IBM Netfinity 3500 Server

Achieving Remote Access using Microsoft Virtual Private Networking

July 1998

Introduction

This white paper describes how to build and configure a single server solution that will leverage the Internet to provide secure remote user access. This technology is called Virtual Private Networking (VPN). This paper focuses exclusively on configuring a Microsoft Virtual Private Network using an IBM Netfinity 3500 server. The work was performed at the IBM Kirkland Programming Center.

Remote Access Options and Problems

The question of how to provide remote access to users has long been a challenge for Network Administrators. The technological concept is not difficult, but the actual logistics required to provide access can be daunting, especially as the number of people requiring remote access grows.

The simplest and most straightforward method for providing remote access in a Windows NT environment is to use straight Remote Access Service (RAS). This provides basic, secure dial-in capabilities, but has significant limitations. The problem is that with straight RAS, there is a one-to-one relationship between the number of users needing access and the number of phone lines and modems required. For instance, if five people need to dial-in simultaneously to check e-mail or retrieve files, then five modems and five phone lines attached to the server are also needed. If a sixth person tries to dial-in, he/she would receive a busy signal and be locked out of the system until one of the original five disconnects.

As an environment grows, so does the need for additional equipment. As the number of people trying to dial-in grows to twenty-five, one hundred, or greater, a business can suddenly find itself overwhelmed in modem and phone line requirements. Clearly a better solution must be found.

Fortunately, an infrastructure capable of handling business needs in this area already exists—the Internet. Internet service providers (ISP) already have large banks of modems and phone lines in place for users to dial into—and the Internet exists as the backbone for network traffic.

Virtual Private Networking – The Concept

Virtual Private Networking (VPN) is a technology that takes advantage of the existing Internet infrastructure and allows businesses to leverage it for remote access. In fact, this technology is not limited to just the Internet, it will work with any TCP/IP-based network.

With VPN, a company can simply attach a server to the Internet and create virtual connection ports that can be accessed over the Internet. VPN supports up to 255 of these ports—which is the same number of simultaneous LAN/RAS connections that Windows NT Server supports.

Microsoft's implementation of VPN involves the Point-to-Point Tunneling Protocol (PPTP) which creates the secure tunnel across TCP/IP-based networks, such as the Internet, between the user's remote client system and the VPN server. The beauty of this protocol is that any Microsoft supported protocol (IPX/SPX, NetBeui, etc.) can be used on the internal network. PPTP will wrap itself around the entire data packet destined for the internal network, protocol and all.

Setting up the user's client systems is a relatively simple task. All that is required is a PPP (Point-to-Point Protocol) connection to the Internet and the installation of Microsoft's PPTP protocol on the client system. Basically, two simultaneous connections are made. The first establishes connectivity to the Internet through an ISP, and the second provides a secure, virtual connection to the VPN server. By choosing an ISP that has local phone numbers for dial-up, long distance charges can be saved as well.

Requirements and Tools

Your setup must include a server capable of running Microsoft Windows NT 4.0 server and two network devices – one attached to the Internet, the other attached to the LAN.

Server:

Hardware

IBM Netfinity 3500 Server. Single Pentium II 233 mhz processor, 256mb RAM configured with the following software.

Software

Microsoft Windows NT Server 4.0, Service Pack 3

Microsoft Proxy Server 2.0 w/ IIS 4.0

Updates

Routing and Remote Access Service (RRAS) Update—download from www.microsoft.com.

RRAS Hotfix from Microsoft—download from www.microsoft.com.
Any additional hotfixes or service packs that become available from Microsoft at a later date.

Client Requirements:

A computer capable of running Windows 9x or Windows NT 4.0 with a PPP connection to an ISP.

Note: To provide this functionality to Windows 95 clients, you must install a Dial-Up Networking update, available from Microsoft at www.microsoft.com.

Setting Up Your Server

IBM's Netfinity 3500 uses advanced hardware technology with updated drivers that were not available when Microsoft manufactured their Windows NT Server 4.0 compact disc. You can find these updated drivers in the *Server Guide* that ships with each server, or you can download them off of the Internet at www.pc.ibm.com/us.

In particular, without the updated Adaptec SCSI controller driver, the Windows NT Setup will not detect the primary hard disk controller and will fail to install. To remedy this, during the installation process, after Windows NT setup has detected the on-board IDE controller, choose to specify another device and insert the floppy disk containing the updated Windows NT driver. Also, Service Pack 3 must be installed before you can update the video driver.

Configuring a Simple VPN Server

Configuring a Microsoft VPN server is a relatively simple process as is indicated in the following steps.

1. After establishing a connection to the Internet, add PPTP to your configuration. To add PPTP:

   a) Open the Control Panel.
   b) Double-click the Network icon to open the Network Properties Window.
   c) Select the Protocols tab.
   d) Click the Add button.
   e) Choose Point-to-Point Tunneling Protocol.

   Since PPTP depends on RAS, adding this protocol will also invoke the RAS installation process, if RAS is not already installed.

2. Next, you will be prompted to choose the number of VPN's that you want to install on this server. Specify the number of simultaneous connections that you want the server to support.

3. Configure the VPN ports in RAS. This involves three steps:

   a) Add the dial-in ports.
   b) Configure the type of service.

c) Configure the network and authentication and encryption settings for the remote dial-in clients.

These tasks are performed from the Remote Access Setup dialog box. If setup does not take you to this automatically, open the Network Properties Window, click on the Services tab, and double-click the RAS service to get to the Remote Access Setup window.

4. Add a port for Dial-in.

   a) Click Add.
   b) Choose VPN1-RASPPTPM.
   c) Click OK.

   This adds VPN1 to your lists of available RAS ports in the RAS setup window. It is best to add and configure this one port first, and then click on the clone button to create the additional ports; otherwise, you will have to configure each port individually.

5. Configure the type of service.

   a) Click the Configure button at the bottom of the window.
   b) Choose whether you want this port to be able to dial-out as a RAS client, receive calls as a RAS server, or both. In most cases, you will choose to receive calls as a RAS server only.
   c) Click OK. You will return to the Remote Access Setup window.

6. Configure the network and authentication and encryption settings for the remote clients.

   a) Click the Network button.
   b) Choose the type of protocol you are running on your internal network
   c) Click Configure. Specify whether you want the dial-in clients to have access to the entire internal network, or just the VPN server.
   d) Choose the type of encryption and authentication that you want to require. The stronger the encryption type, the more secure the network. It is important to remember the client's settings must match the settings on the server.

7. For security purposes, enable PPTP filtering. This causes the adapter connected to the Internet to block all packets except PPTP—this includes TCP/IP utilities such as *ping* and *tracert*. PPTP filtering can only be enabled on Network adapters and cannot be enabled on modems.

8. Enable IP forwarding—otherwise no packets will be passed between the two adapters. To do so:

   a) Open the Control Panel.
   b) Double-click the Network icon.
   c) Select the Protocols tab.
   d) Select TCP/IP Protocol.
   e) Click the Properties button.

f) Select the Routing tab.
g) Check the *Enable IP Forwarding* check box.

9. Suppress the default route on the private network.

   By default, Windows NT places a default route (0.0.0.0) on each network. This causes the server to send packets of unknown IP addresses to the network adapter configured with the default route. You must change the default if a computer is connected to both the Internet and a private network. To suppress the default route:

   a) Open the Windows NT Registry.
   b) Add the *DontAddDefaultGateway* entry to the Registry with a value of REG_DWORD 0x1 in the following location:

      *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\<private network adapter>\Parameters\Tcpip**DontAddDefaultGateway***

      Note: If you don't recognize your network adapter name in the Registry, open a command prompt, run ipconfig and find it from there.

10. Disable source packets.

    RAS changes the source IP address of packets it routes, from the IP address of the client sending the packets to its own source IP address. This must be disabled in order for LAN-to-LAN routing to work.

    On the PPTP server, add the registry entry *DisableOtherSrcPackets* with a value of REG_DWORD 0 in HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RasArp\Parameters. This prevents RAS server from changing the source IP address of the packets it forwards.

11. Add static routes to your private network on the PPTP server by using the ROUTE command at the command prompt. The ROUTE command can help you identify all computers or networks you want your remote PPTP clients to reach.

    For more information on the ROUTE command, see the Windows NT Server version 4.0 *Networking Supplement*, Chapter 4, "Routing in Windows NT or the Microsoft Knowledge Base article, number Q12877, available online at www.microsoft.com. These updates to your routing table must always be available—add them by using the route command with the –p option (for persistent connections) or create a batch file in the startup folder that will execute each time the server is booted.

For more detailed information on configuring a VPN server, consult the Microsoft document *Virtual Private Networking – Installing, Configuring, and Using PPTP with Microsoft Clients and Servers. User and Administrator Guide.*

MS Proxy Server and VPN

At this point, you have a working VPN server that will provide access for remote clients to the local network. For additional security, and/or to provide internal access to the Internet, use VPN technology in conjunction with MS Proxy Server. For our purposes in this paper, we will focus exclusively on providing external access into the internal network, and not on providing Internet access from within the local network. In our example, we are combining MS Proxy Server and the VPN server into one system—although they can exist separately with the PPTP server sitting behind the firewall. Microsoft VPN servers can also exist with third-party firewall products, provided they can pass PPTP packets.

Install the following additional software onto your VPN server:

- MS Proxy Server 2.0
- Internet Information Server 4.0 (earlier versions of the product may not work)
- Routing and Remote Access Service Update (RRAS)
- RRAS hotfix

Although MS Proxy Server is a separate product, you can download the RRAS update and the RRAS hotfix free of charge at www.microsoft.com.

When the RRAS update is installed on a server running MS Proxy Server, IP forwarding is enabled. This allows the Windows NT Server to forward packets from the external Internet to the private internal network. However, this allows all security to be bypassed unless local host filters are configured. This portion of the white paper describes how to correctly and securely configure a MS Proxy-VPN server.

Configuring RRAS

Configure filters on the external network adapter so that only PPTP packets can be passed through. You must set three input and three output filters. All six filters work together to make a complete PPTP filter. The PPTP filtering option you set when configuring a simple VPN server no longer works once RRAS is installed.

1. Before any filters will work, you must enable packet filtering. To do this:
   a) Open the Routing and RAS Admin tool.
   b) Right-click the external interface.
   c) Select *Configure IP Parameters* from the Pop-up Menu.
   d) Select the *Enable Packet Filtering* check box.

2. Set the PPTP filters. As you set the PPTP filters, keep in mind that PPTP uses TCP Port 1723 and IP Protocol ID 47. To set the filters:
   a) From the Start menu, select Programs, Administrative Tools, Routing and RAS Admin.
   b) In the left pane, under IP Routing, click Summary.

c) In the right pane, right-click on the external interface card.
d) Choose Configure Interface to open the IP configuration window.
e) Make sure the *Enable IP router manager on this interface* box is checked.
f) Click the Input Filters button to begin adding the filters. This opens the *IP Packet Filters Configuration* window.
g) Click the *Add* button to open the *Add/Edit IP Filter* window.

   For all input filters, you must add the source network IP address and subnet mask (that is, the address and mask of the external network adapter). If the IP Address and Subnet mask box are grayed out, uncheck the *Source Network* box and check it again—this should clear the problem.
h) In the Protocol box, select Other.
i) Type **47** and click OK. This returns you to the *IP Packet Filters Configuration* window, which lists the filter you just added.
j) To add the second filter, click Add.
k) In the Source port box, type **1723**.
l) In the Destination port box, type **0** and click OK.
m) For the third filter, do the same except type in **0** in the Source port box and **1723** in the Destination Port box.
n) Click OK. This returns you to the *IP Packet Filters Configuration* window.
o) Make sure *Drop all except listed below* is selected and click OK.
p) Select the *Output Filters* button and add the same filters for them.

Configuring the MS Proxy Server

1. Configure the MS Proxy server for an Internet connection and make sure your Local Address Table is configured correctly. Consult the Proxy Server checklist in the Security White Paper on Microsoft Proxy Server available at www.microsoft.com/proxy.

2. For Proxy server and RRAS to work together on the same server, the pre-defined filter PPTP RECEIVE must be enabled on Proxy Server. To do so:

   a) From the Start menu, select Programs, Microsoft Proxy Server, then Microsoft Management Console.
   b) Right-click Socks Proxy.
   c) Select Properties from the pop-up menu.
   d) Click the Security button.
   e) Make sure *Enable Packet filtering on External Interface* is checked.
   f) Click Add.
   g) Choose Pre-defined filter and select PPTP RECEIVE.
   h) Click OK.

For more thorough security information about MS Proxy Server, refer to the *Security White Paper on Microsoft Proxy Server* available at www.microsoft.com/proxy. This document also provides a checklist of security provisions that should be used.

References/Additional Information

IBM Netfinity Server Information – www.pc.ibm.com/us/netfinity

Understanding PPTP White Paper – www.microsoft.com

Security White Paper on Microsoft Proxy Server – www.microsoft.com/proxy

Virtual Private Networking – Installing, Configuring, and Using PPTP with Microsoft Clients and Servers. User and Administrator Guide – www.microsoft.com

Windows NT Server version 4.0 *Networking Supplement*, Chapter 4, "Routing in Windows NT or the Microsoft Knowledge Base article number Q12877 - www.microsoft.com

Published by the IBM Kirkland Programming Center, IBM Corp.