National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

FireEye VX Series Appliance, Version 1.0

Report Number: CCEVS-VR-10835-2017

Dated: 01/19/18

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

The MITRE Corporation

Common Criteria Testing Laboratory

Acumen Security, LLC

Table of Contents

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 in Section 5, the Clarification of Scope in Section 6 and the Validator Comments in Section 11, where operational requirements and restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the FireEye VX Series Target of Evaluation (TOE), which consists of the FireEye VX-5500 and VX-12500 with Software Version 8.0. 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 January 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 U.S. Government Protection Profile for Security Requirements for Protection Profile Compliant.

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. 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 NDcPP Version 1. 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.

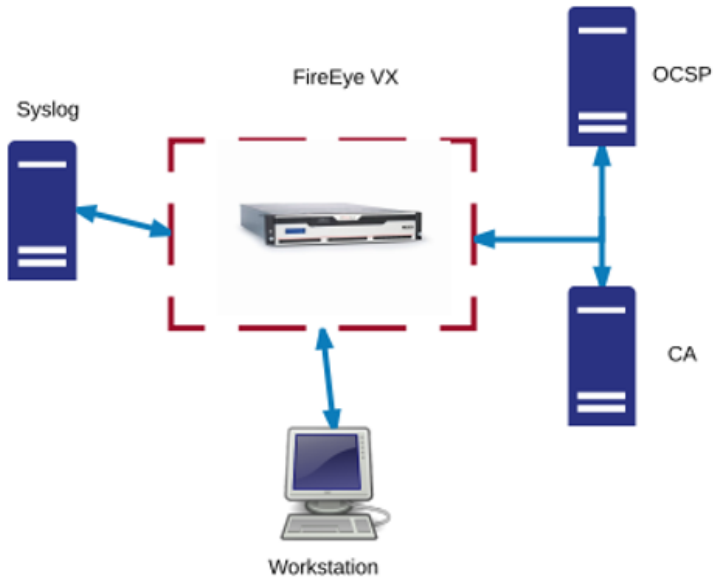
Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	FireEye VX Series Appliances, FireEye VX-5500 and VX-12500 with Software Version 8.0
Protection Profile	U.S. Government Protection Profile for Security Requirements for Network Devices, Version 1.1 with Errata #3 (hereafter referenced as the NDcPP)
Security Target	FireEye VX Security Target
Evaluation Technical Report	VID10835 Common Criteria NDPP Assurance Activity Report, version 3.0
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	Jean Petty, Chris Thorpe

3 Architectural Information

The FireEye Network Threat Prevention Platform identifies and blocks zero-day Web exploits, droppers (binaries), and multi-protocol callbacks to help organizations scale their advanced threat defenses across a range of deployments, from the multi-gigabit headquarters down to remote, branch, and mobile offices. FireEye Network with Intrusion Prevention System (IPS) technology further optimizes spend, substantially reduces false positives, and enables compliance while driving security across known and unknown threats.

The following figure provides a visual depiction of an example of a typical TOE deployment. The TOE boundary is surrounded with **hashed red lines**.



4 Security Policy

The TOE provides the following security functions:

- **Protected Communications.** The TOE protects the integrity and confidentiality of communications as follows:
  - TLS connectivity with the following entities:
    - External LDAP Server (with device level authentication)
    - Audit Server (with device level authentication)
  - SSH connectivity with the following entities:
    - Management SSH Client
- **Secure Administration.** The TOE enables secure local and remote management of its security functions, including:
  - Local console CLI administration

- Remote CLI administration via SSHv2
- Administrator authentication using a local database, via LDAP over TLS
- 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

- **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.
- **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. The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using TLS.
- **Self-Test.** The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.
- **Cryptographic Operations.** The TOE provides cryptographic support for the services described in Table 2. The related FIPS140-2 validation details are provided in Table 3.

Table 2. TOE Provided Cryptography

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

Table 3 FIPS 140 Algorithm Testing References

Algorithm	FIPS 140 CAVP Certificate #
RSA	2605
ECDSA	1193
SP 800-90 DRBG	1638
SHS	3904
HMAC-SHS	3172
AES	4761
CVL	1406

5 Assumptions and Threats

5.1 Assumptions

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.

5.1.1 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).

5.1.2 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).

5.1.3 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.

5.1.4 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.

5.1.5 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.

5.2 Threats

The threats for the Network Device are grouped according to functional areas of the device in the sections below.

5.2.1 Communications with the Network Device

A network device communicates with other network devices and other network entities. The endpoints of this communication can be geographically and logically distant and may pass through a variety of other systems. The intermediate systems may be untrusted providing an opportunity for unauthorized communication with the network device or for authorized communication to be compromised. The security functionality of the network device must be able to protect any critical network traffic (administration traffic, authentication traffic, audit traffic, etc.). The communication with the network device falls into two categories: authorized communication and unauthorized communication.

Authorized communication includes network traffic allowable by policy destined to and originating from the network device as it was designed and intended. This includes critical network traffic, such as network device administration and communication with an authentication or audit logging server, which requires a secure channel to protect the communication. The security functionality of the network device includes the capability to ensure that only authorized communications are allowed and the capability to provide a secure channel for critical network traffic. Any other communication with the network device is considered unauthorized communication. (Network traffic traversing the network device but not ultimately destined for the device, e.g. packets that are being routed, are not considered to be "communications with the network device" – cf. A.NO_THRU_TRAFFIC_PROTECTION in section 5.1.2.)

The primary threats to network device communications addressed in [the NDcPP] focus on an external, unauthorized entity attempting to access, modify, or otherwise disclose the critical network traffic. A poor choice of cryptographic algorithms or the use of non-standardized tunnelling protocols along with weak Administrator credentials, such as an easily guessable password or use of a default password, will allow a threat agent unauthorized access to the device. Weak or no cryptography provides little to no protection of the traffic allowing a threat agent to read, manipulate and/or control the critical data with little effort. Non-standardized tunnelling

protocols not only limit the interoperability of the device but lack the assurance and confidence standardization provides through peer review.

5.2.1.1 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.

5.2.1.2 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.

5.2.1.3 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.

5.2.1.4 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.

6 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 NDcPP.

- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Consistent with the expectations of the NDcPP, 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 NDcPP. Any additional security related functional capabilities included in the product were not covered by this evaluation.

7 Documentation

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

- [ADG] FireEye FIPS 140-2 and Common Criteria Addendum, 1.1

8 TOE Evaluated Configuration

The TOE is comprised of the two models of the FireEye VX Series Appliances with network port configurations, storage, and enclosures as shown in Table 4.

Table 4. TOE Models

	VX 5500	**VX 12500**
Network Ports	4x 10/100/1000BASE-T Ports	4x 10/100/1000BASE-T Ports
Storage	2x 1 TB HDD	2x .9 TB HDD
Enclosure	1RU, Fits 19 inch Rack	1RU, Fits 19 inch Rack

The TOE evaluated configuration consists of one of the appliances listed above. The TOE supports secure connectivity with several IT environment devices listed in Table 5; note that these connected devices are not a part of the TOE and no security claims are made for these devices.

Table 5. Devices that may be part of the IT Environment

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 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.
LDAP AAA Server	No	This includes any IT environment LDAP AAA server that provides authentication services to TOE administrators. The LDAP server must support communications using TLS 1.1 or TLS 1.2.

9 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 VX Series Appliance, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

9.1 Developer Testing

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

9.2 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.

10 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 VX Series Appliance to be Part 2 extended, and meets the SARs contained in the NDcPP. Additionally the evaluator performed the Assurance Activities specified in the NDcPP.

10.1 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 VX Series Appliance 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.

10.2 Evaluation of Development Documentation

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 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.

10.3 Evaluation of Guidance Documents

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 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.

10.4 Evaluation of Life Cycle Support Activities

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.

10.5 Evaluation of Test Documentation and the Test Activity

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 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.

10.6 Vulnerability Assessment Activity

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 NDcPP, and that the conclusion reached by the evaluation team was justified.

10.7 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 NDcPP, and correctly verified that the product meets the claims in the ST.

11 Validator Comments & Recommendations

It is important to note that the TOE consists of only the FireEye VX-5500 and VX-12500 with Software Version 8.0. The validation team suggests that the consumer pay particular attention to the installation guidance to ensure the devices are placed into the evaluated configuration.

As was noted in the Clarification of Scope section of this report, the TOE provides more functionality than was covered by the evaluation. Only the functionality claimed in the SFR’s in the Security Target was evaluated. All other functionality provided by the devices needs to be assessed separately and no further conclusions should be drawn as to their effectiveness, nor can any claims be made relative to their security based upon this evaluation.

12 Annexes

Not applicable.

13 Security Target

The security target for this product's evaluation is FireEye VX Series Appliances Security Target, Version 1.3, January 2018

14 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.

15 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.