Chapter 11

Harden Communications

- Protect LAN Communications
- Protect WAN Communications
- Protect Web Communications with SSL

Three basic security processes can be used to harden network communications: authentication, integrity, and encryption. Computer *authentication* is essential in order to ensure that data is actually coming from and going to appropriate computers. If a communication can spoof its origination, or if a destination can be spoofed, then there is no way to know if the information is correct, and no way to avoid sending confidential information where it should not go. *Integrity* ensures that the data has not changed during transport. If integrity is not guaranteed, then an attacker might successfully change data. *Encryption* protects data by making the message useless to any but those possessing the key. While not every protocol designed for communications security does all three, the best protection for data communications will.

An additional security mechanism, *message signing,* can guarantee that a specific message came from the computer identified as the source of the message. As part of the negotiation process, the client and server are authenticated. If authentication fails, the communication does not proceed. If authentication is successful, each packet sent is signed by the source. Without message signing, session hijacking can occur. Session hijacking is an attack where communications are intercepted and modified en route.

Protect LAN Communications

Communications between computers on the LAN can be secured using either SMB message signing or IPSec. While IPSec is a more secure protocol, it is not as easily implemented, nor available for all versions of Windows. SMB message signing can be configured for Windows NT 4.0 (post service pack 3) as well as Windows XP, Windows Server 2003, and Windows 2000. Windows 95/98 computers running the Directory Services client can also be configured to do SMB message signing. Windows 9*x*, Windows ME, and Windows NT 4.0 cannot use IPSec in transport mode.

NOTE An update for Windows 9*x*, Windows ME, and Windows NT 4.0 allows these OSs to participate in L2TP/IPSec VPNs. This is different, however, than IPSec in transport mode.

Use SMB Message Signing and Session Security for NTLM

Server Message Block (SMB) is the protocol used for file sharing and other communications between Windows computers. It is the basis for NetBIOS communications. SMB signing guarantees the origination of the communication. It is enabled by default on Windows Server 2003 computers but must be configured on the other Windows OSs. Once configured, SMB signing is negotiated during the connection request and systems that cannot use SMB signing may not be able to communicate with those that can. Two different types of configuration can be configured. First, and most effective, is to configure both server and client to always require SMB signing. Alternatively, signing can be established by mutual agreement.

NTLM Session security allows encryption (confidentiality) and integrity to be configured.

HEADS UP!

When SMB signing is required, legacy operating systems and some legacy programs will not be able to communicate. There may also be compatibility issues between later versions of Windows. For example, the KB article 823659 indicates that the secure channel of a trust between Windows NT 4.0 and Windows Server 2003 cannot be reset, that copying files between Windows XP and Windows Server 2003 will be much slower, and that you will not be able to map a network drive from the client.

Configure Message Signing Using Group Policy

To configure SMB message signing in Windows Server 2003, Windows XP, and Windows 2000, use the following Group Policy options:

- Microsoft Network client: Digitally sign communications (always)
- Microsoft Network client: Digitally sign communications (if server agrees)
- Microsoft Network server: Digitally sign communications (always)
- Microsoft Network server: Digitally sign communications (if client agrees)

Configure Message Signing Using Registry Entries

To configure client-side SMB message signing in Windows NT 4.0 post service pack 3, and in Windows 95/98 computers running the Directory Services client, add the REG_DWORD registry value RequireSecuritySignature or EnableSecuritySignature and set the value to 1. To disable SMB signing, set the value to 0. The value location is the registry path

```
HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Services\
LanmanWorkstation\Parameters\RequireSecuritySignature
```

To configure server-side SMB message signing for Windows NT 4.0 post service pack 3, configure the value at the registry path

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\
Parameters\RequireSecuritySignature
```

Windows NT 4.0 must be restarted for the configuration to be enabled.

Configure NTLM Session Security

Two Group Policy Security Options control NTLM Session security settings:

- Network Security: Minimum session Security for NTLM SSP-based (including secure RPC) clients
- Network Security: Minimum session Security for NTLM SSP-based (including secure RPC) servers

For each, four options are available:

- Require message integrity
- Require message confidentiality
- Require NTLMv2 session security
- Require 128-bit encryption

Use IPSec Policies

IPSec is a security protocol built in to the Windows TCP/IP stack of Windows XP, Windows Server 2003, and Windows 2000. An IPSec policy can be configured and assigned that will protect communications by providing mutual computer authentication, encryption, integrity, protection from replay attacks, and message origination authentication. It is also widely used as a security protocol in VPNs. Its use in Windows-based VPNs is discussed in the later section "Use L2TP/IPSec VPNs."

Here are three major uses for IPSec in Windows LANs:

- To provide encryption of communications between two computers
- To manage connections on the basis of IP address and protocol used
- To prevent connections to network resources from rogue computers

IPSec policies are created using Group Policy. A policy can be developed and assigned to a single computer at a time using the local group policy, or configured in a GPO linked to an OU or entire domain and thus implemented on any number of computers.

IPSec is a complex protocol, and to thoroughly understand and troubleshoot IPSec is beyond the scope of this book. A few simple facts, however, will allow you to write and use the simple policies outlined here. These facts are easier to understand by following the policy steps, but these are their basics:

- A policy is composed of rules, filters, and filter actions.
- Rules are composed of settings and a list of filters.
- Filters specify source and destination IP addresses and protocols.
- Filter actions determine what happens if a rule's filter is matched.

- Possible filter actions are: Block, Permit, and Negotiate. Rules are often referred to by their filter action.
- Each rule can have only one filter action; however, a policy may be composed of one or more rules.
- In order for Allow and Negotiate policies to work, each computer involved must have an IPSec policy assigned.
- IPSec policies are not in effect until the policy is assigned.
- Policies may be scripted, or the IPSec Policy Wizard can be used.
- Three methods of authentication are available. Kerberos (only in Windows domains), certificates (all computers must have certificates and must be able to validate them), preshared key (the weakest, but good for testing).

HEADS UP!

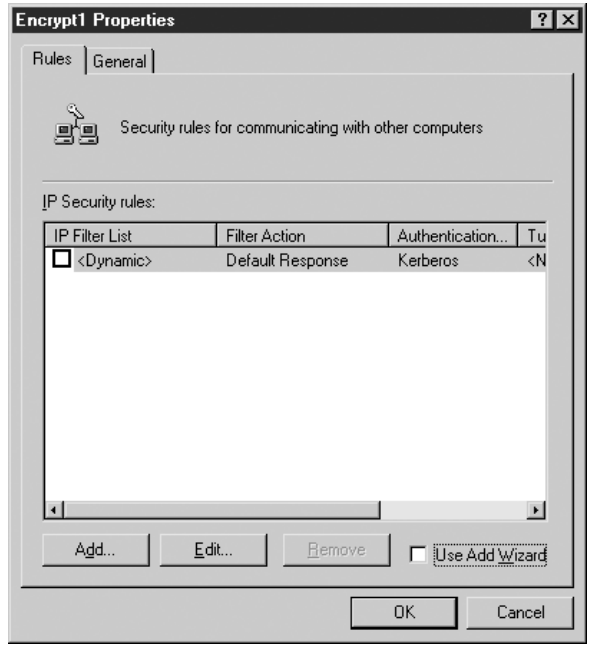
It is possible to create an IPSec policy that can so successfully shut down communications that recovery of the computer system may be a difficult chore. To prevent complications, always test an IPSec policy in a test environment and always start by implementing the policy on one test computer at a time, then moving to a test domain.

Use IPSec for Confidentiality

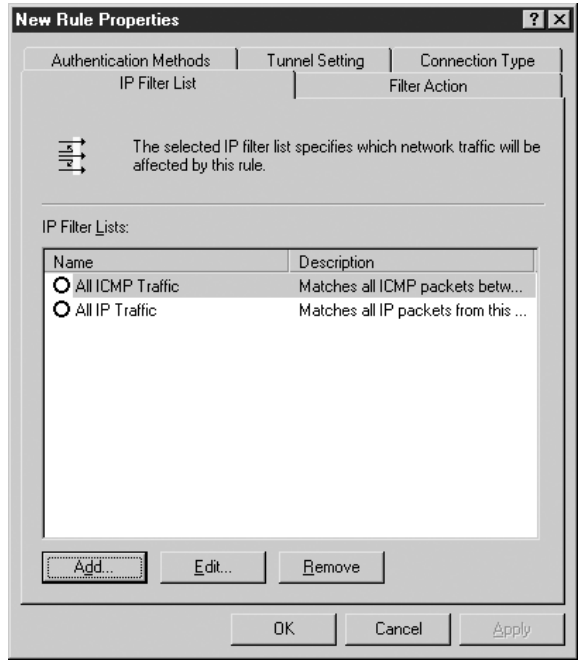
To protect communications between two computers, use an IPSec negotiation policy. The following steps outline how to build a policy that encrypts communication between computer A with an IP address of 192.168.7.55 and computer B, which has an IP address of 192.168.7.155.

1. Add the IP Security Policy Management snap-in to an MMC console on computer A.
2. Right-click the IP Security Policies on Local Computer container, as shown here, and select Create an IP Security Policy.
3. Click Next on the Welcome page.
4. Enter the name **Encrypt1** for the policy and click Next.
5. Uncheck Activate the Default Response Rule.
6. Click Next; then click Finish.

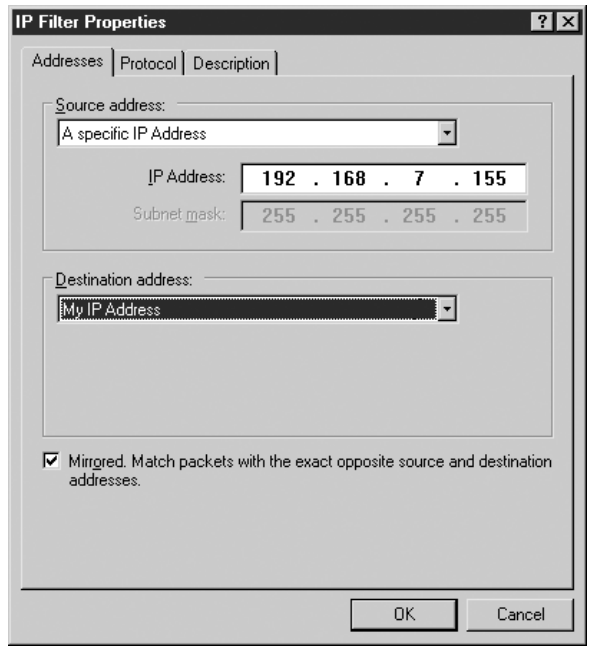
7. On the Encrypt1 Rules page, click Add, as shown here, to add a new rule:



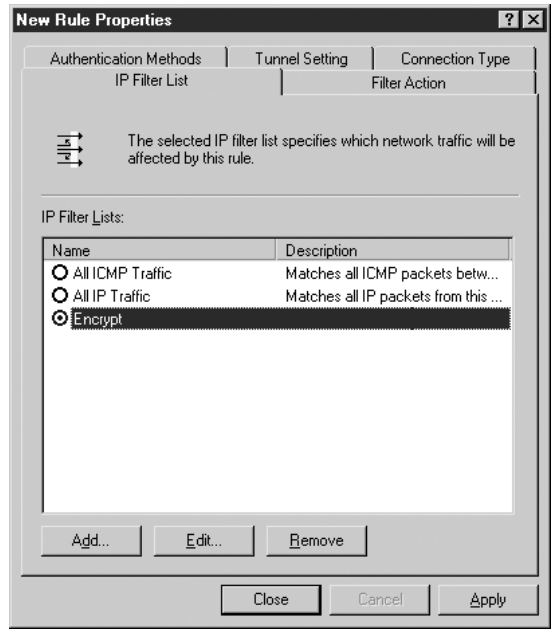
8. On the New Rule Properties IP Filter List page, click Add to create the filter list.



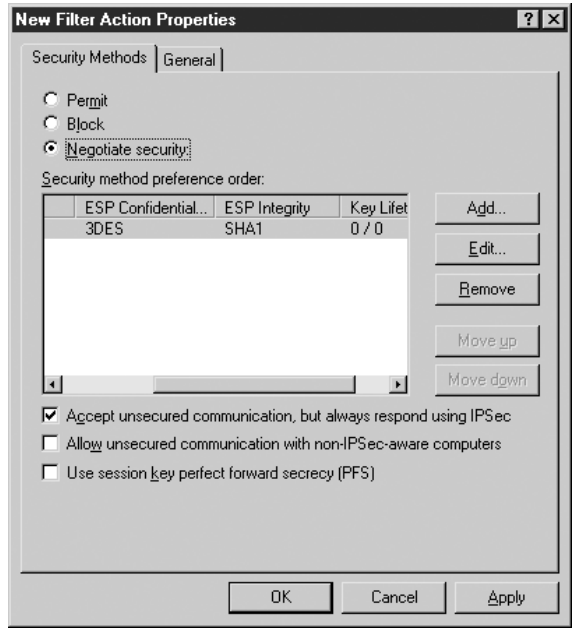
9. Enter **Encrypt** to name the filter list.
10. Uncheck the Use Add Wizard box and click Add to add a filter.
11. In the Source address drop-down list box, select A Specific IP Address.
12. Enter the IP address of computer B, **192.168.7.155**.
13. In the Destination address drop-down list box, select My IP address, as shown here:



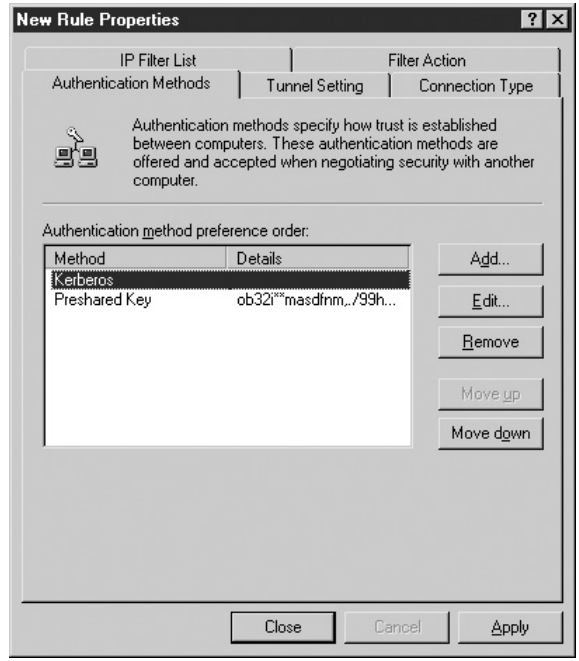
14. Click OK to close the IP Filter Properties list page and click OK to close the IP Filter List page.
15. In the IP Filter List tab, select the Encrypt entry (the list you just created), as shown in the following illustration, and then click the Filter Action tab.



16. Click to deselect the Use Add Wizard button and click Add to add a filter action.
17. On the New Filter Action Properties page, select Negotiate Security.
18. Click Add to add a security method. The default selection, Integrity and Encryption, is acceptable. By default, 3DES and SHA1 are selected. Click OK.
19. Click Accept Unsecured Communication, But Always Respond Using IPSec, as shown here:



20. Select the General page and enter **Negotiate** for the Filter Action name; then click OK.
21. Select Negotiate on the Filter Action page.
22. Select the Authentication Methods page and click Add.
23. Select Use This String (Preshared Key). Enter a long, complex key and then click OK.
24. Select Kerberos in the Authentication Method Preference Order box and click Remove. Click OK to respond to the pop-up. Note in the following illustration that the shared key is partially visible in the interface.



25. Click Close twice to exit the policy.
26. Export the policy and import it on computer B, or re-create the policy on computer B and in both cases change the Source address to that of computer A.
27. On computer A, in the IPSec console, right-click the policy, and select Assign to assign the policy. Until you assign the policy, it is not in effect.
28. Repeat on computer B. (Don't forget to change the IP address you entered in step 11.)

Use IPSec to Manage Connections

In the preceding example, a policy was created that requires all communications between computer A and computer B to be encrypted. It also is a policy that manages connections. Although communications with other computers are unaffected, the policy does restrict communications between computer A and computer B.

IPSec policies can do more than control whether or not two computers must encrypt information sent between them. Polices can manage connections in other ways:

- Block all communications from a specific IP address, or range of IP addresses.
- Block all communications over a specific protocol/port.
- Permit communications from a specific IP address or a range of IP addresses.
- Permit communications over a specific protocol/port.
- Negotiate communication in terms of these items as well as in terms of the ability of a computer to use specified encryption, authentication, and integrity choices.

To use IPSec policies for these features, create a policy using the preceding steps but use the following adjustments.

When adding filters (see step 7) instead of using the IP address information described, use the destination and source IP address information required. In Windows Server 2003, in addition to naming a specific IP address or a specific IP subnet, you may select DNS, DHCP, WINS, or default gateway information. (The computer's TCP/IP configuration information will be used to supply the IP address of the servers from which IP addresses will be used.) Choices in Windows 2000 are more limited.

When adding filters, after managing IP address information, select the Protocol tab on the IP Filter Properties page. Use the Select a Protocol Type drop-down box to select a protocol. Use the Set the IP Protocol Port buttons and text box to set specific boxes. Figure 11-1 shows the configuration to filter on the Telnet protocol.

- Make as many filters as you want, but remember that only one filter action can be selected per rule. If you need to write a policy that blocks all telnet communications to a server but allows an encrypted telnet session from a specific computer, you will need two rules.
- Use the Filter Action page to select the filter action for the rule, or to add a filter action. The Permit filter action is present, for example, but the Block filter action is not.

Use IPSec to Prevent Connections from Rogue Computers

If an IPSec policy requires certificate authentication, and certificate distribution is controlled, then rogue computers can be prevented from connecting to network resources. This type of policy does not specify encryption or integrity. Instead, it simply requires that each computer authenticate using a certificate. If you implement

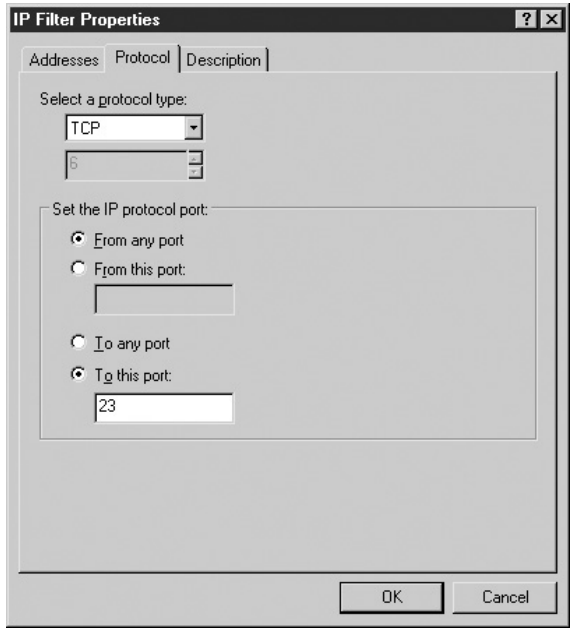


Figure 11-1. Use the IP Filter property pages to identify specific protocols.

a Windows Enterprise Certification Authority and configure automatic certificate enrollment for computers, all computers joined in the domain will have the certificate. Rogue computers, those computers brought from home by employees or brought along by contractors, vendors, and visitors, will not be able to authenticate to protected resource computers on your network.

To protect computers, create a domain IPSec policy that requires certificates for authentication but does not require anything else.

1. Right-click the IP Security Policies on Local Computer container and select Create an IP Security Policy.
2. Click Next on the Welcome page.
3. Enter a name for the policy and click Next.
4. Uncheck Activate the Default Response Rule.
5. Click Next; then click Finish.
6. Click Add to add a filter, and then select the Protocol page. Select All IP Traffic. Examine this filter list by clicking the Edit button. Note that it matches all

traffic with the exception of broadcast, multicast, Kerberos, RSVP, and ISAKMP. You can write a more specific rule to block all traffic if you wish. Click Close to close the page.

7. On the New Rule Properties, select Authentication Methods.
8. Click Add.
9. On the Authentication Method page, select Use a Certificate from This Certification Authority (CA).
10. Use the Browse button to select a copy of the CA certificate. (The Browse button defaults to the Enterprise Trust certificate store of the local computer; you must make sure that a copy of the appropriate CA certificate is in the store of each computer.) Click OK.
11. Select the Filter Action page.
12. Click Add to add a new filter action.
13. Select Negotiate Security.
14. Click Add to create a Security Method.
15. Select Custom, and then select Settings.
16. Click to deselect Data Integrity and Encryption (ESP) and select Data and Address Integrity Without Encryption (AH) as shown in the following illustration. Then click OK.

17. Select the General page and enter a name, **Authentication for the new Filter action**. Then click OK.

18. Select Authentication and click Close; then click OK to close the policy.
19. Assign the policy to all domain computers after testing.

Protect IPSec-Protected Computers During Startup

When IPSec is used to protect communications, there is a brief period of time during computer startup when network connections are possible and yet IPSec is not enforced. This is the point after which the TCP/IP driver and the IPSec driver have started, but the IPSec Policy Agent service has not yet started and applied the local- or domain-configured IPSec policy. To protect computers during this critical time, you can set the computer startup mode to block and set a persistent IPSec policy. Persistent policies are in effect whether or not IPSec policies managed by the IPSec Policy Agent are.

Set Computer Startup State To set the computer startup state to block, use the following **netsh** command:

```
netsh ipsec dynamic set config bootexemptions value=tcp:0:3389:inbound
```

In some cases, you may want to be able to manage the computer (for recovery, for example) by using the Remote Desktop for Administration. You can set this capability by using this command. You must then create a persistent policy that will negotiate the connection between the computer and the administration station.

Set Persistent Policy To set a persistent policy, you must use the **netsh** command. It is not possible to do so using the GUI. A persistent policy is in effect as soon as the IPSec driver starts. You can use such a policy to block all communications, then, in your IPSec policy, Allow the communications required for the specific computer. Creating a persistent policy consists of two steps. First, create an IPSec policy using **netsh** and assign it. Next, set the policy to be persistent.

A full discussion and tutorial on using **netsh** to create IPSec policies is beyond the scope of this book. Commands for assigning and making the policy persistent follow.

NOTE Information on using the **netsh ipsec** command can be found in "Netsh Commands for Internet Protocol Security" at www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/netsh_ipsec.asp.

To assign a policy named blockall:

```
set policy name=blockall assign=yes
```

Make the policy persistent:

```
set store location=persistent
```

Protect WAN Communications

In addition to local area communications, secure remote communications from other networks. Connections with other networks can be secured in a number of ways, but to secure the data as it travels between networks requires additional devices and protocols. Four technologies are currently in use:

- Dial-up access servers have a long history. Many of the legacy systems provide weak authentication and do not encrypt data in flight; however, reliable, securable dial-up access can be implemented using Microsoft tools.
- Virtual private networks (VPNs) are designed to provide tunneled, encrypted, and authenticated communication channels either client-to-server or gateway-to-gateway. Two protocols, PPTP and L2TP/IPSec, are used in Microsoft VPNs.
- The Secure Sockets Layer (SSL) has long been a methodology for authentication and securing communications between client computers and web servers; it is now commonly used as a portal to entire networks.
- Remote access rules can be applied to secure wireless networks. Even though wireless networks are often established as additional internal networks, an intruder could access them from outside the building because no physical access is required to connect to the network. Therefore, wireless networks should be thought about and secured according to remote access rules.

Hardening remote communications consists of hardening servers, clients, devices, and communications streams.

Harden the Remote Access Server

In addition to configuring secure remote access, harden the remote access server.

Harden Installation

Follow standard precautions during installation, including performing the installation offline and applying all service packs and hotfixes before adding the server to the network. Provide two network interfaces and provide secure configuration before connecting to the network.

Harden External Network Interface

The external network interface of the remote access server should provide only the basic connectivity required for the service. Two basic areas need configuration.

First, the external network interface should be configured to

- Remove File and Printer Sharing for Microsoft Networks by clicking to deselect it from the General Properties page of the connection.

- Disable NetBIOS over TCP/IP from the TCP/IP Advanced Properties, WINS tab as shown in Figure 11-2.
- Prevent attempts to dynamically register the network IP address in DNS from the TCP/IP Advanced Properties, DNS tab as shown in Figure 11-3. Attempts to dynamically register the network IP of this interface in an ISP's DNS may not be welcome. In addition, connections from external hosts should be configured on these clients. There is no reason to be resolving the Internet address of the remote access server.

Second, the network interface should be firewalled, and as an extra precaution, the Windows 2000 and Windows Server 2003 RRAS server can be configured to filter all packets on the external interface that are not necessary for remote access. See the later section "Harden Windows Server 2000 and Windows Server 2003 RRAS Configuration."

Restrict Services

Never run additional services on the RRAS server. If the Windows security baseline templates (see Chapter 8) are in use, place RRAS servers in their own OU and configure a GPO and link it to the OU. Enable the RRAS service and/or IAS service as appropriate for servers in the OU.

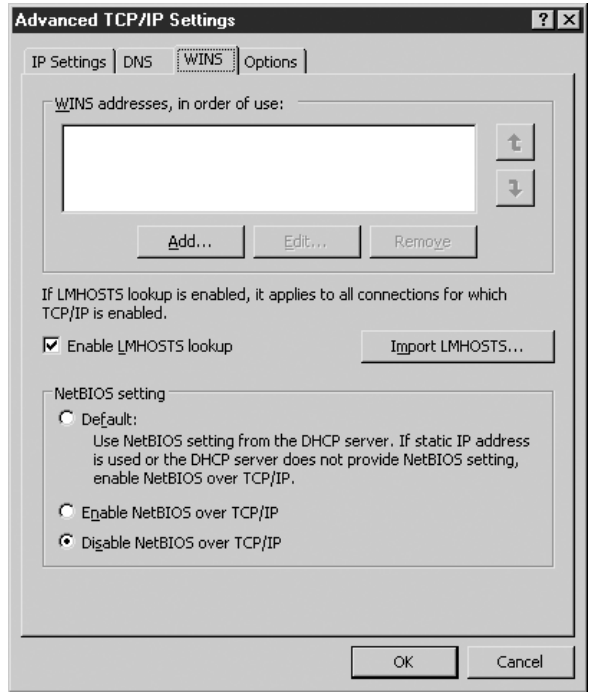


Figure 11-2. Disable NetBIOS over TCP/IP on the external network interface.

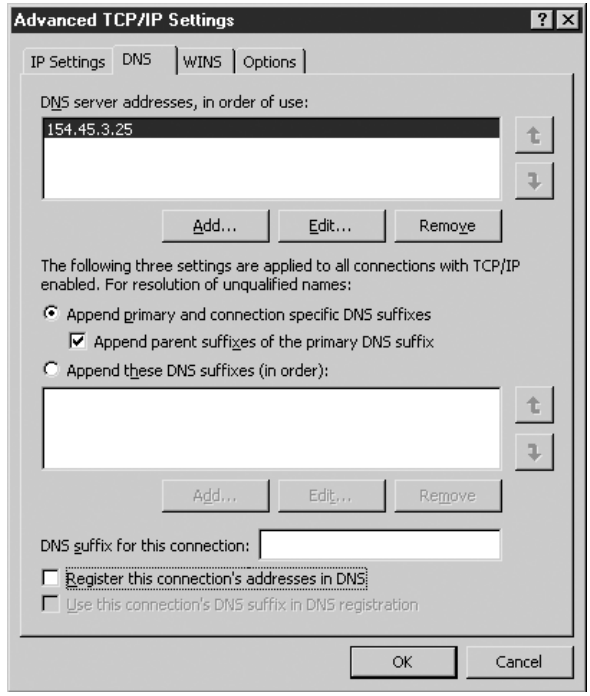


Figure 11-3. Prevent dynamic DNS registration.

Configure Auditing

In addition to auditing using the GPO, additional RAS and RRAS logs should be configured. In Windows NT 4.0, the ppp.log file is not created by default. This log can be created, and Point-to-Point Protocol (PPP) connections will be logged, by adding the Logging value and setting it to 1. The Logging value is of type REG_DWORD and should be added at

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP
```

After the value is set, you must stop and start the RAS service before the file will be created and PPP connections are logged in the SYSTEM32\ppp.log file. Although the original intention of this log file was to provide troubleshooting information, it can serve as a record of PPP connections for your auditing efforts.

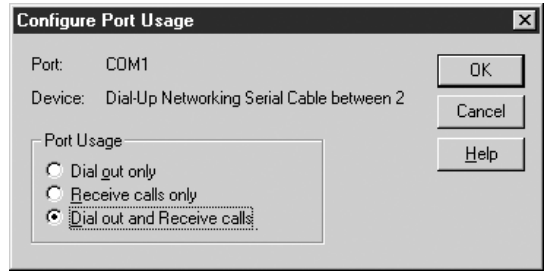
Harden NT 4.0 Remote Access Server Configuration

Windows NT 4.0 provides a basic dial-up Remote Access Service (RAS), and as an add-on, the Routing and Remote Access Service (RRAS). Dial-up access can be secured using MS_CHAPv2 authentication and data encryption, but these choices must be configured. Weaker authentication protocols and lack of encrypted communications were originally provided to ensure the ability to service connections from legacy clients.

Harden Access Port Usage

Use only the required COM port access. In many cases, this means that the RAS server should be configured only to receive calls. If the RAS server is configured for dial-back, however, configure the server for both incoming and outgoing calls.

1. Open the Network interface by right-clicking Network Neighborhood and selecting Properties.
2. Select the Services tab, select Remote Access Service, and then click Properties.
3. From the Remote Access Setup dialog box, click Configure.
4. Select the Dial Out and Receive Calls radio button as shown here:

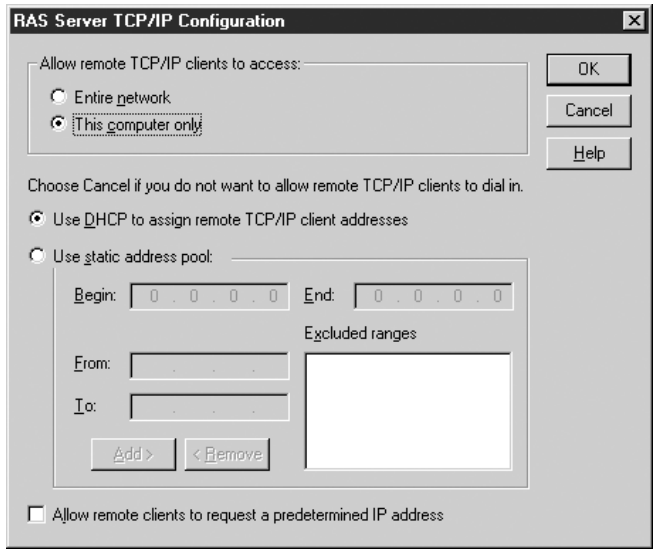


Harden Network Configuration

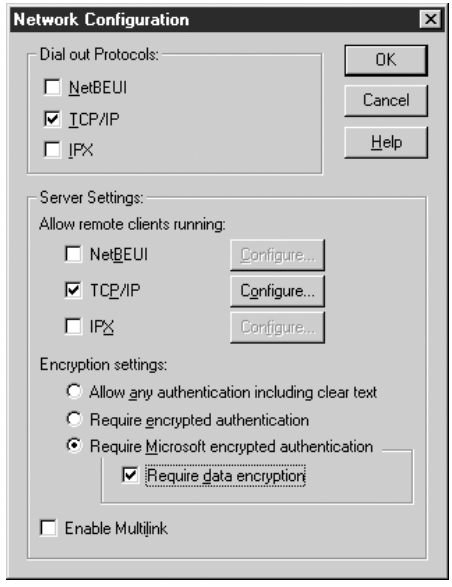
RAS network configuration can be secured by limiting the protocols to those used, and by requiring encryption.

1. From the Remote Access Setup dialog box, click Network.
2. Set the dial-out protocols.
3. Set the Server settings to restrict access from clients. If clients must be running IPX, for example, select only this protocol. Clients attempting to connect using another protocol will be unsuccessful. Select only those protocols your network requires. In this example, only TCP/IP has been selected.
4. Click the Configure button next to the protocol.
5. If clients need access only to specific data and that data can be available on the RAS server, then click This Computer Only in the Allow Remote TCP/IP Clients to Access box as shown in the following illustration. This will prevent

clients from accessing other network resources. The RAS server will not act as a portal to the rest of the network.



6. Click OK.
7. Select Require Data Encryption, as shown in the following illustration. MS-CHAP must be used for authentication to enable data encryption. Table 11-1 provides information on how to select other authentication protocols.



8. Click OK, and then click Continue.

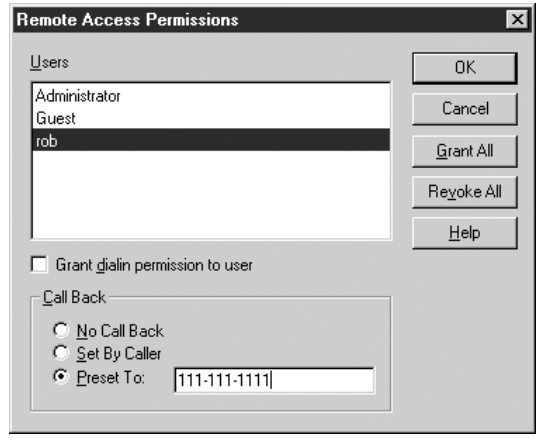
Network Configuration Selection	Authentication Protocols Accepted	Discussion
Allow Any Authentication Including Clear Text	MS-CHAP, SPAP, PAP	Not an acceptable selection.
Require Encrypted Authentication	MS-CHAP, SPAP	Passwords must be encrypted.
Require Microsoft Encrypted Authentication	MS-CHAP, MS-CHAPv2	If you require data encryption, you must use MS-CHAP, or MS-CHAPv2. You cannot use SPAP or PAP. Configure clients to use MS-CHAPv2 for the most secure connection.

Table 11-1. Authentication Choices for Windows NT 4.0 RAS

Harden Client Access

The first step in hardening client access is to provide permission to only those users who should have remote access. The second is by requiring callback where possible. When callback is configured, the server terminates the successful client initial connection and dials the specified phone number. This ensures that the connection can be made only with a designated location. When users always work from the same location, callback can be an effective security measure as long as physical access to the phone line is restricted to the authorized user. When users travel and must use dial-up remote access, callback cannot provide this. Remote access is configured by visiting the user account property pages in User Manager or by using the Remote Access Admin tool.

1. Open Remote Access Admin via Start | Programs | Administrative Tool.
2. From the Users menu, select Permissions.
3. Select the user account from the Users box.
4. Select Grant Dialin Permission to User.
5. If users work from an established phone line (the same phone number all of the time), select Preset To and enter the phone number, as shown here:



6. Configure additional users.
7. Click OK to close the dialog box and then click Exit from the Server menu.

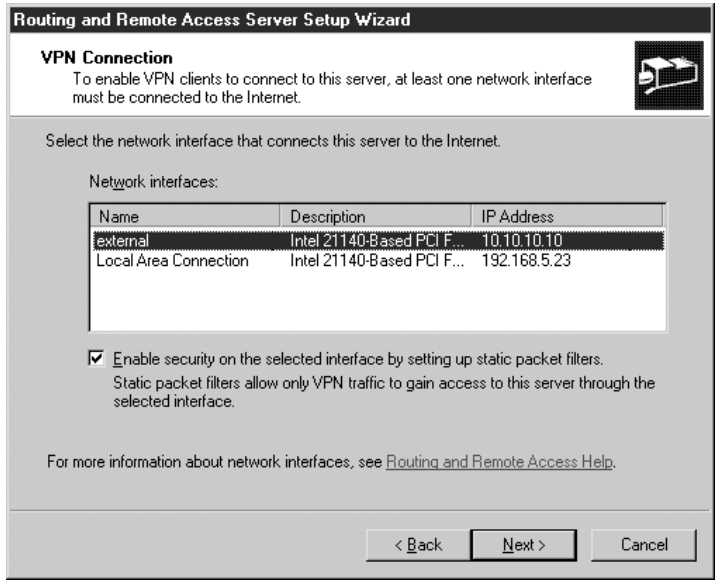
Harden Windows Server 2000 and Windows Server 2003 RRAS Configuration

While Routing and Remote Access Services can be installed on Windows NT 4.0, I recommend avoiding the use of RRAS on Windows NT 4.0. Instead, use Windows 2000 or Windows Server 2003, which provide additional security and manageability. If you must use RRAS on Windows NT, adapt the recommendations given for Windows 2000 and Windows Server 2003 RRAS to Window NT 4.0.

RRAS provides dial-up and VPN remote access. In addition to client-to-server VPNs, RRAS provides gateway-to-gateway VPN services. Network Address Translation (NAT), packet filters, and Remote Access Policies add additional configuration features. Since the versions are so similar, Windows Server 2003 is used for the examples in the following configuration settings. Differences with Windows 2000 will be noted.

Secure External Network Configuration with Packet Filters

Windows Server 2003 packet filters can be configured to secure the external network interface, permitting only VPN traffic access. To do so during RRAS setup, select the external network interface on the VPN Connection page and then select Enable Security On the Selected Interface By. . . as shown here:

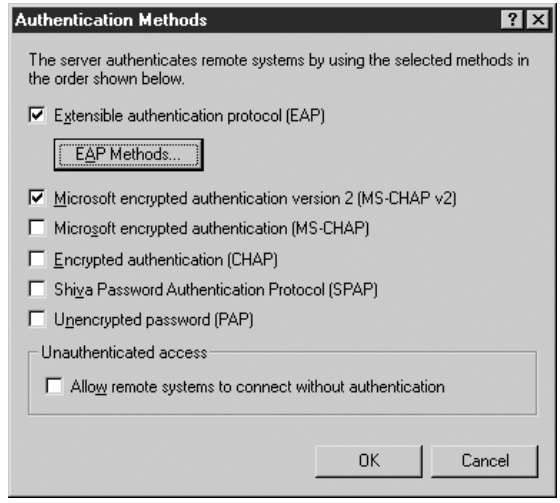


To manage connections after setup, use Remote Access Policies and set Input Filters as discussed in the later section "Use Remote Access Policies."

Harden Authentication

Authentication is configured from the Server Security property page. Currently the best solution is to require smart card authentication. If that is not immediately possible, then restrict the authentication methods possible.

1. Right-click the server in the Routing and Remote Access console and select Properties.
2. Select the Security tab.
3. Click the Authentication Methods button.
4. Deselect Microsoft encrypted authentication (MS-CHAP), as shown in the following illustration. All Microsoft clients from Windows 95 onward can be configured to use MS-CHAPv2, which has many improvements over MS-CHAP. (Do not select legacy remote access communication protocols.)

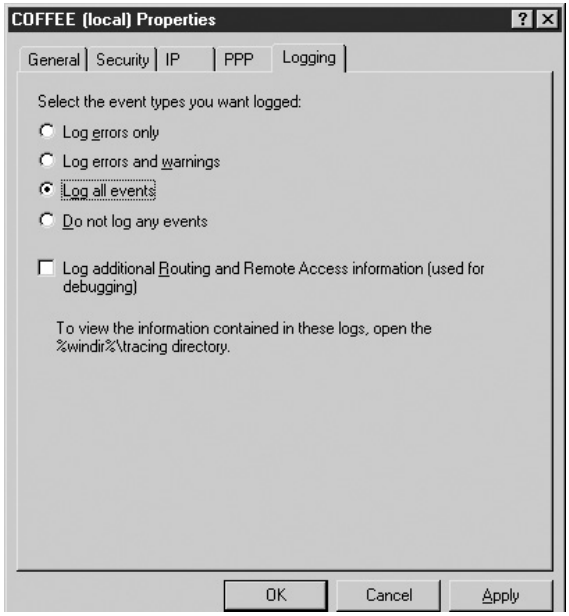


5. Click EAP Methods. The Extensible Authentication Protocol can be used to configure advanced authentication methods, including Protected EAP (PEAP) and smart card or certificate authentication. They are configured in Remote Access Policies, but this property page defines the EAP methods installed on the Remote Access Server.

If IAS should be used for authentication and/or auditing, this is configured on the Security page.

Configure Logging

Additional logging should be configured in order to provide a record of remote access connections. Logging is configured from the Logging page of the remote access server's property pages. Select Log All Events as shown here:



In addition, in Windows Server 2003, a Remote Access logging node in the Routing and Remote Access Console enables configuration of logging. Use the Settings page to limit logging to select logging for authentication, accounting, and status. (If IAS is used, and authentication and accounting tasks are split between different servers, configure authentication and accounting on the respective servers.)

If log files are moved to a SQL Server database, protect communications between the SQL server and the RRAS servers by using IPSec.

You may locate the log files to a different location, but if you do, secure the log files by setting the DACL to access by SYSTEM and Administrators groups only. Audit who accesses the log files.

Use a Firewall

Use a firewall to protect the RRAS and IAS servers. If RADIUS messages must traverse a firewall, create a rule to allow communications for the RADIUS ports listed in Table 11-2.

RADIUS Ports	Authentication Messages	Accounting Messages
Standard	UDP 1812	UDP 1813
Alternative	UDP 1645	UDP 1646

Table 11-2. RADIUS Ports

Configure Client Access

As in Windows NT 4.0, accounts in Windows 2000 and Windows Server 2003 are denied remote access by default. Users must be configured for remote access. If Windows 2000 domains are in native mode, or Windows Server 2003 domains are at least at Windows 2000 functional level, access permission may be configured using Remote Access Policies. Otherwise, access is configured similar to that for Windows NT 4.0 domains.

HEADS UP!

Each user account is configured to Deny access, Allow access, or rely on Remote Access policies. When Remote Access policies are used, connections and attempts to connect are a result of a combination of account dial-in properties and remote access policy constraints. However, if an IAS profile constraint is configured to ignore user dial-in properties, then account dial-in properties are not considered. A user may be configured in account properties to Deny remote access, and yet it may be possible for that account to connect. To evaluate remote access, you must evaluate each remote access policy in addition to user settings.

For each user account, remote access is configured from the Dial-in tab of the user account properties as shown in Figure 11-4.

Use L2TP/IPSec VPNs

Where dial-up access is required, require the use of VPNs and do not allow plain dial-up connections. VPNs are a better choice for security. Two VPN types can be configured. Where possible, use L2TP/IPSec. PPTP is considered to be a less secure VPN protocol than L2TP/IPSec; however, it can provide secure communications if correctly configured. In general, though, L2TP/IPSec is simply a better choice. Important differences in these technologies are listed in Table 11-3.

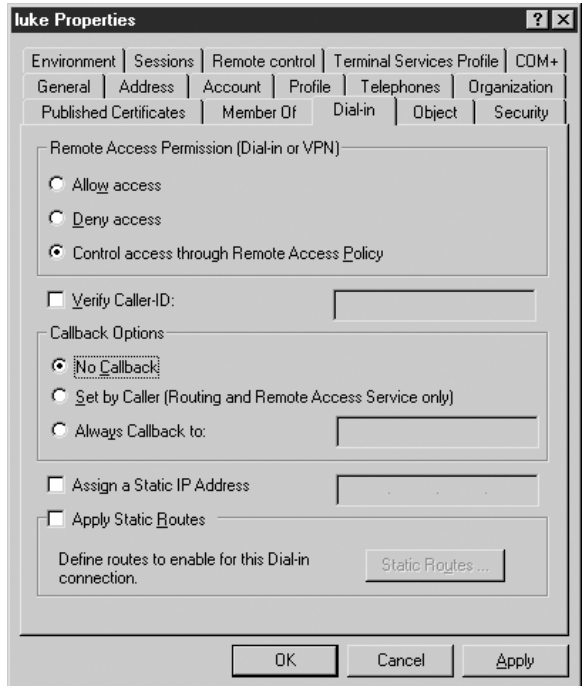


Figure 11-4. Remote access can be controlled via Remote Access Policies.

Technology	PPTP	L2TP/IPSec
Encryption	Microsoft Point-to-Point Encryption (MPPE). Only the data payload is encrypted.	IPSec. Encrypts most parts of the packet.
Tunnel	PPTP	L2TP
Authentication	User based. May be mutual, for example with MS-CHAPv2.	Requires mutual machine authentication via certificates. (Can be configured for shared secret. Do not do so.)
NAT	Typically no problems.	Can cause problems as NAT-T-compliant clients and servers enable the use of IPSec over NAT.

Table 11-3. Differences in PPTP and L2TP/IPSec VPNs

When VPN access is configured during setup, both PPTP and L2TP/IPSec ports are configured on the RRAS server. No configuration is possible directly on the ports. Settings on clients determine which protocol is used; however, if you can restrict VPN access to one or the other, you may delete the other type of communication port.

NOTE The L2TP/IPSec standard as originally written is incompatible with NAT because IPSec-encrypted packets including a checksum calculated over the IPSec source address. Since NAT modifies the source address, packets are considered to be corrupt or modified and dropped when received. NAT-Traversal, or NAT-T, uses UDP to encapsulate the IPSec packet, and therefore the packet can pass through the NAT server without a modification that will cause problems for IPSec. The NAT server must implement NAT-T. The Windows Server 2003 implementation of Internet Key Exchange (IKE), a component of IPSec, can detect NAT-T and use UDP-ESP encapsulation.

Use Remote Access Policies

When remote access policies are used, user accounts in Windows Server 2003 and/or Windows 2000 domains are configured to Control Access Through Remote Access Policy. However, the default remote access policy is configured to deny all remote access requests. Do not delete the default remote access policy.

Remote access policies are used to provide remote access configuration. The beauty of remote access policies is that many policies can be created, each specifically designed for a group of clients, a time of day, or some physical device requirement. This allows for many models of remote access control. While it is not the most desirable response, you can create a weak policy for use with legacy clients, while retaining more secure authentication and encryption for others. The weakest connections do not have to dictate security for the entire organization. Hardening remote access connections can be accomplished by setting up proper remote access policies. The following list of hardening steps is presented during a walkthrough of remote access policy creation for connections by the custom-created Auditors group. When IAS is used to centralize RRAS, additional settings can be configured. Techniques for hardening connections according to policy conditions are listed in Table 11-4. A policy condition is checked when a connection attempt is made. If the properties of a connection match the policy condition in a remote access policy, then the remote access policy is applied.

Condition	Recommendation
Authentication Type	Create policies that deny connections based on the use of legacy authentication types.
Called Station-ID	Combine with user groups and/or times of day and deny access to specific numbers. Identify restraints for allowed connections to a specific number.
Calling Station–ID	Create policy profile restrictions according to the specific location.

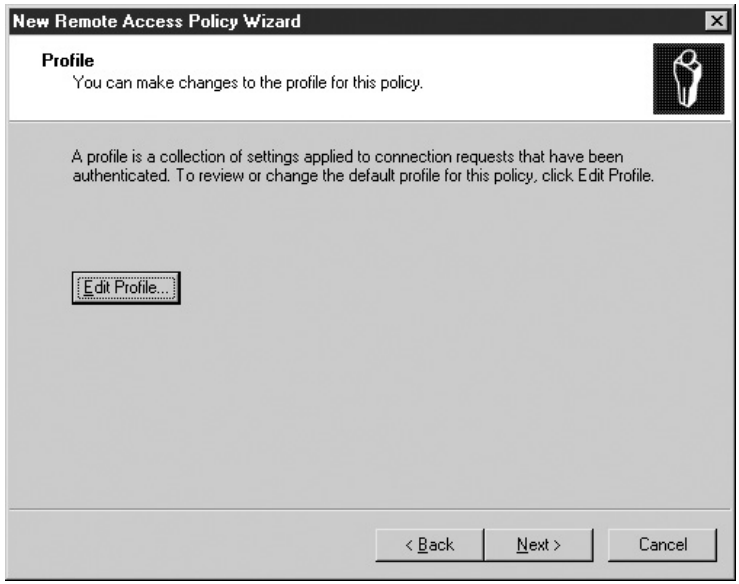
Table 11-4. Policy Conditions

Condition	Recommendation
Day and Time restrictions	Deny or allow access according to the time of day.
Tunnel type	Deny or allow access depending on the protocol; specifically, prevent access via PPTP to force use of L2TP/IPSec.
Windows Groups	Deny or allow access by Windows user group.
Service Type	Deny connections according to the service requested; for example, prevent the use of telnet through this remote access server.

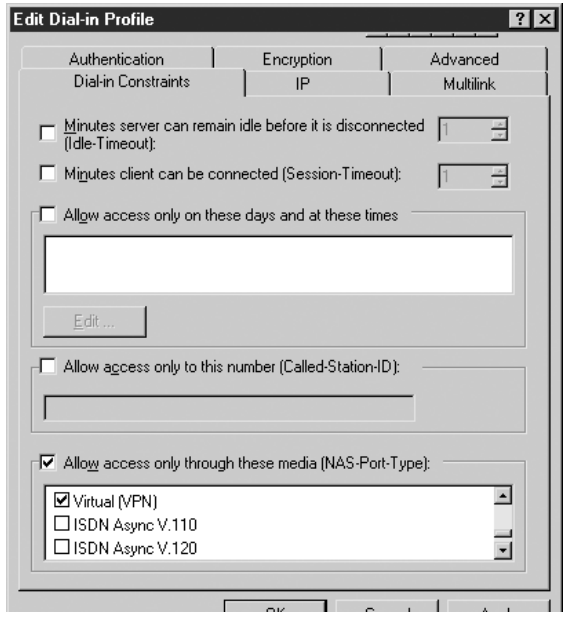
Table 11-4. Policy Conditions *(continued)*

To use remote access policies:

1. Right-click the Remote Access Policy node of the Routing and Remote Access console and select New Remote Access Policy. Then click Next.
2. Select Set Up a Custom Policy, enter a name for the new policy, and then click Next.
3. Click Add to add a policy condition. Select Windows-Groups and click Add.
4. Click Add and enter or browse to and select the Auditors group.
5. Click Grant Remote Access Permissions; then click Next.
6. Click the Edit Profile button to open the Dial-in Profile property pages, as shown here:



7. Restrict connection type to VPN by selecting Allow Access Only Through These Media (NAS Port Type) and then selecting Virtual, as shown here:



8. Harden authentication. Click the Authentication tab; then click EAP Methods.
9. Click Add and select Smart Card or Other Certificate, and then click OK.
10. Click all other checked authentication methods to deselect them.
11. Require Strong Encryption. Select the Authentication tab.
12. Click to deselect Basic Encryption, click to deselect Strong Encryption, and click to deselect No Encryption.
13. Click OK. Then click Next and then Finish.

Harden Remote Access Clients

Client hardening should be done as a matter of installation and upkeep. Of critical importance on remote access clients is the use of a personal firewall and updated antiviral product. In addition, harden authentication, policy use, and encryption on the client. Client configuration can be centralized using Group Policy and for Windows NT 4.0, by creating profiles using the Connection Manager Administration Kit (CMAK). Like IEAK, CMAK is simply a way to create a standard user remote access profile and distribute it from a central location. The profile can be installed as part of an IEAK Package. A version is available for Windows 2000, Windows XP, and Windows Server 2003.

Use IAS to Centralize Authentication, Accounting, and Authorization

The Internet Authentication Service is the Microsoft implementation of RADIUS. When IAS is added to a network, it can provide centralized authentication, authorization, and auditing for remote access. Remote access policies are configured on the IAS server and manage policy for all RRAS servers configured to use the IAS server. (If remote access policies exist on the RRAS server, only the IAS remote access policies will be used.)

Harden the IAS server as you would the RRAS server. In addition, harden authentication and communications between RRAS and IAS servers.

Harden RADIUS/RRAS Authentication

When IAS is used for authentication, a shared secret must be configured on the RRAS and IAS servers and is used to authenticate connections between them. Use a long shared secret (22 characters or more) composed of a random sequence of letters, numbers, and punctuation and change it often. Use a different shared secret for each RADIUS client and RADIUS server pair, and for each RADIUS proxy and RADIUS server pair. (This will not be possible if you specify RRAS servers by IP address range.)

Provide RADIUS Message Authentication and Integrity

Use the Message Authenticator Attribute to protect IAS from spoofed IP addresses. RRAS servers are identified in the IAS properties and used to determine which RRAS servers can connect to IAS. When the Message Authenticator Attribute is used, an MD5 hash of the RADIUS message is made using the shared secret as a key. The IAS server can therefore determine that the message came from an RRAS server with knowledge of the shared secret, not just a server with one of the approved IP addresses. This also guarantees the integrity of the message.

The RADIUS Message Authenticator Attribute is configured on the property page of the RADIUS client in the RADIUS Clients node of the Internet Authentication Services console, as shown in Figure 11-5.

Use IPSec to Secure RADIUS Messages

Use IPSec to secure the entire RADIUS message. Create an IPSec policy that secures all communication between the RRAS and IAS servers.

Secure Wireless Access

Wireless access points (WAPs, or sometimes simply APs) should be considered the equivalent of remote access servers when a policy for their use is designed. While many steps can be taken to make wireless networks more secure without these advanced techniques, these techniques can markedly improve wireless security. A general discussion of hardening the normal wireless network is described in *Hardening Network Infrastructure* by Wes Noonan (McGraw-Hill/Osborne, 2004), a companion book in this series.

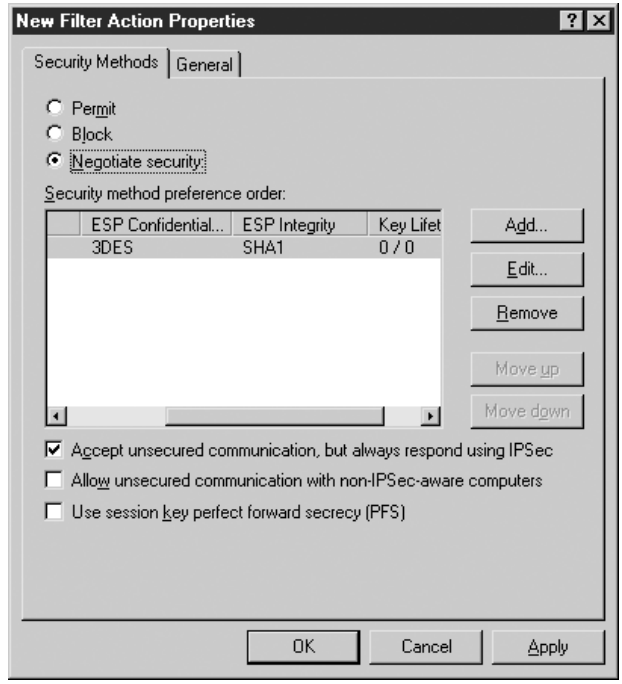


Figure 11-5. Insist on the use of the Message Authenticator Attribute.

The measures described in the sections that follow should be used to secure wireless access using Windows RRAS.

Require APs to Be Sanctioned by IT

A wireless security policy should dictate that APs are to be implemented only by IT and should specify enforcement consequences for setting up a rogue AP. Rogue APs should be disabled, and where security policy dictates, the employee who installs them should be terminated.

Require WPA and/or 802.1x Authentication

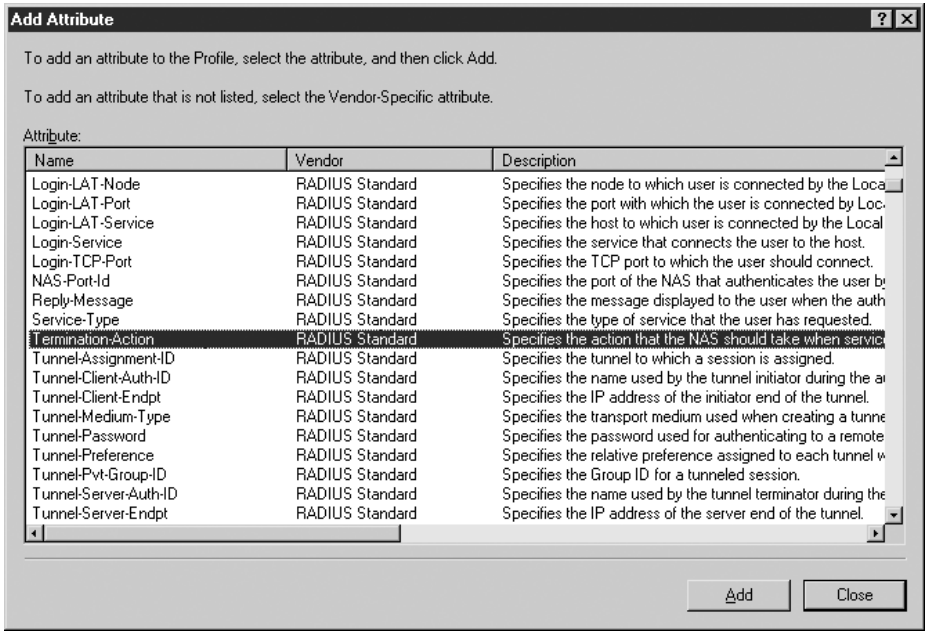
The initial wireless APs did not provide for real authentication. Instead, the network identification of the network is typically all that is required. The identification, or SSID, can easily be discovered and provides no security at all. An alternative to this "open system" authentication mode, a *shared key* can be provided to clients and required for connection. To provide real authentication, and to resolve other security protocol issues, the new Wi-Fi Protected Access (WPA) standard, based on the upcoming 802.11i standard, is available. Unfortunately, device and software modifications are required to use WPA. You can implement 802.1x authentication, Protected EAP (PEAP) authentication, Temporal Key Integrity (TKIP) for key exchange methodologies, and Michael for

integrity, all of which are parts of the standard, using IAS. You must add an upgrade to Windows XP Professional in order to use the new protocols. Windows 2000 IAS will also require an upgrade. You can find 802.1x client software for Windows 2000 and, with a support agreement, for Windows 98, Windows ME, and Windows NT 4.0.

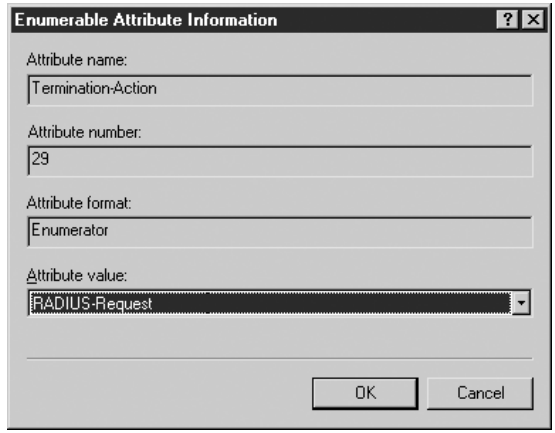
When 802.1x authentication is added, a client requests a connection to the wireless access point, which acts as a RADIUS client. IAS can use Active Directory or its own account database for authentication and remote access policies to allow, deny, and restrict connections. Encryption keys can be automatically issued to authorized clients and changed frequently without client intervention.

To configure 802.1x authentication on IAS:

1. Establish the wireless access point as a RADIUS client in the IAS interface.
2. Configure the wireless AP according to its manufacturer's instructions.
3. Create a Remote Access Policy for wireless clients.
4. Use the Wireless-Other or Wireless 802.11 NAS-Port type Policy condition.
5. Select the Wireless-Other or Wireless 802.11 media in the Allow Access Only Through These Media portion of the Dial-in Constraints.
6. Edit the Remote Access profile, and on the Advanced page click Add, select Termination-Action, as shown here, and then click Add.



7. On the Enumerate Attribute Information dialog, change the Attribute Value to RADIUS-Request as shown in the following illustration. Then click OK. This prevents disconnection when XP clients re-authenticate.

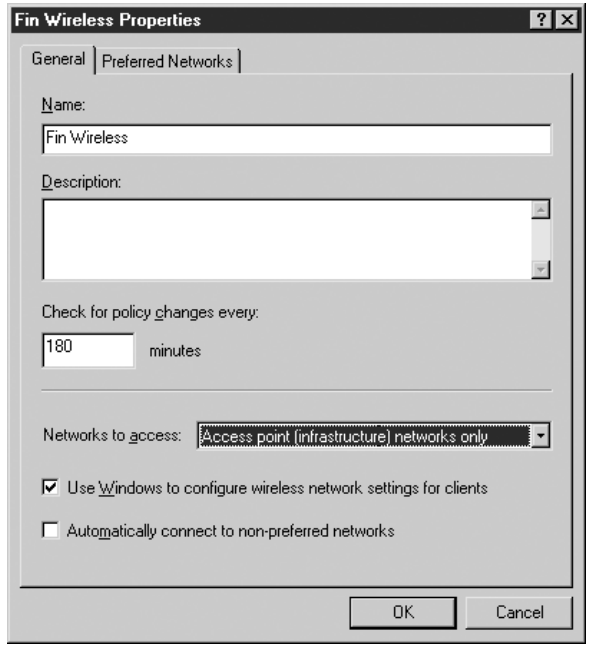


8. Create a Connection Request Policy. Remote Access Policies restrict and manage connections from clients. Connection Request Policies manage RADIUS client. Use the policy to restrict wireless AP to time of day, days of week. Connection Request Policies are created by right-clicking the Connection Request Policies node in IAS. The policy is similar to a Remote Access Policy.

Configure 802.1x client authentication using Group Policy:

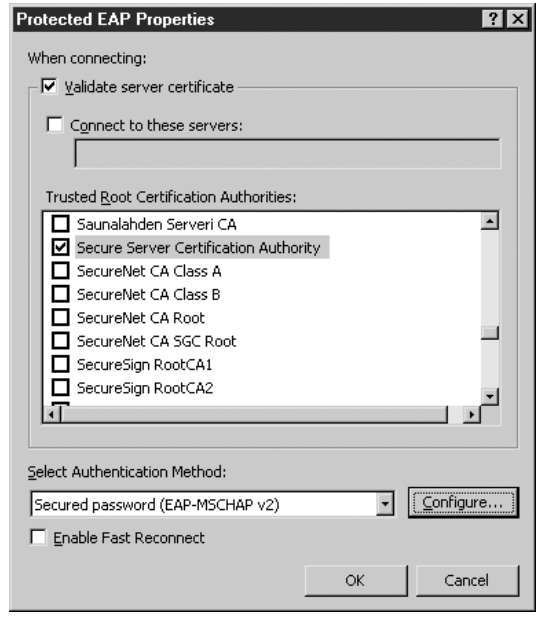
1. Open the GPO for editing and right-click Computer Configuration. Then choose Windows Settings | Security Settings | Wireless Network (IEEE 802.11) Policies.
2. Select Create Wireless Network Policy, and then click Next.
3. On the General tab, in the Networks to Access, select Access Point (Infrastructure) Networks only. This will prevent connections to ad hoc networks, or to client-to-client wireless networks.
4. Select Use Windows to Configure Wireless Networks Settings for Clients. This sets a preference for Windows configuration over a third-party wireless connection that may be installed on the client computer.

5. Leave cleared: Automatically Connect to Non-Preferred Networks, as shown in the following illustration. (You do not want clients to connect to unknown and unapproved networks without user knowledge.)

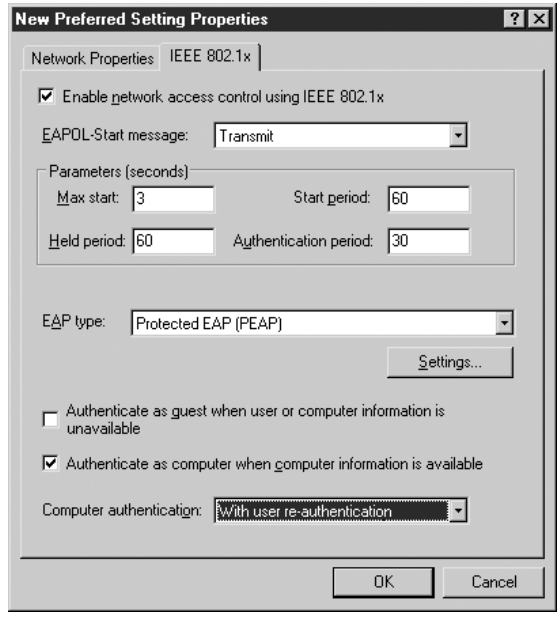


6. Select the Preferred Networks tab and select Add to define and configure 802.1xconfiguration. Restricting accessible networks protects clients from inadvertent connections to rogue networks.
7. Enter the SSID of the network.
8. Select the IEEE 802.1x tab.
9. Select and configure the EAP type. Choices are Smart Card or Other Certificate, or Protected EAP (PEAP).
10. Click the Settings button.
11. Select the trusted root certificate for the server in the Trusted Root Certification Authority box.
12. Select the authentication method in the Select Authentication drop-down box. In this example, as shown in the following illustration, Secured Password (EAP-MSCHAP v2) is selected. This method encrypts the authentication credentials, thus protecting them from a network-based attack. By default, Windows credentials of the logged-on user are used; however, the Configure

button can be used to prevent that, and a dialog for entering a different user ID and password is provided.



13. Click OK to return and review settings as shown here:



Use VPNs

A VPN can be established with the remote access server placed on the network between the AP and the network. Clients connect to the AP in the normal manner, but access to the rest of the network must be established through a VPN connection. This provides authentication, authorization, and confidentiality between the wireless client and the rest of the network.

Protect Web Communications with SSL

Using SSL to protect web-based communications requires the use of certificates. Certificates are used to provide server authentication, proving the web server's identity to the client browser or application. They are also used for secure exchange of secure keys to be used for encrypting communications between client and server. This is the basis for the secure exchange of data for e-commerce and other sensitive web communications.

Client authentication can also be required and is discussed in Chapter 12. Server-side use of SSL is configured in this way:

1. Use the IIS Administration tools to create a certificate request.
2. Forward the request to a public or private certification authority (CA)
3. Install the returned certificate on the web server.
4. Configure site requirements for SSL authentication.