National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

CipherTrust IronMail Secure Email Gateway Software Version 4.0.0

Report Number: CCEVS-VR-06-0017

Dated: 1 May 2006

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

Dr. Jerome Myers
The Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory
COACT CAFE Laboratory
Columbia, Maryland 21046-2587

Table of Contents

List of Figures

List of Tables

1 Executive Summary

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the CipherTrust IronMail Secure Email Gateway Software Version 4.0.0 at EAL2. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on May 1, 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.1, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is a set of software modules that reside within a hardware appliance and execute on top of a hardened operating system. IronMail Secure Email Gateway Software is proprietary application code developed by CipherTrust. The TOE is composed of the following modules within IronMail Secure Email Gateway Software: SMTP Proxy, Spam Queue, Content Filtering, Mail Policy Queue, SMTP Out, GUI Manager, CLI, Alert Manager, Watchdog Daemon, and Logging. The remainder of the IronMail Secure Email Gateway Software modules, along with the operating system, DBMS and hardware, were treated as part of the IT Environment for this evaluated TOE. The software is preinstalled in the distribution of the appliance.

The TOE acts as an email proxy to filter the exchange of email between servers and clients. The TOE examines email for spam and inappropriate content (as defined by the administrator) and filters email that violates the policies. Mail clients can fetch mail from the mail servers via POP3 (Post Office Protocol version 3), IMAP4 (Internet Message Access Protocol Version 4) and their secure variants (POP3S and IMAP4S) by proxying these connections through the IronMail appliance. For the TOE to provide the security functionality specified in the ST, the IT Environment must be correctly configured to ensure that all email traffic is proxied through the IronMail appliance.

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 desire 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 CCEVS' 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 organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifiers

Evaluation Identifiers for CipherTrust IronMail Secure Email Gateway Appliance Version 4.0.0	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	CipherTrust IronMail Secure Email Gateway Appliance Version 4.0.0
Protection Profile	N/A
Security Target	IronMail Secure Email Gateway Appliance Version 4.0.0 Security Target, dated April 27, 2006
Evaluation Technical Report	Evaluation Technical Report for the IronMail Secure Email Gateway Appliance Version 4.0.0, Document No. F2-0306-001, Dated May 1, 2006
Conformance Result	Part 2 conformant and EAL2 Part 3 conformant
Version of CC	CC Version 2.2 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on October 30, 2003.
Version of CEM	CEM Version 2.2 and all applicable NIAP and International Interpretations effective on October 30, 2003
Sponsor	CipherTrust 4800 North Point Parkway Suite 400 Alpharetta, GA 30022
Developer	CipherTrust 4800 North Point Parkway Suite 400 Alpharetta, GA 30022
Evaluator(s)	**COACT Incorporated** Robert L. Roland Anthony M. Busciglio Jeff Burke Christa Lanzisera
Validator(s)	**NIAP CCEVS** Royal Purvis Dr. Jerome Myers

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP/CCEVS Interpretations

National Interpretation I-0405
National Interpretation I-0427

International Interpretations

International Interpretation 003
International Interpretation 008
International Interpretation 016
International Interpretation 019
International Interpretation 031
International Interpretation 049
International Interpretation 064
International Interpretation 084
International Interpretation 085
International Interpretation 116
International Interpretation 127

3 Security Policy

The TOE resides in an appliance that functions as an email proxy. The TOE filters email according to policies configured by the administrator. The TOE also implements a security policy that restricts the management of the TOE to properly identified and authenticated administrators.

3.1 Administrative Security

The Administrative Security provides the necessary functions to allow an administrator to manage and support the TOE Security Function (TSF). Included in this functionality are the rules enforced by the TOE that define unacceptable email and the actions to be taken. Both a GUI and Command Line Interface (CLI) provide the necessary Administrative operator functions to allow an administrator to manage and support the TSF. The Administrator Guide provides information and guidance on the use of the GUI and CLI for Administrator functions.

The TOE maintains two roles for users: administrators and non-administrators. Administrators are required to identify and authenticate themselves to the IT Environment before allowing any modifications to TOE- managed TSF Data. The authentication data used for I&A, username and password, is maintained locally by the IT Environment.

Non-administrators are users who access the TOE via a remote system using POP3 or IMAP client software. Non-administrators have access to TOE-managed functions (specifically email filtering), but do not have authority to modify TOE-managed TSF data.

3.2 Email Filtering

The TOE filters email based upon spam indications, content, and policies configured by the administrator.

Spam is determined from the following:

- Messages explicitly identified as spam.
- Messages sent to specific addresses that are configured as spam traps.
- Message headers containing a specific value in the given field.
- Unknown or inconsistent source or destination addresses for the message

Content filtering is based on the following:

- Presence of specified content, such as offensive words in messages, or specified attachment types which are considered malicious or inappropriate for circulation. .
- Presence of specific attachment types in the message.

Additional policies may address:

- Messages sent by a specific user, group or domain.
- Messages destined to a specific user, group or domain.
- Messages containing specific text in the subject line.
- Messages containing encrypted data

3.3 Security Function Strength of Function Claim

No mechanisms in the TOE require an SOF claim. The claimed minimum strength of function is SOF-basic.

3.4 Protection Profile Claim

This Security Target does not claim conformance to any registered Protection Profile

4 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's IT Environment. This includes information about the connectivity, personnel, and physical side of the environment plus potential threats.

4.1 Connectivity Assumptions

The TOE is intended for use in areas that have physical control and monitoring. It is assumed that:

- The integrity of data maintained by the MySQL database is always ensured.
- DNS information received by the TOE is reliable.

4.2 Personnel Assumptions

The TOE is intended to be managed by competent non-hostile individuals. It is assumed that:

- Authorized administrators are non-hostile and are appropriately trained to use, configure and maintain the TOE.

4.3 Physical Assumptions

The TOE is intended for use in areas that have physical control and monitoring. It is assumed that:

- The TOE resides in a physically controlled access facility that prevents unauthorized physical access.

4.4 Potential Threats

Potential threats are:

- A threat agent may bypass one or more of the TOE's security functions and send malicious data to mail servers being protected by the TOE.

- A threat agent may take advantage of unexpected termination of one or more of the TOE's Security Functions (SF), and send inappropriate information through the TOE in violation of its mail policy.
- A threat agent may circulate dirty, offensive or proprietary information in violation of the TOE policy.
- A threat agent may modify the message content suitably or use variants in the sender or recipient information in order to defeat the protection services offered by the TOE.
- A threat agent may perform security relevant operations on the TOE without being held accountable for it.
- A threat agent may try to violate the mail dissemination policy of the TOE by sending information that the TOE may not want to forward or receive, either because of its origin, destination or subject content.
- A threat agent may send malicious content in an encrypted form in order to violate the TOE's content distribution policy.
- Threat agents may flood the TOE with spam, consuming resources such as memory, bandwidth, processor time and data storage and thus limit the TOE's ability to execute its security functions efficiently.
- A threat agent may download untrusted code to the TOE causing abnormal processes to be executed, which violate the integrity and availability of system assets.

5 Clarification of Scope

The TOE consists of a set of software modules that reside within a hardware appliance. All software is preinstalled in the distribution of the appliance. The following software modules were included in the TOE: SMTP Proxy, Spam Queue, Content Filtering, Mail Policy Queue, SMTP Out, GUI Manager, CLI, Alert Manager, Watchdog Daemon, and Logging. The remainder of the IronMail Secure Email Gateway Software modules, along with the operating system, DBMS and hardware, were treated as part of the IT Environment for this evaluated TOE. In particular, the following modules are outside of the scope of this evaluation:

- Mail Intrustion Detection,
- Anti-virus Queue,
- Anomaly Detection Engine, and
- Application Inspection Engine

Any security features provided by those other components of the appliance have not been evaluated as part of this evaluation.

The TOE requires that the IT Environment has been configured so that all email traffic is proxied through the TOE. This requirement relies upon functionality within the unevaluated portions of the IT Appliance to ensure that all email traffic that is directed through the appliance actually passes through the TOE (i.e. the software modules that were the subject of this evaluation.) The evaluation did not thoroughly analyze those components of the appliance that are part of the IT Environment to confirm that under all circumstances that would be the case, but the proper behavior was observed in all tests. In addition, this requires that other components of the network, in particular, the mail servers, be configured so that they will only accept network traffic from the IronMail appliance. The IT Environment requires that all servers with direct access to the backbone network be trusted to not impersonate the IronMail appliance and that any potentially malicious servers that might impersonate the IronMail appliance be separated from the local network by a firewall that blocks such attempts.

The vendor markets a separate appliance, the Central Management Console, for managing multiple TOEs in large customer applications. Although some documentation for this separate appliance is distributed with the TOE that documentation and the Central Management Console are not covered by this evaluation.

6 Architecture Information

The TOE is proprietary application code executing on top of a hardened FreeBSD kernel. The software runs on an appliance supplied by CipherTrust. The TOE acts as an email proxy to filter the exchange of email between servers and clients. The TOE examines email for spam and inappropriate content (as defined by the administrator) and filters email that violates the policies. The following two diagrams illustrate the placement of the physical and local placement of the IronMail appliance within a networked environment. Figure 1 illustrates a typical deployment. The IronMail appliance is one of many components potentially communicating over the backbone network. The appliance is protected from direct external network attacks by a network boundary protection device that provides firewall functionality.

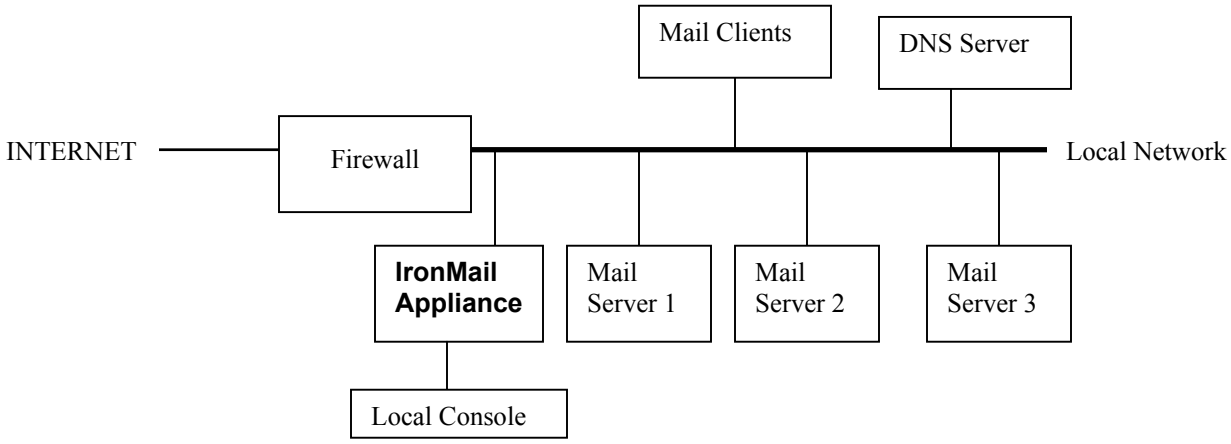

Figure 1: Typical Deployment

The local internal network relies upon the configuration of the various components to ensure that the mail clients cannot directly communicate with mail servers and the mail servers cannot directly communicate with each other. There are three components of the IT Environment with different expected behavior: the component outside of the network boundary, the component inside the network boundary but distinct from the IronMail appliance, and the component that resides upon the IronMail appliance. The environment outside of the network boundary is assumed to be potentially hostile, while the component inside the network boundary that is distinct from the IronMail Appliance is required to be well behaved enough to not bypass the IronMail Appliance for email traffic. This is primarily accomplished by configuration settings on the mail servers. The component of the IT Environment that resides upon the IronMail Appliance is distributed with the TOE and ensures that all email traffic that it receives is handled by the TOE. When the IT Environment is correctly configured, the evaluated configuration presents a logical network configuration illustrated in Figure 2.

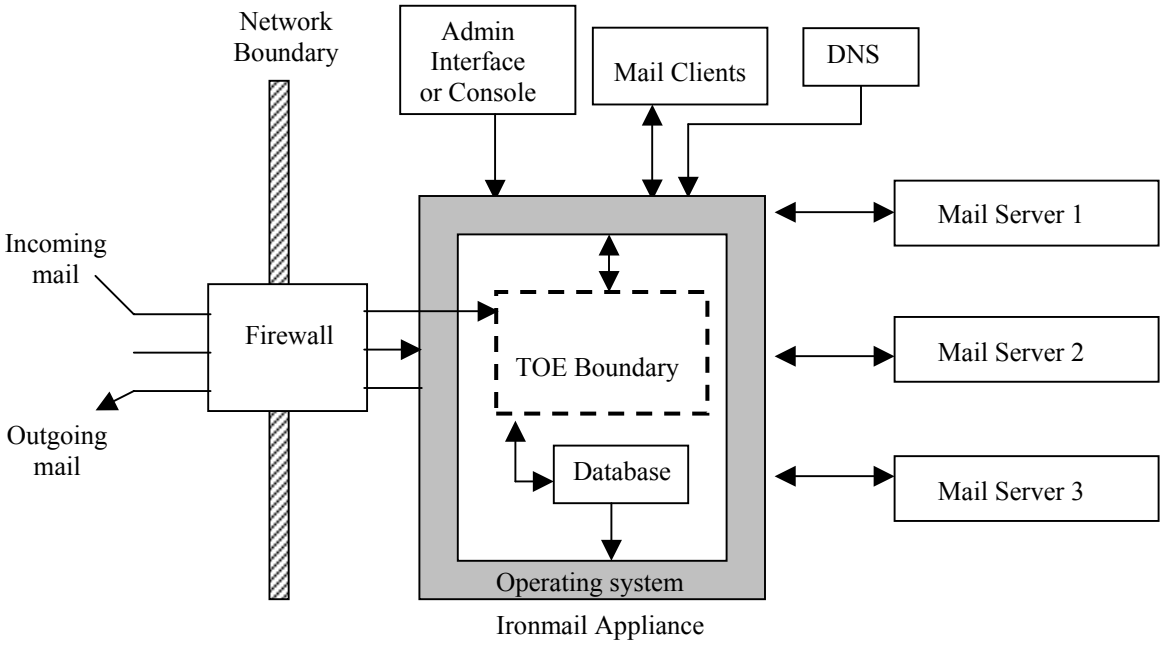

Figure 2: Logical View of Deployment

6.1 TOE Security Functions

The properties of the TOE necessary for the TOE to provide its security functionality are:

- The TSF will enforce email forwarding rules based on policies configured by the administrator.
- The TSF will provide functions and facilities necessary to support the authorized administrators that are responsible for the management of TOE security.
- The TSF will generate audits of security relevant events and make them available for review by administrators

6.2 IT Environment Security Functions

The properties of the IT operational Environment of the TOE necessary for the TOE to be able to provide its security functionality are:

- The IT Environment will require administrators to identify and authenticate themselves.
- The IT Environment will provide a trusted channel for communication between the TOE and remote IT products.

6.3 Non-IT Environment Security Functions

The properties of the non- IT operational Environment of the TOE necessary for the TOE to be able to provide its security functionality are:

- Those responsible for the TOE must ensure that all access credentials, such as passwords, are protected by the users in a manner that maintains IT security objectives.
- Those responsible for the TOE and hardware required by the TOE must ensure that the TOE is delivered, installed, configured, managed, and operated in a manner which maintains IT security objectives.

- Those responsible for the TOE must ensure that the TOE modules critical to security policy are protected from physical attack that might compromise the IT security objectives.
- Those responsible for the TOE will be properly trained and provided the necessary information that ensures secure management of the TOE and the IT Environment.

6.4 Physical Boundary

The TOE is delivered pre-installed on the IronMail appliance. The TOE processor is on a card in the appliance along with the operating system and application modules outside the TOE boundary. Figure 3 illustrates the modules of the TOE as well as their relationship to the IT Environment. Shaded items are part of the IT Environment.

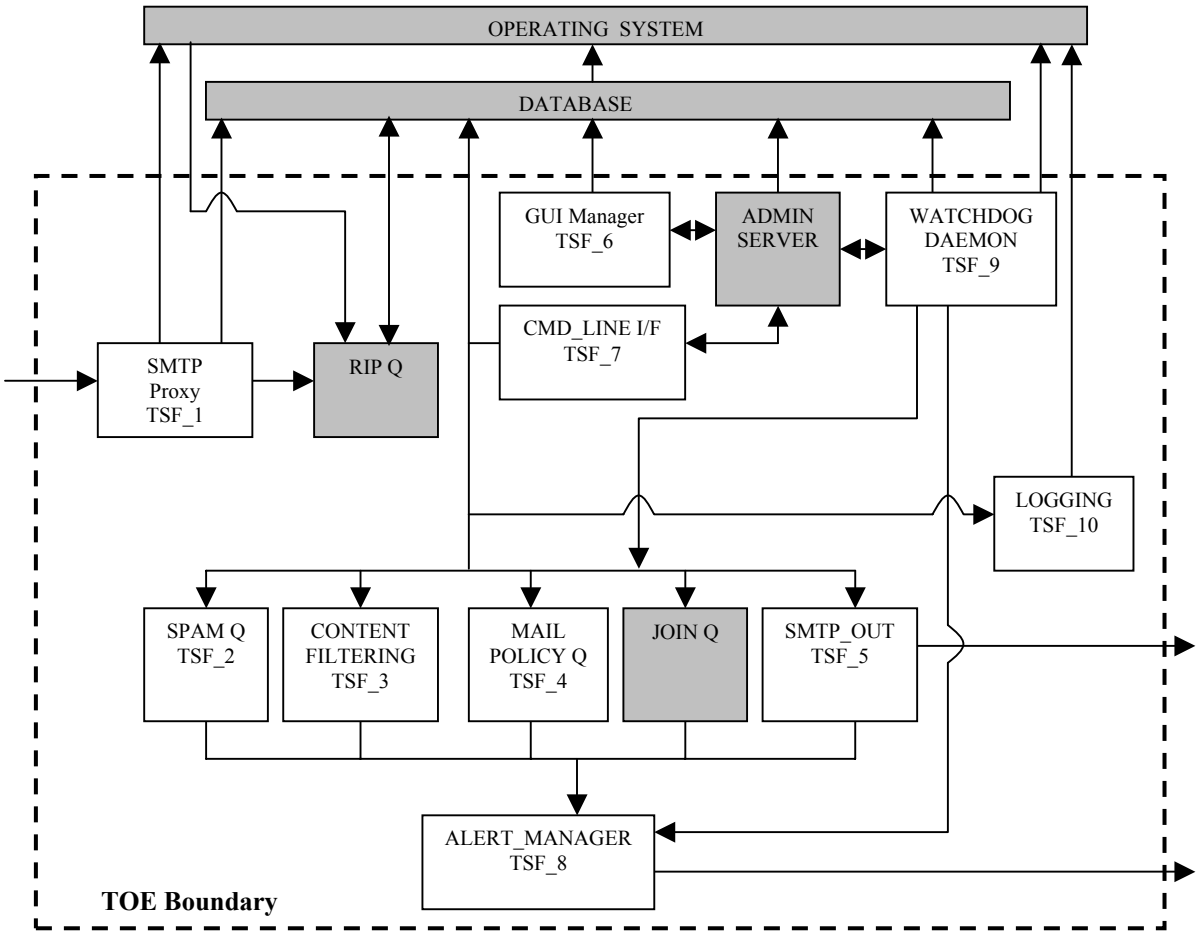

Figure 3: TOE Physical Boundary

6.5 Logical Boundary

The following security functionality is included within the TOE's logical boundary:

- Spam filtering - The Spam Queue uses a variety of tools to inspect messages for characteristics of spam. When a message is found to be spam-like, an administrator-defined action such as drop, quarantine or rename is performed on it.
- Content filtering - The Content Filtering queue scans the message contents for specific text or attachment types, which are considered malicious or inappropriate for circulation

by the TOE. The content filtering queue operates over Attachment Filtering and Content Filtering Policies, each of which can be selectively enabled or disabled.

- Mail policy filtering - This Mail Policy queue allows the TOE to specify Mail Monitoring rules, which allow specific action to be taken on a message based on its sender, recipient or subject line content.
- GUI Manager - The GUI Manager provides a web-based browser interface for the administrators to set and configure the various queue processes. Users may access the GUI Manager through a web browser by connecting to the IronMail appliance's configured address using the secure HTTP protocol.
- Command Line interface - The TOE allows administrators to access much of the functionality found in the graphical user interface (GUI) from a command line. Once the administrator enters a username and password, which are validated by the IT environment, various TOE operations may be accessed by simple commands, where these commands are composed of a command word followed by one or more parameters.
- Alert Manager - The Alert Manager delivers alerts based on policy configurations. The TOE constantly monitors its core subsystems, as well as its ability to communicate with internal mail servers. If any part of the TOE's functionality fails to perform as designed, the TOE generates an alert.
- Logging Engine - The Logging Engine performs all logging and auditing of the Administrator activities. The logging framework allows the administrator to control the output logs and configure them externally through customizable log levels and output mechanisms. The TOE can generate daily reports in HTML, showing detailed information about the incoming and outgoing messages processed by the TOE each day.

7 Product Delivery

The TOE is delivered preinstalled on a CipherTrust IronMail appliance. Purchasers must specify IronMail Secure Email Gateway Software Version 4.0.0 be installed on the appliance when it is shipped. The appliance is delivered via Federal Express with tamper evident tape sealing the package in accordance with the vendor's delivery procedures.

The delivered TOE documentation consists of:

- IronMail 4.0.0 Setup Guide
- IronMail 4.0.0 Product Documentation CD-ROM disc
- Customer letter (information concerning license keys)
- 'Stop Sign' notice with product warnings
- Packing slips (2)

The CD-ROM disc contains the following three documents in electronic form:

- Centralized Management Console User Manual Version 1.5.0
- Manual for IronMail 4.0.0 Version 4.0.0
- QuickStart IronMail 4.0.0 Version 4.0.0

The IronMail Manual and the QuickStart Manual are part of the evaluated TOE documentation. However, the Central Management Console User Manual is not part of the evaluated documentation. The Central Management Console is a separate appliance that the vendor markets to manage multiple TOEs in large customer applications.

8 IT Product Testing

Testing was performed on February 22, 2006 at the CipherTrust facility in Alpharetta, GA. Testing was performed at the vendor facility due to the quantity and types of equipment required to reproduce the vendor tests. Two COACT employees performed the tests. All test configurations operated properly and tests were completed in an expeditious manner.

8.1 Evaluator Functional Test Environment

In addition to the IronMail appliance running IronMail Secure Email Gateway Software Version 4.0.0, the functional test configuration included:

- PCs, with the following software/tools installed:
  - Microsoft Office Suite
  - HyperTerminal
  - Ethereal version 0.10.11
  - Nmap version 1.3.1
  - SSH Software
- 3 - Email Servers
- DNS Server
- Router
- Ethernet Cables
- Load generator
- Software Update and License Generator Server
- LDAP Server
- SCP and FTP servers.
- Syslog Server
- SNMP Server
- Mail Gulper and DSN Generation Server (mail generator)

Figure 4 graphically displays the test configuration used for functional testing.

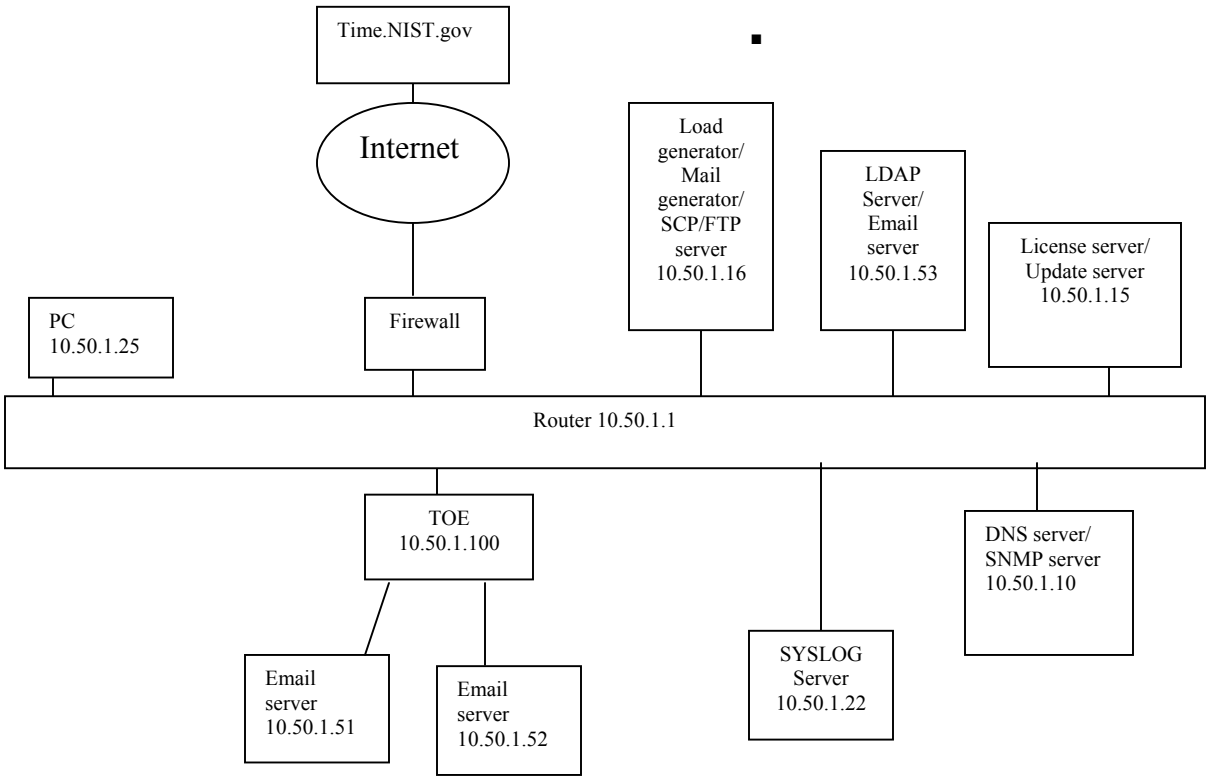

Figure 4: Test Configuration

8.2 Test Assumptions

The functional test environment/configuration requires no test specific assumptions outside of those identified in the ST. The test bed setup used for this set of tests is the same as that used for the functional test suite.

Some subsystems such as the MAIL_POLICY_Q (TSF_4) have licensing requirements before they can be used in an operational environment. The tests assume that such licenses have already been procured.

8.3 Repeated Developer Tests to Confirm Developer Test Results

This section lists tests required to confirm the developer test results. The evaluation team selected to reproduce all the vendor tests because of the dependencies between the tests.

8.4 Functional Test Results

All tests were performed satisfactorily and the results were as expected. The TOE passed all tests. The procedures followed to execute these tests and detailed results are presented in the CipherTrust IronMail Secure Email Gateway Software Version 4.0.0 Functional Test Report for Common Criteria EAL2 Evaluation.

8.5 Evaluator Independent Testing

The tests chosen for independent testing allow the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests is to

give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allow for a finer level of granularity of testing compared to the developer's testing, or provide additional testing of functions that were not exhaustively tested by the developer. The tests allow specific functions and functionality to be tested. The tests reflect knowledge of the TOE gained from performing other work units in the evaluation. For example, specific TSFI behaviors were identified while performing the ADV work units, and tests have been developed to test specific behaviors.

To determine the independent testing to be performed, the evaluators first assessed the level of developer testing corresponding to all TSFIs. The Independent Tests performed were:

- Verify the TOE's ability to drop a message after a potential security violation is identified in the Mail Policy
- Verify the TOE's ability to deliver the original message but also send a copy of it as an attachment to an alternate email address after a potential security violation is identified in the Mail Policy

8.5.1 Evaluator Independent Test Environment

The test environment used to conduct these tests was the same as the environment used in the reproduced vendor testing.

8.6 Evaluator Independent Test Results

All tests were performed satisfactorily and the results were as expected. The TOE passed all tests. The procedures followed to execute these tests and detailed results are presented in the CipherTrust IronMail Secure Email Gateway Software Version 4.0.0 Functional Test Report.

8.7 Evaluator Penetration Tests

8.7.1 Evaluator Assessment of Developer Analysis

The evaluator examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. After consulting the sources identified by the developer used during the initial vulnerability analysis, the evaluator consulted other vulnerability relevant sources of information to verify that the developer considered all available information when developing the non-exploitation rationale. These additional sources include:

- https://cirdb.cerias.purdue.edu/coopvdb/public/
- http://xforce.iss.net/
- http://nvd.nist.gov/
- http://www.cve.mitre.org/

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluator made an assessment of the rationales provided by the developer indicating that the vulnerability is non-exploitable in the intended environment of the TOE. Any possible vulnerability that requires further evaluator analysis, such as, an Attack Potential Calculation was identified as suspect.

The evaluator found six of the developer rationales describing why a particular possibly relevant vulnerability of the TOE was not exploitable to be suspect. Therefore the evaluator tested the TOE to ensure the TOE was properly resistant to the relevant vulnerabilities.

8.7.2 Additional Vulnerabilities

While verifying the information found in the developer's vulnerability assessment the evaluator conducted a search to verify if additional obvious vulnerabilities exist for the TOE. This search included examining the websites identified in section 8.7.1 of this document. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerability. The scope of this analysis included potential obvious vulnerabilities in the component of the IT Environment that reside within the IronMail appliance in its evaluated configuration. The additional analysis conducted by the evaluator identified two additional vulnerabilities that may possibly be relevant to the TOE. Therefore the evaluator tested the TOE to ensure the TOE was properly resistant to the additional identified vulnerabilities. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator.

8.8 Evaluator Penetration Test Identification

As a result of the evaluator's examination of the developer's vulnerability analysis and the independent search for obvious TOE vulnerabilities, the evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the vulnerabilities. The following Penetration tests were performed by the evaluator:

- Verify that the version of Open SSL used with IronMail is not one of the versions of Open SSL affected by the identified vulnerabilities
- Verify that the version of Apache used with IronMail is not one of the versions of Apache affected by the identified vulnerabilities
- Verify that IronMail does not support SSL v2
- Verify that IronMail does not support FFS.

8.9 Actual Penetration Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to the all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the document *Evaluation Technical Report for the IronMail Secure Email Gateway Appliance Version 4.0.0 contains* the verdicts of "PASS" for all the work units.

The evaluation determined the product to meet the requirements for EAL 2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10 Validator Comments

The validator does not have any supplemental comments other than those already captured in the Clarification of Scope section of this report on page 5.

11 Security Target

The Security Target document, IronMail Secure Email Gateway Software Version 4.0.0 Security Target dated April 27, 2006 is incorporated here by reference.

12 List of Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DBMS	Database Management System
DNS	Domain Name Services
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTML	Hypertext Markup Language
IMAP	Internet Message Access Protocol
IT	Information Technology
I&A	Identification and Authentication
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
POP3	Post Office Protocol 3
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSFI	TSF Interface
TSP	TOE Security Policy

13 Bibliography

The following list of standards was used in the evaluation of the IronMail Secure Email Gateway Software Version 4.0.0:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 2.2, dated January 2004
- Common Methodology for Information Technology Security Evaluation, Part 1, Version 2.2, dated January 2004
- Common Methodology for Information Technology Security Evaluation, Part 2, Version 2.2, dated January 2004
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000