Auditing a Nokia IP 330 Check Point Firewall-1 NG FP3
An Auditor’s Perspective

SANS GSNA
Practical Assignment Version 2.1
January 27, 2004

Curtis L. Hefflin, Jr.

Table of Contents

Abstract

This document partially fulfills of the requirements for the GIAC Systems and Network Auditor (GSNA) certification. It is based on an audit of a Nokia CheckPoint Firewall that provides network security protection for a small consulting organization. The technical aspects of this audit were performed during October and November of 2003.

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

1.1 Introduction

This audit is performed on a small organization's primary IP network firewall. The audit target is a Nokia IP 330 running CheckPoint Firewall-1/VPN-1 NG Feature Pack 3 software. The firewall acts as the security gateway separating the internal network, DMZ, 'wildcard' network, and the Internet. The wildcard network is comprised of wireless and wired workstations externally positioned between the Nokia Checkpoint Firewall and the border router. The firewall is also the VPN terminator for remote user access. Remote user client workstations use Checkpoint VPN-1 SecuRemote/SecureClient NG for secure connectivity to the firm's internal network for access to file, development, and test servers.

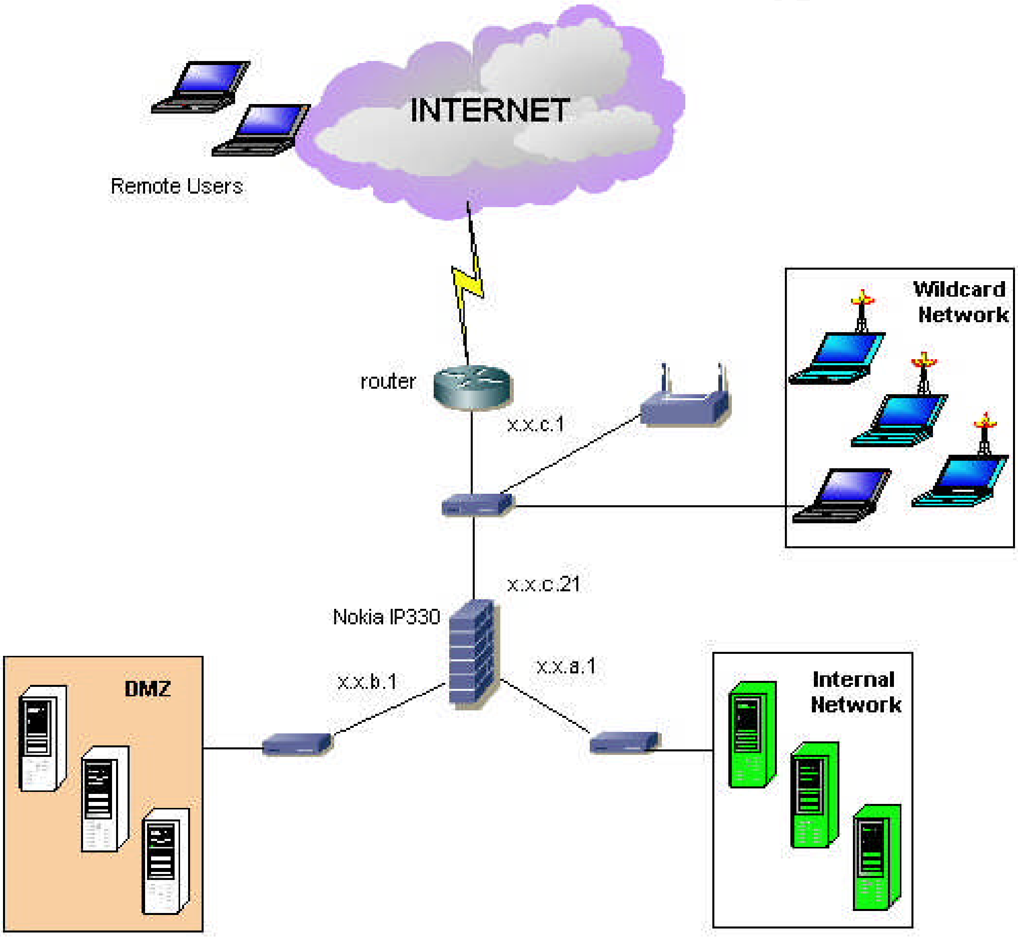
1.2 Identify the system to be audited

This audit is on a Nokia IP 330 Firewall running IPSO 3.6 FCS6 operating system, a BSD unix variant. The firewall software is CheckPoint Firewall-1 NG Feature Pack 3. The following table provides additional firewall configuration details.

Nokia IP330		
Model	IP330	
Memory	64 MB	
SW Release	IPSO 3.6 FCS6	
SW Version	Releng 1061 01.21.2003-230310	
Interface Configuration		
eth-s2p1	Unused	
eth-s2p2	Unused	
eth-s3p1	x.x.a.1	Internal interface—Internal systems provide DNS, print, and file services to internal users. This is also the encryption domain for remote users to access development and test servers.
eth-s4p1	x.x.b.1	DMZ interface—Systems on this net are natted to outside for public and remote user access.
eth-s5p1	x.x.c.21	Outside Interface—Connected via hub to border router. The wildcard network

		is on the x.x.c.x segment.
CheckPoint Firewall Software		
- Check Point VPN-1/FireWall-1 NG Feature Pack 3 (Build 53225) - Check Point SVN Foundation NG Feature Pack 3 (Build 53267) - VPN-1 SecuRemote/SecureClient NG Feature Pack 3 (Build 53328)		

The firewall acts as the security gateway separating the internal network, DMZ, wildcard network, and the Internet. The firewall is also the VPN terminator for remote users. Each network segment is connected via Linksys EtherFast 10/100 Workgroup Hubs. The following is an overview of the logical design.



Organization Network Overview

1.3 Evaluate the risk to the system

An evaluation of risks begins with the identification of threats and potential outcomes. Threats are conditions, circumstances, and events with the potential to cause harm to a system or the information it contains. The security control objectives detailed below considers the variety of threats to which the Nokia Checkpoint Firewall and the information assets it protects will be subject.

1.3.1 Threat Sources

There are a variety of potential threat sources with the capability and in some cases intent to exploit system and design vulnerabilities as they relate to the Nokia Checkpoint Firewall and the assets it protects. Threats can be borne by humans, the system itself, the physical environment, and by nature. Human threats can be either deliberate or accidental. The following list represents threat source groupings [1] for the Nokia Checkpoint Firewall.

- <u>Individuals using network access</u> – The threats in this category are network-based threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature. Potential outcomes include:
    - Unauthorized system access
    - Unauthorized access to system functions
    - Unauthorized disclosure of data
    - Unauthorized modification or destruction of data
    - Disruption of system operations
    - Misuse of system resources
    - Inserting malicious code
    - Passive wiretapping
    - Active wiretapping
    - IP spoofing
    - Traffic analysis
    - Disruption of network communications

- <u>Individuals using physical access</u> – The threats in this category are physical threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature. Potential outcomes include:

  - Hardware destruction
  - Hardware theft
  - Use of unauthorized hardware
  - Active wiretapping
  - Passive wiretapping
  - Unauthorized system access
  - Accidental hardware damage
  - Unauthorized initiation of network connection
  - Unauthorized facility access
  - Destruction of facility components
  - Disruption of system operations

- <u>System problems</u> – The threats in this category are problems with an organization’s information technology systems. Examples include:

  - Misconfigurations
  - Hardware defects
  - Software defects
  - Unavailability of related systems
  - Viruses, worms, malicious code
  - Design flaws
  - Improper configuration
  - Operator error
  - Accidental data damage
  - Accidental hardware damage
  - External network communications failure
  - Internal network component failure
  - System component failure

- <u>Administration/Management problems</u> – The threats in this category are problems with the administration of information security and assurance policies, procedures, and guidelines. Examples include the lack of, or poor:

  - Training programs
  - Security policy
  - Configuration management
  - Backup and recovery
  - Patch management
  - Configuration guidelines
  - Change control
  - Firewall policy

- <u>Other problems</u> – The threats in this category are problems or situations that are outside the control of an organization. This category of threats includes natural disasters that can affect an organization’s information technology systems as well as interdependency risks. Interdependency risks include the unavailability of critical infrastructures (telecommunications, electricity, etc.). Other types of threats outside the control of an organization can also be included here. Examples of these threats include:

  - System component failure
  - Network communications
  - Electromagnetic Interference
  - Lightning

failure
- o Power disturbance/outage
- o Fire
- o Severe Storm
- o Water Damage

1.3.2 General Risks to the System

The following table represents the risks to the Nokia Checkpoint Firewall including the Nokia hardware, IPSO operating system, Checkpoint Firewall NG software, and firewall properties and rulebase configuration

Each of the vulnerabilities listed below would be considered severe if they were fully exploited. The threat/likelihood could be considered low to high depending on the technical and procedural controls that are implemented to mitigate the identified vulnerabilities.

Vulnerability	Treat	Adverse Outcomes (risks)
Inadequate physical security controls to the Nokia Checkpoint Firewall.	The primary threat sources for this vulnerability are individuals with physical access to the office space hosting the organization's computer and network systems. In most cases this includes organization employees, maintenance and cleaning personnel.	Inadequate physical security controls could lead to the following potentially adverse outcomes. • Unauthorized user interacts with a valid users computer system. • Unauthorized user simply turns off a computer or networking device by hitting the off switch or pulling the power cable. • Unauthorized access to system consoles can enable the user to interrupt the boot process to get access to the root prompt. • An attacker can boot the system from a modified boot disk • Physical access also enables password guessing since password lockout feature are not typically enforced at the console. • Unauthorized users can gain access to backup media and printouts of data/information. • An unauthorized user can capture network traffic by accessing hubs and network cables.

Inadequate network access controls to the Nokia IPSO operating system and checkpoint application	The primary threat source for this vulnerability is individuals using network access including organization staff with authorized and unauthorized network access and outsiders with unauthorized access.	Inadequate network access controls to the Nokia IPSO operating system and checkpoint application could lead to unauthorized operating system and application configuration changes. This can in turn lead to additional adverse outcomes, including: • Disruption of network communications • Disruption of system operations • Unauthorized disclosure of data • Unauthorized modification/destruction of data
Misconfiguration of Checkpoint firewall properties and rulebase.	The primary threat source for this vulnerability includes individuals with network and physical access to the Nokia Checkpoint Firewall. In most cases these individuals are organization employees or contract network engineers authorized to access, configure and manage the firewall's properties and rulebase. The likelihood that firewall misconfigurations will occur depend a great deal on the training and experience of the network engineer as well as the policies, procedures, and guidelines this person must comply with.	Considering the critical role the firewall plays in the security of the organization's network accessible assets, poorly configured firewall properties and rules can lead to numerous adverse outcomes. • Disruption of network communications • Disruption of system operations • Unauthorized disclosure of data • Unauthorized modification or destruction of data • Unauthorized system access • Misuse of system resources • Unauthorized initiation of network connection

Misconfiguration of Nokia IPSO operating system	The primary threat source for this vulnerability includes individuals with network and physical access to the Nokia device. In most cases these individuals are organization employees or contract engineers authorized to access, configure and manage the IPSO operating system properties. The likelihood IPSO operating system misconfigurations will occur depends a great deal on the training and experience of the engineer as well as the policies, procedures, and guidelines this person must comply with.	The Nokia IPSO operating system is essentially a highly configurable router that supports a wide range of internet protocols, LAN and WAN technologies, and remote management capabilities. Misconfiguration of this device can lead to numerous issues including: • Disruption of network communications • Disruption of system operations • Unauthorized initiation of network connection • Unauthorized system access
Inadequate policies procedures and guidelines	The primary threat source here is the organization's management and IT staff. Management must direct the development of and enforce compliance to information assurance and policies, procedures, and guidelines.	Solid, well developed, policies, procedures, and guidelines will diminish the likelihood of adverse outcomes of inadequate policies procedures and guidelines including: • Ad hoc firewall policy changes that have not gone through change control procedures • Rulebase implementations counter to security policy • Inadequate backup and recovery procedures can lead to the loss or destruction of vital system information. • Lack of configuration guidelines can lead to inconsistent system configurations.

Inadequate hardware redundancy	The primary threat source for this vulnerability includes hardware and software defects that could cause system crashes and hardware failures.	Single point of failure in a device that plays a critical security and access role poses the risk of interruption of access to important information, software, applications, and services.

1.4 What is the current state of practice, if any?

Auditing perimeter networks appears to be a robust activity with numerous resources available to the auditor. The resources range from general information system auditing to specific Checkpoint Firewall-1 auditing guidelines. The following sections include general resources, books, and websites.

1.4.1 General Resources

Federal and Department of Defense (DoD) agencies provide ample resources in this area due to Federal and DoD Certification and Accreditation requirements. Processes such as NIACAP (National Information Assurance Certification and Accreditation Process) and DITSCAP (DoD Information Technology Security Certification and Accreditation Process) provide security testing and evaluation guidelines for information systems that will operate on Federal and DoD networks. The guidelines are specific and provide solid auditable control and procedural objectives. The following table is excerpted from a DoD information security Requirements Traceability Matrix (RTM). It shows several DoD information system security requirements.

Req. Number	Requirement Description	Source Document	Related Requirements	Audit Method				Comments
				I	D	T	O	
I&A.3	The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user.	TCSEC, 3.1.2.1; 3.2.2.1; 3.3.2.1						
I&A.4	The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP	TCSEC, 3.1.2.1; 3.2.2.1; 3.3.2.1						
AUD.2	The audit trail shall be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur.	DoDD 5200.28, Encl. 3, A.1	TCSEC 2.2.2.2					

(I)nterview, (D)ocument Review, (T)esting Techinque, and (O)bservation

1.4.2 Books

Inside Network Perimeter Security by Stephen Northcutt, Lenny Zelter, et al., is a comprehensive information security book that covers defending network perimeters. It goes in to detail on the integration of various perimeter security devices including routers, firewalls, VPNs, and Intrusion Detection Systems (IDS) and how the devices are best positioned in perimeter security designs. Inside Network Perimeter Security also presents a discussion on assessment techniques. The Internal Assessment section provides several firewall control objectives along with the tools and procedures for testing.

Hacking Exposed provides a detailed view of how hackers, crackers and other unauthorized users view information technologies, both network- and host-based, and the tools and techniques that are used to exploit security vulnerabilities. There is also detailed discussion on how security engineers can mitigated the risks discussed. The authors make the point that "most firewalls are often misconfigured, unmaintained, and unmonitored", thus exposing the protected network to unauthorized access. There are detailed discussions on how to identify and exploit firewall vulnerabilities and misconfigurations using tools such as nmap, netcat, firewalk and hping. The authors also describe countermeasures that security engineers can employ to defend against the various attack techniques presented.

Managing Information Security Risks, The OCTAVE Approach provides methodologies for self-directed security evaluations that was developed at the CERT Coordination Center. It is designed to help an organization identify and rank key information assets; weigh threats to those assets; and analyze vulnerabilities involving technology and practices.

1.4.3 Web Sites

The following short list represents key information security web resources that provide audit guidance.

- http://iase.disa.mil/
  Information Assurance Support Environment (IASE)—IASE is a Department of Defense sponsored clearinghouse for information assurance information.

- http://csrc.ncsl.nist.gov/ and http://csrc.ncsl.nist.gov/pcig/cig.html
  National Institute of Standards & Technology (NIST) Computer Security Resource Clearinghouse—This NIST site provides numerous information assurance and security checklists and implementation guides referred to as STIGs (Security Technical Implementation Guides)

- http://www.cert.org/octave/
  Computer Emergency Response Team (CERT) developed The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method the defines a phased approach to a comprehensive, systematic, context-driven information security risk evaluation.

- http://www.infosyssec.org
  Information Systems Security Resource is a comprehensive security information resource portal that provides links to relevant audit resources including threat risk assessments and guides

- http://www.sans.org
  The SANS (SysAdmin, Audit, Network, Security) Institute is a cooperative research and education organization. It enables security professionals, auditors, system administrators, and network administrators to share the lessons they are learning and find solutions to the challenges they face. The site provides numerous auditing resources via articles and research papers.

- http://www.securityfocus.com
  Security Focus is a comprehensive security portal providing wide and in-depth information in all areas of information assurance and security.

2 Assignment 2 –Create An Audit Checklist

The following tables address the technical and procedural control objectives in auditing the Nokia Checkpoint Firewall. As previously discussed, the device sits behind a border router and filters network traffic to and from the Internet, 'wildcard' LAN, internal LAN, DMZ, and SecuRemote connections.

In identifying the risks for each of the control objectives detailed below, the following terms were used.

Vulnerability— a weakness in an information system, system security practices and procedures, administrative controls, internal controls, implementation, or physical layout that could be exploited by a threat to gain unauthorized access to information or disrupt processing. [1]

Threat—an indication of a potential undesirable event. A threat refers to a situation in which a individual (threat source) could do something undesirable (an attacker initiating a denial-of-service attack against an organization's email server) or a natural occurrence (threat source) could cause an undesirable outcome (a fire damaging an organization's information technology hardware). [1]

Likelihood—an estimate on the likelihood a threat source could or would exploit vulnerability.

Risk—a function of the likelihood of a given threat-source exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization. [6,14]

The control objectives are broken down into seven information assurance and security categories.

Information Assurance and Security Categories	Abbreviation
Policies, Procedures, and Guidelines	PPG
Identification & Authentication	IAU
Physical and Environmental	PEN
Security Design and Configuration	SDC
Continuity	CON
Encryption	ENC
Audit Trail, Monitoring, Analysis and Reporting	ATR

2.1 Policies, Procedures and Guidelines

PPG-1	Check 1 of 21
Description	Information Security Policies, Procedures, and Guidelines.
Reference	1, 3, 10, 20, experience (Note: the numbers correspond to the references in Appendix A)
Control Objective	Ensure that policies, procedures, and guidelines are established for all aspects of information assurance as it relates to the Nokia CheckPoint Firewall. Areas of concern include Security Policy; Configuration Management; Backup and Recovery; Patch Management; Configuration Guides; Change Control; and Firewall Policy.
Risk	Vulnerability Incomplete policies, procedures, and guidelines leaves the Nokia Checkpoint Firewall system vulnerable to ad hoc system configuration and firewall policy changes potentially rendering the system and the assets it protects in a less secure posture. Threat Source The most likely threat source is an organization employee making configuration changes to the Nokia IPSO operating system and the Checkpoint firewall application. Likelihood It is probable that incomplete policies, procedures, and guidelines exist in a small newly formed organization. In this environment it is highly likely the threat source could expose the vulnerability. Potential Outcome The network protection provided by the Nokia Checkpoint Firewall can be undermined without clearly documented policies, procedures, and guidelines. Ad hoc firewall policy changes that have not gone through change control procedures can lead to misconfigurations that expose information to unauthorized disclosure, modification, loss, and/or destruction. Lax or non-existent backup and recovery policies and procedures can lead to prolonged interruption of service, and the loss or destruction of vital system information.
Compliance	Compliance to this control objective is met if the

<table>
<tr><td></td><td>organization has documented policies, procedures, and guidelines.</td></tr>
<tr><td>Testing</td><td>Interview key staff and review the documented policies, procedures, and guidelines as detailed in the following table.
<table>
<tr><th rowspan="2">Test #</th><th rowspan="2">Control Objective to Test</th><th colspan="2">How Reviewed</th><th colspan="2">Compliant</th></tr>
<tr><th>I</th><th>D</th><th>Yes</th><th>No</th></tr>
<tr><td>PPG-1.1</td><td>Security Policy</td><td></td><td></td><td></td><td></td></tr>
<tr><td>PPG-1.2</td><td>Configuration Management</td><td></td><td></td><td></td><td></td></tr>
<tr><td>PPG-1.3</td><td>Backup and Recovery</td><td></td><td></td><td></td><td></td></tr>
<tr><td>PPG-1.4</td><td>Patch Management</td><td></td><td></td><td></td><td></td></tr>
<tr><td>PPG-1.5</td><td>Configuration Guides</td><td></td><td></td><td></td><td></td></tr>
<tr><td>PPG-1.6</td><td>Change Control</td><td></td><td></td><td></td><td></td></tr>
<tr><td>PPG-1.7</td><td>Firewall Policy</td><td></td><td></td><td></td><td></td></tr>
</table>
I-Interview D-Documentation</td></tr>
<tr><td>Analysis</td><td>The interview process and review of documentation is somewhat subjective. Although a checklist is used, the auditor must review and determine the completeness of the documentation.</td></tr>
</table>

2.2 Identification & Authentication

IAU-1	Check 2 of 21
Description	Individual identifier and password access
Reference	5, 8, 16, Experience
Control Objective	Ensure that Nokia IPSO operating system access, Checkpoint application access for management, and SecuRemote access to internal network resources is gained through the presentation of an individual identifier and password.
Risk	Vulnerability Lack of accountability due to shared accounts is the primary vulnerability for this control objective. Threat Source Threats to this vulnerability include authorized users who have been granted user accounts and unauthorized users attempting to access systems via shared or compromised user accounts. Likelihood The likelihood this vulnerability would be exploited is low

	considering that is common practice that all users receive unique logon credentials. However, this is a small and relatively new organization and may not have mature access control polices and procedures in place. They may not necessarily recognize or consider the risks of using shared accounts or having inadequate audit trails. Potential Outcome Inconclusive audit trail of user access to the Nokia Checkpoint Firewall or the assets it protects. If threat sources were to intentionally or accidentally disclose, modify, or destroy protected information, tracking down the responsible individual would be difficult.
Compliance	Compliance to this control objective is met if there are unique accounts and passwords for all authorized users accessing the systems.
Testing	To test for unique accounts 1. Obtain a list of authorized users from management staff. The users will include system administrators and SecuRemote users. 2. Match unique account ID with the individual on the authorized users list. 3. Note any exceptions. 4. Document all accounts and state role. There will likely be system accounts used for internal processes. These should be documented as well.
Analysis	Objective

IAU-2	Check 3 of 21
Description	Password Complexity
Reference	5, 8, 16, Experience
Control Objective	Ensure that passwords are, at a minimum, an 8-12 character mix of case sensitive upper case letters, lower case letters, numbers, and special characters (e.g., 7Turt1e$).
Risk	Vulnerability Weak passwords are relatively easy to compromise given the numerous unix and widows-based tools available to exploit this vulnerability. Poorly configured technical control mechanisms that do not require strong passwords, lockout features, or reuse limits all put the system in a vulnerable position. Threat Source Threats to this vulnerability include authorized users who have

	been granted user accounts and unauthorized users attempting to exploit weak user access mechanisms. These individuals may use physical and network access to exploit the vulnerabilities. Likelihood Given the current state of technical controls available in most security related applications, it is unlikely that a given threat source could exploit weak password vulnerabilities. However, the actual likelihood depends on how well the procedural and technical controls are implemented. Potential Outcome Potential outcomes include the disclosure of corporate information from low valued assets to custom created applications and scripts. Modification of custom application and scripts. Modification of security configurations enabling continued unauthorized access Destruction of custom created applications and scripts would disrupt active projects. Service interruption would prevent remote access to internal systems and development network access
Compliance	Compliance to this control objective is met if the Nokia IPSO operating system, Checkpoint firewall management interface, and SecuRemote logon only accepts passwords that have an 8-12 character mix of case sensitive upper case letters, lower case letters, numbers, and special characters (e.g., 7Turt1e$)
Testing	The following procedures are required to test compliance: 1. Create an account within each application and provide non-compliant passwords. (Use very basic password such as golf, boating, and jazz) 2. Note whether the passwords are accepted. 3. If accepted, log out of the system/application and log back in using the newly created account. 4. Note the success or failure of the logon activity. This procedure is completed and documented for the Nokia IPSO operating system, Checkpoint firewall management interface, and SecuRemote user authentication.
Analysis	Objective

2.3 Physical and Environmental

PEN-1	Check 4 of 21
Description	Physical Access
Reference	2, 16, experience
Control Objective	Ensure that only authorized individuals with need-to-know or need-

	to-access requirements are granted physical access to the Nokia Checkpoint firewall.
Risk	Vulnerability Physical access to the Nokia Checkpoint Firewall by unauthorized personnel can undermine the effectiveness of security and access it is in place to provide. Threat Source Threat sources include organization employees, visitors, and non-employed support and maintenance staff. Likelihood The likelihood of unauthorized physical access in a small office environment is high unless certain mitigating measures are in place. Potential Outcome Physical access can allow unauthorized users to modify system control settings enabling additional access control violations. Physical access can allow the user to gain console access to the system. There is also a potential for service interruption by deliberate or accidental power shut off or removal of network commutations devices or cables. Physical access can potentially result in the loss of the physical device by theft or destruction.
Compliance	Compliance to this control objective is met if physical access controls are in place to control access to the Nokia Checkpoint Firewall.
Testing	Conduct site survey using the physical and environmental security checklist (Appendix B) to ensure that the Nokia Checkpoint Firewall is housed in a locked computer room and held within locked cabinets. Check whether power and network cables are openly exposed.
Analysis	Objective

PEN-2	Check 5 of 21
Description	Power supply
Reference	experience
Control Objective	Ensure the Nokia Checkpoint Firewall is plugged in to an operational uninterruptible power supply (UPS) device.
Risk	Vulnerability Small office environments may have unreliable power supplies and unpredictable voltage fluctuations. They typically do not have backup power sources such as generators.

	Threat Source Threats to this vulnerability are typically non-human in nature. They may include physical and environmental factors such as building supplied power failures and fluctuations, and natural factors such as lightening, severe storms, and flooding. Likelihood The likelihood of a power outage is considered low, however power/voltage fluctuations may occur more frequently. Potential Outcome The primary outcomes include damage or destruction of the Nokia's internal components including: power supply modules, motherboards, memory modules, and hard drives. This can easily result in data and system configuration loss and interruption of access to protected assets and services.
Compliance	Compliance to this control objective is met if the Nokia is plugged into an uninterruptible power supply (UPS) with the following features: • Automatic Voltage Regulation (AVR) • Building wiring fault indicator • Replace battery indicator • Hot swap batteries • Battery management capabilities • Overload Indicator • Status Indicator LEDs • Wide input voltage range
Testing	Conduct site survey using the physical and environmental security checklist (Appendix B) to ensure that the Nokia firewall is plugged in to a UPS device with the minimum features described above.
Analysis	Objective

2.4 Security Design and Configuration

SDC-1	Check 6 of 21
Description	Firewall and Network architecture documentation
Reference	9, 10, experience
Control Objective	Ensure firewall and network architecture is clearly documented and diagramed.
Risk	Vulnerability Poorly documented and diagramed firewall and network architecture does not accurately communicate actual implementation. Threat Source Authorized system administrators implementing configuration

	changes based on poorly documented and diagrammed architecture. Likelihood In a small, rapidly developing organization it is likely the actual implementation is a head of the documentation. Potential Outcome The primary outcome is firewall rulebase misconfigurations which could lead to disruption of service and unauthorized access.
Compliance	Compliance to this control objective is met if the documented firewall and network architecture matches the results of network discovery scanning activities.
Testing	Testing should be carried out using the following procedures: 1. Obtain and review firewall and network documentation and diagrams. 2. Use nmap to ping scan each network segment protected by the Nokia Checkpoint Firewall. 3. Compare the results of the scan to the firewall and network documentation. 4. Note any exceptions.
Analysis	Objective

SDC-2	Check 7 of 21
Description	Firewall business requirements
Reference	Experience
Control Objective	Ensure firewall architecture supports business requirements and security policy.
Risk	Vulnerability The primary vulnerability is an inappropriate amount of access is given to users, administrators, and remote access users due to poor communication between management and security engineers. Threat Source Authorized and unauthorized individuals using network resources are the primary threat sources for the vulnerabilities. Likelihood The likelihood of this vulnerability being exploited is directly related to how well the business requirements are communicated to the individuals responsible for implementing the Nokia Checkpoint Firewall's overall configuration and rulebase. Potential Outcome

	Disclosure of confidential information such as custom application code, proposal drafts, service contracts, etc. This could also led to accidental destruction of valuable information or intellectual property.
Compliance	Compliance to this control objective is somewhat subjective to determine and is based in part on discussions with both the management staff who have developed the organization's business model and the network engineers who implement technical security controls to protect critical assets and information. The auditor must ascertain what assets are most valuable to the organization and what level of access in to and out of each network security zone is required for business purposes.
Testing	Use the following procedures to determine compliance. 1. Interview key management staff using the security requirements questionnaire (Appendix C). 2. Interview network/system engineering staff using the security requirements questionnaire (Appendix C) 3. Review firewall policies/rules to determine if implemented network security meets management expectations and requirements.
Analysis	Subjective

SDC-3	Check 8 of 21
Description	Nokia IPSO operating system security
Reference	Experience
Control Objective	Ensure Nokia IPSO operating system is secure and that unnecessary services are disabled.
Risk	Vulnerability Although the Nokia is installed with the pre-harden IPSO operating systems, it's out of the box configuration will likely have unnecessary and insecure network services enabled. Unnecessary services and a default configuration may provide access for unauthorized users. Threat Source Authorized and unauthorized individuals with network access. This would include inexperienced network engineers who disable the firewall application yet keep the Nokia's interfaces attached and active on the production network. Likelihood It is likely that the various threat sources noted above could exploit an IPSO operating system service. Potential Outcome

	An unauthorized user could gain access to the Nokia IPSO operating system by way of its open and unprotected network services. As a result the unauthorized user could disrupt network services or use the platform to attack other segments of the network.
Compliance	Compliance to this control objective is met if all unnecessary application ports are disabled and that secure applications (SSH and HTTPS) are used for remote management.
Testing	The nmap and Nessus utilities for network scanning and security auditing are used to test this control objective. 1. Review system configuration 2. Research possible vulnerabilities and attacks against the Nokia IPSO operating system using the following internet resources: • CERT CC: http://www.cert.org/nav/index_red.html • Bugtraq: http://www.securityfocus.com/bid 3. Use nmap to scan the Nokia IPSO operating system (be sure the checkpoint firewall is disabled for this activity.) 4. Use Nessus to scan the Nokia IPSO operating system (be sure the checkpoint firewall is disabled for this activity.) 5. Document the findings and map each open udp and tcp port to its service/application. (e.g. 23/tcp-telnet, 80/tcp-http, etc.) Some ports may require additional research to map its corresponding service or application.
Analysis	Objective.

SDC-4	Check 9 of 21
Description	Firewall Application Security
Reference	Experience
Control Objective	Ensure firewall application is secure. Unnecessary services are disabled.
Risk	Vulnerability The default configuration of Checkpoint Firewall-1 may have unnecessary network services enabled. Unnecessary services and a default configuration may provide access points for unauthorized users. Threat Source Authorized and unauthorized individuals with network access. In-experienced system administrators who have not thoroughly tested the firewall prior to production implementation. Likelihood There is a medium likelihood that unauthorized users via network access will compromise the firewall application given its default

	configuration. Potential Outcome An unauthorized user could gain access to the firewall application and alter its configuration. This can in turn be used to disrupt services and access to information resources.
Compliance	Compliance to this control objective is met if all unnecessary application ports are disabled. Additionally, the implemented firewall policy/rulebase must adequately restrict access to the firewall application.
Testing	The nmap and Nessus utilities for network scanning and security auditing are used to test this control objective. 1. Review the firewall policy/rulebase to determine whether access to the firewall application is adequately restricted to authorized hosts and users. 2. Review the $FWDIR/conf/gui-clients file 3. Run the cpconfig command to verify firewall administrators and their level of permissions. 4. Research possible vulnerabilities and attacks against the Checkpoint Firewall application using the following internet resources: • CERT CC: http://www.cert.org/nav/index_red.html • Bugtraq: http://www.securityfocus.com/bid The checkpoint firewall application must be enabled for the following scans 5. Use nmap to scan the Nokia Checkpoint Firewall from an untrusted host. 6. Use Nessus to scan the Nokia Checkpoint Firewall from an untrusted host. 7. Use nmap to scan the Nokia Checkpoint Firewall from a trusted host. (This step will indicate ports, protocols, and services available to management clients.) 8. Use Nessus to scan the Nokia Checkpoint Firewall from a trusted host. 9. Document the findings and map each open udp and tcp port to its service/application. (e.g. 23/tcp-telnet, 80/tcp-http, etc.)
Analysis	Objective

SDC-5, ENC-1	Check 10 of 21
Description	2, 8, 9, Remote management activity security
Reference	Experience
Control Objective	Ensure that Remote management activity to the Nokia IPSO operating system and the firewall application are secured and

	encrypted.
Risk	Vulnerability Nokia ipso operating system permits remote management via telnet and http. Threat Source Authorized and unauthorized users with network analysis tools to capture account information in data transmissions. Likelihood The likelihood in this case depends on the configuration of the IPSO operating system remote management services. Potential Outcome An unauthorized user could capture clear text account information and use it to gain access to the Nokia operating system and alter IPSO and firewall configurations.
Compliance	Compliance is based on a review of the remote management configuration settings for the Nokia IPSO operating system and Checkpoint Firewall application. And, an analysis of captured remote management traffic. All data, including usernames and passwords, transferred between the systems must be encrypted.
Testing	The following procedures should be used to check for compliance for this control objective: 1. Review and document remote management configuration settings for the IPSO operating system. 2. Review and document firewall management settings in the firewall application. 3. Use the ethereal network traffic analyzer to capture remote management network traffic directed at the ipso operating system and the firewall application. 4. Review network captures for any clear text transmissions.
Analysis	Objective

SDC-6	Check 11 of 21
Description	Firewall rulebase
Reference	9, 10, 12, experience
Control Objective	Ensure that the firewall rulebase is logically constructed and annotated and adheres to the organization’s security and firewall policies.
Risk	Vulnerability A poorly constructed and annotated rulebase may have rules inconsistent with the organization’s security and firewall policies. Threat Source

	Authorized individuals (security engineers) with network access to the Nokia Checkpoint Firewall. Security engineers can implement poorly constructed rulesets. Unauthorized individuals with network access are considered threat sources as they may gain access to protected systems as a result of misconfigured rules. Likelihood This is likely to occur when firewall rules are implemented in an ad hoc fashion, during emergencies, or without the guidance of firewall policies and change control procedures. Potential Outcome An unauthorized user can cause a disruption of service, or access key information that could be destroyed, modified, or disclosed. An authorized user may have an inappropriate level of access for the tasks they are required to perform. This may lead to deliberate or accidental destruction, modification, or disclosure of key information.
Compliance	Compliance is based on a thorough review of the firewall configuration and rulebase. The firewall rulebase must be logically constructed and annotated and adheres to the organization's security and firewall policies.
Testing	Examine the organization's firewall and security policies. Review the rulebase for logical construction and proper annotations. Key configuration indicators include: • Network communications not explicitly permitted into a protected network is denied access. • Accepted services should be indicated, except on drop rules where any (all) services are dropped. Otherwise the services permitted should be detailed. • Each rule should be commented indicating the purpose of the rule, date last modified, administrator's name • Tracking should log each rule, or where appropriate an alert should be issued in addition to the log record. • Review global policies • Check that implied rules are logged • Ensure that global policies are consistent with firewall policy and ruleset.
Analysis	There are both subjective and objective elements to testing compliance for this control objective. It is subjective in that there are numerous ways to securely implement a firewall policy. However, there are numerous elements that are objectively verified, including logging, rule comments, and the principle that all traffic not explicitly accepted is denied.

SDC-7	Check 12 of 21
Description	Internal network security
Reference	9, 10, 12, experience
Control Objective	Ensure that access to and from the internal network is appropriately secured.
Risk	Vulnerability The systems within an organization's internal network typically contain the most valuable information assets. A poorly implemented firewall may expose those assets to unauthorized access. Threat Source The primary threat sources are unauthorized users who may exploit firewall misconfiguration vulnerabilities. SecuRemote users also pose a threat as they are given access to internal resources. Likelihood It is likely that unauthorized users could exploit a firewall misconfiguration. Potential Outcome Potential outcomes include information disclosure, unauthorized access, data/information loss and modification. Authorized users who connect via SecuRemote could gain access to systems not intended for their use.
Compliance	Compliance to this control objective is met if the firewall rulebase indicates that internal network access is not permitted from external networks (Internet, DMZ, and wildcard networks). A review of the remote access configuration indicates that SecuRemote users are permitted to access only specific and necessary systems.
Testing	The following test procedures will test for compliance: 1. Review firewall rulebase 2. Review SecuRemote access configuration by reviewing the firewall rulebase and remote access properties. 3. Review the user properties of each SecuRemote user. Check that the location tab indicates specific destination systems. 4. Use the network security tools nmap and firewalk to attempt to enumerate internal network resources from the DMZ, Internet, and wildcard networks. 5. Create a new SecuRemote user, access the internal network and use the superscan4 scanner to attempt to enumerate internal systems.
Analysis	Objective

SDC-8	Check 13 of 21
Description	DMZ network security
Reference	9, 10, 12, experience
Control Objective	Ensure that access to and from the DMZ network is appropriately secured.
Risk	Vulnerability Systems on the DMZ are typical accessible from the Internet and from all organization networks. There is the risk that an unauthorized user who has compromised a DMZ system could initiate another attack from that machine to a host within or outside the organization's network. Therefore, internal and external networks are vulnerable if the firewall system permits DMZ systems to initiate connections to other network segments. Threat Source The primary threat sources are unauthorized users who may exploit firewall misconfiguration vulnerabilities. Likelihood Highly likely unless mitigated at properly configured firewall. Potential Outcome If the chain of events occurred as described above, potential outcomes include information disclosure, unauthorized access, data/information loss and modification.
Compliance	Compliance to this control objective is met if the firewall rulebase indicates that access to DMZ systems is permitted and appropriately logged. The review must also show that any DMZ system initiated traffic is blocked from entering the internal and wildcard networks. Also, any DMZ system initiated traffic destined for the Internet is restricted, logged, and monitored.
Testing	The following test procedures will test for compliance: 1. Review firewall rule base 2. Use the network security tools nmap and firewalk to attempt to enumerate internal network resources from the DMZ. 3. Use the ethereal network traffic analyzer on the internal network to capture any data originating from the DMZ.
Analysis	Objective

SDC-9	Check 14 of 21
Description	Wildcard (wired and wireless segment) network security
Reference	9, 10, 12, experience
Control Objective	Ensure that access to and from the wildcard network is

	appropriately secured.
Risk	Vulnerability In this small office environment WLAN if not properly configured can exposes the entire network to unauthorized access. Reviewing the configuration of the wireless network is out of scope, however securing network traffic to and from the internal network and DMZ is secured at the firewall. Threat Source Unauthorized and authorized individuals with wired and wireless access who are connected to the wildcard network. An additional threat source is system problems associated with the WLAN configuration. Likelihood If the wireless LAN is poorly secured, then it is likely that an unauthorized user could access the organization's resources from that point. Potential Outcome Potential outcomes include information disclosure, unauthorized access, data/information loss and modification.
Compliance	Compliance to this control objective is met if the firewall rulebase indicates that wildcard network traffic is not permitted into the internal network. Internet and DMZ network access is appropriately restricted and logged. An exception to the control objective is granted if the wildcard network system uses SecuRemote encryption to access internal network systems.
Testing	The following test procedures will test for compliance: 1. Review firewall rule base 2. Use the network security tools nmap and firewalk to attempt to enumerate internal resources. 3. Use the ethereal network traffic analyzer on the internal network to capture any data originating from the wildcard network.
Analysis	Objective

SDC-10	Check 15 of 21
Description	SecuRemote Security
Reference	9, 10, 12, experience
Control Objective	Ensure that SecuRemote access is appropriately configured to protect internal network resources.
Risk	Vulnerability SecuRemote enables remote users to access internal systems. If not properly configured and appropriately restricted, remote users

	will have complete network access to all internal systems. Threat Source The primary threat sources are authorized users who have been given remote access to internal systems. There is an additional treat from unauthorized users who compromise the SecuRemote client workstation Likelihood The likelihood depends in large part on the SecuRemote/remote access configuration. Potential Outcome If the SecuRemote/remote access parameters are poorly configured, an authorized or unauthorized SecuRemote user can enumerate the internal network. Potential outcomes include the modification, destruction, or disclosure of valuable information assets.
Compliance	Compliance to this control objective is met if the SecuRemote configuration indicates that remote access global properties, VPN manager properties, and SecuRemote user properties are appropriately configured.
Testing	The following test procedures will test for compliance: 1. Review the remote access VPN basic and advanced properties. 2. Review the user properties of each SecuRemote user. Check that the location tab indicates specific destination systems. 3. Review firewall rulebase to ensure that the remote access rule is logged and commented. 4. Create a new SecuRemote user and attempt to access internal resources. 5. Use the SuperScan network security tool to attempt to enumerate internal network resources from the SecuRemote client. 6. Use the ethereal network analyzer to confirm that data in transit between the SecuRemote client and the Nokia Checkpoint Fireall is encrypted.
Analysis	Objective

SDC-11	Check 16 of 21
Description	IP Spoofing
Reference	8, 9,13, 15, experience
Control Objective	Ensure that the Checkpoint Firewall's defense and anti-spoofing capabilities are appropriately configured to defend against

	network-based attacks such as IP spoofing, Denial of Service, and TCP/IP implementation related attacks.
Risk	Vulnerability IP Spoofing can facilitate successful network based attacks. Threat Source Unauthorized users using deliberate network attack methods. Likelihood Likelihood greatly depends of on whether anti-spoofing and attack defense capabilities are properly configured in the firewall. Potential Outcome Potential harm includes service interruption and system application damage.
Compliance	This control objective is considered compliant if the Checkpoint IP spoofing and SmartDefense capabilities are appropriately configured and engaged.
Testing	The following test procedures will test for compliance: 1. Review firewall properties for appropriate IP address spoofing and logging configuration settings. 2. Review SmartDefense settings to ensure the appropriate checks are enabled and network-based attack activity is logged. 3. Use nmap to attempt to enumerate internal resources. 4. Use Nessus buffer overflow tools to verify SmartDefense setup.
Analysis	Objective

2.5 Continuity

CON-1	Check 17 of 21
Description	System and Configuration Backups
Reference	Experience
Control Objective	Ensure that the Nokia IPSO operating system image, Checkpoint application, and firewall rulebase is regularly backed up and stored off device.
Risk	Vulnerability The Nokia Checkpoint Firewall, like all computer/network devices have mechanical parts that can wear out over time. Hardware and application failures can render a system inoperable and unrecoverable in a timely fashion if their software and configurations are not properly backed-up.

	Threat Source The primary threat sources are operational factors including system component failures (e.g. hard drive, power supply), network component failures (e.g. network interface cards, VPN accelerators), and software crashes. Likelihood Likelihood for this vulnerability to be exposed is considered medium since hardware and software failures do not frequently occur. Potential Outcome Depending on the owner's service contract Nokia hardware can be replaced between 1 and 5 business days. However, without a proper back up of the IPSO image and firewall application configuration, actual downtime could last an additional 24 to 48 hours as the system configuration is brought back to an operational production state This can cost considerable financial resources and lost productivity.
Compliance	This control objective is considered compliant if the system administrator can provide backups of the Nokia IPSO operating system image, Checkpoint application, and firewall rulebase. Backup and restore procedures should be documented and provided.
Testing	The following test procedures will test for compliance: 1. Review backup and recovery policies and procedures. 2. Review the backed-up files and data. 3. If operationally feasible perform a full backup and recovery on the Nokia Checkpoint Firewall using the provided back-up and recovery procedures. 4. Fully test functionality of the Nokia Firewall application - Review the firewall rulebase and policy configuration - Initiate traffic from all segments - Connect remotely using SecuRemote client. - Review firewall logs.
Analysis	Objective

CON-2	Check 18 of 21
Description	Firewall Redundancy
Reference	Experience
Control Objective	Ensure that the Nokia CheckPoint Firewall is not a single point of failure.
Risk	Vulnerability The Nokia Checkpoint Firewall, like all computer/network devices

	have mechanical parts that can wear out over time. Hardware and application failures can render a system unusable and unrecoverable in a timely fashion. As a single point of failure, this could cause significant network availability issues. Threat Source The primary threat sources are operational factors including system component failures (e.g. hard drive, power supply), network component failures (e.g. network interface cards, VPN accelerators), software crashes, and environmental factors that may accelerate or cause hardware failures. Likelihood Likelihood for exposing this vulnerability is considered medium since hardware and software failures do not frequently occur. Potential Outcome Depending on the owner's service contract Nokia hardware can be replaced between 1 and 5 business days. With out hardware redundancy in the form of a dual firewall implementation, actual downtime could last as much as 7 business days. Five days for replacement system to arrive on site. An additional 24-48 hours as the system configuration is brought back to an operational production state, costing considerable financial resources and lost productivity.
Compliance	This control objective is compliant if there is a fully functional secondary firewall operating in standby mode.
Testing	The following test procedures will test for compliance: 1. Review Nokia Firewall redundancy configuration. 2. Test failover capabilities by disrupting network connectivity and power to each system. 3. Monitor application and network connectivity to internal network, wildcard network, DMZ, and the Internet systems.
Analysis	Objective

2.6 Audit Trail, Monitoring, Analysis and Reporting

ATR-1	Check 19 of 21
Description	User access logging
Reference	9, 13, 16, experience
Control Objective	Ensure that user access (Nokia operating system, firewall application, and SecuRemote) attempts are logged and maintained with appropriate level of detail to ensure accountability.

Risk	Vulnerability There is little to no user accountability or audit trial with out appropriate user access logging. Threat Source There are numerous threat sources for this vulnerability including authorized users deliberately or accidentally modifying system configurations and unauthorized users attempting to access system resources. Likelihood Most security related devices and applications log user access, however, these features are highly configurable leaving room for administrator error. Potential Outcome Several adverse outcomes exist including the inability to enforce accountability policies and the inability to trace system changes back to the responsible individuals.
Compliance	This control objective is compliant if the checkpoint firewall access logs indicate user access. The Nokia IPSO operating system must also log all user access attempts.
Testing	For the Checkpoint Firewall Application use the SmartTracker interface tool to 1. Review firewall-1 logs for remote user access. 2. Review audit trail logs for system administrator activity. For the Nokia IPSO operating system either from the Nokia IPSO operating system command line or the Nokia Network Voyager web interface tool: Review all system logs including: • System Message Log • Web Server Access Log • Web Server Error Log • User Login/Logout Activity • Management Activity Log When reviewing user access log data ensure that the following auditable information for each access attempt is recorded • Date and time • User ID • Source and destination address • Success/failure of event
Analysis	Objective

ATR-2	Check 20 of 21
Description	Nokia/Checkpoint network logging
Reference	9, 13, 16, experience
Control Objective	Ensure that network traffic filtered at the firewall is logged and maintained with the appropriate level of detail to assure firewall rulebase performs as expected; alerts are appropriately triggered; and that auditable information for each event is recorded.
Risk	Vulnerability There is little to no accountability or audit trial evidence without an appropriate level of network traffic filtering and firewall logging. Threat Source There are numerous threat sources for this vulnerability including authorized users deliberately or accidentally modifying system configurations and unauthorized users attempting to access system resources. A threat also exists from compromised DMZ systems initiating unauthorized communications to the Internet and the organization's internal and wildcard networks. Likelihood Most network security devices and applications have the capability to log network traffic traversing its network interfaces, however, these features are highly configurable leaving room for error. The likelihood depends on the experience and training of the organization's security administrators and engineers. Potential Outcome Several adverse outcomes exist including the inability to track unusual network activity and provide information to support computer forensic analysis requirements.
Compliance	This control objective is compliant if the logs contain the appropriate level of detail for audit trail purposes.
Testing	The following test procedures will test for compliance: 1. Create network traffic to the Nokia IPSO operating system. 2. Create network traffic to protected systems on the DMZ, wildcard, and internal networks. 3. Create SecuRemote traffic to the checkpoint firewall and internal systems. 4. Review CheckPoint Firewall logs. 5. Review Nokia system and application logs. 6. correlate the firewall logs to the test network traffic.
Analysis	Objective

ATR-3	Check 21 of 21
Description	Log alerts
Reference	13, experience
Control Objective	Ensure that log event alerting features are enabled and functioning properly for the Nokia IPSO operating system and the Checkpoint Firewall application.
Risk	Vulnerability Firewall and security personnel are not aware of serious system and security events. Threat Source All network users inside and outside of the organization attempting to probe and otherwise discover network and system vulnerabilities. System failures and performance warnings are also a threat to system operation if unnoticed. Likelihood Networks and systems are constantly scanned. It is very likely that at some point a unauthorized user will make a concerted effort to probe the network for exploitable vulnerabilities Potential Outcome Repeated attempts at network probing may eventually reveal exploitable vulnerabilities, which may in turn lead to disruption of service or to the modification, destruction, or disclosure of valuable information assets.
Compliance	This control objective is compliant if Nokia IPSO operating system and Checkpoint firewall log event alerting features are configured, enabled, and perform as expected.
Testing	The following test procedures will test for compliance: 1. Review Nokia IPSO operating system logging and alerting configuration. 2. Review firewall logging and alerting configuration. 3. Test alerting capability with network probe attempts from all interfaces of the firewall. 4. Send a test alert from the Nokia IPSO operating system.
Analysis	Objective

3 Assignment 3 – Audit Evidence

The following tools were used during the technical audit activities:

Tool	Version	Purpose	Source
Nmap	2.54BETA31	Port scanning, OS detection	www.insecure.org
Nessus	2.0.7 Plugins 2.0.8.a	Vulnerability scanning	www.nessus.org
SuperScan	4.0	Port scanning	www.foundstone.com
Firewalk	5.0	Access control list testing	www.packetfactory.net
Ethereal	0.9.11	Network analyzer, sniffer	www.ethereal.com
Base64.exe	N/A	Converts binary data to Base64 encoding and vice versa	http://www.rtner.de/software/base64.html

3.1 Audit

PPG-1

Description: Information Security Policies, Procedures, and Guidelines.

Results:
Management and system administration staff were interviewed regarding the following policies, procedures and guidelines and asked to supply supporting documentation for review.

Test #	Control Objective to Test	How Reviewed		Compliant	
		I	D	Yes	No
PPG-1.1	Security Policy	x			x
PPG-1.2	Configuration Management	x			x
PPG-1.3	Backup and Recovery	x			x
PPG-1.4	Patch Management	x			x
PPG-1.5	Configuration Guides	x	x		x
PPG-1.6	Change Control	x			x
PPG-1.7	Firewall Policy	x			x

I-Interview D-Documentation

Assessment:

>>The organization is not compliant with this control objective.

The organization does not have formally documented policies, procedures or guidelines. They are aware of the importance of such items but have not formalized or thoroughly documented the processes. For example, there is a gathering of configuration guides obtained from the Nokia and Checkpoint Knowledge Base web sites. However, the guidelines do not specifically reflect the implemented configuration on the audited system. Patches and updates are applied "as needed", however, there is no formal process for obtaining vulnerability alerts, testing fixes, and implementation. Network diagrams do appear to be up to date, as this is currently a relatively simple network from a logical and physical perspective.

PEN-1

Description: Physical Access to the Nokia Firewall System

Results:
An inspection of the office space including the space housing the firewall and other networking devices was conducted. An actual attempt to subvert physical security was not necessary because the firewall and other networking and computing systems are located in an open office space location. All systems are located on an open-air computer rack within an ordinary office room. Access is relatively unrestricted during normal business hours. A receptionist directs the visitor to the appropriate office space. After normal business hours office building cleaning crews have access to office spaces to empty trash and clean floors.
Appendix B lists questions used during the Physical access discussion.

Assessment:
>>The organization is not compliant with this control objective.
Physical security of the firewall does not exist beyond that provided by a locked office door. The space is accessible by all staff and visitors during normal business hours. The office is locked during off hours; however, cleaning and building maintenance personnel have keys to all offices enabling access during those times.

PEN-2

Description: Power supply

Results:
The physical area containing the firewall was inspected for UPS device installation. It was noted that the Nokia Checkpoint Firewall was plugged into a UPS device that provides the required level of functionality as described below:

- Automatic Voltage Regulation (AVR)
- Building wiring fault indicator
- Replace battery indicator

- Hot swap batteries
- Battery management capabilities
- Overload Indicator
- Status Indicator LEDs

Additionally the site was surveyed for other environmental control technologies and equipment. The following was noted:
-Surge protection power strips
-One fire extinguisher
However, the space did not provide,
-Raised flooring
-Localized cooling system other than that provided by the building for a human work environment.
-Humidity monitor
It was also noted through discussions with the organization's manager that building supplied cooling and heating is curtailed 6:00PM to 6:00AM Monday through Thursday and from 6:00pm Friday to 6:00am Monday.

Appendix B lists questions used during the environmental controls discussion.

Assessment:
>> The organization has a UPS device to protect the Nokia Checkpoint Firewall from voltage spikes and sudden loss of power, and is therefore compliant with the control objective. However, other environmental controls are not adequately implemented to protect against environmental factors that could potentially harm computer systems or mitigate environmental risks such as fires, flooding, and temperature and humidity fluctuations.

SDC-1

Description: Firewall and Network architecture documentation

Results:
The results are based on the testing procedures defined in the SDC-1 checklist item.

Network diagrams were submitted and reviewed.

Results of the discovery scanning activity are below:

```
[root@localhost root]# nmap -sP x.x.b.1-254

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host  (x.x.b.1) appears to be up.
Host  (x.x.b.99) appears to be up.
Host  (x.x.b.102) appears to be up.
Host  (x.x.b.104) appears to be up.
Host  (x.x.b.105) appears to be up.
Host  (x.x.b.106) appears to be up.
```

```
Nmap run completed -- 254 IP addresses (6 hosts up) scanned in 5 seconds


[root@localhost root]# nmap -sP x.x.a.1-254

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host  (x.x.a.1) appears to be up.
Host  (x.x.a.32) appears to be up.
Host  (x.x.a.33) appears to be up.
Host  (x.x.a.34) appears to be up.
Host  (x.x.a.35) appears to be up.
Host  (x.x.a.99) appears to be up.
Host  (x.x.a.101) appears to be up.

Nmap run completed -- 254 IP addresses (7 hosts up) scanned in 6 seconds


[root@localhost root]# nmap -sP x.x.c.1-254

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host  (x.x.c.1) appears to be up.
Host  (x.x.c.2) appears to be up.
Host  (x.x.c.3) appears to be up.
Host  (x.x.c.5) appears to be up.
Host  (x.x.c.6) appears to be up.
Host  (x.x.c.9) appears to be up.
Host  (x.x.c.21) appears to be up.
Host  (x.x.c.111) appears to be up.

Nmap run completed -- 254 IP addresses (8 hosts up) scanned in 15 seconds
```

The supplied network diagram supports the discovery scan on the organization's IP network.

Assessment:
>>The organization is compliant with the control objective.

SDC-3

Description: Nokia IPSO operating system security

Results:
The results are based on the testing procedures defined in the SDC-3 checklist item.

Vulnerability Advisory Search

Vulnerability Name	Short Description	Source	Applicable to Audit System
CERT® Advisory CA-2004-01	Multiple H.323 Message Vulnerabilities	http://www.cert.org/advisories/CA-2004-01.html	NO

CERT® Advisory CA-2003-06	Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP)	http://www.cert.org/nav/index_red.html	NO
CERT® Advisory CA-2002-03	Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)	http://www.cert.org/nav/index_red.html	NO
Bugtraq ID 9020	Nokia IPSO Voyager HTTPDAccessLog.TCL Remote Script injection Vulnerability	http://www.securityfocus.com/bid/9020/info/	**Yes**
Bugtraq ID 8928	Nokia IPSO Unspecified Denial of Service Vulnerability	http://www.securityfocus.com/bid/8928/info/	NO
Bugtraq ID 4089	Multiple Vendor SNMP Request Handling Vulnerabilities	http://www.securityfocus.com/bid/4089	NO
Bugtraq ID 7426	Nokia IPSO Voyager ReadFile.TCL Remote File Reading Vulnerability	http://www.securityfocus.com/bid/7426	NO

Nmap port scanning results are below:

```
root@localhost root]# nmap -v -sU -sT -O -p 1-65535 x.x.c.21

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host  (x.x.c.21) appears to be up ... good.
Initiating Connect() Scan against  (x.x.c.21)
Adding open port 18208/tcp
Adding open port 18196/tcp
Adding open port 18191/tcp
Adding open port 80/tcp
Adding open port 23/tcp
The Connect() Scan took 41 seconds to scan 65535 ports.
Initiating UDP Scan against  (x.x.c.21)
The UDP Scan took 326 seconds to scan 65535 ports.
Adding open port 514/udp
Adding open port 1024/udp
Adding open port 161/udp
For OSScan assuming that port 23 is open and port 1 is closed and neither are
firewalled
Interesting ports on  (x.x.c.21):
(The 131062 ports scanned but not shown below are in state: closed)
Port       State       Service
23/tcp     open        telnet
80/tcp     open        http
161/udp    open        snmp
514/udp    open        syslog
1024/udp   open        unknown
18191/tcp  open        unknown
18196/tcp  open        unknown
18208/tcp  open        unknown

Remote operating system guess: NOKIA IPSO 3.2 Running Checkpoint Firewall-1
Uptime 0.127 days (since Sat Nov 8 05:02:58 2003)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=36098 (Worthy challenge)
IPID Sequence Generation: Incremental
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 368 seconds
[root@localhost root]#
```

Nessus vulnerability scanning results are below:

```
Nessus Scan Report
------------------

SUMMARY

 - Number of hosts which were alive during the test: 1
 - Number of security holes found: 5
 - Number of security warnings found: 9
 - Number of security notes found: 7

TESTED HOSTS

 x.x.c.21 (Security holes found)

DETAILS

+ x.x.c.21:
 . List of open ports:
    o telnet (23/tcp) (Security warnings found)
    o http (80/tcp) (Security hole found)
    o snmp (161/udp)
    o syslog (514/udp)
    o unknown (1024/udp)
    o unknown (18191/tcp)
    o unknown (18196/tcp)
    o unknown (18208/tcp)
    o general/tcp (Security warnings found)
    o general/udp (Security notes found)
    o general/icmp (Security warnings found)

 . Warning found on port telnet (23/tcp)

    The Telnet service is running.
    This service is dangerous in the sense that it is not ciphered - that is,
    everyone can sniff the data that passes between the telnet client and the
    telnet server. This includes logins and passwords.

    You should disable this service and use OpenSSH instead. (www.openssh.com)

    Solution: Comment out the 'telnet' line in /etc/inetd.conf.

    Risk factor : Low
    CVE: CAN-1999-0619

 . Information found on port telnet (23/tcp)

    A telnet server seems to be running on this port

 . Information found on port telnet (23/tcp)

    Remote telnet banner:

 . Vulnerability found on port http (80/tcp) :
    The remote host is using a version of mod_ssl which is older than 2.8.10.

    This version is vulnerable to an off by one buffer overflow which may allow
    a user with write access to .htaccess files to execute arbitrary code on
    the system with permissions of the web server.

    *** Note that several Linux distributions (such as RedHat)
    *** patched the old version of this module. Therefore, this
    *** might be a false positive. Please check with your vendor
    *** to determine if you really are vulnerable to this flaw

    Solution: Upgrade to version 2.8.10 or newer
    Risk factor: High
    CVE: CVE-2002-0653
    BID: 5084

 . Vulnerability found on port http (80/tcp):

    The remote host appears to be running a version of Apache which is older
    than 1.3.28

    There are several flaws in this version, which may allow an attacker to
    disable the remote server remotely. You should upgrade to 1.3.28 or newer.

    *** Note that Nessus solely relied on the version number
    *** of the remote server to issue this warning. This might
    *** be a false positive

    Solution: Upgrade to version 1.3.28
    See also: http://www.apache.org/dist/httpd/Announcement.html
    Risk factor: High
    CVE: CAN-2003-0460
    BID: 8226

 . Vulnerability found on port http (80/tcp):

    The remote host is using a version of mod_ssl which is older than 2.8.7.

    This version is vulnerable to a buffer overflow which, albeit difficult to
    exploit, may allow an attacker to obtain a shell on this host.

    *** Some vendors patched older versions of mod_ssl, so this
    *** might be a false positive. Check with your vendor to determine
    *** if you have a version of mod_ssl that is patched for this
    *** vulnerability


    Solution: Upgrade to version 2.8.7 or newer
    Risk factor: High
    CVE: CVE-2002-0082
    BID: 4189

 . Vulnerability found on port http (80/tcp):

    The remote web server seems to be vulnerable to the Cross Site Scripting
    vulnerability. The vulnerability is caused by the result returned to the
    user when a non-existing file is requested (e.g. the result contains the
    JavaScript provided in the request).

    The vulnerability would allow an attacker to make the server present the
    user with the attacker's JavaScript/HTML code. Since the content is
    presented by the server, the user will give it the trust level of the
```

```
   server (for example, the trust level of banks, shopping centers, etc. would
   usually be high).

   Risk factor: Medium

   Solution: Upgrade to the latest version of WebSphere

   BID: 2401

. Vulnerability found on port http (80/tcp):

   The remote host has the CGI 'hpnst.exe' installed.

   Older versions of this CGI (pre 5.55) are vulnerable to a denial of service
   attack where the user can make the CGI request itself.

   Solution: upgrade to version 5.55
   Risk factor: High
   CVE: CAN-2003-0169

. Warning found on port http (80/tcp)

   The remote Checkpoint Firewall is open to Web administration.

   An attacker use it to launch a brute force password attack against the
   firewall, and eventually take control of it.

   Solution: Disable remote Web administration or filter packets going to this
   port

   Risk factor : Medium

. Warning found on port http (80/tcp)

   The remote host is using a version of OpenSSL which is older than 0.9.6j or
   0.9.7b

   This version is vulnerable to a timing based attack which may allow an
   attacker to guess the content of fixed data blocks and may eventually be
   able to guess the value of the private RSA key of the server.

   An attacker may use this implementation flaw to sniff the data going to
   this host and decrypt some parts of it, as well as impersonate your server
   and perform man in the middle attacks.

   *** Nessus solely relied on the banner of the remote host
   *** to issue this warning

   See also: http://www.openssl.org/news/secadv_20030219.txt
   http://lasecwww.epfl.ch/memo_ssl.shtml
   http://eprint.iacr.org/2003/052/

   Solution: Upgrade to version 0.9.6j (0.9.7b) or newer
   Risk factor: Medium
   CVE: CAN-2003-0078, CAN-2003-0131
   BID: 6884, 7148

. Warning found on port http (80/tcp)

   Your webserver supports the TRACE and/or TRACK methods. It has been shown
   that servers supporting this method are subject to cross-site-scripting
   attacks, dubbed XST for 'Cross-Site-Tracing', when used in conjunction with
   various weaknesses in browsers.
   An attacker may use this flaw to trick your legitimate web users to give
   him their credentials.

   Solution: Disable these methods.


   If you are using Apache, add the following lines for each virtual host in
   your configuration file:

   RewriteEngine on
   RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
   RewriteRule .* - [F]

   If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE
   requests or to permit only the methods needed to meet site requirements and
   policy.

   See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf
   http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html

   Risk factor: Medium

. Warning found on port http (80/tcp)

   The remote host appears to be running a version of Apache which is older
   than 1.3.27

   There are several flaws in this version, you should upgrade to 1.3.27 or
   newer.

   *** Note that Nessus solely relied on the version number
   *** of the remote server to issue this warning. This might
   *** be a false positive

   Solution: Upgrade to version 1.3.27
   See also: http://www.apache.org/dist/httpd/Announcement.html
   Risk factor: Medium
   CVE: CAN-2002-0839, CAN-2002-0840, CAN-2002-0843
   BID: 5847, 5884, 5995, 5996

. Warning found on port http (80/tcp)

   The remote host is using a version of mod_ssl which is older than 2.8.10.

   This version is vulnerable to a flaw which may allow an attacker to
   successfully perform a cross site scripting attack under some
   circumstances.

   *** Note that several Linux distributions (such as RedHat)
   *** patched the old version of this module. Therefore, this
   *** might be a false positive. Please check with your vendor
   *** to determine if you really are vulnerable to this flaw

   Solution: Upgrade to version 2.8.10 or newer
   Risk factor: Low
   CVE: CAN-2002-1157
   BID: 6029

. Information found on port http (80/tcp)

   A web server is running on this port
```

```
 . Information found on port http (80/tcp)

    The remote web server type is:

    Apache/1.3.6 (Unix) mod_auth_pam/1.0a mod_ssl/2.3.11 OpenSSL/0.9.5a

    Solution: You can set the directive 'ServerTokens Prod' to limit the
    information emanating from the server in its response headers.

 . Warning found on port general/tcp

    The remote host does not discard TCP SYN packets which have the FIN flag
    set.

    Depending on the kind of firewall you are using, an attacker may use this
    flaw to bypass its rules.

    See also: http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html
    http://www.kb.cert.org/vuls/id/464113

    Solution: Contact your vendor for a patch
    Risk factor: Medium
    BID: 7487

 . Information found on port general/tcp

    Nmap found that this host is running NOKIA IPSO 3.2 Running Checkpoint
    Firewall-1

. Information found on port general/tcp

    Remote OS guess: Nokia IPSO 3.2-3.5 Running Checkpoint Firewall-1 or NG FP2

    CVE: CAN-1999-0454

 . Information found on port general/udp

    For your information, here is the traceroute to x.x.c.21:
    x.x.c.21

 . Warning found on port general/icmp

    The remote host answers to an ICMP timestamp request. This allows an
    attacker to know the date which is set on your machine.

    This may help him to defeat all your time based authentication protocols.

    Solution: filter out the ICMP timestamp requests (13), and the outgoing
    ICMP timestamp replies (14).

    Risk factor: Low
    CVE: CAN-1999-0524

 . Warning found on port general/icmp

    The remote host answered to an ICMP_MASKREQ query and sent us its netmask
    (255.255.255.0)

    An attacker can use this information to understand how your network is set
    up and how the routing is done. This may help him to bypass your filters.

    Solution: reconfigure the remote host so that it does not answer to those
    requests. Set up filters that deny ICMP packets of type 17.
```

```
     Risk factor: Low
     CVE: CAN-1999-0524

-------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Port to service mapping:

Port	Service	Purpose/Function
23/tcp	telnet	Remote administration
80/tcp	http	Remote administration, Nokia Network Voyager interface
161/udp	snmp	Simple network management protocol. Not used in the current environment.
514/udp	syslog	System logging server. Not used in the current environment.
1024/udp	Reserved	Unknown purpose or function
18191/tcp	CPD	Check Point Daemon Protocol - Download of rulebase from MM to FWM - Fetching rulebase from FWM to MM when starting
18196/tcp	Undefined	Undefined Checkpoint service port
18208/tcp	FW1_CPRID	Check Point Remote Installation Protocol - Protocol used from MM to FWM when installing Secure Updates.

Note: Port number service and purpose/function were based on information obtained from the following sites:

- http://www.iana.org/assignments/port-numbers
- http://www.fw-1.de/aerasec/ng/ports-ng.html

Assessment:

>>The organization is not compliant with this control objective.

Vulnerability advisory web search revealed that the installed version of Nokia IPSO operating system is vulnerable to a web based attack via the Nokia network voyager web interface tool. The full text of the vulnerability description is below:

> *Nokia IPSO is a security operating system for Nokia and partner security applications. Nokia IPSO could allow a remote attacker to view files on the system. A remote attacker with access to the Web-based Voyager management interface could send a specially-crafted URL request to the readfile.tcl script to view files on the system for which the attacker has read permissions.*

Nmap scanning revealed that telnet, http, snmp, syslog and several Checkpoint Firewall NG ports are open.

Nessus security scanning revealed that several open application ports were vulnerable to specific attack methods including cross-site-scripting, timing based attacks, brute force password attacks, and password capture.

The Nokia IPSO operating system is vulnerable to several types of network-based attacks when the firewall software is disabled. This could be the case during system maintenance and troubleshooting activities. IP forwarding is disabled when the firewall application is disabled, however, IP forwarding can be re-enabled at the Nokia operating system command line, exposing internal systems to attack.

SDC-4

Description: Firewall application security

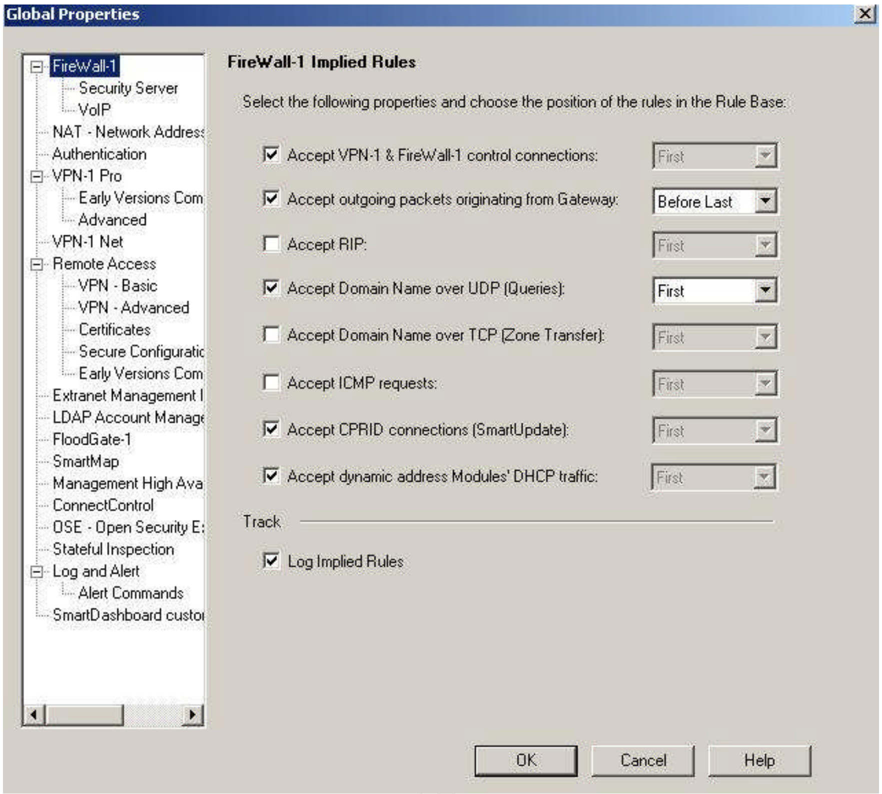
Results:
The results are based on the testing procedures defined in the SDC-4 checklist item.

The $FWDIR/conf/gui-client file contained the appropriate client IP address information.

The $FWDIR/conf/fwmusers file indicates one firewall administrator account.

The following screenshots represent the implemented firewall properties and rules protecting the Nokia Checkpoint Firewall.

Below is the Global Properties configuration interface.



FireWall-1 Implied Rules

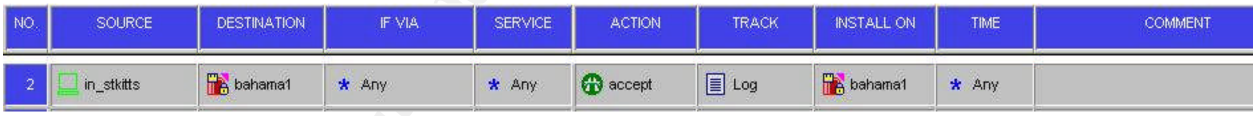
Select the following properties and choose the position of the rules in the Rule Base:

☑ Accept VPN-1 & FireWall-1 control connections:	First
☑ Accept outgoing packets originating from Gateway:	Before Last
□ Accept RIP:	First
☑ Accept Domain Name over UDP (Queries):	First
□ Accept Domain Name over TCP (Zone Transfer):	First
□ Accept ICMP requests:	First
☑ Accept CPRID connections (SmartUpdate):	First
☑ Accept dynamic address Modules' DHCP traffic:	First

Track

☑ Log Implied Rules

Below is the firewall rule permitting access to the firewall module for remote management purposes.



NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
2	in_stkitts	bahama1	* Any	* Any	accept	Log	bahama1	* Any	

Vulnerability Database search results:

Vulnerability Name	Short Description	Source	Applicable to Audit System
CERT[®] Advisory CA-2001-17	Check Point RDP Bypass Vulnerability	http://www.cert.org/advisories/CA-2001-17.html	NO
Bugtraq ID 8524	Check Point Firewall-1 SecuRemote Internal Interface Address Information Leakage Vulnerability	http://www.securityfocus.com/bid/8524	NO
Bugtraq ID 7161	Check Point FW-1 Syslog Daemon Unfiltered Escape Sequence Vulnerability	http://www.securityfocus.com/bid/7161	YES

Bugtraq ID 7159	Check Point VPN-1/Firewall-1 Remote Syslog Data Resource Consumption Vulnerability	http://www.securityfocus.com/bid/7159	YES
Bugtraq ID 4131	Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability	http://www.securityfocus.com/bid/4131	NO
Bugtraq ID 5920	Check Point VPN-1 IKE Aggressive Mode Forcing Vulnerability	http://www.securityfocus.com/bid/5920	NO
Additional Checkpoint Firewall vulnerabilities dating back to 6/1/99 were noted and found not applicable to the Checkpoint Firewall operating in this environment.			

In normal interactions with the Nokia Checkpoint Firewall from a trusted management client host, the following ports, protocols, and services are utilized (as indicated by ethereal network sniffer captures).

Application	Port	Protocol	Service	Purpose/Use
Internet Explorer	80	TCP	HTTP	Used to remotely access the Nokia Network Voyager web-based IPSO operating system configuration tool.
Telnet	23	TCP	Telnet	Used to remotely manage and configure the IPSO operating system
CheckPoint Management Clients (SmartDashboard)	18190	TCP	CPMI	Used for communication between Management Clients (SmartDashboard GUI) and the CheckPoint Management Module.

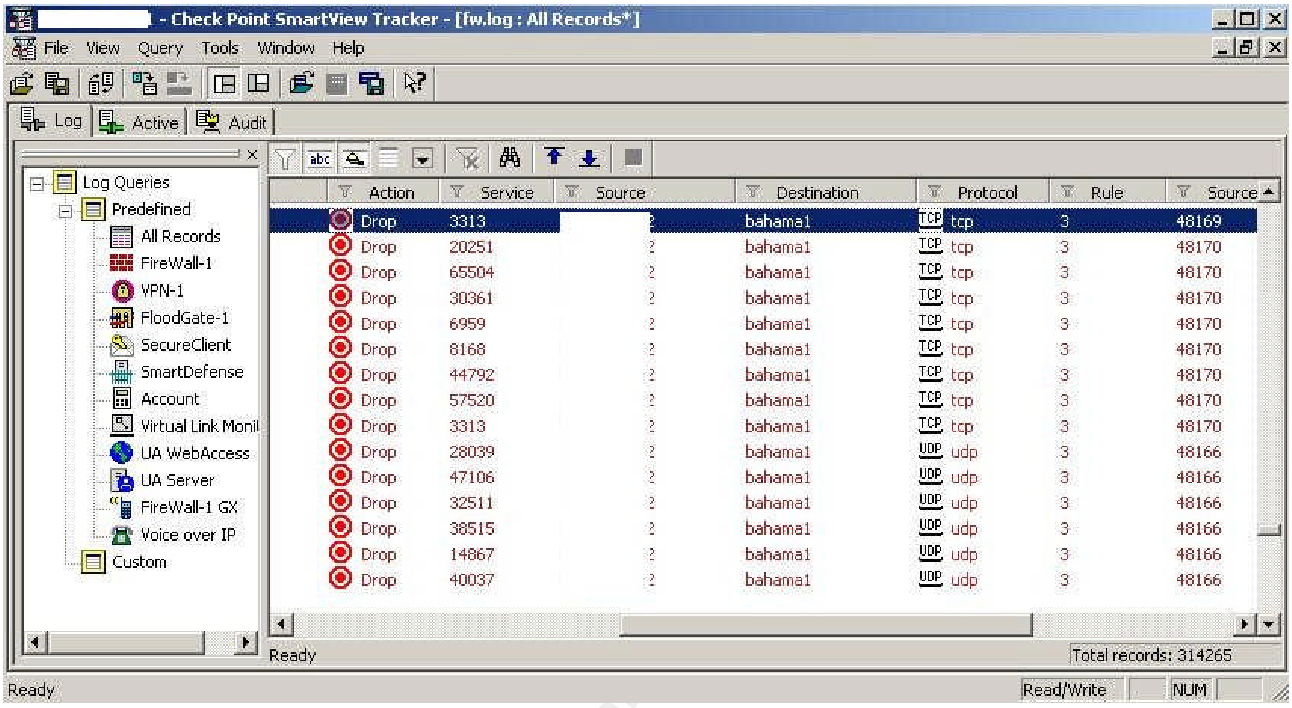
Note: Port number service and purpose/function were based on information obtained from the following sites:

- http://www.iana.org/assignments/port-numbers
- http://www.fw-1.de/aerasec/ng/ports-ng.html

Nmap scan results from an untrusted host are below:

```
[root@localhost root]# nmap -v -P0 -sU -sS -O -p 1-65535 x.x.c.21

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host  (x.x.c.21) appears to be up ... good.
Initiating SYN Stealth Scan against  (x.x.c.21)
Adding open port 264/tcp
Adding open port 18264/tcp
The SYN Stealth Scan took 8835 seconds to scan 65535 ports.
Initiating UDP Scan against  (x.x.c.21)
The UDP Scan took 4063 seconds to scan 65535 ports.
Adding open port 1252/udp
Adding open port 52276/udp
Adding open port 57011/udp
Adding open port 33588/udp
Adding open port 41014/udp
*
*
*
Adding open port 56807/udp
Adding open port 44040/udp
Adding open port 44943/udp
Adding open port 50966/udp
Adding open port 55120/udp
Adding open port 13013/udp
Adding open port 16789/udp
Adding open port 63775/udp
Adding open port 41400/udp
Adding open port 28535/udp
Adding open port 36355/udp
(no udp responses received -- assuming all ports filtered)
For OSScan assuming that port 264 is open and port 500 is closed and neither
are firewalled
For OSScan assuming that port 264 is open and port 500 is closed and neither
are firewalled
For OSScan assuming that port 264 is open and port 500 is closed and neither
are firewalled
Interesting ports on  (x.x.c.21):
(The 131066 ports scanned but not shown below are in state: filtered)
Port       State       Service
264/tcp    open        bgmp
500/tcp    closed      isakmp
18262/tcp  closed      unknown
18264/tcp  open        unknown

No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=2.54BETA31%P=i386-redhat-linux-gnu%D=11/8%Time=3FAD4148%O=264%C=500)
TSeq(Class=RI%gcd=1%SI=9E42%IPID=I%TS=2HZ)
TSeq(Class=RI%gcd=1%SI=D164%IPID=I%TS=2HZ)
TSeq(Class=RI%gcd=1%SI=9EC1%IPID=I%TS=2HZ)
T1(Resp=Y%DF=N%W=4000%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)


Uptime 0.385 days (since Sat Nov  8 05:02:55 2003)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=40641 (Worthy challenge)
IPID Sequence Generation: Incremental


Nmap run completed -- 1 IP address (1 host up) scanned in 12919 seconds
[root@localhost root]#
```

Firewall Log screenshot during nmap scanning from untrusted host:

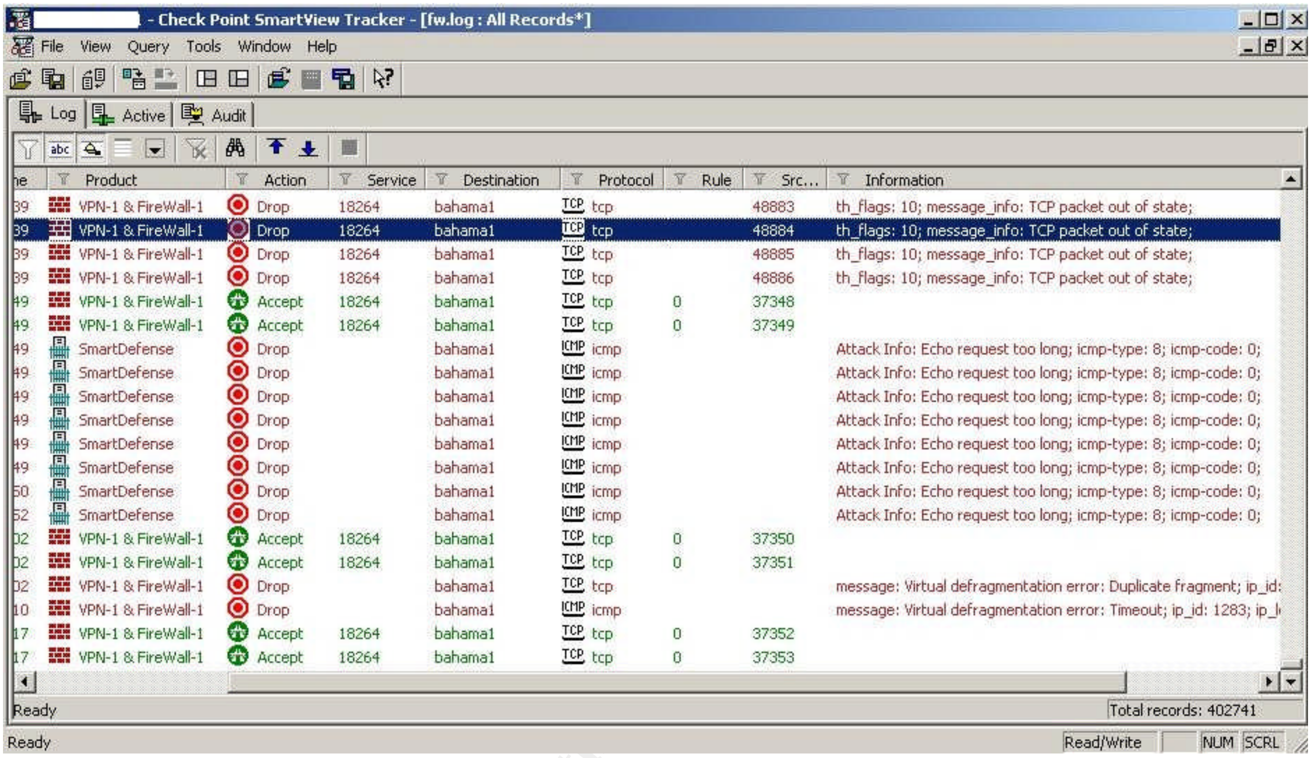


Action	Service	Source	Destination	Protocol	Rule	Source
Drop	3313	[redacted]	bahama1	tcp	3	48169
Drop	20251	[redacted]	bahama1	tcp	3	48170
Drop	65504	[redacted]	bahama1	tcp	3	48170
Drop	30361	[redacted]	bahama1	tcp	3	48170
Drop	6959	[redacted]	bahama1	tcp	3	48170
Drop	8168	[redacted]	bahama1	tcp	3	48170
Drop	44792	[redacted]	bahama1	tcp	3	48170
Drop	57520	[redacted]	bahama1	tcp	3	48170
Drop	3313	[redacted]	bahama1	tcp	3	48170
Drop	28039	[redacted]	bahama1	udp	3	48166
Drop	47106	[redacted]	bahama1	udp	3	48166
Drop	32511	[redacted]	bahama1	udp	3	48166
Drop	38515	[redacted]	bahama1	udp	3	48166
Drop	14867	[redacted]	bahama1	udp	3	48166
Drop	40037	[redacted]	bahama1	udp	3	48166

Nessus vulnerability scanning results from an untrusted host are below.

```
Nessus Scan Report
------------------

SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found: 1
 - Number of security warnings found: 0
 - Number of security notes found: 4

TESTED HOSTS

 x.x.c.21 (Security holes found)

DETAILS

+ x.x.c.21 :
 . List of open ports:
     o unknown (18264/tcp) (Security hole found)
     o rap (256/udp)
     o isakmp (500/udp)
     o unknown (18262/udp)
     o unknown (18264/udp)
     o general/tcp (Security notes found)
     o general/udp (Security notes found)

 . Vulnerability found on port unknown (18264/tcp) :

     The remote host appears to be vulnerable to the Apache Web Server Chunk
     Handling Vulnerability.
     If Safe Checks are enabled, this may be a false positive since it is based
     on the version of Apache.  Although unpatched Apache versions 1.2.2 and
     above, 1.3 through 1.3.24 and 2.0 through 2.0.36, the remote server may be
     running a patched version of Apache

     Solution: Upgrade to version 1.3.26 or 2.0.39 or newer See also:
     http://httpd.apache.org/info/security_bulletin_20020617.txt
     http://httpd.apache.org/info/security_bulletin_20020620.txt
     Risk factor: High
     CVE: CVE-2002-0392
     BID: 5033

 . Information found on port unknown (18264/tcp)

     A web server is running on this port

 . Information found on port unknown (18264/tcp)

     The remote web server type is:

     Check Point SVN foundation/NG FP2

     Solution: We recommend that you configure (if possible) your web server to
     return a bogus Server header in order to not leak information.

 . Information found on port general/tcp

     Remote OS guess: Nokia IPSO 3.6 running CheckPoint FW-1 NG FP2

     CVE: CAN-1999-0454

 . Information found on port general/udp

     For your information, here is the traceroute to x.x.c.21 :
     x.x.c.21

------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Firewall log screenshot during Nessus vulnerability scanning:



[redacted] - Check Point SmartView Tracker - [fw.log : All Records*]
File View Query Tools Window Help
Log
Active
Audit

he	Product	Action	Service	Destination	Protocol	Rule	Src...	Information
39	VPN-1 & FireWall-1	Drop	18264	bahama1	tcp		48883	th_flags: 10; message_info: TCP packet out of state;
39	VPN-1 & FireWall-1	Drop	18264	bahama1	tcp		48884	th_flags: 10; message_info: TCP packet out of state;
39	VPN-1 & FireWall-1	Drop	18264	bahama1	tcp		48885	th_flags: 10; message_info: TCP packet out of state;
39	VPN-1 & FireWall-1	Drop	18264	bahama1	tcp		48886	th_flags: 10; message_info: TCP packet out of state;
49	VPN-1 & FireWall-1	Accept	18264	bahama1	tcp	0	37348	
49	VPN-1 & FireWall-1	Accept	18264	bahama1	tcp	0	37349	
49	SmartDefense	Drop		bahama1	icmp			Attack Info: Echo request too long; icmp-type: 8; icmp-code: 0;
49	SmartDefense	Drop		bahama1	icmp			Attack Info: Echo request too long; icmp-type: 8; icmp-code: 0;
49	SmartDefense	Drop		bahama1	icmp			Attack Info: Echo request too long; icmp-type: 8; icmp-code: 0;
49	SmartDefense	Drop		bahama1	icmp			Attack Info: Echo request too long; icmp-type: 8; icmp-code: 0;
49	SmartDefense	Drop		bahama1	icmp			Attack Info: Echo request too long; icmp-type: 8; icmp-code: 0;
49	SmartDefense	Drop		bahama1	icmp			Attack Info: Echo request too long; icmp-type: 8; icmp-code: 0;
50	SmartDefense	Drop		bahama1	icmp			Attack Info: Echo request too long; icmp-type: 8; icmp-code: 0;
52	SmartDefense	Drop		bahama1	icmp			Attack Info: Echo request too long; icmp-type: 8; icmp-code: 0;
02	VPN-1 & FireWall-1	Accept	18264	bahama1	tcp	0	37350	
02	VPN-1 & FireWall-1	Accept	18264	bahama1	tcp	0	37351	
02	VPN-1 & FireWall-1	Drop		bahama1	tcp			message: Virtual defragmentation error: Duplicate fragment; ip_id:
10	VPN-1 & FireWall-1	Drop		bahama1	icmp			message: Virtual defragmentation error: Timeout; ip_id: 1283; ip_l
17	VPN-1 & FireWall-1	Accept	18264	bahama1	tcp	0	37352	
17	VPN-1 & FireWall-1	Accept	18264	bahama1	tcp	0	37353	

Port to service mapping for untrusted host:

Port	Service	Purpose/Function
264/tcp	FW1_topo	Check Point VPN-1 SecuRemote Topology Requests - Topology Download for SR (build 4100 and higher) and SCI
500/tcp	isakmp	ISAKMP, Internet Security Association and Key Management Protocol, defines procedures and packet formats to establish, negotiate, modify and delete Security Associations. http://www.networksorcery.com/enp/protocol/isakmp.htm
18262/tcp	CP_Exnet_PK	Check Point Extrnet public key advertisement - Protocol for exchange of public keys when configuring Extranet
18264/tcp	FW1_ica_services	Check Point Internal CA Fetch CRL and User Registration Services - Protocol for Certificate Revocation Lists and registering users when using the Policy Server - needed when e.g. FWM is starting

Note: Port number service and purpose/function were based on information obtained from the following sites:

- http://www.iana.org/assignments/port-numbers

- http://www.fw-1.de/aerasec/ng/ports-ng.html

The following test results were obtained by running the same nmap and nessus scans from a trusted host. In this environment the trusted host is the internal firewall management client workstation. For this test a host object was created for the scanning host.

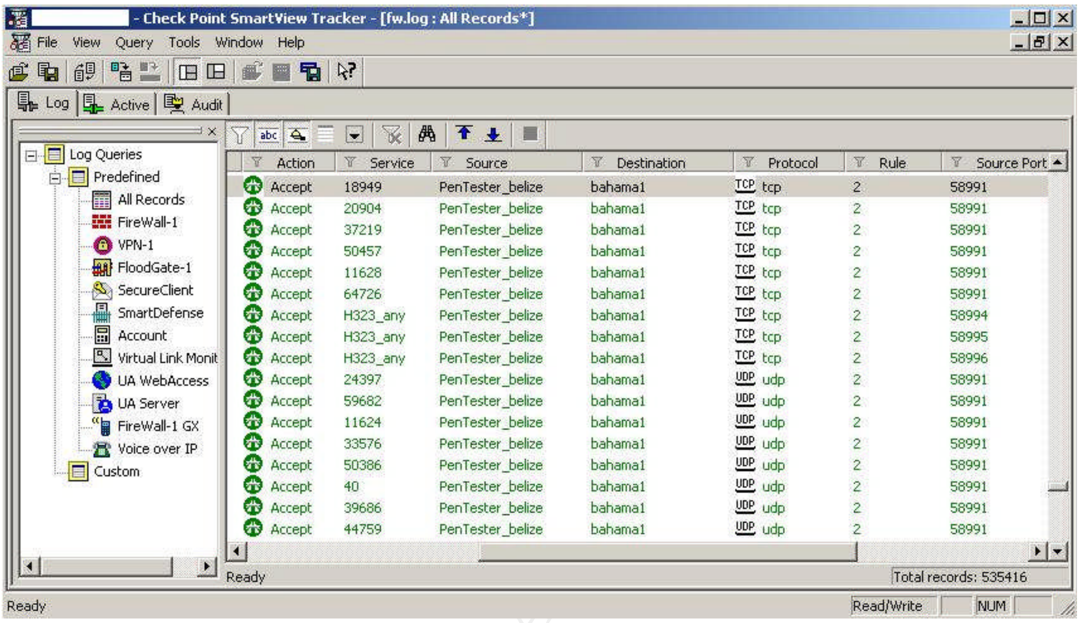
The following nmap scan is from a trusted host to the firewall:

```
[root@localhost root]# nmap -v -P0 -sU -sS -O -p 1-65535 x.x.a.1

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host  (x.x.a.1) appears to be up ... good.
Initiating SYN Stealth Scan against  (x.x.a.1)
Adding open port 80/tcp
Adding open port 262/tcp
Adding open port 18208/tcp
Adding open port 18191/tcp
Adding open port 18209/tcp
Adding open port 18264/tcp
Adding open port 264/tcp
Adding open port 18184/tcp
Adding open port 256/tcp
Adding open port 23/tcp
Adding open port 18183/tcp
Adding open port 1032/tcp
Adding open port 259/tcp
Adding open port 1034/tcp
Adding open port 18187/tcp
Adding open port 1033/tcp
Adding open port 257/tcp
Adding open port 1035/tcp
Adding open port 18190/tcp
Adding open port 18192/tcp
Adding open port 18210/tcp
Adding open port 1031/tcp
Adding open port 18221/tcp
Adding open port 18196/tcp
Adding open port 1036/tcp
Adding open port 900/tcp
The SYN Stealth Scan took 104 seconds to scan 65535 ports.
Initiating UDP Scan against  (x.x.a.1)
The UDP Scan took 325 seconds to scan 65535 ports.
Adding open port 161/udp
Adding open port 53/udp
Adding open port 514/udp
Adding open port 18234/udp
Adding open port 18233/udp
Adding open port 1701/udp
Adding open port 1024/udp
Adding open port 2746/udp
Adding open port 259/udp
Adding open port 500/udp
Adding open port 68/udp
For OSScan assuming that port 23 is open and port 1 is closed and neither are
firewalled
For OSScan assuming that port 23 is open and port 1 is closed and neither are
firewalled
For OSScan assuming that port 23 is open and port 1 is closed and neither are
firewalled
```

```
Interesting ports on  (x.x.a.1):
(The 131032 ports scanned but not shown below are in state: closed)
Port       State       Service
23/tcp     open        telnet
53/udp     open        domain
68/udp     open        dhcpclient
80/tcp     open        http
161/udp    open        snmp
256/tcp    open        rap
257/tcp    open        set
259/tcp    open        esro-gen
259/udp    open        firewall1-rdp
262/tcp    open        arcisdms
264/tcp    open        bgmp
500/udp    open        isakmp
514/udp    open        syslog
900/tcp    open        unknown
1024/udp   open        unknown
1031/tcp   open        iad2
1032/tcp   open        iad3
1033/tcp   open        netinfo
1034/tcp   open        unknown
1035/tcp   open        unknown
1036/tcp   open        unknown
1701/udp   open        unknown
1720/tcp   filtered    unknown
2746/udp   open        unknown
18183/tcp  open        unknown
18184/tcp  open        unknown
18187/tcp  open        unknown
18190/tcp  open        unknown
18191/tcp  open        unknown
18192/tcp  open        unknown
18196/tcp  open        unknown
18208/tcp  open        unknown
18209/tcp  open        unknown
18210/tcp  open        unknown
18221/tcp  open        unknown
18233/udp  open        unknown
18234/udp  open        unknown
18264/tcp  open        unknown

No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=2.54BETA31%P=i386-redhat-linux-gnu%D=1/4%Time=3FF82ADA%O=23%C=1)
TSeq(Class=RI%gcd=1%SI=AFB8%IPID=I%TS=2HZ)
TSeq(Class=RI%gcd=1%SI=6B2B%IPID=I%TS=2HZ)
TSeq(Class=RI%gcd=1%SI=B1C6%IPID=I%TS=2HZ)
T1(Resp=Y%DF=N%W=4000%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=Y%DF=N%TOS=E0%IPLEN=164%RIPTL=148%RID=E%RIPCK=E%UCK=0%ULEN=134%DAT=E)


Uptime 0.109 days (since Sun Jan  4 07:24:58 2004)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=45510 (Worthy challenge)
IPID Sequence Generation: Incremental
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 446 seconds
[root@localhost root]#
```

Firewall Log screenshot during nmap scanning:



Action	Service	Source	Destination	Protocol	Rule	Source Port
Accept	18949	PenTester_belize	bahama1	TCP tcp	2	58991
Accept	20904	PenTester_belize	bahama1	TCP tcp	2	58991
Accept	37219	PenTester_belize	bahama1	TCP tcp	2	58991
Accept	50457	PenTester_belize	bahama1	TCP tcp	2	58991
Accept	11628	PenTester_belize	bahama1	TCP tcp	2	58991
Accept	64726	PenTester_belize	bahama1	TCP tcp	2	58991
Accept	H323_any	PenTester_belize	bahama1	TCP tcp	2	58994
Accept	H323_any	PenTester_belize	bahama1	TCP tcp	2	58995
Accept	H323_any	PenTester_belize	bahama1	TCP tcp	2	58996
Accept	24397	PenTester_belize	bahama1	UDP udp	2	58991
Accept	59682	PenTester_belize	bahama1	UDP udp	2	58991
Accept	11624	PenTester_belize	bahama1	UDP udp	2	58991
Accept	33576	PenTester_belize	bahama1	UDP udp	2	58991
Accept	50386	PenTester_belize	bahama1	UDP udp	2	58991
Accept	40	PenTester_belize	bahama1	UDP udp	2	58991
Accept	39686	PenTester_belize	bahama1	UDP udp	2	58991
Accept	44759	PenTester_belize	bahama1	UDP udp	2	58991

Ready

Total records: 535416

Nessus vulnerability scanning results from a trusted host are below.

```
Nessus Scan Report
------------------

SUMMARY

 - Number of hosts which were alive during the test: 1
 - Number of security holes found: 6
 - Number of security warnings found: 7
 - Number of security notes found: 10

TESTED HOSTS

 x.x.a.1 (Security holes found)

DETAILS

+ x.x.a.1 :
 . List of open ports:
   o telnet (23/tcp) (Security notes found)
   o http (80/tcp) (Security hole found)
   o rap (256/tcp)
   o set (257/tcp)
   o esro-gen (259/tcp)
   o arcisdms (262/tcp) (Security notes found)
   o bgmp (264/tcp)
   o unknown (900/tcp)
   o iad2 (1031/tcp)
   o iad3 (1032/tcp)
```

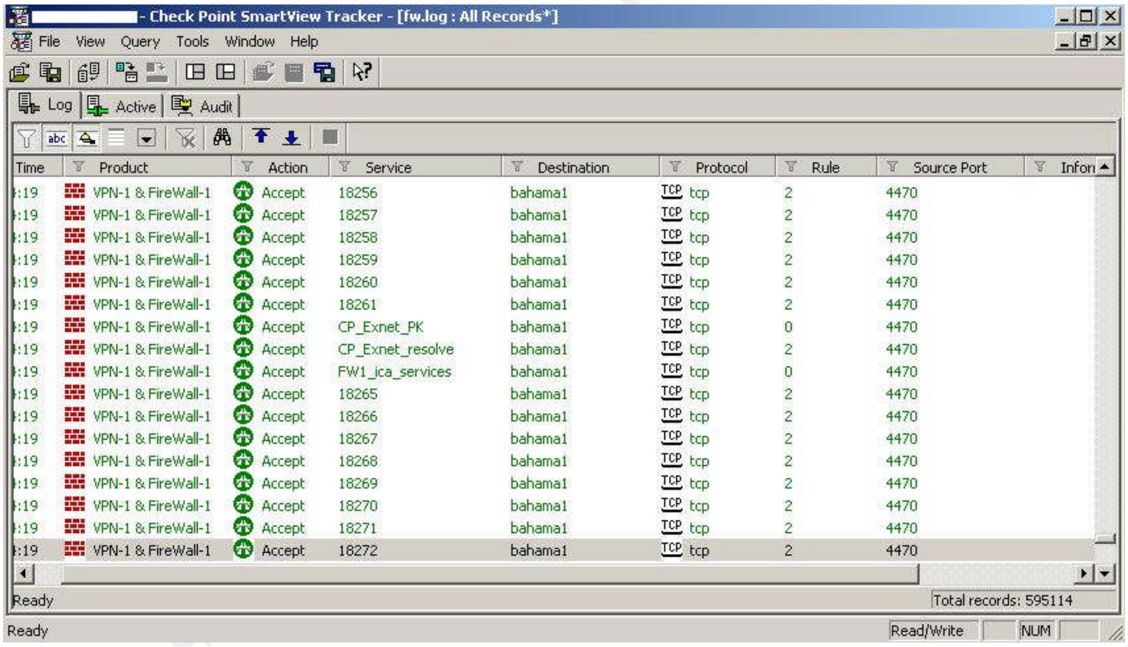
```
  o netinfo (1033/tcp)
  o unknown (1034/tcp)
  o unknown (1035/tcp)
  o unknown (1036/tcp)
  o unknown (18183/tcp)
  o unknown (18184/tcp)
  o unknown (18187/tcp)
  o unknown (18190/tcp)
  o unknown (18191/tcp)
  o unknown (18192/tcp)
  o unknown (18196/tcp)
  o unknown (18208/tcp)
  o unknown (18209/tcp) (Security notes found)
  o unknown (18210/tcp)
  o unknown (18221/tcp)
  o unknown (18264/tcp) (Security hole found)
  o domain (53/udp)
  o bootpc (68/udp)
  o snmp (161/udp)
  o firewall1-rdp (259/udp)
  o isakmp (500/udp)
  o syslog (514/udp)
  o unknown (1024/udp)
  o l2tp (1701/udp)
  o unknown (2746/udp)
  o unknown (18233/udp)
  o unknown (18234/udp)
  o general/tcp (Security notes found)
  o general/udp (Security notes found)
  o general/icmp (Security warnings found)

. Information found on port telnet (23/tcp)


   A telnet server seems to be running on this port

. Information found on port telnet (23/tcp)


   Remote telnet banner:


. Vulnerability found on port http (80/tcp):



  The remote host is using a version of mod_ssl which is older than 2.8.10.

  This version is vulnerable to an off by one buffer overflow which may allow
  a user with write access to .htaccess files to execute arbitrary code on the
  system with permissions of the web server.

      *** Note that several Linux distributions (such as RedHat)
      *** patched the old version of this module. Therefore, this
      *** might be a false positive. Please check with your vendor
      *** to determine if you really are vulnerable to this flaw

      Solution: Upgrade to version 2.8.10 or newer
      Risk factor: High
      CVE: CVE-2002-0653
      BID: 5084

. Vulnerability found on port http (80/tcp) :
  The remote host appears to be running a version of Apache which is older
  than 1.3.28

  There are several flaws in this version, which may allow an attacker to
  disable the remote server remotely.

  You should upgrade to 1.3.28 or newer.

      *** Note that Nessus solely relied on the version number
      *** of the remote server to issue this warning. This might
      *** be a false positive

  Solution : Upgrade to version 1.3.28
  See also : http://www.apache.org/dist/httpd/Announcement.html
  Risk factor : High
  CVE : CAN-2003-0460
  BID : 8226

. Vulnerability found on port http (80/tcp) :


  The remote host is using a version of mod_ssl which is older than 2.8.7.

  This version is vulnerable to a buffer overflow which, albeit difficult to
  exploit, may allow an attacker to obtain a shell on this host.

      *** Some vendors patched older versions of mod_ssl, so this
      *** might be a false positive. Check with your vendor to determine
      *** if you have a version of mod_ssl that is patched for this
      *** vulnerability

  Solution: Upgrade to version 2.8.7 or newer
  Risk factor: High
  CVE: CVE-2002-0082
  BID: 4189

. Vulnerability found on port http (80/tcp):


  The remote web server seems to be vulnerable to the Cross Site Scripting
  vulnerability. The vulnerability is caused by the result returned to the
  user when a non-existing file is requested (e.g. the result contains the
  JavaScript provided in the request).
  The vulnerability would allow an attacker to make the server present the
  user with the attacker's JavaScript/HTML code. Since the content is
  presented by the server, the user will give it the trust level of the server
  (for example, the trust level of banks, shopping centers, etc. would usually
  be high).

  Risk factor: Medium

  Solution: Upgrade to the latest version of WebSphere

  BID: 2401

. Vulnerability found on port http (80/tcp) :

  The remote host has the CGI 'hpnst.exe' installed.
  Older versions of this CGI (pre 5.55) are vulnerableto a denial of service
  attack where the user can make the CGI request itself.

  Solution: upgrade to version 5.55
  Risk factor: High
  CVE: CAN-2003-0169

. Warning found on port http (80/tcp)

  The remote Checkpoint Firewall is open to Web administration.

  An attacker use it to launch a brute force password attackagainst the
  firewall, and eventually take control of it.

  Solution : Disable remote Web administration or filter packets going tothis
  port
  Risk factor : Medium

. Warning found on port http (80/tcp)

  The remote host is using a version of OpenSSL which is older than 0.9.6j or
  0.9.7b

  This version is vulnerable to a timing based attack which may allow an
  attacker to guess the content of fixed data blocks and may eventually be
  able to guess the value of the private RSA key of the server.

  An attacker may use this implementation flaw to sniff the data going to this
  host and decrypt some parts of it, as well as impersonate your server and
  perform man in the middle attacks.

  *** Nessus solely relied on the banner of the remote host
  *** to issue this warning

  See also: http://www.openssl.org/news/secadv_20030219.txt
  http://lasecwww.epfl.ch/memo_ssl.shtml
  http://eprint.iacr.org/2003/052/

  Solution: Upgrade to version 0.9.6j (0.9.7b) or newer
  Risk factor: Medium
  CVE: CAN-2003-0078, CAN-2003-0131
  BID: 6884, 7148

. Warning found on port http (80/tcp)

  Your webserver supports the TRACE and/or TRACK methods. It has been shown
  that servers supporting this method are subject to cross-site-scripting
  attacks, dubbed XST for 'Cross-Site-Tracing', when used in conjunction with
  various weaknesses in browsers.

  An attacker may use this flaw to trick your legitimate web users to give him
  their credentials.

  Solution: Disable these methods.


  If you are using Apache, add the following lines for each virtual host in
  your configuration file :

          RewriteEngine on
          RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
          RewriteRule .* - [F]
```

```
     If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE
     requests or to permit only the methods needed to meet site requirements and
     policy.


     See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf
     http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html

     Risk factor: Medium

   . Warning found on port http (80/tcp)

     The remote host appears to be running a version of Apache which is older
     than 1.3.27

     There are several flaws in this version, you should upgrade to 1.3.27 or
     newer.

     *** Note that Nessus solely relied on the version number
     *** of the remote server to issue this warning. This might
     *** be a false positive

     Solution: Upgrade to version 1.3.27
     See also: http://www.apache.org/dist/httpd/Announcement.html
     Risk factor: Medium
     CVE: CAN-2002-0839, CAN-2002-0840, CAN-2002-0843
     BID: 5847, 5884, 5995, 5996

   . Warning found on port http (80/tcp)

     The remote host is using a version of mod_ssl which is
     older than 2.8.10.

     This version is vulnerable to a flaw which may allow an attacker to
     successfully perform a cross site scripting attack under some circumstances.

     *** Note that several Linux distributions (such as RedHat)
     *** patched the old version of this module. Therefore, this
     *** might be a false positive. Please check with your vendor
     *** to determine if you really are vulnerable to this flaw

     Solution: Upgrade to version 2.8.10 or newer
     Risk factor: Low
     CVE: CAN-2002-1157
     BID: 6029

   . Information found on port http (80/tcp)

     A web server is running on this port

   . Information found on port http (80/tcp)

     The remote web server type is :

     Apache/1.3.6 (Unix) mod_auth_pam/1.0a mod_ssl/2.3.11 OpenSSL/0.9.5a

     Solution : You can set the directive 'ServerTokens Prod' to limit the
     information emanating from the server in its response headers.

   . Information found on port arcisdms (262/tcp)

     The service closed the connection after 2 seconds without sending any data
     It might be protected by some TCP wrapper
```

```
. Information found on port unknown (18209/tcp)

  The service closed the connection after 0 seconds without sending any data
  It might be protected by some TCP wrapper


. Vulnerability found on port unknown (18264/tcp) :

  The remote host appears to be vulnerable to the Apache
  Web Server Chunk Handling Vulnerability.

  If Safe Checks are enabled, this may be a false positivesince it is based on
  the version of Apache.  Although unpatched Apache versions 1.2.2 and above,
  1.3 through 1.3.24 and 2.0 through 2.0.36, the remote server may be running
  a patched version of Apache

  Solution: Upgrade to version 1.3.26 or 2.0.39 or newer
  See also: http://httpd.apache.org/info/security_bulletin_20020617.txt
  http://httpd.apache.org/info/security_bulletin_20020620.txt

  Risk factor: High
  CVE: CVE-2002-0392
  BID: 5033

. Information found on port unknown (18264/tcp)

  A web server is running on this port

. Information found on port unknown (18264/tcp)

  The remote web server type is :

  Check Point SVN foundation/NG FP2

  Solution : We recommend that you configure (if possible) your web server to
  return a bogus Server header in order to not leak information.


. Information found on port general/tcp

  Remote OS guess : Nokia IPSO 3.6 running CheckPoint FW-1 NG FP2

  CVE : CAN-1999-0454

. Information found on port general/udp

  For your information, here is the traceroute to x.x.a.1 :
  x.x.a.1


. Warning found on port general/icmp

  The remote host answers to an ICMP timestamp request. This allows an
  attacker to know the date which is set on your machine.

  This may help him to defeat all your time based authentication protocols.

  Solution: filter out the ICMP timestamp requests (13), and the outgoing
  ICMP timestamp replies (14).

  Risk factor: Low
```

```
   CVE: CAN-1999-0524

 . Warning found on port general/icmp

   The remote host answered to an ICMP_MASKREQ query and sent us its netmask
   (255.255.255.0)

   An attacker can use this information to understand how your network is set
   up and how the routing is done. This may help him to bypass your filters.

   Solution: reconfigure the remote host so that it does not answer to those
   requests.

   Set up filters that deny ICMP packets of type 17.

   Risk factor: Low
   CVE: CAN-1999-0524


------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Firewall log screenshot during Nessus vulnerability scanning:

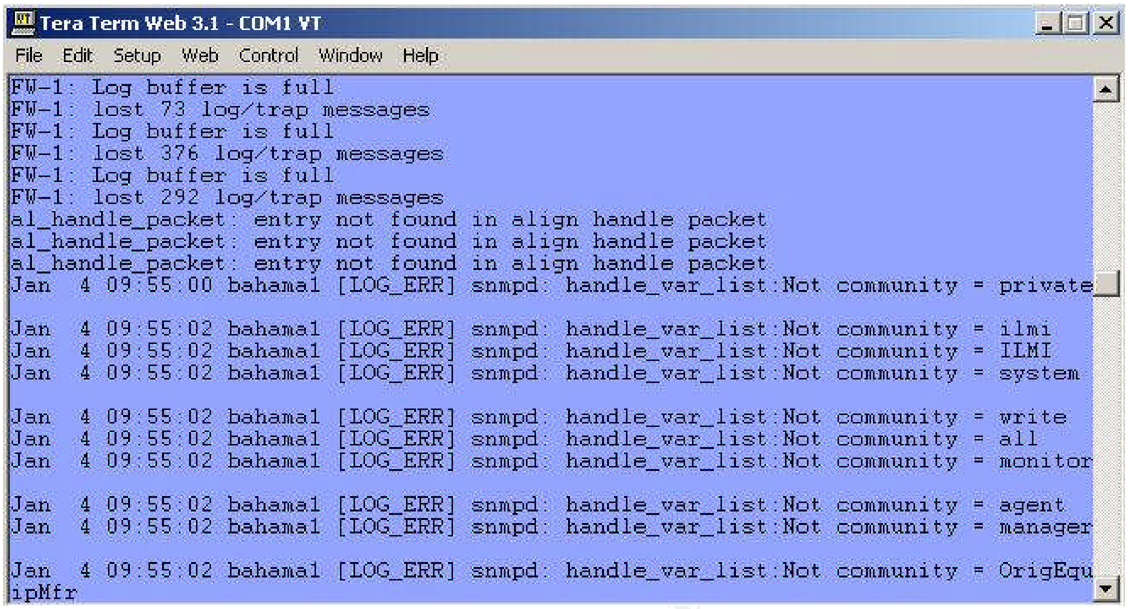


Time	Product	Action	Service	Destination	Protocol	Rule	Source Port	Infor
:19	VPN-1 & FireWall-1	Accept	18256	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	18257	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	18258	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	18259	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	18260	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	18261	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	CP_Exnet_PK	bahama1	tcp	0	4470	
:19	VPN-1 & FireWall-1	Accept	CP_Exnet_resolve	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	FW1_ica_services	bahama1	tcp	0	4470	
:19	VPN-1 & FireWall-1	Accept	18265	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	18266	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	18267	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	18268	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	18269	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	18270	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	18271	bahama1	tcp	2	4470	
:19	VPN-1 & FireWall-1	Accept	18272	bahama1	tcp	2	4470	

Ready Total records: 595114

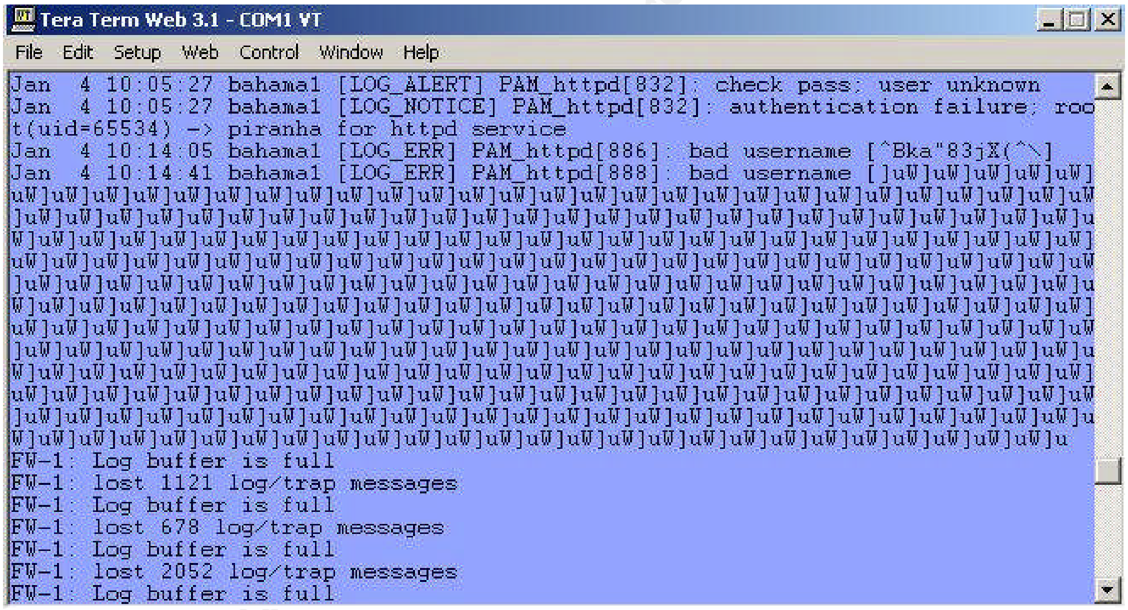
Ready Read/Write NUM

Nokia IPSO console activity during Nessus trusted host scanning:



Tera Term Web 3.1 - COM1 VT
File Edit Setup Web Control Window Help

```
FW-1: Log buffer is full
FW-1: lost 73 log/trap messages
FW-1: Log buffer is full
FW-1: lost 376 log/trap messages
FW-1: Log buffer is full
FW-1: lost 292 log/trap messages
al_handle_packet: entry not found in align handle packet
al_handle_packet: entry not found in align handle packet
al_handle_packet: entry not found in align handle packet
Jan  4 09:55:00 bahama1 [LOG_ERR] snmpd: handle_var_list:Not community = private

Jan  4 09:55:02 bahama1 [LOG_ERR] snmpd: handle_var_list:Not community = ilmi
Jan  4 09:55:02 bahama1 [LOG_ERR] snmpd: handle_var_list:Not community = ILMI
Jan  4 09:55:02 bahama1 [LOG_ERR] snmpd: handle_var_list:Not community = system

Jan  4 09:55:02 bahama1 [LOG_ERR] snmpd: handle_var_list:Not community = write
Jan  4 09:55:02 bahama1 [LOG_ERR] snmpd: handle_var_list:Not community = all
Jan  4 09:55:02 bahama1 [LOG_ERR] snmpd: handle_var_list:Not community = monitor

Jan  4 09:55:02 bahama1 [LOG_ERR] snmpd: handle_var_list:Not community = agent
Jan  4 09:55:02 bahama1 [LOG_ERR] snmpd: handle_var_list:Not community = manager

Jan  4 09:55:02 bahama1 [LOG_ERR] snmpd: handle_var_list:Not community = OrigEqu
ipMfr
```



Tera Term Web 3.1 - COM1 VT
File Edit Setup Web Control Window Help

```
Jan  4 10:05:27 bahama1 [LOG_ALERT] PAM_httpd[832]: check pass; user unknown
Jan  4 10:05:27 bahama1 [LOG_NOTICE] PAM_httpd[832]: authentication failure; roo
t(uid=65534) -> piranha for httpd service
Jan  4 10:14:05 bahama1 [LOG_ERR] PAM_httpd[886]: bad username [^Bka"83jX(^\]
Jan  4 10:14:41 bahama1 [LOG_ERR] PAM_httpd[888]: bad username []uW]uW]uW]uW]uW]
uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW
]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]u
W]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]
uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW
]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]u
W]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]
uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW
]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]u
W]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]
uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW
]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]u
W]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]uW]u
FW-1: Log buffer is full
FW-1: lost 1121 log/trap messages
FW-1: Log buffer is full
FW-1: lost 678 log/trap messages
FW-1: Log buffer is full
FW-1: lost 2052 log/trap messages
FW-1: Log buffer is full
```

Port to service mapping for trusted host:

Port	Service	Purpose/Function
23/tcp	telnet	Remote administration
53/udp	domain	Domain Name Service
68/udp	dhcpclient	Bootstrap Protocol Client
80/tcp	http	World Wide Web HTTP
161/udp	snmp	Simple Network Management Protocol
256/tcp	FW1	Check Point VPN-1 & FireWall-1 Service - Get topology information from MM to FWM

		- Full synchronization for HA configuration
257/tcp	FW1_log	Check Point VPN-1 & FireWall-1 Logs - Protocol used for delivering logs from FWM to MM
259/tcp	FW1_clntauth FW1_clntauth_telnet	Check Point VPN-1 & FireWall-1 Client Authentication (Telnet) - Protocol for performing Client-Authentication at FWM using telnet
259/udp	firewall1-rdp	Check Point VPN-1 FWZ Key Negotiations - Reliable Datagram Protocol - Protocol used for FWZ VPN (supported up to NG FP1 only) - Protocol used by SR/SCl for checking the availability of the FWM/PS
262/tcp	arcisdms	arcisdms
264/tcp	FW1_topo	Check Point VPN-1 SecuRemote Topology Requests - Topology Download for SR (build 4100 and higher) and SCl
500/udp	isakmp	ISAKMP, Internet Security Association and Key Management Protocol, defines procedures and packet formats to establish, negotiate, modify and delete Security Associations. http://www.networksorcery.com/enp/protocol/isakmp.htm
514/udp	syslog	Syslog
900/tcp	FW1_clntauth FW1_clntauth_http	Check Point VPN-1 & FireWall-1 Client Authentication (HTTP) - Protocol for performing Client-Authentication at FWM using HTTP
1024/udp	Reserved	Unknown Purpose
1031/tcp	iad2	BBN IAD
1032/tcp	iad3	BBN IAD
1033/tcp	netinfo-local	Local netinfo port
1034/tcp	activesync	ActiveSync Notifications
1035/tcp	mxxrlogin	MX-XR RPC
1036/tcp	nsstp	Nebula Secure Segment Transfer Protocol
1701/udp	l2f, l2tp	l2f
1720/tcp	h323hostcall	h323hostcall
2746/udp	VPN1_IPSEC_encapsulation	Check Point VPN-1 SecuRemote IPSEC Transport Encapsulation Protocol - Default-Protocol used for UDP encapsulation
18183/tcp	FW1_sam	Check Point OPSEC Suspicious Activity Monitor API - Protocol e.g. for Block Intruder between MM and FWM
18184/tcp	FW1_lea	Check Point OPSEC Log Export API - Protocol for exporting logs from MM
18187/tcp	FW1_ela	Check Point OPSEC Event Logging API

		- Protocol for applications logging to the Firewall log at MM
18190/tcp	CPMI	Check Point Management Interface - Protocol for communication between GUI and MM
18191/tcp	CPD	Check Point Daemon Protocol - Download of rulebase from MM to FWM - Fetching rulebase from FWM to MM when starting
18192/tcp	CPD_amon	Check Point Internal Application Monitoring - Protocol for e.g. getting System Status from MM to FWM
18196/tcp	Unknown	Unknown
18208/tcp	FW1_CPRID	Check Point Remote Installation Protocol - Protocol used from MM to FWM when installing Secure Updates.
18209/tcp	- not defined -	Protocol used in SIC for communication between FWM and ICA (status, issue, revoke)
18210/tcp	FW1_ica_pull	Check Point Internal CA Pull Certificate Service - Protocol used by SIC for e.g. FWM pulling CA's from MM
18221/tcp	CP_redundant	Check Point Redundant Management Protocol - Protocol used for synchronizing primary and secondary MM
18233/udp	FW1_scv_keep_alive	Check Point SecureClient Verification KeepAlive Protocol - Protocol for verifying SecureClient
18234/udp	tunnel_test	Check Point tunnel testing application - Protocol for testing applications through a VPN, used by SR/SCI
18264/tcp	FW1_ica_services	Check Point Internal CA Fetch CRL and User Registration Services - Protocol for Certificate Revocation Lists and registering users when using the Policy Server - needed when e.g. FWM is starting

Note: Port number service and purpose/function were based on information obtained from the following sites:

- http://www.iana.org/assignments/port-numbers
- http://www.fw-1.de/aerasec/ng/ports-ng.html

Assessment:
>>The organization is not compliant with this control objective.

Vulnerability advisory web search revealed that the installed version of Checkpoint Firewall NG FP3 is currently vulnerable to two application exploits. Checkpoint Hotfixes are available for this issue. Additionally, it is noted that misconfigurations of the firewall application could expose the Nokia Checkpoint Firewall or the network systems and applications it protects to vulnerabilities.

Nmap scanning from a non trusted host revealed that several open Checkpoint Firewall NG ports and ISAKMP. All of the open ports are required for various firewall operational activities or SecuRemote connections.

Nessus security scanning from a non-trusted host confirmed the nmap findings. Several false findings are noted. In particular, Nessus identified 18264 as an apache web server. The tcp port actually represents FW1_ica_services, which is used for Check Point Internal CA Fetch CRL and User Registration Services.

Risks to the Nokia Checkpoint Firewall are minimal from non-trusted hosts. The firewall adequately blocks all unauthorized connection attempts.

However, under the current configuration, and in particular firewall rule 2, numerous vulnerabilities to the firewall exist from trusted hosts.

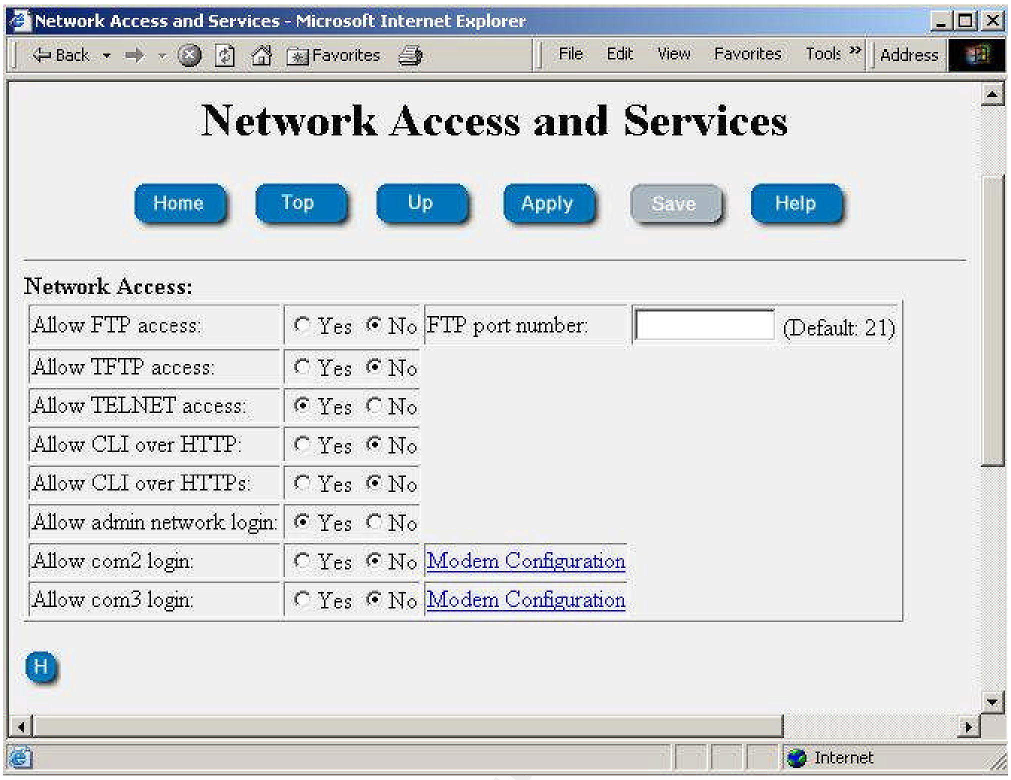
The firewall rule and global policies permitting remote administration are not adequately configured to protect the system.

SDC-5, ENC-1

Description: Remote management activity security

Results:
The results are based on the testing procedures defined in the SDC-5, ENC-1 checklist item.

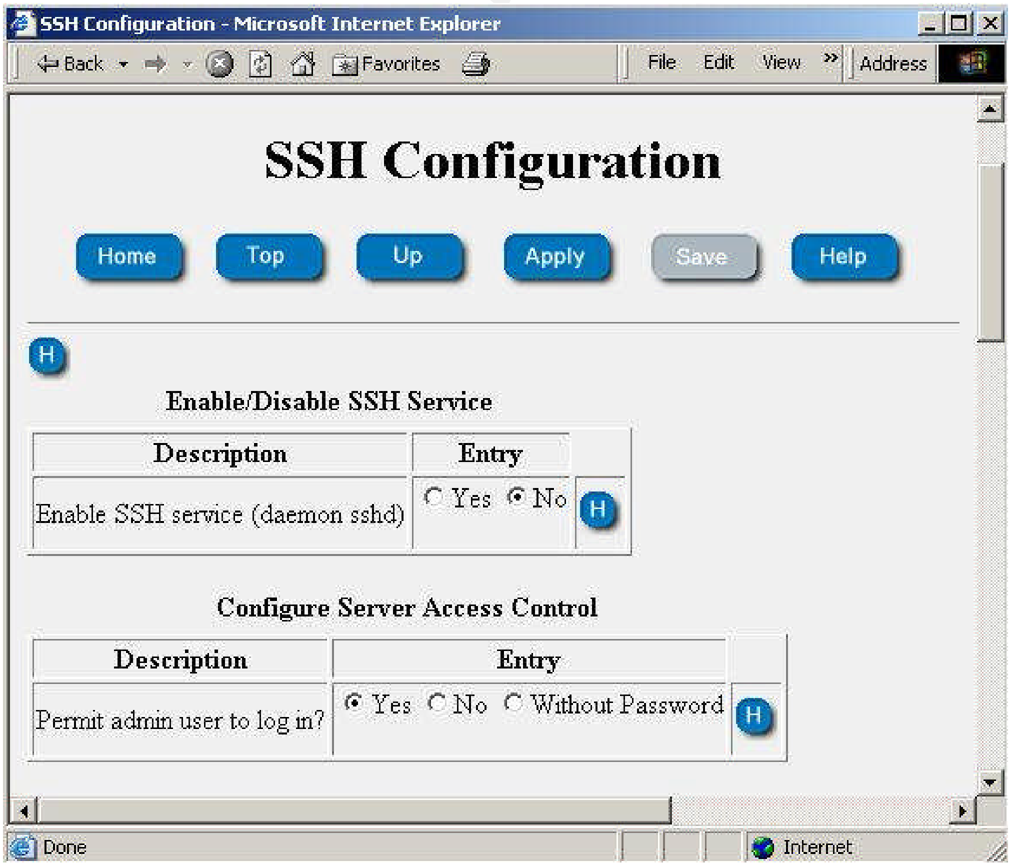
The following Nokia Network Voyager screenshots provide information regarding the remote management configuration settings for the IPSO operating system.



Network Access and Services

Network Access:

Allow FTP access:	○ Yes ● No	FTP port number:		(Default: 21)
Allow TFTP access:	○ Yes ● No			
Allow TELNET access:	● Yes ○ No			
Allow CLI over HTTP:	○ Yes ● No			
Allow CLI over HTTPs:	○ Yes ● No			
Allow admin network login:	● Yes ○ No			
Allow com2 login:	○ Yes ● No	Modem Configuration		
Allow com3 login:	○ Yes ● No	Modem Configuration		



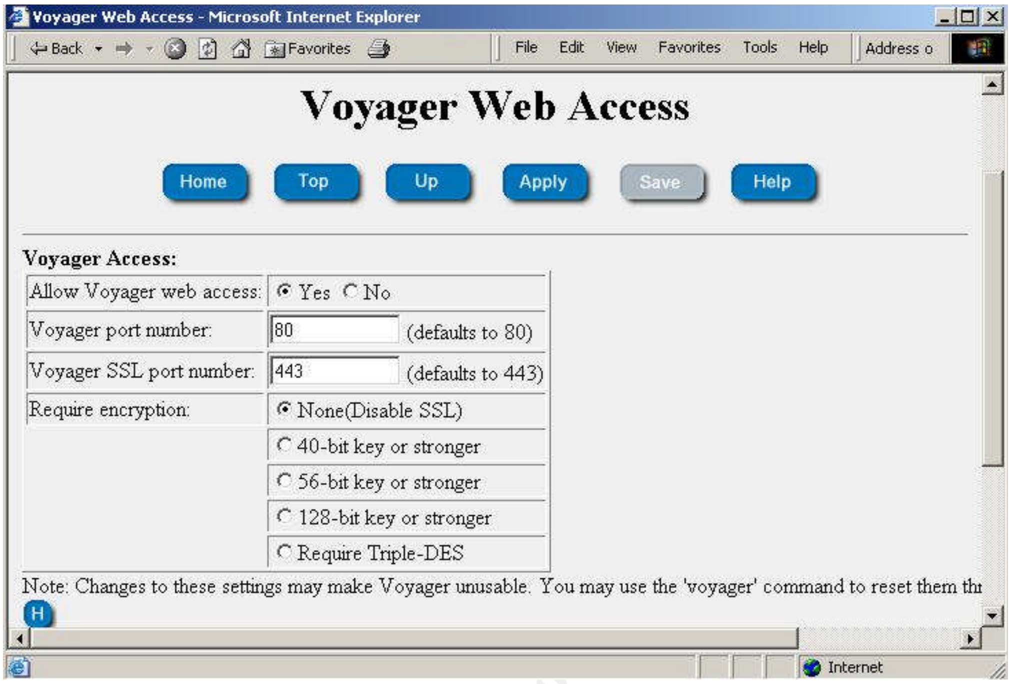
SSH Configuration

Enable/Disable SSH Service

Description	Entry
Enable SSH service (daemon sshd)	○ Yes ● No

Configure Server Access Control

Description	Entry
Permit admin user to log in?	● Yes ○ No ○ Without Password



Voyager Web Access - Microsoft Internet Explorer
Back
Favorites
File Edit View Favorites Tools Help
Address
Home
Top
Up
Apply
Save
Help
Internet

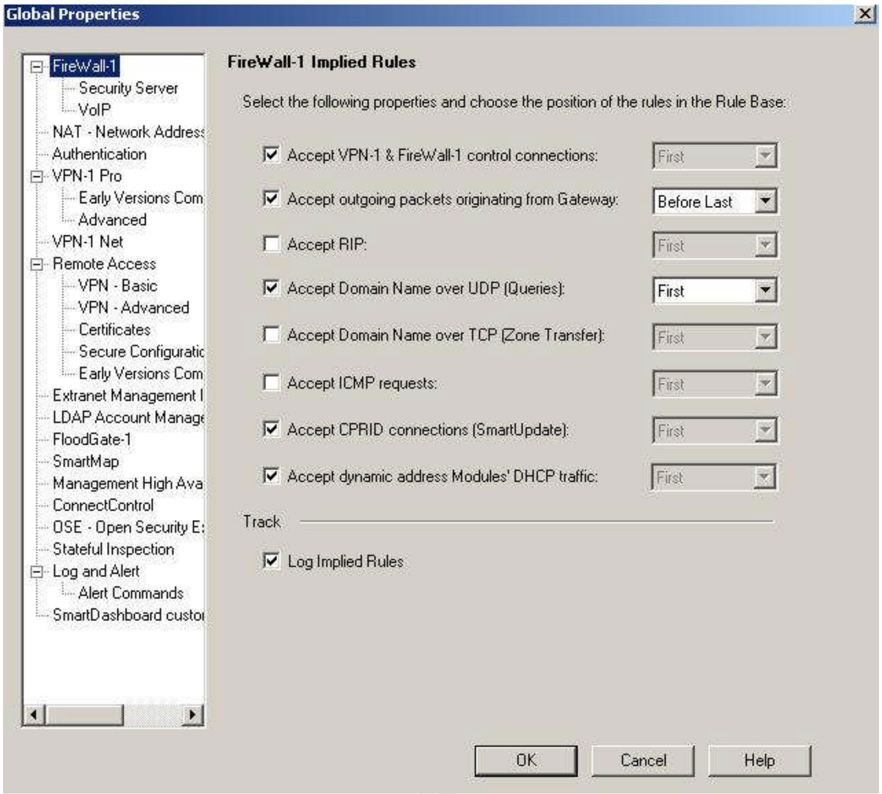
Voyager Web Access

Voyager Access:

Allow Voyager web access:	● Yes ○ No
Voyager port number:	80 (defaults to 80)
Voyager SSL port number:	443 (defaults to 443)
Require encryption:	● None(Disable SSL)
	○ 40-bit key or stronger
	○ 56-bit key or stronger
	○ 128-bit key or stronger
	○ Require Triple-DES

Note: Changes to these settings may make Voyager unusable. You may use the 'voyager' command to reset them thr

The following Checkpoint firewall management configuration screenshots provide information regarding the remote management configuration settings for the Checkpoint Firewall application.



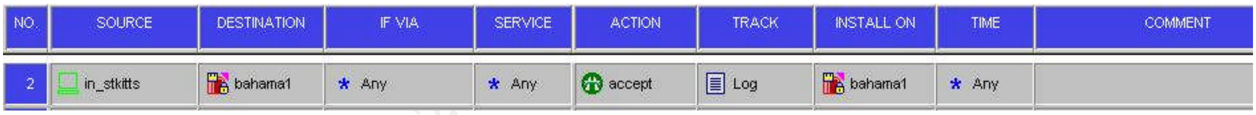
FireWall-1 Implied Rules

Select the following properties and choose the position of the rules in the Rule Base:

- ☑ Accept VPN-1 & FireWall-1 control connections: First
- ☑ Accept outgoing packets originating from Gateway: Before Last
- □ Accept RIP: First
- ☑ Accept Domain Name over UDP (Queries): First
- □ Accept Domain Name over TCP (Zone Transfer): First
- □ Accept ICMP requests: First
- ☑ Accept CPRID connections (SmartUpdate): First
- ☑ Accept dynamic address Modules' DHCP traffic: First

Track

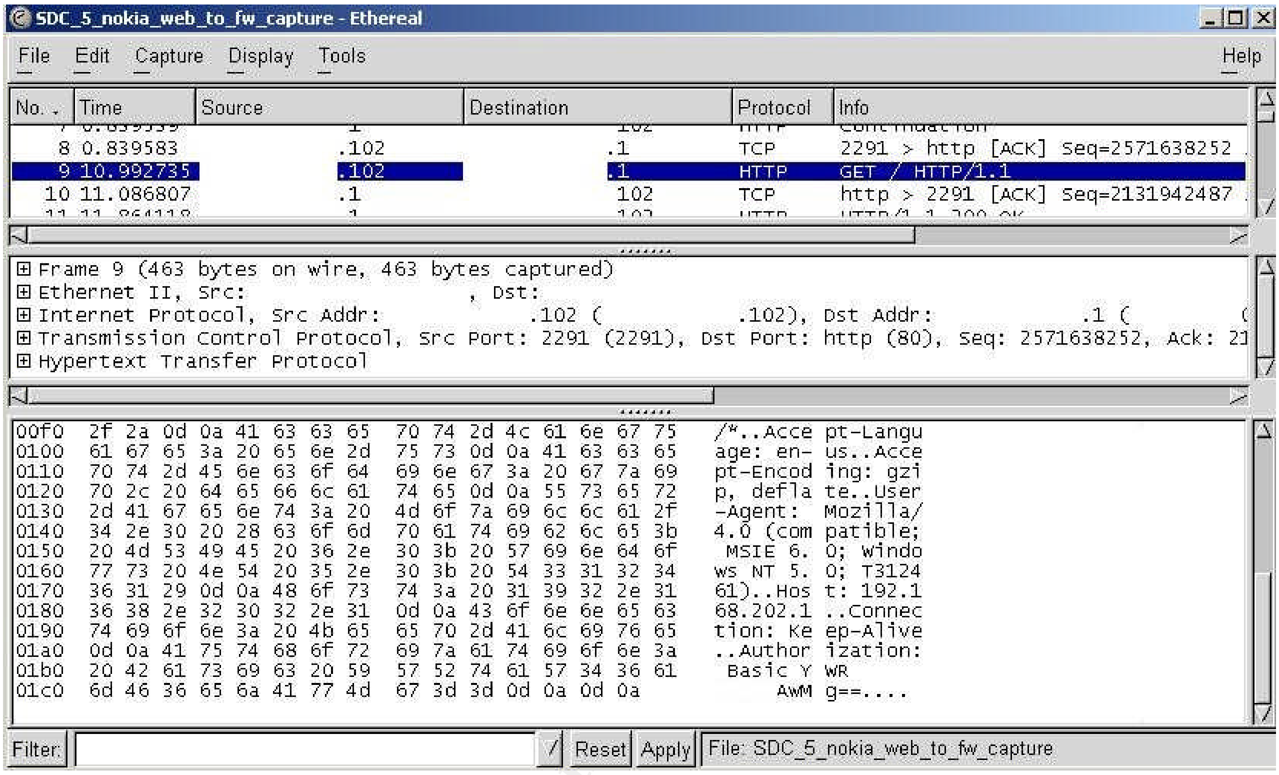
- ☑ Log Implied Rules



NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
2	in_stkitts	bahama1	* Any	* Any	accept	Log	bahama1	* Any	

The following screenshots represent network transmission captures of remote management activity to the Nokia checkpoint firewall .

The first capture is from the management station to Nokia checkpoint firewall using the Nokia Network Voyager web interface to configure the IPSO operating system:

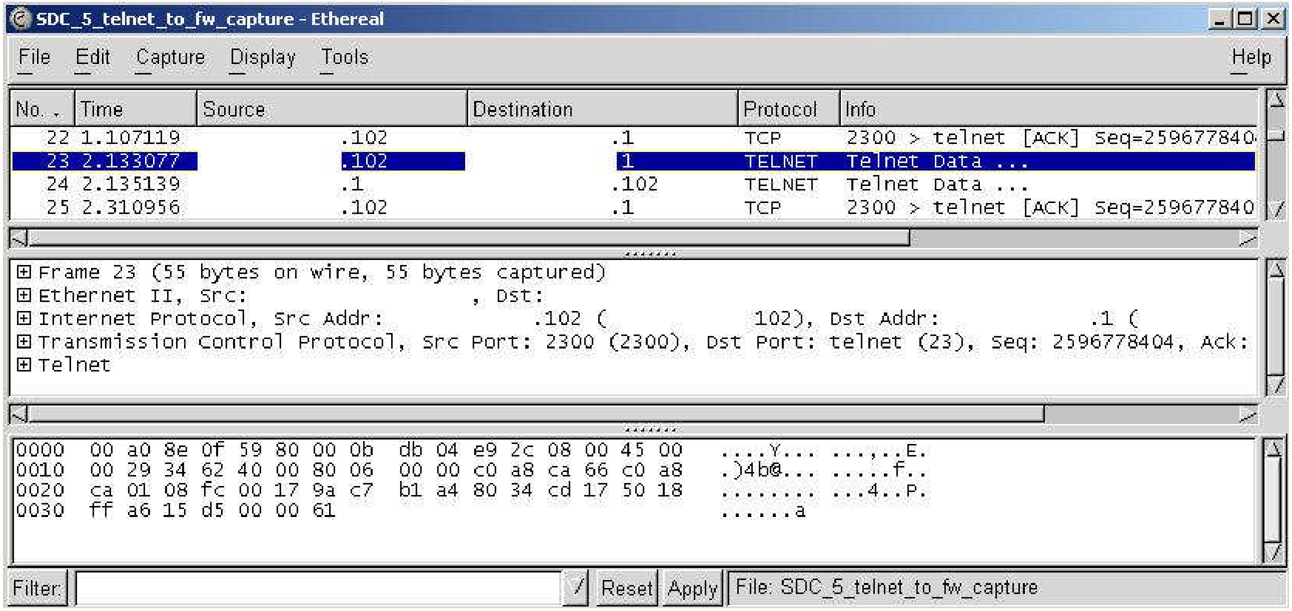


```
No.  Time        Source          Destination     Protocol  Info
  8 0.839583             .102              .1    TCP       2291 > http [ACK] Seq=2571638252
  9 10.992735            .102              .1    HTTP      GET / HTTP/1.1
 10 11.086807            .1               102    TCP       http > 2291 [ACK] Seq=2131942487
```

```
⊞ Frame 9 (463 bytes on wire, 463 bytes captured)
⊞ Ethernet II, Src:                , Dst:
⊞ Internet Protocol, Src Addr:           .102 (          .102), Dst Addr:           .1 (
⊞ Transmission Control Protocol, Src Port: 2291 (2291), Dst Port: http (80), Seq: 2571638252, Ack: 21
⊞ Hypertext Transfer Protocol
```

```
00f0  2f 2a 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   /*..Acce pt-Langu
0100  61 67 65 3a 20 65 6e 2d  75 73 0d 0a 41 63 63 65   age: en- us..Acce
0110  70 74 2d 45 6e 63 6f 64  69 6e 67 3a 20 67 7a 69   pt-Encod ing: gzi
0120  70 2c 20 64 65 66 6c 61  74 65 0d 0a 55 73 65 72   p, defla te..User
0130  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:  Mozilla/
0140  34 2e 30 20 28 63 6f 6d  70 61 74 69 62 6c 65 3b   4.0 (com patible;
0150  20 4d 53 49 45 20 36 2e  30 3b 20 57 69 6e 64 6f    MSIE 6. 0; Windo
0160  77 73 20 4e 54 20 35 2e  30 3b 20 54 33 31 32 34   ws NT 5. 0; T3124
0170  36 31 29 0d 0a 48 6f 73  74 3a 20 31 39 32 2e 31   61)..Hos t: 192.1
0180  36 38 2e 32 30 32 2e 31  0d 0a 43 6f 6e 6e 65 63   68.202.1 ..Connec
0190  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
01a0  0d 0a 41 75 74 68 6f 72  69 7a 61 74 69 6f 6e 3a   ..Author ization:
01b0  20 42 61 73 69 63 20 59  57 52 74 61 57 34 36 61    Basic Y WR
01c0  6d 46 36 65 6a 41 77 4d  67 3d 3d 0d 0a 0d 0a           AwM g==....
```

The following capture is from the management station to Nokia checkpoint firewall using telnet to configure the IPSO operating system:

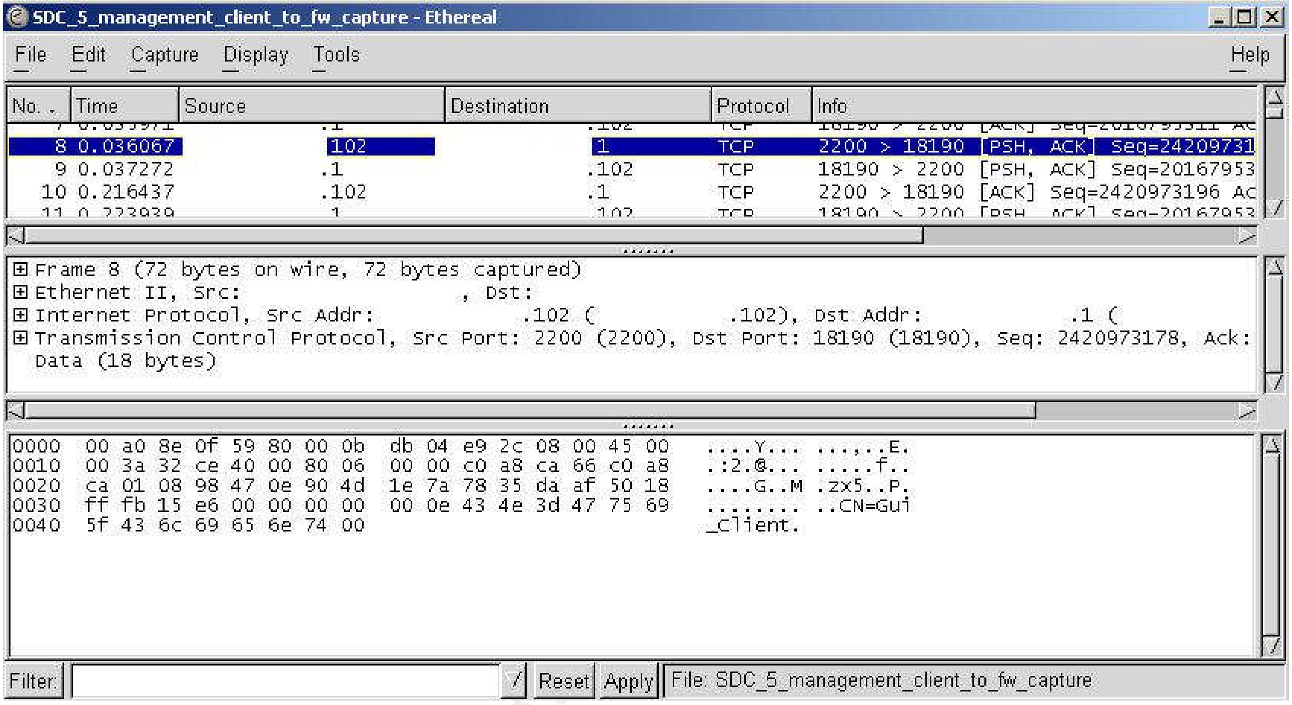


```
No.  Time        Source          Destination     Protocol  Info
 22 1.107119             .102              .1    TCP       2300 > telnet [ACK] Seq=259677840
 23 2.133077             .102              1     TELNET    Telnet Data ...
 24 2.135139             .1                .102  TELNET    Telnet Data ...
 25 2.310956             .102              .1    TCP       2300 > telnet [ACK] Seq=259677840
```

```
⊞ Frame 23 (55 bytes on wire, 55 bytes captured)
⊞ Ethernet II, Src:                , Dst:
⊞ Internet Protocol, Src Addr:           .102 (          102), Dst Addr:           .1 (
⊞ Transmission Control Protocol, Src Port: 2300 (2300), Dst Port: telnet (23), Seq: 259677840 4, Ack:
⊞ Telnet
```

```
0000  00 a0 8e 0f 59 80 00 0b  db 04 e9 2c 08 00 45 00   ....Y... ...,..E.
0010  00 29 34 62 40 00 80 06  00 00 c0 a8 ca 66 c0 a8   .)4b@... .....f..
0020  ca 01 08 fc 00 17 9a c7  b1 a4 80 34 cd 17 50 18   ........ ...4..P.
0030  ff a6 15 d5 00 00 61                               ......a
```

The following capture is again from the management station to Nokia checkpoint firewall using the Checkpoint NG SmartDashboard client firewall management and configuration tool.



```
No. .  Time      Source       Destination   Protocol  Info
  8 0.036067     102            1           TCP       2200 > 18190 [PSH, ACK] Seq=24209731
  9 0.037272    .1            .102          TCP       18190 > 2200 [PSH, ACK] Seq=20167953
 10 0.216437    .102          .1            TCP       2200 > 18190 [ACK] Seq=2420973196 Ac
 11 0.223939    .1            .102          TCP       18190 > 2200 [PSH, ACK] Seq=20167953
```

```
⊞ Frame 8 (72 bytes on wire, 72 bytes captured)
⊞ Ethernet II, Src:                    , Dst:
⊞ Internet Protocol, Src Addr:             .102 (             .102), Dst Addr:            .1 (
⊞ Transmission Control Protocol, Src Port: 2200 (2200), Dst Port: 18190 (18190), Seq: 2420973178, Ack:
  Data (18 bytes)
```

```
0000  00 a0 8e 0f 59 80 00 0b  db 04 e9 2c 08 00 45 00   ....Y... ...,..E.
0010  00 3a 32 ce 40 00 80 06  00 00 c0 a8 ca 66 c0 a8   .:2.@... .....f..
0020  ca 01 08 98 47 0e 90 4d  1e 7a 78 35 da af 50 18   ....G..M .zx5..P.
0030  ff fb 15 e6 00 00 00 00  00 0e 43 4e 3d 47 75 69   ........ ..CN=Gui
0040  5f 43 6c 69 65 6e 74 00                            _Client.
```

Assessment:
>>The organization is not compliant with this control objective.

As indicated by the Nokia configuration screenshots and confirmed by the network traffic captures, IPSO operating system remote management is accomplished via clear text http and telnet services. The base64 encoded login account and password is captured during the web-based Nokia Network Voyager log in. The encoded account and password can be de-coded using the base64.exe utility. The telnet captures reveal the login account and password as well.

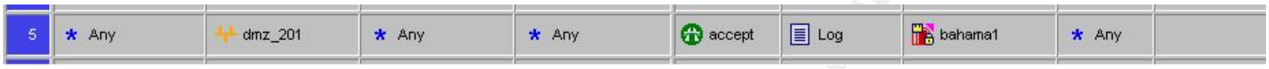
The checkpoint Global Properties settings permit firewall-1/vpn-1 control connections. Firewall-1/VPN-1 captured connection control transmissions were encrypted.

SDC-8

Description: DMZ network security

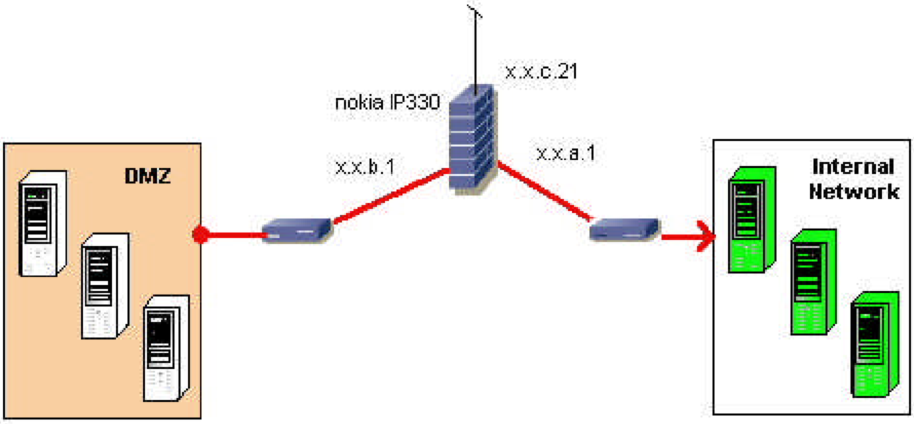
Results:
The results are based on the testing procedures defined in the SDC-8 checklist item.

The following rule allows networks access to DMZ systems from all networks



5	* Any	dmz_201	* Any	* Any	accept	Log	bahama1	* Any

Test scenario
Given that unrestricted access is permitted to the DMZ, a test was developed to simulate a compromised DMZ system's attempt to enumerate internal network systems.



Firewalk and nmap were used to test security. The ethereal network analyzer was used on the internal network to capture any data originating from the DMZ network.

Firewalk results:

```
[root@localhost root]# firewalk -n  -pUDP -s 53 -d 53 x.x.a.1 x.x.a.101
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
UDP-based scan.
Ramping phase source port: 53, destination port: 53
Hotfoot through x.x.a.1 using x.x.a.101 as a metric.
Ramping Phase:
 1 (TTL  1): *no response*
 2 (TTL  2): *no response*
 3 (TTL  3): *no response*
*
*
*
21 (TTL 21): *no response*
```

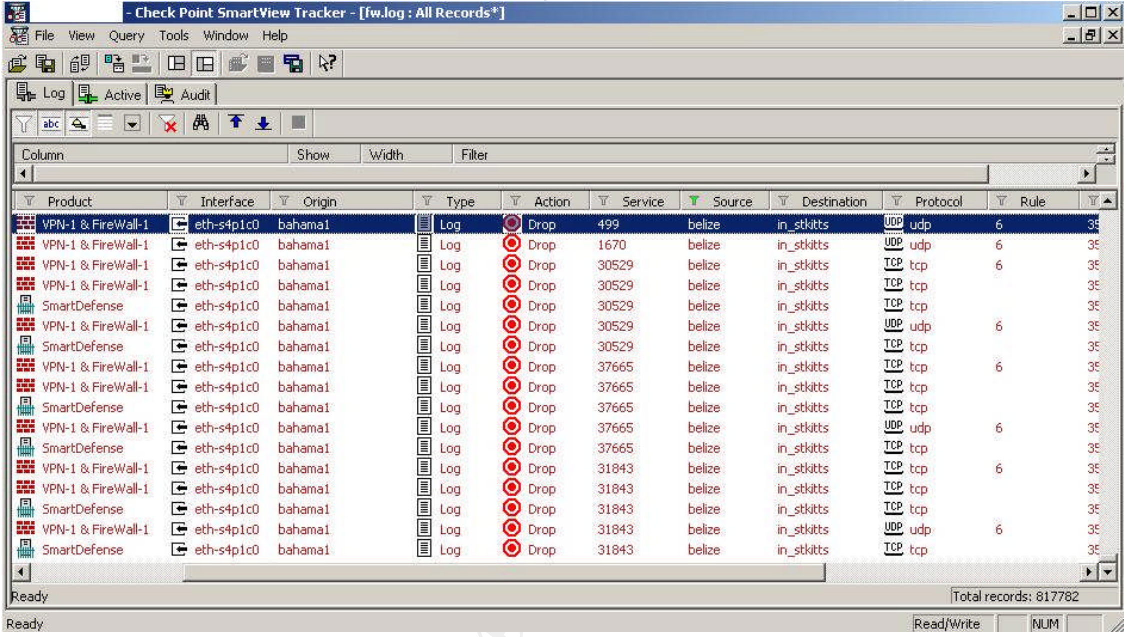
```
22 (TTL 22): *no response*
23 (TTL 23): *no response*
24 (TTL 24): *no response*
25 (TTL 25): *no response*
Scan aborted: hopcount exceeded.

Total packets sent:                  25
Total packet errors:                 0
Total packets caught                 29
Total packets caught of interest     0
Total ports scanned                  0
Total ports open:                    0
Total ports unknown:                 0
[root@localhost root]#
```

Nmap results:

```
root@localhost root]# nmap -v -P0 -sU -sS -O x.x.a.101

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host  (x.x.a.101) appears to be up ... good.
Initiating SYN Stealth Scan against  (x.x.a.101)
The SYN Stealth Scan took 1679 seconds to scan 1554 ports.
Initiating UDP Scan against  (x.x.a.101)
The UDP Scan took 1755 seconds to scan 1459 ports.
Adding open port 1670/udp
Adding open port 499/udp
Adding open port 1404/udp
Adding open port 167/udp
Adding open port 491/udp
Adding open port 374/udp
*
*
*
Adding open port 396/udp
Adding open port 541/udp
Adding open port 95/udp
Adding open port 413/udp
Adding open port 1652/udp
Adding open port 655/udp
(no udp responses received -- assuming all ports filtered)
Warning:  OS detection will be MUCH less reliable because we did not find at
least 1 open and 1 closed TCP port
All 3013 scanned ports on  (x.x.a.101) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=2.54BETA31%P=i386-redhat-linux-gnu%D=11/9%Time=3FAE4FE5%O=-1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)


Nmap run completed -- 1 IP address (1 host up) scanned in 3655 seconds
[root@localhost root]#
```

Ethereal network captures did not pick up any traffic originating from the DMZ network.

The checkpoint firewall logs indicate that all firewalk and nmap traffic was blocked at the DMZ interface (x.x.b.1). The firewall log showed that the firewalk traffic originating from the DMZ was identified as an attack and was blocked by the SmartDefense feature of the Checkpoint firewall.


- Check Point SmartView Tracker - [fw.log : All Records*]
File View Query Tools Window Help
Log Active Audit
abc
Column Show Width Filter

Product	Interface	Origin	Type	Action	Service	Source	Destination	Protocol	Rule	
VPN-1 & FireWall-1	eth-s4p1c0	bahama1	Log	Drop	499	belize	in_stkitts	udp	6	35
VPN-1 & FireWall-1	eth-s4p1c0	bahama1	Log	Drop	1670	belize	in_stkitts	udp	6	35
VPN-1 & FireWall-1	eth-s4p1c0	bahama1	Log	Drop	30529	belize	in_stkitts	tcp	6	35
VPN-1 & FireWall-1	eth-s4p1c0	bahama1	Log	Drop	30529	belize	in_stkitts	tcp		35
SmartDefense	eth-s4p1c0	bahama1	Log	Drop	30529	belize	in_stkitts	tcp		35
VPN-1 & FireWall-1	eth-s4p1c0	bahama1	Log	Drop	30529	belize	in_stkitts	udp	6	35
SmartDefense	eth-s4p1c0	bahama1	Log	Drop	30529	belize	in_stkitts	tcp		35
VPN-1 & FireWall-1	eth-s4p1c0	bahama1	Log	Drop	37665	belize	in_stkitts	tcp	6	35
VPN-1 & FireWall-1	eth-s4p1c0	bahama1	Log	Drop	37665	belize	in_stkitts	tcp		35
SmartDefense	eth-s4p1c0	bahama1	Log	Drop	37665	belize	in_stkitts	tcp		35
VPN-1 & FireWall-1	eth-s4p1c0	bahama1	Log	Drop	37665	belize	in_stkitts	udp	6	35
SmartDefense	eth-s4p1c0	bahama1	Log	Drop	37665	belize	in_stkitts	tcp		35
VPN-1 & FireWall-1	eth-s4p1c0	bahama1	Log	Drop	31843	belize	in_stkitts	tcp	6	35
VPN-1 & FireWall-1	eth-s4p1c0	bahama1	Log	Drop	31843	belize	in_stkitts	tcp		35
SmartDefense	eth-s4p1c0	bahama1	Log	Drop	31843	belize	in_stkitts	tcp		35
VPN-1 & FireWall-1	eth-s4p1c0	bahama1	Log	Drop	31843	belize	in_stkitts	udp	6	35
SmartDefense	eth-s4p1c0	bahama1	Log	Drop	31843	belize	in_stkitts	tcp		35

Ready Total records: 817782

Ready Read/Write NUM

Assessment:
>>The organization is not compliant with this control objective.

Although the traffic from the DMZ to the internal network was blocked at the firewall, the rule permitting access from the Internet is too permissive. As a result, this configuration will expose DMZ systems to numerous network based vulnerabilities and attacks.

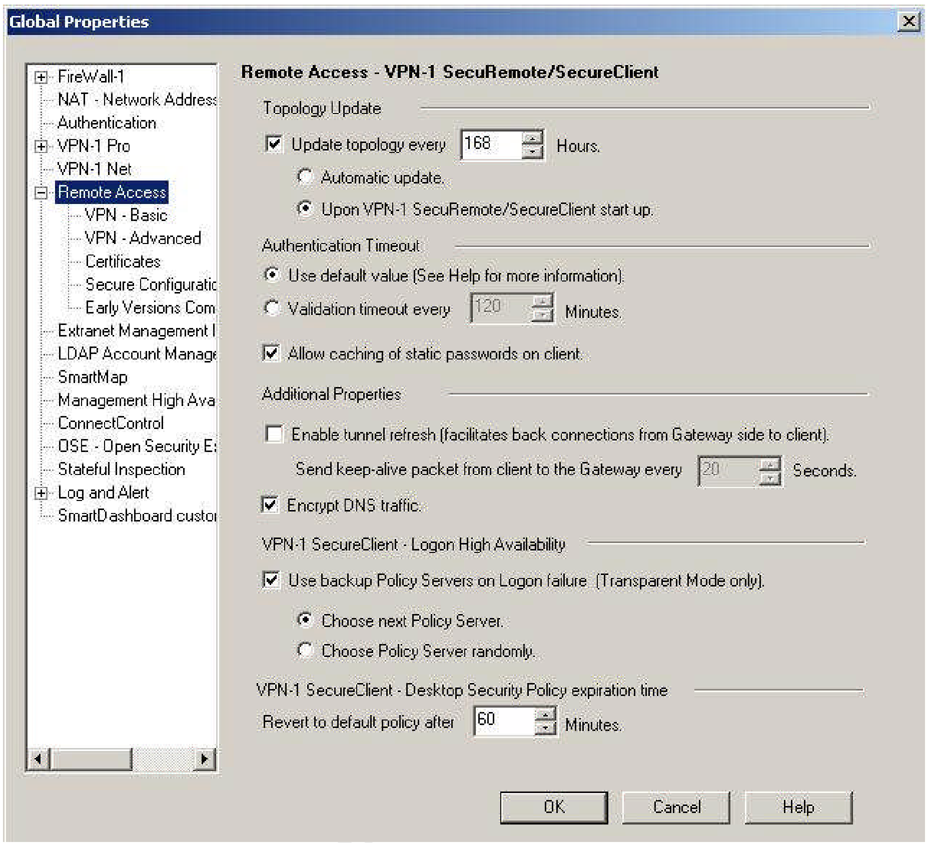
SDC-10

Description: SecuRemote Access and Configuration

Results

The results are based on the testing procedures defined in the SDC-10 checklist item.

The following Checkpoint remote access screenshots provide information regarding the VPN-1 SecuRemote configuration settings.



Remote Access - VPN-1 SecuRemote/SecureClient

Topology Update

☑ Update topology every 168 Hours.

○ Automatic update.

● Upon VPN-1 SecuRemote/SecureClient start up.

Authentication Timeout

● Use default value (See Help for more information).

○ Validation timeout every 120 Minutes.

☑ Allow caching of static passwords on client.

Additional Properties

□ Enable tunnel refresh (facilitates back connections from Gateway side to client).

Send keep-alive packet from client to the Gateway every 20 Seconds.

☑ Encrypt DNS traffic.

VPN-1 SecureClient - Logon High Availability

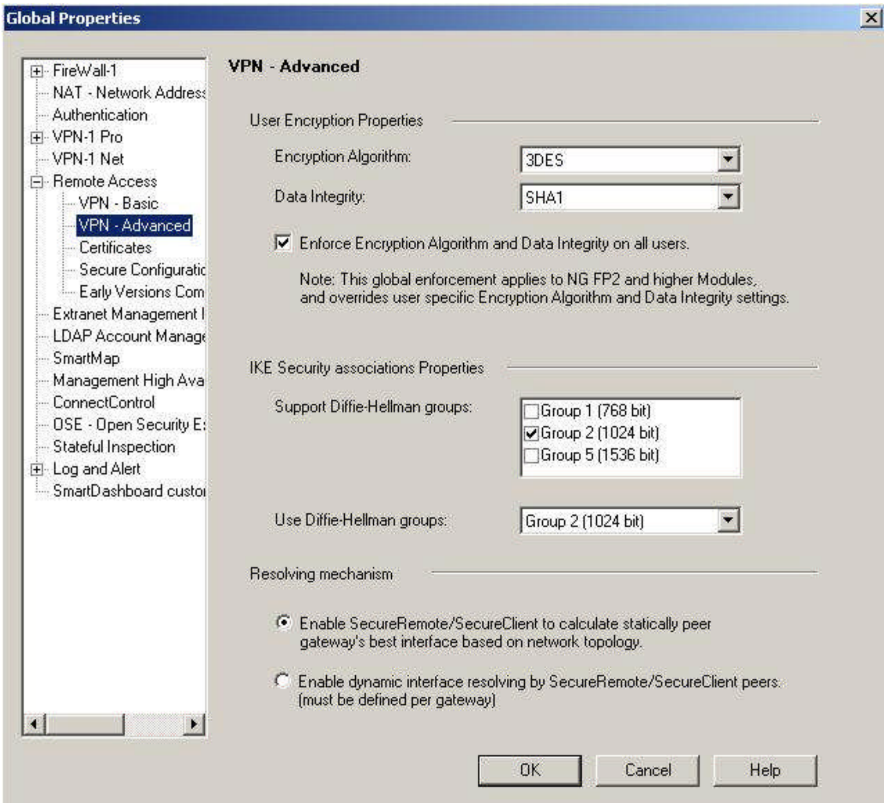
☑ Use backup Policy Servers on Logon failure (Transparent Mode only).

● Choose next Policy Server.

○ Choose Policy Server randomly.

VPN-1 SecureClient - Desktop Security Policy expiration time

Revert to default policy after 60 Minutes.



VPN - Advanced

User Encryption Properties

Encryption Algorithm: 3DES

Data Integrity: SHA1

☑ Enforce Encryption Algorithm and Data Integrity on all users.

Note: This global enforcement applies to NG FP2 and higher Modules, and overrides user specific Encryption Algorithm and Data Integrity settings.

IKE Security associations Properties

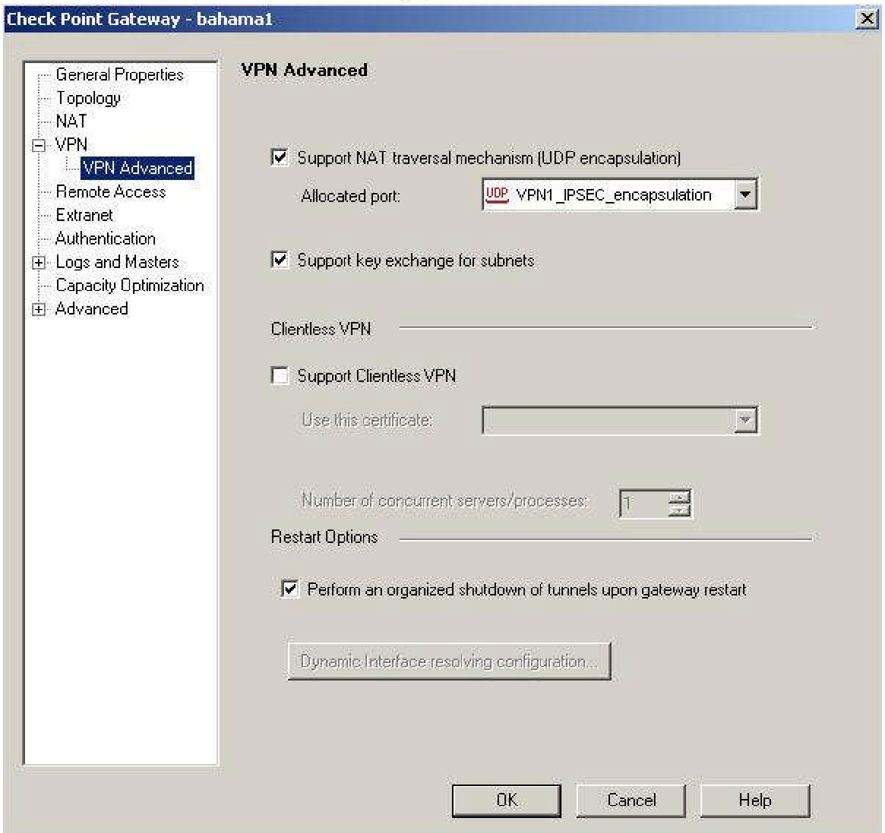
Support Diffie-Hellman groups:
☐ Group 1 (768 bit)
☑ Group 2 (1024 bit)
☐ Group 5 (1536 bit)

Use Diffie-Hellman groups: Group 2 (1024 bit)

Resolving mechanism

● Enable SecureRemote/SecureClient to calculate statically peer gateway's best interface based on network topology.

○ Enable dynamic interface resolving by SecureRemote/SecureClient peers. (must be defined per gateway)



VPN Advanced

☑ Support NAT traversal mechanism (UDP encapsulation)

Allocated port: VPN1_IPSEC_encapsulation

☑ Support key exchange for subnets

Clientless VPN

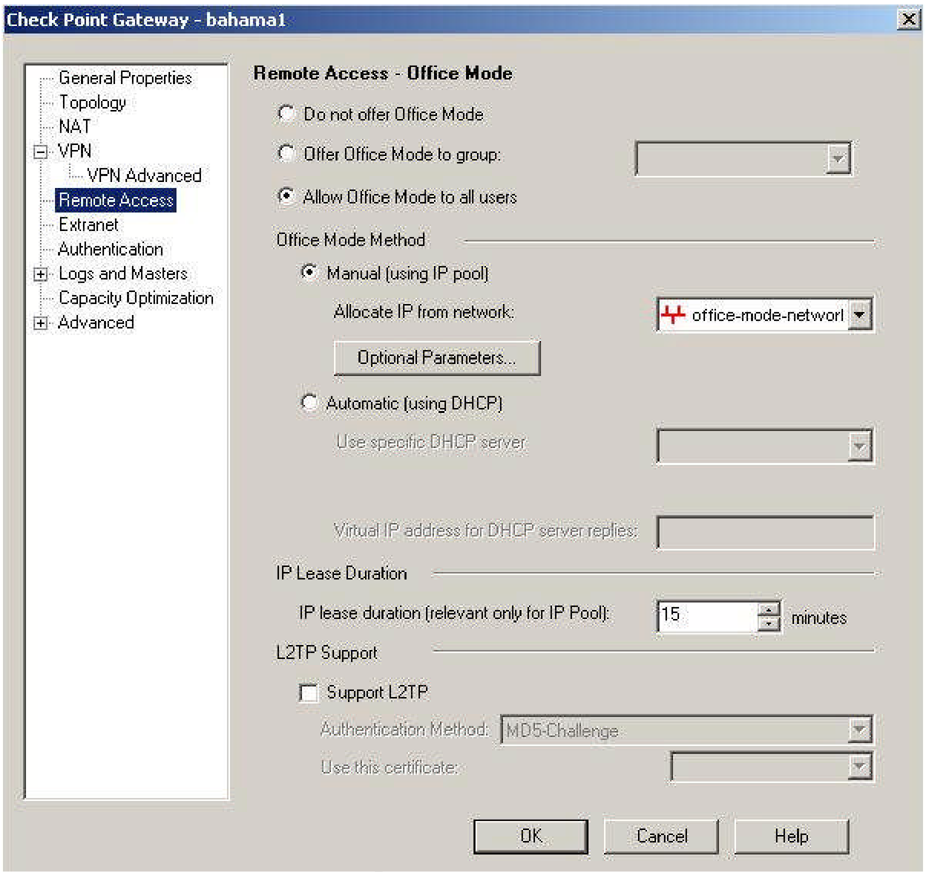
☐ Support Clientless VPN

Use this certificate:

Number of concurrent servers/processes: 1

Restart Options

☑ Perform an organized shutdown of tunnels upon gateway restart



Check Point Gateway - bahama1

Remote Access - Office Mode

○ Do not offer Office Mode

○ Offer Office Mode to group:

● Allow Office Mode to all users

Office Mode Method

● Manual (using IP pool)

Allocate IP from network: office-mode-networl

Optional Parameters...

○ Automatic (using DHCP)

Use specific DHCP server

Virtual IP address for DHCP server replies:

IP Lease Duration

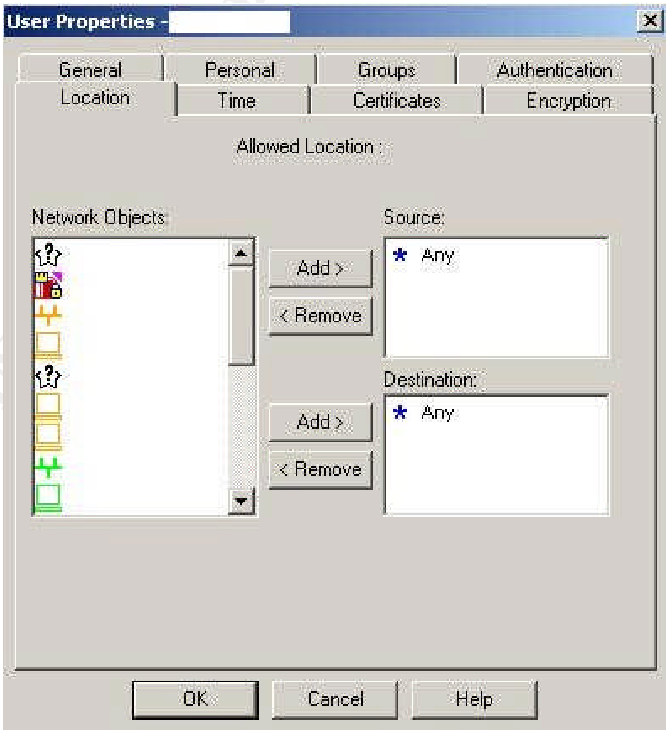
IP lease duration (relevant only for IP Pool): 15 minutes

L2TP Support

☐ Support L2TP

Authentication Method: MD5-Challenge

Use this certificate:



User Properties - [redacted]

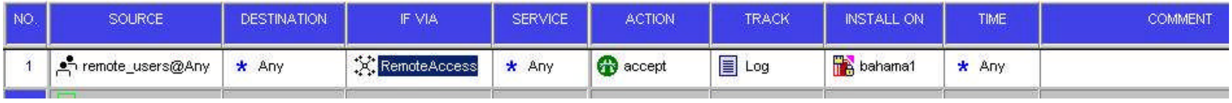
Allowed Location :

Network Objects:

Source: Any

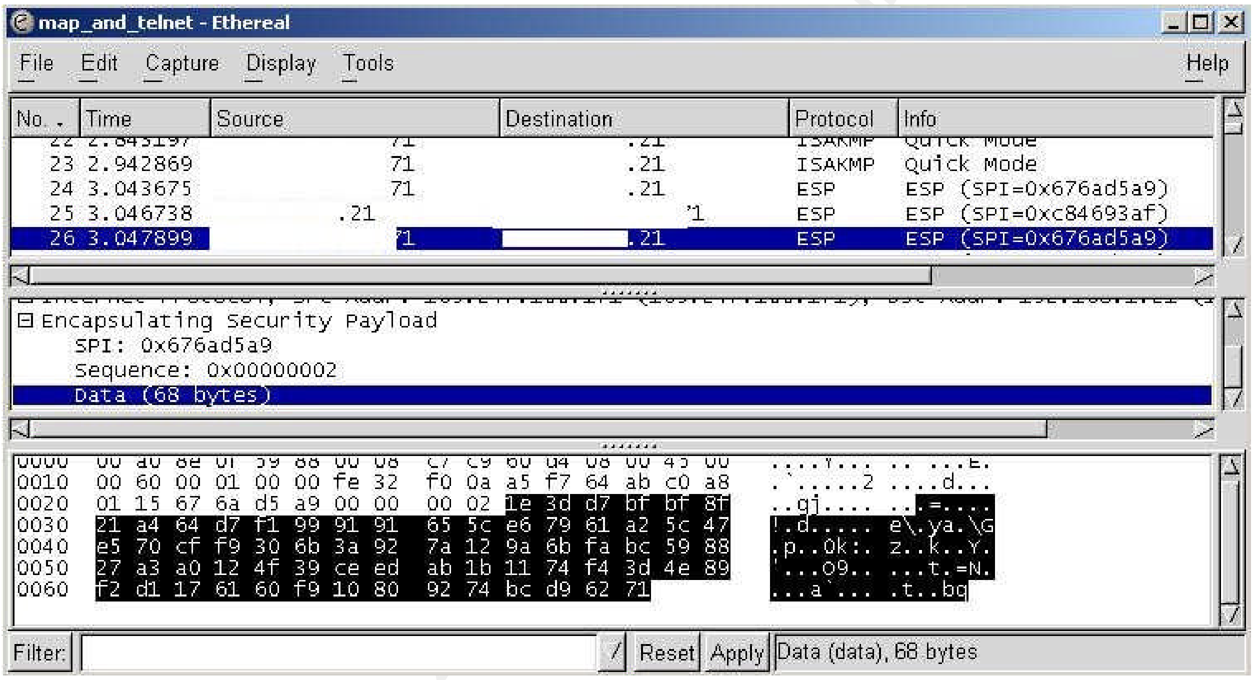
Destination: Any

The following rule permits remote access users to authenticate at the firewall and initiate communication to internal systems



NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	remote_users@Any	* Any	RemoteAccess	* Any	accept	Log	bahama1	* Any	

The following screenshot is a portion of the encrypted traffic originating from the remote client to the firewall.



map_and_telnet - Ethereal
File Edit Capture Display Tools Help

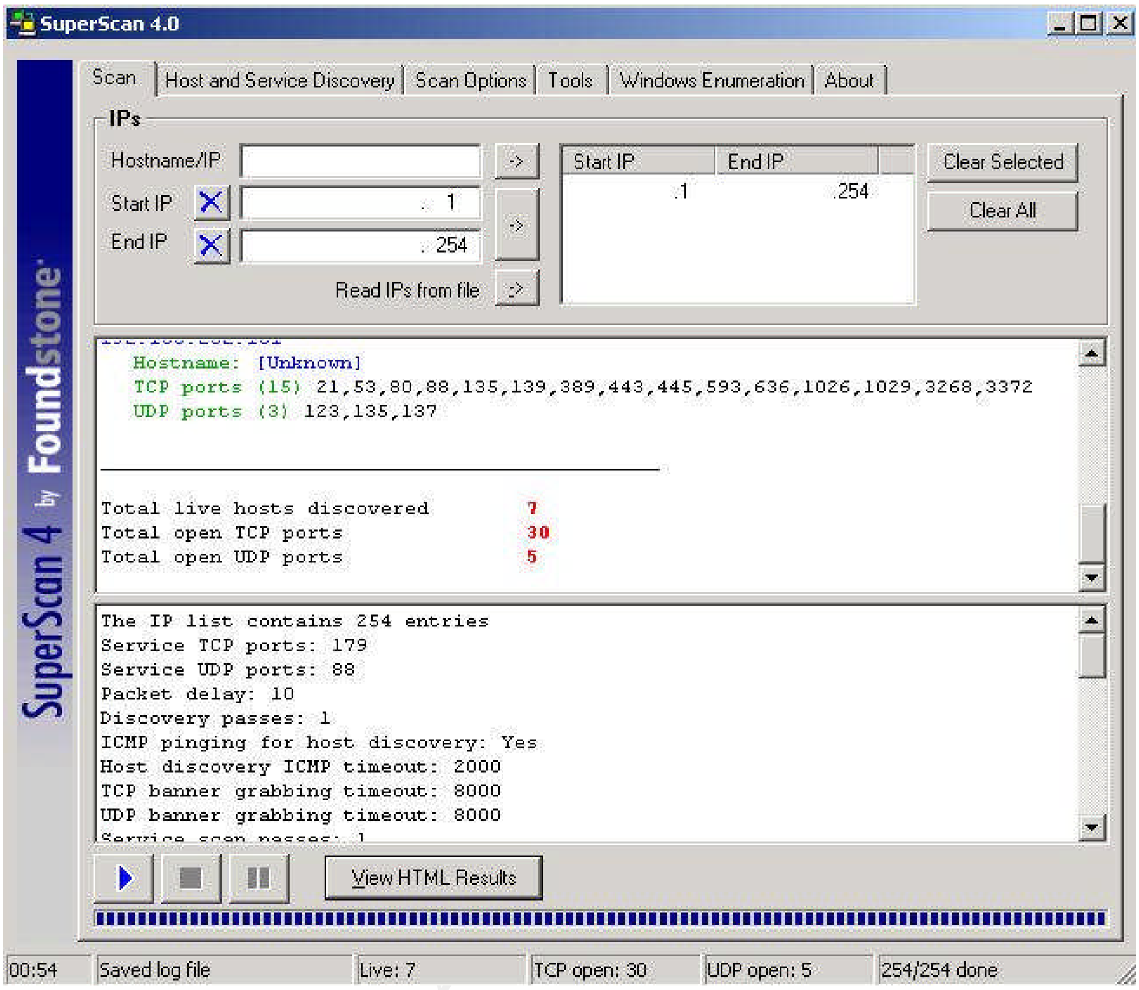
```
No. . Time      Source            Destination       Protocol  Info
   22 2.843197              71              .21    ISAKMP    Quick Mode
   23 2.942869              71              .21    ISAKMP    Quick Mode
   24 3.043675              71              .21    ESP       ESP (SPI=0x676ad5a9)
   25 3.046738           .21                  '1    ESP       ESP (SPI=0xc84693af)
   26 3.047899              '1              .21    ESP       ESP (SPI=0x676ad5a9)
```

```
⊟ Encapsulating Security Payload
     SPI: 0x676ad5a9
     Sequence: 0x00000002
     Data (68 bytes)
```

```
0000  00 a0 8e 01 39 88 00 08  c7 c9 60 d4 08 00 45 00   ....9... ..`...E.
0010  00 60 00 01 00 00 fe 32  f0 0a a5 f7 64 ab c0 a8   .`.....2 ....d...
0020  01 15 67 6a d5 a9 00 00  00 02 1e 3d d7 bf bf 8f   ..gj.... ...=....
0030  21 a4 64 d7 f1 99 91 91  65 5c e6 79 61 a2 5c 47   !.d..... e\.ya.\G
0040  e5 70 cf f9 30 6b 3a 92  7a 12 9a 6b fa bc 59 88   .p..0k:. z..k..Y.
0050  27 a3 a0 12 4f 39 ce ed  ab 1b 11 74 f4 3d 4e 89   '...O9.. ...t.=N.
0060  f2 d1 17 61 60 f9 10 80  92 74 bc d9 62 71         ...a`... .t..bq
```

Data (data), 68 bytes

SuperScan was used on the remote system to enumerate internal systems operating on the x.x.a.1-254 network segment. The following screenshot shows a portion of the SuperScan results.



Start IP: . 1
End IP: . 254

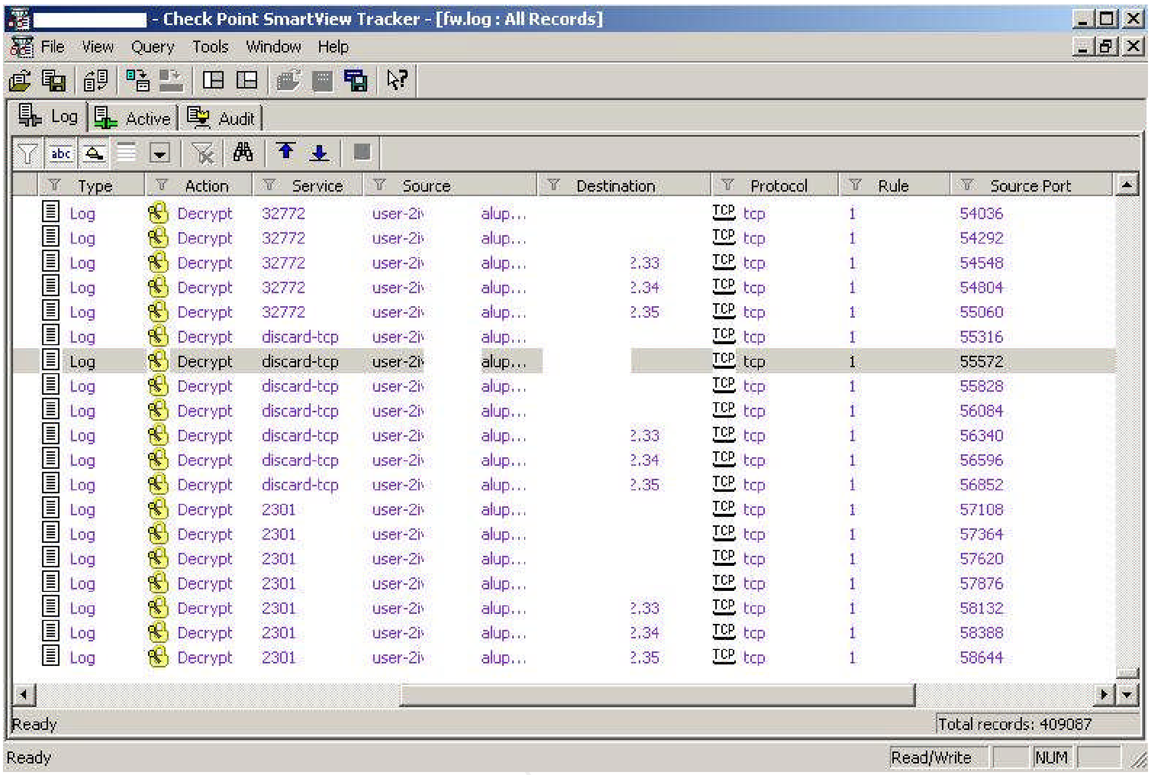
Start IP	End IP
.1	.254

```
   Hostname: [Unknown]
   TCP ports (15) 21,53,80,88,135,139,389,443,445,593,636,1026,1029,3268,3372
   UDP ports (3) 123,135,137

________________________________________________

Total live hosts discovered        7
Total open TCP ports               30
Total open UDP ports               5
```

```
The IP list contains 254 entries
Service TCP ports: 179
Service UDP ports: 88
Packet delay: 10
Discovery passes: 1
ICMP pinging for host discovery: Yes
Host discovery ICMP timeout: 2000
TCP banner grabbing timeout: 8000
UDP banner grabbing timeout: 8000
Service scan passes: 1
```

00:54 | Saved log file | Live: 7 | TCP open: 30 | UDP open: 5 | 254/254 done

The following screenshot shows the SecuRemote traffic permitted into the internal network.



- Check Point SmartView Tracker - [fw.log : All Records]
File View Query Tools Window Help
Log
Active
Audit

Type	Action	Service	Source	Destination	Protocol	Rule	Source Port
Log	Decrypt	32772	user-2i alup…		TCP tcp	1	54036
Log	Decrypt	32772	user-2i alup…		TCP tcp	1	54292
Log	Decrypt	32772	user-2i alup…	2.33	TCP tcp	1	54548
Log	Decrypt	32772	user-2i alup…	2.34	TCP tcp	1	54804
Log	Decrypt	32772	user-2i alup…	2.35	TCP tcp	1	55060
Log	Decrypt	discard-tcp	user-2i alup…		TCP tcp	1	55316
Log	Decrypt	discard-tcp	user-2i alup…		TCP tcp	1	55572
Log	Decrypt	discard-tcp	user-2i alup…		TCP tcp	1	55828
Log	Decrypt	discard-tcp	user-2i alup…		TCP tcp	1	56084
Log	Decrypt	discard-tcp	user-2i alup…	2.33	TCP tcp	1	56340
Log	Decrypt	discard-tcp	user-2i alup…	2.34	TCP tcp	1	56596
Log	Decrypt	discard-tcp	user-2i alup…	2.35	TCP tcp	1	56852
Log	Decrypt	2301	user-2i alup…		TCP tcp	1	57108
Log	Decrypt	2301	user-2i alup…		TCP tcp	1	57364
Log	Decrypt	2301	user-2i alup…		TCP tcp	1	57620
Log	Decrypt	2301	user-2i alup…		TCP tcp	1	57876
Log	Decrypt	2301	user-2i alup…	2.33	TCP tcp	1	58132
Log	Decrypt	2301	user-2i alup…	2.34	TCP tcp	1	58388
Log	Decrypt	2301	user-2i alup…	2.35	TCP tcp	1	58644

Ready Total records: 409087

Ready Read/Write NUM

Assessment:

>>The organization is not compliant with this control objective.

Remote access is not appropriately configured on the firewall. Although, only authorized users can gain access to internal systems, the configuration of individual users is too permissive; any destination within the encryption zone is permitted. In this configuration the encryption zone include all systems operating on the x.x.a.x internal network segment. Once the user authenticates at the firewall he or she will have complete network access to all internal systems. The SuperScan4 results run from the SecuRemote client system confirms the access available to remote users. The firewall log indicates the remote users access is permitted to all internal systems.

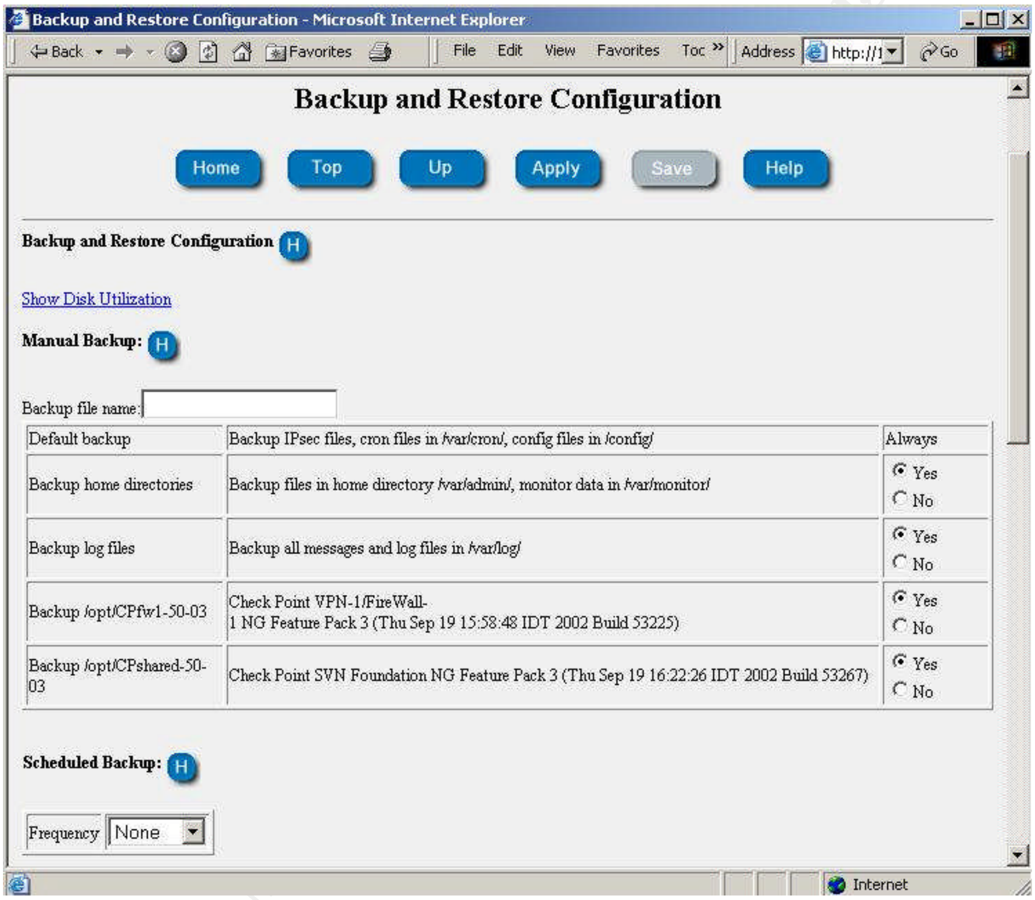
The ethereal network captures indicate that all data in transit is encrypted. However, the initial SecuRemote to Checkpoint Firewall communication revealed the organizations domain name.

CON-1

Description System and Configuration Backups

The results are based on the testing procedures defined in the CON-1 checklist item.

Results
The following screenshot represents the backup and restore configuration for the Nokia Checkpoint Firewall.



Backup and Restore Configuration

Backup and Restore Configuration H

Show Disk Utilization

Manual Backup: H

Backup file name:

Default backup	Backup IPsec files, cron files in /var/cron/, config files in /config/	Always
Backup home directories	Backup files in home directory /var/admin/, monitor data in /var/monitor/	● Yes ○ No
Backup log files	Backup all messages and log files in /var/log/	● Yes ○ No
Backup /opt/CPfw1-50-03	Check Point VPN-1/FireWall-1 NG Feature Pack 3 (Thu Sep 19 15:58:48 IDT 2002 Build 53225)	● Yes ○ No
Backup /opt/CPshared-50-03	Check Point SVN Foundation NG Feature Pack 3 (Thu Sep 19 16:22:26 IDT 2002 Build 53267)	● Yes ○ No

Scheduled Backup: H

Frequency: None

The following file was shown and represents the Checkpoint firewall backup file. This file, along with other checkpoint firewall backups created at various dates, was noted on the Nokia system in the /var/backup directory.

bahama1_nokia_fw_20031227.tgz

Assessment:

>>The organization is partially compliant with this control objective. The Checkpoint Firewall application is adequately backed-up using the Backup and

Restore Configuration feature of the Nokia IPSO operating system. The file is saved on the system in the /var/backup directory and off-system on CD.
The organization does not use the full feature set available for full and automated backups of the Nokia IPSO operating system and Checkpoint firewall application.

At time of review, we were not permitted to restore the system with the available backup file.

There were no documented backup and recovery procedures.

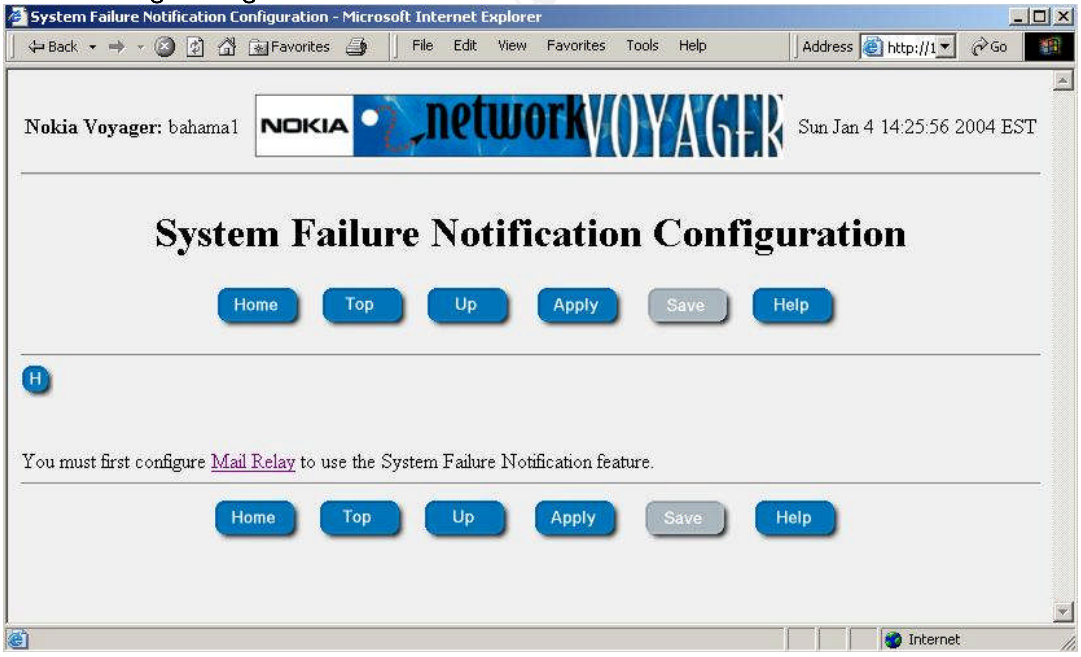
ATR-3

Description: Log alert functionality

Results:

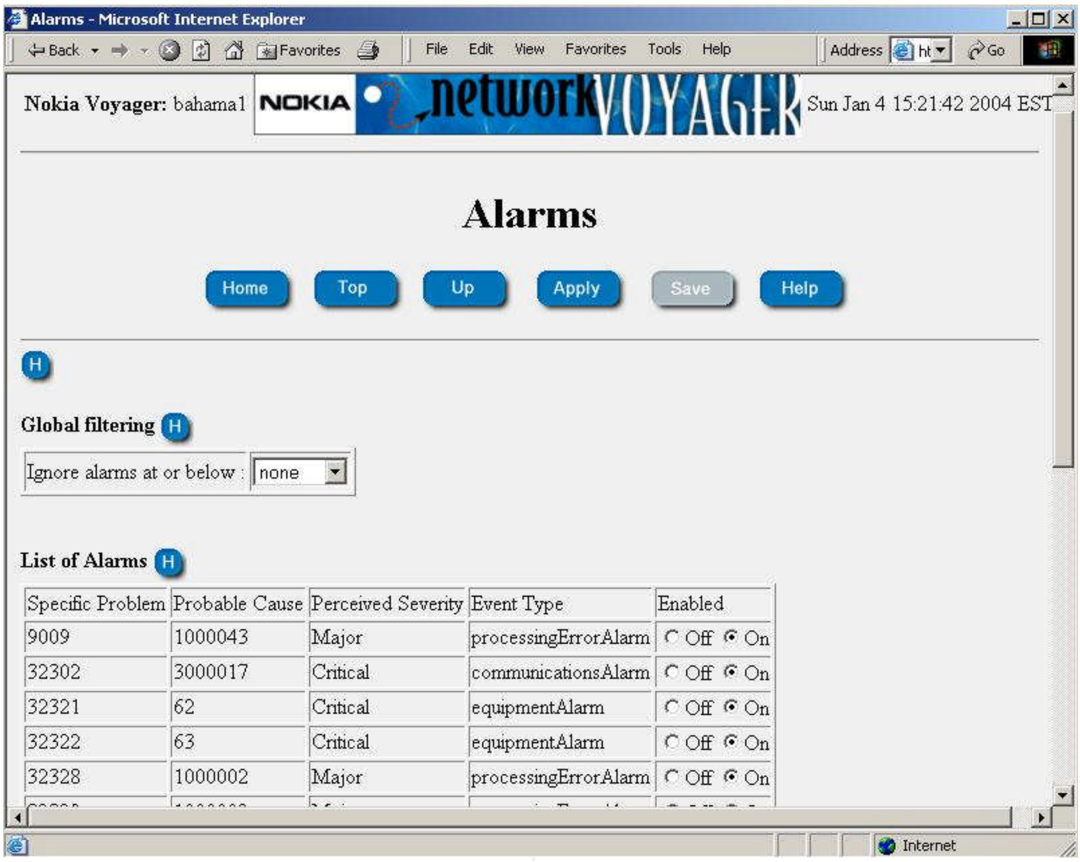
The results are based on the testing procedures defined in the ATR-3 checklist item.

The following screenshots represent the Nokia IPSO operating system logging and alerting configuration.



System Failure Notification Configuration

You must first configure Mail Relay to use the System Failure Notification feature.



Nokia Voyager: bahama1 NOKIA networkVOYAGER Sun Jan 4 15:21:42 2004 EST

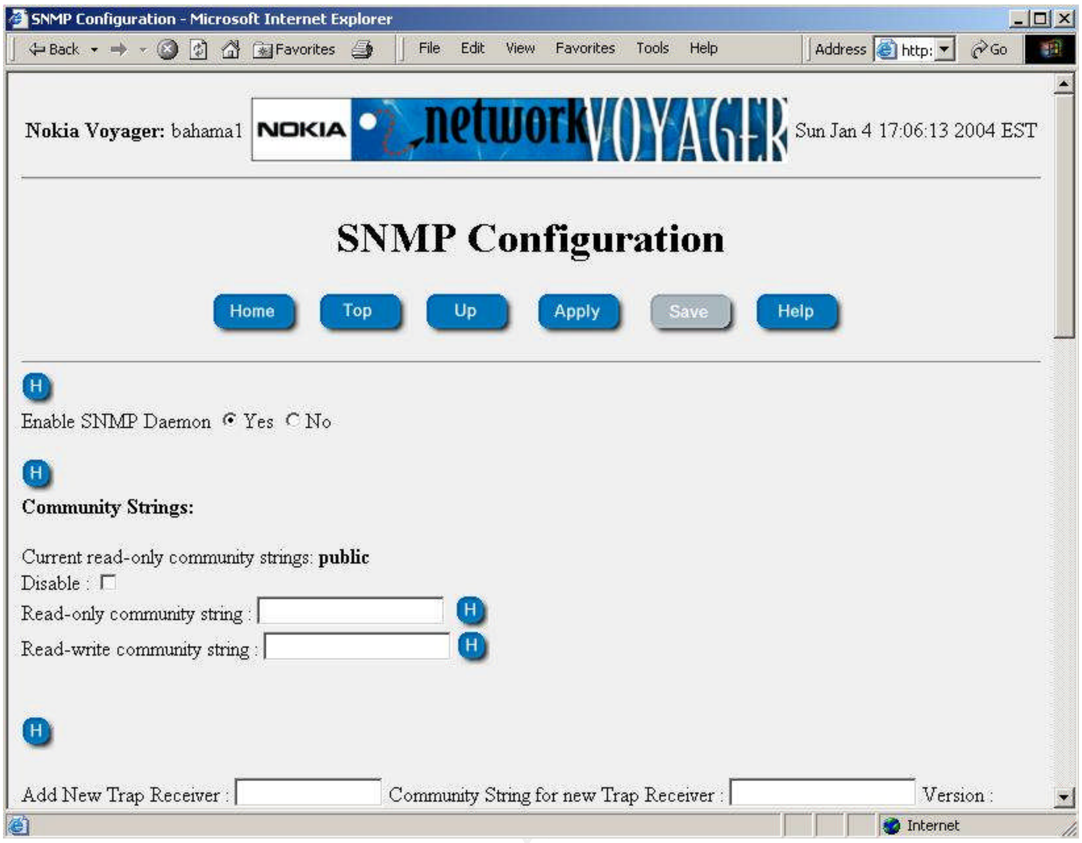
Alarms

Global filtering

Ignore alarms at or below : none

List of Alarms

Specific Problem	Probable Cause	Perceived Severity	Event Type	Enabled
9009	1000043	Major	processingErrorAlarm	○ Off ● On
32302	3000017	Critical	communicationsAlarm	○ Off ● On
32321	62	Critical	equipmentAlarm	○ Off ● On
32322	63	Critical	equipmentAlarm	○ Off ● On
32328	1000002	Major	processingErrorAlarm	○ Off ● On



Nokia Voyager: bahama1 Sun Jan 4 17:06:13 2004 EST

SNMP Configuration

Enable SNMP Daemon ● Yes ○ No

Community Strings:

Current read-only community strings: public
Disable : □
Read-only community string :
Read-write community string :

Add New Trap Receiver : Community String for new Trap Receiver : Version :

The alert features of the Checkpoint Firewall are not enabled as indicated by the track attribute for each rule.
The Log and Alert properties of the firewall are in the default configuration.

>>The organization is not compliant with this control objective.

The alerting features of the Nokia Checkpoint Firewall are not configured.

3.2 Residual Risks

A great deal of residual risk to the organization remains. In each of the information assurance and security areas of concern there exists room for improvement. The lack of documented policies, procedures and guidelines is the most apparent risk to the organization. Given the organization's business model and how information technology resources are used, improvements here will go a long way in assuring the confidentiality, integrity, availability and accountability of protected systems and resources. Clearly defined security, access control, and firewall policies will contribute greatly to securing the environment. The physical environment is well suited for the business needs of the organization. The office space is conducive to business related efforts; however, the space provides little physical and environmental security for the organization's networking and computing devices. In an ideal situation, the organization's information technology assets would be hosted in an environmentally controlled and physically secured computer/data center space. However, there is no justifiable business case for such a costly solution at this stage in the organization's development.

The choice of firewall platform is well suited to meet their business needs. The Nokia IP 330 running Checkpoint Firewall-1/VPN-1 NG provides the appropriate level of port capacity, security features and scalability to meet their requirements. However, a high degree of residual risks to their information assets remains due the overall configuration of both the Nokia IPSO operating system and Checkpoint firewall application.

In most cases the audited control objects were not met. However, in each case there are economically feasible solutions to reduce security risks to an acceptable level.

3.3 System Auditability

The Nokia CheckPoint Firewall-1/VPN-1 NG FP3 system is very auditable. Both systems, the Nokia IPSO operating system and Checkpoint firewall, have rich feature sets in this regard. The distributed nature of the security architecture posed several issues.

- The SecuRemote clients are not auditable. Giving internal network access to remote users can introduce risks not easily controlled. Who has access to the user's workstation? What access control measures are implemented on the workstation? How well is the system defended against computer viruses and worms? All of these issues can have an impact on the security of the organization's protected information assets when that remote user connects.
- Shared user accounts are used for both Nokia IPSO operating system and the firewall manager. As a result, it is fairly difficult to determine who accesses these systems with a reasonable level of certainty.
- The Windows 2000 workstation operating system that supports the Checkpoint firewall configuration client software (Checkpoint Smart Clients) had default security configurations. Minimal security logging is implemented.
- The lack of documentation made it difficult to objectively audit policies, procedures, and guidelines.
- Nokia IPSO operating system and Checkpoint firewall alerting features were not configured and enabled. I could not run tests to trigger an alert for the audit.
- It was not possible to test firewall redundancy. The firewall is a single point of failure. I could not run tests or otherwise audit dual firewall failover capabilities.

4 Assignment 4 – Audit Report or Risk Assessment

4.1 Executive summary

The Nokia CheckPoint Firewall-1/VPN-1 NG audit covered several key information assurance (IA) and security areas of concern, including:

- Policies, Procedures, and Guidelines
- Identification & Authentication
- Physical and Environmental
- Security Design and Configuration
- Continuity
- Encryption
- Audit Trail, Monitoring, Analysis and Reporting

Given the expediency with which this network, and specifically the Nokia Firewall, was stood up, the overall configuration minimally protects the organization's networking, computing, and information assets from immediate compromise. In each of the IA areas of concern noted above technical and procedural controls can be implemented to mitigate security risks to the organization. The sections below summarize the audit findings, recommend technical and procedural mitigations, and estimated cost of remediation.

4.2 Audit findings

The following exceptions to prudent security practices are noted along with any related risks to the organization and its information assets.

4.2.1 Policies, Procedures, and Guidelines

- Information Security Policies, Procedures, and Guidelines (PPG-1).

  Audit Procedure: Interviewed key staff, complete PPG checklist, reviewed available documentation.

  Findings: The organization has not formally documented any information assurance and security policies, procedures, and guideline. Staff is aware of the importance of such items and has taken steps to begin formalizing their documentation.

  Risk: All matters related to information assurance/security are without a solid foundation when formal policies, procedures and guidelines are not documented. This information guides all aspects of security including:

  - Managing and cataloging system configurations. Stable and consistent system configurations lower administration costs and support security patch and software update processes.
  - Setting system backup requirements and establishing system recovery procedures. No backup, no recovery. System hardware and software failures are inevitable, having a system backup and a documented and

practice recovery strategy will reduce the risk of prolong system unavailability.

- Establishing security patch and software update installation processes reduced the risk of exploited system vulnerabilities.
- Developing system configuration guides
- Security policy, Firewall Policy
- Change control policy will eliminate ad hoc firewall rule changes and create audit trails for administrator accountability. Proposed changes are reviewed and approved prior to implementation.

4.2.2 Physical and Environmental

- Physical Access (PEN-1).

  Audit Procedure: Inspected the facility and office space of the organization including the space housing the Nokia Firewall. Interviewed key staff using the physical and environmental security checklist in Appendix B as a guide to the discussion.
  Findings: Physical access to the Nokia Firewall and other networking and computing devices is a not adequately secured. The systems are in an office space more suited for staff. Technical and physical control mechanisms are not implemented to control physical access to networking and computing systems.
  Risk: The office space housing the firewall and various other networking and computing devices does not support physical and environmental security best practices. Although the number of networking and computing devices in use does not warrant data center like facilities, the open nature of the office environment poses significant risk of loss due to theft or unauthorized access.

- Uninterruptible Power Supply (PEN-2).

  Audit Procedure: Inspected the physical area containing the Nokia Checkpoint Firewall and interviewed staff using the physical and environmental security checklist in Appendix B.
  Findings: The UPS implementation does meet the PEN-2 control objective, however, as previously noted the space housing the Nokia Checkpoint firewall was designed and is more suited for office personnel. Environmental control and monitoring technologies are not available. Most notable are water sprinkler system heads above the computing devices.
  Risk: In an office environment, it is appropriate and likely a requirement to have water sprinkler systems. However, if triggered, these sprinkler systems will damage computing equipment.

4.2.3 Security Design and Configuration

- Nokia IPSO operating system security (SDC-3).

Audit Procedure: The Nokia IPSO system configuration was reviewed. The CheckPoint firewall application was disabled to permit unfiltered network security scans of the Nokia IPSO operating system. Scans were completed using the nmap and Nessus security scanners.
Findings: The Nokia is running IPSO 3.6 FCS6, Jan. 2003 release. The scan results indicate that the Nokia IPSO operating system is vulnerable to several types of network-based attacks when the firewall software is disabled. The IPSO operating system application vulnerabilities have been addressed in later releases of the operating system. The system is also implemented with a remote management configuration permitting clear-text telnet and http access.
Risk: The primary risk here is unauthorized access when the firewall software is disabled. The firewall application maybe disabled for maintenance or troubleshooting purposes on the Nokia. There is also the ability to enable IP forwarding, effectively turning the firewall into an IP router.

- Firewall application security (SDC-4).

  Audit Procedure: The checkpoint firewall application is in semi-distributed architecture. The Checkpoint enforcement and management modules are both on the Nokia platform. However, firewall management is handled remotely via a desktop computer system running Windows 2000 workstation operating system. Reviewing the Win2K workstation was not in the scope of this audit. However, there is a trust relationship between the firewall and management client by way of the firewall's configuration, policies and rulebase. It was determined that the best approach in auditing the firewall's application security was to scan the system from an untrusted host and a trusted host.

  Findings: The scan results indicate that the Nokia Checkpoint Firewall is adequately protected from untrusted hosts. When scanned with nmap traffic is dropped. Nessus based scans and attacks were either dropped or successfully blocked by Checkpoint's SmartDefense tool. However, scans and attacks from the trusted host were permitted through. The nmap scan run against the firewall from the trusted host indicated that in addition to the checkpoint firewall-1 NG specific open application ports, telnet, HTTP, DNS, DHCP client, SNMP, and syslog services are running. Nessus also revealed application specific vulnerabilities.

  Risk: A trust relationship exists between the Nokia Checkpoint Firewall and the management client. The security configuration of the Win2K workstation operating system on the management client as well as its physical security may severely weaken the security posture of the entire Firewall system. Again, without the benefit of policies, procedures and guidelines to direct security configurations and access controls the system is open to numerous vulnerabilities.

- Remote management activity security (SDC-5).

  Audit Procedure: Reviewed the Nokia IPSO management configuration settings. Reviewed the Checkpoint Firewall NG Management configuration settings. Used a network analyzer to capture network traffic between the firewall management client and the Nokia Firewall.

  Findings: A review of the Nokia remote management configuration settings indicate that telnet and http is enabled for remote IPSO operating system management. Network data transmission captures of telnet and http logon traffic revealed administrator account userid and password.

  The checkpoint Global Properties settings permit firewall-1/vpn-1 control connections. Firewall-1/VPN-1 captured connection control transmissions were encrypted.

  Risk: Remote management connections to the Nokia IPSO operating system are clear text and vulnerable to capture. Remote management of the Checkpoint firewall application is encrypted. Note that the same account password is used for IPSO and firewall application management.

4.2.4 Continuity

- System and Configuration Backups (CON-1).

  Audit Procedure: Review backup and recovery policies and procedures. Review Nokia IPSO configuration to determine backup implementation. Review the backed-up files and data. Perform a full backup and recovery on the Nokia Checkpoint Firewall using the provided back-up and recovery procedures.

  Findings: Automated backups are not configured on the Nokia firewall. Firewall manager backups are not implemented.

  Risk: Depending on the owner's service contract Nokia hardware can be replaced between 1 and 5 business days, however with out a proper back-up of the IPSO image and configuration actual downtime could last an additional 24 to 48 hours as the system configuration is brought back to an operational production state, costing considerable financial resources and lost productivity.

4.3 Audit recommendations

As a result of the audit findings and risks noted above the following recommendations are presented.

1. IT staff and the organization's management needs to document policies, procedures, and guidelines. The following areas should be addressed.

Keep in mind that these are dynamic documents that will mature and evolve as the organization develops.

- ✓ Security Policy
- ✓ Configuration Management Process
- ✓ Backup and Recovery Procedures
- ✓ Patch Management Process
- ✓ Configuration Guidelines
- ✓ Change Control Process
- ✓ Firewall Policy

All documentation should be version controlled and intranet web accessible.

2. The organization needs to invest in two water resistant, ventilated, lockable computer racks. The racks should be positioned away from sprinkler heads. Although the office is not environmentally controlled for temperature and humidity, conditions are within acceptable levels for the eight networking and computing systems in use. It is also recommended to request that cleaning staff perform their tasks during normal business hours.
3. Secure the Nokia IPSO operating system
    a. Upgrade the IPSO operating system to IPSO 3.7.1 Build004. This version fixes several vulnerabilities including: IP cluster DoS; script injection; OpenSSH; and OpenSSL vulnerabilities.
    b. Disable all clear-text protocols used to access the Nokia IPSO operating system.
    c. Enable SSH and HTTPS (SSL) for remote management purposes.
    d. Create individual accounts for each administrator.
    e. Disable snmp
    f. Configure automated backups of the IPSO image and checkpoint firewall application.
4. Secure access to the firewall application
    a. Upgrade the firewall software to the latest version that includes CheckPoint Application Intelligence feature. NG with Application Intelligence (R55).
    b. Restrict management access to the firewall. (See 5.a and 5.b below.)
    c. Create individual accounts for each administrator
    d. Use widely available best practices to secure and otherwise lockdown the firewall management client workstation.
    e. Provide a means to physically secure the firewall management client workstation (e.g. secure in a lockable cabinet or provide cable locks as a theft deterrent.)
5. Implement a more granular rulebase
    a. Restrict access to the Nokia Checkpoint Firewall to include only the firewall management client workstation. The rule should only permit SSH, HTTPS, CPMI (18190/tcp), and CPRID (18208/tcp).

   b. Uncheck the following Firewall-1 Implied Rules:
      i. Accept VPN-1 & Firewall-1 control connections
      ii. Accept CPRID connections (SmartUpdate)
      iii. Accept dynamic address Modules' DHCP traffic
   c. Deny access to the firewall manager from all other networks and workstations.
   d. For the internal network, add individual workstations to the rule permitting DMZ, wildcard, and Internet access. Remove the internal network object.
   e. Implement client or user authentication from 'wildcard' network that contains both wired and wireless client workstations.
   f. Redefine the DMZ network. (See 6 below)
   g. Subscribe to Checkpoint's SmartDefense. Implement all policies to defend against network-based application attacks.

6. Based on discussions with the management and IT staff, the DMZ as it is currently used does not require Internet accessibility. The organization's website is static and only provides basic corporate and contact information.
   a. Move the public web server content to a web hosting service that provides security, secure email, and 24/7 technical support.
   b. Deny public Internet access to the redefined DMZ.
   c. Include the redefined DMZ in the SecuRemote encryption zone for remote access.
   d. If testing/validation for ongoing business purposes requires Internet accessibility, it should be permitted to only known hosts and restricted to applicable ports and protocols.
7. Implement more granular access to SecuRemote users. Restrict the remote users to specific systems and services.
8. Enable alerting to trigger when remote users access the organization's resources. Monitor logs.
9. Install host-based firewalls on critical system servers to provide an addition layer of defense.
10. Implement backup and recovery strategies on critical systems. Utilize the available features in the Nokia IPSO operating system.
11. Eliminate the Nokia as a single point of failure by implementing dual firewall in failover configuration.
12. System Failure warning alerts should be configured on the Nokia. Upgrade the support contract to improve hardware replacement timelines.

4.4 Costs

Recommendation	Time	Cost
Develop and Document information assurance policies, procedures, and guidelines	120 hours ▸ 40 hours--Security Consultant to support internal policy development effort. ▸ 80 hours combined for IT staff and Management	$4000—Consultant Fees $50—Hard copy documentation
Secure Server Rack (26U Universal Server Rack Mount Cabinet 19 Inch Network Equipmnet Enclosure 36" Deep)	8 hours ▸ IT staff relocates network and server equipment to racks ▸ Tests all systems for correct functionality	$2500—Equipment
Checkpoint Firewall-1 Training (VPN-1/Firewall-1 Management II – NG)	3 days off-site training	$2000—Course costs and travel (courses are available locally)
CheckPoint SmartDefense Service	4 hours ▸ Configuration and testing	$1,000—CheckPoint subscription fee
Norton Internet Security Includes: ▸ Norton AntiVirus™ Professional ▸ Norton™ Personal Firewall: ▸ Norton™ AntiSpam	8 hours ▸ Installation, configuration, and testing	$400—Software
Firewall redundancy ▸ Hardware - Nokia IP 330 - Dual port interface card ▸ Software - Checkpoint Express 50 user license (includes firewall-1/vpn-1, SecuRemote, SmartDefense)	24 Hours ▸ Installation, configuration, and testing	$2500—IP 330 Base System $1000—Dual-port Ethernet card $3500—Software

Backup software (Retrospect Small Business Server v6.5)	8 hours ▸ Installation, configuration, and testing	$260—Software
Implement Nokia and Firewall configuration and rulebase recommendations	32 hours ▸ Configuration and testing	$0
Web Hosting Service for Informational website and email. The following provides a web site hosting directory. http://www.webhostinginspector.com	16 hours ▸ Setup, Configuration and testing	Approx. $10.00/month.
Undocumented costs include Network downtime—In most cases network downtime is required. In each case the tasks can be completed during non-business hours. 40-Hour workweek—IT staff working 16 hours during non-business hours may not be available during normal business hour to maintain a 40-hour work week. Management Hours—Management hours are more costly. Hours not billed to their clients directly impacts revenue.		

4.5 Compensating Controls

The goal in any security effort is to apply the best available technologies and practices in line with the value of the organization's information assets and business model. Although there are significant security improvements needed in this organization, attempting to achieve absolute security is impractical and cost prohibitive. In light of this, several compensating controls exist.

1. Harden all windows-based systems and apply the latest security patches.
2. Utilize TCP/IP filtering capabilities on all windows-based system where appropriate.
3. Currently there is no compelling requirement for public access to the DMZ. Allow access to only authenticated SecuRemote users. Revisit the issue as the organization develops.
4. Periodical assess the network using open-source security tools such as nmap and Nessus.
5. IT staff should regularly review security focused web sites.
6. Management should budget for security related training.

Appendix A—References

1. Alberts, C., Dorofee, A. Managing Information Security Risks: The OCTAVE Approach. New York, NY: Addison-Wesley. (2002)

2. Anonymous. Maximum Security, 3rd Edition. Indianapolis, IN: SAMS. (2001).

3. Atkins, D., Buis, P., et al. Internet Security Professional Reference. Indianapolis, IN: New Riders. (1996).

4. CACI International Inc. "Computer Security Threats" URL: http://www.caci.com/business/ia/threats.html (September, 2003).

5. Garfinkel, S., Spafford, G. Practical UNIX & Internet Security, 2nd Edition. Sebastopol, CA: O'Reilly. (1996).

6. Hash, J. S. "RISK MANAGEMENT GUIDANCE FOR INFORMATION TECHNOLOGY SYSTEMS" URL: http://csrc.nist.gov/publications/nistbul/itl02-2002.txt (February, 2002)

7. Information Assurance Support Environment, URL: http://iase.disa.mil (September, 2003).

8. McClure, S., Scambray, J., Kurtz, G. Hacking Exposed Network Security Secrets & Solutions. New York, NY: Osborne/McGraw Hill. (2001).

9. Northcutt, S., Zeltser, L., Winters, S., Kent Fredrick, K., Ritchey, R. W. Inside Network Perimeter Security. New York, NY: New Riders. (2003).

10. Schetina, E., Green, K., Carlson, J. Internet Site Security. New York, NY: Addison-Wesley. (2002).

11. Spitzner, L. "Auditing Your Firewall Setup" URL: http://www.spitzner.net/audit.html (December, 2000).

12. Spitzner, L. "Building Your Firewall Rulebase" URL: http://www.spitzner.net/rules.html (December, 1999).

13. Spitzner, L. "Intrusion Detection for FW-1: How to Know When You Are Being Probed" URL: http://www.spitzner.net/intrusion.html (December, 2001).

14. Stoneburner, G., Goguen, A., and Feringa, A. "Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology Special Publication 800-30" URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (October 2001).

15. Tanase, M. "IP Spoofing: An Introduction" URL: http://www.securityfocus.com/infocus/1674 (March, 2003).

16. Titpon, H.F., Krause, M. Information Security Management Handbook, 4th Editition. Boca Raton, FL: Auerbach. (2000).

Appendix B—Physical and Environmental Security

Physical Security Checklist	Compliant		Comment
	YES	NO	
Is access to the building restricted (key, code, electronic card)?			
Is there a process for issuing keys, codes, and/or cards that requires proper authorization and background checks?			
Are access logs kept for the computer room?			
Are access logs regularly reviewed?			
Is the computer room isolated or combined with other workspaces?			
What hours do people have access to the computer room?			
Are security and networking devices secured with in the computer room?			
Is the floor elevated?			
Are network cables accessible?			

Environmental Protections Checklist	Compliant		Comment
	YES	NO	
Are smoke detectors present?			
Is a firewall suppression system present?			
Are there fire extinguishers in the room?			
Are there manual fire alarms?			
Are UPS (uninterruptible power supply) devises installed?			
Are emergency power-off switches present inside and outside the computer room?			
Is the temperature of the room set to manufacturer standards?			
Is ventilation to the room adequate?			

Appendix C—Management and IT Questionnaire

1. What is the purpose/mission of the organization?

2. Describe how the network is used in general?

3. How do independent consultants use the network?

4. How is the Internet used?

5. How is the internal network used?

6. How is the DMZ used?

7. What is the primary purpose of the wildcard network?

8. What are the company's most valuable assets?

9. How is the information maintained?

10. What role does information security play in the success of the organization?