مادختساب Cisco VPN 3000 زكرم نيوكت Microsoft RADIUS

المحتويات

المقدمة

خادم مصادقة الإنترنت من Microsoft (IAS) ونظام الإنترنت التجاري من Microsoft (MCIS 2.0) متاحان حاليا. خادم Microsoft RADIUS مناسب لأنه يستخدم Active Directory على وحدة التحكم بالمجال الأساسية لقاعدة بيانات المستخدم الخاصة به. لم تعد بحاجة إلى الاحتفاظ بقاعدة بيانات منفصلة. كما يدعم تشفير 40-بت و 128-بت لاتصالات شبكة VPN لبروتوكول الاتصال النفقي من نقطة إلى نقطة (PPTP). راجع قائمة التحقق من Microsoft: تكوين IAS لوثائق الطلب الهاتفي والوصول إلى VPN للحصول على مزيد من المعلومات.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

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

تثبيت خادم RADIUS وتكوينه على Windows 2000 و Windows 2003

تثبيت خادم RADIUS

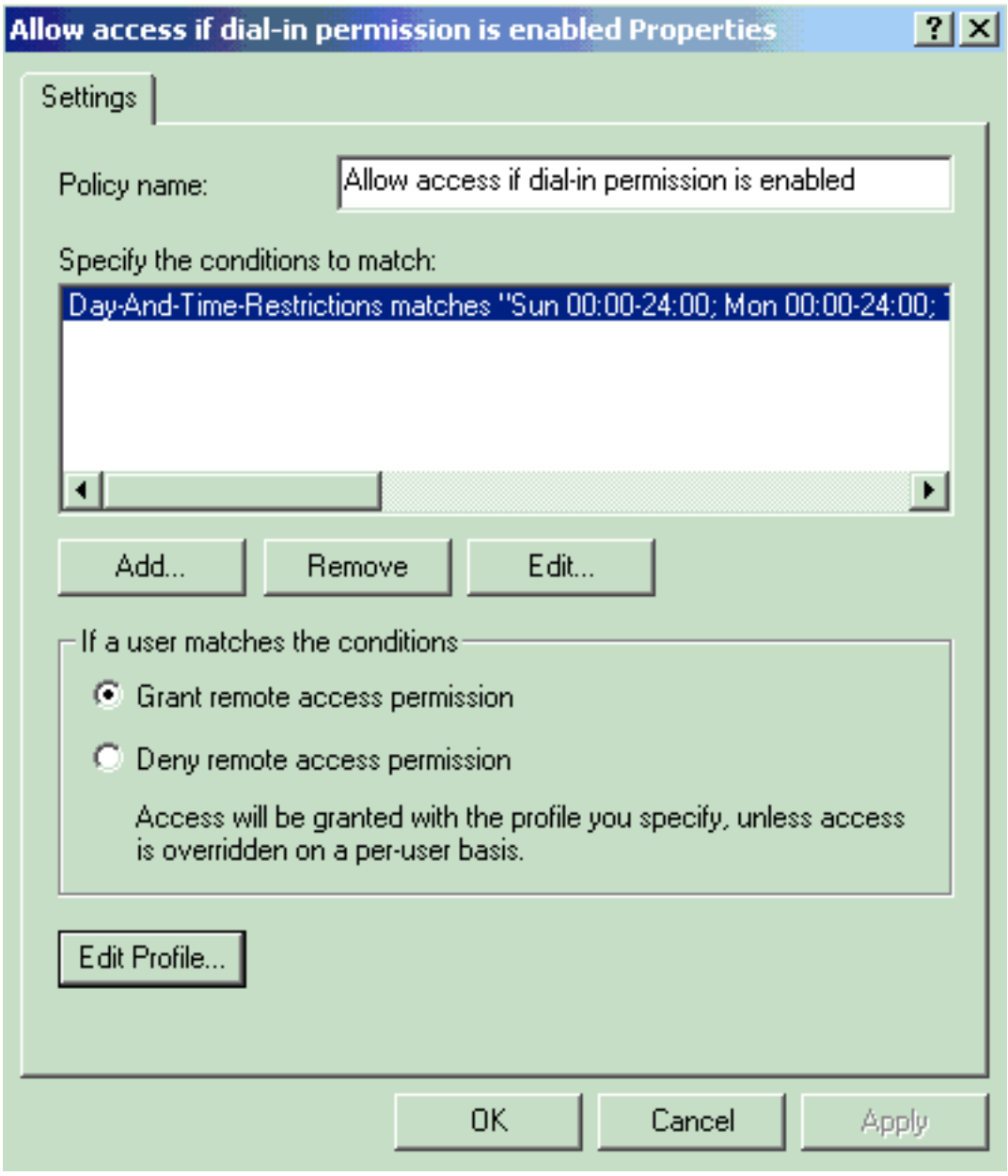
إذا لم يكن خادم RADIUS (IAS) مثبتا بالفعل، فعليك تنفيذ هذه الخطوات للتثبيت. إذا كان خادم RADIUS مثبتا لديك بالفعل، فتابع إلى خطوات التكوين.

1. أدخل القرص المضغوط ل Windows Server وابدأ برنامج الإعداد.
2. انقر على **تثبيت مكونات الوظيفة الإضافية**، ثم انقر على **إضافة/إزالة مكونات Windows**.
3. في المكونات، انقر فوق **خدمات الشبكة** (ولكن لا تحدد أو تمسح خانة الاختيار)، ثم انقر فوق **التفاصيل**.
4. تحقق من **خدمة مصادقة الإنترنت** وانقر فوق **موافق**.
5. انقر فوق **Next (التالي)**.

تكوين خادم Microsoft Windows 2000 باستخدام IAS

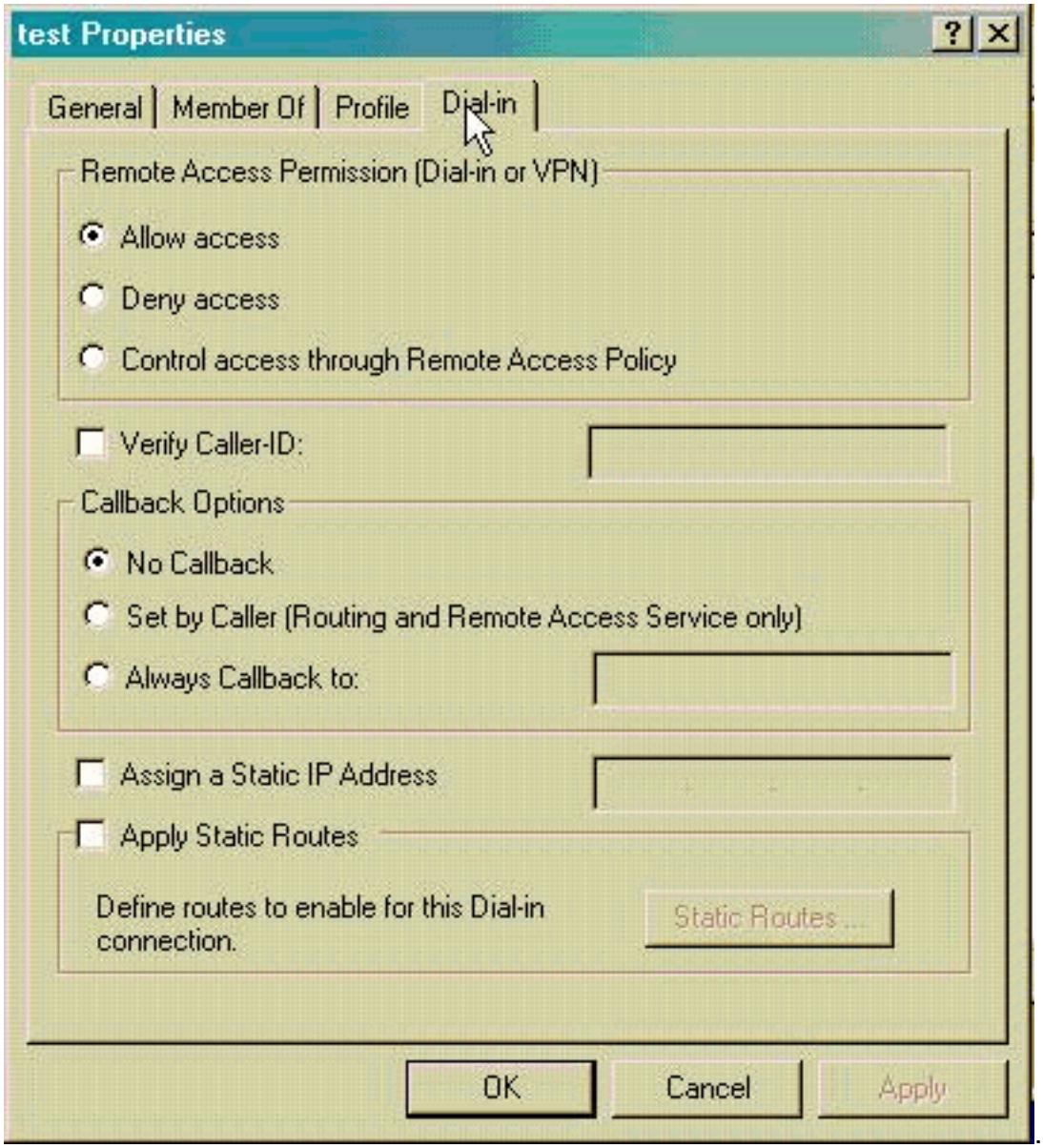
أكمل هذه الخطوات لتكوين خادم RADIUS (IAS) وبدء الخدمة من أجل جعلها متوفرة لمصادقة المستخدمين على مركز VPN.

1. أختر **ابدأ > برامج > أدوات إدارية > خدمة مصادقة الإنترنت**.
2. انقر بزر الماوس الأيمن فوق **خدمة مصادقة الإنترنت**، وانقر فوق **خصائص** من القائمة الفرعية التي تظهر.
3. انتقل إلى علامة التبويب RADIUS لفحص إعدادات المنافذ.إذا إختلفت منافذ مصادقة RADIUS ومنافذ بروتوكول مخطط بيانات المستخدم لمحاسبة RADIUS (UDP) عن القيم الافتراضية المقدمة (1812 و 1645 للمصادقة، 1813 و 1646 للمحاسبة) في المصادقة والمحاسبة، فاكتب إعدادات المنفذ. طقطقت **ok** عندما أنت إنتهيت.**ملاحظة:** لا تغير المنافذ الافتراضية. افصل المنافذ باستخدام الفواصل لاستخدام إعدادات منافذ متعددة لطلبات المصادقة أو المحاسبة.
4. انقر بزر الماوس الأيمن فوق **العملاء** واختر **عميل جديد** لإضافة مركز الشبكة الخاصة الظاهرية (VPN) كعميل مصادقة والتخويل والمحاسبة (AAA) إلى خادم RADIUS (IAS).**ملاحظة:** إذا تم تكوين التكرار بين مركزي VPN 3000 من Cisco، فيجب أيضا إضافة مركز Cisco VPN 3000 الاحتياطي إلى خادم RADIUS كعميل RADIUS.
5. أدخل اسما مألوفا وحدد على هيئة **Protocol Radius**.
6. قم بتعريف مركز VPN باستخدام عنوان IP أو اسم DNS على الإطار التالي.
7. أختر **Cisco** من شريط تمرير العميل-المورد.
8. أدخل سر مشترك.**ملاحظة:** يجب أن تتذكر السر *الدقيق* الذي تستخدمه. أنت تحتاج هذا معلومة in order to شكلت ال VPN مركز.
9. انقر فوق **إنهاء**.
10. انقر نقرا مزدوجا فوق **نهج الوصول عن بعد** وانقر نقرا مزدوجا فوق النهج الذي يظهر في الجانب الأيمن من الإطار.**ملاحظة:** بعد تثبيت IAS، يجب أن يكون نهج الوصول عن بعد موجودا بالفعل.في Windows 2000، يتم منح التخويل استنادا إلى خصائص الطلب الهاتفي لحساب المستخدم ونهج الوصول عن بعد. سياسات الوصول عن بعد هي مجموعة من الشروط وإعدادات الاتصال التي تمنح مسؤولي الشبكة المزيد من المرونة في التصريح بمحاولات الاتصال. تستخدم كل من خدمة التوجيه والوصول عن بعد في Windows 2000 و Windows 2000 IAS نهج الوصول عن بعد لتحديد ما إذا كان سيتم قبول محاولات الاتصال أو رفضها. في كلتا الحالتين، يتم تخزين سياسات الوصول عن بعد محليا. ارجع إلى وثائق Windows 2000 IAS للحصول على مزيد من المعلومات حول كيفية معالجة محاولات



الاتصال.

11. أختر **منح إذن الوصول عن بعد** وانقر فوق **تحرير ملف التعريف** لتكوين خصائص الطلب الهاتفي.
12. حدد البروتوكول المطلوب إستخدامه للمصادقة في علامة تبويب المصادقة. تحقق من **Microsoft Encrypted Authentication الإصدار 2** وقم بإلغاء تحديد جميع بروتوكولات المصادقة الأخرى.**ملاحظة:** يجب أن تتطابق الإعدادات الموجودة في ملف تعريف الطلب الهاتفي هذا مع الإعدادات الموجودة في تكوين مركز VPN 3000 وعميل الطلب الهاتفي. في هذا المثال، يتم إستخدام مصادقة MS-CHAPv2 دون تشفير PPTP.
13. في علامة تبويب التشفير، تحقق من **عدم التشفير** فقط.
14. انقر على **موافق** لإغلاق ملف تعريف الطلب الهاتفي، ثم انقر على **موافق** لإغلاق نافذة نهج الوصول عن بعد.
15. انقر بزر الماوس الأيمن فوق **خدمة مصادقة الإنترنت** وانقر فوق **بدء الخدمة** في شجرة وحدة التحكم.**ملاحظة:** يمكنك أيضا إستخدام هذه الوظيفة لإيقاف الخدمة.
16. أكمل هذه الخطوات لتعديل المستخدمين للسماح بالاتصال.أختر **وحدة التحكم > إضافة/إزالة الأداة الإضافية**.انقر فوق **إضافة** واختر **الأداة الإضافية للمستخدمين المحليين والمجموعات المحلية**.انقر فوق **إضافة (Add)**.تأكد من تحديد **الكمبيوتر المحلي**طقطقة **إنجاز** و**ok**.
17. قم بتوسيع **المستخدم المحلي والمجموعات المحلية** وانقر فوق مجلد **المستخدمين** في الجزء الأيسر. في الجزء الأيمن، انقر نقرا مزدوجا على المستخدم (مستخدم شبكة VPN) الذي تريد السماح بالوصول إليه.
18. انتقل إلى علامة التبويب "الطلب الهاتفي" واختر **السماح بالوصول** بموجب إذن الوصول عن بعد (الطلب الهاتفي



أو VPN).

19. طقطقة **يطبق** و**ok** in order to أتمت الإجراء. يمكنك إغلاق نافذة "إدارة وحدة التحكم" وحفظ جلسة العمل، إذا كان ذلك مطلوبا.يمكن للمستخدمين الذين قمت بتعديلهم الآن الوصول إلى مركز الشبكة الخاصة الظاهرية (VPN) باستخدام عميل الشبكة الخاصة الظاهرية (VPN). تذكر أن خادم IAS يقوم بمصادقة معلومات المستخدم فقط. لا يزال مركز الشبكة الخاصة الظاهرية (VPN) يقوم بمصادقة المجموعة.

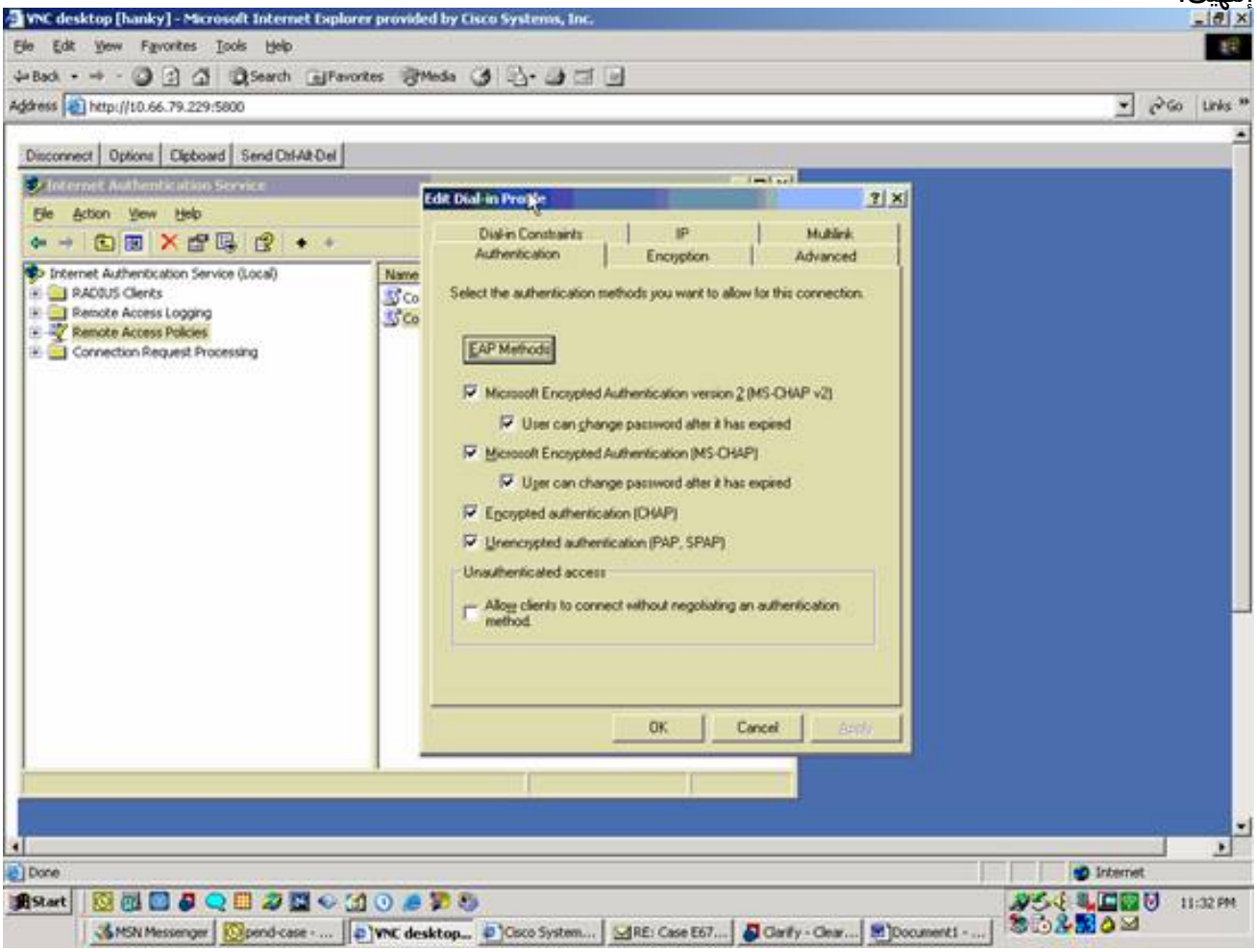
تكوين خادم Microsoft Windows 2003 باستخدام IAS

أكمل هذه الخطوات لتكوين خادم Microsoft Windows 2003 باستخدام IAS.

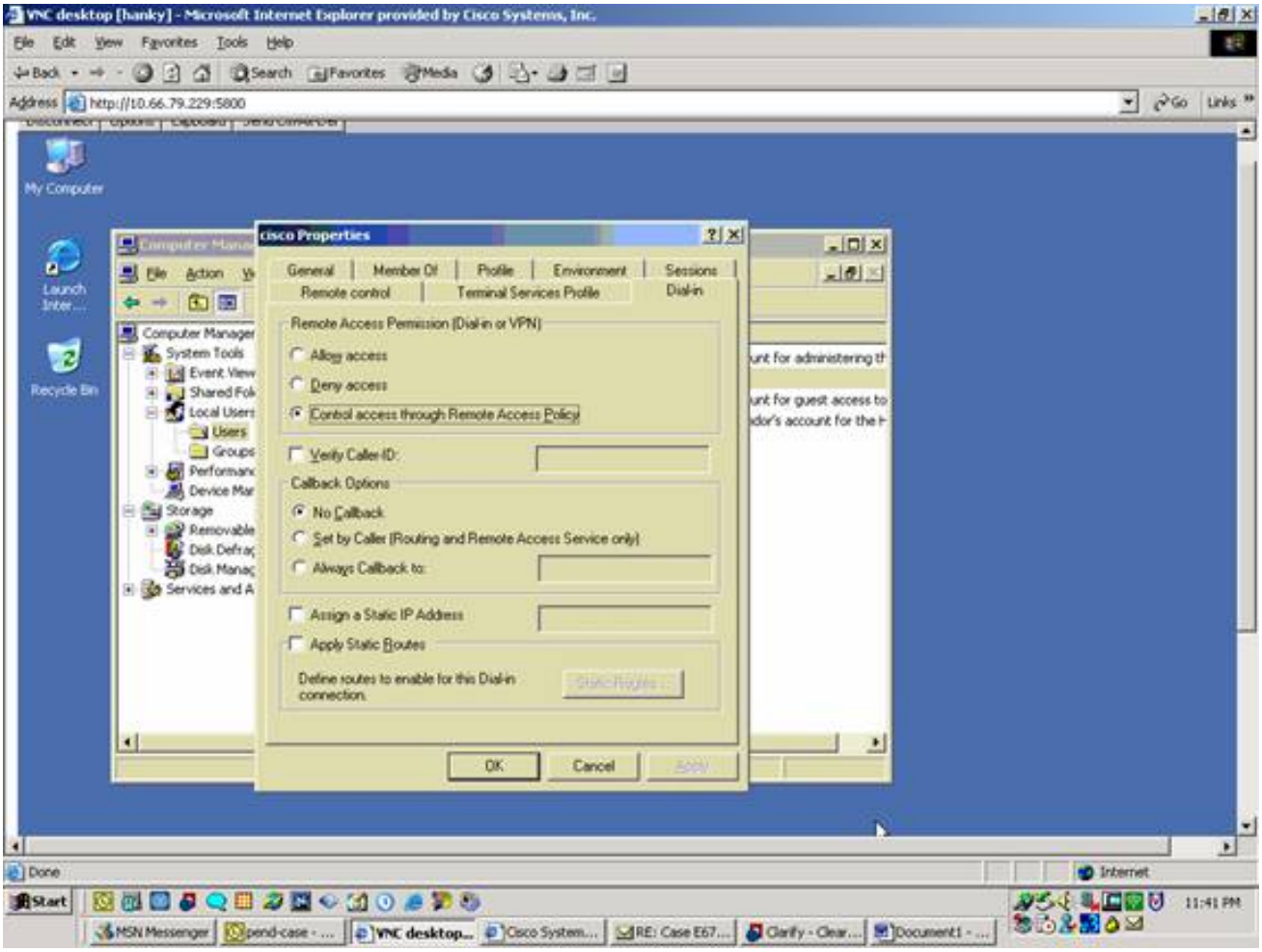
ملاحظة: تفترض هذه الخطوات أن IAS مثبت بالفعل على الجهاز المحلي. وإذا لم تكن هناك مساحة، فقم بإضافة هذا من خلال **لوحة التحكم > إضافة/إزالة البرامج**.

1. أختر **أدوات إدارية > خدمة مصادقة الإنترنت** وانقر بزر الماوس الأيمن على **عميل RADIUS** لإضافة عميل RADIUS جديد. بعد كتابة معلومات العميل، انقر فوق **موافق**.
2. أدخل اسما مألوفا.
3. قم بتعريف مركز VPN باستخدام عنوان IP أو اسم DNS على الإطار التالي.
4. أختر **Cisco** من شريط تمرير العميل-المورد.
5. أدخل سر مشترك.**ملاحظة:** يجب أن تتذكر السر *الدقيق* الذي تستخدمه. أنت تحتاج هذا معلومة in order to شكلت ال VPN مركز.
6. طقطقة **ok** أن يستكمل.

7. انتقل إلى **نهج الوصول عن بعد**، وانقر بزر الماوس الأيمن فوق **الاتصالات بخوادم الوصول الأخرى**، واختر **الخصائص**.
8. أختر **منح إذن الوصول عن بعد** وانقر فوق **تحرير ملف التعريف** لتكوين خصائص الطلب الهاتفي.
9. حدد البروتوكول المطلوب إستخدامه للمصادقة في علامة تبويب المصادقة. تحقق من **Microsoft Encrypted Authentication الإصدار 2** وقم بإلغاء تحديد جميع بروتوكولات المصادقة الأخرى.**ملاحظة:** يجب أن تتطابق الإعدادات الموجودة في ملف تعريف الطلب الهاتفي هذا مع الإعدادات الموجودة في تكوين مركز VPN 3000 وعميل الطلب الهاتفي. في هذا المثال، يتم إستخدام مصادقة MS-CHAPv2 دون تشفير PPTP.
10. في علامة تبويب التشفير، تحقق من **عدم التشفير** فقط.
11. طقطقت **ok** عندما أنت إنتهيت.



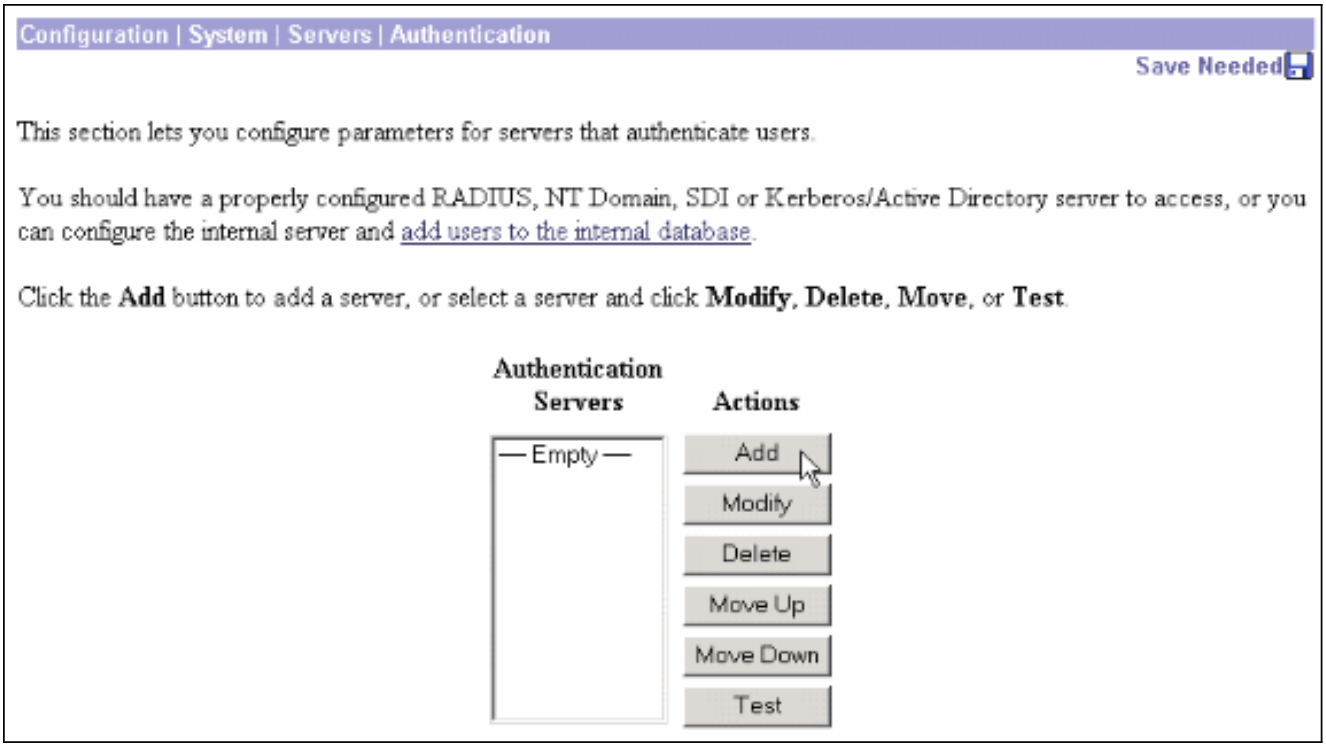
12. انقر بزر الماوس الأيمن فوق **خدمة مصادقة الإنترنت** وانقر فوق **بدء الخدمة** في شجرة وحدة التحكم.**ملاحظة:** يمكنك أيضا إستخدام هذه الوظيفة لإيقاف الخدمة.
13. أختر **أدوات إدارية > إدارة الكمبيوتر > أدوات النظام > المستخدمون المحليون والمجموعات المحلية**، وانقر بزر الماوس الأيمن فوق **المستخدمين** واختر **المستخدمون الجدد** لإضافة مستخدم إلى حساب الكمبيوتر المحلي.
14. أضفت مستعمل مع cisco كلمة "vpnpassword" وفحصت هذا توصيف معلومة.على علامة التبويب "عام"، تأكد من تحديد خيار **كلمة المرور التي لا تنتهي صلاحيتها أبدا** بدلا من الخيار الخاص ب المستخدم الذي يجب عليه تغيير كلمة المرور.في علامة التبويب "الطلب الهاتفي"، أختر الخيار ل **السماح بالوصول** (أو أترك الإعداد الافتراضي ل Control Access من خلال نهج الوصول عن بعد).طقطقت **ok** عندما أنت إنتهيت.



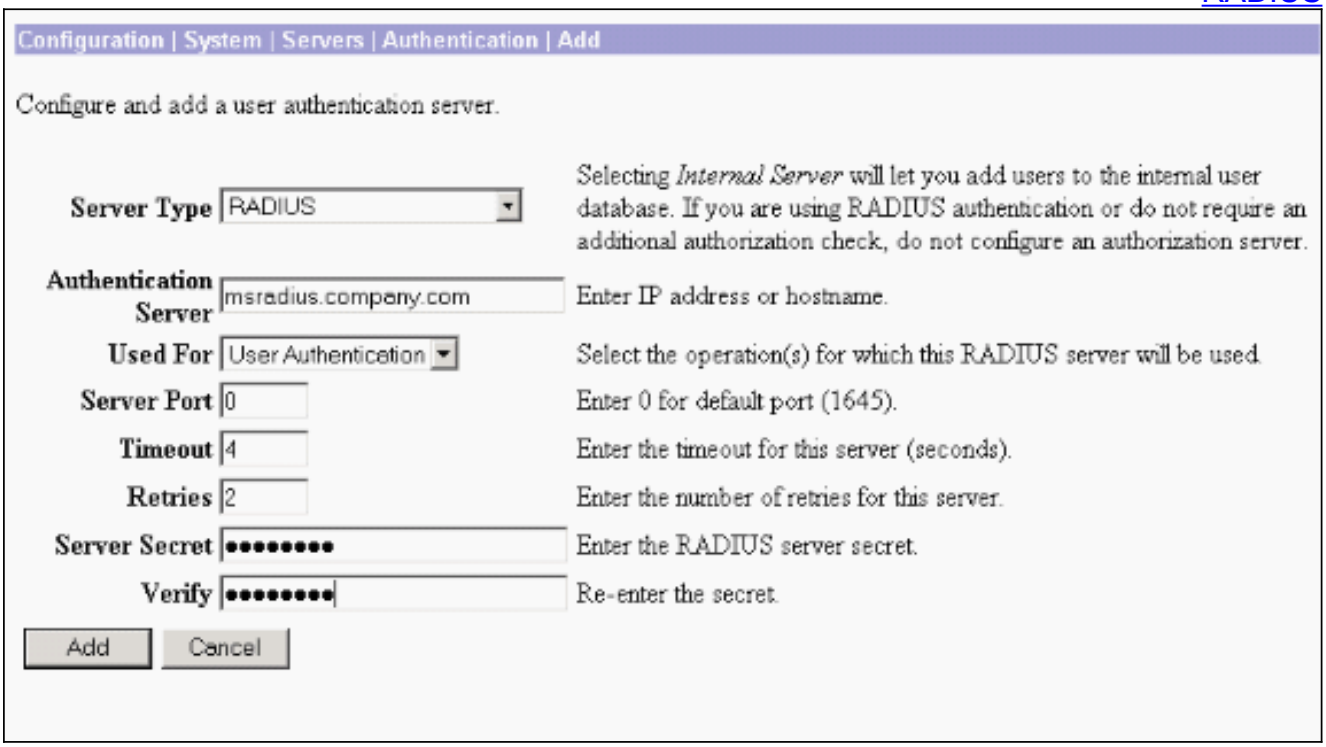
تكوين مركز Cisco VPN 3000 لمصادقة RADIUS

أتمت هذا steps in order to شكلت ال VPN 3000 مركز ل RADIUS صحة هوية.

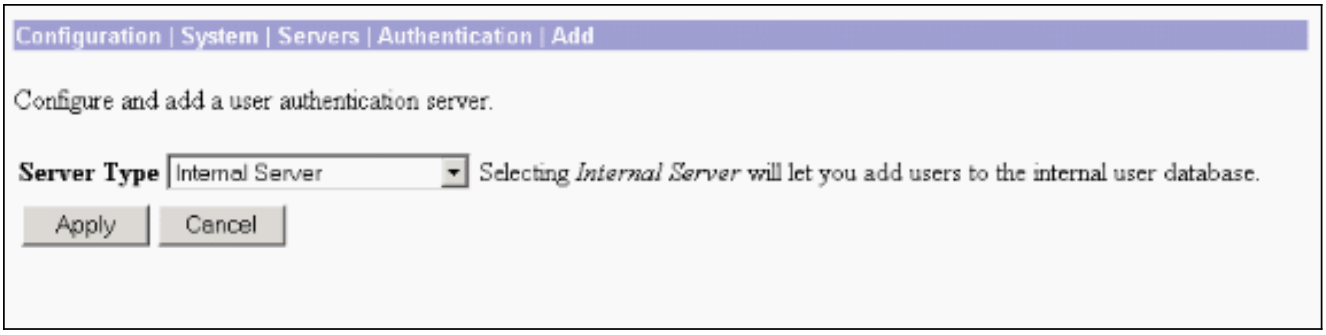
1. قم بالاتصال بمركز الشبكة الخاصة الظاهرية (VPN) باستخدام مستعرض الويب الخاص بك، واختر **التكوين > النظام > الخوادم > المصادقة** من قائمة الإطارات اليسرى.



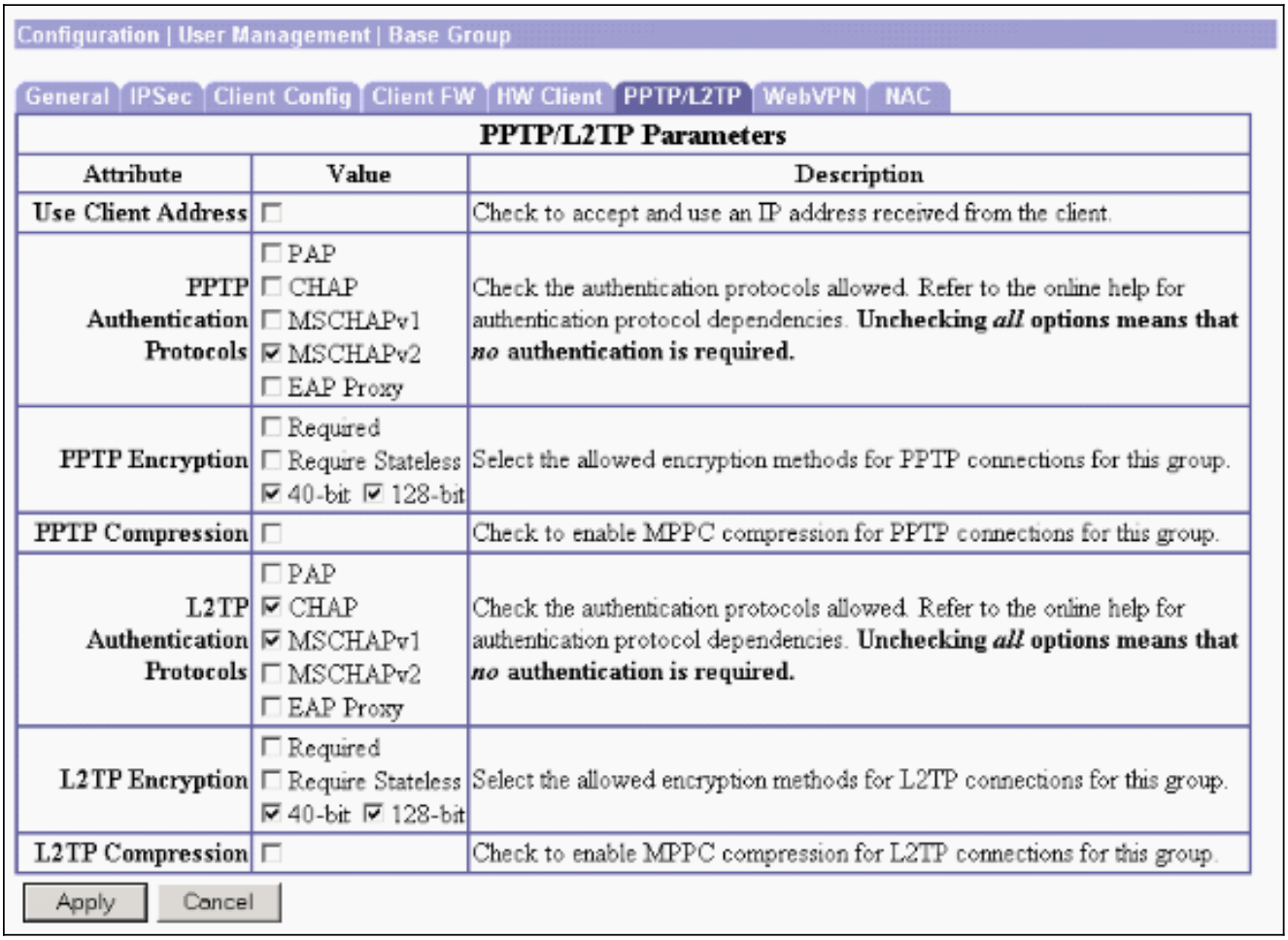
2. طقطقة **يضيف** وبشكل هذا عملية إعداد.نوع الخادم = RADIUSخادم المصادقة = عنوان IP أو اسم المضيف لخادم RADIUS (IAS)منفذ الخادم = 0 (default=1645=0)سر الخادم = نفسه الموجود في الخطوة 8 في القسم الموجود على تكوين خادم RADIUS



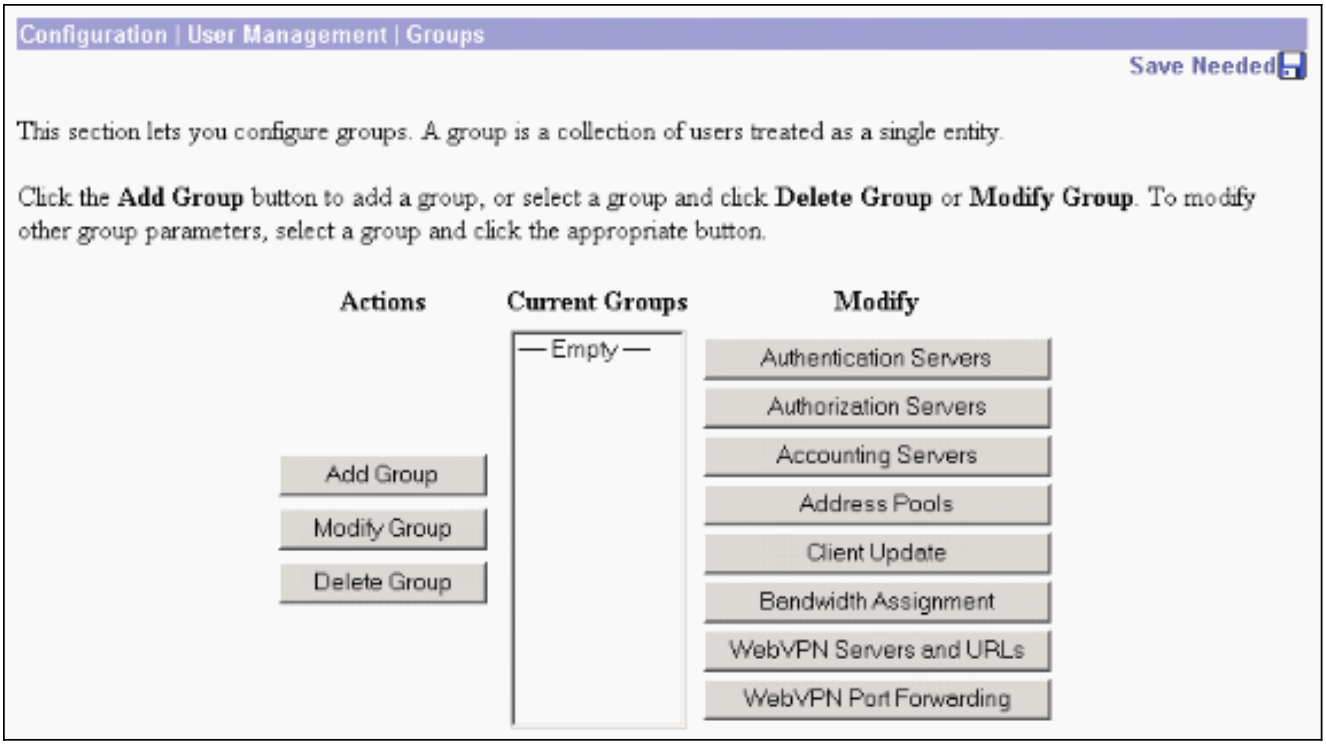
3. انقر فوق **إضافة** لإضافة التغييرات إلى التكوين الجاري تشغيله.
4. انقر فوق **إضافة**، واختر **الخادم الداخلي** لنوع الخادم، وانقر فوق **تطبيق**.تحتاج إلى هذا لاحقا لتكوين مجموعة IPsec (تحتاج فقط إلى نوع الخادم = خادم داخلي).



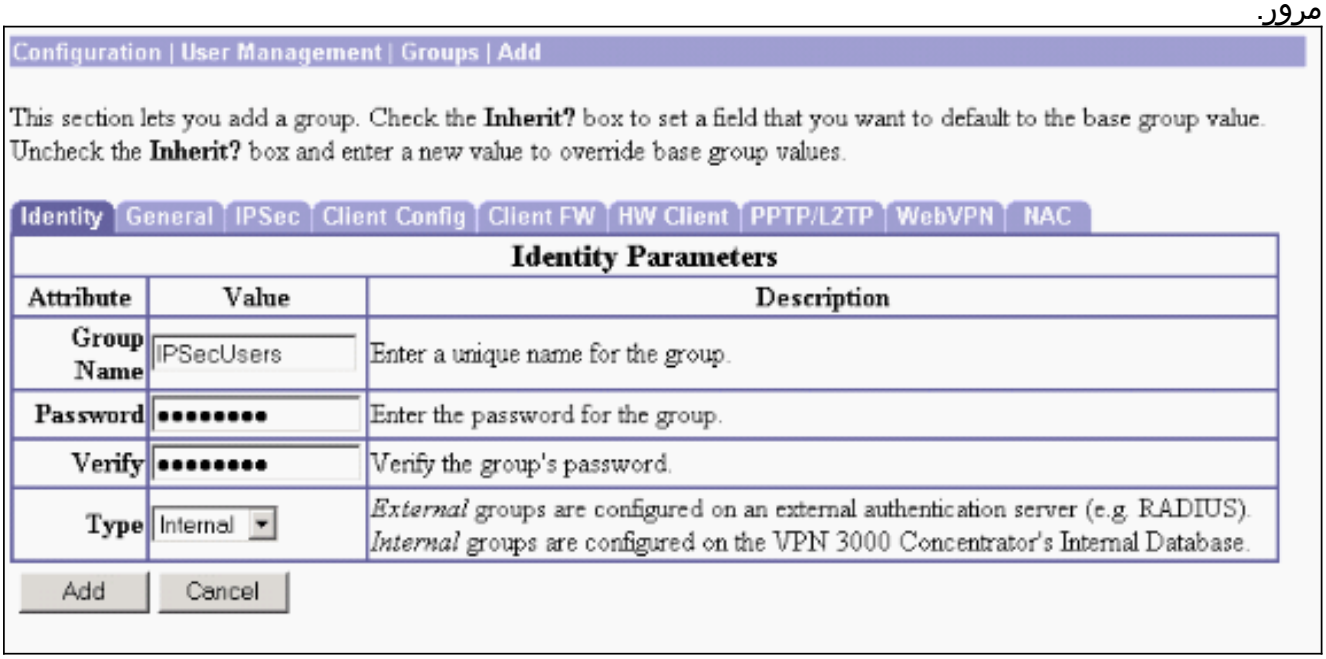
5. قم بتكوين مركز VPN لمستخدمي PPTP أو لمستخدمي عميل **PPTP**.VPNأتمت هذا steps in order to شكلت لمستخدمي PPTP.أختر **تكوين > إدارة المستخدم > مجموعة أساسية**، وانقر فوق علامة التبويب **PPTP/L2TP**.أختر **MSCHAPv2** وألغي تحديد بروتوكولات المصادقة الأخرى في قسم بروتوكولات مصادقة PPTP.



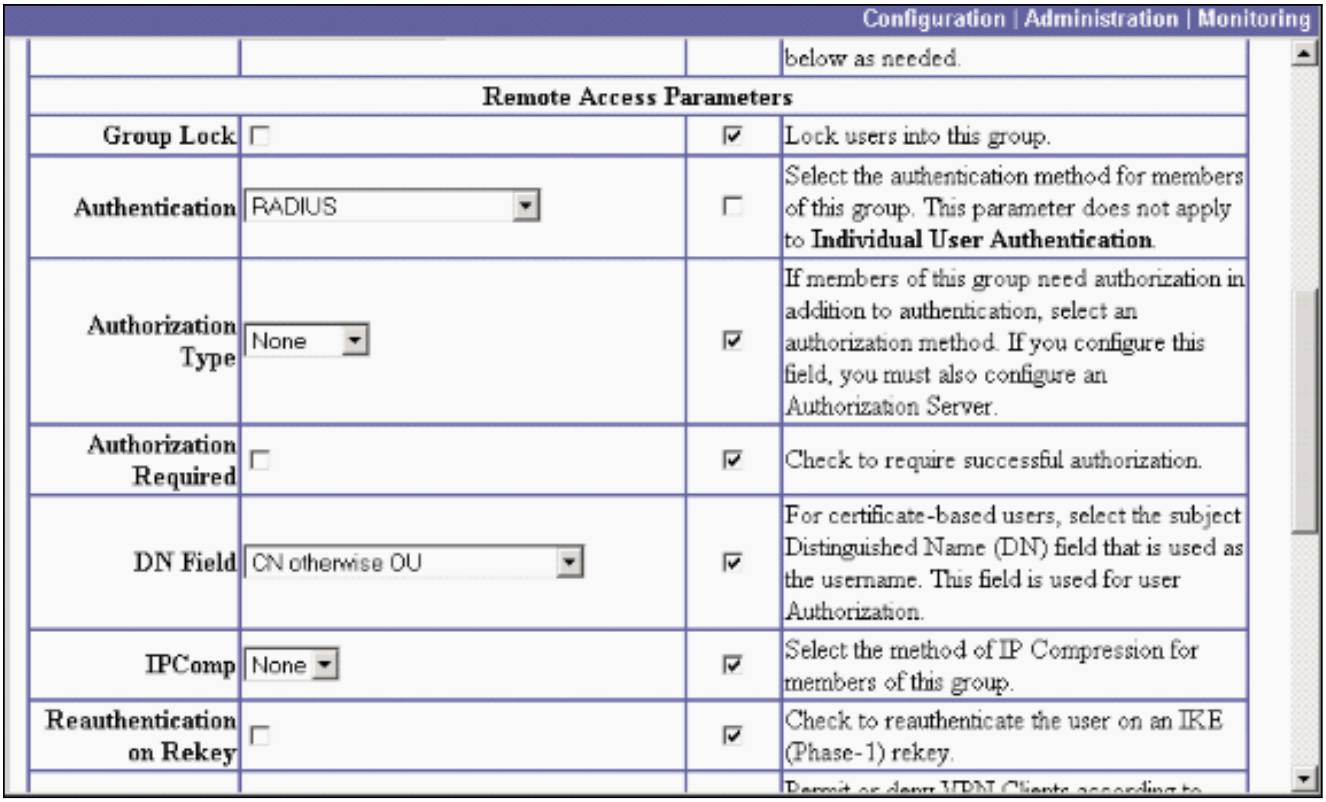
انقر فوق **تطبيق** في أسفل الصفحة لإضافة التغييرات إلى التكوين الجاري تشغيله.والآن عندما يتصل مستخدمو PPTP، تتم مصادقتهم بواسطة خادم IAS) RADIUS).**عميل شبكة VPN**أتمت هذا steps in order to شكلت ل VPN زبون مستخدم.أخترت **تشكيل>مستعمل إدارة>مجموعة** وطقطقة **يضيف** in order to أضفت مجموعة جديد.



اكتب اسم مجموعة (على سبيل المثال، IPsecUsers) وكلمة
مرور.



يتم إستخدام كلمة المرور هذه كمفتاح مشترك مسبقا لمفاوضات النفق.انتقل إلى علامة التبويب IPSec واضبط
المصادقة على
.RADIUS



وهذا يسمح بمصادقة عملاء IPsec عبر خادم مصادقة RADIUS.انقر فوق **إضافة** في أسفل الصفحة لإضافة التغييرات إلى التكوين الجاري تشغيله.الآن عند اتصال عملاء IPsec بالمجموعة التي قمت بتكوينها واستخدامها، تتم مصادقتهم بواسطة خادم RADIUS.

التحقق من الصحة

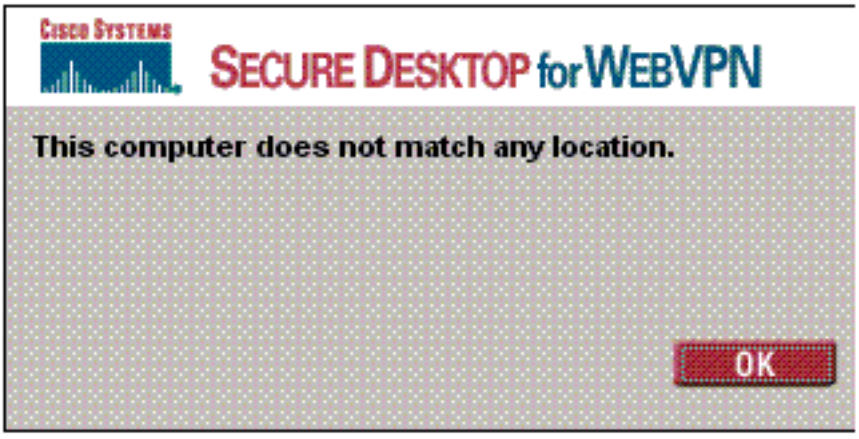
لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

فشل مصادقة WebVPN

توفر هذه الأقسام معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- **المشكلة**: لا يمكن لمستخدمي WebVPN المصادقة مقابل خادم RADIUS ولكن يمكن مصادقتهم بنجاح مع قاعدة البيانات المحلية الخاصة بموجه VPN. يتلقون أخطاء مثل "فشل تسجيل الدخول" وهذه



الرسالة. **السبب**: تحدث هذه الأنواع من المشاكل عادة عند إستخدام أي قاعدة بيانات أخرى غير قاعدة البيانات الداخلية ل مركز التركيز. يؤثر مستخدمو

WebVPN على المجموعة الأساسية عند توصيلهم أولا بالمكثف ويجب عليهم إستخدام طريقة المصادقة الافتراضية. غالبا ما يتم ضبط هذه الطريقة على قاعدة البيانات الداخلية ل Concentrator ولا تكون نصف قطر مكون أو خادم آخر.**الحل**: عندما يقوم مستخدم WebVPN بالمصادقة، يتحقق المكثف من قائمة الخوادم المحددة في **التكوين > النظام > الخوادم > المصادقة** ويستخدم الخادم الأعلى. تأكد من نقل الخادم الذي تريد من مستخدمي WebVPN المصادقة عليه إلى أعلى هذه القائمة. على سبيل المثال، إذا كان يجب أن يكون RADIUS طريقة مصادقة، فأنت بحاجة لنقل خادم RADIUS إلى أعلى القائمة لدفع المصادقة إليه.**ملاحظة:** لا يعني مجرد أن مستخدمي شبكة WebVPN قاموا في البداية بضرب المجموعة الأساسية أنهم محصورون في المجموعة الأساسية. يمكن تكوين مجموعات WebVPN إضافية على مركز التركيز، ويمكن تخصيص المستخدمين لهم بواسطة خادم RADIUS مع تعداد السمة 25 مع ***OU=groupName*** . راجع قفل المستخدمين في مجموعة مركز VPN 3000 باستخدام خادم RADIUS للحصول على شرح أكثر تفصيلا.

فشل مصادقة المستخدم مقابل Active Directory

في خادم Active Directory، من علامة التبويب "حساب" الخاصة بخصائص المستخدم الذي تعرض للفشل، يمكنك مشاهدة خانة الاختيار هذه:

[x] لا تتطلب مصادقة مسبقة

إذا تم إلغاء تحديد خانة الاختيار هذه، **فتحقق منها**، وحاول المصادقة مرة أخرى مع هذا المستخدم.

معلومات ذات صلة

- مركزات Cisco VPN 3000 Series
- أجهزة Cisco VPN 3002 العميلة
- مفاوضة IPSec/بروتوكولات IKE
- صفحة دعم RADIUS (خدمة مصادقة طلب اتصال المستخدم البعيد)
- خدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS)
- 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).