

Global Information Assurance Certification Paper

Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

SANS 2001 Conference – New Orleans GIAC Level 2 Securing Windows

Practical for

John Cusick

April 4, 2001

Step by Step

Configuring Windows 2000 Advanced Server as a Bastion VPN Gateway

Table of Contents

Introduction	3
A Summary of the Windows 2000 IPSec VPN Implementation	3
Installing Windows 2000 Advanced Server	4
Configuring a VPN Server	7
Planning Considerations	7
Our example	8
Configure TCP/IP on the DMZ and WAN adapters	10
Install the Routing and Remote Access Service	11
Configure the Server Properties	13
Configure VPN Ports	18
Configure Logging	20
Configure Routing and Filters	21
Configure Local Policy	27
Obtain and Install a Certificate	30
<u>Client Configuration</u>	35
User and Group Accounts	39
<u>Test It</u>	40
Securing the server as a bastion host	41
Configure TCP/IP Security Settings	41
Disable Unnecessary Services	43
Disable NetBIOS	45
User Accounts	46
Password and Account Lockout Policies	47
Audit Policy	48
User Rights Assignment	49
Security Options	53
Event Logs	59
Disable Source Routing	60
Denial of Service Protection Registry Settings	61
Remove the OS/2 and POSIX Subsystems	63
Disable DirectDraw	64
Disable automatic administrative shares	65
Emergency Repair Disk	66
Conclusion	66
References	67

Introduction

Microsoft's Windows 2000 is the first release of Windows that incorporates native support for the IPSec ("secure IP") standards. The incorporation of these standards has made it possible to implement secure, authenticated and encrypted, communication tunnels, or "Virtual Private Networks" (VPNs), between Windows 2000 hosts on the public Internet.

This paper was written to investigate and document Microsoft's implementation of IPSec as it pertains to remote clients establishing VPN connections to a local area network via a "bastion" Windows 2000 server gateway host. In this context, the term "bastion" refers to a computer that is a fundamental part of a network security system that is exposed to attack, yet tightly secured to minimize damage suffered from any attack.

Specific "step-by-step" instructions are presented for installing and configuring remote access and VPN services on a Windows 2000 Advanced Server, configuring Windows 2000 clients and user accounts for access using IPSec, and further securing the VPN host to minimize its vulnerability on a public network.

As always, it's recommended this be done first in a safe environment, disconnected from the Internet. After testing for functionality and security, the server may then be configured and installed in the public environment.

A Summary of the Windows 2000 IPSec VPN Implementation

Secure – authenticated and encrypted – communication between Windows 2000 clients and servers is accomplished using the Layer 2 Tunneling Protocol (L2TP). This protocol, which is defined in RFC 2661, is a combination of the familiar Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding Protocol (L2F).

The implementation uses L2TP to create the authenticated tunnel between hosts with IPSec providing the data encryption. Encrypted Point-to-Point (PPP) frames are encapsulated within UDP datagrams, with Internet Key Exchange (IKE) traffic traveling to/from UDP 500 and L2TP traffic traveling to/from UDP 1701.

A full range of authentication options are available, from plain text to various forms of Challenge Handshake Authentication Protocol (CHAP) to Extensible Authentication Protocol (EAP), supporting "smart cards" and other mechanisms.

For further detail see the *Microsoft 2000 Server Internetworking Guide* in the *Windows 2000 Resource Kit*⁽¹¹⁾ and *Microsoft Windows 2000 Security Technical Reference*.⁽⁵⁾

Installing Windows 2000 Advanced Server

Install Windows 2000 as a standalone host. Do not make it a member of a domain or active directory structure. As a bastion host, it will need to stand on its own. Other than TCP/IP networking, it is not necessary to install most features and services.

When configuring networking, only select **Client for Microsoft Networks** and **Internet Protocol (TCP/IP)**. While VPN requires the client for Microsoft Networks to be installed, you should unbind it from your external Internet interface, and may unbind it from your other network interface as well.

Obtain and install the latest service pack for Windows 2000. At the time this paper was written, that is *Service Pack 1*, which is available at the following location:

http://www.microsoft.com/windows2000/downloads/recommended/sp1/default.asp

Be sure to check to see if subsequent service packs are released. *Service Pack 2*, for example, is currently being finalized for release in the near future.

Next, update your system with "high" (128 bit) encryption. This is done by installing the *High Encryption Pack for Windows 2000*, which may be obtained at the following location:

http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp

Finally, determine what hot fixes you should install. Hot fixes are patches released between initial software and service pack releases. They frequently are issued to correct security deficiencies. Microsoft has recently provided a *Security Bulletin Search Tool* that facilitates determining what security related hot fixes are available for particular service pack releases.

This tool may be accessed at the following location:

http://www.microsoft.com/technet/security/current.asp

Its use is illustrated on the following two pages.

At the initial page, you select the operating system and service pack level you wish to assess.



After clicking **Go**, you are presented with a page listing the various hot fixes available for this specific configuration.



You may then click on a particular hot fix description to read more detail, download and install it.

Configuring a VPN Server

Planning Considerations

There are a number of planning considerations to make before beginning the actual installation process. Among the issues that need to be considered are the following:

- Whether the VPN server will be used for remote client access and/or network-to-network connections.
- Who will use the service members of your organization only and/or business partners.
- Which remote access security protocol to use Point-to-Point Tunneling Protocol (PPTP) and/or Layer Two Tunneling Protocol (L2TP).
- Whether to use IPSec with L2TP.
- Whether the VPN server will be a member of a domain or directory.
- What certificate authority and certificate distribution method to use with L2TP/IPSec.
- Where to locate the VPN server in relationship to the firewall and perimeters.
- Where and how VPN user authentication will occur.
- What remote access policies are necessary and where will they be maintained.

To assist in planning for your VPN server implementation, I suggest consulting the *Microsoft 2000* Server Deployment Planning Guide and the *Microsoft 2000 Server Internetworking Guide*, each of which are included in the *Windows 2000 Resource Kit*⁽¹¹⁾.

Our example

In this case, we have decided to configure our Windows 2000 VPN server as a bastion gateway host that sits outside the firewall in a "DMZ." It will be used exclusively by remote access clients who are employees of the company. Access will be exclusively via L2TP using IPSec and authentication will be approved or denied based upon account information maintained on a RADIUS server located inside the firewall on the local area network.



Figure 1. Remote access network configuration.

The following sections describe the steps used to implement and test this particular configuration:

- Configure TCP/IP on the DMZ and WAN adapters
- Install the Routing and Remote Access Services
- Configure the Server Properties
- Configure VPN Ports
- Configure Logging
- Configure Routing and Filters
- Configure Local Policy
- Obtain and Install a Certificate
- Client Configuration
- User and Group Accounts
- Test It

Configure TCP/IP on the DMZ and WAN adapters

In this example, the "DMZ Interface" uses 192.168.2.2 with a subnet mask of 255.255.255.0. The "WAN" adapter, named the "IPSec Interface," uses 192.168.111.1 with a subnet mask of 255.255.255.0. Each interface is configured by clicking **Start - Settings - Network and Dial-up Connections**, right-clicking on the interface, selecting **Properties**, clicking on **Internet Protocol (TCP/IP)**, clicking the **Properties** button, and entering the appropriate **IP address** and **Subnet mask**.

🔁 Network and Dia	al-up Connections		
File Edit Viev	IPSec Interface Properties	Internet Protocol (TCP/IP) Properti	es ? X
Address Netw Name A Make New Conne DMZ Interface IPSec Interface	General Sharing Connect using: Intel(R) PR0/100 S Server Ada	General You can get IP settings assigned auto this capability. Otherwise, you need to the appropriate IP settings.	matically if your network supports ask your network administrator for
≟≟LAN Interface	Components checked are used by this Image: The second se	 Obtain an IP address automatica Use the following IP address: — IP address: Subnet mask: Default gateway: 	192.168.111.1 255.255.255.0
	Description Transmission Control Protocol/Interr wide area network protocol that pro across diverse interconnected netw Show icon in taskbar when conner	 Ubtain DNS server address auto Use the following DNS server ad Preferred DNS server: Alternate DNS server: 	Idresses:
Intel(R) PRO/100 S S	1		OK Cancel

Install the Routing and Remote Access Service

Start the Routing and Remote Access (RRAS) configuration by choosing **Start - Programs -Administrative Tools - Routing and Remote Access**. Right-click the server name and select **Configure and Enable Routing and Remote Access**.

Routing and Remote Access		×
$]$ Action View $] \Leftrightarrow \Rightarrow $	🖪 🗙 🖆 😫	
Tree	OGNER (local)	
Routing and Remote Access Server Status	i Configure the Routing and Remote Access Server	
Configure and Enable Ro bisable Routing and Rem	uting and Remote Access ote Access on the Action menu, click ting and Remote Access.	
View	ut setting up a Routing and Remote Access	
Delete Refresh		
Properties		
Help		
Routing and Remote Access Configurat	ion Wizard	

Click Next when the Routing and Remote Access Server Setup Wizard appears.



The following screen appears to offer choices of common RRAS configurations. Don't be misled! While selecting "Virtual private network (VPN) server" might seem a logical choice, it is not the correct one. You must select **Manually configured server** to successfully configure RRAS.¹

Routing and Remote Access Server Setup Wizard	×
Common Configurations You can select from several common configurations.	Ð
 Internet connection server Enable all of the computers on this network to connect to the Internet. 	
C Remote access server Enable remote computers to dial in to this network.	
 Virtual private network (VPN) server Enable remote computers to connect to this network through the Internet. 	
 Network router Enable this network to communicate with other networks. 	
Manually configured server Start the server with default settings.	
< Back Next >	Cancel

Click **Next** to continue, then click **Finish** to complete the RRAS wizard. Click **Yes** to start the RRAS which will then present you with the RRAS Microsoft Management Console (MMC) screen.

¹This appears to be what I might call a "design bug." According to Microsoft Tech Support⁽⁹⁾ this is "by design". According to Microsoft Consulting Services ⁽⁸⁾ this is due to a "bug".

Configure the Server Properties

From the RRAS MMC, you may now configure the properties of your VPN server. Right-click on the server name and select **Properties**.

Routing and Remote Acce	55		
$]$ <u>A</u> ction <u>V</u> iew $]$ \Leftrightarrow \Rightarrow $ $	🗈 <u>n</u> 🗙 😭 🚱 😫		
Tree	BOURGOGNE (local)		
Routing and Remote Access	Name		
Server Status	Routing Interfaces		
Routing I Configur	e and Enable Kouting and Remote Access		
Remote 4 Disable F	touting and Remote Access		
Ports All Tasks	•		
🗄 🖳 IP Routin ————		-	
IPX Routi View	•		
Remote 4			
Export Li	st		
		-	
Propertie	es		
나 사 Help		-	
Upens property sheet for the curr	ent selection.		

Click on the General tab and ensure Router, LAN and demand-dial routing and Remote access server are selected.



Click on the **Security** tab and select the **Authentication provider** you will use. You have a choice between Windows Authentication or RADIUS Authentication.

Since this is a bastion host, we will use **RADIUS authentication**. Windows authentication would require the maintenance of VPN user accounts on the VPN server itself. This may impose some security risks. Instead of maintaining its own user accounts, the VPN server will contact an internal RADIUS server to authenticate users into the local network.

BOURGOGNE (local) Properties	? ×
General Security IP IPX PPP Event Logging	
The authentication provider validates credentials for remote access cl and demand-dial routers.	ients
Authentication provider:	
RADIUS Authentication Configure	
RADIUS Authentication Windows Authentication	-72
The accounting provider maintains a log of connection requests and sessions. Accounting provider:	
Windows Accounting Configure	a

Click **Configure** to specify the RADIUS server configuration, then click **Add**.

Enter the RADIUS Server name or address and enter the UDP Port number used for communication².

Add RADIUS Server			<u>?</u> ×
Server name:	192.168.0.20	01	
Secret:			Change
Time-out (seconds):	5 🔺		.0
Initial score:	30 🔺		
Port:	1645		
🔲 Always use digital sign	natures		
		ОК	Cancel

² You will also need to ensure any firewall between your VPN server and the RADIUS server allows traffic through this port.

Click the **Change** button to enter the secret password that the VPN server will use to access the RADIUS server.



Click **OK** three times to continue, then click the **IP** tab and choose **Static address pool**.

DURGO	GNE (local) I	Properties			?
Genera	I Security		PPP	Event Loggi	ng
E E	nable IP routin	ц <u>к</u> :			
	low IP-based i	emote acces	s and demar	nd-dial conner	ctions
⊢ IP a	iddress assign	ment			
Thi	s server can a	issign IP addi	resses by usir	ng:	
0	Dynamic Hos	t Configuratio	n Protocol (D	HCP)	
•	Static addres	s pool			
	From	То	Number	IP Addr	Mask
	Add	Edit	F	Remove	
Use ti dial-u	he following a p clients.	dapter to obta	ain DHCP, DI	NS, and WIN	S addresses for
Adapt	ter: DMZ	Interface			•
			OK	Cancel	Apply

Click **Add** to add a range of IP addresses the RRAS server can hand out to remote clients. In this example we have selected a range of ten addresses on the local network, 192.168.0.240 through 192.168.0.249. Click **OK**.³

New Address Range		?×
Type a starting IP address a addresses in the range.	and either an ending IP address or the n	umber of
Start IP address:	192.168.0.240	
End IP address:	192.168.0.249	
Number of addresses:	10	
	ОК Са	ncel

Select the adapter that is connected to your private or DMZ network that will be used for DHCP, DNS and WINS. In this case, we selected the DMZ interface which would be used were we to have any DHCP, DNS or WINS traffic.

BOURGOGN	Æ (local) F	Properties				<u>?</u> ×
General	Security I	P IPX	PPP	Event Loggi	ng	
I Enab I Allow IP add This s	ole IP routing v IP-based r ress assignr erver can a	g emote acces ment ssign IP addr	s and demar esses by usi	nd-dial conner	ctions	
C Dy © St	namic Hos atic address	t Configuratio s pool	n Protocol (C	HCP)		
	From 192.168 92.168	To 192.168 Edit	Number 10	IP Addr 192.168 Remove	Mask 255.255	
Use the dial-up c	following ac lients.	lapter to obta	iin DHCP, DI	NS, and WIN	S addresses I	for
Adapter:	DMZ	Interface				
	DMZ LAN I IPSec	Interface Interface Interface	ct adapter			k

³If you will have more than 254 simultaneous users, you will need to span more than one subnet, and then create more than one pool.

To assist with troubleshooting connections, click the **Event Logging** tab and choose **Log the maximum amount of information**. Click **OK** to complete the VPN server properties configuration.

BOURGOGNE (local) Properties	? ×
General Security IP IPX PPP Event Logging	6
Event logging:	
O Log errors only	
C Log errors and warnings	
Log the maximum amount of information Disable event logging	
Enable Point-to-Point Protocol (PPP) logging	
OK Cancel A	pply

Configure VPN Ports

To configure the L2TP ports, right-click Ports and select Properties in the RRAS MMC.

🚊 Routing and Remote Access					
Actionyiew ← → 🔁 🖬 😭 🔛 😭 😫					
Tree Ports					
Routing and Remote Access Name V	Device	Comment	Status		
Server Status 🛛 🙀 WAN Miniport (PPTP) (VPN5-0)	VPN		Inactive		
E- BOURGOGNE (local)	VPN		Inactive		
Routing Interfaces 🛛 🙀 WAN Miniport (L2TP) (VPN4-8)	VPN		Inactive		
Remote Access Client: 💥 WAN Miniport (L2TP) (VPN4-7)	VPN		Inactive		
WAN Miniport (L2TP) (VPN4-6)	VPN		Inactive		
WAN Miniport (L2TP) (VPN4-5)	VPN		Inactive		
Refresh WAN Miniport (L2TP) (VPN4-4)	VPN		Inactive		
Export List WAN Miniport (L2TP) (VPN4-3)	VPN		Inactive		
WAN Miniport (L2TP) (VPN4-2)	VPN		Inactive		
WAN Miniport (L2TP) (VPN4-1)	VPN		Inactive		
Help WAN Miniport (L2TP) (VPN4-0)	VPN		Inactive		
Opens property sheet for the current selection.					

Select the WAN Miniport (L2TP) device and click Configure to continue.

Ports Properties			<u>? ×</u>	
Devices			1	-
Routing and Remote Acces	ss (RRAS) uses the devic	ces listed belo	ow.	ŀ
Device	Used By	Туре	Numb	[
WAN Miniport (PPTP)	RAS/Routing	PPTP	1	•
WAN Miniport (L2TP)	RAS/Routing	L2TP	10	
				M
· · · · · · · · · · · · · · · · · · ·				
Configure				
hg-				
	ОК С	ancel	Apply	

Within the **Configure Device - WAN Miniport (L2TP)** screen, disable **Demand-dial routing connections (inbound and outbound).** Inbound and outbound connections will not be required since we are not creating server-to-server connections, enter the Internet IP address for your VPN server in the **Phone number for this device field**, and type in the maximum number of ports you wish to make available to WAN L2TP connections in the **Maximum ports** field. In this case our external Internet address is 192.168.111.1 and we are allocating a maximum number of 120 ports.

Configure Device - WAN Miniport (L2TP)
You can use this device for remote access requests or demand-dial connections.
Remote access connections (inbound only)
Demand-dial routing connections (inbound and outbound)
Phone number for this device: 192.168.111.1
You can set a maximum port limit for a device that supports multiple ports.
Maximum ports: 120
OK Cancel

Click **OK** to continue. Since we are not using PPTP ports, we limit the available ports for the PPTP device to one (it's not possible to choose zero if RRAS is active).

Configure Device - WAN Miniport (PPTP)	
You can use this device for remote access requests or demand-dial connections.	
Remote access connections (inbound only)	
Demand-dial routing connections (inbound and outbound)	
Phone number for this device:	
You can set a maximum port limit for a device that supports multiple ports.	
Maximum ports:	
OK Cancel	

Click **OK** to continue and click **OK** again to exit the Port configuration utility. If you receive a message indicating current connections may be disconnected, click **Yes** to continue as there are no active current connections.

You will now see the L2TP ports listed in the right pane.

Configure Logging

Click on the **Remote Access Logging** folder in the left pane, then right-click on the **Local File** in the right window and select **Properties**.

Routing and Remote Access	55		
	🖻 📧 🖙 🖳 🔗		
Tree	Remote Access Logging		
Routing and Remote Access Server Status BOURGOGNE (local) Remote Access Clients Ports IP Routing IPX Routing IPX Routing Remote Access Policie Remote Access Loggin	Logging Method	Description C-\WININT\system32\LogFiles perties	
Opens property sheet for the curr	ent selection.		

We wish to maximize logging, so select **Log accounting requests** and **Log authentication requests**, then click **OK** to continue.

Local File Properties	<u>? ×</u>
Settings Local File	
The log contains all the authentication and accounting requests receive by this server. Select the events you want to log.	d
Log accounting requests (for example, accounting start or stop) - recommended	
Log authentication requests (for example, access-accept or access-reject) - recommended	
Log periodic status (for example, interim accounting requests)	
OK Cancel App	ly

Configure Routing and Filters

We will now configure static routes to reach the internal LAN and Internet locations. Double-click **IP Routing** in the left window, right-click **Static Routes** and select **New Static Route**.



Select the internal interface you wish to configure. In this case, we select the "DMZ Interface," and

enter the **Destination** DMZ network 192.168.2.0, **Network mask** 255.255.255.0, and **Gateway** 192.168.2.1, with a **Metric** of 1.



Click **OK** to continue, right-click **Static Routes** and select **New Static Route** again for your external Internet interface. In this case, we select the "IPSec Interface," **Destination** 0.0.0.0, **Network mask** 0.0.0.0, **Gateway** 0.0.0.0 and **Metric** 1 to enable clients to connect from any address on the Internet.

Interface: IPSec Interface Destination: 0.0.0.0 Network mask: 0.0.0.0 Gateway: 0.0.0.0 Metric: 1	Static Route		?×
Destination: 0 ⋅ 0 ⋅ 0 ⋅ 0 Network mask: 0 ⋅ 0 ⋅ 0 ⋅ 0 Gateway: 0 ⋅ 0 ⋅ 0 ⋅ 0 Metric: 1 ★	Interface:	IPSec Interface	•
Network mask: 0 · 0 · 0 · 0 Gateway: 0 · 0 · 0 · 0 Metric: 1 · · · Image: Use this route to initiate demand-dial connections OK Cancel	Destination:	0.0.0.0	
Gateway: 0 . 0 . 0 . 0 Metric: 1	Network mask:	0.0.0.0	
Metric: 1	Gateway:	0.0.0.0	
Use this route to initiate demand-dial connections	Metric:	1 .	
OK Cancel	Use this route to initiate of	demand-dial connections	
		ΟΚ	Cancel

Click **OK** to continue. Click **General** under **IP Routing** in the left pane. In the right pane, right-click on the **IPSec interface** and select **Properties**.

🚊 Routing and Remote Access					
$]$ <u>A</u> ction <u>View</u> $] \Leftrightarrow \Rightarrow $	🖻 💽 🗙 😭 🛃	13			
Tree	General				
Routing and Remote Access Server Status BOURGOGNE (local) Remote Access Clients Ports IP Routing General Static Routes DHCP Relay Agenl IGMP IFX Routing Remote Access Policie Remote Access Loggir	Interface Loopback LAN Interface IPSec Interface Internal DMZ Interface	Type Loopback Dedicated Update Routes Show TCP/IP Inform Show Address Trans Show IP Addresses Show IP Routing Tab Show IP Routing Tab Show UDP Listener P Delete Refresh Properties Help	IP Address 127.0.0.1 Not available 102.142.11 e ation lations ns forts	Administr Up Up Unknown Up	Ope Ope Nor Ope Nor
Opens property sheet for the curre	▲ Int selection.				

On the General tab, click Input Filters.

IPSec Interface Properties	×
General Configuration Multicast Boundaries Multicast Heartbeat	
IP Interface	
Enable IP router manager	
Enable router discovery advertisements	
Advertisement lifetime (minutes):	
Level of preference:	
Send out advertisement within this interval:	
Minimum time (minutes):	
Maximum time (minutes):	
Input Filters Output Filters	
Enable fragmentation checking	
OK Cancel Apply	

Click **Add** in the Input Filters dialog box, then select **Destination network**. Enter the Internet IP address and the subnet mask 255.255.255, select the UDP Protocol, and enter **Source** and **Destination ports** 500 to allow ISAKMP traffic into the VPN server.

Add IP Filter		? ×
Source network		
IP address:		
Subnet mask:	· · · ·	
 Destination network 		
IP address:	192.168.111.1	
Subnet mask:	255 . 255 . 255 . 255	
Protocol:	UDP	•
Source port:	500	
Destination port:	500	
	ОК	Cancel

Click **OK** to continue. Click **Add** in the **Input Filters** dialog box, then select the **Destination network** again. This time, enter UDP **Source** and **Destination ports** 1701 to allow L2TP traffic into the VPN server.

Add IP Filter	<u>? ×</u>
Source network	
IP address:	
Subnet mask:	· · · · ·
🔽 Destination network	
IP address:	192.168.111.1
Subnet mask:	255 . 255 . 255 . 255
Protocol:	UDP 🔽
Source port:	1701
Destination port:	1701
	OK Cancel

In the Input Filters dialog box, select Drop all packets except those that meet the criteria below, then click OK.

These filters control	which packets a	re received for forwarding	or processing on this	; interfa
Receive all pack	kets except those	e that meet the criteria be	ow	
💦 Drop all packets	except those that	at meet the criteria below		
hð ilters:				
Source Address	Source Mask	Destination Address	Destination Mask	Prote
Any	Any	192.168.111.1	255.255.255.255	UDP
Any	Any	192.168.111.1	255.255.255.255	UDF
•				
Add	Edit	Bemove		
			ОК	Cano

On the General tab, click Output Filters, then click Add. Select Source network, and enter the Internet IP address and a Subnet mask of 255.255.255.255. Select the UDP Protocol and enter Source and Destination ports 500.

Edit IP Filter			<u>?</u> ×
Source network			
IP address:	192.168.111.1		
Subnet mask:	255 . 255 . 255 . 255		
Destination network			
IP address:			
Subnet mask:			
Protocol:	UDP	•	
Source port:	500		
Destination port:	500		
	OK	Cano	el

Click **OK** to continue. Click **Add** in the **Output Filters** dialog box, then select the **Source network** again. This time, enter the UDP **Source** and **Destination ports** 1701.

Add IP Filter		? ×
Source network		
IP address:	192.168.111.1	
Subnet mask:	255 . 255 . 255 . 255	:00
Destination network		
IP address:		
Subnet mask:	· · ·	
Protocol:	UDP	
Source port:	1701	
Destination port:	1701	
	OK Car	ncel

In the **Output Filters** dialog box, select **Drop** all packets except those that meet the criteria below, then click **OK**.

Output F	ilters				? ×
These fi	lters control	which packets ar	e received for forwarding	; or processing on this	; interface.
C. Tran	ismit all nack	ets excent those	that meet the criteria be	 Iow	
Filters:	all packets	except those tha	t meet the criteria below		
Source	e Address	Source Mask	Destination Address	Destination Mask	Protocol
192.16	8.111.1	255.255.255	Any	Any	UDP
192.16	8.111.1	255.255.255	Any	Any	UDP
Ad	i	Edit	Remove		
				OK	Cancel

Configure Local Policy

In the left pane, right-click Remote Access Policies and select New Remote Access Policy.

Routing and Remote Access					
📙 Action View	Action View ← → 🔁 📧 🕑 🖽 😰				
Tree	Remote Access C	ients (1)	-		
Routing and Remote Access Server Status BOURGOGNE (local) Remote Access Clients (0) Ports Ports IP Routing IP Routing Remote Access Polici Ope Remote Access Logg New New Help	User Name ⊽ n Remote Access Po	licy	Num		

In the following window, provide a name for your policy.

olicy Name Specify a friendly name for the pol	lieu.
specily a menuly name for the por	nicy.
A Remote Access Policy is a set o meeting certain conditions.	of actions which can be applied to a group of users
Analogous to rules you can apply t specify a set of conditions that mus You can then specify actions to be	to incoming mail in an e-mail application, you can ist be matched for the Remote Access Policy to apply. e taken when the conditions are met.
Policy friendly name:	
Remote Access VPN Clients	

Click **Next** to continue.

At the **Conditions** window, click **Add** to add the following attributes and values:

<u>Attribute</u>	Value
NAS-Port-Type	Virtual(VPN)
Windows-Groups	VPN Users
Called-Station-ID	(Internet IP address of VPN server)
d Remote Access Policy	
Conditions	
Determine the conditions to ma	tch.
Specify the conditions to match	1.
Conditioner	
Londitions:	
Windows-Groups matches "B0	JURGOGNE/VPN_Users'' AND
Called-Station-Id matches "192	2.168.111.1"
1	
Add Remove	Edit

Click Next to continue. Select Grant remote access permissions.

Permissions Determine whether to grant or deny remote access permission. You can use a Remote Access Policy either to grant certain access privileges to a group of users, or to act as a filter and deny access privileges to a group of users. If a user matches the specified conditions:	Pe				
You can use a Remote Access Policy either to grant certain access privileges to a group of users. If a user matches the specified conditions: C Grant remote access permission Deny remote access permission www.settingung.com Cance Cance www.settingung.com Cance		nissions Determine whether to grant or deny re	emote access permissio	ın.	
If a user matches the specified conditions:		You can use a Remote Access Policy group of users, or to act as a filter and	y either to grant certain d deny access privilege	access privileges to s to a group of users.	a
Cance		If a user matches the specified condit	ions:		
C Deny remote access permission		 Grant remote access permission 			
Back Next> Cance		C Deny remote access permission			
< Back Next> Cance					
<u> Back Next></u> Cance					
< Back Next> Cancel C					
< Back Next> Cancel C					
< Back					
Share and a second seco			< Back	Next>	Cancel
				V2	

Click Next to continue then click the **Edit Profile** button, and select the **Authentication** tab. Select the authentication methods allowed for this policy.

Edit Dial-in Profile		_	? ×
Dial-in Constraints	IP	Multilink	
Authentication	Encryption	Advanced	i.
Check the authentication me Extensible Authenticati Select the EAP type which MD5-Challenge Microsoft Encrypted Au Microsoft Encrypted Au	L} ethods which are allowe on Protocol is acceptable for this pr uthentication version 2 (I uthentication (MS-CHAP on (CHAP)	d for this connection.	102
Unauthenticated Access	ation (PAP, SPAP) its to connect without n hod.	egotiating	
[OK Ca	ncel Apply	

Click the **Encryption** tab to define the levels of encryption. We select **Strong** for 56-bit DES and **Strongest** for 3 DES.

Edit Dial-in Profile		? ×
Dial-in Constraints Authentication	IP Encryption	Multilink Advanced
Authentication NOTE: These encryptions and Remote Access Servic Select the level(s) of encry IN No Encryption Basic Strong Strong Strongst	Encryption settings apply only to the W ce. ption that should be allowe	Advanced findows 2000 Routing ed by this profile.
	OK Car	ncel Apply

Click **OK** to save the dial-in profile, then click **OK** to save the policy.

Obtain and Install a Certificate

You must install a local computer certificate on both the VPN server and any clients that will connect to it. The certificates are used by IPSec to authenticate the server and client computers. They may be obtained from a stand-alone or enterprise certificate authority. Since we are configuring this server as a bastion host independent of an enterprise domain, we will install the certificate from a stand-alone certificate authority.

You may obtain one from Microsoft's certificate authority via the Internet at:

http://sectestca2.rte.microsoft.com/certsrv/

At the opening page, select **Request a certificate**.

Microsoft Certificate Services - Microsoft Internet Explorer Elle Edit View Favorites Tools Help Back Forward Sop Refresh Home Search Favorites History Meil Print Address Intip://sectestca2.te.microsoft.com/certsrv/ Image: Search Favorites History Meil Print Microsoft Certificate Services SECTESTCA1 Home Home Meile Print Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: Request a certificate, certificate request Download a CA certificate, certificate chain, or CRL Image: Microsoft.com/certsrv/certrgus.asp	
Elle Edit Yew Favorites Tools Help Back Forward Stop Refresh Home Search Favorites History Mail Print Address Address Intp://sectestca2.te.microsoft.com/certsrv/ Image: Search Favorites History Mail Print Microsoft Certificate Services SECTESTCA1 Home Home Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: Request a certificate, certificate request Download a CA certificate, certificate chain, or CRL Intervet Intervet Intervet	Microsoft Certificate Services - Microsoft Internet Explorer
Back Forward Sop Refresh Home Search Favorites History Mail Print * Address Intp://sectestca2.rte.microsoft.com/certsrv/ Co Links * Microsoft Certificate Services SECTESTCA1 Home * * * * Co Links * Microsoft Certificate Services SECTESTCA1 Home Home *	<u>F</u> ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp
Back Forward Stop Refresh Home Search Favorites History Mail Print Address The http://sectestca2.rte.microsoft.com/certsrv/ Microsoft Certificate Services SECTESTCA1 Home Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: Request a certificate, certificate request Download a CA certificate, certificate chain, or CRL	
Address Inttp://sectestca2.tte.microsoft.com/certsrv/	Back Forward Stop Refresh Home Search Favorites History Mail Print
Microsoft Certificate Services - SECTESTCA1 Home Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	Address 🖉 http://sectestca2.rte.microsoft.com/certsrv/
Microsoft Certificate Services SECTESTCA1 Home Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	
Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people ou communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Belet a task: New the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	Microsoft Certificate Services SECTESTCA1 Home
Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: New the status of a 'pending certificate request Download a CA certificate, certificate chain, or CRL	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: <u>New the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>	Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>	
or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	Line this Mich site to request a partificate for your Mich browser, a mail alignt
or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>	Use this web site to request a certificate for your web browser, e-mail client,
you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	or other program. By using a certificate, you can verify your identity to people
depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	you communicate with over the Web, sign and encrypt messages, and,
tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL 1 http://sectestca2.te.microsoft.com/certsrv/certrgus.asp	depending upon the type of certificate you request, perform other security
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>	tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request. Select a task: <u>Request a certificate</u> View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	
Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>	You can also use this Meh site to download a certificate authority (CA)
Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>	and the set of the set
status of a pending request. Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>	certificate, certificate chain, or certificate revocation list (CRL), or to view the
Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>	status of a pending request.
Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>	
Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL Image: State in the s	Select a task:
View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL Interview Interview Interview Interview	Request a certificate
Download a CA certificate, certificate chain, or CRL Inttp://sectestca2.rte.microsoft.com/certsrv/certrgus.asp Internet	View the status of Ppending certificate request
	The wine status of a periodic request
	Download a CA certificate, certificate chain, or CRL
http://sectestca2.rte.microsoft.com/certsrv/certrgus.asp	
1 http://sectestca2.rte.microsoft.com/certsrv/certrgus.asp	
	Internet
At the next screen, select advanced certificate request.



At the next screen, select Create and submit a request to this CA.



If you receive a Security Warning, you must click Yes to continue.



At the next screen, enter your identifying information and select the **Type of Certificate Needed**. In this case, we want a **Server Authentication Certificate**. Under **Key Options**, select **Create new key set**, **Microsoft Base Cryptographic Provider v1.0**, a **Key Size** of 1024, and check **Use local machine store**. Leave the other options intact unless you have a reason to change them. Click **Submit** to continue.

Microsoft Certific	cate Services - Microsoft Internet Explorer	-
<u>Eile E</u> dit ⊻iew	F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	8
(÷ , =)	🛛 🖸 🕼 🕲 🖻 🗳 🗗 🖨	
Address Ditte://o	and Stop Refresh Home Search Payontes History Mail Print	t Edit Discuss Real.com
], Garces 6 1993/18	seces cazine in closolic on / censiv/ceniquic.asp	
Microsoft Certi	ificate Services SECTESTCA1	<u>Home</u>
Advanced Ce	ertificate Request	
Identifying Infor	rmation:	
Name:	Your name	
E-Mail:	Your email	
Component		
Company.		
Department.		
City:		
State:		
Country/Region:		
Type of Certific	ate Needed	
Type of Gertine	Server Authentiantian Castilianta	
	Server Authentication Certificate	
Key Options:		
	 Create new key set O Use existing key set 	
CSP:	Microsoft Base Cryptographic Provider v1.0	
Key Usage:	⊂Exchange ⊂Signature ⊛Both	
Key Size:	1024 Min: 384 (common key sizes: <u>512 1024</u>)	
	Automatic key container name OUser specified key container name	
	Mark keys as exportable	
	Use local machine store	
	a key in the local machine store.	
	Archive key	
Additional Optic	0.05	
Hach Algorithm:		
riasii Agonulin.	Only used to sign request	
	E Save request to a PKCS #10 file	
Attributes:		
	I F	
	Submit	
e		internet

At the Certificate Issued screen, select Install this certificate.

Microsoft Certificate Services - Microsoft Internet Explorer		_ 8 ×
Eile Edit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		
Stop Refresh Home Search Favorites History Mail Print Edit ⊂	Discuss Real.com	
Address 🗃 http://sectestca2.rte.microsoft.com/certsrv/certfnsh.asp	•	∂Go ∐Links '
Microsoft Certificate Services SECTESTCA1		Home
Certificate Issued		
The certificate you requested was issued to you.		
Install this certificate		
2 Install certificate	🥑 Internet	

You should then see the following:

Microsoft Certificate S	Services - Microsoft Inter	net Explorer				_ 8
jile Edit ⊻iew Favo	orites Tools Help	<u>8</u>	3 B-	4	, iii oo	
Back Forward [dress 🕢 http://sectest	Stop Refresh Ho tca2.rte.microsoft.com/certsr	me Search Favorite: v/certrmpn.asp	s History Mail	Print Edit	Discuss Real.com	∂Go ∫Links
1icrosoft Certificate	e Services SECTES	iTCA1				Home
ertificate Install	led					
our new certifica	ite has been succe	cefully installed				
	ate has been succe					
				\mathbb{A}		
lone					😮 Internet	

You can verify your certificate is installed by starting the MMC and using the **Certificates - Local Computer** snap-in. The newly installed certificate should appear under the **Personal - Certificates** subfolder.





Client Configuration

Each client then needs to follow a similar process to install a Client Authentication Certificate.

2 Microsoft Certificate Services - Microsoft Internet Explorer	- 8
Elle Edit View Fgvorites Iools Help	
back nowine supervised to incread concluster incrementary and prime call backs realized to the second revolution of the s	▼ ∂Go Link
Amount in the second second card and second and second and second and second	er do junite
Microsoft Certificate Services SECTESTCA1	Home
Advanced Certificate Request	
Identifying Information	
Noille, Tourname	
E-Wein. Your small	
Company:	
Department:	
City:	
State	
Country/Region:	
Type of Certificate Needed:	
Client Authentication Certificate	
Key Options:	
Create per lay cet Olice existing lay set	
CPE Microsoft Base Overtranship Revised 40	
Key Lisang C Evolutions - C Brith	
1024 Max1024 (common key sizes <u>piz 1024</u>)	
Automatic key container name O User specified key container name	
Li mark keys as exportatione II lie local machine store	
You must be an administrator to generate or use	
a key in the local machine store.	
□ Archive key	
Additional Options:	
Hash Agorithm: SHA-1 •	
Only used to sign request.	
□ Save request to a PKCS #10 file	
2	
Attributes:	
Submits	
L annu 12	
2	🔮 Internet

On each client computer, create a new "dial-up" Internet connection. Using **Start - Settings - Network** and **Dial-up Connections**, start the **Make New Connection** wizard.

Network Connection Wizard	
	Welcome to the Network Connection Wizard Using this wizard you can create a connection to other computers and networks, enabling applications such as e-mail, Web browsing, file sharing, and printing. To continue, click Next.
	< Back Next > Cancel

Click Next to continue.

Select **Connect** to a private network through the Internet.

Network Connection Wizard	
Network Connection Type You can choose the type of network con your network configuration and your netw	nnection you want to create, based on working needs.
Dial-up to private network Connect using my phone line (moder	n or ISDN).
Dial-up to the Internet Connect to the Internet using my pho	one line (modem or ISDN).
 Connect to a private network to Create a Virtual Private Network (VP) 	t hrough the Internet N) connection or 'tunnel' through the Internet.
 Accept incoming connections Let other computers connect to mine 	by phone line, the Internet, or direct cable.
 Connect directly to another co Connect using my serial, parallel, or in 	mputer nfrared port.
	< Back Next > Cancel

Click Next to continue. Select the method by which the client will access the Internet.⁴

Net	work Connection Wizard
	Public Network Windows can make sure the public network is connected first.
	Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.
	Do not dial the initial connection.
	C Automatically dial this initial connection:
9	
	< Back Next > Cancel

⁴Remote clients attempting to access the VPN server from behind a firewall or other device doing Network Address Translation (NAT) will likely not succeed. This is because IPSec on the client end replaced the original header. Thus, the responding packets from the VPN server cannot find their way back to the originating client. See, for example, "Why Can't IPSec and NAT Just Get Along?" ⁽⁴⁾.

N	etwork Connection Wizard	
	Destination Address What is the name or address of the destination?	I)
	Type the host name or IP address of the computer or network to which you are connecting.	

Host name or IP address (such as microsoft.com or 123.45.6.78):

Click Next to continue. Enter the Internet IP address of the VPN server.

192.168.111.1

< Back Next > Cancel	
< Back Next > Cancel	
< Back Next > Cancel	
< Back Next > Cancel	
	< Back Next > Cancel

Click **Next** to continue. At the **Connection Availability** screen select whether the connection on the client will be available to all users or only the current user, then click **Next** to continue. At the final screen, enter a name for your VPN connection and click **Finish** to exit the wizard.

At the **Connect** screen, click the **Properties** button. Select the **Networking** tab and select the **Layer-2 Tunneling Protocol (L2TP)** in the **Type of VPN server I am calling** box.

Test				
General Options Security Networking Sharing				
Type of VPN server I am calling:				
Layer-2 Tunneling Protocol (L2TP)				
Automatic Point to Point Tunneling Protocol (PPTP) Layer-2 Tunneling Protocol (L2TP)				
Components checked are used by this connection:				
With IPX/SPX/NetBIOS Compatible Transport Pro				
File and Printer Sharing for Microsoft Networks				
Sovell Compatibility Mode Driver Sovell Virtual Private Network				
Install Uninstall Properties				
Description				
Allows your computer to access resources on a Microsoft network.				
UK Cancel				

Click **OK** to save the configuration.

It should be noted here that some knowledgeable users may turn off IPSec in an effort to speed up their connections. This may be determined by examining the following key in the client computer's registry:

```
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\RasMan\Parameters
Name: ProhibitIPSec
Type: REG_DWORD
Value: 1
```

If the key exists, it has been added. Change the **REG_DWORD** value to '0' to enable IPSec.

User and Group Accounts

On your Radius server, domain controller, or wherever your user and group accounts are maintained, establish **Dial-in** permissions for each VPN user. For each user that is allowed VPN access, set the **Remote Access Permission** on the **Dial-in** tab as **Control access through Remote Access Policy**.

John Properties	? ×
General Member Of Profile Dial-in	
Remote Access Permission (Dial-in or VPN)	
C Allow access	
C Deny access	
Control access through Remote Access Policy	
Verify Caller-ID:	-
Callback Options	- 1
• No Callback	
Set by Caller (Routing and Remote Access Service only)	
C Always Callback to:	
Assign a Static IP Address	-
Apply Static Routes	-
Define routes to enable for this Dial-in Static Routes	
OK Cancel App	y

Create a VPN Users group and add each VPN user to it.

Test It

You may then test the dial up connection to verify it works. Verify that the ESP protocol is encrypting packets. The first eight lines of the following dump is an example of a ping sequence:



At the server, you can also check existing client connections in the Network and Dial-up Connections window. Click Start - Settings - Network and Dial-up Connections and double-click the Virtual Private Network connection you wish to examine. Click the Details tab to view the Authentication, Encryption and other information.

General Details		<u>?×</u>
Property Server type Transports Authentication IPSEC Encryption Compression Server IP address Client IP address	Value PPP TCP/IP MS CHAP V2 IPSec, ESP 3DES MPPC 192.168.0.240 192.168.0.241	
	C	lose

Securing the server as a bastion host

Having installed the VPN server and verified it works, we now turn to further securing the server to protect it in a public environment.

There are a number of steps that can be taken to further secure the VPN server so that it can be a bastion host. You do not, however, want to lose functionality! Therefore, I recommend testing after making each of the following configuration changes to verify your VPN server still functions as you want it to.

Configure TCP/IP Security Settings

Although we have already configured port filtering on the Routing and Remote Access Service, we can also filter on the adapters themselves. This ensures filters exist even if the RRAS crashes or is disabled for some reason.

Select Start - Settings - Network and Dial-up Connections, and right-click on the interface you wish to configure. Select Properties, then click on the Internet Protocol (TCP/IP) and click the **Properties** button, click the **Advanced** button, select the **Options** tab, select **TCP/IP filtering**.

© SANS Institute 2000 - 2005





Click **Properties** and at the **TCP/IP Filtering** box, select the **TCP** and **UDP ports** you must allow into and out of your VPN server, as well as the **IP Protocols**. In this case, we are limiting traffic to UDP ports 500 and 1701 for VPN, and 1645 for RADIUS, and we're allowing IP Protocols 50 and 51 for IPSec.

Enable TCP/IP Filtering (All adapters) Permit All Permit All Permit All Permit Only UDP Ports Permit Only IDP Ports 1645 1701 Add Add Add Remove OK Cancel	TCP/IP Filtering		?
Permit All Permit Only TCP Ports S00 1645 1701 Add Remove OK Cancel	🔽 Enable TCP/IP Filt	ering (All adapters)	
Add Add Remove OK OK	C Permit All Permit Only TCP Ports	C Permit All F Permit Only	C Permit All C Permit Only
Add Remove OK Cancel		500 1645 1701	50 51
Remove Remove	Add	Add	Add
OK Cancel	Remove	Remove	Remove
		000	

Disable Unnecessary Services

Windows 2000 comes with a host of services. They can be examined in the Component Services MMC, which may be accessed by **Start - Programs - Administrative Tools - Component Services**.

🚡 Component Services						1×1
] 📸 <u>C</u> onsole <u>W</u> indow <u>H</u>	elp				_ 8	\times
Action ⊻iew ← →						
Tree	Services (Local)					
Console Root	Name	Description	Sta V	Startup	Log On As	
🗄 🙆 Component Services	Sevent Log	Logs event	Started	Automatic	LocalSystem	
🕀 🗑 Event Viewer (Local)	PSEC Policy Agent	Manages I	Started	Automatic	LocalSystem	
Services (Local)	Second Contract Contr	Logical Disk	Started	Automatic	LocalSystem	
	Reg Plug and Play	Manages d	Started	Automatic	LocalSystem	
	Reprotected Storage	Provides pr	Started	Automatic	LocalSystem	
	Remote Procedure Call (RPC)	Provides th	Started	Automatic	LocalSystem	
	Remote Registry Service	Allows rem	Started	Automatic	LocalSystem	
	Routing and Remote Access	Offers rout	Started	Automatic	LocalSystem	
	RunAs Service	Enables st	Started	Automatic	LocalSystem	
	Security Accounts Manager	Stores sec	Started	Automatic	LocalSystem	
	Server .	Provides R	Started	Automatic	LocalSystem	
	www.Task Scheduler	Enables a	Started	Automatic	LocalSystem	
	Windows Management Instrumentation	Provides s	Started	Automatic	LocalSystem	
	Workstation	Provides n	Started	Automatic	LocalSystem	
	Network Connections	Manages o	Started	Manual	LocalSystem	
	Remote Access Connection Manager	Creates a	Started	Manual	LocalSystem	
	Telephony	Provides T	Started	Manual	LocalSystem	
	Windows Management Instrumentation Driver Extensions	Provides s	Started	Manual	LocalSystem	-

Precisely which services you should disable will depend upon your particular server configuration and preferences. You may, for example, require the DNS Client if your VPN server must resolve names, or you may choose to use the Task Scheduler to schedule the execution of tasks. As an overall strategy it's best to eliminate any services you don't need.

By double-clicking on a particular service in the **Component Services** window, then selecting the **Dependencies** tab, one may view which services that particular service depends upon, as well as any other services that may depend upon it. The following, for example, is RRAS:

Routing and Remote Access Properties (Local Computer)	
General Log On Recovery Dependencies	
Some services depend on other services. If a service is stopped or is not running properly, dependent services can be affected.	
"Routing and Remote Access" depends on these services:	
⊕- 😸 NetBIDSGroup ⊕- 🍪 Remote Procedure Call (RPC)	
-	
These services depend on "Routing and Remote Access":	C Y
😲 <no dependencies=""></no>	

I found it necessary to have the Remote Procedure Call (RPC), Server and Workstation services available for RRAS to function, and the Remote Registry Service is assigned for VPN. I would suggest the following services be configured to start automatically:

- Event Log
- IPSEC Policy Agent
- Logical Disk Manager
- Network Connections
- Plug and Play
- Protected Storage
- Remote Procedure Call (RPC) •
- Remote Registry Service

- Routing and Remote Access
- RunAs Service
- Security Accounts Manager
- Server
- Task Scheduler
- Windows Management Instrumentation
- Windows Management Instrumentation Driver Extensions
- Workstation

Telephony

•

You will probably also require the following services to start manually:

• Remote Access Connection Manager

51

Disable NetBIOS

Windows 2000 has a new feature called "Direct Host." This feature provides an alternative method of filesharing (SMB/CIFS) without having to use NetBIOS. It uses TCP port 445 for communication. This may be disabled by **Start - Programs - Administrative Tools - Computer Management**, double-clicking the **Device Manager** in the left pane, clicking **View** and selecting **Show Hidden Devices**, then right-clicking **NetBios over TCPip** and selecting **Disable**.

$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	📙 Computer Management		
Tree dmload	$Action View 4 \Leftrightarrow A$	S 😫 🧸 🗶	
Computer Management (Local) Fs_Rec System Tools Generic Packet Classifier Performance Logs and Alerts IP Traffic Filter Driver System Information IPX Traffic Filter Driver Performance Logs and Alerts IPX Traffic Filter Driver Shared Folders IPX Traffic Filter Driver Device Manager IPX Traffic Filter Driver Disk Management NDIS System Driver NDis System Drives NetBios over Topip Disk Defragmenter NDProxy Disk Defragmenter NULIN NPROXY NetWork Monitor Dr Nulinstall Nullink SPX/SPX/Ne Scan for hardware changes NWLink SPX/SPXIL Protocor Parallel Parallel Parport Parallel Parallel	Tree Computer Management (Local) System Tools Event Viewer System Information Performance Logs and Alerts System Folders Device Manager Event Viewer Device Manager Device Manager Disk Defragment Disk Defragment Digical Drives Removable Storage Services and Applications	dmload Fs_Rec Generic Packet Classifier JP Traffic Filter Driver JPSC driver JPX Traffic Filter Driver JPX Traffic Forwarder Driver KSecDD mmmdd mountmgr NDIS System Driver NDF System Driver NDProxy NetWork Monitor Dr Null NWLink IPX/SPX/Ne NWLink NetBIOS NWLink SPX/SPXII Protocor Packet Driver v2.1 Parallel Parport Parport	



User Accounts

Disable accounts that are not needed. Disable the Guest account by checking Account is disabled.

est Properties	?	×
General Member ()f Profile Dial-in	
Guest		
Full name:		1
Description:	Built-in account for guest access to the computer/do	
🔲 User must cha	nge password at next logon	
🔽 User cannot cl	hange password	
Password nev	er expires	
Account is disa	bled	
C Account is loc	ked out	
	OK Cancel Apply	

Do the same with **the Internet Guest Account**, **Launch IIS Process Account**, **TsInternetUser Account** or any other superfluous account. Rename the **Administrator** account, then create a dummy **Administrator** account with no rights and a difficult to crack password.

Password and Account Lockout Policies

Go to **Start - Programs - Administrative Tools - Local Security Policy** to change the password and account lockout policies.

** Note: If user and group accounts are maintained on a separate server, such as the RADIUS server in our example, I recommend making these changes on that server as well. **

The recommended changes from the default settings for the password history, maximum and minimum password age, password length and complexity, and password storage are as follows:

📑 Local Security Settings		_ 🗆 🗵
] Action ⊻iew] 🗢 →		
Tree	Policy 🛆	Local Setting
Becurity Settings	B Enforce password history	8 passwords remem
🚊 📴 Account Policies	👪 Maximum password age	91 days
🕂 道 Password Policy	🕮 Minimum password age	5 days
🗄 道 Account Lockout F	🕮 Minimum password length	8 characters
🗄 🔂 Local Policies	Beasswords must meet complexity requirements	Enabled
🗄 💼 Public Key Policies	Store password using reversible encryption for all users in the domain	Disabled
🗄 🛃 IP Security Policies on		
•	•	F

The recommended settings for the Account Lockout Policy are as follows:

📑 Local Security Settings		
] Action ⊻iew] 🗢 →		
Tree	Policy 🛆	Local Setting
Security Settings	Count lockout duration	30 minutes
🚊 📴 Account Policies	题 Account lockout threshold	5 invalid logon atte
🕂 📴 Password Policy	👸 Reset account lockout counter after	30 minutes
Account Lockout F		
🗄 🛄 Local Policies		
🗄 🖳 🛄 Public Key Policies		
🗄 🜏 IP Security Policies on		\searrow
		v
•	•	Þ

Audit Policy

Again from **Start - Programs - Administrative Tools - Local Security Policy** we can edit the Audit Policy. Double-click **Local Policies** and then **Audit Policy** in the left pane to display them.

The recommended changes from default are as follows:

📑 Local Security Settings		
] <u>A</u> ction ⊻iew] ← →		
Tree	Policy 🛆	Local Setting
Becurity Settings	B Audit account logon events	Success, Failure
Account Policies	Audit account management	Success, Failure
🗄 📴 Password Policy	Audit directory service access	Failure
🔤 🛄 Account Lockout F	BB Audit logon events	Success, Failure
🗄 📴 Local Policies	B Audit object access	Failure
庄 道 Audit Policy	B Audit policy change	Success, Failure
🕀 🤷 User Rights Assigr	B Audit privilege use	Failure
Security Options	B Audit process tracking	No auditing
🕀 🧰 Public Key Policies	Audit system events	Failure
🗄 🛃 IP Security Policies on		
		- K

Shittle and

User Rights Assignment

By clicking on **User Rights Assignment** in the left pane, the user rights policies are displayed in the right window. A policy may be revised by double-clicking it in the right window.

For each the following User Rights Assignments, I recommend removing all users except Administrators:

- Access this computer from the network
- Backup file and directories
- Bypass traverse checking
- Change the system time
- Log on locally
- Shut down the system

These changes are illustrated on the below and on the following pages.

Access this computer from the network

Access this computer fro	m the network	<u>?</u> ×
Assigned To	Local Policy Setting	Effective Policy Setting
BOURGOGNENWAM_BOURGOG	ine 🗖	
Administrators Backup Operators Power Users Users Everyone BOURGOGNE\IUSR_BOURGOGI		
Add	ned, they override	े a local policy settings.
	10	Cancel

Backup files and directories

Local Security Policy Setting		?	×
Back up files and direc	ctories		
Assigned To	Local Policy Setting	Effective Policy Setting	
Administrators Backup Operators			
Add			
If domain-level policy settings are de	efined, they override I	ocal policy settings.	
		Cancel]

Bypass traverse checking

Local Security Policy Setting		<u>? ×</u>
Bypass traverse check	king	
Assigned To	Local Policy Setting	Effective Policy Setting
Administrators Backup Operators Power Users Users Everyone		N N N
Add If domain-level policy settings are d	efined, they override l	ocal policy settings.
	ОК	Cancel

Change the system time

Change the system time Assigned To Local Effective Administrators Image: Administrators Image: Administrators Power Users Image: Administrators Image: Administrators Add Add If domain-level policy settings are defined, they override local policy settings. If domain-level policy settings are defined, they override local policy settings.	Local Security Policy Setting		?
Assigned To Policy Setting Policy Setting Administrators Image: Control of the set of	Change the system time	e	
Administrators Power Users	Assigned To	Local Policy Setting	Effective Policy Setting
Add If domain-level policy settings are defined, they override local policy settings. OK Cancel	Administrators Power Users		N N
If domain-level policy settings are defined, they override local policy settings.	Add		
OK Cancel			
OK Cancel	If domain-level policy settings are de	fined they override	local policy settings
the les	If domain-level policy settings are de	fined, they override	local policy settings.
	If domain-level policy settings are de	fined, they override	local policy settings.
	If domain-level policy settings are de	fined, they override	local policy settings.
	If domain-level policy settings are de	fined, they override	local policy settings.

Log on locally

La	cal Security Policy Setting			<u>? ×</u>
	Log on locally			
	Assigned To	Local Policy Setting	Effective Policy Setting	
	BOURGOGNE/JUSR_BOURGOG	NE 🗖	4	
	Administrators Backup Operators Power Users Users BOURGOGNE\Guest BOURGOGNE\TsInternetUser			_
	Add	ned, they override	local policy setting	JS.
		OK	Cance	:

Shut down the system

Local Security Policy Setting		<u>? ×</u>
Shut down the system		
Assigned To	Local Policy Setting	Effective Policy Setting
Administrators Backup Operators Power Users		N N
Add	ined, they override	local policy settings.
	OK.	Cancel

Security Options

By clicking **Security Options** in the left pane, we display these policies in the right pane. By doubleclicking a given policy, we can revise its setting. The following revisions are recommended:

Additional restrictions for anonymous connections

Local policy setting: Do not allow enumeration of SAM accounts and shares

Additional restrictions for anonymou Effective policy setting:	us connections
Effective policy setting:	
None. Rely on default permissions	
Local policy setting:	
Do not allow enumeration of SAM accounts	and shares 📃 💌
If domain-level policy settings are defined, the	ey override local policy settings.

Clear virtual memory pagefile when system shuts down

Local policy setting: Enabled

Local Security Policy Setting
Clear virtual memory pagefile when system shuts down
Effective policy setting:
Disabled
Enabled
 Disabled If domain-level policy settings are defined, they override local policy settings.
OK Cancel

Do not display last user name in logon screen

Local policy setting: Enabled

Local Security Policy Setting	
Do not display last user name in logon screen	
Effective policy setting:	
Disabled	
Local policy setting:	
Enabled	
C Disabled	
If domain-level policy settings are defined, they override local policy settings.	
OK Cancel	

LAN Manager Authentication Level

Local policy setting: Send LM & NTLM – use NTLMv2 session security if negotiated



Message text for users attempting to log on

Local policy setting: A message such as "Authorized Access Only! Violators will be prosecuted in accordance with the law."

Local Sec	urity Policy Setting
5	Message text for users attempting to log on
Effective	policy setting:
Local po	licy setting:
Authoriz	ed Access Only! Violators will be prosecuted in accordance with th
If domain	n-level policy settings are defined, they override local policy settings.
	OK Cancel

Message title for users attempting to log on

Local policy setting: A title such as "Warning!"

Local Security Policy Setting
Message title for users attempting to log on
Effective policy setting:
Local policy setting:
Warning!
It domain-level policy settings are defined, they override local policy settings.
OK Cancel

Number of previous logons to cache (in case domain controller is not available)

Local policy setting: **0 logons**

Local Security Policy Setting	?×
Number of previous logons to cache (in case domain contro not available)	olleris
Effective policy setting	
10 logons	
Local policy setting	
Do not cache logons:	
0 Jogons	
If domain-level policy settings are defined, they override local policy set	ettings.
OK Cano	el

Prompt user to change password before expiration ⁵

Local policy setting: 61 days

Considering the Maximum Password age of 91 days recommended above, this should result in users changing passwords every 30 days, while minimizing the need for the Administrator to unlock accounts.

Local Security Policy Setting	<u>? ×</u>
Prompt user to change password before expiration	
Effective policy setting	
14 days	
Local policy setting	
Begin prompting this many days before password expires:	
If domain-level policy settings are defined, they override local policy se	ttings.
OK Canc	el

⁵If user and group accounts are maintained on a separate server, such as the RADIUS server in our example, I recommend making this change on that server as well.

Rename administrator account

Local policy setting: Enter the name of your renamed Administrator account

Local Security Policy Setting	<u>?</u> ×
Rename administrator account	
Effective policy setting:	
Not defined	
Local policy setting:	
Enter new name here	
If domain-level policy settings are defined, they override local po	olicy settings. Cancel

Restrict CD-ROM access to locally logged-on user only

Local policy setting: Enabled

Local Security Policy Setting	<u>?</u> ×
Restrict CD-ROM access to locally logged-on user only	
Effective policy setting:	
Disabled	
Local policy setting:	
Enabled	
C Disabled	
If domain-level policy settings are defined, they override local policy se	ttings.
OK Canc	el

Restrict floppy access to locally logged-on user only

Local policy setting: Enabled

Local Security Policy Setting	
Restrict floppy access to locally logged-on user only	
Effective policy setting:	
Disabled	
Local policy setting:	
Enabled	
O Disabled	
If domain-level policy settings are defined, they override local policy settings.	
OK Cancel	

Shut down system immediately if unable to log security audits

Local policy setting: Enabled

Local Security Policy Setting				
Shut down system immediately if unable to log security audits				
Effective policy setting:				
Disabled				
Local policy setting:				
 Enabled 				
O Disabled				
If domain-level policy settings are defined, they override local policy settings.				
OK Cancel				

Event Logs

I recommend increasing the log file sizes to 20MB and retaining them for 60 days. The **Application Log**, **Security Log**, and **System Log** should therefore be set as follows:

Display name:	System Log								
Log name:	C:\WINNT\svstem32\config\SvsEvent.Evt								
Size	128.0 KB (131,072 bytes)								
Created: Monday, March 19, 2001 12:22:09 PM									
Modified: Monday, April 02, 2001 5:12:19 PM									
Accessed: Monday, April 02, 2001 5:12:19 PM									
Log size									
Maximum log size: 20032 KB When maximum log size is reached:									
					Overwrite events older than 60 days				
					C Do not overwrite events (clear log manually)				
Using a low	-speed connection Clear Log								

The security on the logs should limit full control to administrators and the system. Right-click on the following files and select the **Security** tab to verify and, if necessary, revise the permissions:

%SystemRoot%\system32\SysEvent.Evt %SystemRoot%\system32\SecEvent.Evt %SystemRoot%\System32\AppEvent.Evt

ieneral Security Summary		
Name Madministrators (BOURGOGNE) RSYSTEM	dministrat	i
Permissions: Full Control Modify Read & Execute Read Write	Allow De	eny 1 1 1 1 1 1 1 1 1
Advanced Allow inheritable permissions from object	parent to propagate to	this

Disable Source Routing

```
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\Tcpip\Parameters
Name: DisableIPSourceRouting
Type: REG_DWORD
Value: 2
```

Denial of Service Protection Registry Settings

There are a variety of registry changes that can increase the resistance of a Windows 2000 network stack to denial of service attacks.

SYN attack protection can be improved with the following changes⁶:

```
Hive:
           HKEY LOCAL MACHINE
           System\CurrentControlSet\Services\Tcpip\Parameters
Key:
           SynAttackProtection
Name:
           REG DWORD
Type:
           2
Value:
Hive:
           HKEY LOCAL MACHINE
           System\CurrentControlSet\Services\Tcpip\Parameters
Key:
           TcpMaxHalfOpen
Name:
           REG DWORD
Type:
Value:
           500 (decimal)
           HKEY LOCAL MACHINE
Hive:
           System\CurrentControlSet\Services\Tcpip\Parameters
Key:
           TcpMaxHalfOpenRetried
Name:
Type:
           REG DWORD
           400 (decimal)
Value:
           HKEY LOCAL MACHINE
Hive:
Key:
           System\CurrentControlSet\Services\Tcpip\Parameters
Name:
           NoNameReleaseOnDemand
Type:
           REG DWORD
Value:
           1
Hive:
           HKEY LOCAL MACHINE
           System\CurrentControlSet\Services\Tcpip\Parameters
Key:
           DeadGWDetectDefault
Name:
           REG DWORD
Type:
Value:
           0
Hive:
           HKEY LOCAL MACHINE
           System\CurrentControlSet\Services\Tcpip\Parameters
Key:
Name:
           KeepAliveTime
           REG DWORD
Type:
           300,000 (decimal)
Value:
           HKEY LOCAL MACHINE
Hive:
Key:
           System\CurrentControlSet\Services\Tcpip\Parameters
Name:
           PerformRouterDiscovery
Type:
           REG DWORD
Value:
           0
```

⁶For further details about each setting, see "Security Considerations for Network Attacks" ⁽¹²⁾

Hive: HKEY LOCAL MACHINE System\CurrentControlSet\Services\Tcpip\Parameters Key: Name: Name: Type: Value:

Remove the OS/2 and POSIX Subsystems

Removing these subsystems is part of the C2 Security standard, and will help improve system performance. If you are positive you won't be using them, simply make the following Registry changes:

Delete all subkeys under:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT

Delete the value for Os2LibPath under:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment

Delete the value for Optional under:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems

Delete entries for Posix and OS/2 under:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems

Disable DirectDraw

This prevents direct access to video hardware and memory which is required to meet the basic C2 security standards. Disabling DirectDraw may impact some programs that require DirectX (games), but most business applications should be unaffected. To disable it, edit or create the following key:

HKEY LOCAL MACHINE Hive: SYSTEM\CurrentControlSet\Control\GraphicsDrivers\DCI Key: Name: Timeout Type: REG_DWORD Value: 0 Sharing and a state of the stat

© SANS Institute 2000 - 2005
Disable automatic administrative shares

Because all default installations have these shares, it is best to disable them so as to reduce the number of known targets for a malicious user. These hidden shares with their associated paths are:

C\$, D\$	The root of each partition
ADMIN\$	%System Root%
IPC\$	Temporary connections between servers
PRINT\$	%System Root%\System32\Spool\Drivers

The following registry change will eliminate all but the IPC\$ share:

Hive:	HKEY LOCAL MACHINE
Key:	System\CurrentControlSet\Services\LanmanServer\Parameters
Name:	AutoShareServer
Type:	REG_DWORD
Value:	0

Based upon my experience, eliminating the IPC\$ share disables the VPN server functionality, presumably because VPN requires RPC services.

Emergency Repair Disk

When changes to the system configuration are complete, make an Emergency Repair Disk (ERD). The ERD contains the registry, system file, partition boot sector, and the startup environment information. It can be used to repair the server if it does not start or if system files have become corrupted.

Insert a blank 3¹/₂" floppy disk and go to **Start - Programs - Accessories - System Tools - Backup**. Select **Emergency Repair Disk** at the next screen and check the option to backup the registry at the next window. Put the diskette away in a secure location.

Examine the **%SystemRoot%\repair\RegBack** directory to verify the following files exist:

- default
- ntuser.dat
- sam
- security
- software
- system
- usrclass.dat

Verify the permissions set on the **RegBack** directory are **Full Control** for **Administrators** only.

Conclusion

Congratulations! You have created a bastion host that's ready to serve as a secure VPN gateway to your Internet. Be sure to test it when you "go live" and monitor the logs regularly for signs of suspicious activity.

References

- Bird, T. 2000. "Secure Networking: An Introduction to VPN Architecture and Implementation." Presentation at 2000 Usenix Annual Technical Conference, June 18 - 23, 2000, San Diego, California.
- (2) Brock, A. 2001. "Hardening Windows 2000 Advanced Server for Internet Participation." http://www.sans.org/giactc/gcnt.htm
- (3) Fossen, J. 2001. "Windows 2000 Active Directory and Group Policy." Presentation at SANS New Orleans, January 28 February 2, 2001, New Orleans, Louisiana.
- (4) Fratto, M. 2000. "Why Can't IPSec and NAT Just Get Along?" http://www.networkcomputing.com/1123/1123ws2.html
- (5) Internet Security Systems, Inc. 2000. *Microsoft Windows 2000 Security Technical Reference*. Microsoft Press, Redmond, Washington.
- (6) Ivens, K. 2000. Admin911: Windows 2000 Registry. Osborne/McGraw-Hill, U.S.A.
- (7) Lee, T. and Davies, J. 2000. *Microsoft Windows 2000 TCP/IP Protocols and Services Technical Reference*. Microsoft Press, Redmond, Washington.
- (8) Microsoft Consulting Services. 2000. "Configuring a VPN Solution." http://www.microsoft.com/ISN/whitepapers/configur_vpn_solution.asp?A=0
- Microsoft Corporation. 2001. "Enabling VPN in RRAS Causes Connection Issues to Remote Networks." (Q243374) http://support.microsoft.com/support/kb/articles/q243/3/74.asp
- (10) Microsoft Corporation. 2000. "How to Install a Certificate for Use with IP Security." (Q253498) <u>http://support.microsoft.com/support/kb/articles/q253/4/98.asp</u>
- (11) Microsoft Corporation. 2000. *Microsoft Windows 2000 Resource Kit*. Microsoft Press, Redmond, Washington.
- (12) Microsoft Corporation. 2001. "Security Considerations for Network Attacks." http://www.microsoft.com/technet/security/dosrv.asp
- (13) Microsoft Corporation. 2000. "Windows 2000 Virtual Private Networking Scenario." <u>http://www.microsoft.com/windows2000/library/howitworks/communications/remoteaccess/w2kvpnscenario.asp</u>
- (14) Norberg, S. 2001. *Securing Windows NT/2000 Servers for the Internet*. O'Reilly & Associates, Inc., Sebastopol, California.
- (15) Oryszczyn. J. 2001. "Securing a Windows 2000 Server Connected to the Internet." http://www.sans.org/giactc/gcnt.htm
- (16) Schultz, E. 2000. Windows NT/2000 Security. Macmillan Technical Publishing, U.S.A.