تكوين VPN 3000 Concentrator PPTP باستخدام Cisco Secure ACS لمصادقة Windows RADIUS

المحتويات

المقدمة

يدعم مركز Cisco VPN 3000 أسلوب الاتصال النفقي لبروتوكول نفق من نقطة إلى نقطة (PPTP) لعملاء Windows الأصليين. يدعم مركز التركيز تشفير 40-بت و 128-بت من أجل توصيل آمن يمكن الاعتماد عليه. يصف هذا المستند كيفية تكوين PPTP على مركز VPN 3000 مع Cisco ACS الآمن لـ Windows لمصادقة RADIUS.

ارجع إلى تكوين جدار حماية Cisco Secure PIX لاستخدام PPTP لتكوين إتصالات PPTP إلى PIX.

ارجع إلى تكوين ACS الآمن من Cisco لمصادقة PPTP لموجه Windows لإعداد اتصال جهاز كمبيوتر بالموجه؛ وهذا يوفر مصادقة المستخدم لنظام التحكم في الوصول الآمن (ACS 3.2) من Cisco لخادم Windows قبل السماح للمستخدم بالدخول إلى الشبكة.

قبل البدء

الاصطلاحات

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

المتطلبات الأساسية

يفترض هذا المستند أن مصادقة PPTP المحلية تعمل قبل إضافة Cisco ACS الآمن لمصادقة Windows RADIUS. يرجى الاطلاع على كيفية تكوين VPN 3000 Concentrator PPTP باستخدام المصادقة المحلية للحصول على مزيد من المعلومات حول مصادقة PPTP المحلية. للحصول على قائمة كاملة من المتطلبات والقيود، يرجى الرجوع إلى متى يتم دعم تشفير PPTP على مركز Cisco VPN 3000؟

المكونات المستخدمة

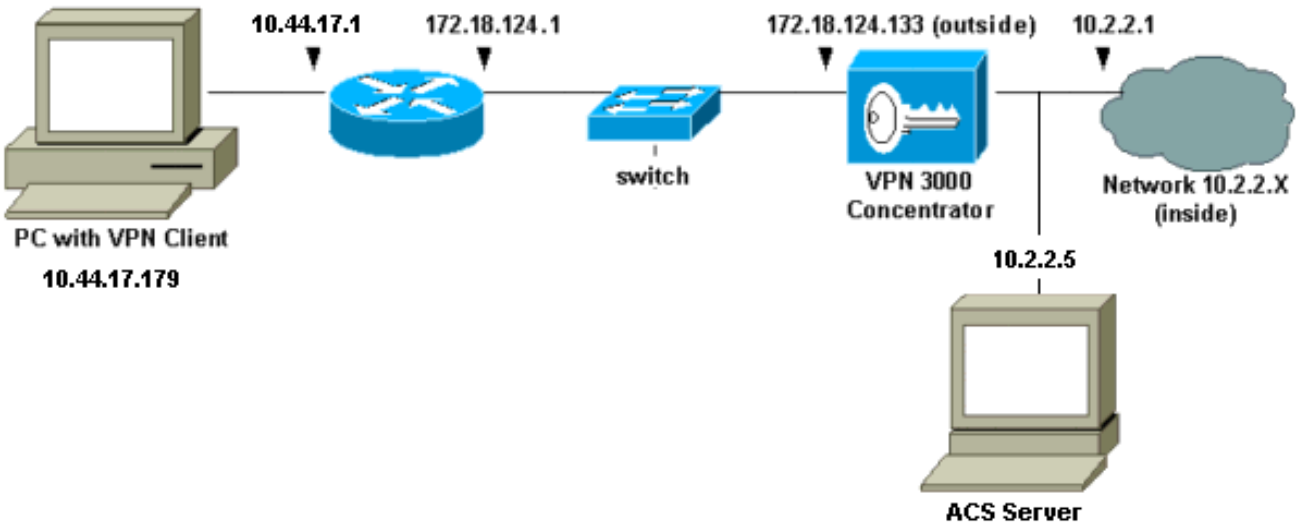
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية أدناه.

- مصدر المحتوى الإضافي الآمن من Cisco لنظام التشغيل Windows الإصدار 2.5 والإصدارات الأحدث
- VPN 3000 Concentrator صيغة c.2.5.2 وفيما بعد (تم التحقق من هذا التكوين باستخدام الإصدار x.4.0.)

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.

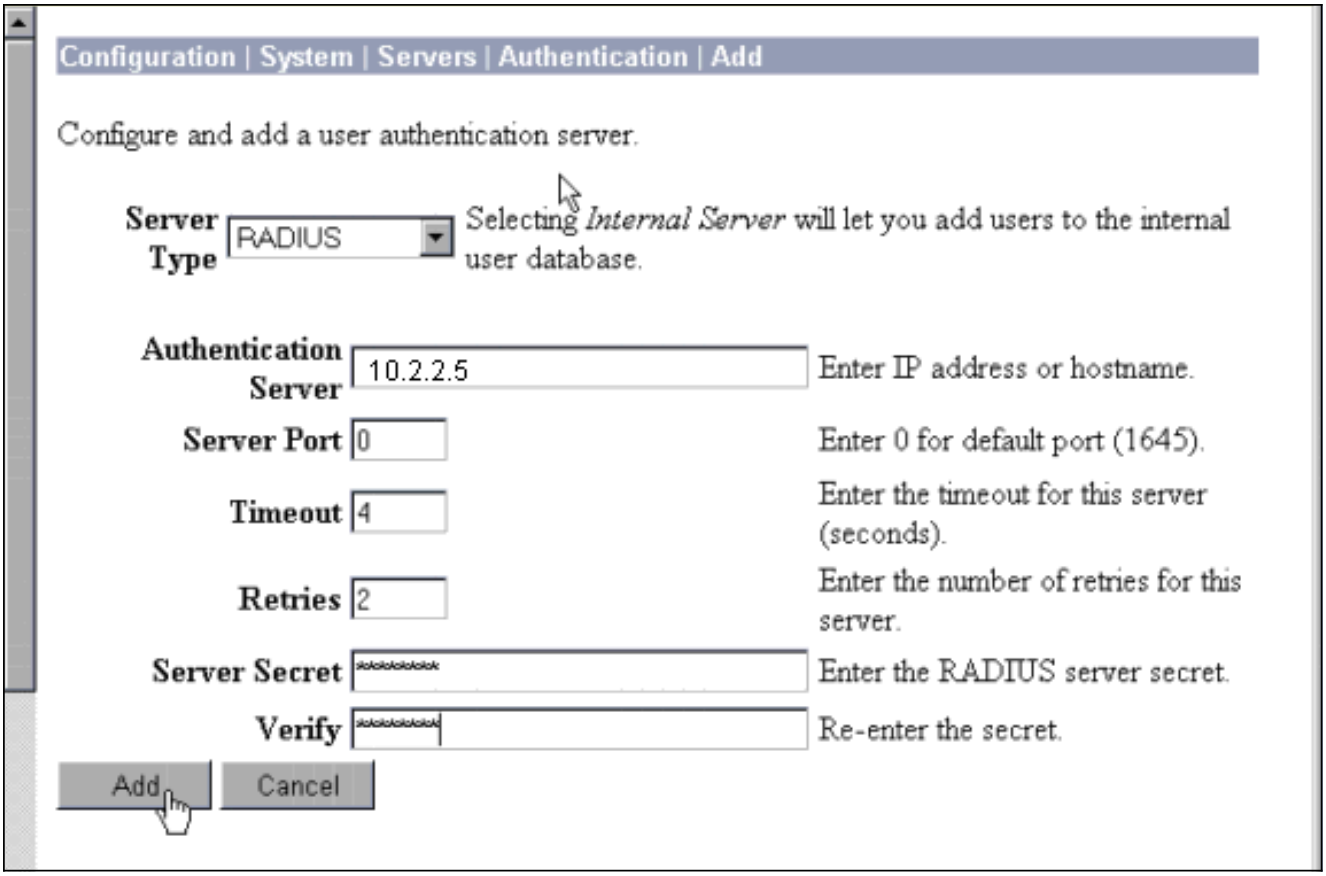


تكوين مركز VPN 3000

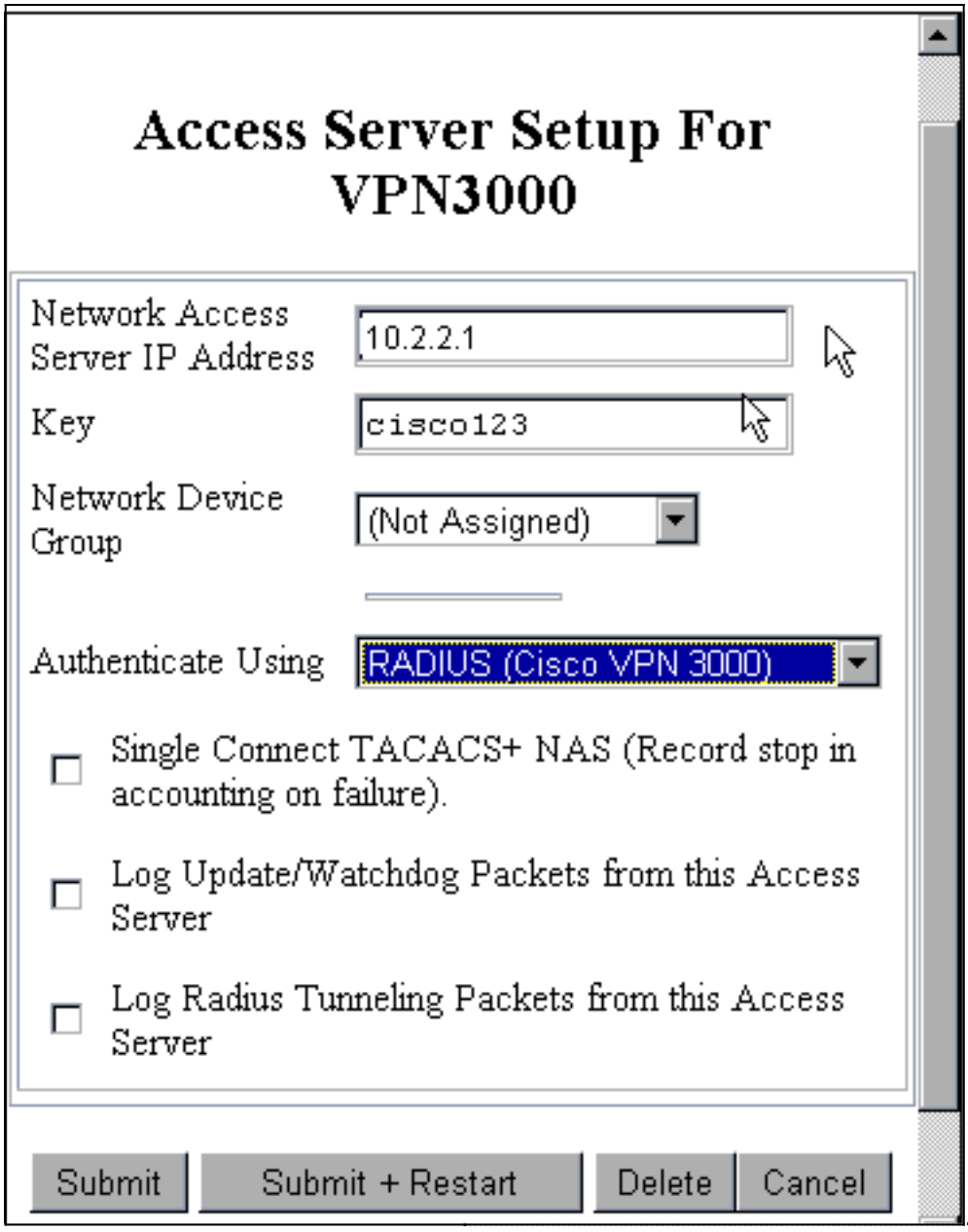
إضافة مصدر المحتوى الإضافي الآمن من Cisco وتكوينه لـ Windows

اتبع هذه الخطوات لتكوين مركز VPN لاستخدام ACS الآمن من Cisco لـ Windows.

1. على مركز VPN 3000، انتقل إلى **التكوين > النظام > الخوادم > خوادم المصادقة** وأضف مصدر المحتوى الإضافي الآمن من Cisco لخادم ومفتاح Cisco123") Windows" في هذا المثال).

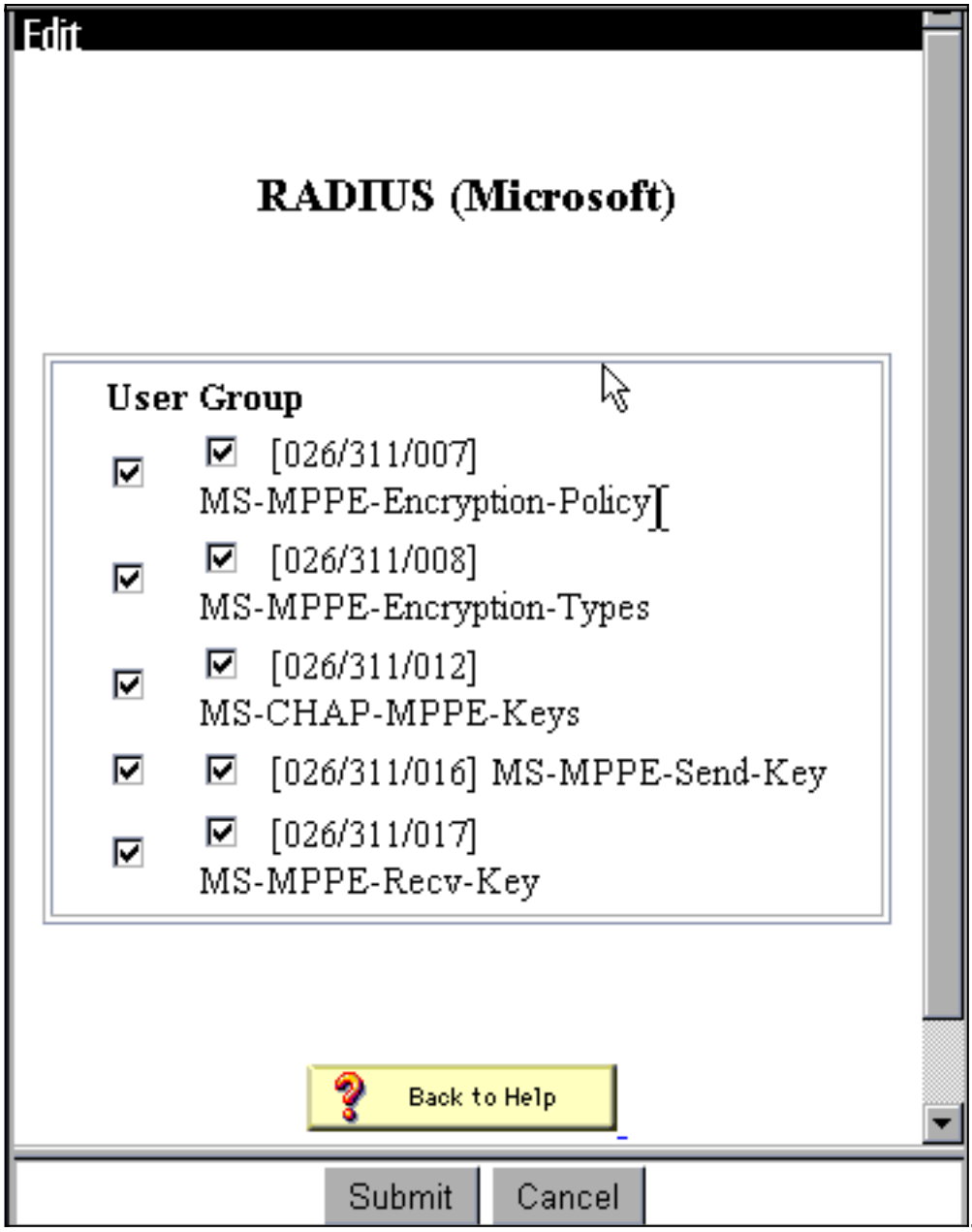


2. في Cisco Secure ACS ل Windows، أضف مركز VPN إلى تكوين شبكة خادم ACS، وحدد نوع



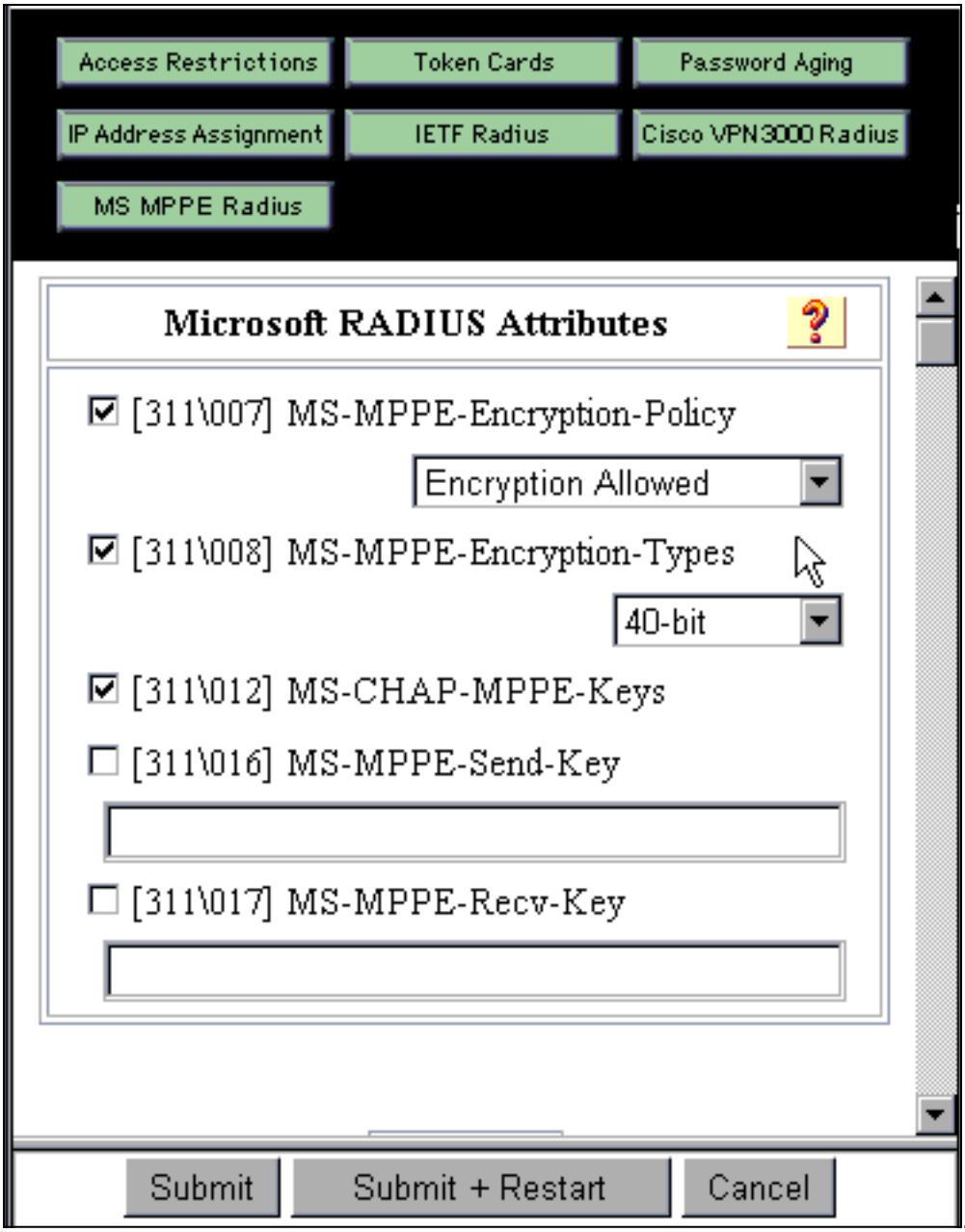
القاموس.

3. في ACS الآمن من Cisco لنظام التشغيل Windows، انتقل إلى **تكوين الواجهة > RADIUS (Microsoft)** وحدد سمات تشفير Microsoft من نقطة إلى نقطة (MPPE) حتى تظهر السمات في واجهة



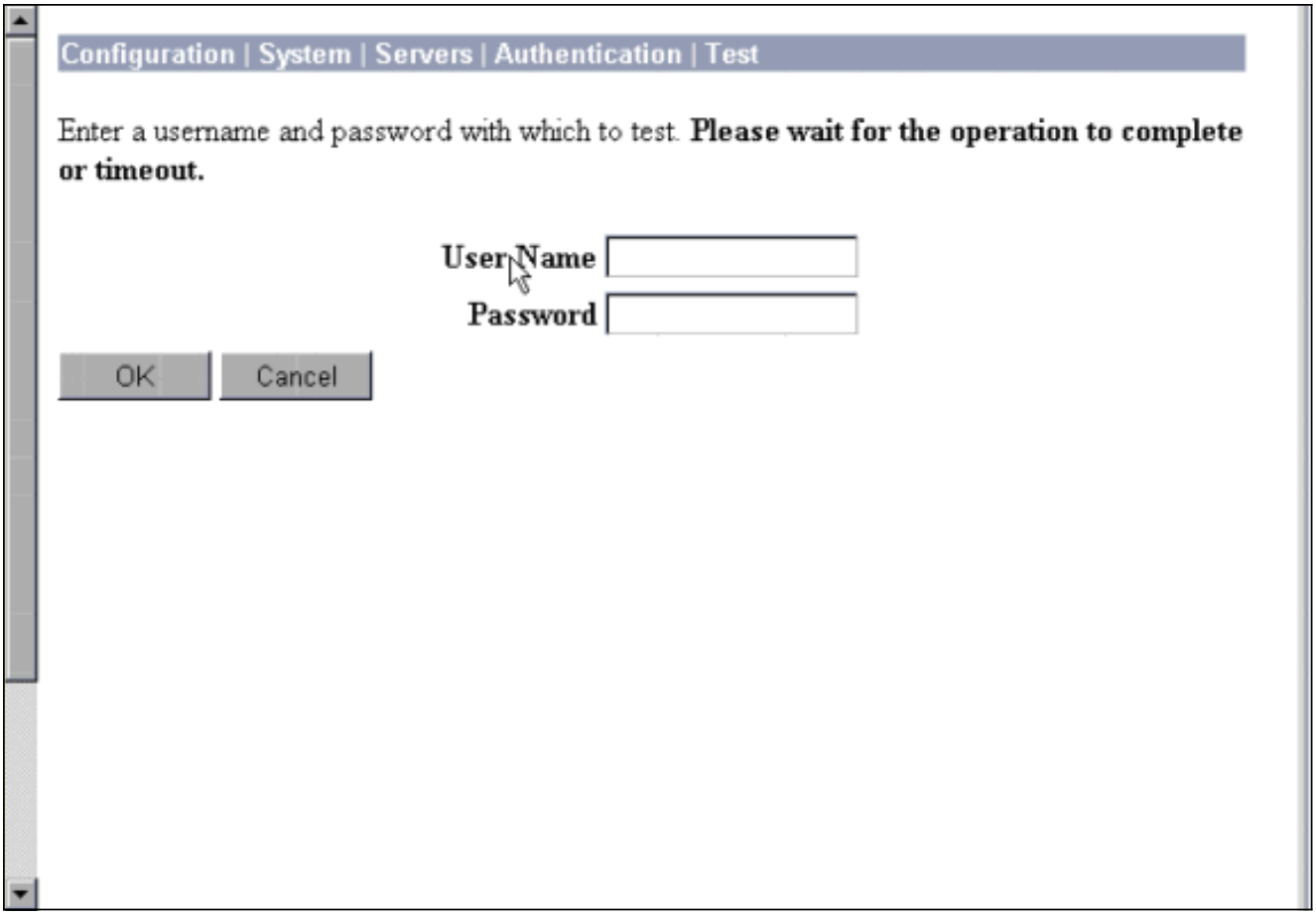
المجموعة.

4. في Cisco Secure ACS ل Windows، أضف مستخدما. في مجموعة المستخدمين، قم بإضافة سمات MPPE (Microsoft RADIUS)، في حالة إحتياجك للتشفير في وقت

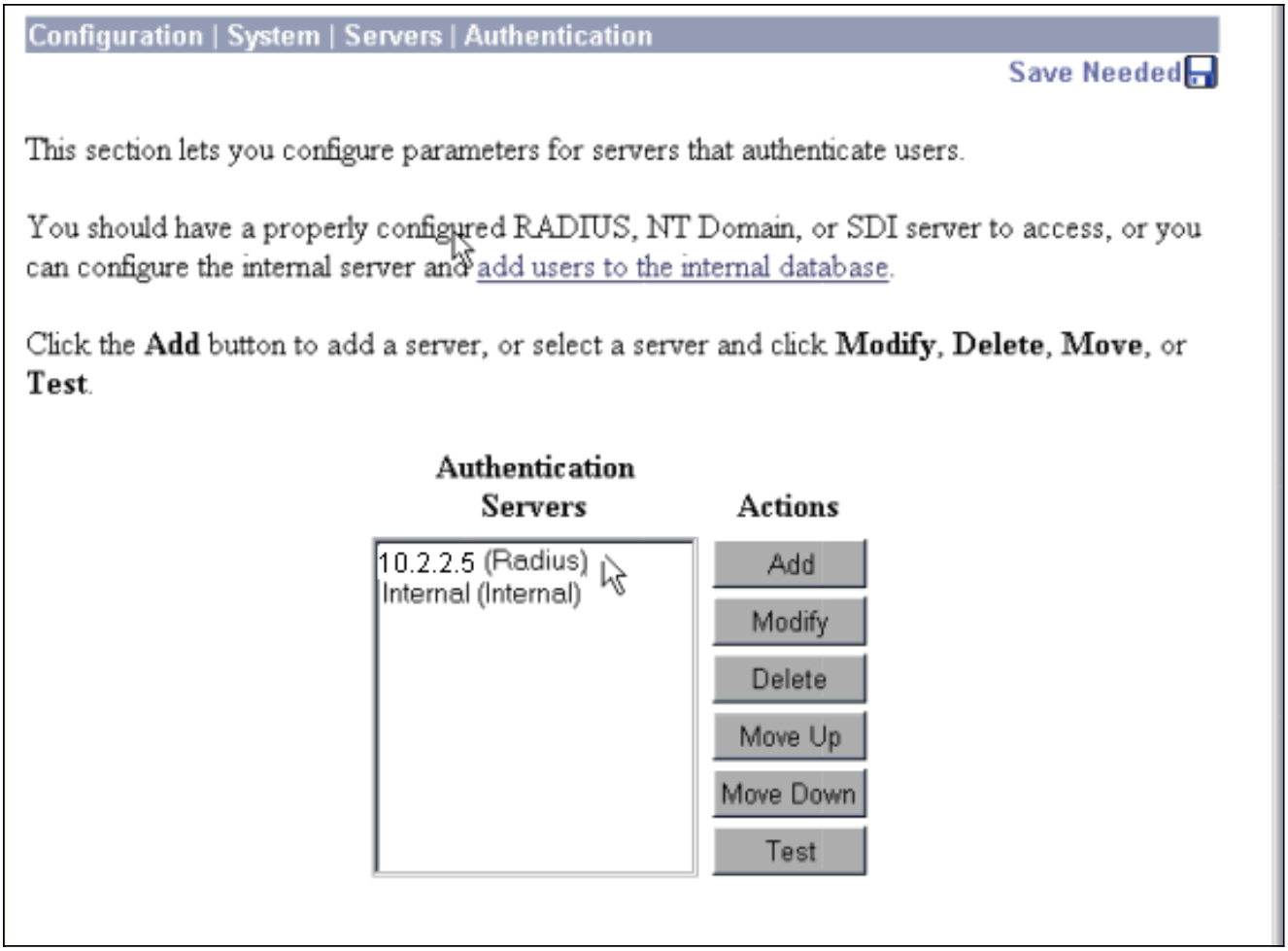


لاحق.

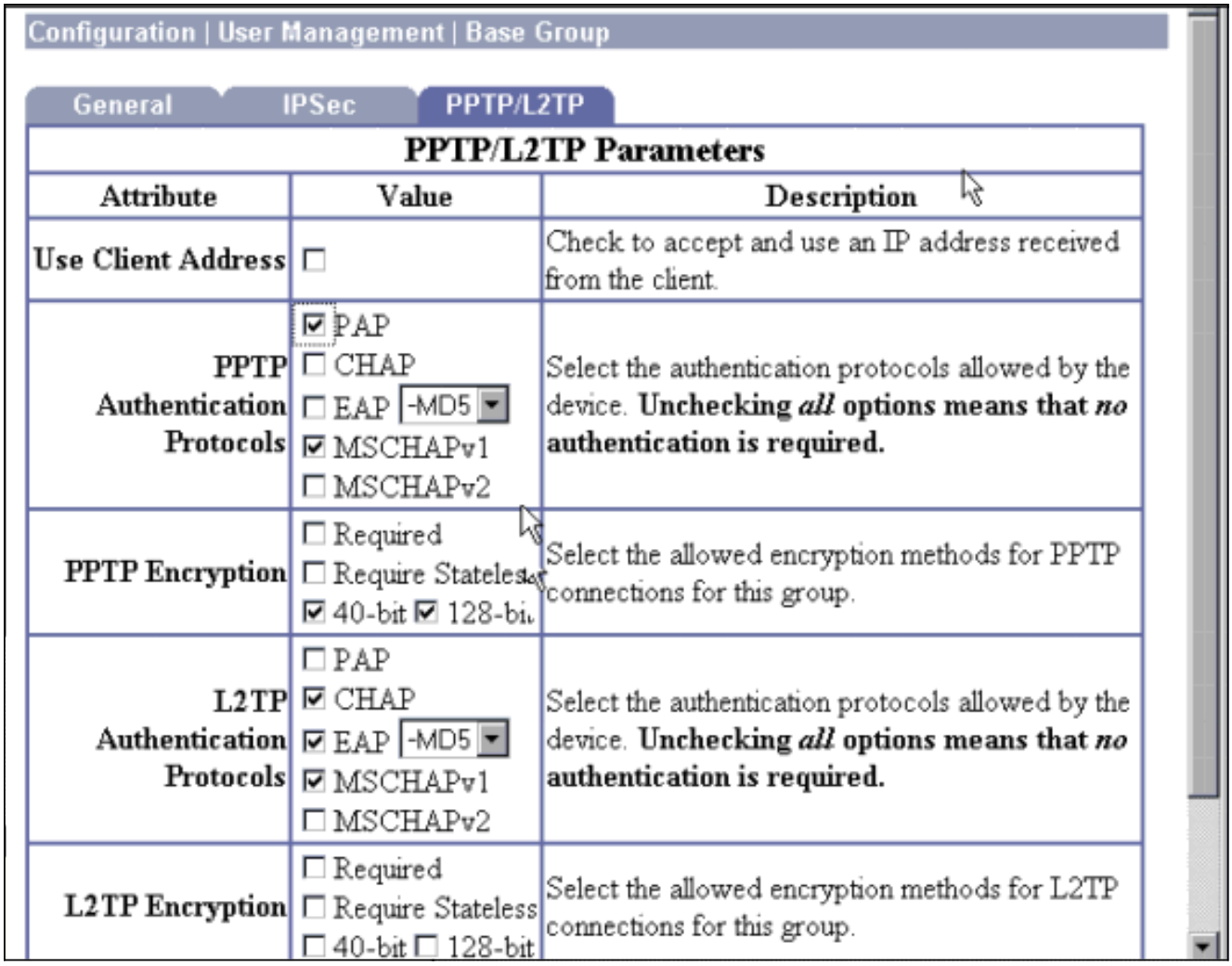
5. على مركز VPN 3000، انتقل إلى **التكوين > النظام > الخوادم > خوادم المصادقة**. حدد خادم مصادقة من القائمة، ثم حدد **إختبار**. اختبر المصادقة من مركز الشبكة الخاصة الظاهرية (VPN) إلى مصدر المحتوى الإضافي الآمن من Cisco لخادم Windows من خلال إدخال اسم مستخدم وكلمة مرور.في مصادقة جيدة، يجب أن يعرض مركز الشبكة الخاصة الظاهرية (VPN) رسالة "نجاح المصادقة". يتم تسجيل حالات الفشل في Cisco Secure ACS ل Windows في **التقارير والنشاط > محاولات فاشلة**. في عملية تثبيت افتراضية، يتم تخزين هذه التقارير على القرص في C:\Program Files\CiscoSecure ACS v2.5\LOG\Failed Attempts.



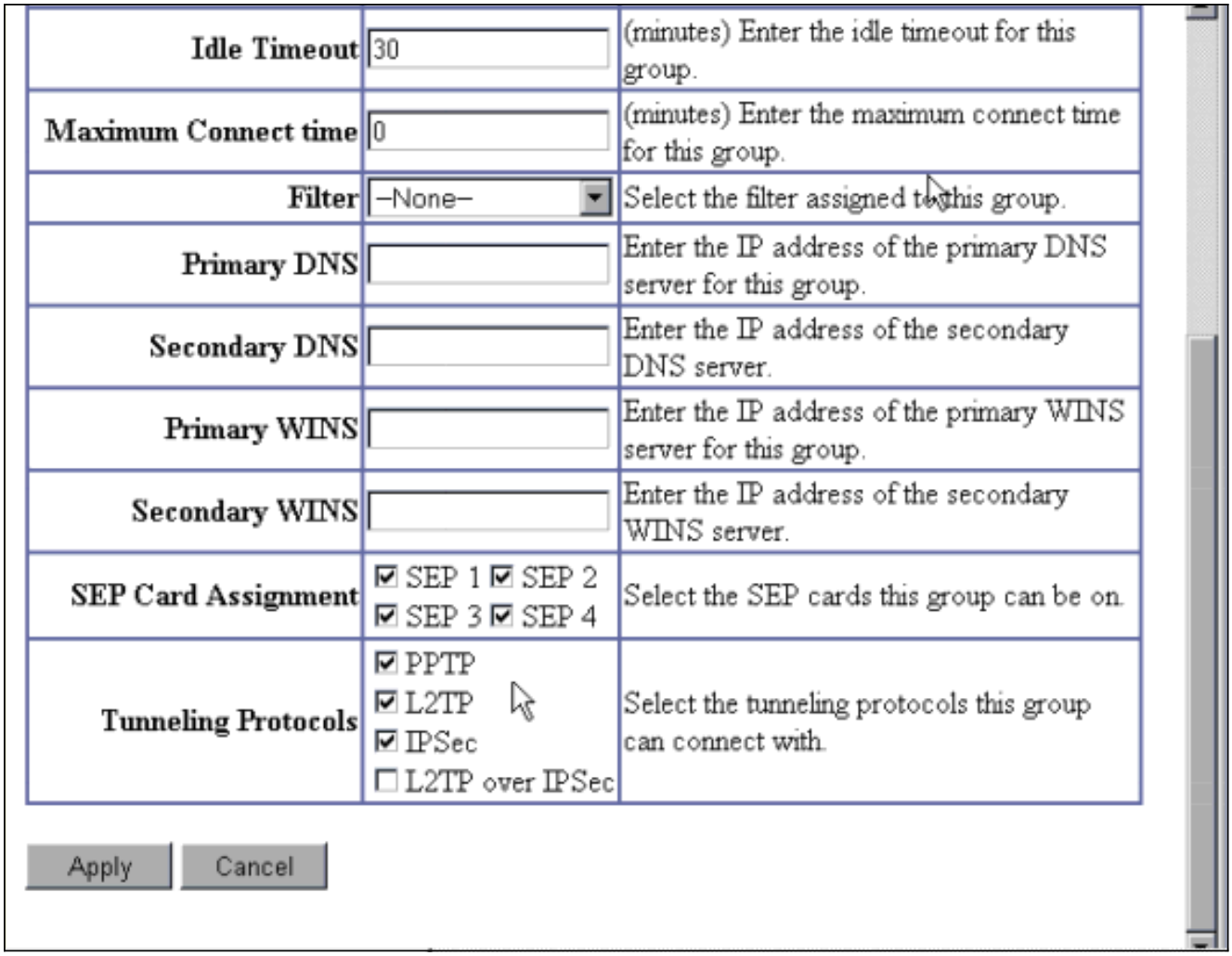
6. بما أنك قد قمت الآن بالتحقق من المصادقة من الكمبيوتر الشخصي إلى مركز VPN ومن المركز إلى ACS الآمن من Cisco لخادم Windows، فيمكنك إعادة تكوين مركز VPN لإرسال مستخدمي PPTP إلى Cisco ACS الآمن ل Windows RADIUS عن طريق نقل مصدر المحتوى الإضافي الآمن من Cisco لخادم Windows إلى أعلى قائمة الخوادم. للقيام بذلك على مركز الشبكة الخاصة الظاهرية (VPN)، انتقل إلى **التكوين > النظام > الخوادم > خوادم المصادقة**.



7. انتقل إلى **التكوين > إدارة المستخدم > المجموعة الأساسية** وحدد علامة التبويب **PPTP/L2TP**. في مجموعة قاعدة مركز الشبكة الخاصة الظاهرية (VPN)، تأكد من تمكين خيارات PAP و MSCHAPv1.



8. حدد علامة التبويب **عام** وتأكد من السماح ب PPTP في قسم بروتوكولات الاتصال النفقي.

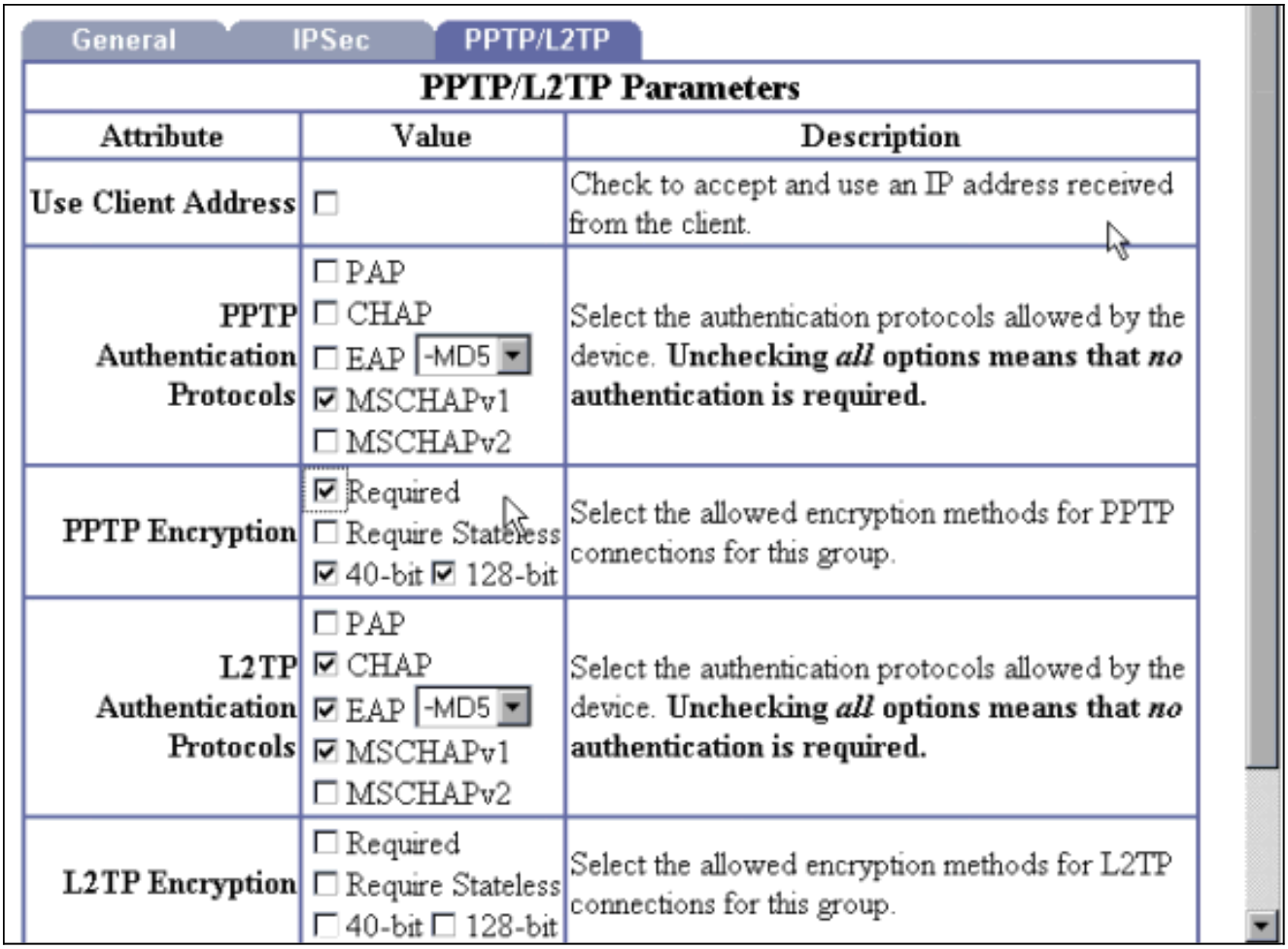


9. اختبر مصادقة PPTP مع المستخدم في ال cisco يؤمن ACS لخادم Windows RADIUS. إذا لم ينجح ذلك، فالرجاء مراجعة قسم تصحيح الأخطاء.

إضافة MPPE (تشفير)

إذا كان مصدر المحتوى الإضافي الآمن من Cisco لمصادقة PPTP Windows RADIUS يعمل دون تشفير، فيمكنك إضافة MPPE إلى مركز VPN 3000.

1. على مركز الشبكة الخاصة الظاهرية (VPN)، انتقل إلى **التكوين > إدارة المستخدم > المجموعة الأساسية**.
2. تحت قسم لتشفير PPTP، تحقق من الخيارات ل **مطلوب**، **40-بت**، و**128-بت**. بما أن ليس كل أجهزة الكمبيوتر تدعم كلا من تشفير 40 بت و 128 بت، تحقق من كلا الخيارين للسماح بالتفاوض.
3. تحت القسم لبروتوكولات مصادقة PPTP، تحقق من الخيار ل **MSCHAPv1**. (لقد قمت بالفعل بتكوين مصدر المحتوى الإضافي الآمن من Cisco لسمات مستخدم Windows 2.5 للتشفير في خطوة سابقة.)



ملاحظة: يجب التعرف على عميل PPTP لتشفير البيانات الأمثل أو المطلوب و MSCHAPv1 (إذا كان هناك خيار).

إضافة محاسبة

بعد إنشاء المصادقة، يمكنك إضافة محاسبة إلى مركز الشبكة الخاصة الظاهرية (VPN). انتقل إلى **التكوين > النظام > الخوادم > خوادم المحاسبة** وأضف مصدر المحتوى الإضافي الآمن من Cisco لخادم Windows.

في مصدر المحتوى الإضافي الآمن من Cisco ل Windows، تظهر سجلات المحاسبة كما يلي.

```
,Date,Time,User-Name,Group-Name,Calling-Station-Id,Acct-Status-Type,Acct-Session-Id
,Acct-Session-Time,Service-Type,Framed-Protocol,Acct-Input-Octets,Acct-Output-Octets
Acct-Input-Packets,Acct-Output-Packets,Framed-IP-Address,NAS-Port,NAS-IP-Address
,CSNTUSER,Default Group,,Start,8BD00003,,Framed,03/18/2000,08:16:20
PPP,,,,,1.2.3.4,1163,10.2.2.1
,CSNTUSER,Default Group,,Stop,8BD00003,30,Framed,03/18/2000,08:16:50
PPP,3204,24,23,1,1.2.3.4,1163,10.2.2.1
```

التحقق من الصحة

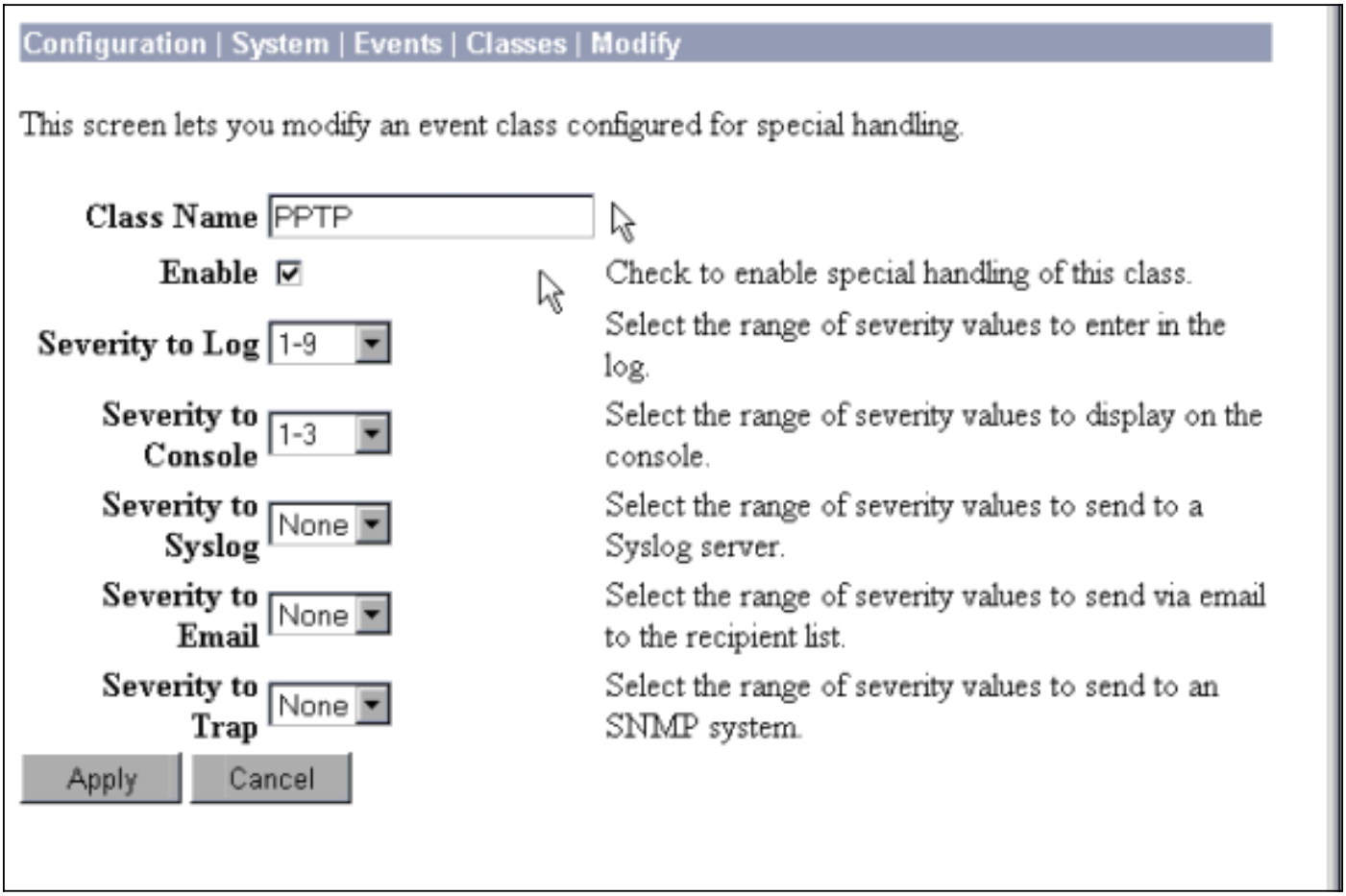
لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

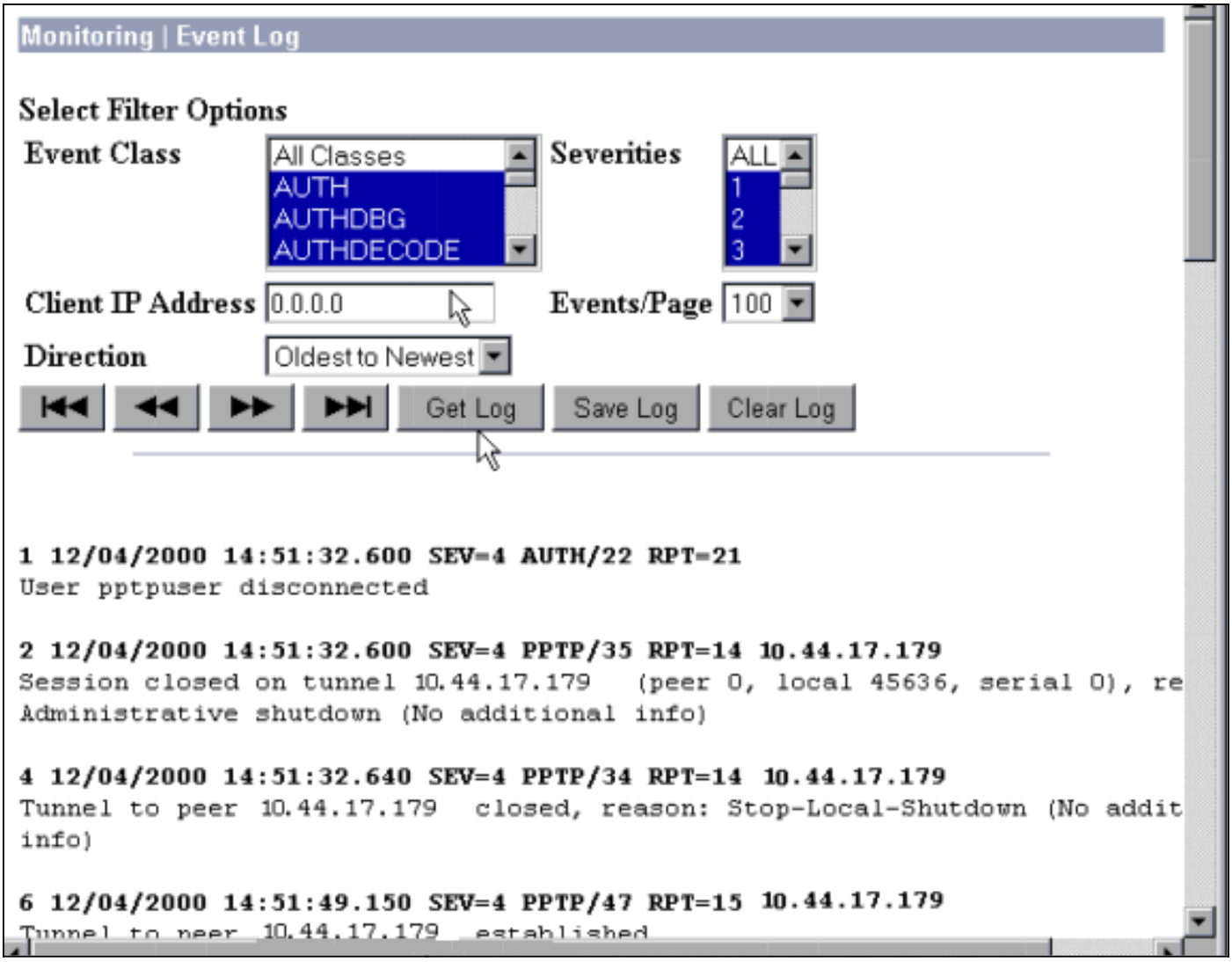
يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تمكين تصحيح الأخطاء

إذا لم تعمل الاتصالات، يمكنك إضافة فئات أحداث PPTP و AUTH إلى مركز VPN بالانتقال إلى **التكوين > النظام > الأحداث > الفئات > التعديل**. يمكنك أيضا إضافة فئات أحداث PPTPDBG، و PPTPDECODE، و AUTHDBG، و AUTHDECODE، ولكن هذه الخيارات قد توفر معلومات كثيرة جدا.



يمكنك إسترداد سجل الأحداث بالانتقال إلى **المراقبة > سجل الأحداث**.



تصحيح الأخطاء - مصادقة جيدة

ستبدو عمليات تصحيح الأخطاء الجيدة على مركز الشبكة الخاصة الظاهرية (VPN) مماثلة لما يلي.

```
SEV=4 PPTP/47 RPT=20 10.44.17.179 09:26:16.390 12/06/2000 1
                    Tunnel to peer 161.44.17.179 established
SEV=4 PPTP/42 RPT=20 10.44.17.179 09:26:16.390 12/06/2000 2
                      Session started on tunnel 161.44.17.179
                SEV=7 AUTH/12 RPT=22 09:26:19.400 12/06/2000 3
                    Authentication session opened: handle = 22
 SEV=6 AUTH/4 RPT=17 10.44.17.179 09:26:19.510 12/06/2000 4
 ,Authentication successful: handle = 22, server = 10.2.2.5
                                                 user = CSNTUSER
  SEV=5 PPP/8 RPT=17 10.44.17.179 09:26:19.510 12/06/2000 5
                                               [ User [ CSNTUSER
                     Authenticated successfully with MSCHAP-V1
                SEV=7 AUTH/13 RPT=22 09:26:19.510 12/06/2000 6
                    Authentication session closed: handle = 22
                SEV=4 AUTH/21 RPT=30 09:26:22.560 12/06/2000 7
                                    User CSNTUSER connected
```

الأخطاء المحتملة

قد تواجه أخطاء محتملة كما هو موضح أدناه.

اسم مستخدم أو كلمة مرور غير صحيحة على Cisco Secure ACS لخادم Windows RADIUS

- إخراج تصحيح أخطاء مركز VPN 3000

```
SEV=4 PPTP/47 RPT=21 10.44.17.179 09:33:03.910 12/06/2000 6
                    Tunnel to peer 10.44.17.179 established

SEV=4 PPTP/42 RPT=21 10.44.17.179 09:33:03.920 12/06/2000 7
                        Session started on tunnel 10.44.17.179

                SEV=7 AUTH/12 RPT=23 09:33:06.930 12/06/2000 8
                    Authentication session opened: handle = 23

SEV=3 AUTH/5 RPT=4 10.44.17.179 09:33:07.050 12/06/2000 9
                Authentication rejected: Reason = Unspecified
            handle = 23, server = 10.2.2.5, user = baduser

SEV=5 PPP/9 RPT=4 10.44.17.179 09:33:07.050 12/06/2000 11
                                        [ User [ baduser
        ( disconnected.. failed authentication ( MSCHAP-V1

                SEV=7 AUTH/13 RPT=23 09:33:07.050 12/06/2000 12
                    Authentication session closed: handle = 23
```

- مصدر المحتوى الإضافي الآمن من Cisco لإخراج سجل Windows

```
Authen failed, baduser,,,CS user,03/18/2000,08:02:47
unknown,,,1155,10.2.2.1
```

- الرسالة التي يراها المستخدم (من Windows 98)

```
Error 691: The computer you have dialed in to has denied access because
.the username and/or password is invalid on the domain
```

يتم تحديد "تشفير MPPE مطلوب" على مركز التركيز، ولكن لم يتم تكوين مصدر المحتوى الإضافي الآمن من Cisco لخادم Windows لأنواع MS-CHAP-MPPE-Keys و MS-CHAP-MPPE

- إخراج تصحيح أخطاء مركز VPN 3000إذا كان AUTHDECODE (مستوى خطورة 1-13) وتصحيح أخطاء PPTP (مستوى خطورة 1-9) قيد التشغيل، يظهر السجل أن مصدر المحتوى الإضافي الآمن من Cisco لخادم Windows لا يرسل السمة 26 (0x1a) الخاصة بالمورد في قبول الوصول من الخادم (سجل جزئي).

```
SEV=13 AUTHDECODE/0 RPT=545 10:01:52.360 12/08/2000 2221
.024E002C 80AE75F6 6C365664 373D33FE     .N.,..u.l6Vd7=3 :0000
....6DF74333 501277B2 129CBC66 85FFB40C     m.C3P.w....f :0010
 ........../..                 16D42FC4 BD020806 FFFFFFFF :0020

SEV=5 PPP/13 RPT=12 10.44.17.179 10:00:29.570 12/08/2000 2028
User [ CSNTUSER ] disconnected. Data encrypt required. Auth server
.or auth protocol will not support encrypt
```

- لا يظهر مصدر المحتوى الإضافي الآمن من Cisco لمخرجات سجل Windows أي حالات فشل.
- الرسالة التي يراها المستخدم

```
Error 691: The computer you have dialed in to has denied access because
.the username and/or password is invalid on the domain
```

معلومات ذات صلة

- صفحة دعم مركز Cisco VPN 3000 Series
- صفحة دعم عميل Cisco VPN 3000 Series
- صفحة دعم IPSec
- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم Windows
- صفحة دعم RADIUS
- صفحة دعم PPTP

- المعيار RFC 2637: بروتوكول الاتصال النفقي من نقطة إلى نقطة (PPTP)
- 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).