Global Information Assurance Certification Paper

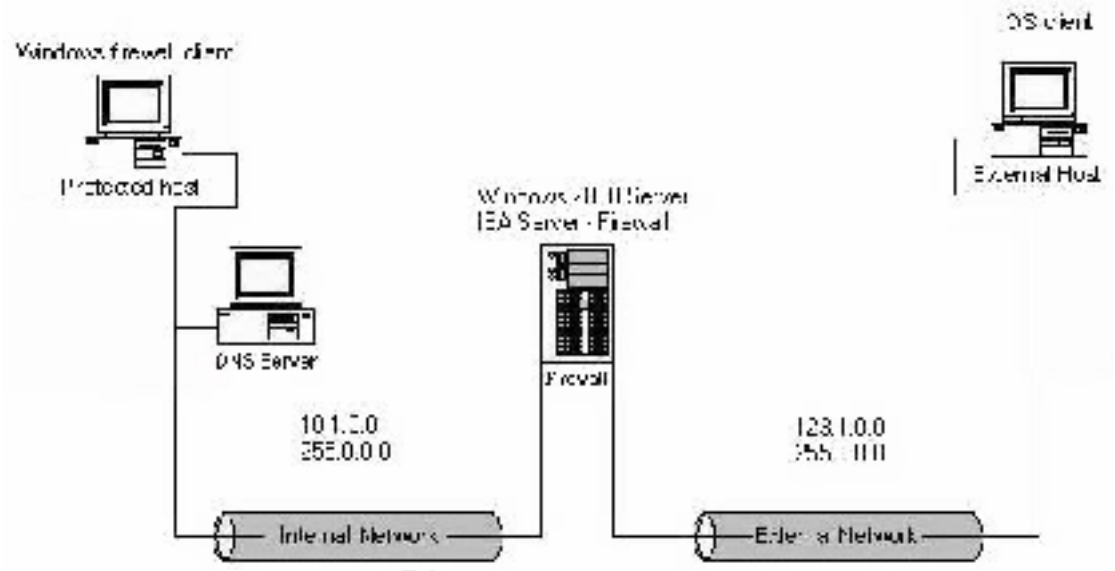
Roger Hall

GSEC
Assignment version – 1.4

A Look at Microsoft ISA Server with Security in Mind
Roger Hall
7/10/02

Introduction

Internet Security and Acceleration Server (ISA) is an extremely useful tool for the security of an organization's network, in particular organizations that have Internet connectivity. Here is the list of ISA's functionalities: Caching, Firewall, VPN, Content screening and Network Address Translation (NAT). Here is a diagram of a small Windows 2000 network with ISA on the network perimeter. See Figure 1.



ISA is Microsoft's answer for a firewall. By virtue of its functionality, it is apparent that Microsoft is answering the call for security related products and improving in that area specifically. ISA does more than just perform firewall functions. Even if you already have a firewall in place, it would be a good idea to have an additional firewall for critical parts of your network to protect important corporate electronic assets. You could also use the caching functionality to implement bandwidth rules to aid in managing resources that may be retrieved from your internal network. This paper will look at key portions of the stand-alone, Standard Edition of ISA Server and ways that you may use it in your network environment.

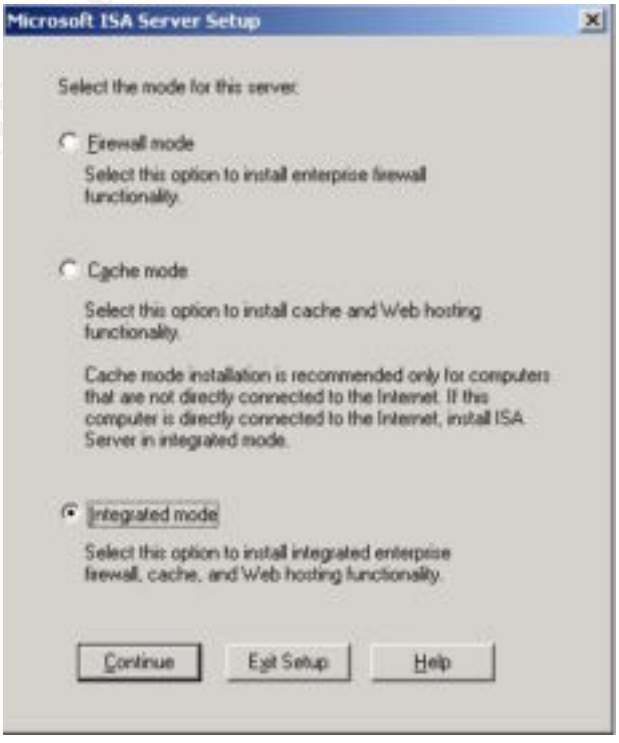
ISA with security in mind

We will touch key aspects of ISA Server as well as some configuration issues to pay attention to. I recently setup ISA Server in a test network environment. The goal of my paper is to help bring out important parts of setup and configuration of ISA should you need to deploy ISA in your organization. ISA runs on Windows 2000 Server, bearing in mind that ISA has many of the same minimum requirements as any Windows 2000 system. Note that it is recommend that you

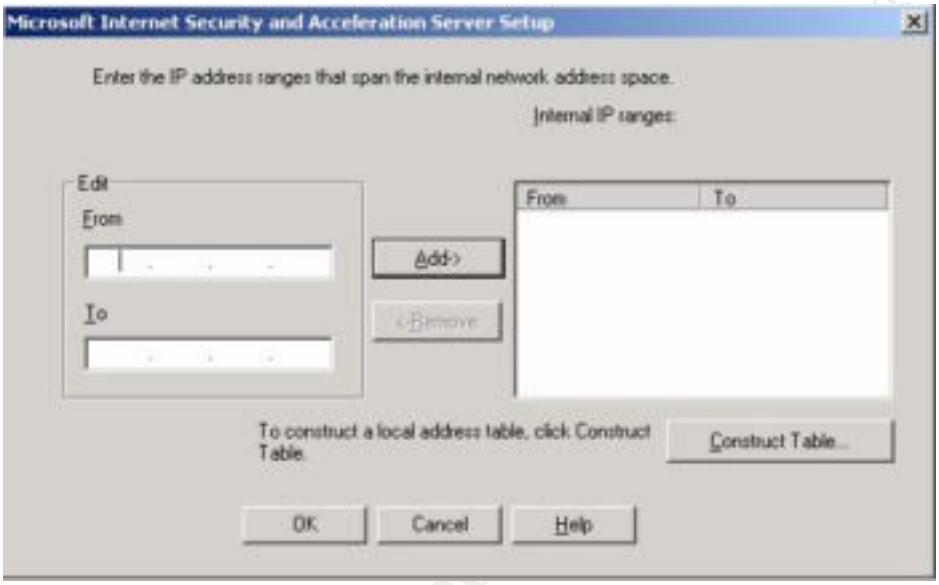
remove IIS during setup for your Windows 2000 Server. During setup, I removed IIS to avoid opening any unnecessary holes in my network. ISA requires that you use NTFS for your server's file system so to be able to use the caching functionality. I formatted all of my server partitions with the NTFS file system.

Microsoft recommends making your server an (ISA only) server. To utilize the firewall functionality, you will need a minimum of two network connections, one for your internal network and one for your Internet connection. While running through ISA setup, you will want to specify your ISA server's function. ISA can operate as Caching Only, Firewall Only, or in Integrated Mode. I will briefly explain each function, then I will share what ISA mode I chose and why. ISA's "Caching" function can provide Internet access to users on your network. The Caching function can download frequently accessed web sites to ISA for network users to access. An example of ISA's use would be to aid in conserving your Internet bandwidth resources. You could schedule ISA to "deny" any web traffic during certain times that you specify. My organization opted to limit Internet access during the hours of 12:00 a.m. until 6:00 a.m. everyday to aid in keeping costs down where Internet use is concerned. Utilizing the caching function, you can log where your network users are going on the Internet. The next function is the Firewall function. This function can protect your network by screening incoming and outgoing traffic, ultimately controlling access to and from your network. The last functionality is a combination of the caching and firewall functions, which is called "Integrated Mode". With this knowledge in mind, I chose "Integrated mode" so my organization could utilize the firewall and caching functionality. Since we are touching on ISA's functions, we will later cover security templates as they relate to each ISA mode or function. I will explain what I learned about each level of security and what security template I used to secure ISA. Now we will cover our next critical part of ISA setup.

Figure 2. ISA Server Setup – ISA Mode selection



The next step is the configuration of the (LAT) otherwise known as the Local Address Table. Proper LAT configuration is an absolute key and critical part of proper configuration of ISA. Below I will further discuss why proper LAT configuration is so important.
(LAT) Local Address Table - Figure 3.



During LAT setup, you will enter your internal trusted network address space. You could choose to enter nothing and ISA will build a LAT for you based on your Windows 2000 network routing table. Making no entries in LAT could open up the potential for error unless you pay close attention to your routing tables. I highly recommend that you manually enter your trusted network address space into the LAT. Please note: it is not a good idea to place addresses outside of your trusted address space in the LAT. If you place an external address in your LAT, requests from that address will be treated as an internal network client and will not be subjected to the same rules / access controls applied to external network or Internet hosts. Pay close attention to detail when specifying addresses in your LAT. After completion of this step, the setup application will re-start ISA services. ISA will then be ready for further configuration.

It is critical after ISA setup to apply all necessary ISA security updates/ patches. There are a number of ways to check for security updates or patches. I checked mine in the following order. First I went to http://windowsupdate.microsoft.com/ to run Windows update against ISA. Another handy tool that should be used is "HFNet Check", which can be found here - http://www.microsoft.com/downloads/release.asp?releaseid=31154.
When you run "HFNetChk" against your server, it can give you a list of hotfixes/ patches that may apply to it. Once you have the list generated with "HFNetchk", you can then go to Microsoft to search for the respective hotfixes/ patches. Once you locate a hotfix, be sure to review the details of the hotfix thoroughly so to

determine whether it is required for your server or not. Just because “HFNetChk” says you are missing a hotfix doesn’t necessarily mean that you must install it on your machine. Know your server well enough to know if you use a specific service or function. Otherwise you could potentially install a hotfix that applies to something that is not used on your server. This could open up a security hole on the server unnecessarily. Next a visit to the Microsoft ISA site is in order to see if any recent service packs have come out. http://www.microsoft.com/isaserver/ I updated and patched Windows 2000 and ISA using all of the ways I just discussed.

Now I will briefly touch on the “Security Configuration Wizard; to include what it does to aid in configuring the ISA Server. Microsoft created the Security Configuration Wizard to aid you in hardening your system. Be wary of using this utility unless you thoroughly understand what it is doing. It does not have an undo feature. The security configuration wizard could potentially change areas of your server that you may not want to change. Should you choose to use the Security Configuration Wizard, make sure that you backup your server first prior to making any changes whatsoever. Take a look at the Windows 2000 server security templates to see what each one does. To take a look at the Security Templates, look in C:\Winnt\security\templates. There are several ways you can review the templates. You could bring the templates up in Word pad. Another way to look at template settings would be to go into control panel, administrative tools, and double click on Local security Policy. Then right click on security settings, select import and select the template you want to look at. Once you have imported the template, you can review the security template to compare your current server settings with the templates. Be very careful not make the template that you are viewing the “effective setting” unless you decide you need to. If you do not choose to use the template’s settings, you could create a custom template that fits your organization and one that ultimately complies with your organizational security policy.

Having just touched on the ISA Security Configuration Wizard and security templates, I will explain all three security levels as well as the security templates that the Security Configuration Wizard uses. I will also share what template I chose and why. We will look at the most restrictive to the least restrictive templates. The first security level is called “Dedicated”; the security template that is associated with it is “hisecws.inf”. It is the most restrictive of the security templates. You would want to use this template if you were going to use ISA as a Firewall only. The second security level is “Limited Services”, the security template that is associated with this level is “securews.inf”. If you are going to use both the Caching and Firewall functionalities, “Limited Services” will be the template to select. The last security level is “Secure”. The security template that is associated with this security level is “basicwk.inf”. Don’t let the name of it fool you, I thought it was strange for Microsoft to call the least restrictive template “secure”. You would think “secure” would be the most restrictive, however it is not. This template is to be used if you are going to run more than ISA on your

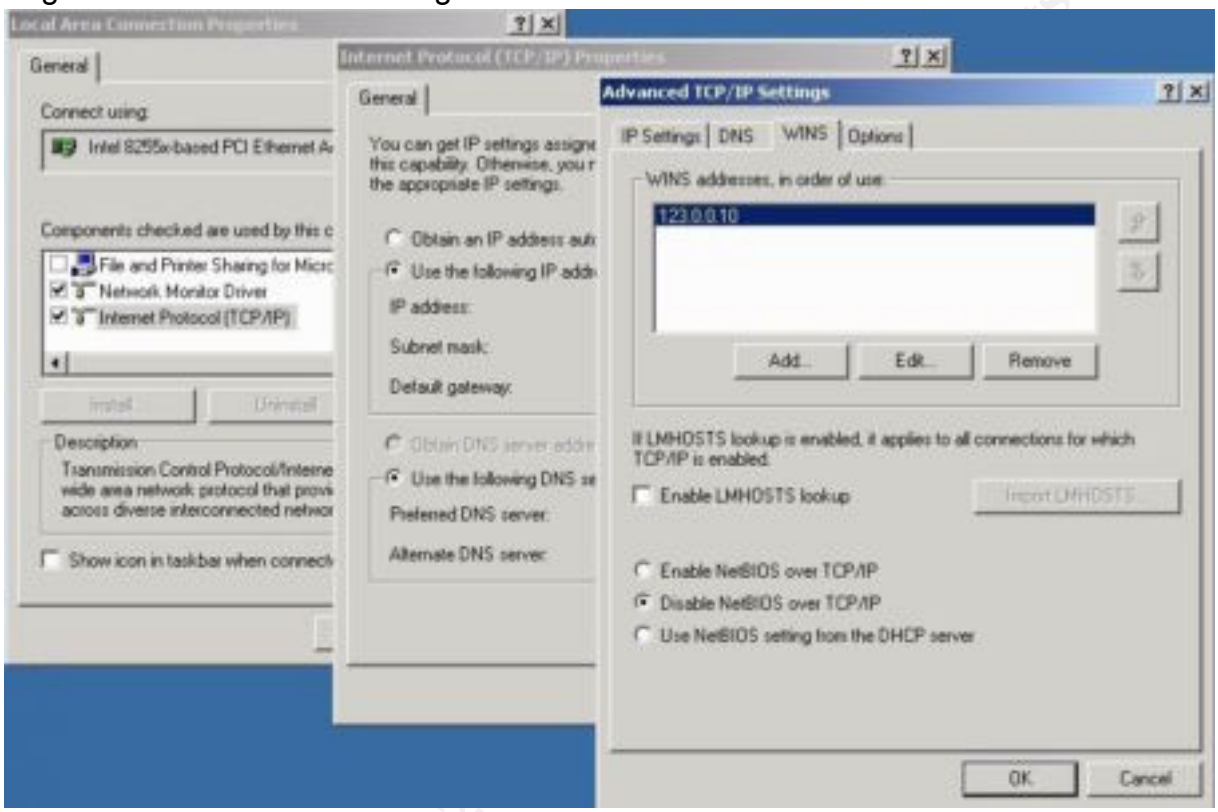
Server. An example of this would be If you were going to run IIS or another application on the server along with ISA.
Earlier I shared that I opted for “Integrated Mode” for ISA setup, I chose to use the “Limited Services” template as my organization opted to use both the Firewall and Caching functionalities.

Now lets analyze ISA’s installation default settings, as it is good to understand them so to prepare to configure ISA further. For “Access Control”, the site and content rule, called the “Allow” Rule is set to permit unlimited access to clients all the time. From a security perspective this sounds bad, but since we are setting it up as a stand alone ISA, there is no enterprise policy to contend with and no defined protocol rules exist yet, which means access is prohibited. You would have to create a protocol rule allowing access to the Internet or any external network addresses in order to open up access. The next default setting concerns “Alerts”, which makes all alerts active. We will touch on “Alerts” as it relates to Intrusion Detection. We will cover this in more detail later as it is imperative to enable ISA to alert you to any intrusions or port scans. The “Caching” setting enables all HTTP and FTP caching. Earlier in the paper we touched on ISA’s “Caching” functionality. Next we have “Client Configuration” relating to our desktops that will point to ISA for Internet accesses; the automatic discovery feature should be enabled to expedite pointing to the ISA for access. The “LAT” or Local Address Table configuration setting was already addressed earlier in the paper and it appears during initial ISA setup. The next server setting is “Packet Filtering”; we will go into more detail on packet filtering later on. Then we have “Publishing” which means you can publish a website from an internal server via ISA. The default is to not publish to the outside web. Lastly, “Routing” default is to enable web proxy clients to access the Internet.

Now we will focus on the hardware configuration of ISA in respect to ISA’s network interface cards or (NICS). We have a multi-homed type of setup as we have two NICS, one for the internal network and one for the external network or Internet. For security, the TCP/IP configuration of the NIC Cards is vital. I looked at the configuration of the external NIC first. It is recommended to disable “File and printer sharing for Microsoft networks” for the external NIC. File and printer sharing advertises shares, which would not be good to advertise on the Internet. The external interface or the Internet connected network card should be the only one configured with a default gateway. Also “Netbios” should be disabled on the external interface, as you certainly don’t want to advertise your network on the Internet in this manner. To do this you will go into the network interface properties of the external NIC, click advanced and then the WINS tab and select “Disable Netbios over TCP/IP”. (See Figure 4 below). This is a good time to recall what we addressed concerning the (LAT) or Local Address Table configuration, Do not place external addresses into your internal address space in the LAT which ISA would see as a local internal network address. “Packet filtering” rules would not apply if you placed your external NIC address into the LAT as packet filtering applies specifically to the external NIC. Any security policy that you

implemented concerning the external NIC would not apply; this would eliminate security altogether. Figure 4 details what I did for this portion of the setup. File and Printer Sharing for Microsoft Networks has been unchecked and Disable Netbios over TCP/IP is selected.

Figure 4. – File Printer Sharing and Netbios over TCP/IP Disabled.



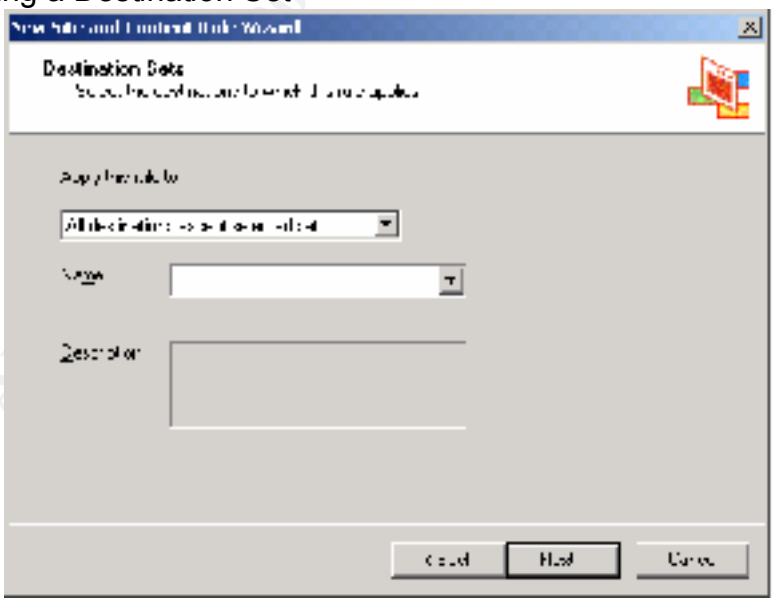
Now lets look at the configuration of the internal NIC. You will want to configure it to use the internal DNS server, which will resolve any inbound requests for machines/services located on the internal network. For example, if you have a web server that you wanted to publish to the Internet while still remaining on the internal network.

Next I will touch on ISA Access Policy. ISA Server rules primarily govern outbound traffic. For inbound traffic, IP Packet Filters, application filters and intrusion detection filters govern the inbound area. You will want to configure the rules/policies based on your organization's security policy. ISA Server allows you to manage the traffic based on network users, security groups, data content, specific applications, or certain network computers. You can also "allow" or "deny" certain protocols; ports based on the policies/ rules you set within ISA. In the ISA Management console, select "Access Policy", underneath this are Site and Content Rules, Protocol Rules and IP Packet Filters that work together in governing the Access Policy. Site and Content Rules govern what network clients, users or security groups that can access sites or content via the ISA Server. I created an "Internet Access" security group on the domain granting access to the folks who would require it. I then granted access to the "Internet

Access" group via the default Site and Content Rule to limit external access. Site and Content Rules work in concert with defined Protocol Rules. Click on the Create a New Site and Content Rule Icon to open the wizard to create a new site rule. The Default Site and Content Rules is to "allow" all sites and all content at all times. Later you may want to create a new Site and Content Rule to further "lock down" outbound traffic. This will help to better control your outbound traffic in place of the default Site and Content Rule which allows all sites and content at all times. Two key parts related to Site and Content Rules are Destinations Sets and Client Address Sets. Destination Sets can be used to block sites or other resources by IP Address, or IP Range or Computer name. Client Address Sets can specify rules to apply to computers based on specific IP addresses. Based on everything covered on access policy thus far, I elected to practice blocking a site. To perform this, open up ISA Management Console, select "Policy Elements", select "Destination Sets". Click on create Destination Set to block the site (for practice, this site is non-existent) www.no-go.com. I named it "No Go Site Block", then in the box labeled "Destination" I typed in the URL and clicked OK. Next within ISA Management Console, Select "Access Policy", click on Create New Site and Content Policy, then name it "No Go Site Block", click next and select "deny". (See Below - Figure 5.)

The following screen (Figure 5) shows Destination Sets. Click the drop down arrow to select the "No Go Site Block", schedule is set to "Always", then click on finish. Administration is super easy when it comes to allowing or blocking Sites.

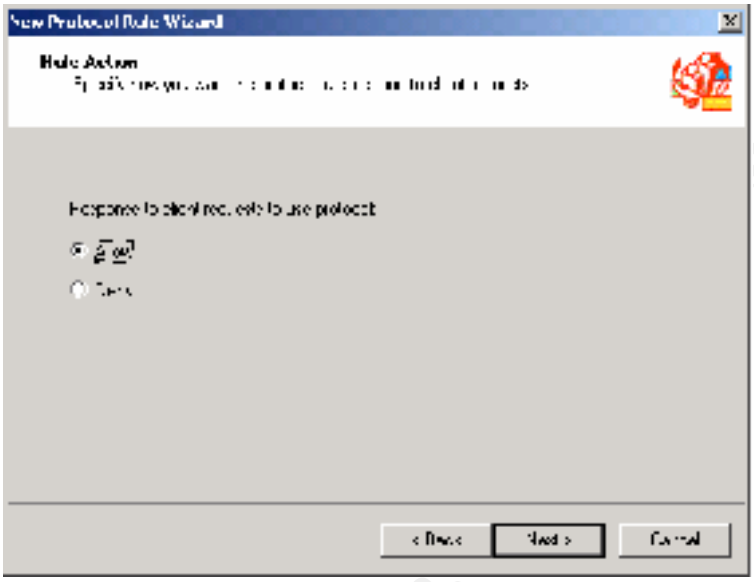
Figure 5. Defining a Destination Set



Now we will examine Protocol rules. Protocol Rules govern what protocols network clients' can use to access the external network or Internet. For example, you could "allow" any AOL Instant Messenger traffic. Not that you would want AOL Instant Messenger on your network at all, but you could "allow" specific folks

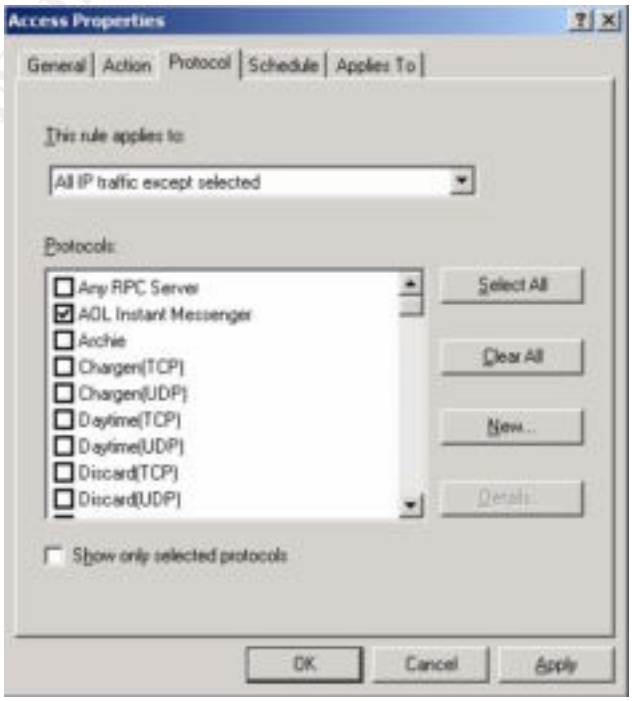
to use AOL Instant Messenger while denying others from using it. Access Policy in ISA can be very useful in this area of application or protocol use specifically.

Figure 6. New Protocol Rule, shows an example of the “New Protocol” Wizard.



You could also set a time schedule as to when a protocol could be utilized. You could do this for any protocol that is defined in “Protocol Definitions”. Protocol Definitions can be found in the ISA Management Console under “Policy Elements”

To create a new protocol rule, select Protocol Rules, Click on the Create a New Protocol Rule Icon to open the wizard to create a new protocol rule. Based on this information, I created a protocol rule allowing AOL Instant Messenger and then I later denied access. Figure 7. Shows the Protocol Rule selecting AOL Instant Messenger.
Figure 7.



For Figures 6 & 7. We selected “allow” AOL Instant Messenger, later we went back and selected “deny”. It effectively blocked the use of AOL Instant Messenger. This is proving to be very useful.

Protocol Rules specifically determine what protocols can be utilized for inbound or outbound access. Another key part of Protocol Rules is Protocol Definitions, which are used to create Protocol Rules. ISA Server already has the common Internet Protocols pre-defined. Protocol definitions “allow” you to create a policy based on TCP/UDP protocol. You can specify within protocol definition properties what port connection it will be based on and whether it will be used on an inbound or outbound connection. After a protocol definition is setup, you can create a policy or rule based on it. To sum up how ISA deals with requests, it verifies that there is a Site and Content rule and a Protocol Rule that allows access to an external or Internet Resource before granting access. If one or the other states “deny”, it will “deny” access to the resource. Earlier I mentioned that the Default Site and Content Rule is to “allow” all sites and all content at all times, but without a Protocol Rule in place to “allow” Internet access, it will “deny” access. Based on this, I re-visited “Access Policy” within the ISA Management Console and selected “Protocol Rules” to setup a rule to open the access. Click on “Create a New Protocol Rule For Internet Access”, in which case I named my rule “Internet Access”. Then click next and choose the effective protocols “HTTP, and FTP etc”. Next comes the schedule setup, I selected “Always”. Earlier I created an “Internet Access” security group. I then selected “Users and groups” and granted the “Internet Access” group Internet Access.

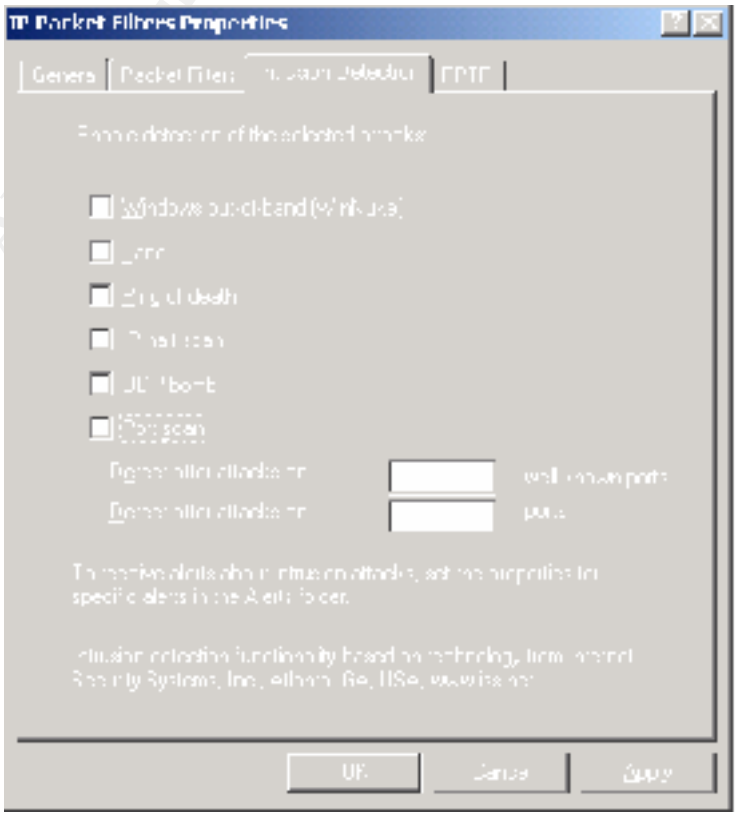
The last area to address in “Access Policy” is packet filtering. Packet filtering is a very useful tool. With Packet Filtering, packets can be filtered by service, port or address. If a packet filter is not defined to “allow” a particular packet through ISA, then ISA will drop it. If a filter has been configured for a particular packet, it will “allow” it through, however the header information in the packets must match the parameters within the filter rule before the packet will be allowed to pass through. ISA offers an optimal filtering method called Stateful Inspection. What this does is ensure that network traffic is behaving normally, which means the connection is “known” or legitimate. Another filter offered is Application Filters, which for the most part govern inbound traffic. The purpose of Application Filtering is to inspect the data portion of a packet and drop any packets that may contain a malicious payload. In the beginning of the paper as we were covering ISA’s Default settings, we touched on “Publishing” Servers. The only way to “Publish” a server is via “Packet Filtering”. I will go over what I did to “Publish” a web server that was on the perimeter of the network. These Packet filters make the web server available to external network clients. To set this up, I went into ISA Management Console and selected “Access Policy”, right clicked on “IP Packet Filters”, selected “New”, selected “filter”, then named the filter the web server name. Next came the “Filter Mode” page, in which case I selected “Allow packet transmission”. I then clicked next to get to “Filter type”, the Pre-defined option was selected, clicked on the drop down box and selected HTTP server (port 80),

then selected ”Computer on the perimeter network”. I placed the IP address of the web server and applied the packet filter to “All Remote Computers”. Then from the Internet I was able to visit my generic website hosted on the published web server.

So to bring “Access Policy” together, Protocol Rules, Site and Content Rules and Packet Filtering all work in concert together to help protect the network. Protocol rules specify what protocols network clients can use to access external network resources. Content and Site Rules “allow” or “deny” what network clients or client address sets can access based on content specified by defined Destination Sets. Packet filtering allows or denies access by service, port or address. Policy setup was the most enjoyable part of configuring ISA for me. ISA security revolves around Access Policy. I have found that it is highly important to setup policies correctly to help protect against any potential attacks against the network.

Now we will briefly touch on another key feature of ISA, (IDS) Intrusion Detection System. ISA has built in Intrusion Detection Filters that you can enable for use. Microsoft pre-configured ISA to detect the following attacks, WinNuke, Land (SYN flood), Ping of Death (Loaded packet attack), Port scans, half scans, and UDP bomb (UDP packet flood). ISA can be setup to “Alert” you to any negative activity. It can be setup to send you an e-mail message, a network message, write to the Event Log, stop the Firewall service or kick off a batch script to perhaps shut down the server. I have ISA setup to alert me via network message if any attack activity occurs. To briefly re-visit Access Policy, “deny” access to the ICMP Protocol. This will prevent the Ping of Death. Take a look at ISA Policy configuration and investigate how ISA could be setup to prevent other attacks from occurring. I setup ISA to detect all of the attacks specified in Figure 8.

Figure 8. (IDS) Intrusion Detection System Properties



There are three key areas in ISA that you can configure to generate logs, Packet Filters, The Firewall Service, and the Web Proxy Service. You can log any service activity to a text file or to a SQL database. You may have any of the three services place logs in the location that you specify. The default location for log placement is in the ISALogs directory located under the ISA Server directory. For performance sake, I placed my log files on a partition separate from the system and caching partitions. For initial setup of logging of the three services, Packet Filters, Firewall Service, and the Web Proxy Service, I selected all Log field options. The Logging options are much too numerous to list here. Here are the fields that I initially setup for ISA. It is really easy to adjust log field options for ISA. For Packet Filters, I chose to Log everything; to include Date, Time, Source IP address, Destination IP address, Protocol used, Source/ Destination ports, Header and Payload. Note that logging can be very processor intensive. I logged excessively so I could view what data I could glean from the log. I recommend doing this, then adjust it to your needs. Logging with Packet filters is important, as it is your network "ingress" log. In other words, everything coming into your network is recorded. For the Firewall Service, again I initially chose to log everything so I could review the logs and look at the data produced by it. Then I adjusted the log field options associated with the firewall service to log only what I really needed. Logging with the Firewall service is important as well as it is your network "egress" log. So based on this, I effectively setup logging for inbound and outbound network traffic. I also setup logging for everything associated with the Web Proxy Service. Based on the Web Proxy Service, I generated statistical reports for analysis. ISA has five predefined reports for you to use to aid in report generation. I used the Web usage report to analyze where network users visited on the Internet via ISA. Logging the right information and paying attention to it is really important. What is the point of logging if you are not going to review it regularly?

Now that we have covered key aspects of ISA Server, now it is time to take a look at client side configuration to work with ISA. There are three types of clients; all three have different functionalities. First we have the web proxy client, you could configure a client machine's web browser manually to point to ISA or the Firewall client could be used to give the same functionality as far as web connectivity via ISA. Next we have the Firewall client which can only be used with Windows. The Firewall client software can update the LAT, configure web proxy functionality automatically for the client machine as well as set the respective network DNS settings for the client machine. The last client we will address is the "SecureNAT" client. SecureNAT can work with all operating systems. To use SecureNAT, you configure the client machine's default gateway to point to ISA's internal NIC. SecureNAT seems to be the easiest of all of the clients to setup. For my environment I selected the Firewall client as it enables you to have more granular control via your ISA access policies. When someone is accessing certain resources via the Firewall service, you can see who is using resources by looking in the ISA Management Console under "Monitoring –

Sessions". To install and use the Firewall Client, go to Start "Run" and type in the \\Servername\mspclnt\setup.exe. It's very beneficial to be able to see this information.

Conclusion

In the near future I will be deploying ISA for use in my organization. I thoroughly enjoyed testing ISA and I am currently working on configuring the most optimal settings for my organization. Internet Security and Acceleration Server is a useful security solution that can provide critical firewall functionality with the bottom line being protecting your organization from the Internet. ISA has many useful tools for you to work with to help you secure your network resources, internal and external. The setup and configuration is fairly concise and easy. ISA is multi-functional with a configuration that allows you to get granular when it comes to security policy. In the big picture, there is no one-stop shop for network security; it takes a many faceted approach to secure a network. A solid security policy in the spirit of Defense in Depth is key in this on-going endeavor. Securely setting up your servers, keeping up with patches, enforcing policy and paying attention to your network are all vital in this. ISA is a useful and powerful tool to aid in this endeavor.

References:

Zubair Alexander, Microsoft ISA Server 2000 Book, 2001

Tom Shinder, Configuring ISA Server, Building Firewalls for Windows 2000 Book, 2001

Karanjit Siyan, Windows 2000 Server, Professional Reference, 2000

Microsoft Website: Internet Security and Acceleration Server Home Page.
http://www.microsoft.com/isaserver
http://www.microsoft.com/isaserver/techinfo/default.asp

Will Schmied "Installing ISA Server", Dec 28,2001
http://www.isaserver.org/pages/article_p.asp?id=261

Tom Shinder "Designing An ISA Server Solution on a Simple Network" Apr 27, 2001.
http://www.isaserver.org/pages/article.asp?id=230

Jim Harrison "ISA Clients - Part 1: General ISA Server Configuration" Nov 06, 2001
http://www.isaserver.org/pages/article.asp?id=238

Microsoft Corporation. Internet Security Accelerator Product Documentation
http://www.microsoft.com/technet/isa/isadocs/default.asp

Microsoft ISA Server 2000, Standard Edition - Installation and Deployment Guide
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/isa/deploy/isastnin.asp

James R. Borck, InfoWorld " ISA Server 2000 locks down resources "September 1, 2000
http://www.infoworld.com/articles/mt/xml/00/09/04/000904mtisa.xml

LabMice.Net Website: "ISA Server Resource Page – Securing ISA Server"
http://www.labmice.net/BackOffice/ISAServer2000/default.htm

Mike Bobbit, InfoSecurityMag.Com, ISA Server Breaks Security Ground
http://www.infosecuritymag.com/articles/january01/departments_products1.shtml