Global Information Assurance Certification Paper

SANS GSNA Certification
GSNA. Auditing Networks, Perimeters and Systems (version 2.1)

Auditing the S-Box Safe@ SOHO VPN/Firewall
An Auditors Perspective

Practical assignment
January 2003

Submitted by: Erik Skovfoged
User: ems001
23-Mar-2003

Assignment 1 – Research in Audit, Measurement Practice and Control

1.1 Abstract

Purpose and Audience

This document contains the practical components of the Certified Audit GSNA assessment.

The subject of this paper is the S-Box, a stateful packet inspection SOHO firewall from CheckPoint. It runs on small propriety Linux box as an appliance called S-Box.
Unlike other cable or DSL routers, S-Box appliances support remote management by ISP, allowing transfer of security management responsibility to a managed security service. This facilitates remote management, firewall security and optional parental control/content filtering and email anti-virus capabilities.

The product is available in Safe@home (firewall with/without VPN) and Safe@office (VPN gateway-to-gateway) editions and is available in an enterprise VPN and "home" version. The VPN version facilitates the creation of an enterprise rulebase that can be deployed throughout an organization. The rulebase of each individual S-Box can be restricted depending on the organization's local requirements.

An audit needs to have a definable scope. Because the VPN S-Box@ office can be integrated into the CheckPoint management station, an auditor has the additional responsibility to verify at least part of the CheckPoint management station. Although this is certainly feasible, such a discussion would limit the value of this paper. It is more important to examine an S-Box in its role as a perimeter security device than as a security aspect of CheckPoint management station. Secondly, a stable management solution will only been available in a few months time, and requires CheckPoint Provider-1 NG FP3, which is a complicated and expensive installation.

Device Name:	**S-Box@home, S-Box@office**
Version:	@home, @office
Version Number:	3.0.30
Role:	SOHO Firewall Proxy
Description:	A perimeter security SOHO device that controls access to and from the internet via a Stateful Packet Inspection firewall. The device operates in 2 modes: 1) Firewall and 2) VPN.

Table 1. Description of the S-Box SOHO firewall

1.2 Introduction

The purpose of an *Information Security Policy* is to provide a concise and realistic guidance for the company staff, suppliers and vendors to follow. In practice, the policies will clearly explain what should or should not be

allowed along with the exception procedures. The policies may be classified as high-level corporation policy, issue-specific, system-specific and procedural-specific policy.

Audit Policy defines the standards for conducting the system and networks auditing and risks assessments. This is a critical feedback process to ensure that the securities policies are followed.

We know that complexity and weak links are a basis for attack. The security of each user depends on the security of all users; and a system is only as secure as the weakest link (Bruce Schneier [6]).
"Always-on" broadband connectivity makes Internet access cheap, fast and easy. Unfortunately, it also leaves the home office or small business wide open to Internet threats, such as hackers and viruses. Even worse, if one is working from home or from a remote site, there is the danger that a PC could be used as a zombie to attack the corporate network.
Like other broadband firewall/routers, the S-Box[1] enables small remote offices to share a single DSL or cable modem connection with all the PCs on a small local LAN with 1 to 25 users. But the S-Box claims to differ from most other small-office routers. In addition to Network Address Translation (NAT) and DPHCP like other SOHO firewalls, the S-Box runs a downsized version of CheckPoint's stateful packet inspection firewall FW-1/VPN-1 on top of a hardened Linux kernel. Stateful inspection firewalls are a hybrid firewall, hopefully mixing the speed of static packet filters (e.g. routers, Microsoft IIS) with the ability of application-layer/proxy firewalls. Besides simply filter packets, they can also track the state of all active sessions. Ports remain closed, when they are not in use, but are opened when requested (if security policy permits) or a response is being sent.
ISPs can manage the S-Box remotely. They can limit the number of PCs that can access the Internet at one time, and they can also create packages of services for the customers. The S-Box, in combination with a management station, also offers antivirus, content filtering and VPN features.

1.3 Evaluate the risk to the system

All systems are at risk. A survey performed by Computer Security Institute [14] showed, that the greatest possibility for an attack on a network comes from inside or as a virus infection usually, through an e-mail. The risk of internal employees is high because they are inside the perimeter defense. (See table 2 below.)

TYPE of CRIME	% Victimized	Average loss in $
Unauthorized insider access	55%	143,000
Theft of proprietary information	26%	1,848,000
Telecom fraud	17%	27,000
Financial fraud	14%	1,471,000

[1] The S-Box is sold under a variety of different brands as Nokia, Celestix, Intrusion and VPN Dynamics. All are using the lightweight version of CheckPoint's VPN/firewall. These brands are selling the same hardware device called S-Box that is made by CheckPoint subsidiary called SofaWare.

System penetration by an outsider	31%	103,000
Sabotage of data or networks	19%	164,000
Denial of Service (DoS)	32%	116,000
Insider abuse of net access	97%	93,500
Telecom eavesdropping	13%	76,500
Virus infection	90%	45,500
Active wiretapping	2%	20,000
Laptop theft	69%	87,000

Table 2**.** Types of Network Crimes CSI [14].

External threats can range from port scans to system compromise. Internal threats can range from employees introducing malicious code (viruses) to installing software tools, in an attempt to gain unauthorized access to company sensitive information.

The manufacturer's reference material S-Boxes claims it is easy to install, which is true. But the S-Box is a threat for the corporate network, if a "rogue" box is installed. It can easily happen, as they typically will be installed by the local non-IT personnel, and not by a skilled network administrator or security personnel. An organization's entire network can be compromised by a "rogue" S-Box installation, as it could open the whole network for attack.

A risk profile will identify exposure, reaction and vulnerability regarding the IT Security (Northcutt [5]). The risk assessment table below identifies the different types of exposure and the risk involved. The reaction time is expected to be high due to lack of qualified IT-personnel at the remote sites. The table below exhibit the exposure and risk rating at a remote site.

Exposure	**What can go wrong**	**Risk Rating**
Internal exposure	Access to all central computing resources via VPN. Internet Browsing and e-mail spoofed.	Medium
Internet exposure	Attack on the corporate backbone network.	Medium-High
Temptation	Corporate data would be open for competitors.	Medium-High
Hacking for 1) fun 2) competitive advantages	Corporate image affected by public disclosure that a computer system or their security was compromised.	Medium
Disgruntled employee makes change to firewall configuration or rules	Access to all central computing resources via VPN.	Low
Error is made by the firewall administrator in the firewall rules	External and internal attacks. Most attacks are due to firewall misconfigurations.	Medium

Denial of Service Attacks	Loss of business critical services over this communication link.	High
Net Scanning	Perimeter security is compromised allowing theft of confidential business information.	Low
Internal Security Breach	Potential exposure of confidential data.	High
External security Breach	Potential exposure of confidential research activities.	Medium
Vandalism or inappropriate use of the Internet resources	Affects corporate image.	Medium-High

Table 3. Risk Assessment.

1.4 Firewall Auditing Checklists

SOHO firewall auditing is new. There is very little information as about a secure configuration. A "secure" configuration is being defined more in terms of what is an acceptable configuration.
An extended search for audit procedures/checklists for a SOHO firewall was conducted on the Internet, among others on the following URLs:

Auditnet:	www.auditnet.org
CERT:	www.cert.org
CIAC:	www.ciac.org
CIS Security:	www.cisecurity.com
Phone boy:	www.phoneboy.com
SANS:	www.sans.org
Lance Spitzner:	www.enteract.com
Security Focus	online.securityfocus.com,
Search Engine:	www.google.com,

Table 4. URLs searched for Firewall Checklists.

There is a lack of information on SOHO firewalls, and an absence of audit checklists in the literature and on the WEB. There were a few "hits" on checklists for "normal" firewalls, but no definitive guidelines or checklists indicating the parameters to be configured in order to obtain a secure SOHO configuration. A search on the CheckPoint S-Box WEB-site using the keywords *S-box* and *checklist* obtained no answer.

In construction of an S-Box checklist, we will use several sources as indicated below.

Lance Spitzner's paper "Auditing Your Firewall Setup"[2] contains good introduction to firewall auditing and basis for a checklist.

The SANS course "Auditing the Perimeter" by Stephen Northcutt[3] is also a

2 Lance Spitzner, "Auditing Your Firewall Setup", http://the.wiretapped.net

good and comprehensive document about audit methodology, with a lot of practical information.

Krishni Naidu's "Firewall Checklist"[4] on the SANS web is both a detailed and a general checklist. It has a lot of items that can be used as a basis for a checklist for a SOHO firewall.

Stéphane Grundschober[5] has created a well structured checklist, which has been a great help in constructing the checklist in this assignment.

The "Management Analytics Firewall Checklist"[6] by Fred Cohen and Associate is an exhaustive introduction to many aspects of a firewall audit, from management awareness to technical details. Unlike many other checklists, it has the form of a "real" checklist, putting simple questions, which can be answered with a "yes" or a "no".

A firewall is only as effective as the rules and configuration parameters, which have been applied to it. CERT (www.cert.org) claims "the most common cause of firewall security breaches is a misconfiguration of the firewall system". Consequently thorough configuration testing of the firewall system itself and the routing, packet filtering and logging capabilities is a prime objective.

According to a second survey, conducted by the Computer Security Institute in spring 2002 [14], 40% of the persons questioned, reported having a security problems from the outside.

This information from CERT and CSI clearly pinpoints, why a firewall should be reviewed regularly. To create a baseline for the audit, following items should be viewed as the key areas for the audit:

- Conduct tests on the firewall
- Conduct tests to verify the firewall rules in place
- Verify that there are no additional network connections
- Review the Checkpoint/S-Box system configuration
- Review the Linux operating system configuration
- Review and test physical security
- Determine the corporate security policies through reviewing current policy documents and through interviews

The following points summarized the current state of SOHO firewall auditing:

- SOHO firewall auditing is new.
- There is no general SOHO firewall auditing checklists.
- SOHO firewall auditing checklists cannot be applied out of the box.
- Firewall auditing lacks attention to business issues.

---

3 Stephen Northcutt, "Track 7, Auditing Networks, Perimeters and Systems", (http://www.sans.org), Jan. 2002.

4 See Krishni Naidu's "Firewall Checklist", http://www.sans.org/checklist/firewall_check.htm, Jan. 2003.

5 Stéphane Grundschober: "Auditing Firewall in a Small Office /Home Office environment", SANS Practical, Sep 2001

6 Fred Cohen and Associates, http://www.all.net/books/audit/Firewall/manal/index.html Jan. 2003.

2 Assignment 2. Create an Audit Checklist

The following checklists have been developed to measure compliance with the security policy. Each control objectives is designed to be as objective and verifiable as possible.

As mentioned above, there are no authoritative auditing procedures or CIS rules available to audit the S-Box firewall/routers. A variety of methods from different sources and manufacturer documentation are used instead. The manufactures references about the S-Box can be found at the following link: http://www.sofaware.com.

The S-Box can be treated as a DHCP-enabled black-box firewall in front of the remote LAN. There might be hidden services running on the S-Box, available to either the LAN side or the WAN side, but documentation mentions only the web configuration interface. Since Web services are prone to security vulnerabilities, more testing is strongly recommended. However this is outside the scope of this audit.

As of February 2003, there are **no** vulnerabilities reported on the S-Box at BugTraq, "www.securityfocus.com".

The SOHO firewall is intended mainly to
1) Provide NAT for an internal network
2) Filter out most unwanted, un-routable and malformed IP-packets
3) Protection against Denial of Service attacks

2.1 Firewall Checklist

Assessment Process:
The following checklist will be followed, to assess the perimeter security provided by the Checkpoint SOHO firewall.
The checklist is an adaptation to SOHO-boxes of the methodology used in "The Management Analytics Firewall Checklist"[7] by Fred Cohen and Associate [12], as it is exhaustive, relevant and easy to use. Stéphane Grundschober [16] has been an inspiration for the structure of the checklist.

2.1.1 Functional Objectives

Item 1: A firewall controls traffic between the Internet and the local LAN
objective subjective | reference: Northcutt
Risk: A normal hub/switch will not have any basic firewall functionalities
Testing: Inspect that the S-Box have two physical interfaces, controlling the traffic. Generate traffic on both interfaces and inspect the result in the log.
passed failed

Item 2: The S-Box protects inside systems from exploitation by outside threats
objective subjective | reference: Fred Cohen and Associate

7 http://www.all.net/books/audit/Firewall/manal/index.html Jan. 2003

Risk: If untrusted systems can see or access the system, they can mount attacks against it, or gather information about applications that may be in use on that system.
Testing: There must be filtering rules for incoming traffic. (Ingress filters). Port scan with Nmap to see if ports are open, closed or stealth.
passed failed

Item 3: The S-Box protects outside systems from exploitation by inside threats
objective subjective | reference: Fred Cohen and Associate
Risk: Rogue applications on the local net, can use the Internet to avoid local security controls or to attack other systems either independently or as part of a distributed attack (e.g. Distributed Denial of Service).
Testing: The Firewall checks outgoing traffic (egress filter). Port scan with Nmap to look for open ports.
passed failed

Item 4: The is designed to protect itself against being used as a launch point for attacking other systems
objective subjective | reference: Fred Cohen and Associate
Risk: Corporate image can be spoiled. WAN / LAN can be attacked. The firewall should be designed to protect itself against being used by attackers as a zombie for attack on the Internet and the local LAN.
Testing: Generate TCP traffic with NTOMax, Port Scan with Nmap. Check vulnerabilities with Nessus (Hatch, B et. al. [3])
passed failed

Item 5: The S-Box is designed to prevent the leakage of sensitive information.
objective subjective | reference: Stéphane Grundschober
Risk: Rouge clients can access corporate net
Testing: The administrator must know what sensitive information exist within the network.
passed failed

2.1.2 Policy Issues

Item 6: Local management knows about security problems
objective subjective | reference: Fred Cohen and Associate
Risk: Lack of security awareness/education can prevent “due care”
Testing: Interview with local management to prove knowledge of security issues
passed failed

Item 7: Local management is aware that a S-Box is only a part of security defense in depth
objective subjective | reference: Northcutt
Risk: Relying only on the firewall for defense of the system, makes the inside LAN vulnerable to virus, trojans, worms and other attacks.
Testing: Decision makers must have taken additional action for internal security. An interview with the local manager must show these actions.
passed failed

Item 8: The S-Box policy is an official organizational policy and is approved and periodically reviewed by top management.
objective subjective | reference: Fred Cohen and Associate
Risk: Lack of policy or lack of compliance to policy brings the organisation at risk
Testing: Check of traffic flow to/from the remote office.

passed failed

Item 9: The security policy specifies, who are the local responsible individuals with adequate control to carry out the policy
objective subjective | reference: Fred Cohen and Associate, Stéphane Grundschober
Risk: The number and type of personnel with security responsibility must be noted
Testing: Check the policy document. Check the security officer, if he knows how to manage the firewall.
passed failed

2.1.3 Documentation Issues

Item 10: S-Box configuration change control procedures are specified in the security policy
objective subjective | reference: Stéphane Grundschober
Risk: Individual local S-Box firewall rules impede compliance with corporate firewall rules
Testing: Check that the procedures are specified and followed
passed failed

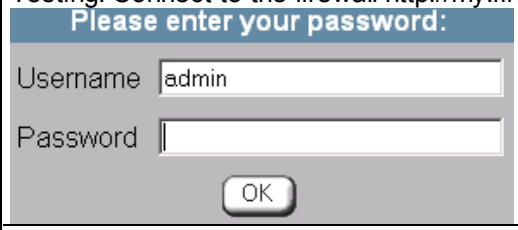
Item 11: The present configuration of the S-Box is documented
objective subjective | reference: Stéphane Grundschober
Risk: Lack of description of the installation can create security concern
Testing: Check if documentation is present and complies with the S-Box configuration.
passed failed

Item 12: Changes to the S-Box configuration are documented in accordance with security policy
objective subjective | reference: Northcutt
Risk: the most common cause of firewall security breaches is a misconfiguration of the firewall system (www.cert.org)
Testing: Changes are checked against the policy; they are documented and written down.
passed failed

Item 13: Sufficient information must be documented with each change in the S-Box rules
objective subjective | reference: Northcutt
Risk: Lack of audit track is the one of the greatest risk to security The most common cause of firewall security breaches is a misconfiguration of the firewall system (CERT)
Testing: Each change documentation must specify: The person who requested the change The reason for the change The person who authorized the change The person who implemented the change The date for the change This is tested by inspecting the written documents and change logs.
passed failed

Item 14: A configuration/rule backup strategy exists.
objective subjective | reference: Stéphane Grundschober
Risk: Lack of backup prevent restoration of firewall rules in case of unintended changes and erasure.
Testing: The strategy is has been tested and works
passed failed

2.1.4 System Administration

Item 15: The S-Box is password protected
objective subjective | reference: Stéphane Grundschober
Risk: Users may disable or change firewall security settings
Testing: Connect to the firewall http://my.firewall and log-in. 
passed failed

Item 16: Account lockout procedure exists
objective subjective | reference: Eric Cole [1, p.298]
Risk: Repetitive login trials should trigger a lock-down of the account for a specified amount of time.
Testing: Use the program Brutus (www.hobbie.net) to make a brute force attack on the login procedure of the S-Box.
passed failed

Item 17: A password construction policy exists
objective subjective | reference: Stéphane Grundschober
Risk: Attempt to log in as default and admin, using same passwords.
Testing: Verify that the admin password complies with the policy. Only one administrator with nontrivial password (See appendix C).
passed failed

Item 18: Access to the S-Box from the outside must be logged on IP and port number
objective subjective | reference: Generally recommended practices
Risk: Rogue access can take control of the S-Box, and must be traced and detected by the logs.
Testing: Verify that access to the S-box from the Internet is logged on IP and Port number.
passed failed

Item 19: Access to the S-Box from inside must be logged on IP and Port number
objective subjective | reference: Generally recommended practices
Risk: “Rogue” access can take control of the S-Box
Testing: Verify that access to the S-box from the inside is logged on IP and Port number.
passed failed

Item 20: The firmware of the S-Box has the latest stable patches
objective subjective | reference: Northcutt
Risk: Unpatched and out-of-date software may be exposed.
Testing: Find the patch level of the S-Box and compare latest stable level from the supplier. 
passed failed

2.1.5 Technical Safeguards

Item 21: There must be no open ports open on the outside of the S-Box
objective subjective | reference: Stéphane Grundschober

Risk: Open ports are the starting point for exploitation
Testing: Use NMAP scan from outside
passed failed

Item 22: There must be no open ports open on the inside of the S-Box
objective subjective | reference: Stéphane Grundschober
Risk: Open port is the starting point for exploitation
Testing: A scan with Nmap must show no open ports (except the management port)
passed failed

Item 23: Open Ports on the S-Box (found by NMAP) must be Vulnerability Scanned
objective subjective | reference: Brian Hatch [3)
Risk: Attack, using the known vulnerabilities on the running services
Testing: Use Nessus to perform vulnerability assessment. The Nessus vulnerability assessment tool must show a negative database match.
passed failed

Item 24. Manual review of the rule base.
objective subjective | reference: Stéphane Grundschober
Risk: The most common cause of firewall security breaches is a misconfiguration of the firewall system (www.cert.org)
Testing: It must comply with the policy and the traffic flow / architecture diagram. Get a dump of the rule base. Check if it complies with the authorized traffic.
passed failed

Item 25: Random, blind, and periodic *outside* testing of the S-Box
objective subjective | reference: Frank Cohen/Stéphane Grundschober
Risk: Errors in the rulebase could leave the net open to attack
Testing: Use NTOMax to generate packets (TCP, UDP and ICMP) from outside of the firewall and TCPDump or another packet capture tool to listen for packets on the other side. Anything, that goes through, must be allowed by the rules and comply with the policy.
passed failed

Item 26: Random, blind, and periodic *inside* testing of the S-Box
objective subjective | reference: Frank Cohen/Stéphane Grundschober
Risk: If untrusted systems can see or access the system, they can mount attacks against it or gather information about applications that may be in use on that system.
Testing: Use NTOMax or ftester generate packets (TCP, UDP and ICMP) from inside of the firewall, and TCPDump or another packet capture tool to listen for packets on the other side. Anything that goes through must be allowed by the rules and comply with the policy.
passed failed

2.1.6 Logging, Detection and Reaction

Item 27: Check of the logs
objective subjective | reference: Stéphane Grundschober
Risk: Access to the firewall and firewall logs may expose confidential information or information useful in developing an attack. Unauthorized “write” access to logs can allow a potential attacker to cover his track.

Testing: Dump of the firewall log, and verify that the previous scans where correctly recorded. It should also include firewall management activities (e.g. bad authentication).
passed failed

Item 28: Log analysis and reaction procedures
objective subjective | reference: Stéphane Grundschober
Risk: Local personnel may not have enough knowledge to recognise unusual situations, and the remote office doesn't have a reaction plan ready.
Testing: The local system administrator must have enough knowledge to recognize unusual patterns in the logs, and have reaction plans to follow.
passed failed

Item 29: The logs must be backed up for an extended period of time
objective subjective | reference: Generally recommended practices
Risk: Without a log trail, attacks can happen without being discovered
Testing: Check the existence of log for an extended period of time, and analyze the log
passed failed

2.1.7 Physical Security

Item 30: The S-Box is secured in a physically secure location
objective subjective | reference: Generally recommended practices
Risk: Unauthorized physical access to firewall and LAN may be used for an attack. Unauthorized access can allow a potential attacker to cover his track. Pressing reset bottom for 5 seconds on the S-Box will enable factory defaults restoration of the S-Box and delete the log.
Testing: Is the S-Box placed in a physically secure location? Physical access is to the S-Box and the local LAN must be limited by locked doors. Only trusted have access into this space.
passed failed

Item 31: The S-Box is not a single point of failure
objective subjective | reference: Generally recommended practices
Risk: Hardware failure, theft.
Testing: presence of a "cold" stand-by proper configured extra S-Box
passed failed

2.1.8 Performance of the S-Box Device

Item 32: The S-Box performs well and don't degrade Internet traffic
objective subjective | reference: Generally recommended practices
Risk: Performance degrading of the S-Box can be a indication of an attack
Testing: We will check the upload and download speed to the ISP, with and without the S-Box
passed failed

3 Assignment 3

Devices as the S-Box SOHO firewall are a small easy-to-use appliance firewall that is relatively inexpensive and fast growing in sales. An audit is performed in order to know the device's security risk in the corporate network
An audit normally contains the following 6 process steps [1]:
1. Audit Planning
2. Entrance Conference
3. Fieldwork
4. Preparing the Report
5. Exit Conference
6. Report to Management

Assignment 3 is dealing with step 3 in the audit process, the *fieldwork*.

Prior to performing the audit, a *written* approval must be obtained from executive management

The results will be communicated to executive management, infrastructure management and system operators.

Planning of the assessment:
The objective of an audit is to determine if there exists compliance with a security policy. When a policy has been adopted, management must have assurance of its compliance.
An assessment is generally an analysis of risk or threat. The assessment will determine if the system is prone to service disruption, subversive attacks or data corruption and will provide information to management in order make judgment, based on facts rather than guesses.

The scope of the assessment will be a stand-alone S-Box firewall. The focus of this audit is, what security risk a SOHO firewall introduces to a local site, and what is the implication for the whole system.

3.1 The Test Conditions and Techniques Used in the Audit

3.1.1 Hardware being tested

SofaWare S-Box Model SBX-133LHE-1
S/N 1234567 MAC 00-xxxxxx-xx-xx-xx

3.1.2 Hardware used for testing

Three PC notebooks were re-configured from scratch with latest patches of Jan. 1. 2003.
- Two Windows 2000 Professional (W2K).
- One Linux 7.3 (Red-Hat.).
- Two small hubs/switches

The first Windows 2000 PC was placed on the local LAN, and configured with the Fyodor's port scanner *Nmap*, the password cracker *Brutus* from

www.hoobie.net and packet capturer program *windump* from windump.polito.it.
The other Windows 2000 notebook was placed on the DMZ between the S-Box and the Internet and configured with *windump*, *Nmap* port scanner and *NTOMax* traffic generator from FoundStone.

The Linux Red Hat notebook was placed on the Internet (WAN), at a remote test site, configured with *Nessus* vulnerability checker (www.nessus.org) and Nmap.

Figure 1 below shows the test setup.

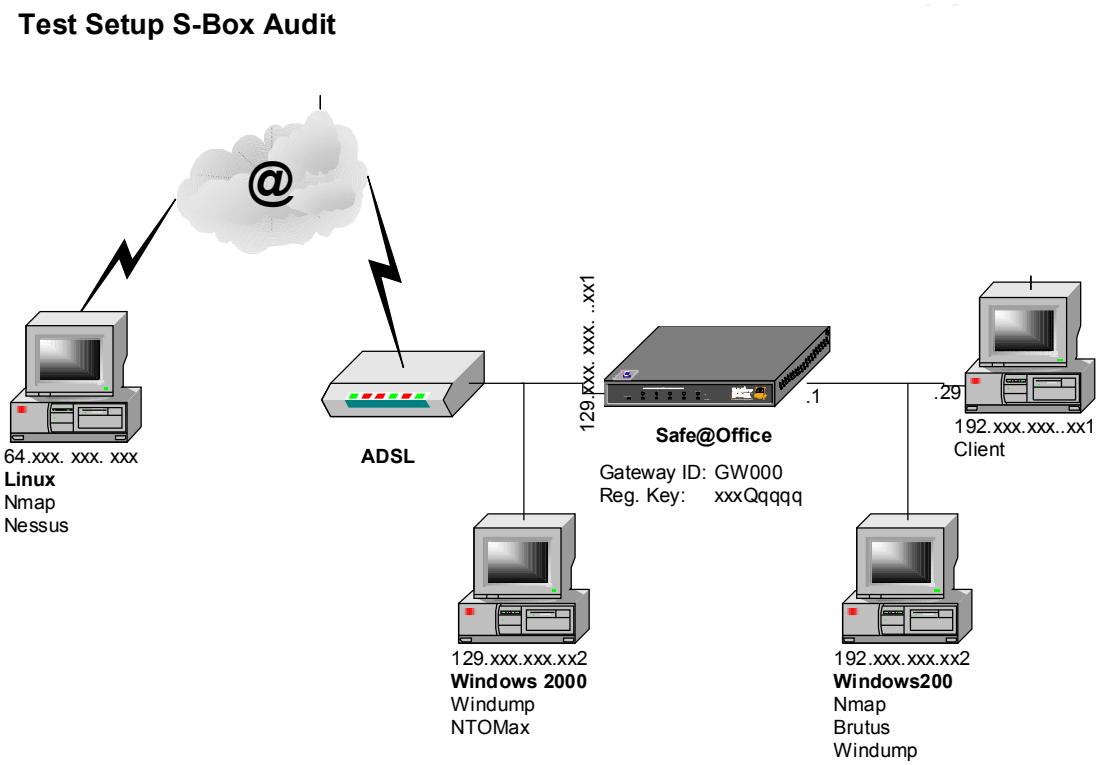


Figure 1 Test Setup for the audit

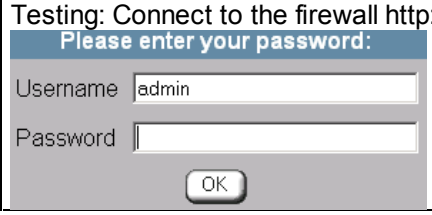
3.2 The 10 Most Important Objectives

Per assignment instructions, 10 items, reflecting the most significant security concerns, were selected from the completed audit checklist for study.
They were:

1) Only authorized users have access to the firewall
2) Firewall software is at the current patch level
3) Firewall logs are secure
4) Only approved applications can access the Internet
5) Access from the Internet is prohibited
6) Access to the Internet from local LAN is restricted
7) Check the firewall rules
8) Logging, detection and reaction
9) Test the physical security.
10) Test for performance degrading using the S-Box

3.3 Conducting the Audit

3.3.1 Objective 1. Only authorized users have access to the S-Box

Item 15: The S-Box is password protected
objective subjective | reference: Stéphane Grundschober
Risk: Users may disable or change firewall security settings
Testing: Connect to the firewall http://my.firewall and log-in 

The user get logged out of the firewall after 1 minute of inactivity

But

1) there is no policy for construction of the password (except it must be at least 5 characters long),

2) there is no lockout procedure

3) the log file doesn't register, which client had logged in to the firewall

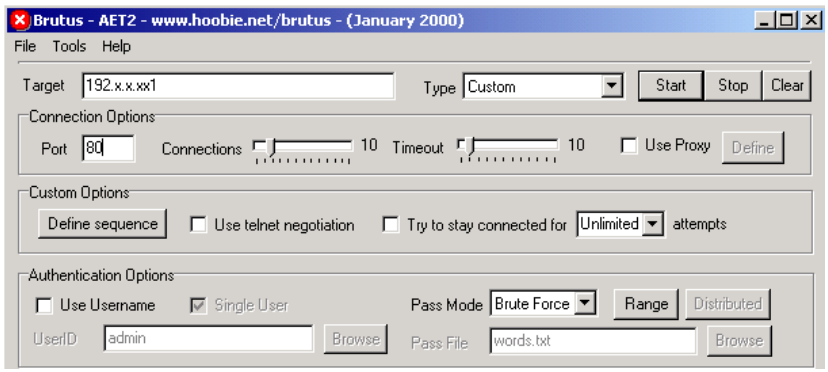
Item 17: A password policy exists

The S-Box only requires password to be 5-25 characters long. Any character can be entered and the password construction does not follow the password rules on the corporate net. Here the password must be a mix of capital and small letters, special characters and numbers (see appendix B), and at least 8 characters long.

Item 16: Account lockout procedure exists.

There exist no account lockout procedures.

It was possible to crack the password, with the password cracker Brutus [www.hobbie.net/brutus] in brute force mode



The log file doesn't register which client had logged in to the firewall

10621

Feb 07

23:12:17

User "admin" logged in ← *No user indication*

10620

Feb 07

23:12:04

User "admin" failed to login ←*incorrect password*

passed failed **Auditor's remark**: The test is passed, as a firewall configuration require authentication, but the password protection is very weak.

3.3.2 **Objective 2.** S-Box software is at the current patch level

Item 20: The firmware of the S-Box has the latest stable patches
objective subjective | reference: Northcutt
Risk: Unpatched and out-of-date software may be exploited.
Testing: Find the patch level of the S-Box delivered, and compare it to the latest stable level patch from the manufacturer. The firmware was 2.0.39. It was not possible to download the latest firmware from the Internet, but the supplier provided us with the latest patch 3.0.30 in 2 days. 
passed failed The test failed. **Auditor's remark.** There are 2 remarks from the auditor, 1) Software is out of date, and 2) No automatic software update procedure can be followed.

3.3.3 **Objective 3. The** S-Box logs are secure

Item 27: Check of the logs
objective subjective | reference: Stéphane Grundschober
Risk: Access to the firewall and firewall logs may expose confidential information or information useful in developing an attack. Unauthorized "write" access to logs can allow a potential attacker to cover his track.
Testing: Dump the firewall log, and verify that the previous scans were correctly recorded. It should also include management activities or bad authentication.
Testing: Place a "sniffer" in front of the firewall and examine, if the S-Box log correspond to the "sniffer" output.

Source
Destination

#
Date
Time
Protocol
IP Address
Port
IP Address
Port

10621
Feb 07
23:12:17
User "admin" logged in ← Client identification missing

10620
Feb 07
23:12:04
User "admin" failed to login (incorrect password)

10619
Feb 07
23:11:52
User "admin" failed to login (incorrect password)

10618
Feb 07
23:11:38
User "admin" failed to login (incorrect password)

10617
Feb 07
22:46:52
UDP
68.17.216.252
50932
129.142.yyy.yyy (S-Box)
137 (NETBIOS)

10616
Feb 07
22:35:52
User "admin" logged in

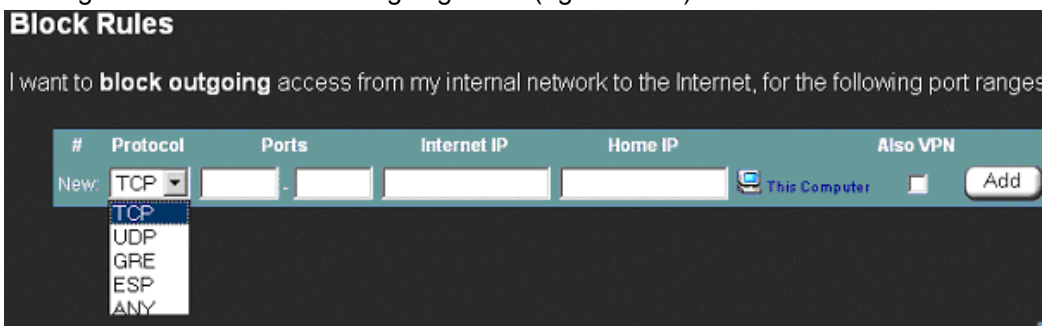
10615
Feb 07
21:55:06
UDP
4.41.57.73
1031
129.142.yyy.yyy (S-Box)
137 (NETBIOS)

10614
Feb 07
21:20:18
TCP
67.40.196.178
3628
129.142.yyy.yyy (S-Box)
21 (FTP)

10613
Feb 07
20:52:40
UDP
212.129.183.10

passed failed The audit test passed, as authorization and rejected traffic is written into the log **Auditor's remark.** But the logging is not very secure. 1) The log is circular and max 100 records long. This means, that tracking can only happen in real time. There is no easy way, to automatically off-load the logs to a log-client. 2) The log doesn't register all traffic. During a **denial of service attack from Nessus, nothing appeared in the log** indicating such an attack, but the packet sniffer registered the attack. **Scanning from Nmap got registered in the log.** 3) The log must work like the "normal" CheckPoint logs, where heavy traffic gets dropped. 4) The log clears if the S-Box is powered off. 5) The log clears if the S-Box is reset (press the reset button for 5 second).

3.3.4 Objective 4. Only approved applications access the Internet

Item 3: The S-Box protects outside systems from exploitation by inside threats
objective subjective | reference: Fred Cohen and Associate
Risk: "Rogue" applications can use the Internet to avoid local security controls or to attack other systems either independently, or as part of a distributed attack (e.g. DDoS).
Testing: The Firewall checks outgoing traffic (egress filter)    The firewall can only check outgoing protocol/port connections, not applications. In this case a software personal firewall as ZoneAlarm, Black Ice etc. is necessary.
passed failed **Auditor's remark.** The test failed as unapproved applications (as RealAudio) are able to access the Internet. Many applications will use port 80 to get to the Internet. The Internet IP in the block rule is not sufficient in the long run, as Internet IP-addresses changes frequently.

3.3.5 Objective 5. Access from the Internet is prohibited

Item 2: The S-Box protects inside systems from exploitation by outside threats
objective subjective | reference: Fred Cohen and Associate
Risk: If untrusted systems can see or access the system, they can mount attacks against it or gather information about applications, which may be in use on and vulnerable on that system.

Testing: An open port is the starting point for exploitation.
The core of the technology in the S-Box is CheckPoint FW-1. Consequently, in order to find a bug in the implementation of the "firewalling feature", one has to break the CheckPoint Firewall, which is outside the scope of this assignment.
The S-Box has 3 levels of security for incoming traffic:
1. Low
External Network can "ping" external interface of the S-Box
2. Medium and 3. High
External Network can't "ping" external interface of the S-Box
Level 3 - High - is chosen.
The test passes, if system being audited does not respond to pings or Nmap scans.

Using NMAP tcp syn scan. From outside → S-Box

Command: Nmap –sS –sP –sU –P0 –O –p 1-65535 129.142.yyy.yyy
(Syn half-open scan, no ping, OS fingerprinting, all ports, not random order xxx.xxx.xxx.xxx is the IP address of the Firewall itself on the public side)
Starting Nmap V. 3.00 (www.insecure.org/nmap/)
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
sendto in send_tcp_raw: sendto(3, packet, 60, 0, 129.142.yyy.yyy, 16) => Operation not permitted
sendto in send_tcp_raw: sendto(3, packet, 60, 0, 129.142.yyy.yyy, 16) => Operation not permitted
Interesting ports on 129.142.yyy.yyy.ip.tele2adsl.dk (129.142.yyy.yyy):
(The 1149 ports scanned but not shown below are in state: filtered)

Port	State	Service
264/tcp	open	bgmp (***CheckPoint Secure Client)***
981/tcp	open	(***Checkpoint SofaWare Management Port***)

Remote operating system guess: Linux 2.1.19 - 2.2.20
Nmap run completed -- 1 IP address (1 host up) scanned in 303 seconds

---

Nessus found the same ports open

timestamps|||scan_start|Tue Feb 4 20:46:40 2003|
timestamps||129.142.yyy.yyy|host_start|Tue Feb 4 20:46:40 2003|
results|129.142.yyy|129.142.yyy.yyy|unknown (264/tcp)
results|129.142.yyy|129.142.yyy.yyy|general/tcp|10336|
Security Note|Nmap found that this host is running Linux 2.1.122 - 2.2.16\n
results|129.142.yyy|129.142.yyy.yyy|unknown (264/tcp)
results|129.142.yyy|129.142.yyy.yyy|unknown (981/tcp)
timestamps|||scan_end|Tue Feb 4 22:17:22 2003|

This 129.142.yyy.yyy address was scanned using Nessus, but Nessus was not able to generate a report at all. It was "hanging" during the vulnerability scan.
However, the "sniffer" log showed several scans from the Nessus server.

We were unable to ping and traceroute to the S-Box address from the external Windows 2000 or a Linux portable. The result was: "Destination Host Unreachable" and "Request Timed out".

The same scanning result was obtained by scanning from the DMZ with FoundStone's SuperScan.

The FoundStone tool NTOMax was used to generate TCP, UDP and ICMP packets from outside side of the S-Box. Windump was used to listen for packets on the inside. Mainly due to Network Address Translation (NAT) and no "allow" rules from the WAN to the LAN, nothing got through the firewall.
If there was a flaw in the NAT implementation or a "man in the middle attack" NAT can fail and the client can be visible (Security Complete [6]), but it wasn't the case

passed failed
Auditor's remark.
The test passes, as no ports, except the management ports, can be seen from the outside
Except every 10 minutes port 500 ISAKMP will open for the VPN tunnels.

Before the S-Box was updated to version 3.0.30, other ports appeared occasionally, such as port 80 (http) and port 443 (https). The same happened occasionally with 161 udp, 256 udp, 520 udp, 514 udp, 520 udp, 31337 udp.

Management of the box is through port 981, which is a web based management interface. It is a relatively new program, and there will probably be many vulnerabilities and misconfigurations, and this port will become a good starting point for attack.
But vulnerability scan with Nessus (with latest patches) on the ports 264 and 981 just got the Nessus program to "hang" and it was necessary to kill the Nessus process to continue. We tried both from a Linux and a Solaris, and obtained the "hang up" result from both of them.

CheckPoint must have done their homework well (and know Nessus)!!

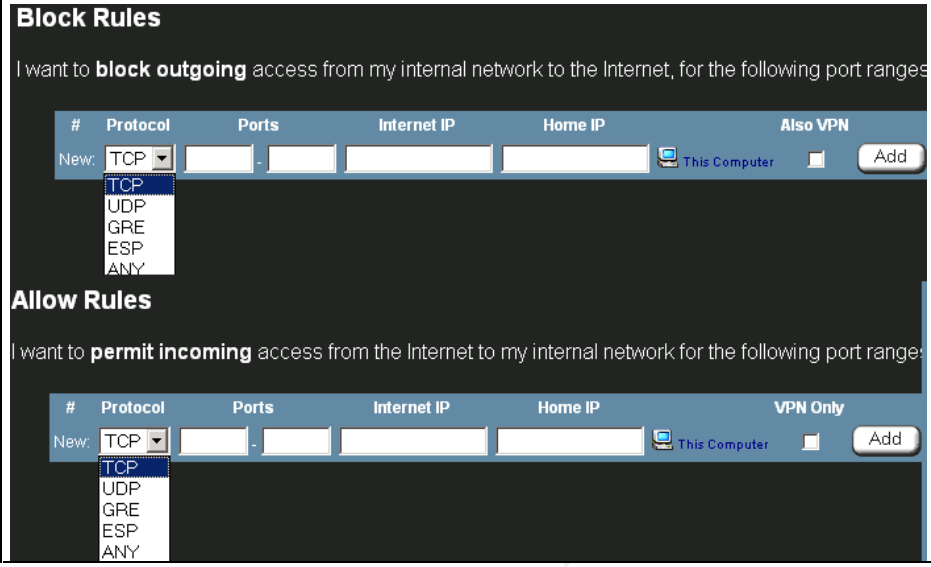
3.3.6 Objective 6. Local LANs access to the Internet is restricted

Item 3: The S-Box protects outside systems from exploitation by inside threats
objective subjective | reference: Fred Cohen and Associate
Risk: Rogue applications can use the Internet to attack other systems either independently or as part of a distributed attack (e.g. Distributed Denial of Service).

Testing: The Firewall checks outgoing traffic (egress filter).
The box has 3 levels of security:
1. Low and 2. Medium
Internal Network can go outside with every protocol
3 High
Internal Network can go outside only for "certain" protocol.
 	
Level 2. Medium (= Low) is chosen.
Nmap Inside→Out scan
Port scan the S-Box with Nmap in order to look for open port
Interesting ports on (yyy.yyy.yyy.yyy):
(The 65531 ports scanned but not shown below are in state: closed)
`Port State Service`
`80/tcp open http`
`264/tcp open CheckPoint Secure Client`
`443/tcp open https`
`981/tcp open SofaWare Administration Port`
`TCP Sequence Prediction: Class=random positive increments`
Difficulty=2752396 (Good luck!)
Sequence numbers: 32E2538A 32639EBB 32C9F833 32E2E6FE 32B38977 329BC562
Remote operating system guess: **Linux 2.1.122 - 2.2.14**
 	
At other times Nmap showed:
53 tcp filtered DNS
67 tcp filtered DHCP
This is traffic necessary for accessing the Internet.

passed fail **Auditor's remark.** The test was passed, because the S-Box protected the Internet from traffic, except from http/https, the management ports and other necessary services.

3.3.7 Objective 7. Verify the S-Box **Rules**

Item 13: Sufficient information must be documented with each change in the S-Box rules
objective subjective | reference: Northcutt
Risk: Lack of audit track is the one of the greatest risk to security The most common cause of firewall security breaches is a misconfiguration of the firewall system (CERT)
Testing: Each documentation of change must specify: The person who requested the change The reason for the change The person who authorized the change The person who implemented the change The date for the change This is confirmed by inspecting the actual written change logs. Dump the rule base. Check if it complies with the authorised traffic. 

passed failed **Auditor's remark.** **The test failed** due to the following. Besides the 3 levels of security 1) Low 2) Medium or 3) High, the S-Box can set up filters, which **allow** incoming traffic and **block** outgoing traffic, specified by protocol and port. But it is not possible to check the exact rule change, except for an entry in the log, indicating that a change has taken place (see log below). 10766 Feb 08 16:45:09 Security level changed: High to Low (requested by user) 10765 Feb 08 16:45:01 Security level changed: Med to High (requested by user) 10764 Feb 08 16:44:54 Security level changed: Low to Med (requested by user) 10763 Feb 08 16:38:49 Security level changed: High to Low (requested by user) ICMP (e.g. ping) get controlled by the general rules (1. Low, 2. Medium, 3. High) It would be desirable, if ICMP could be controlled by the allow/block rules so i.e. only management can use ping. A manual change log book, with all the changes documented, must be kept in a separate safe place. The log book was not found, and its existence was not known by the system administrator.

Item 24. Manual review of the rule base.
objective subjective | reference: Stéphane Grundschober
Risk: The most common cause of firewall security breaches is a misconfiguration of the firewall system (www.cert.org)
Testing: It must comply with the policy and the traffic flow / architecture diagram. Get a copy of the rule base (**security level**, **allow** traffic rules, **block** traffic rules). Check if it complies with the authorised traffic.
passed failed **Auditor's remark.** The test failed, as there was no written documentation of the rules and rule changes. The rules in the S-Box are as default: Open from inside and closed from outside.

3.3.8 Objective 8. Logging, Detection and Reaction

Item 27: Check of the logs.
objective subjective | reference: Stéphane Grundschober
Risk: The log doesn't register all changes, whereby reconstruction of events is impeded
Testing: Get a dump of the firewall log, and verify that the previous scans where correctly recorded. It should also include management activities (e.g. bad authentication).

passed failed

Auditor's remark.

The test failed because the log size was too short, and no reaction plan was defined.
The S-Box recorded events of interest, but a lot of traffic caused problems
Unfortunately, only the latest 100 events are recorded, then they are "pushed" off.
There is no way to automatically off-load the logs to a log-client.

The log doesn't register all traffic.
1) During a denial of service attack from Nessus nothing appeared in the log that indicated such an attack, even though the packet sniffer showed the attack.
2) Scanning from Nmap most entries got registered in the log.
The log must work like the "normal" CheckPoint log where heavy traffic gets dropped.
3) The log clears, if the S-box is powered off/reset
4) Check the existence of a process to analyze the log.
The person responsible must have enough knowledge to recognize unusual situations, and has a reaction plan ready.
Due to the limited functionality of the log system on the S-Box, the administrator is only using the log for debugging purposes. A reaction plan is not defined.

A log example

Source
Destination

#
Date
Time
Protocol
IP Address
Port
IP Address
Port

10621
Feb 07
23:12:17
User "admin" logged in

10620
Feb 07
23:12:04
User "admin" failed to login (incorrect password)

10617
Feb 07
22:46:52
UDP
68.17.216.252
50932
129.142.yyy.yyy (S-Box)
137 (NETBIOS)

10614
Feb 07
21:20:18
TCP
67.40.196.178
3628
129.142.yyy.yyy (S-Box)
21 (FTP)

10613
Feb 07
20:52:40
UDP
212.129.183.110
56361
129.142.yyy.yyy (S-Box)

3.3.9 Objective 9. Test the Physical Security

Item 30: The S-Box is secured in a physically secure location
objective subjective | reference: Generally recommended practices
Risk: Unauthorized physical access to firewall and LAN may be used for an attack... Unauthorized access can also allow a potential attacker to cover his track. Pressing reset button for 5 seconds on the S-Box will enable restoration of factory defaults and delete the log.
Testing: Is the S-Box placed in a physically secure location? Physical access is to the S-Box and the local LAN must be limited by locked doors. Only trusted persons have access into this space.
passed failed **The test passed** All physical access to the offices required a physical access card. No stranger was allowed unaccompanied.

Item 31: The S-Box is not a single point of failure
objective subjective | reference: Generally recommended practices
Risk: Hardware failure, theft.
Testing: presence of a "cold" stand-by proper configured extra S-Box
passed failed The test passed **Auditor's remark.** As an emergency measure, there was a configured spare S-Box locked placed in a safe. I was used as a cold stand-by.

3.3.10 Objective 10. Performance of the S-Box

Item 32: The S-Box performs well and don't degrade Internet traffic
objective subjective | reference: Own
Risk: Performance degrading of the S-Box can be a indication of an attack
Testing: We will check the upload and download speed to the ISP, with and without the S-Box. The speed Test (http://www.teledanmark.dk/menu/sm3152.htm) is offered by the local ISP, and is based on the calculation of up- and download speed, of 4 different test sequences, each of them with 10 seconds duration. **With S-Box** Download in KPBS 114 Upload in KPBS 142 **Without S-Box** Top of Form Download in KPBS 241 Upload in KPBS 146

passed failed **Auditor's remark.** The test failed as the download was down over 50%. This could be due to S-Box software is relative new. This could be corrected in later software releases.

3.4 Measuring Residual Risk

As no ready-to-use checklists existed, this audit was conducted in the context of an auditor's view, and focused on policies and procedures in a small office.

3.4.1 Organizational issues

The computers and the LAN, which the S-Box is intended to secure, are typically purchased and owned by the remote users. This undermines the opportunity for a comprehensive corporate security solution. But it is important for the company, that the remote users are aware of the company's need for security, and that they are aware of their role in reducing the security risk for themselves and the company.

3.4.2 Technological issues

Some limitations were encountered in the audit. They are due to fact that the S-Box product is a new product, and the technology of the S-Box is built upon a small proprietary Linux box, without possibilities of expansion in the hardware. But the software is scalable to a certain extent, and is secure, if it is properly configured.
Most of the weaknesses in the technology portion of this audit occur, as a result from inappropriate configurations of firewall rules. An inexpensive and fast solution would be to let a second security officer review the rulebase, when it is being developed and maintained.

Any open port or enabled service provides some level of risk. It is unrealistic to completely remove this risk, even though the vulnerability test in the audit shows that CheckPoint *really has hardened their box*. However, vulnerability scans at a regular interval, of the S-Box is needed, as it can provide a measure of preventive control by ensuring, that only the necessary services and ports are enabled.

3.4.3 Control objectives

Within the scope of this assignment and the controls defined, the work of the audit achieved most of the desired control objectives. But even after correcting the shortcomings of an S-Box installation risks remain. Additional threat comes from downloaded malware that installs back doors, plants worms or leaves a zombie agent on the local system. In short, many of the highest risks identified remain the same, even with a properly configured S-Box. This is avoided by having "defence in depth", where we install virus scanners on all local equipment and design procedures for maintaining them updated.
The local LAN could also have an intrusion detection system. The open-source, multi-platform intrusion detection system "Snort"[8], is an affordable option.

3.5 Is the System Auditable?

Some of the tests in the Audit are verifiable through simple system

[8] www.snort.org

commands. Other tests in the audit are not verifiable, and depend on claims from the manufacturer.

The S-Box runs on a proprietary operating system based on Linux2.1.122 - 2.2.16 (ref. Nmap), running on a 133 MHz MIPS processor with 2x8mb of flash memory, 32mb of RAM and 5 NIC interfaces (detected by physically opening the S-Box).

It doesn't provide access to the operating system (**no shell prompt**), and is only designed to do the firewall task. Consequently, it is not possible to evaluate the configuration of the operating system, and we have to rely on the vendor to provide patches, when vulnerabilities are discovered. On the other hand, as these devices are designed from the bottom up as firewall appliance, we can expect them to be well designed. The fact, that it was impossible for Nessus to run a scan without "hanging", shows that the manufacture knows the Nessus program well.

We can also expect only the necessary services running, as they are running on a small CPU with little available memory, which invite to restricting the use of services.

Audit of the 1) hardware itself, 2) crash recovery and 3) hardware weaknesses is not possible. A good test would have been to reverse engineer the S-Box, install a custom version of Linux without CheckPoint software, install *iptables* instead and audit this system.

In the future, it is expected that CheckPoint will implement features like a SNMP agents on the S-Box. (Being Linux, it should not be the vulnerable ucd-snmp unpatched). It would facilitate a much better surveillance of the S-Box, which makes it more acceptable for a big organisation.

4 Assignment 4. Audit Report and Risk Assessment

4.1 Executive Summary

Based on a checklist, tests were conducted to evaluate the security of the S-Box in order to verify, if the security rules were functioning. The main point of interest was security of an S-Box in a LAN/ WAN environment in a remote office. A checklist was filled out and interviews were conducted with local staff in order to check their awareness of the security. Ten security areas were identified for inclusion in the scope of this audit. They have been tested and included in assignment 3 of this report. Of the 10 checklist items 4 passed and 6 failed. This result doesn't indicate that the use of the S-Box should be avoided, but rather that the audit was directed towards the areas of security concern.
Security was found to be acceptable, but significant additional measures must be taken to secure the installation properly.

4.2 Audit Findings

Lack of operational security policies makes it difficult to conduct an effective audit, but an audit is an iterative process, where the audit can lead to a new policy and new checklists. This leads to adaptation of new procedures, which again can lead to a new audit and new checklists.

In general a local security officer or a local management should be informed about policies of general security, local setups, change requests, LAN/WAN security and end-user security. This coordination is necessary in order to be able to measure compliance with corporate policy and procedures.

Audits at the remote site should take place at regular intervals to find misconfigured S-Boxes (and other equipment). Scanners, vulnerability checkers and intrusion detection tools, can help detecting obvious security flaws in the local LAN and the S-Box.

Audit Conclusion:
Special consideration should be given to the following items:

- Using a strong password for login is preferable. Especially in combination with a two-factor authentication, such as RSA SecureID.
- The S-Box should be located in a physically secure location.
- Firewall rules should be audited regularly and systematically.
- Re-testing the S-Box is highly recommended, if it is to be used in a VPN situation in a home or remote office.

4.2.1 Objective 1. Only authorized users have access to the S-Box

Risk:
The authentication on the S-Box is very weak.
An intruder could easily take control over the S-Box by guessing the password (by means of password crackers) and attack the corporate net through the S-Box.

It is concealed, who is accessing/attacking the S-Box, as the individual PC accessing the S-Box is not identified by name or IP in the log.
Recommendation:
This flaw must be accepted as a risk, otherwise we have to stop using the S-Box, as it cannot be expected that CheckPoint will mend this deficiency.
Cost:
Introducing a "real" firewall will be costly, but may be necessary.
Compensating controls:
Restricting access to the LAN by using the PC's MAC addresses in the LAN switches. This requires education of the local system administrator.

4.2.2 **Objective** 2. S-Box software is at the current patch level

Risk:
No automatically update of patches to the S-Box takes place. This is a security risk. New or unknown attacks can happen on unpatched S-Boxes.
Recommendation:
Agreement with the manufacturer's sales organisation should be arranged, in order to facilitate automatic scheduled downloads of patches.
Cost:
Ought to be inexpensive. Nowadays it is a common practice for the manufacturers to place new patches on the public Internet.
Compensating controls:
Arrange with the seller to send the patches by post or e-mail, as soon they are available.

4.2.3 **Objective** 3. Are S-Box logs secured?

Risk:
Any person near the S-Box (or the electrical outlet) can erase the log by turning the electricity off. The log has no protection in case of that kind of malicious attack.
Recommendation:
The firewall has to be placed in a locked-up cupboard with an Uninterruptible Power Supply.
Cost:
Probably more than the S-Box, but still relatively inexpensive.
Compensating controls:
Place the S-Box discretely, in order to avoid the prying of non-authorized personnel.

4.2.4 **Objective** 4. Only approved applications can access the Internet

Risk:
The firewall doesn't check the applications, only IP-addresses and ports. Many applications use port 80, which is also the standard HTTP port for browsing on the Internet.
The target of cyber attack has moved from the network infrastructure to the applications, which now is a colossal security risk. "Big" firewalls have the same security problem.
Recommendation:
Add a personal firewall, like ZoneAlarm, to the defence structure, for

application filtering.
Cost:
Relatively inexpensive.
Compensating controls:
Control all the programs, whether they are approved or not, before installing them on the local PCs.

4.2.5 Objective 5. Access from the Internet is prohibited

Risk:
If untrusted systems can see or access the S-Box, they can mount attacks against it, or gather information about applications that may be in use on that system.
Recommendation:
Harden the operating system.
Cost:
None. Already done by the manufacturer.
Compensating controls:
Have a “Packet Sniffer” and/or a “Honey Pot” on the outside of the S-Box.

4.2.6 Objective 6. Access to the Internet from local LAN is restricted

Risk:
Applications can use the local LAN to attack other systems either independently or as part of a distributed attack (e.g. Distributed Denial of Service).
The test was passed, because the S-Box protected the Internet from traffic, except from http/https, the management ports and other necessary services.
Recommendation:
Egress filter on the S-Box.
Cost:
None. Built-in feature.
Compensating controls:
Have a “Packet Sniffer” and/or a “Honey Pot” on the inside of the S-Box.

4.2.7 Objective 7. Check the S-Box rules

Risk:
As mention several times above: *The most common cause of firewall security breaches is a misconfiguration of the firewall system (www.cert.org).*
There is no automatic log of configuration changes and no manual log either.
Changes could make the whole network open and vulnerable to attack.
There is no method of finding out, how and when changes have taken place.
Recommendation:
As the S-Box has no built-in tracking features, a manual log book has to be kept.
In addition every change must be certified by a second security officer and documented in the log book.
Cost:
Requires some extra time, but as the number of changes is few in a life-cycle of an S-Box, the extra hours needed, will be few.

Compensating controls:
None.

4.2.8 **Objective** 8. Logging, detection and reaction

Risk:
No local person has enough knowledge to recognise unusual situations, and the remote office doesn't have a reaction plan ready.
Recommendation:
- Train local personnel in security issues.
- Hire personnel with security knowledge.

Cost:
Expenses used for education must to be compared with the risk of downtime, due to an attack.
Compensating controls:
Write a reaction plan. It will probably have little value, as the log size is too little (only 100 records) to have any real usage for the inexperienced administrator. In case of attack/accident, it will be near impossible to track the course of events.

4.2.9 Objective 9. Test the physical security

Risk:
The necessary physical provisions as locks and identity cards were present, but the S-Box uses DHCP to allocate addresses. With portable PCs, it is possible to connect to the local net without any problems, as to get a DHCP address and subsequently access to the whole LAN and the Internet.
Recommendation:
Put the MAC-addresses of the PCs into the switches on the local LAN and control access to the local net from the switches.
Cost:
None, except initial education.
Compensating controls:
None.

4.2.10 Objective 10. Performance degradation of the S-Box

Risk:
Slow lines can be a sign of an attack (e.g. The Slammer Virus).
Recommendation:
Use a maximum of 5 users on an S-Box with a 256 kbps line, as the S-Box reduces the bandwidth significantly.
Cost:
If there are more than 5 users on the local LAN, a "real'" firewall might be necessary instead of the S-Box.
It will cost at least 5 times more than the S-Box.
Compensating controls:
Wait installing the S-Box, until it is a mature product, and the software is more efficient.

4.3 Audit recommendation

We will recommend regular audit of the local site to ensure security (i.e.

once every year). These audits could help find misconfigured devices. It was clear that security can be significantly increased by strengthening authentication, malware checking and improvement of the security policy.

4.4 Cost

A strong security, relying on a reasonable sound written security policy, effective procedures and personnel, who have been educated in security issues and are aware of the security issues, does not have to be costly.

References

Bibliography

Books:

[1] Cole, Eric. Hackers Beware, New Riders 2002
[2] Hoelzer, David. Track 7 Auditing Principles and Concepts Volume 7.1. SANS Institute, 2002
[3] Hatch, Brian et al. Hacking Linux Exposed, Osborne/McGraw-Hill, 2001
[4] Information Systems Audit and Control Association, "Control Objectives for IT Governance", IT Governance Institute, July 2000
[5] Northcutt, Stephen. Track 7 – Auditing the Perimeter, Volume 7.2 Auditing Networks and Firewalls. SANS Institute, 2002
[6] Schneier, Bruce. Secrets and Lies: Digital Security in a Networked World, Wiley, 2000
[7] Staron, Richard J., ed. Security Complete, Sybex 2001

On-line resources:

[8] Auditnet: www.auditnet.org
[9] CERT: www.cert.org
[10] CIAC: www.ciac.org
[11] CIS Security: www.cisecurity.com
[12] Cohen, Fred and Associate Management Analytics. “Management Analytics Firewall Checklist”, 1995. http://www.all.net/books/audit/Firewall/manal/index.html (2-jan-2003).
[13] Computer Security Auditing & Testing: http://www.insecure.org/sploits.html
[14] Computer Security Institute, 600 Harrison St. San Franciso, 1999/2002
[15] Deploying Firewalls, CERT Coordination Centre: http://www.cert.org/security-improvement/practices/p060.html
[16] Grundschober, Stéphane. Auditing Firewall in a Small Office /Home Office environment, SANS GSNS Practical, Sep 2001, http://www.giac.org/GSNA.php
[17] http://www.packetfactory.net/
[18] Krishni Naidu, “Firewall Checklist”, www.sans.org
[19] Phone boy: www.phoneboy.com
[20] SANS: www.sans.org
[21] Spitzner, Lance. “Auditing your Firewall Setup”, 12 December 2000. http://www.enteract.com/~lspitz/audit.html (15-jan-2003)
[22] Wallyware: Hacker Whacker: See your computer the way hackers do, http://hackerwhacker.com/

Appendix A. Penetration Test Tools

Information Gathering
Nmap – Network scanning, port scanning and OS detection
http://www.insecure.org/nmap/index.html

hping – Tool for port scanning.
http://www.kyuzz.org/antirez/hping.html

netcat - Grabs service banners / versions.
http://packetstorm.securify.com/UNIX/netcat/

firewalk - Determining firewall ACLs.
http://www.packetfactory.net/Projects/Firewalk/

ethereal - Monitoring and logging return traffic from maps and scans.
http://www.ethereal.com/

icmpquery - Determining target system time and netmask.
http://packetstorm.securify.com/UNIX/scanners/icmpquery.c

Leak Test - Gibson, Steve, "LeakTest – Firewall Leakage Tester"
http://grc.com/lt/leaktest.htm

ShieldsUp! - Gibson, Steve: "Determines your machine's current IP address"
http://www.grc.com.

NTOMax – Foundstone, "TCP traffic generator"
http://Foundstone.com

BlackWidow - SoftByteLabs. Web site scanner, site mapping tool, a site ripper, a site mirroring tool and offline browser program.
http:// SoftByteLabs.com

Vulnerability Detection
Nessus - Scans for vulnerabilities.
http://www.nessus.org/

SARA – Another scanner to scan for vulnerabilities.
http://www.www-arc.com/sara/

Password cracking
Brutus – Telnet, FTP and HTTP Password cracker
http://www.hoobie.net/brutus

LC3 – Password cracking utility
http://www.atstake.com/lc3

Intrusion Detection
SNORT – Intrusion Detection System

http://www.snort.org

Appendix B. S-Box Product Features

Product Features according to supplier (www.sofaware.com)

No. of LAN Ports 4
WAN Connection RJ-45
LAN Connection RJ-45
LAN Protocols 10/100BaseTX Combo
WAN Protocols Cable modem
WAN Protocols DSL
No. of WAN Ports 1

Specifications:

CheckPoint Stateful Inspection firewall
Network Address Translation (NAT)
Port Address Translation (PAT)
Protection from Denial of Service attacks
Anti-spoofing
Logging and alerting
Preset security policies
Connectivity
PPPoE support
PPTP support
DHCP server support
DHCP client support
Management
Local Web-based interface
Password protection

Ports/Connectors
SofaWare S-Box:
(1) RJ-45 port for 10/100 WAN connection
(4) RJ-45 switched ports for 10/100 LAN connections

Appendix C. Password construction

In order to be safe and secure passwords must be at least 8 characters in length
Contain characters from all 4 of the following groups:

- Uppercase letters A, B, C... Z
- Lowercase letters a, b, c... z
- Numerals 0, 1, 2... 9
- Special characters -! * ^ + = [ ]

Avoid any of the following:

- Proper names
- Place names
- Brand, product or company names
- Ordinary words
- Obscene words or derivatives from them

Avoid simple letter/numeric substitutions in any of the above, e.g. substituting zeroes and ones for the letters O and L.

Do not base a password on previous passwords.

Appendix D. S-Box Vulnerability list

** From BugTraq www.securityfocus.com ***

There are **no** vulnerabilities reported on the S-Box.