Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Best Practices for Auditing a Watchguard Firebox 700 Firewall: An Auditor's Perspective

James Tarala
GSNA Practical Assignment
Version 2.1
March 2003

Table of Contents

Table of Figures

Abstract

In the process of securing an organization there are many things to consider. One of the biggest questions often asked by enterprises is "Where should we start?" As you look at the current state of practice most often auditors and infosec professionals will say to start where the risk is the greatest. For most organizations that is the network's perimeter, where users from New York to Tel Aviv to Sao Paolo can all attack an organization from the comfort of their own homes. Because of this one of the primary jobs of a network auditor, and a job likely to be requested, is an audit of an organization's perimeter systems.

In this paper one particular system has been chosen to serve as a model for protecting the perimeter of one's network, the Watchguard Firebox 700 firewall. This firewall is a common choice for small to medium businesses who are looking for perimeter protection combined with ease of use, ampleness of features, and overall low total cost of ownership. The Watchguard device covers all of these areas, and provides an organization with features such as stateful packet inspection, GUI configuration modules, proxied SMTP and HTTP, and both mobile user and branch office VPN support. The focus of this discussion will be those features that specifically protect the inner workings of the enterprise, without considering the issue of mobile users and offices.

This paper will provide a network perimeter auditor, who is attempting to audit a Watchguard Firebox 700 device, the tools necessary to audit and help secure the organization. First the current state of practice for network perimeter security will be considered. Next the auditor will review specific steps that can be taken to audit and secure this type of device. Accompanying this checklist will be a sample audit of ten of the more common audit steps to show specific examples of how this type of audit is to be performed. Finally a sample audit report, complete with executive summary and audit findings will help instruct the auditor how to communicate specific findings with those ultimately responsible for the system.

Assignment 1 – Audit, Measurement Practice, and Control

1.1 System Identification

The company being audited in this discussion is a television station affiliate for a national broadcasting network. The company provides local television feed for the television network and news services for the local community. They are not involved in the sale or manufacturing of any goods, however are in the business of providing services and information to their customers, specifically in the way of air-time and advertising. An audit of their network perimeter was requested after the company discontinued service with an outsourced networking company which initially installed and configured all of their perimeter devices (routers, firewalls, etc.). The company's management wanted to ensure that the company had not left themselves backdoor access into the network and also wanted to audit the perimeter's level of security after an attacker had defaced their website.

When examining their network environment there were certain features that were noted as being vital to the company's operations. First the organization maintains a static website which is often modified, even hourly, and is crucial to the overall success of the organization. There is very little room for failure of the corporate website, and customers must be able to access its contents often multiple times throughout the day. Users check the website for local news and information throughout the day and the site must be available 24 hours a day. This site is being hosted on an internal Microsoft Windows 2000 Server running Internet Information Services (IIS) 5.0, as described below:

Server Name:	IP Address:	Purpose:	Operating System:	Patch Level:
Web1	10.0.10.10	Website Hosting	Windows 2000	SP2 + Various Hotfixes Installed
Installed Software:	**Patch Level:**	**CPU:**	**Memory**	**Harddrives:**
Internet Information Services 5.0	Various IIS Hotfixes Installed	700 Mhz	512 MB	2 – 18.2 GB (SCSI - SW Mirrored)

Please note that all server names and internet protocol (IP) addresses have been sanitized and all domain names have been modified. Public IPs have been modified on all diagrams to IPs on the 10.0.0.0 network for discussion purposes only, these are not the real IPs in use on the system. However, enough of the configuration can be given in generic tones to highlight the network configuration

as well as the types of technologies being hosted by the organization to give potential auditors a framework for understanding the procedure being discussed.

It is also crucial that the company maintains uninterrupted contact with the Internet as they receive continual software updates for a proprietary database system that they run internally. This database of information is not available to external users, however must be accessible to internal employees at all times of the day, especially those involved in broadcasting the news. This database provides international news feed to the anchors as they prepare their stories for the air. This database system runs on a Microsoft Windows 2000 server that utilizes a simple third-party database system and viewer application. The server's configuration is as follows:

Server Name:	IP Address:	Purpose:	Operating System:	Patch Level:
NewsDB1	10.0.10.4	Database Application Hosting	Windows 2000	SP2 + Various Hotfixes Installed
Installed Software:	Patch Level:	CPU:	Memory	Harddrives:
Third-party Database Application	No patches installed	1400 Mhz	1 GB	3 – 80 GB (SCSI – HW RAID 5)

Due to budgetary constraints the business decided to acquire one full T1 connection to the Internet for data purposes and felt it unnecessary to provide a backup connection to prevent system downtime. The internet service provider (ISP) managing this connection also manages the company's external Cisco 2500 series router. Although the outsourced networking company noted earlier installed the Cisco equipment, they were not given access to the system's configuration (enable or configuration mode) by the ISP. All requests for configuration changes must be submitted to the ISP in order for changes to be made.

As would be expected of most organizations e-mail is also of vital importance to the overall success of the enterprise. There are no specialized processors of the e-mail internally, simply a standard Microsoft Exchange 2000 server which hosts the companies incoming and outgoing e-mail. As is required by Microsoft to install the Exchange product, IIS 5.0 is also installed on the server, which is occasionally used by internal users only to access Outlook Web Access (OWA) when users are not working at their desktop. This server is also one of the domain controllers for the internal Active Directory domain, along with one other internal machine serving in this capacity. One of the IT administrators noted during the course of the audit that this was a temporary configuration and that Active Directory and Exchange would not co-exist on the same machine in the near future. The server's configuration is as follows:

6

Server Name:	IP Address:	Purpose:	Operating System:	Patch Level:
DC1	10.0.10.5	E-mail	Windows 2000	SP2 + Various Hotfixes Installed
Installed Software:	**Patch Level:**	**CPU:**	**Memory**	**Harddrives:**
Exchange Server 2000; Internet Information Services 5.0; Symantec Anti-Virus for Exchange v2.5	MS Exchange SP1; Various IIS Hotfixes Installed; No Symantec patches installed	1400 Mhz	1 GB	2 – 80 GB (SCSI - HW Mirrored)

However, while e-mail provides only standard messaging for the users the
company has had bad experiences with viruses in the past and it was decided by
management that performance was not as important as security. Therefore all
incoming e-mails should be filtered as they enter the building to ensure that
unsafe attachments do not accidentally compromise internal systems. Therefore
virus filtering for unsafe e-mail attachments was also configured on the server
using Symantec Anti-Virus for Exchange v2.5.

The following is a sanitized diagram of the network being discussed. As can be
noted, a Watchguard Firebox 700 device was chosen to protect the
organization's perimeter. This firewall device is utilizing the default system
hardware as provided by the manufacturer, and is non-upgradeable. The
Watchguard's software firmware version is 6.0 – B1140. The network consists of
only one subnet, and around 200 hosts. Although the organization is on the edge
of requiring another or larger subnet, due to budgetary concerns the organization
decided to stay with one standard class C subnet (24 bit – 255.255.255.0).
Although there are many specialized databases and proprietary applications
running within the organization, only those with exposure to the Internet are
noted for the sake of this discussion.

It should be noted that the firewall device in this environment utilized all three of
the interfaces available on the system, external, DMZ, and trusted. The external
interface (10.0.100.1) connects to the perimeter Cisco 2500 series router that
utilizes a private subnet used only by these two devices (10.0.100.0/24). The
DMZ interface (10.0.10.1) connects to a 16 port 3-com switch that provides layer-
two connectivity to this subnet (10.0.10.0/24). The only other device on this
subnet is the Window 2000 Server hosting the company's website (Web1 –
10.0.10.10). The third, trusted interface (192.168.1.254) connects the firewall to

7

the internal network via another 16 port 3-com switch. All other servers, including DC1 and NewsDB1, the firewall's management workstation (192.168.1.6), and all user workstations reside on this subnet (192.168.1.0/24).
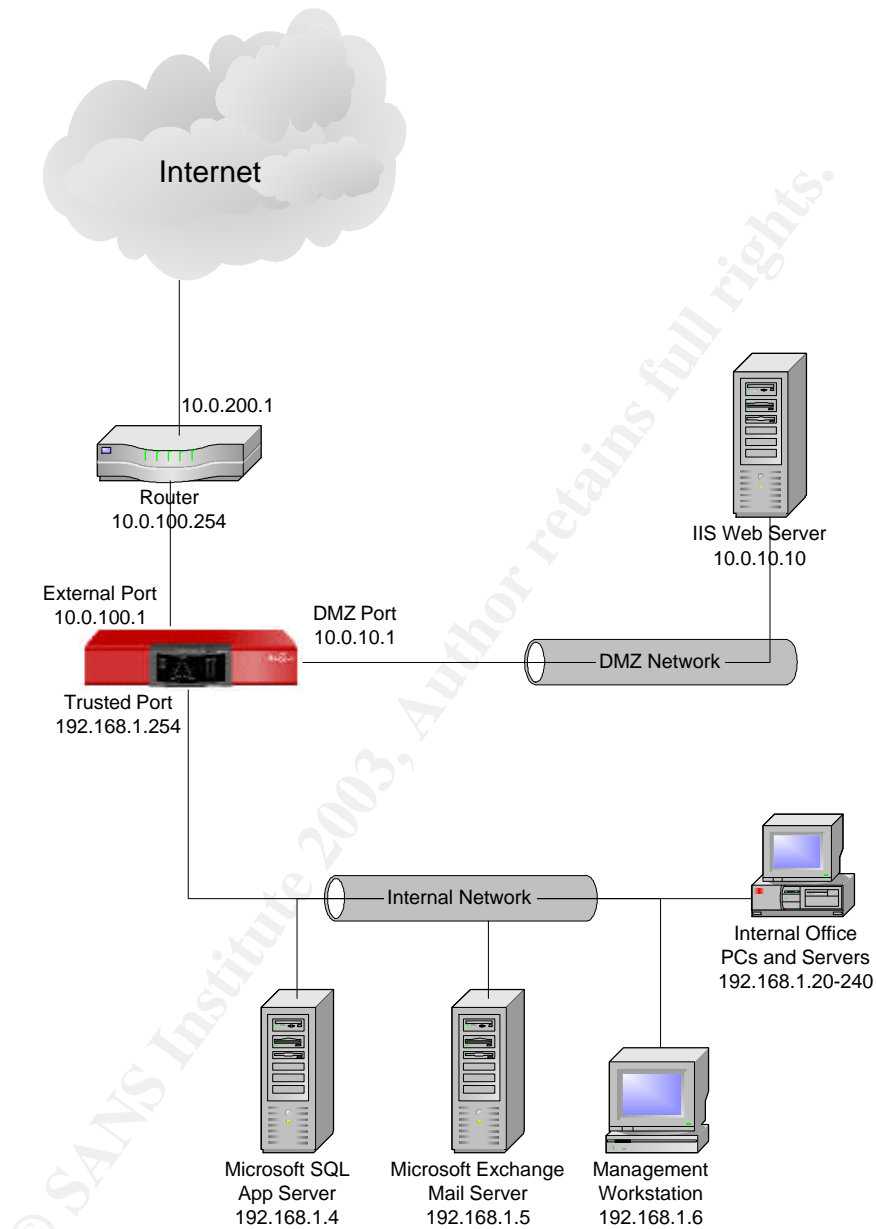

Figure 1 – Network Diagram of Audited Organization

1.2   System Risk Evaluation

As an auditor approaches the organization's network to determine the associated level of risk, there is one major aspect of the organizational structure that deserves primary consideration. This component of the organization is their perimeter. The company being examined in this audit is primarily concerned with image and perception by the community and as a result defacement or compromise of any externally exposed system will cause damage to their perception to the community and thus credibility, which is this company's primary asset.

As was noted earlier, the organization being discussed in this audit is primarily a service oriented television media company. In light of that it should be noted that as a result they do not possess trade secrets of any form that would be valuable to someone outside the company. In fact, due to the nature of their business, if information the company has is not released nearly immediately it is of no use to any of the organization's competition. This information has focused the management's perceived security risk to be at their perimeter rather than on internal threats such as employee behavior. Information theft from within the organization is not a primary concern.

Therefore the primary security investment the company made was in the protection of their perimeter systems. Since they have no traveling or mobile users the issue of whether or not to utilize a VPN at the perimeter was a non-issue. Therefore as the audit for the perimeter systems was conducted there was no need to consider the security of the VPN itself or the dynamic VPN configuration protocol (DVCP) present in Watchguard Firebox 700 systems (although this service has had known vulnerabilities in past versions of the system's software). There was also no need to consider the security of personal computers or laptops traveling outside of the organization due to the staff's lack of mobility.

As a result the focus of the audit discussed in this paper focuses on the maintenance, upkeep, and overall administration of the company's firewall, the Watchguard Firebox 700. The primary evaluation of risk was therefore conducted on this system. Issues such as administrative controls, transport and network layer filtering, application proxies, and maintenance procedure were the primary focus of this audit, as will be noted throughout the review.

Associated with this system are the risks associated with the external systems protected by this firewall. The two major systems which are exposed to the Internet in this environment are an Internet Information Services (IIS) server running on a Microsoft Windows 2000 server on the company's DMZ, and a Microsoft Exchange Server also running on a Microsoft Windows 2000 server, although located within the company's internet network (as noted in section 1.1).

The IIS server hosts the company's web site as well as the web sites of other small community based organizations associated with this company. The web pages hosted on this server are primarily static pages, with no dynamic scripting languages such as Active Server Pages (ASP) or Macromedia Coldfusion in use. The only scripting being done on the site are simple JavaScript commands used for ascetic appeal. As a result all scripting, read and execute privileges on the IIS server have been disabled for security reasons. The only dynamic aspect to the site is a modified JPEG file that is updated at fifteen minute intervals. This is a webcam picture that is uploaded via internal FTP after being downloaded by an automated internal system.

It should also be noted that there is no mail rely in place at this organization and that all internal mail is forwarded through the firewall directly to the internal Microsoft Exchange server. As a result port 25 for incoming SMTP traffic has been allowed to this server. However as noted earlier since there are no external or mobile users the company perceived no need to allow for external POP3 or IMAP access to the mail server. Port 110 was not opened to allow external traffic access to this site and port 80 requests are only being forwarded to the IIS server in the DMZ. It should also be noted that Microsoft requires that IIS be installed during the installation of Microsoft Exchange, and thus is running on the mail system as well.

The final major concern is the risk associated with compromise of the Watchguard Firebox's management workstation. All configuration of the Watchguard device is done via IP or serial communications with the firewall device from this workstation. Due to security concerns, the management station was located within the server area and subject to the same physical protection as the Watchguard system itself. As is expected, compromise of this system could mean potential compromise of the perimeter itself. As a result this paper will discuss the controls put into place to secure this station along with other security risks.

Some of the major risks associated with this device are summarized in the table below. This is not a comprehensive list of potential vulnerabilities, but covers some of the major risks associated with the Watchguard 700 firewall system.

System Vulnerability:	Probability of Exposure:	Potential Impact:
Malicious port 80 tcp traffic could compromise internally protected Microsoft IIS web server.	High – As can been seen on the nightly news or cracker bragging sites, web site defacement incidents are one of the more vulnerable and exposed internet exposures. NIST lists 101 CVEs (common	This vulnerability is of particular concern to this company. One of the company's largest assets is community trust. If people saw the company's web site defaced, then resident's could lose their

	vulnerabilities and exposures) on their website, http://icat.nist.gov.	trust in this company, and thus turn their loyalties elsewhere. The number of viewers for this company directly affects their bottom line through advertising revenues that would be lost in the event of losing customers.
Malicious port 25 tcp traffic could compromise internally protected Microsoft Exchange server.	High – Currently NIST lists 27 CVEs on Microsoft's Exchange sever which could be potentially exploited on this company's network.	The company has experienced times when their e-mail server has been down due to administrator misconfigurations and each time has cost the company's reputation and community's trust as noted above. E-mail lost can also translate directly into lost revenue as most advertising is time sensitive, and lost time receiving an e-mail could mean lost advertisers.
Malicious port 4100-4113 tcp traffic directed at the firewall system.	Low – Exposure of this vulnerability would require an attacker with knowledge of the firewall being utilized and of the particular vulnerabilities associated with these ports. There are currently no vulnerabilities to these ports listed as CVEs.	This could potentially disconnect the company from the internet, thus limiting their access to up-to-date news (their commodity) and thus limit their ability to report it. This again could harm their perception by the community.
Denial-of-service (DOS) attack directed at the firewall or any of the internally protected systems.	Medium – Even though there are no specific software flaws which could lead to unnecessary DOS attacks, there is always the risk that floods of traffic could monopolize the company's bandwidth and limit their service. Although this would most likely require an attack directed at this company.	This could potentially disconnect the company from the internet, thus limiting their access to up-to-date news (their commodity) and thus limit their ability to report it. This again could harm their perception by the community.
Management workstation compromised, allowing attacker to reconfigure or disable firewall device.	Medium – This would require an internal employee or intruder to expose this vulnerability.	This could potentially disconnect the company from the internet, thus limiting their access to up-

11

	Most likely this would occur by someone in the organization misconfiguring the device and thus harming the system.	to-date news (their commodity) and thus limit their ability to report it. This again could harm their perception by the community.

As noted earlier the major purpose for this audit was to protect the organization's perimeter systems. Due to scope limitations, however, the focus of this paper will be on the risks associated with the compromise of the primary perimeter protection unit, the Watchguard Firebox 700 device. All controls noted in the following checklist will focus on the protection of the firewall device and its associated management station. In a full organization audit the protection of the two associated servers would also be of primary concern, however due to scope limitations they will not be discussed in this paper.

1.3   Current State of Practice

In researching the topic of auditing and securing a perimeter Watchguard Firebox 700 device, many resources describing firewalls and their purpose are available both online and in print. However few can be found which describing specifically how to audit Watchguard firewall devices. Therefore in order to determine which specific steps should be considered when auditing the device it was determined that a custom checklist would be required to determine the perimeter's level of security. The biggest concern when determining the checklist was to attempt to cover all of the major areas of firewall security without leaving gaps in the process. Many websites and references were discovered which outlined securing port forwarding and filtering, network address translation, and administrative policies and procedures, but few outlined comprehensive descriptions of how to auditing the system as a whole.

Some of the more useful sources of information found both on the web and in print were as follows:
- The Watchguard, Inc. support website (http://support.watchguard.com)
- SecurityFocus Online Vulnerabilities (http://www.securityfocus.com)
- The SANS reading room (http://www.sans.org/rr/)
- The GIAC GSNA posted practicals on firewall auditing (http://www.giac.org/gsna.php)
- CERT Security Improvement Modules (http://www.cert.org/security-improvement/)
- Inside Network Perimeter Security edited by Stephen Northcutt

While there were many other specific resources available for creating this type of checklist, these resources proved helpful in constructing a comprehensive list of points to consider when auditing and securing a Watchguard Firebox 700 firewall. For a comprehensive listing of references utilized in creating the following checklist, please note the references section at the conclusion of this paper.

The Watchguard and the SecurityFocus websites were both helpful in referencing specific information regarding the Watchguard Firebox 700 system. The Watchguard support page listed many references, including reference guides and user guides for setting up and configuring Watchguard firewall devices. These guides proved invaluable in understanding the specific workings of the Watchguard systems as there are few other sources that specifically describe the inner workings of the systems. The SecurityFocus website also proved useful in outling specific vulnerability reports on this type of firewall. Their database of vulnerabilities was one of the few sites that cataloged specific threats against the firewall device, most often occurring in the system software (discussed more in depth later).

The SysAdmin, Audit, and Network Security (SANS) Institute's reading room and associated Global Information Assurance Certification (GIAC) posted practical assignment listings also proved helpful in researching the topic of firewall security in general with many good references here to firewall auditing and security in general. The site proved useful in providing a framework for securing generic firewall systems, though none specifically addressed the Watchguard device itself.

Finally the CERT security improvement modules and <u>Inside Network Perimeter Security</u> both served as a generic framework outlining the various aspects of securing perimeter firewall devices. They were both especially useful in understanding the scope of securing this type of device. As with any other auditing topic, one of the major concerns in determining a checklist such as this is that there will be holes in the logic of auditing and securing the device. Often it is said that while a network attacker simply needs one vulnerable hole to invade a network, the system administrator must protect against them all. These references help to provide an overall picture of the various aspects to securing and auditing this type of device.

As noted before there are many other sources of excellent information on securing and auditing firewall devices. For the sake of this assignment commonly available resources were utilized, while specific subscription or paid access sites were not referenced in depth. More specific references will be noted throughout the checklist as more in depth information is discussed. These resources, however, provide an overview to the process of researching the topic of network perimeter security and the development of auditing procedures for the Watchguard Firebox 700 device.

Assignment 2 – Audit Checklist

The audit checklist is the most commonly sought after component to any auditor's toolkit when preparing to perform an audit. Unfortunately often the auditor finds himself or herself spending as much, if not more, time researching and compiling the audit checklist as actually performing the audit itself. And unlike many other business processes, this task requires constant updating and development. Just when an auditor thinks he or she has finally mastered the art of auditing a particular device, a new vulnerability or threat is uncovered and the research process must be renewed.

This checklist seeks to be a help to auditors in that position. While the scope of this paper cannot possibly cover all aspects of auditing a network perimeter, it can provide a starting point for those auditing perimeter firewalls, and specific help to those looking to audit a Watchguard Firebox 700 firewall. While the entire research process can never be circumvented, this guide should at least provide the reader with a starting point for performing this type of audit.

The following checklist will provide the reader with a step-by-step guide to securing and auditing this type of firewall device. It will not only discuss the specific item to be audited but explain in detail the rational behind each phase of the audit. With each step the auditor will examine the control being audited for, an evaluation of the control's level of risk, an explanation of how to secure the control, a detailed guide to testing the control, whether it is an objective or subjective test, and supporting references as to the validity of the control. This guide will give the auditor or systems administrator a detailed guide of how to raise the level of security at the perimeter of an organization's network when utilizing a Watchguard Firebox 700 device.

<table>
<tr><td></td><td></td></tr>
</table>

2.1   Administrative Security Controls

2.1.1   Organizational Business/Security Goals Defined

References:	Tudor, Jan. Information Security Architecture. New York: Auerbach Publications. 2001. Hoelzer, David. Auditing Principles and Concepts (7.1). Version 1.1a. The SANS Institute, 2002.
Control Objective:	As the old adage goes, "when you aim at nothing, you will hit it every time," so goes enterprise security policies. Therefore it is vital that the goals of the organization's security program be defined from the beginning. By having these goals in place it will enable future employees to edit the specifics of the program and be able to make intelligent decisions based on a set of goals which drive the enterprise. It will also encourage continued support for the program as people understand the purpose behind the procedures.
Risk Evaluation:	**Potential Risk:** The risk for not being complaint with this control is the lack of standards within an organization. When a organization such as this does not have clearly defined standards or goals, they will then pursue multiple objectives which can divide the interests of the IT staff and divert them from what is truly helpful to secure the organization. **Probability of Exposure:** *High* – Often IT departments are locked into the day to day maintenance of their systems and view goal setting and proper documentation as luxuries which they cannot afford. There is also the likelihood that if goals have been set that these goals are outdated or do not match with the current direction of the business. **Degree of Impact:** *High* – An organization could easily focus on the non-essentials or on issues that don't relate to the overall goals of the business resulting in improper utilization of resources. The potential impact could easily drain the company's finances as well as administrative man-power if they have not set proper goals. Even after

	exhausting resources improperly an organization could still face the real security threats yet be without the resources to properly handle them.
Compliance:	The auditor should expect to find clearly defined goals that drive both the business and security decisions within the organization. These goals should definitely be included in policy documentation, and may likely be visible and repeated through other venues in the organization.
Testing Method:	In order to audit this control the auditor should request a copy of all of the information services documentation and examine it for a defined set of security policies and procedures. To verify that the organization has fulfilled this control the auditor should find a section that clearly defines the goals of the company's security program. The goal of this control is not so much to evaluate whether the goals are appropriate or not, but rather to determine whether or not they exist.
Objective/Subjective:	Objective

2.1.2 Security Policies Defined

References:	Tudor, Jan Killmeyer. Information Security Architecture. Boca Raton, FL: Auerbach Publications. 2001. (pgs. 82-83). Northcutt, Stephen. Inside Network Perimeter Security. Indianapolis, IN: New Riders Publishing. 2003. (pgs. 118-120).
Control Objective:	As a part of deciding appropriate technological security controls for an organization proper security policies must be defined which describe the purposes and methods of securing the environment. These policies will become the backbone of all technology controls implemented in the organization.
Risk Evaluation:	**Potential Risk:** By not defining organizational security policies, the organization leaves security in the hands of each employee, rather than setting definitive standards for how the company will function. Unfortunately, by not setting these policies and procedures, the decision

	making process for mitigating organization risk is placed in the hands of inexperienced end users, rather than in the hands of trained professionals. **Probability of Exposure:** High – As noted earlier, many IT departments ignore this vital aspect of their responsibilities in favor of the urgent needs that face them on a regular basis. There is a great potential that the IT staff have not taken the time to document their policies or that management has not successfully bought into the program. In either case the policies become ineffective, either as non-existent documents, or as a meaningless binder sitting on a shelf. **Degree of Impact:** *High* – An organization faces either the possibility of a higher degree of security incidents or the potential of legal ramifications if these policies are not defined. If employees don't know what's expected of them, they will be unable to fulfill those expectations as it relates to information security. Secondly an organization ties its hands legally if they fail to document these policies from the beginning, often resulting in human resources nightmares due to the lack of clarity on these issues.
Compliance:	Again, as noted in the earlier control, in order for an organization to be incompliance with this control the documentation should exist. While there are various components to the policies that should be present in the documents, the scope of this audit simply requires that the documents be in existence in order to properly evaluate the methodologies in place to audit the system firewall.
Testing:	The auditor should determine primarily if the policies are in existence. The firewall auditor should ask the system administrators for a copy of the required documentation to determine whether or not the policies exist.
Objective/Subjective:	Objective
Comments:	For added value the auditor can suggest that all policies should include some general elements, such as:

	• Date of policy ratification / modifications • Who wrote the policy • The authority which approved the policy • The purpose of the policy • An explanation of the necessity of the policy • Consequences to violating the policy • Should be clear, concise, and specific • Should be realistic • Should support, not hinder, overall organizational goals

2.1.3   Asset Values and Organizational Risks Defined

References:	Harris, Shon. <u>All-in-One CISSP Certification Exam Guide.</u> Berkely, CA: McGraw-Hill / Osborne . 2002. (pgs. 73-98) Ozier, Will. "Risk Analysis and Assessment." <u>Information Security Management.</u> Eds. Harold Tipton and Micki Krause. Boca Raton, FL Auerbach Publications. 1999.
Control Objective:	The purpose of this control is to establish an estimated value for electronic assets within the organization. This should not be confused with placing a dollar amount on electronic assets for tax or depreciation purposes. Rather this step should place a value on the data itself to determine the possible losses that would be incurred in the case of data loss or unavailability due to system compromise, outage, etc. This process will enable the organization's management to determine the appropriate levels of security needed for each segment of their enterprise.
Risk Evaluation:	**Potential Risk:** When an organization has not defined the value of internal assets or properly defined risks, they run the risk of improperly valuing assets and implementing controls to reduce risk in non-vital areas. The company needs to be focused on applying appropriate controls to protect their electronic data. Improper definition of this control exposes the organization to possible improper spending, ill-defined objectives, and not securing those resources that are truly vital to the welfare of the organization.

	Probability of Exposure: *High* – As noted before, proactive security controls are often one of the least implemented of all security controls, often due to perceived value. Thus when security becomes an afterthought and is not implemented within a company from the beginning, or when they outsource or delegate it to another entity, they run a high likelihood of ignoring this control. **Degree of Impact:** *Medium* – The largest possibly impact in this area is the potential for misappropriating resources. By not properly valuing resources, an organization will likely set a value on resources, although informally and without uniform consent. Thus security controls could be implemented which, as noted before, protect the wrong resources with the wrong degree of controls.
Compliance:	In order to achieve compliance on this point the organization must take the time to determine their worth, specifically those items directly protected by the organization's firewall. There are multiple methodologies for evaluating an asset's value, other considerations must be made than simply the purchase value of the asset. Other considerations should include: • Purchase value of the asset • Costs to restore or recreate data lost • Value of employee productivity lost during downtime • Value of losing consumer confidence • Costs to counteract possible negative publicity However, in order to be compliant with this control, the firewall auditor's role is to determine whether or not the documents are in existence.
Testing:	Testing for this administrative control is similar to the other controls of this type. Primarily it involves the auditor determining whether the documentation exists. The auditor should take time with the administrator(s) responsible for this area to review the documentation that describes how each asset value had been determined to ensure that every aspect of the asset's

	value is included in the report, again remembering that policy determination is beyond the major focus of the audit.
Objective/Subjective:	Objective

2.1.4   Personnel Policies Defined

References:	Fithen, William and Allen, Julia and Stoner, Ed. Deploying Firewalls. Carnegie Mellon Software Engineering Institute: Philadelphia, PA. 1999.
Control Objective:	Another major consideration when securing or auditing an organization's policies and procedures as they relate to firewall management is how the organization manages the personnel which have access to their systems. This section describes the management of authorized users in a networked environment, whether they be internal employees, external business partners, or somewhere in between. There are two major concerns that will be addressed here. Primarily an infosec professional must be concerned with the manner in which the organization adds, removes, or changes personnel. Secondly, although often overlooked, is the issue of personnel training and continuing education in the organization. Both issues must be addressed in order to successfully secure the network environment.
Risk Evaluation:	**Potential Risk:** The risk associated with this control is that network users would be able to authenticate against the network even after their service with the organization has ended. This can apply to both regular and contract employees, and should not be taken lightly. By failing to disable accounts, ex-employees have the ability to wreak havoc on the network after they terminate their employment. Secondly, by failing to properly train and educate employees many issues can arise from improperly configuring and maintaining equipment, to improperly utilizing the organization's resources. Both of these issues not only effect employee productivity, but also endanger the systems themselves.

	Probability of Exposure: *Medium* – The likelihood of exposure with this control is dependent on the relationship established between the IT and human resources departments. It's vital that these departments communicate effectively. Due to the high degree of potential impact with this control, many organizations have developed strict policies and procedures dictating how employee user accounts are to be created and removed, as well as defining proper training for company employees before they are able to utilize network resources. **Degree of Impact:** *High* – Should employees be ill-trained or user accounts not be deleted as they should a company runs the risk of having a high degree of impact on their systems. Poorly trained employees can easily disrupt operations through improper system utilization and often reduce the productivity of themselves and others who are forced to cope with their mistakes. Also, should an employee's user account not be removed properly, disgruntled or curious employees could potentially disrupt operations or steal sensitive company records even after they have left the organization. Those users with remote access capabilities increase the potential for impact even more.
Compliance:	The primary objective in securing this control is again to determine whether or not the organization being audited has taken the time to create the documentation and put processes into place to ensure the proper handling of personnel. The auditor should: - Request a copy of the hiring procedure from HR to determine whether they are informed as to the proper process for creating new user accounts on the network. - Request a copy of the hiring procedure from the IT staff to determine if their understanding of how and when to create user accounts is the same as HRs. - Examine a copy of the policies for employee development and training to determine whether network users are being properly trained for their position.

	Again the goal of this test is not to critique the process or types of training being given, but rather to determine whether the company has taken the time to develop these procedures or not.
Testing:	Testing for this administrative control is similar to the other controls of this type. It involves the auditor determining whether the documentation exists. Again the auditor must spend time with the administrator(s) who are responsible for the changes to the organization's personnel, both from the human resources side and the IT side of the process.
Objective/Subjective:	Objective
Comments:	In making recommendations to the organization, the auditor may recommend that there exist specific procedures will need to address how the security team will: • Add or remove employee accounts • Administer contractors and business partners • Modify account privileges • Communicate the need for change with Human Resources • Modify superuser access after a personnel change Administrators of these firewall systems must also have competencies in specific areas of technology, as described by the Carnegie Mellon <u>Networked Systems Survivability Program's Guide to Deploying Firewalls</u>, to ensure the administrator's thorough understanding of the technologies. Those competencies should be in: • TCP/IP protocols, services, and routing • Network architectures • Hardware on which the firewall runs or depends • Software on which the firewall runs or depends, including the operating system • The firewall software • Network security and survivability • Network monitoring • System management techniques

	Not only should the administrators of such systems be thoroughly trained before implementing the devices, but they must be continually educated in the threats that could potentially face the system. These administrators should not only be trained in the skills necessary to install and maintain such a product, but should also be well versed in the potential threats that could face their network. Such a program of study should include vulnerability alerts and vendor updates/announcements as well as the standard competencies described above.

2.1.5 Internet Usage Policy Defined

References:	Tipton, Harold and Krause, Micki. Information Security Management Handbook. Auerbach Publications: New York, NY. 1999.
Control Objective:	As access to the Internet and to resources outside of the bounds of the organization grows, so does the need for clear policies defining the acceptable usage of the technology. Most organizations rely on a continual connection to external resources for the purposes of communication, research, and the like. However not all external resources are profitable for the ongoing development of the organization. Therefore it is imperative that those responsible for perimeter protection enforce standards as to what is and is not accessible by internal users. In order for these administrators to make proper decisions as to what is and what is not acceptable documentation must exist which defines all appropriate and inappropriate access, thus allowing technicians to make technology decisions based on business goals.
Risk Evaluation:	**Potential Risk:** A primary risk of not defining appropriate use of network resources is less efficient employees. Secondly, and often more devastating to the organization is the possibility of creating a "hostile work environment." By failing to properly address this control, many companies have left themselves open to legal suits, financing unemployment for past employees, and hurting overall moral.

	Probability of Exposure: *High* – Most organizations find Internet connectivity a mandatory business requirement, similar to the need for telephones and electricity. However many do not take the time to dictate how those resources are to be utilized until after an incident occurs which effects the organization. Therefore there is a high probability that if a company does not define what appropriate use of an Internet connection entails, that they will be exposed to this risk. **Degree of Impact:** *Low* – Although the degree of impact for this control is noted as low, one should not assume that this control is therefore unimportant. The impact of this control is 'low' compared to the impact of other security controls associated with the firewall device. The primary impact of not implementing this control is the potential for lower employee productivity and effectiveness. However it also opens the door for creating a hostile work environment, which can lead to possible lawsuits and human resources difficulties as a result of improper Internet usage.
Compliance:	The ultimate goal of this control is to determine whether the organization has defined what is acceptable use of the organization's Internet connection. This is again a Boolean (yes/no) control being audited due to the scope and focus of the audit.
Testing:	To audit this control the auditor again must examine the organization's internal documentation. This control is also a true / false condition primarily in that the auditor's primary duty is to ensure that someone has taken the time to define what is acceptable usage of the Internet.
Objective/Subjective:	Objective
Comments:	An administrator should consider what types of possible uses of the Internet exist, and whether or not they will be allowed through the organization's resources. While there is no right or wrong definition as to how to write such a policy, certain types of usage should be considered when developing this policy. Those include:

	• Web content (pornography, gambling, stock quotes, extremist sites) • Outgoing TCP/UDP services allowed (FTP, HTTP, Telnet, SSL) • E-mail content (personal vs. corporate, trade secrets, confidential information) • Other communications services (ICQ, instant messaging, etc.) • Internal PCs acting as servers (peer-to-peer file sharing, GoToMyPC) These are simple some of the decisions an administrator must make when defining acceptable versus unacceptable usage of the organization's Internet connection. The important feature of this control is that someone internally defines acceptable use of this connection. This will empower administrators of perimeter systems to set technology controls on equipment to protect the environment and help promote efficient use of company resources.

2.1.6 Firewall Ruleset Policies Defined

References:	Northcutt, Stephen. Inside Network Perimeter Security. Boston: New Riders Publishing. 2001. Tipton, Harold and Krause, Micki. Information Security Management Handbook. Auerbach Publications: New York, NY. 1999.
Control Objective:	This control defines specific sets of rules that define what type of traffic is allowed into or out of the firewall system. This control does not attempt to describe why or what should or should not be allowed through the firewall. The key objective for this control is that the rules defining inbound and outbound traffic are documented in order that the ruleset defined within the firewall are those written in this document.
Risk Evaluation:	**Potential Risk:** By defining what types of traffic are and are not allowed through the firewall device a standard of appropriate use is defined. The risk in not documenting such rules opens the company to potential illegitimate rules being added to the device

	unknowingly, and without approval. Most administrators are hesitant to remove rules without serious discussion and testing, thus leaving a potential backdoor into an organization until a resolution has been determined. Proper documentation can mitigate this risk and cut down the time for potential exposure. **Probability of Exposure:** *Medium* – While organizations often have the tendency to neglect proper documentation, especially as related to IT, firewall ruleset documentation is often an exception to this rule. While more companies are likely to document what types of traffic are allowed, and what is not allowed through their firewall, this is not to say that exposure to this risk is minimalized. There is still a medium probability that a company will either neglect to document their firewall rulesets, or that once they are documented that they will become out of date as a result of continued updates to the system without changing the documentation. **Degree of Impact:** *Medium* – Depending on the degree of volatility in the firewall ruleset, a company will have varying degrees of impact by neglecting this control. The most common impact to not creating proper documentation is that an administrator will leave an unnecessary port or IP range open on a firewall, thus allowing an attacker to have unnecessary access to internal company resources. As noted earlier, administrators are often fearful of removing rules that they don't understand. However if the rules were properly documented, it would be that much easier to only allow appropriate traffic through the connection.
Compliance:	In order to be in compliance with this control the auditor must ask the following questions of the firewall ruleset documentation. - Does the firewall ruleset documentation exist? - Does the documentation list allowable incoming AP addresses and TCP/UDP ports? - Does the documentation list what internal ports and IP addresses are accessible from outside the network? - Does the documentation define what external

	services are accessible by internal hosts? • Does the documentation define the rational behind each of the above-mentioned hosts? Should the answer to any of these questions be no then the organization is not in compliance with this control.
Testing:	Testing for this control involves examining the documentation for the firewall ruleset to ensure that the primarily the documentation exists. Also the documentation should include all of the above-mentioned aspects to help ensure that only appropriate traffic is being allowed through the firewall device. Since this control is very specific to the firewall itself, an auditor must take the time to not only see if it exists, but also to review the quality of the document. The firewall ruleset documentation should have a distinct section for each of the following items: • Incoming IP addresses allowed • Incoming TCP/UDP ports allowed • Internal IP addresses and TCP/UDP ports accessible from the outside of the organization • Outgoing IP addresses accessible from internal hosts • Specific types of IP traffic accessible from internal hosts (typically defined by port) • Rational for allowing or denying any of the above filters • An implicit deny for all traffic not specifically defined by the policy When testing this control the auditor must determine whether or not each of these section is present in the documentation. The auditor should also examine the document for issues of clarity and conciseness to help ensure that it is easily understood by any responsible for the firewall device now or in the future.
Objective/Subjective:	Subjective

2.1.7 Firewall Change Control Documentation Defined

References:	Tipton, Harold and Krause, Micki. Information Security Management Handbook. Auerbach Publications: New York, NY. 1999.
Control Objective:	This control requires that the administrators define in writing how and when changes are to be made to the firewall system. Without proper planning and pre-defined procedures it will be easy for a firewall administrator to allow for unnecessary changes, improper changes, or changes which deny access to legitimate users. Having the proper procedures defined will protect the organization against poorly planned changes to the environment.
Risk Evaluation:	**Potential Risk:** The risk of not having proper change control documentation is that improper or untested changes could result in a multitude of errors, system downtime, or leave a system vulnerable to unnecessary risk. Therefore all changes to the system should undergo a series of specific steps before they are implemented on a production unit. **Probability of Exposure:** Medium – This control's potential for exposure is again dictated by the administrative policies and procedures that have been defined by the firewall administrator. Unfortunately many organizations do not allow for proper change controls to be put into place to the tyranny of the urgent which reigns within most IT departments. There is a medium chance that an IT administrator has not taken the time to document and clear with management exactly how changes to the firewall device will be accomplished. **Degree of Impact:** *Medium* – The most likely impact to neglecting this control is that an administrator will make a change to the system without fully thinking it through thus causing system down-time through a self-imposed denial of service. Normally administrators making changes to this type of system are overly restrictive when making changes in an attempt to increase the level of security. Unfortunately by doing this an

	administrator will often break a service currently necessary by someone in the organization.
Compliance:	To be in compliance with this control an organization must define the key procedures for ensuring that only appropriate changes are made to the firewall system. The minimum procedures to be defined are: • Change control procedures • Configuration testing procedures • Configuration update procedures • Software / firmware update procedures • Hardware update procedures By defining these standards an organization will help to protect itself against such things as unauthorized changes to the environment, corrupted or incompatible software/firmware upgrades, or self-imposed denial of service attacks. To be in compliance with this control there should be a defined policy for each of the above-mentioned procedures.
Testing:	As noted before, this control, as with other administrative controls should be audited to determine whether or not the documentation exists or not. Again the goal of auditing this control is not to critique the documentation or change control process in place, but rather to ensure that such a process exists and is documented in the organization's policies and procedures.
Objective/Subjective:	Objective

2.1.8   Incident Response and Recovery Policies Defined

References:	Incident Handling: Step-by-Step and Computer Crime Investigation (4.1). The SANS Institute. 2002. Tipton, Harold and Krause, Micki. Information Security Management Handbook. Auerbach Publications: New York, NY. 1999. Northcutt, Stephen. Inside Network Perimeter Security. Boston: New Riders Publishing. 2001.
Control Objective:	This objective outlines the process an organization will go through when responding to a security incident

	within their network. The main idea of this control is that when an incident occurs the security team has a set of procedures to follow which will dictate the team's response in the event of an incident. An incident can be anything from a malicious outsider obtaining access to internal resources, to a hardware failure requiring a system restore, and does not necessarily imply maliciousness in order to be classified as an incident.
Risk Evaluation:	**Potential Risk:** The risk of not having these policies in place is that as a result of an incident an organization could experience unnecessary additional downtime, or possibly even contaminate or lose data to properly investigate the incident. Organizations who do not have a proper policy in place open themselves up to responding improperly to the situation and possibly causing more damage than the initial incident. **Probability of Exposure:** *High* – Unfortunately most organizations leave incident handling policies and procedures undefined until after an incident actually occurs. At this point incident response policies become the company's biggest priority. However, by defining these policies and procedures pro-actively a company can minimize the impact of an incident and hasten the system's recovery time. Therefore this control is noted as having a high exposure rating due to the lack of pro-activity on the part of most organizations. **Degree of Impact:** *Medium* – By not implementing this control, an organization opens itself to potentially suffering unnecessary downtime in the event of a security incident as individuals attempt to determine what should be done in response. They also have the potential for destroying or contaminating data that could have been used as evidence in resulting legal matters by improperly handling the equipment after an incident.
Compliance:	In order to be in compliance with this control the organization must possess a written policy for handling incidents in their organization. That document should define the various aspects of how to respond in the

	case of an incident. Again this control seeks simply to define whether or not the policy is in existence, and not determine its quality.
Testing:	As with some of the other controls, the consideration should be the existence of the incident response documentation within the organization's policies and procedures. The auditor must determine whether or not the organization has planned for the event of security incidents taking place in the organization. The focus should not be the quality of the documents, but rather on its existence, due to the scope of the audit.
Objective/Subjective:	Objective
Comments:	Certain elements should be a part of this document, including, but not limited to, the following: • What classifies as an incident • Who is to be notified in the event of an incident • What steps should be taken to recover from the incident • Are different categories of incidents handled differently • What steps will be taken to protect against further occurrences of an incident • What documentation of the incident should be completed Again, the goal of this control is to provide a framework that details how an organization will respond to an incident in their systems. This framework should then help protect the organization against further incidents caused as a result of improper handling of the initial incident.

2.2   Physical Layer Security Controls

2.2.1   Physical Access Controls Implemented

References:	Harris, Shon. <u>All-in-One CISSP Certification Exam Guide.</u> Berkely, CA: McGraw-Hill / Osborne . 2002.
Control Objective:	This control seeks to limit unauthorized physical access to all networked equipment. Normally organizational business goals specifically address this at the server/network equipment level but do not seek physical security at the workstation level. Again, all decisions should be based on business goals and calculated risk assessments, however both should aspects be considered when formulating a decision.
Risk Evaluation:	**Potential Risk:** By not physically securing a company's network equipment, they run the risk of damage, misconfiguration of the equipment, or even possible theft. Each of these can result in financial consequences to the organization as well as potential system downtime. **Probability of Exposure:** *Medium* – In order for an attacker to exploit the vulnerability left by failing to secure the control, he would need physical access to the device. Although not impossible or even implausible, it would require work and strong initiative to begin to exploit it. **Degree of Impact:** *High* – Due to the potential impact for failing to secure this control, it is noted as a high level of impact. Not only does this control open the device to theft or damage, but it allows an attacker full control over the device and its configuration. Most all devices of this type have a method of resetting the device if you have physical access to it, the Watchguard is no exception. Thus as the saying goes, if an attacker has physical access to a device, the level of security is zero.
Compliance:	In order to achieve compliance in this are there are many things an organization can do to help secure their environment. Some things which can be utilized

	to help control who has access to what networked devices are: • Door and server Locks • Personnel Monitoring • Video Surveillance • Access Logging While there are many ways of implementing the above controls, the major issue is that the controls are in place. For example, there are many types of physical locks that can be utilized (cipher, numeric keypads, proximity / smart card readers, biometrics, etc.) and an organization will decide which to implement based on their security requirements and budgetary allowances.
Testing:	An auditor needs to ensure that proper levels of these controls are in place in order to certify compliance in this area. Controls should be in proportion to the level of security and amount of risk an organization faces. Door and server locks can be objectively quantified if they are in place. Personnel monitoring can be tested to see if there are individuals assigned to patrolling the premises looking for suspicious activity (such as security guards). Video surveillance should be in place near sensitive equipment for theft deterrent and auditing purposes, although both their presence and monitoring should be determined before noting compliance. Various forms of access auditing can also be utilized, such as sign in sheets, proximity cards with auditing capabilities, etc, based on the organization's needs. The auditor needs to check each of these areas of concern based on the risk assessment noted above.
Objective/Subjective:	Subjective

2.2.2   Management Station Secured

References:	Harris, Shon. All-in-One CISSP Certification Exam Guide. Berkely, CA: McGraw-Hill / Osborne . 2002. "Watchguard Firebox System User Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62UserGuide.pdf (March 23, 2003).

Control Objective:	This control is concerned with the security of a feature specific to Watchguard Firebox products. All Watchguard Firebox devices are controlled through a management workstation with proprietary software installed on it. All management of the firewall device should be configured through this one machine. The goal of this control is that access to this machine should be limited to only those authorized to manage the Watchguard system.
Risk Evaluation:	**Potential Risk:** As noted with securing the physical premises where the network equipment is kept, so must the location of the Watchguard management station be secure. By not physically securing workstation, they run the risk of damage, misconfiguration of the equipment, or even possible theft. Each of these can result in financial consequences to the organization as well as potential system downtime. **Probability of Exposure:** *Low* – In order for this security control to be exposed, an attacker would need physical access to the management station (or virtual if remote management software is enabled on the workstation) and the passwords to the firewall device. It would also require knowledge of how to configure the device if the password was compromised. Therefore this control has a low probability of exposure. **Degree of Impact:** *Medium* – Failing to secure this control is nearly as dangerous as failing to secure physical access to the Watchguard device. With physical access to the Watchguard management workstation an individual is able to reconfigure any or all of the settings enabled on the device. The difference between this control and the impact of failing to physically secure the device itself is that only reconfiguration, and not theft, damage, or re-setting the device can occur from this station.
Compliance:	Compliance with this control involves first securing the management workstation with all of the controls noted elsewhere in this section (2.2) to help secure physical

	access to the device. Secondly logon privileges to this device (a Windows based workstation) should be limited though local security account policies on the Windows device, (as noted in the testing description). Finally the Watchguard firebox should be configured to only accept management connections from the IP address of the machine(s) designated as management stations (as noted in the testing description).
Testing:	To test this control the auditor should first perform all of the physical security control audits as noted in this section (2.2) concerning the management workstation. Once these control objectives have been satisfied, two specific controls should be audited to determine whether or not the station has been secured. First, local security policies should be set on the workstation with the Watchguard management software installed on it. To do this the auditor should note the following: • The machine must be a PC running Microsoft Windows 2000 or XP Professional with authentication required for logon. • Under the local computer settings for this PC, the machine should be configured to only allow a local group (ie. Watchguard Administrators) to have the user account right of "log on locally." • That group should then be audited to determine if the proper domain or local user accounts are a member of this group, and no more than necessary are allowed. Secondly the auditor should test whether or not multiple IPs have the ability to manage the device. In order to check for these items: • The Watchguard management software should be installed on a machine that has not been noted as the management station. • The auditor should then attempt to connect to the Firebox being tested via an IP connection and with the help of the systems administrator,

36

	login to the device. • If the auditor is able to connect to the Watchguard system in this manner there have not been controls set for IP based restrictions for managing the machine. • If access is denied for the connection, even after proper user credentials have been supplied, then the device has been enabled for restricted management (this assumes proper user credentials have been set and audited separately).
Objective/Subjective:	Subjective
Comments:	It should be noted that Watchguard devices can be configured in two ways. The first way is to have a PC directly connected to the Watchguard device via a console type cable to the PC's serial port to the management port on the Watchguard. This method is required for initial configuration of the device. The second method for management is available after initial configuration and allows for IP based configuration of the device. It is after initial configuration, when the firewall is in this state, that the security controls should be most strictly enforced.

2.2.3   Environmental Security Controls Implemented

References:	Harris, Shon. <u>All-in-One CISSP Certification Exam Guide.</u> Berkely, CA: McGraw-Hill / Osborne . 2002.
Control Objective:	This control seeks to secure the physical setting of the organization by controlling the environment where information is being stored. These controls are outside of the range of server hardware or OS type, but instead focus on core environmental concerns for protecting an organization's data.
Risk Evaluation:	**Potential Risk:** The biggest risk to not properly securing environment controls near the firewall device is that damage to the device will come as a result. By not taking the time to properly maintain the physical environment where the Watchguard firewall is kept, the organization runs the risk of damaging the device through negligence of the

37

	product. **Probability of Exposure:** *Medium* – It can often be seen that physical equipment closets are storage areas for more than networking equipment. Items from janitorial supplies to miscellaneous computing equipment are all common items that can be found near equipment such as this. This auditor has even seen a leaking bottle of bleach stored over a production Watchguard 700 device. If the device is surrounded by equipment that is improperly stored near the device, physical damage may occur. **Degree of Impact:** *Medium* – By not securing the control the organization opens itself up to physically damaging the firewall device. Physical damage to the device can result in additional expenditures, system downtime, and downgraded performance, all of which are detrimental to the organization's proper functioning.
Compliance:	Compliance for this control involves securing the physical environment by providing a physical location that is optimal for the storage of information. Specific controls should be in place to help promote a longer lifespan for organizational equipment and reduced downtime. Such controls should include, but are not limited to having: • An uninterruptible source of electricity • A fire suppression system • A fire/smoke detection system • Physical access controls • Humidity controls • Temperature controls • A dust free environment • A clean/well-organized environment By ensuring that the above-mentioned controls in place, system administrators will help to protect against hardware failures and thus promote security. In this case the control helps protect against self-imposed denial of service attacks against the organization.

Testing:	In order to test this control the auditor should seek to ensure that each of the above mentioned controls are in place and functioning properly. This involves testing each of the areas individually to ensure compliance. For example, many of these controls will be able to be tested by simply noting their existence (such as a clean / well organized environment and physical access controls) which most all will require testing of individual systems within the facility. These tests will also most likely require the involvement of other departments whom are co-responsible for the systems mentioned (physical plant). While a lengthy description of auditing this control is beyond the scope of this paper, the control needs to be thoroughly tested in order to achieve compliance. Electrical continuity and fire suppression by be tested through attempting to access the systems in a controlled fashion (disabling power, running fire system maintenance tests). Temperature and humidity controls may also be tested through determining the actual levels of each with a non-biased test unit (personal thermometers, etc.).
Objective/Subjective:	Objective – UPS, fire suppression/detection, physical access controls, temperature, humidity Subjective – Dust-free, clean, well-organized

As part of GIAC practical repository.

2.3   Network Layer Security Controls

2.3.1   IP Source Filtering Enabled

References:	"Watchguard Firebox System User Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62UserGuide.pdf (March 23, 2003). Naidu, Krishni. "S.C.O.R.E. Firewall Checklist." URL: http://www.score.org (November 1, 2002). Fithen, William and Allen, Julia and Stoner, Ed. Deploying Firewalls. Carnegie Mellon Software Engineering Institute: Philadelphia, PA. 1999.
Control Objective:	This control dictates that the Watchguard Firebox system is utilizing IP based filters in order to restrict which traffic is allowed past the firewall. The goal is to allow only acceptable traffic past the device based on where the packet originated from (source address).
Risk Evaluation:	**Potential Risk:** By not filtering the firewall's traffic by external source IP address a company exposes itself to potential intrusions from individuals bent on attacking the network. This is especially true of those attempting to hide their address by using one of those marked as private. **Probability of Exposure:** *High* – The firewall device is located at the perimeter of the network and thus has a high probability of exposure. People from Brazil to Sri Lanka have access to this device at any time during the day due to the nature of the Internet. Anyone seeking to attack this device from an improper IP address could do so at will. **Degree of Impact:** *Medium* – By not limiting what ranges of IP addresses have access to the firewall device the company is only opening the door slightly to allow others to see the device and connect to resources that the firewall allows. The potential impact could be someone compromising the device remotely, especially one using a spoofed or improper IP.

Compliance:	In order to be incompliance with this control both of the described tests must pass. First when examining the Watchguard firewall's GUI configuration screens the following IP ranges should be present on the Blocked Sites dialog box: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16 Secondly, when testing this control from outside of the firewall, the testing computer should not be able to connect inside of the protected network. There should be a denied response when attempting to connect through the firewall using a tool such as telnet through the command line.

Testing:	Testing of this control should first involve discussing which IP addresses are being denied access with the system administrator. The documented list of which IPs are being denied should then be compared to what is actually configured in the blocked sites list.
	
	 The auditor should first determine whether the Watchguard device has been configured to only allow non-RFC 1918 addresses to connect from outside of the network. In order to test this aspect of the control the auditor should:
	
	 1. Connect to the firewall device from the management workstation using the read-only password.
	 2. Open the policy manager configuration utility.
	 3. Open the setup menu, and choose Blocked Sites.
	 4. Verify that each of the following three ranges are present in the dialog box which appears:
	
	     10.0.0.0/8
	     172.16.0.0/12
	     192.168.0.0/16
	
	 Once the auditor has determined that the device has been configured, the auditor must then ensure that the policy has been enabled by testing connections from outside of the Watchguard firewall's external interface.

41

	To do this the auditor must: 1. Logon to a computer outside of the local network being audited which has nmap installed on it. 2. Choose a port that is listening on the firewall and attempt to connect to it using the nmap command with a decoyed (spoofed) IP address on the blocked sites list. 3. An example of a possible nmap command to utilize with a Watchguard firewall is: Nmap –sS –P0 –T3 –v –p 80 –D 10.10.10.10 10.0.200.1 4. As a result of the test the auditor's IP address should be added to the Watchguard's temporary blocked IP address list, and the auditor should not be able to access any service on the Watchguard or on the network protected by the firewall (ie. HTTP – port 80).
Objective/Subjective:	Objective

2.3.2 IP Incoming / Outgoing Filtering Enabled

References:	"Watchguard Firebox System User Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62UserGuide.pdf (March 23, 2003). Naidu, Krishni. "S.C.O.R.E. Firewall Checklist." URL: http://www.score.org (November 1, 2002). Fithen, William and Allen, Julia and Stoner, Ed. Deploying Firewalls. Carnegie Mellon Software Engineering Institute: Philadelphia, PA. 1999.
Control Objective:	This control requires that specific ports or services utilize access control lists (ACLs) on each of their individual configurations. These filters are again based on IP address and restrict both the source and destination IPs for both incoming and outgoing traffic and are configured on a per service basis. These filters must be in place if the administrator is going to secure connections through the device.
Risk Evaluation:	**Potential Risk:** This risk again exposes a company unnecessarily by

	not filtering the firewall's traffic by external source IP address a company exposes itself to potential intrusions from individuals bent on attacking the network. This is especially true of those attempting to hide their address by using one of those marked as private. **Probability of Exposure:** *High* – The firewall device is located at the perimeter of the network and thus has a high probability of exposure. Again, people from Brazil to Sri Lanka have access to this device at any time during the day due to the nature of the Internet. Anyone seeking to attack this device from an improper IP address could do so at will. **Degree of Impact:** *Medium* – By not limiting what ranges of IP addresses have access to the firewall device the company is only opening the door slightly to allow others to see the device and connect to resources that the firewall allows. The potential impact could be someone compromising the device remotely, especially one using a spoofed or improper IP.
Compliance:	In order to be in compliance with this control the auditor must observe that the proper IP filters have been set on each of the firewall services according to the firewall ruleset documentation. First the auditor should observe that the proper controls have been configured in the Watchguard's policy manager when the rules are compared with the firewall ruleset documentation using the GUI tools. Secondly the auditor should observe the proper results when attempting to make a connection using a command such as telnet from the command-line. The results of the second test will vary based on which rules have been configured on the device.
Testing:	In the Watchguard System Manager's Policy Manager windows, the administrator can configure each of the individual services that are allowed into or out of the Firebox system. This will allow or disallow access to particular ports based on external or internal IP address and whether the connection is inbound or outbound.

	1. Connect to the firewall device from the management workstation using the read-only password.
	2. Open the policy manager configuration utility.
	3. Observe the graphical representation of a service that is being allowed or disallowed into the network.
	4. Each service represented has a list of internal or external IP addresses that are allowed to make a connection using that port based on whether the connection is inbound or outbound.
	Once the auditor has determined what IP filters have been enabled on the system, the auditor must determine whether those filters are in place in actuality. The specifics on testing this feature will be based on the individual configuration of the network and the firewall ruleset defined earlier. However as an example for the network in question, in order to determine whether an internal user could connect via FTP to an external FTP site, the following test could be used:
	1. On an internal Windows workstation click on the start button, and then choose Run.
	2. From the Run line type 'cmd' and then click on the button marked "OK."
	3. From the command line type the following command: telnet ftp.microsoft.com 21
Objective/Subjective:	Objective

2.3.3   Public / Private IP Addresses Used Appropriately

| **References:** | Northcutt, Stephen. Inside Network Perimeter Security. Boston: New Riders Publishing. 2001. Fithen, William and Allen, Julia and Stoner, Ed. Deploying Firewalls. Carnegie Mellon Software Engineering Institute: Philadelphia, PA. 1999. |
| **Control Objective:** | This control states that public and private IP addresses should be utilized within the network in their appropriate respective locations. Simply put, hosts requiring public Internet access should use public IPs, |

	and private internal hosts should utilize private IPs.
Risk Evaluation:	**Potential Risk:** When an organization improperly uses public IP addresses as a part of their internal address space they open themselves to exposure to external probes and attacks. This can be avoided by utilizing proper private IP address ranges and Network Address Translation in the network. **Probability of Exposure:** *High* – If an organization chooses to maintain public IP addresses as a part of their internal IP address space they leave themselves vulnerable to external users probing an potentially attacking their internal systems with greater ease. Again, due to the worldwide nature of the Internet, an organization leaves itself very vulnerable to external probes and attacks, often automated, should they choose to allow external users access to their private space. This in combination with improper filtering rules can leave the organization even more exposed. **Degree of Impact:** *High* – An organization opens itself to potential system compromise should they choose to configure their internal address space with public addresses. Often it is a matter of convenience and lack of manpower to make a successful change, however this should not stop a company from properly configuring their IP space.
Compliance:	To be in compliance with this control IP addresses should be used only in their designated areas. Public IP addresses should only be noted on the external interface or the DMZ interface of the Watchguard device. Private IP addresses should only be found on the internal interface or the DMZ interface. Should there be the wrong type of address on either the public or private interface, then this control is not incompliance. Private IP addresses are in the range: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16

Testing:	In order to properly test for this control the auditor must determine whether or not the network has been designed properly. In order to do this the auditor must: 1. First examining the network diagrams provided to the auditor by the system administrators. This assumes first of all that a network diagram is available to the auditor. 2. Secondly the auditor should examine the IP subnets configured to assure that there are no external IP addresses being used internally. 3. To further verify whether or not the organization is in compliance with this control the auditor should request a copy of the routing tables from each of the network routers, with the help of the network administrators. If there are no inappropriate public IP ranges listed in the routing tables for the internal routers, then it can be shown that the organization is in compliance with this control.
Objective/Subjective:	Objective

2.4   Transport Layer Security Controls

2.4.1   Firewall Ruleset Matched to Documented Ruleset

References:	Tipton, Harold and Krause, Micki. Information Security Management Handbook. Auerbach Publications: New York, NY. 1999.
Control Objective:	This control dictates that the documented set of rules, or types of traffic, defining what is allowed through the firewall, matches what is actually configured on the firewall device (as noted in the firewall ruleset documentation – see 2.1.5). By ensuring that the documentation and the firewall configuration match, one is assured that only allowed traffic as defined by the business logic of the organization are allowed to pass through the firewall device into the internal network.
Risk Evaluation:	**Potential Risk:** Once an organization has defined which types of traffic are allowed into and out of the network, those rules need to be evaluated at regular intervals against what is actually configured in the firewall. If the documentation does not match the configuration of the device, the differences need to be examined and evaluated. **Probability of Exposure:** *Medium* – An organization runs the risk of exposing unsecured services when they don't know definitively what ports or services are allowed through the firewall. Again, anyone with access to the Internet potentially could access one of these open ports should they exist. **Degree of Impact:** *Medium* - By not evaluating the differences between the firewall's documentation and the actual firewall configuration a company exposes itself to open backdoors and possible attack, by allowing intruders access through unnecessary services, unmonitored ports, or unsecured IPs.

Compliance:	Compliance with this control assumes compliance with the rules stated previously. Without specifically defining what types of traffic are allowed through the system it is impossible to be assured that only organizationally allowable traffic can be passed through the system. The key to compliance with this control is first that the documentation for the firewall system exists. Secondly it is vital that the documentation is reviewed and updated regularly to match the organization's business goals. Finally, the documented ruleset must match the ruleset that is actually configured on the firewall device to ensure compliance.
Testing:	The auditor should obtain a copy of the documented ruleset as a prerequisite for auditing this control. Once the auditor has obtained a copy of the ruleset, accompanied by the firewall administrator, the auditor should compare the rulesets rule by rule until it can be ensured that the list of allowed ports in the documentation matches those rules actually configured on the firewall. Specifically on a Watchguard Firebox 700 device an auditor should perform the following steps: 1. Connect to the Watchguard device through the management workstation using the read-only password. 2. Open the policy manager to observe the configured services on the Watchguard device. 3. Compare the policies defined on the Watchguard with those defined in the ruleset documentation. 4. Occasional services will need to be examined in detail by selecting the service and clicking on the modify button, which then allows the auditor to observe each individual service's details.
Objective/Subjective:	Objective

2.4.2 Unnecessary Ports Disabled

References:	Fithen, William and Allen, Julia and Stoner, Ed.

	Deploying Firewalls. Carnegie Mellon Software Engineering Institute: Philadelphia, PA. 1999. Sonnenreich, Wes and Yates, Tom. Building Linux and OpenBSD Firewalls. Wiley Computer Publishing: New York, NY. 2000.
Control Objective:	This control seeks to ensure that only allowable and necessary services are allowed through the firewall system at the transport layer. Many times due to lack of understanding or improper configuration services are allowed to pass through the firewall device without being properly filtered. This control seeks to stop these unnecessary services from passing through the device unhindered.
Risk Evaluation:	**Potential Risk:** By leaving unnecessary ports on a firewall open, it exposes internal devices to possible attack. Each open port on a device such as this exposes the organization to another service with a potential vulnerability that an attacker could exploit. If a vulnerability is found with that port, the internal system could be compromised and threaten the organization's internal resources. **Probability of Exposure:** *High* – Again, this aspect exposes the internal system to all Internet hosts with a desire to probe for vulnerabilities. The exposure for this control is again only limited by the number of potential attackers with a connection to the Internet worldwide. **Degree of Impact:** *Medium* – The potential impact neglecting this control could cause against internal systems is dependent on each internal system's level of security. This exposure only becomes a vulnerability when the internal system which is being exposed by the firewall has a flaw which opens it up to attack. Potential impacts include anything from temporary downtime to full system compromise.
Compliance:	Compliance with this control means that the system administrator understands each of the services that are allowed to pass through the firewall device, and only those services that are necessary for the proper functioning of the organization are allowed through.

	These rules will vary by the organization, however there are certain principles that should be followed as the firewall device is configured. First of all it should be observed that only appropriate ports are allowed through to internal IPs. For example, if a web server is listening for requests on port 80, and there are no other ports that the server listens on for web services, then only port 80 traffic should be allowed through to this device, and not every port for this IP. Traffic should be minimized to only allow the minimum required for functionality and thus follow the principle of least privilege as it refers to IP traffic. Secondly only necessary ports should be forwarded through based on the type of transport traffic is required. If the host is listening for traffic on port 25 TCP only, then the firewall should forward traffic only for the TCP portion of the port, not both TCP and UDP traffic. Administrators often open unnecessary holes in their perimeter based on lack of understanding of what is required for a service to function. It is all too common to see firewalls configured to allow through traffic that is unnecessary by this definition. Finally it should be observed that there are only ports being forwarded which match running internal services. If an organization is not running an internal DNS server that is accessible by the Internet, then the organization has no need to specifically forward through inbound DNS requests. However is the organization is running a web server which needs to be accessible to the outside world, then port 80 TCP should be allowed and forwarded through the device.
Testing:	The auditor's rule is to examine both the rules defined in the firewall's documentation and the firewall's configuration to determine whether or not each of the allowable services are necessary to the overall functionality of the organization. First the rules defined in the firewall must be matched to the rules defined in the ruleset documentation (see 2.4.1). Once these rules have been compared the auditor should seek to ascertain whether these rules are appropriate based on the business model of the

50

	organization. In this role the auditor is asked to play judge over the rulesets of the organization's firewall. In order to determine the appropriateness of the rules, the auditor should base the decision on: • Is the correct port aligned with the correct service (ie. DNS with port 53)? • Does the administrator understand why a port is opened? • Does the opened port correspond with a legitimate business service? Finally, the auditor should run a scan of the external interface of the Watchguard device in order to determine whether or not unnecessary services are listening on the external connection of the firewall. IN order to do this the auditor should: 1. Login to a computer with an Internet connection outside of the network being audited that has nmap software available. 2. Run the nmap command to test that ports are listening on the external interface of the device, making sure not to scan for any ports listed on the blocked list. 3. A sample nmap command which could be run against a device with a default configuration would be: Nmap –sS –sU –P0 –T3 –v –p 2-110,112-512,515-2048,2050-5999,6006-7099,7101-7999,8001- 10.0.200.1 The command should result in only ports open that were expected and configured on both the firewall device and documented on the firewall ruleset.
Objective/Subjective:	Subjective

2.5　Application Layer Security Controls

2.5.1　Inbound Application Proxies Enabled

References:	Northcutt, Stephen. <u>Inside Network Perimeter Security.</u> Boston: New Riders Publishing. 2001. "Watchguard Firebox System Reference Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62ReferenceGuide.pdf (March 23, 2003).
Control Objective:	This control states that the system administrator will enable the application proxy services for any inbound application for which Watchguard has provided a corresponding proxy. By enabling this feature the administrator allows the firewall device to filter inbound traffic based on application layer controls, thus stopping unnecessary or harmful packets from entering the network.
Risk Evaluation:	**Potential Risk:** The risk to not utilizing this feature on the firewall device is that someone could possibly pass malformed packets to the internal device, which would cause a system compromise. By placing a proxy in between a service and the external user exploits possible on the internal system are buffered by the proxy device, thus defending it from attack. **Probability of Exposure:** *Medium* – Although anyone with Internet access could be a potential attacker with access to these services, due to the more sophisticated nature of this type of attack there is a smaller pool of potential individuals who could attempt this type of attack. Although there are GUI tools available, which can be used to exploit services being protected by a proxy device. **Degree of Impact:** Medium – Ignoring this control could also leave an organization vulnerable to system compromise and exploitation. Most likely the type of attack this control protects against is a denial of service that would bring down the protected system, although there are remote code vulnerabilities that can also be executed against

	the same services.
Compliance:	In order for an organization to be in compliance with this control the firewall administrator must first match the list of services allowed through the firewall device with those services for which Watchguard provides an application layer proxy service. Watchguard provides application layer proxies for the following services: • SMTP • FTP • HTTP • DNS By enabling these proxy services external users are forced to abide by a set of rules which the administrators sets for what types of requests can be made of the internal network. For example, if an inbound SMTP proxy is enabled on the Watchguard Firebox device, all incoming e-mail are scanned via the ruleset on the firewall device. Thus an administrator can exclude certain mail content, attachments, etc. from ever reaching the internal SMTP mail server. An administrator can therefore enforce rules which state no user is to open an attachment with the extension *.exe by enabling the filter which rejects all e-mail attachments which have this three letter extension. Similar services are available for each of the other three incoming proxy services and thus allow administrators further control when enforcing organizational security policies. Each of these rules is configurable separately, and not all three need be present in every environment. It is important to note that these proxies should only be present when there is an internal server processing requests from the external network on the corresponding port. For example, if the organization is not hosting an internal SMTP mail server, there is no reason to configure an inbound SMTP proxy service.
Testing:	The auditor examining these services is primarily checking to see whether they are configured on the firewall device or not. The key for the auditor is to ensure that the proper inbound proxy services have been configured on the device, no more, no less.

	The auditor must specifically:
	1. Determine which of the four services noted above are being hosted internally in the organization. 2. Connect to the firewall system from the management workstation using the read-only password. 3. Open the policy manager for the Watchguard device. 4. Compare the list of proxy services configured in the Watchguard system's Policy Manager. There should be an inbound application proxy configured for each of the four services that are hosted internally. 5. Examine the specific rulesets for each of the proxy services configured to note if appropriate controls are in place. Ideally the auditor should be able to examine firewall documentation that describes which inbound filters are in place for each of these proxied services and compare that list to what is actually configured. In doing so it can be determined if the device has been properly configured. 6. Once a proxy service has been determined, the auditor can observe the port banners with the telnet command to determine whether or not the service is actually being proxied by the firewall. 7. For example, if the auditor was checking whether or not incoming SMTP proxying was being done, the following telnet command could be run against the device: telnet 10.0.200.1 25 The results of the above command should be a generic port banner, and not the OS specific banner of the machine being protected by the proxy.
Objective/Subjective:	Subjective

2.5.2 Outbound Application Proxies Enabled

References:	"Watchguard Firebox System Reference Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62ReferenceGuide.pdf

	(March 23, 2003). Northcutt, Stephen. <u>Inside Network Perimeter Security.</u> Boston: New Riders Publishing. 2001.
Control Objective:	This control states that the system administrator will enable the application proxy services for any outbound application for which Watchguard has provided a corresponding proxy. By enabling this feature the administrator allows the firewall device to filter outbound traffic based on application layer controls, thus stopping unnecessary or harmful packets from leaving the network.
Risk Evaluation:	**Potential Risk:** While inbound proxies protect internal servers from outside attacks, outbound proxies do the opposite. Outbound proxying will protect internal devices from potential attacks on the outside. A company risks having its internal hosts compromised when not utilizing some form of outbound proxy. Specifically it protects against malicious code being executed from an outside source (such as ActiveX, Java, or JavaScript), thus compromising the integrity of the machine. **Probability of Exposure:** *Low* – This exposure, although a very real threat, has less of a potential exposure than others. In order for an internal system to be exposed to such an attack they must visit a web site that contains malicious code and have their browser settings set such that they would be vulnerable to being exploited. Also in many cases it requires that the user allow the malicious code to execute, which hopefully they've been trained to avoid. **Degree of Impact:** *High* – However, should a user neglect the various controls set in place to protect against this form of malicious code, the compromise could range from the installation of a moderate virus to full system compromise potentially leaving a backdoor through the firewall into the internal network.
Compliance:	In order for an organization to be in compliance with this control the firewall administrator must first match the list of services allowed through the firewall device with those services for which Watchguard provides an application

	layer proxy service. Watchguard provides application layer proxies for the following services: • SMTP • FTP • HTTP • DNS By enabling these proxy services internal users are forced to abide by a set of rules which the administrators sets for what types of requests can be made of the external network. For example, if the system administrator has configured the outgoing HTTP proxy service on the firewall device, organizational policies that restrict outbound web based traffic can be enforced. If the organization has limits on what type of content can be viewed (gambling, pornography, extremist, etc.) then these rules can be enforced via the outbound HTTP proxy service. The organization can also restrict which types of controls a user can view (ie. ActiveX, Java, JavaScript, etc.) via this proxy service. It can even be used to cache web sites frequently visited by internal users for faster web page loading and preserving external bandwidth. Similar services are available for each of the other three outgoing proxy services and thus allow administrators further control when enforcing organizational security policies. Each of these rules is configurable separately, and not all three need be present in every environment. The proxy service should only be enabled if that particular type of traffic is allowed outside of the environment. If outbound FTP traffic, for instance, is always denied by organizational security policy, then port 21 should be blocked outgoing, and the FTP proxy service should not be configured.
Testing:	The auditor examining these services is primarily checking to see whether they are configured on the firewall device or not. The key for the auditor is to ensure that the proper outbound proxy services have been configured on the device, no more, no less. The auditor must specifically:

	1. Determine which of the four services noted above are being hosted internally in the organization.
	2. Connect to the firewall system from the management workstation using the read-only password.
	3. Open the policy manager for the Watchguard device.
	4. Compare the list of proxy services configured in the Watchguard system's Policy Manager. There should be an inbound application proxy configured for each of the four services that are hosted internally.
	5. Examine the specific rulesets for each of the proxy services configured to note if appropriate controls are in place. Ideally the auditor should be able to examine firewall documentation that describes which outbound filters are in place for each of these proxied services and compare that list to what is actually configured. In doing so it can be determined if the device has been properly configured.
	6. Once a proxy service has been determined, the auditor can observe the port banners with the telnet command to determine whether or not the service is actually being proxied by the firewall.
	7. For example, if the auditor was checking whether or not outgoing HTTP proxying was being done, the following telnet command could be run against an external address: telnet www.msn.com 80 The results of the above command should be a generic port banner, and not the OS specific banner of the machine being protected by the proxy.
Objective/Subjective:	Subjective

2.6   Firewall Operating System Security Controls

2.6.1   User Authentication Enabled

References:	"Watchguard Firebox System User Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62UserGuide.pdf (March 23, 2003).
Control Objective:	This control secures access through the firewall based on user authentication. This control becomes especially useful when it is configured alongside of a proxy based service such as "Proxied HTTP," which will restrict HTTP traffic through the firewall (see 2.5.1 & 2.5.2). The control requires that some external form of authentication be utilized to help protect the system and possibly reduce the number of user authentications required to use the system.
Risk Evaluation:	**Potential Risk:** This feature enables outbound requests to be authenticated and logged by an internal device. The risk associated with this control is that users would abuse their network connection and access resources inappropriately without being logged or tracked. By using authentication an organization helps to ensure that only appropriate users utilize appropriate resources, and that when they misuse their privileges that they are tracked. **Probability of Exposure:** *High* – Most organizations have employees who, whether they realize it or not, are not going to follow the company's security policy as it relates to Internet usage. Unless some technological control is put into place to stop them, most company employees will utilize this resource without concern for how it relates to their company's standards. Thus a company will have a high exposure to potential vulnerabilities associated with neglecting this control. **Degree of Impact:** *Low* – Most impact associated with the neglect of this control comes in the form of lost employee productivity, with more extreme forms of misuse

	potentially resulting in an atmosphere of a hostile workplace, an HR issue. However there is less likelihood of network or system compromise with this control than with others mentioned.
Compliance:	To be in compliance with this control the administrator needs to enable user based authentication on the Firebox system. When this service is enabled the user has the ability to connect to the web server running on port 4100 of the Watchguard system and authenticate against the system. Authentication is enabled by default on the Watchguard system, however it must be utilized with a proxy service in order to be of any value (such as HTTP or FTP). The default mode of authentication is Firebox based, where users and groups are maintained on the system itself. For further security and simplified user access, the Watchguard also provides the following forms of authentication: • Firebox • Windows NT Server • RADIUS Server • CRYPTOCard Server • SecurID Server
Testing:	The auditor can determine if user authentication is configured by two separate tests. First the auditor can determine whether or not the service is configured by: 1. Connect to the Watchguard firewall device via the management workstation using the read-only password. 2. Open the firewall Policy Manager. 3. Open the Setup menu and choose Firewall Authentication. 4. If the firewall is configured to utilize authentication the dialog box that appears will indicate that configuration. Secondly the auditor can attempt to see if the firewall configuration software is running on port 4100 on the firewall device. In order to test for this the auditor should:

	1. Login to an internal workstation with network access to the Watchguard device.
	2. Click on the Start button, and choose Run.
	3. Enter 'cmd' and then click 'OK.'
	4. From the command line type the following command: telnet 192.168.1.254 4100.
	5. If the telnet command returns unsuccessful, then the authentication service is not listening on the firewall device. If the device returns a successful connection, then the authentication service is probably running on the device.
	After determining that the firebox system is utilizing authentication, the auditor should attempt to connect to the IP address of the internal interface on the Watchguard system, on port 4100. For example, if the internal IP of the system is 192.168.1.254, then the auditor would connect to http://192.168.1.254:4100 and access the java based authentication applet. If the auditor is able to authenticate the java applet should then be minimized and the auditor should have access to HTTP or FTP services as requested.
Objective/Subjective:	Objective

2.6.2 Running / Installed Services Minimized

References:	"Watchguard Firebox System User Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62UserGuide.pdf (March 23, 2003). Northcutt, Stephen. Inside Network Perimeter Security. Boston: New Riders Publishing. 2001.
Control Objective:	This control seeks to secure the system by only allowing services to be enabled on the system that are required to meet the business goals of the organization. By disabling all but the needed services the system is less likely to have a service running which has a vulnerability should one be released. The system also becomes less complex and requires that one less service be locked-down by the administrator.
Risk Evaluation:	**Potential Risk:** The risk to this control is that a vulnerable system's

	service would be enabled unnecessarily, and thus open the system up to a vulnerability. By disabling unnecessary services, there are that fewer opportunities for an attacker to exploit the system and gain access to resources illegitimately. **Probability of Exposure:** *Medium* – The probability of this risk's exposure is dependent upon the configuration of the firewall and the services that are available and are unnecessarily installed. If the services are only available on the internal or DMZ interfaces, then there is a low degree or potential exposure. However, if the services are installed and available on the external interface, then the exposure could be great. **Degree of Impact:** *High* – Should this potential risk become exposed, especially to the external connections of the firewall, the potential impact which could occur would be great. Unnecessary services are often left unpatched and unmonitored, leaving the system vulnerable to attack. If an external attacked found this vulnerability and exploited it, the resulting impact could again reach the level of total system compromise through the use of malicious code or arbitrarily executed commands.
Compliance:	Compliance for this control mandates that the system administrator first determines which services are required to be running on the Watchguard system. Fortunately for the administrator of this system there are few services that are configurable on this type of device compared to other software based firewall devices. In the world of network firewalls there are two major types of firewalls on the market. The first type of firewall is the software based firewall. Software based systems require an underlying operating system (such as Microsoft Windows) to be installed before the firewall software can be installed. The other type of device is the hardware based system. These devices typically are firmware based or are integrated into another operating system (such as an embedded Linux solution).

Testing:	While typically firmware based systems, such as Watchguard, with their own proprietary software, often do not have as many services installed on the system, it is still important for the administrator to verify than no unnecessary services are installed. To verify what is running on the system an administrator can run a port scanning application, such as NMap to determine what ports have been opened on the system. When testing the system the auditor should find first all of the ports that have been defined in the firewall ruleset. Beyond those ports the auditor should find the following ports opened:
	• 4100 – Authentication Applet • 4101 – WSEP and management station • 4103 – Receiving port for WebBlocker database • 4105 – Watchguard service • 4106 – WebBlocker • 4107 – WSEP and Firebox
	In order to scan for whether or not unnecessary services are enabled, the auditor should:
	1. Download and install the latest version of nmap from http://www.insecure.org on a machine on the outside of the network. 2. From the command line on that workstation the auditor should issue the following command: nmap – 3. The auditor may have to execute this command multiple times, checking for smaller ranges of ports due to the blocked services list on the Watchguard device. If this happens the auditor will notice the nmap timing out. 4. The final resulting list of open ports will list all of the open services on the external connection of the firewall device.
	If any ports other than those founding the ruleset or listed above are listening for connections then those ports need to be investigated to determine if there is a misconfiguration or compromise of the system.
Objective/Subjective:	Subjective

2.6.3 Operating System Patch Level Updated

References:	"Watchguard Firebox System User Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62UserGuide.pdf (March 23, 2003). "Watchguard Firebox System Firebox III Hardware Guide." 2003. URL: http://help.watchguard.com/docs/FBIII700500HardwareGuide.pdf (March 23, 2003).
Control Objective:	This control states that the operating system, or in this case firmware level, of the system is the most current stable version of the system software. By staying up to date with the most recent version of the software and all patches, the system is more protected against known vulnerabilities against the system. By having the correct software installed known flaws in the system's software will be hardened and less likely be exploited.
Risk Evaluation:	**Potential Risk:** By not staying updated with the most current version of the system's software, an administrator exposes the corporation to unnecessary risk. Software updates are most often released to patch known system vulnerabilities. By not staying up to date on these patches, the system becomes open to external compromise and thus jeopardizes the internal network's resources. **Probability of Exposure:** *Low* – With the Watchguard system there are very few known exploits known and listed as common vulnerabilities and exposures (CVEs). Most known issues are associated with previous released of the system (Firebox II) versus the current system type (Firebox III). However the few Firebox III vulnerabilities are associated with the DVCP protocol used with VPN configuration, not installed on this system. Therefore the probability for this exposure is low. **Degree of Impact:** *Low* – Due to the nature of the potential exploits against the Watchguard firewall the level of potential impact against an organization is low. There are very few exploits available against unique Watchguard services and software flaws. However those that are available for previous versions are all primarily denial of service vulnerabilities.
Compliance:	In order to be in compliance with this objective, the firewall

	system should be up-to-date with the most recent version of the firewall firmware or operating system with all patches applied. As of the writing of this document (March 2003), the most updated version of the software is version 6.1 SP1 Strong Encryption. As long as the software is up to this version level, there are no patches that need to be installed on the system. New versions of the software can be obtained by logging into the secure web site at http://support.watchguard.com/, (only available to registered Watchguard customers). Administrators need to check regularly with the vendor's website or documentation to stay updated with the most current stable release of the software. Watchguard makes it easy for the administrator to stay on top of the most recent issues by providing it's own bugtraq type of service, known as Livesecurity Service, which notified administrators who have registered their systems what updates they need to apply. This Watchguard service also makes the administrator aware of other system related software vulnerabilities, such as the recent Sendmail and Snort vulnerabilities released in early March. It is also recommended that administrators of these systems utilize another service, such as SecurityFocus (http://www.securityfocus.com) to see if other known vulnerabilities have been found in the software. Typically vendors are good about releasing information on vulnerabilities for which they have fixes, however by checking a neutral third party web site the administrator can see if there are other known faults in the system.
Testing:	To test this control the auditor needs to verify the software version of the Firebox system being audited. This can be verified by: 1. Opening the System Manager on the management workstation. 2. Once in System Manager the auditor can open the system's policy manager, open the Help menu, and then select About Watchguard. 3. Once this is selected a dialog box will appear which will note the current software version that the firewall system is at. 4. This version number can then be compared to the most recent version of the software from the Watchguard support website (http://support.watchguard.com) to see whether the system is in compliance with this control.

64

Objective/Subjective:	Objective

2.7   Firewall Maintenance Controls

2.7.1   System Logging Enabled & Exported

References:	Fithen, William and Allen, Julia and Stoner, Ed. Deploying Firewalls. Carnegie Mellon Software Engineering Institute: Philadelphia, PA. 1999. Northcutt, Stephen. Inside Network Perimeter Security. Boston: New Riders Publishing. 2001. "Watchguard Firebox System User Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62UserGuide.pdf (March 23, 2003).
Control Objective:	This control notes that the logs of all noteworthy activities at the firewall device are logged and exported to an external syslog server for later analysis. This control seeks to ensure that primarily logging has been properly enabled on the firewall, and secondly that those logs are being exported to another internal device (syslog server) where, in the event of a break-in, they can be analyzed and protected from unauthorized modification.
Risk Evaluation:	**Potential Risk:** If this control is not utilized properly, then an attacker has the opportunity to compromise the system without ever being detected or traced by someone within the organization. The attacker will thus be free to exploit internal systems at will, without ever being detected, due to logs being the primary and often the only opportunity an administrator has to notice illegitimate network exposure. **Probability of Exposure:** *High* – Any connection or attempted connection with the firewall or associated network should be logged and recorded. This way in the event of a security incident the IT personnel have the opportunity to try to determine what was compromised and respond to the incident appropriately. Due to every connection to or through the device being a potential incident, there is a high probability to not having this control in place.

	Degree of Impact: *Medium* – The greatest impact to not enabling this control is that an incident could occur through the firewall which compromises an internal host and the system administrators not have a proper understanding of what occurred in order to clean up after the incident. Also, without logging system events there is often no way to know for sure whether or not an incident has occurred.
Compliance:	In order to be in compliance with this control, as noted above, the system must first have logging enabled on the device. Logging is enabled by default on the system and is configured by adding the IP address of the internal IP to the WSEP Log Hosts configuration windows on the firebox system. Secondly the system administrator should enable logging to another server within the organization. This is to ensure that in the event of a system compromise, that the log files will be preserved and the attack can be recognized. Watchguard Firebox 700 devices have the ability to forward all logged entries to a syslog server that can be used to analyze the logs. This also lessens the need for additional administrators to have access to the system, as the logs can be monitored on another device.
Testing:	An auditor can easily determine if logging is enabled on the Watchguard system. When the auditor opens System Manager on the management workstation, the default screen that opens is a partial log-view of recent events. From here the auditor can further determine if log files are being saved by opening the LogViewer application and examining all of the saved system logs on the device. An auditor can also determine if syslog logging has been enabled on the device in two ways. 1. First the auditor should open System Manager on the management workstation. 2. Once this is open the auditor needs to open the policy manager, and select Setup, then logging. 3. In the dialog box that opens the auditor should select the syslog tab and determine which IP is

67

	being used to record all logs.
	4. An auditor should also then examine the syslog server itself to determine whether logs are actually being recorded on the device from the Watchguard.
Objective/Subjective:	Objective

2.7.2 Administrator Access Restricted

References:	"Watchguard Firebox System User Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62UserGuide.pdf (March 23, 2003).
Control Objective:	The goal of this control is to verify that there are a limited number of administrators who have access to the Watchguard device.
Risk Evaluation:	**Potential Risk:** The risk to this control is that too many individuals obtain administrative access to internal systems. With this level of privilege being the highest possible, improper utilization of this account can lead to system compromise both by internal or external resources. **Probability of Exposure:** *Low* – Due to the relatively few people with access to this level of security privilege the exposure to this vulnerability is low. Only those explicitly given one of the two administrator passwords would have the potential to violate this control by giving out the passwords to the system. Although the nature of administrative access to the Watchguard device is an issue of itself (only two administrative passwords present, read-only and read-write). **Degree of Impact:** *High* – If the administrator account was improperly utilized or if it became available to someone who should not have access to this level of authority, the degree of impact would be high. This could lead to system reconfiguration, which could eventually lead to internal system compromise. Thus those with access to administrative privileges should be limited to protect

	against exposure.
Compliance:	An organization is in compliance with this control if they have a limited number of administrators with access to the system. First one must understand levels of administrative access to Watchguard Firebox 700 devices. With this device there are two levels of access available, read and read/write access. As would be expected the read configuration allows a user to view the configuration, log files, etc. without being able to change the actual system configuration. Read/write administrators have both the ability to view the configuration as well as make modifications to it as well. Unfortunately at this time there is no way to integrate directory services authentication with administrative permissions, only user permissions as discussed earlier. An organization must first determine which administrators should have access to the device. Typical recommendations are that no more than 2 to 3 administrators have access to either level of authority at any one time. It is also recommended, however, that more than one administrator have rights to the machine to allow for a proper overlap in duties. This password should also be changed at regular intervals (typically every 30-45 days), and kept in written form in a secured location in the event of an emergency.
Testing:	Unfortunately this control is often difficult to audit, considering the nature of the issue. Administrators may often divulge this information unknowingly and thus violate the control without an auditor ever being aware of the breech. For basic testing of this control the auditor should survey the IT administration to see who has access to the device and at what level. But, as would be expected, the auditor must rely on the trustworthiness of those interviewed. However, an auditor may request the logs noting the change frequency of the password in order to determine whether or not the password is being changed at regular intervals, or when administrative personnel changes.

Objective/Subjective:	Subjective

2.7.3   System Backup Procedure Implemented

References:	"Watchguard Firebox System User Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62UserGuide.pdf (March 23, 2003).
Control Objective:	This control seeks to ensure that the system configuration for the Watchguard device is backed up at regular intervals. By backing up the system configuration files administrators have the opportunity to restore the firewall device to the state it was in prior to a system failure.
Risk Evaluation:	**Potential Risk:** The potential risk to not implementing this control is that in the event of a system failure an administrator would need to take more time to restore the system, leaving more downtime, and potentially not restoring the device to its proper configuration. If there was no original configuration documentation made, then potentially the administrator might restore the system to a different state than the original baseline. **Probability of Exposure:** *Medium* – There is a chance that system failure would cause the system's configuration to be reset, or need to be reconfigured. This would be most likely be due to a system failure which required the replacement of the original equipment. **Degree of Impact:** *Low* – Should the system lose its configuration due to a system failure or compromise of some time the time it would take to restore the system to its original configuration would be minimal, considering the ease of system use. This process would be slightly more difficult if proper system documentation was not present. However most system administrators would be able to restore this configuration to at least workable levels in a low amount of time.
Compliance:	In order to be in compliance with this control the

	system administrator needs to devise a policy and procedure that schedules the backup of the system configuration files for the Watchguard device. In order to function properly there is one main configuration file that needs to be backed up whenever modifications are made to the firewall configuration.

In order to understand how to create a backup procedure for the Watchguard, one must first understand how Watchguard stores the configuration. Whenever an administrator makes a change to the Watchguard system the configuration for the system is first saved as a *.cfg file saved on the management station's hard drive. By default the file is saved with the convention (internal IP address).cfg. For example if the firebox's internal IP address was 10.1.10.1, the default configuration file name would be 10.1.10.1.cfg. Once this file has been saved to the hard drive the Watchguard will prompt the administrator whether or not the file should be uploaded to the firebox. If the administrator says yes, then the file is uploaded, the system is rebooted, and all configuration changes have been made.

Therefore the backup strategy for the Watchguard configuration simply involves backing up the *.cfg file which is created at configuration time. This file, along with a copy of the System Monitor software (used to change/upload system configurations), should then be backed up, labeled appropriately, and kept in a secure physical location. The file should be backed up every time a change is made to the system, but may go months without being backup up again, assuming no change have been made.

Like any other backup this backup should be tested regularly to help ensure that there has been no corruption to the file, and can be used to restore a configuration if needed. |
| **Testing:** | To test to see whether this control is in place the auditor should ask the system administrator to see a copy of the backup of the file and test to see if it is a valid, uncorrupt configuration file. If the file is available, then the first part of this objective has been met. |

71

	Secondly the auditor should attempt to restore this file to a non-production Watchguard Firebox 700 device, if it is available, to see whether or not the file is a valid, usable file. If the file is available, and can be restored to another unit, then this objective has been met. Often times, however, this objective can be difficult to actually test due to the availability of a spare Watchguard 700 device. In the event a device is not available the administrator should take the time to open the configuration file in a text editor (such as notepad) to see that the file is a valid, readable file, and that it is not corrupted. It is often even easier to test by opening that file with a spreadsheet application such as Microsoft Excel, and importing it as a delimited file.
Objective/Subjective:	Objective

2.8 Conclusion

The above checklist should provide both system administrators and network auditors with a starting point for determining exactly how they will approach the securing and auditing of a Watchguard Firebox 700 firewall device. Each organization should keep in mind that they will need to determine the precise level of security required for their environment and adjust their plans for auditing appropriately. Unfortunately in information security there is no one size fits all model for securing this type of device.

Now that a baseline for what needs to be audited has been determined, the next phase will involve actually completing an audit, using the above checklist as a model. Assignment 3 will outline in further detail ten of the checklist steps to give administrators and auditors an example of how to actually perform an audit of this type of system.

Assignment 3 – Sample Audit

3.0   Overview

Having already determined the various areas, which should be considered when auditing a Watchguard Firebox 700 Firewall, an auditor should now possess a reasonable checklist for determining the security level of one of these devices. As an example of how to follow through on the actual audit, the following section (3.1) has been added in order to demonstrate an audit of one of these systems performed for Local Media, Inc. (a fictitious name). The following is an example of ten of the controls noted in the previous section, which are most applicable to the audit of the system, five of which are stimulus/response tests. These examples include samples of information discovered during an actual audit of a system in production, in the environment described earlier (1.1), however the information as you see below has been 'sanitized' in order to protect the identity of the organization whose systems were audited.

3.1   Sample Audit Steps

2.2.2   Management Station Secured

Results:

Subjective – FAIL

Audit Type:

Observation

Evaluation:

In evaluating the management station's level of security there were a few issues that were discovered during the course of the audit. First of all the management station was located in the same room as the Watchguard Firebox 700 device and all of the other server and networking equipment. Therefore it would be fair to say that the level of security for the management station was the same as that of the server and networking equipment itself, including the Watchguard 700 device itself. The area where this equipment is kept has only two entrances. One of these entrances remains locked 24 hours a day and the other is unlocked 24 hours a day. The locked entrance was found propped open many times during the course of the audit and people freely moved into and out of it without being audited. The other entrance was used constantly by technicians in order to

access a room adjacent to the server area in order to utilize video editing equipment. Again people entered and left this area without being audited.

The Microsoft Windows 2000 computer the workstation software was running on did have restricted local logon policies as described in the audit checklist (2.2.2). However it was also noted that when the management workstation was initially audited the screen was open to a standard windows desktop. Even though an additional password is required to access the configuration of the Watchguard device (either read-only or change), the configuration files themselves were accessible to anyone with physical access to the device. All Watchguard configuration files are stored by default in "c:\Program Files\Watchguard" on the management station. Anyone with access to these files (*.cfg) has the ability to determine how the firewall device is configured. Therefore the security of the firewall is only as secure the station used to configure it.

An administrator should remember that should someone obtain a copy of the configuration files they would have the ability to load the Watchguard software on any internal machine and use those files to reconfigure the firewall via IP. The Watchguard software is common to all firewall devices, and can be obtained from any Watchguard partner. This would then allow an individual to attempt to break the configuration password from anywhere inside the network, and then reconfigure the device.

It should also be noted that the user found logged into the device had Windows NTFS rights to the Watchguard *.cfg files, and could have easily transferred those files to a floppy disk or to an FTP server. Screen shots of what was found can be viewed below.
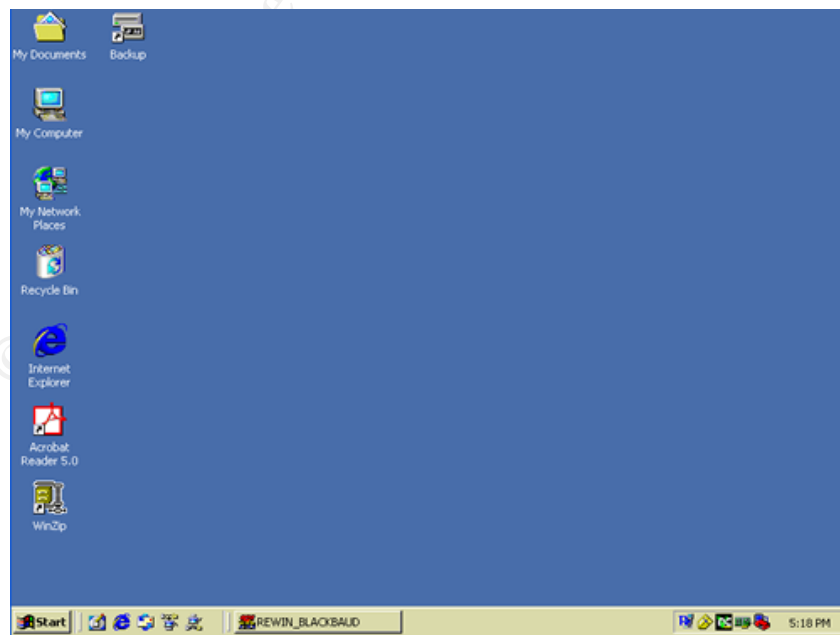
Figure 2 – Unlocked Management Workstation

2.3.1   IP Source Filtering Enabled

Results:

Objective – FAIL

Audit Type:

Stimulus / Response

Evaluation:

It was noted that when checking the configuration of whether IP source filtering was enabled or not that the following IP addresses were being blocked by the Watchguard system:
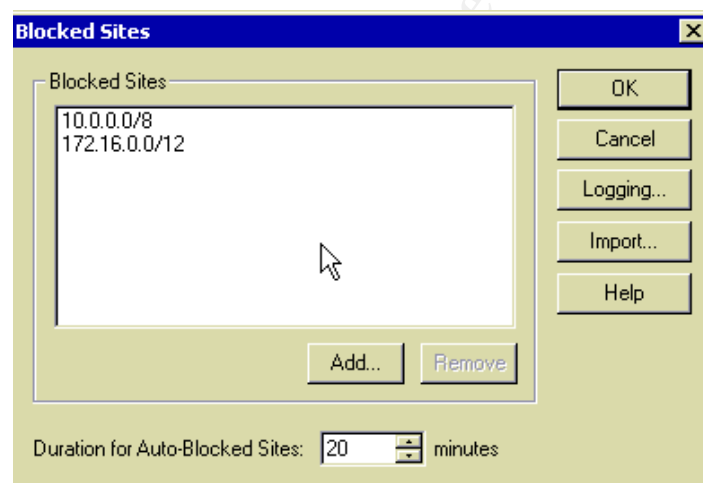
Figure 3 – Blocked Sites Dialog Bock

While most of the private addresses noted by RFC 1918 were included in this blocked sites listing, it was noted that the class C range of 192.168.0.0/24 – 192.168.255.0/24 was not included in this listing. Secondly it was noted that no other ranges of IPs were removed from this list (ie. Overseas IPs, known malicious computer user domains, blacklists, etc). However, after discussing this with the business managers of the company it was discovered that the company's goal was to provide information to people, wherever they were, whoever they were. Their business goals dictated that they should not block any legitimate user from access to their information. Regardless of this policy it was noted that any address in the 192.168.0.0/16 range should have been blocked from entering the external interface of the device.

To ensure that the above noted addresses were indeed being blocked from passing through the firewall a test was performed to determine whether IPs were actually being blocked from the external connection. In order to do this the auditor must attempt to connect to a known running service on the firewall, using a spoofed IP address, and have the connection timeout.

Therefore first it had to be determined that there was a valid listening port on the Watchguard device which was indeed accessible from outside of the firewall. To test this the HTTP service was chosen (which was allowed on the company's configuration) which runs on port 80 tcp. To ensure this port was indeed running on this particular device the following command was issued from outside of the firewall (destination IP address has been modified):

Nmap –sS –P0 –T3 –v –p 80 10.0.200.1

The results of running this command are as follows:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host 10.0.200.1.isp.net (10.0.200.1) appears to be up ... good.
Initiating SYN Stealth Scan against 10.0.200.1.isp.net (10.0.200.1)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on 10.0.200.1.isp.net (10.0.200.1):
Port      State      Service
80/tcp    open       unknown
Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds
```

Figure 4 – Initial nmap Scan Results

Therefore when examining the output of the above command it can be seen that tcp port 80 is currently open on the IP address being scanned. Next, in order to determine whether or not any IP addresses are being filtered by the Watchguard device, the nmap command should be run again, this time using a spoofed addresses in one of the blocked IP address spaces. This can be tested by running the above command but with an additional switch (-D 10.10.10.10). This switch will spoof the source address of the machine doing the nmap scan. The full command will therefore look as follows (destination IP address has been modified):

Nmap –sS –P0 –T3 –D 10.10.10.10 –v –p 80 10.0.200.1

The results of this scan were:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host 10.0.200.1.isp.net (10.0.200.1) appears to be up ... good.
Initiating SYN Stealth Scan against 10.0.200.1.isp.net (10.0.200.1)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on 10.0.200.1.isp.net (10.0.200.1):
Port      State      Service
80/tcp    filtered   unknown
Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds
```

Figure 5 – Filtered nmap Scan Results

After running this command from outside of the firewall, it was noted that the packet was detected by the firewall and recorded in the on-screen logviewer, noting it as a spoofed source address. After the second command was executed all subsequent attempts to connect to the network from the same IP were filtered and no connections were able to be made for 30 minutes (due to the temporary IP block list). The reason port 80 was chosen in the above example was that port 80 runs a known service (HTTP) which is running and responsive on the device. Therefore since the service is running the Watchguard did detect this IP address as a spoofed address, and did deny the connection to the firewall, therefore filtering the IP traffic as it should. However, since only two of the three IP address ranges, which definitely should be blocked (as noted above), were present in this device's configuration, this aspect of the audit was still noted as failed.

2.3.2   IP Incoming / Outgoing Filtering Enabled

Results:

Objective – PASS
Audit Type:

Observation

Evaluation:

When checking individual ports, which were allowed through the system to determine whether or not IP filtering had been configured according to all business rules, it was determined that indeed the proper IP filtering had been enabled on the firewall device. For this organization, due to their policy of allowing anyone access to their web and mail services, and the necessity for administrators to configure internal devices remotely from anywhere, it was easy to determine how IP port level filtering should be enabled. The business logic dictated that any IP address be allowed to enter to specific servers within the environment (as noted in figure 1). Below are screenshots taken from the management station, which shows port configuration, and a sample service

configuration (Proxied-HTTP). When examining these port settings it was noted that everything was configured correctly.
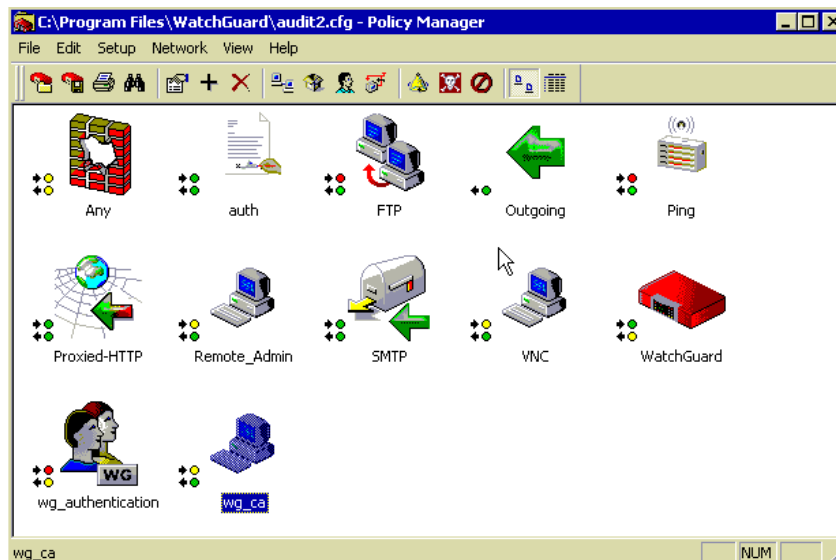

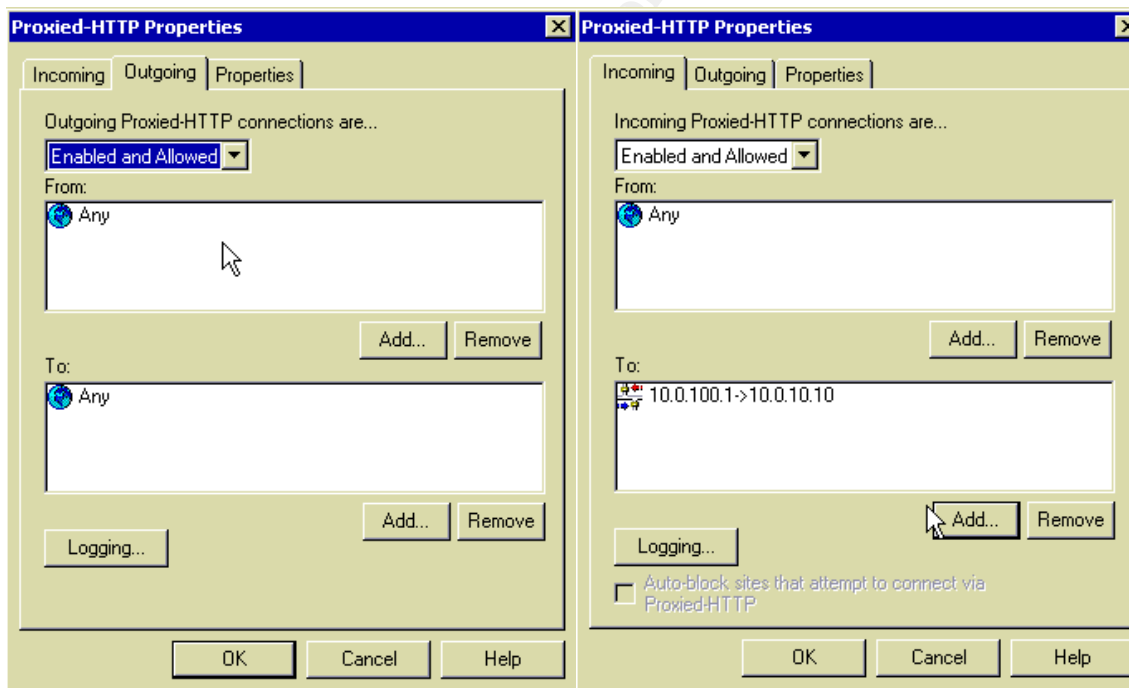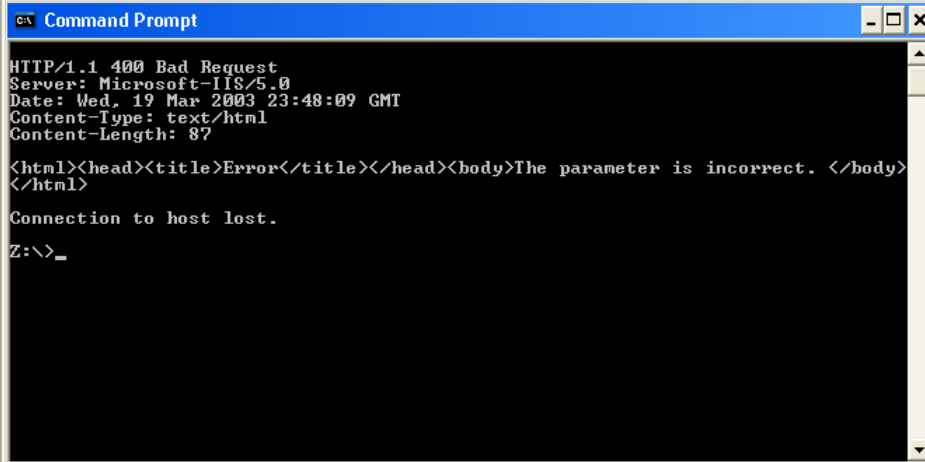**Figure 6 – Watchguard Policy Manager**

Figure 7 – Proxied Port Incoming / Outgoing IP Restrictions

A check was also performed to note whether an actual connection could be performed through the firewall device to an internal listening server. To test that the port was indeed configured correctly and accepting connections, telnet requests were made of the individual listening ports inside the network. Below is a sample of one of the telnet displays done from outside of the network to the internal Microsoft IIS web server. The command "telnet 10.0.200.1 80" was used

79

with the following invalid "GET" statement to produce the following results (please note the IP address noted above has been sanitized to protect this network):

Figure 8 – Inbound Telnet to Port 80

As a result it was noted when completing these tests that IP filtering, other than those noted in 2.3.1, were not being done on these particular ports, as per the company's business requirements. Since any 'real' IP address is allowed to connect to the network from the external interface, this audit control indeed matches the company's business model and is noted as a pass.

2.4.2 Firewall Ruleset Matched to Documented Ruleset

Results:

Objective – FAIL

Audit Type:

Observation

Evaluation:

When evaluating this control the organization's system administrators were asked for the documentation used to define the firewall's ruleset. Unfortunately when asked for this documentation the reply was that if the documentation did exist, the administrators were not aware of it. The original configuration of the device had been outsourced to a third party consulting firm who configured the device as they saw fit. They used what they felt were appropriate rules for the network environment and if the consultants did document the firewall ruleset it was not provided to the administrators responsible for the upkeep of the system. Below is a screen capture showing the ports that were configured to be allowed through the device as well as a table outlining the configured services on the

system (only transport rules shown). Although without original ruleset documentation it was impossible to compare the two. Therefore this control was noted as a fail.
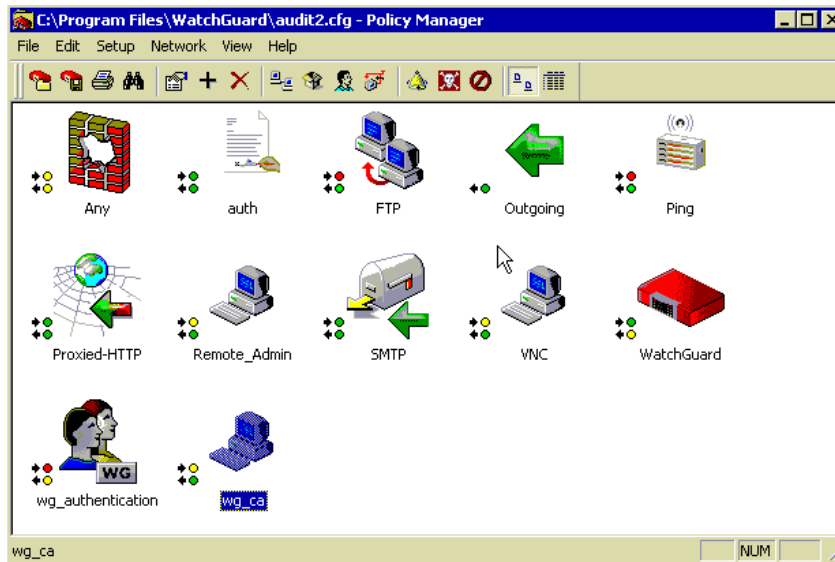
Figure 9 – Watchguard Policy Manager

Service:	Port:	Allowed/Denied:	Incoming/Outgoing:
Authorization	113 tcp	Allowed	Incoming
Authorization	113 tcp	Allowed	Outgoing
FTP	21 tcp	Denied	Incoming
FTP	21 tcp	Allowed	Outgoing
Outgoing	Any	Allowed	Outgoing
Ping	ICMP	Denied	Incoming
Ping	ICMP	Allowed	Outgoing
Proxied_HTTP	80 tcp	Allowed	Incoming
Proxied_HTTP	80 tcp	Allowed	Outgoing
Remote_Admin	4899 tcp	Restricted	Incoming
Remote_Admin	4899 tcp	Allowed	Outgoing
Proxied_SMTP	25 tcp	Allowed	Incoming
Proxied_SMTP	25 tcp	Allowed	Outgoing
VNC	5900 tcp	Restricted	Incoming
VNC	5900 tcp	Allowed	Outgoing
Watchguard	4103 tcp 4105 tcp	Allowed	Incoming
Watchguard	4103 tcp 4105 tcp	Restricted	Outgoing
Wg_Authentication	4100 tcp	Denied	Incoming
Wg_Authentication	4100 tcp	Restricted	Outgoing
Wg_CA	4112 tcp 4113 tcp	Restricted	Incoming

Wg_CA	4112 tcp 4113 tcp	Allowed	Outgoing
Any	Any	Restricted	Incoming
Any	Any	Restricted	Outgoing

Figure 10 – Configured Firewall Services

2.4.2   Unnecessary Ports Disabled

Results:

Subjective – PASS

Audit Type:

Stimulus / Response

Evaluation:

In evaluating whether or not unnecessary ports were allowed to pass through the firewall device, first the ports were configured to be allowed to pass through the device were noted. A graphical representation of the allowed ports is noted in the following screen capture taken from the management station (or see above table, 2.4.2).
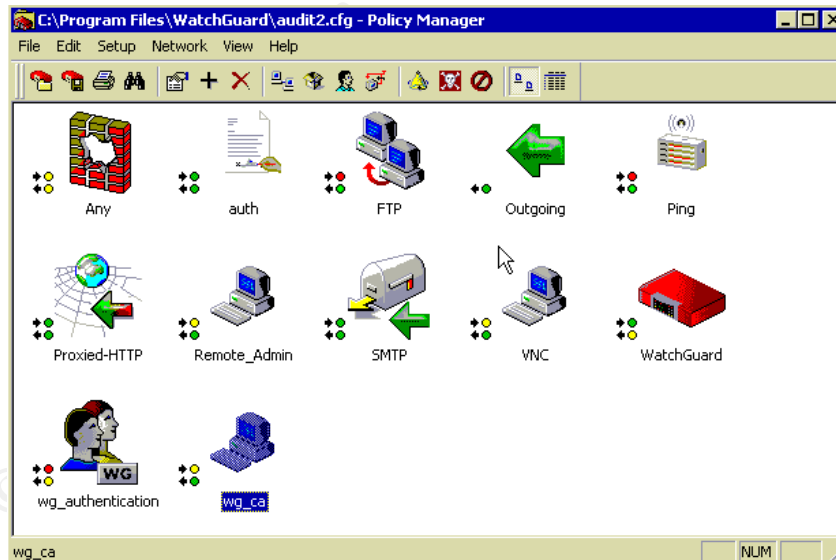
Figure 11 – Watchguard Policy Manager

It was also noted that in the firewall configuration that certain ports were marked as "Blocked Ports" within the system's "Blocked Ports" configuration. This can be accessed by:

82

1. Connecting to the Watchguard device from the management workstation using the read-only configuration password.
2. Opening the Policy Manager dialog box (from the top of the configuration console).
3. Choosing the menu option, Setup, then selecting "Blocked Ports."
4. The Blocked Ports dialog box will appear, noting each port blocked by the firewall device. Any IP address trying to connect to the Watchguard firewall using one of these ports will automatically be added to the temporary blocked IP list.

The following is a screen shot noting some of the ports that were noted as blocked by the system:
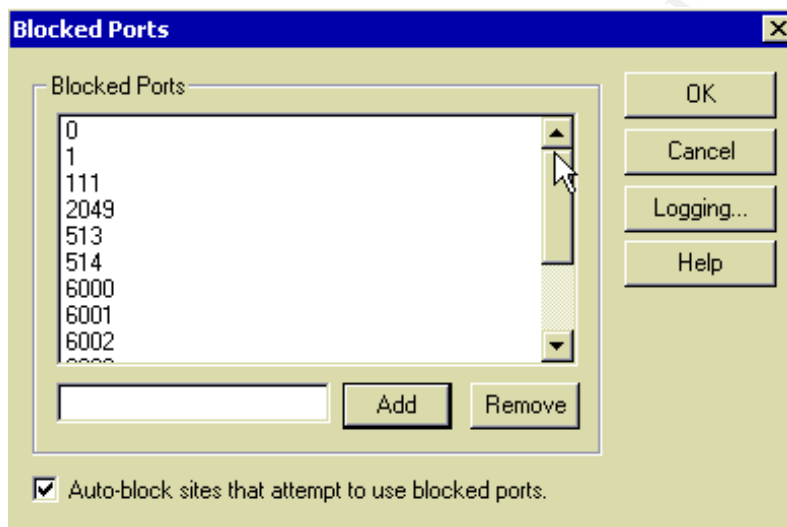
Figure 12 – Policy Manager's Blocked Ports List

While there are other services that could have been added to this list (small services, etc.), it should be noted that the original configuration was set liberally due to the setting noted on the above screen capture (Auto-block sites that attempt to use blocked ports). With this feature enabled, any IP attempting to connect to one of these ports, purposefully or not, will be added to the temporary blocked sites list, which denies all IP traffic from that address for a specified period of time (in this case 30 minutes).

To ensure that there were no other ports listening for connections which were not listed in the above tools or on the blocked sites list, nmap was used to scan the external interface from the outside of the network using the following sanitized command (IP address has been modified):

Nmap -sS -sU -P0 -T3 –v –p 2-110,112-512,515-2048,2050-5999,6006-7099,7101-7999,8001- 10.0.200.1

Due to the extensive output of running this command, especially with the UDP port listing, a summary of the output is listed below. It should also be noted that

83

this scan was run after 11:00pm against the system. This was at a time when the particular office building was open, but when users would not be actively using the Internet connection as frequently. That is why there were no UDP ports displayed on the scan that were expected in the results (due to incoming connections initiated from within the subnet). At other times when nmap scans were performed various UDP ports were displayed, but random, and different each time, depending on when the scan was run. Although when trying to connect to one of these miscellaneous open UDP ports, the connections were always refused (most likely due to the stateful inspection feature on the firewall). The nmap command consistently noted the following ports as listening on the Watchguard device:

Port	State	Service
25/tcp	Open	smtp
80/tcp	Open	http
113/tcp	Open	auth
4103/tcp	Open	unknown
4105/tcp	Open	unknown
4112/tcp	Filtered	unknown
4113/tcp	Filtered	unknown
4899/tcp	Open	unknown
5900/tcp	Open	vnc

It should be noted that allowing nmap scanning had to be accomplished with the help of the system administrator, as the auto-block port setting noted above had to be disabled to allow nmap to scan the system for listening ports. Initial tests failed due to nmap stalling whenever it attempted to connect to a port listed on the blocked port list. It was decided that the most prudent course of action would be to test only those ports that were not listed on the Watchguard's blocked ports list. However, initial tests were run to ensure the blocked list was actually functioning. In order to test the blocked ports list the following command was run (with 111 being an example of one of the blocked ports):

nmap –sS –P0 –T3 –v –p 111 10.0.200.1

As a result of this command, the nmap session sat at the scanning prompt for 24 hours (timing out), and eventually stopped with a Ctrl-C keystroke. It was therefore determined that the blocked port list functioned appropriately for this port. Subsequent tests were run on each of the Watchguard's blocked ports to ensure that access to the device would be denied from these ports. The blocked ports for this device are 0,1,111,513,514,2049,6000-6005,7100, and 8000. The administrators of this system should also consider automatically blocking other ports, such as 23, 139, etc. that are commonly scanned for on the Internet.

This test was noted as a pass due to only the appropriate and necessary ports that were expected were visible when conducting the scan and no unnecessary ports were noticed.

2.5.1   Inbound Application Proxies Enabled

Results:

Objective – PASS

Audit Type:

Stimulus / Response

Evaluation:

This control seeks to determine whether or not the appropriate inbound application layer proxies are enabled on the Watchguard device to provide another layer of protection to incoming traffic. Below is a screen capture noting all incoming and outgoing ports, including proxied services:
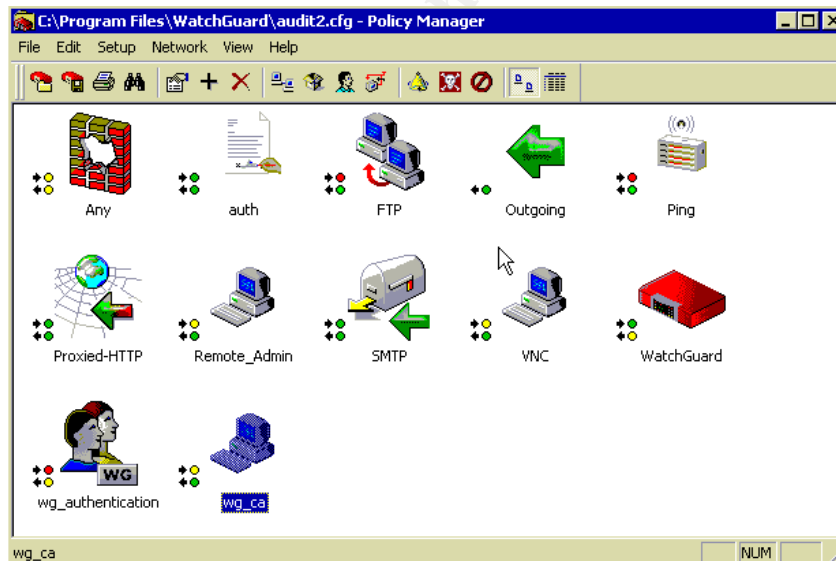
Figure 13 – Watchguard Policy Manager

In examining this screen it should be noted that the system allows for incoming proxy services on SMTP mail. This is the only service currently configured in this environment that is appropriate for inbound proxying to be done. It can also be noted on the property sheet of the incoming SMTP proxy a sampling of some of the settings possible with this service.
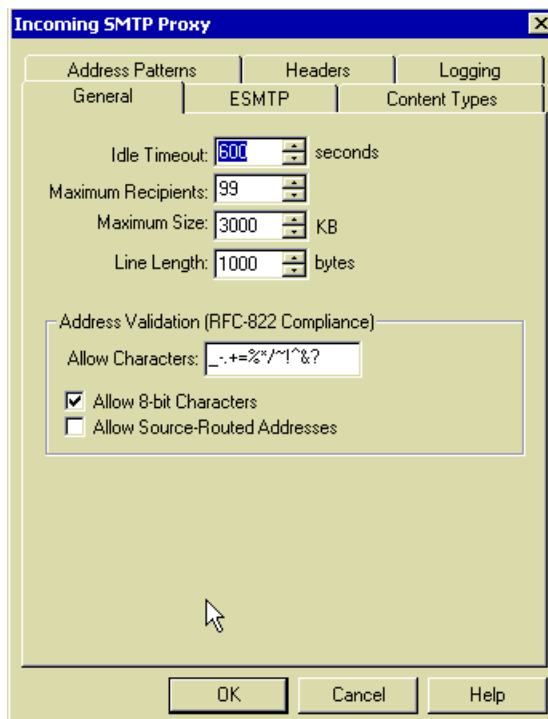
Figure 14 – Incoming SMTP Proxy Settings
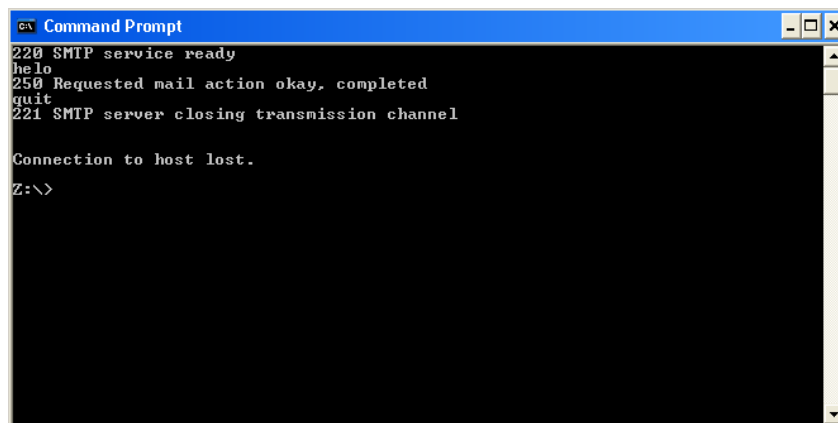
To test to ensure that proxying was indeed being performed on incoming SMTP connections a test was performed to see whether the appropriate port banners were displayed when connecting to port 25 via telnet. In order to test this the following command was used from outside of the network (IP sanitized):

telnet 10.0.200.1 25

Since the internal server accepting SMTP connections is a Microsoft Exchange 2000 server, the port banners should indicate the following line:

Microsoft ESMTP MAIL Service, Version: 5.0.2195.5329

However instead of the above default Microsoft banner being displayed (as was displayed when connecting to the SMTP server from an internal IP address) the following banner was observed:

As part of GIAC practical repository.

Figure 15 – Output of External Telnet to Port 25

As can be seen the banner has been changed to reflect the generic banner used by the Watchguard service listening for incoming SMTP connections. Therefore it can be assured that indeed the Watchguard itself is accepting the incoming connection requests and proxying them to the internal server, rather than simply forwarding the connections to the internal Microsoft Exchange 2000 server. Therefore this control is noted as a pass.

2.5.2 Outbound Application Proxies Enabled

Results:

Objective – FAIL

Audit Type:

Stimulus / Response

Evaluation:

This control checks to determine whether or not the appropriate outbound proxy services have been enabled on the Watchguard Firebox system. In the organization currently being audited it was determined that the only appropriate outbound proxy service was the Proxied-HTTP service. When examining the port configurations for this device the following settings are observed, which would cause one to assume that this service has been enabled:
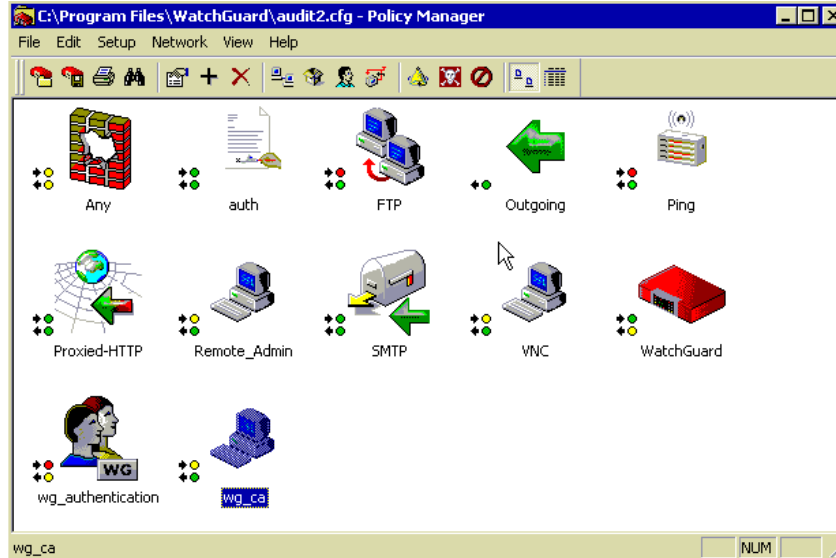
Figure 16 – Watchguard Policy Manager

However, after further investigation of the system's configuration and the user's ability to utilize web services, it was determined that this service was not configured correctly. The following screen capture notes the settings that were configured to be blocked on the system (especially take note of blocked ActiveX controls).
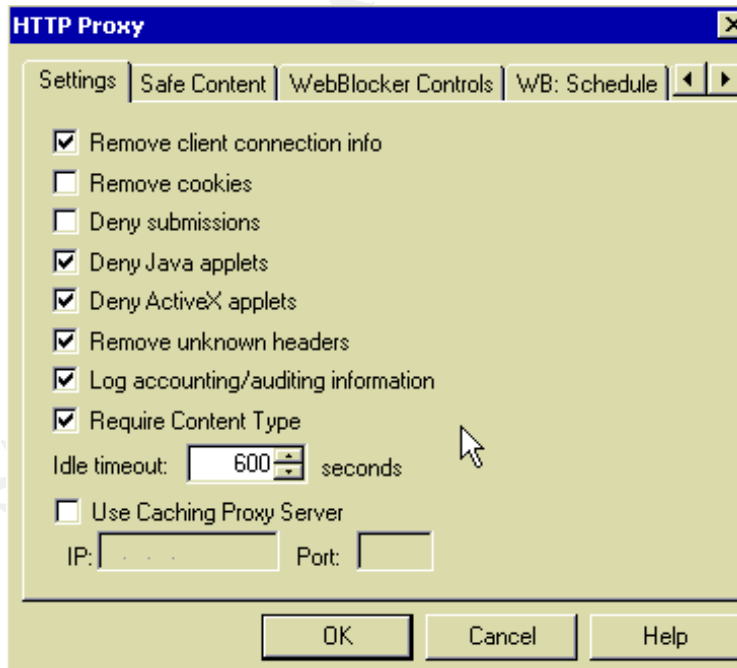

Figure 17 – Outgoing HTTP Proxy Settings

However, when connecting an internal web browser to a site that requires an ActiveX control to be downloaded and installed, the browser was able to download the ActiveX control and execute it, as observed in a screen shot from a

browser on the internal network accessing a Microsoft Terminal Services Web Client home page (requiring ActiveX):
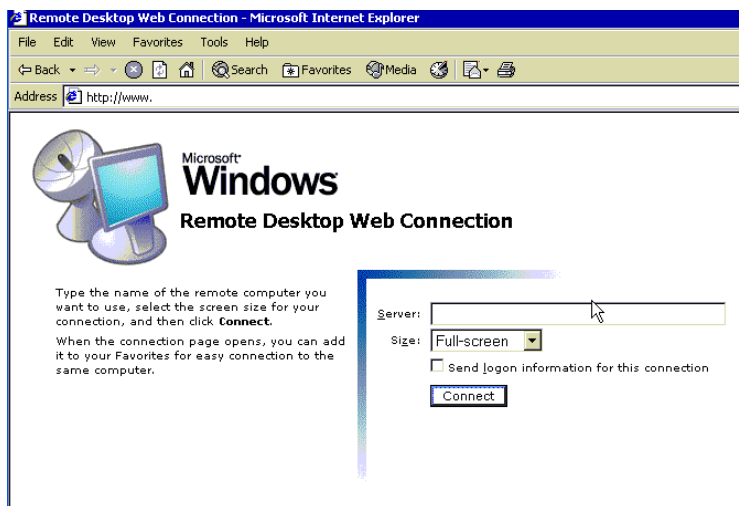
Figure 18 – Web Browser Utilizing ActiveX Control

Another option for determining whether or not this proxy service is enabled is do utilize the telnet command, as was done when testing inbound proxy services. In order to test outbound proxy services the same logic can be applied as above, and the auditor can view the HTTP banners when connecting to an external web site from a host residing off of the internal interface of the Watchguard firewall. In order to test this feature the auditor should first connect to a web site using telnet with a connection that is known to not utilize proxy services. The following is a sample command that can be used for this:

telnet www.msn.com 80
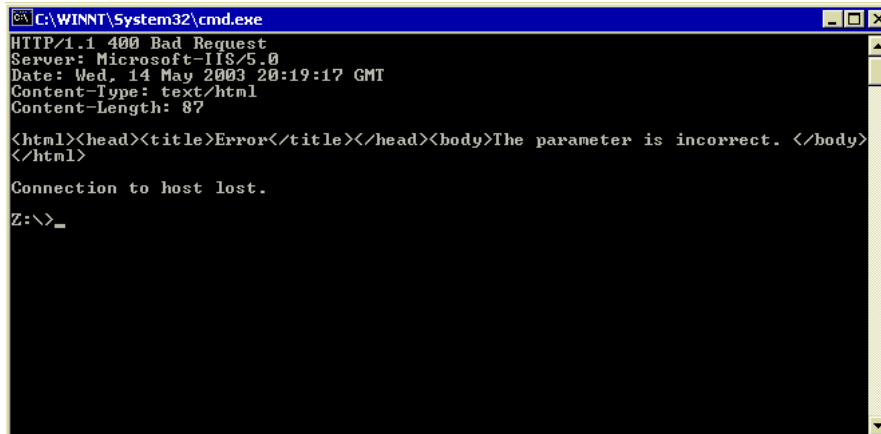
Once the connection has been established, the auditor should type random characters, and then press <Enter> twice. When the auditor does this, the following results will display:

Figure 19 – External Telnet to Port 80

However when performing the same command (with the following characters and <Enter>) from within the internal network protected by the Watchguard firewall, the results should look display a different HTTP banner, as was noted earlier when testing the SMTP service via telnet. Unfortunately when running the same command as was run externally from within the firewall the same results are returned, as follows:

Figure 20 – Internal Telnet to Port 80

Thus it must be determined that the HTTP proxy service has not been enabled for outgoing connections. This, along with the ActiveX test noted above, supports the auditor's findings when examining the Watchguard's GUI configuration. It must be concluded that there is no outbound HTTP proxy being utilized at this time.

It was later determined that the service was indeed configured correctly according to the businesses needs, however the proxy service was never enabled on the system. In the above noted configuration screen there is a check box that enables the proxy service. This check box was left unchecked on this system. Therefore clients were able to browse the web without utilizing a proxy between them and the external connection. This control is therefore noted as a fail.

2.6.1 User Authentication Enabled

Results:

Objective – FAIL

Audit Type:

Stimulus / Response

Evaluation:

This control audits whether users are required to utilize an authentication service before being able to make connections outside of the internal network. There are various ways of authenticating with this type of firewall device as noted in the description of this control. Normally it can be difficult to audit this control, especially if Windows authentication is selected, due to the transparency of the authentication proxy. However for this environment it was noted that the default Firebox authentication type was selected, which requires a special action on the part of the user before accessing external resources. The following screen captures note this configuration:
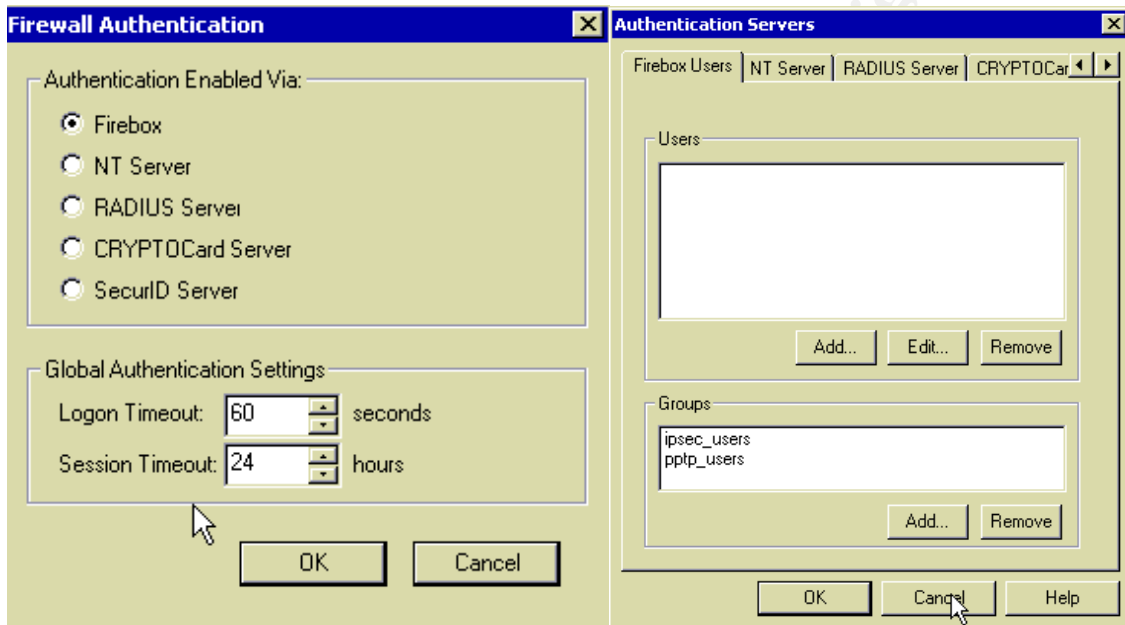

Figure 21 – Firebox Authentication Settings

It should be noticed than on both of these screens the Firebox authentication control was selected, however no firebox users were configured on this device. It was also determined when observing a user browse to an external web site that the Java control, which shows that the user has successfully authenticated against the Watchguard device, was not visible on user's system tray. Notice on the following screen capture that there is no specialized icon for the internal user on the Windows toolbar as should be if this control is configured properly (lower-right):
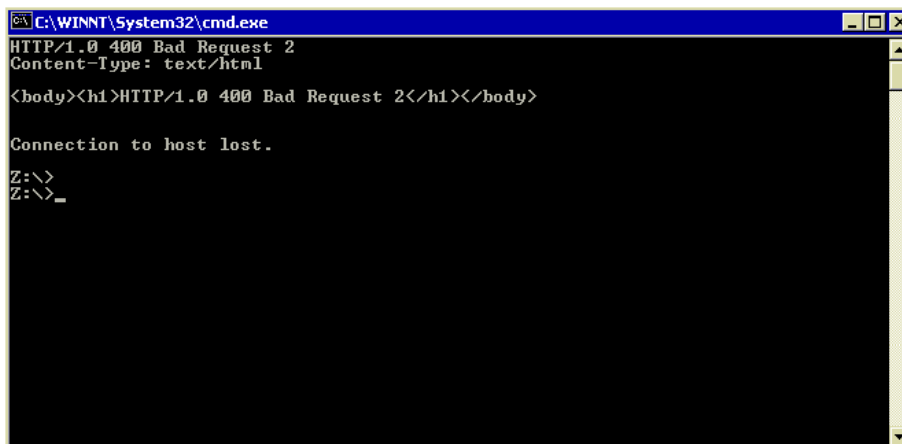
Figure 22 – Active Web Browser Without Authentication Applet on the Windows System Tray (Lower-Right)

The auditor can also test to determine whether or not the Watchguard authentication service is running on the Watchguard through issuing a telnet command to port 4100 to determine whether or not that service is listening for connections. Therefore from an internal IP address off of the internal interface of the Watchguard device, the auditor should issue the following command:

telnet 192.168.1.254 4100

If there is a listening service on this port, there should be some form of response when issuing the command. However to ensure that the service is the Watchguard authentication service listening on port 4100 the results should utilize HTTP, since the authentication service utilizes a Java applet running via a web browser on that port. Therefore the results of the command should be similar to the proxied-HTTP test run earlier and look similar to the following screen capture:

Figure 23 – Telnet to Port 80 (Watchguard Authentication)

Therefore since users are able to connect to external resources without authenticating against any internal authentication server (Firebox, Windows NT, or otherwise), even though there was a listening service on TCP port 4100 (the Watchguard authentication service), it must be noted that this service is not in use and therefore the control is noted as a fail.

2.6.3   Operating System Patch Level Updated

Results:

Objective – FAIL

Audit Type:

Observation

Evaluation:

This control seeks to determine whether or not the firmware for the Watchguard Firebox 700 is up to date with the current software release from Watchguard Systems, Inc. Thankfully for a system like this it is relatively easy to maintain and to determine whether or not the system is at the appropriate level since there is only one software package which ever needs to be updated. As of the writing of this paper (March 2003) the current software version released by the manufacturer is version 6.1 SP1 strong encryption. As noted in the following screenshot, the version of software running on the system is 6.0 – B1140. Since the current software level (which fixes known vulnerabilities and system bugs) is not on the system, this control is notes as a fail.
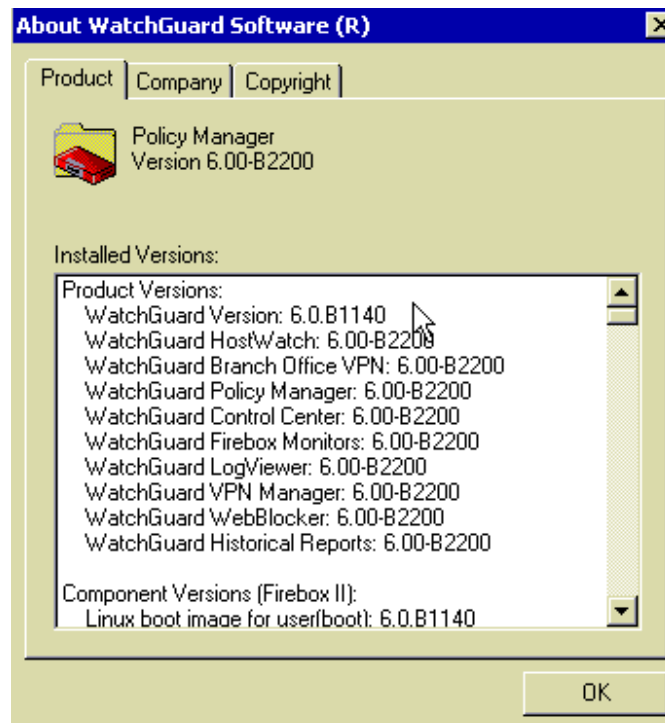
Figure 24 – Watchguard Software Version

2.7.1   System Logging Enabled

Results:

Objective – FAIL

Audit Type:

Observation

Evaluation:

When examining the system logging settings on the firewall device it was noted that there were some serious problems with the Watchguard device's configuration. This control notes that system logging should be enabled on the device and that the logging should be exported to another system log server device (syslog or similar) to protect the log files from possible compromise.

However, when examining the location of the logs it was determined that not only were the logs not being sent to an external server, but they were not being saved onto the management station either. Only logs in the current buffer that were being displayed in the current traffic monitor session were available to the system administrators. The following screen capture notes first the common location for log files on the management station (notice note are listed):
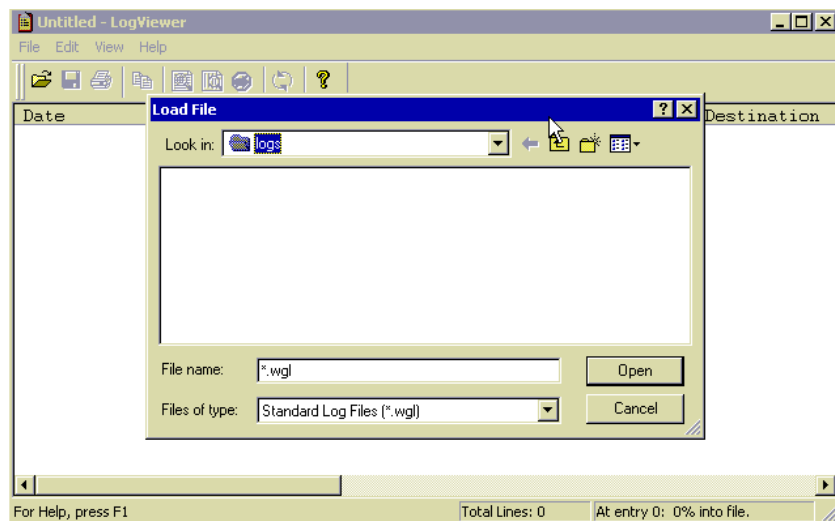
Figure 25 – Watchguard Log Viewer

To follow up on this test a search of the management workstation's file system was done, looking for files ending in the extension of *.wgl (default MIME type for Watchguard log files). As can be noted in the search box below, no files of this type were found on the management workstation.
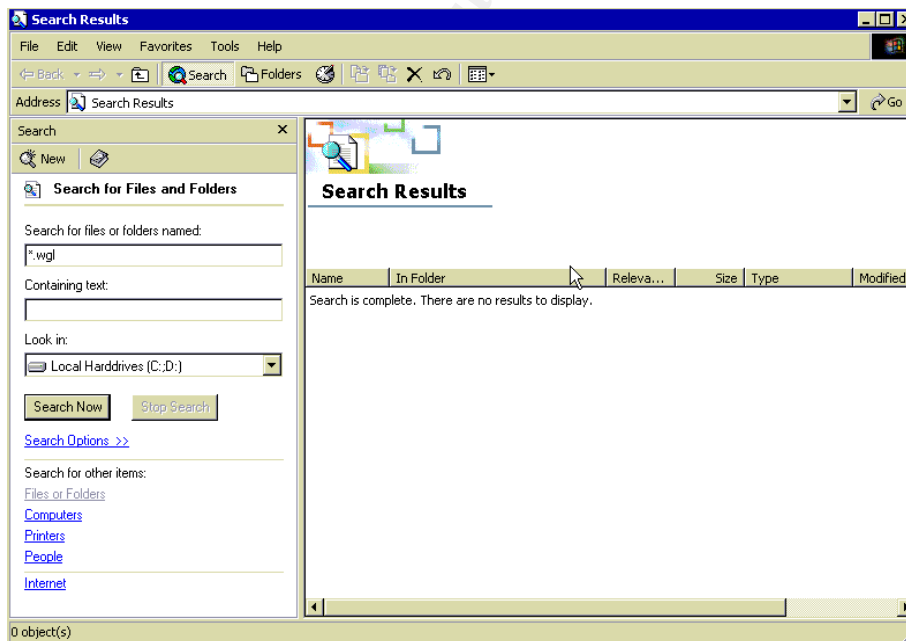

Figure 26 – Search for Watchguard Log Files

Finally to determine whether or not a syslog or similar server was being used to store the log files instead of the management workstation, the following configuration was noted, which shows that no external system logging server was being utilized.
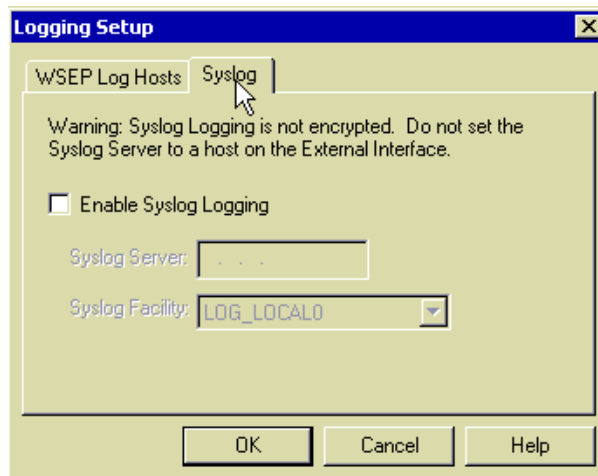
Figure 27 – Watchguard Logging Setup Configuration

When approached on this issue the administrators said that they were not aware that the log files were not being stored anywhere on the network, but that even if they were being stored due to time limitations they had never taken the time to view old log files. They occasionally viewed the traffic monitor, but it seemed this was done more for curiosity sake than to seriously or to regularly monitor the system's log for problems. As a result of these configuration settings this control was noted as a fail.

3.2   Residual Risk Measured

After completing the audit checklist as described above, there still remained residual risks to the organization's network environment, as would be expected. The scope of this audit was only comprised of the perimeter Watchguard Firebox 700 firewall device, although there were many other systems at this organization, perimeter devices included, which could easily have been included in the scope of a thorough audit of the environment. As can be noted from the diagram of this network (see figure 1), there were many other devices operating in and around the network's perimeter which all could also pose potential risks to the organization.

When examining the firewall system itself there were not many topics left uncovered during the course of the audit, although there are other features which could be examined if they were enabled in the organization. For example this company had only one main office with no traveling users requiring remote access to the environment. Therefore the virtual private network (VPN) features both for branch offices and mobile users were not included as a part of the scope of this audit. Nor was the proprietary Watchguard Dynamic VPN Control Protocol (DVCP) included as a part of this audit since this feature is only used to connect branch offices via VPN tunnels, and this company had no branch offices.

As would be expected, there were still multiple risks left un-addressed by the scope of this audit. Two of the primary concerns in this particular environment are the Microsoft IIS web server running in the company's DMZ and the Microsoft Exchange server that is located within the internal trusted network. No tests were performed against these systems during the course of this audit, as defined by the scope, yet serious concerns were raised with the organization regarding the configuration and maintenance of these devices.

Also located on the perimeter of this network was a Cisco 2500 series router that was originally implemented prior to the release of the SNMP vulnerability released in early 2002. However the device is wholly managed by the organization's ISP and the IT administrator responsible for the perimeter did not have access to the system. Therefore this device was also not included in the scope of this audit, however there are many possible concerns referencing this device. These include, but are not limited to the SNMP vulnerability, properly configured access control lists (ACLs), and utilization of proper authentication. This device forwards all external traffic to the internal firewall device for filtering decisions and the focus of this audit did not include the device.

Again the purpose of this audit was to determine whether or not the Watchguard device was configured appropriately and that it did not allow inappropriate access to internal systems. As was noted earlier an outsourced company was responsible for the implementation of the device and shortly after its

implementation the outsourced IT provider fell from favor in the eyes of the organization's administration. Therefore this limited audit was conducted to assure that only appropriate individuals had access to internal systems and that the Watchguard device was indeed configured properly.

Although it was not listed in the scope of this audit, it was discussed with the organization's management the issue of possible vulnerabilities at the network's perimeter, specifically considering the Microsoft IIS and Exchange servers open to the external world. It was decided that at a later date an additional audit would be performed on these systems as they had run out of funding for this particular project. At the conclusion of this audit the security level of these perimeter devices was noted as a concern to management and it appears that they will be examining the issue in more depth shortly.

3.3   Audit Evaluation

In evaluating the audit conducted the major concern faced by this auditor were the claims concerning the system's response to malformed packets or to any form of denial of service (DOS) attack against the network, although the Watchguard device does support features that supposedly protect against both. Due to the nature of the business and their constant reliance on the Internet connection it was not felt that tests such as these would be appropriate. The organization even utilizes the connection during off peak hours, which ruled out early morning testing. The company did not own another device that could be used as a spare system should tests such as these break the functionality of the primary system.

Also, most importantly, since this type of firewall's only mechanism for protecting against an attack is the software itself, not configurations, it was felt that even if a vulnerability was discovered, the most the company could do would be to request a firmware update. Although tests could have been performed using tools such as Trinoo or others, it was felt that for the purposes of this audit, those features would not be appropriate to test. For these reasons malformed packets and DOS type vulnerabilities were not used during testing.

Another major difficulty in attempting to audit the Watchguard device in this particular environment was the lack of proper documentation. When attempting to evaluate some of the aspects of the environment it was impossible to properly conduct that phase of the audit due to the fact that there wasn't a definitive baseline established before the audit to compare the audited results with. For example, it was impossible to determine whether or not the firewall ruleset was the same as the documented ruleset since there wasn't any original documentation to compare the current configuration with. This was true with many of the subjective administrative controls, considering many of these controls were not properly documented by the organization.

Overall the major goal of the audit was felt to have been accomplished, verifying the configuration after the parting of the outsourced IT firm who initially installed the system. Even though not every control was given a passing score during the audit, the majority of the controls noted in the audit checklist were able to be tested during the course of the review.

Assignment 4 – Sample Audit Report

4.0 Executive Summary

In examining the organization's firewall, the prime purpose of this audit was to ascertain the security level of the device now that Security Consulting, Inc. (fictitious name) is no longer managing the device and Local Media, Inc. (fictitious name) has taken ultimate responsibility for the device. In examining the portion of the organization's network that is exposed to the Internet there were many aspects of the device's configuration that could have been considered, however this audit's purpose focused it on the Watchguard Firebox 700 that is serving as the company's firewall.

In examining the firewall many aspects were considered when evaluating the device, the following are the major types of controls considered during the course of the audit:

- Administrative Security Controls
- Physical Layer Controls
- Network Layer Controls
- Transport Layer Controls
- Application Layer Controls
- Firewall Operating System Security Controls
- Firewall Maintenance Controls

During the course of the review it was found that no "backdoor" controls were left over by Security Consulting, Inc. that would allow them access to the internal network now that their contract of service has ended. Even though there should be no major concerns to this company re-accessing the network, there are other security concerns that should not be taken lightly. Each of these concerns represents a potential security vulnerability that could endanger Local Media's assets and should be addressed as soon as it is feasible.

Finally it should be noted that this audit covered only the network's firewall and thus only a portion of the network which is vulnerable to attacks from the Internet. Specifically the company should consider evaluating other network perimeter devices such as the Cisco 2500 series router, the Microsoft Internet Information Services (IIS) server which hosts the company's website, and the Microsoft Exchange Server which handles all of the company's e-mail. Each of these devices could have potential vulnerabilities that could affect the company as much, if not more, than having vulnerabilities on the firewall.

4.1 Audit Findings & Associated Risks

During this evaluation there were many positive and negative aspects of the device noted. The following are a sample of the major concerns that should be addressed by the organization in order to increase the level of security of the firewall device. The company needs to consider:

1.   Securing the management computer used to configure the firewall device.

When examining the location of the computer used to manage the firewall it was noticed that it was located in an unsecured area where multiple people had access to the device throughout the day. This is especially concerning considering the fact that there are employees at the facility twenty-four hours a day, often unsupervised by IT managers or administrators. It was also noticed that the computer's screen was open and accessible to anyone, even without a password (see figure 2). Both of these concerns could potentially allow someone access to reconfigure the firewall without authorization, thus causing a risk to the organization.

2.   Re-configuring the network IP blocked sites list to include only necessary sites that should legitimately be connecting to the company's internal resources.

It was noticed when testing to see if any IP addresses were being blocked from the outside the organization that only two of the necessary three lists of addresses were blocked from this list (see figure 3). These addresses are often used by individuals attempting to spoof or hide their real identity when connecting to the network, usually for malicious purposes. When someone attempts to hide their identity during a network attack they will often use one of these three address ranges. It should also be noted that these address ranges are never legitimately used on the Internet. Therefore this setting should be reconfigured to block anyone attempting to access the network in this way.

3.   Documenting the firewall rules that define what type of network traffic is allowed into or out of the network firewall.

When examining the firewall's documentation it was noticed that the company had possession of the original product documents, user guides, etc., however there was no documentation found on how the device was actually setup. Local Media, Inc. spent a good deal of money to hire an outside firm to setup and configure this device for them. However in the event on an emergency there would be no way to accurately know how to re-configure the device to its current state. Also due to this lack of documentation it is impossible to know what configuration settings have been approved by management and which have not. This leaves the firewall vulnerable to someone adding a rule to it without approval and jeopardizing the security of the internal network.

4.   Configuring outbound proxying of all internal requests to view web pages.

One of the abilities the firewall device has is to intercept all outbound requests from the internal network to the Internet and record, protect, and restrict which websites people visit. This process can not only improve employee productivity by limiting unnecessary usage of the Internet, but it can also help to protect the company's internal electronic assets. There are many types of viruses and malicious bits of programming code which can be launched through a visit to a malicious website. By turning on this feature some of this negative exposure can be limited, and employees can be restricted as to what types of websites are viewed. This can help the human resources department to promote a healthy work environment free of possible hostile sites. It was noticed during the audit that these features were not properly enabled on the firewall device (see figure 15).

5.   Enabling firewall authentication in order to restrict and track outbound network connections.

Along with restricting and recording what types of websites are viewed in the organization, the firewall device can limit and control access to outside resources based on who is attempting to access the site. This allows those requiring access to the Internet for research purposes to freely visit appropriate sites for their position, while others who don't require access to the Internet can be blocked from such sites. This is done by providing user credentials to the system before being allowed to surf the Internet. When auditing the device it was noticed that this feature had not been enabled on the device (see figure 17), thus allowing anyone full access to all Internet resources at all times of the day. This is especially important due to management's concern over the potential misuse of the Internet during off-peak hours when many are working in the building unmonitored.

6.   Updating the software version on the firebox system to the latest version of the software.

It was also observed when auditing the system that the firewall device does not have the most recent version of the Watchguard Firebox software installed on the system (see figure 19). This is important to consider when one remembers the purpose of such software updates. New software for devices like this typically do not introduce new features or abilities to the firewall, but rather fix potential vulnerabilities or problems with the system. Therefore it is vital that the software version stays updated on this type of system.

7.   Enabling logging of all system events to an internal server which will store and record system events from the firewall.

Most concerning when auditing the firewall device was the lack of system event logging configured on the device (see figures 22 and 23). Whenever malicious network traffic, inappropriate use of the system, or system errors happen these events are typically logged to a server somewhere in the network. These logs can be used to analyze potential attacks against the network, troubleshoot device failures, or record inappropriate system use. It is therefore vital that these logs not only be saved, but also saved on a protected internal system. As was stated before, these logs are not being saved at all on any server in the organization, and thus the system should be reconfigured to save these events to an internal device that can be free from external tampering.

It should also be noted that many positive things were noticed during the audit process. These settings are not noted in this report, but should not go unmentioned. The original administrators of this system enabled many of the settings necessary for securing the network. Unfortunately there are still other settings that must be enabled in order to properly protect the company's resources.

4.2   Audit Recommendations

As a result of the above-mentioned findings in the audit and their associated risks, certain steps should be taken in order to protect the network against potential threats from outside of the network. Each of the following recommendations will correspond with the respective audit finding and associated risk noted above. Again, it should be remembered that these recommendations are only to secure the perimeter firewall device, and do not cover associated risk concerning the other perimeter devices such as the Cisco router, Microsoft IIS server, and Microsoft Exchange server.

As a result of the audit findings, it is recommended that Local Media, Inc. take the following steps to help protect their network:

1.   Implement additional physical security controls around the location of the firewall and all associated networking equipment. There are already door locks on all entrances to this area, however, as noted, one of these locks is rarely used, allowing people access throughout the day. A control or process should be put in place to further limit access to this area, and if possible, a way to track who gains access to this area should be implemented as well.

2.   The company's firewall administrator should determine a list of legitimate external users of the company's website and e-mail with the help of the company's management. This list of potential users should be used to restrict external access to the company's network based on IP address, thus denying illegitimate users of access to internal resources.

3.   IT staff need to take the time to document the policies and procedures related to the administration of the company's network resources, including the firewall. Although when observing the staff it was noted that they have many responsibilities already, by implementing proper administrative controls such as these, they can help to prevent unnecessary threats to the organization, both internally and externally.

4.   Noting both the lack of outbound website proxying and desktop software to help protect users when surfing the Internet, the company should implement controls to help protect the internal network by restricting the type of sites viewable to internal users (ie. ActiveX controls, JavaScript, etc.). There are many ways to implement these controls, the firewall configuration being one of the ways to accomplish this.

5.   It should also be determined who, for business reasons, needs access to external Internet resources for any purpose. As a result of this determination appropriate levels of user authentication should be enabled through the firewall device for users with needs to access external resources. Firewall authentication should be considered as a prime control to help protect these resources.

6.   The company should also consider implementing a policy for maintaining the software levels of its equipment and a way to follow through to see that they have been done. IT staff should develop a plan for how it's most likely that they will make the effort to update their software. This should be considered not only for the firewall device, but for all other systems within the organization.

7.   A standard for maintaining and analyzing log files should be setup within the organization. Due to the lack of log files found for the firewall device it is safe to assume that there are other systems where logging is not being performed or managed properly. The company should again invest the time to set policies and procedures for how logging is going to be performed. Most importantly, however is that a process be instituted for reviewing these logs to maintain a higher level of network security.

4.3   Costs

When examining the possible improvements that should be considered to increase the level of security in this organization, the cost to make these improvements is negligible. When considering the possible costs there are multiple factors to consider – financial resources, time, and manpower. When looking at the various improvements suggested as a part of this audit the majority of the resources required will be in time and manpower. Only the first recommendation concerning physical control of the network equipment could possibly incur capital expenditures by the organization.

As in many organizations, to properly secure the organization, an appropriate level of time and manpower resources should be invested. The company already possesses all of the technology equipment necessary to properly lock down their site. In this case it is a matter of implementing the recommendations of the audit and empowering the IT staff to continue to stay current with system configurations and maintenance that will help to ensure the long-term security of this facility.

The following is a table that outlines specifically what resources the company should expect to utilize in order to secure each of the above-mentioned items:

Security Control:	Financial Cost to Implement:	Man-hour Cost to Implement:
1. Implement stronger physical security around network equipment.	$100 – To purchase an additional door lock to the network equipment area and duplicate keys for those people with legitimate needs to access the area.	1 hour – to purchase additional door lock. 1 hour – to install additional door lock. 1 hour – to distribute keys to appropriate employees.
2. Block inappropriate outside users of the web and e-mail servers.	$0 – The equipment is already available.	3 hours – to research which IPs to block. 1 hour – to implement blocked external IPs.
3. Document the network environment, including Watchguard firewall.	$0 – The equipment is already available.	4 hours – to fully map the network environment, including the perimeter. 3 hours – to document Watchguard firewall configuration.
4. Implement website proxying to protect internal employee computers.	$0 – The equipment is already available.	1 hour – to configure Watchguard HTTP proxy. 2 hours – to configure client workstations to utilize HTTP proxy.
5. Only allow certain employees unlimited Internet access.	$0 – The equipment is already available.	1 hour – to configure Watchguard HTTP authentication. 2 hours – to configure client workstations to utilize Watchguard authentication. 4 hours – to train employees (4 groups, 1 hour each) on how to use the authentication applet.

105

6. Install current software updates and patch levels.	$0 – The equipment is already available.	1 hour – to download and install the software.
7. Setup a log file record and review program.	$0 – If the company uses existing hardware (such as the management station or DC2 to log system messages. $1500-$2000 – If the company decides to purchase a dedicated server to record these files.	2 hours – to install and configure internal syslog server (5 hours if utilizing dedicated system). 1 hour – to configure the Watchguard firewall to utilize the syslog server.

4.4   Compensating Controls

Although the goals of the organization's security policy should be to attempt to secure their electronic assets, this particular company's policy should not be to attempt to achieve 100% security. To due the nature of the business, the cost to secure these resources at that level would be more than is justified by the company's business model. However, as noted before, there are many steps that the company can take to help protect the resources at the perimeter of their network with minimal financial drain on the company.

After examining the overall network and perimeter concerns, there are certain steps which are recommended to be implement first due to their importance and low requirements in financial and manpower resources.

1.   A policy should be put into place requiring the use of the locks on the entrance to the room holding the network equipment. These doors should remain locked, especially during off-peak hours, and keys given to the limited number of individuals requiring access to the facility.
2.   The IP address range 192.168.0.0/24 should be added to the firewall device's blocked site list to restrict external traffic.
3.   The firewall administrator should document the current port forwarding by the firewall in the case of equipment failure.
4.   In the configuration settings for the firewall device's HTTP proxy, the WebBlocker feature should be enabled with the default settings that will provide a cautious level of outbound protection for Internet users.
5.   The latest version of the software firmware should be obtained from the Watchguard website (http://www.watchguard.com) and installed on the system.
6.   System event logging should be enabled on the Watchguard device until another internal server can be configured to hold those log files more securely.

106

Throughout the entire process of auditing and attempting to secure the perimeter of the organization's network it should be remembered that the firewall is but one piece of the overall security of the organization. Even at the company's perimeter there are other potential risks that could cause damage to their electronic assets. Auditing and securing the firewall is a wonderful first step, but should not be secured at the expense of ignoring the other possible threats. Continued monitoring and audits of these network devices will also ultimately contribute to the long-term security of the network.

Also, since network address translation (NAT) is being utilized on the firewall device along with stateful packet inspection, the only machines in the company that face considerable risk from outside attacks are the company's web and e-mail servers. Therefore, in order to further secure the perimeter of the network, particular attention should be given to hardening these two servers against attacks. While there are many things that could be considered when securing these devices, there are a few which should be considered primarily:

- Operating system version and patch levels on the servers
- Host-based firewalls could be installed on each of the servers
- Un-necessary services disabled on each machine
- Strong passwords utilized for accounts on each system

There are many other compensating controls that could be used on these systems, however since these systems were not in the scope of this audit, they were examined with only cursory attention.

5.0   Conclusion

When all is said and done, the ultimate goal of the security audit in most facilities should be to increase the current state of information security, raising it to the next level. While in some environments (military, etc) it is inappropriate for there to be a security breach of any kind, most environments should look at the security audit as an opportunity to improve their security stance and not necessarily to fully lock down the environment.

That being said, the security auditor of this firewall device should view the audit as an opportunity to work along-side of the system administrators to increase the level of perimeter security. This means that the auditor should not use the above checklist as a club to hold over the head of the administrator, but rather as a point of encouragement, to give the organization goals and realistic ways the environment can be further secured. The auditor should therefore approach this project with a spirit of cooperativeness and helpfulness to assist the organization in meeting their security goals.

Finally it should be remembered that the firewall is but one part of an overall security program. Simply because an organization follows and implements all of the above points does not mean that the organization's systems have been secured. The firewall is but one piece in an overall puzzle to secure the entire networked environment. However, by following the above checklist, one can sleep easier knowing that at least one portion of the environment is moving towards a secure state of operations.

References

Defense-in-Depth Firewalling Basics Student Guide. Version 1.4 Watchguard Technologies, Inc., 2001.

Defense in Depth Virtual Private Networking Course Guide. Version 1.2. Watchguard Technologies, Inc., 2001.

"iAppliance Web – Appliance Review." URL: http://www.iapplianceweb.com/appReview/IAW_SECURITY_APPLIANCES/7 (November 1, 2002)

"ICAT Metabase: A CVE Based Vulnerability Database." URL: http://icat.nist.gov/icat.cfm (April 22, 2003)

Incident Handling: Step-by-Step and Computer Crime Investigation (4.1). The SANS Institute. 2002.

Perimeter Protection Defense-in-Depth (2.3). Version 2.2. The SANS Institute, 2002.

Perimeter Protection Firewall Technology (2.2). Version 2.2. The SANS Institute, 2002.

"SecurityFocus HOME Mailing List: Bugtraq." June 28, 2001. URL: http://online.securityfocus.com/archive/1/194076 (November 1, 2002)

"SecurityFocus HOME Mailing List: Bugtraq." July 9, 2002. URL: http://online.securityfocus.com/archive/1/281218 (November 1, 2002)

"Watchguard Bundles VPN Devices with McAfee Tools." November 12, 2001. URL: http://www.nwfusion.com/news/2001/1112watchguard.html (November 1, 2002).

"Watchguard Firebox System Firebox III Hardware Guide." 2003. URL: http://help.watchguard.com/docs/FBIII700500HardwareGuide.pdf (March 23, 2003).

"Watchguard Firebox System High Availability Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62HighAvailabilityGuide.pdf (March 23, 2003).

"Watchguard Firebox System Reference Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62ReferenceGuide.pdf (March 23, 2003).

"Watchguard Firebox System User Guide Firebox System 6.2." 2003. URL: http://help.watchguard.com/docs/v62UserGuide.pdf (March 23, 2003).

Fithen, William and Allen, Julia and Stoner, Ed. Deploying Firewalls. Carnegie Mellon Software Engineering Institute: Philadelphia, PA. 1999.

Harris, Shon. All-in-One CISSP Certification Exam Guide. Berkely, CA: McGraw-Hill / Osborne . 2002.

Hill, Mark. "Audit and Control Checklist for the Elron Internet Manager (IM) Firewall: An Auditor's Perspective." February 2002. URL: http://rr.sans.org (November 1, 2002)

Hoelzer, David. Auditing Principles and Concepts (7.1). Version 1.1a. The SANS Institute, 2002.

Naidu, Krishni. "S.C.O.R.E. Firewall Checklist." URL: http://www.score.org (November 1, 2002).

Northcutt, Stephen. Auditing the Perimeter (7.2). The SANS Institute, 2002.

Northcutt, Stephen. Inside Network Perimeter Security. Boston: New Riders Publishing. 2001.

Sonnenreich, Wes and Yates, Tom. Building Linux and OpenBSD Firewalls. Wiley Computer Publishing: New York, NY. 2000.

Tipton, Harold and Krause, Micki. Information Security Management Handbook. Auerbach Publications: New York, NY. 1999.

Tu, James. "Auditing a Nokia 440 Check Point Firewall-1 Firewall: An Auditor's Perspective." June 2002. URL: http://rr.sans.org (November 1, 2002).

Tudor, Jan. Information Security Architecture. Auerbach Publications: New York, NY. 2001.