L2TP عبر IPsec بين مركز Windows 2000 و VPN 3000 باستخدام مثال تكوين الشهادات الرقمية

المحتويات

المقدمة

يوضح هذا المستند الإجراء بالتفصيل المستخدم للاتصال بمركز VPN 3000 من عميل Windows 2000 باستخدام العميل المدمج L2TP/IPSec. من المفترض أن تستخدم الشهادات الرقمية (المرجع المصدق الجذر المستقل (CA) بدون بروتوكول تسجيل الشهادة (CEP)) لمصادقة إتصالك بموجه الشبكة الخاصة الظاهرية (VPN). يستخدم هذا المستند خدمة ترخيص Microsoft للتوضيح. ارجع إلى موقع Microsoft على الويب للحصول على وثائق حول كيفية تكوينه.

ملاحظة: هذا مثال فقط لأن مظهر شبكات Windows 2000 يمكن أن يتغير.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

المعلومات الواردة في هذا المستند خاصة بسلسلة مركز VPN 3000 من Cisco.

الأهداف

في هذا الإجراء، تكمل الخطوات التالية:

1. الحصول على شهادة جذر.
2. الحصول على شهادة هوية للعميل.
3. قم بإنشاء اتصال ب VPN 3000 بمساعدة معالج اتصال الشبكة.
4. قم بتكوين مركز VPN 3000.

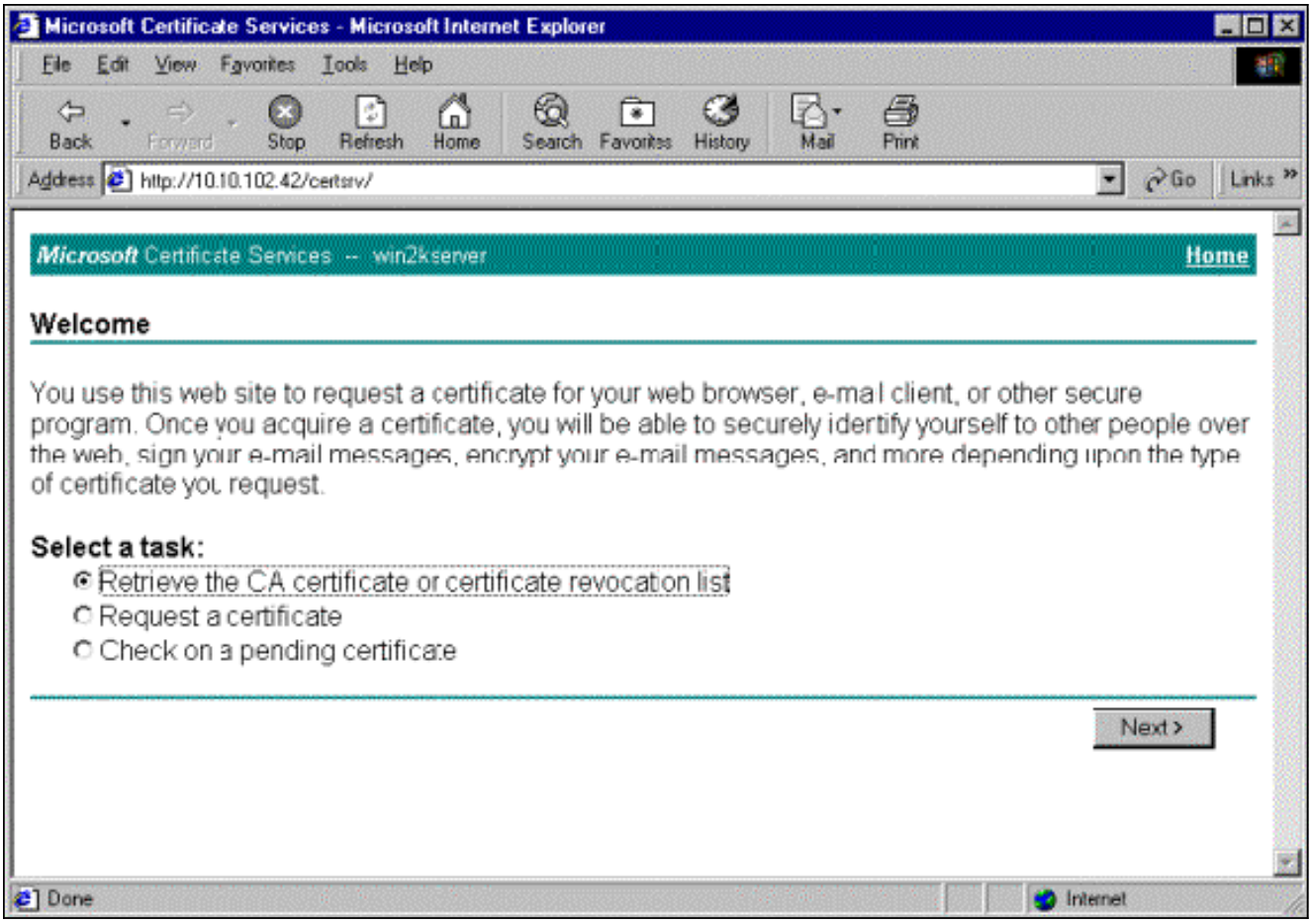
الاصطلاحات

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

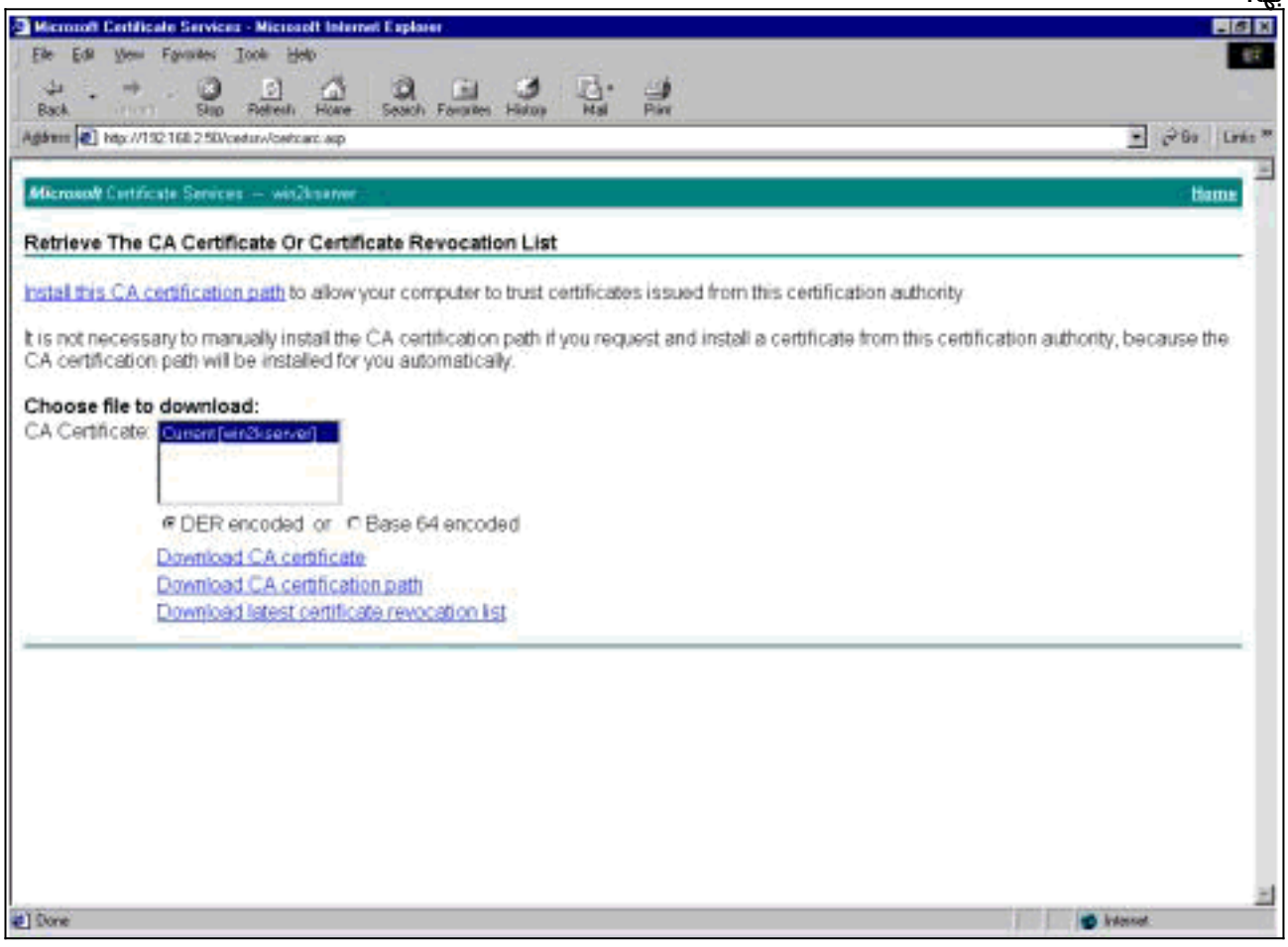
الحصول على شهادة جذر

أكمل هذه التعليمات للحصول على شهادة جذر:

1. افتح نافذة مستعرض واكتب في عنوان URL لهيئة شهادة Microsoft (عادة http://servername أو عنوان IP الخاص ب CA/certsrv).نافذة الترحيب الخاصة باسترداد الشهادات وطلبات العرض.
2. في نافذة الترحيب ضمن تحديد مهمة، أختر **إسترداد شهادة CA أو قائمة إلغاء الشهادة** وانقر فوق **التالي**.



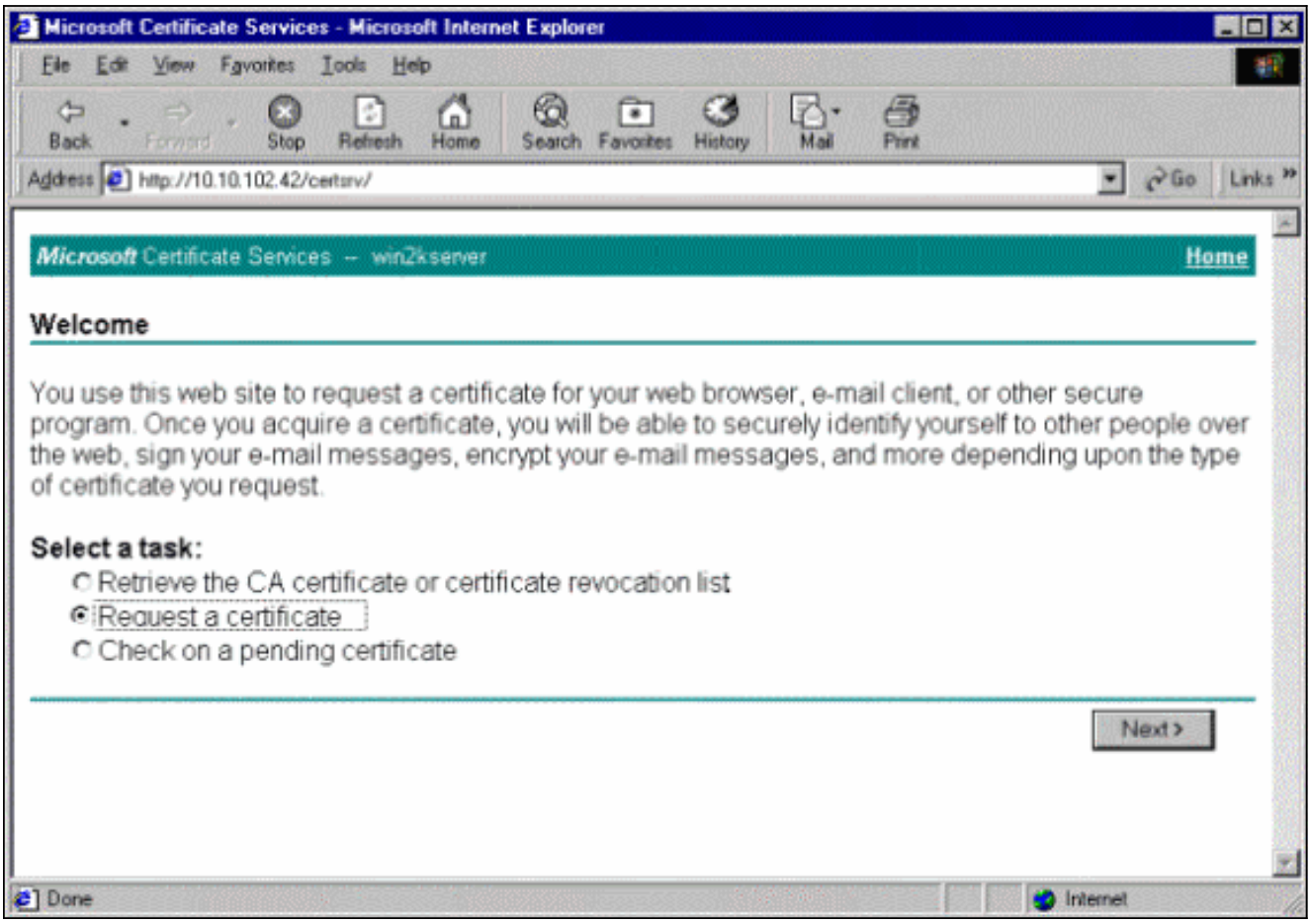
3. من نافذة قائمة إسترداد شهادة المرجع المصدق أو إبطال الشهادة، انقر على **تثبيت مسار شهادة المرجع المصدق هذا** في الركن الأيسر.يؤدي ذلك إلى إضافة شهادة المرجع المصدق إلى مخزن مراجع الشهادات الجذر الموثوق بها. هذا يعني أن أي شهادات تصدر عن هذا المرجع المصدق لهذا العميل موثوق بها.



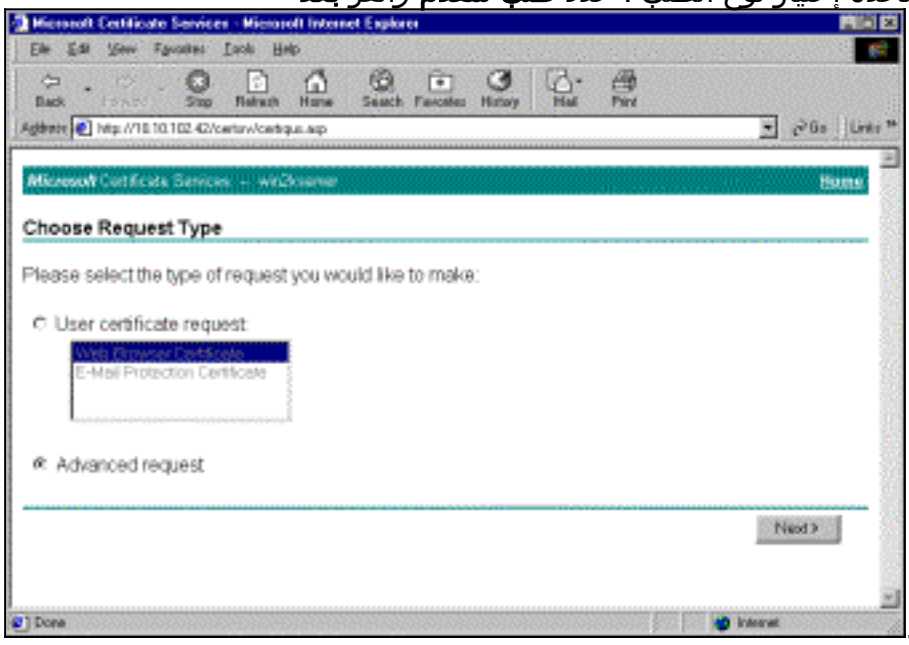
الحصول على شهادة هوية للعميل

أكمل الخطوات التالية للحصول على شهادة هوية للعميل:

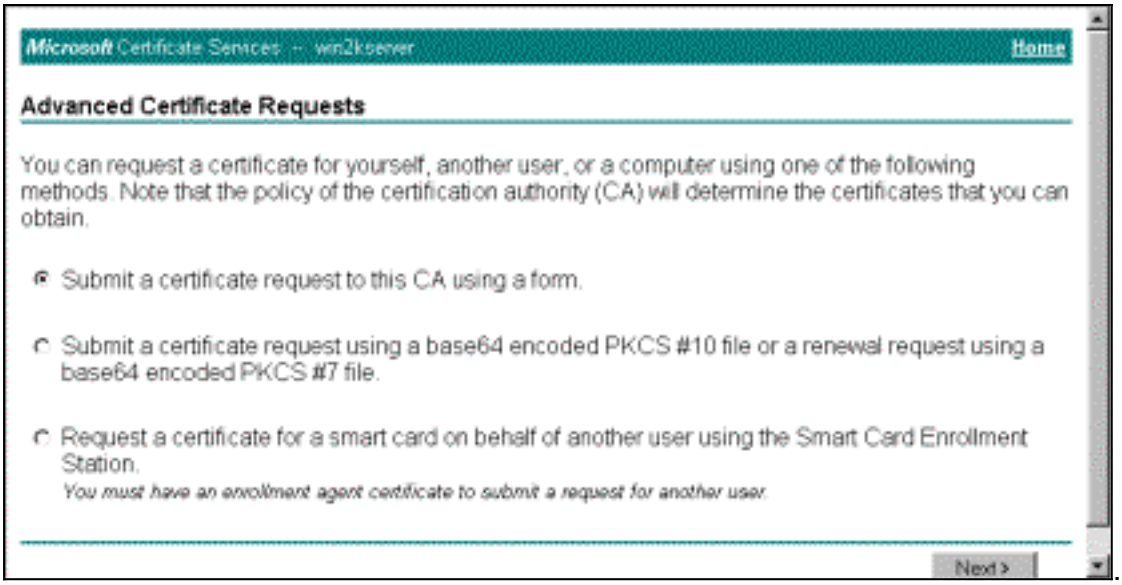
1. افتح نافذة متصفح وأدخل عنوان URL لهيئة شهادة Microsoft (عادة http://servername أو عنوان IP الخاص ب CA/CERTSRV).نافذة الترحيب الخاصة باسترداد الشهادات وطلبات العرض.
2. من نافذة الترحيب، تحت تحديد مهمة، أختر **طلب شهادة**، وانقر **بعد ذلك**.



3. من نافذة إختيار نوع الطلب ، حدد **طلب متقدم** وانقر **بعد ذلك**.

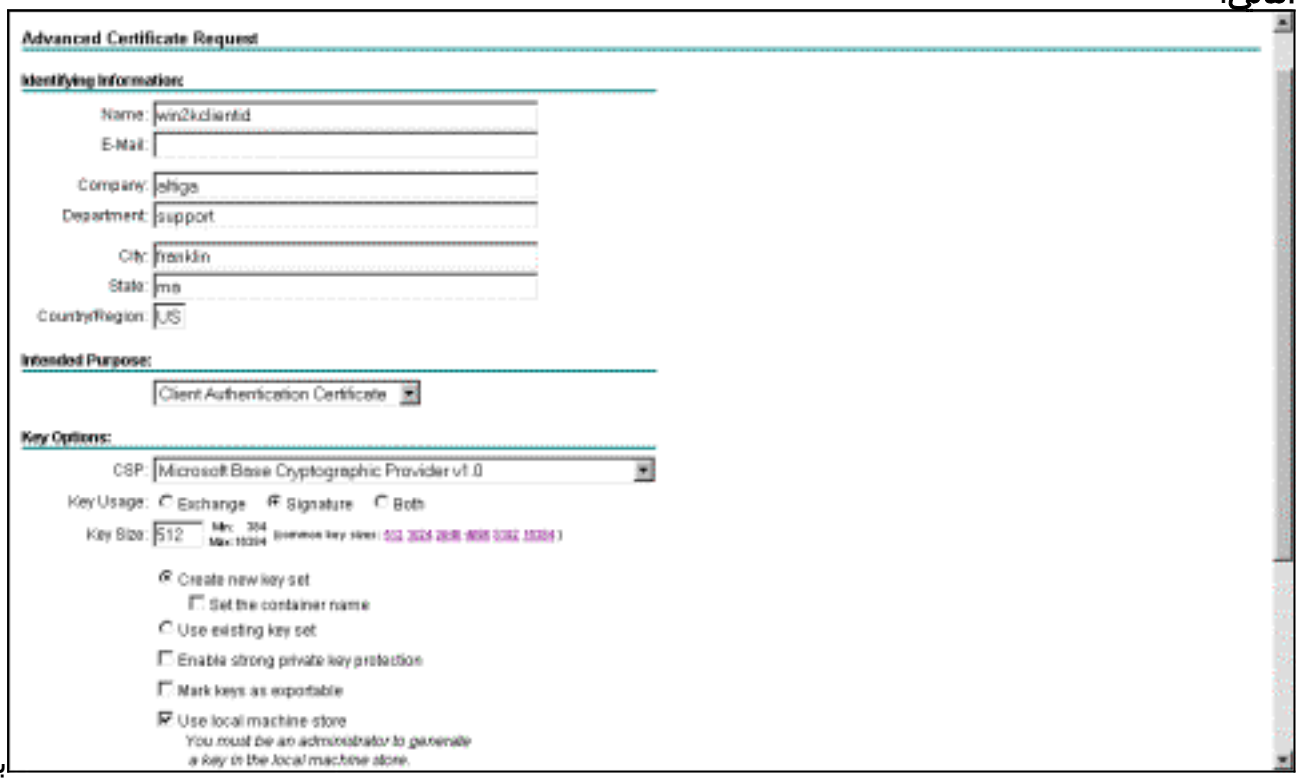


4. من نافذة طلبات الشهادات المتقدمة، حدد **إرسال طلب شهادة إلى المرجع المصدق هذا باستخدام**

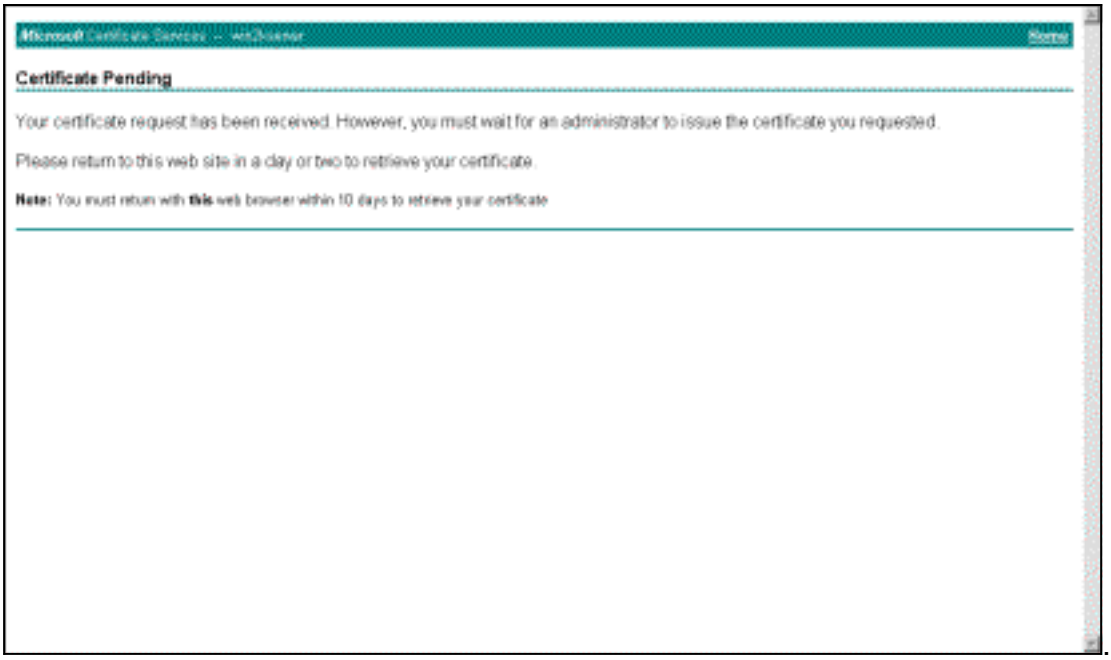


نموذج.

5. تعبئة الحقول كما في هذا المثال.يجب أن تتوافق قيمة الوكالة (الوحدة التنظيمية) مع المجموعة المكونة على مركز الشبكة الخاصة الظاهرية (VPN). لا تحدد حجم مفتاح أكبر من 1024. تأكد من تحديد خانة الاختيار **لاستخدام مخزن الجهاز المحلي**. عندما تنتهي، انقر **التالي**.

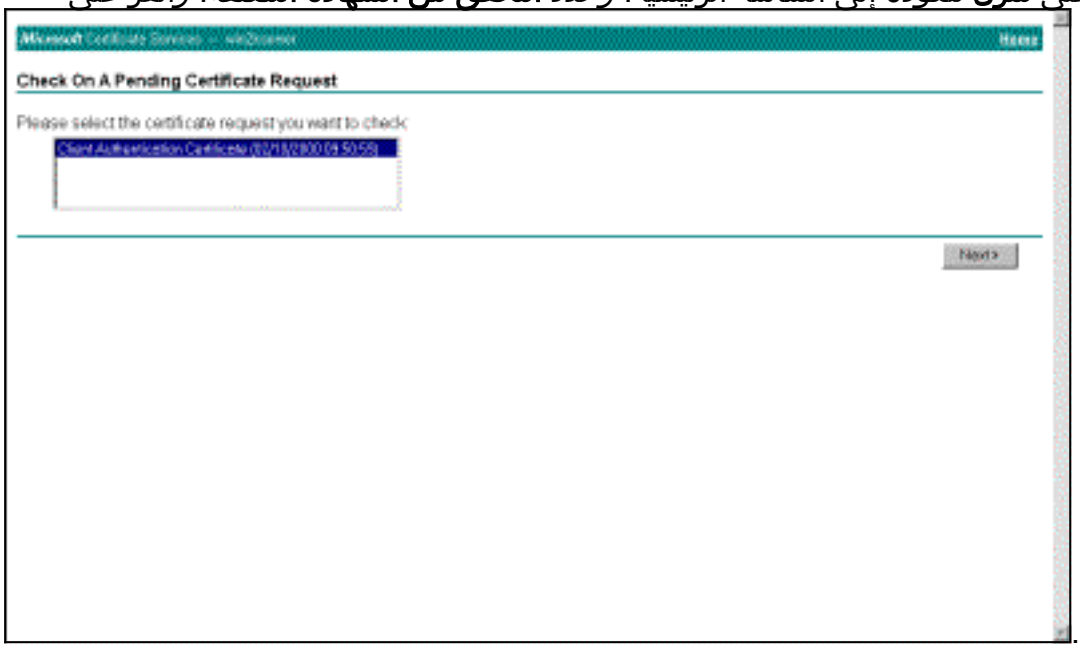


بنا ء على كيفية تكوين خادم CA، تظهر هذه النافذة أحيانا. إذا كان كذلك، اتصل بمسؤول



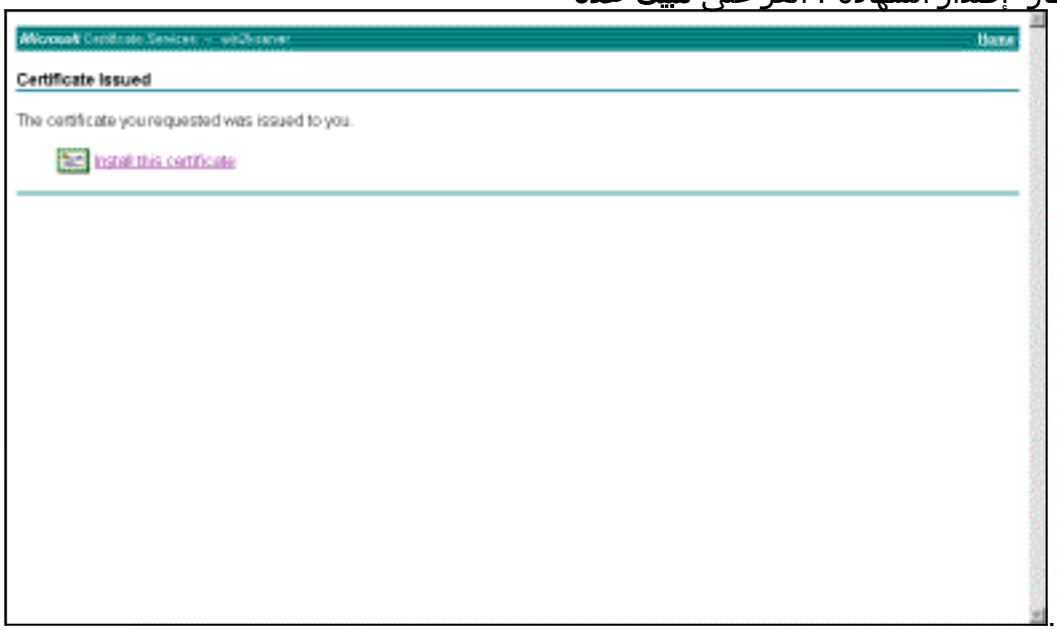
CA.

6. انقر على **منزل** للعودة إلى الشاشة الرئيسية، وحدد **التحقق من الشهادة المعلقة**، وانقر على



التالي.

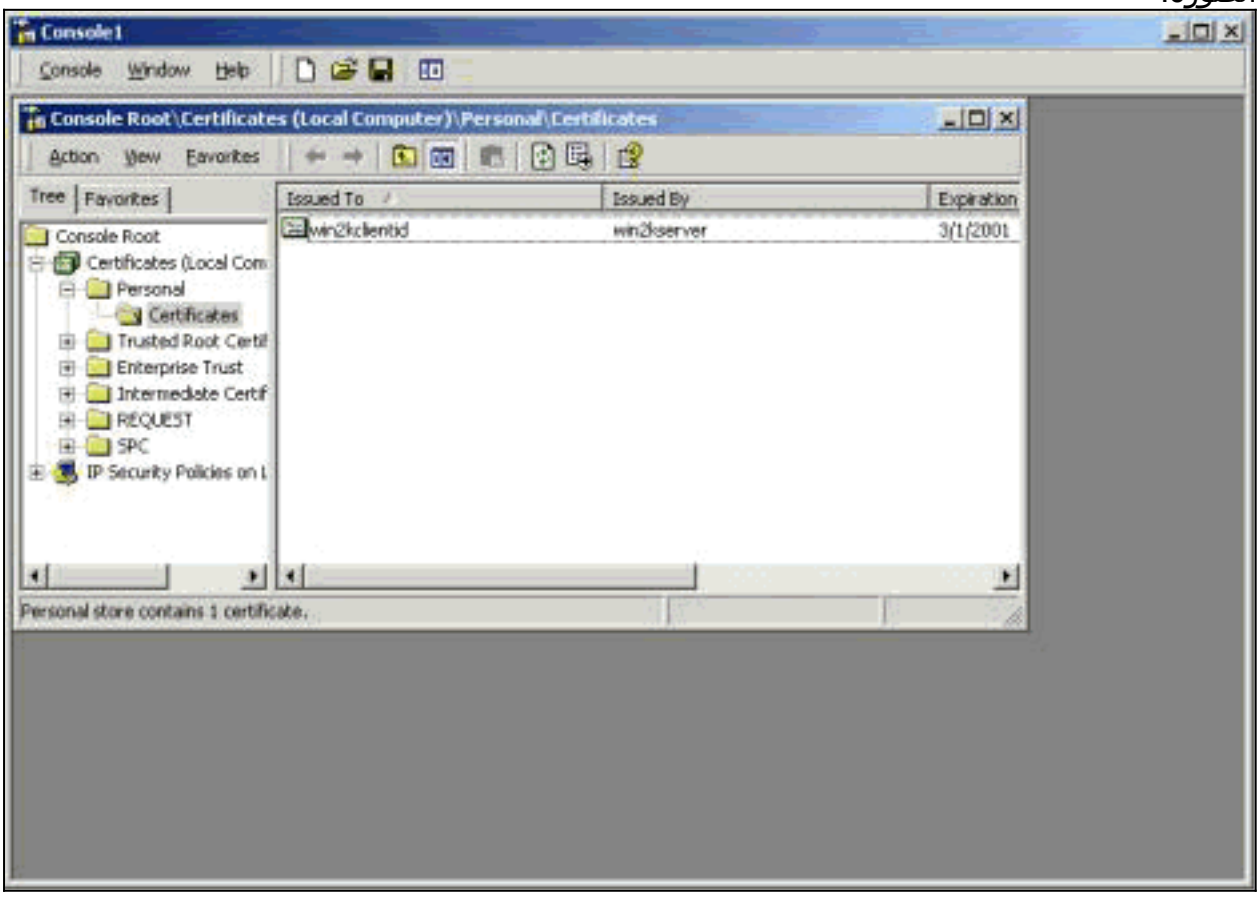
7. في الإطار "إصدار الشهادة"، انقر على **تثبيت هذه**



الشهادة.

8. لعرض شهادة العميل الخاصة بك، حدد **Start > Run**، وقم بتنفيذ وحدة تحكم الإدارة (MMC) من Microsoft.

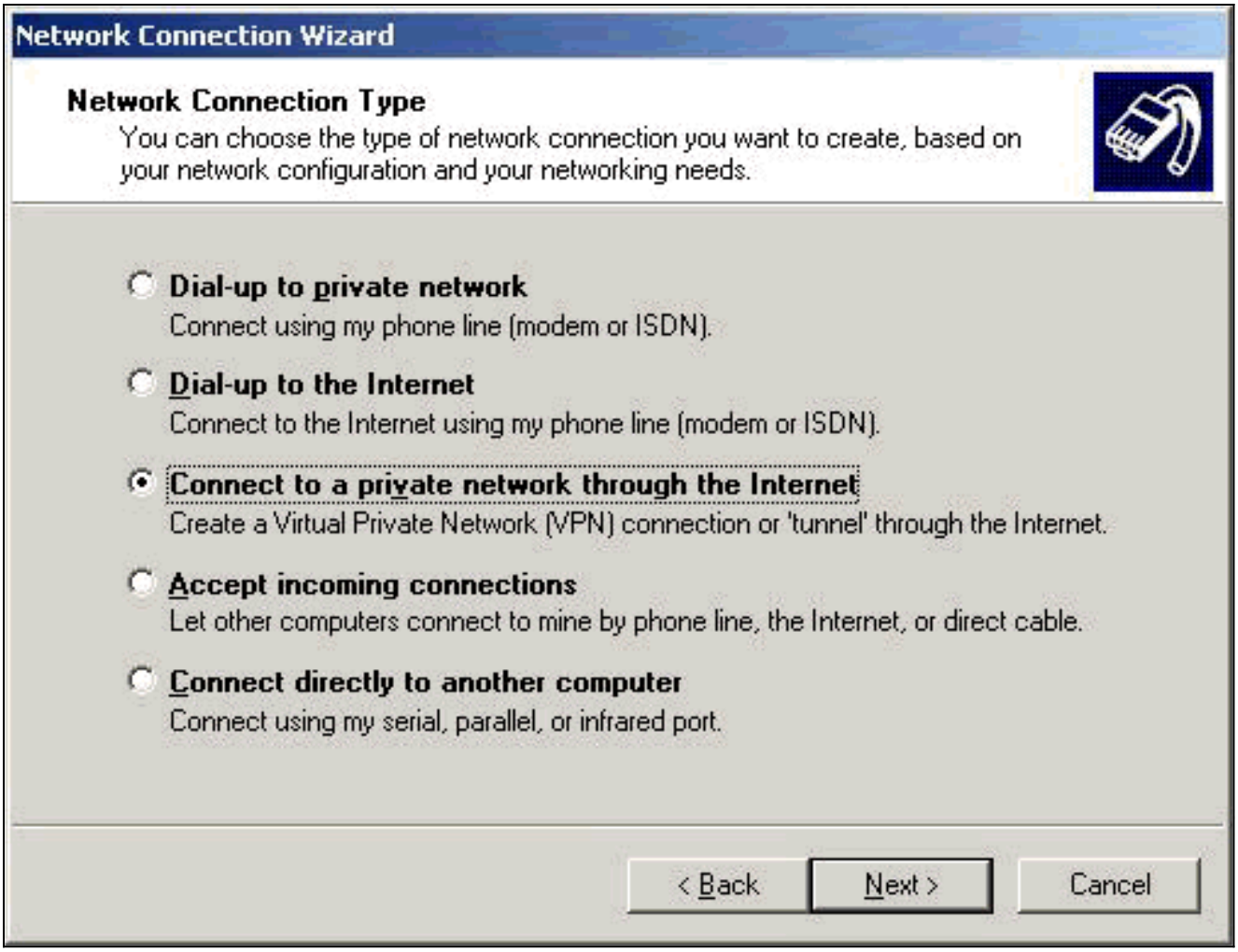
9. انقر فوق **وحدة التحكم** واختر **إضافة/إزالة الأداة الإضافية**.
10. انقر على **إضافة** واختر **شهادة** من القائمة.
11. عندما تظهر نافذة تسألك عن نطاق الشهادة، أختر **حساب الكمبيوتر**.
12. تحقق من وجود شهادة خادم CA تحت مراجع التصديق الجذر الموثوق بها. تحقق أيضا من أن لديك شهادة عن طريق تحديد **جذر وحدة التحكم > شهادة (كمبيوتر محلي) > شخصي>شهادات**، كما هو موضح في هذه الصورة.



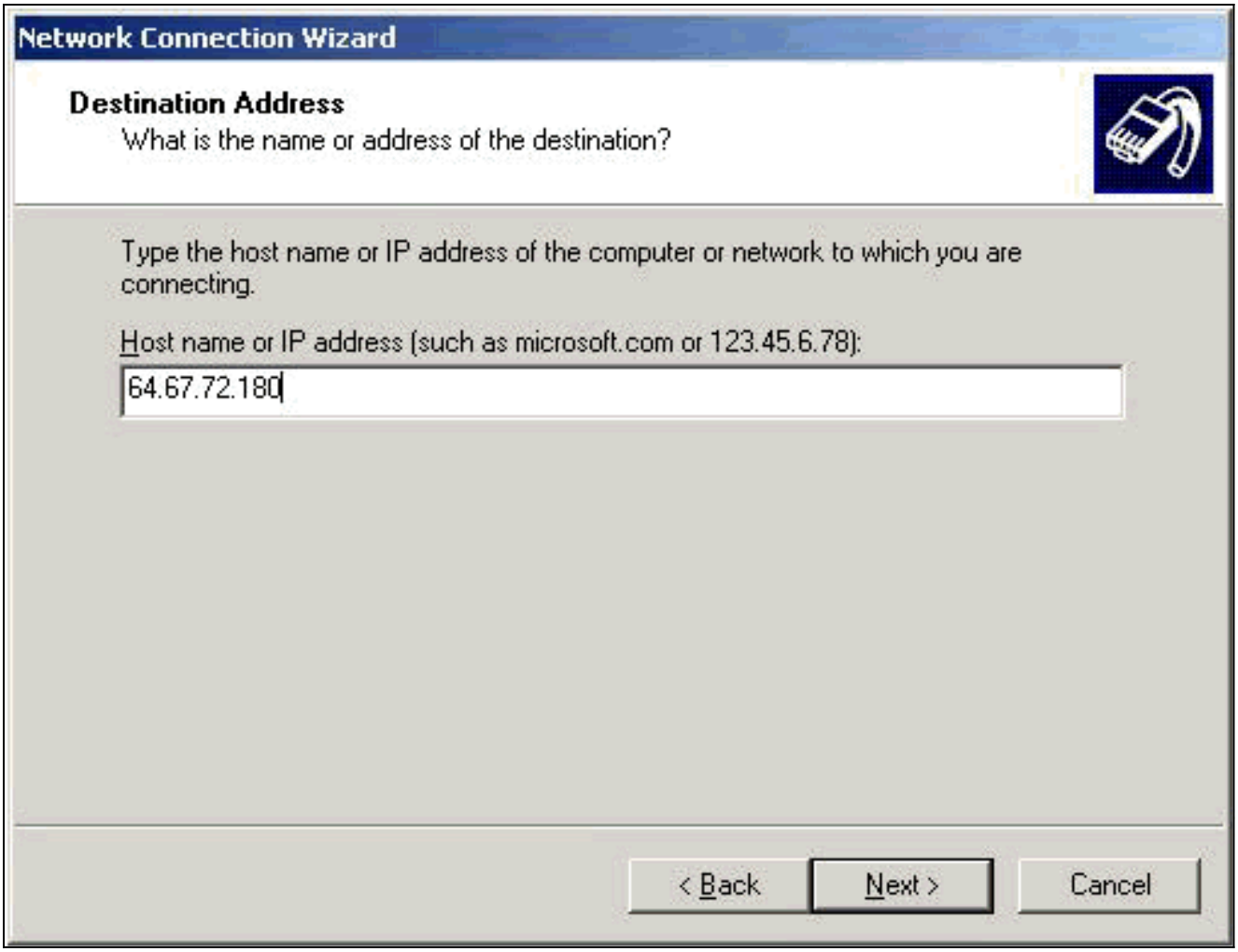
إنشاء اتصال ب VPN 3000 باستخدام معالج اتصال الشبكة

أتمت هذا إجراء in order to خلقت توصيل إلى ال VPN 3000 مع مساعدة من الشبكة توصيل مرشد:

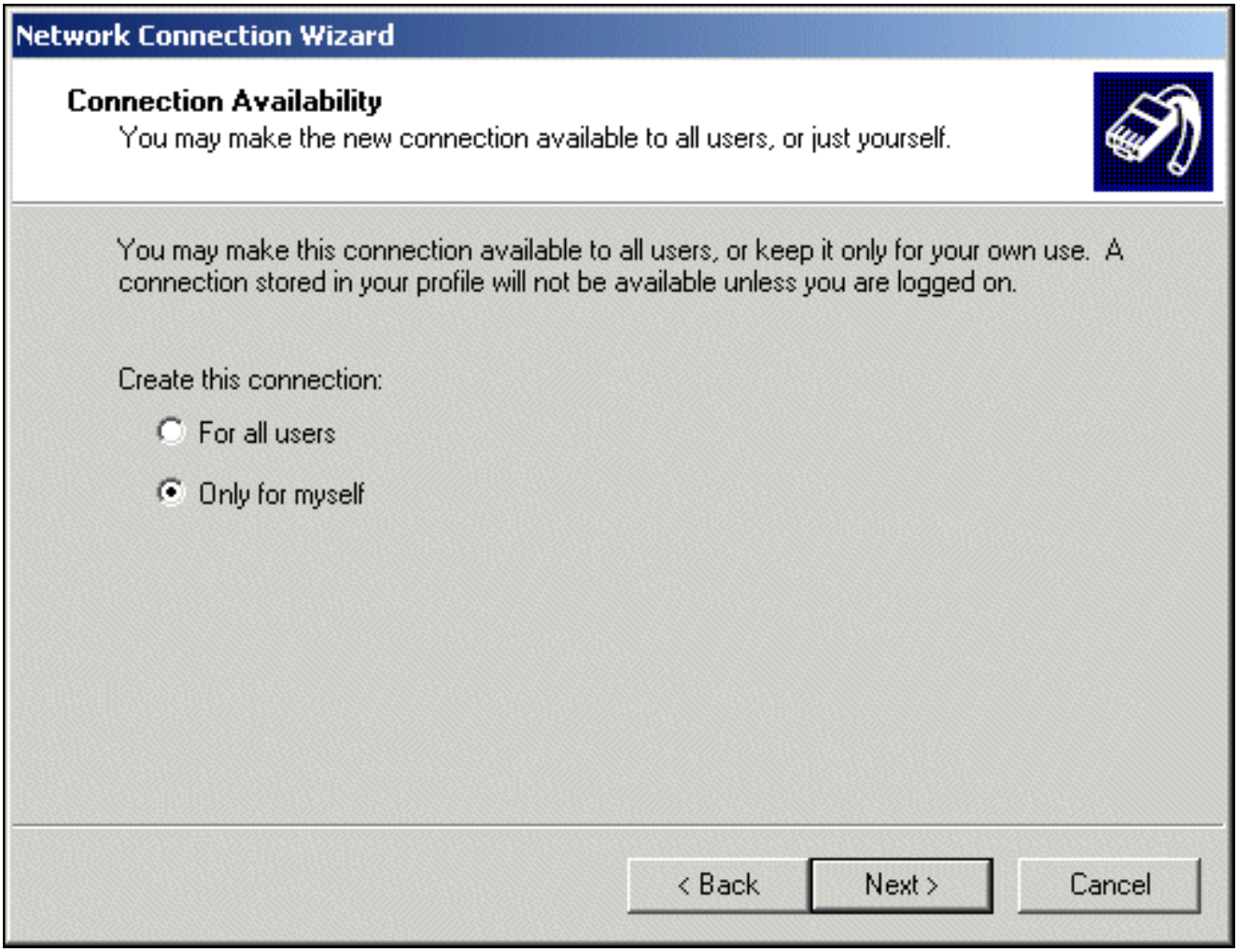
1. انقر بزر الماوس الأيمن على **مواضع شبكتي**، واختر **خصائص**، ثم انقر على **إجراء توصيل جديد**.
2. من نافذة "نوع اتصال الشبكة"، أختر **الاتصال بشبكة خاصة من خلال الإنترنت** ثم انقر على **التالي**.



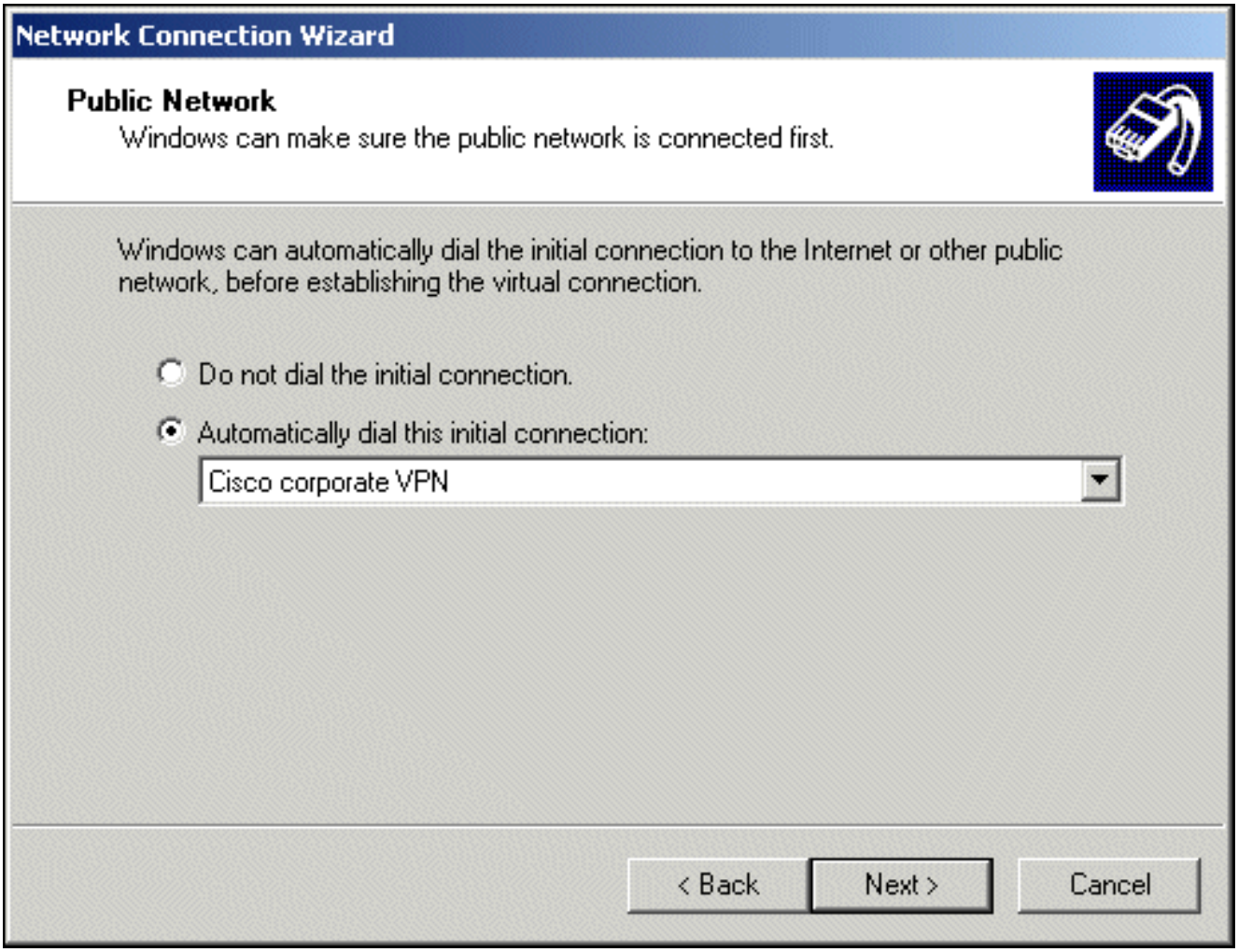
3. دخلت المضيف إسم أو عنوان من القارن عام من ال VPN مركز، وطقطقة **بعد ذلك**.



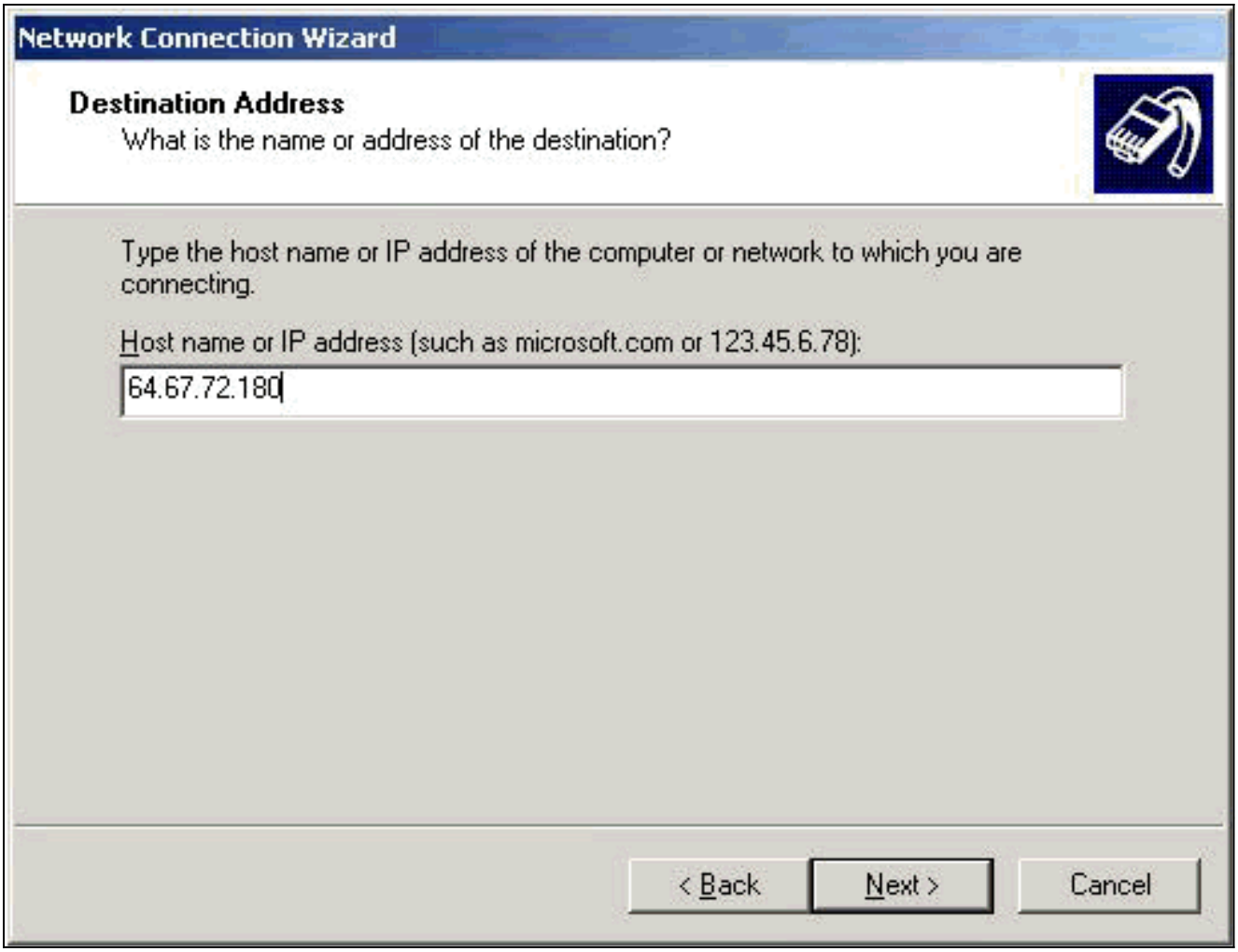
4. في إطار "توفر الاتصال"، حدد **لنفسي فقط** وانقر فوق **التالي**.



5. في نافذة الشبكة العامة، حدد ما إذا كنت تريد طلب الاتصال الأولي (حساب ISP) تلقائيا.

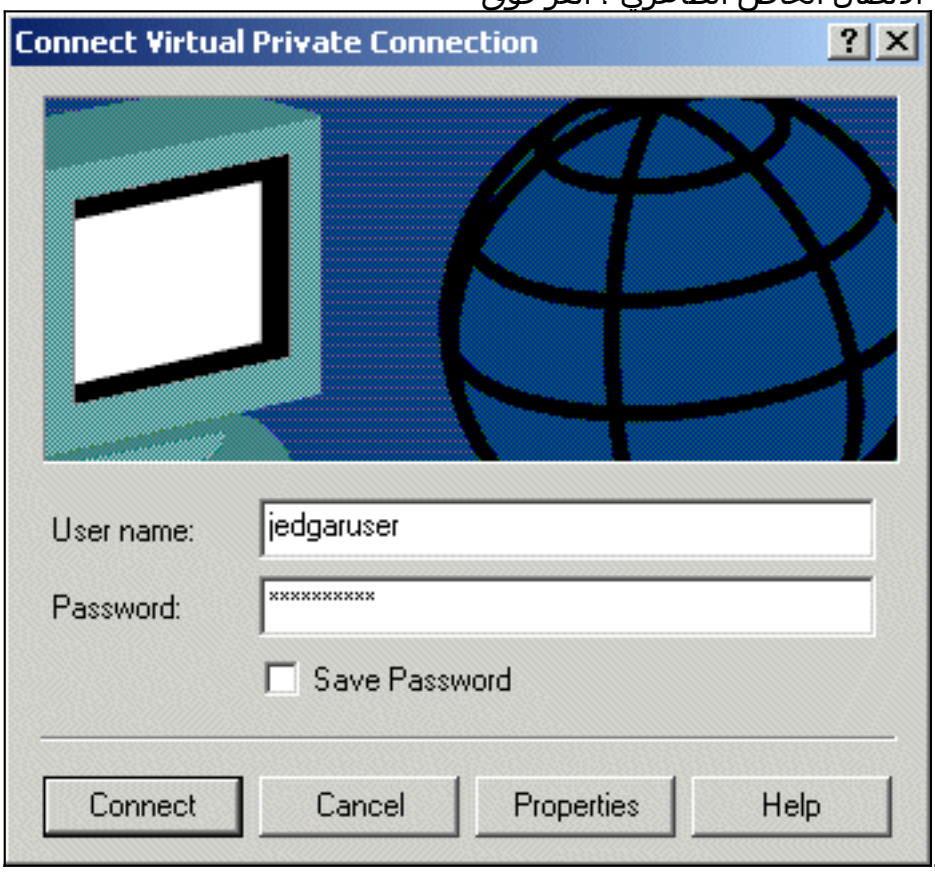


6. دخلت على الغاية عنوان شاشة، المضيف إسم أو عنوان من ال VPN 3000 مركز، وطقطقة **بعد ذلك**.

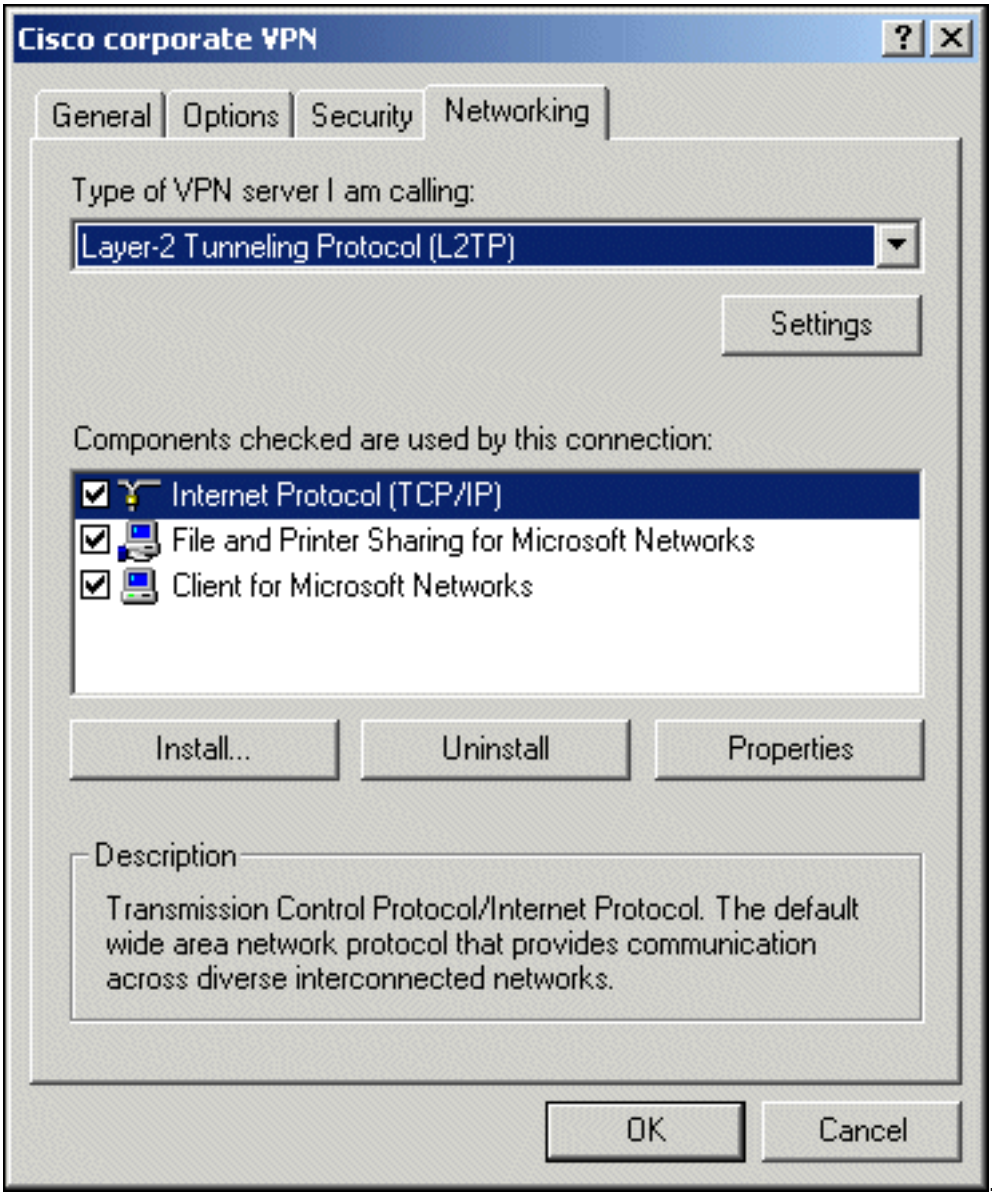


7. في إطار "معالج توصيل الشبكة"، أدخل اسما للاتصال ثم انقر على **إنهاء**.في هذا المثال، يسمى الاتصال "Cisco Corporate VPN".

8. في إطار "الاتصال الخاص الظاهري"، انقر فوق **خصائص**.

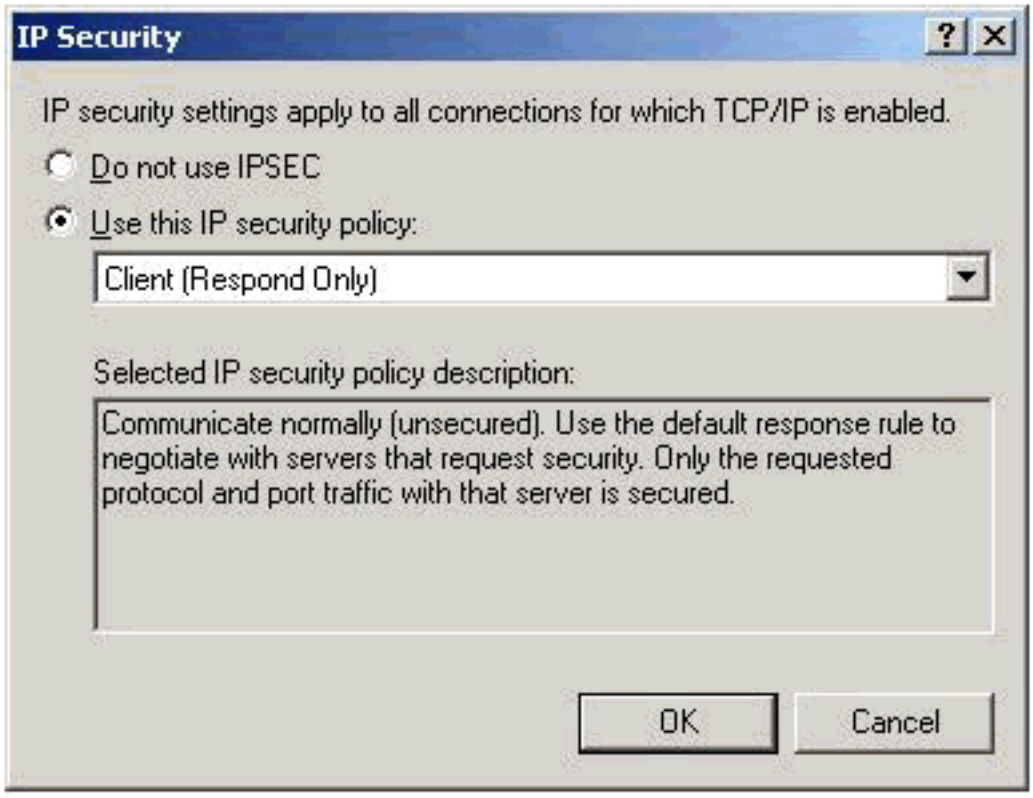


9. في إطار الخصائص، حدد علامة تبويب الشبكة.
10. تحت نوع خادم VPN الذي أتصل به، أختر **L2TP** من القائمة المنسدلة، وقم بإبراز **بروتوكول الإنترنت TCP/IP**، وانقر فوق



خصائص.

11. حدد **متقدم** > **خيارات** > **خصائص**.
12. في نافذة أمان IP، أختر **إستخدام سياسة أمان IP**



هذه.

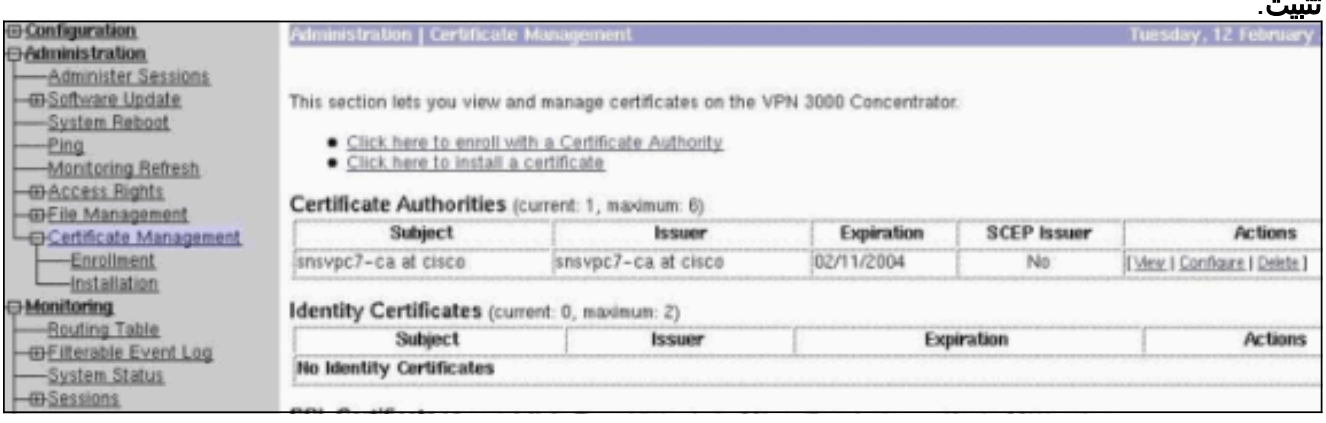
13. أختر نهج **العميل (الاستجابة فقط)** من القائمة المنسدلة، ثم انقر فوق **موافق** عدة مرات حتى تعود إلى شاشة الاتصال.
14. دخلت in order to بدأت توصيل، username وكلمة، وطقطقة **توصيل**.

تكوين مركز VPN 3000

الحصول على شهادة جذر

أتمت هذا steps in order to نلت شهادة جذر ل ال VPN 3000 مركز:

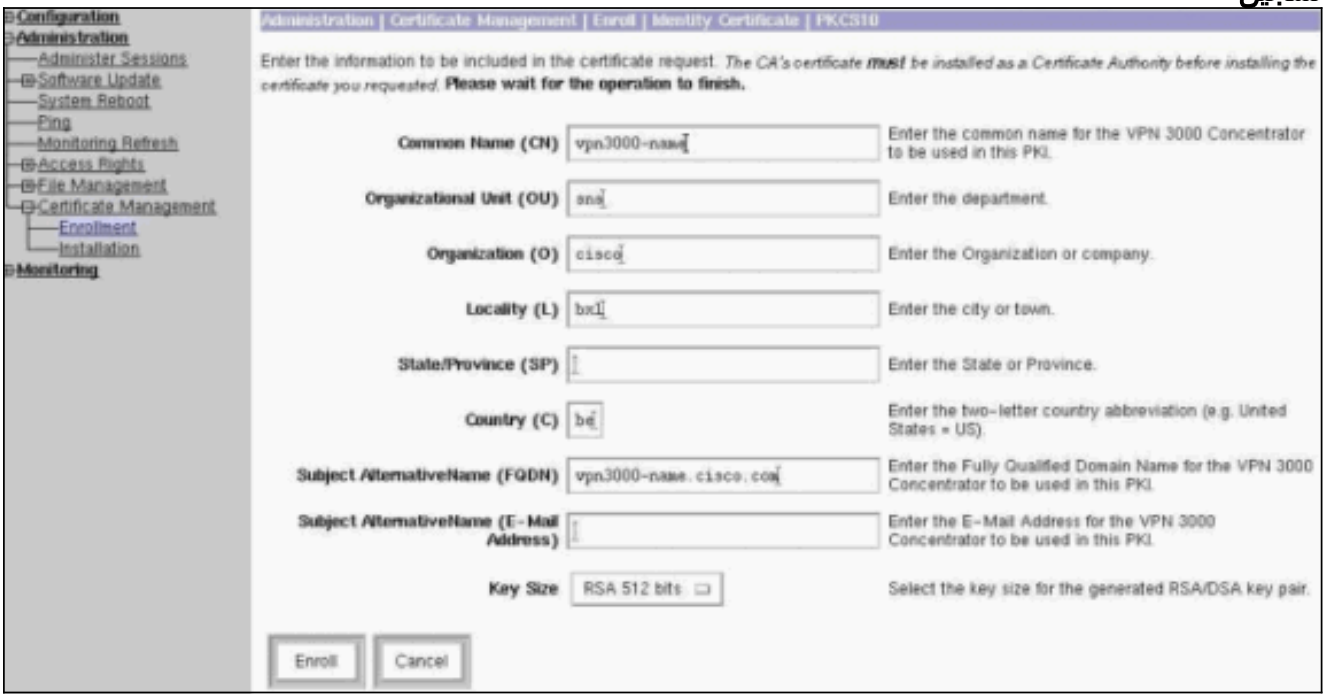
1. قم بتوجيه المستعرض إلى المرجع المصدق (عادة ما يكون http://ip_add_of_ca/certsrv/)، **واسترد شهادة المرجع المصدق أو قائمة إلغاء الشهادة**، وانقر فوق **التالي**.
2. انقر على **تنزيل شهادة المرجع المصدق** واحفظ الملف في مكان ما على القرص المحلي.
3. على مركز VPN 3000، حدد **إدارة > إدارة الشهادات**، وانقر **هنا لتثبيت شهادة** و**تثبيت شهادة CA**.
4. انقر فوق **تحميل الملف من محطة العمل**.
5. انقر **تصفح** وحدد ملف شهادة CA الذي قمت بتنزيله للتو.
6. قم بتمييز اسم الملف وانقر **تثبيت**.



الحصول على شهادة هوية مركز VPN 3000

أتمت هذا steps in order to نلت شهادة هوية ل VPN 3000 Concentrator:

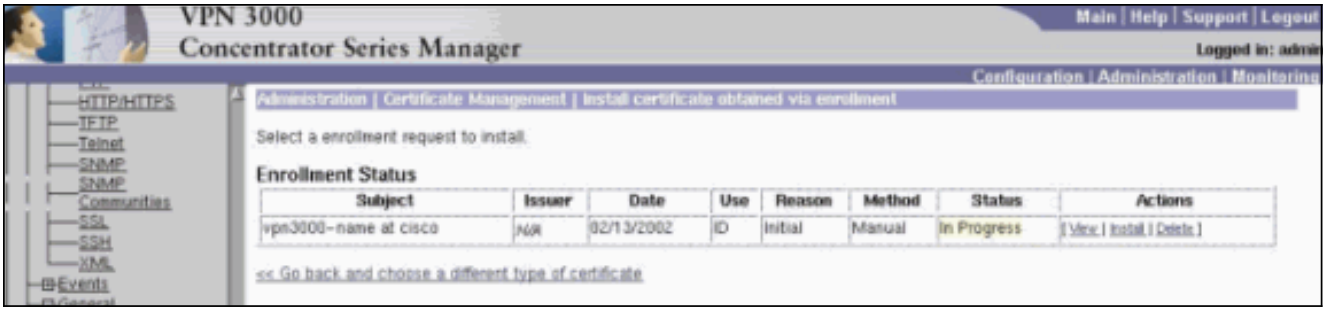
1. حدد **ConfAdministration > إدارة الشهادات > تسجيل > شهادة الهوية**، ثم انقر **تسجيل عبر طلب PKCS10 (يدوي)**. املأ النموذج كما هو موضح هنا وانقر فوق **تسجيل**.



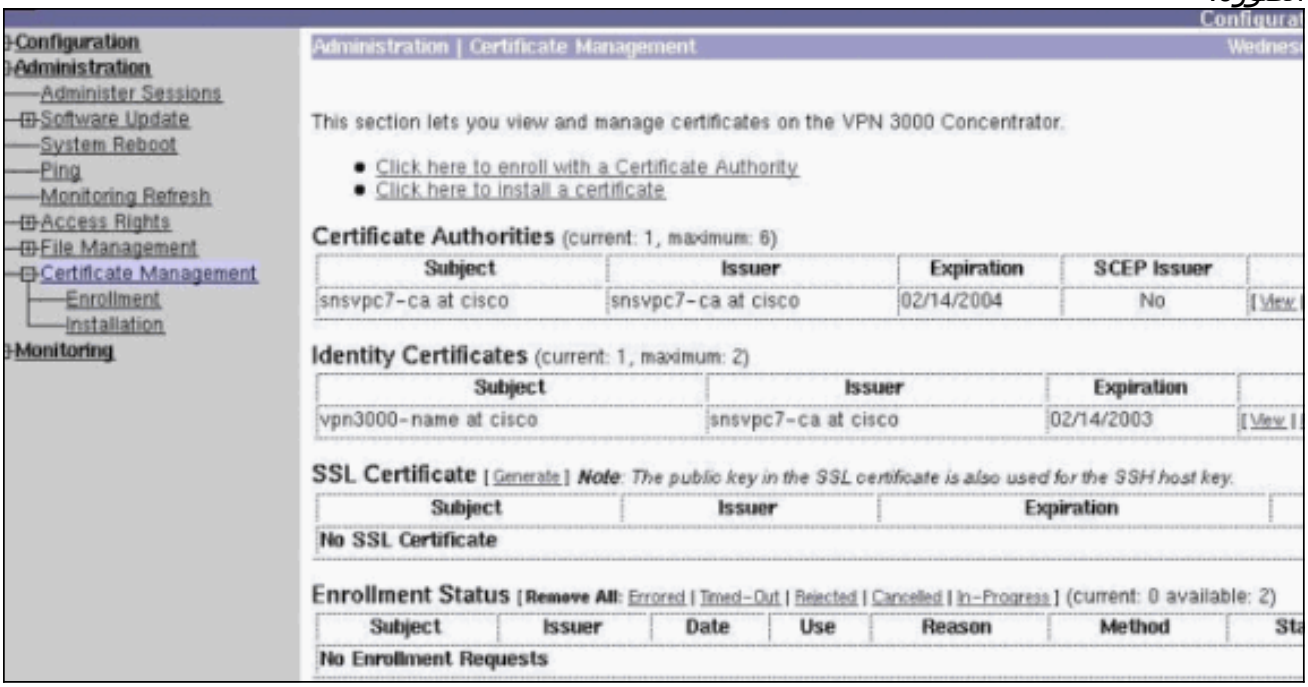
تظهر نافذة المستعرض مع طلب الشهادة. يجب أن يحتوي على نص مشابه لهذا المخرج:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMDAwLW5hbWUxDDAKBgNVBAsTA3Nu
czEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAcTA2J4bDELMAkGA1UEBhMCYmUwWjAN
BgkqhkiG9w0BAQEFAANJADBGAkEAx7K+pvE004qILNNw3kPVWXrdlqZV4yeOIPdh
C8/V5Yuqq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG
SIb3DQEJDjElMCMwIQYDVR0RBBowGIIWdnBuMzAwMC1uYW1lLmNpc2NvLmNvbTAN
BgkqhkiG9w0BAQQFAANBABzcG3IKaWnDLFtrNf1QDi+D7w8dxPu74b/BRHn9fsKI
=X6+X0ed0EuEgm1/2nfj8Ux0nV5F/c5wukUfysMmJ/ak
-----END NEW CERTIFICATE REQUEST-----
```

2. قم بتوجيه المستعرض إلى خادم CA الخاص بك، وفحص **طلب شهادة**، وانقر فوق **التالي**.
3. تحقق من **الطلب المتقدم**، انقر **التالي**، وحدد **إرسال طلب شهادة باستخدام ملف PKCS #10 مرمز للأساس64 أو طلب تجديد باستخدام ملف PKCS #7 مرمز للأساس 64**.
4. انقر فوق **Next (التالي)**. قص ولصق نص طلب الشهادة الظاهر سابقا في منطقة النص. انقر على **إرسال**.
5. استنادا إلى كيفية تكوين خادم CA، يمكنك النقر فوق **تنزيل شهادة CA**. أو بمجرد إصدار الشهادة من المرجع المصدق، ارجع إلى خادم المرجع المصدق وتحقق **من الشهادة المعلقة**.
6. انقر فوق **التالي**، ثم حدد طلبك، ثم انقر فوق **التالي** مرة أخرى.
7. انقر على **تنزيل شهادة المرجع المصدق**، واحفظ الملف على القرص المحلي.
8. على مركز VPN 3000، حدد **إدارة > إدارة الشهادات > تثبيت**، وانقر **تثبيت الشهادة التي تم الحصول عليها من خلال التسجيل**.يمكنك عندئذ عرض طلبك المعلق بالحالة "قيد التقدم" كما هو الحال في هذه الصورة.



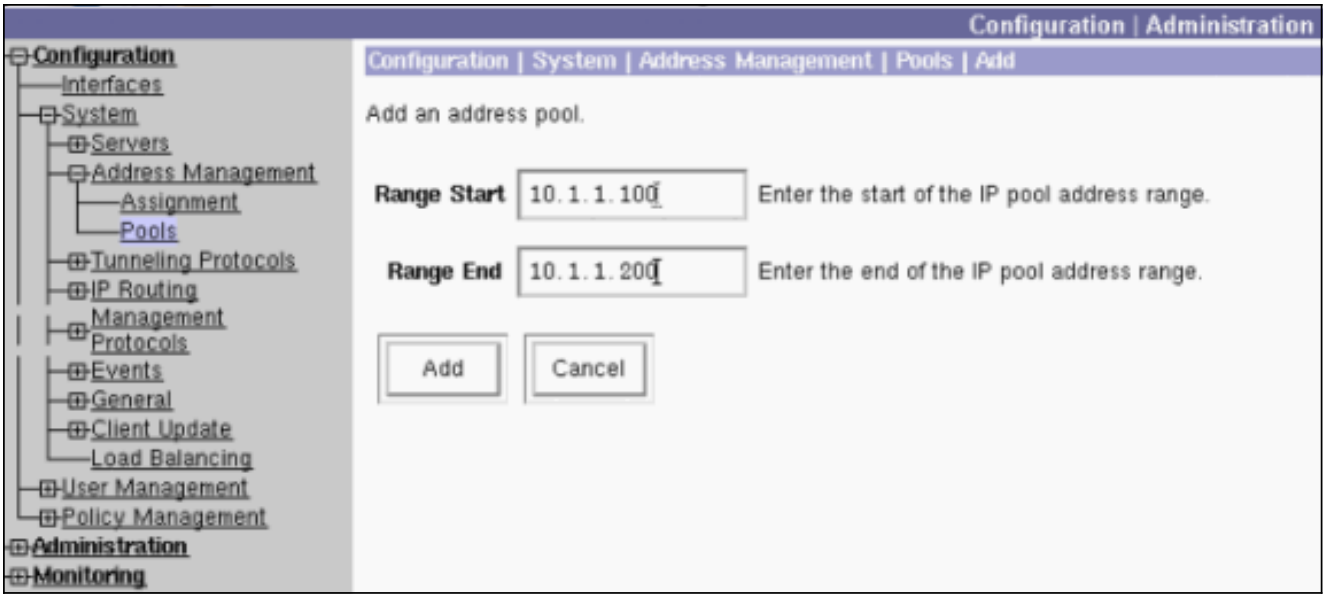
9. انقر فوق **تثبيت**، يتبعه **تحميل الملف من محطة العمل**.
10. انقر على **إستعراض** وحدد الملف الذي يحتوي على شهادتك التي تم إصدارها من قبل المرجع المصدق.
11. قم بتمييز اسم الملف وانقر **تثبيت**.
12. حدد **إدارة > إدارة الشهادات**. تظهر شاشة مماثلة لهذه الصورة.



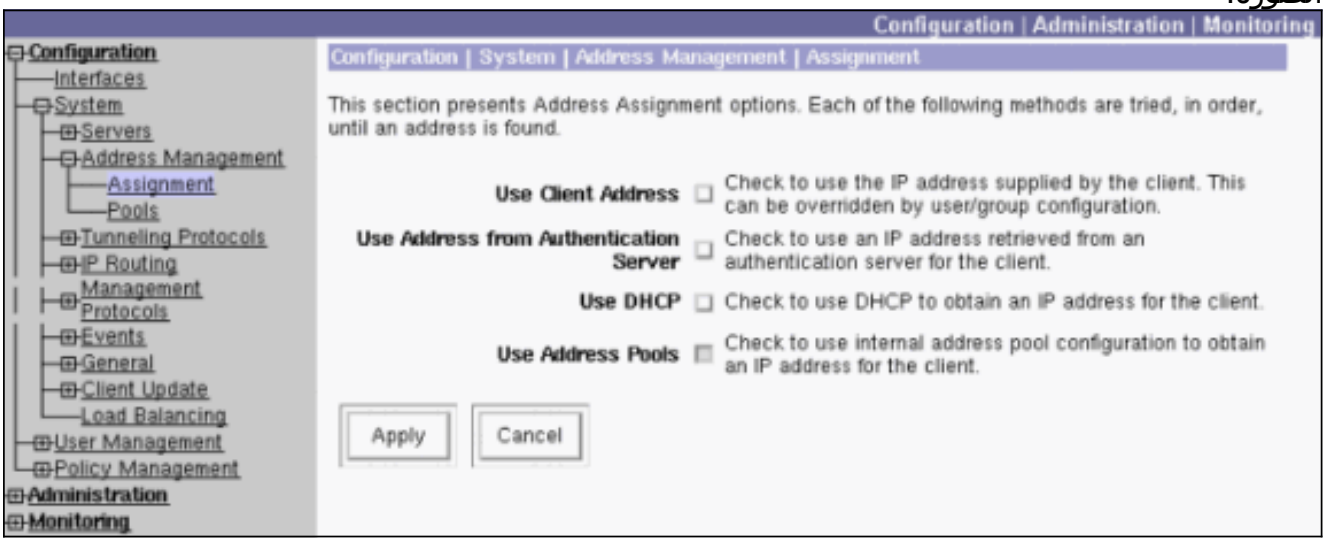
تكوين تجمع للعملاء

أتمت هذا إجراء in order to شكلت بركة للعملاء:

1. من أجل تخصيص نطاق متاح من عناوين IP، قم بتوجيه متصفح إلى الواجهة الداخلية لمركز VPN 3000 وحدد **تكوين > نظام > إدارة العناوين > تجمعات > إضافة**.
2. حدد نطاق من عناوين IP لا تتعارض مع أي أجهزة أخرى على الشبكة الداخلية، وانقر فوق **إضافة**.



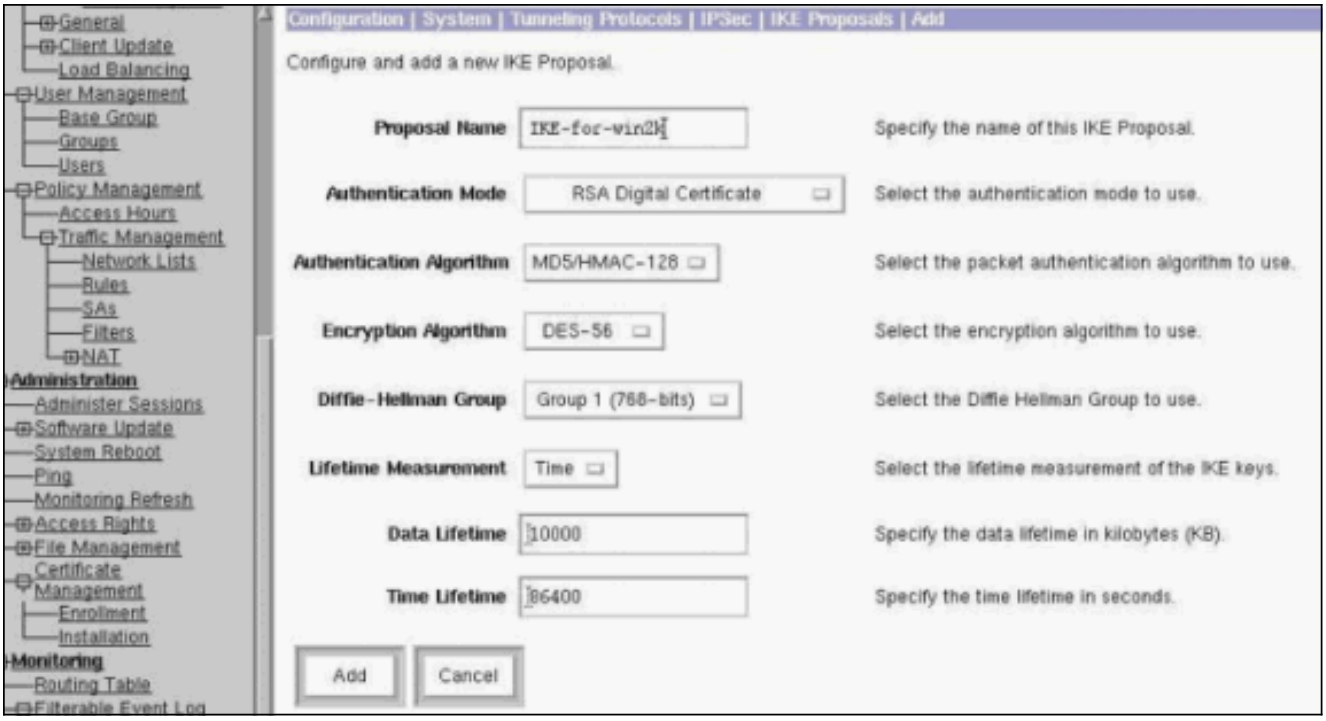
3. لتبليغ مركز VPN 3000 لاستخدام التجمع، حدد **التكوين > النظام > إدارة العناوين > التعيين**، حدد مربع **إستخدام تجمعات العناوين**، وانقر **تطبيق**، كما هو الحال في هذه الصورة.



تكوين اقتراح IKE

أكمل الخطوات التالية لتكوين اقتراح IKE:

1. حدد **تكوين > نظام > بروتوكولات الاتصال النفقي > IPSec > مقترحات IKE**، انقر فوق **إضافة** وحدد المعلمات، كما هو موضح في هذه الصورة.



2. انقر فوق **إضافة**، قم بتمييز العرض الجديد في العمود الأيمن، وانقر فوق **تنشيط**.

تكوين SA

أكمل هذا الإجراء لتكوين اقتران الأمان (SA):

1. حدد **تشكيل > إدارة السياسة > إدارة حركة المرور > SA** وانقر **ESP-L2TP-TRANSPORT**.إذا لم تكن sa هذه متوفرة أو إذا كنت تستخدمها لغرض آخر، فقم بإنشاء sa جديد مماثل لهذا الغرض. الإعدادات المختلفة ل SA مقبولة. قم بتغيير هذه المعلمة استنادا إلى نهج الأمان.
2. حدد الشهادة الرقمية التي قمت بتكوينها سابقا تحت القائمة المنسدلة **الشهادة الرقمية**. حدد مقترح تبادل مفتاح الإنترنت (IKE-**for-win2k**).**ملاحظة:** هذا غير إلزامي. عند اتصال عميل L2TP/IPSec بموجه تركيز الشبكة الخاصة الظاهرية (VPN)، يتم تجربة جميع اقتراحات IKE التي تم تكوينها أسفل العمود النشط **لتكوين** الصفحة **> النظام > بروتوكولات الاتصال النفقي > IPSec > مقترحات IKE** بالترتيب.تظهر هذه الصورة التكوين المطلوب ل SA:

تكوين المجموعة والمستخدم

أكمل هذا الإجراء لتكوين المجموعة والمستخدم:

1. حدد **تكوين > إدارة المستخدم > مجموعة أساسية**.
2. تحت علامة التبويب "عام"، تأكد من التحقق من **L2TP عبر IPSec**.
3. تحت علامة التبويب IPSec، حدد SA **ESP-L2TP-Transport**.
4. تحت علامة التبويب PPTP/L2TP، قم بإلغاء تحديد جميع خيارات **تشفير L2TP**.
5. حدد **تشكيل > إدارة المستخدم > مستخدمون** وانقر **إضافة**.
6. أدخل الاسم وكلمة المرور اللذين تستخدمهما للاتصال من عميل Windows 2000. تأكد من تحديد **مجموعة أساسية** ضمن تحديد المجموعة.
7. تحت علامة التبويب "عام"، تحقق من **بروتوكول L2TP عبر** بروتوكول **IPSec** للاتصال النفقي.
8. تحت علامة التبويب IPSec، حدد SA **ESP-L2TP-Transport**.
9. تحت علامة التبويب PPTP/L2TP، قم بإلغاء تحديد جميع خيارات **تشفير L2TP**، وانقر **إضافة**.يمكنك الآن الاتصال باستخدام تعليمات عميل Windows 2000 من L2TP/IPSec.**ملاحظة:** لقد أخترت تكوين المجموعة الأساسية لقبول اتصال L2TP/IPSec البعيد. كما يمكن تكوين مجموعة تتطابق مع حقل الوحدة التنظيمية (OU) في SA لقبول الاتصال الوارد. التكوين مماثل.

معلومات التصحيح

```
SEV=8 IKEDBG/0 RPT=3868 10.48.66.76 12:47:24.430 02/15/2002 269
                    :Mismatched attr types for class DH Group
                                  Rcv'd: Oakley Group 2
                                  Cfg'd: Oakley Group 7

SEV=8 IKEDBG/0 RPT=3869 10.48.66.76 12:47:24.430 02/15/2002 271
                :Phase 1 failure against global IKE proposal # 16
```

```
                    :Mismatched attr types for class DH Group
                                    Rcv'd: Oakley Group 2
                                    Cfg'd: Oakley Group 1

SEV=8 IKEDBG/0 RPT=3870 10.48.66.76 12:47:24.430 02/15/2002 274
                Proposal # 1, Transform # 2, Type ISAKMP, Id IKE
                                 :Parsing received transform
              :Phase 1 failure against global IKE proposal # 1
               :Mismatched attr types for class Encryption Alg
                                       Rcv'd: DES-CBC
                                    Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3871 10.48.66.76 12:47:24.430 02/15/2002 279
              :Phase 1 failure against global IKE proposal # 2
               :Mismatched attr types for class Encryption Alg
                                       Rcv'd: DES-CBC
                                    Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3872 10.48.66.76 12:47:24.430 02/15/2002 282
              :Phase 1 failure against global IKE proposal # 3
               :Mismatched attr types for class Encryption Alg
                                       Rcv'd: DES-CBC
                                    Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3873 10.48.66.76 12:47:24.430 02/15/2002 285
              :Phase 1 failure against global IKE proposal # 4
                    :Mismatched attr types for class DH Group
                                    Rcv'd: Oakley Group 2
                                    Cfg'd: Oakley Group 1

SEV=8 IKEDBG/0 RPT=3874 10.48.66.76 12:47:24.430 02/15/2002 288
              :Phase 1 failure against global IKE proposal # 5
                    :Mismatched attr types for class DH Group
                                    Rcv'd: Oakley Group 2
                                    Cfg'd: Oakley Group 1

SEV=8 IKEDBG/0 RPT=3875 10.48.66.76 12:47:24.430 02/15/2002 291
              :Phase 1 failure against global IKE proposal # 6
               :Mismatched attr types for class Encryption Alg
                                       Rcv'd: DES-CBC
                                    Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3876 10.48.66.76 12:47:24.430 02/15/2002 294
              :Phase 1 failure against global IKE proposal # 7
               :Mismatched attr types for class Encryption Alg
                                       Rcv'd: DES-CBC
                                    Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3877 10.48.66.76 12:47:24.430 02/15/2002 297
              :Phase 1 failure against global IKE proposal # 8
               :Mismatched attr types for class Encryption Alg
                                       Rcv'd: DES-CBC
                                    Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3878 10.48.66.76 12:47:24.430 02/15/2002 300
              :Phase 1 failure against global IKE proposal # 9
               :Mismatched attr types for class Encryption Alg
                                       Rcv'd: DES-CBC
                                    Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3879 10.48.66.76 12:47:24.430 02/15/2002 303
             :Phase 1 failure against global IKE proposal # 10
                    :Mismatched attr types for class DH Group
                                    Rcv'd: Oakley Group 2
```

```
                                        Cfg'd: Oakley Group 1

SEV=8 IKEDBG/0 RPT=3880 10.48.66.76 12:47:24.430 02/15/2002 306
            :Phase 1 failure against global IKE proposal # 11
                    :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 2
                                        Cfg'd: Oakley Group 1

SEV=8 IKEDBG/0 RPT=3881 10.48.66.76 12:47:24.430 02/15/2002 309
            :Phase 1 failure against global IKE proposal # 12
              :Mismatched attr types for class Encryption Alg
                                           Rcv'd: DES-CBC
                                       Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3882 10.48.66.76 12:47:24.430 02/15/2002 312
            :Phase 1 failure against global IKE proposal # 13
              :Mismatched attr types for class Encryption Alg
                                           Rcv'd: DES-CBC
                                       Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3883 10.48.66.76 12:47:24.430 02/15/2002 315
            :Phase 1 failure against global IKE proposal # 14
                    :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 2
                                        Cfg'd: Oakley Group 1

SEV=8 IKEDBG/0 RPT=3884 10.48.66.76 12:47:24.430 02/15/2002 318
            :Phase 1 failure against global IKE proposal # 15
                    :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 2
                                        Cfg'd: Oakley Group 7

SEV=8 IKEDBG/0 RPT=3885 10.48.66.76 12:47:24.430 02/15/2002 321
            :Phase 1 failure against global IKE proposal # 16
                    :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 2
                                        Cfg'd: Oakley Group 1

SEV=8 IKEDBG/0 RPT=3886 10.48.66.76 12:47:24.430 02/15/2002 324
              Proposal # 1, Transform # 3, Type ISAKMP, Id IKE
                                  :Parsing received transform
             :Phase 1 failure against global IKE proposal # 1
                    :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 1
                                        Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3887 10.48.66.76 12:47:24.430 02/15/2002 329
             :Phase 1 failure against global IKE proposal # 2
                    :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 1
                                        Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3888 10.48.66.76 12:47:24.430 02/15/2002 332
             :Phase 1 failure against global IKE proposal # 3
                    :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 1
                                        Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3889 10.48.66.76 12:47:24.430 02/15/2002 335
             :Phase 1 failure against global IKE proposal # 4
              :Mismatched attr types for class Encryption Alg
                                           Rcv'd: DES-CBC
                                       Cfg'd: Triple-DES
```

```
SEV=8 IKEDBG/0 RPT=3890 10.48.66.76 12:47:24.430 02/15/2002 338
             :Phase 1 failure against global IKE proposal # 5
              :Mismatched attr types for class Encryption Alg
                                          Rcv'd: DES-CBC
                                       Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3891 10.48.66.76 12:47:24.430 02/15/2002 341
             :Phase 1 failure against global IKE proposal # 6
                    :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 1
                                       Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3892 10.48.66.76 12:47:24.430 02/15/2002 344
             :Phase 1 failure against global IKE proposal # 7
                    :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 1
                                       Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3893 10.48.66.76 12:47:24.430 02/15/2002 347
             :Phase 1 failure against global IKE proposal # 8
                    :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 1
                                       Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3894 10.48.66.76 12:47:24.430 02/15/2002 350
             :Phase 1 failure against global IKE proposal # 9
                    :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 1
                                       Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3895 10.48.66.76 12:47:24.430 02/15/2002 353
            :Phase 1 failure against global IKE proposal # 10
              :Mismatched attr types for class Encryption Alg
                                          Rcv'd: DES-CBC
                                       Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3896 10.48.66.76 12:47:24.430 02/15/2002 356
            :Phase 1 failure against global IKE proposal # 11
                    :Mismatched attr types for class Hash Alg
                                          Rcv'd: SHA
                                          Cfg'd: MD5

SEV=8 IKEDBG/0 RPT=3897 10.48.66.76 12:47:24.430 02/15/2002 358
            :Phase 1 failure against global IKE proposal # 12
                    :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 1
                                       Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3898 10.48.66.76 12:47:24.430 02/15/2002 361
            :Phase 1 failure against global IKE proposal # 13
                    :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 1
                                       Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3899 10.48.66.76 12:47:24.430 02/15/2002 364
            :Phase 1 failure against global IKE proposal # 14
              :Mismatched attr types for class Encryption Alg
                                          Rcv'd: DES-CBC
                                       Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3900 10.48.66.76 12:47:24.430 02/15/2002 367
            :Phase 1 failure against global IKE proposal # 15
                    :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 1
```

```
                                        Cfg'd: Oakley Group 7

SEV=8 IKEDBG/0 RPT=3901 10.48.66.76 12:47:24.430 02/15/2002 370
            :Phase 1 failure against global IKE proposal # 16
                   :Mismatched attr types for class Hash Alg
                                              Rcv'd: SHA
                                              Cfg'd: MD5

SEV=8 IKEDBG/0 RPT=3902 10.48.66.76 12:47:24.430 02/15/2002 372
              Proposal # 1, Transform # 4, Type ISAKMP, Id IKE
                                    :Parsing received transform
             :Phase 1 failure against global IKE proposal # 1
                   :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 1
                                        Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3903 10.48.66.76 12:47:24.430 02/15/2002 377
             :Phase 1 failure against global IKE proposal # 2
                   :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 1
                                        Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3904 10.48.66.76 12:47:24.430 02/15/2002 380
             :Phase 1 failure against global IKE proposal # 3
                   :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 1
                                        Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3905 10.48.66.76 12:47:24.430 02/15/2002 383
             :Phase 1 failure against global IKE proposal # 4
              :Mismatched attr types for class Encryption Alg
                                           Rcv'd: DES-CBC
                                       Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3906 10.48.66.76 12:47:24.430 02/15/2002 386
             :Phase 1 failure against global IKE proposal # 5
              :Mismatched attr types for class Encryption Alg
                                           Rcv'd: DES-CBC
                                       Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3907 10.48.66.76 12:47:24.430 02/15/2002 389
             :Phase 1 failure against global IKE proposal # 6
                   :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 1
                                        Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3908 10.48.66.76 12:47:24.430 02/15/2002 392
             :Phase 1 failure against global IKE proposal # 7
                   :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 1
                                        Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3909 10.48.66.76 12:47:24.430 02/15/2002 395
             :Phase 1 failure against global IKE proposal # 8
                   :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 1
                                        Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3910 10.48.66.76 12:47:24.430 02/15/2002 398
             :Phase 1 failure against global IKE proposal # 9
                   :Mismatched attr types for class DH Group
                                        Rcv'd: Oakley Group 1
                                        Cfg'd: Oakley Group 2
```

```
SEV=8 IKEDBG/0 RPT=3911 10.48.66.76 12:47:24.430 02/15/2002 401
            :Phase 1 failure against global IKE proposal # 10
              :Mismatched attr types for class Encryption Alg
                                          Rcv'd: DES-CBC
                                       Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3912 10.48.66.76 12:47:24.430 02/15/2002 404
            :Phase 1 failure against global IKE proposal # 11
                 :Mismatched attr types for class Auth Method
                     Rcv'd: RSA signature with Certificates
                                    Cfg'd: Preshared Key

SEV=8 IKEDBG/0 RPT=3913 10.48.66.76 12:47:24.430 02/15/2002 407
            :Phase 1 failure against global IKE proposal # 12
                    :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 1
                                       Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3914 10.48.66.76 12:47:24.430 02/15/2002 410
            :Phase 1 failure against global IKE proposal # 13
                    :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 1
                                       Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=3915 10.48.66.76 12:47:24.430 02/15/2002 413
            :Phase 1 failure against global IKE proposal # 14
              :Mismatched attr types for class Encryption Alg
                                          Rcv'd: DES-CBC
                                       Cfg'd: Triple-DES

SEV=8 IKEDBG/0 RPT=3916 10.48.66.76 12:47:24.430 02/15/2002 416
            :Phase 1 failure against global IKE proposal # 15
                    :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 1
                                       Cfg'd: Oakley Group 7

 SEV=7 IKEDBG/28 RPT=20 10.48.66.76 12:47:24.430 02/15/2002 419
                  IKE SA Proposal # 1, Transform # 4 acceptable
                                 Matches global IKE entry # 16

SEV=9 IKEDBG/0 RPT=3917 10.48.66.76 12:47:24.440 02/15/2002 420
                                 constructing ISA_SA for isakmp

SEV=8 IKEDBG/0 RPT=3918 10.48.66.76 12:47:24.490 02/15/2002 421
                      : SENDING Message (msgid=0) with payloads
                   HDR + SA (1) + NONE (0) ... total length : 80

SEV=8 IKEDBG/0 RPT=3919 10.48.66.76 12:47:24.540 02/15/2002 423
                      : RECEIVED Message (msgid=0) with payloads
    HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

SEV=8 IKEDBG/0 RPT=3920 10.48.66.76 12:47:24.540 02/15/2002 425
                      : RECEIVED Message (msgid=0) with payloads
    HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

SEV=9 IKEDBG/0 RPT=3921 10.48.66.76 12:47:24.540 02/15/2002 427
                                       processing ke payload

SEV=9 IKEDBG/0 RPT=3922 10.48.66.76 12:47:24.540 02/15/2002 428
                                          processing ISA_KE

 SEV=9 IKEDBG/1 RPT=104 10.48.66.76 12:47:24.540 02/15/2002 429
                                    processing nonce payload
```

```
SEV=9 IKEDBG/0 RPT=3923 10.48.66.76 12:47:24.600 02/15/2002 430
                                                constructing ke payload

 SEV=9 IKEDBG/1 RPT=105 10.48.66.76 12:47:24.600 02/15/2002 431
                                              constructing nonce payload

SEV=9 IKEDBG/0 RPT=3924 10.48.66.76 12:47:24.600 02/15/2002 432
                                           constructing certreq payload

SEV=9 IKEDBG/0 RPT=3925 10.48.66.76 12:47:24.600 02/15/2002 433
                                Using initiator's certreq payload data

 SEV=9 IKEDBG/46 RPT=61 10.48.66.76 12:47:24.600 02/15/2002 434
                                  constructing Cisco Unity VID payload

 SEV=9 IKEDBG/46 RPT=62 10.48.66.76 12:47:24.600 02/15/2002 435
                                     constructing xauth V6 VID payload

 SEV=9 IKEDBG/48 RPT=39 10.48.66.76 12:47:24.600 02/15/2002 436
                                                       Send IOS VID

 SEV=9 IKEDBG/38 RPT=20 10.48.66.76 12:47:24.600 02/15/2002 437
                    Constructing VPN 3000 spoofing IOS Vendor ID payload
                                (version: 1.0.0, capabilities: 20000001)

 SEV=9 IKEDBG/46 RPT=63 10.48.66.76 12:47:24.600 02/15/2002 439
                                              constructing VID payload

 SEV=9 IKEDBG/48 RPT=40 10.48.66.76 12:47:24.600 02/15/2002 440
                                                  Send Altiga GW VID

SEV=9 IKEDBG/0 RPT=3926 10.48.66.76 12:47:24.600 02/15/2002 441
                                       ...Generating keys for Responder

SEV=8 IKEDBG/0 RPT=3927 10.48.66.76 12:47:24.610 02/15/2002 442
                                  : SENDING Message (msgid=0) with payloads
(HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13
  VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 229 +

SEV=8 IKEDBG/0 RPT=3928 10.48.66.76 12:47:24.640 02/15/2002 445
                              : RECEIVED Message (msgid=0) with payloads
    (HDR + ID (5) + CERT (6) + SIG (9) + CERT_REQ (7) + NONE (0
                                                  total length : 1186 ...

 SEV=9 IKEDBG/1 RPT=106 10.48.66.76 12:47:24.640 02/15/2002 448
                                                       Processing ID

SEV=9 IKEDBG/0 RPT=3929 10.48.66.76 12:47:24.640 02/15/2002 449
                                              processing cert payload

 SEV=9 IKEDBG/1 RPT=107 10.48.66.76 12:47:24.640 02/15/2002 450
                                            processing RSA signature

SEV=9 IKEDBG/0 RPT=3930 10.48.66.76 12:47:24.640 02/15/2002 451
                                                       computing hash

SEV=9 IKEDBG/0 RPT=3931 10.48.66.76 12:47:24.650 02/15/2002 452
                                        processing cert request payload

SEV=9 IKEDBG/0 RPT=3932 10.48.66.76 12:47:24.650 02/15/2002 453
                        Storing cert request payload for use in MM msg 4

 SEV=9 IKEDBG/23 RPT=20 10.48.66.76 12:47:24.650 02/15/2002 454
                             Starting group lookup for peer 10.48.66.76
```

```
   SEV=9 IKE/21 RPT=12 10.48.66.76 12:47:24.650 02/15/2002 455
No Group found by matching IP Address of Cert peer 10.48.66.76

   SEV=9 IKE/20 RPT=12 10.48.66.76 12:47:24.650 02/15/2002 456
          :No Group found by matching OU(s) from ID payload
                                                    ,ou=sns

    SEV=9 IKE/0 RPT=12 10.48.66.76 12:47:24.650 02/15/2002 457
                                          [Group [VPNC_Base_Group
  No Group name for IKE Cert session, defaulting to BASE GROUP

SEV=7 IKEDBG/0 RPT=3933 10.48.66.76 12:47:24.750 02/15/2002 459
                                          [Group [VPNC_Base_Group
                        (Found Phase 1 Group (VPNC_Base_Group

 SEV=7 IKEDBG/14 RPT=20 10.48.66.76 12:47:24.750 02/15/2002 460
                                          [Group [VPNC_Base_Group
                       Authentication configured for Internal

 SEV=9 IKEDBG/19 RPT=20 10.48.66.76 12:47:24.750 02/15/2002 461
                                          [Group [VPNC_Base_Group
          IKEGetUserAttributes: default domain = fenetwork.com

    SEV=5 IKE/79 RPT=4 10.48.66.76 12:47:24.770 02/15/2002 462
                                          [Group [VPNC_Base_Group
                         Validation of certificate successful
                        (CN=my_name, SN=6102861F000000000005)

SEV=7 IKEDBG/0 RPT=3934 10.48.66.76 12:47:24.770 02/15/2002 464
                                          [Group [VPNC_Base_Group
                        (peer ID type 9 received (DER_ASN1_DN

 SEV=9 IKEDBG/1 RPT=108 10.48.66.76 12:47:24.770 02/15/2002 465
                                          [Group [VPNC_Base_Group
                                                  constructing ID

SEV=9 IKEDBG/0 RPT=3935 10.48.66.76 12:47:24.770 02/15/2002 466
                                          [Group [VPNC_Base_Group
                                       constructing cert payload

 SEV=9 IKEDBG/1 RPT=109 10.48.66.76 12:47:24.770 02/15/2002 467
                                          [Group [VPNC_Base_Group
                                     constructing RSA signature

SEV=9 IKEDBG/0 RPT=3936 10.48.66.76 12:47:24.770 02/15/2002 468
                                          [Group [VPNC_Base_Group
                                                   computing hash

 SEV=9 IKEDBG/46 RPT=64 10.48.66.76 12:47:24.800 02/15/2002 469
                                          [Group [VPNC_Base_Group
                                   constructing dpd vid payload

SEV=8 IKEDBG/0 RPT=3937 10.48.66.76 12:47:24.800 02/15/2002 470
                       : SENDING Message (msgid=0) with payloads
     (HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) + NONE (0
                                          total length : 1112 ...

   SEV=4 IKE/119 RPT=4 10.48.66.76 12:47:24.800 02/15/2002 473
                                          [Group [VPNC_Base_Group
                                                PHASE 1 COMPLETED

   SEV=6 IKE/121 RPT=4 10.48.66.76 12:47:24.800 02/15/2002 474
                       Keep-alive type for this connection: None
```

```
                    SEV=6 IKE/122 RPT=4 10.48.66.76 12:47:24.800 02/15/2002 475
(Keep-alives configured on but peer does not support keep-alives (type = None

                  SEV=7 IKEDBG/0 RPT=3938 10.48.66.76 12:47:24.800 02/15/2002 476
                                                  [Group [VPNC_Base_Group
                                (Starting phase 1 rekey timer: 21600000 (ms

                  SEV=8 IKEDBG/0 RPT=3939 10.48.66.76 12:47:24.810 02/15/2002 477
                                : RECEIVED Message (msgid=781ceadc) with payloads
               (HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0
                                                  total length : 1108 ...

                  SEV=9 IKEDBG/0 RPT=3940 10.48.66.76 12:47:24.810 02/15/2002 480
                                                  [Group [VPNC_Base_Group
                                                          processing hash

                  SEV=9 IKEDBG/0 RPT=3941 10.48.66.76 12:47:24.810 02/15/2002 481
                                                  [Group [VPNC_Base_Group
                                                    processing SA payload

                   SEV=9 IKEDBG/1 RPT=110 10.48.66.76 12:47:24.810 02/15/2002 482
                                                  [Group [VPNC_Base_Group
                                                 processing nonce payload

                   SEV=9 IKEDBG/1 RPT=111 10.48.66.76 12:47:24.810 02/15/2002 483
                                                  [Group [VPNC_Base_Group
                                                            Processing ID

                       SEV=5 IKE/25 RPT=4 10.48.66.76 12:47:24.810 02/15/2002 484
                                                  [Group [VPNC_Base_Group
                                    :Received remote Proxy Host data in ID Payload
                                      Address 10.48.66.76, Protocol 17, Port 1701

                   SEV=9 IKEDBG/1 RPT=112 10.48.66.76 12:47:24.810 02/15/2002 487
                                                  [Group [VPNC_Base_Group
                                                            Processing ID

                       SEV=5 IKE/24 RPT=4 10.48.66.76 12:47:24.810 02/15/2002 488
                                                  [Group [VPNC_Base_Group
                                     :Received local Proxy Host data in ID Payload
                                         Address 10.48.66.109, Protocol 17, Port 0

                              SEV=8 IKEDBG/0 RPT=3942 12:47:24.810 02/15/2002 491
                                           QM IsRekeyed old sa not found by addr

                       SEV=5 IKE/66 RPT=4 10.48.66.76 12:47:24.810 02/15/2002 492
                                                  [Group [VPNC_Base_Group
                            IKE Remote Peer configured for SA: ESP-L2TP-TRANSPORT

                  SEV=9 IKEDBG/0 RPT=3943 10.48.66.76 12:47:24.810 02/15/2002 493
                                                  [Group [VPNC_Base_Group
                                                      processing IPSEC SA

                    SEV=7 IKEDBG/27 RPT=4 10.48.66.76 12:47:24.810 02/15/2002 494
                                                  [Group [VPNC_Base_Group
                                  IPSec SA Proposal # 1, Transform # 1 acceptable

                  SEV=7 IKEDBG/0 RPT=3944 10.48.66.76 12:47:24.810 02/15/2002 495
                                                  [Group [VPNC_Base_Group
                                                     !IKE: requesting SPI

                                  SEV=8 IKEDBG/6 RPT=4 12:47:24.810 02/15/2002 496
                                     IKE got SPI from key engine: SPI = 0x10d19e33
```

```
SEV=9 IKEDBG/0 RPT=3945 10.48.66.76 12:47:24.810 02/15/2002 497
                                          [Group [VPNC_Base_Group
                                  oakley constucting quick mode

SEV=9 IKEDBG/0 RPT=3946 10.48.66.76 12:47:24.810 02/15/2002 498
                                          [Group [VPNC_Base_Group
                                        constructing blank hash

SEV=9 IKEDBG/0 RPT=3947 10.48.66.76 12:47:24.820 02/15/2002 499
                                          [Group [VPNC_Base_Group
                                  constructing ISA_SA for ipsec

SEV=9 IKEDBG/1 RPT=113 10.48.66.76 12:47:24.820 02/15/2002 500
                                          [Group [VPNC_Base_Group
                               constructing ipsec nonce payload

SEV=9 IKEDBG/1 RPT=114 10.48.66.76 12:47:24.820 02/15/2002 501
                                          [Group [VPNC_Base_Group
                                          constructing proxy ID

SEV=7 IKEDBG/0 RPT=3948 10.48.66.76 12:47:24.820 02/15/2002 502
                                          [Group [VPNC_Base_Group
                                         :Transmitting Proxy Id
                    Remote host: 10.48.66.76  Protocol 17  Port 1701
                      Local host:  10.48.66.109  Protocol 17  Port 0

SEV=9 IKEDBG/0 RPT=3949 10.48.66.76 12:47:24.820 02/15/2002 506
                                          [Group [VPNC_Base_Group
                                             constructing qm hash

SEV=8 IKEDBG/0 RPT=3950 10.48.66.76 12:47:24.820 02/15/2002 507
                         : SENDING Message (msgid=781ceadc) with payloads
(HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0
                                         total length : 156 ...

SEV=8 IKEDBG/0 RPT=3951 10.48.66.76 12:47:24.820 02/15/2002 510
                       : RECEIVED Message (msgid=781ceadc) with payloads
                         HDR + HASH (8) + NONE (0) ... total length : 48

SEV=9 IKEDBG/0 RPT=3952 10.48.66.76 12:47:24.830 02/15/2002 512
                                          [Group [VPNC_Base_Group
                                                  processing hash

SEV=9 IKEDBG/0 RPT=3953 10.48.66.76 12:47:24.830 02/15/2002 513
                                          [Group [VPNC_Base_Group
                                            loading all IPSEC SAs

SEV=9 IKEDBG/1 RPT=115 10.48.66.76 12:47:24.830 02/15/2002 514
                                          [Group [VPNC_Base_Group
                                      !Generating Quick Mode Key

SEV=9 IKEDBG/1 RPT=116 10.48.66.76 12:47:24.830 02/15/2002 515
                                          [Group [VPNC_Base_Group
                                      !Generating Quick Mode Key

SEV=7 IKEDBG/0 RPT=3954 10.48.66.76 12:47:24.830 02/15/2002 516
                                          [Group [VPNC_Base_Group
                                                    :Loading host
                                              Dst: 10.48.66.109
                                               Src: 10.48.66.76

     SEV=4 IKE/49 RPT=4 10.48.66.76 12:47:24.830 02/15/2002 517
                                          [Group [VPNC_Base_Group
```

```
() Security negotiation complete for User
Responder, Inbound SPI = 0x10d19e33, Outbound SPI = 0x15895ab9

SEV=8 IKEDBG/7 RPT=4 12:47:24.830 02/15/2002 520
IKE got a KEY_ADD msg for SA: SPI = 0x15895ab9

SEV=8 IKEDBG/0 RPT=3955 12:47:24.830 02/15/2002 521
pitcher: rcv KEY_UPDATE, spi 0x10d19e33

SEV=4 IKE/120 RPT=4 10.48.66.76 12:47:24.830 02/15/2002 522
[Group [VPNC_Base_Group
(PHASE 2 COMPLETED (msgid=781ceadc

SEV=8 IKEDBG/0 RPT=3956 12:47:24.840 02/15/2002 523
pitcher: recv KEY_SA_ACTIVE spi 0x10d19e33

SEV=8 IKEDBG/0 RPT=3957 12:47:24.840 02/15/2002 524
KEY_SA_ACTIVE no old rekey centry found with new spi 0x10d19e33, mess_id 0x0
```

معلومات أستكشاف الأخطاء وإصلاحها

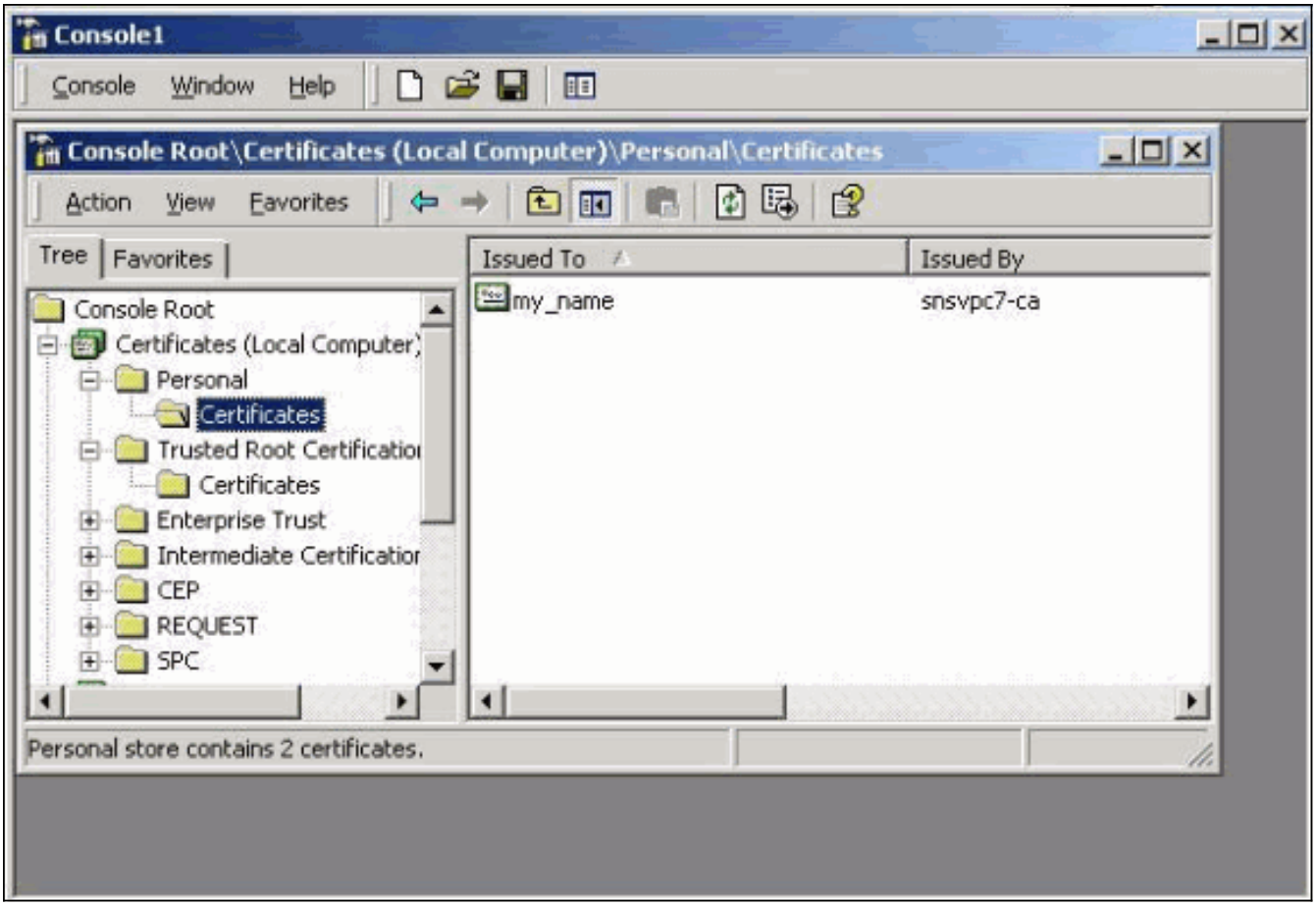
يوضح هذا القسم بعض المشاكل الشائعة وأساليب أستكشاف الأخطاء وإصلاحها لكل منها.

- يتعذر بدء تشغيل الخادم.

من المرجح أن خدمة IPSec لم تبدأ. حدد **ابدأ > برامج > أدوات إدارية > الخدمة** وتأكد من تمكين **خدمة IPSec**.

- خطأ 786: لا توجد شهادة جهاز صالحة.

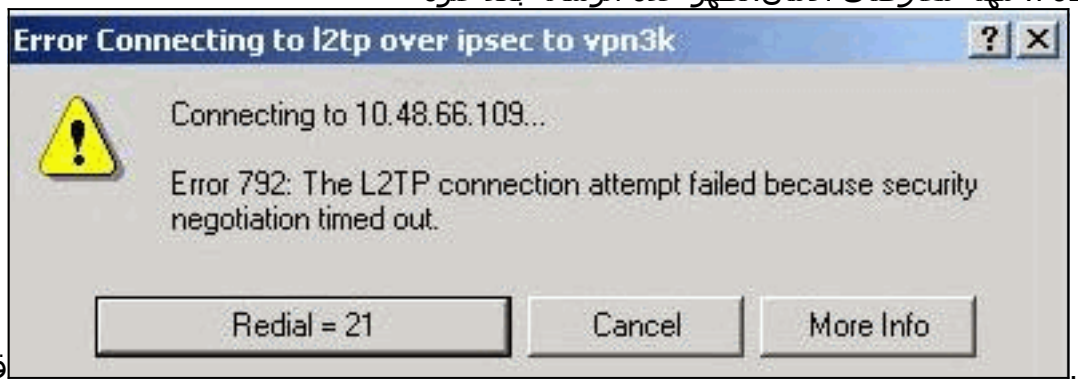
يشير هذا الخطأ إلى وجود مشكلة في الشهادة الموجودة على الجهاز المحلي. من أجل النظر إلى ترخيصك بسهولة، حدد **ابدأ > تشغيل**، وقم بتنفيذ MMC. انقر فوق **وحدة التحكم** واختر **إضافة/إزالة الأداة الإضافية**. انقر على **إضافة** واختر **شهادة** من القائمة. عندما تظهر نافذة تسألك عن نطاق الشهادة، أختر **حساب الكمبيوتر**.الآن يمكنك التحقق من أن شهادة خادم CA موجودة تحت **مراجع التصديق الجذر الموثوق فيها**. يمكنك أيضا التحقق من أن لديك شهادة بتحديد **جذر وحدة التحكم > الترخيص (كمبيوتر محلي) > شخصي > شهادات**، كما هو موضح في هذه الصورة.



انقر على **الشهادة**. تحقق من صحة كل شيء. في هذا المثال، هناك مفتاح خاص مرتبط بالشهادة. ومع ذلك، انتهت صلاحية هذه الشهادة. هذا هو سبب

المشكلة.

- خطأ 792: مهلة مفاوضات الأمان.تظهر هذه الرسالة بعد فترة



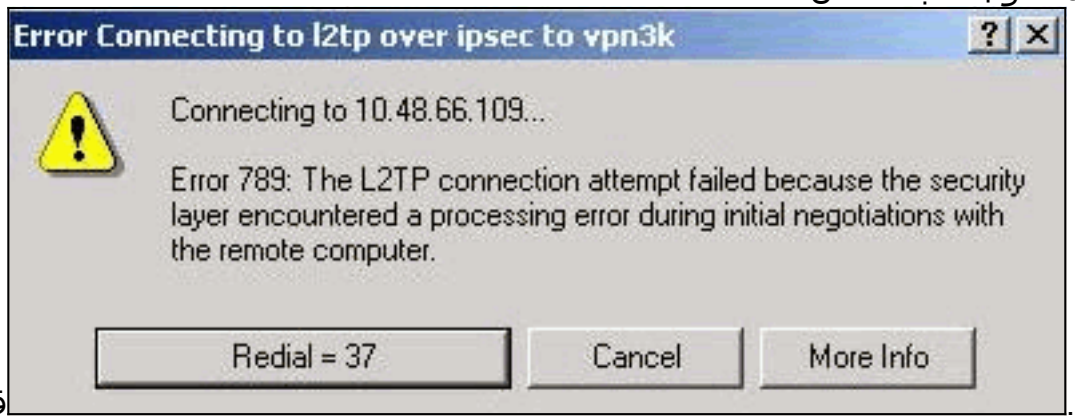
طويلة. قم بتشغيل تصحيح الأخطاء ذات الصلة كما هو موضح في الأسئلة المتداولة حول مركز Cisco VPN 3000. اقرأوا من خلالها. تحتاج أن ترى شيئا مشابها لهذا الناتج:

```
SEV=8 IKEDBG/0 RPT=7002 10.48.66.76 15:06:13.500 02/15/2002 9337
                :Phase 1 failure against global IKE proposal # 6
                  :Mismatched attr types for class DH Group
                                  Rcv'd: Oakley Group 1
                                  Cfg'd: Oakley Group 2

SEV=8 IKEDBG/0 RPT=7003 10.48.66.76 15:06:13.510 02/15/2002 9340
                :Phase 1 failure against global IKE proposal # 7
```

```
:Mismatched attr types for class Auth Method
    Rcv'd: RSA signature with Certificates
        Cfg'd: Preshared Key

SEV=8 IKEDBG/0 RPT=7004 10.48.66.76 15:06:13.510 02/15/2002 9343
:Phase 1 failure against global IKE proposal # 8
:Mismatched attr types for class DH Group
        Rcv'd: Oakley Group 1
        Cfg'd: Oakley Group 7

SEV=7 IKEDBG/0 RPT=7005 10.48.66.76 15:06:13.510 02/15/2002 9346
All SA proposals found unacceptable

SEV=4 IKE/48 RPT=37 10.48.66.76 15:06:13.510 02/15/2002 9347
Error processing payload: Payload ID: 1

SEV=9 IKEDBG/0 RPT=7006 10.48.66.76 15:06:13.510 02/15/2002 9348
:IKE SA MM:261e40dd terminating
flags 0x01000002, refcnt 0, tuncnt 0

SEV=9 IKEDBG/0 RPT=7007 15:06:13.510 02/15/2002 9349
sending delete message
```

وهذا يشير إلى أن اقتراح IKE لم يتم تكوينه بشكل صحيح. تحقق من المعلومات الواردة من قسم تكوين مقترح IKE في هذا المستند.

- خطأ 789: تواجه طبقة الأمان خطأ



معالجة. قم بتشغيل تصحيح الأخطاء ذات الصلة كما هو موضح في الأسئلة المتداولة حول مركز Cisco VPN 3000. اقرأوا من خلالها. تحتاج أن ترى شيئا مشابها لهذا الناتج:

```
SEV=8 IKEDBG/0 RPT=7686 15:36:32.030 02/15/2002 11315
    Proposal # 1, Transform # 2, Type ESP, Id DES-CBC
:Parsing received transform
:Phase 2 failure
:Mismatched attr types for class Encapsulation
        Rcv'd: Transport
        Cfg'd: Tunnel

SEV=5 IKEDBG/0 RPT=7687 15:36:32.030 02/15/2002 11320
AH proposal not supported

SEV=4 IKE/0 RPT=27 10.48.66.76 15:36:32.030 02/15/2002 11321
[Group [VPNC_Base_Group
!All IPSec SA proposals found unacceptable
```

- الإصدار المستخدمحدد **مراقبة > حالة النظام** لعرض هذا الإخراج:

```
VPN Concentrator Type: 3005
    Bootcode Rev: Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 2000 05:36:41
Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Version 3.5.Rel Nov 27 2001 13:35:16
        Up For: 44:39:48
    Up Since: 02/13/2002 15:49:59
        RAM Size: 32 MB
```

معلومات ذات صلة

- مفاوضة IPSec/دعم منتجات بروتوكولات IKE
- 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).