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

Document Version: 2.0

2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History

Version	Date	Changes
Version 1.0	January 23, 2023	Initial Release
Version 1.1	March 31, 2023	Updated Algorithms
Version 1.2	September 15, 2023	Updated based on ECR comments
Version 1.3	November 17, 2023	Updated based on 2nd Round of ECR comments
Version 1.4	February 28, 2024	Updated selections for SFRs
Version 1.5	April 23, 2024	Updated CAVP Mapping
Version 1.6	May 30, 2024	Minor updates to TSS.
Version 1.7	July 28, 2024	Updated for addressing internal review comments
Version 1.8	August 23, 2024	Updated based on Check-out ECR comments
Version 1.9	August 28, 2024	Updated based on 2nd round Check-out ECR comments
Version 2.0	October 17, 2024	Firmware version entry updated to 10.0.4

Contents

1 Introduction 5
1.1 Security Target and TOE References 5
1.2 TOE Overview 6
1.3 TOE Description 7
1.3.1 Physical Boundaries 8
1.3.2 Security Functions Provided by the TOE 10
1.3.3 TOE Documentation 14
1.4 TOE Environment 14
2 Conformance Claims 15
2.1 CC Conformance Claims 15
2.2 Protection Profile Conformance 15
2.3 Conformance Rationale 15
2.3.1 Technical Decisions 15
3 Security Problem Definition 18
3.1 Threats 18
3.2 Assumptions 19
3.3 Organizational Security Policies 22
4 Security Objectives 23
4.1 Security Objectives for the Operational Environment 23
5 Security Requirements 25
5.1 Conventions 26
5.2 Security Functional Requirements 26
5.2.1 Security Audit (FAU) 26
5.2.2 Cryptographic Support (FCS) 29
5.2.3 Identification and Authentication (FIA) 34
5.2.4 Security Management (FMT) 37
5.2.5 Protection of the TSF (FPT) 38
5.2.6 TOE Access (FTA) 39
5.2.7 Trusted Path/Channels (FTP) 39
5.3 TOE SFR Dependencies Rationale for SFRs 40
5.4 Security Assurance Requirements 40
5.5 Assurance Measures 41
6 TOE Summary Specification 42

6.1 Cryptographic Key Destruction 53
6.2 CAVP Table 54
7 Acronym Table 58

1 Introduction

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

1.1 Security Target and TOE References

This section provides the information needed to identify and control the TOE and the ST.

Table 1 – TOE/ST Identification

Category	Identifier
ST Title	FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4 Security Target
ST Version	2.0
ST Date	17 October 2024
ST Author	Acumen Security, LLC.
TOE Identifier	FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4
TOE Hardware	Physical Appliances: AX5600 CM4600 CM7600 CM9600 EX3600 EX5600 EX8600 FX6600 HX4600 NX2600 NX3600 NX4600 NX5600 NX6600 NX8600 VX5600 VX12600 Virtual Appliances: CM7500V CM1500V CM2500V EX5500V FX2500V HX4502V HX4600V NX1500V NX2500V NX2550V NX4500V

Category	Identifier
	NX6500V NX7500V NX8500V NX10500V
TOE Software	TRFEOS (AX): 10.0.4 TRFEOS (CM): 10.0.4 TRFEOS (EX): 10.0.4 TRFEOS (FX): 10.0.4 TRFEOS (HX): 10.0.4 TRFEOS (NX): 10.0.4 TRFEOS (VX): 10.0.4
TOE Developer	Trellix FireEye Security Holdings US LLC
Key Words	Network device, Security Appliance

1.2 TOE Overview

FireEye AX, CM, EX, FX, HX, NX, and VX Series are network devices comprised of hardware and software. The virtual devices as defined in Table 1 are considered virtual network devices as defined in Case 1 of NDcPP 2.2e 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 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.

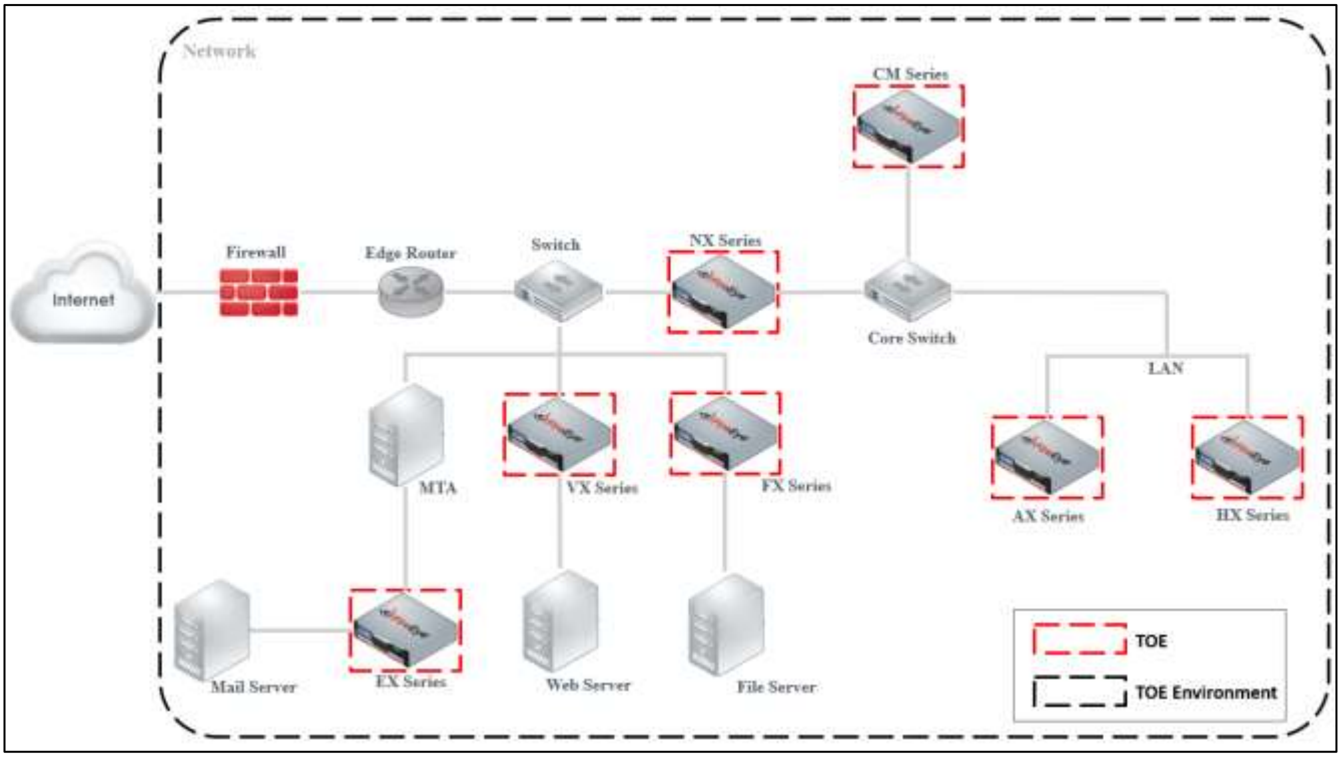
FireEye Network Security (NX) is an effective cyber threat protection solution that helps organizations minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in Internet traffic.

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.

1.3 TOE Description

This section provides an overview of the TOE deployment, including physical boundaries, security functions, and relevant TOE documentation and references. Figure 1 below depicts a typical TOE deployment in a network. It provides a sample representation of where each of the FireEye AX, CM, EX, FX, HX, NX, and VX Series are typically deployed. The TOE is not distributed and does not require all variants or series to function. Instead, each model variant of each series is a standalone TOE. The purpose of Figure 1 is to represent how various instances of the TOEs are deployed in a typical network.



[1]**Figure 1 - Representative TOE Deployment**

1.3.1 Physical Boundaries

Each instance of the TOE is a hardware and software solution implemented in one of the security appliance models listed in Table 2. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the FireEye Common Criteria 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.

An instance of the TOE consists of a physical or virtual appliance instance of one of the models listed in Table 2.

Table 2 – TOE Physical Boundary Components

Model	CPU	Network Interfaces	Storage	Dimensions	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
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

[1] Each instance of the TOE is a hardware and software solution implemented in one of the security appliance models and each of the different model is a standalone TOE.

Model	CPU	Network Interfaces	Storage	Dimensions	Firmware
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
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

Model	CPU	Network Interfaces	Storage	Dimensions	Firmware
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

1.3.2 Security Functions Provided by the TOE

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

1.3.2.1 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.

1.3.2.2 Cryptographic Support

The TOE provides cryptographic support for the services described in Table 3. The related CAVP validation details are provided in Table 4.

Table 3 – 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.
For all cryptographic operations performed by the TOE, the cryptographic algorithms have been validated as identified in the table below.

Table 4 – CAVP Algorithm Testing References

Functions	Algorithms	Mode Supported	CAVP Certs.	Name	OE
Data Encryption	AES-CBC, AES-CTR, AES-GCM	CBC, CTR, GCM (128, 256)	A2624	Trellix OpenSSL FIPS Object Module	TRFEOS 10.0 on Intel(R) Xeon (R) E-2334 (Rocket Lake) TRFEOS 10.0 on Intel(R) Xeon (R) Gold 6330 (Ice Lake) TRFEOS 10.0 running on ESXi Hypervisor v7.0 on Intel(R) Xeon(R) CPU E5-4620 v4(Broadwell)
Hash	SHS (Cryptographic hashing)	SHA-1, SHA-256, SHA-384, SHA-512	A2624	Trellix OpenSSL FIPS Object Module	
Random Number Generator	Counter DRBG HMAC DRBG	CTR_DRBG (AES-256), HMAC_DRBG(SHA-512)	A2624	Trellix OpenSSL FIPS Object Module	
Key Generation	RSA KeyGen (FIPS186-4)	Mode: n(2048,3072), n = 2048,3072 SHA(256)	A2624	Trellix OpenSSL FIPS Object Module	
	ECDSA KeyGen (FIPS186-4) ECDSA KeyVer (FIPS186-4)	P-256, P-384, P-521	A2624	Trellix OpenSSL FIPS Object Module	
	DSA KeyGen (FIPS186-4)	(L,N): (2048,256)	A2624	Trellix OpenSSL FIPS Object Module	

	Safe Primes Key Generation	modp-2048(DH-14)
		modp-4096(DH-16)
			NA	No NIST CAVP, CCTL has performed all assurance/evaluation activities.	

		modp-8192(DH-18)			
Key Establishment	KAS ECC SSC Sp800-56Ar3 (Domain Parameter Generation)	P-256, P-384, P-521	A2624	Trellix OpenSSL FIPS Object Module	
	KAS-FFC-SSC Sp800-56Ar3 (Domain Parameter Generation)	MODP-2048	A2624	Trellix OpenSSL FIPS Object Module	

	KAS-FFC-SSC Sp800-56Ar3 (safe-prime)
	(Domain Parameter Generation)
		modp-2048(DH-14)
		modp-4096(DH-16)
		modp-8192(DH-18)
			NA	No NIST CAVP, CCTL has performed all assurance/evaluation activities.	

Digital Signature services	ECDSA SigGen (FIPS186-4) ECDSA SigVer (FIPS186-4)	P-256, P-384, P-521	A2624	Trellix OpenSSL FIPS Object Module	
	RSA SigGen (FIPS186-4) RSA SigVer (FIPS186-4)	Mode: n(2048, 3072), n = 2048,3072 SHA(256)	A2624	Trellix OpenSSL FIPS Object Module	
Keyed Hash	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	Mode: SHA-1, SHA-256, SHA-384, SHA-512	A2624	Trellix OpenSSL FIPS Object Module	

The Trellix OpenSSL FIPS Object Module provides cryptographic operations related to entropy.

1.3.2.3 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.

1.3.2.4 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[2]
- 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

1.3.2.5 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.

1.3.2.6 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.

1.3.2.7 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[3]
- SSH connectivity with the following entities:
  - Management SSH Client

[2] VX series models doesn't support Web UI Feature and hence HTTPS and TLSS selection-based SFRs are not applicable to the VX Series Models

[3] VX series models doesn't support Web UI Feature and hence testing with Management Web Browser(TLS client) is not applicable to the VX Series Models

1.3.3 TOE Documentation

The following documents are essential to understanding and controlling the TOE in the evaluated configuration:

- FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4 Guidance, version 1.4

1.4 TOE Environment

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 above. The TOE also supports secure connectivity with several other IT environment devices as listed in Table 5. 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). Figure 1 provides a visual depiction of an example of a typical TOE deployment.

Table 5 – Required IT Environmental Components

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

2 Conformance Claims

This section identifies the TOE conformance claims, conformance rationale, and relevant Technical Decisions (TDs).

2.1 CC Conformance Claims

The TOE is conformant to the following:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017 (Extended)
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision 5, April 2017 (Conformant)

2.2 Protection Profile Conformance

This ST claims exact conformance to the following:

- collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)

2.3 Conformance Rationale

This ST provides exact conformance to the items listed in the previous section. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile (PP), performing only the operations defined there.

2.3.1 Technical Decisions

All NIAP TDs issued to date and applicable to NDcPP v2.2e have been considered. Table 6 identifies all applicable TDs.

Table 6 – Relevant Technical Decisions

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0527: Updated to Certificate Revocation Testing (FIA_X509_EXT.1)	Yes	
TD0528: NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	Yes	
TD0536: NIT Technical Decision for Update Verification Inconsistency	Yes	
TD0537: NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	No	The ST does not include FCS_TLSC_EXT.2.3 SFR.
TD0546: NIT Technical Decision for DTLS – clarification of Application Note 63	No	The ST does not include DTLS SFRs.
TD0547: NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Yes	
TD0555: NIT Technical Decision for RFC Reference incorrect in TLSS Test	Yes	

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0556: NIT Technical Decisions for RFC 5077 question	Yes	
TD0563: NIT Technical Decision for Clarification of audit date information	Yes	
TD0564: NIT Technical Decision for Vulnerability Analysis Search Criteria	Yes	
TD0569: NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	Yes	
TD0570: NIT Technical Decision for Clarification about FIA_AFL.1	Yes	
TD0571: NIT Technical Decision for Guidance on how to handle FIA_AFL.1	Yes	
TD0572: NIT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	Yes	
TD0580: NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Yes	
TD0581: NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	Yes	
TD0591: NIT Technical Decision for Virtual TOEs and hypervisors	Yes	
TD0592: NIT Technical Decision for Local Storage of Audit Records	Yes	
TD0631: NIT Technical Decision for Clarification of public key authentication for SSH Server	Yes	
TD0632: NIT Technical Decision for Consistency with Time Data for vNDs	Yes	
TD0635: NIT Technical Decision for TLS Server and Key Agreement Parameters	Yes	
TD0636: NIT Technical Decision for Clarification of Public Key User Authentication for SSH	No	SSH client functionality is not supported
TD0638 : NIT Technical Decision for Key Pair Generation for Authentication	Yes	
TD0639: NIT Technical Decision for Clarification for NTP MAC Keys	Yes	
TD0670: NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	No	Mutual TLS is not supported
TD0738: NIT Technical Decision for Link to Allowed-With List	Yes	

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0790: NIT Technical Decision: Clarification Required for testing IPv6	Yes	
TD0792: NIT Technical Decision: FIA_PMG_EXT.1 - TSS EA not in line with SFR	Yes	
TD0800: Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	No	IPsec is not claimed

3 Security Problem Definition

The security problem definition has been taken directly from the NDcPP specified in Section 2.2 and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any Organizational Security Policies (OSPs) that the TOE is expected to enforce.

3.1 Threats

The threats included in Table 7 are drawn directly from the NDcPP specified in Section 2.2.

Table 7 – 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 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.

ID	Threat
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.

3.2 Assumptions

The assumptions included in Table 8 are drawn directly from NDcPP.

Table 8 – 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. **Applied TD0591**
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).

ID	Assumption
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. (The paragraph that follows is for x509v3 cert-based authentication. If not relevant, remove) 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.

ID	Assumption
A.VS_ISOLATION	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.

3.3 Organizational Security Policies

The OSPs included in Table 9 are drawn directly from the NDcPP.

Table 9 – OSPs

ID	OSP
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4 Security Objectives

The security objectives have been taken directly from the NDcPP and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the Operational Environment

Security objectives for the operational environment assist the TOE in correctly providing its security functionality. These objectives, which are found in the table below, track with the assumptions about the TOE operational environment.

Table 10 – Security Objectives for the Operational Environment

ID	Objectives for the Operational Environment
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE’s trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

ID	Objectives for the Operational Environment
OE.RESIDUAL_INFORMATION	The Security Administrator ensures 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. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
OE.VM_CONFIGURATION	For vNDs, the Security Administrator ensures that the VS and VMs are configured to • Reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • Correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting).

5 Security Requirements

This section identifies the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revisions 5, April 2017, and all international interpretations.

Table 11 – SFRs

Requirement	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG_EXT.1	Protected Audit Event Storage
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FCS_HTTPS_EXT.1(not applicable to VX series models due to unavailability of web UI feature)	HTTPS Protocol
FCS_NTP_EXT.1	NTP Protocol
FCS_RBG_EXT.1	Random Bit Generation
FCS_SSHS_EXT.1	SSH Server Protocol
FCS_TLSC_EXT.1	TLS Client Protocol without Mutual Authentication
FCS_TLSS_EXT.1(not applicable to VX series models due to unavailability of web UI feature)	TLS Server Protocol
FIA_AFL.1	Authentication Failure Management
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU_EXT.2	Password-based Authentication Mechanism
FIA_UAU.7	Protected Authentication Feedback
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FIA_X509_EXT.3	X.509 Certificate Requests
FMT_MOF.1/Functions	Management of Security Functions Behaviour
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
FMT_MTD.1/CoreData	Management of TSF Data
FMT_MTD.1/CryptoKeys	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on security roles

Requirement	Description
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_TST_EXT.1	TSF Testing
FPT_STM_EXT.1	Reliable Time Stamps
FPT_TUD_EXT.1	Trusted Update
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_SSL_EXT.1	TSF-initiated Session Locking
FTA_TAB.1	Default TOE Access Banner
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1/Admin	Trusted Path

5.1 Conventions

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.
- Where operations were completed in the PP and relevant EPs/Modules/Packages, the formatting used in the PP has been retained.
- Extended SFRs are identified by the addition of “EXT” after the requirement name.

5.2 Security Functional Requirements

This section includes the security functional requirements for this ST.

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions;

b) All auditable events for the not specified level of audit; and

c) *All administrative actions comprising:*

- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
- *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*

- *[no other actions];*

d) *Specifically defined auditable events listed in Table 12*.

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, *information specified in column three of Table* 12*.*

Application Note: This SFR has been updated as per TD0563

Table 12 – Security Functional Requirements and Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_STG_EXT.1	None	None
FCS_CKM.1	None	None
FCS_CKM.2	None	None
FCS_CKM.4	None	None
FCS_COP.1/DataEncryption	None	None
FCS_COP.1/SigGen	None	None
FCS_COP.1/Hash	None	None
FCS_COP.1/KeyedHash	None	None
FCS_HTTPS_EXT.1[4]	Failure to establish a HTTPS Session	Reason for failure
FCS_NTP_EXT.1	• Configuration of a new time server • Removal of configured time server	• Identity if new/removed time server
FCS_RBG_EXT.1	None	None
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSS_EXT.1[5]	Failure to establish a TLS Session	Reason for failure

[4] VX series models doesn't support Web UI Feature and hence this selection-based SFR is not applicable to the VX Series Models

[5] VX series models doesn't support Web UI Feature and hence this selection-based SFR is not applicable to the VX Series Models

Requirement	Auditable Events	Additional Audit Record Contents
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address)
FIA_PMG_EXT.1	None	None
FIA_UIA_EXT.1	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)
FIA_UAU_EXT.2	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)
FIA_UAU.7	None	None
FIA_X509_EXT.1/Rev	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store	• Reason for failure of certificate validation • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None	None
FMT_MOF.1/Functions	None	None
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None
FMT_MTD.1/CoreData	None	None
FMT_MTD.1/CryptoKeys	None	None
FMT_SMF.1	All management activities of TSF data	None
FMT_SMR.2	None	None
FPT_SKP_EXT.1	None	None
FPT_APW_EXT.1	None	None
FPT_TST_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None
FTA_SSL.3	The termination of a remote session by the session locking mechanism	None
FTA_SSL.4	The termination of an interactive session	None

Requirement	Auditable Events	Additional Audit Record Contents
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism	None
FTA_TAB.1	None	None
FTP_ITC.1	• Initiation of the trusted channel • Termination of the trusted channel • Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1/Admin	• Initiation of the trusted path • Termination of the trusted path. • Failure of the trusted path functions.	None

Application Note: Refer FAU_GEN.1.1 and FAU_GEN.1.2 for additional information in the audit records for FAU_GEN.1.

5.2.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1
For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 FAU_STG_EXT.1 Protected Audit Event Storage

FAU_STG_EXT.1.1
The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2
The TSF shall be able to store generated audit data on the TOE itself. In addition [

- The TOE shall consist of a single standalone component that stores audit data locally].

FAU_STG_EXT.1.3
The TSF shall [overwrite previous audit records according to the following rule*: [overwrite oldest record first]*] when the local storage space for audit data is full.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1
The TSF shall generate **asymmetric** cryptographic key in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;
- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1
- FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526].

]

5.2.2.2 FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1
The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526].

]

Application Note: This SFR has been updated as per TD0580 and TD0581

5.2.2.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1
The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes]];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [
  - logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeroes];

]
that meets the following: *No Standard*

5.2.2.4 FCS_COP.1/DataEncryption Cryptographic Operations (AES Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption
The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in* [CBC, CTR, GCM] *mode* and cryptographic key sizes [128 bits, 256 bits] that meet the following:

AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772].

5.2.2.5 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen
The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm [

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048, 3072 bits]
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256, 384, 512 bits]

]
that meet the following: [

- For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,
- For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4

].

5.2.2.6 FCS_COP.1/Hash Cryptographic Operations (Hash Algorithm)

FCS_COP.1.1/Hash
The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] and **message digest sizes [160, 256, 384, 512] bits** that meet the following: *ISO/IEC 10118-3:2004*.

5.2.2.7 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash
The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [160 bits, 256 bits, 384 bits, 512 bits] **and message digest sizes [160, 256, 384, 512] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

5.2.2.8 FCS_HTTPS_EXT.1 HTTPS Protocol[6]

FCS_HTTPS_EXT.1.1
The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2
The TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3
If a peer certificate is presented, the TSF shall [not require client authentication] if the peer certificate is deemed invalid.

[6] VX series models doesn't support Web UI Feature and hence this selection-based SFR is not applicable to the VX Series Models.

5.2.2.9 FCS_NTP_EXT.1 NTP Protocol

FCS_NTP_EXT.1.1
The TSF shall use only the following NTP version(s) [NTP v3 (RFC 1305), NTP v4 (RFC 5905)].

FCS_NTP_EXT.1.2
The TSF shall update its system time using [

- Authentication using [SHA1] as the message digest algorithm(s);
  ].

FCS_NTP_EXT.1.3
The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

FCS_NTP_EXT.1.4
The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

5.2.2.10 FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1
The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [HMAC_DRBG (any), CTR_DRBG (AES)].

FCS_RBG_EXT.1.2
The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [*[one]* software-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

5.2.2.11 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1
The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [4256, 4344, 6668, 8332, 8308 section 3.1].

FCS_SSHS_EXT.1.2
The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [password-based].

Application Note: This SFR has been updated as per TD0631

FCS_SSHS_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than *[256K]* bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4
The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com].

FCS_SSHS_EXT.1.5
The TSF shall ensure that the SSH public-key based authentication implementation uses [ssh-rsa, rsa-sha2-512, rsa-sha2-256] as its public key algorithm(s) and rejects all other public key algorithms.

Application Note: This SFR has been updated as per TD0631

FCS_SSHS_EXT.1.6
The TSF shall ensure that the SSH transport implementation uses [hmac-sha2-256, hmac-sha2-512, implicit] as its MAC algorithm(s) and rejects all other MAC algorithm(s).
Application Note: The "implicit" selection means that when aes*-gcm@openssh.com is negotiated as the encryption algorithm in FCS_SSHS_EXT.1.4, the MAC algorithm field is ignored and GCM is implicitly used as the MAC.

FCS_SSHS_EXT.1.7
The TSF shall ensure that [diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512] and [no other methods] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8
The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

5.2.2.12 FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

FCS_TLSC_EXT.1.1
The TSF shall implement [TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

] and no other ciphersuites.

FCS_TLSC_EXT.1.2
The TSF shall verify that the presented identifier matches [the reference identifier per RFC 6125 section 6, IPv4 address in SAN, IPv6 address in the SAN].

FCS_TLSC_EXT.1.3
When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_TLSC_EXT.1.4
The TSF shall [present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves/groups] in the Client Hello.

5.2.2.13 FCS_TLSS_EXT.1 TLS Sever Protocol Without Mutual Authentication[7]

FCS_TLSS_EXT.1.1
The TSF shall implement [*TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

] and no other ciphersuites.

FCS_TLSS_EXT.1.2
The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [TLS 1.1].

FCS_TLSS_EXT.1.3
The TSF shall perform key establishment for TLS using [Diffie-Hellman parameters with size [2048 bits], ECDHE curves [secp256r1, secp384r1, secp521r1] and no other curves]].

FCS_TLSS_EXT.1.4
The TSF shall support [session resumption based on session tickets according to RFC 5077].

Application Note: This SFR has been updated as per TD0569

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1
The TSF shall detect when an Administrator configurable positive integer within *[1 to 15]* unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending Administrator from successfully establishing a remote session using any authentication

[7] VX series models doesn't support Web UI Feature and hence this selection-based SFR is not applicable to the VX Series Models.

method that involves a password until *[unlocks the user]* is taken by an Administrator; prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed*]*.

5.2.3.2 FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1
The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [“’”[8], “+”, “-“, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “\”, “[“, “]”[9], “^”, “_”[10], “`”[11], “{“, “|”[12], “}”, and “~”]]
b) Minimum password length shall be configurable to between [*15*] and [*32*] characters.

Application Note: This SFR has been updated as per TD0792

5.2.3.3 FIA_UIA_EXT.1 User Identification and Authentication[13]

FIA_UIA_EXT.1.1
The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [no other actions].

FIA_UIA_EXT.1.2
The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

5.2.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1
The TSF shall provide a local [password-based] authentication mechanism to perform local administrative user authentication.

5.2.3.5 FIA_UAU.7.1 Protected Authentication Feedback

FIA_UAU.7.1
The TSF shall provide only *obscured feedback* to the administrative user while the authentication is in progress **at the local console**.

[8] Single-quote character

[9] Left and right square brackets (the bottom part of the square bracket hidden by the underlying convention of the selection operation).

[10] Underscore, which is hidden by the underlining convention of the selection operation.

[11] Backtick character

[12] Vertical bar/pipe character

[13] VX series models doesn’t support Web UI Feature and hence this SFR is not applicable to the VX Series Models.

5.2.3.6 FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev
The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates**.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 6960].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
  - *Server certificates presented for TLS shall have the Server Authentication purpose(id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
  - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsagefield.*
  - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose(id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2/Rev
The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.2.3.7 FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1
The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [HTTPS, TLS] and [no additional uses].

FIA_X509_EXT.2.2
When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate].

Application Note: This SFR has been updated as per TD0537.

5.2.3.8 FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1
The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2
The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MOF.1/Functions Management of Security Functions Behaviour.

FMT_MOF.1.1/Functions
The TSF shall restrict the ability to [modify the behaviour of] the functions [transmission of audit data to an external IT entity, handling of audit data] to *Security Administrators*.

5.2.4.2 FMT_MOF.1/ManualUpdate Management of Security Functions Behavior

FMT_MOF.1.1/ManualUpdate
The TSF shall restrict the ability to enable the function *to perform manual updates to Security Administrators.*

5.2.4.3 FMT_MTD.1/CoreData Management of TSF Data

FMT_MTD.1.1/CoreData
The TSF shall restrict the ability to manage the *TSF data to Security Administrators.*

5.2.4.4 FMT_MTD.1/CryptoKeys Management of TSF Data

FMT_MTD.1.1/CryptoKeys
The TSF shall restrict the ability to manage the cryptographic keys to Security administrators.

5.2.4.5 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1
The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using [*digital signature*] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- [
    - Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);
    - Ability to modify the behaviour of the transmission of audit data to an external IT entity;
    - Ability to manage the cryptographic keys
    - Ability to configure the cryptographic functionality;
    - Ability to re-enable an Administrator account;
    - Ability to set the time which is used for time-stamps;
    - Ability to configure NTP;
    - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
    - Ability to import X.509v3 certificates to the TOE's trust store;
    - Ability to manage the trusted public keys database
    - No other capabilities

    ].

Application Note: This SFR has been updated as per TD0631

5.2.4.6 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1
The TSF shall maintain the roles:

- *Security Administrator*

FMT_SMR.2.2
The TSF shall be able to associate users with roles.

FMT_SMR.2.3
The TSF shall ensure that the conditions

- *The Security Administrator role shall be able to administer the TOE locally;*
- *The Security Administrator role shall be able to administer the TOE remotely;*

are satisfied.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FTP_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1
The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2
The TSF shall prevent the reading of plaintext administrative passwords.

5.2.5.2 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric, and private keys)

FPT_SKP_EXT.1.1
The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.2.5.3 FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.1
The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2
The TSF shall [allow the Security Administrator to set the time, synchronise time with an NTP server].

Application Note: This SFR has been updated as per TD0632

5.2.5.4 FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1
The TSF shall run a suite of the following self-tests [during initial start-up (on power on)] to demonstrate the correct operation of the TSF: [*Cryptographic POST, Software Integrity Test*].

5.2.5.5 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1
The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [*the most recently installed version of the TOE firmware/software*].

FPT_TUD_EXT.1.2
The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [*no other update mechanism*].

FPT_TUD_EXT.1.3
The TSF shall provide means to authenticate firmware/software updates to the TOE using a [*digital signature*] prior to installing those updates.

5.2.6 TOE Access (FTA)

5.2.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1
The TSF Shall, for local interactive sessions, [

- terminate the session]

after a Security Administrator-specified time period of inactivity.

5.2.6.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1
The TSF shall terminate **a remote** interactive session after a *Security Administrator-configurable time interval of session inactivity.*

5.2.6.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1
The TSF shall allow **Administrator**-initiated termination of the **Administrator's** own interactive session.

5.2.6.4 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1
Before establishing **an administrative user** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

5.2.7 Trusted Path/Channels (FTP)

5.2.7.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1
The TSF shall **be capable of using [TLS] to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [no other capabilities]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2
The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3
The TSF shall initiate communication via the trusted channel for *[audit logging]*.

5.2.7.2 FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin
The TSF shall **be capable of using [SSH, TLS, HTTPS] to** provide a communication path between itself and **authorized** remote **Administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and provides detection of modification of the channel data**.

FTP_TRP.1.2/Admin
The TSF shall permit remote **Administrators** to initiate communication via the trusted path.

FTP_TRP.1.3/Admin
The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions*.

5.3 TOE SFR Dependencies Rationale for SFRs

The NDcPP contains all the requirements claimed in this ST. As such, the dependencies are not applicable since the PP has been approved.

5.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the PP which are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table 13.

Table 13 – Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE Summary Specification
Development (ADV)	ADV_FSP.1	Basic functionality specification
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support (ALC)	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests (ATE)	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment (AVA)	AVA_VAN.1	Vulnerability survey

5.5 Assurance Measures

The TOE satisfied the identified assurance requirements. This section identifies the Assurance Measures applied by FireEye to satisfy the assurance requirements. The following table lists the details.

Table 14 – TOE Security Assurance Measures

SAR Component	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ALC_CMS.1	
ATE_IND.1	Vendor will provide the TOE for testing.
AVA_VAN.1	Vendor will provide the TOE for testing. Vendor will provide a document identifying the list of software and hardware components.

6 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 15 – TOE Summary Specification SFR Description

Requirement	Rationale
FAU_GEN.1	TOE is a standalone device. The TOE generates a comprehensive set of audit logs that identify specific TOE operations whenever an auditable event occurs. Auditable events are specified in section 5.2.1, Table 12. Each of the events is specified in the audit record is in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. For generating/importing of, changing, and deleting of certificates and associated keys, the TOE logs the certificate ID (SHA-1 Fingerprint) for TLS and "identity" for SSH which directly maps to a unique key pair. The audit trail consists of the individual audit records; one audit record for each event that occurred. As noted above, the information includes at least all of the required information. The log buffer is circular, so newer messages overwrite older messages after the buffer is full. The first message displayed is the oldest message in the buffer. The TOE does not have an interface to modify audit records.
FAU_GEN.2	The TOE ensures that each auditable event is associated with the user that triggered the event. For example, for a human user, the user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is included in the audit record.
FAU_STG_EXT.1	TOE is a standalone TOE that stores audit data locally. The TOE can be configured to export syslog records to a specified, external syslog server. The TOE also stores a limited set of audit records locally on the TOE and continues to do so if the communication with the syslog server goes down. The TOE protects communications with an external syslog server via TLS. The TOE transmits its audit events to all configured syslog servers in real-time. If the TLS connection fails, the TOE continues to store audit records locally on the TOE and will transmit any locally stored contents when connectivity to the syslog server is restored. Local audit records are stored in a directory that does not allow administrators to modify the contents. The amount of audit data that can be stored locally is configurable by setting the local log rotation parameters (e.g. see the logging files rotation CLI commands). The TOE defaults to rotating the log file when it reaches 256MB and retaining 40 compressed archives. This results in storing 10.25GB of uncompressed logs. When the local log is full, the oldest archive file is deleted to allow a new log to be created so the TOE overwrites previous audit records.
FCS_CKM.1	In support of secure cryptographic protocols, the TOE supports RSA key generation schemes as specified in FIPS 186-4, with key sizes of 2048 and 3072 bits. These keys are used in support of digital certificates and keyed authentication for TLS and SSH. The TOE supports Elliptic Curve key generation of P-256, P-384, P-521. The keys are used in support of ECDH key exchange as part of TLS. The TOE supports DHG14(2048 bits) key generation in support of DH key exchanges as part of TLS.

<table>
<tr><th>Requirement</th><th>Rationale</th></tr>
<tr><td></td><td>The TOE supports DHG14(2048 bits), DH16(4096 bits) and DH18(8192 bits) key generation in support of DH key exchanges as part of SSH.

The relevant NIST CAVP certificate number is listed in Table 4.</td></tr>
<tr><td>FCS_CKM.2</td><td>In support of secure cryptographic protocols, the TOE supports several key establishment schemes, including:
• ECC based key exchange based on NIST SP 800-56Ar3;
• FFC based key exchange based on NIST SP 800-56Ar3;
• FFC using ‘safe-prime’ based key exchange based on NIST SP 800-56Ar3
<table>
<tr><th>Scheme</th><th>SFRs</th><th>Service</th></tr>
<tr><td>ECC</td><td>FCS_TLSC_EXT.1
FCS_TLSS_EXT.1</td><td>Audit Server
Remote Administration</td></tr>
<tr><td>FFC</td><td>FCS_TLSC_EXT.1
FCS_TLSS_EXT.1</td><td>Audit Server
Remote Administration</td></tr>
<tr><td>FFC Safe Primes</td><td>FCS_TLSC_EXT.1
FCS_TLSS_EXT.1
FCS_SSHS_EXT.1</td><td>Audit Server
Remote Administration</td></tr>
</table>
The relevant NIST CAVP certificate number is listed in Table 4.
FFC safe Primes (DH Group 14, DH Group 16 and DH Group 18) are used in SSH and FFC safe Primes (DH Group 14) is used in TLS. DH Groups 14, 16 and 18 are used for implementing SSH which protects the remote management session between the remote management workstation and the TOE.</td></tr>
<tr><td>FCS_CKM.4</td><td>Table 16 identifies the keys used by the TSF. All keys from non-volatile memory are stored plaintext and are ACL protected from unauthorized access as described in FPT_SKP_EXT.1 and the Storage/Protection column. The TSF meets all requirements specified in the NDcPPv2.2e for destruction of keys. All keys within the TSF are securely destroyed as per the descriptions given in Table 16 below.</td></tr>
<tr><td>FCS_COP.1/DataEncryption</td><td>The TOE provides symmetric encryption and decryption capabilities using 128-bit and 256-bit AES as specified in ISO 18033-3, in CBC mode and CTR mode as described in ISO 10116 and GCM mode as described in ISO 19772. AES is implemented in the following protocols: TLS and SSH.
The relevant NIST CAVP certificate number is listed in Table 4.</td></tr>
<tr><td>FCS_COP.1/Hash</td><td>The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 as specified in ISO/IEC 10118-3:2004 which are implemented in the following parts of the TSF:
• NTP – SHA1
• TLS and SSH - SHA1, SHA-256, SHA-384, SHA-512;
• Digital signature verification as part of trusted update validation - SHA-256
• Hashing of passwords in non-volatile storage - SHA-512
• Conditioning entropy data – SHA-512

The relevant NIST CAVP certificate number is listed in Table 4.</td></tr>
<tr><td>FCS_COP.1/KeyedHash</td><td>The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”
HMAC is implemented in the following protocols: TLS and SSH. The characteristics of the HMACs used in the TOE are given in the following table:
<table>
<tr><th>Algorithm</th><th>Hash function</th><th>Block size</th><th>Key size</th><th>Digest size</th></tr>
<tr><td>HMAC-SHA-1</td><td>SHA-1</td><td>512 bits</td><td>160 bits</td><td>160 bits</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Requirement</th><th>Rationale</th></tr>
<tr><td></td><td><table>
<tr><td>HMAC-SHA-256</td><td>SHA-256</td><td>512 bits</td><td>256 bits</td><td>256 bits</td></tr>
<tr><td>HMAC-SHA-384</td><td>SHA-384</td><td>1024 bits</td><td>384 bits</td><td>384 bits</td></tr>
<tr><td>HMAC-SHA-512</td><td>SHA-512</td><td>1024 bits</td><td>512 bits</td><td>512 bits</td></tr>
</table>The relevant NIST CAVP certificate number is listed in Table 4.</td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>The TOE provides cryptographic signature generation and verification services using:
• RSA Signature Algorithm with key size of 2048 bits or 3072 bits,
• ECDSA Signature Algorithm with NIST curves P-256, P-384 and P-521.

RSA signature generation and verification are used for the TLS and SSH protocols. Additionally, ECDSA signature verification is used in TLS.
The relevant NIST CAVP certificate number is listed in Table 4.</td></tr>
<tr><td>FCS_HTTPS_EXT.1</td><td>The TOE provides management functionality over an HTTPS connection using the TLS implementation described above and is therefore subject to claiming FCS_HTTPS_EXT.1 in a server capacity. This applies to all the devices claimed in this Security Target, except VX Model Devices. VX model devices don't support WebUI.

The TOE does not use HTTPS in a client capacity. The TOE's HTTPS protocol complies with RFC 2818.

RFC 2818 is HTTP over TLS. The TOE web GUI operates on an explicit TCP port designed to natively speak TLS. The web server attempts to send closure Alerts prior to closing a connection in accordance with section 2.2.2 of RFC 2818.</td></tr>
<tr><td>FCS_NTP_EXT.1</td><td>The TOE supports time updates using NTPv3 and NTPv4. The TOE authenticates updates using an administrator configured symmetric key and SHA1. The TOE rejects broadcast and multicast time updates. With the help of configured symmetric key and SHA1 message digest algorithm ensures the timestamp it receives from an NTP timeserver is from an authenticated source and the integrity of the time has been maintained. The TOE does not place a limit on the number of NTP time sources that can be configured.</td></tr>
<tr><td>FCS_RBG_EXT.1</td><td>The TOE implements a NIST-approved CTR_DRBG(AES-256) and HMAC_DRBG(SHA-512), as specified in SP 800-90A.
When a request for random bits from /dev/random is made, the Kernel HMAC_DRBG(SHA-512) is used to generate the requested random bits, and the reseed threshold is decremented.
For general cryptographic operations, a CTR_DRBG(AES-256) from OpenSSL is used to generate random bits.
The entropy source used to seed the Deterministic Random Bit Generator is a random set of bits supplied from one software noise source. (This ST considers the sources 'software' simply because the entropy sources are not considered True Random Number Generators (TRNGs) based on random properties of physical processes.) The 512-bit seed value contains at least 256 bits of entropy.
The relevant NIST CAVP certificate numbers are listed in Table 4 and 5.</td></tr>
<tr><td>FCS_SSHS_EXT.1</td><td>The TOE is an SSH server, enabling administrators to remotely manage the TOE using the CLI.
The SSH server is capable of using both RSA public keys and passwords for client authentication to the remote server.
The TOE uses username presented by the client as the user's identity. The TOE then authorizes the connection if the presented public key matches an authorized public key for the claimed identity. This is verified by confirming that the presented private key corresponds to the public key associated with the user in the 'authorized_keys' file on the TOE filesystem. The presented public key algorithm is consistent with the signature</td></tr>
</table>

Requirement	Rationale
	verification algorithms selected in FCS_COP.1/SigGen. The password-based authentication acts as a fallback option in case the public key authentication fails. Large SSH packets are defined as those greater than 256K bytes. This is accomplished by buffering all data for a particular SSH packet transmission until the buffer limit is reached and then dropping the packet if this limit is exceeded which is inline with the RFC 4253. The TOE supports the following cryptographic algorithms: • ssh-rsa (RSA with SHA-1), rsa-sha2-512, rsa-sha2-256; • aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, and aes256-gcm@openssh.com; • hmac-sha2-256, hmac-sha2-512, implicit • diffie-hellman-group14-sha1, diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512. The TOE SSH server is capable of rekeying. The TOE implements two thresholds: • When 1 GB of data is transferred between using an encryption key; and • When 1 hour has elapsed. The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey. All session keys are rekeyed at the same time (e.g. confidentiality and integrity keys). The TOE server maintains an SSH server hostkey fingerprint which can be used by an SSH client to detect server authenticity.
FCS_TLSC_EXT.1	The TOE has a single trusted channel(syslog channel) which make use of TLS to connect to Audit server. The syslog channel client supports TLS protocol version 1.2 and are restricted to the following ciphersuites: • TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 • TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 Ciphersuites can be restricted through administrator configuration. The reference identifier for the syslog server is configured by the administrator using the available administrative commands in the CLI. The reference identifiers must be an IPv4 address, IPv6 address, or a hostname(FQDN). TOE does not support SRV, and URI identifiers. When the reference identifier is a hostname, the TOE compares the hostname against all the entries in the Subject Alternative Name extension. If the hostname does not match any of the entries, then the verification fails. If the certificate does not contain any entries in the SAN, the TSF will continue to compare the hostname against the Common Name (CN). If the hostname does not match the CN, then the verification fails. For both SAN and CN the hostname must be an exact match or wildcard match. In the case of a wildcard match, the wildcard must be the left-most component, wildcard matches a single component, and there are at least two non-wildcard components.

Requirement	Rationale
	TOE does not support IPv4 and IPv6 in CN; however, supported in SAN. When the reference identifier is an IP address, the TOE converts the IP address to a binary representation in network byte order. IPv4 addresses are converted directly from decimal to binary as specified in RFC 3986, IPv6 addresses are converted as specified in RFC 5952. The TOE compares the binary IP address against all the iPAddress entries in the Subject Alternative Name extension. If there is not an exact binary match, then the verification fails. The TLS channel is terminated if verification fails. The TOE does not support certificate pinning. The syslog TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: secp256r1, secp384r1, and secp521r1. The non-TOE server can choose to negotiate the elliptic curve from this set for any of the mutually negotiable elliptic curve cipher suites and no additional configuration is required. The TOE also supports key agreement using the server's RSA public key or DHG14 (2048 bits).
FCS_TLSS_EXT.1	The TOE has a single trusted path over the remote web GUI which acts as a TLS server. This applies to all the devices claimed in this Security Target, except VX Model Devices. VX model devices don't support WebUI Feature, therefore this SFR is not applicable to VX series models. The server only allows TLS protocol version 1.2 (rejecting any other protocol version, including SSL 2.0, SSL 3.0 and TLS 1.0, TLS 1.1 and any other unknown TLS version string supplied) and is restricted to the following ciphersuites by default: • TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 • TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 Ciphersuites can be restricted through administrator configuration. The TLS server is capable of negotiating ciphersuites that include DHE, and ECDHE key agreement schemes. The DHE key agreement parameters as per 'FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1' are restricted to DHG14 (2048 bits) and are hardcoded into the server. The ECDHE key agreement parameters are restricted to secp256r1, secp384r1, and secp521r1. The TOE supports session resumption of the single HTTPS context using session tickets. The session tickets are encrypted using symmetric algorithm AES with a 128-bit key and are consistent with FCS_COP.1/DataEncryption. Session tickets are structured as specified in Section 4 of RFC 5077 and encrypted using AES with a 128-bit key.
FIA_AFL.1	The TOE is capable of tracking authentication failures for each of the claimed authentication mechanisms (username/password, SSH public key) for SSH administration method and claimed authentication mechanisms (username/password) for GUI administration method.

Requirement	Rationale
	The administrator can configure the maximum number of failed attempts using the CLI interface via the aaa authentication attempts command. The configurable range is between 1 and 15 attempts. When a user account has sequentially failed authentication the configured number of times, the account will be locked. The locking mechanism can be configured to remain locked until an administrator unlocks the account, or it can be configured to unlock after a specified period of time. If the administrator is required to intervene to unlock an account, this is done using the CLI via the aaa authentication attempts reset CLI command. The aaa authentication attempts commands apply to authentication attempts through both SSH and the GUI. The failed authentication lockout does not apply to the local console, ensuring administrative access is always available. If the unlocking mechanism is automatically applied after a specified time period, then the user account will be unlocked when the specified number of seconds have elapsed since the locking mechanism was engaged. Irrespective of whether an administrator intervened or whether the elapsed time occurred, when a locked account is unlocked, the failure counter associated with that user is reset to 0. If a user succeeds at authenticating before the locking mechanism has been enabled, the failure counter is reset to 0. If the lockout attempts is set to, for example, 5 attempts, then the user will be locked out after the 5th consecutive failed login attempt. This means that the 6th and subsequent attempts will fail to gain access to the TOE even if the credential being offered is correct.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “’”, “+”, “-“, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “?”, “[“, “\”, “]”, “^”, “_”, “`”, “{“, “|”, “}”, and “~”. The minimum password length is settable by the Authorized Administrator and can range from 15 to 32 characters.
FIA_UIA_EXT.1, FIA_UAU_EXT.2	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Administrative access to the TOE is facilitated through one of several interfaces: • Directly connecting to each TOE appliance • Remotely connecting to each appliance via SSHv2 • Remotely connecting to appliance GUI via HTTPS/TLS Regardless of the interface at which the administrator interacts, the TOE prompts the user for a credential. Only after the administrative user presents the correct authentication credentials will they be granted access to the TOE administrative functionality. No TOE administrative access is permitted until an administrator is successfully identified and authenticated. The TOE provides a local password-based authentication mechanism. The process for authentication is the same for administrative access whether administration is occurring via direct connection or remotely. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative credential associated with the user account (e.g., password or SSH public/private key response). The TOE then either grants administrative access (if the combination of username and credential is correct) or indicates that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.

Requirement	Rationale
	The TOE does not permit any administrative function to be accessible until after an administrator is successfully identified and authenticated, but the TOE does display the warning banner prior to requiring user identification and authentication.
FIA_UAU.7	For all authentication at the local CLI the TOE does not echo any characters when the administrative password is entered so that the password is obscured.
FIA_X509_EXT.1/Rev FIA_X509_EXT.2 FIA_X509_EXT.3	The TOE performs X.509 certificate validation at the following points: • TOE TLS client authentication of server X.509 certificates; • When certificates are loaded into the TOE, such as when importing CAs, certificate responses and other device-level certificates (such as the web server certificate presented by the TOE TLS web GUI[14]). In all scenarios, certificates are checked for several validation characteristics: • If the certificate 'notAfter' date is in the past, then this is an expired certificate which is considered invalid; • If the certificate 'notBefore' date is in the future, then the certificate is considered invalid; • The certificate chain must terminate with a trusted CA certificate; • Server certificates consumed by the TOE TLS client must have a 'serverAuthentication' extendedKeyUsage purpose; A trusted CA certificate is defined as any certificate loaded into the TOE trust store that has, at a minimum, a basicConstraints extension with the CA flag set to TRUE. Certificate revocation checking is performed on the leaf and intermediate CA certificates using OCSP responders as a part of authentication step. There is no difference in handling of revocation checking during authentication irrespective of whether a full certificate chain or only a leaf certificate is being presented. The OCSP signing certificate must have the OCSP signing purpose in the extendedKeyUsage extension. As X.509 certificates are not used for either trusted updates or firmware integrity self-tests, the code-signing purpose is not checked for in the extendedKeyUsage, hence the requirement for Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field is trivially satisfied. The TOE has a trust store where root CA and intermediate CA certificates can be stored. The trust store is not cached: if a certificate is deleted, it is immediately untrusted. If a certificate is added to the trust store, it is immediately trusted for its given scope. The TOE compares each certificate presented as part of a communication to every certificate included in the trust store. If the presented certificate matches a certificate chain included in the trust store, the connection is validated and allowed to proceed. If a presented certificate does not match a certificate chain within the trust store, the connection is immediately rejected. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for all TLS and HTTPS peer entities. Certificates are used to authenticate and establish a secure communication channel for the audit server. The TOE allows each TLS service to be configured with its certificate in the TLS profile. Once the certificate is configured for an audit server using a TLS profile, that certificate will be used for all audit server connection authentication.

[14] VX series models doesn't support Web UI Feature and hence this selection-based SFR is not applicable to the VX Series Models.

Requirement	Rationale
	The X.509 certificates for each of the given scenarios are validated using the certificate path validation algorithm defined in RFC 5280, which can be summarized as follows: • The public key algorithm and parameters are checked • The current date/time is checked against the validity period revocation status is checked • Issuer name of X matches the subject name of X+1 • Name constraints are checked • Policy OIDs are checked • Policy constraints are checked; issuers are ensured to have CA signing bits • Path length is checked • Critical extensions are processed If, during the entire trust chain verification activity, any certificate under review fails a verification check, then the entire trust chain is deemed untrusted and the TLS connection is terminated, as TLS is only trusted channel. As part of the verification process, OCSP is used to determine whether the certificate is revoked or not. If the OCSP responder cannot be contacted, then the TOE will choose to automatically reject the certificate in this case. The administrator does not determine the default handling of certificates**.** Instructions for configuring the trusted IT entities to supply appropriate X.509 certificates are captured in the guidance documents. The TOE is capable of generating certificate signing requests (CSRs). The user can select the size of the key as 2048 or 3072 bits. In addition to adding the public key to the certificate details, the user can provide information for the Common Name, Organization, Organizational Unit, and Country. No device-specific details are collected and added to the certificate request to be signed.
FMT_MOF.1/Functions	The TOE restricts the ability to modify the behavior of transmission of audit data to an external IT entity (Audit Server(FQDN or IP address), OCSP responder, TLS ciphersuites), handling of audit data (number of logs to retain) to Security Administrators.
FMT_MOF.1/ManualUpdate	The TOE restricts the ability to perform software updates to the Admin role.
FMT_MTD.1/CoreData	The only access the TOE allows prior to the successful identification and authentication of a user, is the access banner displayed at each login prompt. No other security functions are accessible. The TOE implements role-based access control to manipulate the TSF data. Administrative users are required to login before being provided with access to any administrative functions. The TOE supports several types of administrative user roles. Collectively these roles comprise the Security Administrator. The supported roles include: • Admin: The system administrator is a “super user” who has all capabilities. The primary function of this role is to configure the system. • Monitor: The system monitor has read-only access to some things the admin role can change or configure. • Operator: The system operator has a subset of the capabilities associated with the admin role. Its primary function is configuring and monitoring the system. • Analyst: The system analyst focuses on data plane analysis and possesses several capabilities, including setting up alerts and reports. • Auditor: The system auditor reviews audit logs and performs forensic analysis to trace how events occurred.

Requirement	Rationale
	Each of the predefined administrative roles have a set of permissions that will grant them access to the TOE data, though with some roles, the access is limited. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to all the privileged levels. The term "Security Administrator" is used in this ST to refer to any user which has been assigned a role that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Users without the appropriate privilege level do not have access to TOE functionality including administration of X.509 certificates via TOE's trust store.
FMT_MTD.1/CryptoKeys	The TOE implements a set of cryptographic protocols and algorithms. The users are only granted limited access to the keys directly. All cryptographic protocols and algorithms the TOE implements are listed in Table 4 (Sect. 1.3.2.2). Cryptographic keys the TOE uses together with their storage and method of destruction are listed in Table 16 (Sect. 6.1) Management of cryptographic keys is through the CLI and WebUI[15] as part of managing and configuring SSHv2 and TLS. All key management operations occur through the CLI as well as WebUI commands.
FMT_SMF.1	The TOE can be managed via the CLI (console & SSH) or GUI (HTTPS). The specific management capabilities include: • Ability to administer the TOE locally (CLI); • Ability to administer the TOE remotely (GUI & CLI); • Ability to configure the access banner (GUI & CLI); • Ability to configure the session inactivity time before session termination (CLI); • Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates (CLI); • Ability to configure the authentication failure parameters (CLI); • Ability to modify the behavior of the transmission of audit data to an external IT entity and the handling of local audit data (CLI); • Ability to manage the cryptographic keys (GUI & CLI) • Ability to configure the cryptographic functionality (CLI); • Ability to re-enable an Administrator account (CLI); • Ability to set the time which is used for time-stamps (GUI & CLI); • Ability to configure NTP (CLI); • Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors (GUI & CLI); • Ability to import X.509v3 certificates to the TOE's trust store (GUI & CLI) • Ability to manage the trusted public keys database (CLI).
FMT_SMR.2	See FMT_MTD.1/CoreData.
FPT_APW_EXT.1	The TOE stores Security Administrator passwords. All passwords are stored in a secure directory that is not readily accessible to administrators. The passwords are stored SHA-512 hashed and not in plaintext.
FPT_SKP_EXT.1	The TOE stores all private keys in plaintext in a secure directory that is not readily accessible to administrators; hence no interface access. Refer to section Table 16 for key storage details.

[15] Only VX series models doesn't support Web UI Feature.

Requirement	Rationale
FPT_TST_EXT.1	The TOE runs a suite of self-tests during initial start-up to verify its correct operation. If any of the tests fail, the TOE will enter into an error state until an Administrator intervenes. During the system bootup process (power on or reboot), all the cryptographic modules perform the Cryptographic Power on Startup Test (POST). The Cryptographic POST verifies that each cryptographic algorithm specified in FCS_COP.1 requirements is passing a Known Answer Test (KAT). The KAT demonstrates that the algorithm is functioning properly by invoking the algorithm with hard coded keys and messages and comparing the result to a pre-computed, known to be correct value. TOE performs Cryptographic POST that is indicated as 'FIPS crypto POST'. The Software Integrity Test is run automatically on start-up, and whenever the system images are loaded. A digital signature verification is used to confirm the image file to be loaded has not been corrupted and has maintained its integrity. These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected. Both of these functions are required to ensure that the TOE is operating as expected and data that the user expects to be encrypted in not transferred in plaintext.
FPT_TUD_EXT.1	The Security Administrator can query the software version running on the TOE and the most recently downloaded software version, so the TOE does support delayed activation. Following successful authentication authorized administrators can perform management actions such as query the current version of the TOE software using CLI commands 'show version'. When software updates are made available by FireEye, the Security Administrator can download them from authorized website, and install them manually, at which time the system first verifies the integrity of the downloaded image before installing. No other update mechanism is available. Software updates are downloaded to the TOE via an 'image fetch' command on the CLI. Software images will not be installed without explicit administrative intervention. The TOE image files are digitally signed (2048-bit RSA/SHA-256) by the vendor, so their integrity can be verified during the upgrade process. An image that fails an integrity check will not be installed. An image that passes an integrity check will be installed. The new image remains inactive until the TOE is rebooted to the new image. Installed image integrity is further verified against tampering before the new image is allowed to become active on reboot, and failure will revert to the previous valid image.
FPT_STM_EXT.1	The clock function is reliant on the system clock provided by the underlying hardware. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The time can be manually updated by a Security Administrator or automatically updated using NTP synchronization for both physical and virtual TOE.
FTA_SSL_EXT.1 FTA_SSL.3	A Security Administrator can configure maximum inactivity time for administrative sessions through the TOE GUI and CLI interfaces. The configuration of inactivity periods can be configured to be anywhere from 0.25-35791 minutes and are applied on a per user interface basis. The configured inactivity period will be applied to both local and remote sessions in the same manner. When the interface has been idle for more than the configured period of time, the session will be terminated and will require authentication to establish a new session.
FTA_SSL.4	A Security Administrator is able to exit out of both local and remote administrative sessions using the exit command from CLI and using 'LOGOUT' option from GUI.

Requirement	Rationale
FTA_TAB.1	Security Administrators can define a custom login banner that will be displayed at the following available interfaces: • Local CLI • Remote CLI • Remote GUI This banner will be displayed prior to allowing Security Administrator access through those interfaces. The advisory notice and the consent warning message can be configured differently for remote and local access interface.
FTP_ITC.1	The TOE supports communication with following authorized IT entity: • Audit Server This connection is secured through a TLS connection, with the TOE acting as a TLS client. The encryption uses AES to protect the data from disclosure, and HMACs to ensure data integrity by verifying that it has not been modified. TLS provides assured identification of the non-TSF endpoint by validating X.509 certificates. The TOE retains a trusted store of certificate authorities which it uses to verify digital signatures on those non-TSF certificates. The TOE is responsible for initiating the trusted channel with the external trusted IT entities.
FTP_TRP.1/Admin	All remote administrative communications take place over a secure encrypted session. Remote CLI connections take place over an SSHv2 tunnel. The SSHv2 session is encrypted using AES encryption to protect confidentiality and uses HMACs to protect integrity of traffic. Remote GUI[16] connections take place over a HTTPS/TLS connection. The TLS session is encrypted using AES encryption and uses HMACs to protect integrity. The remote administrators can initiate both SSHv2 and HTTPS/TLS communications with the TOE.

[16] VX series models doesn’t support Web UI Feature and hence they cannot be managed through remote WebUI.

6.1 Cryptographic Key Destruction

The table below describes the key zeroization provided by the TOE and as referenced in FCS_CKM.4.

Table 16 – Key Zeroization

Keys/CSPs	Type	Origin	Keys/CSP Storage Location	Method of Zeroization
Diffie Hellman private key	DH Key	TOE generated	RAM	Keys are overwritten with zeros when session closes.
Diffie Hellman public key	DH Key	TOE generated	RAM	Keys are overwritten with zeros when session closes.
SSH Private Key	RSA Private Key	TOE generated	ACL protected directory	Key is overwritten with zeros when the compliance declassify zeroize command is issued.
SSH Public Key	RSA Public Key	TOE generated	n/a - public	Key is overwritten with zeros when the compliance declassify zeroize command is issued.
SSH Session Key	AES Key	TOE generated	RAM	Keys are overwritten with zeros when session closes.
TLS Private Key	RSA Private Key	TOE generated	ACL protected directory	Key is overwritten with zeros when the compliance declassify zeroize command is issued.
TLS Private Key	ECDSA Private Key	Administrator Configured	ACL protected directory	Key is overwritten with zeros when the compliance declassify zeroize command is issued.
TLS Public Key	RSA Public Key	TOE generated	n/a - public	Key is overwritten with zeros when the compliance declassify zeroize command is issued.
TLS Public Key	ECDSA Public Key	Administrator Configured	n/a - public	Key is overwritten with zeros when the compliance declassify zeroize command is issued.
TLS Session Encryption Key	AES Key	TOE generated	RAM	Keys are overwritten with zeros when session closes.
TLS Session Integrity Key	HMAC Key	TOE generated	RAM	Keys are overwritten with zeros when session closes.
NTP Key	NTP Key	Administrator Configured	ACL protected directory	Key is overwritten with zeros when the compliance declassify zeroize command is issued.

Non-volatile keys are overwritten with zeros using a single pass when the administrator disables CC mode. As part of the disablement function, the device is power cycled to zeroize keys in volatile memory.

RAM is volatile storage location and ACL protected directories are non-volatile storage location.

6.2 CAVP Table

Table 17 – CAVP Table

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_CKM.1	RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	Trellix OpenSSL FIPS Object Module Version 1.0.3	RSA KeyGen (FIPS186-4)	A2624
	ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	Trellix OpenSSL FIPS Object Module Version 1.0.3	ECDSA KeyGen (FIPS186-4) ECDSA KeyVer (FIPS186-4)	A2624
	FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1	Trellix OpenSSL FIPS Object Module Version 1.0.3	DSA KeyGen (FIPS186-4)	A2624
	FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526].	Trellix OpenSSL FIPS Object Module Version 1.0.3	Safe Primes Key Generation	Testing for FFC Schemes using safe-prime groups is done as part of testing in CKM.2.1.
FCS_CKM.2	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3 "Recommendation for Pair-Wise Key Establishment	Trellix OpenSSL FIPS Object Module Version 1.0.3	KAS ECC SSC Sp800-56Ar3 (Domain Parameter Generation)	A2624

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	Schemes Using Discrete Logarithm Cryptography”			
	Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3 “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”	Trellix OpenSSL FIPS Object Module Version 1.0.3	KAS-FFC-SSC Sp800-56Ar3 (Domain Parameter Generation)	A2624
	FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526].	NA	No NIST CAVP, CCTL has performed all assurance/evaluation activities.	This test has been successfully tested in FTP_TRP.1/Admin Test #1, FTP_ITC.1 Test #1 and FCS_SSHS_EXT.1.7 Test #2 since only SSH SFRs use safe-prime groups.
FCS_COP.1/ DataEncryption	The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in* [CBC, CTR, GCM] *mode* and cryptographic key sizes [128 bits, 256 bits] that meet the following: *AES as specified in ISO 18033-3,* [CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772].	Trellix OpenSSL FIPS Object Module Version 1.0.3	AES-CBC, AES-CTR, AES-GCM	A2624
FCS_COP.1/ SigGen	Elliptic Curve Digital Signature Algorithm and cryptographic key	Trellix OpenSSL FIPS Object	ECDSA SigGen (FIPS186-4)	A2624

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	sizes [256, 384, 512 bits] For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4	Module Version 1.0.3	ECDSA SigVer (FIPS186-4)	
	RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048, 3072 bits] For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	Trellix OpenSSL FIPS Object Module Version 1.0.3	RSA SigGen (FIPS186-4) RSA SigVer (FIPS186-4)	A2624
FCS_COP.1/ Hash	The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits that meet the following: ISO/IEC 10118-3:2004.	Trellix OpenSSL FIPS Object Module Version 1.0.3	SHA-1, SHA-256, SHA-384, SHA-512	A2624
FCS_COP.1/ KeyedHash	The TSF shall perform keyed-hash message authentication in	Trellix OpenSSL FIPS Object	HMAC-SHA-1, HMAC-SHA-256,	A2624

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	accordance with a specified cryptographic algorithm [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [160 bits, 256 bits, 384 bits, 512 bits] and message digest sizes [160, 256, 384, 512] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.	Module Version 1.0.3	HMAC-SHA-384, HMAC-SHA-512	
FCS_RBG_EXT.1	CTR_DRBG (AES-256) HMAC DRBG (SHA-512)	Trellix OpenSSL FIPS Object Module Version 1.0.3	Counter DRBG HMAC DRBG (SHA-512)	A2624

7 Acronym Table

Acronyms should be included as an Appendix in each document.

Table 18 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
CRL	Certificate Revocation List
DTLS	Datagram Transport Layer Security
EP	Extended Package
GUI	Graphical User Interface
IP	Internet Protocol
NDcPP	Network Device Collaborative Protection Profile
NIAP	Nation Information Assurance Partnership
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PP	Protection Profile
RSA	Rivest, Shamir & Adleman
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security

TSF	TOE Security Functionality
	TSF = TOE for pND
	TSF = TOE + VS for vND

TSS	TOE Summary Specification