

Global Information Assurance Certification Paper

Copyright SANS Institute Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering "Security Essentials: Network, Endpoint, and Cloud (Security 401)" at http://www.giac.org/registration/gsec Your assignment is to use resources on the Internet to research an important security issue. The security field changes rapidly, and often the most up-to-date information can only be found on the Internet. As such, it is critical that we as security professionals are able to use the Internet to find the information we need.

You MUST use at least FIVE cited sources, and at least THREE of them must be from the Internet. You may use additional sources, such as books, magazine articles, etc., if necessary.

Your research may cover an exploit or vulnerability, a particular technology, a tutorial or "how to", a legal or regulatory issue, and so on. In writing your paper, you should do more than just write a "book report" that repeats back what you have read in your sources. See below for the specific criteria by which your paper will be evaluated.

She had a set of the s

Author:Jack Green

Submitted to partially fulfill the requirements for the GSEC certification

Installing Microsoft's Internet Security and Acceleration Server (ISAS): Getting Started and Testing.

Thursday, November 01, 2001

Introduction:

Installing a test firewall environment is challenging and time consuming. It is also necessary for gaining a practical understanding of firewall concepts and practices. The purpose of this discussion is to mitigate some of these challenges by describing the process for setting up a simple, scalable and affordable firewall lab. Since Microsoft offers free trial versions of the software, the lab will use their products.

Additionally, I will briefly review resources that discuss security issues, resources for obtaining patches, and news/support groups for ISAS.

What is ISAS?

A Microsoft product new on the market, ISAS is one of the products included in the .NET family. In the interest of brevity, I won't list all the services. That being said, among its offerings are the following services:

- VPN
- Intrusion Detection
- NAT
- Bandwidth Allocation
- Email Content screen
- Firewall services

A complete discussion of ISAS' capabilities is well beyond the scope of this paper. The references listed at the end provide a detailed discussion of ISAS features.

Test Environment Hardware.

Figure 1 shows our basic lab.

<u>Windows firewall client</u> – any windows compatible PC. The firewall client is not compatible with other OS'es

<u>Firewall</u> - Pentium 300 MHz or higher. 256 RAM, at least 1GB and 20mb+ for SIAS installation, 2 Ethernet cards.

External Client – any PC running any OS

<u>Network Cables or hubs</u> – either two hubs and four standard (straight through) cables or two crossover cables. Appendix A shows the configuration for crossover cables



Test Environment Software

<u>Windows 200 Server Evaluation Edition</u> - available through TechNet, many Microsoft based conferences or through the mail. If nothing else, it may be obtained at

http://www.microsoft.com/windows2000/edk/default.asp

for the price of shipping and handling.

Internet Security and Acceleration Server - is available for download at

http://support.microsoft.com/directory/content.asp?ID=FH;EN-US;ISAS&SD=gn&FR=0&LN=EN-US

Installing ISAS

As mentioned previously, ISAS runs on a multi-homed Windows 2000 server (or better). You must have routing between the external and internal (protected) networks. If you're unfamiliar with setting up routing on a Windows 2000 server, Appendix B will guide you through installing RIP v2 on the firewall.

Once routing is enabled, we are ready to install ISAS. Inset the disk in the CD and let autorun take over. After reading any release notes/ readme files, we'll choose *Install ISA Server*.



The install routine eventually challenges you for a CD Key. The evaluation key is **880-2897414**¹. During the installation process, you may choose from a number of installation options. Any of them will serve since we're focusing on the firewall services. As shown below, since our installation is on a standalone server we must install a stand-alone ISA server.

¹ This is an evaluation key available at <u>http://www.microsoft.com/ISASERVER/downloads/evalDL.asp</u>



Choosing server mode gives us three options; firewall only, cache only or integrated. I'll choose *Integrated Mode* because I may want to play with the caching features later.

© SANS Institute 2000 - 2005



The ISA install routine will stop the WWW service. We are alerted to the fact that, should we choose to run IIS on this machine, we must reconfigure the IIS listening port. ISA server uses port 80 on the external interface.



The next screen is for configuring the web cache settings. I'll choose the default and move on to more interesting things.

The *Local Address Table* (LAT) contains the IP ranges of you trusted network. You may choose to let ISAS construct the LAT for you but check it carefully as it will interpolate ranges for you. I'll elect to enter the ranges manually. The ranges include the network number and the broadcast address.

Microsoft Internet Security and Acceleration Server Setup
Enter the IP address names that shan the internal network address share
Internal IP ranges:
From To
192.168.1.0 Add>
To KRenove
To construct a local address table, click Construct Construct Table
OK Cancel Hep
Sector 1 1 - A C C State Hanner C CCCC State State C C C State C C C C C C C C C C C C C C C C C C C

The installation routine continues to install files the gives us the opportunity to launch the getting started wizard. Let's forgo the wizard and let the installer finish up. We'll look at the ISAS MMC a little later. Let's install the firewall client next.

Installing the Firewall Client

The Firewall client is a WinSock proxy client that runs on the protected Windows (only) PC's. Basically the firewall intercepts WinSock calls from each client and redirects those requests to the client chosen internet host.

The client install is installed on a share in the path "\\ISAServerName\mspcInt\"

In our case, the ISAS is named Watcher2K.

	<u> </u>	
мо г	🖬 Document - WordPad	
My L	File Edit View Insert Format Help	
My	Arial 🔽 10 💌 Western 💌 🖪 🖊 🗓 💭	
	······································	
Му		
Ru	in ? 🗙	
	Type the name of a program folder, document, or	
Į	Internet resource, and Windows will open it for you.	
0	Dpen: //Watcher2k/mspcInt/SETUP.EXE	
	OK Cancel Browse	
	Start 🛛 🧭 🈂 🗍 🗒 Document - WordPad	1:09 PM

For our introduction, the client installs as easily as that. There are several relatively painless ways to deploy it, including web-based installs and policy based installs. Those topics are well beyond this paper's purview.

Configuring ISAS

IP Packet Filters - Block ICMP

By default we can use ICMP to ping hosts outside the firewall. By allowing outbound ICMP we run the risk of participating in an internally launched DDOS smurf attack against an external host. We can block all outgoing ICMP and prevent our internal clients from launching an echo reply to the victim.

Launching the *ISA Management Monitor*, expand *Access Policy*, the click *IP Packet Filters.* As we see below, ICMP outbound is set to allow.



A test on our firewall client shows that ICMP outbound is allowed:

C:\>ping 159.105.165.17

Pinging 159.105.165.17 with 32 bytes of data:

Reply from 159.105.165.17: bytes=32 time<10ms TTL=127 Reply from 159.105.165.17: bytes=32 time<10ms TTL=127 Reply from 159.105.165.17: bytes=32 time<10ms TTL=127 Reply from 159.105.165.17: bytes=32 time<10ms TTL=127

Ping statistics for 159.105.165.17: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms Let's delete the allow ICMP outbound filter by selecting it and clicking *Delete a Packet Filter*. Next we *Create a Packet Filter* using the wizard's prompts:

- 1) Name the filter **ICMP Outbound** is fine.
- 2) Click Block
- 3) On the dropdown box choose ICMP all Outbound
- 4) Leave the **Default IP addresses for each external interface...** selected
- 5) Leave the All remote Computers selected
- 6) Click Finish

Your screen should look like this.

Doct					
File Ec	-0				
	<u> </u>				
Arial Arial Tree Arial Thernet Security and Acceleration Server Arial Ar	Configure Fire for WATCHER2K ISA Server acts as your corporcomputers are fully secured. I computers, better protecting you Use this taskpad to configure	ewall Pro orate network's g ISA Server's secu our network. e security settings	otection ateway to the Internet. It is t rity wizard and packet filters , create packet filters and so	herefore imperative that ISA ng options secure your ISA S at packet filtering properties.	Gerver erver
	Available Packet Filtere:				
IP Packet Filters	Available Facket Filters.	Modo [Description	Former	Eilter ture
🗄 🕀 🔄 Publishing			Jeschpuon		Custom Silter
Bandwidth Rules		Allow		WATCHER2K	DNS lookup
Policy Elements		Allow		WATCHER2K	ICMP pipe response
		Block		WATCHER2K	ICMP all outbound
		Allow		WATCHER2K	
H - Ma Network Configuration		Allow		WATCHER2K	ICMP timeout
Client Configuration		Allow		WATCHER2K	ICMP unreachable
	Secure Your ISA Server Computer	Configure a Pack	ket Create a Packet usion	: Filter	5
	Help		Up		Home
u 🧕			·		
				,	
object(s) (plus 1 hidden) (Disk free space: 2.76 GB)					3.48 MB 📃 My Computer
🖁 Start 🔢 🚰 🎒 🛛 🔕 CLIENTS	🗒 Document - WordPad	ISA B	Management		2:4:

Now back to our test we see that our pings are timing out.

C:\>ping 159.105.165.17

Pinging 159.105.165.17 with 32 bytes of data:

Request timed out. Request timed out. Request timed out. Request timed out.

Ping statistics for 159.105.165.17: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms

Protocol Rule – Allow Web Services

A protocol rule determines which which TCP/UDP protocols the firewall clients may access. Launching the *ISA Management Monitor*, expand *Access Policy*, then click *Configure Protocol Rules*. As we see below, no rules exist to allow Internet services hence services are denied.



To confirm this we'll try to request http services from our external network host(159.105.165.17). As seen below, services are rejected.



Let's create a Protocol rule to allow for web services"

- 1) Click Create a Protocol Rule for Internet Access
- 2) Name the rule, in my case, Allow Web then click Next
- 3) Choose Selected Protocols. HTTP, FTP, and etc. should be selected.
- 4) You may choose a schedule, I'll select Always
- 5) The Client Type is Any Request
- 6) You are shown a summary screen, select Finish once you are satisfied

Now back to our browser on the internal client, we see that we are able to connect.



Site and Content Rule – Block Lurid Site

Site and Content Rules allows us a measure of control over which sites our users may visit at any given time. Perhaps a site, a *Lurid Site*, has become popular. By surfing over to this site we have become convinced this site is not work related.

🖉 Home Page - Microsoft Internet Explorer	- 🗆 🗵	
File Edit View Favorites Tools Help	(1)	
🗇 Back 🗸 🖘 🛪 🔕 🕼 🔞 Search 💽 Favorites 🚳 History 🛛 🛃 🎒		
Address http://XXX.YYY.165.17/	Links »	
Click here for lurid entertainment		
🖉 Done 😵 Internet		
🙀 Start 🛛 👩 🍊 🎲 🔹 🔯 Microsoft Firewall Client 🛛 🖉 Home Page - Microsof	3 7:08 /	AM

In order to block our site we must first define it as a destination. Launching the *ISA Management Monitor*, expand *Destination Set*, then click *Create a Destination Set*. As we see below, you may name a destination and provide a brief descriptor (top left). Once you click on *Add*, a screen pops up allowing us to enter a domain name or, in our case, an IP to be blocked. The domain name would be preferable in a production environment, I have not set up DNS or a host file to resolve in our test environment. Enter the IP and click *OK*.

My Document Action View (← → 🕒 🕅 🗙 🛱 🕅 🔗			
New Destination Set Image: Second S	Destination R2K Jude one or more computer ules, destination sets includ rules and server publishing	Sets s or directories on specific computers. e computers that are not in your internal network. rules, destination sets usually include computers	that are in your
R Add Edit Remove	ion Sets: Description Allow clients	Destinations	
Add/Edit Destination ? X C Destination: Browse To include all computers in a domain, type ".domain. C IP addresses: From: From: 159 . 105 . 165 . 17 To (optional)	alion Set Delete a Destination	on Set Configure a Destination Set	
To include a specific directory in the destination set, type the path below. To include all the files, use this format: /dir/*. To select a specific file, use this format: /dir/filename. Path:	Help	Up	Home
DK Cancel	nagement		1:08 PM

Right click *Site and Content Rules* from the *Access Policy* window. Clicking *Create a Site and Content Rule* will launch the wizard. I'll name this rule **Block Lurid Site**.



On the next screen we choose deny. I could also choose to redirect the request to a warning page on another server.



The wizard asks to which destination set the rule will apply. We want our *Specified destination set* from the dropdown box. Choose the destination we just created, **Lurid Site**.

File Ec	15A Management New Site and Content Rule Wizard		×			1			_ 기 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
Arial	Destination Sets Select the destinations to which this rule	applies.						\sim	Go
For H	E Apply this rule to: Specified destination set	I		ified destination compute content rules.	rs can be acce	ssed by speci	fic	U.	
	Name: Lurid Site	•		otion	Action 0	oplies To	Schodulo	Dectination	
E	Description: A popular site			ption	Allow Cl Allow Allow A	ient Set ny request	Always Always Always	AllowTestSite All destinations	
	,								
24 ob		< Back Next >	Cancel					Þ	
For Help,	Protocol Definitions Content Groups Dial-up Entries Cache Configuration Extensions Extensions Extensions Lient Configuration H.323 Gatekeepers	Create a Site and Content Rule	Delete a Site and Content Rule	Configure a Site and Content Rule					
⊡-⊡ ⊕-∰ M	-					r —			-
R		Help		Up			Hon	1e	_
• I						J		J	
24 object(s	s) (plus 1 hidden) (Disk free space: 2.76 GB)					3.48	MB	🚽 My Computer	
🚮 Start	🛛 🙆 🈂 🗐 🔤 🖾 CLIENTS	🗐 Site - WordPad	ISA Manag	ement				🤣 7:1	15 AM

The next screen lets us apply the rule to a schedule. Lastly, we can choose to specify a user name, a group, an IP address or any request to which the rule will be applied. I'll let it apply to everyone.



Now to test our rule, I launch the browser and try to request our blocked site. The results are shown below. Had we redirected to a page that said, "This site not allowed" we would've given more information to our users.

🚈 The page cannot be displayed - Microsoft Internet Explorer	_ 8 ×
File Edit View Favorites Tools Help	
🛛 🗇 Back 👻 🔿 👻 🙆 🚮 🛛 🔞 Search 🕋 Favorites 🖓 History 🛛 🛃 🗃	
Address 🛃 http://159.105.165.17/	▼ @Go ∐Links »
The page cannot be displayed There is a problem with the page you are trying to reach and it cannot be displayed.	<u>*</u>
Please try the following:	
 Click the <u>Refresh</u> button, or try again later. Open the <u>159.105.165.17</u> home page, and then look for links to the information you want. 	
 If you typed the page address in the Address bar, make sure that it is spelled correctly. 	
 Verify that the Internet access policy on your network allows you to view this this page. 	
 If you believe you should be able to view this directory or page, please contact the Web site administrator by using the e-mail address or phone number listed on the 	-
🖉 Done	ernet
😭 Start 📔 🙆 🧐 📋 🔍 Microsoft Firewall 🖗 The page canno 🗐 Document - Word	- 🤣 7:15 AM

Discussion

Resources for ISA Users

The newsgroup - Comp.security.firewalls

Microsoft ISA Home - http://www.microsoft.com/isaserver/default.asp

ISA server organization - http://www.isaserver.org

Bug reports:

As of September 20, 2001 there are only a handful of reported bugs and patches including:

- a potential memory leak in the H323 ASN DLL.
- scripting can be executed in the error return pages from the ISA server.
- many open sockets when the client reaches a high open-and-close connection rate (600/sec.)

- ISA was returning incorrect checksums to Ethernet adapters using hardware checksum
- ISA does not filter and flow traffic routed by a 2000 server using the QOS Packet Scheduler Service.
- a registry patch to block and log all outbound ICMP traffic that is sent from the internal network to the external network
- the logging module prevents the logging of the "Rule#1" and "Rule#2" fields for certain UDP traffic

These reports and their corresponding patches may be found at Microsoft as well as http://www.isaserver.org/pages/bugs/patches.htm .

<u>Summary</u>

This paper presented a procedure for establishing a test environment in which to prove ISA firewall rules. For a minimal investment, a student/professional can develop policies *in vitro* before deploying to the production environment. The sample rules are not presented as exhaustive.

Future topics of research into the use of Microsoft's ISA server might include:

- writing the rules for sans.org's top twenty
- exploring the caching functions
- testing and evaluating the Secure Nat functions of ISA
- testing and evaluating the intrusion detection functions
- reviewing 3rd party add-ons to ISA

References

"Microsoft Download Center." http://www.microsoft.com/downloads/search.asp (26 Oct. 2001)

"Windows 2000 Advanced Server Trial Offer." http://www.microsoft.com/windows2000/edk/default.asp (26 Oct. 2001)

"Microsoft Internet Security and Acceleration Server – Home." <u>http://www.microsoft.com/isaserver/default.asp</u> (26 Oct. 2001)

"Microsoft ISA Server Firewall and Cache resource site." http://www.isaserver.org. (30 Oct. 2001)

Huegen, Craig. "CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks. "<u>http://www.cert.org/advisories/CA-1998-01.html</u>. (13 March 2000)

Mingus, Larry. Ethernet Crossover Cable - DIY How-to Guide. <u>http://www.makeitsimple.com/how-to/dyi_crossover.htm</u>. (10, July 1998)

Shinder, Thomas Dr., Shinder, Debra Littlejohn, Grasdal, Martin. <u>Configuring ISA</u> <u>Server 2000</u>. Rockland, MA: Syngress Media Inc. 2001

Simmons, Curt. <u>Microsoft ISA Configuration & Administration.</u> San Francisco: Hungry Minds, Inc. 2001

Appendix A

Cross	sover		Straight	Through
Ca	ble		Ca	ble
RJ-45	RJ-45		RJ-45	RJ-45
PIN	PIN		PIN	PIN
1 Rx+ 2 Rc- 3 Tx+ 6 Tx-	3 Tx+ 6 Tx- 1 Rc+ 2 Rc-	RJ-4511 Male	1 Tx+ 2 Tx- 3 Rc+ 6 Rc-	1 Rc+ 2 Rc- 3 Tx+ 6 Tx-

Appendix B – Routing and Remote Access (RRAS)

Enabling routing on a multi-homed Windows 2000 system is straightforward. Start RRAS from

Start => programs => Administrative tools => Routing and Remote Access. A right-click on the server (Watcher2K here) will display the screen below:



We are setting up a Network router

	}							
My Docum	ents	and Remote Access			_ 🗆 ×	1		
	Action	Routing and Remote Access Server	Setup Wizard	×				
My Comp	Tree Routing	Common Configurations You can select from several com	mon configurations.	<u></u>			×	
My Netw Place: Recycle		 Internet connection serve Enable all of the computers of Remote access server Enable remote computers to of Virtual private network (° Enable remote computers to of Network router Enable this network to comm 	er h this network to connect to the Ir dial in to this network. /PN) server sonnect to this network through the unicate with other networks.	iternet. e Internet.	ting, click ess	SA Server		
Intern Explori 100pdi		Manually configured ser Start the server with default s	rer ettings. < Back N	ext > Cancel		I ISA Server About		
		1				ting to ISA r		1
l	J			© 200	0 Microsoft Cc	prporation. All rights reserved	sl.	
Start	: 🛛 🗹 🌔	A Microsoft ISA Server Setup	Routing and Remote A	GSEC - WordPad				8:45 AM

Routing only IP



No dial out for us



The service starts up and you are presented with a screen much like this. You'll notice that I've named my interfaces internal net and external net. I renamed my interfaces at the *Network and Dial Up Connections* page (Right-click *My Network Places*).

You'll notice that the interfaces are enabled. You may also see that you've had Ethernet traffic (not shown here) in the *Incoming/Outgoing Bytes* column. The process is complete!

My Documents						
	Routing and Remote Acce	55				
	Action View					
My Computer	Tree	Routing Interfaces				_
	Reuting and Remote Access	LAN and Demand Dial Interf	∇ Type	Status	Connection S	Dev
	Server Status		Loopback	Enabled	Connected	
	🖻 🐻 WATCHER2K (local)	Internal Net	Dedicated	Enabled	Connected	Inte
Places	Routing Interfaces	External Net	Dedicated	Enabled	Connected	Inte
@	Remote Access Policie	اليې Internal	Internal	Enabled	Connected	
	🗄 🛅 Remote Access Loggin					
Recycle Bin						
Internet						
Explorer						
100pdisk						
			J		ļ	
🏽 🕄 🍊 🎲 🗍 🗐 Rou	uting and Remote A 🗒 GSEC	- WordPad 📃 🖻 Netw	ork and Dial-up Con			
N.S.						

Since this is our private network, let's use the RIP protocol. Right-clicking on General, we add a new routing protocol.





Sh. thill

Cycle through choosing both interfaces.





RIP is enabled when both interfaces appear as shown.