デジタル証明書を使用した Windows 2000 と VPN 3000 コンセントレータ間の L2TP over IPSec の設定例

内容

概要

このドキュメントでは、L2TP/IPSec 組み込みクライアントを使用している Windows 2000 クライアントから VPN 3000 コンセントレータに接続する手順について順を追って説明します。デジタル証明書(Certificate Enrollment Protocol(CEP)を使用しないスタンドアロンルート認証局(CA))を使用して、VPNコンセントレータへの接続を認証することを前提としています。このドキュメントでは、説明のために Microsoft 証明書サービスを使用します。設定方法については、Microsoft Webサイトを参照してください。

注：これは、Windows 2000の画面の外観が変更される可能性がある場合の例です。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco VPN 3000コンセントレータシリーズのものです。

目的

この手順では、次の手順を実行します。

1. ルート証明書を取得します。
2. クライアントのID証明書を取得します。
3. ネットワーク接続ウィザードを使用して、VPN 3000への接続を作成します。
4. VPN 3000 コンセントレータの設定.

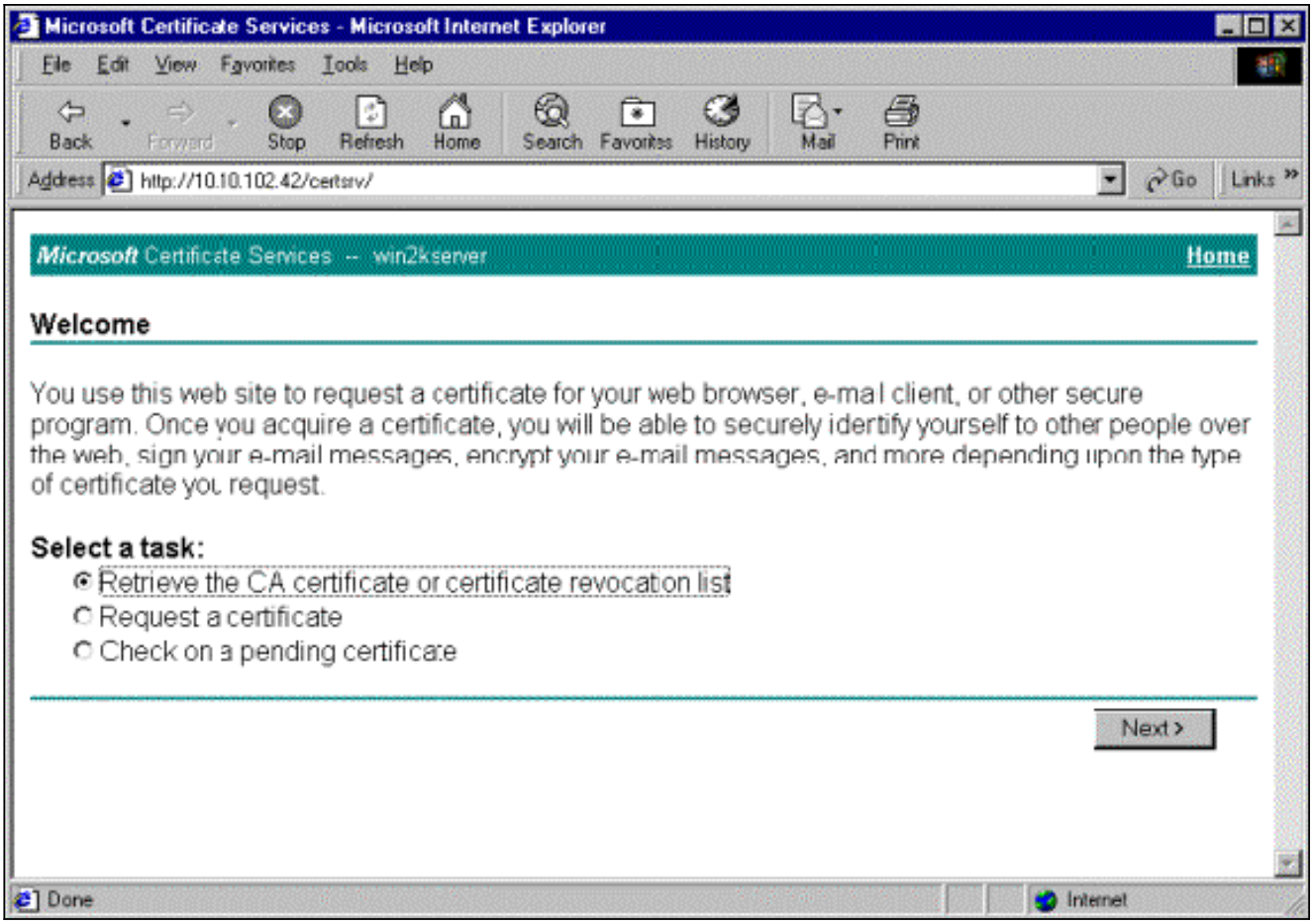
表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

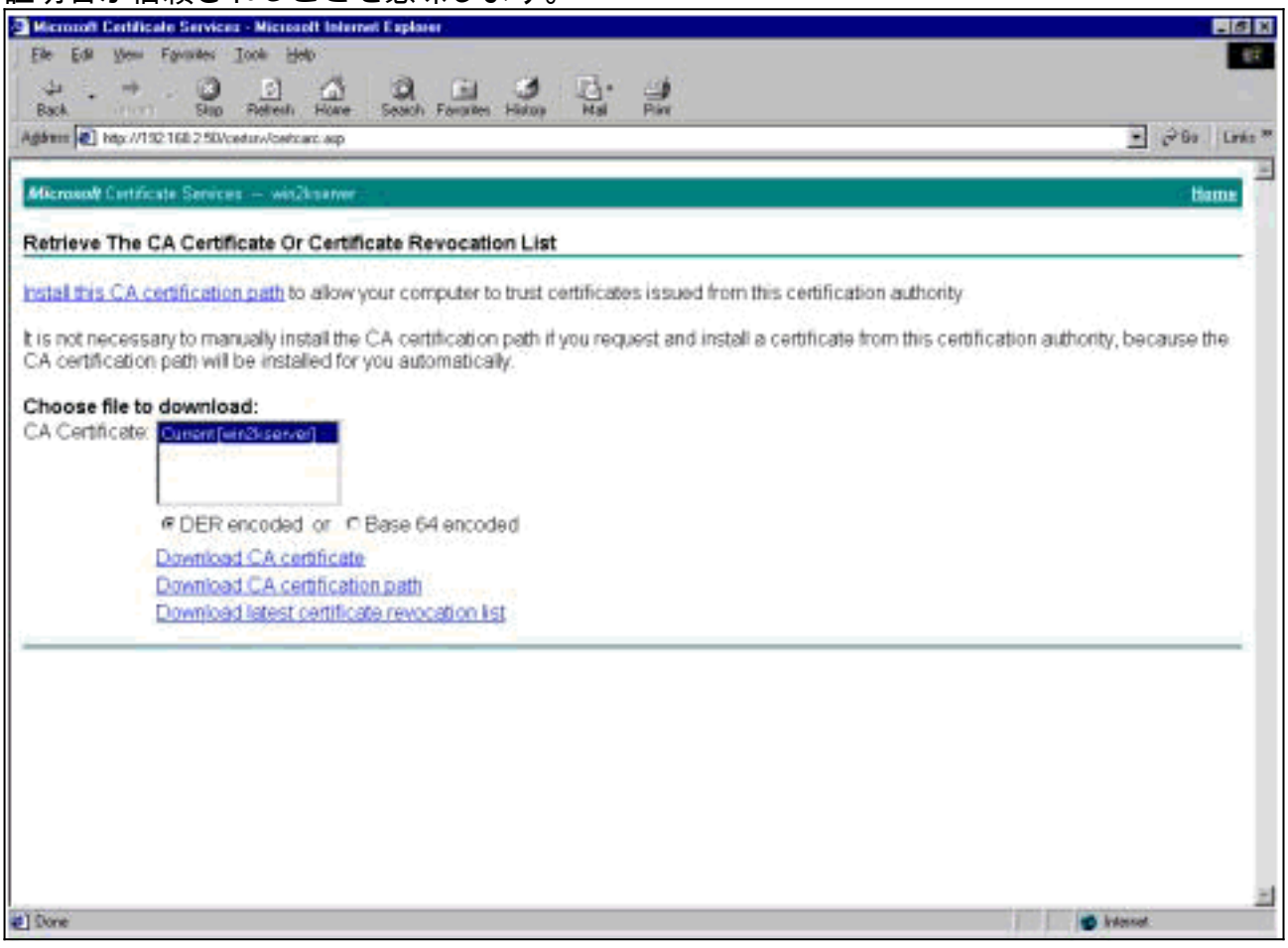
ルート証明書の取得

ルート証明書を取得するには、次の手順を実行します。

1. ブラウザウィンドウを開き、Microsoft認証局のURL(通常はhttp://servernameまたはCA/certsrvのIPアドレス)を入力します。証明書の取得と要求の[Welcome]ウィンドウが表示されます。
2. [Welcome]ウィンドウの[Select a task]で、[Retrieve the CA certificate or certificate revocation list] を選択し、[Next] をクリックします。



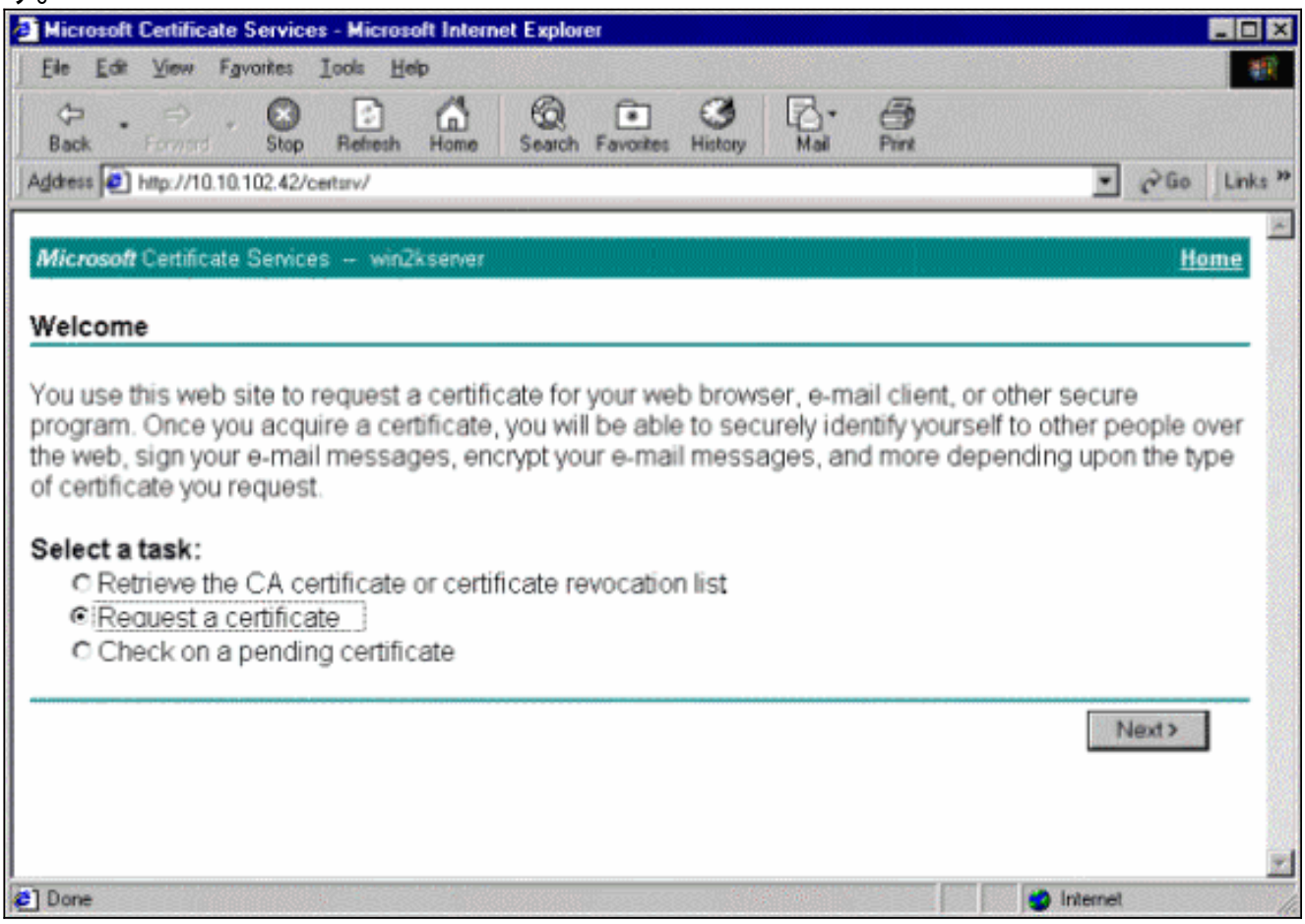
3. [Retrieve the CA certificate or certificate revocation list]ウィンドウで、左側にある[Install this CA certification path] をクリックします。これにより、CA証明書がTrusted Root Certificate Authoritiesストアに追加されます。これは、このCAがこのクライアントに発行するすべての証明書が信頼されることを意味します。



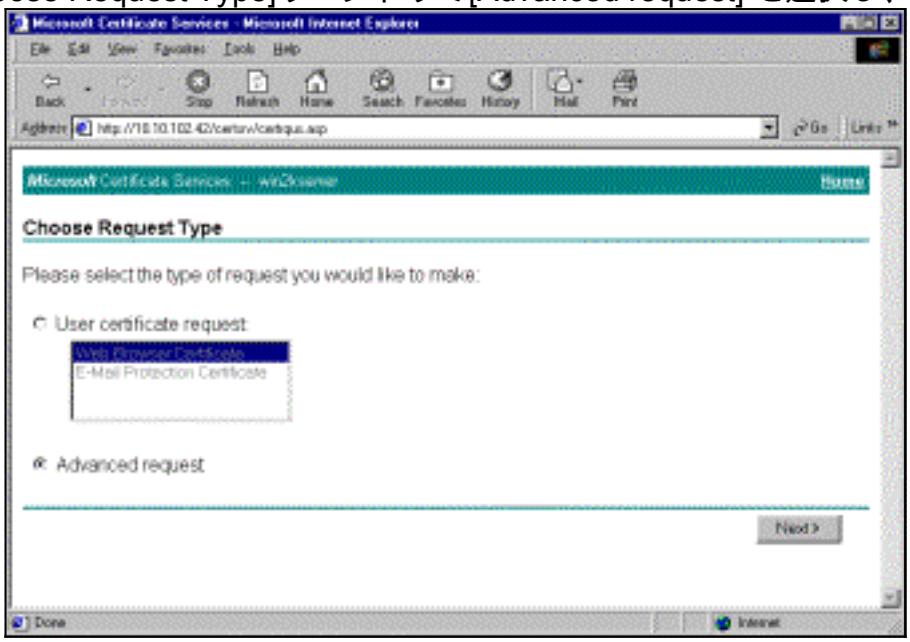
クライアントのID証明書の取得

クライアントのID証明書を取得するには、次の手順を実行します。

1. ブラウザウィンドウを開き、Microsoft認証局のURL(通常はhttp://servernameまたはCA/certsrvのIPアドレス)を入力します。証明書の取得と要求の[Welcome]ウィンドウが表示されます。
2. WelcomeウィンドウのSelect a taskで、**Request a certificate**を選択し、**Next**をクリックします。

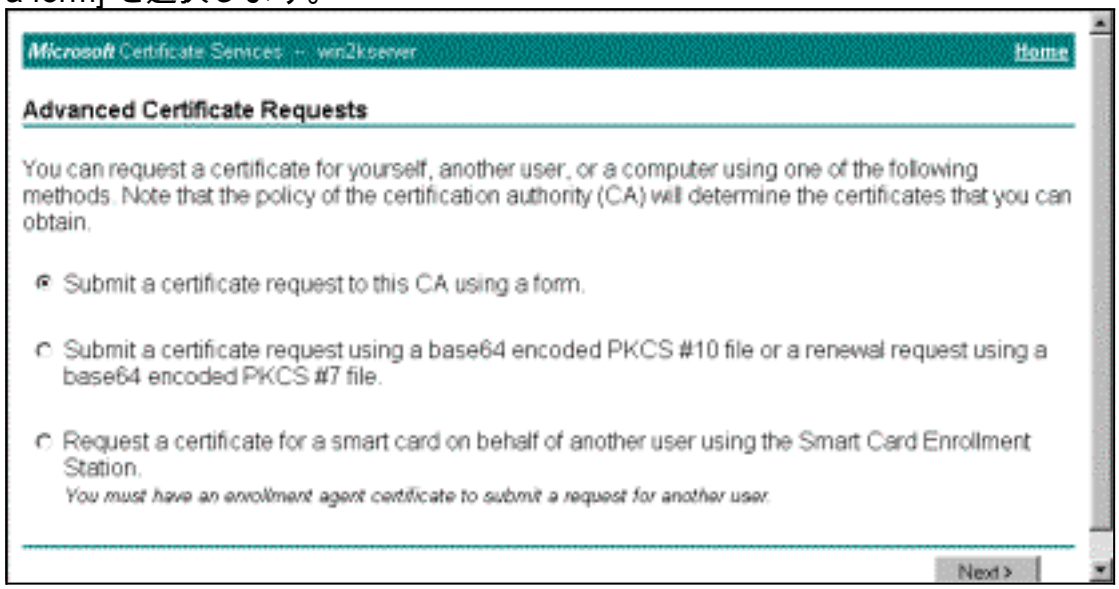


3. [Choose Request Type]ウィンドウで[Advanced request] を選択し、[Next] をクリックします。

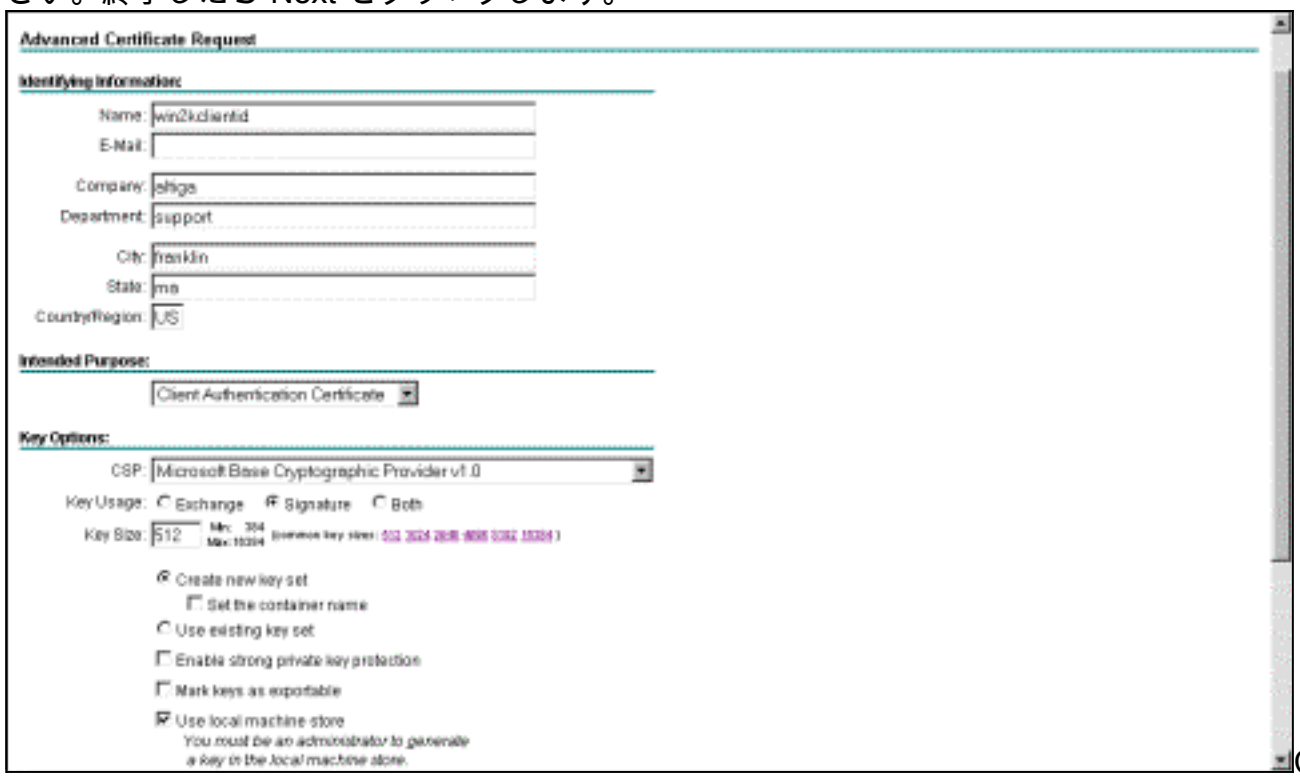


4. [Advanced Certificate Requests]ウィンドウで、[Submit a certificate request to this CA using

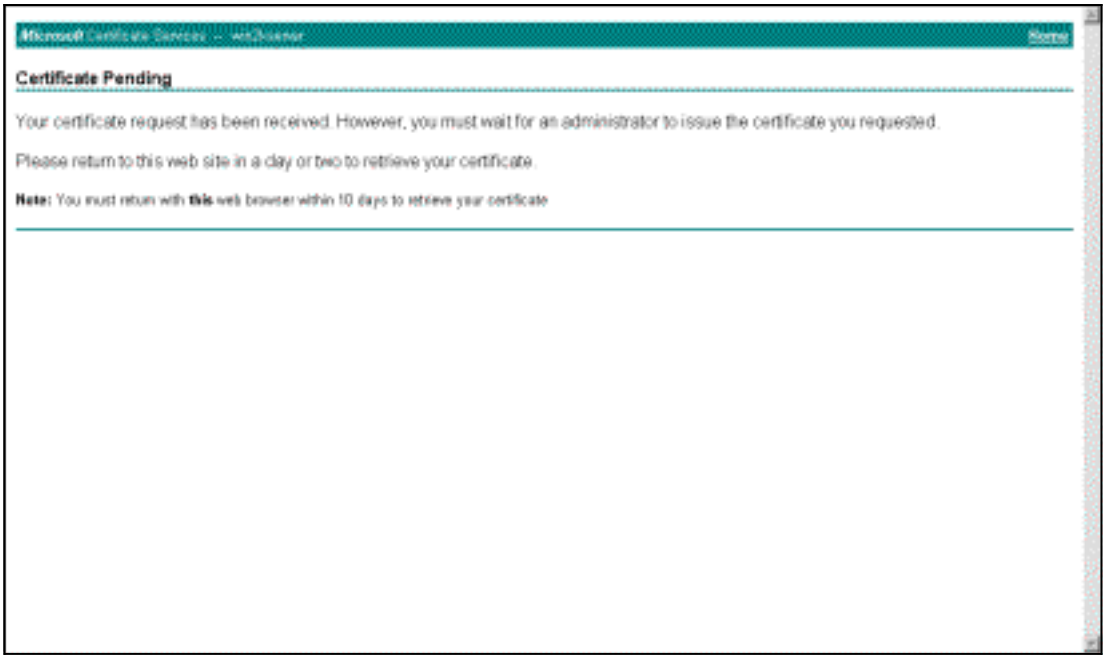
a form] を選択します。



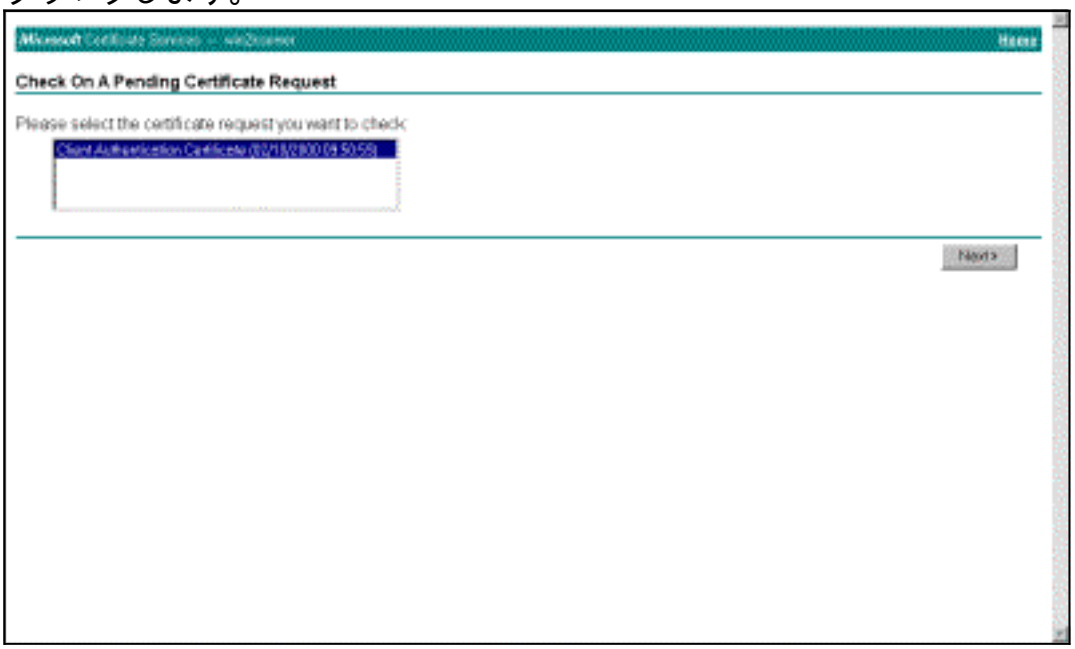
5. この例のようにフィールドに入力します。Department（組織単位）の値は、VPNコンセントレータで設定されたグループと一致する必要があります。1024より大きいキーサイズは指定しないでください。必ず[Use local machine store] チェックボックスをオンにしてください。終了したら Next をクリックします。



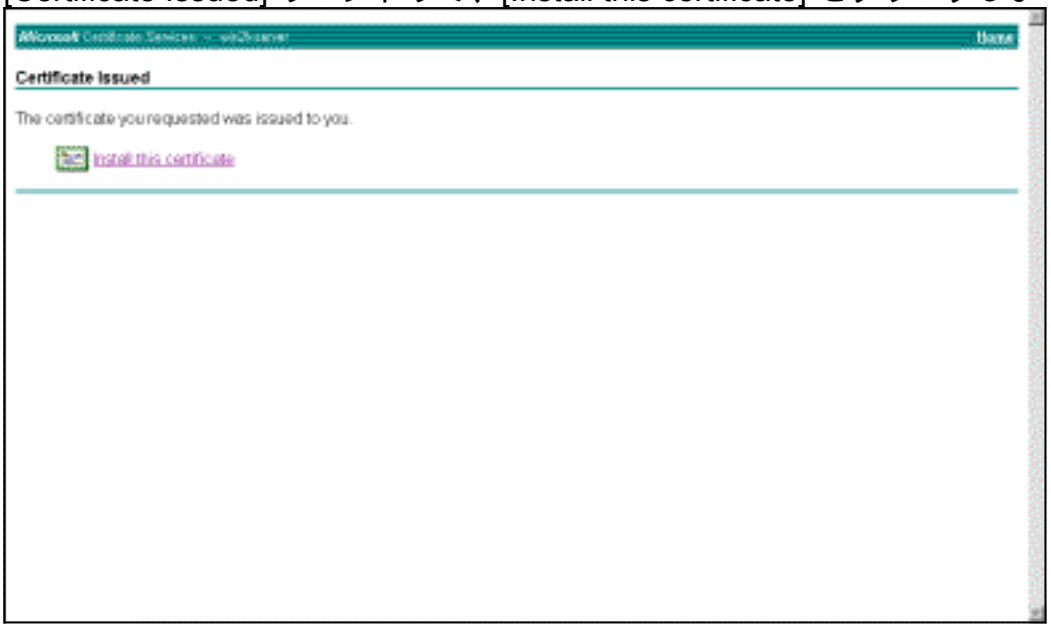
CAサーバの設定方法によっては、このウィンドウが表示されることがあります。その場合は、CA管理者に連絡してください。



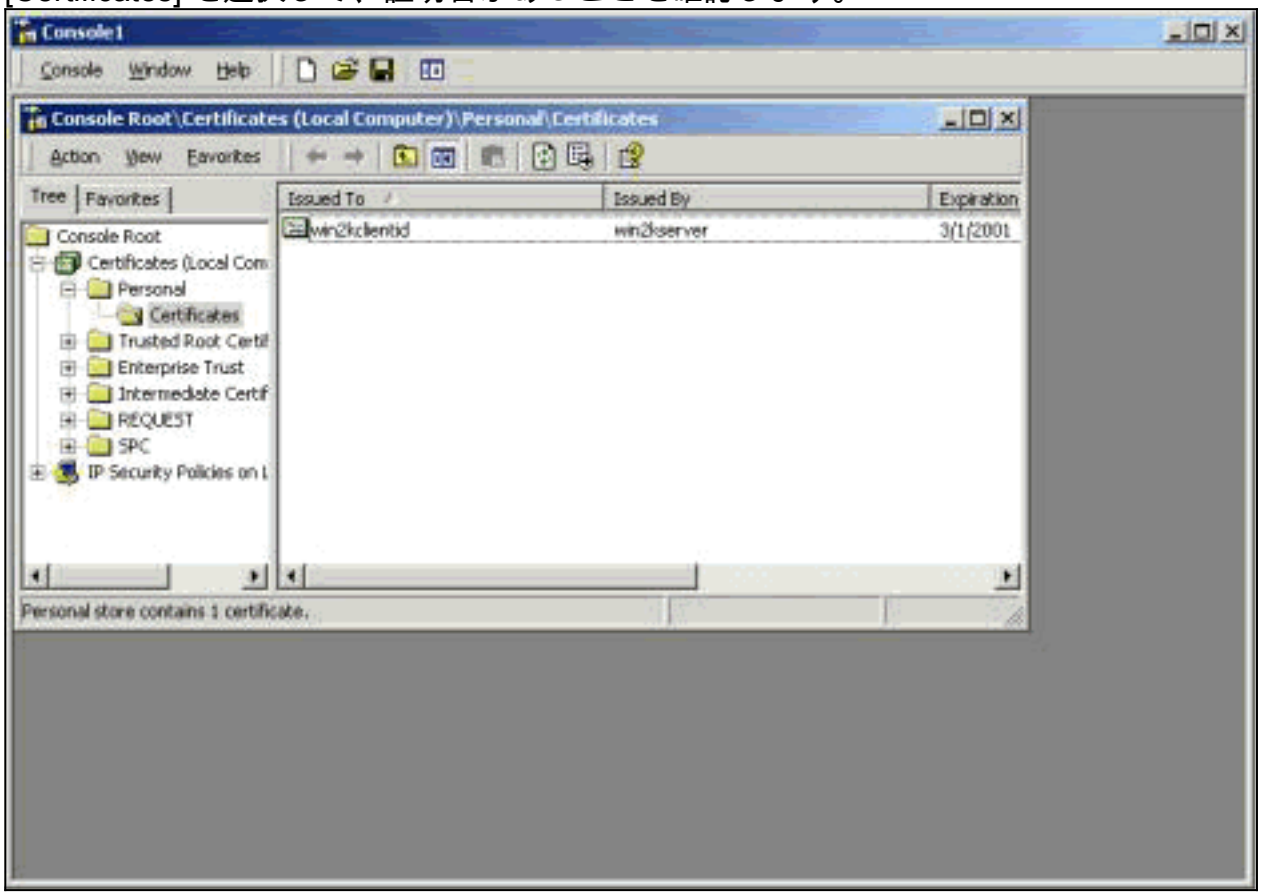
6. **Home**をクリックしてメイン画面に戻り、**Check on pending certificate**を選択して、**Next**をクリックします。



7. [Certificate Issued] ウィンドウで、[Install this certificate] をクリックします。



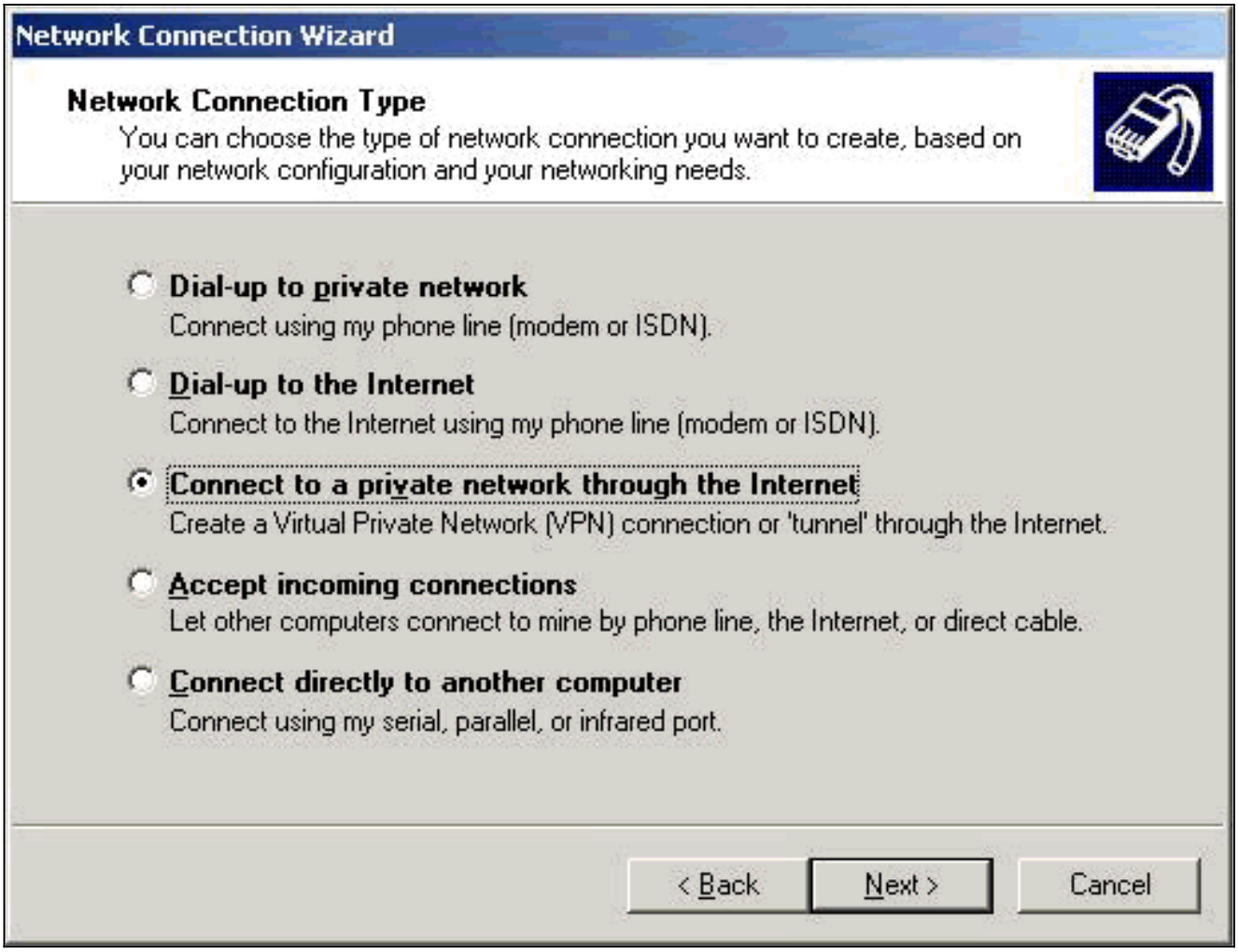
8. クライアント証明書を表示するには、[Start] > [Run] を選択し、Microsoft管理コンソール(MMC)を実行します。
9. **Console**をクリックし、**Add/Remove Snap-in**を選択します。
10. **Add**をクリックし、リストから**Certificate**を選択します。
11. 証明書の範囲を確認するウィンドウが表示されたら、[Computer Account] を選択します。
12. CAサーバの証明書が[Trusted Root Certification Authorities]の下にあることを確認します。また、次の図に示すように、[Console Root] > [Certificate (Local Computer)] > [Personal] > [Certificates] を選択して、証明書があることを確認します。



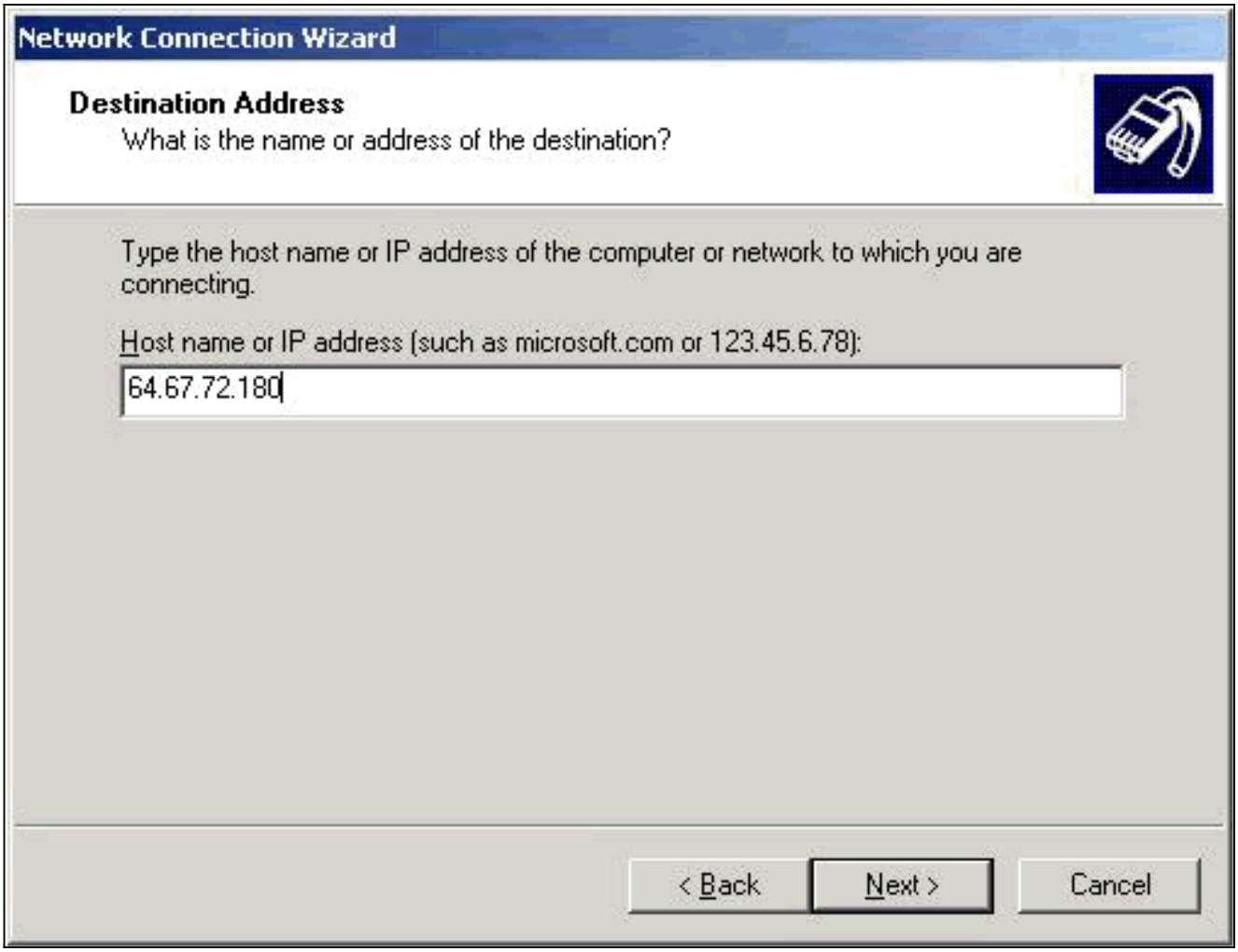
ネットワーク接続ウィザードを使用したVPN 3000への接続の作成

ネットワーク接続ウィザードを使用してVPN 3000への接続を作成するには、次の手順を実行します。

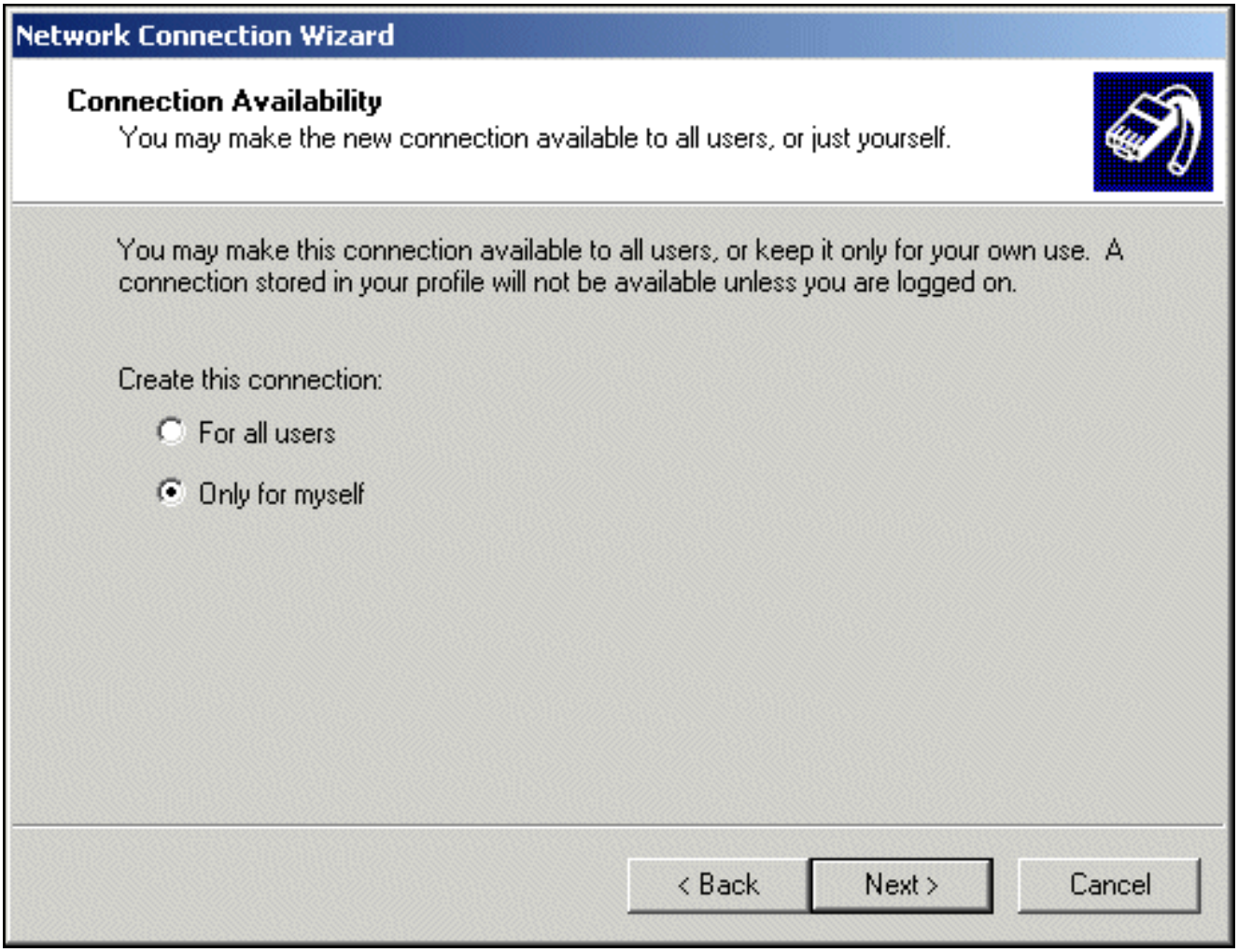
1. **My Network Places**を右クリックし、**Properties**を選択して、**Make New Connection**をクリックします。
2. Network Connection Typeウィンドウで、**Connect to a private network through the Internet**を選択し、**Next**をクリックします。



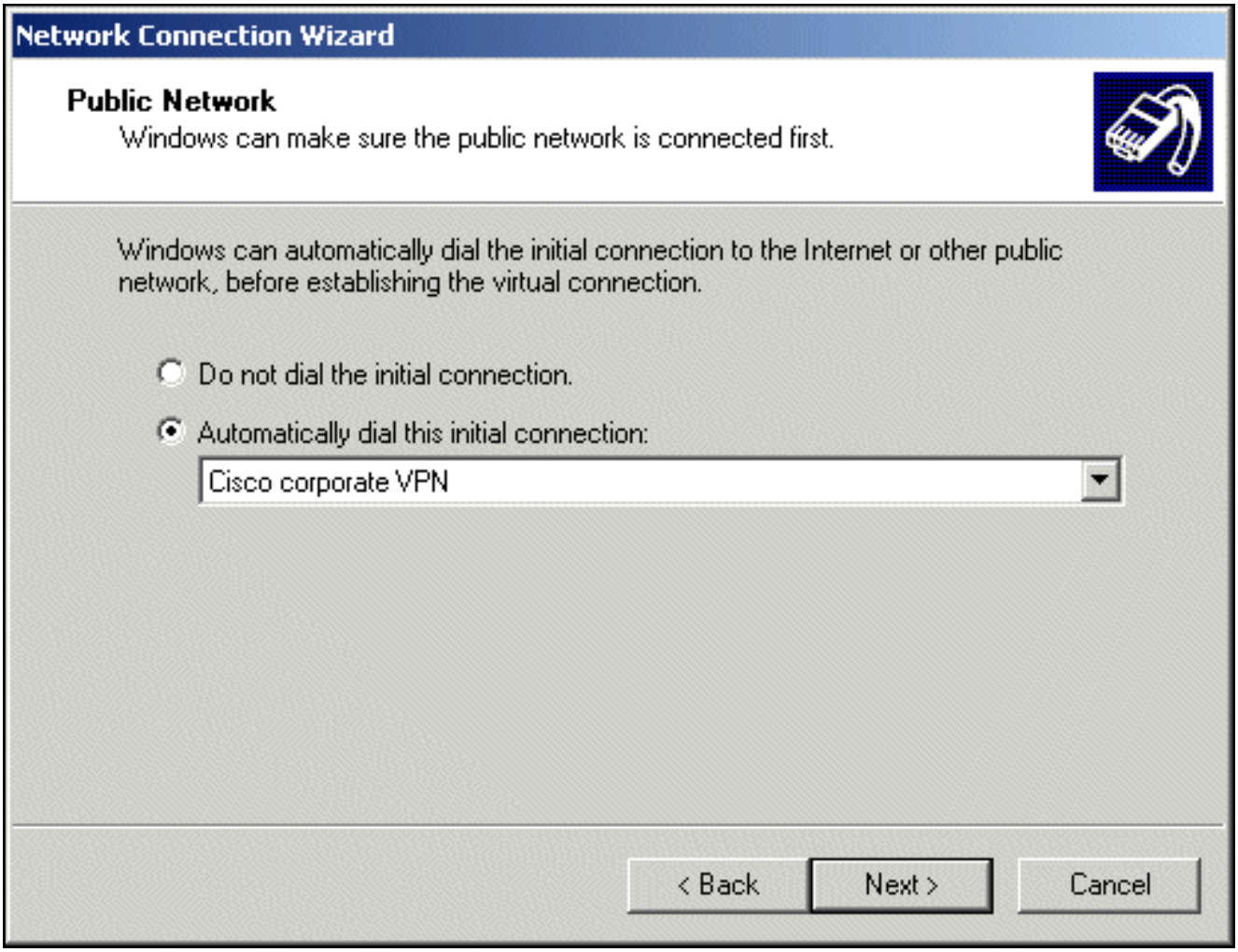
3. VPNコンセントレータのパブリックインターフェイスのホスト名またはIPアドレスを入力し、**Next**をクリックします。



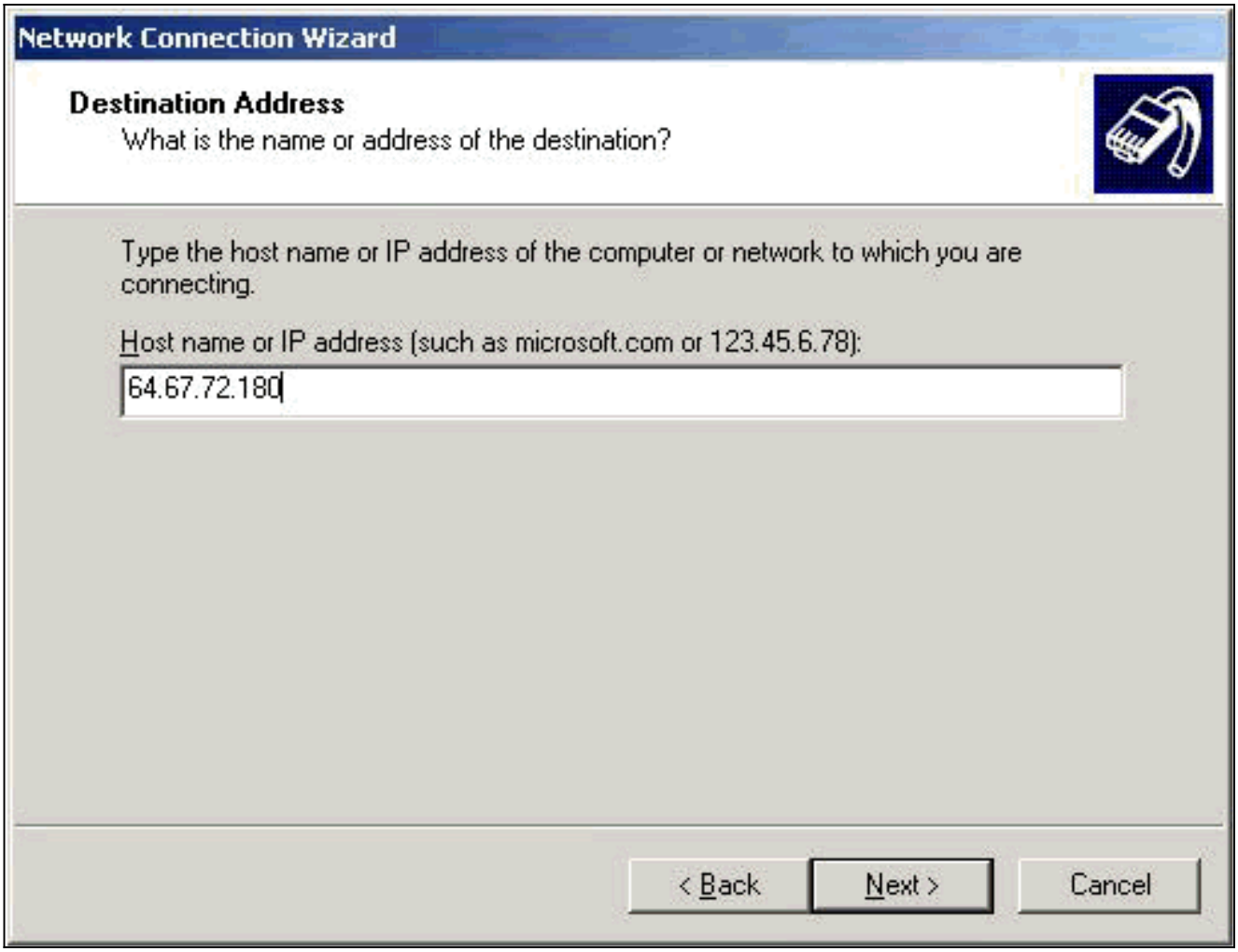
4. [Connection Availability]ウィンドウで、[Only for myself] を選択し、[Next] をクリックします。



5. [パブリックネットワーク(Public Network)]ウィンドウで、最初の接続（ISPアカウント）を自動的にダイヤルするかどうかを選択します。

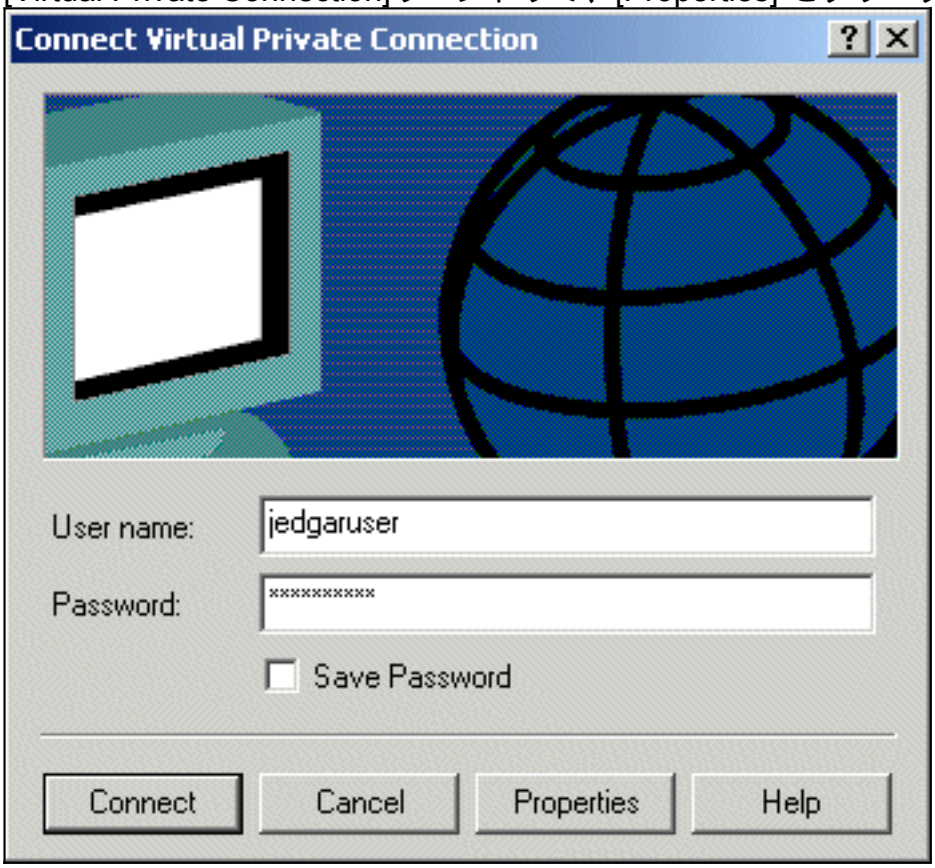


6. Destination Address画面で、VPN 3000コンセントレータのホスト名またはIPアドレスを入力し、**Next**をクリックします。

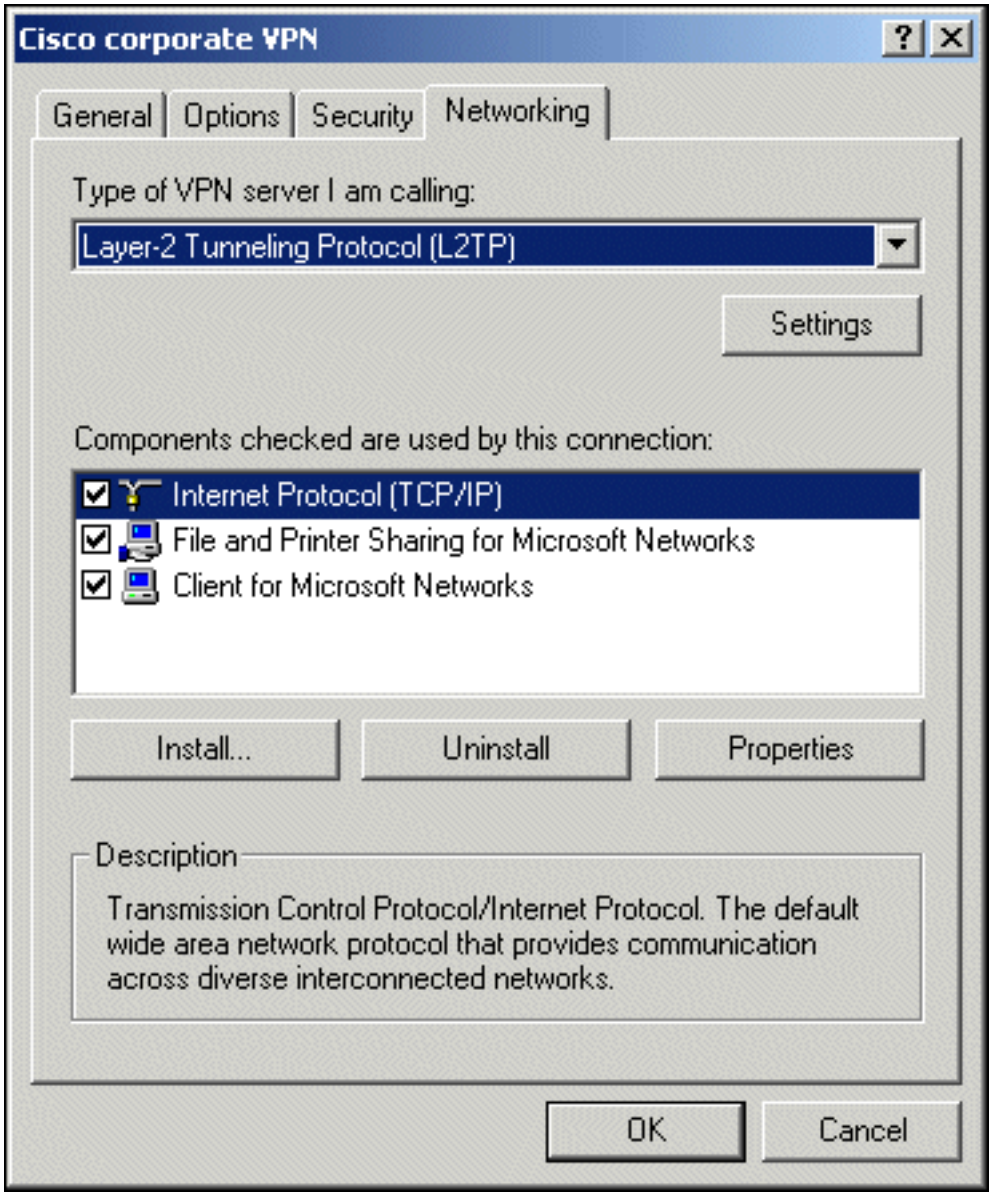


7. [Network Connection Wizard]ウィンドウで、接続の名前を入力し、[Finish] をクリックします。この例では、接続の名前は「Cisco corporate VPN」です。

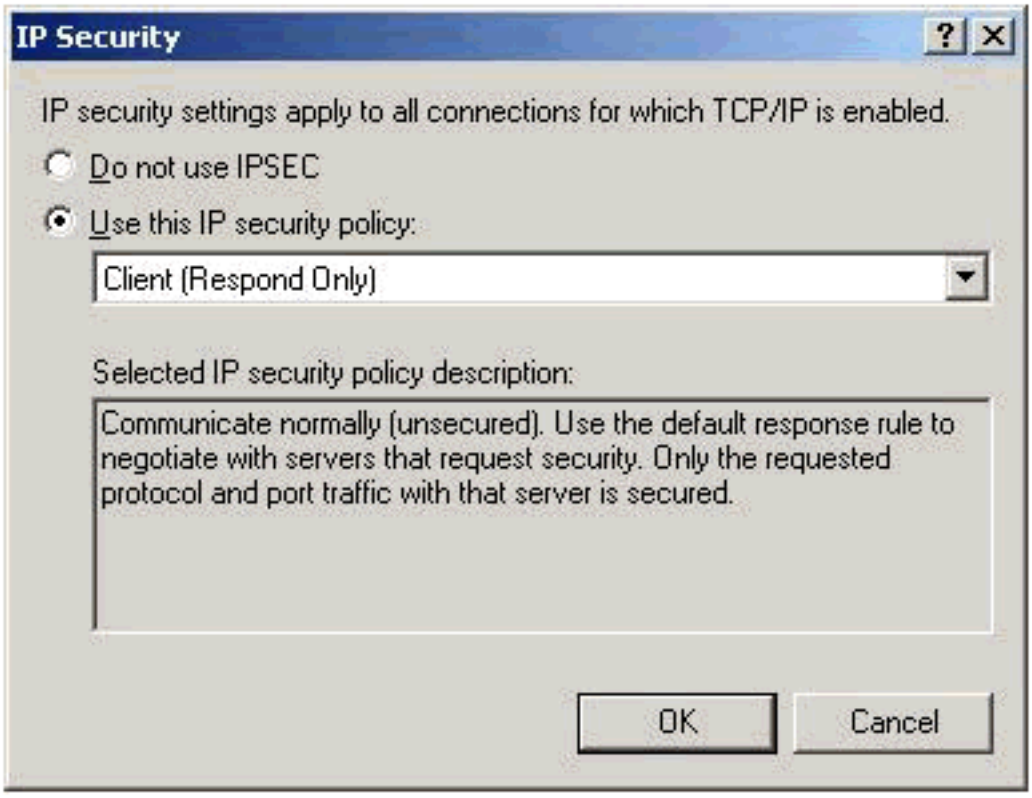
8. [Virtual Private Connection]ウィンドウで、[Properties] をクリックします。



9. Propertiesウィンドウで**Networking**タブを選択します。
10. Type of VPN server I am callingの下で、プルダウンメニューから**L2TP**を選択し、**Internet Protocol TCP/IP**を強調表示して、**Properties**をクリックします。



11. [Advanced] > [Options] > [Properties] を選択します。
12. [IP Security]ウィンドウで、[Use this IP security policy] を選択します。



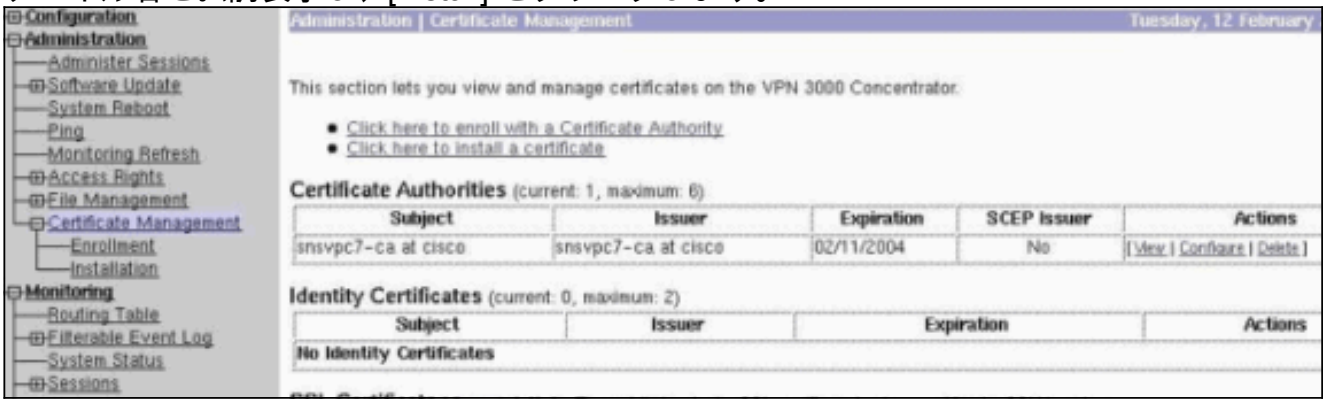
13. プルダウンメニューから**Client (Respond Only)**ポリシーを選択し、[Connect]画面に戻るまで**OK**を何度かクリックします。
14. 接続を開始するには、ユーザ名とパスワードを入力し、**Connect**をクリックします。

VPN 3000 コンセントレータの設定

ルート証明書の取得

VPN 3000コンセントレータのルート証明書を取得するには、次の手順を実行します。

1. ブラウザでCA(通常はhttp://ip_add_of_ca/certsrv/など)を指定し、[Retrieve the CA certificate or certificate revocation list] をクリックして、[Next] をクリックします。
2. [Download CA certificate] をクリックし、ファイルをローカルディスク上の任意の場所に保存します。
3. VPN 3000コンセントレータで、**Administration > Certificate Management**の順に選択し、**Click here to install a certificate**および**Install CA Certificate**をクリックします。
4. [Upload File from Workstation] をクリックします。
5. **Browse**をクリックし、ダウンロードしたCA証明書ファイルを選択します。
6. ファイル名を強調表示し、[Install] をクリックします。



VPN 3000コンセントレータのID証明書の取得

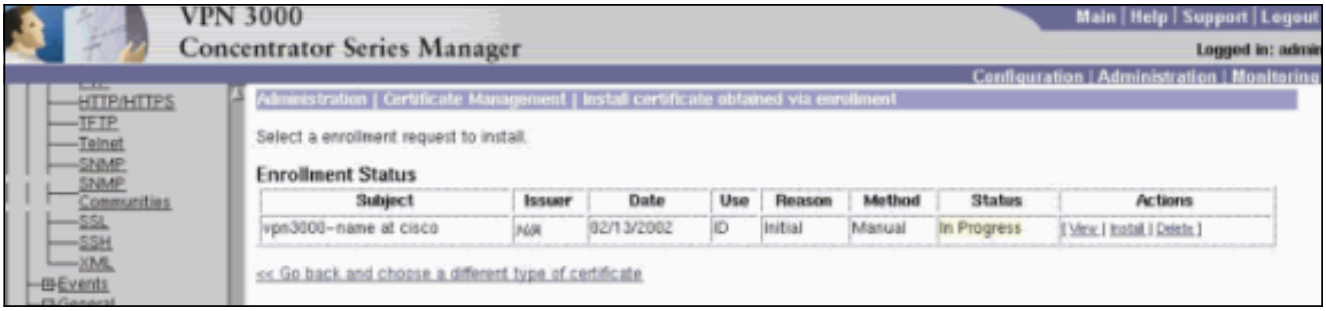
VPN 3000コンセントレータのID証明書を取得するには、次の手順を実行します。

1. [ConfAdministration] > [Certificate Management] > [Enroll] > [Identity Certificate] を選択し、[Enroll via PKCS10 Request (Manual)] をクリックします。 ここに示すようにフォームに入力し、[Enroll] をクリックします。

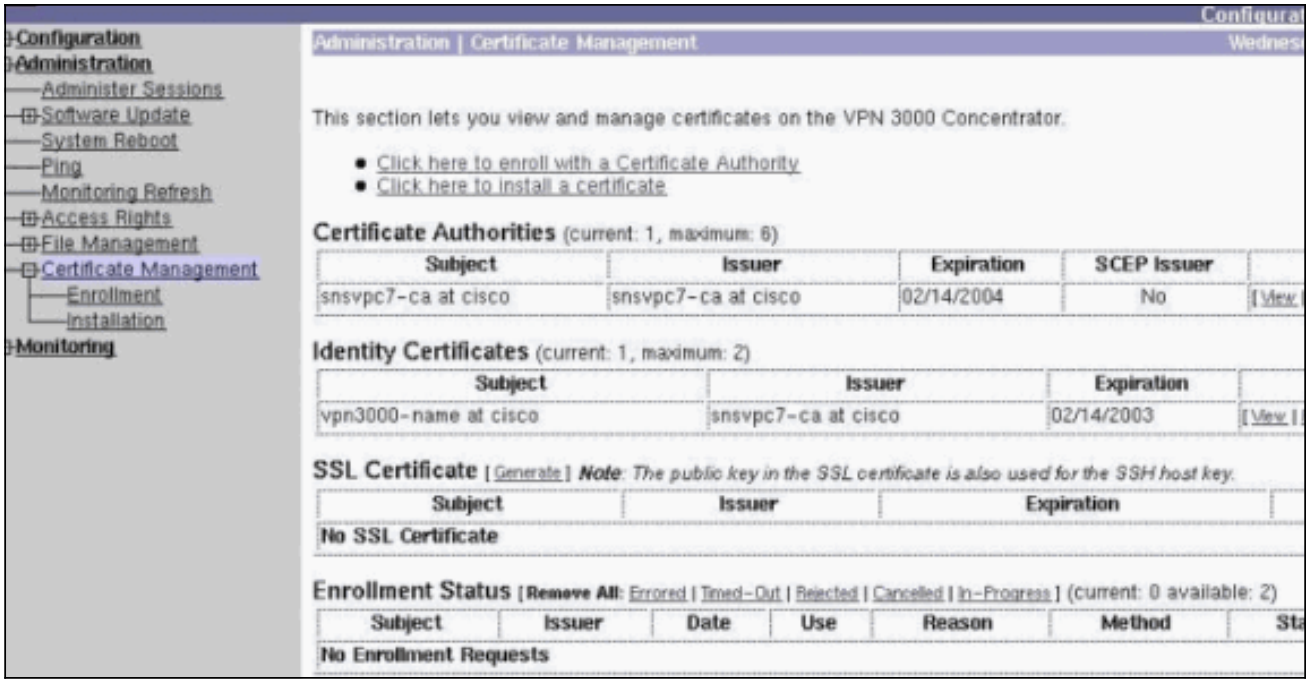
   証明書要求を示すブラウザウィンドウが表示されます。次のようなテキストが必要です。

```
-----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. ブラウザでCAサーバを指定し、[Request a certificate] をオンにして、[Next] をクリックします。
3. [Advanced Request] をオンにし、[Next] をクリックして、[Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file] を選択します。
4. [next] をクリックします。上記のテキスト領域に表示されている証明書要求のテキストをカットアンドペーストします。[Submit] をクリックします。
5. CAサーバの設定方法に基づいて、[Download CA certificate] をクリックできます。または、CAによって証明書が発行されるとすぐに、CAサーバに戻り、[Check on a pending certificate] をオンにします。
6. **Next**をクリックしてリクエストを選択し、再度**Next**をクリックします。
7. [Download CA certificate] をクリックし、ファイルをローカルディスクに保存します。
8. VPN 3000コンセントレータで、**Administration > Certificate Management > Install**の順に選択し、**Install certificate obtained via enrollment**をクリックします。次の図に示すように、保留中の要求のステータスが[In Progress]になります。



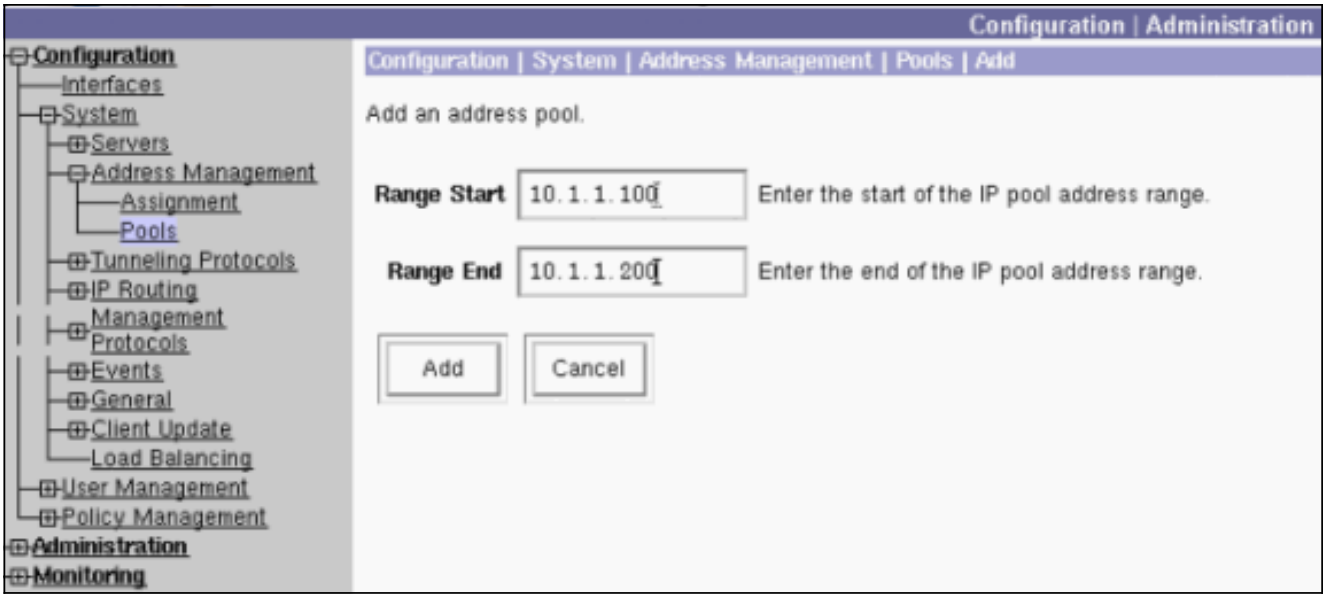
9. [Install] をクリックし、続いて[Upload File from Workstation] をクリックします。
10. [Browse] をクリックし、CAによって発行された証明書を含むファイルを選択します。
11. ファイル名を強調表示し、[Install] をクリックします。
12. [Administration] > [Certificate Management] を選択します。次のような画面が表示されます。



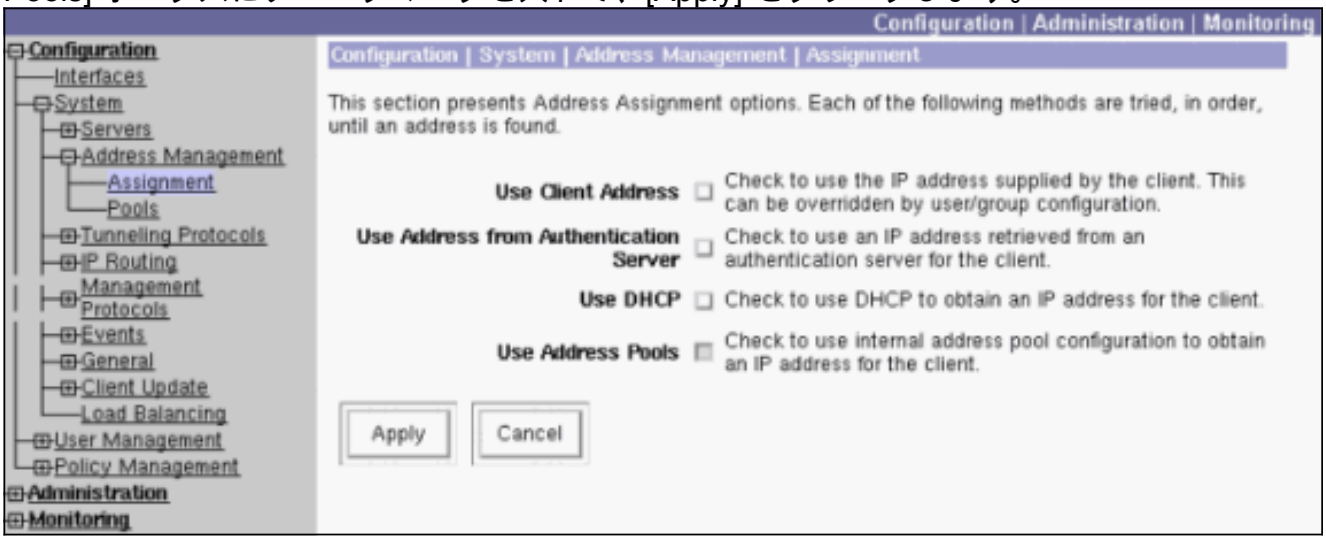
クライアントのプールの設定

クライアントのプールを設定するには、次の手順を実行します。

1. 使用可能なIPアドレスの範囲を割り当てるには、ブラウザでVPN 3000コンセントレータの内部インターフェイスをポイントし、**Configuration > System > Address Management > Pools > Add**の順に選択します。
2. 内部ネットワーク上の他のデバイスと競合しないIPアドレスの範囲を指定し、**Add**をクリックします。



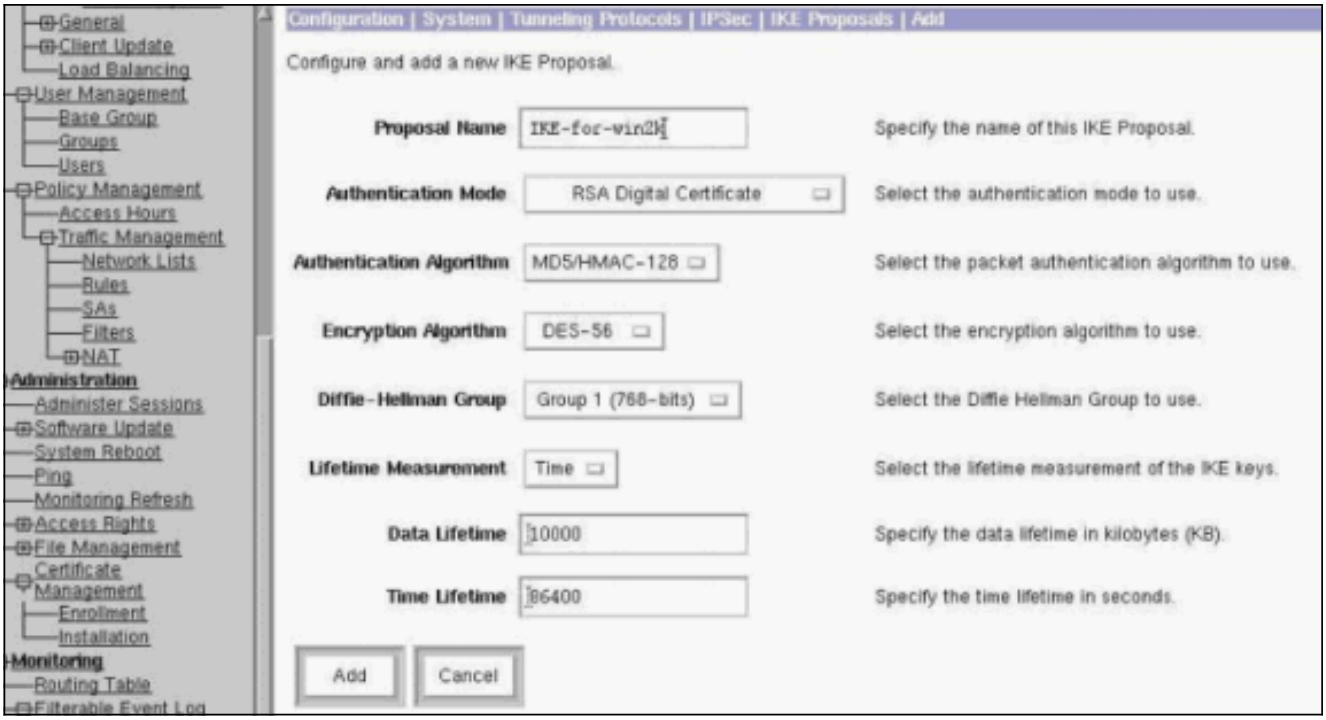
3. プールを使用するようにVPN 3000コンセントレータに指示するには、次の図のように、[Configuration] > [System] > [Address Management] > [Assignment] を選択し、[Use Address Pools] ボックスにチェックマークを入れて、[Apply] をクリックします。



IKEプロポーザルの設定

IKEプロポーザルを設定するには、次の手順を実行します。

1. 次の図に示すように、[Configuration] > [System] > [Tunneling Protocols] > [IPSec] > [IKE Proposals] を選択し、[Add] をクリックしてパラメータを選択します。



2. **Add**をクリックし、右側の列で新しい提案を強調表示して、**Activate**をクリックします。

SAの設定

セキュリティアソシエーション(SA)を設定するには、次の手順を実行します。

1. **Configuration > Policy Management > Traffic Management > SA**の順に選択し、**ESP-L2TP-TRANSPORT**をクリックします。このSAが使用できない場合、または他の目的で使用する場合は、このSAと同様の新しいSAを作成します。SAに対して異なる設定を使用できます。セキュリティポリシーに基づいて、このパラメータを変更します。
2. [Digital Certificate] プルダウンメニューで、以前に設定したデジタル証明書を選択します。**IKE-for-win2k** Internet Key Exchange(IKE)プロポーザルを選択します。**注：これ**は必須ではありません。L2TP/IPSecクライアントがVPNコンセントレータに接続する際には、[Configuration] > [System] > [Tunneling Protocols] > [IPSec] > [IKE Proposals] ページの [active]列で設定されているすべてのIKEプロポーザルが順番に試行されます。次の図に、SAに必要な設定を示します。

グループとユーザの設定

グループとユーザを設定するには、次の手順を実行します。

1. [Configuration] > [User Management] > [Base Group] を選択します。
2. Generalタブで、**L2TP over IPSec**にチェックマークが付いていることを確認します。
3. [IPSec]タブで、[ESP-L2TP-TRANSPORT] SAを選択します。
4. [PPTP/L2TP]タブで、[L2TP Encryption] オプションをすべてオフにします。
5. **Configuration > User Management > Users**の順に選択し、**Add**をクリックします。
6. Windows 2000クライアントからの接続に使用する名前とパスワードを入力します。Group Selectionで**Base Group**を選択していることを確認します。
7. Generalタブで、**L2TP over IPSec**トンネリングプロトコルをチェックします。
8. [IPSec]タブで、[ESP-L2TP-TRANSPORT] SAを選択します。
9. [PPTP/L2TP]タブで、[L2TP Encryption] オプションをすべてオフにして、[Add] をクリックします。これで、L2TP/IPSec Windows 2000クライアントを使用して接続できます。**注：**リモートL2TP/IPSec接続を受け入れるようにベースグループを設定することを選択しました。SAのOrganization Unit（OU；組織単位）フィールドに一致するグループを設定して、着信接続を受け入れることもできます。設定は同じです。

デバッグ情報

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

271 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3869 10.48.66.76
```

```
  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

274 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3870 10.48.66.76
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

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

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

285 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3873 10.48.66.76
  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

288 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3874 10.48.66.76
  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

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

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

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

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

303 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3879 10.48.66.76
  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

306 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3880 10.48.66.76
  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

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

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

315 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3883 10.48.66.76
  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

318 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3884 10.48.66.76
  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

321 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3885 10.48.66.76
  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

324 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3886 10.48.66.76
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

329 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3887 10.48.66.76
  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

332 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3888 10.48.66.76
  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

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

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

341 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3891 10.48.66.76
  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

344 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3892 10.48.66.76
  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

347 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3893 10.48.66.76
  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

350 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3894 10.48.66.76
  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

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

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

358 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3897 10.48.66.76
  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

361 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3898 10.48.66.76
  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

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

367 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3900 10.48.66.76
  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

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

372 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3902 10.48.66.76
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

377 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3903 10.48.66.76
  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

380 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3904 10.48.66.76
  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

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

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

389 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3907 10.48.66.76
  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

392 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3908 10.48.66.76
  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

395 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3909 10.48.66.76
  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

398 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3910 10.48.66.76
  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
```

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

404 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3912 10.48.66.76
  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

407 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3913 10.48.66.76
  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

410 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3914 10.48.66.76
  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

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

416 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3916 10.48.66.76
  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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

442 02/15/2002 12:47:24.610 SEV=8 IKEDBG/0 RPT=3927 10.48.66.76
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

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

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

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

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

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

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

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

454 02/15/2002 12:47:24.650 SEV=9 IKEDBG/23 RPT=20 10.48.66.76
```

```
Starting group lookup for peer 10.48.66.76

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

474 02/15/2002 12:47:24.800 SEV=6 IKE/121 RPT=4 10.48.66.76
```

```
Keep-alive type for this connection: None

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

496 02/15/2002 12:47:24.810 SEV=8 IKEDBG/6 RPT=4
```

```
IKE got SPI from key engine: SPI = 0x10d19e33

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

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

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

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

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

502 02/15/2002 12:47:24.820 SEV=7 IKEDBG/0 RPT=3948 10.48.66.76
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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

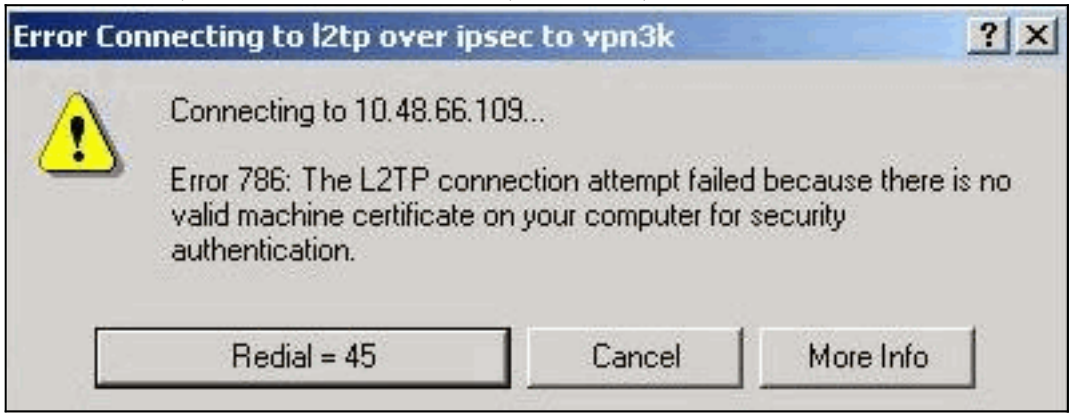
トラブルシューティング情報

このセクションでは、いくつかの一般的な問題とそれぞれのトラブルシューティング方法について説明します。

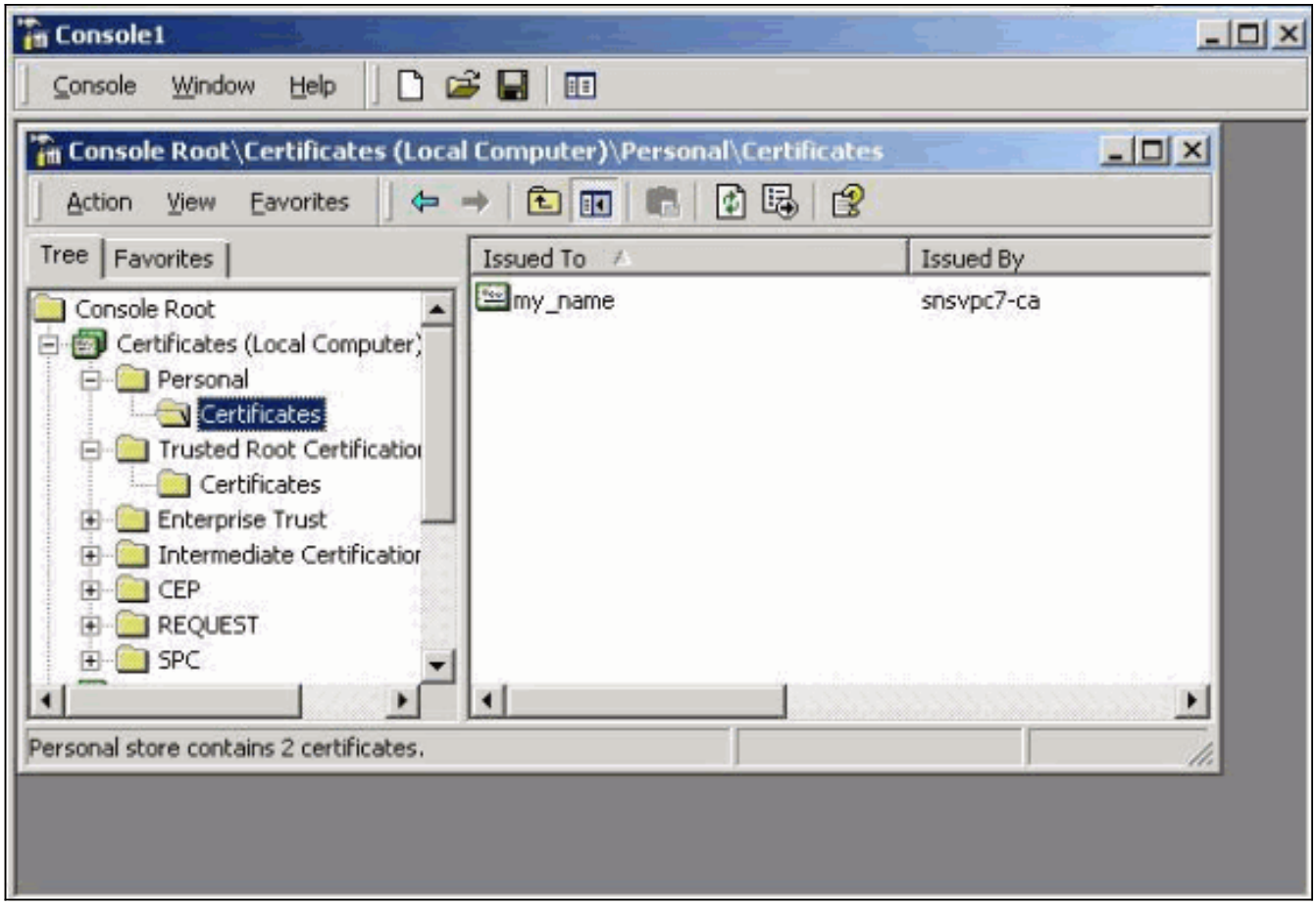
- サーバーを起動できません。

ほとんどの場合、IPSecサービスは開始されていません。[Start] > [Programs] > [Administrative tools] > [Service] を選択し、**IPSecサービス**が有効になっていることを確認します。

- Error 786:有効なコンピューター証明書がありません。



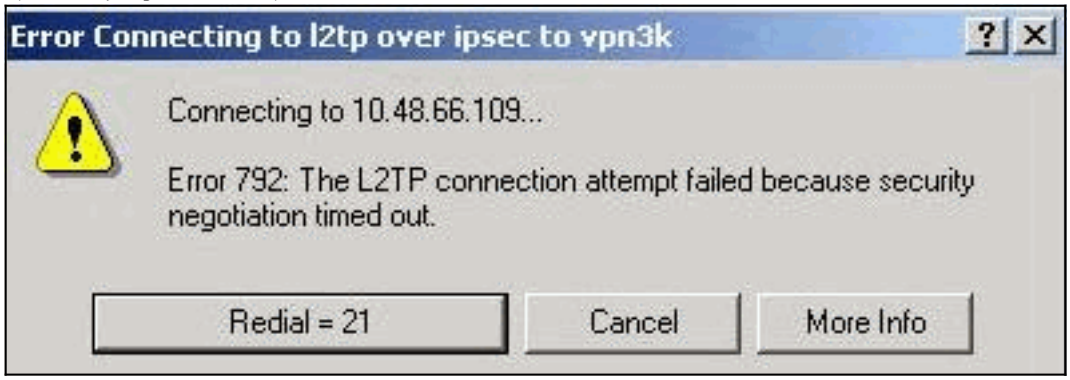
このエラーは、ローカルコンピューターの証明書に問題があることを示しています。証明書を簡単に確認するには、[Start] > [Run] を選択し、MMCを実行します。**Console**をクリックし、**Add/Remove Snap-in**を選択します。**Add**をクリックし、リストから**Certificate**を選択します。証明書の範囲を確認するウィンドウが表示されたら、[Computer Account] を選択します。これで、CAサーバの証明書が[Trusted Root Certification Authorities] の下にあることを確認できます。次の図に示すように、[Console Root] > [Certificate (Local Computer)] > [Personal] > [Certificates] を選択して、証明書があることを確認することもできます。



証明書をクリックします。すべてが正しいことを確認します。この例では、証明書に関連付けられた秘密キーがあります。ただし、この証明書は期限切れです。これが問題の原因です

。

- Error 792:セキュリティネゴシエーションのタイムアウト。このメッセージは長い時間が経過すると表示されます。



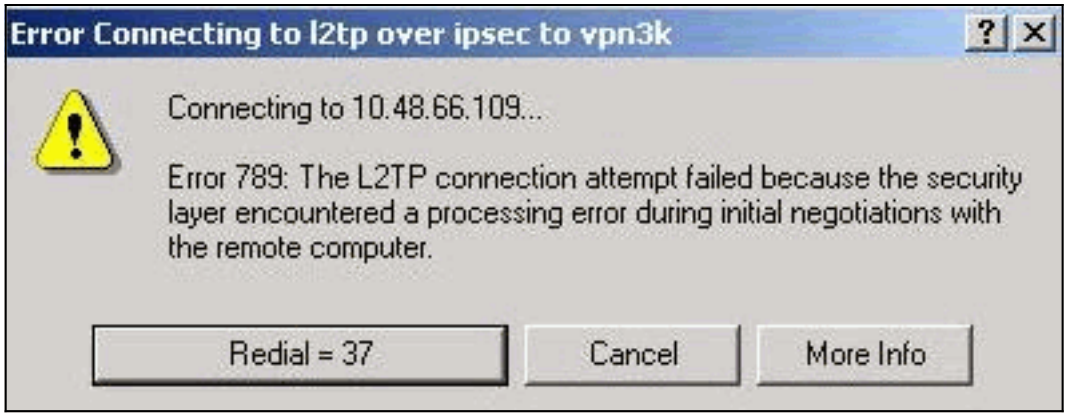
「Cisco VPN 3000コンセントレータに関するFAQ」で説明されている該当するデバッグをオンにします。最後まで読みなさい。次のような出力が表示される必要があります。

```
9337 02/15/2002 15:06:13.500 SEV=8 IKEDBG/0 RPT=7002 10.48.66.76
  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

9340 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7003 10.48.66.76
```

```
  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

9343 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7004 10.48.66.76
  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

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

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

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

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

これは、IKEプロポーザルが正しく設定されていないことを示します。このドキュメントの「IKEプロポーザルの設定」セクションの情報を確認します。

- Error 789:セキュリティ層で処理エラーが発生しました。



「Cisco VPN 3000コンセントレータに関するFAQ」で説明されている該当するデバッグをオンにします。最後まで読みなさい。次のような出力が表示される必要があります。

```
11315 02/15/2002 15:36:32.030 SEV=8 IKEDBG/0 RPT=7686
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

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

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

- 使用バージョン[Monitoring] > [System Status] を選択して、次の出力を表示します。

```
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
```

関連情報

- IPSecネゴシエーション/IKEプロトコル製品に関するサポートページ
- テクニカルサポート - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。