Protect and Optimize Your VPN

Essential Techniques for Setup, Deployment, and Security
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose the VPN solution that best meets your business requirements</td>
<td>3</td>
</tr>
<tr>
<td>Avoid using split tunneling in your VPN connections</td>
<td>6</td>
</tr>
<tr>
<td>Implement a virtual private network for secure remote access, Part 1</td>
<td>7</td>
</tr>
<tr>
<td>Implementing a Virtual Private Network, Part 2: Configuring the server</td>
<td>11</td>
</tr>
<tr>
<td>Take control of your WLAN connections for a more secure Vista</td>
<td>14</td>
</tr>
<tr>
<td>The VPN wars: Which tunneling method is most secure?</td>
<td>18</td>
</tr>
<tr>
<td>Protect your network with VPN quarantine controls</td>
<td>22</td>
</tr>
<tr>
<td>Protect your network from telecommuter security threats</td>
<td>25</td>
</tr>
<tr>
<td>Protect remote clients by properly configuring Windows Firewall</td>
<td>30</td>
</tr>
<tr>
<td>Configure ISA Server to ensure secure communications between</td>
<td>34</td>
</tr>
<tr>
<td>remote offices</td>
<td></td>
</tr>
<tr>
<td>Don’t let hackers intercept your data: Protect it with a VPN</td>
<td>37</td>
</tr>
<tr>
<td>Validate your LAN-to-LAN VPN internally prior to its final deployment</td>
<td>40</td>
</tr>
</tbody>
</table>
Choose the VPN solution that best meets your business requirements

by Debra Littlejohn Shinder, MCSE

With the ever increasing need to support remote office workers and to securely interconnect partner sites, organizations invariably look to virtual private networking as their preferred solution. Not surprisingly, VPNs differ in their scope and purpose, so it’s important to identify which solution is most appropriate for meeting your business needs.

To help you decide on the best VPN solution for your organization, we’ll:

• Describe the most common VPN connections you’ll need to set up.
• Discuss the technology behind VPN authentication and encryption.
• Highlight key areas to consider when choosing a particular type of VPN.

Employees, business partners, customers, and others may need to access the resources on your company’s intranet. They could dial in to a remote access server, but it’s often more convenient and more cost-effective to use the internet. Unfortunately, the internet is a public non-secure network and as such can present a substantial risk to the communications that occur between parties.

Virtual private networks solve this problem by creating a secure tunnel between the endpoints of a communication channel. Security is implemented via authentication (requiring entities to prove their identity), encryption (masking real data as cipher text), or some combination thereof.

Types of VPNs
There are several ways to categorize VPNs. We’ll look first at the two ways in which VPN connections can be made. Then, we’ll discuss the popular VPN technologies supported by Windows 2000 Server and Windows Server 2003.

VPN topologies
In general, VPNs can connect in two different ways: Remote Access VPN, which is shown in Figure A, and Site-to-Site VPN, which is shown in Figure B. We describe their differences briefly here:

• Remote Access VPN. A single computer establishes a connection to a VPN server. The server can also act as a VPN gateway, providing access to other computers on the internal network.

• Site-to-Site VPN. Gateways at both ends of the connection establish a virtual private link between two LANs, allowing the computers on one LAN to communicate with those on the remote LAN.

VPN protocols
The three most popular VPN protocols in use today are:

• PPTP. Uses the Point-to-Point Tunneling Protocol (PPTP) and the Microsoft Point-to-Point Encryption Protocol (MPPE).

• L2TP. Uses the Layer 2 Tunneling Protocol (L2TP) and Internet Protocol Security (IPSec) for encryption.

• IPSec Tunneling Mode. Uses IPSec both to establish the tunnel and to provide encryption.
A fourth type of specialized VPN technology uses the Secure Sockets Layer (SSL) to create and secure the tunnel. SSL VPNs use the web browser to access remote applications, removing the requirement for VPN client software and reducing administrative overhead.

**Windows support**

Windows 2000 Server and Windows Server 2003 support PPTP and L2TP VPN protocols. Both operating systems can also use IPSec in tunnel mode, although Microsoft recommends this primarily for cases where the other end of the connection doesn’t support PPTP or L2TP.

Each VPN technology has advantages and disadvantages. Let’s look a little more closely at each.

**PPTP**

PPTP was developed by Microsoft. It’s based on the Point-to-Point Protocol (PPP) and uses the same authentication methods. Its level of security depends in part on which authentication method you choose, as described here:

- **Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) v.2.** Combined with a strong password policy, MS-CHAP provides good PPTP security.
- **Extensible Authentication Protocol-Transport Level Security (EAP-TLS).** With certificate-based smart card authentication, EAP-TLS provides even more security. This method requires a Public Key Infrastructure (PKI), so there’s more administrative overhead involved.

**Note:** PPP was designed as a remote access protocol for connecting to a dial-up server. It operates at the data link layer. PPTP encapsulates PPP packets within an IP packet, with a General Routing Encapsulation (GRE) header added that encrypts the GRE payload.

PPTP uses MPPE to encrypt VPN traffic. MPPE provides for data confidentiality using the RC4 algorithm. The encryption keys are 40 or 128 bit and are generated by the MS-CHAP, MS-CHAP v.2, or EAP-TLS authentication method.

**Note:** Early versions of PPTP had many security vulnerabilities. Most of these have been addressed in later releases and by using the proper authentication method.

PPTP is compatible with many different systems, making it a popular choice in cross-platform environments. These systems include:

- Windows 9x, Me, NT, 2000, XP, and Server 2003 operating systems include built-in PPTP client software.
- Macintosh OS X 10.2 and above also support PPTP out of the box.
- Client software for Linux and UNIX is readily available.

**Additional PPTP considerations**

Finally, when determining if PPTP is right for your circumstances, consider the following:

- You can use PPTP with client computers that are behind a Network Address Translation (NAT) device, as most NAT implementations include a PPTP editor.
- PPTP works well for point-to-point connections, but wasn’t designed for site-to-site connections.
- We recommend PPTP for organizations that need a medium level of security, easy implementation, and a high level of interoperability.

**L2TP**

The Layer 2 Tunneling Protocol was jointly developed by Microsoft and Cisco. It combines elements of PPTP and Cisco’s Layer 2 Forwarding (L2F) protocol. L2TP was designed to be more secure than PPTP because it uses certificate-based authentication in addition to PPP authentication.

L2TP uses IPSec to encrypt the VPN traffic. IPSec encryption provides data confidentiality like MPPE, but it goes further, providing the following security mechanisms for each packet:

- **Data integrity.** Assurance that the data hasn’t been modified in transit.
- **Data origin authentication.** Verification that the data really came from the sender who claims to have sent it.
- **Replay protection.** Prevents a hacker from capturing a transmission, such as the authentication process, and replaying it to gain access.

As is the case with PPTP, L2TP provides a high degree of support on different platforms, as described here:

- L2TP client software is built into Windows 2000, XP, and Server 2003. Microsoft provides L2TP client software for Windows 9x, Me, and NT as a free download.
- Macintosh OS X v. 10.3 (Panther) includes an L2TP client.
- An L2TP client/daemon for Linux is available.