AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report

Certificate Number: 2002/22

Secure Computing Corporation

Gauntlet Firewall V6.0

Issue 1.0
April 2002

Issued by: -

Defence Signals Directorate - Australasian Certification Authority

CERTIFICATION STATEMENT

Gauntlet Firewall version 6.0 (herein referred to as Gauntlet) is a product developed by Network Associates Incorporated (the product is now owned by Secure Computing Corporation) which controls access between an internal trusted network and an external untrusted network. Gauntlet offers application -level security services that regulate communications in both directions in compliance with established organisational security policies.

This report describes the evaluation findings of the Gauntlet product to the Common Criteria (CC) Evaluation Assurance Level (EAL) 4, and includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product to meet its CC EAL 4 level of assurance. It concludes that the product has met the target Assurance Level of CC EAL 4.

Originator _____

Chris Pennisi
Certifier
Defence Signals Directorate

Approval _____

Doug Stuart
Manager, Australasian Information Security Evaluation Program
Defence Signals Directorate

Authorisation _____

Lynwen Connick
Australasian Certification Authority
Defence Signals Directorate

TABLE OF CONTENTS

Chapter 1 Introduction

Intended Audience

1.1 This certification report states the outcome of the IT security evaluation of the Gauntlet Firewall Version 6.0 (hereafter referred to as Gauntlet) developed by Network Associates Inc. It is intended to assist potential users when judging the suitability of the product for their particular requirements, and to advise security administrators on ensuring the product is used in a secure manner.

Identification of Target of Evaluation

1.2 The version of Gauntlet evaluated was **version 6.0**, developed by Network Associates Incorporated (NAI), with several patches applied. Details of these patches can be found in Appendix C of this report.

1.3 The security functionality offered by Gauntlet is implemented entirely in software.

1.4 The evaluated component of Gauntlet excludes the IPSec Virtual Private Network (VPN) functionality and only includes a subset of the available proxies.

1.5 The evaluated configuration of Gauntlet requires the certified version of Solaris 8 operating system, including Adminsuite version 3.0.1. For further details on the evaluated configuration of Solaris 8, refer to the Solaris 8 Security Target and Certification Report available at the Communications-Electronics Security Group (CESG) web site, http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/index.asp.

1.6 For further details of the evaluated components of Gauntlet, including details of how to identify the evaluated version, refer to Appendix C.

Evaluation

1.7 The evaluation was carried out in accordance with the rules of the Australasian Information Security Evaluation Program (AISEP) which is described in Evaluation Memorandum 1 and Evaluation Memorandum 2 (refs [1], [2] respectively). In addition, the conditions outlined in the Common Criteria Recognition Arrangement (ref [18]) were also upheld during the evaluation and certification of this product.

1.8 The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation (TOE), Gauntlet Firewall version 6.0, in meeting its Security Target (ref [9]). The criteria against which the TOE is judged are expressed in the Common

Criteria Part 3 (ref [5]). This describes how the degree of assurance can be expressed in terms of the levels EAL1 to EAL7. The methodology used is described in the Common Evaluation Methodology (CEM) and Evaluation Memoranda 4 and 5 (refs [6,7,8]).

1.9 The evaluation was sponsored, and the product developed, by United States based Network Associates Incorporated (NAI). During the latter stages of the evaluation, Secure Computing Corporation (SCC) acquired the Gauntlet product from NAI and assumed sponsorship of the evaluation.

1.10 A listing of the documentation used during the evaluation of this product is included or referenced in Appendix A of this Report.

1.11 The evaluation was performed by CSC Australia, between July 2000 and February 2002, and was monitored by the Certification Group on behalf of the Australasian Certification Authority (ACA). At the end of the evaluation, an Evaluation Technical Report (ETR) (ref [10]) describing the evaluation and its results was presented to the ACA. The Certification Report was then produced, based on the contents of the ETR and the Certification Group's knowledge of the evaluation.

1.12 The Security Target (ref [9]) claimed an assurance level for the product of CC EAL4.

General Points

1.13 Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher evaluation levels) that exploitable vulnerabilities remain undiscovered.

1.14 EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained through an informal model of the TOE security policy.

1.15 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

1.16 EAL4 also provides assurance through the use of development environment controls, TOE configuration management including automation and evidence of secure delivery procedures.

1.17 Gauntlet should only be used within the defined TOE security environment in accordance with the specified assumptions, as explained in section 3.1 of the ST (ref [9]). Additionally, the security requirements on the IT and non-IT environment must be fully understood in order to determine the suitability of the product in its assumed operational environment, as explained in section 5.2 of (ref [9]). Users should be aware of the certifiers' recommendations as given in Chapter 4 of this report.

1.18 Ultimately, it is the responsibility of the user to ensure that Gauntlet meets their requirements. For this reason, it is ***strongly*** recommended that a prospective user of the product obtain a copy of the Security Target (ref [9]) from the product vendor, and reads this Certification Report thoroughly prior to deciding whether to purchase the product.

Scope of the Evaluation

1.19 The scope of the evaluation is limited to those claims made in the Security Target. All security related claims in the Security Target were evaluated by CSC Australia. A summary of the Security Target is provided in Annex B of this Certification Report.

1.20 Potential users are encouraged to contact their national security authority for further advice on the suitability of this product when used in conjunction with other evaluated products to protect national security and non-national security information.

Chapter 2 Security Overview of Gauntlet

2.1 Potential users are strongly recommended to read the Security Target (ref [9]). This explains the security functionality of the Gauntlet product in greater detail, as well as the intended environment and method of use for the product. A summary of the Security Target can be found in Appendix B. A full copy of the Security Target can be obtained from the sponsor of the evaluation.

Functionality of the TOE

2.2 This section provides a summary of the operational role of the TOE together with the security functions that it is designed to perform.

2.3 The TOE is a software based application gateway and traffic -filter firewall that supports only those services specifically configured by the firewall administrator, and only those that can be implemented securely. Gauntlet offers application-level security services that regulate communications in both directions.

2.4 The TOE provides secure access and inter-network communications between private, trusted networks (termed "internal") and public, untrusted networks such as the Internet (termed "external"), or between organisations within a private network.

2.5 The TOE provides:

a) Control over access to services

b) Prevention of the flow of IP packets for which no service in either direction is permitted

c) Mediation of IP packets corresponding to services for which proxies are provided

d) Forwarding of just those IP packets corresponding to un-proxied services that have been authorised by administrators for direct passage through the firewall.

2.6 The TOE relies on security functionality provided by the Solaris 8 operating system. The Solaris 8 operating system provided audit functionality to record and review security related events and identification and authentication mechanisms to ensure only authorised personnel can access the TOE.

Architecture of the TOE

2.7 This section provides a summary of the architectural design of the TOE together with the security functions it is designed to perform.

2.8 The Gauntlet firewall system is a software application that is made up of a number of modules that provide application-level security services, IP screening facility, and the UNIX operating system management utilities.

2.9 Gauntlet comprises the following architectural components:

a) **GFW Kernel Module.** The GFW module comprises a module to the kernel's TCP/IP communications software driver ensuring that all packets are diverted from the operating system before reaching the TCP/IP stack to the Gauntlet driver.

b) **GFW Kernel Driver.** The GFW kernel driver comprises a packet-screening driver that holds packet-screening rules, IP spoofing rules and NAT rules and applies them to the packets it receives from the GFW kernel module driver. The driver ensures that certain IP and ICMP packets are blocked and audit records are generated for various TCP/IP errors and unauthorised events that would normally go unreported (source routed IP packets, ICMP redirect packets, and IP packets destined for unserved TCP ports.)

c) **Initialisation Module.** The initialisation module runs automatically at boot time and is responsible for starting the other user mode processes that run. Under Solaris, this component is implemented as a set of startup scripts called during the Solaris boot process.

d) **Proxies.** The proxies module comprises a set of individual proxy programs each of which mediates a particular type of service (i.e., high level protocol), although in some cases the proxy is 'generic' and can be used with different types of service. The programs are based on a common set of primitive routines (the proxy library) that provide a standard process environment for each proxy to run in, and factor out service (i.e., protocol) independent security checks. Each proxy program uses these primitive routines to initialise itself to listen (via a 'socket') on the appropriate TCP or UDP port for the service it is mediating, to determine from Gauntlet's databases what security rules apply to that service, and to scan the rules to conduct security checks.

e) **Auth Server.** The auth server stores user authentication credentials and other parameters for authorised end-users of authenticated services on host systems in the connected networks, and manages the challenge/response dialogue for each authenticated service based on these parameters.

f) **Log Service.** The log service comprises a server program and programs that are

used by the administration GUI to provide summary and exception reports based on audit records. Audit records are generated by the GFW kernel driver, the initialisation module, auth server, the proxy module and the administration GUI. The records are collected by the log service's server program for storage in a central logging location. The Gauntlet log service includes a space monitor program, which can be configured to write a final message and shut down the firewall when the disk storage space for logging files becomes too small, thus preventing the loss of logging of auditable events.

g) **Administration GUI.** The administration GUI comprises a Java based client program and a server. Its main purpose is to provide a user interface to maintain the central *netperm-table*, packet screening rules, IP spoofing rules, NAT rules, and Gauntlet configuration table (*gauntlet.conf*) database files that record all administration, configuration, and security rules information.

h) **Content Scanning.** The content scanning component provides scanning for:

- Removal of Java and Active X from HTTP pages

i) **Gauntlet Databases.** Gauntlet has four main databases: the netperm-table, the Gauntlet configuration file, parameters for the Gauntlet driver, and the authentication database. The packet screening rules are in the Gauntlet configuration file. A number of other parameter files are used to specify security-relevant parameters: e.g., filtering criteria for the audit functions (both routine and exception reporting).

Security Policy

2.10 The following security policies are enforced by Gauntlet:

a) Security management policy, defining the administrators role and interaction with the TOE.

b) Identification and authentication policy, defining access rights and privileges to protect assets from loss or disclosure by specifying applicable rules for users and management.

c) User data protection policy, specifying requirements for the protection of data by the TSFs for both authenticated and unauthenticated services.

d) Protection of the TSFs policy, defining the requirements that enable the resources being controlled by the TSF to be protected from alteration or tampering.

e) TOE session establishment policy, defining the capability of the TOE to restrict session establishment.

f) Security audit policy, defining the audit generation and review capabilities of the TOE.

2.11 The security policy model is summarised in chapter 3.3 of the ETR (ref [10]). Alternatively, the security policy model (ref [16]) may be requested from the developer.

2.12 In order for the TOE to comply with the security policy model, the Gauntlet product should only be used within the defined TOE security environment in accordance with the secure usage assumptions, as explained in section 3.1 of the Security Target (ref [9]).

Documentation

2.13 Before using the product, administrators and security managers should ensure that they are aware of, and fully understand the relevant operational documentation. In addition, they should ensure they read Chapter 4 of this document, and associated administration and user manuals contained on the product CD-ROM (refs [11] - 14]). Finally, administrators should download a copy of the EAL4 Addendum (ref [15]) from the SCC web site, http://www.securecomputing.com/gauntlet /gauntlet_patch.cfm.

Chapter 3 Evaluation Findings

Introduction

3.1 The evaluation of Gauntlet followed a course consistent with the generic evaluation work program described in the ITSEM (ref [17]) and the CEM (ref [6]), with work packages structured around the evaluator actions described in the Common Criteria (CC) Part 3 (ref [5]). The results of this work are reported in the ETR (ref [10]) under the CC headings. This report summarises the general results, followed by the findings in relation to the security functionality claimed in the Security Target (ref [9]).

Security Target Evaluation

3.2. The purpose of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

TOE Description (ASE_DES.1)

3.3. The TOE Description adequately described the product type, and the scope and boundaries of the TOE in general terms both in a physical and a logical way.

3.4. The above results have enabled the certifiers to conclude that the ST has met the requirements for the TOE Description, and consider it suitable to be used (in part) as a basis for the evaluation.

Security Environment (ASE_ENV.1)

3.5. The statement of the TOE security environment adequately identified and explained the assumptions about the intended usage of the TOE (and its environment), and the known threats to the protected assets of the TOE (and its environment). There were no explicit organisational security policies with which the TOE had to comply with.

3.6. The above results have enabled the certifiers to conclude that the ST has met the requirements for the Security Environment, and consider it suitable to be used (in part) as a basis for the evaluation.

ST introduction (ASE_INT.1)

3.7. The ST introduction identified and adequately described the ST and the TOE. It contained an ST overview in narrative form, and contained a CC conformance claim to meet the predefined assurance level of EAL4.

3.8. The above results have enabled the certifiers to conclude that the ST has met the requirements for the ST introduction, and consider it suitable to be used (in part) as a basis for the evaluation.

Security Objectives (ASE_OBJ.1)

3.9. The statement of the TOE and environmental security objectives were adequately defined, and were clearly traceable back to the identified threats countered by the TOE, and the assumptions on the TOE and its environment. The security objectives rationale demonstrated that the security objectives were suitable to counter the identified threats and cover the identified assumptions.

3.10. The above results have enabled the certifiers to conclude that the ST has met the requirements for the Security Objectives, and consider it suitable to be used (in part) as a basis for the evaluation.

Protection Profile (PP) Claims (ASE_PPC.1)

3.11. The ST did not claim conformance to any PPs.

IT Security Requirements (ASE_REQ.1)

3.12. The statement of the TOE Security Functional Requirements (SFRs) correctly identified the SFRs drawn from CC Part 2 (ref [4]), and the TOE Security Assurance Requirements (SARs) for EAL4 from CC Part 3 (ref [5]). The justification for using the pre-defined EAL4 assurance package was sufficient.

3.13. Security requirements on the IT environment were identified. All operations on the IT security requirements were completed, and the relevant dependencies were satisfied. The security requirements rationale demonstrated that the IT security requirements were suitable to meet the security objectives. It also demonstrated that the set of IT security requirements together forms a mutually supportive and internally consistent whole.

3.14. The above results have enabled the certifiers to conclude that the ST has met the requirements for the IT Security Requirements, and consider it suitable to be used (in part) as a basis for the evaluation.

Explicitly stated IT Security Requirements (ASE_SRE.1)

3.15. The ST did not contain any explicitly stated IT security requirements.

TOE Summary Specification (ASE_TSS.1)

3.16. The TOE summary specification (TSS) adequately described the IT security functions and the assurance measures of the TOE. The TSS traced and clearly mapped all IT security functions to the TOE security functional requirements demonstrating that all TOE security functions contribute to the satisfaction of at least one TOE security functional requirement.

3.17. The IT security functions were informally specified to an appropriate level of detail. Security mechanisms were easily traced back to the relevant TOE security functions.

3.18. The TOE summary specification rationale demonstrated that the IT security functions were suitable to meet the TOE security functional requirements, and that the

combination of IT security functions work together to also satisfy the TOE security functional requirements. The rationale also demonstrated, aided by a mapping, that the assurance measures met the assurance requirements for EAL4.

3.19. The TOE summary specification stated that there were no IT security functions that are realised by a probabilistic or permutational mechanism.

3.20. The above results have enabled the certifiers to conclude that the ST has met the requirements for the TOE Summary Specification, and consider it suitable to be used (in part) as a basis for the evaluation.

ST Evaluation Result

3.21. The certifiers consider that the above results have demonstrated that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the evaluation.

Common Criteria EAL4 Security Assurance Requirements

3.22. EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained through an informal model of the TOE security policy.

3.23. The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

3.24. EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures. The results of this evaluation are discussed below.

Configuration Management (ACM)

3.25. Configuration management is one method or means for establishing that the functional requirements and specifications are realised in the implementation of the TOE. Configuration management meets these objectives by requiring discipline and control in the processes of refinement and modification of the TOE and the related information. Configuration management systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorised.

Configuration Management (CM) Capabilities (ACM_CAP.4)

3.26. The TOE reference was assessed to be unique to each version of the TOE. In addition, the TOE was correctly labelled with its reference.

3.27. The CM documentation included a configuration list, CM plan, and an acceptance plan, and adequately described the method used to uniquely identify the configuration items. The configuration list correctly described the configuration items of the TOE. The CM plan adequately described how the CM system was being used to uniquely identify the configuration items.

3.28. The CM system was demonstrated to operate in accordance with the CM plan, and that all configuration items were being effectively maintained under the CM system. The CM system provided adequate measures to ensure that only authorised changes are made to the configuration items. The CM system appropriately supported the generation of the TOE.

3.29. An acceptance plan was also provided that adequately described the procedures used to accept modified or newly created configuration items as part of the TOE.

3.30. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in July 2001.

3.31. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Configuration Management Capabilities assurance component for EAL4.

Configuration Management Automation (ACM_AUT.1)

3.32. The CM system provided an adequate automated means by which only authorised changes were made to the TOE implementation representation (i.e. the source code), and an automated means to support generation of the TOE.

3.33. The CM plan adequately described the automated tools and how they are used in the CM system.

3.34. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in July 2001.

3.35. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Configuration Management Automation assurance component for EAL4.

Configuration Management Scope (ACM_SCP.2)

3.36. The CM documentation correctly showed that the CM system tracks the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

3.37. The CM documentation adequately described how the configuration items were being tracked by the CM system.

3.38. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in July 2001.

3.39. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Configuration Management Scope assurance component for EAL4.

Delivery and Operation (ADO)

3.40. This aspect of the evaluation examines the requirements for the measures, procedures, and standards concerned with secure delivery, installation and operational use of the TOE, ensuring that the security protection offered by the TOE is not compromised during transfer, installation, start-up and operation.

Delivery (ADO_DEL.2)

3.41. The delivery documentation adequately described all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

3.42. The procedures and technical measures for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site, were adequately described. The delivery documentation also adequately described how the various procedures allowed for the detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

3.43. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in July 2001.

3.44. However, during the certification period the certifiers received letters from the sponsor and the evaluators (ref [19], [20] respectively) indicating that there had been a change in the delivery procedures as a result of the acquisition of Gauntlet by SCC. The certifiers concluded that these changes do not invalidate the evaluator's findings.

3.45. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Delivery assurance component for EAL4.

Installation, Generation and Start-Up (ADO_IGS.1)

3.46. The operational documentation adequately described the steps necessary for secure installation, generation, and start-up of the TOE.

3.47. The evaluators confirmed that the installation and generation of the TOE was achieved through the application of the documented procedures.

3.48. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Installation, Generation and Start-Up assurance component for EAL4.

Development (ADV)

3.49. This aspect of the evaluation examines the requirements for the stepwise refinement of the TSF from the TOE summary specification in the ST, down to the actual implementation. Each of the resulting TSF representations provides information to help determine whether the functional requirements of the TOE have been satisfied.

Functional Specification (ADV_FSP.2)

3.50. The functional specification informally described the TSF and its external interfaces, including a description on the purpose and method of use of all external TSF interfaces, while also providing complete details of all effects, exceptions and error messages.

3.51. The functional specification was found to be internally consistent and to completely represent the TSF. This was supported by a rationale justifying that the TSF did in fact completely represent the TSF.

3.52. Furthermore, the functional specification was determined to be an accurate and complete instantiation of the TOE security functional requirements.

3.53. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Functional Specification assurance component for EAL4.

High-Level Design (ADV_HLD.2)

3.54. The presentation of the High-Level Design was informal and found to be internally consistent. It adequately described the structure of the TOE in terms of sub-systems, and the security functionality provided by each sub-system of the TSF.

3.55. The High-Level Design identified all underlying hardware, firmware and software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware or software.

3.56. The High-Level Design identified all interfaces to the sub-systems of the TSF, together with an identification of the interfaces that are externally visible. The purpose and method of use of all these interfaces were adequately described, including details of the effects, exceptions and error messages. Finally, the separation of the TOE into TSP-enforcing and other sub-systems was correctly described.

3.57. Furthermore, the High-Level Design was determined to be an accurate and complete instantiation of the TOE security functional requirements.

3.58. As a result of the above determinations, the certifiers conclude that the TOE fully meets the High-Level Design assurance component for EAL4.

Low-Level Design (ADV_LLD.1)

3.59. The presentation of the Low-Level Design was informal and found to be internally consistent. The Low-Level Design adequately described the TSF in terms of modules,

and the purpose of each of these modules. The interrelationships between the modules in terms of provided security functionality and dependencies on other modules were also adequately described.

3.60. The Low-Level Design described how each TSP-enforcing function was provided, and identified all interfaces to the modules of the TSF, including all interfaces that are externally visible. The purpose and method of use of all these interfaces were adequately described, including details of the effects, exceptions and error messages. Finally, the separation of the TOE into TSP-enforcing and other modules was correctly described.

3.61. Furthermore, the Low-Level Design was determined to be an accurate and complete instantiation of the TOE security functional requirements.

3.62. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Low-Level Design assurance component for EAL4.

Implementation (ADV_IMP.1)

3.63. The developer provided the entire source code for the implementation representation. A subset of the implementation representation corresponding to approximately to 45% of the TSF was used by the evaluators.

3.64. The implementation representation was found to unambiguously define the TSF to a level of detail such that the TSF could be generated without any further design decisions. In addition, the implementation representation was confirmed to be internally consistent.

3.65. Furthermore, the implementation representation was determined to be an accurate and complete instantiation of the TOE security functional requirements.

3.66. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Implementation assurance component for EAL4.

Representation Correspondence (ADV_RCR.1)

3.67. An analysis of the correspondence between all adjacent pairs of the TSF representation was provided. This analysis demonstrated that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation, which was the implementation.

3.68. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Representation Correspondence assurance component for EAL4.

Security Policy Model (ADV_SPM.1)

3.69. The developer provided a TOE Security Policy (TSP) model that was presented informally, and described the rules and characteristics of all the relevant security policies. A rationale was included that appropriately demonstrated that it was complete

and consistent with all of the identified security policies.

3.70. The developer also demonstrated that the correspondence between TSP model and the functional specification showed that all of the security functions in the functional specification were consistent and complete with respect to the TSP model

3.71. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Security Policy Model assurance component for EAL4.

Guidance Documents (AGD)

3.72. This aspect of the evaluation examines the requirements directed at the understandability, coverage and completeness of the operational documentation provided by the developer. This documentation, which provides two categories of information, for users and administrators, is an important factor in the secure operation of the TOE.

Administrator Guidance (AGD_ADM.1)

3.73. The administrator guidance clearly described the administrative functions and interfaces, instructions on how to administer the TOE securely, all assumptions regarding user behaviour that are relevant to the secure operation of the TOE, all security parameters under the control of the administrator, and each type of security-relevant event relative to the administrative functions being performed, including changing the security characteristics of entities under control of the TSF.

3.74. The guidance also contained appropriate warnings about functions and privileges that need to be controlled in a secure environment, and indicated secure values if applicable.

3.75. The administrator guidance described all security requirements for the IT environment that were relevant to an administrator, and was consistent with all other documentation supplied for the evaluation.

3.76. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Administrator Guidance assurance component for EAL4.

User Guidance (AGD_USR.1)

3.77. The user guidance clearly described the functions and interfaces available to the non-administrative users of the TOE, and the use of user-accessible security functions provided by the TOE. There were no appropriate warnings about user -accessible security functions and privileges that should be controlled in a secure processing environment that needed to be described.

3.78. All user responsibilities necessary for the secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of the TOE security environment, were clearly presented.

3.79. The user guidance described all security requirements for the IT environment that were relevant to a user, and was consistent with all other documentation supplied for the evaluation.

3.80. It was noted that user interaction with the TOE was minimal, only requiring an understanding of the proxy-user authentication process. However, all of the above requirements were upheld.

3.81. As a result of the above determinations, the certifiers conclude that the TOE fully meets the User Guidance assurance component for EAL4.

Life-Cycle Support (ALC)

3.82. This aspect of the evaluation examines the requirements for assurance through the adoption of a well-defined life-cycle model for all the steps of the TOE development, correct use of tools and techniques, and the security measures used to protect the development environment.

Development Security (ALC_DVS.1)

3.83. The development security documentation adequately described all the physical, procedural, personnel, and other security measures that were necessary to protect the confidentiality and the integrity of the TOE design and implementation in its development environment. It also provided evidence that these security measures were being followed during the development and maintenance phases of the TOE.

3.84. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in July 2001.

3.85. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Development Security assurance component for EAL4.

Life-Cycle Definition (ALC_LCD.1)

3.86. The life-cycle definition documentation adequately described the model used to develop and maintain the TOE, and how the model provides the necessary control measures used during these phases.

3.87. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in July 2001.

3.88. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Life-Cycle Definition assurance component for EAL4.

Tools and Techniques (ALC_TAT.1)

3.89. All development tools use during the implementation phase were determined to be well defined. The documentation associated with these tools unambiguously defined the meaning of all statements, including the implementation-dependent options, used in the

implementation.

3.90. The above determinations were also supported by the results of a site visit to the development environment conducted by the evaluators in July 2001.

3.91. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Tools and Techniques assurance component for EAL4.

Tests (ATE)

3.92. Testing helps to establish that the TOE security functional requirements are met. Testing provides assurance that the TOE satisfies at least the TOE security functional requirements, although it cannot establish that the TOE does no more than what was specified. Testing at this level of assurance is also directed towards the internal structure of the TSF, such as the testing of subsystems (identified in the High-Level Design) against their specification.

Coverage (ATE_COV.2)

3.93. The test coverage analysis adequately demonstrated the correspondence between the tests identified in the test documentation and the TSF described in the functional specification, and that the coverage was complete.

3.94. The developer's functional testing covered all TSFs specified in the functional specification.

3.95. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Coverage assurance component for EAL4.

Depth (ATE_DPT.1)

3.96. The depth analysis adequately demonstrated that the tests identified in the test documentation were sufficient to demonstrate that the TSF operates in accordance with its high-level design.

3.97. The developer's functional testing covered all sub-systems and sub-system interfaces specified in the high-level design of the TSF.

3.98. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Depth assurance component for EAL4.

Functional Testing (ATE_FUN.1)

3.99. The provided test documentation consisted of test plans, test procedure descriptions, expected test results and actual test results. The documentation identified the security functions that were tested and the goals of each test. The test procedure descriptions described the scenarios for testing each security function. The scenarios did not require that the tests be ordered in any way.

3.100. The expected test results showed the anticipated outputs from the successful execution of these tests, and the test results demonstrated that each security function behaved as specified.

3.101. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Functional Testing assurance component for EAL4.

Independent Testing (ATE_IND.2)

3.102. Independent testing was conducted to confirm that the TOE operates as specified in the documentation supplied for the evaluation. The configuration of the TOE (and its environment) used during testing was consistent with the evaluated configuration, as stipulated in the ST (ref [9]) and the operational guidance (refs [11] - [15]). In addition, an equivalent set of resources was used that were utilised during the developer functional testing of the TSF.

3.103. A 20% sample of the developer tests was selected to verify the developer's test results. All tests executed by the evaluators from the selected sample of developer tests produced the expected results, consistent with the results produced by the developer's own functional testing.

3.104. The evaluators based their own independent testing on the sample identified above, and extended their testing to investigate the behaviour of the data flow control policy of the TOE. Adhoc testing was also performed where appropriate. All tests were sufficiently documented to enable the tests (and their results) to be reproducible.

3.105. The overall outcome of the developer and evaluator testing effort showed that the TOE security functions have been implemented correctly in the TOE. A summary of the evaluator testing effort for this component can be found in section 5.18 of the ETR (ref [10]).

3.106. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Independent Testing assurance component for EAL4.

Vulnerability Assessment (AVA)

3.107. This aspect of the evaluation examines the requirements directed at the identification of exploitable vulnerabilities. Specifically, it addresses those vulnerabilities introduced in the construction, operation, misuse, or incorrect configuration of the TOE.

Misuse (AVA_MSU.2)

3.108. The guidance documentation appropriately identified all possible modes of operation of the TOE, including operation following failure or operational error, their consequences and implications for maintaining secure operation. The guidance documentation was also determined to be complete, clear, consistent and reasonable.

3.109. The guidance documentation appropriately listed the assumptions about the intended

environment, and all the requirements for external security measures. The developer provided analysis of the guidance documentation demonstrated that it was complete. The evaluators confirmed that this analysis showed that relevant guidance is provided for secure operation in all modes of operation of the TOE.

3.110. The evaluators repeated the installation and configuration procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation, and that all insecure states could be detected using this documentation.

3.111. However, during the certification period the certifiers discovered that the administrative documentation did not clearly explain how to configure the ***http-gw*** web proxy in a secure manner. To resolve the matter, the administrative documentation was updated to provide appropriate guidance. Further information can be found in chapter 4 of this report.

3.112. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Misuse assurance component for EAL4.

Strength of Function (AVA_SOF.1)

3.113. The Security Target did not make a strength of function claim.

3.114. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Misuse assurance component for EAL4.

Vulnerability Analysis (AVA_VLA.2)

3.115. The developer provided a vulnerability analysis searching for ways in which a user can violate the TSP. The documentation showed that none of the identified vulnerabilities were exploitable in the intended environment for the TOE. It also justified that the TOE is resistant to obvious penetration attacks.

3.116. The evaluators performed their own independent vulnerability analysis and conducted penetration testing to ensure that the identified vulnerabilities had been addressed.

3.117. Additional testing did not identify any vulnerabilities that were not considered by the developer. The overall outcome of the evaluator penetration testing effort showed that there are no exploitable vulnerabilities of the TOE in its intended environment.

3.118. Finally, the evaluators determined that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential. A summary of the evaluator testing effort for this component can be found in section 5.25 of the ETR (ref [10]).

3.119. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Vulnerability Analysis assurance component for EAL4.

Specific Functionality

3.120. The TOE Security Functional Requirements and the TOE Security Functions provided by Gauntlet are specified in sections 5.1 and 6.1 of the Security Target (ref [9]) and summarised in Appendix B of this report.

3.121. The evaluators found that the product correctly and effectively provided the functionality specified in the Security Target (ref [3]).

Discussion of Certification Issues

3.122. During the certification process, two issues were discovered and addressed by the certifiers. These issues have been identified and discussed in 3.44 and 3.111 of this report, and were suitability addressed during the certification process. As a result, there are no remaining unresolved issues following certification of Gauntlet.

General Observations

3.123. The certifiers would like to acknowledge the invaluable assistance provided Secure Computing Corporation and Network Associates Inc (NAI) staff during the evaluation. Without the due attention to problems found, and their technical assistance, the process could not have succeeded in the same time frame.

3.124. Further, the certifiers would like to acknowledge the efforts of CSC Australia in ensuring prompt delivery of the Evaluation Technical Report for certification.

Chapter 4 Conclusions

Certification Result

4.1 After due consideration of the Evaluation Technical Report (ref [10]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that Gauntlet has met the requirements of the Common Criteria EAL 4 Assurance level.

Scope of the Certificate

4.2 The certificate applies only to version 6.0 of the product. This certificate is only valid when the Gauntlet product is installed and configured in its evaluated configuration. The evaluated configuration of Gauntlet is described in the EAL4 Addendum (ref [15]) and Appendix C and should be verified on receipt of the delivered product.

Recommendations

4.3 The following recommendations include information highlighted by the evaluators during their analysis of the developer's deliverables, during the conduct of the evaluation, and during the additional activities performed by the Certification Group.

4.4 Gauntlet should only be used in accordance with the intended environment described in section 3.1 (Assumptions) of the Security Target (ref [9]) and the EAL4 Addendum (ref [15]). Importantly, the evaluated configuration does not include the full functionality offered by the Gauntlet product.

Functionality not part of the evaluated configuration

4.5 Potential users of the TOE are advised that the evaluation of Gauntlet has excluded the authentication mechanism used by the Gauntlet GUI administration tool. It is strongly recommended that users implement appropriate physical procedures to ensure that only authorised administrators have physical and logical access to the TOE.

4.6 Potential users of the TOE are advised that the evaluation of Gauntlet has excluded the use of the remote administration tool. Users are recommended to disable this tool during the installation of the TOE in order to comply with the stipulated environment. Procedures regarding the disabling of this functionality can be found in the guidance documentation (refs [11] - [15]).

4.7 Potential users of the TOE are advised that the evaluation of Gauntlet has excluded the implementation of IPSec. Potential purchasers are advised to consider other appropriately evaluated products in meeting their requirements.

4.8 Potential users of the TOE are advised that the evaluated configuration of Gauntlet does not include a virus scanning capability. Potential purchasers are advised to consider other appropriately evaluated products in meeting their requirements.

4.9 Potential users of the TOE are advised that the evaluated version of Gauntlet does not include the full set of proxies available in the product. Users are strongly recommended to ensure that the evaluated proxies, defined in Appendix C, are those required for use in their particular environment.

Evaluated Configuration of the TOE

4.10 Potential purchasers of the TOE should be aware that the evaluated configuration only allows two physical network connections to the TOE. The TOE's network configuration consists of an external connection (usually to the Internet via a router) and an internal network connection. The Certification Group recommends that this information be taken into consideration when deploying the TOE in a network security solution.

Secure Configuration of the Gauntlet Web Proxy

4.11 The Gauntlet web proxy includes functionality to support the HTTP CONNECT method, which is a standard mechanism that allows a client to create a tunnel through an HTTP proxy. The CONNECT method is required to allow SSL connections to be established through the web proxy, but the default configuration allows the client to specify any TCP port on which to create the tunnel.

4.12 The Certification Group strongly recommends that if administrators of the TOE are using the web proxy, formally described as http-gw, as part of their system configuration, the following configuration line should be added to the netperm-table (located in the /usr/local/etc directory):

http-gw: permit-ssl-ports 443 80

4.13 This will ensure that the HTTP CONNECT method can only be used to establish a connection to the HTTP or SSL protocol. If this configuration line is not added to the firewall configuration an unauthorised connection to any TCP/IP service can be tunneled through the web proxy if it is enabled.

4.14 If the organisation’s security policy does not allow SSL connections to be established through the firewall, then administrators may wish to disable the use of the HTTP CONNECT method entirely. This can be done by inserting the following configuration line in place of the one above:

http-gw: deny-ssl-ports *

Importance of the EAL-4 Addendum

4.15 Potential purchasers of the TOE are strongly recommended to obtain a copy of the EAL4

addendum when purchasing the TOE from SCC. Procedures outlining how to obtain a copy of the EAL4 Addendum can be found in Appendix C of this report. The EAL4 Addendum contains necessary guidance for an administrator to install and configure the TOE in its evaluated configuration.

Qualifications of the Administrator

4.16 To ensure the competent administration of the TOE, Administrators of the TOE should be trained in Unix administration and have sound knowledge of Internet protocols such as HTTP, TCP/IP, FTP and Telnet.

Reliance on the evaluated configuration of Solaris 8

4.17 Administrators of the TOE should be aware that for the TOE to operate as defined in the Security Target (ref [3]), it relies on supporting security functionality provided by the evaluated version of the Solaris 8 operating system. Therefore, administrators SHOULD ensure that Gauntlet is installed on the evaluated configuration of the Solaris 8 operating system. For further details on the evaluated configuration of Solaris 8, refer to the Solaris 8 Security Target and Certification Report available at the Communications-Electronics Security Group (CESG) web site:

http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/index.asp.

Importance of a network security policy when installing and configuring the TOE

4.18 The network security policy must define all possible connections and services allowed between the trusted and the untrusted network. It is the responsibility of the administrator to ensure that the configuration of the TOE in its intended environment is contributing to the satisfaction of the security policy.

4.19 Administrators should note that Gauntlet does not counter any external threats to the availability of the TOE. Since all communications between the external and internal network pass through the TOE, in its intended environment, a denial of service attack could be conducted against the TOE preventing information passing from the external network to the internal network (and vice-versa).

4.20 While this type of threat does not invalidate the security objectives of the TOE, the TOE provides a log space checking utility which provides alerts to the administrator when the TOE is running out of log space, which is indicative of a denial of service attack. It is recommended that administrators configure this utility to ensure that notification is received so appropriate action can be taken. Further guidance on this utility can be found in the EAL4 Addendum (ref [15]).

Appendix A References

[1] Evaluation Memorandum No.1- Description of the AISEP
Defence Signals Directorate
EM 1, Issue 1.1, March 1997

[2] Evaluation Memorandum No.2 - The Licensing of the AISEFs
Defence Signals Directorate
EM 2, Issue 1.0, August 1994

[3] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model (CC)
CCIMB-99-031, Version 2.1, August 1999

[4] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements
CCIMB-99-032, Version 2.1, August 1999

[5] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements
CCIMB-99-033, Version 2.1, August 1999

[6] Common Methodology for Information Technology Security Evaluation (CEM)
CEM-99/045, Version 1.0, August 1999

[7] Manual of Computer Security Evaluation Part I - Evaluation Procedures
Defence Signals Directorate
EM 4, Issue 1.0, April 1995
(EVALUATION-IN-CONFIDENCE)

[8] Manual of Computer Security Evaluations Part II - Evaluation Tools and Techniques
Defence Signals Directorate
EM 5, Issue 1.0, April 1995

[9] Gauntlet Firewall Version 6.0 Security Target
Network Associates Incorporated
Version 3.1, February 2002
(COMMERCIAL-IN-CONFIDENCE)

[10] Gauntlet Firewall Version 6.0 Evaluation Technical Report

CSC Australia
Issue 1.1, February 2001
(EVALUATION-IN-CONFIDENCE, COMMERCIAL-IN-CONFIDENCE)

[11] Gauntlet Firewall Administrators Guide Version 6.0
Network Associates Incorporated
Issue NAI-192-0048-6

[12] Gauntlet Firewall for UNIX Advanced Administrator's Manual Version 6.0
Network Associates Incorporated
Issue NAI-192-0049-1

[13] Gauntlet Firewall Getting Started Guide Version 6.0
Network Associates Incorporated
Issue NAI-192-0061-4

[14] Gauntlet Firewall Services Guide Version 6.0
Network Associates Incorporated
Issue NAI-192-0028-1

[15] Gauntlet Firewall Version 6.0 EAL-4 Addendum
Network Associates Incorporated
Issue NAI-192-0068-1

[16] Gauntlet 6 Security Policy Model
Network Associates Incorporated
Issue 2.2, 22nd August 2001

[17] Information Technology Security Evaluation Methodology (ITSEM)
Commission of European Communities
Version 1.0, 10 September 1993

[18] Arrangement on the Recognition of Common Criteria Certificates (in the field of Information Technology Security)
Available from: http://www.commoncriteria.org/registry/ccra-final.html

[19] Information regarding evaluation deliverables resulting from SCC's acquisition of Gauntlet
Facsimile from Jason Lamar to Chris Pennisi
Received 25th March 2002

[20] Evaluator Assessment regarding changes in delivery procedures of the TOE

Facsimile from Jodie Poole to Doug Stuart
Received 26th March 2002

Appendix B Summary of the Security Target

Security Target

B.1 A brief summary of the Security Target (ref [3]) is given below. Potential purchasers should attempt to obtain a copy of the full Security Target to ensure that the security enforcing functions meet the requirements of their security policy.

Security Objectives for the TOE

B.2 Gauntlet has the following IT Security objectives:

a) The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.

b) The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.

c) The TOE must mediate the flow of all information from users on a connected network to users on another network.

d) Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.

e) The TOE must protect itself against attempts by unauthorised users to bypass, deactivate, or tamper with TOE security functions.

f) The TOE must provide a means to record a readable audit trail of security-related events with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.

g) The TOE must provide user accountability for information flows through the TOE and for authorised administrator use of security functions related to audit.

h) The TOE must provide functionality that enables an authorised administrator to use the TOE security functions, and must ensure that only authorised administrators are able to access such functionality.

i) The TOE must provide functionality that enables an authorised administrator to use the TOE security functions, and must ensure that only authorised administrators are able to access such functionality.

j) The TOE must provide the means for an authorised administrator to control and

limit access to TOE security functions by an authorised external IT entity.

Security Objectives for the Environment

B.3 Gauntlet has the following environmental objectives

a) The TOE is physically secure.

b) The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.

c) There are no general-purpose computing capabilities (e.g. the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

d) The TOE does not host public data.

e) Authorised administrators are non-hostile and follow all administrator guidance; however, they are capable of error.

f) Information can not flow among internal and external networks unless it passes through the TOE.

g) Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g. a console port) if the connection is part of the TOE.

h) Human users including authorised administrators can not access the TOE remotely from the internal or external networks.

i) The TOE must be delivered, installed, administered and operated in a manner that maintains security.

j) Authorised administrators are trained in and responsible for: the establishment and maintenance of security policies and practices; user awareness; and operating system and internet protocol operation.

k) The operating system will provide functions to the TOE to: provide time-stamping; assist in audit entry recording and sorting and provide password-checking functionality

Secure Usage Assumptions

B.4 The following assumptions relate to the operation of the TOE:

a) The TOE is physically secure.

b) Malicious attacks aimed at discovering exploitable vulnerabilities is considered

low.

c) There are no general-purpose computing and storage repository capabilities on the TOE.

d) The TOE does not host public data.

e) Authorised administrators are non-hostile and follow all administrator guidance (contained within (refs [11] - [15])).

f) Authorised administrators are trained in all relevant protocols and operating systems.

g) Information can not flow among the internal and external networks unless it passes through the TOE.

h) Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection if the connection is part of the TOE.

i) No one may access the TOE remotely from the internal or external networks.

j) Users will not install software that may bypass the TOE.

Threats addressed by the TOE

B.5 The following threats are addressed by the TOE:

a) An unauthorised person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

b) An unauthorised person may repeatedly try to guess authentication data in order to use information to launch attacks on the TOE.

c) An unauthorised person may use valid identification and authentication data obtained to access functions provided by the TOE.

d) An unauthorised person may carry out spoofing in which information flow through the TOE into a connected network by using spoofed source address.

e) An unauthorised person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.

f) Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

g) An unauthorised person may read, modify or destroy security critical TOE

configuration data.

h) An unauthorised person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attackers actions.

Threats addressed by the TOE Environment

B.6 The following threat is addressed by the TOE Environment:

a) The TOE may be inadvertently configured, used and administered in an insecure manner by either authorised or unauthorised persons.

Organisational Security Policies

B.7 There are no identified organisational security policies relevant to the operation of the TOE.

Summary of the TOE Security Functional Requirements

The TOE security functional requirements (SFRs) are tabulated below. Full description and explanation of these SFRs can be found in Section 5.1 of the Security Target (ref [9]).

Class FAU: Audit

FAU_GEN.1 Audit data generation

FAU_SAR.1 Audit review

FAU_SAR.3 Selectable audit review

FAU_STG.1 Protected audit trail storage

FAU_STG.4 Prevention of audit data loss

Class FCS: Cryptographic Support

FCS_COP.1 Cryptographic Operation

Class FDP: User data protection

FDP_IFC.1 Subset information flow control (1)

FDP_IFC.1 Subset information flow control (2)

FDP_IFF.1 Simple security attributes (1)

FDP_IFF.1 Simple security attributes (2)

Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

FIA_UID.2 User identification before any action

FIA_UAU.1 Timing of authentication

FIA_UAU.4 Single use authentication mechanisms

FIA_ATD.1 User attribute definition

Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

FMT_MSA.3 Static attribute initialisation

FMT_SMR.1 Security Roles

Class FPT: Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSF

Class FTA: TOE Access

FTA_TSE.1 TOE session establishment

Security Requirements for the IT Environment

B.8 Gauntlet has the following requirements on the IT environment, which are provided by the evaluated version of the Solaris 8 Operating system:

Class FAU: Audit

FAU_SAR.1 Audit review

FAU_SAR.3 Selectable audit review

FAU_STG.1 Protected audit trail storage

Class FIA: Identification and Authentication

FIA_UAU.1 Timing of authentication

FIA_UID.2 User identification before any action

Class FPT: Protection of TSF

FPT_STM.1 Reliable time stamps

Security Requirements for the Non-IT Environment

B.9 There are no identified Security Requirements for the non-IT Environment.

Summary of the TOE Security Functionality

B.10 Gauntlet's TOE Security Functions (TSFs) are grouped under the following categories; Security Audit, Identification and Authentication, Access Control and Data Exchange. Full description and explanation of these TSFs can be found in section 6.1 of the Security Target (ref [9]).

Appendix C Identification of the TOE

Configuration for Evaluation

C.1 The evaluation was conducted on the Gauntlet Firewall Version 6.0. The evaluated software components of The TOE have been identified below.

Software

C.2 The Software elements of Gauntlet are as follows:

a) 1 x CD-ROM containing the Gauntlet Firewall Software, Version 6.0

C.3 The following patches, available on the SCC web-site, http://www.securecomputing.com/gauntlet_patch.cfm, also form part of the evaluated configuration:

PATCH	VERSION	PATCH	VERSION
Authsvr.patch	1	Crfwcert.patch	1
Crontab.patch	1	Edatupdate.patch	1
Ednload.patch	1	Espmc.patch	1
Espmd.patch	1	Frequentcheck.patch	2
ftp-pdk.patch	2	Fwregister.patch	1
Getroot.patch	1	Gfw.patch	2
Gui.patch	2	http-pdk.patch	3
Iiop-pdk.patch	2	Ipe-patch	1
Ipfs.patch	1	Jre.patch	1
Login-sh.patch	1	Mmp.patch	1
Oracle.patch	1	Plug-pdk.patch	2
Proxymgr.patch	1	Rootusr.patch	3

Rtsp-pdk.patch	2	Snmp.patch	1
Socks5-gw.patch	1	Ssod.patch	1
Stdlogd.patch	2	Stdlogespmc.patch	1
tn-gw.patch	1	Trans.patch	1
Udp-pdk.patch	2	Up242.patch	1
Vscan.patch	1	Vsrequest.patch	1
Checkspace.patch	2	Smtp.patch	1
Csmap.patch	2		

C.4 As stated in Chapter 4, The evaluated configuration of Gauntlet excludes the IPSec Virtual Private Network (VPN) functionality, virus scanning capability and only includes the following proxy services:

a) Terminal Services (TELNET)

b) Electronic mail (SMTP (smap/smapd) and POP 3)

c) Plug gateway

d) File transfer services (FTP)

e) Web Services (HTTP) - Refer to Chapter 4 for advice on using this proxy

f) SQL services (Orance*SQL, Microsoft SQL and Sybase)

g) SNMP (Simple Network Management Protocol)

h) Removal of Java and Active X from HTTP Services

Gauntlet also includes configured versions of the TCP plug proxy for:

a) LDAP (certificate management);

b) Usenet news (NNTP);

c) Web services (SSL);

d) AOL;

e) Compuserve;

f) Lotus Notes;

g) NNTP;

h) NetBIOS-tcp;

i) NetMeeting; and

j) X.500

Third Party Software

C.5 The third party software used in the evaluation of the TOE is as follows. Note that the following software does contribute to the TOE security functionality implemented by Gauntlet as outlined above in Appendix B - Security Requirements for the IT Environment:

a) Sun Solaris 8 First Customer Shipment (FCS)

b) Adminsuite Version 3.0.1 FCS

with patches:

c) 108875-07 and 108879-02 for SPARC platforms

C.6 This evaluation is only valid for the above-mentioned version of Gauntlet running on the Sun Solaris operating system. No other versions, operating systems or third party software are part of the evaluated configuration.

Hardware

C.7 Hardware configuration for the TOE is described in the Solaris 8 Security Target and Certification Report available at the CESG web site, http://www.cesg.gov.uk/assurance/iacs/itsec/cpl/index.asp.

C.8 Please note that none of the hardware identified above implements any of the security functionality offered by the TOE. The minimum recommended hardware configurations for the above hardware platforms are located in section 2.2 of the Security Target (ref [9]).

Procedures for determining the evaluated version of the TOE

C.9 In order for an administrator to determine if a delivered product is in fact the evaluated product, the following procedures can be followed in making that determination.

C.10 When administrators are placing an order for the product, they should receive a Media Kit.

This contains a copy of the TOE on CD-ROM, which is shrink-wrapped, and a printed order number on the packaging.

C.11 Once a copy of the Media Kit has been received, the administrator should inspect the shrink-wrap packaging for any signs of tamper. Any indication of tamper should be reported immediately to SCC and the product returned. Administrators will need to contact SCC, providing their order number, to initiate posting of the Customer ID letter. The Customer ID letter contains a unique "Customer ID Number".

C.12 Administrators should then check that the Order Number on the Media Kit matches the Customer ID in the Customer ID Letter. If there is any discrepancy between the Order Number and the Customer ID Number administrators should report this to SCC immediately.

C.13 To configure the TOE in the evaluated configuration it is necessary for Administrators to obtain a copy of the EAL4 Addendum (ref [15]). This can be done by logging into the SCC web-site at the following URL, http://www.securecomputing.com/gauntlet_patch.cfm. Administrators should note that the Customer ID Number is required to access this web- site.

C.14 Operational documentation (refs [11] - [14]) is delivered in soft copy with Gauntlet on CD-ROM. Upon receiving the delivered TOE, Administrators should seek to verify its authenticity by calculating a checksum on the delivered CD-ROM and comparing this with the checksum posted on the SCC Security web site, http://www.securecomputing.com/gauntlet_patch.cfm. Procedures for performing this verification check can be found in the EAL-4 Addendum (ref [15]).