



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>

Auditing a Microsoft Internet Security and Acceleration 2004 Server as it Protects Outlook Web Access 2003

An Internal Auditor's Perspective

By

Peter Denticio, CISSP
GSNA Practical Assignment
Version 3.2, Option 1
October 19, 2004

Abstract:

I will be performing an audit on a Microsoft Internet Security and Acceleration (ISA) 2004 Server from the perspective of an internal auditor. I will ascertain whether or not the Microsoft ISA server has been implemented in accordance to our organization's internally developed configuration standard. Also, I will be taking into consideration that this ISA Server is not configured as a firewall, but is in this one Interface configuration, acting as a reverse-proxy to our Exchange 2003 Environment. It just happens that it also provides some application-layer firewall capabilities in the process.

Note: Pay particular attention to the scope, as it's strictly limited to retain focus throughout this audit process.

© SANS Institute 2004, Author retains full rights

Table of Contents

Introduction:	4
1. - Research in Audit, Measurement Practice and Control	5
1.1 Description of the system	5
Section A - Scope	5
Section B – Describe the system and its role in the organization	6
Section C – What is a secure configuration?	9
1.2 Describe the most significant risks to the system	10
1.3 Current State of Practice	11
2. – Create Audit Checklist	12
3. – Perform Audit	24
4. – Audit Report	63
4.1 Executive Overview	63
4.2 Findings	64
4.3 Conclusion	72
References	73

© SANS Institute 2004, Author retains full rights

Introduction:

It's ironic that today's Internet has become more like a battlefield, considering that the origin of what became the Internet was spawned out of the Advanced Research Projects Agency (ARPA), an arm of the Defense Department.

General Douglas MacArthur once said *"There is no security on earth; there is only opportunity."* It appears to me that hackers, crackers, or whatever term is politically correct this week, have taken what this former military leader said a bit too literally. They seem to think that any system that they can get to is an opportunity for them. I'm reasonably certain that was not what was meant by MacArthur's statement, but it seemed to fit the "war" that we as security professionals are fighting.

The Internet has had an enormous impact on our daily business and personal lives. It's almost impossible to find an organization that does not have some reliance on the Internet for conducting business, even if it's only for email.

Today most organizations' reliance on email in their day to day business has increased to a point that email is a critical system in many IT operations. To that end, the typical organization will look for ways to allow their employees to access their email while they're away from the office. There are several methods available today; handhelds, smart-phones, laptops, and the ubiquitous web browser available just about wherever you may find yourself.

There are many ways of remotely accessing an Exchange 2003 system. The four main ones are:

1. Virtual Private Network (VPN)
2. Handheld devices (Blackberry or OMA)
3. Outlook Web Access (OWA)
4. RPC over HTTP

Our organization has been using VPN and handheld technologies for quite some time with older versions of Microsoft Exchange, both of which have been proven to provide sufficient levels of security controls. Unfortunately, both the VPN, and handheld options for remote access have their own specific drawbacks when it comes to usability, administrative, financial, as well as security considerations.

VPN connectivity, before Exchange 2003, was one of the most secure ways of accessing Exchange remotely as long as it is configured properly. However, it may not be the most cost effective means of achieving remote access.

Depending on how you deploy your VPN infrastructure, there are many factors that weigh in. We do provide VPN access for network access, but seeing as that is not the subject of this paper we will not be going any further down that road.

In a lot of organizations handheld devices are all the rage. The drawback to these cutting edge devices is they are rather costly. Not only are the devices and their monthly wireless bills expensive, but the administrative overhead they place on IT departments is fairly steep as well. Again, we provide this method of access for certain individuals, but it's not cost effective to give out handheld devices to all employees in order to provide remote email access.

When it comes right down to it, not everyone will need full access to all network resources. For those who don't, and also don't warrant the necessity of a handheld device, there are two other methods of remote access that we've chosen for our Exchange 2003 users; Outlook Web Access (OWA) or Remote Procedure Call (RPC) Over HTTP (Actually HTTPS in our case).

According to Microsoft's "Exchange Server 2003 and Exchange 2000 Server Front-End and Back-End Topology Guide"¹ In Chapter 6;

The preferred method of deployment is for the front-end server to be on the intranet with the back-end servers and to use an advanced firewall as your perimeter network. You only need to follow this section if you have certain requirements where you must place your Exchange front-end server in the perimeter network.

Combining the previous Microsoft quote and a risk assessment (see section 1.2), our organization has decided to implement a Microsoft Internet Security and Acceleration (ISA) 2004 Server to help mitigate the security risks involved in allowing access to an internal system from the Internet. In the configuration our organization has deployed it will act as both a reverse proxy, and an application layer firewall.

1. - Research in Audit, Measurement Practice and Control

1.1 Description of the system

Section A - Scope

I am limiting the scope of this audit to just the ISA 2004 Server and the relevant portions of the firewall and Exchange Front End Server configuration. If I were to expand the scope to fully include the firewall and Front End Server it would make this an exceedingly long process and lose the objectivity of the audit. Also, I am limiting the physical security aspects to just gaining access to the ISA server. If I were to include all other factors such as, environment, power etc. it would turn into a full data center audit, as well.

Section B – Describe the system and its role in the organization.

Our organization has deployed Outlook Web Access utilizing the Microsoft Internet Security and Acceleration (ISA) 2004 Server in combination with both Front-end and Back-end Exchange 2003 Servers.

According to Microsoft's ISA Server 2004 literature² *"ISA Server 2004 provides unique levels of protection for OWA Web sites. With the easy-to-use interface of ISA Server 2004, organizations can quickly set up a Web publishing rule that enforces secure forms-based authentication. ISA Server 2004 also stops attacks against e-mail servers, both through Secure Sockets Layer (SSL) decryption, which enables SSL traffic to be inspected for malicious code, and through HTTP filtering, which provides deep inspection of application content. In addition, ISA Server 2004 uses preauthentication to prevent anonymous user logins, a key attack vector aimed at internal servers."*

The ISA 2004 Server includes a forms-based authentication (FBA) filter for screening all communications to the Outlook Web Access server. The FBA filter will expire connections based on a specified period of time and forces users to re-authenticate. More importantly the FBA filter prevents the caching of user credentials to the local browser. Both of these features of the FBA filter mitigate the two biggest risks in using Outlook Web Access on Internet kiosks and other publicly accessible web browsers. The FBA filter also forces the use of SSL encryption, which is not used as often as you would think.

Another key feature of the forms-based authentication is the ability for the ISA server to act as an intermediary, whereas the user does not connect directly to the OWA server unauthenticated. The ISA Server actually accepts the authentication requests and passes the user on to the OWA server only after they have filled out the authentication form, thus preventing any direct unauthenticated access directly with the Exchange Front-End Server.

Our organization has put together a standards document for implementing this solution for us. They have done considerable research and invested a lot of resources into this standard. It is a 60 page document with a lot of graphics and screenshots, so I will sum up the main configuration ideas, as well as directing you to look over *diagram 1* to get a visual idea of how it is configured.

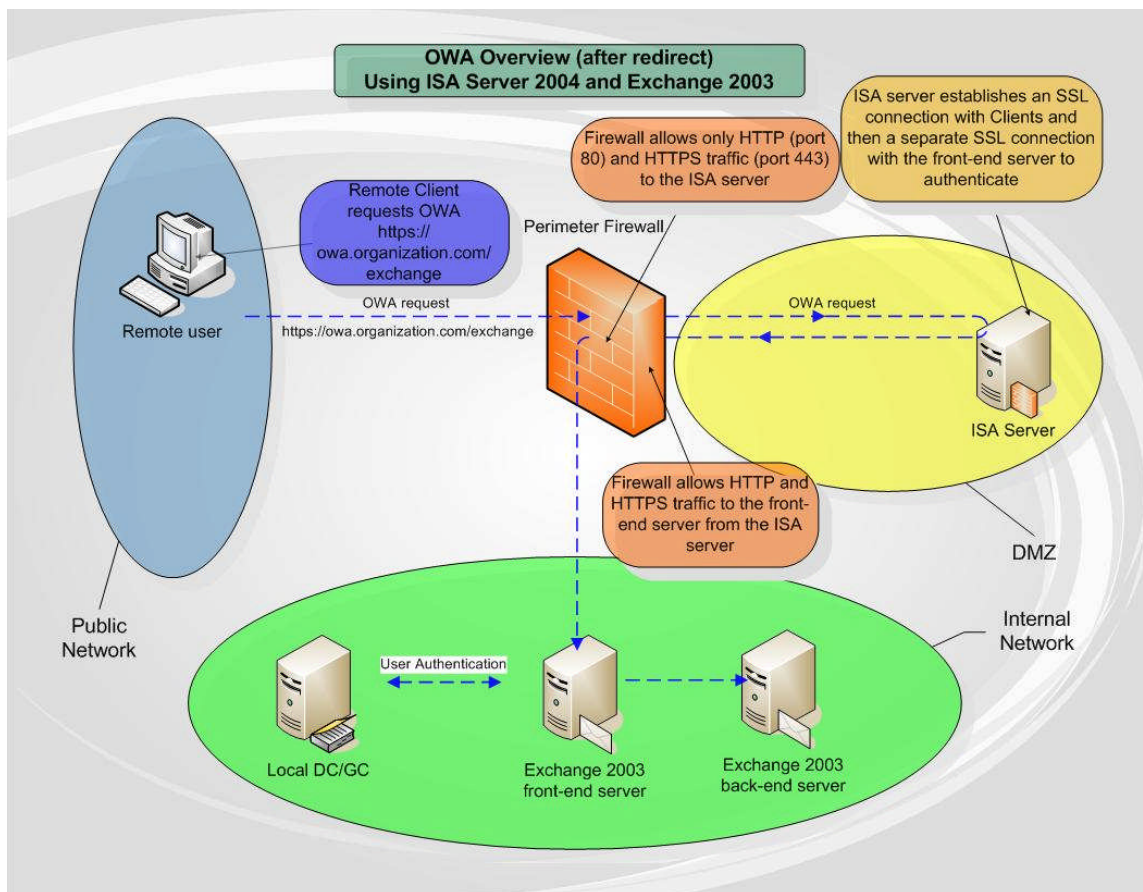


Diagram 1

Our organization has a standard firewall configuration that will not be a part of this audit, except for its use in the information flow of this system. The firewall will limit access to the ISA server to only the necessary ports to establish the communications, as described below. As you can see in diagram 1, the ISA server resides in a DMZ behind a firewall.

The firewall translates the IP addresses as they come into the DMZ, from public to private addressing. The access from the ISA server into the Internal network is not translated, but is locked down to specific IP addresses and ports that can traverse the firewall from the DMZ to the Internal network.

The ISA 2004 Server works in this unhomed, or single network interface configuration, as a reverse-proxy or web-cache. When you “publish” a web page or service, the ISA 2004 server creates a “listener” that listens on a particular IP address and port that you specify. The listener will proxy³ your request on to the server on our Internal network. The complete process is as follows:

1. A client attempts to open a connection to <http://owa.organization.com>, we use this in conjunction with a redirect to simplify the access.

2. In our case DNS tells us that owa.organization.com is xxx.xxx.xxx.172 and sends an HTTP request to this address on TCP port 80.
3. The firewall lets this in because there is a rule that permits anything to connect to TCP port 80 on the xxx.xxx.xxx.172 address and translates incoming requests on this address to the DMZ IP address of 192.168.xxx.34.
4. The ISA server has a listener on TCP port 80 on 192.168.xxx.34 that allows only **two** acceptable URL's to be proxied on to the Internal network. <http://owa.organization.com> and <http://owa.organization.com/exchange> (All others are refused by way of limiting the URL within the HTTP filter on the ISA listener). These two possible requests are proxied to the Exchange 2003 Front End Server on IP address 192.168.xxy.103 which is not translated by the firewall but has a rule to allow 192.168.xxx.34 to connect to 192.168.xxy.103 on TCP port 80.
5. The Exchange Front End Server has a separate web server instance listening on 192.168.xxy.103 on TCP port 80 that has only the /default.htm and /exchange/default.htm files in it. The default.htm file is a simple redirect to the full HTTPS URL <https://owa.organization.com/exchange>.
6. The browser then attempts a connection on to the same IP address of xxx.xxx.xxx.172 on TCP port 443 using the above URL. The firewall lets this in because there is a rule permitting anything to connect to TCP port 443 on the xxx.xxx.xxx.172 address and translates incoming requests on this address to the DMZ IP address of 192.168.xxx.34.
7. The ISA server has a listener on TCP port 443 on 192.168.xxx.34. This listener has the FBA filter enabled on it which forces the user to provide credentials for authentication before sending on the authentication request.
8. When the user fills out the authentication form, the request with the credentials gets proxied on to the Front End server using HTTPS communications on IP address 192.168.xxy.103. This is allowed by a firewall rule that permits TCP communications on port 443 between IP address 192.168.xxx.34 of the OWA listener on the DMZ network and IP address 192.168.xxy.103 of the OWA web site on the Front End server on the Internal network.
9. Because of the ISA server based FBA filter, the Front End Server will not receive any "anonymous" user requests. The form will not send a request unless the authentication information is filled out. The logon credentials are passed from the ISA Server to the Front End Server and then to the Active Directory Domain Controller for authentication to the Exchange 2003 system.
10. After successful logon we have a happy Outlook Web Access user.
11. The FBA filter authenticates you without the use of a cookie so no authentication information is stored on the machine you establish your connection on.
12. The FBA filter will logoff the user after a specified timeout period, which can be set differently for when you are accessing OWA from a public web

browser, such as an Internet kiosk or Internet café, or when you access from a private browser, such as home workstation or laptop.

Section C – What is a secure configuration?

The following are the main configuration points from our internal standard for the secure implementation of an ISA 2004 Server as a connection point for external email web access:

- Place ISA Server in DMZ behind existing standard firewall. (Audit checklist # 1)
- Place ISA Server in physically protected environment. (Audit checklist # 2)
- Disable all un-needed services on the ISA Server. (Audit checklist # 3)
- Make sure all patches have been applied. (Audit checklist # 4)
- Disable Microsoft Management Console (MMC) Access. (Audit checklist # 5)
- Only allow Remote Administration access from our internal network. (Audit checklist # 6)
- Only allow TCP ports for HTTP (80) and HTTPS (443) traffic for OWA IP address from Internet to DMZ. (Audit checklist # 7)
- Only allow HTTP (TCP port 80) and HTTPS (TCP port 443) traffic for OWA traffic on 192.168.xxx.34 from DMZ to 192.168.xxy.103 on Internal Network. (Audit checklist # 8)
- Only allow HTTPS (TCP port 443) to be enabled on the OWA Listener for the OWA IP address (in this case 192.168.xxx.34). (Audit checklist # 9)
- Only allow the two URL's <http://owa.organization.com> and <http://owa.organization.com/exchange> to be accepted on the redirect listener. Refuse all others. (Audit checklist # 10)
- On Exchange front End Server verify the there are separate Redirect and Exchange Outlook Websites using HTTP and HTTPS respectively. Redirect website should have /default.htm and /exchange/default.htm files only. (Audit Checklist # 11)
- Within Forms-Based authentication set timeout to 22 minutes on “public” browser and 60 minutes for “private”. (Audit checklist # 12)

Note: Due to the scope limit of just the ISA server as a security control for Outlook Web Access to an Exchange 2003 system, we are going to assume for this exercise that the Exchange Front End Server has already passed its own audit. We will however check some items such as, Audit checklist # 11, on the Front End server as it directly pertains to this audit scope. In a real life audit we would check the Front End server for physical security, patches, etc.

1.2 Describe the most significant risks to the system

The ISA 2004 Server itself is in place to mitigate the risks normally associated with exposing a Microsoft Exchange Server running IIS to the Internet. These risks exist even though the server may reside behind a firewall. There are also risks inherent in any system that is used to conduct business on a daily basis.

On page 14 of the NIST Special Publication 800-30⁴ document entitled “Risk Management Guide for Information Technology Systems” it defines Risk as:

“**Risk** is a function of the **likelihood** of a given **threat-source’s** exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organization.”

The following Threat table illustrates the two major threats that face a standard OWA implementation.

Threat Table			
No.	Threat Description	Possible Sources	Likelihood
1	Attacks on IIS by means of HTTP based exploits	Hackers, Virus/Worm propogation,	High
2	Attacks on other OS based services or misconfiguration	Hackers, Virus/Worm propogation	High
3	Anonymous access to OWA Server	Hackers, Virus/Worm propogation	High
4	Session hijack on public browsers	Hackers, disgruntled employees, competitors	Medium

You would think the assets that are affected by the Outlook Web Access solution are strictly limited to email and its possibility of confidentially risk if that email were to be compromised. However there are other issues to be considered. If the OWA Server were to be compromised it could be an access point to all other systems within a given environment. If a users logon credentials were compromised they could conceivably be used to access other systems on your network. With that thought in mind the following assets table will illustrate the assets that could be affected by a security breach on the OWA server in our environment.

Assets Table	
No.	Asset
1	Remote Access to email
2	Proprietary Data
3	Confidential Client Data

The last category to explore in the realm of risk is Vulnerability. The following table will describe the major vulnerabilities of the Exchange OWA system, as well as evaluate the degree of exposure and the potential impact on the organization in the event of successful exploitation.

Vulnerability Table			
No.	Vulnerability	Exposure	Impact
1	Patches not up to date	High	Data Compromise, Server unavailability
2	misconfiguration	High	Data Compromise, Server unavailability

1.3 Current State of Practice

With the release of the Microsoft Internet Security and Acceleration 2004 Server product there has been more activity in providing better security for remote email access.

I've personally seen fairly large companies using Exchange Outlook Web Access with no encryption, which in turn sends clear text logon credentials over the Internet!! The usual answer when questioned on this practice is "It's only E-mail." I usually respond with, "The username and password that you're sending in clear text over the Internet is also your username and password for logging on to your corporate network. Do you usually hand that information out to anyone who asks?"

There is a wealth of information on the following sites that pertain to the configuration and protection of remote email services for Exchange systems. There are several articles and tutorials on each of these sites.

Microsoft's ISA Server home page⁵
<http://www.microsoft.com/isaserver>

The ISAServer.org Web Site⁶
<http://www.isaserver.org>

The MSEXchange.org Web Site⁷
<http://www.msexchange.org>

2. – Create Audit Checklist

ITEM #	Item Title
1	Proper Placement of ISA server in DMZ
Reference	
NIST Special Publication 800-44 entitled “Guidelines on Securing Public Web Servers” tells us in Section 8.1 “Network location is the first and in many respects most critical networking decision that affects Web server security.”	
Risk	
Placement of ISA Server on Internal network could expose internal environment to possible security risks if for any reason the ISA server is compromised. This is a high risk as it could compromise other internal servers. The likelihood is also high.	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none">1. Physically verifying the placement of server, by tracing back the network cable to the specific DMZ switch.2. Correlating the interface information from the firewall configuration to match up with the interface configuration on the ISA server.	

Audit Item #1 Evidence:

Audit Item #1 Findings:

ITEM #	Item Title
2	Physical Server Security
Reference	
<p>CERT published "Securing Network Servers", in the section entitled "Allow only appropriate physical access to computers" it states, "If unauthorized persons can physically access a computer, the integrity of that system is at considerable risk. If a system is connected to internal networks, then intruders can access resources in a way that bypasses all of your network perimeter defenses."</p> <p>http://www.cert.org/security-improvement/practices/p074.html</p>	
Risk	
<p>There are many risks to be mitigated by having proper physical security. Such as, theft, tampering, data access, and data compromise. For this audit we are not going to look at environmental risks, only whether someone can physically access the system. The environmental risks would fall under a Data Center audit, which is out of scope for this audit</p>	
Objective or Subjective	Objective
Testing Procedure	
<p>1. Verify that server is in a locked data center</p>	

Audit Item #2 Evidence:

Audit Item #2 Findings:

ITEM #	Item Title																																								
3	Disabling of un-needed services on the ISA server																																								
Reference																																									
<p>Thomas Shinder authored a checklist for securing an ISA 2000 Server. It still has merit for the ISA 2004 server even though there are some major differences in the two. http://www.isaserver.org/tutorials/ISA_Server_Security_Checklist_Part_1_Securing_the_Operating_System_and_the_Interface.html</p> <p>“Microsoft Windows Server 2003 Security Guide” for additional information on this. http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en</p> <p>There are a few services that were added to the list by our internal ISA configuration standard, as well as some services that are disabled by default. They are denoted by asterisks.</p>																																									
Risk																																									
Every un-needed service introduces the possibility of more vulnerabilities. It's always prudent to reduce this risk.																																									
Objective or Subjective	Objective																																								
Testing Procedure																																									
<p>Check that the following un-needed services are disabled:</p> <table> <tbody> <tr> <td>Alterer</td><td>Network DDE DSDM*</td></tr> <tr> <td>Automatic Updates</td><td>Network Location Awareness (NLA)</td></tr> <tr> <td>Background Intelligent Transfer Service</td><td>Performance Logs and Alerts</td></tr> <tr> <td>Clipbook</td><td>Print Spooler</td></tr> <tr> <td>Computer Browser</td><td>Routing and Remote Access*</td></tr> <tr> <td>DHCP Client</td><td>Server</td></tr> <tr> <td>Distributed File System</td><td>Telnet</td></tr> <tr> <td>Distributed Link Tracking Server*</td><td>Terminal Services Session Directory*</td></tr> <tr> <td>File Replication</td><td>Themes*</td></tr> <tr> <td>Human Interface Device Access*</td><td>Uninterruptible Power Supply*</td></tr> <tr> <td>IMAPI CD-Burning COM Service*</td><td>WebClient*</td></tr> <tr> <td>Indexing Service</td><td>Windows Audio*</td></tr> <tr> <td>Internet Connection Firewall (ICF) / (ICS)</td><td>Windows Image Acquisition (WIA)*</td></tr> <tr> <td>Intersite Messaging</td><td>Windows Installer</td></tr> <tr> <td>Kerberos Key Distribution Center</td><td>Windows Management Instrumentation</td></tr> <tr> <td></td><td>Windows Management Instrumentation Driver Extensions</td></tr> <tr> <td>License Logging</td><td>Wireless Configuration*</td></tr> <tr> <td>Messenger</td><td>WMI Performance Adapter</td></tr> <tr> <td>NetMeeting Remote Desktop Sharing</td><td></td></tr> <tr> <td>Network DDE</td><td></td></tr> </tbody> </table>		Alterer	Network DDE DSDM*	Automatic Updates	Network Location Awareness (NLA)	Background Intelligent Transfer Service	Performance Logs and Alerts	Clipbook	Print Spooler	Computer Browser	Routing and Remote Access*	DHCP Client	Server	Distributed File System	Telnet	Distributed Link Tracking Server*	Terminal Services Session Directory*	File Replication	Themes*	Human Interface Device Access*	Uninterruptible Power Supply*	IMAPI CD-Burning COM Service*	WebClient*	Indexing Service	Windows Audio*	Internet Connection Firewall (ICF) / (ICS)	Windows Image Acquisition (WIA)*	Intersite Messaging	Windows Installer	Kerberos Key Distribution Center	Windows Management Instrumentation		Windows Management Instrumentation Driver Extensions	License Logging	Wireless Configuration*	Messenger	WMI Performance Adapter	NetMeeting Remote Desktop Sharing		Network DDE	
Alterer	Network DDE DSDM*																																								
Automatic Updates	Network Location Awareness (NLA)																																								
Background Intelligent Transfer Service	Performance Logs and Alerts																																								
Clipbook	Print Spooler																																								
Computer Browser	Routing and Remote Access*																																								
DHCP Client	Server																																								
Distributed File System	Telnet																																								
Distributed Link Tracking Server*	Terminal Services Session Directory*																																								
File Replication	Themes*																																								
Human Interface Device Access*	Uninterruptible Power Supply*																																								
IMAPI CD-Burning COM Service*	WebClient*																																								
Indexing Service	Windows Audio*																																								
Internet Connection Firewall (ICF) / (ICS)	Windows Image Acquisition (WIA)*																																								
Intersite Messaging	Windows Installer																																								
Kerberos Key Distribution Center	Windows Management Instrumentation																																								
	Windows Management Instrumentation Driver Extensions																																								
License Logging	Wireless Configuration*																																								
Messenger	WMI Performance Adapter																																								
NetMeeting Remote Desktop Sharing																																									
Network DDE																																									

Audit Item #3 Evidence:

Audit Item #3 Findings:

ITEM #	Item Title
4	Make sure patches are up to date on ISA Server and check for other vulnerabilities
Reference	
<p>For the Windows 2003 underlying operating system, check on the Microsoft Security Bulletin Search. http://www.microsoft.com/technet/security/CurrentDL.aspx</p> <p>For the ISA 2004 Server, check the Windows Security Site and also check the ISA Server download section on Microsoft's web site. http://www.microsoft.com/isaserver/downloads/2004.asp</p>	
Risk	
Security patches fix known vulnerabilities to the system.	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. For the OS Run Microsoft Baseline Security Analyzer which will check the current OS patches by comparing what's installed to the downloaded mssecure.xml file from Microsoft. 2. For the ISA 2004 server, check the Microsoft web site (At the time of this writing there were ISA 2004 security patches). 3. Run a Nessus Vulnerability scan against the ISA server from the DMZ network. 	

Audit Item #4 Evidence:

Audit Item #4 Findings:

ITEM #	Item Title
5	Disable Microsoft Management Console for remote access.
Reference	
<p>There seems to be a serious lack of evidence supporting whether there is any form of encryption while utilizing the MMC remote administration for the ISA server. For that reason we will not be using this form of remote administration until we look further into this issue. We will stick to Terminal Services for remote administration for its inherent encryption. As of SP2 on Windows 2000 128 bit encryption is mandatory.</p> <p>http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/128bit.asp</p>	
Risk	
<p>Reduce likelihood of eavesdropping on administrative communications by ensuring encryption is in use. Protects passwords and configuration "leakage".</p>	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. Verify that Microsoft Management Console (MMC) access is disabled in the System Policy Editor. . On the ISA server start the ISA Management Console and click on Firewall Policy then on the right side pane click on Tasks. Under System Policy Tasks click on Edit System Policy. Then under the Remote Management folder click on Microsoft Management Console (MMC) and verify that it is disabled. 2. Attempt to connect using the MMC from the DMZ, Internet and Internal networks. 	

ITEM #	Item Title
6	Restrict remote admin access to internal network using Terminal Services
Reference	
Personal experience is my guidance here. It's common sense to restrict administrative access to a single administrator computer or a restricted group of computers.	
Risk	
Reduce the risk of unauthorized administrative access to the ISA server.	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. Verify settings on the ISA server are set to allow Terminal Services only from administrative Network IP addresses 192.168.xxy.0/24 in our case. On the ISA server start the ISA Management Console and click on Firewall Policy then on the right side pane click on Tasks. Under System Policy Tasks click on Edit System Policy. Then under the Remote Management folder click on Terminal Server and verify that it is enabled. Then under the From tab verify that the Remote Management Computers group is there. Highlight the group and click Edit to verify the IP addresses in this group. 2. Attempt to connect via Terminal Services from the DMZ, Internet and Internal networks. 	

Audit Item #6 Evidence:

Audit Item #6 Findings:

ITEM #	Item Title
7	Verify that only HTTP and HTTPS are available to the OWA IP address from the Internet to the DMZ
Reference	
<p>NIST Special Publication 800-44 entitled "Guidelines on Securing Public Web Servers" tells us in Section 8.2.1 "a firewall that is protecting a Web server should block all access to the Web server from the Internet except for HTTP (TCP port 80) and/or HTTPS (TCP port 443)".</p>	
Risk	
<p>This system only needs HTTP and HTTPS, TCP ports 80 and 443 respectively to be accessible from the Internet into the DMZ (see diagram 1). To allow any other protocols and ports from the Internet into the DMZ network is unnecessary and introduces more risks due to misconfiguration or other system vulnerabilities.</p>	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. Check firewall access-list to verify access from Internet (any) to tcp ports 80 (www) and 443. 2. From a workstation outside of the firewall use Nessus to verify the open ports, which should only be TCP ports 80 and 443 on IP address xxx.xxx.xxx.174. This will also show the difference in a vulnerability scan from Outside the firewall and one done from the DMZ shown in test 4.3 	

Audit Item #7 Evidence:

Audit Item #7 Findings:

ITEM #	Item Title
8	Verify that only HTTP and HTTPS are open for OWA traffic from ISA OWA and OWA Redirect listeners on the DMZ network to the OWA and Redirect Sites on the Internal network.
Reference	
NIST Special Publication 800-44 entitled "Guidelines on Securing Public Web Servers" tells us in Section 8.2.1 "a firewall that is protecting a Web server should block all access to the Web server from the Internet except for HTTP (TCP port 80) and/or HTTPS (TCP port 443)".	
Risk	
Communications should be locked down as to only the necessary addresses, protocols and ports (see diagram 1). To allow any other addresses, protocols and ports from the DMZ into the Internal network is unnecessary and introduces more risks due to misconfiguration or other system vulnerabilities.	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. Using SuperScan from Foundstone.com on the ISA server, verify that the ISA address of 192.168.xxx.34 can only communicate with the Front End server IP of 192.168.xxy.103 on TCP ports 80 and 443 ports. Set the source IP address for 192.168.xxx.34, and scan for TCP and UDP. 2. Verify in the firewall policy that only DMZ IP address 192.168.xxx.34 is only permitted access to Internal address 192.168.xxy.103 on TCP ports 80 (HTTP) and 443 (HTTPS). 	

Audit Item #8 Evidence:

Audit Item #8 Findings:

ITEM #	Item Title
9	On ISA server the OWA listener should only be configured for HTTPS access (TCP port 443) on IP address for hostname owa.organization.com.
Reference	
<p>Personal experience and our internal standards document agree on this one. The OWA Redirect should be the only listener to allow HTTP communications. The actual OWA listener should be configured to only allow HTTPS communications to it. Although both of the Listeners answer on the same IP address they are logically separate.</p>	
Risk	
<p>This risk is if for any reason the client were to send logon credentials via HTTP rather than HTTPS, you could expose those credentials for them to be easily picked up on. The forms-based authentication will only work with HTTPS enabled; protecting this authentication process, but it should be checked anyway.</p>	
Objective or Subjective	Objective
Testing Procedure	
<p>Because both the OWA Redirect and the OWA Listeners share the same IP address (192.168.xxx.34) we will have to rely on the following tests to verify this functionality.</p> <ol style="list-style-type: none"> 1. Verify that the OWA Redirect is the only listener using HTTP by inspecting the OWA Redirect listener and make sure that the OWA Redirect is only set to listen on HTTP. Do this In the ISA Server management console. Highlight the Firewall Policy in the left side pane; then over in the right side pane under Toolbox – Web Listeners – OWA Redirect Listener – rightclick and then click on properties. Under the Networks tab it should be set for 192.168.xxx.34 and under the Preferences tab it should only have the HTTP enabled using port 80. Then click on Authentication and only “integrated” should be checked. 2. Follow the same steps in test 1 to verify that the OWA Listener is set to 192.168.xxx.34 under the Network tab, HTTPS (SSL) port 443 under the Preferences tab. Click on Authentication and verify that OWA Forms-Based is the only one checked. 	

Audit Item #9 Evidence:

Audit Item #9 Findings:

ITEM #	Item Title
10	Only allow the two URL's http://owa.organization.com and http://owa.organization.com/exchange to be accepted on the redirect listener. Refuse all others.
Reference	
Personal experience and the Internal configuration document are the source of this check.	
Risk	
Because the OWA Redirect listener is set to listen on HTTP port 80, there is the possibility of someone or something trying to exploit the service by sending either a buffer overflow or some other malformed http request. By locking the site down to only allow these two URL's we can mitigate that risk.	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. On the ISA server verify that the OWA Redirect Publishing Rule set properly. Under the Firewall Policy view double-click the OWA Redirect Rule. Then click on the Traffic tab. Click on Paths there should only be two paths "/" and "/exchange/". 2. Verify Error for wrong paths in ISA server 3. From Browser verify that http://owa.organization.com and http://owa.organization.com/exchange redirect you properly to the Forms-Based Authentication page. 1. By trying different incorrect forms of the URL's verify that you get the error message "Error Code: 403 Forbidden. The server denied the specified Uniform Resource Locator (URL). Contact the server administrator. (12202)" If the "Paths" restriction wasn't in place it would pass the "malformed" URL's to the Front End Exchange Server and receive a "page not found" error. 	

Audit Item #10 Evidence:

Audit Item #10 Findings:

ITEM #	Item Title
11	On Exchange front End Server verify the there are separate Redirect and Exchange Outlook Websites using HTTP and HTTPS respectively. Redirect website should have /default.htm and /exchange/default.htm files only.
Reference	
<p>The sources of this control are personal experience, our Internal Standards document and the article by Thomas Shinder found at this link⁸, http://www.isaserver.org/tutorials/ISA_Server_Security_Checklist_Part_1_Securing_the_Operating_System_and_the_Interface.html, which states “Do Not Install Applications and Services on the ISA Server”. Even though the ISA Server is proxying all connections to the Front End Exchange Server, we felt that it was necessary to separate the Redirect site and the OWA site within the Front End Server. It was felt to be a security risk to install IIS on the ISA server had to allow this functionality on Front End Exchange Server. The actual redirect script is housed on the Front End Exchange Server in a separate site within IIS listening on HTTP port 80 only. The OWA site is a separate site listening on the same IP address but only on HTTPS port 443.</p>	
Risk	
<p>In order to allow the redirection (a requirement we have to live with) to take place we have to allow unauthenticated web access to the redirect script. To have this script be in the same “site” as the OWA code could expose the OWA site to anonymous connection attempts.</p>	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. On the Exchange Front End Server verify that there are two separate web “sites” running. Open the Internet Information Services (IIS) Manager and expand the Web Sites folder. There should be an owa.organization.com site and an OWA http redirect site. You can also see in the right pane the address is 192.168.xxy.103 and the TCP port is set to 80 for the OWA http redirect, and that for the owa.organization.com site the SSL port is set to 443. 2. In the IIS Manager highlight the owa.organization.com web site and view the path structure in the right pane. 3. In the IIS Manager highlight the OWA http redirect web site and view the path structure in the right pane. 	

ITEM #	Item Title
12	Within Forms-Based authentication set timeout to 22 minutes on “public” browser and 60 minutes for “private”.
Reference	
<p>The timeouts for the Forms-Based authentication are set by default to 22 and 60 minutes for public and private respectively.</p>	
Risk	
<p>If the timeouts don't function properly someone could walk up to a session left open by an OWA user and possibly gain access. The timeout will help mitigate this risk.</p>	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. Verify settings on ISA OWA Listener. Do this In the ISA Server management console. Highlight the Firewall Policy in the left side pane; then over in the right side pane under Toolbox – Web Listeners – OWA Listener – rightclick and then click on properties. Then click on Preferences and then Authentication then click on Configure to verify the settings 2. Log into OWA using each of the choices of Public and Private and wait to see if they timeout properly. 	

Audit Item #12 Evidence:

Audit Item #12 Findings:

3. – Perform Audit

The top 10 out of the original 12 will be shown in this section.

ITEM #	Item Title
1	Proper Placement of ISA server in DMZ
Reference	
NIST Special Publication 800-44 entitled “Guidelines on Securing Public Web Servers” tells us in Section 8.1 “Network location is the first and in many respects most critical networking decision that affects Web server security.”	
Risk	
Placement of ISA Server on Internal network could expose internal environment to possible security risks if for any reason the ISA server is compromised. This is a high risk as it could compromise other internal servers. The likelihood is also high.	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none">1. Physically verifying the placement of server, by tracing back the network cable to the specific DMZ switch.2. Correlating the interface information from the firewall configuration to match up with the interface configuration on the ISA server.	

Audit Item #1 Evidence:

Test 1.1:

Physically verified the only network cable connected to the ISA server does, in fact, connect to the same switch Cisco 3500 Series switch on port 5 that the Firewall DMZ port is plugged into on port 6.

Test 1.2:

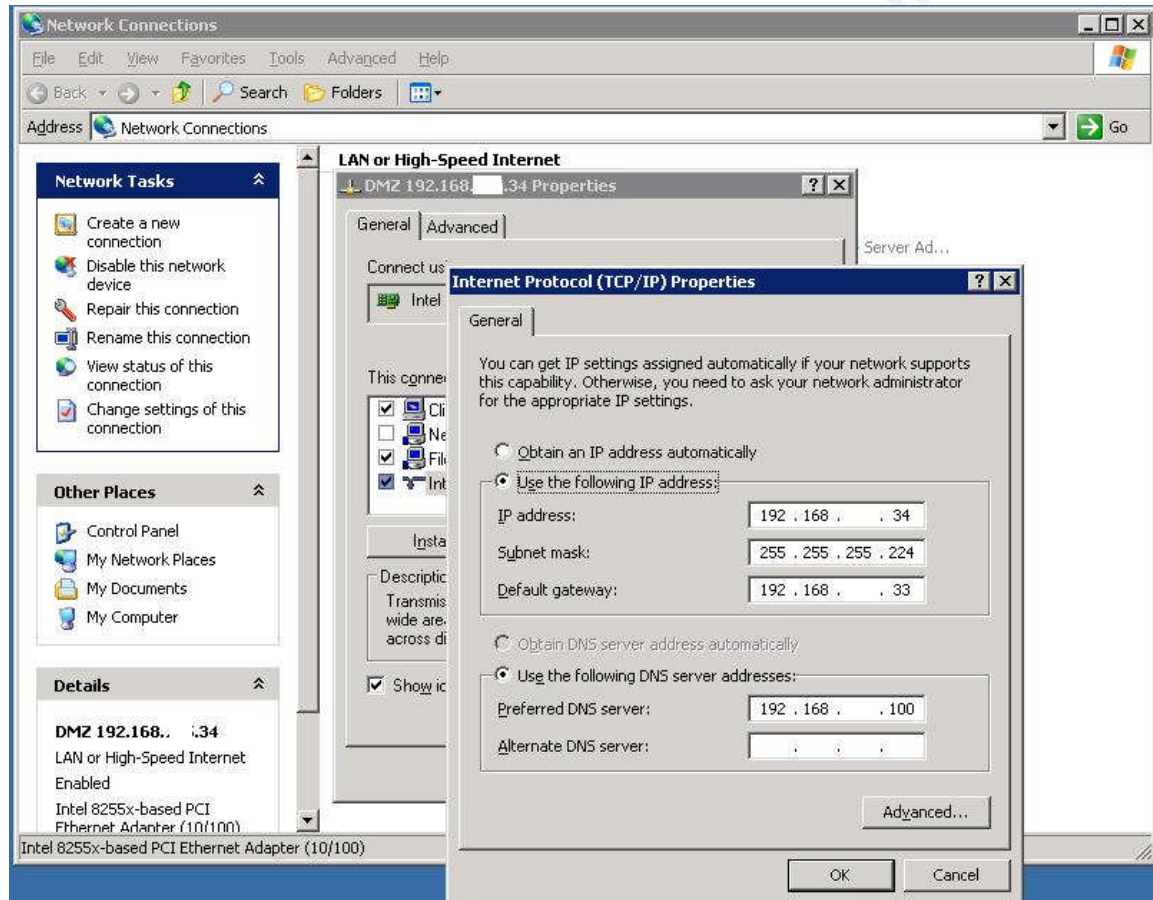
Interface information obtained from the Firewall configuration:

ip address outside xxx.xxx.xxx.172 255.255.255.192

ip address inside 192.168.xxy.4 255.255.255.0

ip address DMZ-slot:2 192.168.xxx.33 255.255.255.224

Interface information obtained from the ISA 2004 Server



Clearly the DMZ-slot2:2 Interface on the firewall and the DMZ interface (only one) on the ISA server share the same network.

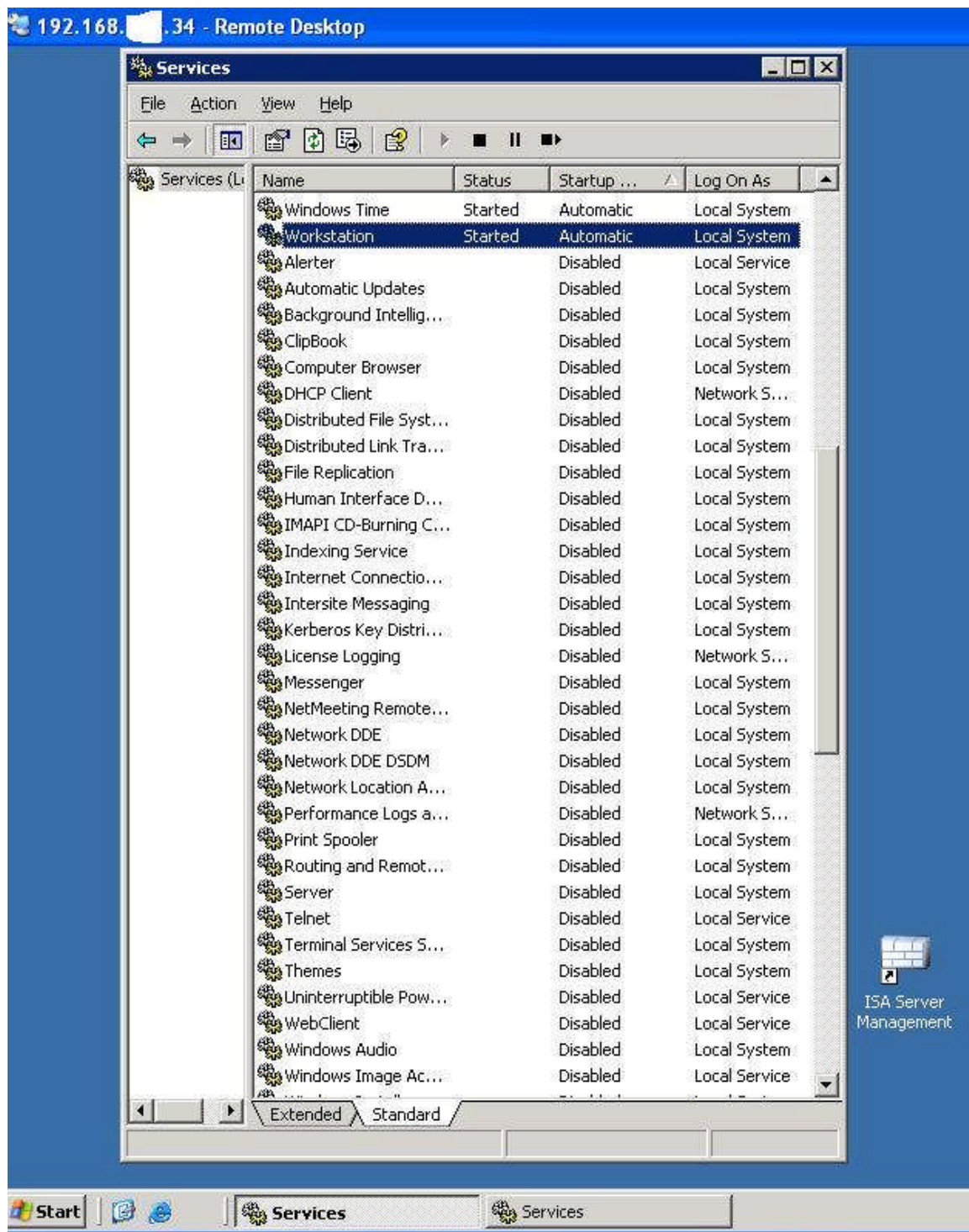
Audit Item #1 Findings: PASS

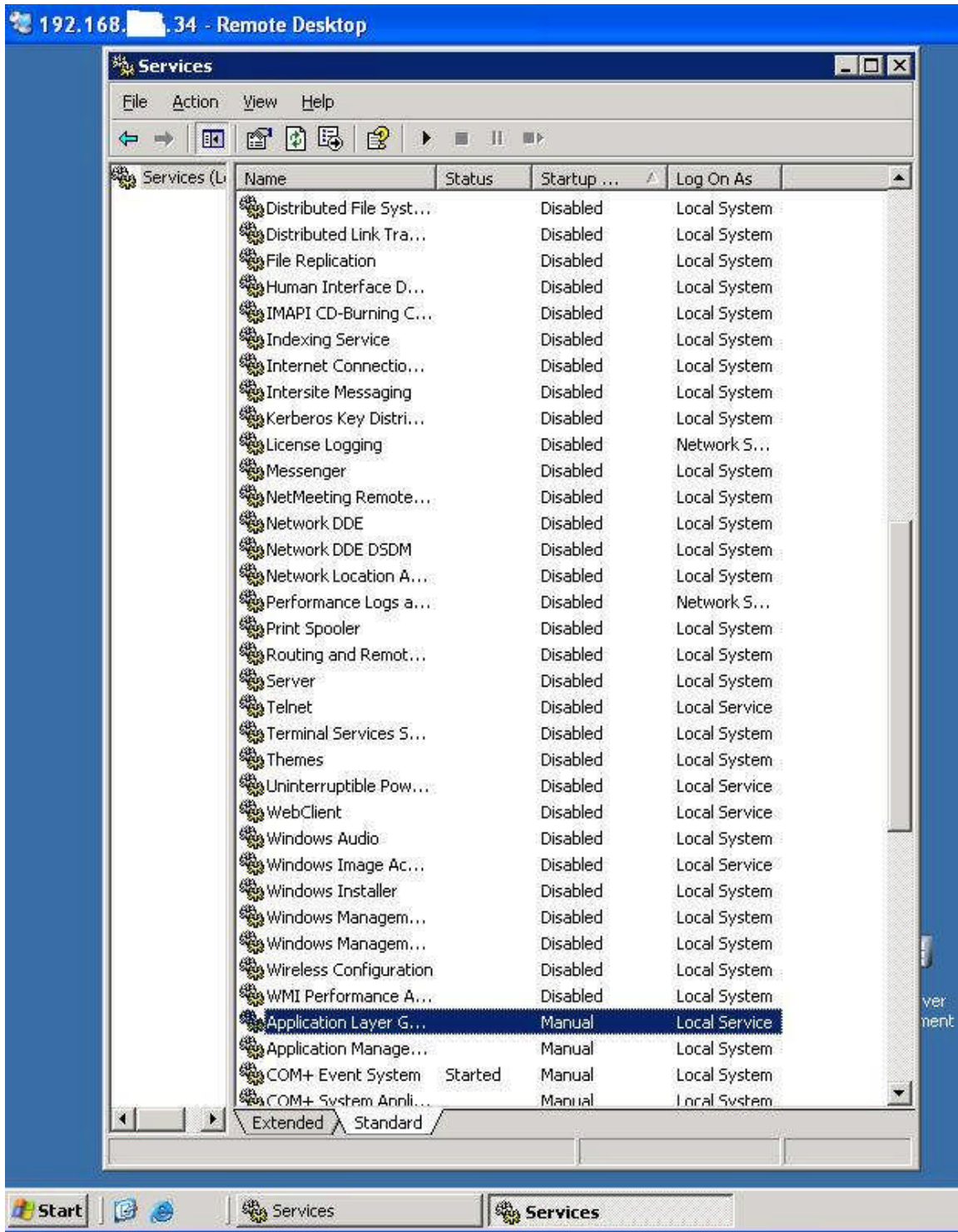
It was verified by these two tests that the ISA 2004 Server is deployed in an isolated DMZ segment as shown in diagram 1 in the system description section..

ITEM #	Item Title																																								
3	Disabling of un-needed services on the ISA server																																								
Reference																																									
<p>Thomas Shinder authored a checklist for securing an ISA 2000 Server. It still has merit for the ISA 2004 server even though there are some major differences in the two. http://www.isaserver.org/tutorials/ISA_Server_Security_Checklist_Part_1_Securing_the_Operating_System_and_the_Interface.html</p> <p>“Microsoft Windows Server 2003 Security Guide” for additional information on this. http://www.microsoft.com/downloads/details.aspx?FamilyId=8A2643C1-0685-4D89-B655-521EA6C7B4DB&displaylang=en</p> <p>There are a few services that were added to the list by our internal ISA configuration standard, as well as some services that are disabled by default. They are denoted by asterisks.</p>																																									
Risk																																									
Every un-needed service introduces the possibility of more vulnerabilities. It's always prudent to reduce this risk.																																									
Objective or Subjective	Objective																																								
Testing Procedure																																									
<p>Check that the following un-needed services are disabled by viewing services.</p> <table> <tbody> <tr> <td>Alterer</td><td>Network DDE DSDM*</td></tr> <tr> <td>Automatic Updates</td><td>Network Location Awareness (NLA)</td></tr> <tr> <td>Background Intelligent Transfer Service</td><td>Performance Logs and Alerts</td></tr> <tr> <td>Clipbook</td><td>Print Spooler</td></tr> <tr> <td>Computer Browser</td><td>Routing and Remote Access*</td></tr> <tr> <td>DHCP Client</td><td>Server</td></tr> <tr> <td>Distributed File System</td><td>Telnet</td></tr> <tr> <td>Distributed Link Tracking Server*</td><td>Terminal Services Session Directory*</td></tr> <tr> <td>File Replication</td><td>Themes*</td></tr> <tr> <td>Human Interface Device Access*</td><td>Uninterruptible Power Supply*</td></tr> <tr> <td>IMAPI CD-Burning COM Service*</td><td>WebClient*</td></tr> <tr> <td>Indexing Service</td><td>Windows Audio*</td></tr> <tr> <td>Internet Connection Firewall (ICF) / (ICS)</td><td>Windows Image Acquisition (WIA)*</td></tr> <tr> <td>Intersite Messaging</td><td>Windows Installer</td></tr> <tr> <td>Kerberos Key Distribution Center</td><td>Windows Management Instrumentation</td></tr> <tr> <td></td><td>Windows Management Instrumentation Driver Extensions</td></tr> <tr> <td>License Logging</td><td>Wireless Configuration*</td></tr> <tr> <td>Messenger</td><td>WMI Performance Adapter</td></tr> <tr> <td>NetMeeting Remote Desktop Sharing</td><td></td></tr> <tr> <td>Network DDE</td><td></td></tr> </tbody> </table>		Alterer	Network DDE DSDM*	Automatic Updates	Network Location Awareness (NLA)	Background Intelligent Transfer Service	Performance Logs and Alerts	Clipbook	Print Spooler	Computer Browser	Routing and Remote Access*	DHCP Client	Server	Distributed File System	Telnet	Distributed Link Tracking Server*	Terminal Services Session Directory*	File Replication	Themes*	Human Interface Device Access*	Uninterruptible Power Supply*	IMAPI CD-Burning COM Service*	WebClient*	Indexing Service	Windows Audio*	Internet Connection Firewall (ICF) / (ICS)	Windows Image Acquisition (WIA)*	Intersite Messaging	Windows Installer	Kerberos Key Distribution Center	Windows Management Instrumentation		Windows Management Instrumentation Driver Extensions	License Logging	Wireless Configuration*	Messenger	WMI Performance Adapter	NetMeeting Remote Desktop Sharing		Network DDE	
Alterer	Network DDE DSDM*																																								
Automatic Updates	Network Location Awareness (NLA)																																								
Background Intelligent Transfer Service	Performance Logs and Alerts																																								
Clipbook	Print Spooler																																								
Computer Browser	Routing and Remote Access*																																								
DHCP Client	Server																																								
Distributed File System	Telnet																																								
Distributed Link Tracking Server*	Terminal Services Session Directory*																																								
File Replication	Themes*																																								
Human Interface Device Access*	Uninterruptible Power Supply*																																								
IMAPI CD-Burning COM Service*	WebClient*																																								
Indexing Service	Windows Audio*																																								
Internet Connection Firewall (ICF) / (ICS)	Windows Image Acquisition (WIA)*																																								
Intersite Messaging	Windows Installer																																								
Kerberos Key Distribution Center	Windows Management Instrumentation																																								
	Windows Management Instrumentation Driver Extensions																																								
License Logging	Wireless Configuration*																																								
Messenger	WMI Performance Adapter																																								
NetMeeting Remote Desktop Sharing																																									
Network DDE																																									

Audit Item #3 Evidence:

Test 3.1:






```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\pete.dentico>net start
These Windows services are started:

COM+ Event System
Cryptographic Services
Distributed Link Tracking Client
Distributed Transaction Coordinator
DNS Client
Error Reporting Service
Event Log
Help and Support
IPSEC Services
Logical Disk Manager
Microsoft Firewall
Microsoft ISA Server Control
Microsoft ISA Server Job Scheduler
Microsoft ISA Server Storage
MSSQL$MSFW
Network Connections
Plug and Play
Protected Storage
Remote Access Connection Manager
Remote Procedure Call (RPC)
Remote Registry
Secondary Logon
Security Accounts Manager
Shell Hardware Detection
Symantec AntiVirus
Symantec AntiVirus Definition Watcher
Symantec Event Manager
Symantec Settings Manager
System Event Notification
Task Scheduler
TCP/IP NetBIOS Helper
Telephony
Terminal Services
Windows Time
Workstation

The command completed successfully.

C:\Documents and Settings\pete.dentico>_
```

Audit Item #3 Findings: PASS

By reviewing the three previous screenshots you can see that all of the Services that should be disabled, are disabled.

ITEM #	Item Title
4	Make sure patches are up to date on ISA Server and check for other vulnerabilities
Reference	
<p>For the Windows 2003 underlying operating system, check the Microsoft Security Bulletin Search. http://www.microsoft.com/technet/security/CurrentDL.aspx</p> <p>For the ISA 2004 Server, check the Windows Security Site and also check the ISA Server download section on Microsoft's web site. http://www.microsoft.com/isaserver/downloads/2004.asp</p>	
Risk	
Security patches fix known vulnerabilities to the system.	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. For the OS Run Microsoft Baseline Security Analyzer which, among other things, will check the current OS patches by comparing what's installed to the downloaded mssecure.xml file from Microsoft. 2. For the ISA 2004 server, check the Microsoft web site (At the time of this writing there were no ISA 2004 security patches). 3. Run a Nessus Vulnerability scan against the ISA server from the DMZ network. 	

Audit Item #4 Evidence:

Test 4.1:

Note: Please keep in mind that in the previous step we verified that the server service is disabled. The Microsoft Baseline Security Analyzer can not run without

the Server service running on the scanned machine. We enabled the Server service temporarily for this scan.

Computer name: DMZONE\XXXISA01
IP address: 192.168.xxx.34
Security report name: DMZONE - XXXISA01 (10-14-2004 2-54 PM)
Scan date: 10/14/2004 2:54 PM
Security update database version: 2004.10.12.0
Office update database version: 11.0.0.7005
Security assessment: Severe Risk (One or more critical checks failed.)

Security Updates

Score	Issue	Result	
Check Windows failed Security (critical) Updates		6 critical security updates are missing. 3 security updates could not be confirmed.	
	Security Update	Description	Reason
	MS04-030	Vulnerability in WebDav XML Message Handler Could Lead to a Denial of Service (824151)	File version is less than expected. [C:\WINDOWS\system32\msxml3.dll, 8.40.9419.0 < 8.50.2162.0]
	MS04-031	Vulnerability in NetDDE Could Allow Remote Code Execution (841533)	File version is less than expected. [C:\WINDOWS\system32\nddenb32.dll, 5.2.3790.0 < 5.2.3790.173]
	MS04-032	Security Update for Microsoft Windows (840987)	File version is less than expected. [C:\WINDOWS\system32\ntkrnlpa.exe, 5.2.3790.0 < 5.2.3790.175]

	MS04-034	Vulnerability in Compressed (zipped) Folders Could Allow Code Execution (873376)	File version is less than expected. [C:\WINDOWS\system32\zipfldr.dll, 6.0.3790.0 < 6.0.3790.198]
	MS04-037	Vulnerability in Windows Shell Could Allow Remote Code Execution (841356)	File version is less than expected. [C:\WINDOWS\system32\shell32.dll, 6.0.3790.168 < 6.0.3790.205]
	MS04-038	Cumulative Security Update for Internet Explorer (834707)	File version is less than expected. [C:\WINDOWS\system32\browseui.dll, 6.0.3790.186 < 6.0.3790.212]
	MS03-030	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	Please refer to 306460 for a detailed explanation.
	MS04-016	Vulnerability in DirectPlay Could Allow Denial of Service (839643)	Please refer to 306460 for a detailed explanation.
	MS04-028	Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)	Please refer to 306460 for a detailed explanation.
Check MSXML failed Security (non-critical) Updates	1 products are using a service pack not at the latest version or have other warnings.		
	Security Update MSXML 3.0	Description MSXML 3.0 SP4	Reason The latest service pack for this product is not installed. Currently SP4 is installed. The latest service pack is SP5.
Check Office passed Updates	No critical security updates are missing.		
Check SQL Server/M SDE Security Updates	Instance MSFW: No critical security updates are missing.		
Check Windows Media Player	No critical security updates are missing.		

Security Updates	
Check MDAC passed	No critical security updates are missing.
Security Updates	

Windows Scan Results

Vulnerabilities

Score	Issue	Result																				
Check failed (critical)	Automatic Updates	The Automatic Updates system service is not correctly configured.																				
Check failed (non-critical)	Password Expiration	Some user accounts (2 of 4) have non-expiring passwords. <table><tr><th>User</th><th>Weak Password</th><th>Locked Out</th><th>Disabled</th></tr><tr><td>Guest</td><td>Weak</td><td>-</td><td>Disabled</td></tr><tr><td>SUPPORT_388945a0</td><td>-</td><td>-</td><td>Disabled</td></tr><tr><td>ISAAdmin</td><td>-</td><td>-</td><td>-</td></tr><tr><td>pete.dentico</td><td>-</td><td>-</td><td>-</td></tr></table>	User	Weak Password	Locked Out	Disabled	Guest	Weak	-	Disabled	SUPPORT_388945a0	-	-	Disabled	ISAAdmin	-	-	-	pete.dentico	-	-	-
User	Weak Password	Locked Out	Disabled																			
Guest	Weak	-	Disabled																			
SUPPORT_388945a0	-	-	Disabled																			
ISAAdmin	-	-	-																			
pete.dentico	-	-	-																			
Best practice	Windows Firewall	Windows Firewall is not installed or configured properly, or is not available on this version of Windows.																				
Check passed	Local Account Password Test	Some user accounts (1 of 4) have blank or simple passwords, or could not be analyzed. <table><tr><th>User</th><th>Weak Password</th><th>Locked Out</th><th>Disabled</th></tr><tr><td>Guest</td><td>Weak</td><td>-</td><td>Disabled</td></tr><tr><td>SUPPORT_388945a0</td><td>-</td><td>-</td><td>Disabled</td></tr><tr><td>ISAAdmin</td><td>-</td><td>-</td><td>-</td></tr><tr><td>pete.dentico</td><td>-</td><td>-</td><td>-</td></tr></table>	User	Weak Password	Locked Out	Disabled	Guest	Weak	-	Disabled	SUPPORT_388945a0	-	-	Disabled	ISAAdmin	-	-	-	pete.dentico	-	-	-
User	Weak Password	Locked Out	Disabled																			
Guest	Weak	-	Disabled																			
SUPPORT_388945a0	-	-	Disabled																			
ISAAdmin	-	-	-																			
pete.dentico	-	-	-																			
Check passed	File System	All hard drives (1) are using the NTFS file system. <table><tr><th>Drive Letter</th><th>File System</th></tr><tr><td>C:</td><td>NTFS</td></tr></table>	Drive Letter	File System	C:	NTFS																
Drive Letter	File System																					
C:	NTFS																					
Check passed	Autologon	Autologon is not configured on this computer.																				
Check passed	Guest Account	The Guest account is disabled on this computer.																				
Check passed	Restrict Anonymous	Computer is properly restricting anonymous access.																				
Check passed	Administrators	No more than 2 Administrators were found on this computer. <table><tr><th>User</th></tr><tr><td>ISAAdmin</td></tr><tr><td>pete.dentico</td></tr></table>	User	ISAAdmin	pete.dentico																	
User																						
ISAAdmin																						
pete.dentico																						

Additional System Information

Score	Issue	Result												
Best practice	Auditing	Logon Success auditing is enabled, however Logon Failure auditing should also be enabled.												
Best practice	Services	Some potentially unnecessary services are installed.												
		<table><tr><th>Service</th><th>State</th></tr><tr><td>Telnet</td><td>Stopped</td></tr></table>	Service	State	Telnet	Stopped								
Service	State													
Telnet	Stopped													
Additional Shares information	2 share(s) are present on your computer.													
	<table><tr><th>Share</th><th>Directory</th><th>Share ACL</th><th>Directory ACL</th></tr><tr><td>ADMIN\$</td><td>C:\WINDOWS</td><td>Admin Share</td><td>BUILTIN\Administrators - F, CREATOR OWNER - F, NT AUTHORITY\SYSTEM - F</td></tr><tr><td>C\$</td><td>C:\</td><td>Admin Share</td><td>BUILTIN\Administrators - F, CREATOR OWNER - F, NT AUTHORITY\SYSTEM - F</td></tr></table>	Share	Directory	Share ACL	Directory ACL	ADMIN\$	C:\WINDOWS	Admin Share	BUILTIN\Administrators - F, CREATOR OWNER - F, NT AUTHORITY\SYSTEM - F	C\$	C:\	Admin Share	BUILTIN\Administrators - F, CREATOR OWNER - F, NT AUTHORITY\SYSTEM - F	
	Share	Directory	Share ACL	Directory ACL										
ADMIN\$	C:\WINDOWS	Admin Share	BUILTIN\Administrators - F, CREATOR OWNER - F, NT AUTHORITY\SYSTEM - F											
C\$	C:\	Admin Share	BUILTIN\Administrators - F, CREATOR OWNER - F, NT AUTHORITY\SYSTEM - F											
Additional Windows information	Version	Computer is running Windows 2000 or greater.												

Internet Information Services (IIS) Scan Results

Score	Issue	Result
Check not performed	IIS Status	IIS is not running on this computer.

Desktop Application Scan Results

Vulnerabilities

Score	Issue	Result
Check passed	IE Zones	Internet Explorer zones have secure settings for all users.
Check passed	IE Enhanced Security Configuration for Administrators	The use of Internet Explorer is restricted for administrators on this server.
Check passed	IE Enhanced Security Configuration for Non-Administrators	The use of Internet Explorer is restricted for non-administrators on this server.

Test 4.2:

According to Microsoft's ISA Server site, at the time of this writing there are no security updates for the ISA 2004 Server. However, there is a non security related update that fixes a processor count issue that could cause a licensing violation on multiprocessor machines. This update has not been installed.

Test 4.3:

Nessus Scan Report

SUMMARY

- Number of hosts which were alive during the test : 1
- Number of security holes found : 0
- Number of security warnings found : 1
- Number of security notes found : 6

TESTED HOSTS

192.168.xxx.34 (Security warnings found)

DETAILS

+ 192.168.xxx.34 :

- . List of open ports :
 - o www (80/tcp) (Security notes found)
 - o https (443/tcp) (Security warnings found)
- . Information found on port www (80/tcp)
 - A web server is running on this port
- . Warning found on port https (443/tcp)
 - The SSLv2 server offers 4 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack
 - Solution: disable those ciphers and upgrade your client software if necessary
- . Information found on port https (443/tcp)
 - A SSLv2 server answered on this port
- . Information found on port https (443/tcp)
 - A web server is running on this port through SSL
- . Information found on port https (443/tcp)
 - Here is the SSLv2 server certificate:
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 4102471 (0x3e9947)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=ZA, O=Thawte Consulting (Pty) Ltd., CN=Thawte SSL Domain CA
Validity
Not Before: Sep 14 18:57:49 2004 GMT
Not After : Sep 14 18:57:49 2005 GMT
Subject: CN=owa.Organization.com, OU=Domain Validated, OU=Go to <https://www.thawte.com/repository/index.html>, OU=Thawte SSL123 certificate,

```

O=owa.Organization.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:de:c2:1a:c1:cc:09:ba:4d:44:ed:8a:62:fe:61:
        61:0a:51:aa:c1:8b:6b:99:fd:69:60:17:b2:a2:95:
        d9:63:f5:f0:26:86:a2:fb:04:2c:f1:33:4a:34:d6:
        0e:3a:f7:17:5e:c4:40:45:db:94:70:0c:44:ba:20:
        8b:14:71:c9:6a:a5:37:9b:30:0c:d4:34:d4:8c:d2:
        02:c7:d6:f5:11:dc:c9:ea:54:a7:11:5b:82:ca:d0:
        b3:1e:d4:c7:07:81:5f:d1:a9:22:10:4e:e3:8e:a7:
        89:83:fd:14:3a:0b:aa:62:df:7a:d2:3a:a4:43:9a:
        bf:8b:b9:b3:00:8e:b5:97:dd
      Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client
Authentication
  Authority Information Access:
    OCSP - URI:http://ocsp.thawte.com
    CA Issuers -
      URI:http://www.thawte.com/repository/Thawte_SSL_Domain_CA.crt

    X509v3 Basic Constraints: critical
      CA:FALSE
  Signature Algorithm: md5WithRSAEncryption
    59:08:f1:c9:af:37:f5:96:e6:12:5b:e3:9a:b4:7b:19:8f:59:
    59:83:72:f2:6e:f7:68:db:b0:00:d0:0e:2e:7e:02:3d:f3:20:
    8b:20:f6:39:37:7c:75:cc:fa:6e:44:f8:43:15:a1:15:95:55:
    55:a9:5d:cf:02:ae:a0:cb:ca:3c:f7:45:1b:c3:80:56:28:23:
    dc:b3:06:45:4a:ff:65:e3:ca:08:2d:62:8a:b4:9a:c7:02:9d:
    23:b4:c8:9c:9d:70:f9:42:2e:6a:10:91:2a:91:14:ef:0c:3c:
    b4:4f:f8:07:fc:48:77:15:16:6d:de:be:c1:72:f1:51:2e:96:
    93:77
. Information found on port https (443/tcp)
  Here is the list of available SSLv2 ciphers:
  RC4-MD5
  EXP-RC4-MD5
  RC2-CBC-MD5
  EXP-RC2-CBC-MD5
  DES-CBC-MD5
  DES-CBC3-MD5
. Information found on port https (443/tcp)
  This SSLv2 server also accepts SSLv3 connections.
  This SSLv2 server also accepts TLSv1 connections.
-----
This file was generated by the Nessus Security Scanner

```

Audit Item #4 Findings: FAIL

While the Microsoft Baseline Security Analyzer in test 4.1 checks several different items, we primarily are focusing on the security updates. They are not up to date at the time of this audit. Recommendations on mitigating this issue will be in the Audit Recommendations section. There are some other findings within the MBSA scan that I think should be commented on.

- The Automatic Update Service is not configured. MBSA sights this as a failure, but for a server I don't believe it is. There should be a testing procedure in place before a security update gets installed.
- Password expiration is not set for the ISAadmin account, which is the renamed administrator account. This is in violation with our password policy and must be addressed.
- Logon Failure auditing should be enabled.
- There are two shares listed, but that is only because we had to start the Server service, normally this service is disabled.

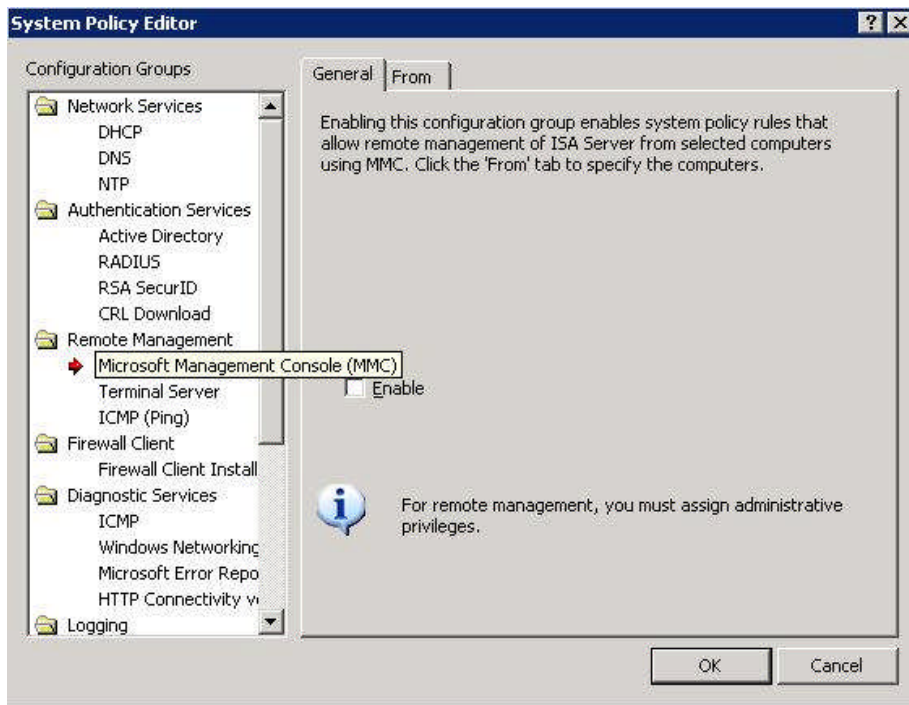
The Nessus scan in test 4.3 shows tells us the only services it could find on this host are running on ports 80 and 443. It does give a warning that two weak ciphers are being offered for clients.

© SANS Institute 2004, Author retains full rights.

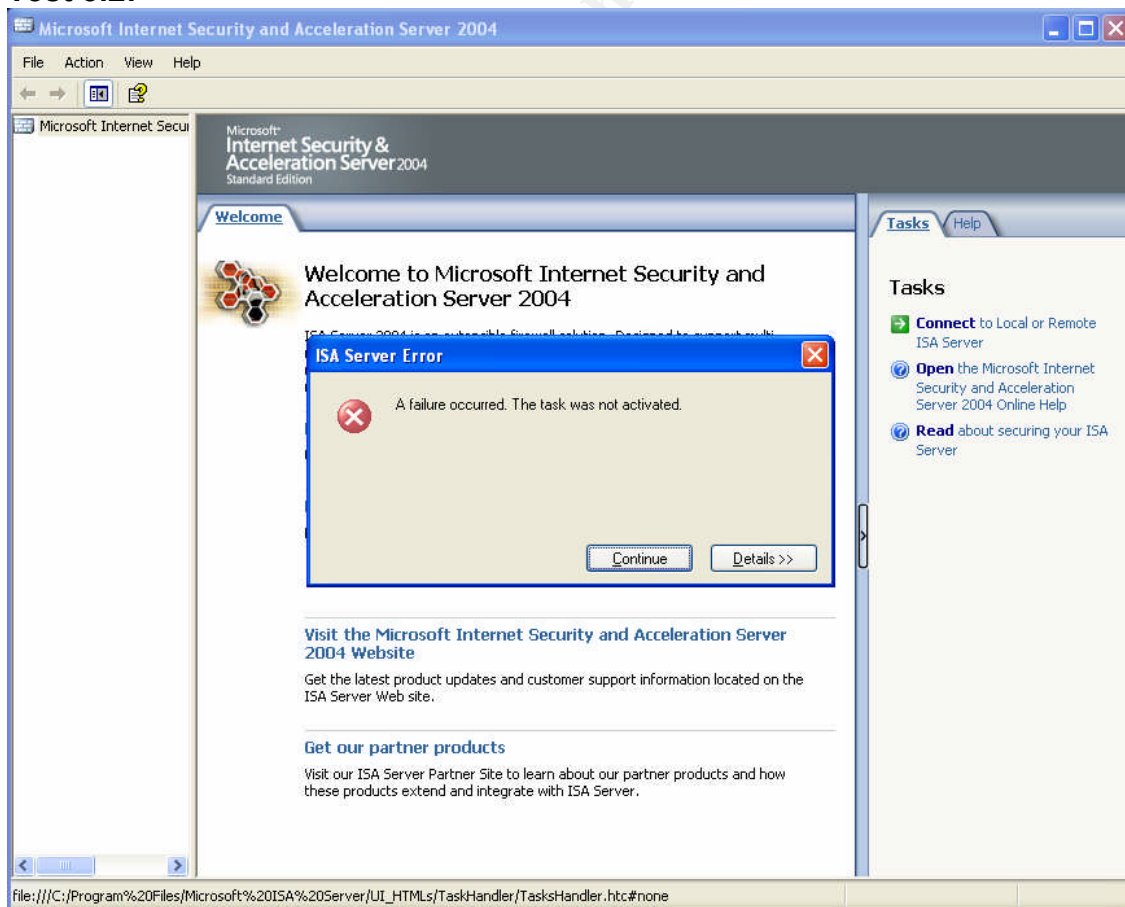
ITEM #	Item Title
5	Disable Microsoft Management Console for remote access.
Reference	
<p>There seems to be a serious lack of evidence supporting whether there is any form of encryption while utilizing the MMC remote administration for the ISA server. For that reason we will not be using this form of remote administration until we look further into this issue. We will stick to Terminal Services for remote administration for its inherent encryption. As of SP2 on Windows 2000 128 bit encryption is mandatory.</p> <p>http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/128bit.asp</p>	
Risk	
<p>Reduce likelihood of eavesdropping on administrative communications by ensuring encryption is in use. Protects passwords and configuration "leakage".</p>	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. Verify that Microsoft Management Console (MMC) access is disabled in the System Policy Editor. . On the ISA server start the ISA Management Console and click on Firewall Policy then on the right side pane click on Tasks. Under System Policy Tasks click on Edit System Policy. Then under the Remote Management folder click on Microsoft Management Console (MMC) and verify that it is disabled. 2. Attempt to connect using the MMC from the DMZ and Internal networks. 	

Audit Item #5 Evidence:

Test 5.1:



Test 5.2:



Audit Item #5 Findings: PASS

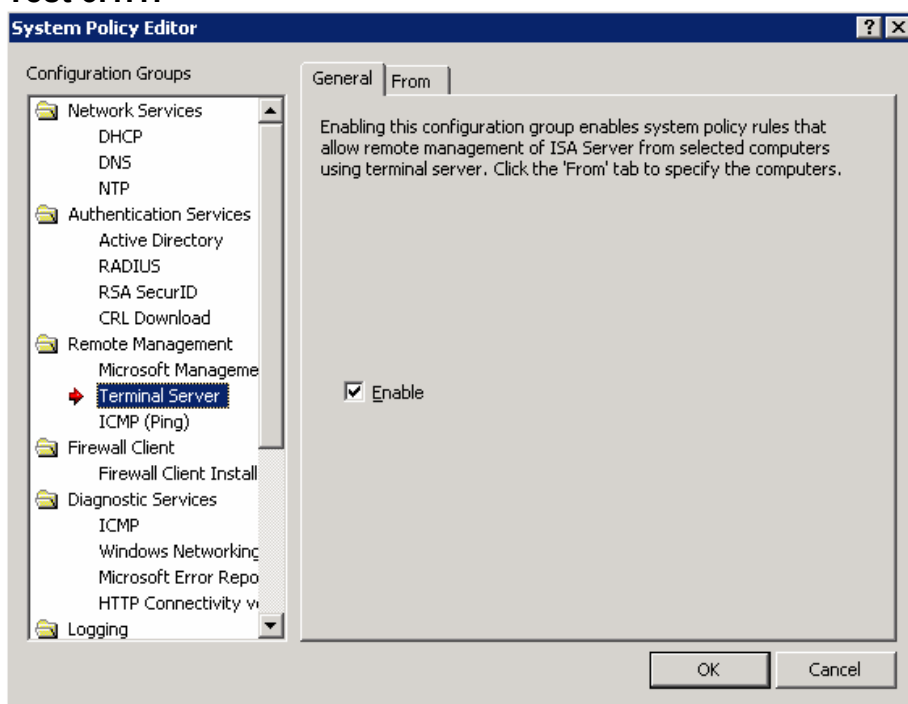
In Test 5.1 you can see that the Microsoft Management Console is disabled. I have the ISA 2004 management console installed on my audit laptop, and failed to connect to the ISA Server from both the DMZ and Internal networks.

© SANS Institute 2004, Author retains full rights.

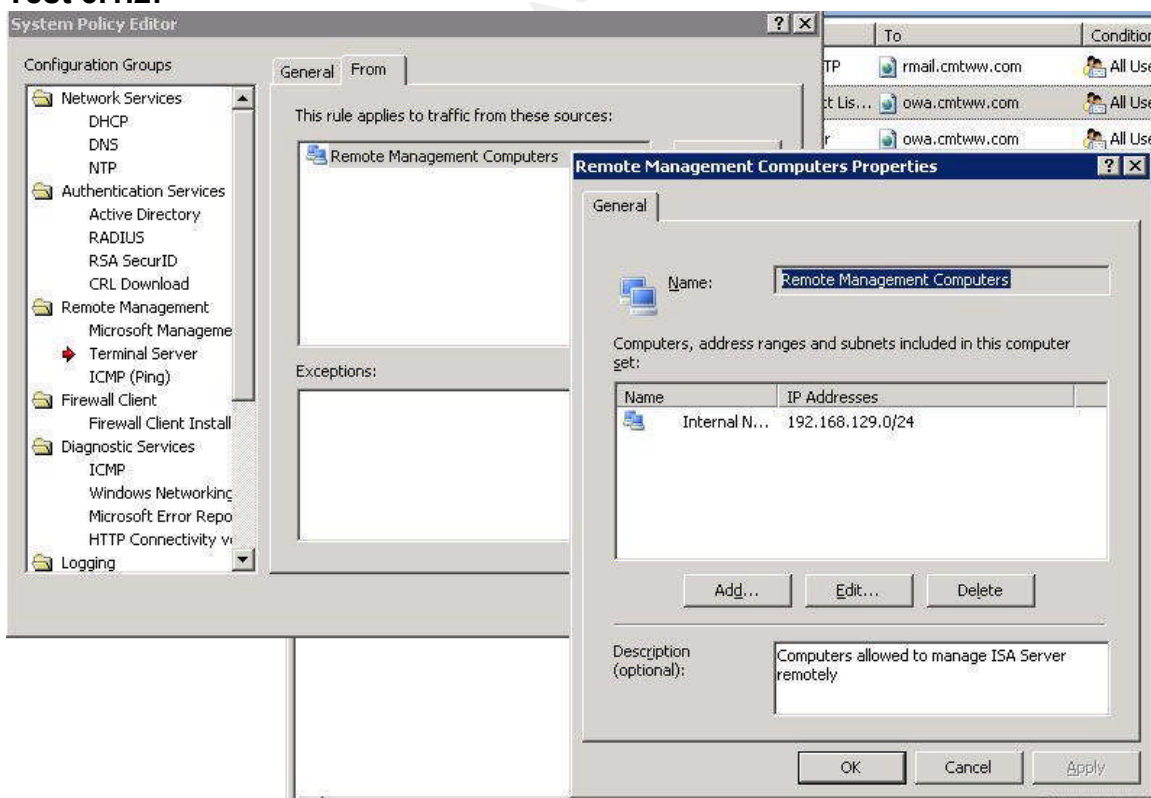
ITEM #	Item Title
6	Restrict remote admin access to internal network using Terminal Services
Reference	
Personal experience is my guidance here. It's common sense to restrict administrative access to a single administrator computer or a restricted group of computers.	
Risk	
Reduce the risk of unauthorized administrative access to the ISA server. The DMZ network is not a suitable environment for allowing administrative access to the ISA server. Because of the nature of the DMZ network being accessed from the Internet the possibility exists that another machine in the DMZ, if compromised, could access this system.	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. Verify settings on the ISA server are set to allow Terminal Services only from administrative Network IP addresses 192.168.xxy.0/24 in our case. On the ISA server start the ISA Management Console and click on Firewall Policy then on the right side pane click on Tasks. Under System Policy Tasks click on Edit System Policy. Then under the Remote Management folder click on Terminal Server and verify that it is enabled. Then under the From tab verify that the Remote Management Computers group is there. Highlight the group and click Edit to verify the IP addresses in this group. 2. Attempt to connect via Terminal Services from the DMZ and Internal networks. Internal should work fine, but connection from the DMZ network should fail. 	

Audit Item #6 Evidence:

Test 6.1.1:



Test 6.1.2:



Test 6.2:



Audit Item #6 Findings: PASS

The two tests show that the administrative access to the ISA Server is restricted to our Internal network where our administrator workstations reside. The first test (6.1.1) shows the ISA Server administrative settings, and (6.1.2) shows the restriction to the internal subnet.

Test 6.2 shows that while my audit laptop was plugged into the DMZ network I could not connect to the ISA server via Terminal Services. I felt it not necessary to include a test for connecting via Terminal Services from the Internal network, as all my ISA configuration verifications were done using this method.

ITEM #	Item Title
7	Verify that only HTTP and HTTPS are available to the OWA IP address from the Internet to the DMZ
Reference	
<p>NIST Special Publication 800-44 entitled "Guidelines on Securing Public Web Servers" tells us in Section 8.2.1 "a firewall that is protecting a Web server should block all access to the Web server from the Internet except for HTTP (TCP port 80) and/or HTTPS (TCP port 443)".</p>	
Risk	
<p>This system only needs HTTP and HTTPS, TCP ports 80 and 443 respectively to be accessible from the Internet into the DMZ (see diagram 1). To allow any other protocols and ports from the Internet into the DMZ network is unnecessary and introduces more risks due to misconfiguration or other system vulnerabilities.</p>	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. Check firewall access-list to verify access from Internet (any) to tcp ports 80 (www) and 443. 2. From a workstation outside of the firewall use Nessus to verify the open ports, which should only be TCP ports 80 and 443 on IP address xxx.xxx.xxx.174. This will also show the difference in a vulnerability scan from Outside the firewall and one done from the DMZ shown in test 4.3 	

Audit Item #7 Evidence:

Test 7.1

This is the access-list that is applied to the Outside interface.

```
access-list acl_mdc_outside_access_1 permit icmp any any echo-reply
access-list acl_mdc_outside_access_1 permit icmp any any time-exceeded
access-list acl_mdc_outside_access_1 permit icmp any any unreachable
access-list acl_mdc_outside_access_1 permit icmp any any parameter-problem
access-list acl_mdc_outside_access_1 permit tcp any host xxx.xxx.xxx.174 eq www
access-list acl_mdc_outside_access_1 permit tcp any host xxx.xxx.xxx.174 eq https
access-list acl_mdc_outside_access_1 permit tcp any host xxx.xxx.xxx.xxx eq www
access-list acl_mdc_outside_access_1 permit tcp any host xxx.xxx.xxx.xxx eq https
access-list acl_mdc_outside_access_1 permit tcp any host xxx.xxx.xxx.xxx eq www
access-list acl_mdc_outside_access_1 permit tcp any host xxx.xxx.xxx.xxx eq https
access-list acl_mdc_outside_access_1 permit udp any host xxx.xxx.xxx.xxx eq 5500
access-list acl_mdc_outside_access_1 permit tcp any host xxx.xxx.xxx.xxx eq https
access-list acl_mdc_outside_access_1 permit udp any host xxx.xxx.xxx.xxx eq radius
access-list acl_mdc_outside_access_1 permit tcp any host xxx.xxx.xxx.xxx eq www
access-list acl_mdc_outside_access_1 permit tcp any host xxx.xxx.xxx.xxx eq tacacs
```

Test 7.2

Nessus Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details

Hosts which were alive and responding during test	1
Number of security holes found	3
Number of security warnings found	2

Host List

Host(s)	Possible Issue
owa.organization.com	Security hole(s) found

[\[return to top \]](#)

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
owa.organization.com	www (80/tcp)	Security warning(s) found
owa. organization.com	https (443/tcp)	Security notes found
owa. organization.com	general/tcp	Security hole found
owa. organization.com	general/udp	Security notes found

Security Issues and Fixes: owa.organization.com		
Type	Port	Issue and Fix
Warning	www (80/tcp)	<p>It seems that it's possible to disclose fragments of source code of your web applications which should otherwise be inaccessible. This is done by appending +.htr to a request for a known .asp (or .asa, .ini, etc) file.</p> <p>Solution : install patches from Microsoft (see MS00-044) Risk factor : Serious CVE : CVE-2000-0457, CVE-2000-0630 BID : 1193, 1488 Nessus ID : 10680</p>
Informational	www (80/tcp)	<p>A web server is running on this port Nessus ID : 10330</p>
Informational	www (80/tcp)	<p>The following directories were discovered: /exchange</p> <p>While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards</p> <p>Nessus ID : 11032</p>
Informational	www (80/tcp)	<p>The remote web server type is : Microsoft-IIS/6.0</p> <p>Solution : You can use urlscan to change reported server for IIS. Nessus ID : 10107</p>
Informational	www (80/tcp)	<p>The remote host appears to be running a version of IIS which allows remote users to determine which authentication schemes are required for confidential webpages.</p> <p>Specifically, the following methods are enabled on the remote webserver: - IIS NTLM authentication is enabled</p> <p>Solution : None at this time Risk Factor : Low CVE : CAN-2002-0419 Nessus ID : 11871</p>
Informational	www (80/tcp)	<p>Here is the nikto report: ----- - Nikto 1.30/1.15 - www.cirt.net + No HTTP(s) ports were found open on the server 'xxx.xxx.xxx.174'.</p> <p>Nessus ID : 10864</p>
Informational	https (443/tcp)	<p>A SSLv2 server answered on this port Nessus ID : 10330</p>
Informational	https (443/tcp)	<p>An unknown service is running on this port through SSL. It is usually reserved for HTTPS</p>

Informational	https (443/tcp)	<p>Nessus ID : 10330</p> <p>Here is the TLSv1 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 4102471 (0x3e9947) Signature Algorithm: md5WithRSAEncryption Issuer: C=ZA, O=Thawte Consulting (Pty) Ltd., CN=Thawte SSL Domain CA Validity Not Before: Sep 14 18:57:49 2004 GMT Not After : Sep 14 18:57:49 2005 GMT Subject: CN=owa.xxxxxxx.com, OU=Domain Validated, OU=Go to https://www.thawte.com/repository/index.html, OU=Thawte SSL123 certificate, O=owa.xxxxxxx.com Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (1024 bit) Modulus (1024 bit): 00:de:c2:1a:c1:cc:09:ba:4d:44:ed:8a:62:fe:61: 61:0a:51:aa:c1:8b:6b:99:fd:69:60:17:b2:a2:95: d9:63:f5:f0:26:86:a2:fb:04:2c:f1:33:4a:34:d6: 0e:3a:f7:17:5e:c4:40:45:db:94:70:0c:44:ba:20: 8b:14:71:c9:6a:a5:37:9b:30:0c:d4:34:d4:8c:d2: 02:c7:d6:f5:11:dc:c9:ea:54:a7:11:5b:82:ca:d0: b3:1e:d4:c7:07:81:5f:d1:a9:22:10:4e:e3:8e:a7: 89:83:fd:14:3a:0b:aa:62:df:7a:d2:3a:a4:43:9a: bf:8b:b9:b3:00:8e:b5:97:dd Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication Authority Information Access: OCSP - URI:http://ocsp.thawte.com CA Issuers - URI:http://www.thawte.com/repository/Thawte_SSL_Domain_CA.crt</p> <p>X509v3 Basic Constraints: critical CA:FALSE Signature Algorithm: md5WithRSAEncryption 59:08:f1:c9:af:37:f5:96:e6:12:5b:e3:9a:b4:7b:19:8f:59: 59:83:72:f2:6e:f7:68:db:b0:00:d0:0e:2e:7e:02:3d:f3:20: 8b:20:f6:39:37:7c:75:cc:fa:6e:44:f8:43:15:a1:15:95:55: 55:a9:5d:cf:02:ae:a0:cb:ca:3c:f7:45:1b:c3:80:56:28:23: dc:b3:06:45:4a:ff:65:e3:ca:08:2d:62:8a:b4:9a:c7:02:9d: 23:b4:c8:9c:9d:70:f9:42:2e:6a:10:91:2a:91:14:ef:0c:3c: b4:4f:f8:07:fc:48:77:15:16:6d:de:be:c1:72:f1:51:2e:96: 93:77</p>
Informational	https (443/tcp)	<p>Nessus ID : 10863</p> <p>This SSLv2 server also accepts TLSv1 connections.</p>
Vulnerability	general/tcp	<p>Nessus ID : 10863</p> <p>Your machine answers to TCP packets that are coming from a multicast address. This is known as the 'spank' denial of service attack.</p> <p>An attacker may use this flaw to shut down this server and saturate your network, thus preventing you from working properly.</p> <p>Solution : contact your operating system vendor for a patch. Filter out multicast addresses (224.0.0.0/4)</p> <p>Risk factor : High</p>

Vulnerability	general/tcp	<p>Nessus ID : 11901</p> <p>Your machine answers to TCP packets that are coming from a multicast address. This is known as the 'spank' denial of service attack.</p> <p>An attacker may use this flaw to shut down this server and saturate your network, thus preventing you from working properly.</p> <p>Solution : contact your operating system vendor for a patch. Filter out multicast addresses (224.0.0.0/4)</p> <p>Risk factor : High Nessus ID : 11901</p>
Vulnerability	general/tcp	<p>Your machine answers to TCP packets that are coming from a multicast address. This is known as the 'spank' denial of service attack.</p> <p>An attacker may use this flaw to shut down this server and saturate your network, thus preventing you from working properly.</p> <p>Solution : contact your operating system vendor for a patch. Filter out multicast addresses (224.0.0.0/4)</p> <p>Risk factor : High Nessus ID : 11901</p>
Warning	general/tcp	<p>The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.</p> <p>An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are:</p> <ol style="list-style-type: none"> 1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network. 2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines. 3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time. <p>Solution : Contact your vendor for a patch Risk factor : Low Nessus ID : 10201</p>
Informational	general/udp	<p>For your information, here is the traceroute to 12.39.241.174 : ***Blanked out*** Nessus ID : 10287</p>

This file was generated by [Nessus](#), the open-sourced security scanner.

Audit Item #7 Findings: PASS

In the firewall access-list you can see that incoming ICMP is disabled, and that the only open ports for our host owa.organization.com on IP address xxx.xxx.xxx.174 are TCP ports 80 and 443, which show up in the access-list as www and https respectively.

In the Nessus scan you will note that only TCP ports 80 and 443 have been found, although the scan did seem to think found some security holes. I think those holes are mostly false alarms, and will be addressed in the Audit Report, but it doesn't change the scoring for this audit test. This audit test was to determine if the firewall properly filters access to the ISA server from the Internet, which it does.

© SANS Institute 2004, Author retains full rights.

ITEM #	Item Title
8	Verify that only HTTP and HTTPS are open for OWA traffic from ISA OWA and OWA Redirect listeners on the DMZ network to the OWA and Redirect Sites on the Internal network.
Reference	
NIST Special Publication 800-44 entitled "Guidelines on Securing Public Web Servers" tells us in Section 8.2.1 "a firewall that is protecting a Web server should block all access to the Web server from the Internet except for HTTP (TCP port 80) and/or HTTPS (TCP port 443)".	
Risk	
Communications should be locked down as to only the necessary addresses, protocols and ports (see diagram 1). To allow any other addresses, protocols and ports from the DMZ into the Internal network is unnecessary and introduces more risks due to misconfiguration or other system vulnerabilities.	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. Using SuperScan from Foundstone.com on the ISA server, verify that the ISA address of 192.168.xxx.34 can only communicate with the Front End server IP of 192.168.xxy.103 on TCP ports 80 and 443 ports. Set the source IP address for 192.168.xxx.34, and scan for TCP and UDP. 2. Verify in the firewall policy that only DMZ IP address 192.168.xxx.34 is only permitted access to Internal address 192.168.xxy.103 on TCP ports 80 (HTTP) and 443 (HTTPS). 	

Audit Item #8 Evidence:

Test 8.1:

SuperScan Report - 10/18/04 21:23:56

IP 192.168.xxy.103	
TCP Ports (2)	
80	World Wide Web HTTP
443	HTTP protocol over TLS/SSL
TCP Port	Banner
80 World Wide Web HTTP	HTTP/1.1 400 Bad Request Content-Type: text/html Date: Tue, 19 Oct 2004 14:09:55 GMT Connection: close -----: --
443 HTTP protocol over TLS/SSL	HTTP/1.1 302 Redirect Content-Length: 156 Content-Type: text/html Location: https://192.168.xxy.103/exchange/ Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET Date: Tue, 19 Oct 2004 14:09:55 GMT Connection: close

IP 192.168.xxy.104	
TCP Ports (2)	
80	World Wide Web HTTP
443	HTTP protocol over TLS/SSL
TCP Port	Banner
80 World Wide Web HTTP	HTTP/1.1 400 Bad Request Content-Type: text/html Date: Tue, 19 Oct 2004 14:09:55 GMT Connection: close -----: --
443 HTTP protocol over TLS/SSL	HTTP/1.1 401 Unauthorized Content-Length: 1656 Content-Type: text/html Server: Microsoft-IIS/6.0 WWW-Authenticate: Basic realm="192.168.xxy.104" X-Powered-By: ASP.NET Date: Tue, 19 Oct 2004 14:09:55 GMT Connection: close

IP 192.168.xxy.105	
TCP Ports (2)	
80	World Wide Web HTTP
443	HTTP protocol over TLS/SSL
TCP Port	Banner
80 World Wide Web HTTP	HTTP/1.1 302 Redirect -----: --- Content-Type: text/html Location: http://./Microsoft-Server-ActiveSync/ Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET Date: Tue, 19 Oct 2004 14:09:55 GMT Connection: close
443 HTTP protocol over TLS/SSL	HTTP/1.1 302 Redirect Content-Length: 175 Content-Type: text/html Location: https://192.168.xxy.105/Microsoft-Server-ActiveSync/ Server: Microsoft-IIS/6.0

X-Powered-By: ASP.NET
Date: Tue, 19 Oct 2004 14:09:55 GMT
Connection: close

Total hosts discovered	3
Total open TCP ports	6
Total open UDP ports	0

Test 8.2:

The following lines from the access-list are highlighted to show the limited access of the Listeners on 192.168.xxx.34 in the DMZ to the OWA site on 192.168.xxy.103 in the Internal network.

```
access-list acl_mdc_DMZ-slot:2_access_1 permit icmp 192.168.xxx.32 255.255.255.224 any echo-reply
access-list acl_mdc_DMZ-slot:2_access_1 permit icmp 192.168.xxx.32 255.255.255.224 any unreachable
access-list acl_mdc_DMZ-slot:2_access_1 permit udp 192.168.xxx.32 255.255.255.224 host 192.168.128.125 eq domain
access-list acl_mdc_DMZ-slot:2_access_1 permit udp 192.168.xxx.32 255.255.255.224 192.168.xxy.100
255.255.255.254 eq domain
access-list acl_mdc_DMZ-slot:2_access_1 permit udp 192.168.xxx.32 255.255.255.224 host 192.168.130.23 eq domain
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.34 host 192.168.xxy.103 eq www
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.34 192.168.xxy.104 255.255.255.254 eq www
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.34 host 192.168.xxy.103 eq https
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.34 192.168.xxy.104 255.255.255.254 eq https
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.35 host 192.168.xxy.103 eq www
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.35 192.168.xxy.104 255.255.255.254 eq www
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.35 host 192.168.xxy.103 eq https
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.35 192.168.xxy.104 255.255.255.254 eq https
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.37 host 192.168.xxy.103 eq www
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.37 192.168.xxy.104 255.255.255.254 eq www
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.37 host 192.168.xxy.103 eq https
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.37 192.168.xxy.104 255.255.255.254 eq https
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.36 host 192.168.xxx.3 eq 5506
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.36 host 192.168.xxx.3 eq 5560
access-list acl_mdc_DMZ-slot:2_access_1 permit udp host 192.168.xxx.36 host 192.168.xxx.3 eq 5500
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.36 host 192.168.xxx.3 eq 2000
access-list acl_mdc_DMZ-slot:2_access_1 deny ip 192.168.xxx.32 255.255.255.224 10.0.0.0 255.0.0.0
access-list acl_mdc_DMZ-slot:2_access_1 deny ip 192.168.xxx.32 255.255.255.224 172.16.0.0 255.240.0.0
access-list acl_mdc_DMZ-slot:2_access_1 deny ip 192.168.xxx.32 255.255.255.224 192.168.0.0 255.255.0.0
access-list acl_mdc_DMZ-slot:2_access_1 deny ip 192.168.xxx.32 255.255.255.224 152.146.0.0 255.255.0.0
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp 192.168.xxx.32 255.255.255.224 any eq ftp
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp 192.168.xxx.32 255.255.255.224 any eq www
access-list acl_mdc_DMZ-slot:2_access_1 permit icmp 192.168.xxx.32 255.255.255.224 any
access-list acl_mdc_DMZ-slot:2_access_1 permit udp 192.168.xxx.32 255.255.255.224 any eq ntp
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp 192.168.xxx.32 255.255.255.224 any eq https
```

Audit Item #8 Findings: FAIL

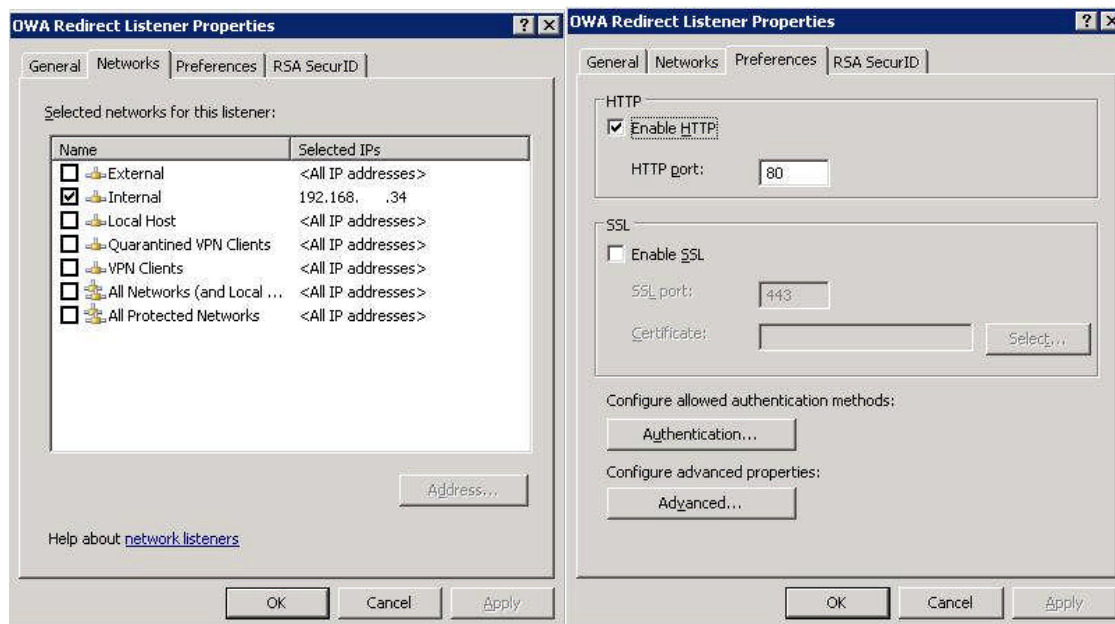
In Test 8.1 I sourced the scan from the IP address 192.168.xxx.34 and did a scan of the whole class C network that the Exchange Front-End server resides on. We can see that the source IP address can see two other IP's that it should not. When you correlate that test with Test 8.2 you can see why.

In test 8.2 you can see highlighted in yellow the two lines in the configuration necessary for this to work. I have highlighted in green two un-necessary openings that should be closed. These two lines allow IP's 192.168.xxy.104 and 104 to be seen by the source IP of the ISA Server.

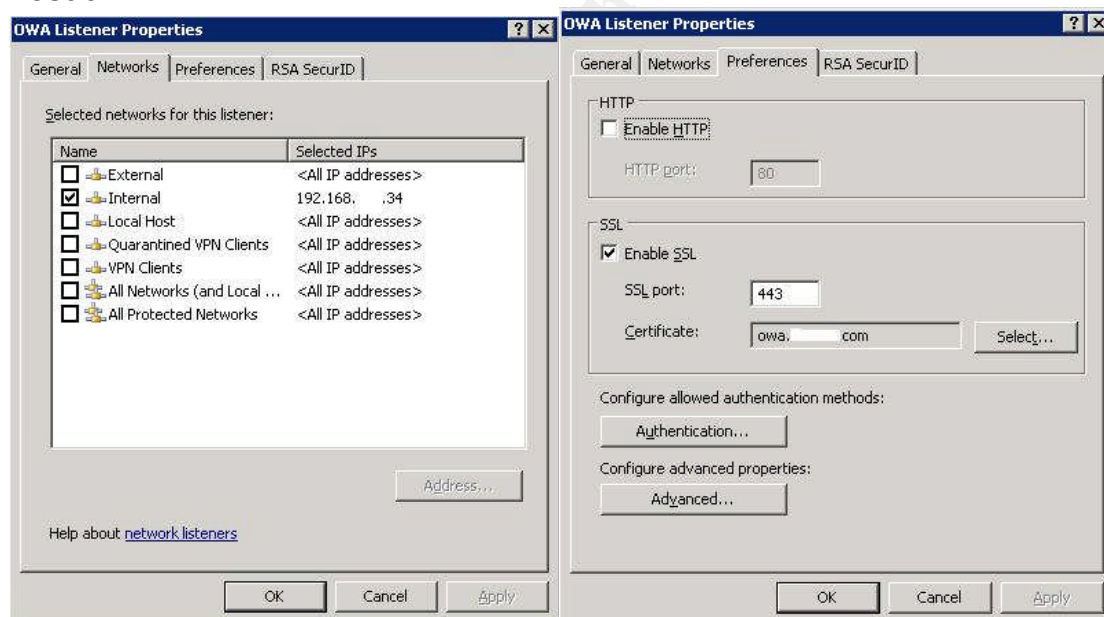
ITEM #	Item Title
9	On ISA server the OWA listener should only be configured for HTTPS access (TCP port 443) on IP address for hostname owa.organization.com.
Reference	
<p>Personal experience and our internal standards document agree on this one. The OWA Redirect should be the only listener to allow HTTP communications. The actual OWA listener should be configured to only allow HTTPS communications to it. Although both of the Listeners answer on the same IP address they a logically separate.</p>	
Risk	
<p>This risk is if for any reason the client were to send logon credentials via HTTP rather than HTTPS, you could expose those credentials for them to be easily picked up on. The forms-based authentication will only work with HTTPS enabled; protecting this authentication process, but it should be checked anyway.</p>	
Objective or Subjective	Objective
Testing Procedure	
<p>Because both the OWA Redirect and the OWA Listeners share the same IP address (192.168.xxx.34) we will have to rely on the following tests to verify this functionality.</p> <ol style="list-style-type: none"> 1. Verify that the OWA Redirect is the only listener using HTTP by inspecting the OWA Redirect listener and make sure that the OWA Redirect is only set to listen on HTTP. Do this In the ISA Server management console. Highlight the Firewall Policy in the left side pane; then over in the right side pane under Toolbox – Web Listeners – OWA Redirect Listener – rightclick and then click on properties. Under the Networks tab it should be set for 192.168.xxx.34 and under the Preferences tab it should only have the HTTP enabled using port 80. 2. Follow the same steps in test 1 to verify that the OWA Listener is set to 192.168.xxx.34 under the Network tab, HTTPS (SSL) port 443 under the Preferences tab. Click on Authentication and verify that OWA Forms-Based is the only one checked. 	

Audit Item #9 Evidence:

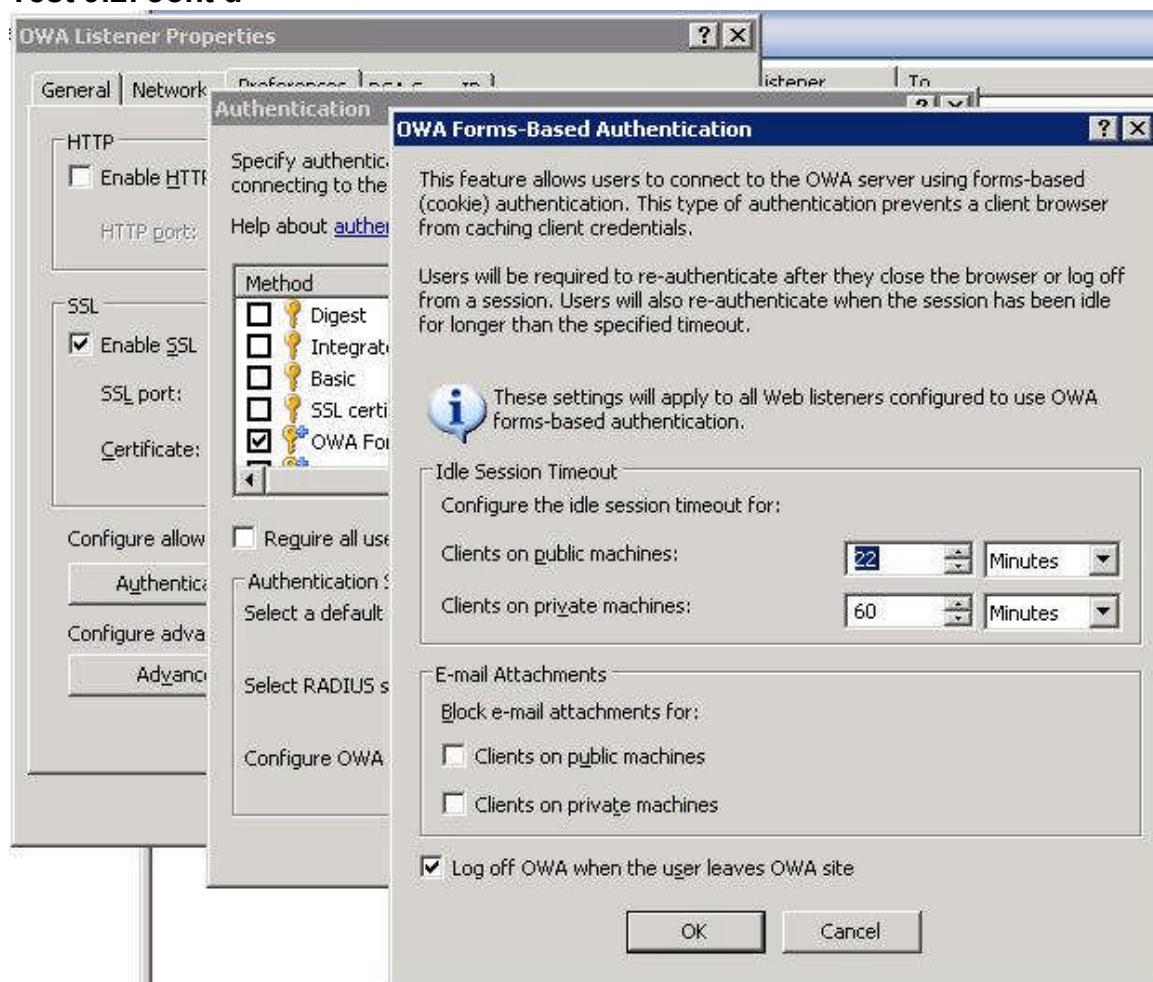
Test 9.1:



Test 9.2:



Test 9.2: cont'd

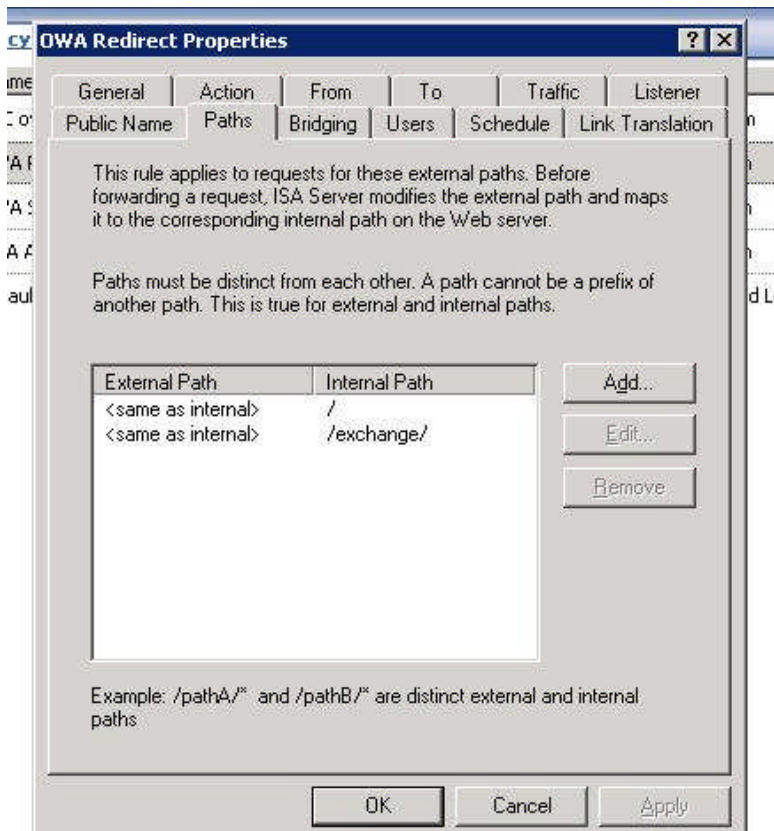


Audit Item #9 Findings:

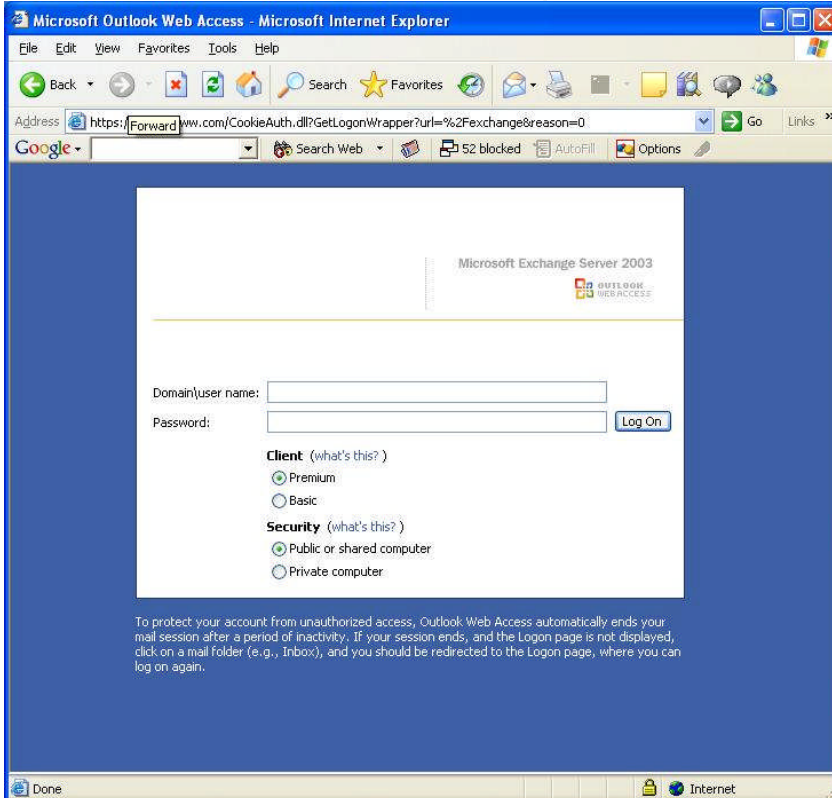
All of the tests show that the Listeners are configured in compliance with the standards document. However, if you note in the E-mail attachments section of this configuration page that there exists the possibility of blocking e-mail attachments on public or private machines. This is another item that is worth looking into. See Audit Report for more details.

ITEM #	Item Title
10	Only allow the two URL's http://owa.organization.com and http://owa.organization.com/exchange to be accepted on the redirect listener. Refuse all others.
Reference	
Personal experience and the Internal configuration document are the source of this audit check.	
Risk	
Because the OWA Redirect listener is set to listen on HTTP port 80, there is the possibility of someone or something trying to exploit the service by sending either a buffer overflow or some other malformed http request. By locking the site down to only allow these two URL's we can mitigate that risk.	
Objective or Subjective	Objective
Testing Procedure	
<ol style="list-style-type: none"> 1. On the ISA server verify that the OWA Redirect Publishing Rule set properly. Under the Firewall Policy view double-click the OWA Redirect Rule. Then click on the Traffic tab. Click on Paths there should only be two paths "/" and "/exchange/". 2. From Browser verify that http://owa.organization.com and http://owa.organization.com/exchange redirect you properly to the Forms-Based Authentication page. 3. By trying different malformed URL's, verify that you get the error message "Error Code: 403 Forbidden. The server denied the specified Uniform Resource Locator (URL). Contact the server administrator. (12202)" If the "Paths" restriction wasn't in place it would pass the "malformed" URL's to the Front End Exchange Server and receive a "page not found" error. 4. By trying the malformed URL's above against the Front-End Server from the Internal network you can see the error message is different than from Test 10.4. The Front-End Server gives 404 errors. <i>In order accomplish this test you have to "trick" your audit workstation into thinking the host owa.organization.com is really the Internal server address of 192.168.xxy.103. You can do this by adding the line "192.168.xxy.103 owa.organization.com" in your "hosts" file. This line may vary in different OS's.</i> 	

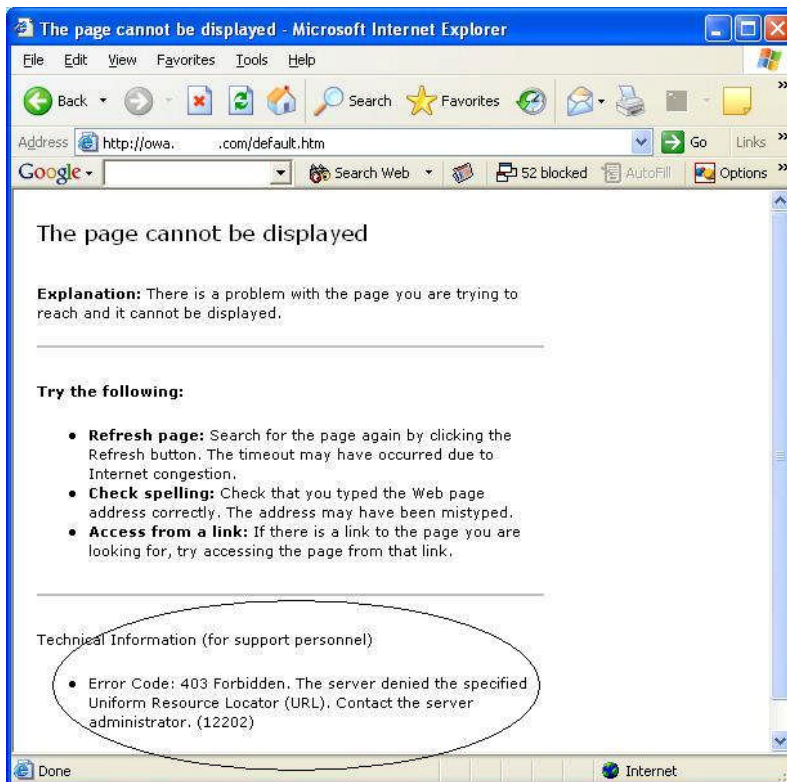
Audit Item #10 Evidence:
Test 10.1:



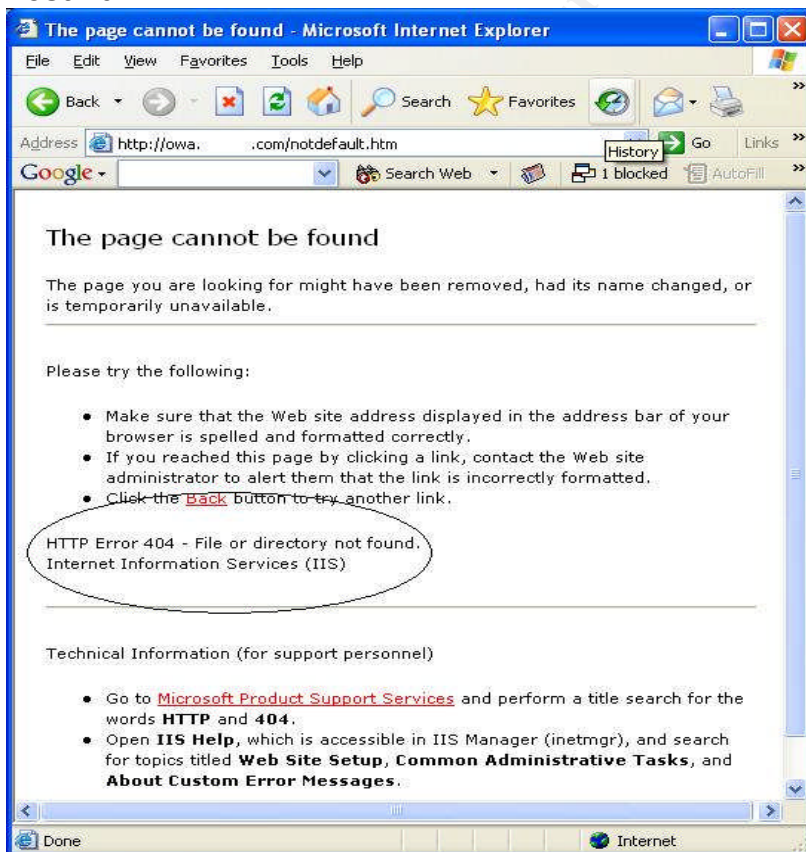
Test 10.2:



Test 10.3:



Test 10.4



Audit Item #10 Findings: PASS

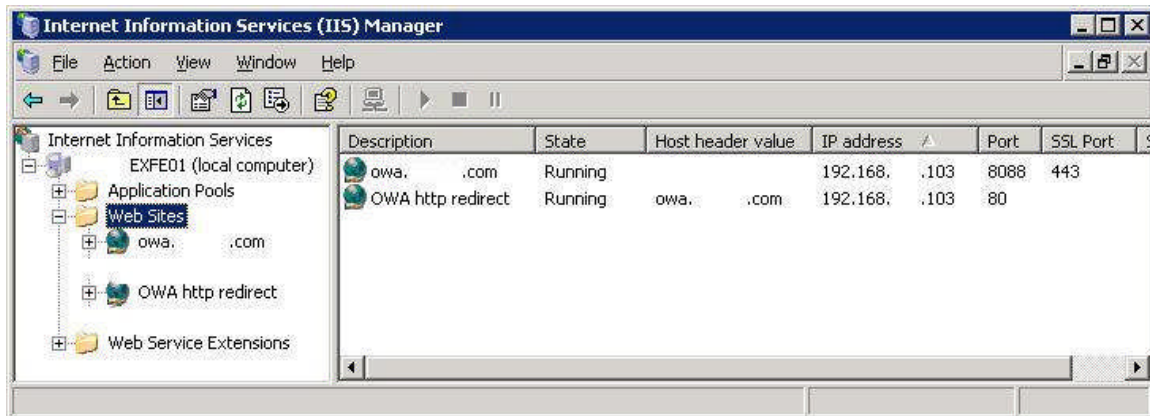
Test 10.1 shows the allowed URL's via the "Paths" parameter within the OWA Redirect Web Publishing Rule. Test 10.2 shows the Forms-Based Logon page after typing in the two valid URL's using HTTP Redirect. Test 10.4 shows that any different forms of the URL's fail with a "403 Forbidden" error. That "403" error is coming from the ISA Server not the Front End Server, this is shown in test 10.4 where you should receive a "404" error.

© SANS Institute 2004, Author retains full rights.

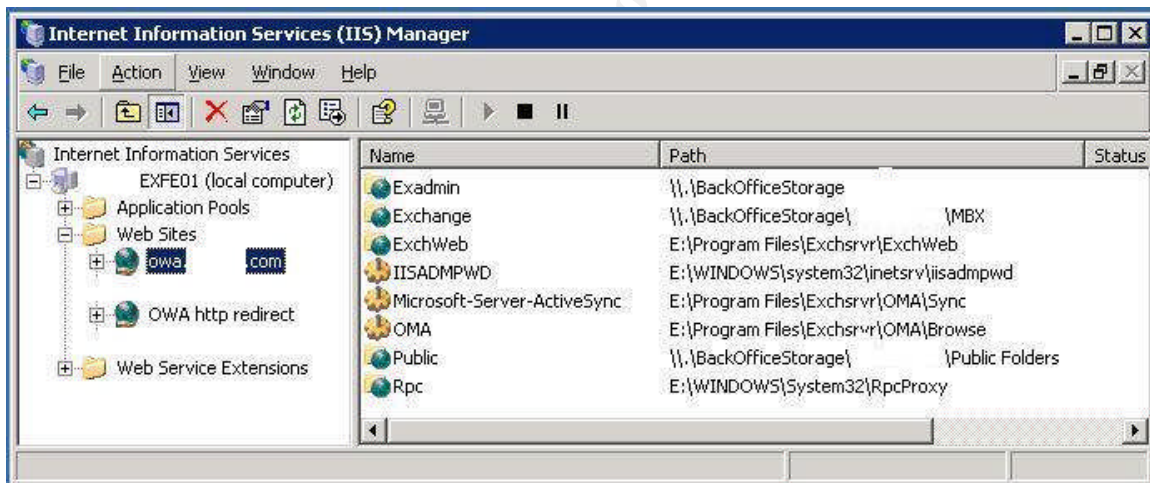
ITEM #	Item Title
11	On Exchange front End Server verify the there are separate Redirect and Exchange Outlook Websites using HTTP and HTTPS respectively. Redirect website should have /default.htm and /exchange/default.htm files only.
Reference	
<p>The sources of this control are personal experience, our Internal Standards document and the article by Thomas Shinder found at this link³, http://www.isaserver.org/tutorials/ISA_Server_Security_Checklist_Part_1_Securing_the_Operating_System_and_the_Interface.html, which states “Do Not Install Applications and Services on the ISA Server”. Even though the ISA Server is proxying all connections to the Front End Exchange Server, we felt that it was necessary to separate the Redirect site and the OWA site within the Front End Server. It was felt to be a security risk to install IIS on the ISA server had to allow this functionality on Front End Exchange Server. The actual redirect script is housed on the Front End Exchange Server in a separate site within IIS listening on HTTP port 80 only. The OWA site is a separate site listening on the same IP address but only on HTTPS port 443.</p>	
Risk	
<p>In order to allow the redirection (a requirement we have to live with) to take place we have to allow unauthenticated web access to the redirect script. To have this script be in the same “site” as the OWA code could expose the OWA site to anonymous connection attempts.</p>	
Objective or Subjective	Objective or Subjective
Testing Procedure	
<ol style="list-style-type: none"> 4. On the Exchange Front End Server verify that there are two separate web “sites” running. Open the Internet Information Services (IIS) Manager and expand the Web Sites folder. There should be an owa.organization.com site and an OWA http redirect site. You can also see in the right pane the address is 192.168.xxy.103 and the TCP port is set to 80 for the OWA http redirect, and that for the owa.organization.com site the SSL port is set to 443. 5. In the IIS Manager highlight the owa.organization.com web site and view the path structure in the right pane. 6. In the IIS Manager highlight the OWA http redirect web site and view the path structure in the right pane. 	

Audit Item # 11 Evidence:

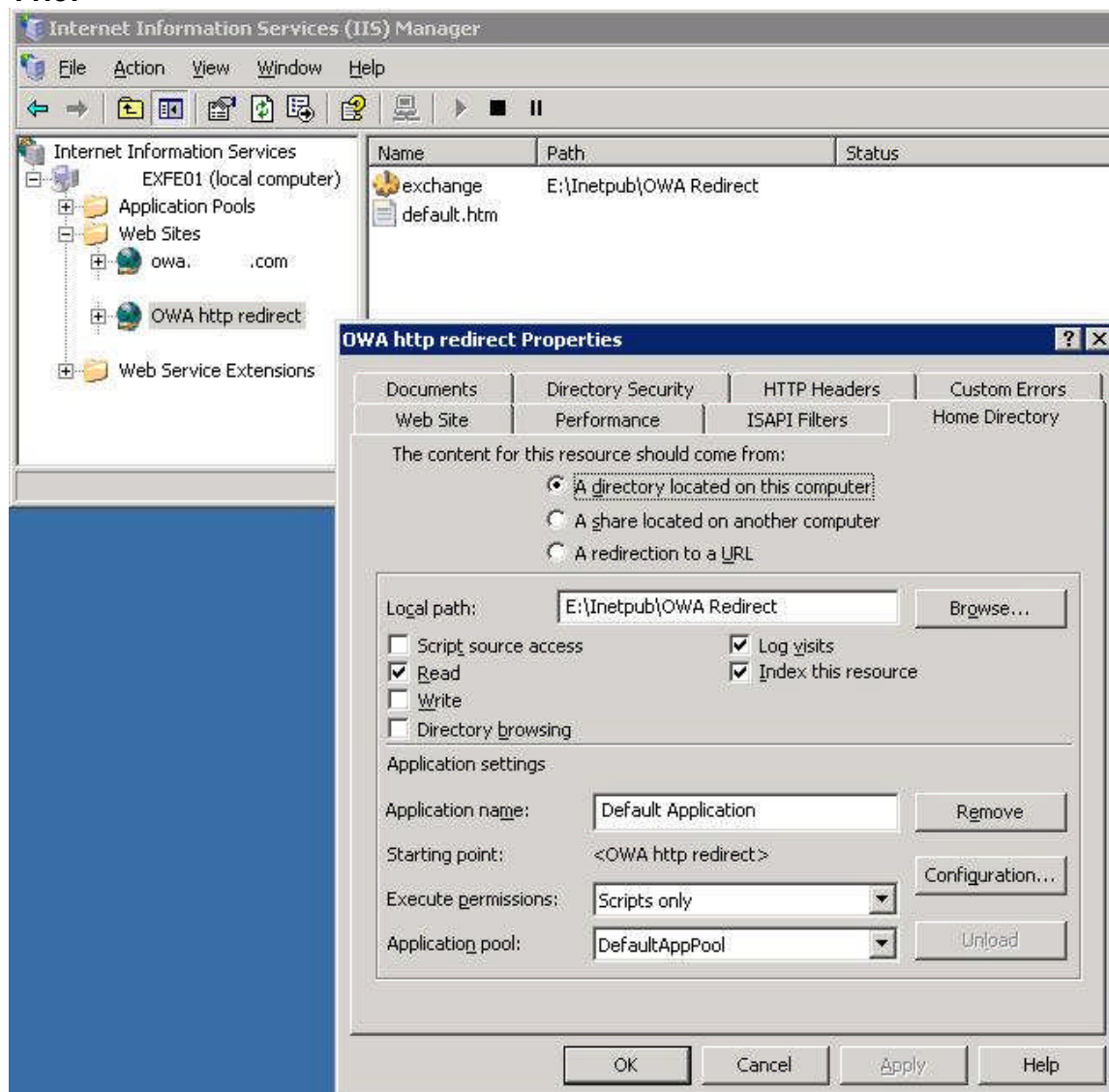
Test 11.1:



Test 11.2:



Test 11.3:



Audit Item # 11 Findings: PASS

The three tests for Audit Item # 11 show everything is in compliance with the internal standards document. However, you should note on test 11.1 that according to the screen capture there is a TCP port 8088 associated with the owa.organization.com web site. This is due to the fact that you cannot leave this field blank. According to the author of the internal standards document it was decided to go with an arbitrary number, rather than leave it at port 80. This TCP port is not allowed through the firewall, as you can see in Audit Item # 8.

4. – Audit Report

4.1 Executive Overview

This audit was commissioned to determine if the ISA 2004 Server used for protecting connections to an Exchange 2003 Front-End Server is configured according to the internally created implementation standard. Opportunities for improving security were also taken into consideration.

Certain assumptions will have to be taken into consideration for this audit. Most importantly is the limitation of the scope to the ISA 2004 Server. While the firewall, Exchange Front-End server and Data Center are touched on for the parts that they play in the implementation of this system, they are not fully audited. Each of these items that are touched on for this audit could be expanded into a full audit, but that might cause us to lose focus on our objective.

There is no policy to consult for this particular device or implementation. All I had to rely on for this audit was an internal implementation standard, personal experience, and research available on a few web sites listed in the references section at the end of this document.

After careful scrutiny of the implementation standard our organization has put together on the ISA 2004 Server for protecting remote access to an Exchange 2003 system, a checklist of 12 items was developed to perform the audit. Most of these audit checks contain multiple tests to execute.

Of these 12 audit checks, 2 of them fail to meet the standard and 3 uncovered some potential issues for the authors of the implementation standard to research. The failures were caused by lack of policy and procedural documentation for the maintenance of the system and not following through and tightening up after testing phase. The implementation standard was well thought out and covered a good portion of the security considerations that should be looked at for an implementation such as this.

© SANS Institute 2004, Author retains full rights.

4.2 Findings

The following table represents the basic findings of the audit.

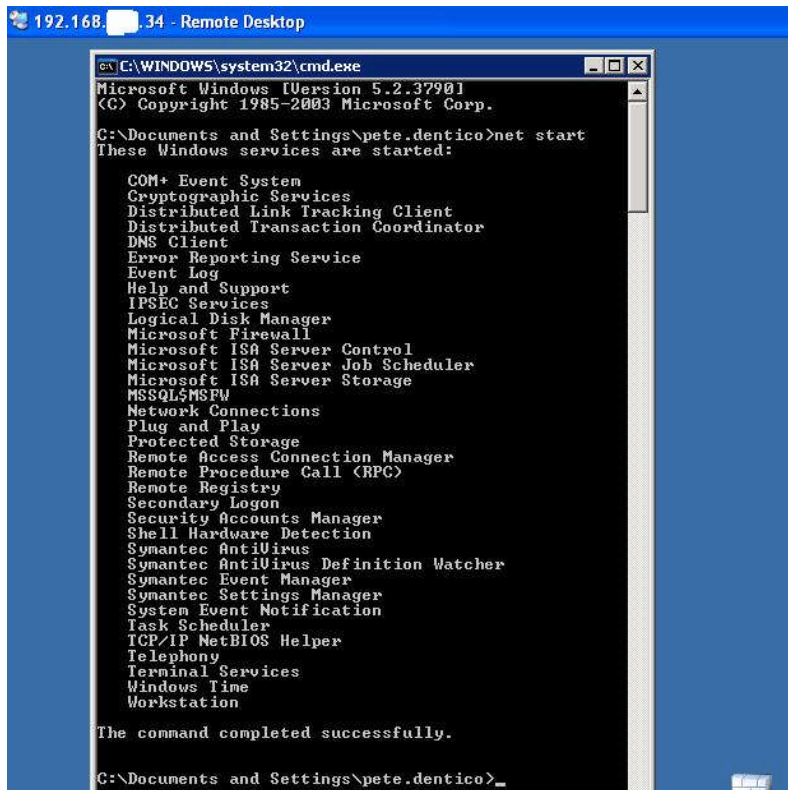
Audit Findings			
Audit Reference	Audit Test	Pass or Fail	Risk Level
1	Proper Placement of ISA server in DMZ	Pass	High
2	Physical Server Security	Pass	High
3	Disabling of un-needed services on the ISA server	Pass*	Medium
4	Make sure patches are up to date on ISA Server and check for other vulnerabilities	Fail	High
5	Disable Microsoft Management Console for remote access.	Pass	Medium
6	Restrict remote admin access to internal network using Terminal Services	Pass	High
7	Verify that only HTTP and HTTPS are available to the OWA IP address from the Internet to the DMZ	Pass*	High
8	Verify that only HTTP and HTTPS are open for OWA traffic from ISA OWA and OWA Redirect listeners on the DMZ network to the OWA and Redirect Sites on the Internal network.	Fail	High
9	On ISA server the OWA listener should only be configured for HTTPS access (TCP port 443) on IP address for hostname owa.organization.com.	Pass*	High
10	Only allow the two URL's http://owa.organization.com and http://owa.organization.com/exchange to be accepted on the redirect listener. Refuse all others.	Pass	Medium
11	On Exchange front End Server verify the there are separate Redirect and Exchange Outlook Websites using HTTP and HTTPS respectively. Redirect website should have /default.htm and /exchange/default.htm files only.	Pass	High
12	Within Forms-Based authentication set timeout to 22 minutes on "public" browser and 60 minutes for "private".	Pass	High

**Even though the audit point was passed there is some further consideration on these points.*

The review of the audit points will be taken in numerical order, not in order of importance. There are a few points denoted by asterisks that while testing, uncovered concerns worth looking into further.

Audit Item # 3: PASS*

This audit point showed the services that were disabled at the time of the audit. They match the internal standards document, therefore passing the audit point. I would like to point out that there might be some room for reducing the existing number of services. As you can see in the below screen-shot there are still quite a few services running.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790.1]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\pete.dentico>net start
These Windows services are started:

COM+ Event System
Cryptographic Services
Distributed Link Tracking Client
Distributed Transaction Coordinator
DNS Client
Error Reporting Service
Event Log
Help and Support
IPSEC Services
Logical Disk Manager
Microsoft Firewall
Microsoft ISA Server Control
Microsoft ISA Server Job Scheduler
Microsoft ISA Server Storage
MSSQL$MSFW
Network Connections
Plug and Play
Protected Storage
Remote Access Connection Manager
Remote Procedure Call (RPC)
Remote Registry
Secondary Logon
Security Accounts Manager
Shell Hardware Detection
Symantec AntiVirus
Symantec AntiVirus Definition Watcher
Symantec Event Manager
Symantec Settings Manager
System Event Notification
Task Scheduler
TCP/IP NetBIOS Helper
Telephony
Terminal Services
Windows Time
Workstation

The command completed successfully.

C:\Documents and Settings\pete.dentico>
```

Recommendation:

Further review by the authors of the implementation document might still find a few more services that could be disabled, possibly the “Plug and Play”, “Help and Support”, “Remote Registry” and a few others. This should be reviewed on a test machine and may help to reduce the possibility of vulnerabilities that can be leveraged against the system.

Costs: Labor for testing

Audit Item # 4: FAIL

This audit point was checked to establish if security updates are regularly being performed on the system. As you can see in the following excerpt from the MBSA scan the system has not been updated to the latest patches.

Score	Issue	Result		
Check Windows failed Security Updates (critical)		6 critical security updates are missing. 3 security updates could not be confirmed.		
		Security Update	Description	Reason
		MS04-030	Vulnerability in WebDav XML Message Handler Could Lead to a Denial of Service (824151)	File version is less than expected. [C:\WINDOWS\system32\msxml3.dll, 8.40.9419.0 < 8.50.2162.0]
		MS04-031	Vulnerability in NetDDE Could Allow Remote Code Execution (841533)	File version is less than expected. [C:\WINDOWS\system32\nddenb32.dll, 5.2.3790.0 < 5.2.3790.173]
		MS04-032	Security Update for Microsoft Windows (840987)	File version is less than expected. [C:\WINDOWS\system32\ntkrnlpa.exe, 5.2.3790.0 < 5.2.3790.175]
		MS04-034	Vulnerability in Compressed (zipped) Folders Could Allow Code Execution (873376)	File version is less than expected. [C:\WINDOWS\system32\zipfldr.dll, 6.0.3790.0 < 6.0.3790.198]
		MS04-037	Vulnerability in Windows Shell Could Allow Remote Code Execution (841356)	File version is less than expected. [C:\WINDOWS\system32\shell32.dll, 6.0.3790.168 < 6.0.3790.205]
		MS04-038	Cumulative Security Update for Internet Explorer (834707)	File version is less than expected. [C:\WINDOWS\system32\browseui.dll, 6.0.3790.186 < 6.0.3790.212]
		MS03-030	Unchecked Buffer in DirectX Could Enable System Compromise (819696)	Please refer to 306460 for a detailed explanation.

	MS04-016	Vulnerability in DirectPlay Could Allow Denial of Service (839643)	Please refer to 306460 for a detailed explanation.
	MS04-028	Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)	Please refer to 306460 for a detailed explanation.

Not all of these security updates would actually affect this system due to the disabling of services shown in Audit point 3, and the restriction of running applications on the ISA server as described in the reference for Audit point 11. This does not excuse the absence of proper security update scheduling, but it does show a Defense-In-Depth⁹ approach to security by not relying on just patching alone to protect from vulnerabilities.

Also the Nessus vulnerability scan reported one security warning as shown below. This is not considered a high security risk, but should be addressed.

- . Warning found on port https (443/tcp)
 - The SSLv2 server offers 4 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack
 - Solution: disable those ciphers and upgrade your client software if necessary
- . Information found on port https (443/tcp)
 - Here is the list of available SSLv2 ciphers:
 - RC4-MD5
 - EXP-RC4-MD5
 - RC2-CBC-MD5
 - EXP-RC2-CBC-MD5
 - DES-CBC-MD5
 - DES-CBC3-MD5

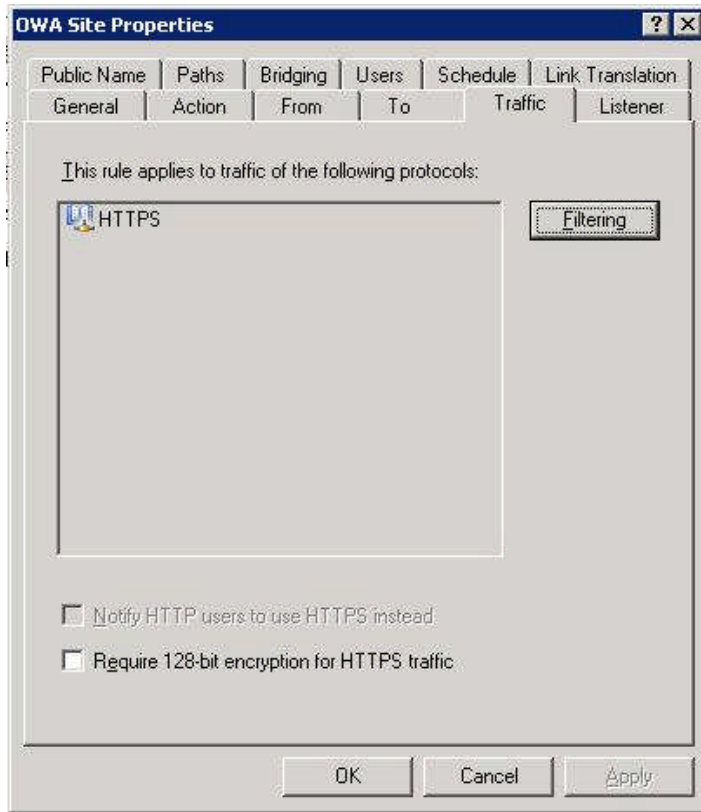
Recommendations:

There is no procedural documentation for the maintenance and monitoring of this system. Through discussion with the authors I have determined that they are in the process of evaluating an automated security patch management system. While this only addresses the security updates, there needs to be further investment into an ongoing plan for system maintenance.

Costs: Labor to draft plan

Further, for the SSL weak cipher it needs to be determined where this is to be enforced. Currently SSL is enabled on both the ISA and Front-End servers, but

neither are enforcing strong ciphers (128 bit encryption). On the ISA server you can enable it by double clicking the **OWA Site** publishing rule in the ISA Server management console and clicking on the **Traffic** tab. There you can see the checkbox to force 128 bit SSL encryption (shown below).



Costs: Labor time to test

Audit Item # 7: PASS*

This item passed the criteria it was supposed to check, but in doing so the Nessus scan showed that there were some security concerns. See excerpt of Nessus scan results below:

Warning www
(80/tcp) It seems that it's possible to disclose fragments of source code of your web applications which should otherwise be inaccessible. This is done by appending +.httr to a request for a known .asp (or .asa, .ini, etc) file.

Solution : install patches from Microsoft (see MS00-044)
Risk factor : Serious
CVE : [CVE-2000-0457](#), [CVE-2000-0630](#)
BID : [1193](#), [1488](#)
Nessus ID : [10680](#)

Vulnerability general/tcp

Your machine answers to TCP packets that are coming from a multicast address. This is known as the 'spank' denial of service attack.

An attacker may use this flaw to shut down this server and saturate your network, thus preventing you from working properly.

Solution : contact your operating system vendor for a patch.
Filter out multicast addresses (224.0.0.0/4)

Risk factor : High

Nessus ID : [11901](#)

Warning general/tcp

The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are:

1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network.
2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines.
3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time.

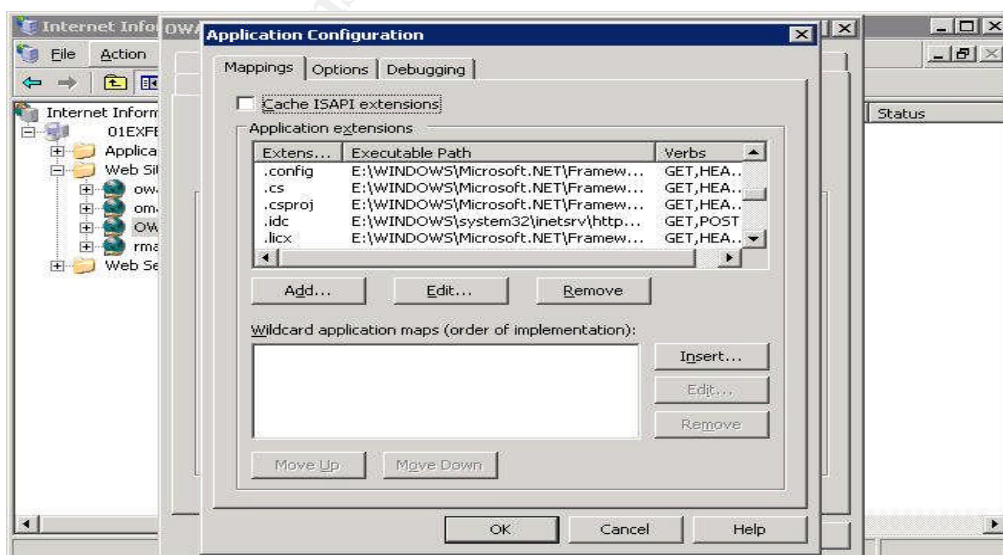
Solution : Contact your vendor for a patch

Risk factor : Low

Nessus ID : [10201](#)

I believe after checking these that they are all false alarms. The first is dated in 2000 and only applies to IIS version 4 & 5. This solution is using IIS 6 on the Front-End Server. Further, the Nessus plugin note¹⁰ for this test goes on to say, *"Solution : .htr script mappings should be removed if not required."*

In this screen-shot from the Front-End server you can see that while sorted by extension there is no .htr listed.



The next result comes from the Nessus scan and states *"Your machine answers to TCP packets that are coming from a multicast address. This is known as the 'spank' denial of service attack."* I believe this to be a false alarm as well. According to the following excerpt from the Cisco configuration example¹¹ entitled *"Tunneling IP Multicast Packets Through a PIX Firewall"*

Background Theory

As explained in the [PIX documentation](#), the PIX Firewall does not pass multicast packets, even though many routing protocols use multicast packets to transmit their data. Cisco considers it inherently dangerous to send routing protocols across the PIX Firewall.

As for the last warning in the scan report that states *"The remote host uses non-random IP IDs"*. This is a relatively low priority concern and I propose no recommendations.

Audit Item # 8: FAIL

This audit item checked failed for the proper filtering of traffic from the DMZ to the Internal network as it applies to this system. All that is necessary is for IP address 192.168.xxx.34 in the DMZ to have TCP ports 80 and 443 permitted to the Internal address of 192.168.xxy.103. As you can see in the firewall config there are two lines highlighted in yellow, which allow this to happen properly. What should be noted is that the two lines highlighted in green allow the IP address of 192.168.xxx.34 to communicate to two other IP addresses (192.168.xxy.104&105) on TCP ports 80(www) and 443(https).

```
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.34 host 192.168.xxy.103 eq www
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.34 192.168.xxy.104 255.255.255.254 eq www
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.34 host 192.168.xxy.103 eq https
access-list acl_mdc_DMZ-slot:2_access_1 permit tcp host 192.168.xxx.34 192.168.xxy.104 255.255.255.254 eq https
```

After discussing this result with the author of the configuration document and the firewall administrator, it was determined that the openings were there for testing, but never removed.

Recommendations:

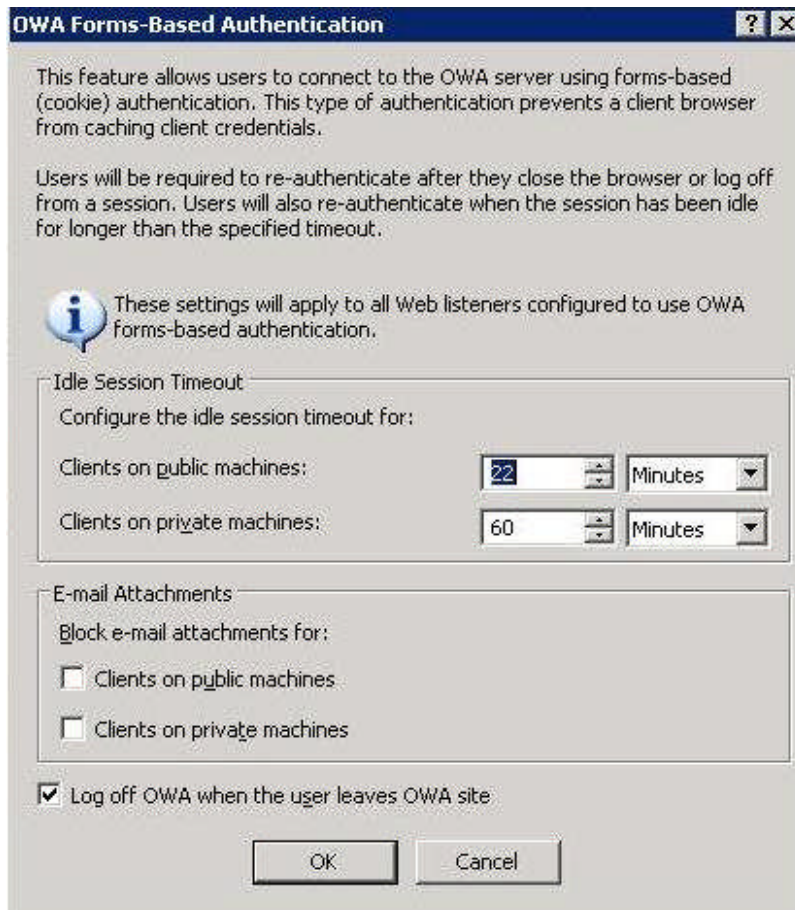
In order for this sort of situation to not happen again, it is my recommendation that the firewall administrator should take note of any openings in the firewall for the purposes of "testing" and periodically review the firewall configurations. They should harass the "testers" frequently in order to close these holes as soon as the testing is done. (Although I suggest harassing in a nice way;)

Costs: None

Audit Item # 9: PASS*

This item passed for compliance to the Configuration document. OWA Forms-Based authentication gives us the option to choose the type of machine we are connecting from in the logon screen, either "Public" or "Private". That allows us to have a separate timeout for either choice. We have implemented a timeout of 22 minutes for "Public" workstations and 60 minutes for "Private".

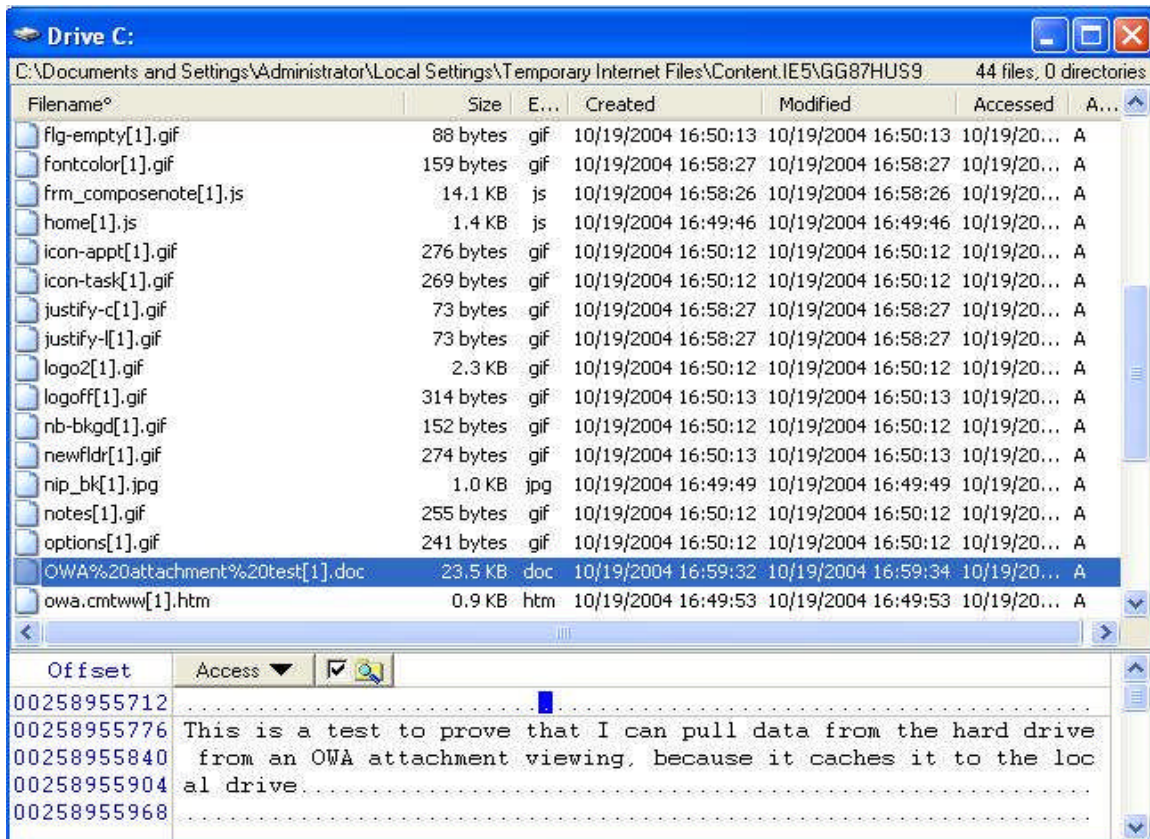
Another feature of the Forms-Based authentication is the ability to disable e-mail attachments for either "Public" or "Private" workstations. This is shown below.



The screenshot shows a Windows-style dialog box titled "OWA Forms-Based Authentication". It contains the following elements:

- Header:** Title bar with "OWA Forms-Based Authentication" and standard window controls.
- Text:** "This feature allows users to connect to the OWA server using forms-based (cookie) authentication. This type of authentication prevents a client browser from caching client credentials." and "Users will be required to re-authenticate after they close the browser or log off from a session. Users will also re-authenticate when the session has been idle for longer than the specified timeout."
- Information Icon:** A blue 'i' icon with the text: "These settings will apply to all Web listeners configured to use OWA forms-based authentication."
- Idle Session Timeout:** A section with the label "Configure the idle session timeout for:" containing two rows:
 - "Clients on public machines:" with a numeric spinner set to "22" and a "Minutes" dropdown.
 - "Clients on private machines:" with a numeric spinner set to "60" and a "Minutes" dropdown.
- E-mail Attachments:** A section with the label "Block e-mail attachments for:" containing two unchecked checkboxes:
 - ☐ Clients on public machines
 - ☐ Clients on private machines
- Log off OWA:** A checked checkbox labeled "Log off OWA when the user leaves OWA site".
- Buttons:** "OK" and "Cancel" buttons at the bottom.

In the current configuration document they are both unchecked. I would caution that allowing the ability to view or save e-mail attachments is quite risky when using "Public" workstations, or any workstations outside of your control. When you open an attachment in Outlook Web Access, the attachment is cached locally to view. This cached file is left behind for anyone with access to the system to see. I ran a few experiments and found it quite easy to view the files. In one case when going in the Temporary Internet Files folder to view the attachment it caused the opening of the browser to logon to the OWA server. It was quite easy to bypass with the WinHex tool, by opening up the local drive and viewing the file as shown below.



Now if this was a confidential document it would be very easy for someone to gain the contents of this file, which could be very dangerous. It also brings up the point of user security awareness training. If the users are aware of the risks involved in viewing attachments on public workstations perhaps they would be less inclined to do so.

Recommendations:

I would highly recommend that the blocking of attachments for "Public" workstations be reviewed and implemented. Also as users are given access to the Outlook Web Access they should receive some training on the perils of viewing e-mail and or e-mail attachments on "public" workstations.

4.3 Conclusion

The use of an ISA 2004 server to protect Outlook Web Access in an Exchange 2003 environment is an elegant solution, provided it's implemented properly. The authors of our internal configuration document were thorough and covered most of the considerations for a secure implementation. Some important security considerations were brought to light by the process of this audit. Most importantly is the consideration of maintaining and monitoring a system once it's put into production. This is one of the shortcomings of a lot of good implementation plans and I can't stress the importance of continued diligence after the initial implementation of any technology or system.

References

¹ Microsoft's "Exchange Server 2003 and Exchange 2000 Server Front-End and Back-End Topology Guide Chapter 6:
<http://www.microsoft.com/technet/prodtechnol/exchange/guides/E2k3FrontBack/75555003-90f3-4dcf-b04f-cda1b80e477c.mspx>

² Microsoft Product Overview:
<http://www.microsoft.com/isaserver/evaluation/overview/default.asp> - See section entitled "Securely and Easily Make E-mail Available to Employees Outside the Network".

³ Proxy Server definition as defined by WordIQ.com:
http://www.wordiq.com/definition/Proxy_server

⁴ NIST Special Publication 800-30 document entitled "Risk Management Guide for Information Technology Systems
<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

⁵ Microsoft's ISA Server home page:
<http://www.microsoft.com/isaserver>

⁶ The ISAServer.org Web Site:
<http://www.isaserver.org>

⁷ The MSeXchange.org Web Site:
<http://www.msexchange.org>

⁸ Shinder, Thomas. "ISA Server Security Checklist - Part 1: Securing the Operating System and the Interface", Feb 05, 2002
http://www.isaserver.org/tutorials/ISA_Server_Security_Checklist_Part_1_Securing_the_Operating_System_and_the_Interface.html

⁹ Defense-in-Depth is described in this article from The Information Warfare Site (no noted author)
<http://www.iwar.org.uk/iwar/resources/belvoir-iw-course/dis.htm>

¹⁰ Nessus Test Microsoft IIS Source Fragment Disclosure:
<http://cgi.nessus.org/plugins/dump.php3?id=10680>

¹¹ Cisco Configuration Example "Tunneling IP Multicast Packets Through a PIX Firewall"
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00800943fe.shtml