



# 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  
"Auditing Systems, Applications, and the Cloud (Audit 507)"  
at <http://www.giac.org/registration/gсна>

# **GSNA Practical Assignment v.1.2 (October 2001)**

## **Auditing Microsoft's Internet Security and Acceleration Server 2000 (Standalone Configuration) From A Business Point of View**

---

**Garrett ANDERSON**

**(January 2002)**

# Table of Contents

ISA Server (standalone configuration).....	1
Research .....	1
Audit Subject .....	1
Current State of ISA Server Auditing .....	2
Need for Improvement.....	3
Objective Elements .....	4
Subjective Elements .....	5
Checklist.....	6
Objective Tests .....	6
Documentation .....	6
Physical Security .....	7
ISA Server .....	8
Subjective Evaluation .....	27
Cost of Loss.....	28
Value of a Countermeasure .....	38
Audit.....	39
Description of the Audited Device and Its Environment.....	40
Organization .....	40
ISA Server .....	40
LAN.....	40
WAN.....	40
The Risks to the System.....	41
Audit Results .....	42
Physical Security .....	42
Post-Installation Image .....	42
Segregation of Roles .....	43
Simple TCP/IP Services.....	43
NIC Configuration .....	44
Intrusion Detection.....	45
IP Packet Fragmentation .....	47
Unnecessary Packet Filters .....	47
Web Publishing .....	49
Nessus / Nmap.....	49
Analysis.....	52
Evaluation of Audit Procedure .....	55
List of References .....	57
Printed .....	57

## Tables

Table 1 - Audit Subject .....	2
Table 2 - Tools for Objective Measurements.....	5
Table 3 - Level of Attraction.....	29
Table 4- Potential Degree of Damage Schedule.....	30
Table 5 - Risk Evaluation.....	34
Table 6 - Weighted Value for the Potential Degree of Damage .....	34
Table 7 - Vulnerability Multiplier .....	35
Table 8 - Sample Vulnerability Calculation .....	36
Table 9 - Exposure.....	37
Table 10 - Cost-of-Loss Example Calculation.....	38
Table 11 - Summary of the Audit Environment .....	41
Table 12 - Risks and Exploits to the Audited System.....	42
Table 13 - Evaluation of the Worth of Threaten Assets.....	53
Table 14 - Risk Rating Report Card .....	53
Table 15 - Cost of Loss thru Data Loss.....	54
Table 16 - Cost of Loss thru Denial of Service .....	54
Table 17 - Cost of Loss thru Misappropriation of Resources.....	55
Table 18 - Recommend Course of Action.....	55

© SANS Institute 2000 - 2002. Author retains full rights.

## Figures

Figure 1 - Advanced Settings Dialog .....	11
Figure 2 - Simple TCP/IP Services.....	12
Figure 3 - Mode Selection Dialog Box .....	13
Figure 4 - Construct LAT Dialog Box .....	15
Figure 5 – Authentication Type Dialog Box.....	16
Figure 6 - Outgoing Web Traffic Authentication .....	17
Figure 7 - IP Packet Filtering Properties (General Tab) .....	18
Figure 8 - IP Packet Filtering Properties (Intrusion Detection Tab) .....	19
Figure 9 - Test of Packet Fragmentation .....	20
Figure 10 - IP Fragment and Option Filtering .....	21
Figure 11 - Use Remote Default Gateway for VPN Clients .....	22
Figure 12- Allow All Protocol Rule .....	23
Figure 13 - HTTP Redirector Filter Properties Dialog Box.....	26
Figure 15 - Indication of a ISA Server being a Domain Controller .....	43
Figure 16 - Missing Simple TCP/IP Services .....	44
Figure 17 - External Interface on Audited System.....	45
Figure 18 - Intrusion Detection Enabled .....	46
Figure 19 - Detected Attacks are Not Enabled .....	46
Figure 20 - Event Journal: Detection of an Nmap Port Scan.....	47
Figure 21 - IP Packet Filters .....	48
Figure 22 - ICMP Time Exceeded Message .....	48

© SANS Institute 2000 - 2002. Author retains full rights.

# ISA Server (standalone configuration)

## Research

### Audit Subject

I have chosen as the subject of this paper Microsoft's Internet Security and Acceleration Server 2000 (ISA Server) in its standalone configuration. ISA Server is an application proxy firewall and that runs on Windows 2000 Server, Advanced Server and Datacenter versions. The current numerical version of the product is 3.0. ISA Server, as a product, is an "evolution" of Microsoft's Proxy Server 2.0.

The product is available in Enterprise and Standard editions. The Enterprise Edition permits setting up of an array of ISA Server and centrally managing their configuration via Active Directory. This facilitates the creation of an enterprise rulebase that can be deployed throughout an organization. The rulebase of each individual ISA Server can be further restricted depending on the organization's local requirements. Needless to say, this feature has a lot of advantages for a large organization. However, it comes at a cost and that is having an IT department that is large enough to manage it.

The other version, the Standard Edition, has the same firewall and proxy functionalities as the Enterprise Edition but it is limited to a "standalone" mode. The rulebase is unique to each ISA Server and it does not depend on presence of an Active Directory.

I have selected to limit this research paper to the "standalone" configuration for two reasons. One, an audit needs to have a definable scope. Because the Enterprise Edition is integrated into the Active Directory, an auditor has the additional responsibility to verify at least part of the Active Directory. Although this is certainly feasible, such a discussion would limit the value of this paper. It is more important to examine an ISA Server in its role as a perimeter security device than as a security aspect of Active Directory. Two, the standalone configuration is more likely to be encountered by an auditor. Although the Enterprise Edition will generate more cash for Microsoft, there will be more deployments in medium-size organizations of the standalone configuration. Most of these deployments will be "default" installations that by their very nature are security risks.

Both the Enterprise and Standard Editions can be installed in a "standalone" configuration. If the Active Directory is not configured for ISA Server, the Enterprise Edition will be installed in the "standalone" configuration.

Paper's Subject	
<b>Name:</b>	<b>Microsoft ISA Server 2000</b>
<b>Version:</b>	Standard Edition
<b>Version Number:</b>	3.0
<b>Type (Device, Program, System)</b>	Program
<b>Role:</b>	Firewall Proxy
<b>Description:</b>	A perimeter security device that controls access to and from the external via packet, circuit and application layer filtering. The program operations in three modes: Firewall, Cache and Integrated.

**Table 1 – Paper's Subject**

## **Current State of ISA Server Auditing**

ISA Server auditing is in its infancy. There is an active discussion of how one can configure it to perform this or that task but there is very little consolidated information as to what constitutes a secure configuration<sup>1</sup>. Basically, a “secure” configuration is being defined more in terms of what is an “insecure” configuration.

Tom Shinder's book, Configuring ISA Server 2000<sup>2</sup>, is by far the best source of information on the security aspects of an ISA Server. In fact, Chapter 3 is entitled “Security Concepts and Security Policies”.

Throughout my research I was impressed by the mass of information on ISA Server. I was also very surprised by the absence of audit checklists. There are checklists in the help file<sup>3</sup> on how to install or deploy ISA Server but there are no checklists listing what parameters need to be configured in order to have a secure configuration. Neither Tom Shinder's book or Microsoft website contains such checklists. In fact, a search of the Microsoft's ISA Server site using the keywords “checklist” and “security” yields only the ISA help file and installation guide.

Confronted with this situation, I looked at more general firewall checklists. Three sources stood out above the others. Lance Spitzner's paper, “Auditing Your Firewall Setup”<sup>4</sup> is excellent. Although it is not a detailed checklist, it contains the right amount of information to help someone through the initial steps. There is an overwhelming amount of information on firewalls and that is both a “help” and a “hindrance”. This paper gets you over this initial obstacle.

The next source is the SANS course “Auditing Routers and Firewalls” by Stephen Northcutt<sup>5</sup>. This may seem strange to cite this source when one considers that this paper is part of the SANS certification process. However, after reviewing a number of other sources, this is the only source of information that came close to providing a well-rounded Firewall Auditing Checklist.

<sup>1</sup> Discussion can be found at <http://www.isaserver.org> or [news://msnews.microsoft.com/microsoft.public.isaserver](http://news.microsoft.com/microsoft.public.isaserver).

<sup>2</sup> Dr. Thomas W. Shinder, Configuring ISA Server 2000 – Building Firewalls for Windows 2000.

<sup>3</sup> Filename: isa2k.chm.

<sup>4</sup> Lance Spitzner, “Auditing Your Firewall Setup”, <http://the.wiretapped.net/security/info/papers/security/lance-spitzner/audit.html>

<sup>5</sup> Stephen Northcutt, Track 7 – Auditing Networks, Perimeters and Systems, (<http://www.sans.org>), presented at the SANS Conference, San Diego, California, October 2001

Finally, Krishni Naidu's Firewall Checklist<sup>6</sup> can only be described by an oxymoron: a very detailed general checklist. Although this checklist cannot be applied to an ISA Server "as is", it has enough technical detail to build a checklist for an ISA Server.

One thing characterizes the general firewall checklists. They all are technology-oriented. Of course, this is normal but it highlights the lack of attention that the audit process pays to business issues.

In summary, the following points characterize the current state of ISA Server auditing.

- ISA Server Auditing is new.
- There are no ISA Server Auditing Checklists.
- General Firewall Auditing Checklists cannot be applied "as is".
- Firewall auditing lacks attention to business issues.

## Need for Improvement

The need to improve the current situation with regard to ISA Server auditing comes down following points.

1. General checklists lack the detailed information needed for an ISA Server audit.
2. Firewall auditing needs to be both technology and business oriented.

To use Krishni Naidu's Firewall Checklist as an example to highlight the first point, Item 12 refers to SSH. Secure Shell is not normally a part of a Windows 2000 system. (It could be, though). Item 13 instructs the auditor to insure that FTP is placed in a different subnet from the protected. "Publishing" a FTP server (as it is called in ISA terminology) in such a manner would probably necessitate the deactivation of the FTP's server protection against a FTP Bounce Attack<sup>7</sup>. Not necessarily a good idea. However, the essence of both points, "don't communicate in the clear" and "protect your network from FTP", do apply to an ISA Server but the details do not.

With regard to the second point, both an ISA Server and an audit exist to support a business activity. Coming from technology a background, people who audit firewalls tend to look them from a technology standpoint.

Recently while working for a client, I was presented with an audit that was performed by a major "computer manufacturer / service provider". The audit entailed the review of the security at two "off-shore" sites. Of course, the pitiful security situation was well known throughout the company. After one week of on-site inspections and an "impressive" invoice, a list of the security violations and ways to correct them was presented. Nowhere in the document was there any information on the value of fixing the problems. (I am talking about "value" of a countermeasure in terms of its "return on investment" and not its actual cost of acquisition).

---

<sup>6</sup> See Krishni Naidu's Firewall Checklist at [http://www.sans.org/checklist/firewall\\_check.htm](http://www.sans.org/checklist/firewall_check.htm). Another good place to replace to visit is [http://rr.sans.org/firewall/firewall\\_list.php](http://rr.sans.org/firewall/firewall_list.php).

<sup>7</sup> This is a socket pooling and IIS 5.0 issue. See [http://www.isaserver.org/shinder/tutorials/ftp\\_on\\_isa.htm](http://www.isaserver.org/shinder/tutorials/ftp_on_isa.htm).



Businesses live in a real world that is full of risk. We, as investors, are always looking to make the “big killing”. But the bigger return always comes to those who are willing to assume the most risk. Also, the biggest losses go to those who unfortunately assumed the most risk. Those who assume little or no risk, have little or no return on their investment. This remark can certainly be condemned as an over simplification. But we would all agree that we use “return on investment” as a criteria when we measure the efficiency of a manager. Being a good manager, then, implies that that person has to be very lucky or he has to be someone who can weigh risk and work effectively with uncertainty.

Auditing of such high-cost items as information systems and their security features needs to present the value of the countermeasures that it proposes as recommendations. Some may say that auditing of technical systems should be limited to technical aspects. “Does it work or doesn’t?” Of course, that is the *raison-d’être* of audit. But, this question leads to another. “Do we fix it or not?” In my opinion, this is a necessity that is being ignored.

Some may argue that a technical auditor is not capable of making such business assessments. Considering the gap between business issues, on the one hand, and technological issues, on the other, I would argue that the technical person is the only one who can bridge this gap. Think about it for a moment. How many sales managers and accountants are using Linux on their workstations? “Technical” people have to make the effort to bridge this gap. “Business” people just will not do it.

It was from this prospective that I developed a checklist to audit an ISA Server. The primary sources that I used were:

- A test platform
- Tom Shinder’s book, Configuring ISA Server 2000<sup>8</sup>.
- Kim Simmon’s book, ISA Server 2000<sup>9</sup>.
- John Carroll’s book, Computer Security<sup>10</sup>.
- Microsoft’s Course 2160A, “Déploiement et gestion de Microsoft Internet Security and Acceleration Server 2000”<sup>11</sup>.
- <http://www.isaserver.org>

## Objective Elements

As with any firewall checklist, follow points can be measured objectively.

- The presence of documentation.
- The hardware configuration.
- The basic software configuration.

---

<sup>8</sup> Dr. Thomas W. Shinder, Configuring ISA Server 2000 – Building Firewalls for Windows 2000. I had a very nice email discussion with Tom on need for an auditing checklist. He is working on writing one for the <http://www.isaserver.org> site.

<sup>9</sup> Kim Simmons, MCSE ISA Server 2000.

<sup>10</sup> John Carroll, Computer Security.

<sup>11</sup> I took the course in France. As a side note, there were a lot of stability problems with the French version of ISA Server. In fact, the instructor announced the SP2 for W2K deactivated the VPN function of RRAS.

- The state of the ports.
- The presence of services.
- The presence of a particular type of network traffic.

Tools that can be used to measure these items are presented in Table 2 - Tools for Objective Measurements.

Tools		
Name	Description	Source
<b>Nmap (Nmapnt)</b>	Port Scanner	<a href="http://www.insecure.org/nmap">http://www.insecure.org/nmap</a> <a href="http://www.eeye.com/html/Research/Tools/nmapnt.html">http://www.eeye.com/html/Research/Tools/nmapnt.html</a>
<b>Nessus</b>	Vulnerability Scanner	<a href="http://www.nessus.org">http://www.nessus.org</a>
<b>Hping2</b>	Packet generator	<a href="http://www.hping.org/">http://www.hping.org/</a>
<b>Tcpdump (Windump)</b>	Sniffer	<a href="http://www.tcpdump.org/">http://www.tcpdump.org/</a> <a href="http://netgroup-serv.polito.it/windump/">http://netgroup-serv.polito.it/windump/</a>
<b>Fport</b>	Utility: port number / program name	<a href="http://www.foundstone.com/knowledge/free_tools.html">http://www.foundstone.com/knowledge/free_tools.html</a>
<b>Netstat</b>	Utility: port numbers	Part of the W2K
<b>Network Monitor</b>	Sniffer	Delivered with W2K Server
<b>ISAinfo.vbs</b>	Diagnostic Tool.	<a href="http://www.isaserver.org/pages/learning%20zone.htm#free">http://www.isaserver.org/pages/learning%20zone.htm#free</a>

**Table 2 - Tools for Objective Measurements**

Most of these tools are Unix-based. During my testing, I came to the conclusion that it is best to use the Unix version of any network “scanning” tools. Apparently the Windows 2000 NDIS architecture does not lend itself very well to the level of manipulation that some of these scanning tools require.

Remember that measure objective elements of any firewall checklist can only go so far. A firewall is system within itself as well as being part of a bigger system. A system is the sum of its parts. The overall value of an objectively measured element can be influenced by other elements. Moreover, binary conditions are measurable while qualitative evaluations still have an element of subjective.

## Subjective Elements

There are a large number of elements that are tied to the operation of an ISA Server that can only be measured subjectively. For example, management’s attitude toward security, the competence of the system administrator and the morale of the employees are all elements that contribute to the security that is provided by an ISA Server. The elements can only be measured subjectively.

Because subjective elements have more impact on the business-side of an ISA Server audit, I have group into the following “global” subjective elements.

- Cost of Loss
- Value of a Countermeasure

When an element is measured subjectively, the concept of degree has to be considered. “Excellent, Very Good, Good, Poor, Very Poor” is an example of degrees by which subjective elements can be measured. Because we can measure these elements on a scale, we need to assign quantitative values to our assessment. All of this may seem confusing for the moment but it is necessary to the “business” part of the audit.

## Checklist

### Objective Tests

#### Documentation

Acceptable Use Policies	
<b>Test</b>	Are they published?
<b>Out of Spec Condition</b>	Not published.
<b>Description:</b> Acceptable Use Policies need to be published for computer materiel utilization, Internet Access, and Email Use. The auditor should also make of subjectively evaluation of the quality with regard to the company’s objective and overall security.	

Security Policies	
<b>Test</b>	Are they published?
<b>Out of Spec Condition</b>	Not published.
<b>Description:</b> The organization needs to have a published a security policy that covers physical security, computer operations and networking. Pay particular attention to the fact that it is published. Some organizations have purchased “securities policies” that they do not publish.	

Change Control Policy for ISA Configuration	
<b>Test</b>	Are they published?
<b>Out of Spec Condition</b>	Not published.
<b>Description:</b> A change control policy needs to cover the responsibilities and actions. Who approves a change? Who implements a change? Who verifies that the change has been properly implemented? Are backups of the configuration required prior to every change?	

<b>Operational Procedures and Checklists</b>	
<b>Test</b>	Are they being used?
<b>Out of Spec Condition</b>	Complete absence of procedures and checklists.
<b>Description:</b> Operational Procedures and Checklists are very important regardless of the size of an organization. The quality of the procedures and checklists need to be weighed in relationship to the size of the organization. A small organization may have only very general procedures.	

<b>ISA Server Logbook</b>	
<b>Test</b>	Is it maintained?
<b>Out of Spec Condition</b>	No ISA Server Logbook.
<b>Description:</b> A logbook needs to be maintained of the ISA Server. It should document that server's configuration and record any modifications.	

### ***Physical Security***

<b>Access Control</b>	
<b>Test</b>	Is there access control?
<b>Out of Spec Condition</b>	Unauthorized personnel can gain physical access to the server.
<b>Description:</b> Access control is very important. An unprotected ISA Server would be a prime target during a physical security attack <sup>12</sup> .	

<b>Fire Prevention / Suppression</b>	
<b>Test</b>	Are Fire Prevention / Suppression in place?
<b>Out of Spec Condition</b>	Absence of a fire extinguisher.
<b>Description:</b> Outside of being a fairly obvious physical security issue, fire prevention is an indication of management's attitude toward security.	

<b>Universal Power Supply</b>	
<b>Test</b>	Installed?
<b>Out of Spec Condition</b>	Absence.
<b>Description:</b> In a strange way, a power outage can be considered as a denial of service attack. Although the internal network would still be protected in the event of an outage, the ISA Server is no longer fulfill its role of providing secure access to the Internet.	

<sup>12</sup> Eric Cole, Hackers Attention Danger!, p. 729.

## ISA Server

### Installation

Minimum Recommended Hardware / Software Requirements	
Test	Are the hardware and software requirements met?
Out of Spec Condition	No meeting anyone of the minimum requirements.
<p><b>Description:</b> The recommended requirements are as followings:</p> <p>Hardware</p> <ul style="list-style-type: none"><li>• <b>Processor: Pentium II 300mHz</b></li><li>• <b>RAM: 256mB</b></li><li>• <b>Disk Space: 2.2gB</b></li><li>• <b>NIC: 2</b></li></ul> <p>Software:</p> <ul style="list-style-type: none"><li>• <b>OS: Windows 2000 Server, Advanced Server or Datacenter</b></li><li>• <b>Service Pack Level: 2</b></li></ul> <p>This information can be obtained by running <i>msinfo32.exe</i>.</p>	

Post-Installation Image	
Test	Is there a post-installation disk image?
Out of Spec Condition	Absence.
<p><b>Description:</b> ISA Server in its standalone Standard Edition version is very difficult to backup. This is due to three facts.</p> <ol style="list-style-type: none"><li>1. NSBackup does not backup the ISA Server Configuration.</li><li>2. The ISA Server Configuration Backup Utility does not backup the system state.</li><li>3. ISA Server is machine-dependent.</li></ol> <p>Simply reinstalling the OS and ISA Server and then “importing” the configuration file will not work. The best and only backup solution is to make a disk image immediately after the installation is completed. Next, regular backup of the ISA Server configuration need to be made. In the event that restoration becomes necessary, load the image and then restore the ISA Server Configuration backup.</p>	

## Windows 2000 Host

Security Configuration	
Test	Have the security template(s) been applied?
Out of Spec Condition	No templates have been applied.
<b>Description:</b> ISA Server is configured and administered through a MMC plug-in call the ISA Management Console. When the plug-in is started for the first time, a configuration wizard comes up. This wizard will guide the system administrator through the configuration process. One part of this process is the security configuration of the underlying machine; in other words, Windows 2000 itself. A dialog box presents three different level of security: Secure, Limited Services, and Dedicated. This is somewhat obscure as there is very little information given to the user as to what these levels mean in terms of what is happening to the underlying OS. Other sources indicate the meaning of the three levels. <sup>13</sup>	

Security Level	Server Templates	Domain Controller Templates
Secure	Basicsv.inf	Basicdc.inf
Limited Services	Securiews.inf	Securedc.inf
Dedicated	Hisecws.inf	Hisecdc.inf

How the security for the Windows 2000 machine is setup is not really a part of ISA Server audit. It should be verify for no obvious security breaches. The essential thing is to verify that ISA Server has been installed as “default” installation. Neither the installation nor the operation of the ISA Server requires that the underlying OS security be configured.

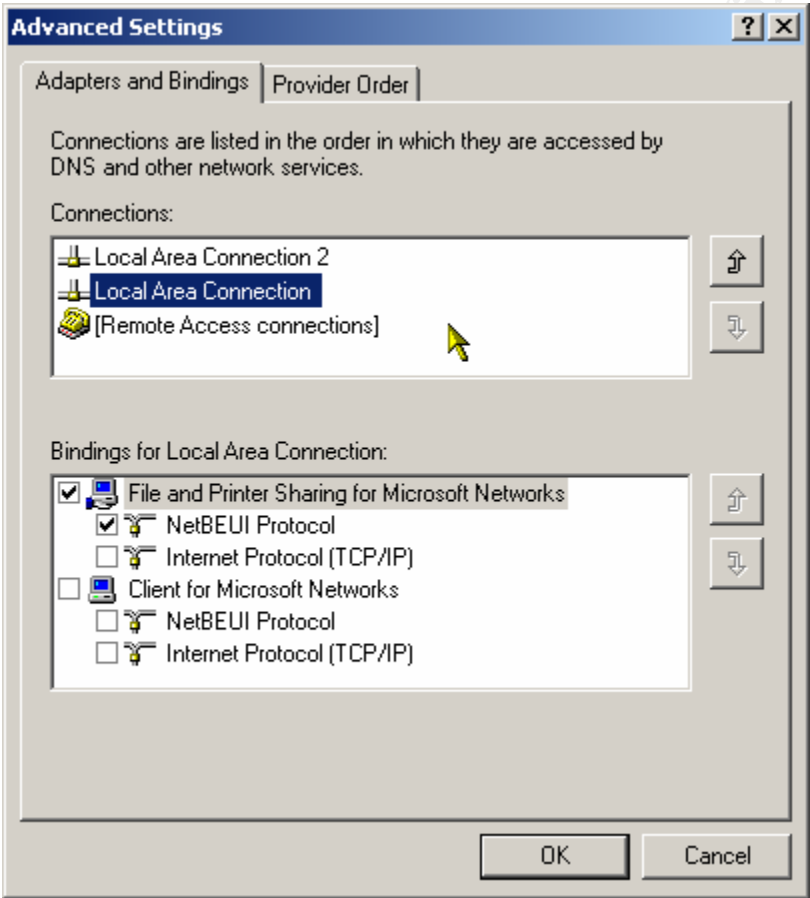
An auditor can verify the application of security templates via the Security Configuration and Analysis MMC plug-in.

Segregation of Roles	
Test	Are other unnecessary roles active on the ISA Server?
Out of Spec Condition	Yes.
<p><b>Description:</b> An ISA Server that is fulfilling the role of a perimeter security devise should be dedicated to the role. However, ISA Server is an application firewall and there is nothing in the design of ISA Server that blocks the machine that it is running from being used for other roles. In fact, an ISA Server can also be a domain controller. This is a very dangerous situation but in some very small organization it may be necessary. If no other machines are available, then this would constitute a risk but not an “out of spec” condition.</p> <p>To verify if the ISA Server is fulfilling other roles, an auditor can check the installed programs from the control program. If the ISA Server is also a domain controller, the Local Users and Groups node of the Computer Management MMC plug-in will have a white “X” in a red circle.</p>	

<sup>13</sup> Kim Simmons, MSCE ISA Server 2000 Exam Prep, p.267

<b>NTFS</b>	
<b>Test</b>	Are system / boot volumes the NTFS?
<b>Out of Spec Condition</b>	No.
<p><b>Description:</b> It is very unlikely that an audit will encounter this condition, however, it is possible. The ISA Server only requires the disk will the cache data is storage be formatted NTFS. Thus, it is possible to have a dual-booted PC being used as an ISA Server. The ISA Server should be dedicated. Additional roles can be tolerated in extreme situation. The risk that a non-secure OS could be booted on a machine that is setting on the network perimeter is totally unacceptable.</p> <p>To verify this condition, the auditor needs to use the Computer Management MMC plug-in (Disk Management node).</p>	

© SANS Institute 2000 - 2002, Author retains full rights.

Network Interface Card Configuration	
Test	Are dangerous services active on external adapters?
Out of Spec Condition	Yes.
<p><b>Description:</b> Dangers services are File and Printer Sharing and Clients for MS Networks. There could be others though depending on how the machine is set up. The dangers services normally removed from external adapters. Dialup connections also need to be check. For “permanent” connections, an auditor can verify Advanced Settings Dialog Box (Network and Dialup Connections / Advanced / Advanced Settings).</p>	
	
Figure 1 - Advanced Settings Dialog	

Network Monitor Installed	
Test	Is Network Monitor Installed?
Out of Spec Condition	No.
<p><b>Description:</b> Network Monitor is delivered with all versions of Windows 2000 except Professional. It is a convenient way to quickly monitor traffic that is going through the ISA Server. In the event that an intrusion is suspected, this is one built-in monitoring tool that could come in handy. In any case, there is no reason not to install it.</p>	



### Simple TCP/IP Services – Not Installed

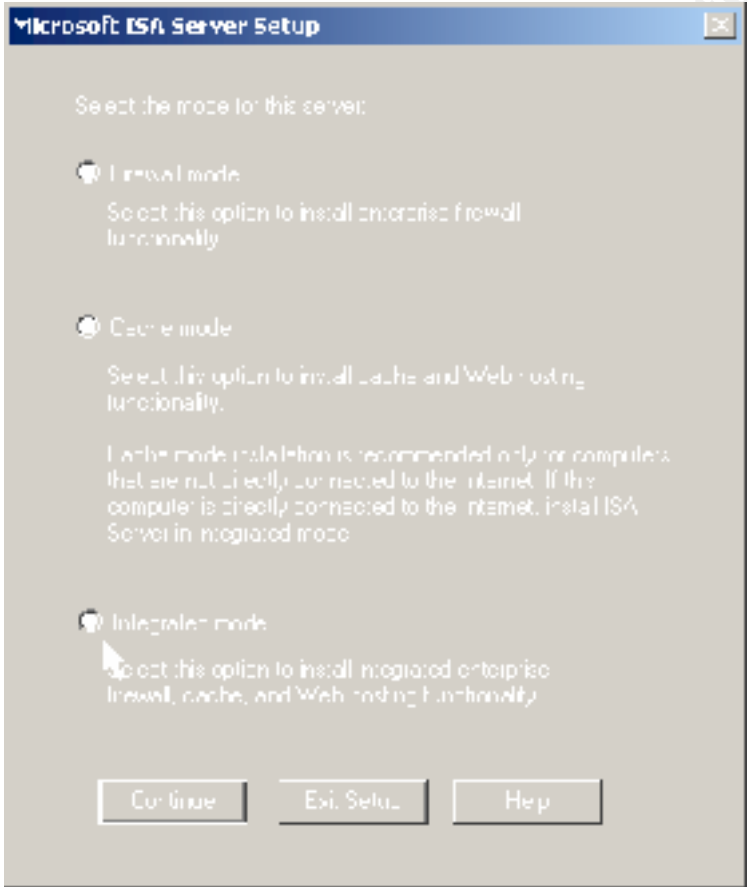
<b>Test</b>	Are Simple TCP/IP Service installed?
<b>Out of Spec Condition</b>	Yes.

**Description:** On an ISA Server, there is no need for these services. An auditor can very easily verify this point with a “netstat –an”. The presence of ports 7, 9, 13, 17, and 19 indicate that Simple TCP/IP Services are install.

```
CMD
TCP    192.168.0.33:1311    63.121.29.7:80
TCP    192.168.0.33:1313    63.121.29.7:80
TCP    192.168.0.33:1315    63.121.29.7:80
TCP    192.168.0.33:1317    63.121.29.7:80
TCP    192.168.0.33:1319    63.121.29.7:80
TCP    192.168.0.33:1396    63.121.29.7:80
TCP    192.168.0.33:1411    63.121.29.7:80
UDP    0.0.0.0:7           *:
UDP    0.0.0.0:9           *:
UDP    0.0.0.0:13          *:
UDP    0.0.0.0:17          *:
UDP    0.0.0.0:19          *:
UDP    0.0.0.0:135         *:
UDP    0.0.0.0:445         *:
UDP    0.0.0.0:1029        *:
UDP    0.0.0.0:1037        *:
UDP    0.0.0.0:3456        *:
UDP    127.0.0.1:1444       *:
UDP    127.0.0.1:1555       *:
UDP    127.0.0.1:1664       *:
UDP    127.0.0.1:2147       *:
UDP    192.168.0.33:5000    *:
C:\WINNT>
```

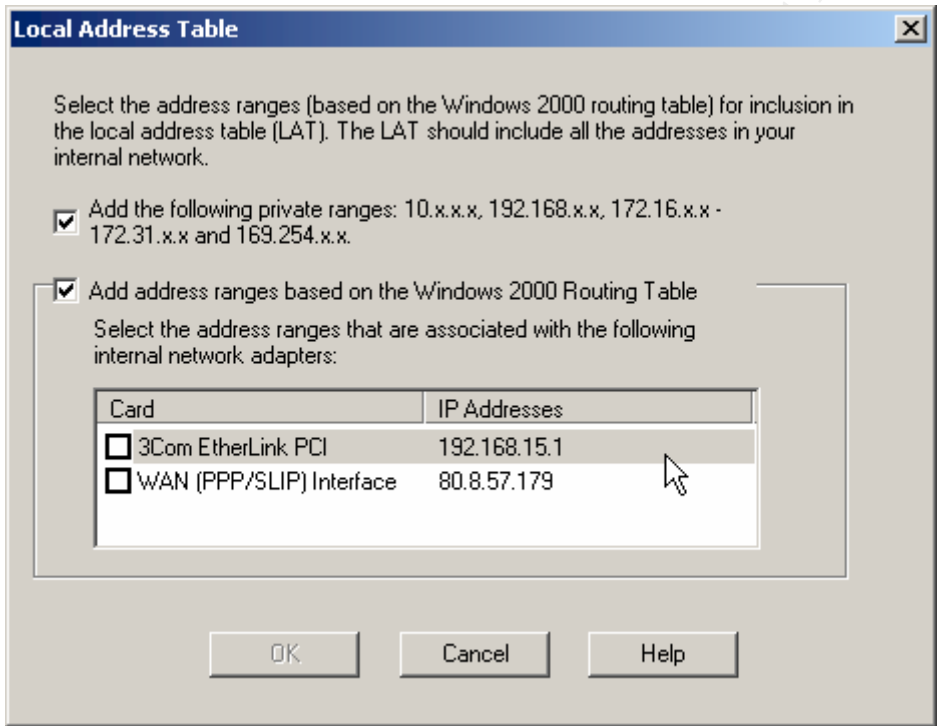
Figure 2 - Simple TCP/IP Services

## Configuration

Integrated Mode Enabled	
Test	Was ISA Server installed integrated mode?
Out of Spec Condition	No.
<p><b>Description:</b> ISA Server can be installed in one of three modes: Firewall, Cache and Integrated. Integrated mode should be selected for a standalone configuration because it will provide better monitor for Internet traffic. An auditor can determine is the Integrated mode has been selected by the presence of the Web Proxy Service.</p>  <p>The screenshot shows the 'Microsoft ISA Server Setup' window. It prompts the user to 'Select the mode for this server:'. There are three radio button options: 'Firewall mode' (with a description to install encrypted firewall functionality), 'Cache mode' (with a description to install cache and Web hosting functionality, and a note that it's recommended only for computers not directly connected to the Internet), and 'Integrated mode' (with a description to install integrated enterprise firewall, cache, and Web hosting functionality). The 'Integrated mode' radio button is selected. At the bottom are 'Continue', 'Exit Setup', and 'Help' buttons.</p>	
<b>Figure 3 - Mode Selection Dialog Box</b>	

Hotfixes installed	
Test	Are the latest hotfixes installed?
Out of Spec Condition	No.
<p><b>Description:</b> A list of the bugs and hotfixes for ISA Server can be found at <a href="http://www.isaserver.org/pages/bugs/patches.htm">http://www.isaserver.org/pages/bugs/patches.htm</a>. The ISAinfo.vbs will check the registry and report what hotfixes have been applied. ISAinfo.vbs can be obtained at <a href="http://www.isaserver.org/pages/learning%20zone.htm#free">http://www.isaserver.org/pages/learning%20zone.htm#free</a>. An auditor can also check to see what hotfixes have been install by looking at the registry key <b>HKLM/Software/Microsoft/FPC/Hotfixes</b>.</p>	

© SANS Institute 2000 - 2002, Author retains full rights

Local Address Table – only necessary addresses	
<b>Test</b>	Does LAT contain only the addresses of the internal network?
<b>Out of Spec Condition</b>	No.
<p><b>Description:</b> The Local Address Table includes of the addresses the make out the internal network. During installation process, it is possible to automatically construct the LAT. This does simplify the installation process but it adds RFC1918 addresses to the LAT. The presence of all the RFC1918 addresses is an indication of a default installation – Vulnerability #1 on the SANS/FBI Top 20<sup>14</sup>. An auditor can verify the address range in the LAT through the ISA Management Console MMC plug-in.</p>	
	
<p><b>Figure 4 - Construct LAT Dialog Box</b></p>	

<sup>14</sup> <http://www.sans.org/top20.htm>.

Authentication – Incoming Web Traffic	
Test	Is Basic Authentication authorized?
Out of Spec Condition	Yes.

**Description:** With ISA Server, it is possible to publish websites and do reverse caching. In this case, ISA Server will handle the incoming authentication on the behalf of the client. Four types of authentication are offered: Basic, Certificate, Digest and Integrated. Because Basic Authentication is not secure in that it transmits the password in Base64, it should not be permitted. The authentication is configured on the ISA Server properties page.

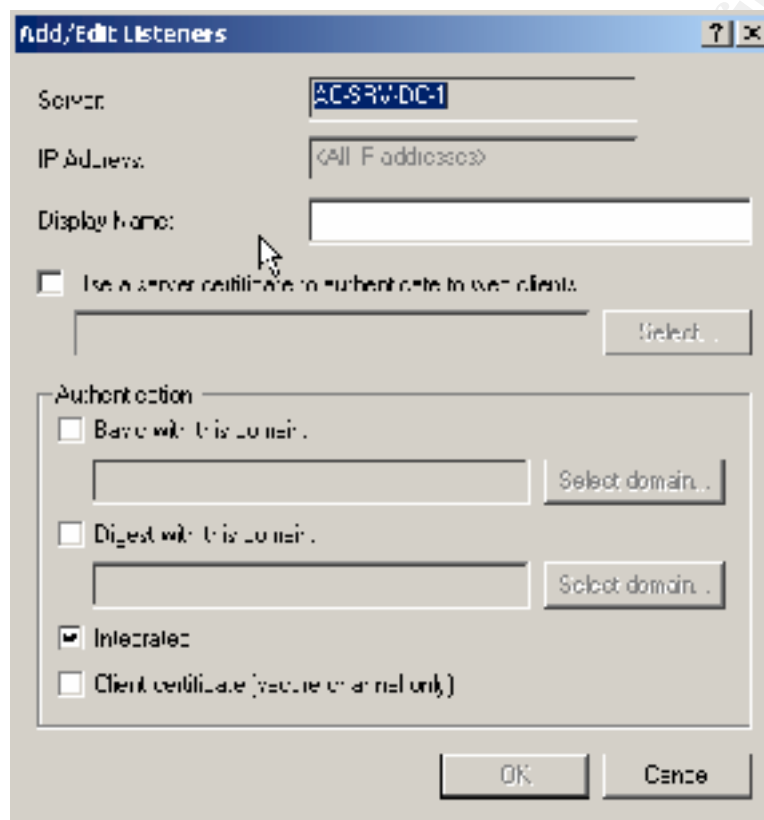


Figure 5 – Authentication Type Dialog Box

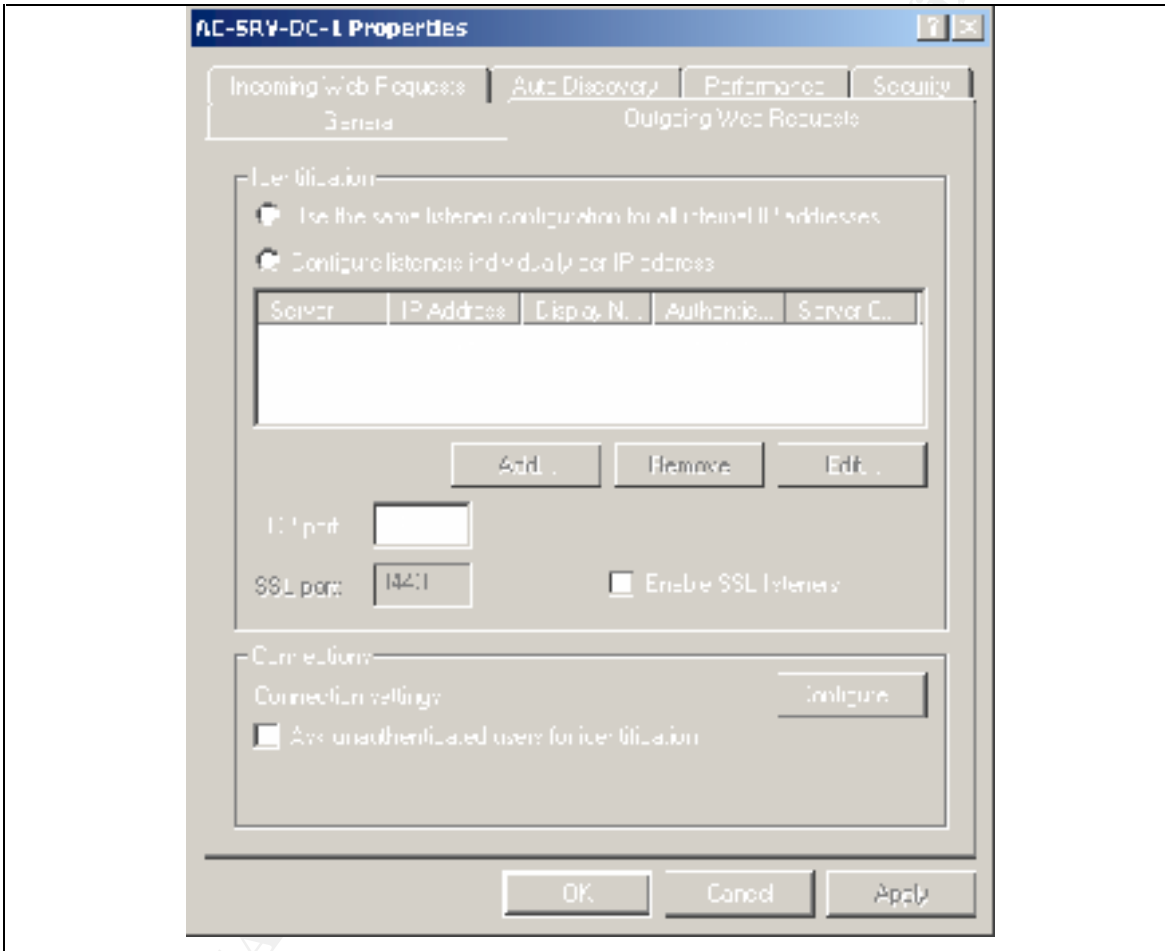
Another method to test this condition is with tcpdump. While capturing packets, request a protected web page. The HTTP header from the website will indicate the type of authorization that is permitted by the ISA Server.

## Authentication – Outgoing Web Traffic

<b>Test</b>	Is authentication for unauthenticated users required?
-------------	---

<b>Out of Spec Condition</b>	No.
------------------------------	-----

**Description:** Outgoing web traffic is logged by ISA Server. Unless the “Ask unauthenticated users for identification” checkbox is checked, the log records users as “anonymous”. When the checkbox is checked, usernames are recorded in the log and unauthenticated users (i.e., users connected to the internal network but not logged in) are asked for a username and password.



**Figure 6 - Outgoing Web Traffic Authentication**

## IP Packet Filtering Enabled

<b>Test</b>	Is IP Packet Filtering Enabled?
<b>Out of Spec Condition</b>	No.

**Description:** IP Packet Filtering is enabled by default. It only applies to the external interface of an ISA Server. There is only one situation when it is acceptable to disable this functionality and that is when ISA Server is on the inside of a back-to-back firewall configuration (i.e., two firewalls with the DMZ in the middle).

In addition to verifying the configuration parameter, an auditor should verify via Nmap. “nmap -sT -p0 <IP of External Interface>” will all open ports if IP Packet Filtering is not enabled.

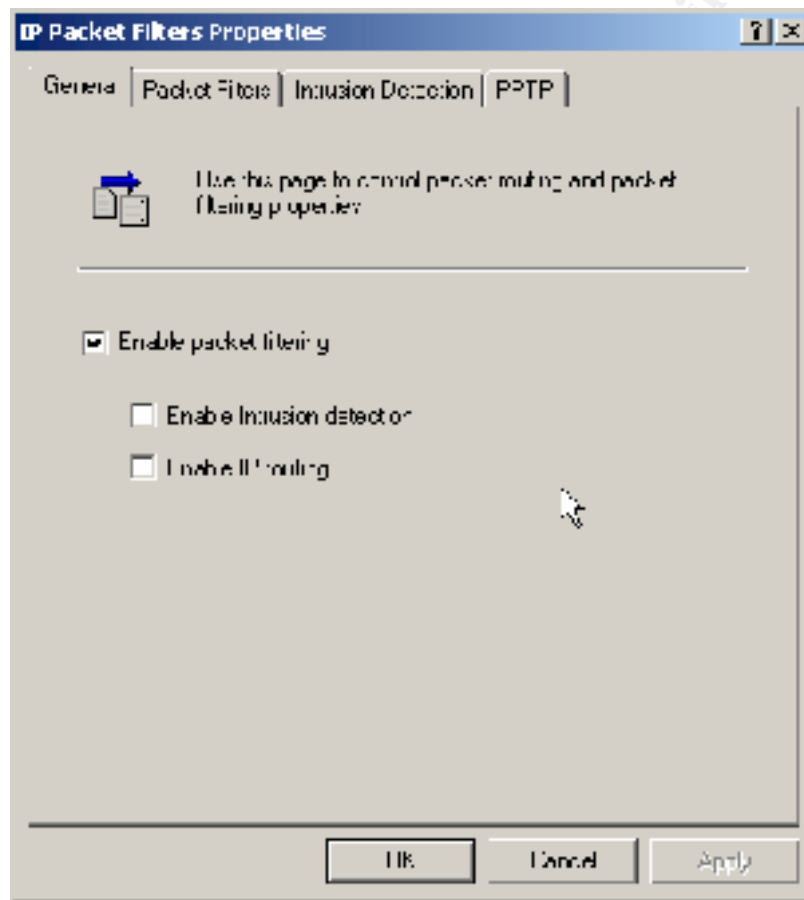
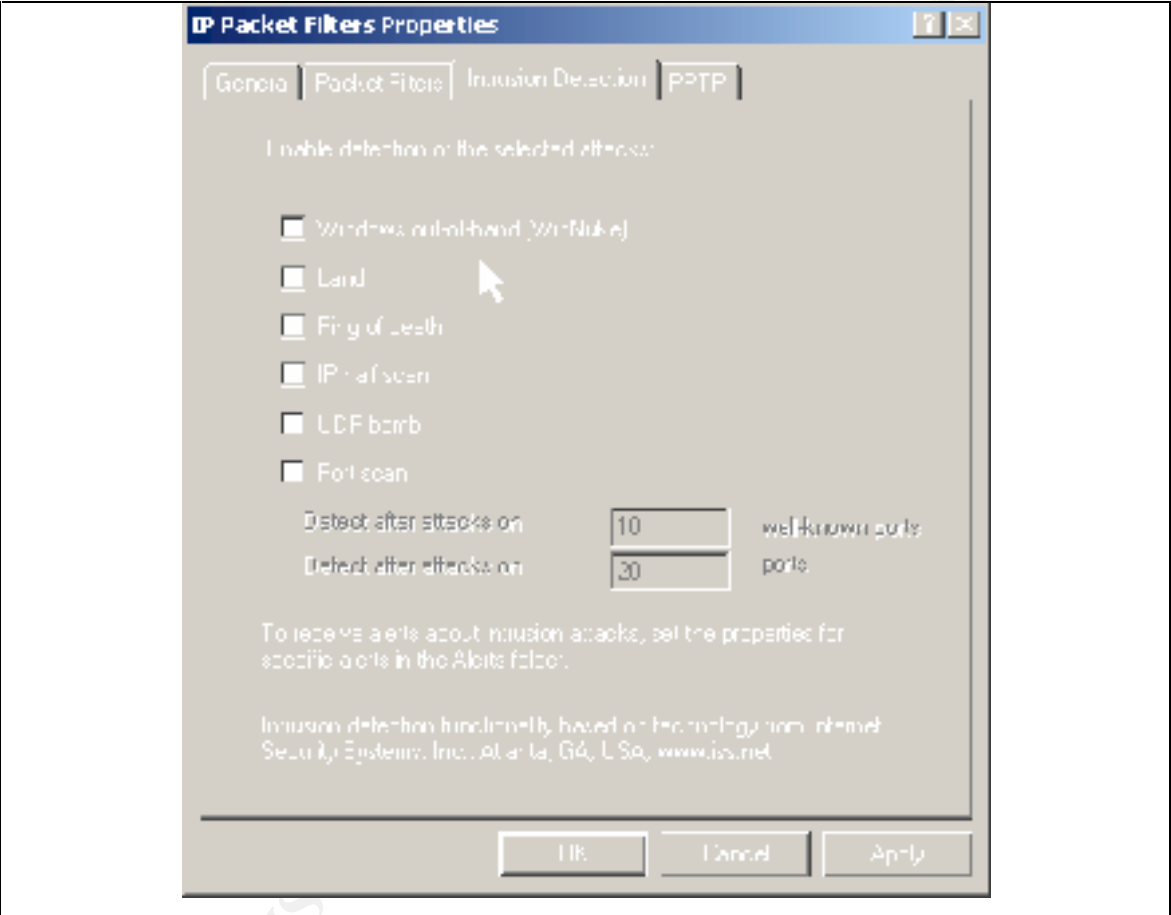


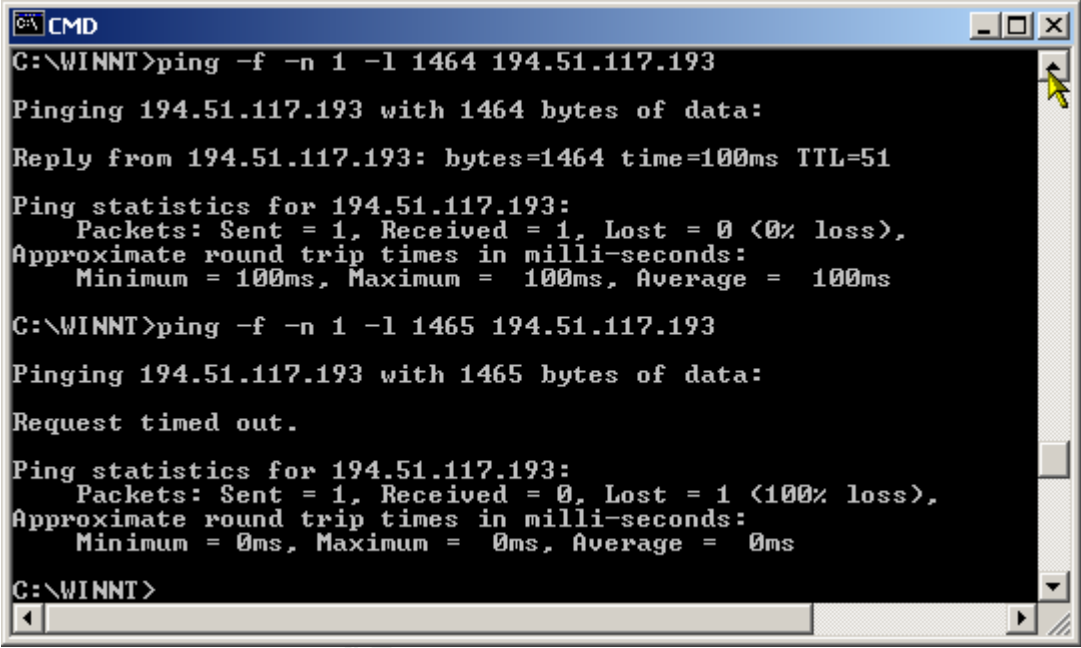
Figure 7 - IP Packet Filtering Properties (General Tab)

Intrusion Detection Enabled	
Test	Is Intrusion Detection enabled?
Out of Spec Condition	No.
<p><b>Description:</b> By default, intrusion detection is not enabled. It needs to be. The auditor should verify the IP Packet Filtering Properties dialog box, do an “nmap -sT -P0 &lt;IP of External Interface&gt;”, and review the Application Event Journal. The port scan will be detected if intrusion detection is enabled.</p>	
	
Figure 8 - IP Packet Filtering Properties (Intrusion Detection Tab)	

Intrusion Alerts – Emailed	
Test	Are intrusion alerts being emailed to the system administrator?
Out of Spec Condition	No.
<p><b>Description:</b> By default, intrusion alerts are only logged to the event journal. They should be configured to send an email to the system administrator. The auditor should verify that they are configured in the Monitoring / Alerts node of the ISA Management Console MMC plug-in. If they are configured, the auditor should then do a port scan and verify with the system administrator that an email was generated.</p>	



## IP Packet Fragmentation Filtering Enabled

Test	Is IP Packet Fragmentation Filtering enabled?
Out of Spec Condition	No.
<p><b>Description:</b> By default, this option is not enabled. It should be in order to avoid “packet fragmentation” exploits, such as Jolt2<sup>15</sup>. To verify this condition, the auditor should insure that it is enabled, create a IP Packet Filter for the ICMP Echo Reply and the do a fragmented ping to the external interface. If it is impractical to enable an echo reply, a verification of the IP Packet Filtering log (IPEXTD&lt;date&gt;) should indicate the block traffic: “ICMP 8 0 Fragment Block”.</p> 	

```
C:\WINNT>ping -f -n 1 -l 1464 194.51.117.193

Pinging 194.51.117.193 with 1464 bytes of data:

Reply from 194.51.117.193: bytes=1464 time=100ms TTL=51

Ping statistics for 194.51.117.193:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 100ms, Maximum = 100ms, Average = 100ms

C:\WINNT>ping -f -n 1 -l 1465 194.51.117.193

Pinging 194.51.117.193 with 1465 bytes of data:

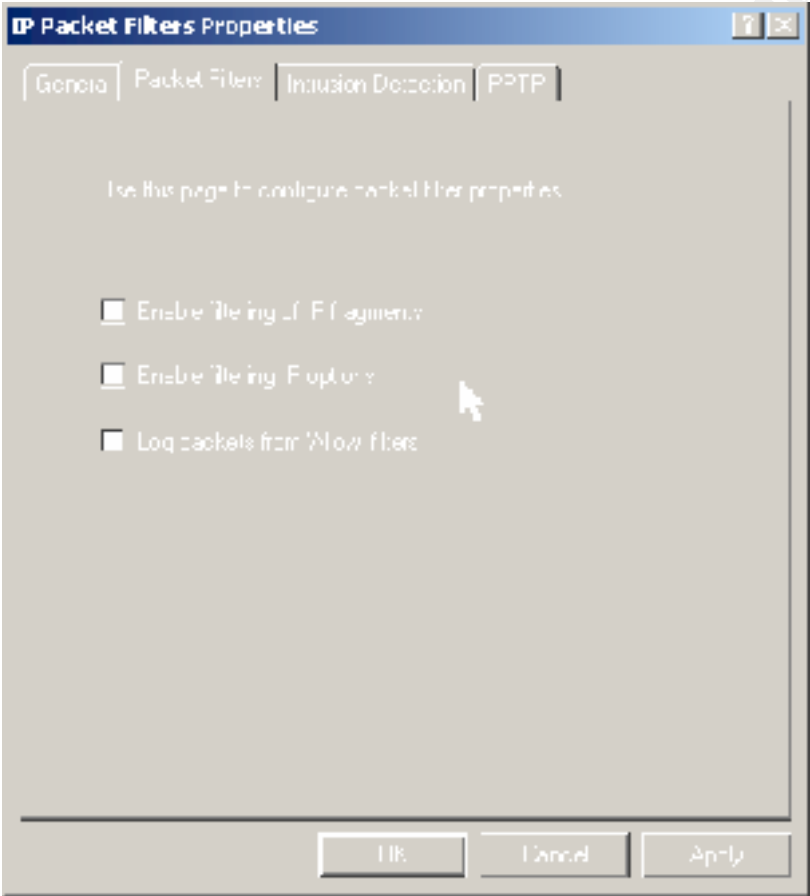
Request timed out.

Ping statistics for 194.51.117.193:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\WINNT>
```

Figure 9 - Test of Packet Fragmentation

<sup>15</sup> Eric Cole, Hackers Attention Danger!, Pp. 214-215.

IP Option Filtering Enabled	
Test	Is IP Option Filtering enabled?
Out of Spec Condition	No.
<p><b>Description:</b> This option is not enabled by default. It needs to be enabled in order to protect the ISA Server from exploits that use the IP Options. If it is enabled and intrusion detection is enabled as well, a “nmap -sX -P0 -p 80 &lt;IP of External Interface&gt;” will be indicated in the event journal.</p>	
 <p>The screenshot shows the 'IP Packet Filters Properties' dialog box with the 'Packet Filter' tab selected. The dialog contains three unchecked checkboxes: 'Enable Filtering of Fragments', 'Enable Filtering of Options', and 'Log packets from 'Allow' filters'. The 'OK', 'Cancel', and 'Apply' buttons are visible at the bottom of the dialog.</p>	
<p><b>Figure 10 - IP Fragment and Option Filtering</b></p>	

## VPN Clients – Use Remote Default Gateway

<b>Test</b>	Are VPN clients required to “Use Remote Default Gateway”?
<b>Out of Spec Condition</b>	No.

**Description:** VPN traffic is “private”. This condition creates a number of security problems. One very serious situation occurs when VPN users that can connect to the LAN and at the same time connect to other sites via their ISP’s default gateway. When this happens, all protocol rules are circumvented. To avoid this problem and insure that other Internet traffic for a VPN client is going through the ISA Server, the “Use Remote Default Gateway” checkbox needs to be checked when the VPN client is configured.

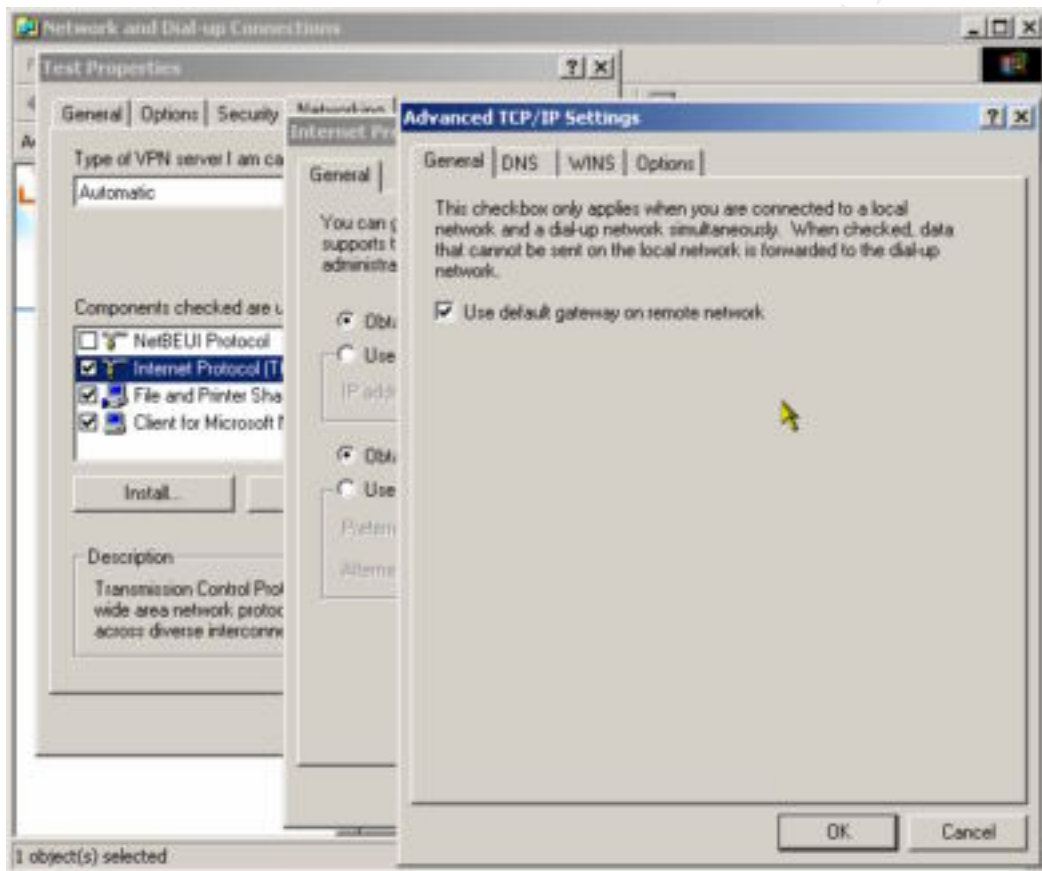
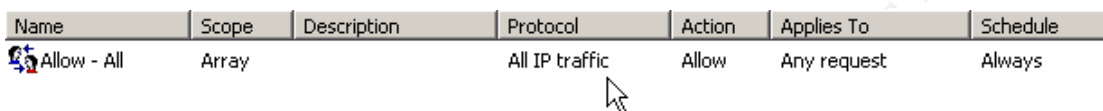


Figure 11 - Use Remote Default Gateway for VPN Clients

## Access Policy

No “Allow All” Protocol Rule	
<b>Test</b>	Is there a protocol rule that allows all traffic?
<b>Out of Spec Condition</b>	Yes.
<p><b>Description:</b> With SecureNAT clients, an “allow all” protocol rules will permit any outgoing TCP/UDP defined traffic. ISA Server has a number of predefined TCP/UDP traffic definition take cannot be deleted. An “allow all” protocol is an indication that the permitted outgoing Internet has not defined thought out. The auditor should verify this with via the “Access Policy / Protocol Rules” node of the ISA Management Console.</p>  <p style="text-align: center;"><b>Figure 12- Allow All Protocol Rule</b></p> <p>After a number of tests, I have come to the conclusion that trying to test this condition with nmap cannot be done. The command “nmap -sA -g53 &lt;IP Address Outside of the Firewall&gt;” should indicate the presence of a firewall by indicating which ports are filtered. When this test is done from the internal network, ISA Server always reports the same ports as being “unfiltered”. This result is always the same regardless of the active protocol rules.</p>	

No Unnecessary Packet Filters	
<b>Test</b>	Are there unnecessary packet filters?
<b>Out of Spec Condition</b>	Yes.
<p><b>Description:</b> Packet filters are applied to the external interface. By default, everything is denied but ISA Server has some preconfigured filters. They authorize among other things certain type of ICMP traffic (but not ICMP Echo Replies). The auditor needs to verify that ICMP Echo Replies, Time and Unreachable messages are blocked. Blocked traffic is recorded in the IPPEXTD&lt;date&gt; log file. Pay cost attention to forgotten filters. These filters that were created for a particular reason that is not no longer valid. Tools like Nmap and Nessus can also help the auditor to detect unnecessary packet filters.</p>	

No Unnecessary Protocol Definitions	
<b>Test</b>	Are there unnecessary protocol definitions?
<b>Out of Spec Condition</b>	Yes.
<p><b>Description:</b> The protocol definitions that are delivered with ISA Server cannot be deleted. They can only be “disabled”. Sometimes, these predefined protocol definitions are insufficient and custom-made ones need to be defined. If the reason these protocol definitions are no longer valid, they must be disabled. The same is true for predefined protocol definitions.</p>	

<b>Site &amp; Content Rules</b>	
<b>Test</b>	Do the Site and Content Rules enforce the organization's acceptable use policy?
<b>Out of Spec Condition</b>	No.
<b>Description:</b> Site and Content Rules control the HTTP traffic. If the organization restricts content or access to only certain sites, the Site and Content Rules must have definitions that enforce the organization policy. An auditor can test this condition quite quickly. If the organization does not permit the downloading of MP3 files, the auditor should attempt to download one. If the Site and Content Rules are properly configured, the download will fail.	

## Publishing

<b>No Web Publishing on ISA Server</b>	
<b>Test</b>	Is IIS being published from the ISA Server?
<b>Out of Spec Condition</b>	Yes.
<b>Description:</b> It is a very bad practice to publish a Web server that resides on the ISA Server. By its very nature, traffic is being permit to have access to the ISA Server through a well-known source of exploits. The Unicode Vulnerability <sup>16</sup> , for example, can give a hacker immediate access to the ISA Server.  To determine if a web server is being published on an ISA Server, the auditor needs to check the web publishing rules (ISA Management Console MMC Plug-in / Publishing node) for the ISA Server name and the IP Packet Filters. When doing "self" web publishing, an ISA Server has to have a packet filter authorizing HTTP, HTTPS, FTP and Gopher traffic.	

<b>FTP – ISA Server Publishing</b>	
<b>Test</b>	Is FTP being published on the ISA Server itself?
<b>Out of Spec Condition</b>	Yes.
<b>Description:</b> Publishing an FTP server on the ISA Server itself opens up a vulnerability called a FTP Port or Bounce Attack. Verifying this condition is a two-step process. First with "netstat -an", checked that port 21 is no longer assigned to address 0.0.0.0. This indicates the socket-pooling has been deactivated. Next check the registry for the key <b>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Msftpsvc\Parameters\</b> . If the value "EnablePortAttack" is set to 1, then FTP service is vulnerable <sup>17</sup> .	

<sup>16</sup> Sans/FBI Top 20 - <http://www.sans.org/top20.htm>.

<sup>17</sup> [http://www.isaserver.org/shinder/tutorials/ftp\\_on\\_isa.htm](http://www.isaserver.org/shinder/tutorials/ftp_on_isa.htm).

<b>MS-Exchange is not published using RPC</b>	
<b>Test</b>	Is MS Exchange published with RPC?
<b>Out of Spec Condition</b>	Yes.
<p><b>Description:</b> It is possible to publish an Exchange Server that is located on the internal network. There are several protocols that one can use to obtain access to the Exchange Server from the external network but one that should never be use is RPC. The auditor needs to check the Server Publishing Rules for the Exchange RPC protocol. (ISA Management Console / Publishing node).</p> <p>Nessus should be able to detect this condition but I have been to test it.</p>	

© SANS Institute 2000 - 2002, Author retains full rights.

## Application Filters

HTTP Redirector	
Test	Is all Web traffic forced to go through the Web Proxy Service?
Out of Spec Condition	No.

**Description:** In the event that the Web Proxy Service is stopped, it is possible for Web traffic to be sent directly from the client to the site. The condition is set as shown in Figure 13 - HTTP Redirector Filter Properties Dialog Box.

This is an unacceptable condition because it effectively circumvents the logging of outgoing web traffic. The checkbox “If the local service is unavailable, redirect requests to requested Web server” must be unchecked.

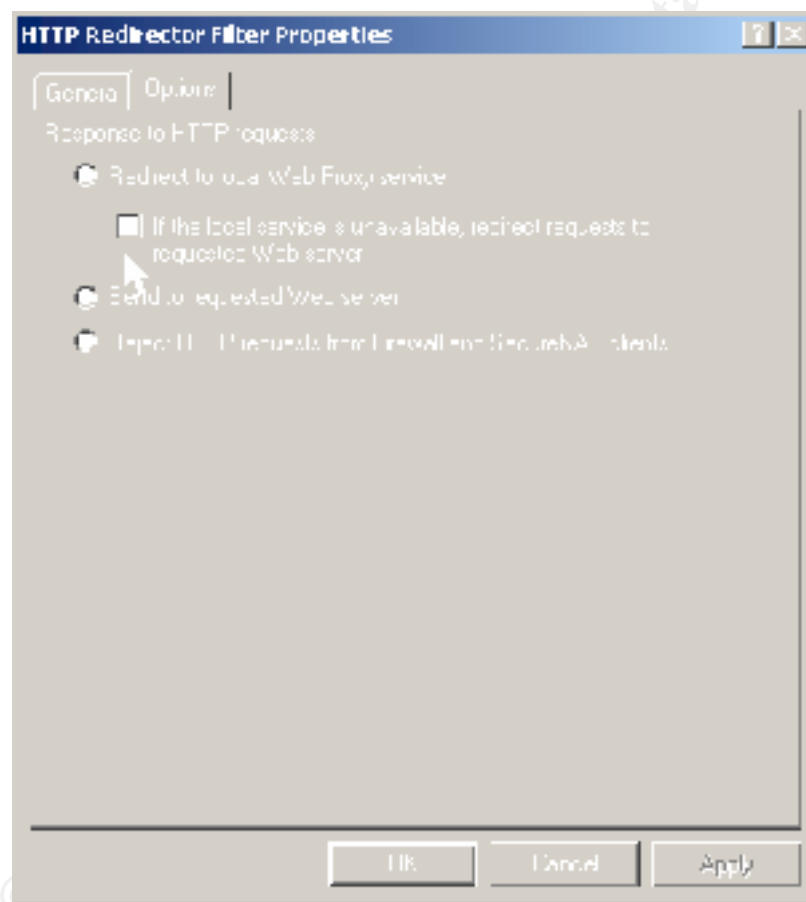


Figure 13 - HTTP Redirector Filter Properties Dialog Box

## Vulnerability Scan

Nessus – External Scan	
Test	Were serious security vulnerabilities detected?
Out of Spec Condition	Yes.
<p><b>Description:</b> Nessus is the best vulnerability testing tool. As part of an audit, an external scan should be made. For simplicity's sake, all options including a "nmap -sS" should be selected.</p> <p>Warning: This is a dangerous and time-consuming process. Written permission must be obtained prior to run any scan. Moreover, key personnel need to be informed and available to repair any damage. A particular problem with Nessus scanning of an ISA Server is that the Web Proxy Service's logging function will generate errors that are recorded in the event journal.</p>	

## Subjective Evaluation

The ISA Server is a firewall. A firewall is an "access" control device. An organization's objective for implementing and maintaining access control is the protection of its information, image, and productive resources.

The threats that ISA Server and any other firewall address are:

- ✓ Data Loss
- ✓ Improper Disclosure
- ✓ Data Manipulation
- ✓ Denial of Service
- ✓ Misappropriation of Resources.

The definition of data loss is apparent. Usually data loss is through employee incompetence or negligence. Of course, making regular backups, good employee training and up to date documentation and procedures are the best protection against data loss from the "inside". However, an organization still needs to protect its data from attacks coming from the "outside".

To delete or even modify an organization's data, an "outside" attack has to obtain access to the "inside". Once inside that attacker uses "tools" to do the damage. These tools can be those that the attacker introduces via a Trojan horse or those that are already in place like Microsoft Internet Information Service<sup>18</sup>. A firewall cannot stop an attacker from using these tools once he has gained access. It can only contribute to the overall system of preventing an attacker from gaining access.

The point of this somewhat long presentation of the obvious is that a firewall, and this particular case, ISA Server, is part of a system of protection. The strength of one part can compensate for the weakness of another. For example, one can argue that good employee training and tight access control to an organization's internal network can reduce the risk incurred in the event that system backup failed once in a while.

---

<sup>18</sup> <http://www.sans.org/top20.htm>.



In determining the cost of loss, one has to consider probability. Cost of loss is classified in terms of the threats. At the end of the analysis, the cost of loss is a dollar value by threat. The ISA Server that is being audited contributes to these final values. The contribution, however, is more or less in function of the threat. For example, an ISA Server makes a larger contribution at preventing the misappropriation of resources than employee training. Directory and file security makes a large contribution to preventing data loss than ISA Server does. So, when evaluating the results of his testing, an auditor has to consider the ISA Server as part of a system and as part of an organization.

To facilitate this process, John Carroll's book, Computer Security, has a chapter entitled "Threat Evaluation"<sup>19</sup>. It is an excellent description of this process. The next few passages are summary of this chapter and how it should be applied to the analysis of an ISA Server.

### **Cost of Loss**

According to John Carroll:

*Because cost-of-loss estimates have a high probabilistic content, they are less reliable than cost-of-countermeasures estimates.*

*Mathematically, one can express cost of loss by the relationship:*

$$C = H \times W \times A \times P \times V \text{ or } C = H \times W \times A \times P \times U$$

*where H = hazard, W = worth, A = attraction, P = Probability, V = vulnerability and U is a joint function or vulnerability (V) and risk (R).*

*Hazard is a binary (1 or 0) variable that, when set equal to zero, removes a potential cause of loss from further consideration.*

*Worth is that total value of the asset threatened, expressed in dollars.*

*Attraction is a number between zero and one; it is that proportion of the value of an asset under consideration which is subject to attack...*

*Vulnerability is a measure of the probable extent of a successful attack on an asset...*

*[Risk] permits factoring into the loss equation existing conditions that tend to exacerbate loss.*

*Probability (sometimes called exposure) can be thought of as the number of times during any given year that an attack on the asset under consideration is likely to occur.<sup>20</sup>*

### **How to Calculate Attraction**

Mr. Carroll provides a number of tables. For the example, the "Level of Attraction" table below.

---

<sup>19</sup> John Carroll, Computer Security, Chapter 22 "Threat Evaluation", Pp. 297-322.

<sup>20</sup> John Carroll, Computer Security, Pp.299-301.

Level of Attraction <sup>21</sup>		
Level	Meaning	Multiplier
0	All	1
1	Many	0.1
2	Few	0.01
3	Very Few	0.001
4	Handful	0.0001

**Table 3 - Level of Attraction**

We tend to think of an asset as an entity. Most of the time, however, an asset is composed of several things. A car is thought of as a whole but really it is a collection of parts: motor, chassis, wheels, seats, carpeting, radio, and more. Some of these parts are more important than others; some have more value than others. In the area of information management, an organization will assign a value to its information but not all of it is important. For example, in a customer database, the address is not important without the name but the name is still important without the address. The name, however, constitutes a smaller portion of the database than the address. Mr. Carroll uses a good example of the phenomenon.

*...suppose [that] the asset were a file of 1,000,000 records, containing sensitive personal information. If the value of each record in terms of the damage its disclosure would cause were \$1,000, the worth of the file would be 1,000,000,000. However, if only 100 of the persons listed in the file were of sufficient importance that anybody would want to know about them, the attraction of this would equal 100/1,000,000 or 0.0001, and its actual cost would be only \$100,000.<sup>22</sup>*

I personally prefer the example of the “misappropriation of resources”. Internet surfing is a misappropriation of resources. Think about it. For better or for worse, it happens everyday but how much does it cost an organization?

Let us say that an employee has an annual salary of \$40K. Add in training, office space, computer, bandwidth, coffee, and electricity, this employee can cost an organization as much as \$70K. Now, let us say that he is “misappropriated” by the [www.nasdaq-boom-boom.com](http://www.nasdaq-boom-boom.com) many times during the day. “Many” is level 2 or a factor of 10%. Ten percent or \$7K of an organization’s resources is going to [www.nasdaq-boom-boom.com](http://www.nasdaq-boom-boom.com). Now if he is “misappropriated” only a few times during the day, only 1% or \$700 is going to [www.nasdaq-boom-boom.com](http://www.nasdaq-boom-boom.com).

Of course, one can dispute the “multipliers” of this table as being too high or too low. What is important to remember about this table is that it helps an auditor much a quantitative translation of adjectives. Alternative to using this table would be “all or nothing” rule and that would be unrealistic.

<sup>21</sup> John Carroll, Computer Security, p.300.

<sup>22</sup> John Carroll, Computer Security, p.300.

## How to Calculate Vulnerability

Vulnerability is a function of

1. the potential degree of damage that would result from a successful attack<sup>23</sup>, and
2. the mitigating or intensifying risk factors.

When an asset is *successfully* attack there will be damage but not all of it will be destroyed. Take a computer for example. A disk crash will not completely destroy a computer. Of course, you will have to replace disk but will not have to replace the computer. How much is the disk in terms of the computer? Remember, the disk is only a part of the computer. If the disk was system volume, that would be a catastrophic loss. If it was an old 1gB that was use for temporary storage, then it would negligible. The Potential Degree of Damage Schedule is shown in the Table 2.

Potential Degree of Damage Schedule <sup>11</sup>			
Level	Classification	Meaning	Numerical Vulnerability
0	No Loss		0.0
1	Negligible	<sup>1</sup> / <sub>10</sub> of 1%	0.001
2	Minor	1%	0.01
3	Serious	10%	0.1
4	Critical	Half	0.5
5	Catastrophic	90%	0.9

**Table 4- Potential Degree of Damage Schedule**

Risks are conditions that either increase or decrease the potential degree of damage. A door is a form of protection. The absence of a lock on the door is a risk of thief, for example, because it is easier to open the door.

With regard to an ISA Server, some risks are very objective and some are not. The measuring absence of documentation is very objective. Determining whether or not employees are careless in terms of security is almost completely subjective. In any case, there are risks tied to the operation of an ISA Server. Below is a list of risks that the auditor has to take into consideration when evaluating the cost of loss.

- **Documentation**
- **Installation & Physical Security**
- **Configuration / Rulebase**
- **Management's Attitude toward Security**
- **System Administrator Competence**
- **User Competence**
- **Notoriety**

---

<sup>23</sup> Mr. Carroll is description of vulnerability is somewhat confusing because he uses the term vulnerability to refer to both "a degree of damage" and "a degree of damage with risk factored in". The former is V and the latter is U. In order to add some clarity, I am using the terms "degree of damage" for V and "vulnerability" for U.

- **Defense in Depth**

To applied risks to the potential degree of damage, each risk is evaluated on a scale and then they are factored into the vulnerability to obtain a weighted average. Like the Potential Degree of Damage Schedule, “the lower the number” means “the lower the risk”. Below are scales for each risk with some guidelines on how to evaluate them.

<b>Risks</b>	
<b><u>Documentation</u></b>	<p><b>0 – Excellent.</b> Procedures and configuration documentation as well as operation logs are maintained and reviewed.</p> <p><b>1 – Very Good.</b> Procedures and configuration documentation is available but operations are not being logged.</p> <p><b>2 – Good.</b> Procedures and configuration documentation are present but incomplete. Operations are not being logged.</p> <p><b>3 – Poor.</b> Procedures are present but configuration documentation is absent.</p> <p><b>4 – Very Poor.</b> Procedures and configuration documentation are absent.</p>
<b><u>Installation &amp; Physical Security</u></b>	<p><b>0 – Excellent.</b> The ISA Server is kept in a locked room. There is a fire suppression system. The backups are stored safely.</p> <p><b>1 – Very Good.</b> The ISA Server is secure but certain components such as a fire suppression system are not completely satisfactory.</p> <p><b>2 – Good.</b> The ISA Server is maintained in a computer room but the room is not locked at all times or non IT personnel have access to this room.</p> <p><b>3 – Poor.</b> The ISA Server is maintained in an open workspace although “administrators” are the only ones who are allowed to logon to the machine.</p> <p><b>4 – Very Poor.</b> The ISA Server is open to all everyone. The administrator account and its password are common knowledge and rarely changed.</p>

© SANS Institute

<b><u>Configuration / Rulebase</u></b>	<p><b>0 – Excellent.</b> The access policy or rulebase limits all incoming and outgoing traffic by specific “allow” rules. For example, HTTP access is denied except to specific sites. Moreover, the “internal network” servers are not published.</p> <p><b>1 – Very Good.</b> Rulebase reflects the organization’s security policy but outgoing traffic is limited to Internet activity is allowed. Intrusion detection is enabled and email alerts are being sent to an “administrator” group.</p> <p><b>2 – Good.</b> Outgoing access is “loose” with IRC traffic permitted. Intrusion detection is enabled but alerts are only being recorded in the system event journal. Packet filtering is enabled.</p> <p><b>3 – Poor.</b> All outgoing traffic is allowed by there is no publishing of servers on the “internal network”. Intrusion detection is not enabled. Packet filtering is enabled.</p> <p><b>4 – Very Poor.</b> All outgoing traffic is allowed and intrusion detect is not enabled. Servers on the “internal network” are published to the Internet. Packet filtering is not enabled.</p>
<b><u>Management’s Attitude toward Security</u></b>	<p><b>0 – Excellent.</b> Management’s attitude is proactive with regular reviews of practices and procedures being performed. User and system administrator training are budgeted and the training is provided throughout the year.</p> <p><b>1 – Very Good.</b> Management’s attitude is proactive but policies do not always materialize into actions.</p> <p><b>2 – Good.</b> Management’s attitude is reactive to detected security problems.</p> <p><b>3 – Poor.</b> Management rarely reactions to security problems. Security is a political problem in the organization that is addressed only in function to higher managements priorities. Security is considered to be an “indispensable” but “non-productive” activity.</p> <p><b>4 – Very Poor.</b> Management is hostile to security issues. Security is an obstacle to doing “business”.</p>

<p><b><u>System Administrator Competence</u></b></p>	<p><b>0 – Excellent.</b> The system administrator is experienced with the system that he is working on. He is trained and certified on ISA Server and Windows 2000.</p> <p><b>1 – Very Good.</b> The system administrator is experienced with the system that he is working on. However, he is not certified. (In this case, certification is not a sign of technical competence but professional competence).</p> <p><b>2 – Good.</b> The system administrator is experienced but not with the system that he is working on. An example of this would be a Unix or Mac administrator that is moving into network administration and then finding himself responsible for the ISA Server’s configuration and administration.</p> <p><b>3 – Poor.</b> The system administrator is trained and perhaps certified but he has very little professional experience.</p> <p><b>4 – Very Poor.</b> The system administrator is not a professional “informatician”. System administration is an additional duty. An example of such a situation would be the “server” being maintained by the Head Accountant.</p>
<p><b><u>User Competence</u></b></p>	<p><b>0 – Excellent.</b> Users receive formal training on all office productivity applications that the organization uses. Moreover, formal security “in-briefing” are given to all new hires. To ensure that security awareness is maintained, regular security bulletins are published and employees attend regular security seminars.</p> <p><b>1 – Very Good.</b> Users receive training and security in-briefings but it is not an ongoing and documented process.</p> <p><b>2 – Good.</b> Users receive training on all office productivity applications but security is not address or it is include as a minor part of “other” training. There is program to ensure that employees are “security-conscience”.</p> <p><b>3 – Poor.</b> Some training and perhaps an occasional security reminder.</p> <p><b>4 – Very Poor.</b> It is hopefully assumed by management that employees are immediately operational when they are hired. Thus, users do not receive training or any information on good security practices. A telltale sign of such an environment are the absence of passwords or passwords being posted on the machines.</p>

<b>Notoriety</b>	<p><b>0 – None.</b> A very small SOHO that does not have a “web” site.</p> <p><b>1 – Very Little.</b> A small organization in terms of the number of clients and the sales volume. There could be a “web” presence would be hosted by an ISP. There would be no HREF link from that website and to the ISA Server. An attitude of “security through obscurity” by management is an indication of this level of notoriety.</p> <p><b>2 – Known.</b> An organization that is well known to a specific group of people but not the general public. An example would be a start-up that has just received a large amount of investment capital from a venture capitalist.</p> <p><b>3 – Well Known.</b> An organization that is well known to the general public.</p> <p><b>4 – Household Word.</b> The organization has brand recognition and is a known through out a very large population.</p>
<b>Defense in Depth</b>	<p><b>0 – Excellent.</b> Backups are planned, performed and tested. Users are trained. Encryption is used. There are guards present. In other words, security is the omnipresent throughout the organization.</p> <p><b>1 – Very Good.</b> Backups are performed and regularly tested. Passwords are changed regularly. There is a budget for IT Security.</p> <p><b>2 – Good.</b> Backups are performed but not tested. Users do get some training and the IT Staff is certified.</p> <p><b>3 – Poor.</b> An occasional backup is made. There are locks on doors but people come and go as they please.</p> <p><b>4 – Very Poor.</b> No backups. No verifications of logs. No fire extinguishers. Basically, the ISA Server was just installed because someone said that the organization needed “protection”. Now the organization is under the false impression that an ISA Server is all they need to be secure.</p>

**Table 5 - Risk Evaluation**

In the calculation of vulnerability the potential degree of damage receives a weighted value according to the table below.

Level of the Potential Degree of Damage	Weighted Value
0 – No Loss (0%)	0
1 – Negligible (0.1%)	1
2 – Minor (1%)	2
3 – Serious (10%)	6
4 – Critical (50%)	8
5 – Catastrophic (90%)	10

**Table 6 - Weighted Value for the Potential Degree of Damage**

This weighted value is then added to the average of the risks. The sum is used with the following table to determine a multiplier for the cost-of-loss equation.

Average Risk + Weighted Potential Damage	Multiplier
0	0.00
1	0.00
2	0.01
3	0.03
4	0.05
5	0.07
6	0.10
7	0.30
8	0.50
9	0.70
10	0.90
11	0.95
12	0.97
13	0.99
14	1.00

**Table 7 - Vulnerability Multiplier**

This is a lot of information and I am certain that, at first view, it is very confusing. The best way to understand method is by working through an example. Take the situation of a well-known organization confronted with a data loss. The organization has estimated that an attack that resulted in a data loss would be serious. In other words, it would affect 10% of its data. (Ten percent is the value of the data that will be unrecoverable. It is not the quantity in terms of gigabytes). The auditor has already evaluated the eight areas of risk. Look at the table below and work through the calculations.



<b>Threat: Data Loss</b>				
		<b>Evaluation</b>	<b>Level</b>	<b>Value</b>
<b>Potential Degree of Damage</b>		<b>Serious (10%)</b>	3	6
<b>Risk</b>	<b>Documentation</b>	<b>Very Little.</b> Documentation is done in an informal manner because of workload constraints.	3	3
	<b>Installation &amp; Physical Security</b>	<b>Good.</b> Planned out installation with access control.	2	2
	<b>Configuration / Rulebase</b>	<b>Poor.</b> Allow all access and Web Server Publishing.	3	3
	<b>Management Attitude to Security</b>	<b>Good.</b> Security conscience but not security advocates.	2	2
	<b>System Administrator Competence</b>	<b>Excellent.</b> Trained and Certified.	0	0
	<b>User Competence</b>	<b>Good.</b> Trained but not very security conscience.	2	2
	<b>Notoriety</b>	<b>Well Known.</b>	3	3
	<b>Defense in Depth</b>	<b>Very Good.</b> Backups are very well organized and managed.	3	3
<b>Total</b>				18
<b>Average (pessimistically rounded down)</b>				2
<b>Average Risk + Weighted Potential Degree of Damage</b>				8
<b>Multiplier for Cost-of-Loss Equation</b>				0.50

**Table 8 - Sample Vulnerability Calculation**

### How to Calculate Exposure

Exposure is the probability that a successful attack will occur during a specified period of time. In the Cost-of-Loss equation, it is the P variable. Personally, I prefer the term exposure because of its relationship with security. We often talk of exposed systems. In terms of the equation we are investigating a system's exposure to attack.

Mr. Carroll wrote in 1977 that exposure is something that is very hard to estimate.

Historical records regarding attacks seldom exist the extent that valid probabilistic estimates can be made using them.<sup>24</sup>

Is this still a valid assertion? Probably. However, 25 years later, we are all aware that attacks through the Internet as almost constant. Still, Mr. Carroll's remark, "...an estimate of probability is usually made subjectively by a knowledgeable official..."<sup>25</sup> holds true.

As an auditor, you have to assign a level of exposure to the system that you are auditing. You do this based on your own professional experience and the information that you gather through interviewing key personnel in the organization.

<sup>24</sup> John Carroll, Computer Security, p.304

<sup>25</sup> John Carroll, Computer Security, p.304

The table below provides list of different levels of probability that an auditor can use with determining a level of exposure.

Exposure <sup>26</sup>			
Level	Classification	Meaning	Numerical Probability
0	Never	Once every 3,000 years	$1/3,000 = 0.000333$
1	Rarely	Once every 300 years	$1/300 = 0.00333$
2	Seldom	Once every 30 years	$1/30 = 0.0333$
3	Once in 3 years		$1/3 = 0.333$
4	Once in 4 months		$365/12 = 3.3$
5	Once in two weeks		$365/11 = 33.3$
6	Daily		$365*1.1 = 333$
7	Several times a day	10 times a day	$365*9.12 = 3330$

**Table 9 - Exposure**

### Example Calculation

Continuing with the calculation for vulnerability presented in Table 8 - Sample Vulnerability Calculation, the table below is an example of the full cost-of-loss equation.

Through the interviewing process with the data owner (i.e., the site manager) and the data guardian (i.e., the IT Manager), the auditor has determined that \$5M is threaten by a data loss of attack. This \$5M figure is based on the size of organization, the quantity of data transactions in a year, and the organization's activity. Is this a subjective figure? Yes and no. It is subjective in that it is an estimate but it is objective from the standpoint that is it based on the observation of measurable facts. As a rule of thumb, an auditor can appraise the value of an organization's data asset based on one year's sales volume or one year's operational cost. The sales volume method is more valid if the organization's data is its source of revenue. A "Think-Tank" would be an example of this type of organization.

Of the \$5M, it is also determined that only 50% is attractive to an attacker. Again, this is a subjective estimate based on the auditor's professional experience and observations.

The organization in this example relies heavily on Internet connectivity. External users can initiate communications to the organization through PPTP, HTTP, NNTP, SMTP, and FTP. Considering this environment, it would be safe to take a pessimistic view and say that organization will be the victim of a successful attack at least once during the next few years. Using Table 9 - Exposure, this would result in a probability of 0.333 (Level 3 Exposure).

<sup>26</sup> John Carroll, Computer Security, p.304.

Cost-of-Loss Example for Data Loss		
$C = H \times W \times A \times P \times U$		
$\$0.8M = 1 \times \$50M \times 0.1 \times 0.333 \times 0.50$		
Variable	Value	Remarks
H – Hazard	1	The Threat is Real.
W – Worth	\$50M	Value of the asset threatened by a Data Loss Attack.
A – Attraction	50%	Only 50% of the asset is attractive to an attacker.
P – Exposure or Probability of an attack	0.333	Table 9 - Exposure
U – Vulnerability of the Asset	0.50	Table 8 - Sample Vulnerability Calculation

**Table 10 - Cost-of-Loss Example Calculation**

The \$800K is the Cost-of-Loss from the standpoint of what the organization should provision each year. Instead of moving \$8K to reserves via an accounting transaction, a proactive organization would program this sum to the acquisition of countermeasures against this threat.

At this point, we have arrived at a dollar figure of how much is it worth to “fix the problem”. The next question to be addressed is “How to best rate of return”.

### ***Value of a Countermeasure***

The cost of countermeasures is a fairly straightforward subject. Basically, they are operational costs that can be determined from a catalog. What is important from the perspective of an audit recommendation is adapting the countermeasures to the organization.

SANS Education presented the concept of Time Based Security.<sup>27</sup> This concept is based on the idea that protection (pt) afforded by a system has to be greater than time required to detect (dt) an intrusion plus the time required to react (rt) to it. In other words,

$$\text{Protection (pt)} > \text{Detection (dt)} + \text{Reaction (rt)}.$$

The concept is easy to understand and, in fact, it seems almost rhetorical. What is interesting with this concept is the distribution of cost. Protection, like a lock on a door, costs money. Detection, like an alarm system, costs more money. Reaction, like a security guard service, costs even more money.

Extrapolating from the above formula, we can conclude:

$$\text{pt}(\$) < \text{dt}(\$) + \text{rt}(\$).$$

I previously stated that cost-of-countermeasures are more operational costs as opposed to investment. Of course, they can sometimes take the form of an investment such as the

<sup>27</sup> Carla Wendt, *Track 7 – Auditing Networks, Perimeters and Systems*, p.1-7, SANS Institute, <http://www.sans.org>, Conference, San Diego, California, October 2001. This concept was developed and published by a Mr. Schwartu.

acquisition of another server with Windows 2000 and ISA Server. However, these investments will still need to be depreciated and depreciation is an operational cost.

Operational costs have an impact on cash flow. As a general rule, larger organizations have more cash and manage it better than smaller organizations. This means that as an organization grows in size, the more it can spend on countermeasures. This is obvious, of course, but let us consider it from the standpoint of time-based security.

There are third elements: protection, detection and reaction. An organization has a certain amount of cash to spend on the acquisition of countermeasures. Where should it spend this money – in protection, detection or reaction? The answer to that question depends on the size of the organization. Back to the formula again:

$$\begin{array}{c} \text{pt (organization / cash)} \\ < \\ \text{dt (bigger organization / more cash)} \\ < \\ \text{rt (biggest organization / most cash).} \end{array}$$

In terms of recommending countermeasures in an ISA Server environment, this could be translated into

$$\begin{array}{c} \text{pt (Better Security Policy and More Restrictive Rulebase)} \\ < \\ \text{dt (Acquisition of IDS Software)} \\ < \\ \text{rt (Hiring of another system administrator).} \end{array}$$

In terms of example cited in Table 10 - Cost-of-Loss Example Calculation, improving the organization's Documentation, Installation & Physical Security, and Configuration / Rulebase by just on level in each category could result in the cost-of-loss being reduced from \$800K to \$500K. In a large organization, this \$300K savings would cover the cost of an additional system administrator. In a small organization with only \$50K of assets threatened by an attack resulting in data loss, the savings would be \$3K. In this case, the applying this savings to training on how to improve the ISA Server's configuration and administrator would be more justified.

The following are points to remember when recommending countermeasures.

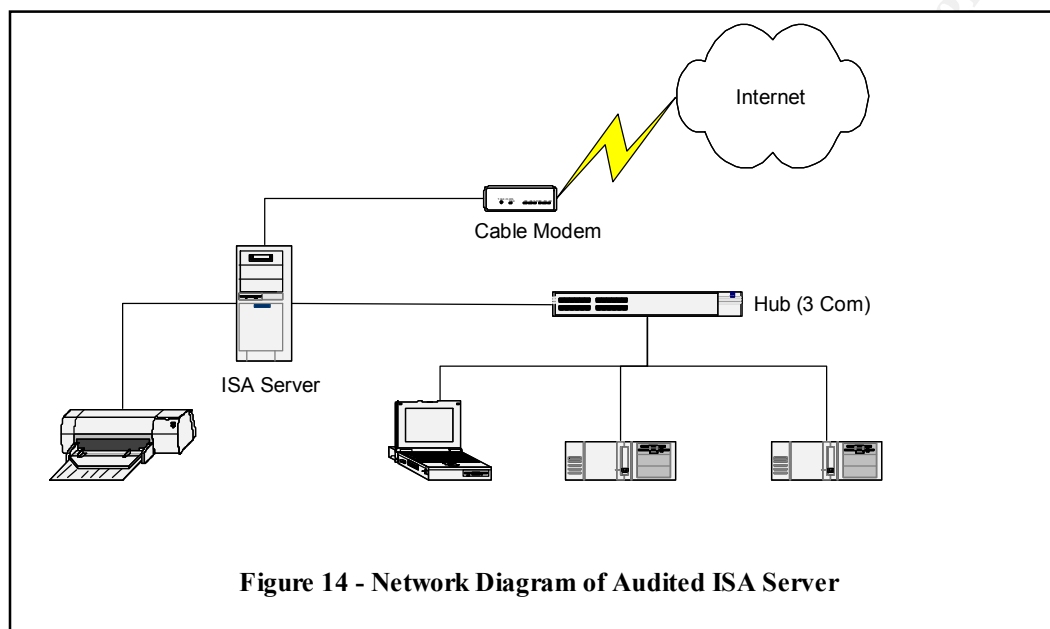
1. They are costs that have to be absorbed by the organization, and
2. They should be justified in terms of the savings generated by reduction in the cost-of-loss.

## **Audit**

Auditing is a privileged activity and it is unwise to divulge information that was obtained as a result of an audit. In terms of a security audit, the reasons are quite apparent. An auditor should let the "audit ordering" authority release any information. If this is not possible, as in the case of this research paper, the auditor must obtain permission prior to any disclosure.

The organization that kindly permitted me to perform an audit of their ISA Server has requested that their identity remain confidential are some obvious reasons. The deficiencies that I detected in their configuration have been corrected.

## Description of the Audited Device and Its Environment



## Organization

The organization is a small business that is engaged in custom software development, usually for the Microsoft Office Suite. The company's sales volume is close to \$220K and it produces approximately 30 invoices per year.

## ISA Server

The ISA Server running on an Intel Pentium IV computer with 256MB of RAM. The server has two NICs: one is connected to the cable modem and the other is connected to a 3Com hub. The server is also being used as a Windows 2000 Domain Controller, HTTP Server and File & Print Server. The ISA Server is controlling access to the organization's website. The web is an extranet.

## LAN

The Local Area Network is composed of the server (ISA/Domain Controller), one portable computer and two desktops. The portable is running Windows 2000 Professional and the two desktops are several different operating systems: Windows 2000 Professional, and Windows 98se.

## WAN

The WAN connection is via a cable modem provided by the ISP and IP addresses are assigned by DHCP.

<b>Organization</b>	Small software development business specializing in add-ons to the MS Office Suite.  Two full employees (the owners) and university students doing internships.
<b>ISA Server Hardware</b>	Pentium IV, 256mB, 60gB, 2 – NICs, CDRW
<b>ISA Server – OS Version</b>	Windows 2000 Server. French Version
<b>ISA Server – Version</b>	ISA 2000 Version 3.0 French Version. Enterprise Edition. 120-day trial version.
<b>Service Packs</b>	Service Pack 2
<b>Hot Fixes</b>	None. (It is not possible to applied Hotfixes to the trial version of ISA Server).
<b>LAN Composition</b>	One server with three workstations (2 desktops and 1 notebook). Desktops are AMD K6.
<b>WAN Connection</b>	Cable modem to the ISP.
<b>Windows 2000 Domain</b>	Installed.
<b>Location of Domain Controller</b>	On the same machine as the ISA Server.
<b>Workstations Hardware</b>	Desktops: Pentium II and K6.  Notebook: Pentium III.
<b>Workstation OS Configurations</b>	Windows 98 and Windows 2000.
<b>Application Software</b>	Office 2000 and Visual Studio
<b>Servers / Accessible from Internet / Location</b>	HTTP / Yes / On the ISA Server

Table 11 - Summary of the Audit Environment

## The Risks to the System

Like any firewall, ISA Server has the mission of controlling access. By controlling access – whether it is “incoming” or “outgoing”, ISA Server makes a significant contribution to the protection of an organization’s assets. These assets are information, image and productive resources. The greatest risk to an ISA Server is that it fails to control access. The risk itself can manifest itself in several forms.

Risks and Exploits	
<b>Denial of Service</b>	Jolt2 <sup>28</sup>
<b>Malicious access to data</b>	Unicode Vulnerability <sup>29</sup> being exploited on the ISA Server
<b>Unauthorized use of resources</b>	Loki and Reverse WWW Shell <sup>30</sup>

<sup>28</sup> <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0305>.

<sup>29</sup> <http://www.sans.org/top20.htm>.

**Table 12 - Risks and Exploits to the Audited System**

## **Audit Results**

The organization's objective in using ISA Server was to have "protection from malicious external access at the lowest cost possible while staying within the Microsoft family of products." They also saw in ISA Server the "panacea" of easy installation and administration. Unfortunately, this lead directly to the worst vulnerability: the Default Installation<sup>31</sup>.

Ten items of the audit's checklist are presented below. They highlight what can only be described as a very dangerous situation.

## **Physical Security**

The organization is a very small: two people, the business owners, and number of university students who are doing "internships". The ISA Server is setup in an open space. Everyone in the organization knows that administrator's password. Considering the size of the organization, this may not be a problem if it were not for the fact that the administrator is log into the system throughout day and there is no password on the screen saver.

Backups are limited to the developed software and these are being made to CDs. According to the one of owners, this is being done a regular basis but there never had been a need to restore the data. In the others, the ISA Server is not backed up, the backup system is untested and anyone can easily modify the configuration of the ISA Server.

## **Post-Installation Image**

There was no post-installation image of the ISA Server. This point was not considered to be very important by the business owners until the discussion turned to the problems that they had encountered when they setup their ISA Server.

Installing the ISA Server software was straightforward. The setup wizard worked as they expected but there of general absence of knowledge about the TCP/IP protocol. Configuring the Access Policy and the Policy Elements was a frustrating process that finally ended with a workable setup but only after a lot of trial and error. In the end, they estimated that they had spent more than two days over period of three weeks setting up their ISA Server. The configuration was, of course, not documented. When I asked them how much time it would take them to set up an ISA Server if theirs crashed, they estimated one day. When the "one" day figure was compared to the 15 minutes required to load an image, the problem of not having a post-installation image became clear.

---

<sup>30</sup> Although Loki does not run on a Windows platform, a network that is protected by an ISA Server can contain a platform that is affected by Loki. Linux 2.0.x is an example. What is interesting about this exploit is described by Internet Security Systems: "This program is a working proof-of-concept to demonstrate that data can be transmitted somewhat secretly across a network by hiding it in traffic that normally does not contain payloads."

(<http://xforce.iss.net/static/1452.php>). Reverse WWW Shell is described at <http://packetstorm.widexs.nl/groups/thc/fw-backd.htm>. The author of this article wrote, "This backdoor should work through any firewall which has got the security policy to allow users to surf the WWW (World Wide Waste) for information for the sake and profit of the company." Scary.

<sup>31</sup> <http://www.sans.org/top20.htm>.

## Segregation of Roles

ISA Server was placed on the best machine in the organization. Using the “best machine” in the organization for the domain controller was also considered a necessity. Needless to say, the principle of segregation of roles had been violated. Is this an “out of spec”? In this particular case, the answer is “not” because the organization did not have any alternative. It is a very dangerous situation, nonetheless.

I confirmed that fact that the ISA Server was indeed the domain controller because the Local Users and Group node was deactivated.

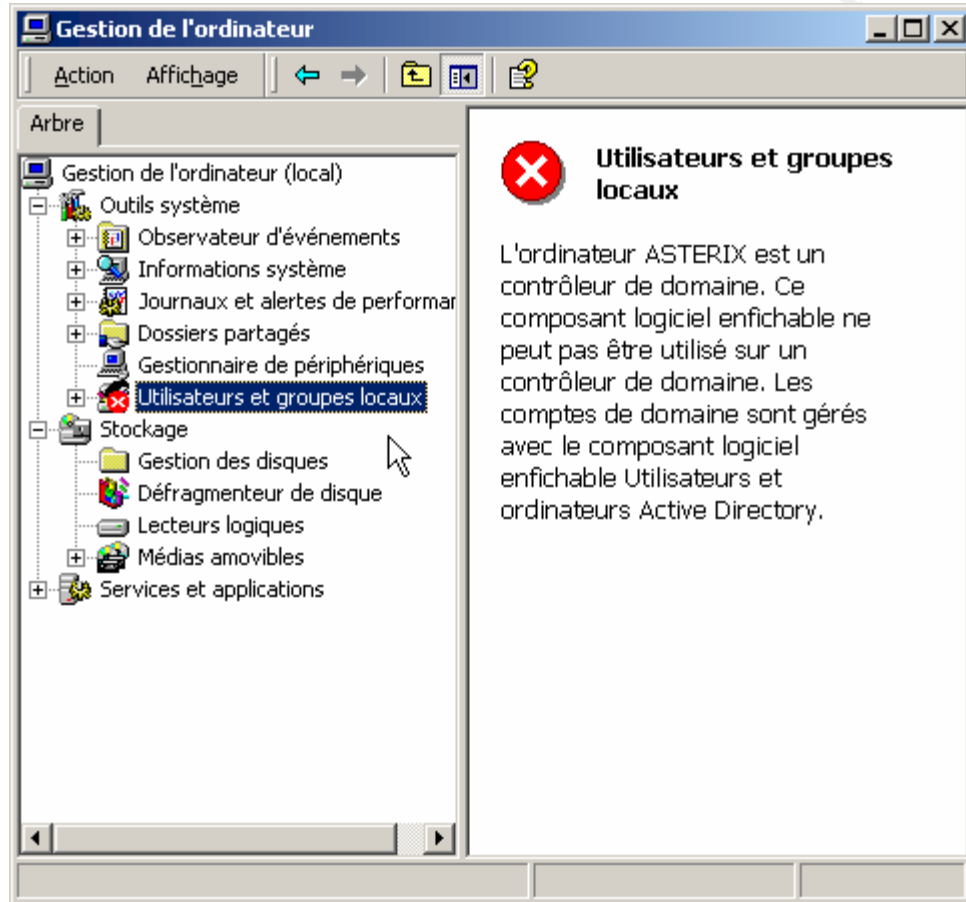


Figure 15 - Indication of an ISA Server being a Domain Controller

## Simple TCP/IP Services

At this point in the audit, I was certain that I was looking at a default installation in an organization that had very little networking experience. Default installations are not always bad in every respect. This point was driven home when I checked the ISA Server for the Simple TCP/IP Services (– or “Useless” services according to Nessus). The “netstat” command indicated that they were not installed. By default they are not installed. Figure 16 - Missing Simple TCP/IP Services is a result of this command. Note that the ports for the Simple Services are not presents: 7 (Echo), 9 (Discard), 13 (Daytime), 17 (Quote of the Day) and 19 (Chargen).



```
C:\>netstat -an | more
```

Connexions actives

Proto	Adresse locale	Adresse distante	Etat
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:53	0.0.0.0:0	LISTENING
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:464	0.0.0.0:0	LISTENING
TCP	0.0.0.0:593	0.0.0.0:0	LISTENING
TCP	0.0.0.0:636	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1029	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1044	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1046	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1720	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3002	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3003	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3004	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3005	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3006	0.0.0.0:0	LISTENING

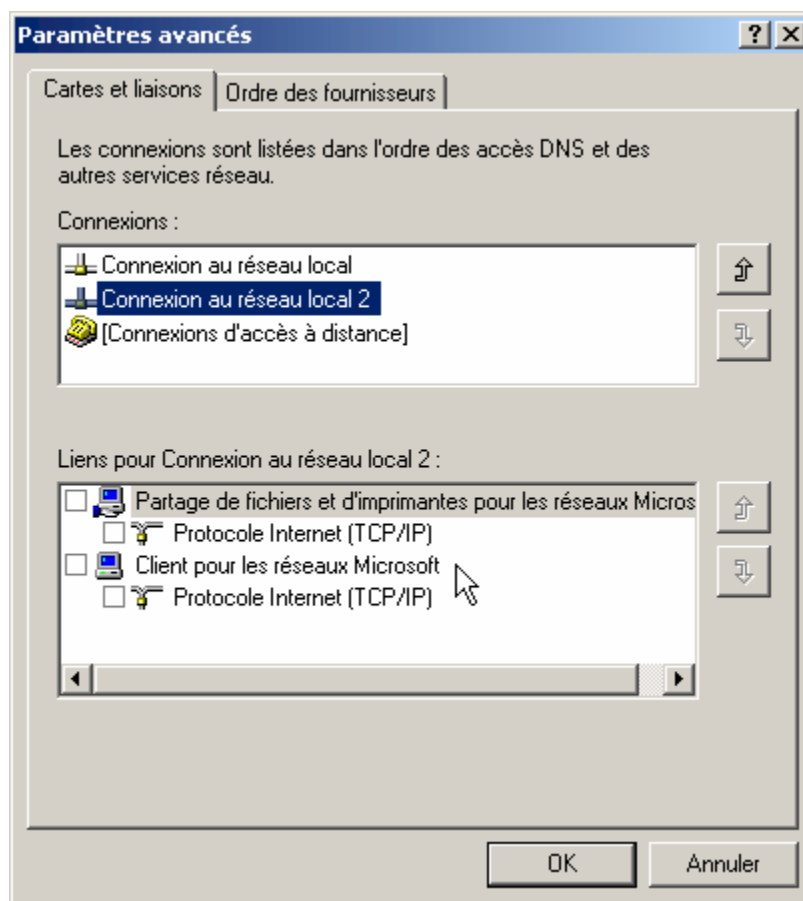
Figure 16 - Missing Simple TCP/IP Services

## NIC Configuration

A verification of the bindings on the network interface card indicated that not everything was a default installation. The most dangerous services, *File and Printer Sharing* and *Client for Microsoft Networks*, had been deactivated on the external interface. Interestingly, I discovered through talking with one of the business owner's that this had been done because of ZoneAlarm. Apparently, he had some experience with ZoneAlarm and he remembered the advice to disable these services from any external adapter.

Figure 17 - External Interface on Audited System is a screenshot of the external interface on the audited system. "Connexion au réseau 2" translates as LAN Connection 2. This was the WAN / External Interface<sup>32</sup>. Notice that *File and Printer Sharing* (Partage des fichiers...) and *Client for Microsoft Networks* (Client pour...) are not selected.

<sup>32</sup> I suggested that they rename the NICs to describe their position in the network. It was be unfortunate to modification of the LAN interface when believing that it was the WAN interface.



**Figure 17 - External Interface on Audited System**

## Intrusion Detection

The two screenshots (Figure 18 - Intrusion Detection Enabled and Figure 19 - Detected Attacks are Not Enabled) below show one of the problems in configuring ISA Server's intrusion detection. Although they enabled the intrusion detection but they did not enable the attacks. This situation is very easy to detect. Doing a "nmap -sS -p0 -p 1-1024 <External IP Address>" will write a number of warning message to the event journal. "Figure 20 - Event Journal: Detection of an Nmap Port Scan" is a screenshot of one of these messages.

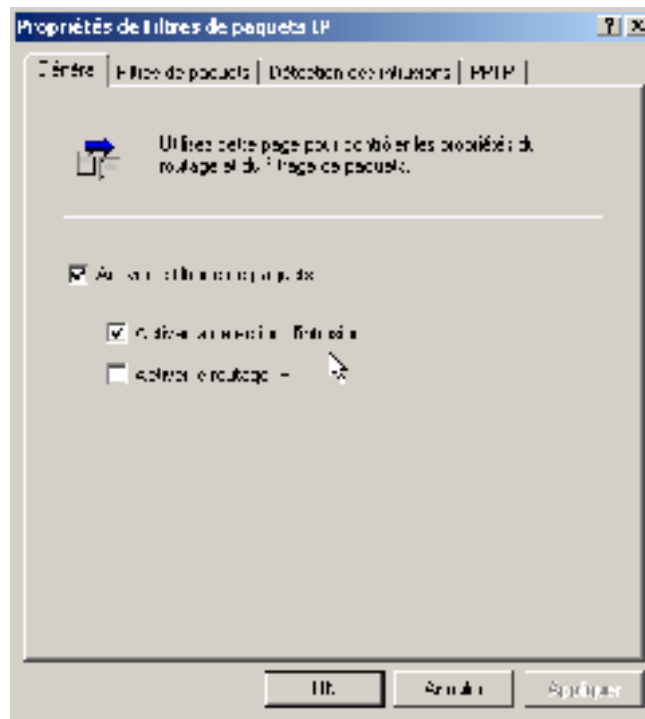


Figure 18 - Intrusion Detection Enabled

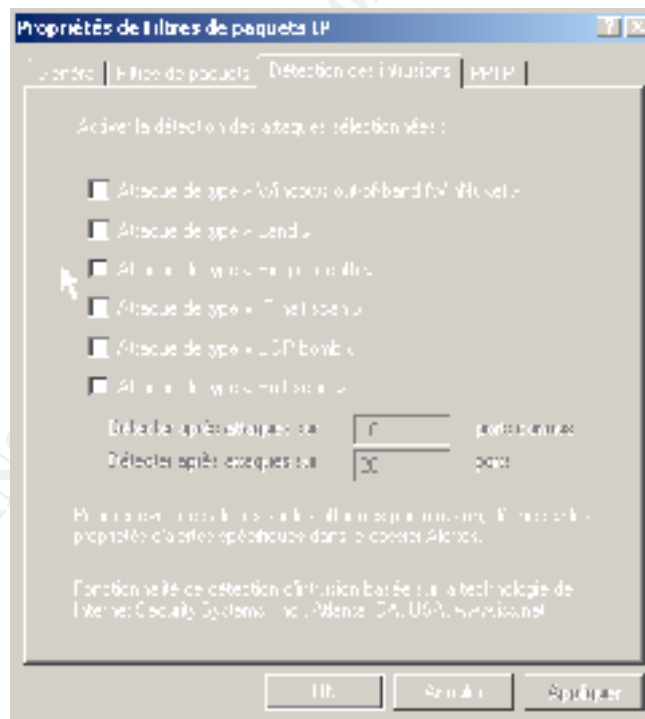


Figure 19 - Detected Attacks are Not Enabled

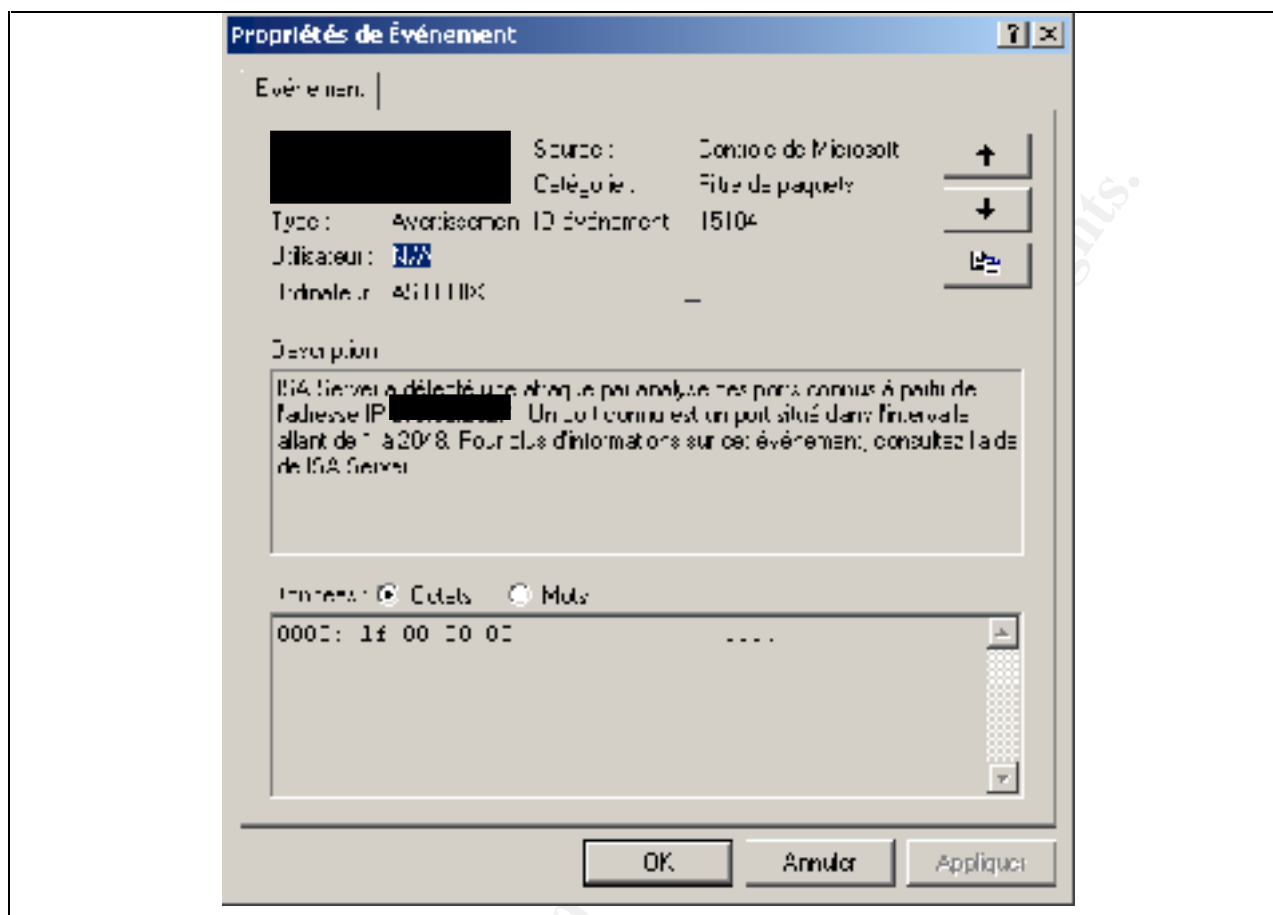


Figure 20 - Event Journal: Detection of an Nmap Port Scan

## IP Packet Fragmentation

The IP Packet Fragmentation filter was not activated. The command “hping2” indicated that fragmentation was permitted. To test this condition I used this command:

```
hping -f -c 1 -d 1500 -i <IP ADDRESS>.
```

The fact that there was a reply indicated that fragmented packets were not being filtered. I then activated the IP Packet Filtering option and repeated the same hping command. No reply.

## Unnecessary Packet Filters

As I described earlier, the setting up process was one of trial and error. This is no more apparent in the IP Packet Filter definitions. All outgoing ICMP traffic was authorized. ISA Server was setup this way because the business owners wanted to be able to ping the ISA Server from the Internet. “It was easier to authorize everything than to configure all of the options on the packet filtering.”

Nom	Action	Protocole	Sens	Port local	Port distant
Tous	Autoriser	Tout le trafic IP			
Autoriser la règle	Autoriser				
Client DHCP	Autoriser	UDP	Les deux	68	67
Délai ICMP dans	Autoriser	ICMP	en entrée		
Extinction de so...	Autoriser	ICMP	en entrée		
Filtre DNS	Autoriser	UDP	Les deux	Tous les ports	53
FTP sortant	Autoriser	TCP	Les deux	Tous les ports	21
HTTP entrant	Autoriser	TCP	en entrée	80	Tous les ports
HTTP sortant	Autoriser	TCP	Les deux	Tous les ports	80
HTTPS sortant	Autoriser	TCP	Les deux	Tous les ports	443
ICMP en sortie	Autoriser	ICMP	en sortie		
ICMP inaccessible...	Autoriser	ICMP	en entrée		
Ping	Autoriser	ICMP	en entrée		
Ping Essai 2	Autoriser	ICMP	Les deux		
POP3 sortant	Autoriser	TCP	en entrée	110	Tous les ports
Réponse ping IC...	Autoriser	ICMP	en entrée		
SMTP sortant	Autoriser	TCP	en entrée	25	Tous les ports

Figure 21 - IP Packet Filters

This method did indeed authorize the ICMP Echo Reply but it all authorized ICMP Time Exceeded messages. A “ping” in one window and a “windump” in another demonstrated this.

```

Window #1

C:\>ping -l 1500 -f -n 1 213.56.XXX.xxx

Pinging 213.56.XXX.xxx with 1500 bytes of data:

Packet needs to be fragmented but DF set.

Ping statistics for 213.56.XXX.xxx:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>

=====

Window #2

C:\Scans>windump proto ICMP
windump: listening on \Device\Packet_{A0DEF696-5BBC-4363-BB6B-763D36255913}
03:30:47.818279 213.56.XXX.xxx > frstq134: icmp: ip reassembly time exceeded

1211 packets received by filter
0 packets dropped by kernel

C:\Scans>

```

Figure 22 - ICMP Time Exceeded Message

## Web Publishing

The extranet was being published on the ISA Server. This, in itself, is a serious situation. Because there was an alternative, publishing the extranet on a desktop running Windows 2000 Professional, I considered this to be an “out of spec” condition. The results of the Nessus vulnerability test also pointed out the fact that the Unicode Vulnerability<sup>33</sup> had not yet been patched.

## Nessus / Nmap

The results of the Nessus vulnerability test were as follows. In running this test, I simply clicked on the “Enable All” button in order to perform all of the tests. Overkill? Of course, it was. Nessus is such a complete tool that I considered that it was more likely that I would forget to do a test if I tried to select them on an individual basis.

### Nessus Scan Report

-----

#### SUMMARY

- Number of hosts which were alive during the test : 1
- Number of security holes found : 2
- Number of security warnings found : 3
- Number of security notes found : 3

#### TESTED HOSTS

213.56.xxxx.xxx (Security holes found)

#### DETAILS

- + 213.56.xxxx.xxx :
  - . List of open ports :
    - o general/udp (Security notes found)
    - o smtp (25/tcp) (Security notes found)
    - o http (80/tcp) (Security hole found)
    - o general/icmp (Security warnings found)
  - . Information found on port general/udp

For your information, here is the traceroute to 213.56.xxxx.xxx :  
?

- . Information found on port smtp (25/tcp)

---

<sup>33</sup> <http://www.sans.org/top20.htm>.

Remote SMTP server banner :  
asterix.xxxxxxxx.xxx Microsoft ESMTP MAIL Service, Version: 5.0.2195.2966  
ready at Sat, 19 Jan 2002 04:13:42 +0100  
214-This server supports the following commands:214 HELO EHLO STARTTLS  
RCPT  
DATA RSET MAIL QUIT HELP AUTH TURN ATRN ETRN BDAT VRFY

. Vulnerability found on port http (80/tcp) :

When IIS receives a user request to run a script, it renders the request in a decoded canonical form, then performs security checks on the decoded request. A vulnerability results because a second, superfluous decoding pass is performed after the initial security checks are completed. Thus, a specially crafted request could allow an attacker to execute arbitrary commands on the IIS Server.

Solution: See MS advisory MS01-026  
Risk factor: High  
CVE : CAN-2001-0333

. Vulnerability found on port http (80/tcp) :

There's a buffer overflow in the remote web server through the ISAPI filter.

It is possible to overflow the remote web server and execute commands as user SYSTEM.

Solution: See  
<http://www.microsoft.com/technet/security/bulletin/ms01-033.asp>  
Risk Factor :  
High

. Warning found on port http (80/tcp)

The remote web server appears to be running with Frontpage extensions.

You should double check the configuration since a lot of security problems have been found with FrontPage when the configuration file is not well set up.

Risk factor : High if your configuration file is not well set up

CVE : CVE-1999-0386

. Warning found on port http (80/tcp)

It seems that the DELETE method is enabled on your web server  
Although we could not exploit this, you'd better disable it

Solution : disable this method

Risk factor :

Medium

. Information found on port http (80/tcp)

The remote web server type is :  
Microsoft-IIS/5.0

We recommend that you configure your web server to return  
bogus versions, so that it makes the cracker job more difficult

. Warning found on port general/icmp

The remote host answers to an ICMP timestamp  
request. This allows an attacker to know the  
date which is set on your machine.

This may help him to defeat all your  
time based authentications protocols.

Solution : filter out the icmp timestamp  
requests (13), and the outgoing icmp  
timestamp replies (14).

Risk factor : Low

CVE : CAN-1999-0524

-----  
This file was generated by the Nessus Security Scanner

Two nmap scans were also performed: one for TCP and the other for UDP. Ports 25 and 110 were open in order to send email. The organization did not maintain an email server. Instead they relied totally on their ISP for email support. Port 80 is open for web publishing. Port 1720 is for H.323 Video-conferencing. Outside of the serious problems that were discovered by Nessus, it is reassuring to compare the results of the nmaps with Figure 16 - Missing Simple



TCP/IP Services. You will notice that there are a several ports that are open on the internal interface but effectively filtered on the external interface.

```
nmap -sS -P0 -O -v -p 1-65535 --max_rtt_timeout=50 -oN AsterixTCPStealth 213.56.xxx.xxx
```

Interesting ports on (213.56.xxx.xxx) :

(The 65531 ports scanned but not shown below are in state: filtered)

Port	State	Service
25/tcp	open	smtp
80/tcp	open	http
110/tcp	closed	pop-3
1720/tcp	open	unknown

```
nmap -sU -P0 -p 1-65535 -oN AsterixUDPa --max_rtt_timeout=50 213.56.xxx.xxx  
All 65535 scanned ports on (213.56.xxx.xxx) are: filtered
```

```
# Nmap run completed at Sat Jan 19 10:17:45 2002 -- 1 IP address (1 host up)  
scanned in 786 seconds
```

## Analysis

It is quite apparent that the ISA Server is “out of spec”. The situation is a beautiful example of the hazards of a default installation. What started out as a very seductive solution for having “easy” and secure access to the Internet, ended up after three weeks of frustration as a very dangerous installation. One could say that the real source of the insecurity was IIS and not ISA Server. That is true but the ISA Server with its poorly configured access policy is contributing to the insecurity. Moreover, the design of ISA Server as a security product can be called into question. What is the security of being able to install insecure applications on the firewall itself? Of course, this is recognized as a very bad practice but the ability to combine roles on one machine is, from a marketing standpoint, very seductive.

Taking the businessman’s point of view, my reaction to the fact that the ISA Server is “out of spec” would be this: “So what? I don’t see the problem. I have a computer at home that is connected to the Internet all of time. I have never had any problems with it. So what if we get hacked? Just reinstall everything from the backup and we can get back to business. In any case, I’ve already has already spent too much on computers.” As frustrating as it may be to computer professionals, this reaction to a request “Spend more money – it is out of spec” is more than justified. A request formulated as “We need to spend this much in order to save that much” would be much more warmly receive. So, how does one calculate this with regard to the audited system?

ISA Server, like any firewall, counters the following threats: Data Loss, Data Manipulation, Improper Disclosure, Denial of Service, and Misappropriation of Resources. After talking to the business owners, the following evaluation of their assets in terms of these threats was established.

<b>Threat</b>	<b>Total Worth of the Asset</b>	<b>Percentage of the Asset that is actually threaten</b>
<b>Data Loss</b>	<b>\$220,000 (1y of Sales)</b>	<b>10%</b>
<b>Data Manipulation</b>	<b>\$0</b>	<b>0%</b>
<b>Improper Disclosure</b>	<b>\$0</b>	<b>0%</b>
<b>Denial of Service</b>	<b>\$1,000 (1d of Sales)</b>	<b>100%</b>
<b>Misappropriation of Resources</b>	<b>\$70,000 (1y Employee Cost)</b>	<b>10%</b>

**Table 13 - Evaluation of the Worth of Threaten Assets**

Whether one agrees with these estimates is not really important for this example. What is important is that the business owners agreed to their validity. Therefore, they were (at the beginning process) willing to except eventual cost-of-loss evaluation. One can call this getting early “buy-in” to the audit results.

Because of the IIS vulnerability and the poor access policy, the probability of a successful attack occurring was set at “Once every 2 weeks”. Using Table 9 - Exposure, this gives a probability of 33.3.

The Level of Potential Degree of Damage was agreed to be “Catastrophic” for a Data Loss and “Critical” for a Denial of Service and a Misappropriation of Resources. (See Table 4- Potential Degree of Damage Schedule.)

With regard to the risks, the organization got the following report card:

<b>Documentation</b>	<b>Very Poor</b>	<b>4</b>
<b>Installation &amp; Physical Security</b>	<b>Very Poor</b>	<b>4</b>
<b>Configuration / Rulebase</b>	<b>Very Poor</b>	<b>4</b>
<b>Management's Attitude toward Security</b>	<b>Good</b>	<b>2</b>
<b>System Administrator Competence</b>	<b>Very Poor</b>	<b>4</b>
<b>User Competence</b>	<b>Good</b>	<b>2</b>
<b>Notoriety</b>	<b>Little</b>	<b>1</b>
<b>Defense in Depth</b>	<b>Poor</b>	<b>3</b>

**Table 14 - Risk Rating Report Card**

This yields an average of 3.

The next three tables show the cost-of-loss calculations for each threat.

Data Loss		
$C = H \times W \times A \times P \times U$		
$\$727,254 = 1 \times \$220,000 \times 0.1 \times 0.333 \times 0.99$		
Variable	Value	Remarks
H – Hazard	1	The Threat is Real.
W – Worth	\$220,000	Value of the asset threatened by a Data Loss Attack.
A – Attraction	10%	Only 10% of the asset is attractive to an attacker.
P – Exposure or Probability of an attack	33.3	Table 9 - Exposure
U – Vulnerability of the Asset	0.99	Table 7 - Vulnerability Multiplier

Table 15 - Cost of Loss thru Data Loss

Denial of Service		
$C = H \times W \times A \times P \times U$		
$\$31,635 = 1 \times \$1,000 \times 1 \times 3.33 \times 0.95$		
Variable	Value	Remarks
H – Hazard	1	The Threat is Real.
W – Worth	\$1,000	Value of the asset threatened by a Data Loss Attack.
A – Attraction	100%	100% of the asset is attractive to an attacker.
P – Exposure or Probability of an attack	33.3	Table 9 - Exposure
U – Vulnerability of the Asset	0.95	Table 7 - Vulnerability Multiplier

Table 16 - Cost of Loss thru Denial of Service

Misappropriation of Resources		
$C = H \times W \times A \times P \times U$		
$\$221,445 = 1 \times \$70,000 \times 0.1 \times 3.33 \times 0.95$		
Variable	Value	Remarks
H – Hazard	1	The Threat is Real.
W – Worth	\$70,000	Value of the asset threatened by a Data Loss Attack.
A – Attraction	10%	Only 10% of the asset is attractive to an attacker.
P – Exposure or Probability of an attack	33.3	Table 9 - Exposure
U – Vulnerability of the Asset	0.95	Table 7 - Vulnerability Multiplier

**Table 17 - Cost of Loss thru Misappropriation of Resources**

The total potential “cost-of-loss” is \$978,354 or almost 5 times the annual sales volume. The ISA Server was “out of spec” condition for the computer professional. It is now a “bet the business” problem for the businessman. Clearly, a certain amount of funds need to be spent in order to reduce this figure to something more reasonable.

The exposure – a successful attack every two weeks – needs to be reduced. Applying patches to IIS would definitely help. But this would only solved the immediate problem and ignore the long-term one. A more durable solution needs to be put in place – a solution that would improve the business’s technical competences and its Defense in Depth.

I would recommend the following course of action:

Action	Cost
Contracting an outside consultant to properly configuration IIS and ISA Server.	\$5,000
Microsoft Training and Certification for one of the business owners.	\$25,000 <sup>34</sup>
Purchase a dedicated machine for ISA Server.	\$4,000

**Table 18 - Recommend Course of Action**

This would result in reducing the cost-of-loss from \$978,354 to \$8,825 or a 3000% return on investment. Of course, the biggest savings are in closing the vulnerability with IIS but who can guarantee that an equally devastating vulnerability will not be discovered in the future? The additional expense in training and hardware will pay off in the medium-term in the form of higher technical competence and greater defense in depth.

## Evaluation of Audit Procedure

The audit procedure has following strong points:

<sup>34</sup> This figure includes 4 weeks of loss business time.

- It can correctly identify an insecure configuration.
- It can assign a dollar value to this condition.
- It is a very good educational process for the auditor and the audited organization.

However, it has a number of weak points.

- It is not automated.
- It is not complete.
- It can only correctly identify extreme conditions.

The audit procedure is manpower intensive. The test audit required over three days to prepare, perform, and report. Moreover, this was done in an environment that was clearly identifiable. The ISA Server was blatantly “out of spec”. What would have happened if the environment had more subtle conditions of insecurity? Take the presence of a Reverse WWW Shell as an example. To detect this insecurity, one would have to rely on historical data to determine patterns in HTTP traffic. It is economical to do this? In an environment that permits all HTTP traffic, of course, it is. However, such environment is looking for inexpensive solutions and not restricting HTTP traffic is an inexpensive solution. Monitoring HTTP historical traffic makes this solution expensive and there is the paradox.

Auditing is a form of insurance. Insurance always costs too much until one is confronted with a catastrophic loss. Through education, people have come to accept the need for insurance. Auditing, on the other hand, is not at that point yet. Thus auditing needs to be as much a business and an educational process as a control process.

Outside of the ability to assign a value to an insecure situation, the procedure is not viable business activity. By not being automated, it requires an excessive amount of billable time. By not being able to check everything in a short period of time, subtle insecure conditions are overlooked.

So what is the alternative? Nessus? Perhaps. But the audit procedure demonstrated something that Nessus cannot: the source of the insecure condition. In the case of the test audit, the procedure showed that ISA Server as a product was not insecure. IIS was insecure. The access policy that was set up by the business owners was insecure. ISA Server itself was secure. Just running Nessus would not have demonstrated this.

So where does the procedure need to go from here? In my opinion, starting to audit an ISA Server from the standpoint of ISA Server is wrong. It is too tightly coupled with Windows 2000. The operating system and ISA Server need to be audited together. Manually, this would be an impossible task. Therefore, I think that an acceptable objective for ISA Server auditing would be to extend the automated Windows 2000 audit procedure that Steve Elky<sup>35</sup> developed to include ISA Server. Is it possible? I do not know. Is it desirable? Yes. Yes. Yes.

---

<sup>35</sup> [http://www.sans.org/newlook/digests/auto\\_audit.htm](http://www.sans.org/newlook/digests/auto_audit.htm).

## List of References

### Printed

\_\_\_\_\_, Déploiement et gestion de Microsoft Internet Security and Acceleration Server 2000, course work documentation, Material No: 2160ACP.

Bierman, Harold Jr., Charles P. Bonini and Warren H. Hausman, Quantitative Analysis for Business Decisions, Fifth Edition, ISBN: 0-256-01918-5, Richard D. Irwin, Inc., 1977.

Carroll, Dr. John M., Computer Security, ISBN: 0-913708-28-3, Butterworth Publishers, 1977.

Cole, Eric, Hackers Attention Danger!, ISBN: 2-7440-1273-4, CampusPress, 2001. (Originally published in English by New Riders Publishing. Title: Hackers Beware.)

Holzer, Juergen and Marc Pflugmann, TCP/IP, ISBN: 2-7429-2044-7, Micro Application, 2001.

McClure, Stuart, Joel Scambray and George Kurtz, Hacking Exposed: Network Security Secrets and Solutions, ISBN: 0-07-212127-0, Osborne/McGraw-Hill, 1999.

Northcutt, Stephen, Track 7 – Auditing Networks, Perimeters and Systems, Sans Institute, (<http://www.sans.org>), course material, Sans Conference, San Diego, California, October 2001.

Shinder, Dr. Thomas W. and Debra Littlejohn Shinder, Configuring ISA Server 2000: Building Firewalls for Windows 2000, ISBN: 1-928994-29-6, Syngress Publishing, Inc., 2001.

Simmons, Kim and Masaru Ryumae, MSCE ISA Server 2000, ISBN: 1-57610-957-7, Coriolis, 2001.

### Internet

Center for Internet Security, <http://www.cisecurity.org>

CERT, <http://www.cert.org>

Common Vulnerabilities and Exposures, <http://cve.mitre.org>

Hping2, <http://www.hping.org/>

Nessus, <http://www.nessus.org>

Internet Security Systems, <http://www.iss.net/>

Internet Security Systems, Description of Loki, <http://xforce.iss.net/static/1452.php>

ISAServer.org, <http://www.isaserver.org>

ISCA Labs, Certification Report on ISA Server,  
<http://www.icsalabs.com/html/communities/firewalls/certification/rxvendors/microsoftisas2000/index.shtml>

Microsoft ISA Server, <http://www.microsoft.com/isaserver/>

Nmap, <http://www.insecure.org/nmap>

NmapNT, <http://www.eeye.com/html/Research/Tools/nmapnt.html>

Reverse WWW Shell, Description of, <http://packetstorm.widexs.nl/groups/thc/fw-backd.htm>

SANS, <http://www.sans.org>

SANS/FBI Top 20 Vulnerabilities, <http://www.sans.org/top20.htm>

SANS Firewall Checklist, [http://www.sans.org/checklist/firewall\\_check.htm](http://www.sans.org/checklist/firewall_check.htm)

TCPdump, <http://www.tcpdump.org/>

Windump, <http://netgroup-serv.polito.it/windump/>

© SANS Institute 2000 - 2002, Author retains full rights.