National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

FireEye, Inc.

1440 McCarthy Blvd

Milpitas, CA 95035

FireEye Series Appliances

Report Number: CCEVS-VR-VID10675-2015
Dated: February 1 2016
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell

Patrick Mallett

Brad O'Neill

Common Criteria Testing Laboratory

Anthony Busciglio

Dereck Oshin

1. Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of FireEye's FireEye HX Series Appliances. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by Acumen Security and completed in February 2016. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant.

The Target of Evaluation (TOE) is the FireEye HX Series Appliances.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the Protection Profile for Network Devices (NDPP) with Errata #3. This Validation Report applies only to the specific version of the TOE as evaluated. 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 is consistent with the evidence provided.

The technical information included in this report was obtained from the FireEye TBD Series Appliances Security Target and analysis performed by the Validation Team.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance 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(s) to which the product is conformant.
- 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
TOE	FireEye HX Series Appliances
Protection Profile	U.S. Government Protection Profile for Security Requirements for Network Devices, Version 1.1 with Errata #3
Security Target	FireEye HX Series Appliances Security Target, version 1.0
Evaluation Technical Report	VID 10675 Common Criteria NDPP Assurance Activity Report, Version 1.0
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	FireEye, Inc.
Developer	FireEye, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Montgomery Village, MD
CCEVS Validators	Paul Bicknell, Patrick Mallett, Brad O'Neill

3. ARCHITECTURAL INFORMATION

Note: The following architectural description is based on the description presented in the Security Target.

3.1. TOE EVALUATED CONFIGURATION

The TOE consists of the FireEye HX series appliances. These products include the HX4400, HX4400D, HX 4402, and HX 9402. These products provide organizations with the ability to continuously monitor endpoints for advanced malware and indicators of compromise.

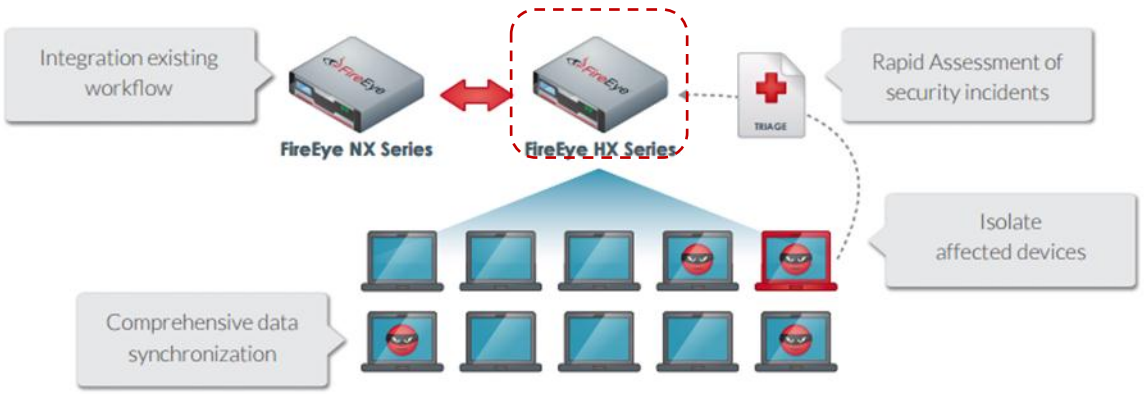
FireEye HX Series Appliances (HX 4400, HX 4400D, HX 4402, HX 9402)

The FireEye HX series appliances enable security operations teams to correlate network and endpoint activity. Organizations can automatically investigate alerts generated by FireEye Threat Prevention Platforms, log management, and network security products, apply intelligence from FireEye to continuously validate Indicators of Compromises on the endpoints and identify if a compromise has occurred and assess the potential risk. Further, organizations can quickly triage the incident to understand the details and contain compromised endpoints with a single click and contain compromised devices within a single click workflow.

TOE Evaluated Configuration

The TOE evaluated configuration consists of one of the HX series appliances listed above. The TOE also supports (sometimes optionally) secure connectivity with several other IT environment devices**.**

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line. Each TOE interconnection is through an SSH secured channel



TOE Example Deployment

3.2. PHYSICAL SCOPE OF THE TOE

The TOE is a hardware and software solution that makes up the appliances as described above in Section **Error! Reference source not found.**. The TOE guidance documentation is considered to be part of the TOE.

3.3. LOGICAL SCOPE OF THE TOE

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security Audit
2. Cryptography Support
3. User Data Protection
4. Identification & Authentication
5. Security Management
6. Protection of the TSF
7. Trusted Path/Channel
8. TOE Access

3.3.1. Security Audit

The FireEye HX Series Appliances provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include: failure on invoking cryptographic functionality such as establishment, termination and failure of a TLS session; establishment, termination and failure of an SSH session; modifications to the group of users that are part of the authorized administrator roles; all use of the user identification mechanism; any use of the authentication mechanism; any change in the configuration of the TOE, changes to time, initiation of TOE update, indication of completion of TSF self-test, maximum sessions being exceeded, termination of a remote session; and initiation and termination of a trusted channel.

The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using TLS and the TOE can determine when communication with the syslog server fails.

The logs for all of the appliances can be viewed on the TOE via the TOE CLI. The records include the date/time the event occurred, the event/type of event, the user ID associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to clear audit data stored locally on the TOE.

3.3.2. Cryptographic Support

The TOE provides cryptographic support for the following features,

- TLS connectivity with the following entities:
  - External LDAP Server
  - Audit Server
  - Management Web Browser
- SSH connectivity with the following entities:
  - Management SSH Client
- Secure software update

3.3.3. User Data Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

3.3.4. Identification & Authentication

The TOE performs three types of authentication: device-level authentication of remote IT Environment devices (e.g., audit servers and LDAP servers) and user authentication for the Authorized Administrator of the TOE (both locally and remotely). Device-level authentication of remote IT Environment devices allows the TOE to establish a secure channel with an IT Environment trusted peer. The secure channel is established only after each device authenticates the other. This device-level authentication is performed via TLS authentication.

The TOE provides authentication services for administrative users to connect to the TOEs secure GUI or CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. In the Common Criteria evaluated configuration, the TOE is configured to require a minimum password length of 15 characters, as well as, mandatory password complexity rules. The TOE provides two administrator authentication methods:

- Authentication against a local user database
- Authentication via LDAP over TLS (part of the TOE IT environment)

Password-based authentication can be performed on any TOE administrative interface including local CLI, remote CLI over SSH, and remote GUI over HTTPS.

3.3.5. Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. Management can take place over a variety of interfaces including:

- Local console command line administration at each of the appliances
- Remote command line administration via SSHv2 at each of the appliances
- Remote GUI administration via TLS

While the TOE provides multiple interfaces to perform administration, all functionality available via the command line interface is limited. All general and security administration for all of the appliances will take place at one of several locations including,

- Remote GUI administration to the appliance being managed over HTTPS,
- Remote CLI administration to each appliance over an SSH tunnel over HTTPS,
- Local administration via direction connection.

The TOE provides the ability to securely manage:

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE; and
- Update to the TOE.

The TOE supports several administrator roles, including,

- Admin: The system administrator is a "super user" who has all capabilities.
- Monitor: The system monitor has read-only access
- Operator: The system operator has a subset of the capabilities associated with the admin role.
- Analyst: The system analyst focuses on data plane analysis.
- Auditor: The system auditor reviews audit logs and performs forensic analysis.

These roles are collectively known as the "Authorized Administrator"

The TOE supports the configuration of login banners to be displayed at time of login and inactivity timeouts to terminate administrative sessions after a set period of inactivity.

3.3.6. Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally the TOE software is a custom-built hardened version of Linux and access to memory space is restricted to only required software services.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually, or can configure the TOE to use NTP to synchronize the TOE's clock with an external time source. Finally, the TOE performs testing to verify correct operation of the security appliances themselves.

The TOE verifies all software updates via digital signature and requires administrative intervention prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

3.3.7. TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE also displays an Authorized Administrator configured banner on both the GUI and CLI management interfaces prior to allowing any administrative access to the TOE.

3.3.8. Trusted Path/Channel

The TOE supports several types of secure communications, including,

- Trusted paths with remote administrators over SSH,
- Trusted paths with remote administrators over TLS,
- Trusted channels with remote IT Environment audit servers over TLS,
- Trusted channels with remote IT Environment LDAP servers over TLS.

Each of these trusted paths/channels are secured using either TLS or SSH.

4. ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1. ASSUMPTIONS

The Security Problem Definition, including the assumptions, may be found in the *Protection Profile for Network Devices*, version 1.1, 8 June 2012 (NDPP). That information has not been reproduced here and the NDPP should be consulted if there is interest in that material.

4.2. 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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Network Devices.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

5. DOCUMENTATION

The following documents were available with the TOE for evaluation:

1. [AAR] FireEye HX Series Appliances Assurance Activity Report, version 1.0
2. [AGD] FireEye HX Series Appliances FIPS Mode and Common Criteria Addendum, version 1.0
3. [EAR] FireEye HX Series Appliances Entropy Assessment Report, version 1.0
4. [EQUIV] FireEye HX Series Appliances Equivalency Analysis, version 1.0
5. [ST] FireEye HX Series Appliances Security Target, version 1.0

6. EVALUATED CONFIGURATION

See section 3.1.

7. IT PRODUCT TESTING

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for the FireEye HX Series Appliances, which is not publically available.

7.1. Testing Overview

A test plan was developed in accordance with the Testing Assurance Activities specified in the NDPPv1.1 with Errata 3. Testing was conducted at two locations, including,

- FireEye, Inc. facilities in Reston, VA,

The Evaluation Team successfully performed the following activities during independent testing:

- Placed TOE into evaluated configuration by executing the preparative procedures
- Successfully executed the NDPP Assurance-defined tests
- Successfully executed the selection-based Assurance-defined tests associated with the following SFRs,
    - FCS_SSH_EXT.1,
    - FCS_TLS_EXT.1,

It was determined after examining the Test Report and full set of test results provided by the evaluators the testing requirements for NDPPv1.1 with Errata #3 are fulfilled.

7.2. EVALUATION TEAM INDEPENDENT TESTING

The evaluation team verified the product according to the documents listed in Section 5 and ran the tests specified in the NDPP.

8. RESULTS OF THE EVALUATION

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the FireEye HX Series Appliances to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

8.1. 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 policies and assumptions, a statement of security requirements claimed to be met by the FireEye HX Series Appliances that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the NDPP.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.2. EVALUATION OF THE DEVELOPMENT (ADV)

The evaluation team applied each EAL 1 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 contained in the Security Target's TOE Summary Specification. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

8.3. EVALUATION OF THE GUIDANCE DOCUMENTS (AGD)

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases

of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

8.4. EVALUATION OF THE LIFE CYCLE SUPPORT ACTIVITIES (ALC)

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.5. EVALUATION OF THE TEST DOCUMENTATION AND THE TEST ACTIVITY (ATE)

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDPP, and that the conclusion reached by the evaluation team was justified.

8.6. VULNERABILITY ASSESSMENT ACTIVITY (VAN)

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the NDPP, and that the conclusion reached by the evaluation team was justified.

8.7. 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 test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the NDPP, and

correctly verified that the product meets the claims in the ST.

9. VALIDATOR COMMENTS & RECOMENDATIONS

The validators have no further comments about the evaluation results.

10. ANNEXES

Not applicable

11. SECURITY TARGET

The Security Target for this product's evaluation is FireEye HX Series Appliances Security Target Version 1.0, November 20, 2015.

12. GLOSSARY

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

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 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.