National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

FireEye EX Series Appliances v9.0

Report Number:	**CCEVS-VR-VID11126-2021**
Dated:	**May 28, 2021**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Farid Ahmed
Joyce Baidoo
Anne Gugel
John Hopkins University APL

Patrick Mallett, Ph.D.
Jerome Myers, Ph.D.
The Aerospace Corporation

Common Criteria Testing Laboratory

Kenji Yoshino

Danielle F Canoles

Kevin Zhang

Thibaut Marconnet

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 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 EX 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 May 2021. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security as summarized in the Assurance Activity Report for FireEye EX Series Appliances v9.0 (AAR). 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 2.2e [NDcPP].

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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP] and all applicable NIAP technical decisions for the technology. 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 and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretations 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.

The target of evaluation is the FireEye EX Series Appliances and the associated TOE guidance documentation.

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.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	FireEye EX Series Appliances v9.0
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]
Security Target	FireEye EX Series Appliances v9.0 Common Criteria Security Target, Version 1.1
Evaluation Technical Report	Assurance Activity Report for FireEye EX Series Appliances v9.0
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, LLC
CCEVS Validators	Farid Ahmed Joyce Baidoo Anne Gugel Patrick Mallett Jerome Myers

Table 1 – Identification

3 Architectural Information

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

The TOE is comprised of four models of the FireEye EX Series Appliances as shown below.

	EX3500	EX5500	EX8400	EX8500
Monitoring Interface Ports	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+ (supporting 10GigE Fiber, 10GigE Copper, 1GigE Copper), 2x 1GigE BaseT
Management Ports	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
Storage	4x 2TB disk / 4TB virtual disk RAID 10	4x 2TB Disk / 4TB virtual disk RAID 10	2x 512 GB Disk / 512 GB virtual disk RAID 1	4x 2TB Disk / 4TB virtual disk RAID 10
Enclosure	1 Rack Unit	2 Rack Unit	2 Rack Unit	2 Rack Unit
Processor	Intel Xeon E3-1240 v6 (Kaby Lake)	Intel Xeon E5-2620 v4 (Broadwell)	AMD Opteron 6380 (Piledriver)	Intel Xeon E5-2640 v4 (Broadwell)
TOE Type	Stand-alone physical network device	Stand-alone physical network device	Stand-alone physical network device	Stand-alone physical network device

Table 2 – EX Series Appliances (1)

	EX5500V
Monitoring Interface Ports	2x 1GigE interfaces
Management Ports	2x 1GigE interfaces
CPU Cores	8
Memory	16 GB
Storage	384 GB
Processor	Intel Xeon E5-4620 v4 (Broadwell)
Hypervisor	VMware vSphere ESXi 6.7
TOE Type	Stand-alone virtual network device

Table 3 – EX Series Appliances (2)

The TOE is a hardware and software solution that is comprised of the security appliance models described above. The TOE guidance documentation that is considered to be part of the TOE is the FireEye EX Series Appliances v9.0 Common Criteria Guidance Addendum document and is downloadable from the FireEye website.

The network on which the TOE resides is considered part of the environment. The software is pre-installed and is comprised of only the software versions identified above. In addition, software updates are downloadable from the FireEye website. A login ID and password is required to download the software update.

4 Security Policy

The TOE is comprised of several security features, as identified below.

- **Protected Communications.** The TOE protects the integrity and confidentiality of communications as follows:
  - TLS connectivity with the following entities:
    - Audit Server
    - Email Server
    - Management Web Browser
  - 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
  - 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
- **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 be set manually or using authenticated NTP.
- **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 the ST.

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.

ID	Assumption
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 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 cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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. For vNDs, this assumption applies to the physical platform on which the VM runs.
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). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device 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 ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules 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 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. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA

ID	Assumption
	certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
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.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_ADMINISTRATOR	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATON	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

Table 4 – Assumptions

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.

ID	Threat
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.
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	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

Table 5 – Threats

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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP].
- 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 PP and applicable Technical Decisions. Any additional security related functional capabilities that may be 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 EX Series Appliances v9.0 Common Criteria Guidance Addendum [AGD]

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration consists of the following hardware and software when configured in accordance with the documentation specified in section 6. The TOE is comprised of four models of the FireEye EX Series Appliances as shown below.

	EX3500	EX5500	EX8400	EX8500
Monitoring Interface Ports	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+ (supporting 10GigE Fiber, 10GigE Copper, 1GigE Copper), 2x 1GigE BaseT
Management Ports	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
Storage	4x 2TB disk / 4TB virtual disk RAID 10	4x 2TB Disk / 4TB virtual disk RAID 10	2x 512 GB Disk / 512 GB virtual disk RAID 1	4x 2TB Disk / 4TB virtual disk RAID 10
Enclosure	1 Rack Unit	2 Rack Unit	2 Rack Unit	2 Rack Unit
Processor	Intel Xeon E3-1240 v6 (Kaby Lake)	Intel Xeon E5-2620 v4 (Broadwell)	AMD Opteron 6380 (Piledriver)	Intel Xeon E5-2640 v4 (Broadwell)
TOE Type	Stand-alone physical network device	Stand-alone physical network device	Stand-alone physical network device	Stand-alone physical network device

Table 6 – EX Appliances (1)

	EX5500V
Monitoring Interface Ports	2x 1GigE interfaces
Management Ports	2x 1GigE interfaces
CPU Cores	8
Memory	16 GB
Storage	384 GB
Processor	Intel Xeon E5-4620 v4 (Broadwell)
Hypervisor	VMware vSphere ESXi 6.7
TOE Type	Stand-alone virtual network device

Table 7 – EX Appliances (2)

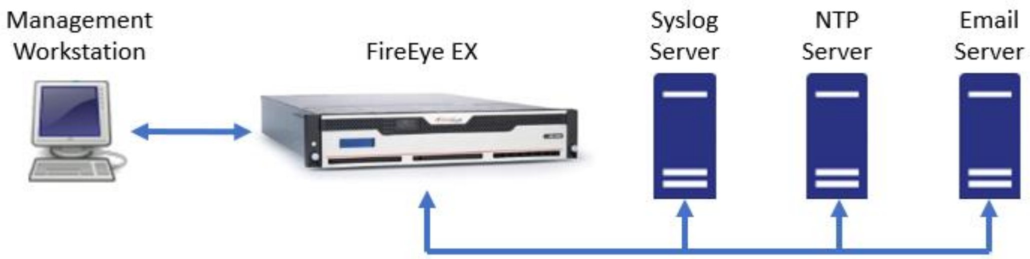
The TOE evaluated configuration consists of one of the NX series appliances listed above. The TOE has been evaluated to work with the following devices in the IT environment. Some components are required to operate the TOE, while other components may be included at the discretion of the administrator.

Component	Required	Usage/Purpose Description for TOE performance
Virtual Hardware	Yes (for EX5500V)	Virtual hardware provided by VMware vSphere ESXi 6.7 and Intel Xeon E5 (Broadwell)
Management Workstation with Web Browser/SSH Client	Yes	This includes any IT Environment Management workstation with a Web Browser and an 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 TLS 1.2 may be used.
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.
NTP Server	No	NTP server supporting SHA-1 integrity verification.
Email Server	No	SMTP server sends messages to the TOE. The SMTP server must support communications using TLS 1.1 or TLS 1.2.

Table 8 – IT Environment Components

The EX5500V was tested on a Dell PowerEdge R830.

The following figure provides a visual depiction of an example of a typical TOE deployment.



The TOE is a hardware and software solution that is comprised of the security appliance models described above. The TOE guidance documentation that is considered to be part of the TOE is the FireEye EX Series Appliances v9.0 Common Criteria Guidance Addendum document and is downloadable from the FireEye website.

The network on which the TOE resides is considered part of the environment. The software is pre-installed and is comprised of only the software versions identified above. In addition, software updates are downloadable from the FireEye website. A login ID and password is required to download the software update.

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 the FireEye EX Series Appliances v9.0, 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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]. The Independent Testing activity is documented in the Section 4.0 of the Assurance Activities Report, which is publicly available, and is not duplicated here. Multiple test beds were constructed to exercise Application Software capabilities and claimed security functionality. The following tooling was used as part of the test activities:

- OpenSSH (7.6)
- XCA (2.1.0)
- Google Chrome (88.0.4324)
- Apache 2 (2.4.29)
- Acumen-fuzzer (1.0)
- Acumen-TLSC-2.2e (10/19/2020)
- Acumen-TLSS-2.2e (10/19/2020)
- Acumen-SSH (10/19/2020)
- rsyslog (8.32.0)
- NTP (4.2.8p10)
- Postfix (3.3.0)
- Dovecot (2.2.33.2)
- OpenSSH (7.6)
- OpenSSL (1.1.1)
- Wireshark (3.0.6)
- Firefox (86.0.1)
- XCA (2.1.2)
- NTP (4.2.8p10)
- X509-mod (v1.1)
- Acumen-fuzzer (1.0)
- Tcpreplay (4.3.2)
- Wireshark (3.2.1)
- NTP (4.2.8p14)
- Wireshark (3.2.1)
- NTP (4.2.8p14)

- Wireshark (3.2.1)
- Dnsmasq (2.82)

8.3 TOE Testing Timeframe and Location

- The TOE specific testing was conducted during the timeframe of March 2020 through May 2021.
- The TOE specific testing was conducted at Acumen Security CCTL located at Rockville, MD.

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) and as summarized in the Assurance Activity Report for FireEye EX Series Appliances v9.0. 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 EX 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 NDcPP.

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 EX 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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP].

The validators 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 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 validators 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 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 validators 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 found that the TOE was identified. Additionally, the team verified that both the TOE and its supporting documentation are consistently reference the same version and use the same nomenclature. The evaluation team also verified that the vendor website identified the TOE version accurately.

The validators 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 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 validators 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

On 20 May 2021, the evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The following sources of public vulnerability information were searched:

- NIST National Vulnerability Database (NVD)
- US-CERT: https://www.kb.cert.org/vuls/search/
- SecurITeam Exploit Search: https://securiteam.com/
- Zero Day Initiative: https://www.zerodayinitiative.com/advisories/published/
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/?type=nexpose

The search terms used included:

- openssl-1.0.1e-60.el7.1.fe
- OpenSSH 6.4
- curl-7.61.1-2.el7.centos.fe
- openldap-2.4.40-8.el7.fe
- httpd-2.4.41-6.1.fe

- login 2.11
- ssmtp 2.60
- postfix-2.11.0-1.el7.fe
- ntp-4.2.6p5-25.el7.1.fe
- stunnel-5.35-1.el7.fe
- rsyslog-7.4.7-12.el7.fe
- pam_ldap-183
- nss_ldap-253-42.el5_7.4
- pam-1.1.8-12.el7_1.1
- xmlsec1-1.2.20-7.el7_4
- net-snmp-libs-5.7.2-24.el7
- Intel Xeon E3-1240 v6 (Kaby Lake)
- Intel Xeon E5-2620 v4 (Broadwell)
- Intel Xeon E5-2640 v4 (Broadwell)
- AMD Opteron 6380 (Piledriver)
- FireEye EX

The validators 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.

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

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in FireEye EX Series Appliances v9.0 Common Criteria Guidance Addendum [AGD] document. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

Please see the FireEye EX Series Appliances Security Target [ST].

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:

- Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
- Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
- Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
- Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
- collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]
- FireEye EX Series Appliances v9.0 Common Criteria Security Target [ST]
- Assurance Activity Report FireEye EX Series Appliances v9.0. Version 1.1, May 2021[AAR]
- FireEye EX Series Appliances v9.0 Common Criteria Guidance Addendum [AGD]