National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

FireEye v.6.0

Report Number: CCEVS-VR-VID10458-2011
Version 1.0
September 21, 2011

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 6940
Fort George G. Meade, MD 20755-6940

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is FireEye v.6.0. The TOE was evaluated by the Booz Allen Hamilton Common Criteria Test Laboratory (CCTL) in the United States and was completed in September 2011. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3. The evaluation was for Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.2 (Flaw Reporting Procedures). The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org).

FireEye detects malware by analyzing suspicious e-mail and network flows in virtual victim machines. The FireEye appliance identifies malicious attacks, including those targeting web browsers. It secures against both widespread and targeted network malware without relying on manual IT analysis. Signature matching is used in the IDS process, but the IDS process does not rely on the signature matching components or updated signatures to function properly. After definitively confirming a targeted malware attack, the FireEye appliance is integrated into a network to block the attack, quarantine the infected host and alert Administrators to the incident.

The FireEye appliance, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the TOE's Security Target.

The cryptography used in this product has not been FIPS-certified, nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The technical information included in this report was largely derived from the Evaluation Technical Report and associated test reports produced by the evaluation team. The FireEye Security Target version 1.1, dated 11 May 2011 identifies the specific version and build of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the FireEye appliance by any agency of the US Government and no warranty of the product is either expressed or implied.

2 Evaluation Details

Evaluated Product	FireEye v.6.0
Sponsor & Developer	FireEye, Milpitas, CA
CCTL	Booz Allen Hamilton, Linthicum, Maryland
Completion Date	September 2011
CC	*Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009

Interpretations	None.
CEM	*Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Evaluation Class	EAL2 Augmented ALC_FLR.2
Description	The TOE is the FireEye appliance, which is a security software product developed by FireEye, Inc. as an Intrusion Detection System.
Disclaimer	The information contained in this Validation Report is not an endorsement of the FireEye product by any agency of the U.S. Government, and no warranty of the IDS product is either expressed or implied.
PP	US Government Protection Profile Intrusion Detection System System for Basic Robustness Environments v.1.7
Evaluation Personnel	Kevin Micciche Amit Sharma Jeremy Sestok
Validation Body	NIAP CCEVS

2.1 Threats to Security

Table 2 summarizes the threats that the evaluated product addresses.

Table 2 – Threats

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.
A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
Improper security configuration settings may exist in the IT System the TOE monitors.
Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

Vulnerabilities may exist in the IT System the TOE monitors.
The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
Inadvertent activity and access may occur on an IT System the TOE monitors.
Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3 Identification

The product being evaluated is FireEye v.6.0.

4 Security Policy

4.1 Security Audit

The e-mail MPS, web MPS, Malware-Analysis, and CMS instances all perform their own auditing. Each appliance audits its own behavior and stores its syslog, or audit data in its respective internal database. CMS receives detections of audit events from all other instances and can display the aggregated audit data through reports via the CLI or WebUI. Administrators can either use the CLI or WebUI on each instance of FireEye to view and sort audit data for that particular appliance, or they use the CLI or WebUI on the CMS to view audit data for all FireEye appliances. Audit data can be sorted based on the following: date and time, subject identity, event type, and outcome of event. Audit data is provided to the Administrator as columnar results as Linux syslog file data.

All user actions and cryptographic actions on the TOE are audited by the CLI. The CLI is a universal backend for WebUI and LCD commands, which are translated into CLI commands and forwarded to the TOE component where they are executed, Config or Events Storage.

4.2 Identification and Authentication

All users must be identified and authenticated to the TOE via username and password before being allowed to perform any actions on the TOE. The exception to this is that users are allowed to perform TOE functions via the password protected LCD panel without identifying themselves to the TOE. Since a username is not required to authenticate to the LCD panel, it is assumed that individuals with physical access to the TOE will also be users of the TOE. The LCD panel is meant for initial setup only, and as such is not part of the TSF for the evaluated configuration. The TOE maintains specific security attributes about users in order to correctly identify them with their TOE-associated abilities as well as for future authentication attempts. If a user enters incorrect credentials multiple times, he or she is forbidden from re-attempting to authenticate until a set amount of time has elapsed. The number of incorrect attempts allowed is pre-determined by the Administrator. In addition, the TOE appliances authenticate to the

MPC Network and the MPC Network authenticates to the TOE appliances in order to pass updates to the Updates component. This authentication is performed through the use of vendor supplied username and password and through the use of certificates.

4.3 Security Management

The TOE maintains two roles – Administrator and Monitor. Users under the Administrator role have the ability to perform all administrative functions (e.g. user management, audit management) and monitoring functions.

Users under the Monitor role are able to perform all changes pertaining to monitoring functionality, but are not allowed to perform any other administrative functionality (i.e. user management, audit configuration). Users can perform limited configuration functions via the LCD panel. All functions performed from the LCD panel can also be performed from the WebUI or CLI once the user has authenticated to the WebUI or CLI. The LCD panel is meant for initial setup only, and therefore is not included in the evaluated configuration. Additionally, most functions performed from the CLI can also be performed from the Web UI, with the exception of reviewing audit data.

4.4 Protection of the TSF

The TOE is expected to ensure the security and integrity of all data that is stored locally and accessed remotely. The TOE ensures that all local system data is available to any remote trusted IT products (i.e. other TOE components). Additionally, the transmitted and received data is protected against unauthorized viewing by third parties through the use of encryption. All data transferred is monitored for changes during transmission, and integrity verification measures are taken if modifications have been detected. Time stamps are added to all audit logs and system events in order to maintain accurate records. The system clock time is kept accurate by automatically getting accurate time readings from the NTP Server to which the FireEye appliance is connected.

4.5 Encrypted Communications

The TOE is expected to utilize sufficient security measures to protect its data in transmission, which means it needs to utilize cryptographic methods and trusted channels. The TOE generates cryptographic keys to protect transmitted data. The TOE is also responsible for destroying these same keys when they are no longer needed.

Administrators and Monitors who access the TOE remotely rely on a trusted path to secure their communication with the TOE via the WebUI. This trusted path is established using OpenSSL 0.9.8e. OpenSSL is also used for protected communication to/from the MAX Network. Additionally, users who access the TOE via the CLI must use OpenSSH 3.8.1p1 functionality to secure their communications with the TOE. OpenSSH functionality is also used for protection of data transferred between TOE components.

4.6 Intrusion Detection System

The TOE monitors the network's web and e-mail traffic for detected malicious code, service requests, and service configuration, among other information. Anything that the TOE determines is malicious becomes an event. General information is recorded for

each event, and each type of event has more specific classifications that are recorded. See Section 9.1.6 for more information on the data that is collected by the TOE.

The TOE analyzes recorded data on a statistical, signature, virtual machine, and/or heuristic basis. Each analytical result is recorded with basic information, as well as changes in the OS or network, and whether or not a buffer overflow was attempted. Administrators and Monitors are able to view the data via the WebUI or CLI. Once a threat has been detected, the system sends an alarm to the Administrator or Monitor. Depending on the deployment (inline or SPAN/tap), the TOE is also capable of dropping the traffic that was shown to represent a threat.

Data in the system is protected from unauthorized deletion or modification. System data is archived to a local file once the predefined number of events has been recorded to the internal database. An alarm is used to alert Administrators and Monitors of this issue.

5 Assumptions

5.1 Intended Usage Assumptions

Table 1 – Intended Usage Assumptions

The TOE has access to all the IT System data it needs to perform its functions.
The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
The TOE is appropriately scalable to the IT System the TOE monitors.
There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) on the TOE.
The TOE will connect to the MAX Network for signature updates and to upload detected malware.

5.2 Personnel Assumptions

Table 2– Personnel Assumptions

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
The TOE can only be accessed by authorized users.

5.3 Physical Assumptions

Table 3 – Physical Assumptions

The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

6 Clarification of Scope

The TOE includes all the code that enforces the policies identified (see Section 4).

The evaluated configuration of the TOE includes the FireEye v.6.0 product that is comprised of the following:

- 2000 Series Appliance
- 4000 Series Appliance
- 5000 Series Appliance
- 7000 Series Appliance
- 8000 Series Appliance

6.1 System Requirements

The following components are provided on the appliances for the TOE:

Hardware Components

FireEye running on a 1000 Series appliance

- Traffic Monitoring Ports: 0
- Physical Appliance Size: 1U
- LCD Panel: Yes
- Throughput: 50Mbps or handles up to 25 appliances as CMS

FireEye running on a 2000 Series appliance

- Traffic Monitoring Ports: 2
- Physical Appliance Size: 1U half-depth
- LCD Panel: No
- Throughput: 50 Mbps

FireEye running on a 4000 Series appliance

- Traffic Monitoring Ports: 4
- Physical Appliance Size: 1U half-depth
- LCD Panel: Yes
- Throughput: 250 Mbps

FireEye running on a 5000 Series appliance

- Traffic Monitoring Ports: 4
- Physical Appliance Size: 2U half-depth
- LCD Panel: Yes
- Throughput: 200,000 emails per day

FireEye running on a 7000 Series appliance

- Traffic Monitoring Ports: 4
- Physical Appliance Size: 2U half-depth
- LCD Panel: Yes
- Throughput: 1 Gbps

FireEye running on an 8000 Series appliance

- Traffic Monitoring Ports: 4
- Physical Appliance Size: 2U half-depth
- LCD Panel: Yes
- Throughput: 500,000 e-mails per day

Note: *Software Requirements are not needed as the product is shipped on hardware. All software is provided with the TOE and no additional software can be added.*

In the evaluated configuration, the TOE will consist of three machines running the analysis and central management functions of the TOE. No non-TOE software is required to run the TOE.

7 Architectural Information

The TOE's boundary has been defined in Figure 1.

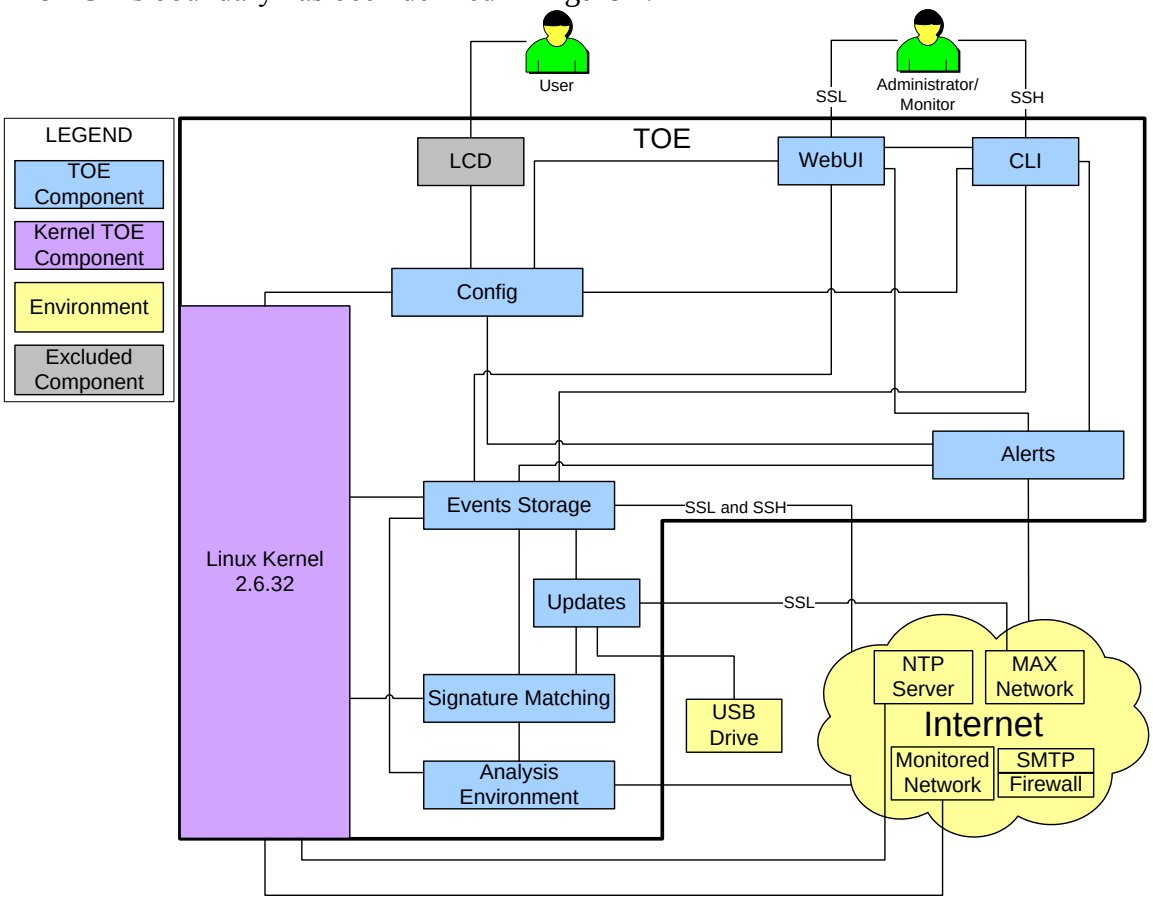

Figure 1 – TOE Boundary for MPS and Malware-Analysis Appliances

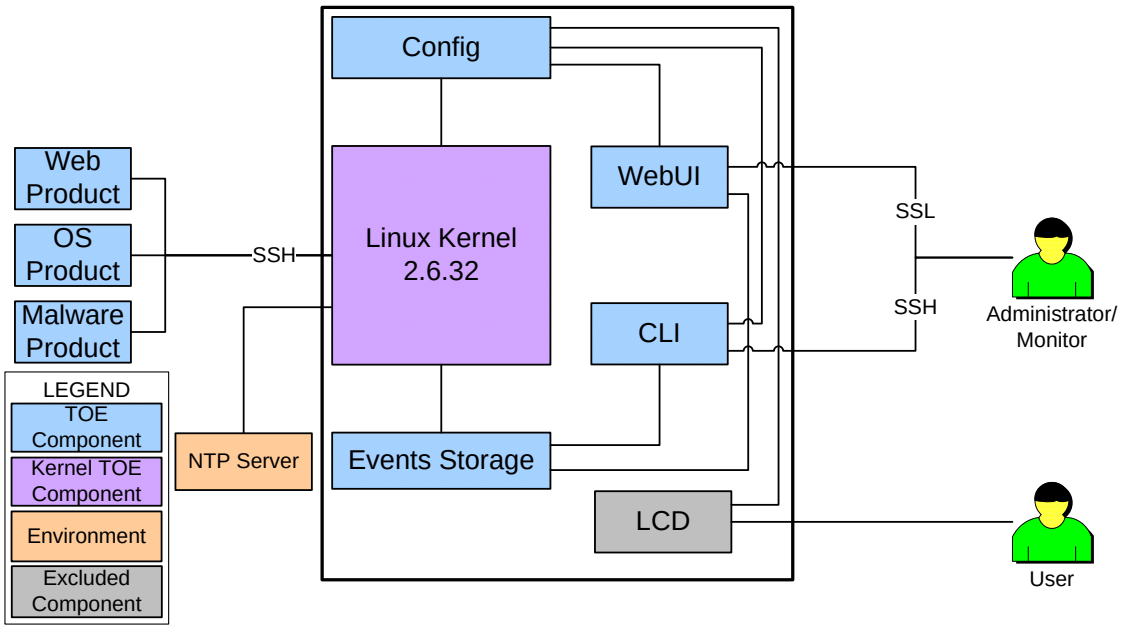

Figure 2 – Central Management System TOE Boundary

7.1 TOE Components

7.1.1 Config

Component of FireEye that contains and modifies all FireEye system configurations, user configurations and auditing options.

7.1.2 CLI

Command-line interface that uses OpenSSL SSH functionality and allows Administrators to perform administrative functions. Monitors do not have access to the CLI.

7.1.3 WebUI

Browser-based interface that OpenSSL and allows Administrators to perform administrative functions, and allows both Administrators and Monitors to perform monitoring functions.

7.1.4 Linux Kernel v.2.6.32

The Kernel is Linux v2.6.32 and holds basic system functionality that is important in the TOE. The kernel is physically contained in the FireEye appliance and provides OS functionality to the rest of the TOE, including capture, clock, and audit functionalities. The basic functionality of the operating system beyond this is not security relevant for the evaluated configuration.

7.1.5 Analysis Environment

Creates and manages virtual machines that are used for simulated traffic to determine if suspicious traffic and binaries are malicious in nature.

7.1.6 Signature Matching

Checks data against known malware and botnet traffic to determine if the traffic needs to be run by the analysis environment.

7.1.7 Events Storage

Records information regarding infections and callbacks on systems within the network, and applies basic identifying information.

7.1.8 Alerts

Mechanism for notifying Administrators or Monitors in the event of a detected infection or callback.

7.1.9 Internet

The Internet contains the Monitored Network, the NTP Server, and the MAX Network. Additionally, the TOE can configure alerts to be sent to the Internet via SMTP, SNMP, and HTTP POST methods. The command line SMTP client used for email notifications is v2.5.1.

7.1.10 Monitored Network

In the evaluated configuration, all internet traffic passing through the switch FireEye is connected to is also passed into FireEye. This data gets sent through the Statistical, Signature, and Heuristic analysis. If the traffic is determined to be suspicious from using any of the previous analysis methods, then the traffic is sent through Virtual Machine analysis. All data transferred, including but not limited to URLs, executables, and code, is evaluated.

7.1.11 NTP Server

FireEye appliances utilize NTP Servers by default. An NTP Server keeps the system up to date with the latest system time from their servers. In this case, it is used for accurate timestamps on audit and system data.

7.1.12 FireEye Malware Protection Cloud (MPC) Network

The FireEye MPC Network circulates the latest malware analysis intelligence to participating FireEye appliances, ensuring customer data, intellectual property, and resources are safeguarded from the threat of network malware and botnets. The ability to connect to the MPC Network to receive signature updates and to upload detected malware is included in the evaluated configuration. The MPC Network itself is a component of the operational environment in the evaluated configuration because it is a server that sits in a server room at FireEye HQ. It's a trusted IT product with which the TOE can interact, but it's not considered part of the TOE since it belongs to the vendor and not the customer.

7.1.13 USB

While system updates can come from the Internet, a user can also load the updates onto a USB drive and plug it into the FireEye appliance physically. This allows users an

alternate way to install updates, which must be encrypted on upload and decrypted on install. USB drives also cannot be mounted to install untrusted software to FireEye.

8 Documentation

The documents were evaluated to satisfy assurance requirements:

Component	Document(s)	Rationale
ADV_ARC.1 Security Architecture Description	FireEye v.6.0 TOE Design Specification Version 1.1	This document describes the security architecture of the TOE.
ADV_FSP.2 Security-enforcing functional specification	FireEye v.6.0 Functional Specification Version 1.1	This document describes the functional specification of the TOE with complete summary.
ADV_TDS.1 Basic Design	FireEye v.6.0 TOE Design Specification Version 1.1	This document describes the architectural design of the TOE.
AGD_OPE.1 Operational User Guidance	• Email MPS 5000-8000 Quick Start Guide • FireEye 6.0 CLI Guide • FireEye CMS Operator's Guide 6.0 • FireEye Email MPS Operator's Guide 6.0	This document describes the operational user guidance for FireEye v.6.0.
AGD_PRE.1 Preparative Procedures	• FireEye Web MPS 6.0 Operator's Guide • MPS 1000-2000 Quick Start Guide • MPS 4000-7000 Quick Start Guide • Evaluated Configuration for FireEye v.6.0	This document describes the preparative procedures that need to be done prior to installing FireEye v.6.0.
ALC_CMC.2 Use of a CM system	FireEye Configuration Management Plan	This document describes the authorization controls for the TOE.
ALC_CMS.2 Parts of the TOE CM coverage	FireEye Configuration Management Plan	These documents describe the CM scope of the TOE.
ALC_DEL.1 Delivery Procedures	FireEye Configuration Management Plan	This document describes product delivery for FireEye v.6.0 and a description of all procedures used to ensure objectives are not compromised in the delivery process.
ALC_FLR.2 Flaw reporting procedures	FireEye Configuration Management Plan	This document describes the processes taken for flaw remediation for the TOE.
ASE_CCL.1 Conformance Claims	FireEye v.6.0 Security Target v1.1	This document describes the CC conformance claims made by the TOE.
ASE_ECD.1 Extended Components Definition	FireEye v.6.0 Security Target v1.1	This document provides a definition for all extended components in the TOE.
ASE_INT.1 Security Target Introduction	FireEye v.6.0 Security Target v1.1	This document describes the Introduction of the Security Target.
ASE_OBJ.2 Security Objectives	FireEye v.6.0 Security Target v1.1	This document describes all of the security objectives for the TOE.
ASE_REQ.2 Derived Security Requirements	FireEye v.6.0 Security Target v1.1	This document describes all of the security requirements for the TOE.

Component	Document(s)	Rationale
ASE_SPD.1 Security Problem Definition	FireEye v.6.0 Security Target v1.1	This document describes the security problem definition of the Security Target.
ASE_TSS.1 TOE Summary Specification	FireEye v.6.0 Security Target v1.1	This document describes the TSS section of the Security Target.
ATE_COV.1 Evidence of Coverage	Test Plan for FIREEYE, INC. FireEye v.6.0	This document provides an analysis of coverage for the TOE.
ATE_FUN.1 Functional Testing	Test Plan for FIREEYE, INC. FireEye v.6.0	This document describes the functional tests for the TOE.
ATE_IND.2 Independent Testing - sample	Independent Testing Plan for FIREEYE, INC. FireEye Series v.6.0	This document describes the independent testing for the TOE.
AVA_VAN.2 Vulnerability Analysis	Vulnerability Analysis for FIREEYE, INC. FireEye v.6.0	This document describes the vulnerability analysis of the TOE.

Table 8 – Assurance Documents Evidence

These documents were provided as evaluation evidence, only the documents under the ASE and AGD Classes (bolded and underlined) are provided to customers who have purchased the TOE.

9 TOE Acquisition

The NIAP-certified FireEye product is acquired via normal sales channels, and physical delivery of the TOE is coordinated with the end customer by FireEye, Inc.

10 IT Product Testing

The test team's test approach is to test the security mechanisms of the FireEye v.6.0 by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. Each TOE external interface is to be described in FireEye design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, TOE Design (TDS), Functional Specification (FSP), Security Architecture (ARC) and the vendor's test plans will be used to demonstrate test coverage of all EAL2 requirements for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.
- provide IDS functionality to the TOE

Security functional requirements will be determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

The evaluation team will create a test plan that contains a sample of the vendor functional test suite, and supplemental functional testing of the vendors' tests. Booz Allen will also perform vulnerability assessment and penetration testing.

10.1 TEST METHODOLOGY

10.1.1 Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of FireEye. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The Evaluation Team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications
  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network. This test was specialized for the following interfaces:
  - WebUI
  - CLI
- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
- Vulnerability Scanner (Nessus)
  This test used the Nessus Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE. The scanner probes a wide range of vulnerabilities that includes but is not limited to the following:

Backdoors	Gain root remotely	RPC
CGI abuses	General	Settings
Denial of Service	Miscellaneous	SMTP Problems
Finger abuses	Netware	SNMP
Firewalls	NIS	Untested
FTP	Port scanners	Useless services

Gain a shell remotely	Remote file access

- TCP Malformed Packet Flooding
  This test attempted to shutdown TOE resources by flooding the network with large amounts of malformed tcp packets.
- Unauthenticated Access / Directory Traversal Attack
  This test used "URL hacking" to attempt to access protected TOE resources by injecting unexpected input into requests that were sent to the TOE. This was done using two different approaches to URL exploitation.
  - The first part attempted to access protected TOE resources as an unauthenticated outsider.
  - The second part attempted to access local TOE resources that should be protected from any remote access (unauthenticated and authenticated).
- SQL Injection / Cross Site Scripting Attack / Cross Site Request Forgery (Paros, WebScarab)
  This test executed automated SQL Injection and Cross Site Scripting attacks against the TOE. The evaluators determined any fields or variables that could be prone to attack. They then used a scanner, which contained a large database of standard strings that are used for testing SQL Injection and Cross Site Scripting issues. These strings were input into the various fields and variables and the output was analyzed for inconsistencies.
- Web Server Vulnerability Scanner (Nikto)
  This test used the Nikto web server vulnerability scanner to test for any known vulnerabilities that could be present in the TOE's web interfaces. This scanner probed a wide range of vulnerabilities that included the following:

File Upload.	Denial of Service.
Interesting File / Seen in logs.	Command Execution / Remote Shell.
Misconfiguration / Default File.	SQL Injection.
Information Disclosure.	Authentication Bypass.
Injection (XSS/Script/HTML).	Software Identification
Remote File Retrieval	Remote source inclusion.

- Vulnerability Scanner (Retina)
  This test uses the Retina Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE.
  The scanner probes a wide range of vulnerabilities that includes but is not limited to the following:

Accounts	DoS	Service Control
Anti-Virus	IP Services	Spyware
Backdoors	Registry	Web Services
CGI Scripts	Remote Access	CVE Issues
Database Issues	RPC Services	SecurityFocus BID Issues

10.1.2 Vulnerability Results

During vulnerability analysis of the TOE, no issues were found that would require patching of the product or configuration changes within an admin supplemental guide.

11 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the FireEye v.6.0 TOE meets the security requirements contained in the Security Target.

The criteria against which the FireEye TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the FireEye v.6.0 TOE is EAL2 augmented with ALC_FLR.2. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed in September 2011. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

12 Validator Comments/Recommendations

12.1 Secure Installation and Configuration Documentation

The "Evaluated Configuration for FireEye v.6.0" defines the recommendations and secure usage directions for the TOE as derived from testing and should be obtained from the vendor.

12.2 Supported Cipher Suites

The TOE supports several cipher suites for SSL and SSH with AES 256 bit and AES 128 bit as the default option. Listed below are the other potential options that can be leveraged by the client.

SSH encryption algorithms: aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr

SSH MAC algorithms: hmac-md5,hmac-sha1,hmac-ripemd160, hmac-sha1-96,hmac-md5-96

SSL: TLS RSA WITH AES 256 CBC SHA, TLS DHE RSA WITH 3DES EDE CBC SHA

13 Security Target

The security target for this product's evaluation is FireEye v.6.0 Security Target, Version 1.1, 11 May 2011.

14 List of Acronyms

Acronym	Definition
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CLI	Command-line Interface
CMS	Central Management System
COTS	Commercial Off the Shelf
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GUI	Graphical User Interface
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IP	Internet Protocol
IRC	Internet Relay Chat
IT	Information Technology
LCD	Liquid Crystal Display
MAX	Malware Analysis and Exchange
NIAP	National Information Assurance Partnership
OS	Operating System
OSI	Open System Interconnection
PCM	Platform Configuration and Management
PP	Protection Profile
SNMP	Simple Network Management Protocol
SMTP	Same Message Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
URL	Uniform Resource Locator
VM	Virtual Machine

15 Terminology

Terminology	Definition
Administrator	User of the TOE who has access to both administrative functions and monitor functions.

Attack	A botnet or malware callback event on the system.
Attacker	An entity that attempts to send malicious code or traffic to a system on the installed network.
Botnet	Set of software "robots" or "zombies" that are controlled remotely by a command and control server.
Botnet server	Command and control server that directs the operation of a botnet.
Callback event	Callback events are generated when the appliance observes outbound communications associated with a remote Command and Control server (C&C). This could include botnet command and control communications, uploads of confidential information as well as downloads of secondary payloads (such as keyloggers or spyware). Callback events indicate that there is an established communication between a bot-infected host and its C&C Server.
Command-line interface	The FireEye appliance has a CLI interface for administering the appliance.
Central Management System	Has a web-based graphical user interface for managing multiple FireEye appliances.
Event	Indicates a type of security intrusion or attack.
Graphical User Interface	The FireEye appliance has a web-based GUI for managing the appliance.
Heuristic analysis	Expert-based analysis that determines the susceptibility of a system towards particular threats using various decision rules or weighing methods.
Infection	When a machine on the network has malware or botnet programs.
Malware	Malicious software used by attackers to disrupt, cause data loss, or gain unauthorized access to computer systems.
MPC Network	A multi-enterprise alliance focused on protecting customers from botnets and other stealthy, targeted malware. The ability to connect to the MPC Network to receive signature updates and to upload detected malware is included in the evaluated configuration. The MPC Network itself is a component of the operational environment in the evaluated configuration because it is a server that sits in a server room at FireEye HQ. It's a trusted IT product with which the TOE can interact, but it's not considered part of the TOE since it belongs to the vendor and not the customer.
Monitor	User of the TOE who only has access to monitoring functions.
Role	Assigned to a user, allows users controlled access to TOE components. In this case, the three roles are Administrator, Monitor, and LCD panel administrator.
Scanner	IDS component that actively looks through data flows and traffic to find suspicious items.
Sensor	IDS component that views data flows and traffic passing through to find suspicious items.
System Administrator	See Authorized System Administrator.
User	In the evaluated configuration, a user is a global term for Administrators and Monitors.
Virtual Machine	A software program that runs an instance of an operating system. The operating system runs on top of a program that emulates a hardware system. In the evaluated configuration, each VM is isolated by address space and their virtual connections are isolated by bridges.
External IT entity	Any IT product or system, trusted or not, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between an end user and the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

16 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 2.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 2.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 2.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2.
5. FireEye v.6.0 Security Target, Version 1.1, May 11, 2011
6. Evaluation Technical Report for a Target of Evaluation "FireEye v.6.0" Evaluation Technical Report v0.3 dated July 28, 2011.