Global Information Assurance Certification Paper

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

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

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

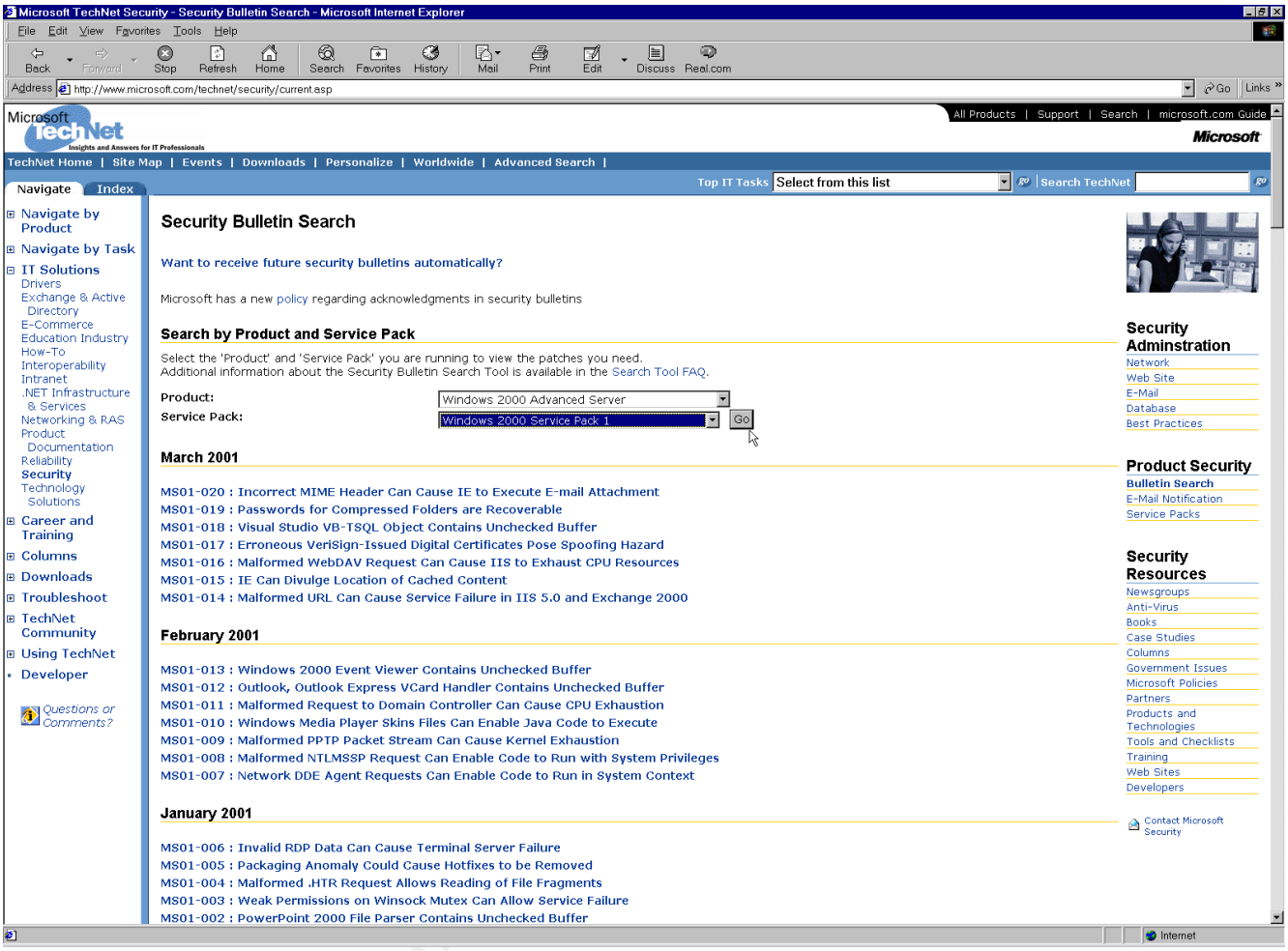
Finally, determine what hot fixes you should install. Hot fixes are patches released between initial software and service pack releases. They frequently are issued to correct security deficiencies. Microsoft has recently provided a *Security Bulletin Search Tool* that facilitates determining what security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

This tool may be accessed at the following location:

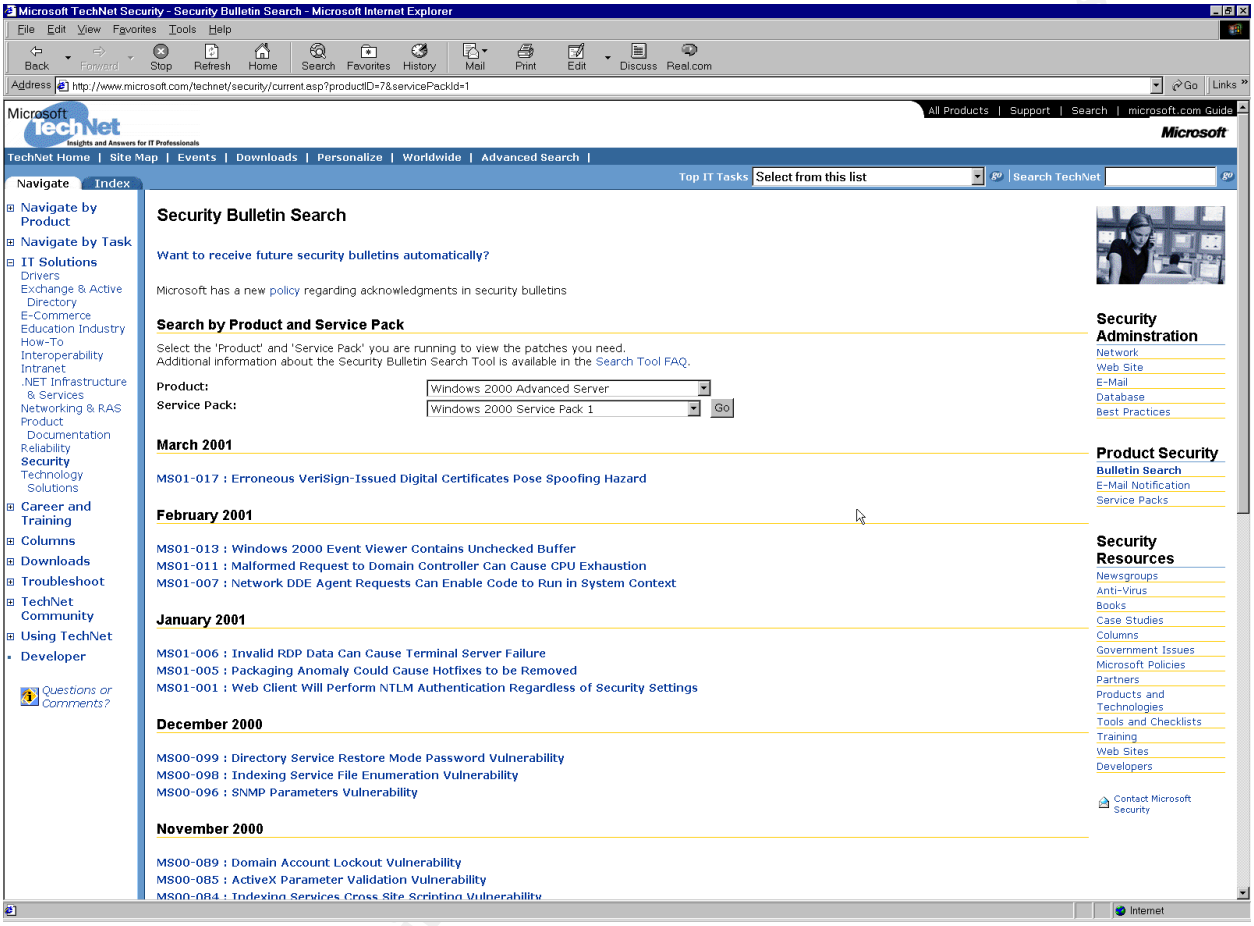
http://www.microsoft.com/technet/security/current.asp

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.

This configuration is depicted in Figure 1.

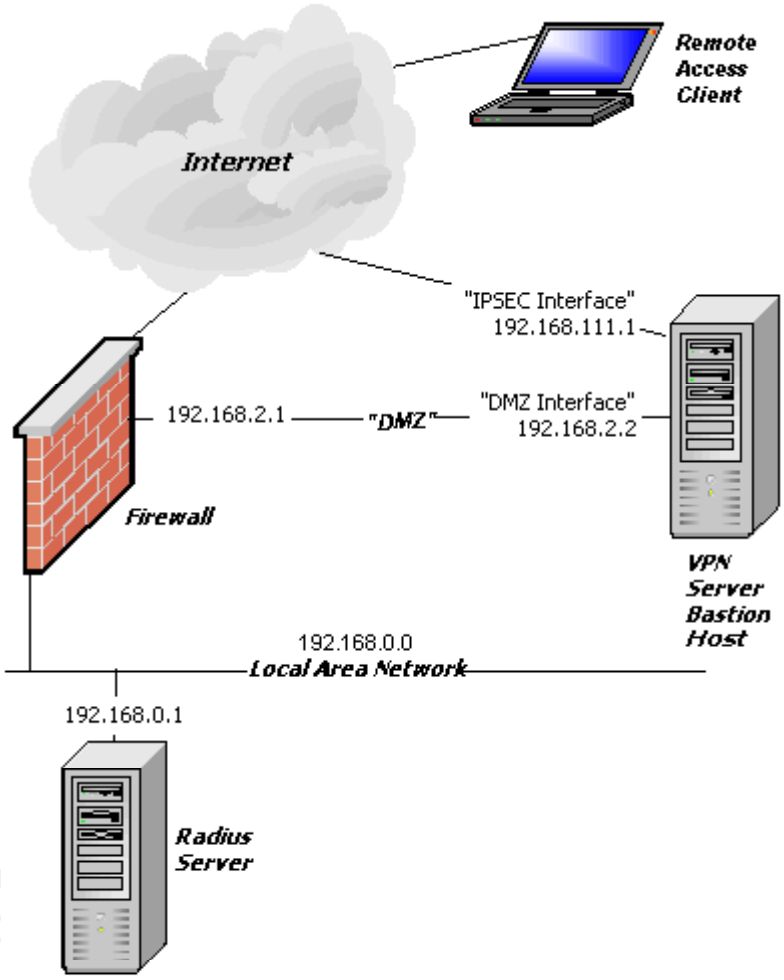


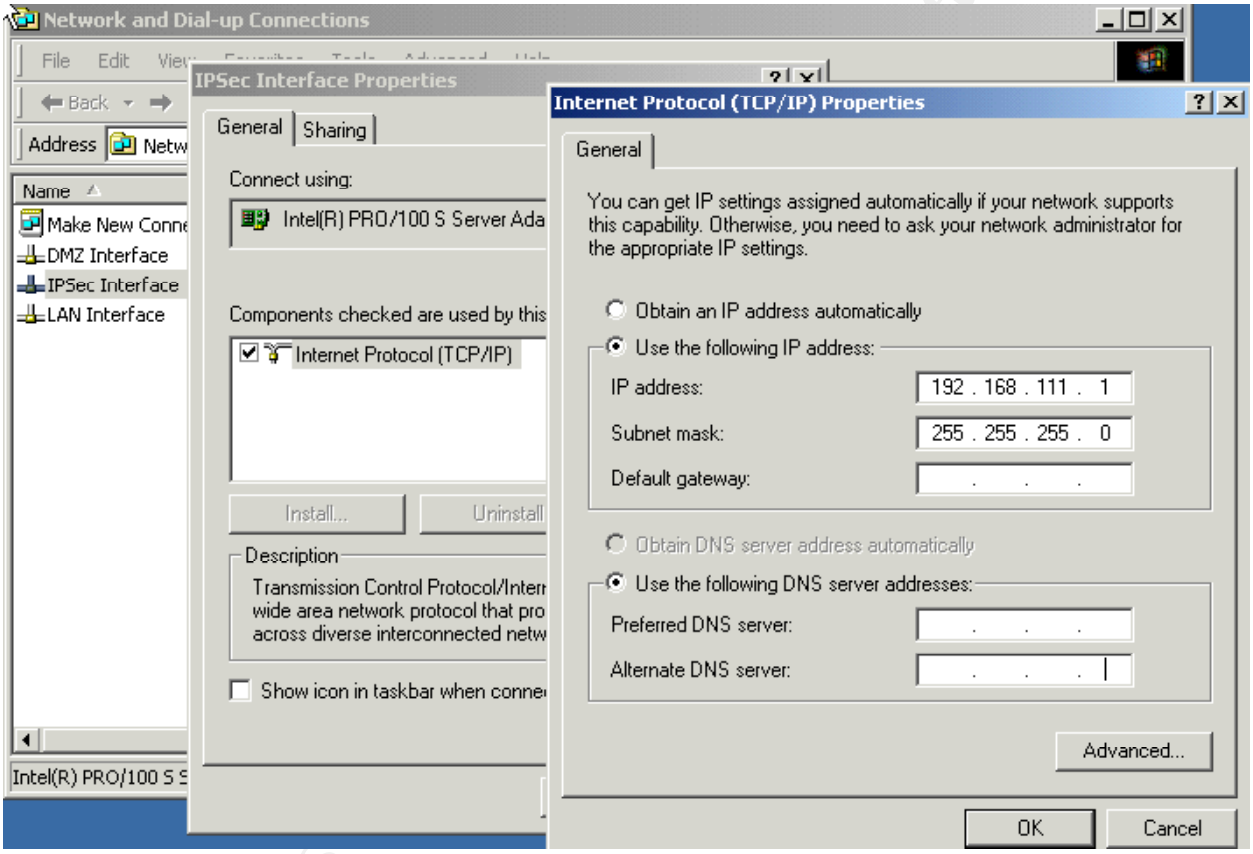
Figure 1. Remote access network configuration.

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

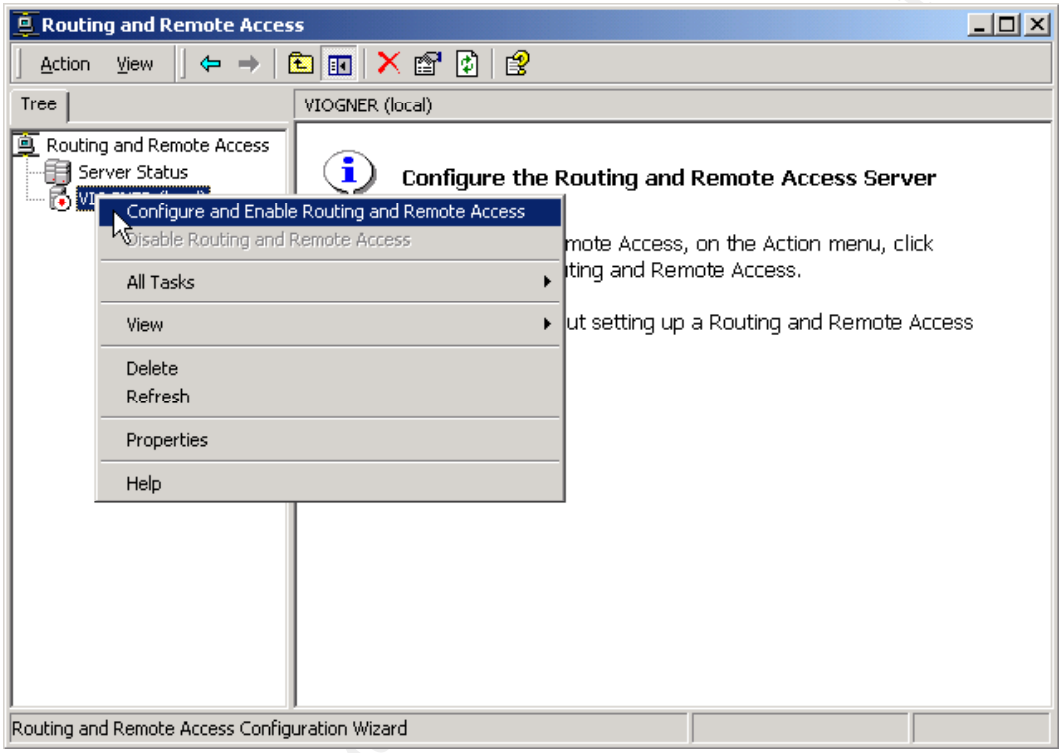
Configure TCP/IP on the DMZ and WAN adapters

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**.

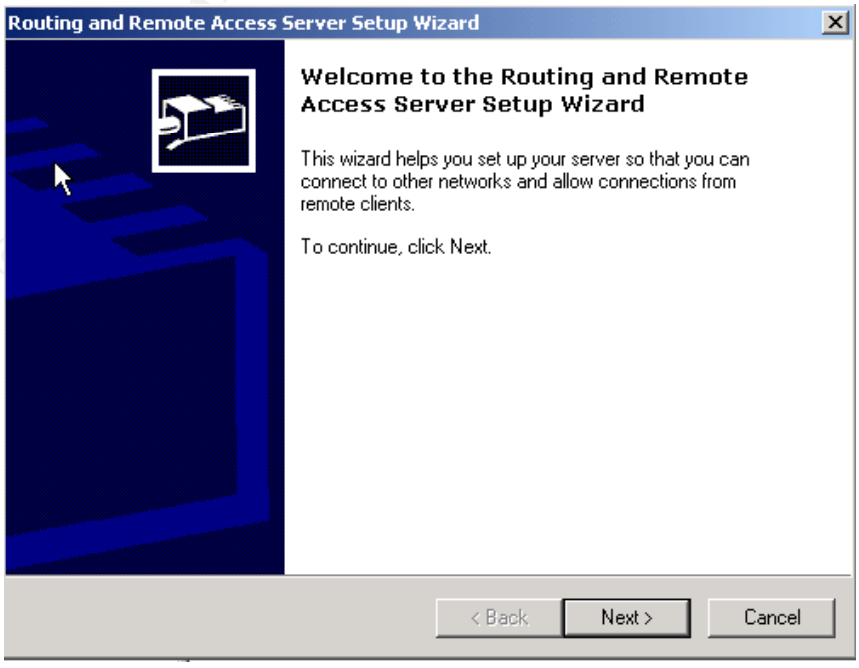


Install the Routing and Remote Access Service

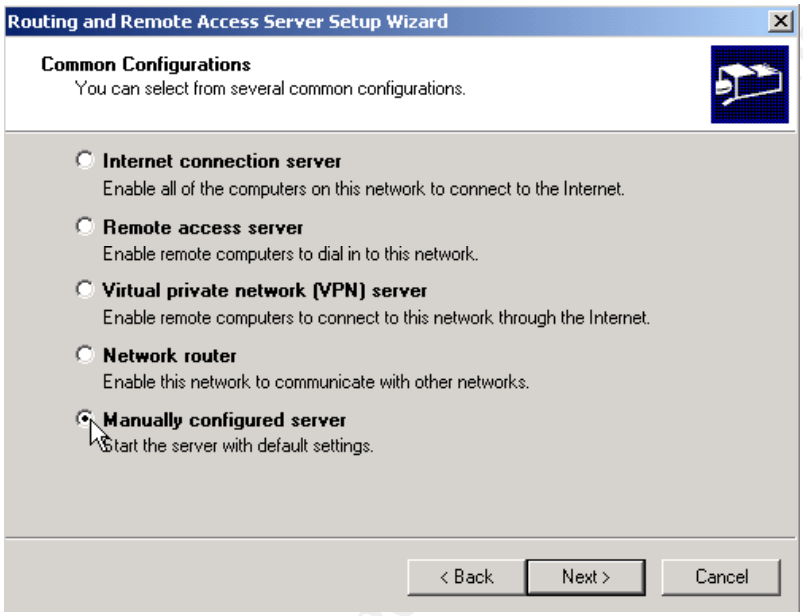
Start the Routing and Remote Access (RRAS) configuration by choosing **Start - Programs - Administrative Tools - Routing and Remote Access**. Right-click the server name and select **Configure and Enable Routing and Remote Access**.



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]

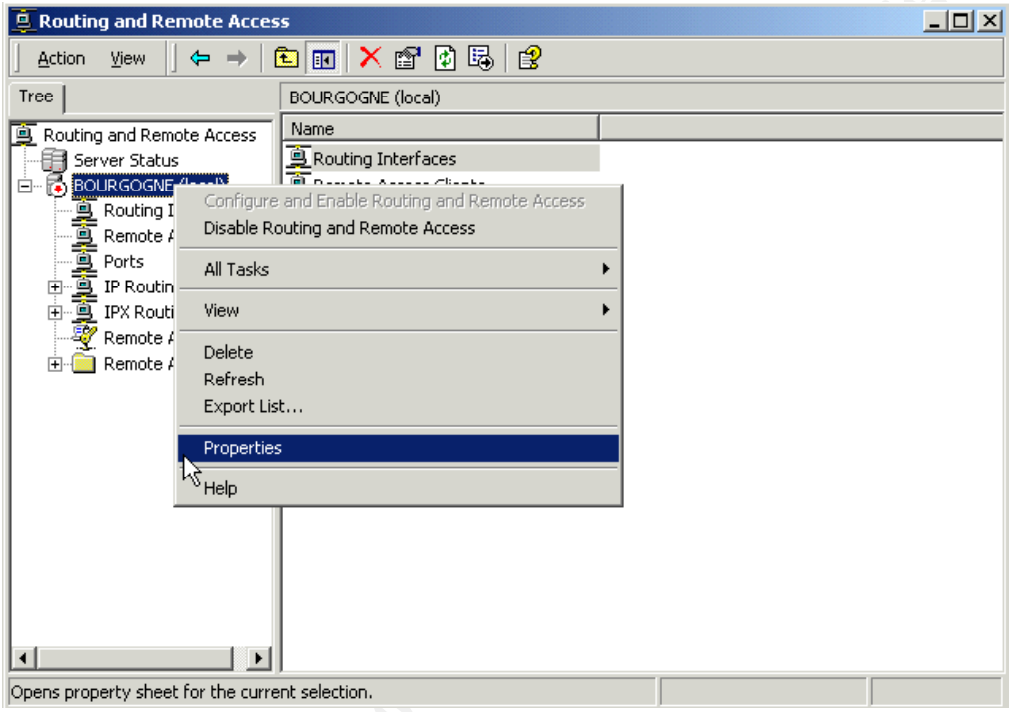


Click **Next** to continue, then click **Finish** to complete the RRAS wizard. Click **Yes** to start the RRAS which will then present you with the RRAS Microsoft Management Console (MMC) screen.

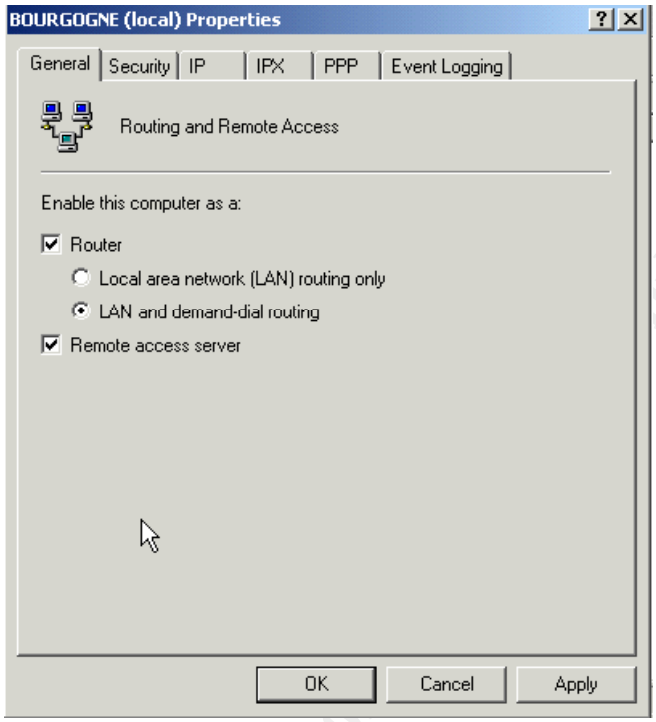
[1]This appears to be what I might call a "design bug." According to Microsoft Tech Support [9] this is "by design". According to Microsoft Consulting Services [8] this is due to a "bug".

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**.

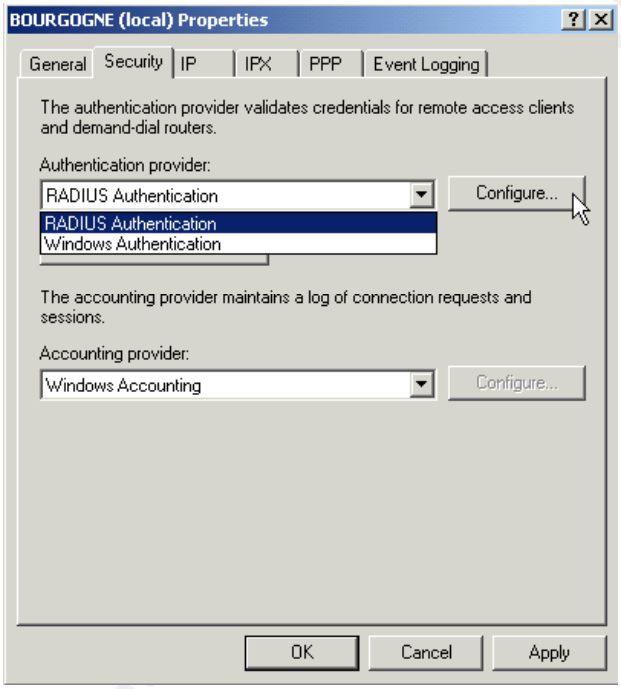


Click on the **General** tab and ensure **Router**, **LAN and demand-dial routing** and **Remote access server** are selected.



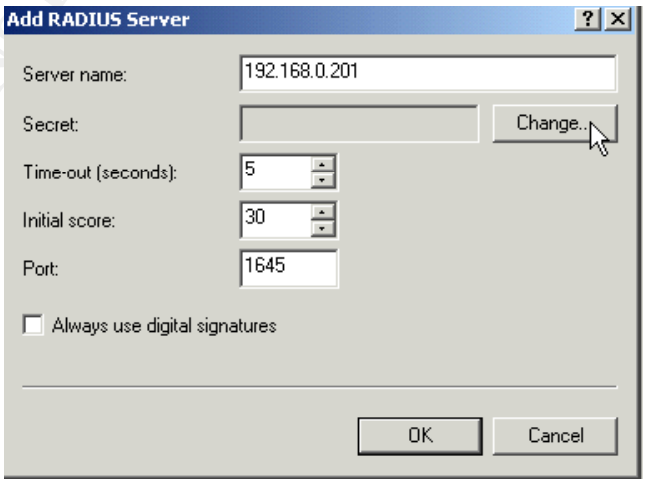
Click on the **Security** tab and select the **Authentication provider** you will use. You have a choice between Windows Authentication or RADIUS Authentication.

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.



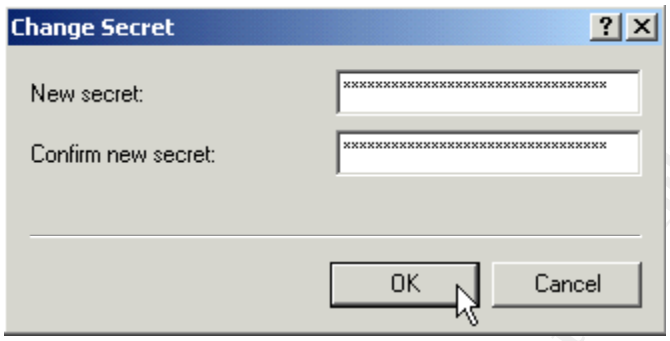
Click **Configure** to specify the RADIUS server configuration, then click **Add**.

Enter the RADIUS **Server name** or address and enter the UDP **Port** number used for communication[2].

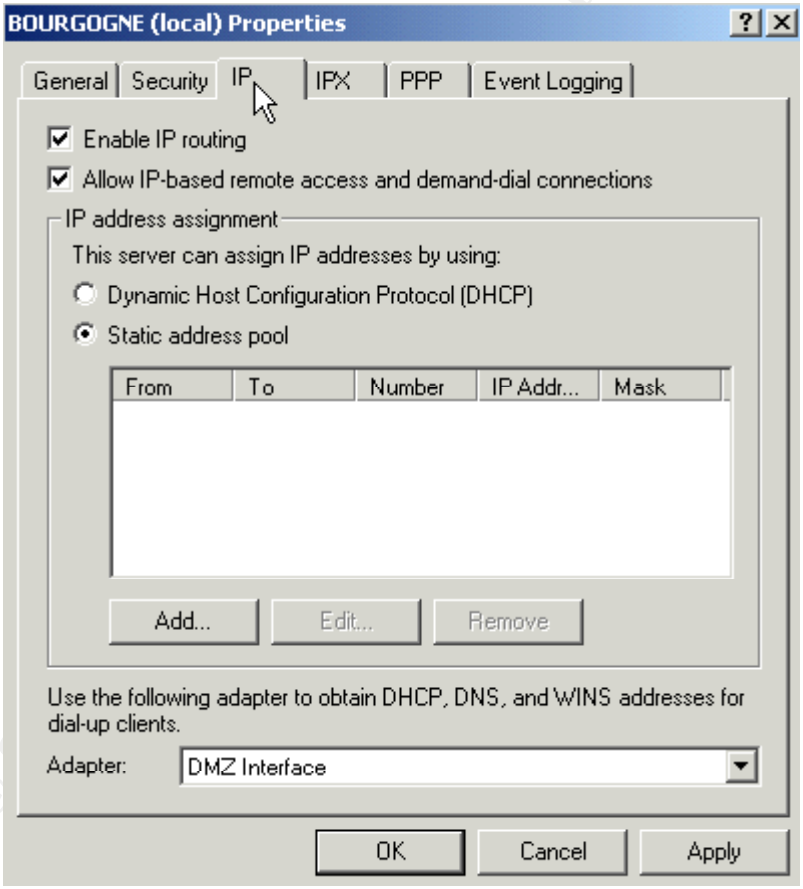


[2] You will also need to ensure any firewall between your VPN server and the RADIUS server allows traffic through this port.

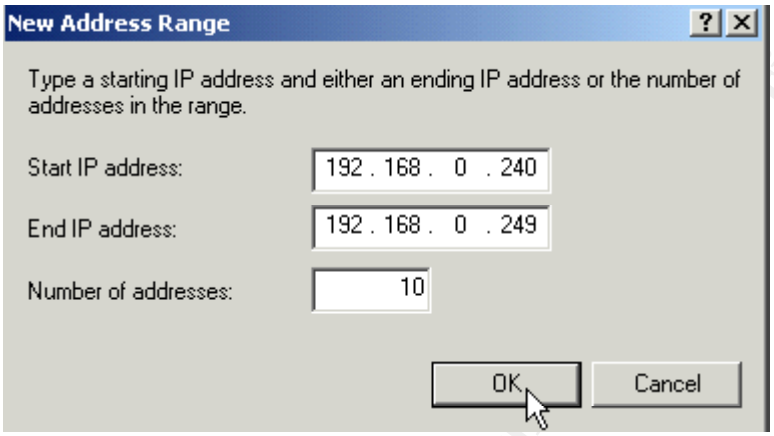
Click the **Change** button to enter the secret password that the VPN server will use to access the RADIUS server.



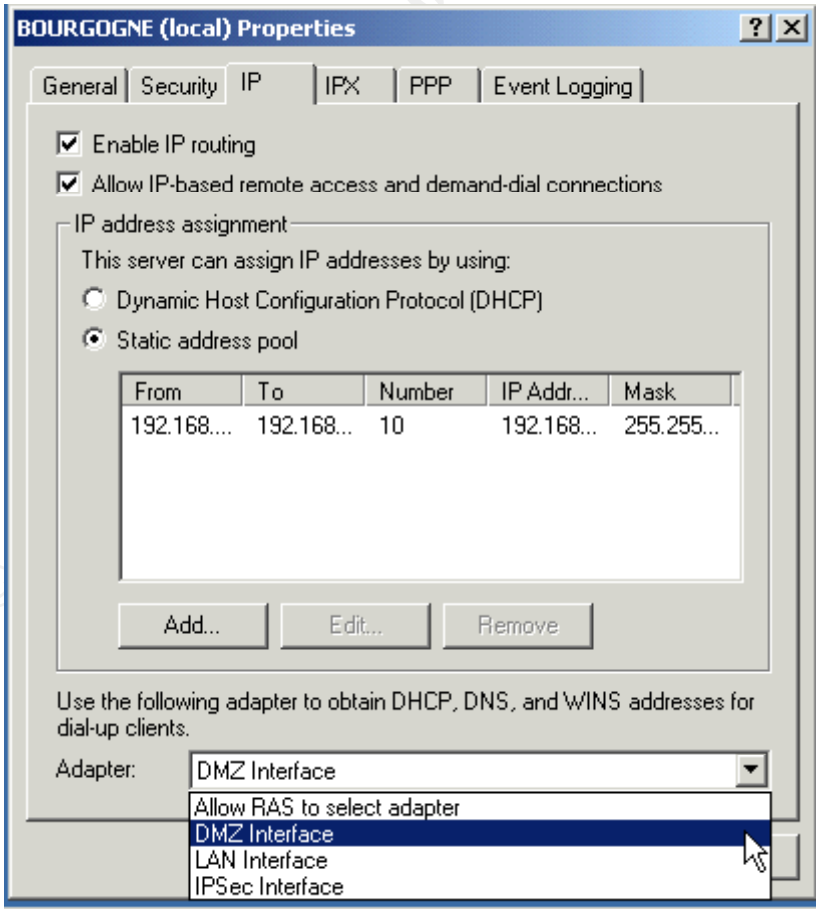
Click **OK** three times to continue, then click the **IP** tab and choose **Static address pool**.



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]

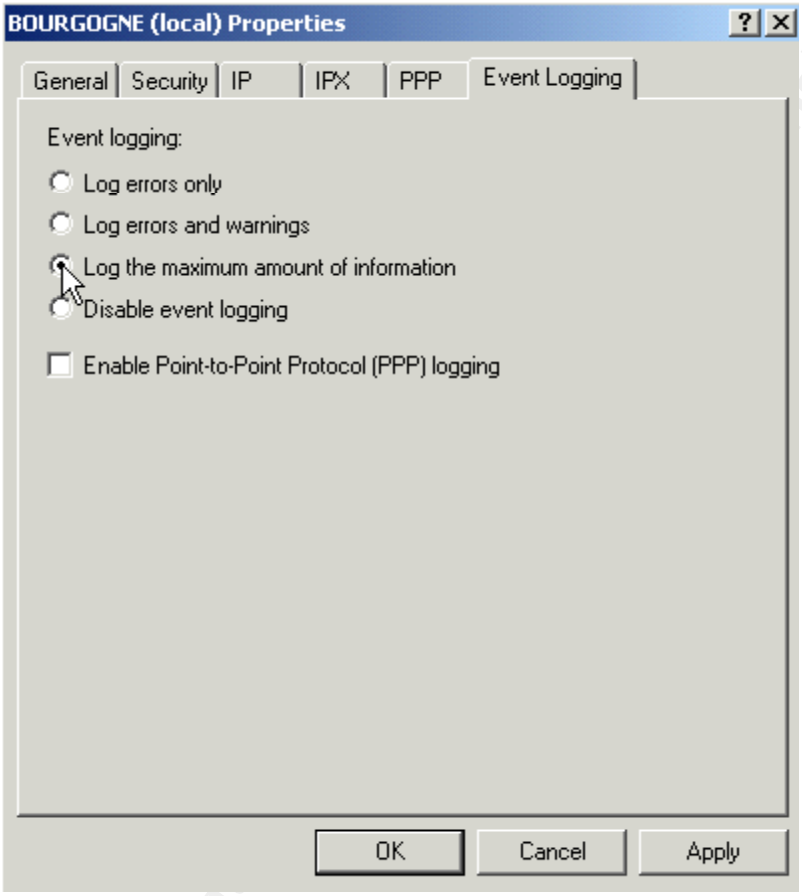


Select the adapter that is connected to your private or DMZ network that will be used for DHCP, DNS and WINS. In this case, we selected the DMZ interface which would be used were we to have any DHCP, DNS or WINS traffic.



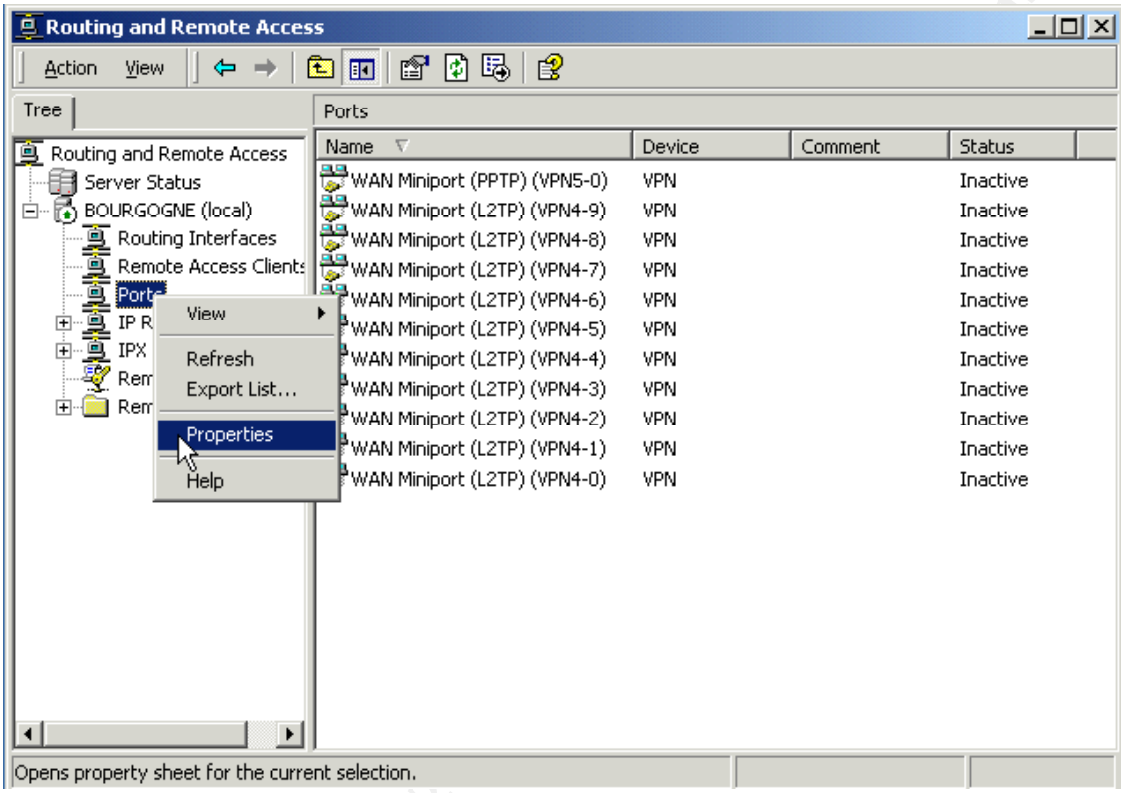
[3]If you will have more than 254 simultaneous users, you will need to span more than one subnet, and then create more than one pool.

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.

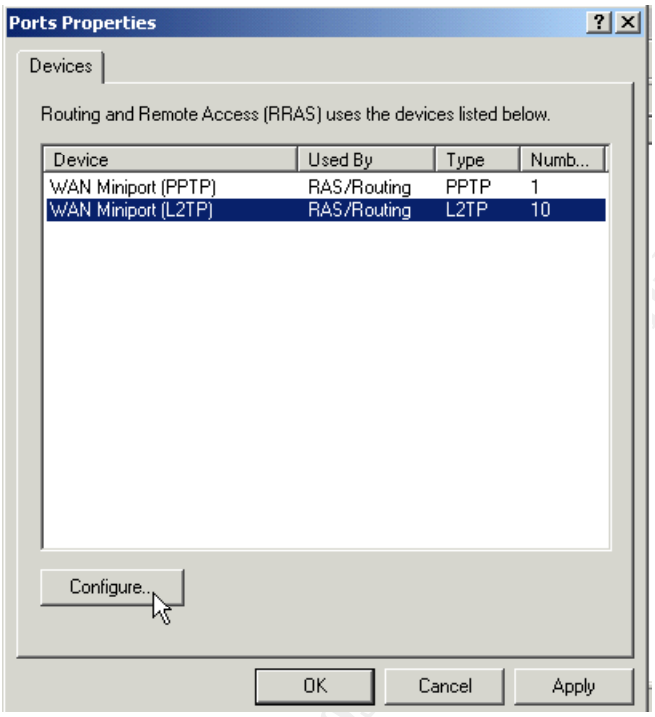


Configure VPN Ports

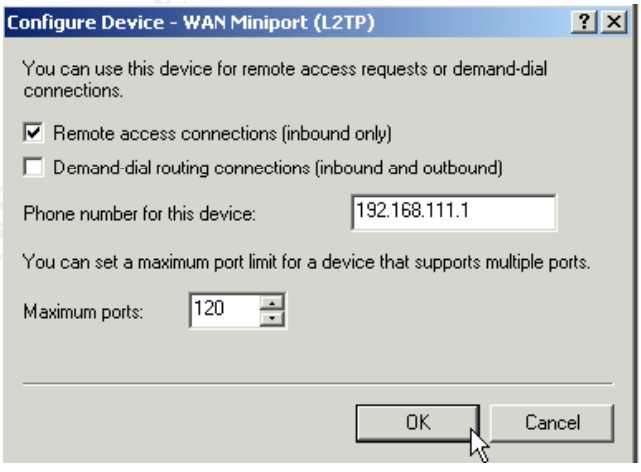
To configure the L2TP ports, right-click **Ports** and select **Properties** in the RRAS MMC.



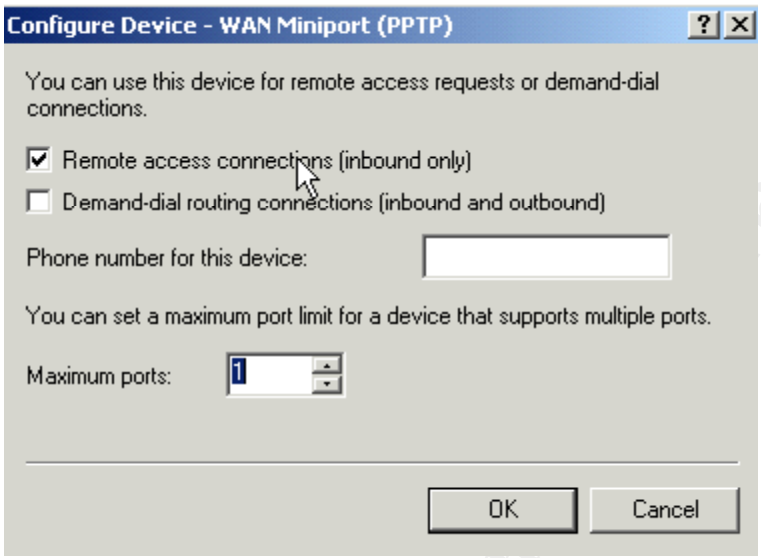
Select the **WAN Miniport (L2TP)** device and click **Configure** to continue.



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.



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).

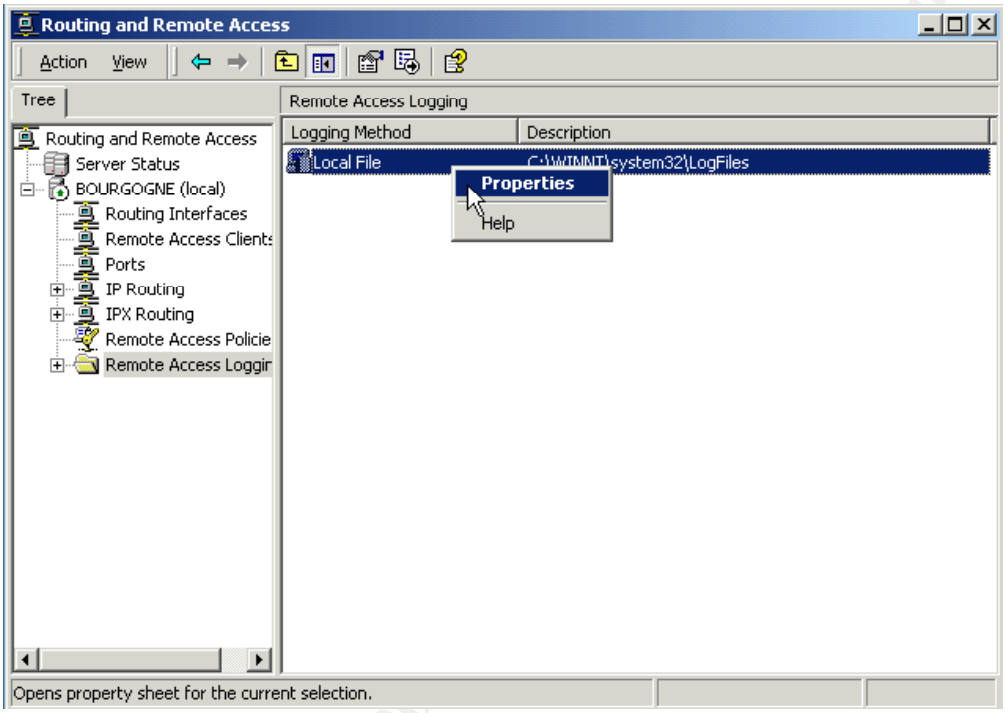


Click **OK** to continue and click **OK** again to exit the Port configuration utility. If you receive a message indicating current connections may be disconnected, click **Yes** to continue as there are no active current connections.

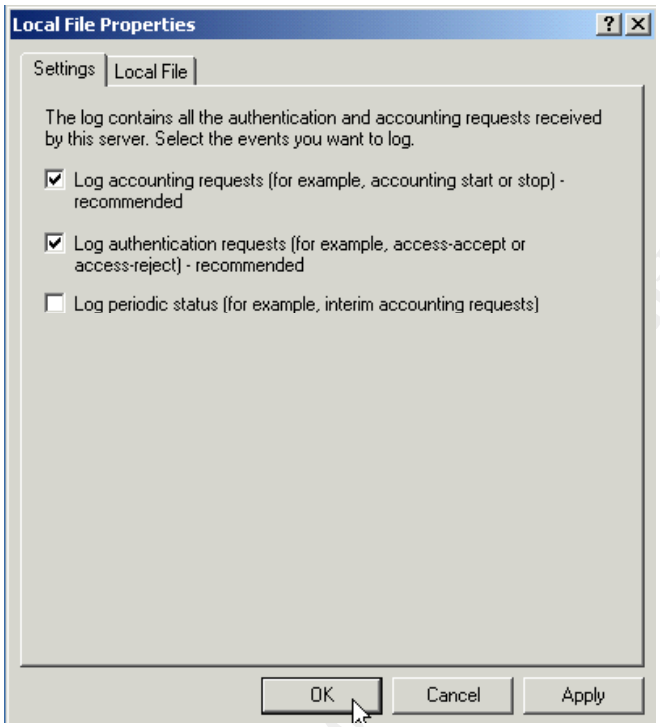
You will now see the L2TP ports listed in the right pane.

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**.

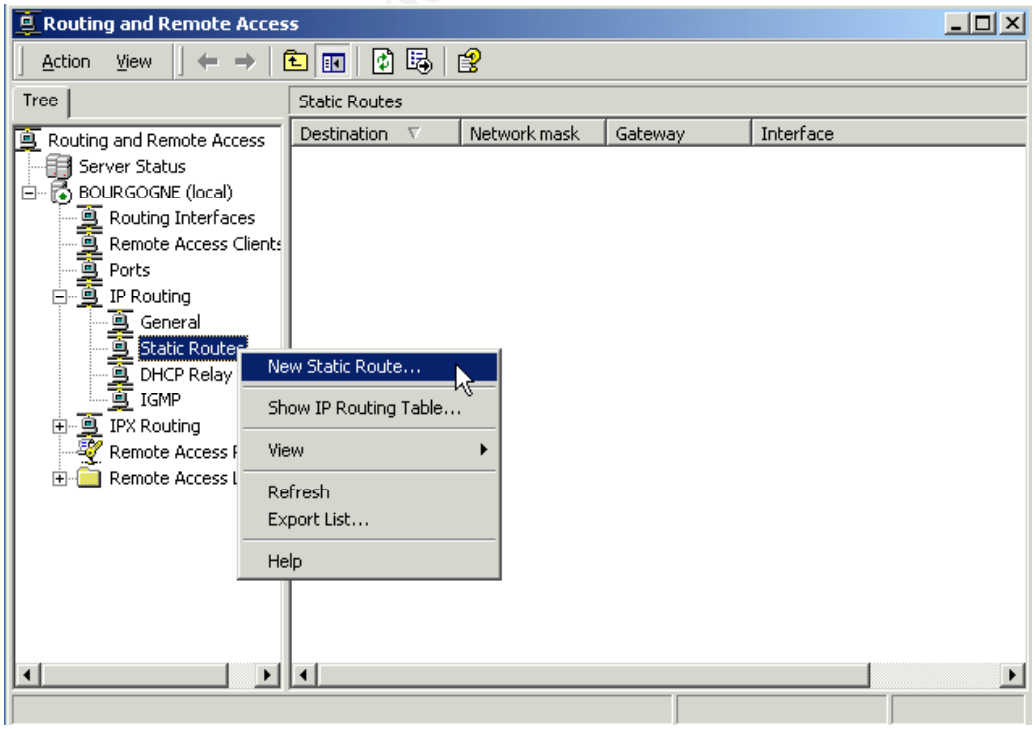


We wish to maximize logging, so select **Log accounting requests** and **Log authentication requests**, then click **OK** to continue.



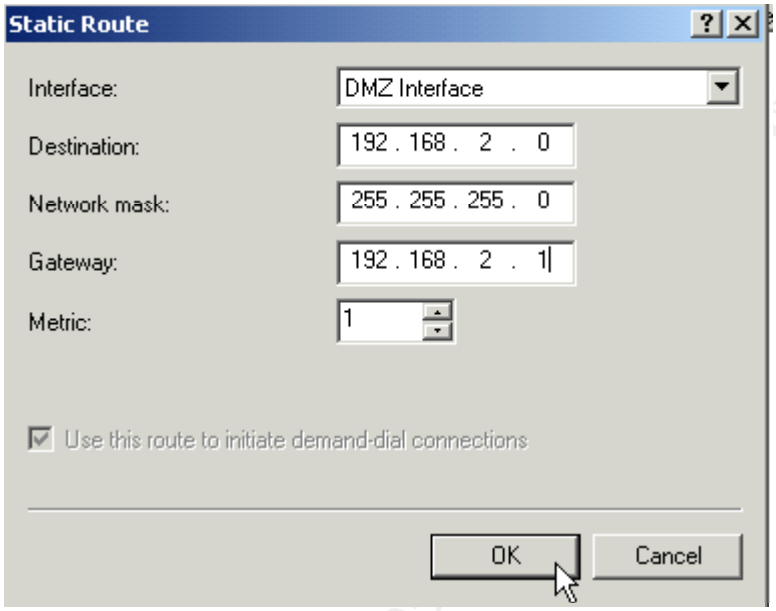
Configure Routing and Filters

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**.

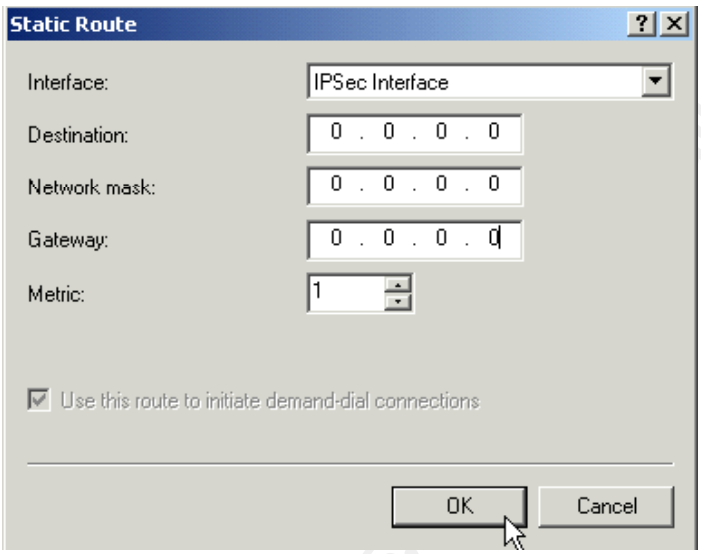


Select the internal interface you wish to configure. In this case, we select the "DMZ Interface," and

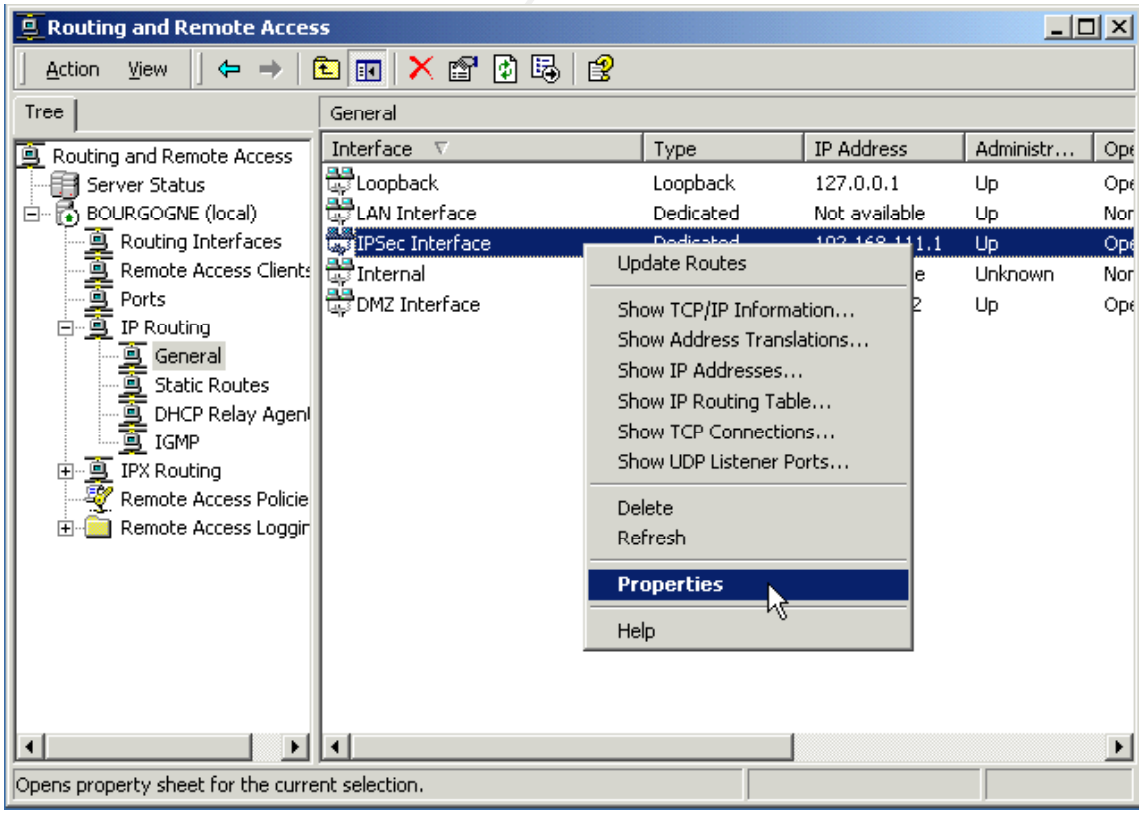
enter the **Destination** DMZ network 192.168.2.0, **Network mask** 255.255.255.0, and **Gateway** 192.168.2.1, with a **Metric** of 1.



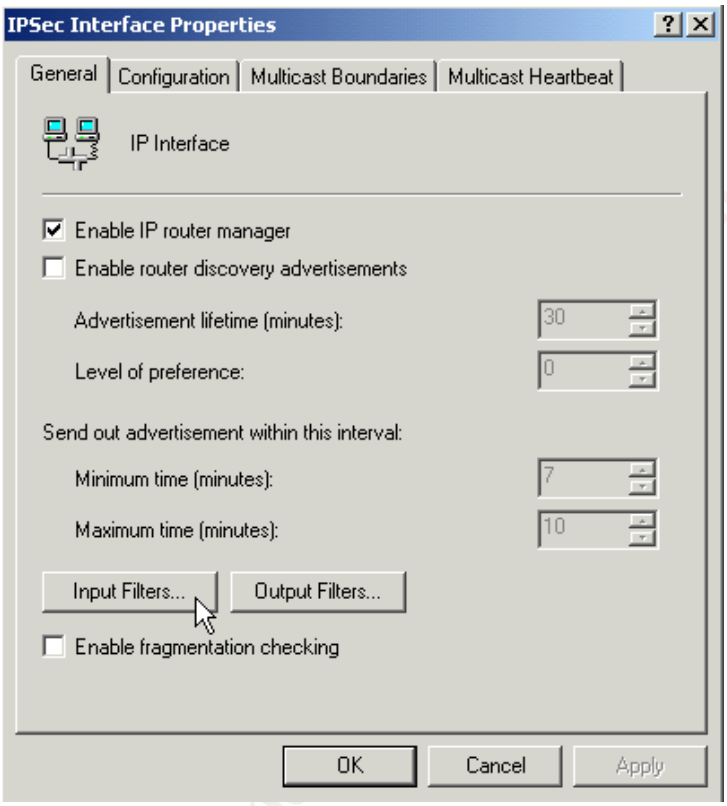
Click **OK** to continue, right-click **Static Routes** and select **New Static Route** again for your external Internet interface. In this case, we select the "IPSec Interface," **Destination** 0.0.0.0, **Network mask** 0.0.0.0, **Gateway** 0.0.0.0 and **Metric** 1 to enable clients to connect from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



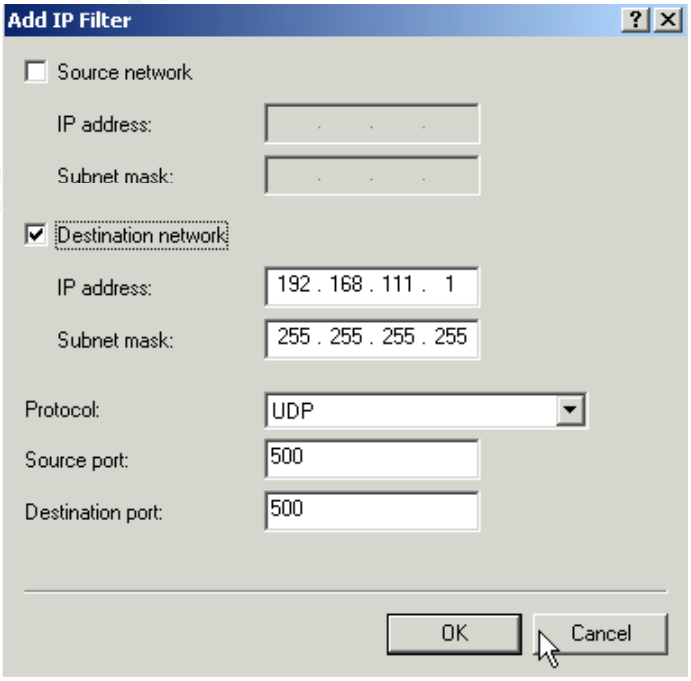
Click **OK** to continue. Click **General** under **IP Routing** in the left pane. In the right pane, right-click on the **IPSec interface** and select **Properties**.



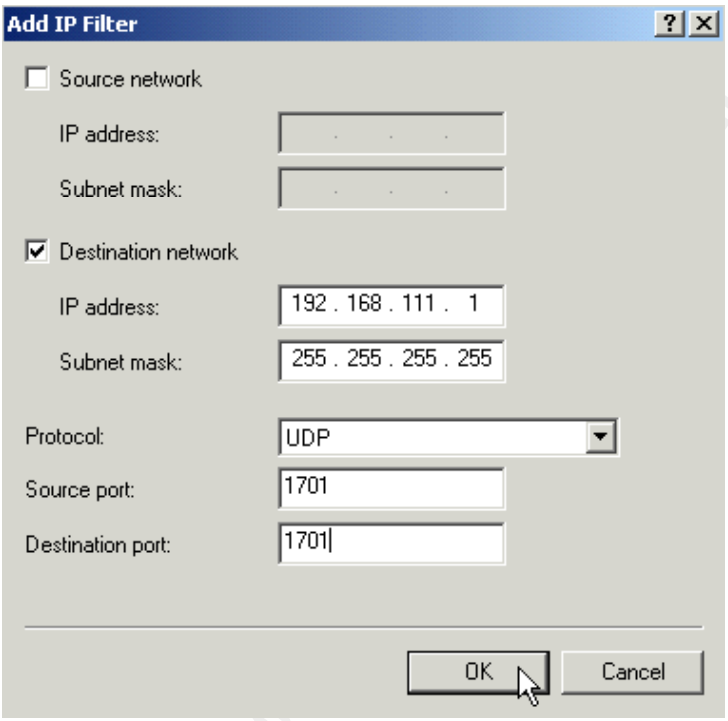
On the **General** tab, click **Input Filters**.



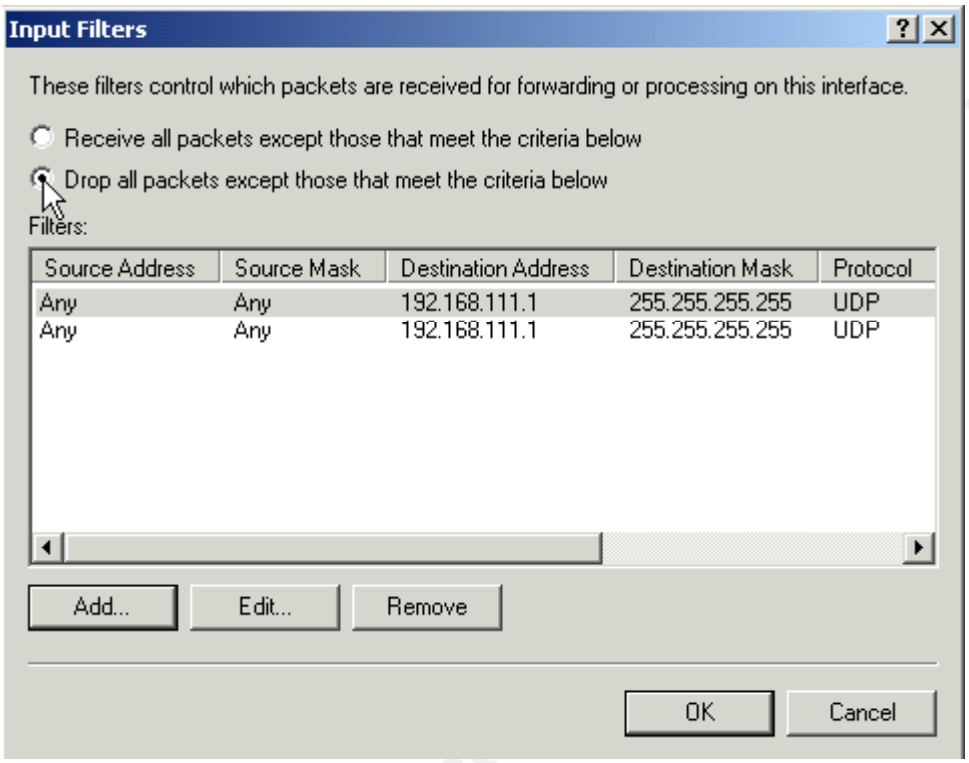
Click **Add** in the Input Filters dialog box, then select **Destination network**. Enter the Internet IP address and the subnet mask 255.255.255.255, select the UDP Protocol, and enter **Source** and **Destination ports** 500 to allow ISAKMP traffic into the VPN server.



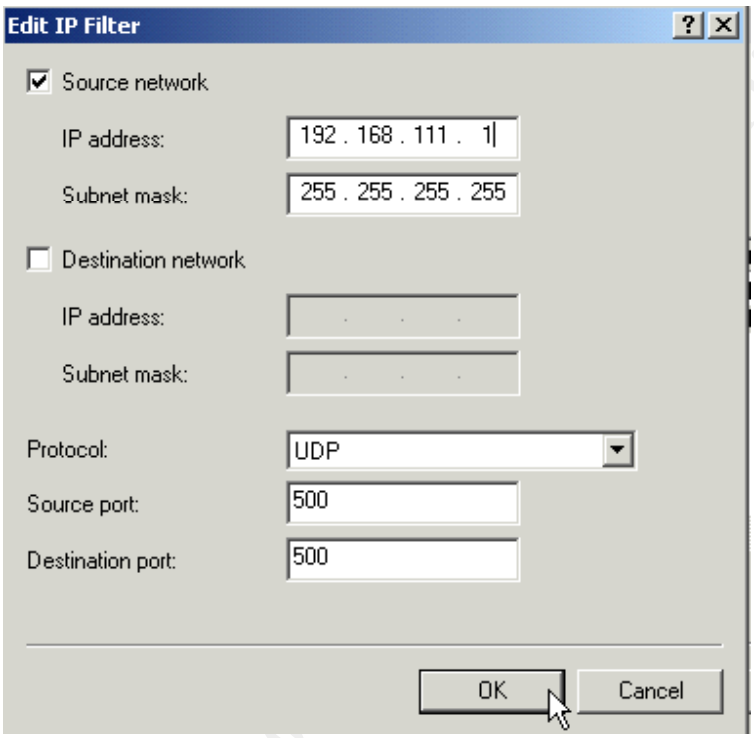
Click **OK** to continue. Click **Add** in the **Input Filters** dialog box, then select the **Destination network** again. This time, enter UDP **Source** and **Destination ports** 1701 to allow L2TP traffic into the VPN server.



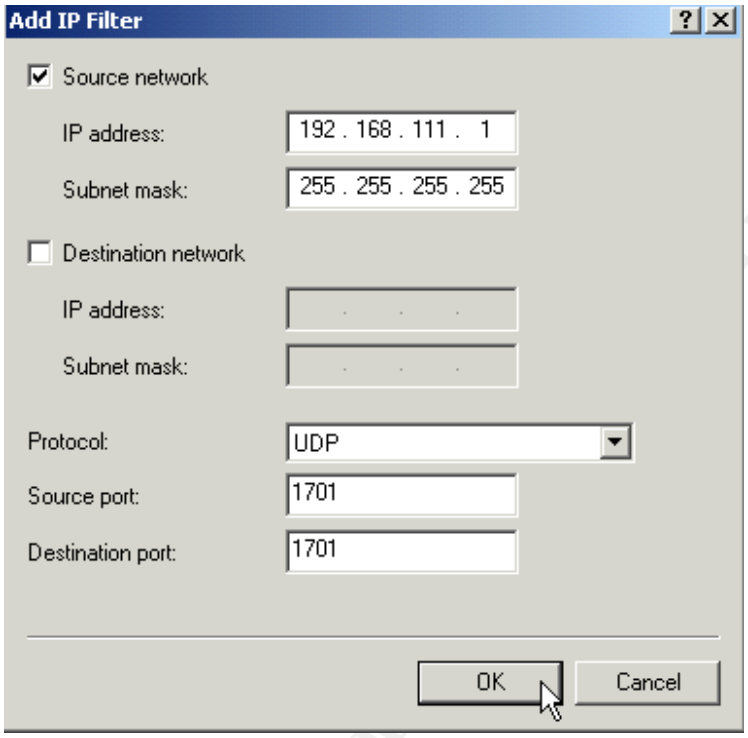
In the **Input Filters** dialog box, select **Drop all packets except those that meet the criteria below**, then click **OK**.



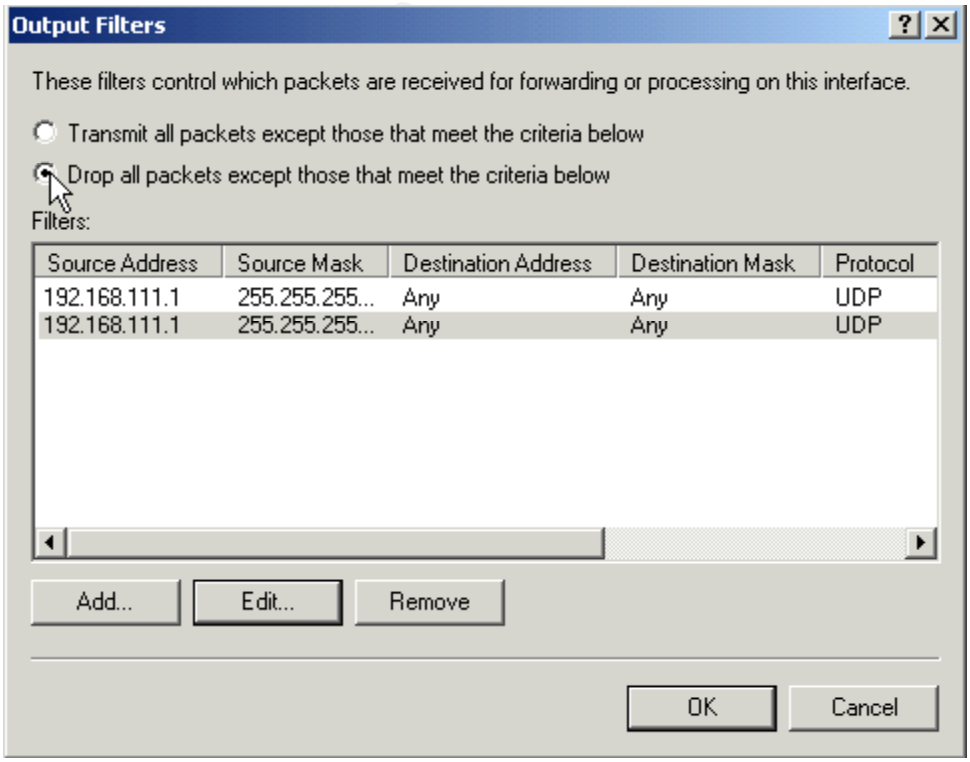
On the **General** tab, click **Output Filters**, then click **Add**. Select **Source network**, and enter the Internet **IP address** and a **Subnet mask** of 255.255.255.255. Select the UDP **Protocol** and enter **Source** and **Destination ports** 500.



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.

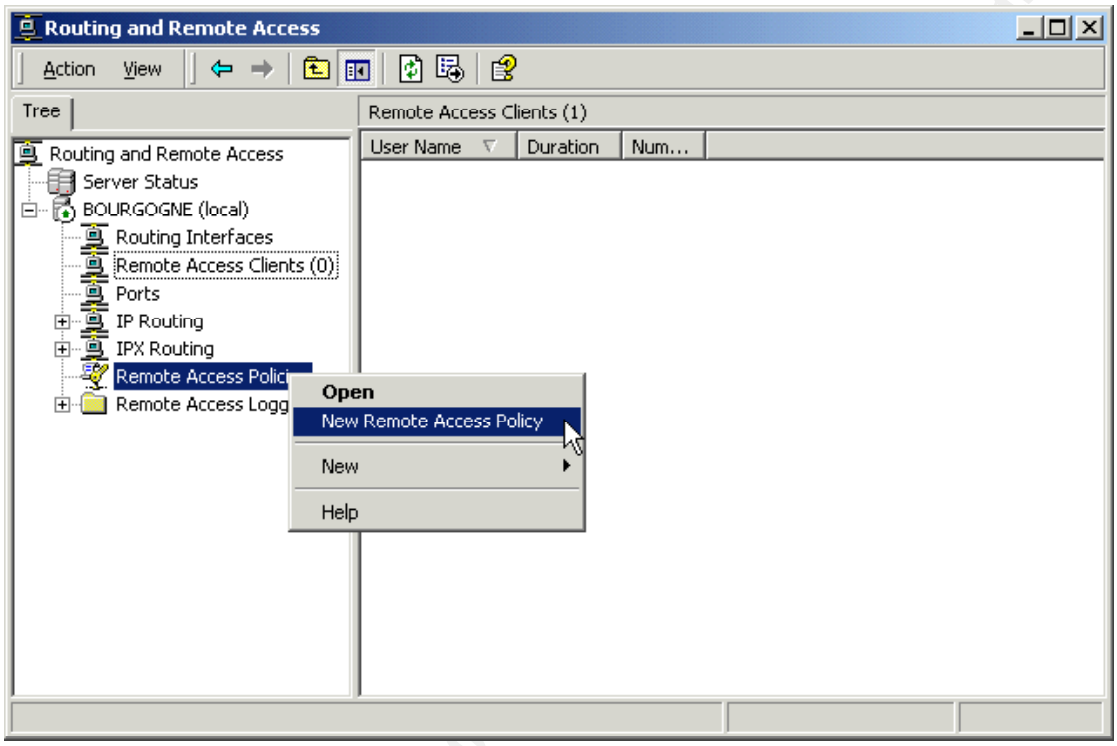


In the **Output Filters** dialog box, select **Drop** all packets except those that meet the criteria below, then click **OK**.

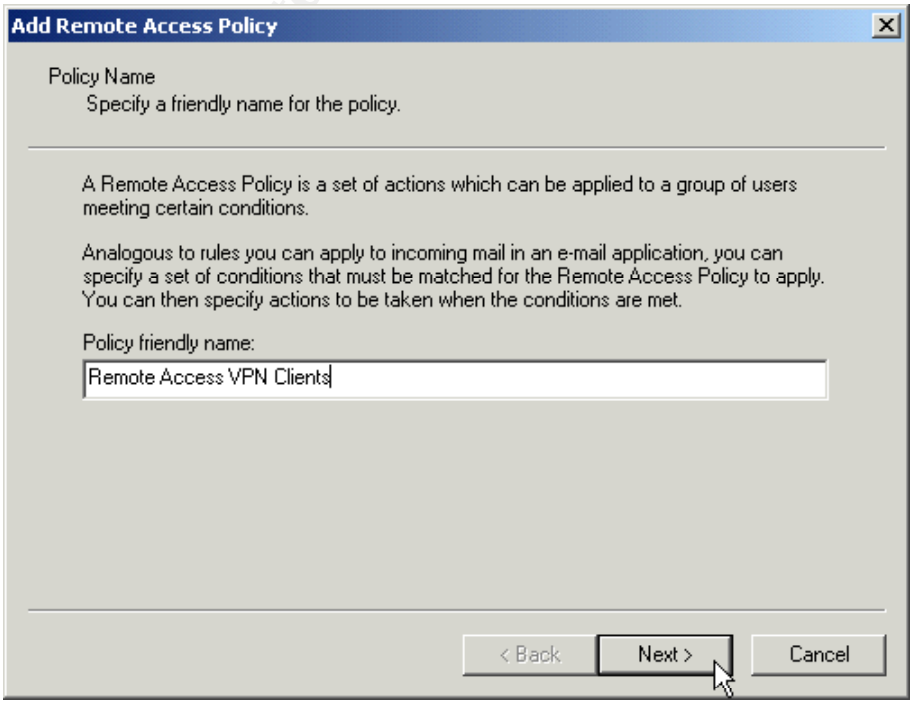


Configure Local Policy

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



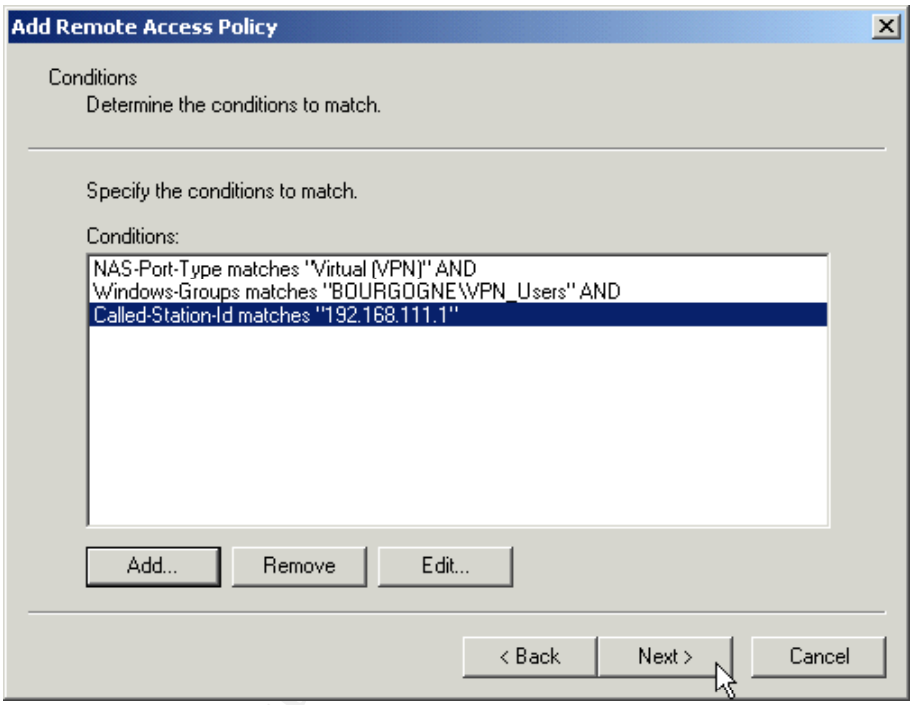
In the following window, provide a name for your policy.



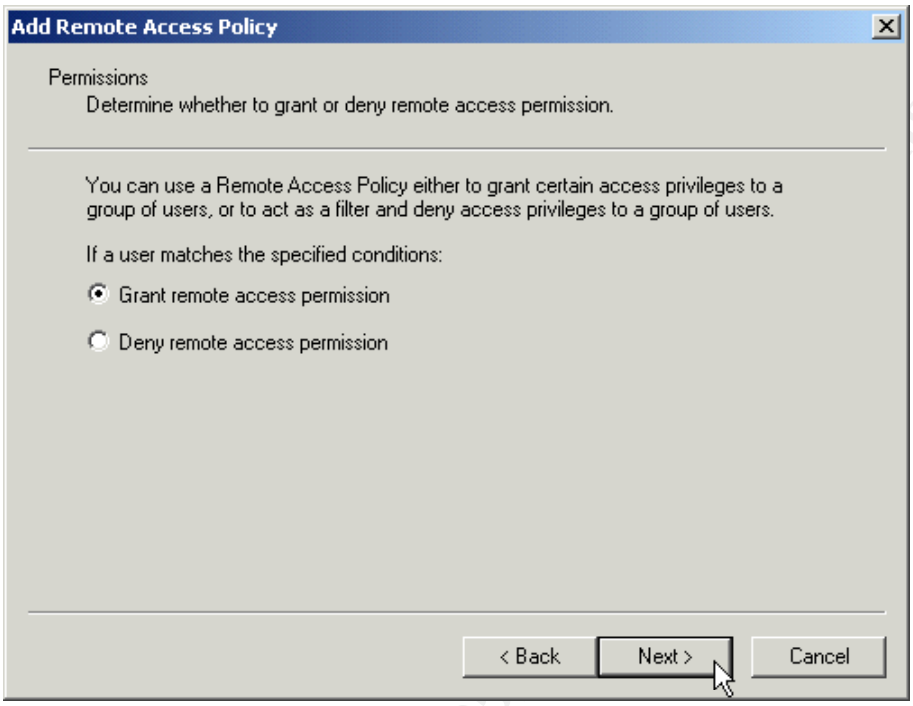
Click **Next** to continue.

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

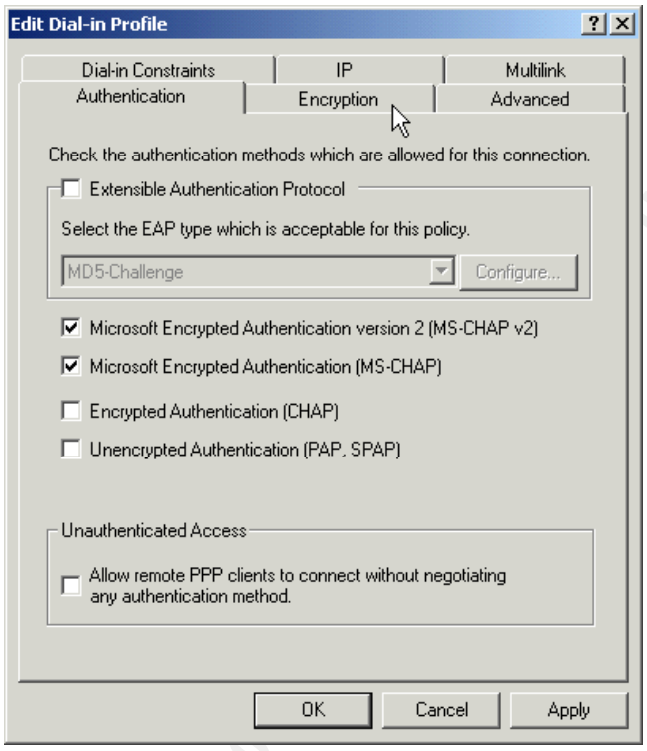
Attribute	**Value**
NAS-Port-Type	Virtual(VPN)
Windows-Groups	VPN Users
Called-Station-ID	(Internet IP address of VPN server)



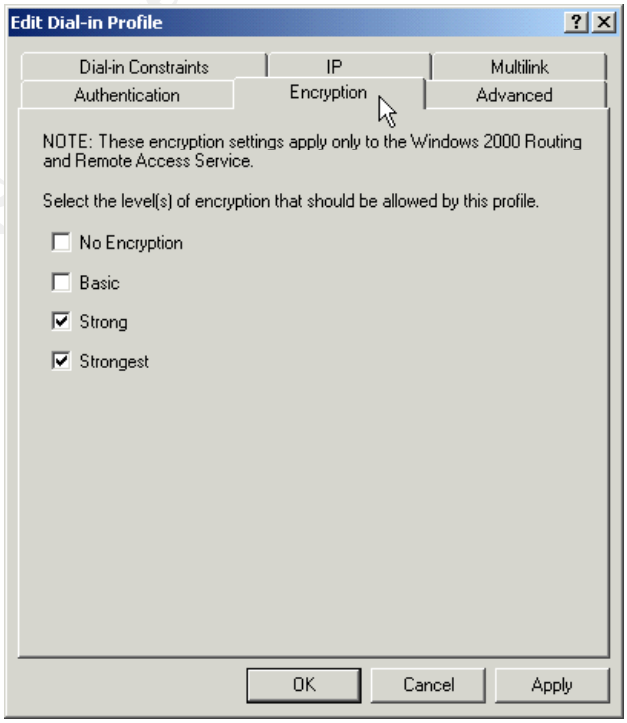
Click **Next** to continue. Select **Grant remote access permissions**.



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



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



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

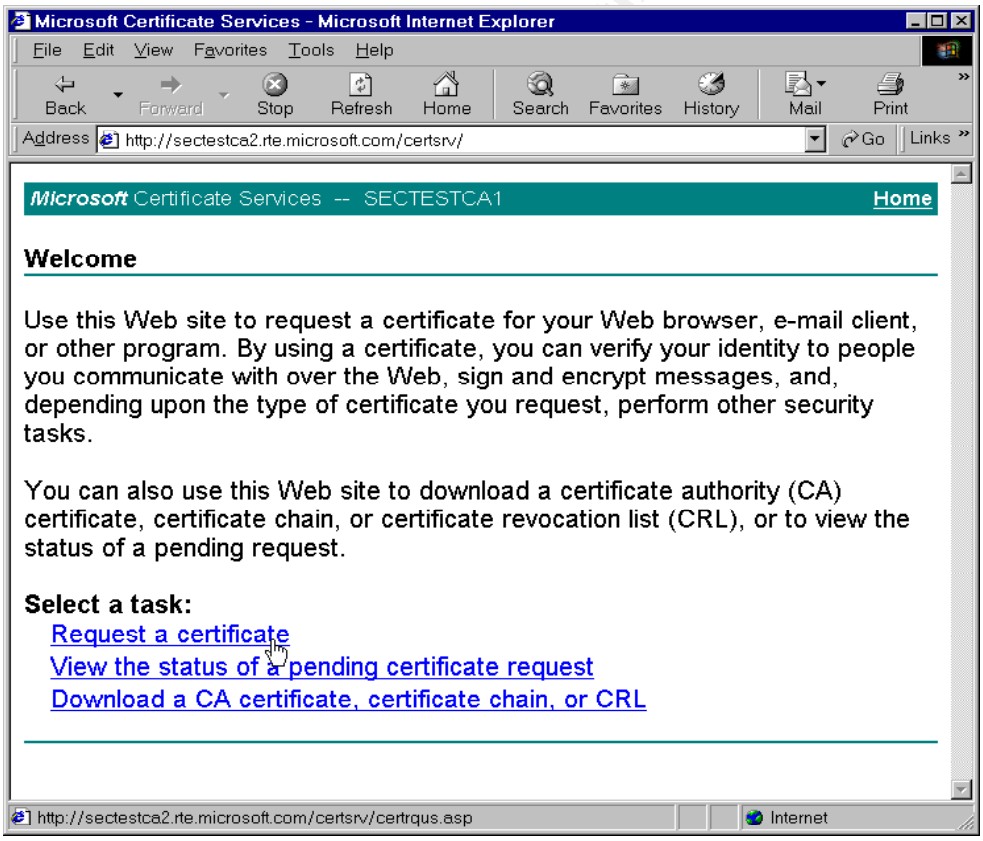
Obtain and Install a Certificate

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.

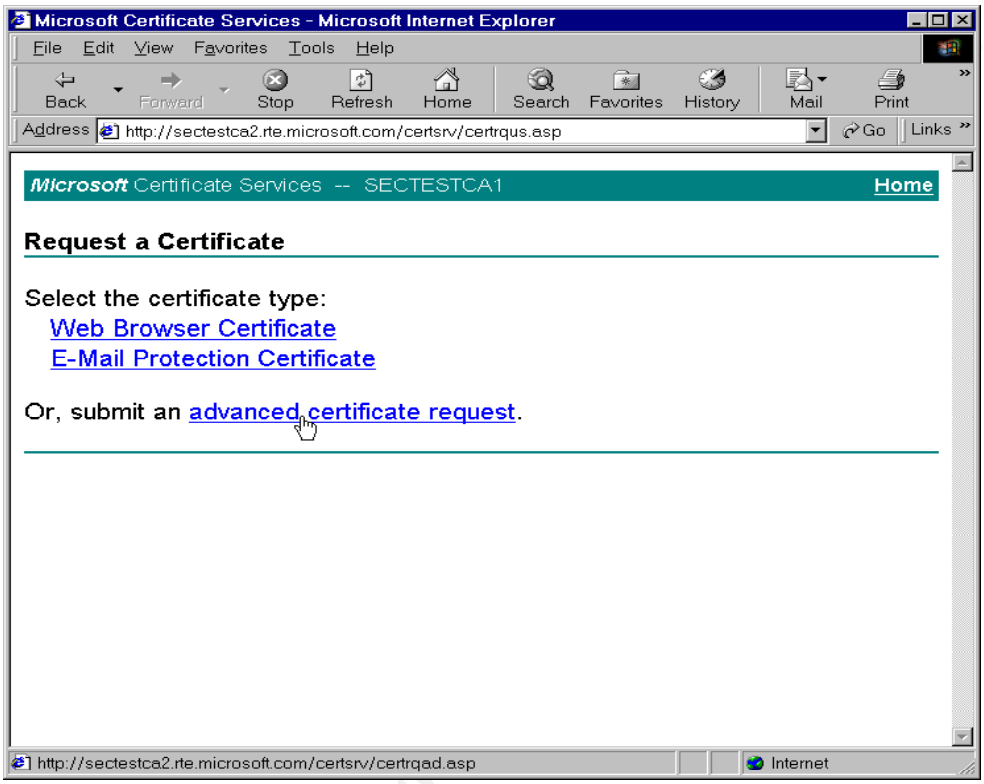
You may obtain one from Microsoft's certificate authority via the Internet at:

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

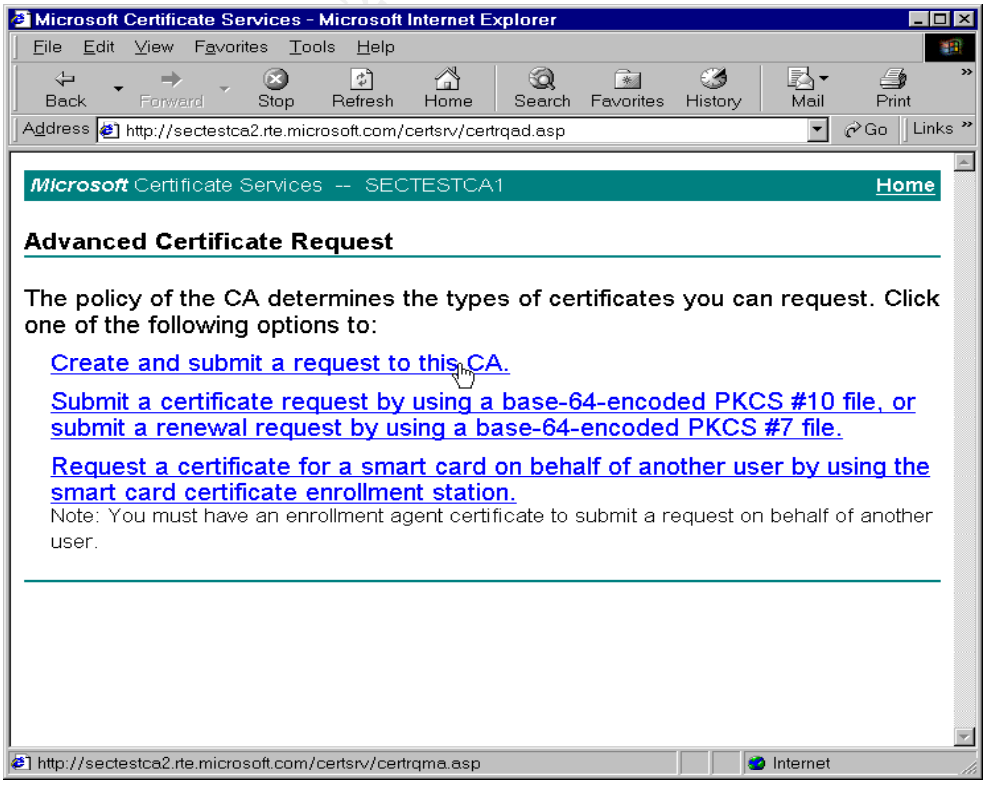
At the opening page, select **Request a certificate**.



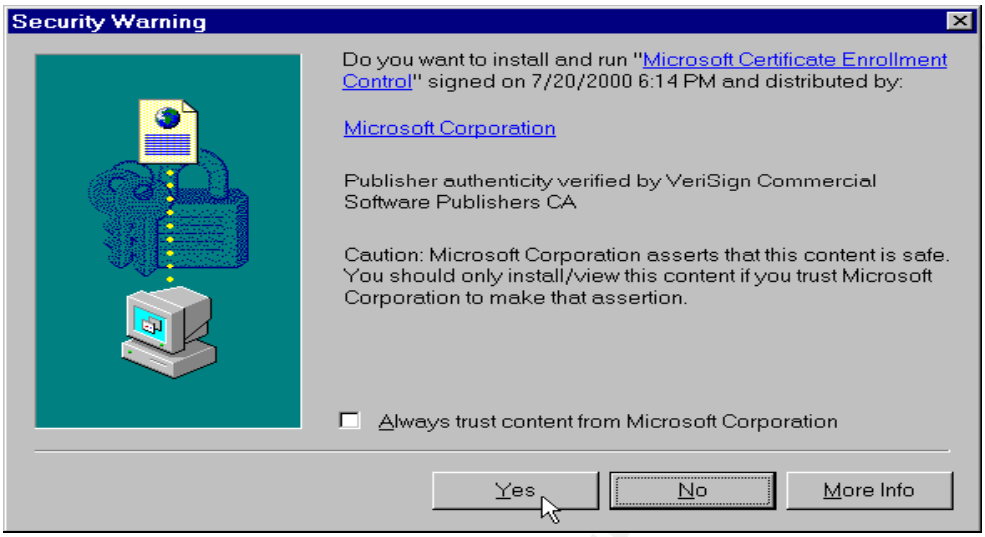
At the next screen, select **advanced certificate request**.



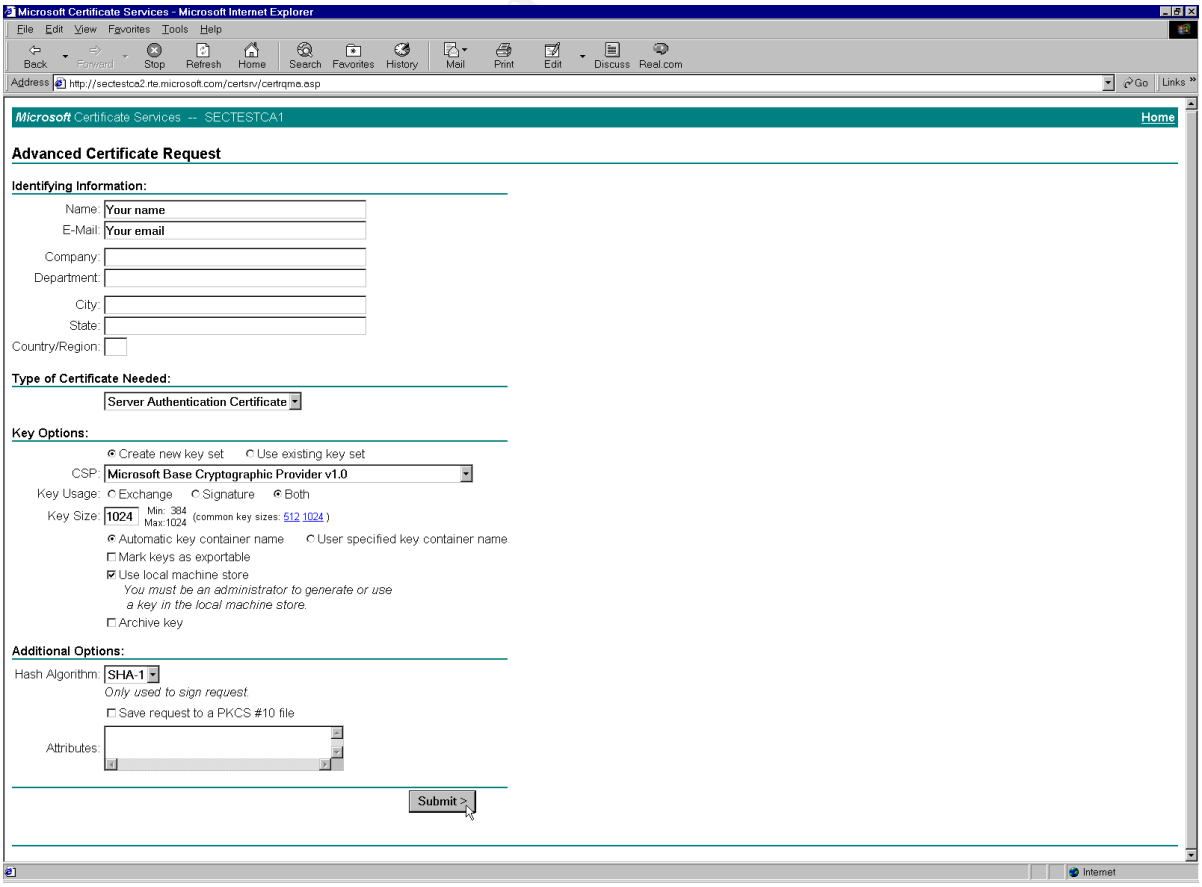
At the next screen, select **Create and submit a request to this CA**.



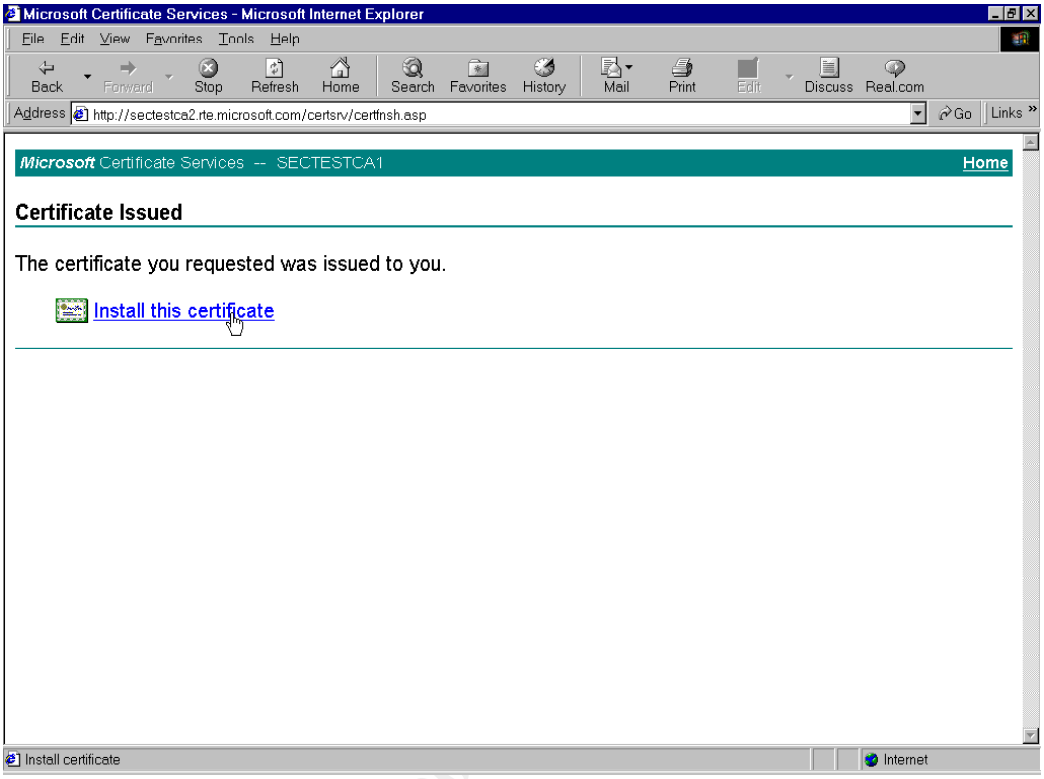
If you receive a **Security Warning**, you must click **Yes** to continue.



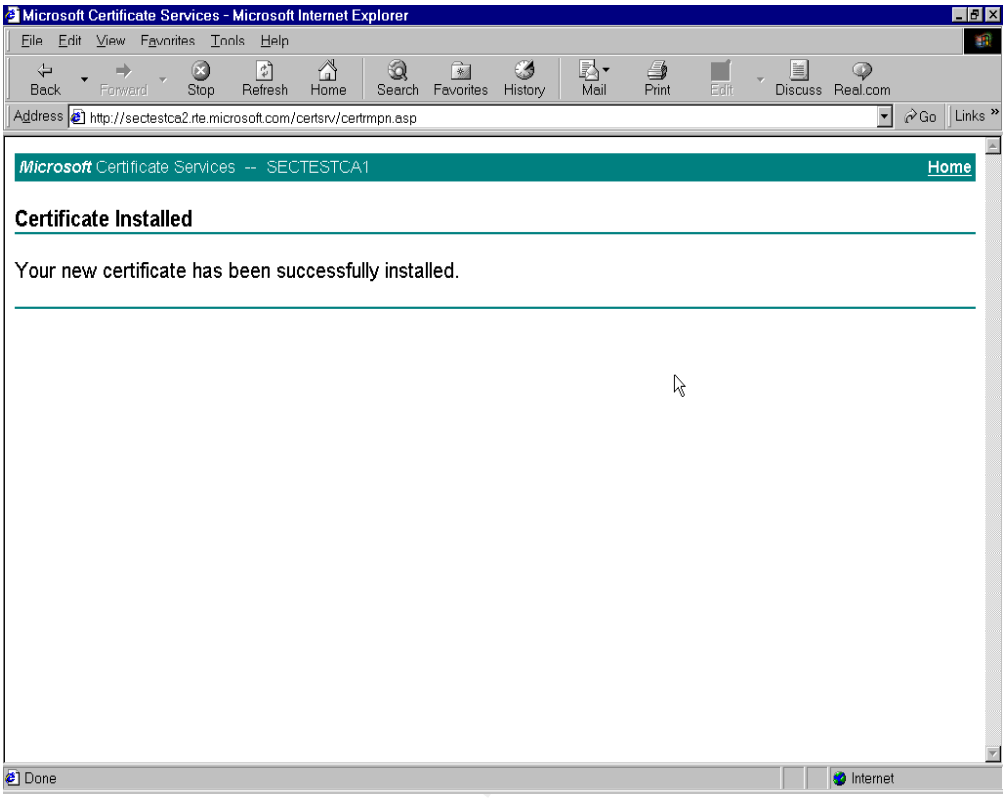
At the next screen, enter your identifying information and select the **Type of Certificate Needed**. In this case, we want a **Server Authentication Certificate**. Under **Key Options**, select **Create new key set**, **Microsoft Base Cryptographic Provider v1.0**, a **Key Size** of 1024, and check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



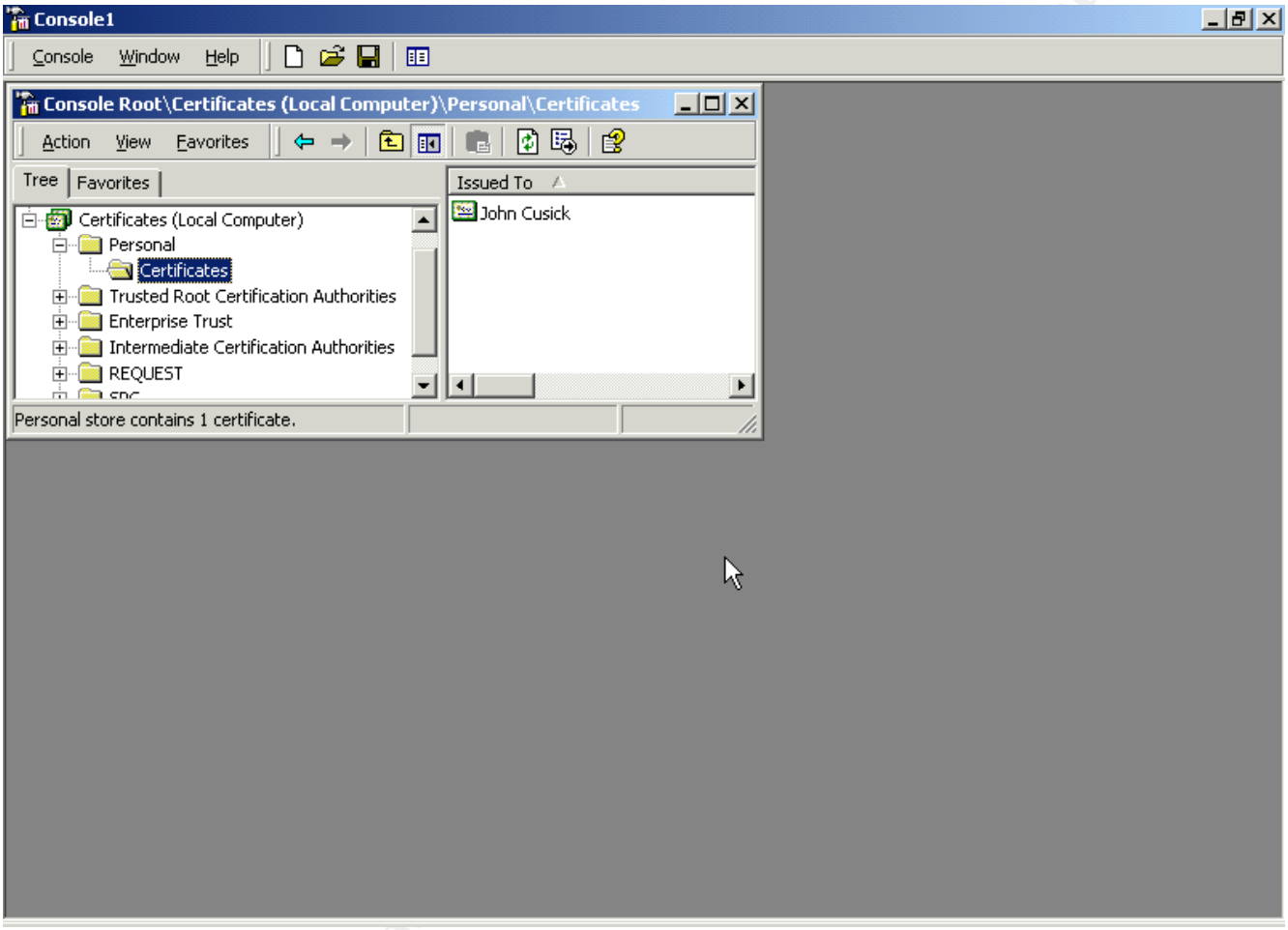
At the **Certificate Issued** screen, select **Install this certificate**.



You should then see the following:

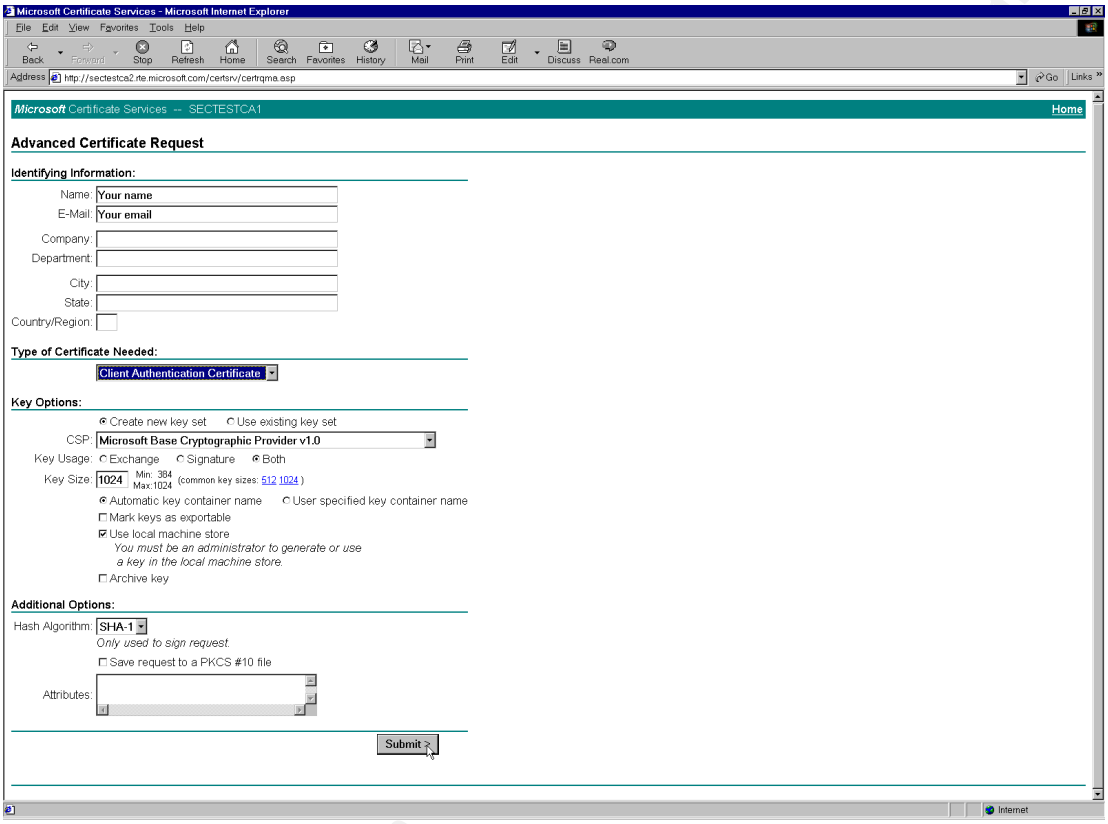


You can verify your certificate is installed by starting the MMC and using the **Certificates - Local Computer** snap-in. The newly installed certificate should appear under the **Personal - Certificates** subfolder.



Client Configuration

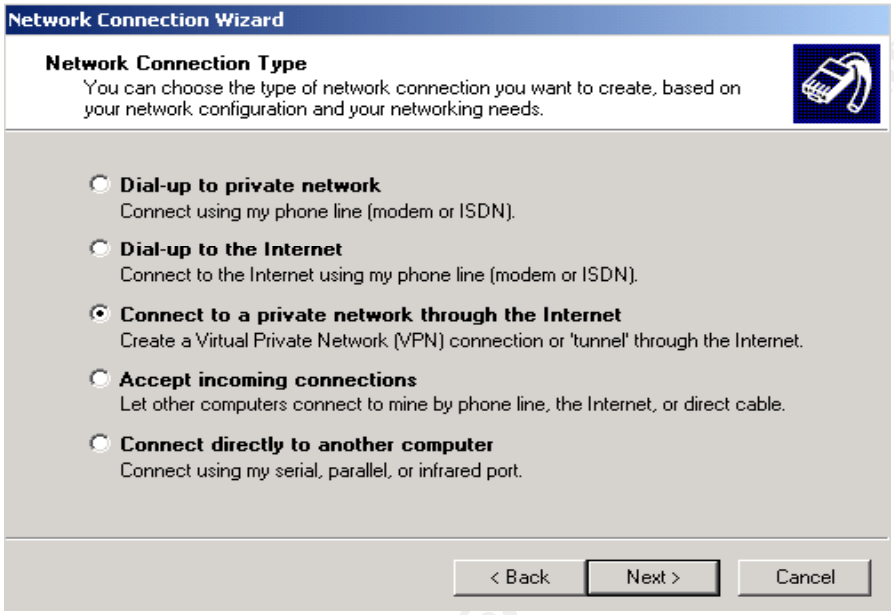
Each client then needs to follow a similar process to install a **Client Authentication Certificate**.



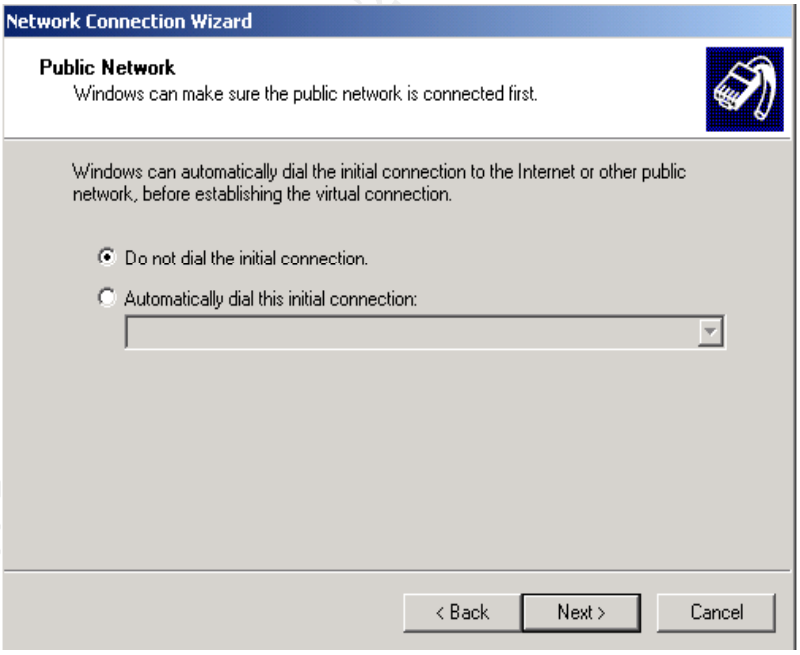
On each client computer, create a new "dial-up" Internet connection. Using **Start - Settings - Network and Dial-up Connections**, start the **Make New Connection** wizard.

Click **Next** to continue.

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

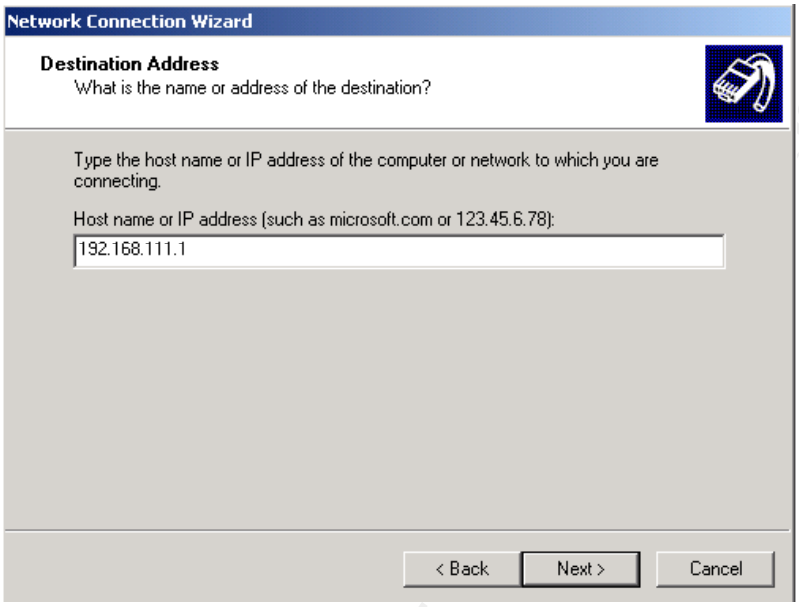


Click **Next** to continue. Select the method by which the client will access the Internet.[4]



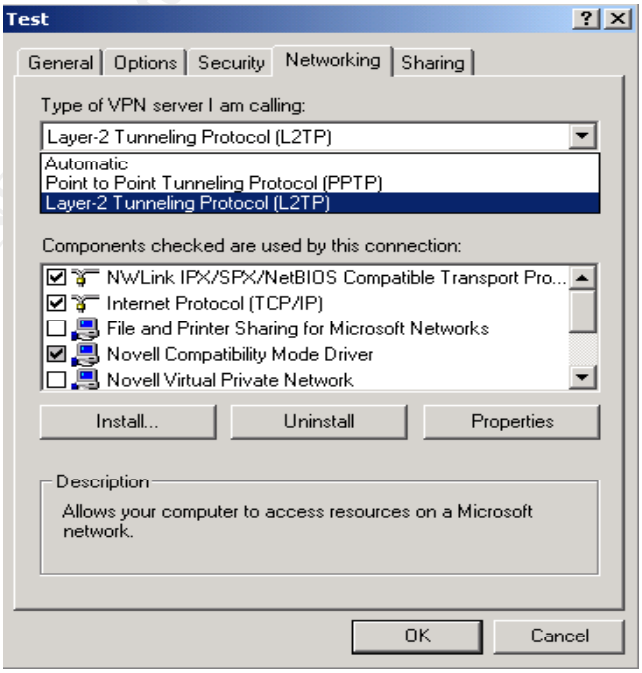
[4]Remote clients attempting to access the VPN server from behind a firewall or other device doing Network Address Translation (NAT) will likely not succeed. This is because IPSec on the client end replaced the original header. Thus, the responding packets from the VPN server cannot find their way back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

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



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.



Click **OK** to save the configuration.

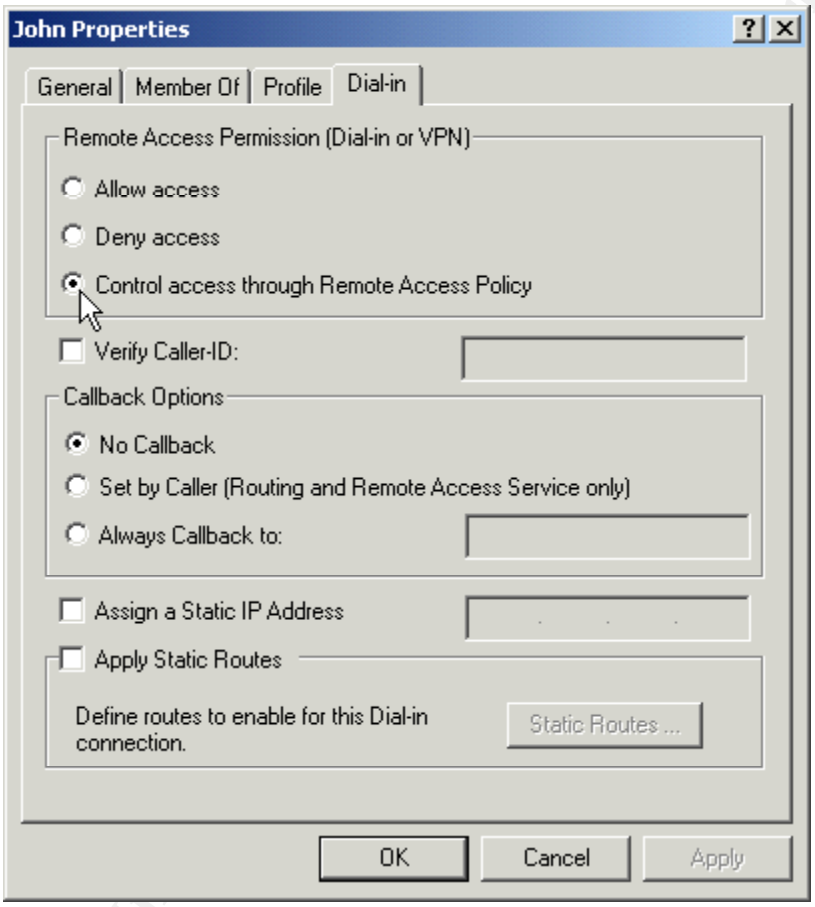
It should be noted here that some knowledgeable users may turn off IPSec in an effort to speed up their connections. This may be determined by examining the following key in the client computer's registry:

```
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

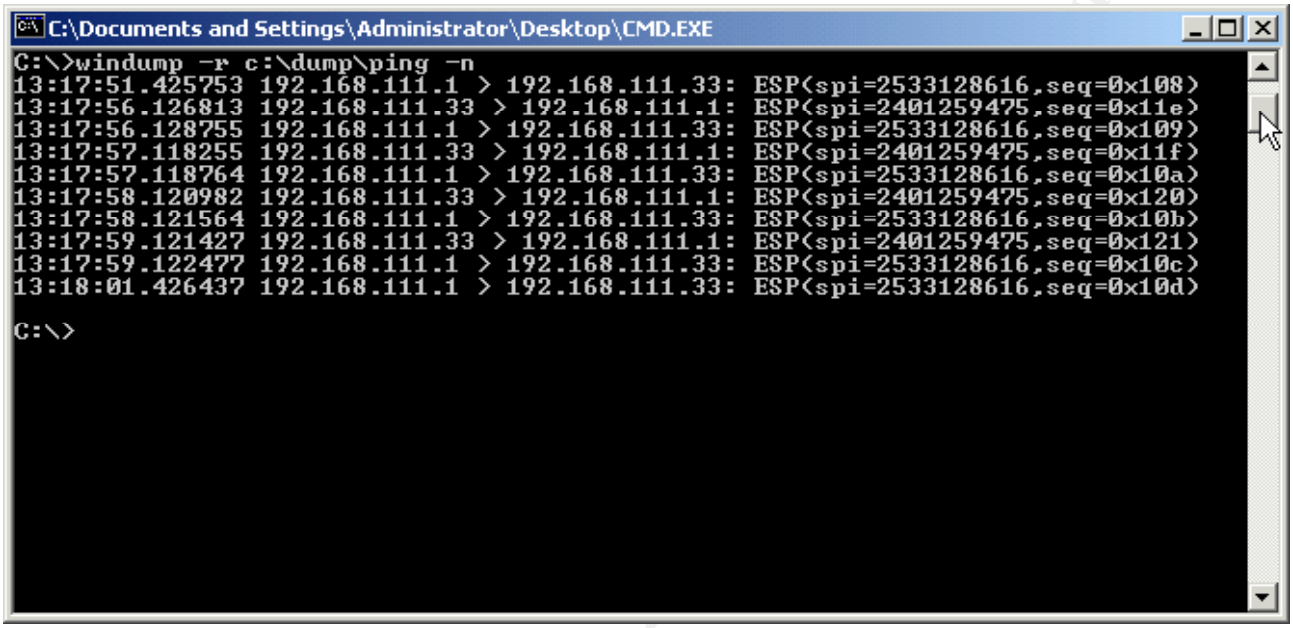
On your Radius server, domain controller, or wherever your user and group accounts are maintained, establish **Dial-in** permissions for each VPN user. For each user that is allowed VPN access, set the **Remote Access Permission** on the **Dial-in** tab as **Control access through Remote Access Policy**.



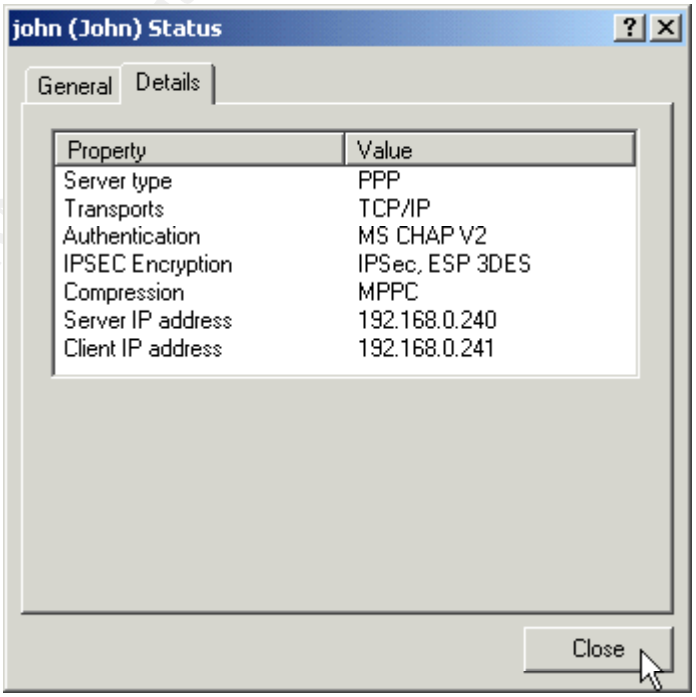
Create a VPN Users group and add each VPN user to it.

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.



Securing the server as a bastion host

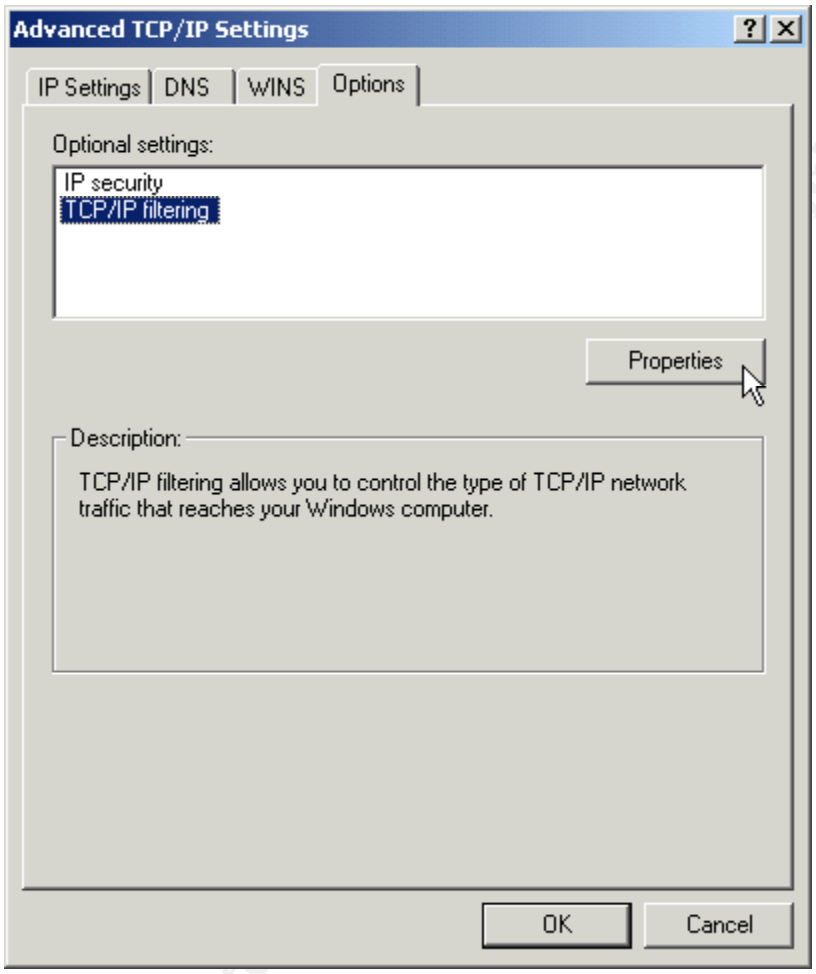
Having installed the VPN server and verified it works, we now turn to further securing the server to protect it in a public environment.

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.

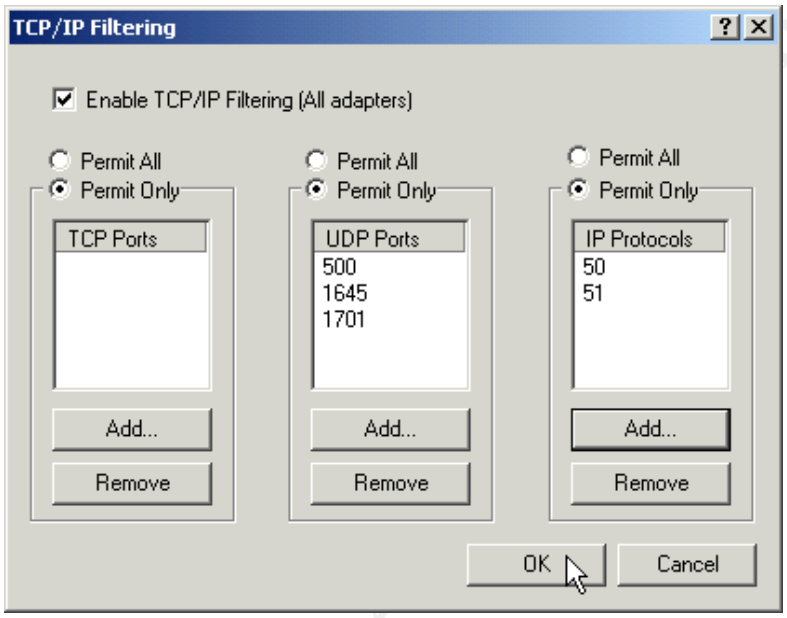
Configure TCP/IP Security Settings

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**.

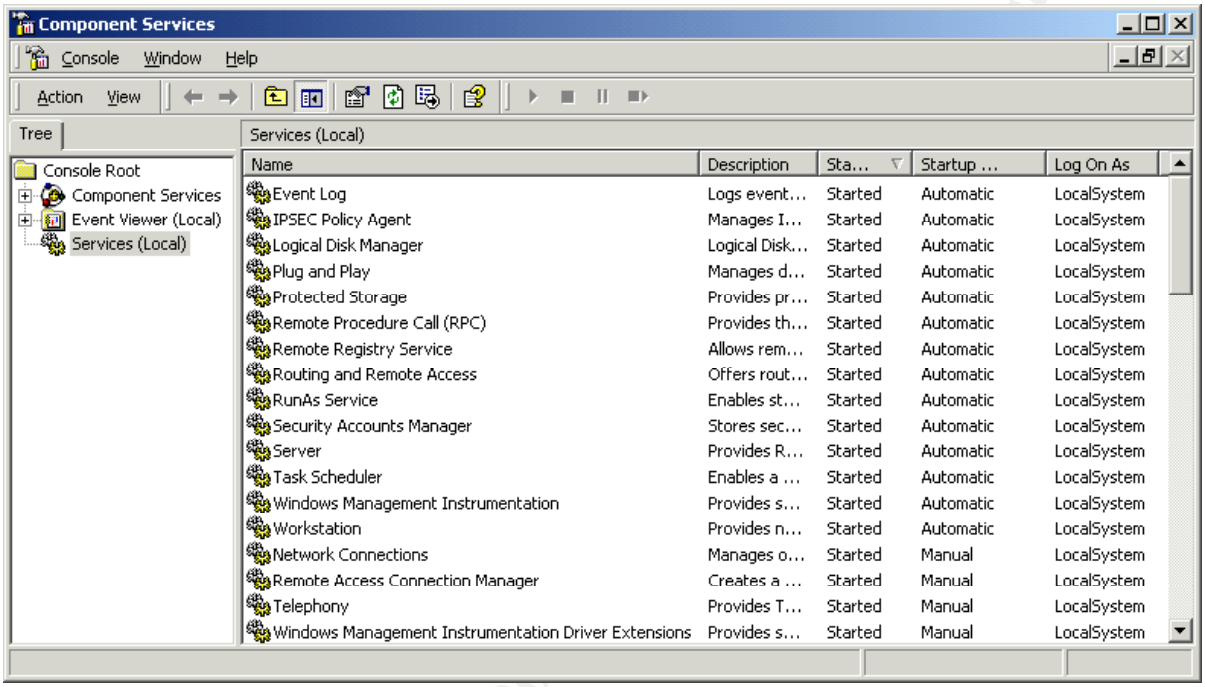


Click **Properties** and at the **TCP/IP Filtering** box, select the **TCP** and **UDP ports** you must allow into and out of your VPN server, as well as the **IP Protocols**. In this case, we are limiting traffic to UDP ports 500 and 1701 for VPN, and 1645 for RADIUS, and we're allowing IP Protocols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



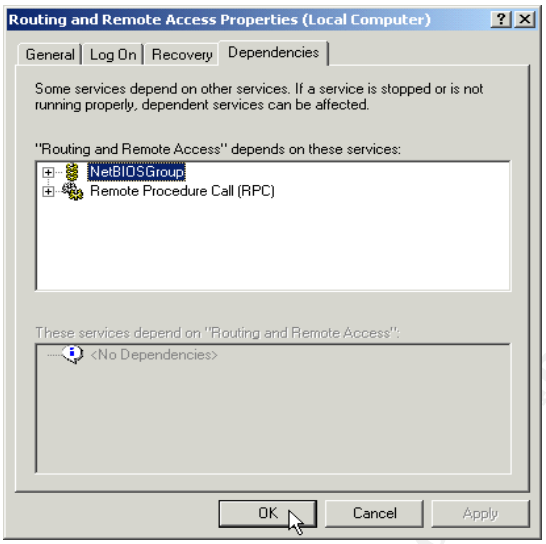
Disable Unnecessary Services

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**.



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:



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:

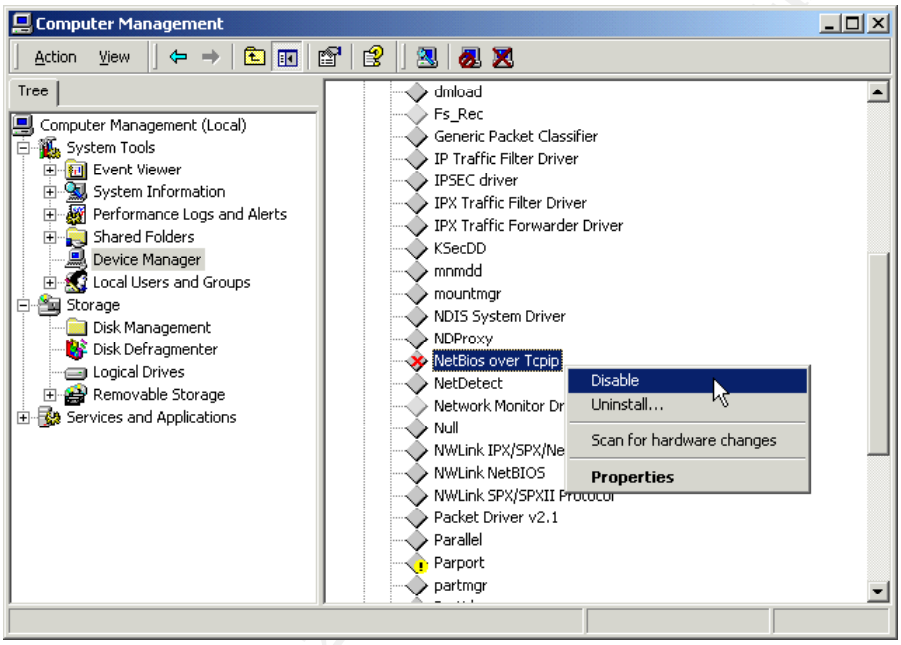
- Event Log
- IPSEC Policy Agent
- Logical Disk Manager
- Network Connections
- Plug and Play
- Protected Storage
- Remote Procedure Call (RPC)
- Remote Registry Service
- Routing and Remote Access
- RunAs Service
- Security Accounts Manager
- Server
- Task Scheduler
- Windows Management Instrumentation
- Windows Management Instrumentation Driver Extensions
- Workstation

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

- Remote Access Connection Manager
- Telephony

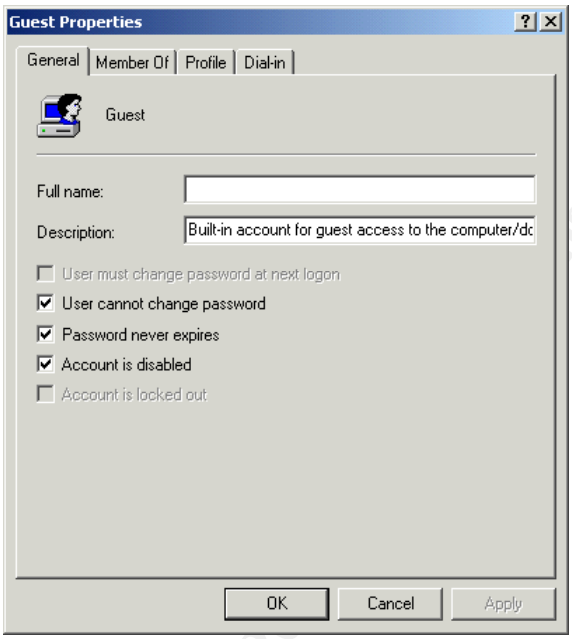
Disable NetBIOS

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**.



User Accounts

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



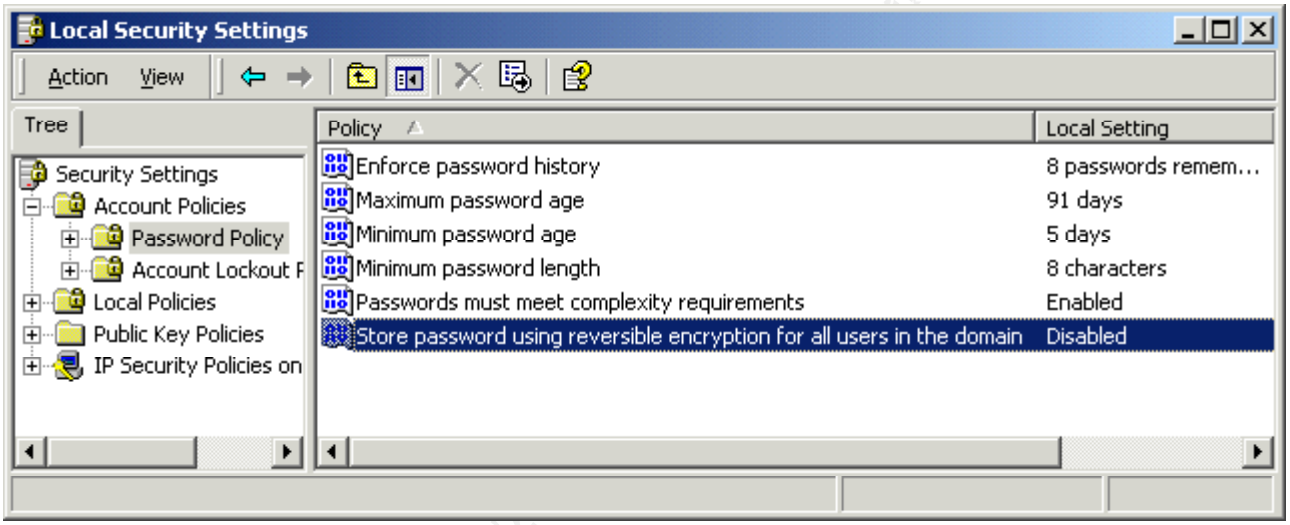
Do the same with **the Internet Guest Account**, **Launch IIS Process Account, TsInternetUser Account** or any other superfluous account. Rename the **Administrator** account, then create a dummy **Administrator** account with no rights and a difficult to crack password.

Password and Account Lockout Policies

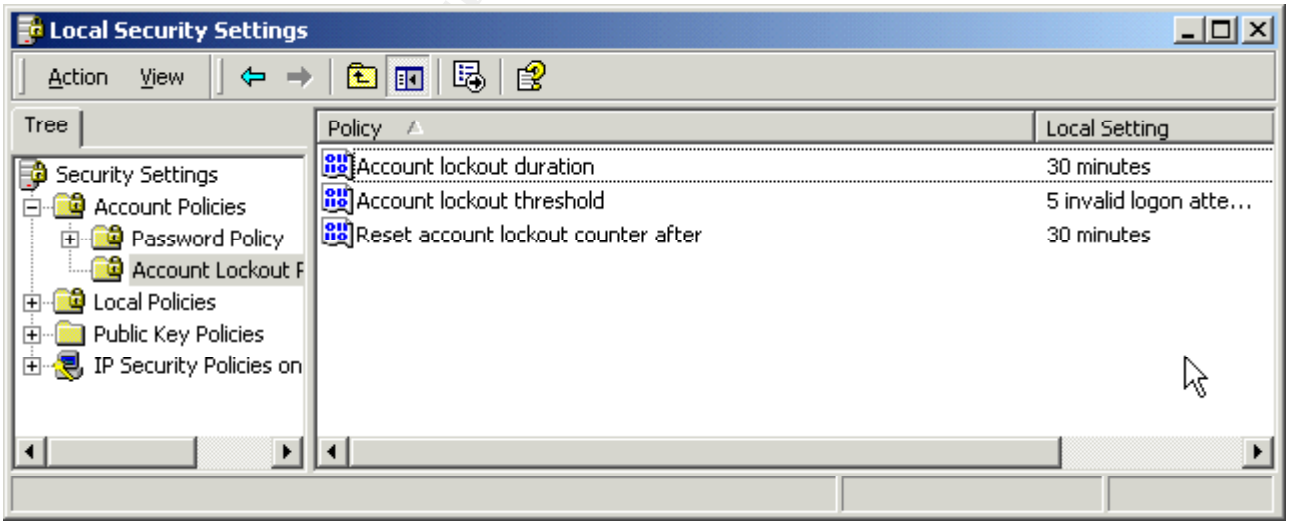
Go to **Start - Programs - Administrative Tools - Local Security Policy** to change the password and account lockout policies.

** 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:



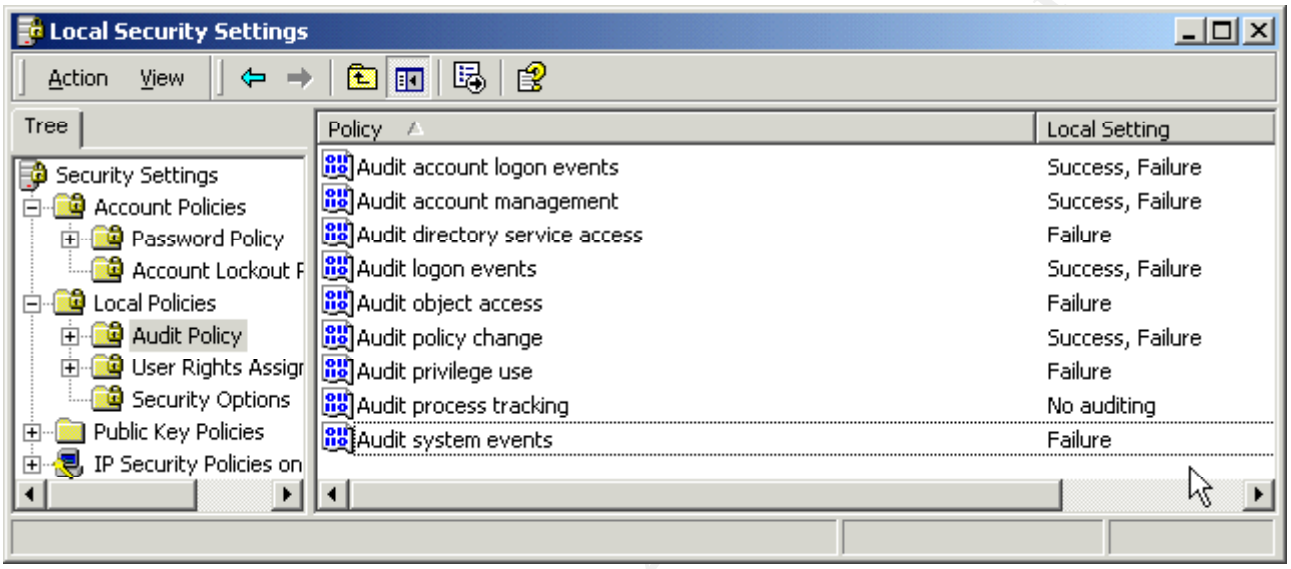
The recommended settings for the **Account Lockout Policy** are as follows:



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:



User Rights Assignment

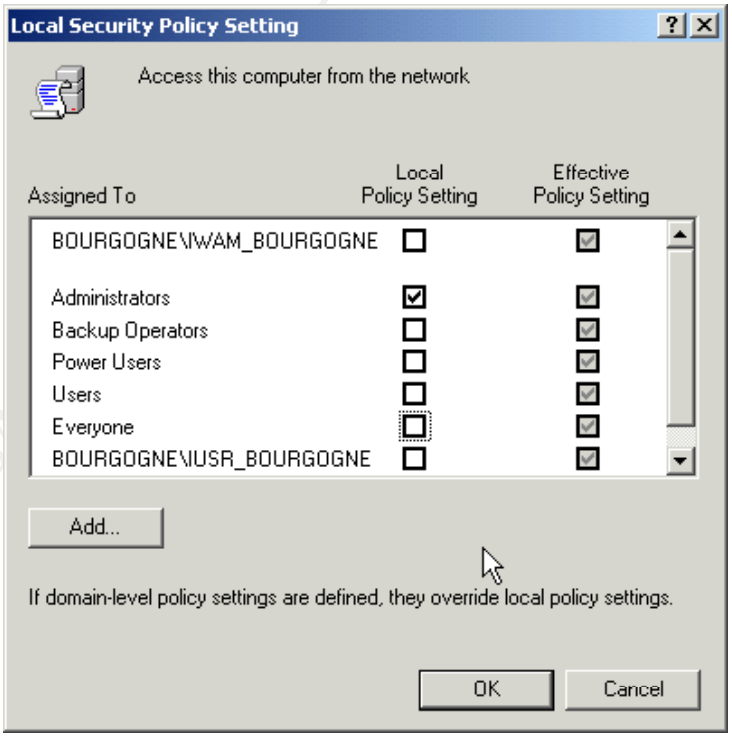
By clicking on **User Rights Assignment** in the left pane, the user rights policies are displayed in the right window. A policy may be revised by double-clicking it in the right window.

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

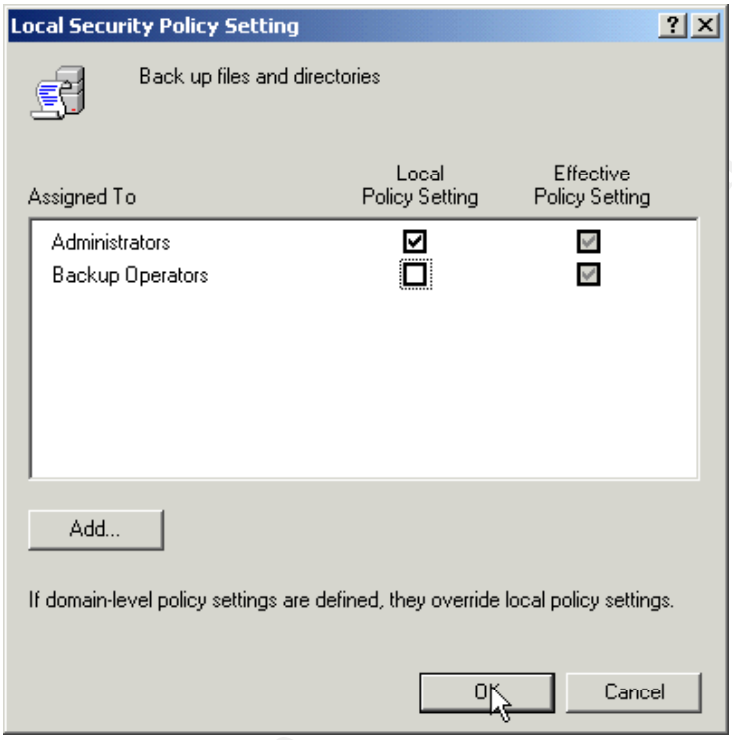
- Access this computer from the network
- Backup file and directories
- Bypass traverse checking
- Change the system time
- Log on locally
- Shut down the system

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

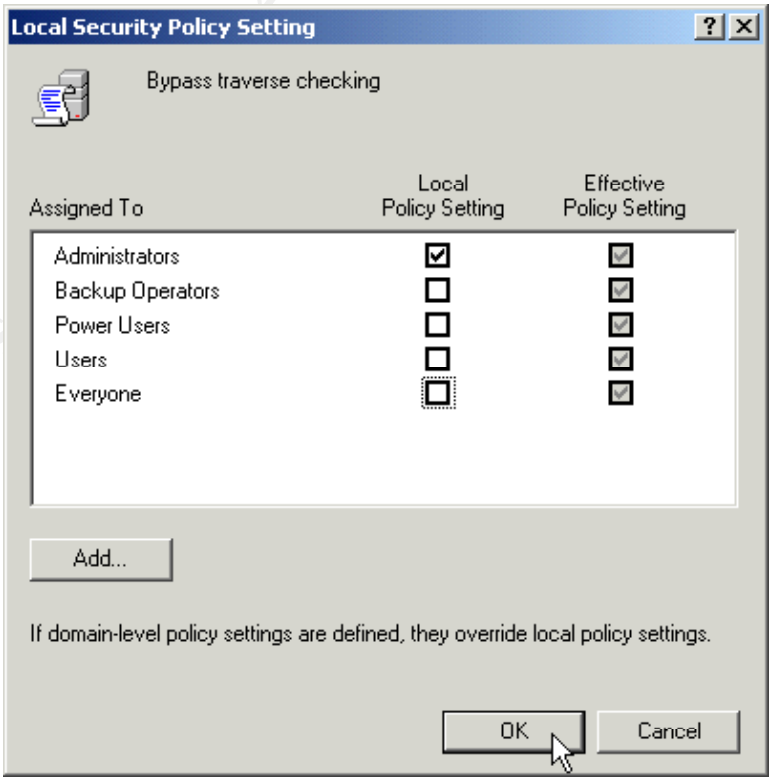
Access this computer from the network



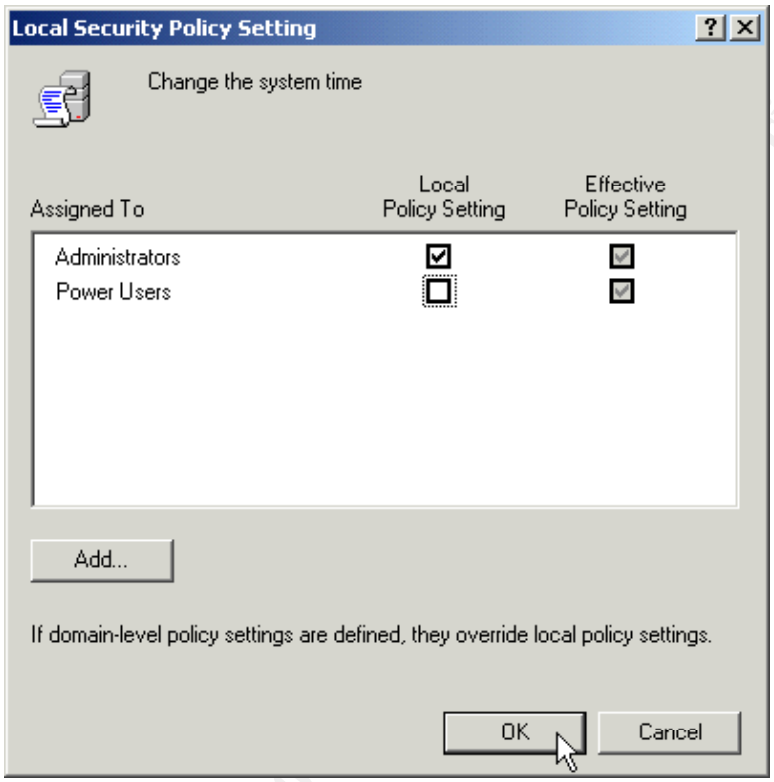
Backup files and directories



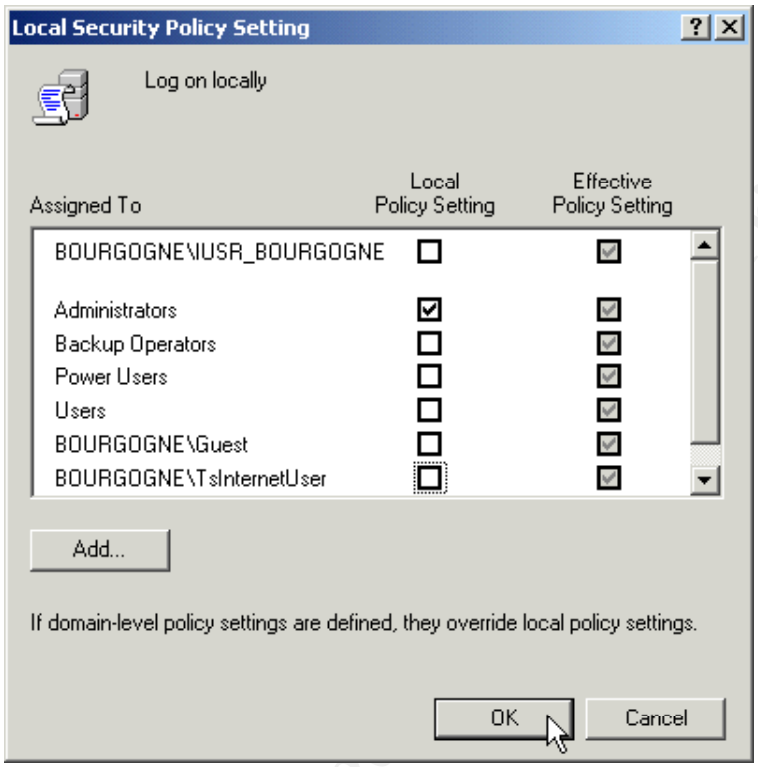
Bypass traverse checking



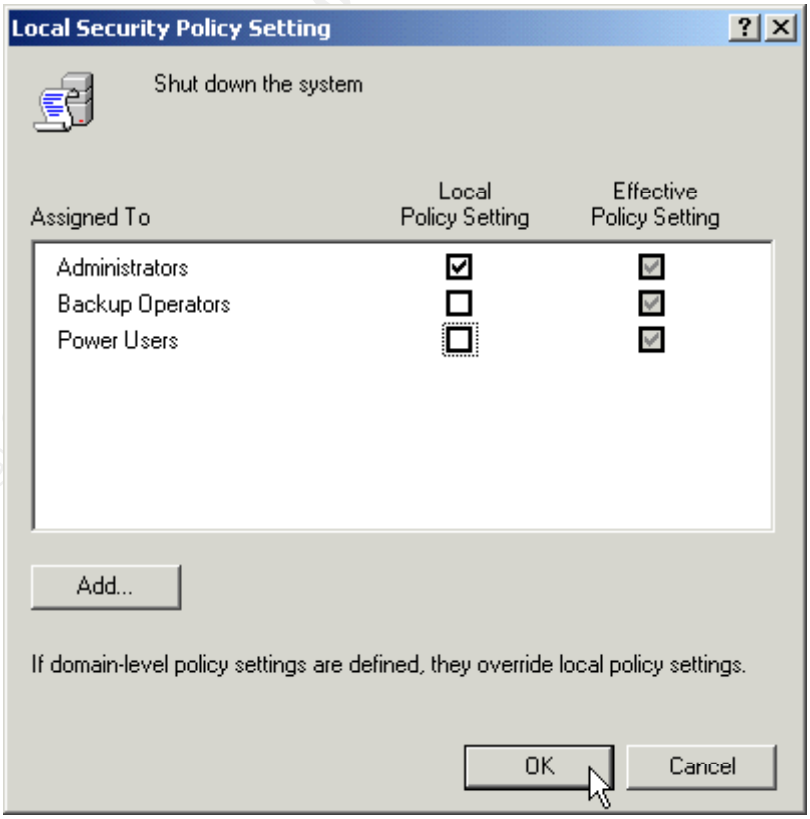
Change the system time



Log on locally



Shut down the system

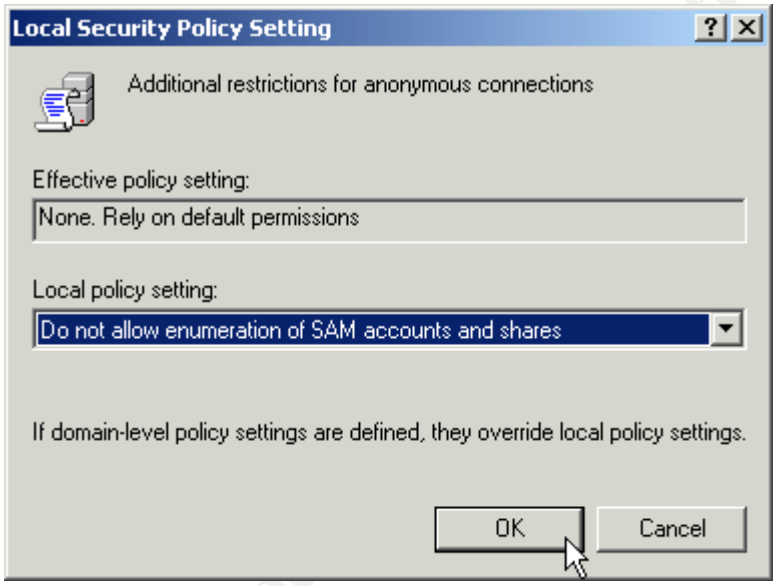


Security Options

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

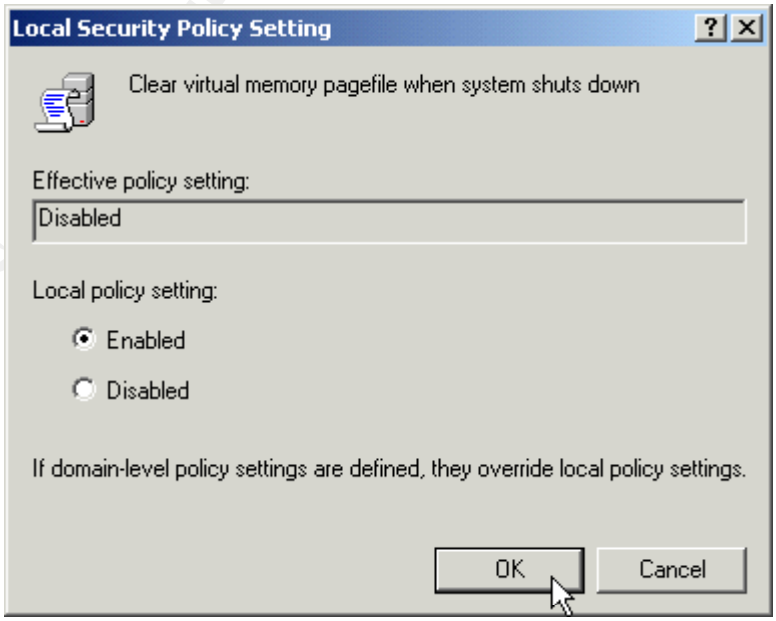
Additional restrictions for anonymous connections

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



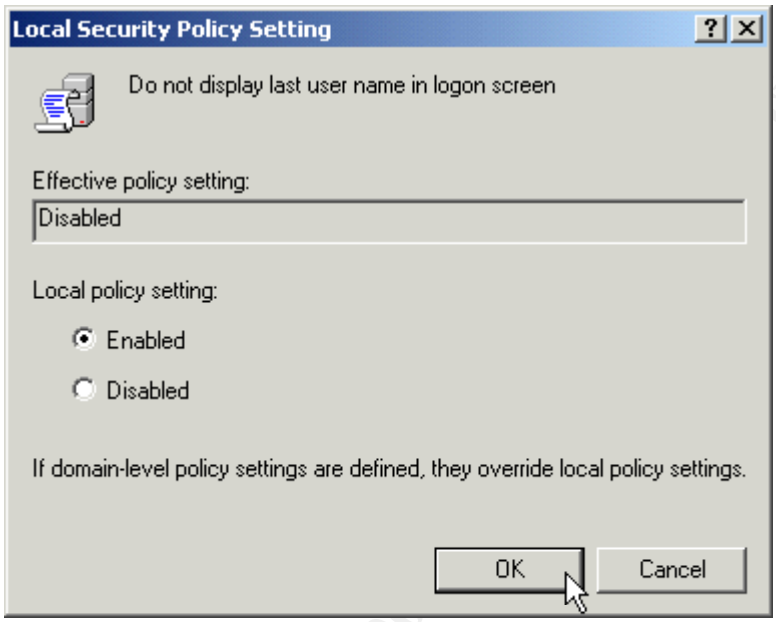
Clear virtual memory pagefile when system shuts down

Local policy setting: **Enabled**



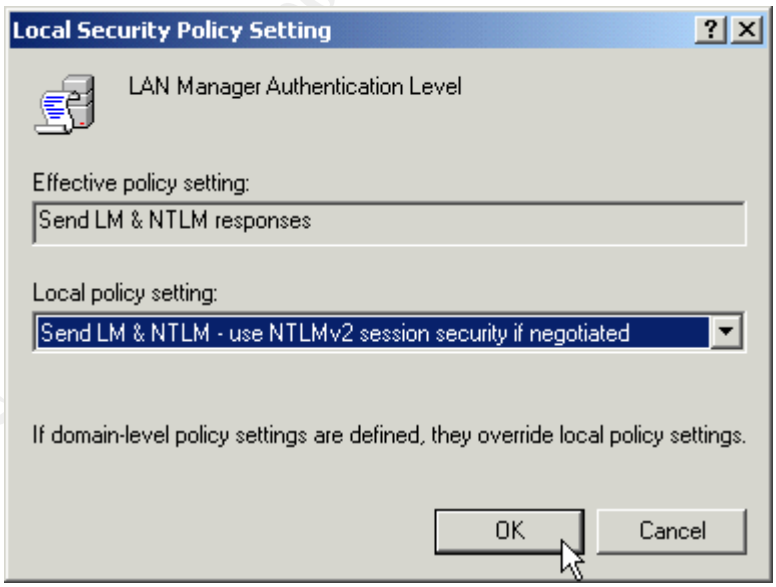
Do not display last user name in logon screen

Local policy setting: **Enabled**



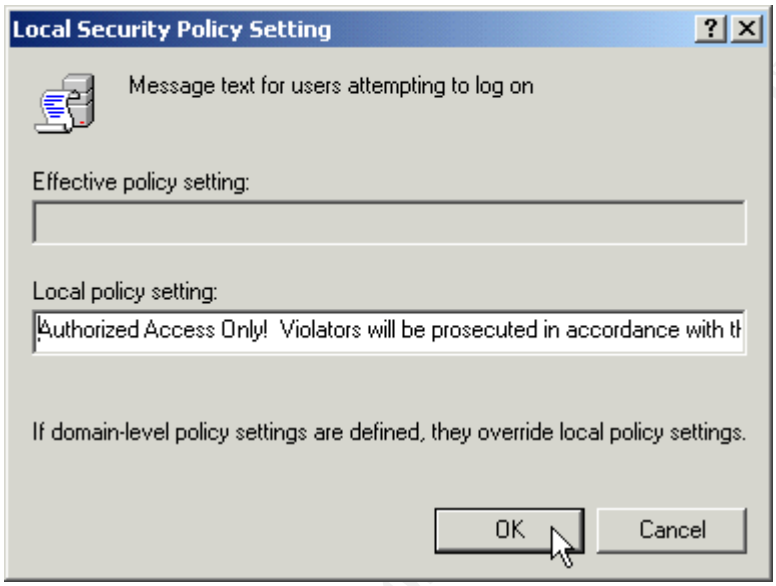
LAN Manager Authentication Level

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



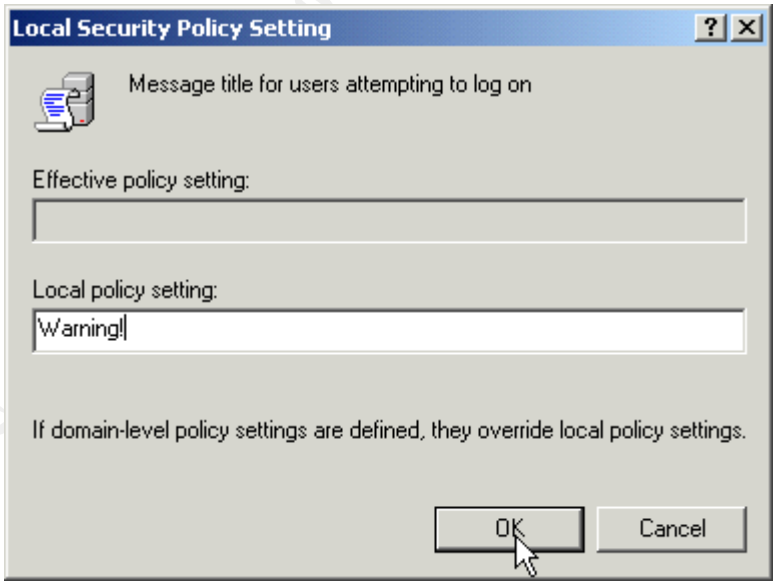
Message text for users attempting to log on

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



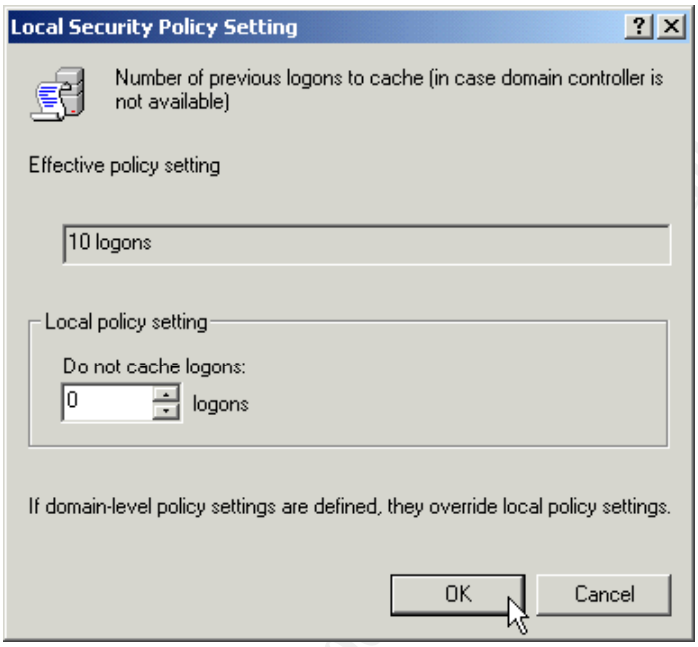
Message title for users attempting to log on

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



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

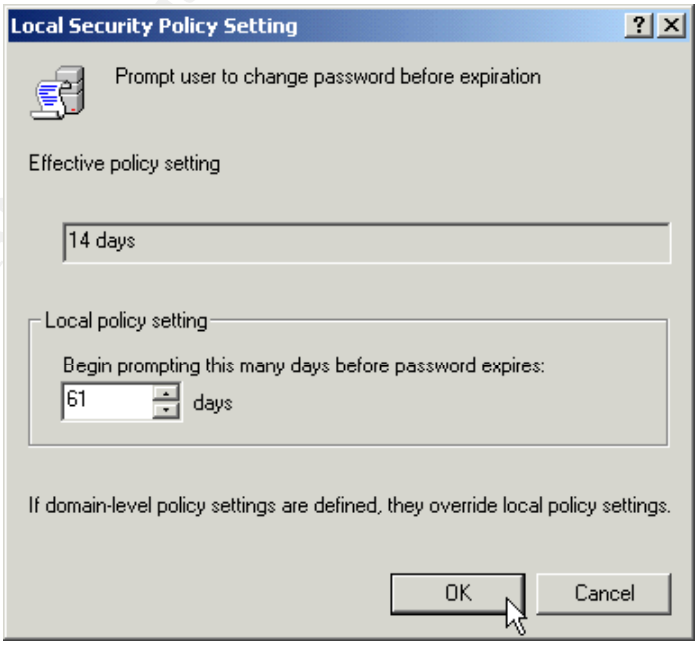
Local policy setting: **0 logons**



Prompt user to change password before expiration [5]

Local policy setting: **61 days**

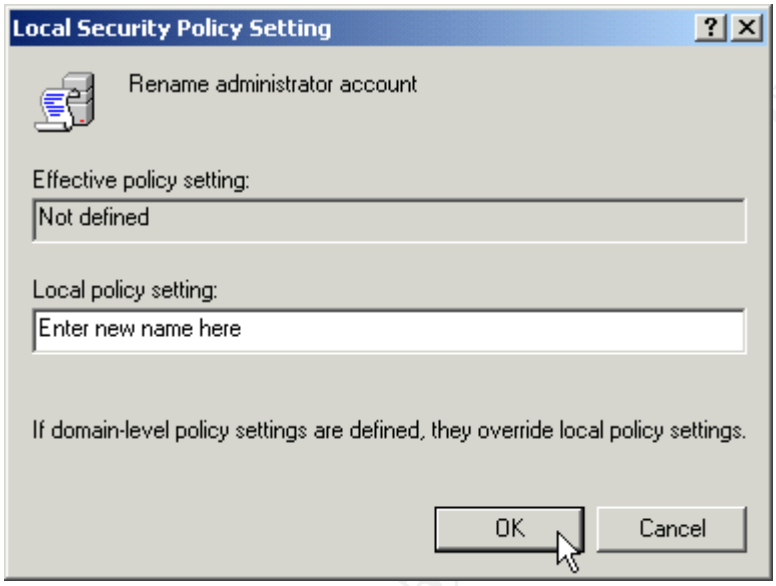
Considering the Maximum Password age of 91 days recommended above, this should result in users changing passwords every 30 days, while minimizing the need for the Administrator to unlock accounts.



[5] If 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.

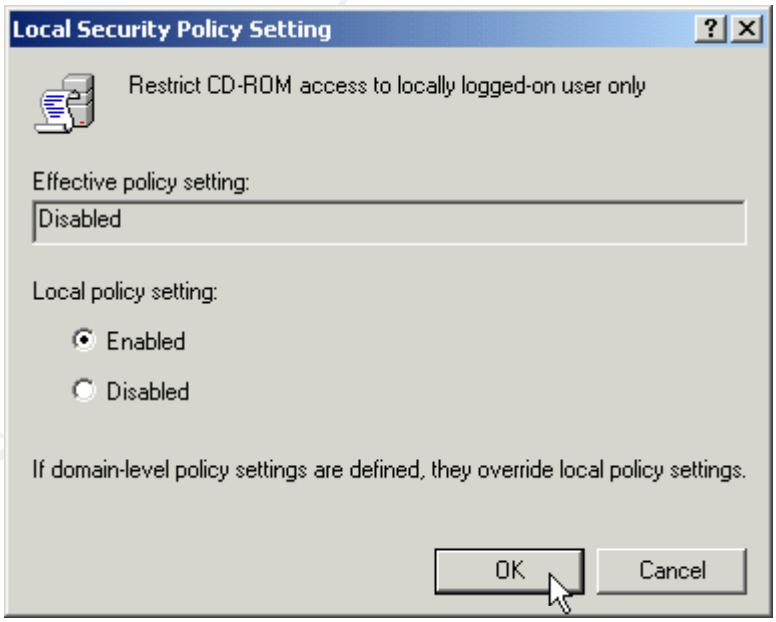
Rename administrator account

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



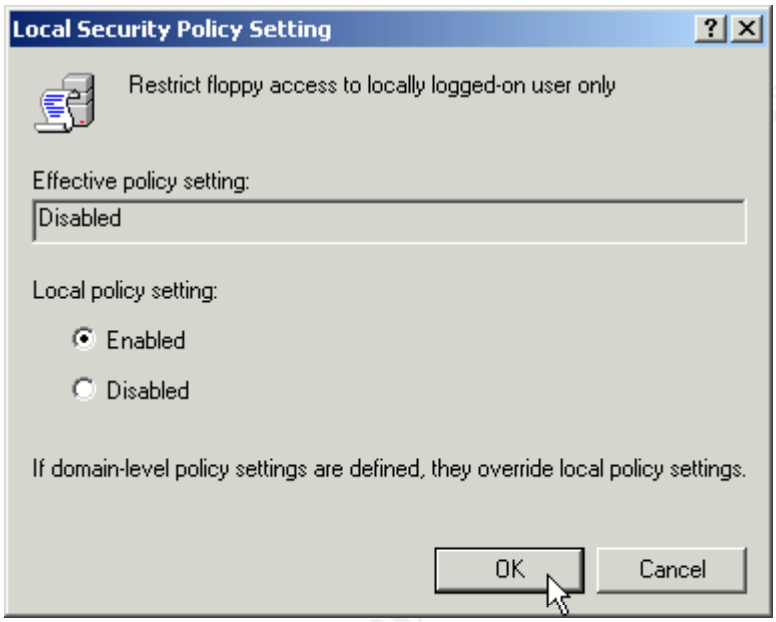
Restrict CD-ROM access to locally logged-on user only

Local policy setting: **Enabled**



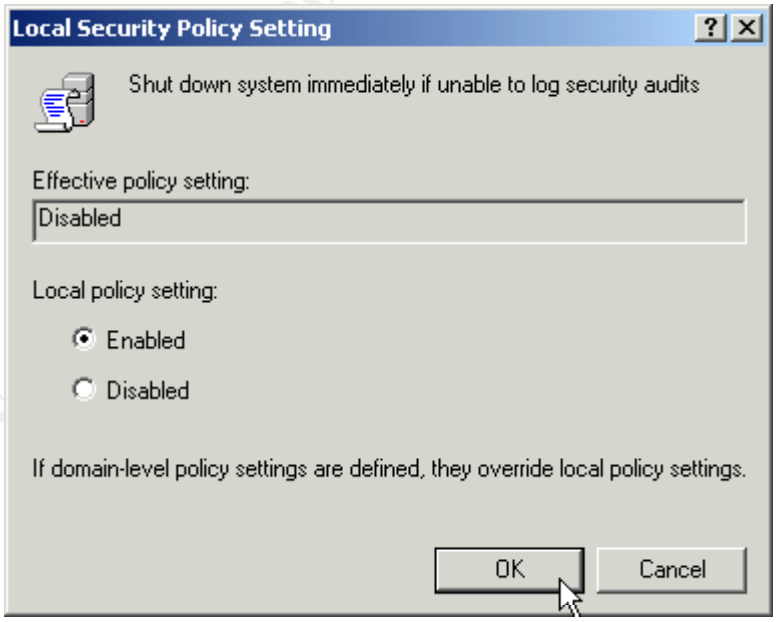
Restrict floppy access to locally logged-on user only

Local policy setting: **Enabled**



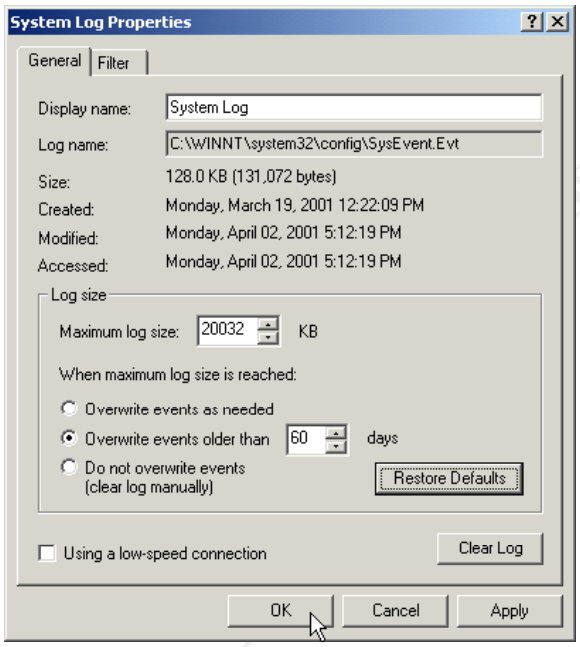
Shut down system immediately if unable to log security audits

Local policy setting: **Enabled**



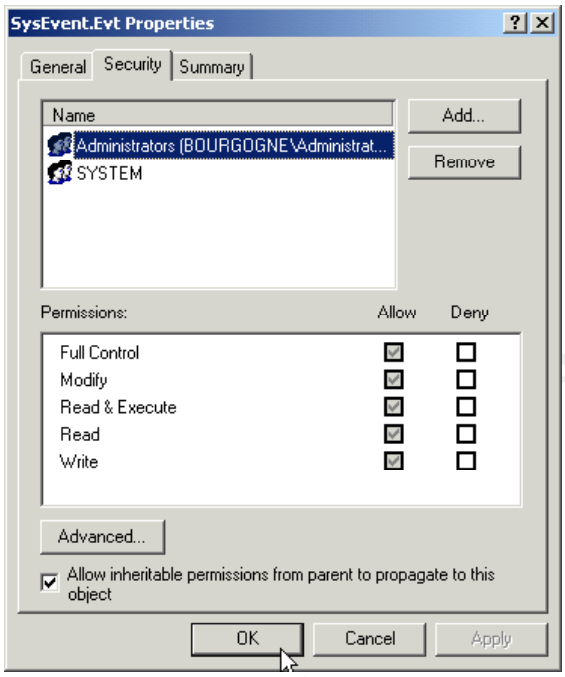
Event Logs

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:



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



Disable Source Routing

Disable source routing by creating the following registry key:

```
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 changes[6]:

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

Hive:       HKEY_LOCAL_MACHINE
Key:        System\CurrentControlSet\Services\Tcpip\Parameters
Name:       TcpMaxHalfOpen
Type:       REG_DWORD
Value:      500 (decimal)

Hive:       HKEY_LOCAL_MACHINE
Key:        System\CurrentControlSet\Services\Tcpip\Parameters
Name:       TcpMaxHalfOpenRetried
Type:       REG_DWORD
Value:      400 (decimal)

Hive:       HKEY_LOCAL_MACHINE
Key:        System\CurrentControlSet\Services\Tcpip\Parameters
Name:       NoNameReleaseOnDemand
Type:       REG_DWORD
Value:      1

Hive:       HKEY_LOCAL_MACHINE
Key:        System\CurrentControlSet\Services\Tcpip\Parameters
Name:       DeadGWDetectDefault
Type:       REG_DWORD
Value:      0

Hive:       HKEY_LOCAL_MACHINE
Key:        System\CurrentControlSet\Services\Tcpip\Parameters
Name:       KeepAliveTime
Type:       REG_DWORD
Value:      300,000 (decimal)

Hive:       HKEY_LOCAL_MACHINE
Key:        System\CurrentControlSet\Services\Tcpip\Parameters
Name:       PerformRouterDiscovery
Type:       REG_DWORD
Value:      0
```

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

```
Hive:       HKEY_LOCAL_MACHINE
Key:        System\CurrentControlSet\Services\Tcpip\Parameters
Name:       EnableICMPRedirects
Type:       REG_DWORD
Value:      0
```

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:

```
Hive:       HKEY_LOCAL_MACHINE
Key:        SYSTEM\CurrentControlSet\Control\GraphicsDrivers\DCI
Name:       Timeout
Type:       REG_DWORD
Value:      0
```

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 3½" 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

(1) 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

(9) 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) http://support.microsoft.com/support/kb/articles/q253/4/98.asp

(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." http://www.microsoft.com/windows2000/library/howitworks/communications/remoteaccess/w2kvpnscenario.asp

(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.