Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

INSTALLING THE WINDOWS 2000 REMOTE ACCESS SERVER BEHIND THE FIREWALL

© SANS Institute 2004, Author retains full rights.

Prepared by: **Sivakumar Ganesan**
Version Number: **GSEC Practical Requirements (v.1.4b)**
Date: **April 7, 2004**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ABSTRACT

Day by day there are new security threats and the vulnerability of corporate information systems is increasing. At the same time, business is expecting high service availability in this competitive world. Information availability is on high priority and business demands that information should be available at any time from anywhere. Mostly the remote offices are connected to central data facility through Internet with Virtual Private Network where the High speed Broad Band Internet network is available. However, there are places where a proper Internet infrastructure is still not available. In such a situation, the users have to rely on the Dial-up (PSTN) network.

Remote users will normally connect to a Remote Access server (RAS server) at the corporate data centre. Remote access facility is used for services like data sharing, email, and web access. This facilitates access to corporate data and helps remote users in taking quick business decisions at the remote locations. While allowing remote access services, it is important to secure the local network from the external vulnerability. Most of the corporate networks are normally protected from external network (Internet) through a firewall. However, the RAS server bypasses the firewall. Even though RAS server has its own security features like User Authentication, Remote Access Policy and Client IP Filtering etc but the server is vulnerable to Denial of Service and Spoofing attacks. To harden the RAS server, we need to provide more protection to the RAS server by putting it behind a Firewall. This paper explains the steps needed for this activity.

Introduction

In this document we will see how to move the windows 2000 remote access server from local network to DMZ (behind the Firewall) with fully secured Remote access. The document has the following sections :

1. ***Terminology used.***
2. ***Situation before placing RAS server behind the firewall and its disadvantages.***
3. ***Steps taken to put the RAS Server behind the firewall and its configuration details.***

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. *Terminology Used*

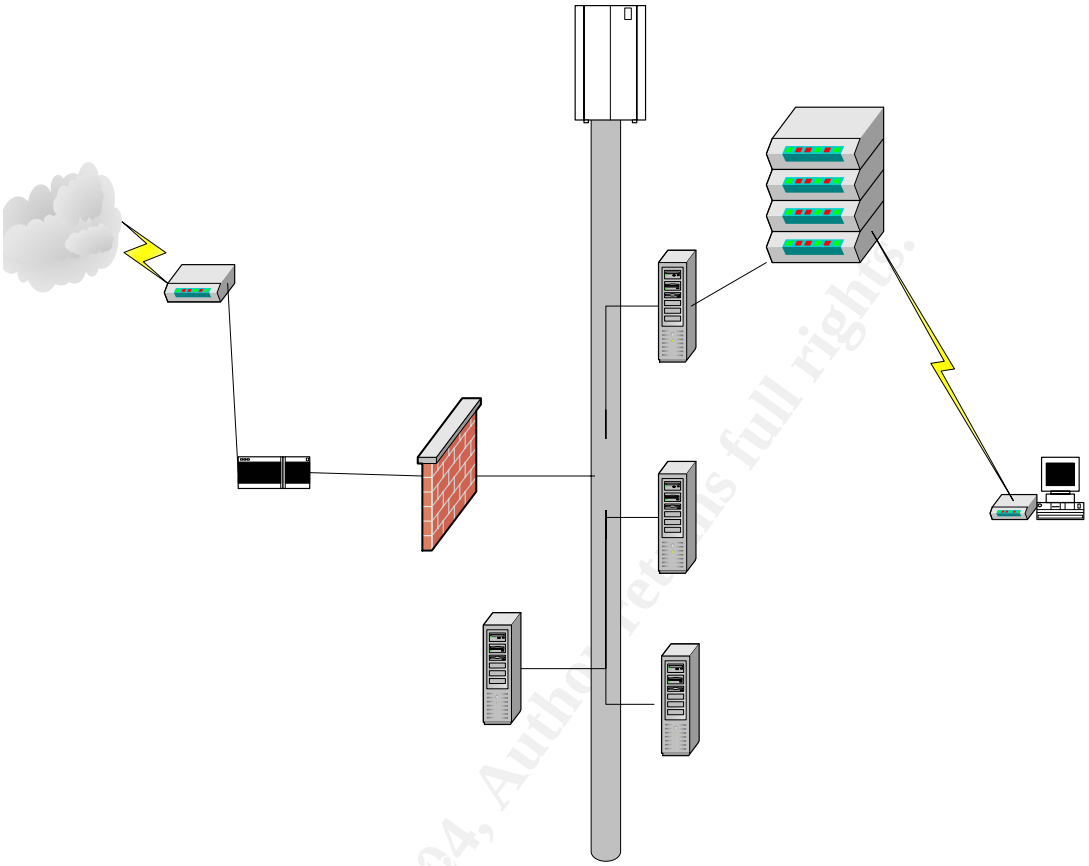
PSTN - The public switched Telephone Network
PPTP – **"***point to point tunneling protocol, which is used to create a tunnel to encapsulate traffic sent over the Public networks. This protocol supports variety of networking protocols including IP an IPX protocols***"***1*
L2TP/IPSEC- **"***A protocol for sending encrypted and digitally signed transmissions Over TCP/IP. Uses both Authentication Header (AH) for digital signing (data Integrity) and Encapsulated Security Payload (ESP) for encrypting data"2 & 11*
DNS - it's a network service, which will convert the IP Address in to host name and vice versa for network client
EAP- **"**Extensible Authentication protocol, it's a protocol which will allow additional protocols like Kerberos, and Hardware Devices like smartcard will be used for authentication**"***3 & 12*
IAS – Microsoft Internet Authentication Server
RADIUS- Remote Authentication Dial-In User Service
MSCHAP- Microsoft Implementation of Challenge Handshake Authentication Protocol
MSCHAP v2 - Microsoft Implementation of Challenge Handshake Authentication Protocol version 2
CHAP- Challenge Handshake Authentication Protocol
DHCP - A network service, which distributes IP address and default gateway to the network hosts.
PAP – Password Authentication Protocol
ISP - Internet Service Provider
DMZ- Demilitarized Zone (a computer or small subnetwork that sits between a Trusted Internal Network (LAN) and an untrusted external network (Internet))

2. Situation before moving the RAS Server behind the Firewall

The Following picture (pic.1) explains how the Remote access server was placed in the local network and configured before moving behind the Firewall. As shown in the picture, the Remote Access server was installed as one of the Member server in the windows 2000 Domain with 16-port AT&T Modem pool. The Modem pool was connected to the PBX Hunting line, so when user dials-in to the RAS server, one of the free modem will answer the call and establish the connection with the client. The Remote Access Server was configured with windows authentication and pool of IP Address to assign to the dial-in Client.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Picture 1



When the user dials to the Remote Access Server it will then authenticate and assign one of the Free IP address available in the static IP pool. The static IP Address Range which was configured in the IP pool of Remote access server was different from the Local network IP Address range of Remote access server (e.g. Like the Remote access server IP pool Range from 10.100.100.11 to 10.100.100.30 and the local network IP address is 192.168.1.0 with subnet mask 255.255.255.0). The Remote access server was doing the routing between Dialup Network and Local Network.

In the above setup the only protection to accessing the Local network through Remote access client is windows authentication. When the user gets authenticated they get all privileges like a local user. They can access any service in the Local network.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In this situation, the Remote access Clients are not in our direct control like local users. This can lead to the following problems:

► the remote computer operating system may not have latest patches. This could lead to propagation of virus resident on the remote computer to other computers on the network.

► Virus Pattern Files may not be up to date like local computers, where the local administrator will be monitoring and updating critical patches immediately but for remote location you will be depending on the users, you have to ask them to download the critical patches and update their system, which may or may not happen on time.

► Enforcing Password Change may not be possible as the remote dial in user do not have the facility to change the password by them. They may have to rely on administrator to reset their password. Also having the same password for a long time leaves the system vulnerable to the hackers who get more time to guess the password and attempt to log into the network.

► Since these users are accessing the corporate network bypassing the Firewall, the services available to the remote users cannot be restricted (any port restrictions applied to the firewall will not be applicable to these users),

To overcome these kinds of risks we decided to move the Remote Access server from the local network and put it behind the firewall (DMZ).

3. *Installing the Remote Access server behind the Firewall*

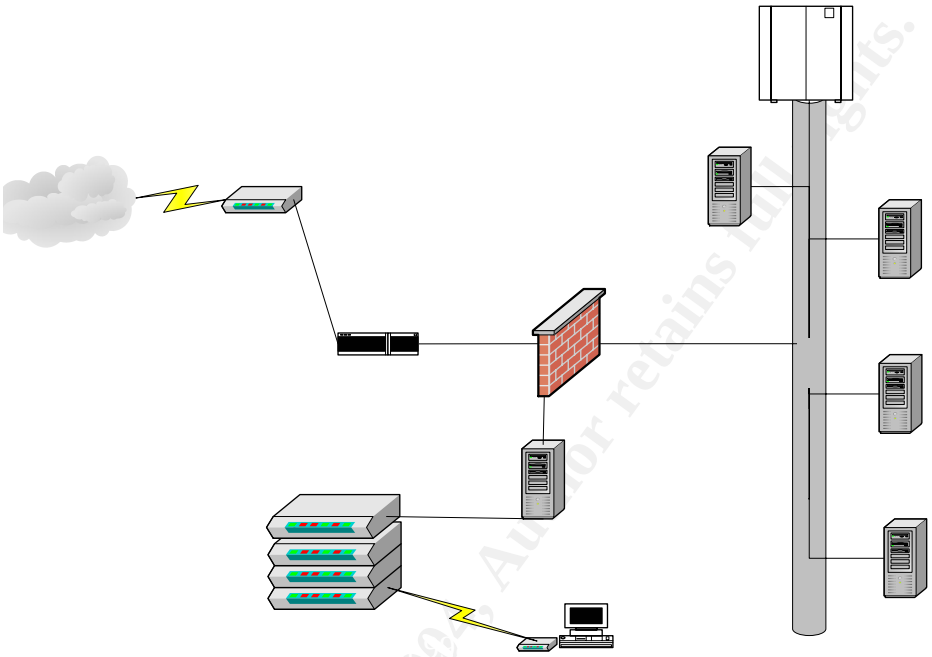
Installing the Routing and Remote Access server behind the Firewall consist of five major steps which are as follows:

1. Installation of the windows 2000 Routing and Remote Access standalone Server
2. Creating the Dial-In users and Group in Active Directory and apply the remote access policy for the Groups
3. Configuring the Firewall for access control on the Dial-In users
4. Installing the IAS Server to enable the RADIUS Authentication
5. Configuring the Remote access Client

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The following picture will show how the Routing and Remote Access Server is physically placed in the network behind the firewall (in the DMZ):

Picture 2



In the above picture, the RAS server is installed in the DMZ as a standalone server and connected to the Modem pool with PBX line. RAS server was configured as RADIUS Client so Whenever the Remote access Client dials in to modem pool, the Remote Access server sends the user credential and connection parameter information in the form of a RADIUS Message to the RADIUS Server (IAS Server). The RADIUS Server authenticates and authorizes the RADIUS Client request and sends back the RADIUS message response. If the remote access Client is a valid user then RADIUS server will send in the response message saying connection attempt is authenticated and authorized otherwise the RADIUS server will send a message saying not authorized either if the login information is not authentic or connection information is not authorized. The RAS server was configured with Static IP pool (Range 10.100.100.11 to 10.100.100.90) to provide IP address to the Remote Access Clients, and the IP pool was divided into three different ranges as follows: **Range**1 is from 10.100.100.11 to 10.100.100.40, **Range2** is from 10.100.100.31 to 10.100.100.60 and **Range3** is from 10.100.100.61 to 10.100.100.90. Each range was assigned to one of the user Group in the Active directory.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ISP

Internet

Three User group were created in the Active directory according to the users service need like the Users in the **Group1** will be allowed to access only the FTP Server, Users in the **Group2** will be allowed access the Mail server only and users in the **Group3** will be allowed access the FTP & Mail Server.

While creating the remote access users in the active directory go to the **Dial-in** Tab and select option called **Assign Static IP address** and enter the IP address for that user depending on the group he belongs to like if he is a FTP user then he will belong to **group1** and the **IP range** for the **group1** is **range1** then enter one of the IP address from that Range1 manually to that users and so on. It's easy to apply polices for a group rather then the users level. When you assign an IP address to the users through user account then users will not be allowed to change by themselves which will thereby avoid the users playing with RAS Client. I will be explaining the detailed security feature about this in creating the Active Directory Users and Groups in later part of this document.

In the above picture (Pic.2) you can see the Firewall which is placed in between the Local Network (Trusted network) and External Network (untrusted Network (Internet)). Normally, the firewall will have three ports viz., Trusted (LAN), External (Internet) and optional (DMZ). In the DMZ normally internet bound traffic servers like FTP, HTTP, DNS and web servers will be installed to avoid the external users coming into the internal network. So when you place the RAS server in this subnet you can limit the user accessing the Local network. We will see in more details about firewall configuration in the later explanations to follow.

In the above picture (pic.2), the IAS server is acting as a RADIUS server which does the AAA authentication to the user login. It is configured to do the RADIUS Authentication and accounting of the user login. It has lot of security features which we will be made clear in the later part of this document.

In the above picture (pic.2), you can see the Windows 2000 DC (DC= Domain Controller) which is Active Directory Domain Controller which is configured with **Native mode**. Windows 2000 domain controller operates in two different modes one is **Mixed Mode** and other one is **Native Mode**. In the security point of view the **Native Mode** has more features than the **mixed mode**.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In the Mixed mode when you create Remote access user in the **Dial-in** tab you can see the **Remote access Permission** (Dial-In or VPN) has only two options either **access** or **deny** and **call back** option but in the **Native mode** other than the **Access** or **Deny** you will have one more option called **Control through Remote access policy. O**ther than this you have following options like **Verify the Caller ID**, **Assign a Static IP Address** and **apply Static Route** and so on I will be explaining these security features in detail in **Dial-up users and Group creation.** If you are running the windows 2000 domain still in Mixed Mode then its better to move into the Native Mode. Before moving into Native Mode make sure that there is no windows NT4.0 Domain controller present in the same Domain.

The Core switch which is present in the above picture is the Main network switch, where all the server in the data center and Local Network Edge switches were connected, the mail server and FTP servers were configured to serve a mail & FTP service to the internal (Local) and remote users, the router which is connected in the external port of the Firewall is configured with the Internet IP: address and connected to the **ISP** (Internet service Provider) through Digital Leased Line modem.

The following section will explain the installation and configuration of the RAS server, IAS server as a RADIUS Server, Firewall configuration, creation of a user group and applying the Remote access policy for the Group, selecting the authentication methods and protocols and so on.

3.1 *Step-by-Step configuration of Routing and Remote Access Server*

"On the **Start** menu of Windows 2000 server, click **Programs**, **Administrative Tools**, and **Routing and Remote Access**.

The Configure Routing and Remote Access (RRAS) wizard starts. Click on **Next,** now the Common Configurations dialog box appears. Select **Remote access server** and Click **Next**

The Dialog box will appear and ask you to select a configuration type based on the complexity of your network (this dialog box will appear only if you're installing the Remote access server in the windows 2000 standalone server, if you are installing the remote access server on the windows 2000 active Directory member server or Domain controller it will not show this dialog box) in that select the **Set up an advanced remote access server** and Click on **Next**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Now the dialog box will ask you to **configure the Supported Remote access Client Protocol**; by default the TCP/IP will be selected, click **next**

The next dialog box gives the option of allowing the RAS server to assign IP addresses, either by acting as a DHCP server itself or by using an existing DHCP server on the network. Your choice depends on how your network is configured and whether a combined RAS/DHCP server can handle the peak load you anticipate placing on the server. In this we select from a specified range of address and Click next

The next dialog box will ask you to enter the Address assignment, click on **New**, now you will get a dialog box saying new Address Range. In that enter the start IP address: (e.g. 10.100.100.11) and end IP address (e.g. 10.100.100.90) now you will get the Number of address (e.g.80) calculated by the system click **OK** to close the dialog box now you will be back to Address Range Assignment dialog box in the address range you can see for an e.g. From 10.100.100.11, To 10.100.100.90 and Number 90 is available IP address in that range. This you can change according to your need. Now click on **Next**

The next dialog box will ask you to configure RAS to use either a RADIUS server for central authentication or a Windows IAS server. The Windows IAS server can be installed on the RAS server or run on a separate server. Select **No**, I don't want to set up this server to use RADIUS now. (As of now we install the Remote Access server with Windows Authentication after installing the Internet Authentication server we will configure the Remote Access server as RADIUS Client) click **Next**

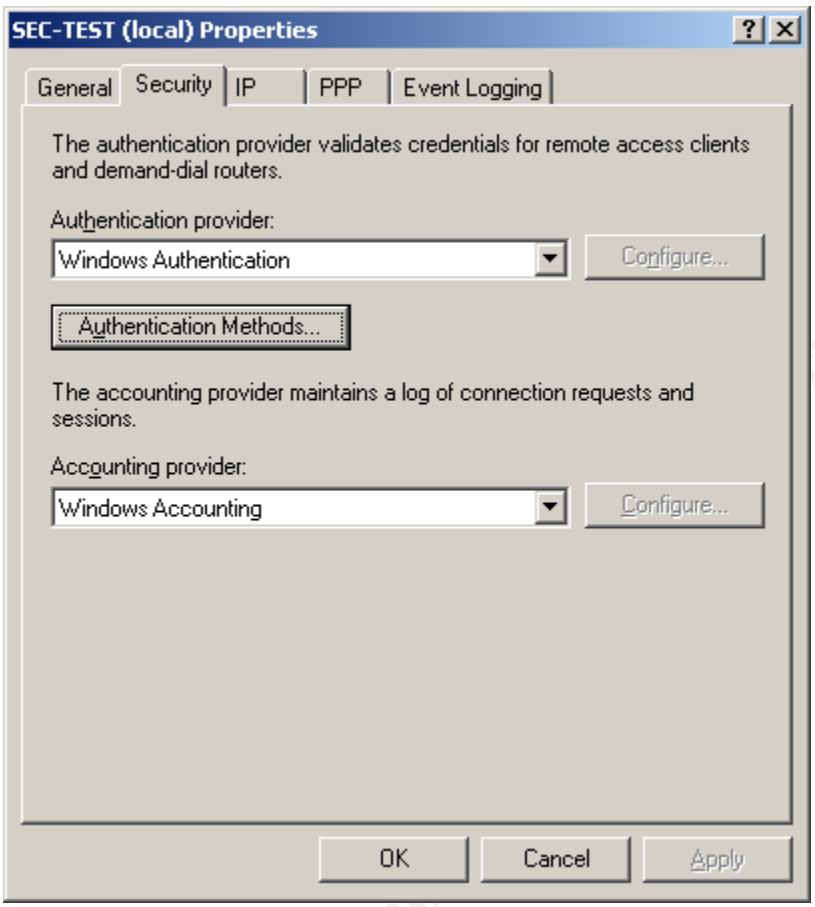
The Dialog box will say completing the Routing and Remote Access Server Setup Wizard. Click on **Finish**

The dialog box will appear saying to support the relaying DHCP message from remote access Client; you must configure the properties of DHCP Relay Agent with the IP address of your DHCP Server Click on OK

Now you will be back to Routing and remote access console now Right click the RAS server in the **Routing and Remote Access snap-in**, which should be visible after the RRAS wizard has completed. Click **Properties** and choose the **Security** tab.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Picture 3

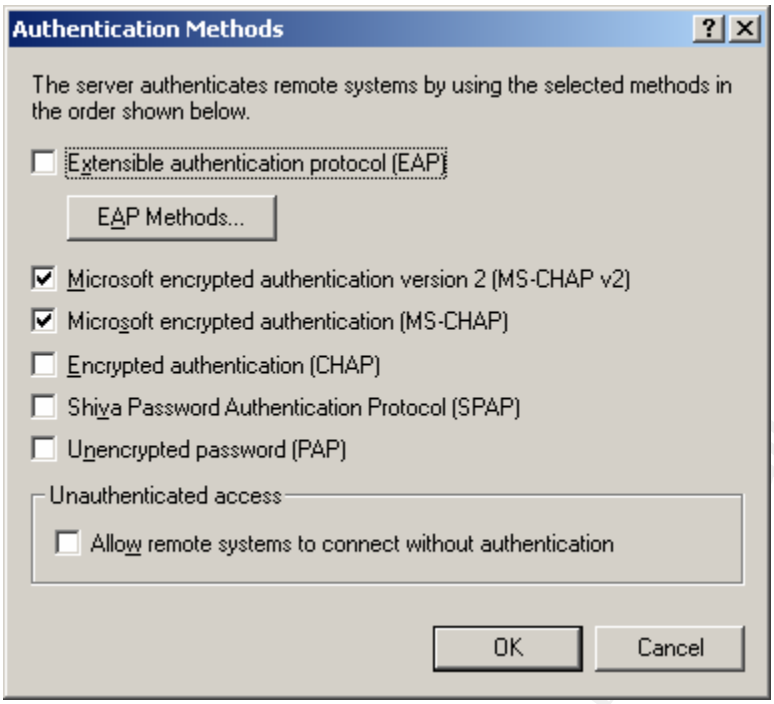


In the **Authentication Provider** window choose **Windows Authentication**. Now click on **Authentication Methods**

You will get following screen:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Picture 4



In Authentication Methods disable:

EAP

Unauthenticated access

Then enable these items, as shown in the above screenshot:

MS-CHAP v2

Microsoft Challenge Handshake Authentication Protocol Version 2

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol

Disable the **CHAP** and **PAP** (these are low security protocols)

Click **OK** to return to the **Security** tab. In **Accounting Provider,** choose Windows **Accounting** (as of now we will select the Windows accounting and we will change this setting in to RADIUS accounting after Configuring the IAS server),

On the **IP** tab,

Enable **IP routing**.

Allow IP-based remote access and demand-dial connections.

Use DHCP for addresses or static pool.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

On the **PPP** tab, select:

Enable Multilink

BAP or BACP

LCP

Software compression

On the **Event Logging** tab,

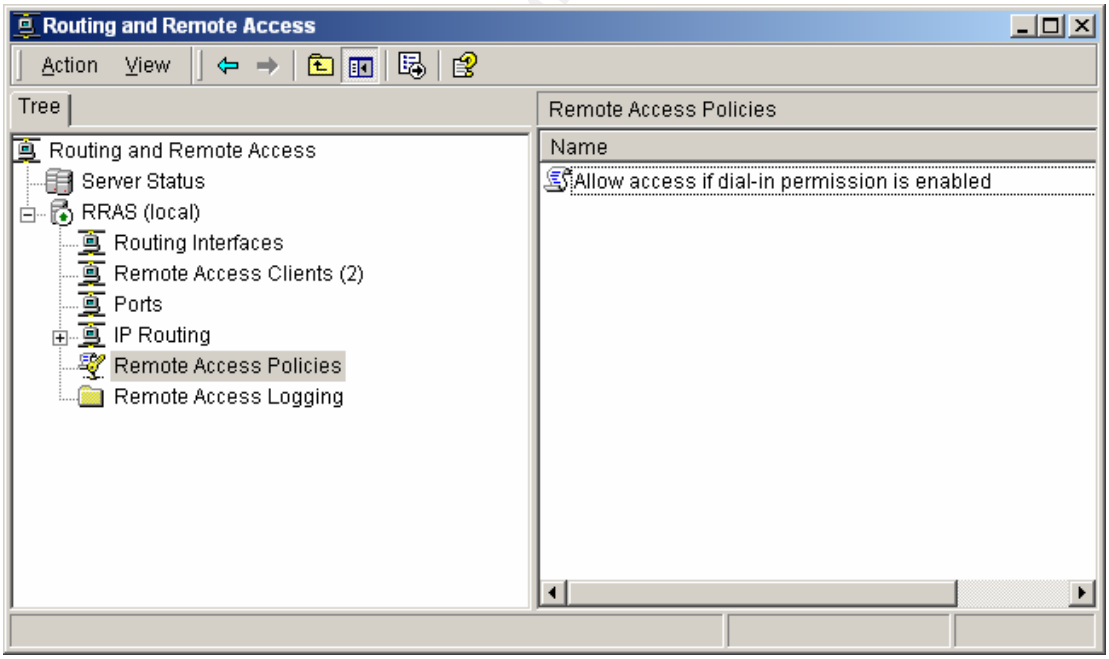
Select **Log the maximum amount of information**.

At the end of this process you are warned that you have to select more than one authentication method. You are asked if you want to read the RAS help files in order to properly configure authentication. The primary issue is that you need to set Remote Access Policies to allow, for example, MS_CHAP v2.

Configuring the Remote Access Policies

The default remote access policy **Allow access if dial-in permission is enabled**, as shown in the following screenshot, select the default policy and go to the **Properties**

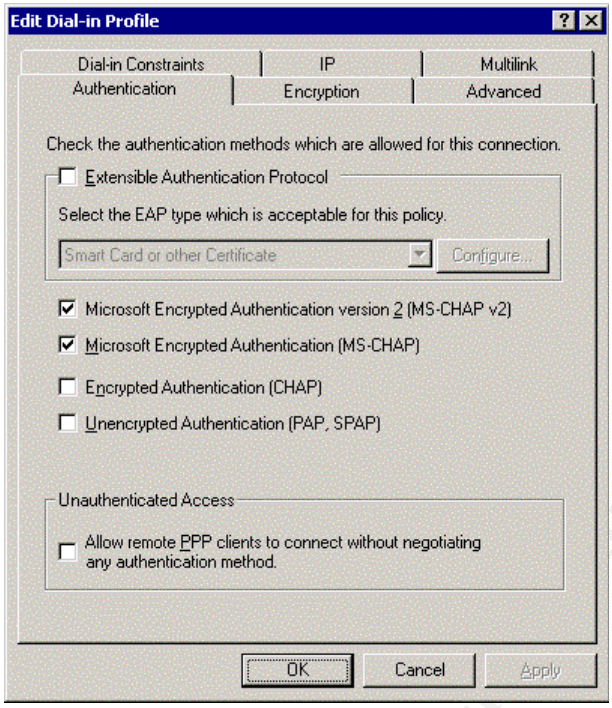
Picture 5



Click **Edit** the profile. You will get the following screen:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Picture 6



On the **Authentication** Tab

Set the policy to allow these items, as shown in the above screenshot:

Which are more secure then other two

MS-CHAP v2

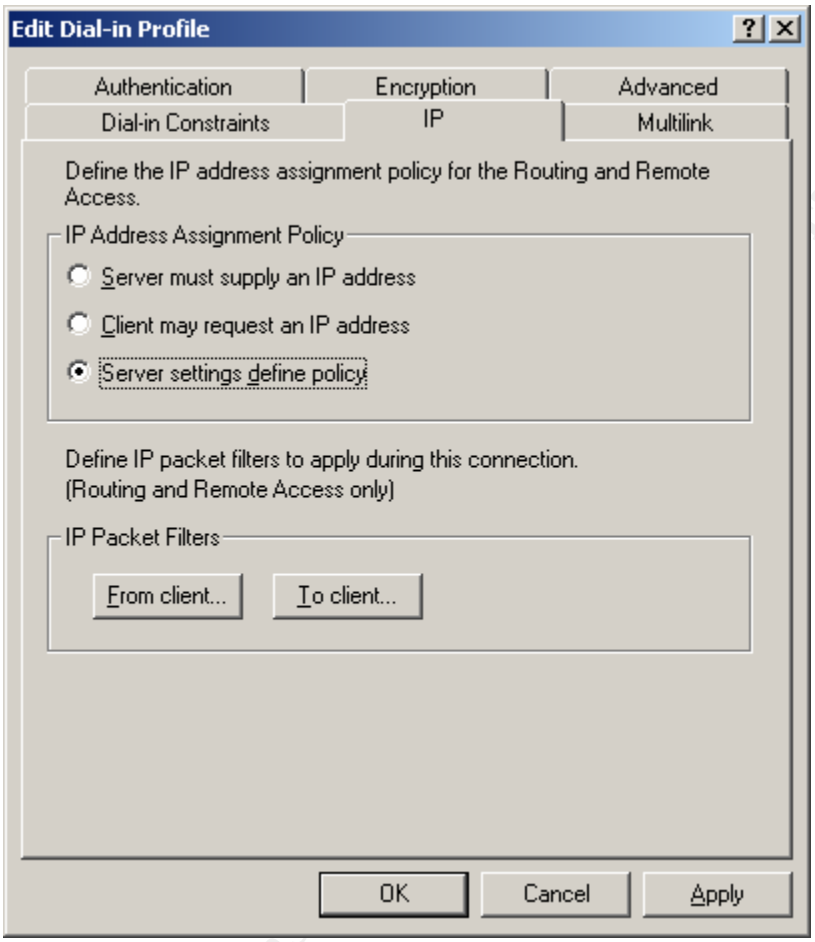
MS-CHAP

And deselect the CHAP, PAP (when all the remote access clients are running with windows 2000 then no need for these protocols. Plus its low security protocols)"*4*

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

On the **IP** Tab:

Picture 7



In the IP address Assignment Policy select the policy which one will be applicable for you:

*** Sever must supply an IP address** – Server will assign the IP address to Dial –in host form DHCP or IP Address poll depending on your configuration

*** Client May request an IP Address** – In this the sever will supply a IP address to the Dial-in host if the Dial-in was already configured with IP address then it will accept that.

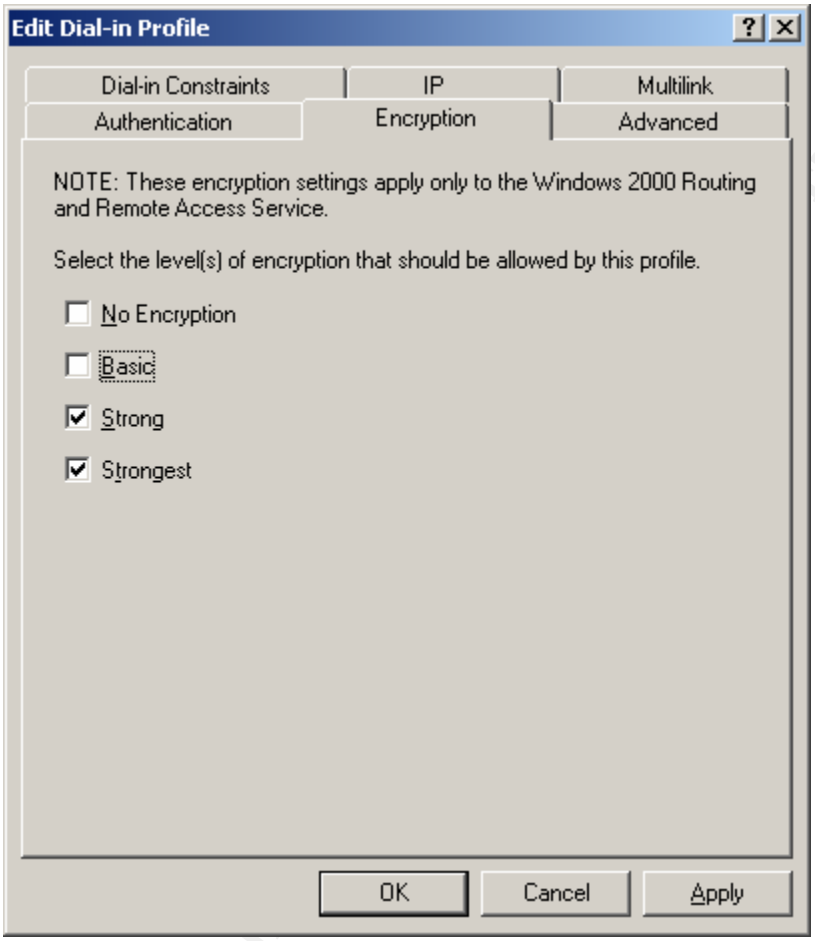
*** Server setting defines policy** – This specifies that the TCP/IP address assignment setting of the server is used. For e.g. The server may be configured to dynamically assign IP address as users connect.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In the above options select the third one where the **Server Setting Defines Policy.**

On the **Encryptions** Tab:

Picture: 8



You can set encryption properties. For these encryption strengths:
Select the **Strongest** and uncheck all others for better security.

Strongest

For dial-up and PPTP-based VPN connections, MPPE with a 128-bit key is used. For L2TP over IPSec-based VPN connections, triple DES (3DES) encryption is used. This option is available only after the Windows 2000 High Encryption Pack is installed.

By default when you install the RAS server there were 10 VPN port created in that five are PPTP port and other five are L2TP port.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

When comparing with PPTP to L2TP both of them have some advantage and disadvantage. Both PPTP and L2TP/IPsec use PPP to provide an initial envelope for data and then append additional headers for transport through the inter-network however there are some differences which is as follows:

"1. PPTP, data encryption begins after the PPP connection is completed with L2TP/IPsec data encryption begins before the PPP connection process by negotiating an IPSec Security association

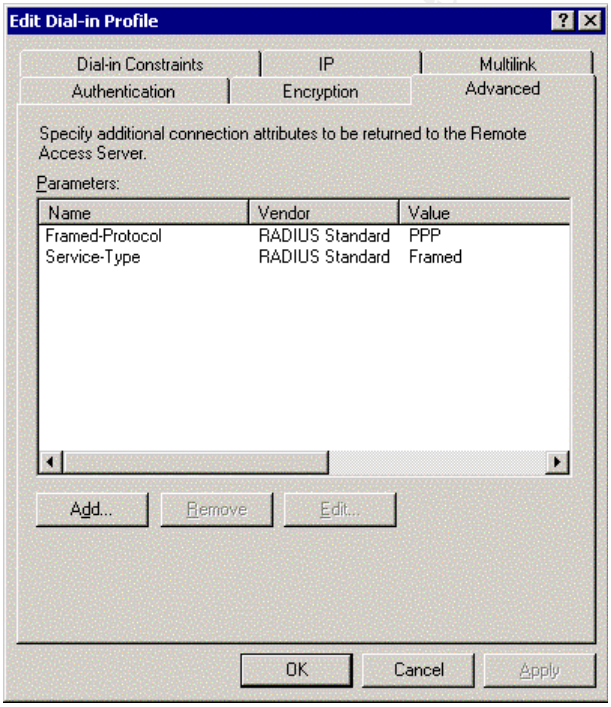
2. PPTP connection require only user level authentication through PPP based authentication protocol. L2TP/IPsec require the same level authentication and in addition, computer-level authentication using computer Certificates." [5]

*"Advantage **over L2TP/IPsec to PPTP** is: IPSec ESP provides per-packet data origin authentication, data integrity, and confidentiality .by contrast; PPTP provides only per-packet data Confidentiality*

*Advantage **over PPTP to L2TP is PPTP** does not require Certificate Infrastructure.L2TP require a Certificate infrastructure for issuing Computer Certificates to the VPN server Computer and all VPN Client Computers."* [6]

On the **Advanced** Tab

Picture: 9



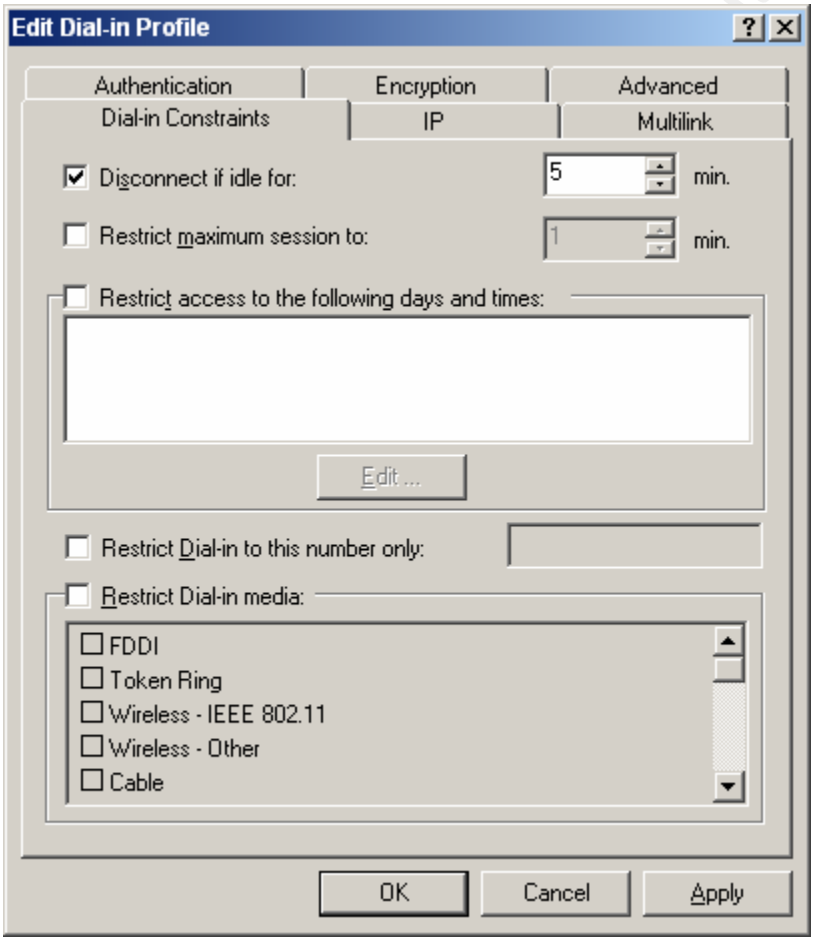
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

"*You can set advanced properties to specify the series of RADIUS attributes that are sent back to the RADIUS client by the IAS server. RADIUS attributes are specific to performing RADIUS authentication and are not used by the remote access server. By default,* ***Framed-Protocol*** *is set to* ***PPP*** *and* ***Service-Type*** *is set to* ***Framed****.*

The only attributes that are used by the Routing and Remote Access service are ***Account-Interim-Interval****,* ***Framed-Protocol****,* ***Framed-MTU****,* ***Reply-Message****, and* ***Service-Type****."7(page -33)*

On the **Dial in constraints** tab

Picture 10



Disconnect if idle for: Specifies whether to disconnect a dial-up connection after no activity occurs for a specific period of time.

Restrict maximum session to: Specifies whether to limit the length of a dial-in session.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Restrict access to the following days and times: Specifies whether dial-up connections for the members of a group dial-in profile are restricted to certain days and times.

Restrict Dial-in to this number only: Specifies whether to restrict dial-in access to a single number.

Restrict Dial-in media: Specifies whether to restrict Dial-in access based on the type of media used. For eg. If you only want to allow Dial-in connections that use modems, select this check box, and then select the Async check box.

In this configuration we will configure only the **Disconnect if idle for 5 Mints** all others you can configure according to your need. Now we have completed the Remote server installation

3.2 *Dialup user and Group Creation*

"To create Dial-in Users Group click on **start**, select **programs** and **Active Directory users and computer** in the windows 2000 Domain controller now you will get a dialog box in that right click on the users and go to **new** in that select the Group, now you will have a screen where you have to enter the Group name." (Create Group name as you wish) for the test we will create three groups namely Group1, Group2 and Group3 and we will add the members only the FTP user put in the Group1, all the mail users will be there in the Group2 and in the Group3 the users who has the permission to access both FTP and Mail be added as we said before the IP address for the Group1 will be allotted from range1 (IP range: from 10.100.100.11 to 10.100.100.30) and group2 will be allotted from Range2 (IP address from 10.100.100.31 to 10.100.100.60) and Group3 three will be allotted from range3 (IP : address fro 10.100.100.61 to 10.100.100.90).

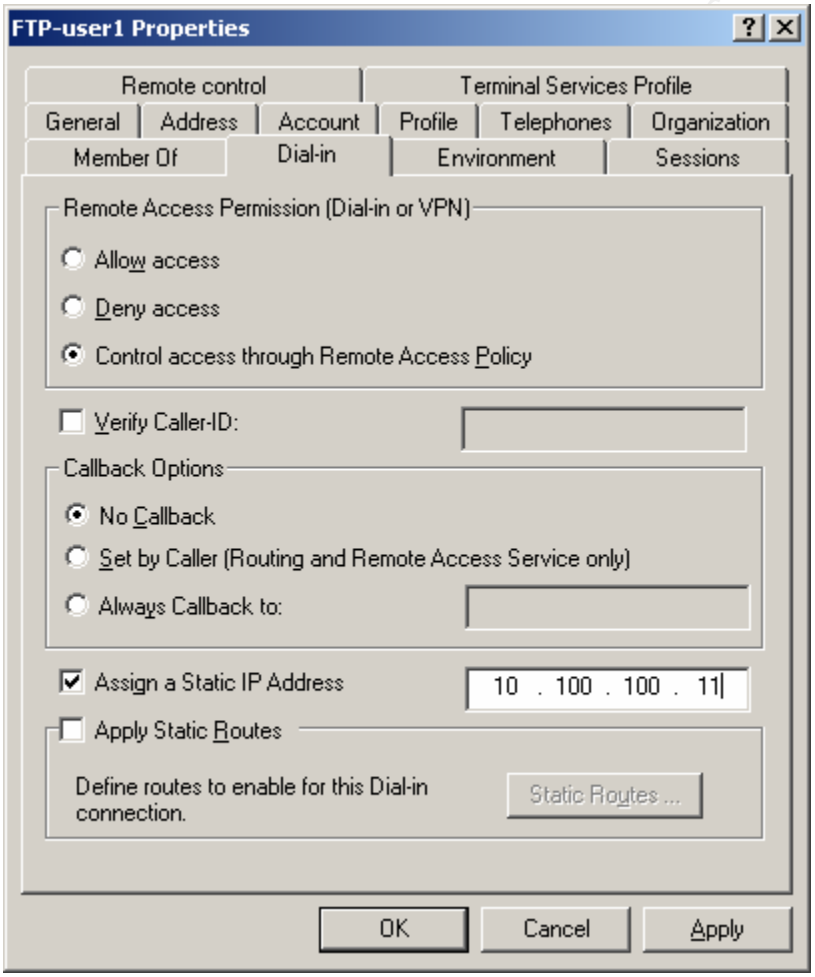
After creating the groups right **"**Click on the **Users** in the Active Directory and users snap-in and select new and click on users, now you will get new object dialog box in that enter users first name, last name and login ID (for e.g. ftp-user1) then click on **next**, now the new dialog box will appear to where you have to enter the password and click on **next** and in the next screen click on **finish** now you will be back to the main screen. Double click on the **Users** and select the newly created user and go to the property of the user and select the **Member of** Tab. Being a FTP user add this user into the Group1, then go to the **Dial-In** tab and select the following Remote Access permission as shown in the Screenshot (Pic. 8), then create one more user called Mail-user1 and go to the **Member of** Tab and add in the Group2 .**"***8*

The group2 is meant for the mail users and this group is mapped with IP address range of Range2 then goes to the **Dial–In** tab and configure as

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

shown in the snapshot below. After finishing that it comes to the users again and right clicks on the users and select **New**, in that select users and create user called **Mail & FTP User.** Then go to the property of users and go to the Member of tab, add this user in to the Group3 which is configured with permission to access both FTP and Mail server. Also the group3 is mapped with IP range of Range3 then go to the **Dial-In** tab go to the Remote access permission and select the options as shown in the snapshot below. The picture below shows the windows 2000 native mode users dial-In property. In the Mixed Mode you will have only three options like **Allow Access, Deny Access and Callback options**. Whereas, in the Native mode you will have more future like **Control Access through remote access policy, Verify Caller ID, assign static IP Address and Apply the Static routes** and so on

Picture 11



The dial-in properties of a Windows 2000 user account are:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Remote Access Permission (Dial-in or VPN)

Select the **Control access through Remote access policy** for better security

Verify Caller ID

When you enable this option the RAS server verifies the Caller's phone number. If the caller phone number matches with the configured phone number, then the connection attempt is accepted otherwise denied. For enabling this option the Caller ID must be supported by caller's phone system and remote access server call answering equipment that supports passing the caller ID information. Otherwise you can not use this option.

Callback Options

Select the third Option **Always call back to this number** this will give you more control than other options. But if the users are road warrior then you cannot go for these options.

Assign a Static IP Address

With this option you can assign a specific IP address to the user when a connection is made. It needs some Manual process where you have to assign the IP address to each dial-in user according to the Group they belong to and IP address Range (we need this setting for firewall control).

Apply Static Routes

"When this property is enabled, you can define a series of static IP routes that are added to the routing table of the Remote Access server when a connection is made. This setting is designed for user accounts that Windows 2000 routers use for demand-dial routing." 7(page-22)

3.3 *Firewall Configuration*

In the Firewall policy, incoming from the external port to the internal port is by default always denied. If you want to open a one particular service then you have to enable that service only. Mostly the Firewall is working on the basis of Source, Destination, Protocol and Service Type.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Current Configuration

The firewall is connected with the different network as: Trusted Network (local network Address is: 192.168.1.0), external network (e.g. internet subnet address is: 192.x.x.x) and optional network (DMZ is 10.100.100.0). The RAS server is installed in the DMZ. Also, in the configured Dialup user group each user group was already configured with different IP range (for e.g. Group1 as IP Address Range: 10.100.100.11 to 10.100.100.30). As the firewall provides services based on the source address, the Dial-up users will be authorized to use permitted services only.

Example of Firewall Policy

Source	Destination	Service	Port	Interface	Direction	Permission
From 10.100.100.11 to 10.100.100.30	192.168.1.5	**FTP**	20	DMZ	IN	Permit
			21	DMZ	IN	Permit
From 10.100.100.31 to 10.100.100.60	192.168.1.6	**SMTP**	25	DMZ	IN	Permit
		POP3	110	DMZ	IN	Permit
From 10.100.100.61 to 10.100.100.90	192.168.1.5	**FTP**	21	DMZ	IN	Permit
	192.168.1.6	**FTPdata**	20	DMZ	IN	Permit
		SMTP	25	DMZ	IN	Permit
		POP3	110	DMZ	IN	Permit
Any	any			DMZ	IN	Deny

3.4 *Internet Authentication server Configuration (RADIUS Server)*

This service is not installed by default. Go to the Windows 2000 Server Control Panel, click the **Add/Remove Program,** then click **the Add/Remove windows components** and then select **Details** in the Networking **services.** Here you got to select the Subcomponents of Networking services and select the **Internet Authentication service** and click on **OK** now you will be back to windows Components dialog box in that click **Next** after completion of installation you will get a dialog box saying you have successfully completed the windows Components Wizard. To close this wizard click on **finish** now you will be back to Add/Remove Program screen and now you click on **Close.**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

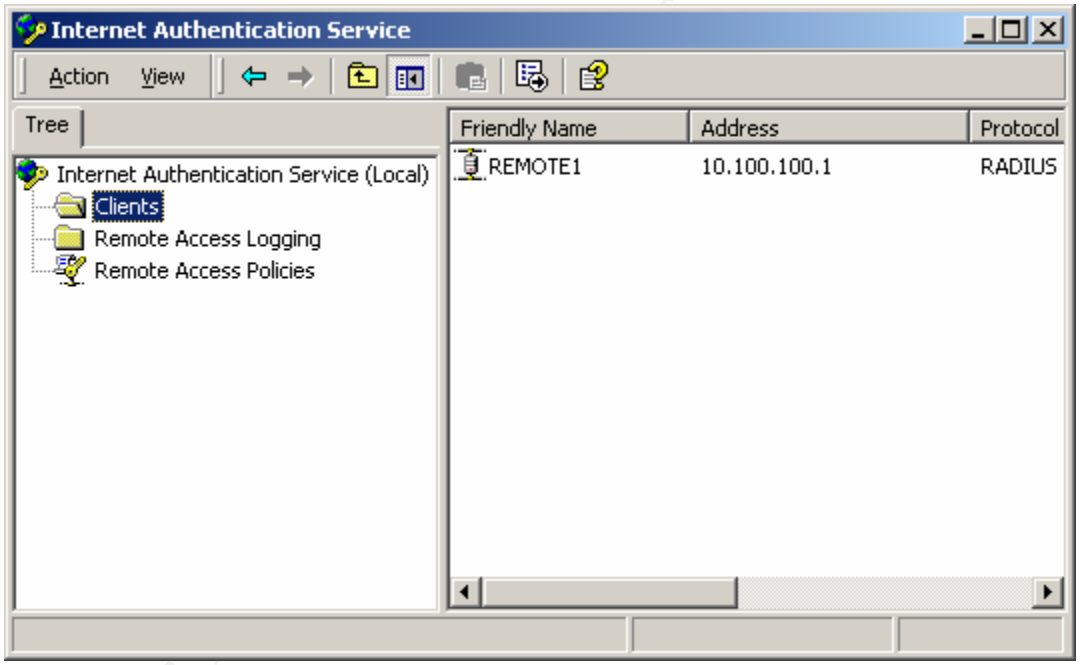
The Internet Authentication Service configuration has the following four main components:-

1 **Internet Authentication Service**
2 **Clients**
3 **Remote Access Logging**
4 **Remote Access Policy**

3.4.1 Internet Authentication Service

Go to the **Administrative tools** and Open the **Internet Authentication Service** as shown in the snapshot

Picture12



To configure the properties of an IAS server, right-click on the **Internet Authentication Service**, and then select **properties** and here you get the Property dialogue box where you select the **Service Tab.**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

► **SERVICE Tab**

"*The Service Tab is used to do the following:*

- *Type a name of the server to distinguish it from other IAS servers. The default name is IAS.*
- *Enable or disable the logging of rejected or discarded authentication requests in the Windows 2000 system event log. This option is enabled by default.*
- *Enable or disable the logging of successful authentication requests in the Windows 2000 system event log. This option is enabled by default.*

► ***RADIUS Tab***

*The **RADIUS** tab is used to do the following:*

- *Enumerate the list of UDP ports over which RADIUS authentication messages are sent and received. By default, IAS uses UDP ports 1812 and 1645. UDP port 1812 is the reserved RADIUS-authentication port described in RFC 2138. UDP port 1645 is used by earlier RADIUS clients.*
- *Enumerate the list of UDP ports over which RADIUS accounting messages are sent and received. By default, IAS uses UDP ports 1813 and 1646. UDP port 1813 is the reserved RADIUS accounting port described in RFC 2139. UDP port 1646 is used by earlier RADIUS clients.*

► ***Realms Tab***

*The **Realms** tab is used to configure a prioritized list of find-and-replace rules to manipulate realm names before name-cracking and authentication. Pattern-matching syntax is used to specify the strings to find and replace Find-and-replace rules can be added, edited, and removed. The rules are applied to the incoming user name in the order in which they are listed. Use the **Move Up** and **Move Down** buttons to specify the order.*

3.4.2 *Clients*

To add a new RADIUS client for the IAS server do the following steps :

- Right-click on the **Clients**
- And click on the New **Client**. (The IAS New Client wizard will guide you through the procedure)
- To modify an existing client's properties, right-click the client name and then click **Properties**.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In the **Properties** of a RADIUS client select **Settings** which is used to:

Specify a friendly name for the RADIUS client. This name does not have to correspond to the DNS, NetBIOS, or computer name of the RADIUS client.

Specify either the IP address or the DNS name of the RADIUS client. If you specify the DNS name, you can verify that the name is being resolved to the correct address. If the DNS name is associated with multiple IP addresses, you can choose the address to use.

Specify the vendor of the RADIUS client. Select **RADIUS standard** for a vendor-independent client. For a Windows 2000 Routing and Remote Access server, select **Microsoft**.

Specify whether the client must always include the RADIUS signature attribute (also known as a digital signature) in Access-Request messages for connection requests using the MS-CHAP v1, and MS-CHAP v2 authentication protocols. With EAP, the signature attribute is always required. If you enable this, you must ensure that the RADIUS client is configured to always send the signature attribute. Otherwise, IAS will discard the Access-Request upon receipt.

Specify and verify the shared secret. The shared secret is a password used between IAS and this specific RADIUS client to mutually verify identity. Both IAS and the RADIUS client must be configured with the same shared secret for successful communication to occur. The shared secret can be up to 128 bytes long, and it is case-sensitive, and can contain alphanumeric and special characters. To protect your IAS server and your RADIUS clients from dictionary and denial-of-service attacks, make the shared secret a long (more than 16 characters) sequence of random letters, numbers, and punctuation.

3.4.3 *Remote Access Logging*

Remote access logging in the Internet Authentication Service administrative tool is used to configure log file settings. To access the properties for local logging, click **Remote Access Logging**, right-click **Local File**, and then click **Properties**.

Settings Tab

The **Settings** tab in **Local File Properties**:

The **Settings** tab is used to:

- Enable or disable the logging of accounting requests in the IAS log file. Accounting requests include Accounting-On, Accounting-Off, Accounting-Start, and Accounting-Stop messages. IAS logs only accounting requests sent by the RADIUS client. If the RADIUS client is not configured for RADIUS accounting, then accounting requests for that client are not logged. This setting is not enabled by default.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Enable or disable the logging of authentication requests in the IAS log file. This setting is not enabled by default.
- Enable or disable the logging of interim accounting requests in the IAS log file. This setting is not enabled by default.

Local File Tab

The **Local File** tab in **Local File Properties**:
The **Local File** tab is used to:

- Enter the log file format. The database-compatible format is an ODBC-compatible format that is typically selected when you want to move the log file information to a database program. The IAS format is an ID-value paired format that provides information on all RADIUS attributes in the RADIUS message. By default, IAS format is selected.
- Enter the duration of the log file or its maximum size. By default, **unlimited file size** is selected.
- Enter the location of the IAS log file.**"***6(page 60 – 65)*

3.4.4 Remote Access Policy

A remote access policy is a named rule that consists of the following elements

- Conditions
- Remote Access Permissions
- Profile

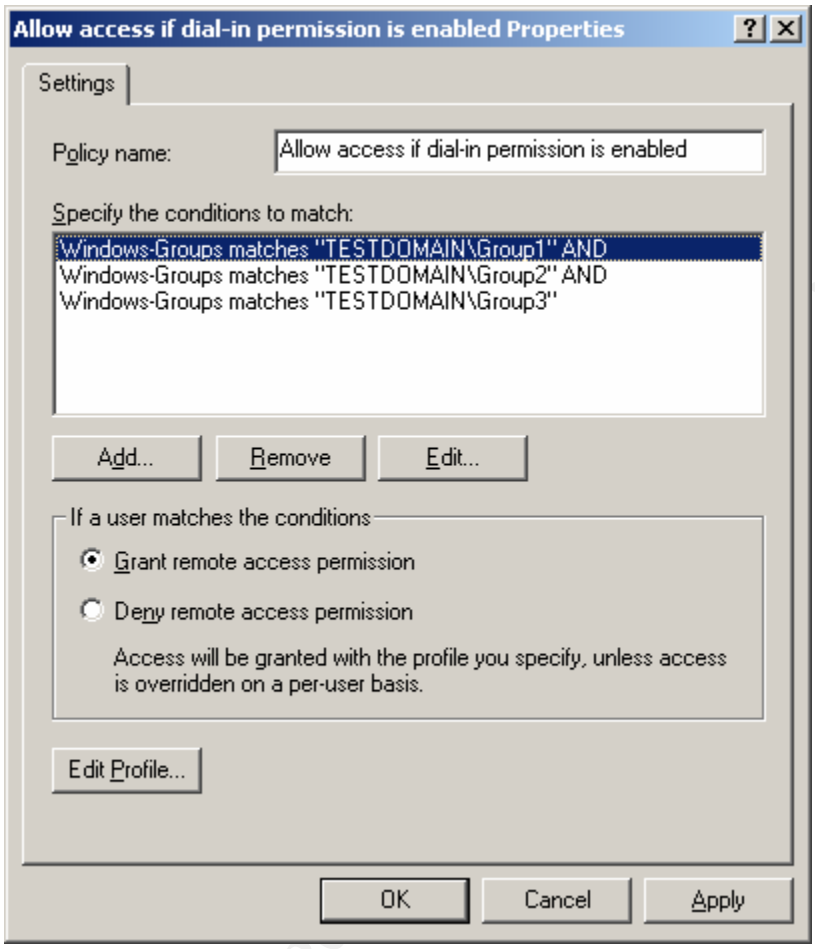
➢ Open the remote access policy and remove the default one
➢ Click on Add and select the Windows Group
➢ Select Grant access permission

The following screen shot shows how the group policy was created and added in the policy list:

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Picture 13



Click **Edit** the Profile.

You will get the new screen in that select the **Authentication** Tab

In that select the MS-CHAP V2 and MSCHAP which are Secured protocol, disable the other two (CHAP and PAP)

On the **IP** tab

In the IP Address Assignment Policy

Select the **Server settings define policy -** This specifies that the TCP/IP address assignment setting of the server is used. For e.g. The server may be configured to dynamically assign IP address as users connect.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

On the **Encryption** tab

Select **Strongest**

Strongest

For dial-up and PPTP-based VPN connections, MPPE with a 128-bit key is used. For L2TP over IPSec-based VPN connections, triple DES (3DES) encryption is used. This option is available only after the Windows 2000 High Encryption Pack is installed.

Then leave all other tabs as default

Now you have completed the RADIUS server Configuration

"Note: By default, MS-CHAP v1 for Windows 2000 supports LAN Manager Authentication used by older Microsoft operating systems such as Windows NT 3.5 and Windows 95. You can prohibit the use of LAN Manager Authentication with MS-CHAP v1 by setting Allow LM Authentication ***(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Remote Access\Policy)*** *to* ***0*** *on the IAS server.*

If a user attempts authentication through MS-CHAP with an expired password, MS-CHAP prompts the user to change the password while connecting to the server. Other authentication protocols do not support this feature, effectively locking out the user with the expired password."7(page 12)

Configuring Windows 2000 Routing RAS Server for RADIUS

"*On a Routing and Remote Access server, RADIUS authentication and accounting is configured from the* ***Security*** *tab on the properties of a Routing and Remote Access server (right-click the server name in the Routing and Remote Access administrative tool, and then click* ***Properties****).Shows the* ***Security*** *tab for the Routing and Remote Access server properties:*

To configure the Routing and Remote Access server for RADIUS authentication, select ***RADIUS Authentication*** *in* ***Authentication provider****. To configure the Routing and Remote Access server for RADIUS accounting, select* ***RADIUS Accounting*** *in* ***accounting provider****.*

The authentication settings for a RADIUS server:
The ***Add/Edit RADIUS Server*** *dialog box is used to do the following:*

- *Enter the DNS name or IP address of the RADIUS server.*
- *Enter the shared secret.*

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- *Enter the amount of time in seconds to wait for a response from this RADIUS server before trying another RADIUS server.*
- *Enter the initial responsiveness score of this RADIUS server.*
- *Enter the UDP port used by the Routing and Remote Access service for sending and receiving RADIUS authentication messages.*
- *Enter whether the Routing and Remote Access server must always include the RADIUS signature attribute in Access-Request messages for PAP, CHAP, MS-CHAP v1, and MS-CHAP v2. With EAP, the signature attribute is always required. If you enable this, you must ensure that the RADIUS server is configured to always receive the signature attribute. This is the RADIUS client setting that corresponds to the IAS RADIUS client setting called* ***Client must always send the signature attribute in the request****.*

The settings for a ***RADIUS server for accounting****:*

The ***Add/Edit RADIUS Server*** *dialog box is used to:*

- *Enter the DNS name or IP address of the RADIUS server.*
- *Enter the shared secret.*
- *Enter the amount of time in seconds to wait for a response from this ADIUS server before trying another RADIUS server.*
- *Enter the initial responsiveness score of this RADIUS server.*
- *Enter the UDP port used by the Routing and Remote Access service for sending and receiving RADIUS accounting messages.*
- *Enter whether the Routing and Remote Access server sends the RADIUS Accounting-On and Accounting-Off messages when the Routing and Remote Access service is started and stopped.***"***7(page 65-67)*

3.5 Remote Access Client Configuration

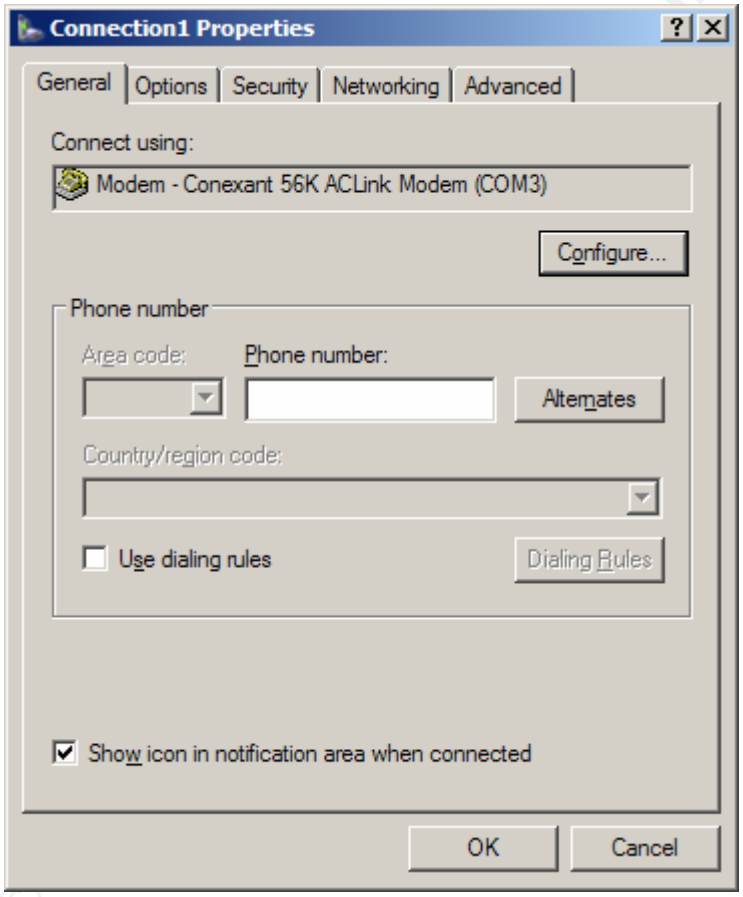
After installing the Modem in Client do the following steps

1. "Go to the **Start** and **Control Panel**
2. Double click on **network and Dial-up Connection**
3. double click on **Make new connection** – now you will get a Network connection wizard
4. Click on **Next** –now you will get a dialog box in that select **Dial-up to private Network**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5. Click **Next** –now you will get a new screen where you have to enter your RAS server modem phone number and click **next**
6. now you will get a new screen saying **connection Availability** in that you will have two option to create this connection in that select only for **myself** and click **Next**
7. now you will have screen saying Completing the network Connection Wizard – in this type the name that you want to use for this connection e.g. .type: Connection1 and click **Finish**
8. now you will get a screen asking your user Name: Password, Dial
   In that click on **Properties** – now you have following screen."*10*

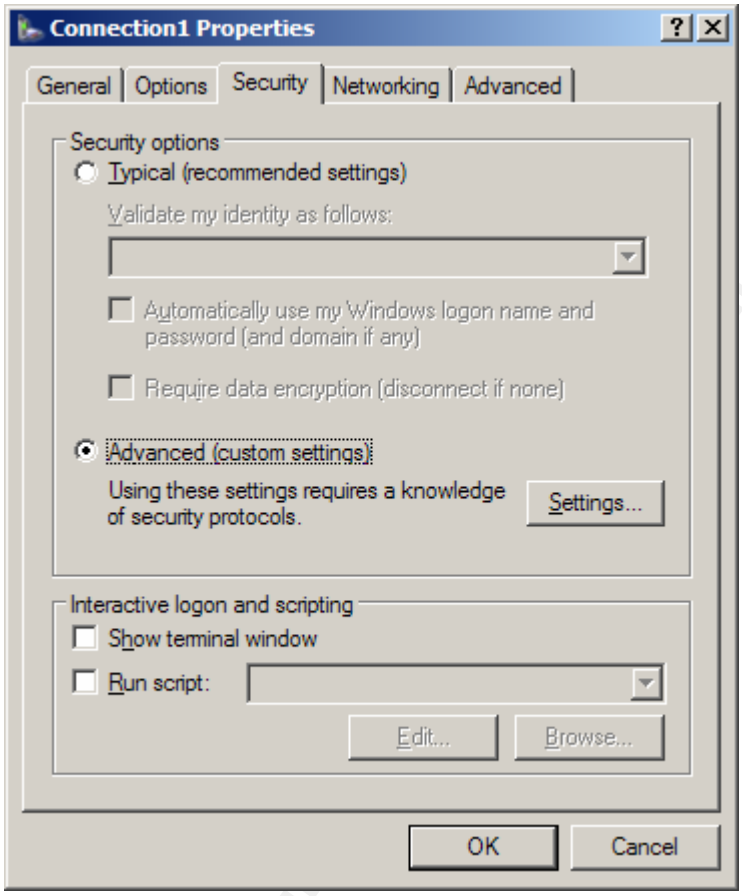
Picture 14



9. Select the **Security** Tab and go to security options
   In that select the **Advanced** Option and click on **settings** as shown in Picture 15.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Picture 15



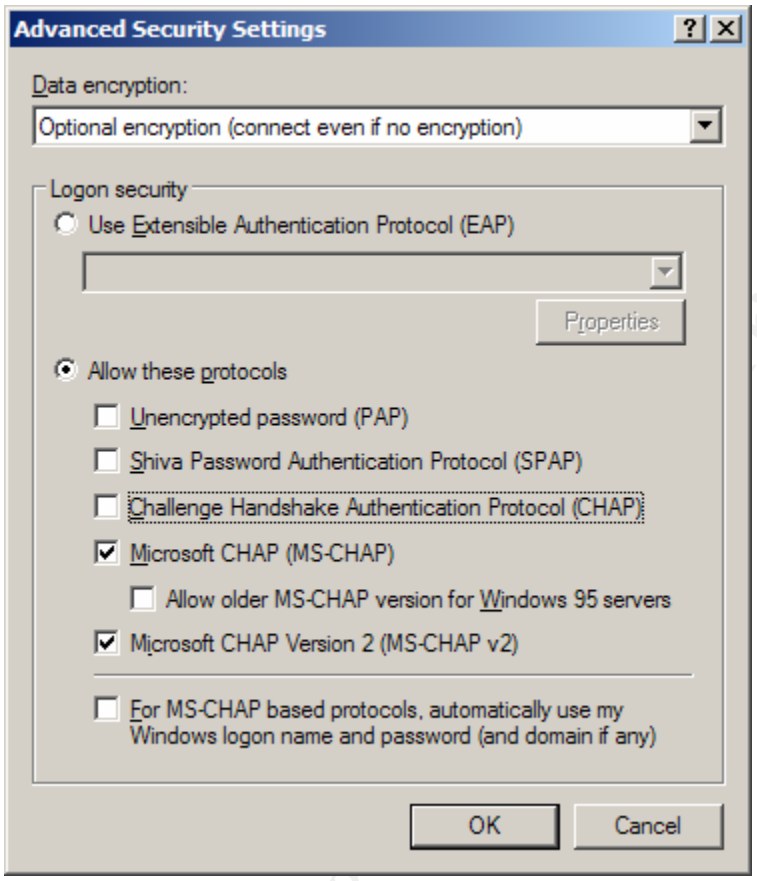
10. Now you will get the **advance security setting** dialog box

In that you will have three options like:

Data Encryption
Logon Security
Allow these Protocols

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Picture16



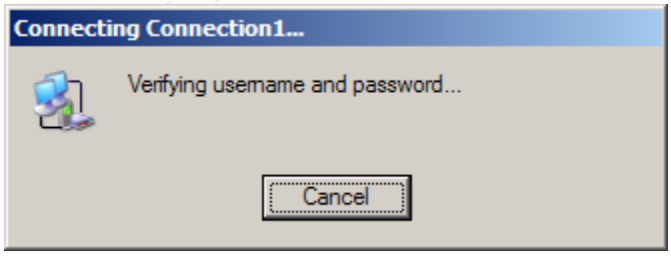
11. "*In the protocol list select only the **MS-CHAP** and **MS-CHAP v2** And Click **OK**"9* now you will be back to dialup connection screen, in that enter your
User Name: ftp-user1
Password: ********
Dialing Number: xxxxxxxx (this will be your RAS server modem number)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Picture17

12. Once you click on **Dial** the modem will dial on to your RAS server and negotiate the connection. After negotiating the connection, RAS will verify the Username and Password as shown in the Screenshot bellow

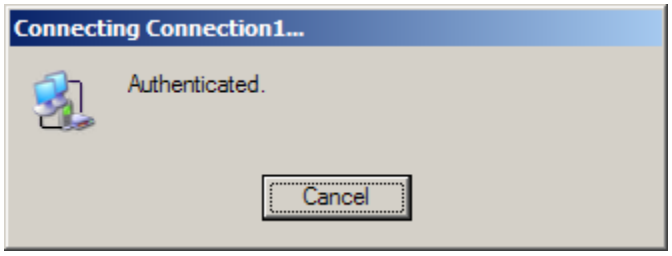
Picture18



13. Once the user name and password is ok you will get the following screen saying **Authenticated**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Picture19



And finally you get a dialog box saying **connected**

Now you have completed the **Remote access Client Configuration**

Note: for more detail see reference: ***10***

Conclusion:

Considering the security vulnerability of a RAS Server, it is essential to Ensure that the server is properly protected. The steps defined above Provide a low cost solution for an organization which already has Firewall in place. The cost of this setup may increase if the Firewall is not already set. This solution increase security of the RAS server.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Reference

1. http://www.microsoft.com/windows2000/en/server/help/sag_RASS_PPTP.htm(Point to Point Tunneling Protocol Terminology Description)

2. http://www.microsoft.com/windows2000/en/server/help/sag_RASS_L2TP.htm (Layer Two Tunneling Protocol Terminology Description)

3. http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/AUTH_EAP.asp(Extensible Authentication Protocol (EAP) Terminology description)

4. http://www.microsoft.com/serviceproviders/support/isp_ras_configuration.asp (Routing and Remote Access server configuration details from Microsoft)

5. http://www.winnetmag.com/Articles/ArticleID/5188/pg/2/2.html (Point to point Tunneling Protocol Advantage and disadvantages)

6. http://www.microsoft.com/windows2000/docs/VPNClient_AdminGuide.doc (Layer Two Tunneling protocols Advantage and Disadvantages from Microsoft server Document)

7. http://www.microsoft.com/windows2000/docs/IAS.doc (Complete details of Installing and Configuring of Internet Authentication Service with RADIUS Server and RADIUS Client)

8. http://sfghdean.ucsf.edu/cns/w2k/manageW2K.htm (Window 2000 Active directory User creation steps)

9. http://www.microsoft.com/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/sag_RRAS-Ch1_92.asp (Dial-up Remote access users Authentication method selection)

10. http://www.nbcs.rutgers.edu/newdocs/win2000/win2000.php3 (Remote Access Client Installation Screenshots)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

11. http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/l2tpt.htm#wp5939 (Layer Two Tunneling protocol with IPSec Terminology Description)

12. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wceeap/html/cxconExtensibleAuthenticationProtocol.asp (Extensible Authentication Protocol (EAP) Terminology description)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.