



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 permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at <http://www.giac.org/registration/gcwn>

Implementing a Secure Wireless Network for a Windows Environment

GCWN Practical Version 5.0
Option 2 – Topics in Windows Security

Dan Thompson
22 March 2005

© SANS Institute 2000 - 2005, Author retains full rights.

Table of Contents

1 Abstract.....	3
2 Introduction.....	4
2.1 Description of terms, concepts, and scope.....	4
2.2 Overview of the network configuration.....	5
3 Configuring the Network.....	9
3.1 Installing and Configuring a CA	9
3.1.1 Installing Certificate Services.....	9
3.1.2 Installing a Certificate on the RADIUS Server	11
3.2 Installing and Configuring a Radius Server.....	13
3.2.1 IAS Installation.....	13
3.2.2 IAS Configuration	14
3.3 Configuring AD users and the RADIUS policies for access.....	16
3.4 Microsoft Internet Security and Acceleration Server 2004	23
3.4.1 Installing and Configuring Microsoft ISA Server 2004	23
3.4.2 Configuring ISA to accept a DHCP address from the ISP	27
3.4.3 Checking for internet connectivity.....	32
3.4.4 Configuring ISA for a VPN and to allow for RADIUS pass-through.....	33
3.4.5 Configuring the ISA rules for the desired access levels.....	39
3.5 Configuring the Wireless Access Points.....	44
3.5.1 Configuring a Linksys Access Point.....	45
3.5.2 Configuring a D-Link Access Point.....	50
4 Configuring the Windows XP client.....	52
4.1 Configuring the wireless settings.....	52
4.2 Configuring the VPN client.....	55
5 Auditing the Wireless Network for Security and Deviation Effects.....	57

Conclusions.....	59
References.....	60

© SANS Institute 2000 - 2005, Author retains full rights.

1 Abstract

The goal of this paper is to be an easy to follow guide for configuring and securing a wireless network in a windows environment. Specifically we will look at configuring Microsoft Internet Security and Acceleration (ISA) Server 2004, Microsoft Certificate Services Server, Microsoft Internet Authentication Service, various off-the-shelf wireless access points, and the steps involved for configuring a VPN for connecting wireless clients as part of a defense-in-depth approach to 802.11 wireless networking. In the interest of space, a domain model will be discussed in depth using WPA Radius, however deviations from that will be touched on so that companies can start with the configurations and equipment they have now, and then build on it later. Additionally, basic wireless sniffing / hacking techniques will be covered lightly, so that administrators can audit the security of their networks and feel confident with the end product.

© SANS Institute 2000 - 2005, Author retains full rights.

2 Introduction

For some, the wireless world is a scary place, and rightly so! I believe, however, that there are several configurations available today that allow for very secure networking to be done free of the confines of normal wired environments. This paper will focus on one such configuration that is a holistic approach to a secure wireless Windows network, and then show deviations from that configuration so that administrators can implement the pieces they feel most comfortable with today, and add the other pieces later as time and money allow. Before diving in too deep, several terms and concepts should be discussed so that readers of different skill levels can be brought to a similar level of understanding.

2.1 Description of terms, concepts, and scope

To begin, wireless, as it is referred to in this paper, is defined by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 specification for wireless local area networks (WLAN), and will specifically focus on 802.11 b/g networks¹. WLANs are simply a “type of (network) that uses high-frequency radio waves rather than wires to communicate between nodes”.² This works, generally speaking, much the way the radio in a car works. Using this same analogy, many cars can receive the same signal from the radio tower, and in the same way, many computers can receive the same signal from the wireless antenna, or access point. While the radio stations are all public, I venture to say that most office networks are not meant to be so; thus the need for security.

The first such attempt at security was a protocol called the Wireless Equivalency Protocol, or WEP, however the sense of security it provided was short lived.

³Two major papers, from teams at Berkeley⁴ and the University of Maryland (UMD)⁵, attacked the design of WEP as flawed on various grounds. The Berkeley paper demonstrated weaknesses due to key reuse and weak message authentication. The UMD paper showed the weaknesses of 802.11 access control mechanisms, even those based on WEP's cryptographic authentication.

A later paper argued that the weak message authentication made it possible to inject traffic into the network.⁶ Although long-key length

¹ <http://standards.ieee.org/getieee802/802.11.html>

² “WLAN”. webopedia.com. 16 January 2004. 18 March 2005.
<<http://www.webopedia.com/TERM/W/WLAN.html>>

³ Footnotes 3 – 6 are references from within the “Wireless LAN Security: A Short History” (See footnote 7) paper, however are provided here with current links verified on 18 March 2005.

⁴ Borisov, Nikita, Ian Goldberg, and David Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11." 18 March 2005. <<http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>>

⁵ Arbaugh, William A., Narendar Shankar, and Y.C. Justin Wan. "Your 802.11 Wireless Network has No Clothes." 30 March 2001. 18 March 2005. <<http://www.cs.umd.edu/~waa/wireless.pdf>>.

⁶ Arbaugh, William A. "An inductive chosen plaintext attack against WEP/WEP2." IEEE Document 802.11-01/230, May 2001. 18 March 2005.
<<http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/1-230.zip>>

versions of WEP were released to the market, the flaws in WEP were not due to a short key. The flaws persist in any version of WEP, whether a short export-crippled key is used or a reasonably long key. One member of the 802.11 working group memorably described WEP as "unsafe at any key length" and urged the working group to redesign WEP⁷.⁸

These flaws in the initial security measures for WLANs is what brings us to the place we are today, a public that is generally untrusting of wireless networks. Since WEP was broken however, several new encryption and security measures have been introduced, such as, WPA™ and WPA2™, and most recently the 802.11i standard was ratified by IEEE.⁹ As of the writing of this paper, these measures remain very secure, and very good options for those wanting to provide protection for their wireless networks. However, this paper takes a step further and offers a solution that combines the security that WPA offers with the strength of tried and true VPN and firewall technologies, to provide a security in-depth approach that will ultimately transcend any weaknesses that may later be found in any one of the components.

The scope of this paper will be limited to the installation and configuration of the components needed to make this wireless scenario function properly and securely; over and above what is normally found on Windows 2000 / 2003 domain networks. It is assumed that the readers have at least a good working knowledge of domains, and the setup process to create them, as well as networking in general. Some infrastructure type of services will be touched on, such as Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP), however only changes and additions will be discussed as it is also assumed that the reader will be performing these actions on a domain that is functioning properly to begin with, including the utilization of these services. While the directions given in this guide will be easy to follow, and the configuration has been verified on several occasions, both in production and non-production environments; as with any new installation, "outside forces" can adversely affect the outcome, which is why a working knowledge of the Windows domain environment is needed. Lastly, it is highly recommended that these configurations be first tested in a test environment, similar to, if not identical to, that actual network that will be configured in the production environment. This will aid administrators in identifying possible trouble areas and allow time for adaptations to be made.

2.2 Overview of the network configuration

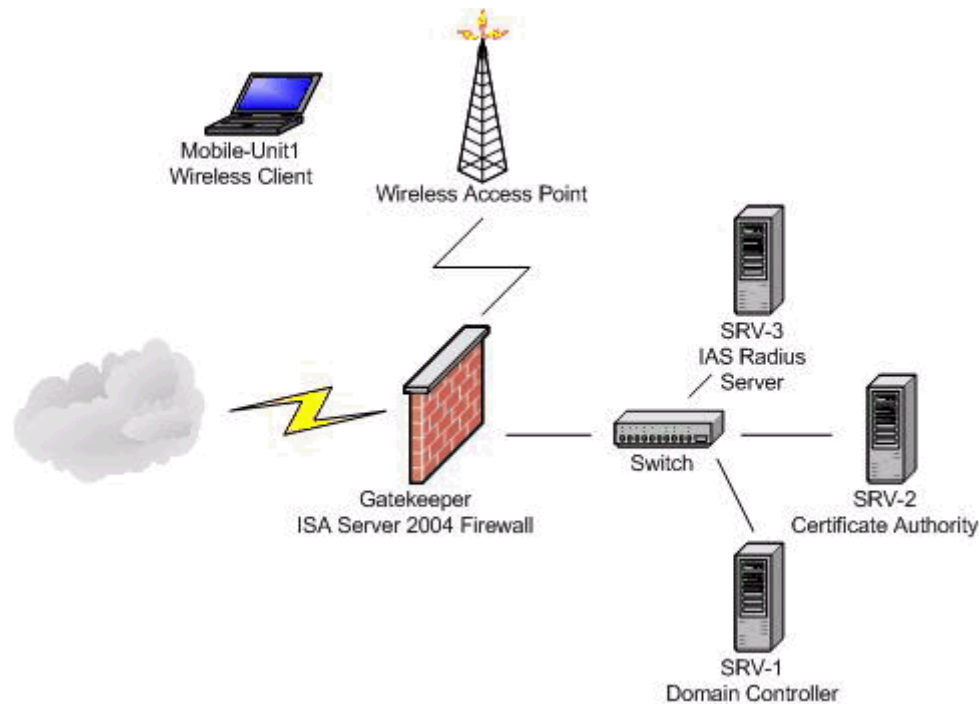
⁷ Walker, Jesse R. "Unsafe at any key size; an analysis of the WEP encapsulation." IEEE Document 802.11-00/362, October 2000. 18 March 2005.

<<http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip>>.

⁸ Gast, Matthew. "Wireless LAN Security: A Short History". O'Reilly Wireless DEVCENTER. 19 April 2002. 18 March 2005. <<http://www.oreillynet.com/lpt/a/1728>>.

⁹ For more information on WPA and 802.11i, see Elio Perez's paper, "802.11i (How we got here and where we are headed) as an excellent reference guide to wireless security in general, which can be found here, <http://www.giac.com/certified_professionals/practicals/gsec/4034.php>

The network used in this paper will be the testnet.msft domain and will be laid out as illustrated below:



IP Address Scheme

Segment	Subnet Address	Subnet Mask
Internal	172.1.0.0	255.255.0.0
Wireless Perimeter	192.168.1.0	255.255.255.0
External	DHCP Assigned	DHCP Assigned

Server Configuration

Gatekeeper	
Processor(s)	(2) Pentium III, 800 MHz
RAM	512 MB Memory
Hard Drive(s)	(2) 18 GB Hard Drive (Software RAID 1 mirrored)
Network Card(s)	(1) Realtek Gigabit Ethernet (internal network) (1) CNet Pro200 PCI 10/100 (wireless perimeter) (1) NetServer 10/100TX PCI (external network)
Operating System	Microsoft Windows Server 2003 Enterprise Edition (current patch level).
IP Address(es)	<ul style="list-style-type: none"> Internal - 172.1.0.1 Wireless Perimeter – 192.168.1.2 External – DHCP Assigned
Role or Function	<ul style="list-style-type: none"> ISA 2004 Firewall system providing internet proxy services VPN gateway.

SRV-1	
Processor(s)	(2) Pentium III, 1 Ghz
RAM	1.5 GB Memory
Hard Drives	(2) 40 GB Hard Drive (Software RAID 1 mirrored)
Network Card(s)	(1) Realtek Gigabit Ethernet (internal network)
Operating System	Microsoft Windows Server 2003 Enterprise Edition (current patch level).
IP Address(es)	<ul style="list-style-type: none"> Internal - 172.1.0.2
Role or Function	<ul style="list-style-type: none"> Domain Controller DNS DHCP
SRV-2	
Processor(s)	(1) Pentium III, 1 Ghz
RAM	512 MB Memory
Hard Drive(s)	(2) 40 GB Hard Drive (Software RAID 1 mirrored)
Network Card(s)	(1) Realtek Gigabit Ethernet (internal network)
Operating System	Microsoft Windows Server 2003 Enterprise Edition (current patch level).
IP Address(es)	<ul style="list-style-type: none"> Internal - 172.1.0.3
Role or Function	<ul style="list-style-type: none"> Domain Controller DNS Certificate Authority
SRV-3	
Processor(s)	(1) Pentium III, 1 Ghz
RAM	512 MB Memory
Hard Drive(s)	(2) 40 GB Hard Drive (Software RAID 1 mirrored)
Network Card(s)	(1) Realtek Gigabit Ethernet (internal network)
Operating System	Microsoft Windows Server 2003 Enterprise Edition (current patch level).
IP Address(es)	<ul style="list-style-type: none"> Internal - 172.1.0.4
Role or Function	<ul style="list-style-type: none"> IAS RADIUS server
Mobile-Unit1	
Processor(s)	AMD-K6 500 MHz
RAM	128 MB Memory
Hard Drive(s)	(1) 10 GB Hard Drive
Network Card(s)	(1) Linksys Wireless-G Notebook Adapter
Operating System	Microsoft Windows XP Professional SP2 (current patch level)
IP Address(es)	<ul style="list-style-type: none"> Wireless Perimeter – DHCP Assigned
Role or Function	Wireless / VPN Client

This type of network layout is referred to as a 3-leg perimeter network. The perimeter network in this case is our wireless network, however many people use this segment, also commonly referred to as the Demilitarized Zone (DMZ), for their servers which publish services to the internet. For people who have such a segment already configured, I would recommend configuring yet another segment for the wireless perimeter. The reason for putting these publishing servers in their own network is because we have to assume that at some point they will be compromised because of flaws either in the operating systems themselves or in the components that comprise the services they provide to the internet. The wireless network is placed on its own segment to mitigate attacks of an entirely different nature. As discussed earlier, wireless networks are inherently insecure and the flaws that exist in these networks are that of the actual transmission and encryption protocols and schemes, something for which there are no patches for. While the argument can be made that since both networks have a high risk of compromise they could be isolated together in the same DMZ, it is my opinion that there is no need to expand the attack surface of either network by combining the potential flaws, especially when all that is required is an additional network card in the ISA server and a small switch or hub to connect all the access points.

By establishing this perimeter network for our wireless to exist in, we create a sandbox of sorts for our users, and then grant them access into either our main network or onto the internet, or both, depending on the constraints the network administrators wish to impose. These access restrictions will come in the form of a dual factor authorization scheme followed by access restrictions placed on the user that authenticates. Our first layer of defense will come from WPA RADIUS authentication which will grant users access to the wireless network itself. Once the wireless connection is established, a VPN tunnel will be created through the firewall and onto whatever network we choose to let the given user have access to, giving us our second line of defense. With this scenario, wireless traffic will flow through an encrypted tunnel wrapped inside another encrypted tunnel. By doing this, we are not relying on one security scheme, but multiple schemes. WPA could be broken completely, and this would still be a secure form of communication with your network. As a matter of fact, you could use this same idea with WEP, or no encryption at all for that matter, and still have a decent level of security. These two scenarios will be discussed later in the configuration section for those administrators using older equipment that does not support the new 802.11i standards or WPA in general. An additional point to keep in mind is that since we are using a true firewall to separate the wireless users from the rest of the network, should the wireless segment be compromised through such means as a cracked WPA or WEP key, the main network is still safe because the firewall is standing in the middle.

This single firewall design configured in a 3-leg perimeter is being used with the small business in mind, however the ideas and concepts presented in this paper can be easily adapted to larger networks which use a firewall on either side of a DMZ. In cases such as these, the configuration discussed in this paper would be a good starting point for the front (internet facing) firewall.

The back (internal network facing) firewall configuration is outside of the scope of this paper, but great guides for many different configuration ideas can be found at ISAServer.org¹⁰.

3 Configuring the Network

3.1 Installing and Configuring a Certificate Authority

To be successful in our implementation, there needs to be a Certificate Authority (CA) on the network for the purpose of giving the RADIUS server a certificate for authenticating the wireless clients using Protected Extensible Authentication Protocol (PEAP). However, developing a full Public-Key Infrastructure (PKI) for the network for the sole purpose of giving out one certificate is overkill, and admittedly a poor use of such an awesome service. In the interest of space, a single enterprise root CA will be configured and used to issue a certificate to the RADIUS server, but administrators who do not have this service in use already on their networks are highly encouraged to fully explore this service and the ways to design a solid PKI. Administrators who are unfamiliar with this will most certainly want to browse through the “Public Key Infrastructure for Windows Server 2003” section of the *Windows Server System* site¹¹, and I would personally recommend reading Norman Christopher-Knight’s paper *Implementing a Windows 2003 PKI from an Existing Windows 2000 Network*¹². Administrators who already have an existing PKI, or administrators who wish to develop their own PKI can skip to section 3.1.2 *Installing a Certificate on the RADIUS Server*, after they have done so. Administrators wishing to simply explore the wireless solution presented in this paper should continue on to the next section for an install of certificate services.

3.1.1 Installing Certificate Services

Before installing certificate services, first we must install Internet Information Services (IIS) so that we can utilize the web enrollment feature. To do this, go to the control panel on the server you wish to make a CA and click “Add / Remove Programs” followed by clicking the “Add/Remove Windows Components” button. Next, double click “Application Server” from the list of available Windows Components and then double click “Internet Information Services (IIS)” from the Application Server list. From the Internet Information Services window, double click “World Wide Web Service”, and finally, put a check in the box next to “World Wide Web Service”. Click “OK” in all the windows, and then choose “Next” on the Windows Components Wizard. To conclude the installation of IIS, click “Finish”.

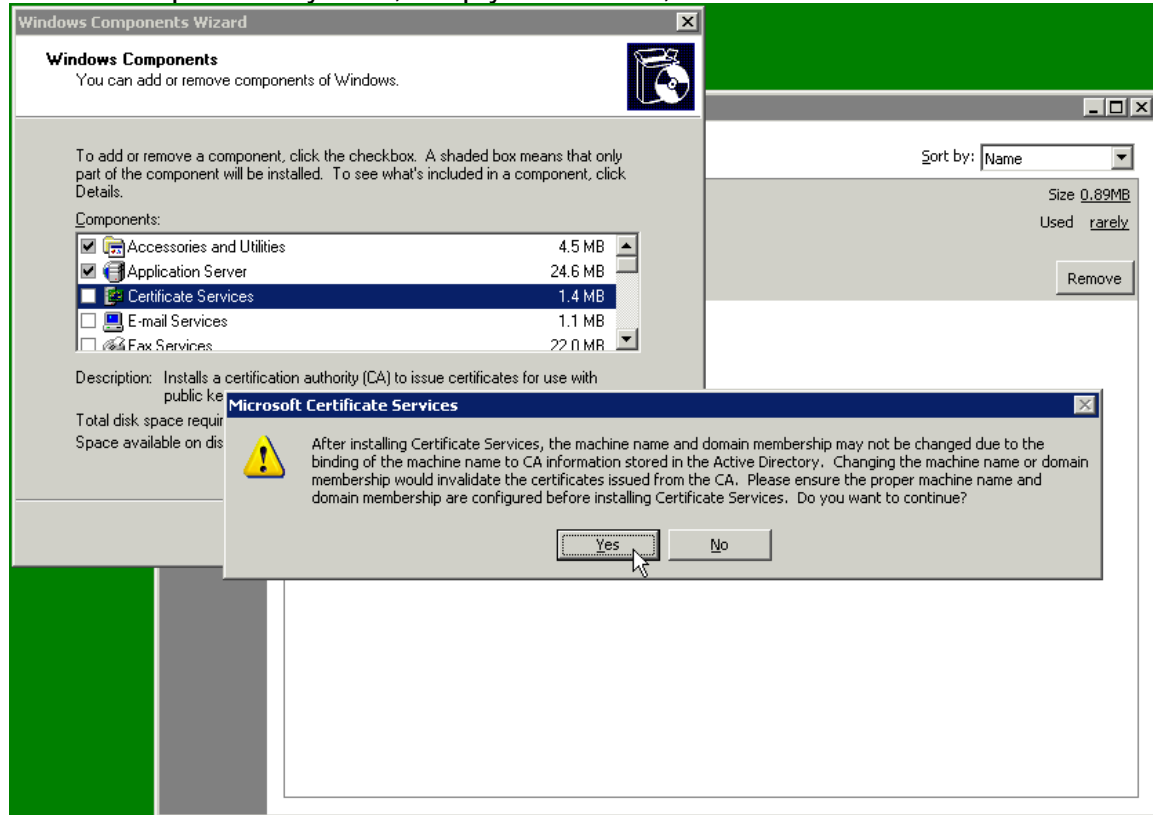
Now the server is ready to have Certificate Services installed on it. From the “Add or Remove Programs” window, click the “Add/Remove Windows Components” button again, and this time put a check in the box beside “Certificate Services”. A popup will appear letting you know that once the

¹⁰ <http://www.isaserver.org>

¹¹ <http://www.microsoft.com/windowsserver2003/technologies/pki/default.msp>

¹² http://www.giac.com/certified_professionals/practicals/gcwn/0265.php

service is installed administrators cannot change the name or the domain membership of the system, simply click “Yes”, and then “Next”.



For the purpose of this paper, we will install an Enterprise root CA, which is done by clicking the radio button next to “Enterprise root CA”, followed by clicking “Next”. For more information on the different types of CAs, see Microsoft’s website on “Defining CA Roles in the Trust Hierarchy”¹³. The next step is to name the CA; for the testnet.msft domain this will simply be “EnterpriseRoot”.

¹³ http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dssch_pki_gydb.asp

Once you have determined a name fitting to your organizations naming conventions, click “Next”. Following that, administrators will be asked to provide a location for both the certificate database and the certificate database log. It is recommended that these be stored in locations other than the default locations, and preferably on a different partition. While this is simply an attempt at “security through obscurity”, it can be effective in thwarting casual attacks. Following the placement of the various certificate components, administrators will be asked to stop IIS for the purpose of the installation, assuming this IIS server is not being used to host other websites, click “Yes”. Administrators will then be asked to enable active server pages, which is necessary for the web enrollment service, click “Yes”, and then choose “Finish” from the Windows Components Wizard.

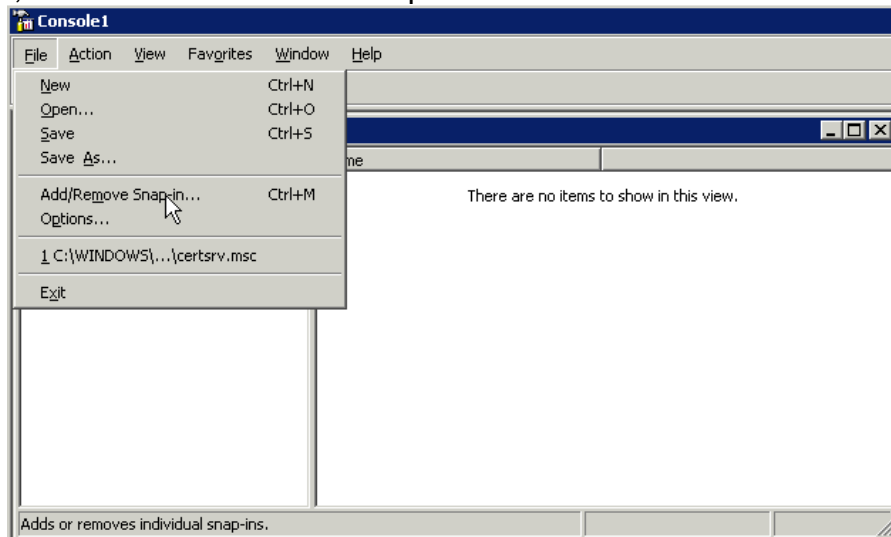
3.1.2 Installing a Certificate on the RADIUS Server

From the server where RADIUS will be installed, use Internet Explorer to browse to the certificate request page on the CA. For the testnet.msft network, this will be <http://srv-2/certsrv>. It is fairly common for this site to be relocated for added security, if the CA was already in place (not installed using the section 3.1.1 guide) administrators may want to consult the notes from the install, or the corporate security policy, for the correct location. Administrators who followed the 3.1.1 guide will use the default [//servername/certsrv](http://servername/certsrv) address.

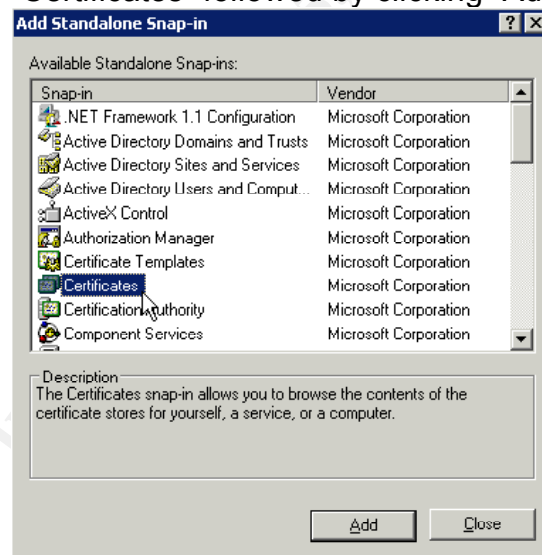
Administrators will be prompted to enter a username and password, after successfully authenticating with the server, and then will be presented with the Microsoft Certificate Services website. Click the “Download a CA certificate, certificate chain, or CRL” link from the “Select a task” menu. Next, click the link that says “install this CA certificate chain”, this will allow our server to trust certificates issued from our CA server. The last step will be to click “Yes” to the dialog box informing you that the website is adding a certificate to the computer.

Now that we have installed the CA’s certificate on the server, we can request a computer certificate for the RADIUS server itself. Since we have an

Enterprise Certificate Authority, we can request a certificate using the “certificates” snap-in. To do this, click the “Start” button, followed by clicking “Run...” and then typing *mmc* and then clicking “Ok”. From the File menu inside Console1, choose “Add/Remove Snap-in...”.

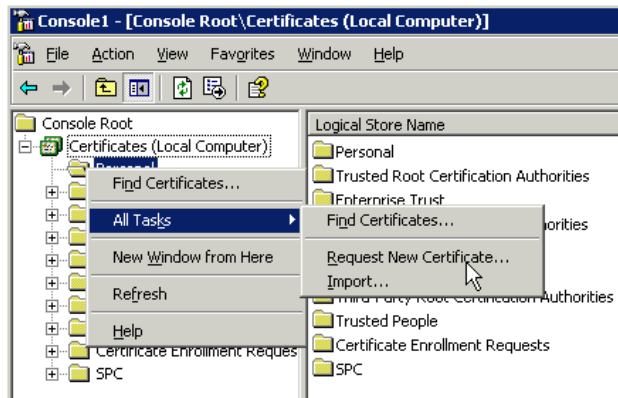


Next, click the “Add...” button at the bottom of the “Add/Remove Snap-in” window, and choose “Certificates” followed by clicking “Add”.



Administrators will be then asked what they want to manage certificates for, and for the purpose of the RADIUS certificate, choose “Computer Account” and then “Next”, and “Finish”. Click “Close” to the “Add Standalone Snap-in” window and then “Ok” in the “Add/Remove Snap-in” window.

Once back inside the Console1 window, expand the “Certificates (Local Computer)” and then right mouse click on “Personal”, and choose “All Tasks”, “Request New Certificate”.



This will spawn the “Certificate Request Wizard”, from here click “Next”. From the “Certificate types” field, choose “Computer” and then click “Next”. Enter in a name for the certificate, such as the server name, and then click “Next”. Finally, click “Finish”, and then administrators will be notified that the certificate request was successful; click “Ok”.

We now have a computer certificate installed that can be used for the PEAP authentication of the wireless users.

3.2 Installing and Configuring a RADIUS Server

Remote Authentication Dial-In User Service (RADIUS) is an industry standard protocol used to provide authentication. A RADIUS client (typically a dial-up server, VPN server, or wireless access point) sends user credentials and connection parameter information in the form of a RADIUS message to a RADIUS server. The RADIUS server authenticates the RADIUS client request, and sends back a RADIUS message response.¹⁴

There are a number of RADIUS products available on the market today, such as Funk Software’s Steal Belted RADIUS¹⁵, however I personally find that Microsoft’s implementation is just fine. Installing a RADIUS server using Microsoft Internet Authentication Service is extremely straight forward and the management of it is just as easy, and most importantly, it comes free with Windows 2000 and 2003 server products.

3.2.1 IAS Installation

Before beginning the installation, it is a good idea to review “Chapter 3: Creating a Member Server Baseline” and “Chapter 9: Hardening IAS Servers” from the Windows Server 2003 Security Guide¹⁶ for ideas on how to properly secure a Microsoft IAS server.

To begin the installation, open up the control panel on the server you wish to implement RADIUS, and open the “Add / Remove Programs” applet. From

¹⁴ Security Hardening Guide: Microsoft Internet Security and Acceleration Server 2004 Standard Edition.

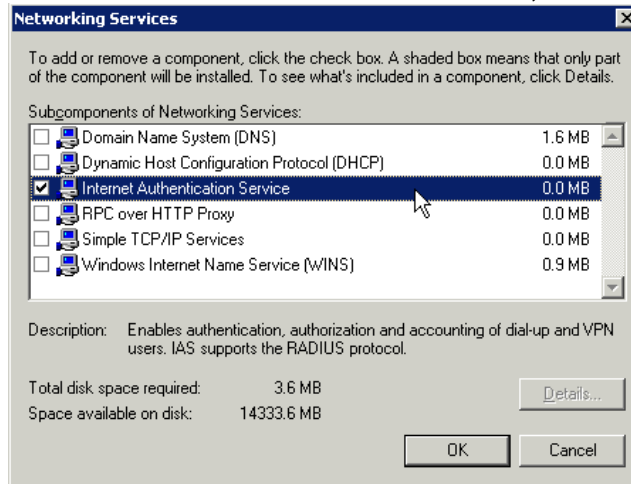
Redman: Microsoft Corporation. 7 March 2005

<<http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/securityhardeningguide.mspx>>

¹⁵ Funk Software’s Steal Belted RADIUS can be found here, <http://www.funk.com/radius/default.asp>

¹⁶ <http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.msp>

there, click on the “Add / Remove Windows Components” button. A Windows Components Wizard will appear, scroll down in the list until you see “Networking Services” and then double click it. Next, put a check in the box next to “Internet Authentication Service” and then click “OK”, “Next”, and “Finish”.

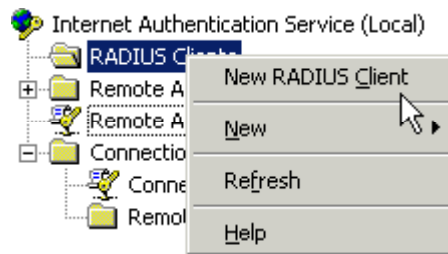


Internet Authentication Service (IAS) is now installed and ready to configure.

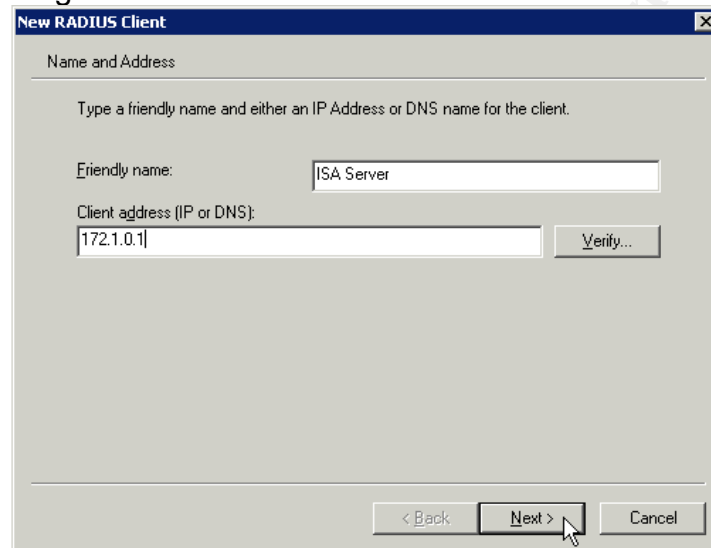
3.2.2 IAS Configuration

Configuration of IAS is done through the Internet Authentication Service console and can be found by clicking “Start”, “Run”, and then typing `ias.msc` and hitting enter. Once inside the console, the first thing that needs to be done is registering the IAS server with Active Directory. This is done by simply right mouse clicking on “Internet Authentication Service (Local)” at the top of the left hand pane and clicking “Register Server in Active Directory”. After doing so, a pop up will appear asking if you wish to authorize the computer to read the users’ dial-in properties (necessary to authenticate users in Active Directory), simply click okay, and then okay to the message confirming that the computer is now authorized.

Next we need to establish our RADIUS clients. These clients are computers that are allowed to make requests of the RADIUS server, and then the server replies with a “Yes or No” type of answer to the client based on the settings in Active Directory. In our case, the ISA server and our wireless access points will both be clients of the RADIUS server as both will be making requests to the server. The ISA will be requesting access for the purpose of authenticating VPN access and the access points will be requesting information for the purpose of WPA authentication. To create these clients, right mouse click on the “RADIUS Clients” link in the left hand pane of the console window and choose “New RADIUS Client”.



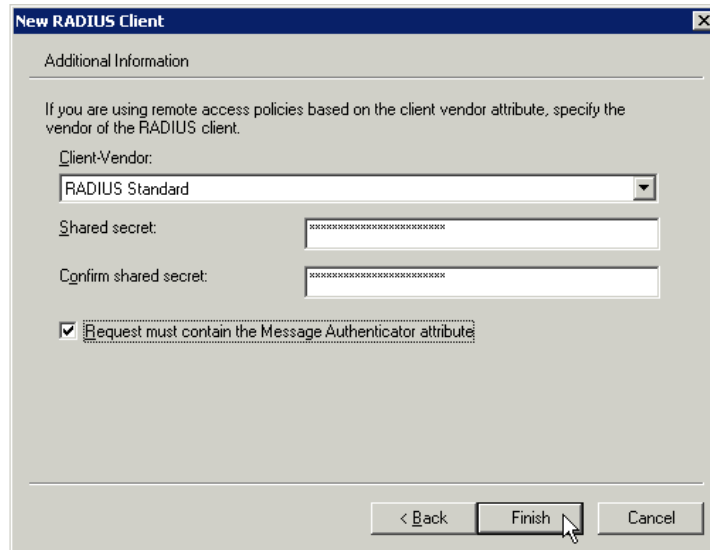
Inside the “New RADIUS Client” dialog box, enter the “Friendly name” and the “Client Address”. The “Friendly Name” is simply a name that is easy for you as the administrator to remember. For the ISA server, simply name it “ISA Server” and then enter the IP address of the internal interface card of that server, followed by clicking “Next”.



Next, we need to specify the “Client-Vendor”, which for both of our clients will be “RADIUS Standard”, and then enter the “Shared secret”. The shared secret for the ISA server will be *this is my shared secret*. When planning for your shared secret, it is important to make it complex as possible, Microsoft recommends a minimum of 22-characters with a “random sequence of letters, numbers, and punctuation” to protect against dictionary type of attacks¹⁷. Additionally, put a check in the box next to “Request must contain message authentication attribute”.

¹⁷ “To configure the Message Authenticator attribute and shared secret” [Microsoft Windows Server System](http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_ias_client_MessageAuth.asp). 19 March 2005.

<http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_ias_client_MessageAuth.asp>



To provide protection from spoofed Access-Request messages and RADIUS message tampering, each RADIUS message can be additionally protected with the RADIUS Message Authenticator attribute, which is described in RFC 2869, "RADIUS Extensions."

The RADIUS Message Authenticator attribute is a Message Digest 5 (MD5) hash of the entire RADIUS message. The shared secret is used as the key. If the RADIUS Message Authenticator attribute is present, it is verified. If it fails verification, the RADIUS message is discarded. If the client settings require the Message Authenticator attribute and it is not present, the RADIUS message is discarded.¹⁸

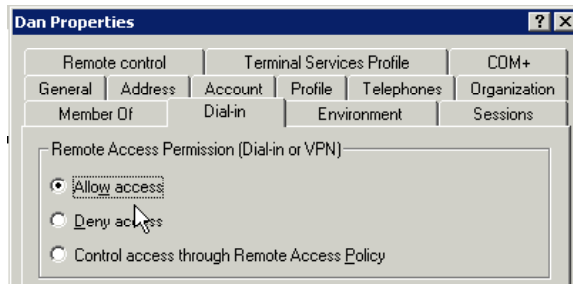
After those configurations are set, finish the client configuration by clicking "Finish".

This process will then need to be repeated for each of the RADIUS clients. Also note that with the access points tested in this paper, none supported the Message Authenticator attribute, consult with the wireless access point vendor prior to using this function, as it clients will not be able to connect if this is improperly configured.

3.3 Configuring AD users and the RADIUS policies for access

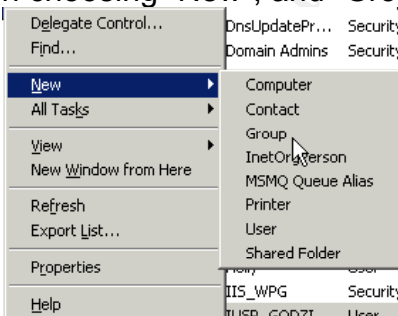
There are actually two ways to allow users to authenticate through our RADIUS server; one through Active Directory, and the second through the remote access policy on the RADIUS server itself. The first way would be to go to each user's property sheet in Active Directory, and set the "Remote Access Permission (Dial-in or VPN)" attribute to "Allow access".

¹⁸ "Message Authenticator attribute" Microsoft Windows Server System 25 February 2005
<http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_ias_messauth.asp>.

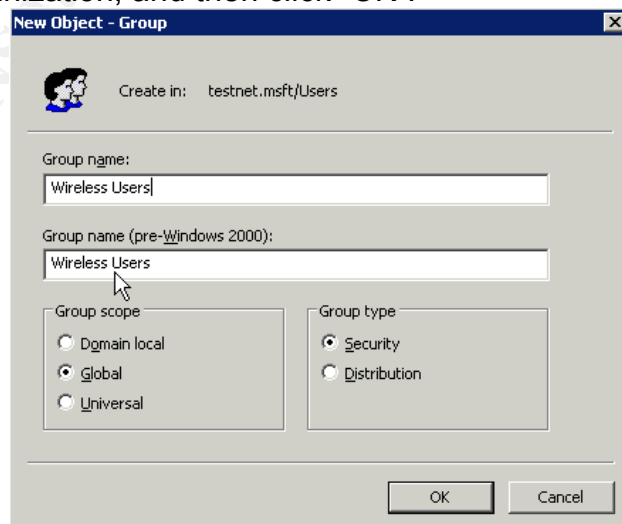


This method works, however it doesn't offer a lot of control, nor does it scale very well when you're talking about allowing lots of users. Even if you're starting off with just three users, for example, if it is feasible that in the future several more will need to be able to connect, you'd be better served to go ahead and do the second option to make management easier in the long run.

The second option is to establish who can connect through the remote access policy on the RADIUS server. Before we go to the RADIUS server though, there are a few things to do in Active Directory to make things easy for us. First, in Active Directory create a group for the wireless users. This can be done by right mouse clicking on the Organizational Unit (OU) you want the group to be contained in and then choosing "New", and "Group".



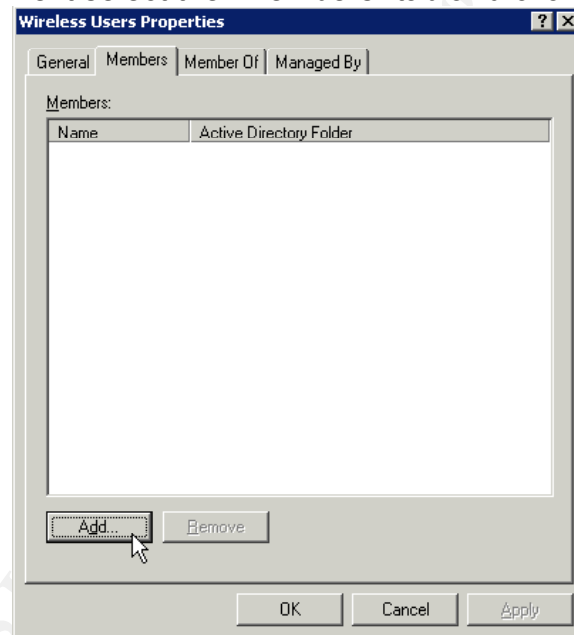
Next assign the group a name, for ease of recognition, *wireless users* is used in the testnet.msft domain, however administrators can use what ever name that fits the naming conventions of their organization. Following the name, assign the group scope, which will need to be a "Universal Group" and group type that apply to your organization, and then click "OK".



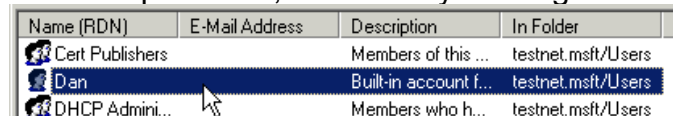
Discussions of the differences between the scopes and types are outside of the scope of this paper, however information on this topic can be found on Microsoft's website¹⁹. Also note, if you have a Microsoft Exchange server in your organization and you are using the "Active Directory Users and Computers" snap-in with the Exchange components installed, creating this group will have two more steps involved, simply click "Next" at the end of the last step mentioned above. Following that, put a check in the box beside "Create an Exchange e-mail address" if applicable, and click "Next" and then "Finish".



Now that our group is created, add the users to that group who will be connecting using the wireless / VPN solution we are creating. There are several ways to accomplish this; however I find the easiest way to add several users to a group is right mouse click on the group created for the wireless users and choose properties. Next select the "Members" tab and click "Add..."



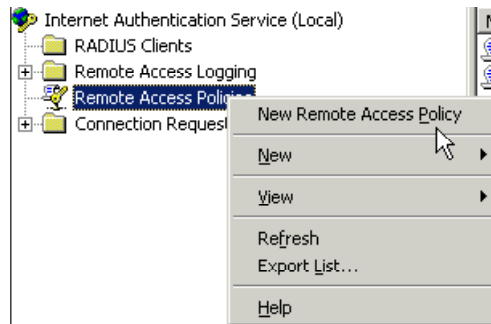
Inside the "Select Users, Contacts, Computers, or Groups" dialog box, click "Advanced" and then "Find Now", this will list all the user and group objects in Active Directory. Next, scroll until you find the user you wish to add to the group, and then double click the object, or you can hold down the "Ctrl" key on your keyboard and select multiple users, followed by clicking "OK".



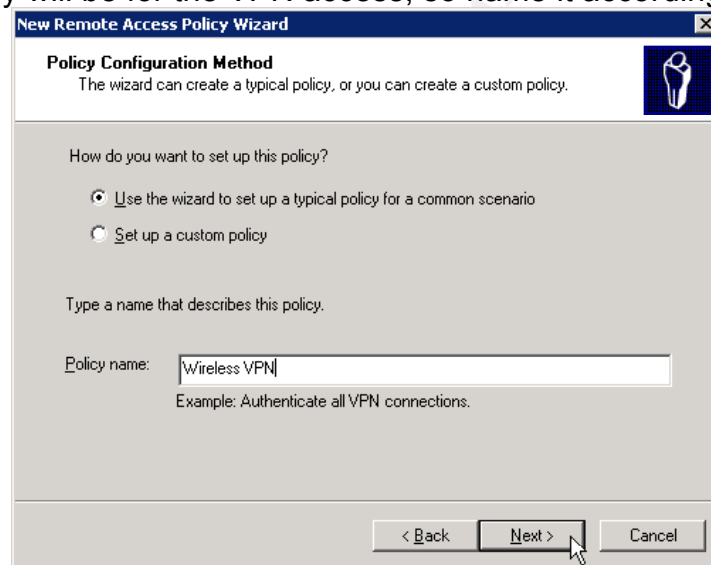
Once all the users desired are added, click "Apply" and "OK" on the "Wireless Users Properties" box.

¹⁹ http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_adgroups_3groupscopes.asp

Now that we have our group established and our users added, we need to configure the Remote Access Policy with the appropriate settings for our needs. On the RADIUS server, open the Internet Authentication Service console and right mouse click on the “Remote Access Policies” and choose “New Remote Access Policy”, which will launch the “New Remote Access Policy Wizard”.



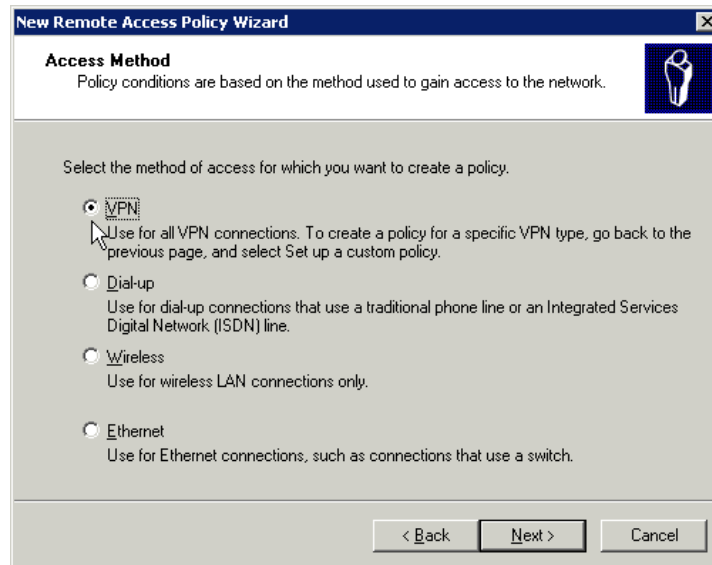
Once the wizard appears, click “Next”, and then select “Use the wizard to set up a typical policy for a common scenario”, and then name the policy. This particular policy will be for the VPN access, so name it accordingly.



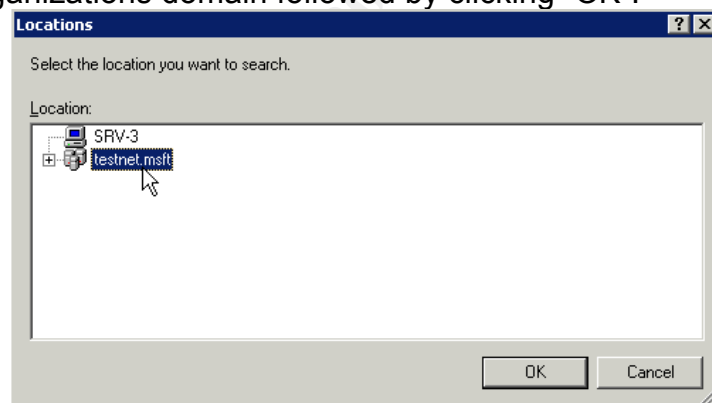
By selecting “Set up a custom policy”, administrators can have full control of every aspect of the policy, however I feel that the wizard does an excellent job of creating rules that will suit our purposes, and at the same time reduce the amount of “head scratching” new administrators will inevitably face when configuring these rules for the first time. For those interested in a more detailed look into these policies, more information is available on Microsoft’s website²⁰.

After the policy has been named, click “Next” to continue and then select “VPN” from the list of access methods, followed by clicking “Next” again.

²⁰ http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_rap_elements.asp



On the screen that follows, the group we created earlier will be granted for access. This is done by selecting the “Group” radio button, clicking “Add...”, and then clicking “Advanced”. At the top of the “Select Groups” dialog box, take note of the “From this location” field. The location we will be adding from is the domain, and not the local server where RADIUS is installed. If the name of the server is displayed in this field, click the “Locations...” button on the right, and select your organizations domain followed by clicking “OK”.



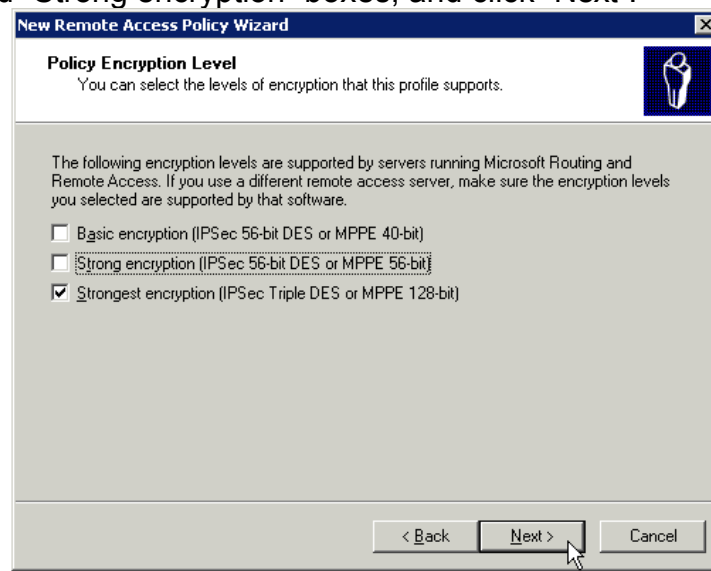
Note that if you are logged in locally to the RADIUS server instead of being logged in as a domain user, you will be prompted to provide domain user credentials after clicking the “Locations...” button.

Once the “From this location:” is set to the domain, click “Find Now” and then find the group created for the wireless users and double click it and then click “OK”.



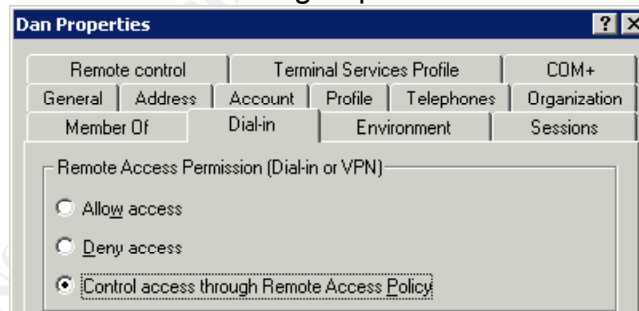
Now that the access group has been added, click “Next”. For our scenario, MS-CHAPv2 is all that will be needed, so ensure that a check is in the box next to it and then click “Next”. On the following screen, all of the encryption levels are displayed. To enforce the strongest possible encryption, uncheck the “Basic

encryption” and “Strong encryption” boxes, and click “Next”.



If you are using clients other than those mentioned in this paper, consult the manufacturer to see what encryption options are available, however for the purpose of this paper, this configuration will work well. Finally, review the settings and then click “Finish”.

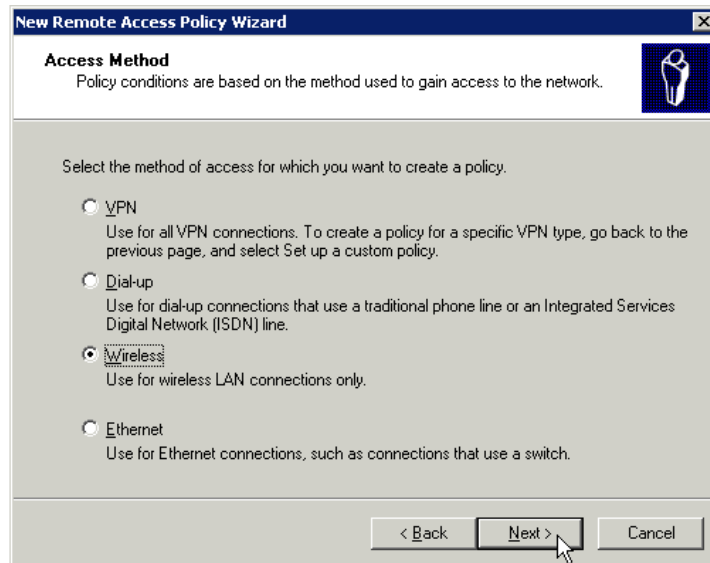
At this point, a basic access policy for the VPN has been configured and is ready to use. By default, when creating a new user in Active Directory, the “Remote Access Permissions” are set to “Control access through Remote Access Policy”, so in the future if an administrator wishes to add new clients to the list of people with access to the wireless network, all that needs to be done is add the user to the *Wireless Users* group.



As a best practice, it's a good idea to review the users' property sheets to make sure that the Dial-in properties have not been modified at an earlier date. Additionally, several other options are available to administrators on this portion of the user properties sheet, more information on those options is available on Microsoft's website²¹.

Next, we'll create a rule for our WPA RADIUS authentication. Follow the steps outlined above, except this time choose “Wireless” from the list of Access Methods, and click “Next”.

²¹ http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_rap_user_prop.asp



Again, choose the group to grant access to and click “Next”. Next, for the authentication type, choose “Protected EAP (PEAP)” from the drop down menu, and select “Configure”. By default, it will select the server certificate for the RADIUS server and it will have “Secured password” as the EAP Type, additionally, administrators will want to “Enable Fast Reconnect” by putting a check in the box next to it, and then click “OK”, “Next”, and “Finish”.

At this point, all the wireless clients who successfully authenticate with the RADIUS server will be granted access to the wireless network. To demonstrate the flexibility of this solution however, let me offer an additional scenario. Say for instance there are areas in the building where everyone can connect wirelessly, and other areas where only senior staff should be able to connect wirelessly. With IAS we can further modify the access policies to accommodate this. For the purpose of the testnet.msft domain, let’s say that the TWAP-1 access point covers the area where all wireless users can connect, and TWAP-2 services the area for restricted access only.

First, right mouse click on the Wireless access policy created previously, and choose properties. From the properties windows, click the Add button and choose “Client-Friendly-Name” from the list of Attribute types, and then select “Add...”. Next, enter the friendly name that was created for the client, in this case it will be TWAP-1, and then click “OK”, “Apply”, and “OK”.

The next step will be to return to AD and create a group for the senior staff members who will be permitted to connect, and then add that group to the “Wireless Users” group created earlier in this guide. This will ensure that the senior members will be able to connect to TWAP-1 as well as TWAP-2.

The last step is to create another access policy identical to the previous wireless policy, except this time choose the “Senior Staff Wireless” group instead of the “Wireless Users” group, and when adding the “Client-Friendly-Name”, use TWAP-2 instead of TWAP-1. This will create policies appropriate for restricting access based on the access point, as well as the user group; and can effectively limit areas of the building to certain users!²²

3.4 Microsoft Internet Security and Acceleration Server 2004

Microsoft Internet Security and Acceleration (ISA) Server 2004 is the advanced stateful packet and application-layer inspection firewall, virtual private network (VPN), and Web cache solution that enables enterprise customers to easily maximize existing information technology (IT) investments by improving network security and performance.

ISA Server contains a full featured, application-layer aware firewall that helps protect organizations of all sizes from attack by both external and internal threats. ISA Server performs deep inspection of Internet protocols such as Hypertext Transfer Protocol (HTTP), which enables it to detect many threats that traditional firewalls cannot detect. The integrated firewall and VPN architecture of ISA Server support stateful filtering and inspection of all VPN traffic. The firewall also provides VPN client inspection for Microsoft Windows Server 2003-based quarantine solutions, helping to protect networks from attacks that enter through a VPN connection. In addition, a completely new user interface, wizards, templates, and a host of management tools help administrators avoid common security configuration errors.²³

3.4.1 Installing and Configuring Microsoft ISA Server 2004

As with any type of installation, it is important to harden the operating system itself against attacks before configuring services to run on it, and then check your configurations at the end to ensure that you have followed the best practice recommendations for those particular services. Since this server will be a frontline of defense for the network while configured as a firewall, this is especially true. Before beginning the installation of ISA server administrators will want to read “Chapter 11: Hardening Bastion Hosts” of the Windows Server 2003 Security Guide²⁴; as well as the ISA Server 2004 Security Hardening Guide²⁵ after ISA has been installed. Note that the “bastion host.inf” configuration file mentioned in the Windows Server 2003 Security Guide is too restrictive in its original state to allow for a successful configuration as outlined in this guide and altering the inf file provided by Microsoft is outside of the scope of this paper.

Also, as per the security guides mentioned above, the ISA server is not a member of the testnet.msft domain. While a separate domain can be configured to control all the servers in the DMZ and thus further separating them from the internal network and providing a centralized management scheme, it is my opinion that such a configuration is overkill for the size of the network outlined in this paper and thus outside of the scope of this paper.

²² This statement assumes that the wireless access points are far enough apart that users could not connect to TWAP-1 while in an area serviced by TWAP-2.

²³ “What is ISA Server 2004?”. Microsoft Windows Server System. 15 February 2005. 28 February 2005. <<http://www.microsoft.com/isaserver/evaluation/overview/default.asp>>.

²⁴ <http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx>

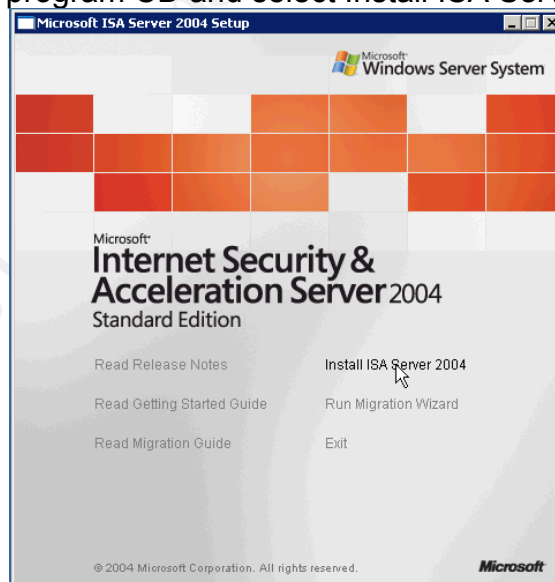
²⁵ <http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/securityhardeningguide.mspx>

Administrators should consider their network size and current security policies when deciding on this aspect of the whole security model. Since the RADIUS server mentioned elsewhere in this paper is a member of the testnet.msft domain, all wireless users will be authenticated using their domain user account credentials, regardless of the membership of the ISA server itself. That being said, either configuration; an ISA server as a member of a workgroup or of a DMZ domain, will function the same as it pertains to the configuration in this paper.

First, the ISA server needs to have its network adapter cards configured with the appropriate addresses. All interfaces should be configured with static addresses, with the exception of the interface that is attached directly to the internet, which can use a DHCP assigned address. Since extra configuration is required of the ISA server to accept and use a DHCP assigned address, this configuration type will be used during the installation and configuration segment. It is also recommended to assign a recognizable name to each interface to make setup and administration of the ISA server easier.

Once the operating system is sufficiently locked down and the IP addresses configured, we can begin the installation and configuration of Microsoft ISA Server 2004. While this paper assumes no level of understanding of Microsoft ISA Server 2004, it is always a good idea to get at least a basic understanding of products before you attempt to administer them. For a solid introduction I would recommend reading both *Understanding ISA Firewall Networks (v1.1)*²⁶ and *Configuring ISA Server 2004*²⁷.

The installation of Microsoft ISA Server 2004 (ISA) is fairly straight forward. Insert your program CD and select Install ISA Server 2004.

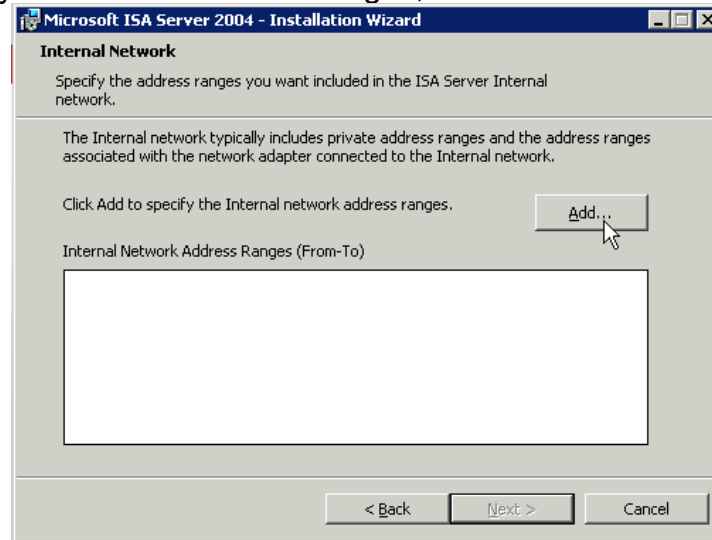


The installer is prompted to accept the normal Microsoft agreement and then prompted for User Name, Organization, and Product Serial Number. Enter the values that apply and continue by choosing “Next”. At the next screen, simply

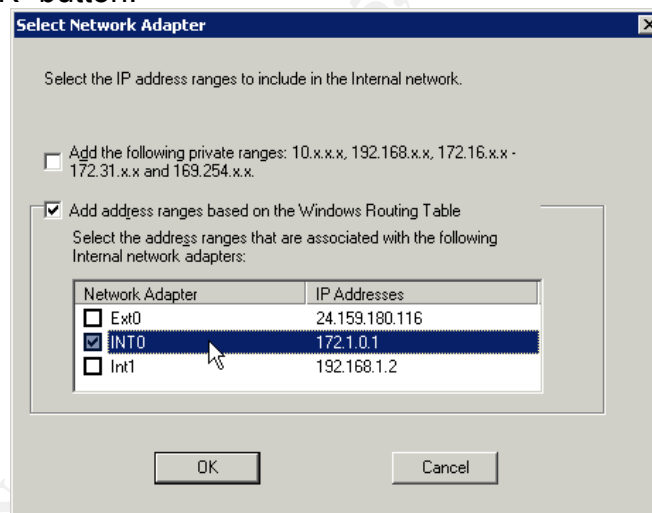
²⁶ <http://www.isaserver.org/articles/2004isafirewallnetworks.html>

²⁷ <http://www.isaserver.org/articles/Configuring-ISA-Server-2004-Chapter2.html>

choose “Typical” and then choose “Next”. The following screen requests that the installer specify the internal address ranges;



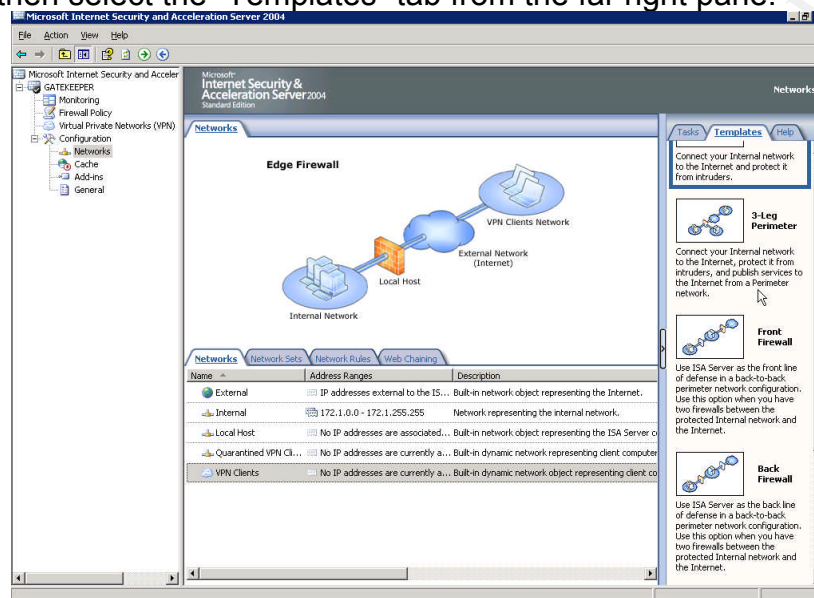
Select add and then click the “Select Network Adapter” button. On the screen that follows, uncheck the box that says “Add the following private ranges...” and then check the box that is next to the adapter card of the internal network, and then click the “OK” button.



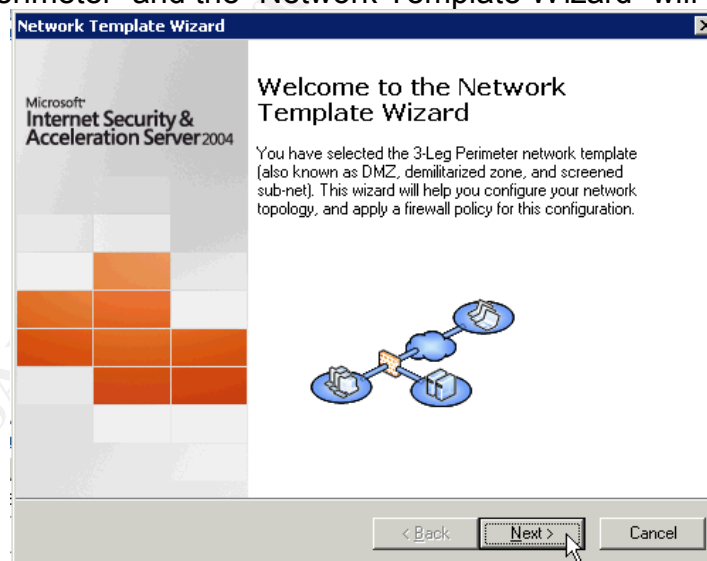
The installer will be presented with a warning about misconfigured routing tables, click “OK”, and “OK” and then click “Next”. Select “Next” to the remaining prompts and ISA will install. Once the Installation Wizard Completed screen appears, put a check in the box next to “Invoke ISA Server Management when the wizard closes” and then choose “Finish”. At this point the Microsoft Internet Security and Acceleration Server 2004 management console should appear, click the “Firewall Policy” link in the left hand pane and note the firewall policy list in the right hand pane. By default ISA installs with the “Last Default rule” which blocks all access to all networks and serves as a catch all to deny access to anything that has not been explicitly allowed by the administrator.

To simplify the configuration process of ISA Server, Microsoft has provided us with various configuration templates that serve as great starting

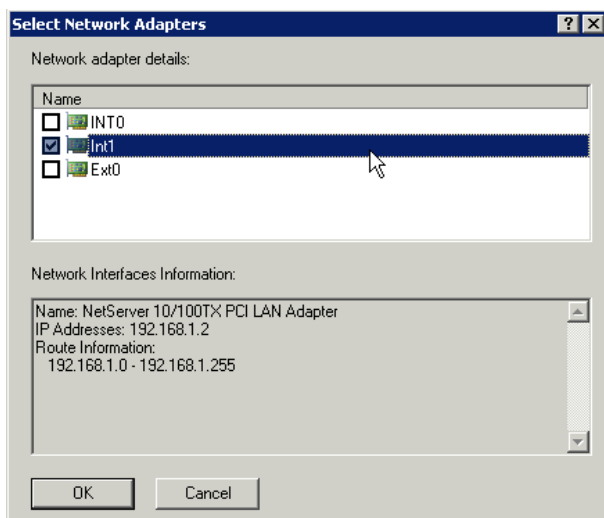
points for our configurations. At this point we will go ahead and apply the “3-Leg Perimeter” template. Please note that if you already have an ISA firewall configuration in place, applying these templates will **delete** your current running configuration. It is recommended, as always, to try these configurations out on a non-production server first and then add the policies you need to your running configuration once you feel you have mastered them. From the ISA management console, select “Networks” under “Configuration” on the left hand pane, and then select the “Templates” tab from the far right pane.



Click “3-Leg Perimeter” and the “Network Template Wizard” will begin.



Click “Next” until you reach the portion of the wizard where it asks you to define the Perimeter Network IP Addresses. Click “Add Adapter”, and then choose the network interface card that is attached to your wireless segment and click “OK”.



After selecting “Next”, you will be asked to select a firewall policy, choose “Block All”, then “Next”, and then “Finish”. Complete the template installation by clicking “Apply” from the top of the screen.

After the initial installation is complete, download any updates to ISA 2004 that may be available²⁸. As of this writing, ISA Server 2004 Service Pack 1 is the latest patch for the application. The installation is very straight forward, however see “ISA Server 2004 Standard Edition Service Pack 1 Released” for installation tips and a list of the fixes and improvements provided by the service pack, see ISAserver.org’s informative guide²⁹.

3.4.2 Configuring ISA to accept a DHCP address from the ISP

The next step is to configure the ISA server to allow DHCP traffic from the ISP to itself so that the server can receive a DHCP assigned address. This configuration is common in scenarios where a cable modem or digital subscriber line (DSL) is used for internet access. If your particular network accesses the internet by some means that allows for a static address, such as a T1 connection, please proceed to section 3.1.3 *Checking ISA internet connectivity*. If you do not intend to connect your network to the internet at all, please proceed to section 3.1.4 *Configuring ISA Rules to allow RADIUS pass-through*.

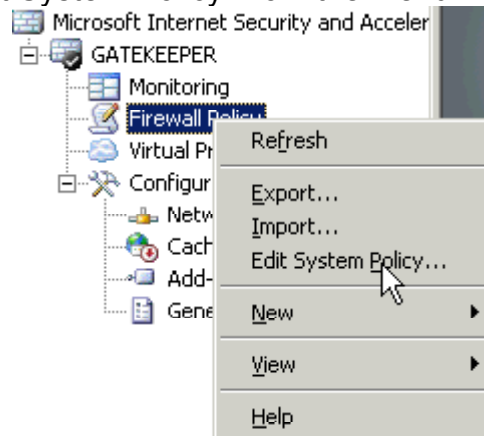
If the ISA server was connected to the internet prior to the installation, it is likely that the network card already has a DHCP assigned address associated with it, however after the server is rebooted or the DHCP lease runs out, connectivity will be lost. In the interest of insuring proper configuration, release the IP address by typing `ipconfig /release` at the command prompt. The command prompt can be reached by clicking the “Start” button, selecting “Run” from the programs menu, and typing `cmd` followed by clicking the “OK” button. Confirm that the server now has an IP address of 0.0.0.0 on its external interface card by typing `ipconfig` at the command prompt and hitting enter. Now we can be confident that when the server has an IP address on its external interface

²⁸ <http://www.microsoft.com/isaserver/downloads/2004.asp>

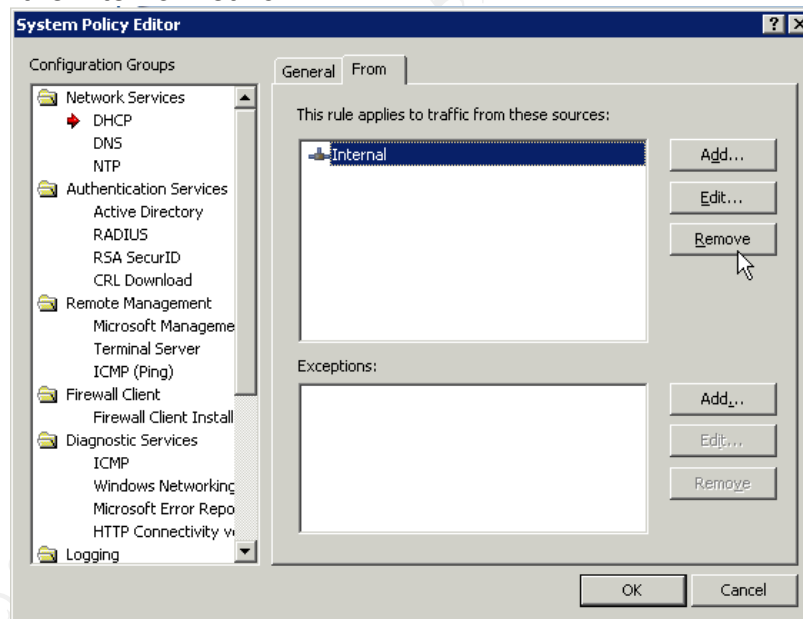
²⁹ <http://www.isaserver.org/articles/2004sp1.html>

again, our server is configured correctly.

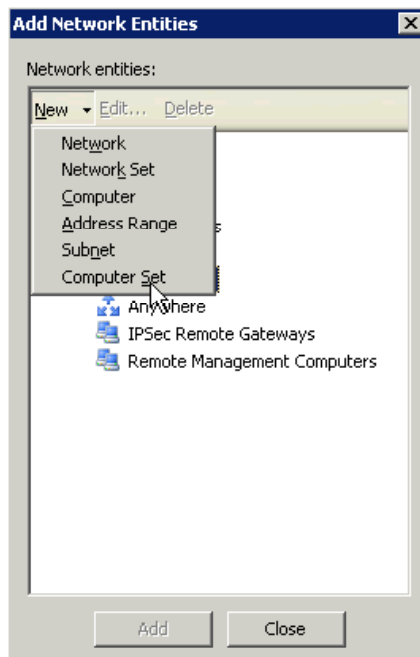
Return to the ISA Server Management console and right click on “Firewall Policy” and select “Edit System Policy” from the menu.



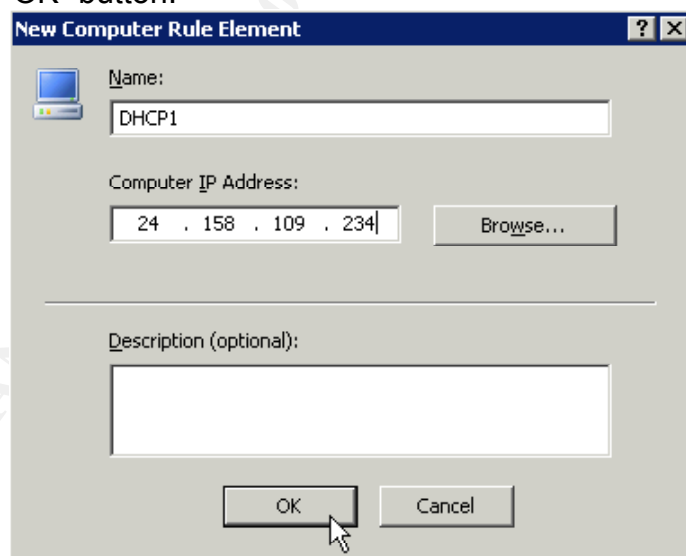
From the System Policy Editor, choose DHCP from the left hand pane, insure that there is a check in the box beside “Enable” and then select the “From” tab. To begin, it is a good idea to remove the “Internal” network from the “This rule applies to traffic from these sources” list. Since our server is configured with static internal addresses, there will never be a need to receive an address from a system on the internal network.



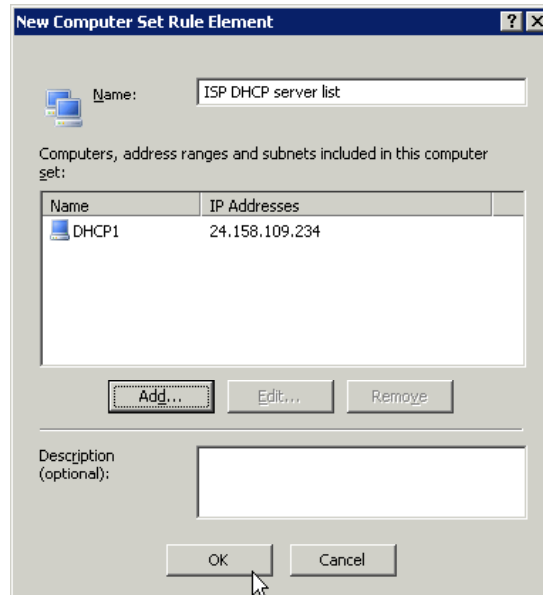
Once that is removed, click “Add” to insert the addresses of your ISP’s DHCP servers. From within the “Add Network Entities” dialog box, select “New” and then choose “Computer Set” from the drop down menu.



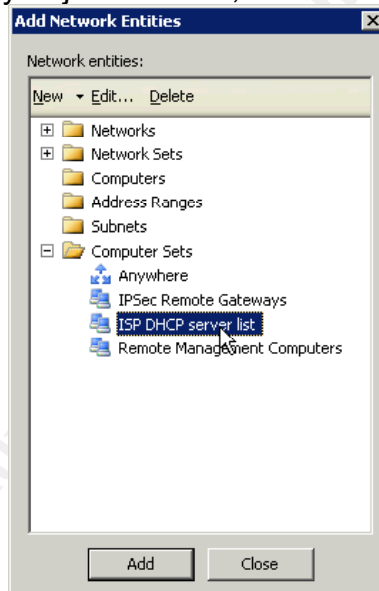
Enter a name that will be easily recognizable by administrators, such as “ISP DHCP server list” and then click the “Add” button and choose “Computer” from the drop down menu. At this point you should call your ISP and get the IP addresses of their DHCP servers. For every IP address, repeat this process. In the “New Computer Rule Element” dialog box from the previous step, enter a name that is recognizable and then enter in the IP address of the DHCP server followed by the “OK” button.



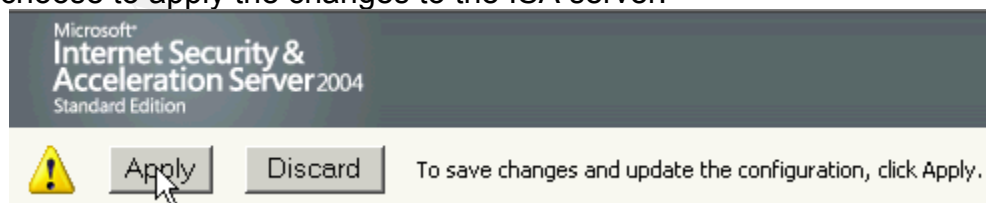
When all the server addresses are entered, click “OK”,



select the “Computer Set” you just created, and then click add and close.



At this point you can click “OK” at the bottom of the “System Policy Editor”, and then choose to apply the changes to the ISA server.



Once the changes are applied, you can return to the command prompt and type `ipconfig /renew` and the server will receive a DHCP assigned IP address.

If your ISP is unreachable, or if the addresses they provide you with do not allow for a successful completion of the above step, you can return to the “System Policy Editor” and add the “External” network to the list of sources that your server will receive DHCP from.



It is not recommended that you leave your server configured in this manner, however you can do this as a troubleshooting step. Once this has been applied, return to the command prompt and repeat the `ipconfig /renew` command. Once your server has successfully received its address, type `ipconfig /all` and note the IP address of the DHCP server. Insure that this address is one that you have listed in your “ISP DHCP server list” object.

Additionally, in some cases, such as firewalls using Windows 2000 Server instead of Windows 2003, it may be necessary to turn off Automatic Private IP Addressing (APIPA). “With APIPA, DHCP clients can automatically self-configure an IP address and subnet mask when a DHCP server isn’t available. When a DHCP client boots up, it first looks for a DHCP server in order to obtain an IP address and subnet mask. If the client is unable to find the information, it uses APIPA to automatically configure itself with an IP address from a range that has been reserved especially for Microsoft.”³⁰ If after the above configuration has been done and the interface card facing the internet is showing an IP address in the range of 169.254.0.1 – 169.254.255.254, disabling of APIPA will be needed. “To disable APIPA, you need to create a key in the Windows registry at, `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\[your_adapter's_MAC_address]`. Create the Value **IPAutoconfigurationEnabled** and set it to 0x0.”³¹

Some service providers may require the use of Point-to-Point over Ethernet (PPoE) connections (see the documentation that came with the modem to find out if this is required). If this is the case with your ISP, see

³⁰ “APIPA”. webopedia.com. 18 September 2003. 7 March 2005.
<<http://www.webopedia.com/TERM/A/APIPA.html>>

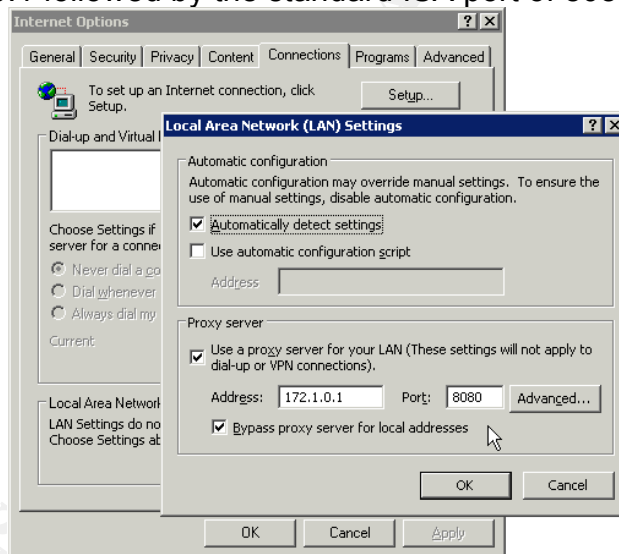
³¹ Alencar, Alexandre C. “How to Set up an ISA Server with a Cable Modem Connection.” [ISAserver.org](http://www.isaserver.org). 19 July 2004. 27 February 2005.
<http://www.isaserver.org/tutorials/How_to_Set_up_an_ISA_Server_with_a_Cable_Modem_Connection.html>

Microsoft's article "How to configure a PPOE connection in ISA Server 2004"³².

3.4.3 Checking for Internet Connectivity

Generally, if you want a client to connect to the internet through the ISA server, or any other network for that matter, you must create a rule to do so. However, as part of the default System Policy on the ISA server, the local system (the ISA server itself) can connect to *.microsoft.com, *.windows.com, and *.windowsupdate.com with no rule changes / additions to the Firewall Policy. In order to connect to those web sites though, one change needs to be made to your browser so that it will connect to the internet using ISA.

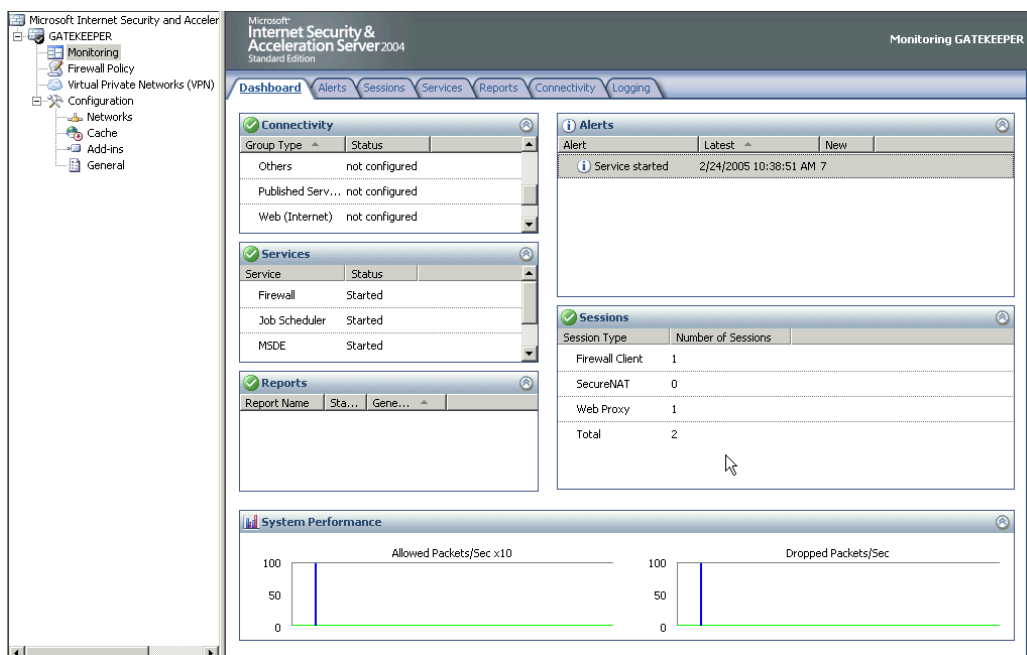
To configure this setting in Microsoft Internet Explorer (IE), open IE and click on the "Tools" link on the main menu bar and choose "Internet Options". From here select the "Connections" tab and then click the "LAN Settings..." button from the bottom. In the "Local Area Network (LAN) Settings" dialog box, but a check in the "Use a proxy server..." box and also in the "Bypass proxy..." box and fill in the address of the internal interface card on your ISA server. This will be the same configuration you use on all your internal clients to allow them to connect through your ISA server. For the test network in this paper, this address is 172.1.0.1 followed by the standard ISA port of 8080.



Following entering the appropriate numbers, simply click "OK" and "OK", close IE and then reopen it again. At this point you will be able to browse to www.microsoft.com and confirm your configuration.

If at any point the ISA server stops providing a service you have configured it for, consulting the "Dashboard" is an excellent place to start your troubleshooting efforts. The "Dashboard" is located in the ISA management console by clicking the "Monitoring" link on the left hand pane, and then selecting the "Dashboard" tab from the right hand pane.

³² <http://support.microsoft.com/?scid=kb;en-us;837830>



The “Alerts” section of the “Dashboard” will notify the administrator of any misconfigured rule, critical system and server information, and all other alerts configured for the server. This function is surprisingly valuable, and does an excellent job at pointing out problem areas in the server **and** giving advice as to how to fix the problem. As an ISA administrator, this “Dashboard” area is something to become very familiar with.

3.4.4 Configuring ISA for a VPN and to allow for RADIUS pass-through

In previous versions of ISA server, configuring a reliable VPN was a major headache and not very intuitive at all. For the ISA 2004 edition, Microsoft has heard the administrator’s cries, and answered with a wonderful set of well thought out dialogs and wizards that make this portion of the configuration a snap.

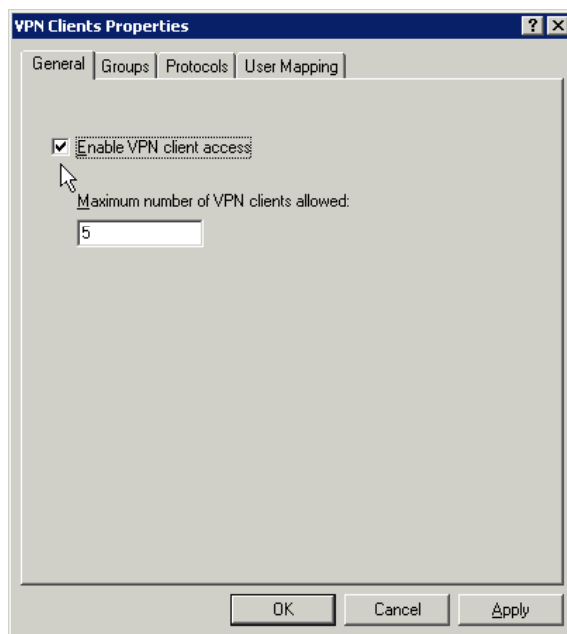
To begin, open the ISA management console and select the “Virtual Private Networks (VPN)” link from the left hand pane and click the “VPN Clients” tab. Start by clicking the “Verify that VPN Client Access is Enabled” link.



Verify that VPN Client Access is Enabled

Allow remote clients to connect to the network using a VPN connection.

Inside the “VPN Clients Properties” dialog box, start on the “General” tab and put a check in the box next to “Enable VPN client access” and set the maximum number of clients allowed. The default here is 5.

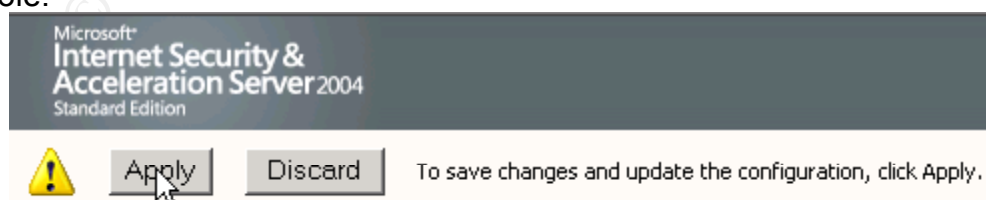


The groups tab is for configuring which domain groups have VPN access and is used to further enforce your domain settings, however since we are going to be using a RADIUS server to handle all this for us, this tab can be ignored. On the protocols tab, we want to only use the most secure connection protocols possible, so uncheck the “Enable PPTP” box and select the “Enable L2TP/IPSec” to allow only L2TP/IPSec tunneling. For those administrators who have special clients who can only use PPTP, this option is obviously available, however keep in mind that a L2TP/IPSec VPN client can be downloaded and installed from Microsoft³³ that will allow the 9x and NT4 family of operating systems to be compatible.

The differences between these two protocols is outside of the scope of this paper, however Microsoft provides very detailed information on each which on their website³⁴.

The next tab is the “User Mapping” tab, and is used for mapping non-Windows clients to a Windows namespace. If you have Linux VPN clients, this setting may be required, however for the purpose of this paper, no non-Windows clients will be discussed, and this tab can be ignored.

Following these configurations click “Apply” and then “OK” and then apply the changes to the server by clicking “Apply” at the top of the management console.



Next in the configuration, click the “RADIUS Server” link from within the

³³ <http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp>

³⁴ http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_VPN_und07.asp

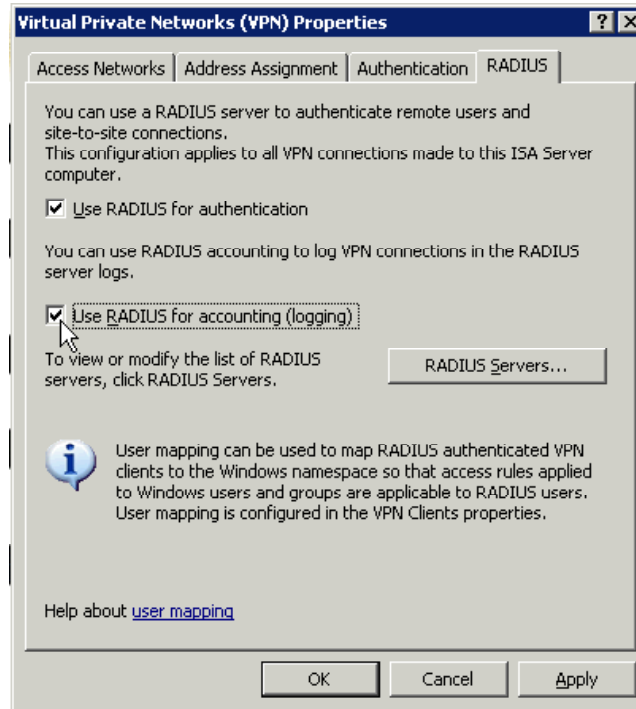
right pane of the administrator console to configure the RADIUS server settings.



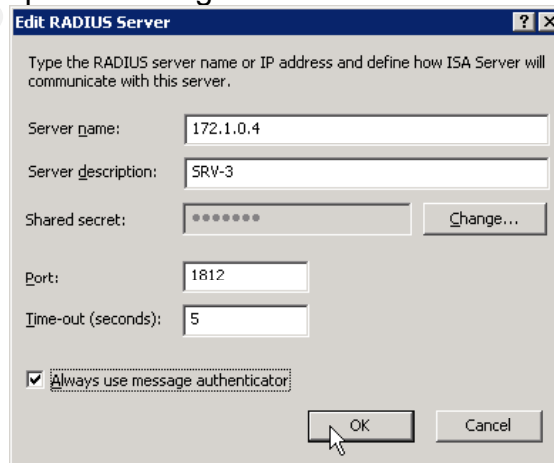
Specify Windows Users or select a RADIUS Server

Specify the Windows users (domain groups) allowed VPN access or, if using RADIUS authentication, select the RADIUS authentication server.

For our purposes, we want to use RADIUS for both authentication and accounting, so put a check in the box next to both of those choices.



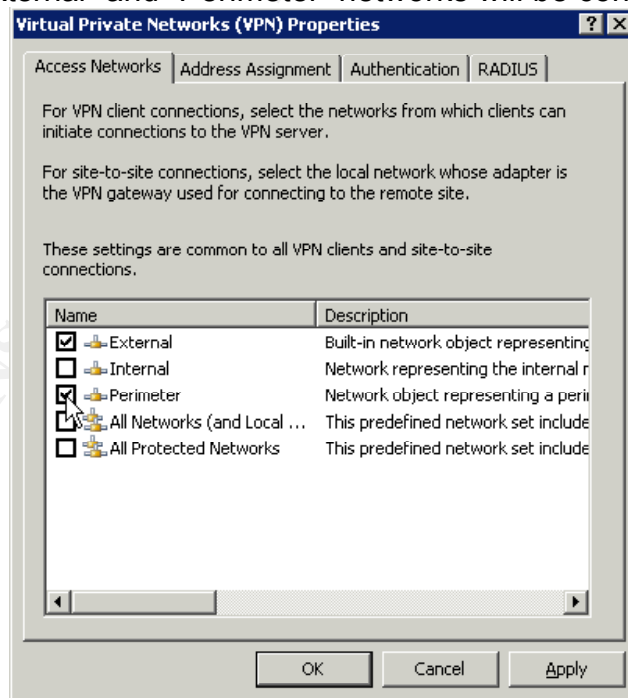
Following those selections, click the “RADIUS Servers” button to specify the RADIUS server(s) on your network. In the “RADIUS Servers” dialog box, click the add button and fill in the appropriate information. The RADIUS server on this domain is 172.1.0.4 and the shared secret is *this is my shared secret*. Also, put a check in the box next to “Always use message authenticator” (This feature is described further in the 3.3.2 *IAS Configuration* section of this paper.). All the other values can be left at their default values unless you have configured your RADIUS server with special settings.



After those values have been entered, click “OK” and “OK”, and then click

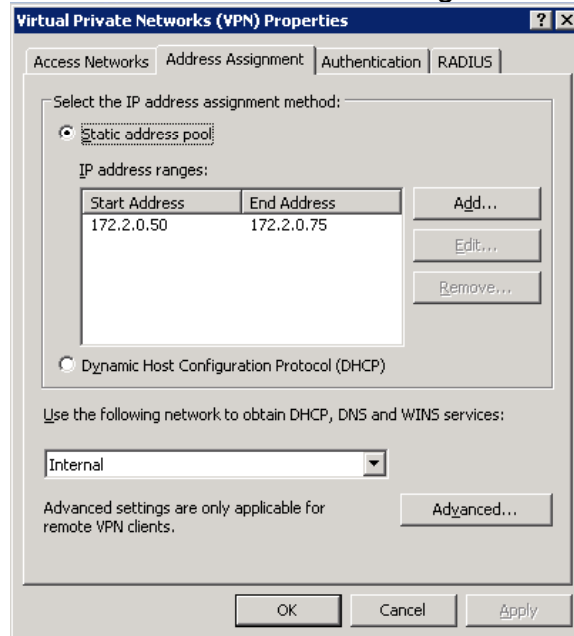
“Apply”. Following clicking “Apply”, the administrator will be prompted with a warning saying that in order for those settings to take place, RRAS needs to be restarted and doing so will disconnect any currently connected VPN clients. Since we currently have no VPN clients configured, this is not an issue and “OK” is to be clicked.

Next, select the “Access Networks” tab to choose which networks will be allowed to connect to the VPN server. At this point, a bit of discussion is required. If you have wireless clients who will only be connecting when they are inside your wireless local area network (WLAN), then you can simply choose “Perimeter” and uncheck “External”. Doing this will limit the VPN connections to the wireless perimeter interface card on your ISA server, and will keep people on the internet side from being able to connect. However, if your clients regularly travel and connect to wireless networks outside of your WLAN, in hotels or coffee shops for instance, you may consider leaving the “External” network selected. What you can accomplish by doing this, is ensure that your wireless clients are always protected, even if they are connected to unsecured wireless networks such as common in hotels and other “open” networks. As discussed before, regardless of whether WPA is enabled or if no encryption is enabled, your wireless clients are still protected by the strong encryption of IPSec through the VPN tunnel back to your office network *and* if DNS and the wireless clients are configured as outlined else where in this paper, the user will be unaware of the difference between when they are connected at work, or when they are sitting on the beach in Tahiti! So these options can be fully explored, both “External” and “Perimeter” networks will be configured.



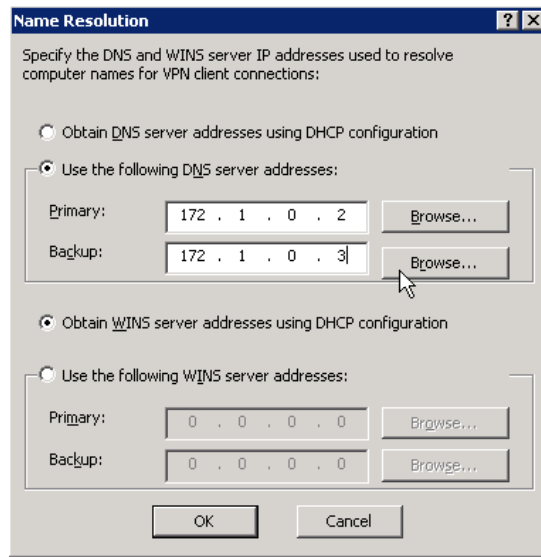
Following the selection of the networks you wish to use, select the Address Assignment tab. For the purpose of the testnet.msft domain, we will configure an address pool on the ISA server itself. This can actually be done on a DHCP

server already implemented on the network, however you would need to create a super scope that hands out addresses for both your main network, and also address for the VPN network as the ISA server handles the two as different networks. I find it to be easier to simply have all the VPN configurations on one server, including the address pool, and then let the internal DHCP server worry about only the internal network clients. To do this, click the radio button next to “Static address pool” and then click “Add...”. Enter the address range that you wish to have for the VPN network; this will need to be a subnet that is not used by the ISA server on any of its network interface cards³⁵. For the testnet.msft network, this range will be 172.2.0.50 – 172.2.0.75. After the address range is entered, click “OK”.

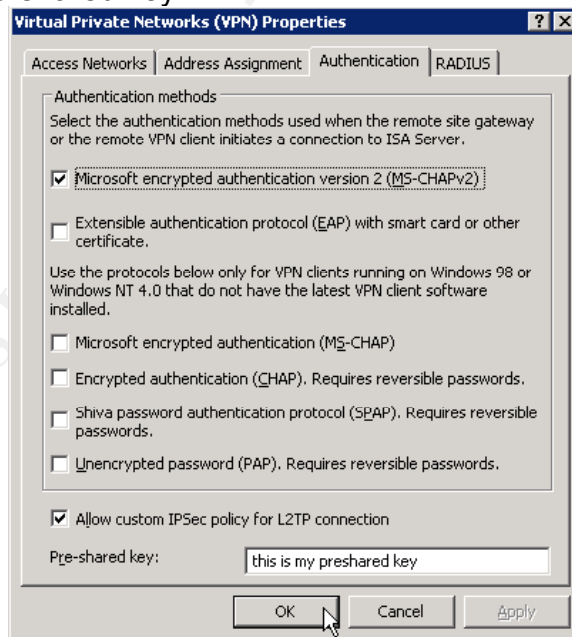


Next, configure the internal DNS servers that the VPN clients will use by clicking the advanced button and adding the appropriate values, and then click “OK”, and “Apply”.

³⁵ For information on subnets and subnetting, see Learn To Subnet.com, www.learntosubnet.com



After configuring the appropriate settings, choose the “Authentication” tab to configure the different authentication methods. For the testnet.msft network, MS-CHAPv2, and the IPsec Pre-shared key are all that will be used, however depending on your networks needs and configuration, you may want to consider alternate authentication methods. For a discussion of these different methods, see Microsoft’s page concerning this topic³⁶. After putting a check in the box beside “Microsoft encrypted authentication version 2 (MS-CHAPv2)”, also put a check in the box next to “Allow custom IPsec Policy for L2TP connection” and enter in a strong pre-shared key.



To finish, click “Apply” and “OK” and then apply the changes to the server by clicking the “Apply” button at the top of the management console window.

Section three of the VPN configuration page has actually already been

³⁶http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_ias_protocols.asp

completed through the process of the steps outlined above, so these links can be skipped.



Verify VPN Properties and Remote Access Configuration

Verify that VPN properties, such as protocols and access points, are defined according to your network requirements.

3.4.5 Configuring the ISA rules for the desired access levels

This particular section will require a lot of planning on the part of most administrators. Charting out what protocols and hosts should be accessible to VPN clients, especially if they are connecting from the internet side of your firewall, deserves some thought. For those administrators, who wish to simply grant internet access to the wireless users, this step will be quite simple. Unfortunately this will most likely not be the standard configuration for a vast majority of administrators out there. Most will have users who will need to function on the network wirelessly, just as if they were logged into a wired workstation on the LAN. While some will argue that the authentication process traversed to reach this point is far greater than that of someone who is simply sitting at a wired workstation, and therefore lax policies are acceptable, I would argue that these administrators are a stolen laptop away from having most of these security measures mitigated. Once a laptop, which has been properly configured to seamlessly integrate with this type of network falls into the wrong hands, password auditing is really all that stands between the attacker and your network, just as it would if they were sitting at a wired workstation in your office. In the interest of space, I will show a handful of such configurations that will demonstrate the basic principles and techniques involved and in doing so, empower administrators to adapt this to their particular company security policies.

To begin configuring the policies, click “View Firewall Policy for the VPN Clients Network” link.



View Firewall Policy for the VPN Clients Network

Verify that Firewall Policy rules for the **VPN Clients Network** are defined in accordance with your network and corporate security requirements.

Subsequently, and for future reference, this same screen can be reached by clicking the “Firewall Policy” link from the left hand pane in the ISA management console window.

The first policy we will explore is one that will allow our internal DNS forwarder to function properly, and ultimately will be required for our wireless clients to surf the internet, which will be the next rule we look at. “A forwarder is a Domain Name System (DNS) server on a network used to forward DNS queries for external DNS names to DNS servers outside of that network.”³⁷ “To use forwarders to manage the DNS traffic between your network and the Internet, configure the firewall used by your network to allow only one DNS server to communicate with the Internet. When you have configured the other DNS servers in your network to forward queries they cannot resolve locally to

³⁷ “Understanding forwarders”. Microsoft Windows Server System. 28 February 2005.

<http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_DNS_und_Forwarders.asp>.

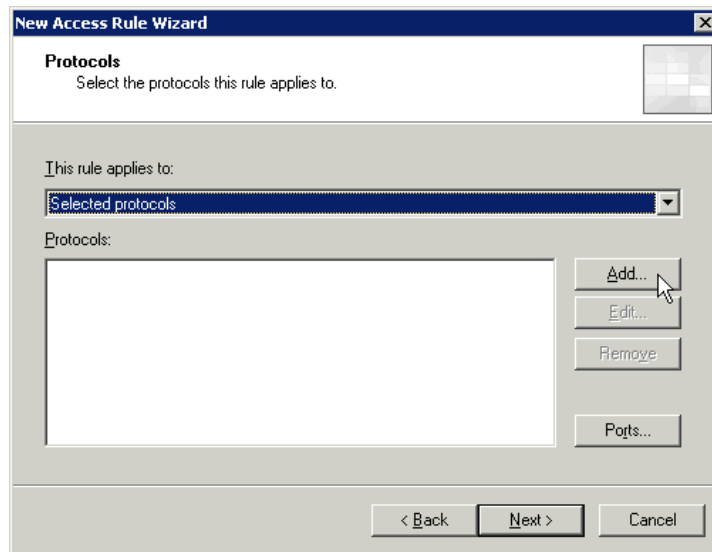
that DNS server it will act as your forwarder.”³⁸ This is accomplished by right mouse clicking the “Firewall Policy” link, and selecting “New” and then “Access Rule...”.

To begin, right mouse click on the “Firewall Policy” link on the left hand side and choose “New” and then “Access Rule”. The next step in the process will require a bit of decision making. Since this is the first rule we have configured, now is a good time to decide on a naming convention. It is my personal opinion that it is easier to create rules for computers / networks and then configure the rules for the protocols desired for those computers / networks. Some administrators may find it easier to manage by creating rules for specific protocols and then adding the computers / networks that have access to those protocols. In any case, I find that naming the rule based on who or what it serves and where that traffic is going to be the easiest way to label them. For example, this first rule will be for a DNS forwarder, which in the case of the testnet.msft domain, the DNS server is named SRV-2, and the traffic will be flowing from the server to the internet. With this in mind, the rule will be named *SRV-2 > Internet*. Using this line of thought, any other protocol SRV-2 is allowed to send to the internet will be added to this rule later. For administrators who think better in terms of services, something like *DNS forwarder > Internet* would work great. The important thing, I believe, is to establish a system that is easy to remember and recognize, and then stick to it. For the purpose of this paper, rules will be created using the *computer / network > traffic destination* naming convention.

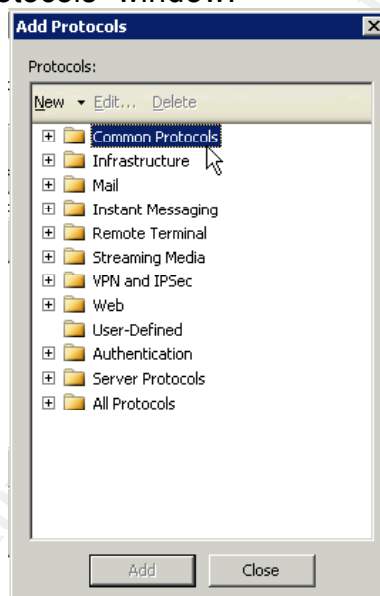
Once you have established your naming convention, enter the name for the rule and then click “Next”. The next screen determines the rule action. In our case, we are creating a rule to allow for access, so select “Allow”, and then click next. Following this, we now will select the appropriate protocol for the rule. To do this, use the drop down menu and click on “Selected protocols” and then click “Add...” from the right.

³⁸ “Using forwarders”. Microsoft Windows Server System. 28 February 2005.

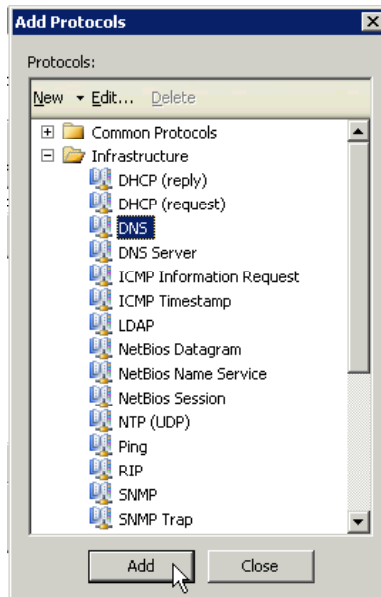
<http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_DNS_imp_UsingConditionalForwarders.asp>.



This will open the “Add Protocols” window.

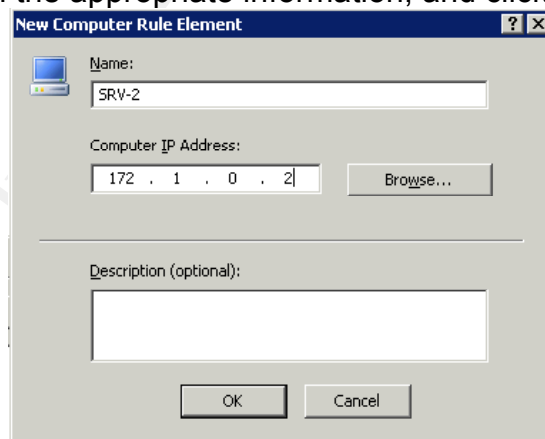


This particular window is one that administrators should familiarize themselves with. The protocols are all organized in easy to recognize folders by their function and some are overlapping. DNS, for example, is an “Infrastructure” protocol, but can be found in the “Common Protocols”, “Infrastructure”, and “All Protocols” containers. To select DNS, expand the “Infrastructure” container and select “DNS” and then click “Add”.



Since SRV-2 will not be hosting DNS records for internet users to query, it is not necessary to add "DNS Server". There are several other protocols available in which there are both an application protocol and an application server protocol. Take care to select the correct protocol when creating the rules. Ask yourself, am I creating this rule to provide a service, or to connect to a service. Generally speaking, "Access Rules" will use the application protocols, while "Publishing Rules" will use the application server protocols.

After the DNS protocol has been added, click "Close" to close the "Add Protocol" window, and then click "Next". The next screen asks us who the traffic for this rule will come from, to add SRV-2, click "Add" and select "New" and "Computer" and fill in the appropriate information, and click "OK"

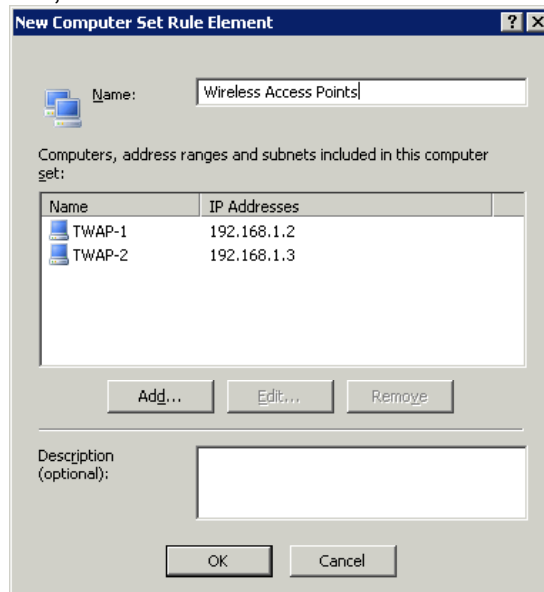


This process will then add that server to our toolbox, and it can be used again as needed. This process will eventually need to be repeated for each computer / network that will have a rule made involving it.

After clicking "OK", expand the "Computers" container and double click the SRV-2 object we just created, and then click "Next" from the "Access Rules Sources" page. Now we need to define where the traffic is going, which is done with the same process as before, click "Add", and this time just expand the

“Networks” container and double click “External”, click “Close”, and then “Next”. The next screen allows you to restrict the users who are authorized to use this rule from the client machine. For the purpose of this rule, the “All Users” group is fine, so simply click “Next”, “Finish”, and then “Apply”. Now the internal DNS server will be able to forward DNS requests to the internet.

A rule will also need to be created allowing the wireless access points to send their RADIUS traffic to the RADIUS server itself. To do this, create a rule for RADIUS and RADIUS accounting, and instead of adding each wireless access point individually, administrators can add them as a group. Instead of choosing “Computer” from the “New Rule Element” drop down menu, choose “Computer Set”, name it, and then add all the wireless access points to it.



To allow the VPN users to connect to the internet, two rules will need to be created, one rule that allows the VPN users to access the DNS server on the internal network, and a second rule that allows the VPN users to access HTTP, and HTTPS on the internet. Using the same process as outlined above, these rules are simple to create. ISA server even created a “VPN Clients” object for us inside the “Networks” container to further simplify the creation of those rules.

The previous rules allowed us to give access to a computer or network for the purpose of using a specific protocol. The next set of rules, are rules that allow the firewall to act as a proxy for that service, making it appear that the firewall is the one actually hosting the service. We will utilize this function to publish an internal DNS server to the wireless perimeter so that our VPN clients can resolve the name of the VPN server they are attaching to. As mentioned earlier, this will allow us to simplify the client configuration and allow that client to connect regardless of which arm of the network they are attaching from. This type of rule is also the type of rule used to publish a web server or mail server.

To create this rule, right mouse click again on the “Firewall Policy” link on the left and choose “New” and then “Server Publishing Rule”. Name the rule according to the naming convention earlier, however keep in mind that for publishing rules, only one protocol can be published per rule. Following adding

the name, click “Next”. The next screen requests the server IP address, and in the case of the testnet.msft domain, it is 172.1.0.2, configure that and then click “Next”. Select the protocol from the drop down menu, and as mentioned previously, we are publishing a service, so DNS Server should be chosen (conveniently Microsoft limited the choices on this drop down box to the services objects), and then click “Next”. Since we are only interested in publishing this service to our wireless users, select the “Perimeter” network from the list of networks to listen on, and then click “Next”, “Finish”, and “Apply”. Now, wireless users who have authenticated to the access points, but have yet to connect to the VPN will be able to make DNS requests to the internal network. As a note, administrators may want to consider creating a stand along DNS server for the sole purpose of hosting this one record. Since the wireless perimeter is potentially a hostile network, this DNS server should in actuality be treated the same as the DNS server that hosts the external namespace for the organization. For simplicities sake, and in the interest of space, this is not employed on the testnet.msft domain, however it would be strongly encouraged for actual deployments.

On the DNS server, a host record will need to be created for wireless.testnet.msft which resolves to the wireless perimeter facing network interface card of the ISA server, which in the case of the testnet.msft domain, will be 192.168.1.1. For administrators who are also configuring VPN access for the external network, they will want to also have a host record created on their external DNS name space for wireless.testnet.msft that points to the internet facing network interface card of their ISA server. This will allow, as suggested before, for one configuration to be made on the client, and it will work, regardless of where the client is.

With these rules having been created, administrators should have a good feel as to how the process works. By repeating the steps outlined above, administrators can adapt these techniques to provide for whatever services their wireless clients need access to. For more ideas on rules and ways this server can be utilized, see [ISAserver.org](http://www.isaserver.org)³⁹. This is truly and excellent resource, as Thomas Shinder and his team are very thorough in their explanations and responses to questions.

3.5 Configuring the Wireless Access Points

It has been my experience that configuring access points is similar between the different models and manufacturers, however it is important to remember for this section of the install guide, that access points other than those outlined here will most definitely be different. Use this section of the guide as a means to get an idea of how the setup is configured, and then consult your hardware installation / configuration documentation for the exact methods used for the specific units in question. Also keep in mind that different revisions of the firmware installed on the access points may also differ in their configuration and available options; consult with your manufacturer for the latest available firmware updates. As much information as possible will be provided

³⁹ <http://www.isaserver.org>

for each access point represented here, so that the results can be duplicated for those who have the same hardware deployed on their networks.

Additionally, if you are considering buying new hardware, be sure to consult the manufacturers' website to determine the AP that is right for the network you are designing. Without question, the access points should support WPA if not the full 802.11i standard, which as of this writing will provide the best level of security currently available. Also, bargain hunters may benefit from buying slightly older models that can be upgraded to support WPA, however use caution as most manufacturers will release different revisions of the same model number, some of which may not support the upgrade you are planning on. Again, consult with the manufacturer before making your purchase.

3.5.1 Configuring a Linksys Access Point

The following is the access point used in this section of the paper:

TWAP-1	
Manufacturer	Linksys
Model Number	WRT54G ver. 2
Firmware Version	V3.03.6
IP Address(es)	192.168.1.11

Before beginning the configuration portion of the install, it is important to point out that doing the initial install of the access point is easier done attached to a workstation instead of the ISA server. This will help rule out any problems encountered as being firewall rule related and will minimize random rule creation such is common during moments of frustration with an ISA server. Once the initial configuration is set, plug the access point in to the network interface card designated on the ISA server for the wireless perimeter network and ensure that the end attached to the access point is plugged into a LAN port and not the WAN port. This particular model of access point can also function as a broadband router, which is what the WAN port is intended to service, however for the purpose of this installation, this functionality will not be needed. It could be argued that the WAN port be utilized as means of adding extra protection for the wireless network, however it is my opinion that the level of protection offered by this solution is minimal compared to the amount of extra configuration required to gain it. The use of a wireless router instead of just an access point is indicative of networks that have hardware currently in place that is being redeployed to meet the configuration scenario represented here.

To begin the configuration process, follow the manufacturer's setup procedures for the initial install. Once the initial setup is complete, login to the access point and click on the "Administration" tab. Change the router password to a secure password which can be a maximum 32 characters, but unfortunately cannot include any spaces⁴⁰. Also, change the web access from HTTP to HTTPS by unchecking the box next to HTTP and putting a check in the box next

⁴⁰ "Help: Management" 7 March 2005 <<http://192.168.1.1/help/HManagement.asp>>

to HTTPS, and disable Wireless Access Web by selecting the “Disable” radio button.

LINKSYS
A Division of Cisco Systems, Inc. Firmware Version: v3.03.6

Wireless-G Broadband Router WRT54G

Administration

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Management | Log | Diagnostics | Factory Defaults | Firmware Upgrade | Config Management

Router Password

Local Router Access

Router Password: [password field]
Re-enter to confirm: [password field]

Web Access

Access Server: ☐ HTTP ☒ HTTPS
Wireless Access Web: ☐ Enable ☒ Disable

Remote Router Access

Remote Management: ☐ Enable ☒ Disable
Management Port: 8080
Use https: ☐

UPnP

UPnP: ☐ Enable ☒ Disable

Local Router Access: You can change the Router's password from here. Enter a new Router password and then type it again in the Re-enter to confirm field to confirm.

Web Access: Allows you to configure access options to the router's web utility. **More...**

Remote Router Access: Allows you to access your router remotely. Choose the port you would like to use. You must change the password to the router if it is still using its default password.

UPnP: Used by certain programs to automatically open ports for communication. **More...**

Save Settings Cancel Changes

CISCO SYSTEMS

This will ensure the use of a strong password over an SSL connection and will also keep the wireless users from being able to manage the access point. Select “Save Settings” to commit the changes and then add the certificate for the access point when prompted and login again. Now you will notice that the session is secured using SSL and any further communications will be protected.

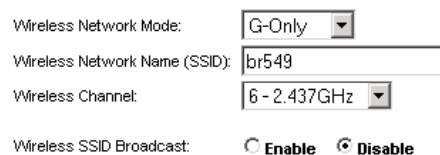
Next, select the “Wireless” tab and click the “Basic Wireless Settings” link. First choose the Wireless Network Mode from the list of Mixed Mode, B-only, or G-only. For the testnet.msft network, the only clients that will be connecting are G compatible, so G-only will be selected. Administrators will want to look at the clients who will be connecting to the access point and make their decision based on those clients. In mixed mode, both B and G mode clients will be able to connect, but remember that the connection speed will be slowed to the lowest common denominator. If there are 10 G clients and 1 B client, all 11 will communicate at B speeds. For more detailed information on wireless B and G networks and on the 802.11 standards, see IEEE’s documentation which can be found on their website⁴¹.

After deciding the network mode, assign your wireless network a service set identifier (SSID) name. This SSID is nothing more than, as the name implies, an identifier, much the same way that workgroup names define

⁴¹<http://standards.ieee.org/getieee802/802.11.html>

workgroups. For most networks, using the same SSID throughout the organization is acceptable, and since RADIUS will be used to define who has access, there is no need to define unique SSID and encryption keys as a means of allowing access to the network as has been used by administrators in the past. Additionally, this SSID should not be anything private, as it is easily discoverable by wireless sniffing tools, even with the SSID broadcast function turned off. I recommend using an SSID that is easily recognizable to administrators, however may be obscure to the public and outside of the normal naming convention for the organization. While this attempt at “security through obscurity” may ultimately provide little defense, in areas of dense wireless activity, it may at least keep your access points from standing out to potential attackers.

Following setting the SSID, configure the Wireless SSID Broadcast to “Disable” (the wireless channel, which was skipped, can be left at the default setting). While I did mention that the SSID can be discovered even while the SSID broadcast is turned off, and I do believe that security through obscurity rarely works, it is still considered a best practice to disable this function. After making these selections, click “Save Settings”, and then “Continue” from the screen that pops up.

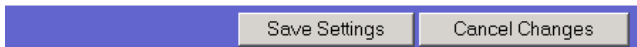


Wireless Network Mode: G-Only

Wireless Network Name (SSID): br549

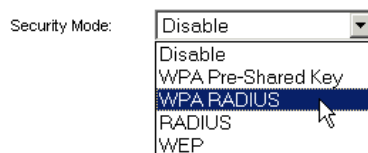
Wireless Channel: 6 - 2.437GHz

Wireless SSID Broadcast: ☐ Enable ☒ Disable



Save Settings Cancel Changes

The next step is to define the wireless security mode. Click the “Wireless Security” link and then use the drop down menu and select “WPA RADIUS”.



Security Mode: Disable

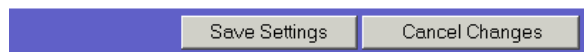
Disable

WPA Pre-Shared Key

WPA RADIUS

RADIUS

WEP

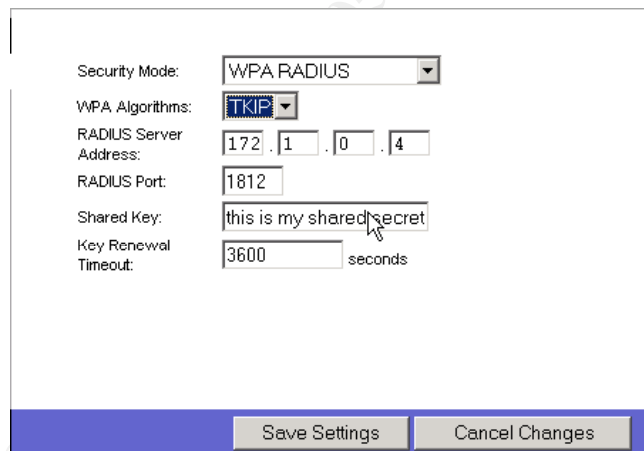


Save Settings Cancel Changes

Selecting WPA RADIUS will then allow for entering in the appropriate RADIUS server information. The first option is which WPA Algorithm to use; either TKIP or AES. While TKIP is not actually an algorithm, it is a key management protocol; the important thing to note is that AES is part of the new WPA2 standard, and is not backward compatible to devices that only support WPA. “WPA2 is based upon the Institute for Electrical and Electronics Engineers’ (IEEE) 802.11i amendment to the 802.11 standard, which was ratified on July 29, 2004. The primary difference between WPA and WPA2 is that WPA2 uses a more advanced encryption technique called AES (Advanced Encryption Standard), allowing for compliance with FIPS140-2 government security

requirements.”⁴² TKIP, however, will most likely be around for a while to provide backward compatibility to these older devices. It is important to take into account all of the access points on the network, and what they support, as this will determine whether you will use AES or TKIP. By configuring all the access points identically, users who have access rights through RADIUS to roam, will be able to move about between these access points with relative seamless connection⁴³; while reducing the administrative burden of configuring the clients and access points. While the XP client that comes with Service Pack 2 supports AES, one of the access points used on the network does not, so all access points on the testnet.msft network will be configured for TKIP. As of this writing however, the Wi-Fi Alliance maintains that “WPA remain(s) technically sound and secure”⁴⁴, so no need to worry unless you must be in compliance with FIPS140-2. If all of the access points and clients will support AES, simply choose AES here and in the client configuration as well. For more information on the differences between the two, see David Halasz’s article entitled “IEEE 802.11i and wireless security”.⁴⁵

Next, enter in the appropriate information into the remaining fields. As per the configuration of the testnet.msft network, the RADIUS server address is 172.1.0.4, the RADIUS port is the default 1812, the Shared Key is *this is my shared secret*, and the Key Renewal Timeout can be left at the default value of 3600.



The screenshot shows a configuration window for WPA security. The 'Security Mode' is set to 'WPA RADIUS'. The 'WPA Algorithms' dropdown is set to 'TKIP'. The 'RADIUS Server Address' is entered as '172.1.0.4'. The 'RADIUS Port' is '1812'. The 'Shared Key' is 'this is my shared secret'. The 'Key Renewal Timeout' is '3600 seconds'. At the bottom, there are 'Save Settings' and 'Cancel Changes' buttons.

Following these changes, select “Save Settings” and then click “Continue” from the next screen.

⁴² “Wi-Fi Alliance press release: Wi-Fi Alliance Introduces Next Generation of Wi-Fi ® Security”. Wi-Fi Alliance. 1 September 2004. 15 March 2005. < <http://www.wi-fi.org/OpenSection/ReleaseDisplay.asp?TID=4&ItemID=181&StrYear=2004&strmonth=9>>.

⁴³ This statement assumes the access points are arranged in the building in a manner that provides overlapping cells of coverage. Discussion on the placement of access points is outside of the scope of this paper, however for more information on this topic see the *TechRepublic* article entitled “Get IT Done: How to place your wireless access point” located here, <http://techrepublic.com.com/5100-6264-5035244.html#>.

⁴⁴ “Wi-Fi Alliance press release: Wi-Fi Alliance Introduces Next Generation of Wi-Fi ® Security”. Wi-Fi Alliance. 1 September 2004. 15 March 2005. < <http://www.wi-fi.org/OpenSection/ReleaseDisplay.asp?TID=4&ItemID=181&StrYear=2004&strmonth=9>>.

⁴⁵ <http://www.embedded.com/showArticle.jhtml?articleID=34400002>.

Additionally, since this particular unit is a router and considers itself the gateway, we need to add a route its routing table so that it knows where 172.1.0.4 actually is. To do this, click the “Setup” link followed by the “Advanced Routing” link. For the operating mode, choose “Router” from the drop down menu, then choose “LAN & Wireless” from the RIP drop down menu. Choose a name for the route, such as “TWAPtoInternal”(the name cannot contain spaces), and then enter the appropriate IP information. For the testnet.msft domain, the destination LAN IP is 172.1.0.0 and the subnet mask is 255.255.0.0, and the default gateway is 192.168.1.1, which is the perimeter facing interface card of the ISA server. Confirm these settings by clicking the “Save Settings” button, followed by clicking the “Continue” button.

Advanced Routing	
Operating Mode	Router
Dynamic Routing	RIP: LAN & Wireless
Static Routing	Select set number: 1 (TWAPtoInternal) Delete This Entry
	Enter Route Name: TWAPtoInternal
	Destination LAN IP: 172.1.0.0
	Subnet Mask: 255.255.0.0
	Default Gateway: 192.168.1.1
Interface: LAN & Wireless	
Show Routing Table	
Save Settings Cancel Changes	

Again, note that this only needs to be done because this particular access point is also a router, had this unit been only an access point, these steps could have been skipped.

Finally, this unit needs to be set up to handle DHCP requests for the wireless users. This is done on the “Setup” tab and under “Basic Setup”. Enable the DHCP by selecting the radio button across from “DHCP Server”, and then enter the starting address followed by the number of clients who will be connecting. For the testnet.msft, those values will be 192.168.1.100 and 50 respectively. Also, configure the DNS server to the address 192.168.1.1, as this is the address of the perimeter facing network interface card of the ISA server that is now publishing the DNS service to the network. Save the configuration by clicking “Save Settings” and then “Continue”.

For the purpose of the testnet.msft network, this is all that needs to be configured on the access point, however I do want to address one last setting that is available, and that is the “Wireless MAC Filter” link. For smaller networks with a small number of clients this option can be a consideration for administrators wishing to add a small amount of additional security. The way that MAC address filtering works is simply allowing or disallowing access based

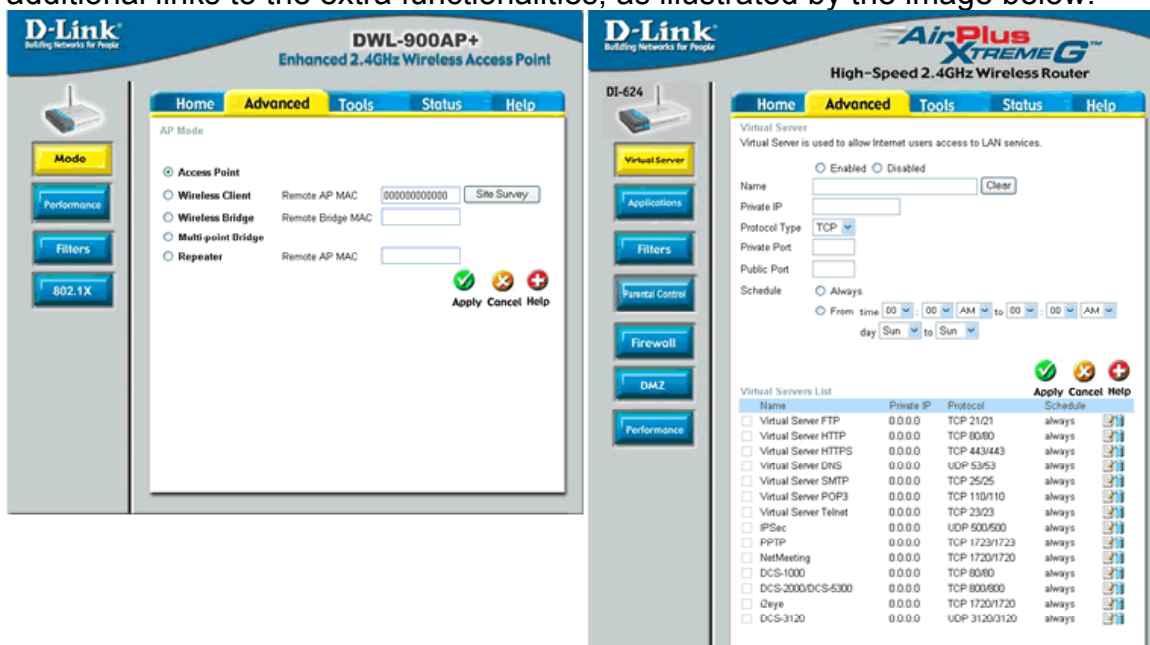
upon the wireless interface card's Media Access Control (MAC) address, which is an address assigned to the card from the manufacturer. However, creating these MAC address lists can be quite laborious for a large number of clients, which will need to be repeated for each access point. This option simply doesn't scale very well. Additionally, MAC addresses can be spoofed by attackers; meaning a malicious user can monitor the wireless traffic and collect a list of MAC addresses that are able to communicate on the network, and then mask the MAC address of their interface card with one that is permitted on the network, thus bypassing this security measure. With this in mind, it simply does not make sense to use this method because of the amount of effort required to configure it versus the amount of effort required to defeat it.

3.5.2 Configuring a D-Link Access Point

The following is the access point used in this section of the paper:

TWAP-2	
Manufacturer	D-Link
Model Number	DI-624 Revision C3
Firmware Version	2.50
IP Address(es)	192.168.1.12

The configuration process for the D-Link is much the same as the Linksys, which is really what this section is designed to show. Again, the model used is a wireless router instead of just an access point, so there is lots of functionality that will not be utilized. Most of the interfaces look the same across vendor platforms; however, as mentioned before, the routers will have additional links to the extra functionalities, as illustrated by the image below:



The image on the left is taken from a D-Link DWL-900AP+, which is just an

access point, and the one on the right is taken from the DI-624 wireless router used on the testnet.msft network. Note that even though the two were manufactured almost 2 years apart, the interface has the same look and feel; the only difference is the links to the added functionality the newer unit provides.

When it comes to configuration, the D-Link unit actually has a convenient wizard that takes administrators through the basic setup process, including changing the admin password. After this initial setup and with the “Home” tab selected, click the “Wireless” link on the left to open the properties sheet for the wireless settings. This is the page where the wireless security settings can be configured.

The screenshot displays the D-Link AirPlus Xtreme G DI-624 High-Speed 2.4GHz Wireless Router configuration interface. The left sidebar contains navigation buttons: Wizard, Wireless (highlighted), WAN, LAN, and DHCP. The main content area is titled 'Wireless Settings' and includes a sub-header 'These are the wireless settings for the AP(Access Point)Portion.' The settings are as follows:

- Wireless Radio: ☒ On ☐ Off
- SSID:
- Channel: ☐ Auto Select
- Super G Mode:
- Extended Range Mode: ☐ Enabled ☒ Disabled
- 802.11g Only Mode: ☒ Enabled ☐ Disabled
- SSID Broadcast: ☐ Enabled ☒ Disabled
- Security: ☐ None ☐ WEP ☒ WPA ☐ WPA-PSK

Below these settings is the '802.1X' section with fields for RADIUS Server 1 IP (172.1.0.4), Port (1812), Shared Secret (masked), RADIUS Server 2 IP (Optional) (0.0.0.0), Port (0), and Shared Secret (empty). At the bottom, there are two footnotes and three buttons: Apply, Cancel, and Help.

*Enabling Extended Range Mode will automatically disable Super G with Static Turbo and SSID Broadcast mode.
*Super G with Dynamic Turbo and Super G with Static Turbo mode only operates in Channel 6.

Note that, while the interface looks different from the Linksys model, all the basic configurations are the same, with a few exceptions. First, administrators will notice that there are extra modes that this unit supports such as Super G mode and Extended Range Mode. These additions are proprietary options and do not work unless you also use a D-Link wireless interface card that is suited for those modes. These types of “extra frills” are common among the different wireless vendors; however they usually are not compatible from vendor to

vendor. For the purpose of the testnet.msft network, these features will not be used, however if the router you are configuring has these options available, refer to the manufacturer's product information for the exact specifications of those features. Secondly, administrators will want to notice that this particular unit does not have an option to choose between AES and TKIP as was available with the Linksys. After conducting a brief experiment with the client, by trying to connect to the access point using AES and then TKIP, it was determined that this model only supports TKIP. It was my assumption that this would be the case, and it is further my assumption that this is the case for all access points with no option to choose between AES and TKIP, however administrators may want to test this theory before throwing access points away because of a need for AES. The easiest way to do this is, set both the AP and the client (configured elsewhere in this paper) to use WPA-PSK and set it to TKIP for the initial connection. If that is successful, change the client to connect using AES. If it connects with no other changes to the access point, then it supports both. If it only connects with one or the other, obviously it will only support the one.

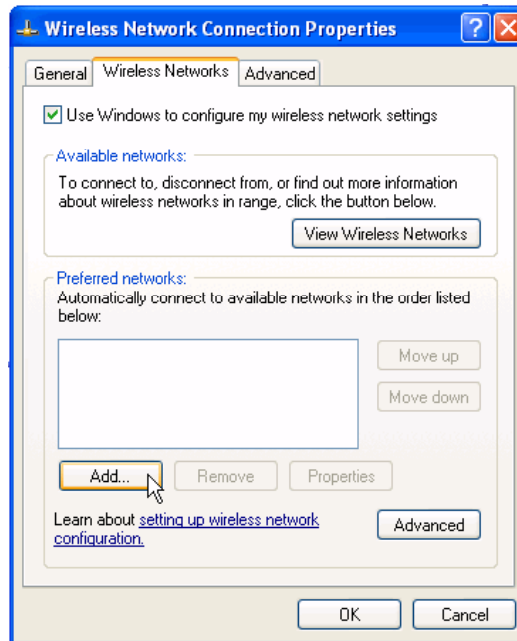
As mentioned earlier, because this particular unit only supports TKIP, all the access points in the testnet.msft network will also need to be configured to use TKIP. Likewise, had this access point only supported WPA-PSK (pre-shared key), all the other access points would need to be configured for WPA-PSK as well, or separate networks would need to be created and roaming would not be as seamless. This is the unfortunate downside to using existing equipment instead of getting all new equipment that is identical, however it is important, I feel, to show this as I believe it to be a scenario representative of what many administrators face.

For the purpose of the testnet.msft network, this is all that will need to be configured on the D-Link Access point.

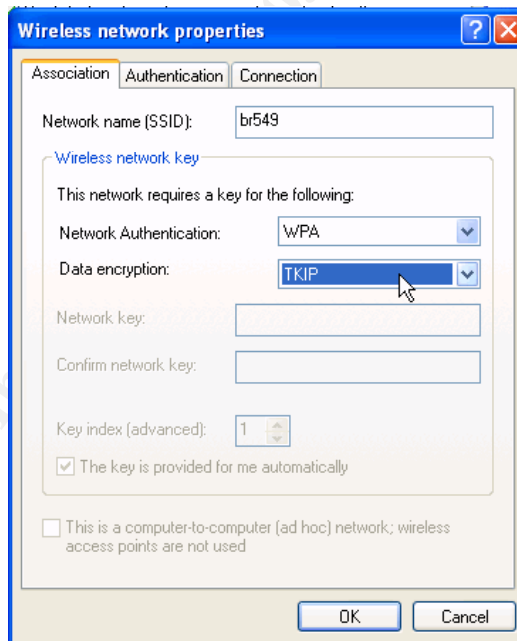
4 Configuring the Windows XP client

4.1 Configuring the wireless settings

To configure the wireless connection settings, go to the control panel and click the link in the upper left that says "Switch to Classic View", and then double click on "Network Connections". Next, right mouse click on the "Wireless Network Connection" icon and choose properties, followed by clicking the "Wireless Networks" tab.



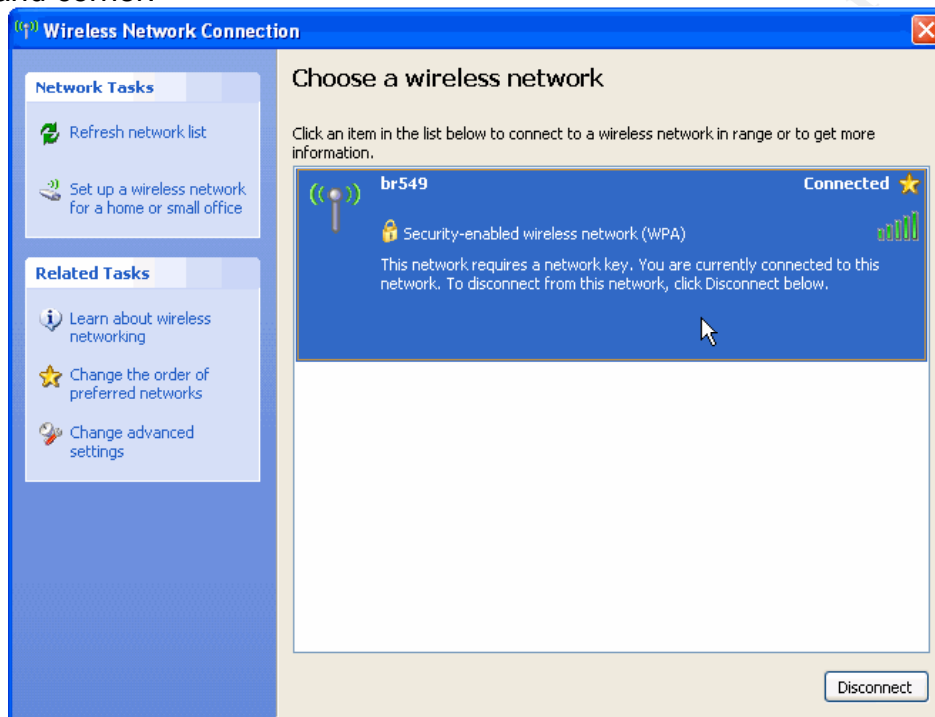
From inside the “Wireless Network Connection Properties” window, click the “Add” button. On the association tab, enter in the SSID as entered on the access points, and then change the “Network Authentication” to “WPA” and the “Data Encryption” to “TKIP”.



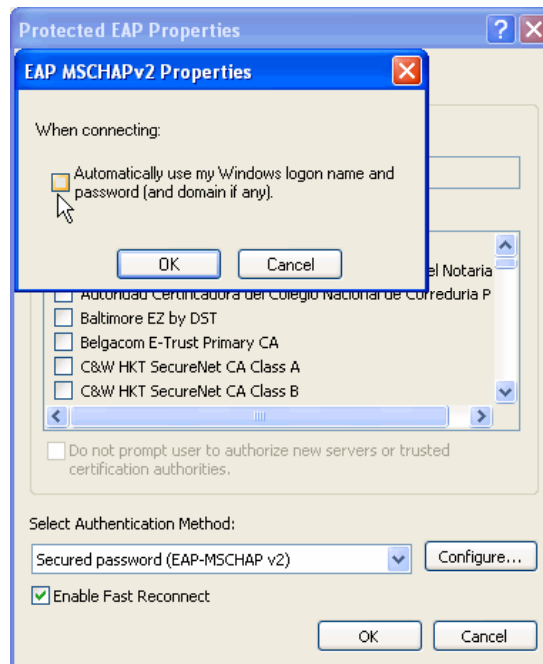
Next, choose the “Authentication” tab and change the EAP type to “Protected EAP (PEAP)”, and then make sure that the two check boxes below that are cleared, followed by clicking the “Properties” button. Once inside the “Protected EAP Properties” dialog box, uncheck the box that says “Validate server certificate”, this is done simply because the client has not been given a certificate from the root CA, and has no rights on the wireless network to verify it. Next, choose “Secured password (EAP-MSCHAP v2)” from the authentication methods drop down box, put a check in the box next to “Enable Fast

Reconnect”, and then click “OK” until you are back to the “Network Connections” window.

Once this is finished, the wireless network should automatically connect, using your Windows domain user credentials for authentication. If it does not connect automatically, right mouse click on the “Wireless Network Connection” and choose “View Available Wireless Networks”, select the wireless network configured from the previous step, and then choose “Connect” from the lower right hand corner.



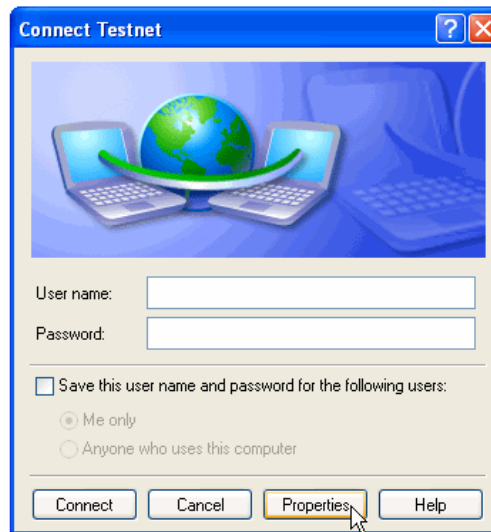
For administrators who manage laptops that are not members of the domain, after choosing the secured password as the authentication method and enabling fast reconnect from the previous step, click the configure button and then clear the box that says “Automatically use my Windows logon name and password (and domain if any)” check box. This will then prompt the user for Windows domain credentials when the wireless connection is first being initiated.



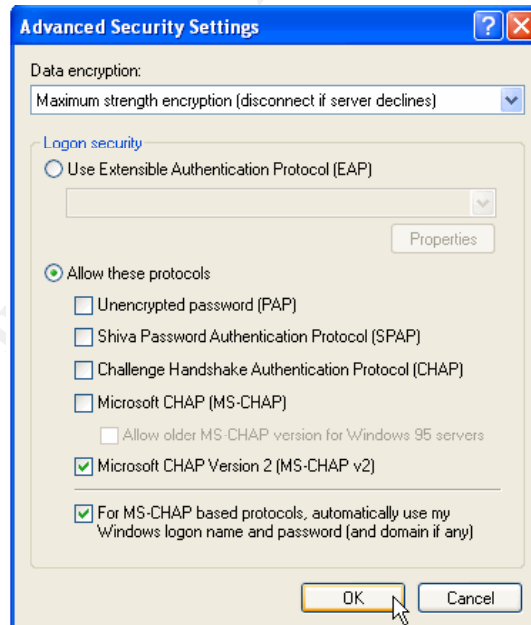
4.2 Configuring the VPN client

The next phase of the solution involves configuring a simple VPN client. This is done from within the “Network Connection” window mentioned in the previous section. Once there, click the “Create a new connection” link from the upper left hand corner, and then click “Next” on the “Welcome to the New Connection Wizard”. From the next screen, choose “Connect to the network at my workplace”, click “Next”, and then choose “Virtual Private Network connection” and click “Next” again at the bottom of the screen. After choosing the VPN network, we need to name the connection. This name can be anything, as it will just be used to represent this particular connection. For the testnet.msft domain, this will simply be named “Testnet”. After naming the connection, click “Next”.

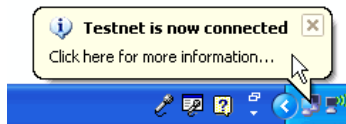
The next screen asks us to select the VPN server to connect to. If you opted to allow connections to the VPN from both the perimeter network, and the external network, and made the appropriate changes to both the ISA server rules and the DNS server that hosts your domain’s external name space, enter the host name configured for the VPN connection. However, if you did not wish to configure those options, simply enter the IP address of the perimeter network facing network adapter card on the ISA server, and then click “Next”, and then complete the wizard by clicking “Finish”. The wizard will then create a connectoid for the Testnet network, and then administrators will be prompted enter in a username and password. From this window, prior to entering in the username and password, click the “Properties” button.



Inside the VPN connection's properties box, select the "Security" tab, and then select the radio button beside "Advanced (custom settings)", and then click the "Settings" button. From the "Data encryption" drop down menu, choose "Maximum strength encryption (disconnect if server declines)" and then ensure that only MS-CHAP v2 is selected from the list of allowed protocols. Additionally, for the laptops that are domain members, put a check in the box to automatically use the Windows logon information, for laptops that are not domain members, leave this blank. After the appropriate settings are configured, click "OK".



Next, click the "IPSec settings..." button, and put a check in the box beside "Use pre-shared key for authentication" and enter the key as configured in the ISA server configuration section of this install guide. After the key is entered, click "Ok" and "Ok", and the connection should initiate automatically. If it does not, simply right mouse click on the connectoid, and choose connect.



With that, the client is configured to access the main network wirelessly, through the VPN tunnel.

As one additional step, a shortcut for the connectoid of the VPN network can be placed in the “Startup” programs folder, and this connection will automatically be made for the user once they login.

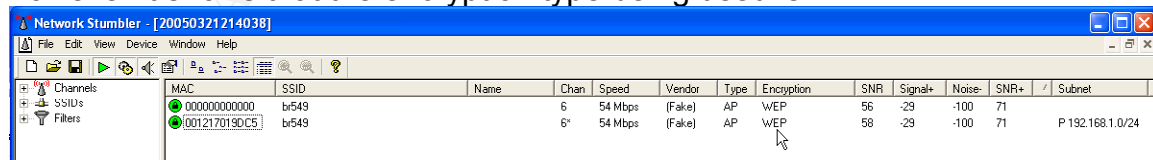
5 Auditing the Wireless Network for Security and Deviation Effects

Now that all this security has been painstakingly configured into, what seems like, a bomb proof solution to our wireless problem, how do we know for sure that it works? Well, we can see that it works because our clients are able to connect and access the things we given them rights to, but how do we know that it’s secure? The only sure fire way is to do an audit on the system, and when it comes to wireless networks, there is no shortage of tools designed to help us. Some once said that it’s a good idea to keep your friends close, and your enemies closer, and to do that, we need to understand what it is our attackers are hitting us with. So let’s go wardriving!

Wardriving is defined by Webopedia as:

The act of driving around in a vehicle with a laptop computer, an antenna, and an 802.11 wireless LAN adapter to exploit existing wireless networks. Set on promiscuous mode, the wireless adapter, typically a NIC, will receive packets within its range. Wardriving exploits wireless networks that have ranges that extend outside the perimeter of buildings in order to gain free internet access or illegal access to an organization’s data.⁴⁶

Using programs such as netstumbler⁴⁷ and airtsnort⁴⁸, attackers can discover our wireless networks, and break our WEP keys, had we used WEP, sometimes in under a second!⁴⁹ However, our current network has netstumbler stumped. When used against the testnet.msft, it identifies the network with no problem, however it shows that the encryption type being used is WEP!



Admittedly, this will probably be fixed soon to show that it is in fact a WPA network, but for now, hopefully at least some of the attackers will be spinning

⁴⁶ “wardriving” [Webopedia](http://www.webopedia.com/TERM/w/wardriving.html) 12 August 2003. 21 March 2005. <<http://www.webopedia.com/TERM/w/wardriving.html>>.

⁴⁷ <http://www.netstumbler.com>

⁴⁸ <http://airsnort.shmoo.com>

⁴⁹ “Introduction” [Airsnot Homepage](http://airsnort.shmoo.com) 31 December 2004. 21 March 2005. <<http://airsnort.shmoo.com>>.

their wheels trying to crack a WEP key instead of a WPA key. Had it shown a WPA key though, currently as of the writing of this paper, there are no known cracks for WPA RADIUS. WPA Pre-shared Key (WPA-PSK) on the other hand, is a different story all together.

As an example of a deviation from the complete solution provided in this paper, administrators may have opted to use WPA-PSK instead of the full WPA RADIUS implementation. On the surface, all that really seems to be lost is the option to limit users to being able to connect to certain access points, along with a little less hassle in ISA and IAS rule creation. However, since its release, WPA has been found to be, in some cases, even easier to crack than WEP. Robert Moskowitz, Senior Technical Director for ICSA Labs, wrote in his paper entitled "Weakness in Passphrase Choice in WPA Interface":

The normal practice is to have a single PSK within an ESS. To generate any PTK, an device only needs to learn the two MAC Addresses and nonces (and the selected ciphersuite). All of this is available in the initial exchange, from the ASSOCIATE through the 4-way handshake. Any device can passively listen for these frames and then generate the PTK. If the device missed these frames, it can send a DISASSOCIATE against the STA and force the STA to perform the ASSOCIATE through the 4-way handshake again.

Thus, even though each unicast pairing in the ESS has unique keys (PTK) there is nothing private about these keys to any other device in the ESS.⁵⁰

So whereas with WEP it takes 5 – 10 million encrypted packets⁵¹ to guess the key, with a weak WPA pre-shared key, only the initial handshake needs to be captured. This allows the attacker to be near the network for a far less amount of time to gather the information needed, and then slip away to do an offline dictionary attack, where as the WEP attacker needs to be near the network for long enough to gather all those packets. These offline attacks can be done with a program like coWPAtty⁵² which is a dictionary attack tool designed to crack WPA. However, as noted by Moskowitz in his paper, passphrases of 20 characters or longer using complex character strings can begin to effectively deter such attacks. Also noted on the SecuriTeam website⁵³,

Fortunately, off line dictionary attacks are not terribly effective against WPA-PSK networks, due to the IEEE selection of the pbkdf2 algorithm for PSK hashing. For a dictionary attack to be effective, it must take each dictionary word and perform 4096 iterations of HMAC-SHA1 with two nonce values and the supplicant and authenticator MAC addresses.

⁵⁰ Moskowitz, Robert. "Weakness in Passphrase Choice in WPA Interface". WNN Wi-Fi Net News. 4 November 2003. 21 March 2005. <<http://wifinetnews.com/archives/002452.html>>.

⁵¹ "Introduction" Airsnort Homepage 31 December 2004. 21 March 2005. <<http://airsnort.shmoo.com>>.

⁵² <http://new.remote-exploit.org/images/5/5a/Cowpatty-2.0.tar.gz>

⁵³ <http://www.securiteam.com>

Joshua Wright optimized the ipad and opad calculations in an attempt to optimize this process, but he was only able to accommodate approximately 70 words/second on a Pentium 4 3.8 GHz system (5570 bogomips).⁵⁴

The best thing to do, if WPA-PSK must be used, is to use as long of a pre-shared key as possible that is complex, and use AES instead of TKIP. However, as is the point of this paper, regardless of the wireless encryption used, there is still very strong authentication and encryption being used through the VPN tunnel. If the key was compromised, the attacker still has a giant hurdle to overcome before being able to access the main network.

Other deviations from the complete solution might be to implement this scenario in a workgroup instead of a domain. To do this, the accounts would need to be configured on the RADIUS server itself instead of the domain controllers, and the option to configure the client so that the authentication process does not automatically use the Windows logon information would need to be utilized as discussed earlier in section 4.1 Configuring the wireless settings.

Conclusions

In conclusion, from all the widespread press about the security problems with Wi-Fi networks, it is painfully obvious that a solution needs to be presented to safeguard them. Simply creating single layered defense for this problem has not worked in the past, and in fact, has fueled the distrust for wireless implementations. However, using a defense-in-depth approach, similar to those used successfully in protecting our wired networks, I believe administrators can be just as comfortable with their wireless LANs as they are their wired LANs. By employing tried and true VPN technology, the wireless network can thrive in a secure environment regardless of the current situation of the wireless encryption itself. By combining the strength of the current 802.11i and 802.1x standards with this VPN solution results in an even stronger, holistic approach to the problem.

⁵⁴ <http://www.securiteam.com/tools/6L00F0ABPC.html>

References

- Alencar, Alexandre C. "How to Set up an ISA Server with a Cable Modem Connection." ISAserver.org. 19 July 2004. 27 February 2005.
<http://www.isaserver.org/tutorials/How_to_Set_up_an_ISA_Server_with_a_Cable_Modem_Connection.html>.
- "APIPA". webopedia.com. 18 September 2003. 7 March 2005.
<<http://www.webopedia.com/TERM/A/APIPA.html>>.
- Arbaugh, William A. "An inductive chosen plaintext attack against WEP/WEP2." IEEE Document 802.11-01/230, May 2001. 18 March 2005.
<<http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/1-230.zip>>
- Arbaugh, William A., Narendar Shankar, and Y.C. Justin Wan. "Your 802.11 Wireless Network has No Clothes." 30 March 2001. 18 March 2005.
<<http://www.cs.umd.edu/~waa/wireless.pdf>>.
- Borisov, Nikita, Ian Goldberg, and David Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11." 18 March 2005.
<<http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf>>
- "CoWPAtty – Offline WPA PSK Dictionary Attack Tool". SecuriTeam. 11 November 2004. 22 March 2005.
<<http://www.securiteam.com/tools/6L00F0ABPC.html>>
- Gast, Matthew. "Wireless LAN Security: A Short History". O'Reilly Wireless DEVCENTER. 19 April 2002. 18 March 2005.
<<http://www.oreillynet.com/lpt/a/1728>>.
- "Help: Management" 7 March 2005 <<http://192.168.1.1/help/HManagement.asp>>
- "Introduction" Airsnort Homepage 31 December 2004. 21 March 2005.
<<http://airsnort.shmoo.com>>.
- "Message Authenticator attribute" Microsoft Windows Server System 25 February 2005.
<http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_ias_messauth.asp>.
- Moskowitz, Robert. "Weakness in Passphrase Choice in WPA Interface". WNN Wi-Fi Net News. 4 November 2003. 21 March 2005.
<<http://wifinetnews.com/archives/002452.html>>.

Security Hardening Guide: Microsoft Internet Security and Acceleration Server 2004 Standard Edition. Redman: Microsoft Corporation. 7 March 2005
<http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/securityhardening_guide.msp>

“To configure the Message Authenticator attribute and shared secret” Microsoft Windows Server System. 19 March 2005.
<http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_ias_client_MessageAuth.asp>.

“Understanding forwarders”. Microsoft Windows Server System. 28 February 2005.
<http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_DNS_und_Forwarders.asp>.

Using forwarders”. Microsoft Windows Server System. 28 February 2005.
<http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_DNS_imp_UsingConditionalForwarders.asp>.

Walker, Jesse R. "Unsafe at any key size; an analysis of the WEP encapsulation." IEEE Document 802.11-00/362, October 2000. 18 March 2005.
<<http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip>>.

“wardriving” Webopedia 12 August 2003. 21 March 2005.
<<http://www.webopedia.com/TERM/w/wardriving.html>>.

“What is ISA Server 2004?”. Microsoft Windows Server System. 15 February 2005. 28 February 2005.
<<http://www.microsoft.com/isaserver/evaluation/overview/default.asp>>.

“Wi-Fi Alliance press release: Wi-Fi Alliance Introduces Next Generation of Wi-Fi ® Security”. Wi-Fi Alliance. 1 September 2004. 15 March 2005.
<<http://www.wi-fi.org/OpenSection/ReleaseDisplay.asp?TID=4&ItemID=181&StrYear=2004&strmonth=9>>.

“WLAN”. webopedia.com. 16 January 2004. 18 March 2005.
<<http://www.webopedia.com/TERM/W/WLAN.html>>