CHAPTER 7

Routing and Remote Access Service, VPN, and Firewalls

IN THIS CHAPTER

- Routing and Remote Access Service Basics
- Using the RRAS Firewall
- Remote Access Basics
- Configuring Remote Access
- Troubleshooting Routing and Remote Access Issues

The Routing and Remote Access service (RRAS) is a vital component of Small Business Server 2003. The role of this service has been expanded from previous versions to provide new functionality that greatly improves security. Also, new wizards are available to automatically configure many aspects of remote access. These improvements are not limited only to the server portion but also to the client configuration as well.

In this chapter you learn the fundamentals of the RRAS along with examples on how to configure the most common options. Also, detailed information on accessing your server remotely is presented to give you some insight on the different methods available and when to use them.

Routing and Remote Access Service Basics

RRAS provides many essential services to your SBS network. However, many of its functions are determined by the way your server and network are configured.

The four major functions of RRAS are to provide the following services:

- Basic firewall
- Network address translation routing
- Remote access via dial-up
- Remote access via VPN

In SBS 2003 Standard Edition all these functions are handled by RRAS. If you have ISA Server 2004 installed (as part of SBS 2003 Premium Edition), the first two functions are taken over by ISA Server.

If you have ISA Server 2004 installed, you can skip the following sections up to the "Remote Access Basics" section because they do not apply to you. See Chapter 23, "Internet Security and Acceleration Server 2004 Basics," for information on configuring ISA Server as your firewall.

Using the RRAS Firewall

If you already ran the Configure Email and Internet Connection Wizard (CEICW) it is likely that you have configured the built-in firewall without much effort (or maybe without even knowing). Because the process is relatively simple, this chapter focuses on detailing the particulars of this service and providing in-depth information about certain common features.

Let's start by describing the main function of a firewall. The job of any firewall is to separate your internal (trusted) network from an external (not trusted) network, such as the Internet. This is an important function because it reduces the surface attack area of your network by exposing only those services that need to be accessed from outside.

For a firewall to be effective, both networks must be physically separated. Hence, one of the requirements to use RRAS as a firewall is that you must have two network cards. One card is connected to the local network, and the other card is connected to the Internet side, as shown in Figure 7.1.

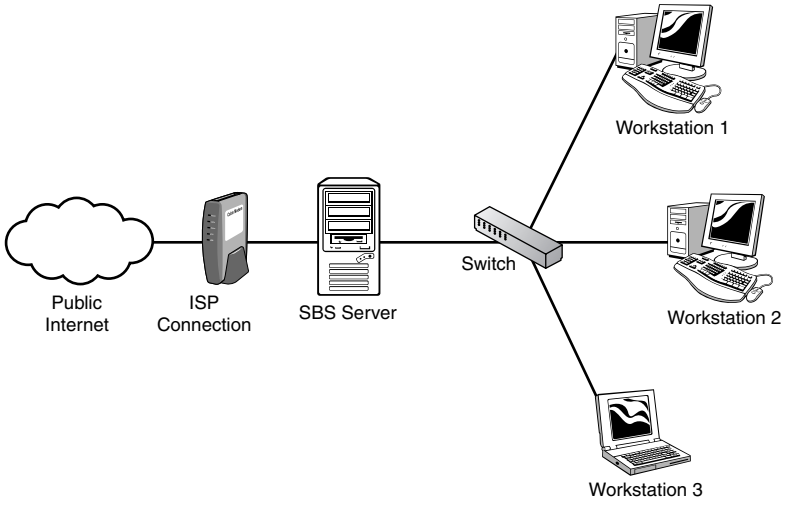

FIGURE 7.1 Network diagram of a typical installation using SBS as the firewall.

RRAS acts as a basic firewall because it can filter traffic only at the network layer (based the properties of the IP packet). Although it is not as fancy as ISA Server 2004, you still can protect your network effectively by restricting access not only by port number but also by source or destination address among other things.

Remember that although firewalls are important, they are not the be-all and end-all of network security. There are ways around firewalls (such as VPNs), and there is always the potential for having a vulnerable service behind an open port. Also, keep in mind that an improperly configured firewall can create a false sense of security.

Best Practice—Use ISA 2004 If You Have SBS 2003 Premium

If you already own the SBS 2003 Premium Edition, it is strongly suggested that you install ISA Server 2004. Not only does it provide a much more sophisticated firewall than RRAS, you also get more detailed reports and more control over what your users can access.

CEICW and the RRAS Firewall

Although CEICW takes care of most of the firewall configuration, you might be wondering exactly what it does. Understanding why and how ports are opened by the wizard is an important step toward improving your network security.

Table 7.1 lists the most common ports used in a typical SBS installation. By default, eight ports (marked with an asterisk) can be opened by the CEICW. Also, you can manually add other ports if you deem it necessary.

TABLE 7.1 TCP Ports Used in a Typical SBS 2003 Installation

TCP Port	Service	Description
21*	FTP	Enables the external file transfer
25*	SMTP	Enables incoming SMTP mail in Exchange
80*	IIS	Enables all nonsecure browser access, including: IIS websites and HTTPS redirectors
110	POP3	Enables external access to Exchange POP3 server
143	IMAP4	Enables external access to Exchange IMAP4 server
443*	IIS	Enables all secure browser access, including OWA, OMA, RWW, and RPC over HTTP
444*	Windows SharePoint Services	Enables external access to the SharePoint (Companyweb) website.
1723*	PPTP clients	Enables external PPTP VPN connections
3389*	Terminal Services	Enables access to Terminal Services using the Remote Desktop protocol
4125*	Remote Web Workplace	Enables Remote Desktop Connection via the Remote Web Workplace interface

**Denotes a port defined in the CEICW by default.*

Which ports are opened by the CEICW depends on the choices you make running it. For example, TCP port 444 will be opened only if you select Windows SharePoint Services Intranet Site on the Web Services Configuration screen.

Best Practice—Open Ports Only as Needed

Only open ports that are really necessary; opening ports that are not required can put your network at risk.

For example, if you use the POP3 Connector to retrieve email, allowing inbound SMTP access is not necessary. Unselect E-mail from the Services Configuration screen in CEICW to close it.

One nice feature of configuring your firewall using the CEICW is that if you have a hardware router/firewall installed on your network it can be automatically configured. If the device supports Universal Plug and Play (UPnP) the CEICW will not only open the ports on the RRAS firewall but also will open/forward the appropriate ports on the device. This eliminates much of the guesswork when manually configuring the hardware firewall.

Configuring the RRAS Firewall

As previously mentioned, the CEICW configures most basic functions of the RRAS firewall. However, there are a couple of things that you might want to do that are not directly configurable using the wizard. This section presents an overview of three common scenarios for configuring the firewall in an SBS network.

Creating a Packet Filter

At some point you might need to open an uncommon port to remotely access a service that resides on the server. For example, you might have a handheld device that needs IMAP4 or POP3 access to your mailbox in Exchange. Although opening another port in not really a best practice, sometimes you don't have a choice (although in this case you might want to consider buying a device that supports Exchange ActiveSync).

To create a packet filter to allow IMAP4 access (port TCP 143) through the RRAS firewall, follow these steps. These steps assume that the CEICW has been already run at least once.

1. Open the Server Management Console. On the left pane expand Standard Management and then select To Do List. Under Network Tasks and click on Connect to the Internet to open the Configure Email and Internet Connection Wizard.
2. On the welcome screen click Next. Assuming that you have already run CEICW previously, select Do Not Change Connection Type on the next screen and click Next.
3. Select Enable Firewall and click Next. On the Services Configuration Screen (see Figure 7.2) select all the services that you want to enable.

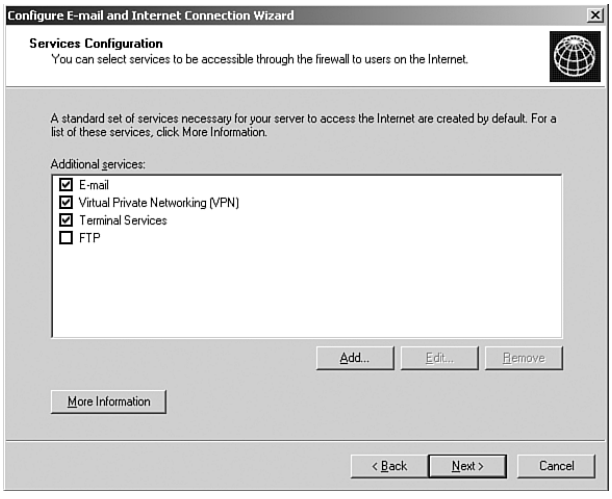

FIGURE 7.2 Services Configuration screen in the Configure Email and Internet Connection Wizard.

4. Click Add to create a new service. On the Add or Edit a Service screen (see Figure 7.3), enter **IMAP** as the service name, select TCP for the protocol, and enter **143** for the port number. Click OK to add the service and make sure that the check box next to the new service is selected. Click Next.

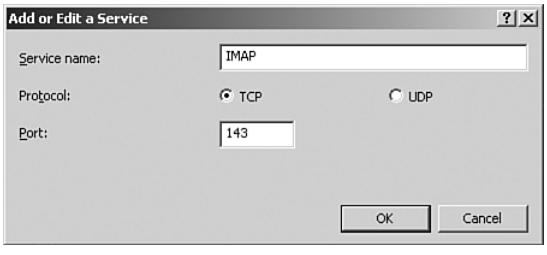

FIGURE 7.3 Add or Edit a Service screen in the Configure Email and Internet Connection Wizard.

5. Finish the wizard by clicking Next on the following screens and selecting Do Not Change Current Web Server Certificate and Do Not Change Internet E-Mail Configuration.
6. Optional: If you have a firewall in front of SBS that supports Universal Plug and Play (UPnP), the wizard attempts to configure it automatically. However, if your firewall does not support UPnP or it's disabled, you need to forward port 143 manually. Consult your router/firewall user guide for further instructions.

If the Microsoft Exchange IMAP4 service is running (which is disabled by default), you should be able to access the service externally.

Packet Forwarding to Another Device

There are cases where you need to allow access to an internal resource not allocated on the server. For example, you might have a web cam running on your network that you want to access remotely. For the purpose of this example, assume that the camera can be accessed via TCP port 8080.

The following steps outline how to forward a port from the external interface of your SBS box to a device located on the internal network:

1. Before configuring the port forwarding, make sure that the target device has a static IP assigned or a DHCP reservation.
2. Open the Routing and Remote Access console in Administrative Tools. Click on your server name to expand it and drill down to IP Routing, NAT/Basic Firewall. On the right pane right-click on Network Connection and select Properties.
3. On the Network Connection Properties screen click on the Services and Ports tab. Click on Add to bring up the Add Service Screen (see Figure 7.4). Type **`Webcam`** in the Description of Service box and select the TCP protocol. Enter **`8080`** as the Incoming and Outgoing Port and type the static IP of the device on the Private Address box. Click OK to save the changes and click OK again to close the Network Connection Properties.

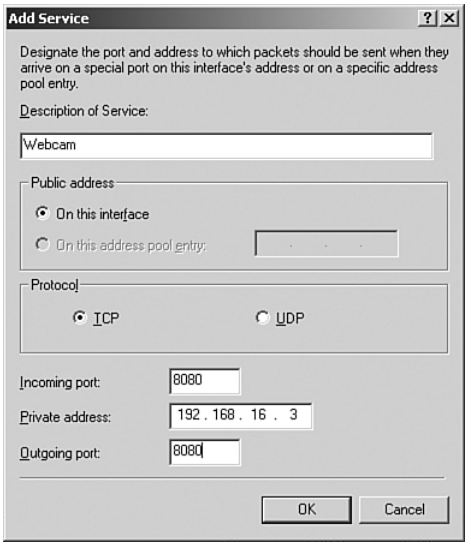

FIGURE 7.4 Add Service Screen on the Network Connection Properties of the RRAS Firewall

4. Optional: If you have a firewall in front of SBS you will need to forward port 8080 manually (even if your router is UPnP capable). Consult your router/firewall user guide for further instructions.

You should be able to access the webcam remotely by using the public IP of your server.

NOTE

One interesting feature that the RRAS firewall provides is port address translation. In other words, you can redirect traffic from one port on the external interface to another port on the target.

This is particularly useful for companies that have a single static IP. For example, assume that you have a Terminal Server alongside an SBS box, and you need to be able to access them both using RDP directly. You could change the listening port number on one of the servers, but that would prevent using Remote Web Workplace (RWW) to access it. A better alternative would be to leave both at 3389, but create forward port 3390 on the external interface and translate it to 3389 on the internal network. RWW keeps working, you have direct RDP access, and everybody is happy!

Filtering Connections

In some circumstances you might want to block certain IPs from reaching your server. For example, if you have seen numerous wrong password attempts from a specific IP, it might be wise to prevent it from even knocking at your door. Another use would be to block SMTP traffic (TCP port 25) from a specific IP address to curb spam.

With RRAS you can filter connections based on the source or destination IP address, port number, and protocol. The following steps outline the procedure to block a specific IP address from connecting to the server:

1. Open the Routing and Remote Access console in Administrative Tools. Click on your server name to expand it and drill down to IP Routing, NAT/Basic Firewall. On the right pane right-click on Network Connection and select Properties.
2. On the Network Connection Properties screen, click on Inbound Filters. Click on New to open the Add IP Filter screen (see Figure 7.5). Select the source network and on the IP address box type the address of the offending machine. For the subnet mask you can either specify a range of machines or, if you just want to block a single IP, type **`255.255.255.255`**. Click OK three times.

After completing the procedure the offending machine should be blocked at the firewall from attempting to contact your server. If you feel adventurous, you might want to play with those settings to restrict traffic based on the protocol and port number.

Best Practice—Regularly Test Your Firewall

Every once in a while get a port scanner and scan the external interface of your server. Make sure that every port you see open is supposed to be that way.

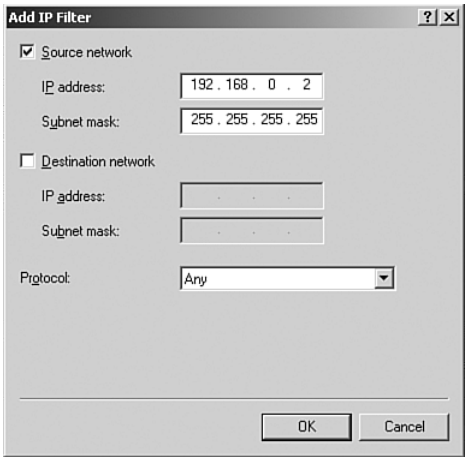

FIGURE 7.5 Add IP Filter screen on the Network Connection Properties of the RRAS firewall.

Remote Access Basics

There are many ways to access your server remotely. Although this section focuses on remote access using virtual private networks (VPNs) or dial-up, other remote access options are mentioned to compare them in terms of functionality and ease of use.

If you were to take a poll asking users what they like most about SBS, you would find that the ability to work remotely ranks high. Being able to read your mail and access files—or even your computer—from anywhere has become a necessity in today's business world, and it's one of the major reasons why people choose SBS.

Fortunately, remote access in SBS 2003 has improved significantly over previous versions. Not only it is easier to configure, but SBS also has a wide array of options to connect remotely in specific scenarios. Thanks to these improvements working remotely is more feasible than ever before, not to mention more secure.

Remote Access Options

Although working remotely can be a blessing, it can also become a nightmare (and I'm not talking about working at home at 2:00 a.m.!). SBS does a great job protecting your network, but enabling remote access is always a risk. On the other hand, this risk can be minimized by carefully considering all your remote access options and following the security best practices such as enforcing complex passwords and changing them frequently.

This discussion begins by addressing the following questions:

- What can you do with dial-up or VPN access?
- Is VPN or dial-up access necessary?
- When should you use VPN versus dial-up?

- How does VPN compare with other remote access alternatives?
- Which users need VPN or dial-up access?

Dial-up remote access is similar to accessing the Internet through a dial-up account. You connect to the server using a modem directly through a phone line. One of the main advantages of this is that you can access the network remotely even in the event of an Internet outage. The main disadvantage is speed; in most cases, the maximum speed attainable is 33.6 kbps, which is very slow. Another disadvantage is that you must have a line dedicated (at least partially) for this kind of access. Having said that, a dial-up connection will behave as part of your internal network (albeit much slower). In fact, you can even use it to connect to the Internet through your own server.

Virtual private networks on the other hand use a public network infrastructure (such as the Internet) to create a private link between two networks or computers. In other words, when you establish a VPN you are creating a secure tunnel between your computer and the remote network that goes through the Internet.

Not only can you access all the resources of the network as if your computer was physically connected to it, but traffic is encrypted in both directions while it travels the public network. When you connect to the VPN you can potentially do everything a local user would do (although it will be slower).

Best Practice—Enable Password Policies

Weak passwords and remote access do not mix. Enforcing a strong password policy is essential to keeping your data secure. Teach your users how to create pass phrases that are easier to remember and difficult to crack, and have your users change them regularly.

Risks of Using VPNs

VPNs are powerful, but they also present certain risks. Because VPN traffic is trusted, it effectively bypasses the firewall. This means that if you connect through VPN to a computer that has been infected with a virus or worm, you can potentially compromise the whole network because the virus/worm has unrestricted access to it. Also, if a hacker were to obtain access to the VPN, he would have access to the network, not just to a particular machine or service.

One of the main concepts in securing your network is to always give users the minimum access necessary to do their jobs. In that spirit the first thing you should evaluate is whether giving them VPN or dial-up access is required.

Best Practice—VPNs Are Not a Panacea

Although SBS makes VPNs easy, the truth is that they can be dangerous in the wrong hands. With so many options for remote access available in SBS, using VPNs is no longer a requirement. If a user only needs email access, it would be foolish to use VPN for that purpose.

Alternatives to VPNs

In the past VPNs were essential to work remotely. However, many new features in SBS 2003 make VPNs unnecessary in many cases. Table 7.2 shows several alternatives to VPNs for accomplishing certain tasks.

TABLE 7.2 Alternatives to Using VPN for Certain Activities

Activity	Alternative
Read email	Outlook Web Access—Access your email using a web browser.
	Outlook with RPC over HTTP—All the functionality of Outlook but remotely.
Connect to computers remotely	Remote Web Workplace—To connect to any workstation or server on your network.
Access files on the road	SharePoint—For files that need to be shared among several users either locally or remotely.
	Offline files—For files that are not being shared among users and that need to be available even when the network is not available.
	Remote Web Workplace—It can also be used to transfer files (if enabled).

In many cases using these alternatives can provide a better end-user experience. Also, from a practical standpoint using alternative methods can sometimes be the only way to access resources remotely because some providers may block VPN traffic while still allowing other (more common) protocols.

Guidelines for Using VPNs

From the previous discussion it becomes clear that VPNs are not for everyone. The question remains how to decide when the use of a VPN is really warranted. This section addresses these concerns by examining some common usage scenarios.

For administrative purposes VPNs can be really useful. The ability to see the whole network at once can be helpful for domain administrators to help diagnose and solve problems that involve several machines. Additionally, administrators are generally tech-savvy and take better care of their machines than regular users. Considering all this, granting administrators VPN access has many advantages and an acceptable risk level.

VPNs can also be helpful for users running an application locally that requires connecting to a resource in your network that is not available from the outside. For example, a user might need to connect to a database remotely. Setting VPN access for such users, where they can access the resource as required is a good idea.

Another example worth mentioning is printing to the SBS shared fax printer while you are on the road. You can potentially send faxes from anywhere in the world that has Internet access.

Best Practice—Practicing Safe VPN

Never establish a VPN from a computer not under your control (such as at an Internet Café). You will be giving that computer unrestricted access to your whole network and placing your network at risk.

Even allowing users to connect from their shared home PC is not a great idea because you don't have control of how well-kept those machines are. However, you can try to minimize that risk by implementing Network Quarantine Control. Use the following link to learn more about it:
`http://www.microsoft.com/windowsserver2003/techinfo/overview/quarantine.mspx`

Configuring Remote Access

Configuring remote access using dial-up or VPN could not be easier with SBS 2003. As usual the built-in wizards take care of most of the heavy work, and they even take care of configuring the workstations.

Configuring the Server

The following steps outline how to run the Remote Access Wizard:

1. Open the Server Management Console. On the left pane expand Standard Management and then select To Do List. Under Network Tasks, click on Configure Remote Access.
2. On the welcome screen click Next. To enable remote access using VPN or dial-up, select Enable Remote Access and check the VPN Access and the Dial-in Access boxes (as shown in Figure 7.6). Click Next.

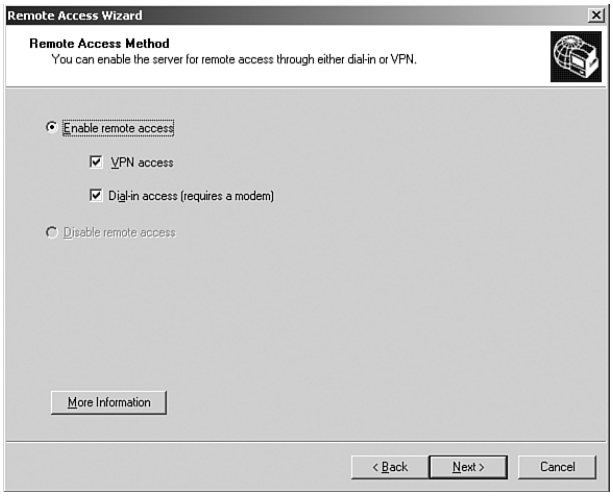

FIGURE 7.6 Remote Access Method screen in the Remote Access Wizard.

3. If the Client Addressing screen appears, you should either select the DHCP server to hand out the IP addresses to the remote clients (which is normally the SBS box) or set a static block of addresses for that purpose.
4. On the VPN Server Name screen type in the FQDN or public IP address of the server and click Next. This is the address that will be used to connect to the server

remotely, so a public DNS record should exist that points to the public IP of your server. You can create a new one—for example, vpn.smallbizco.net—or you could just use the same FQDN for which the SSL certificate was issued.

5. If you selected dial-up access in the Remote Access Method screen, the next screen asks you which modem(s) you want to use for incoming dial-up calls. Select the appropriate modem (as shown in Figure 7.7) and click Next. Remember that this modem should be used exclusively for remote access. If you have only one modem and you plan to use it as a fax, go back and disable dial-up remote access.

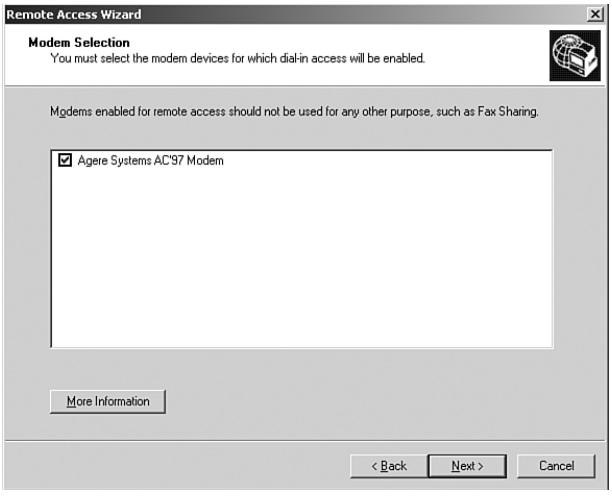

FIGURE 7.7 Modem Selection screen in the Remote Access Wizard.

6. The next screen asks you for the phone number to access the modem(s) selected in step 5. The primary phone number is required; only use the alternate if you have more than one line. Enter the phone number(s) and click two times to finish the wizard.

The server is now configured to accept incoming VPN connections. If you have a router/firewall in front of SBS that is not configured automatically, you need to forward port 1723 to the SBS box and allow protocol GRE 47 (sometimes called PPTP passthrough in some routers) for it work. Finally, if you haven't done so already, make sure that you enforce strong password policies in your network.

NOTE

This chapter focuses exclusively on using Point-to-Point Tunneling Protocol (PPTP) VPNs to connect individual devices to the network. However, other kinds of VPNs might adjust better to your situation. For example:

- Layer 2 Tunneling Protocol (L2TP) is commonly used as an alternative to PPTP. Although its functionality is similar, L2TP provides a higher level of security. This protocol uses certificates

that are issued to the clients to mutually authenticate against the server, thus allowing you to restrict people from connecting using unapproved machines. Implementing L2TP requires a fair amount of manual configuration on both the client and the server.

- Gateway to Gateway VPNs are commonly used when a permanent connection between two offices is desired. Normally, this type of VPN requires a hardware router that supports that capability.

Configuring the Clients

Configuring the clients to connect remotely using VPN or dial-up is the easiest part of this process. If you already ran the Remote Access Wizard and the server is properly configured, the client configuration is almost automatic.

For computers that will be part of the domain but for which the Connect Computer Wizard has not been run yet, just select the Install Connection Manager when you are setting up the new computer on the Server Management Console. After that, run the Connect Computer Wizard (`http://sbs/ConnectComputer`) and wait for the applications to install.

For computers that already have been joined using the Connect Computer Wizard you need to redeploy the Connection Manager. Follow these steps:

1. Open the Server Management Console. On the left pane, expand Standard Management and then select Client Computers. On the right side, click Assign Applications to Client Computers.
2. On the Assign Applications Wizard, select the computers you want to deploy the Connection Manager and click Next.
3. Unselect any application you don't want to redeploy and click Next. On the next screen, select Install Connection Manager and click Next two times to finish the wizard.
4. The next time you log on to the client, the Connection Manager will be installed.

Finally, for any other computer you can download and install the Connection Manager from RWW. Follow these steps:

1. On the client open Internet Explorer and go to the RWW site (`http://mail.smallbizco.net/remote`). Unselect I'm Using a Public or Shared Computer and log in with your domain credentials.
2. On the welcome screen click on Download Connection Manager (as shown in Figure 7.8). Save the file to a location on your computer and run it. The program installs the Connection Manager to your machine.

After the Connection Manager has been installed, you should have an icon on your desktop named Connect to Small Business Server. You can also find it by opening the Connect To menu (or Network Connections folder).

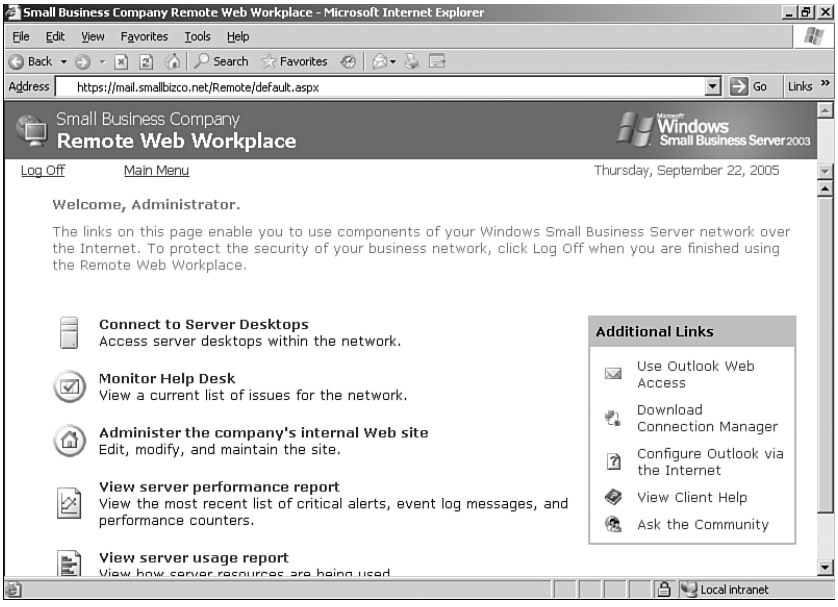

FIGURE 7.8 Connection Manager in RWW.

To connect via dial-up or VPN double-click on the desktop icon and type your domain credentials. If you want to connect using VPN, just click Connect. However, if you want to connect using dial-up, select Properties (see Figure 7.9) and select Dial a Phone Number to Connect. Click OK and then click Connect.

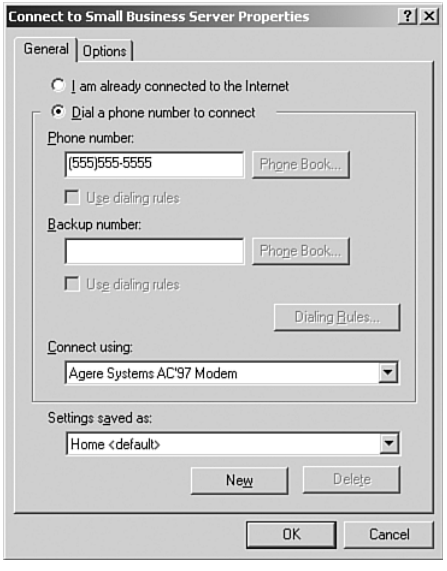

FIGURE 7.9 Connect to Small Business Server Properties screen.

Troubleshooting Routing and Remote Access Issues

Troubleshooting RRAS issues can sometimes be a painful process. So many elements are involved that pinpointing the cause of the problem is not as straightforward as you might hope. This section begins by addressing troubleshooting techniques for some of the most common problems.

A Service Cannot Be Accessed Remotely

You already configured the firewall, and you still cannot access a certain service from the Internet. There are many reasons why this problem can occur, but you can try to identify the problem in a systematic approach.

- Rerun the CEICW and make sure that the appropriate boxes are selected and that the required ports are opened.
- If you have a firewall in front of the server, make sure that the port is opened and forwarded to the SBS external network card.
- Verify that the service you want to access is running. Also, make sure that it's listening on the appropriate port. On the SBS box run `netstat -ano` in a command prompt to determine which processes are listening in which ports.
- Try connecting to the resource from the internal network first. For example, if you have trouble accessing SMTP, type **Telnet 192.168.16.2 25** from any machine on the network to see whether you get a response from Exchange SMTP server.
- Connect a computer on the external segment of the SBS server making sure that it's on the same subnet as the external network card. Try to connect from that location (using the external network card IP address). If you are successful, rule out that the problem is within the SBS box.
- Check whether your ISP is blocking that protocol. If this is the case, you might need to change ISPs or get a business class service that does not have such restrictions. Alternatively, you can use third-party services to redirect traffic to other ports (for example, DynDNS.org offers redirection for SMTP traffic).
- If you are using a DNS record (for example, `mail.smallbizco.net`) to access the resource, try using the public IP instead. Also, verify that the DNS record is resolving to the correct IP. Two great web resources for troubleshooting DNS issues are `www.dnsstuff.com` and `www.dnsreport.com`.
- Use a port scanner from different locations to determine where the fault occurs. FoundStone's SuperScan v4 is a great tool for this job (available for free at `http://www.foundstone.com/resources/proddesc/superscan4.htm`). Online scanners such as ShieldsUP (`www.grc.com`) are also useful.

You Want to Access Your Server Remotely, But Only a Dynamic IP Address Is Available

Ideally, everyone running SBS should have a static IP address. However, the reality is that sometimes you can't get a static IP in your area, or the cost is prohibitive.

You can use a dynamic DNS service to keep a DNS record that always resolves to your most current IP address. You can obtain this service from several third-party sites, such as:

- `www.DynDNS.org`
- `www.TZO.com`
- `www.ZoneEdit.com`

Using such services requires having either a router capable of running a dynamic DNS client or installing the client on your server. Also, some ISPs prevent certain services from being accessed remotely (most notably SMTP and HTTP access).

You Cannot Connect Remotely Using VPN—Error 721

If you cannot connect remotely using VPN, one possible cause is that port 1723 is not being forwarded to the SBS box. However, if you get error 721, this is usually caused if the GRE (Generic Routing Encapsulation) protocol is blocked.

If you are using a router, you must make sure that you enable protocol (not port!) GRE 47 through the router. This is sometimes called *PPTP* or *VPN passthrough*.

You Connect to the VPN Successfully, But You Can't Access Any Resources

This issue is likely caused by a routing problem. For a VPN to work, both machines must be on different subnets. In other words, if your server internal IP address is 192.168.16.2 with a subnet mask of 255.255.255.0, the machine originating the VPN connection can be on any range of IP addresses except 192.168.16.x.

This is a common problem for administrators who manage more than one SBS network. If you install and support SBS systems regularly and you plan to use VPN to access them, you should put your own network on a different subnet as your clients.

You Cannot Establish More Than Five Simultaneous VPN Connections

By default when you run the Remote Access Wizard, it creates only five VPN ports for PPTP and another five ports for L2TP. If this is insufficient, you need to increase the number of PPTP ports available. Follow these steps:

1. Open the Routing and Remote Access console in Administrative Tools. Click on your server name to expand it, right-click on Ports, and select Properties.
2. On the Port Properties screen, select WAN Miniport (PPTP) and click Configure to open the Configure Device dialog box (see Figure 7.10). On the Maximum Ports box select the appropriate number of ports that you want to have available.

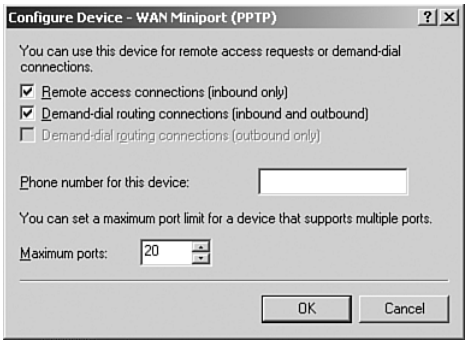

FIGURE 7.10 Configure WAN Miniport (PPTP) screen.

Internet Access Is Sluggish or Blocked While Connected to the VPN

Unfortunately, this is the expected behavior. When you activate the VPN connection, Internet traffic has to go through that connection, making it sluggish. If you are using ISA Server the client most likely will not be able to connect because it doesn't have the firewall client or the proxy settings enabled. In which case, the only workaround is to set the client to use ISA while connected to the VPN.

VPN Connection Keeps Disconnecting After a Period of Inactivity

By default the VPN connection will be dropped by the clients after 10 minutes of no activity. Although it is a good practice to disconnect the VPN as soon as you have finished using it, in some cases it might be necessary to increase this limit.

To modify that behavior, right-click on Connect to Small Business Server on the client and select Properties. Click on the Options tab, change the box that says Idle Time Before Disconnecting, and click OK.

More Troubleshooting Resources

You can find additional troubleshooting resources for the RRAS in Microsoft's TechNet:

- NAT/basic firewall troubleshooting—`http://www.microsoft.com/technet/prodtechnol/windowsserver2003/troubleshooting/routera.mspx`
- VPN troubleshooting—`http://www.microsoft.com/technet/prodtechnol/windowsserver2003/troubleshooting/vpn.mspx`

Summary

The RRAS in SBS 2003 provides important security features to your network. It also provides remote access capabilities via VPN and dial-up. Configuring these services can be achieved by running the built-in wizards and further modified to add more advanced features.

This chapter focused on detailing the features of the RRAS, configuring it as a NAT/basic firewall and to accept incoming VPN and dial-up connections. Also, the VPN capabilities of SBS were described in depth with special attention on enhancing the security of your network. However, firewalls and VPNs are a vast subject, and only so much can be covered in one chapter. The reader is encouraged to further familiarize himself with other firewall and VPN options not covered in this book.

Best Practice Summary

- Use ISA 2004 if you have SBS 2003 Premium—If you already own the SBS 2003 Premium Edition, install and use ISA 2004 instead of relying on RRAS for your firewall.
- Open ports only as needed—Only open ports that are really necessary; opening ports that are not required can put your network at risk.
- Regularly test your firewall—Every once in a while get a port scanner and scan the external interface of your server.
- Enable password policies—Weak or unchanging passwords are a security risk to your network, especially when remote access is enabled.
- VPNs are not a panacea—Think twice before enabling inbound VPN access to your SBS network and consider all the security risks of doing so.
- Practice safe VPN—Never establish a VPN from a computer that is not under your control.