L2TP Over IPsec Between Windows 2000 and VPN 3000 Concentrator Using Digital Certificates Configuration Example

Document ID: 14117

Contents

Introduction

This document shows the step−by−step procedure used to connect to a VPN 3000 Concentrator from a Windows 2000 client using the L2TP/IPSec built−in client. It is assumed that you use digital certificates (stand−alone root Certification Authority (CA) without Certificate Enrollment Protocol (CEP)) to authenticate your connection to the VPN Concentrator. This document uses the Microsoft Certificate Service for illustration. Refer to the Microsoft website for documentation on how to configure it.

Note: This is an example only because the appearance of the Windows 2000 screens can change.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is for the Cisco VPN 3000 Concentrator series.

Objectives

In this procedure, you complete these steps:

1. Obtain a root certificate.
2. Obtain an identity certificate for the client.
3. Create a connection to the VPN 3000 with the help of the Network Connection Wizard.
4. Configure the VPN 3000 Concentrator.

Conventions

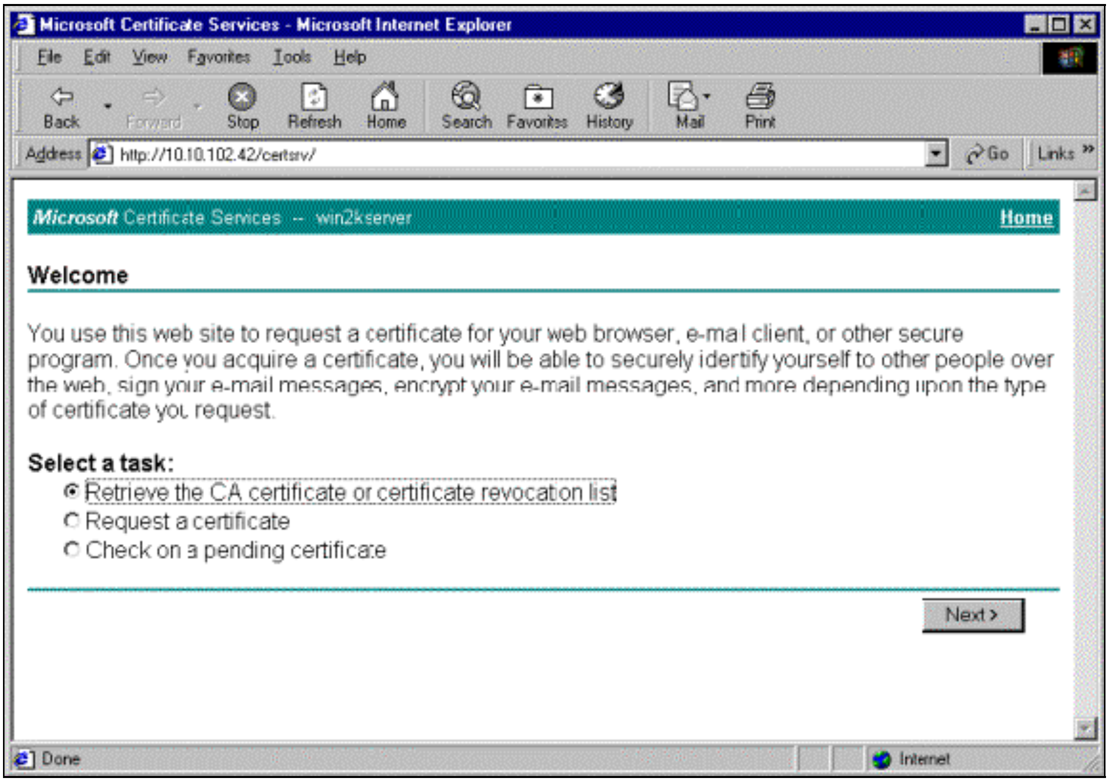
For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Obtain a Root Certificate

Complete these instructions in order to obtain a root certificate:

1. Open a browser window and type in the URL for the Microsoft Certificate Authority (usually http://servername or the IP address of CA/certsrv).

   The Welcome window for certificate retrievals and requests displays.
2. On the Welcome window under Select a task, choose **Retrieve the CA certificate or certificate revocation list** and click **Next**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Address http://10.10.102.42/certsrv/
Go
Links
Microsoft Certificate Services -- win2kserver
Home
Next >
Done
Internet

Welcome

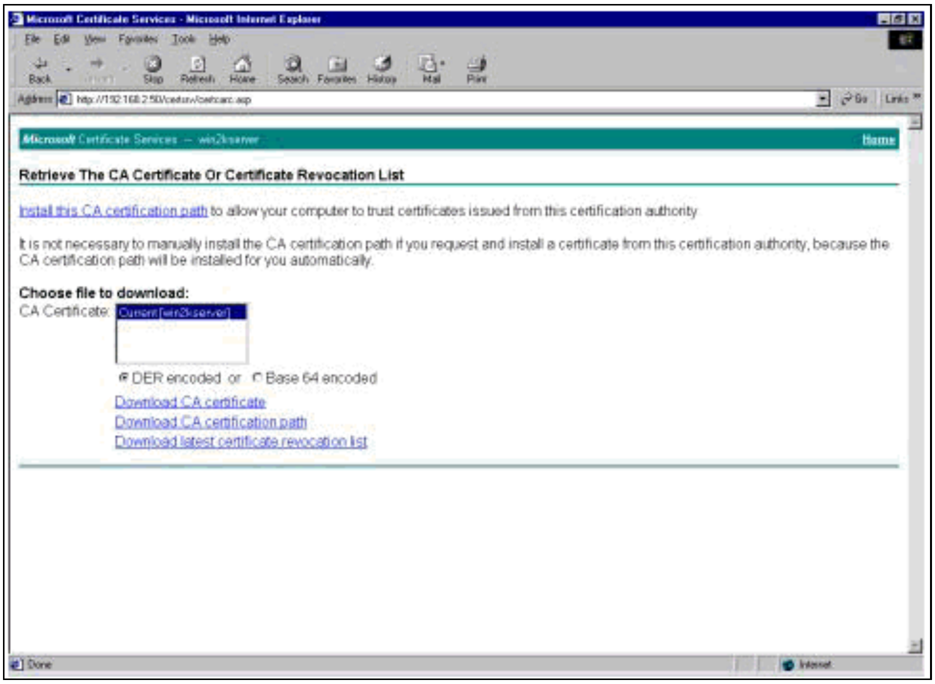
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

● Retrieve the CA certificate or certificate revocation list
○ Request a certificate
○ Check on a pending certificate

3. From the Retrieve the CA certificate or certificate revocation list window, click **Install this CA certification path** in the left corner.

   This adds the CA certificate to the Trusted Root Certificate Authorities store. This means that any certificates this CA issues to this client are trusted.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.2.50/certsrv/certcarc.asp
Go Links
Microsoft Certificate Services -- win2kserver
Home
Done
Internet

Retrieve The CA Certificate Or Certificate Revocation List

Install this CA certification path to allow your computer to trust certificates issued from this certification authority

It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.

Choose file to download:

CA Certificate: Current [win2kserver]

● DER encoded or ○ Base 64 encoded

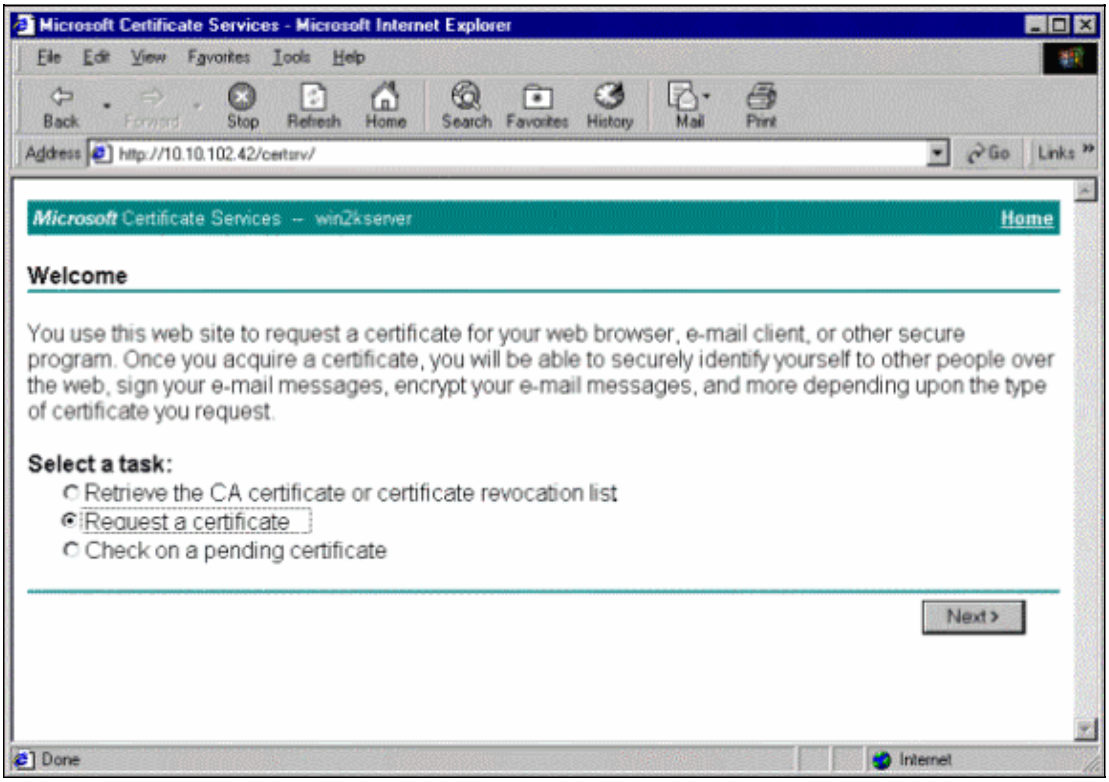
Download CA certificate
Download CA certification path
Download latest certificate revocation list

Obtain an Identity Certificate for the Client

Complete these steps in order to obtain an identity certificate for the client:

1. Open a browser window and enter the URL for the Microsoft Certificate Authority (usually http://servername or IP address of CA/certsrv).

   The Welcome window for certificate retrievals and requests displays.
2. From the Welcome window, under Select a task, choose **Request a certificate**, and click **Next**.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://10.10.102.42/certsrv/
Go Links
Microsoft Certificate Services -- win2kserver
Home
Next >
Done
Internet

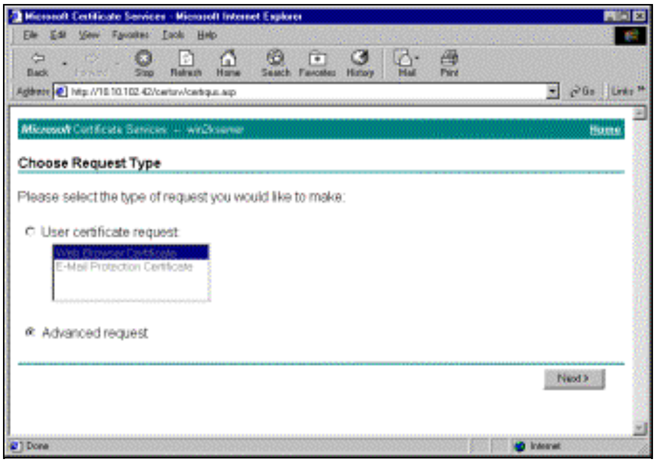
Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list
● Request a certificate
○ Check on a pending certificate

3. From the Choose Request Type window, select **Advanced request** and click **Next**.



Microsoft Certificate Services - Microsoft Internet Explorer

Address: http://10.10.102.42/certsrv/certrqus.asp

Microsoft Certificate Services -- win2kserver — Home

Choose Request Type

Please select the type of request you would like to make:

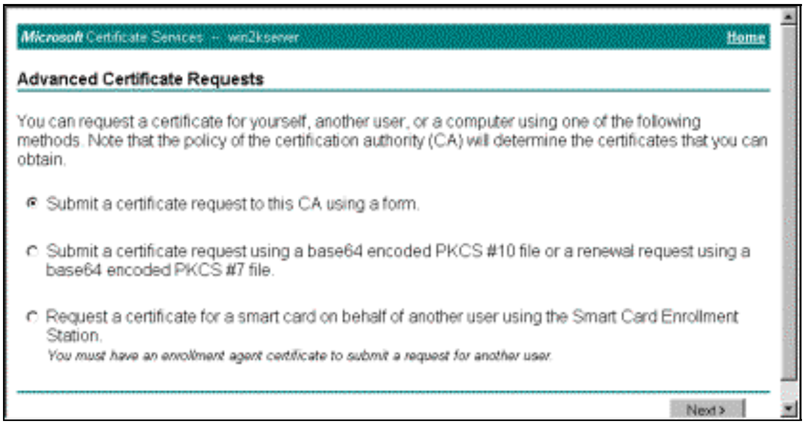
○ User certificate request:

Web Browser Certificate
E-Mail Protection Certificate

● Advanced request

Next >

4. From the Advanced Certificate Requests window, select **Submit a certificate request to this CA using a form**.



Microsoft Certificate Services -- win2kserver — Home

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

● Submit a certificate request to this CA using a form.

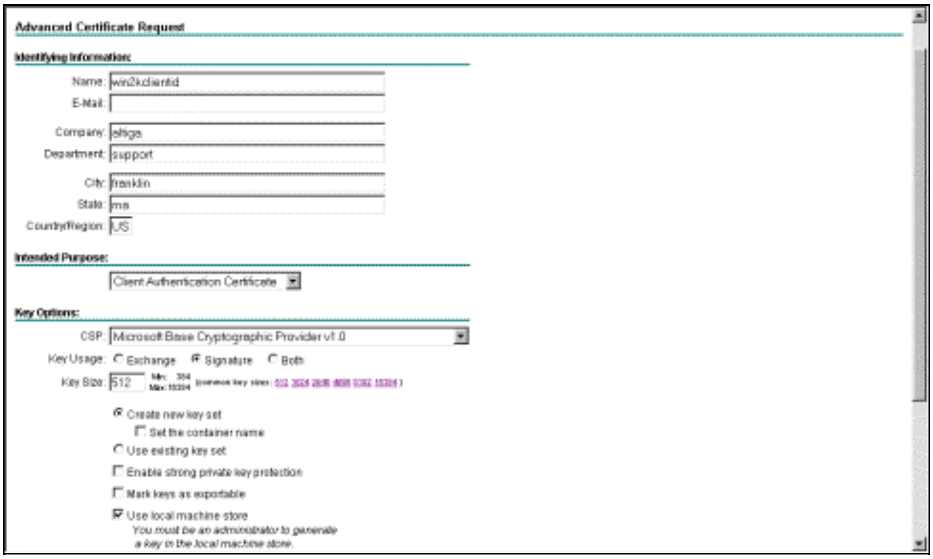
○ Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

○ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

Next >

5. Fill in the fields as in this example.

   The value for Department (organizational unit) needs to match the group configured on the VPN Concentrator. Do not specify a key size larger than 1024. Be sure to select the checkbox for **Use local machine store**. When you are finished, click **Next**.



Advanced Certificate Request

Identifying Information:

Name: win2kclientid
E-Mail:
Company: aftiga
Department: support
City: franklin
State: ma
Country/Region: US

Intended Purpose:

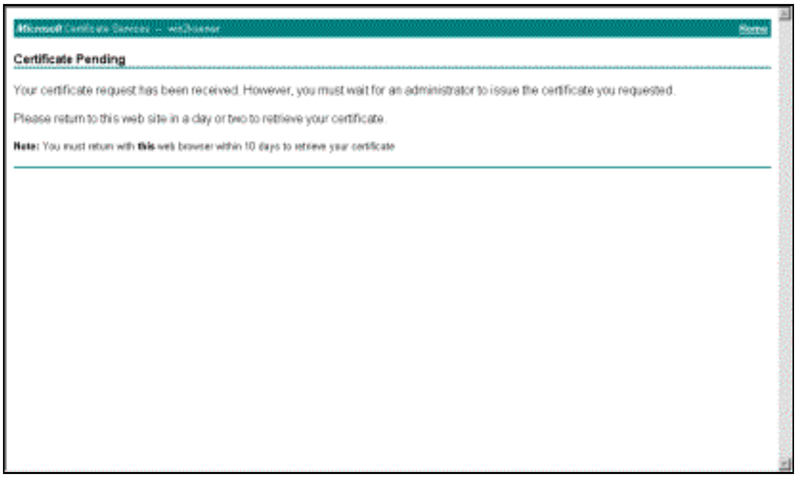
Client Authentication Certificate

Key Options:

CSP: Microsoft Base Cryptographic Provider v1.0
Key Usage: ○ Exchange ● Signature ○ Both
Key Size: 512 Min: 384 Max: 16384 (common key sizes: 512 1024 2048 4096 8192 16384)

● Create new key set
□ Set the container name
○ Use existing key set
□ Enable strong private key protection
□ Mark keys as exportable
☑ Use local machine store
You must be an administrator to generate a key in the local machine store.

Based on how the CA server is configured, this window sometimes appears. If it does, contact the CA administrator.



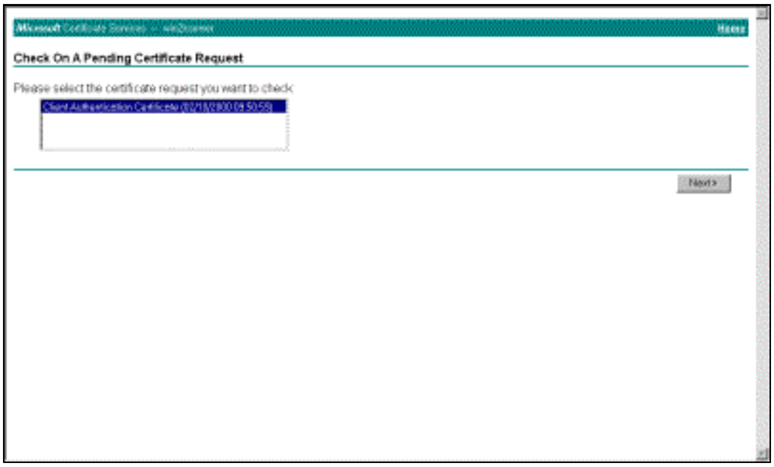
Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with **this** web browser within 10 days to retrieve your certificate

6. Click **Home** to get back to the main screen, select **Check on pending certificate**, and click **Next**.

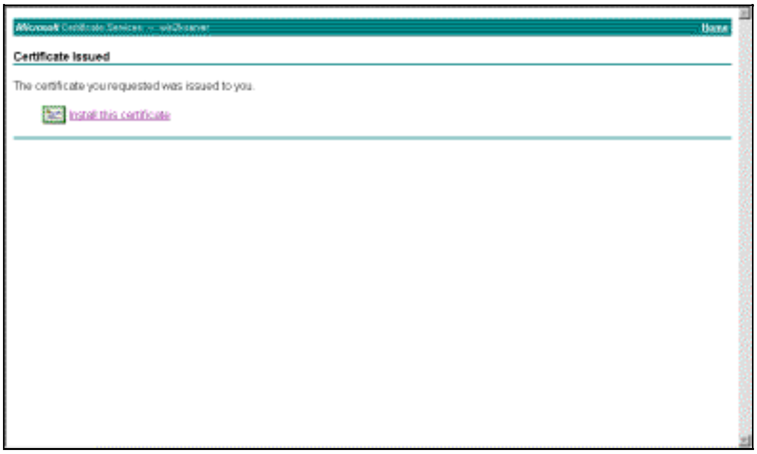


Check On A Pending Certificate Request

Please select the certificate request you want to check:

Client Authentication Certificate (02/18/2000 09:50:55)

7. On the Certificate Issued window, click **Install this certificate**.

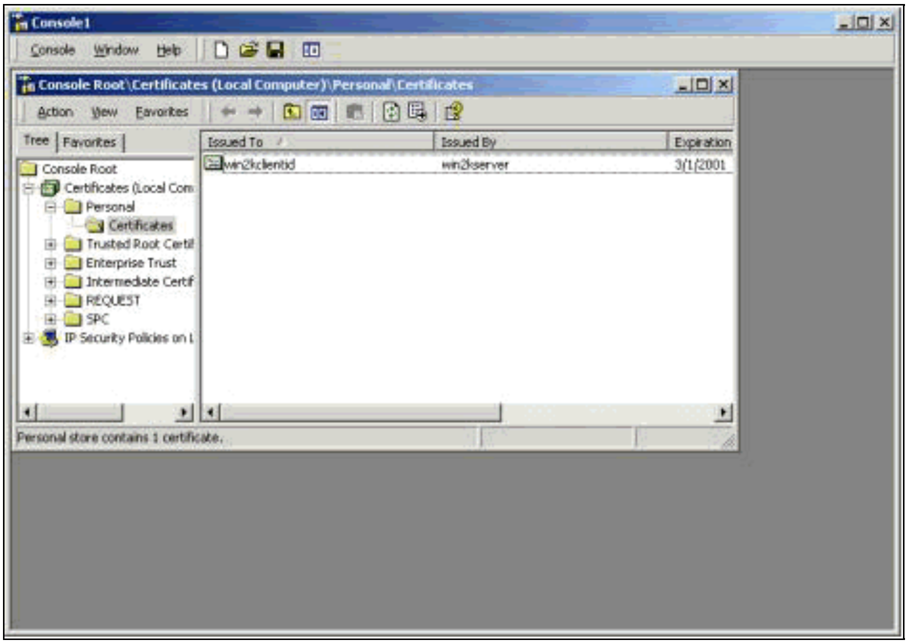


Certificate Issued

The certificate you requested was issued to you.

Install this certificate

8. In order to view your client certificate, select **Start** > **Run**, and perform Microsoft Management Console (MMC).
9. Click **Console** and choose **Add/Remove Snap−in**.
10. Click **Add** and choose **Certificate** from the list.
11. When a window appears that asks you the scope of the certificate, choose **Computer Account**.
12. Verify that the certificate of the CA server is located under the Trusted Root Certification Authorities. Also verify that you have a certificate by selecting **Console Root** > **Certificate (Local Computer)** > **Personal** > **Certificates**, as shown in this image.



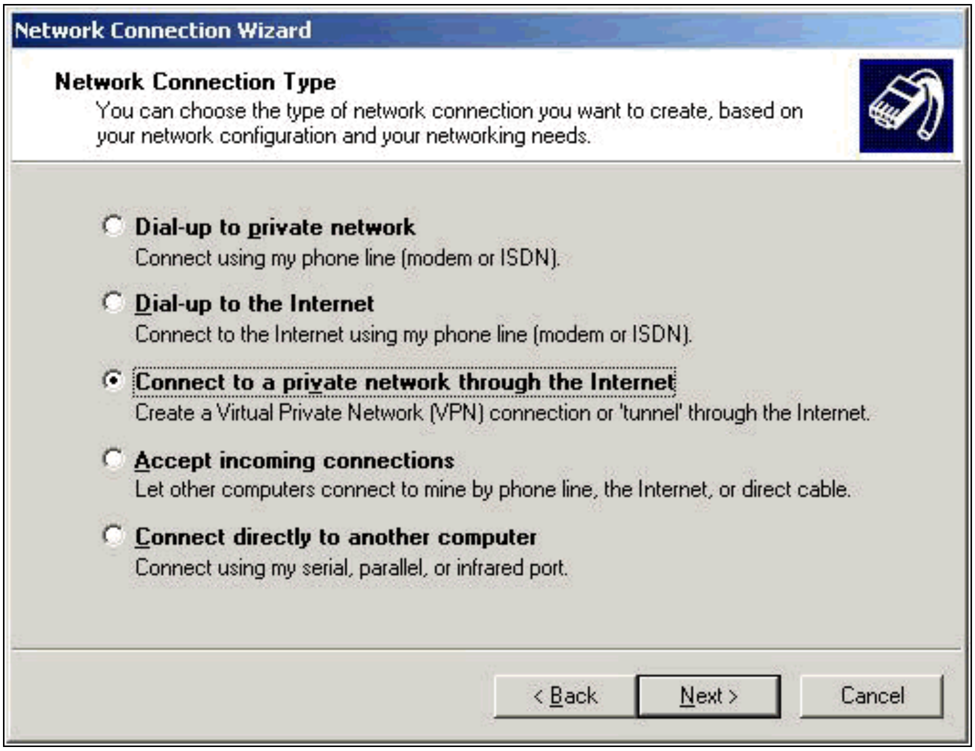
Issued To	Issued By	Expiration
win2kclientid	win2kserver	3/1/2001

Personal store contains 1 certificate.

Create a Connection to the VPN 3000 Using the Network Connection Wizard

Complete this procedure in order to create a connection to the VPN 3000 with the help of the network connection wizard:

1. Right−click **My Network Places**, choose **Properties** and click **Make New Connection**.
2. From the Network Connection Type window, choose **Connect to a private network through the Internet** and then click **Next**.



Network Connection Type
You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

○ **Dial-up to private network**
Connect using my phone line (modem or ISDN).

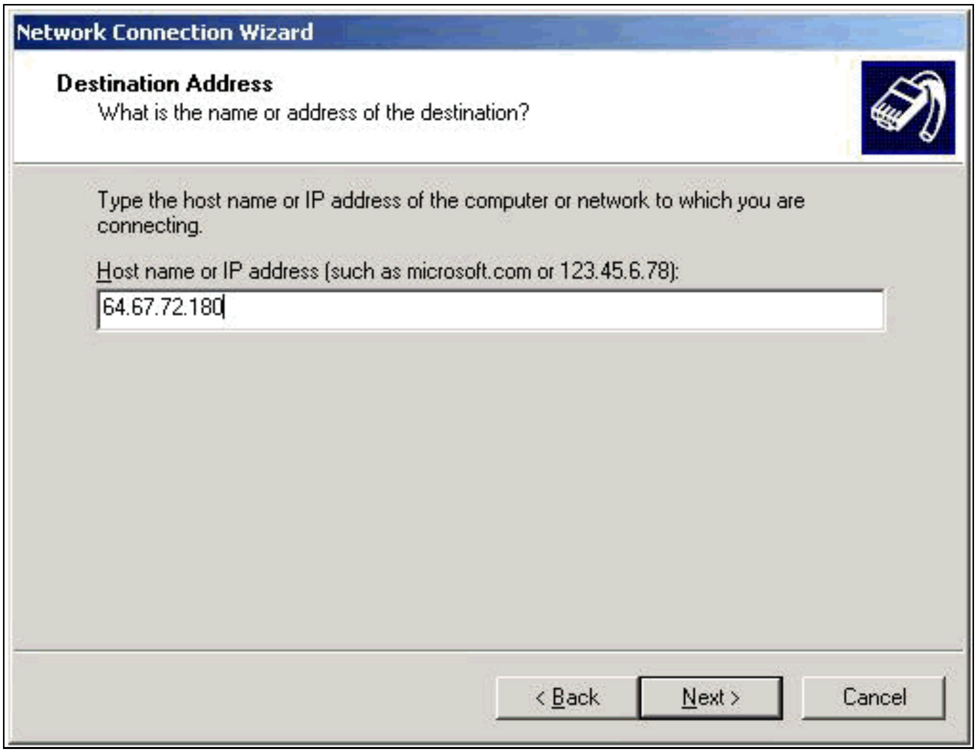
○ **Dial-up to the Internet**
Connect to the Internet using my phone line (modem or ISDN).

● **Connect to a private network through the Internet**
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.

○ **Accept incoming connections**
Let other computers connect to mine by phone line, the Internet, or direct cable.

○ **Connect directly to another computer**
Connect using my serial, parallel, or infrared port.

3. Enter the host name or IP address of the public interface of the VPN Concentrator, and click **Next**.



Network Connection Wizard

Destination Address

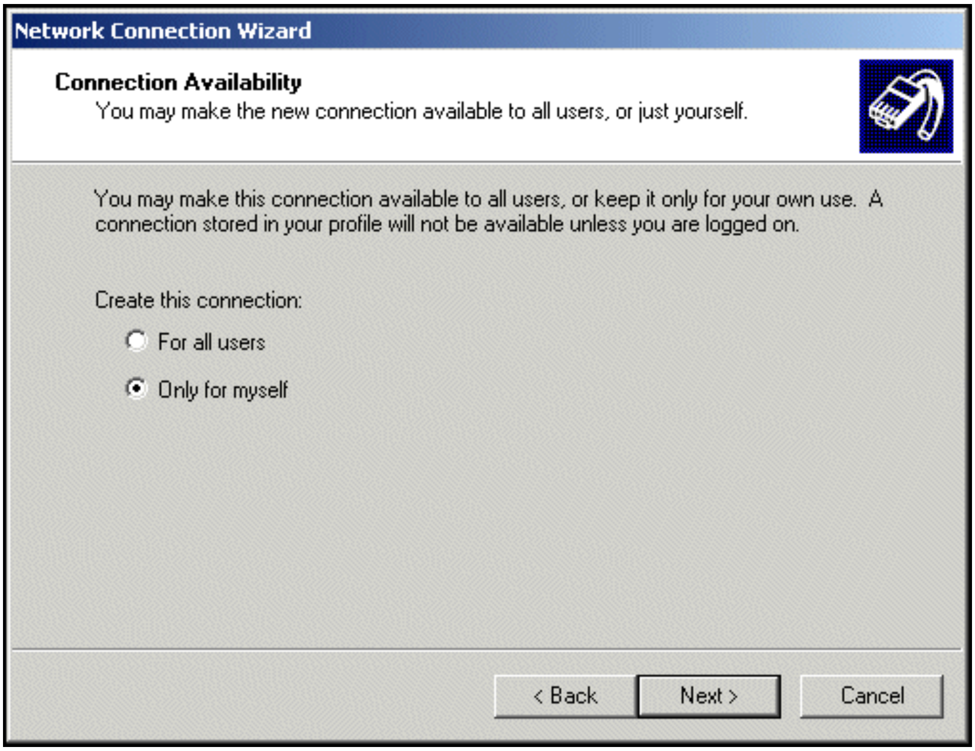
What is the name or address of the destination?

Type the host name or IP address of the computer or network to which you are connecting.

Host name or IP address (such as microsoft.com or 123.45.6.78):

64.67.72.180

4. On the Connection Availability window, select **Only for myself** and click **Next**.



Network Connection Wizard

Connection Availability

You may make the new connection available to all users, or just yourself.

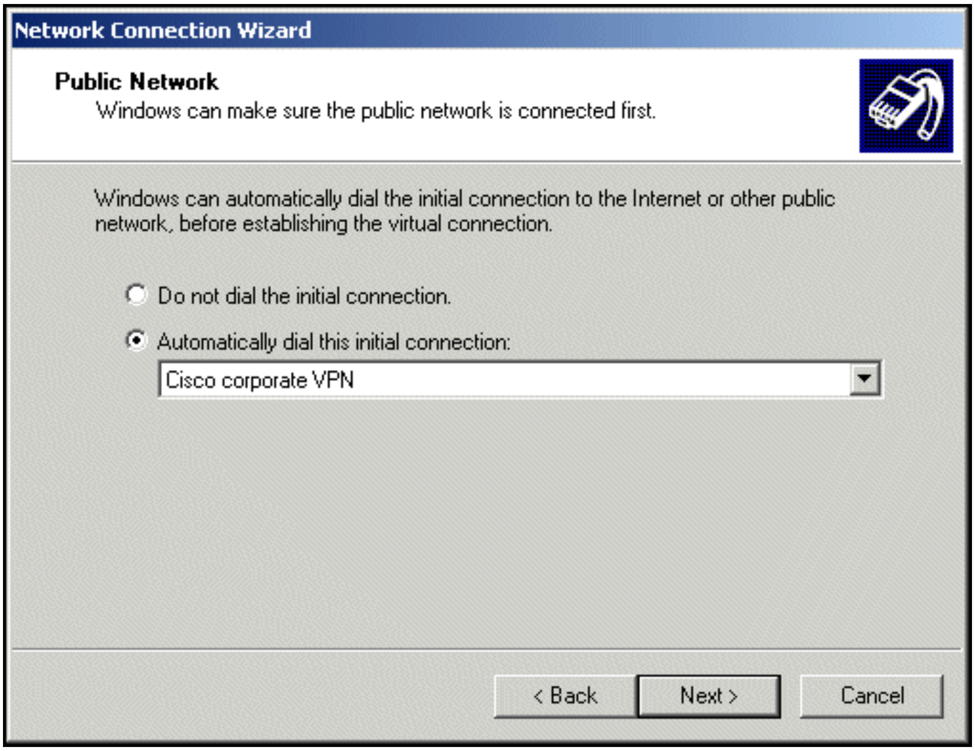
You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.

Create this connection:

○ For all users

● Only for myself

5. On the Public Network window, select whether to dial the initial connection (the ISP account) automatically.


Network Connection Wizard

Public Network

Windows can make sure the public network is connected first.

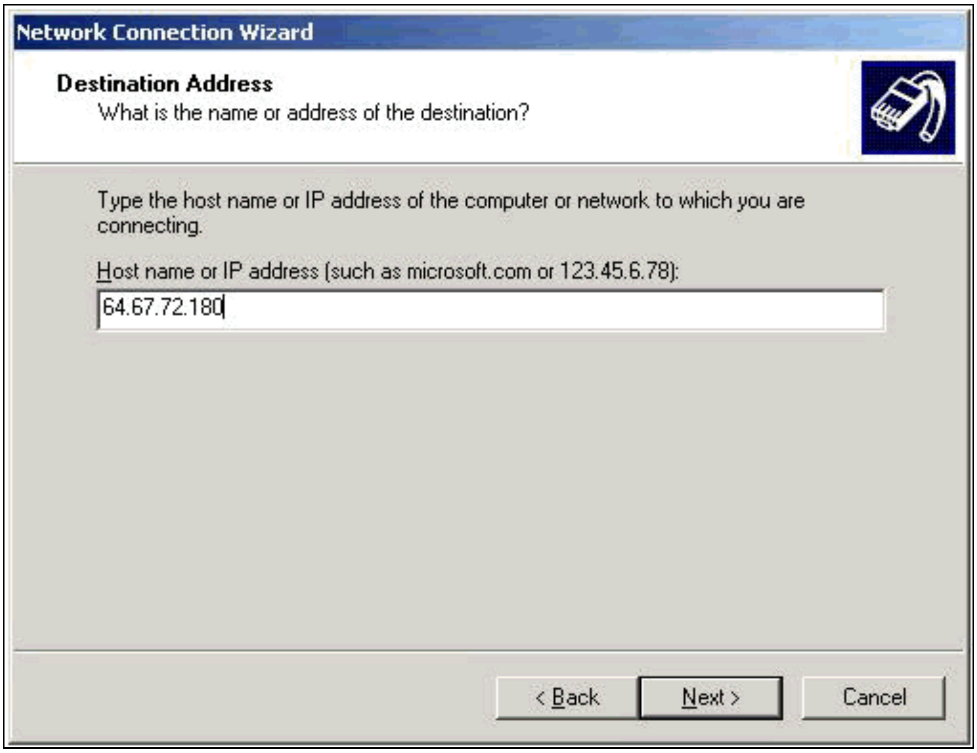
Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

○ Do not dial the initial connection.

● Automatically dial this initial connection:

Cisco corporate VPN

6. On the Destination Address screen, enter the host name or IP address of the VPN 3000 Concentrator, and click **Next**.


Network Connection Wizard

Destination Address

What is the name or address of the destination?

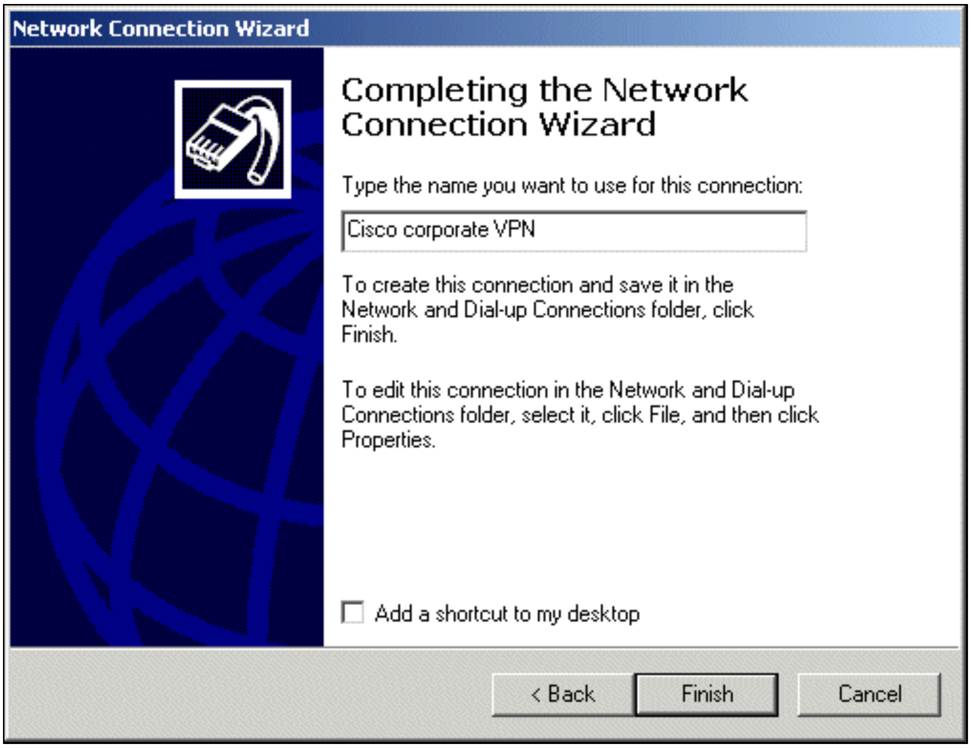
Type the host name or IP address of the computer or network to which you are connecting.

Host name or IP address (such as microsoft.com or 123.45.6.78):

64.67.72.180

7. On the Network Connection Wizard window, enter a name for the connection and click **Finish**.

   In this example, the connection is named "Cisco corporate VPN."



Network Connection Wizard

Completing the Network Connection Wizard

Type the name you want to use for this connection:

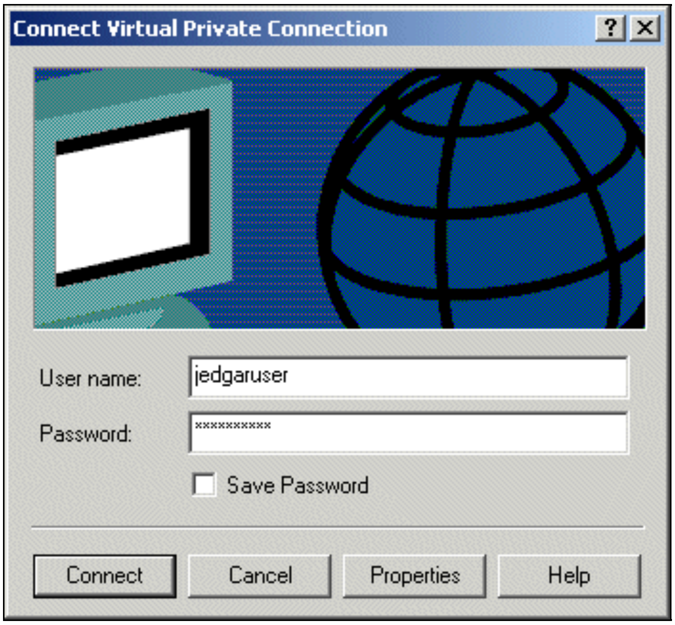
Cisco corporate VPN

To create this connection and save it in the Network and Dial-up Connections folder, click Finish.

To edit this connection in the Network and Dial-up Connections folder, select it, click File, and then click Properties.

□ Add a shortcut to my desktop

8. On the Virtual Private Connection window, click **Properties**.



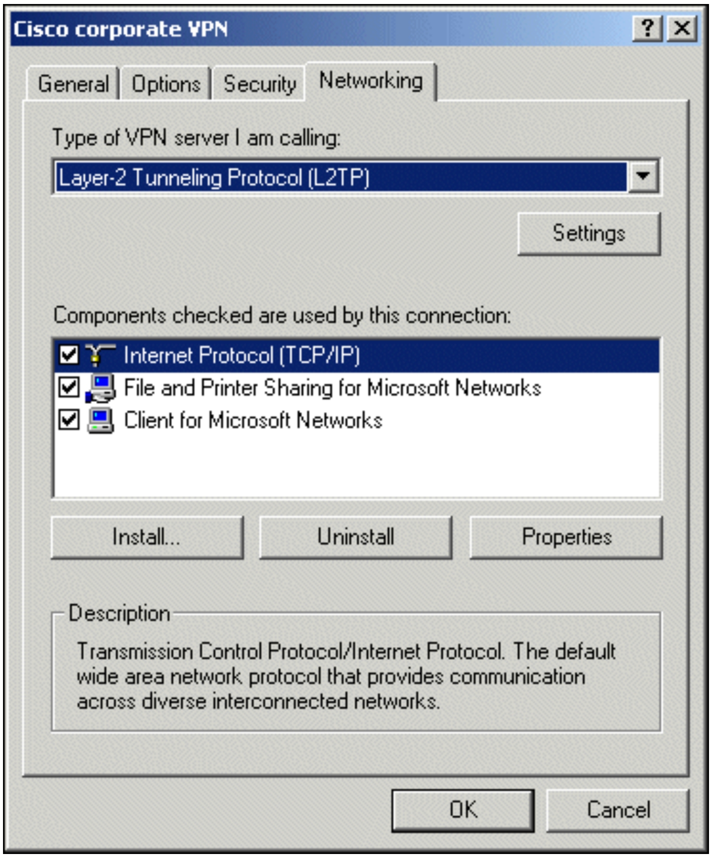
Connect Virtual Private Connection

User name: jedgaruser

Password: ***********

□ Save Password

9. On the Properties window, select the Networking tab.
10. Under Type of VPN server I am calling, choose **L2TP** from the pull−down menu, highlight **Internet Protocol TCP/IP**, and click **Properties**.


Cisco corporate VPN

Type of VPN server I am calling:

Layer-2 Tunneling Protocol (L2TP)

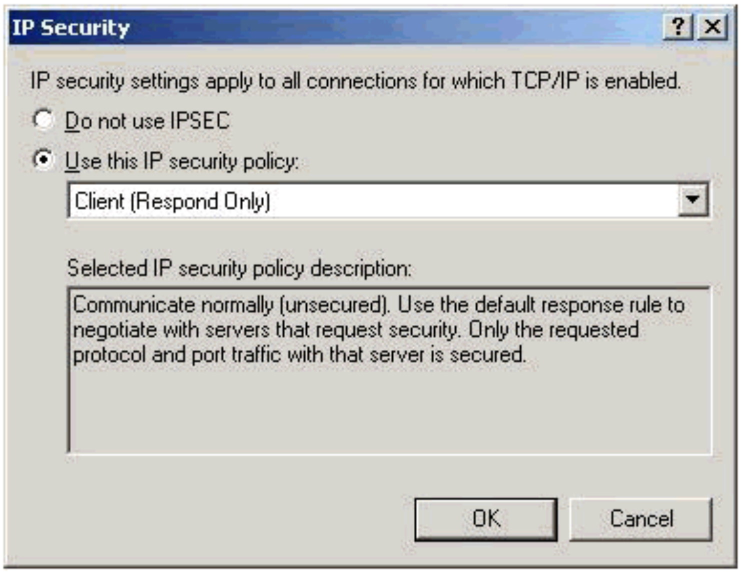
Components checked are used by this connection:

☑ Internet Protocol (TCP/IP)
☑ File and Printer Sharing for Microsoft Networks
☑ Client for Microsoft Networks

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

11. Select **Advanced** > **Options** > **Properties**.
12. On the IP Security window, choose **Use this IP security policy**.


IP Security

IP security settings apply to all connections for which TCP/IP is enabled.

○ Do not use IPSEC
● Use this IP security policy:

Client (Respond Only)

Selected IP security policy description:

Communicate normally (unsecured). Use the default response rule to negotiate with servers that request security. Only the requested protocol and port traffic with that server is secured.

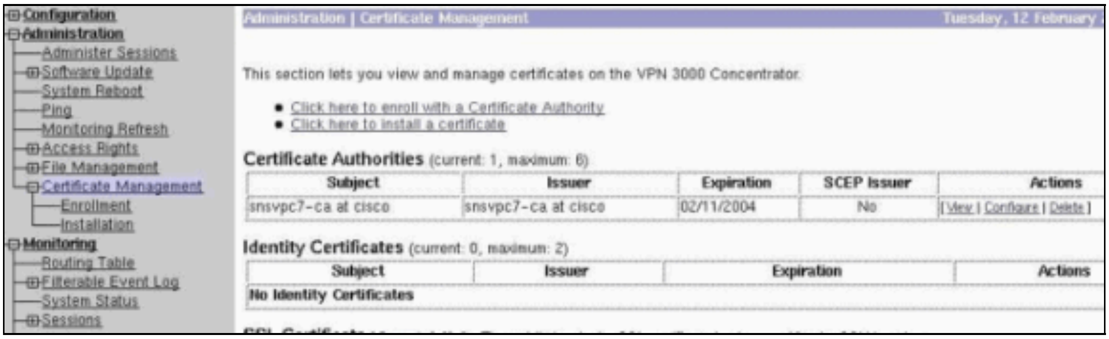
13. Choose the **Client (Respond Only)** policy from the pull−down menu, and click **OK** several times until you return to the Connect screen.
14. In order to initiate a connection, enter your username and password, and click **Connect**.

Configure the VPN 3000 Concentrator

Obtain a Root Certificate

Complete these steps in order to obtain a root certificate for the VPN 3000 Concentrator:

1. Point your browser to your CA (usually something such as http://ip_add_of_ca/certsrv/), **Retrieve the CA certificate or certificate revocation list**, and click **Next**.
2. Click **Download CA certificate** and save the file somewhere on your local disk.
3. On the VPN 3000 Concentrator, select **Administration > Certificate Management**, and click **Click here to install a certificate** and **Install CA Certificate**.
4. Click **Upload File from Workstation**.
5. Click **Browse** and select the CA certificate file that you have just downloaded.
6. Highlight the filename and click **Install**.



This section lets you view and manage certificates on the VPN 3000 Concentrator.

- Click here to enroll with a Certificate Authority
- Click here to install a certificate

Certificate Authorities (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
snsvpc7-ca at cisco	snsvpc7-ca at cisco	02/11/2004	No	[View | Configure | Delete]

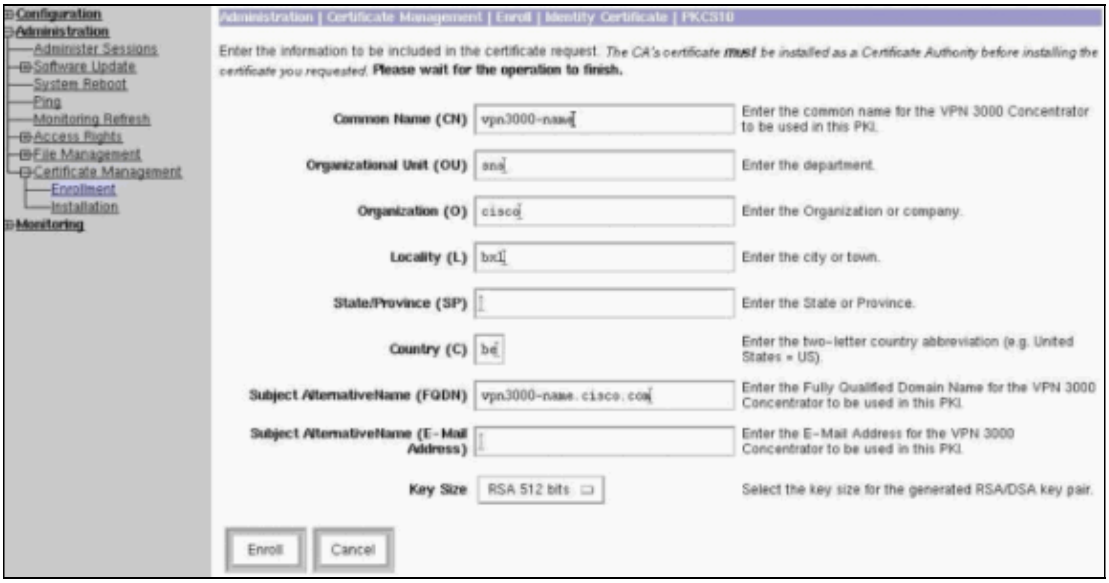
Identity Certificates (current: 0, maximum: 2)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

Obtain an Identity Certificate for the VPN 3000 Concentrator

Complete these steps in order to obtain an identity certificate for the VPN 3000 Concentrator:

1. Select **ConfAdministration > Certificate Management > Enroll > Identity Certificate**, then click **Enroll via PKCS10 Request (Manual)**. Fill out the form as shown here and click **Enroll**.



Enter the information to be included in the certificate request. *The CA's certificate **must** be installed as a Certificate Authority before installing the certificate you requested.* **Please wait for the operation to finish.**

Common Name (CN)	vpn3000-name	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU)	sns	Enter the department.
Organization (O)	cisco	Enter the Organization or company.
Locality (L)	bxl	Enter the city or town.
State/Province (SP)		Enter the State or Province.
Country (C)	be	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)	vpn3000-name.cisco.com	Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
Subject AlternativeName (E-Mail Address)		Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.
Key Size	RSA 512 bits	Select the key size for the generated RSA/DSA key pair.

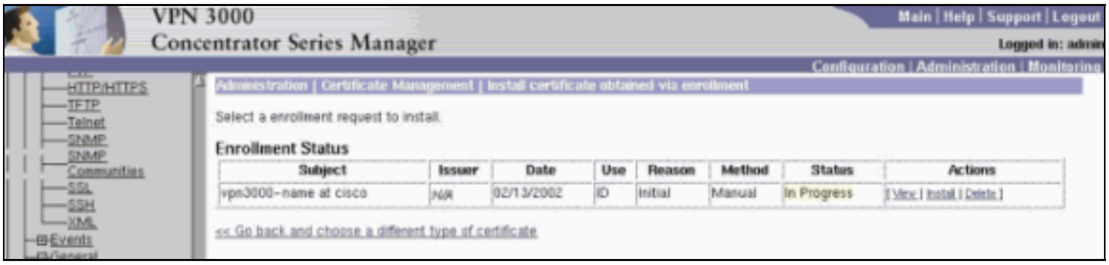
A browser window pops up with the certificate request. It needs to contain text similar to this output:

```
-----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. Point your browser to your CA server, check **Request a certificate**, and click **Next**.

3. Check **Advanced Request**, click **Next**, and select **Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**.
4. Click **Next**. Cut and paste the text of the certificate request shown previously in the text area. Click **Submit**.
5. Based on how the CA server is configured, you can click **Download CA certificate**. Or as soon the certificate has been issued by the CA, go back to your CA server and check **Check on a pending certificate**.
6. Click **Next**, select your request, and click **Next** again.
7. Click **Download CA certificate**, and save the file on the local disk.
8. On the VPN 3000 Concentrator, select **Administration > Certificate Management > Install,** and click **Install certificate obtained via enrollment**.

   You then see your pending request with a status of "In Progress," as in this image.


VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
HTTP/HTTPS
TFTP
Telnet
SNMP
SNMP Communities
SSL
SSH
XML
Events
General

Administration | Certificate Management | Install certificate obtained via enrollment

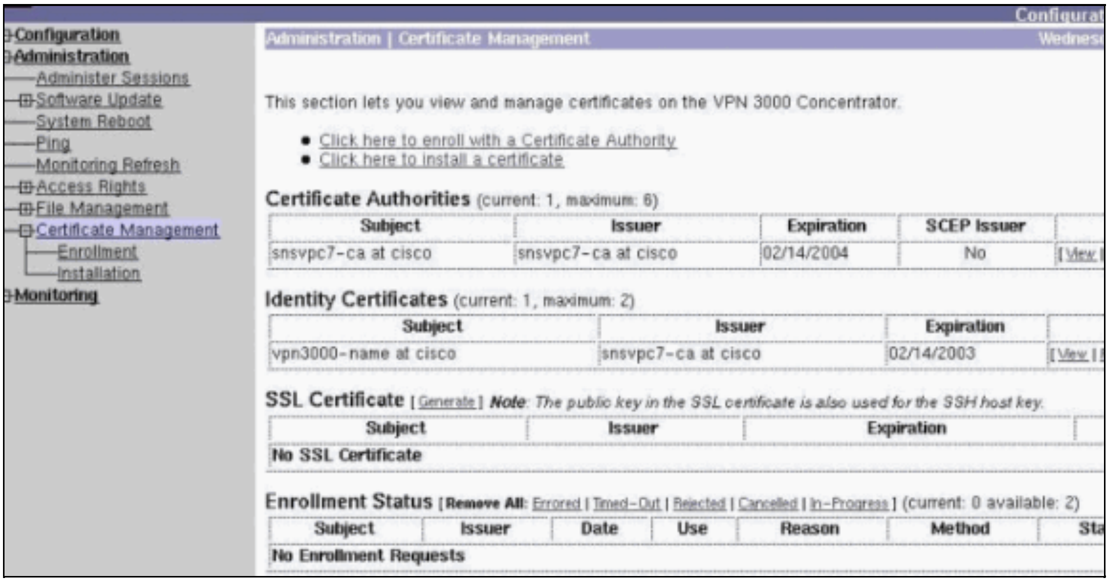
Select a enrollment request to install.

Enrollment Status

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
vpn3000-name at cisco	N/A	02/13/2002	ID	Initial	Manual	In Progress	[View | Install | Delete]

<< Go back and choose a different type of certificate

9. Click **Install**, followed by **Upload File from Workstation**.
10. Click **Browse** and select the file that contains your certificate issued by the CA.
11. Highlight the filename and click **Install**.
12. Select **Administration > Certificate Management**. A screen similar to this image appears.



Administration | Certificate Management

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- Click here to enroll with a Certificate Authority
- Click here to install a certificate

Certificate Authorities (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	
snsvpc7-ca at cisco	snsvpc7-ca at cisco	02/14/2004	No	[View

Identity Certificates (current: 1, maximum: 2)

Subject	Issuer	Expiration	
vpn3000-name at cisco	snsvpc7-ca at cisco	02/14/2003	[View

SSL Certificate [Generate] ***Note**: The public key in the SSL certificate is also used for the SSH host key.*

Subject	Issuer	Expiration	
No SSL Certificate			

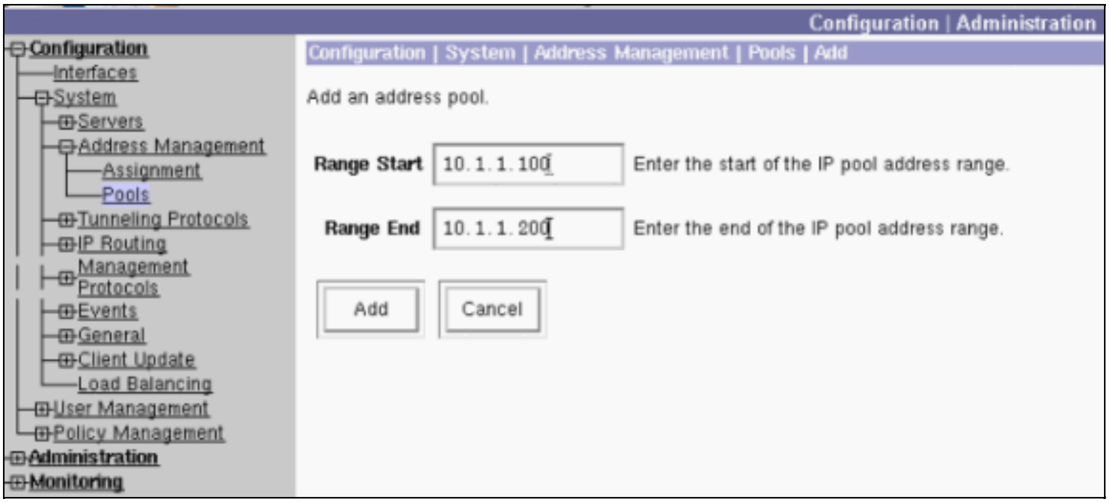
Enrollment Status [**Remove All**: Errored | Timed-Out | Rejected | Cancelled | In-Progress] (current: 0 available: 2)

Subject	Issuer	Date	Use	Reason	Method	Sta
No Enrollment Requests						

Configure a Pool for the Clients

Complete this procedure in order to configure a pool for the clients:

1. In order to assign an available range of IP addresses, point a browser to the inside interface of the VPN 3000 Concentrator and select **Configuration > System > Address Management > Pools > Add**.
2. Specify a range of IP addresses that do not conflict with any other devices on the inside network, and click **Add**.



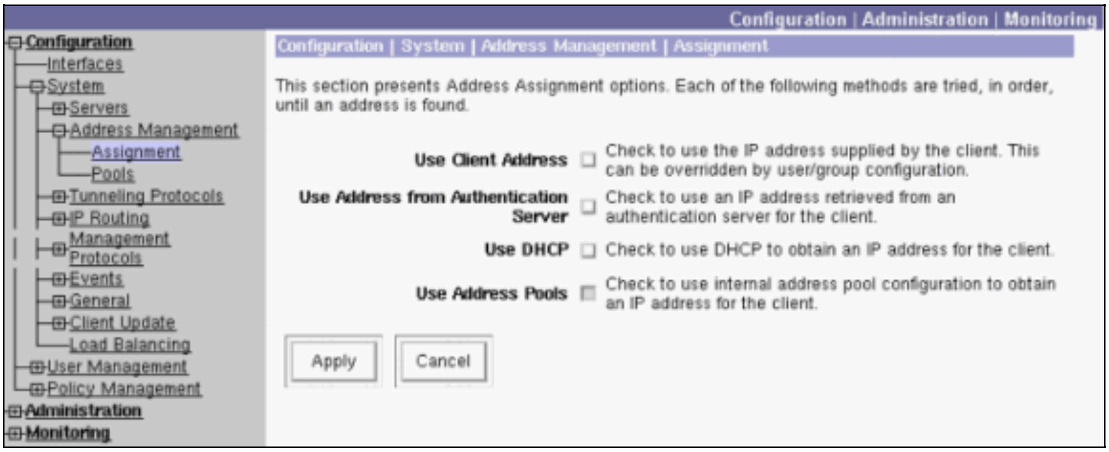
Configuration | System | Address Management | Pools | Add

Add an address pool.

Range Start 10.1.1.100 Enter the start of the IP pool address range.

Range End 10.1.1.200 Enter the end of the IP pool address range.

3. In order to tell the VPN 3000 Concentrator to use the pool, select **Configuration > System > Address Management > Assignment**, check the **Use Address Pools** box, and click **Apply**, as in this image.



Configuration | System | Address Management | Assignment

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

Use Client Address □ Check to use the IP address supplied by the client. This can be overridden by user/group configuration.

Use Address from Authentication Server □ Check to use an IP address retrieved from an authentication server for the client.

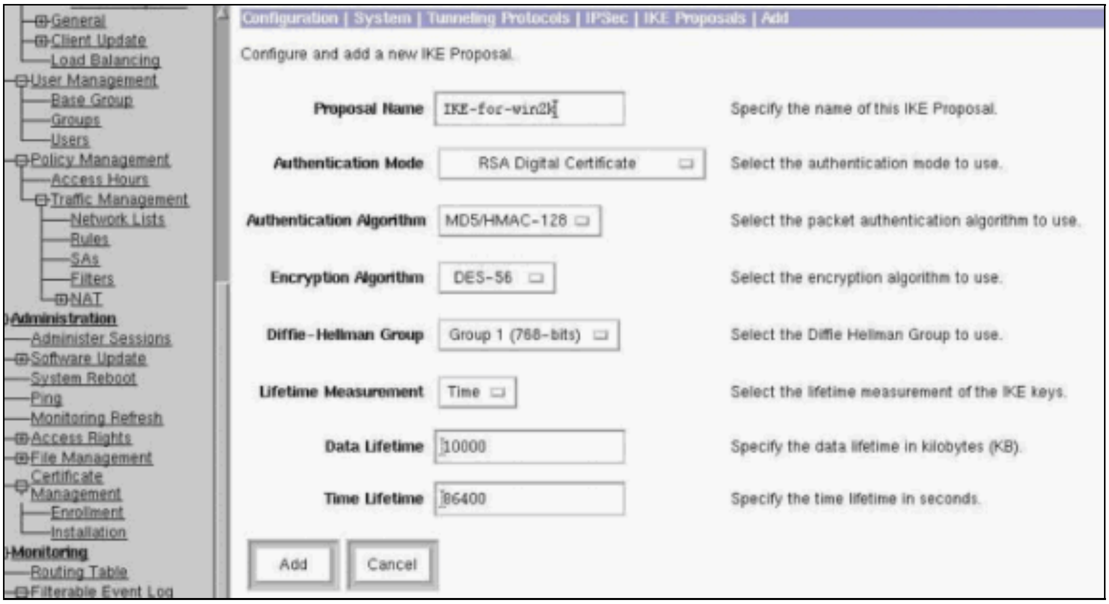
Use DHCP □ Check to use DHCP to obtain an IP address for the client.

Use Address Pools ☑ Check to use internal address pool configuration to obtain an IP address for the client.

Configure an IKE Proposal

Complete these steps in order to configure an IKE proposal:

1. Select **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals**, click **Add** and select the parameters, as shown in this image.



Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Add

Configure and add a new IKE Proposal.

Proposal Name	IKE-for-win2k	Specify the name of this IKE Proposal.
Authentication Mode	RSA Digital Certificate	Select the authentication mode to use.
Authentication Algorithm	MD5/HMAC-128	Select the packet authentication algorithm to use.
Encryption Algorithm	DES-56	Select the encryption algorithm to use.
Diffie-Hellman Group	Group 1 (768-bits)	Select the Diffie Hellman Group to use.
Lifetime Measurement	Time	Select the lifetime measurement of the IKE keys.
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime	86400	Specify the time lifetime in seconds.

2. Click **Add**, highlight the new proposal in the right column, and click **Activate**.

Configure the SA

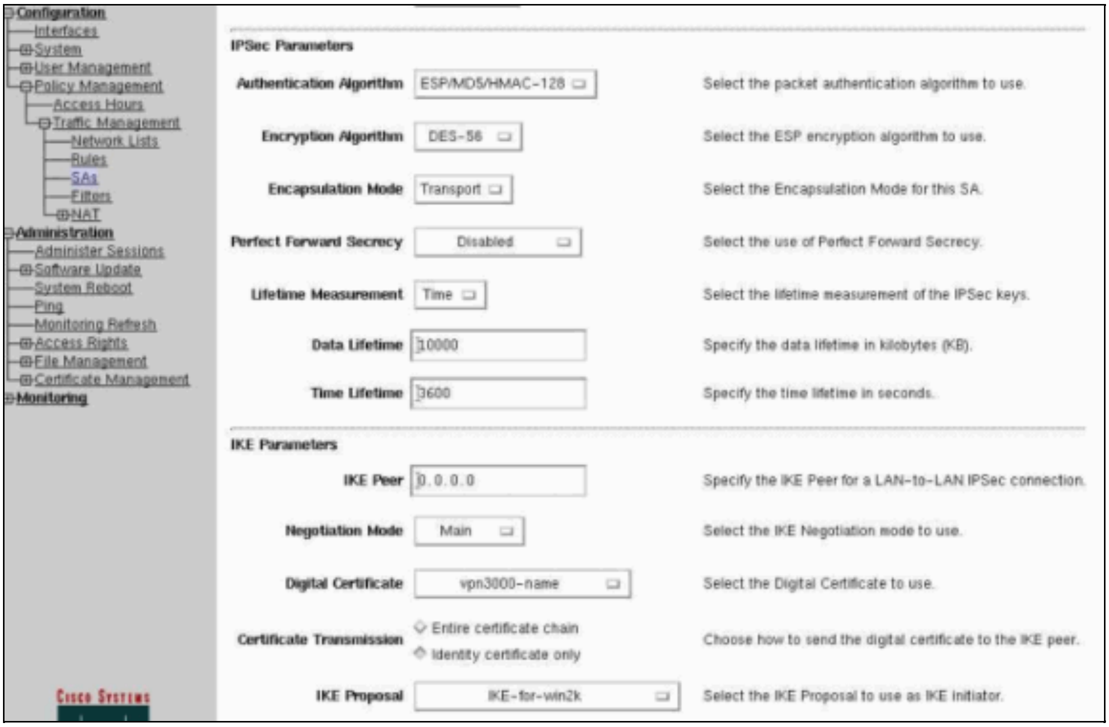
Complete this procedure in order to configure the Security Association (SA):

1. Select **Configuration > Policy Management > Traffic Management > SA** and click **ESP−L2TP−TRANSPORT**.

   If this SA is not available or if you use it for some other purpose, create a new SA similar to this one. Different settings for the SA are acceptable. Change this parameter based on your security policy.
2. Select the digital certificate that you have configured previously under the **Digital Certificate** pull−down menu. Select the **IKE−for−win2k** Internet Key Exchange (IKE) proposal.

   Note: This is not mandatory. When the L2TP/IPSec client connects to the VPN Concentrator, all the IKE proposals configured under the active column of the page **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals** are tried in order.

   This image shows the configuration needed for the SA:



IPSec Parameters

Authentication Algorithm: ESP/MD5/HMAC-128 — Select the packet authentication algorithm to use.

Encryption Algorithm: DES-56 — Select the ESP encryption algorithm to use.

Encapsulation Mode: Transport — Select the Encapsulation Mode for this SA.

Perfect Forward Secrecy: Disabled — Select the use of Perfect Forward Secrecy.

Lifetime Measurement: Time — Select the lifetime measurement of the IPSec keys.

Data Lifetime: 10000 — Specify the data lifetime in kilobytes (KB).

Time Lifetime: 3600 — Specify the time lifetime in seconds.

IKE Parameters

IKE Peer: 0.0.0.0 — Specify the IKE Peer for a LAN-to-LAN IPSec connection.

Negotiation Mode: Main — Select the IKE Negotiation mode to use.

Digital Certificate: vpn3000-name — Select the Digital Certificate to use.

Certificate Transmission: ○ Entire certificate chain ○ Identity certificate only — Choose how to send the digital certificate to the IKE peer.

IKE Proposal: IKE-for-win2k — Select the IKE Proposal to use as IKE initiator.

Configure the Group and User

Complete this procedure in order to configure the Group and User:

1. Select **Configuration > User Management > Base Group**.
2. Under the General tab, make sure that **L2TP over IPSec** is checked.
3. Under the IPSec tab, select the **ESP−L2TP−TRANSPORT** SA.
4. Under the PPTP/L2TP tab, uncheck all the **L2TP Encryption** options.
5. Select **Configuration > User Management > Users** and click **Add**.
6. Enter the name and password that you use to connect from your Windows 2000 Client. Make sure that you select **Base Group** under the Group Selection.
7. Under the General tab, check the **L2TP over IPSec** tunneling protocol.
8. Under the IPSec tab, select the **ESP−L2TP−TRANSPORT** SA.
9. Under the PPTP/L2TP tab, uncheck all the **L2TP Encryption** options, and click **Add**.

   You are now able to connect with the help of the L2TP/IPSec Windows 2000 Client.

   Note: You have chosen to configure the base group to accept the remote L2TP/IPSec connection. It is also possible to configure a group that matches the Organization Unit (OU) field of the SA to accept the incoming connection. The configuration is identical.

Debug Information

```
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
```

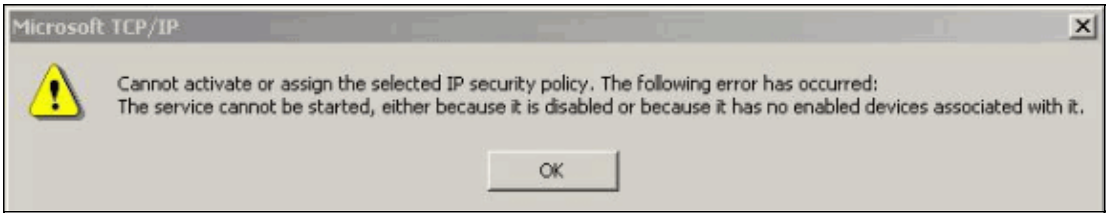
```
Group [VPNC_Base_Group]
processing SA payload

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
```

Troubleshoot Information

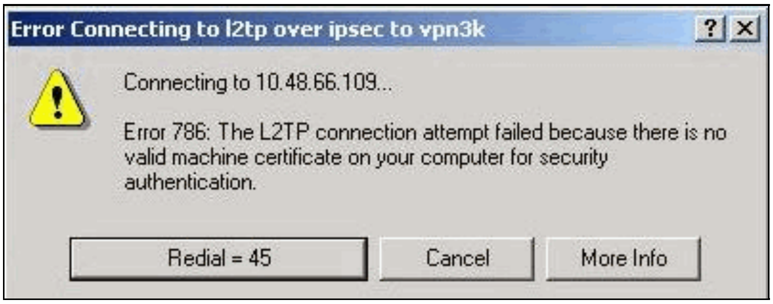
This section illustrates some common problems and the troubleshooting methods for each.

- The server cannot be started.



Cannot activate or assign the selected IP security policy. The following error has occurred:
The service cannot be started, either because it is disabled or because it has no enabled devices associated with it.

  Most likely, the IPSec service is not started. Select **Start > Programs > Administrative tools > Service** and make sure that the **IPSec service** is enabled.
- Error 786: No valid machine certificate.

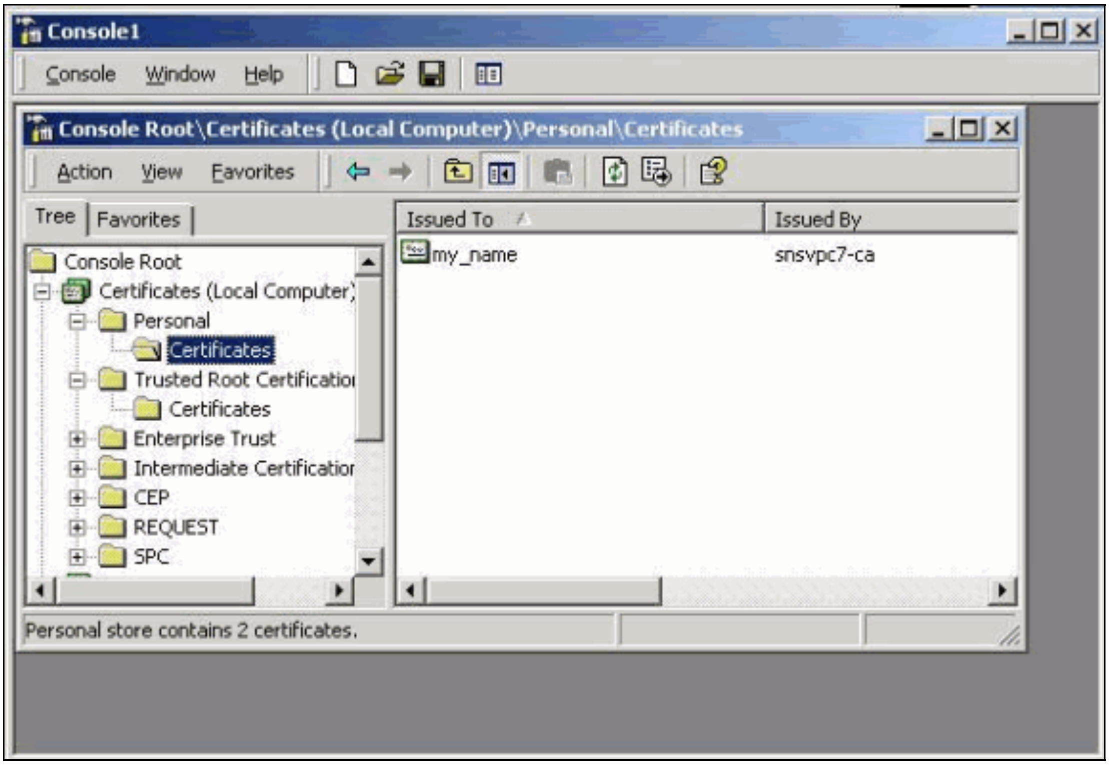


Connecting to 10.48.66.109...

Error 786: The L2TP connection attempt failed because there is no valid machine certificate on your computer for security authentication.

1. This error indicates a problem with the certificate on the local machine. In order to easily look at your certificate, select **Start > Run**, and execute MMC. Click **Console** and choose **Add/Remove Snap−in**. Click **Add** and choose **Certificate** from the list. When a window appears that asks you the scope of the certificate, choose **Computer Account**.

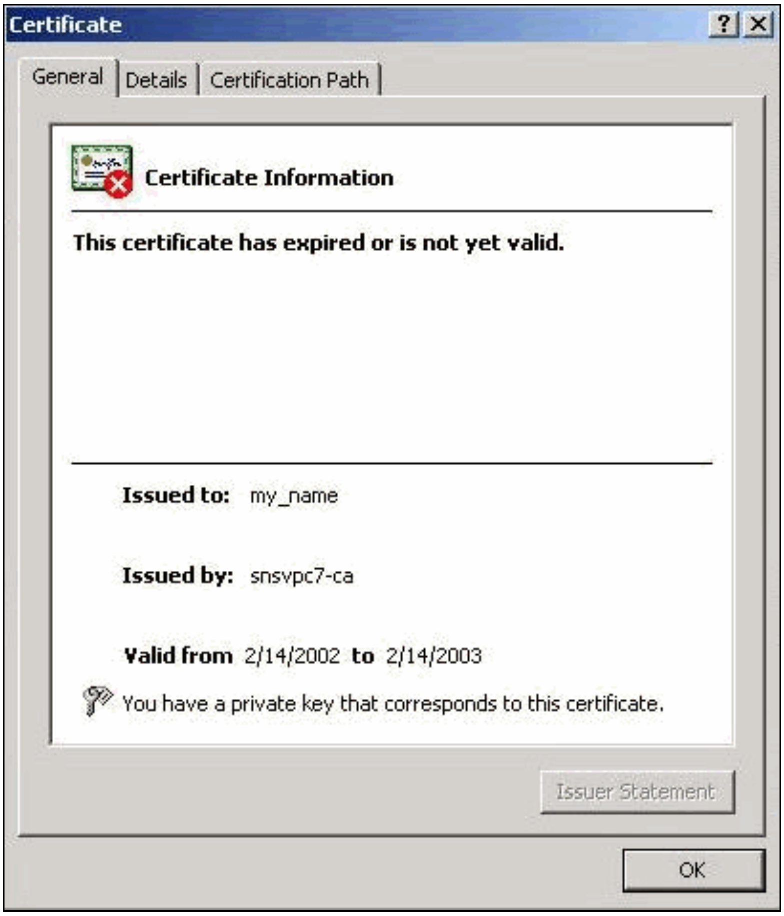
   Now you can verify that the certificate of the CA server is located under the **Trusted Root Certification Authorities**. You can also verify that you have a certificate by selecting **Console Root > Certificate (Local Computer) > Personal > Certificates**, as shown in this image.


Console1
Console Window Help
Console Root\Certificates (Local Computer)\Personal\Certificates
Action View Favorites
Tree Favorites
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certificatior
Certificates
Enterprise Trust
Intermediate Certificatior
CEP
REQUEST
SPC

Issued To	Issued By
my_name	snsvpc7-ca

Personal store contains 2 certificates.

2. Click the **certificate**. Verify that everything is correct. In this example, there is a private key associated with the certificate. However, this certificate has expired. This is the cause of the problem.



Certificate Information

This certificate has expired or is not yet valid.

Issued to: my_name

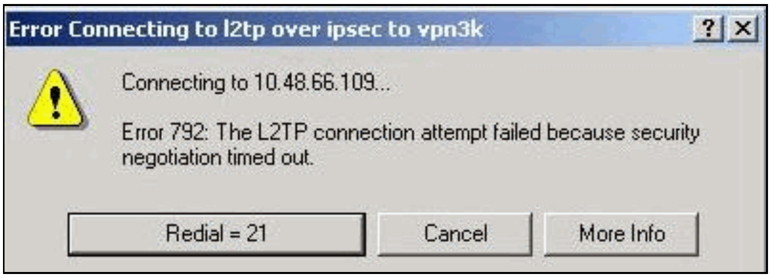
Issued by: snsvpc7-ca

Valid from 2/14/2002 **to** 2/14/2003

You have a private key that corresponds to this certificate.

- Error 792: Security negotiation timeout.

  This message appears after a long period.



Error Connecting to l2tp over ipsec to vpn3k

Connecting to 10.48.66.109...

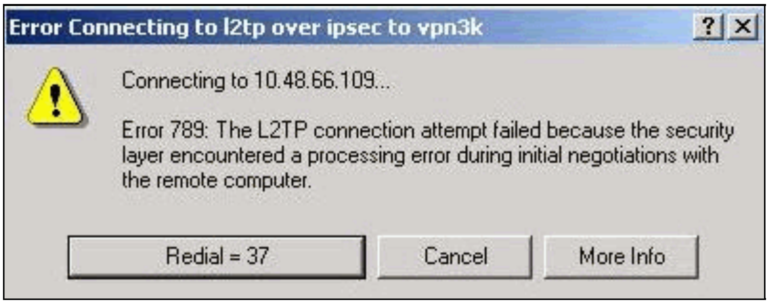
Error 792: The L2TP connection attempt failed because security negotiation timed out.

Turn on the relevant debugs as explained in the Cisco VPN 3000 Concentrator FAQ. Read through them. You need to see something similar to this output:

```
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
```

This indicates that the IKE proposal has not been configured properly. Verify the information from the Configuring an IKE Proposal section of this document.

- Error 789: Security layer encounters a processing error.



Error Connecting to l2tp over ipsec to vpn3k

Connecting to 10.48.66.109...

Error 789: The L2TP connection attempt failed because the security layer encountered a processing error during initial negotiations with the remote computer.

Turn on the relevant debugs as explained in the Cisco VPN 3000 Concentrator FAQ. Read through them. You need to see something similar to this output:

```
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!
```

- Version Used

  Select **Monitoring** > **System Status** to view this output:

```
VPN Concentrator Type: 3005
Bootcode Rev: Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 2000 05:36:4
Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Version 3.5.Rel Nov 27 2001
Up For: 44:39:48
Up Since: 02/13/2002 15:49:59
RAM Size: 32 MB
```

Related Information

- **IPSec Negotiation/IKE Protocols Product Support**
- **Technical Support − Cisco Systems**

Updated: Jan 19, 2006 Document ID: 14117