موجه IOS: مصادقة وكيل المصادقة الوارده مع VPN و IPSec لتكوين عميل ACS

المحتويات

المقدمة

تتيح ميزة وكيل المصادقة للمستخدمين إمكانية تسجيل الدخول إلى شبكة أو الوصول إلى الإنترنت عبر HTTP، مع إسترداد ملفات تعريف الوصول الخاصة بهم وتطبيقها تلقائيا من خادم TACACS+ أو RADIUS. الا تكون ملفات تعريف المستخدم نشطة إلا في حالة وجود حركة مرور نشطة من المستخدمين المصادق عليهم.

تم تصميم هذا التكوين لعرض مستعرض الويب على 10.1.1.1 واستهدافه إلى 10.17.17.17. ظر لتكوين عميل VPN للاتصال من خلال نقطة نهاية النفق 10.31.1.111 للوصول إلى شبكة 10.17.17.x، يتم إنشاء نفق IPSec ويحصل الكمبيوتر على عنوان IP من تجمع RTP-POOL (ظر أنه يتم تنفيذ تكوين الوضع). يتم بعد ذلك طلب المصادقة بواسطة مرور (مخزن على خادم Cisco 3640. بعد أن يدخل المستخدم اسم مستخدم وكلمة المستخدم، يتم إضافة قائمة الوصول التي تم تمريرها من الخادم إلى قائمة TACACS+ في 10.14.14.3)، يتم الوصول 118.

المتطلبات الأساسية

المتطلبات

قبل محاولة هذا التكوين، تأكد من استيفاء المتطلبات التالية:

- تم تكوين عميل Cisco VPN لإنشاء نفق IPSec باستخدام موجه Cisco 3640.
- تم تكوين خادم TACACS+ لوكيل المصادقة. راجع قسم "المعلومات ذات الصلة" للحصول على مزيد من المعلومات.

المكونات المستخدمة

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

- نظام Cisco IOS؟ البرنامج الإصدار 12.4
- موجّه Cisco 3640
- عميل شبكة VPN من Cisco لنظام التشغيل Windows الإصدار 4.8 (يجب أن يعمل أي عميل لشبكة VPN الإصدار 4.x والإصدارات الأحدث)

ملاحظة: تم إدخال الأمر **ip auth-proxy** في البرنامج Cisco IOS Software، الإصدار 12.0.5.T. تم إختبار هذا التكوين باستخدام برنامج Cisco IOS، الإصدار 12.4.

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

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

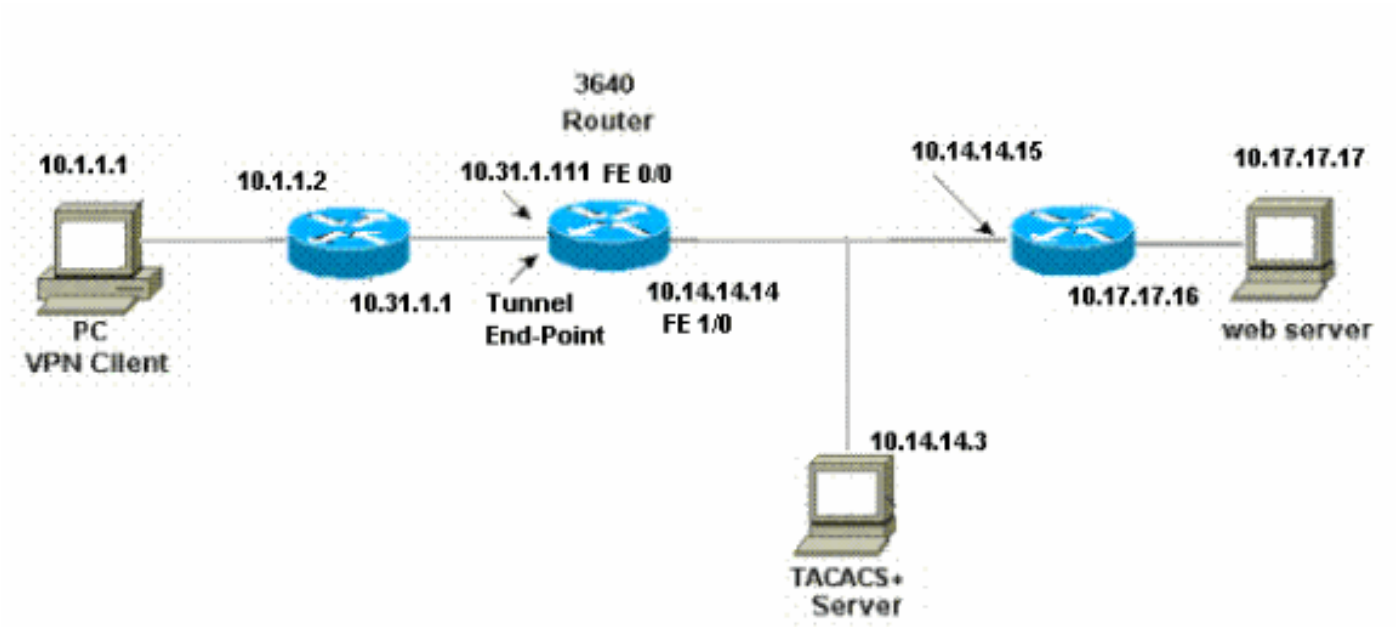
التكوين

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

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوين

المجوم 3640

```
Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3640
!
!--- The username and password is used during local
authentication. username rtpuser password 0 rtpuserpass

!--- Enable AAA. aaa new-model

!--- Define server-group and servers for TACACS+. aaa
group server tacacs+ RTP
 server 10.14.14.3
!

!--- In order to set authentication, authorization, and
accounting (AAA) authentication at login, use the aaa
authentication login command in global configuration
mode

aaa authentication login default group RTP local
aaa authentication login userauth local
aaa authorization exec default group RTP none
aaa authorization network groupauth local
aaa authorization auth-proxy default group RTP
enable secret 5 $1$CQHC$R/07uQ44E2JgVuCsOUWdG1
enable password ww
!
ip subnet-zero
!
!--- Define auth-proxy banner, timeout, and rules. ip
auth-proxy auth-proxy-banner http ^C
Please Enter Your Username and Password:
^C
ip auth-proxy auth-cache-time 10
ip auth-proxy name list_a http
ip audit notify log
ip audit po max-events 100
cns event-service server
!
!--- Define ISAKMP policy. crypto isakmp policy 10
 hash md5
 authentication pre-share
 group 2

!--- These commands define the group policy that !--- is
enforced for the users in the group RTPUSERS. !--- This
group name and the key should match what !--- is
configured on the VPN Client. The users from this !---
group are assigned IP addresses from the pool RTP-POOL.
crypto isakmp client configuration group RTPUSERS
 key cisco123
 pool RTP-POOL
!
!--- Define IPSec transform set and apply it to the
dynamic crypto map. crypto ipsec transform-set RTP-
TRANSFORM esp-des esp-md5-hmac
```

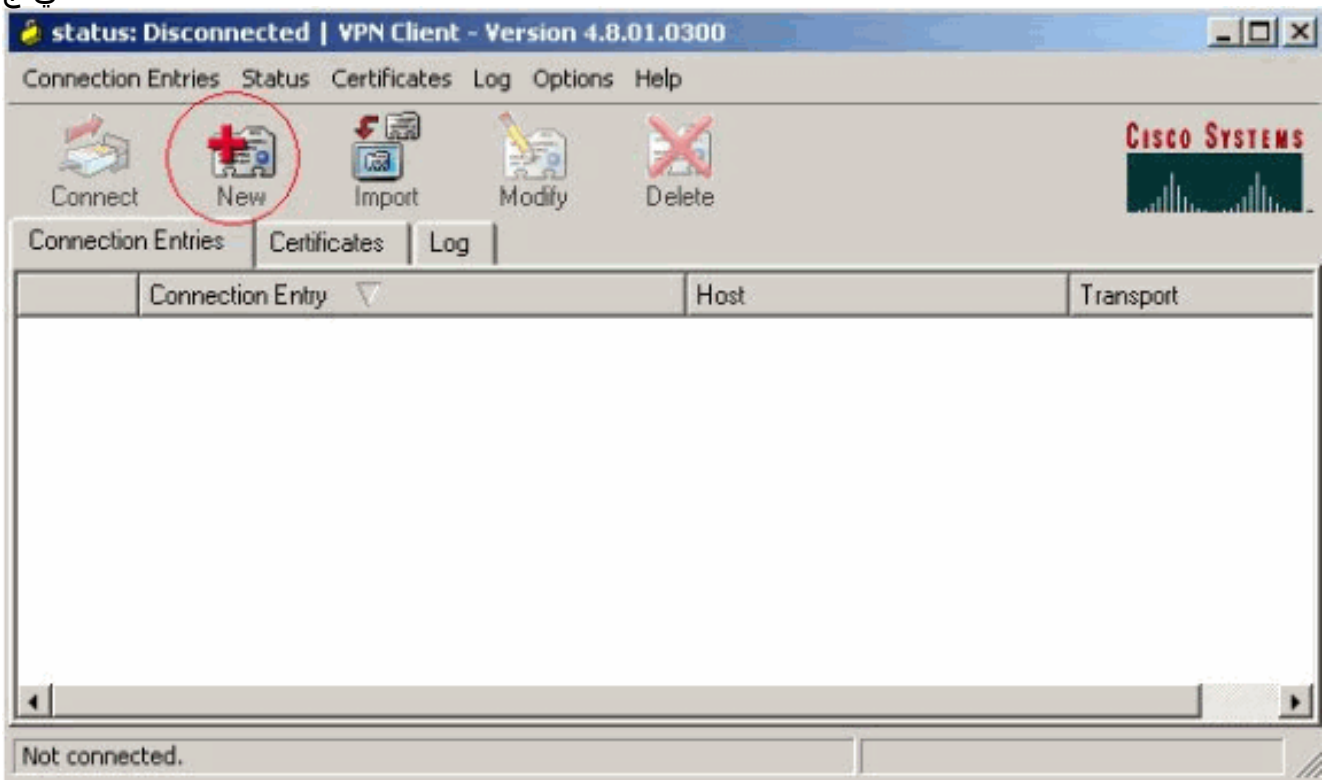
```
!
crypto dynamic-map RTP-DYNAMIC 10
 set transform-set RTP-TRANSFORM
!
!--- Define extended authentication (X-Auth) using the
local database. !--- This is to authenticate the users
before they can !--- use the IPSec tunnel to access the
resources. crypto map RTPCLIENT client authentication
list userauth

!--- Define authorization using the local database. !---
This is required to push the 'mode configurations' to
the VPN Client. crypto map RTPCLIENT isakmp
authorization list groupauth
crypto map RTPCLIENT client configuration address
initiate
crypto map RTPCLIENT client configuration address
respond
crypto map RTPCLIENT 10 ipsec-isakmp dynamic RTP-DYNAMIC
!
interface FastEthernet0/0
 ip address 10.31.1.111 255.255.255.0
 ip access-group 118 in
 no ip directed-broadcast

!--- Apply the authentication-proxy rule to the
interface. ip auth-proxy list_a
 no ip route-cache
 no ip mroute-cache
 speed auto
 half-duplex

!--- Apply the crypto-map to the interface. crypto map
RTPCLIENT
!
interface FastEthernet1/0
 ip address 10.14.14.14 255.255.255.0
 no ip directed-broadcast
 speed auto
 half-duplex
!
!--- Define the range of addresses in the pool. !--- VPN
Clients will have thier 'internal addresses' assigned !-
-- from this pool. ip local pool RTP-POOL 10.20.20.25
10.20.20.50
ip classless
ip route 0.0.0.0 0.0.0.0 10.14.14.15
ip route 10.1.1.0 255.255.255.0 10.31.1.1

!--- Turn on the HTTP server and authentication. !---
This is required for http auth-proxy to work. ip http
server
ip http authentication aaa
!
!--- The access-list 118 permits ISAKMP and IPSec
packets !--- to enable the Cisco VPN Client to establish
the IPSec tunnel. !--- The last line of the access-list
118 permits communication !--- between the TACACS+
server and the 3640 router to enable !--- authentication
and authorization. All other traffic is denied. access-
list 118 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111
access-list 118 permit udp 10.1.1.0 0.0.0.255 host
10.31.1.111 eq isakmp
access-list 118 permit tcp host 10.14.14.3 host
```

```
10.31.1.111
!
!--- Define the IP address and the key for the TACACS+
server. tacacs-server host 10.14.14.3 key cisco
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password ww
!
end
```

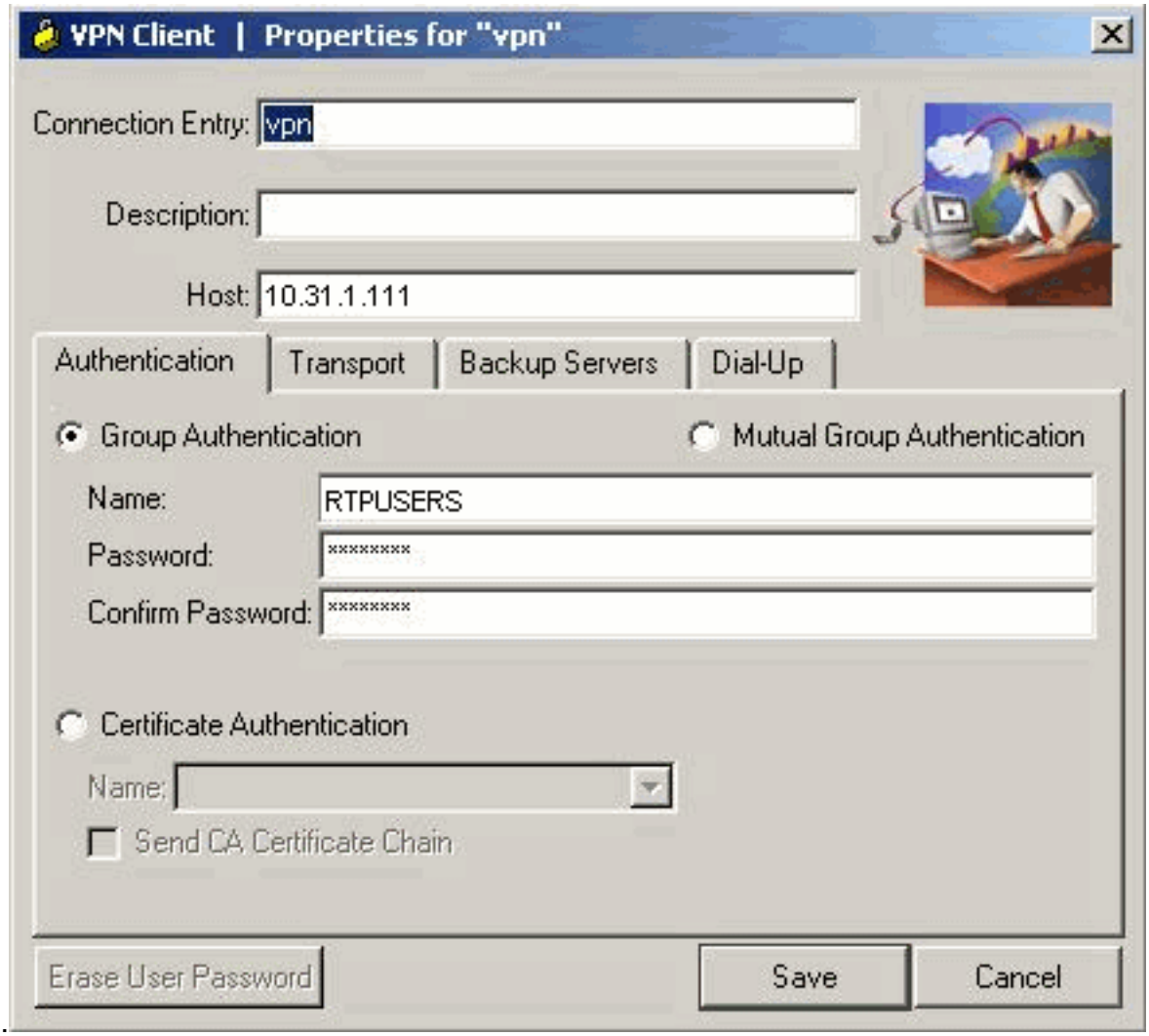
تكوين VPN Client 4.8

أتمت هذا steps in order to شكلت الـ VPN زبون 4.8:

1. أخترت **بداية>برنامج>Cisco Systems VPN زبون>VPN زبون**.
2. انقر على **جديد** لتشغيل الإطار "إنشاء اتصال VPN جديد".

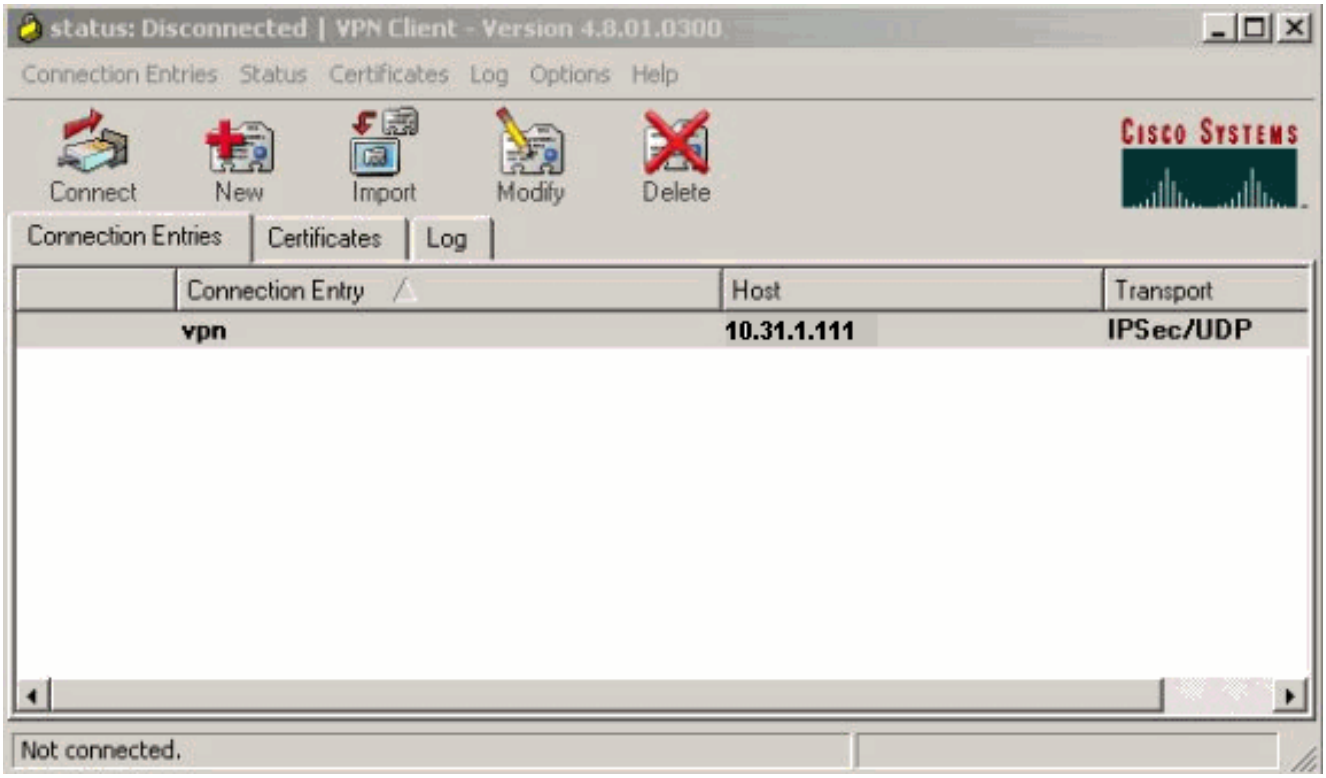


3. أدخل اسم "إدخال الاتصال" مع وصف. أدخل عنوان IP الخارجي للموجه في المربع المضيف. ثم أدخل اسم مجموعة VPN وكلمة المرور، وانقر على



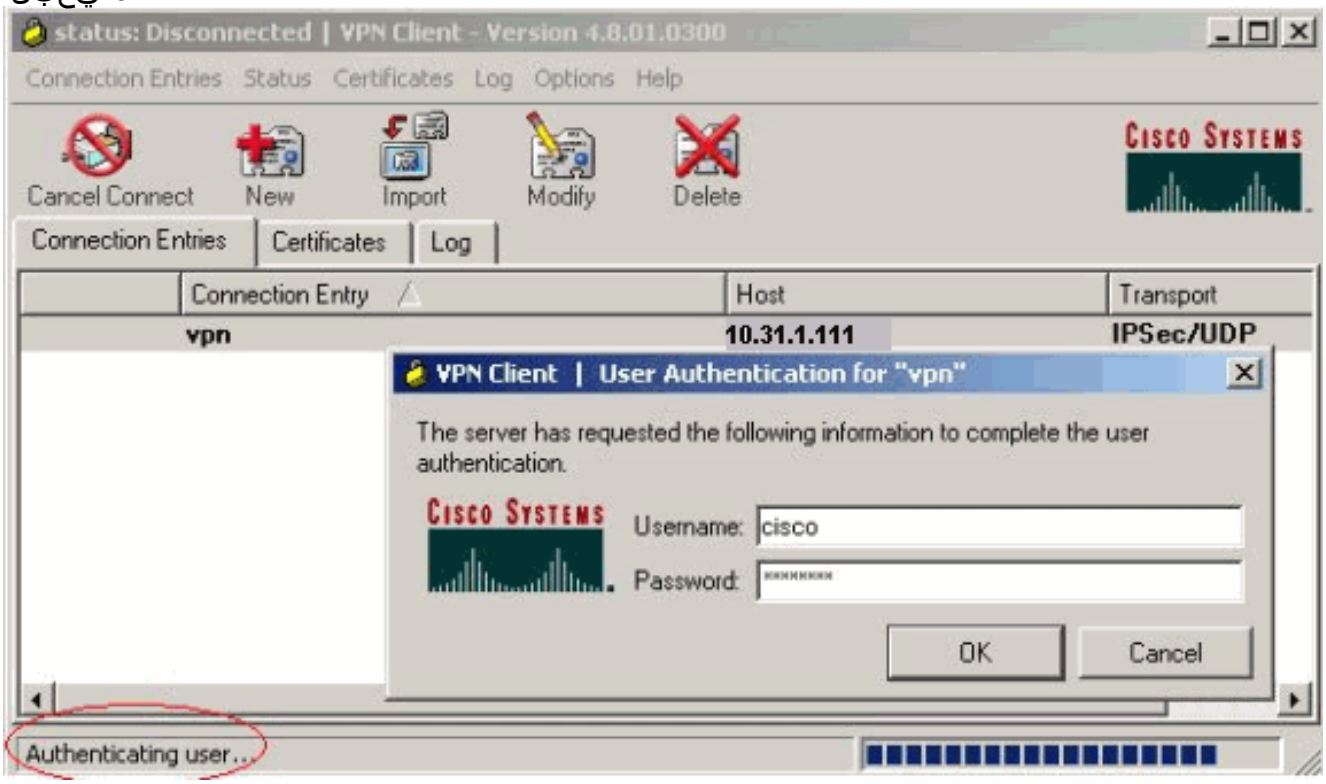
حفظ.

4. انقر على الاتصال الذي تريد إستخدامه وانقر فوق **الاتصال** من الإطار الرئيسي لعميل شبكة VPN.

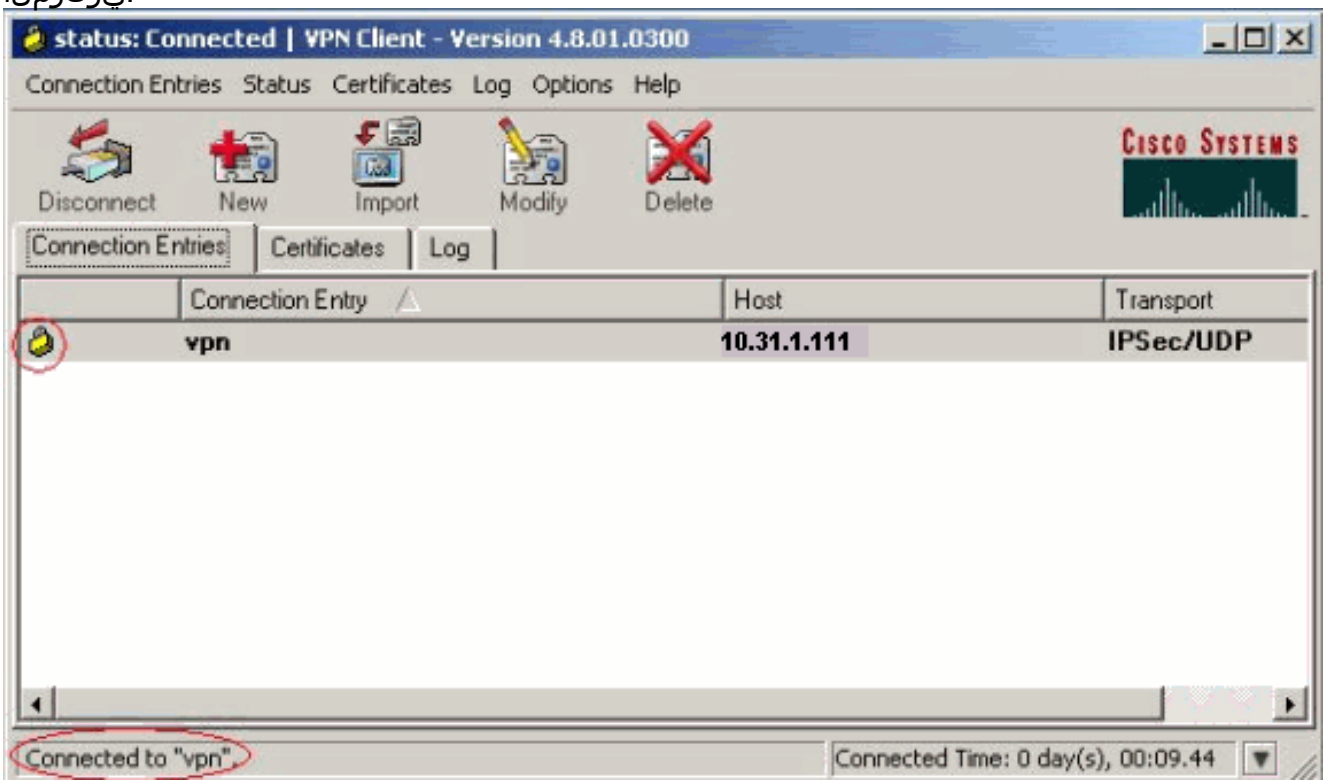


5. عند المطالبة، أدخل معلومات اسم المستخدم وكلمة المرور للإرسال وانقر فوق **موافق** للاتصال بالشبكة

البعيدة.



يتم اتصال عميل شبكة VPN بالموجه في الموقع المركزي.



تكوين خادم TACACS+ باستخدام ACS الآمن من Cisco

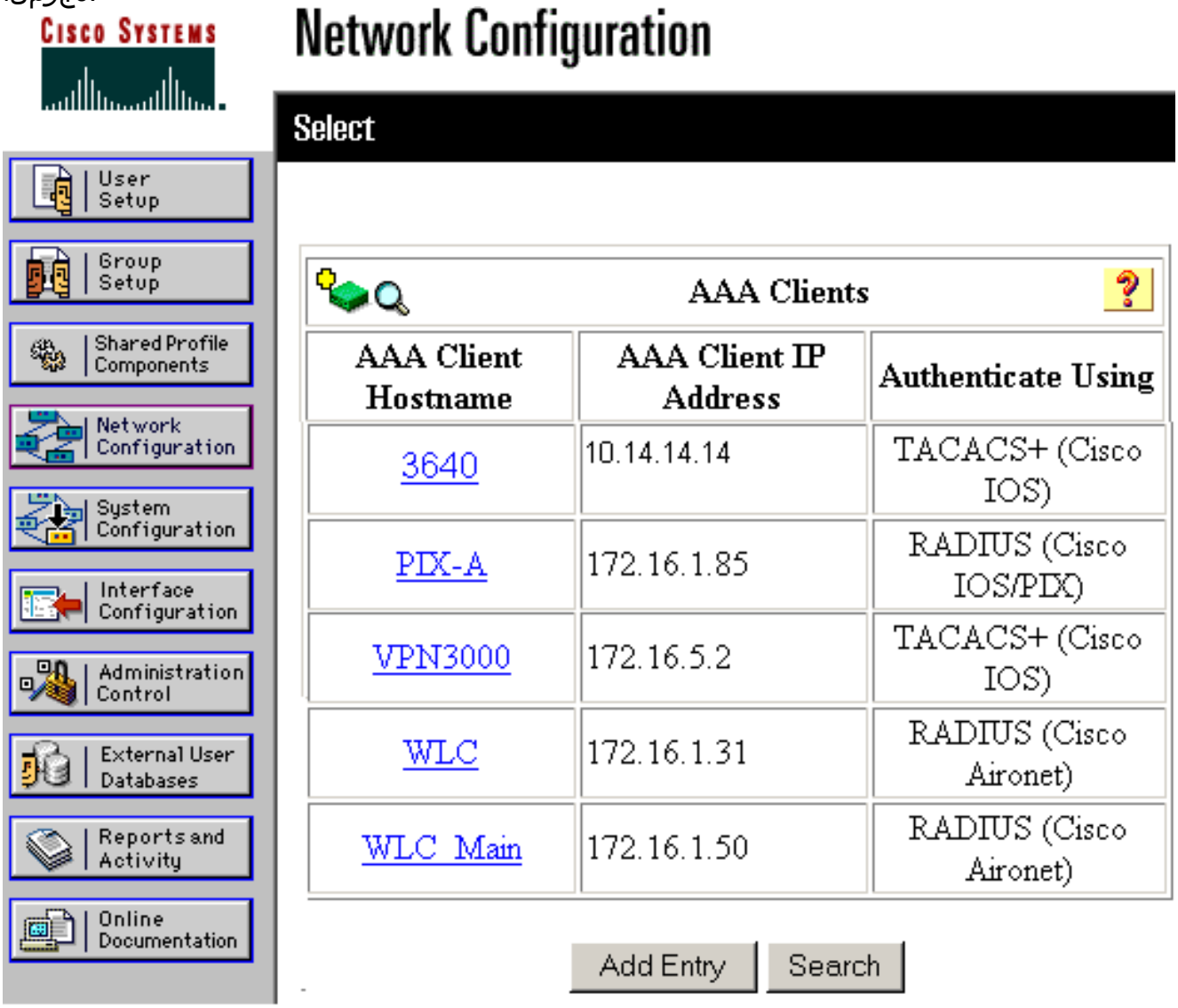
أتمت هذا steps in order to شكلت TACACS+ في cisco يأمن ACS:

1. يجب تكوين الموجه لتحديد موقع مصدر المحتوى الإضافي الآمن من Cisco للتحقق من بيانات اعتماد المستخدم.على سبيل المثال:

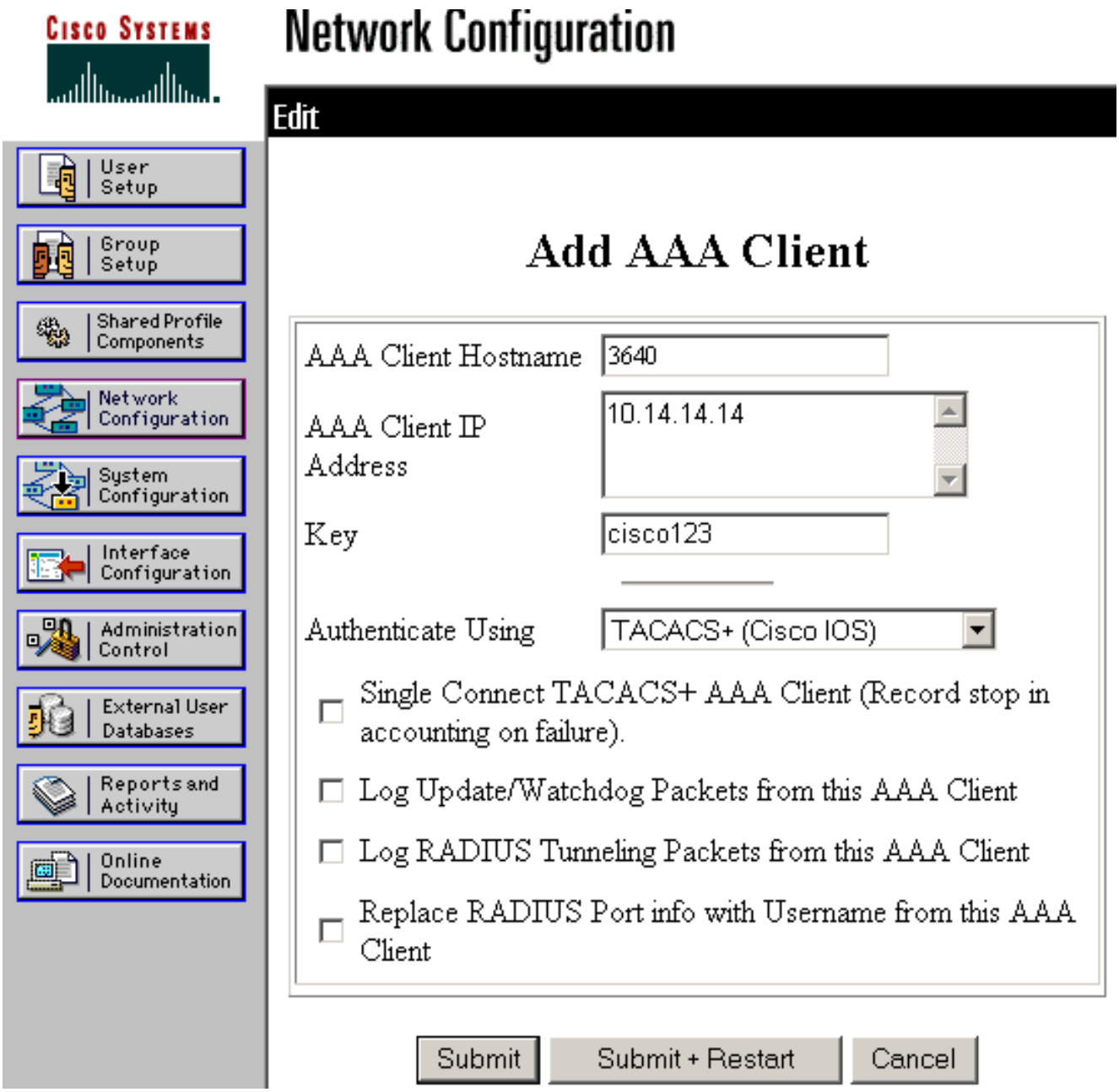
```
3640(config)#
aaa group server tacacs+ RTP
```

```
3640(config)#
tacacs-server host 10.14.14.3 key cisco
```

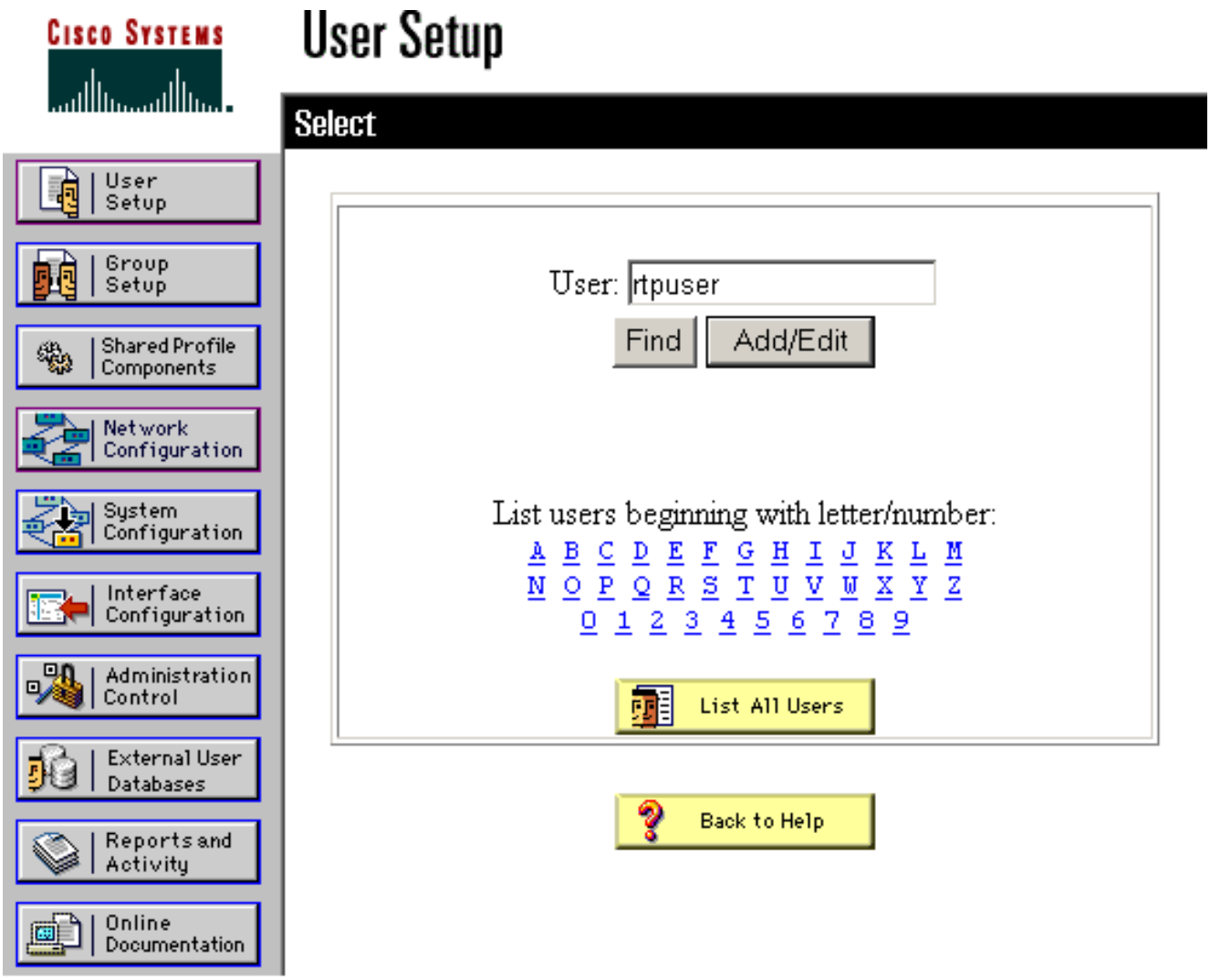
2. أخترت **شبكة تشكيل** على اليسار وطقطقة **يضيف مدخل** أن يضيف مدخل للمسحاج تخديد في إما ال TACACS+ دان ل قاعدة معطيات. أخترقاعدة بيانات الخادم وقفا لتكوين الموجه.



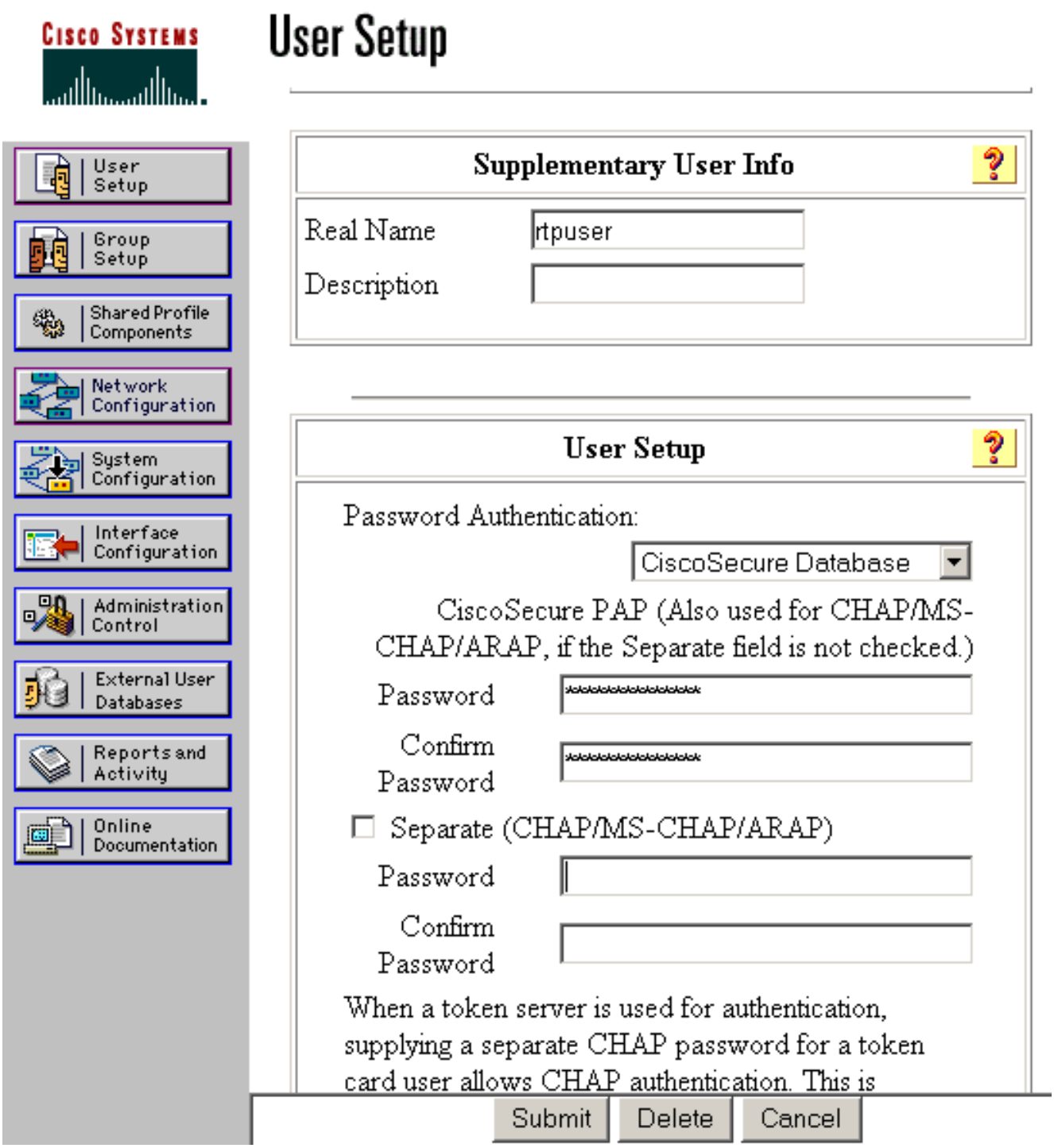
3. يتم إستخدام المفتاح للمصادقة بين الموجه 3640 وخادم ACS الآمن من Cisco. إذا كنت ترغب في تحديد بروتوكول TACACS+ للمصادقة، فأختر **TACACS+ (Cisco IOS)** في قائمة المصادقة باستخدام القائمة
المنسدلة.



4. دخلت ال username في المستعمل مجال في ال cisco يأمن قاعدة معطيات، بعد ذلك طقطقة **يضيف/يحرر**.في هذا المثال، اسم المستخدم هو rtpuser.



5. في الإطار التالي، أدخل كلمة مرور المستخدم.في هذا مثال، الكلمة rtpUserPass. يمكنك تعيين حساب المستخدم إلى مجموعة إذا أردت. عند الانتهاء، انقر فوق إرسال.



تكوين ميزة النسخ الاحتياطية

عندما يصبح خادم RADIUS الأساسي غير متاح، سيتم تجاوز فشل الموجه إلى خادم RADIUS النشط التالي للنسخ الاحتياطي. سيستمر الموجه في إستخدام خادم RADIUS الثانوي إلى الأبد حتى إذا كان الخادم الأساسي متوفرا. عادة ما يكون الخادم الرئيسي هو الخادم عالي الأداء والخادم المفضل. إذا لم يكن الخادم الثانوي متاحا، يمكن إستخدام قاعدة البيانات المحلية للمصادقة باستخدام الأمر AAA authentication login default group rtp local .

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

قم بإنشاء نفق IPSec بين جهاز الكمبيوتر الشخصي وموجه 3640 من Cisco.

افتح مستعرض على الكمبيوتر أو رشإليه على http://10.17.17.17. يعترض موجه Cisco 3640 حركة مرور HTTP هذه، ويثير وكيل المصادقة، ويطلب من مستخدم وكلمة مرور. يرسل Cisco 3640 اسم المستخدم/كلمة المرور إلى خادم TACACS+ للمصادقة. في حالة نجاح المصادقة، يجب أن تكون قادرا على رؤية صفحات الويب على خادم الويب على 10.17.17.17.

يتم دعم بعض أوامر **العرض أو امسح** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- show ip access lists — يعرض قوائم التحكم في الوصول (ACL) القياسية والموسعة التي تم تكوينها على موجه جدار الحماية (يتضمن إدخالات قوائم التحكم في الوصول التي تمت إضافة إدخالات قائمة التحكم في الوصول (ACL) الديناميكية (ACL) الديناميكية). تم إزالتها بشكل دوري استنادا إلى ما إذا كان المستخدم يصدق أو لا. هذا الإخراج يعرض قائمة الوصول 118 قبل تشغيل وكيل المصادقة:
```
3640#show ip access-lists 118
   Extended IP access list 118
   10 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111 (321 matches)
   20 permit udp 10.1.1.0 0.0.0.255 host 10.31.1.111 eq isakmp (276 matches)
   30 permit tcp host 10.14.14.3 host 10.31.1.111 (174 matches)
```
  يعرض هذا الإخراج قائمة الوصول 118 بعد تشغيل وكيل المصادقة بنجاح من قبل المستخدم:
```
3640#show ip access-lists 118
   Extended IP access list 118
   permit tcp host 10.20.20.26 any (7 matches)
   permit udp host 10.20.20.26 any (14 matches)
   permit icmp host 10.20.20.26 any
   10 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111 (379 matches)
   20 permit udp 10.1.1.0 0.0.0.255 host 10.31.1.111 eq isakmp (316 matches)
   30 permit tcp host 10.14.14.3 host 10.31.1.111 (234 matches)
```
  تتمثل الأسطر الثلاثة الأولى من قائمة الوصول في الإدخالات المحددة لهذا المستخدم والتي تم تنزيلها من خادم TACACS+.
- show ip auth-proxy cache — يعرض إما إدخالات وكيل المصادقة أو تكوين وكيل المصادقة الجاري تشغيله. الكلمة الأساسية ذاكرة التخزين المؤقت لسرد عنوان IP للمضيف، ومصادقة وكيل المصادقة، وحالة الاتصالات التي تستخدم رقم منفذ المصدر، وكلمة المرور. إذا كانت حالة وكيل المصادقة ESTAB، تكون مصادقة المستخدم ناجحة.
```
3640#show ip auth-proxy cache
   Authentication Proxy Cache
   Client IP 10.20.20.26 Port 1705, timeout 5, state ESTAB
```

استكشاف الأخطاء وإصلاحها

ارجع إلى وكيل مصادقة استكشاف الأخطاء وإصلاحها الأوامر التحقق والتصحيح، بالإضافة إلى معلومات استكشاف الأخطاء وإصلاحها الأخرى.

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، ارجع إلى المعلومات المهمة في أوامر تصحيح الأخطاء.

معلومات ذات صلة

- تكوين وكيل المصادقة
- تكوينات وكيل المصادقة في Cisco IOS
- تفويض وكيل المصادقة في مخادم TACACS+ و RADIUS
- صفحة دعم عميل شبكة VPN من Cisco
- صفحة دعم جدار حماية IOS

- صفحة دعم IPSec
- صفحة دعم RADIUS
- طلبات التعليقات (RFCs)
- صفحة دعم TACACS/TACACS+
- TACACS+ في وثائق IOS
- الدعم الفني - 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).