GIAC
CERTIFICATIONS

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

Implementing a Windows 2003 VPN Infrastructure

Christopher J. Delay Jr.
November 21, 2003
Version 1.4b
Option 1
GSEC

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

In an increasingly competitive business environment, as well as the increasing need for businesses to be able to access their data, email and documents, anytime, anywhere, it is becoming more and more difficult to juggle the diametrically opposed ideals of access and security. Several widespread methods for accessing this data remotely are Dial-Up Networking, Virtual Private Networking, Web Mail, and Web Based Terminal Services, such as Citrix MetaFrame. Virtual Private Networking has been, and will continue to be a popular method for remote access, especially with the wide availability of high-speed internet access, in hotels and at home.

Introduction

In the following pages I will introduce you to Virtual Private Networking in Windows 2003. This is a "How To" create a VPN Infrastructure from scratch. This "How To" can be used to implement a VPN in you existing network, or to create a VPN in a test lab, so that you can evaluate whether it meets your needs and requirements. The first section will familiarize you with some terminology that will be used in the remainder of the text. The second section will show you how to implement a secure VPN with Windows Server 2003, including the setup of all the necessary components of the VPN Infrastructure.

Terminology

Active Directory- The Directory Service implemented in Windows 2000 and Windows 2003.
DHCP- A network service which distributes IP addresses as well as other information such as default gateway to clients in a TCP/IP based network.
DNS- A network service that converts IP Addresses to host name and vice versa for network clients.
EAP- Extensible Authentication Protocol, a protocol which allows additional protocols such as Kerberos, and Hardware Devices such as smart cards to be used for authentication.
IAS- Microsoft's implementation of Remote Authentication Dial In User Service (RADIUS), which allows centralized authentication for Dial Up Networking and Virtual Private Networking.
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.
MMC- Microsoft Management Console, Consoles for centralized management of network services, and host computers.
MSCHAP- Microsoft's Implementation of Challenge Handshake Authentication Protocol (CHAP), used for authentication, some enhancements to CHAP including storing hashed passwords instead of the cleartext passwords stored when using CHAP.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

PPTP- Point to Point Tunneling Protocol used to create a tunnel to encapsulate traffic sent over public networks, supports a variety of networking protocols including IP and IPX.

Implementing a Windows 2003 VPN Infrastructure

This section assumes that you have a basic understanding of networking and TCP/IP. In the following pages we will be implementing the VPN Infrastructure from scratch, including installing Active Directory. If you have some the core services already implemented in your network, you may not have to install some of the components and services listed below, you would simply use those services and components you already have installed. I would strongly suggest that you create this VPN Infrastructure in a lab environment, and thoroughly test it, before implementing it in a production network. I would also recommending further locking down the operating system (http://www.nsa.gov/snac/index.html) by applying a security template. What security template to apply is outside of the scope of this article, but you can either apply one of the templates that ship with Windows, get a template from somewhere else, for example the NSA has some security templates for download, or create your own.

The components necessary for a secure Windows 2003 VPN Infrastructure are Active Directory, DHCP, DNS, IAS, Certificate Server, and a VPN Server. You may already have Active Directory running in your network, in that case you could incorporate your AD Infrastructure into this VPN Infrastructure. Assuming you have AD already running you may have all or several of all the components previously listed, but for the "How To" we are going to build the entire environment from scratch, and you can customize your installation, to fit your current environment.

Network Setup

The first thing that you need to do is to install Windows 2003 on two servers or workstations, you can also use VMWare if you have limited access to hardware. We need to build two servers, depending on your environment, you can build out a server for each service. However, we will build, one server which will run Active Directory, IAS, DHCP, DNS, Certificate Services, and the second server will handle VPN Connections. You will also need a client machine, running Windows XP to test the VPN. You can connect all three machines together on a single hub, we will be simulating an Intranet and Internet by simply using two separate IP ranges, and letting the VPN Server route between them to simulate access to the Intranet from the internet. The first server will need one network card and a private IP address assigned to it. You can use your own addressing scheme however in this "How To" we will be using the 192.168.1.0/24 addressing scheme for the "Internal Network", and the 10.0.0.0/24 addressing scheme for the external network. For the first server assign the address

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

192.168.1.1, the subnet mask 255.255.255.0, and default gateway 192.168.1.1. The VPN Server should have two network cards, one assigned with IP address 192.168.1.2/24 default gateway 192.168.1.1. The second network card should be assigned the IP address 10.0.0.1/24 with no default gateway. Once the Active Directory Installation is complete on Server1, which will be described in the following paragraphs add the IP address 192.168.1.1 as the DNS server on the TCP/IP of Server1, and the TCP/IP Properties of the interface with the 192.168.1.2 IP address on Server2 which will be the VPN Server.

Active Directory Setup

The first thing we need to do is to install Active Directory on the first server, which from now on will be referred to as Server1. To install Active Directory on Server1, left mouse click on the "Start" button, select "run", and type "dcpromo". This will start the Active Directory Installation Wizard. Once the Active Directory Installation Wizard starts, click "Next". You will then be prompted that down-level clients may not be able to log on or access network resources, click "Next".

You will now be prompted, whether you are creating a domain controller for an existing domain or creating a domain controller for a new domain. If you are adding this domain controller to your existing domain, select "domain controller for existing domain". However, if you are creating a new domain, for production, or for testing, select "domain controller for a new domain", and click "Next". For the purposes of this "How To", we will be selecting "Domain Controller for a new domain".

On the next screen it will ask you what type of domain you wish to create. If this is a new stand alone domain, or outside of your existing forest, select "Domain in a Forest". If you are adding this domain as a child to a parent domain, in your existing forest, select "Child Domain in an existing Tree", and if you want the new domain to exist in the existing forest, but want to start a new tree, select the last option, "Domain Tree in an existing Forest". For the purposes of this "How To" we will be selecting "Domain in a Forest", after selecting "Domain in a Forest", click "Next".

Active Directory relies heavily on DNS, not only for name resolution, but also for clients to be able to locate critical services such as the Key Distribution Center, and LDAP Servers through SRV records. So in the next screen you will be prompted, whether you would like to configure the server to point towards an existing DNS Server ("Yes, I will configure the DNS Client") or if you would like to install DNS on the server you are setting up, "No, just install and configure DNS on this computer". In order to use Active Directory Integrated Zones, which allow Secure Dynamic Updates, Multimaster Replication, a more efficient replication scheme, you must install DNS on Domain Controllers. Since we are setting up a new Active Directory Installation, as well, we will go ahead and install DNS. If you are setting up the VPN infrastructure in your production network, you may or may not install DNS on Domain Controllers, depending on your Infrastructure. So, select "No, just install and configure DNS on this computer", and click "Next".

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Since we are creating a new domain, we are then prompted for New Domain Name. If you are implementing this in a Production network, you may have a naming convention you use for naming new domains, however, if installing in a lab you can use your existing naming convention, to simulate your network, or you can name the domain whatever you want. I used vpntest.local in my lab environment, the .local denoting that it is a private network. So enter a name in the text box, and click "Next".

You will then be prompted for the NETBIOS name, in order to support down-level clients, just accept the default and click "Next".

Next you will be prompted on where you would like Database and Log files stored. You can accept the default, however, depending on your hardware configuration, and performance issues you may want to separate the database and log files on separated disks, since databases usually receive more reads then rights, and the inverse is true of log files. Once you have chosen the location for your database and log files, click "Next".

You will then be asked for a storage location for Shared System Volume (Sysvol). Sysvol is where files that must be accessed by other computers such as logon scripts are stored as well as files that must be replicated. Once again depending on the hardware you have and performance issues decide where the appropriate place is to store Sysvol, and then click "Next".

Then you will be prompted for permissions, as in should permissions be compatible with Pre-Windows 2000 Operating systems. This adds the everyone group to the "Pre-Windows 2000 Compatible Access Group" which allows the Everyone Group to now have read access to all objects in Active Directory. It is strongly recommended for security reasons, that you upgrade all clients and servers to at least Windows 2000 so you can use "Permissions Compatible only with Windows 2000 or Windows Server 2003 Operating Systems" setting. Since we will be using only Windows 2003 Server, and Windows XP, in the "How To", we will select the "Permissions Compatible only with Windows 2000 or Windows Server 2003 Operating Systems" setting, and click "Next".

In the following screen you will be prompted for a Directory Services Restore Password. It is extremely important that you do not forget the password that you enter here. This password will be used if you ever have to restart the Domain Controller in Directory Service restore mode, to perform an authoritative or non-authoritative restore, as well as use the ntdssutil to defragment or move the directory database. Enter a password, and then click "Next".

You will then be presented with a summary of the selections you have previously made, click next. The Active Directory Wizard Installation Wizard will then install active directory and DNS. Then the wizard will inform you that it has completed the Active Directory Installation, click "Finish". You will then be prompted restart Windows, click "Restart Now".

When Windows restarts, log in as a domain administrator. We will now raise the functionality. Raising the domain functionality and forest functionally to Windows 2003, so that all functionally enhancements introduced in Windows 2003 will now be available. *Note: All domain controllers must be running Windows Server 2003 for the functionality to be raised to 2003, this is also an*

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

irreversible process, once you raise the functionality, you cannot go back. To raise the domain functionality, open the "Active Directory Domains and Trusts" mmc. Then right click on the domain node, and select "Raise Domain Functionality Level" from the popup menu. Select Windows 2003, and then click "Raise". To raise the forest functionality level, right click the "Active Directory Domain and Trusts" node in the "Active Directory Domain and Trusts" mmc, and select "Raise Forest Functional Level" from the popup menu, select Windows Server 2003, and click "Raise".

DNS Setup

When DNS is installed by the Active Directory Installation Wizard, only a forward lookup zone is created, to ensure that DNS works with applications that use reverse NSlookups, we are going to add a Reverse Lookup Zone. To add a reverse lookup zone, go into the Administrative tools and open the "DNS" mmc. Expand the Server node in the "DNS" mmc, then right click on "Reverse Lookup Zone", and then click "New Zone". This will start the New Zone Wizard, click "Next", at the Welcome screen. You will then be prompted for new zone type, select "Primary Zone", and make sure that "Store the zone in Active Directory" is checked, and then click next. Next you will be prompted for the "Active Directory Zone Replication Scope" accept the default "To all DNS Servers in the Active Directory Domain…" and click "Next". You will then be prompted for the first three octets of the IP address so that the Reverse Lookup Zone can be created, type 192.168.1. Then you will be prompted for the type of dynamic updates, select secure dynamic updates, and click next. Then you will be informed that you have completed the Wizard, click "Finish".

DHCP Setup

We now have a Domain Controller running Active Directory, and DNS. The next step is to install DHCP on Server1. DHCP will not only be used to distribute IP addresses to any hosts on the "Internal" Network, but will also work in conjunction with the DHCP Relay Agent, to distribute IP address to VPN Clients. To install DHCP, open the Control Panel, and then double-click on Add/Remove Programs. Once the "Add/Remove Programs" applet opens, click on "Add/Remove Windows Components", this will launch the "Windows Components Wizard". Click on "Network Services", and then click the "Detail" button. In the Networking Services applet check Dynamic Host Configuration Protocol (DHCP), and then click "OK". On the Windows Component Wizard, click next. The "Windows Component Wizard" will now install DCHP, you will be prompted for the Windows 2003 Server Media if it is not in the CD Drive.

You must now authorize the DHCP Server, and create a scope. Launch the "DHCP" mmc from Administrative Tools. Click on Action in the Menu Bar, and click "Authorize" to authorize the DHCP Server. Right click on the domain node, and select "New Scope" from the popup menu. Click "Next" on the Welcome to the New Scope Wizard screen. Next you will be prompted for a

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Scope Name, enter a scope name, and optionally a description, and then click "Next". In the scope IP range type 192.168.1.1 as the Start IP address, then enter 192.168.1.254 as the End IP address, and finally enter 255.255.255.0 as the Subnet Mask, then click "Next". You will be then prompted for exclusions, for this "How To" we are using 192.168.1.1-2 on the two servers, so we will enter Start IP Address 192.168.1.1 and End IP address 192.168.1.2, then click "Next". If you are using more then two servers, make the necessary adjustments in the exclusion range. Next you will be prompted for the Lease Duration, for the purposes of this "How To" we can accept the default value of 8 Days, and then click next. We will then be prompted to configure DHCP options, we will add an option for the Default Gateway and DNS, so select "Yes, I want to configure these options now", and click "Next". For the default gateway, enter 192.168.1.1, and click next. In "Domain Name and DNS Servers", type the domain name, then in the DNS section type the IP address of the DNS Server, in this case 192.168.1.1, and click "add", then click "Next". When prompted for WINS Servers, click "Next" since we will not be adding any WINS Servers, then click "Next". On the Activate Scope screen, make sure "Yes, I want to activate the scope now" is selected and click "Next". On the "Completing the New Scope Wizard, click "Finish".

Adding Users and Groups

You should now populate Active Directory with Users and Groups. For this "How To", you need one global security group, which I will refer to as Group1 and one user, which I will refer to as User1. You may create as many users as you wish. User1 must be made a member of Group1. Group1 will be the group which is granted VPN access, so anyone you wish to add VPN access to must be made a member of Group1. To make life a little bit easier, you may want to name Group1 VPNUSers, VPNAccess, or something that denotes the purpose of the group.

To create a new user open the "Active Directory Users and Computers" mmc (sometimes referred to as the aduc). Right click on the Users (Organizational Unit) OU, and select new from the popup menu, then select "User". Enter a user name and a log on name and click "Next". Enter a password and confirm the password. Uncheck User must change password at next logon, and check User cannot change password, and password never expires, and click next. *Note: These are settings that should only be used in a test environment, in a production environment the user should change the password at next logon, so that the user can create a password, that can easily be remembered, and so that the person responsible for creating accounts does not know user passwords. Also, in a production environment, User cannot change password, should be unchecked, password never expires should be unchecked, since this poses a security risk, and account should be disabled, until the new user account is actually going to be used.*

To create a new group open the "Active Directory Users and Computers" mmc. Right click on the Users OU, and select new from the popup menu, then

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

select “Group”. Enter a name for the group, make sure the Group Scope is set to global, and Group Type is set to Security, and then click “OK”. We must now add at least one user to the new group, so that later on we can test the VPN. Now, click on the Users OU, and in the details pane, right click on the group, you just created, and click on properties on the popup menu. Click on the members tab, in the group properties, and click the “add” button. Enter the username of the user you previously created, and click “OK”, then click “OK” in the Group Properties Dialog Box.

IAS and Remote Access Policy Setup

Next we are going to Install Internet Authentication Service (IAS) on Server1. IAS will be used to authenticate users connecting to the VPN. To install IAS, open the Control Panel, and then double-click on Add/Remove Programs. Once the Add/Remove Programs applet opens, click on “Add/Remove Windows Components”, this will launch the “Windows Components Wizard”. Once the “Windows Components Wizard” is open, select “Networking Services”, and click “Details”. Check “Internet Authentication Services” checkbox, and click “OK. Then click next on the “Windows Components Wizard” applet. And click “Finish” when IAS is finished installing.

Before we configure IAS, we must first register it in active directory. So open the “Internet Authentication Service” mmc, from Administrator Tools, and right click on Internet Authentication Service, and on the popup menu click “Register Server in Active Directory”, then click “OK”. After you register IAS with Active Directory, right click on the Radius Clients folder within “IAS” mmc, and from the popup menu select “New Radius Client”. When the New Radius Client wizard opens, name the new Radius Client “VPN”, then enter the IP address of the VPN Server (192.168.1.2) and click next. On the additional information screen, make sure RADIUS Standard is selected as the “Client-Vendor”, and enter a shared secret, and confirm it. It is important that you remember this shared secret, because later you will need to enter it on the VPN Server. Make sure the “Request must contain the Message Authenticator attribute” checkbox is unchecked, and click “Finish”.

Next you must specify Remote Access Policies to allow Group1 to be able access the VPN, encryption level, as well as what type of authentication will be used. In a production environment, or as you do further testing in a lab environment, you would add additional Remote Access Policies, to secure remote access. Some examples of additional policies you could implement include what times can a user use remote access, how long sessions can last, packet filters, and so on.

In the “IAS” mmc, right click on Remote Access Policies, and in the popup menu select New Remote Access Policy, on the welcome screen, click “Next”. You will then be asked whether you want setup a typical policy or a custom policy. Right now we are just setting up a basic policy, later on you can go back and add additional policies. Give a Name to the policy such as “VPN” or “VPN Remote access”, click next. You will then be prompted for an Access Method, in

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

this scenario we are setting up a VPN, so select VPN, and click “Next”. You will now be asked if you want to base access on a user account basis or a group basis. From a day to day management standpoint, it is better use group, because then you can manage Remote Access by just adding or removing user accounts from a security group. So select Group, and click “add”, and add the group you previously created, and click “OK”, and then “Next”. Then you will be prompted on what type of authentication you would like to use, you can use EAP if you are planning to install a certificate on each Remote Access Client, or if you intend to use Smart Cards or some other third-party authentication method. If you do not plan to use certificates or smart cards, you would most likely use MSCHAPv2, you could use MSCHAP if you have down-level clients that do not support MSCHAPv2. MSCHAPv2 supports mutual authentication, whereas MSCHAP only supports one-way authentication. So, check the checkbox for MS-CHAPv2, and click “Next”. You will then be prompted for what level of encryption you would like to use. You can choose between 40-bit, 56-bit, and 128-Bit Encryption. In this case, and in most cases, we would want to choose the highest level of encryption, so we will uncheck the check boxes for “Basic Encryption”, and “Strong Encryption”, and leave the “Strongest Encryption” checkbox, checked, then click next, and finally click Finish to close the wizard.

VPN Server Setup

Now we will move onto Server2 and setup the VPN Server, and the DHCP Relay agent. Before moving forward we must first add the VPN Server to the domain we created previously. Open up Control Panel, Double Click on “System”, click on the “Computer Name” tab, click the “change” button, select domain, enter the name of the domain you previously created, click “OK”. You will then be prompted to authenticate with the domain as an administrator, type <domain name>\Administrator, in the username textbox, and then type the administrator password in the password text box, and then click “OK”, Click “OK” again to close the applet, and then you will be prompted to restart the system, click “Restart Now”, to complete the process. To setup the VPN Server, open the “Routing and Remote Access” mmc, and right click on the server node, and from the popup menu select “Configure and Enable Routing and Remote Access”, at the Welcome screen, click “Next”. On the configuration screen, select Remote access (dialup or VPN), and click “Next”. On the Remote Access screen check the VPN checkbox, and click “Next”. On the VPN connection select the network interface that is connected to the “Internet”, and make sure the security checkbox is checked and click “Next”. On the IP Address assignment screen, select automatically, and click “Next”. Next on the Managing Multiple Remote Access Servers screen, click “Yes, setup this server to work with a RADIUS server”, and click next. On the Radius Server Selection screen, enter the IP address of Server1 in the Primary RADIUS server text box, and enter the shared secret that you previously entered while setting up IAS on Server1 into the Shared Secret text box, click “Next”, then “Finish”. You will then receive a dialog box informing you that you need to setup a DHCP relay agent and point it at the DHCP Server.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

So now we will configure the DHCP Relay agent. Expand the IP Routing node within the Routing and Remote Access mmc. Right click on DHCP Relay agent, and from the popup menu select “properties”. Enter the address of the DHCP Server, which in this case is 192.168.1.1, then click “add”, and then “OK”

Certificate Services Setup

In order to use L2TP for encapsulating data sent through the VPN, we must install a certificate on the VPN Server, and later on the VPN Client, to do this we will set up a group policy to force members of the domain to autoenroll for certificates. Before we can force autoenrollment, we must first add certificate services to our domain. Log back onto Server1 as the domain Adminstrator. To install Certificate Services, open the Control Panel, and then double-click on “Add/Remove Programs”. Once the “Add/Remove Programs” applet opens, click on “Add/Remove Windows Components”, this will launch the “Windows Components Wizard”. Once the “Windows Components Wizard” is open, check “Certificate Services”, (you will be warned that you cannot rename the computer after certificate services is installed, or joined or removed from a domain, click “Yes” to acknowldedge the warning). You will then be prompted for CA Type, select Enterprise root CA, then click next. On the next screen, enter a Name for the CA, and click “Next”. On the Certificate Databases screen, accept the default location, and click “Next”. Certificate Services will then install, when it is finished installing click “Finish”. You will be warned that Web Enrollment will not be active until IIS is installed, click “OK” to acknowledge the warning.

We must now create the group policy, to force the Certificate Auto-Enrollment. Open the Active Directory User and Computers, and right click on the domain node, and from the popup menu click “properties”. When the Domain Properties opens up, select the Group Policy tab. Now click edit, to edit the Default Domain Policy. Expand the Computer Configuration node, then expand the Windows Settings node, then expand the Security Settings node, then expand the Public Key Policies node, then right click on Automatic Certificate Request Settings, from the popup menu click New, then click Automatic Certificate Request. When the welcome screen opens, click “Next”, on the Certificate Template screen, and highlight computer, and then click next, then “Finish”. We now must refresh the Group Policy on Server1 and Server2 so they will autoenroll for certificates. On both Server1 and Server2, click on the “Start” button, then “Run”, and type “cmd”, in the Run text box, and click “OK”. When the cmd console opens type “gpupdate”, and then press the enter key.

VPN Test Client Setup

Now we must setup the client, to test the VPN. We will now use two network settings to simulate both Intranet connectivity and Internet Connectivity, so that we can test the VPN. When we want to connect to the Intranet to add the Windows XP to the domain we will configure the TCP/IP Properties, to

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

automatically obtain an IP address and DNS Server, then when we test the VPN we will manually configure the IP address of 10.0.0.2/24.

So configure the XP Machine or VM to automatically obtain an IP address and DNS Servers, and add the Machine to the domain. After the machine reboots to finish the process of adding it to the domain, change the IP address on the machine to 10.0.0.2/24, with no default gateway, and no DNS Servers.

Now we will add the both the PPTP and L2TP VNP connections to the client machine. Open the Control Panel, if the control panel is in "Category View", click "Switch to Classic View", then double-click on "Network Connections". Then click on "Create a New Connection". On the welcome screen click "Next", when prompted for Network Connection Type, choose "Connect to the network at my workplace", and then click "Next". On the Network Connection screen, select "Virtual Private Network connection", and then click "Next".

In the Connection Name Screen you can type whatever you feel is appropriate for the name but you should include "PPTP" in the name, because this will be a PPTP Connection. After you enter a name Click Next. On the VPN Server Selection Screen, type 10.0.0.1, and click "Next". You will then be prompted whether the connection should be available for Anyone's Use or My use only, select whatever setting is appropriate, for your circumstance, then click "Next", then "Finish". When the Connect Dialog box opens, click on the "Properties" button, and then click on the "Networking" tab, and change the "Type of VPN" to PPTP VPN, then click "OK". In the Connect Dialog box, then type in the username text box, <domain name>\<username> (The name of the Domain you created followed by a backslash, and then the username you created earlier in this "How To"). Then in the Password text box, type the appropriate password, and click "connect". Once the VPN finishes connecting, open a cmd console and type ping 192.168.1.1 just to verify connectivity to the internal network. Then right click on the network icon in the system tray and from the popup menu click "disconnect", to disconnect the VPN.

Now we will create the L2TP Connection. Open the Control Panel, if the control panel is in "Category" View, click "Switch to Classic View", then double-click on network connections. Then click on "Create a New Connection". On the welcome screen click "Next", when prompted for Network Connection Type, choose "Connect to the network at my workplace", and then click "Next". On the Network Connection screen, select "Virtual Private Network connection", and then click "Next".

In the Connection Name Screen you can type whatever you feel is appropriate for the name but you should include "L2TP" in the name, because this will be a L2TP Connection, after you enter a name click "Next". You will then be asked if you want to dial the PPTP connection, select "Do not dial the Initial Connection". On the VPN Server Selection Screen, type 10.0.0.1, and click "Next". You will then be prompted whether the connection should be available for Anyone's Use or My use only, select whatever setting is appropriate, for your circumstance, then click "Next", then "Finish. When the Connect Dialog box opens, click on the "Properties" button, and then click on the "Networking" tab,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

and change the “Type of VPN” to L2TP IPsec VPN, then click “OK”. In the Connect Dialog box, then type in the username text box, <domain name>\<username> (The name of the Domain you created followed by a backslash, and then the username you created earlier in this “How To”). Then in the Password text box, type the appropriate password, and click “connect”. Once the VPN finishes connecting, open a cmd console and type ping 192.168.1.1 just to verify connectivity to the internal network.

Final Notes

You have now completed creating the VPN Infrastructure. You can now add other services or applications such as IIS to the internal network, to test if you can access these service or applications from the VPN. You can also go about changing Remote Access Policies, and testing them to see how they may affect Remote Access Users. And if you are using or planning on using a certificate or smart card to authenticate Remote Access Users, you can configure your VPN to use EAP Authentication.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

1) Holme, Dan; Orin, Thomas. "MCSA/MCSE Self-Paced Training Kit (Exams 70-292 and 70-296): Upgrading Your Certification to Microsoft Windows Server 2003". Microsoft Press. 2003. 105-123.

2) Microsoft Corporation. "HOW TO: Create an Active Directory Server in Windows Server 2003". http://support.microsoft.com/default.aspx?scid=kb;en-us;324753.

3) Microsoft Corporation. "HOW TO: Install and Configure a DHCP Server in an Active Directory Domain in Windows Server 2003". http://support.microsoft.com/default.aspx?scid=kb;en-us;323360

4) Microsoft Corporation. "HOW TO: Install and Configure a Virtual Private Network Server in Windows Server 2003". http://support.microsoft.com/default.aspx?scid=kb;en-us;323441.

5) Microsoft Corporation. "HOW TO: Set Up Routing and Remote Access for an Intranet in Windows Server 2003 Enterprise Edition and Windows Server 2003 Standard Edition". http://support.microsoft.com/default.aspx?scid=kb;en-us;323415.

6) Microsoft Corporation. "Step-by-Step Guide for Setting Up VPN-based Remote Access in a Test Lab". http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/rmotevpn.asp. Published: March 2003.

7) Microsoft Corporation. "Use Virtual Private Networks for Secure Internet Data Transfer". http://www.microsoft.com/windowsxp/pro/using/howto/gomobile/vpns.asp. Posted: September 16, 2003.

8) Microsoft Corporation. " Virtual Private Networking with Windows Server 2003: An Example Deployment" http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/deploy/confeat/vpnexamp.asp. Published: April 2003.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.