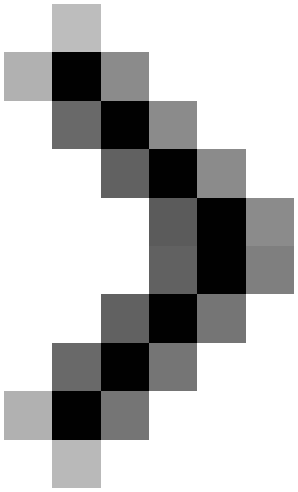
Configure Windows Server 2008 to remotely access SSL VPN Server (Part 2)

In the first part, we talked about some of Microsoft's previous VPN and VPN protocols. To continue what we have seen in part one, we will give you a description of the network example that will be used in configuring the VPN gateway to be able to



Configure Windows Server 2008 to remotely access SSL VPN Server (Part 1)

Thomas Shinder

In the first part, we talked about some of Microsoft's previous VPN and VPN protocols. To continue what we have seen in part one, we will give you a description of a network example that will be used in configuring the VPN gateway to support SSTP connectivity from Vista SP1 clients. .

We will not cover all the steps, but we will assume that you have installed DC and enabled roles such as DHCP, DNS and Certificate Services on that server. The server certificate type is Enterprise, so you will configure an enterprise CA on your network. The VPN server will be entered into the domain before starting the steps below. Vista clients need to be upgraded to SP1 version before following this guide.

We need to perform some of the following procedures:

1. Install IIS on the VPN server
2. Request a computer certificate for the VPN server using the IIS Certificate Request Wizard
3. Install the RRAS server role on the VPN server
4. Activate the RRAS Server and configure it to be a VPN server and NAT
5. Configure NAT server to publish CRL
6. Configure User Account to allow dial-up connections
7. Configure IIS on the Certificate Server to allow HTTP connections for the CRL directory
8. Configure HOSTS file on VPN client
9. Use PPTP to connect to the VPN server
10. Obtain the CA certificate from the Enterprise CA
11. Client configuration to be able to use SSTP and Connect for VPN Server using SSTP

Install IIS on the VPN Server

You may find it strange because usually we still recommend that you never place a web server (Web server) in front of a network protection device. This is because we do not need to keep the Web server on a VPN server but only need to use it at some point. Because the Web enrollment site including Windows Server 2008 Certificate Server is not useful for requesting computer certificates. In fact, it is absolutely not used. What is interesting here is that you can get a computer certificate using the Web enrollment site.

To solve this problem, we will take advantage of enterprise CA. When using enterprise CA, you can make a request to an online certificate server. The online request for a computer certificate is allowed when you use the IIS Certificate Request Wizard and request a 'Domain Certificate' - a domain certificate. This problem only works when the computer requests a certificate with the Enterprise CA domain name.

Follow these steps on the VPN server to install the IIS Web server role:

1. Open Windows **Server Server Manager**

2. In the left pane of the console, click the **Roles** button

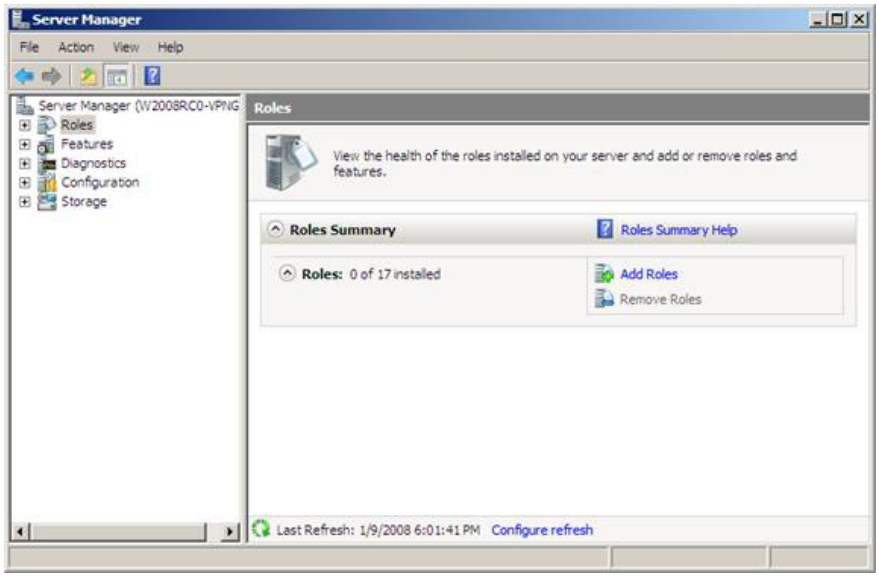


Figure 1

3. Click the **Add Roles** link in the right part of the right pane.

4. Click **Next** on the *Before You Begin* window

5. Check the **Web Server (IIS)** checkbox on the *Select Server Roles* window and then click **Next** .

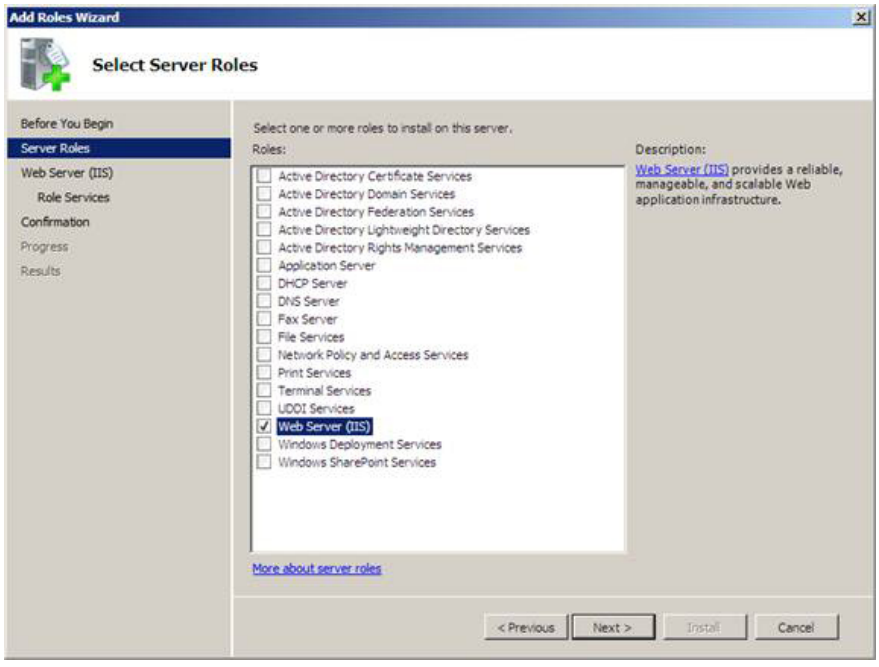


Figure 2

6. Read the information on the *Web Server (IIS)* window if necessary. This is a great overview for using IIS7 as a Web server, but since we will not use IIS Web server on the VPN server, this information does not apply to

their scenario. me.

7. On the *Select Role Services* window, there are a number of options already selected. Even if you use the default options, it doesn't make sense to use the Certificate Request Wizard. So check the **Security options** to have the *Role Service* for the Certificate Request Wizard and then click **Next** .

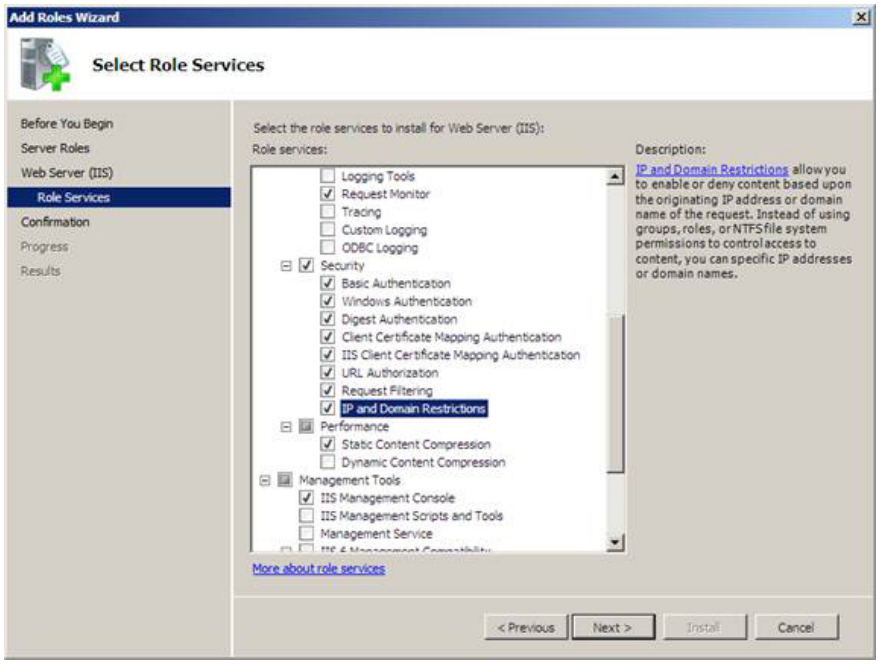


Figure 3

8. Review the information on the *Confirm Installation Selections* window and click **Install** .

9. Click **Close** on the *Installation Results* window

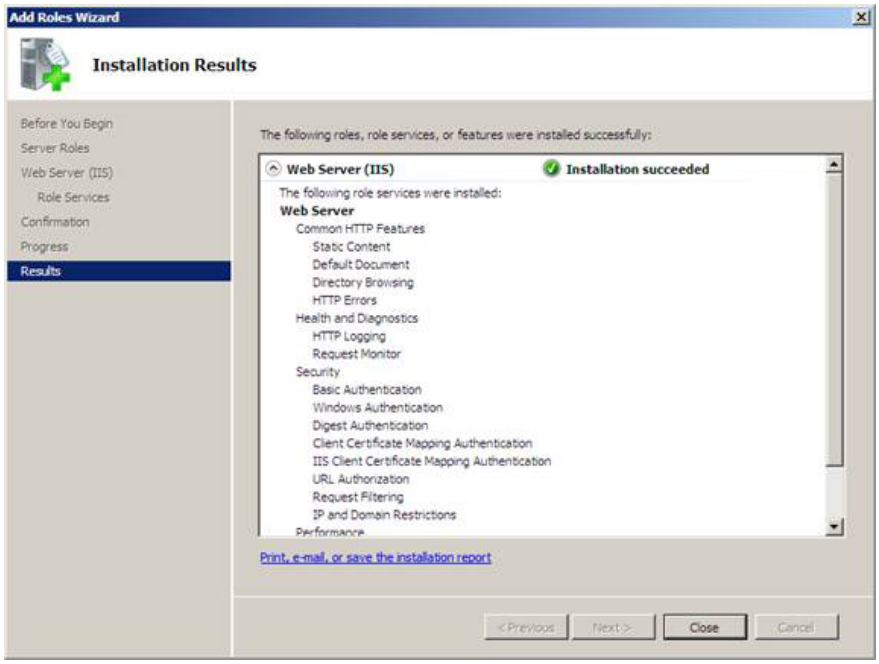


Figure 4

Request a computer certificate for VPN Server using the IIS Certificate Request Wizard

The next step is to request a computer certificate for the VPN server. The VPN server needs a computer certificate to be able to create an SSL VPN connection with the SSL VPN client. The commonly used name on the certificate must be valid for the name that the VPN client will use to connect to the SSL VPN gateway. This means that you need to create a generic DNS entry for the name on the certificate to resolve the extended IP address on the VPN server, or the IP address of the NAT device in front of the VPN server will redirect the connection to SSL. VPN server.

Follow the steps below to request and install a computer certificate on the SSL VPN server:

1. In *Server Manager* , expand the **Roles** section in the left pane, then open **Web Server (IIS)** . Click **Internet Information Services (IIS) Manager** .

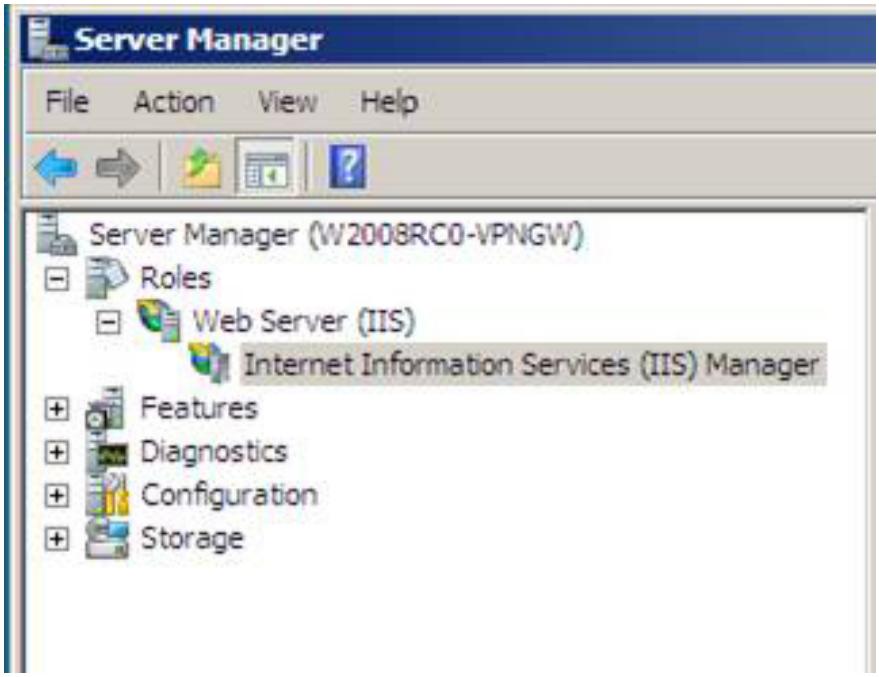


Figure 5

2. In the *Internet Information Services (IIS) Manager* console that appears in the right pane, click the name of the server. In this example, the name of the server is **W2008RC0-VPNGW** . Click the **Server Certificates** icon in the right pane of the IIS console.

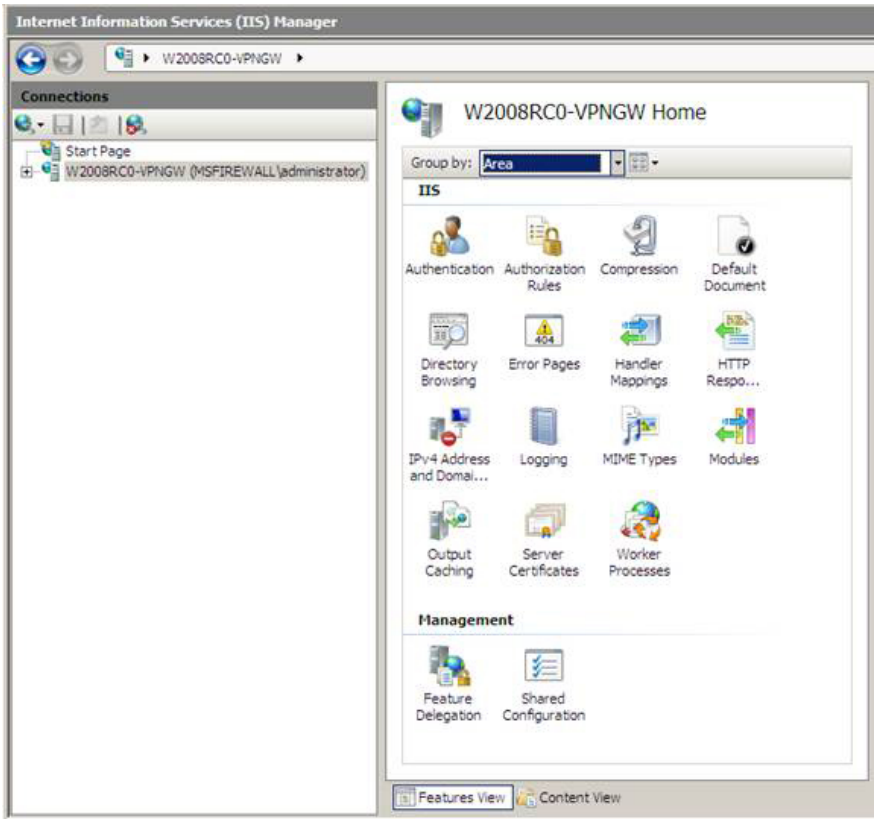


Figure 6

3. In the right pane of the console, click the **Create Domain Certificate link** .

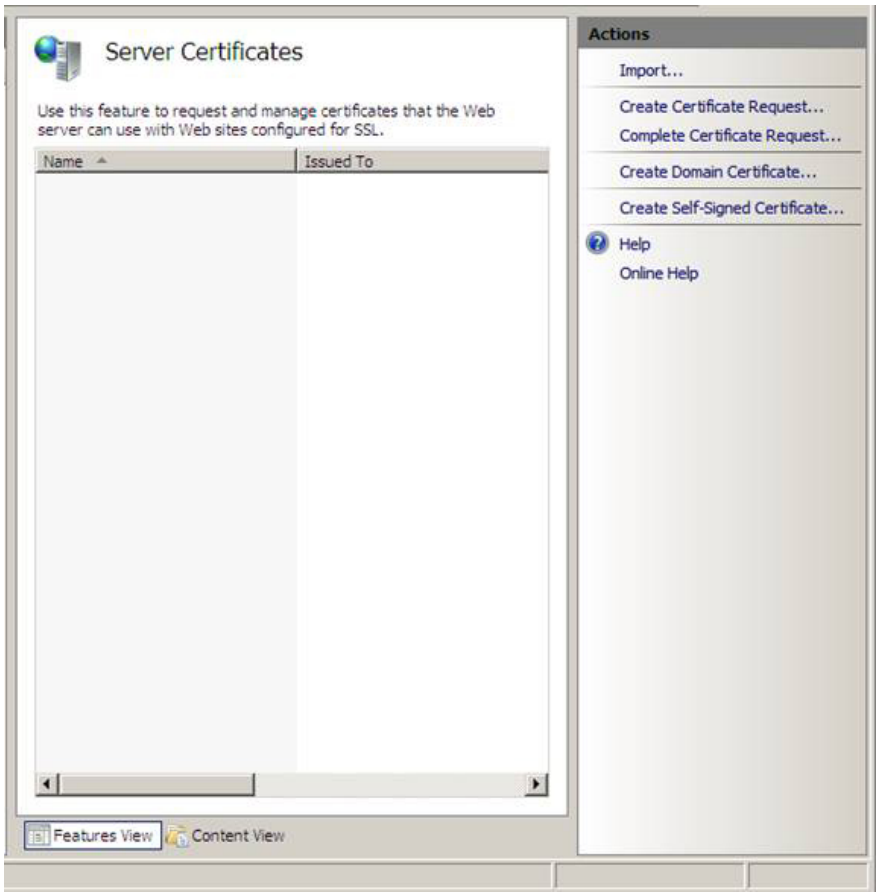


Figure 7

4. Read the information on the *Distinguished Name Properties* window. The most important item on this window is the **Common Name** . This name is the name that VPN clients will use to connect to the VPN server. You will need to have a generic DNS entry for this name so that it can deal with the VPN server's external interface or the common address of the NAT device before the VPN server. In this example, we will use the generic name **sstp.msfirewall.org** . Then, we will create HOSTS file entries on the VPN client so that it can be done with this name. Click **Next** .

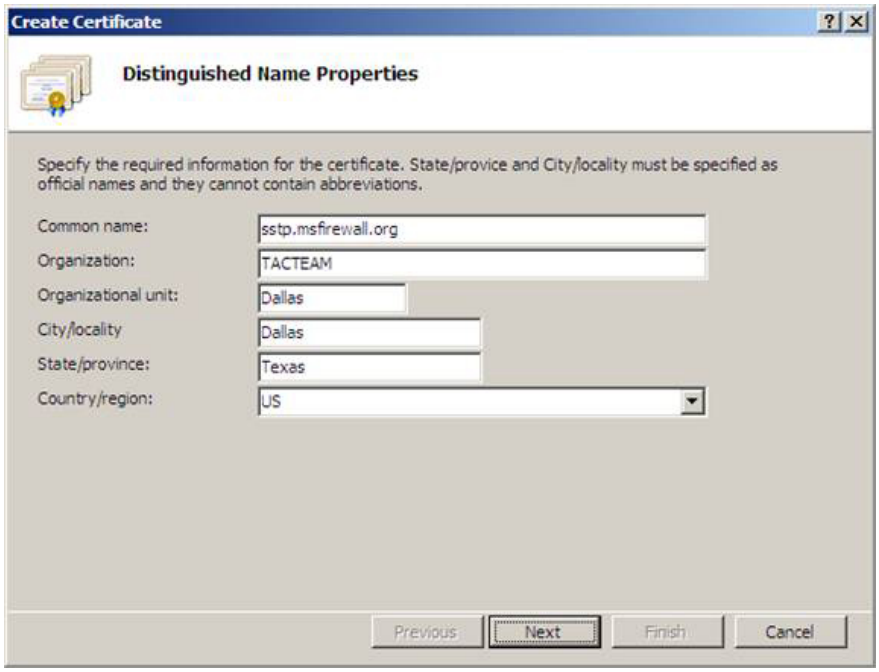


Figure 8

5. On the *Online Certification Authority* window, click the **Select** button. In the *Select Certification Authority* dialog box, click the name of Enterprise CA and then click **OK** . Enter the name of the certificate in the **Friendly name** text box. In this example we use the **SSTP Cert** name to know that it is being used for the SSTP VPN gateway.

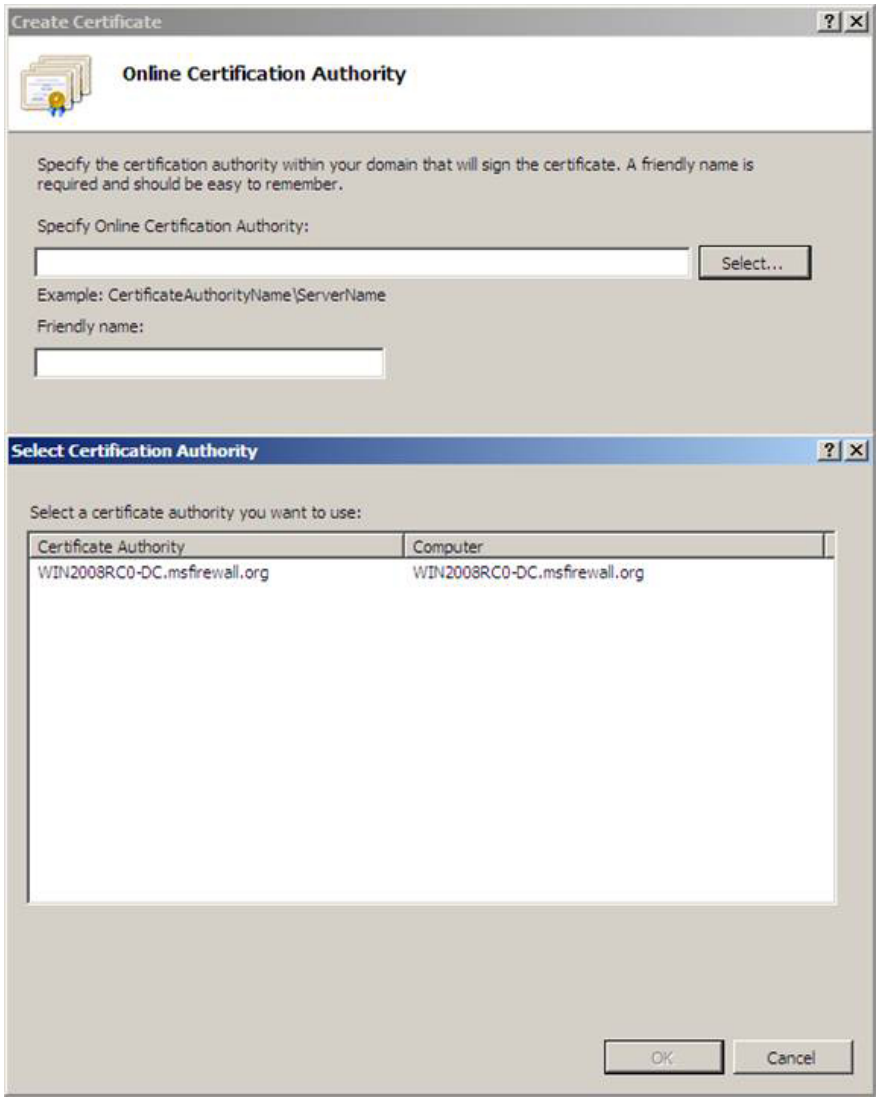


Figure 9

6. Click **Finish** on the *Online Certification Authority* window

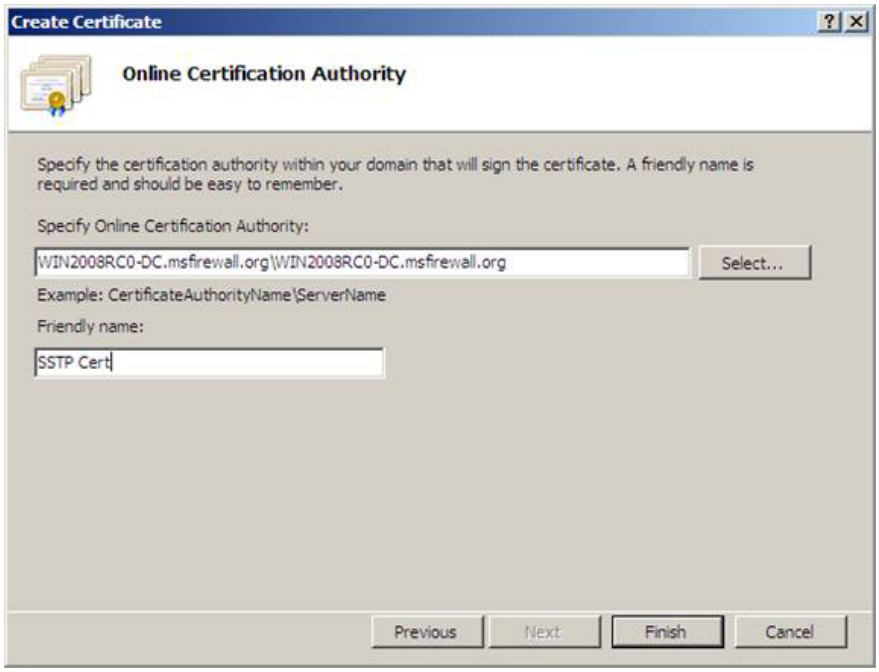


Figure 10

7. The utility will run and then no longer appear. After this point, you will see the certificate appear in the IIS console. Double-click the certificate and you can see the generic name in the **Issued** to section and we will have a private key corresponding to the certificate. Click **OK** to close the *Certificate* dialog box.

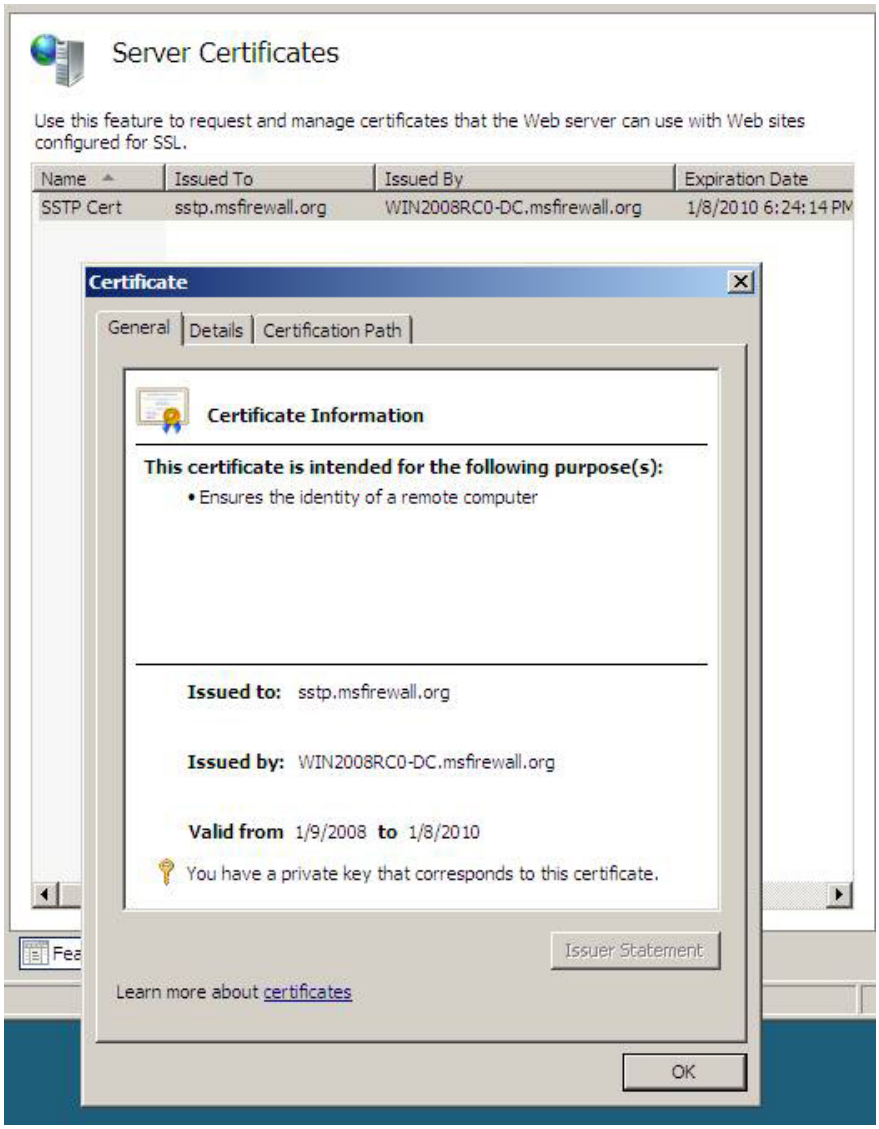


Figure 11

We now have a certificate and can install the RRAS Server Role. Note that you must install the certificate before installing the RRAS Server Role. If you do not do so, you will encounter some problems because you will have to use a fairly complicated command line routine to connect the certificate to the SSL VPN listener.

Install RRAS Server Role on VPN Server

To install the RRAS Server Role, follow the steps below:

1. In *Server Manager* , click the **Roles** button in the left part of the console

2. In the *Roles Summary* section, click the **Add Roles** link.

3. Click **Next** on the *Before You Begin* window

4. On the *Select Server Roles* window, check the **Network Policy and Access Services** check box, and then

click **Next** .

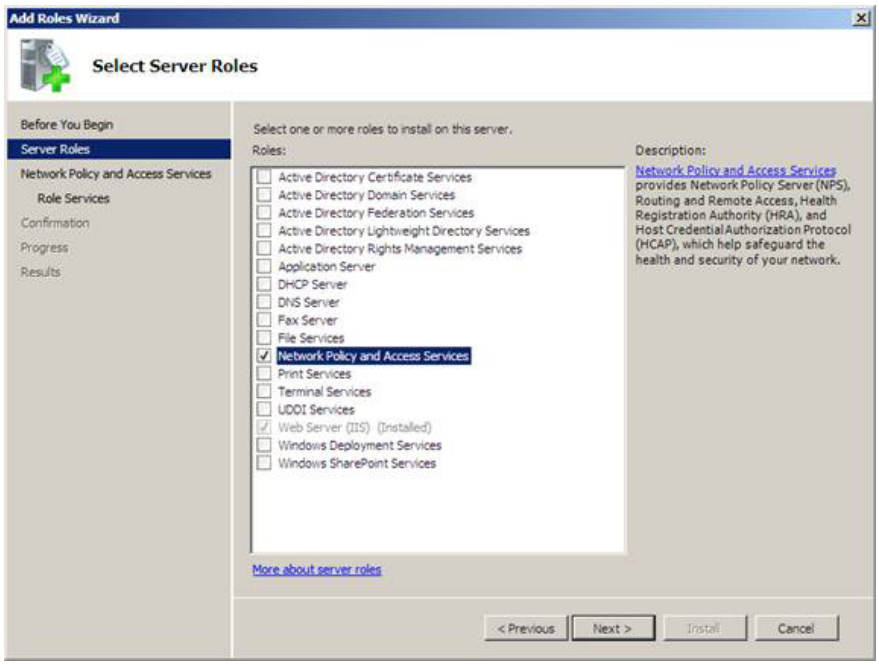


Figure 12

5. Read the information on the *Network Policy and Access Services* window. Most of this information tells us about the new Network Policy Server (the policy server is still called Internet Authentication Server [IAS] as the RADIUS server), all of which are not currently applicable to our scenario. . Click **Next** .

6. On the *Select Role Services* window, check the **Routing and Remote Access Services** check box. When checking this box, the utility will also automatically check the **Remote Access Service** and **Routing** checkboxes. Click **Next** .

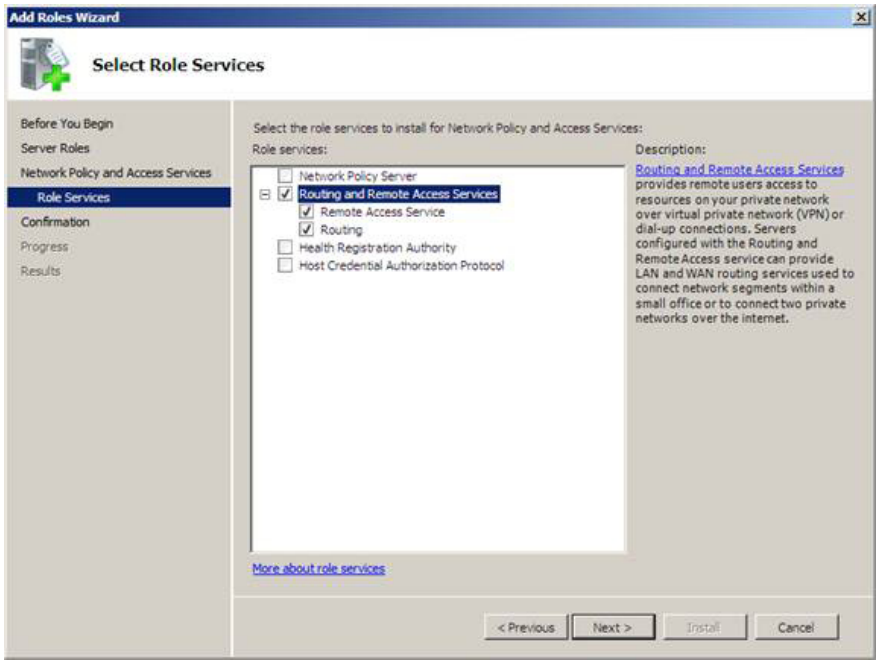


Figure 13

7. Click **Install** on the *Confirm Installation Selections* window.

8. Click **Close** on the *Installation Results* window.

Enable RRAS Server and configure it to become a NAT and VPN server

Now that the RRAS server server role is now installed, we need to enable RRAS service, the same way we did with previous versions of Windows. We need to enable VPN server features and NAT services. The need to activate the VPN server component is clear, but you may wonder why it is necessary to activate the NAT server. The reason is that external clients can increase access to the Certificate Server to be able to connect to the CRL. If the SSTP VPN client cannot download the CRL then the SSTP VPN connection will fail.

To allow access to the CRL we will configure the VPN server into a NAT server and publish the CRL using reverse NAT. In a real environment you may have a firewall (such as the ISA Firewall) located in front of the Certificate Server certificate server, so you will publish the CRL using a firewall. However, in this example the firewall used is Windows Firewall on the VPN server, so we need to configure the VPN server to be a NAT server.

Follow the steps below to enable RRAS service:

1. In *Server Manager* , open the **Roles** section in the left pane of the console. Open the **Network Policy and Access Services section** and then click the **Routing and Remote Access** button. Right-click **Routing and Remote Access** and then click **Configure and Enable Routing and Remote Access** .

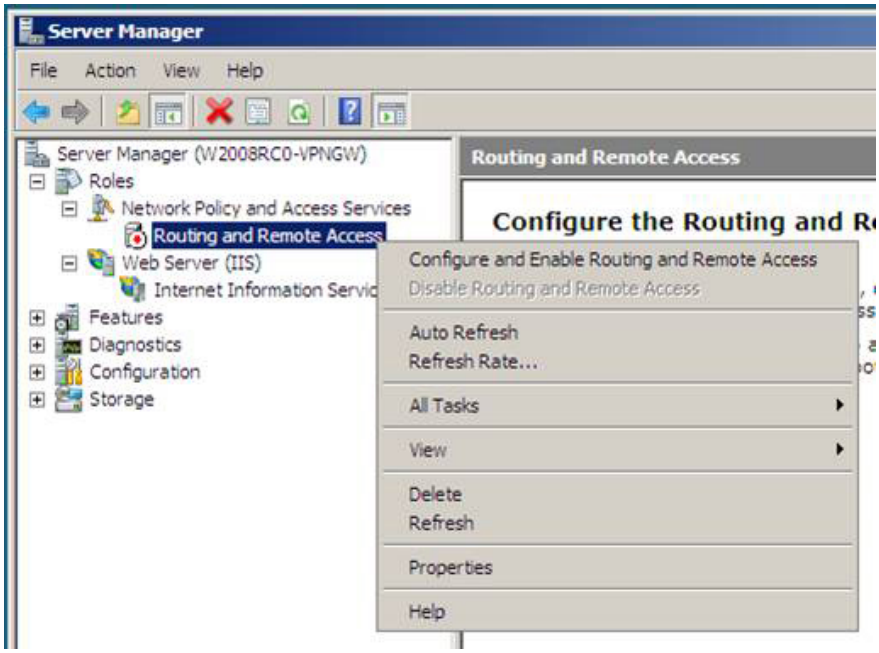


Figure 14

2. Click **Next** on the *Welcome to the Routing and Remote Access Server Setup Wizard* window

3. On the *Configuration* window, select the **Virtual private network (VPN) access and NAT option** and click **Next** .

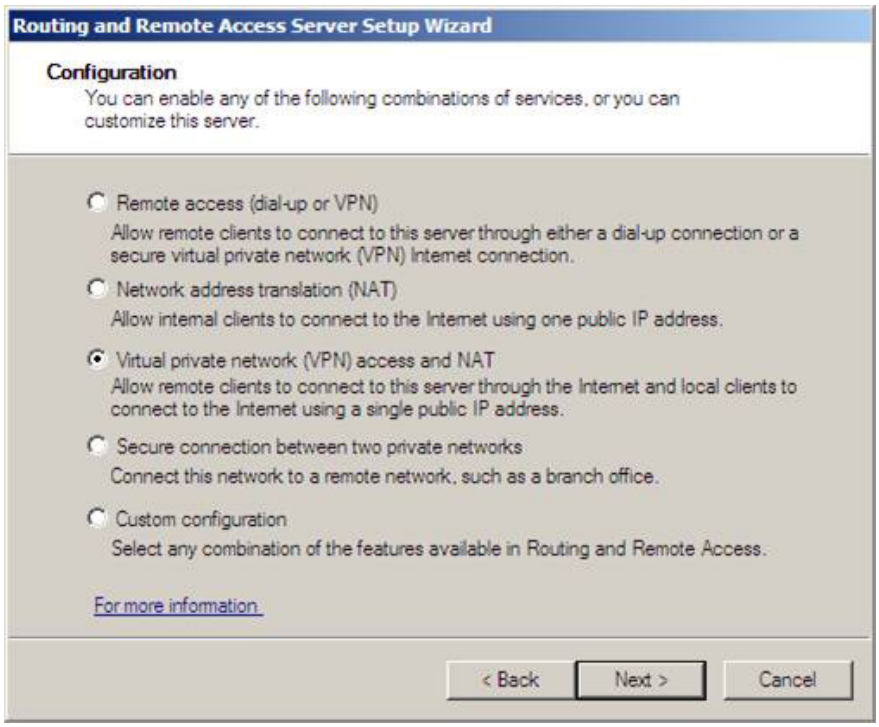


Figure 15

4. On the *VPN Connection* window, select the NIC in the Network interfaces section, which has the external interface of the VPN server. Then click **Next** .

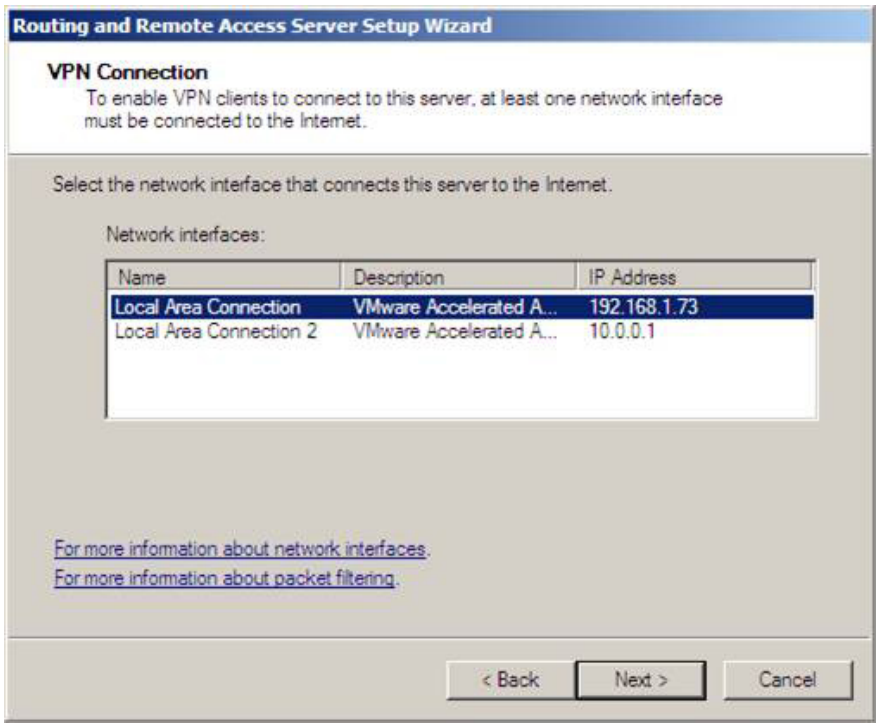


Figure 16

5. On the *IP Address Assignment* window, select the **Automatically** option. We can choose this option because we have a DHCP server installed on the domain controller behind the VPN server. If you have not set up a DHCP server, then select the **From a specified range of addresses option** and then provide a list of addresses that the VPN server can use when connecting to the network through the VPN gateway. Click **Next** .

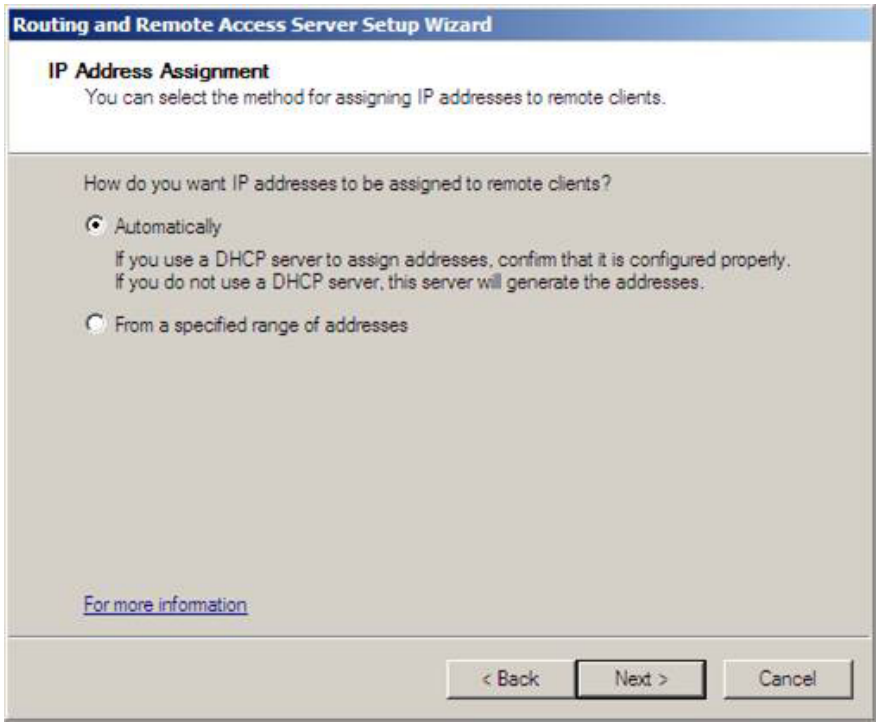


Figure 17

6. In the *Managing Multiple Remote Access Servers* window, select **No, use Routing and Remote Access to authenticate connection requests** . This is the option we use when there is no NPS or RADIUS server. Because the VPN server is a member of the domain, you can authenticate users using domain accounts. If the VPN server is not a domain member, only local accounts on the new VPN server can be used, unless you decide to use the NPS server. Click **Next** .

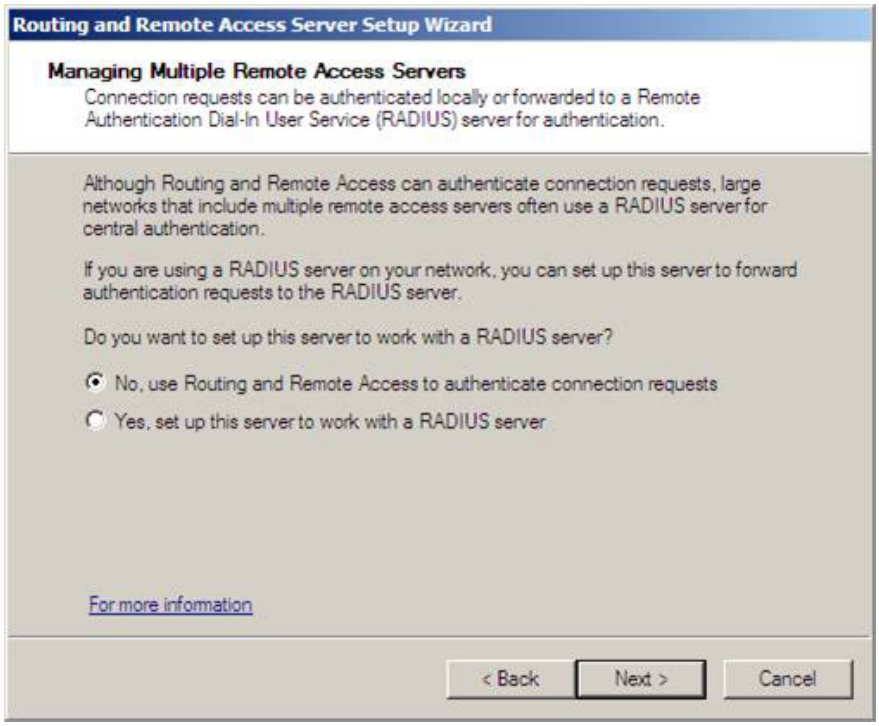


Figure 18

7. Read the summary information on the *Completing the Routing and Remote Access Server Setup Wizard* window and click **Finish** .

8. Click **OK** in the *Routing and Remote Access* dialog box, which is a dialog box informing you that forwarding DHCP messages requires a forwarding agent.

9. In the left pane of the console, open **Routing and Remote Access** , then click the **Ports** button. In the middle of the panel, you will see connections for SSTP.

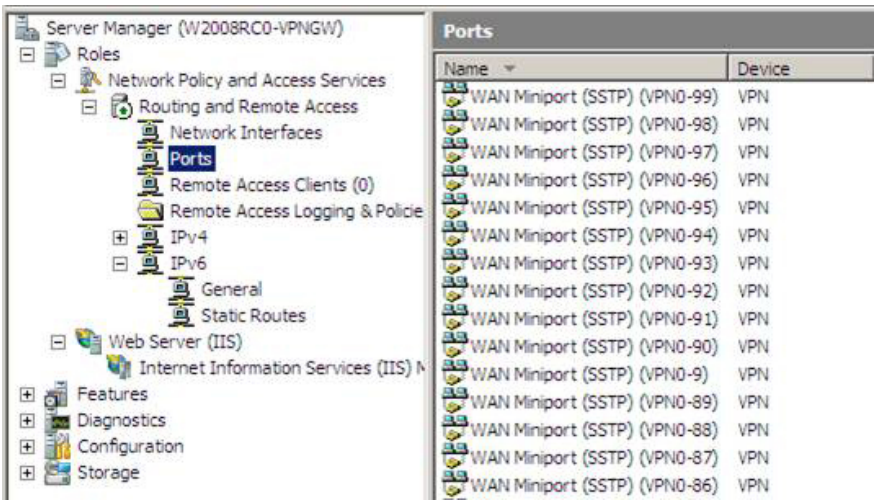


Figure 19

Configure NAT server to publish CRL

As we mentioned earlier, SSL VPN clients need to be able to download the CRL to confirm that the server certificate on the VPN server has not been canceled. To do this, you need to configure a certificate server device to forward HTTP requests to the CRL location to the certificate server.

So, do you know what URL the SSL VPN client needs to connect to to download the CRL? This information is introduced right inside each certificate itself. If you go to the VPN server again and double-click the certificate on the IIS console (this is because you did it first), you will be able to find this information. Click the Details tab of the certificate and scroll down to the CRL Distribution Points section, then click on that item. In the lower panel, you can see different distribution points based on the protocol used to access these points. In the certificate screen in the figure below, you can see that we need to allow SSL VPN client access to the CRL via the URL:

http://win2008rc0-dc.msfirewall.org/CertEnroll/WIN2008RC0-DC.msfirewall.org.crl

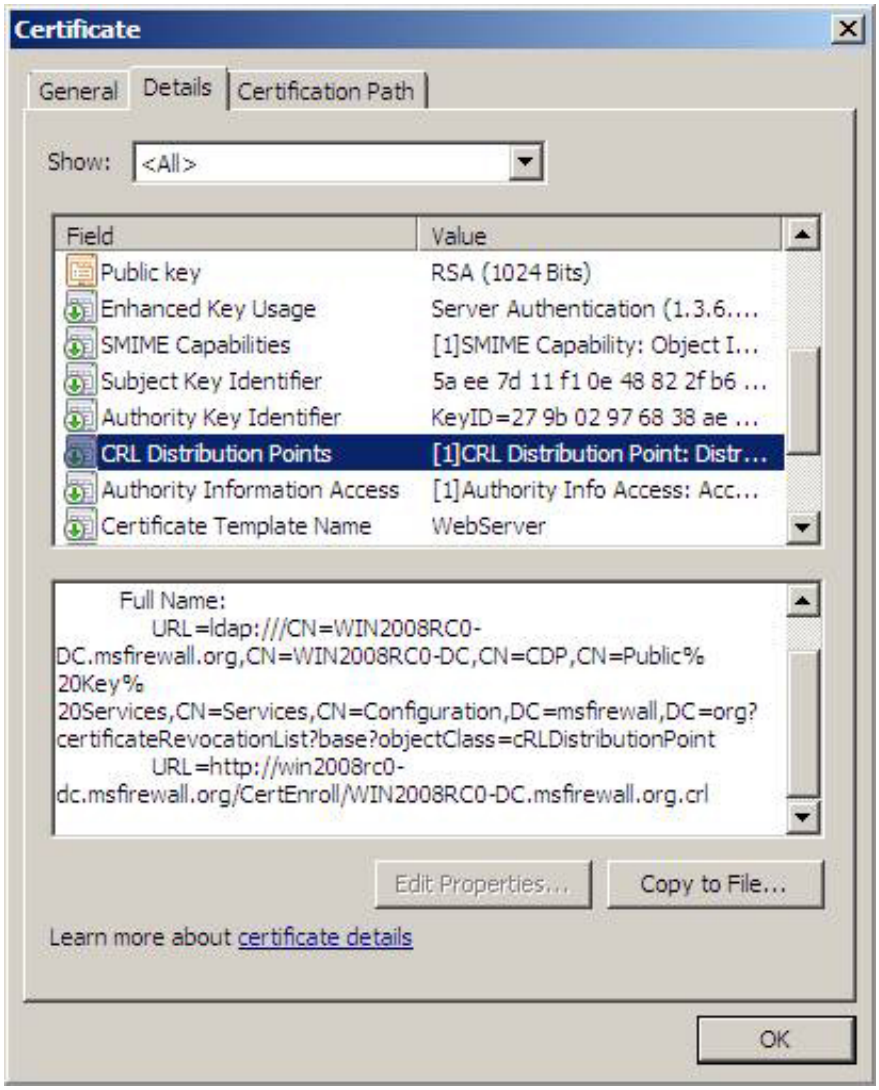


Figure 20

For this reason, you need to create them a DNS entry for this name so that external VPN clients can execute that name with the IP address on the device, the device here will perform reverse NAT or reverse proxy to allow access to the Certificate Server website. In this example, we need to have win2008rc0-dc.msfirewall.org to resolve the IP address on the external interface of the VPN server, the host will reverse the NAT connection with the Certificate Server.

If you are using a 'new' firewall (such as the ISA Firewall), it is possible to publish a more secure CRL site by allowing only access to the CRL without going to the entire site. However, in this article we will limit the ability of a simple NAT device like what RRAS NAT provides. You should note here that using the default CRL site name may not be a safe way because it reveals the name of the computer on the Internet. You can create a CDP (CRL Distribution Point) to avoid this if it is important to expose the private name of the CA in the public DNS.

Following these steps to configure RRAS NAT can forward HTTP requests to the Certificate Server:

1. In the left pane of *Server Manager* , open the **Routing and Remote Access section** , then open the **IPv4** section. Click the **NAT** button.

2. In the *NAT* button, right-click the external interface, in the middle of the console. In this example, the name of the external interface is **Local Area Connection** , then click **Properties** .

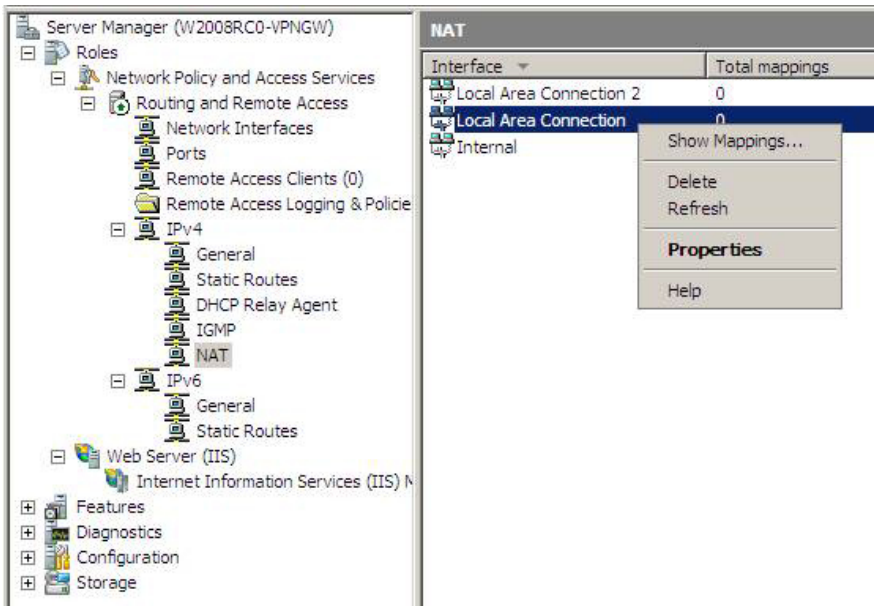


Figure 21

3. In the *Local Area Connection Properties* dialog box, check the **Web Server (HTTP)** checkbox. When doing so, the **Edit Service** dialog **box** will appear. In the **Private Address** text box, enter the certificate server's IP address on the internal network. Click **OK** .

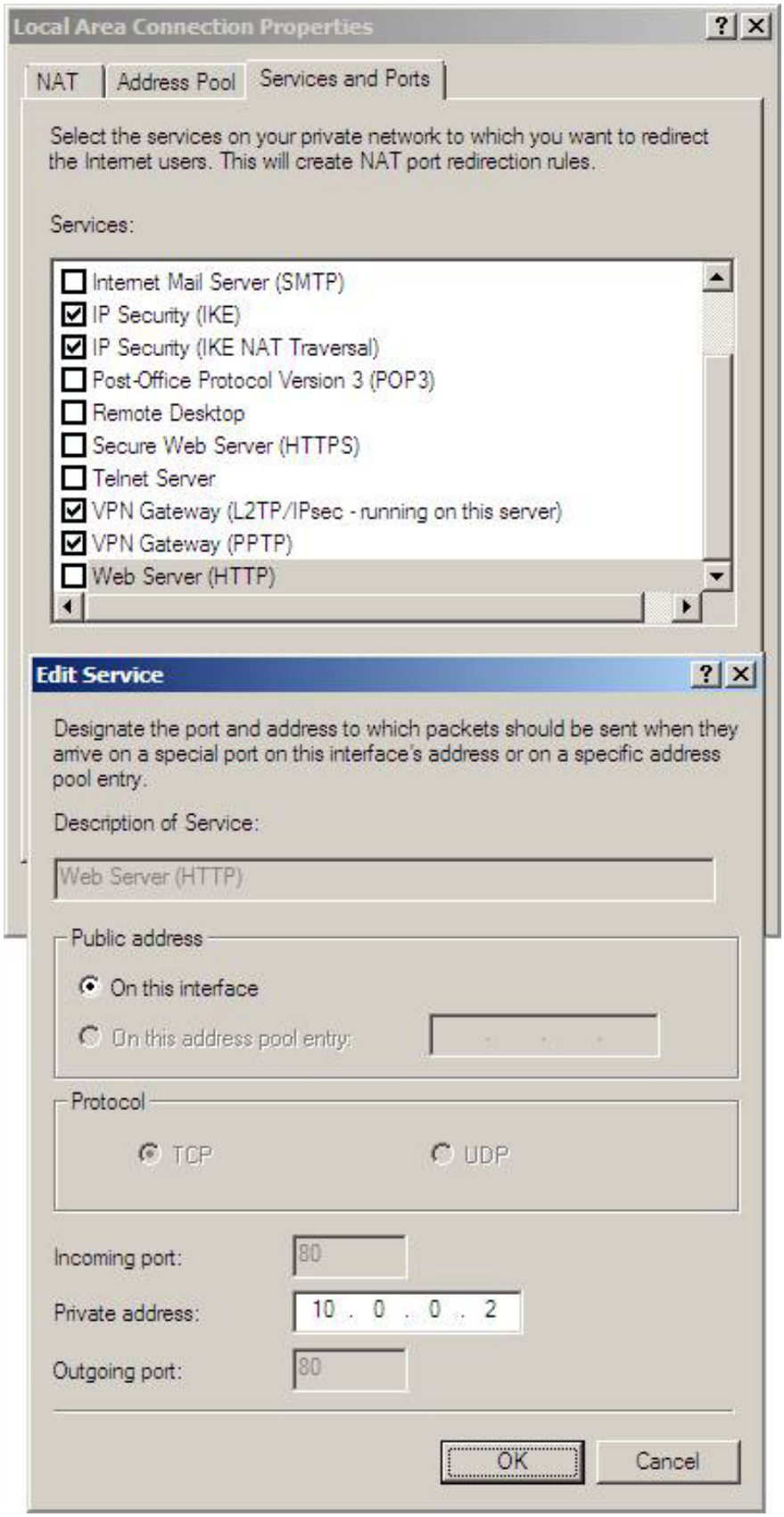

Local Area Connection Properties
NAT
Address Pool
Services and Ports
Select the services on your private network to which you want to redirect the Internet users. This will create NAT port redirection rules.
Services:
Internet Mail Server (SMTP)
IP Security (IKE)
IP Security (IKE NAT Traversal)
Post-Office Protocol Version 3 (POP3)
Remote Desktop
Secure Web Server (HTTPS)
Telnet Server
VPN Gateway (L2TP/IPsec - running on this server)
VPN Gateway (PPTP)
Web Server (HTTP)
Edit Service
Designate the port and address to which packets should be sent when they arrive on a special port on this interface's address or on a specific address pool entry.
Description of Service:
Web Server (HTTP)
Public address
On this interface
On this address pool entry:
Protocol
TCP
UDP
Incoming port:
80
Private address:
10 . 0 . 0 . 2
Outgoing port:
80
OK
Cancel

Figure 22

4. Click **OK** in the *Local Area Connection Properties* dialog box.

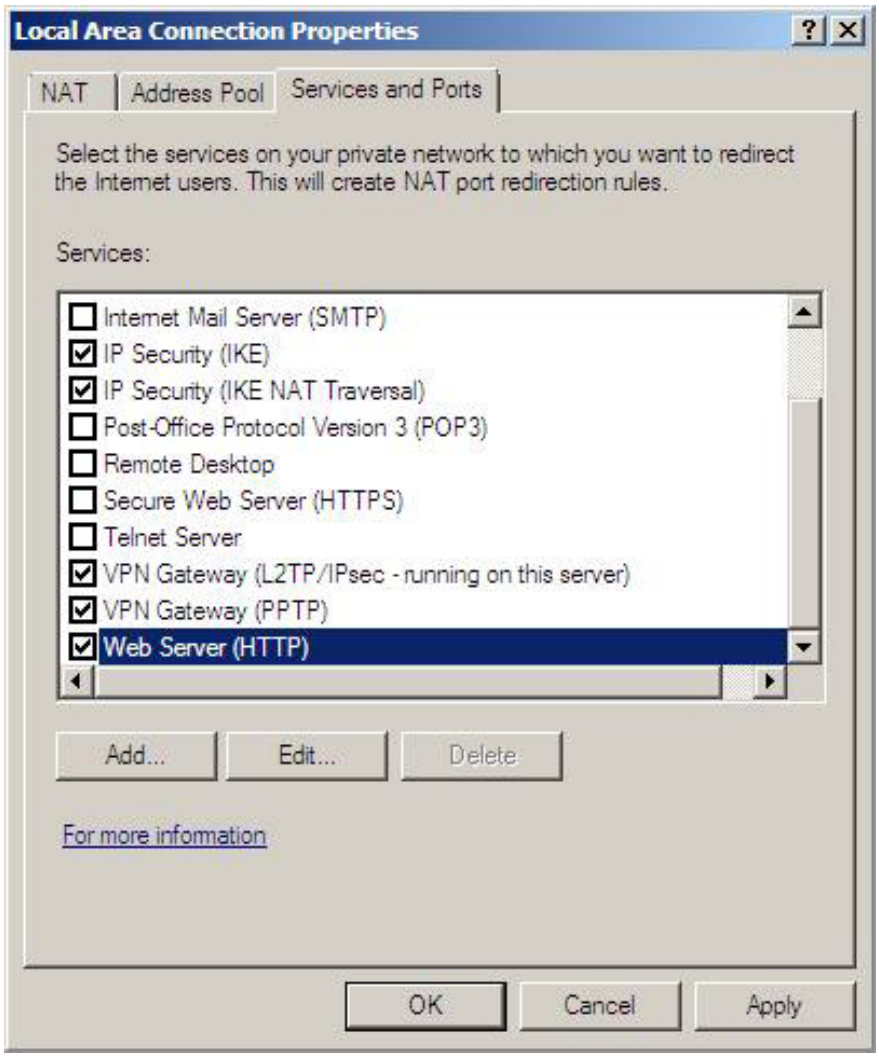
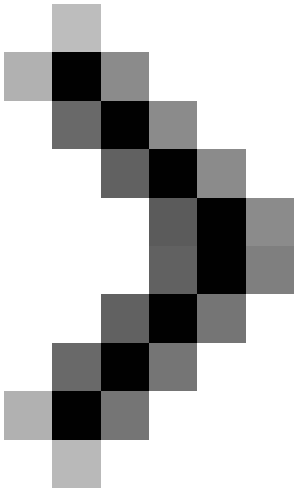


Figure 23

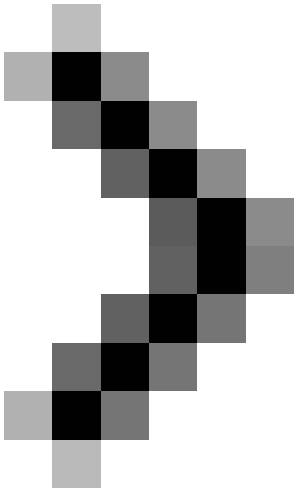
Now that the NAT server is installed and configured, we can turn our attention to configuring the CA server and the SSTP VPN client.

Conclude

In this article, I have discussed how to configure SSL VPN server using Windows Server 2008. We went into the issues of installing IIS on the VPN server, asking and install server certificate, install and configure RRAS and NAT services. In the next part of this series, we'll conclude by showing you how to configure the CA server and the SSTP VPN client.



Configure Windows Server 2008 to remotely access SSL VPN Server (Part 3)



Configure Windows Server 2008 to remotely access SSL VPN Server (Part 4)

You finished reading the article "**Configure Windows Server 2008 to remotely access SSL VPN Server (Part 2)**" 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.
