Global Information Assurance Certification Paper

A guide to implementing a more secure Windows 2000 VPN using L2TP over IPSEC

By Brian Andreu

GSEC Version 1.3

Table of Contents

Abstract/Introduction

The purpose of this document is to provide general guidelines for implementing a Windows 2000 VPN using L2TP over IPSec. Included in this document will be a section on enabling remote access on the VPN server with Routing and Remote Access. Additionally, there will be a section on creating a Certificate Authority through Windows 2000 Certification Services. These sections will provide the necessary steps to allow remote VPN clients a successful connection to the VPN using L2TP over IPSec.

Due to the cost saving benefits, businesses are now taking a closer look at VPN solutions. No longer do IT professionals have to maintain and support a large modem pool in order for remote users to connect to the corporate network. A VPN allows a remote user to take advantage of a persistent Internet connection to communicate from a remote location such as home back to the corporate network. This could also bring about a reduction in call charges for users. The reason is because typically, only local charges to their ISP are incurred rather than long-distance costs.

What exactly is a VPN? According to the Windows 2000 Virtual Private Networking Scenario white paper:

> The use of both public and private networks to create a network connection is called a virtual private network (VPN). A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. With a VPN, you can send data between two computers across a shared or public network in a manner that emulates a point-to-point private link. Virtual private networking is the act of creating and configuring a virtual private network.

The white paper takes this a step further with regards to point-to-point emulation by stating:

> To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information, which allows the data to traverse the shared or public network to reach its endpoint. To emulate a private link, the data is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. The link in which the private data is encapsulated and encrypted is a virtual private network (VPN) connection.

An obvious concern with implementing a VPN within a company is security. The concept of remote users coming into the corporate network over the Internet should raise a concern with any IT manager. With the release of Windows 2000, Microsoft has included the ability to configure the Windows 2000 operating system as a VPN server using the more secure L2TP/IPSec protocol.

Why use L2TP/IPSec over the traditional PPTP?

One of the first decisions that need to be made when implementing a Windows 2000-based VPN is whether to use L2TP/IPSec or PPTP. If security is the driving factor, then L2TP/IPSec is the clear choice. Here's why. Microsoft and Cisco Systems, Inc. made the decision to collaborate on virtual private networking by merging their protocols, PPTP and L2F, into one hybrid protocol. The resulting protocol of that collaboration is Layer 2 Tunneling Protocol, or L2TP. L2TP over IPSec provides the following:

- Per packet data authentication (proof that the data was sent by the authorized user)
- Data integrity (proof that the data was not modified in transit)
- Replay protection (prevention from resending a stream of captured packets)
- Data confidentiality (prevention from interpreting captured packets without the encryption key).

In contrast, PPTP provides only per packet data confidentiality. The key security strength of L2TP with IPSec is the use of certificates during computer-level authentication as well as user-level authentication through a PPP authentication protocol. When PPP packets are exchanged during user-level authentication, the packets are already encrypted due to the initial establishment of the IPSec security associations (SAs). Since the PPP packets are already encrypted before the exchange takes place, offline dictionary attacks are only feasible after the PPP packets have been successfully decrypted.

Because L2TP over IPSec uses the Triple Data Encryption Standard (3DES) algorithm, its data encryption is much stronger than PPTP's. 3DES is for use only in North America and is designed for high-security environments (Norman, pg. 3). If this level of security as well as the associated overhead is not necessary, DES which uses one 56-bit key (3DES uses three 56-bit keys) can be used.

L2TP over IPSec not only provides computer-level and user-level authentication and data encryption but also offers data authentication. To accomplish data authentication, L2TP over IPSec uses Hash Message Authentication Code (HMAC) Message Digest 5 (MD5). This hashing algorithm creates a 128-bit hash to authenticate data (Norman, pg. 3).

Configuring the VPN Server

For the design and implementing of the Windows 2000 VPN sever, two areas will be assessed for the initial stages of the implementation plan:

- Network configuration assessment
- Remote access configuration

Network Configuration Assessment

In a simple network solution, an organization will typically have a local area network, or segment based upon a flat TCP/IP address structure. Using the diagram in Figure 1, this

fictional corporate network scenario is using the private network address of 10.10.0.0 with a subnet mask of 255.255.0.0. The VPN server contains two host adapters that have been installed based on the manufacturers specifications. One host, or LAN adapter is connected to the corporate network segment. The second host, or WAN adapter has the VPN server connecting directly to the Internet. Once drivers are installed and functioning, both adapters appear as local area connections in the Network and Dial-up Connections folder. TCP/IP must also be configured for each of the adapters. The LAN adapter is configured using an IP address of 10.10.0.19 with a subnet mask of 255.255.0.0. The WAN adapter connecting to the Internet is configured using a static IP address of 192.168.33.22 with a subnet mask of 255.255.255.0 as allocated by the Internet service provider (ISP) for the organization. (NOTE: For purposes of this practical, the IP address provided by the ISP is considered a 'private' address.)

As part of the planning process, administrators will also want to plan for the number of remote clients that will be allowed to connect through the VPN. Since this scenario is based around a simple network solution, the bandwidth for the one VPN server should be able to accommodate at least 50 connections.

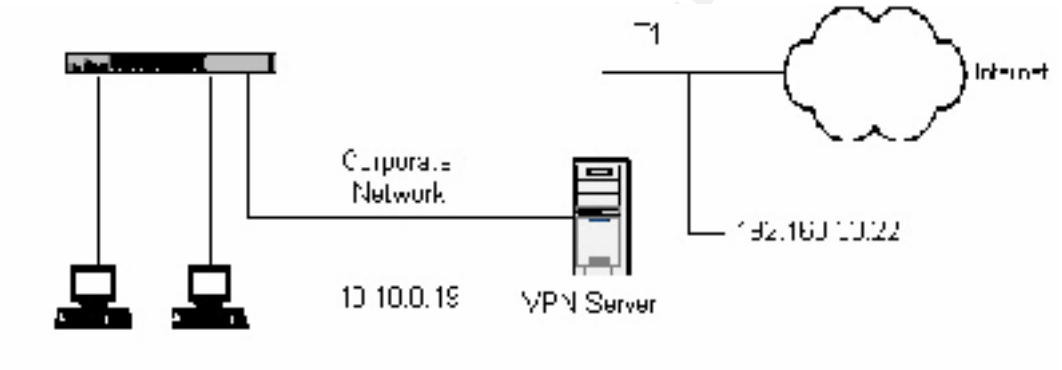

Figure 1

Routing Access Configuration
The next phase is to configure the VPN server for remote access. The following steps show how to configure the VPN server for remote access using Routing and Remote Access.

1. Open the **Routing and Remote Access** console in the **Administrative Tools** folder.
2. Right-click the VPN server and then click **Configure and Enable Routing and Remote Access**. The Routing and Remote Access Server Setup wizard starts, click **Next**.
3. Select **Virtual private network [VPN] server**, as shown in Figure 2, and click **Next**.

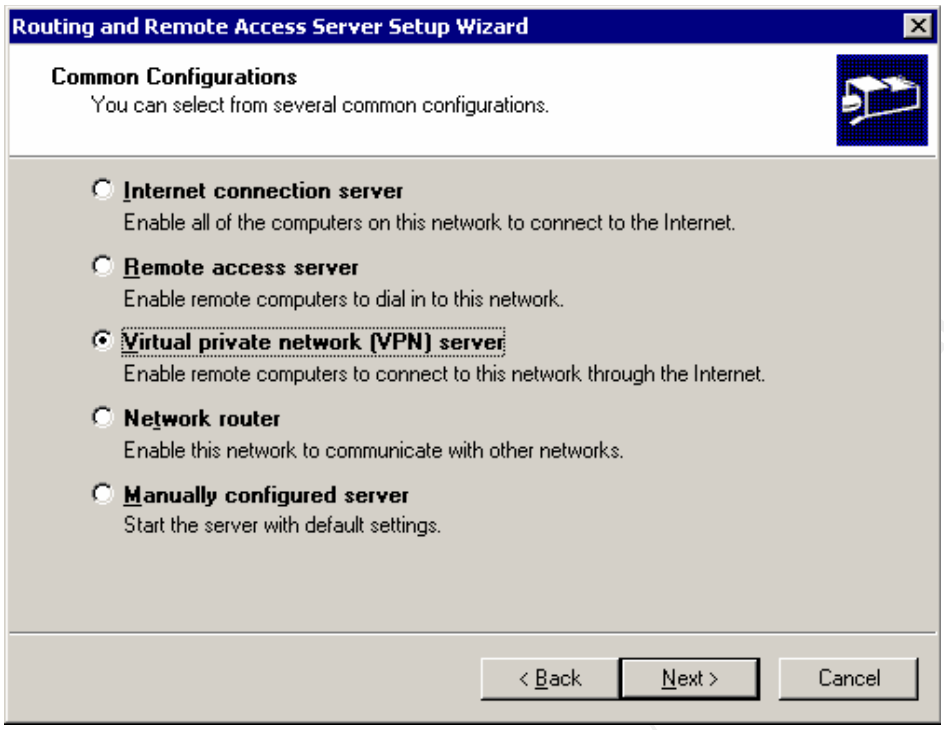

Figure 2

4. The Remote Client Protocols screen appears next. Note that TCP/IP should already be installed and configured before configuring RRAS. Select **Yes, all of the available protocols are on this list** and click **Next** as shown in Figure 3.

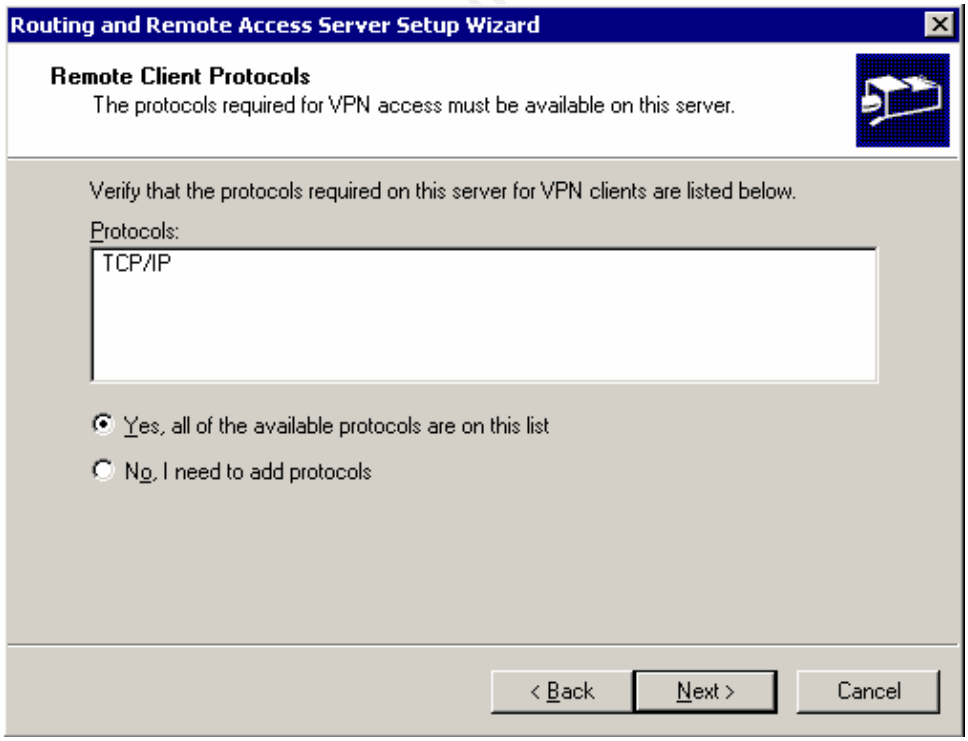

Figure 3

5. In the Internet Connection window, select the Internet connection as specified by the WAN adapter Internet IP address. Click **Next**.
6. In the Network Selection window, select the network to which the VPN clients will be assigned. Click **Next**.
7. Choose a method to assign IP addresses to the clients. If DHCP has been implemented within the organization, select **Automatically** to have the DHCP server assign addresses. The second option is to configure the VPN server to assign addresses based on a specified range. NOTE: If this option is chosen and there is a DHCP server within the organization, the specified range of addresses will need to be excluded from the range configured on the DHCP server to prevent potential IP address conflicts. For this scenario, assume DHCP will assign addresses. Select **Automatically** and click **Next**.
8. The next screen gives the option to configure this server to use a Remote Authentication Dial-In User Service (RADIUS). Select **No, I don't want to set up this server to use RADIUS now** and click **Next**.
9. The final screen simply states that the configuration of the VPN server is now complete. Click **Finish** to complete the Routing and Remote Access Server Setup wizard.
10. The Routing and Remote Access Service will now start.

Finally, before remote users can make VPN connections to the server, they must be given remote access permission. Remote access permission can be enabled in one of two ways as shown in Figure 4 under the Dial-in properties of the user account:

- *Allow Access*. User is allowed remote access. The default setting is **Deny access**.
- *Control access through Remote Access Policy*. Configurable with the Routing and Remote Access console to determine the remote users remote access permission.

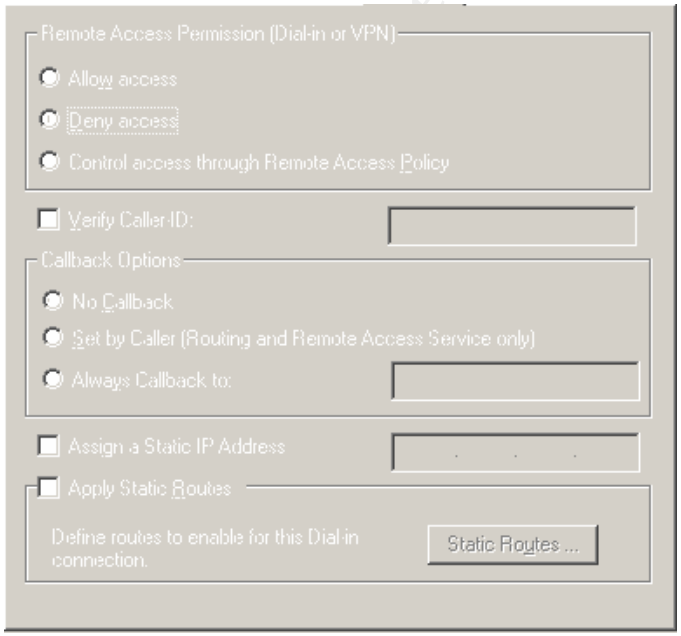

Figure 4

A Final Analysis
Essentially, packet filters are configured on the Windows 2000 VPN server. The WAN adapter on the VPN server is automatically configured to block all packets except the PPTP and L2TP packets. This is essentially by design as described in the following Microsoft knowledge base article:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q243374

Since the end goal is to only allow clients to connect using L2TP, PPTP needs to be disabled. Execute the following steps to completely disable PPTP on the VPN server:

1. Launch the Routing and Remote Access console.
2. Expand the server snap-in node for the VPN server.
3. Right-click on **Ports** and select **Properties**.
4. Verify the device **WAN Miniport (PPTP)** is selected and click **Configure**.
5. Uncheck each of the following flags as shown in Figure 5: **Remote access connections (inbound only)** and **Demand-dial routing connections (inbound and outbound)**.

Figure 5

This tightens security on the VPN server even more by preventing hackers from getting to computers on the private network. Keep in mind that this filtering will also prevent remote users from accessing any applications that might be on this VPN server. Therefore, the ideal solution here is to maintain the server as a dedicated VPN server.

By default, the number of VPN ports that are created when choosing *Virtual private network (VPN)* server are 128 PPTP and 128 L2TP ports. Since PPTP has been disabled, this leaves only the 128 L2TP ports. The number of ports can be adjusted in the Routing and Remote Access console. This is done within the Ports properties.

The Certificate Authority

The Certificate Authority issues the digital certificates to the VPN server as well as the VPN client. The remote VPN clients and the VPN server must have a common Certification Authority. Secondly, both machines must have a computer certificate that was issued by the common CA. Windows 2000 server includes the required computer certificates. These digital certificates are used to create digital signatures and public-private key pairs. Certificates are signed documents that match public keys to other information, such as a name or an e-mail address. The issuing CA signs these certificates. A CA's signature guarantees that the public key belongs to the issuing party. The Certificate Authority can be either a third-party entity such as Verisign or, a Windows 2000 Certification Authority server, which is the basis of this section. When choosing a CA model, consider the following types:

- Enterprise Root CA. A top-level CA that uses Active Directory to determine both the identity and the security permissions of the requestor of the certificate. This model is recommended for organizations that will only be issuing certificates to users and computers within the organization. Obviously, this model requires Active Directory as well as DNS.
- Stand Alone Root CA. A top-level CA that does not require Active Directory nor does it require the server to be a member of any domain. This model is recommended for organizations that will be issuing certificates outside the organization.

There is also what is called enterprise and stand-alone subordinate CAs. These CAs are considered less trusted in the hierarchy. Obviously these CAs do require a root CA. A subordinate CA usually issues certificates for specific uses, such as secure e-mail, or smart card authentication (enterprise subordinate only.)

Installing and Configuring the Certificate Authority Service

This section will outline the steps necessary for configuring the Certificate Authority. This Certificate Authority will be a stand-alone root CA. The CA that is installed on the Windows 2000 server includes Web pages that remote users can access to submit their certificate requests. These certificates will be requested and issued through Internet Explorer. Therefore, Internet Information Services will be configured on the Windows 2000 server running the Certificate Authority Service.

Since certificates are based on timestamps, first verify the server has the correct date and time. Once this is done, execute the following steps to install the Certification Authority service:

1. Launch **Control Panel** and double-click the **Add/Remove Programs** icon.
2. Click the button labeled **Add/Remove Windows Components** and check the **Certificates Services** checkbox. A warning dialog box will appear stating that after installing this service, the computer cannot be renamed, join a domain, or be removed from one.
3. Click **Yes** to continue and then click **Next**.

Now that Certificate Services are installed on the server, the next step is to configure the Certification Authority service.

1. *Certification Authority Type*. Select **Standalone Root CA** and click **Next** as shown in Figure 6.

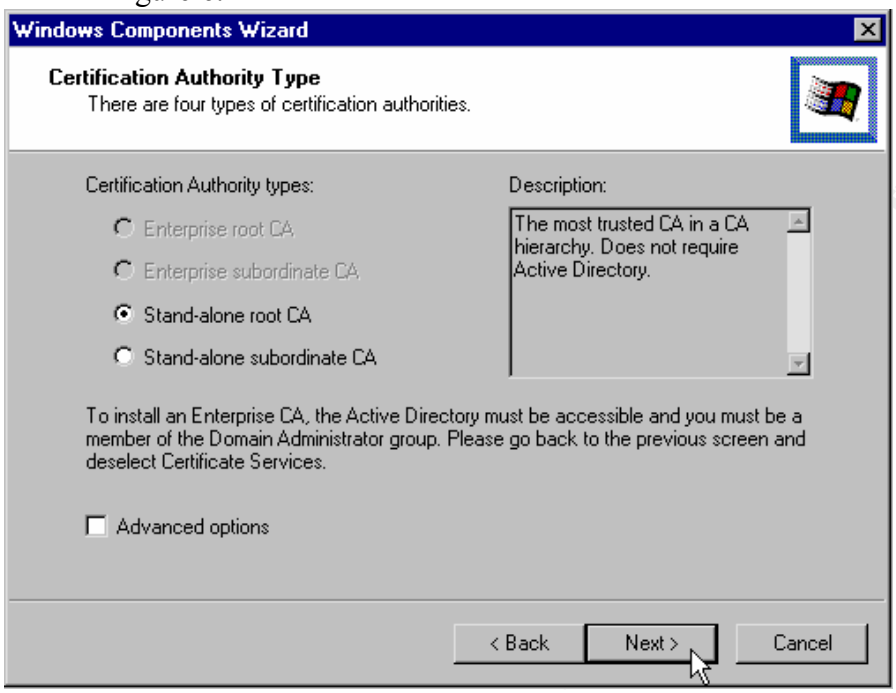

Figure 6

2. *CA Identifying Information*. Here, several defaults are already specified. These defaults are: Country/Region, the validity time of the certificate (two years), and the expiration date/time. Specify additional information as necessary. The CA name is required information. Specify a name that meets the naming standards of the organization. (See Figure 7)

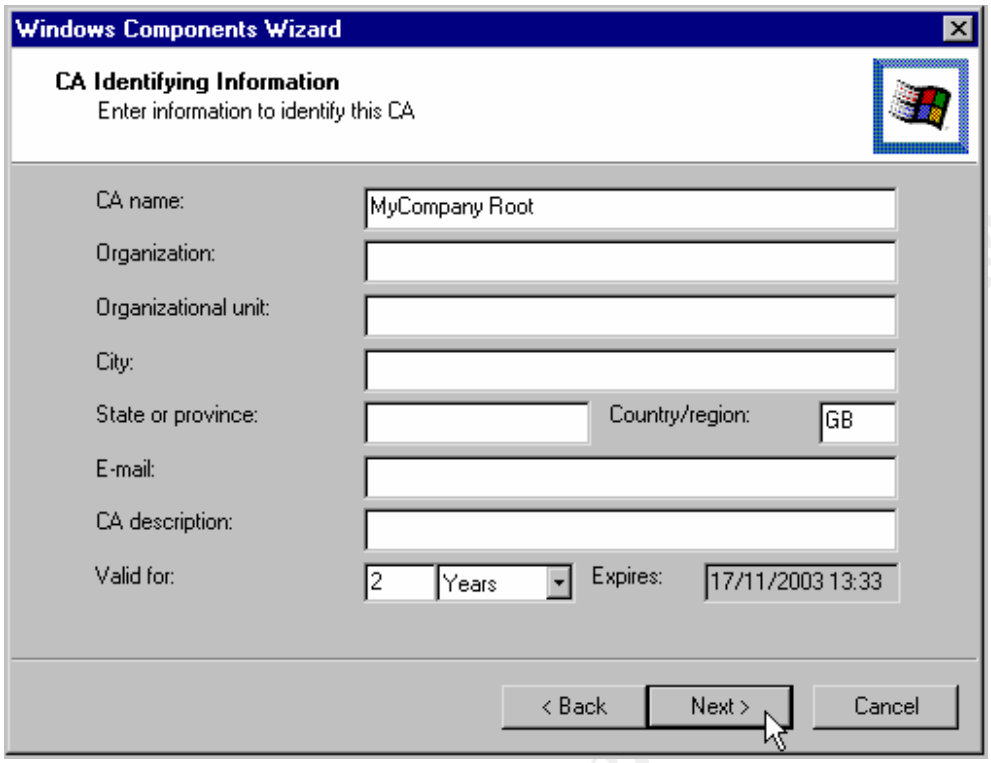

Figure 7

3. *Data Storage Location*. Information inputted here is specific to the certificate database as well as the associated database log. Accept the defaults and click **Next**. A warning dialog box will appear stating that IIS is running on the computer and must be stopped to proceed. IIS needs to be stopped in order to create the virtual directory used to deploy the certificates. After clicking **OK,** the virtual directory will install. The Windows 2000 installation source files will need to be available in order to complete this step successfully. Once the installation is complete, click the **Finish** button and then click **Close**. The server will not need to be rebooted.

This completes the installation phase. The following components were added to the system as part of the install:

- *Certification Authority*. The console for managing CAs on which Certificate Services are installed. This tool is accessed from the Administrative Tools group on the Certificate Authority server.
- *Certificates*. A Microsoft Management Console (MMC) snap-in used to manage existing certificates for user accounts, computers, and services.
- *Certificate Services Web enrollment support*. As mentioned earlier, remote users will have access to Web pages on the CA to submit their certificate requests. These Web pages are located at http://*server*/certsrv where *server* is the name of the Windows 2000 CA.

The Certification Process

In Windows 2000, there are two ways to explicitly request certificates: the Certificate Request Wizard and the Certificate Services Web Pages. The Certificate Request Wizard is only available if requesting a certificate from an enterprise CA. The Certificate Services Web Pages can be used to request certificates from either a stand-alone CA or an enterprise CA. Since the example install specified a stand-alone CA, Certificate Services Web Pages will be used to request certificates for both the VPN server and the client. This is also called down-level client certificate distribution.

Certification Process – Client Consideration

In order to initiate the request, the client workstation as well as the RRAS server must be able to connect to the CA server. Normally, this should not be an issue with the RRAS server since it is most likely on the corporate network. However, if the client is a remote machine, this could pose an issue. Since the recommendation is to disable PPTP, the remote VPN client will be unable to connect to the corporate network. The ideal scenario is to complete the certificate request phase with the remote machine on the corporate network. If this is impossible, consider enabling PPTP temporarily in order for the remote VPN client to connect. These are merely suggestions to consider.

Certification Process – The Preliminaries

In order to submit the certificate request, execute the following steps on both the VPN server and the client machine:

1. As stated earlier, certificates are based on timestamps. Verify the correct date and time on these machines, as was done for the CA server.
2. Open Internet Explorer and point the browser to the following URL: http://*server*/certsrv where *server* is the name of the Windows 2000 CA. The home page for Microsoft Certificate Services will load. Note the CA server name displayed at the top, as shown in Figure 8.

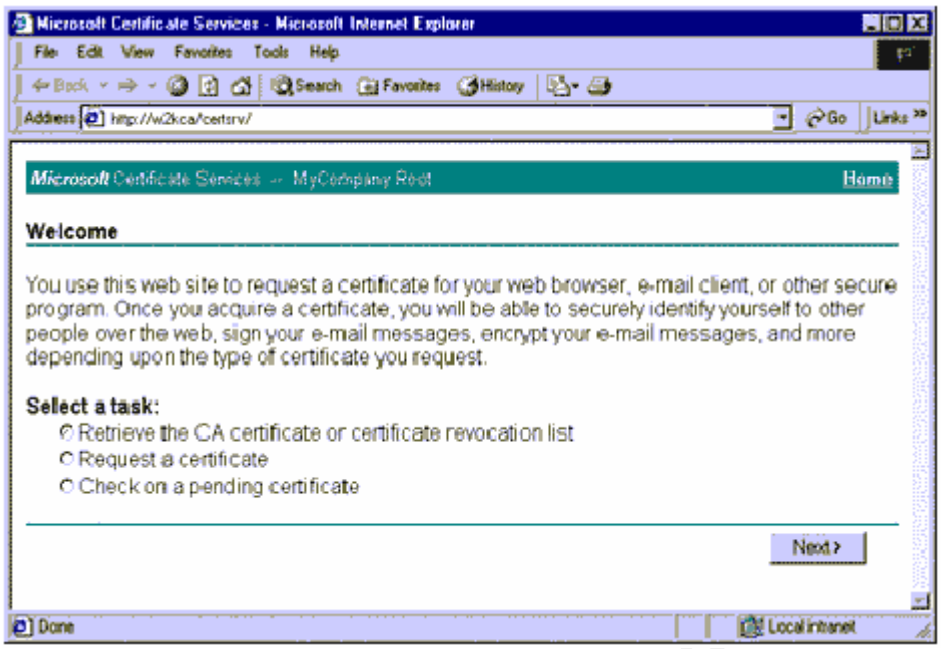

Figure 8

3. On the **Welcome** page under **Select a task**, click **Retrieve the CA certificate or certificate revocation list** and then click **Next**.
4. Click **Install this CA certification path** as shown in Figure 9. This selection allows the computer to trust all the certificates issued by this certification authority (CA).

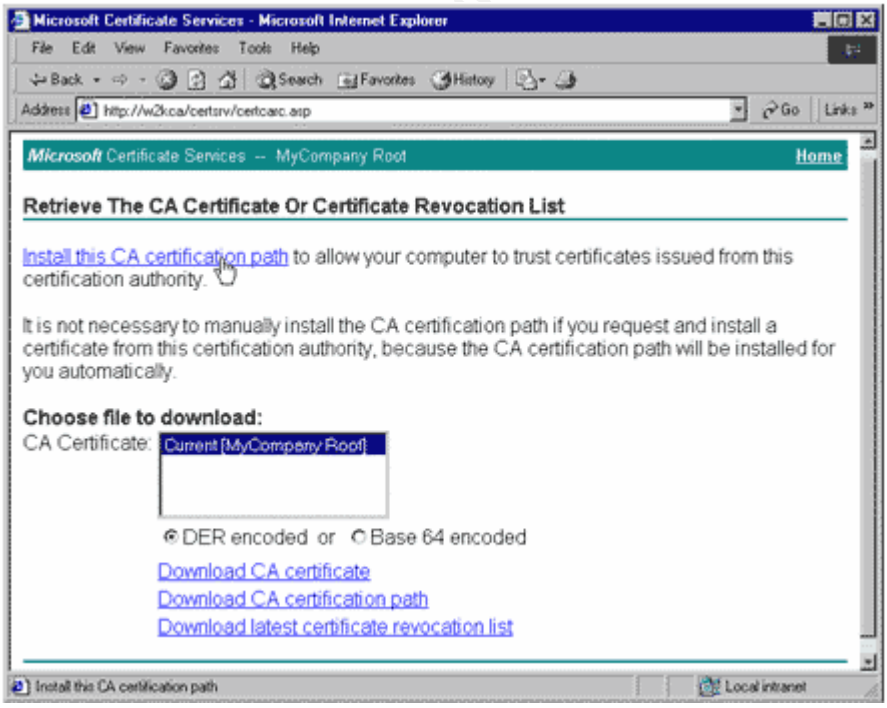

Figure 9

A warning message will appear prompting for confirmation to add the certificate to the machines Root Store. Certificate information will also be displayed, including the name of the certificate, the fact that it was self-issued, and other information, such as the time validity, serial number, and unique thumbprint. Click **Yes**.

5. The final screen is simply an informational screen regarding the successful install of the CA certificate.

Certification Process – Requesting the Certificate

This phase of the certification process will involve requesting a computer certificate. Execute the following steps to request a computer certificate:

1. Click **Home** or connect to the Certificate Web site as done in step 2 from the previous section.
2. On the **Welcome** page under **Select a task**, verify the default **Request a certificate** is selected as shown in Figure 10. Click **Next**.

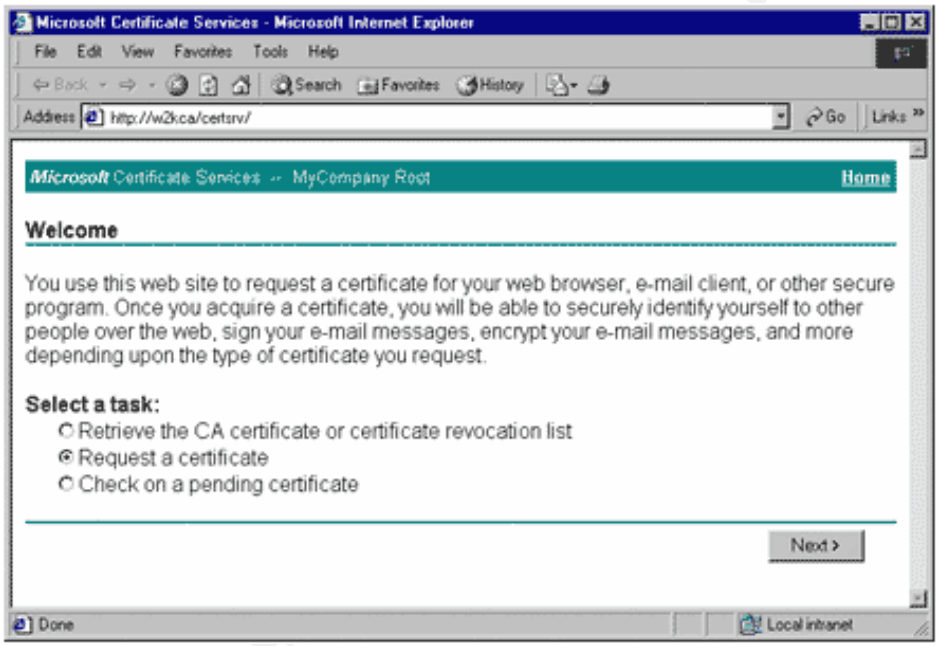

Figure 10

3. On the **Choose Request Type** page, note the default selection **User Certificate Request**. As stated earlier, IPSec uses computer certificates for computer-level authentication. To modify this setting, click **Advanced request** and then click **Next**.
4. Accept the default selection of **Submit a certificate request to this CA using a form** and click **Next**.
5. Now the details of the required certificate must be provided. This information provides two purposes: One, it allows the CA administrator (who must manually inspect each certificate request) to identify the requestor and check that the information being supplied is in accordance with acceptance policies. Two, this information determines the certificate's specification in terms of its usage and

security. For the RRAS server certification request, provide an applicable name such as RRAS server. For the **Intended Purpose**, specify **Server Authentication Certificate** (see Figure 11). For the VPN client, also provide an applicable name. However, for the **Intended Purpose** specify Client Authentication Certificate. Under the section **Key Options**, select **Create new key set.** Also select the **Use Local Machine Store** check box. This is key when requesting a certificate for a computer. Accept the other **Key Options** by clicking **Submit**. An informational screen will appear stating that the certificate is pending. This means that the certificate is waiting to be issued by the administrator. Once issued, the requestor must retrieve the certificate within 10 days.

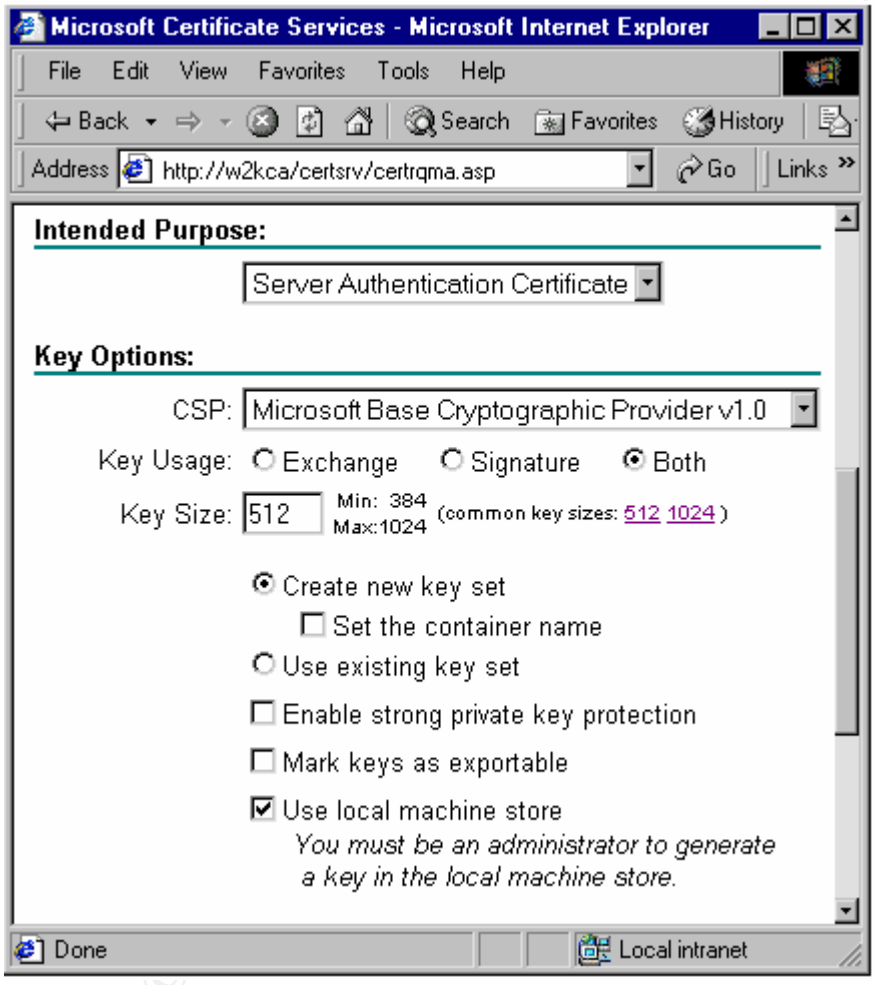

Figure 11

For the purposes of this scenario, the default Key Options were acceptable. Consider these additional options as well:

- *Cryptographic Service Provider (CSP*). Performs cryptography algorithms for authentication, encoding, and encryption.
- *Key Usage*. How the private key be used. "Exchange" means that the private key can be used to enable the exchange of sensitive information. "Signature" means

that the private key can be used only to create a digital signature. "Both" means that the key can be used for both exchange and signature functions.

- *Key Size.* The length, in bits, of the public key on the certificate. In general, the longer the key, the more secure it is. A longer key might be considered in a production environment.

Certification Process – Issuing the Certificate

As the role of the administrator, issue the requested certificates via the Certification Authority console on the CA server as follows:

1. Under the **Pending Requests** folder identify the new requests as shown in Figure 12. There should be two requests for this scenario, one request for the RRAS server and one for the client machine. Take the time to horizontal scroll through the column information. It is here where the administrator will verify the requestor's information before issuing the certificate.
2. To issue the certificate, right-click on the certificate in the details pane and select **All Tasks > Issue**. The entry will be removed from the **Pending Requests** folder and placed into the **Issued Certificates** folder.

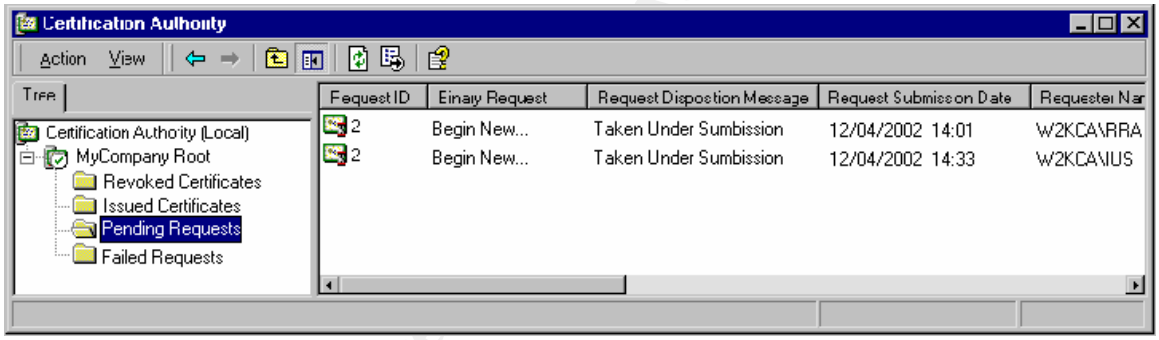

Figure 12

Certification Process – Installing the Certificate

As the role of the requestor, execute the following steps from both the RRAS server and the client machine:

1. Click **Home** or reconnect to the Certificate Web site.
2. Select **Check on a pending certificate** and click **Next.**
3. Select the requested certificate. If this is the only certificate requested by this machine, it will be selected by default. Click **Next.**
4. The next screen, as shown in Figure 13 displays the certificate was issued. Click on **Install this certificate**.

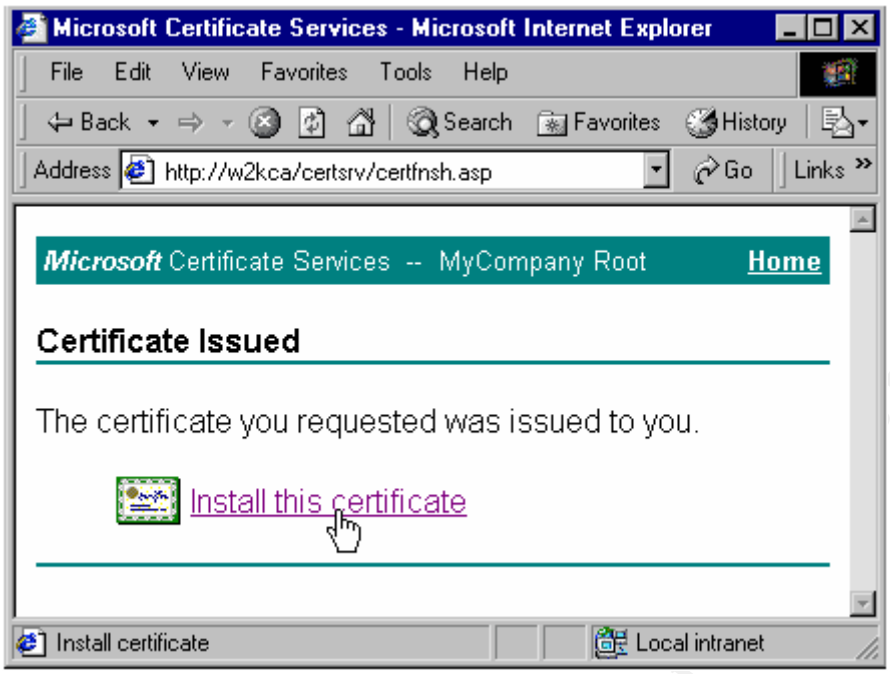

Figure 13

5. The final screen is an informational screen indicating the certificate has been successfully installed and to close the browser.

Certification Process – Final Analysis

In the initial phase of the certification process, a CA root certificate was installed on both the RRAS server and the VPN client computer. Computer certificates were then requested by each of the machines via the Certificate Services Web Page. Once the certificates were issued, each of the requesting computers was able to install the certificate, again through the Certificate Services Web Page. Upon a successful install of the certificate, the machines can now use IPSec.

Windows 2000 automatically generates IPSec policies for L2TP/IPSec connections. Because of this, the final step for VPN connectivity is to stop and restart the RRAS service on the RRAS server. Once this is done, the client machine should be able to make a VPN connection to the corporate LAN. The default L2TP Rule policy is in use on the server when the RRAS server is listening on L2TP ports and on the remote workstation when the client tries to connect over L2TP/IPSec. However, by default, this automatic IPSec policy for L2TP connections is hidden and is only viewable whenever it is in use. The policy is considered to be the L2TP Rule.

Additional Client Side Considerations

When weighing the options on whether to implement a Windows 2000 VPN using L2TP/IPSEC, one must also consider the client side as well. Both Windows 2000 and Windows XP as a VPN client support both L2TP/IPSec and PPTP by default. Other Windows clients such as Windows 98 and ME support only PPTP.

By default, Windows 2000 and Windows XP clients will attempt to make a VPN connection using L2TP/IPSec. If this fails, the client will then try to connect using a PPTP connection. Once the client connects successfully, verify the **Ports** listed in the RRAS Console. An active entry for a WAN Miniport (L2TP) VPN device indicates a successful L2TP/IPSec connection.

Ensure that the client's Internet connection is not going through a network address translation (NAT) server. Microsoft's IPSec implementation has known problems with NAT. Finally, if a firewall is in place between the client and the VPN server, the firewall may need to be reconfigured to allow the L2TP/IPSec connection through. This can be accomplished by opening UDP port 500 and IP port 50.

Summary and Conclusion

The methodologies described within this document are to provide the reader with insight on configuring a Windows 2000 VPN using only LT2P/IPSec. The decision to go with this more secure VPN is a decision that requires careful planning and consideration. This document should serve as a tool for just that scenario. LPT2/IPSec, when implemented correctly can ensure a much higher degree of security for the corporate VPN.

References

The Cable Guy. "Layer Two Tunneling Protocol in Windows 2000." August 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0801.asp (10 April 2002).

Microsoft Corporation. "Implementing a Microsoft Windows 2000 Network Infrastructure." Course Workbook. April 2000.

Microsoft Corporation. "Windows 2000 Virtual Private Networking Scenario." White Paper. 22 March 2000. URL: http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remoteaccess/w2kvpnscenario.asp (10 April 2002).

Norman, Ryan. "PPTP vs. L2TP: Which VPN protocol is right for you?" 15 September 2001. URL: http://www.win2000mag.com/Articles/Index.cfm?ArticleID=21991&pg=1 (19 April 2002).

Bailey, Carol. "Certifying your VPN." 22 February 2002. URL: http://www.zdnet.com.au/newstech/security/story/0,2000024985,20263625,00.htm (10 April 2002).

Bailey, Carol. "Customize the security of L2TP/IPSec connections." 18 December 2001. URL: http://www.techrepublic.com/article.jhtml;jsessionid=HPSZ3X1J3BCB2QD23UZCFEY?id=r00220011218cba01.htm (12 April 2002).

Microsoft Corporation. "L2TP over IPSec Connections." Windows 2000 Server Resource Kit: Supplement 1. 08 November 2000. URL: http://www.microsoft.com/WINDOWS2000/techinfo/reskit/en/Intwork/inbe_vpn_fxif.htm (10 April 2002).

Microsoft Corporation. "HOW TO: Allow Remote Users to Access Your Network in Windows 2000 (Q300434)." 09 April 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q300434#4 (15 April 2002).

Microsoft Corporation. "Enabling VPN in RRAS Causes Connection Issues to Remote Networks (Q243374)." 11 February 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q243374 (15 April 2002).

Elkins, Asa. "Layer 2 Tunneling Protocol (L2TP) with Internet Protocol Security (IPSec), as an alternative to the Microsoft's PPTP." 17 March 2001. URL: http://www.giac.org/practical/Asa_Elkins_GCNT.doc (19 April 2002).

Ellister, Mark. "Enabling Windows 2000 IPSec Using Certificates." 21 August 2001. URL: http://www.giac.org/practical/mark_ellister_gcnt.zip (19 April 2002).