National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

IronPort Messaging Gateway Version 5.1.2

Report Number: CCEVS-VR-VID10144-2008
Dated: 28 June 2008
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 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)
Jerome Myers (Senior Validator)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Jean Petty
Quang Trinh
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Validator Comments in Section 10.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the IronPort Messaging Gateway Version 5.1.2. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of IronPort Messaging Gateway Version 5.1.2 was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 27 March 2008.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation was performed to conform with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005 Evaluation Assurance Level 2 (EAL 2) and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 2.3, August 2005. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the IronPort Messaging Gateway Security Target. The evaluation team determined the product to be Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 2. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is IronPort Systems Messaging Gateway Version 5.1.2 running on IronPort Systems hardware appliance versions C150, C350, C600, C650, X1000 and X1050 provided by IronPort Systems, Inc. The TOE monitors Simple Mail Transfer Protocol (SMTP) email traffic in the IT environment between an external and an internal network when the environment is configured to send all port 25 traffic through the TOE. The TOE provides multiple independent physical interfaces that can be used to separate internal and external networks. The TOE can be configured to monitor email traffic sent from the internal network to the external network, or vice versa.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence reviewed.

During this evaluation, the Validators monitored the activities of the SAIC evaluation team, 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 Validators 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 Validators conclude that the SAIC 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, 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 conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) 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;
- The Protection Profile to which the product is conformant; and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	IronPort Messaging Gateway Version 5.1.2
Protection Profile	None
Security Target	*IronPort Messaging Gateway Version 5.1.2 Security Target*, Version 1.0, 24 April 2008
Dates of evaluation	December 5, 2005 through March 27, 2008
Evaluation Technical Report	*Evaluation Technical Report for IronPort Messaging Gateway* Version 5.1.2, Part 1 (Non-Proprietary), Version 1.0 24 April 2008, Part 2 (Proprietary), Version 1.0 24 April 2008
Conformance Result	Part 2 extended and Part 3 conformant, EAL 2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on December 5, 2005
Common Evaluation Methodology (CEM) version	CEM version 2.3, August 2005 and all applicable NIAP and International Interpretations effective on December 5, 2005
Sponsor	IronPort Systems, Inc., 950 Elm Avenue, San Bruno, CA 94066
Developer	IronPort Systems, Inc., 950 Elm Avenue, San Bruno, CA 94066
Common Criteria Testing Lab	Science Applications International Corporation (SAIC), Columbia, MD
Evaluators	Terrie Diaz, Jean Petty, and Quang Trinh of SAIC
Validation Team	Jerome Myers and Mike Allen of The Aerospace Corporation

3 Organizational Security Policy

The IronPort Messaging Gateway performs the following security functions:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TOE
- Mail Intrusion Detection

The TOE monitors network traffic sent and received on port 25 containing SMTP email messages. The location of the TOE in the network in the IT environment in the evaluated configuration requires email network traffic pass through the TOE.

The TOE monitors the traffic by performing the following traffic analysis techniques:

- Signature analysis
- Detection of spam
- Application of content filters
- Application of virus outbreak filters

The TOE can take one or more of the following actions in order to enforce an email message policy (i.e. to enforce the implicit IDS security policy):

- Generate an email to an administrator containing an alarm
- Generate an alarm that is written to a log file that can be examined using the administrator console
- Drop the email message
- Bounce the email message
- Archive the email message
- Add a blind-carbon copied recipient to the email message
- Modify the email message

The TOE is controlled by rule sets that are specific to each analysis technique; there are administratively-configurable rule sets as follows:

- Anti-spam rules

- Content filter rules
- Virus outbreak filter rules

Anti-spam, content filter, and virus outbreak rules are each implemented as collections of TOE configuration settings that can be specified using administrator console interfaces. Rules are configured such that they are applied to specific groups of users based on email message attributes (Envelope Recipients, Envelope Sender, From: header, or Reply-To: header) in order to perform each type of analysis as described above.

4 Assumptions and Clarification of Scope

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be employed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product, defines the threats that the product is designed to counter and the organizational security policies which the product is designed to comply.

Following are the assumptions identified in the Security Target:

- It is assumed the TOE is appropriately scalable to the IT System the TOE monitors and has access to all the IT System data it needs to perform its functions.
- It is assumed network traffic sent and received on port 25 can not flow among the internal and external networks unless it passes through the TOE.
- It is assumed the processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access and modifications.
- It is assumed those responsible to manage the TOE are competent individuals, that only authorized users can gain access to the TOE, and that they are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

Following are the organizational security policies levied against the TOE and its environment as identified in the Security Target.

- All data collected and produced by the TOE shall only be used for authorized purposes and must be protected.
- The TOE must be protected from unauthorized accesses and disruptions of TOE data and functions.
- Users of the TOE must be accountable for their actions within the system.
- The TOE must collect data that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity.
- The TOE must perform analytical processes and information to derive conclusions about inappropriate activity (past, present, or future) on collected system data and appropriate response actions taken.

Following are the threats levied against the TOE and its environment as identified in the Security Target. The threats that are identified are mitigated by the TOE and its environment. All of the threats identified in the ST are addressed.

- An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
- An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

- An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
- An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
- An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
- An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
- An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
- Unauthorized attempts to access TOE data or security functions may go undetected.

The TOE provides a secure environment for sending and receiving email messages by monitoring network traffic received on port 25 containing SMTP email messages. The TOE performs signature analysis, detection of spam, application of content filters, and application of content filters on collected email network traffic and records corresponding event data.

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- Administrators are warned to choose strong passwords. The TOE only requires passwords to be 6 characters or more. This is insufficient to meet the Strength of Function requirements unless additional complexity is assumed. Users are directed to page six of the IronPort AsyncOS 5.1 Common Criteria Guide for guidance in choosing appropriate passwords.

- The TOE uses e-mail messages for alerts, particularly to signal audit log reaching 90% capacity. This means that the TOE must rely on the IT environment to deliver these messages in a correct and timely manner. Users must confirm that this is a valid assumption.

- The TOE relies on signature files to perform some of the security functions associated with anti-virus and anti-spam detection. These signature files were not examined as part of this evaluation and no claims of correctness or comprehensiveness are made. The user must rely on other third-party analyses performed by organizations such as ICSA Labs for such evaluations.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target. Figure 1 shows a typical deployment of the TOE.

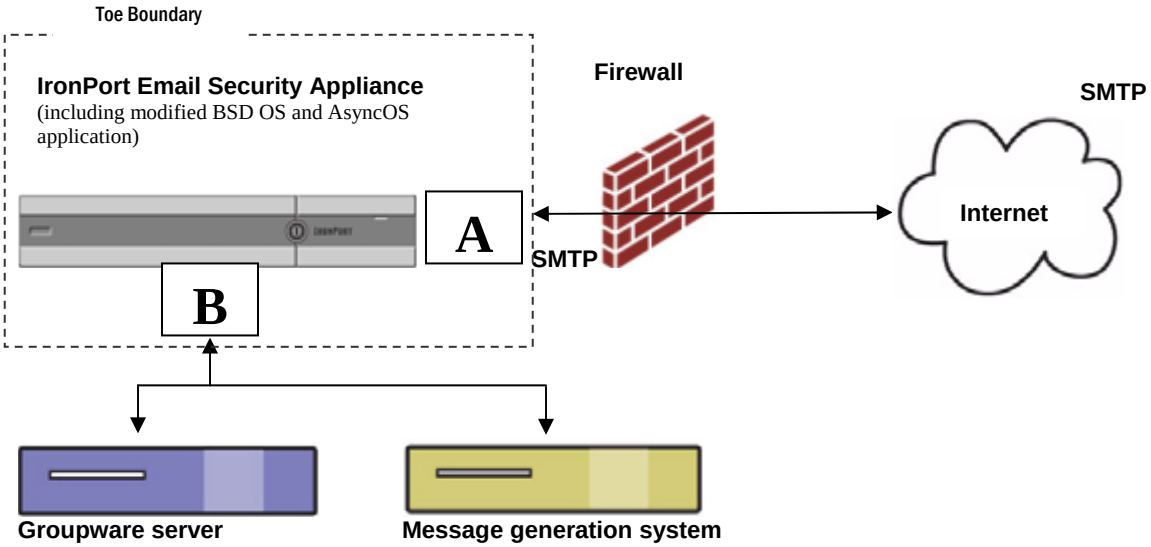

Figure 1: TOE Boundry

The IronPort Messaging Gateway appliance is a high-performance appliance designed to meet the email infrastructure needs of enterprise networks. The IronPort appliance eliminates spam and viruses, enforces corporate policy, secures the network perimeter, and reduces the Total Cost of Ownership (TCO) of enterprise email infrastructure.

IronPort Systems combine hardware, a hardened operating system, application, and supporting services to produce a purpose-built, rack-mount server appliance dedicated for enterprise messaging.

The AsyncOS operating system supports RFC 2821 compliant Simple Mail Transfer Protocol (SMTP) to accept and deliver messages. The IronPort appliance is designed to be easy to configure and manage. Most reporting, monitoring, and configuration commands are available through both the web-based graphical user interface (GUI) via HTTP and the interactive Command Line Interface (CLI) which is accessed from a direct serial connection for the system. The IronPort appliance also provides a logging capability, allowing the administrator to configure log subscriptions spanning the functionality of the entire system.

The TOE in its intended environment can be described in terms of the following components:

IronPort appliance hardware – Provides runtime environment for modified FreeBSDv4.11 operating system (AsyncOS) and includes getty administrator console interface (via the appliance serial port).

IronPort modified BSD operating system component – Provides runtime environment for AsyncOS application software component. The AsyncOS is a "hardened" operating system achieved by removing all unnecessary services. This increases security and optimizes system performance. The custom I/O-driven scheduler is optimized for concurrent I/O events required by the email gateway versus the preemptive time slicing of the CPU in traditional operating systems. AsyncFS, the file system underlying AsyncOS, is optimized for millions of small files and ensures data recoverability in the case of system failure.

IronPort AsyncOS application software component – Monitors SMTP protocol email network traffic sent and received on port 25 and takes action based on administratively-configurable rules. It provides web and terminal administrator console interfaces.

SMTP email server application – Used by email senders and receivers to send and receive email. It is also used by the TOE to send alerts to administrators.

Web browser application – Provides an environment for presenting GUI TSFI that are made accessible via the HTTP protocol.

Terminal application – Provides console interfaces that are accessible using a serial connected terminal.

6 Documentation

The following is a list of the documentation provided by the vendor with the TOE or available from the vendor to a purchaser of the IronPort Messaging Gateway. All of the documentation listed below was included in the scope of the evaluation.

The following documents are electronically available on a CD for all models:

- AsyncOS 5.1.2 Release Notes
- AsyncOS 5.1 Advanced User Guide
- AsyncOS 5.1 User Guide
- AsyncOS 5.1 Getting Started Guide
- AsyncOS 5.1 CLI Reference Guide

Additionally, the following documents are available in hardcopy format on the C350, C650, X1000 & X1050 appliances:

- AsyncOS 5.1.2 Release Notes
- AsyncOS 5.1 Advanced User Guide
- AsyncOS 5.1 User Guide

The C150 appliance includes the following documents in hardcopy format:

- AsyncOS 5.1.2 Release Notes

All of the above documents are available on the ironport.com web site. Access to the documents requires a login to the support portal with a customer key.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security audit, Identification and authentication, Security management, Protection of the TSF, Intrusion Detection (EXP). All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The evaluation team re-ran the entire manual test suite between three appliance models; X1050, C150 and C650. In addition to rerunning the vendor's tests, the evaluation team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the vendor's test suite, or areas where the ST did not seem completely clear. All were run as manual tests.

The vendor provided the IronPort appliances, management console, and the necessary computers for the test environment.

The following hardware is necessary to create the test configuration:

- TOE Hardware
  - IronPort hardware appliance versions X1050, C150 and C650
- IT Environment Hardware
  - Three commodity Windows PC's (one supporting as a Windows server)

The following software is required to be installed on the machines used for the test:

- TOE Software
  - Above TOE Hardware running AsyncOS version 5.1.2
- IT Environment Software
  - Software running on sender machine:
    - Windows operating system (XP)
    - MS Outlook mail client
    - An SMTP stress testing tool, such as multimail 2.0 (http://www.codeproject.com/KB/applications/multimail.aspx)
  - Software running on recipient machine, which is also used to access TOE admin interfaces:
    - Windows operating system (XP)
    - MS Outlook mail client
    - Web browser (MS IE 6.0)

        - Terminal software capable of communicating via serial interface (Hyperterminal).
    - Software running on bcc recipient machine:
        - Windows operating system (XP)
        - MS Outlook mail client
    - Software running on test machine #3, the bcc recipient machine:
        - Windows Server operating system (2003)
        - Groupware mail server (MS Exchange)

In addition to developer testing, the evaluation team conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

7.3 Vulnerability Testing

The evaluators developed vulnerability tests to address the Protection of the TSF security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

8 Evaluated Configuration

The evaluated configuration requires one IronPort hardware appliance versions C150, C350, C600, C650, X1000 or X1050 running IronPort AsyncOS software v5.1.2. The TOE can be configured to monitor email network traffic sent from the internal network to the external network, or vice versa. For specific configuration settings required in the evaluated configuration see IronPort AsyncOS 5.1 Common Criteria Guide for IronPort Appliances, Part Number 421-0073, dated April 24, 2008. A typical configuration is shown in Figure 1.

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.3, dated August 2005; the Common Evaluation Methodology (CEM), Version 2.3, dated August 2005; and all applicable International Interpretations in effect on December 5, 2005. The evaluation confirmed that the IronPort Messaging Gateway Version 5.1.2 product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 extended, and assurance requirements (Part 3) for EAL 2. The details of the evaluation are recorded in the CCTL's evaluation technical report; Final Evaluation Technical Report for the IronPort Messaging Gateway Version 5.1.2, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the IronPort Messaging Gateway Security Target Version 5.1.2 Security Target, Version 1.0, 20 June 2008.

The Validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validator 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 Validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of threats, policies, and assumptions, a statement of security requirements claimed to be met by the IronPort Messaging Gateway Version 5.1.2 product 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 ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. In addition the evaluation team ensured changes to the implementation representation are controlled and that TOE associated configuration item modifications is properly controlled.

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 deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed identification of the TOE and allows for detection of unauthorized modifications of the TOE. The evaluation team followed the IronPort AsyncOS 5.1 Advanced User Guide for IronPort Appliances, IronPort AsyncOS 5.1 User Guide for IronPort Appliances, IronPort AsyncOS 5.1 CLI Reference Guide, and IronPort AsyncOS 5.1

Common Criteria Guide for IronPort Appliances to test the installation procedures to ensure the procedures result in the evaluated configuration.

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 provides the security functions. The design documentation consists of a functional specification and high-level design documents. 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 ensured the adequacy of the guidance documents in describing how to securely administer the TOE. The IronPort AsyncOS 5.1 Advanced User Guide for IronPort Appliances, IronPort AsyncOS 5.1 User Guide for IronPort Appliances, IronPort AsyncOS 5.1 CLI Reference Guide, and IronPort AsyncOS 5.1 Common Criteria Guide for IronPort Appliances were assessed during the design and testing phases of the evaluation to ensure it was complete.

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 design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team exercised the complete Vendor test suite and devised an independent set of team test 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 exploitable flaws or weaknesses in the TOE based upon the developer vulnerability analysis and the evaluation team's vulnerability analysis, and 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 the entire set of the vendor's test suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the IronPort Messaging Gateway product meets the claims stated in the Security Target. The validation team also wishes to add the following notations about the use of the product.

- Administrators are warned to choose strong passwords. The TOE only requires passwords to be 6 characters or more. This is insufficient to meet the Strength of Function requirements unless additional complexity is assumed. Users are directed to page six of the IronPort AsyncOS 5.1 Common Criteria Guide for guidance in choosing appropriate passwords.

- The TOE uses e-mail messages for alerts, particularly to signal audit log reaching 90% capacity. This means that the TOE must rely on the IT environment to deliver these messages in a correct and timely manner. Users must confirm that this is a valid assumption.

11 Security Target

The Security Target is identified as IronPort Messaging Gateway Security Target Version 5.1.2 Security Target, Version 1.0, dated 20 June 2008. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2.

12 Glossary

The following definitions are used throughout this document:

CC	Common Criteria
CM	Configuration Management
DO	Delivery Operation
EAL	Evaluation Assurance Level
GUI	Graphical User Interface; a human interface that maps computer functions to graphical objects that the user can manipulate by means of a pointing device to perform tasks. Contrast with command-line interface, which requires the user to type text-based commands to perform tasks.
HTTP	HyperText Transfer Protocol
I/O	Input/Output
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirement(s)
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSC	TSF Scope of Control

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 2.3, August 2005.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Requirements, Version 2.3, August 2005.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Requirements, Version 2.3, August 2005.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

[5] IronPort Messaging Gateway Version 5.1.2 FINAL Non-Proprietary ETR – Part 1.

[6] IronPort Messaging Gateway Version 5.1.2 FINAL Proprietary ETR – Part 2 and Supplemental Team Test Plan.

[7] IronPort Messaging Gateway Version 5.1.2 Security Target, Version 1.0, 20 June 2008.

[8] IronPort AsyncOS 5.1 Common Criteria Guide for IronPort Appliances, Part Number: 421-0073, 10 June 2008.

[9] IronPort Vulnerability Analysis, Version 0.6, 10 June 2008.

[10] IronPort Strength of Function Analysis, Version 0.5, 10 June 2008.

[11] Evaluation Team Test Report for IronPort Messaging Gateway Version 5.1.2, Version 1.0, 24 April 2008.

[12] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.