Global Information Assurance Certification Paper

1. Overview

This paper will begin by describing some of the risks with existing implementations of Microsoft Point-to-Point Tunneling Protocol (PPTP). The purpose of presenting the vulnerabilities of Microsoft's PPTP is to encourage the user that implementing PPTP poses a definite threat to the network infrastructure it should be protecting.

Next this paper will present Layer 2 Tunneling Protocol (L2TP) with Internet Protocol Security (IPSec), as an alternative to the Microsoft's PPTP. This paper will describe the infrastructure requirements and how to implement L2TP with IPSec between two Microsoft Windows 2000 hosts.

2. Microsoft's Point-to-Point Tunneling Protocol

Microsoft released its PPTP implementation with Windows NT 4.0 Workstation and Server. Microsoft's initial implementation of PPTP supported MS-CHAP and PAP authentication protocols.[1]

Microsoft encrypts the PPTP data by using a session key. The session key is produced as the result of the MS-CHAP authentication. The session key is derived from the MD4 hash has of the user-supplied password. This MD4 hash of the user's password is used to as the 40-bit session key to perform RSA RC4 data encryption.[1]

In 1998, Bruce Schneier of Counterpane Systems and Mudge of L0pht Heavy Industries performed an analysis of Microsoft's PPTP implementation. The analysis found several areas of concern, which were published in the 1998 paper.[2]

Schneier and Mudge's paper describe how to break Microsoft's MS-CHAP, how to break RC4 data encryption, and how to attach the control channel. [2]

To enable data encryption in MS PPTP, MS-CHAP challenge/response must be implemented. A clear text and hashed password authentication method is also available, but neither allows data encryption. [2]

Microsoft used 2 hash functions, Lan Manager and Windows NT. The Lan Manager hash function uses DES encryption and Windows NT hash is based on MD4. The Windows NT hash is significantly hard to break than Lan Manager, but, by default, the Lan Manager hash is generally sent with the Windows NT hash. This allows an attacked to

---

[1] Point-to-Point Tunneling Protocol (PPTP) FAQ. http://www.microsoft.com/ntserver/commserv/deployment/moreinfo/pptpfaq.asp. Posted: December 11, 1998

[2] Schneier, Bruce, and Mudge. Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP). http://www.counterpane.com/pptp.pdf. 1998

break the weaker Lan Manager hash and use it to produced the stronger Windows NT hash. [2]
Based on the knowledge of how the hash functions are created, Schneier and Mudge present how to produce the password, based on the hash value. [2]

Microsoft uses Microsoft Point-to-Point Encryption (MPPE) to protect a stream of PPTP data. MPPE relies on a pre-shared key and uses RC4 with either 40-bit or 128-bit key. Schneier and Mudge found the security of the key to be no greater than the security of the password. [2]

Mudge and Schneier also found the PPTP control channel to be susceptible to Denial of Service (DoS) attacks. In addition to others, Mudge and Schneier found that iterating through the values for the Packet Type field in the PPTPPacketHeader cause a NT Kernel panic, which resulted in a Blue Screen of Death. [2]

Micorosft reviewed this paper released a significant update to their PPTP implementation. Microsoft released Dial-Up Networking 1.3, which implemented MS-CHAPv2 and an updated version of MPPE. Schneier and Mudge reviewed the new implementation and found significant improvements in security and performance. MS-CHAPv2 no longer sends both the Lan Manager and Windows NT hashes, by default. Mudge and Schneier also found the implementation to be more resistance to many of the DoS attacks in the original implementation. [3]

Though Microsoft made several implementation improvements, Microsoft's PPTP implementation still relies on the user's password as the basis for creating session keys for authentication and encryption. This reliance on user password makes the implementation, as weak as any user's password.

3. Alternatives to PPTP

With the release of Windows 2000, Microsoft has provided a standard's based replacement to PPTP in Layer 2 Tunneling Protocol (L2TP). L2TP is a combination of PPTP and Cisco's Layer 2 Forwarding. L2TP does not define or negotiate any type of data encryption. L2TP relies on Internet Protocol Security (IPSec) to provide data encryption.

L2TP uses User Datagram Protocol (UDP) messages for both data and control messages. Both the data and tunnel maintenance messages use UDP port 1701 for the client and server. Because L2TP uses UDP vice TCP, a connection-based protocol, L2TP uses message sequencing to ensure delivery of L2TP messages. When L2TP is combined with IPSec, the L2TP packets are encapsulated inside IPSec packets.

[3] Schneier, Bruce, David Wagner and Mudge. Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2). http://www.counterpane.com/pptpv2.pdf. October 19, 1999.

3.1. Infrastructure Requirements:

L2TP with IPSec requires the following protocols: Encapsulating Security Payload (ESP), Internet Key Exchange (IKE), and L2TP. As discussed earlier, L2TP using UDP port 1701. Internet Key Exchange requires UDP port 500 and ESP requires IP Protocol ID 50. Notice that ESP requires a different IP protocol, not a UDP or TCP port.

Assuming there is a firewall protecting the intranet from the Internet, the placement of the L2TP server directly affects what IP filters are required on the firewall. If the L2TP server is outside of the firewall, the firewall will have to filter IKE and LT2P. If the L2TP is within the intranet, the firewall will have to filter IKE and ESP. The filtering configuration is required because the L2TP packets are encapsulated with the ESP packets.

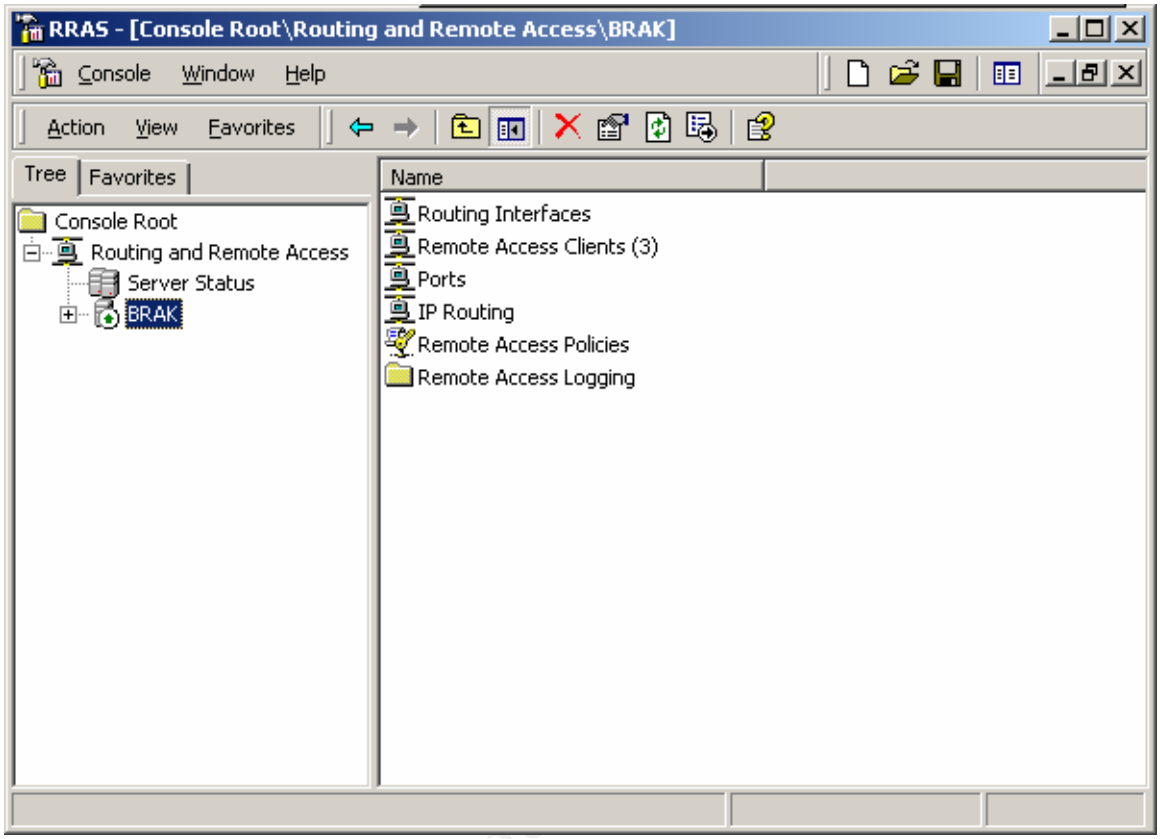
RRAS filters are applied after the IPSec module removes the ESP header.

To use L2TP and IPSec, a computer certificate must be installed on both the VPN client and server.

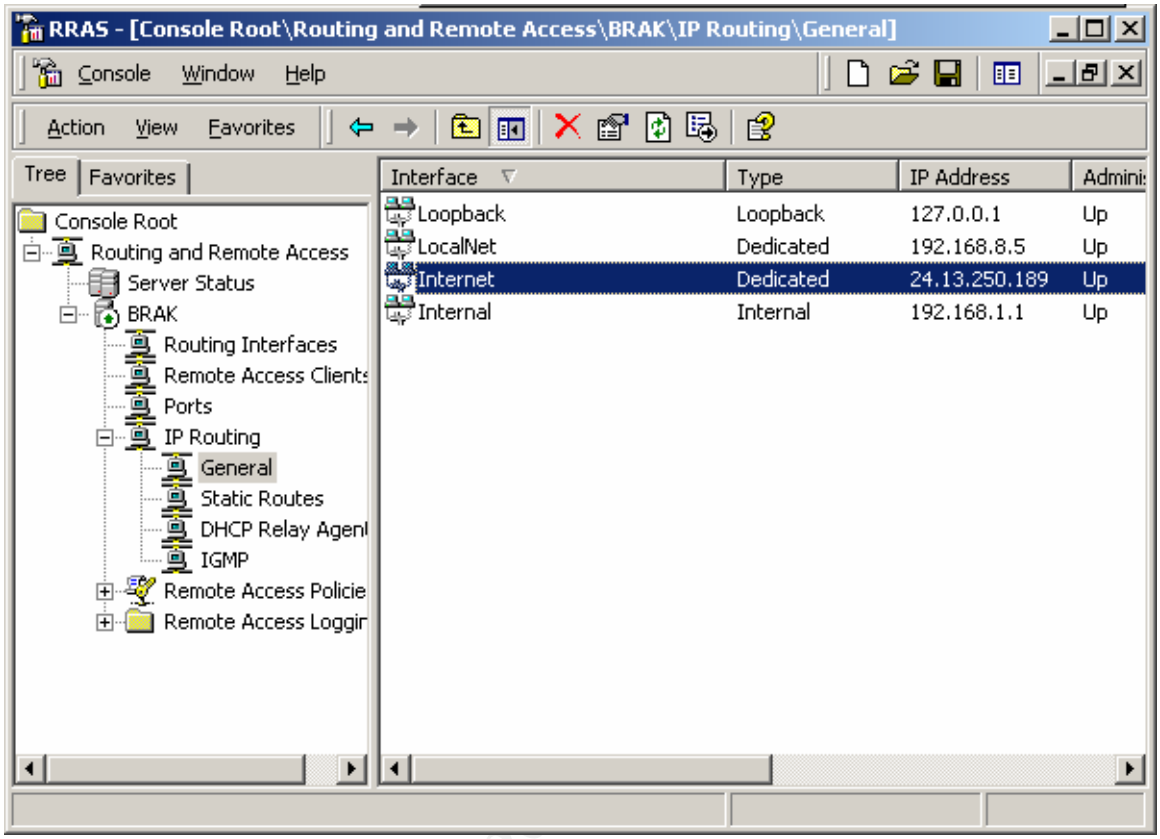
3.2. RRAS Filters for L2TP with IPSec

The following directions will demonstrated how to configure Routing and Remote Access Server (RRAS) interface filters for L2TP and IPSec.

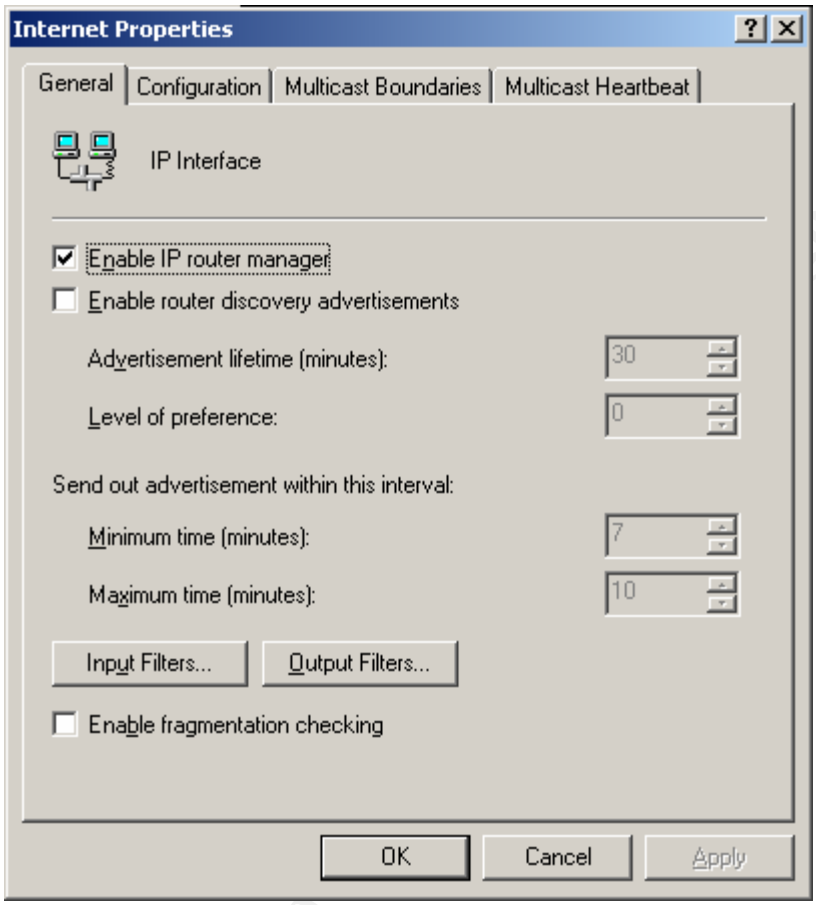
1. Start the MMC for Routing and Remote Access.
2. If the RRAS server you want to configure is not available, right-click Server Status, and choose add server. Select the RRAS server and click OK. You should see a screen similar to the following:



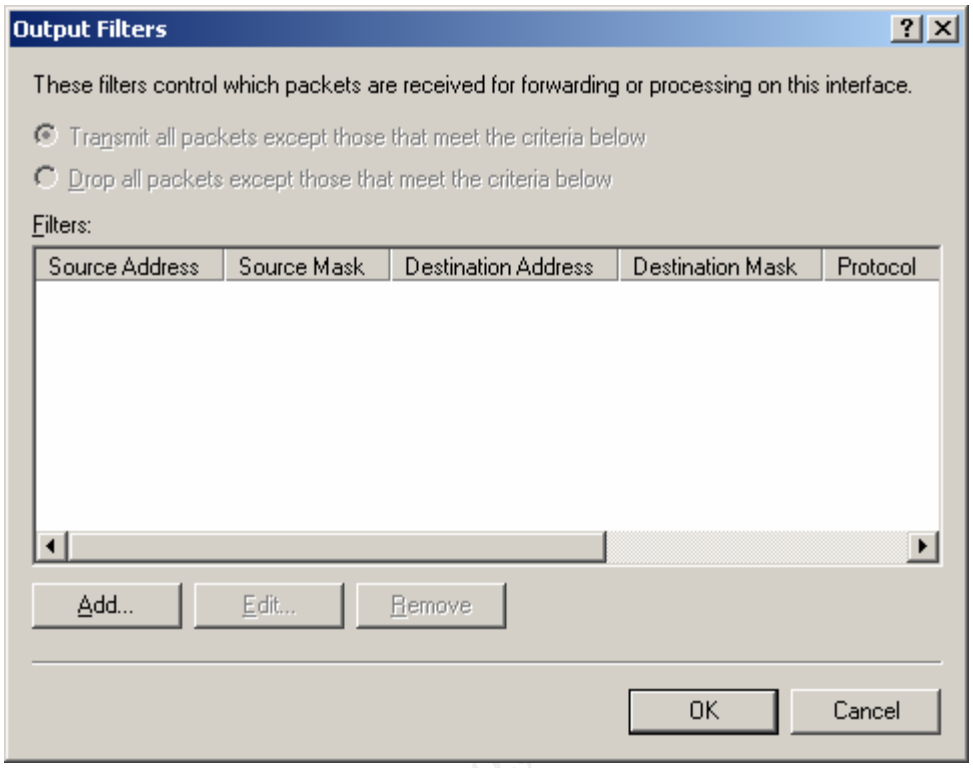
3. Expand the RRAS server object, expand the IP routing object, and select General, as shown below:



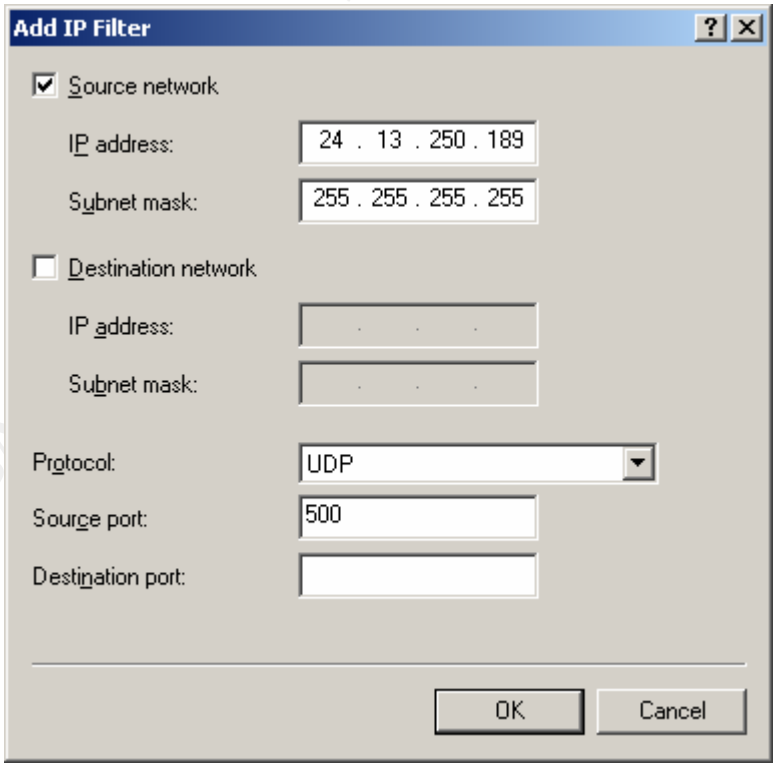
4. Double-click the interface that will accept the VPN connections. (In this example the Internet interface will accept the connections.)



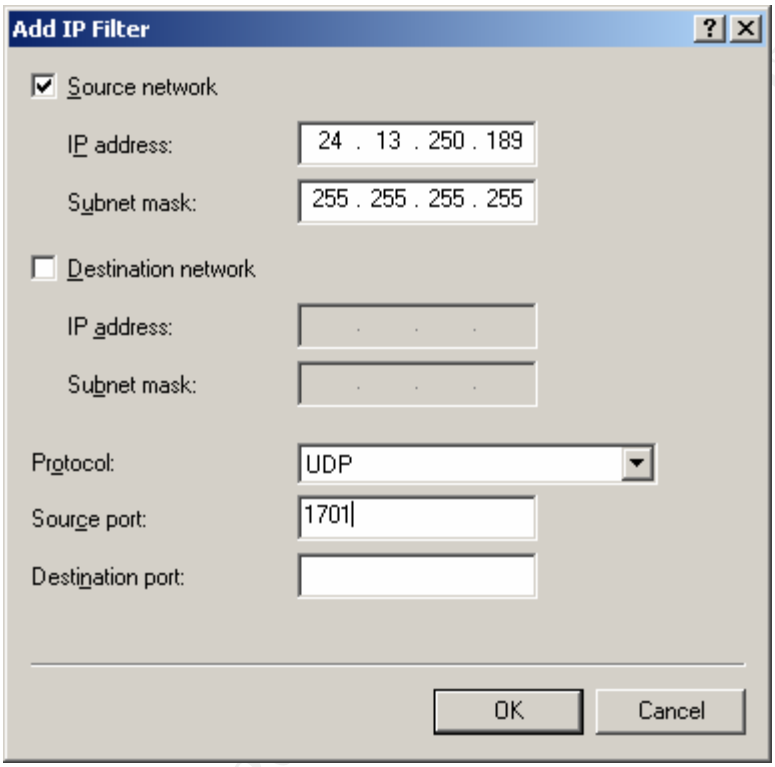
5. Click the Output Filters… button. You should see a window similar the window shown below.



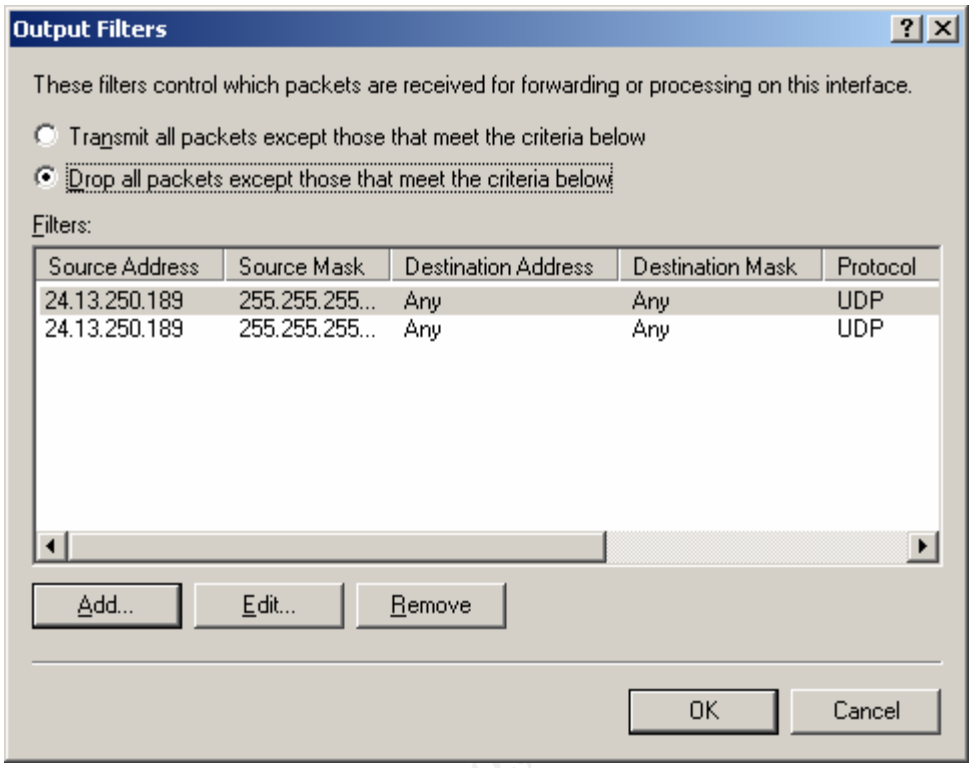
6. Click Add… to create a new filter.



7. Enable the Source network check box and fill in the IP address of the interface that will accept the L2TP connections. Set the protocol to UDP and supply a source port of 500.
8. Click OK to return to the previous window.
9. Click Add… to create the filter for L2TP traffic as shown below.



10. Click OK to return to the previous screen.
11. Make sure the radio button to Drop all packets expect those that meet the criteria below is selected. (This is depicted below.)



12. Repeat steps 5-11, choosing Input Filters…, instead of Output Filters. Instead of supplies source IP address and port information, provide Destination IP address and port information.

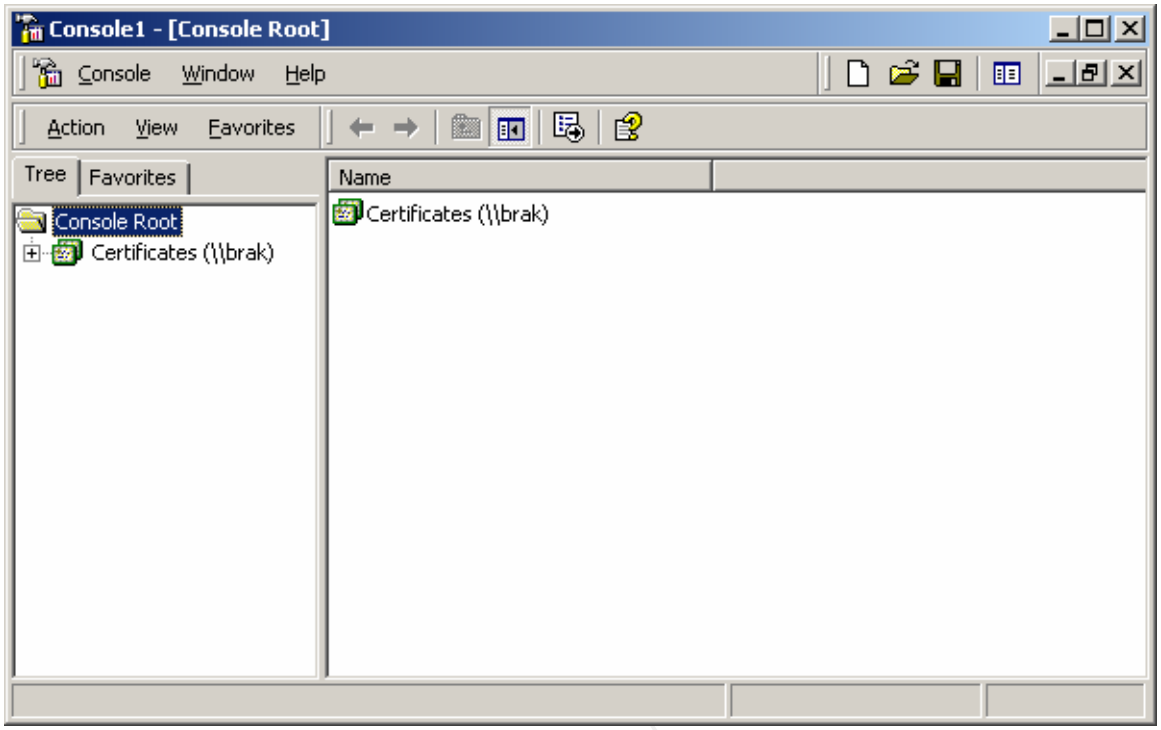
Note that although we intend to use IPSec to encrypt the data, we do not specify RRAS input or output filters for ESP traffic (IP Protocol ID 50). We do not need to specify the ESP information, because the IPSec module removes the ESP header, prior to the enforcement of the RRAS filters.

3.3. Authentication Requirements

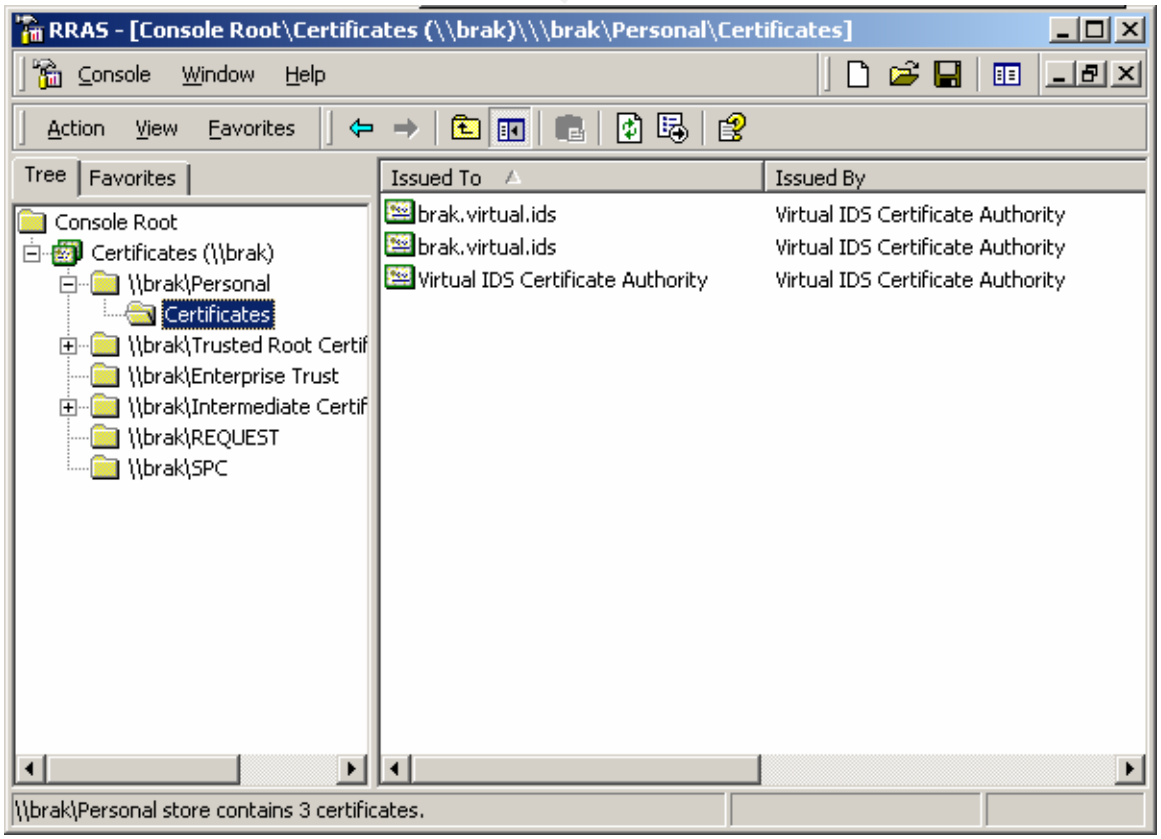
Windows 2000 can provide authentication to L2TP/IPSec sessions via certificates or Microsoft's integrated Kerberos.

The following directories will demonstrate how to ensure a computer certificate is available for IPSec use.

1. Start an MMC, click Start, select Run, and type MMC on the command line.
2. Select Add/Remove Snap-in from the Console menu.
3. Click Add, select Certificaties, click Add, select Computer Account, click Next and choose the appropriate option. Provide the name of the computer and click Finish.
4. Click OK to return to the MMC console. You should have a window similar to the window shown below:



5. Expand the Certificates object, expand the Personal object, and click Certificates, as shown below:

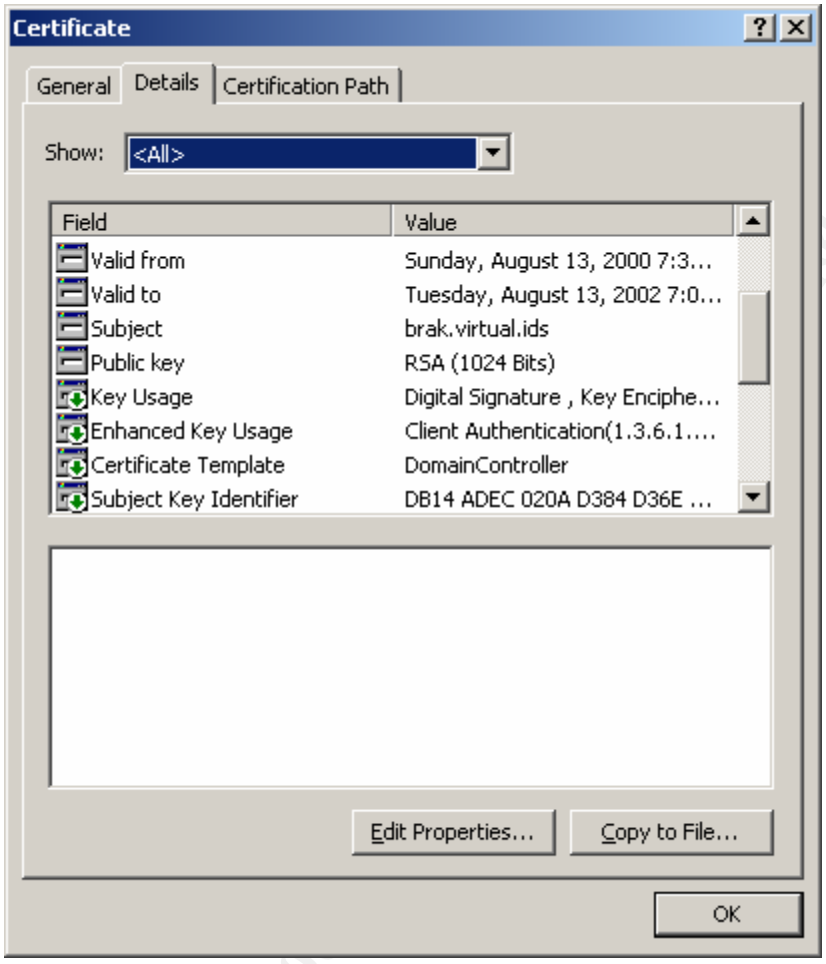


6. Notice there are 3 certificates available. Below are the certificate requirements for IPSec:
    - Certificate stored in computer account (machine store)
    - Certificate contains an RSA public key that has a corresponding private key that can be used for RSA signatures
    - Used within certificate validity period
    - The root certification authority is trusted
    - A valid certification authority chain can be constructed by the CAPI module
    - IPSec does not require the machine certificate to be an IPSec type of certificate because existing certificate authorities may not issue these type of certificates[4]

Windows2000 supplies 2 certificate templates that can be used by group policy objects to automatically issue certificates. Either the domain controller template or the computer template will issue certificates that meet the above requirements.

To determine the template used for any of the certificates, double-click the certificate in question and click the Details tab, as shown below:

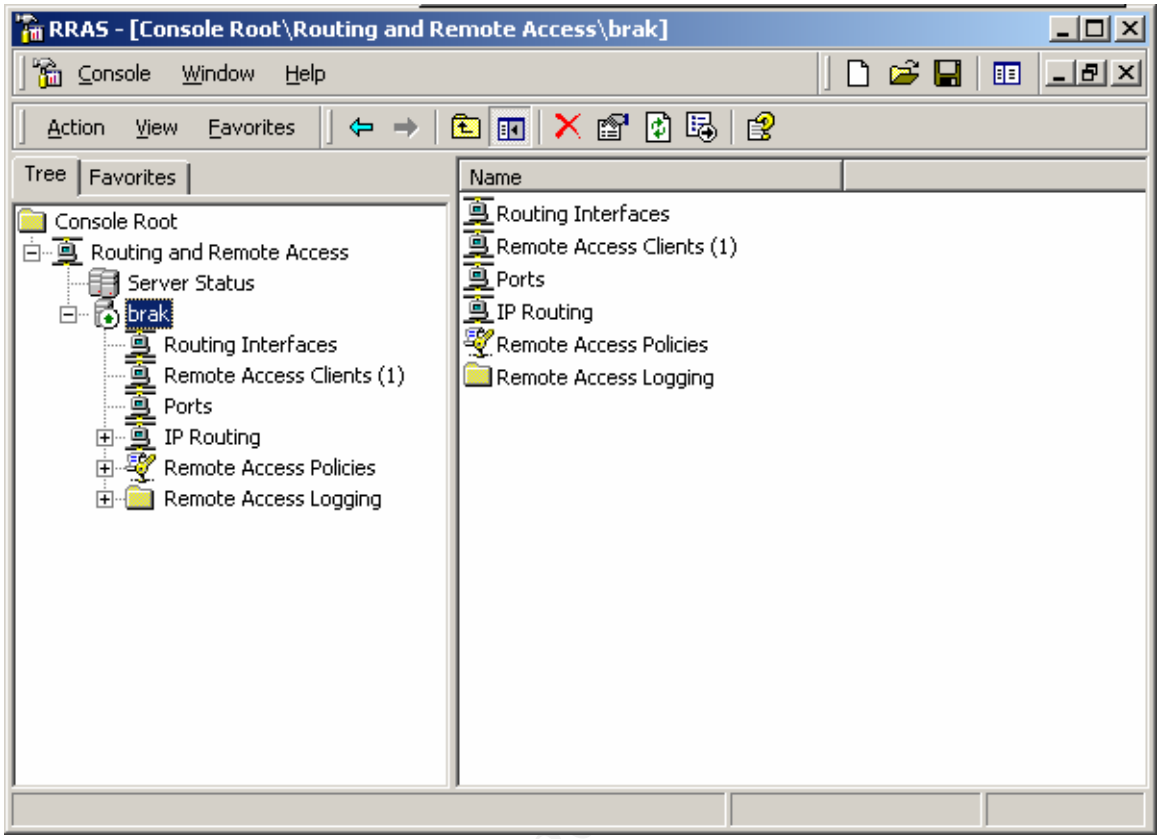
[4] Step-by-Step Guide to Internet Protocol Security (IPSec). http://www.microsoft.com/windows2000/library/planning/security/ipsecsteps.asp. Posted 2/17/2000.



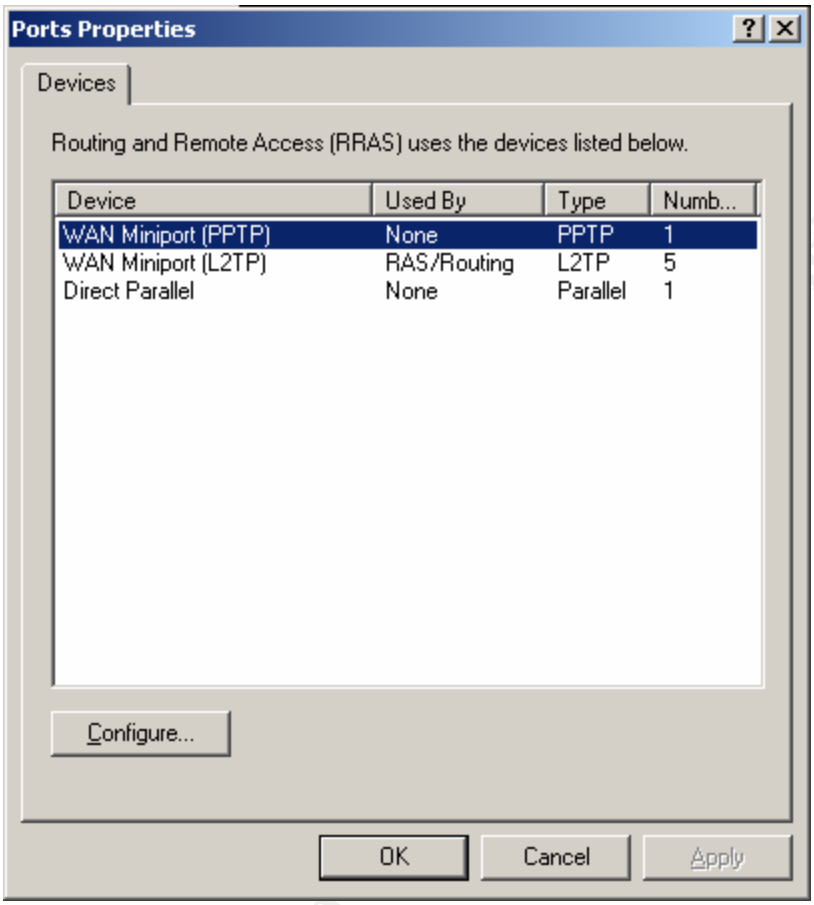
Notice the Certificate template field. This example is for a domain controller.

3.4. L2TP Server Configuration

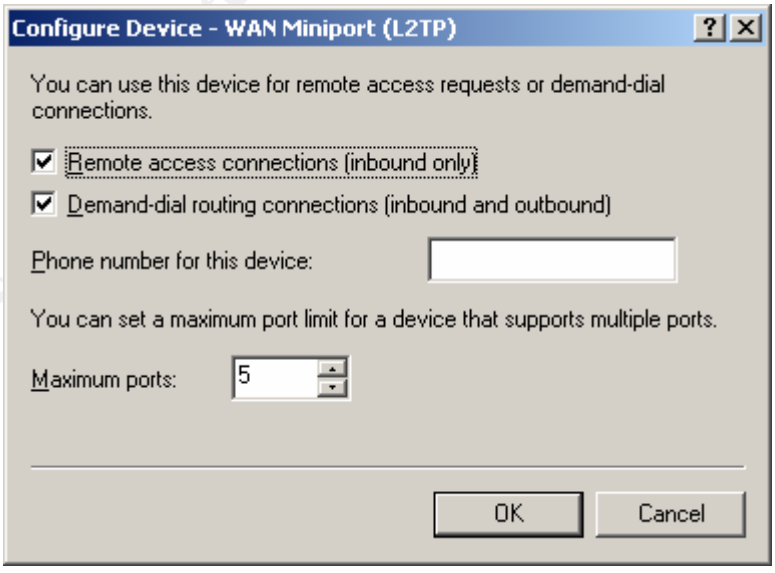
To enable the Windows2000 RRAS server to be able to accept L2TP connection, the server must have L2TP ports enabled. To verify there are L2TP ports available, start the RRAS MMC console. If the RRAS server is not available under the Routing and Remote Access object, right-click Server Status and click add. Follow the prompts to add a RRAS server to the console. Once the server is available, expand the server so the Ports object is displayed (see below).



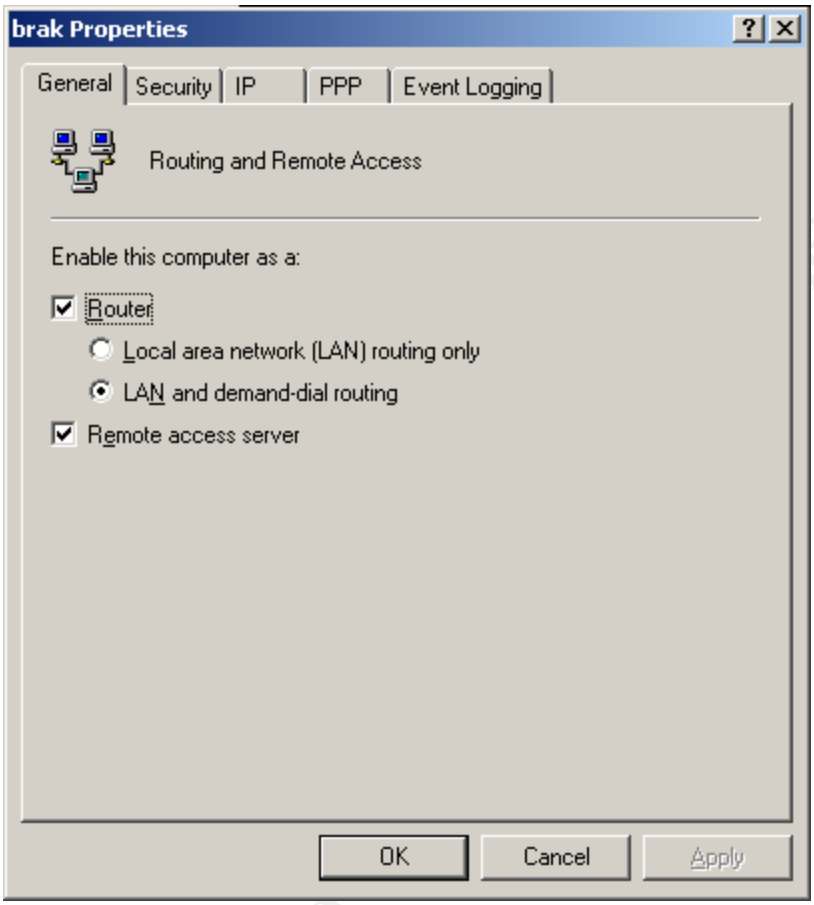
Right-click the Ports object and select properties. The following window will be displayed:



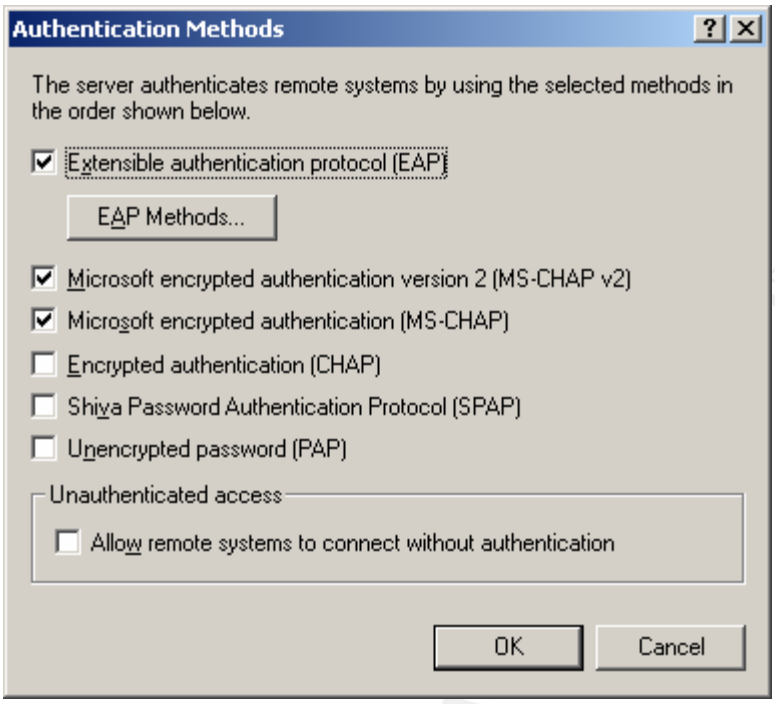
Double-click any of the lines to configure the ports for RRAS access. The L2TP ports should be configured for Remote access connections and Demand-dial routing.



Now right-click the server object and select properties. The following dialog box will be displayed:



Configure the L2TP server to be a demand-dial router and a remote access server. Then click the Security tab. Clicking the Windows Authentication button will display the following screen:



Enable Extensible authentication protocol.

3.4.1. Remote Access Policy

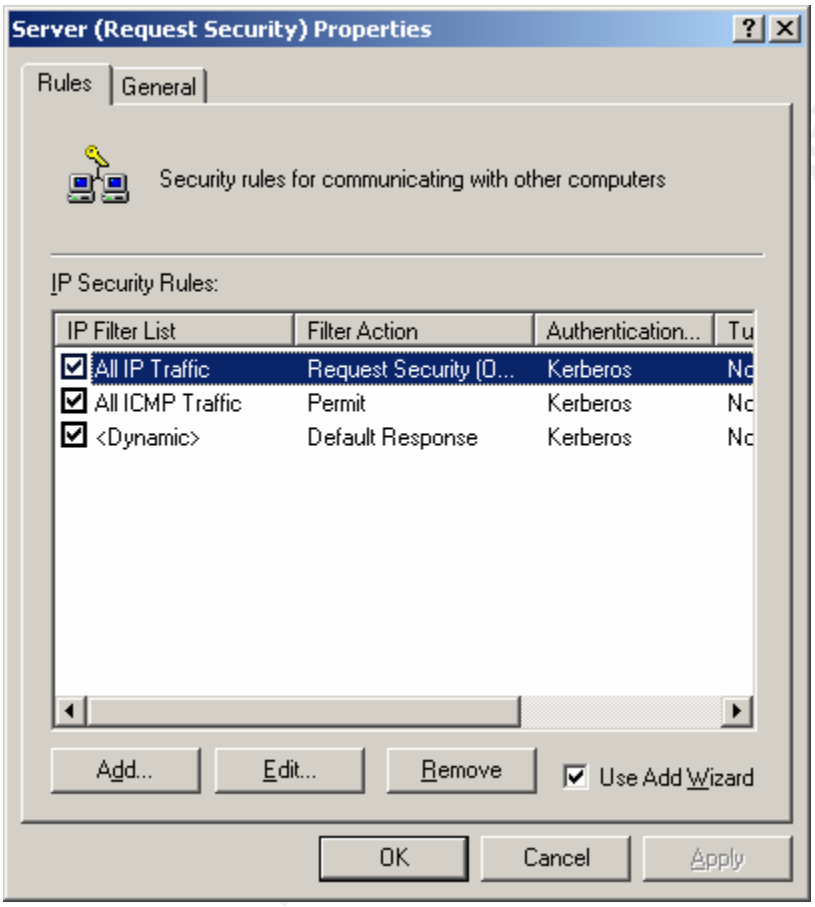
Next a RRAS Remote Access Policy is required. To create a RRAS Remote Access Policy, right-click the Remote Access Policies object and select New Remote Access Policy. Name the policy and click Next. Add a condition. The condition can check Windows group member, which is a good way to control access. If you have not create an Active Directory group, create a local domain group called VPN users for example. Use this group to create a condition based on Windows-Group. Click next and select Grant remote access permission. Click Next, then Finish to complete the policy creation.

3.4.2. IP Security Policy

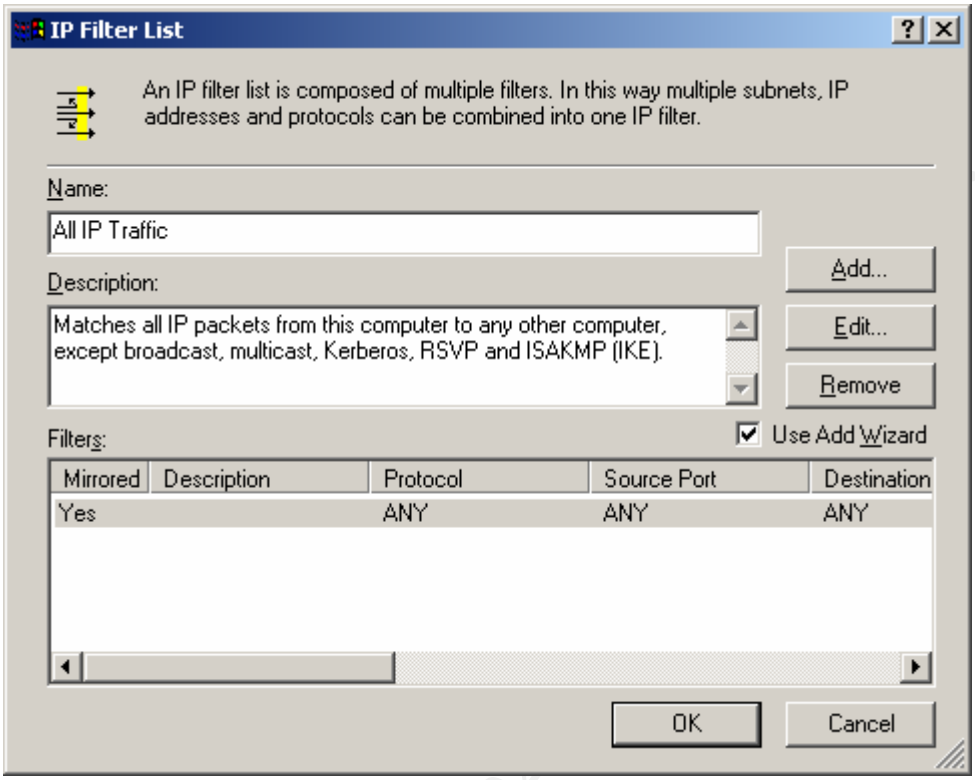
The last step to preparing the server is to create an IP Security policy on the RRAS server. This policy will require IP Sec between the RRAS client and the RRAS server. When the RRAS server starts, it is supposed to automatically create an IPSec policy on the server. During the creation of this paper, neither the client nor the server automatically create the IPSec policy. Both the policy on the client and server had to be created.

To create the IPSec policy on the server, start an MMC console and add the snap-in for IP Security Policy Management for the local computer. Notice that Windows2000 includes

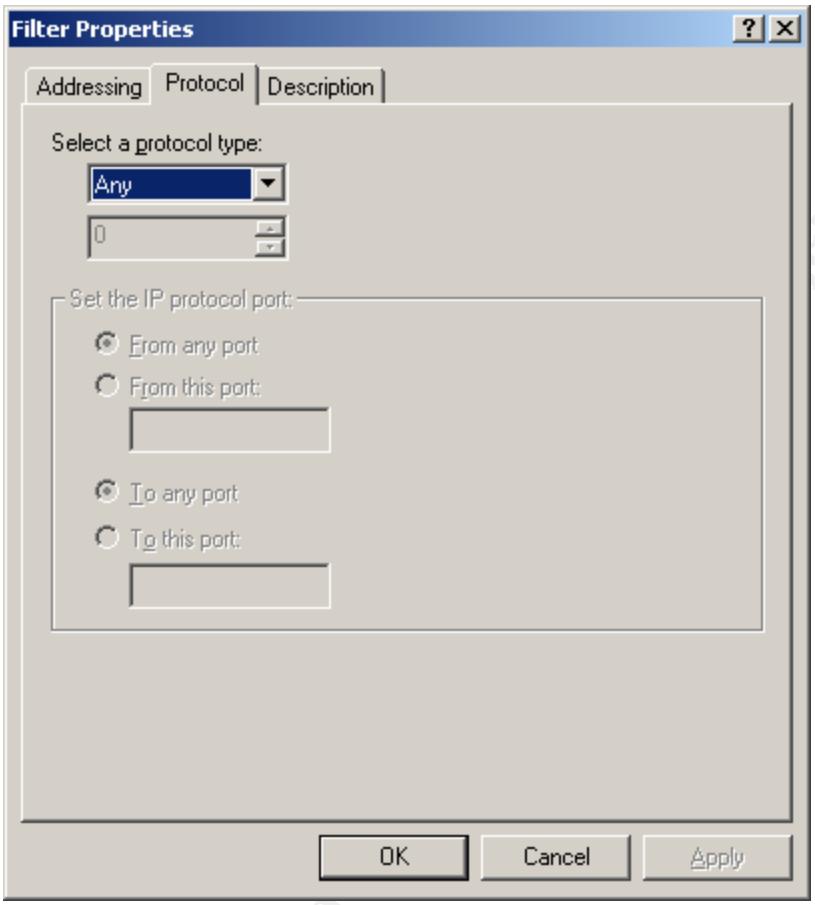
3 different policies: client, server, and secure server. Double-click the server policy to display the following window:



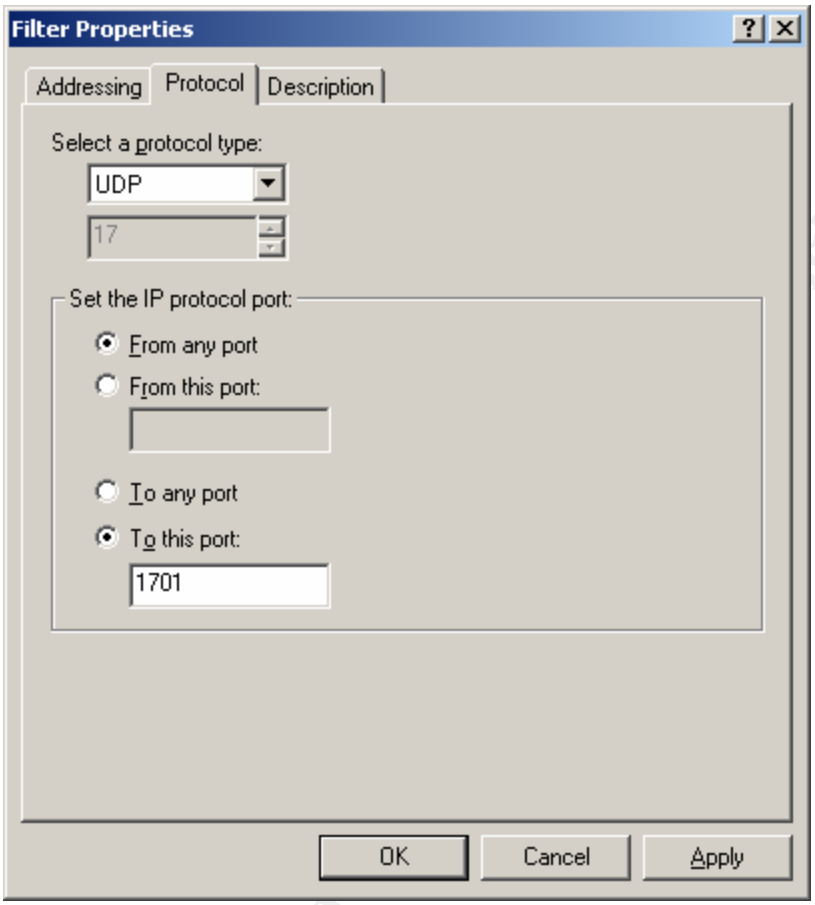
Double-click All IP Traffic and double-click All IP Traffic a second time. The following window should be displayed:



Double-click the highlighted row and then click the Protocol tab. The following dialog box will be displayed:



Use the drop-down box to select UDP as the protocol. Then select the To This Port radio button and fill in 1701 as the port. This is shown below.



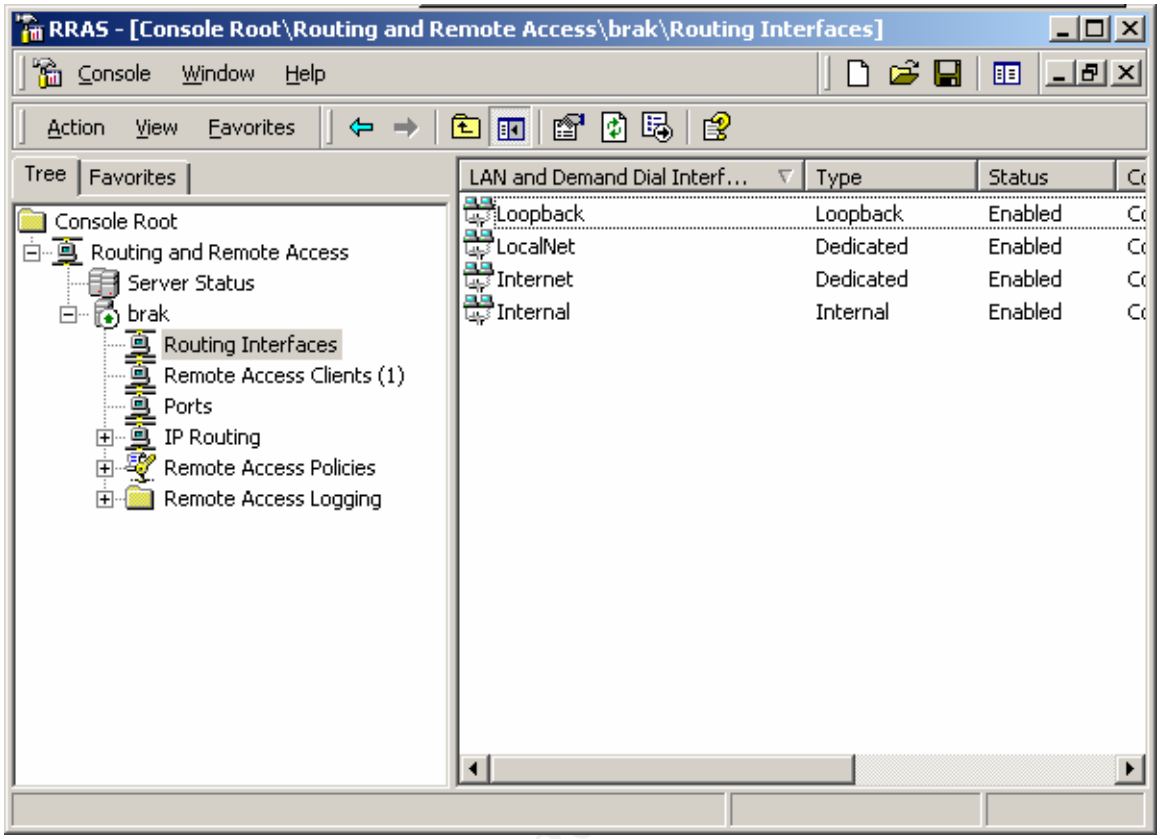
Click OK, Close, Close, Close, Close to return the main IP Security Policy console.

3.5. L2TP Client Configuration

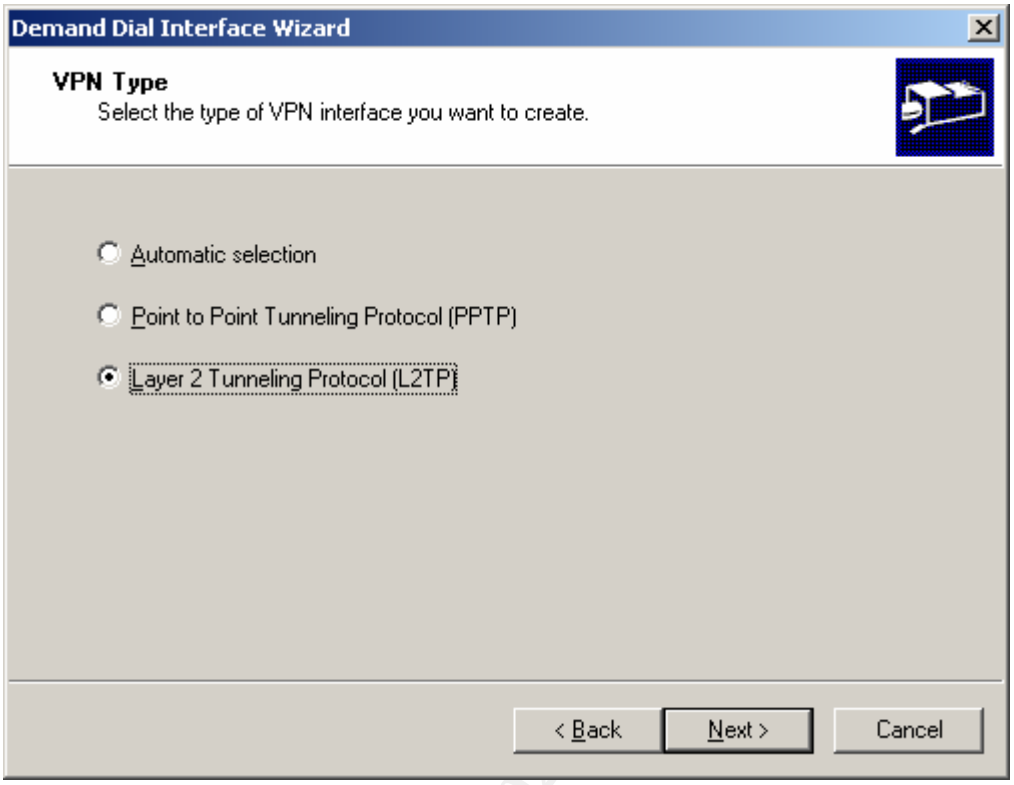
The L2TP Client can either be a demand-dial connection or a client VPN connection. This section will describe how to create the demand-dial connection.

First the L2TP demand dial connection requires an IP Sec Policy. To create the IPSec Policy, repeat the steps in section 3.4.2.

After the IPSec Policy is created, open the RRAS MMC on the demand-dial end-point. Open the server object and select Routing Interfaces. The console should look similar to the picture below.



Right-click Routing Interfaces and select new Demand-Dial Interface. This will activate the Demand Dial Interface Wizard. Click Next to continue. Provide a meaningful name for the Demand Dial interface and click Next. The following dialog box will be displayed.



Select Layer 2 Tunneling Protocol (L2TP). The Automatic selection choice is suppose to first attempt an L2TP connection, and if that fails, try a PPTP connection. Based on packet traces of the sessions, selecting Automatic did not initiate any L2TP packets. Instead only data to create a PPTP session was captured.

Type the DNS name or IP address of the RRAS Server. Click Next. Accept the default to only route IP packets and select Next. Now supply user name credentials that were authorized as a RAS user. Click next and click Finish.

This completes the configuration.

4. Trouble-shooting Tips

- Make sure the RRAS server is auditing logon events, success and failures. The ISAKMP service, which performs the key exchanges, will post events to the Security Event log, if logon events are audited. The events include information such as which encryption algorithms were requested and which were sent. This is especially useful in the event of an mismatch.
- Make sure both the client and the server are using the high encryption pack or not. This makes troubleshooting the key exchanges easier. If the client or server request a higher level of security than available, an application is generated by the ISAKMP/Oakley service.