National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Marconi

SA-400 Firewall Version 1.3

Report Number: CCEVS-VR-04-0067

Dated: 7 July 2004

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Mike Allen

John Nilles

Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

COACT, Incorporated

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of the Marconi SA-400 Asynchronous Transfer Mode (ATM) Firewall. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by COACT Incorporated, and was completed during June 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by COACT. The evaluation determined that the product is both **Common Criteria Part 2 and Part 3 conformant,** and meets the assurance requirements of **EAL 2**. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfy the needs for protection of sensitive information as defined by DoD Standard 8500.2. All security functional requirements are derived from Part 2 of the Common Criteria.

The product provides Enterprise Networks with IP/ATM Firewall capabilities at OC-12 line rate. In the evaluated configuration, the appliance must be managed via a serial console or from a web browser/administrative workstation located on a physically protected and isolated LAN connected to the TOE by a 10/100 Ethernet port. The graphic interface allows the administrator to configure filtering rules, monitor connections and logs. The interface also allows the administrator to start, stop, and reset the Firewall. The serial console is used for initial configuration of the TOE, user management, trouble shooting, setting the clock and additional management functions.

The validation team monitored the activities of the COACT evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test reports. The validation team determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the validation team concludes that the COACT findings are accurate, the conclusions justified, and the conformance claims correct.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Marconi SA-400 Firewall Version 1.3
Protection Profile	None
Security Target	Marconi SA-400 Firewall, Version 1.3 Security Target Dated May 27, 2004
Evaluation Technical Report	*Marconi SA-400 Firewall Version 1.3 Evaluation Technical* Report dated May 27, 2004
Conformance Result	Part 2 and Part 3 conformant, EAL 2
Sponsor	Marconi
Developer	Marconi
Evaluators	COACT Incorporated
Validators	The Aerospace Corporation

3. SECURITY POLICY

The Marconi SA-400 enforces the following security policies:

3.1. Security Audit Policy.

The TOE provides auditing/logging functions to record Trusted Security Function (TSF) security relevant events on its local hard drive. The logs are separated into System Logs, Web Interface Logs, Connections Logs, Monitor Log and Disallowed Connections Log. An authorized user has the ability to review these files from the Graphical User Interface (GUI) on the management workstation. Each authorized user has equal access to the security functions. The Log files are saved on a protected portion of the local hard drive. The size and number of log files can be controlled. For security purposes, a user cannot purge the log files. The "SYSLOG" function along with the "logrotate" facility manage the log files.

3.2. Identification and Authentication Policy.

The identification process is a sub-set of the Administrator Management Process. It is used to verify that the administrator has proper identification by means of "login name" and "password" before allowing interaction with the TOE. Proper identification allows the administrator to have access to the Command Line Interface (Cli) and Web interface.

3.3. Security Management.

The TOE is managed by a serial interface for initial configuration (setting IP address, allowable GUI users, selecting speed of the OC-12 card, Inactivity timeout period, diagnostics, system shutdown, logging) and an Ethernet interface for configuring the firewall filtering security functions and viewing system logs. Before being able to manage the Firewall, the user must be authorized through the identification/authorization process. Ultimately, the administrator must verify that the rules they assign/establish are correct for their network security policy. For detailed information on managing specific policies, configurations, etc., refer to the SA-400 User's Manual.

3.4. Filtering Policy.

The firewall implements a traffic filtering policy; it either passes or blocks traffic on a per-packet basis in accordance with a rule-set that is configurable by an authorized administrator. Datagram parameters are taken into account in the policy at the ATM and IP level. By default, the firewall rule set includes PVC filtering rules that allow datagrams required for initial call setup to pass through the firewall. These rules are documented in the SA 400 User's manual.

3.4.1. ATM level Filtering Parameters

At the ATM level filter rules can be set for SVC (Switched Virtual Circuits), PVC (Permanent Virtual Circuits) . For SVC Filtering rules are set using the direction of travel across the firewall, SPANS (Simple Protocol for ATM Network Signalling) and/or UNI (User-to-Network Interface) source and destination addresses and the SPANS Service Access Points (SAP). For PVC circuits rules can be set based upon Virtual Path Identifier (VPI), Virtual Channel Identifier (VCI), and the direction of travel. All rules are configured to indicate the action taken in the event a rule is triggered.

3.4.2. IP level Filtering Parameters

At the IP level, filtering rules can be set based upon source and/or destination addresses, source and destination ports, specifically identified protocols ((TCP, UDP, ICMP or IGMP) and the direction of travel across the firewall.

4. ASSUMPTIONS

4.1. Usage Assumptions

The firewall administrators are trained to use the TOE, and are trusted to enforce all relevant security aspects of the TOE and their organisation.

4.2. Environmental Assumptions

The Marconi firewall is located in a physically protected, secure facility in order to prevent physical access to the TOE by anyone other than authorized personnel.

The management LAN is isolated and contains only the management workstation and the firewall(s) under management.

5. ARCHITECTURAL INFORMATION

The Target of Evaluation is the Marconi SA-400 Firewall, Version 1.3. The SA-400 provides networks with reliable IP/ATM Firewall capabilities at OC-12 line rate. The appliance is managed by a web interface accessible through a 10/100 Ethernet port or via the console serial interface. The web interface allows the administrator to configure tables via a Graphical User Interface (GUI). The interface also allows the administrator to start, stop, and reset the Firewall. A log is available to review administrator and system interactions. The management workstation or console is not part of the TOE.

The SA-400 Firewall is composed of a number of logical subsystems.

- Information Flow Control Processes (The Main Extraction Process, Call Set-up Process, PVC Filtering Process, SVC ATM Filtering Process, IP Filtering Process and Monitor Process functions)
- Auditing Process
- Identification/Authorisation/Access Process
- GUI Rule Management Process
- Administrator Management

Together these logical subsystems provide security functionality for the TOE.

5.1. Information Flow Control Processes

The information flow control process provides the TOE firewall filtering capabilities. These capabilities include IP filtering based upon Destination address, source address, type, and port (for TCP and UDP) and ATM filtering based upon the VPI, VCI , network-layer service access point (NSAP) source and destination.

5.2. Auditing Process

The SA-400 provides auditing/logging functions to record TSF security relevant events on its local hard drive. The logs are separated into System Logs, Web Interface Logs, Connections Logs, Monitor Log and Disallowed Connections Log. An authorized user reviews these files from the GUI on the management workstation. A user cannot purge the log files. The “SYSLOG” function along with the “logrotate” facility manages the log files.

5.3. Identification/Authorisation/Access Process

The identification process is used to verify that the administrator has proper identification by means of “login name” and “password” before allowing interaction with the SA-400. In addition, the SA-400 can be configured to deny login except from a specific IP address and disconnect a session after a specified period of inactivity.

5.4. GUI Rule Management Process

The SA400 web interface is used to configure the firewall filtering rule set and logs.

5.5. Administrator Management

The SA-400 console serial interface is used to configure and manage the firewall this includes: setting the IP address, allowable GUI users, setting the inactivity timeout period, diagnostics, system shutdown, and logging.

6. DOCUMENTATION

The following documentation was used as evidence for the evaluation of the Marconi SA-400 Firewall Version 1.3.

1. Bill of Material Structure Report, Rev B, 06/24/2002;
2. Bill of Materials Import Management System, 06/24/2002;
3. Class Code Matrix, 06/26/2002.
4. Configuration Change Management (CCM) Part Entry Form (PEF) Processing and Related Functions, Rev. A, 06/2001;
5. Configuration Management Plan, Rev. A, 05/30/2001;
6. Control of Internal Business Process Documentation Procedure, Rev. A, 09/2000;
7. Control of Unreleased Product (CUP) Checklist, Rev. A, 12/19/2001;
8. Engineering Change Notice (ECN) Data Entry Work Instruction, Rev. B, 06/23/2000;
9. Engineering Change Notice Procedures, Rev. H, 06/21/2000;
10. Marconi Document #PRST-4150-001 (Handling, Storage, Preservation, and Delivery of Products), Revision C, 01/23/2002;
11. Marconi SA-400 Firewall Version 1.3 Security Target, May 27, 2004;
12. Marconi SA-400 High Level Design Document with Security Functional Specifications, Revision 2.3, July 10, 2003.
13. Marconi SA-400 QA Test Procedures for Release 1.3, Revision 1.7, February 4, 2004;
14. Marconi SA-400 Security Firewall Quickstart Guide, Software Version 1.3.0, Revision C, July 02, 2002;
15. Marconi SA-400 Security Firewall User's Manual, Software Version 1.3.0, Issue D, April 16, 2004;
16. New Product Release Engineering Change Notice (ECN) Requirements Checklist, Rev. A, 12/19/2001;
17. Procedure for the Control of Unreleased Product, Rev. C, 08/2000;
18. Product Configuration Management System Help, Rev. H, 12/19/2001;
19. Product Deviation Requirements Checklist, Rev. B, 12/19/2001;
20. Release Document Registration, Rev. A, 08/09/2001;
21. Released Product Change Engineering Change Notice (ECN) Requirements Checklist, Rev. A, 12/19/2001;
22. SA-400 CLI Error Conditions and Messages, Version 1.1, October 27, 2003.
23. SA-400 Common Criteria Certification Correspondence Mapping Revision 3.5, November 5, 2003.
24. SA-400 Common Criteria Certification Developer Vulnerability Analysis Revision 1.3, March 1, 2004.
25. SA-400 Common Criteria Certification Strength of Function, Revision 1.4, March 17, 2004;
26. SA-400 GUI Error Conditions and Messages, Version 1.1, October 27, 2003;
27. SA-400 Installation Guide "Evaluated Configuration" for Common Criteria Certification (CCC), Revision 1.0, 06-03-2002;
28. SA-400 Product Requirements Document (PRD), Rev. 1.7, February 20, 2002.

29. SA-400 Test Coverage, Revision 1.2, 2/11/04
30. SA-400 Test Results.xls, 6/14/02

7. IT PRODUCT TESTING

7.1. Developer Testing

At EAL2, testing must demonstrate correspondence between the tests and the functional specification. However complete testing is not required; "coverage analysis need not demonstrate that all security functions have been tested, or that all external interfaces to the TSF have been tested."[1]

The vendor testing included tests for security functionality described in the ST and identified below:

- Information Flow Control Processes (The Main Extraction Process, Call Set-up Process, PVC Filtering Process, SVC ATM Filtering Process, IP Filtering Process and Monitor Process functions)
- GUI Rule Management Process
- Auditing Process
- Identification/Authorisation/Access Process
- Administrator Management

7.2. Evaluator Independent Testing

The evaluation team performed the TOE installation, as specified in the Installation, Generation and Startup documentation, reran developer tests, then developed and performed functional and vulnerability testing using two test configurations. Figure 1, depicted below, incorporates two ATM switches and was used to support IP testing and manual tests. Figure 2, also depicted below, shows the second test configuration which incorporated a Smartbits load generator to perform ATM and IP testing.

[1] CEM, V1.0, paragraph 6.8.2.2 (application note for EAL2:ATE_COV.1)

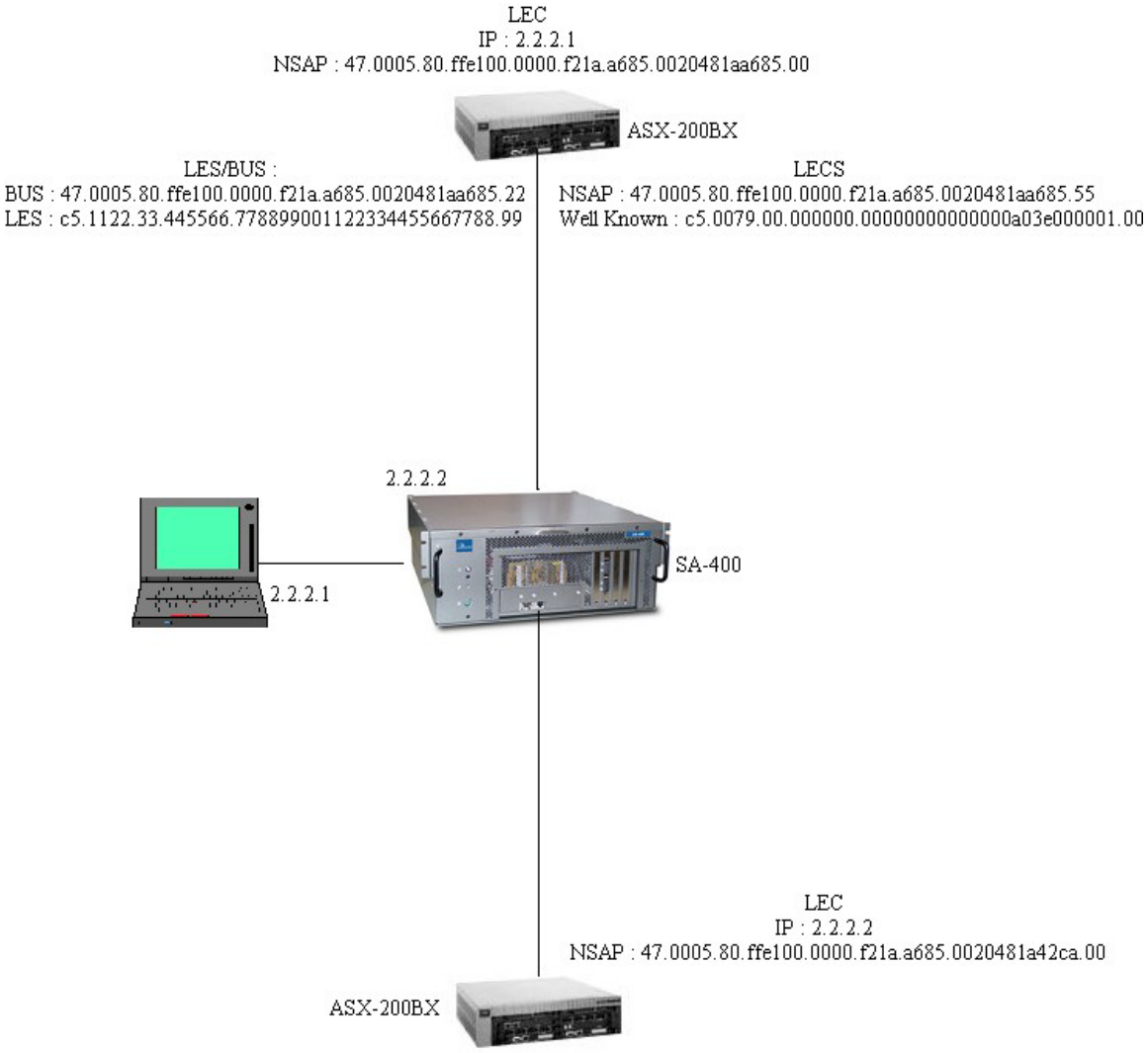

Figure 1 Test Bed Setup 1

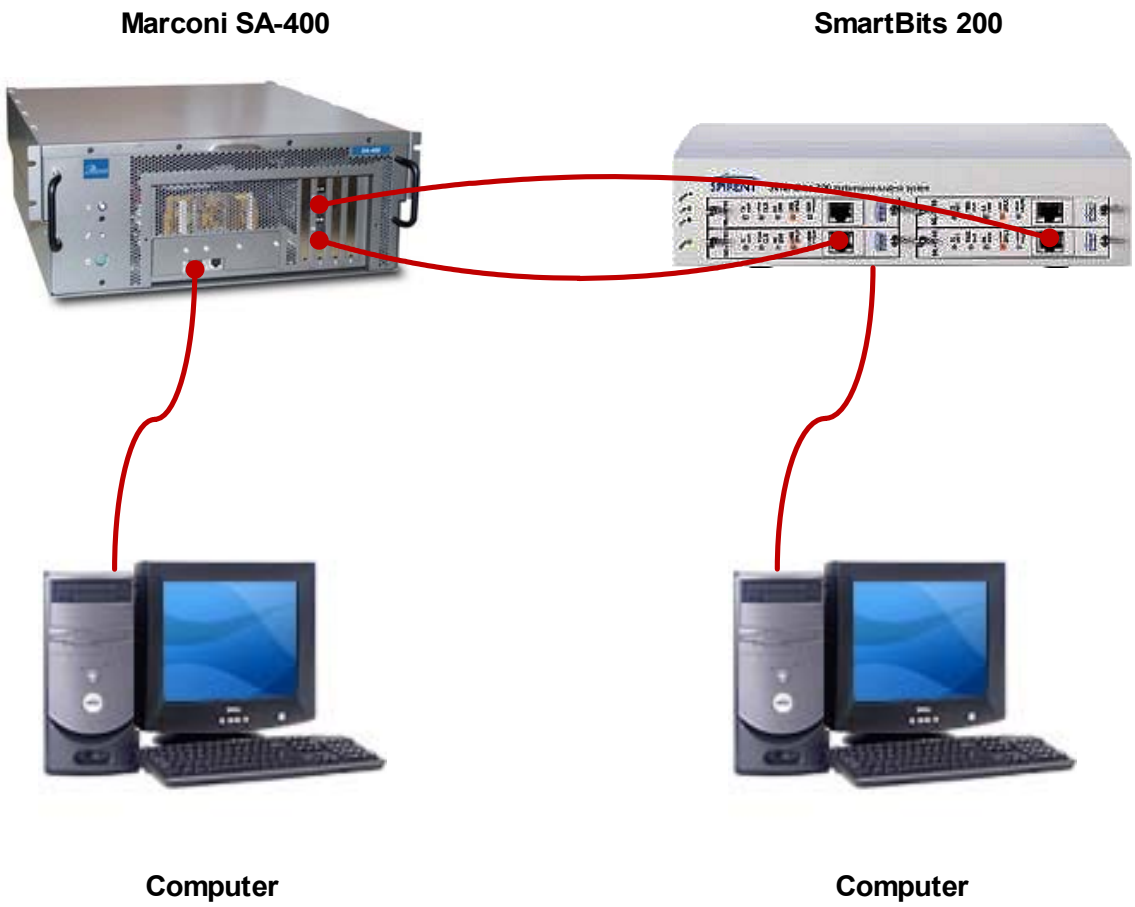

Figure 2 Test Bed Setup 2

8. EVALUATED CONFIGURATION

The evaluation configuration consists of the Marconi SA-400 Firewall Version 1.3 model 405-1200-300-S. The evaluated configuration requires:

- Local logging and storage of audit records.
- Local timestamp generator for use in audit records.
- The Ethernet port used to manage the TOE is connected to a LAN that contains only trusted administration systems (e.g. only the management workstation).
- Physical access to the TOE is limited to trusted administrators of the TOE.

In the evaluated configuration, the TOE includes an IP/ATM 622 Mbps OC-12c firewall line card. The vendor also offers an IP/ATM 155 Mbps OC-3c firewall line card. The security characteristics of the OC-3c card were **not** evaluated and therefore its use **is prohibited** in the evaluated configuration.

In addition, the SA-400 includes the capability to import/export the firewall rule set. The use of this feature was **not** analyzed during the evaluation and therefore its use **is prohibited** in the evaluated configuration.

9. RESULTS OF THE EVALUATION

The evaluation was conducted based upon the Common Criteria (CC), Version 2.1, dated August 1999 [1,2,3,4]; the Common Evaluation Methodology (CEM), Version 1.0, dated August 1999 [6]; and all applicable National and International Interpretations in effect on 16 April 2002. The evaluation confirmed that the SA-400 Firewall product is compliant with the Common Criteria Version 2.1, functional requirements (Part 2) and assurance requirements (Part 3) for EAL2. The details of the evaluation are recorded in the Evaluation Technical Report, Marconi SA-400 Firewall Version 1.3 Evaluation Technical Report dated May 27, 2004. The product was evaluated and tested against the claims presented in the Marconi SA-400 Firewall Version 1.3 Security Target dated May 27, 2004.

The validation team followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation team's results are correct and complete.

9.1. Evaluation of the Marconi SA-400 Firewall Version 1.3 Security Target (ASE)

The evaluation team applied each EAL 2 ASE CEM work unit. Evaluation team action during the course of the ST evaluation ensured that the ST contained a description of the environment in terms of threats, assumptions and policies; a statement of security requirements claimed to be met by the Marconi SA 400 firewall that are consistent with the Common Criteria; and product security function descriptions that support the requirements.

9.2. Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensures that the integrity of the TOE is adequately preserved; in particular, that configuration management provides confidence to the consumer that the TOE and documentation used for evaluation are the ones prepared for distribution. It also ensures that the TOE is accurately and uniquely identified such that the consumer is able to identify the evaluated TOE and discern one version from another. Configuration Management (CM) systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking changes and by ensuring that all changes are authorized. The Evaluation Team identified and analyzed the CM process to ensure that its documented procedures were followed and the procedures were employed during the course of this evaluation. The evaluation team ensured that the following items were considered configuration items: TOE implementation, design documentation, test documentation, and user guidance.

9.3. Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to securely deliver, install, configure, and operationally use the TOE; and ensured that the security protection offered by the TOE was not compromised during that process.

9.4. Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF implements/employs the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

9.5. Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team verified the adequacy of the administrator guidance in describing how to securely administer the TOE.

9.6. Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team tests and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

9.7. Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain obvious vulnerabilities that can be exploited in the evaluated configuration, based upon the developer strength of function analysis and the developer vulnerability analysis as well as the evaluation team's performance of penetration tests.

9.8. Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test further demonstrated the claims in the ST.

10. VALIDATOR COMMENTS

The validation team observations support the evaluation teams conclusion that the Marconi SA 400 version 1.3 meets the claims stated in the Security Target. The validation team also wishes to emphasize that the TOE must be installed and operated in the evaluated configuration in order to ensure that the TOE provides the security functionality described in the security target.

11. SECURITY TARGET

Marconi SA-400 Firewall Version 1.3 Security Target *dated* May 27, 2004 is included here by reference.

12. GLOSSARY

Acronym	Description
AAL	ATM Adaptation Layer
ATM	Asynchronous Transfer Mode
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FCP	Firewall Control Processor
FIP	Firewall Inline Processor
GUI	Graphical User Interface
ICMP	Internet Control Message Protocol
IDE	Integrated Drive Electronics
IGMP	Internet Group Multicast Protocol
ILMI	Interim Local Management Interface
IP	Internet Protocol
LANE	Local Area Network Emulation
MPOA	Multi-Protocol Over ATM
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NNI	Network-to-Network Interface
NSA	National Security Agency

Acronym	Description
NSAP	Network Service Access Point
PCI	Peripheral Component Interconnect
PNNI	Private Network-to-Network Interface
PP	Protection Profile
PVC	Permanent Virtual Connection
SAP	SPANS Service Access Point
SPANS	Simple Protocol for ATM Network Signaling
ST	Security Target
SVC	Switched Virtual Connection
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
UDP	User Datagram Protocol
UNI	User-to-Network Interface
URL	Uniform Resource Locator
VCI	Virtual Channel Identifier
VPI	Virtual Path Identifier

13. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] Marconi SA-400 Firewall, Version 1.3 Security Target dated May 27, 2004.

[8] Marconi SA-400 Firewall Version 1.3 Evaluation Technical Report dated May 27, 2004.