Creating SSL Server 2008 Server with ISA 2006 Firewalls (Part 2)

In this section, we will configure a user account that allows dialup access, and then configure this CDP to allow anonymous HTTP connections.

Network Administration **- In the first part of this series we looked at some of the disadvantages of remote VPN access at public access points, and the method of using the SSTP protocol to overcome these problems. By enabling VPN connections to do so through a TCP 443 SSL link allowed by all firewall systems in these environments.**

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

We then installed the Certificate Service (licensing service) on the SSL VPN server. After installing the license on the VPN server, we also installed RRAS VPN and NAT services on the VPN gateway. In addition, we have completed the configuration of the NAT server on the Gateway VPN to forward the HTTP connections to the forward ISA Firewall for execution on the CA that hosts the CDP.

In this section, we will configure a user account that allows dialup access, and then configure this CDP to allow anonymous HTTP connections. We will then complete this process by configuring the ISA Firewall to allow the necessary connections to the VPN server and CDP Website.

Configure user accounts to allow dial-up connections

User accounts need to be licensed for dial-up access before they can connect to a Windows VPN server that is a member of an Active Directory domain. The best method we can apply is to use a Network Policy Server (NPS) and use the default user account license used to allow remote access based on NPS Policy. However, we have not yet installed a NPS in this situation so we will have to manually configure the dial-in license for this user.

We need to do the following steps to enable the dial-in license on the user account that we want to connect to the SSL VPN server. In this example we will enable dial-in access for the default domain administrator account:

1. At the **Domain Controller** , open the **Active Directory User and Computers Console** from the **Administrative Tools** menu.

2. In the left pane of this Console, expand the domain name and click on the **User** node. Then double click on the Administrator account.

3. Click the **Dial-in** tab. The default setting in this tab is **Control access through NPS Network Policy** . Since we do not have any NPS server in this situation, we will change this setting to **Allow Access** as shown in Figure 1, then click **OK** .

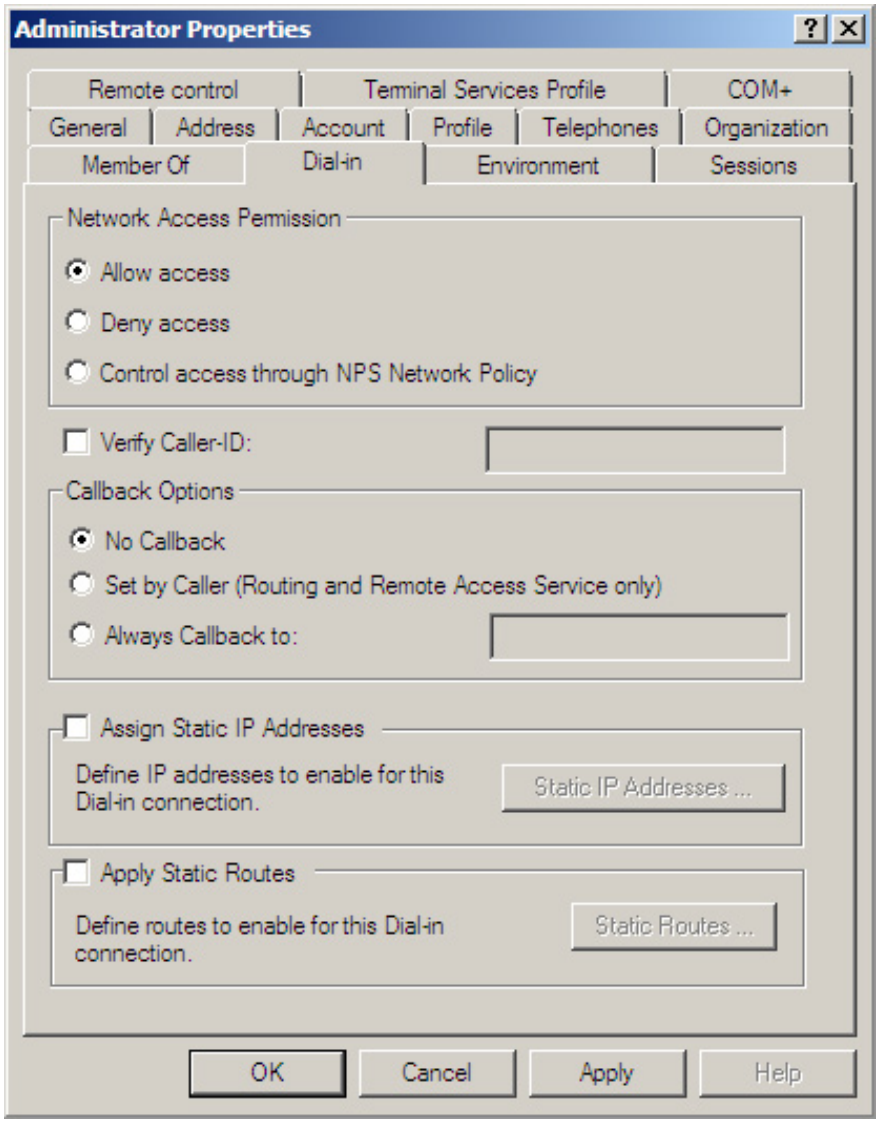

Figure 1: Properties dialog of the Administrator account.

Configure IIS on the Certificate Server to allow HTTP connection for the CRL directory

For some reason, when the installation wizard performs the Certificate Services Website installation, it will configure the CRL directory using an SSL connection. In terms of security, this is a pretty good idea, but the problem is that the URI on this license has not been configured using SSL. Since we are using the default settings for CDP in this article, we will have to turn off the SSL request on the CA Website for the CRL directory path.

Follow these steps to undo the SSL request for the CRL folder:

1. In the **Administrative Tools** menu, open **Internet Information Services (IIS) Manager** .

2. In the left pane of the **IIS Console** , expand the server name and expand the **Sites** node. Expand the **Default Website** node then click on the **CertEnroll** node as shown in Figure 2.

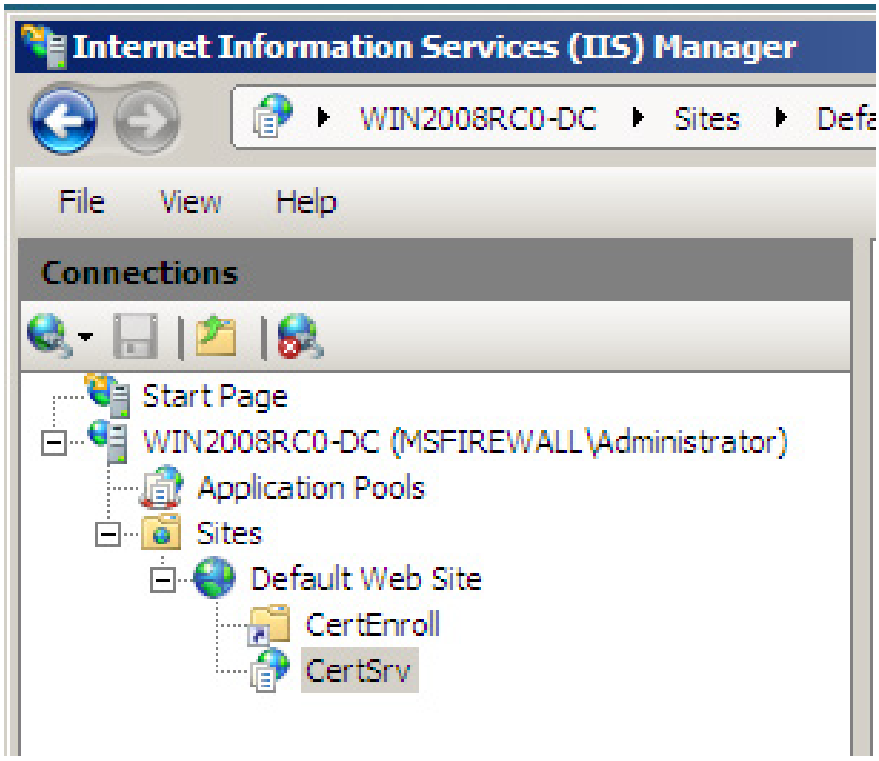

Figure 2: Access the CertEnroll node in IIS Manager.

3. If you check in the middle table of this console we will see that the CRL is located in this virtual directory as shown in Figure 3. To check the contents of this virtual directory, just click on the **Content View** button on the side. end of the middle table.

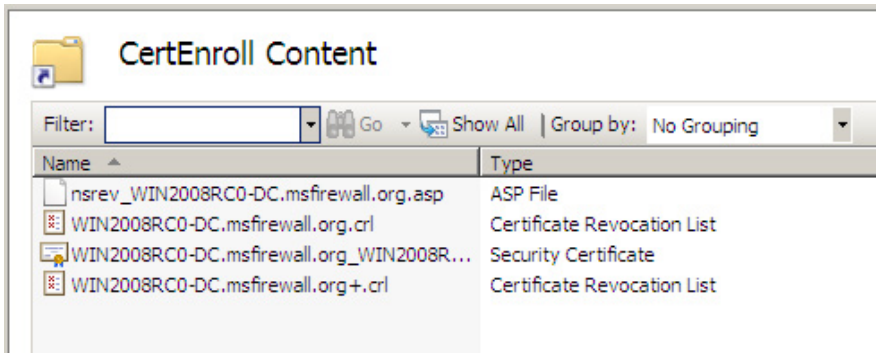

Figure 3: CRL in CertEnroll.

4. Click on the **Features View** button at the bottom of the middle panel, then double-click the **SSL Settings** icon.

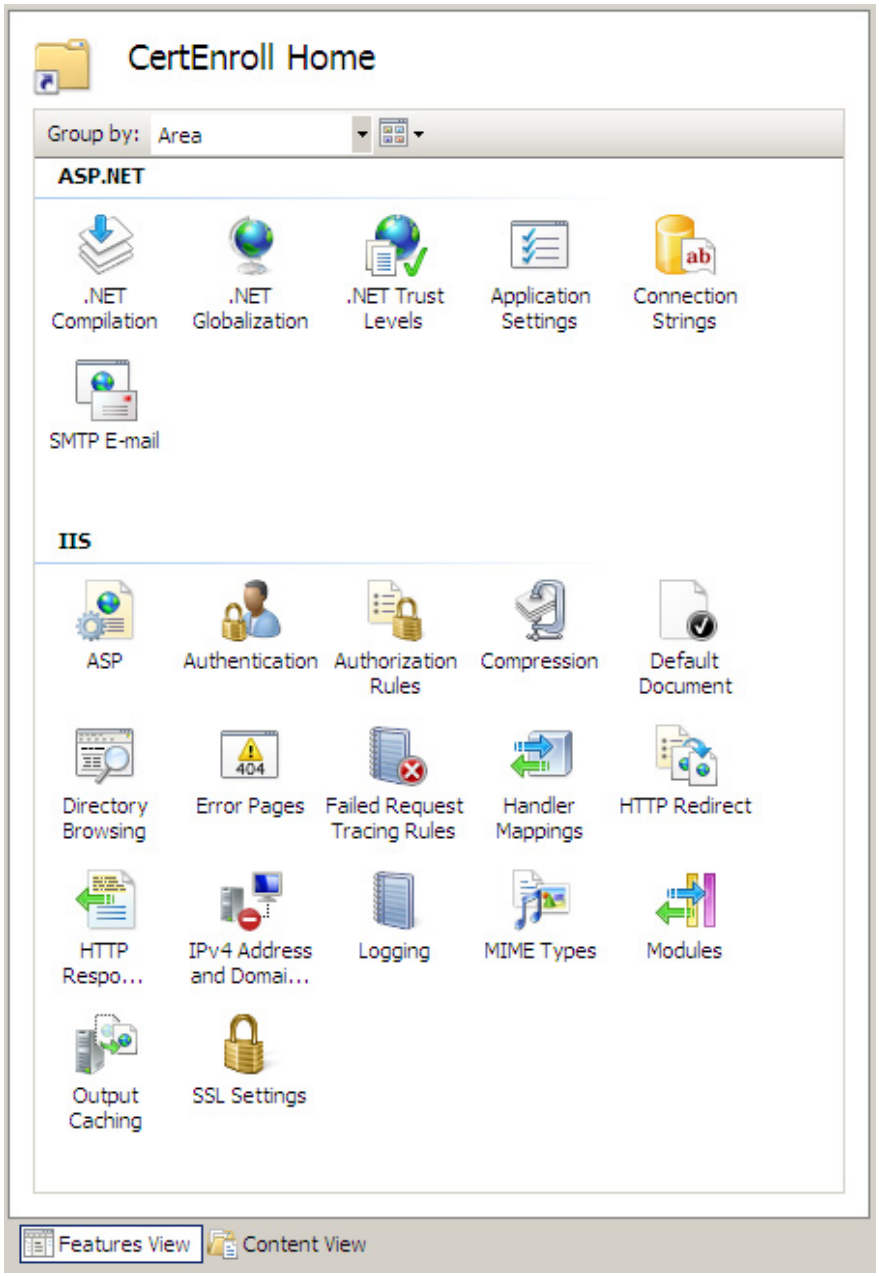

Figure 4: Content of CertEnroll virtual directory.

5. Then the **SSL Settings** page will appear. **Uncheck** the **Require SSL checkbox** and then click the **Apply** link in the right panel of this Console.

Figure 5: SSL Settings page.

6. Close the **IIS Manager Console** after you see the message *The changes have been successfully saved* (the *changes have been successfully saved*).

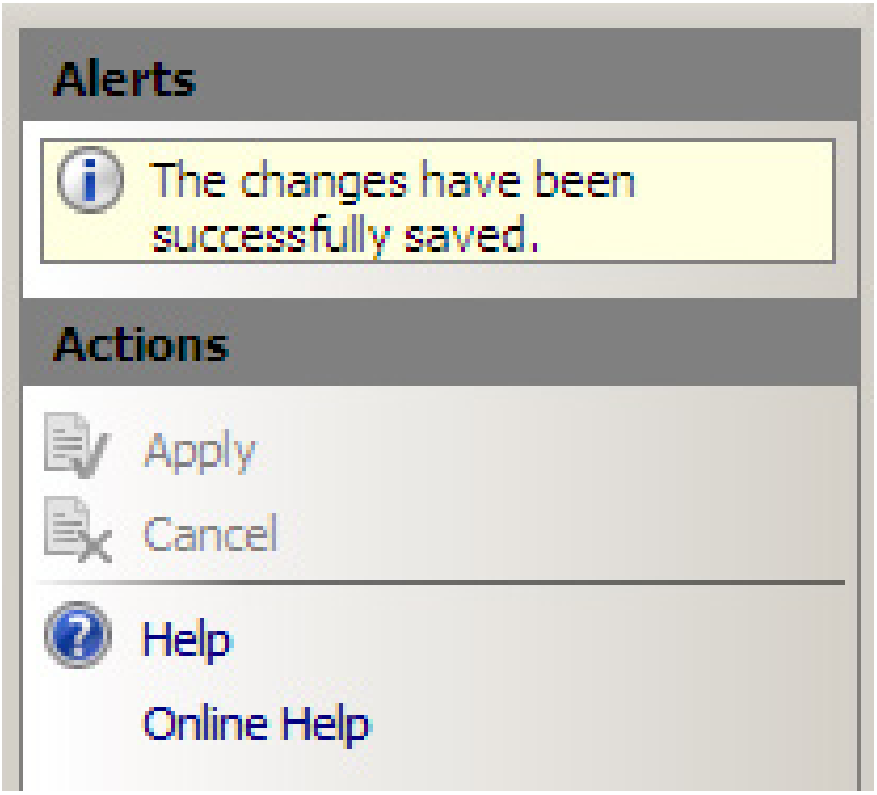

Figure 6: The message indicates the installation process was successful.

Configure the ISA Firewall with a PPTP VPN server, SSL VPN and the Web Publishing Rules of CDP

Here we will proceed to configure the ISA Firewall. We need to create three Publishing Rules to support this

process, including:

1. A Web Publishing Rule allows access to SSL VPN to CRL Distribution Point (CDP).
2. A Server Publishing Rule allows internal SSL connections to the SSTP server that allows the SSTP connection to be established with this VPN server.
3. A Server Publishing Rule allows PPTP access to the VPN server, so the VPN client can access the CA license from the Enrollment Website on the network behind the VPN server.

After creating the necessary permissions for the workstation, we can cancel the PPTP Rule. Or we can leave the PPTP Rule or use L2TP / IPSec instead of PPTP for a more secure connection. The reason we can leave another VPN protocol enabled is that only Windows Vista SP1 clients support SSTP.

Before starting this process, you might wonder why we use a Server Publishing Rule for SSTP connection. In general, if we use a Web Publishing Rule instead of a Server Publishing Rule, we can control access to the SSTP server based on the path and Public Name. We can even tighten this rule by configuring the HTTP Security Filter.

We will configure the CDP Web Publishing Rule:

1. In the **ISA Firewall Console** , click on the **Firewall Policy** node and then select the **Tasks** tab in the **Task Pane** , then click the **Publish Websites** link.

2. On the **Welcome to the New Web Publishing Rule Wizard page** , enter a name for this Rule in the **Web Publishing Rule name** box. In this example we will name this rule as *CDP Site* . Then click **Next** .

3. On the **Select Rule Action** page, select the **Allow** option and click **Next** .

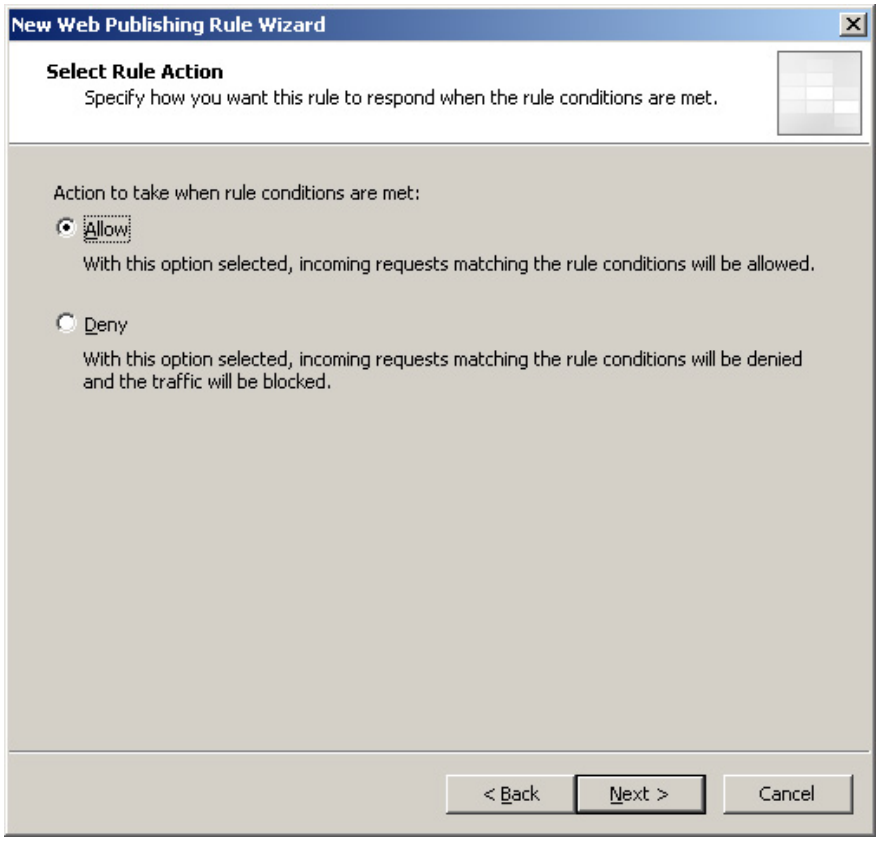

Figure 7: Select the action for Rule on the Select Rule Action page.

4. On the **Publishing Type** page, select the **Publish a single Web site option or load balancer option,** and then click **Next** .

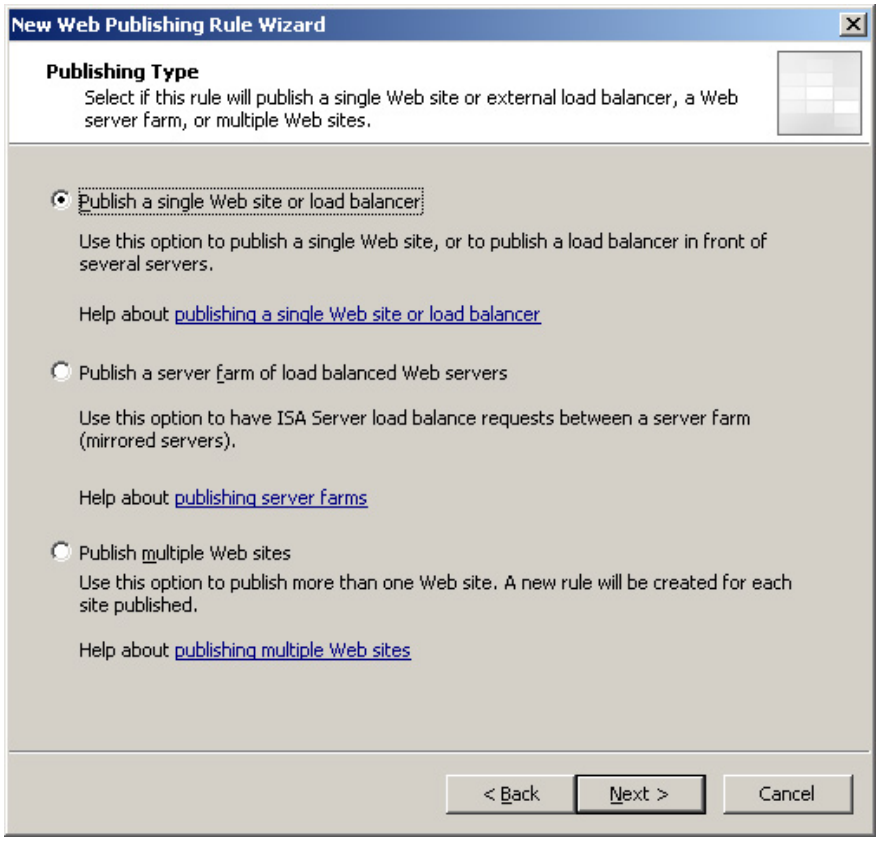

Figure 8: The Publishing Type page of the New Web Publishing Rule Wizard.

5. On the **Server Connection Security** page, select the option **Use non-secured connection to connect to published Web server or server farm** . We choose this option because the SSTP VPN client does not use SSL to connect to CDP. Then click **Next** .

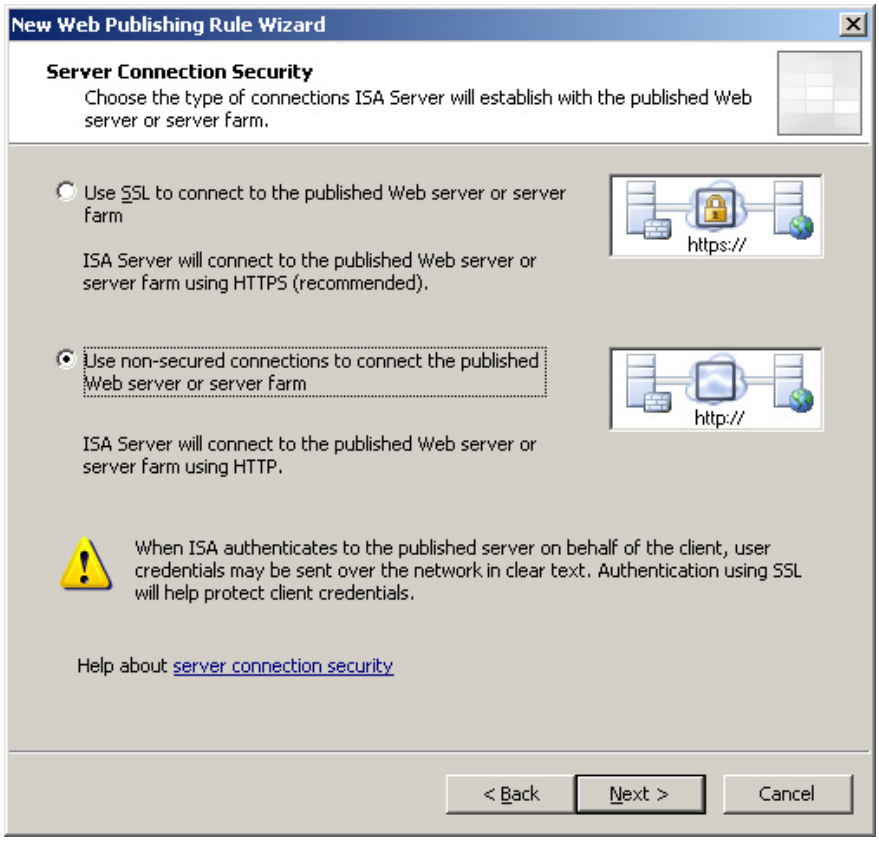

Figure 9: Server Connection Security page of the New Web Publishing Rule Wizard.

6. On the **Internal Publishing Details** page, enter a name for **CDP Website** in the **Internal site name** box. Since we are using HTTP, we can enter any name for CDP. If there is an SSL Publishing Rule, we will have to enter this name on the Website Certificate of this page. Select the box **Use a computer name or IP address to connect to the published server** (use **a computer name or IP address to connect to the** created server) and then enter the external communication IP address of the VPN server . In this case, the IP address on the external interface of the VPN server is *10.10.10.2* . This address will allow the NAT server on the VPN server to forward the HTTP connection to the CDP Website. Now click **Next** .

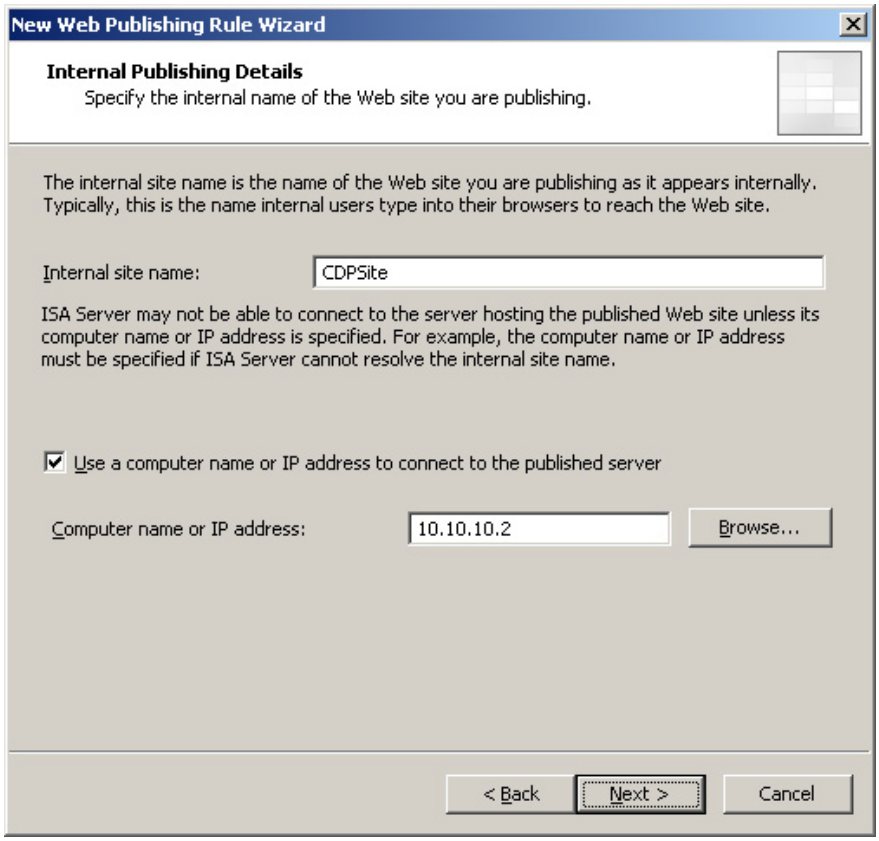

Figure 10: The Internal Publishing Details page of the New Web Puiblishing Rule Wizard.

7. When the SSTP VPN client calls the CRL, it will use the address on this license. In the first part of this series, the URL on this license gives the CRL a *http://win2008rc0-dc.msfirewall.org/CertEnroll/WIN2008RC0-DC.msfirewall.org.crl* . To secure the Web Publishing Rule, we can limit the number of paths that external clients can access through this Web Publishing Rule. Since we only want to grant access to the CRL, we will enter the path */CertEnroll/WIN2008RC0-DC.msfirewall.org.crl* to prevent external users from *accessing* other paths on the Certificate Server. We do not need to forward the Host Header because there is no Host Header used on the Certificate Server Website. Then click **Next** .

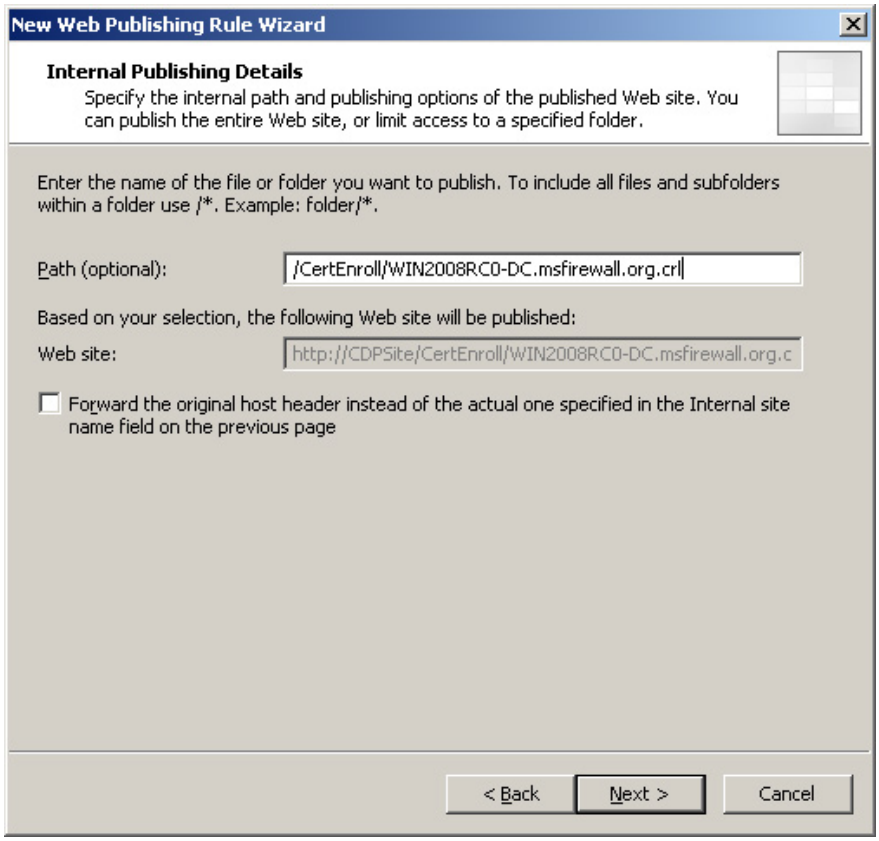

Figure 11: The Internal Publishing Detail page of the New Web Puiblishing Rule Wizard.

8. We can fix this rule by only allowing clients to enter the correct host name to access it via the Web Publishing Rule. The host name is listed in the CDP area of ??this license, in this case *win2008rc0-dc.msfirewall.org* . On the **Public Name Details** page, select **this Domain name option (type below)** from the drop-down list of the **Accept requests for field** . In the **Public name** box, enter *win2008rc0-dc.msfirewall.org* . We do not need to edit this path because we have configured it on the previous page of this wizard. Now click **Next** .

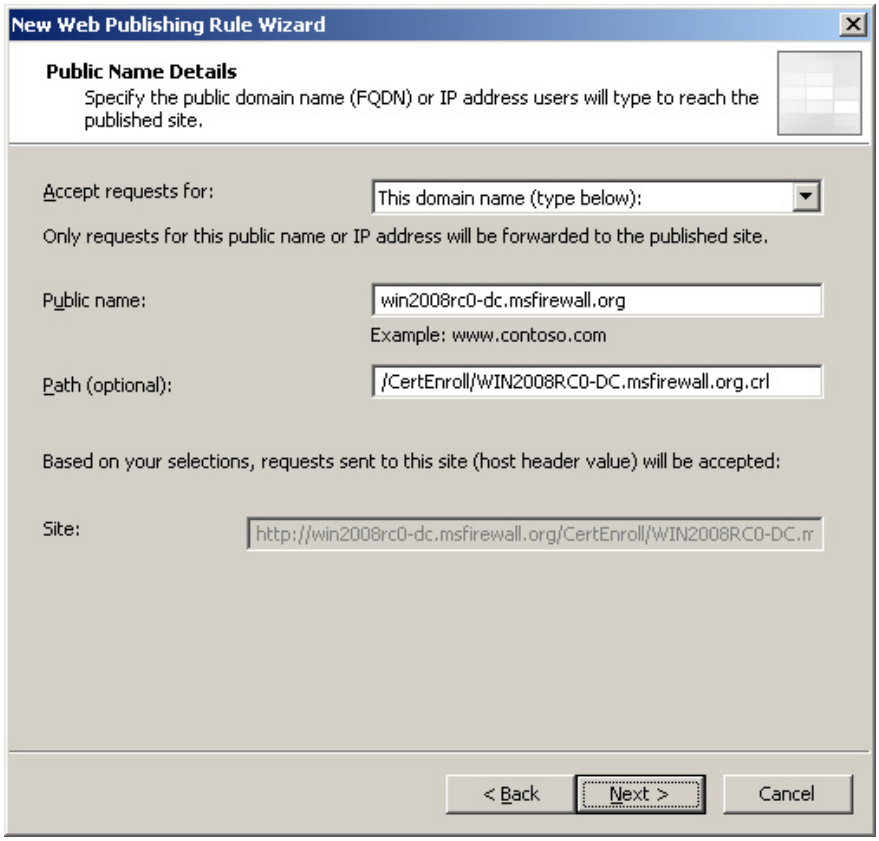

Figure 12: The Public Name Details page of the New Web Publishing Wizard.

9. Click the **New** button on the **Select Web Listener** page.

10. On the **Welcome to the New Web Listener Wizard page** , enter a name for the **Web Listener** in the **Web listener name** box. In this example we will enter the name of the *Web Listener HTTP* . Then click **Next** .

11. On the **Client Connection Security** page, select the option **Do not require SSL secured connections with clients** . We select this option because the SSTP client does not use SSL to access CDP. Then click **Next** .

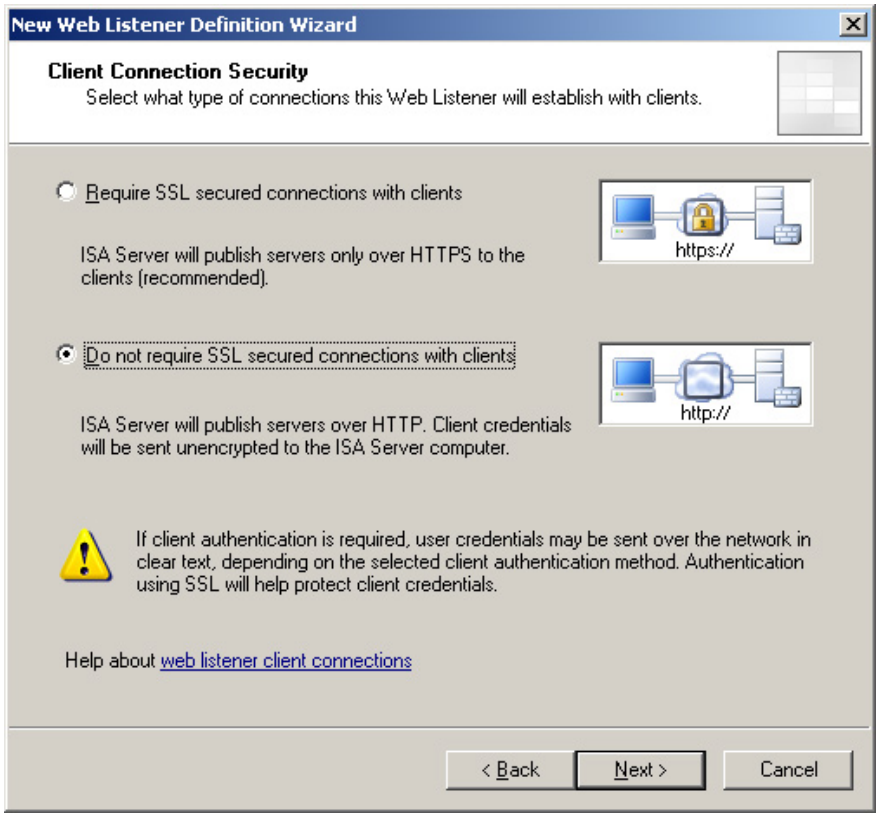

Figure 13: Client Connection Security page of the New Web Listener Definition Wizard.

12. On the **Listener IP Address Website** , select the **Extermal** checkbox. We do not need to select IP addresses because in this example we have only one IP address on the external interface of the ISA Firewall. If the check boxes remain the same in ISA Server, the data sent to the client via this Web Listener will be compressed when the client is requesting this data to select the compression option. Then click **Next** .

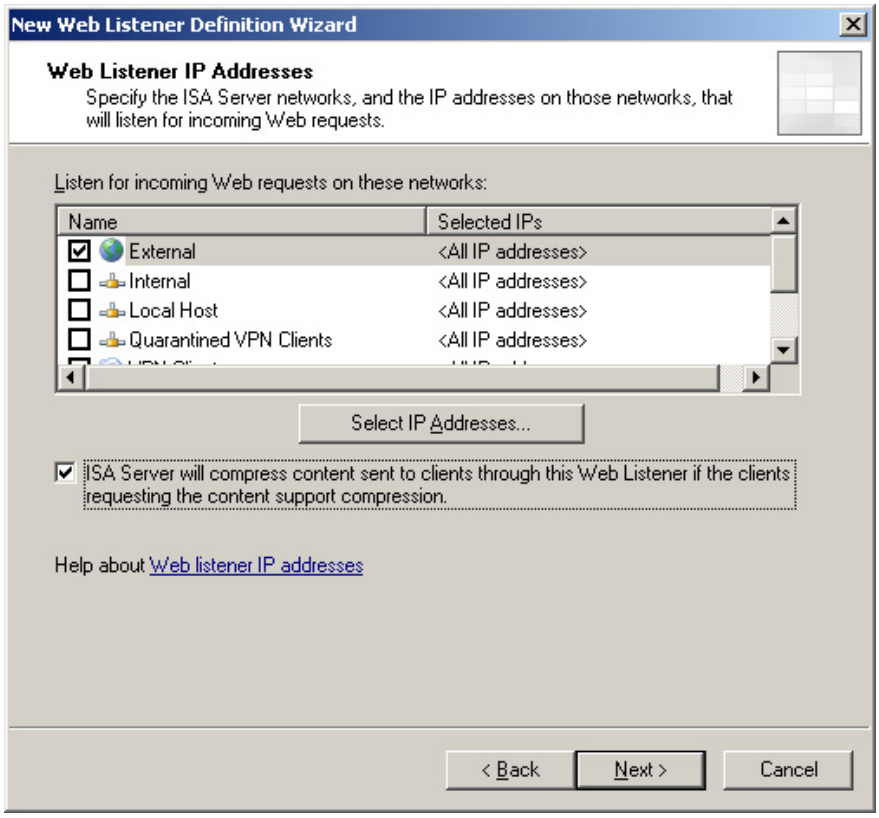

Figure 14: Select the External checkbox on the Listener IP Address Website of the New Web Listener Definition Wizard.

13. On the **Authentication Settings** page, select the **No Authentication** option in the drop-down list **Select how clients will provide credentials to the ISA Server** (select the method of sending the license to ISA Server). This SSTP client cannot authenticate while accessing the CDP, so we must not enable authentication on this Listener. However, we can enable it if we need to use this Listener for other Web Publishing Rules, but we must ensure that all users are allowed to access it in the absence of authentication. Then click **Next** .

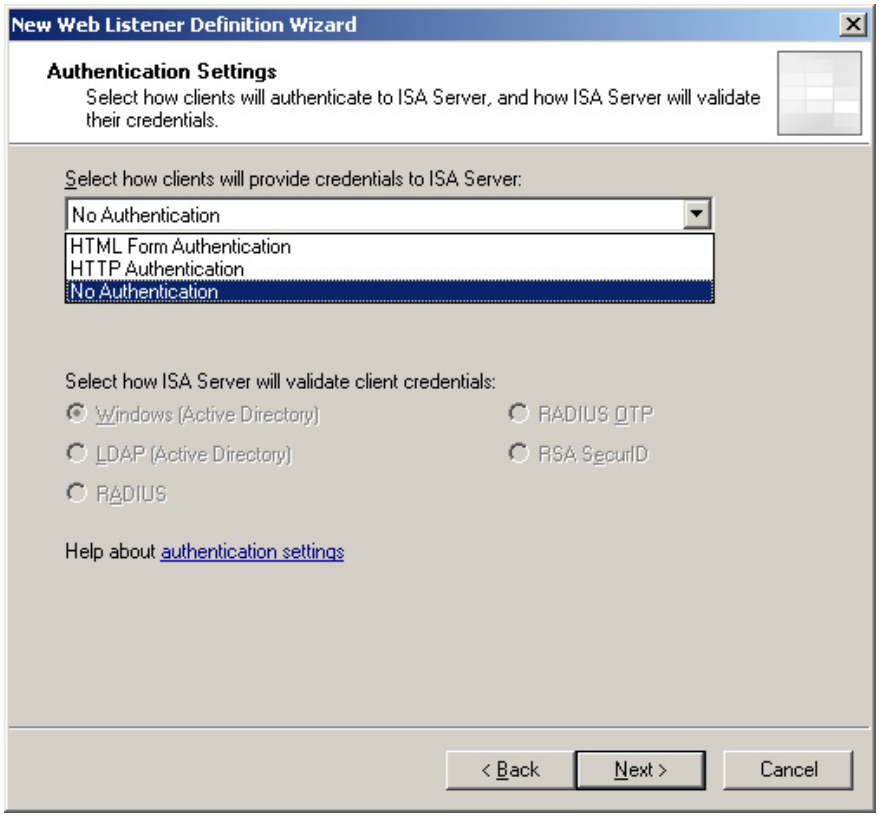

Figure 15: The Authentication Settings page of the New Web Listener Definition Wizard.

14. Click **Next** on the **Single Sign On Settings page** .

15. Click **Finish** on the **Completing the New Web Listener Wizard page** .

16. Click **Next** on the **Select Web Listener** page.

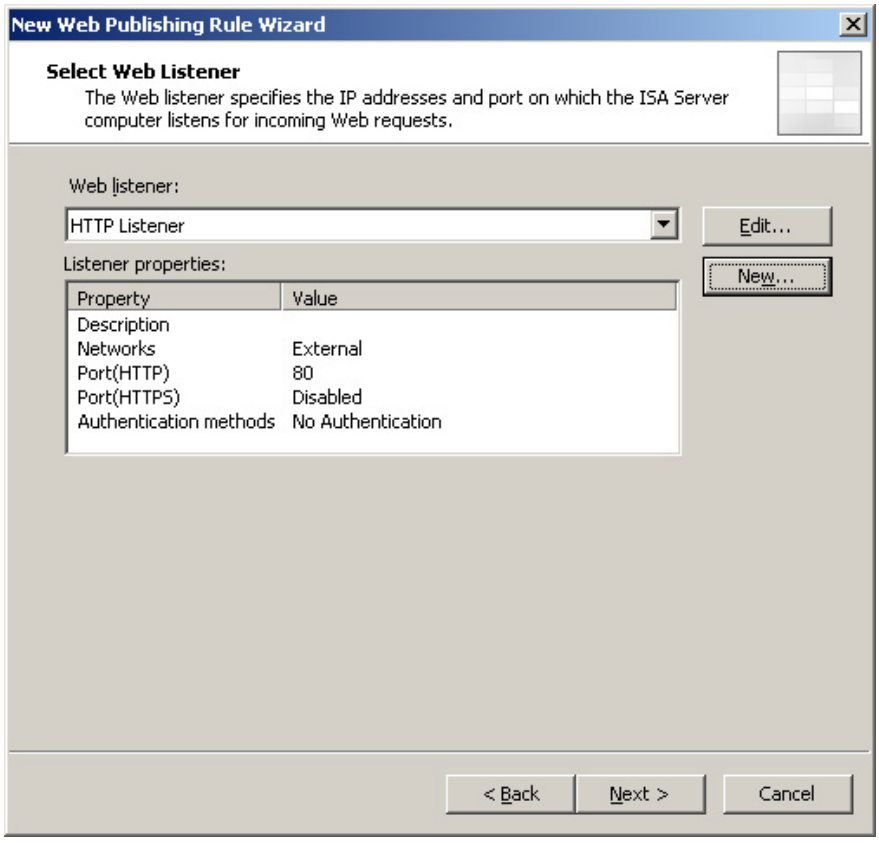

Figure 16: Select Web Listener page of the New Web Publishing Rule Wizard.

17. On the **Authentication Delegation** page, select the option **No delegation, and client cannot authenticate directly** in the drop-down list. Since no authentication process is performed on this connection, we do not need to authorize authentication. Then click **Next** .

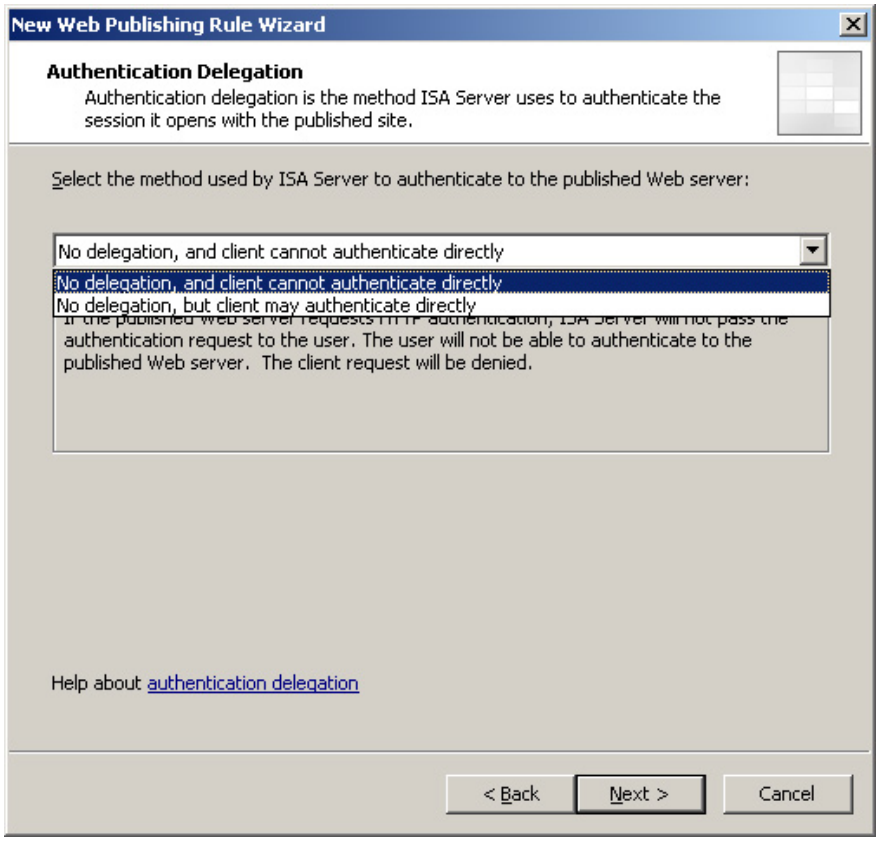

Figure 17: Authentication page of the New Web Publishing Rule Wizard.

18. On the **User Sets** page, keep the default settings. Click **Next** .

19. Click **Finish** on the **Completing the New Web Publishing Rule Wizard page** .

Next, we will create the Server Publishing Rule for the PPTP server:

1. In the **ISA Firewall Console** , click the **Firewall Policy** node. Select the **Tasks** tab in the **Task Pane** and then click **Publish Non-Web Server Protocols** .

2. On the **Welcome to the New Server Publishing Rule Wizard page** , enter a name for this Rule in the **Server Publishing Rule name** box. In this example we will enter the name PPTP VPN. Then click **Next** .

3. On the **Select Server** page, enter the IP address on the external network of this VPN server. In this example, the external interface of the VPN server is *10.10.10.2* , so we will enter this address into the **Server IP address** box and then click **Next** .

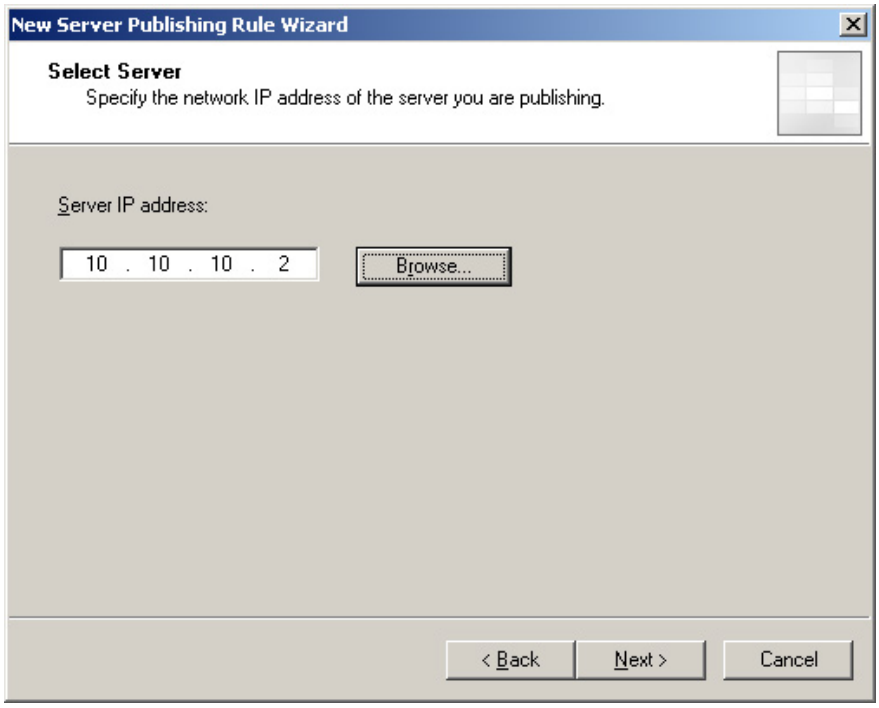

Figure 18: Enter the IP address for the server on the Select Server page.

4. On the **Select Protocol** page, select the **PPTP Server** option in the **Selected protocol** list. Then click **Next** .

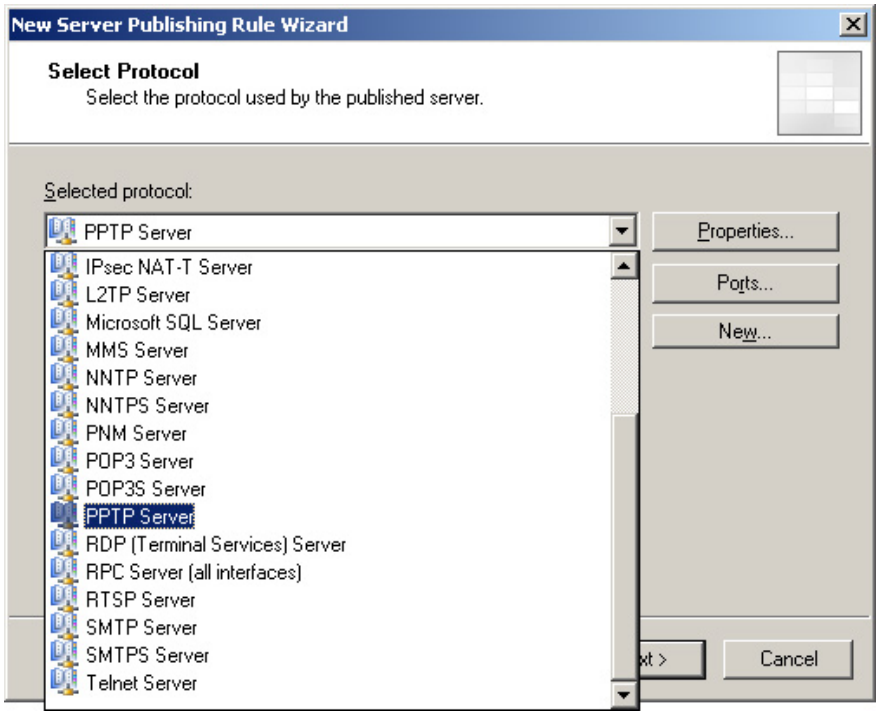

Figure 19: Select the protocol on the Select Protocol page.

5. On the **Network Listener IP Addresses page** , select the **External** checkbox and then click **Next** .

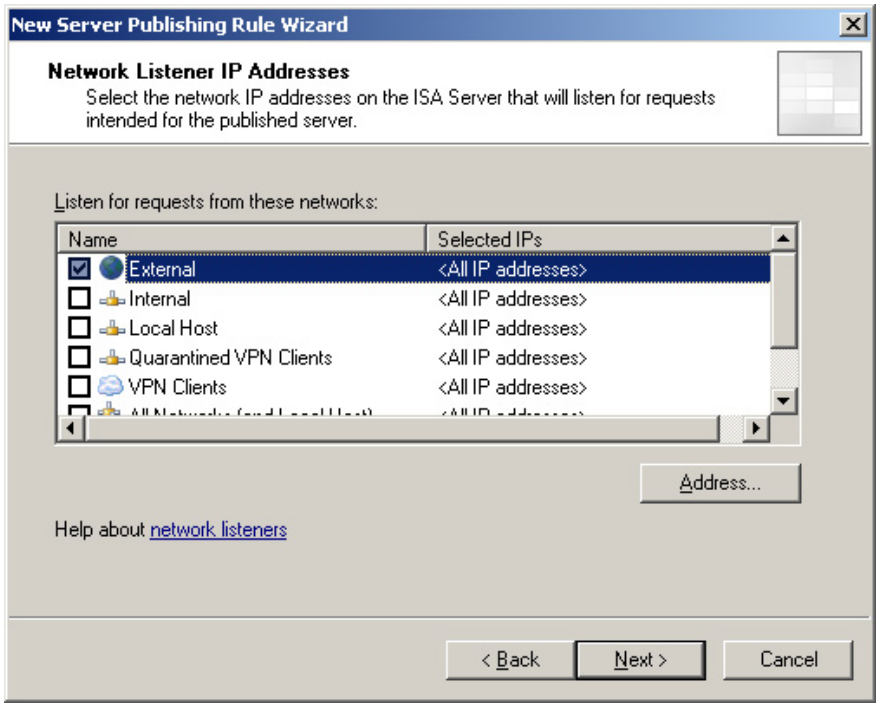

Figure 20: Select the External checkbox on the Network Listener IP Addresses page.

6. Click **Finish** on the **Completing the New Server Publishing Rule Wizard page** .

Here we will complete the Publishing Rule configuration by creating a Server Publishing Rule for the SSTP protocol that is actually an HTTPS Server Publishing Rule:

1. In the **ISA Firewall Console** , click the **Firewall Policy** node in the left **pane** , select the **Tasks** tab in the **Task Pane,** and then click **Publish Non-Web Server** .

2. On the **Welcome to the New Server Publishing Rule Wizard page** , enter a name for the Server Publishing Rule in the **Server Publishing Rule name** box. In this example we will use the *SSTP Server* name. Then click **Next** .

3. On the **Select Server** page, enter the IP address on the external interface of the VPN server in the **Server IP address** box. In this example we enter the address *10.10.10.2* . Then click **Next** .

4. On the **Select Protocol** page, select the **HTTPS Server** option from the **Selected Protocol** list. Then click **Next** .

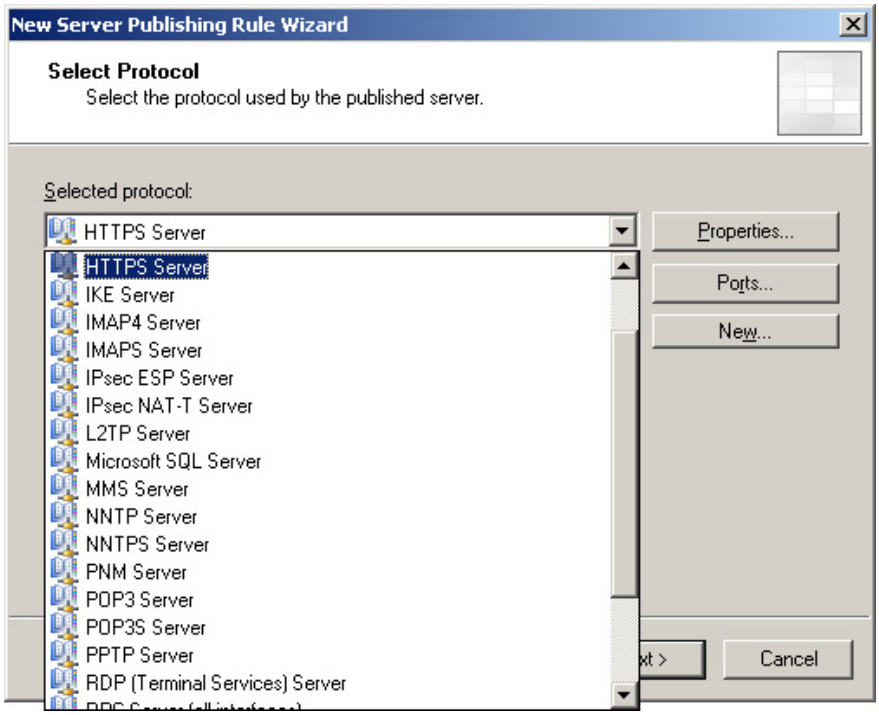

Figure 21: Selected Protocol page of the New Server Publishing Rule Wizard.

5. On the **Network Listener IP Address page** , select the meeting to select **External** and then click **Next** .

6. Click **Finish** on the **Completing the New Server Publishing Rule Wizard page** .

7. Click **Apply** to save the changes and update the Firewall Policy. Click **OK** in the **Saving Configuration Changes** dialog box.

Conclude

In this section, we have configured the dial-in licenses for a user account. We then moved to CDP Web Server so that an anonymous HTTP connection can be made through it. And we create two Server Publishing Rules and a Web Publishing Rule in the ISA Firewall to allow connections to the VPN server and CRL Distribution Point. In the next and final part of this series, we will configure the VPN server to connect to the SSL VPN server and reconfirm those connections by checking the information on this client, the server. VPN and at the ISA Firewall.