

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

for the

FireEye HX Series Appliances 4.0, Version 1.0

Report Number: CCEVS-VR-VID10892-2018

Dated: 31 July 2018

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

Jean Petty

Chris Thorpe

Patrick Mallett, PhD

Lisa D. Mitchell

Jenn Dotsen

Common Criteria Testing Laboratory

Acumen Security, LLC

Table of Contents

1	Executive Summary	4
2	Identification	5
3	Architectural Information	7
4	Security Policy	8
5	Assumptions, Threats & Clarification of Scope	10
5.1	Assumptions	10
5.2	Threats.....	11
5.3	Clarification of Scope	12
6	Documentation	13
7	TOE Evaluated Configuration	14
7.1	Evaluated Configuration.....	14
7.2	Excluded Functionality	Error! Bookmark not defined.
8	IT Product Testing	15
8.1	Developer Testing	15
8.2	Evaluation Team Independent Testing.....	15
9	Results of the Evaluation	16
9.1	Evaluation of Security Target	16
9.2	Evaluation of Development Documentation	16
9.3	Evaluation of Guidance Documents	16
9.4	Evaluation of Life Cycle Support Activities	17
9.5	Evaluation of Test Documentation and the Test Activity	17
9.6	Vulnerability Assessment Activity	17
9.7	Summary of Evaluation Results	17
10	Validator Comments & Recommendations	19
11	Annexes	20
12	Security Target	21
13	Glossary	22
14	Bibliography	23

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the FireEye HX Series Appliances Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in July 2018. 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 and meets the assurance requirements defined in the Collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314 (NDcPPv2.0e).

The Target of Evaluation (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. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the NDcPP. 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 are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

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 4.0
Protection Profile	Collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018 (NDcPPv2.0e)
Security Target	FireEye HX Series Appliances Security Target
Evaluation Technical Report	FireEye HX Series Appliances ETR
CC Version	Version 3.1 Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	FireEye, Inc.
Developer	FireEye, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd Rockville, MD 20850
CCEVS Validators	Jean Petty Chris Thorpe Patrick Mallett

	Jenn Dotson Lisa Mitchell
--	------------------------------

3 Architectural Information

The TOE is classified as network devices that provide a managed solution for managing the security posture of connected end points. The FireEye HX Series Appliances are network devices providing organizations with the ability to continuously monitor endpoints for advanced malware and indicators of compromise.

The HX 4502v is a virtual appliance version of the TOE, and the hardware and virtualization layer are included in the TOE boundary. There may only be one instance of the HX 4502v virtual appliance installed on the physical hardware platform. Thus, the TOE is considered to be a network device as defined in NDcPP v2.0e modified by a few TDs.

4 Security Policy

The logical boundary of the TOE includes those security functions implemented exclusively by the TOE.

Security Audit

The TOE keeps local and remote audit records of security relevant events. The TOE internally maintains the date and time which can either be set manually or synchronized with an NTP server.

Cryptographic Operations

The TOE provides cryptographic support for the services and the related FIPS140-2 validation details are provided in the table below.

Cryptographic Method	Use within the TOE
TLS Establishment	Used to establish initial TLS session.
SSH Establishment	Used to establish initial SSH session.
ECDSA Signature Services	Used in TLS session establishment.
RSA Signature Services	Used in TLS session establishment. Used in SSH session establishment Used in secure software update
SP 800-90 DRBG	Used in TLS session establishment. Used in SSH session establishment
SHS	Used in secure software update
HMAC-SHS	Used to provide TLS traffic integrity verification Used to provide SSH traffic integrity verification
AES	Used to encrypt TLS traffic Used to encrypt SSH traffic

Protected Communications

The TOE protects the integrity and confidentiality of communications such as SSH connectivity with the Management SSH Client. Additionally, the TOE provides TLS connectivity with the following entities: Audit Server (with device level authentication) and Management Web Browser.

Secure Administration

The TOE enables secure local and remote management of its security functions, including:

- Local console CLI administration
- Remote CLI administration via SSHv2
- Remote GUI administration via HTTPS/TLS
- Administrator authentication using a local database
- Timed user lockout after multiple failed authentication attempts

- Password complexity enforcement
- Role Based Access Control - the TOE supports several types of administrative user roles. Collectively these sub-roles comprise the “Security Administrator”
- Configurable banners to be displayed at login
- Timeouts to terminate administrative sessions after a set period of inactivity
- Protection of secret keys and passwords

Self-Test

The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.

Trusted Update

The TOE ensures the authenticity and integrity of software updates through digital signatures and requires administrative intervention prior to the software updates being installed.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumption	Description
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the [NDcPP] will not include any requirements on physical tamper protection or other physical attack mitigations. The [NDcPP] will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys,

Assumption	Description
	keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Threat	Description
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.

Threat	Description
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	Security mechanisms of the network device generally build up from roots of trust to more complex sets of mechanisms. Failures could result in a compromise to the security functionality of the device. A network device self-testing its security critical components at both start-up and during run-time ensures the reliability of the device's security functionality.

5.3 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 NDcPPv2.0e.
- 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.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- FireEye HX Series Appliances Security Target
- FireEye HX Series Appliances Operational User Guidance and Preparative Procedures

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE evaluated configuration consists of one of the following HX series appliances,

- HX 4402
- HX 4502
- HX 4502v

The TOE also supports (sometimes optionally) secure connectivity with several other IT environment devices, including,

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with Web Browser/SSH Client	Yes	This includes any IT Environment Management workstation with a Web Browser and a SSH client installed that is used by the TOE administrator to support TOE administration through HTTPS and SSH protected channels. Any SSH client that supports SSHv2 may be used. Any web browser that supports TLS 1.1 or greater may be used.
NTP Server	No	The TOE supports communications with an NTP server to synchronize date and time.
Syslog server	No	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE. The syslog server must support communications using TLS 1.1 or TLS 1.2.

8 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 FireEye HX Series Appliances, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDcPP. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

9 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 5 and CEM version 3.1 rev 5. 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.

9.1 Evaluation of Security Target

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 NDcPP.

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.

9.2 Evaluation of Development Documentation

The evaluation team applied each 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 NDcPP 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.

9.3 Evaluation of Guidance Documents

The evaluation team applied each 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 NDcPP 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.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each 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.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP 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 NDcPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each 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 NDcPPv2.0e, and that the conclusion reached by the evaluation team was justified.

9.7 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 NDcPPv2.0e,

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

10 Validator Comments & Recommendations

The validators suggest that the consumer pay special attention to the evaluated configuration of the device(s) and the specific functionality defined within the Security Target. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Only the functionality implemented by the security functional requirements within the Security Target was evaluated. Other functionality included in the product was not assessed as part of this evaluation.

The product contains more functionality than was covered by the evaluation. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

FireEye HX Series Appliances Security Target, version 1.2, July 2018.

13 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.

14 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 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.