MAS 90 Client/Server and Virtual Private Networking

MAS 90® Internet Capabilities over VPN

Technology White Paper

Sage™ Software, Inc.

Table of Contents

MAS 90 Client/Server and the Internet

The value of a Virtual Private Network (VPN) resides in the fact that an insecure public network (the Internet) can be used to securely connect accounting and bookkeeping departments from various remote offices. In addition, it is cheaper and easier to implement than one might think.

Network administrators are being forced to come up with secure, flexible and easy-to-administer solutions that are inexpensive. Those facing these challenges will say that traditional methods leave much to be desired. This is the challenge of remote access, and the benefit of Virtual Private Networking. Whether the user is a MAS 90 system administrator trying to post journal entries from off-site or a salesperson in need of inventory information to close a deal—the fact that the information exists is not enough. The data must be quickly and easily accessible.

Virtual Private Networking provides a secure, low-cost wide area network

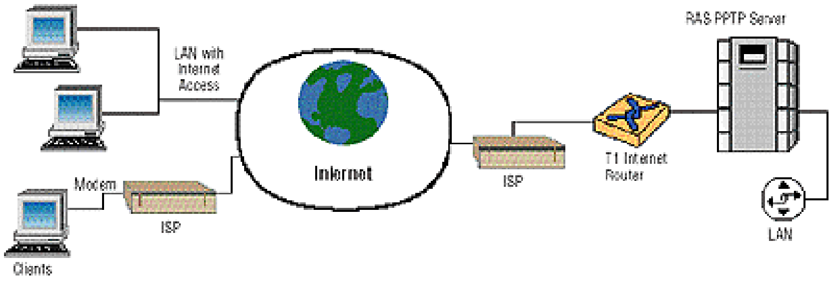
What Is VPN?

Virtual Private Networking (VPN) technology allows the use of an insecure public network (the Internet) for securely transferring private information. Instead of connecting through expensive public telephone lines, remote users can connect to the Internet and then “tunnel” through to their corporate server (See Figure 1). Similarly, you can avoid data transport costs by connecting two remote sites over the Internet instead of leasing an ATM (Asynchronous Transfer Mode) connection.

The Internet provides a free information “highway”

For example, there is no need to build a network to connect sites from New York to California; the Internet already provides this connection. Just as you would not plan to travel from New York to Los Angeles by building your own highway, you can leverage the existing public information infrastructure for moving data at reduced costs.

Figure 1. A Virtual Private Network. Network clients gain Internet access using a variety of methods. Then, by tunneling through the Internet, they form a secure connection with the remote server.



Problems and Solutions

Problems with traditional RAS and Leased Line scenarios include:

Eliminate long-distance costs for remote or traveling users

- Hardware costs and support—Not only are modem banks expensive, but they often lock you into a solution from a specific vendor. Upgrading a modem bank can be a significant expense. This increases hardware costs, support and administration headaches.
- Data transport costs—800 numbers and long-distance charges can be incredibly expensive to support traveling users. The costs of leasing and maintaining higher bandwidth site-to-site connections, though they are decreasing, are still significant.
- Low bandwidth—Traditional methods require access to a telephone line at low bandwidth, even if T1-speed Internet access from a LAN is in place.

The benefits of VPNs include:

- Keeping up with technology—With VPN, users apply technology independently of the server side, and each user may choose the best available method. For example, a single T1 line (1.54 Mbps) can support many remote clients using analog lines, ISDN, ADSL, cable modems or a network router. This is clearly more cost-effective and easier than managing large modem banks with various devices. It is the client's ISP (not the company's server) that must support the technology they are using. In most cases, the better-prepared ISP can handle basic support issues, such as client configuration and connectivity troubleshooting.
- No more busy signals—In contrast to the "traditional" remote access situation, if 10 users remain idle while reading e-mail messages, they will not be wasting any bandwidth (See Figure 2). Clients only use resources when they actually transfer data. Avoiding the "one port, one connection" effect allows many more concurrent connections within a fixed bandwidth.

VPN means more connections are possible over a fixed bandwidth

- Convenience—Today, Internet access is available through dial-up connections or over LANs. They are often more readily available and LAN Internet access is usually faster than the use of analog lines.
- Easy to implement and manage—Users on a Windows NT® Server-based network could be as close as an hour away from implementing a VPN while being able to use existing user accounts! Choose between the existing network infrastructure or outsource management to an ISP.

What Is PPTP?

PPTP makes Virtual Private Networks secure

Point-to-Point-Tunneling-Protocol (PPTP) is based on a set of standards ratified by the Internet Engineering Task Force (IETF) and is an extension to RFC 1171. This ensures that users will not be stuck with a single-vendor solution. Although Microsoft® only supports the Windows operating systems, PPTP clients can and have been written by third-party companies for Mac, UNIX® and other clients. Depending on how users implement a VPN, clients may not need to support this technology at all.

How to Implement a VPN?

A VPN can be implemented in several ways. The first is software-based with at least one NT Server running PPTP and Windows clients. The benefit is that it is cheap (free with current Microsoft Operating Systems) and easy to configure; but the problem is that it is only supported if the OS was written by Microsoft.

VPNs can be configured directly on the user's own servers, or through an Internet Service Provider (ISP)

What if this is not good enough? Users can choose a hardware-based VPN router from any of a number of vendors (3Com®, Ascend®, etc.). This router will automatically encrypt the data sent between two or more sites, and is therefore best suited for connecting LANs. UNIX-based systems are good candidates for this method of VPN implementation. A major benefit is that the existing network requires only minimal reconfiguration. Though VPN routers may be fast, this solution is often more expensive and will require some router configuration knowledge.

The third option is to outsource the VPN by having an Internet Service Provider (ISP) implement and manage it. This way, all remote users can continue using the same PPP connections (with no client reconfiguration) and still connect to existing network resources over the Internet. This is great when there are many remote users and user support is a considerable issue. The drawback is that users have less control over administration and policies. Outsourcing is best for larger companies that can choose an ISP with many Points of Presence (POPs) to avoid long-distance charges.

The final option is to utilize network-based Virtual Private Network services from a large network provider like AT&T or Concentric. While this really does not actually use PPTP or L2TP to encrypt the data, these network providers are large enough to allow several remote sites to connect to their local PPP connections where the user never actually touches the public Internet. This is essentially a huge WAN network with local telephone numbers maintained by a third party.

Choose encryption strength to balance performance with security

Accounting Data and Security

Remote access and security are not normally mentioned in the same sentence. In addition to enhanced MAS 90 security, VPN requires stringent Network Security. Two major issues involve authentication and data transport. Each implementation method entails various security measures. There are also several third-party products available, such as those based on the Remote Authentication Dial-In User Service (RADIUS) specification or Security Dynamics Technologies, Inc.'s SecureID.

For data transport, it is vital that encryption be used. Encryption strength ranges from 40-bit (for best performance) to 128-bit (for maximum security), based on the specific implementation.

As with all servers having a route to the Internet, one recommendation is to use some type of firewall to protect the network. The VPN server can be placed on either side of the firewall, depending on the network design. The most secure scenario would be to place the VPN server inside the dedicated firewall.

Unless users have working Internet experience, consulting with a specialist in this area can avoid many of the potential problems created by exposing the VPN device to the Internet.

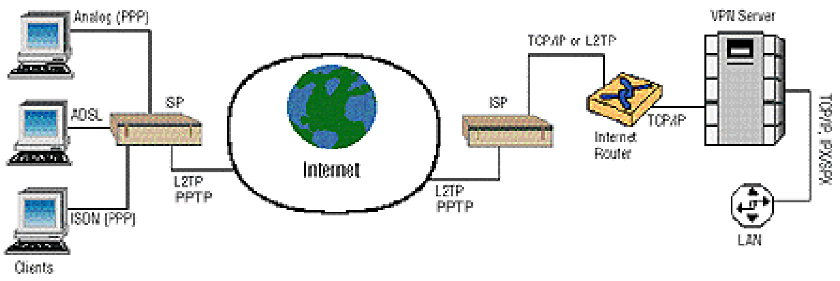


Figure 2. An outsourced VPN. All client types connect normally to their ISP. The ISP encrypts all data sent over the Internet and decrypts data at the remote network.

There are currently several protocols to choose from:

- *Point-to-Point Tunneling Protocol (PPTP)*—Microsoft's software-based standard is available free as part of current Microsoft OSs (Windows 95/98 and NT 4.0 and later).

- *Layer 2 Tunneling Protocol (L2TP)*—The future standard. Microsoft, Cisco and a host of other vendors are working on consolidating PPTP and L2F (Layer 2 Forwarding) into one specification. L2TP will be backward-compatible and available from Microsoft in the near future.

- *IPSecure (IPSec)*—Currently under development. When released, IPSec will handle the sending of encrypted data over the Internet. Final specifications are not yet available, but do not expect it to completely replace L2TP, since it is designed for LAN-LAN connections. However, Microsoft will support this protocol upon release.

Getting Started with Software Based VPN

The major benefit of setting up a Windows-based VPN include easy set-up and administration, and an unbeatable price (free…at least included with NT and Win9x). Look at the basic steps involved in setting up a Microsoft-based VPN.

For Microsoft-based systems, a software-based VPN provides the lowest-cost solution

Who is eligible? Microsoft currently supports PPTP on Windows NT Server (up to 256 concurrent connections), Windows NT Workstation (one connection at a time) and Windows 95. Rest assured both Windows 98 and NT 5.0 also support PPTP. For other client types (such as Mac and UNIX), users must obtain client software from a third party or go with an outsourced or hardware-based solution.

As with any "secure" solution, vulnerabilities can be found. Such was the case with Microsoft's implementation of PPTP in June 1998. Reports stated that passwords and data could potentially be stolen or compromised. The discoverers, B. Schneier and P. Mudge, at Counterpane Systems, claimed that this was the end of PPTP and that Microsoft's protocol should be deemed insecure. Microsoft, on the other hand, responded quickly with hot-fixes and claims to have addressed most of the problems.

Who should you believe, and what does this mean to you? If the proper patches are applied, a Microsoft-VPN continues to form a reasonably secure network (nothing is "bulletproof").

Moreover, it illustrates the importance of always thoroughly investigating the most recent patches before implementing a "secure" solution. More information can be found on the following sites:

www.counterpane.com/pptp.html—Counterpane Systems' original report of the problem, most of which have been addressed.

www.microsoft.com/security—The general security site for Microsoft.

Building A Secure Tunnel

Microsoft supports MS-CHAP (Challenge-Handshake Authentication Protocol) for authenticating remote users. This method is usually secure enough because it never actually sends the password over the line. However, check into third-party products such as the aforementioned RADIUS or SecureID if users are interested in additional authentication security.

If the VPN server is multi-homed (that is, has access to the Internet and a remote network), it is important to enable packet-filtering on the Internet interface. Though this is not a complete “firewall,” this feature recommendation restricts all access to the server except PPTP traffic (no more IP-based or NetBIOS attacks).

For PPTP to work from behind a firewall, all routers along the way must allow data to pass on Port 1723 and IP Protocol #47. Though this is usually not a problem on the Internet, users may need to verify their own network configuration. The default encryption is 40-bit, but for greater security upgrade to 128-bit (for North American use only). Finally, it is a good idea to enable auditing of logon attempts.

Bandwidth and latency factors affect the performance of the VPN

Bandwidth and Latency

While MAS 90 has been enhanced to perform admirably in a low bandwidth / high latency environment, the performance of accounting applications relies heavily on these factors.

For a Remote Access MAS 90 client using a direct telephone line connection, 28.8 kb is usually sufficient for acceptable MAS 90 performance. However in a Virtual Private Network scenario, processing overhead caused by encryption will affect performance. While Microsoft estimates less than a 10-percent decrease in performance, if the user is supporting many concurrent connections then consider switching to 33.6 kb as a minimum connection in VPN environments and closely monitoring server performance. For heads-down data entry, users may want to allow for up to 56 kb per user to ensure efficiency in the data entry process.

Latency is another potential problem due to the nature of the Internet itself—there is no promise that throughput will be consistent (after all, it is a public network). Latency is a function of the response time of each of the servers touched by a particular transmission. Picture bandwidth as the number of lanes on the street, and latency is a result of both the number of traffic lights and cars that are on the street. If guaranteed throughput is critical, check with the ISP about getting a service-level agreement.

Setting It Up

Setting up a VPN on a Microsoft Windows-based network is quite simple.

Server Installation

Configuring the server for a software-based VPN

On the server, first install the Remote Access Service (also known as "Dial-Up Server") if it is not already installed, by going to the Services tab in Network Properties.

While still in the area, install the Point-to-Point Tunneling Protocol (PPTP) by going to the Protocols tab in Network Properties. The PPTP install will ask how many VPNs to set up. Make this number equal to the maximum number of concurrent connections that the user plans to support.

Next, tell RAS to use the newly created virtual device (named VPN# - RASPPTPM). These logical devices work exactly like modems—configure them for dial-out, dial-in or both. Simply click on "Add…" on each port that should be enabled and specify it for dial-in.

Next, be sure to grant dial-in permissions to the appropriate accounts in User Manager or the newly installed RAS Administrator.

Finally, if the server is multi-homed, the user will need to enable IP Forwarding to reach other machines on the network. Also, the user should increase security on the server by enabling PPTP packet-filtering. Both options can be enabled in the TCP/IP properties. Assuming this machine has a connection to the Internet, the VPN server awaits!

Client Installation

Configuring workstations for a software-based VPN

On the client side (Windows 95/98 or NT 4.0), the process is very much the same.

First, install Dial-Up Networking (if it is not already installed).

Next, install PPTP and configure at least one virtual port.

After rebooting, set up a new Dial-Up Networking connection. But, instead of entering a telephone number, enter the name or IP address of the remote server. For the "modem", specify the VPN Port (named "RASPPTPM" on NT or "Microsoft VPN Adapter" on Windows 95).

Now, when in need of tunneling over the Internet, the user will first connect to the Internet (either via a LAN connection or by dialing up the ISP). Then, the user will make a second DUN connection (the one with the IP Address) to the remote server and authenticate on the remote server. Now, the user will be able to access the remote network resources (via the tunnel) as well as the Internet (via the ISP). If you are new to NT RAS, check out "Additional Information" for a resource that offers step-by-step configuration instructions.

On the MAS 90 Side

Once the VPN is configured to allow access to the network across the virtual network, the user is then ready to try MAS 90 Client/Server over the Internet.

First, make sure to ping from the client to the server and vice versa, both by host name and IP address. This is to ensure that all the TCP/IP traffic is being routed appropriately between the workstation and the server. The user should also be able to use the mping.exe utility found in the MAS 90\Home directory on the workstation to make sure that the client can access the specific port that the MAS 90 Host is listening on. If these items succeed, the user should now be able to successfully connect to MAS 90 from a workstation via the VPN.

MAS 90 client/server (3.31 and above) features that support the VPN option

New MAS 90 Features

Additional enhancements to MAS 90 will enable some of the Internet capabilities and the user will want to use these in many VPN environments.

Crystal Reports™ Web Server — With version 3.31 of the MAS 90 Client/Server for Windows NT, the software can take advantage of the Seagate Crystal Reports Web server mechanism to view reports. This option consists of installing the Crystal Reports Web Server on an NT Server with Internet Information Server (IIS), and configuring the MAS 90 workstations under Preferences to point to the Web reports server name and virtual directory. The Crystal Web Reports Viewer (ActiveX™ control) is then used to view Crystal reports and forms in a Web browser as opposed to the Crystal Runtime Viewer. The biggest benefit to this is that the Web server "page serves" the reports to the Web viewer. This means that if the user only wants to see page 1, 25, and 250…that is all the data which is sent over the network connection, thus minimizing network traffic (ideal in any scenario but essential in VPN environments). Note that this feature is not yet available for the UNIX platform.

Enhanced MAS 90 Security — Enabling the MAS 90 system administrator to maintain more discrete control of MAS 90 access is an important part of VPN enabling MAS 90. The system administrator can now specify whether or not to show a list of users at logon — making it more difficult to break into MAS 90 without knowing user ID and Password. The system administrator can also

specify a minimum password length, further tightening security. Additionally, the administrator can turn on "Intruder Detection" which will lock out a user after a specified number of failed logon attempts. Used in combination, these features make MAS 90 significantly more difficult to break into without explicit authorization and access.

Low Bandwidth Environment Switch — Enabling the low speed connection checkbox in the Workstation Preferences, tells the MAS 90 client that there may be a delay in downloading the screen form and necessary client-side code. The client will then display a "Form Loading" notice when the screen is not yet enabled due to bandwidth or latency issues.

Third Party Information

Refer to these 3rd party information sources for detailed VPN information:

Recommended reading: We recommend additional study before implementing a VPN

Internet.com's VPN information site:
http://webopedia.internet.com/TERM/V/VPN.html

Microsoft's Internet Service Network VPN site:
http://www.microsoft.com/ISN/hot_topic_vpn.asp

SCO's information on VPN:
http://www.sco.com/products/internet/products/sco_security1.htm

**56 Technology
Irvine, CA 92618
800-854-3415
www.sota.com**

The capabilities, system requirements and/or compatibility with third-party products described herein are subject to change without notice. Contact Sage Software for current information. Always consult a network specialist to discuss the security risks involved before implementing any VPN solution. Sage Software, Inc. is not responsible for the content or maintenance of the above Web sites. All information supplied by these companies is their sole responsibility, and Sage Software, Inc. does not endorse their claims. Sage Software does not warrant the information contained within this white paper.