Creating SSL Server 2008 Server with ISA 2006 Firewalls (Part 3)

In the previous two sections, we have explored some of the limitations of accessing VPNs from public networks, and then configured the CDP Website and ISA Firewall.

Network Administration **- In the previous two articles we learned some limitations of VPN access from public networks, and then implemented the configuration of CDP Website and ISA Firewall. In addition, we have also activated user accounts for Dial-in access.**

>> Create an SSL Server 2008 Server with ISA 2006 Firewalls (Part 1)
>> Create an SSL Server 2008 Server with ISA 2006 Firewalls (Part 2)

In the third and final part of this series, we will configure the SSL VPN client to connect to the SSTP SSL VPN server, and then verify this connection. At the same time, we will check some authentication information on the SSL VPN client, ISA Firewall and RRAS server to confirm that the SSTP connection was successful.

Configure HOSTS file on VPN client

Next we will perform the remaining operations on the workstation. The first thing to do is configure the HOSTS file so that we can simulate a public DNS structure. There are two names that we need to include in the HOSTS file. The first name is the name of the VPN server (defined by the Subject Name on the license that we connect to the SSL VPN server), the other name is CDP URL (also appears in this license). Information about CDP has been mentioned in part one.

Keep in mind that these names will be associated with the IP addresses on the external interface of the ISA Firewall receiving incoming connections as settings in the **Publishing Rule** and **Listener** .

The two names that we need to enter into the HOSTS file in this example are:

192.168.1.72 sstp.msfirewall.org
192.168.1.72 win2008rc0-dc.msfirewall.org

Follow these steps on the Vista SP1 VPN client to configure the HOSTS file:

1. Click the **Start** menu, enter *c: windowssystem32driversetchosts* into the search box and press **Enter** .

2. In the **Open With** dialog box, select **Notepad** .

3. Enter the items into the HOSTS file according to the format shown in Figure 1.

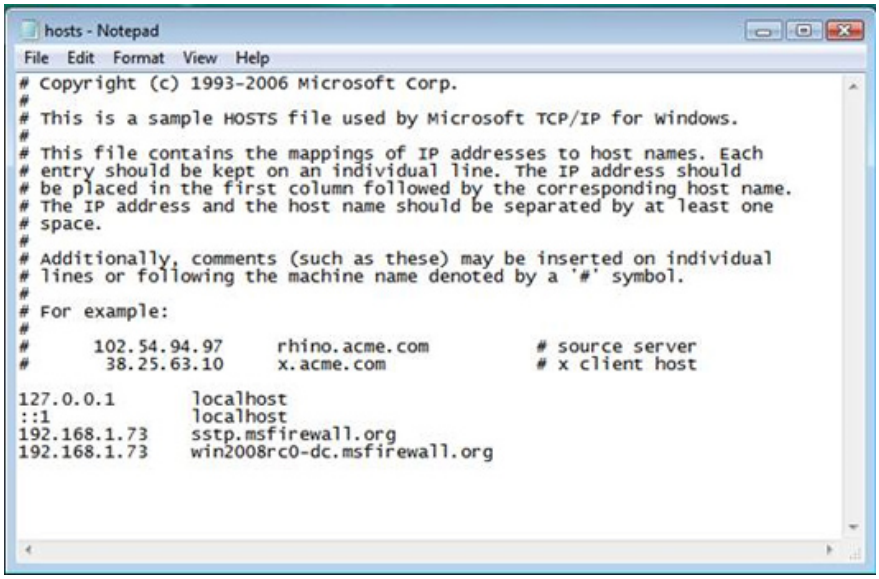

Figure 1: Content of HOSTS file in Notepad.

4. Then save and close this file.

Use PPTP to connect to the VPN server

The next step is to create a VPN connection (dial-up) on the Vista SP1 client to enable the establishment of an initial VPN connection to the VPN server. Because this workstation is not a domain member, the CA license will not be automatically installed on the Trusted Root Certificate Authorities license storage area. If this workstation is a domain member, the auto-license feature will take care of this process because we have installed an Enterprise CA.

The easiest way to do this is to create a PPTP connection from the Vista Vista VPN client to the Windows Server 2008 VPN server. By default, the VPN server will support PPTP connections and the client will prioritize PPTP connection than L2TP / IPSec and SSTP. First we need to create a connectoid VPN or connection object. Perform the following operations on the VPN client:

1. On the VPN client, right-click the network icon and select **Network and Sharing Center** .

2. In the **Network Sharing Center** window, click the **Set up a connection or network link** in the left panel.

3. On the **Choose a connection option page** , select **Connect to a workplace** and then click **Next** .

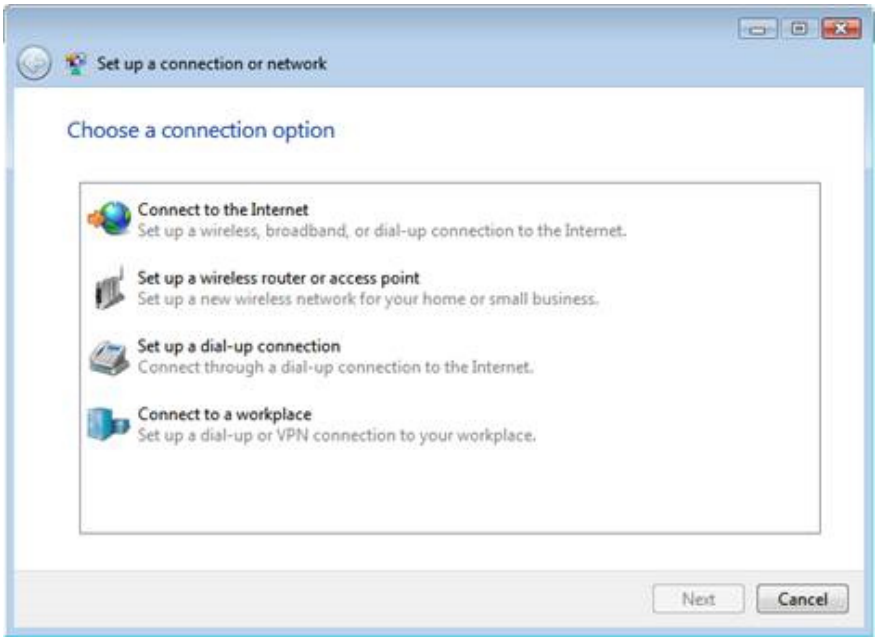

Figure 2: Select connection options for workstations.

4. On the **How do you want to connect page** , select **Use my Internet connection (VPN)** .

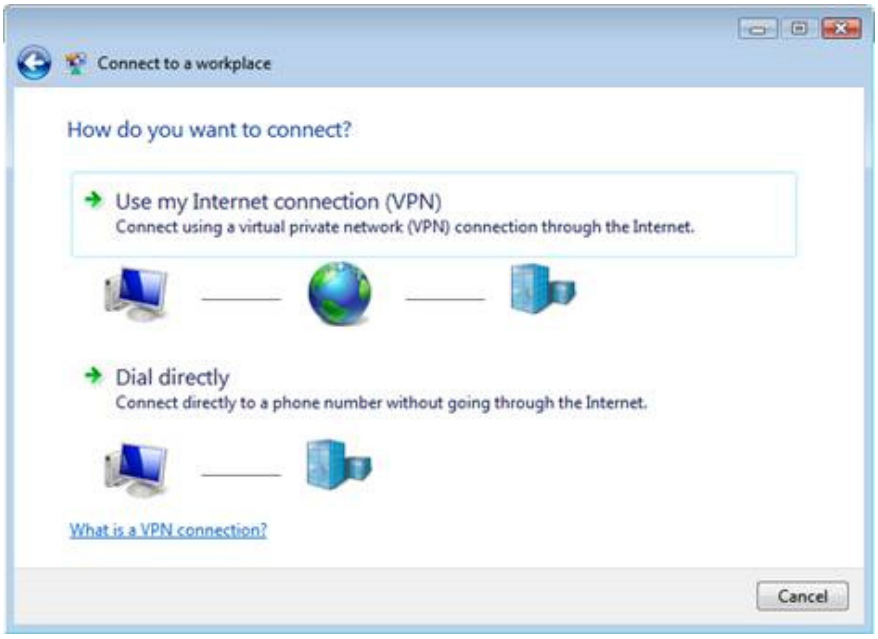

Figure 3: Select connection method.

5. On the **Type the Internet address page to connect to** , enter the name of the SSL VPN server. Make sure that this name is the same as the *Common Name* on the license used by the SSL VPN server. In this example, the name to enter is *sstp.msfirewall.org* . Then enter a **Destination Name** . In this example we will enter *SSL VPN* and then click **Next** .

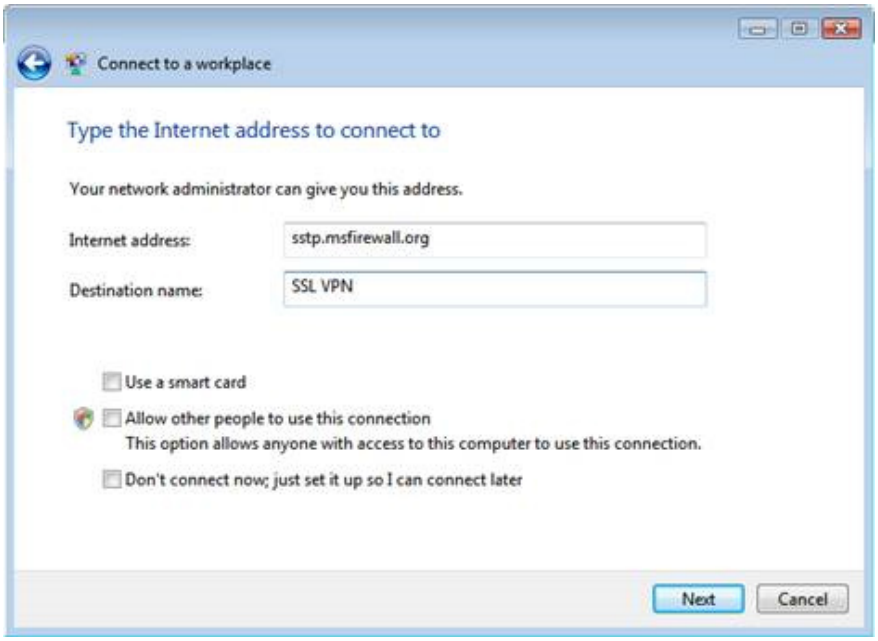

Figure 4: Enter the network address and destination server for the connection.

6. On the **Type your user name and password page** , enter the **User Name** , **Password** and **Domain** and click **Connect** .

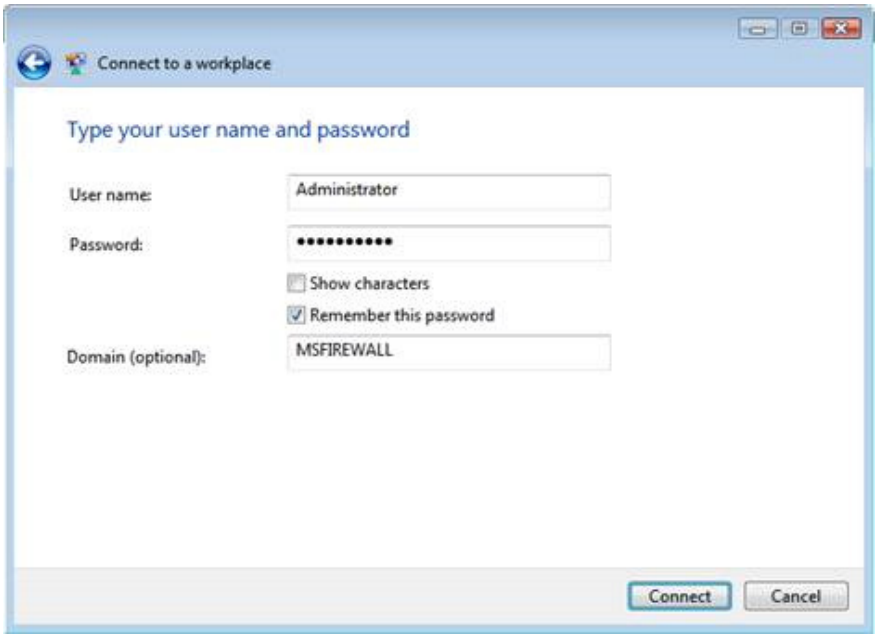

Figure 5: Register username and password.

7. On the page **You are connected** click **Close** .

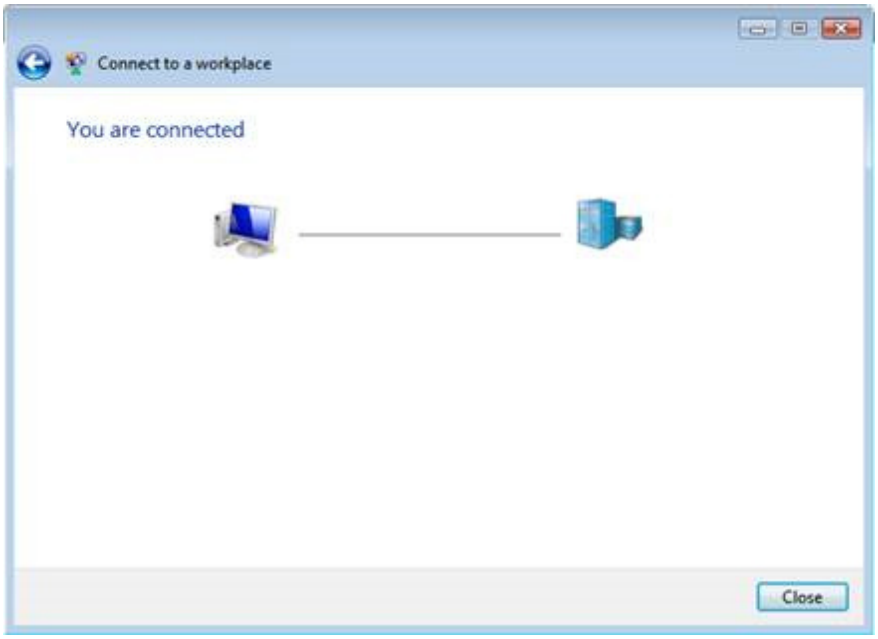

Figure 6: Connecting successfully.

8. Select the **Work** option on the **Select a location for the 'SSL VPN' network page** .

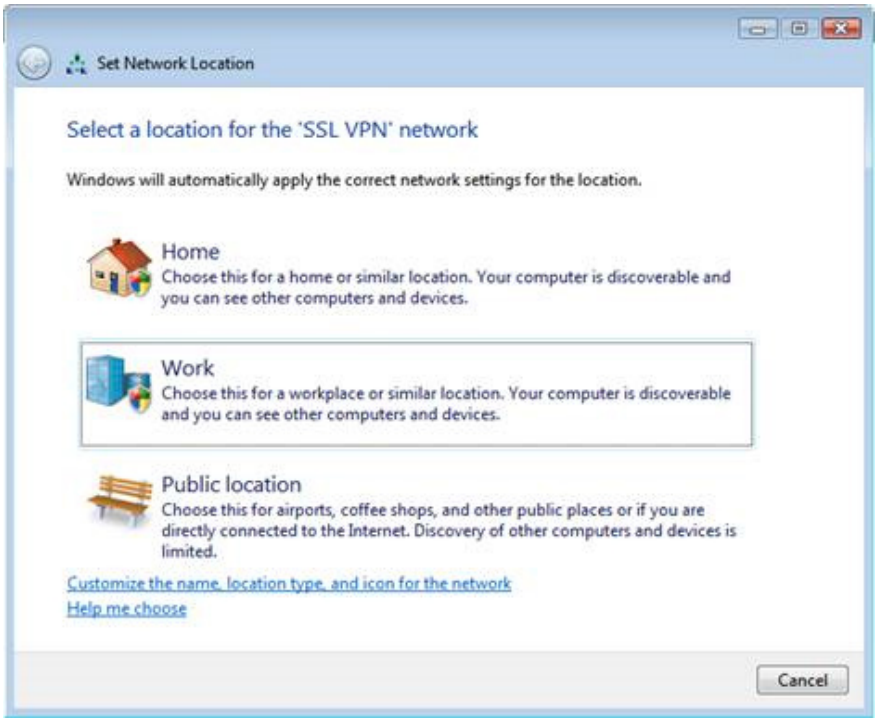

Figure 7: Selecting a location for the SSL VPN network.

9. Click **Continue** on the UAC message.

10. Click **Close** on the **Successfully set network settings page** .

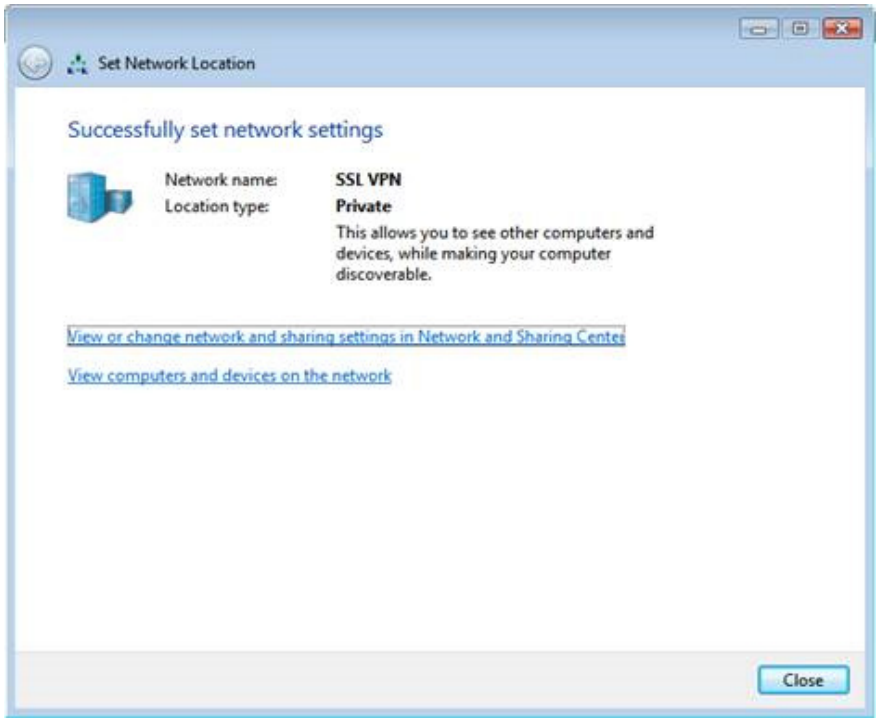

Figure 8: Successful network installation.

11. In the **Network and Sharing Center** , click the **View** status link in the **SSL VPN** area as shown in Figure 9. We will then see the **SSL VPN Status** dialog box with the VPN connection type shown as **PPTP** . Click the **Close** button on this dialog box.

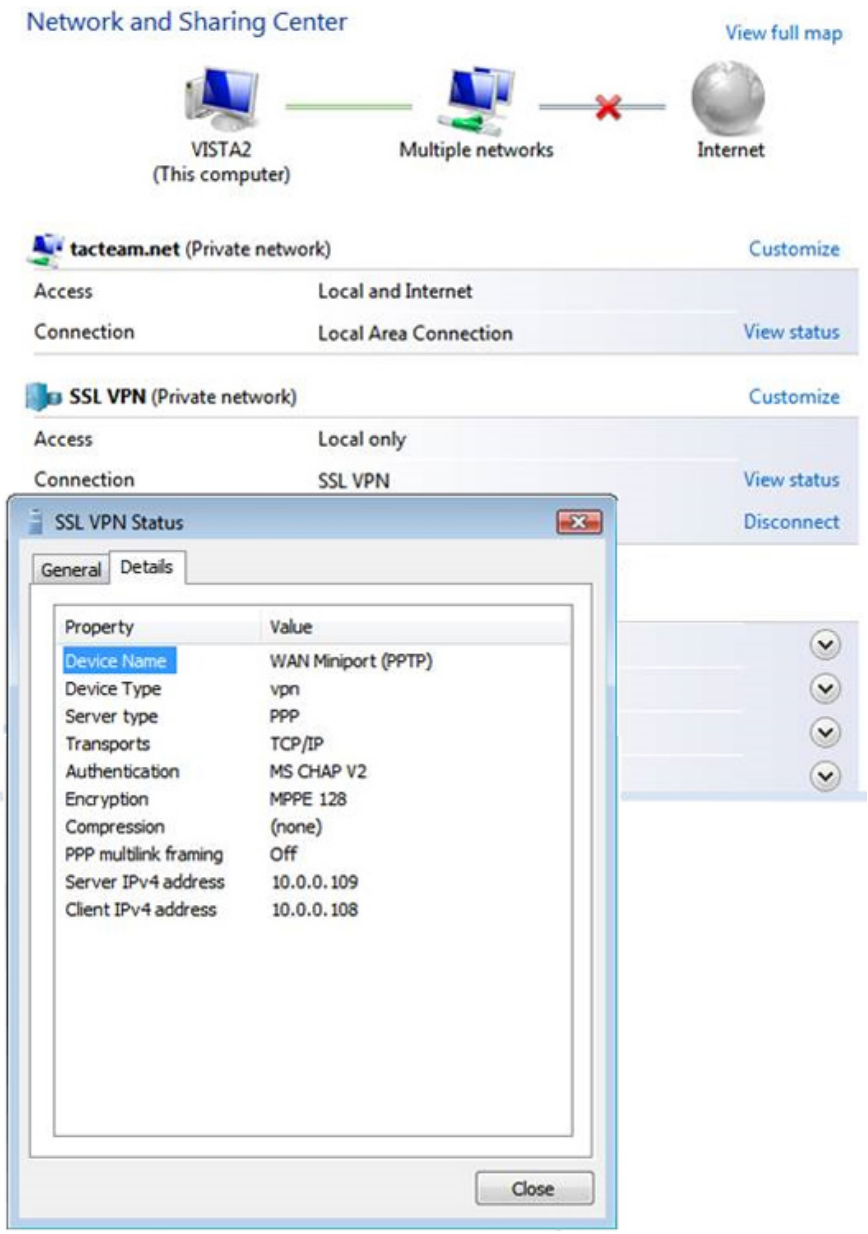

Figure 9: Confirm the newly established VPN connection type.

12. Open **Command Prompt** and ping *Domain Controller* . In this example, the Domain Controller IP address is *10.0.0.2* . If the VPN connection is successful, we will get a response from this Domain Controller.

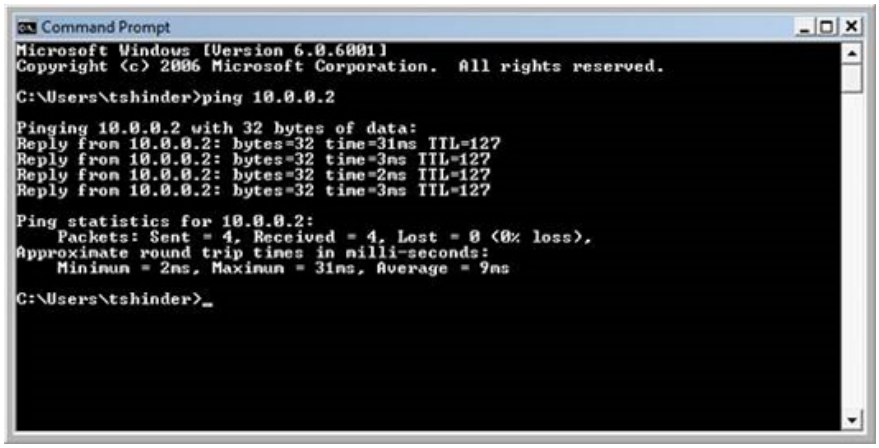

Figure 10: Feedback displayed when ping Domain Controller.

Create a CA license from the Enterprise CA

The SSL VPN client needs to authorize the CA that issued the license to be used by the SSTP VPN server. To set up this trust we need to install the CA license of the CA that created the license for the VPN server. We can do this by connecting automatic CA pages on the intranet and installing this license in the Trusted Root Certification Authorities license area of ??the VPN client.

Follow these steps to create a license from Web Enrollment:

1. On the VPN client, connect to the VPN server via PPTP link, enter *http://10.0.0.2/certsrv* into the address bar in **Internet Explorer** and press **Enter** .

2. Enter a valid username and password in the **Crednetials** dialog box. In this example we will use the username and password of the default domain administrator account.

3. On the Web Enrollment **Welcome** page, click the **Download a CA certificate, certificate chain, or CRL link** .

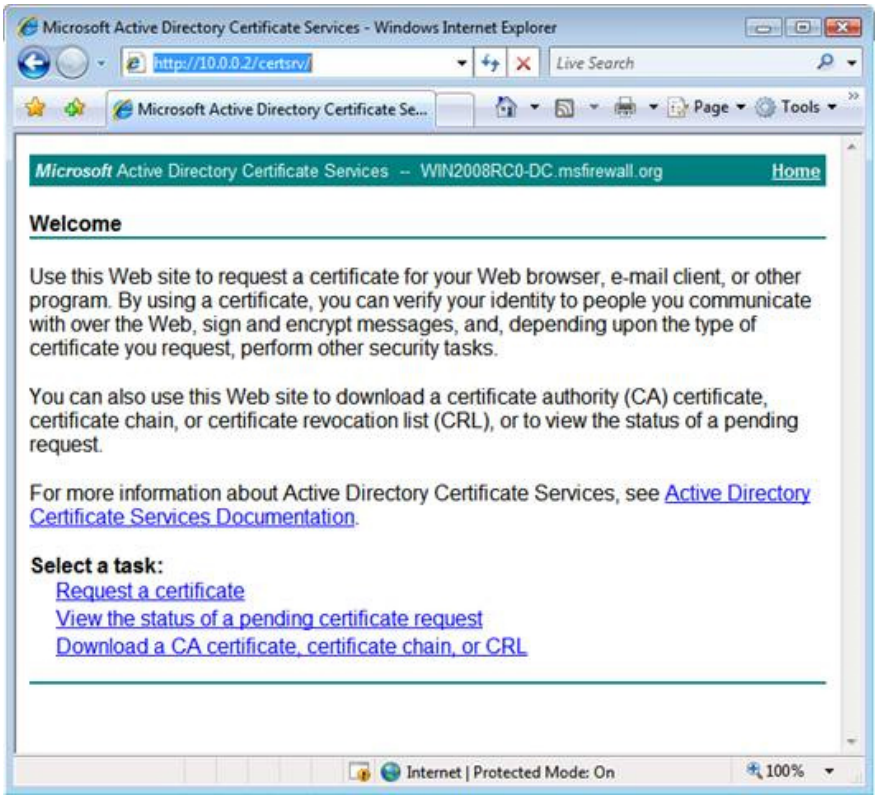

Figure 11: Web Enrollment Welcome page.

4. Click the **Allow** button in the warning dialog box that looks like this: *A website wants to open web content using this program on your computer* (A Web *site wants to open web data using this program on* the system). Next, click the **Close** button on the dialog box **Did you notice the Information bar** if it appears.

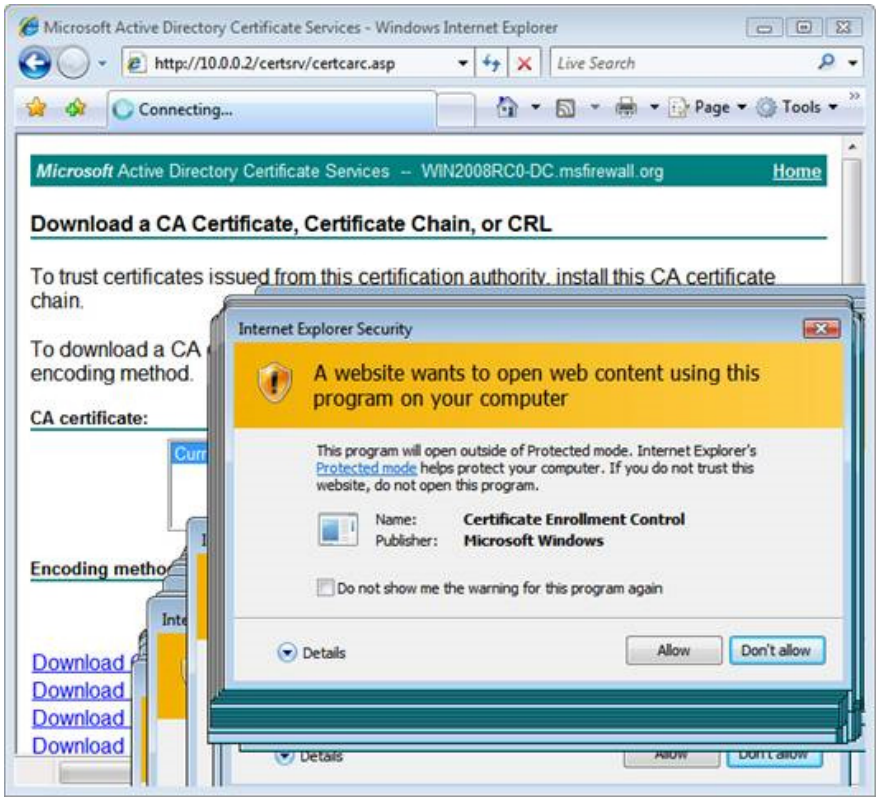

Figure 12: A warning appears after clicking the link in step 3.

5. Note that the information bar informs us that this Web site may not display correctly because the ActiveX Control has been blocked. However this is not important and we will download the CA license and use the **Certificates MMC** to install this license. Click the **Download CA Certificate link** .

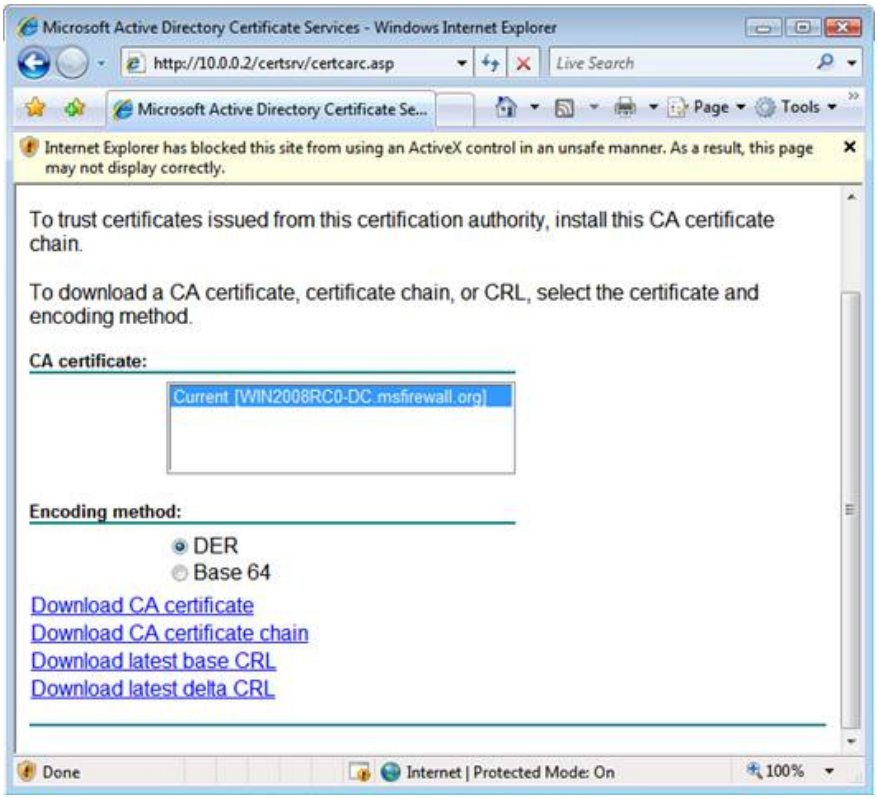

Figure 13: Download list.

6. In the **File Download - Security Warning** dialog box, click the **Save** button and save the license to the screen.

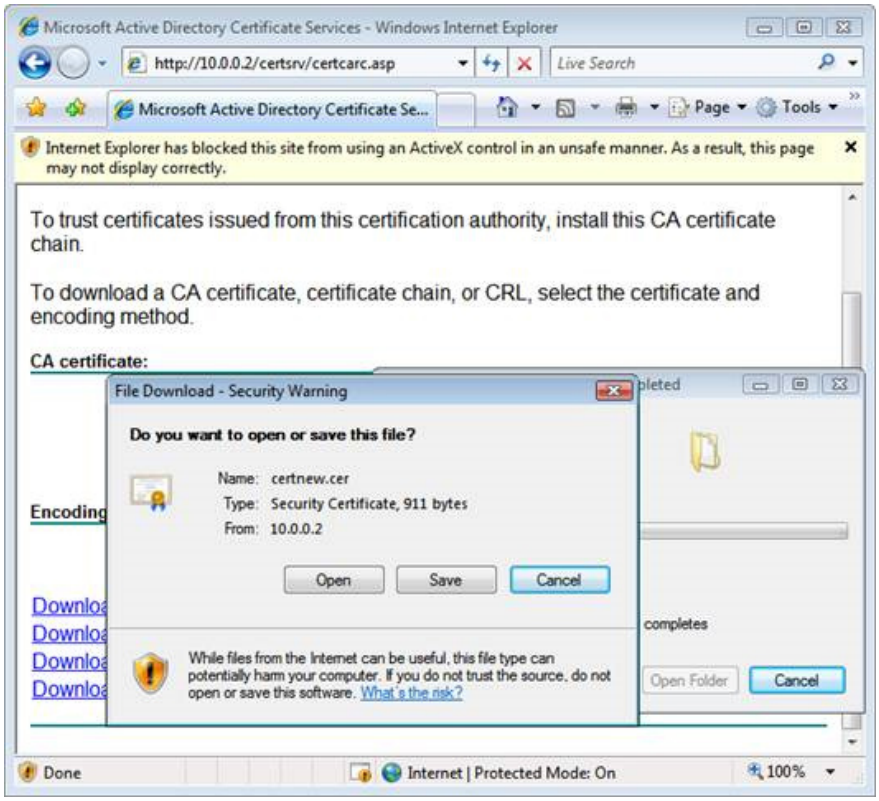

Figure 14: Save the CA license to the screen.

7. Click the **Close** button on the **Download complete** dialog box and then close **Internet Explorer** .

Next we need to install the **CA** license into the license storage area T **rusted Root Certification Authorities** of the VPN client. Follow these steps:

1. **Go to** the **Start** menu, enter *mmc* in the **Search** box and press **Enter** .

2. Click **Continue** in the UAC dialog box.

3. In the **Console1** window, go to the **File** menu and then click **Add / Remove Snap-in** .

4. In the **Add or Remove Snap-ins** dialog box, click the **Certificates** item in the **Available snap-ins list** and click **Add** .

5. On the **Certificates snap-in page** , select the **Computer account** option and then click **Finish** .

6. On the **Select Computer** page, select the **Local computer** option and then click **Finish** .

7. Click **OK** on the **Add or Remove Snap-ins** dialog box.

8. In the left pane of this **Console** , expand the **Certificates** node **(Local Computer)** and then expand the **Trusted Root Certification Authorities** node. Click on the **Certificates** node. Right-click the **Certificates** node and select **All Tasks | Import** .

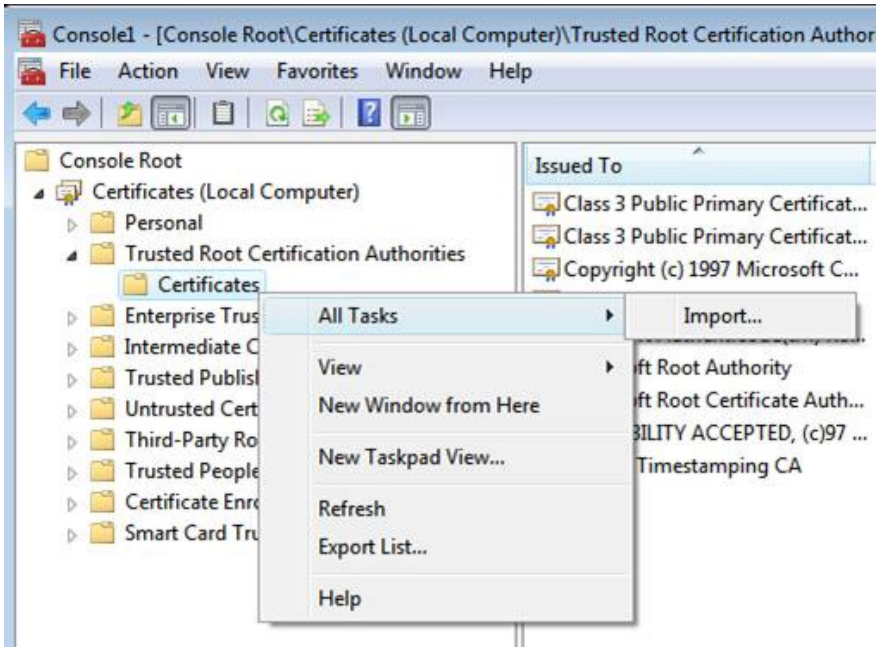

Figure 15: Importing the license into the Trusted Root Certification Authorities area.

9. Click **Next** on the **Welcome to the Certificate Import Wizard page** .

10. On the **File to Import** page, use the **Browse** button to find this license and click **Next** .

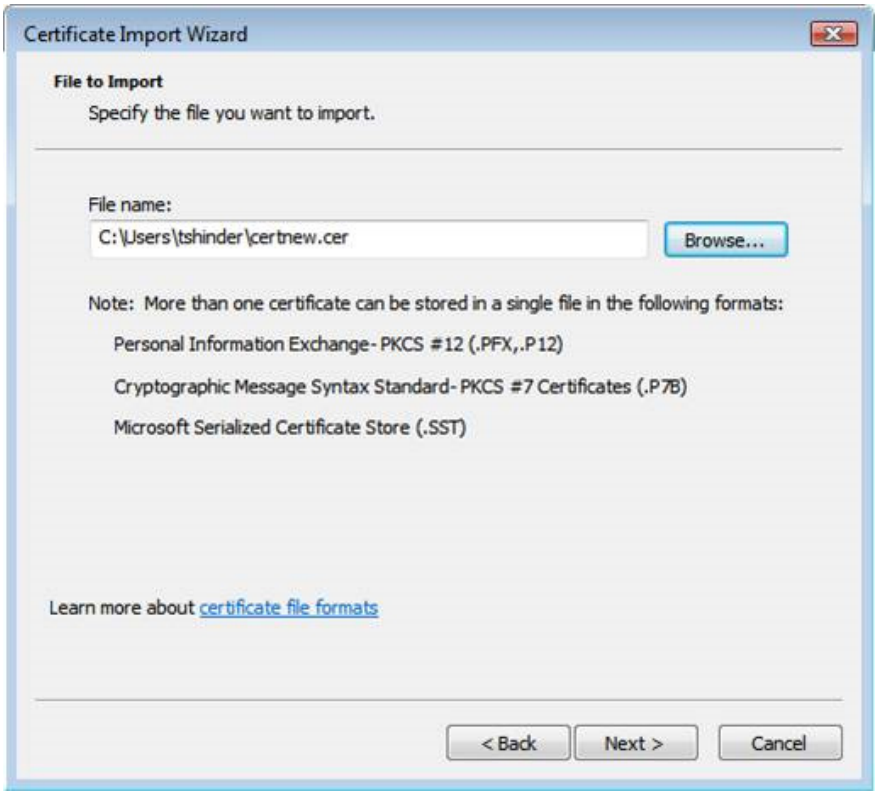

Figure 16: Search for the license to import.

11. On the **Certificate Store** page, confirm that the option **Place all certificates in the following store** is selected and Trusted Root Certification Authorities will appear in the **Certificate Store** field as shown in Figure 17. Then click **Next** .

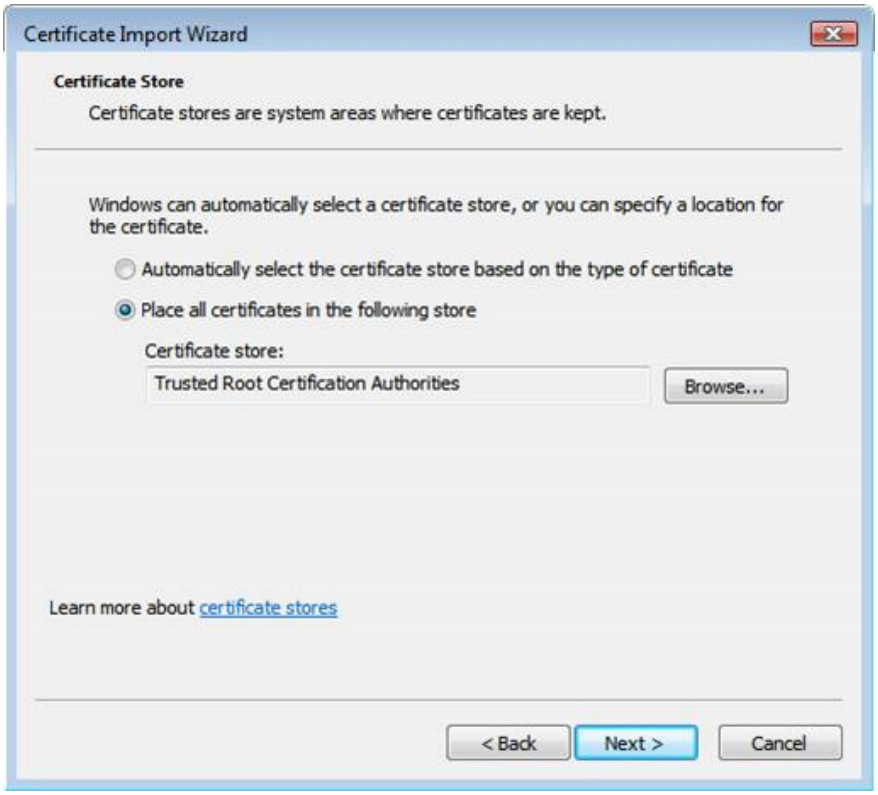

Figure 17: Selecting a storage area for the imported license.

12. Click **Finish** on the **Completing the Certificate Import page** .

13. Click **OK** in the dialog box that says the import process was successful.

14. This license will then appear in **Console1** as shown in Figure 18.

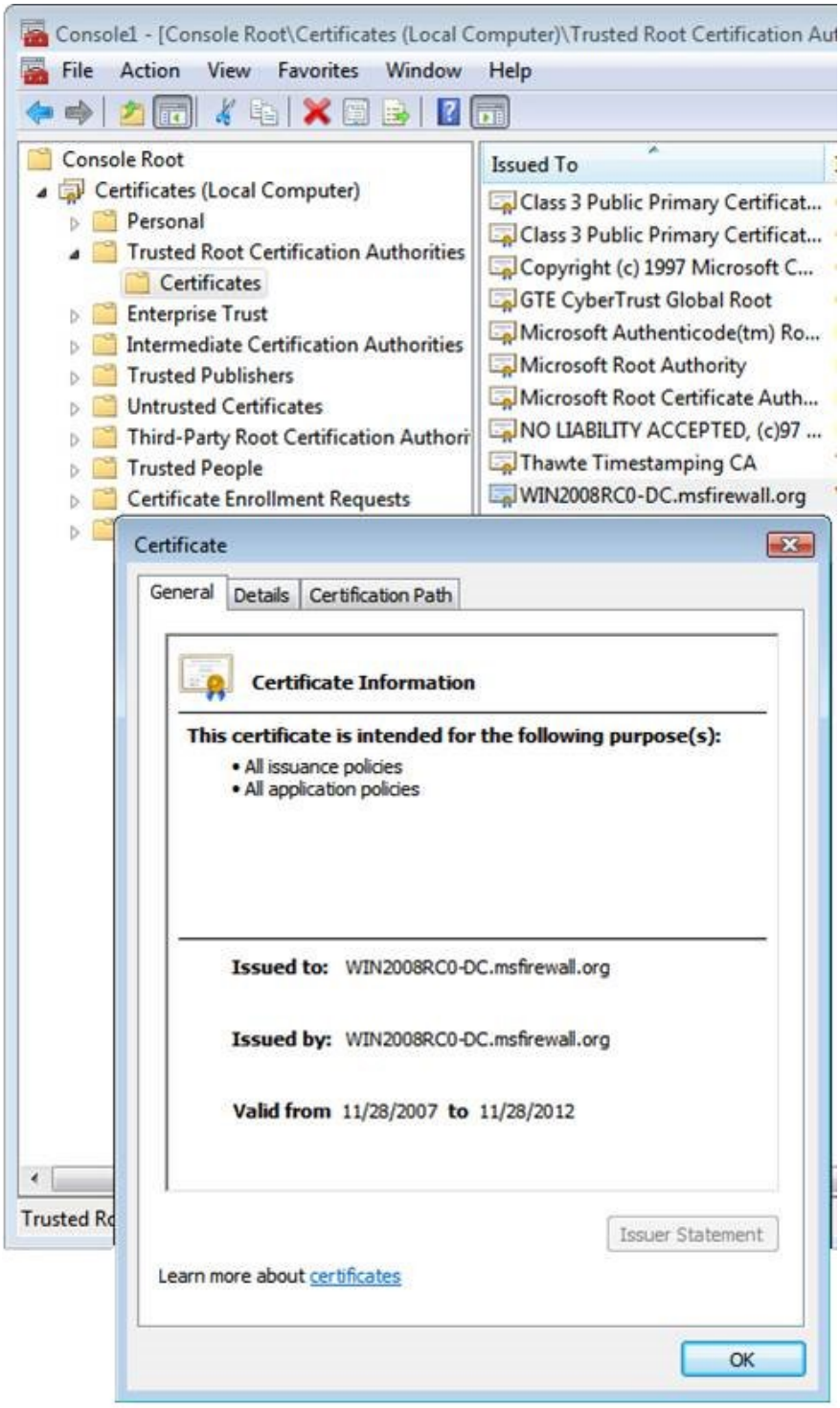

Figure 18: License displayed in Console1 after successful import.

15. Close the **MMC Console** .

Configure the client to use SSTP and connect to the VPN server using SSTP

Now we need to disconnect the VPN and then configure the VPN client to use SSTP for the VPN protocol. In a production environment, we will not interfere with the user's work if we use the Connection Manager Administration Kit to create VPN connectoid for them to install on the client using SSTP, or only configure SSTP ports. on the VPN server.

This depends on the environment, as we arrange everything so that users can use PPTP while deploying licenses. Of course, we can always deploy out-of-bandwidth licenses, such as through websites or email, in which case we don't need to allow PPTP. However, if there are some downgraded clients that do not support SSTP, then we need to allow PPTP or L2TP / IPSec, so we will not be able to cancel all ports outside of SSTP. In that case, we will have to manually configure or an updated CMAK software.

Another option is to connect the SSTP Listener to a specific IP address in the RRAS server. Then, we can create a separate CMAK package that points to the IP address on the SSL VPN server receiving SSTP connections. Other addresses on the SSTP VPN server will receive PPTP and L2TP / IPSec connections.

Perform the following actions to disconnect the SSTP session and configure the VPN client's connectoid to use SSTP:

1. On the VPN client, open the **Network and Sharing Center** .

2. In the **Network and Sharing Center** window, click on the **Disconnect** link at the bottom of the **View Status** link. The SSL VPN will disappear from the **Network and Sharing Center** .

3. In the **Network and Sharing Center** , click the **Manage network connections link** .

4. Right-click **SSL VPN and** select **Properties** .

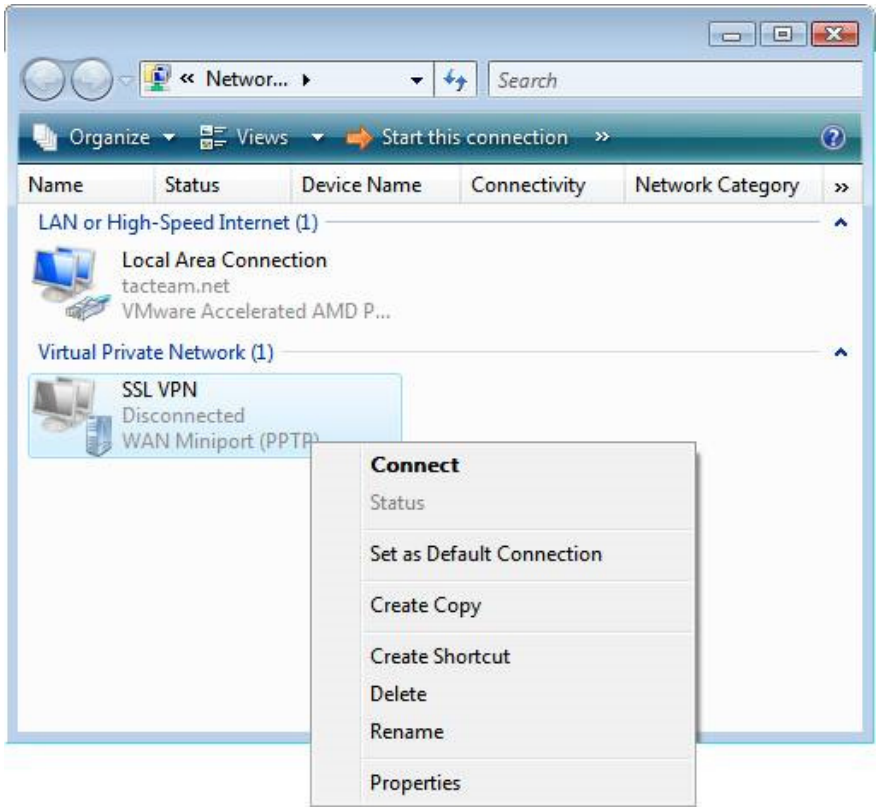

Figure 19: Open the properties dialog of SSL VPN.

5. In the **SSL VPN Properties** dialog box, select the **Networking** tab. In the drop-down list of **Type of VPN** , select **Secure Socket Tunneling Protocol (SSTP)** . Click **OK** .

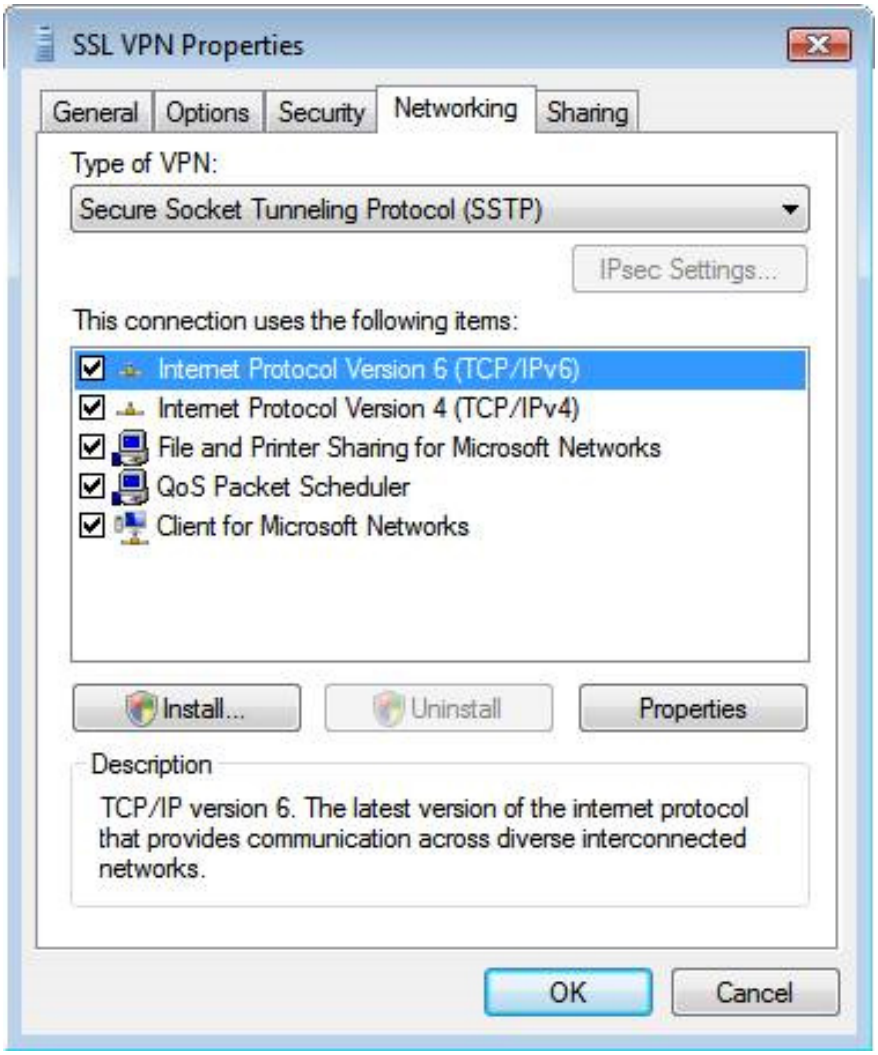

Figure 20: Property page of SSL VPN.

6. Double-click **SSL VPN connectoid** in the **Network Connections** window.

7. In the **Connect SSL VPN** dialog box, click the **Connect** button.

8. When the connection is complete, click on **SSL VPN connectoid** in the **Network Connections** window and select **Status** .

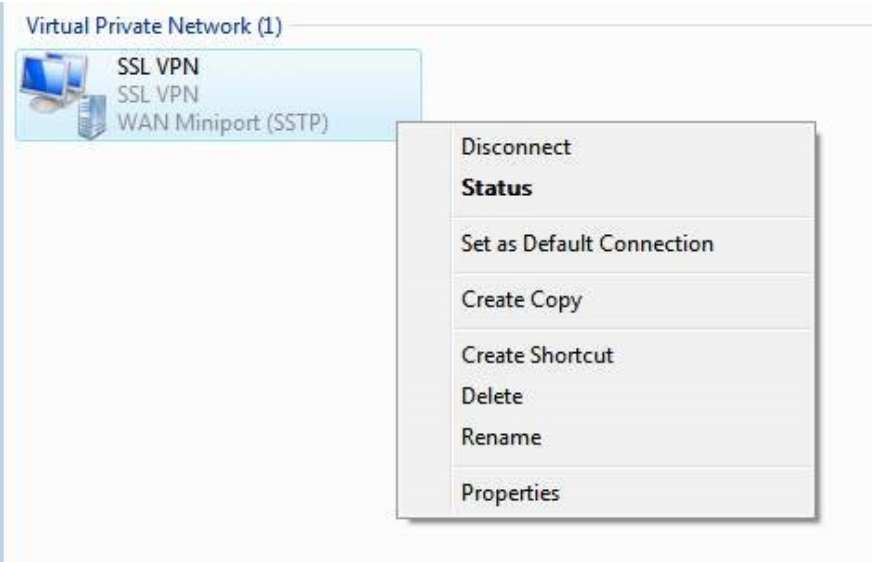

Figure 21: Select Status in the context menu of SSL VPN connectoid.

9. In the **SSL VPN Status** dialog box, we can see that the **SSTP WAN Miniport** connection has been established.

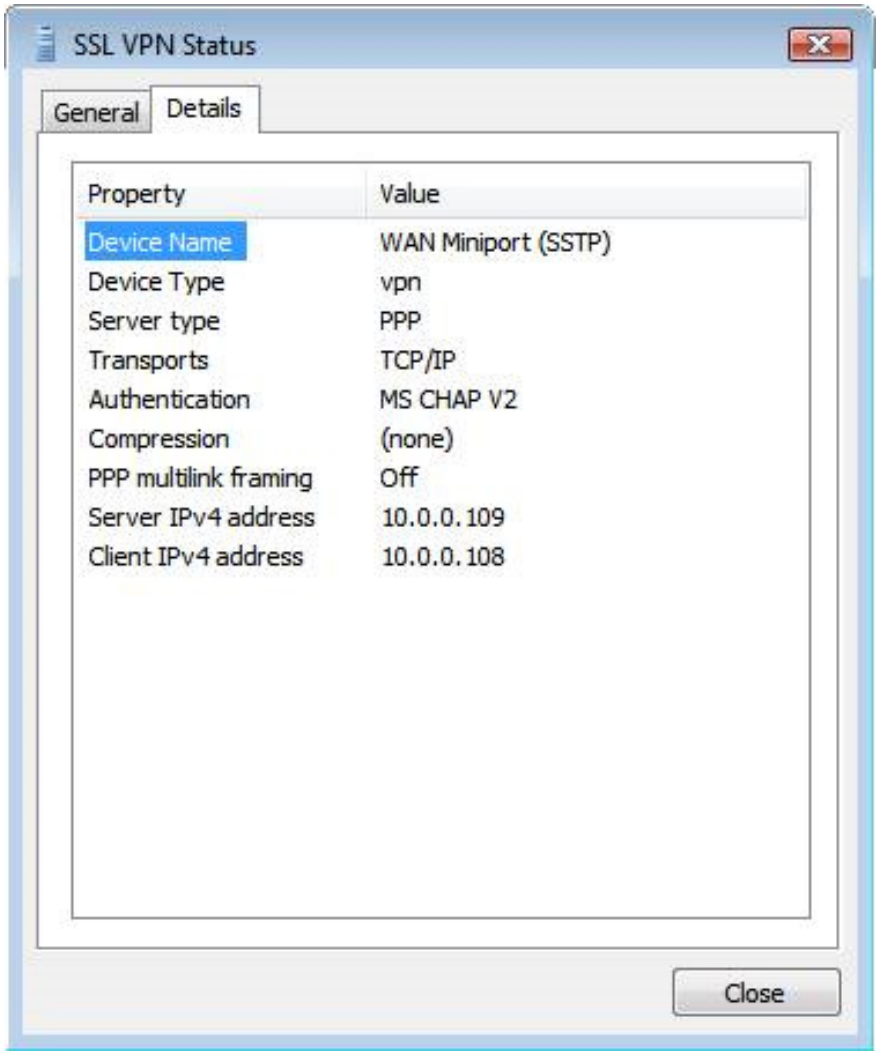

Figure 22: SSL VPN Status dialog box.

10. If you access the VPN server and then open the **Routing and Remote Access** console, we will confirm that the SSTP connection has been established.

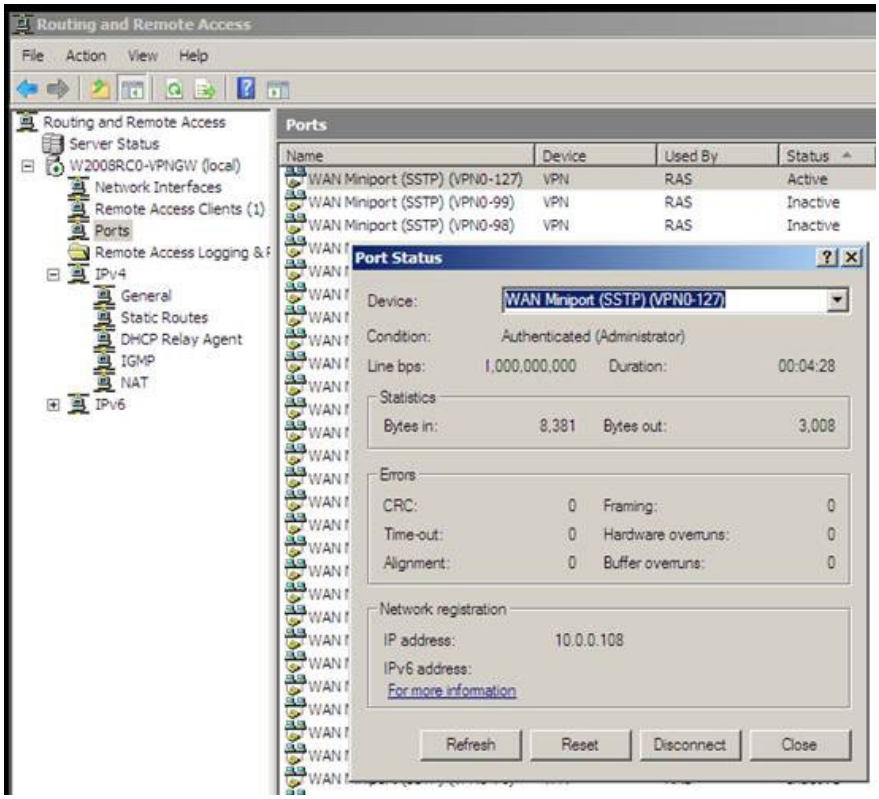

Figure 23: Confirm the SSTP connection in the Routing and Remote Access console.

If checked in the **ISA Firewall console** , we will see some logs of the SSL VPN connection.

Log Time	Client IP	Destination IP	Destination Port	Protocol	Action	Rule
1/29/2008 7:29:48 PM	192.168.1.70	255.255.255.255	1211	Unidentified IP Tr...	Denied Connection	Default rule
1/29/2008 7:30:05 PM	192.168.1.70	255.255.255.255	1211	Unidentified IP Tr...	Denied Connection	Default rule
1/29/2008 7:30:22 PM	192.168.1.76	10.10.10.2	443	HTTPS Server	Initiated Connect...	SSTP Server

Figure 24: Some records in the ISA Firewall.

Conclude

In the last part of a three-part series on how to create Windows Server 2008 SSL VPN server using the 2006 ISA Firewall, we have completed the configuration for user accounts, CRL Website, ISA Firewall and SSL VPN client. . We have finished the series with completing the SSTP connection and confirming that the connection was successful.

You finished reading the article "**Creating SSL Server 2008 Server with ISA 2006 Firewalls (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.