The following are the steps you would need to take if you want to configure a VPN on a Windows 2003 server where you only have a single network card (NIC) exposed to the Internet. What we will do here is configure a site-to-site VPN so that clients can connect securely while still allowing other types of web traffic such as HTTP (port 80) and/or RDP (port 3389) to connect. This method sets up a secure tunnel for clients while allowing other types of web-based services to still be open and exposed on the same network card.

Normally, when you set up a VPN, you should use a dedicated network card and a dedicated card for other traffic. In most cases, a site-to-site VPN would be the only service set up on a single network card and the firewall would be controlled by an external firewall in front of the server. But Microsoft does provide a way to configure Windows Server 2003 to allow VPN and other web services on the same card.

The way to do this is to have the VPN be the front facing network service exposed to the Internet. Then we configure Windows 2003 to run Network Address Translation (NAT) services to manage the traffic coming in from this card. The big problem is that you usually have to have a remote firewall configured in front of this server. But Microsoft provides a useful component in the NAT services called "Basic Firewall". This has a similar interface to Windows Firewall so it can be configured to allow / deny ports and services while the VPN is enabled. Here are the steps to configure Windows 2003:

In Administrative Tools, open the **Routing and Remote Access** dialog.


If you have the **Windows Firewall** running on your server, you will see a dialog that says that ICF must be disabled before continuing. If you see this dialog, you must disable your Windows Firewall before continuing. The next couple of steps show how to do this.


In Administrative Tools, open the **Services** dialog and find the **Windows Firewall/Internet Connection Sharing (ICS)** entry. Click the "Stop the service" link to stop the service.


Double-click the service and set it's Startup type to "Disabled". This will make it so that the Windows Firewall does not run anymore and is completely disabled. Click OK.


Right-click your server name in the Routing and Remote Access dialog (it should be the item with little server icon that has a red stop square on top of it) and select **Configure and Enable Routing and Remote Access**.


Click Next on the Routing and Remote Access Server Setup Wizard.


Select **Custom configuration** and click Next.


In the Custom Configuration, select **VPN access** and **NAT and basic firewall** and click Next.


Click Finish to complete the setup.


When you click Finish, a dialog will ask you if you want to start the server and being running the Routing and Remote Access. Choose Yes.


After you wait for just a second, the routing server comes online and you will see a tree of options open up underneath your server icon. Your server icon will also change from a red square to a green square to show you that it has been started successfully.


Right-click the **NAT/Basic Firewall** and choose **New Interface** from the context menu.


We are going to configure the firewall settings for the connection that has the VPN running on it. Choose your network card by name from the list. In most cases, this will be **Local Area Connection** as this is the default name of the NIC that Windows assigns.


in the Network Address Translation Properties dialog, select **Basic firewall only**.


Click on the **Services and Ports** tab and click on **IP Security (IKE)**.


Once you click on the IP Security (IKE) entry, a edit box will immediately come up. You need to set up where NAT should route this traffic when received in the firewall. Just set all traffic to route directly to the local server (since this is where all the services are running) by setting the IP to itself (127.0.0.1).


Do the same with **IP Security (IKE NAT Traversal)**, **VPN Gateway (L2TP/IPSec - running on this server)**, and **VPN Gateway (PPTP)**. Each one will need to be set to 127.0.0.1 the same as the above dialog. NOTE: For any other ports you want to open, do the same process to expose them in the firewall. The IP Security and VPN Gateway are the only required to enable the VPN to actually show from the NAT service. Then click OK.


Right-click the server name (the one with the green icon) and select **Properties**.


Click on the **IP** tab and select **Static address pool**. This will enable the Add button. Click the Add button to edit the range IP's. You need to set a static range of IP addresses that will be used on the internal network that the VPN creates.


Set a range for the IP addresses that will be assigned for the local network that the VPN creates. The Number of addresses will automatically be calculated for you. Click OK.

**VERY IMPORTANT:** Make sure you set a range for the IP addresses that is unique and not likely to be on another network or there will be conficts if the client connects from a network with the same subnet.


Click OK to close the properties dialog.


In Administrative Tools, open the **Computer Management** tool (unless you are running Active Directory on your server and then you would need to add the user from there). Tree open Local Users and Groups -> Users and right-click Users to select **New User...**.


Create the new user as you would normally. Click the Create button and then click Close to close the dialog.


Right-click the new user account you just created and select **Properties**.


We have to enable this account to allow VPN login to this server. On the user properties dialog, click on the **Dial-in** tab. Then select **Allow access**. Click OK to apply the change.
