



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Auditing Checkpoint NG Firewall

An Auditor's Perspective

GIAC System and Network Auditor (GSNA)
Practical Assignment Version 3.2 Option 1

Jaimin Shah
October 3, 2004

Auditing Checkpoint NG Firewall

An Auditor's Perspective

Table of Contents

<u>Abstract</u>	3
<u>Assignment 1 – Research in Audit, Measurement Practice, and Control</u>	4
1.1 <u>Introduction</u>	4
1.2 <u>System Description and Audit Scope</u>	4
1.3 <u>Security Policy</u>	5
1.4 <u>Network Schema</u>	6
1.5 <u>Evaluate the Risk to the System</u>	7
1.5.1 <u>Threat Identification</u>	7
1.5.2 <u>The Threat Matrix</u>	8
1.6 <u>Current State of the System</u>	10
<u>Assignment 2 – Create an Audit Checklist</u>	12
2.1 <u>Checklist Categories</u>	12
2.2 <u>Physical Security</u>	13
2.3 <u>Security Policy and Documentation</u>	13
2.4 <u>Change Control Management</u>	15
2.5 <u>Firewall Access and Configuration</u>	16
2.6 <u>Firewall Rule-base Validation</u>	19
<u>Assignment 3 – Conduct the Audit</u>	24
3.1 <u>Physical Security</u>	24
3.2 <u>Security Policy and Documentation</u>	26
3.3 <u>Change Control Management</u>	28
3.4 <u>Firewall Access and Configuration</u>	31
3.5 <u>Firewall Rule-base Validation</u>	37
3.6 <u>Residual Risks</u>	46
3.7 <u>Is the System Auditable?</u>	46
<u>Assignment 4 – Follow up Audit Report</u>	47
4.1 <u>Executive Summary</u>	47
4.2 <u>Technical Summary</u>	48
4.3 <u>Audit Findings</u>	49
4.4 <u>Cost Factor</u>	53
4.5 <u>Compensating controls</u>	53
<u>References</u>	55
<u>Appendix A: Security Policy</u>	57
<u>Appendix B: Baseline of the Firewall</u>	58

Abstract

The purpose of this document is to partially fulfill the GIAC Systems and Network Auditor (GSNA) certification. The defense in-depth strategy of the organization includes various devices and technology staged in a layered approach. However, the focus of this document is only on the single perimeter security device to satisfy the detail requirements of GSNA Practical assignment. The document is based on an audit of a Checkpoint firewall that provides security protection for an organization. The document is focused on auditing and comparing the criteria defined in the corporate security policy to the access defined in the firewall policy. The technical aspect of the audit was conducted during August of 2004.

© SANS Institute 2004, Author retains full rights.

Assignment 1 – Research in Audit, Measurement Practice, and Control

1.1 Introduction

This audit was performed on a primary firewall that protects e-commerce business web sites for an organization. The purpose of the firewall is to provide a layer of protection for the corporate e-commerce related assets as well as to facilitate daily traffic from the corporate personnel to maintain the e-commerce operations. The firewall acts as security gateway separating the Internet and the corporate e-commerce environment. The e-commerce assets consist of web servers, application servers and database servers configured and strategically placed in various zones.

In today's fast-paced environment, a business may change its service as well as its needs in a short duration. Ensuring the firewall policy does not lag behind the security policy is a crucial challenge for all security personnel. A routine audit can provide a missing vision for the security personnel. The primary goal of this audit process was to compare the criteria defined in the corporate security policy with the implemented firewall policy. To effectively analyze the corporate security environment an extensive checklist has been developed.

1.2 System Description and Audit Scope

The target of the audit process is running Checkpoint Firewall NG with Application Intelligence (R54). The firewall is deployed on the Nokia security platform IP 530. The role of the firewall is to protect the corporate e-commerce environment. The firewall infrastructure is skillfully architected by deploying a multiple Demilitarized Zones (DMZ) and placing servers in the appropriate DMZ. All traffic to and from the DMZ networks traverses through the firewall. In short, the purpose of the firewall is to act as a security gateway segmenting the Internet and the corporate e-commerce assets.

As per the SANS Auditing Networks, Perimeters and Systems Manual, "Auditing, in general, is best described as the function of measuring something against a standard". In order to audit a firewall device and its operations, an auditor must compare and evaluate against the standards. The standards may vary from business to business; however, organization standards are usually defined in the corporate security policy. The primary objective of this security audit is to compare and analyze the corporate security policy with the established firewall policy. In order to conduct a comprehensive audit, the scope is also focused on analyzing and evaluating the defined security documentation, security policies and the change control management. The audit scope also included evaluating the physical location of the firewall and the enforced surrounding physical and environmental controls.

The scope of this audit does not include auditing or evaluating the base operating systems (OS) of the firewall device. The Checkpoint firewall can be hosted on various platforms such as the Nokia IP security platform, the Windows platform and various flavors of the UNIX platform. As per the Checkpoint NG AI manuals and knowledge base web site, the Checkpoint Firewall-1 can be implemented over various UNIX flavors such as Solaris 8, Linux Kernels version 7.0, 7.2, 7.3 and AIX 5.2.

The firewall devices are usually one component of the layered defense. The defense-in-depth architecture of an organization encompasses various devices and technology staged strategically to provide layers protection. A usual security audit reviews the “big picture” for an organization; however, for this practical assignment, reviewing all of the layered security protection devices is not feasible. Thus, the scope does not concentrate or evaluate other skillfully architected defense in-depth devices.

Assumption: For this scope, assumption is made that all of other devices in the security layered strategy have been appropriately configured and maintained with the best security practices.

The organization has deployed the Checkpoint firewall on the Nokia IP Security Platform. The assumption is made that the underlying base OS has been installed and configured correctly by vendor specific guidelines as well as well known best practices have been applied. The assumption is also made that the base OS is kept up-to-date with vendor recommended security patches. Any exceptions made in the configuration of the base OS is documented and distributed among the security personnel.

Various authors have written SANS practical focusing on the auditing and securing the underlying base OS for the firewall.

Nokia Platform: www.giac.com/practical/Jame_Tu_GSNA.doc

www.giac.org/practical/GSNA/Curtis_Hefflin_GSNA.pdf

Windows Platform: www.giac.org/practical/GSNA/Derek_Geborek_GSNA.pdf

www.giac.org/practical/GSNA/Tamer_Eltoni_GSNA.pdf

UNIX Platform: www.giac.org/practical/GCUX/YongSeok_Oo_GCUX.pdf

www.giac.org/practical/GCUX/Christopher_Talianek_GCUX.pdf

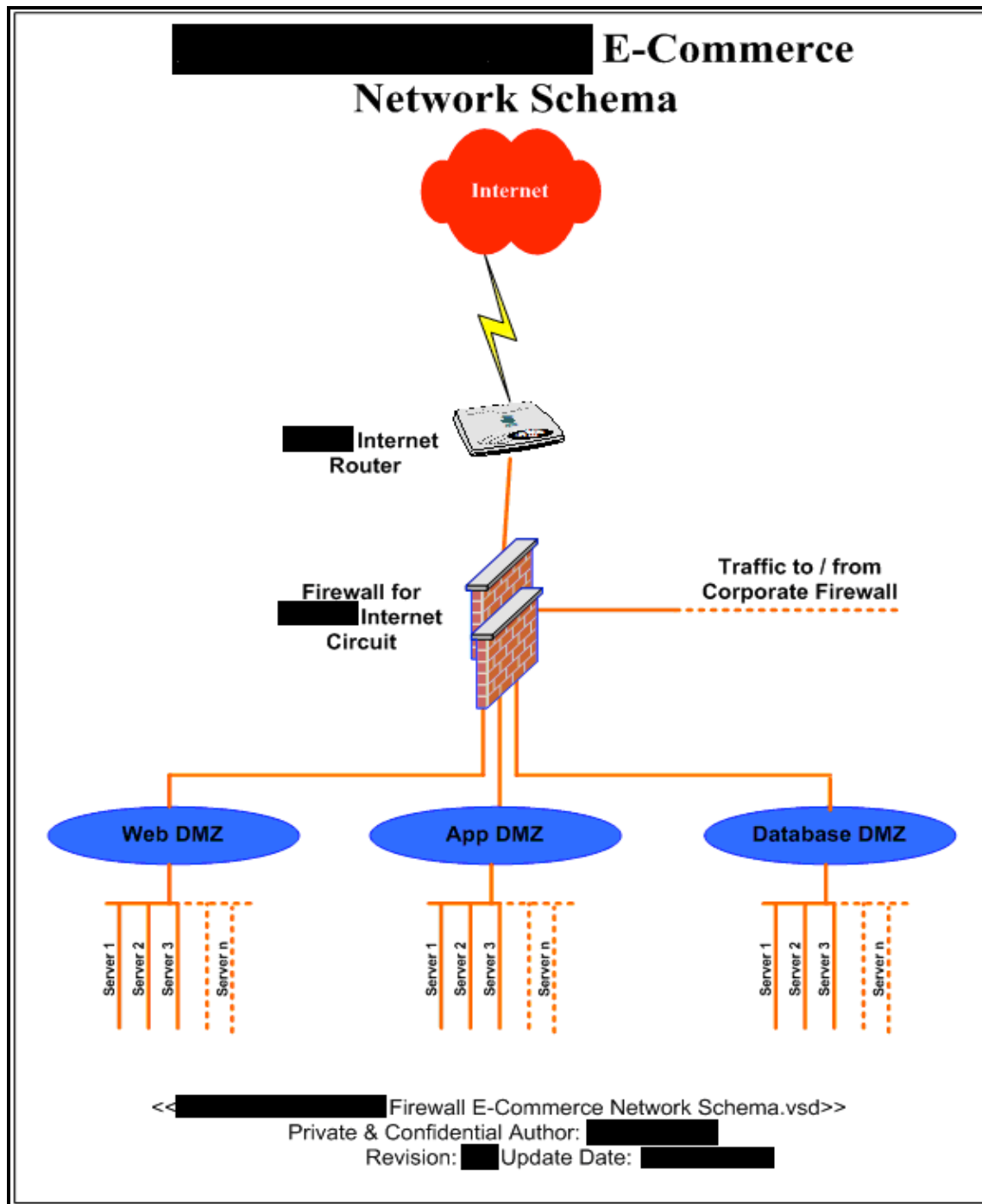
1.3 Security Policy

The security policy is a document that frequently changes to meet the constantly evolving business needs and requirements. Each time a modification made to the security policy, that change should be reflected to all layers of implemented security infrastructure, especially the firewalls. The security policy should be balanced and appropriate (Bennett). An overly weak security policy may prevent a good security implementation, while overly strong security policy may undermine the implementation (Bennett). “A security policy is the set of decisions that collectively determines an organization’s posture toward security” (Cheswick). In general, the security policy should be based on the business requirements analysis, a proper security analysis and a risk analysis.

Security personnel have provided a copy of the corporate security policy. The security policy is sanitized and does not include name or IP address of any devices. A small portion of the organization’s security policy is included in Appendix A.

1.4 Network Schema

The security personnel have provided a sanitized version of the network schema. The network schema does not include any IP address of devices or the make and model of any networking gears. However, it clearly depicts the network traffic flow.



1.5 Evaluate the Risk to the System

In order to evaluate the risk associated with any security devices, it is imperative to understand the role and the purpose of the individual devices. It is essential to document what it is the device protecting and what it can not protect against. In this risk evaluation, the internal servers located in the multi-tier DMZ are considered the critical assets to the organization. There are various audit frameworks available for an auditor to evaluate risk to the systems. The basic risk evaluation starts with the identification of threats and listing the potential impact associated with each threat.

1.5.1 Threat Identification

There are two potential threat factors, or threat sources, that can impact the operation of the firewall services: the natural factor and the human factor. The impact from a threat originating from any of these factors could prove to be detrimental to the firewall service.

The Natural Threat Factor:

- Fire
- Flood
- Hurricane
- Tornado
- Earthquake

The risk associated from the natural threat factor can be easily evaluated against various in place protection measurements. The flood, hurricane, tornado and earthquake are depending on geographical location of the firewall.

The Human Threat Factor

- Internal – Intentional
- Internal – Accidental
- External – Intentional

Treat Source	Motivation / Actor	Potential Impact
Internal – Intentional (Malicious)	Anger, Grudge, Curiosity, Financial gain	Moderate – disclosure / exposure, loss or destruction of data, service outages, theft
Internal – Accidental (Non-Malicious)	None	Low – Loss of data, service outages
External – Intentional (Hackers, Espionage)	Thrill, Challenge, Financial gain	Severe – DoS attacks, disclosure / exposure, loss or destruction of data, service outages, compromised assets

1.5.2 The Threat Matrix

The threat matrix, also known as the risk matrix, is established by listing the likelihood (low, medium, high) and the potential impact level (low, moderate and severe). The potential impact is also elaborated by listing the physical consequences generated by the listed threat factor to the organization. The likelihood vs. the potential impact can also be graphed to provide a detail analysis with the risk associated with the audit scope.

Treat Source	Motivation / Actor	Likelihood	Potential Impact
Natural Disaster	None	Low	Severe – Financial impact, loss of data, service outages, potential damage to the firewall hardware
Disgruntled Admin deliberately leaving security holes or gap in firewall policy	Internal – Intentional	Low	Severe – Financial impact, disclosure / exposure, confidential information leak, compromised assets, potential future attacks (on compromised assets), service outage
Disgruntled Employee launching attacks (such as DoS) from inside the network	Internal – Intentional	Low	Moderate – Financial impact, disclosure / exposure, confidential information leak, compromised assets, service outage
Hacking attempts from inside the network	Internal – Intentional	High	Severe – Financial impact, reputation, disclosure / exposure, compromised assets, potential future attacks (on compromised assets), service outage
Disgruntled Admin or employee gain physical access and shuts down or steal firewalls hardware	Internal – Intentional	High	Moderate – Financial impact, service outage, theft

Admin error in firewall policy (leads to exposure)	Internal – Accidental	Medium	Moderate – Financial impact, disclosure / exposure, compromised assets, potential future attacks (on compromised assets), service outage
Admin error in firewall policy (leads to outages)	Internal – Accidental	Medium	Low – Financial impact, service outage
Admin or employee shuts down firewall or remove the power cables	Internal – Accidental	Low	Low – Financial impact, service outage, potential damage to the firewall hardware
Network based attacks from the Internet	External – Intentional	High	Severe – Financial impact, reputation, disclosure / exposure, service outage
External breach of corporate assets	External – Intentional	High	Severe – Financial impact, reputation, disclosure / exposure, confidential information leak, compromised assets, potential future attacks (on compromised assets), service outage
Deliberate destruction of firewall location / facility	External – Intentional	Low	Severe – Financial impact, service outage, potential damage to the firewall hardware
Hardware failure that leads to service outage	None	Low	Moderate – Financial impact, service outage
Software failure that leads to service outage	None	Low	Moderate – Financial impact, service outage
Service outage from Internet Service Provider	None	Low	Severe – Financial impact, service outage

1.6 Current State of the System

In the auditing process of a security system, a security device or a security architecture, various areas should be thoroughly considered and reviewed. Even though focus and scope of the audit may be the security devices, areas such as defense in-depth strategy, or the “big picture”, should also be reviewed. In the scope of any security device audit, the physical environmental controls, the change management, as well as the security policy and documentation area should not be overlooked.

Audit information on any security device such as a firewall, especially for Checkpoint is relatively easy to research. The Checkpoint firewall is one of the most robust and highly deployed firewalls. Many resources such as books, articles, and various industry standards are available for an auditor. Various known subject matter experts, such as Lance Spitzner, have written articles on auditing the firewalls.

Below are a few of the well-known web sites that can assist in research in auditing the firewalls.

- www.auditnet.org – This web site offers various Audit Programs and checklists written by various auditor and security professionals.
- www.iscaca.com – The Information Systems Audit and Control Association web site offers various publications and standards information for a security auditor. It provides audit guidelines and standards to assist any security auditor.
- www.sans.com/rr – SANS Reading Room offers white papers and articles written by various security professionals. These articles range from providing general subject matter knowledge to the in-depth technical knowledge in the security field.
- www.giac.com – SANS Global Information Assurance Certification web site offers SANS practical papers submitted by numerous authors for various GIAC certifications.
- www.nist.gov – The National Institute for Standards and Technology web site provides various standards publications. The Computer Security Division of the NIST has an extensive list of security publications available via the web site csrc.nist.gov.
- www.securitydocs.com – This web site provides various security arena white papers and articles.
- www.itsecurity.com – This web site offers various white papers, checklist and articles in the security arena.

Below are a few well-known security books and articles that can be used for reference.

- Lance Spitzner – www.spitzner.net – He is one of the subject matter expert in the security arena. His research and articles have provided the basic guidelines in the security and the auditing field.
- “Information Security Management Handbook” By Harold Tipton and Micki Krause– This book is a comprehensive information security handbook and it should be used as reference guide for any security auditor.
- “Firewalls and Internet Security: Repelling the Wily Hacker” By William Checswick, Steven Bellovin and Aviel Ruben – This book provides fundamental understanding of firewalls, policies, threat, as well as providing details on how to protect an organization.

A few of the general resources that can be used for research and reference include:

- www.google.com – An Internet search engine useful in researching and narrowing the subject content.
- www.phoneboy.com – A great general knowledge site focused on the Checkpoint firewall.
- www.checkpoint.com – Checkpoint’s knowledge base articles, user reference guides and manuals offered on their web site for understanding the fundamentals of the Checkpoint firewall.

© SANS Institute 2004, Author retains full rights.

Assignment 2 – Create an Audit Checklist

The purpose of the checklist is to assist one in conducting an audit of the subject listed in the scope. It provides a mechanism for an auditor to remain within the boundaries of the defined scope. The checklist were composed and obtained by comparing the target of the scope to known standards.

2.1 Checklist Categories

The criteria for this checklist is compiled and derived from the personal experience, various posted SANS GSNA practical assignments, generally accepted security practices available from organizations such as ISACA, NSA, NIST, and various known papers written by subject matter experts such as Lance Spitzner. Some of the audit checklist listed below are driven and derived from the organization's established security policy.

The checklist for auditing Checkpoint NG AI Firewall is composed of five major categories:

1. Physical Security
2. Security Policy and Documentation
3. Change Control Management
4. Firewall Access and Configuration
5. Firewall Rule-base Validation

The format of the each audit checklist contains six fields:

1. Checklist Number: Audit checklist number
2. Control Objective: Defined by the organization
3. Reference: Research information
4. Checklist Type: Two possible types for this field: the subjective or the objective
5. Risk: The potential risk associated with the defined control objective
6. Verification / Compliance Criteria: List the audit action or list the detailed steps involved for testing the control objective

2.2 Physical Security

Checklist Number	Physical Security 1
Control Objective	Firewall services should not be hindered by the physical environmental controls.
Reference	Lance Spitzner, James Tu, Personal experience, Generally accepted practices
Checklist Type	Subjective
Associated Risk	Lack of physical environmental controls may result in outage in the firewall services or cause damage to the physical hardware of the firewall.
Verification / Compliance Criteria	Visit the location where the firewall is residing to inspect and measure the placed environmental controls such as temperature, humidity and water. Request an established procedure (if any) that maintains and monitors the environmental controls.

Checklist Number	Physical Security 2
Control Objective	Ensure limited authorized physical access is allowed.
Reference	William Cheswick, Harold Tipton, Terry Cavender, Generally accepted practices
Checklist Type	Objective
Associated Risk	Lack of physical access controls can be detrimental to the firewall operation. Unauthorized personnel can potentially shutdown, remove network cables or steal the firewall hardware. In short, unauthorized personnel access can eliminate the effectiveness of logical security controls surrounding the firewalls.
Verification / Compliance Criteria	Visit the location where the firewall is residing to inspect and measure the placed access controls. Request security personnel to provide information on physical access deployment mechanism (if any). Based on the type of technology used, obtain physical access logs as well as the list of authorized users. Request an established procedure (if any) for assigning approved access to a user.

2.3 Security Policy and Documentation

Checklist Number	Security Policy and Documentation 1
Control Objective	Corporate security policy must be defined indicating traffic to and from the protected network. The firewall policy must be derived from the criteria listed in the corporate security policy.
Reference	William Cheswick, Rose Collin, Bennett Todd, Personal experience, Generally accepted practices

Checklist Type	Objective
Associated Risk	In general, the implementation of the firewall policy should be the enforcement of the security policy. If the firewall policy is not derived and shaped from the corporate security policy, potential unauthorized or uncontrolled access may exist to and from the protected network. Such undocumented access may potentially jeopardize the organization's overall security posture.
Verification / Compliance Criteria	Is there a corporate security policy defined? Is the security policy defined to specifically allow authorized traffic to and from the protected networks? Request the security personnel to provide a copy of the corporate security policy. Note: Most organizations will not provide a hard copy of the firewall policy. Review the firewall policy along with the security personnel.

Checklist Number	Security Policy and Documentation 2
Control Objective	Any proposed changes to the security policy must be appropriately reviewed, approved and documented by the security team members prior to implementing changes on the firewall.
Reference	Bennett Todd, John Wack, Personal experience, Generally accepted practices
Checklist Type	Objective
Associated Risk	The lack of a through review process for assessing the risk associated with the proposed changes may lead to exposure for the protected assets. In short, any unapproved, undocumented changes may potentially jeopardize the organization's overall security posture.
Verification / Compliance Criteria	Request security personnel to provide established procedure for updating the corporate security policy. Verify that proposed changes are being documented as well as approved by the security team members. Note: In most organizations, the approval process is accomplished via email. Request security personnel to provide previous emails indicating the approval process.

Checklist Number	Security Policy and Documentation 3
Control Objective	A backup policy and procedure must be defined to backup the firewall configuration, firewall policy and firewall logs.
Reference	Bennett Todd, Harold Tipton, Rose Colin, Corporate objective, Personal experience, Generally accepted practices
Checklist Type	Objective

Associated Risk	<p>The written backup policy and procedure ensures crucial firewall operation related files are being backed up at routine interval. Not having appropriate backup procedure may cause an outage in the firewall services in the event of disaster. Such outage in firewall services may result in loss of productivity, and/or potential attacks to corporate assets leading to a financial impact.</p> <p>The firewall logs may contain potential evidence or a trend that may be needed in case of any forensic investigation.</p>
Verification / Compliance Criteria	Request the security personnel to provide a copy of established backup policy and procedure. Review the details of the back up policy and procedures. Request an established procedure (if any) for restoring the backup files.

2.4 Change Control Management

Checklist Number	Change Control Management 1
Control Objective	Firewall policy must not be modified unless the proposed changes are approved by the security personnel.
Reference	Corporate Objective, Personal experience, Generally accepted practices
Checklist Type	Objective
Associated Risk	If the firewall policy is being updated without an authorization and approval process, potential unauthorized access may exist to and from the protected network. Such undocumented access may potentially jeopardize the organization's overall security posture.
Verification / Compliance Criteria	Request the security personnel to provide previous email communications indicating the approval or the authorization process for the proposed changes to firewall policy. Request and review the security policy documenting such requirements.

Checklist Number	Change Control Management 2
Control Objective	Any modification to the firewall policy must be tracked and thoroughly documented.
Reference	SANS, Lance Spitzner, Terry Cavender, Personal experience, Generally accepted practices
Checklist Type	Objective/Subjective
Associated Risk	An audit trail or log for tracking changes assists during troubleshooting. Also, documenting all changes may assist in the event of disaster.
Verification / Compliance Criteria	<p>Request the security personnel to provide copy of the established tracking document. Also, obtain a snapshot of the firewall audit logs depicting changes made by the security personnel.</p> <p>Note: The audit logs are one of the three types of logs recorded by the Checkpoint firewall log monitoring utility, the Checkpoint SmartView Tracker.</p>

Checklist Number	Change Control Management 3
Control Objective	Any firewall vendor patches or OS vendor patches must be approved or authorized prior to implementing on the firewall.
Reference	Personal experience, Generally accepted practices
Checklist Type	Objective/Subjective
Associated Risk	Even though patches and services packs may be critical to operations, applying them without testing and approval process may result in outage in firewall services. An outage in firewall services may result in loss of productivity and/or potential attacks to corporate assets leading to a financial impact.
Verification / Compliance Criteria	Request the security personnel to provide pervious emails communication indicating the approval or the authorization from security personal on the patch implementation. Request established procedure (if any) for the security patch management and implementation.

2.5 Firewall Access and Configuration

Checklist Number	Firewall Access and Configuration 1
Control Objective	Only authorized security personnel from the preconfigured hosts may be permitted to access and manage the firewall policy.
Reference	Harold Tipton, Checkpoint Manuals, Personal experience, Generally accepted practices
Checklist Type	Objective
Associated Risk	Firewall policy access must be restricted to ensure that firewall is not susceptible to potential exploits.
Verification / Compliance Criteria	Request security personnel to provide a list of all firewall administrators with the assigned access rights. To obtain the user access information, various available methods can be used. For example, execute the “CPCONFIG” command on the Checkpoint management server. Request an established procedure (if any) for assigning approved access to a user.

Checklist Number	Firewall Access and Configuration 2
Control Objective	Any remote management of the firewall must be conducted over secure protocols.
Reference	Harold Tipton, Lance Spitzner, William Cheswick, Personal experience, Generally accepted practices
Checklist Type	Objective

Associated Risk	If remote management traffic is not conducted over secure protocols, someone on the network can potentially capture network traffic and may gain access to the firewall architecture.
Verification / Compliance Criteria	Request security personnel to provide established procedure (if any) for the remote management. If the established procedure does not exist, request security personnel to show the “step-by-step” remote management. Note: There are multiple ways to manage a firewall operation. Identify the established firewall management technology. Based on the implemented technology, request to provide few snapshots of the daily remote management.

Checklist Number	Firewall Access and Configuration 3
Control Objective	Stay up-to-date on the firewall vendor recommended patches.
Reference	Terry Cavender, Checkpoint website, Generally accepted practices
Checklist Type	Objective
Associated Risk	If the firewall software is not up-to-date with the latest vendor specific patches and hotfixes, the firewall may be susceptible to exploits based on newly discovered vulnerabilities. The latest patch from a vendor may provide a fix to the latest identified vulnerabilities or potential bug fixes.
Verification / Compliance Criteria	Request the security personnel to provide a list of the existing version and build information of the Checkpoint firewall. Compare to the latest information available on the vendor's Website. To obtain the firewall version information, various methods can be used. For example, the detailed version stamp can be obtained by the Checkpoint firewall SmartView Update utility. Note: There may be various legitimate reasons for not patching firewalls to the latest patch. Request security personnel to provide documented exceptions for any required patches that are not deployed.

Checklist Number	Firewall Access and Configuration 4
Control Objective	Firewall architecture must provide high availability for the business mission critical services. Firewalls must not become a single point of failure.
Reference	SANS Manuals, Personal experience, Generally accepted practices
Checklist Type	Objective
Associated Risk	Firewall services are crucial to daily e-commerce business operations. Outage in the firewall services may result in loss of productivity and/or potential attacks to corporate assets leading to a financial impact.

Verification / Compliance Criteria	<p>Review the provided network schema for fault tolerance or high availability configuration. Request the security personnel to provide additional details to support the objective.</p> <p>Note: There are multiple ways to architect a fault tolerance firewall infrastructure. Identify the implemented technology providing high availability. Based on the implemented technology, request to schedule a high availability or fail over test.</p>
---	--

Checklist Number	Firewall Access and Configuration 5
Control Objective	Firewall policy, firewall logs and firewall configuration must be routinely backed up.
Reference	Lance Spitzner, Rose Colin, Personal experience, Generally accepted practices
Checklist Type	Objective
Associated Risk	<p>Not having the appropriate backup may result in outage in firewall services in the event of disaster. Outage in firewall services may result in loss of productivity, and/or potential attacks to corporate assets leading to a financial impact.</p> <p>The firewall logs may contain potential evidence or a trend that may be needed in case of any forensic investigation.</p>
Verification / Compliance Criteria	<p>Request security personnel to provide a copy of established firewall backup policy and procedures. Request security personnel to provide verification indicating firewall logs, firewall policy and firewall configuration files are being backed up at defined routine interval.</p> <p>Note: Verification may be an automated email by the backup software indicating files are being backed up at routine interval.</p>

Checklist Number	Firewall Access and Configuration 6
Control Objective	Routinely review the firewall policy and the security policy.
Reference	Bennett Todd, Corporate Objective, Personal experience, Generally accepted practices
Checklist Type	Objective
Associated Risk	The security policy and firewall policy should be reviewed at defined intervals. It provides a mechanism to modify or adjust the policies, if needed. The review process identifies any violations in the policies and allows an opportunity to correct them. In short, if the security policy and the firewall policy are routinely reviewed, then it will improve the security posture of the organization.
Verification / Compliance Criteria	<p>Request security personnel to provide a copy of established procedures (if any) on reviewing the firewall policy and the security policy. Request a verification indicating that the control objective is being enforced.</p> <p>Note: Is the review interval specifically defined in the security policy?</p>

Checklist Number	Firewall Access and Configuration 7
Control Objective	Firewall logs must be routinely reviewed.
Reference	Lance Spitzner, Personal experience, Generally accepted practices
Checklist Type	Objective / Subjective
Associated Risk	Firewall logs provide a wealth of information on any potential security intrusions / incidents. Firewall logs also provide a tool for troubleshooting for any access issues. Routinely reviewing firewall logs also identifies any violations in both of the security policy and the firewall policy.
Verification / Compliance Criteria	Request security personnel to provide established procedure (if any) on monitoring the firewall logs. Request to provide verification indicating that the control objective is being enforced.

2.6 Firewall Rule-base Validation

Checklist Number	Firewall Rule-base Validation 1
Control Objective	Ensure that the Stealth Rule is in place to protect against the attacks that are aimed at the firewall.
Reference	Lance Spitzner, Terry Cavender, Checkpoint Manuals, Personal experience, Generally accepted practices
Checklist Type	Objective
Associated Risk	The Stealth Rule should be placed at the top of the rule base. As Checkpoint Manuals indicate that the Stealth Rule “protects your firewall from port scanning, spoofing and other types of direct attacks”. If the stealth rule is not defined, the firewall itself is not protected against vast directed attacks.
Verification / Compliance Criteria	Review the firewall policy with security personnel to ensure the existence of the Stealth Rule and relative location of the stealth rule in the rule base. Note: Only rules that required a direct connection to the firewall should be defined above the Stealth Rule.

Checklist Number	Firewall Rule-base Validation 2
Control Objective	Ensure that the Drop Rule or Cleanup Rule is place to explicitly drop the “undefined” traffic.
Reference	Lance Spitzner, Checkpoint Manuals, Personal experience
Checklist Type	Objective

Associated Risk	Corporate policy indicates that only explicitly defined traffic is allowed to and from the protected network. As Checkpoint manuals indicate that by placing the cleanup rule “the firewall drops all communication attempts that do not match a rule”.
Verification / Compliance Criteria	Review the firewall policy with security personnel to ensure the existence of the drop rule. Note: For the Drop Rule or the Cleanup Rule to be effective, it should be placed as the last rule in the rule base. Ensure that detail logging is enabled for the Drop Rule or the Cleanup Rule.

Checklist Number	Firewall Rule-base Validation 3
Control Objective	Any inbound traffic to the protected network must correspond to the approved and authorized inbound traffic rules defined in the security policy.
Reference	Corporate objective, Personal experience
Checklist Type	Objective
Associated Risk	Any undocumented or unauthorized traffic access may jeopardize the organization's overall security posture.
Verification / Compliance Criteria	Review the firewall policy with security personnel. Compare the inbound traffic requirement listed in the security policy with the inbound access rules defined in the firewall policy. Identify any anomalies in either the firewall policy or the security policy. Note: Additional inbound firewall policy verification can be accomplished via any available third party scanners, such as NMAP.

Checklist Number	Firewall Rule-base Validation 4
Control Objective	Any outbound traffic from the protected network must correspond to the approved and authorized outbound traffic rules defined in the security policy.
Reference	Corporate objective, Personal experience
Checklist Type	Objective
Associated Risk	Any undocumented or unauthorized traffic access may jeopardize the organization's overall security posture.
Verification / Compliance Criteria	Review the firewall policy with security personnel. Compare the outbound traffic requirement listed in the security policy with the outbound access rules defined in the firewall policy. Identify any anomalies in either the firewall policy or the security policy. Note: Additional outbound firewall policy verification can be accomplished via any available third party scanners, such as NMAP.

Checklist Number	Firewall Rule-base Validation 5
-------------------------	--

Control Objective	Firewall must provide an audit trail of all traffic (except noise traffic).
Reference	Lance Spitzner, Corporate objective, Personal experience
Checklist Type	Objective
Associated Risk	Firewall logs are vital source of data for troubleshooting and reporting any security intrusion or incident. Firewall logs may also contain potential evidence that may be needed in case of any forensic investigation.
Verification / Compliance Criteria	Review the firewall policy and firewall logs with security personnel. Identify that all inbound and outbound rules in the firewall policy have logging enabled. Request the security personnel to provide the firewall logs indicating the inbound and the outbound traffic is being logged. Note: The noise traffic may not necessarily be logged.

Checklist Number	Firewall Rule-base Validation 6
Control Objective	Firewall logs or the audit trail must include any action taken by security personnel.
Reference	Jeff Lowder, Corporate objective, Personal experience
Checklist Type	Objective
Associated Risk	Firewall logs are vital source of data for troubleshooting and reporting security intrusion or incident. Logging and capturing all actions taken by the administrator with time stamp provides detail audit trail. Audit tails may provide sufficient information during the recovery process in case of accidental or intentional actions taken by the administrator (as indicated in the threat matrix section).
Verification / Compliance Criteria	Review the firewall policy and the firewall logs with security personnel. Request the security personnel to provide the firewall logs indicating actions taken by security personnel. Note: Checkpoint firewall audit logs tracks every action taken by the firewall administrators.

Checklist Number	Firewall Rule-base Validation 7
Control Objective	Firewall should be configured to protect against potential network based Denial of Services (DoS) attacks.
Reference	Lance Spitzner, Checkpoint Manuals, Personal experience, Generally accepted practices
Checklist Type	Objective / Subjective
Associated Risk	In general, the firewalls are prone to receive flood of attack attempts. The firewall design should be resilient enough to protect against these attacks. The network based Denial of service (DoS) attacks are mainly aimed to cause an outage in the firewall services. A layer of protection should be placed and configured to defend the firewall operations against the known network based DoS attacks and any future unknown attacks.

Verification / Compliance Criteria	<p>There are various mechanisms in the defense in-depth strategy that can be in placed to prevent against the network based DoS attacks. Identify the implemented technology that provides the layer of protection.</p> <p>Checkpoint offers a Smart Defense Subscription that can be purchased and implemented. As Checkpoint Manuals, the Checkpoint Smart Defense Subscription allows organization to block various types of known network attacks and entire categories of emerging or unknown attacks.</p> <p>Has the Checkpoint Smart Defense subscription been purchased? If the Checkpoint Smart Defense is purchased, request security personnel to provide an evidence of the subscription update dates. Review the defined firewall Smart Defense policy with the security personnel. Verify that Smart Defense is kept up to date.</p> <p>If the Checkpoint Smart Defense Subscription is not purchased, identify and list the implemented technology providing the layer of protection.</p>
---	--

Checklist Number	Firewall Rule-base Validation 8
Control Objective	All interfaces of the firewall must be configured with Anti-Spoofing capabilities.
Reference	William Cheswick, Tipton Harold, Personal experience, Generally accepted practices
Checklist Type	Objective
Associated Risk	To protect the firewall from any potential spoofing attacks, all interfaces should be configured with Anti-Spoofing capabilities. An improperly configured firewall may not provide a sufficient protection layer to prevent against various types of known spoof attacks.
Verification / Compliance Criteria	<p>Request security personnel to provide a few snapshots of Anti-Spoofing configuration. Review the firewall policy with security personnel.</p> <p>Note: An Anti-Spoofing configuration can be verified via multiple methods, such as the firewall rule-base, as well as the Smart Defense subscription configuration.</p>

Checklist Number	Firewall Rule-base Validation 9
Control Objective	Firewall should be configured to hide the internal network architecture.
Reference	Lance Spitzner, Jeff Lowder, Personal experience, Generally accepted practices
Checklist Type	Objective / Subjective
Associated Risk	Various methods, including the Network or Protocol Address Translation (NAT/PAT), should be used by the firewalls to protect internal network architecture. Implementing various “hiding” mechanisms provides a layer of protection from an attacker to address sweep or map the internal resources.

Verification / Compliance Criteria	<p>Request security personnel to provide snapshots indicating the implemented technology to hide the protected networks. Review the firewall policy and the firewall logs with security personnel to verify as well as list the “hiding” mechanism that is being implanted.</p> <p>Note: There are various techniques can be utilized to hide the internal network infrastructure. The most common methodology used to hide internal protected network assets is called the Network Address Translation or the Port Address Translation (NAT/PAT).</p>
---	--

Checklist Number	Firewall Rule-base Validation 10
Control Objective	Routinely review and remove any temporary rules created in the firewall policy.
Reference	Corporate Objective, Personal experience, Generally accepted practices
Checklist Type	Objective / Subjective
Associated Risk	There may be a need for temporary rules for troubleshooting or testing. However, if the temporary rules are not routinely reviewed and removed, potential unauthorized access may exist to and from the protected network. Such undocumented access may potentially jeopardize the organization's overall security posture.
Verification / Compliance Criteria	Review the firewall policy with security personnel. Compare the inbound and the outbound traffic requirements listed in the security policy with the inbound and the outbound access defined in the firewall policy. Identify and discuss the purpose for the temporary rules. Are there any timelines defined to remove the temporary rules? Are the temporary rules removed by the defined timeline?

Even though the scope of this audit is focused on the Checkpoint NG AI Firewall protecting the e-commerce environment of an organization, the majority of the above checklists can be remolded and reapplied towards Checkpoint NG AI Firewall configured in various other capacities. Also, some of the above listed checklists can be utilized for the other firewall technologies offered by vendors such as Cisco PIX, Juniper / NetScreen, or Symantec.

Assignment 3 – Conduct the Audit

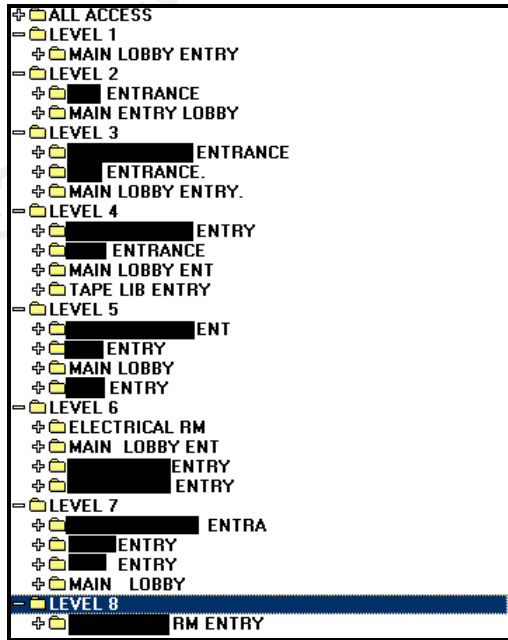
Establishing the audit checklist is the most complex element during the security audit. As the SANS Auditing Networks, Perimeters and Systems Manuals indicated that if the research or the audit planning is successfully done, the fieldwork should be simple to do. Since the audit boundaries have already been defined in the checklists, conducting audits is relatively easy.

The format of the actual audit checklist contains six fields.

- Checklist Number: Audit checklist number
- Control Objective: Defined by the organization
- Expected Results: List the expected results
- Actual Results: List actual results based on conducted audit
- Comments: Any additional comments from the security personnel or the auditor to support results of the conducted audit
- Pass / Fail / Pass with a caution flag: Did the audit findings meet the control objective?

3.1 Physical Security

Checklist Number	Physical Security 1
Control Objective	Firewall services should not be hindered by the physical environmental controls.
Expected Results	An organization must provide adequate environmental and physical controls to protect the firewalls from naturally occurring conditions (such as temperature, humidity), natural disasters (such as hurricane, tornado), fire, flood and from malicious destruction.
Actual Results	<p>The following information was obtained during the interview process with various security team members as well as visiting the organization's data center.</p> <ul style="list-style-type: none"> • The firewalls are located in the Computer Room of the Data Center building. • The Computer Room has the established climate controls to monitor temperature, humidity and moisture to protect the physical firewalls as well as other network and server infrastructure. • The Computer Room is architected with the fire barrier walls. • Organization has established an Operation Department who is responsible to monitor and maintain the environmental control variables.
Comments	
Pass / Fail	Pass – Audit met the control objective

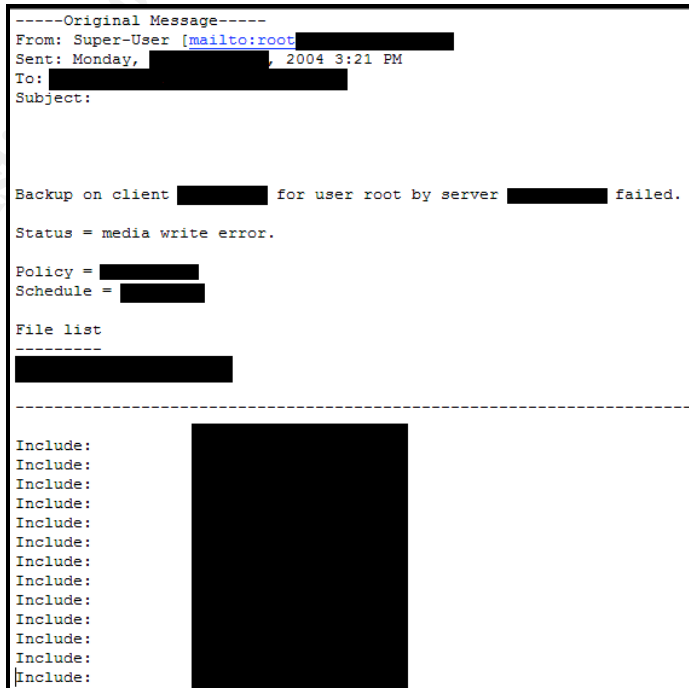
Checklist Number	Physical Security 2
Control Objective	Ensure limited authorized physical access is allowed.
Expected Results	An adequate physical access control provides a security barrier to the firewall operations. It deters an attacker's attempts to defeat any logical controls placed on the firewall.
Actual Results	<p>The following information was obtained during the interview process with various security team members as well as visiting the organization's data center.</p> <ul style="list-style-type: none"> Organization has developed a physical badge system and the badge assignment and monitor process is maintained by the Operation Department. Only authorized employees have access to the Data Center. Not all of the employees of the Data Center have access to the Computer Room. Only authorized and approved employees have access to the Computer Room. Operations Department has placed cameras at various strategic locations to monitor the activity around the Data Center and the Computer Room. <p>Below snapshot depicts the various defined physical access levels for the organization's data center.</p> 
Comments	The physical access badges do not have employee pictures or the assigned badges are not color coded for access. Both of these parameters may add visibility and thus improve the surrounding overall physical security. However, the presented evidence was sufficient to meet the defined control objective.
Pass / Fail	Pass – Audit met the control objective

3.2 Security Policy and Documentation

Checklist Number	Security Policy and Documentation 1
Control Objective	Corporate security policy must be defined indicating traffic to and from the protected network. The firewall policy must be derived from the criteria listed in the corporate security policy.
Expected Results	The Security Policy and Documentation governs the traffic flow by the firewall. "Your security policy is the single most important part of your firewall setup, and indeed your overall security stance" (Bennett). Todd Bennett also indicated that "does your policy permit anything that's not explicitly prohibited, or does it prohibit everything that's not explicitly permitted?" Most security policy should be around the second premises.
Actual Results	<p>The following information was obtained during the interview process with various security team members as well as reviewing the corporate security policy.</p> <ul style="list-style-type: none"> • A small portion of the corporate security policy is listed in Appendix A. • Security Department has a well defined security policy specifically allowing access to and from the protected networks. • As per the security personnel, the majority of the firewall policy rules are derived from the access detailed in the security policy.
Comments	
Pass / Fail	Pass – Audit met the control objective

Checklist Number	Security Policy and Documentation 2
Control Objective	Any proposed changes to the security policy must be appropriately reviewed, approved and documented by the security team members prior to implementing changes on the firewall.
Expected Results	A written procedure indicating the approval process for implementing changes on the security policy.
Actual Results	<p>The following information was obtained during the interview process with various security team members.</p> <ul style="list-style-type: none"> • All proposed changes to the security policy are approved by the security personnel. Majority of the approval process is accomplished via email. • Any proposed changes to the security policy are being appropriately documented. • The submitted email communication indicates the request for proposed security policy changes as well as approval response from the security personnel. • Due to the confidential information contained within the email communication, the evidence is not presentable for this practical.

Comments	All proposed changes are approved by the security personnel prior to implementing changes on the firewall. Even though it is not required by the control objective, a document should be developed to track all proposed changes made to the security policy.
Pass / Fail	Pass with a caution flag – See comments

Checklist Number	Security Policy and Documentation 3
Control Objective	A backup policy and procedure must be defined to backup the firewall configuration, firewall policy and firewall logs.
Expected Results	A written backup procedure indicating the criteria for backing up the firewall configuration, firewall policy and firewall logs.
Actual Results	<p>The following information was obtained during the interview process with various security team members.</p> <ul style="list-style-type: none"> Part of the corporate security policy addresses the backup policy; however, there is no backup procedure defined by the security personnel. There are no written documents indicating or suggesting a list of crucial files that needs to be backed up routinely. Even though there is not defined backup procedure, the crucial files are being backed up at routine interval. Backup software is configured to send automated email indicating all successful and any failures encountered during the backup process. <p>Below snapshot depicts an automatically generated email from the backup solution listing the files and the servers that are being backed up.</p>  <p>The screenshot shows an email titled '-----Original Message-----' from 'Super-User [mailto:root@redacted]' sent on Monday, 2004 3:21 PM. The subject is redacted. The body of the email states: 'Backup on client [redacted] for user root by server [redacted] failed. Status = media write error. Policy = [redacted] Schedule = [redacted]'. It then lists a 'File list' with a redacted box. At the bottom, there is a list of 'Include:' statements followed by a large redacted box.</p>

Comments	Security policy has addressed some information on the backup policy. Even though the firewall configuration, the firewall policy and the firewall logs are being backed up, there are no supporting defined backup procedures. The control objective clearly indicates that written backup procedures must be present.
Pass / Fail	Fail – See Comments

3.3 Change Control Management

Checklist Number	Change Control Management 1
Control Objective	Firewall policy must not be modified unless the proposed changes are approved by the security personnel.
Expected Results	A process indicating a request or a proposal for change as well as a process indicating the approval mechanism.
Actual Results	<p>The following information was obtained during the interview process with various security team members.</p> <ul style="list-style-type: none"> • All proposed changes to the firewall policy are approved by the security personnel. • A majority of the approval process is accomplished via email. The security team members have provided copies of previous email communications. • The submitted email communication indicates the request for proposed firewall policy changes (from various departments) as well as approval response from the security personnel. • Due to the confidential information contained within the email communication, the evidence is not presentable for this practical.
Comments	
Pass / Fail	Pass – Audit met the control objective

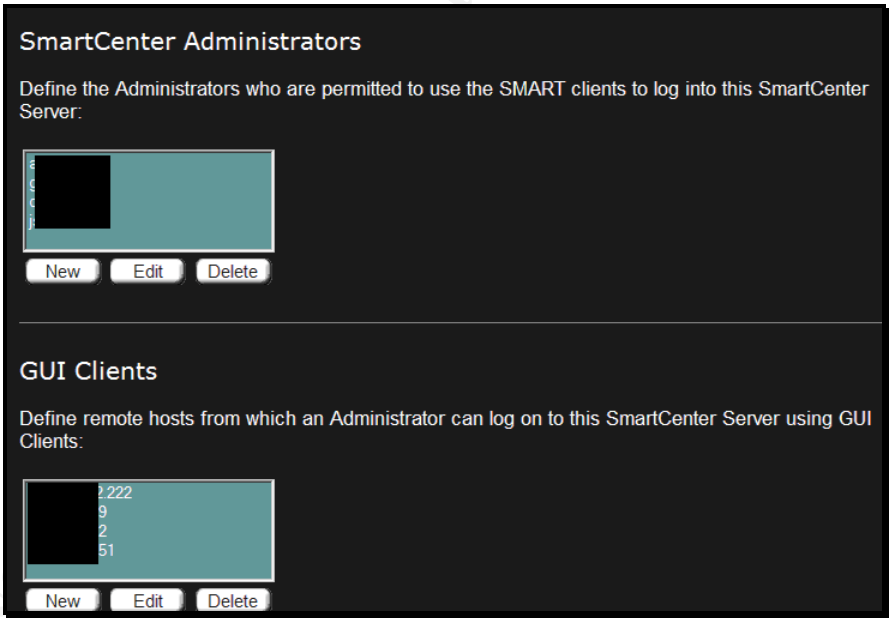
Checklist Number	Change Control Management 2
Control Objective	Any modification to the firewall policy must be tracked and thoroughly documented.
Expected Results	Any approved changes to the firewall policy must be documented and tracked. A document listing all previous minor or major changes to the firewall policy.

Actual Results	<p>The following information was obtained during the interview process with various security team members.</p> <ul style="list-style-type: none">Security team members share a common firewall policy tracking document detailing necessary information and actions.Security team has provided a copy of the tracking document which depicts the changes made to the firewall policy. <p>Below snapshot depicts the tracking document listing the minor and/or major updates to the firewall policy.</p>																																																																																																	
	<table><tr><th colspan="8">Firewall Modification Issue Tracker</th></tr><tr><th colspan="4">Issue Request Information</th><th colspan="4">Action Taken</th></tr><tr><th>No#</th><th>Issue Date</th><th>Request Date</th><th>Requestor's POC</th><th>Issue Detail</th><th>Action Date</th><th>Action Description</th><th>Close Date</th><th>Resolved By</th></tr><tr><td>18</td><td>3-Jun</td><td>6-Jun</td><td></td><td></td><td>4-Jun</td><td></td><td>12-Jun</td><td></td></tr><tr><td>19</td><td>11-Jun</td><td>12-Jun</td><td></td><td></td><td>11-Jun</td><td></td><td>14-Jun</td><td></td></tr><tr><td>20</td><td>16-Jun</td><td>24-Jun</td><td></td><td></td><td>23-Jun</td><td></td><td>15-Jul</td><td></td></tr><tr><td>21</td><td>21-Jun</td><td>28-Jun</td><td></td><td></td><td>28-Jun</td><td></td><td>2-Aug</td><td></td></tr><tr><td>22</td><td>7-Jul</td><td>8-Jul</td><td></td><td></td><td>8-Jul</td><td></td><td>23-Jul</td><td></td></tr><tr><td>23</td><td>20-Jul</td><td>27-Jul</td><td></td><td></td><td>27-Jul</td><td></td><td>2-Aug</td><td></td></tr><tr><td>24</td><td>30-Jul</td><td>2-Aug</td><td></td><td></td><td>2-Aug</td><td></td><td>2-Aug</td><td></td></tr><tr><td>25</td><td>3-Aug</td><td>4-Aug</td><td></td><td></td><td>4-Aug</td><td></td><td></td><td></td></tr></table>	Firewall Modification Issue Tracker								Issue Request Information				Action Taken				No#	Issue Date	Request Date	Requestor's POC	Issue Detail	Action Date	Action Description	Close Date	Resolved By	18	3-Jun	6-Jun			4-Jun		12-Jun		19	11-Jun	12-Jun			11-Jun		14-Jun		20	16-Jun	24-Jun			23-Jun		15-Jul		21	21-Jun	28-Jun			28-Jun		2-Aug		22	7-Jul	8-Jul			8-Jul		23-Jul		23	20-Jul	27-Jul			27-Jul		2-Aug		24	30-Jul	2-Aug			2-Aug		2-Aug		25	3-Aug	4-Aug			4-Aug			
	Firewall Modification Issue Tracker																																																																																																	
	Issue Request Information				Action Taken																																																																																													
	No#	Issue Date	Request Date	Requestor's POC	Issue Detail	Action Date	Action Description	Close Date	Resolved By																																																																																									
	18	3-Jun	6-Jun			4-Jun		12-Jun																																																																																										
	19	11-Jun	12-Jun			11-Jun		14-Jun																																																																																										
	20	16-Jun	24-Jun			23-Jun		15-Jul																																																																																										
	21	21-Jun	28-Jun			28-Jun		2-Aug																																																																																										
	22	7-Jul	8-Jul			8-Jul		23-Jul																																																																																										
23	20-Jul	27-Jul			27-Jul		2-Aug																																																																																											
24	30-Jul	2-Aug			2-Aug		2-Aug																																																																																											
25	3-Aug	4-Aug			4-Aug																																																																																													
Comments	<p>Updates to the firewall policy is being documented and tracked via the common document; however, as per the security team members, due to time constraints, all changes to the firewall policy may not get fully tracked or documented. The tracking document is behind in listing all of the changes to the firewall policy.</p>																																																																																																	
Pass / Fail	Fail – See Comments																																																																																																	

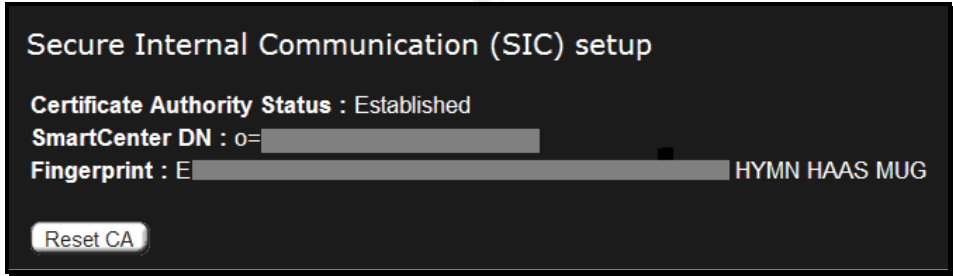
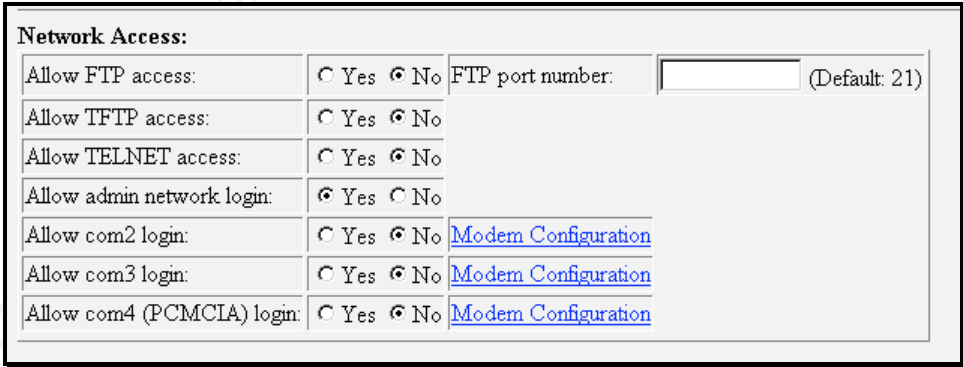
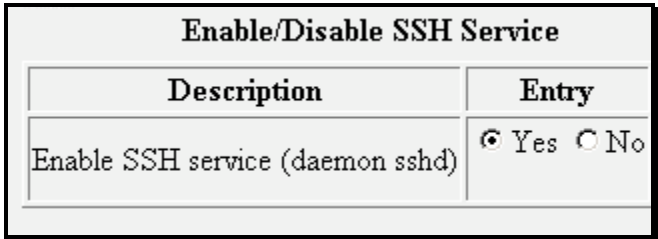
Checklist Number	Change Control Management 3
Control Objective	Any firewall vendor patches or OS vendor patches must be approved or authorized prior to implementing on the firewall.
Expected Results	Applying patches to production systems may cause an outage in the firewall services; therefore, all patches should be approved, authorized and fully tested in the lab environment prior to the implementation. To meet the control objective, security team should provide a document or email communications indicating the approval process as well as a document or email communication indicating the proper planning steps are accomplished.

Actual Results	<p>The following information was obtained during the interview process with various security team members.</p> <ul style="list-style-type: none"> Any major or minor firewall patches are approved and authorized by security personnel prior to implementation. A majority of the approval process is accomplished via email. Security team members have provided copies of the few previous email communications. The submitted email communications indicates the request for patch implementation with defined potential impact and benefits. The email communications also indicate the approval response from the security personnel. As indicated by the security personnel, all critical patches are tested in the lab environment prior to implementation. Prior to the patch implementation, a general outage notices is sent via email to all impacted audience listing the time and the date of unavailability of firewall services. Due to the confidential information contained within the email communication, the evidence is not presentable for this practical. <p>Below snapshot depicts the copy of the firewall service outage notice.</p> <div data-bbox="592 905 1256 1667" data-label="Image"> </div>
Comments	
Pass / Fail	Pass – Audit met the control objective


3.4 Firewall Access and Configuration

Checklist Number	Firewall Access and Configuration 1
Control Objective	Only authorized security personnel from the preconfigured hosts may be permitted to access and manage the firewall policy.
Expected Results	To access checkpoint firewall management GUI administrator have to create not only a user ID, but configure the hosts IP address. An evidence showing configuration with authorized users and authorized host IP address.
Actual Results	<p>The following information was obtained during the interview process with various security team members.</p> <ul style="list-style-type: none"> • There are 4 hosts listed that can provide firewall management. • There are 4 users listed that can administrator the firewall operation. <p>Below snapshot depicts the configuration showing the user IDs and their IP address.</p>  <p>Note: The user IDs and IP addresses has been obscured. Only the last octet of the IP address is displayed.</p>
Comments	
Pass / Fail	Pass – Audit met the control objective

Checklist Number	Firewall Access and Configuration 2
Control Objective	Any remote management of the firewall must be conducted over secure protocols.

Expected Results	As per the Checkpoint Manuals, "Checkpoint's Secure Internal Communication (SIC) enhances networks security by securing the administrative communication" All administrative traffic and enforcement traffic is established over secure protocols.
Actual Results	<p>The following information was obtained during the interview process with various security team members.</p> <ul style="list-style-type: none"> • Even though there are various hosts listed as the potential access points, security team members utilize one central server to update the firewall policy. • The SIC has been established among all of the firewall components. All Checkpoint administrative communication and policy enforcement communication is being encrypted. • Communication with the Nokia Platform established over the HTTP protocol, not over the HTTPS protocol. The communication with the Nokia platform (using Voyager) is not being encrypted. • Telnet and FTP services are disabled on the Nokia Platform. Only the SSH protocol is allowed. <p>Below snapshot depicts the established Secure Internal Communication (SIC).</p>  <p>Below snapshots depicts configuration of Nokia listing the available services.</p>  

Comments	Even though the scope of this audit specifically does not include the base OS on the Nokia Platform, the communication with the Nokia devices should be established over the encrypted protocols or over the secure channels.
Pass / Fail	Pass – Audit met the control objective

Checklist Number	Firewall Access and Configuration 3																					
Control Objective	Stay up-to-date on the firewall vendor recommended patches.																					
Expected Results	Per Checkpoint web site the latest patch available for Checkpoint NG Application Intelligence firewall application is NG R55 HFA 08 (as of August 2004).																					
Actual Results	<p>The following information was obtained during the interview process with various security team members.</p> <p>Security personnel have provided the version information from the Smart Update utility for the firewall module.</p> <div><table><thead><tr><th>Check Point</th><th>NG_AI</th><th>R54, HFA_410_R54, HFA_412_R54</th></tr></thead><tbody><tr><td>Check Point</td><td>NG_AI</td><td>R54, HFA_410_R54, HFA_412_R54</td></tr><tr><td>Check Point</td><td>NG_AI</td><td>R54</td></tr><tr><td>Check Point</td><td>NG_AI</td><td>R54</td></tr><tr><td>Check Point</td><td>NG_AI</td><td>R54</td></tr><tr><td>Check Point</td><td>NG_AI</td><td>R54</td></tr><tr><td>Check Point</td><td>NG_AI</td><td>R54</td></tr></tbody></table></div> <ul style="list-style-type: none">• The current version of the existing firewall is NG AI R54 HFA 412.• All of the latest patches for the build R54 have been implemented.• Security personnel are fully aware of latest release build R55 and associated post R55 patches. They have indicated that R55 build is being tested in the lab and waiting for the final approval process.• Security personnel did not have any documented impact or risk analysis for not applying the latest patches. Security personnel did not have any supporting documents listing the exceptions or detailed reasons for not applying the latest patches.	Check Point	NG_AI	R54, HFA_410_R54, HFA_412_R54	Check Point	NG_AI	R54, HFA_410_R54, HFA_412_R54	Check Point	NG_AI	R54	Check Point	NG_AI	R54	Check Point	NG_AI	R54	Check Point	NG_AI	R54	Check Point	NG_AI	R54
Check Point	NG_AI	R54, HFA_410_R54, HFA_412_R54																				
Check Point	NG_AI	R54, HFA_410_R54, HFA_412_R54																				
Check Point	NG_AI	R54																				
Check Point	NG_AI	R54																				
Check Point	NG_AI	R54																				
Check Point	NG_AI	R54																				
Check Point	NG_AI	R54																				
Comments	Even though the latest build R55 is under heavy testing in controlled lab environment, the defined control objective was not met. At the time of audit, the firewall was not at the up-to-date on the vendor specific patches or the build version.																					
Pass / Fail	Fail – See Comments																					

Checklist Number	Firewall Access and Configuration 4
Control Objective	Firewall architecture must provide high availability for the business mission critical services. Firewalls must not become a single point of failure.
Expected Results	Any technologies architected providing high availability or a fault tolerance to the firewall operations should be in place.

Actual Results

The following information was obtained during the interview process with various security team members.

- The firewalls are deployed on the Nokia Platform. Two firewalls are configured in the Active/Passive mode using Nokia's VRRP technologies.
- The network diagram is listed in section 1.4 also depicts the high availability configuration.

Below snapshot depicts the VRRP configuration of the Nokia platform.

<u>Firewall 1</u>	
Flags	On LocalReceive
7 interface enabled	
7 virtual routers configured	
	0 in Init state
	0 in Backup state
	7 in Master state

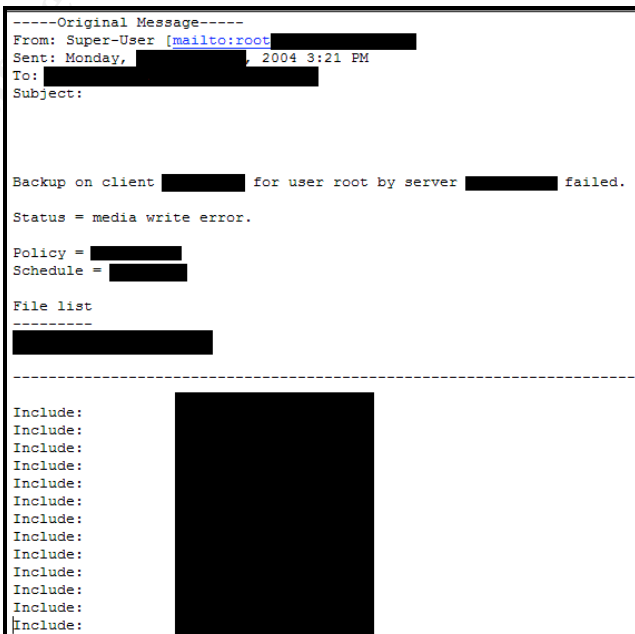
<u>Firewall 2</u>	
Flags	On LocalReceive
7 interface enabled	
7 virtual routers configured	
	0 in Init state
	7 in Backup state
	0 in Master state

Below snapshot depicts the VRRP test accomplished by unplugging one of the network cables from the primary firewall.

<u>Firewall 1</u>	
Flags	On LocalReceive
6 interface enabled	
6 virtual routers configured	
	0 in Init state
	0 in Backup state
	6 in Master state

<u>Firewall 2</u>	
Flags	On LocalReceive
7 interface enabled	
7 virtual routers configured	
	0 in Init state
	6 in Backup state
	1 in Master state

Comments	
Pass / Fail	Pass – Audit met the control objective

Checklist Number	Firewall Access and Configuration 5
Control Objective	Firewall policy, firewall logs and firewall configuration must be routinely backed up.
Expected Results	Proof indicating the firewall policy, the firewall logs and the firewall configuration are being backed up at defined routine interval.
Actual Results	<p>The following information was obtained during the interview process with various security team members.</p> <ul style="list-style-type: none"> The Checkpoint firewall management server is configured on the Checkpoint's Secure Platform operating system. At this point, there is no backup software available to automatically backup the required files. Security administrator has to manually execute the "BACKUP ALL" command on the Secure Platform to back up the firewall policy, the firewall configurations and the firewall logs. The file generated through the "BACKUP ALL" command is TFTP to a defined server. The files on the TFTP server are backed up using the corporate deployed backup mechanism. Thus, the firewall configuration, the firewall policy and the firewall logs are being fully backed up. Security personnel have provided an automatically generated email from the backup software depicting the success of the last few days of full backup. <p>Below snapshot depicts an automatically generated email from the backup solution listing the files and the servers that are being backed up.</p>  <pre> -----Original Message----- From: Super-User [mailto:root@redacted] Sent: Monday, [redacted], 2004 3:21 PM To: [redacted] Subject: Backup on client [redacted] for user root by server [redacted] failed. Status = media write error. Policy = [redacted] Schedule = [redacted] File list ----- [redacted] ----- Include: Include: Include: Include: Include: Include: Include: Include: Include: Include: Include: Include: Include: Include: </pre>

Comments	
Pass / Fail	Pass – Audit met the control objective

Checklist Number	Firewall Access and Configuration 6
Control Objective	Routinely review the firewall policy and the security policy.
Expected Results	A defined process or procedure indicating the reviewing or updating to the firewall policy and the security policy is occurring at routine interval. Security policy should define the interval to review the security policy and firewall policy to remove any anomalies.
Actual Results	<p>The following information was obtained during the interview process with various security team members.</p> <ul style="list-style-type: none">• The interval of routine review for the firewall policy or the security policy is not defined in the corporate security policy.• Security personnel have indicated that the firewall policy as well as the security policy was last thoroughly reviewed and updated about two months ago.
Comments	The audit has met the control objective. The review interval is not defined or listed in the security policy.
Pass / Fail	Pass with a caution flag – See comments

Checklist Number	Firewall Access and Configuration 7
Control Objective	Firewall logs must be routinely reviewed.
Expected Results	A defined process or procedure indicating the review of the firewall log is occurring at routine interval. A common practice suggests that the firewall logs should be reviewed daily.

Actual Results	<p>The following information was obtained during the interview process with various security team members.</p> <ul style="list-style-type: none">• The firewall logs are reviewed daily to identify any anomalies and potential security breach.• The firewall logs are thoroughly reviewed at least once a week to catch any missed events. <p>Below snapshot depicts the routine login of the security personnel to the SmartView Tracker (Firewall log monitoring utility).</p>																																																																																																																																	
	<table><tr><th>Date</th><th>Time</th><th>Application</th><th>Subject</th><th>Operation</th></tr><tr><td>18Aug2004</td><td>13:17:43</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr><tr><td>19Aug2004</td><td>3:21:03</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log In</td></tr><tr><td>19Aug2004</td><td>3:22:49</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr><tr><td>19Aug2004</td><td>4:08:53</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log In</td></tr><tr><td>19Aug2004</td><td>4:10:18</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr><tr><td>19Aug2004</td><td>4:47:04</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log In</td></tr><tr><td>19Aug2004</td><td>4:55:24</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr><tr><td>19Aug2004</td><td>15:30:31</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log In</td></tr><tr><td>19Aug2004</td><td>15:36:55</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log In</td></tr><tr><td>19Aug2004</td><td>15:59:05</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr><tr><td>19Aug2004</td><td>15:59:08</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr><tr><td>20Aug2004</td><td>10:48:57</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log In</td></tr><tr><td>20Aug2004</td><td>11:04:50</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr><tr><td>20Aug2004</td><td>11:29:47</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log In</td></tr><tr><td>20Aug2004</td><td>11:32:31</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr><tr><td>20Aug2004</td><td>14:04:10</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log In</td></tr><tr><td>20Aug2004</td><td>14:32:03</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr><tr><td>24Aug2004</td><td>14:47:39</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log In</td></tr><tr><td>24Aug2004</td><td>14:47:53</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr><tr><td>24Aug2004</td><td>14:49:08</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log In</td></tr><tr><td>24Aug2004</td><td>15:25:33</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr><tr><td>24Aug2004</td><td>15:30:00</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log In</td></tr><tr><td>24Aug2004</td><td>15:32:39</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr><tr><td>25Aug2004</td><td>10:48:42</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log In</td></tr><tr><td>25Aug2004</td><td>10:57:05</td><td>SmartView Tracker</td><td>Administrator Login</td><td>Log Out</td></tr></table>	Date	Time	Application	Subject	Operation	18Aug2004	13:17:43	SmartView Tracker	Administrator Login	Log Out	19Aug2004	3:21:03	SmartView Tracker	Administrator Login	Log In	19Aug2004	3:22:49	SmartView Tracker	Administrator Login	Log Out	19Aug2004	4:08:53	SmartView Tracker	Administrator Login	Log In	19Aug2004	4:10:18	SmartView Tracker	Administrator Login	Log Out	19Aug2004	4:47:04	SmartView Tracker	Administrator Login	Log In	19Aug2004	4:55:24	SmartView Tracker	Administrator Login	Log Out	19Aug2004	15:30:31	SmartView Tracker	Administrator Login	Log In	19Aug2004	15:36:55	SmartView Tracker	Administrator Login	Log In	19Aug2004	15:59:05	SmartView Tracker	Administrator Login	Log Out	19Aug2004	15:59:08	SmartView Tracker	Administrator Login	Log Out	20Aug2004	10:48:57	SmartView Tracker	Administrator Login	Log In	20Aug2004	11:04:50	SmartView Tracker	Administrator Login	Log Out	20Aug2004	11:29:47	SmartView Tracker	Administrator Login	Log In	20Aug2004	11:32:31	SmartView Tracker	Administrator Login	Log Out	20Aug2004	14:04:10	SmartView Tracker	Administrator Login	Log In	20Aug2004	14:32:03	SmartView Tracker	Administrator Login	Log Out	24Aug2004	14:47:39	SmartView Tracker	Administrator Login	Log In	24Aug2004	14:47:53	SmartView Tracker	Administrator Login	Log Out	24Aug2004	14:49:08	SmartView Tracker	Administrator Login	Log In	24Aug2004	15:25:33	SmartView Tracker	Administrator Login	Log Out	24Aug2004	15:30:00	SmartView Tracker	Administrator Login	Log In	24Aug2004	15:32:39	SmartView Tracker	Administrator Login	Log Out	25Aug2004	10:48:42	SmartView Tracker	Administrator Login	Log In	25Aug2004	10:57:05	SmartView Tracker	Administrator Login
Date	Time	Application	Subject	Operation																																																																																																																														
18Aug2004	13:17:43	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
19Aug2004	3:21:03	SmartView Tracker	Administrator Login	Log In																																																																																																																														
19Aug2004	3:22:49	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
19Aug2004	4:08:53	SmartView Tracker	Administrator Login	Log In																																																																																																																														
19Aug2004	4:10:18	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
19Aug2004	4:47:04	SmartView Tracker	Administrator Login	Log In																																																																																																																														
19Aug2004	4:55:24	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
19Aug2004	15:30:31	SmartView Tracker	Administrator Login	Log In																																																																																																																														
19Aug2004	15:36:55	SmartView Tracker	Administrator Login	Log In																																																																																																																														
19Aug2004	15:59:05	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
19Aug2004	15:59:08	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
20Aug2004	10:48:57	SmartView Tracker	Administrator Login	Log In																																																																																																																														
20Aug2004	11:04:50	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
20Aug2004	11:29:47	SmartView Tracker	Administrator Login	Log In																																																																																																																														
20Aug2004	11:32:31	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
20Aug2004	14:04:10	SmartView Tracker	Administrator Login	Log In																																																																																																																														
20Aug2004	14:32:03	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
24Aug2004	14:47:39	SmartView Tracker	Administrator Login	Log In																																																																																																																														
24Aug2004	14:47:53	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
24Aug2004	14:49:08	SmartView Tracker	Administrator Login	Log In																																																																																																																														
24Aug2004	15:25:33	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
24Aug2004	15:30:00	SmartView Tracker	Administrator Login	Log In																																																																																																																														
24Aug2004	15:32:39	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
25Aug2004	10:48:42	SmartView Tracker	Administrator Login	Log In																																																																																																																														
25Aug2004	10:57:05	SmartView Tracker	Administrator Login	Log Out																																																																																																																														
Comments																																																																																																																																		
Pass / Fail	Pass – Audit met the control objective																																																																																																																																	

3.5 Firewall Rule-base Validation

Checklist Number	Firewall Rule-base Validation 1
Control Objective	Ensure that the Stealth Rule is in place to protect against the attacks that are aimed at the firewall.
Expected Results	To protect firewall itself from any potential attacks, the Stealth Rule must be in placed. As per Lance Spitzner, “this is a standard rule that every rulebase should have”.

Actual Results

The following information was obtained during the interview process with the security personnel as well as reviewing the firewall policy along with the security personnel.

- The Stealth Rule is in place to protect the firewall from any potential attacks directed towards the firewall.
- Full logging is defined to capture probes and attacks that directed towards the firewall but dropped by the Stealth Rule.

Below snapshot depicts the Stealth Rule implementation in the firewall policy.



Below snapshot depicts the effect of the Stealth Rule. The firewall logs indicate the traffic being dropped due to the Stealth Rule.


Note: The IP addresses of the firewalls have been obscured and only the last octet is displayed.

Time	Srv.	Source	Destination
11:37:25	TCP 445	.184.42	.252
11:39:25	TCP 445	.24.196	.252
11:53:21	TCP 445	.72.212	.252
11:55:43	UDP 1026	.9.48	.252
11:55:44	UDP 1027	.130.195	.252
11:56:08	TCP 445	.98.92	.252
12:00:04	TCP 445	.120.219	.252
12:24:16	TCP 9001	.227.185	.252
12:24:18	TCP 9001	.227.185	.252
12:33:36	TCP 445	.140.160	.252
12:55:46	TCP 5554	.0.48.173	.252
12:55:46	TCP 9898	.0.48.173	.252
12:57:24	TCP 445	.151.19	.252
13:00:58	TCP 445	.140.160	.252
13:05:02	UDP 135	.209.252	.252
13:05:02	UDP 1026	.209.252	.252
13:15:01	TCP 445	.140.160	.252
13:28:27	TCP 445	.204.33	.252

Below snapshot depicts the impact of the Stealth Rule. (NMAP utility is used to scan the IP address of the firewalls.)

Time	Origin	Service	Source	Destination
9:09:18		TCP 25	.240	.254
9:09:20		TCP 3160	.240	.254
9:09:20		TCP 8765	.240	.254
9:09:20		TCP 3161	.240	.254
9:09:21		TCP 139	.240	.254
9:09:22		TCP 80	.240	.254
9:09:22		TCP 22	.240	.254
9:09:22		TCP 25	.240	.254
9:09:22		TCP 515	.240	.254
9:09:22		TCP 23	.240	.254
9:09:22		TCP 21	.240	.254
9:09:22		TCP 6000	.240	.254
9:09:23		TCP 1025	.240	.254
9:09:23		TCP 7100	.240	.254
9:09:23		TCP 25	.240	.254
9:09:23		TCP 4000	.240	.254
9:09:24		TCP 110	.240	.254
9:09:27		UDP 123	.240	.254

Comments	
Pass / Fail	Pass – Audit met the control objective

Checklist Number	Firewall Rule-base Validation 2
Control Objective	Ensure that the Drop Rule or Cleanup Rule is place to explicitly drop the “undefined” traffic.
Expected Results	Since the corporate policy is to explicitly drop any undefined traffic, there should be a Drop Rule or a Cleanup Rule placed as the last rule in the firewall rule base. The detail logging should be enabled for this rule. The logged traffic provides immense amount of troubleshooting information for the security personnel.
Actual Results	<p>The following information was obtained during the interview process with the security personnel as well as reviewing the firewall policy along with the security personnel.</p> <ul style="list-style-type: none"> • The Drop Rule is in place as the last rule to drop any undefined traffic. • Full logging is defined to capture traffic that is being dropped by the Drop Rule. <p>Below snapshot depicts the Drop Rule implementation in the firewall policy.</p> 
Comments	
Pass / Fail	Pass – Audit met the control objective

Checklist Number	Firewall Rule-base Validation 3
Control Objective	Any inbound traffic to the protected network must correspond to the approved and authorized inbound traffic rules defined in the security policy.
Expected Results	Based on the criteria listed in the security policy, the inbound traffic is allowed only on certain protocols to the specific destination.
Actual Results	<p>The following information was obtained during the interview process with the security personnel as well as reviewing the firewall policy along with the security personnel.</p> <ul style="list-style-type: none"> • The defined inbound traffic rules are derived from the criteria listed in the security policy. • The firewall policy controls the inbound traffic from the internet, to the multi-tier DMZ. The firewall policy also controls the inbound management traffic from the defined sources from the corporate network. • The inbound traffic rules are constructed in a logical order. • Throughout the firewall policy the defined rules are separated with appropriate comment headers and separated with the inbound traffic for each defined DMZ.

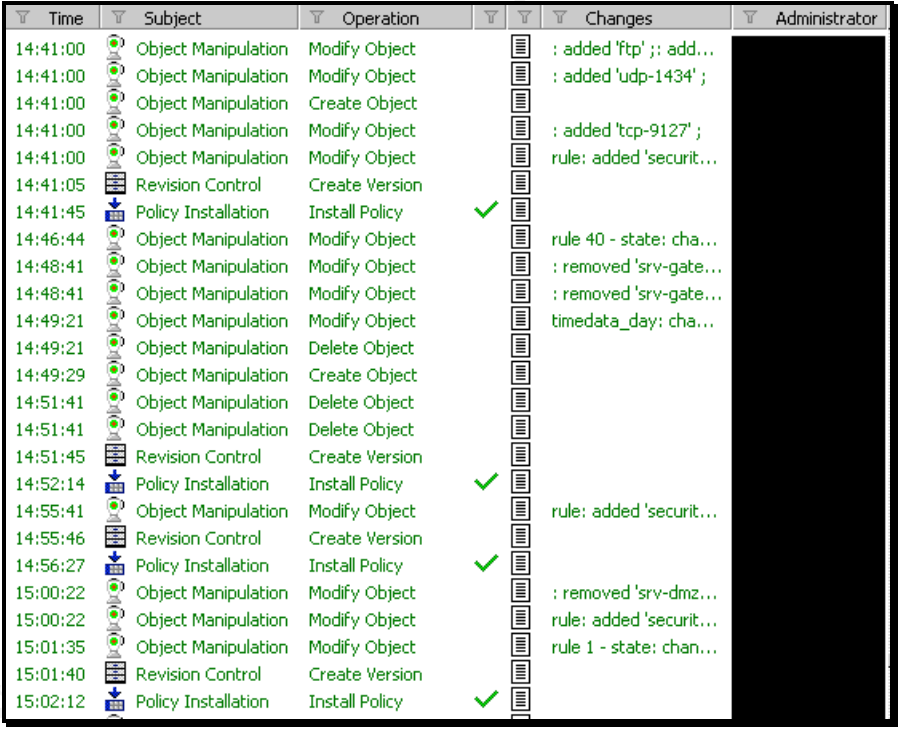
Comments	
Pass / Fail	Pass – Audit met the control objective

Checklist Number	Firewall Rule-base Validation 4
Control Objective	Any outbound traffic from the protected network must correspond to the approved and authorized outbound traffic rules defined in the security policy.
Expected Results	Based on the criteria listed in the security policy, the outbound traffic is allowed only on a few protocols to the specified servers.
Actual Results	<p>The following information was obtained during the interview process with the security personnel as well as reviewing the firewall policy along with the security personnel.</p> <ul style="list-style-type: none"> • The defined outbound traffic rules are derived from the criteria listed in the security policy. • The firewall policy controls the outbound traffic to the internet, from the multi-tier DMZ and the outbound management traffic to the defined corporate resources. • The outbound traffic rules are constructed in a logical order. • There are two rules created for outbound traffic that are not defined in the security policy. As indicated by the security personnel, these rules are defined for a business need and requirement. The security personnel have provided the approved document listing the reason for exception for these rules.
Comments	During the discussion with security personnel, there were two rules that were identified as business related outbound traffic. Security personnel has document listing approved exception; however, the information on this traffic was not documented in the security policy.
Pass / Fail	Pass with a caution flag – See comments

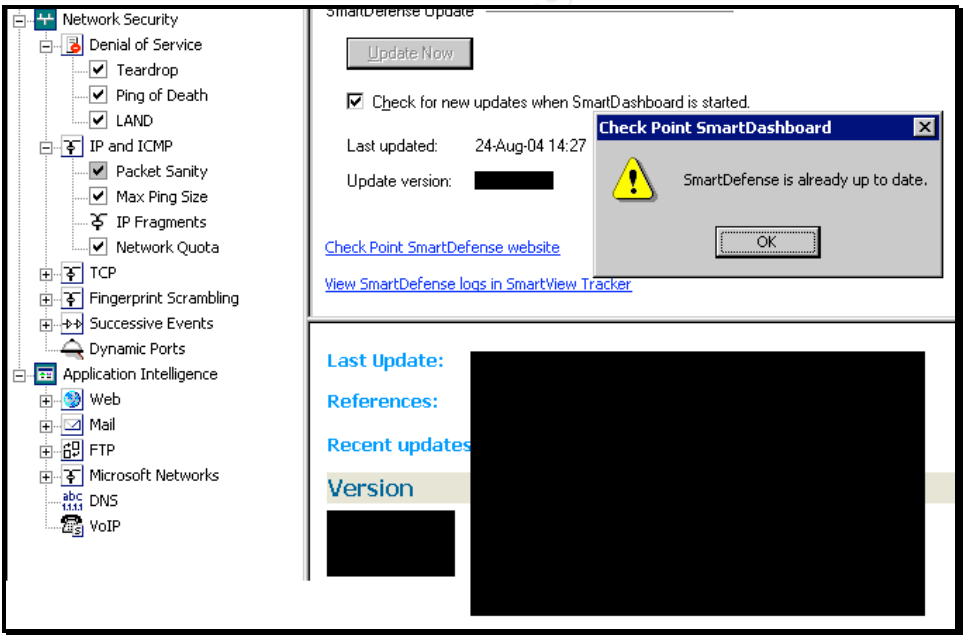
Checklist Number	Firewall Rule-base Validation 5
Control Objective	Firewall must provide an audit trail of all traffic (except noise traffic).
Expected Results	The firewall policy should be configured to log all the inbound and the outbound traffic. To reduce the amount of logging, the noise traffic may not be required to log.

Actual Results	<p>The following information was obtained during the interview process with the security personnel as well as reviewing the firewall policy along with security personnel.</p> <ul style="list-style-type: none">The defined firewall inbound and outbound rules have detail logging enabled.Due to the confidential information contained in the firewall policy, the evidence (indicating logging is enabled for every rule) is not presentable for this practical.Some of the noise rules were also defined to log. <p>Below snapshot depicts the rule based indicating that some of the noise traffic is configured to log.</p> <table><tr><td>* Any</td><td>* Any</td><td>UDP bootp UDP UDP-2989</td><td>drop</td><td>- None</td><td>* Policy Targets</td><td>* Any</td></tr><tr><td>* Any</td><td>* Any</td><td>Grp-Blockec</td><td>drop</td><td>Log</td><td>* Policy Targets</td><td>* Any</td></tr><tr><td>* Any</td><td>* Any</td><td>NBT</td><td>drop</td><td>- None</td><td>* Policy Targets</td><td>* Any</td></tr><tr><td>* Any</td><td>mcast-vrrp</td><td>* Any</td><td>drop</td><td>Log</td><td>* Policy Targets</td><td>* Any</td></tr></table>	* Any	* Any	UDP bootp UDP UDP-2989	drop	- None	* Policy Targets	* Any	* Any	* Any	Grp-Blockec	drop	Log	* Policy Targets	* Any	* Any	* Any	NBT	drop	- None	* Policy Targets	* Any	* Any	mcast-vrrp	* Any	drop	Log	* Policy Targets	* Any
* Any	* Any	UDP bootp UDP UDP-2989	drop	- None	* Policy Targets	* Any																							
* Any	* Any	Grp-Blockec	drop	Log	* Policy Targets	* Any																							
* Any	* Any	NBT	drop	- None	* Policy Targets	* Any																							
* Any	mcast-vrrp	* Any	drop	Log	* Policy Targets	* Any																							
Comments	Logs generated by the noise rules do not provide any additional troubleshooting or store any crucial evidence. Even though there may be available space to store the logs, the noise traffic may be configured not to log.																												
Pass / Fail	Pass – Audit met the control objective																												

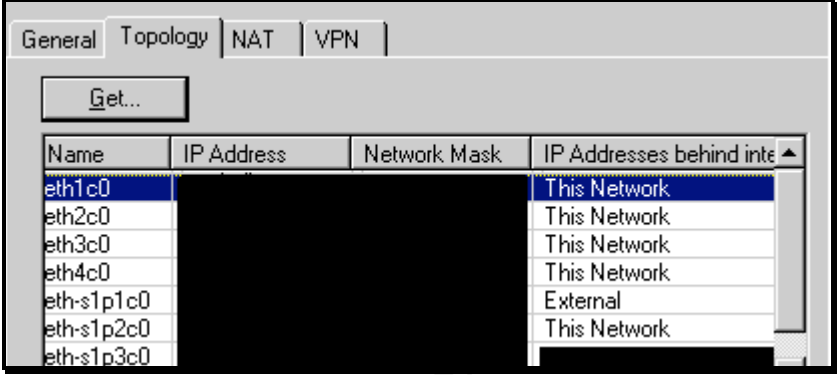
Checklist Number	Firewall Rule-base Validation 6
Control Objective	Firewall logs or the audit trail must include any action taken by security personnel.
Expected Results	Any action taken by any user with administrative rights must be logged. Checkpoint SmartView Tracker utility provides detailed audit logs for every action taken by the firewall administrator. Audit tails may provide sufficient information during the recovery process in case of accidental or intentional actions taken by the administrator (as indicated in the threat matrix section).

Actual Results	<p>The following information was obtained during the interview process with security personnel as well as reviewing the firewall policy along with the security personnel.</p> <ul style="list-style-type: none"> The SmartView Tracker utility provides the audit logs that track every action taken by the security team members. Audit logs indicate that all actions performed by administrators were being captured in the firewall logs. The audit logs indicate that the “Revision Control” feature of the Checkpoint firewall is being utilized, prior to implementing each significant modification to the firewall policy. The revision control feature saves the previous version of the firewall policy. Also, the previously stored firewall policy can also be restored via this feature. <p>Below snapshot depicts the firewall logs listing actions taken by the administrators.</p>  <p>Note: The user IDs for the administrators have been obscured</p>
Comments	
Pass / Fail	Pass – Audit met the control objective

Checklist Number	Firewall Rule-base Validation 7
Control Objective	Firewall should be configured to protect against potential network based Denial of Services (DoS) attacks.



























































































Expected Results	To protect the firewall from various known network based DoS attacks and emerging unknown attacks, a layer of defense must be in place. Checkpoint offers a paid subscription to Smart Defense technologies. If Checkpoint Smart Defense is not purchased, list the mechanisms to protect the firewalls from potential network based DoS attacks.
Actual Results	<p>The following information was obtained during the interview process with the security personnel as well as reviewing the firewall policy along with the security personnel.</p> <ul style="list-style-type: none"> The Security Department has purchased the Checkpoint Smart Defense subscription and the subscription is kept up-to-date. The Smart Defense has been configured to block some of the known network based DoS attacks. The Smart Defense is configured to automatically check for any new available Smart Defense updates from the Checkpoint site. <p>Below snapshot depicts the Smart Defense subscription configuration.</p> 
Comments	
Pass / Fail	Pass – Audit met the control objective

Checklist Number	Firewall Rule-base Validation 8
Control Objective	All interfaces of the firewall must be configured with Anti-Spoofing capabilities.
Expected Results	To prevent any potential network based attacks, as per the Checkpoint Manuals, “for anti-spoofing to be most effective, it should be configured on all gateway interfaces.” The anti-spoofing configuration protects the organization from potential attacker to penetrate the internal networks.

Actual Results	<p>The following information was obtained during the interview process with the security personnel as well as reviewing the firewall policy along with the security personnel.</p> <ul style="list-style-type: none"> All interfaces of the e-commerce firewalls were configured with Anti-Spoofing to prevent from potential spoofing attacks. <p>Below snapshot depicts anti-spoofing configuration listing all interfaces.</p>  <p>Note: The IP addresses and subnet mask has been obscured.</p>
Comments	
Pass / Fail	Pass – Audit met the control objective

Checklist Number	Firewall Rule-base Validation 9
Control Objective	Firewall should be configured to hide the internal network architecture.
Expected Results	A common practice of hiding internal network architecture should be in placed. A Network Address Translation or Port Address Translation should be used. The NAT/ PAT protects from potential attacker mapping the internal network.

© SANS Institute

Actual Results	<p>The following information was obtained during the interview process with the security personnel as well as reviewing the firewall policy along with the security personnel.</p> <ul style="list-style-type: none">Depending on the traffic requirements, a combination of both static network address translation and hide network address translation was implemented to protect the internal infrastructure.Appropriate measurements have been taken to hide and protect internal resources. <p>Below snapshot depicts the utilization of the Network Address Translation implementation in the firewall policy.</p> <table><tr><td> [Redacted]</td><td> [Redacted]</td><td> Any</td><td> Original</td><td> Original</td><td> Original</td></tr><tr><td> [Redacted]</td><td> [Redacted]</td><td> Any</td><td> Original</td><td> Original</td><td> Original</td></tr><tr><td> [Redacted]</td><td> [Redacted]</td><td> Any</td><td> [Redacted]</td><td> Original</td><td> Original</td></tr><tr><td> [Redacted]</td><td> [Redacted]</td><td> Any</td><td> [Redacted]</td><td> Original</td><td> Original</td></tr><tr><td> [Redacted]</td><td> Any</td><td> Any</td><td> [Redacted]</td><td> Original</td><td> Original</td></tr></table>	 [Redacted]	 [Redacted]	 Any	 Original	 Original	 Original	 [Redacted]	 [Redacted]	 Any	 Original	 Original	 Original	 [Redacted]	 [Redacted]	 Any	 [Redacted]	 Original	 Original	 [Redacted]	 [Redacted]	 Any	 [Redacted]	 Original	 Original	 [Redacted]	 Any	 Any	 [Redacted]	 Original	 Original
 [Redacted]	 [Redacted]	 Any	 Original	 Original	 Original																										
 [Redacted]	 [Redacted]	 Any	 Original	 Original	 Original																										
 [Redacted]	 [Redacted]	 Any	 [Redacted]	 Original	 Original																										
 [Redacted]	 [Redacted]	 Any	 [Redacted]	 Original	 Original																										
 [Redacted]	 Any	 Any	 [Redacted]	 Original	 Original																										
Comments	A separate audit should be performed for all applications that are being hosted from the protected network. Any crucial information that may allow an attacker to map the internal network infrastructure should not be leaked through any of the hosted applications.																														
Pass / Fail	Pass – Audit met the control objective																														

Checklist Number	Firewall Rule-base Validation 10
Control Objective	Routinely review and remove any temporary rules created in the firewall policy.
Expected Results	It is normal to have temporary rules created for testing or troubleshooting; however, temporary rules should be documented with comments. A forgotten temporary rule may leave potential hole that can be exploited. All temporary rules should have a removal date defined and should be communicated to all security personnel.
Actual Results	<p>The following information was obtained during the interview process with the security personnel as well as reviewing the firewall policy along with the security personnel.</p> <ul style="list-style-type: none"> There were few rules found in the firewall policy that were temporarily created for testing. Some of the temporary rules did not include comments such as the creation date, the expiration date, the responsible department or the creator of rule. There was no established document listing these exceptions.

Comments	There were few rules that were created but had no information on deactivation date. Security team member indicated that these rules were created a while back, but forgot to remove them. As the objective indicates, temporary and testing rules should be routinely reviewed and removed from the firewall policy.
Pass / Fail	Fail – See Comments

3.6 Residual Risks

The residual risks are the risks that exist after considering the effect of mitigating controls. The overall firewall architecture, design and the configuration is resilient to various known attacks. The defense in-depth design provides layers of protection for the business critical services and operations.

In today's technology age, the vulnerabilities have been discovered at rapid rate and attacks have become more sophisticated. Hence, there is an inherent risk by allowing the inbound HTTP and HTTPS protocols. However, the e-commerce business depends on these inbound services. The organization has taken some extra measurements and actions to contain and mitigate the existing residual risks.

As per the information gathered from various audit programs, (available at the www.auditnet.org) the risk in general obstructs the defined objectives of the organizations. To mitigate residual risks, the organization has to define and place some internal controls surrounding the objective. The auditing process provides assurance that internal controls mitigate risks at the organization's acceptable tolerance.

3.7 Is the System Auditable?

The overall audit process was not hindered by any major obstacles and it was accomplished successfully. The developed checklist was sufficient and effective to audit the defined scope. The audit process did not include any Denial of Service attacks. Due the fact that the firewalls were in production, the security personnel did not authorize or approve of conducting any network based DoS attacks on the firewalls or the security architecture of the organization. The audit checklist relied on the evidence of the network based DoS attack parameters defined or configured in the Smart Defense implementation. By the time the audit process was completed, the latest patch for Checkpoint NG was still under rigorous testing in the lab environment, so the final verification of latest patch was not concluded.

The defense-in-depth architecture of an organization usually encompasses various devices staged strategically to provide layers of security. The scope of the audit did not include various crucial pieces in the security architecture, such as an upstream router. A separate audit should be conducted to evaluate the upstream router, as well as the base operating system of the firewalls. Also, a separate audit should be conducted to evaluate web applications, databases and any other applications that are being hosted from the e-commerce protected environment.

Assignment 4 – Follow up Audit Report

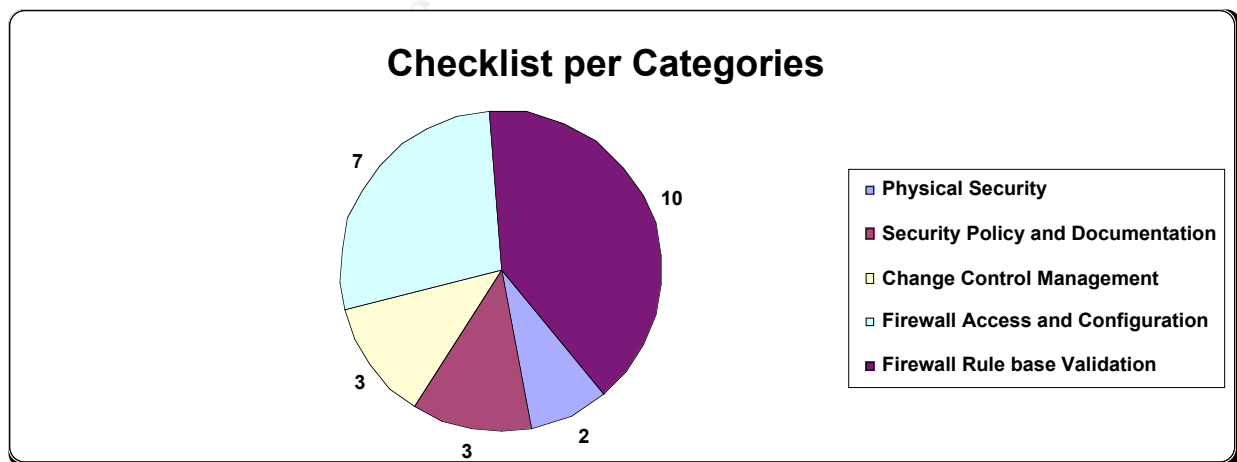
4.1 Executive Summary

The overall audit process was not hindered by any major obstacles and it was accomplished successfully. The primary objective of the audit was to examine the security policy and verify that firewall policy was derived from the criteria listed in the security policy. The overall objectives detailed in the security policy are adequate with few exceptions. The overall firewall policy is consistent with criteria listed in the security policy with few undocumented rules. The firewall, in general, is effectively enforcing the criteria listed in the corporate security policy and providing protection as indicated in the security policy. The firewall infrastructure is architected to meet the guidelines defined in the security policy.

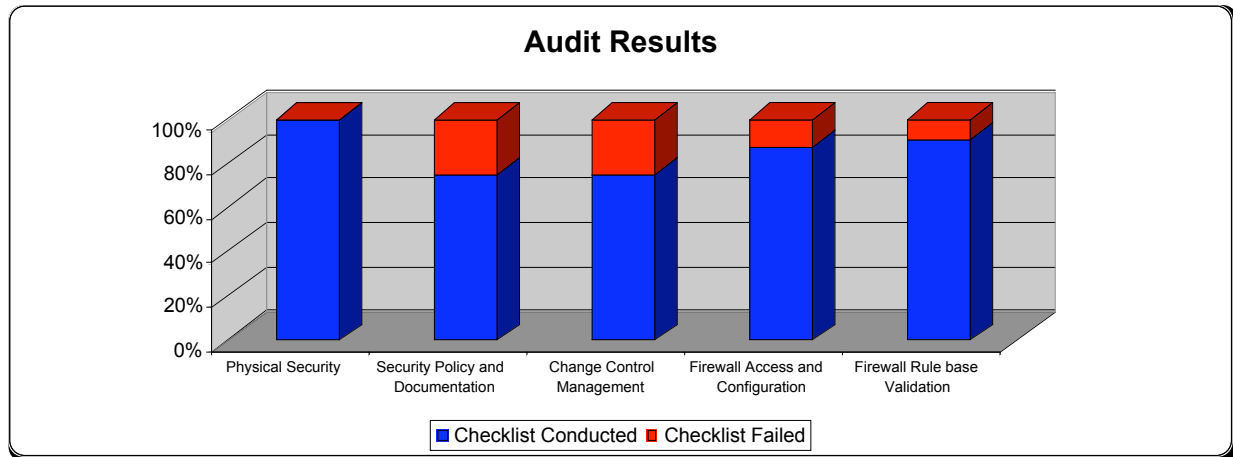
The audit was conducted over following five major categories:

1. Physical Security
2. Security Policy and Documentation
3. Change Management Control
4. Firewall Access and Configuration
5. Firewall Rule-base Validation

Based on the above listed categories, there were 25 checklist generated to assist the audit process for the defined scope. The graph shown below depicts the breakdown for the checklist per categories.



The organization did not meet four of the conducted checklist for the control objectives. The graph shown below depicts the breakdown of the audit success vs. audit failure ratio for each category.



The organization has passed the audit with an overall 84% score.

The organization has developed an outstanding procedure for establishing the baseline of the firewall utilization. The information gathered from routine snapshots adds tremendous value to the organization. By frequently measuring the existing conditions, the organization may gain a visibility that can assist for any potential future expenditure in the security arena. A few snapshots of the firewall baseline are listed in the Appendix B.

The recommendations for the four failed audit checklist items are listed in the Technical Summary section. The risk and cost associated to fix or remediate the failed audit is also elaborated in the Technical Summary section.

4.2 Technical Summary

The overall conducted audit was successful. Security team members have provided all requested documents as well as necessary evidences to support the control objectives. The security personnel have provided full assistance and cooperation through out the audit process. The primary objective of the audit was to examine the security policy and verify that the firewall policy was derived from the criteria listed in the security policy.

The audit was conducted over five major categories. There were 25 checklist compiled to encompass the five categories. Each checklist was graded with the Pass, Fail, or Pass with a caution flag. The below table shows the number of audit failure as well as number of checklist items that were “pass with a caution flag”.

	Checklist Conducted	Checklist Failed	Pass with a caution flag
Physical Security	2	0	0
Security Policy and Documentation	3	1	1
Change Control Management	3	1	0
Firewall Access and Configuration	7	1	1
Firewall Rule base Validation	10	1	1

There were four checklist items that did not pass audit. There were 3 checklist items that were passed with a caution flag. The grade pass with a caution flag indicates that objective was met; however, the caution flag was raised to indicate that the minor information was not available or the minor steps were not taken by the security team members.

4.3 Audit Findings

There were 25 audit checklists compiled to perform a through audit of the scope. This section provides the summary for the audit findings. This section also provides the recommendation for failed audits and lists the estimated cost factors for remediation.

- The organization has placed adequate environmental and physical controls to protect the firewalls as well as network and server infrastructure. Proper access control has been placed to allow limited authorized physical access.
- The organization has developed a well defined security policy indicating traffic to and from the protected network. Organization has also developed well defined sets of documents to track proposed changes to the corporate policies. Organization does not have a defined detail backup procedure.
- There is an adequate change control management in placed. However, some of the crucial supporting or tracking documents does not get updated on a timely manner. Some of the approved and authorized changes in the firewall policy have not been fully tracked with the existing procedure.
- The firewalls have been architected and configured to meet the security policy. The firewalls are configured in a high availability mode to provide fault tolerance in the firewall services. The firewalls are not at the latest vendor released build. The organization has defined an objective to review the firewall policy and security policy routinely; however, a review time interval has not been defined in the policy.

- The overall firewall policy is derived from the criteria listed in the corporate security policy with exception of a few rules that are deemed business critical and were not documented in the security policy. The firewall policy is logically constructed as well as well appropriately annotated. The firewall logs, the firewall configuration and the firewall policy are being routinely backed up; however, user intervention may be required during the backup process.

The below section discusses about the four failed audit checklist with appropriate recommendations as well as provides an estimated cost factor for remediation. The security posture of the organization may improve by implementing the recommendations for the items in the audit checklist that failed. The recommendations may also assist the organization to effectively maintain the efficiency in and around the protected environment.

Checklist Number	Security Policy and Documentation 3
Control Objective	A backup policy and procedure must be defined to backup the firewall configuration, firewall policy and firewall logs.
Pass / Fail	Fail
Risk	The firewall policy, the firewall configuration and firewall logs are being routinely backed up. However, a defined backup procedure does not exist. If the procedures for backing up the firewall configuration, the firewall policy and the firewall logs are not documented, the necessary files may not get backed up. Also, any change in the security team may introduce disruption in backup requirement. Establishing the documented backup procedure reduces the potential crucial disruption of services.
Recommendation	<p>The organization has established various policy and procedures in the security arena. The backup policy is defined, but the backup procedure has not been documented.</p> <ul style="list-style-type: none"> Establish a separate backup procedure. Detail all essential files such as the firewall configuration, the firewall logs and the firewall policy that must be backed up in the procedure. Define a backup interval in the backup policy and procedure. Review the Checkpoint Knowledge base articles to ensure all necessary Checkpoint configuration files are being backed up. Establish change control, or tracking document, to update the backup procedure.
Cost	The cost to implement the above recommendation should be very minimal. One of the security team members can develop the backup policy and procedure in a relatively short period of time. The cost is offset by gaining the established backup policy and procedure to ensure validity of essential files being backed up correctly.

Checklist Number	Change Control Management 2
-------------------------	------------------------------------

Control Objective	Any modification to the firewall policy must be tracked and thoroughly documented.
Pass / Fail	Fail
Risk	Tracking any minor and/or major changes to the firewall policy provides an audit trail. In case of disaster, documented changes may be very a useful tool during the recovery phase.
Recommendation	<p>The organization has established a tracking document to record any firewall policy changes. However, perhaps due to time constraints, not all of the firewall policy changes are being documented.</p> <ul style="list-style-type: none"> • Ensure all changes (minor and/or major) to the firewall policy are tracked and thoroughly documented. • Develop a mechanism to enforce updating the tracking document.
Cost	The cost to implement the above recommendation should be very minimal. For security team members it may take few additional minutes to thoroughly document changes to the firewall policy.

Checklist Number	Firewall Access and Configuration 3
Control Objective	Stay up-to-date on the firewall vendor recommended patches.
Pass / Fail	Fail
Risk	If the firewall software is not up-to-date with latest vendor specific patches, the firewall may be susceptible to exploits based on newly discovered vulnerabilities.
Recommendation	<p>The rate of vulnerabilities and patch availability has increased over the last few months; however, during the same duration, the rate of attacks on exploiting the vulnerabilities has increased tremendously. Exploits are developed within a very short duration after vulnerabilities have been discovered.</p> <ul style="list-style-type: none"> • Develop a procedure or a patch matrix indicating the criticality of the patch vs. the patch deployment time. For example, high category patches must be applied within X number of day(s), or medium category patches should be applied within Y number day(s). • Adhere to the guidelines developed in the patch matrix. • Formulate a procedure or a plan providing guidelines on general steps to perform prior to applying patches, such as backing up critical files. • Developed a controlled lab environment to simulate the production environment. It may assist in expediting the patch testing. • Establish a document indicating any business decisions that may cause delay in the deployment of the latest vendor recommended patches.
Cost	The cost to implement the above recommendation should be moderate. The cost may increase based on the depth of test lab development. The increased cost is offset by reducing the amount of time to deploy the patches. Implementing the latest possible patches reduces the possibility of being exploited; in short, it may potentially minimize the downtime in firewall services.

Checklist Number	Firewall Rule-base Validation 10
Control Objective	Routinely review and remove any temporary rules created in the firewall policy.
Pass / Fail	Fail
Risk	Temporary rules are usually created for testing and troubleshooting. If the temporary rules are not routinely reviewed and removed, potential unauthorized access may exist to and from the protected network. Such undocumented access may potentially jeopardize the organization's overall security posture.
Recommendation	<p>It is understandable that test or temporary rules exist in the firewall policy. However, it is imperative that all temporary rules must be periodically reviewed and removed.</p> <ul style="list-style-type: none"> • Provide sufficient comments such as creation date, deactivation date, creator of rule and responsible department on each test or temporary rule in the firewall policy. • Define the time interval in the security policy to review and remove any test or temporary rules in the firewall policy. • Adhere to the defined time interval to review the firewall policy.
Cost	The cost to implement the above recommendation should be very minimal. The time for one of the security personnel to add comments to all of the defined temporary rules is relatively minimal. If the habit of adding comments of test rules is developed and enforced, it may prevent potential unauthorized access to and from the protected network.

Following section includes the recommendations on each three audit checklist items that received pass with a caution flag. Since all three of them pass the audit, the cost factor should be very minimal to implement the suggested recommendations.

Checklist Number	Security Policy and Documentation 2
Control Objective	Any proposed changes to the security policy must be appropriately reviewed, approved and documented by the security team members prior to implementing changes on the firewall.
Pass / Fail	Pass with a caution flag
Recommendation	<p>All proposed changes are approved by the security personnel prior to implementing changes on the firewall; however, they are not being fully documented prior to implementation stage.</p> <ul style="list-style-type: none"> • Enforce a mechanism to ensure that all changes to the security policy are documented promptly.

Checklist Number	Firewall Access and Configuration 6
Control Objective	Routinely review the firewall policy and the security policy.

Pass / Fail	Pass with a caution flag
Recommendation	<p>The control objective indicated to routinely review the security and firewall policy. However, the defined review interval is not listed in the security policy,</p> <ul style="list-style-type: none"> Define and document an interval in the security policy to ensure both firewall and security policy is reviewed. Enforce a mechanism to ensure the review process occurs at the defined interval.

Checklist Number	Firewall Rule-base Validation 4
Control Objective	Any outbound traffic from the protected network must correspond to the approved and authorized outbound traffic rules defined in the security policy.
Pass / Fail	Pass with a caution flag
Recommendation	<p>There were two rules that were identified as business related traffic; Even though security personnel have provided the approved document listing exceptions, the information on this traffic was not documented in the security policy.</p> <ul style="list-style-type: none"> Review and update the security policy to ensure that all allowed traffic to and from the protected network is appropriately documented.

4.4 Cost Factor

The cost variable is dependent on various factors such as allocation of manpower and allocation or purchase of potential assets. The cost factor is also dependent on the organization's priorities as well as necessity to meet the defined Service Level Agreements (SLAs). Each organization has to strike a balance between cost factor and achieved benefit. In any event, if the cost outweighs a defined known risk, then appropriate document should be developed listing all acceptable risks.

The cost to remediate the above mentioned recommendation appears to be moderate because majority of the recommendations are not requiring technology changes. The majority of the cost associated with the above mentioned audit findings is allocation of the manpower.

Security management always faces a tradeoff between the cost factor and the benefits for any future security expenditures. Research from various written articles (can be found via www.google.com) can be used to understand the security ROI models, the risk exposure reduction as well as the threat protection models.

4.5 Compensating controls

It is always a challenge for security personnel to provide the highest level of security, while balancing the business needs and requirements. Providing a business service over the internet will always be exposed to a degree of risk. The function of the security personnel is to minimize the associated risk. In a majority of cases, the cost factor governs the defense in-depth strategy of an organization. Hence, if an organization is not able to purchase various potential security devices, they have to rely heavily on controls placed on the firewall operations. Meanwhile, it should be understood and discussed that there is no absolute security achieved by one or a few devices.

At this organization, some of the compensating controls are already in place, such as the Host based and the Network based Intrusion Detection Systems (IDS). In light of this, there are several compensating controls that exist.

1. Apply the latest vendor recommended specific OS patches, application patches, applicable security patches and hotfixes.
2. Ensure that the servers placed in the multi-tier DMZ environment are hardened and configured by following the generally accepted best security practices.
3. Define a policy and procedure that conducts vulnerability and risk assessment at a defined interval of the protected e-commerce environment.
4. Focus on achieving and maintaining strong change control management. Strict change management is essential for obtaining higher desired security levels.
5. Monitor the Host based and the Network based IDS logs routinely. Establish an Incident Response Team that can react quickly and aggressively, once a threat is identified.
6. If budget permits, a layer of protection can be added by implementing a host based firewall on the business critical servers.
7. Provide appropriate training for all team members who are a part of the security team, web developing team, as well as the network / system support team to maintain the highest level of knowledge and understanding.

Famous quotes from two security subject matter experts can put things in perspective:

- Bruce Schneier (www.schneier.com) “security is not a product, it is a process”.
- Marcus Ranum (www.ranum.com) “An ounce of prevention is worth a pound of detection”.

References

1. Bennett, Todd. "Auditing Firewalls: A practical Guide," URL: <http://www.itsecurity.com/papers/p5.htm> (14 July 2004).
2. Cavender, Terry. "Checkpoint Firewall Audit Program" January 2000. URL: <http://www.auditnet.org/docs/CheckpointFirewall.PDF> (15 July 2004).
3. Checkpoint knowledge base, reference guides and manuals. URL: <http://www.checkpoint.com> (18 July 2004).
4. Cheswick, William, Bellovin, Steven and Ruben, Aviel. editors. Firewalls and Internet Security: Repelling the Wily Hacker. Second edition. Addison-Wesley 2003.
5. Colin, Rose. "Computer Security Audit Checklist." April 8, 2002. URL: <http://www.itsecurity.com/papers/iomart2.htm> (15 July 2004).
6. Contribution based on personal accumulated experience and knowledge.
7. Horne, Jeff. "Auditing a Symantec VelociRaptor Firewall An Independent Auditor's Perspective." November 2003. URL: http://www.giac.org/practical/GSNA/Jeff_Horne_GSNA.pdf (18 July 2004).
8. Lowder, Jeff. "Administrator's Report on Auditing a Netscreen-100 Firewall." August 7, 2003. URL: http://www.giac.org/practical/GSNA/Jeff_Lowder_GSNA.pdf (18 July 2004).
9. SANS Various Authors. Auditing Networks, Perimeters and Systems. The SANS Institute 2004.
10. Spitzner, Lance. Auditing your Firewall Setup." December 12, 2000. URL: <http://www.spitzner.net/audit.html> (15 July 2004).
11. Spitzner, Lance. "Building your Firewall Rulebase." January 26, 2000. URL: <http://www.spitzner.net/rules.html> (15 July 2004).
12. Tipton, Harold and Micki Krause, editors. Information Security Management Handbook. Fourth edition. Auerbach Publications, 2000.
13. Tu, James. "Auditing a Nokia 440 Checkpoint Firewall -1 An Auditor's Perspective." June 2002. URL: http://www.giac.org/practical/James_Tu_GSNA.doc (18 July 2004).

14. Various Audit Programs; various authors. URL: <http://www.auditnet.org> (15 July 2004).
15. Wack, John, Cutler, Ken and Pole Jamie. "Guidelines on Firewalls and Firewall Policy." January 2002. URL <http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf>. (15 July 2004).

© SANS Institute 2004, Author retains full rights.

Appendix A: Security Policy

The below snapshot depicts a small portion of the established corporate security policy. It provides details of the traffic flow to and from the protected e-commerce environment.

Security Policy for e-commerce hosting site

The purpose of the security policy is to define traffic allowed to and from the protected e-commerce hosting environment.

Traffic to Web DMZ

- o From the internet, allow the HTTP and HTTPS protocols to all of the web server's defined IP address.
- o Provide necessary NAT to all incoming HTTP and HTTPS traffic
- o Provide web developers and network / systems engineers management capabilities (from specific sources, to specific destinations, on specific ports).
- o Allow any additional network management (such as SNMP) traffic from the corporate networks (from specific sources, to specific destinations, on specific ports).
- o Inbound IDS traffic from corporate IDS management servers (from specific sources, to specific destinations, on specific ports).

Traffic to APP DMZ

- o From Web DMZ allow defined protocols to defined servers in defined servers in the App DMZ
- o Provide web and application developers and network / systems engineers management capabilities (from specific sources, to specific destinations, on specific ports).
- o Allow any additional network management (such as SNMP) traffic from the corporate networks (from specific sources, to specific destinations, on specific ports).
- o Inbound IDS traffic from corporate IDS management servers (from specific sources, to specific destinations, on specific ports).

Traffic to Database DMZ

- o From Web DMZ allow defined protocols to defined servers in defined servers in the database DMZ
- o From App DMZ allow defined protocols to defined servers in defined servers in the database DMZ
- o Provide database administrators and network / systems engineers management capabilities (from specific sources, to specific destinations, on specific ports).
- o Allow any additional network management (such as SNMP) traffic from the corporate networks (from specific sources, to specific destinations, on specific ports).
- o Inbound IDS traffic from corporate IDS management servers (from specific sources, to specific destinations, on specific ports).

Traffic to Corporate

- o No traffic should originate from the any of the multi-tier DMZ to the corporate unless it is specifically defined.
- o For application synchronization, from defined App servers to corporate internal app servers (from specific sources, to specific destinations, on specific ports).
- o For database synchronization, from defined database servers to corporate internal database servers (from specific sources, to specific destinations, on specific ports).

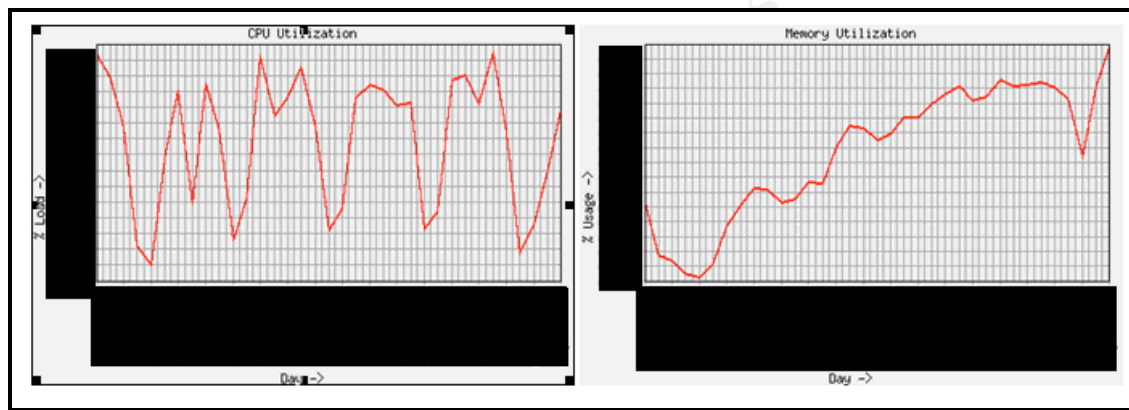
From any DMZ

- o When required for patch management, allow outbound HTTP, HTTPS and DNS traffic (from specific sources, to specific destinations).

Appendix B: Baseline of the Firewall

The organization has done an outstanding job in establishing the baseline of firewall utilization. The security personnel maintain the firewall hardware (Nokia platform) utilization baseline, firewall software (Checkpoint) utilization baseline as well as the network bandwidth utilization baseline. The organization has established procedure to generate snapshots of firewall utilization at a defined interval. Comparing the routine snapshots with the baseline as well as with the snapshots of the previous interval provides great visibility in identifying any anomalies. It also assists in identifying any potential bottlenecks. The information gathered by routine snapshots provides guidelines to make sound decisions on any future investments in the security arena.

Firewall hardware utilization snapshot obtain via the Nokia Voyager.



Firewall Software utilization snapshot obtain via the Checkpoint SmartView Monitor.

