

## Howto - Intro to Network Security 3

In Part 2 of this article series, I walked you through the process of installing an Enterprise Certificate Authority that was to be used by a VPN Server. In this article, I will continue the discussion by showing you how to configure the necessary VPN Server. For the purposes of this article series, I will be installing the Network Policy Server onto the same physical computer as will be used for the VPN Server. In a real world deployment, you would usually want to use two separate computers to host these roles. Hosting both roles on the same computer should only be done in a lab environment.

**Basic Configuration Tasks** Before I show you how to configure this server to act as a VPN server, you must perform some basic configuration tasks. Essentially, this means that you must install Longhorn Server and configure it to use a static IP address. The IP address must fall into the same range as the domain controller that you configured previously. The server's Preferred DNS Server setting in its TCP/IP configuration should point to the domain controller that you set up earlier in this series, since it is also acting as a DNS server. After you finish performing the VPN server's initial configuration, you should use the PING command to verify that the VPN server can communicate with the domain controller.

**Joining a Domain** Now that you have specified the machine's TCP/IP configuration and tested its connectivity, it's time to get started with the real configuration tasks. The first thing that you will have to do is to join the server to the domain that you created earlier in this series. The process of joining a domain works very similarly in Longhorn Server to the way that it works in Windows Server 2003. Right click on the Computer command found on the server's Start menu. Upon doing so, Longhorn will open the Control Panel's System applet. Now, click the Change Settings button found in the Computer Name, Domain, and Workgroup Settings section of this screen. Doing so will reveal the System Properties sheet. The System Properties sheet is nearly identical to the one found in Windows Server 2003. Click the Change button to reveal the Computer Name Changes dialog box. Now, select the Domain radio button found in the dialog box's Member of section. Enter the name of your domain into the Domain field and click OK. You should now see a dialog box prompting you for a set of credentials. Enter the username and password for a domain administrator account, and click the Submit button. After a brief delay you should see a dialog box welcoming you to the domain. Click OK, and you'll see another dialog box telling you that you must restart your computer. Click OK one more time, followed by the Close button. When you restart the computer, it should be a member of the domain that you specified.

**Installing Routing and Remote Access** Now it's time to install the Routing and Remote Access service. We will then configure this service to act as a VPN server. Begin the process by opening the Server Manager. You can find a shortcut to the Server Manager on a Administrative Tools menu. When the Server Manager opens, scroll to the Roles Summary section found in the details pane. Now, click the Add Roles link to launch the Add Roles Wizard. When the wizard opens, click Next to bypass the Welcome screen. You should now see a screen prompting you to which roles you want to install on the server. Click the checkbox corresponding to the Network Access Services option. Click the Next button and you will be taken to a screen that presents you with an introduction to the Network Access Services. Click Next one more time and you will see a screen prompting you to select the Network Access Services components that you want to install. Select the check boxes corresponding to Network Policy Server, and Routing and Remote Access Services. When you select the Routing and Remote Access Services check box, the Remote Access Service, Routing, and Connection Manager Administration Kit check boxes will be selected automatically. You must leave the Remote Access Service check box selected because this will install the components that will be necessary for the server to act as a VPN. The other two check boxes are optional. If you want the server to function as a NAT router or to use routing protocols such as IGMP proxy or RIP, then you'll need to leave the Routing check box selected. Otherwise, you can deselect it. Click the Next button and you will be taken to a screen that displays a summary of the services that are about to be installed. Assuming that everything looks good, click the Install button to begin the installation process. It is anybody's guess as to how long the services will take to install when a final version of Longhorn Server is released. However, on my test server that is running a beta version of Longhorn, the installation process took several minutes to complete. In fact, the server gives the illusion that it has locked up during the installation process. When the installation process completes, click the Close button. After the Network Access Services have been installed, it is time to configure the Routing and Remote Access Services to accept VPN connections. Begin by entering the MMC command at the server's Run prompt. Doing so will open an empty Microsoft Management console. Choose the Add/Remove Snap-in command from the File menu. Windows will now display a list of available snap-ins. Choose the Routing and Remote Access Snap-in from the list, and click the Add button, followed by the OK button. The Routing and Remote Access snap in should now be loaded into the console. Right-click on the console's Server Status container and select the Add Server command from the resulting shortcut menu. When prompted, choose the This Computer option and click OK. The console should now display a listing for your server. Right click on the listing for the server and select the Configure and Enable Routing and Remote Access command from the resulting shortcut menu. This will cause Windows to open the Routing and Remote Access Server Setup Wizard. Click Next to bypass the wizard's welcome screen. You should now see a screen asking you which configuration you want to use. Choose the Remote Access (dial-up or VPN) option and click Next. The following screen will give you a choice between configuring dial-up or VPN access. Choose the VPN check box and click Next. The wizard will now take you to the VPN connection page. Now, choose the network interface that will be used by clients to connect to the VPN server and deselect the Enable Security on the Selected Interface by Setting up Static Packet Filters check box. Click Next and then select the From a Specified Address option and click Next again. At this point, you'll see a screen asking you to enter an IP address range that can be assigned to VPN clients. Click the New button and enter a beginning and an ending address for the IP address range. Click OK, followed by Next. Windows will now open the Managing Multiple Remote Access Server's page. The next step in the process is to choose the Yes option to configure the server to work with a Radius server. You will now be prompted to enter the IP address for your Radius server. Because

NPS will be running on the same box as the Routing and Remote Access Services, just enter the servers own IP address as the primary and secondary Radius server address. You will also be prompted to enter a shared secret. For demonstration purposes, just enter rras as the shared secret. Click Next followed by Finish. You will now see a couple of warning messages. Just click OK to close each message. The last step in the RRAS configuration process is to set up the authentication scheme. To do so, right click on the listing for your server and select the Properties command from the resulting shortcut menu. When you see the server's properties sheet, go to the Security tab. Now add EAP-MSCHAPv2 and PEAP to the Authentication Methods section and click OK.