Creating SSL Server 2008 Server with ISA 2006 Firewalls (Part 1)

In this article we will configure the SSTP VPN server and configure the ISA Firewall to allow the SSTP VPN client to connect back to the SSTP VPN server.

Network Administration **- A problem with firewalls or routers at public Internet access points is that they always want to simplify things. They will not block VPN connections because they do not want to destroy your session.**

In terms of security and administration, it is easy to use only two HTTP and HTTPS protocols that are being used by most users. This makes network troubleshooting much easier for network service providers that support Internet access at these access points.

Of course, if we need to use a VPN connection and are making connections at these access points, it will be difficult when the network in use needs to be supported and the only way to provide that service is a network level VPN connection.

Windows Server 2008 integrates the SSTP VPN protocol. Basically, SSTP, Secure Socket Tunnel Protocol, is PPP (Point-To-Point Protocol) on SSL (Secure Sockets Layer). SSTP allows users to connect to the VPN server via port 443 of TCP, just like other SSL connections, and it works with Web Proxy that has not been authenticated, so even if the access point uses a system ISA firewall for external access, SSTP connections will still work normally.

In this article we will configure the SSTP VPN server and configure the ISA Firewall to allow the SSTP VPN client to connect back to the SSTP VPN server. The ISA Firewall will be configured with two Publishing Rules, including a Server Publishing Rule that allows connection back to the SSTP server and a Web Publishing Rule that allows connection back to the CRL distribution point (CDP).

First we will examine the sample network system for this configuration:

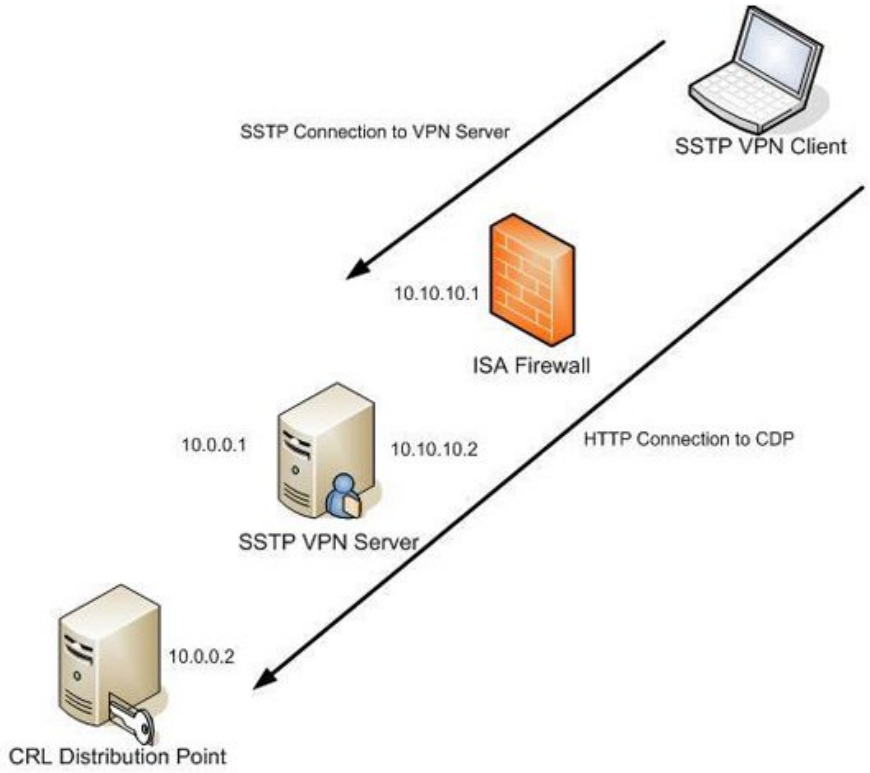

Figure 1: Network model.

We need to pay attention to two data connections. First, an SSTP connection needs to be made through the ISA Firewall to end at the SSTP SSL VPN server. The second connection needs to take two steps through the network (the first step is an HTTP connection made through the ISA Firewall, and the second step is done through the SSL VPN gateway to CDP). To support this process we need to configure the SSL VPN gateway to become a NAT server that performs reverse NAT to allow access to CDP behind the VPN server.

Note, the SSTP VPN client must use the Windows Vista SP1 version. Vista RTM version does not support SSTP.

In this example, the ISA Firewall is not a member of the domain because the domain member is not needed in this case. If you want to enroll the ISA Firewall as a domain member, you will have to configure the ISA Firewall to use a router behind the internal interface of the ISA Frirewall because the internal domain communication does not work with NAT devices in this connection. This router will be placed together with the VPN server, so external communication and internal communication will appear on network IDs that reflect these communications on the SSTP VPN gateway system.

SSTP VPN gateway is a domain member so we can take advantage of Windows authentication process. If we don't want the SSTP VPN gateway to be a domain member, we can install a Network Policy Server on the corporate network and configure the VPN server to use it for authentication and computation (the Network Policy Server server in Windows Server 2008 replaces ISA server in Windows Server 2003).

The CDP computer on the local network is a Domain Controller for the msfirewall.org domain. Functional servers installed on this computer include Active Directory Certificate Services, DHCP Server, DNS Server, Active Directory Domain Services, and WINS Server features.

We need to take the following steps:

1. Install IIS on the VPN server.
2. Request a system certificate for the VPN server using the IIS Certificate Request Wizard.
3. Install RRAS function server on VPN server.
4. Activate RRAS server and then configure it to become a NAT server and VPN.
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 the ISA Firewall with a PPTP VPN server, SSL VPN server and CDP's Web Publishing Rule.
9. Configure HOSTS file on VPN client.
10. Use PPTP to connect to the VPN server.
11. Create a CA Certificate from the Enterprise CA.
12. Configure the ISA Firewall with an SSL VPN Server Publishing Rule and CDP.
13. Configure the client to use SSTP and connect to the VPN server using SSTP.

Install IIS on the VPN server

Normally we don't put a Web Server on a network security device, but if we do so we won't need to keep the Web Server on the VPN server because we only use it for a short time. This is because the Web Enrollment Site integrated in Windows Server 2008 Certificate Server is no longer useful in requesting computer licenses, at least no longer available on Windows Server 2008 and Windows Vista environments. However, we can still use the Web Enrollment Site to create a Computer Certificate as if it was installed, but in fact Computer Certificate is not installed.

To solve this problem we can use Enterprise CA. With the Enterprise CA we can send a request to the online Certificate Server. The online request for a Computer Certificate is allowed when the IIS Certificate Request Wizard is used and requests a Domain Certificate. This request can only be performed when the system (sending a Domain Certificate request) belongs to the same domain as the Enterprise CA.

To install the IIS Web Server we need to do the following:

1. Open **Windows Management Console** .

2. In the left pane of this Console, click on the **Roles** node.

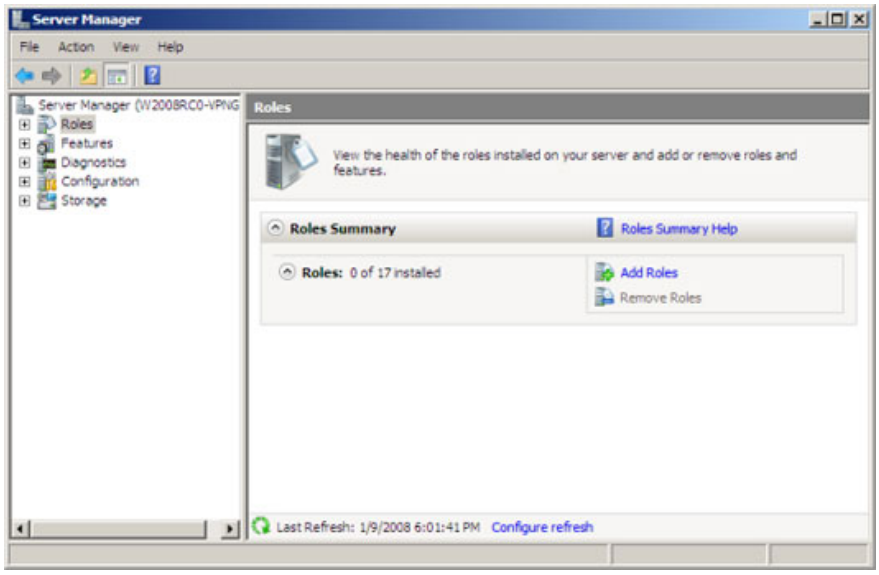

Figure 2: Server Manager window.

3. Click the **Add Roles** link on the right panel.

4. On the **Before You Begin** page, click **Next** .

5. Select the **Web Server (IIS) check box** on the **Select Server Roles** page. Click **Next** .

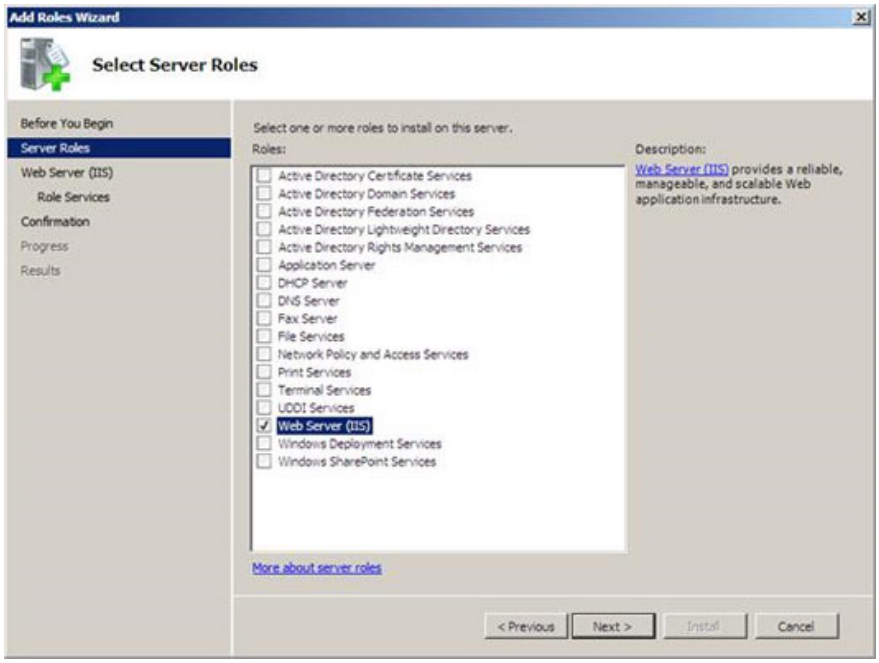

Figure 3: Select Server Roles page.

6. Check the information on the **Web Server (IIS) page** if you want. These are general information about using IIS 7 as a Web Server, but since we do not use the IIS Web Server on the VPN server, we will ignore this information. Click **Next** .

7. On the **Select Role Services** page, select a number of options. However, if you use these options, you will not be able to use the **Certificate Request Wizard** because there is no **Role Service** for the **Certificate Request Wizard** , so we will select all the options in **Security** . Then click **Next** .

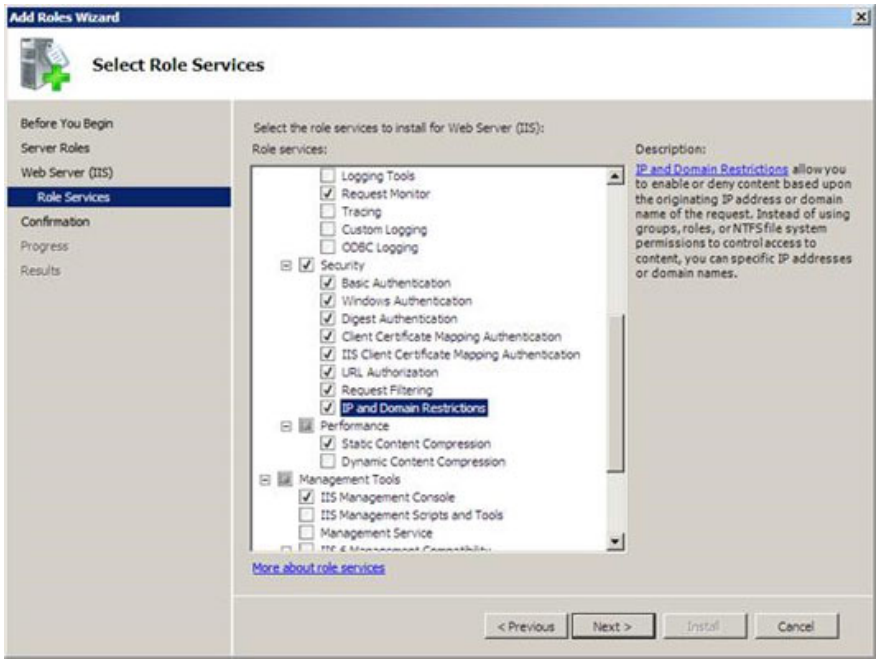

Figure 4: Select the checkboxes in Security on the Select Server Roles page.

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

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

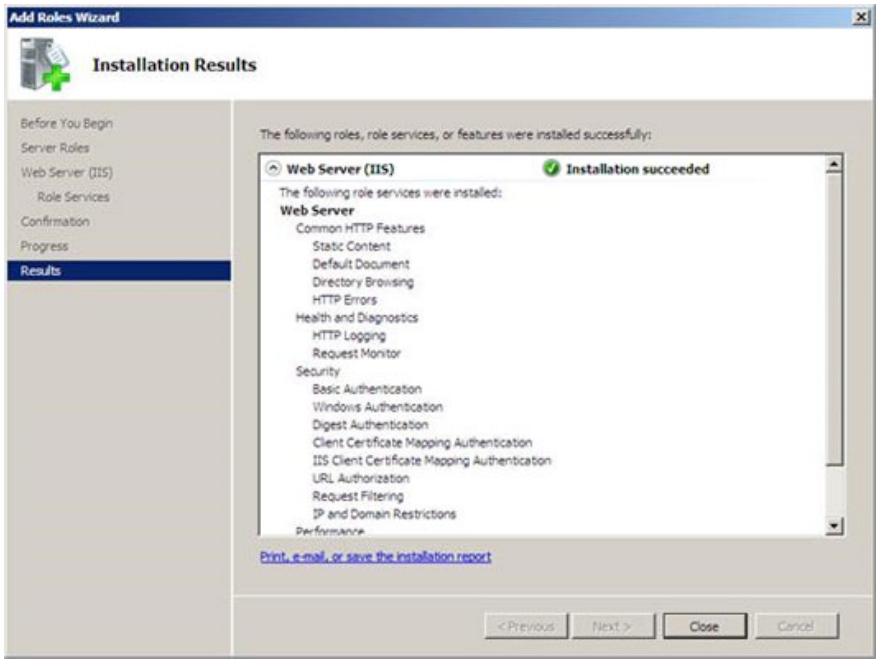

Figure 5: Complete installation of IIS Web Server.

Create a Machine Certificate for the VPN server using the IIS Certificate Request Wizard

In the next step we will request a Machine Certificate for the VPN server. The VPN server needs a Machine Certificate to create an SSL VPN connection with the SSL VPN client. Usually the name on the Certificate must match the name that the VPN client uses to connect to the SSL VPN Gateway. That means we will have to create a public DNS entry for this Certificate's name to handle the external IP address on the VPN server, or the IP address of a NAT device in front of the VPN server will forward the connection. Connect this to SSL VPN server.

Perform the following steps to request and install Computer Certificate on SSL VPN server:

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

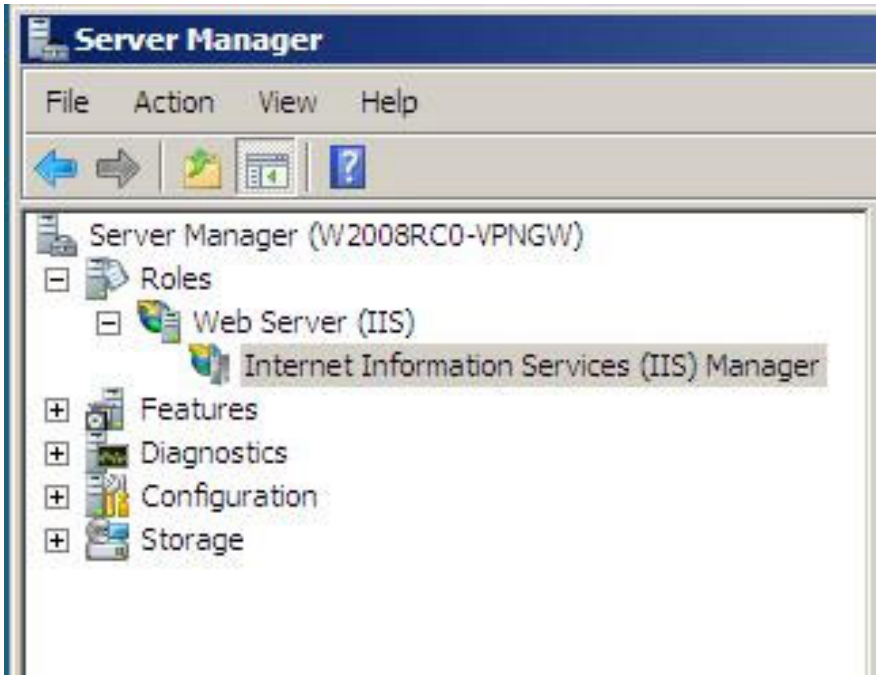

Figure 6: Access to IIS Manager.

2. In **IIS Manager Console** appears in the right pane, click on the name of this server. In this example, the name of the server is *W2008RC0-VPNGW* . Next click on the Server Certificate icon in the right pane of the IIS Manager Console.

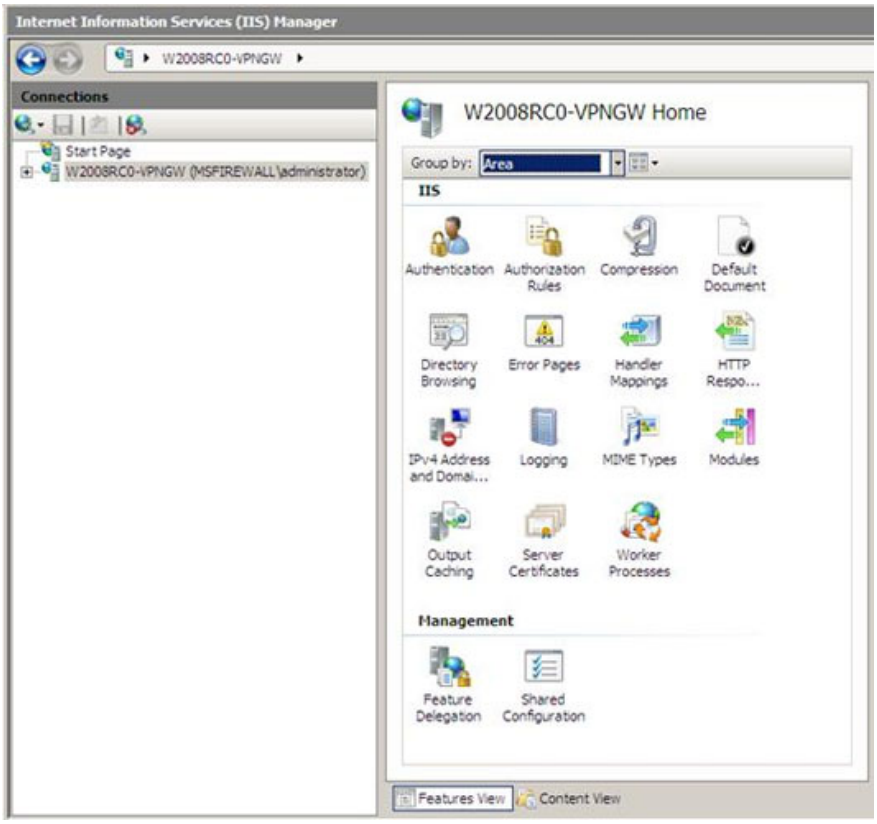

Figure 7: Access to the sample server W2008RC0-VPNGW.

3. In **Action,** click on the **Create Domain Certificate link** .

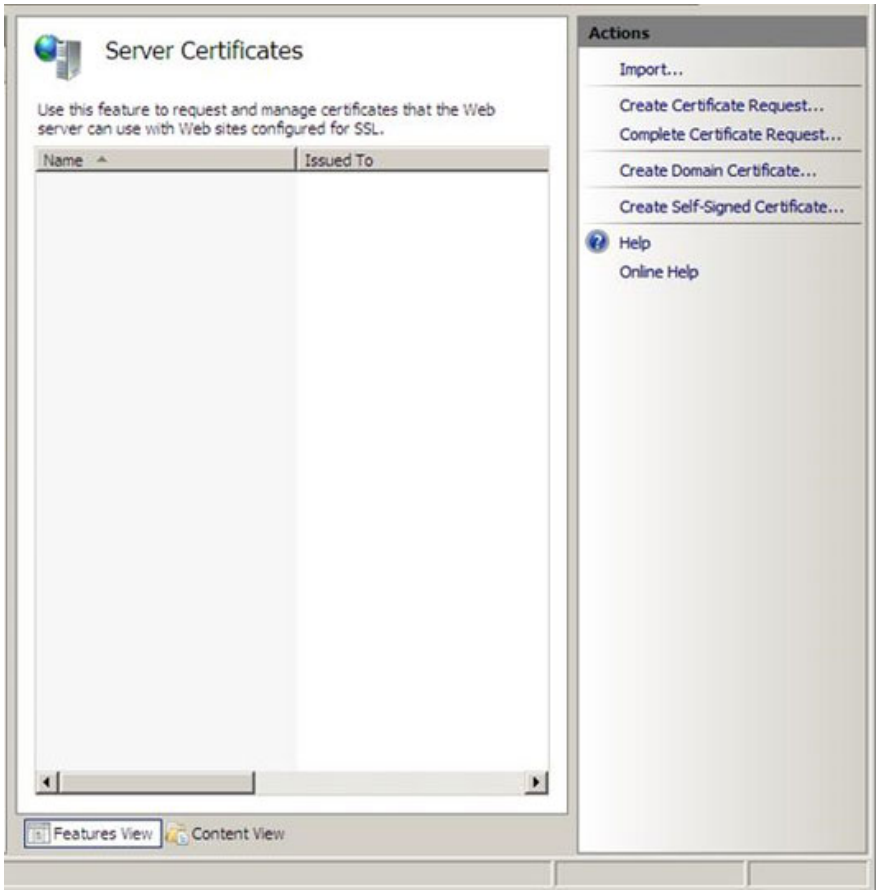

Figure 8: Server Certificates page.

4. Enter the information on the **Distinguished Name Properties** page. Note the **Common Name** section, here enter the name that the VPN client uses to connect to the VPN server. We will need a public DNS entry for this name to be processed for the external communication of the VPN server or the public address of the NAT device in front of the VPN server. In this example we will enter *sstp.msfirewall.org* into the **Common Name** . Then we will create *HOSTS* file entries on the VPN client so that it can handle this name. Now click **Next** .

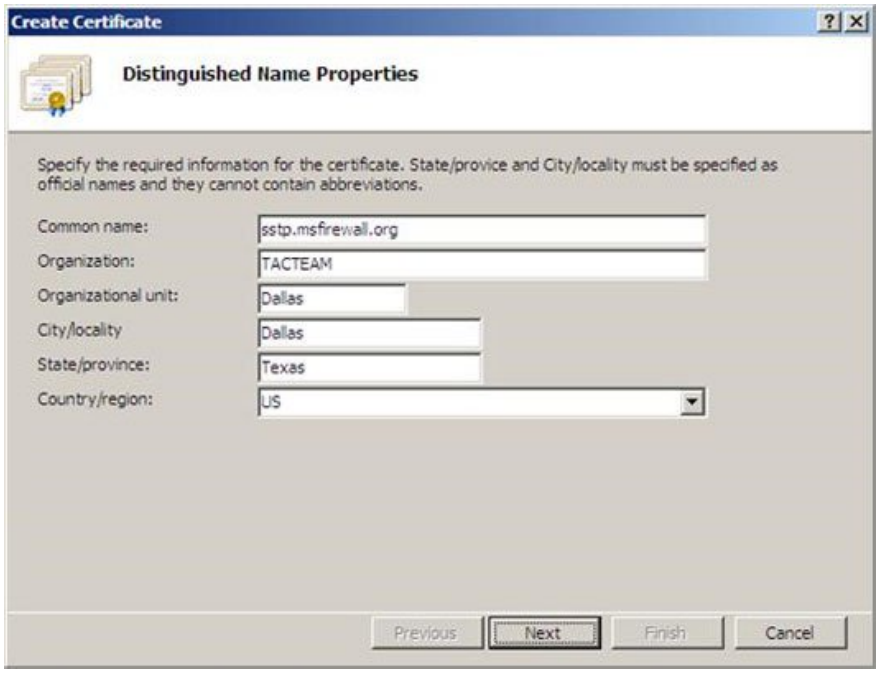

Figure 9: Distinguished Name Properites page.

5. On the **Online Certification Authority** page, click the **Select** button. In the **Select Certification Authority** dialog box, click the name of the **Enterprise CA** and then click **OK** . Enter a name for the Certificate in the **Friendly name** box. In this example, we'll enter the name for this certificate, **SSTP Cert** .

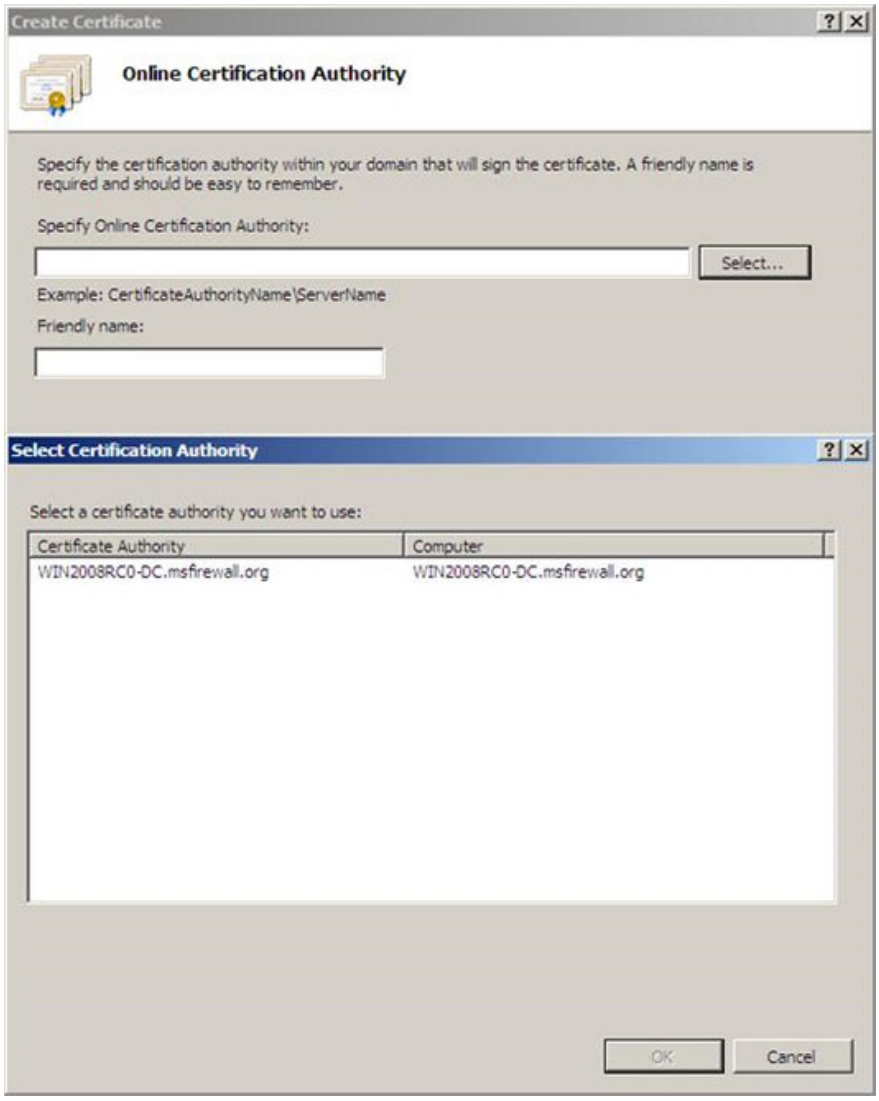

Figure 10: Select the Certificate Authority.

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

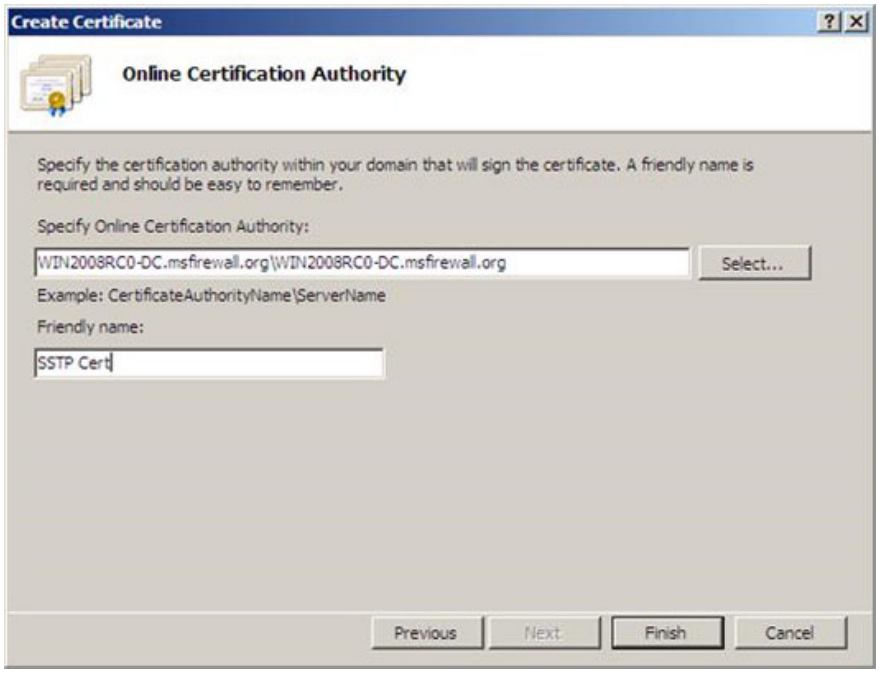

Figure 11: Online Certification Authority page.

7. Next the wizard will run and close itself. We will see this Certificate appear in the **IIS Manager Console** . Double clicking on this Certificate will see the **Common name** in the **Issued to** area, and we will have a **Private Key that** matches this Certificate. Click **OK** to close the Certificate dialog box.

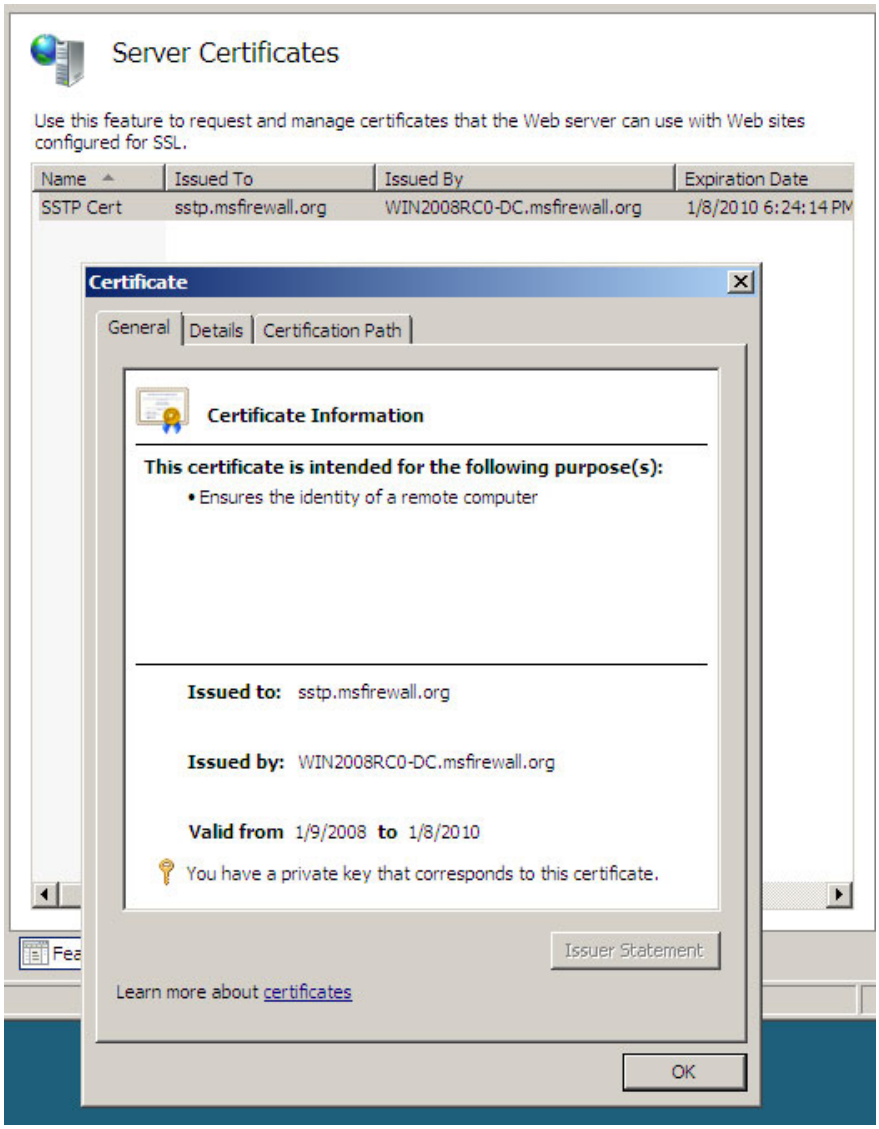

Figure 12: Certificate property page.

Once you have a Certificate, you can install the RRAS Server Role. Note that before installing the RRAS Server Role, we will have to install the Certificate. If you do not do so, after installing, you will have to use a very complicated command to connect this Certificate to the SSL VPN Listener.

Install RRAS Server Role on VPN server

To install the RRAS Server Role, follow these steps:

1. In **Server Manager** , click the **Role** node in the left pane.

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

3. On the **Before You Begin** page, click **Next** .

4. On the **Select Server Roles** page, select the **Network Policy and Access Services check box** and click **Next** .

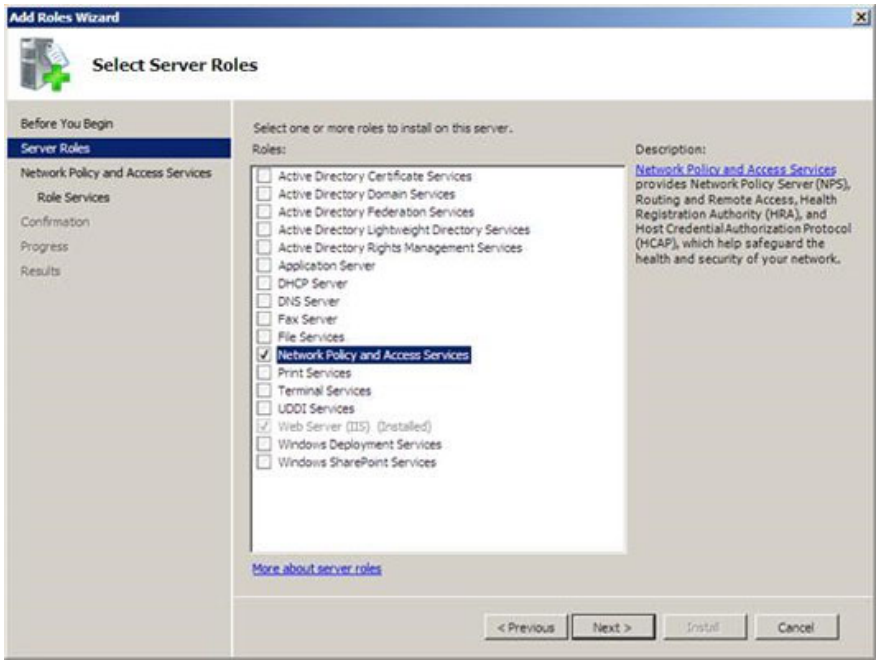

Figure 13: Select the Network Policy an Access Services check box on the Select Server Roles page.

5. Check the information on the **Network Policy and Access Services page** . Most of this information is about the new **Network Policy Server** (commonly known as **Internet Authentication Server** , a RADIUS server) and NAP is not used in our case, and then click **Next** .

6. On the **Select Role Services** page, select the **Routing and Remote Access Services check** box, then the **Remote Access Service** and **Routing** dialog boxes will be selected. Next click **Next** .

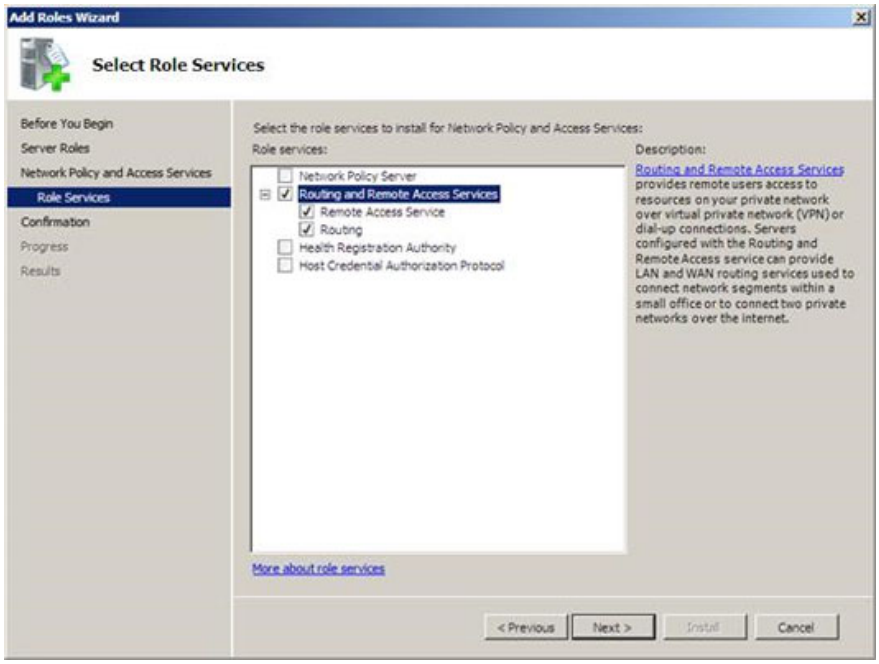

Figure 14: Select the Routing and Remote Access Services check box on the page Select Role Services.

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

8. On the **Installation** page, click **Close** .

Activation and configuration of RRAS Server becomes NAT and VPN servers

Now that the RRAS function server is installed, we need to enable RRAS service and enable the VPN server feature. Perhaps you are asking why the NAT server must be activated? We need to enable the NAT server so that external clients can access the Certificate Server to connect to the CRL. If the SSL VPN client cannot download the CRL, then the SSTP VPN connection will fail.

To allow the workstation to access the CRL we will have to configure the VPN server as a NAT server and then publish the CRL using this NAT switch server. The SSL VPN client will first connect to the ISA Firewall (configured with a Web Publishing Rule that allows you to make the necessary URL connection to access the CRL). This Web Publishing Rule is also configured to forward the request to the external interface of the NAT server. The NAT server on the VPN server will be configured to forward the HTTP request to the Certificate Server containing this CRL.

To enable RRAS service, we need to do the following:

1. In **Server Manager** , expand the **Role** node in the left pane. Then expand the **Network Policy and Access Services** node **and** then click the **Routing and Remote Access** node. Next right-click on the **Routing and Remote Access** node **and** select **Configure and Enable Routing and Remote Access** .

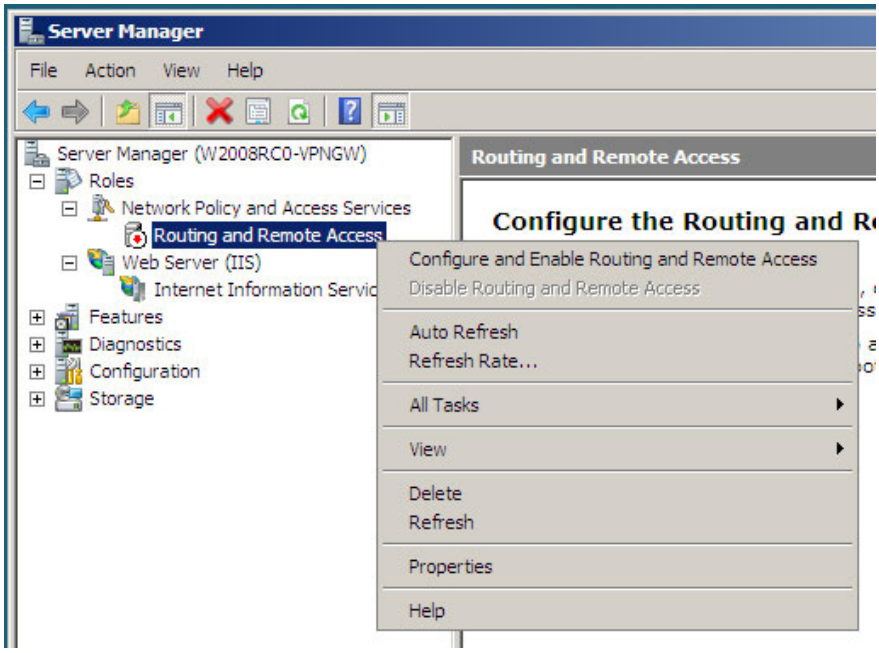

Figure 15: Configuring and enabling Routing and Remote Access.

2. On the **Welcome** page of the **Routing and Remote Access Server Setup Wizard** , click **Next** .

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

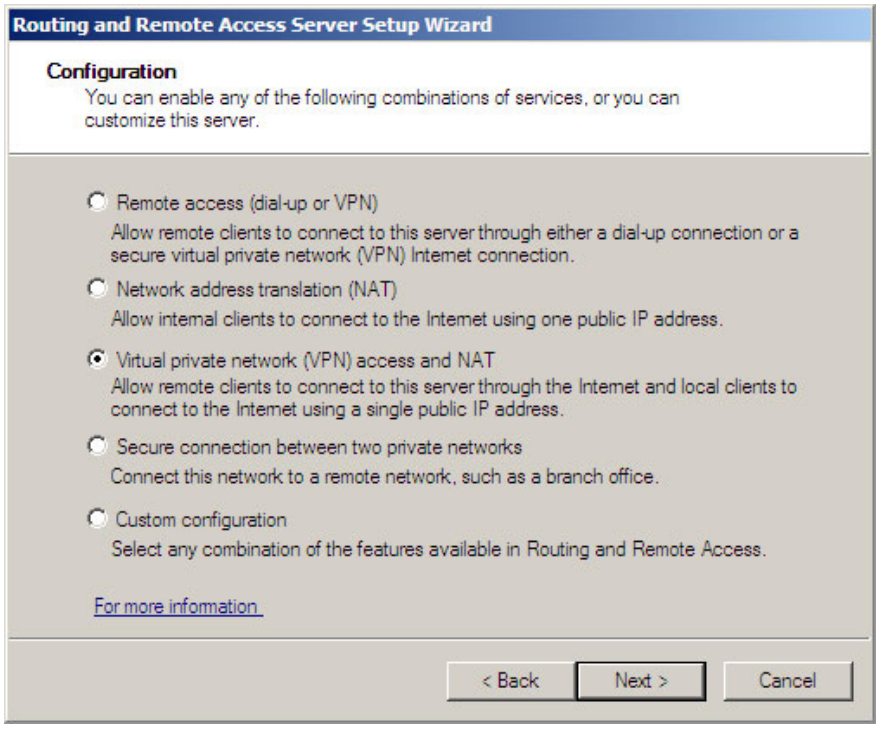

Figure 16: Select the option Virtual private network (VPN) access and NAT on the Configuration page

4. On the **VPN Connection** page, select the **NIC** in the **Network interfaces** area that displays the external interface of the VPN server. Click **Next** .

5. On the **IP Address Assignment** page, select the **Automatically** option. We can choose this option because the DHCP server is installed on the Domain Controller behind the VPN server. If you do not have a DHCP server, you will have to select the **From a specified range of addresses** (from **a specified address range**) then enter the list of addresses that VPN clients can use when connecting to the network through VPN Gateway. Now click **Next** .

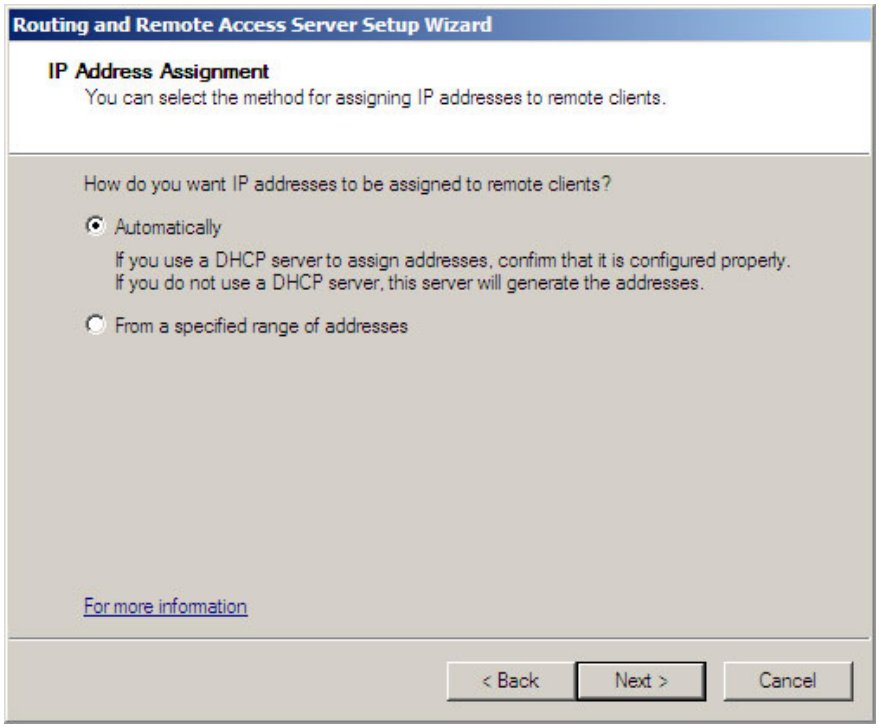

Figure 17: The page specifies the IP address.

6. On **Managing Multiple Remote Access Servers page** , select option N **o, use Routing and Remote Access to authenticate connection requests** . This is the option we use when there is no NPS or RADIUS server. Since the VPN server is a domain member, we can use domain accounts to authenticate users. If the VPN server is not a domain member, only local accounts on the VPN server can be used if we do not use the NPS server. Then click **Next** .

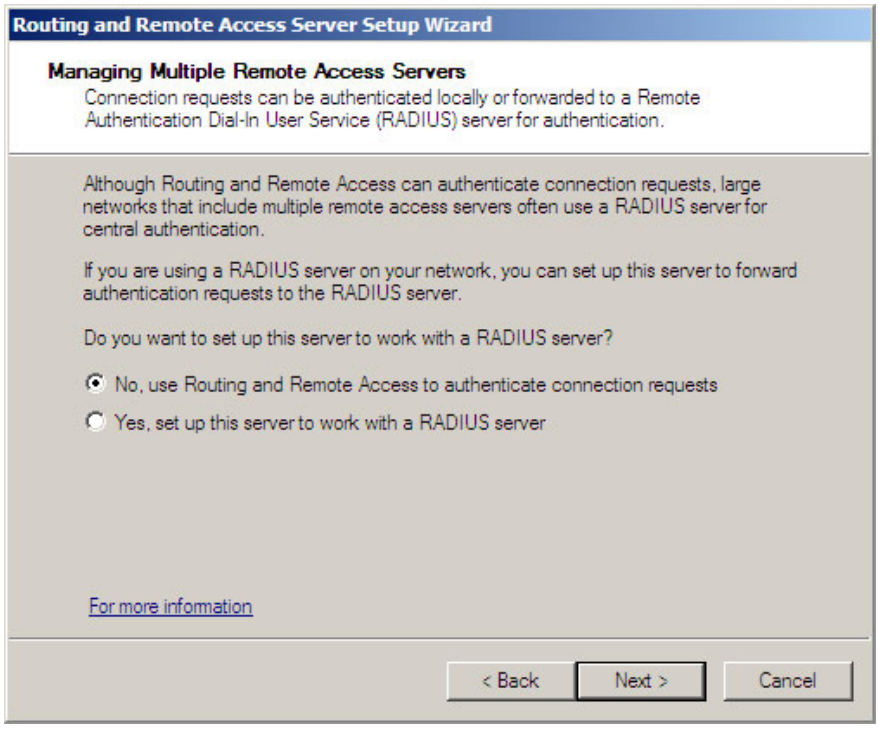

Figure 18: Managing multiple Remote Access Server owners.

7. Check the configuration information on the **Completing the Routing and Remote Access Server Setup Wizard page** and click **Finish** .

8. Click **OK** on the **Routing and Remote Access** dialog box to indicate that the mail forwarding process on DHCP needs a DHCP forwarding agent.

9. In the left pane, expand the **Routing and Remote Access** node **and** then click the **Ports** node. You will then see WAN Miniport connections for SSTP appear.

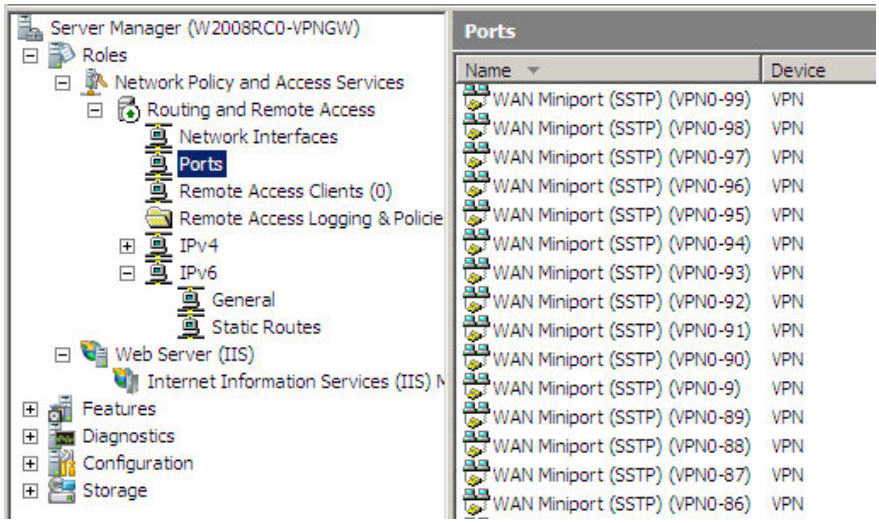

Figure 19: List of WAN Miniport connections for SSTP.

Configure NAT server to publish CRL

As mentioned above, the SSL VPN client needs to download the CRL to confirm that the Certificate Server on the VPN server is not canceled. To do this, we need to configure a device in front of the Certificate Server to forward HTTP requests to the CRL address to the Certificate Server.

To find out which URL the SSL VPN client needs to connect to to download the CRL, go to the VPN server and then double-click Certificate in the IIS Console. Select the Details tab of this Certificate and navigate to the CRL Distribution Points section and then click on this item. In the table below you will see many different distribution points based on the protocol used to access these points. In the Certificate shown below we need to allow SSL VPN clients to access the CRL via the URL: *http://win2008rc0-dc.msfirewall.org/CertEnroll/WIN2008RC0-DC.msfirewall.org.crl.*

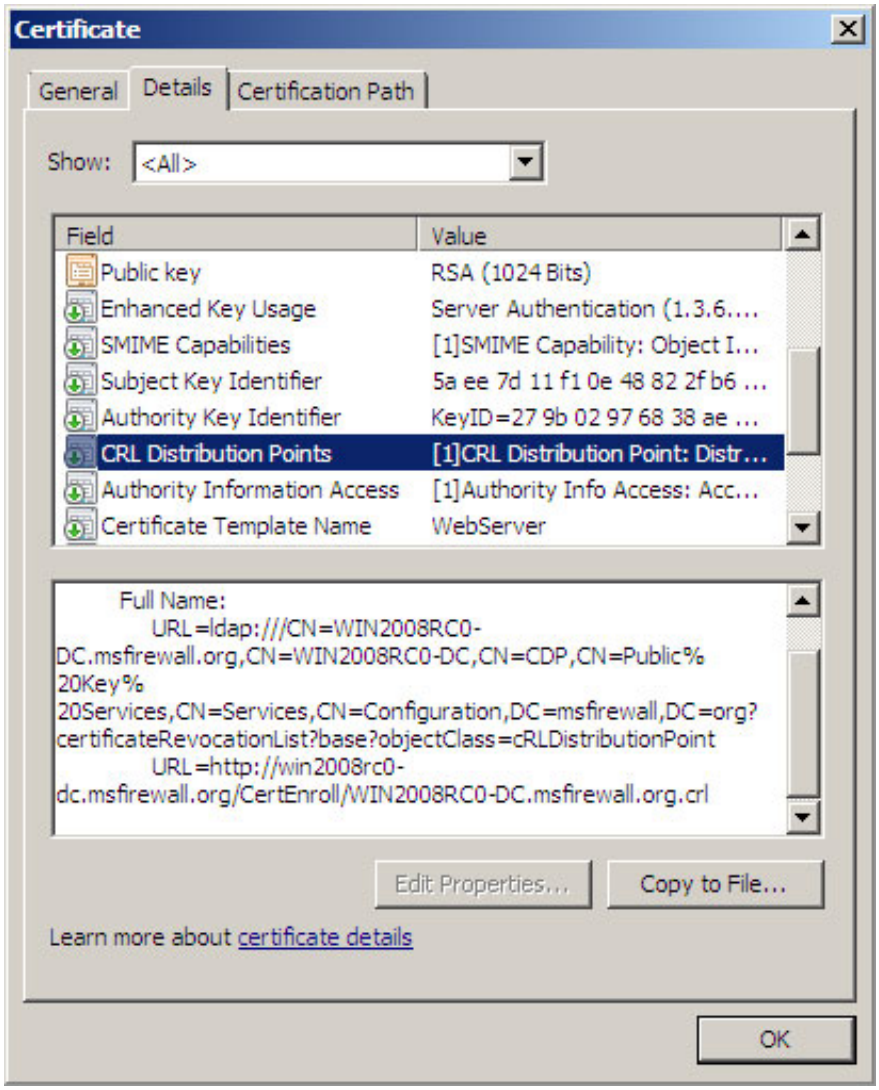

Figure 20: Sample URL that the SSL VPN client uses to access the CRL.

So we need to create a Public DNS entry for this name so that external VPN clients can handle this name for an IP address on the external interface of the ISA Firewall. In this example we will have to handle win2008rc0-dc.msfirewall.org for the IP address on the external interface of the ISA Firewall. When making a connection to the external interface of the ISA Firewall, the ISA Firewall will forward this connection to the NAT server on the VPN server that will then perform a NAT transformation and send this connection to the CA hosting the CDP.

Note that the default CRL page name may not be secure because it exposes the name of the personal computer on the Internet. We can create a private CDP (CRL Distribution Point) to prevent this if considering exposing the CA's personal computer name in Public DNS is a security issue.

Do the following to configure the RRAS NAT to forward HTTP requests to the Certificate Server:

1. In the left pane of **Server Manager** , expand node **Routing and Remote Access** and then expand the **IPv4** node, click on the **NAT** node.

2. In the **NAT** node, right-click on the external interface (In this example, the name of the external interface is *Local Area Connection*) and then select **Properties** .

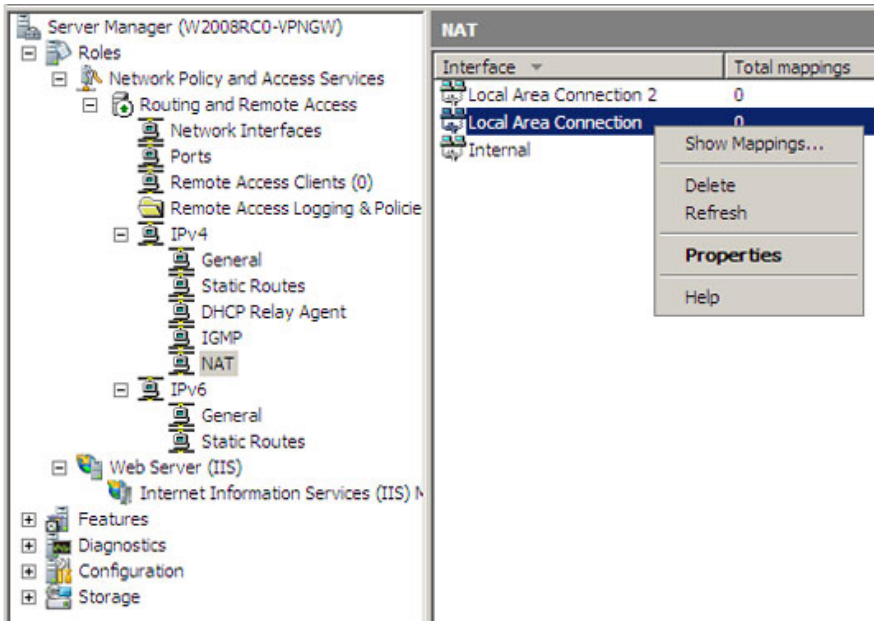

Figure 21: Open the properties window of the external interface.

3. In the **Local Area Connection Properties** dialog box, select the **Web Server (HTTP) check box** . The **Edit Service** dialog **box** will then appear. In the **Private Address** box, enter the IP address of the Server Certificate on the local network. Done, click **OK** .

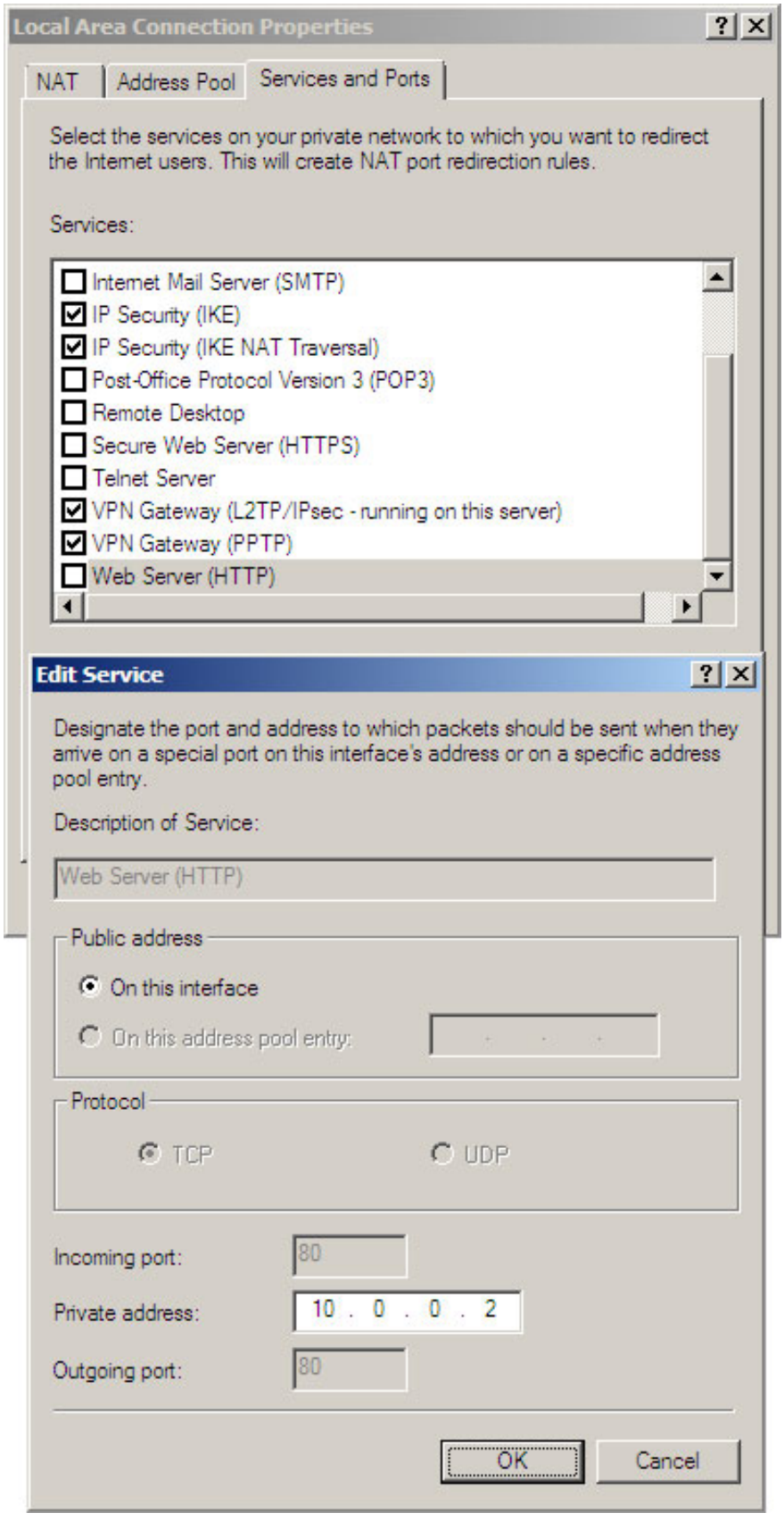

Figure 22: Enter the IP address of the Certificate Server on the internal network for the Provate Address.

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

Now that the NAT server is configured and installed, in the next section we will configure the CA server, ISA Firewall and SSTP VPN client.

Conclude

In this section we have explored some of the disadvantages of public remote access jcacs VPN access and the SSTP protocol method that helps overcome these problems by enabling VPN connections to make a connection. SSL connection over TCP port 443 is allowed through all firewalls in these environments. We then installed the Certificate service on the VPN server to create a Computer Certificate. After installing this Certificate on the SSL VPN server, we installed RRAS VPN and NAT services on the VPN Gateway. And we have finished configuring the NAT server on the VPN gateway to forward incoming HTTP connections forwarded by the ISA Firewall to perform on the CA that stores the CDP. In the next section, we will configure the CA server, ISA Firewall and SSTP VPN client.