصول الديناميكي. ويتميز مضيف آخر، يعمل على انتحال عنوانك الذي تمت مصادقته، بإمكانية الوصول خلف جدار الحماية. مع الوصول الديناميكي، هناك أحتمالية أن يستضيف غير مصرح به، يقوم بانتحال عنوانك المصدق عليه، فيحصل على الوصول خلف جدار الحماية. لا يتسبب وصول القفل والمفتاح في مشكلة انتحال العناوين. يتم تعريف المشكلة هنا كمشكلة للمستخدم فقط.

الأداء

ويتأثر الأداء في هاتين الحالتين.

- تفرض كل قائمة وصول ديناميكية إعادة بناء قائمة وصول على محرك تحويل السيليكون (SSE). وهذا يتسبب في إبطاء مسار تحويل SSE مؤقتا.
- تتطلب قوائم الوصول الديناميكية تسهيل مهلة الخمول (حتى إذا تم ترك المهلة إلى الإعداد الافتراضي). لذلك، لا يمكن تحويل قوائم الوصول الديناميكية إلى SSE. يتم معالجة هذه الإدخالات في مسار التحويل السريع للبروتوكول.

راقب تكوينات موجه الحدود. يقوم المستخدمون عن بعد بإنشاء إدخالات قائمة الوصول على الموجه الحدودي. تنمو قائمة الوصول وتتقلص بشكل ديناميكي. تتم إزالة الإدخالات بشكل ديناميكي من القائمة بعد انتهاء صلاحية فترة الخمول أو الحد الأقصى للمهلة. تقلل قوائم الوصول الكبيرة من أداء تحويل الحزم.

متى يمكن إستخدام وصول القفل والمفتاح

فيما يلي مثالان على متى تستخدم الوصول بالقفل والمفتاح:

- عندما تريد أن يكون المضيف البعيد قادرا على الوصول إلى مضيف في الشبكة الداخلية الخاصة بك من خلال الإنترنت. يحد الوصول إلى تقنية القفل والمفتاح من الوصول إلى ما وراء جدار الحماية الخاص بك على أساس مضيف فردي أو شبكة.
- عندما تريد مجموعة فرعية من البيئات المضيفة على شبكة ما للوصول إلى مضيف على شبكة بعيدة محمية بواسطة جدار حماية. باستخدام الوصول بالقفل والمفتاح، يمكنك تمكين مجموعة مرغوبة من البيئات المضيفة فقط من الوصول عن طريق جعلها مصادقة من خلال خادم TACACS+ أو RADIUS.

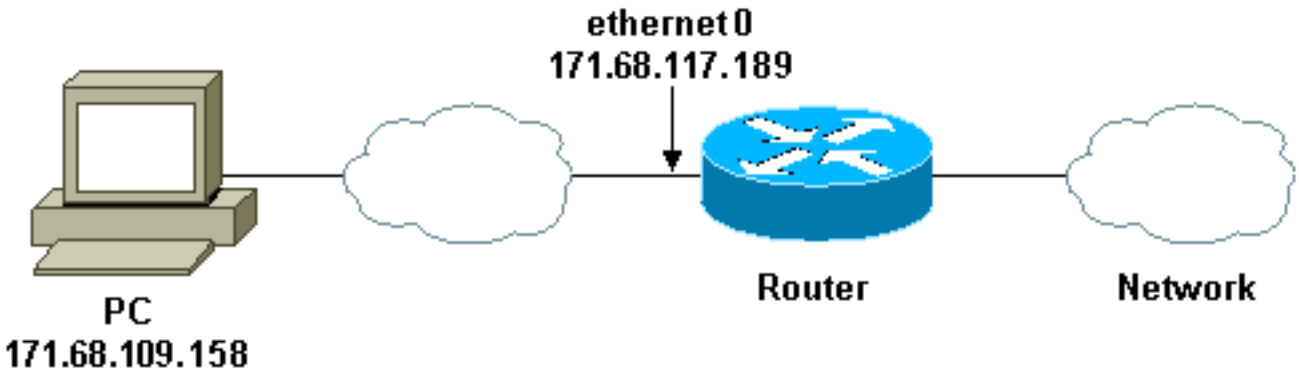
عملية الوصول إلى القفل والمفتاح

تصف هذه العملية عملية الوصول القفل والمفتاح.

1. يقوم مستخدم بفتح جلسة عمل على برنامج Telnet إلى موجه حدود تم تكوينه للوصول القفل والمفتاح.
2. يستقبل برنامج Cisco IOS حزمة Telnet. وهو يجري عملية مصادقة المستخدم. يجب على المستخدم تمرير المصادقة قبل السماح بالوصول. تتم عملية المصادقة بواسطة الموجه أو خادم وصول مركزي مثل خادم TACACS+ أو RADIUS.

نموذج التكوين واستكشاف الأخطاء وإصلاحها

الرسم التخطيطي للشبكة



توصي Cisco باستخدام خادم TACACS+ لعملية استعلام المصادقة الخاصة بك. يوفر TACACS+ خدمات المصادقة والتفويض والمحاسبة. كما يوفر أيضا دعم البروتوكول ومواصفات البروتوكول وقاعدة بيانات أمان مركزية.

يمكنك مصادقة المستخدم على الموجه أو مع خادم TACACS+ أو RADIUS.

ملاحظة: تكون هذه الأوامر عامة ما لم يذكر خلاف ذلك.

في الموجه، يلزمك **اسم مستخدم** للمستخدم للمصادقة المحلية.

```
username test password test
```

يتسبب وجود **تسجيل الدخول المحلي** على خطوط vty في إستخدام اسم المستخدم هذا.

```
line vty 0 4
 login local
```

إذا كنت لا تثق في أن المستخدم يصدر الأمر **access-enable**، فيمكنك القيام بأحد الأمرين:

- قم بإقران المهلة بالمستخدم على أساس كل مستخدم.

```
username test autocommand access-enable host
timeout 10
```

أو

- فرض أن يكون لدى كافة المستخدمين الذين يدخل Telnet نفس المهلة.

```
line vty 0 4
 login local
autocommand access-enable host timeout 10
```

ملاحظة: ال 10 في الصياغة هي مهلة *وضع الخمول* لقائمة الوصول. ويتم تجاوزه بالمهلة المطلقة في قائمة الوصول الديناميكي.

قم بتحديد قائمة الوصول الموسعة التي يتم تطبيقها عند تسجيل مستخدم (أي مستخدم) في الموجه وإصدار الأمر

access-enable. تم تعيين الحد الأقصى للوقت المطلق ل "الثقب" هذا في عامل التصفية إلى 15 دقيقة. بعد 15 دقيقة، تغلق الفتحة ما إذا كان أي شخص يستخدمها أم لا. يجب أن يكون اسم **قائمة** الاختبارات موجودا ولكنه ليس كبيرا. تحديد الشبكات التي يمكن للمستخدم الوصول إليها عن طريق تكوين عنوان المصدر أو الوجهة (هنا، المستخدم غير محدود).

```
access-list 120 dynamic testlist timeout 15 permit ip any any
```

حدد قائمة الوصول اللازمة لحظر كل شيء باستثناء القدرة على إستخدام Telnet في الموجه (لفتح فتحة، يحتاج المستخدم إلى إستخدام Telnet في الموجه). عنوان IP هنا هو عنوان IP للموجه الخاص بالإيثرنت.

```
access-list 120 permit tcp any host 171.68.117.189 eq telnet
```

هناك **رفض** ضمني **الكل** في النهاية (غير مدرج هنا).

تطبيق قائمة الوصول هذه على الواجهة التي يأتي المستخدمون إليها.

```
interface ethernet1
ip access-group 120 in
```

لقد انتهيت.

هذا ما يبدو عليه عامل التصفية على الموجه الآن:

```
Router#show access-lists
Extended IP access list 120
    Dynamic testlist permit ip any any log 10
    (permit tcp any host 171.68.117.189 eq telnet (68 matches 20
```

لا يتمكن المستخدمون الذين يحصلون على حق الوصول إلى شبكتك الداخلية من رؤية أي شيء حتى يقوموا بوضع برنامج Telnet بالموجه.

ملاحظة: يمثل **الرقم 10** هنا مهلة *وضع الخمول* لقائمة الوصول. ويتم تجاوزه بالمهلة المطلقة في قائمة الوصول الديناميكي.

```
telnet 2514A%
... Trying 171.68.117.189
.Connected to 2514A.network.com
.'[^' Escape character is

User Access Verification

Username: test
Password: test

.Connection closed by foreign host
```

يبدو المرشح هكذا.

```
Router#show access-lists
Extended IP access list 120
```

```
Dynamic testlist permit ip any any log 10
(permit ip host 171.68.109.158 any log (time left 394
(permit tcp any host 171.68.117.189 eq telnet (68 matches 20
```

هناك ثقب في عامل التصفية لهذا المستخدم الواحد استنادا إلى عنوان IP المصدر. عندما يقوم شخص آخر بذلك، سترى *ثقبين*.

```
Router#show ip access-lists 120
    Extended IP access list 120
Dynamic testlist permit ip any any log 10
  permit ip host 171.68.109.64 any log
 permit ip host 171.68.109.158 any log
(permit tcp any host 171.68.117.189 eq telnet (288 matches 20
```

يمكن لهؤلاء المستخدمين الحصول على وصول IP كامل إلى أي عنوان IP للوجهة من عنوان IP *للمصدر الخاص بهم*.

إستخدام TACACS+

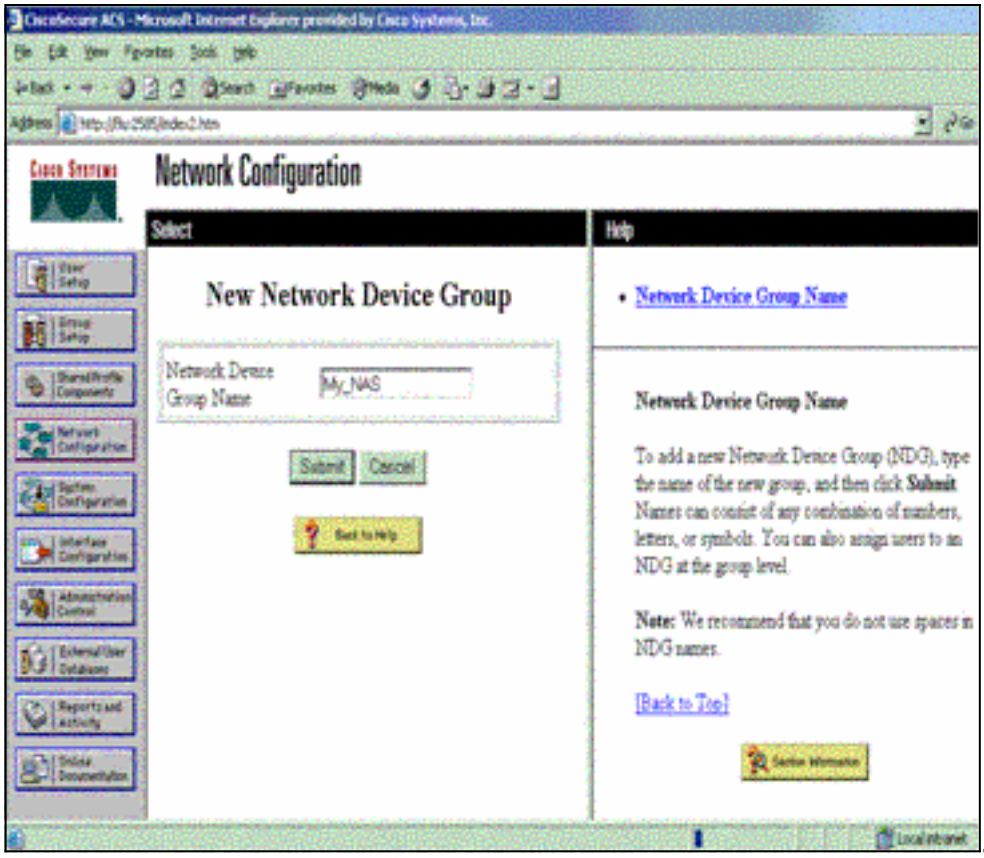
تكوين TACACS+

قم بتكوين خادم TACACS+ لإجبار المصادقة والتفويض على خادم TACACS+ لاستخدام TACACS+، كما يوضح هذا الإخراج:

```
aaa new-model
!
!
aaa authentication login default group tacacs+ local
+aaa authorization exec default group tacacs
 tacacs-server host 10.48.66.53 key cisco123
```

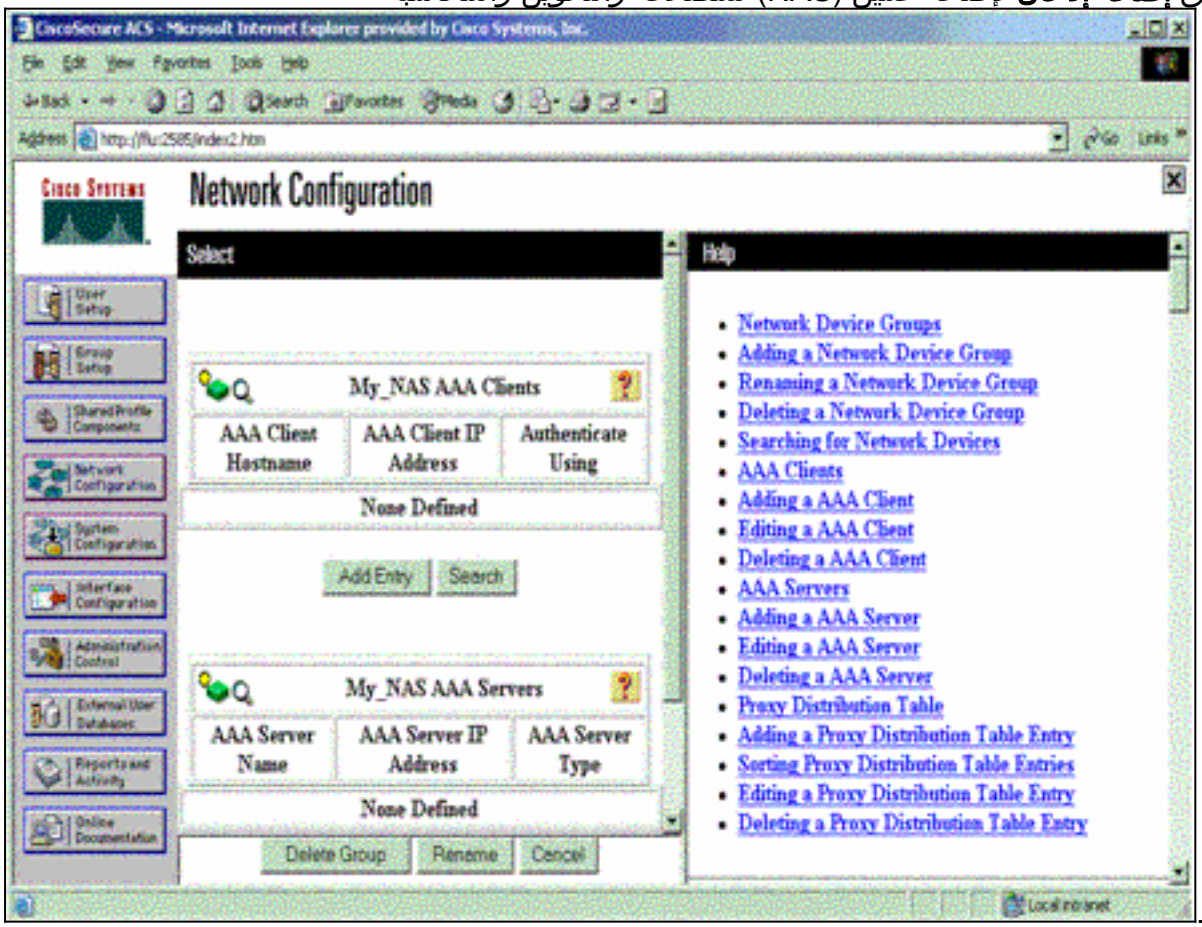
أكمل الخطوات التالية لتكوين TACACS+ على Cisco ACS الآمن ل Windows:

1. افتح مستعرض ويب. أدخل عنوان خادم ACS الخاص بك، والذي يكون في شكل **http://*<IP_ADDRESS>* أو *DNS_NAME*>:2002**. (يستخدم هذا المثال منفذا افتراضيا لعام 2002.) قم بتسجيل الدخول كمسؤول.
2. طقطقة **شبكة تشكيل**. انقر فوق **إضافة إدخال** لإنشاء مجموعة أجهزة شبكة تحتوي على خوادم الوصول إلى الشبكة (NAS). أدخل اسما للمجموعة وانقر فوق



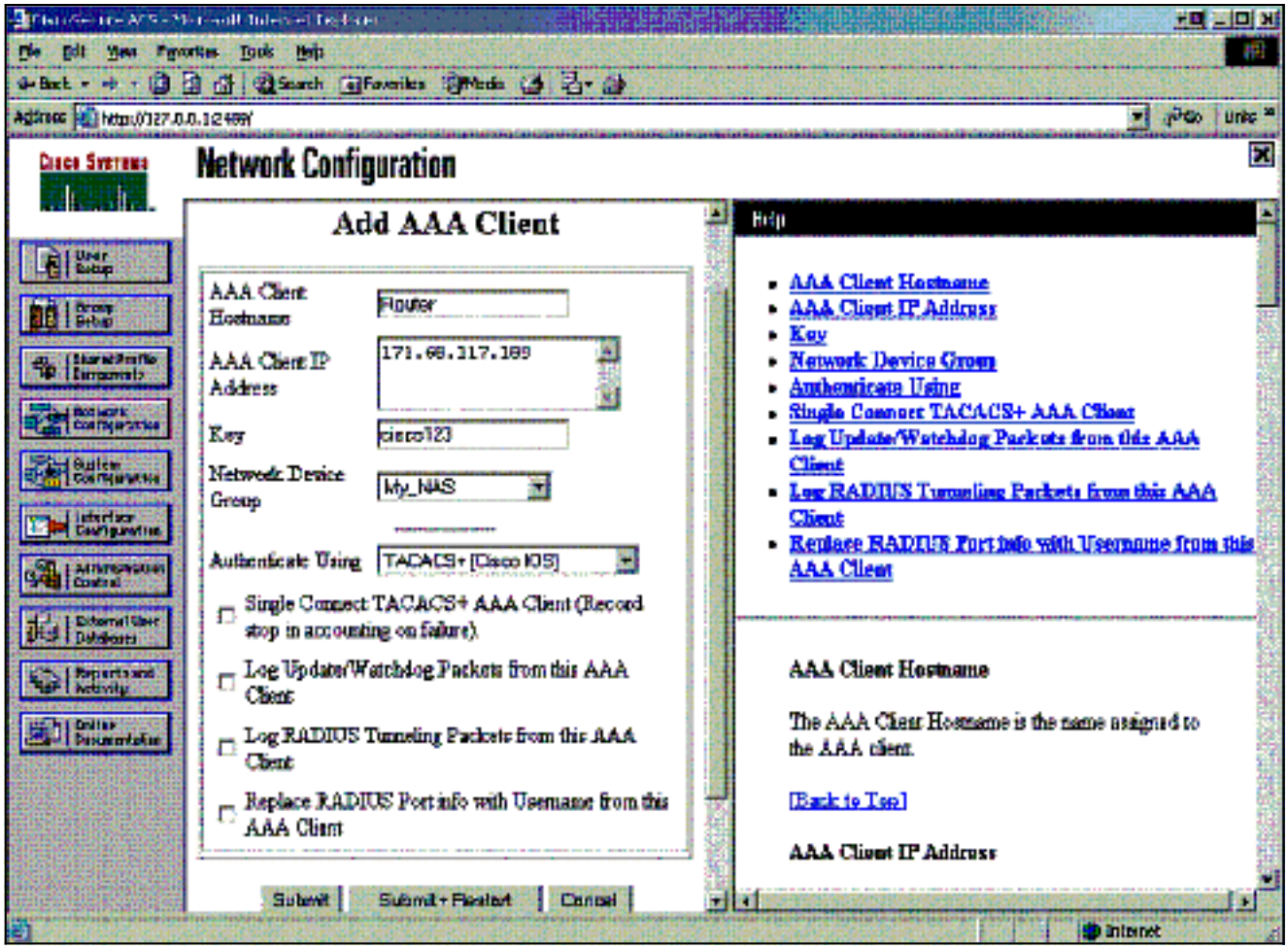
إرسال.

3. انقر فوق **إضافة إدخال** لإضافة عميل (NAS) للمصادقة والتخويل والمحاسبة

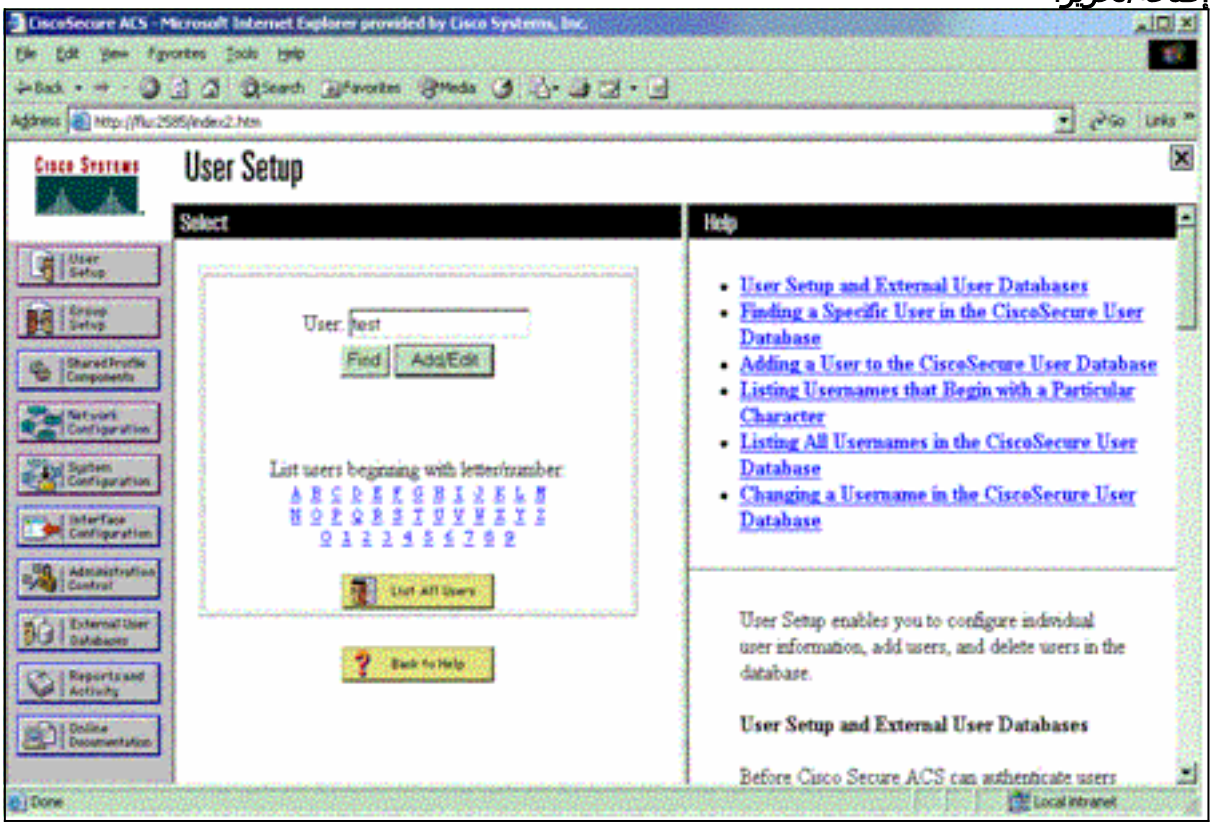


(AAA).

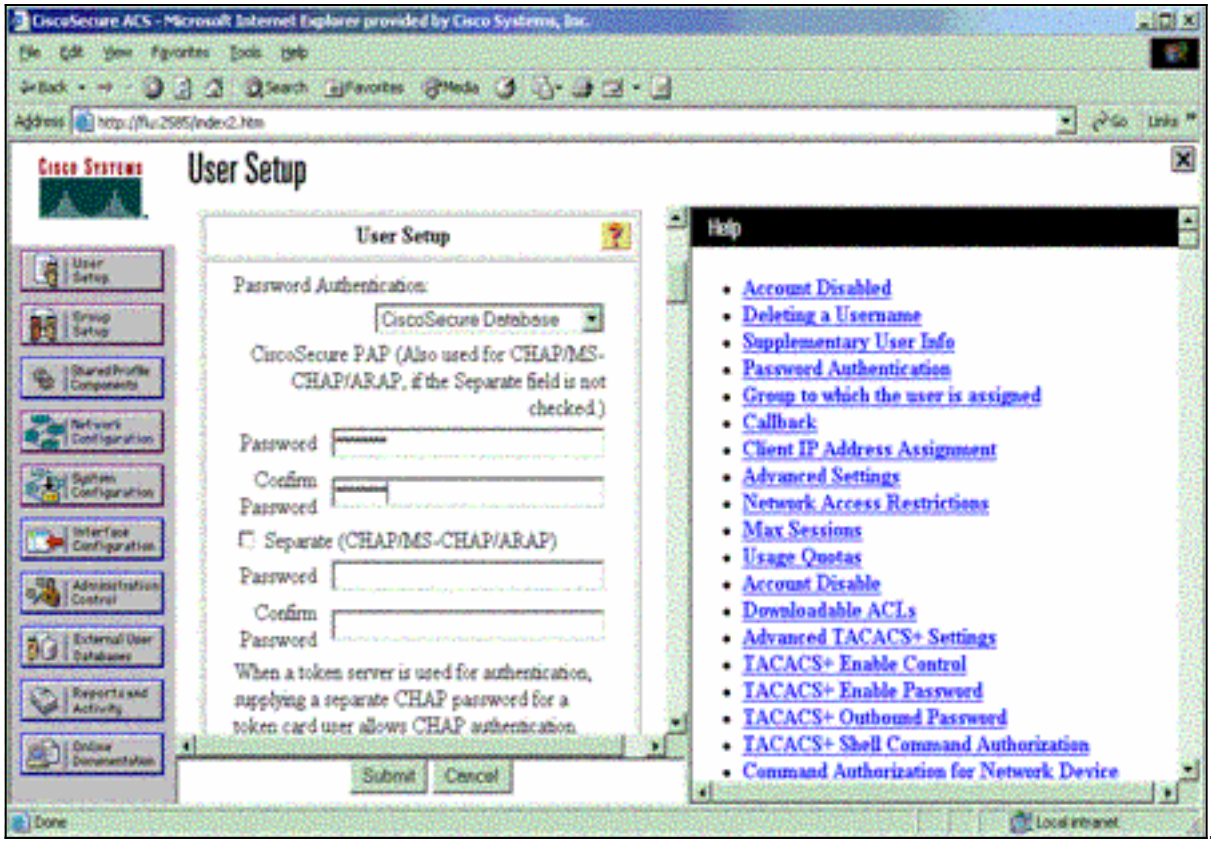
4. أدخل اسم المضيف وعنوان IP والمفتاح المستخدم لتشفير الاتصال بين خادم AAA و NAS. حدد **TACACS+ Cisco IOS)** كطريقة مصادقة. عند الانتهاء، انقر فوق **إرسال +إعادة تشغيل** لتطبيق التغييرات.



5. انقر على **إعداد المستخدم**، وأدخل معرف المستخدم، وانقر فوق **إضافة/تحرير**.

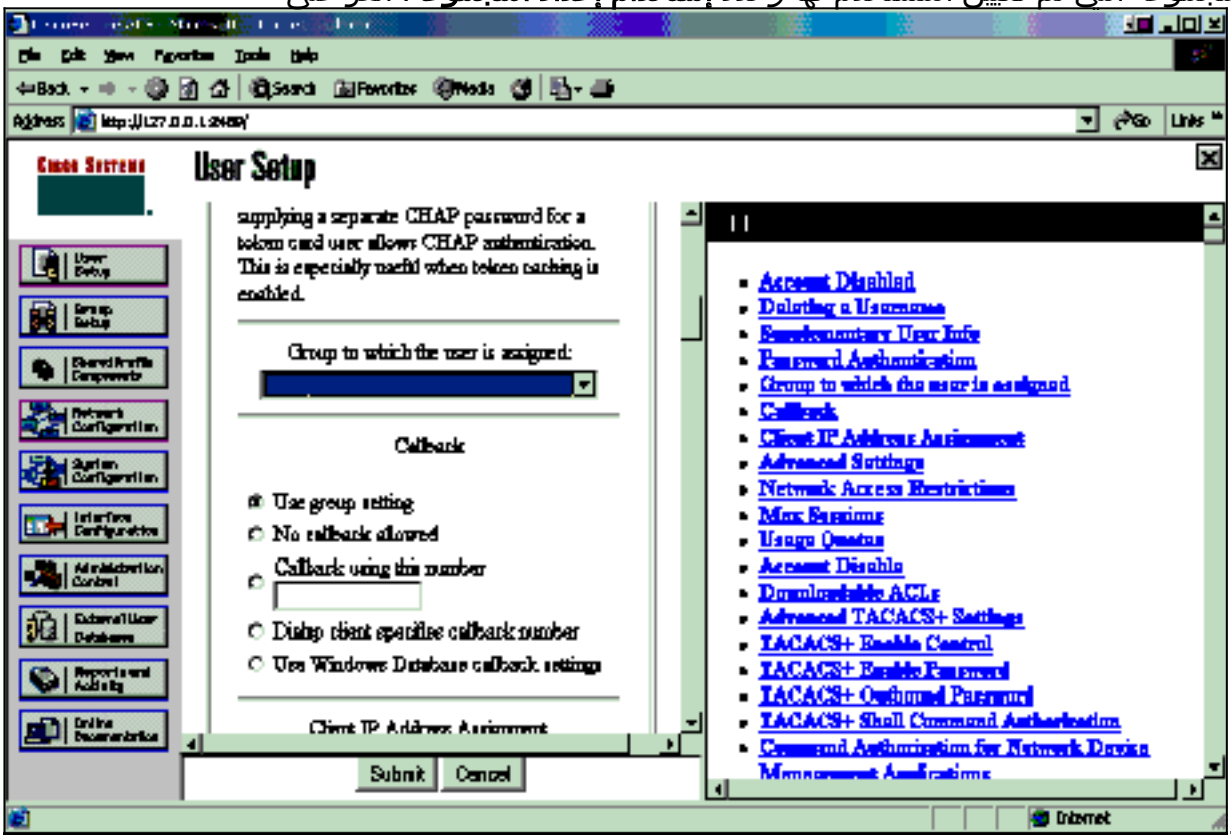


6. أختر قاعدة بيانات لمصادقة المستخدم. (في هذا المثال، يتم إستخدام "إختبار" للمستخدم، ويتم إستخدام قاعدة البيانات الداخلية ل ACS للمصادقة). أدخل كلمة مرور للمستخدم، وقم بتأكيد كلمة



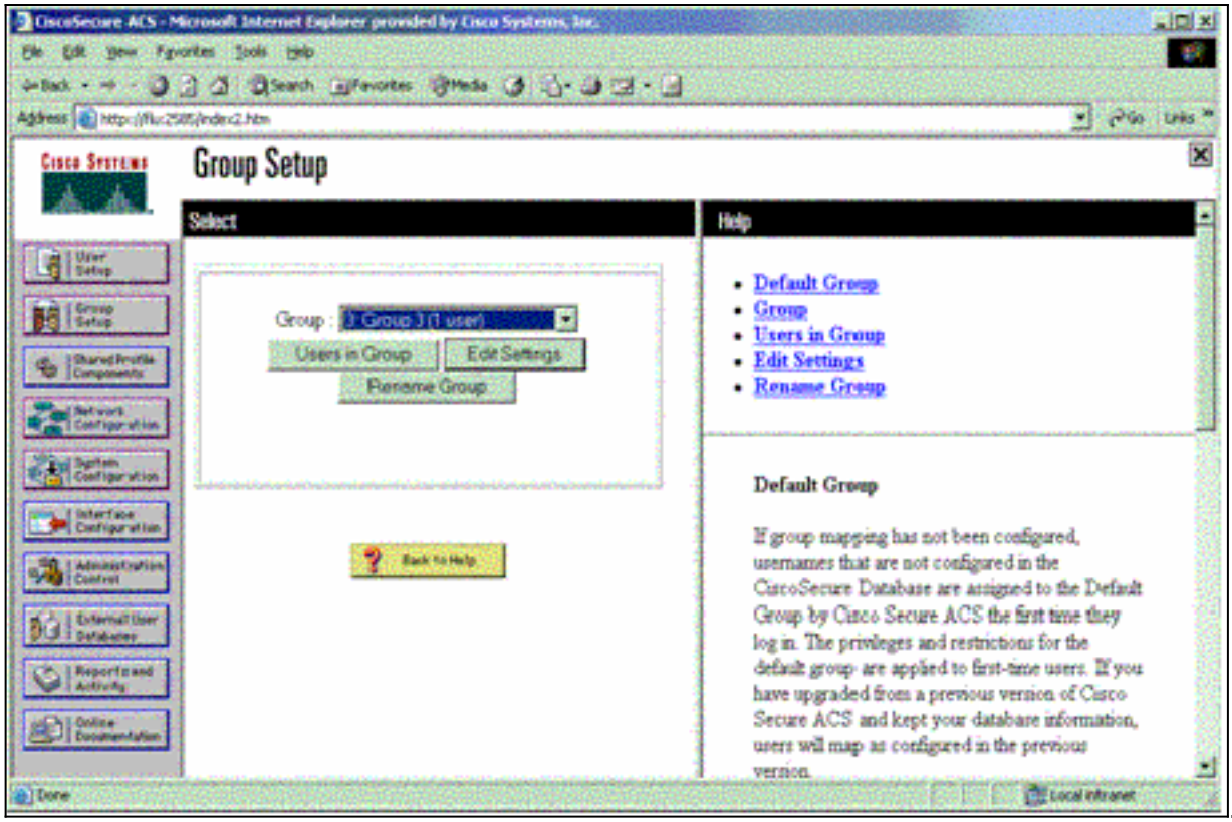
المرور.

7. أختر المجموعة التي تم تعيين المستخدم لها وحدد **إستخدام إعداد المجموعة**. انقر على



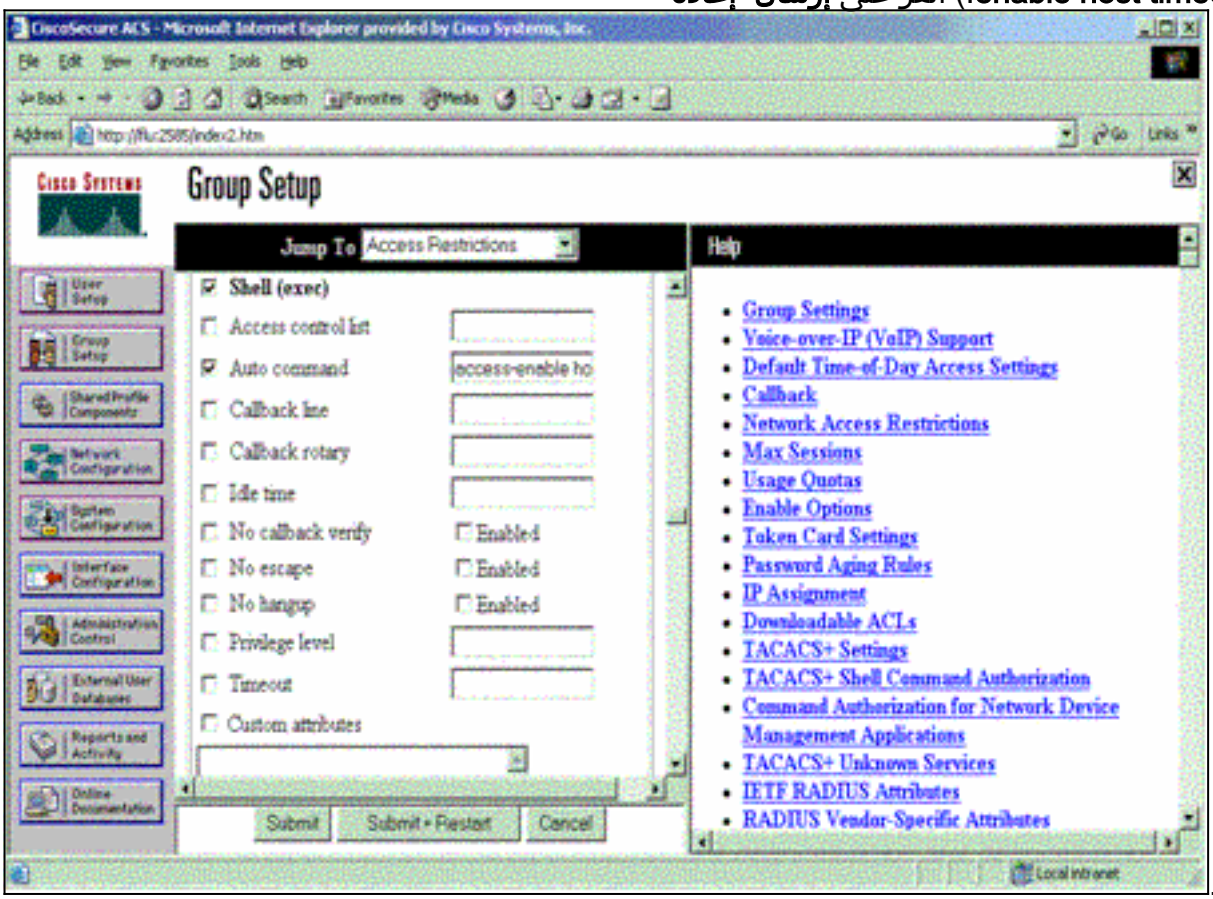
إرسال.

8. انقر على **إعداد المجموعة**. حدد المجموعة التي تم تعيين المستخدم لها في الخطوة 7. طقطقة **يحرر عملية**



إعداد.

9. قم بالتمرير لأسفل إلى قسم إعدادات TACACS+. حدد المربع ل **Shell EXEC**. حدد المربع **للأمر الآلي**. أدخل الأمر التلقائي الذي سيتم تنفيذه عند تفويض المستخدم الناجح. (يستخدم هذا المثال الأمر **access-enable host timeout 10**.) انقر على **إرسال+إعادة**



تشغيل.

أستكشاف أخطاء TACACS+ وإصلاحها

أستخدم أوامر **تصحيح الأخطاء** التالية على وحدات التخزين المتصلة بالشبكة (NAS) لاستكشاف أخطاء TACACS+ وإصلاحها.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- **debug tacacs authentication**—يعرض معلومات حول عملية مصادقة TACACS+. متوفر فقط في بعض إصدارات البرامج. إذا لم يكن متوفرا، فاستخدم **tacacs** الخاصة **بتصحيح الأخطاء** فقط.
- **debug tacacs authorization**—يعرض معلومات حول عملية تفويض TACACS+. متوفر فقط في بعض إصدارات البرامج. إذا لم يكن متوفرا، فاستخدم **tacacs** الخاصة **بتصحيح الأخطاء** فقط.
- **debug tacacs events** — يعرض معلومات من عملية مساعد TACACS+. متوفر فقط في بعض إصدارات البرامج. إذا لم يكن متوفرا، فاستخدم **tacacs** الخاصة **بتصحيح الأخطاء** فقط.

أستخدم هذه الأوامر لاستكشاف أخطاء AAA وإصلاحها:

- **debug aaa authentication**— يعرض معلومات حول مصادقة AAA/TACACS+.
- **تصحيح أخطاء تفويض المصادقة والتفويض والمحاسبة (AAA)**—يعرض معلومات حول تفويض AAA/TACACS+.

يظهر إخراج نموذج **تصحيح الأخطاء** هنا عملية مصادقة وتفويض ناجحة على خادم ACS TACACS+.

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
==========================================================
Router#
AAA/BIND(00000009): Bind i/f
'AAA/AUTHEN/LOGIN (00000009): Pick method list 'default
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication start request id 9
TPLUS: Authentication start packet created for 9()
TPLUS: Using server 10.48.66.53
TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
(expect 16 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 28 bytes response
TPLUS(00000009)/0/82A2E088: Processing the reply packet
TPLUS: Received authen response status GET_USER (7)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
(expect 16 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 28 bytes response
TPLUS(00000009)/0/8347F3FC: Processing the reply packet
TPLUS: Received authen response status GET_PASSWORD (8)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
```

```
TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
                TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
                                (expect 6 bytes data)
                TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 18 bytes response
TPLUS(00000009)/0/8347EE4C: Processing the reply packet
(TPLUS: Received authen response status PASS (2
   'AAA/AUTHOR (0x9): Pick method list 'default
TPLUS: Queuing AAA Authorization request 9 for processing
         TPLUS: processing authorization request id 9
      TPLUS: Protocol set to None .....Skipping
                TPLUS: Sending AV service=shell
                   TPLUS: Sending AV cmd
(TPLUS: Authorization request created for 9(tne-1
   TPLUS: using previously set server 10.48.66.53
                    +from group tacacs
TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
                TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
                TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
                TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
                               (expect 44 bytes data)
                TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 56 bytes response
TPLUS(00000009)/0/8347F508: Processing the reply packet
TPLUS: Processed AV autocmd=access-enable host timeout 10
TPLUS: received authorization response for 9: PASS
     =AAA/AUTHOR/EXEC(00000009): processing AV cmd
          AAA/AUTHOR/EXEC(00000009): processing AV
           autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000009): Authorization successful
```

إستخدام RADIUS

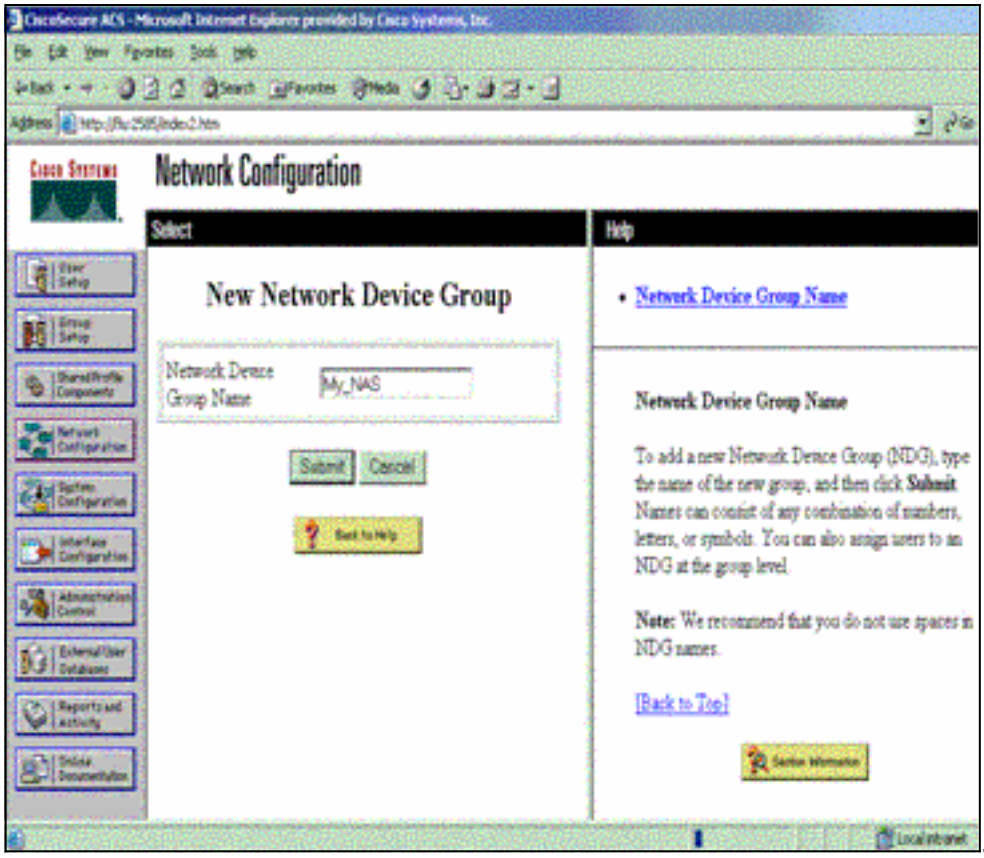
تكوين RADIUS

لاستخدام RADIUS، قم بتكوين خادم RADIUS لفرض إجراء المصادقة على خادم RADIUS باستخدام معلمات التخويل (الأمر التلقائي) التي سيتم إرسالها إلى أسفل في السمة 26 الخاصة بالمورد، كما هو موضح هنا:

```
aaa new-model
                                                                !
                                                                !
                aaa authentication login default group radius local
                  aaa authorization exec default group radius local
                      radius-server host 10.48.66.53 auth-port 1645
                                   acct-port 1646 key cisco123
```

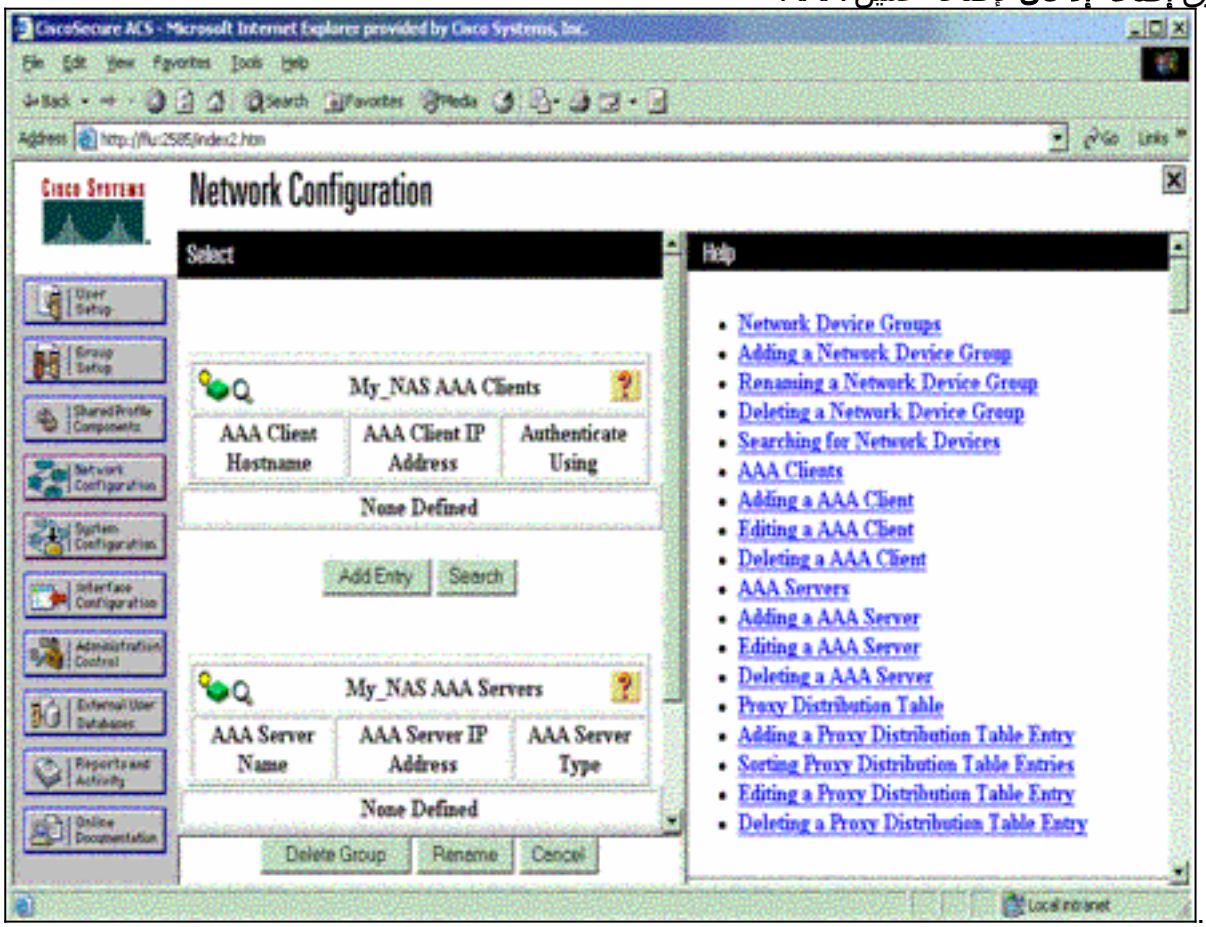
أتمت هذا steps أن يشكل RADIUS على cisco يأمن acs ل Windows:

1. افتح مستعرض ويب وأدخل عنوان خادم ACS الخاص بك، والذي يكون في شكل ***http://<IP_ADDRESS> أو DNS_NAME>*:2002**. (يستخدم هذا المثال منفذا افتراضيا لعام 2002.) قم بتسجيل الدخول كمسؤول.
2. طقطقة **شبكة تشكيل**. انقر فوق **إضافة إدخال** لإنشاء مجموعة أجهزة شبكة تحتوي على وحدات التخزين المتصلة بالشبكة (NAS). أدخل اسما للمجموعة وانقر فوق



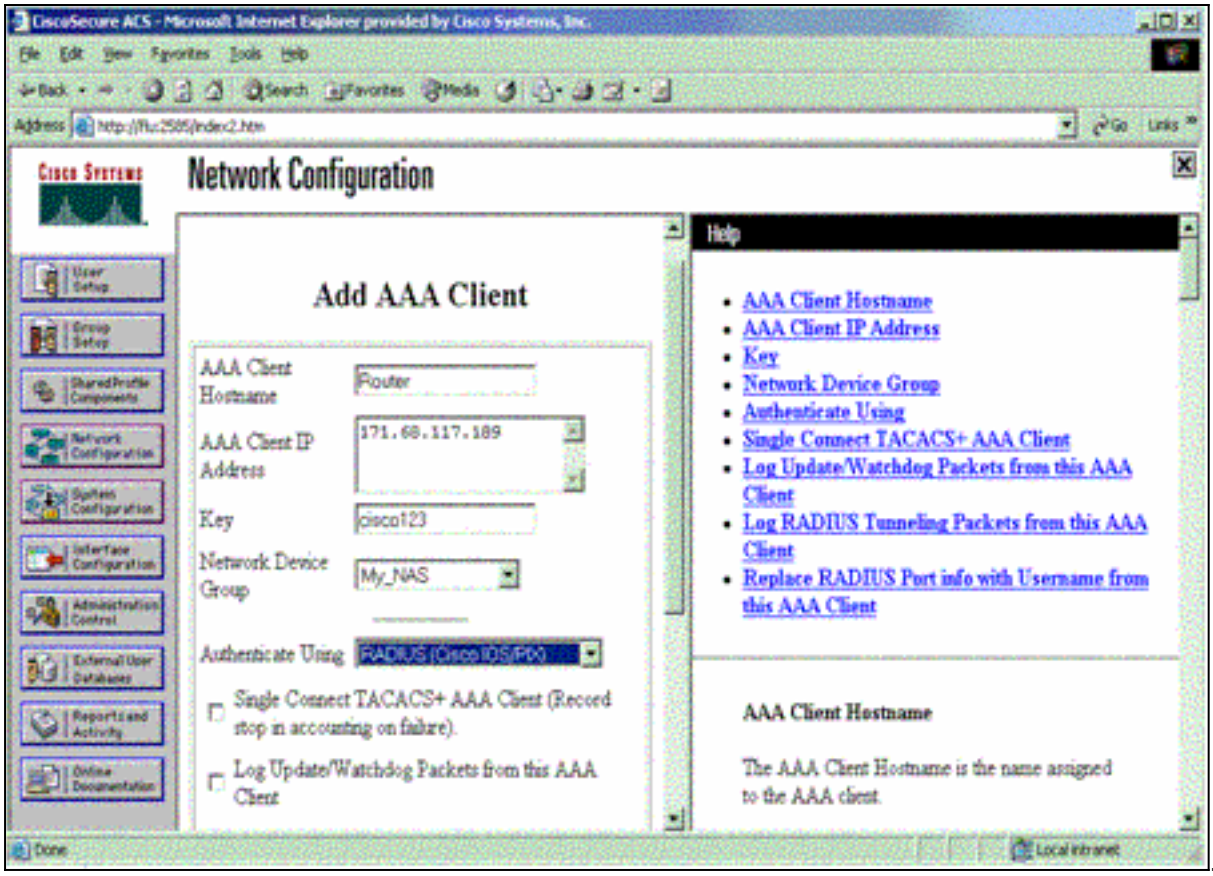
إرسال.

3. انقر فوق **إضافة إدخال** لإضافة عميل AAA



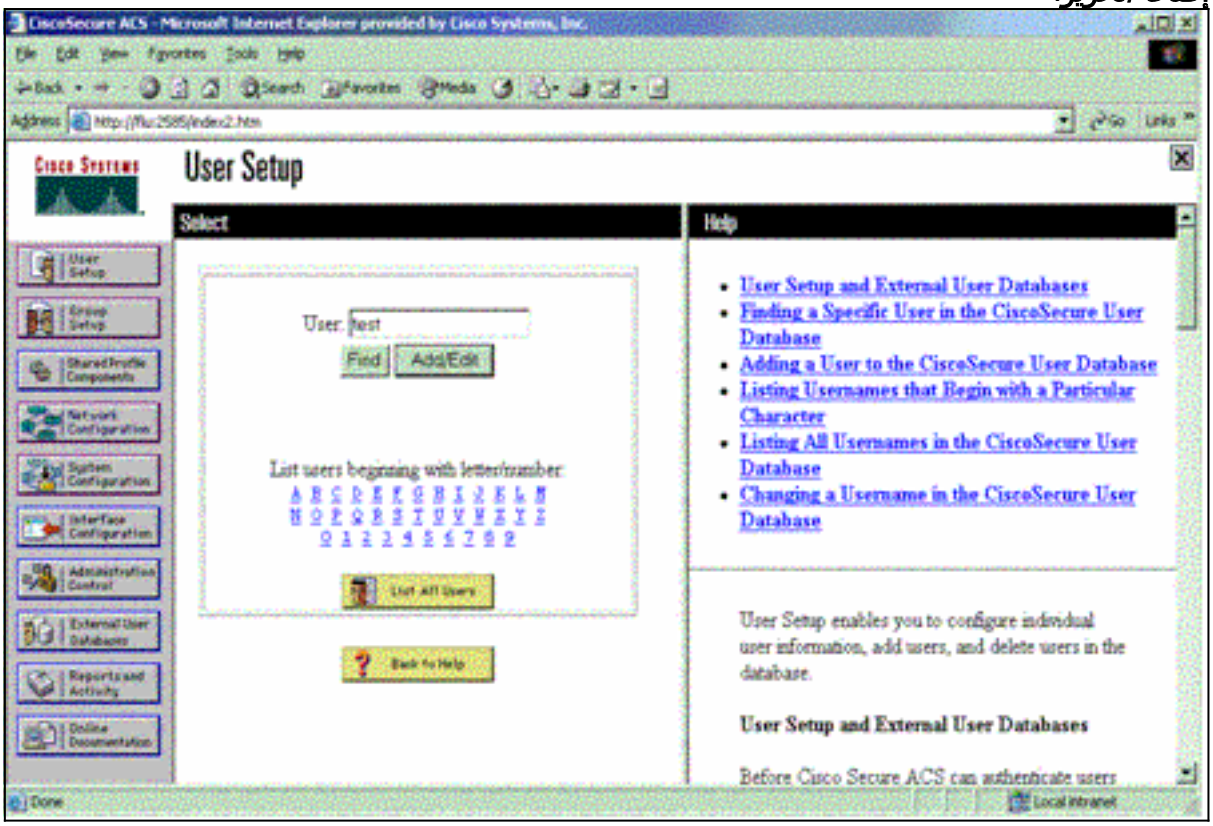
NAS)).

4. أدخل اسم المضيف وعنوان IP والمفتاح المستخدم لتشفير الاتصال بين خادم AAA و NAS. حدد **RADIUS (Cisco IOS/PIX)** كطريقة مصادقة. عند الانتهاء، انقر فوق **إرسال +إعادة تشغيل** لتطبيق

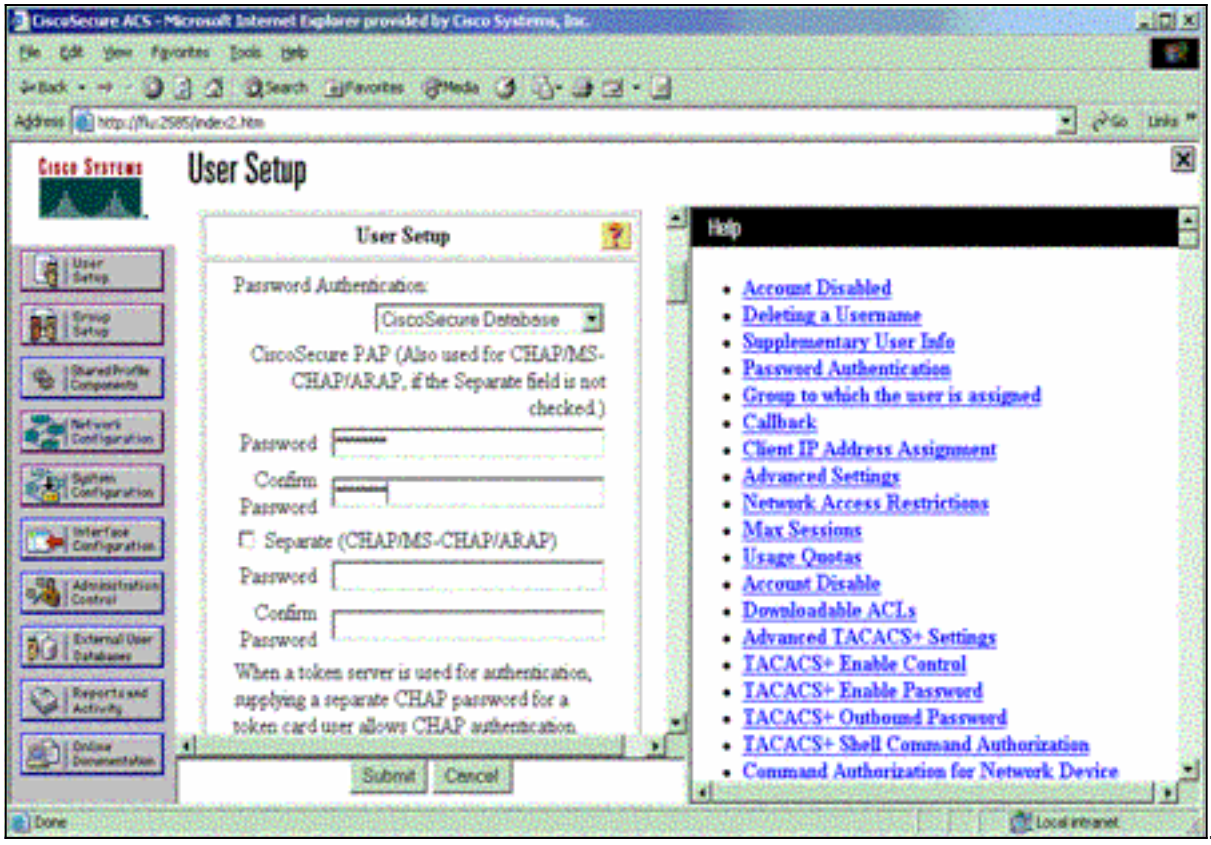


التغييرات.

5. انقر على **إعداد المستخدم**، وأدخل معرف المستخدم، وانقر فوق **إضافة/تحرير**.

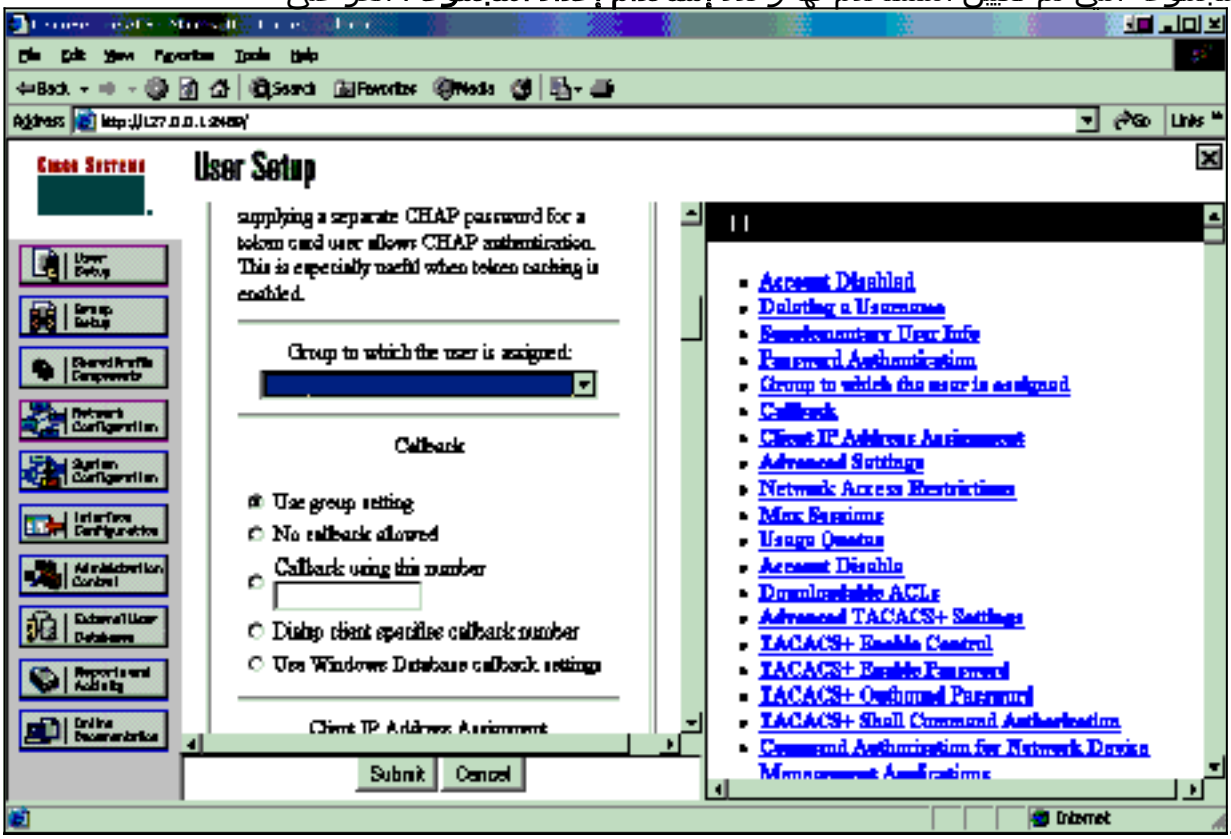


6. أختر قاعدة بيانات لمصادقة المستخدم. (في هذا المثال، يتم إستخدام "إختبار" للمستخدم، ويتم إستخدام قاعدة البيانات الداخلية ل ACS للمصادقة). أدخل كلمة مرور للمستخدم، وقم بتأكيد كلمة



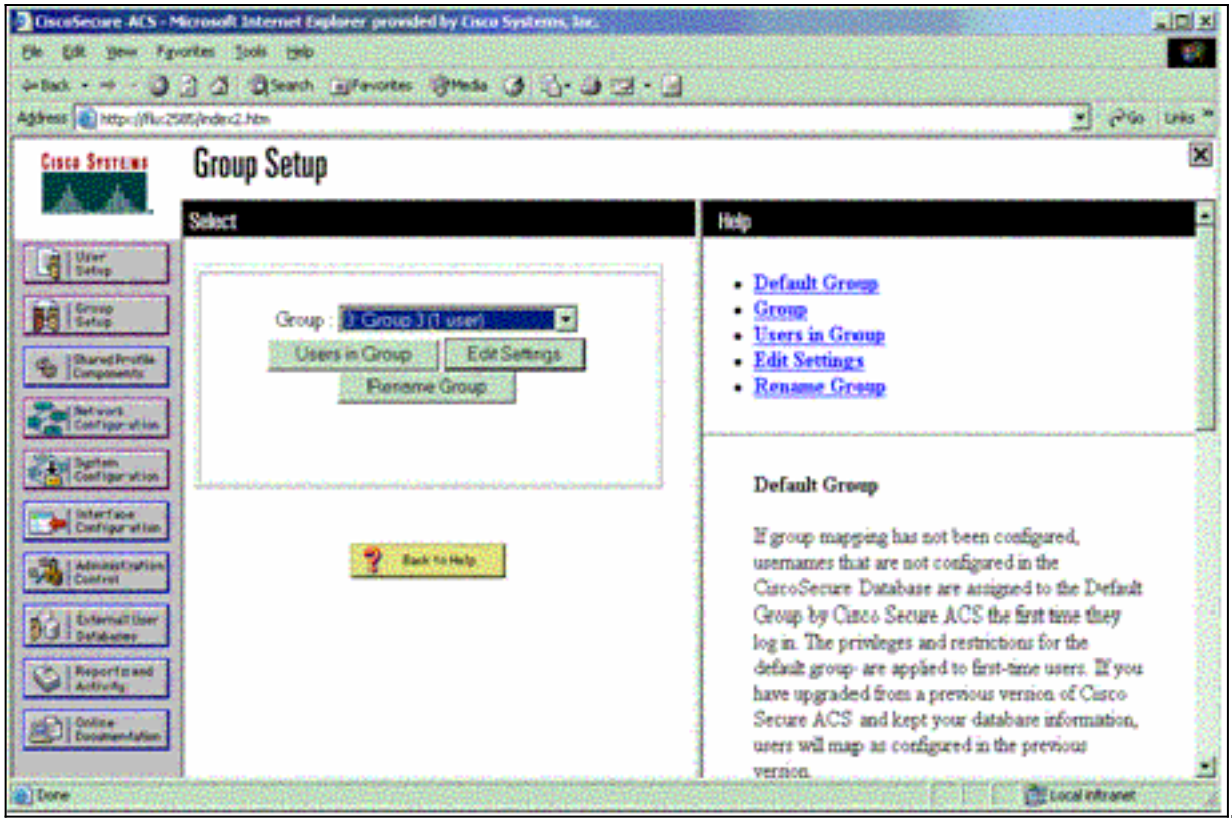
المرور.

7. أختر المجموعة التي تم تعيين المستخدم لها وحدد **إستخدام إعداد المجموعة**. انقر على



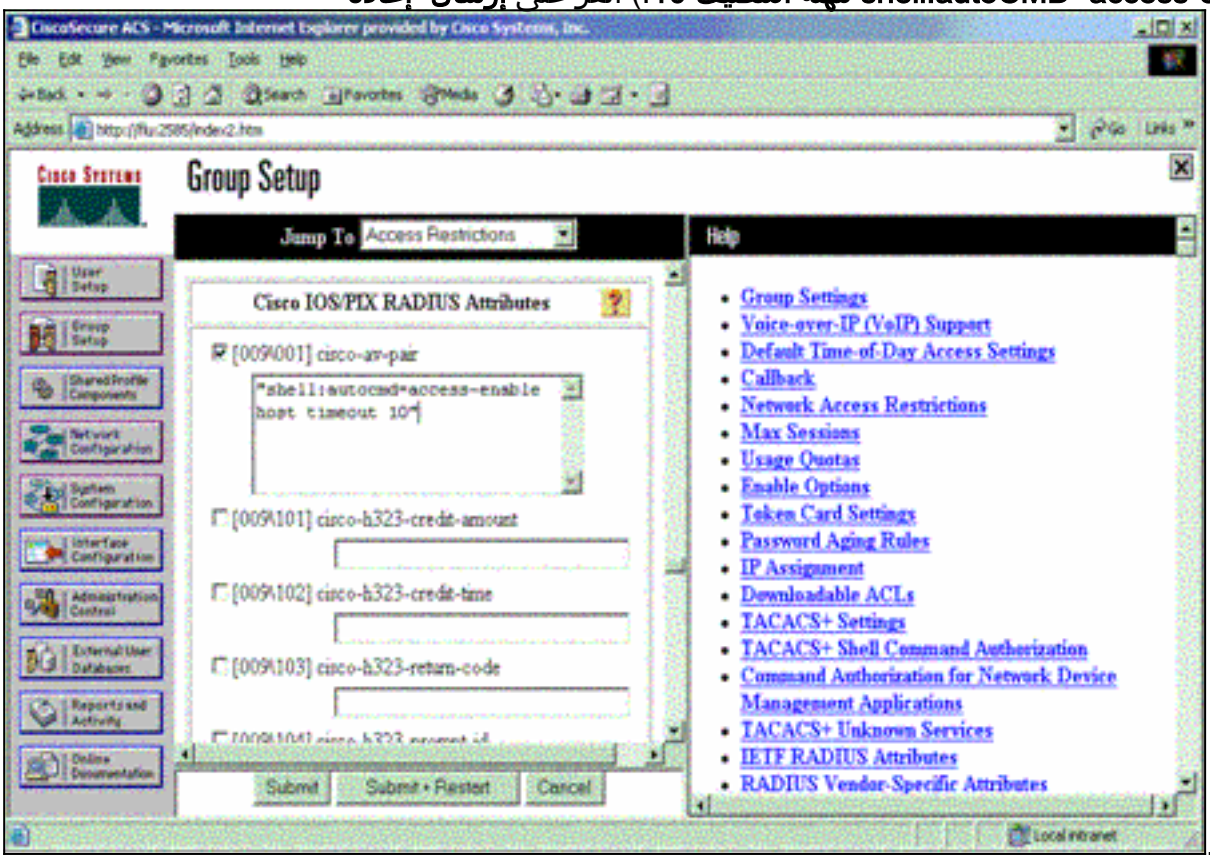
إرسال.

8. انقر فوق **إعداد المجموعة** وحدد المجموعة التي تم تعيين المستخدم لها في الخطوة السابقة. طقطقة **يحرر عملية**



إعداد.

9. قم بالتمرير إلى أسفل إلى قسم سمات Cisco IOS/PIX RADIUS. حدد المربع الخاص **بزوج-AV من Cisco**. أدخل الأمر **shell** الذي سيتم تنفيذه عند تفويض المستخدم الناجح. (يستخدم هذا المثال **shell:autoCMD=access-enable مهلة المضيف 10**.) انقر على **إرسال+إعادة**



تشغيل.

أستكشاف أخطاء RADIUS وإصلاحها

أستخدم أوامر **تصحيح الأخطاء** هذه على NAS لاستكشاف أخطاء RADIUS وإصلاحها.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- **debug radius**—يعرض المعلومات المرتبطة ب RADIUS.

أستخدم هذه الأوامر لاستكشاف أخطاء AAA وإصلاحها:

- **debug aaa authentication**— يعرض معلومات حول مصادقة AAA/TACACS+.
- **تصحيح أخطاء تفويض المصادقة والتفويض والمحاسبة (AAA)**—يعرض معلومات حول تفويض AAA/TACACS+.

يظهر إخراج نموذج **تصحيح الأخطاء** هنا عملية مصادقة وتفويض ناجحة على ACS الذي تم تكوينه ل RADIUS.

```
Router#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on

  Radius protocol debugging is on
  Radius packet protocol debugging is on
============================================================
Router#
  AAA/BIND(00000003): Bind i/f
'AAA/AUTHEN/LOGIN (00000003): Pick method list 'default
" :RADIUS/ENCODE(00000003): ask "Username
  RADIUS/ENCODE(00000003): send packet; GET_USER
" :RADIUS/ENCODE(00000003): ask "Password
  RADIUS/ENCODE(00000003): send packet; GET_PASSWORD
  RADIUS:  AAA Unsupported     [152] 5
[RADIUS:   74 74 79                    [tty
  RADIUS(00000003): Storing nasport 66 in rad_db
,RADIUS/ENCODE(00000003): dropping service type
radius-server attribute 6 on-for-login-auth" is off"
  RADIUS(00000003): Config NAS IP: 0.0.0.0
  RADIUS/ENCODE(00000003): acct_session_id: 1
  RADIUS(00000003): sending
  RADIUS/ENCODE: Best Local IP-Address 172.18.124.1
  for Radius-Server 10.48.66.53
RADIUS(00000003): Send Access-Request to 10.48.66.53:1645
  id 21645/1, len 77
- RADIUS:  authenticator 5A 95 1F EA A7 94 99 E5
  BE B5 07 BD E9 05 5B 5D
"RADIUS:  User-Name           [1]   7   "test
* RADIUS:  User-Password       [2]   18
  RADIUS:  NAS-Port            [5]   6   66
[RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5
"RADIUS:  Calling-Station-Id  [31]  14  "171.68.109.158
RADIUS:  NAS-IP-Address      [4]   6   171.68.117.189
,RADIUS: Received from id 21645/1 10.48.66.53:1645
  Access-Accept, len 93
- RADIUS:  authenticator 7C 14 7D CB 33 19 97 19
  4B C3 FC 25 21 47 CD 68
  RADIUS:  Vendor, Cisco       [26]  51
  RADIUS:   Cisco AVpair       [1]   45
"shell:autocmd=access-enable host timeout 10"
  RADIUS:  Class               [25]  22
RADIUS:   43 49 53 43 4F 41 43 53 3A 61 63 31 32 37 63 30
  [CISCOACS:ac127c0]
[RADIUS:   31 2F 36 36                 [1/66
  RADIUS(00000003): Received from id 21645/1
  AAA/AUTHOR/EXEC(00000003): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000003): Authorization successful
```

معلومات ذات صلة

- أمان قفل ومفتاح IOS من Cisco
- صفحة دعم TACACS/TACACS+
- TACACS+ في وثائق IOS
- صفحة دعم RADIUS
- طلبات التعليقات (RFCs)
- 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).