National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4

Report Number:	**CCEVS-VR-VID11413-2024**
Dated:	**10/18/2024**
Version:	**1.2**

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

Daniel Faigin
Marybeth Panock
Mike Quintos

The Aerospace Corporation

Common Criteria Testing Laboratory

Yogesh Pawar
Reema Nagwekar
Saniya Shaikh
Calvin Sneed

Intertek Acumen Security

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 AX, CM, EX, FX, HX, NX, and VX 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 October 2024. 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 of the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP].

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 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 Protection Profile. 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 AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4
Protection Profile	Collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]
Security Target	FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4 Security Target
Evaluation Technical Report	Evaluation Technical Report for FireEye AX, CM, EX, FX, HX, NX, And VX Series Appliances running TRFEOS 10.0.4
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Trellix, Inc.
Developer	FireEye, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd Suite 395 Rockville, MD 20850
CCEVS Validators	Daniel Faigin, Marybeth Panock, and Mike Quintos

3 Architectural Information

3.1 TOE Overview

FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances are network devices comprised of hardware and software. The virtual devices as defined in Table 1 of the ST are considered virtual network devices as defined in Case 1 of NDcPP v2.2e running on general purpose hardware and virtualization system which are outside of the TOE. In the virtual case, the TOE boundary represents the virtual network device only. The hardware appliances are physical devices comprised of the TOE firmware running on bare metal, where the TOE boundary is inclusive of hardware and software. The Trellix Appliances runs on a pre-installed, hardened TRFE(Trellix FireEye) operating system(TRFEOS) and comes pre-loaded with the TRFEOS software. TRFEOS runs on all platforms with version 10.0.4. Please see Section 1.3 of the ST for additional details on the TOE models.

The FireEye Malware Analysis (AX) series is a group of forensic analysis platforms that give security analysts hands-on control over powerful auto-configured test environments to safely execute and inspect advanced malware, zero-day and advanced persistent threat (APT) attacks embedded in Web pages, email attachments and files.

FireEye Central Management (CM) series consolidates the administration, reporting and data sharing of the FireEye products in one easy-to-deploy, network-based solution.

The FireEye Email Security (EX) Series Appliances are network devices that secure against advanced email attacks by using signature-less technology to analyze email attachments and quarantine malicious emails.

The FireEye Threat Prevention (FX) platform protects data assets against attacks originating in a wide range of file types. Web mail, online file transfer tools, the cloud, and portable file storage devices can introduce malware that can then spread to file shares and content repositories.

The FireEye Endpoint Security (HX) Appliances are network devices providing organizations with the ability to continuously monitor endpoints for advanced malware and indicators of compromise.

FireEye Network Security (NX) is an effective cyber threat protection solution that helps organizations minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in Internet traffic.

The FireEye Network Threat Prevention Platform (VX) 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.

Note: Each model of the TOE shares an identical codebase employing all NDcPP required functionality. Breach detection, email analysis, endpoint monitoring, IPS, malware analysis, and threat prevention features are not evaluated as part of the Common Criteria certification and are excluded by the evaluation.

4 Security Policy

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, Version 2.2e, hereafter referred to as NDcPP v2.2e or NDcPP.

4.1 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.

4.2 Cryptographic Support

The TOE provides cryptographic support for the services described in Table 2 below and in ST Section 1.3.2.2 Cryptographic Support. The related CAVP validation details can be found in Table 4: CAVP Algorithm Testing References in the same section of the ST. SFR to CAVP mapping, along with the cryptographic algorithms selected, is provided in Table 17: CAVP Table in ST Section 6 TOE Summary Specification.

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
Random Bit Generation	Used in TLS session establishment Used in SSH session establishment
Hashing	Used in secure software update Used in NTP integrity
HMAC	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

The TOE utilizes Trellix OpenSSL FIPS Object Module cryptographic library which provides operations related to entropy. For all cryptographic operations performed by the TOE, the cryptographic algorithms have been validated as identified in the ST CAVP table referenced above.

4.3 Identification and Authentication

The TOE authenticates administrative users using a username/password combination. The TOE does not allow access to any administrative functions prior to successful authentication. The TOE validates and authenticates TLS clients and servers using X.509 certificates for all claimed certificate uses.

The TOE supports passwords consisting of alphanumeric and special characters and enforces minimum password lengths. The TSF supports authentication based on certificates. Certificates are used to authenticate trusted channels, not administrators. The TOE only allows users to view the login warning banner prior to authentication. Remote administrators are locked out after a configurable number of unsuccessful authentication attempts.

4.4 Security Management

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 (note: remote Web UI is not supported on VX series models)
- 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 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

4.5 Protection of the TSF

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

4.6 TOE Access

The TOE can be configured to display a warning and consent banner when an administrator attempts to establish an interactive session over the CLI (local or remote) or remote web UI (Only VX series models don’t support Web UI Feature). The TOE also enforces a configurable inactivity timeout for remote administrative sessions.

4.7 Trusted Path/Channels

The TOE protects the integrity and confidentiality of communications as follows:

- TLS connectivity with the following entities:
    - Audit Server
    - Management Web Browser (note: remote Web UI is not supported on VX series models)
- SSH connectivity with the following entities:
    - Management SSH Client

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.

Table 3: Assumptions

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). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
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.

ID	Assumption
	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 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.

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.

Table 4: Threats

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

ID	**Threat**
	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.

ID	Threat
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.

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 PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation. See section 7.2 of this report for additional information on product functionality that is not included in the scope of evaluation.

6 Documentation

The following documents were provided with the TOE for evaluation:

- FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4 Security Target [ST], Version 2.0, October 17, 2024
- FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4 Guidance [AGD], Version 1.4, October 17, 2024

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

Each instance of the TOE is a hardware and software solution implemented in one of the security appliance models listed in Table 6. The TOE guidance documentation identified in Section 6 of this report is considered to be part of the TOE and can be downloaded from the NIAP 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.

The TOE is comprised of seven models of the FireEye Appliances as shown in Table 5.

Table 5: TOE Physical Boundary Components

Model	CPU	Network Interfaces	Storage	Dimen sions	Firmware
Physical Models					
AX5600	Intel Xeon E-2334 (Rocket Lake)	2x 1GigE BaseT	2 x 4TB disk / 4 TB virtual disk RAID 1	1 RU	TRFEOS 10.0.4
CM4600	Intel Xeon E-2334 (Rocket Lake)	2x 1GigE BaseT	4x 4TB disk / 8TB virtual disk RAID 10	1 RU	TRFEOS 10.0.4
CM7600	Intel Xeon Silver 4314 (Ice Lake)	2x 1GigE BaseT	4x 4TB disk / 8TB virtual disk RAID 10	2 RU	TRFEOS 10.0.4
CM9600	Intel Xeon Silver 4316 (Ice Lake)	2x 1GigE BaseT	4x 10TB disk / 20TB virtual disk RAID 10	2 RU	TRFEOS 10.0.4
EX3600	Intel Xeon E-2334 (Rocket Lake)	2x 1GigE BaseT	4x 4TB disk / 8TB virtual disk RAID 10	1 RU	TRFEOS 10.0.4
EX5600	Intel Xeon Silver 4314 (Ice Lake)	2x 1GigE BaseT	4x 4TB disk / 8TB virtual disk RAID 10	2 RU	TRFEOS 10.0.4
EX8600	Intel Xeon Silver 4316 (Ice Lake)	2x 1GigE BaseT	4x 4TB disk / 8TB virtual disk RAID 10	2 RU	TRFEOS 10.0.4
FX6600	Intel Xeon Silver 4316 (Ice Lake)	2x 1GigE BaseT	4x 4TB disk / 8TB virtual disk RAID 10	2 RU	TRFEOS 10.0.4
HX4600	Intel Xeon E-2378 (Rocket Lake)	2x 1GigE BaseT	4x 4TB disk / 8TB virtual disk RAID 10	1 RU	TRFEOS 10.0.4
NX2600	Intel Xeon E-2334 (Rocket Lake)	2x 1GigE BaseT	2 x 4TB disk / 4 TB virtual disk RAID 1	1 RU	TRFEOS 10.0.4

Model	CPU	Network Interfaces	Storage	Dimensions	Firmware
NX3600	Intel Xeon E-2378 (Rocket Lake)	2x 1GigE BaseT	2 x 4TB disk / 4 TB virtual disk RAID 1	1 RU	TRFEOS 10.0.4
NX4600	Intel Xeon Silver 4314 (Ice Lake)	2x 1GigE BaseT	2 x 4TB disk / 4 TB virtual disk RAID 1	2 RU	TRFEOS 10.0.4
NX5600	Intel Xeon Silver 4314 (Ice Lake)	2x 1GigE BaseT 2x 10G BaseT	2 x 4TB disk / 4 TB virtual disk RAID 1	2 RU	TRFEOS 10.0.4
NX6600	Intel Xeon Gold 6330 (Ice Lake)	2x 10G BaseT 2x SFP	2 x 10TB disk / 10TB virtual disk RAID 1	2 RU	TRFEOS 10.0.4
NX8600	Intel Xeon Platinum 8380 (Ice Lake)	2x 10G BaseT 2x SFP 2x 100G QSFP	2 x 10TB disk / 10TB virtual disk RAID 1	2 RU	TRFEOS 10.0.4
VX5600	Intel Xeon E-2334 (Rocket Lake)	2x 1GigE BaseT	2 x 4TB disk / 4 TB virtual disk RAID 1	1 RU	TRFEOS 10.0.4
VX12600	Intel Xeon Gold 6330 (Ice Lake)	2x 10G BaseT	4x 4TB disk / 8TB virtual disk RAID 10	2 RU	TRFEOS 10.0.4
Virtual Models					
CM7500V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
CM1500V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
CM2500V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
EX5500V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
FX2500V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
HX4502V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4

Model	CPU	Network Interfaces	Storage	Dimensions	Firmware
HX4600V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
NX1500V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
NX2500V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
NX2550V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
NX4500V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
NX6500V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
NX7500V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
NX8500V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4
NX10500V	ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4 (Broadwell)	NA	NA	NA	TRFEOS 10.0.4

The following environmental components are required to operate the TOE in the evaluated configuration. The TOE evaluated configuration consists of any of the AX, CM, EX, FX, HX, NX, and VX series appliances listed in Table 5 above. The TOE also supports secure connectivity with several other IT environment devices as listed in Table 6 below. The virtual appliances are tested on a Dell PowerEdge R830 with VMware vSphere ESXi 7.0 and Intel(R) Xeon(R) CPU E5-4620 v4(Broadwell).

Table 6: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Virtual Hardware	Yes (for virtual appliances)	Virtual hardware provided by VMware vSphere ESXi 7.0 and Intel Xeon E5-4620 v4 (Broadwell).

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with Web Browser and 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 support TLS 1.2 may be used.
Audit server	Yes	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 1.2.
NTP Server	Yes	NTP server supporting SHA-1 integrity verification.

Figure 1 provides a visual depiction of how various instances of TOE models are deployed in a typical network.

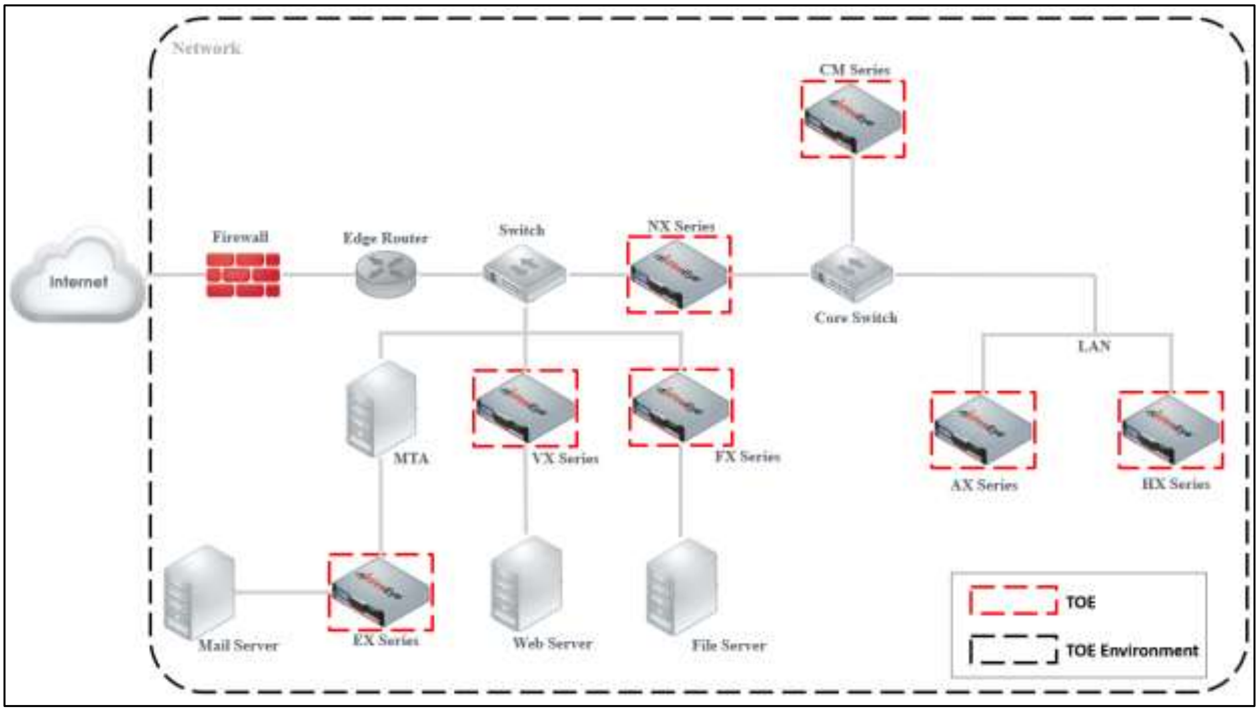

Figure 1 – Representative TOE Deployment

7.2 Excluded Functionality

As noted in Section 3.1 of this document and in the last paragraph of ST Section 1.2 TOE Overview, each model of the TOE shares an identical codebase employing all NDcPP required functionality. Breach detection, email analysis, endpoint monitoring, IPS, malware analysis, and threat prevention features are not evaluated as part of the Common Criteria certification and are excluded by the evaluation.

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 AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4, which is not publicly available. The Assurance Activities Report provides an overview of testing, with the test configuration and tools in Section 4, test cases in Sections 5 and 7, and the prescribed assurance activities in Section 6.

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 to the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP].

Testing occurred from April 2023 to October 2024, and was conducted using the following TOE models: EX3600, VX12600, and CM2500V. 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 AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4 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 AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4 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 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 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 collaborative Protection Profile for Network Devices, Version 2.2e [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 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 collaborative Protection Profile for Network Devices, Version 2.2e [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 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.

9.5 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 collaborative Protection Profile for Network Devices, Version 2.2e [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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP], and that the conclusion reached by the evaluation team was justified.

9.6 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.

In compliance with AVA_VAN.1, the evaluator examined sources of publicly available information to identify potential vulnerabilities in the TOE. The sources of examined are as follows:

- https://nvd.nist.gov/view/vuln.search

- http://cve.mitre.org/cve
- https://www.cvedetails.com/vulnerability-search.php
- https://www.kb.cert.org/vuls/search/
- www.exploitsearch.net
- www.securiteam.com
- http://nessus.org/plugins/index.php?view=search
- http://www.zerodayinitiative.com/advisories
- https://www.exploit-db.com
- https://www.rapid7.com/db/vulnerabilities

The evaluator examined public domain vulnerability searches by performing a keyword search. The terms used for this search were based on the vendor’s name, product name, and key platform features leveraged by the product. As a result, the evaluator performed a search using the following keywords:

- FireEye
- Trellix
- TRFEOS 10.0
- AX5600
- CM4600
- CM7600
- CM9600
- EX3600
- EX5600
- EX8600
- FX6600
- HX4600
- NX2600
- NX3600
- NX4600
- NX5600
- NX6600
- NX8600
- VX5600
- VX12600
- CM1500V
- CM2500V
- CM7500V
- EX5500V
- FX2500V
- HX4502V
- HX4600V
- NX1500V
- NX2500V

- NX2550V
- NX4500V
- NX6500V
- NX7500V
- NX8500V
- NX10500V
- Intel Xeon E-2334 (Rocket Lake)
- Intel Xeon Silver 4314 (Ice Lake)
- Intel Xeon Silver 4316 (Ice Lake)
- Intel Xeon E-2378 (Rocket Lake)
- Intel Xeon Gold 6330 (Ice Lake)
- Intel Xeon Platinum 8380 (Ice Lake)
- Intel Xeon E5-4620 v4 (Broadwell)
- Dell PowerEdge R830
- Trellix OpenSSL FIPS Object Module
- libcrypt.so
- OpenSSH 7.4p1
- Apache 2.4.62 (CentOS Linux)
- OpenSSL 1.0.2zh

The vulnerability search was performed on September 26, 2024. No open vulnerabilities applicable to the TOE were 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 addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e [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 collaborative Protection Profile for Network Devices, Version 2.2e [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 configuration guide document listed in Section 6. No other versions of the TOE, either earlier or later, were evaluated.

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. See Section 7.2 of this report for product functionality that is not included in the scope of evaluation.

Additional functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Annexes

Not applicable.

12 Security Target

FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4
Security Target [ST], Version 2.0, October 17, 2024

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, April 2017.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5, April 2017.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5, April 2017.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
5. FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4 Security Target, Version 2.0. October 17, 2024.
6. FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4 Guidance, Version 1.4, October 17, 2024.
7. Assurance Activity Report for FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4, Version 1.7, October 17, 2024.
8. Evaluation Technical Report for FireEye AX, CM, EX, FX, HX, NX, And VX Series Appliances running TRFEOS 10.0.4, Version 1.5, October 17, 2024.
9. Vulnerability Assessment for FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances, Version 1.7, September 26, 2024.
10. Master Test Plan - The FireEye Email Security (EX3600), Version 1.2, August 21, 2024.
11. Master Test Plan - The FireEye Email Security (EX3600), Version 1.4, October 10, 2024.
12. Master Test Plan - The FireEye Network Threat Prevention Platform (VX12600), Version 1.2, August 21, 2024.
13. Master Test Plan - The FireEye Network Threat Prevention Platform (VX12600), Version 1.3, October 4, 2024.
14. Master Test Plan - The FireEye Central Management (CM2500V), Version 1.2, August 21, 2024.
15. Master Test Plan - The FireEye Central Management (CM2500V), Version 1.4, October 10, 2024.