Global Information Assurance Certification Paper

EXTERNAL AUDIT OF A NETWORK SEGMENT'S PERIMETER FIREWALL:

An Independent Auditor's perspective

GIAC System and Network Auditor (GSNA) Practical Assignment v2.1

Robert Dooling
May 2003

Table of Contents

Introduction

This document is the report for an external firewall audit performed on the firewall placed in front of the screened e-mail network segment at XYZ, Inc., in partial fulfillment of the requirements for the GIAC Systems and Network Auditor (GSNA) certification. The audit fieldwork was performed between March 7 and April 4, 2003.

The report consists of four assignments, several appendices, and references, as listed in the Table of Contents.

Research in Audit, Measurement, and Control

This is an audit of a network segment's perimeter firewall – risks to the network segment from other sources are considered; however, the focus of the audit fieldwork and this report is a single system that provides the main protection for this network.

Audited System:

The system under audit is a Check Point VPN-1 Pro integrated firewall / VPN (Virtual Private Network) device. The firewall specifications are defined in the table below:

System	Check Point VPN-1 Pro Firewall / VPN
Version	4.1 SP5 (Build #41510)
OS	NT 4.0 SP6

This device provides protection through packet filtering for several (four) e-mail servers located in a screened network segment, as well as numerous PCs and servers located on the internal network segments.
The Check Point VPN-1 device provides dynamic (stateful) packet filtering. The VPN-1 also provides secure connections for remote users to access their e-mail in a host/network VPN configuration. NAT (Network Address Translation) is provided for traffic communicating with Internal PCs and servers to use private IP addresses, thus preventing exposure of internal addressing schemes to outsiders. The e-mail servers are statically mapped to public IP addresses, and therefore do not require NAT. A border router exists between the firewall and the Internet connection, providing an additional layer of defense.
These publicly-accessible e-mail servers are important to XYZ Inc.'s business, as they provide remote e-mail access to traveling employees, thereby reducing geographical boundaries to communication and information sharing. Over half (~60) of XYZ's full time employees travel away from their home office location for approximately 40 weeks per year.
The router and firewall combination architecture provides 'defense in depth', whereby the difficulty of breaking into the network is increased due to the additional number of devices providing perimeter protection which would have to be defeated.
A typical implementation of this setup would have the router filtering to a limited extent, and permitting all other traffic to pass through, and the firewall providing additional, more restrictive (and stateful) filtering, completed with a 'deny all undefined traffic rule.' This configuration allows the router and firewall to each concentrate their resources on what they do best: "use the router to filter out all absolutes (and focus on routing), and let the firewall take care of everything else (stateful filtering, etc.)." [1]
The VPN-1 in this environment provides filtering, VPN authentication, NAT, and Denial of Service (DoS) protection; this device performs no virus scanning or URL filtering. Virus scanning is performed by a separate system, and is outside of the scope of this

[1] Collaborative. Auditing the Perimeter. SANS Institute: 2002.

audit. VPN process configuration, encryption, and security controls are a separate topic from firewall protection; and will only be reviewed as pertaining to the VPN-1 device itself and the corresponding rules in the ACL. Web access is not available through this firewall; therefore URL and web content filtering is also out of scope.
The Check Point system resides in a network environment that is roughly depicted in the following section, “Risk to the System.”

Risk to the System:

This device restricts access to e-mail servers containing potentially sensitive data in the screened segment, as well as systems on an internal network. Remote users establish VPN connections through this device to gain access to the organization's data. E-mail communications are utilized by remote workers for order submissions, inventory updates and tracking, and financial processing information, in addition to the more mundane daily, administrative purposes.

The risks presented by this arrangement include illegitimate access to the e-mail servers, unauthorized access to the internal networks, illegitimate VPN connections to the e-mail servers, and the potential for DoS attacks which could effectively shut down the organization's e-mail function.

Malicious attackers who gain access to the e-mail servers could gather sensitive customer data, install backdoor trojan software to advance further attacks unnoticed, or entirely erase the server data.

Because the e-mail servers reside in a screened segment, intruders who gain access to these systems would be effectively cordoned off from accessing other, internal systems. However, if an attacker has been able to find an exploitable flaw to gain access to the screened segment, the potential exists that this same flaw, or a different one, could be exploited to gain access further into the internal networks.

Sensitive customer data could be used to blackmail the organization, to gain competitive advantage through espionage, to advance identity theft schemes, or in any number of other malevolent activities.

Backdoor software could be installed, remaining undetected for long periods of time while harvesting and transmitting critical information such as customer data, login credentials, and sensitive internal communications. Upon discovery of a trojan horse program, the integrity of all system data can no longer be trusted, from the date of the last known 'clean' backup.

Security can be compromised despite laudable firewall practices if internal controls (procedural or technical) are ineffective, or break down. Therefore, it is critical to ensure that policies and procedures in place are communicated, enforceable, and updated to reflect changes to the organization's environment. Technical security controls must be closely monitored, be subject to change control policies, and ensured to be resilient and reliable.

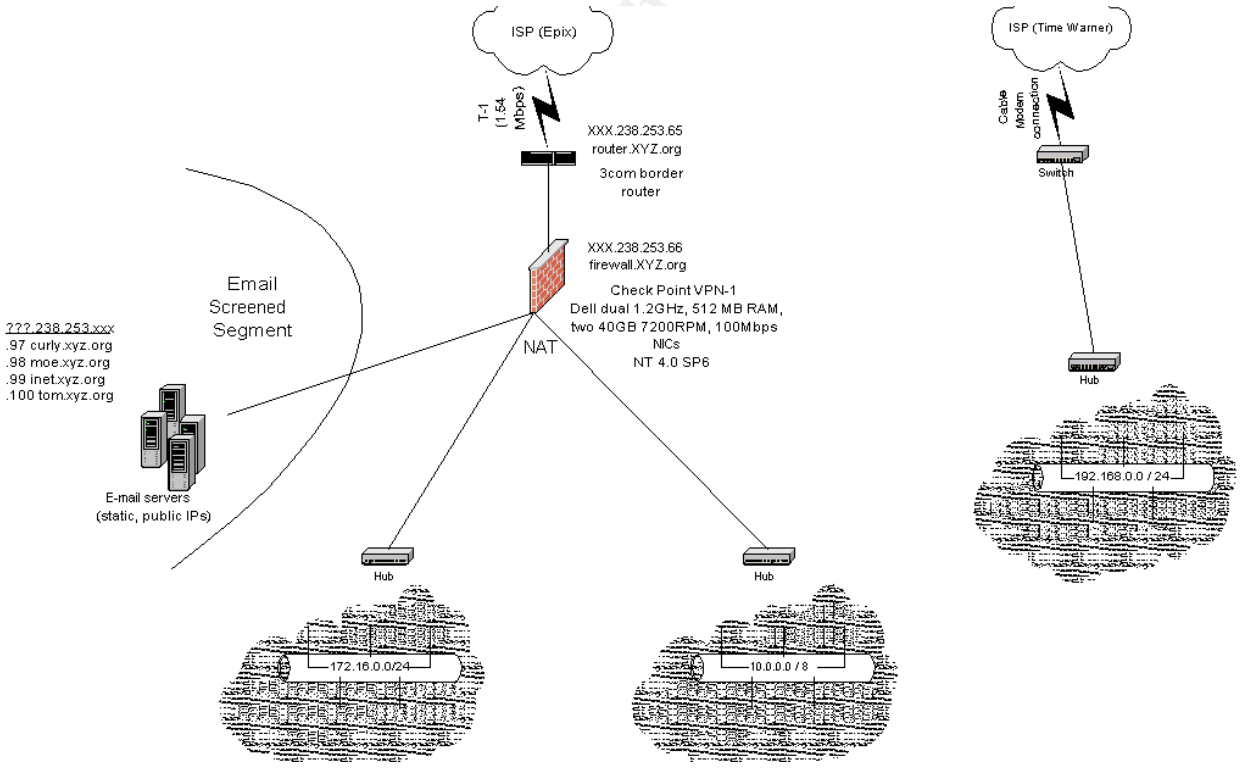
The consequences of e-mail server data erasure can range from minimal annoyance to devastation, depending on the backup policies and practices.

Due to a limited IT budget within the organization, money and resources to perform formal system audits are scarce. This firewall was identified as the top priority for auditing for several reasons: this firewall provides the main filtering activities for the systems that are considered most critical to business sales, communications, and continuity. It is also the final layer of security for these systems in the 'defense in depth' scheme. No other single system within XYZ's network is relied upon to provide as critical security protection, or whose failure would be as significant, as this firewall. Because this firewall is in the principal position of providing security for crucial data, the risk of compromise or failure of this system is of the utmost concern. For these and

other reasons, evaluating this system initially, as the most critical defense point, takes precedence over other systems in the organization. This audit can be used as a guideline for conducting further system audits, in descending order of criticality.

The logical flow of data through this device includes information of all three sensitivity classes: critical information (e.g., customer credit card information), operational information (e.g., order numbers, inventory data), and management and configuration information (e.g., time and expense reports, human resources files). The value of these kinds of data is difficult to quantify without extensive studying of sample files, which falls outside of the scope of this audit. However, according to the CIO, it is a safe approximation that roughly 50-75% of revenue generated for XYZ Inc. depends on information transferred between these email servers, to some degree. This estimate clearly justifies the importance of securing these systems.
One of the most preliminary and basic steps in securing these systems involves designing and implementing an appropriate architecture tailored to support the security policy and needs of these systems.

The screened e-mail network segment is comprised of a Border Router plus Firewall / VPN combination architecture, as depicted below:



This layout has the following characteristics [2]:

[2] Ibid.

- moderate cost
- difficult to audit
- moderate security:
  - resistant to DoS
  - moderately resistant to penetration
  - problem of ‘VPN piggybacking’: uncertainty regarding VPN-connected remote users’ additional network connections

The following table defines general risks – risks identified prior to commencement of audit fieldwork, without detailed knowledge of network architecture or existing security controls in place. These risks could apply to any organization conducting similar business, with similar architecture and information processing needs:

Vulnerability	**Threat / Likelihood** *Low / Moderate / High*	**Risk** *Low / Moderate / Significant / High*	**Consequences**
Inadequate access controls allow unauthorized users to access and control perimeter security devices.	Moderate / High: Studies show that a high percentage of perimeter security devices retain the manufacturers' default (public knowledge) administrative username and/or password, or easily guessed parameters.	**High**: An attacker who compromises a perimeter security device theoretically can cause unlimited damage, from simply erasing the rulebase, to making small and potentially unnoticeable changes for future attacks, to installing backdoor / sniffing software to gather further system access credentials sensitive information.	Connectivity downtime, time and financial cost of repair, recovery, and forensics efforts, unavailability of critical information, potential loss of confidentiality and integrity of information (if it can't be determined whether information has been tainted, it must be assumed to be so).
Inadequate preventative controls or corrective measures against Denial of Service (DoS) attacks.	Moderate: The entire XYZ environment includes two separate Internet connections (different ISPs), which could potentially allow for re-routing of all traffic through one, if necessary. Additionally, the screened segment is protected by two layers of security devices. The ISPs may have controls in place to help reduce the frequency or effectiveness of these attacks as well. However, DoS attacks remain among the easiest and effective, and therefore most	**Low / Moderate** (*depending on the timing and duration of outage*): Temporarily blocked email access would considerably impair day-to-day operations, but not the long-term livelihood of the organization.	e-mail access is important for traveling employees; unavailability of information and access to resources, customer dissatisfaction due to employees not being able to perform their work.

	popular forms of inflicting damage due to a plethora of automated tools.		
Inadequate system controls lead to security breach / leak of non-customer related internal data.	Moderate: Attackers are often able to find sensitive information that has been inadvertently made accessible. Insiders may also leak sensitive information via e-mail, intentionally or inadvertently.	**Moderate**: Negative public exposure and degraded reputation would be minimal but could undermine confidence in the organization's handling and securing information. Depending on the level of sensitivity of the leaked information (e.g., 1-3: critical, operational, management and configuration) and value of the information, the risk of such a leak varies widely.	Loss of confidentiality of internal information, loss of customer confidence.
Inadequate system controls lead to security breach / leak of customer-related internal data.	Moderate: Attackers are often able to find sensitive information that has been inadvertently made accessible. Insiders may also leak sensitive information via e-mail, intentionally or inadvertently.	**High**: Negative public exposure, degraded reputation, and lack of customer confidence could be substantial.	Loss of confidentiality of internal customer information, loss of customer confidence, reduction of customer base, potential litigation.
Incorrect or misconfigured ACL allows unauthorized / malicious traffic into the network.	Moderate / High: ACLs can often become overly complex and confusing over time, especially in organizations with high turnover of administrators. This makes the possibility of an extraneous rule, misconfigured source / destination, incorrect placement (ordering) of rule very feasible, especially in the absence of regular auditing.	**Significant**: Depending on the nature of the breach, attacker effects could run the gamut: malicious code to infect / crash systems, network enumeration, backdoor / sniffer installation for further infliction, etc.	Possible loss of confidentiality, data integrity and availability, recovery costs. The magnitude of these consequences and recovery costs depend largely on if /

			how quickly the breach is detected.
Unidentified / unsecured connection points bypassing the perimeter protection allow unrestricted access to / transfer of data out of the internal network.	High: The proliferation of cheap and simple Wireless Access Points (WAPs), Personal Digital Assistants (PDAs), and laptops, in addition to often poorly documented modem usage makes the potential for connection into, and/or data transfer out of the internal network quite possible. In addition, even legitimate users connected remotely through the VPN pose threats because of the unknown factor of their other connections and systems security (i.e., an unaware remote user's laptop may contain trojan / keystroke logging software). This is a two-sided threat in that these systems pose a threat to the network based on the possibility that they contain and may introduce malicious software into the environment, and can be easily used to transfer sensitive outside of the scope of restrictions (inadvertently or intentionally). Because of the difficulty in restricting and tracking the access and data transfer activities of such systems, organizations must rely strongly on user education and policies to control these threats and prevent intrusions / data leaks. Unfortunately, these two areas are often neglected or poorly addressed by many organizations' Information Technology (IT) departments.	**High**: The introduction of unknown systems and access to the network poses innumerable risks to the environment, spanning the entire range of risks due to unauthorized access and loss of information.	Loss of confidentiality and data integrity, damage to systems requiring recovery costs.

Current State of Practice:

Several good resources were identified to help with planning efforts, and provide focus to the audit. Sample audit checklists for other Check Point devices, of varying usefulness, were reviewed. Helpful information was located mainly through:

- Internet searches:
  - google: Check Point audit steps,
  - google: Check Point firewall administration,
  - google: Check Point audit,
  - google: firewall audit,
  - google: network perimeter vulnerability assessment,
  - google: firewall policy best practices,
  - google: firewall rulebase develop,
  - etc;
- the SANS online practical repository;
- SecurityFocus (http://www.securityfocus.com) searches:
  - Check Point VPN-1,
  - Firewall vulnerability,
  - etc;
- Personal library of information security-related books and articles (please see 'References' section); and
- the auditor's company intranet and network drives.

Numerous documents less specifically related to Check Point, referring to overall firewall auditing and best practices, were located through established information security-related websites, co-workers, and SANS seminar materials. Lastly, research was performed to locate guidance on conducting audits generally.
Resources that were integral in researching and developing this audit plan are included in the 'References' section.

Administrative Guidance:
The most beneficial list of steps for conducting an audit from an administrative standpoint was the "Six Step Audit Process", originally presented by David Hoelzer during the SANS conference, and documented in the Auditing Principles and Concepts publication. The six steps are:

1. Audit Planning
2. Entrance Conference
3. Fieldwork
4. Preparing the Report
5. Exit Conference
6. Report to Management

Although not all of these steps will be applicable in every single audit, this list (further broken into detailed steps in the listed reference) provides an excellent model for how

an audit should ideally be conducted. From defining scope, planning and scheduling, resources and responsibilities, professional attitude and integrity, client relationships, results presentation, etc., this process is the most practical and informative set of instructions that was identified for managing an audit from beginning to end.

General Technical Guidance:
The list of steps for conducting Vulnerability Assessments presented by John Green during the SANS conference was partially applicable and helpful from a technical perspective:

- Determine areas of responsibility
- Secure the perimeter
- Secure the DMZ
- Eliminate externally accessible vulnerabilities
- Eliminate internally accessible vulnerabilities
- Search for trojan horse programs [3]

Although not all of the steps listed above were necessary for this audit, this section provides a helpful overview of the actions to be taken in a thorough vulnerability assessment, and the reasoning behind each one.

Several sources were identified providing information on the kind of "blind" external vulnerability assessment that was to be conducted for XYZ, including:

- PriceWaterhouseCoopers' "Network Security Assessment" [4]
- Comm-Tract's IT Network Security Solutions: External Assessment Deliverables [5]
- NIST Special Publication 800-41 -- Guidelines on Firewalls and Firewall Policy

Check Point - Specific Technical / Procedural Audit Checklists:
Checklists are a helpful method to plan, execute, and document an audit, from both a technical and procedural standpoint. Checklists should also serve as reference for interested parties in the future.
Some aspects of firewall auditing are well-known and generally agreed-upon: any traffic which is not explicitly allowed should be denied (with some exceptions for "open" / research-oriented organizations), only allow outbound traffic with a source IP address from your address space (blocks spoofed packets), etc.
Other, more objective, standards are widely advocated, but often not followed:

> "When you make security more complex than it needs to be, you create vulnerability,[6]"

is a common sense fact about information security. In practice, however, many firewall rulebases become large and unwieldy over time, probably due in part to poor change management policies. Most firewall administrators would give little attention to this, considering it an unavoidable nuisance. What they might not realize, or choose to

[3] Green, John. Auditing Networks with Nmap and Other Tools. SANS Institute: 2002.
[4] http://www.issa-ct.org/Events/archive/2001/0109 Network Security Assess.ppt
[5] http://www.comm-tract.com/netsec.htm#securecheck
[6] David Hoelzer – SANS Network Security, Washington, D.C. – Track 7, Day Two: Auditing the Perimeter

ignore, is that this complexity exponentially increases the chance of an unnoticed loophole in the firewall.

Most of the checklists that were located through research were either too high-level, lacked a well-defined scope (covered tangential topics while missing items of critical importance), or were very outdated. I found this to be especially true of organizations' internal IT documents, which seemingly are passed from one year and one administrator to the next without any reality check, review, or update.
No single audit checklist was identified that included all of the steps the author deemed necessary to conduct a successful audit of XYZ, Inc.'s Check Point device. Due in large part to differences in organizational cultures and network structures, none of the checklists individually would be suitable. Therefore, the audit checklist utilized for this assignment is a compilation from the resources mentioned above, prior work experiences, co-workers' experiences, and the author's determinations based on the unique needs of XYZ, Inc..

Audit Checklist

Purpose > This checklist defines the scope of this external firewall audit by providing a list of twenty (20) audit steps, each assigned to one of eight categories, which, when combined, cover the most important aspects of firewall security for the XYZ organization. Performing, assessing and documenting the results of these steps will provide the basis for a report to be provided to management detailing the most pressing controls weaknesses and issues, and suggested steps for remediation, with the ultimate goal being to improve the protection provided to the e-mail screened network segment by this firewall.

The eight categories are:

- Firewall System (FW-),
- Underlying Operating System (OS-),
- Firewall Access Control List (ACL-),
- Firewall Configuration (CFG-),
- Firewall Administration (ADM-),
- Perimeter Access (PER-),
- Physical Security (PHYS-), and
- Policy and Procedural items (PP-).

Note > Scope determination discussions with XYZ management clearly identified a few specific requests and restrictions for this audit. Most importantly, management communicated that due to the relatively simple and homogenous nature of the screened segment (small number of systems, small number of applications / services), there was not great concern or interest in a thorough technical review of the firewall or surrounding systems. Rather, management was primarily concerned with what they perceived to be "sloppy" administration practices, lack of documentation, and general lack of procedural controls around the firewall. *Therefore, the objectives of this review are to focus primarily on procedural, as opposed to technical, issues surrounding the firewall.* Management expects the results of these procedural reviews to provide benefit across the organization, although only this network segment is to be audited. Technical issues are not to be ignored, of course, but less emphasis was placed on analyzing these items.

Additionally, management and Information Security (IS) personnel decided that the technical evaluations that would take place should do so with very little internal information provided to the auditor; in other words, the auditor should act as an uninformed outsider to perform reconnaissance, or "discover" the XYZ network, and enumerate and locate vulnerabilities as possible. This is primarily for two reasons: (1) internal (albeit informal) network security audits have been performed in the recent past, and (2) concerns for confidentiality and privacy of internal network information. *Therefore, this audit was performed almost entirely from outside of the XYZ Inc. network*, with very limited information provided to the auditor. In addition, IS personnel were concerned about service interruptions to the firewall, and requested that certain techniques such as throughput / load testing, DoS attacks, and vulnerability exploitation

be avoided. This made some typical network security audit steps unfeasible (e.g., network monitoring / sniffing, certain nessus plug-ins, and internal-to-external outbound scans), and made some audit testing steps less thorough than would be considered ideal. However, this approach was deemed acceptable, and actually preferable, to the management team who requested the audit.

Note > Descriptions in **bold text** indicate audit steps for which results are reported in Assignment 3.
Note > Only the primary reference(s) for each audit item are listed; other references may have provided similar information.

Firewall System Items

FW-1	
Description	Ensure that only the applications and services which are necessary and justifiable are installed / running on the firewall machine, and that access controls to these services are sufficient.
References	1, 6
Control Objective	Reduce the potential for vulnerabilities in the firewall by ensuring that no unnecessary services are running.
Risk	Threat: Superfluous services provide additional connection points and therefore potential conduits for unauthorized access, whether through software vulnerabilities or misconfiguration as a result of administration error. Likelihood: The likelihood of a vulnerability being exploited on a firewall is relatively high because, by nature, the firewall is externally accessible, and it provides an extremely enticing target due to the aforementioned authority they possess. Consequences: The consequences of a firewall system compromise are likely very high – ranging from Denial of Service (for a 'fail-close' firewall), to an intruder gleaning rulebase and configuration information or even modifying the rulebase for future use, to unrestricted access to everyone (in the case of a 'fail-open' firewall).
Compliance	The firewall will either be compliant or not – if each and every service running on the machine is necessary and justified by organizational need, the system passes. Otherwise, an exception is noted.
Testing	• Review of the Windows NT Services list (Automatic and Manual start services) for appropriateness Start – Programs – Administrative Tools -- Services • Review of the Check Point administrative console; • Scanning and network information utilities including: ▪ SuperScan (see options used and results at **Appendix B**), ▪ Nmap (see options used and results at **Appendix C**), ▪ Nessus (see options used and results at **Appendix D**), ▪ Firewalk (see options used and results at **Appendix E**), ▪ Netstat –anp (displays all active network connections and protocol statistics in numerical form, sorted by protocol; see information at **Appendix I**), and ▪ Fport /p – (displays all active network connections and the

	corresponding application and process ID, sorted by protocol; see information at **Appendix J**); • Discussion with firewall administrator(s), business owners, and appropriate Information Security and Information Technology management personnel for validation of services' justification
Objective / Subjective	Objective – the results of this step are repeatable and verifiable: services which are installed on the firewall can be definitively identified through operating system and firewall application review, various scanning techniques, and system command output. Determination of whether a service is necessary or not depends on the organization's justification, taking into account their unique needs.

FW-2	
Description	**Availability / Reliability of system.**
References	10, 17
Control Objective	Ensure that the system performs reliably and maintains high levels of availability; failover and redundancy measures should be in place to address system failures.
Risk	Threat: A firewall system that is not reliable or highly available may lead to failure (closed, resulting in DoS, or even worse, open, resulting in unrestricted access); reliability issues may lead to user dissatisfaction and/or attempts to subvert or circumvent the firewall. Likelihood: The likelihood of reliability issues will depend largely on other audit items, including change management (**PP-2**), operating system security (**OS-1**), and environmental controls (**PHYS-2**). Consequences: Lack of availability, unrestricted access, user dissatisfaction.
Compliance	Compliance in terms of reliability / availability should be measured as pass/fail, based on SLA specifications of expected uptime (continuous and/or expressed as a percentage). Redundancy and failover items can be measured as pass / fail based on existence of redundant systems and failover plans, although unique organizational constraints should be considered in determining this.
Testing	Determine average system uptime, scheduled downtime, and Service Level Agreements (SLAs) based on discussion and review of relevant documentation. Determine level of redundancy / failover plans based on discussion.
Objective / Subjective	Objective – conformance to SLAs in terms of system uptime can be measured objectively. Subjective – redundant/failover systems are important for large

	enterprises which critical communication needs and infrastructures, but may not be financially justifiable for smaller, less Internet-dependent organizations. Cost / benefit considerations should be taken into account when evaluating XYZ's uptime and redundancy arrangements.

FW-3	
Description	**System performance.**
References	10, 12
Control Objective	Ensure that the system hardware provides adequate resources to perform firewall duties at a high level of performance, and that established metrics are consistently monitored to prevent downtime and performance problems.
Risk	Threat: A firewall system with inadequate resources is prone to crash (lack of availability), fail (closed, resulting in DoS, or even worse, open, resulting in unrestricted access – lack of reliability), and slow processing and throughput (poor performance, leading to user dissatisfaction and/or attempts to subvert or circumvent the firewall; consistent poor performance may also require extensive changes to the firewall, undermining stability). Likelihood: Depending on throughput requirements increasing and the complexity of the firewall rulebase, previously adequate hardware resources can quickly become insufficient. Consequences: Lack of availability, unrestricted access, poor performance, instability.
Compliance	Compliance with this audit item would fall in a range of several values. For example: inadequate hardware resources (failing), adequate but could use upgrade(s) to improve performance, and sufficient hardware for performance needs. Likewise, monitoring, alerting, and values could be assessed values in between simply compliant / non-compliant (e.g., compliant, but needs improvement). Informal, infrequent, or non-existent monitoring and alerting activities would be grounds for failure.
Testing	Review, compare, and evaluate system hardware specifications (CPU, RAM, HDD, network interfaces, etc.) against manufacturer specifications and reasonability for sufficiency. Additionally, determine, based on discussion, whether performance monitoring takes place (formally or informally, utilizing tools and reports or ad hoc), and whether thresholds and alerts have been set and configured. (Given a generous budget, an auditor could utilize a commercial tool such as Spirent Communications' WebSuite Firewall Module to

	measure firewall throughput, NAT performance, resistance to DoS attacks, etc.)
Objective / Subjective	Objective / Subjective – minimum hardware specifications are typically provided by software vendors. These can be compared objectively against production specifications for compliance. A certain amount subjective judgment must be used to take into consideration the organization's environment (total users, average throughput, etc.) when evaluating the sufficiency of the hardware. In addition, monitoring and alerting activities should necessarily take place, but no single standard exists to specify what should be monitored, how often, or at what levels alerts should be triggered.

Firewall Access Control List Items

ACL-1	
Description	The firewall rulebase is configured securely to prevent unauthorized traffic.
References	14, 16
Control Objective	The firewall rulebase should reflect and support an organization's defined security policy, driven by business needs, if one exists (refer to **PP-1**), to be fully and tactically aligned with the organization's objectives.
Risk	Threat: Given the wealth of simple and free tools, attackers can and will eventually locate loopholes in a rulebase and exploit them to gain unauthorized access to the system and/or protected network(s). Likelihood: Depending on the level of documentation and how driven the firewall rulebase is by policies, rules can easily become removed from the intended business justifications. Consequences: An insecurely configured rulebase effectively defeats the purpose of a firewall's existence. Firewall rulebases that are not configured based on organizationally defined needs tend to less effectively allow and deny appropriate traffic.
Compliance	Each rule in the firewall can be verified for accuracy and appropriateness with business owners; other rules which should be always be in place can be checked for their presence – this is a binary compliance check. Any traffic that is allowed to pass through the firewall without a legitimate business purpose is noted as an exception.
Testing	Port scan (SuperScan, nmap) from external network (Internet) to

	screened network; attempt to map out rulebase with traceroute-based Firewalk tool (refer to **Appendices B, C,** and **E**, respectively). Confirm any type of traffic that is allowed through the firewall for a legitimate purpose with business owners. Any unexpected / dangerous results should be immediately communicated to appropriate personnel to remediate, and included in the report. Confirm that services which should require authentication are defined so in the rulebase; test this requirement by attempting to access the system without proper credentials. Research and cross-reference port / vulnerability scan results against exploit database (e.g., CVE). **Note >** these scans took place with written approval from management, without publicizing the exact dates and times to the IS staff, per request. **Note >** This audit does not include scanning from internal network segments, due to management restrictions; nor can most internal systems be scanned from the Internet, due to NAT activities performed at the firewall.
Objective / Subjective	The appropriateness of firewall rules can be determined objectively, with the assistance of business process "owners".

ACL-2	
Description	The firewall is configured to protect certain ports against well-known exploits and vulnerabilities, as defined in the SANS Top 20 Common Vulnerable Ports list.
References	Appendix F, 22
Control Objective	Eliminate "low-hanging fruit" (i.e., easily-exploited vulnerabilities) in order to provide a more difficult target than adjacent networks.
Risk	<u>Threat:</u> Well-known and popular vulnerabilities can be readily exploited using a wealth of information to gain access to the internal network. <u>Likelihood:</u> The most commonly known vulnerabilities, which often have readily-available automated exploit tools available, are the most likely to be exploited because of the lower skill level required and the enticement of potentially further lax security within the network. <u>Consequences:</u> Breaches or DoS of the firewall or access gained to sensitive internal systems.
Compliance	Each relevant item in the SANS list can be checked for appropriate protection from the firewall – this is a binary check. If any items on the SANS list are not appropriately protected against

	in the rulebase, an exception is to be noted.
Testing	Port and vulnerability scans from external network to protected system (refer to **FW-1** and **ACL-1**); observation of rulebase to confirm appropriate protections. This step will mainly utilized the freeware scanning / vulnerability assessment / penetration testing tool "Nessus"; the plug-ins are to be correlated to the Top 20 list (**Appendix F**), where applicable, to ensure all items are checked for. For example, included in the Top Twenty list are the following vulnerabilities specific to Windows systems, listed with the corresponding Nessus plug-in(s) that check for it: **W1**: Internet Information Services (IIS) http://cgi.nessus.org/plugins/dump.php3?id=10943 **W3**: Microsoft SQL Server http://cgi.nessus.org/plugins/dump.php3?id=10862 http://cgi.nessus.org/plugins/dump.php3?id=10144 http://cgi.nessus.org/plugins/dump.php3?id=11214 **W4**: NETBIOS – Unprotected Windows Networking Shares http://cgi.nessus.org/plugins/dump.php3?id=10150 **W9**: Remote Registry Access http://cgi.nessus.org/plugins/dump.php3?id=10428 **Note >** This is not an exhaustive list of the plug-ins to be utilized to verify protection against the Top Twenty list; however, enabling "all but dangerous" plug-ins option within Nessus will successfully check for each of these vulnerabilities.
Objective / Subjective	This item can be objectively assessed. It is both verifiable and repeatable.

ACL-3	
Description	The firewall rulebase is configured efficiently to reduce complexity, resource-intensive processing, and confusion.
References	3, 4, 7
Control Objective	Maintaining an efficient rulebase reduces resource-intensive processing, and complexity and confusion, which can lead to mistakes in rule ordering, possibly negating critical rules.
Risk	"It is a source of amusement for many people to review the so-called *blue laws* of a region…Computers have no common sense -- they just do what they are told no matter how silly it is. With a firewall, it is critical to keep the rulebase as efficient as possible and to periodically review the rules to make sure they are still relevant." [7] Threat: Inefficient rulebases lead to strain on resources (potential DoS / reliability issues), and incorrectly ordered rules, which can negate

[7] Fennelly, Carole. Building Your Firewall, Part 3.

	some rules entirely. Likelihood: The likelihood increases over time, and depends on the complexity of the rulebase and the diligence of administrators in maintaining good documentation. Consequences: Performance and/or reliability issues; possible security breaches due to incorrect rule ordering.
Compliance	A series of ratings should be applied to this item to evaluate the efficiency of the rulebase (i.e., 1 (efficient and simple) – 5 (inefficient, overly complex and confusing), with a rating of 3 being adequate. Any rulebase with an extraordinarily high number of rules (~ >50), poor or nonexistent rule documenting / notes, or multiple duplicate / incorrectly ordered rules should be noted as an exception.
Testing	Rules should initially be written with the aid of flow charts and/or policy statements to most accurately define filters, and align them with business goals. Confirm this is the case based on discussion with firewall administrator(s), business owners, and management. Review sample documents and attempt to make correlations between original documents and current rulebase. Verify that a manageable number of rules are present, considering the role of the firewall and nature of the network environment (no more than ~25). Review use of the 'Comments' fields to determine how often / how well useful information is provided for interpreting and describing rules for the sake of clarity, and continuity of knowledge.
Objective / Subjective	This is a fairly subjective item: the auditor should consider the number of systems and types of traffic required when evaluating the number of rules. Use of 'Comments' field, flow charts, and policy statements is more objective.

Firewall Administration Items

ADM-1	
Description	Firewall logs are configured to log appropriate data (permit and deny actions for connection types as deemed important (administrative access, SMTP, etc.), firewall rule applied, source IP and port, encryption scheme and method, alerts, NAT'ing, etc.). These logs are monitored, reviewed regularly, and maintained. Alerts are configured to notify appropriate personnel when warranted. Additionally, ensure that the log file size is sufficient to

	capture all data for the time period in between backups.
References	1, 12, 16, 20
Control Objective	Logging of proper firewall data combined with alerting mechanisms can help in identifying potential attackers ahead of time or in the act, identifying trends in malicious entry attempts, troubleshooting network issues and rulebase misconfigurations, and providing an audit trail for investigation in the event of a security breach.
Risk	Threat: Inadequate logging hinders attack detection and response, leading to costly downtime and potentially contaminated data without awareness of the problem. Lack of alerting or regular review also inhibits detection, to an only slightly lesser extent. Likelihood: Attacks or attempted attacks are inevitable for a system with a public network connection; lack of logging/alerting almost certainly will lead to slower response time to allow attacks to progress. Consequences: The success and affects of attacks will vary widely, but without logging, there may always be uncertainty as to whether attacks have occurred, and if so, the extent of the damage. When security breaches do occur, critical data that could be used to reconstruct the attack sequence will not be available. If log files are not allocated sufficient hard drive space, critical data may be overwritten or not logged at all.
Compliance	Compliance is essentially binary – either data is logged and maintained for review, and alerts configured, or not. There is room to make additional comments regarding the type of data logged, the frequency of log reviews, and alerting triggers also. The adequate size of log files can be determined based on historical file sizes requirements.
Testing	Firewall logging and alerting configuration cannot be physically confirmed through review of the administrative console. Instead, physical proof should be obtained that certain scanning and probing activities (Appendices **A - E**) were detected, recorded with an appropriate level of detail, and, since the scans were unannounced, in some cases, they should have produced alerts when conducted for prior audit steps. Interviews with appropriate personnel, review of formal policies, and obtaining sample copies of historical logs are used to determine compliance with monitoring and review, log file size, etc.
Objective / Subjective	Objective – existence and review of logs is verifiable and repeatable. Adequacy of monitoring, reviewing, alerting, and file size are somewhat more subjective, but can reasonably be assessed uniformly by multiple independent parties. Log evidence

	that scanning activities were detected and recorded can be verified and repeated.

ADM-2	
Description	**Administrative remote access methods to the firewall are sufficiently restricted, secured, and accountable.**
References	3
Control Objective	Restricting and securing the locations and methods of administrative access to the firewall helps to reduce the likelihood of unauthorized parties eavesdropping to obtain login credentials or other sensitive information, or, if credentials are obtained, being able to connect without gaining physical access to one of the allowed systems.
Risk	Threat: Allowing administrators to connect to the system from anywhere using any connection method opens the door for outsiders to eavesdrop on unencrypted sessions and lift sensitive information. Remote administration also lessons the accountability and traceability of administrative actions. Likelihood: Any passing of credentials in cleartext presents a significant possibility of this information being "sniffed", or captured by eavesdroppers. Remote administration is somewhat more harmless because of the tight-knit nature of the organization; however, it should not be underestimated as a risk. Consequences: Eavesdropping of cleartext credentials could give an attacker complete control over the firewall, if remote administration is allowed.
Compliance	Compliance can be measured in binary terms – conforming or non-conforming. Any unencrypted protocols that are allowed to remotely access the firewall should be noted as exceptions; if source IPs are not limited, this is an exception as well. Additionally, if each administrator does not use a separate account for access, this would constitute a segregation of duties issue.
Testing	Review of the rulebase, based on scanning and rulebase mapping efforts (**Appendices B, C, D** and **E**) and discussion with administrators, to determine what access methods are allowed to connect to the firewall, and which sources are allowed to connect. Specifically, the following types of traffic may be allowed to connect, and should be considered for appropriateness, if so: ▪ telnet (port 23) ▪ ssh (port 22) ▪ HTTP (port 80) ▪ HTTPS (port 443)

	Review any applicable policy, and discuss access methods with firewall administrators regarding practice in actuality.
Objective / Subjective	Objective – administrative access should be limited to a small number of sources, or ideally from the console only. Administrative access should occur only over one of the known securely encrypted protocols (e.g., SSL, SSH). (Note: if administration is restricted to the console only, no administrative access should be permitted from any sources, over any protocol. Additionally, ensure that the default firewall remote administration services are disabled.)

ADM-3	
Description	**Firewall system configuration, rulebase, logs and other critical files are backed up regularly, and stored in a secure location; restoration is periodically practiced.**
References	8, 11
Control Objective	Regular backup of critical firewall system data is important for prompt and relevant data recovery in the event of a system failure. Maintaining this data provides for an audit trail to analyze changes that have been made, and can prove to be indispensable for investigations of breach, and the ensuing legal processes.
Risk	Threat: Failure to maintain backups can lead to long downtimes and unnecessary effort and confusion in rebuilding the firewall in the event of a system failure. The lack of audit trail can increase the difficulty of ascertaining who made changes to the firewall, and when. If security breaches are discovered to have occurred in the past, critical data that could be used to reconstruct the attack sequence and serve as legal evidence will not be available. Likelihood: The likelihood of a system failure depends on other items, such as performance (**FW-**3), availability / reliability (**FW-2**) and environmental controls (**PHYS-2**), but would typically be considered fairly low. Consequences: Increased downtime, lack of accountability, lack of evidence.
Compliance	Whether files are backed up or not is a binary determination; whether all of the necessary files are included, the frequency (and type) of backup, secure storage, and frequency of practice restorations can be assessed intermediate ratings (e.g., best practice, adequate, failing).
Testing	Review of sample backup data, media storage, and restoration policies; discussion with appropriate personnel regarding which data is included and how often backups are performed, and examination of backup data list.

Objective / Subjective	This is a relatively objective determination, although some subjectivity is required to assess the sufficiency of frequency and storage location, based on the organization.

ADM-4	
Description	**Firewall administration duties are sufficiently segregated from other responsibilities.**
References	5
Control Objective	Segregation of duties helps to prevent conflicts of interest, and allocation of excessive control to individuals. Additionally, appointing a full-time firewall administrator(s) should allow for sufficient time and resources to perform duties such as closely monitoring security alerts, etc. for relevant items.
Risk	Threat: Multiple roles and responsibilities consolidated to one individual leads to inadequate time and attention paid to important administrative duties, and can provide an environment for excessive authority without proper checks and balances. Likelihood: Segregation of duties is especially common and problematic in small, informally-structured IT organizations. Consequences: Inadequate attention to all responsibilities, lack of 'checks and balances', lack of accountability.
Compliance	Firewall administration should ideally be separated into at least two positions: operating system and application administrators. These individuals should not hold other related responsibilities such as network administrator or help desk supervisor. Compliance can be measured as either pass or fail, if this is not the case.
Testing	Discuss titles and responsibilities with management and relevant members of the IT and IS staff; review any available organization chart (see **Appendix K**); confirm with user account listings.
Objective / Subjective	This item can be measured objectively – it is verifiable and repeatable.

Perimeter Access Items

PER-1	
Description	The firewall and surrounding network configuration has been adequately documented and is regularly revised to reflect changes.
References	8, 13, 14

Control Objective	Frequently updated and thorough network documentation helps the entire Information Technology staff to keep updated with changes, thereby reducing confusion and potential for errors. Additionally, detailed network documentation can assist in technology asset management efforts to reduce overall IT infrastructure costs.
Risk	Threat: Attempting to secure a network without knowing exactly what needs to be secured is an exercise in futility. Non-existent, inadequate, or outdated network documentation prevents Information Security from fully understanding what needs to be protected, and what vulnerabilities may exist and require remediation. Additionally, if network documentation is not performed in conjunction with network change management and asset tracking efforts, unidentified and unprotected access points are more likely to exist, which could be used as surreptitious conduits into the network (refer to **PER-2**). Likelihood: The probability of network documentation becoming out of sync with actual systems depends on the size and complexity of the network, and the importance placed on documentation throughout the IT department. The more outdated documentation becomes, the more difficult it becomes to bring it up-to-date. Consequences: Ignorance about internal systems is especially harmful to attempts to effectively manage a firewall's rulebase, where rules must be constantly kept current based on system purpose, location, address, name, etc. Rogue entry points into the internal network pose a serious threat in that they can bypass the firewall entirely (**PER-2**). Lastly, not knowing what systems exist within the network can lead to inefficient IT asset tracking and replacement.
Compliance	Network documentation across and within different types of organizations exists to widely varied extents. Ratings therefore typically will not be limited to simply 'exists' / 'does not exist'. Intermediate ratings should be applied based on the completeness, level of detail, recentness, and dissemination / availability of this information (should be communicated to all appropriate personnel, and restricted from individuals without a need). These ratings depend highly on the nature of the organization and the complexity of the IT environment.
Testing	Functional testing should be accomplished through simple scanning tools and command line utilities (nmap, SuperScan, ping, tracert, host; refer to Appendices **C, B, L, N, A,** respectively) to verify networked systems as are "alive" and named as documented and discussed, and that unknown or "rogue" systems are not present in the network. Review relevant network documentation (e.g., segment diagrams

	(logical and physical); operating system, software, hardware, host names, IP addresses, connections, etc.). Determine, based on discussion and observation of current network systems, the level of accuracy and completeness of documentation. Evaluate the clarity of the information, and the extent of communication of this information to stakeholders.
Objective / Subjective	Partially objective – the existence, completeness, and recentness of each of type of documentation mentioned above; partially subjective – evaluating the appropriateness of the level of detail, clarity, and dissemination of information must take into account the differing organizational characteristics of each client.

PER-2	
Description	Communication lines that bypass the firewall are limited and adequately protected.
References	10, 16
Control Objective	Identifying and securing all communication lines that bypass the firewall is critical to prevent intrusions into the network where the firewall cannot deny or even 'see' the data.
Risk	A network's security is only as strong as the weakest link, so even a single unknown / unsecured access point can compromise the entire network, despite otherwise sound perimeter security. Perimeter protection is not comprehensive until all access points into the network have been identified and secured. This includes connection points, which are not routed through traditional perimeter protection devices such as routers and firewalls, such as modems, machines engaging in VPN, and Wireless Access Points (WAPs) and Wireless Clients (WCs). Threat: Traffic that can circumvent the firewall may pass between the public Internet and internal network without any filtering, or even logging; administrators may not even be aware that the traffic is being passed. This could allow malicious or sensitive data to pass undetected. Likelihood: The proliferation of notebooks, tablet PCs, PDAs, and WAPs and WCs, along with remaining legacy modems makes for a very high likelihood in most organizations that an unidentified access point will exist if they are not prohibited by policy and/or constantly searched for and removed. Consequences: An attacker who is able to connect through any one of these points can, at the very least, work to enumerate the network from within, or, at the worst, completely compromise protection devices or critical systems.

Compliance	Compliance is binary; it is measured by whether each and every access point has been identified and secured. If not, the item is noted as an exception. Because the nature of these additional access points means that even one unidentified / unsecured connection can compromise the entire network, there is no room for intermediate ratings. Clearly-worded policies should define requirements and restrictions for accessing the network via these means.
Testing	Wardialing (using freeware such as THC-SCAN or commercial tool such as PhoneSweep), and WAP detection and security audit (freeware tool such as Net Stumbler, or commercial tools including Wireless Security Auditor (WSA)) should all be conducted to identify any connection points of these types. Network documentation should be reviewed and compared to the findings to determine if all connections have been accounted for. Additionally, basic security checks should be performed for all VPN and WAP devices, as such unsecured (by default settings) devices are nearly as dangerous as unknown devices, because they can be easily compromised. Existing policies should be reviewed for clarity and precision of terms regarding remote access, PDA use, etc. The user community should be polled to evaluate awareness of, and compliance to, these policies.
Objective / Subjective	Mainly objective – the number of additional access points as compared to what is known and documented is verifiable and repeatable. Subjective criteria may be applied to some extent in evaluating the security of VPN and WAP devices (e.g., encryption bit-level implemented, restrictions on remote users' ability to install personal software, etc.). Policy evaluation will also be mainly subjective.

PER-3	
Description	The firewall and the systems it protects have been baselined with a 'known good system state'.
References	5
Control Objective	Baselines help to provide information about not only whether or not systems have changed, but how, and what effect(s) these changes have had. This is helpful to determine when anomalies are occurring on the firewall, or within the protected systems of the internal network, and can be useful for investigation purposes in the event of a security breach. Automated baselining provides more frequent and objective baselines, but must be verified. Baselines are related to policy in that they can be compared to what has been determined *should* be done, versus what *has* been done.

Risk	Threat: Intrusions may occur or malware may be present on sensitive systems without XYZ's knowledge if they don't leave "tracks" (i.e., installing a fake, trojaned logging program in place of the legitimate version), or if logging and monitoring are not consistently performed. Malicious users can then continue to further penetrate the network, potentially undetected. Likelihood: The likelihood of attacks going undetected in the absence of baselining depends on the sophistication of the attacker and diligence of firewall administrators in logging and reviewing potential malicious traffic (**ADM-1**). There is a fairly high possibility of a trojaned program existing somewhere in the network if end users do not closely comply with an Acceptable Use Policy (**PP-1**). Consequences: Without knowing what a system / network should 'normally' look like ("known good system state"), it is difficult or impossible to determine when irregularities are occurring. This reduces the likelihood of (timely) detection of problems / security breaches, which exacerbates the issue of not being able to trust potentially contaminated data, programs, and processes.
Compliance	The audit should measure the discrepancies between the policy and actuality, and determine changes that have taken place since the baseline to come in closer compliance with the policy. Each important system and identifiable metric (e.g., network traffic level) should have a baseline in storage. This is a binary check. Assessing the adequacy, use, and effectiveness of these baselines requires more intermediary ratings.
Objective / Subjective	Existence of baselines is an objective assessment; results are verifiable and repeatable. Assessment of the quality of baselines is more subjective based on the auditor's opinion of which parameters are relevant and important.

Firewall Configuration Items

CFG-1	
Description	The firewall is configured to appropriately handle unexpected data, including fragmented packets, spoofed IP addresses, etc. and prevent network enumeration and DoS attacks.
References	13, 16
Control Objective	▪ Denying spoofed packets prevents external packets attempting to fool the internal network into thinking they come from an authorized or trusted network segment or

	host. ▪ Fragmented packets should be denied to prevent efforts to sneak malevolent activity past firewalls or Intrusion Detection Systems (IDSes). ▪ Network enumeration should be prevented by disabling or greatly restricting the trafficking of ICMP packets. ▪ DoS attacks can be prevented or reduced by blocking sources and certain patterns of traffic by most modern firewalls.
Risk	Threat: Deliberately misformed data packets may be able to bypass firewall filtering and create undetected attacks. Network enumeration may be performed to gain insight into the internal network. DoS may be created to debilitate legitimate user traffic to the network. Likelihood: Readily available tools can be used to create spoofs or fragmented packets and enumerate networks. If any attacker is unable to penetrate the network, tools are available to create DoS attacks as well. Many of these tools are simple enough for relative novices to accomplish these activities, making for a high likelihood of these attempts. Consequences: Spoofs and fragmented packets both attempt to fool and/or circumvent protection devices, bypassing the rules and underlying security policy, which can lead to passing malicious data into, or sensitive data out of, the internal network. Network enumeration can give potential attackers the information needed to accomplish their exploits. DoS attacks can lead to unavailability of resources, or the possibility of a completely unprotected network, in the event of a firewall 'fail-open'.
Compliance	Each of these configuration items can be measured as present or not -- a binary check.
Testing	▪ Ensure there are ingress filtering rule(s) in place to deny incoming traffic with internal / private / loopback / unallocated / broadcast source IP addresses. ▪ Egress filtering should block outgoing traffic with a source other than internal address space in order to block outbound spoofing, identify possible trojan'ed hosts, and prevent overwhelmed NAT devices from leaking private IPs. ▪ All source-routed packets should be blocked. ▪ ICMP should be disabled (or limited to specific IPs that can use it for administrative / troubleshooting purposes). ▪ Nessus scans can be configured to test for DoS vulnerabilities and protection (**Appendix D**). * ▪ Simple dos utilities such as ping, tracert, nslookup for network enumeration (refer to **Appendices L, N, A**)

	▪ Attempt to send spoofed-source and/or fragmented packets through the firewall with a custom packet crafting tool (e.g., nmap); determine success based on replies received *** Note >** those steps which cannot be physically conducted by the auditor must rely on discussion, review of documentation, and/or limited / indirect observation.
Objective / Subjective	These are independently-verifiable and repeatable tests; therefore they are objective.

CFG-2	
Description	The firewall is correctly configured to perform Network Address Translation (NAT) and/or Port Address Translation (PAT), if available and necessary.
References	11
Control Objective	Prevent sensitive internal network addressing information from being exposed to the public.
Risk	<u>Threat:</u> Use of network addressing information to assist in network enumeration and identification of potential vulnerabilities in the network based on port / service correlation. <u>Likelihood:</u> Network enumeration and identification of services running are among the most basic, and initial activities that a malicious attacker might attempt to infiltrate a network, making a high likelihood of this threat being realized. <u>Consequences:</u> Exposing internal addressing (IPs and ports) schemes gives potential attackers important information to carry out exploits, significantly lowers the difficulty of identifying which exploits may be successfully carried out against network systems.
Compliance	The use of NAT and PAT can be measured in binary. **Note >** PAT is not necessary or required in all environments; XYZ should not necessarily be faulted if it is not utilized.
Testing	Discuss the firewall configuration for NAT parameters which should be identified as either 'HIDE' or 'SOURCE STATIC' public IP. Attempt to ping and/or tracert to internal systems (based on hostname) from the Internet to verify private addressing (refer to **Appendices L** and **M**, respectively for descriptions and appropriate switches for these tools).
Objective / Subjective	This is an objective test.

Firewall Operating System Items

OS-1	
Description	The firewall's underlying operating system is securely configured and regularly updated to maintain security.
References	1, 3, 9
Control Objective	Securing the underlying operating system of a firewall is critical to keeping intruders out of the system and thereby maintaining the integrity of the rulebase.
Risk	Threat: Underlying operating systems security flaws can be exploited to take control of the firewall or crash the system. Likelihood: Firewalls' operating systems are often overlooked in attempts to harden or lock-down perimeters; however, the sheer number of updates and patches related to vulnerabilities in Windows' products makes the potential for an existing exploit on the firewall fairly high, especially if regular patching procedures are not well-defined and followed, as part of a change management policy (see **PP-2**). Consequences: Exploits in the underlying operating system could allow an attacker to take control of the system, effectively opening the organization's network wide open, or crash the system, DoS'ing the organization, depending on the impact / privilege level gained as a result of the exploit.
Compliance	The OS should ideally be in a 'bare-bones' configuration, with no unnecessary applications / services running or ports open. Compliance can be measured as pass / fail, with additional feedback provided at each level. Any significant deviation from a known, accepted standard (e.g., NSA, SANS Gold Standard) results in a failure.
Testing	Compare the operating system patch level and security settings to best practices / Gold Standards and identify any discrepancies. Additionally, review organizational patching / change control policies to determine the appropriateness of updating procedures. Nessus, nmap, netstat, Fport, and similar utilities can be used to test compliance, as well as observation of the system.
Objective / Subjective	This is an objective test, when comparing to a widely-accepted standard such as the NSA Guide.

Physical Security Items

PHYS-1	
Description	**Determine whether physical access to the firewall system is adequately restricted.**
References	1, 7, 10
Control Objective	Physical security helps ensure that only appropriate individuals have access to configure and modify the firewall parameters, or glean sensitive information about it.
Risk	Threat: Physical access to the firewall would allow an attacker to defeat any and all logical security controls with ease. Likelihood: Attempting to gain physical access to the firewall seems a fairly blatant, and therefore unlikely technique; however, "social engineering" and other such subtle techniques make the task more likely than might be expected. The relatively small, familiar nature of the XYZ organization makes the likelihood of an intruder gaining unnoticed access to the firewall system quite unlikely; conversely, the generally friendly and trusting culture make an inviting target. Consequences: Poor physical security, although often overlooked, poses an enormous risk because all other controls can be compromised if people can physically reach the system. Malicious intruders could intentionally, or innocent users could inadvertently, modify the firewall configuration to allow unauthorized traffic into / out of the network segment.
Compliance	There are multiple levels of compliance for this item: physical security controls can range from non-existent, to inadequate, needs improvement, etc., through adequate.
Testing	Steps to be followed in assessing physical security include: First-hand observation and discussion with appropriate IT and organizational security personnel regarding access restrictions such as locks, security guards, video cameras, etc. Attempt to subvert physical security (see **Appendix G**).
Objective / Subjective	Subjective – the adequacy of physical security controls depends largely on a subjective evaluation of the environment and its data and determination of what level of such controls is necessary to be considered sufficient.

PHYS-2	
Description	**Determine whether environmental controls surrounding the firewall provide adequate safeguards.**
References	9, 16
Control Objective	Environmental safeguards can help to protect critical data and systems from the negative effects of their natural surroundings and

	disasters.
Risk	Threat: Naturally occurring conditions as well as natural disasters can potentially have adverse effects, including humidity / water, overheating due to temperature, fire destruction, etc. Likelihood: While the likelihood of a natural disaster is quite low, based on XYZ's geographical location (Northeast U.S.), the potential for damage from day-to-day hazards such as heat and humidity is always real. Consequences: Consequences can range from system crashes / instability due to heat to complete loss of systems and data due to natural disaster, with extraordinary associated costs for equipment, recovery efforts, and lost information and business.
Compliance	There are multiple levels of compliance for this item: environmental controls can range from non-existent, to inadequate, needs improvement, etc., through adequate. Certain of the most basic and critical controls must be present (e.g., climate control, fire extinguisher), or the item should be failed.
Testing	First-hand observation and discussion with appropriate IT and organizational maintenance personnel regarding the existence of environmental controls such as fire suppression (extinguishers and halon sprinklers), backup power, climate control, raised floors, humidity control, etc. For obvious reasons, these controls will not be functionally tested.
Objective / Subjective	Subjective – the adequacy of environmental controls depends largely on a subjective evaluation of the risks to the environment and its data and determination of what level of such controls is necessary to be considered sufficient.

Policy and Procedural Items

PP-1	
Description	**Determine whether relevant Information Security policies and procedures (Corporate Security policy, Acceptable Internal Use policy, etc.) exist, and establish accountability, manageability, and authority, as well as goals and expectation levels for security controls.**
References	4, 18, 23
Control Objective	Policies and defined procedures for all aspects of network security set expectations for end-users, information security staff, and management, and establish accountability and enforcement for non-compliance as a deterrent:.

	"By establishing a policy, you are implying that enforcement can or will follow. Without security policies, enforcement of them is not possible." [8]
Risk	Threat: Lack of established and communicated policies leaves out the most fundamental aspect of controlling security: user compliance. If users are not aware of policies or are under the impression that security is not important or likely to be enforced, they are much more likely to engage in risky computing practices (e.g., opening unknown attachments, downloading personal software, etc.). In addition, lack of security policies does not give management realistic expectations for the security of the organization's information, and does not provide accountability for the responsible personnel. Likelihood: Since security typically represents a tradeoff for reduced convenience, users will likely revert to insecure, but convenient computing practices in the absence of effective policies. Consequences: Perimeter protection can be easily undermined by lack of internal user education, awareness, and cooperation with security efforts. Whether intentional or inadvertent, end user insecure computing can create disastrous consequences within a network. If expectations have not been set and agreed upon for the organization's information security, management has no criteria against which to evaluate the security department or evaluate the company's improvement or relative standing as compared to the industry.
Compliance	The existence of adequate policies is a pass or fail assessment; the determination of communication and enforcement is more of a variable check.
Testing	Obtain and review copies of relevant policies. Discuss awareness and enforcement with management and user community. Assess the completeness and appropriateness of these policies. For example, a security policy should address the following items: • What information is the firewall protecting?; • Expectations for the firewall; • Define acceptable risk levels; • What actions are authorized, and for whom?[9] The policies to review should include, at a minimum, some form of Corporate Computer Security, Acceptable Use, Physical Security, and Incident Handling, or some combination thereof.
Objective /	Existence of policies is an objective test; adequacy of these policies

[8] Ibid.
[9] Collaborative. Auditing the Perimeter.

Subjective	is considerably more subjective, taking into account organizational attributes (size, culture, etc.).

PP-2	
Description	**A formal change management policy exists which defines the procedure to be followed in requesting changes, testing changes, modifying the firewall configuration, and backing-out changes, when necessary.**
References	8, 12
Control Objective	Change control is essential for maintaining tight control over the firewall rulebase and configuration. An efficient change control policy is important especially when considering updating and patching needs. A separate escalated / emergency change management policy may exist to address critical security-related change needs. Formal approval is important to consider the security implications of each and every change, in isolation, and in conjunction with existing rules and configurations. Receipt of change requests through a single channel helps the firewall administrator(s) to prevent the rulebase from becoming overly complex with overlapping and redundant rules. Change request / approval audit trails help to retroactively understand the justification for rule modifications, for use in further auditing and cleanup. Testing changes in a separate environment helps to prevent accidentally created security loopholes and/or costly downtime in production. A back-out procedure to reverse adverse changes (as formally defined) in a timely and thorough fashion is an important remediation control. A change management process should establish an audit trail for modifications, as well.
Risk	Threat: Lack of change control with regards to the firewall rulebase and configuration leads to poor validation of rule modifications and confusion in ordering, and system updating without appropriate testing. Likelihood: Depending on the frequency of rule modification needs and system updates, as well as how clearly assigned firewall roles and responsibilities are (**ADM-4**), lack of validation and confusion may become very probable. Consequences: Non-existent or poorly communicated change management policies fail to ensure that change requests go through the proper channels of approval prior to implementation, and are sufficiently tested to determine any adverse effects. Lack of change control can lead to improperly approved (or

	unapproved) changes being implemented, potentially creating security holes. Failure to properly test rule / configuration changes and software updates / patches can lead to system instability and downtime. Lack of back-out procedures can make reversing these improper changes an overly complicated and political task.
Compliance	This policy is to include changes in the form of user rule requests and administrator configuration modifications, as well as operating system and application updating / patching. Change request / approval / denial documentation should be retained for historical records. The existence of formal change control and back-out policies can be assessed as either present or not. The matters of how well communicated and how closely followed these policies are more difficult to assign discrete measures, and should be evaluated on a sliding scale.
Testing	Review of existing policies, discussion with appropriate personnel regarding awareness of, and adherence to the policy, and review of past change request / approval forms. Confirm the existence of an identically configured test instance / environment, based on hardware, software, and network configurations. Discuss scheduled downtimes for rollout of changes in the production environment.
Objective / Subjective	The existence of these policies is evaluated objectively; it is verifiable and repeatable. Evaluation of the effectiveness of the policies is much more subjective, as the rating can change depending on whom is interviewed on the subject, and the level of formality expected by the auditor. The size and culture of the organization must be considered in assessing this aspect.

Audit Evidence

Note > some results of stimulus / response tests cannot be included in the Appendices per management instructions.

FW-2	
Description	**Availability / Reliability of system.**
Results	Average system uptime is approximately 7 days (see **Appendix M**). System restart requiring approximately 60 seconds of downtime performed each weekend during night, with outside network connection cut off; other downtime is scheduled at least 48 hours in advance and outside of business peak hours, per discussion. No formal SLAs have been developed for the firewall. Management and end users did not express any disappointment or concerns regarding the system's availability. Redundancy is not currently addressed in XYZ's Check Point firewall arrangement; however, considering the acceptable levels of performance (**FW-3**) and stability, environmental controls in place (**PHYS-2**), and tight budget constraints, this will not be considered an exception. In the future, XYZ may want to consider addressing these aspects, as described by Check Point's Performance and Availability offerings (e.g., process offloading, load balancing, QoS, redundancy, etc.)[10].
Assessment	System is adequately available and reliable; however, SLAs should be considered to confirm and enforce adherence, and even provide incentives for above average performance. **Minor exception noted.**

FW-3	
Description	**System performance.**
Stimulus / Response	Administrators agreed to allow a copy of SiSoft's SANDRA[11] (System ANalyser, Diagnostic and Reporting Assistant) Advanced to be run on the firewall machine during off-business hours to baseline the system's hardware, software, and devices. The resulting report displayed a wealth of information about the system configuration, including the basic specifications required to assess adequacy of performance capabilities, as listed below.
Results	The hardware specifications of the firewall appear sufficient based on Check Point's minimum requirements[12], comparable Check

[10] http://www.checkpoint.com/products/connect/vpn-1_pro_performance.html
[11] http://www.sisoftware.net/index.html?dir=&location=pinformation&langx=en&a=
[12] http://www.checkpoint.com/products/connect/vpn-1_pro_sysreq.html

	Point appliance specifications[13], and based on the level of activity at XYZ and their performance needs: • Dual 1.2GHz processors • 512 MB RAM • Two 40GB 7200RPM HDD • 100Mbps Nicks *(XYZ activity through this firewall includes traffic from approximately 75 users. According to firewall administrators and network engineers, peak traffic to this Check Point firewall averages no more than 200Mbps, and an estimated 20 concurrent users. Gigabit Ethernet network cards should be considered if throughput requirements increase.)* Infrequent performance monitoring is accomplished through system utilities (Windows NT Performance monitor, etc.). No reports are generated or distributed; no alerts have been set. Efforts are currently underway to acquire packaged software to set thresholds and alerting mechanisms.
Assessment	Monitoring and alerting efforts should continue to be formalized. **Minor exception noted.**

ADM-2	
Description	**Administrative remote access methods to the firewall are sufficiently restricted, secured, and accountable.**
Stimulus / Results	Observe an administrator attempt to connect to the firewall from the console, an internal system, and an external system; attempt to connect via multiple protocols, including telnet, SSH, HTTP, and HTTPS. Discuss and observe with administrators the number and uniqueness of administrator accounts.
Results	Per observation of attempted connections, and scanning of the rulebase, only console and SSH remote management are allowed for administrative access to the firewall. However, this access is not restricted to certain source IPs. Multiple administrators access the firewall with one administrative account, which has the default username. No formal policy exists to communicate or enforce administrative access restrictions.
Assessment	Access should be severely limited to a small number of Source IPs, each administrator should have a unique account established for use; policy should be formalized and communicated. **Exceptions noted.**

[13] http://www.checkpoint.com/products/choice/platforms/windows_midrange.html

ADM-3	
Description	**Firewall system configuration, rulebase, logs and other critical files are backed up regularly, and stored in a secure location; restoration is periodically practiced.**
Results	Per review of informal backup policy, discussion with administrator, and review of historical backup data, it appears that critical firewall data is being sufficiently backed up: weekly incremental and monthly full backups to magnetic tape, stored at an off-site, secured vendor for "several years." Restoration is practiced on an informal schedule of approximately once per quarter. Backed up data includes firewall configuration and rulebase files, operating system settings, and firewall logs. This was confirmed by observation of an informal "restoration" practice on a non-production system.
Assessment	Compliant.

ADM-4	
Description	**Firewall administration duties are sufficiently segregated from other responsibilities.**
Results	Firewall administration is not segregated between the operating system and application level. In addition, each firewall administrator holds another role within the department, based on discussion. A Security department organization chart was prepared and validated with XYZ based on the auditor's understanding of roles and responsibilities (**Appendix K**). (Firewall administrators cannot be confirmed by reviewing the system user account listings as all administrators share one generic account (refer to **ADM-2**).)
Assessment	Segregation of duties issues exists throughout the security department, largely due to inadequate numbers of personnel. **Exception noted.**

PER-1	
Description	**The firewall and surrounding network configuration has been adequately documented and is regularly revised to reflect changes.**
Stimulus / Response	Based on discussions with various IT staff and observation of data center and PC layouts, it is obvious that the existing network documentation is considerably outdated and therefore inaccurate. Functional testing using simple scanning and command line utilities (refer to **Appendices C, B, L, N, A**) on documented system IPs often provides unexpected results (e.g., could not find host when expected, different hostname / IP combination, find hosts that don't exist in documentation).

Results	The network documentation is outdated and inaccurate, IT asset management / inventory is completely untracked. Individuals within IS have different information and understanding of the network layout.
Assessment	There seems to be no communication / cooperation between procurement, IT Asset management, and network documentation efforts. **Exceptions noted.**

PHYS-1	
Description	**Determine whether physical access to the firewall system is adequately restricted.**
Stimulus / Response	Attempts to subvert physical security were approved by the CIO – access to semi-important systems was gained outside of the data center; 'piggy-backing' attempts into the data center were unsuccessful.
Results	Physical access to systems in the data center is well controlled by locks and video cameras; **some unsecured systems containing potentially sensitive information about network layout were located.** This situation defeats the firewall by allowing unauthorized persons to view the data from the terminal, or possibly remotely, if the PCs are not restricted by the firewall. Refer to **Appendix G** for individual test step descriptions and results.
Assessment	**Minor exception noted.**

PHYS-2	
Description	**Determine whether environmental controls surrounding the firewall provide adequate safeguards.**
Results	All environmental controls that should reasonably be expected to be in place, considering the size, value, location, and budget of XYZ were noted, including: ▪ fire extinguishers (2), ▪ raised floors, ▪ climate control, ▪ UPS and moderate sized power generator, and ▪ a humidity monitoring and controlling system.
Assessment	Compliant.

PP-1	
Description	**Determine whether relevant organizational policies and**

	procedures (organizational information security policy, acceptable internal use policy, etc.) exist, and establish accountability, manageability, and authority, as well as goals and expectation levels for security controls.
Stimulus / Response	Discuss with a broad range of XYZ employees their awareness of, and, (to be kept confidential), compliance with existing security-related policies. Determine response to violations of policy, in accordance with policy. Based upon brief interviews with approximately 12 personnel across all business lines and organizational levels, awareness of Corporate Computer Security Policy is high, but users are not aware of any enforcement mechanisms or repercussions for violations; therefore, users routinely violate the policy for convenience, entertainment, etc.
Results	The computer security policy is practically rendered ineffective by lack of adherence. Refer to **Appendix H**.
Assessment	The policy should be updated with enforcement and repercussion clauses. **Exception noted.**

PP-2	
Description	**A formal change management policy exists which defines the procedure to be followed in requesting changes, testing changes, modifying the firewall configuration, and backing-out changes, when necessary. This policy is to include changes in the form of user rule requests and administrator configuration modifications, as well as operating system and application updating / patching. Change request / approval / denial documentation should be retained for historical records.**
Results	Existing organizational change management policy is too general to apply well to firewall changes. In addition, it is not well communicated or enforced. No formal documentation exists for change requests / approvals; decisions are made by an ad hoc committee of IS staff based on discussions with business owners. Major changes (e.g., service packs) are tested in a non-production environment; no formal back-out policy is defined for adverse rule changes, etc.
Assessment	Change management policy should be updated and tailored to Information Security. Request forms and an approval process should be defined, communicated, and enforced. Rule changes should be tested outside of production prior to implementation, and back-out procedures should be established. **Exceptions noted.**

Residual Risk

In every audit, a certain level of residual risk will be identified – no level of control can entirely erase exposure. Some residual risk is tolerable; this level of acceptable risk varies by environment, based on the importance of the system to the organization, as measured against the cost in time, money, personnel, and organizational impact of eliminating each area of exposure.
Without regards to resource constraints, there are many areas of improvement that can be identified in XYZ's setup:

- failover / redundancy provisions,
- separation of duties,
- increased personnel,
- increased end-user training and awareness,
- improved communication between business units and documentation, and
- greater attention to logging and monitoring.

However, the realities of XYZ's organizational culture require that each of these areas of exposure and related countermeasure be reasonably analyzed in order to make a determination whether to accept the risk or take additional measures to reduce or eliminate it. Although often difficult to quantify due to the intangible nature and difficulty in placing monetary value on system data, financial measures such as ROI (Return on Investment) can be used to help define criteria to address these questions and justify additional expenditures to management.
Considering XYZ's unique environment and organizational needs, it is obvious that considerable risk remains in this network segment, despite the apparently secure configuration of the primary protective device, the VPN-1 firewall. Poor procedural controls have led to a situation where multiple opportunities exist for security lapses.
It should be noted, however, that the majority of these remaining risks are posed by insider threat; the perimeter is actually fairly well protected from outsiders. Internal users and administrators do not have the appropriate policies for guidance and controls for prevention of security incidents. While the IT and IS staff are relatively small, tightly knit groups, the possibility always exists for insider attacks, whether intentional or inadvertent. The lack of controls and monitoring present in the organization make these risks relatively easy to manifest themselves, and very difficult to track or mitigate.
Fortunately, most of these residual risks can be improved with relatively low expenditures of time, effort, and especially money (as compared to expensive technological solutions). Considering this fact, XYZ would be well advised to work towards closing these control gaps.
Most of the controls to close these gaps could conceivably be easily implemented, however, there may be significant user community and administrator resistance to implementing more stringent controls, due to the culture of the organization.
Control objectives identified in the audit checklist could be largely achieved with implementation of policies and procedural adjustments. The policies to be implemented are essentially corrective in nature, as the paper itself carries no enforcement in itself. It is the procedures that must be established to force compliance that will provide

preventative measures.

Is the System Auditable?

The VPN-1 system is auditable from most perspectives. External scans are not entirely successful in identifying issues because of other filtering devices; the firewall cannot be scanned in isolation in this environment. If the logging, monitoring, and other advanced capabilities are enabled on the system, as some are at XYZ, these provide excellent sources for auditing. However, when control items are completely absent, audit items cannot be assessed to any measure beyond 'non-compliant.' Much of procedural audit steps must be based on discussion, observation, and stimulus/response, to some extent. These methods are not as tangible and recordable as technical steps, but if multiple individuals verify them, they can serve as effective audit evidence.
Overall, the system was quite auditable, although in considerably different fashion than a typical firewall review, due to management requests and restrictions.

Audit Report

Executive Summary:

This audit focused mainly on procedural controls, per management request. The procedural audit items were effectively assessed based on discussions, observation, and limited functional testing. The results and recommendations of these steps can likely be applied beneficially across the organization. In addition, based on the limited technical auditing performed, the e-mail screened network segment firewall seems very securely configured, from a technical standpoint, and therefore, the systems behind it appear to be well protected. However, significant procedural deficiencies exist in the organization that could work to undermine the technical security controls in place, as noted below.

Audit Findings:
The following exceptions were noted:

Firewall System Audit Item 2 (FW-2): No formal SLAs have been developed for the firewall.
Audit Item Description: Availability / Reliability of system.
Audit Step(s) Taken: Determine average system uptime, scheduled downtime, and Service Level Agreements (SLAs) based on discussion and review of relevant documentation.
Root cause: Lack of formalized procedures; lack of emphasis on documenting policies and expectations.

Firewall System Audit Item 3 (FW-3): Infrequent performance monitoring is accomplished through system utilities (Performance monitor, etc.). No reports are generated or distributed. Efforts are currently underway to acquire packaged software to set thresholds and alerting mechanisms.
Audit Item Description: Performance of system.
Audit Step(s) Taken: Review, compare, and evaluate system hardware specifications (CPU, RAM, HDD, network interfaces, etc.) for sufficiency. Additionally, determine whether performance monitoring takes place (formally or informally, utilizing tools and reports or ad hoc), and whether thresholds and alerts have been set and configured.
Root cause: No established System Maintenance policies; inadequate resources (e.g., personnel are not trained or knowledgeable on performance monitoring, alerting, and reporting); lack of emphasis on formally defined responsibilities.

Firewall Administration Audit Item 2 (ADM-2): …this (SSH) access is not restricted to certain source IPs. Multiple administrators access the firewall with one administrative

account, which has the default username. No formal policy exists to communicate or enforce administrative access restrictions.
Audit Item Description: Administrative access methods to the firewall are sufficiently restricted, secured, and accountable.
Audit Step(s) Taken: Review of the rulebase to determine what access methods are allowed to connect to the firewall, and which sources are allowed to connect.
Review of appropriate policy and discussion with firewall administrator(s) regarding actual practice of administrative access.
Root cause: Lack of formally documented Administration policies and procedures.

Firewall Administration Audit Item 4 (ADM-4): Firewall administration duties are not appropriately segregated on an operating system versus application level, or from other roles within the Data Security department. This may lead to conflicts of interest, lack of accountability, and inadequate resources to effectively manage this device.
Audit Item Description: Firewall administration duties are sufficiently segregated from other responsibilities.
Audit Step(s) Taken: Discuss titles and responsibilities with management and relevant members of the IT and IS staff; review any available organization chart (see **Appendix K**); confirm with user account listings..
Root cause: Insufficient personnel within the Data Security department; duplication of assigned efforts due to roles and responsibilities not being clearly defined.

Perimeter Access Audit Item 1 (PER-1): The network documentation is outdated and inaccurate; IT asset management / inventory is not formally tracked. Individuals within IS have different information and understanding of the network layout.
Audit Item Description: The firewall and surrounding network configuration has been adequately documented and is regularly revised to reflect changes.
Audit Step(s) Taken: Based on discussions with various IT staff and observation of data center and PC layouts, it is obvious that the existing network documentation is considerably outdated and therefore inaccurate. Functional testing using simple scanning and command line utilities (refer to **Appendices C, B, L, N, A**) on documented system IPs often provides unexpected results (e.g., could not find host when expected, different hostname / IP combination, find hosts that don't exist in documentation).
Root cause: Lack of policy to require network documentation and correlation of network changes with change management process; no established IT asset tracking procedure.

Physical Security Audit Item 1 (PHYS-1): …some unsecured systems containing potentially sensitive information about network layout were located.
Audit Item Description: Determine whether physical access to the firewall is adequately restricted.

Audit Step(s) Taken: Attempts to subvert physical security were approved by the CIO – access to semi-important systems was gained outside of the data center; 'piggy-backing' attempts into the data center were unsuccessful.
Root cause: Lack of policy regarding data distribution and poor understanding and tracking of internal systems.

Policy and Procedural Items Audit Item 1 (PP-1): The computer security policy is practically rendered ineffective by lack of adherence.
Audit Item Description: Determine whether relevant organizational policies and procedures (organizational information security policy, acceptable internal use policy, etc.) exist, and establish accountability, manageability, and authority, as well as goals and expectation levels for security controls.
Audit Step(s) Taken: Discuss with a broad range of XYZ employees their awareness of, and, (to be kept confidential), compliance with existing security-related policies. Determine response to violations of policy, in accordance with policy.
Based upon brief interviews with approximately 12 personnel across all business lines and organizational levels, awareness of Corporate Computer Security Policy is high, but users are not aware of any enforcement mechanisms or repercussions for violations; therefore, users routinely violate the policy for convenience, entertainment, etc.
Root cause: Lack of emphasis on communication of, and adherence to, corporate policies from upper management.

Policy and Procedural Items Item 2 (PP-2): Existing organizational change management policy is too general to apply well to firewall changes. In addition, it is not well communicated or enforced. No formal documentation exists for change requests / approvals; decisions are made by an ad hoc committee of IS staff based on discussions with business owners. Major changes (e.g., service packs) are tested in a non-production environment; no formal back-out policy is defined for adverse rule changes, etc.
Audit Item Description: A formal change management policy exists which defines the procedure to be followed in requesting changes, testing changes, modifying the firewall configuration, and backing-out changes, when necessary. This policy is to include changes in the form of user rule requests and administrator configuration modifications, as well as operating system and application updating / patching. Change request / approval / denial documentation should be retained for historical records.
Audit Step(s) Taken: Review of existing policies, discussion with appropriate personnel regarding awareness of, and adherence to the policy, and review of past change request / approval forms. Confirm the existence of an identically configured test instance / environment. Discuss scheduled downtimes for application of changes in the production environment.
Root cause: Lack of emphasis on formal policies; lack of appropriate approval channels from different business units and levels for change approvals.

Background / Risk:

The audit issues noted above can be roughly grouped into six categories. In order of severity, they are as follows:

- Computer security and Change management **policies are not well followed due to lack of enforcement and dictated procedures**. This renders them effectively non-existent, **and leaves users free to engage in risky computer activities**, and haphazard modifications to the firewall rulebase.
- Outdated network documentation leaves open the **possibility of unidentified and unsecured entry points** into the network, completely bypassing firewall security. Additionally, it **reduces the effectiveness of IT asset management**, and can lead to **confusion and misconfiguration of firewall rules**.
- Generic administrative account usernames, multiple individuals sharing an administrative account, and unrestricted remote management locations all greatly **undermine the authentication, authorization, and accountability** of individuals making significant changes to the firewall system.
- Lack of formal performance monitoring, reporting, or monitoring leaves open the possibility for **firewall instability** and crashes, which could potentially go unnoticed for a period of time. This downtime could be both extremely costly and dangerous, as security restrictions could be completely lifted in the event of a firewall failure.
- Systems with some **potentially sensitive information were physically available for access** to anyone inside the building, leaving the potential for stolen or compromised data.
- Network layout, **systems**, and data contained therein are **not adequately assigned to a responsible, independent party, documented, or tracked**, in large part due to **insufficient personnel**.

Audit Recommendations:

- The IT and IS teams should work with management to define and enact updated policies, complete with enforcement and repercussion clauses. Strong efforts must be made to promote user "buy-in" to accept these culturally significant changes, including question-and-answer sessions, thorough explanatory materials to promote the value of changes, and end-user awareness education, complete with individual sign-off.
    - Updated, thorough policies and training materials, to include 'Computer Security Policy', 'Acceptable Use Policy', 'End User Security Awareness and Responsibility,' 'Incident Response Policy,' 'Change Management Policy', and XXX. Each of these should include explicitly defined procedures for each responsible party.
    - Mandatory user education should be conducted (most likely web-based, for remote users), and each employee in the organization (including Information Security and Management personnel) should

be required to sign a form acknowledging their understanding of, and agreement with, the new policies (certain policies will be applicable to only some employees).

Policies should be drawn up to advance the state of XYZ's IT department along the Capability Maturity Model (CMM), as defined by Carnegie Mellon, as tailored to an information security department: "…an effective means for modeling, defining, and measuring the maturity of the processes used by (information security) professionals."[14]

XYZ's information security processes, which mostly occur on an ad-hoc basis, would be considered to be between the initial (1) and repeatable (2) maturity levels; efforts should be directed towards making these processes more repeatable (to withstand loss of personnel), standardized, more formally defined and documented, and automated, where possible. These actions should take place on an enterprise-level, utilizing a holistic approach.

- Greater attention and cooperation should be paid between procuring, deploying, and tracking IT assets.
  - IT assets should be systematically tracked from the purchasing phase, through the end of their life cycle. A procedure should be defined to track and share this information between departments.
- Changes should be made to administrative accounts in terms of passwords, individuals who can use them, methods of access, and accessible locations.
  - Establish and enforce (through firewall settings and rules) acceptable administration policies for password complexity, and access methods and locations. Reconsider the number and role of users with administrative access for segregation of duty and individual accountability issues.
- All systems containing potentially sensitive data should be located in the secured data center.
  - Relocate systems and/or thoroughly review data available on public systems and transfer sensitive data to systems within secured areas.
- Performance monitoring and logging efforts should continue towards formalization.
  - Continue to implement and fine-tune these activities to promote more consistent monitoring to ensure high availability of this critical system. In addition, a SLA should be developed between the IT department and upper management to set expectations for system availability and performance.
- *Consider bringing additional trained and skilled personnel (possibly on a temporary basis) into the Information Security department to help alleviate the individual workload and ensure that sufficient efforts can be put forth on all critical activities.** Failing this, a formal risk assessment should be conducted

[14] http://www.sei.cmu.edu/cmm/cmm.html

to identify the most critical risk areas and assign the existing resources to remediate these areas first, at the minimum.

** Management has communicated that the hiring of additional IS personnel is not currently a viable alternative, due to budget limitations.*

Steps such as these should be re-evaluated on a consistent basis indefinitely and re-performed, if necessary, as part of an organizational internal audit effort. Identifying and fixing problems should focus on the root causes, such as the lack of adequate emphasis on formalized and communicated policies and procedures. In addition, from a technical perspective, scans should take place regularly; policy and baselines can be evaluated based on the evolving results. Consider the use of a tool such as Ndiff (http://www.vinecorp.com/ndiff/) for 'change detection' to track differences between nmap scan results to help assess improvements / regression in perimeter security, and be vigilant for potential unapproved changes.

Note > Strengthening perimeter defense tends to move attackers focus towards malware, so defensive tools to address this should be given additional attention.

Costs:

The cost of implementing these recommendations, in terms of time, effort, money, and functionality / maintainability compromises, appear to be minimal, due to the fact that they are mainly procedural, rather than technological changes.

An effort has been made to estimate the time (in man hours), cost (*beyond labor*), impact on system/network performance / maintainability, based on the auditor's understanding of the organization's resources. In addition, an attempt has been made to estimate the difficulty of implementing the changes in terms of cultural change resistance, due to the significant impact on the end users.

With the existing personnel temporarily reassigned to address these items, the recommendations could be reasonably expected to be implemented within the following parameters:

Recommendation	Time	Cost	Priority	Performance / Maintainability Impact	User Community Resistance
Updated policies; end user education	30 hours (10 hours for each two InfoSec personnel; 5 hours for each of two managers' review and	$250 (Policy manual printing and binding, training materials, etc.)	**H**	None	Possibly significant due to increased restrictions and concern of repercussions for violations.

	update); 2 hours for each employee for training and sign-off				
Develop procedure and system to improve communication between individuals responsible for procuring, deploying, and tracking IT assets	Between 40-80 hours, depending on level of automation desired	$0 - $500, depending on whether a simple, in-house system is developed to shared information, or packaged software is purchased	**M / H**	None	Slight resistance possible due to increased coordination efforts.
Reconsider administrative role assignments, formally establish acceptable administrative access terms and create corresponding rules	10 hours	$0	**M**	Maintainability of the firewall may become slightly less convenient for administrators if they are restricted access based on location and/or protocol.	Resistance from information security staff who are restricted from administration.
Relocate sensitive information from publicly-accessible systems	20 hours (thorough searching, transfer of data to protected systems, and/or physical relocation of PCs)	$0	**L / M**	None	Possible resistance from customers if the number of publicly available PCs has to be reduced.
Continue efforts to obtain, implement, and fine-tune	60 hours (+ ongoing tuning)	$200	**L / M**	Performance should eventually	None

software for monitoring and alerting.				improve and be optimized with use of such software.	
Develop a performance and availability SLA based upon agreed expectations between IT and management.	20 hours (2 IT personnel, 2 managers @ 5 hours each)	$50	**L / M**	None – if anything, overall availability should improve as the IT department strives to meet or exceed the SLA for potential incentives.	None.
Totals:	~200 hours	~$750		Minimal	Moderate

For the minimal costs delineated above, these recommendations could greatly increase the value of the security provided by the firewall, with little to no effect on functionality or performance.
The cost / benefit tradeoff of such security controls must be considered when determining the ideal level of additional security expenditures.
The task of quantifying costs of expected security incidents can be very difficult, and typically requires a great amount of estimating intangibles. One method of calculating such costs uses the following basic formula:

P (L) x S (L) = R (E)

where:

P (L) = the probability of the potential loss

S (L) = the severity of the potential loss

R (E) = the total risk exposure [15]

Expenditures should be made until the point where additional expenditures would no longer outweigh the benefits provided in terms of reduced risks of exposure (i.e., a $10,000 IDS that is calculated to provide a reduction of only $1,000 annually of risk, based on the cost of risks multiplied by the likelihood, would not be a justified expenditure).

[15] Taylor, Laura. Security Scanning is not Risk Analysis. http://www.intranetjournal.com/articles/200207/se_07_14_02a.html

Compensating Controls:

Existing policies and procedures, while far from ideal, constitute some measure of compensating controls, until more effective policies can be implemented. The informal performance monitoring which currently takes place helps to reduce the likelihood of serious system problems.
The relatively low cost and effort of the recommendations noted above makes the suggestion of further compensating controls for cost / effort considerations somewhat unnecessary; however, there are some actions that can be taken at little-to-no cost which may help to improve information security at XYZ going forward:

- Improved communication and accountability of all XYZ employees regarding appropriate and acceptable use of company IT assets;
- Subscription by firewall administrators (and other Information Security personnel) to relevant e-mail security bulletins, etc. (e.g., BugTraq, SANS NewsBites and Security Alert Consensus);
- Increased informal performance monitoring and establishment of metrics;
- Consider negotiating with the corporation's insurance provider to include "Cyber-Insurance" coverage in the policy [16]. This would provide for reimbursement for many of the costs involved in a security incident. While far from an ideal control, this would at least help to reduce the financial impact of a breach, with little investment required.
- Periodic vulnerability assessments using freely-available software (e.g., nmap, Nessus, Kismet, etc.); and
- Consider the implementation of a shared source Intrusion Detection System (IDS) to be placed on the screened e-mail network segment and/or internal networks. An IDS would be helpful in identifying incidents as they occur, thereby reducing the time required to react to and eliminate the threat, as defined by the Time Based Security (TBS) concept (P > D + R). [17] However, an IDS deployed in these areas are still only a detective control, whereas more ideal preventative controls would focus on tightening the perimeter defense as much as possible (increasing P). In addition, given the limited personnel resources and experience in this are, an effectively deployed IDS may not currently be feasible in the XYZ environment.

Each of these actions can be undertaken at a minimal level of cost and effort to provide significant improvements to the perimeter network security at XYZ. If they are done informally, they can be effective; if policies are prepared to require and enforce such actions, they are more likely to be taken seriously and carried into the future.

[16] http://seattletimes.nwsource.com/html/businesstechnology/134502269_cyberinsurance29.html
[17] Hoelzer, David. Auditing Principles and Concepts

Appendices

Appendix A – Enumeration

Action > identify hostnames through 'host' utility script, run from a Linux shell; infer functions / services provided by systems based on these names, if possible.

lookups.sh:

```
host xxx.238.253.97 >> hostnames.txt
host xxx.238.253.98 >> hostnames.txt
host xxx.238.253.99 >> hostnames.txt
host xxx.238.253.100 >> hostnames.txt
host xxx.238.253.69 >> hostnames.txt
host xxx.238.253.70 >> hostnames.txt
host xxx.238.253.71 >> hostnames.txt
host xxx.238.253.103 >> hostnames.txt
host xxx.238.253.65 >> hostnames.txt
host xxx.238.253.66 >> hostnames.txt
host aaa.97.65.10 >> hostnames.txt
date >> hostnames.txt
```

hostnames.txt:

```
97.253.238.xxx.in-addr.arpa domain name pointer curly.XYZ.org.
98.253.238.xxx.in-addr.arpa domain name pointer moe.XYZ.org.
99.253.238.xxx.in-addr.arpa domain name pointer inet.XYZ.org.
100.253.238.xxx.in-addr.arpa domain name pointer tom.XYZ.org.
Host 69.253.238.xxx.in-addr.arpa not found: 3(NXDOMAIN)
Host 70.253.238.xxx.in-addr.arpa not found: 3(NXDOMAIN)
Host 71.253.238.xxx.in-addr.arpa not found: 3(NXDOMAIN)
Host 103.253.238.xxx.in-addr.arpa not found: 3(NXDOMAIN)
65.253.238.xxx.in-addr.arpa domain name pointer router.XYZ.org.
66.253.238.xxx.in-addr.arpa domain name pointer firewall.XYZ.org.
10.65.97.xxx.in-addr.arpa domain name pointer rrcs-aaa-xxx-97-65-
10.biz.aa.com.
Fri Mar 7 12:14:08 EST 2003
```

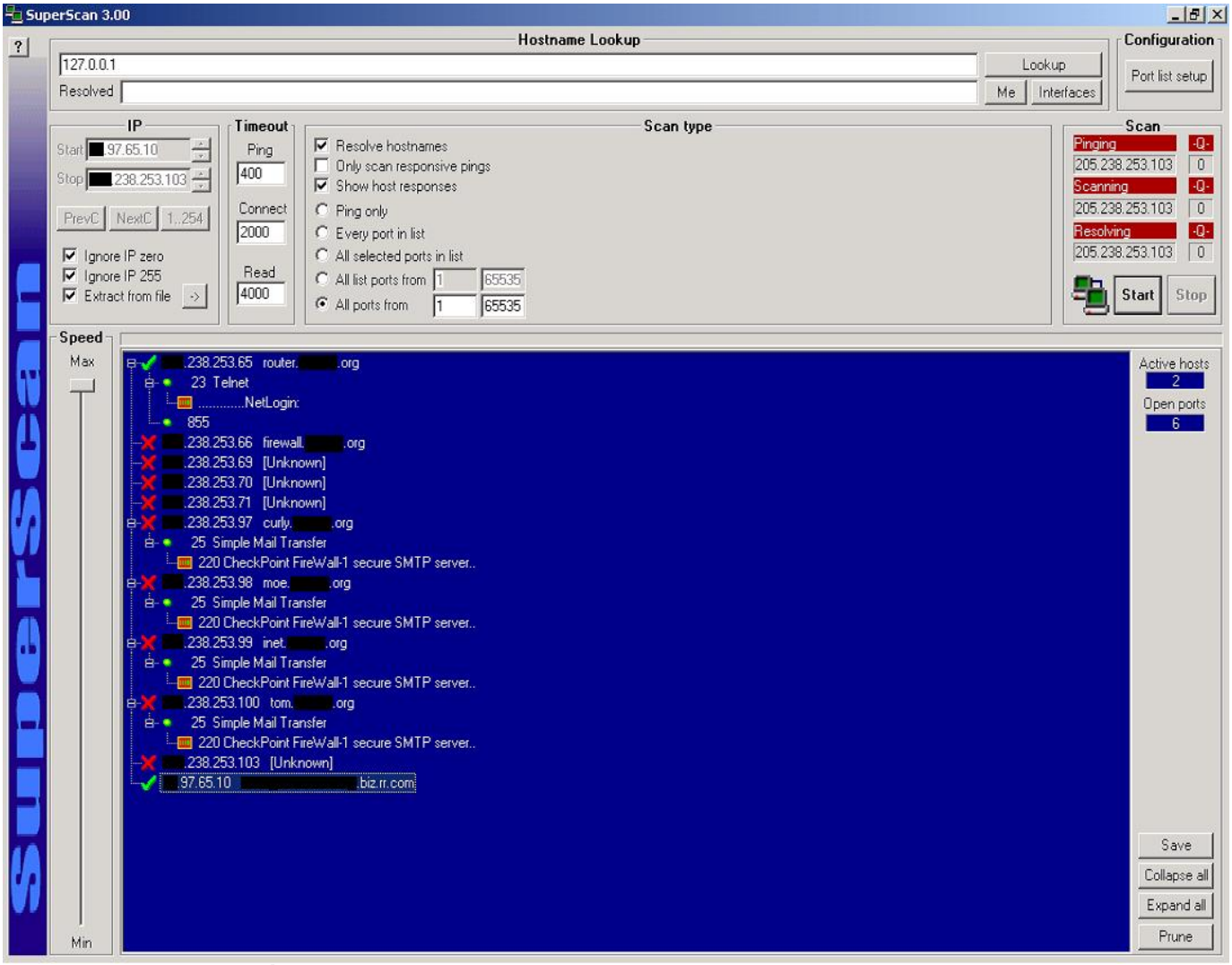
Appendix B – SuperScan port scanning

Action > port scan each identified system to ascertain what ports are open / listening, what service(s) may be running, and what type and version of software are providing these services.

SuperScan 3.00 results saved to text file:

```
* + xxx.238.253.65   router.XYZ.org
        |___    23  Telnet
                |___ .............NetLogin:
        |___   855
  - xxx.238.253.66   firewall.XYZ.org
  - xxx.238.253.69   [Unknown]
  - xxx.238.253.70   [Unknown]
  - xxx.238.253.71   [Unknown]
  + xxx.238.253.97   curly.XYZ.org
        |___    25  Simple Mail Transfer
                |___ 220 CheckPoint FireWall-1 secure SMTP server..
  + xxx.238.253.98   moe.XYZ.org
        |___    25  Simple Mail Transfer
                |___ 220 CheckPoint FireWall-1 secure SMTP server..
  + xxx.238.253.99   inet.XYZ.org
        |___    25  Simple Mail Transfer
                |___ 220 CheckPoint FireWall-1 secure SMTP server..
  + xxx.238.253.100   tom.XYZ.org
        |___    25  Simple Mail Transfer
                |___ 220 CheckPoint FireWall-1 secure SMTP server..
  - xxx.238.253.103   [Unknown]
* - aaa.97.65.10   rrcs-aaa-24-97-65-10.biz.aaa.com
```

SuperScan 3.00 results screen capture:



Appendix C – Nmap scanning

Action > port scans were run against each identified system to determine what ports / protocols were not filtered, and which ports / services might be running to determine potential security issues.

Note > nmap scans were run against each using multiple options / switches in order to ensure that all available information was being gathered, and to reduce false positives. For space considerations, not all results are included here. The different connect type scan results are each displayed for the border router, the only device which provided significant information. Otherwise, sparse results were obtained by each of the scans. Some of the options used include:
-sS (stealth)
-sT (full connect)
-sN (Null)
-sF (Fin)
-sU (UDP)
-sO (IP)
-sA (Ack scan; suggested for firewall scans)
-P0 (no ping)
-v (verbose)
-p 1-65535 (all ports)
-g 20, 22, 25, 53 (source port (FTP-Data, SSH, SMTP, DNS)

Nmap 2.54 results:

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Host curly.XYZ.org (xxx.238.253.97) appears to be down, skipping it.
Host moe.XYZ.org (xxx.238.253.98) appears to be down, skipping it.
Host inet.XYZ.org (xxx.238.253.99) appears to be down, skipping it.
Host tom.XYZ.org (xxx.238.253.100) appears to be down, skipping it.

Nmap run completed -- 4 IP addresses (0 hosts up) scanned in 30 seconds


# nmap 3.20 scan initiated Fri Apr  4 18:33:52 2003 as: nmap -sA -O -F -v -P0
-oN ack.txt xxx.238.253.65
Warning:  OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
Interesting ports on router.xyz.org (xxx.238.253.65):
(The 1158 ports scanned but not shown below are in state: UNfiltered)
Port       State       Service
137/tcp    filtered    netbios-ns
138/tcp    filtered    netbios-dgm
139/tcp    filtered    netbios-ssn
Remote operating system guess: AOS/VS on a Data General mainframe

# Nmap run completed at Fri Apr  4 18:34:17 2003 -- 1 IP address (1 host up)
scanned in 24.500 seconds
```

```
# nmap 3.20 scan initiated Fri Apr  4 18:48:36 2003 as: nmap -sF -O -F -v -P0
-oN fin.txt xxx.238.253.65
Insufficient responses for TCP sequencing (0), OS detection may be less
accurate
Insufficient responses for TCP sequencing (0), OS detection may be less
accurate
Insufficient responses for TCP sequencing (0), OS detection may be less
accurate
Interesting ports on router.xyz.org (xxx.238.253.65):
(The 1158 ports scanned but not shown below are in state: closed)
Port       State       Service
137/tcp    open        netbios-ns
138/tcp    open        netbios-dgm
139/tcp    open        netbios-ssn
No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.20%P=i686-pc-linux-gnu%D=4/4%Time=3E8E1A04%O=137%C=1)
T1(Resp=N)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
T5(Resp=Y%DF=N%W=0%ACK=O%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=AR%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=O%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=54%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=F)


# Nmap run completed at Fri Apr  4 18:49:24 2003 -- 1 IP address (1 host up)
scanned in 48.905 seconds


# nmap 3.20 scan initiated Fri Apr  4 18:49:59 2003 as: nmap -sN -O -F -v -P0
-oN null.txt xxx.238.253.65
Insufficient responses for TCP sequencing (0), OS detection may be less
accurate
Insufficient responses for TCP sequencing (0), OS detection may be less
accurate
Insufficient responses for TCP sequencing (0), OS detection may be less
accurate
Interesting ports on router.xyz.org (xxx.238.253.65):
(The 1158 ports scanned but not shown below are in state: closed)
Port       State       Service
137/tcp    open        netbios-ns
138/tcp    open        netbios-dgm
139/tcp    open        netbios-ssn
No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.20%P=i686-pc-linux-gnu%D=4/4%Time=3E8E1A54%O=137%C=1)
T1(Resp=N)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
```

```
T5(Resp=Y%DF=N%W=0%ACK=O%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=AR%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=O%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=54%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=F)



# Nmap run completed at Fri Apr  4 18:50:44 2003 -- 1 IP address (1 host up)
scanned in 44.928 seconds

# nmap 3.20 scan initiated Fri Apr  4 17:42:20 2003 as: nmap -sU -v -P0 -oN
results.txt xxx.238.253.65
Interesting ports on router.xyz.org (xxx.238.253.65):
(The 1459 ports scanned but not shown below are in state: closed)
Port       State       Service
42/udp     open        nameserver
53/udp     open        domain
67/udp     open        dhcpserver
68/udp     open        dhcpclient
77/udp     open        priv-rje
137/udp    open        netbios-ns
138/udp    open        netbios-dgm
139/udp    open        netbios-ssn
161/udp    open        snmp
162/udp    open        snmptrap
520/udp    open        route

# Nmap run completed at Fri Apr  4 17:42:56 2003 -- 1 IP address (1 host up)
scanned in 36.230 seconds

# nmap 3.20 scan initiated Fri Apr  4 18:44:10 2003 as: nmap -sS -O -F -v -P0
-oN stealth.txt xxx.238.253.65
Interesting ports on router.xyz.org (xxx.238.253.65):
(The 1157 ports scanned but not shown below are in state: closed)
Port       State       Service
23/tcp     open        telnet
137/tcp    filtered    netbios-ns
138/tcp    filtered    netbios-dgm
139/tcp    filtered    netbios-ssn
Remote operating system guess: AOS/VS on a Data General mainframe
TCP Sequence Prediction: Class=trivial time dependency
                         Difficulty=1 (Trivial joke)
IPID Sequence Generation: Incremental

# Nmap run completed at Fri Apr  4 18:44:36 2003 -- 1 IP address (1 host up)
scanned in 26.556 seconds
```

Appendix D – Nessus Scanning

Action > vulnerability scans were run against each identified system to locate potential security issues, assign severity ratings, and identify recommendations.

Nessus results:

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

Scan Details	
Hosts which where alive and responding during test	6
Number of security holes found	0
Number of security warnings found	6

Host List	
Host(s)	**Possible Issue**
xxx.238.253.100	Security warning(s) found
xxx.238.253.99	Security warning(s) found
xxx.238.253.66	Security note(s) found
xxx.238.253.98	Security warning(s) found
xxx.238.253.65	Security warning(s) found
xxx.238.253.97	Security warning(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
xxx.238.253.100	general/tcp	Security warning(s) found
xxx.238.253.100	general/udp	Security notes found

Security Issues and Fixes: xxx.238.253.100		
Type	**Port**	**Issue and Fix**
Warning	general/tcp	The remote host uses non-random IP IDs, that is, it is

		possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things. Solution : Contact your vendor for a patch Risk factor : Low
Informational	general/udp	For your information, here is the traceroute to xxx.238.253.100 : bbb.73.192.1 ccc.30.101.209 ccc.30.101.250 ccc.30.101.187 aaa.48.0.178 aaa.126.168.5 aaa.123.9.78 aaa.122.10.101 aaa.122.12.106 aaa.123.137.21 aaa.125.176.74 ddd.224.123.41 eee.37.155.195 fff.74.34.182 ddd.224.88.102 ?

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
xxx.238.253.99	general/tcp	Security warning(s) found
xxx.238.253.99	general/udp	Security notes found

Security Issues and Fixes: xxx.238.253.99

the ip packets sent by this host.

An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things.

Solution : Contact your vendor for a patch

	aaa.123.9.78 aaa.122.10.101 aaa.122.12.110 aaa.123.137.25 aaa.125.176.74 ddd.224.123.41 eee.37.155.164 fff.74.34.182 ddd.224.88.102 ?

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
xxx.238.253.66	general/tcp	Security notes found

Security Issues and Fixes: xxx.238.253.66		
Type	**Port**	**Issue and Fix**
Informational	general/tcp	The remote host is considered as dead - not scanning

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
xxx.238.253.98	general/tcp	Security warning(s) found
xxx.238.253.98	general/udp	Security notes found

Security Issues and Fixes: xxx.238.253.98		

	ccc.30.101.250 ccc.30.101.187 aaa.48.0.174 aaa.126.168.5 aaa.123.9.78 aaa.122.10.101 aaa.122.12.110 aaa.123.137.25 aaa.125.176.74 ddd.224.123.41 eee.37.155.131 fff.74.34.182 ddd.224.88.102 ?

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
xxx.238.253.65	general/icmp	Security warning(s) found
xxx.238.253.65	general/tcp	Security warning(s) found
xxx.238.253.65	general/udp	Security notes found

Security Issues and Fixes: xxx.238.253.65

Informational	general/udp	For your information, here is the traceroute to xxx.238.253.65 : bbb.73.192.1 ccc.30.101.209 ccc.30.101.250 ccc.30.101.187 aaa.48.0.178 aaa.126.168.5 aaa.123.9.78

	ccc.30.101.250 ccc.30.101.187 aaa.48.0.178 aaa.126.168.5 aaa.123.9.78 aaa.122.10.101 aaa.122.12.106 xxx.238.253.65

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
xxx.238.253.97	general/tcp	Security warning(s) found
xxx.238.253.97	general/udp	Security notes found

Security Issues and Fixes: xxx.238.253.97		
Type	**Port**	**Issue and Fix**
Warning	general/tcp	The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things. Solution : Contact your vendor for a patch Risk factor : Low
Informational	general/udp	For your information, here is the traceroute to xxx.238.253.97 : bbb.73.192.1 ccc.30.101.209 ccc.30.101.250 ccc.30.101.187 aaa.48.0.178 aaa.126.168.5 aaa.123.9.78 aaa.122.10.101 aaa.122.12.110 aaa.123.137.25 aaa.125.176.74 ddd.224.123.41 eee.37.155.164 fff.74.34.182 ddd.224.88.102 ?

This file was generated by Nessus, the open-sourced security scanner.

Appendix E – Firewalk ACL enumeration results

Action > The traceroute-based Firewalk was run against the border router and firewall in an attempt to map out the ACLs of each.

Note > As with the nmap scans, multiple Firewalk scans were run with different options (e.g., source port), but limited results each time. It is apparent that the border router would not allow this traffic through or reply, based on the final response from each scan coming from the local ISP. Only two of the scan results are displayed below, for space purposes.

Firewalk 5.0 results:

```
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
UDP-based scan.
Ramping phase source port: 53, destination port: 33434
Hotfoot through router.xyz.org using firewall.xyz.org as a metric.
Ramping Phase:
expired [bbb.73.192.1]
expired [ccc.30.101.209]
expired [ccc.30.101.250]
expired [ccc.30.101.187]
expired [aaa.48.0.162]
expired [aaa.126.168.5]
expired [tbr2-p012301.wswdc.ip.isp.net]
expired [tbr2-p013701.phlpa.ip.isp.net]
expired [gbr1-p80.phlpa.ip.isp.net]
expired [gar1-p360.phlpa.ip.isp.net]
expired [pos-3-1-0-hrbe.2isp.net]
expired [pos3-0-0-svcr05.2isp.net]
expired [fe4-0-0-svcr04.2isp.net]
expired [s3-0-twnd.2isp.net]
expired [xyz-gw.customer.2isp.net]
*no response*
*no response*
*no response*
*no response*
*no response*
*no response*
*no response*
*no response*
*no response*
*no response*

Total packets sent:                25
Total packet errors:               0
Total packets caught               92
Total packets caught of interest   15
Total ports scanned                0
Total ports open:                  0
Total ports unknown:               0
```

```
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
UDP-based scan.
Ramping phase source port: 53, destination port: 33434
Hotfoot through firewall.xyz.org using inet.xyz.org as a metric.
Ramping Phase:
expired [bbb.73.192.1]
expired [ccc.30.101.209]
expired [ccc.30.101.250]
expired [ccc.30.101.187]
expired [aaa.48.0.174]
expired [aaa.126.168.5]
expired [tbr2-p012301.wswdc.ip.isp.net]
expired [tbr2-p013701.phlpa.ip.isp.net]
expired [gbr2-p30.phlpa.ip.isp.net]
expired [gar1-p370.phlpa.ip.isp.net]
expired [pos-3-1-0-hrbe.2isp.net]
expired [pos3-0-0-svcr05.2isp.net]
expired [fe4-0-0-svcr04.2isp.net]
expired [s3-0-twnd.2isp.net]
expired [xyz-gw.customer.2isp.net]
*no response*
*no response*
*no response*
*no response*
*no response*
*no response*
*no response*
*no response*
*no response*
*no response*

Total packets sent:                25
Total packet errors:               0
Total packets caught               92
Total packets caught of interest   15
Total ports scanned                0
Total ports open:                  0
Total ports unknown:               0
```

Appendix F – SANS Top 20 Common Vulnerable Ports listing

Appendix A - Common Vulnerable Ports In this section, we list ports that are commonly probed and attacked. Blocking these ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far better rule is to block all unused ports. And even if you believe these ports are blocked, you should still actively monitor them to detect intrusion attempts. A warning is also in order: Blocking some of the ports in the following list may disable needed services. Please consider the potential effects of these recommendations before implementing them.

Keep in mind that blocking these ports is not a substitute for a comprehensive security solution. Even if the ports are blocked, an attacker who has gained access to your network via other means (a dial-up modem, a trojan e-mail attachment, or a person who is an organization insider, for example) can exploit these ports if not properly secured on every host system in your organization.

- Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
- RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)
- NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)
- X Windows -- 6000/tcp through 6255/tcp
- Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)
- Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)
- Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)
- "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)
- Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/udp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)
- ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and destination unreachable messages **except** "packet too big" messages (type 3, code 4). (This item assumes that you are willing to forego the legitimate uses of ICMP echo request in order to block some known malicious uses.)

In addition to these ports, block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses, private (RFC1918 and network 127) and IANA reserved addresses. Also block source routed packets or any packets with IP options set.

Appendix G – Physical Security Checklist and Results

Description	**Review data center physical and environmental security controls.**
Testing	Discuss with IT operations personnel what controls are in place, observe controls as possible, and verify effectiveness where practical.
Expected results	Data center should include protective controls such as alarms, cameras, and locks, as well as environmental controls to protect the systems from forces of nature.
Actual results	Adequate physical controls including electronic locks, video cameras, and alarms are in place at the data center. Environmental controls include fire suppression, multiple UPSes, climate control, and raised floors.
Assessment	No exception noted.
Description	**Attempt to gain access to secured data systems.**
Testing	Attempt to "piggyback" behind authorized employees into the restricted data center.
Expected results	Authorized employees should make it their duty to ensure no one follows them into restricted areas and deny access to anyone who attempts to do so.
Actual results	Each followed employee (3) noticed the auditor's attempt to follow them into the data center and demanded to see valid identification; entry was refused, and the door was locked upon lack of I.D.
Assessment	No exception noted.
Description	**Attempt to locate sensitive data on unsecured systems.**
Testing	Briefly examine data residing on public terminals in XYZ's reception area and unsecured office space using 'search' function to locate any sensitive information pertaining to a number of key words, as identified by management.
Expected results	No sensitive data should be accessible from systems outside of the data center or other restricted areas.
Actual results	Among the 13 systems available for public use on the XYZ premises, 4 were found to include some amount of sensitive, but not critical, data. Searching for 12 key words provided by management and manually reviewing each matching file identified these files.
Assessment	Minor exception noted.

Appendix H – Policies Interviews Questions and Results

Action > The following questions were asked of a pre-determined sample of 12 XYZ employees, across all levels and departments of the organization (i.e., staff – executive; IT – Marketing). The questions are purposefully closed-ended, in order to better quantify the results.

Question	**Response**			
	Yes	**No**	**Unsure**	**Abstain**
Are you aware of an XYZ Corporate Security Policy?	**11**	**1**	**-**	**-**
Are you aware of how this policy affects you?	**9**	**2**	**1**	**-**
Are you aware of an XYZ Acceptable Internal Use policy?	**10**	**-**	**2**	**-**
Are you aware of how this policy affects you?	**9**	**1**	**-**	**-**
Have these policies been well-communicated and emphasized to employees?	**6**	**5**	**1**	**-**
Are you aware of any repercussions / enforcement mechanisms regarding adherence to these policies?	**1**	**9**	**2**	**-**
Are you in full compliance with these policies (anonymous response; policies available to review at the time of interview)?	**2**	**7**	**1**	**2**
Are these policies generally regarded as being effective?	**5**	**7**	**-**	**-**

Appendix I – Netstat description and switches

Description > the following text is the DOS prompt output to provide information on the netstat utility and its associated switches.

C:\>netstat -help

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

-a *Displays all connections and listening ports.*
-e *Displays Ethernet statistics. This may be combined with the -s option.*
-n *Displays addresses and port numbers in numerical form.*
-p proto *Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.*
-r *Displays the routing table.*
-s *Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.*
interval *Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.*

The following parameters of the netstat command were used in the audit steps listed herein:

C:\>netstat -an

Appendix J – Fport description and switches

» Fport

Identify unknown open ports and their associated applications
Copyright 2002 (c) by Foundstone, Inc.
http://www.foundstone.com

fport supports Windows NT4, Windows 2000 and Windows XP

fport reports all open TCP/IP and UDP ports and maps them to the owning application. This is the same information you would see using the 'netstat -an' command, but it also maps those ports to running processes with the PID, process name and path. Fport can be used to quickly identify unknown open ports and their associated applications.

Usage:

C:\>fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

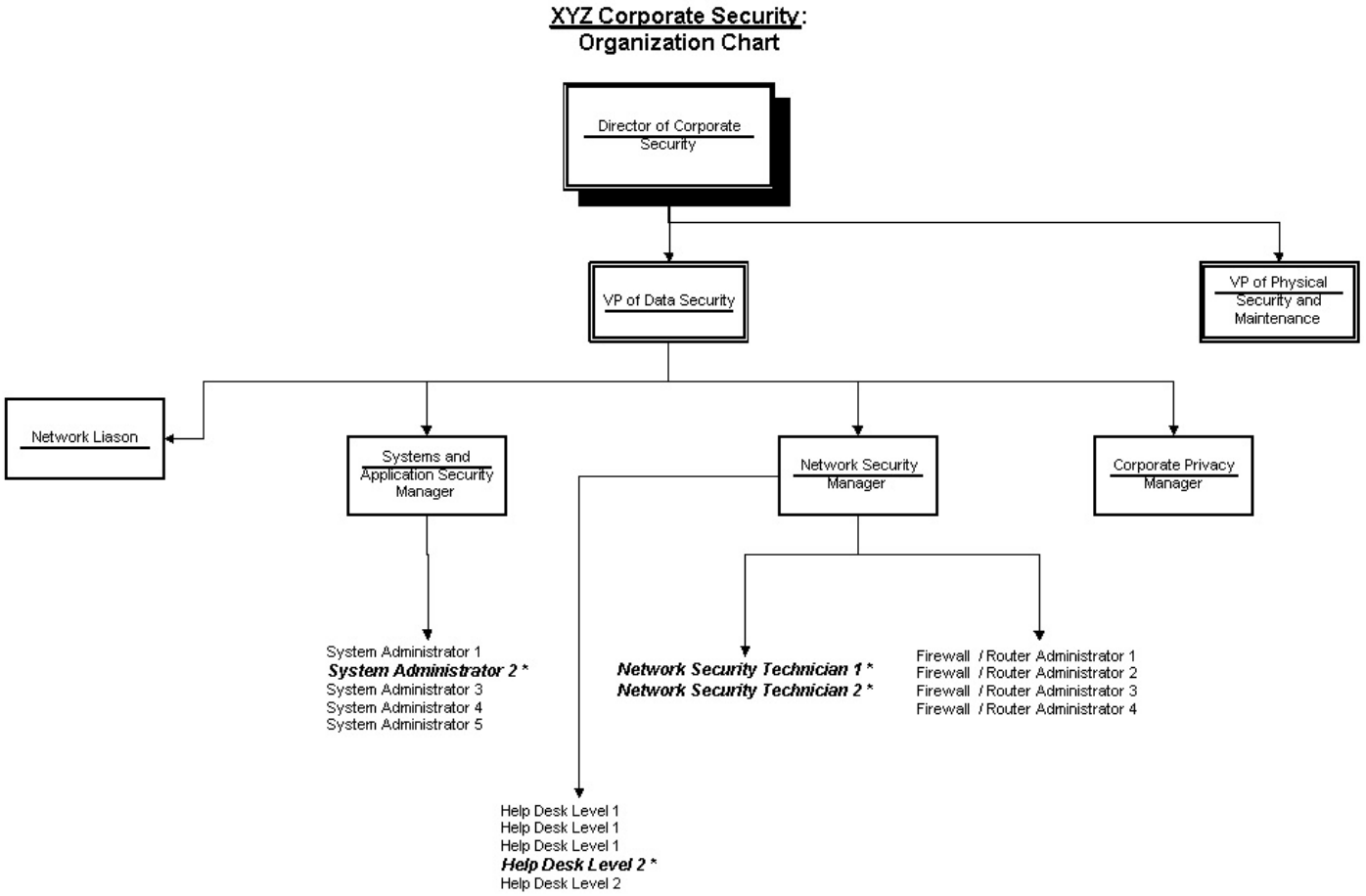
Pid Process Port Proto Path
392 svchost -> 135 TCP C:\WINNT\system32\svchost.exe
8 System -> 139 TCP
8 System -> 445 TCP
508 MSTask -> 1025 TCP C:\WINNT\system32\MSTask.exe
392 svchost -> 135 UDP C:\WINNT\system32\svchost.exe
8 System -> 137 UDP
8 System -> 138 UDP
8 System -> 445 UDP
224 lsass -> 500 UDP C:\WINNT\system32\lsass.exe
212 services -> 1026 UDP C:\WINNT\system32\services.exe

The program contains five (5) switches. The switches may be utilized using either a '/' or a '-' preceding the switch. The switches are;

Usage:
/? usage help
/p sort by port
/a sort by application
/i sort by pid
/ap sort by application path

Appendix K – Information Security Department Organization Chart

(prepared by auditor based on discussion with management and personnel; actual names not included)



** Bold italics indicates a firewall / router adminstrator serving in an additional role*

Appendix L – Ping description and switches

Description > the following text is the DOS prompt output to provide information on the ping utility and its associated switches.

C:\>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] destination-list

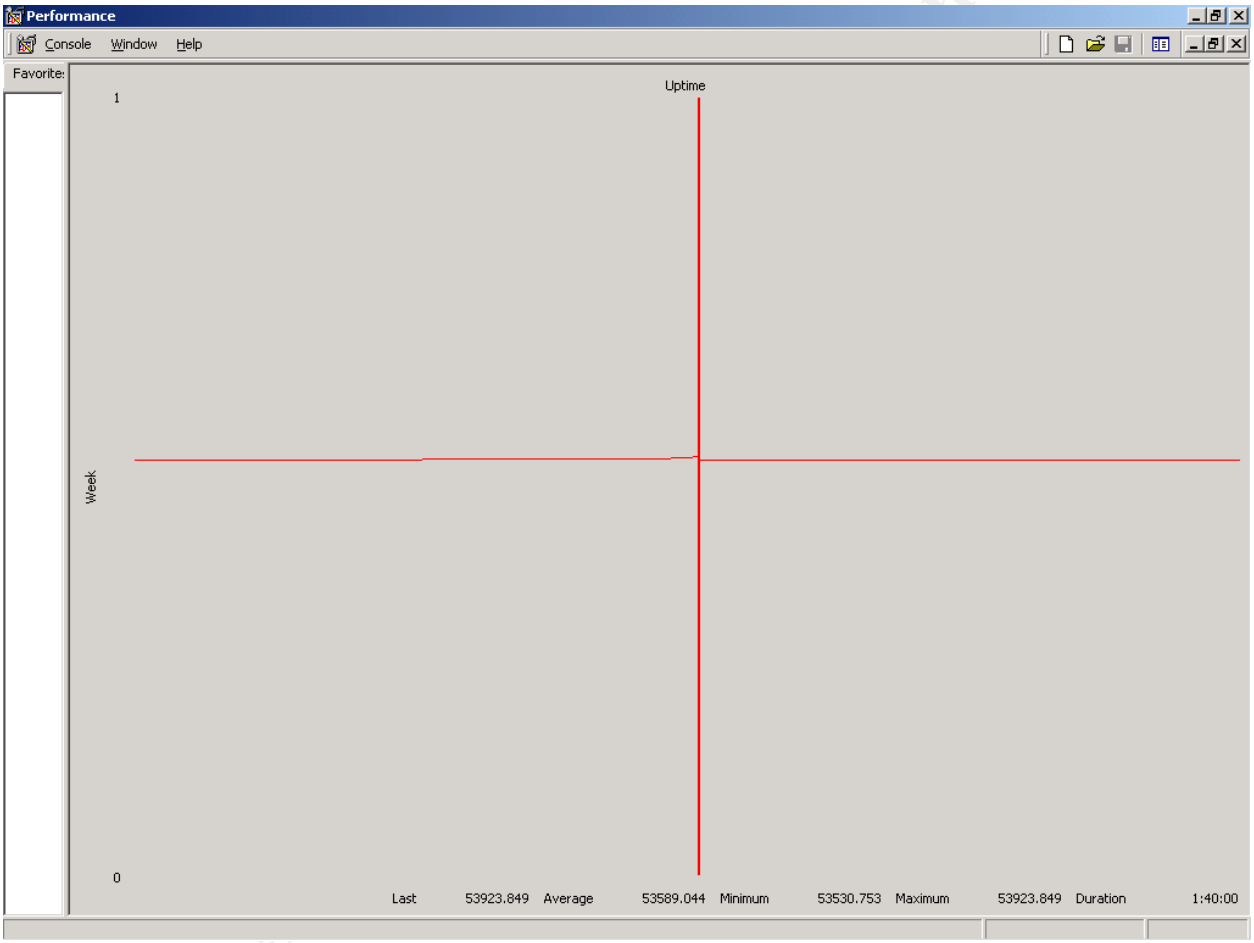
Options:
-t Ping the specified host until stopped.
To see statistics and continue - type Control-Break;
To stop - type Control-C.
-a Resolve addresses to hostnames.
-n count Number of echo requests to send.
-l size Send buffer size.
-f Set Don't Fragment flag in packet.
-i TTL Time To Live.
-v TOS Type Of Service.
-r count Record route for count hops.
-s count Timestamp for count hops.
-j host-list Loose source route along host-list.
-k host-list Strict source route along host-list.
-w timeout Timeout in milliseconds to wait for each reply.

The following parameters of the ping command were used in the audit steps listed herein:

C:\>ping -n 2 -w 5000 system.xyz.org

Appendix M – System Uptime

Description > This is a screenshot of the simple system uptime tracking (using Windows NT Performance Monitor) that was run on the CheckPoint firewall, per the auditor's request (i.e., it is not normally run). The vertical axis was set to measure a week's time, which is how long the system is typically kept up before a brief reboot. Because the monitor was set to update every second, the horizontal slope of the tracking line is extremely low.



Appendix N – Tracert description and switches

Description > the following text is the DOS prompt output to provide information on the tracert utility and its associated switches.

C:\>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:
-d Do not resolve addresses to hostnames.
-h maximum_hops Maximum number of hops to search for target.
-j host-list Loose source route along host-list.
-w timeout Wait timeout milliseconds for each reply.

The following format of the tracert command was used in the audit steps listed herein:

C:\>tracert -w 5000 system.xyz.org

REFERENCES

Printed Sources:

1) Collaborative. Auditing Networks, Perimeters, and Systems Hands-On Workbook. The SANS Institute, 2003.

2) Collaborative. Auditing the Perimeter. The SANS Institute, 2002.

3) Collaborative. Guide to Securing Microsoft Windows NT Networks. Ft. Meade: NSA, September 2001.

4) Fennelly, Carole. Building Your Firewall, Parts 1 - 3. Wizards' Guide to Security: 2001.

5) Green, John. Auditing Networks with Nmap and Other Tools. The SANS Institute, 2002.

6) Hare, Chris, and Siyan, Karanjit. Internet Firewalls and Network Security (2nd Edition). Indianapolis: New Riders Publishing, August 1996.

7) Hoelzer, David. Auditing Principles and Concepts. The SANS Institute, 2002.

8) Hook, Richard. CheckPoint FireWall-1 Work Plan. Vienna: Andersen Worldwide, 19 June 2003.

9) Nelson, Paul. Auditing a Checkpoint Firewall. SANS Online Practical Repository, 7 June 2002.

10) Norton, Peter. Network Security Fundamentals. Indianapolis: SAMS, 2000.

11) Radtke, Ryan, and Richardson, Michael. How to Perform a Network Security Assessment. Vienna: Protiviti, Inc., 31 October, 2002. 19-23, 21-38, 64-89)

12) Tu, James. Auditing a Nokia 440 CheckPoint Firewall-1 Firewall: An Auditor's Perspective. SANS Online Practical Repository, June 2002.

URL materials:

13) Beaver, Kevin. "Firewall best practices." Network Security Tip – Firewall best practices. 11 July 2002.
URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci838215,00.html (18 November 2002).

14) Cavender, Terry. "CheckPoint Firewall Audit Work Program." January 2000.
URL: http://www.auditnet.org/docs/CheckpointFirewall.txt (18 March 2003).

15) Deraison, Renaud. "Nessus manual page." February 2003.
URL: http://www.nessus.org/doc/nessus.html (7 March 2003)

16) Deraison, Renaud. "Nessusd manual page." February 2003.
URL: http://www.nessus.org/doc/nessusd.html (7 March 2003)

17) Fyodor. "The Art of Port Scanning." Nmap: The Art of Port Scanning. 6 September 1997.
URL: http://www.insecure.org/nmap/nmap_doc.html (13 February 2003).

18) Fyodor. "Nmap network security scanner man page."
URL: http://www.insecure.org/nmap/data/nmap_manpage.html (13 February 2003).

19) Lindstedt, Sandy. "Firewall Audit." 15 June 1999.
URL: http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=179 (19 March 2003).

20) Oliphant, Alan. "IT Auditing Without Pain – The Internet – Part 10 – Firewalls." 1 April 2002.
URL: http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=430 (19 March 2003).

23) Ryan, John T. "Security Logs and CheckPoint Firewall-1". 4 June 2001.
URL: http://www.sans.org/rr/firewall/logs.php (18 April 2003).

21) Van Der Kooij, Hugo. "Nessus F.A.Q.." 29 April 2002.
URL: http://www.nessus.org/doc/faq.html (8 March 2003).

22) "Mitigating the SANS / FBI Top Twenty with CheckPoint Software Technologies." 2003.
URL: http://www.checkpoint.com/products/downloads/top20_sans_wp.pdf (17 April 2003).

URL General Research Resources:

URL: http://www.auditnet.org

URL: http://www.cerias.purdue.edu/coast/firewalls/

URL: http://www.cert.org

URL: http://www.cisecurity.com

URL: http://www.phoneboy.com/fom-serve/cache/372.html (mailing list archives)

URL: http://www.theiia.org/itaudit/

URL: http://honor.trusecure.com/pipermail/firewall-wizards/

http://www.firewall-1.org/

http://www.deathstar.ch/security/fw1/

http://www.mrcorp.net/intro_to_CP.htm