Global Information Assurance Certification Paper

A Baseline Audit of an Astaro Security Linux™ 4.008 Firewall. An Auditors Perspective

GIAC System and Network Auditor (GSNA)

Practical Version 2.1

Candidate: Chris Lethaby

SUBMISSION DATE: 17 JULY 2003

TABLE OF CONTENTS

Abstract:

In this paper we address the baseline audit of Astaro Security Linux 4.008, an application gateway firewall. Through a process of co-operative policy development with the client, and industry best practice research, we produce a baseline checklist against which the firewall's multiple controls are tested. We reported that over ninety-nine percent of the checklist's best practice standards for firewall performance were either met or exceeded. We conclude, through quantitative risk analysis, that the firewall would deliver a positive return on security investment, and considerably lower I.T related risk within the client's organization.

1 ASSIGNMENT 1 – RESEARCH IN AUDIT, MEASUREMENT, PRACTICE AND CONTROL

> ***Baseline;***
>
> *Pronunciation: 'bAs-"lIn*
>
> *Function: noun*
>
> *Usage: often attributive*
>
> *Date: 1750*
>
> *1 : a line serving as a basis; especially : one of known measure or position used (as in surveying or navigation) to calculate or locate something*
>
> *2 a : either of the lines leading from home plate to first base and third base that are extended into the outfield as foul lines b : BASE PATH*
>
> *3 : a boundary line at either end of a court (as in tennis or basketball)*
>
> ***4 : a set of critical observations or data used for comparison or a control***
>
> *5 : a starting point <the baseline of this discussion>*
>
> *From Merriam-Webster Dictionary online; http://www.m-w.com*

1.1 Setting The Scene

The audit I present concerns itself with an **Astaro[1] Security Linux™ 4.008** Firewall. As I am not able to publish the results of work I perform in my current role due to corporate policies, it was necessary to develop a scenario that would allow me to exhibit the requisite skills to pass the GSNA course which include the "soft" business competencies required to negotiate and manage a successful audit.

Questions the scenario attempts to answer are:

- Who is our customer?
- Who are we working with?
- Who is setting the scope?
- Who is performing the audit?

[1] http://www.astaro.com

- Who are we reporting to?

Only by attempting to answer these questions can we present a paper that addresses all the requirements of the assignment. Without the scenario vehicle, our audit would have been left to focus on the technical skills and analysis, missing we believe, much of the core value within the GSNA course.

In our scenario, the Astaro Security Linux firewall has been selected for use as an Internet gateway by an SME company named SimCoat Plastics, a fictitious plastics injection moulding and extrusion manufacturer. Think of this company as the 'everyman' of small and medium sized enterprises who make export widgets and are yearning to be an international player through the development of an Internet presence.

SCP has recently undertaken to expand their online presence and migrate their email from their ISP, to an in-house deployment, while at the same time redesigning their existing Corporate Internet access. Previously this used a simple NAT solution via a Cisco 3620 border router.

The development of a new infrastructure with public services necessitated that they consider the addition of a DMZ, while there were additional requirements from management to provide detailed Internet usage logging, anti-virus protection for Email, and Content filtering to mitigate Cyber-slacking and inappropriate use of company resources. These all require some form of application level proxies.

After surveying the market, Alan, the local Network administrator has proposed the use of Astaro Security Linux, a Linux based firewall solution that provides all the required functionality specified to him by management.

While Alan has the support of the Information Systems manager, senior management has recognized the importance of this infrastructure to the company's 5-year strategic vision, and has opted to provide governance of the development process through the establishment of an ongoing InfoSys assurance program for the new Online Infrastructure.

Part of this in-house developed process is to establish pre-deployment "best practice" baselines for critical infrastructure elements such as the Astaro Firewall, with ongoing system monitoring designed to provide assurance that the system state is being maintained, between yearly compliance audits.

1.2 Enter the auditors.

We have been contacted by SimCoat Plastics via phone to provide a 'Best Practice' baseline audit of a new firewall installation they have in development.

After a short phone conversation with them, we made an appointment for an icebreaker meeting at SCP for the following week, where we outlined our audit process and developed the audit scope.

1.3 Audit Process.

Our Audit process follows a Seven Step plan.

1. Engagement
    - Initial Scope exploration
    - Contractual negotiation
    - Information Gathering

2. Audit Planning
    - Risk Assessment
        - Qualitative, or
        - Quantitative
    - Data collection
    - Research
    - Control Checklist development and consultation.
    - Final scope definition
    - Timeline development
3. Entrance Conference
    - Introduction
    - Audit rationale discussion
    - Audit subject definition
    - Scope definition
    - Role definitions
    - Process description
    - Timeline presentation.
4. Fieldwork
    - Audit plan execution
5. Report Preparation
6. Exit Conference
    - Present Technical findings to Business and Technical specialists
    - Present proposed mitigation strategy for discovered risks where residual risk is unacceptably high.
7. Management report
    - High Level management précis.

Attendee's at the engagement meeting included the I.S Manager, the Financial Controller, and the Operations Manager.

During the meeting we were told that the audit target is currently deployed in an isolated development network that completely mimics the production deployment, and that Astaro Security Linux™ 4.008 has been installed and configured in the test environment by Alan and Sven, the company's network administrator and senior support engineer respectively.

1.4 Audit Scope

After some discussion and clarification, the following audit scope was proposed.

The audit is to consider the target system and:

1. Perform a Risk Assessment to evaluate the overall risk the company faces to their Internet infrastructure and express this in financial terms suitable for presentation to senior management.
2. Assess the importance of the Firewall as a technical control in mitigating this risk and express this in terms suitable for presentation to senior management.
3. Baseline the connectivity requirements between firewall domains based on corporate policies and industry best practices.
4. Provide guidance and assistance in the development of a Baseline Firewall Policy that meets company policy and 'best practice' guidelines.
5. Baseline the firewall's performance in translating the Firewall Policy into effective technical controls.
6. Comment on the overall appropriateness of the chosen Firewall technology based on Industry 'best practices' and corporate policy.

This scope aims to assist the customer develop a security baseline configuration and deployment for their firewall through consultation, co-operation and negotiation in an open, transparent and professional process.

Outside the scope of this particular audit:

- Physical Controls
  - Site and Building Perimeter Security
  - Site and Facility Access Controls
  - Personnel Work Area Separation
  - Power, and Network Cabling
  - Fire Detection and Suppression
  - HPAV
  - Offsite Backups
- Administrative Controls
  - Procedural and process controls.
  - Personnel Controls
  - Hiring/Exit
  - Security Awareness Training
  - Testing methodologies
  - Segregation and Rotation of Roles
  - Disaster Recovery Plans
- Technical Exclusions
  - ISP Managed Border Router
  - Switches, Hubs and other Network infrastructure
  - All other computer systems.

At the end of this engagement meeting, we requested network diagrams, corporate policies, organization charts, and any other operational policies or supporting documentation the attendees may have had relevant to the firewall.

We explained that receipt of these documents was a prerequisite for the development of an audit plan that reflected both the company's corporate policies and industry best practice models.

On return to our offices, we emailed each attendee our standard Qualitative Risk Assessment form for them to fill-in and return. These forms were collated for use later in developing our risk analysis.

1.5 Describe the system to be audited.

The system is a generic 1U Intel Pentium III 800 MHz server with 512MB Ram, a 4mb on-board PCI video card, dual power supplies, 4 PCI Network Interface Cards, and twin 18Gb SCSI Hard-drives configured in RAID 0 running the Linux based **Astaro[2] Security Linux™ v. 4.008** firewall distribution.

Astaro Security Linux™ 4.0 is one of a breed of emerging firewall distributions based on a Linux 2.4.x kernel with Netfilter and IPTables. This particular application firewall distribution is described as having the following features;

Firewall

- Stateful Packet Inspection Firewall
- Security Proxies for HTTP, HTTPS, SMTP, POP3, DNS, IDENT, SOCKS
- User Authentication (Local User Database or remotely via Radius, Windows NT/2000/XP, Microsoft Active Directory, LDAP, Novell Directory Services)
- User definable Service and NetworkGroups, standard services are predefined
- DoS Protection (ICMP flood, TCP SYN flood, UDP flood, Smurf, Trinoo, IP Spoofing)
- Portscan Detection

System Management

- Remote Administration via WebAdmin (128-bit encrypted)
- System and Pattern Updates via Internet (PGP secured)
- Logging via Syslog, SNMP, ASCII, WELF (WebTrends format)
- IP Accounting
- Out-of-band Management via External Modem
- SelfMonitor for maximizing Uptime
- Network Diagnostic Tools
- Complete Configuration Backup and Restore
- Predefined Reports
- Hot Standby (via Serial/Ethernet,synchronizes configuration)
- Optional: Astaro Global Configuration Manager

IPSec VPN

- Net-to-Net, Host-to-Net, Host-to-Host
- NAT Traversal, Virtual IP

[2] http://www.astaro.com

- Authentication via passphrase (PSK), certificates (X.509v3) or keys (RSA)
- PKI Management of X.509 certificates
- Algorithms via AES (Rijndael), 3DES,Blowfish, Twofish, Serpent, MD5, SHA1 or SHA2
- Deflate Compression
- Perfect Forward Secrecy (PFS)
- Dynamic firewall settings per IPSec connection/IPSec user
- Option: Astaro Remote IPSec Client (for MS Windows PCs)

PPTP VPN:

- Host-to-Net
- MPPE 40/ Data Encryption
- MSCHAPv2 Authentication
- Radius authentication for PPTP user
- Dynamic firewall settings per PPTP user

Content Filter:

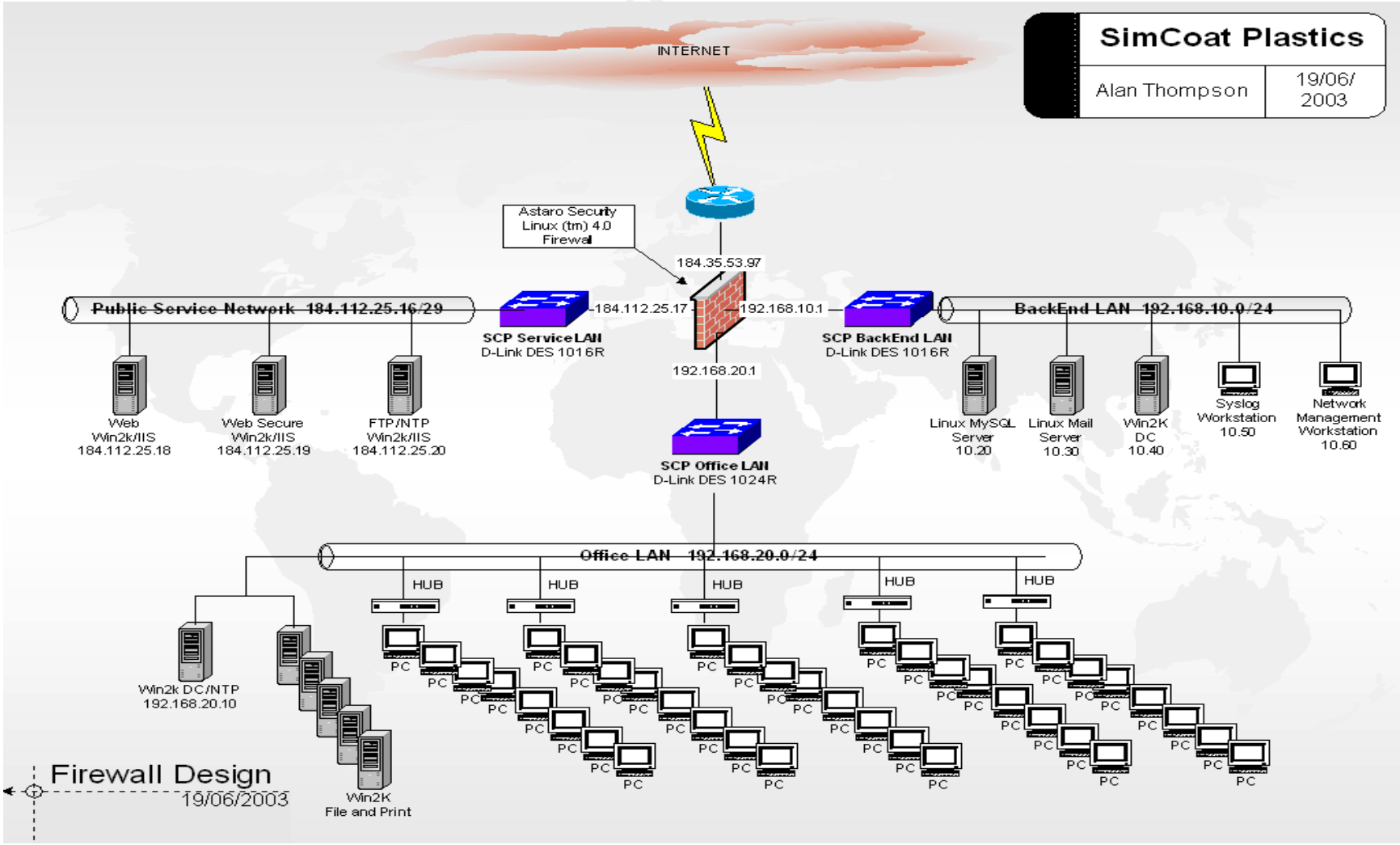
- Web Code Filter for dangerous contents (e.g. ActiveX)
- Web Privacy Filter (e.g. Cookies, Web Bugs)
- Spam Protection (extensive toolkit)
- User definable string filters for HTTP/SMTP/POP3
- Transparent encryption of SMTP traffic (TLS)
- Optional: Virus Protection for SMTP/POP3 (daily updated virus scanner)
- Optional: Surf Protection for HTTP (daily updated URL list), Black/White List

The network diagram below and the attached SimCoat Plastics Firewall Policy (see Appendix 7.1), that arrived via email from Sarah the I.S manager, details the proposed network architecture and services delivered by the Astaro firewall.

As the firewall protects both the DMZ service network and the corporate LAN, it is the central access and egress control from the Internet to the public services offered by SimCoat Plastics, while also doubling as a corporate access gateway to the Internet.

Within the design, this application gateway firewall must be capable of providing Stateful Packet Inspection, Network Address Translation for corporate network access, application proxies for DNS, FTP and HTTP Internet access, and an SMTP proxy for email.

Figure 1-1. Network Design -Logical



1.6 Evaluate the Risk to the System

Our agreed scope states that we must:

> *"Perform a Risk Assessment to evaluate the overall risk the company faces in to their Internet infrastructure and express this in financial terms suitable for presentation to senior management."*
>
> *"Assess the importance of the Firewall as a technical control in mitigating this risk and express this in terms suitable for presentation to senior management."*

For the first of these, we must use a Quantitative RA approach, while the second calls for a subjective assessment based on our InfoSec expertise.

1.6.1 Definition of Terms

Often during an engagement, we encounter a number of misconceptions surrounding the terms used to describe Security and Audit processes. People often use terms such as threat, risk and exposure interchangeably when they are in fact different features of the security landscape.

We find it useful to define the following terms at the outset so each attendee may understand the audit process and goals more fully.

Risk , the probability that a *Threat* will take advantage of *Vulnerability*.

Threat , any potential danger to information or a system.

Vulnerability, is a software, hardware or procedural weakness that may provide an attacker an exploitable entry point to the resource or system that enables them to exercise their threat.

Exposure is an instance of a *Threat* successfully exploiting a *Vulnerability* that produces a measurable negative effect in terms of information or system Integrity, Confidentiality or Availability.

Inherent Risk is the natural measure of risk associated with a potential exposure when no mitigation controls are taken into account.

Residual Risk is risk associated with an exposure when *Risk* mitigation controls are taken into account.

1.6.2 Risk Assessment

The *Information technology – Code of practice for information security management ISO/IEC 17799:2000(E)* states that a Risk Assessment is:

"… a systematic consideration of:

> *a) the business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets;*
>
> *b) the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.*

While a Risk Assessment (RA) is a fundamental prerequisite of ISO 17799, there are no prescriptive approaches to measuring risk, nor are there any approved methodologies outlined in the standard. It is widely accepted however that two general approaches to RA are commonly taken, Quantitative and Qualitative.

In a Quantitative approach, real values are applied to the cost of security failures and the controls applied to mitigate an exposure. Each of the parameters that are evaluated in a RA such as asset value, threat probability, vulnerability frequency, exposure cost, and mitigation cost are entered into a Risk Calculation to arrive at a Quantitative measure of Risk.

In a Qualitative assessment, risks, assets and exposures are assigned qualitative values relative to the seriousness of impact or loss, or sensitivity of assets. In many ways these are simpler to perform as the Auditor can develop a Qualitative assessment through techniques such as one-on-one interviews with non-technical personnel, questionnaires phone interviews and panel brain-storming sessions.

1.6.2.1 Audit Universe Identification

Section 4.1 of the *ISACA IS Auditing Procedure #1 IS Risk Assessment Measurement*, states that;

> *"IS audit risk assessment measurement is a methodology to produce a risk model to optimise the assignment of IS audit resources through a comprehensive understanding of the organisation's IS environment and the risks associated with each auditable unit.*

Section 4.2 then expands on this:

> *The objective of a risk model is to optimise the assignment of IS audit resources through a comprehensive understanding of the IS audit universe and risks associated with each universe item.*

While the context of the above quotes take the IS Audit Universe to mean every system within an organizations IS infrastructure, the use of a risk based approach to evaluating a single system in the assignment of audit resources is no less important. This approach allows us to concentrate on what is important within the context of our audit scope and gives definition to the materiality of each control.

To perform a Risk Assessment it is first necessary to understand the function of the audit universe and the nature of the threats against this set of auditable controls. In the scope of our Audit assignment the Audit Universe is a single system though the auditable controls which this system applies within the IS infrastructure are multiple.

1.6.2.2 Understanding the Audit Subject

Firewalls by their design are centralized network access controls that must reliably transform corporate policies into effective technical controls, while providing reliable access and egress to corporate and public services. As such, the firewall does not generate revenue nor is it a part of the SimCoat Plastics' core business function of producing plastic widgets.

The firewall is an example of a Risk Management control within the I.T infrastructure, designed in this case to reduce the risk of an exposure to both the public web services and the corporate network. To evaluate the risk within the context of the audit we must define each control and consider what exposure a failure of the control would have on SimCoat Plastic's I.T infrastructure and by implication it's business.

From the SimCoat Plastics policy library and the Business Case documents we have discerned that the controls they wish to effect via the new firewall are:

Table 1-1. Security Control Objectives effected by the Firewall.

Control Objective 1	Application of access and egress controls via Stateful Packet Filtering between Zones, with emphasis on controlled Internet access to exposed public servers.
Control Objective 2	Proxy based WWW access, authorisation, and logging with content filtering aimed at reducing Cyber-slacking.
Control Objective 3	Anti-Virus SMTP and POP3 Proxying of Corporate Email.

The next step is to consider the threats against each of these controls and assess the controls in a more granular manner.

1.6.2.3 Threat Universe:

Firewalls are the primary point of attack for external threats and may also be the target of internal threats by disgruntled employees.

The nature of the threats against the firewall, its services and controls from any vector within the local network or Internet may include but is not limited to:

Application Attacks against services.

- Buffer Overflows (e.g. SMTP/HTTP proxy)
- Command Exploitation through poor input validation.
- Authentication attacks.
- Management Interfaces
- Proxies
- Services

Denial of Service attacks

- Port effective resource starvation (e.g. syn/udp half-scans/fragmentation)

- Service or System resource starvation (e.g. large or multiple AV scanning)
- Bandwidth resource starvation.

Network Protocol attacks

- Address Spoofing
  - Reserved and RFC 1918 source addresses
  - Internal networks
- Routing
  - Loose source routing
  - Strict source routing
- ICMP attacks
  - Redirects
  - Fragmentation
    - Tiny
    - Overlapping
    - Missing
    - Reassembled Packet Too Long
  - Out of Sequence packets
  - Out of Spec packets
  - Unknown or unsupported protocols.

Apart from direct attacks against the firewall itself, we know that the firewall is also responsible for protecting other network assets from attacks directed at *'non authorized'* services between zones, as described in the Firewall Policy. Non-authorized services would be any services running on a system that are not explicitly described in the '*allow'* access rules within the Firewall Policy and firewall rule set, (these would ideally be identical).

An example may be a local loop-back service, a SMTP, SNMP or localized Syslog daemon, or an undocumented service specific to a particular application such as a backup utility.

Such services in the above diagram are the NTP daemon and Terminal Services, along with the native Windows SMB services running on the three Windows 2000/IIS 5.0 http/ftp servers. No access should be allowed to any of these services from the Internet.

1.6.2.4 Return On Security Investment or Materiality

In addressing the need to perform a Risk Assessment, we note that there is a very large set of threats, attack vectors, vulnerabilities, and exposures to be measured. Ironically, this is one of the difficulties of performing RA's; the risk universe is too numerous for us to calculate meaningful metrics for each of possibly 1000's of possible Risks, Exposures and probabilities.

Instead, as Auditors we use our subjective knowledge to propose examples which suitably illustrate the Return On Security Investment (ROSI) or Risk Mitigation value, that a specific control returns to the company. This in turn sets the Materiality of each auditable control.

The ISACA IS Auditing Guideline on Planning the IS Audit states:

> *"In the planning process the IS Auditor should normally establish levels of materiality such that the audit work will be sufficient to meet the audit objectives and will use audit resources efficiently. In planning sufficient audit work to meet the audit objectives, the IS Auditor should identify the relevant control objectives and determine, based on materiality, which controls will be examined. With respect to a specific control objective, a material control is a control or group of controls without which control procedures do not provide reasonable assurance that the control objective will be met."*

Here, the primary control for the mitigation of risks to within SCP is the firewall, which in turn affects the three identified controls on the I.S Infrastructure and user population. To perform a RA we must evaluate the Exposure a failure in each of these controls would have on the company, and express this quantitatively (scope item A.). Then we can use these values to calculate the firewall's value expressed as a Return On Security Investment (ROSI).

The ROSI (or $ value of Inherent Risk – Residual Risk) can be expressed using the following calculation.

ROSI($) = (ALE before implementing safeguard) – ((ALE after implementing safeguard) + (annual cost of safeguard))

ALE in the above calculation represents the *Annualised Loss Expectancy* in dollar terms. This is the sum of the *Single Loss Expectancy* multiplied by the *Annualised Rate of Occurrence*. The ARO is expressed as a value that represents the estimated probability of a specific threat occurring in a year, which is quoted as having the range 0 – 1.0. However when we consider threats such as Denial Of Service attacks that may happen many times during the year, this value may either be greater than 1 (ARO > 1), or once every few years (ARO < 1.0).

We change the test to express the probability as the number of days per year that an Exposure may occur, which has the range 0 – 365.

ALE ($) = SLE ($) x ARO (0 à 365)

In the above ALE equation, SLE represents the sum of the *Asset Value* multiplied by the *Exposure Factor*. The Exposure Factor is the estimated impact of an Exposure expressed as a percentage of the assets combined value, which is the sum of, hardware, software, support costs, business revenue, and data value.

SLE = Asset Value ($) x Exposure Factor (%)

Without access to automated RA systems such as the CRAMM[1] toolkit that provide statistical and empirically derived values for the impact of exposures and probability of threats, values for the ARO and Exposure factor must be subjectively estimated by the auditor.

[1] http://www.cramm.com/

This is the inherent problem with Quantitative assessments; some of the factors must be derived in a non-empirical subjective manner. As an example, the Risk of compromise to an unpatched NT4/IIS 4.0 web server placed on the Internet would be universally recognized as Extremely High, yet expressing this as a probability will either require a transformation of this subjective estimate into an Quantitative metric, or direct measurement through testing. This is often why a qualitative RA method is used in preference to the quantitative; the inputs are easier to estimate.

Gathering quantitative metrics for the some of the following examples was made easier by requesting project related documentation during the initial engagement meeting. From this business knowledge five figures have been extracted for use within our RA.

Table 1-2. Annual Costs of Support and previous exposures

Development Cost. (Internet Presence)	$16,000
Annualised Firewall support costs	$22,500
Estimated Revenue	$185,000 → $250,000 pa
Virus Costs last year (3 incidents)	$35,000
Cyber-Slacking Costs. (25% Workforce of 80 x 1 hour day @ $25 hr)	$500 per day

After conducting brief phone interviews with the project's management team, we also acquired an estimate of the company's intellectual property that is retained in the form of CAD Blueprints for extrusion dies and moulds on fileservers in the Corporate LAN.

Table 1-3. Company Intellectual Property value estimate.

Intellectual Property 18 yrs of company IP development	$750,000 (redevelopment cost for total loss)

Using these costs we can estimate the value in dollar terms the firewall's controls represent to the company. First, we propose 4 Risk scenarios with accompanying vulnerabilities and exposures.

Table 1-4. Risk Scenarios 1 to 4.

Risk 1. Cyber-slacking	
Threat.	Cyber-slacking caused by the firewalls failure to effectively manage Internet access, authorization and accounting, and apply effective content filtering.
Vulnerability:	Misconfiguration of proxy, Content filtering or Windows Authentication DC.
Exposure:	**SLE= $500** = $500 per day x *n* days (from Business Case)

Risk 2. Virus Outbreak	
Threat.	Email borne virus outbreak.
Vulnerability:	Untimely/Inaccurate pattern updates.
Exposure:	**SLE= $11,666** = $35,000/3 (from Business Case)
Risk 3. Public DMZ system compromise.	
Threat:	Web-server system compromise, through 'unauthorized' port attack. Total loss of web-server content and system integrity.
Vulnerability	Unpatched stateful Packet-Filtering failure or weakness, or ruleset misconfiguration.
Exposure:	**SLE = $7294** = $2500 (6 days labor @ $45hr for site rebuild for 3 systems + External developer @ $1000) + $ 4794 = Revenue loss (($250,000/365) * 7)
Risk 4. Corporate Asset Exposure.	
Threat:	A hacker compromises the corporate network and either destroys the companies intellectual property or holds it for ransom/sells it. This is a worst-case scenario with exposures across all Zones.
Vulnerability:	A downloaded binary contains a Trojan that uses the uncontrolled access to the Internet to dial home.
Exposure:	**SLE =$89,340** = 60,000 [IP loss = .10 x $750,000] + 4725 [Rebuild = 14 * (45 * 7.5 + 1000)] + 9589 [Revenue Loss = (14 * (250,000/365))] Sum of multiple exposures. Assume worst-case scenario results in 14-day recovery period with 10% loss of Intellectual Property due to incomplete backups of locally stored files.

1.6.2.5 Calculating ROSI and Materiality

In the equation above, two values are used for the *Annualised Loss Expectancy,* one pre-control and one post-control. Therefore, to calculate the ROSI we must propose two values for the *ARO f*or each of the Risks and calculate both the pre and post-control *ARO*'s.

This is where we need to develop some subjective estimates for each ARO based on our expertise. In the first two Risk scenarios' we have documented Pre-control ARO's

from the Business Case, so arriving at the ROSI that the Firewall's controls provide in these two risk scenarios is relatively easy.

For the last two risk scenarios there is no existing ARO baseline. In fact, the company hasn't had an on-site Internet presence before so we must estimate the Pre-Control ARO based on our subjective expertise.

The ISACA IS Auditing Guideline, Use of Risk Assessment in Audit Planning states in section 2.2.1 that:

> *"All risk assessment methodologies rely on subjective judgments at some point in the process (e.g. for assigning weightings to the various parameters). The IS Auditor should identify the subjective decisions required in order to use a particular methodology and consider whether these judgments can be made and validated to an appropriate level of accuracy."*

In Qualitative Risk Assessment terms, the pre-control ARO we must determine for Risk Scenario 3 is the *Inherent Risk* associated with placing a Windows 2000 IIS 5.0 web server on the Internet in an uncontrolled environment. All of the server's potentially vulnerable services are considered in this assessment, including IIS, as while the post-control environment still permits access to the http service from the Internet, the firewall restricts uncontrolled egress back to the Internet.

An example that illustrates the importance of egress filtering is the Nimda worm that used an outbound TFTP connection to retrieve the *admin.dll* worm code from previously infected servers. If egress via TFTP was restricted, the Unicode vulnerable host was not infected with Nimda via the Unicode vector (there were other infection vectors outside our discussion), even though it was vulnerable to the Unicode exploit.

As not all IIS 5.0 specific vulnerabilities require egress to result in a successful attack and some realised Exposure, we apply a weighting of 0.5 to the sum of Windows 2000 and IIS 5.0 vulnerabilities we discovered from the last 12 months that are detailed below. These were found by searching the CVE Metabase at ICAT for vulnerabilities whose *consequence* (a searchable field) might result in *root* access (ICAT's terminology, it should be *administrator* in a Windows context), from *remote* sources. These search criteria excluded lower risk vulnerabilities and those that would not be mitigated by access and egress filtering at the firewall.

Table 1-5. ICAT CVE Search Results: Win2K/IIS 5.0, Remote & Root

Windows 2000[2] http://icat.nist.gov/icat.cfm?cvename=CAN-2002-1214
IIS 5.0 http://icat.nist.gov/icat.cfm?cvename=CAN-2003-0226 http://icat.nist.gov/icat.cfm?cvename=CAN-2003-0225 http://icat.nist.gov/icat.cfm?cvename=CAN-2003-0224 http://icat.nist.gov/icat.cfm?cvename=CAN-2003-0109 http://icat.nist.gov/icat.cfm?cvename=CAN-2002-0869 http://icat.nist.gov/icat.cfm?cvename=CAN-2002-1180 http://icat.nist.gov/icat.cfm?cvename=CAN-2002-0364

[2] Source: http://icat.nist.gov

Using our expert-weighting schema we arrive at an Inherent Risk value of 4 for the Pre-Control ARO in Risk Scenario 3. This says that the probability or Inherent Risk of placing an unprotected Windows 2000, IIS server on the Internet is that it will be compromised with a *root* level attack via the network 4 times per year. Given the research undertaken in this area by the Honeynet Project[3], this seems a reasonable conclusion.

In the case of Scenario 4, a system compromise is only a matter of time, as they have already had 3 virus outbreaks in the last year. Eventually, a system will become compromised via a Trojan-bearing executable or some similar threat vector that's dials home, unless controls are put into place to control both WWW and Internet access.

Furthermore, the packet inspection afforded via Cisco IOS is insufficient to strictly enforce access and egress from the Internet to the publicly available servers in the DMZ. If SimCoat Plastics had implemented a DMZ with their existing Cisco Router, it's possible that the weaker controls applied may contribute in the future to some form of infrastructure compromise.

We have subjectively estimated a pre-control ARO for Risk Scenario 4 based on the above assumptions.

Table 1-6. Pre and Post Firewall ARO tables for Risk Scenarios 1 through 4.

Risk 1	ARO	Control	Justification
Pre	241	Nil	Business case, current existing uncontrolled risk.
Post	2.0	Authorization/ Accounting & Content Filtering	We feel that it's arguable that for two days per year a misconfiguration of either the firewall or the Windows Domain controller used for Authentication occurs.
Risk 2	**ARO**	**Control**	**Justification**
Pre	3.0	Nil	Business case, existing uncontrolled risk.
Post	0.5	Virus Scanning SMTP Proxy	We feel that it's arguable that once every two years an AV pattern file may be too late, inaccurate, or not applied in a timely manner.
Risk 3	**ARO**	**Control**	**Justification**
Pre	4.0	Nil	Professional Judgment
Post	0.2	Stateful Packet Filtering	We feel that it's arguable that once every 5 years a misconfiguration of the firewall's access rules may allow uncontrolled access to a vulnerable non-authorized service on one of the DMZ hosts.

[3] http://project.honeynet.org

Risk 4	ARO	Control	Justification
Pre	0.5	IOS Nat & Packet Filtering	Professional Judgment
Post	0.1	Stateful Packet Filtering	We feel it's possible that once every 10 years a weakness in the Firewall, it's implementation or configuration may allow a penetration of the corporate network to occur.

By inserting the figures into a simple table we are able to calculate the ROSI for each of the Firewalls Critical Controls and evaluate the Materiality based on these figures.

Table 1-7. Firewall Return on Security Investment Calculation.

Risk	SLE $	ARO Pre-FW	ALE Pre-FW	ARO Post-FW	ALE Post-FW	ROSI
Risk 1.	**500**	241	$120,500	2	$1,000	$119,500
Risk 2.	**11,666**	3	$34,998	0.5	$5,833	$29,165
Risk 3.	**7,294**	4	$29,176	0.2	$1,458	$27,718
Risk 4.	**89,340**	0.5	$44,670	0.1	$8,934	$35,736
			$229,344		**$17,225**	
				Firewall Support	**$22,500**	
					ROSI	**$172,394**

It's interesting to note here that the Content Filtering provides the greatest ROSI, and should therefore be regarded as having the greatest Materiality in our audit. This conclusion provides considerable support for undertaking the Quantitative Risk assessment, as the business can now see the effect on the "bottom" line each of the firewall's controls will have.

Having established the materiality of each of the Critical Controls and the Firewalls total ROSI or Materiality we can now create a checklist that reflects these values.

1.7 Current State of Practice.

1.7.1 Auditing

When approaching this project we knew that many other GSEC, GCUX, GCFW and GSNA candidates had written papers related to Linux and Firewalls in general, so our first point of call was the

- SANS Reading Room, and the
- GIAC Certified Students and Posted Practicals page

After scouring through a dozen or so submissions we had developed a loose framework for approaching the Audit but needed more information on Audit processes and Security

Policies. The aim was to reflect a real-world scenario, and have the Audit Checklist driven by company policy.

Our search regime is to use Copernic Professional[4] with each search engine set to retrieve 100 queries maximum followed by the Intermediate filtering option. We also duplicate any critical searches using different international groups of search engines. It's truly surprising what you find when you search using European search engines.

Our quest for information took us many places including:

- The Institute of Internal Auditors; Audit Reference Library
- Auditing Firewalls: A Practical Guide
- Securityfocus: Introduction to Security Policies (Four-Part series)
- Securityfocus: Assessing Internet Security Risk (five-part series)
- SecurityFocus: Justifying the Expense of IDS, Part One: An Overview of ROIs for IDS
- State of Texas; Department of Information Resources; Policies, Standards, & Guidelines
- Risk Assessment Models and Evolving Approaches
- CIO Magazine: Finally a Real Return on Security Spending
- Information Systems Audit and Control Association; Standards, Guidelines and Procedures

Of these by far the most influential is the last. We will not detail each of the many references we reviewed that were sourced from ISACA, as the list would be very long. It's sufficient to say that we began with *ISACA Guideline # 050.010.020, Planning*, which set the framework for the entire project.

1.7.2 Astaro.

When it comes to establishing controls related to the configuration of a system, we never forget to consult the vendor documentation. In the end this was the source for the all of the controls related to configuring the application level proxies and the system itself, and formed the basis of the Firewall Policy in appendix 7.1.

- Astaro Security Linux V4 Manual

In addition to reading the manual we also installed Astaro 4.0 into a VMware™ virtual machine for the purpose of evaluating the firewalls base operating system and assessing the Linux OS hardening section of the audit checklist. This proved invaluable as we soon discovered that Astaro is a heavily modified Linux distribution, based we believe on Red Hat[5].

Its security posture seems based on the concept of delivering the operating system as a Black-box or appliance, with all administration provided by the Web-Admin interface. As shell access is actively discouraged we eventually took the position that the audit goals

[4] http://www.copernic.com

[5] http://www.redhat.com

were best served by focusing our attention on the interfaces to the firewall rather than the base OS.

1.7.3 Firewalls:

Given the ubiquitous nature of firewalls and their pre-eminence as the technical control of choice for Network Engineers and Administrators, it's not surprising that there is an abundance of material related to auditing them available on the Internet. However that is not to say that this is all good material, much of what can be casually 'googled' for is too simplistic in nature to be used by an auditor without considerable development of the concepts they espouse. There are however some excellent resources available if one is prepared to scratch below the surface.

In establishing a firewall performance baseline for the purposes of certification, the most well known name in the business is undoubtedly ICSA Labs[6]. An examination of their web site reveals *The Modular Firewall Certification Criteria Version 4.0,* which sets baseline standards for submitted firewall products in relation to the certification program across a range of different firewall implementations.

In total there are four modules available[7]:

- Baseline Module – Applicable to all products assessed
- Residential
- Small to Medium Business
- Corporate

These were useful documents when considering the Packet Filtering baseline section of the Audit Plan. When considering the application gateways within Astaro Security Linux, ICSA Labs also have an accreditation process for content filtering products:

- Web Content Filtering & Management

This also proved useful in understanding audit criteria for the HTTP Content filtering and Proxy controls within Astaro.

As a general reference we found the *NIST Firewall Guide and Policy Recommendations*[8] an excellent all-round source of information relating to firewalls, their architectures, configuration, and testing.

Next on the list of useful documents in terms of auditing systems and network resources for open ports and weak services, is the *Open Source Security Testing Methodology Manual*[9]. The manual describes itself as;

> *"a definitive standard for unpriviledged security testing in any environment from the outside to the inside."*

This was used as the primer for performing network based assessments of the firewalls packet filtering controls.

[6] http://www.icsalabs.com
[7] http://www.icsalabs.com/html/communities/firewalls/certification/criteria
[8] http://csrc.nist.gov/publications/nistpubs
[9] http://www.isecom.org/projects/osstmm.htm

While we could fill another page or two with other references including many from the Sans Reading Room and previous SANS practicals of accredited security practitioners, the most useful Firewall Audit process we discovered was

- ISACA: Procedures for Information Systems Auditing # 7, Firewalls

This document provides the framework for the many of the controls within our Audit Checklist with specifics gleaned from the sources above and below, man pages for any tools used such as Nmap or N-Stealth and personal experience.

In relation to the application proxies we've already established that 2 of the 3 critical control objectives we wish to Audit pertain directly to proxy services. The audit analysis of each has four facets, the first relating to establishing a baseline configuration, the second to the effectiveness of the control, the third relates to the security of the service in respect to it's resistance to attack and compromise, while the last is concerned with detecting failure or compromise of the control.

Our approach then is to:

- Establish preventative configuration baseline controls.
- Test each control's effectiveness in implementing policy.
- Test each control's susceptibility to attack and compromise.
- Assess each control's effectiveness in detecting compromises.

We additionally used methodologies in the following to establish tests to for audit checklist items:

- OWASP; Guide to Building Secure Web Applications V 1.1.1

1.7.4 Linux Systems:

When approaching the control requirements for a Linux firewall host, there are also a large number of guides on hardening Linux, and again, not all are created equal.

The fact remains that the multitude of Linux derivations in the market place makes the task of writing a single document to harden Linux very difficult. Even those that exist such as the Centre for Internet Security's Linux Benchmark V 1.0,[10] fail to provide the same level of guidance that the CIS Windows 2000 guides provide in terms of suitability for purpose.

It's the age-old InfoSec question " how much security do I need?" A: "what's the risk?"

If we consider that a Firewall that protects several hosts and applies a number of other controls within the infrastructure is inherently of more value than an ftp serving documentation, then it follows that the firewall needs a higher degree of security consideration when hardening it.

Many of the guides available provide systematic instructions on manually editing sensitive configuration files as a process to harden the system. While this may arrive at an increased level of security, thorough testing of each step would be required to ensure that everything else the system is designed to do still worked after making each change. This is time consuming and unsustainable in almost any environment.

[10] http://www.cisecurity.org/bench_linux.html

What we desire is a simple menu driven security tool that can both configure and audit the security of a system relative to some established security profiles, such as *home desktop, corp desktop, file and print server, web server, dns/ldap server, CA,* and finally *firewall*.

Many but not all of the vendors have these in-built tools to set and test the security configuration of their distribution, e.g. Debian has *Checksecurity*, SuSE has *seccheck* OpenBSD has */etc/security* and Mandrake has *msec*.

Additionally, there are a number of Open Source projects aimed at providing the user community with simple point and shoot security hardening tools. Three worth mentioning are Tiger, Bastille and the CISscan but each requires installing on the host OS before they can be used as benchmarking tools, and that is not a possibility in this audit.

In the end we resolved to use the tried and tested method of manually auditing the host based on a select number of best practices. Both Bastille[11] and *msec* from Mandrake[12] provided useful guides in establishing what level of security is appropriate for a firewall. Bastille uses *Lax, Moderate* and *Paranoid* settings for both Workstation and Server giving 6 levels of security while Mandrake's *msec* has levels 0 – 5.

Two sources that proved invaluable were;

- Securing & Optimizing Linux: The Ultimate Solution v2.0
- Center for Internet Security, Linux Benchmark V 1.0

The first of these is a recently released update of the well-known *Securing & Optimizing Linux: Red Hat Edition v1.3.*

These four resources contribute to the Linux OS controls within our checklist, however due to the Black-Box nature of the Astaro distribution we decided, after investigating the applicability of these guidelines within our VMware installation, not to conduct an overly exhaustive audit of the base OS. We advised the client that it would be best to consider the system a Black-Box and focus the audit program on baselining its performance and assessing its externally available interfaces.

[11] http://www.bastille.org
[12] http://www.mandrake.com

2 ASSIGNMENT 2 – CREATE AN AUDIT CHECKLIST

2.1 Audit Styles

There are two common approaches to conducting Audits. In the first the auditor takes the role of policing the subjects conformance to a predefined standard, baseline or policy. In these audits the auditor assesses the state of the audit subject at a fixed point in time and reports it's compliance with the standard, baseline or policy used as a measure. The goal is not to improve the security state of the audit subject, simply to measure and report it.

The second approach, and the one we use, differs in that the audit process goal is not to simply measure the systems conformance to some measure at point in time, but to consultatively develop a set of measures specific to the audit subject through negotiation with the system owners and administrators, and subsequently assess the systems compliance with this agreed state at some agreed point in the future.

This approach differs in that it attempts, through negotiation and agreement, to raise the level of security within the audit subject to a mutually agreed baseline before the audit is conducted. By providing the opportunity for systems owners and administrators to contribute to the baseline, and then affording them time to modify the audit subjects state to assure conformance, all parties to the audit have significant buy-in, with a common desire to achieve a satisfactory outcome.

In the end this provides the customer with an increased confidence in the state of their systems, and their staff's ability to securely administer them. In our experience this approach results in a win-win outcome for all involved as the audit process increases the security of the audit subject while the baseline assists in the maintenance of this known good state.

2.2 Baseline Checklist Development

As suggested above, our checklist was co-developed with the system administrators and owners subsequent to the Entrance Conference where we introduced the goals and process. During the Entrance Conference we attempted to develop a collaborative rapport with the individual members of the audit audience by focusing on a successful business outcome for SCP.

During the checklist development process we took the rudimentary Firewall Policy that had been developed by the system administrators and expanded this by explicitly defining the configuration of the firewall in a system blueprint.

This takes the implicit instruction outlined in other SCP corporate policies and interprets these as explicit security controls affected by the firewall.

2.2.1 Risk Analysis.

While developing the checklist we sought to establish a consensus of opinion on the relative risks, threats and exposures the firewall controls were designed to mitigate. A necessary precursor to this qualitative risk assessment was the establishment of common terms of reference for all parties involved.

With this in mind we introduced the following qualitative risk assessment tables.

Table 2-1. Likelihood of Occurrence

Oid	Likelihood	Description
A	Negligible	Unlikely to occur
B	Very Low	Likely to occur once every 5 years
C	Low	Likely to occur once every 2 years
D	Medium	Likely to occur once every year.
E	High	Likely to occur once every 6 months
F	Very High	Likely to occur once a month
G	Extreme	Imminent, may occur at any time.

Table 2-2. Impact Severity Levels

Sid	Impact Severity	Description
I	Insignificant	Will have almost no impact if threat is realized and exploits vulnerability
II	Minor	Will have minor effect on system. It will require minimal effort to repair or reconfi gure system.
III	Significant	Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals. May cause political embarrassment. Will require some expenditure of resources to repair.
IV	Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. It will require expenditure of significant resources to repair.
V	Serious	May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise or large amount of company information or services.
VI	Critical	May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of company's information or services.

Table 2-3. Risk Calculation.

Oid / Sid	I	II	III	IV	V	VI
A	Very Low	Very Low	Low	Low	Low	Low
B	Very Low	Low	Low	Low	Moderate	Moderate
C	Low	Low	Moderate	Moderate	High	High
D	Low	Low	Moderate	High	High	High
E	Low	Moderate	High	High	High	Very High
F	Low	Moderate	High	High	Very High	Very High
G	Low	Moderate	High	Very High	Very High	Very High

2.3 Checklist

After establishing the Qualitative Risk assessment scale above, we proceeded to develop the checklist using Risk Assessment descriptors for each control as indicated in the table in the right.

O-S/P-C-D
OID
SID
Risk

- O = Objective.
- S = Subjective.
- P = Preventative (test or configuration).
- C = Corrective (event)
- D = Detective (test or event).
- Oid = Occurrence ID from Table 2-1.
- Sid = Severity ID from Table 2-2
- RISK is calculated from Table 2-3

As stated previously the checklist attempts to assess compliance and residual risk in four areas;

- Assess compliance with configuration baseline.
- Assess each control's effectiveness in implementing policy.
- Assess each control's susceptibility to attack and compromise.
- Assess each control's effectiveness in detecting failures or compromises.

Objective, Testing and References	Compliance/Expected Results	Risk	
I AUDIT PLAN: *Objective(s): ISACA Standard 050.010 (Audit Planning) section 2.1.2 states: "The IS auditor should develop an audit plan that takes into consideration the objectives of the auditee relevant to the audit area and its technology infrastructure."* *Source(s):* ISACA Guideline; Planning, Document # 050.010.020 **Note:** Each of the following steps in the Audit Plan section comes from the above source.			
I.A <u>Knowledge of the Organization</u> *Objective(s): Section 2.2.1 states: "As a part of the planning process IS auditors should obtain an understanding of the organisation and its processes. In addition to giving the IS auditor an understanding of the organisation's operations and its IS requirements, this will assist the IS auditor in determining the significance of the IS resources being reviewed as they relate to the objectives of the organisation."* *Source(s):* ISACA Guideline; Planning, Document # 050.010.020	Interviews should be conducted, questionnaires developed and processed, and documents retrieved from the business supporting the development of the audit subject and its business function. The management structure should also be understood with clear responsibilities defined for the audit plan and program signoff.	Failure to develop a clear understanding of the audit subject's context within the organization may result in a failure by the auditor to develop an Audit Program that satisfies the business requirements as they are laid out in the scope.	O/P B IV LOW

Objective, Testing and References	Compliance/Expected Results	Risk	
I.B Materiality *Objective(s): Section 2.3.1 states: "In the planning process, the IS auditor should ordinarily establish levels of planning materiality such that the audit work will be sufficient to meet the audit objectives and will use audit resources efficiently. For example, in the review of an existing system the IS auditor will evaluate materiality of the various components of the system in planning the audit program for the work to be performed. The IS auditor should consider both qualitative and quantitative aspects in determining materiality."* *Objective(s): Adjust the scope of the review using the information on sensitivity of the services that the firewall is intended to protect, the identified risks, and the likelihood of their occurrence.* *Source(s):* ISACA: Procedure 7, Firewalls	Performance and delivery of a documented Risk Assessment used to establish the materiality of major control objectives.	Failure to develop a clear understanding of each control's materiality may result in the expenditure of disproportionate amounts of time and resources on controls of low materiality and the inverse in relation to controls of high materiality.	O/P B IV LOW
I.C Planning Documentation: *Objective(s): Section 3.1.1 states: "The IS auditor's work papers should include the audit plan and the program."* *Source(s):* ISACA Guideline; Planning, Document # 050.010.020	The plan you are reading.	Failure to produce a plan may result in poor execution of the Audit, as objectives will not be clearly stated.	O/P B IV LOW
I.D Plan Endorsement: *Objective(s): Section 3.2.1 states:*	Management endorsement of the audit program and the audit plan.	Failure to attain management 'signoff' for this plan may have two potentially negative	O/P

Objective, Testing and References	Compliance/Expected Results	Risk	
"To the extent appropriate, the audit plan, audit program and any subsequent changes should be approved by the audit management." *Source(s):* ISACA Guideline; Planning, Document # 050.010.020		outcomes: the plan may fail to produce the outcome desired by management by failing to fully understand, document and deliver the requisite goals. The audit might also encounter a higher degree of audit resistance from the operational staff if management are not seen to openly endorse the program at the highest levels.	B III LOW
I.E Audit Program: *Objective(s): Section 3.3.1 states: "A preliminary program for a review should ordinarily be established by the IS auditor before the start of the work. This audit program should be documented in a manner that will permit the IS auditor to record completion of the audit work and identify work that remains to be done. As the work progresses, the IS auditor should evaluate the adequacy of the program based on information gathered during the audit. When the IS auditor determines that the planned procedures are not sufficient, the IS Auditor should modify the program accordingly."* *Source(s):* ISACA Guideline; Planning, Document # 050.010.020	The preliminary review is the execution of this audit plan as below. The audit should be viewed as a flexible process that adjusts to ensure that the goals of the audit are attained. It's possible that the results may require that the plan be amended or adjusted to reflect new information as it comes to hand.	Failing to recognize that the audit may produce results that influence the evaluation of the audit system may result in certain audit goals not being realized.	O/P B III LOW
II FIREWALL DOCUMENTATION			

Objective, Testing and References	Compliance/Expected Results	Risk	
II.A Corporate Policies *Objective(s): Attain all corporate policies that pertain to the Firewall and systems it protects. Assess the application of these policies within the Firewall Policy.* *Source(s):* ISACA: Procedure 7, Firewalls	Best Practice Baseline Policies: Acceptable Use Account Management Admin/Special Access Change Management Disaster Recovery Incident Management Network Configuration Passwords Physical Security Privacy Software Licensing Virus Protection Server Hardening Firewall Policy	Failure to reference a broad base of security policies will prevent the development of a Firewall Policy and Audit checklist that represents the company's security posture.	O/P B III LOW
II.B Firewall Policy *Objective(s): Test that a Firewall Policy exists that explicitly defines the firewall configuration including proxy services, SIPF ruleset, monitoring, backups, and administrative access.* *Source(s):* ISACA: Procedure 7, Firewalls, NIST Guidelines on Firewalls; sp800-41, Section 4.3		Failure to develop and reference an explicit firewall policy will fail to provide a baseline for the audit checklist.	O/P B V MOD
III ASTARO 4.008 SYSTEM CONFIGURATION		All configuration errors have the potential to increase the	

Objective, Testing and References	Compliance/Expected Results	Risk	
CONFIGURATION *Objective(s): To establish a baseline configuration for the firewall based on the customers firewall policy, which reflects vendor and industry best practices. In the System tab, open the Settings menu and check the following settings in the General System Settings window:* *Source(s):* SCP Firewall Policy, SCP Server Security Policy, Astaro Manual, ISACA: Procedure 7, Firewalls		likelihood of introducing avulnerability, or of one being exploited. This risk applies to all System Configuration Controls below in addition to any additional Risks identified.	
III.A Hostname: *Objective(s): Ensure the hostname is correctly configured.* *Source(s):* SCP Firewall Policy	Hostname: star.scp.net	Misidentification of the system may result in alerts and syslog events being overlooked.	O/P B III LOW
III.B Administrator e-mail addresses: *Objective(s): Whenever certain important events occur, such as port scans, failed logon attempts, or reboots, as well as whenever the self-monitor or Up2Date systems generate alerts or reboots, the Astaro security system will send a notification e-mail to the administrator.* *Source(s):* SCP Firewall Policy, Astaro Manual, ISACA: Procedure 7, Firewalls	Administrator e-mail addresses: trouble@scp.net skoenig@scp.net help@scp.net	Failure to receive timely event notifications from the firewall may result in attacks, compromises, service failures, and configuration changes going unnoticed which could contribute or directly cause a failure in one of the Firewalls critical controls.	O/P B V MOD

Objective, Testing and References	Compliance/Expected Results	Risk	
III.C NTP Settings *Objective(s): Confirm NTP Settings* *Source(s):* SCP Firewall Policy,, Astaro Manual *Objective(s): Precision of Date and Time: The date and time recorded in the log by the Firewall Log Event must reflect the exact date and must minimally reflect the exact second in time that the event occurred.* *Source(s):* L03, ICSA Labs Baseline Module	Time zone: AEST NTP server: NTP Server Canberra	Failure to establish an enterprise time zone and ensure that systems record events accurately can result in poor correlation of events and low event resolution power during incidents. This can contribute to the response time, which can in turn increase the impact of an event.	O/P B II LOW
III.D Web Admin Settings *Objective(s): Administrative Interface Authentication: To access the Administrative Functions, the Firewall must have the capability to require authentication through an Administrative Interface using an Authentication Mechanism.* *Source(s):* , ICSA Labs Baseline Module, Section AD3, SCP Firewall Policy, SCP Server Security Policy	Test the Web Admin interface to see whether it requires authentication.	Failure to authenticate administrative users may lead to system compromise through unauthorised access.	O/P C IV MOD
III.E Web Admin Timeout *Objective(s): Restrict Access to the Web-Admin interface using the least-privilege principal by minimizing the timeout value for the administrative interface.* *Source(s):* Astaro Manual, SCP Firewall Policy, SCP Server Security Policy	Web Admin Timeout Timeout (seconds): 300 seconds	Leaving the admin interface logged on could provide an insider unauthorised access to the management interface if either management console is left unattended.	O/P C IV MOD

Objective, Testing and References	Compliance/Expected Results	Risk	
III.F Allowed networks: *Objective(s): Restrict Access to the Web-Admin interface using the least-privilege principal by explicitly specifying the IP addresses of hosts that are allowed to log on to the Web Admin interface.* *Objective(s):* Astaro Security Note: *As soon as you can determine which computer(s) will be used to administer the security system (e.g., your IP address on the internal network) replace the Any entry in the Allowed Networks menu with a smaller network.* *Source(s):* SCP Firewall Policy, SCP Server Security Policy, Astaro Manual	Allowed networks: Management-host01 Management-host02	Unrestricted access to the Web Admin https interface may allow an insider to launch a brute force attack against it.	O/P B III LOW
III.G Authentication methods: *Objective(s): Check that the authentication method used for the Web Admin interface is set only to Local Accounts.* *Source(s):* SCP Firewall Policy, SCP Server Security Policy, Astaro Manual	Authentication methods: Local Accounts	Using Local Accounts ensures that even if the Windows Domain accounts are compromised, the firewalls administrator accounts are protected.	O/P B IV LOW
III.H Allowed users: *Objective(s): Restrict Access to the administrative interfaces using the least-privilege principal.*	Allowed users: admin	Requiring individual accounts ensures an audit trail is available. Without the audit trail unapproved changes may be	O/P B

Objective, Testing and References	Compliance/Expected Results	Risk	
interfaces using the least-privilege principal. *Source(s):* SCP Firewall Policy, SCP Server Security Policy, Astaro Manual *Source(s):*	alanthomson svenkoenig	made with impunity.	IV LOW
III.I License for all Services *Objective(s): Check to see that the firewall has a currently valid license for the proxy services and functions SCP wish to utilize. In the System tab, open the Licensing menu and check the following settings:* *Source(s):* SCP Acceptable Use Policy, Astaro Manual	Registration date: Jun 2003 Network interfaces: Unlimited Protected Network Devices: Unlimited Up2Date Virus protection: Enabled Up2Date Surf protection: Enabled	Failure to have a current license may result in multiple exposures as the system may cease to function in varying degrees.	O/P B V MOD
III.J SSH-Status *Objective(s): Restrict Access to the administrative interfaces using the least-privilege principal.* *Objective(s):* **Astaro Security Note:** *We recommend that the SSH service be disabled when not in active use.* *Source(s):* SCP Firewall Policy, Astaro Manual	SSH Status: Disabled	Providing a second management interface over the network is unnecessary as all management functions must be performed via the Web Admin interface. Having SSH running is another point of potential compromise.	O/P C III LOW
III.K Up2Date Configuration *Objective(s): Check to see that the* ***Up2Date*** *service is configured to retrieve Up-Dates regularly*	Up2Date Configuration Automatic Pattern Up2date: Enabled	Ensuring timely implementation of security patches and anti-virus pattern updates reduces	O/P

Objective, Testing and References	Compliance/Expected Results	Risk	
is configured to retrieve Up-Dates regularly *Objective(s): Astaro Security Note: The Up2Date Service makes it easy to keep your security system software, including virus definitions, system patches, and security features, current.* *Source(s):* SCP Firewall Policy, Astaro Manual	Interval: Daily	the likelihood of exposure through any vulnerabili ties they mitigate.	C IV LOW
III.L Firewall Backup *Objective(s): The conduct and maintenance of backups are key points to any firewall administration policy. All firewalls should be subject to a Day Zero backup. All firewalls should be backed up immediately prior to production release. As a general principal, all firewall backups should be full backups. There is no real requirement or need for incremental backups.* *Source(s):* NIST Guidelines on Firewalls; sp800-41, Section 5.6 Firewall Backups *Objective(s): Verify continuity plans for firewalls are in accordance with those of other high-availability services, as firewalls ordinarily are components related to services with high-availability requirements.* *Source(s):* ISACA: Procedure 7, Firewalls			
	Email Backup	Failure to regularly and completely back up the firewall	O/P

Objective, Testing and References	Compliance/Expected Results	Risk	
			O/P
III.M Email Backup *Objective(s): Check to see that the Email Backup option is configured in line with the Firewall Policy.*	*Enabled and configured to use:* *trouble@scp.net* *skoenig@scp.net* *swilson@scp.net*	completely back up the firewall reduces the company's ability to implement effective change control processes and affects the availability of the system through disaster recovery processes.	B MOD
III.N Backup Interval *Source(s):* SCP Firewall Policy *Objective(s): Check that the Email Backup interval is configured correctly.* *Objective(s):* **Astaro Security Note:** *After every system change, be sure to make a backup. This will ensure that the most current security system settings are always available.* *Source(s):* SCP Firewall Policy, Astaro Manual	Backup Interval: Daily	As above.	
			O/P B III

Objective, Testing and References	Compliance/Expected Results	Risk	
			LOW
III.P Syslog Configuration *Objective(s): In the System tab, open the Syslog menu and check the following settings in the Syslog settings window:* *Source(s):* Astaro Manual *Objective(s): Ensure logging is configured.* *Source(s):* Section L01, Logging, ICSA Labs Baseline Module *Objective(s): Monitor, audit and incident response. Monitor firewall alerts on a continuous basis. Review the procedures to review the logs in an effective and timely manner and to deal with potential harmful traffic.* *Source(s):* ISACA: Procedure 7, Firewalls *Source(s):*	Syslog Configuration Remote Syslog Hosts: Authentication Logs: Syslog-Station-01 Daemon Logs: Syslog-Station-01 Kernel Logs: Syslog-Station-01 Notification: Syslog-Station-01 SMTP Relay Logs: Syslog-Station-01	Failure to record events may result in events occurring which are not responded too, and a lack of evidence or audit trail when investigating an event.	O/P B III LOW
III.Q User Authentication *Objective(s): To ensure that the correct User Authentication service is selected for the Application Gateway services.* *Objective(s):* **Astaro Security Note***: The security system supports User Authentication using the*	User Authentication: Radius Server Settings. Status: Disabled SAM (NT/2000/XP) Server Settings.	Lack of user authentication may result in an abuse of network resources as unauthorised actions may be taken with impunity.	O/P C

Objective, Testing and References	Compliance/Expected Results	Risk	
SOCKSv5, SMTP, and HTTP proxy services, and can control which users are allowed to use which services. *Source(s):* SCP Firewall Policy, Astaro Manual pg 60	Status: Enabled PDC: WIN2KDC PDC Address: 192.168.10.40 BDC: WIN2KDC BDC Address: 192.168.10.40 LDAP Server Settings. Status: Disabled		IV MOD
III.R WebAdmin Site Certificate *Objective(s): To ensure that the Firewall is correctly identifying itself when using certificates for cryptographic services such as SSL and IPSec. In the System tab, open the Web Admin Site Certificate menu and check the following settings:* *Source(s):* SCP Firewall Policy, Astaro Manual pg 60	WebAdmin Site Certificate: Country code: Australia State or region: Victoria City: Melbourne Company: SimCoat Plastics Org. unit: InfoSec Contact e-mail: trouble@scp.net Firewall hostname: star.scp.net	Correctly identifying the system via the Site Certificate minimises he possibility of a Man in the Middle attack.	O/P B II LOW
III.S Hosts *Objective(s): Ensure that the Hosts, services and Networks defined in the Firewall Policy are reflected in the Firewall asset list.In the Definitions tab, open the Networks menu and*	WebServer01 184.112.25.18 WebServer02 184.112.25.19 FTPServer01 184.112.25.20 MySQL-Server 192.168.10.20 Mail-Server 192.168.10.30	Failure to correctly implement the SIPF rules may result in the exposure of a host to attack on an unauthorised service.	O/P C

Objective, Testing and References	Compliance/Expected Results	Risk	
check that the following hosts are defined: *Source(s):* SCP Firewall Policy, Astaro Manual pg 80	Mail-Server 192.168.10.30 Win2KDC01 192.168.10.40 Syslog-Host 192.168.10.50 Management01 192.168.10.60 Management02 192.168.10.61 Win2KDC02 192.168.20.10		V MOD
III.T Networks *Objective(s): Ensure that the Hosts, services and Networks defined in the Firewall Policy are reflected in the Firewall asset list. In the Definitions tab, open the Networks menu and check that the following Networks are defined:* *Source(s):* SCP Firewall Policy, Astaro Manual pg 80	Internet 0.0.0.0/0 Public Zone 184.112.25.16/29 Backend Zone 192.168.10.0/24 Office Zone 192.168.20.0/24	As above.	O/P C V MOD
III.U Local User Accounts *Objective(s): Review the procedures used for device administration (including at least physical access and administrators passwords, for example, to reduce the risk of tampering the connections thru unauthorised access.* *Source(s):* ISACA: Procedure 7, Firewalls	Local User Accounts: admin alanthomson svenkoenig	Ensuring only those accounts that are required reduces the chance of unauthorised configuration changes, and provides an audit trail	O/P C

Objective, Testing and References	Compliance/Expected Results	Risk	
Objective(s): In the Definitions tab, open the Networks menu and check that the following users and only the following users are defined. *Source(s):* SCP Password Policy, SCP Server Security Policy, SCP Firewall Policy, Astaro Manual pg 85			IV MOD
IV CONFIGURATION: UNUSED SERVICES *Objective(s): To check that all unused services are disabled. Any unused network services or applications should be removed or disabled.* *Source(s):* NIST Guidelines on Firewalls; sp800 -41, Section 5.2		*"Unused applications are often used to attack firewalls because many administrators neglect to implement default-restrictive firewall access controls. In addition, unused network services and applications are likely to run using default configurations, which are usually much less secure than production-ready application or service configurations. "*	
IV.A NAT *Objective(s): In the Network tab, open the Nat menu and check that no Nat rules are configured.* *Source(s):* SCP Server Security Policy, SCP Firewall Policy, Astaro Manual	No NAT rules defined	As IV above	O/P B III LOW

Objective, Testing and References	Compliance/Expected Results	Risk	
IV.B PPTP Roadwarrior Network Access *Objective(s): In the Network tab, open the PPTP Roadwarrior Network Access menu and check that the PPTP Roadwarrior Network Access Server is disabled.* *Source(s):* As in V.A above	Status: Disabled	As IV above	O/P B III LOW
IV.C Quality of Service *Objective(s): In the Network tab, open the QOS menu and check that QOS is not configured.* *Source(s):* SCP Firewall Policy	No QoS Rules	As IV above	O/P B III LOW
IV.D IPSec VPN *Objective(s): In the IPSec VPN Tab, open the Connections menu and check that the following services are disabled:* *Source(s):* SCP Firewall Policy	Status: Disabled IKE Debugging: Disabled NAT Traversal: Disabled	As IV above	O/P B III LOW
IV.E Ident Relay *Objective(s): In the Proxies Tab, open Ident menu and check that the Ident Relay proxy is configured as expected:*	Status: Disabled	As IV above	O/P B

Objective, Testing and References	Compliance/Expected Results	Risk	
configured as expected: *Source(s):* SCP Firewall Policy			III LOW
IV.F <u>SOCKS 5 Proxy</u> *Objective(s): To ensure that the SOCKS 5 Proxy Service is enabled and configured in line with best practices and company policy to provide the maximum protection to users and company resources. In the Proxies tab, open the SOCKS menu and check that the SOCKS Proxy is configured with the expected parameters.* *Source(s):* SCP Firewall Policy, SCP Audit Policy, SCP Acceptable Use Policy	Status: Disabled Allowed Networks: Empty User Authentication: Disabled Authentication Methods: Empty	Ensuring that only the required services are enabled and are configured properly reduces the likelihood of misconfiguration that may lead to a vulnerability and exposure.	
V CONFIG: ENABLED SERVICES *Objective(s): To check that only the desired services are enabled and that they are configured in line with best practices and company policies.*			

Objective, Testing and References	Compliance/Expected Results	Risk	
V.A <u>DHCP Server</u> *Objective(s): Check that the DHCP server is running and that it is configured with the expected parameters. In the Network tab, open the DHCP Server Tab and check that it is configured as expected.* *Source(s):* SCP Firewall Policy	DHCP Server*:* *Status:* enabled *Network to serve:* Corporate LAN *Range Start:* 192.168.20.64 *Range End:* 192.168.2.253 *DNS Server 1:* 192.168.20.1 *DNS Server 2:* blank *Gateway IP:* 192.168.20.1 *WINS Server:* 192.168.20.10 *WINS Node Type:* P Node: Peer WINS Only *Static Mappings:* none configured	Ensuring that only the services that are required are enabled and that they are configured properly reduces the likelihood of misconfiguration that may lead to a vulnerability and exposure. Also, failure of the system to perform as expected and required can lead to the users attempting to circumvent the controls imposed by the system.	O/P B III LOW
V.B <u>Traffic Accounting</u> *Objective(s): Audit network utilization. In the Network tab, open the Accounting menu and check that Traffic Accounting is configured to monitor the following networks.* *Source(s):* SCP Audit Policy, SCP Acceptable Use Policy	Traffic Accounting: Status: Enabled Interfaces: Public DMZ Corporate LAN Backend LAN Internet	Failure to have a complete audit trail can reduce the organizations ability to respond to an event.	O/P B III LOW

Objective, Testing and References	Compliance/Expected Results	Risk	
V.C Port Scan Detection *Objective(s): Check that the Port Scan Detection service is running. In the Network tab, open the Portscan Detection menu and check that the Portscan Detection service is configured with the expected parameters.* *Source(s):* SCP Firewall Policy *Objective(s): Confirm firewall rules discover external attempts to scan for commonly scanned ports (regardless of whether systems actually exist to listen on such ports).* *Source(s):* ISACA: Procedure 7, Firewalls	Port Scan Detection: Status: Enabled Action taken on portscanner traffic: drop (blackhole)	Failure to implement PSD may enable an attacker to successfully enumerate the systems services, which in turn may lead to an attack on a system.	O/P C IV MOD
V.D HTTP Proxy *Objective(s): To ensure that the HTTP Proxy is enabled and configured in line with best practices and company policy to provide the maximum protection to users and company resources.* *Objective(s): In the Proxies tab, open the HTTP menu and check that the HTTP Proxy service is configured with the expected parameters.* *Source(s):* SCP Firewall Policy, SCP Audit Policy, SCP Acceptable Use Policy	Status: Enabled Authentication: User Authentication Anonymity: Standard Caching: Enabled TCP Port: 8080 Allowed Networks: Corporate LAN Allowed Services: FTP (20/21), HTTP, HTTPS Authentication: NT/2000/XP Server	Ensuring that only the required services are enabled and are configured properly reduces the likelihood of misconfiguration that may lead to a vulnerability and exposure. This is o one of the Critical Controls identified in the Risk Analysis. Failure to implement the Proxy effectively will contribute to continued Cyber-Slacking.	O/P C IV MOD

Objective, Testing and References	Compliance/Expected Results	Risk	
V.E Content Filtering *Objective(s): To ensure that the Content Filtering Service is enabled and configured in line with best practices and company policy to provide the maximum protection to users and company resources.* *Objective(s): In the Proxies tab, open the HTTP menu and click on the 'edit' SimCoat policy option under the Surf Protection Profiles box, and check that policy is configured with the expected parameters.* *Source(s):* SCP Firewall Policy, SCP Audit Policy, SCP Acceptable Use Policy	Categories: 1. Criminal Activities 2. Drugs 3. Extremistic_Sites 4. Games_Gambles 5. Job_Search 6. Nudity 7. Private_Homepages 8. Weapons *Users:* Empty *Source Network:* Corporate LAN *Whitelist:* Empty *Blacklist:* Empty	As above. This is also one of the Critical Controls identified in the Risk Analysis. Failure to implement the Content Filtering effectively will contribute to continued Cyber-Slacking.	O/P C IV MOD

Objective, Testing and References	Compliance/Expected Results	Risk	
V.F DNS Proxy *Objective(s): To ensure that the DNS Proxy Service is enabled and configured in line with best practices and company policy to provide the maximum protection to users and company resources. In the Proxies tab, open the DNS menu and check that the DNS Proxy is configured with the expected parameters.* *Source(s):* SCP Firewall Policy, SCP Audit Policy, SCP Acceptable Use Policy	Status: Enabled DNS admin e-mail: trouble@scp.net Interfaces to listen on: Backend Zone Corporate LAN Public DMZ Allowed Networks: Backend_Zone_Network Corporate_Lan_Network Public_DMZ_Network Forwarding Name Servers: 1x9.1xx.5.xxx 1x9.1xx.2.xxx 1x9.1xx.2.xxx	Ensuring that only the required services are enabled and are configured properly reduces the likelihood of misconfiguration that may lead to a vulnerability and exposure. Failure of the system to perform as expected and required can lead to the users attempting to circumvent the controls i mposed by the system.	O/B B III LOW
V.G POP3 Proxy *Objective(s): To ensure that the POP3 Proxy Service is enabled and configured in line with best practices and company policy to provide the maximum protection to users and company resources. In the Proxies tab, open the POP3 menu and check that the Transparent POP3 Proxy is configured with the expected parameters.*	Configured Proxied Networks Source: Corporate_Lan_Network Destination: MailServer01 Virus Protection: Enabled	This is one of the Critical Controls identified in the Risk Analysis. Failure to impl ement the POP3 Proxy effecti vely may contribute to Viru s Outbreaks and contribute to poor use of company resources in dealing with SPAM.	O/P E IV

Objective, Testing and References	Compliance/Expected Results	Risk	
parameters. *Source(s):* SCP Firewall Policy, SCP Audit Policy, SCP Acceptable Use Policy			HIGH
V.H SMTP Proxy *Objective(s): To ensure that the SMTP Proxy Service is enabled and configured in line with best practices and company policy to provide the maximum protection to users and company resources. In the Proxies tab, open the SMTP menu and check that the Proxy is configured with the expected parameters.* *Source(s):* SpamAssassin™ Documentation *Source(s):* SCP Acceptable Use Policy, SCP Firewall Policy, Astaro Manual	Status: Enabled Hostname MX: mail.scp.com Postmaster Address: *postmaster@scp.net* Max message size: 5MB Incoming Mail: SMTP Routes Table *Domain name:* scp.net *SMTP host:* Mail-Server01 Outgoing Mail: Allowed Networks Corporate_Lan_Network Mail-Server01 Use smarthost: Disabled Use callouts: Disabled Sender Blacklist: Enabled Spam detection: Enabled *Action:* Quarantine *Strategy:* Conservative	Ensuring that only the required services are enabled and are configured properly reduces the likelihood of misconfiguration that may lead to a vulnerability and exposure. This is also one of the Critical Controls identified in the Risk Analysis. Failure to implement the SMTP Proxy effectively will contribute to continued Virus Outbreaks and poor use of company resources in dealing with SPAM.	O/P E IV

Objective, Testing and References	Compliance/Expected Results	Risk	
	Block RCPT hacks: Enabled Virus Protection: Enabled *Action:* Quarantine Realtime Blackhole Lists (RBL): Enabled *Action:* Reject *Zones:* Blackholes.mail-abuse.org File extension filter: Enabled *Extensions:* .com, .pif, .bat, .vbs, .scr, .exe Expression filter: Enabled		HIGH
VI CONFIG: PACKET FILTERING *Objective(s): To ensure that the Stateful Inspection Packet Filter is configured in line with best practices and company policy to provide the maximum protection to users and company resources. In the Packet Filter, open the Rules menu and check that the SIPF Rules are configured with the expected parameters.*			
VI.A <u>Packet Filter</u> *Objective(s): Review firewall rules to verify every packet is by default denied unless a specific rule exists to permit the packet to proceed but only to a destination system in the DMZ segment. Identify the filtering rules in place (to determine if*	Compliance requires that the ruleset effectively restrict unauthorized access to network assets in line with the least privilege principals detailed in the SCP firewall policy.	Ensuring that only the required rules are implemented ensures that access is restricted to potentially vulnerable services.	O/P E

Objective, Testing and References	Compliance/Expected Results	Risk	
they address all the issues included in the security policy and other applicable threats identified during the risk analysis). Verify that the overall firewall rule restrict access, unless specifically allowed by the rules. *Source(s):* ISACA: Procedure 7, Firewalls	Inversely it must also provide the required access to network resources as required by the firewall policy. The Ruleset below was developed in conjunction with SCP technicians to effectively implement SCP policies.		V HIGH

VI.A Cont'd

Objective(s): In many cases, firewall policy can be verified using one of two methodologies. The first methodology, and by far the easiest, is to obtain hardcopies of the firewall configurations and compare these hardcopies against the expected configuration based on defined policy. All organizations, at a minimum, should utilize this type of review.

Source(s): NIST Guidelines on Firewalls; sp800 -41, Section 4.3 Testing Firewall Policy

From Hostname	Service(s)	To Server	Rule
Corp LAN DC02	NTP	Syslog Wkstn	Allow
Corp LAN DC02	Windows-SMB	Backend LAN-DC01	Allow
Corporate Lan [20.0/24]	Any	Any	Log-Reject
Syslog Wkstn	NTP	FTP Server01	Allow
Management-PC 1	MS Terminal Services	Public DMZ	Allow
Management-PC 2	MS Terminal Services	Public DMZ	Allow
Management-PC 1	FTP {active}	Public DMZ	Allow
Management-PC 2	FTP {active}	Public DMZ	Allow
All RFC 1918 Private	Any	Any	Log-Reject
Any	HTTP	Web Server01	Allow
Any	HTTPS	Web Server02	Allow
Any	FTP {active}	FTP Server01	Allow
Public_DMZ [25.16/29]	SYSLOG	Syslog Wkstn	Allow
Web Server02	MySQL {3306}	MySQL Server	Allow
Any	Any	Any	Log-Reject

Objective, Testing and References	Compliance/Expected Results	Risk	
VI.B <u>Config: ICMP Settings</u> *Objective(s): To ensure that the Stateful Inspection Packet Filter is configured in line with best practices and company policy to provide the maximum protection to users and company resources. In the Packet Filter, open the ICMP menu and check that the ICMP Rules are configured with the expected parameters.*	Config: ICMP Settings: ICMP Settings. ICMP Forwarding: Enabled ICMP on Firewall: Enabled Traceroute Settings. Firewall is traceroute visible: Enabled Firewall forwards traceroute: Enabled Traceroute from Firewall: Disabled PING Settings. Firewall is PING visible: Enabled Firewall forwards PING: Enabled PING from firewall: Disabled	Ensuring that only the required rules are implemented ensures that access is restricted to potentially vulnerable services. Additionally allowing the use of PING permanently reduces the support overhead of troubleshooting network related problems. This in turn minimises on-the-fly firewall changes to test connectivity.	O/P B III LOW

Objective, Testing and References	Compliance/Expected Results	Risk	
VII LINUX OS *Objective(s): Evaluate the Firewall's Base OS Hardening.* **Procedure:** Have one of the SCP administrators log on to the Web-Admin interface and in the **System>Settings** Tab Enable the SSH Daemon. Then have them log on to the FW via SSH, and SU to ROOT. Perform each of the tests below, copying and pasting the output to a log file named according to the test. **NB: Upon completion disable the SSH Daemon again.**			
VII.A Root Account. *Objective(s): To ensure that "root" logins are automatically logged out after an acceptable period of inactivity. Check the profile file **(/etc/profile)** to see whether the TMOUT value is set.* **# cat /etc/profile** *Source(s):* Securing and Optimizing Linux: The Ultimate Solution	TMOUT=1800	"Despite the notice to never if they are not on the server, sign in as "root" and leave it unattended (ed. see Astaro Docs which recommend not to use SSH), administrators might still stay on as "root" or forget to logout after finishing their work and leave their terminals unattended." This might provide unauthorised admin access to the firewall, leading to total system compromise.	O/P D III MOD

Objective, Testing and References	Compliance/Expected Results	Risk	
VII.B Default File Permissions. *Objective(s): To assess the default umask.* **# cat /etc/profile** *Source(s):* Securing and Optimizing Linux: The Ultimate Solution, Center For Internet Security, Linux Benchmark v1.0.0	This is both an objective and subjective assessment. The default umask should be set as restrictive as possible. The most restrictive setting would be 077 while 022 is considered acceptable.	"The umask command can be used to determine the default file creation mode on your system. It is the octal complement of the desired file mode. If files are created without any regard to their permissions settings, the user could inadvertently give read or write permission to someone that should not have this permission."	O/P B III LOW
VII.C Inittab Configuration. *Objective(s): A.) To ensure that "Linux Single" mode is protected. The use of sulogin will require the user to enter the root password before continuing to boot into single-user mode by making init (8) run the program sulogin (8) before dropping the machine into a root shell for maintenance.* *Objective(s): B.) To ensure that the system cannot be inadvertently rebooted via the keyboard when sharing a KVM switched console/keyboard.* *Source(s):* Securing and Optimizing Linux: The Ultimate Solution, Center For Internet Security, Linux Benchmark v1.0.0	**A.)** NB: "***rc s***" is the Single User Mode Runtime Level. Compliance: ls:S:wait:/sbin/init.d/rc S ~~:S:respawn:/sbin/sulogin	**A.)** "Linux has a special command (linux single) also known as 'single-user mode', which can be entered at the boot prompt during startup of the system. The single-user mode is generally used for system maintenance. You can boot Linux in single-user mode by typing at the LILO boot prompt the following command:LILO: linux single This will place the system in Run level 1 where you'll be logged in as the super-user 'root', and where you won't even have to	O/P D

Objective, Testing and References	Compliance/Expected Results	Risk	
# cat /etc/inittab	**B.)** The ca::ca::ctrlaltdel: line should be commented out as below. **#**ca::ctrlaltdel:/sbin/shutdown -r -t X now	where you won't even have to type in a password! Requiring no password to boot into root under single-user mode is a bad idea!" **B.)** In shared environments with racked and stacked systems it is common for multiple systems to utilise KVM type Keyboard, Mouse and Monitor switches. One of the potential risks in these environments is inadvertently rebooting the wrong system via the Ctrl-Alt-Del keystroke combination.	III MOD

Objective, Testing and References	Compliance/Expected Results	Risk	
VII.D Lilo.Conf Configuration and Security. *Objective(s): To ensure that command line parameters such as "linux single" are authorized before being processed by LILO, the Linux boot loader.* **# cat /emergency/boot/etc/lilo.conf** *Objective(s): As this file now contains an unencrypted password it is important that it is readable only by "root".* **# ls -al /emergency/boot/etc/lilo.conf** *Source(s):* Securing and Optimizing Linux: The Ultimate Solution, Center For Internet Security, Linux Benchmark v1.0.0	The file should contain the following lines *restricted* *password*=<some password> NB: Lilo.conf must contain both of the above. If only "password" is used, the system will require the password every time it is rebooted. The "restricted" parameter uses the password test only when command line parameters are entered during boot. ***-rw-------** 1 root root xxx Mon D HH:SS /emergency/boot/etc/lilo.conf*	"LILO is the most commonly used boot loader for Linux. It manages the boot process and can boot Linux kernel images from floppy disks, hard disks or can even act as a "boot manager" for other operating systems. LILO is very important in the Linux system and for this reason, we must protect it the best we can. The most important configuration file of LILO is the lilo.conf file, and it resides under the /etc directory."	O/P B IV LOW
VII.E User Accounts and Groups *Objective(s): To assess and minimize the existence of unnecessary User and Group Accounts.* **# cat /etc/passwd** **# cat /etc/groups** *Source(s):* Securing and Optimizing Linux: The Ultimate Solution, Center For Internet Security, Linux Benchmark v1.0.0	This is a subjective assessment. The account and group membership should in the auditors view reflect the functionality of the system.		S/P B III LOW

Objective, Testing and References	Compliance/Expected Results	Risk	
VII.F Programs with root-owned bits. *Objective(s): To assess and minimize the number of executables with either the SUID or SGID parameter set.* **# find / -type f \(-perm -04000 -o -perm -02000 \) -exec ls -l {} \;** *Source(s):* Securing and Optimizing Linux: The Ultimate Solution, Center For Internet Security, Linux Benchmark v1.0.0	This is a subjective assessment. The system should have the absolute minimum number of programs and files with either SUID or SGIID set.	"A regular user will be able to run a program as root if it is set to SUID root. All programs and files on your computer with the 's' bits appearing on its mode, have the SUID (-rwsr-xr-x) or SGID (-r-xr-sr-x) bit enabled. Because these programs grant special privileges to the user who is executing them, it is important to remove the 's' bits from root-owned programs that won't absolutely require such privilege."	S/P B III LOW
VII.G Group and World-writable Files. *Objective(s): To assess and minimize the number of Group and World writable files on the system.* To locate all group & world-writable files on the system, use the command: **# find / -type f \(-perm -2 -o -perm -20 \) -exec ls -lg {} \;** To locate all group & world-writable directories on the system, use the command: **# find / -type d \(-perm -2 -o -perm -20 \) -exec ls -ldg {} \;**	This is a subjective assessment. The system should have the absolute minimum number of files or directories that are Group or World writable.	"Group and world writable files and directories, particularly system files, can be a security hole if a cracker gains access to your system and modifies them. Additionally, world writable directories are dangerous, since they allow a cracker to add or delete files as he or she wishes in these directories. In the normal course of operation, several files will be writable, including some from the /dev/, /var/catman/ directories, and all	S/P B III

Objective, Testing and References	Compliance/Expected Results	Risk	
-exec ls -ldg {} \; *Source(s):* Securing and Optimizing Linux: The Ultimate Solution, Center For Internet Security, Linux Benchmark v1.0.0		/var/catman/ directories, and all symbolic links on your system" Securing and Optimizing Linux: The Ultimate SolutionPg 87	LOW
VII.H Check Fstab configuration. *Objective(s): To assess "root" only access to mountable drives.* **# cat /etc/fstab > vii.h.log** *Source(s):* Securing and Optimizing Linux: The Ultimate Solution, Center For Internet Security, Linux Benchmark v1.0.0	Any entires for *floppy* and *cdrom* should have *nosuid* set if they exist at all. The ideal configuration would see no *supermount* entries whatsoever.	"Removable media is one vector by which malicious software can be introduced on to the system. By forcing these file systems to be mounted with the `nosuid` option, the administrator prevents users from bringing set-UID programs onto the system via CD-ROMs and floppy disks."	O/P B III LOW
VII.I Zero password accounts. *Objective(s): To verify that no accounts exist with empty passwords* **# awk -F: '($2 == "") { print $1 }' /etc/shadow** *Source(s):* Securing and Optimizing Linux: The Ultimate Solution, Center For Internet Security, Linux Benchmark v1.0.0	The command should return no lines of output.	"An account with an empty password field means that anybody may log in as that user without providing a password at all."	O/P B III LOW

Objective, Testing and References	Compliance/Expected Results	Risk	
VII.J UID 0 accounts *Objective(s): Verify that no UID 0 accounts exist other than root* **# awk -F: '($3 == 0) { print $1 }' /etc/passwd** *Source(s):* Securing and Optimizing Linux: The Ultimate Solution, Center For Internet Security, Linux Benchmark v1.0.0	The command should only return the word "root".	"Any account with UID 0 has superuser privileges on the system. The only superuser account on the machine should be the `root` account."	O/P B III LOE
VII.K System Overview *Objective(s): To assess the overall security posture of the base Linux OS. Using the auditors expert judgment in consultation with the SCP engineers, assess the overall configuration of the system.* *Objective(s): Consider the evidence of baseline hardening, removal of unnecessary binaries, services, compilers, shells, etc. Try to develop a sense of the vendors overall approach to securing the system. Note any observations that diminish or affect the systems security.* *Source(s):* Securing and Optimizing Linux: The Ultimate Solution, Center For Internet Security, Linux Benchmark v1.0.0, Personal experience	This is a very subjective assessment. We instinctively develop an opinion while performing the audit; this checklist item simply attempts to record the overall consensus impression, and allow the audit team to investigate the system further based on their joint expertise.	This is a catchall assessment item. The risk of not providing an opportunity to provide a general impression may result in vulnerabilities slipping through the cracks, as they are not easily detected by any other checklist item.	S/P B IV LOW
VIII FIREWALL PERFORMANCE *Objective(s): In this section of the audit we design and execute a range of tests to evaluate the effectiveness of the SIPF and application proxies*			

Objective, Testing and References	Compliance/Expected Results	Risk	
in enforcing SCP policies.			
SIPF: *Objective(s): Design and perform testing of traffic that will be affected by SIPF, to verify its proper functioning. Confirm the firewall has been tested by scanning every segment, including the DMZ segment, from every other segment to identify what packets can and cannot get through. Provide reasonable assurance the results are consistent with the overall security policy.* *Source(s):* ISACA: Procedure 7, Firewalls *Objective(s): The second methodology (see # 36 above) involves actual in-place configuration testing. In this methodology, the organization utilizes tools that assess the configuration of a device by attempting to perform operations that should be prohibited.* *Source(s):* NIST Guidelines on Firewalls; sp800-41, Section 4.3 Testing Firewall Policy Using NMAP , perform the suite of port scans detailed in Appendix 7.2. **NB: Perform each of the tests with the PortScan Detector enabled (a) and disabled (b).** *Source(s):* Open Source Security Testing Methodology Manual, pg 21, Port Scanning	IP addresses of live systems and Open, Closed or Filtered ports: All unauthorised ports should be filtered or closed. In each test where the PortScan Detector is Enabled there should be no OPEN ports anywhere, regardless of existent Allow rules in the firewall ruleset. Where the PSD has been disabled, only the ports detailed in each of the following subsections should be OPEN.	A failure in the performance of the SIPF may result in a vulnerable service or system being exploited through the weak access control, resulting in some measure of exposure to the company. As this is a primary control within the firewall, it is imperative that it preforms as expected and accurately regulates access and egress under a wide range of conditions.	

Objective, Testing and References	Compliance/Expected Results	Risk	
VIII.A PortScan Detection and Event Notification. *Objective(s): Confirm firewall rules discover external attempts to scan for commonly scanned ports (regardless of whether systems actually exist to listen on such ports). Using any suitable portscanner, attempt to enumerate listening services on the external Internet interface of the firewall.* *Objective(s): Confirm Event Notifications for checklist items III.N User Auth, III.J Email Backup, III.H Up2Date Service and the above PSD Event are all sent to the addresses defined in checklist item III.B.* *Source(s):* ISACA: Procedure 7, Firewalls	The Portscan detector should detect the port-scan and then silently Drop all connection attempts as per the SCP Firewall policy. The Scan should show no OPEN ports. The PSD should generate both Syslog Events and Alert Emails to the Administrator addresses outlined in III.B above.	Timely notification of attack can afford the company the precious minutes required to respond effectively to mitigate any newly identified vulnerability or threat that the port-scan represents.	O/C F I LOW
VIII.B Internet -> External Firewall Interface *Objective(s): Test connectivity and SIPF from the Internet to the Firewall's external interface.* *Source(s):* See: SIPF Performance above	Only the following IP:Port combinations should be OPEN. 184.35.53.97:25	A failure in the performance of the SIPF may result in a vulnerable service or system being exploited through the weak access control, resulting in some measure of exposure to the company. As this is a primary control within the firewall, it is imperative that it preforms as expected and accurately regulates access and egress under a wide range of conditions.	O/P D IV HIGH

Objective, Testing and References	Compliance/Expected Results	Risk	
VIII.C Internet à Public DMZ *Objective(s): Test connectivity and SIPF from the Internet to the Public DMZ Hosts. Use any valid Internet Source address.* *Source(s):* See: SIPF Performance above	Only the following IP:Port combinations should be OPEN. 184.112.25.18:80 184.112.25.19:443 184.112.25.20:21	See VIII.B risk above.	O/P D IV HIGH
VIII.D Public DMZ à Public DMZ Interface *Objective(s): Test for listening services on the Public DMZ firewall interface.* *Source(s):* See: SIPF Performance above	Only the following IP:Port combinations should be OPEN. 184.112.25.17:53	See VIII.B risk above.	O/P C IV MOD
VIII.E Public DMZ à Internet *Objective(s): Test connectivity and SIPF from the Public DMZ Hosts to the Internet.* **NB:** Use an authorized Internet Destination address. Use our external Cabl e System. **NB:** All egress should be denied except NTP access as defined in the Firewall Policy	Only the following IP:Port combinations should be allowed egress. 184.112.25.20→ 129.127.40.3:123 184.112.25.20→ 203.21.84.4:123	See VIII.B risk above.	O/P B III LOW

Objective, Testing and References	Compliance/Expected Results	Risk	
VIII.F Public DMZ à Backend LAN *Objective(s): Test connectivity and SIPF from each of the Public DMZ Hosts to the Backend LAN. Use each Public DMZ Source address in turn to perform the tests.* *Source(s):* As above	Only the following IP:Port combinations should be OPEN. 184.112.25.20→ 192.168.10.20:3306 184.112.25.18-20→ 192.168.10.50:514	See VIII.B risk above.	O/P B III LOW
VIII.G Public DMZ à Corporate LAN *Objective(s): Test connectivity and SIPF from the Public DMZ to the Corporate LAN. Use any Public DMZ Source address to perform the tests, as all access should be denied.* *Source(s):* See: SIPF Performance above *Objective(s): Confirm systems on the DMZ segment are set up so that they cannot initiate communications with the interior. Again, if exceptions exist, evaluate the specific risks, justification and compensating controls* *Source(s):* ISACA: Procedure 7, Firewalls	No IP:Port combinations should be OPEN.	See VIII.B risk above.	O/P B III LOW
VIII.H Backend LAN à Backend LAN Interface	Only the following IP:Port combinations should be OPEN.	See VIII.B risk above.	O/P

Objective, Testing and References	Compliance/Expected Results	Risk	
Objective(s): Test for listening services on the Backend LAN firewall interface. *Source(s):* See: SIPF Performance above	should be OPEN. 192.168.10.100:53 192.168.10.30→ 192.168.10.100:25 192.168.10.60→ 192.168.10.100:443 192.168.10.61→ 192.168.10.100:443		B III LOW
VIII.I <u>Backend LAN à Internet</u> *Objective(s): Test connectivity and SIPF from the Backend LAN to the Internet. Use any Backend LAN Source address to perform the tests, as all access to the Internet should be denied.* **NB:** Use an authorized Internet Destination address. Use our external Cable System. **NB:** All egress should be denied as defined in the Firewall Policy	No IP:Port combinations should be OPEN.	See VIII.B risk above.	O/P B III LOW
VIII.J <u>Backend LAN à Public DMZ</u> *Objective(s): Test connectivity and SIPF from the Backend LAN to the Public DMZ. Use any Backend LAN address to perform the tests, as all access should be denied.* *Source(s):* See: SIPF Performance above.	Only the following IP:Port combinations should be OPEN. 192.168.10.60→ 184.112.25.17-19:21 192.168.10.61→ 184.112.25.17-19:21 192.168.10.60→ 184.112.25.17-19:3389 192.168.10.61→ 184.112.25.17-19:3389	See VIII.B risk above.	O/P B III LOW
VIII.K <u>Backend LAN à Corporate LAN</u> *Objective(s): Test for listening services on the Corporate LAN firewall interface*	No IP:Port combinations should be OPEN.	See VIII.B risk above.	O/P

Objective, Testing and References	Compliance/Expected Results	Risk	
Corporate LAN firewall interface. *Source(s):* See: SIPF Performance above. *Objective(s): Confirm systems on any DMZ segment are set up so that they cannot initiate communications with the interior. Again, if exceptions exist, evaluate the specific risks, justification and compensating controls* *Source(s):* ISACA: Procedure 7, Firewalls			B III LOW
VIII.L Corporate LAN à Corporate LAN Interface *Objective(s): Test connectivity and SIPF from the Backend LAN to the Corporate LAN. Use any Backend LAN Source address to perform the tests, as all access to the Corporate LAN should be denied.* *Source(s):* See: SIPF Performance above.	Only the following IP:Port combinations should be OPEN. 192.168.20.1:25 192.168.20.1:53 192.168.20.1:8080	See VIII.B risk above.	O/P B III LOW
VIII.M **Corporate LAN à Internet** *Objective(s): Test connectivity and SIPF from the Corporate LAN to the Internet. Use any Corporate LAN Source address to perform the tests, as all access to the Internet should be denied except which utilizes the proxies.* **NB:** Use an authorized Internet Destination address. Use our external Cable System.	No Destination IP:Port combinations on the Internet should be reachable directly.	See VIII.B risk above.	O/P B III

Objective, Testing and References	Compliance/Expected Results	Risk	
NB: All egress should be denied as defined in the Firewall Policy *Source(s):* See: SIPF Performance above			LOW
VIII.N Corporate LAN à Public DMZ *Objective(s): Test connectivity and SIPF from the Corporate LAN to the Public DMZ. Use any Corporate LAN Source address to perform the tests, as all access to the Internet should be denied except that which utilizes the proxies.* *Source(s):* See: SIPF Performance above	No Destination IP:Port combinations in the Public DMZ should be reachable.	See VIII.B risk above.	O/P B III LOW
VIII.O Corporate LAN à Backend LAN *Objective(s): Test connectivity and SIPF from the Corporate LAN to the Backend. Use any Corporate LAN Source address to perform the initial tests, as all access to the Backend LAN should be denied except that which utilizes the proxies, with the exception of the Corporate LAN DC Win2KDC02.* *Source(s):* See: SIPF Performance above	Only the following IP:Port combinations should be OPEN. 192.168.20.10→ 192.168.10.40:445	See VIII.B risk above.	O/P B III LOW
IX PROXY PERFORMANCE *Objective(s): To assess the performance of each service in providing effective controls as defined in the Firewall Policy.*		Ensuring that the required services are enabled and are configured properly reduces the likelihood of misconfiguration that may lead to a vulnerability and exposure.	

Objective, Testing and References	Compliance/Expected Results	Risk	
Objective(s): Design and perform testing of traffic that will be affected by each of the proxy controls, considering the following: • *Confirm all traffic is directed to the proxy* • *Confirm that all traffic of the type being proxied is only processed from the address of the proxy.* *Source(s):* ISACA: Procedure 7, Firewalls, SCP Firewall Policy		and exposure.	
IX.A DNS Proxy. *Objective(s): See F: Proxy Performance.* A. From each of the 3 SCP subnets open a shell and use *nslookup* or *host* to resolve www.giac.org. B. From each of the above hosts, set the resolver to use the ISP's remote DNS server via the "server" command, and retest the resolution of www.giac.org	A. Each client should be able to resolve the host to: Name: giac2.giac.org Address: 65.173.218.106 Aliases: www.giac.org B. Each host should fail to resolve www.giac.org	Failure of the system to perform as expected and required can lead to the users attempting to circumvent the controls i mposed by the system.	O/P B III LOW
IX.B HTTP/S & FTP Proxy. *Objective(s): See F: Proxy Performance. Using a Web-browser configured to use the local subnets Firewall Interface IP address and Port 8080 as it's proxy, test each of the following Url's using the credentials of a user within a regular Windows Domain employee group.*	For either the Public DMZ or the Backend LAN, there should be no Connectivity to the WWW via the Squid proxy. 1 (a-j) = Failure to connect to proxy. 2 (a–j) = Failure to connect to proxy. 3a = Successful negotiation of a connection subsequent to authorisation	Ensuring that the required services are enabled and are configured properly reduces the likelihood of misconfiguration that may lead to a vulnerability and exposure. This is also one of the Critical Controls identified in the Risk	O/P

Objective, Testing and References	Compliance/Expected Results	Risk	
Windows Domain employee group. Use each combination available between network (1-3) and Url (a-i). 1 = Public DMZ 2 = Backend LAN 3 = Corporate Lan a) http://www.giac.org b) http://www.playboy.com c) http://www.undercoverexperience.co.uk d) http://www.skinheadz.com e) http://www.monster.com f) http://www.gunsmagazine.com g) http://www.gambling.com h) http://www.organja.com i) http://www.hackcanada.com/telco/miscarchive.html j) ftp://mirror.aarnet.edu.au *Source(s):* Personal experience, SCP Firewall Policy	connection subsequent to authorisation. Syslog should record successful authorisation event with user credentials, and authorisation source. 3(b-i) Each of these should fail with a different proxy response for each category of event. 3b = Pornography 3c = Swimwear/Lingerie/Nudity 3d = Hate and Discrimination 3e = Job Search 3f = Weapons 3g = Gambling 3h = Illegal Drugs 3i = Illegal Activities 3j = Successful negotiation of FTP session to remote archive site subsequent to user authorisation.	Controls identified in the Risk Analysis. Failure to implement the Squid Proxy effectively will contribute to continued Cyber Slacking.	E III MOD
IX.C POP Proxy. *Objective(s): See F: Proxy Performance. Using a POP3 client from each of the local subnets to test the Firewall and it's POP3 proxy.*	For either the Public DMZ or the Backend LAN, there should be no Connectivity to the POP3 proxy.	Ensuring that the required services are enabled and are configured properly reduces the likelihood of misconfiguration that may lead to a vulnerability and exposure.	O/P E

Objective, Testing and References	Compliance/Expected Results	Risk	
Use each of the following networks: 1 = Public DMZ 2 = Backend LAN 3 = Corporate Lan	For the Corporate LAN (3), the Firewalls POP3 proxy should provide transparent access to the Mail Server on the Backend LAN, allowing users to retrieve their mail effectively.	and exposure. This is also one of the Critical Controls identified in the Risk Analysis. Failure of the POP3 Proxy to effectively control email-borne Virii will contribute to continued Virus Outbreaks.	IV HIGH
IX.D <u>SMTP Proxy.</u> *Objective(s): See F: Proxy Performance. Using an SMTP client from each of the local subnet, test the Firewall and it's SMTP proxy.* From each of the following networks attempt a connection to port 25 on the firewalls interface; 1 = Public DMZ 2 = Backend LAN 3 = Corporate Lan 4 = Internet For each successful connection attempt to send: a) A plain-text email, b) An html-based email, c) Each of the Anti-Virus Test files as attachments; Eicar.com, Eicar.com.txt,	For either the Public DMZ or the Backend LAN, there should be no Connectivity apart from the Mail Server. to the SMTP proxy, Access should be allowed from any host on the Corporate LAN and Internet. Each case of tests A and B should be successful, while all tests under C and D should be received by the SMTP proxy but result in the email being quarantined by the Kapersky Antivirus system. Check the Proxy Content Manager under the Proxies tab in Web Admin to see whether the emails in C(I to iv) and any of D have be quarantined.	As IX.C above. Failure of the SMTP Proxy to effectively control email-borne Virii will contribute to continued Virus Outbreaks.	O/P E IV

Objective, Testing and References	Compliance/Expected Results	Risk	
Eicar_com.zip, and Eicarcom2.zip d) Each of the extension test files: .vbs, .bat, .pif, .exe or , and a .scr attachment. *Source(s):* http://www.eicar.org			HIGH
IX.E Logging. *Objective(s): Monitor, audit and incident response. Monitor firewall alerts on a continuous basis. Review the procedures to review the logs in an effective and timely manner and to deal with potential harmful traffic.* *Objective(s): Determine the logging functionality in place.* *Source(s):* ISACA: Procedure 7, Firewalls, SCP Firewall Policy	This is a subjective assessment. Assess the logging functionality of the Firewall, both local and via the remote syslog facility. Critical events should be logged such as authorisation failures of proxy services and Management Interfaces, Virus events, Dropped or Denied packet-filter events and PortScans.	Failure to record events may result in events occurring which are not responded too, and a lack of evidence or audit trail when investigating an event.	O/D D II LOW
IX.F Backups. *Objective(s): The conduct and maintenance of backups are key points to any firewall administration policy. All firewalls should be subject to a Day Zero backup. All firewalls should be backed up immediately prior to production release. As a general principal, all firewall backups should be full backups. There is no real requirement or need for incremental backups.*	Encrypted Backup files should be received daily via Email by each of the three administrative email addresses defined in the Firewall Policy. Additionally, Syslog must record these significant events also so as to maintain an effective audit trail.	Failure to regularly and completely back up the firewall reduces the company's ability to implement effective change control processes and affects the availability of the system via disaster recovery processes.	O/P C

			III

Objective, Testing and References	Compliance/Expected Results	Risk	
			C
Source(s): NIST Guidelines on Firewalls; sp800 -41, Section 5.6 Firewall Backups *Objective(s): Verify continuity plans for firewalls are in accordance with those of other high -availability services, as firewalls ordinarily are components related to services with high -availability requirements.*			MOD
ISACA: Procedure 7, Firewalls			O/D C I LOW

Objective, Testing and References	Compliance/Expected Results	Risk	
X VULNERABILITY ASSESSMENT **X.A Bulk Vulnerability Scan** *Objective(s): Firewall installations as well as systems and other resources must be audited on a regular, periodic basis. In some cases, these periodic reviews can be conducted on paper by reviewing hardcopy configurations provided by appropriate systems administration staff. In other cases, periodic reviews should involve actual audits and vulnerability assessments of production components.* Using ISS Internet Scanner 6.21 XPU 30, scan each of the Firewalls Interfaces using the Unix WebServer 5 policy with the Firewalls PSD service disabled. 1 = Public DMZ 2 = Backend LAN 3 = Corporate Lan 4 = Internet *Source(s):* NIST Guidelines on Firewalls; sp800 -41, Section 4.7 Testing Firewall Policy	This is a both an objective and subjective assessment. Compliance would be attained if there were an acceptably low number of identified vulnerabilities (objective tests) considering (subjective evaluation) the systems security related functionality as a Firewall. Ideally the reported number of vulnerabilities would be Zero however bulk scanners identify a large number of weaknesses that may or may not be important in our context. For example attaining a SMTP Banner is sometimes reported as Vulnerability, when in fact it may be obfuscation as the host may be misrepresenting itself as a different OS and SMTP daemon.	The purpose of a vulnerability scan is to discover hitherto unidentified risks. The risk of not performing the scan is that we may miss some undiscovered weakness in the system. These tests do not measure control's compliance but rather attempt to detect the lack of a control.	SO/D N/A N/A N/A
X.B HTTP Scan *Objective(s): Test the Web Admin interface for common http vulnerabilities.* A. From either of the Management Host systems create a connection profile for the Web Admin interface in SSL-Proxy on port 443, with port	This is an objective assessment. There should be no 'real' vulnerabilities reported by the scan.	The Web Admin service is the default administrative interface. Compromise of this interface may result in a total system compromise. These tests do not measure	O/D B

Objective, Testing and References	Compliance/Expected Results	Risk	
interface in SSL-Proxy on port 443, with port 80 used as the localhost listening port. Use N-Stealth to assess the https interface for vulnerabilities by redirecting the scan through 127.0.0.1:80. *Source(s):* The Open Web Application Security Project		control's compliance but rather attempt to detect the lack of a control.	V MOD
X.C Web Admin Access. *Objective(s): Test the Web Admin interface Authentication.* A.) Using a web-browser from one of the two Backend LAN Management Hosts attempt to log onto the Web Admin interface with bogus credentials. B.) Using a known-good username enter a blank password C.) Using a known-good username enter a bogus password	Test A. Access should be denied Test B. Access should be denied No prompts should be returned that disclose a Good account name. This inhibits brute force account name guessing. Test C. Access should be denied Prompts should not be returned that disclose which parameter failed. This inhibits brute force account name guessing.	The Web Admin service is the default administrative interface. Compromise of this interface may result in a total system compromise. These tests do not measure control's compliance but rather attempt to detect the lack of a control.	O/D B V IV

3 ASSIGNMENT 3. AUDIT FIELDWORK

3.1 Audit Scoring

To measure the audit subject's compliance with the audit checklist we use a qualitative scoring schema. This reflects the subjective nature of the assessment process and provides consistency throughout the assessment.

Table 3-1. Scoring Criteria

Score	Condition
1	Fails, poses immediate high-risk vulnerability.
2	Partially fails, performs unexpectedly, poses low risk vulnerability.
3	Passes, meets control expectations.
4	Passes, exceeds requirements, provides additional features.

Using this criteria we scored the Audit Checklist in the following table.

Table 3-2. Audit Results.

ü	1	2	3	4	ü	1	2	3	4	ü	1	2	3	4	ü	1	2	3	4	ü	1	2	3	4
Planning					**Services-Off**					VII.H					IX.B.1e		ü			IX.D.1a			ü	
I.A		ü			IV.A		ü			VII.I					IX.B.1f		ü			IX.D.1b			ü	
I.B		ü			IV.B		ü			VII.J					IX.B.1g		ü			IX.D.1c			ü	
I.C		ü			IV.C		ü			VII.K				ü	IX.B.1h		ü			IX.D.1d			ü	
I.D		ü			IV.D		ü			**SIPF Perf**					IX.B.1i		ü			IX.D.2a			ü	
I.E		ü			IV.E		ü			VIII.A		ü			IX.B.1j		ü			IX.D.2b			ü	
Policies					IV.F		ü			VIII.B		ü			IX.B.2a		ü			IX.D.2c			ü	
II.A		ü			**Services-On**					VIII.A		ü			IX.B.2b		ü			IX.D.2d			ü	
II.B		ü			V.A		ü			VIII.B		ü			IX.B.2c		ü			IX.D.3a			ü	
Configuration					V.B		ü			VIII.C		ü			IX.B.2d		ü			IX.D.3b			ü	
III.A		ü			V.C		ü			VIII.D		ü			IX.B.2e		ü			IX.D.3c			ü	
III.B		ü			V.D		ü			VIII.E		ü			IX.B.2f		ü			IX.D.3d			ü	
III.C		ü			V.E		ü			VIII.F		ü			IX.B.2g		ü			IX.D.4a			ü	
III.D		ü			V.F		ü			VIII.G		ü			IX.B.2h		ü			IX.D.4b			ü	
III.E		ü			V.G		ü			VIII.H		ü			IX.B.2i		ü			IX.D.4c			ü	

III.F	ü	V.H	ü	VIII.I	ü		IX.B.2j	ü	IX.D.4d		ü
III.G	ü	**SIPF-Config**		VIII.J		ü	IX.B.3a	ü	IX.E	ü	
III.H	ü	VI.A	ü	VIII.K		ü	IX.B.3b	ü	IX.F	ü	
III.I	ü	VI.B	ü	VIII.L		ü	IX.B.3c	ü	IX.G	ü	
IIIJ	ü	**Linux OS**		VIII.M		ü	IX.B.3d	ü	**Vuln-Assmt**		
III.K	ü	VII.A	ü	VIII.N		ü	IX.B.3e	ü	X.A1	ü	
III.L	ü	VII.B	ü	VIII.O		ü	IX.B.3f	ü	X.A2	ü	
III.M	ü	VII.A	ü	**Proxy Perf**			IX.B.3g	ü	X.A3	ü	
III.N	ü	VII.B	ü	IX.A.a		ü	IX.B.3h	ü	X.A4	ü	
III.O	ü	VII.C	ü	IX.A.b		ü	IX.B.3i	ü	X.B	ü	
III.P	ü	VII.D	ü	IX.B.1a		ü	IX.B.3j	ü	X.Ca	ü	
III.Q	ü	VII.E	ü	IX.B.1b		ü	IX.C.1	ü	X.Cb	ü	
III.R	ü	VII.F	ü	IX.B.1c		ü	IX.C.2	ü	X.Cc	ü	
	ü	VII.G	ü	IX.B.1d		ü	IX.C.3	ü	X.Cd	ü	

3.2 Audit Control Evidence.

In this section we present 10 examples of control audits from the Audit Checklist above that we consider critical to assuring that the firewall is functioning as desired and baselined accordingly.

3.2.1 Checklist Item II.b: Firewall Policy.

3.2.1.1 Purpose:

The purpose of testing this audit item is to ensure that the operation of the firewall is documented with an explicit configuration defined at the outset. This in turn defines how each of the firewall's controls are applied to SimCoat Plastics I.S. infrastructure. The Firewall policy must reflect and apply corporate policy.

3.2.1.2 II.b Test

The original policy was provided early in the engagement prior to the Entrance Conference. Subsequently we were able to work with SCP engineers to more explicitly define the policy through analysis of and reference to the Astaro Firewall User Guide.

3.2.1.3 II.b Compliance Evidence:

See Appendix 7.1 Below.

3.2.1.4 II.b Conclusion

Complies with checklist.

3.2.2 Checklist Item V.d: HTTP-S, FTP Proxy Configuration.

3.2.2.1 Purpose:

The HTTP Proxy is one of the critical controls SCP wish to implement. We have confirmed its Materiality by performing the Risk Assessment detailed in Section 1.6.2. It is envisaged that it will save the company a considerable amount of money and improve productivity.

By assessing the configuration in the first instance we can ensure that it will perform as expected. If this test is successful it can be followed by stimulus-response testing to ensure it functions correctly.

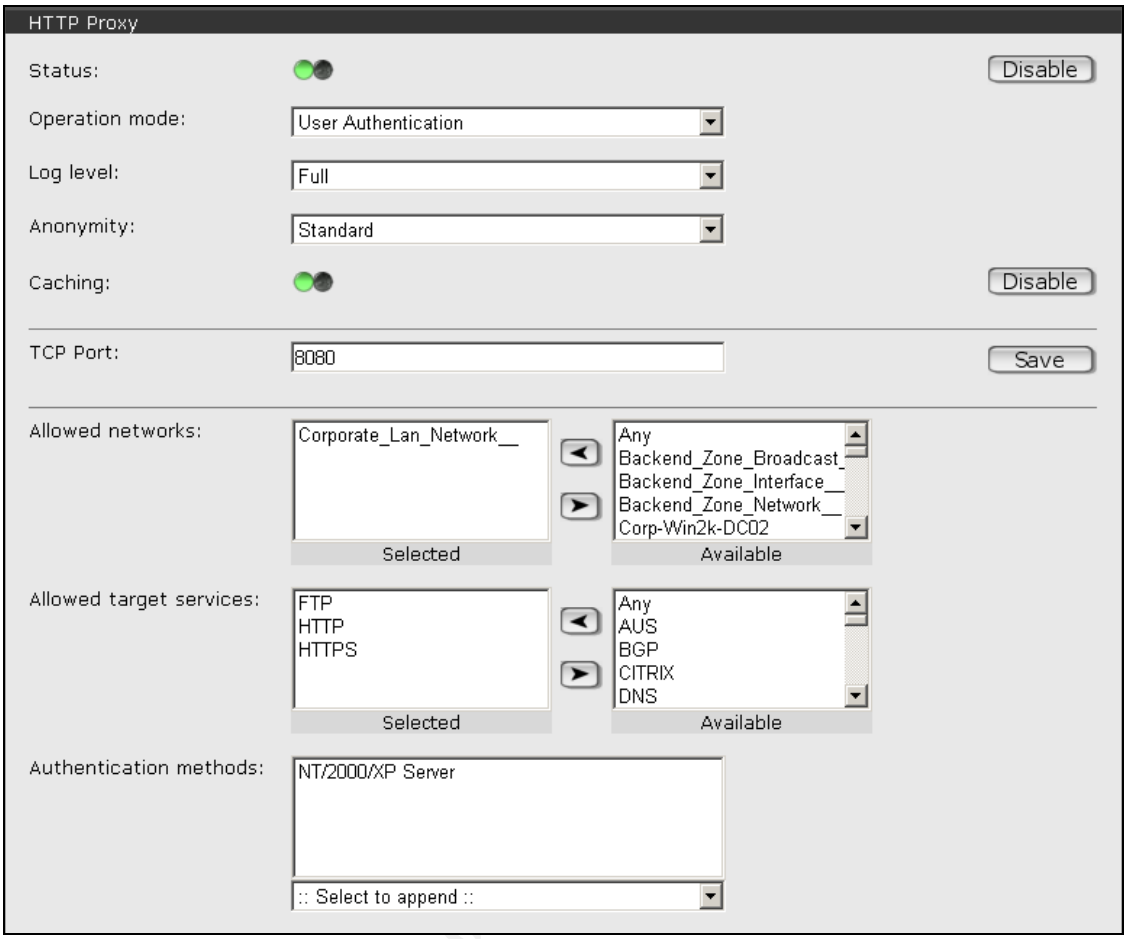
3.2.2.2 V.d Test

With one of the SCP administrators performing the work, we had them log onto the Astaro Web Admin interface from one of the two authorised management stations and open the ***Proxies>HTTP*** tab from the menu. Then, we checked that each item in the service control panel conformed to the expected configuration as detailed in item *V.D* of the checklist. The SCP Firewall Policy in Appendix 7.1 defined the expected configuration.

3.2.2.3 V.d Compliance Evidence:

The screenshot below shows compliance with desired configuration in Checklist Item *V.D* that was defined by the SCP Firewall Policy in Appendix 7.1.

Figure 3-1. Compliance Evidence Audit Item V.D.



3.2.2.4 V.D Conclusion

The configuration of the HTTP Proxy complies with the checklist.

3.2.3 Checklist Item VI: SMTP Proxy.

3.2.3.1 Purpose:

The SMTP Proxy is another of the critical controls SCP wish to implement. We have confirmed its Materiality by performing the Risk Assessment detailed in Section 1.6.2. It is envisaged that it will save the company a considerable amount of money and improve productivity by decreasing the number of Virus outbreaks per year, through the implementation of a SMTP Antivirus gateway.

By assessing its configuration in the first instance we can ensure that it will perform as expected. If this test is successful it can be followed by stimulus-response testing to ensure it functions as required.

3.2.3.2 VI Test

With one of the SCP administrators performing the work, we had them log onto the Web Admin interface from one of the two authorised management stations, and open the

Proxies>SMTP tab from the menu. Then, we checked that each item in the service control panel conformed to the expected configuration as detailed in item *VI* of the checklist. The SCP Firewall Policy in Appendix 7.1 defined the expected baseline configuration.

3.2.3.3 VI Compliance Evidence:

The screenshots 1-4 below show compliance with the expected configuration in Checklist Item *VI*.

Figure 3-2. SMTP Compliance Evidence 1.

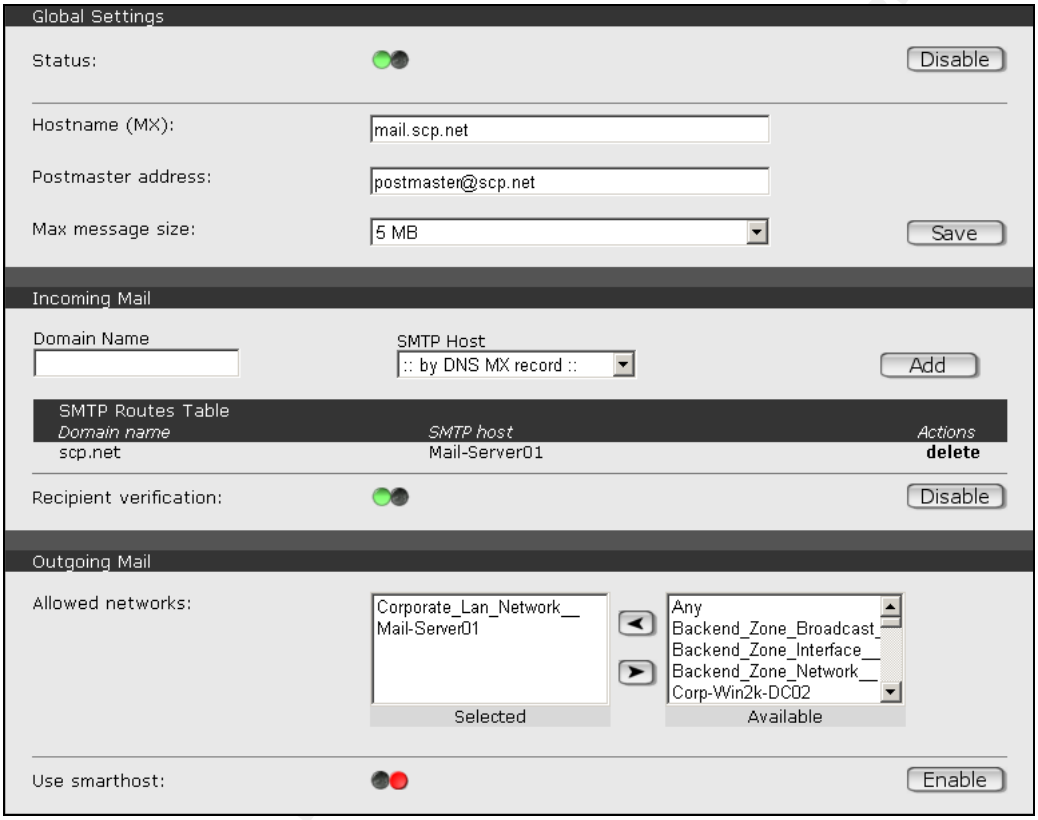


Figure 3-3. SMTP Compliance Evidence 2.

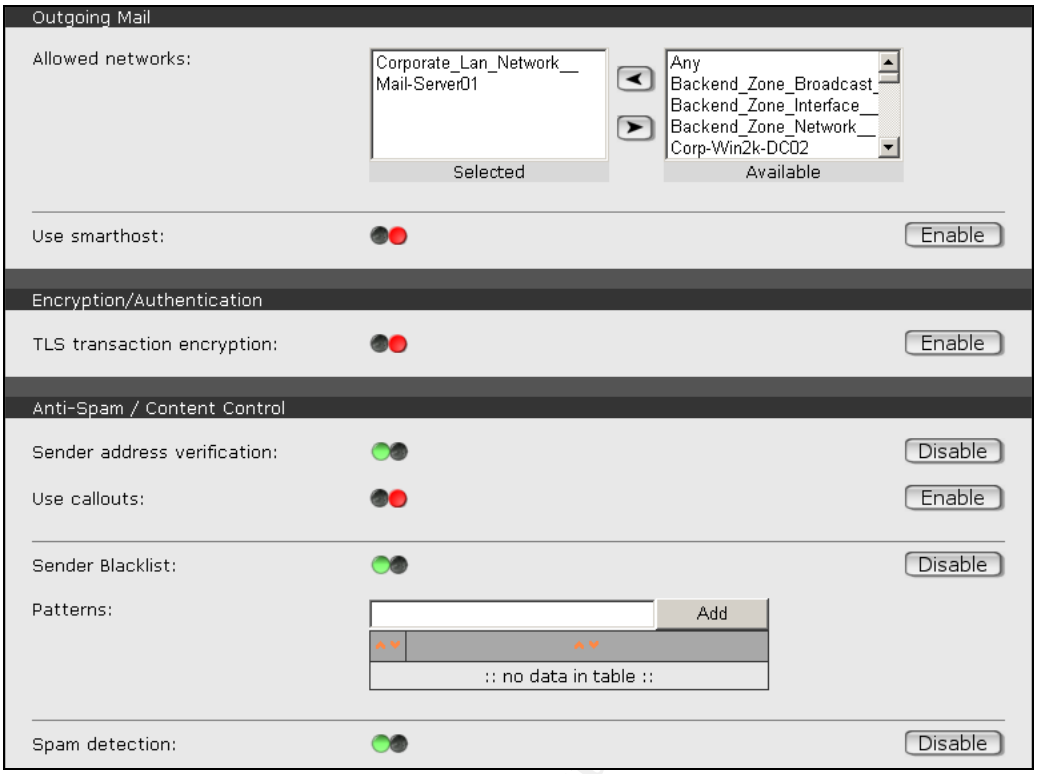


Figure 3-4. SMTP Compliance Evidence 3.

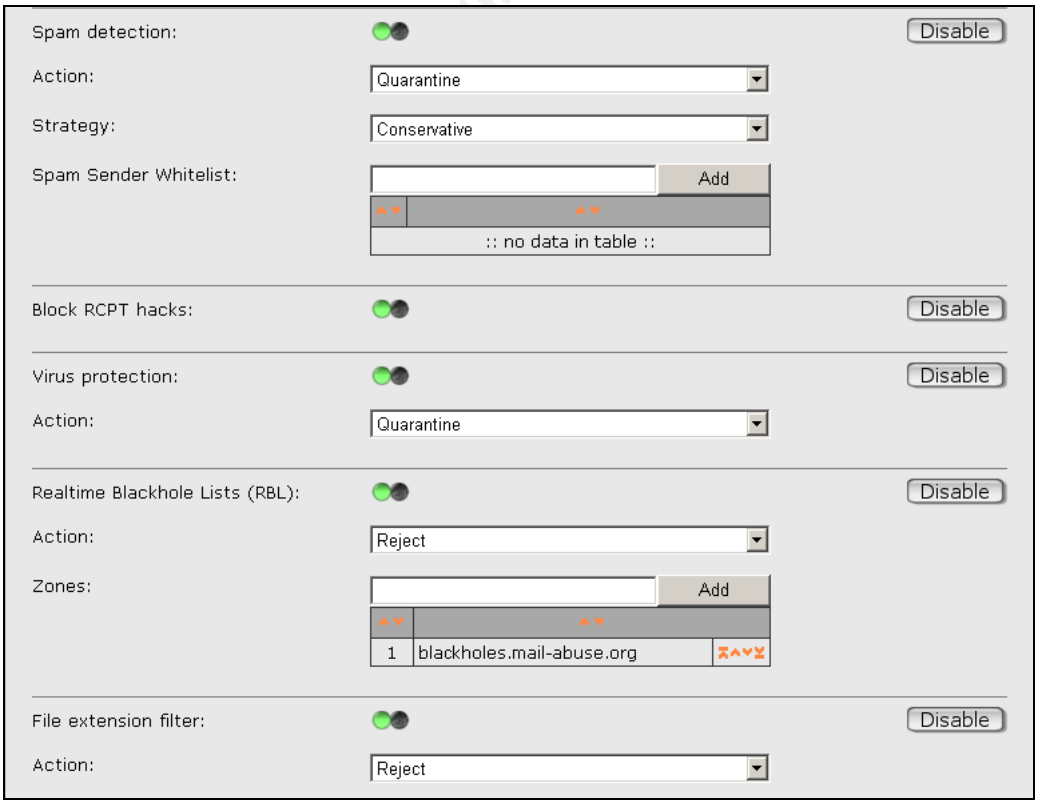
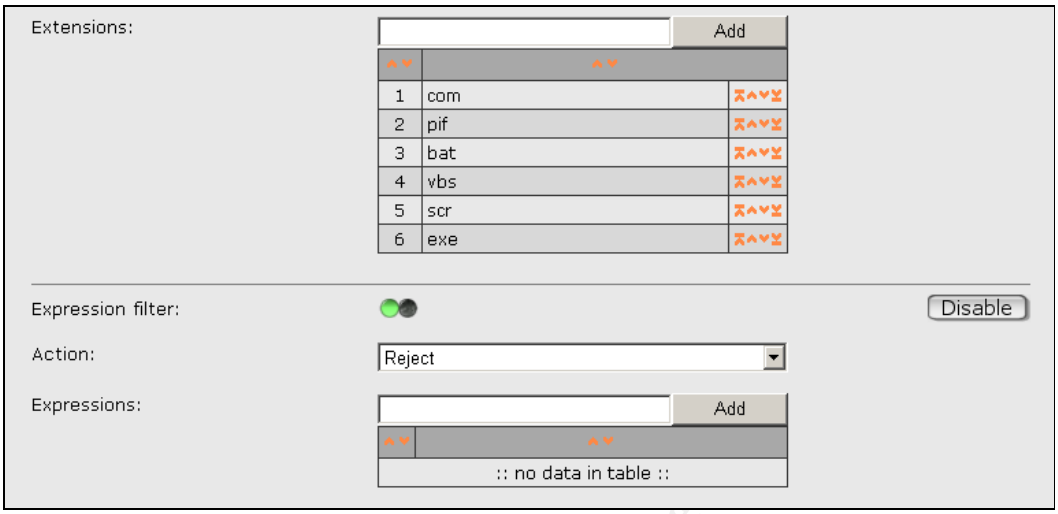


Figure 3-5. SMTP Compliance Evidence 4.



3.2.3.4 V.D Conclusion

The configuration of the SMTP Proxy complies with the checklist.

3.2.4 Checklist Item VI.a: SPIF Ruleset.

The Stateful Inspection Packet Filter is the most critical control that SCP wishes to implement within their I.S infrastructure. We have confirmed its Materiality by performing the Risk Assessment detailed in Section 1.6.2. This control provides cumulative benefits to the company by protecting its multiple assets from attack and misuse. These attacks may come from outside and inside the company so it is imperative that the Packet Filtering rules applied to the companies network access and egress are effective, robust and accurate.

By assessing the configuration in the first instance we can ensure that it will perform as expected. If this test is successful it can be followed by stimulus-response testing to ensure it functions correctly.

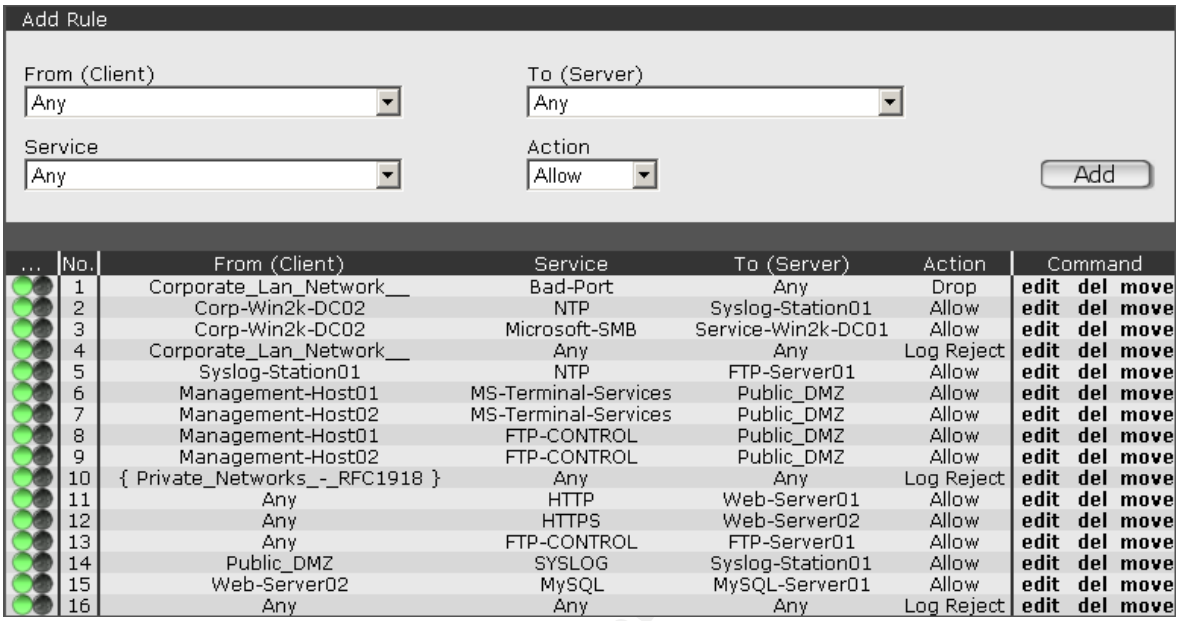
3.2.4.1 Test.

With one of the SCP administrators performing the work, we had them log onto the Web Admin interface from one of the two authorised management stations, and open the ***Packet Filter>Rules*** tab from the menu. Then, they checked that each line in the packet filters rule set conformed with the expected configuration as detailed in item *VI* of the checklist. The SCP Firewall Policy in Appendix 7.1 defined the expected configuration.

3.2.4.2 Compliance Evidence:

The screenshot below shows compliance with the expected configuration in Checklist Item *VI*.a.

Figure 3-6. SIPF Ruleset Compliance



...	No.	From (Client)	Service	To (Server)	Action	Command
	1	Corporate_Lan_Network__	Bad-Port	Any	Drop	edit del move
	2	Corp-Win2k-DC02	NTP	Syslog-Station01	Allow	edit del move
	3	Corp-Win2k-DC02	Microsoft-SMB	Service-Win2k-DC01	Allow	edit del move
	4	Corporate_Lan_Network__	Any	Any	Log Reject	edit del move
	5	Syslog-Station01	NTP	FTP-Server01	Allow	edit del move
	6	Management-Host01	MS-Terminal-Services	Public_DMZ	Allow	edit del move
	7	Management-Host02	MS-Terminal-Services	Public_DMZ	Allow	edit del move
	8	Management-Host01	FTP-CONTROL	Public_DMZ	Allow	edit del move
	9	Management-Host02	FTP-CONTROL	Public_DMZ	Allow	edit del move
	10	{ Private_Networks_-_RFC1918 }	Any	Any	Log Reject	edit del move
	11	Any	HTTP	Web-Server01	Allow	edit del move
	12	Any	HTTPS	Web-Server02	Allow	edit del move
	13	Any	FTP-CONTROL	FTP-Server01	Allow	edit del move
	14	Public_DMZ	SYSLOG	Syslog-Station01	Allow	edit del move
	15	Web-Server02	MySQL	MySQL-Server01	Allow	edit del move
	16	Any	Any	Any	Log Reject	edit del move

3.2.4.3 VI.a Conslusion

The configuration of the SIPF ruleset complies with the checklist.

3.2.5 Checklist Item VIII.a: PSD and Event Notification:

3.2.5.1 Purpose:

Receiving timely information from the firewall in response to significant events such as System or Daemon Failures, Unauthorised Login Attempts, Port Scans, Virus Pattern File and System Updates is an important feature of a Black-Box type system such as Astaro Security Linux. It allows the busy system administrator to focus on more immediate concerns while having confidence that the Firewall will alert her when an event requires attention.

Testing that these detective email alerts are sent when expected will ensure that the system administrators are notified in a timely manner.

3.2.5.2 VIII.a Test:

All of the tests required were either performed during other audit checklist tests or occurred as part of the systems normal operation.

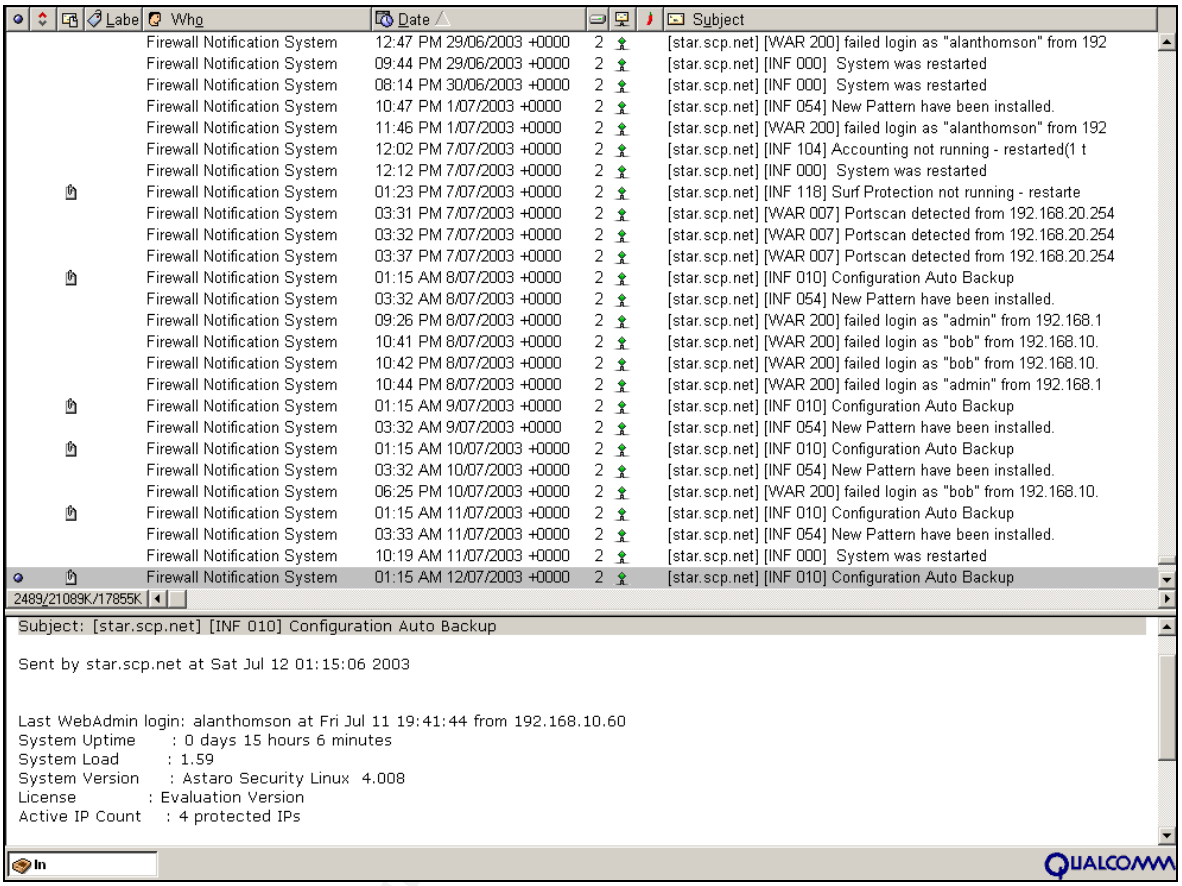
For example, the *PortScan Detected* event occurred as part of the SIPF tests, the *System Restart* event occurred as expected after a restart, and *New Pattern have been installed* events happened automatically as defined by the firewall's Up2date configuration. Logon failures generated *Failed Logon* alerts and *Configuration Auto Backups* were received daily as expected, conforming with the configuration defined in checklist controls III.j-l

3.2.5.3 Compliance Evidence:

The screenshot below shows compliance with the expected configuration in Checklist Item *VIII*.a. Note the classes and details in the Subject line of each Alert Email.

Figure 3-7. Evidence of Email events for PSD and other Alerts in Eudora client of Network Admin.

Note the failed login warnings for *bob* and *admin* created during the execution of checklist item X.C.



3.2.5.4 VIII.a Conslusion

The Firewall sends email Alert Events in response to a number of stimuli as expected. The alerting service complies with checklist item VIII.a and further supports multiple checklist items compliance.

3.2.6 Checklist Item VIII.l: SIPF Performance, Corporate LAN to Corporate LAN interface

3.2.6.1 Purpose.

Firewalls provide protection to network assets. The threat to these assets is generally perceived to be greatest from the Internet, diminishing as trust increases throughout the I.S infrastructure. In the SCP design this would equate to the Backend Zone being the most trusted, then the Corporate LAN, then the DMZ and finally the Internet as the least trusted.

As we trust the Internet the least and consider it the source of the greatest threat, then it follows that testing the controls applied by the external interface of the Firewall is of more importance than testing the Backend LAN's interface. However in this instance we

have chosen to present this scan because of the firewall's failure to perform as expected.

3.2.6.2 VIII.l Test.

Using the batch file detailed in appendix 7.2, perform a suite of Nmap scans using the following command from any external Internet host:

 # scan 192.168.20.1 PSD_OFF

In our test environment this constituted scanning the firewall from a host on the 192.18.20.0/24 subnet. We choose to present the PSD_OFF scan as the PSD_ON method was abandoned early in the SIPF Performance assessment due to the effectiveness of the Port Scan Detector. This modification to the testing procedure conforms to ISACA audit principals that state that the testing regimen should be flexible and react to changes or outputs from the earlier checklist tests.

3.2.6.3 VIII.l Compliance Evidence:

As detailed in Appendix 7.3 there is a considerable amount of evidence to assess. Only a few important evidence traces are presented here that support the expected compliance of the firewall.

As stated in checklist item VIII.l which is derived from the Firewall Policy, only Ports 25 (SMTP), 8080 (HTTP Proxy) and 53 (DNS) should be OPEN on the internal Corporate LAN facing interface.

Figure 3-8. Packet Filter Logging Evidence 1.

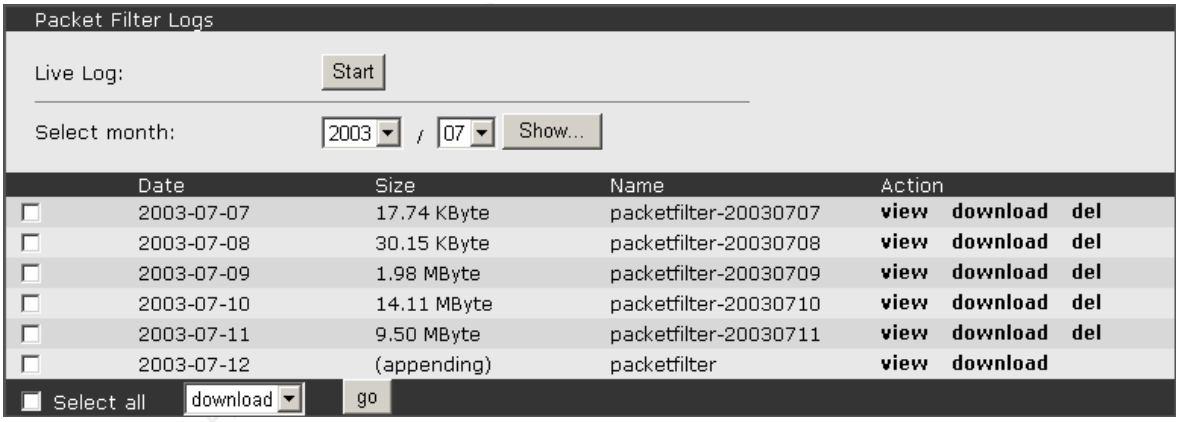
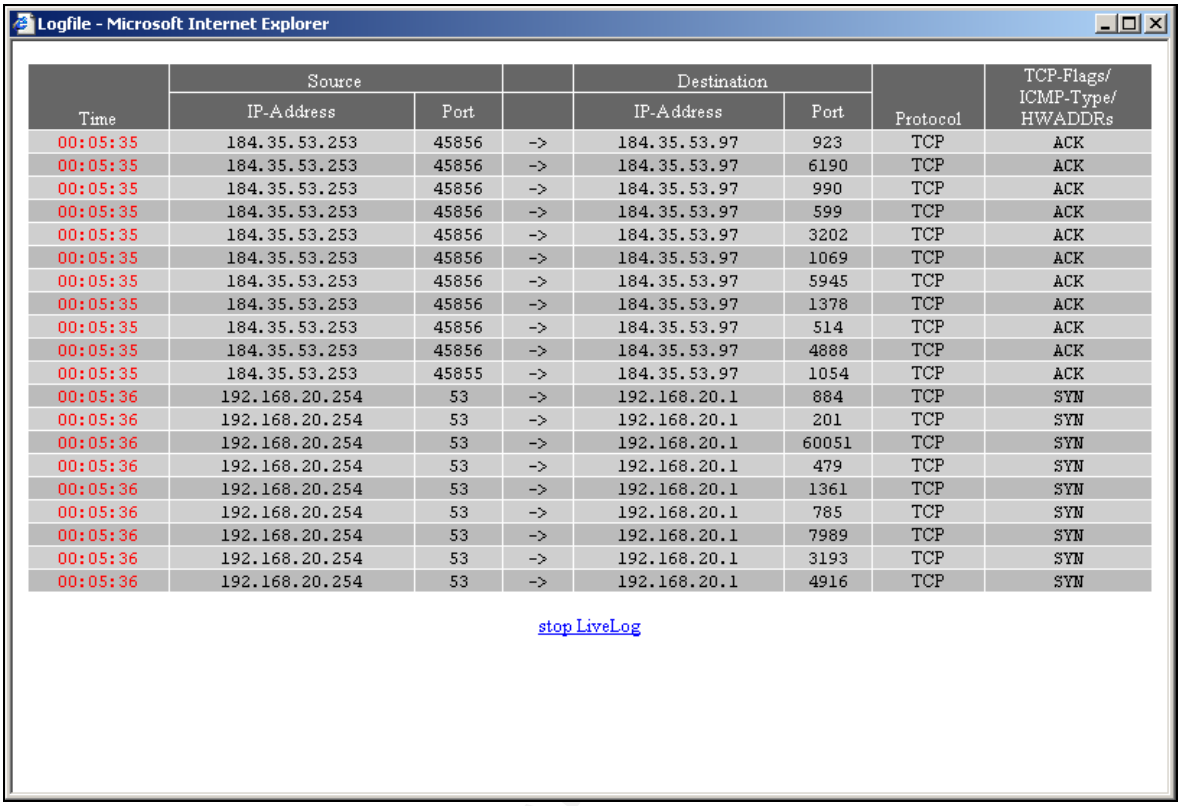


Figure 3-9. Packet Filter LiveLog interface showing two concurrent Nmap scans.



Time	Source IP-Address	Source Port		Destination IP-Address	Destination Port	Protocol	TCP-Flags/ ICMP-Type/ HWADDRs
00:05:35	184.35.53.253	45856	->	184.35.53.97	923	TCP	ACK
00:05:35	184.35.53.253	45856	->	184.35.53.97	6190	TCP	ACK
00:05:35	184.35.53.253	45856	->	184.35.53.97	990	TCP	ACK
00:05:35	184.35.53.253	45856	->	184.35.53.97	599	TCP	ACK
00:05:35	184.35.53.253	45856	->	184.35.53.97	3202	TCP	ACK
00:05:35	184.35.53.253	45856	->	184.35.53.97	1069	TCP	ACK
00:05:35	184.35.53.253	45856	->	184.35.53.97	5945	TCP	ACK
00:05:35	184.35.53.253	45856	->	184.35.53.97	1378	TCP	ACK
00:05:35	184.35.53.253	45856	->	184.35.53.97	514	TCP	ACK
00:05:35	184.35.53.253	45856	->	184.35.53.97	4888	TCP	ACK
00:05:35	184.35.53.253	45855	->	184.35.53.97	1054	TCP	ACK
00:05:36	192.168.20.254	53	->	192.168.20.1	884	TCP	SYN
00:05:36	192.168.20.254	53	->	192.168.20.1	201	TCP	SYN
00:05:36	192.168.20.254	53	->	192.168.20.1	60051	TCP	SYN
00:05:36	192.168.20.254	53	->	192.168.20.1	479	TCP	SYN
00:05:36	192.168.20.254	53	->	192.168.20.1	1361	TCP	SYN
00:05:36	192.168.20.254	53	->	192.168.20.1	785	TCP	SYN
00:05:36	192.168.20.254	53	->	192.168.20.1	7989	TCP	SYN
00:05:36	192.168.20.254	53	->	192.168.20.1	3193	TCP	SYN
00:05:36	192.168.20.254	53	->	192.168.20.1	4916	TCP	SYN

3.2.6.3.1 VIII.I SYN Scan 1, all 65535 Ports.

Counter to the expected results as outlined in the checklist we have an extra port OPEN, port 8110, as we can see in the Nmap log below.

Figure 3-10. Nmap Syn Scan Log.

```
# nmap (V. 3.00) scan initiated Thu Jul 10 18:59:18 2003 as: nmap -sS -vn -oA
SynScan-1-192.168.20.1_PSD_OFF -p 1-65535 192.168.20.1

Interesting ports on star.scp.net (192.168.20.1):

(The 65531 ports scanned but not shown below are in state: filtered)

Port       State       Service
25/tcp     open        smtp
53/tcp     open        domain
8080/tcp   open        http-proxy
8110/tcp   open        unknown

# Nmap run completed at Thu Jul 10 20:04:37 2003 -- 1 IP address (1 host up) scanned
in 3919 seconds
```

3.2.6.3.2 VIII.I ACK Scan 1, all 65535 Ports.

As expected from an ACK scan, the same four ports as above are identified as UNfiltered, including the erroneous port 8110. Sending a SYN/ACK to the UNfiltered port solicited a Reset (RST), whereas the SIPF filtered ports would have sent an ICMP

Port Unreachable message. The is in line with the Firewall Policies ANY ANY LOG-REJECT rule as the SIPF was not maintaining state for any outbound connections from the destination ports.

If it had, the SYN/ACK packet would have reached a closed port and the system may have responded with a RESET or in some other manner depending on how the developer of the IP stack conforms with RFC's.

Figure 3-11. Nmap Ack Scan Log.

```
# nmap (V. 3.00) scan initiated Thu Jul 10 21:01:25 2003 as: nmap -sA -vn -oA
AckScan-1-192.168.20.1_PSD_OFF -p 1-65535 192.168.20.1

Interesting ports on star.scp.net (192.168.20.1):

(The 65531 ports scanned but not shown below are in state: filtered)

Port       State       Service
25/tcp     UNfiltered  smtp
53/tcp     UNfiltered  domain
8080/tcp   UNfiltered  http-proxy
8110/tcp   UNfiltered  unknown

# Nmap run completed at Thu Jul 10 22:29:06 2003 -- 1 IP address (1 host up) scanned
in 5261 seconds
```

Note: All other ACK Scans using source ports reported the same 4 ports as UNfiltered.

3.2.6.3.3 VIII.I FIN Scan 1, all 65535 Ports

A "stateful" test that might show Ports 25, 53 and 8080 as OPEN if a simple "Stateless" Packet Filter is used. OPEN in this instance would indicate that the Stateless Packet Filter passed the packet and that the target system quietly ignored the FIN packet when received on it's OPEN port. On closed ports the normal response is a RESET while Stateful Inspection Filtered Ports should send an ICMP Port Unreachable message.

In this case the Firewall meets expectations for a SIPF and Filters the FIN received on the 3 expected ports, providing support that it's stateful inspection engine was not maintaining an active session's state in memory, and was therefore not expecting a FIN from the scanning host. Consequently it responded with an ICMP Port Unreachable (filtered) message as expected for all 65535 ports.

Figure 3-12. Nmap Fin Scan Log.

```
# nmap (V. 3.00) scan initiated Thu Jul 10 23:26:36 2003 as: nmap -sF -vn -oA
FinScan-1-192.168.20.1_PSD_OFF -p 1-65535 192.168.20.1

All 65535 scanned ports on star.scp.net (192.168.20.1) are: filtered


# Nmap run completed at Fri Jul 11 01:22:21 2003 -- 1 IP address (1 host up)
scanned in 6944 seconds
```

Note: All other FIN Scans using source ports reported all ports filtered also.

3.2.6.3.4 VIII.I XMAS Scan 1, all 65535 Ports

This Out Of Spec test uses packets with unexpected Flag combinations to test the firewalls SIPF capabilities again. A Stateful Firewall using a REJECT rule should send ICMP Port Unreachable messages for all received packets.

This is exactly what we expected from this test and the output below confirms compliance with our expectations.

Figure 3-13. Nmap Xmas Tree Scan Log.

```
# nmap (V. 3.00) scan initiated Fri Jul 11 02:09:10 2003 as: nmap -sX -vn -oA XmasScan-1-192.168.20.1_PSD_OFF -p 1-65535 192.168.20.1

All 65535 scanned ports on star.scp.net (192.168.20.1) are: filtered

# Nmap run completed at Fri Jul 11 04:04:52 2003 -- 1 IP address (1 host up) scanned in 6942 seconds
```

3.2.6.3.5 VIII.I FRAG Scans

Each of the FRAG scans performed in accordance with the primary scan type used. I.e. the Fragmented Syn scan showed 4 Ports OPEN including the erroneous port 8110, while the Fragmented FIN scan showed all ports filtered.

3.2.6.3.6 VIII.I UDP Scans

UDP scans are difficult to analyse. They can be painfully slow and return confusing results depending on the target system's implementation of the respective RFC's.

The results of our initial scans were inconclusive. The first scan (se Fig 3.12), of all 65535 ports reported 64,000 ports to be OPEN while all the subsequent source port scans showed all ports to be Filtered (see Fig 3.13).

Figure 3-14. Nmap UDP Scan Log 1

```
# nmap (V. 3.00) scan initiated Sat Jul 12 14:05:10 2003 as: nmap -sU -vn -oA UDPScan-1-192.168.20.1_PSD_OFF -p 1-65535 192.168.20.1

Interesting ports on star.scp.net (192.168.20.1):

(The 1001 ports scanned but not shown below are in state: closed)

Port       State      Service

1/udp      open       tcpmux

……and line by line until…

65535/udp  open       unknown

# Nmap run completed at Sat Jul 12 19:51:44 2003 -- 1 IP address (1 host up) scanned in 20794 seconds
```

Figure 3-15. Nmap UDP Scan Log 2.

```
# nmap (V. 3.00) scan initiated Sat Jul 12 19:51:51 2003 as: nmap -sU -vn -oA
UDPScan-2-192.168.20.1_PSD_OFF -g 21 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 192.168.20.1

All 4310 scanned ports on star.scp.net (192.168.20.1) are: filtered

# Nmap run completed at Sat Jul 12 19:59:12 2003 -- 1 IP address (1 host up)
scanned in 441 seconds
```

Upon investigating the syslog logs on the Syslog Workstation we can see that the firewall was dropping the UDP packets sent by Nmap. As the man page for Nmap suggests, if the firewall drops packets, Nmap, knowing that UDP is connectionless and does not send acknowledgement packets, thinks the port is OPEN.

The UDP scan log is erroneous, and all the UDP ports can be considered closed.

Table 3-3. Syslog log for UDP scan.

```
2003-07-12 00:59:57 UTC Kernel.Info 192.168.10.100 kernel: UDP Drop: IN=eth2
OUT= MAC=00:40:05:e1:39:f4:00:00:39:8f:01:b4:08:00 SRC=192.168.20.254
DST=192.168.20.1 LEN=48 TOS=0x00 PREC=0x00 TTL=128 ID=2966 PROTO=UDP
SPT=1577 DPT=45270 LEN=28

2003-07-12 00:59:57 UTC Kernel.Info 192.168.10.100 kernel: UDP Drop: IN=eth2
OUT= MAC=00:40:05:e1:39:f4:00:00:39:8f:01:b4:08:00 SRC=192.168.20.254
DST=192.168.20.1 LEN=48 TOS=0x00 PREC=0x00 TTL=128 ID=2967 PROTO=UDP
SPT=1577 DPT=45271 LEN=28

2003-07-12 00:59:58 UTC Kernel.Info 192.168.10.100 kernel: UDP Drop: IN=eth2
OUT= MAC=00:40:05:e1:39:f4:00:00:39:8f:01:b4:08:00 SRC=192.168.20.254
DST=192.168.20.1 LEN=48 TOS=0x00 PREC=0x00 TTL=128 ID=2968 PROTO=UDP
SPT=1577 DPT=45272 LEN=28

2003-07-12 00:59:58 UTC Kernel.Info 192.168.10.100 kernel: UDP Drop: IN=eth2
OUT= MAC=00:40:05:e1:39:f4:00:00:39:8f:01:b4:08:00 SRC=192.168.20.254
DST=192.168.20.1 LEN=48 TOS=0x00 PREC=0x00 TTL=128 ID=2969 PROTO=UDP
SPT=1577 DPT=45273 LEN=28
```

3.2.6.4 VIII.I Conclusion.

In light of the erroneous OPEN port 8110 but in consideration of subsequent discoveries we report that this item scores a 2, i.e. the checklist item *"Partially fails, performs unexpectedly, poses low risk vulnerability".*

This score reflects information that came to hand after investigating this issue. The Astaro Known Issues document for Astaro Security Linux 4 reports the following issue;

Figure 3-16. ASL Known Issues item for port 8110.

ID415 f 4.000 Predefined Any-Any Rule in POP3 Proxy opens port 8110 to outside

---

Description: When enabling Transparent POP3 Proxy, the predefined Any-Any Rule opens a port reachable from anywhere.

Workaround: Fit the rule to your needs

Fix: 4.008 (ISO only)

In addition to this discovery it is also patently clear that this system does not have 64,000 UDP ports OPEN, as supported by the syslog logs above.

3.2.7 Checklist Item IX.b: HTTP/s and FTP Proxy Performance.

3.2.7.1 Purpose.

One of the critical controls SCP wish to implement with the firewall. We have confirmed its Materiality by performing the Risk Assessment detailed in Section 1.6.2.

Having confirmed it's configuration compliance we now wish to test the controls effectiveness in implementing company policy.

3.2.7.2 IX.b Test

As outlined in the checklist a Web Browser was configured on each of the three SCP subnets to use the Firewall's subnet interface as an HTTP Proxy listening on port 8080.

Then each of the URL's from the checklist (a-j) was pasted into the browser by one of the system administrators.

3.2.7.3 IX.b Compliance Evidence:

Both the Backend LAN and the Public DMZ hosts rejected attempts to connect to the proxy in line with the SCP Firewall Policy, the expected configuration detailed in Checklist item V.d and the Compliance Evidence in section 3.2.3.3 above.

From the Corporate LAN we provide two evidentiary screenshots below as examples.

Figure 3-17. Content Filtering test IX.b.d

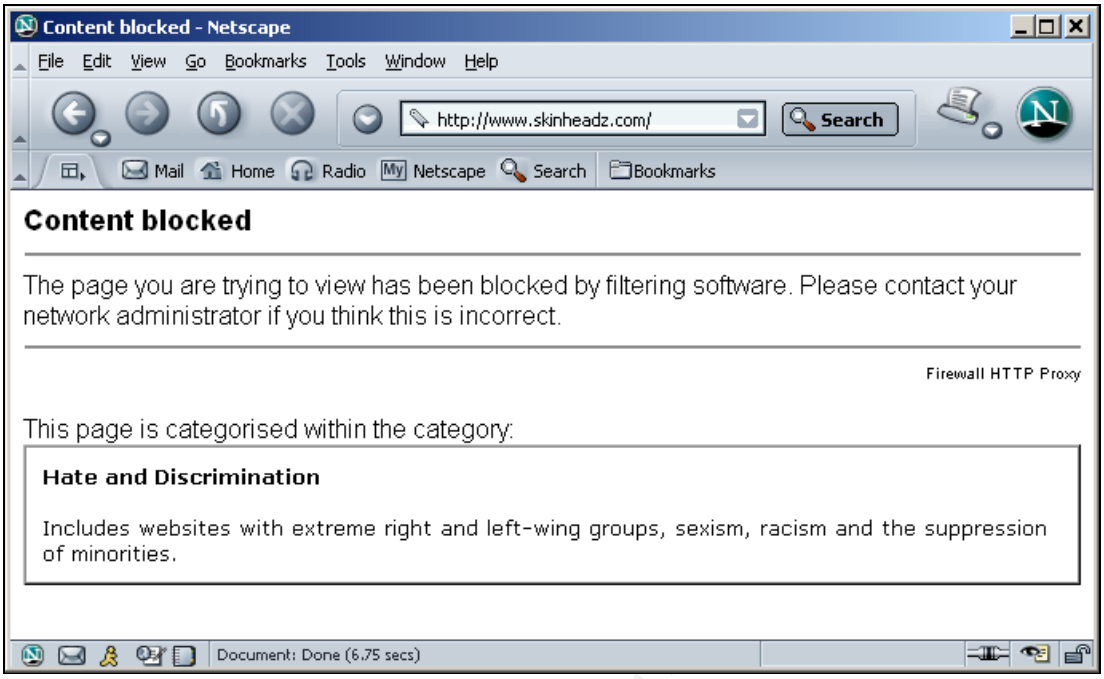
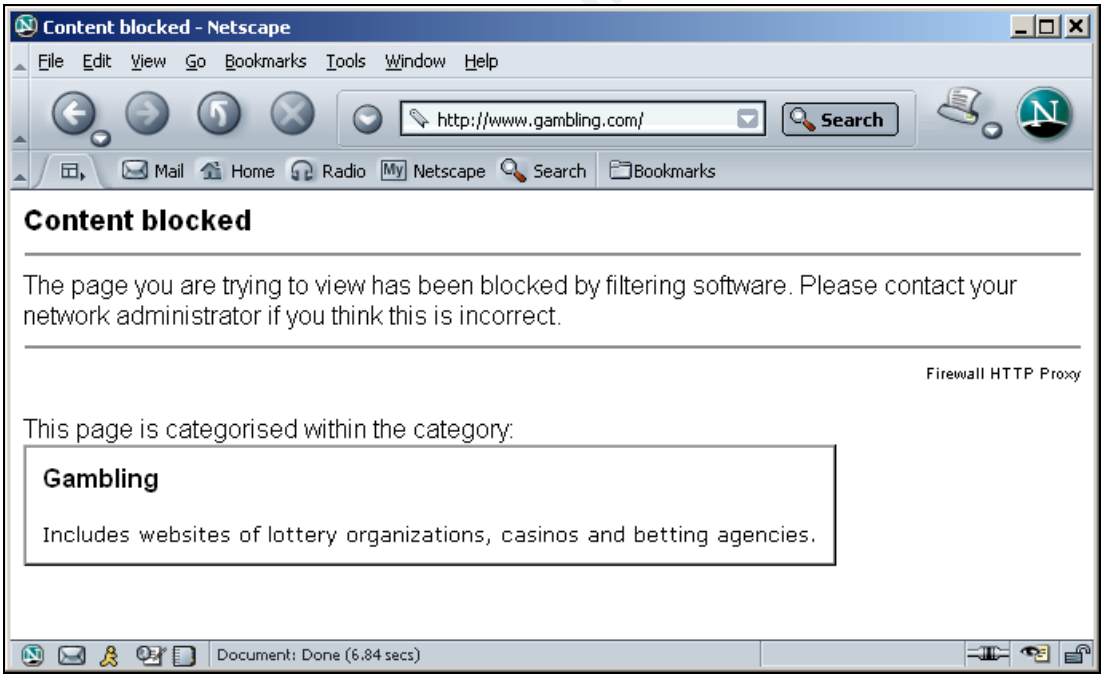


Figure 3-18. Content Filtering test IX.b.g



All other test sites performed as expected, complying with the expected response as detailed in Checklist Item IX.b above.

3.2.7.4 IX.b Conclusion:

The HTTP/S, FTP proxy complies with the checklist and performs as expected.

3.2.8 Checklist Item IX.d: SMTP Proxy Performance

One of the critical controls SCP wish to implement with the firewall. We have confirmed its Materiality by performing the Risk Assessment detailed in Section 1.6.2.

Having confirmed it's configuration compliance we now wish to test the controls effectiveness in implementing company policy.

3.2.8.1 IX.d Test.

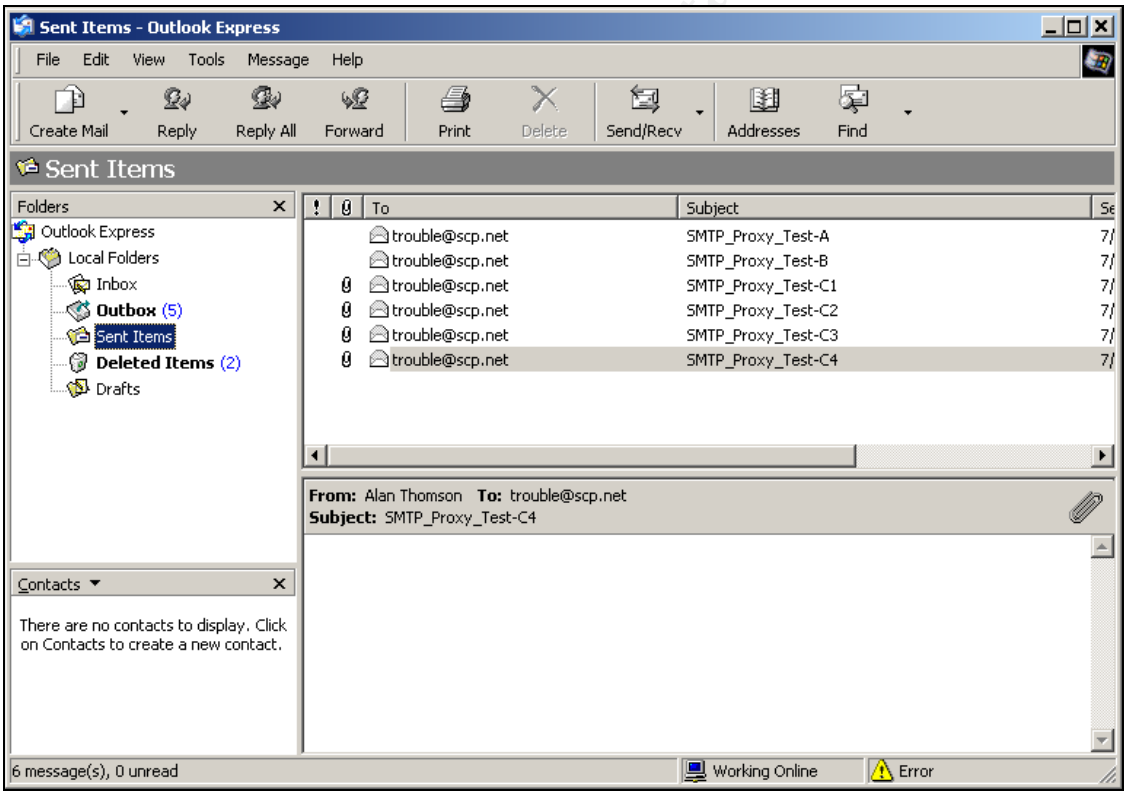
As outlined in the checklist we use an SMTP client to send a suite of messages through the SMTP proxy to trouble@scp.net, an alias for both of SCP's system and network administrators. In this case we had one of the administrators use a host on the development network's Corporate LAN to send each of the ten messages.

3.2.8.2 IX.d Compliance Evidence:

3.2.8.2.1 IX.d Anti-Virus Tests

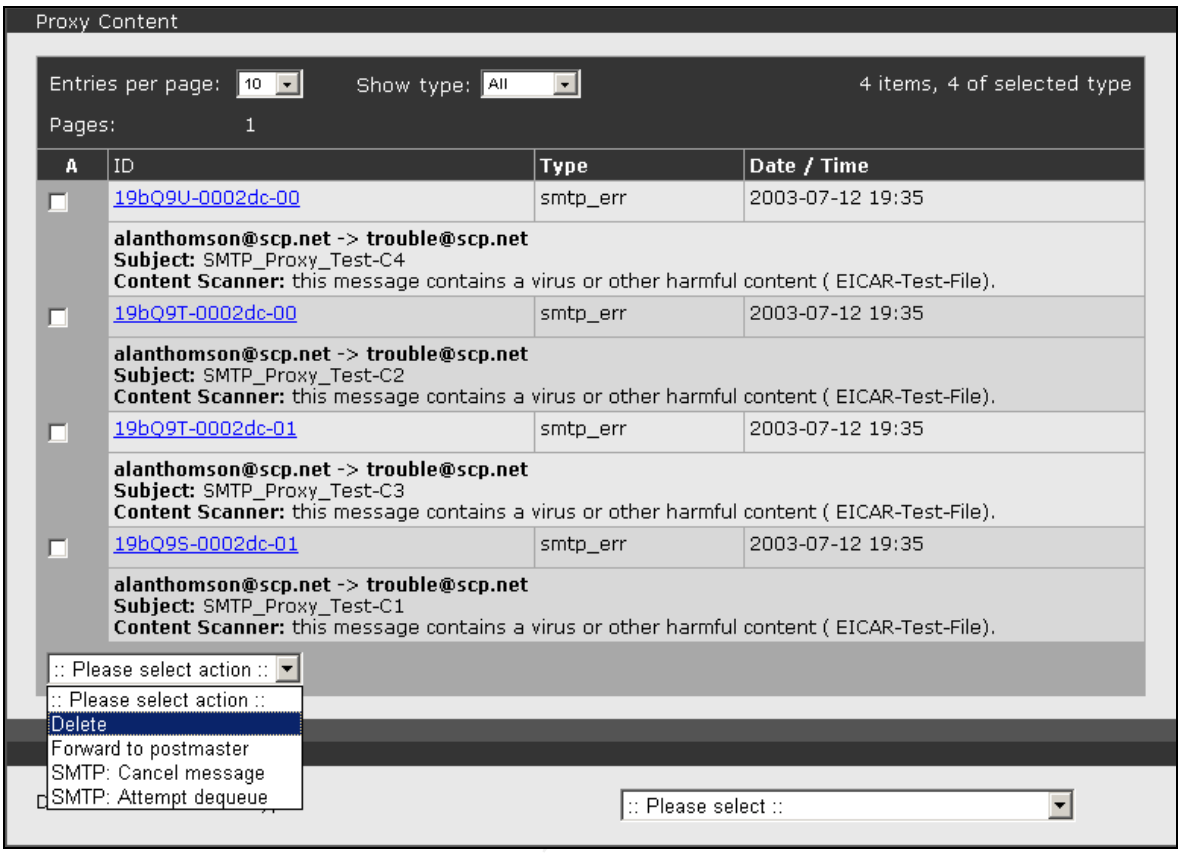
In this first example we provide evidence of the SMTP gateway's Kapersky Labs Antivirus scanner detecting the four EICAR test files we sent as attachments.

Figure 3-19. Outlook Express Sent Items window showing the 4 messages sent.



In the next image we see each of the four EICAR messages being quarantined by the Proxy Content Manager.

Figure 3-20. Proxy Content manager with 4 quarantined Virus test messages.

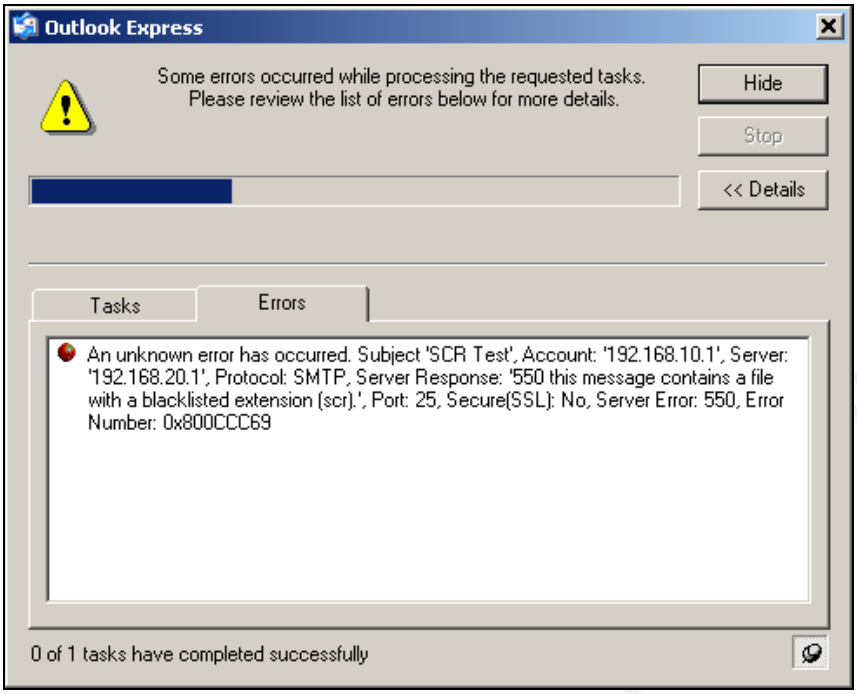


3.2.8.2.2 IX.d Extension Test Compliance

In this example we see the SMTP gateway taking a more proactive stance and refusing to accept the message transfer, returning an Error 550 message to the Outlook Express client.

The firewall exceeds expectations as the 550 message is informative and useful to the end user in that it explicitly describes the reason for refusing the message transfer. This should lower the number of support calls to the companies Help Desk.

Figure 3-21. SMTP Gateway explicitly denying a forbidden extension attachment.



3.2.8.3 IX.d Conclusion:

The SMTP Gateway complies with the checklist and performs above the required level.

3.2.9 Checklist Item X.a: Bulk Vulnerability Scan.

3.2.9.1 Purpose:

Using tools such as Nessus[1] or ISS[2] Internet Scanner allows us to efficiently evaluate the system for a large number of common vulnerabilities.

3.2.9.2 X.a Test.

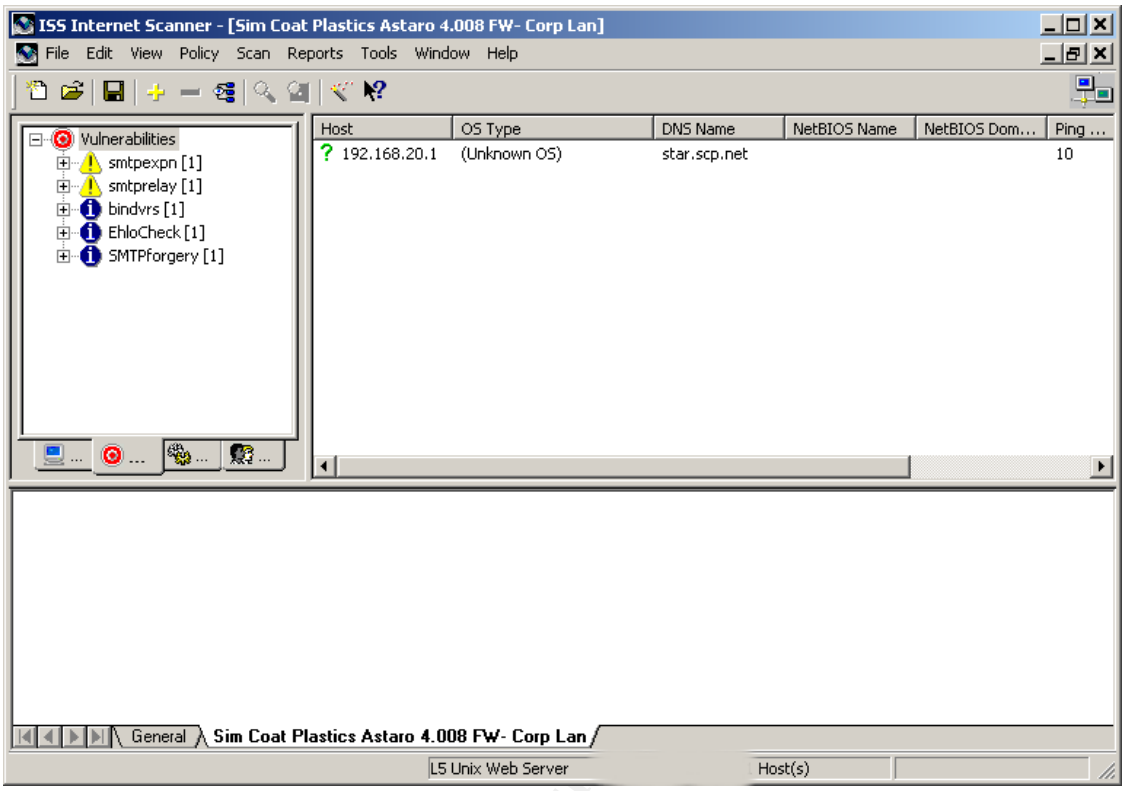
As outlined in the checklist we took a laptop into the test environment with ISS Internet Scanner 6.21 installed and scanned each of the Firewalls internal interfaces using the Unix Web Server Level 5 signature policy.

The example below shows the scanner configured to scan the Corporate LAN interface 192.168.20.1. We choose this example as the Firewall has the most listening services configured on this interface, and in turn the scanner reported the most vulnerabilities here.

[1] http://www.nessus.org

[2] http://www.iss.net

Figure 3-22. ISS Internet Scanner after scannin g the firewall's Corporate LAN interface.



3.2.9.3 X.a Compliance Evidence:

See Appendix 7.6 for report details.

There are five vulnerabilities reported, three Low risk vulnerabilities and two Medium Risk. We will examine each of these in turn.

3.2.9.3.1 smtpexpn: SMTP EXPN command (CAN-1999-0531)

Applies to Internet, Backend and Corporate LAN firewall interfaces.

This is a false positive. According to the RFC (821) it is considered acceptable for a server to respond with a 250 (success) or 550 (failure) when the server supports the EXPN command (from the ISS Vulnerability Catalogue).

Upon checking the scanner log file we see that the server responded with a '*550 Administrative prohibition'* message.

Figure 3-23. ISS Scanner SMTP Expn Test log evidence.

```
# Time Stamp(0x5dc):192.168.20.1 smtpexpn: (1057975454) Sat Jul 12 12:04:14
Exploit smtpexpn on host 192.168.20.1 returned 0x0
Target state is COMPLETE
Found active TCP service 192.168.20.1 on port 25
# Started the smtpexpn check...
# BANNER '220 mail.scp.net ESMTP ready.'
# SERVICE 'ESMTP' VERSION ''
# 550 Administrative prohibition
Vulnerable SMTP server: EXPN is enabled
# Finished the smtpexpn check...
```

3.2.9.3.2 smtprelay: Third-party mail relaying can be used to obfuscate the origin of emails

Applies to Backend and Corporate LAN firewall interfaces.

This is an example of an insignificant positive. It's not false as some would state, the SMTP gateway does relay mail, that's exactly what SCP have implemented the SMTP proxy to do.

3.2.9.3.3 bindvrs: BIND servers can be remotely queried for their version numbers

Applies to Public DMZ, Backend and Corporate LAN firewall interfaces.

At first this appeared to be a potentially serious vulnerability. A check shows that Astaro Security Linux 4.008 is running Bind Ver 8.3.3-REL.

```
D:\dig>dig @192.168.10.100 version.bind chaos txt

; <<>> DiG 9.2.2 <<>> @192.168.10.100 version.bind chaos txt
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41
;; flags: qr aa rd  ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
VERSION.BIND.           0       CH      TXT     "8.3.3-REL"

;; Query time: 0 msec
;; SERVER: 192.168.10.100#53(192. 168.10.100)
;; WHEN: Sun Jul 13 16:33:17 2003
;; MSG SIZE  rcvd: 64
```

3.2.9.3.3.1 Known Vulnerabilities in BIND ver 8.3.3

A check of ICAT[3] the Common Vulnerabilities and Exposures metabase at NIST shows that there are 3 known vulnerabilities for BIND 8.3.3.

[3] http://icat.nist.gov

CAN-2002-1221
Summary:
BIND 8.x through 8.3.3 allows remote attackers to cause a denial of service (crash) via SIG RR elements with invalid expiry times, which are removed from the in ternal BIND database and later cause a null dereference.
Published Before:
11/29/2002
Severity:
Medium

CAN-2002-1220
Summary:
BIND 8.3.x through 8.3.3 allows remote attackers to cause a denial of service (termination due to assertion failure) via a request for a subdomain that does not exist, with an OPT resource record with a lar ge UDP payload size.
Published Before:
11/29/2002
Severity:
Medium

CAN-2002-1219
Summary:
Buffer overflow in BIND 4 versions 4.9.10 and earlier, and 8 versions 8.3.3 and earlier, allows remote attackers to execute arbitrary code via a certain DNS serv er response containing SIG resource records (RR).
Published Before:
11/29/2002
Severity:
High

Additionally, a check of the Known Issues document for Astaro 4.008 gives no indication that these vulnerabilities have been mitigated, however a review of Astaro Up2Date announcements from the docs.Astaro.org website shows that this issue was resolved on the 13th Nov 2002.

- Up2Date 3.12 Announcment.

NB: It's comforting to note that the patch for Astaro was released less than 24 hours after the original CERT announcement.

- CERT® Advisory CA-2002-31 Multiple Vulnerabilities in BIND

It's not reported but assumed that the vendor (Astaro) applied the patch supplied by ISC[4], BIND's developer.

- BIND 8.3.3 Patch

3.2.9.3.4 SMTPforgery: SMTP server allows fake hostnames in HELO and EhloCheck: SMTP daemon supports EHLO (CAN-1999-0531)

Applies to Internet, Backend and Corporate LAN firewall interfaces.

[4] http://www.isc.org

ISS Scanner reports these as Low Risk events. In the auditor's opinion this item does not represent any level of risk to SCP. The use of bogus host-names could be controlled through the use of Call-Outs, however some remote system administrators consider this rude behaviour and we do not recommend their use. Additionally, using callouts to enforce hostname identification can be the cause of mail delivery problems due to timeouts, connection errors, NAT, routing and name resolution problems.

This is an insignificant item.

3.2.9.3.5 X.a Conclusion.

Compliance achieved. We advise that there are no vulnerabilities that represent a level of risk to SCP that requires a mitigation effort.

3.2.10 Checklist Item X.b: HTTP Vulnerability Scan.

3.2.10.1 Purpose:

Test the administrative interface of the firewall for known vulnerabilities. Considering the measures taken to restrict access to the interface itself through packet filtering, there is a low probability of any vulnerability ever being exploited, as it would require access to either of the management workstations

3.2.10.2 X.b Test

As described above, download SSL Proxy / Sniffer from Compass Security[5] and install on one of the management workstations, and then define a connection profile for the Firewalls Web Admin interface. Then, redirect an HTTP scan using N-Stealth by N-Stalker[6] through the HTTPS tunnel created by SSL Proxy to the web server of the Firewall.

[5] http://www.csnc.ch

[6] http://www.nstalker.com

Figure 3-24. SSL Proxy. Note the connection description, logging and connection information.

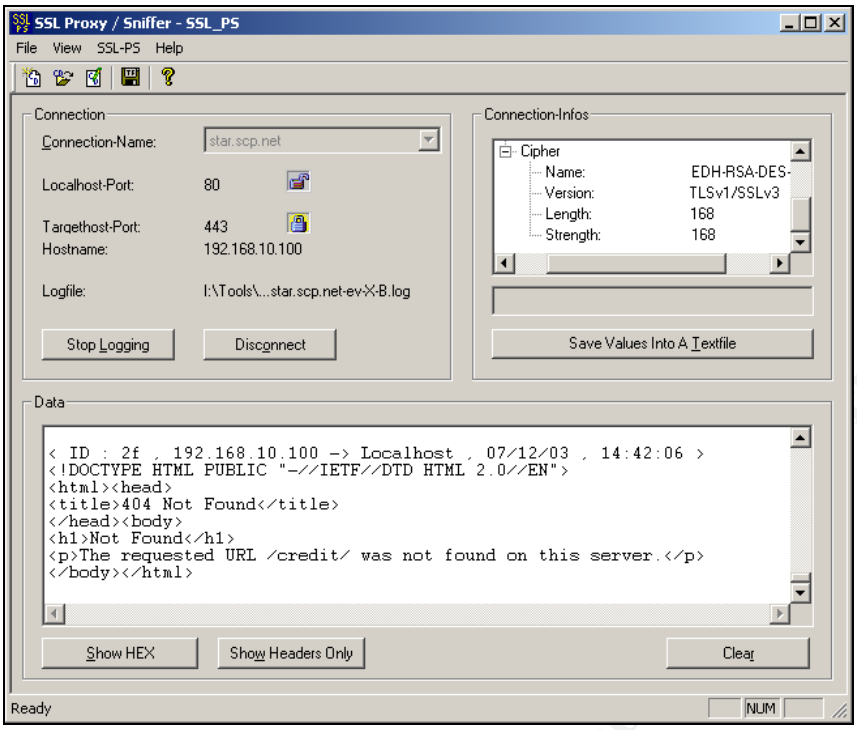
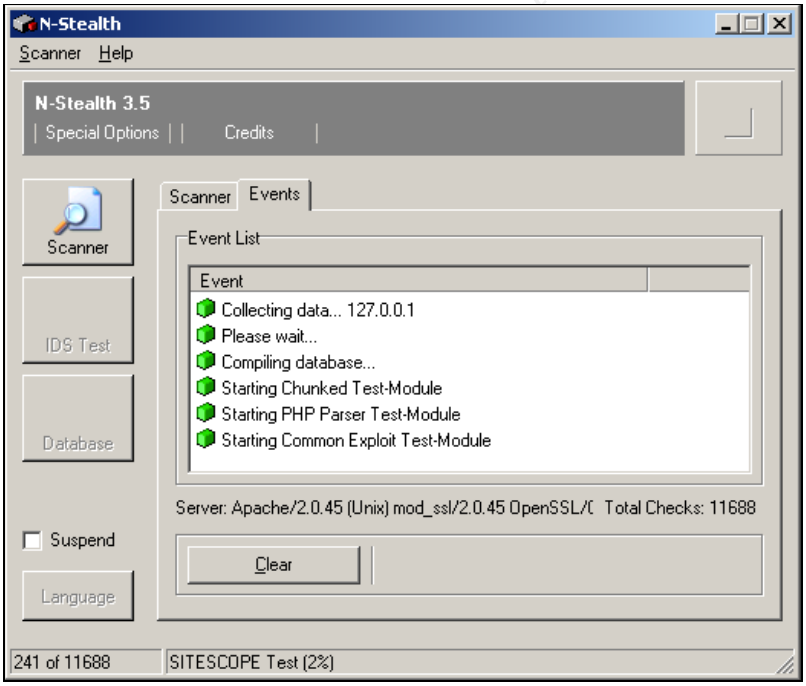


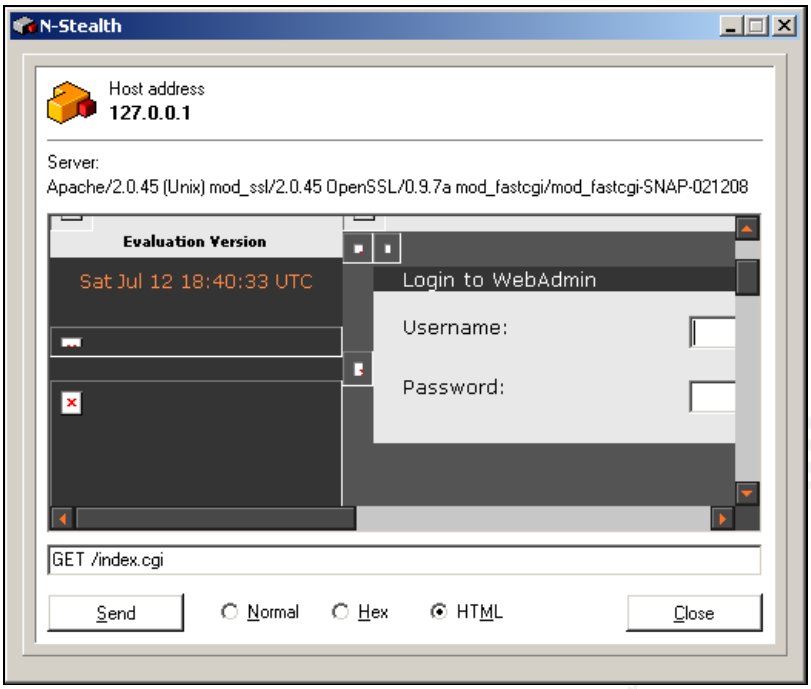
Figure 3-25. N-Stealth scanning localhost:80 which is redi rected to the https Web Admin server



3.2.10.3 X.b Compliance Evidence:

Appendix 7.4 shows that N-Stealth reported six vulnerabilities. The first four pertain to Netscape Enterprise Server only and may immediately be considered false positives, while the last two proved erroneous on testing which the image below shows.

Figure 3-26. Testing both index.cgi and update.pl returns the Web Admin log on page.



3.2.10.4 X.b Conclusion:

Compliance achieved, no substantiated vulnerabilities detected in the Web Admin interface.

3.2.11 Measure of Residual Risk

As the system has complied with every measure in the audit checklist bar one where it partially failed, we believe the Residual Risk to SCP and the Firewall itself to be VERY LOW (from Table 5, section 1). Not only can we estimate this qualitatively, but the Risk Assessment we performed in section 1.6 estimates a Quantitative figure for the ALE of the residual risk to the network as $17,225 per annum.

The single exception to checklist item VIII.l poses a VERY LOW risk in the auditor's opinion. There is no listening service on Port 8110 therefore connection attempts fail, so we see limited opportunity for this vulnerability to be exploited in any way.

3.2.12 Is the System Auditable?

This system has a number of excellent features that contribute to the ease with which its services can be audited. In addition to the auditable items above, such as email alerts and packet filter live-logs, there are local and remote syslog logs, local MRTG cpu, memory and traffic accounting logs for each subnet, specific logs for each of the proxy daemons including those not utilised by SCP such as IPSec and PPTP, as well as admin access logs, self-monitor daemon and kernel logs. This all makes auditing its functionality easy and is line with the detective audit trail features expected in a modern firewall.

If the system has audit weaknesses anywhere, it is that it is designed to be a Black-Box operating system. The manual discourages the use of SSH, and indeed the system is striped so bare as to make using the console almost pointless. There are few binaries

with common utilities like *adduser* removed, restricting the user quota to the three pre-configured Astaro users detailed in the user manual.

Each of the service daemons is chrooted adding to the robust design of the system but also making auditing the system problematic, especially as there is no technical user manual that describes the operating system and daemon configuration. In fact none of the proxy daemons are addressed by name at all in the Astaro Security Linux user manual, leaving the user ignorant to the software used to provide the application proxy services.

We fully understand and support the presumed reasoning behind this Black-box approach to building a firewall distribution, as it discourages and reduces the likelihood that the inexperienced user will attempt to manage and configure the system from the shell.

However, this lack of detailed information makes trouble shooting erroneous behaviour such as the additional port 8110 problematic, as it's unclear where to begin when looking for a resolution.

As an example even after finding the reference to the open port 8110 in the Known Issues document we still had to SSH into our test VM-Ware system to ascertain that the POP3 proxy being used is *POP3 Virus Scanner Proxy*[7] (great name). Even now we're still not exactly sure why port 8110 is open.

In summary we believe the lack of a detailed system level technical manual impairs this systems ability to be audited easily, however that is not to say that it cannot be audited, it's simply a matter of research and developing an understanding of the system through investigation and analysis.

At a functional level the audit trail is comprehensive, timely and simple to access via the Web Admin interface, syslog and email alerts.

Q. Were there any controls that could not be tested?

A. None that we encountered.

[7] http://sourceforge.net/projects/pop3vscan/

4 ASSIGNMENT 4. AUDIT REPORT

4.1 Executive Summary.

Information Security has a life cycle. The foundations of this lifecycle are the security policies upon which every other measure, procedure or process within your organization is based. The security policy sets the company security posture, and no defined posture results in unknown and uncontrolled security risks.

In establishing new and critical infrastructure such as a firewall, it's imperative that the systems deployment be based on a sound and explicit security policy. This Firewall Policy forms the baseline by which it's successful performance or failure can be measured throughout its lifetime.

During our engagement with SCP we have enjoyed considerable support from management and operational staff in establishing a sound Firewall Policy and baselining its implemented performance through audit. The collaborative approach to developing the baseline configuration of the Astaro Security Linux firewall has reaped significant benefits for SimCoat Plastics:

- ✓ Industry Best Practice Firewall Policy.
- ✓ Documented, stable Firewall Configuration.
- ✓ 99% implementation compliance with the Baseline Audit Checklist and Firewall Policy.
- ✓ Significant reduction in existing operational Risk.
- ✓ Significant dollar returns to the company through;
  - i. Increased productivity.
  - ii. Increased revenue (Internet presence).
  - iii. Increased user confidence.

In an analysis of the risk that your Information Systems infrastructure would be subjected to if the firewall were absent, and the value the firewall returns to your company, we have developed the Return on Security Investment table below. Please refer to section 1.6 above for details.

Table 4-1. Firewall Return on Security Investment

Risk	SLE $	Pre-FW ARO	Post-FW ALE	Post-FW ARO	Post-FW ALE	ROSI
Risk 1.	**500**	241	$120,500	2	$1,000	$119,500
Risk 2.	**11,666**	3	$34,998	0.5	$5,833	$29,165
Risk 3.	**7,294**	4	$29,176	0.2	$1,458	$27,718
Risk 4.	**89,340**	0.5	$44,670	0.1	$8,934	$35,736
			$229,344		**$17,225**	
				Firewall Support	**$22,500**	
					ROSI	**$172,394**

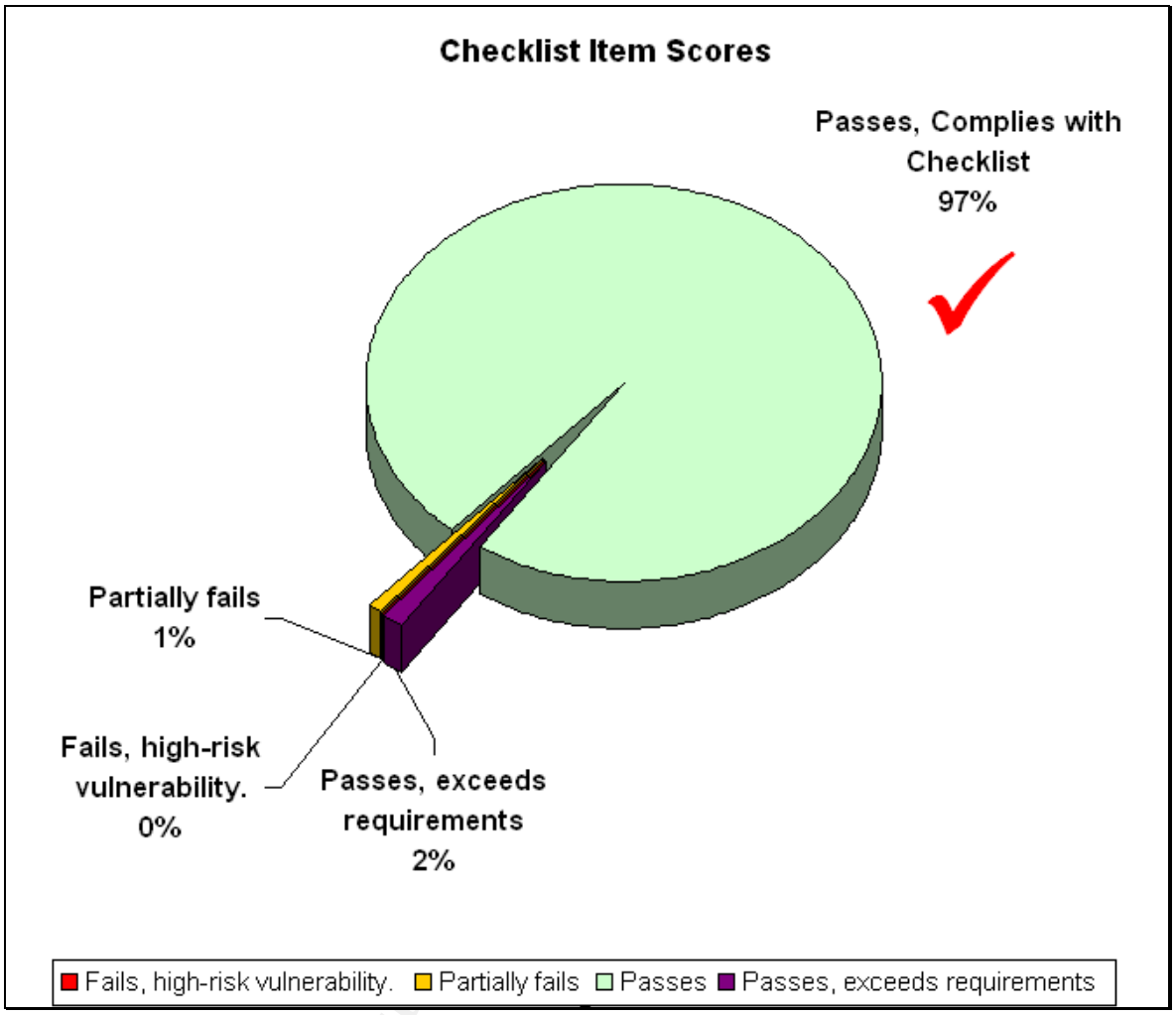
Even using four relatively simple examples from a risk profile that may include thousands of potential threat and exposure scenarios, we can see that SCP's investment in a sound security posture through the implementation of this application gateway firewall pays dividends to the tune of $172,400 Per Annum.

In assessing the firewalls role in managing risk associated with providing public web services and corporate internet access, we believe the firewall reduces the current email-borne Virus risk from Very High to Low, while the World Wide Web authentication and content filtering capabilities will ensure that Cyber-slacking, while not eliminated altogether, will be significantly reduced by as much as 85 percent. The protection afforded the online web servers reduces the risk of a web server related compromise from *Very High* to *Moderate.*

Overall, implementing an application gateway such as Astaro significantly reduces the likelihood of a major exposure occurring, and is an effective risk management tool for SimCoat Plastics. With the co-operation we have received, we believe we have raised the confidence that senior management can have in the firewalls ability to protect your organization.

Audit has shown through rigorous testing, that the firewall is capable of withstanding a high degree of abuse and attack while maintaining the integrity of its controls. In summary we believe that Astaro has performed very well within its industry sector, and providing that it is managed well, will be an excellent choice for your intended implementation.

Figure 4-1. Audit Checklist Compliance Graph.



Finally, we believe that in light of the very high compliance rate and the measurable return on security investment, the audit program has been a considerable success, with there being a very small amount of uncontrolled residual risk discovered by the audit program. Please refer to our recommendations below for suggestions in dealing with this risk.

4.2 Audit Findings.

4.2.1 Items that achieved checklist compliance

In each of the major classes of audit items the Astaro firewall, as it was configured prior to the audit, performed extremely well. This was the audits goal, though rigorous testing of the firewall's features and services provides confidence that Astaro can perform to industry best practice expectations. The scoresheet details each of the checklist items in the table below.

Table 4-2. Scoring Criteria.

Score	Condition

1	Fails, poses immediate high-risk vulnerability.
2	Partially fails, performs unexpectedly, poses low risk vulnerability.
3	Passes, meets control expectations.
4	Passes, exceeds requirements, provides additional features.

Table 4-3. Audit Checklist Results.

ü	1	2	3	4	ü	1	2	3	4	ü	1	2	3	4	ü	1	2	3	4	ü	1	2	3	4
Planning					**Services-Off**					VII.H					IX.B.1e			ü		IX.D.1a			ü	
I.A		ü			IV.A		ü			VII.I					IX.B.1f			ü		IX.D.1b			ü	
I.B		ü			IV.B		ü			VII.J					IX.B.1g			ü		IX.D.1c			ü	
I.C		ü			IV.C		ü			VII.K				ü	IX.B.1h			ü		IX.D.1d			ü	
I.D		ü			IV.D		ü			**SIPF Perf**					IX.B.1i			ü		IX.D.2a			ü	
I.E		ü			IV.E		ü			VIII.A			ü		IX.B.1j			ü		IX.D.2b			ü	
Policies					IV.F		ü			VIII.B			ü		IX.B.2a			ü		IX.D.2c			ü	
II.A		ü			**Services-On**					VIII.A			ü		IX.B.2b			ü		IX.D.2d			ü	
II.B		ü			V.A		ü			VIII.B			ü		IX.B.2c			ü		IX.D.3a			ü	
Configuration					V.B		ü			VIII.C			ü		IX.B.2d			ü		IX.D.3b			ü	
III.A		ü			V.C		ü			VIII.D			ü		IX.B.2e			ü		IX.D.3c			ü	
III.B		ü			V.D		ü			VIII.E			ü		IX.B.2f			ü		IX.D.3d			ü	
III.C		ü			V.E		ü			VIII.F			ü		IX.B.2g			ü		IX.D.4a			ü	
III.D		ü			V.F		ü			VIII.G			ü		IX.B.2h			ü		IX.D.4b			ü	
III.E		ü			V.G		ü			VIII.H			ü		IX.B.2i			ü		IX.D.4c			ü	
III.F		ü			V.H		ü			VIII.I		ü			IX.B.2j			ü		IX.D.4d				ü
III.G		ü			**SIPF-Config**					VIII.J			ü		IX.B.3a			ü		IX.E			ü	
III.H		ü			VI.A		ü			VIII.K			ü		IX.B.3b			ü		IX.F			ü	
III.I		ü			VI.B		ü			VIII.L			ü		IX.B.3c			ü		IX.G			ü	
IIIJ		ü			**Linux OS**					VIII.M			ü		IX.B.3d			ü		**Vuln-Assmt**				
III.K		ü			VII.A		ü			VIII.N			ü		IX.B.3e			ü		X.A1			ü	

III.L	ü	VII.B	ü	VIII.O	ü	IX.B.3f	ü	X.A2	ü
III.M	ü	VII.A	ü	**Proxy Perf**		IX.B.3g	ü	X.A3	ü
III.N	ü	VII.B	ü	IX.A.a	ü	IX.B.3h	ü	X.A4	ü
III.O	ü	VII.C	ü	IX.A.b	ü	IX.B.3i	ü	X.B	ü
III.P	ü	VII.D	ü	IX.B.1a	ü	IX.B.3j	ü	X.Ca	ü
III.Q	ü	VII.E	ü	IX.B.1b	ü	IX.C.1	ü	X.Cb	ü
III.R	ü	VII.F	ü	IX.B.1c	ü	IX.C.2	ü	X.Cc	ü
	ü	VII.G	ü	IX.B.1d	ü	IX.C.3	ü	X.Cd	ü

The 10 items we use to illustrate the audit process (see Section 3.2), exhibit a high degree of conformance to the audit checklists desired and expected performance, with the exception of a single low risk vulnerability discovered in checklist item *VIII.i.*

4.2.2 Checklist Items that failed compliance

4.2.2.1 Failed Checklist Item VIII.i

During testing this item demonstrated a failure in the firewall's Stateful Inspection Packet Filtering, with several port scans detecting TCP Port 8110 as OPEN. During investigation into this erroneous behaviour it was discovered that this is a known issue with Astaro Security Linux 4.008 due to a coding error in a default allow rule that is implemented when the transparent POP3 proxy is enabled.

As this only applies to the Corporate LAN interface, and there is no listening service on port 8110 to exploit, we assert that this is a VERY LOW risk vulnerability should be accepted (See recommendations below).

4.2.3 Items that surpassed checklist compliance

Two items were scored as performing above the level of compliance required or expected.

4.2.4 Checklist Item VII.K

The first item to score highly was the base-operating system configuration. Before we discuss the rationale behind our score we should disclose that the subjective baseline for OS hardening we used was a hardened off the shelf Linux distribution such as Red Hat or Mandrake with the Centre For Internet Security Linux Benchmark v 1.0 applied, and then used as a base for a Firewall. When comparing these two Linux firewall development scenarios with Astaro, the latter clearly has a far more developed security posture compared to either of the former two.

Below are some screen shots grabbed during the execution of checklist item VII.K that provide additional evidence above the checklist items (see Section VII), of the degree of hardening the base Linux OS has been subjected too.

There are minimal binaries and utilities, including no utilities to add additional users; multiple partitions for the chrooted daemons, self-monitoring daemons, backup scripts, and the automated PGP signed (by Astaro) up2date service.

We believe that the overall security stance of the base OS is a significant improvement over what could reasonably be developed by a SCP system administrator based on either of the two general-purpose distributions above. Please note the use of the proviso "*reasonably*".

Figure 4-2. Evidence of Astaro hardening, /bin and /sbin directories with minimal binaries.

```
loginuser@star:/bin > cd /sbin
loginuser@star:/sbin > ls
ainstall        fsck.ext3       insmod          modprobe        pyramid-lcd.pl  ssh-keygen
aiui            ftl_check       killall         netcat          reboot          ssh-keyscan
arp             ftl_format      killall5        nwepgen         rmmod           sshd
aus             halt            lcd-getip       pack_cis        route           sulogin
cardctl         halt_called     lcd-write       pattern_aus     runlevel        swapoff
cardmgr         hwclock         lcd-yesno       pattern_install scp             swapon
cmos            ide_info        lcdstop         pcic_probe      scsi_info       telinit
console         ifconfig        ldconfig        pcinitrd        shutdown        traceroute
consoletype     ifport          lilo            pidof           sln             vconfig
depmod          ifuser          lsmod           ping            ssh             wlancfg
dump_cis        init            mgetty          poweroff        ssh-add         wlanctl-ng
fsck            init.d          mingetty        prism2dl        ssh-agent       wland
loginuser@star:/sbin > cd /bin
loginuser@star:/bin > ls
adjtime             df                  htpasswd            ntpdate             tail
apt                 diff                ip                  passwd              tar
avsocketmultiplexer du                  kill                ps                  tc
awk                 echo                license             reiserfsck          touch
basename            expr                ln                  rm                  tr
bash                find                loadkeys            rmdir               umount
cat                 gpg                 login               sash                uname
chgrp               gpg_sign            ls                  sed                 usleep
chmod               grep                mkdir               sh                  wc
chown               gunzip              mount               sleep               wfe_passwd
cnotifier           gzip                mschapv2            sort                zcat
cp                  head                mv                  stty                zgrep
date                hostname            netstat             su
dbmmanage           htdigest            notify_mail         sync
loginuser@star:/bin >
```

Figure 4-3. Hardening evidence 2, minimal /usr/bin and /usr/sbin binaries plus multiple chrooted daemons.

```
loginuser@star:/usr/bin > ls
blink_num       jmacs           loadkeys        openssl         setfont         ssh-keyscan     vim
blink_scroll    joe             logger          passwd          setleds         stat            w
bzip2           last            md5sum          perl            splitmail       sudo            xargs
chroot          lastlog         metasend        perl5.00503     ssh             tac             zip
clear           ldapsearch      mii-diag        recode          ssh-add         tee
cut             less            mimencode       scp             ssh-agent       test
file            lesspipe.sh     nice            seq             ssh-keygen      vi
loginuser@star:/usr/bin > cd /usr/sbin
loginuser@star:/usr/sbin > ls
cfgft1          fpipemon        httpd           ppipemon        syslogd         wanpipe_lxdialog
chpasswd        fsck            klogd           pppconfig       usermod
cpipemon        fsck.ext3       mod_fastcgi.so  psd-watch.pl    wancfg
cron            ft1_exec        mppipemon       sshd            wanconfig
loginuser@star:/usr/sbin > cd /var
loginuser@star:/var > ls
aua             chroot-ha       chroot-pppoe    chroot-snmp.mrtg lib            run
chroot-ahi      chroot-identd   chroot-pptp     chroot-socks    lock            shm
chroot-bind     chroot-ipsec    chroot-pptpc    chroot-squid    log             tmp
chroot-dhcpc    chroot-pop3     chroot-report   cron            mdw
chroot-dhcps    chroot-pppd     chroot-smtp     empty           recovery
loginuser@star:/var >
```

4.2.4.1 Checklist item IX.D

In the second high scoring checklist item, the SMTP Proxy does not simply filter attachments by quarantining them as was required, but actually denies the transfer of the message from the client to the SMTP server (see evidence).

This prevents malicious attachments being transferred into the SimCoat Plastics perimeter, providing a greater degree of control over this potential virus infection vector. For this reason we scored checklist item IX.D highly.

4.3 Audit Recommendations

The management and administrative staff of SimCoat Plastics have done an excellent job of managing the risk associated with deploying an on-line infrastructure. Through the use of policies based on SANS Sample Policies[1], they have developed a base from which to build a secure I.S infrastructure. The Firewall represents a realisation of this work and functions as a cornerstone of the company's security posture.

In performing the audit above we focused on the preventative and detective functionality of the Firewall. Our recommendation to SCP is that they now turn to the administrative, organisational, and physical controls within the company and examine these in relation to the security life-cycle management of the firewall.

Things to consider are:

- Firewall SIPF rule changes: who approves, how, and when are changes applied, tested, and documented.
- Anti-Spam and Anti-Virus management, blacklists, extension filters and quarantine procedures.
- Regular log analysis beyond the automated Alert system.
- Regular paper audits of SPIF rules and system configuration based on the Baseline Checklist we present above.
- Change management of the Baseline Checklist and firewall policy.
- Regular functional testing and vulnerability assessments.
- Watch lists for each of the vendors associated with the Firewall.
- Physical access.
- Redundancy and disaster recovery.

Additionally, we assert that while the detective capabilities of the firewall itself through logs and an alert emails is excellent, the firewall does nothing to detect attacks directed against the publicly available services within SCP's public DMZ. For these attacks to be detected we would suggest the implementation of an IDS system.

Two approaches can be used here, either network or host based. Host based provides some additional functionality over that afforded by Network based though this may come at an extra cost. One critical feature that SCP should consider when evaluating IDS is that a host-based system will be able to operate above the SSL layer, thereby detecting attacks masked with SSL/TLS encryption. All Network IDS systems will fail to

[1] http://www.sans.org/resources/policies/

detect attacks over encrypted tunnels leaving your e-commerce server vulnerable if network IDS is deployed.

4.3.1 Residual un-controlled risk.

In respect to the single failed audit item we recommend that SCP accept the Very Low risk associated with this minor vulnerability.

An attempt to mitigate this Very Low risk through the implementation of an explicit DROP-LOG rule for port 8110 was tested on the development firewall's Corporate LAN interface, but failed again under re-testing, showing Port 8110 as OPEN still.

Table 4-4. Attempted SIPF Ruleset amendment.

No.	From Hostname	Service(s)	To Server	Rule
1	Corporate Lan [20.0/24]	Port 8110	Corp-LAN FW Interface	Log-Reject

It is believed that the scripts used to automate the initialisation of the transparent POP3 proxy, insert an allow rule for port 8110 into the SIPF ruleset before the user configurable rules. This is an unfortunate error on the part of the Astaro engineers and one that we hope to see fixed soon via the Up2date patch service.

If management decide that the risk associated with this vulnerability is unacceptable, it is possible to disable the transparent POP3 proxy and simply allow users to access the Mail Server via an Allow rule for port 110 between the Corporate LAN and the target mail server.

This might provide an acceptable solution if the existent Very Low risk is unacceptable, as an email message that resides on the mail-server has already been scanned inbound by the SMTP gateway antivirus service before delivery to the Mail Server.

Applying additional scanning via the transparent POP3 may be seen by some as redundant, however we would recommend that you continue to apply multiple layers of scanning inbound and outbound as there can often be a time lag between an email message arriving from the Internet, and the end-user downloading it to their system via POP3.

During this period (a weekend perhaps), the firewall may receive a pattern update that can detect any new virus residing on the Mail Server. Applying secondary anti-virus scanning via the transparent POP3 proxy will reduce the likelihood of virus outbreak within the Corporate LAN in this scenario.

We believe the single open port to be a much smaller risk with a far smaller probability of being exploited than an email borne virus infection.

4.4 Audit Conclusion

We recommend that the management of SimCoat Plastics confer accreditation on the audit and proceed to sign-off on the production implementation of the Astaro firewall. We understand the proposed change control plan details the use of the development system's configuration backup as the basis for building the production system. This migration process assures continued compliance with the audited baseline for the production system, and is supported by the auditors.

We would be happy to return at a future point in time to be discussed, and re-audit the system to ensure the firewalls integrity is maintained throughout it's security lifecycle.

5 DEFINITIONS

The following words, acronyms and abbreviations are referred to in this document.

Term	Definition
ALE	Annualised Loss Expectancy
ARO	Annualised Rate of Occurrence
DMZ	De-Militarised Zone
IP	Intellectual Property
LAN	Local Area Network
MRTG	Multi Router Traffic Grapher
MTA	Mail Transfer Agent
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
OS	Operating System
RA	Risk Assessment
ROSI	Return on Security Investment
SANS	SysAdmin, Audit, Network, Security
SCP	SimCoat Plastics
SLE	Single Loss Expectancy
SSL	Secure Sockets Layer (used by HTTPS)

6 REFERENCES

Anatomy of a Stateful Firewall
http://www.giac.org/practical/gsec/Lisa_Senner_GSEC.pd f

Application-Level Firewalls: Smaller Net, Tighter Filter
http://www.networkcomputing.com/1405/1405f3.html

Apache httpd Project
http:///httpd.apache.org/

Astaro Security Linux 4.008
http://www.astaro.com

Astaro Security Linux Documentation
http://docs.astaro.org

Auditing Firewalls: A Practical Guide
http://www.itsecurity.com/papers/p5.htm

Australian Communications-Electronic Security Instruction 33
http://www.dsd.gov.au/infosec/acsi33/

CERT: Deploying Firewalls
http://www.cert.org/security-improvement/modules/m08.html

CERT: Practices about hardening and securing systems
http://www.cert.org/security-improvement/index.html#Harden

Detecting Loadable Kernel Modules (LKM)
http://www.linuxsecurity.com/resource_files/host_security/lkm.htm

Finally a Real Return on Security Spending
http://www.cio.com/archive/021502/security.html

Freefire Library,Hardening Ressourcs
http://www.freefire.org/lib/hardening.en.php3

Improving Apache
http://www.infosecuritymag.com/articles/april01/f eatures1_web_server_sec.shtml

Internet Security Systems; Internet Scanner
http://www.iss.net

ISACA: The Information Systems Audit and Control Association & Foundation
http://www.isaca.org/

ISACA: Standards, Guidelines and Procedures
http://www.isaca.org/standard/stdownload.htm
http://www.isaca.org/standard/guidelne.htm

Kapersky Lab
http://www.kaspersky.com/

Linux Administrator's Security Guide
http://www.seifried.org/lasg/

Linux Journal: Security Tools in Linux Distributions, Part I
http://www.linuxjournal.com/article.php?sid=6361

Linux Journal: Security Tools in Linux Distributions, Part II
http://www.linuxjournal.com/article.php?sid=6362

NIST: Guidelines on Firewalls and Firewall Policy
http://csrc.nist.gov/publications/nistpubs/

Nmap home
http://www.insecure.org

The Center for Internet Security; Level-1 Benchmark and Scoring Tool for Linux
http://www.cisecurity.com/

The Institute for Security and Open Methodologies; Open Source Security Testing Methodology Manual
http://www.isecom.org/

The Institute of Internal Auditors; Audit Reference Library
http://www.theiia.org/itaudit/index.cfm?fuseaction=reflibhome

The Open Web Application Security Project
http://www.owasp.org/
Risk Assessment Models and Evolving Approaches
http://www.gammassl.co.uk/topics/IAAC.htm

SANS: The Packet Filter: A Basic Network Security Tool
http://www.sans.org/rr/firewall/packet_filter.php

SANS: The SANS Security Policy Project
http://www.sans.org/resources/policies/

Securing and Optimizing Linux 1.3
http://www.linuxsecurity.com/docs/Securing-Optimizing-v1.3/

Securing & Optimizing Linux: The Ultimate Solution v2.0
http://www.openna.com/products/books/sol/solus.phpw

SecurityFocus; Introduction to Security Policies (Four-Part series)
http://www.securityfocus.com/infocus/1193

SecurityFocus; Assessing Internet Security Risk (five-part series)
http://www.securityfocus.com/infocus/1591

Squid Web Proxy Cache home
http://www.squid-cache.org/

State of Texas; Department of Information Resources
www.dir.state.tx.us/security/policies/

Sysadmin Magazine Linux rockery

http://www.samag.com/linux/

7 APPENDICES

7.1 Appendix 1 SimCoat Plastics Firewall Policy.

SimCoat Plastics Internal: Registered and Restricted

This document is released subject to conditions described in;
SimCoat Plastics Information Sensitivity Policy

SCP INTERNET FIREWALL POLICY

Last modified on June 18, 03

Table of Contents

OVERVIEW OF FIREWALL POLICY

Due to the increasingly hostile environment on the Internet, SimCoat Plastics has established a networking policy that protects the SimCoat Plastics computing resources from potential intruders. The goals of this policy are to prevent unauthorized use of SimCoat Plastics resources and the loss of data invariably associated with break-ins, and also to protect the confidentiality of data stored on SimCoat Plastics machines. Access to the Internet's immense resources is not restricted arbitrarily; however, inherently insecure services are prohibited. Secure methods for accessing external resources are provided whenever they are available.

The system will be configured and deployed in line with the following Corporate Security policies:

SimCoat Plastics_Acceptable_Use_Policy.doc
SimCoat Plastics_Anti-virus_Guidelines.doc
SimCoat Plastics_Audit_Policy.doc
SimCoat Plastics_Change_Management_Policy.doc
SimCoat Plastics_Email_Policy.doc
SimCoat Plastics_Information_Sensitivity_Policy.doc
SimCoat Plastics_Network_Access_Security_Policy.doc
SimCoat Plastics_Password_Policy.doc
SimCoat Plastics_Risk_Assessment_Policy.doc
SimCoat Plastics_Server_Security_Policy.doc

DEFINITION OF SECURITY ZONES

Because different groups inside SimCoat Plastics require different levels of access to external and internal resources, SimCoat Plastics has been divided into three security zones. Each of these zones has a different level of exposure to external and internal

threats, and consequently access among the zones is restricted to maintain a high overall level of security. There are four security zones currently defined:

Demilitarised Zone: This is a moderate security zone providing Public access to SimCoat Plastics Internet services. The DMZ is protected by traffic filtering, but the user base of these machines is not trusted, so the other zones are protected from the DMZ by traffic filtering at the Firewall.

Backend Zone: This is a high security zone. It is protected from all other zones by traffic filtering. This zone is intended for operational purposes only that require trusted users to have extraordinary access to individual machines.

Corporate Zone: This is the moderate-high security zone. It is protected from the Internet by traffic filtering, and the Internet is protected from it by traffic filtering. This is intended to be the largest group of machines administered by SimCoat Plastics, and its security should be managed to protect all machines. Services are to be provided to support ordinary, everyday access to and from the Internet, but may be restricted to only secure protocols. The user base of these machines is untrusted.

List of Permitted TCP Service Access Vectors

In addition to the services listed below, ICMP traffic among the security zones is limited to:

- echo request
- echo reply
- time exceeded
- unreachables
- parameter problem

Internet to **SimCoat Plastics DMZ:**

1. HTTP on port 80 to: *www.SCP.com*
2. HTTPS on port 443 to: *www.ecom.SCP.com*
3. FTP client sessions to: *ftp.SCP.com*
4. SMTP mail to SMTP proxy: *mail.SCP.com*

DMZ to **Backend Zone:**

1. To Syslog server
2. Secure HTTPS server to MySQL server only.

DMZ to **Corporate Zone:**

1. NIL

Backend Zone to **Internet:**

1. NIL

Backend Zone to **Corporate Zone.**

1. NIL

Backend Zone to **DMZ.**

1. NTP to NTP server
2. Management Station to Terminal Services

Corporate Zone to **Public DMZ** :

1. HTTP and HTTPS access to Public web servers.

NB: clients must use and authenticate to *cache.SCP.com* first.

2. FTP client sessions to: *ftp.SCP.com*

Corporate Zone to **Backend Zone:**

1. SMTP and POP to *corpmail.SCP.com*
2. Windows SMB/Netbios from CorpZone DC to BackendZone DC.
3. NTP from CorpZone DC to BackendZone DC.
4. Controlled, as authorised access to MySQL server (may include SSH).

   Note: Must be approved by IS manager and Direct Line manager.

Corporate Zone to **Internet:**

1. DNS via DNS proxy on Firewall
2. HTTP and HTTPS. Clients must use and authenticate to *cache.SCP.com* as a proxy server.

   Note: Web Access will be subject to inline content filtering in line with appropriate use policies.
3. FTP client sessions.

Anti-spoofing Rules

Anti-spoofing rules must be applied to protect against spoofed attacks for RFC 1918 networks.

FIREWALL CONFIGURATION BLUEPRINT:

1. Only 2 administrator accounts will be used for managing the firewall, those of Alan Thomson and Sven Koenig. Password and account management will comply with the SCP Password and Server Security Policies.
2. Ensure each of the DMZ and Backend Hosts are uniquely identified, along with the Corporate LAN DC.
3. Apply least privileges principals throughout the configuration of the Firewall.

7.1.1 Base OS Hardening.

To provide additional hardening to the base OS, perform the following task.

1.) Add a Root login timeout value of 30 minutes to the /etc/profile file. Open /etc/profile with vim and add the following line somewhere after the "HISTSIZE=" line;

TMOUT = 1800

7.1.2 Base Firewall Configuration

- Hostname: star.scp.net
- Administrator e-mail addresses:

- trouble@scp.net
- skoenig@scp.net
- help@scp.net

- Time zone: AEST
- NTP server: NTP Server Canberra
- **Web Admin Interface:**
  - Timeout (seconds): 300 seconds
  - Allowed networks:
    - Management-host01
    - Management-host02
  - Authentication methods:
    - Local Accounts
- Allowed users:
  - admin
  - alanthomson
  - svenkoenig

7.1.3 Services:

- SSH Status: Disabled
- Up2Date Configuration
  - Automatic Pattern Up2date: Enabled
  - Interval: Daily
- Email Backup
  - *Enabled and configured to use:*
    - *trouble@scp.net*
    - *skoenig@scp.net*
    - *swilson@scp.net*
  - Backup Interval
    - Daily
  - Backup Encryption:
    - Enabled, and pass-phrase entered
- Syslog Configuration
  - Remote Syslog Hosts:
    - Authentication Logs: Syslog-Station-01
    - Daemon Logs: Syslog-Station-01
    - Kernel Logs: Syslog-Station-01
    - Notification: Syslog-Station-01
    - SMTP Relay Logs: Syslog-Station-01
- User Authentication:
  - Radius Server Settings.
  - Status: Disabled
  - SAM (NT/2000/XP) Server Settings.
  - Status: Enabled
    - PDC: WIN2KDC
    - PDC Address: 192.168.10.40
    - BDC: WIN2KDC
    - BDC Address: 192.168.10.40
  - LDAP Server Settings.
  - Status: Disabled
- WebAdmin Site Certificate:
  - Country code: Australia
  - State or region: Victoria
  - City: Melbourne
  - Company: SimCoat Plastics

- Org. unit: InfoSec
- Contact e-mail: trouble@scp.net
- Firewall hostname: star.scp.net

- Local User Accounts:
  - admin
  - alanthomson
  - svenkoenig
- DHCP Server:
  - *Status:* enabled
  - *Network to serve:* Corporate LAN
  - *Range Start:* 192.168.20.64
  - *Range End:* 192.168.2.253
  - *DNS Server 1:* 192.168.20.1
  - *DNS Server 2:* blank
  - *Gateway IP:* 192.168.20.1
  - *WINS Server:* 192.168.20.10
  - *WINS Node Type:* P Node: Peer WINS Only
  - *Static Mappings:* none configured
- Traffic Accounting:
  - Status: Enabled
  - Interfaces:
    - Public DMZ
    - Corporate LAN
    - Backend LAN
    - Internet
- Port Scan Detection:
  - Status: Enabled
  - Action taken on portscanner traffic: drop (blackhole)

7.1.4 Packet Filtering:

Implement the following ruleset.

From Hostname	Service(s)	To Server	Rule
Corp LAN DC02	NTP	Syslog Wkstn	Allow
Corp LAN DC02	Windows-SMB	Backend LAN-DC01	Allow
Corporate Lan [20.0/24]	Any	Any	Log-Reject
Syslog Wkstn	NTP	FTP Server01	Allow
Management-PC 1	MS Terminal Services	Public DMZ	Allow
Management-PC 2	MS Terminal Services	Public DMZ	Allow
Management-PC 1	FTP {active}	Public DMZ	Allow
Management-PC 2	FTP {active}	Public DMZ	Allow
All RFC 1918 Private	Any	Any	Log-Reject
Any	HTTP	Web Server01	Allow

Any	HTTPS	Web Server02	Allow
Any	FTP {active}	FTP Server01	Allow
Public_DMZ [25.16/29]	SYSLOG	Syslog Wkstn	Allow
Web Server02	MySQL {3306}	MySQL Server	Allow
Any	Any	Any	Log-Reject

7.1.5 ICMP Rules

- Config: ICMP Settings:
- ICMP Settings.
  - ICMP Forwarding: Enabled
  - ICMP on Firewall: Enabled
- Traceroute Settings.
  - Firewall is traceroute visible: Enabled
  - Firewall forwards traceroute: Enabled
  - Traceroute from Firewall: Disabled
- PING Settings.
  - Firewall is PING visible: Enabled
  - Firewall forwards PING: Enabled
  - PING from firewall: Disabled

7.1.6 Application Proxies:

In addition to the filtering of TCP network connections provided by traditional stateful firewalls, the Astaro firewall will provide the following Application Proxy firewall services:

1. SMTP Proxy with AntiVirus.
2. HTTP/S Proxy with Windows Domain Authentication.

   Note: This is complies with the *SimCoat Plastics Password Policy* Section C**. Application Development Standards.**
3. HTTP/S Content Filtering.

7.1.6.1 SMTP-Proxy Configuration

All efforts will be made to protect SCP resources through the use of all reasonable Anti-Spam, and Antivirus facilities available within the SMTP proxy. All effort will be made to minimise any user impact.

The SMTP proxy shall be configured as follows:

- Status: Enabled
- Hostname MX: mail.scp.com
- Postmaster Address: *postmaster@scp.net*
- Max message size: 5MB
- Incoming Mail: SMTP Routes Table
- *Domain name:* scp.net
- *SMTP host:* Mail-Server01
- Outgoing Mail: Allowed Networks
  - Corporate_Lan_Network
  - Mail-Server01
- Use smarthost: Disabled
- Use callouts: Disabled

- Sender Blacklist: Enabled
- Spam detection: Enabled
  - *Action:* Quarantine
  - *Strategy:* Conservative
- Block RCPT hacks: Enabled
- Virus Protection: Enabled
  - *Action:* Quarantine
- Realtime Blackhole Lists (RBL): Enabled
  - *Action:* Reject
  - *Zones:* Blackholes.mail-abuse.org
- File extension filter: Enabled
  - *Extensions:* .com, .pif, .bat, .vbs, .scr, .exe
- Expression filter: Enabled

7.1.6.2 POP3 Proxy

All efforts will be made to protect SCP resources through the use of all reasonable Anti-Spam, and Antivirus facilities available within the POP3 proxy. All effort will be made to minimise any user impact.

The POP3 proxy shall be configured as follows:

- Configured Proxied Networks
  - Source: Corporate_Lan_Network
- Destination: MailServer01
- Virus Protection: Enabled

7.1.6.3 HTTP-Proxy Configuration

The HTTP/S Proxy will be configured to use local Windows 2000 Domain accounts for authenticating access to the internet as follows:

- Status: Enabled
- Authentication: User Authentication
- Anonymity: Standard
- Caching: Enabled
- TCP Port: 8080
- Allowed Networks: Corporate LAN
- Allowed Services: FTP, HTTP, HTTPS
- Authentication: NT/2000/XP Server

7.1.6.4 HTTP/S Content Filtering

Certain classes of content have been classified as non business related and the Content Filtering service will be configured as follows:

- Categories:
  - Criminal Activities
  - Drugs
  - Extremistic_Sites
  - Games_Gambles
  - Job_Search
  - Nudity
  - Private_Homepages
  - Weapons
- *Users:* Empty
- *Source Network:* Corporate LAN
- *Whitelist:* Empty
- Blacklist: Empty

-

7.2 NB !! : Ensure that the each:

- **NAT,**
- **PPTP,**
- **IPSec VPN,**
- **QoS,**
- **Ident Relay,and**
- **SOCKS 5 Proxy**

services are <u>disabled</u> AND <u>unconfigured</u> !

This Classified Document is maintained by trouble@scp.net.au

Thanks to Chris Lethaby for assistance in compiling this document.

7.3 Appendix 2. NMAP Scan Batch File

The Open Source Security Testing Methodology Manual describes a comprehensive program of activities to be completed when performing a Port Scan. The batch file below is an interpretation and implementation of this process.

Performing a thorough automated scan like this is a very prudent measure. As an auditor we may not have a lot of time to test the firewall so we have to be as efficient as possible. After all, while we may have days to find any weaknesses, hackers may spend weeks, months or years testing the firewall.

>| snip

```
@echo off
REM A q&d batch file by Chris Lethaby to make NMAP scans a bit easier
REM
REM MD5.exe courtesy of http://www.fourmilab.ch/md5/
REM Soon.exe courtesy of
http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/soon -
o.asp
REM Rar.exe for DOS (unlicensed) courtesy of http://download.com.com/3000 -
2250-10044377.html
REM choice.exe and sleep.exe courtesy of the Windows 2000 Resource Kit
(Licenced)
REM Nmap courtesy of http: //www.nmap.org

COLOR 0A
If "%1"=="" GOTO Help
If "%2"=="" GOTO Help
GOTO menu

:menu
cls
echo.
echo What would you like to do?
echo.
echo Choice
echo.
echo A. Read the detailed README that describes each of the options below ?
```

```
echo B. Perform a series of SynScans using source ports 21, 22, 25, 53, 80,
and 443.
echo C. Perform an AckScan using Source Port 80
echo D. Perform an FinScan
echo E. Perform an Xmas Tree Scan
echo F. Perform an Fragmentted Scan
echo G. Perform a UDP port scan? (This takes a very long time!)
echo H. Perform the whole kit and caboodle ??
echo I. EXIT
echo.
GOTO choice

:choice
choice /c:abcdefghi /N Choose A, B, C, D, E, F, G, H, or I ?
IF ERRORLEVEL 9 GOTO exit
IF ERRORLEVEL 8 GOTO Monty
IF ERRORLEVEL 7 GOTO UDPScan
IF ERRORLEVEL 6 GOTO FragScan
IF ERRORLEVEL 5 GOTO XmasScan
IF ERRORLEVEL 4 GOTO FinScan
IF ERRORLEVEL 3 GOTO AckScan
IF ERRORLEVEL 2 GOTO SynScan
IF ERRORLEVEL 1 GOTO readme

:readme
notepad %systemdrive%\scan\readme2.txt
GOTO menu

:SynScan
echo.
echo ############################################################
echo #                                                          #
echo #        Starting a Syn scan of the target system           #
echo #        This will take a few hours to a few  days.          #
echo #                                                          #
echo ############################################################
echo.

REM Perform a series of Syn Scans (1-65535) using source ports 20, 21, 25,
53, 80, and 443.
echo The Syn Scan started at > SynScan-%1_%2-time.log
now >> SynScan-%1_%2-time.log
echo Now performing a default  -sS scan
echo.
nmap -sS -vn -oA SynScan-1-%1_%2 -p 1-65535 %1
sleep 2
echo Now performing a  -sS scan with source port 20
nmap -sS -vn -oA SynScan-2-%1_%2 -g 20 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a  -sS scan with source port 21
nmap -sS -vn -oA SynScan-3-%1_%2 -g 21 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a  -sS scan with source port 25
nmap -sS -vn -oA SynScan-4-%1_%2 -g 25 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a  -sS scan with source port 53
nmap -sS -vn -oA SynScan-5-%1_%2 -g 53 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
```

```
echo Now performing a -sS scan with source port 80
nmap -sS -vn -oA SynScan-6-%1_%2 -g 80 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sS scan with source port 443
nmap -sS -vn -oA SynScan-7-%1_%2 -g 443 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo The Syn Scan ended at >> SynScan-%1_%2-time.log
now >> SynScan-%1_%2-time.log
sleep 2
md5 SynScan*.* > SynScan-%1_%2.md5
rar a -df -m5 %1_%2_Syn_Scan.rar SynScan*.*
sleep 2
IF "%Scan%"=="Monty" GOTO AckScan
GOTO menu

:AckScan
echo.
echo ############################################################
echo #                                                          #
echo #       Starting a Ack scan of the target system           #
echo #        This will take a few hours to a f ew days.         #
echo #                                                          #
echo ############################################################

echo The Ack Scan started at > AckScan-%1_%2-time.log
now >> AckScan-%1_%2-time.log
echo Now performing a default -sA scan
echo.
nmap -sA -vn -oA AckScan-1-%1_%2 -p 1-65535 %1
sleep 2
echo Now performing a -sA scan with source port 20
nmap -sA -vn -oA AckScan-2-%1_%2 -g 20 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sA scan with source port 21
nmap -sA -vn -oA AckScan-3-%1_%2 -g 21 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sA scan with source port 25
nmap -sA -vn -oA AckScan-4-%1_%2 -g 25 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sA scan with source port 53
nmap -sA -vn -oA AckScan-5-%1_%2 -g 53 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sA scan with source port 80
nmap -sA -vn -oA AckScan-6-%1_%2 -g 80 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sA scan with source port 443
nmap -sA -vn -oA AckScan-7-%1_%2 -g 443 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo The Ack Scan ended at >> AckScan-%1_%2-time.log
now >> AckScan-%1_%2-time.log
sleep 2
md5 AckScan*.* > AckScan-%1_%2.md5
rar a -df -m5 %1_%2_Ack_Scan.rar AckScan*.*
sleep 2
```

```
IF "%Scan%"=="Monty" GOTO FinScan
GOTO menu

:FinScan
echo.
echo ############################################################
echo #                                                          #
echo #       Starting a Fin scan of the target system           #
echo #       This will take a few hours to a few days.          #
echo #                                                          #
echo ############################################################

echo The Fin Scan started at > FinScan-%1_%2-time.log
now >> FinScan-%1_%2-time.log
echo Now performing a default  -sF scan
echo.
nmap -sF -vn -oA FinScan-1-%1_%2 -p 1-65535 %1
sleep 2
echo Now performing a -sF scan with source port 20
nmap -sF -vn -oA FinScan-2-%1_%2 -g 20 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sF scan with source port 21
nmap -sF -vn -oA FinScan-3-%1_%2 -g 21 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sF scan with source port 25
nmap -sF -vn -oA FinScan-4-%1_%2 -g 25 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sF scan with source port 53
nmap -sF -vn -oA FinScan-5-%1_%2 -g 53 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sF scan with source port 80
nmap -sF -vn -oA FinScan-6-%1_%2 -g 80 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sF scan with source port 443
nmap -sF -vn -oA FinScan-7-%1_%2 -g 443 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo The Fin Scan ended at >> FinScan-%1_%2-time.log
now >> FinScan-%1_%2-time.log
sleep 2
md5 FinScan*.* > FinScan-%1_%2.md5
sleep 2
rar a -df -m5 %1_%2_Fin_Scan.rar  FinScan*.*
sleep 2
IF "%Scan%"=="Monty" GOTO XmasScan
GOTO menu

:XmasScan
echo.
echo ############################################################
echo #                                                          #
echo #       Starting a Xmas scan of the  target system         #
echo #       This will take a few hours to a few days.          #
echo #                                                          #
echo ############################################################
echo.
echo The Xmas Scan started at > XmasScan-%1_%2-time.log
```

```
now >> XmasScan-%1_%2-time.log

echo.
echo Now performing a default  -sX scan
echo.
nmap -sX -vn -oA XmasScan-1-%1_%2 -p 1-65535 %1
sleep 2
echo Now performing a  -sX scan with source port 20
nmap -sX -vn -oA XmasScan-2-%1_%2 -g 20 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a  -sX scan with source port 21
nmap -sX -vn -oA XmasScan-3-%1_%2 -g 21 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a  -sX scan with source port 25
nmap -sX -vn -oA XmasScan-4-%1_%2 -g 25 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a  -sX scan with source port 53
nmap -sX -vn -oA XmasScan-5-%1_%2 -g 53 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a  -sX scan with source port 80
nmap -sX -vn -oA XmasScan-6-%1_%2 -g 80 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a  -sX scan with source port 443
nmap -sX -vn -oA XmasScan-7-%1_%2 -g 443 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo The Xmas Scan ended at >> XmasScan-%1_%2-time.log
now >> XmasScan-%1_%2-time.log
sleep 2
md5 XmasScan*.* > XmasScan-%1_%2.md5
sleep 2
rar a -df -m5 %1_%2_Xmas_Scan.rar XmasScan*.*
sleep 2
IF "%Scan%"=="Monty" GOTO FragScan
GOTO menu


:FragScan
echo.
echo ###############################################################
echo #                                                             #
echo # Starting a series of Fragmented scans of the target system  #
echo #      This will take a few hours to a few days.              #
echo #                                                             #
echo ###############################################################
echo.
echo The Frag Scan started at > FragScan-%1_%2-time.log
now >> FragScan-%1_%2-time.log
echo Now performing a Full Fragmented  -sS scan
echo
nmap -sS -vnf -oA FragScan-1-%1_%2 -p 1-65535 %1
sleep 2
echo Now performing a Fragmented  -sA scan.
nmap -sA -vnf -oA FragScan-2-%1_%2 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a Fragmented  -sF scan.
```

```
nmap -sF -vnf -oA FragScan-3-%1_%2 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a Fragmented -sX scan.
nmap -sX -vnf -oA FragScan-4-%1_%2 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo The Frag Scan ended at >> FragScan-%1_%2-time.log
now >> FragScan-%1_%2-time.log
sleep 2
md5 FragScan*.* > FragScan-%1_%2.md5
sleep 2
rar a -df -m5 %1_%2_Frag_Scan.rar FragScan*.*
sleep 2
IF "%Scan%"=="Monty" GOTO UDPScan
GOTO menu

:UDPScan
echo.
echo ############################################################
echo #                                                          #
echo #       Starting a UDP scan of the target system           #
echo #     This will take 5 hours to 5 weeks... seriously !     #
echo #                                                          #
echo ############################################################
echo.
echo The UDP Scan started at > UDPScan-%1_%2-time.log
now >> UDPScan-%1_%2-time.log
echo Now performing a default -sU scan
echo
nmap -sU -vn -oA UDPScan-1-%1_%2 -p 1-65535 %1
sleep 2
echo Now performing a -sU scan with source port 20
nmap -sU -vn -oA UDPScan-2-%1_%2 -g 20 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sU scan with source port 21
nmap -sU -vn -oA UDPScan-3-%1_%2 -g 21 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sU scan with source port 25
nmap -sU -vn -oA UDPScan-4-%1_%2 -g 25 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sU scan with source port 53
nmap -sU -vn -oA UDPScan-5-%1_%2 -g 53 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sU scan with source port 80
nmap -sU -vn -oA UDPScan-6-%1_%2 -g 80 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo Now performing a -sU scan with source port 443
nmap -sU -vn -oA UDPScan-7-%1_%2 -g 443 -p 1-1524,2300-2400,3100-3250,4800-
6200,7900-8100,10001-10050,32770-33550,60000-60100 %1
sleep 2
echo The UDP Scan ended at >> UDPScan-%1_%2-time.log
now >> UDPScan-%1_%2-time.log
sleep 2
md5 UDPScan*.* > UDPScan-%1_%2.md5
sleep 2
rar a -df -m5 %1_%2_UDP_Scan.rar UDPScan*.*
```

```
sleep 2
GOTO menu

:Monty
SET Scan=Monty
echo.
echo ################################################################
echo #                                                              #
echo #     Ok we're going to scan the target(s) top to bottom.      #
echo #       There are 39 Scans in total so I suggest you           #
echo #    stop watching the console and stay alert for problems     #
echo #                              : -)                            #
echo #                                                              #
echo ################################################################
echo.
sleep 2
GOTO SynScan

:Help
echo.
echo ################################################################
echo #                                                              #
echo #     !!          How to use this script          !!          #
echo #                                                              #
echo # Run scan.bat [IP_address(s) ^<space^> PSD_ON or PSD_OFF]     #
echo #                                                              #
echo #                                                              #
echo ################################################################
echo.
GOTO end

:exit
color
sleep 3
exit
:end
```

7.4 Appendix 3. Checklist VIII.l Evidence of Task Completion

Output of Dir /s command for Checklist item VIII.l evidence directory.

```
Volume in drive E is Tools
 Volume Serial Number is B011 -73CF

 Directory of E: \GSNA\Project\portscan\VIII.L

13/07/2003  08:3 4p    <DIR>         .
13/07/2003  08:34p     <DIR>         ..
13/07/2003  08:32p     <DIR>         192.168.20.1_PSD_OFF_Ack_Scan
10/07/2003  11:26p           11,420 192.168.20.1_PSD_OFF_Ack_Scan.rar
13/07/2003  08:32p     <DIR>         192.168.20.1_PSD_OFF_Fin_Scan
11/07/2003  02:09a            9,785 192.168.20.1_PSD _OFF_Fin_Scan.rar
13/07/2003  08:32p     <DIR>         192.168.20.1_PSD_OFF_Frag_Scan
11/07/2003  07:07a           64,605 192.168.20.1_PSD_OFF_Frag_Scan.rar
13/07/2003  08:32p     <DIR>         192.168.20.1_PSD_OFF_Syn_Scan
10/07/2003  09:01p           11,399 192.168.20.1_PSD_O FF_Syn_Scan.rar
13/07/2003  07:00p     <DIR>         192.168.20.1_PSD_OFF_UDP_Scan
12/07/2003  08:36p          206,166 192.168.20.1_PSD_OFF_UDP_Scan.rar
13/07/2003  08:32p     <DIR>         192.168.20.1_PSD_OFF_Xmas_S can
11/07/2003  05:21a          126,881 192.168.20.1_PSD_OFF_Xmas_Scan.rar
13/07/2003  08:34p              65 Checklist
```

```
13/07/2003  08:34p                 0 Checklist_VIII.l.log
               8 File(s)        430,321 bytes

 Directory of E:\GSNA\Project\portscan\VIII.L\192.168.20.1_PSD_OFF_Ack_Scan

13/07/2003  08:32p      <DIR>          .
13/07/2003  08:32p      <DIR>          ..
10/07/2003  10:29p                 507 AckScan -1-192.168.20.1_PSD_OFF.gnmap
10/07/2003  10:29p                 588 Ack Scan-1-192.168.20.1_PSD_OFF.nmap
10/07/2003  10:29p               1,322 AckScan -1-192.168.20.1_PSD_OFF.xml
10/07/2003  11:26p                 106 AckScan -192.168.20.1_PSD_OFF -time.log
10/07/2003  11:26p               1,632 AckScan -192.168.20.1_PSD_OFF.md5
10/07/2003  10:38p                 678 AckScan -2-192.168.20.1_PSD_OFF.gnmap
10/07/2003  10:38p                 569 AckScan -2-192.168.20.1_PSD_OFF.nmap
10/07/2003  10:38p               1,362 AckScan -2-192.168.20.1_PSD_OFF.xml
10/07/2003  10:48p                 678 AckScan -3-192.168.20.1_PSD_OFF.gnmap
10/07/2003  10:48p                 569 AckScan -3-192.168.20.1_PSD_OFF.nmap
10/07/2003  10:48p               1,362 AckScan -3-192.168.20.1_PSD_OFF.xml
10/07/2003  10:57p                 678 AckScan -4-192.168.20.1_PSD_OFF.gnmap
10/07/2003  10:57p                 569 AckScan -4-192.168.20.1_PSD_OFF.nmap
10/07/2003  10:57p               1,362 AckScan -4-192.168.20.1_PSD_OFF.xml
10/07/2003  11:07p                 708 AckScan -5-192.168.20.1_PSD_OFF.gnmap
10/07/2003  11:07p                 618 AckScan -5-192.168.20.1_PSD_OFF.nmap
10/07/2003  11:07p               1,484 AckScan -5-192.168.20.1_PSD_OFF.xml
10/07/2003  11:16p                 708 AckScan -6-192.168.20.1_PSD_OFF.gnmap
10/07/2003  11:16p                 618 AckScan -6-192.168.20.1_PSD_OFF.nmap
10/07/2003  11:16p               1,484 AckScan -6-192.168.20.1_PSD_OFF.xml
10/07/2003  11:26p                 709 AckScan -7-192.168.20.1_PSD_OFF.gnmap
10/07/2003  11:26p                 619 AckScan -7-192.168.20.1_PSD_OFF.nmap
10/07/2003  11:26p               1,486 AckScan -7-192.168.20.1_PSD_OFF.xml
              23 File(s)         20,416 bytes

 Directory of E:\GSNA\Project\portscan\VIII.L\192.168.20.1_PSD_OFF_Fin_Scan

13/07/2003  08:32p      <DIR>          .
13/07/2003  08:32p      <DIR>          ..
11/07/2003  01:22a                 360 FinScan -1-192.168.20.1_PSD_OFF.gnmap
11/07/2003  01:22a                 309 FinScan -1-192.168.20.1_PSD_OFF.nmap
11/07/2003  01:22a                 880 FinScan -1-192.168.20.1_PSD_OFF. xml
11/07/2003  02:09a                 106 FinScan -192.168.20.1_PSD_OFF -time.log
11/07/2003  02:09a               1,632 FinScan -192.168.20.1_PSD_OFF.md5
11/07/2003  01:30a                 588 FinScan -2-192.168.20.1_PSD_OFF.gnmap
11/07/2003  01:30a                 388 Fi nScan-2-192.168.20.1_PSD_OFF.nmap
11/07/2003  01:30a               1,114 FinScan -2-192.168.20.1_PSD_OFF.xml
11/07/2003  01:37a                 588 FinScan -3-192.168.20.1_PSD_OFF.gnmap
11/07/2003  01:37a                 388 FinScan -3-192.168.20.1_PSD_OFF.nm ap
11/07/2003  01:37a               1,114 FinScan -3-192.168.20.1_PSD_OFF.xml
11/07/2003  01:45a                 588 FinScan -4-192.168.20.1_PSD_OFF.gnmap
11/07/2003  01:45a                 388 FinScan -4-192.168.20.1_PSD_OFF.nmap
11/07/2003  01:45a               1,114 FinScan -4-192.168.20.1_PSD_OFF.xml
11/07/2003  01:53a                 588 FinScan -5-192.168.20.1_PSD_OFF.gnmap
11/07/2003  01:53a                 388 FinScan -5-192.168.20.1_PSD_OFF.nmap
11/07/2003  01:53a               1,114 FinScan -5-192.168.20.1_PSD_OFF.xml
11/07/2003  02:01a                 588 FinScan -6-192.168.20.1_PSD_OFF.gnmap
11/07/2003  02:01a                 388 FinScan -6-192.168.20.1_PSD_OFF.nmap
11/07/2003  02:01a               1,114 FinScan -6-192.168.20.1_PSD_OFF.xml
11/07/2003  02:09a                 589 FinScan -7-192.168.20.1_PSD_OFF.gnmap
11/07/2003  02:09a                 389 FinScan -7-192.168.20.1_PSD_OFF.nmap
11/07/2003  02:09a               1,116 FinScan -7-192.168.20.1_PSD_OFF.xml
              23 File(s)         15,831 bytes
```

```
 Directory of E:\GSNA\Project\portscan\VIII.L\192.168.20.1_PSD_OFF_Frag_Scan

13/07/2003  08:32p    <DIR>          .
13/07/2003  08:32p    <DIR>          ..
11/07/2003  06:27a               475 FragScan-1-192.168.20.1_PSD_OFF.gnmap
11/07/2003  06:27a               578 FragScan-1-192.168.20.1_PSD_OFF.nmap
11/07/2003  06:27a             1,251 FragScan-1-192.168.20.1_PSD_OFF.xml
11/07/2003  07:07a               108 FragScan-192.168.20.1_PSD_OFF-time.log
11/07/2003  07:07a             1,007 FragScan-192.168.20.1_PSD_OFF.md5
11/07/2003  06:36a               692 FragScan-2-192.168.20.1_PSD_OFF.gnmap
11/07/2003  06:36a               602 FragScan-2-192.168.20.1_PSD_OFF.nmap
11/07/2003  06:36a             1,423 FragScan-2-192.168.20.1_PSD_OFF.xml
11/07/2003  06:52a            93,370 FragScan-3-192.168.20.1_PSD_OFF.gnmap
11/07/2003  06:52a           211,589 FragScan-3-192.168.20.1_PSD_OFF.nmap
11/07/2003  06:52a           332,565 FragScan-3-192.168.20.1_PSD_OFF.xml
11/07/2003  07:07a            93,370 FragScan-4-192.168.20.1_PSD_OFF.gnmap
11/07/2003  07:07a           211,589 FragScan-4-192.168.20.1_PSD_OFF.nmap
11/07/2003  07:07a           332,566 FragScan-4-192.168.20.1_PSD_OFF.xml
              14 File(s)      1,281,185 bytes

 Directory of E:\GSNA\Project\portscan\VIII.L\192.168.20.1_PSD_OFF_Syn_Scan

13/07/2003  08:32p    <DIR>          .
13/07/2003  08:32p    <DIR>          ..
10/07/2003  08:04p               483 SynScan-1-192.168.20.1_PSD_OFF.gnmap
10/07/2003  08:04p               588 SynScan-1-192.168.20.1_PSD_OFF.nmap
10/07/2003  08:04p             1,298 SynScan-1-192.168.20.1_PSD_OFF.xml
10/07/2003  09:01p               106 SynScan-192.168.20.1_PSD_OFF-time.log
10/07/2003  09:01p             1,632 SynScan-192.168.20.1_PSD_OFF.md5
10/07/2003  08:14p               666 SynScan-2-192.168.20.1_PSD_OFF.gnmap
10/07/2003  08:14p               569 SynScan-2-192.168.20.1_PSD_OFF.nmap
10/07/2003  08:14p             1,350 SynScan-2-192.168.20.1_PSD_OFF.xml
10/07/2003  08:23p               666 SynScan-3-192.168.20.1_PSD_OFF.gnmap
10/07/2003  08:23p               569 SynScan-3-192.168.20.1_PSD_OFF.nmap
10/07/2003  08:23p             1,350 SynScan-3-192.168.20.1_PSD_OFF.xml
10/07/2003  08:33p               666 SynScan-4-192.168.20.1_PSD_OFF.gnmap
10/07/2003  08:33p               569 SynScan-4-192.168.20.1_PSD_OFF.nmap
10/07/2003  08:33p             1,350 SynScan-4-192.168.20.1_PSD_OFF.xml
10/07/2003  08:42p               690 SynScan-5-192.168.20.1_PSD_OFF.gnmap
10/07/2003  08:42p               618 SynScan-5-192.168.20.1_PSD_OFF.nmap
10/07/2003  08:42p             1,466 SynScan-5-192.168.20.1_PSD_OFF.xml
10/07/2003  08:52p               690 SynScan-6-192.168.20.1_PSD_OFF.gnmap
10/07/2003  08:52p               618 SynScan-6-192.168.20.1_PSD_OFF.nmap
10/07/2003  08:52p             1,466 SynScan-6-192.168.20.1_PSD_OFF.xml
10/07/2003  09:01p               691 SynScan-7-192.168.20.1_PSD_OFF.gnmap
10/07/2003  09:01p               619 SynScan-7-192.168.20.1_PSD_OFF.nmap
10/07/2003  09:01p             1,468 SynScan-7-192.168.20.1_PSD_OFF.xml
              23 File(s)         20,188 bytes

 Directory of E:\GSNA\Project\portscan\VIII.L\192.168.20.1_PSD_OFF_UDP_Scan

13/07/2003  07:00p    <DIR>          .
13/07/2003  07:00p    <DIR>          ..
12/07/2003  07:51p         1,352,334 UDPScan-1-192.168.20.1_PSD_OFF.gnmap
12/07/2003  07:51p         3,162,556 UDPScan-1-192.168.20.1_PSD_OFF.nmap
12/07/2003  07:51p         4,367,253 UDPScan-1-192.168.20.1_PSD_OFF.xml
12/07/2003  08:36p               106 UDPScan-192.168.20.1_PSD_OFF-time.log
12/07/2003  08:36p             1,632 UDPScan-192.168.20.1_PSD_OFF.md5
12/07/2003  07:59p               588 UDPScan-2-192.168.20.1_PSD_OFF.gnmap
12/07/2003  07:59p               388 UDPScan-2-192.168.20.1_PSD_OFF.nmap
12/07/2003  07:59p             1,114 UDPScan-2-192.168.20.1_PSD_OFF.xml
```

```
12/07/2003  08:06p               588 UDPScan -3-192.168.20.1_PSD_OFF.gnmap
12/07/2003  08:06p               388 UDPScan -3-192.168.20.1_PSD_OF F.nmap
12/07/2003  08:06p             1,114 UDPScan -3-192.168.20.1_PSD_OFF.xml
12/07/2003  08:14p               588 UDPScan -4-192.168.20.1_PSD_OFF.gnmap
12/07/2003  08:14p               388 UDPScan -4-192.168.20.1_PSD_OFF.nmap
12/07/2003  08:14p             1,114 UDPScan -4-192.168.20.1_PSD_OFF.xml
12/07/2003  08:21p               588 UDPScan -5-192.168.20.1_PSD_OFF.gnmap
12/07/2003  08:21p               388 UDPScan -5-192.168.20.1_PSD_OFF.nmap
12/07/2003  08:21p             1,114 UDPScan -5-192.168.20.1_PSD_OFF.xml
12/07/2003  08:29p               588 UDPScan -6-192.168.20.1_PSD_OFF.gnmap
12/07/2003  08:29p               388 UDPScan -6-192.168.20.1_PSD_OFF.nmap
12/07/2003  08:29p             1,114 UDPScan -6-192.168.20.1_PSD_OFF.xml
12/07/2003  08:36p               589 UDPScan -7-192.168.20.1_PSD_OFF.gnmap
12/07/2003  08:36p               389 UDPScan -7-192.168.20.1_PSD_OFF.nmap
12/07/2003  08:36p             1,116 UDPScan -7-192.168.20.1_PSD_OFF.xml
              23 File(s)      8,896,425 byt es

 Directory of E: \GSNA\Project\portscan\VIII.L\192.168.20.1_PSD_OFF_Xmas_Scan

13/07/2003  08:3 2p     <DIR>          .
13/07/2003  08:32p      <DIR>          ..
11/07/2003  04:04a               361 XmasScan -1-192.168.20.1_PSD_OFF.gnmap
11/07/2003  04 :04a              310 XmasScan -1-192.168.20.1_PSD_OFF.nmap
11/07/2003  04:04a               883 XmasScan -1-192.168.20.1_PSD_OFF. xml
11/07/2003  05:21a               108 XmasScan -192.168.20.1_PSD_OFF -time.log
11/07/2003  05:21a             1,655 Xm asScan-192.168.20.1_PSD_OFF.md5
11/07/2003  04:12a               589 XmasScan -2-192.168.20.1_PSD_OFF.gnmap
11/07/2003  04:12a               389 XmasScan -2-192.168.20.1_PSD_OFF.nmap
11/07/2003  04:12a             1,117 XmasScan -2-192.168.20.1_PSD_OFF. xml
11/07/2003  04:20a               589 XmasScan -3-192.168.20.1_PSD_OFF.gnmap
11/07/2003  04:20a               389 XmasScan -3-192.168.20.1_PSD_OFF.nmap
11/07/2003  04:20a             1,117 XmasScan -3-192.168.20.1_PSD_OFF.xml
11/07/2003  04:35a            93,387 XmasScan -4-192.168.20.1_PSD_OFF.gnmap
11/07/2003  04:35a           211,606 XmasScan -4-192.168.20.1_PSD_OFF.nmap
11/07/2003  04:35a           332,629 XmasScan -4-192.168.20.1_PSD_OFF. xml
11/07/2003  04:51a            93,387 XmasScan -5-192.168.20.1_PSD_OFF.gnmap
11/07/2003  04:51a           211,606 XmasScan -5-192.168.20.1_PSD_OFF.nmap
11/07/2003  04:51a           332,629 XmasScan -5-192.168.20.1_PSD_OFF. xml
11/07/2003  05:06a            93,387 XmasScan -6-192.168.20.1_PSD_OFF.gnmap
11/07/2003  05:06a           211,606 XmasScan -6-192.168.20.1_PSD_OFF.nmap
11/07/2003  05:06a           332,629 XmasScan -6-192.168.20.1_PSD_OFF. xml
11/07/2003  05:21a            93,388 XmasScan -7-192.168.20.1_PSD_OFF.gnmap
11/07/2003  05:21a           211,607 XmasScan -7-192.168.20.1_PSD_OFF.nmap
11/07/2003  05:21a           332,631 XmasScan -7-192.168.20.1_PSD_OFF. xml
              23 File(s)      2,5 57,999 bytes

    Total Files Listed:
          137 Fil e(s)     13,222,365 bytes
           20 D ir(s)  18,642,722,816 bytes free
```

7.5 Appendix 4. N-Stealth Report

N-Stealth Report

N-Stealth report for lister (127.0.0.1)
Date: 12/07/2003 3:50:37 PM

Scan Rule: Normal

127.0.0.1

Host name: **lister**
Port: 80
Server: Apache/2.0.45 (Unix) mod_ssl/2.0.45 OpenSSL/0.9.7a mod_fastcgi/mod_fastcgi-SNAP-0212082101

Server may have HTTP vulnerabilitie s/exposures. 6 item(s)

?WP-START-VER Test

Risk Level: Medium
Location: http://127.0.0.1/?wp-start-ver

Common Netscape Enterprise Vulnerability/Exposure - False positives are known for this item.

?WP-STOP-VER Test

Risk Level: Medium
Location: http://127.0.0.1/?wp-stop-ver

Common Netscape Enterprise Vulnerability/Exposure - False positives are known for this item.

?WP-UNCHECKOUT Test

Risk Level: Medium
Location: http://127.0.0.1/?wp-uncheckout

Common Netscape Enterprise Vulne rability/Exposure - False positives are known for this item.

?WP-USR-PROP Test

Risk Level: Medium
Location: http://127.0.0.1/?wp-usr-prop

Common Netscape Enterprise Vulnerability/Exposure - False positives are known for this item.

INDEX Test

Risk Level: Medium
Location: http://127.0.0.1/index.cgi

Common Vulnerability/Exposure.

UPDATE Test

Risk Level: Medium
Location: http://127.0.0.1/update.pl

Common Vulnerability/Exposure.

N-Stealth 3.5 Build 55

7.6 Appendix 5.

Screen Captures of the ISS Internet Scanner Report. Attempts to import the RTF formatted document failed.

Figure 7-1, ISS Internet Scanner Report.

Network Host Assessment Report **Sorted by IP Address** **07/12/2003**

This report lists the hosts discovered by Internet Scanner after scanning the network, and for each host, identifies network services, user details, banner details, and vulnerabilities.
Intended audience: This report is intended for security technicians (Security Administrators, Network Administrators, Workstation Support Engineers, or Helpdesk Support Engineers).
Purpose: For each host, the report provides the IP address, the DNS Name, the operating system type, and the status of the host (reachable or unreachable). The report also provides information about services, users, and banners identified by Internet Scanner.
Related reports: For a brief description of the hosts identified by Internet Scanner after scanning the network, see the Line Management/Host Assessment reports.

Vulnerability Severity: H High M Medium L Low

Session Information

Session Name:	Sim Coat Plastics Astaro 4.008 FW- Corp Lan	**File Name:**	Sim Coat Plastics Astaro 4.008 FW- Corp Lan_20030712A
Policy:	LS Unix Web Server	**Key:**	XXXXXXXXXXXXXXXXXXXXXXXX
Hosts Scanned:	1	**Hosts Active:**	1
Scan Start:	7/12/2003 12:29:03PM	**Scan End:**	7/12/2003 1:05:52PM
Comment:	From Corp Lan Host		

IP Address {DNS Name}	Operating System	Status
192.168.20.1 {star.scp.net}	(Unknown OS)	Reachable

Service Details:

Service Name	*Short Description*	*Port #*	*Type*
domain	domain	53	TCP
httpd	httpd	8,080	TCP
Smtp	Smtp	25	TCP

Others

Additional Information *More Information*

IP Address {DNS Name}	Operating System	Status

Vulnerability Details:

M **smtpexpn: SMTP EXPN command (CAN-1999-0531)**

Simple Mail Transfer Protocol (SMTP)-compliant applications, such as the Sendmail program EXPN, could allow an attacker to determine if an account exists on a system. Such information could provide an attacker significant assistance in executing a brute force attack on user accounts. EXPN provides additional information concerning users on the system, such as if particular users exist and users' full names. This information could also assist an attacker in further attacks.

Remedy:

If you are running Sendmail, add the line 'Opnoexpn' to your Sendmail configuration file, usually located in /etc/sendmail.cf. For other mail servers, contact your vendor for information on how to disable the expand command.

--AND--

Upgrade to the latest version of Sendmail (8.11.4 or later), available from the Sendmail Consortium Web site. See References.

--OR--

Apply the appropriate patch for your system, available from the Sendmail Consortium FTP site. See References.

M **smtprelay: Third-party mail relaying can be used to obfuscate the origin of emails (CAN-19-**

Some SMTP servers support third-party or %style mail relaying. Third-party mail relaying occurs when a mail server processes a mail message where neither the sender nor the recipient is local to the server's mail domain.

While third party relaying has some legitimate purposes, such as allowing mail messages to be routed around known mail problems, email hijackers (or spammers) primarily use it to obscure their identity while sending large amounts of junk mail.

Remedy:

Reconfigure your SMTP server to enforce that all mail messages must either originate or terminate locally (on the mail host). Information on how to secure your mail system against relaying is available from the "How Can I Fix the Problem?" document listed in the references.

L **bindvrs: BIND servers can be remotely queried for their version numbers**

BIND (Berkeley Internet Name Domain) servers support the ability to be remotely queried for their version numbers. An attacker could use this feature to query computers for vulnerable versions of BIND. This information could be useful to an attacker in performing an attack.

Remedy:

Disable the BIND version query feature. Refer to the BIND documentation for information on this procedure.

L **EhloCheck: SMTP daemon supports EHLO (CAN-1999-0531)**

SMTP daemons that support Extended HELO (EHLO) can release information that could be useful to an attacker in performing an attack. Attackers have been known to use the EHLO command to determine configuration information on SMTP daemons.

Remedy:

SMTP as defined in RFC 2821 (see References) requires EHLO. Some SMTP implementations allow you to disable EHLO, but this capability is neither required nor consistent across products.

If you are uncomfortable with the information that the Extended SMTP features can reveal, you may choose to disable EHLO on your mail server (if applicable), or switch to a mail server that allows EHLO to be disabled. Consult your mail server documentation or contact your vendor for information on whether it is possible to modify your mail server configuration to disable EHLO.

L **SMTPforgery: SMTP server allows fake hostnames in HELO**

The SMTP server was found to accept any hostname issued to it in the HELO command. This lack of authorization could allow users to more easily forge mail from your mail server.

Remedy:

Upgrade your Mail Transfer Agent (MTA) to a version that supports more rigorous validation of hostnames. It may be possible to configure your mail server to do this, therefore, refer to your documentation.