Global Information Assurance Certification Paper

James Tu

SANS GSNA

Practical Assignment Version 2.0

June 2002

Auditing a Nokia 440 Check Point Firewall -1 Firewall: An Auditor's Perspective

Contents

Disclaimer

This document sanitizes a delivered Checkpoint Firewall -1 Audit Report performed by me. It extracts actual text to provide a sample of the breadth and depth of th e actual audit process. Due to the nature of the information provided, all listed ip a ddresses are randomly altered.

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

1.1 Introduction

The objective of this security audit was to ensure the company firewall is in compliance with established security policy. The targeted firewalls are Nokia 440 Check Point Firewall-1 appliances (Check Point Firewall-1 version 4.1sp5a, VRRP fail over enabled), which perform stateful packet inspection on all inbound and outbound corporate office Internet traffic, and provide dynamic and static address translation. This is THE primary defence for the organization.

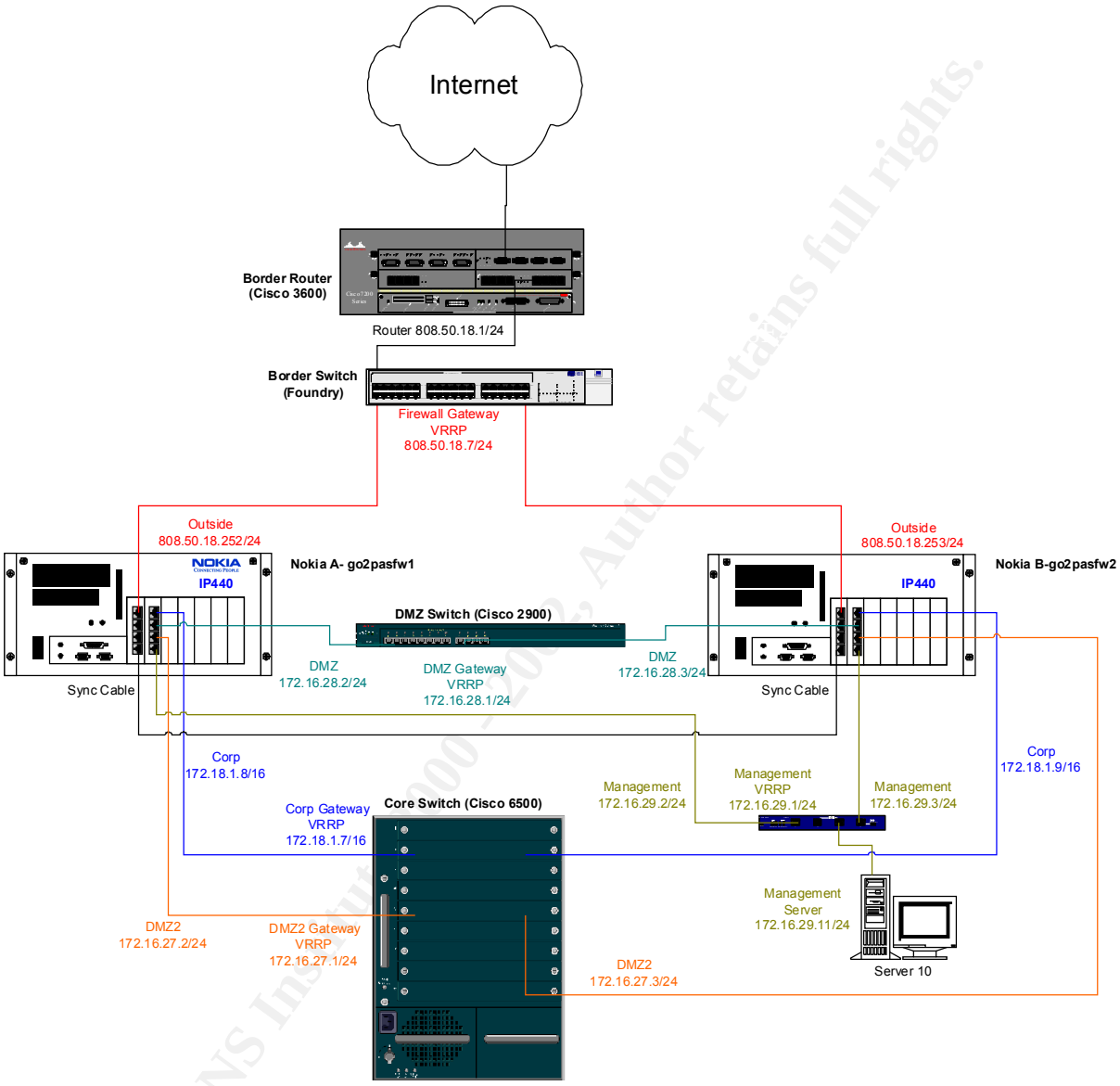
Any mistakes in configuring the firewall, or the compromise of the firewall appliance itself, will directly affect the business operations, and the integrity, availability and confidentiality of the corporate data, due to the fact that this firewall is the only public entry point, and the company is employing an internal flat virtual LAN. It means if one of the internal hosts is compromised, it could be used to attack all the company's important application servers and database servers.

The scope of this audit project is limited to the Nokia Check Point Firewall-1 firewall security architecture, which includes two Nokia 440 appliances, the Nokia appliance configuration, and the firewall rule base.

Assume the upstream CISCO router and the Foundry switch are configured according to best practice with appropriate ingress and egress filtering. And the windows based firewall management station itself is hardened and immune to compromise.

1.2 Description of the system

Network Diagram:



Configuration:

Package	Nokia A	Nokia B
Operating System Software	IPSO 3.4.1 (includes SNMP f ix)	IPSO 3.4.1 (includes SNMP fix)
Administrator Name	admin	admin
Administrator Password	****	****
Checkpoint Software	FireWall-1 Version 4.1 Se Pack 5a	FireWall-1 Version 4.1 Service Pac

Interface	Nokia A IP Address	Nokia B IP Address
Eth-s1p1c0	808.50.18.252	808.50.18.253
Eth-s1p4c0	State Synchronization Cable	State Synchronization Cable
Eth-s2p1c0	172.18.1.8	172.18.1.9
Eth-s2p2c0	172.16.27.2	172.16.27.3
Eth-s2p3c0	172.16.28.2	172.16.28.3
Eth-s2p4c0	172.16.29.2	172.16.29.3

Interface	Network Purpose	Virtual IP Address
Eth-s1p1c0	Outside	208.50.18.7
Eth-s1p4c0	State Synchronization Cable	State Synchronization Cable
Eth-s2p1c0	Corporate Network	172.18.1.7
Eth-s2p2c0	DMZ2	172.16.27.1
Eth-s2p3c0	DMZ	172.16.28.1
Eth-s2p4c0	Firewall Management	172.16.29.1

	Wiring Connection Table				
	Primary firewall	Secondary firewall	vrrp IP	Primary IP	Secondary IP
S1P1	outside Foundry Port 21	outside Foundry Port 23	808.50.18.7	808.50.18.252	808.50.18.253
S1P2	empty	empty			
S1P3	empty	empty			
S1P4	secondary firewall S1P4	primary firewall S1P4	n/a	10.150.200.1	10.150.200.2
S2P1	6509 blade 7 port 43	6509 blade 9 port 14	172.18.1.7	172.18.1.8	172.18.1.9
S2P2	6509 blade 7 port 6	6509 blade 6 port 3	172.16.27.1	172.16.27.2	172.16.27.3
S2P3	2900 port 1	2900 port 6	172.16.28.1	172.16.28.2	172.16.28.3
S2P4	netgear port 3	netgear port 1	172.16.29.1	172.16.29.2	172.16.29.3

1.3 Risk to the architecture in review

Obviously the firewall is used to separate the un -trusted public network to the internal trusted network. Per communication with the network engineering team, no Access control lists are placed on the upstream CISCO router, all the outside traffics are directly hitting the firewall, and it is susceptible to deny of service attack. In the event of DOS attack, due to heavy load issue, administrator may not be able to log into the firewall to review the log and modify the rule base to block the offending source. The internal private network is a single flat virtual network, and the firewall does not limit any outbound traffic. Any compromise, a single internal host, will be able to comprise the whole company network.

High availability is achieved by using Nokia's award winning VRRP protocol to conduct automatic fail over.

1.4 Current state of practice

Lowder's [1] *paper on firewall management and internal attacks :*

The benefits of having a firewall are:

- Protection of the organizer's network from intruders
- Protection of external networks from intruders within the organiz ation
- Protection from "due care" lawsuits
- Increased ability to enforce network standards and policies
- Centralized internet work audit capability

As Lowder further mentioned, three attacks/threats each modern firewall should be able to address:

- Internet Pro tocol (IP) Source Address Spoofing
- TCP Hijacking
- Denial of Services

Although Lowder did not suggest an audit check list, but he did provide a solid fir e-wall standards as:

Under Firewall Configuration

a. Default policy (allow or deny) on network connections
b. Physical locations of firewall.
c. Logical location of firewall in relation to other network nodes
d. Firewall system access policy.
    1. Authorized individuals
    2. Authentication methods
    3. Policy on remote configuration
e. Supported services
    1. Inbound
    2. Outbound
f. Blocked services
    1. Inbound
    2. Outbound

Under Backups

a. Frequency of incremental backups
b. Frequency of system backups
c. Archive of backups
d. Off-site backup requirements

Review/comments on Lowder's paper:

A good firewall audit policy should be consistent with the deployed firewall sta n-dards. The audit process should include the review of the default security policy, a l-lowed services and blocked services, backup procedures, access control and finally make sure the firewall is in deed configured correctly into preventing IP source a d-dress spoofing, TCP hijacking and certain type of deny of service attack like TCP SYN attack, ICMP Echo Flood.

Ben Rothke's [2] *presentation at WebSec 2000 on testing Check Point firewall -1:*

His definition of firewall is:

- Protection from all known hacker atta cks
- All traffic from inside to outside and vice -versa must pass through the firewall
- The firewall itself is immune to penetration
- An expensive ways to slow down a network -Marcus Ranum

An excellent firewall audit list is followed:

- Review corporate firewall policy
- Review network infrastructure
- Interview firewall and system administrators
- Run host & network assessment scans
- Review Firewall-1 configuration
- Review Firewall-1 rule base
- Put it all together in a report
- Fix problems
- Redo as necessary

Under Policy:

Policy is a critical element of the effective and successful operation of a firewall. A firewall cannot be effective unless it is deployed in the context of working policies that govern its use and administration. Most firewalls operate in an environment where everything is denied. Only that which is specifically authorized is a llowed.

Under Services/protocols/users:

Too many services can hinder the efficiency of the firewall, each service should be authorized, if not disable it.

Under Log review:

The logs should reflect any network scans.

Under rule base review:

Stealth rule ensures that no body can directly connect or communicate to the fir e-wall, other than administrators that are GUI authorized.

Under configuration:

- Ensure FW is appropriately configured
- Determine latest patch installation
- Review system settings
- Only necessary services and applications are run
- No direct modem connection

Review/comments on Rothke's paper:

I believe this is the best firewall audit checklist available so far, and most of hi s steps are incorporated into the actual creation of the audit checklist. Both subjective and objectives audit list are used. For each objective control list, reviewing the system configuration settings will be done first, then, if possible, followed wit h scanning and penetrating tests to objectively verify the settings.

Lance Spitzner 's [4] [7] *papers on auditing your firewall & Rule Base:*

Here is a summary of Lance's audit checklist:

1. Define what you expect, means the firewall security policy.
2. Audit Methodology
    a. Test the firewall itself. Port scans from both internal and external, scanning for icmp, udp and tcp. Identify, what, if any ports are open on your firewall. Disable unnecessary ports.

       Make sure every rule base should have a lockdown rule at the begin-ning that denies any traffic to the firewall.

    b. Test the rule base. Scan from each network segment between each other.

    c. Investigate further to determine what potential vulnerabilities exist for the accessible resources.

Review/comments on Spitzner's pap er:

Understand the firewall security policy, and understand the firewall configuration, only allow authorized services to run on the firewall itself. Check the lockdown rule and its placement. When running nmap scan, make multiple runs, scanning for icmp, udp and tcp and comparing the results.

There are many good resources, which provide excellent documents describing the methodology and tools for auditing a firewall. Please review the references list for further reading.

1.5 Need of Improvement

This audit will adopt most of the above mentioned firewall audit methodology, audit checklist, but will improve on the following areas:

There are not many available information addressing the Nokia appliance configur a-tion issue itself, the specific port/services r unning, configuration settings, suggested remote management configuration, image backup, restore and how to make it i m-mune to attack. This audit hopefully will add value and detail info the understanding of the Nokia appliance secure configuration and mana gement.

Major efforts spent on the understanding of various of Firewall -1 service ports, http://phoneboy.com [9], Check Point Firewall-1 tech documents [10] and internet research were done extensively, the final result s presented in this audit report will help other folks to better explain and understand the nmap scan results on Check Point firewall-1 firewall.

This audit also emphasized that for each reviewed manual rule/configuration setting, if possible, should be fo llowed with scanning, penetrative testing to double check and verify the configuration. If nmap is used, multiple runs using icmp, tcp and udp are employed to get better and more accurate results.

Most of the resources on firewall auditing focus more on th e rule base, but due to the unique firewall architecture here: Nokia appliances as the gateway implementing the policy. It is beneficial to include in depth auditing on the Nokia appliance in addition to the firewall rule base. Here we break down the actua l firewall audit into two parts, they are:

- The Nokia 440 appliance audit
- Firewall rule base audit

2. Assignment 2 – Create an Audit Checklist

2.1 Current firewall security policy

Many efforts were spent to understand the company security policy and its firewall security policy/standard and procedures, if any. Here is the company security policy:

Corporate Security Policy: Information is a corporate asset and must be protected. Security controls must be applied consistent with the value of the informatio n. Critical information will require more stringent controls.

Under Internet and Extranet:

All Internet access must be made through the Overture firewall…

All public connections must be controlled via the perimeter firewall prior to accessing the private network.

Firewall definition :

A firewall as a system with the following set of characteristics:

- All traffic between the two networks must pass through the firewall.
- Deny by default.
- Only traffic that is authorized by the local security policy will be allowed to pass.
- The firewall itself is immune to penetration.
- The system must provide adequate logging and auditing features.

There were no formal written firewall policy and procedures; here is the implied "idea" policy per interviewing with firewall ad ministrators:

Local Firewall Policy:

- Deny all services by default.
- Traffic initiated from outside (internet): only to selected static NATed servers located at the DMZ zone with r estricted port and services per application. It means all hosts with public accessible ip address assigned must locate at the DMZ zone.
- Traffic initiated from inside to outside (Internet): based on business needs.
- Traffic initiated form inside to DMZ: only authorized services.
- Traffic initiated from DMZ to private network: only au thorized services.
- Traffic to the firewall and management station: only from authorized loc a-tion/hosts.

- Only authorized firewall administrators can access the firewall and its ma n-agement station, rule change should go through change management control.
- No public IP addresses assigned directly to internal hosts/devices. All sites will follow the corporate wide private ip address assignment scheme managed by corp. systems/network engineering.
- Centralized logging and management capability of all corporate offi ce fire-walls.
- Check Point firewall-1 on a Nokia appliance as corporate office network fir e-wall standard.

The format of the audit checklist is made of the following 7 fields, they are:

1. List number
2. Control objective
3. References
4. Objective or subjective
5. Why to audit, risk involved
6. Audit commands/actions
7. Expected results

2.2 Nokia 440 audit checklist

There is no specific audit checklist on Nokia appliance available; this list is mainly based on this author's past experiences, the general methodology and recommendations from the reviews of the state of current practice. The main goal is to verify that the Nokia gateway itself immune to penetration or compromise.

We asked the firewall administrator to fill out the following form to provide Nokia Appliance related information. Here is the form:

Questions	**Response**
Purpose of the Nokia Appliance	Enforce the corporate security policy
Physical location	Server room
Management access method	SSH, SSL web access from inside interfaces
User Accounts	All admin level users, total three users
Services should be running on the Nokia	Firewall-1 module
Backup	Undocumented, sometime
Patch/Image Update	Undocumented, sometime

The Nokia appliance audit checklist has seven items, here they are:

List number	**Nokia Appliance Audit 1**
Control objective	The Nokia appliance is located at a physical secure location.
References	Rothke, Lowder, Northcutt, others
Objective or Subjective	Objective
Why to audit, risks involved	If anyone can access the Nokia appliance, can easily cause deny of service, like turn off the power, unplug the network cable, steal the firewall.
Audit commands/actions	Visit the locked server room.
Expected results	Nokia appliance should be located at the secure server room.

List number	**Nokia Appliance Audit 2**
Control objective	The Nokia appliance's image and patch is current.
References	Lowder, Northcutt, Bothke, Spitzner and own experiences
Objective or Subjective	Objective
Why to audit, risks involved	The newest image and patch normally will fix a lot of known vulnerabilities after the previous image release.
	Most of the existing exploits may only work with the old image version/patch level.
Audit commands/actions	Using Nokia Voyager web browser, click configuration, then show configuration summary.
Expected results	Image: IPSO-2.4.1-FCS10-12.12.2001-210900-910
	Installed Packages: Check Point FireWall-1 (Strong) Version 4.1 SP-5a (Mon Jan 21 13:45:13 IST 2002 Build 341561)

List number	Nokia Appliance Audit 3
Control objective	The Nokia appliance have a user access control list
References	Own experiences, Lowder
Objective or Subjective	Objective
Why to audit, risks involved	Prevent shared accounts and default accounts, make user accountable.
Audit commands/actions	Using Nokia Voyager web browser to verify, under security and access configuration.
Expected results	Separate users accounts.

List number	Nokia Appliance Audit 4
Control objective	Secure protocols/methods are used to conduct remote management, SSL and SSH v2
References	Own experiences, Cheswick, Spitzner, Lowder
Objective or Subjective	Objective
Why to audit, risks involved	SSL and SSH will transmit password in encrypted form, to prevent network sniffing. Http and telnet transmit password in clear text
Audit commands/actions	Using Nokia Voyager web browser to verify, under security and access configuration
Expected results	Under Network Access and Services:
	Access: telnet access & admin network login should be disabled.
	Services: all disabled
	Under Voyager Web Access:
	Access: web access enabled, SSL security enabled
	TCP ports: voyager (HTTP): 80, SSL Voyager (HTTPS): 443
	Under SSH (Secure Shell)
	SSH services: enabled
Audit commands/actions	RUN netstat -na on the Nokia box
Expected results	Only SSL (443) and SSH (22) are enabled, no port 23 (telnet) and port 80 open

List number	Nokia Appliance Audit 5
Control objective	The Nokia appliance's log is reviewed regularly and backed up
References	Common experiences, Lowder, Spitzner, Rothke
Objective or Subjective	Subjective
Why to audit, risks involved	Logs are used to monitor any security intrusion, and system errors. Should be backed up and stored at a secure location for Future investigation and troubleshooting purpose.
Audit commands /actions	Ask the firewall administrator, if yes, verify the voyage login access, and see the log for backup action taken in the past and backup tape.
Expected results	Regular backup and view log daily.

List number	Nokia Appliance Audit 6
Control obje ctive	The Nokia's configuration is backed up securely, and after each configur a-tion change
References	Nokia manual, own experiences, Lowder
Objective or Subjective	Objective and Subjective
Why to audit, risks involved	In the event of hardware failur e, the fastest way to install a new replac e-ment Nokia is to use the saved Configuration backup files. It should be backed up after each configuration change. Then the backup files must be transfer Out of the Nokia box to a safe location.
Audit commands/ actions	Ask the firewall administrator: if they have performed backup, and if they transfer the backup out the Nokia to another secure location. Using Nokia Voyager web browser to verify, under backup and restore configuration,
Expected results	They sho uld backup after each configuration change, then ftp the image out.

List number	Nokia Appliance Audit 7
Control objective	The Nokia should have no open ports on its external interface, and only SSH and SSL on its internal interfaces for remote manage ment, plus ne c-essary default firewall -1 service ports.
References	Spitzner, Rothke and own experiences, Nmap web site, Cheswick, Lowder
Objective or Subjective	Objective
Why to audit, risks involved	No open ports, no vulnerability. Especially for its ex ternal interface, which is accessible from the public network.
Audit commands/actions	Use Nmap to SCAN all the interfaces, both TCP and UDP scan. External Interface: nmap -sS -P0 -p1-1024 -n -r -vv -oN hss.txt 808.50.18.252 nmap -sT -P0 -p1-1024 -n -r -vv -oN hst.txt 808.50.18.252 nmap -sU -P0 -p1-1024 -n -r -vv -oN hsu.txt 808.50.18.252 Internal Interface: nmap -sT -p1-65535 172.18.1.8 > scan2.txt nmap -sU -p1-65535 172.18.1.8 > udp.txt nmap -sS -p1-65535 172.18.1.8 > sscan.txt
Expected r esults	External interface: no open ports Internal interface: port 22 (SSH), port 443 (SSL)

List number	Nokia Appliance Audit 8
Control objective	Verity VRRP high availability function of the Nokia pair.
References	Rothke, own experiences. Nokia manual
Objective or Subjective	Objective
Why to audit, risks involved	High availability is vital to this company, against firewall hardware pro b-lems. The firewall is the only entry point.

Audit commands/actions	SSH to the primary Nokia box, run show vrrp, verify the master status, SSH to the backup Nokia box, run show vrrp, verify the backup status. Unplug the external interface cable to the primary Nokia, repeat the above ssh procedures, to verity the new vrrp status on both the primary and backup.
Expected results	Firewall still pass traffic as normal, run show vrrp command, the backup Nokia will become the primary

2.3 Firewall rule base checklist

Again, a survey form was filled out by the firewall administrator, detailing the known supported applications and authorized protocols. Here is the form:

Application	Host Name	internal ip address	external ip address	Protocol	Traffic Direc-tion
Receiving Mail Server	vito	172.18.28.10	808.50.18.10	smtp	in-bound
OWA mail server	exch2	172.18.1.158	808.50.18.112	https	in-bound
pop/imap server1	xchg	172.18.1.159	808.50.18.11	pop/imap	in-bound
pop/imap server2	exchg1	172.18.1.156	808.50.18.111	pop/imap	in-bound
PPTP server	win2k-vpn	172.18.2.31	808.50.18.50	pptp	in-bound
SSH server	bruno	172.18.1.54	808.50.18.9	ssh	in-bound
Firewall hide NAT			808.50.18.5	any	out-bound
Nokia External Interfaces			808.50.18.252		
Nokia External Interfaces			808.50.18.253		
Nokia External VIP			808.50.18.7		
CISCO upstream router			808.50.18.1		

The firewall rule base audit check has a total of seven items, here they are:

List number	**Firewall Rulebase Audit 1**
Control objective	Only authorized applications and protocols are allowed to pass the firewall.
References	Rothke, own experiences, nmap web site, Spitzner
Objective or Subjective	Objective
Why to audit, risks involved	The security policy is to deny everything by default, and only allow authorized applications and protocols to pass the firewall. Undocumented applica tions, protocols and open service ports are grounds to suspect compromised hosts, backdoors. Close unnecessary server ports to limit the vulnerabilities without affecting the normal applications.
Audit commands/actions	Login the firewall client GUI, policy editor, manual review the rule base, make sure proper rules are in place to support the applications. Nmap scan from the outside. nmap -sS -vv -n -r -oN hnss.txt 808.50.18.0/24 nmap -sT -vv -n -r -oN hnst.txt 808.50.18.0/24
Expected results	Only authorized applications and protocols are allowed to pass the firewall. R e-fer to the application survey form.

List number	Firewall Rulebase Audit 2
Control objective	Only authorized hosts can access the firewall and management host, drop other access
References	Rothke on stealth rule, own experiences
Objective or Subjective	Objective
Why to audit, risks involved	Limit who can access and Nokia and management console to protect the Nokia and management console. Drop other connection.
Audit commands/actions	Run https to Nokia (https://172.18.1.8) from host 172.18.1.119 Run https to Nokia (https://172.18.1.8) from host 172.18.108.99 Review the firewall rule on GUI policy editor, see if we can find the rules
Expected results	Per firewall adm inistrator, only users from Scanner (172.18.1.116) can access the Nokia to run SSH and SSL.

List number	Firewall Rulebase Audit 3
Control objective	There should be a general drop rule at last, and log the drop actions.
References	Own experiences, check point firewall manual, firewall forum on Internet
Objective or Subjective	Objective
Why to audit, risks involved	Review the drop rule will reveal any hacking activities, or just host configuration errors. Firewall default will drop any unauthorized rules, but will not log the info. So this drop all rule will need to be created and logged.
Audit commands/actions	Review the GUI, make sure the last firewall rule is the drop all rule. It is logged. Review the firewall log; see it has logged all the pr evious nmap scan results.
Expected results	the drop rule: any any any drop short gateways any last drop rule and drop log will reveal the nmap scan.

List number	Firewall Rulebase Audit 4
Control objective	Log should be enabled on all the rules; una uthorized actions should be logged. Logs are backed up and reviewed regularly.
References	Lowder, Rothke
Objective or Subjective	Objective & subjective
Why to audit, risks involved	Log is the only way to track down any past intrusion activities. Revie w the drop log, will reveal any past intrusion attempt and for troubleshooting purpose.
Audit commands/actions	Use GUI policy editor, make sure log in enabled on each rule, ask the firewall administrator on backup, if yes, show backup log. Run GUI log viewer; find any activities related to the May 21 outside nmap scan activities.
Expected results	Logs are enabled on the entire rule, and log viewer should show the drop a c-tions on the nmap scan conducted on May 21. Logs are backup to tape regularly.

List number	Firewall Rulebase Audit 5
Control objective	Change control should be in place on any rule change
References	Own experiences, Lowder
Objective or Subjective	Subjective
Why to audit, risks involved	Any rule change should be examined again fi rewall security policy, document why, who requested, who made the change.
Audit commands/actions	Ask the firewall administration on docs to review, review the GUI policy editor to see the comments field.
Expected results	Written doc on firewall change co ntrol, and use comment filed on GUI policy

	editor to specify who, when.

List number	**Firewall Rulebase Audit 6**
Control objective	SYNDefender should be used.
References	Lowder, Goncalves & Brown
Objective or Subjective	Objective
Why to audit, risks inv olved	Again Deny of Service Attack.
Audit commands/actions	Firewall GUI, Policy Properties setup, under SYNDefender, verify the SYN gateway or Passive SYN Gateway is selected.
Expected results	Enabled on the firewall properties setup

List number	**Firewa ll Rulebase Audit 7**
Control objective	Anti spoofing should be enforced on the gateway interface.
References	Lowder
Objective or Subjective	Objective
Why to audit, risks involved	Spoofing is a technique by which an intruder attempts to gain unauthor ized access by altering a packet's IP address to make it appear as though the packet originated in a part of the network with higher access privileges. For example, a packet originating on the Internet may be disguised as a local network packet.
Audit com mands/actions	GUI policy editor, manage, network objects, gateway object, interfaces, check settings
Expected results	Under Valid Addresses: This net.

3. Assignment 3 – Conduct the Audit

The format to present the actual audit results is made of the foll owing 7 fields, they are:

1. List number
2. Control objective
3. Audit commands/actions
4. Expected results
5. Actual results
6. Pass or Fail
7. Comments (optional)

3.1 Nokia appliance audit

List number	Nokia Appliance Audit 1
Control objective	The Noki a appliance is located at a physical secure location.
Audit commands/actions	Visit the locked server room
Expected results	Nokia appliance should be located at the secure server room.
Actual results	Nokia appliance is located at the server room. NOC monitors the room via a video camera. Only selected individuals with access badge can access the room.
Pass or Fail	Pass

List number	Nokia Appliance Audit 2
Control objective	The Nokia appliance's image and patch is current.
Audit commands/actions	Using Nokia Voyager web browser, click configuration, then show co n-figuration summary
Expected results	Per http://www.checkpoint.com, current image: IPSO -2.4.1-FCS10-12.12.2001-210900-910 Check Point FireWall -1 (Strong) Version 4.1 SP -5a (Mon Jan 21 13:45:13 IST 2002 Build 341561)
Actual results	Current selected image: IPSO -2.4.1-FCS10-12.12.2001-210900-910 Installed Packages: Check Point FireWall -1 (Strong) Version 4.1 SP -5a (Mon Jan 21 13:45:13 IST 2002 Build 341561)
Pass or Fail	Pass

List number	Nokia Appliance Audit 3
Control objective	The Nokia appliance has a user access control list.
Audit commands/actions	Using Nokia Voyager web browser to verify, under security and access configuration
Expected results	Separate users accounts for each firewall administrator.
Actual results	Username: admin, alex, charley,monitor, root, all have Admin type, e x-cept monitor as Monitor Type.
Pass or Fail	Pass

List number	Nokia Appliance Audit 4
Control objectives	Secure protocols/methods are used to co nduct remote management, SSL and SSH v2.
Audit commands/actions	Using Nokia Voyager web browser to verify, under security and access configuration
Expected results	Under Network Access and Services: Access: telnet access & admin network log in should be disabled. Services: all disabled Under Voyager Web Access: Access: web access enabled, SSL security enabled TCP ports: voyager (HTTP): 80, SSL Voyager (HTTPS): 443 Under SSH (Secure Shell) SSH services: enabled
Actual results	Under Network Access and Services: Access: telnet access & admin network login should be disabled. Services: all disabled Under Voyager Web Access: Access: web access enabled, SSL security enabled TCP ports: voyager (HTTP): 80, SSL Voyager (HTTPS): 443 Under SSH (Secure Shell) SSH services: enabled Protocol versions: 1 and 2 Admin login: permitted Authentication modes: DSA, Password, RSA
Audit commands/actions	RUN netstat -na on the Nokia box
Expected results	Only SSL (4430 and SSH (22) are enabled , no port 23 (ftp) and port 80 open

Actual results	go2pas-fw1[admin]# netstat -na Active Internet connections (including servers) Proto Recv-Q Send-Q Local Address Foreign Address (state) tcp 0 0 *.22 *.* LISTEN tcp 0 0 *.256 *.* LISTEN tcp 0 0 *.259 *.* LI STEN tcp 0 0 *.262 *.* LISTEN tcp 0 0 *.264 *.* LISTEN tcp 0 0 *.265 *.* LISTEN tcp 0 0 *.443 *.* LISTEN tcp 0 0 *.900 *.* LISTEN tcp 0 0 *.1056 *.* LISTEN tcp 0 0 *.1057 *.* LISTEN tcp 0 0 *.1058 *.* LISTEN tcp 0 0 *.1059 *.* LISTEN tcp 0 0 *.1060 *.* LISTEN tcp 0 0 *. 1061 *.* LISTEN tcp 0 0 *.18183 *.* LISTEN tcp 0 0 *.18184 *.* LISTEN tcp 0 0 *.19190 *.* LISTEN tcp 0 0 *.19191 *.* LISTEN tcp 0 0 10.150.200.1.256 10.150.200.2.1038 ESTA B- LISHED tcp 0 428 10.150.200.1.1111 10.150.200.2.256 ESTA B- LISHED tcp 0 0 127.0.0.1.80 *.* LISTEN tcp 0 0 127.0.0.1.1387 127.0.0.1.19190 TIME_WAIT tcp 0 0 127.0.0.1.1388 127.0.0.1.19190 TIME_WAIT tcp 0 0 127.0.0.1.1389 127.0.0.1.19190 ESTA B- LISHED tcp 0 0 127.0.0.1.1390 127.0.0.1.19190 ESTA B- LISHED tcp 0 0 127.0.0.1.1391 127.0.0.1.19190 ESTA B- LISHED tcp 0 0 127.0.0.1.1392 127.0.0.1. 19190 ESTA B- LISHED tcp 0 0 127.0.0.1.1393 127.0.0.1.19190 ESTA B- LISHED tcp 0 0 127.0.0.1.1394 127.0.0.1.19190 ESTA B- LISHED tcp 0 0 127.0.0.1.19190 127.0.0.1.1389 ESTA B- LISHED tcp 0 0 127.0.0.1.19190 127.0.0.1.1390 ESTA B- LISHED tcp 0 0 127.0.0.1.19190 127.0.0.1.1391 ESTA B- LISHED tcp 0 0 127.0.0.1.19190 127.0.0.1.1392 ESTA B- LISHED tcp 0 0 127.0.0.1.19190 127.0.0.1.1393 ESTA B- LISHED tcp 0 0 127.0.0.1.19190 127.0.0.1.1394 ESTA B- LISHED tcp 0 384 172.16.29.2.3211 172.16.29.11.257 ESTA B- LISHED tcp 0 0 172.18.1.8. 22 172.18.106.11.1092 ESTA B- LISHED tcp 0 888 172.18.1.8.22 172.18.106.31.1348 ESTA B- LISHED udp 0 0 *.259 *.* udp 0 0 *.514 *.* udp 0 0 ::.514 ::.* go2pas-fw1[admin]# Port 22 And port 443 there, no port 23 (telnet) and port 80 (http)

Pass or Fail	Pass
Comments	There are more open ports than necessary, mostly are default Check Point firewall-1 features/services. Per admin survey, only firewall -1 module are used, should disable most of the other ports.

List number	**Nokia Appliance Audit 5**
Control objective	The Nokia appliance's log is reviewed regularly and backed up.
Audit commands/actions	Ask the firewall administrator, if yes, verify the voyage login access, and see the log for backup action taken in the past and backup tape.
Expected results	Regular backup and view log daily.
Actual results	Per firewall administrator, logs are not reviewed daily, nor backed up.
Pass or Fail	Fail

List number	**Nokia Appliance Audit 6**
Control objective	The Nokia's configuration is backed up securely, and after each configur a-tion change.
Audit commands/actions	Ask the firewall admi nistrator: if they have performed backup, and if they transfer the backup out the Nokia to another secure location. Using Nokia Voyager web browser to verify, under backup and restore co n-figuration,
Expected results	They should backup after each configura tion change, then ftp the image out.
Actual results	Under Voyager backup and restoration configuration: backup /opt/firewall -1-strong. V4.1.sp -5a is enabled, only one backup file is available, which is fw1 -2002-04-04.tgz Asked firewall administrator for any backup policy and procedures, it is told that no policy on backup and restoration, the only backup done is just for testing purpose. The backup file stays in the Nokia, not transferred out.
Pass or Fail	Fail

List number	**Nokia Appliance Audit 7**
Control objective	The Nokia should have no open ports on its external interface, and only SSH and SSL on its internal interfaces for remote management, plus necessary default firewall-1 service ports.
Audit commands/actions	Use Nmap to SCAN all the interfaces, both TCP and UDP scan. External Interface: nmap -sS -P0 -p1-1024 -n -r -vv -oN hss.txt 808.50.18.252 nmap -sT -P0 -p1-1024 -n -r -vv -oN hst.txt 808.50.18.252 nmap -sU -P0 -p1-1024 -n -r -vv -oN hsu.txt 808.50.18.252 Internal Inter face: nmap -sT -p1-65535 172.18.1.8 > scan2.txt nmap -sU -p1-65535 172.18.1.8 > udp.txt nmap -sS -p1-65535 172.18.1.8 > sscan.txt
Expected results	External interface: no open ports except port 264 and port 265 Internal interface: port 22 (SSH), por t 443 (SSL)

External Interface:

```
# nmap (V. 2.54BETA22) scan initiated Tue May 21 21:13:43
2002 as:
nmap -sS -P0 -p1-1024 -n -r -vv -oN hss.txt 808.50.18.252
Interesting ports on  (808.50.18.252):
(The 1020 ports scanned but not shown below are in state:
filtered)
Port       State       Service
53/tcp     closed      domain
264/tcp    open        bgmp
265/tcp    open        unknown
500/tcp    closed      isakmp
```

Actual Results

```
# Nmap run completed at Tue May 21 21:17:09 2002   -- 1 IP ad-
dress (1 host up)
```

scanned in 206 seconds

```
# nmap (V. 2.54BETA22) scan initiated Tue May 21 21:18:49
2002 as: nmap  -sT -P0
-p1-1024 -n -r -vv -oN hst.txt 808.50.18.252
Interesting ports on  (808.50.18.252):
(The 1020 ports scanned but not shown below are in s  tate:
filtered)
Port       State       Service
53/tcp     closed      domain
264/tcp    open        bgmp
265/tcp    open        unknown
500/tcp    closed      isakmp


# Nmap run co mpleted at Tue May 21 21:22:04 2002  -- 1 IP ad-
dress (1 host up) scanned in 195 seconds

# nmap (V. 2.54BETA22) scan initiated Tue May 21 21:22:52
2002 as: nmap  -sU -P0
-p1-1024 -n -r -vv -oN hsu.txt 808.50.18.252
All 1024 scanned ports on  (808.50.18.252 ) are: filtered

# Nmap run completed at Tue May 21 21:43:41 2002   -- 1 IP ad-
dress (1 host up) scanned
```

in 1249 seconds

Internal interface:

nmap -sT -p1-65535 172.18.1.8 > scan2.txt

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on  (172.18.1.8):
(The 65517 ports scanned but not shown below are in state:
closed)
Port       State       Service
22/tcp     open        ssh
256/tcp    open        rap
259/tcp    open        esro -gen
262/tcp    open        arcisdms
264/tcp    open        bgmp
265/tcp    open        unknown
443/tcp    open        https
900/tcp    open        unknown
1056/tcp    open        unknown
```

Pass or Fail	Pass*, please review the comments section for detail.

Comments	External interface: Port 264:use d for secure client (Secure Remote) build 4100 later to fetch network topology and encryption keys from a Firewall-1 Management console. Firewall -1 will only listen to this port on a ma n-agement console. Port 265: used by firewall -1 to exchange public keys with other hosts. Internal interface: Port 22/tcp: SSH for remote management Port 256/tcp: used for three important things: exchange of CA and DH keys in FWZ and SKIP encryption between two Firewall -1 management consoles. Secure remote build 4005 and ear lier uses this port to fetch the network topology and encryption keys from a fireall -1 management console. When installing a po l-icy, the management console uses this port to push the policy to the firewall. Port 259/tcp: for client authentication, should d isable. Modify fwauthd.conf file. Port 259/udp: for FWZ encryption to manage the encrypted session (Secure R e-mote and Firewall-1 to Firewall -1 VPNs), should disable. FWZ is no longer used as the encryption protocol by Check Point firewal -1 after v4.1. Port 262/tcp: used by netsod, which is the single sign -on daemon. Modify the fwauthd.conf to disable it. Port 264/tcp: used for secure client (Secure Remote) build 4100 later to fetch network topology and encryption keys from a Firewall -1 Management console. Firewall-1 will only listen to this port on a management console. Port 265/tcp: used by firewall -1 to exchange public keys with other hosts. Port 443/tcp: SSL for remote management Port 514/udp: syslog, actually no use here per firewall administrator, sho uld dis-able it. Port 900/tcp: used by Firewall -1's HTTP client authentication mechanism. Modify fwauthd.conf file to disable. Port 1056/tcp: firewall -1 security servers, not used here per firewall administrator, modify fwauthd.conf to disable. Port 1057/tc p: firewall-1 security servers, not used here per firewall administrator, modify fwauthd.conf to disable. Port 1058/tcp: firewall -1 security servers, not used here per firewall administrator, modify fwauthd.conf to disable. Port 1059/tcp: firewall -1 security servers, not used here per firewall administrator, modify fwauthd.conf to disable. Port 1060/tcp: firewall -1 security servers, not used here per firewall administrator, modify fwauthd.conf to disable. Port 1061/tcp: firewall -1 security servers, not used here per firewall administrator, modify fwauthd.conf to disable. Port 18183/tcp: used for SAM (Suspicious Activity Monitoring, for intrusion dete c-tion), should be disabled by modifying fwopsec.conf. Port 18184/tcp: used for log export API (lea), should be disabled by modifying fwopsec.conf. Port 19190/tcp: user authority simple protocol. Port 19191/tcp: used for user authentication API. Various parts of firewall -1 bind to various ports on this system. Typically, they i n-tercept connections traversing thro ugh the firewall, but in order for this to work correctly, they must bind to their own port and listen. In general, the services bound to these ports do not pose any sort of security risk. If no policy is in place or the policy permits access to these port s, inadvertently, the processes the m-selves are smart enough to reject direct requests to these ports. In the case of the SAM and LEA ports, these ports require authentication in much the same way that remote management does, so it is not believed to be a s ecu-rity risk.

List number	Nokia Appliance Audit 8
Control objective	Verify VRRP high availability function of the Nokia pair.
Audit commands/actions	SSH to the primary Nokia box, run iclid, sh vrrp, verify the master status, SSH to the backup Nokia box, run iclid, sh vrrp, verify the backup status. Unplug the external interface cable to the primary Nokia, repeat the abov e ssh procedures, to verity the new vrrp status on both the primary and backup.
Expected results	Firewall still pass traffic as normal, run show vrrp command, the backup Nokia will become the primary.

Actual results	Here is the normal vrrp status: From the primary Nokia go2pass -fw1: Last login: Thu Jun 6 21:50:32 2002 from 172.18.106.11 IPSO 3.4.1 -FCS10 #910: 12.12.2001 210900 Warning: imported path contains relative components Terminal type? [vt100] go2pas-fw1[admin]# iclid go2pas-fw1> sh vrrp VRRP State Flags: On,LocalReceive 15s coldstart delay (completed) 5 interface enabled 5 virtual routers configured 0 in Init state 0 in Backup state 5 in Master state go2pas-fw1> from the backup Nokia go2pass -fw2: Last login: Thu Jun 6 21:52:32 2002 from 172.18.106.11 IPSO 3.4.1 -FCS10 #910: 12.12.2001 210900 Warning: imported path contains relative components Terminal type? [vt100] go2pas-fw2[admin]# iclid go2pas-fw2> sh vrrp VRRP State Flags: On,LocalReceive 15s coldstart delay (completed) 5 interface enabled 5 virtual routers configured 0 in Init state 5 in Backup state 0 in Master state go2pas-fw2> After unplug and power down go2pass -fw1, verified the firewall still passes traffic as normal, ssh to go2pass -fw2 again Last login: Thu Jun 6 21 :54:16 2002 from 172.18.106.11 IPSO 3.4.1 -FCS10 #910: 12.12.2001 210900 Warning: imported path contains relative components Terminal type? [vt100] go2pas-fw2[admin]# iclid go2pas-fw2> sh vrrp VRRP State Flags: On,LocalReceive 15s coldst art delay (completed) 5 interface enabled 5 virtual routers configured 0 in Init state 0 in Backup state 5 in Master state go2pas-fw2>

Pass or Fail	Pass

3.2 Firewall Rule Base Audit

List number	Firewall Rulebase Audit 1
Control objective	Only authorized applications and protocols are allowed to pass the firewall.
Audit commands/actions	Nmap scan from the outside. nmap -sS -vv -n -r -oN hnss.txt 808.50.18.0/24
	nmap -sT -vv -n -r -oN hnst.txt 808.50.18.0/24
Expected results	Only authorized applications and protocols are allowed to pass the firewall. Refer to the application survey form.

Actual results

Nmap scan from the outside.

nmap -sS -vv -n -r -oN hnss.txt 808.50.18.0/24

```
# nmap (V. 2.54BETA22) scan initiated Tue May 21 22:05:24
2002 as:
nmap -sS -vv -n -r -oN hnss.txt 808.50.18.0/24
Interesting ports on  (808.50.18.0):
(The 1541 ports scanned but  not shown below are in state:
filtered)
Port       State       Service
80/tcp     closed      http
Interesting ports on  (808.50.18.1):
(The 1540 ports scanned but not shown below are in state:
closed)
Port       State       Service
23/tcp     open        telnet
79/tcp     open        finger

Interesting ports on  (808.50.18.5):
(The 1540 ports scanned but not shown below are in state:
filtered)
Port       State       Service
53/tcp     closed      doma in
256/tcp    open        rap

Interesting ports on  (808.50.18.7):
(The 1541 ports scanned but not shown below are in state:
filtered)
Port       State       Service
53/tcp     closed      domain

Interesting ports on  (808.50.18.8):
(The 1538 ports scanned but not shown below are in state:
closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
25/tcp     open        sm tp
111/tcp    open        sunrpc

Interesting ports on  (808.50.18.9):
(The 1541 ports scanned but not shown below are in state:
filtered)
Port       State       Service
22/tcp     open        ssh

Interesting ports on  (808.50.18.10):
(The 1540 ports scanned but not shown below are in state:
filtered)
Port       State       Service
25/tcp     open        smtp
53/tcp     closed      domain

Interesting ports  on  (808.50.18.11):
(The 1539 ports scanned but not shown below are in state:
filtered)
Port       State       Service
53/tcp     closed      domain
110/tcp    open        pop -3
143/tcp    open        imap2

Interesting ports on  (808.50.18.34):
(The 1540 ports scanned but not shown below are in state:
filtered)
Port       State       Service
23/tcp     open        telnet
53/tcp     closed      domain

Interesting ports on  (808.50.18.50):
```

Pass or Fail	Fail
Comments	Discovered a new host 808.50.18.8, outside the firewall, installed by Networ k-ing group Internal router 172.18.1.1 is exposed to the outside (808.50.18.34) with telnet open. No one call recalls this. PPTP server 808.50.18 .50 does not need tcp port 53 open.

List number	**Firewall Rulebase Audit 2**
Control objective	Only authorized hosts can access the firewall and management host, drop other access
Audit commands/actions	Run ssh to Nokia 172.18.1.8 from host 172.18.106 .11 Review the firewall rule on GUI policy editor, see if we can find the rules
Expected results	Per firewall administrator, only users from Scanner (172.18.1.116) can access the Nokia to run ssh and ssl.
Actual results	Manual rule review: rule 8: scanner to FW -Cluster any accept gateway any comment: firewall GUI rule 13: any Fw -Cluster any drop log gateway any it looks OK, but there is an any rule in rule 6: rule 6: Internal -LAN any any accept gateway any So, anyone can access th e firewall, rule 8 and rule 13 are bypassed by rule 6 SSH login from host 172.18.106.11, not scanner host, worked. Last login: Thu May 23 21:51:14 2002 from 172.18.106.11 IPSO 3.4.1 -FCS10 #910: 12.12.2001 210900 Warning: imported path contains relative c omponents Terminal type? [vt100]
Pass or Fail	Fail

List number	**Firewall Rulebase Audit 3**
Control objective	There should be a general drop rule at last, and log the drop actions
Audit commands/actions	Review the GUI, make sure the last firewall rule is the drop all rule and it is logged. Review the firewall log; see it has logged all the previous nmap scan results.
Expected results	The drop rule: any any any drop short gateways any last drop rule and drop log will reveal the nmap scan.
Actual results	GUI policy review: Rule 52: any any any drop long Gateways any last rule Log report: Please review the log report follows the Firewall rulebase audit 4.
Pass & Fail	Pass

List number	**Firewall Rulebase Audit 4**
Control objecti ve	Log should be enabled on all the rules; unauthorized actions should be logged. Logs are backed up and reviewed regularly.
Audit commands/actions	Use GUI policy editor, make sure log in enabled on each rule Run GUI log viewer; find any activities rela ted to the May 21 outside nmap scan activities.
Expected results	Logs are enabled on the entire rule, and log viewer should show the drop a c-tions on the nmap scan conducted on May 21.

Actual results	Yes, logs are enabled for each firewa ll rule per GUI policy editor Per firewall administrator, logs are not backed up at all. Each day, the management station run log switch, all the logs are stored on the firewall management station Per log report on May 21, 2002, firewall did log all the dr op actions from the outside nmap scan as expected. Here is the part of the log report: The nmap source host is 66.74.253.36, the nmap command used is: nmap -sS -vv -n -r -oN hnss.txt 808.50.18.0/24, the report only shows one of the hosts, ip address: 808.5 0.18.9, only ssh is allowed, other should be dropped. Log report follows this table
Pass or Fail	Fail, no regular log backup

Partial firewall drop log report to reflect the May 21 nmap scan:

Record No	Date	Time	Action	Service	Source	Destination	Rule	Source Port
2377640	21-May-02	22:10:02	drop	281	66.74.253.36	808.50.18.9	52	43315
2377641	21-May-02	22:10:02	drop	280	66.74.253.36	808.50.18.9	52	43315
2377642	21-May-02	22:10:02	drop	282	66.74.253.36	808.50.18.9	52	43315
2377643	21-May-02	22:10:02	drop	283	66.74.253.36	808.50.18.9	52	43315
2377644	21-May-02	22:10:02	drop	284	66.74.253.36	808.50.18.9	52	43315
2377645	21-May-02	22:10:02	drop	285	66.74.253.36	808.50.18.9	52	43315
2377646	21-May-02	22:10:02	drop	286	66.74.253.36	808.50.18.9	52	43315
2377647	21-May-02	22:10:02	drop	287	66.74.253.36	808.50.18.9	52	43315
2377648	21-May-02	22:10:02	drop	288	66.74.253.36	808.50.18.9	52	43314
2377649	21-May-02	22:10:02	drop	289	66.74.253.36	808.50.18.9	52	43314
2377650	21-May-02	22:10:02	drop	290	66.74.253 .36	808.50.18.9	52	43314
2377668	21-May-02	22:10:03	drop	288	66.74.253.36	808.50.18.9	52	43315
2377669	21-May-02	22:10:03	drop	289	66.74.253.36	808.50.18.9	52	43315
2377670	21-May-02	22:10:03	drop	290	66.74.253.36	808.50.18.9	52	43315
2377671	21-May-02	22:10:03	drop	291	66.74.253.36	808.50.18.9	52	43314
2377672	21-May-02	22:10:03	drop	292	66.74.253.36	808.50.18.9	52	43314
2377673	21-May-02	22:10:03	drop	293	66.74.253.36	808.50.18.9	52	43314
2377674	21-May-02	22:10:03	drop	294	66.74.253.36	808.50.18.9	52	43314
2377675	21-May-02	22:10:03	drop	295	66.74.253.36	808.50.18.9	52	43314
2377676	21-May-02	22:10:03	drop	296	66.74.253.36	808.50.18.9	52	43314
2377677	21-May-02	22:10:03	drop	297	66.74.253.36	808.50.18.9	52	43314
2377678	21-May-02	22:10:03	drop	298	66.74.253.36	808.50.18.9	52	43314
2377682	21-May-02	22:10:03	drop	291	66.74.253.36	808.50.18.9	52	43315

List number	**Firewall Rulebase Audit 5**
Control objective	Change control should be in place on any rule change.
Audit commands/actions	Ask the firewall administration on docs to review, review the GUI policy editor to see the comments field.
Expected results	Written doc on firewall change control, and use comment filed on GUI policy editor to specify who, when.
Actual results	No change control po licy in place.
Pass or Fail	Fail

List number	Firewall Rulebase Audit 6
Control objective	SYNDefender should be used.
Why to audit, risks involved	Against Deny of Service Attack.
Audit commands/actions	Firewall GUI, Policy Properties setup, under SY NDefender, verify the SYN gateway or Passive SYN Gateway is selected.
Expected results	Enabled on the firewall properties setup.
Actual results	Under GUI prosperities setup, and SYNDdfender, under Method, None is selected.
Pass or Fail	Fail

List numbe r	Firewall Rulebase Audit 7
Control objective	Anti-spoofing should be enforced on the gateway interface
Audit commands/actions	GUI policy editor, manage, network objects, gateway object, inte r-faces, check settings.
Expected results	Under Valid Addresses : This net.
Actual results	Under valid addresses, Any is selected. No spoof tracking on the interface.
Pass or Fail	Fail

3.3 Is the system securable?

Apparently the Nokia Check Point firewall -1 based the security system is securable; there are not major configuration issues with the Nokia firewall itself. Some default services should be disabled, because they are not used, please review Nokia appliance audit list 7 for detail, but they do not pose any security issues. Nokia VRRP High availability is implemented correctly.

On the firewall rule sets, obviously more work needed to be done, basis control settings like SYNDefender, anti spoofing should be enabled, change control should be in place, so only authorized services and hosts can be accessed from the outside. The key to mitigation is to have written procedures on change control, firewall backup and log review analysis policy, those are the root cause of the issues. The company should purchase some log reporting/analysis tools such as NetIQ firewall suite software, and utilize the feature like scheduled reporting to study and analysis the log, pay special attention to the drop log.

Again, most of the control objectives are easily to be achieved, if proper firewall administration and configuration training are conducted and proper modifications are done.

The total cost to mitigate all the risks discovered will include the purchase of log review/reporting tools ($3,000) and maybe 30 man-hours to write procedures, and some configuration modifications.

3.4 Is the system auditable?

The overall audit process is a success; the checklist is effective and is sufficient to evaluate the firewall system. The efforts are on the Nokia appliance itself and the firewall rule base. The areas that are overlooked are t he security of the upstream router, the firewall management station security. All together, make up the complete defense in depth security systems. Also due to the fact that we are doing an audit on a production systems, deny of service type of testing ar e not conducted, so the fir e-wall's SYNDefender feature is not tested.

More testing may be conducted to do a penetrate testing to the hosts exposed to the Internet; provide those info to the sys admin, to make those hosts as secure as po s-sible. Because they have open ports, firewall cannot block them, so effective patch level should be applied and tracked.

The company is moving to upgrade the Internet access to 100MBps, and the plan is to establish VPN to access the company's front and back net, which are co -hosted at other sites. It will be nice to verify the firewall performance is up to par, under those high bandwidth and heavy load situation.

The management does not limit any outbound Internet access, so nothing can be audited in terms of firewall's out bound enforcement. Which should be addressed. Also even though the default firewall has 5 interface enabled, all the hosts are l o-cated inside the private network, no audit could be done between DMZ and private network, in normal firewall configuration, sta tic NATed hosts should only be located in DMZ (a separate interface of the Nokia firewall). This is a violation of the "idea" firewall standard per interviewing with the firewall administrators.

No formal approved written firewall security policy and manag ement procedures made it very difficult to clearly define the audit control objectives; supposedly the a u-dit is to audit against the compliance of the firewall policy.

Overall the audit is a success, the findings and recommendations followed will help the company to further enhance the security.

4. Assignment 4 – Follow Up Report

4.1 Executive summary

There is no published firewall security policy, logs are not reviewed and backed up. If the company systems were penetrated (whether from within or from th e outside), these would make it more difficult to discipline or prosecute the offender. The co m-pany should develop and adopt a simple, clear and well -communicated corporate firewall security policy, along with detail implementation, change control and conf igu-ration procedures, which can then be implemented by appropriate technical staff and (equally important) audited against. We recommend the company to establish and publish to all staff its corporate firewall security policy.

Check Point Software's Firewa ll-1(FW-1) was effectively configured to meet the business functions of email and VPN connectivity, and was configured to block/filter most of the unauthorized external access from the Internet while allowing unr e-stricted internal access to any Internet re sources. Nokia's VRRP high availability i m-plementation is a big plus, and is working and configured properly.

Most of the findings/recommendations can be addressed without incurring much of the cost. Again, proper security policy/procedures here will fix most of the problems.

It is strongly recommended to use some type of firewall log analysis tools to suppl e-ment the existing Check Point Firewall -1 default logging/reporting features, which are weak and difficult to use. NetIQ's Webtrend firewall suite is one of the leading firewall log parsing/reporting product, which costs less than $3,000.

No hosts should be allowed to locate outside the firewall, and internal router should not be accessible form Internet via FTP, those two issues should be addressed i m-mediately. Based on the implied firewall security policy, all static NATed hosts should be placed in a separated firewall DMZ zone, in reality, none of those hosts are l o-cated in the DMZ, it may take some careful planning to migrate to the DMZ zone without disrupting the normal services.

4.2 Audit findings/Risk/Recommendations/Costs/Compensating controls

Here is a summary of failed audit list, along with detail risk involved, recommend a-tions, cost and compensation controls:

List number	Nokia Appliance Aud it 5
Control objectives	The Nokia appliance's log is reviewed regularly and backed up.
References	Common experiences, Lowder, Spitzner
Risk	Logs are used to monitor any security intrusion, and system errors. Should be backed up and stored at a secure location for future invest i-gation and troubleshooting purpose. Due to the fact that the firewall rule allows anyone to access the Nokia, the risk is high and the compromise of the Nokia appliance will totally disable the company security.
Recommendations	The root cause is the lack of written firewall security policy and related configuration and management procedures. Proper firewall administration training is another good way to make sure the firewall administrator understand that timely log revi ew is able to d e-tect any intrusion attempts, then prevent real security breach. Configure the SNMP or a SYSLOG server to retrieve Nokia log inform a-tion.
Costs	5 hours to enable the SNMP or SYSLOG configuration.
Compensation controls	Just use voyage or SSH to review the log manually each day.

List number	Nokia Appliance Audit 6
Control objectives	The Nokia's configuration should be backed up securely, and after each configuration change.
References	Nokia manual, own experiences, Lowder
Risk	In the event of hardware failure, the fastest way to install a new r e-placement Nokia is to use the saved configuration backup files. It should be backed up after each configuration change. Then the backup files must be transfer out of the Nokia box to a safe location.
Recommendations	The root cause is still the lack of policy, procedures and proper training. Make a simple shell script to perform regular backup, also ftp out to a secure location. Share with administrator the importance of timely restore from a disa s-ter situation like total hardware failure, yes, Nokia uses a regular hard drive, it will fail eventually. Make sure run the backup after need configuration change.
Costs	Minimum, 2 hours to write a backup and image transfer procedures, and another 5 hours to write a simple shell script.
Compensation controls	Just do it right now.

List number	Firewall Rulebase Audit 1
Control objectives	Only authorized applications and protocols are allowed to pass the fir e-wall.
References	Rothke, own e xperiences, nmap web site, Spitzner
Risk	The security policy is to deny everything by default, and only allow a u-thorized applications and protocols to pass the firewall. Undocumented applications, protocols and open service ports are grounds to suspec t compromised hosts, back doors. Close unnecessary server ports to limit the vulnerabilities without affec t-ing the normal applications.
Recommendations	The root cause is the lack of security policy and the change control. Proper firewall training is a nother way to prevent this happen again. Document and justify each rule change, modification, use the GUI comments column to write down the rule description, who enables the rule, till when, for what purpose. Take out those unauthorized hosts i m-mediately!
Costs	5 hours to develop the change control policy/procedures, and disable the offending rules immediately. Work with network engineering to move the host into the firewall DMZ zone, with proper NATing and protocol enabled.
Compensation controls	Just do it now.

List number	Firewall Rulebase Audit 2
Control objectives	Only authorized hosts can access the firewall and management host, drop other access
References	Ben Rothke on stealth rule, own experiences
Risk	Nokia appliance is THE device to enfo rce the security policy, and ma n-agement station is THE place to modify the rule sets, If those are co m-promised, then the company becomes unprotected.
Recommendations	The root cause is the lack of firewall administration training. Regular firewall auditi ng will help to discover the issue. Always put the firewall access and management rule on top, then follow with a drop rule.
Costs	1 hour time to move the rule to the top, and verify.
Compensation controls	Implementing immediately.

List number	Firewall Rulebase Audit 4
Control objectives	Log should be enabled on all the rules; unauthorized actions should be logged. Logs are backed up and reviewed regularly.
References	Lowder
Risk	Log is the major mean to track down any past intrusion activities. R e-view the drop log, will reveal any past intrusion attempt and for troubl e-shooting purpose.
Recommendations	The root cause is the lack of written firewall security policy and related configuration and management procedures. Proper firewall admini stration training is another good way to make sure the firewall administrator understand that timely log review is able to d e-tect any intrusion attempts, then prevent real security breach. NetIQ's Webtrend firewall suite is a good product to do log review, alert and baseline reporting. Drop rules should be reviewed and followed up daily.
Costs	$3,000 plus 10 hours of installation and configuration, initial report te m-

	plates creation.
Compensation controls	For the time being, just enable logs on all the firewall rules, run log switch each night, review each day using the firewall GUI log viewer, pay attention to action DROP.

List number	**Firewall Rulebase Audit 5**
Control objectives	Change control should be in place on any rule change.
References	Own experiences, Lowder
Risk	Any rule change should be reviewed again firewall security policy, document why, who requested, who made the change Due to the fact that the firewall is the major defense layer between un - trusted network and internal trusted net work, any rule change demands careful evaluation and documentation, with justification.
Recommendations	The root cause if the lack of firewall security policy and change control policy. A proper audit of paper or email info, justification will help, als o document on the firewall GUI's comments column.
Costs	5 hours to develop the change control process.
Compensation controls	Review the rules, document as much as possible now, and find out the rest.

List number	**Firewall Rulebase Audit 6**
Control objec tives	SYNDefender should be used.
References	Lowder, Goncalves & Brown
Risk	Again Deny of Service Attack.
Recommendations	There are many kind of deny of services attack, Sync attack is one of the most common cyber DOS attack now. Firewall SYNDefe nder should be enabled, along with proper upstream router configuration, to work together to deal with the deny of services attack. Lack of proper firewall administration training is the root cause.
Costs	1 hour to enable the Check Point Fiewall -1's SYNDe fender feature u n- der policy property, SYNDefender.
Compensation controls	Do it immediately

List number	**Firewall Rulebase Audit 7**
Control objectives	Anti spoofing should be enforced on the gateway interface.
References	Lowder
Risk	Spoofing is a te chnique by which an intruder attempts to gain unautho r- ized access by altering a packet's IP address to make it appear as though the packet originated in a part of the network with higher access privileges. For example, a packet originating on the Internet may be dis- guised as a local network packet.
Recommendations	Anti spoofing should be done on both the upstream router and the fir e- wall interface, the root cause of this problem is lack of proper firewall administration training.
Costs	1 hour to enable t he firewall interface anti -spoofing feature. Should s e- lect this NET.
Compensation controls	Do it immediately!

5 References

1. Lowder, Jeffery. Firewall Management and Internet Attacks, Inform a-tion Security Management Handbook 4th Edition, Harold Tipton.
2. Rothke, Ben, Testing Checkpoint Firewalls, WebSec 2000 -San Francisco, CA, Session 16.
3. Fieldman, Jeffrey, Securing/Configuring Windows NT Server, Chec k-point web site, May 27, 1999
4. Spitzner, Lance. "Auditing your Firewall Set -up". URL: http://www.enteract.com/~lspitz/audit.html (13 Aug. 2001)
5. Cheswick, William. Firewall and Internet Security.
6. Tipton Harold, Information Security Management Handbook, 4 th edition.
7. Spitzner, Lance,"Building your firewall R ule Base" URL:http://www.enteract.com/~lspitz , January 26, 2000
8. Northcutt, Stephen. Track 7 – Auditing Information Systems, Volume 7.3 Auditing Routers and Firewall . SANS Institute, 2002
9. http://phoneboy.com
10. Check Point Firewall-1 Technical Manuals
11. http://www.nmap.org
12. Goncalves, Marcus, Check Point Firewall -1 Administration Guide.
13. Cheswick, William. Firewall and Internet Security.