Create a Site-to-site VPN on ISA 2006 (Part 4)

In this part 4, we will continue with configuring the main office ISA Firewall in the Remote Site Network, which is used to create the site to site VPN connection between the head office and the branch office. After creating the Remote Site Network, we can use the Answer File Wizard to create the t file

Create a Site-to-site VPN on ISA 2006 (Part 1)
Create a Site-to-site VPN on ISA 2006 (Part 2)
Create a Site-to-site VPN on ISA 2006 (Part 3)

Configure the main office ISA firewall at the main office with the Remote Site Network used in the site to site VPN connection between the head office and the branch office.

In the first three parts of the series using the Branch Office Connectivity Wizard to connect the ISA Firewall between the main office and the branch office, we discussed the network infrastructure for example, going through important concepts in Create site to site virtual private network, configure network services to support and install CSS, main office ISA Firewall, branch office ISA Firewall. At the end of lesson 3 we are stopping when the branch office ISA Firewall is ready to accept the answer file that will be used in the Branch Office Connectivity Wizard.

In this part 4, we will continue with configuring the main office ISA Firewall in the Remote Site Network, which is used to create the site to site VPN connection between the head office and the branch office. After creating the Remote Site Network, we can use the Answer File Wizard to create an answer file that will be used by the Branch Office Connectivity Wizard to create a site to site VPN connection. The Branch Office Connectivity Wizard will also allow you to automatically link the branch office ISA Firewall to the domain, providing the highest level of security and flexibility possible.

Create Remote Site Network for Branch Office connections via site to site virtual private network

Now we need to create the remote class network, initiating the site to site VPN connection from the head office to the branch office. After configuring the site to site virtual private network completely, we can create the answer file and copy it to the root (root) folder on the C: drive of the branch ISA Firewall. The Branch Office Connectivity Wizard will automatically find the answer file to complete the site to site VPN connection configuration.

Follow these steps to create a site to site virtual private network connection from the main office ISA Firewall to the branch office ISA Firewall:

1. On the CSS machine, expand the **Arrays** node, then the **Main** array button. Click on **Virtual Private networks (VPN)** and **Remote Sites** tab between the ISA Firewall console frame and the **Tasks** tab in the

Task Pane. On the Task Pane, click the **Create VPN Site to Site Connection link** .

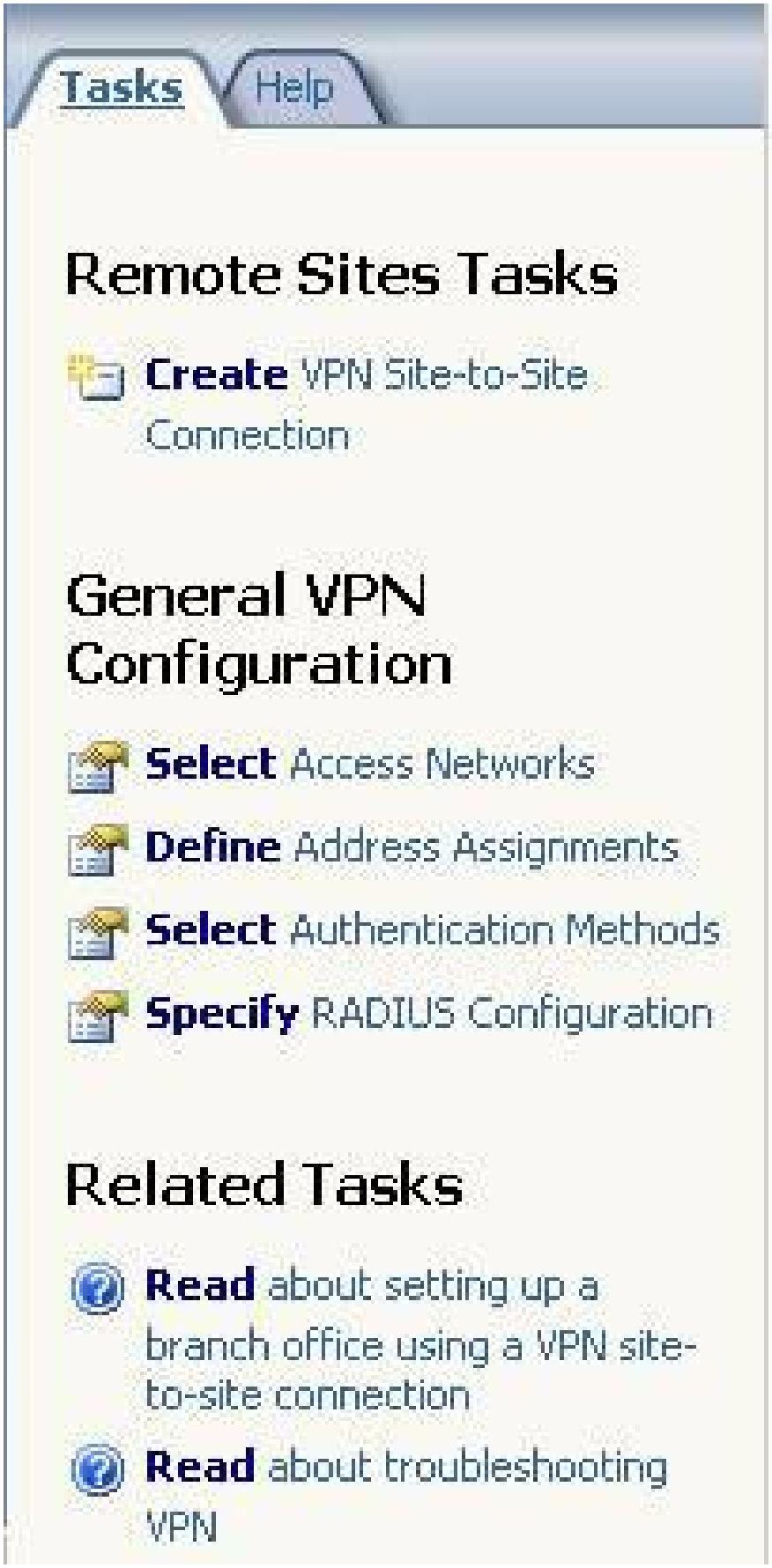
Tasks
Help
Remote Sites Tasks
Create VPN Site-to-Site Connection
General VPN Configuration
Select Access Networks
Define Address Assignments
Select Authentication Methods
Specify RADIUS Configuration
Related Tasks
Read about setting up a branch office using a VPN site-to-site connection
Read about troubleshooting VPN

Figure 1

2. On the **Welcome to the Create** [sic] page, **VPN Site to Site Connection Wizard** , enter the remote class name in the **Site to site network name box** . This is the demand-dial interface name on the ISA Firewall, which will accept the upcoming connection of the branch office ISA Firewall. You need to create user accounts on the machine, with dial-in access rights with the same name. The wizard will notify you to create a user account after completing the installation process. Click **Next** .

Figure 2

3. On the **VPN Protocol** page, select **Layer Two Tunneling Protocol (L2TP) over IPSec** . This option is more suitable for you when connecting two ISA Firewalls in a site to site virtual private network connection. You can only use the Branch Office Connectivity Wizard when you have the ISA Firewall on both sides of the site to site VPN link. And the Branch Office Connectivity Wizard only works when you use the L2TP / IPSec or IPSec tunnel model. The IPSec tunnel should be avoided because it is less secure and has less performance than L2TP / IPSec, since there is no header compression mechanism. If using PPTP as a VPN protocol, the option to create an answer file based on the remote network configuration will not work. Click **Next** .

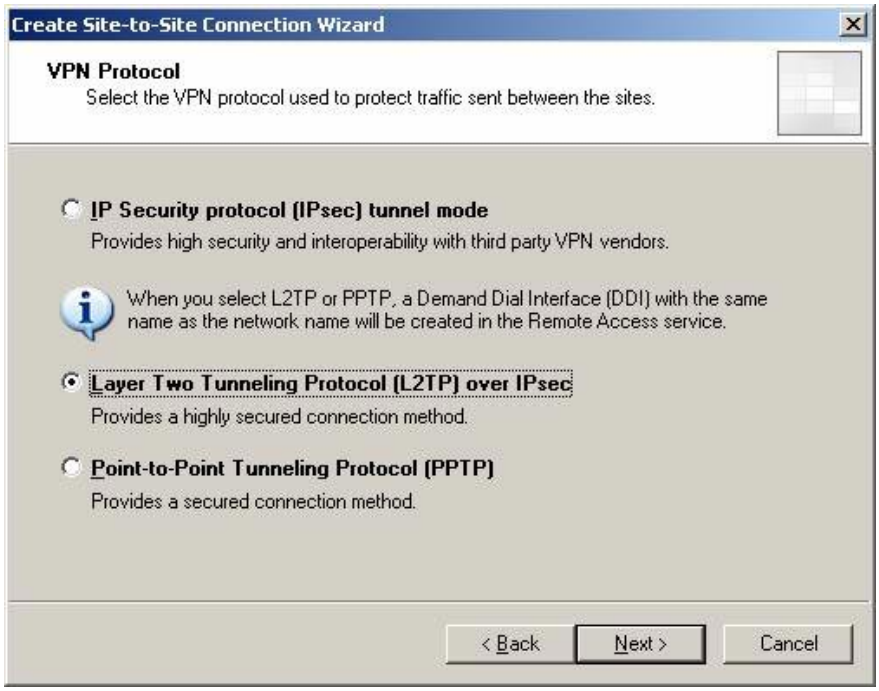

Figure 3

4. A warning dialog box will appear, telling you that you need to create a user account with the same name as the demand-dial interface, which you provide to Remote Site Network from the start of the Wizard. We will create this account at the end of the site to site Remote Site Network virtual private network connection. Click **OK** .

Figure 4

5. On the **Local Network VPN Settings page** , select the method the ISA Firewall will use to assign IP addresses to remote access VPN clients and VPN gateways. In our current example, the main office has a

DHCP server on the subnet. So we will choose **Dynamic Host Configuration Protocol (DHCP)** . Note that DHCP is not supported for multi-member ISA Firewall arrays. Click **Next** .

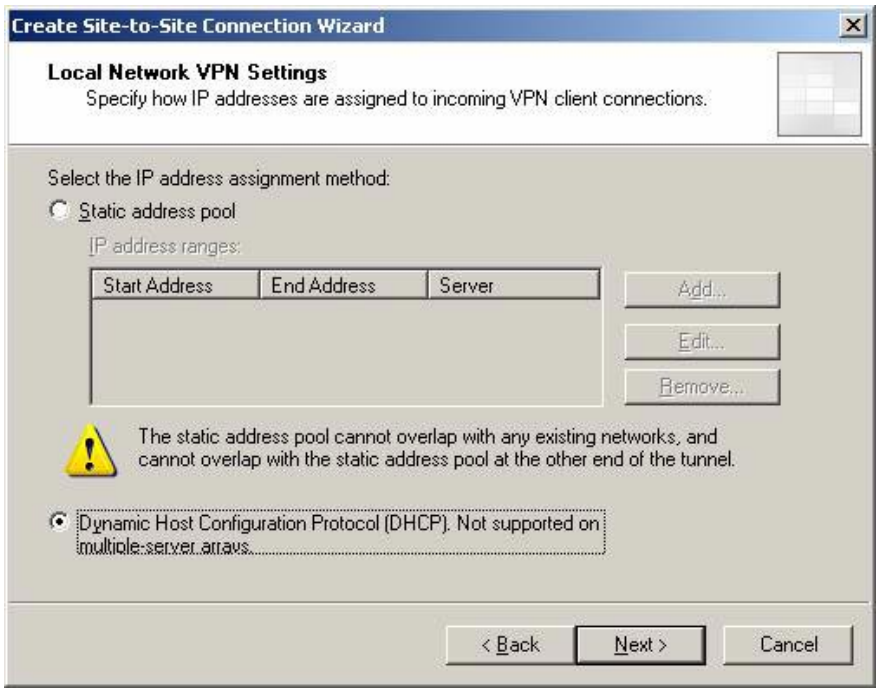

Figure 5

6. Accept the default settings on the connection owner page. Since this is a single member ISA Firewall array, only a single machine can be the owner of the connection. If we have multiple members in this ISA Firewall array, and using NLB then NLB will automatically assign connection ownership to the site to site VPN connection. Click **Next** .

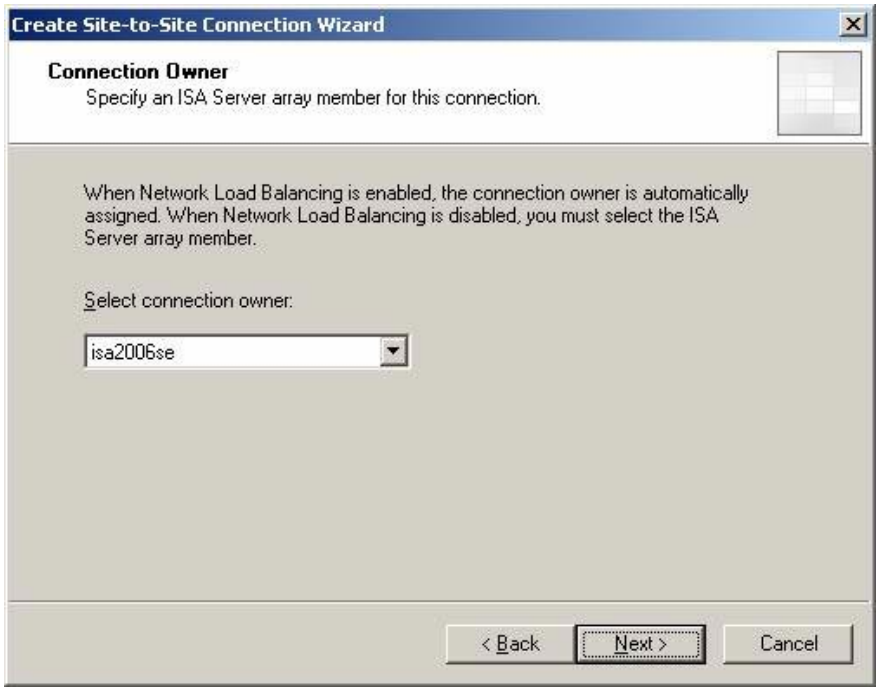

Figure 6

7. On the **Remote Site Gateway** page, you need to enter the FQDN or IP address of the branch ISA Firewall. In this example, the IP address of the branch ISA Firewall is **192.168.1.73** , and enter the box next to it. (Note that this is a private IP address in the lab. In a production environment, of course the ISA Firewall will be on the network and have a normal IP address). Enter the IP address in the **Remote site VPN server box** and click **Next** .

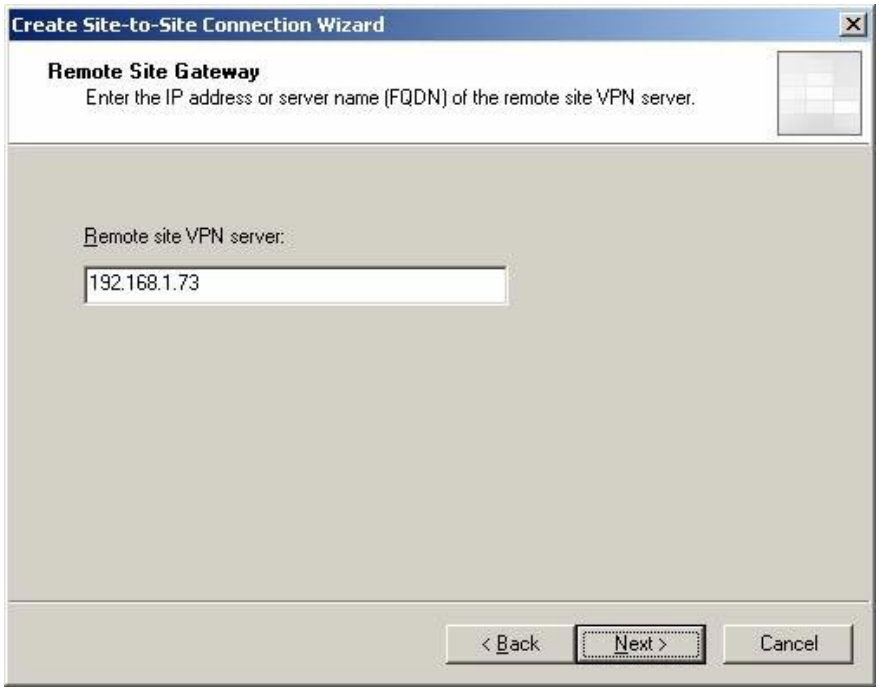

Figure 7

8. On the **Remote Authentication** page, enter the **authentication** information that the main ISA Firewall can use to connect to the branch ISA Firewall in the site to site VPN connection. Put a checkmark in the **Allow the local site** checkbox **to initiate connections to the remote site, using this user account** , then enter the information **User name** , **Domain** , **Password** and **Confirm Password** into the corresponding boxes.

   I prefer to use local accounts on machines rather than domain accounts. In fact, we can use domain accounts in this case, because the branch office ISA Firewall will not become a domain member until the process of creating the site to site VPN connection is set. up. In our case, you will have to create a user account with the name **Main** on the branch ISA Firewall named **ISA2006BRANCH** . This helps explain the information in the picture below. Click Next.

Figure 8

9. On the **L2TP / IPSec Outgoing Authentication page** , select the certificate **authentication** mechanism or the 'pre-shared' key. In a production environment, you should start with the pre-shared key and after everything works as expected, switch to certificate authentication.

Select **Pre-shared key authentication** and enter the key. In this example I used **123** key for simplicity, and in a production environment, you need to use a composite key with more than 14 characters. Click **Next** .

Figure 9

10. On the **Incoming L2TP / IPSec Authentication page** , select the **authentication** method you want the branch office ISA Firewall to use when creating the IPSec connection with the main ISA Firewall. In this example, I will use the same method as on the main office: the pre-shared key with the key value of **123** . Click **Next** .

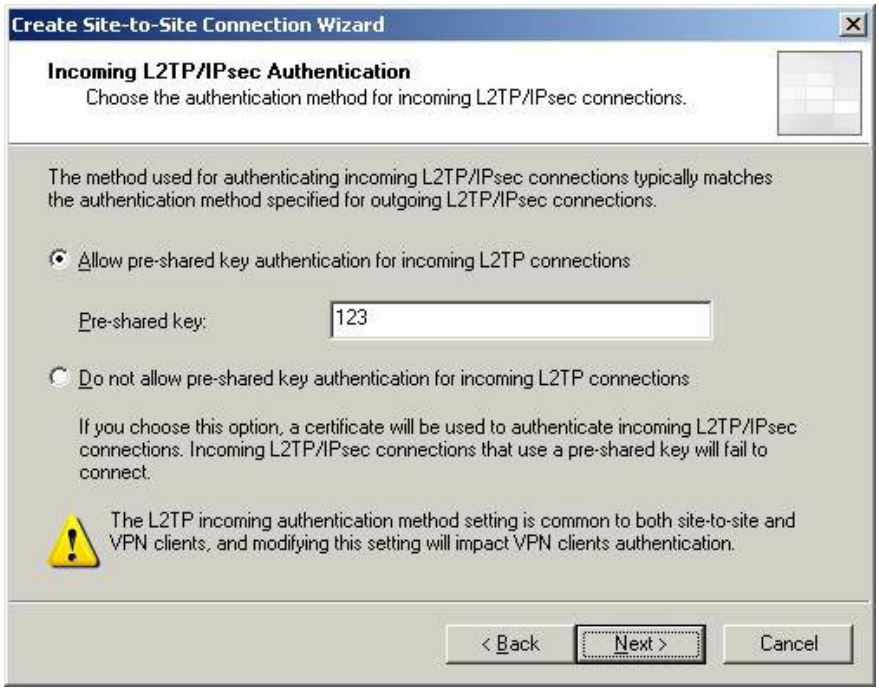

Figure 10

11. On the **Network Addresses** page, you need to enter the IP address limit used on the Remote Site Network. Then click the **Add** button. In the **IP Address Range Properties** dialog box, enter the address limit used on the branch office. In this example, the extensions are located on the network ID **10.0.1.0/24** . Enter **10.0.1.0** in the **Start address** box and **10.0.1.255** in the **End address** box. Click **OK** .

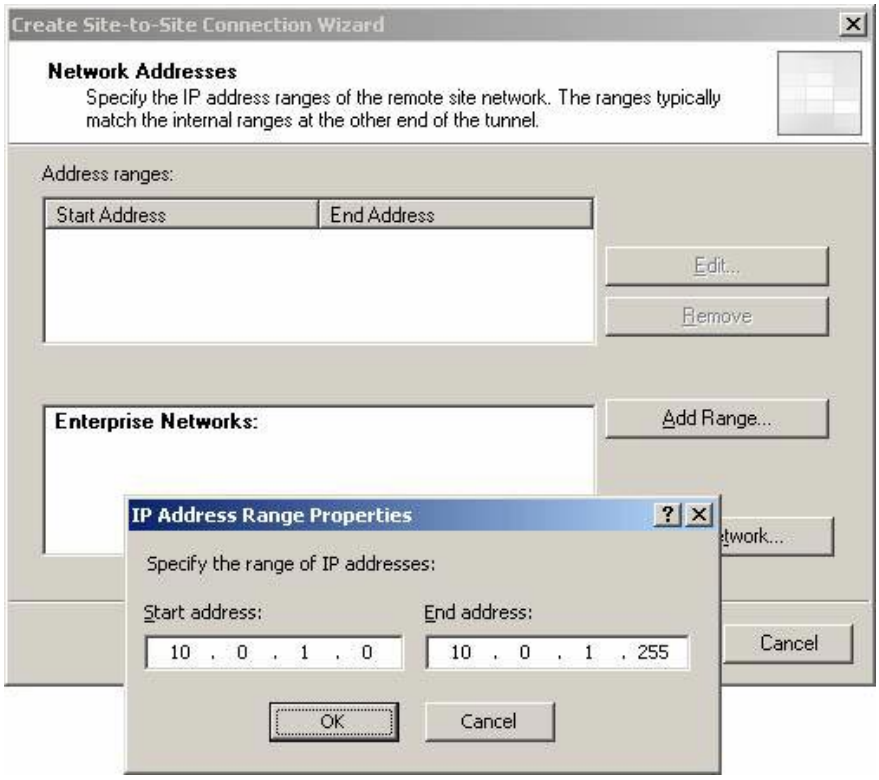

Figure 11

12. The branch address limit appears on the **Network addresses** page. Click **Next** .

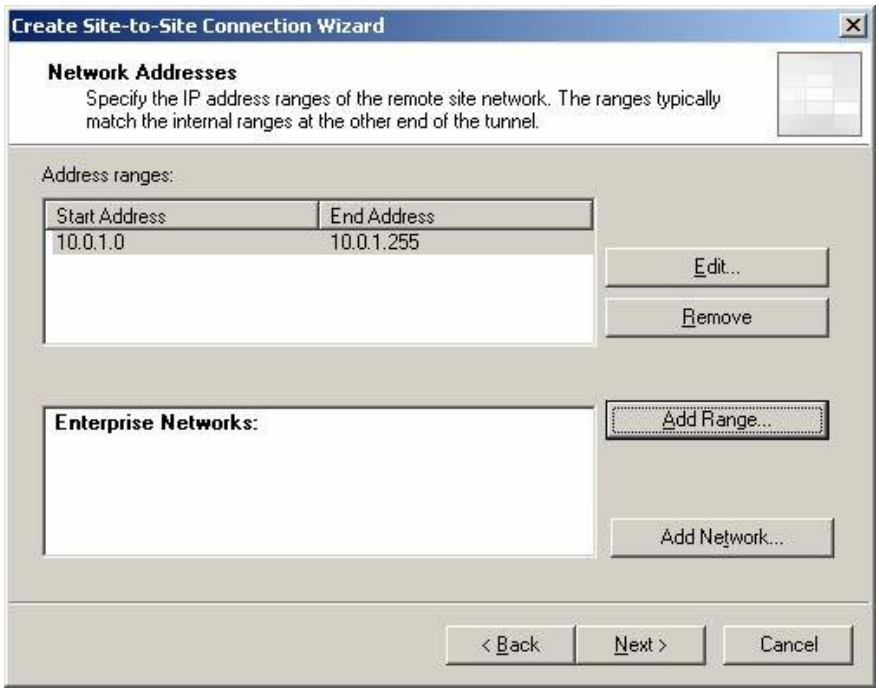

Figure 12

13. On the **Remote NLB** page, uncheck the checkbox in **The remote site is enabled for Network Load Balancing** because we do not use NLB at the branch office. Click **Next** .

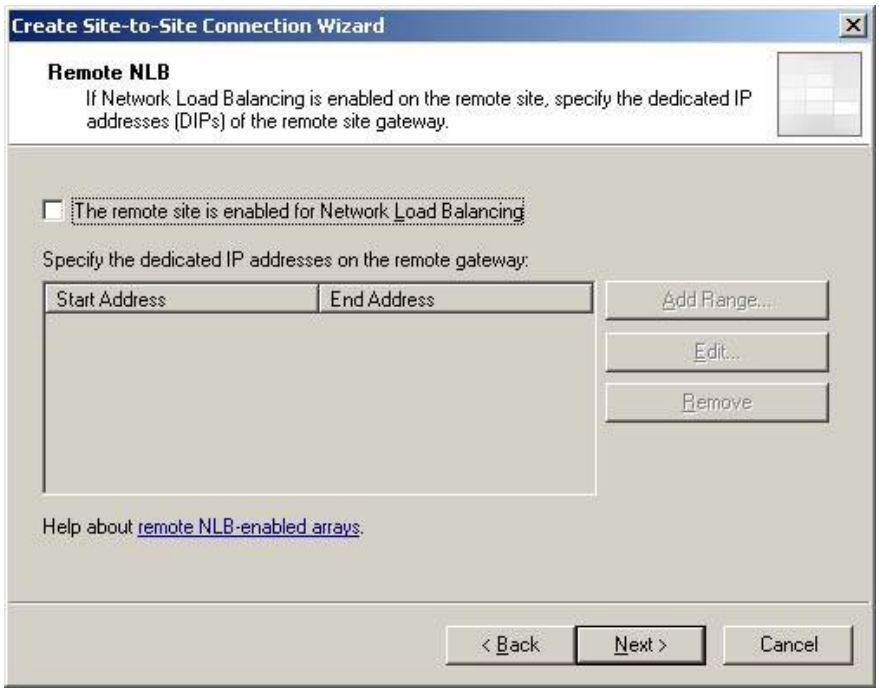

Figure 13

14. On the **Site to Site Network Rule page** , accept the default **Create a network specifying a route relationship option** and the default rule name. Click **Next** .

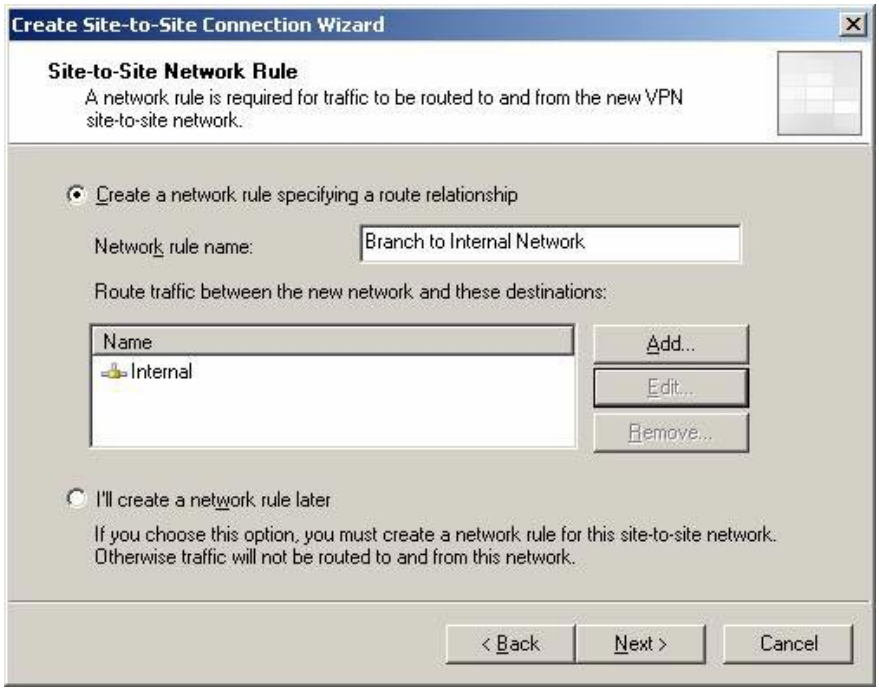

Figure 14

15. On the **Site to Site Network Access Rule page** , you can create an Access Rule that controls the traffic that flows through the site to site virtual private network at the main office ISA Firewall. In this example, we will choose **Create an allow access rule** . Leave the default name for the Access Rule in the **Access Rule name** box. From the **Apply the rule to these protocols list** , select **All outbound traffic** . Later we will lock up some things, but now, at the beginning, you need to make sure whether the site to site VPN settings are successful and whether the branch office ISA Firewall can link to the domain. After the site to site VPN connection is established, we will lock some functions to access the appropriate intradomain (internal) contacts and to gain server access. Click **Next** .

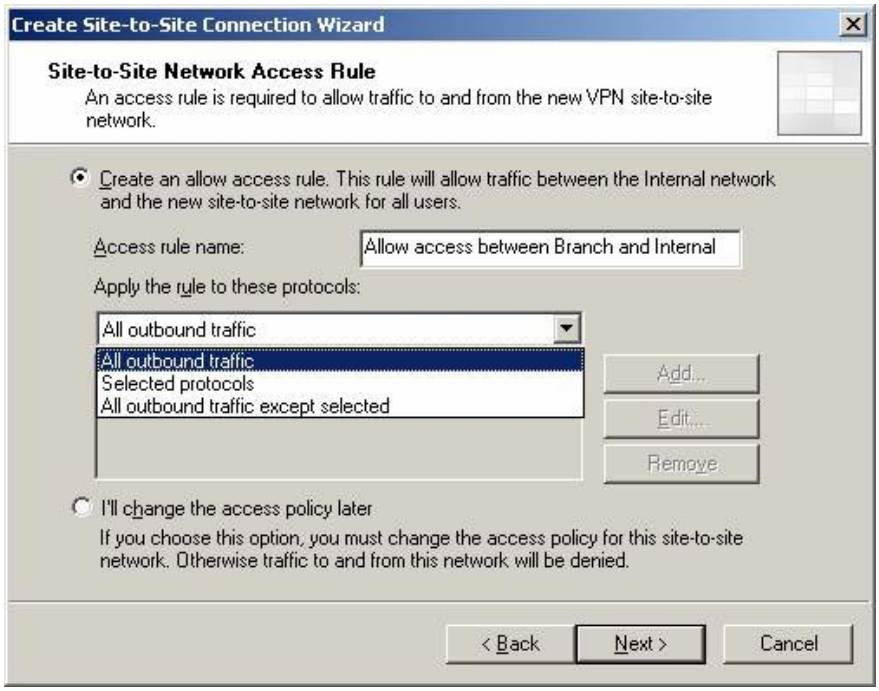

Figure 15

16. On the **Completing the New VPN Site to Site Network Wizard page** , click **Finish** .

Figure 16

17. **Remaining VPN** Dialog **Site to Site Tasks** notifies you that you need to create a user account on the host ISA Firewall so that the branch office ISA Firewall can be used to authenticate the site to site VPN connection. Click **OK** .

Figure 17

18. Click **Apply** to record all changes and update the firewall policy. Click OK in the **Apply New Configuration** dialog box.

19. Click on the **Branch** information in the class list of site to site VPN connections and **Tasks** tab. Note, in the **Related Tasks** list there is a new option: **Create Answer File for Remote VPN Site** . This option will be applied after creating a remote site to site VPN and will only work in ISA 2006 Enterprise Edition. If you use ISA 2006 Standard Edition, you will have to do all this yourself, without any 'benefit' or answer files supported.


Tasks
Help
Remote Sites Tasks
Create VPN Site-to-Site Connection
Edit Selected Network
Delete Selected Network
Disable Selected Network
View Settings Summary
General VPN Configuration
Select Access Networks
Define Address Assignments
Select Authentication Methods
Specify RADIUS Configuration
Related Tasks
Monitor Site Sessions
Read about setting up a branch office using a VPN site-

Figure 18

Now we need to do the configuration task: create the user account the branch ISA Firewall will use to authenticate the main ISA Firewall. Follow these steps on the main office ISA Firewall computer (NOT CSS) to create user accounts and complete the configuration:

1. Right-click **My Computer** and select the **Manage** command.

Figure 19

2. In the **Computer Management** console, expand the **System Tools** button, then the **Local Users and Groups** button. Right-click on an empty location in the right pane and click the **New User** command.

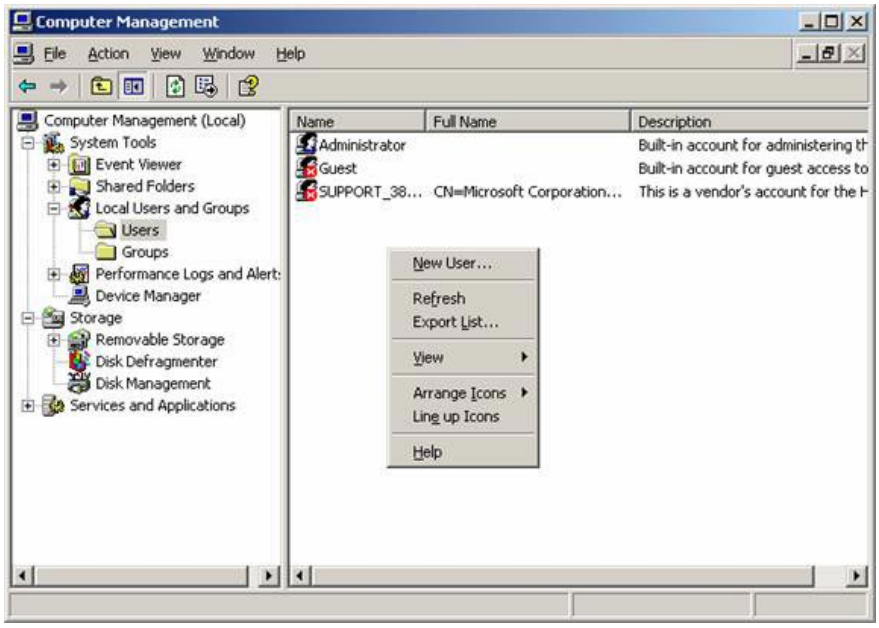

Figure 20

3. In the **New User** dialog box, enter **Branch** in the **User name** box. This is an extremely important setting, because the user's name must be the same as the name assigned in the demand dial interface on the main ISA Firewall connected to the branch ISA Firewall. Enter the password and verify the password. Uncheck the **User must change password at next logon box** and check for **User cannot change password** and **Password next expires** . Click **Create** .

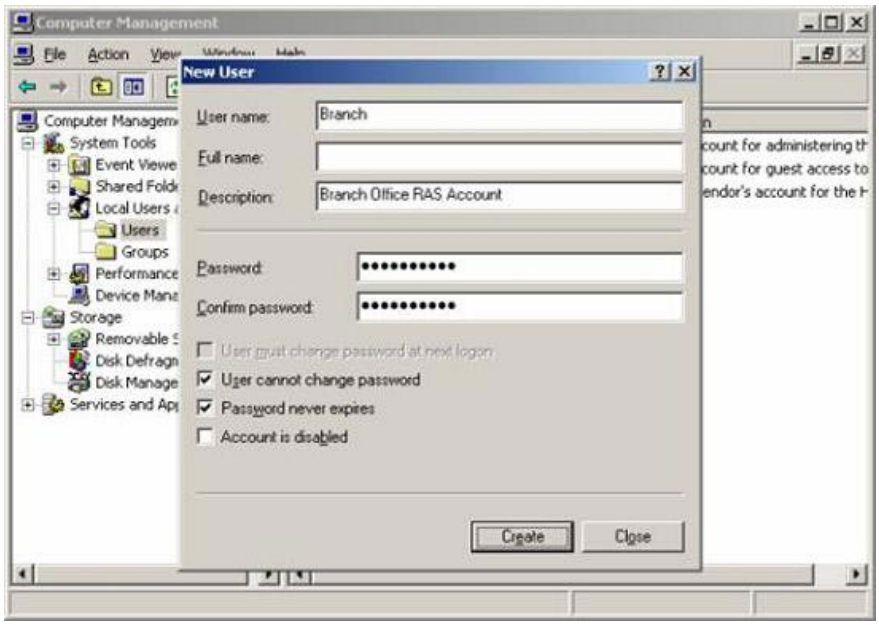

Figure 21

4. Click **Close** in the **New User** dialog box.

5. Double-click the **Branch** user, the **Branch Properties** dialog box appears.

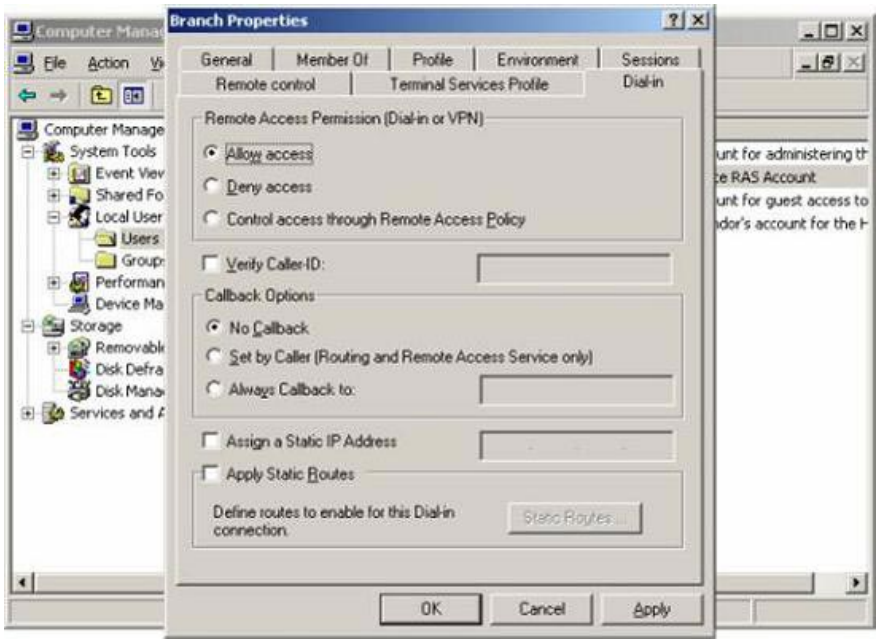

Figure 22

6. Close the **Computer Management** console.

7. Restart the ISA Firewall machine.

Summary

Part four of the site to site VPN virtualization series uses this Branch Office Connect Wizard, we have reviewed the procedures needed to create the Remote Site Network. We have also created a user account at the main office server that the branch office ISA Firewall will use to establish a site to site connection from the branch office to the main office. In the next part of this series, we will join the site to site VPN Program Answer File Wizard to create the answer file transmitted to the branch ISA Firewall.

Create a Site-to-site VPN on ISA 2006 (Part 5)