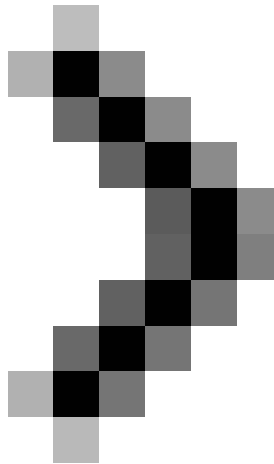
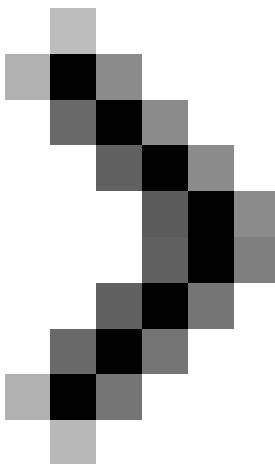


# Introduction to Network Access Protection (Part 3)

In Part 2 of this series, we went through the entire Enterprise Certificate Authority (ECA) installation process used by a server. In this article, I will continue the discussion by showing you how to configure the necessary VPN server.



**Introduction to Network Access Protection (Part 1)**



## **Introduction to Network Access Protection (Part 2)**

**In Part 2 of this series, we went through the entire Enterprise Certificate Authority (ECA) installation process used by a 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, we will install the Network Policy Server to a computer that is configured as the computer used for the VPN server. In real world deployments you always want to use two separate computers to configure its roles. Configuring both roles on the same computer should only be done in the lab.

### **Basic configuration tasks**

Before discussing how to configure this server as a VPN server, you must perform some basic configuration tasks. In essence, that means you have to install Longhorn Server and configure it to use a static IP address. The IP address must be placed in the same range of domain controllers that you have previously configured. The server's Preferred DNS Server setting in its TCP / IP configuration needs to specify the domain controller you set up in this series when it is also executing as a DNS server. After you finish executing the VPN server's initialization configuration, you should use the 'ping' command to verify that the VPN server has communicated with the domain controller.

### **Connect to a domain**

You have specified the machine's TCP / IP configuration and checked its connection and now it's time to start with the actual configuration tasks. The first thing to do is to enter the domain name into the server you created in the previous section. The process of entering a domain name on Longhorn Server is similar to that in Windows Server 2003. Right-click the Computer command found on the server's Start menu. To do so, with

Longhorn Server you will open the Control Panel System applet. Now click on the Change Settings button in the Computer Name, Domain, and Workgroup Settings section of this screen. That way you will discover the properties of the System Properties system. System Properties is no different than in Windows Server 2003. Click the Change button to enter the Computer Name Changes dialog box. Click the Domain button, enter the domain name in the Domain field and click OK.

You should see the dialog box that is prompted to set up some functions. Enter the username and password for the domain admin account, click the Submit button. After a while you will see a welcome dialog. Click OK and you will see a dialog box telling you to restart the computer. Click OK again, after the Close button. When restarting the computer, you will be a member of the specified domain.

### **Install remote access and routing**

You must now install the remote access service and route Routing and Remote Access. We will then proceed to configure this service to work as on a VPN server. Start the process by opening the Server Manager. You can find a shortcut to Server Manager on the Administrative Tools menu. When Server Manager opens, drag the section in the details window and then click the Add Roles link to create the Add Roles Wizard.

When the wizard opens, click Next to bypass the original window. You should watch the window prompting you to choose which role to install on the server. Click the checkbox corresponding to the Network Access Services option. Click the Next button and you will see a screen that introduces Network Access Services network access services. Click Next again and you will see a window asking you which Network Access Services components you want to install. Select the checkboxes for Network Policy Server and Routing and Remote Access Services.

When you select Routing and Remote Access Services, Routing and Remote Access Services, Remote Access Service remote access, Routing routing, and Connection Manager Administration Kit, the checkboxes are automatically ticked. . You must uncheck the Remote Access Service check box that has been selected because it will install the components that will be needed for the server to work as a VPN. The other two checkboxes are optional. If you want the server to function as a NAT router or use protocols such as IGMP proxy or RIP, then you need to uncheck the Routing section.

Click Next and you will see a window showing the types of services you will have installed. If everything goes well, click the Install button to begin the installation process. Maybe what you want to know here is how long it will take to install this for the final version of Longhorn Server released. Our test was performed on a test version of Longhorn Server and the installation took a few minutes to complete. In fact, the server will give you the feeling that it is locked during installation. When the installation is complete, click the Close button.

After you install Network Access Services, you configure Routing and Remote Access Services to accept VPN connections. Start by entering the MMC command into the server's RUN command window. By doing so you will open a blank Microsoft Management console (MMC). Select Add / Remove Snap-in from the File menu. Windows will show you a list of available software modules. Select the Routing and Remote Access software module in that list and click the Add button then click OK. This software module will be loaded into the working interface.

Right-click on the console's Server Status section and select Add Server from the resulting shortcut menu. When prompted, select this computer option and click OK. The user interface will display a list of your servers. Right-click the list with the server and select Configure and Enable Routing and Remote Access from that menu. The Routing and Remote Access Server Setup Wizard window will open.

Click Next to bypass the wizard's welcome screen. You should look at the following window, which asks you which configuration you want to use. Select the Remote Access option (dial-up or VPN) and click Next. The following window will give you a choice between configuring dial-up or VPN access. Select the VPN checkbox and click Next.

The wizard will take you to the VPN connection section, select the network interface that will be used by the client to connect to the VPN server and uncheck Enable Security on the Selected Interface by Setting up Static Packet Filters checkbox. Click next and then select the From a Specified Address, then click Next again.

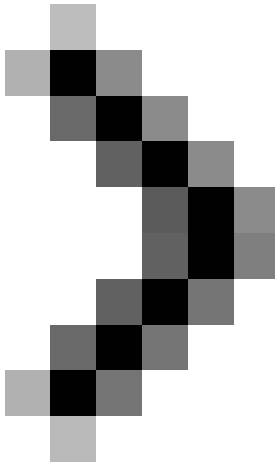
Here, you will see a window asking you to enter the range of IP addresses that can be assigned to VPN clients. Click the Next button and enter the first and last addresses for the range of IP addresses. Click OK, then Next. Windows will open the Managing Multiple Multiple Access Server window

The next step in this process is to select the Yes option to configure the server to work with a Radius server. You will be prompted to enter the IP address for the Radius server. Because NPS will run with Routing and Remote Access Services, you only need to enter the servers with the primary IP address and the secondary Radius address. You will also be prompted to enter a similarly issued secret. For demonstration purposes, simply enter rras. Click Next then Finish. You will see a few warnings. Click OK to close these alerts.

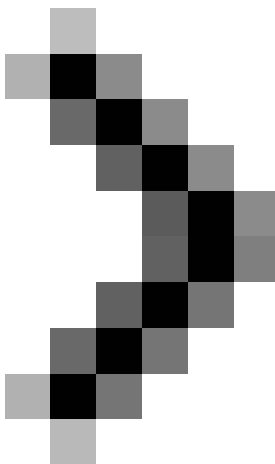
The final step in the RRAS configuration process is to set up the validation diagram. To do this, right-click on the server list and select Properties. When you see the server properties, go to the Security tab. Add EAP-MSCHAPv2 and PEAP to the Authentication Methods section and click OK.

## **Conclude**

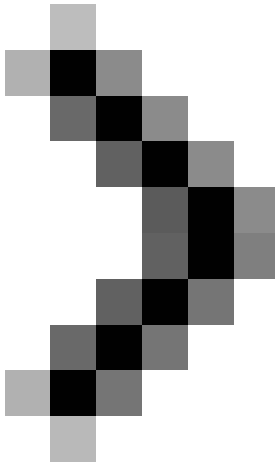
In this section, we have shown you how to install and configure Remote Access and Routing Services and Routing and Remote Access Services in a way that allows the server to work as a VPN server. . In the next article in this series, I will continue the discussion by showing you how to configure the Network Policy Server component.



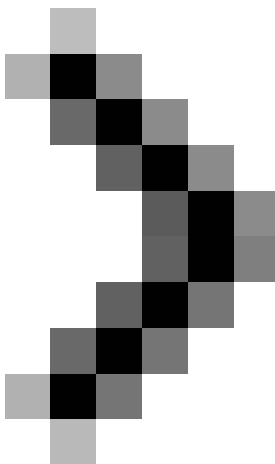
#### **Introduction to Network Access Protection (Part 4)**



#### **Introduction to Network Access Protection (Part 5)**



**Introduction to Network Access Protection (Part 6)**



**Introduction to Network Access Protection (Part 7)**

You finished reading the article "**Introduction to Network Access Protection (Part 3)**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

---