FireEye CM, FX, EX, and NX Series Appliances

FireEye, Inc.
Common Criteria Security Target
Document Version: 1.0

Prepared By:
Acumen Security
18504 Office Park Dr
Montgomery Village, MD 20886

www.acumensecurity.net

Table Of Contents

Revision History

Version	Date	Description
0.1	April 4, 2015	Initial release
0.2	June 19, 2015	Updated to reflect evaluation, comments, etc.
0.3	July 30. 2015	Updated based on validator comments
1.0	August 7, 2015	Updated to 1.0 and complete validators comments.

1 Security Target Introduction

1.1 Security Target and TOE Reference

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

Category	Identifier
ST Title	FireEye CM, FX, EX, and NX Series Appliances Security Target
ST Version	1.0
ST Date	August 7, 2015
ST Author	Acumen Security, LLC.
TOE Identifier	FireEye CM, FX, EX, and NX Series Appliances
TOE Hardware Versions	CM Series Appliances: CM 4400, CM 7400, CM 9400 FX Series Appliances: FX 5400, FX 8400 EX Series Appliances: EX 3400, EX 5400, EX 8400, EX 8420 NX Series Appliances: NX 900, NX 1400, NX 2400, NX 4400, NX 4420, NX 7400, NX 7420, NX 7500, NX 10000, NX 9450, NX 10450
TOE Software Version	CM Series Appliances: 7.6.0 FX Series Appliances: 7.6.0 EX Series Appliances: 7.6.0 NX Series Appliances: 7.6.0
TOE Developer	FireEye, Inc.
Key Words	Network Device, Security Appliance,

Table 1 TOE/ST Identification

1.2 TOE Overview

The TOE consists of several families of appliances working together to form the network protection solution. Collectively, the product families provide email, file, and network security with a centralized management platform. Each family performs a specific role in the overall network protection, as described in section 1.3 below.

1.2.1 TOE Product Type

FireEye CM, FX, EX, and NX Series Appliances are a centrally managed network protection solution comprised of multiple 1RU or 2RU appliances. Each appliance runs a custom-built hardened version of Linux with only the required services enabled.

1.3 TOE Description

The TOE is comprised of several families of appliance. This section provides a description of each of the appliances within the FireEye CM, FX, EX, and NX Series Appliances Target of Evaluation (TOE). The following sections provide an overview of the functionality provided by each appliance family and the physical characteristics of each platform within each family.

1.3.1 CM Series Appliances: CM 4400, CM 7400, CM 9400

The FireEye® CM series is a group of management platforms that consolidates the administration, reporting, and data sharing of the FireEye NX, EX, and FX series in one easy-to-deploy, network-based platform. Within the FireEye deployment, the FireEye CM enables real-time sharing of the auto-generated threat intelligence to identify and block advanced attacks targeting the organization. It also enables centralized configuration, management, and reporting of FireEye platforms.

	CM 4400	CM 7400	CM 9400
Network Ports	2x 10/100/1000BASE-T Ports	2x 10/100/1000BASE-T Ports	2x 10/100/1000BASE-T Ports

	CM 4400	CM 7400	CM 9400
Storage	4x 600 GB HDD, RAID 10, 2.5 inch	4x 600 GB HDD, RAID 10, 2.5 inch	4x 800 GB SSD, RAID 10, 2.5 inch
Enclosure	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Processors	AMD Opteron 6328	AMD Opteron 6380	AMD Opteron 6380
Crypto Algorithm Implementation	FireEye Algorithms Implementation, FireEye Image Signature Verification	FireEye Algorithms Implementation, FireEye Image Signature Verification	FireEye Algorithms Implementation, FireEye Image Signature Verification
Operating System	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)
Application Software	image-cms.img	image-cms.img	image-cms.img

Table 2 CM Series Appliances

1.3.2 FX Series Appliances: FX 5400, FX 8400

The FireEye® FX series is a group of threat prevention platforms that protect content 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 spread to file shares and content repositories. The FireEye FX platform analyzes network file shares and enterprise content management stores to detect and quarantine malware brought in by employees and others that bypass next-generation firewalls, IPS, AV, and gateways.

	FX 5400	FX 8400
Performance	Up to 80,000 Files Per Day	Up to 160,000 Files Per Day
Network Interface Ports	2x 10/100/1000BASE-T Ports	2x 10/100/1000BASE-T Ports
Storage	2x 600 GB HDD, RAID 1, 2.5 inch, FRU	2x 600 GB HDD, RAID 1, 2.5 inch, FRU
Enclosure	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Processors	AMD Opteron 6328	AMD Opteron 6380
Crypto Algorithm Implementation	FireEye Algorithms Implementation, FireEye Image Signature Verification	FireEye Algorithms Implementation, FireEye Image Signature Verification
Operating System	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)
Application Software	image-fmps.img	image-fmps.img

Table 3 FX Series Appliances

1.3.3 EX Series Appliances: EX 3400, EX 5400, EX 8400, EX 8420

The FireEye® EX series secures against advanced email attacks. As part of the FireEye Threat Prevention Platform, the FireEye EX uses signature-less technology to analyze every email attachment and successfully quarantine spear-phishing emails used in advanced targeted attacks.

	EX 3400	EX 5400	EX 8400	EX 8420
Performance	Up to 150,000 emails per day	Up to 300,000 emails per day	Up to 600,000 emails per day	Up to 600,000 emails per day
Network Ports	2x 10/100/ 1000BASE-T Ports	2x 10/100/ 1000BASE-T Ports	2x 10/100/1000BASE-T Ports	2x 1000BASE-SX Fiber Optic Ports
Storage	2x 600 GB HDD, RAID 1, 2.5 inch	2x 600 GB HDD, RAID 1, 2.5 inch	2x 600 GB HDD, RAID 1, 2.5 inch	2x 600 GB HDD, RAID 1, 2.5 inch
Enclosure	1RU, Fits 19 inch Rack	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Processors	AMD Opteron 6328	AMD Opteron 6328	AMD Opteron 6380	AMD Opteron 6380
Crypto Algorithm	FireEye Algorithms	FireEye Algorithms	FireEye Algorithms	FireEye Algorithms

	EX 3400	EX 5400	EX 8400	EX 8420
Implementation	Implementation, FireEye Image Signature Verification	Implementation, FireEye Image Signature Verification	Implementation, FireEye Image Signature Verification	Implementation, FireEye Image Signature Verification
Operating System	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)
Application Software	image-emps.img	image-emps.img	image-emps.img	image-emps.img

Table 4 EX Series Appliances

1.3.4 NX Series Appliances: NX 900, NX 1400, NX 2400, NX 4400, NX 4420, NX 7400, NX 7420, NX 7500, NX 10000, NX 9450, NX 10450

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

	NX 900	NX 1400	NX 2400	NX 4400
Performance (User Count)	50	100	500	2500
Network Ports	2x 10/100/1000 BASE- T Port	2x 10/100/1000 BASE- T Port	4x 10/100/1000 BASE-T Ports	4x 10/100/1000 BASE- T Ports
Storage	Single 500 GB HDD	Single 500 GB HDD	Single 500 GB HDD	2x 600 GB HDD
Enclosure	1RU, Fits 19 inch Rack	1RU, Fits 19 inch Rack	1RU, Fits 19 inch Rack	1RU, Fits 19 inch Rack
Processors	AMD Opteron 3365	AMD Opteron 4334	AMD Opteron 4334	AMD Opteron 6328
Crypto Algorithm Implementation	FireEye Algorithms Implementation, FireEye Image Signature Verification	FireEye Algorithms Implementation, FireEye Image Signature Verification	FireEye Algorithms Implementation, FireEye Image Signature Verification	FireEye Algorithms Implementation, FireEye Image Signature Verification
Operating System	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)
Application Software	image-wmps.img	image-wmps.img	image-wmps.img	image-wmps.img

Table 5 NX Series Appliances NX 900, NX 1400, NX 2400, NX 4400

	NX 4420	NX 7400	NX 7420
Performance (User Count)	2500	10000	10000
Network Ports	4x 1000 BASE-SX Fiber Optic Port	4x 10/100/1000 BASE- T Ports	4x 1000 BASE-SX Fiber Optic Port
Storage	2x 600 GB HDD	2x 600 GB HDD	2x 600 GB HDD
Enclosure	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Processors	AMD Opteron 6328	AMD Opteron 6380	AMD Opteron 6380
Crypto Algorithm Implementation	FireEye Algorithms Implementation, FireEye Image Signature	FireEye Algorithms Implementation, FireEye Image Signature	FireEye Algorithms Implementation, FireEye Image Signature

	NX 4420	NX 7400	NX 7420
	Verification	Verification	Verification
Operating System	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)
Application Software	image-wmps.img	image-wmps.img	image-wmps.img

Table 6 NX Series Appliances NX 4420, NX 7400, NX 7420

	NX 7500	NX 9450	NX 10000	NX 10450
Performance (User Count)	10000	20000	40000	40000
Network Ports	4x 10/100/1000 BASE- T Ports	4x SFP+, 4xSFP ports	2x 10GBASE - SR/ SW 850nm	8 x SFP+
Storage	4x 900 GB HDD	4x 900 GB HDD	2x 800 GB SSD	4x 800 GB SSD, RAID
Enclosure	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Processors	Intel Xeon E5-2680	AMD Opteron 6380	AMD Opteron 6380	AMD Opteron 6380
Crypto Algorithm Implementation	FireEye Algorithms Implementation, FireEye Image Signature Verification	FireEye Algorithms Implementation, FireEye Image Signature Verification	FireEye Algorithms Implementation, FireEye Image Signature Verification	FireEye Algorithms Implementation, FireEye Image Signature Verification
Operating System	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)	CentOS 6.5 (kernel version 3.10.53)
Application Software	image-wmps.img	image-wmps.img	image-wmps.img	image-wmps.img

Table 7 NX Series Appliances NX 7500, NX 9450, NX 10000, NX 10450

1.4 TOE Evaluated Configuration

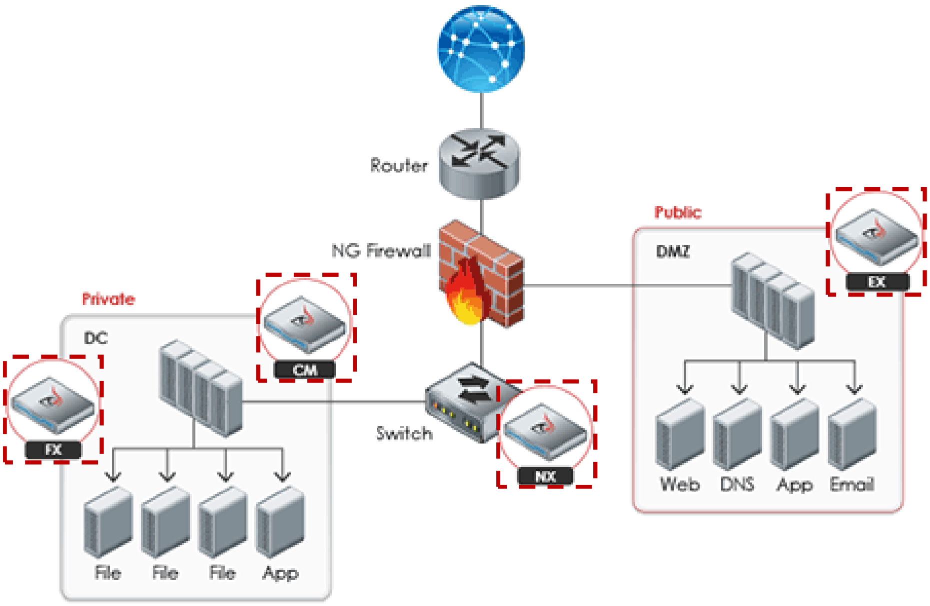
The TOE evaluated configuration consists of at least two of the products listed above. At minimum, the TOE must include a CM appliance to facilitate configuration of the other network devices and at least one of the other network devices listed above (FX, EX, or NX). The deployed network devices (FX, EX, or NX) are collectively referred to as the Local Management System (LMS). The evaluated TOE must include at least one FX, EX, or NX appliance but may include a combination of all of the appliances.

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

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with Web Browser/SSH Client	Yes	This includes any IT Environment Management workstation with a Web Browser and a SSH client installed that is used by the TOE administrator to support TOE administration through HTTPS and SSH protected channels. Any SSH client that supports SSHv2 may be used. Any web browser that supports TLS 1.0 or greater may be used.
NTP Server	No	The TOE supports communications with an NTP server to synchronize date and time.
Syslog server	No	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.
LDAP AAA Server	No	This includes any IT environment LDAP AAA server that provides authentication services to TOE administrators.

Table 8 IT Environment Components

The following figure provides a visual depiction of an example of a typical TOE deployment. The TOE boundary is surrounded with **hashed red lines**. Each TOE interconnection is through an SSH secured channel.



1.5 TOE Architecture

1.5.1 Physical Boundaries

The TOE is a hardware and software solution that is comprised of the security appliance models described above in Section 1.3. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the FireEye FIPS 140-2 and Common Criteria Addendum document and is downloadable from the http://fireeye.com web site.

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 in Section 1.1. In addition, the software images are also downloadable from the FireEye website. A login ID and password is required to download the software image.

1.5.2 Logical Boundaries

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- Security Audit
- Cryptography Support
- User Data Protection
- Identification & Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channel
- TOE Access

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the [NDPP] as necessary to satisfy testing/assurance measures prescribed therein.

1.5.2.1 Security Audit

The FireEye CM, FX, EX, and NX Series Appliances provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include: failure on invoking cryptographic functionality such as establishment, termination and failure of a TLS session; establishment, termination and failure of an SSH session; modifications to the group of users that are part of the authorized administrator roles; all use of the user identification mechanism; any use of the authentication mechanism; any change in the configuration of the TOE, changes to time, initiation of TOE update, indication of completion of TSF self-test, maximum sessions being exceeded, termination of a remote session; and initiation and termination of a trusted channel.

The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using TLS and the TOE can determine when communication with the syslog server fails.

The logs for all of the appliances can be viewed on the TOE via the CM GUI. Audit record generated on LMS are sent to the CM for review via an SSH secured connection. The records include the date/time the event occurred, the event/type of event, the user ID associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to clear audit data stored locally on the TOE.

1.5.2.2 Cryptographic Support

The TOE provides cryptographic support for the following features,

- TLS connectivity with the following entities:
  - External LDAP Server
  - Audit Server
  - Management Web Browser
- SSH connectivity with the following entities:
  - Inter-TOE communications
  - Management SSH Client
- Secure software update

The cryptographic services provided by the TOE are described below.

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

Table 9 TOE Provided Cryptography

This cryptography has been validated for conformance to the requirements of FIPS 140-2, as identified below. Each of these algorithms are implemented as either part of the FireEye Algorithms Implementation version 1.0 (RSA, ECDSA, DRBG, SHS, HMAC, and AES) or as part of FireEye Image Signature Verification Implementation (RSA and SHS).

Algorithm	FIPS 140 CAVP Certificate #
RSA	Cert. #1759, 1758
ECDSA	Cert. #696
SP 800-90 DRBG	Cert. #843
SHS	Cert. #2837, 2836
HMAC-SHS	Cert. #2195
AES	Cert. #3447

Table 10 FIPS 140 Algorithm Testing References

1.5.2.3 User Data Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

1.5.2.4 Identification and Authentication

The TOE performs three types of authentication: device-level authentication of remote IT Environment devices (e.g., audit servers and LDAP servers), device-level authentication between separate TOE components (e.g., CM to FX authentication and vice versa) and user authentication for the Authorized Administrator of the TOE. Device-level authentication of remote IT Environment devices allows the TOE to establish a secure channel with an IT Environment trusted peer. The secure channel is established only after each device authenticates the other. This device-level authentication is performed via TLS authentication. Device-level authentication for inter-TOE communications allows the TOE to establish a secure channel between separate TOE components to facilitate secure administration and audit transmission. The secure channel is established only after each device authenticates the other. This device-level authentication is performed via SSH authentication.

The TOE provides authentication services for administrative users to connect to the TOEs secure GUI or CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. In the Common Criteria evaluated configuration, the TOE is configured to require a minimum password length of 15 characters, as well as, mandatory password complexity rules. The TOE provides two administrator authentication methods:

- Authentication against a local user database
- Authentication via LDAP over TLS (part of the TOE IT environment)

Password-based authentication can be performed on any TOE administrative interface including local CLI, remote CLI over SSH, and remote GUI over HTTPS.

1.5.2.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. Management can take place over a variety of interfaces including:

- Local console command line administration at each of the appliances
- Remote command line administration via SSHv2 at each of the appliances
- Remote GUI administration via TLS

While the TOE provides multiple interfaces to perform administration, all functionality available via the command line interface is limited. All general and security administration for all of the appliances will take place at one of several locations including,

- Remote GUI administration to the appliance being managed over HTTPS,
- Remote GUI administration to the CM appliance which in turn manages the remote appliances over HTTPS,
- Remote CLI administration to each appliance over an SSH tunnel over HTTPS,
- Local administration via direction connection.

Configuration changes associated with the paired LMS devices are pushed from the CM appliance to the associated LMS device over an SSHv2 secured channel.

The TOE provides the ability to securely manage:

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE; and
- Update to the TOE.

The TOE supports several administrator roles, including,

- Admin: The system administrator is a "super user" who has all capabilities.
- Monitor: The system monitor has read-only access
- Operator: The system operator has a subset of the capabilities associated with the admin role.
- Analyst: The system analyst focuses on data plane analysis.
- Auditor: The system auditor reviews audit logs and performs forensic analysis.

These roles are collectively known as the "Authorized Administrator"

The TOE supports the configuration of login banners to be displayed at time of login and inactivity timeouts to terminate administrative sessions after a set period of inactivity.

1.5.2.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally the TOE software is a custom-built hardened version of Linux and access to memory space is restricted to only required software services.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually, or can configure the TOE to use NTP to synchronize the TOE's clock with an external time source. Finally, the TOE performs testing to verify correct operation of the security appliances themselves.

The TOE verifies all software updates via digital signature and requires administrative intervention prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

1.5.2.7 Trusted Path/Channels

The TOE supports several types of secure communications, including,

- Trusted paths with remote administrators over SSH,
- Trusted paths with remote administrators over TLS,
- Trusted channels with remote IT Environment audit servers over TLS,
- Trusted channels with remote IT Environment LDAP servers over TLS,
- Trusted inter-TOE communications between separate TOE components over SSH.

Each of these trusted paths/channels are secured using either TLS or SSH.

1.5.2.8 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE also displays an Authorized Administrator configured banner on both the GUI and CLI management interfaces prior to allowing any administrative access to the TOE.

2 Conformance Claims

2.1 CC Conformance

This TOE is conformant to:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 4, September 2012: Part 2 extended
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 4, September 2012: Part 3

2.2 Protection Profile Conformance

This TOE is conformant to:

- Protection Profile for Network Devices, Version 1.1, 08 June 2012 [NDPP].
- Security Requirements for Network Devices Errata #3, 3 November 2014 [ERRATA#3]

2.3 Conformance Rationale

This Security Target provides exact conformance to Version 1.1 of the Network Device Protection Profile. The security problem definition, security objectives and security requirements in this Security Target are all taken from the Protection Profile performing only operations defined there.

3 Security Problem Definition

The security problem definition has been taken from [NDPP] and is reproduced here for the convenience of the reader.

3.1 Assumptions

3.1.1 A.NO_GENERAL_PURPOSE

It is assumed that 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.

3.1.2 A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

3.1.3 A.TRUSTED_ADMIN

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.2 Threats

3.2.1 Communications with the TOE (T.UNAUTHORIZED_ACCESS)

Network devices communicate with other network devices, as well as administrators, over the network. The endpoints of the communication can be both geographically and logically distant from the TOE, and pass through a variety of other systems. These intermediate systems may be under the control of the adversary, and offer an opportunity for communications with the TOE to be compromised. While these communications fall into three distinct categories (the TOE communicating with a remote administrator; the TOE communicating in a distributed processing environment with another instance or instances of itself; and the TOE communicating with another IT entity that is not another instance of the TOE (e.g., an NTP server or a peer router)), the threats to the communication between these endpoints are the same.

Plaintext communication with the TOE may allow critical data (such as passwords, configuration settings, and routing updates) to be read and/or manipulated directly by intermediate systems, leading to a compromise of the TOE. Several protocols can be used to provide protection; however, each of these protocols have myriad options that can be implemented and still have the overall protocol implementation remain compliant to the protocol specification listed in the RFC. Some of these options can have negative impacts on the security of the connection. For instance, using a weak encryption algorithm (even one that is allowed by the RFC, such as DES) can allow an adversary to read and even manipulate the data on the encrypted channel, thus circumventing countermeasures in place to prevent such attacks. Further, if the protocol is implemented with little-used or non-standard options, it may be compliant with the protocol specification but will not be able to interact with other, diverse equipment that is typically found in large enterprises.

Even though the communication path is protected, there is a possibility that the external entity (be it a remote administrator, another instance of the distributed TOE, or a trusted IT entity such as a peer router) could be duped into thinking that a malicious third-party user or system is the TOE. For instance, a middleman could intercept a connection request to the TOE, and respond to the external entity as if it were the TOE. In a similar manner, the TOE could also be duped into thinking that it is establishing communications with a legitimate remote entity when in fact it is not. An attacker could also mount a malicious man-in-the-middle-type of attack, in which an intermediate system is compromised, and the traffic is proxied, examined, and modified by this system. This attack can even be mounted via encrypted communication channels if appropriate countermeasures are not applied. These attacks are, in part, enabled by a malicious attacker capturing network traffic (for instance, an authentication session) and "playing back" that traffic in order to fool an endpoint into thinking it was communicating with a legitimate remote entity.

3.2.2 Malicious Updates (T.UNAUTHORIZED_UPDATE)

Since the most common attack vector used involves attacking unpatched versions of software containing well-known flaws, updating network device firmware is necessary to ensure that changes to threat environment are addressed. Timely application of patches ensures that the system is a "hard target", thus increasing the likelihood that product will be able to maintain and enforce its security policy. However, the updates to be applied to the product must be trustable in some manner; otherwise, an attacker can write their own "update" that instead contains malicious code of their choosing, such as a rootkit, bot, or other malware. Once this "update" is installed, the attacker then has control of the system and all of its data.

Methods of countering this threat typically involve hashes of the updates, and potentially cryptographic operations (e.g., digital signatures) on those hashes as well. However, the validity of these methods introduces additional threats. For instance, a weak hash function could result in the attacker being able to modify the legitimate update in such a way that the hash remained unchanged. For cryptographic signature schemes, there are dependencies on

1. the strength of the cryptographic algorithm used to provide the signature, and
2. the ability of the end user to verify the signature (which typically involves checking a hierarchy of digital signatures back to a root of trust (a certificate authority)).

If a cryptographic signature scheme is weak, then it may be compromised by an attacker and the end user will install a malicious update, thinking that it is legitimate. Similarly, if the root of trust can be compromised, then a strong digital signature algorithm will not stop the malicious update from being installed (the attacker will just create their own signature on the update using the compromised root of trust, and the malicious update will then be installed without detection).

3.2.3 Undetected System Activity (T.ADMIN_ERROR, T.UNDETECTED_ACTIONS, T.UNAUTHORIZED_ACCESS)

While several threats are directed at specific capabilities of the TOE, there is also the threat that activity that could indicate an impending or on-going security compromise could go undetected. Administrators can unintentionally perform actions on the TOE that compromise the security being provided by the TOE; for instance, a mis-configuration of security parameters. Processing performed in response to user data (for example, the establishment of a secure communications session, cryptographic processing associated with a protected session) may give indications of a failure or compromise of a TOE security mechanism (e.g., establishment of a session with an IT entity when no such sessions should be taking place). When indications of activity that may impact the security of the TOE are not generated and monitored, it is possible for harmful activity to take place on the TOE without responsible officials being aware and able to correct the problem. Further, if no data are kept or records generated, reconstruction of the TOE and the ability to understand the extent of any compromise could be negatively affected.

While this PP requires that the TOE generates the audit data, these data are not required to be stored on the TOE, but rather sent to a trusted external IT entity (e.g., a syslog server). These data may be read or altered by an intervening system, thus potentially masking indicators of suspicious activity. It may also be the case that the TOE could lose connectivity to the external IT entity, meaning that the audit information could not be sent to the repository.

3.2.4 Accessing the TOE (T.UNAUTHORIZED_ACCESS)

In addition to the threats discussed in Section 2.1 dealing with the TOE communicating with various external parties that focus on the communications themselves, there are also threats that arise from attempts to access the TOE, or the means by which these access attempts are accomplished. For example, if the TOE does not discriminate between administrative users that are allowed to access the TOE interactively (through a locally connected console, or with a session-oriented protocol such as SSH) and an administrative user with no authority to use the TOE in this manner, the configuration of the TOE cannot be trusted. Assuming that there is this distinction, there is still the threat that one of the allowed accounts may be compromised and used by an attacker that does not otherwise have access to the TOE.

One vector for such an attack is the use of poor passwords by authorized administrators of the TOE. Passwords that are too short, are easily-guessed dictionary words, or are not changed very often, are susceptible to a brute force attack. Additionally, if the password is plainly visible for a period of time (such as when a legitimate user is typing it in during logon) then it might be obtained by an observer and used to illegitimately access the system.

Once a legitimate administrative user is logged on, there still are a number of threats that need to be considered. During the password change process, if the TOE does not verify that it is the administrative user associated with the account changing the password, then anyone can change the password on a legitimate account and take that account over. If an administrative user walks away from a logged-in session, then another person with no access to the device could sit down and illegitimately start accessing the TOE.

3.2.5 User Data Disclosure (T.USER_DATA_REUSE)

While most of the threats contained in this PP deal with TSF and administrative data, there is also a threat against user data that all network devices should mitigate. Data traversing the TOE could inadvertently be sent to a different user; since these data may be sensitive, this may cause a compromise that is unacceptable. The specific threat that must be addressed concerns user data that is retained by the TOE in the course of processing network traffic that could be inadvertently re-used in sending network traffic to a user other than that intended by the sender of the original network traffic.

3.2.6 TSF Failure (T. TSF_FAILURE)

Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TSF.

3.3 Security Objectives for the TOE

The security objectives have been taken from [NDPP] and are reproduced here for the convenience of the reader.

3.3.1 Protected Communications (O.PROTECTED_COMMUNICATIONS)

To address the issues concerning transmitting sensitive data to and from the TOE described in Section 2.1, "Communications with the TOE", compliant TOEs will provide encryption for these communication paths between themselves and the endpoint. These channels are implemented using one (or more) of three standard protocols: IPsec, TLS/HTTPS, and SSH. These protocols are specified by RFCs that offer a variety of implementation choices. Requirements have been imposed on some of these choices (particularly those for cryptographic primitives) to provide interoperability and resistance to cryptographic attack. While compliant TOEs must support all of the choices specified in the ST, they may support additional algorithms and protocols. If such additional mechanisms are not evaluated, guidance must be given to the administrator to make clear the fact that they are not evaluated.

In addition to providing protection from disclosure (and detection of modification) for the communications, each of the protocols described in this document (IPsec, SSH, and TLS/HTTPS) offer two-way authentication of each endpoint in a cryptographically secure manner, meaning that even if there was a malicious attacker between the two endpoints, any attempt to represent themselves to either endpoint of the communications path as the other communicating party would be detected. The requirements on each protocol, in addition to the structure of the protocols themselves, provide protection against replay attacks such as those described in Section 2.1, usually by including a unique value in each communication so that replay of that communication can be detected.

(FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1, FPT_SKP_EXT.1, FTP_ITC.1, FTP_TRP.1, (FCS_IPSEC_EXT.1, FCS_SSH_EXT.1, FCS_TLS_EXT.1, FCS_HTTPS_EXT.1), (FPT_ITT.1(1), FPT_ITT.1(2)))

3.3.2 Verifiable Updates (O.VERIFIABLE_UPDATES)

As outlined in Section 2.2, "Malicious Updates", failure by the Security Administrator to verify that updates to the system can be trusted may lead to compromise of the entire system. A first step in establishing trust in the update is to publish a hash of the update that can be verified by the System Administrator prior to installing the update. In this way, the Security Administrator can download the update, compute the hash, and compare it to the published hash. While this establishes that the update downloaded is the one associated with the published hash, it does not indicate if the source of the update/hash combination has been compromised or can't be trusted. So, there remains a threat to the system. To establish trust in the source of the updates, the system can provide cryptographic mechanisms and procedures to procure the update, check the update cryptographically through the TOE-provided digital signature mechanism, and install the update on the system. While there is no requirement that this process be completely automated, administrative guidance documentation will detail any procedures that must be performed manually, as well as the manner in which the administrator ensures that the signature on the update is valid.

(FPT_TUD_EXT.1, FCS_COP.1(2), FCS_COP.1(3))

3.3.3 System Monitoring (O.SYSTEM_MONITORING)

In order to assure that information exists that allows Security Administrators to discover intentional and unintentional issues with the configuration and/or operation of the system as discussed in Section 2.3, "Undetected System Activity", compliant TOEs have the capability of generating audit data targeted at detecting such activity. Auditing of administrative activities provides information that may hasten corrective action should the system be configured incorrectly. Audit of select system events can provide an indication of failure of critical portions of the TOE (e.g., a cryptographic provider process not running) or anomalous activity (e.g., establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the system) of a suspicious nature.

In some instances there may be a large amount of audit information produced that could overwhelm the TOE or administrators in charge of reviewing the audit information. The TOE must be capable of sending audit information to an external trusted entity, which mitigates the possibility that the generated audit data will cause some kind of denial of service situation on the TOE. This information must carry reliable timestamps, which will help order the information when sent to the external device.

Loss of communication with the audit server is problematic. While there are several potential mitigations to this threat, this PP does not mandate that a specific action takes place; the degree to which this action preserves the audit information and still allows the TOE to meet its functionality responsibilities should drive decisions on the suitability of the TOE in a particular environment.

(FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1, FPT_STM.1)

3.3.4 TOE Administration (O.TOE_ADMINISTRATION)

In order to provide a trusted means for administrators to interact with the TOE, the TOE provides a password-based logon mechanism. The administrator must have the capability to compose a strong password, and have mechanisms in place so that the password must be changed regularly. To avoid attacks where an attacker might observe a password being typed by an administrator, passwords must be obscured during logon. Session locking or termination must also be implemented to mitigate the risk of an account being used illegitimately. Passwords must be stored in an obscured form, and there must be no interface provided for specifically reading the password or password file such that the passwords are displayed in plain text.

(FIA_UIA_EXT.1, FIA_PMG_EXT.1, FIA_UAU.7, FMT_MTD.1, FMT_SMF.1, FMT_SFR.1, FPT_APW_EXT.1, FTA_SSL_EXT.1, FTA_SSL.3)

3.3.5 Residual Information Clearing (O.RESIDUAL_INFORMATION_CLEARING)

In order to counter the threat that user data is inadvertently included in network traffic not intended by the original sender, the TSF ensures that network packets sent from the TOE do not include data "left over" from the processing of previous network information.

(FDP_RIP.2)

3.3.6 TSF Self-Test (O.TSF_SELF_TEST)

In order to detect some number of failures of underlying security mechanisms used by the TSF, the TSF will perform self-tests. The extent of this self-testing is left to the product developer, but a more comprehensive set of self-tests should result in a more trustworthy platform on which to develop enterprise architecture.

(FPT_TST_EXT.1)

3.3.7 O.DISPLAY_BANNER

The TOE will display an advisory warning regarding use of the TOE.

(FTA_TAB.1)

3.3.8 O.SESSION_LOCK

(The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.)

(FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4)

3.4 Security Objectives for the Operational Environment

The security objectives have been taken from [NDPP] and are reproduced here for the convenience of the reader.

3.4.1 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.

3.4.2 OE.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

3.4.3 OE.TRUSTED_ADMIN

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner

4 Security Requirements

This section identifies the Security Functional Requirements for the TOE and/or Platform. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated: September 2012 and all international interpretations.

4.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the PP itself, the formatting used in the PP has been retained.

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs. Formatting conventions outside of operations matches the formatting specified within the PP.

4.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear below in Table 11 are described in more detail in the following subsections.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_STG_EXT.1	None.	
FCS_CKM.1	None.	
FCS_CKM_EXT.4	None.	
FCS_COP.1(1)	None.	
FCS_COP.1(2)	None.	
FCS_COP.1(3)	None.	
FCS_COP.1(4)	None.	
FCS_TLS_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS session.	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_SSH_EXT.1	Failure to establish an SSH session Establishment/Termination of an SSH session	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session. Establishment/Termination of a HTTPS session.	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RBG_EXT.1	None.	
FDP_RIP.2	None.	
FIA_PMG_EXT.1	None.	

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UIA_EXT.1	All use of the authentication mechanism.	Provided user identity, origin of the attempt authentication mechanism. (e.g., IP address)
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FMT_MTD.1	None.	
FMT_SMF.1	None.	
FMT_SMR.2	None.	
FPT SKP EXT.1	None.	
FPT APW EXT.1	None.	
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT TUD EXT.1	Initiation of update.	No additional information.
FPT TST EXT.1	None.	
FPT_ITT.1	None.	
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_SSL.4	The termination of an interactive session.	No additional information.
FTA_TAB.1	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	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

Table 11 TOE Security Functional Requirements and Auditable Events

4.2.1 Class: Security Audit (FAU)

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 <u>not specified</u> level of audit; and
c) *All administrative actions;*
d) [Specifically defined auditable events listed in Table 1].

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 PP/ST, [information specified in column three of Table 1].

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.

FAU_STG_EXT.1 External Audit Trail 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 implementing the [TLS] protocol.

4.2.2 Class: Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation (For Asymmetric Keys)

FCS_CKM.1.1: **Refinement:** The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance with

- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;*
- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")*
- *NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes]*

and specified cryptographic key sizes *equivalent to, or greater than, a symmetric key strength of 112 bits.*

FCS_CKM_EXT.4 Cryptographic Key Zeroization

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

FCS_COP.1(1) Cryptographic Operation (for data encryption/decryption)

FCS_COP.1.1(1) **Refinement:** The TSF shall perform *[encryption and decryption]* in accordance with a specified cryptographic algorithm [AES *operating in* [CBC, GCM]] and cryptographic key sizes 128-bits and 256-bits that meets the following:

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- **[NIST SP 800-38D]**

FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1(2) **Refinement:** The TSF shall perform **cryptographic signature services** in accordance with a **[**

1. RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater, or
2. Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater]

that meets the following:

Case: RSA Digital Signature Algorithm

- **FIPS PUB 186-2 or FIPS PUB 186-3, "Digital Signature Standard"**

Case: Elliptic Curve Digital Signature Algorithm

- **FIPS PUB 186-3, “Digital Signature Standard”**
- **The TSF shall implement "NIST curves" P-256, P-384 and [P-521] (as defined in FIPS PUB 186-3, "Digital Signature Standard").**

FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)

FCS_COP.1.1(3) **Refinement**: The TSF shall perform *[cryptographic hashing services]* in accordance with a specified cryptographic algorithm **[SHA-1, SHA-224, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 224, 256, 384, 512] bits** that meet the following: *FIPS Pub 180-3, "Secure Hash Standard.*

FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1.1(4) **Refinement:** The TSF shall perform *[keyed-hash message authentication]* in accordance with a specified cryptographic algorithm HMAC**-[SHA-1, SHA-224, SHA-256, SHA-384, SHA-512], key size [*512 or 1024 bits*], and message digest sizes [160, 224, 256, 384, 512] bits** that meet the following: *FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard.*

FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using [CTR_DRBG (AES)] seeded by an entropy source that accumulated entropy from [a software-based noise source; a TSF-hardware-based noise source].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [256 bits] of entropy at least equal to the greatest security strength of the keys and authorization factors that it will generate.

FCS_TLS_EXT.1 Explicit: TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

Mandatory Ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites: [TLS_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_ SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384].

FCS_SSH_EXT.1 Explicit: SSH

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and [no other RFCs].

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

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [65,535 bytes] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [AEAD_AES_128_GCM, AEAD_AES_256_GCM].

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses [SSH_RSA] and [no other public key algorithms,] as its public key algorithm(s).

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [hmac-sha1, hmac-sha2-256, hmac-sha2-512].

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

FCS_HTTPS_EXT.1 Explicit: HTTPS

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 as specified in FCS_TLS_EXT.1.

4.2.3 Class: User Data Protection (FDP)

FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] all objects.

4.2.4 Class: Identification and Authentication (FIA)

FIA_PMG_EXT.1 Password Management

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

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: ["!", "@", "#", “$”, “%”, “ ”, “&”, “*”, “(“, ”)”];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall require the following actions prior to allowing 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

FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

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

FIA_UAU.7 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.

4.2.5 Class: Security Management (FMT)

FMT_MTD.1 Management of TSF Data (for general TSF data)

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

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 update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates*;
- *[<u>No other capabilities</u>]*

FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- **Authorized Administrator**

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

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

are satisfied.

4.2.6 Class: Protection of the TSF (FPT)

FPT_SKP_EXT.1 Extended: Protection of TSF Data (for reading of all symmetric keys)

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

FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

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

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

FPT_STM.1 Reliable Time Stamps

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

FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

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

FPT_TST_EXT.1: TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 **Refinement:** The TSF shall protect TSF data from *disclosure* ***and detect its modification*** when it is transmitted between separate parts of the TOE **through the use [SSH].**

4.2.7 Class: TOE Access (FTA)

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.

FTA_SSL.3 TSF-initiated Termination

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

FTA_SSL.4 User-initiated Termination

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

FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 **Refinement:** 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.

4.2.8 Class: Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall **use [TLS]** to provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [authentication server]** 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 and remote authentication*].

FTP_TRP.1 Trusted Path

FTP_TRP.1.1 **Refinement:** The TSF shall **use [SSH, TLS, HTTPS]** provide a **trusted** communication path between itself and **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 detection of modification of the communicated data.*

FTP_TRP.1.2 **Refinement:** The TSF shall permit **remote administrators** to initiate communication via the trusted path.

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

4.3 TOE SFR Dependencies Rationale for SFRs

The Protection Profile for Network Devices with Errata #3 contains all the requirements claimed in this Security Target. As such, the dependencies are not applicable since the PP has been approved.

4.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the Protection Profile for Network Devices with Errata #3 which are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Assurance Class	Components	Components Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing – Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis

Table 12 Security Assurance Requirements

4.5 Rationale for Security Assurance Requirements

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). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.

4.6 Assurance Measures

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

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),

SAR Component	How the SAR will be met
	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). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
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 ALC_CMS.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, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
ATE_IND.1	FireEye will provide the TOE for testing.
AVA_VAN.1	FireEye will provide the TOE for testing.

Table 13 TOE Security Assurance Measures

5 TOE Summary Specification

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

TOE SFR	Rationale
FAU_GEN.1	The TOE generates a comprehensive set of audit logs that identify specific TOE operations whenever an auditable event occurs. Auditable events include: failure on invoking cryptographic functionality such as establishment, termination and failure of a TLS session; establishment, termination and failure of an SSH session; modifications to the group of users that are part of the authorized administrator roles; all use of the user identification mechanism; any use of the authentication mechanism; any change in the configuration of the TOE, changes to time, initiation of TOE update, indication of completion of TSF self-test, maximum sessions being exceeded, termination of a remote session; and initiation and termination of a trusted channel. 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. The audit trail consist 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. Administrators are instructed to monitor the log buffer to view the audit records. The first message displayed is the oldest message in the buffer. The TOE can be configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using TLS and the TOE can determine when communication with the syslog server fails. The logs for all of the appliances can be viewed on the TOE via the CM GUI. Audit record generated on an LMS are sent to the CM for review via an SSH secured connection. The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to clear audit data stored locally on the TOE.
FAU_GEN.2	The TOE ensures that each auditable event is associated with the user that triggered the event. For example, a human user, 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	The TOE may 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 at the same time logs are written locally. If the TLS connection fails, the TOE will store audit records locally on the TOE, and will transmit any locally stored contents when connectivity to the syslog server is restored. Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.
FCS_CKM.1	In support of secure cryptographic protocols, the TOE supports several key generation schemes, including, • FFC Diffie-Hellman as specified in NIST SP 800-56A, • ECDH Diffie-Hellman as specified in NIST SP 800-56A,

TOE SFR	Rationale
	• RSA Key Transport as specified in SP NIST 800-56B. The TOE is fully compliant to both SP 800-56A and SP 800-56B.
FCS_CKM_EXT.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs). All keys within the TOE are zeroizable. See below for more information on how and when key zeroization takes place.
FCS_COP.1(1)	The TOE provides symmetric encryption and decryption capabilities using 128 and 256 bit AES in CBC mode and 128 and 256 bit AES in GCM mode as described in NIST SP 800-38A and NIST SP 800-38D. AES is implemented in the following protocols: TLS and SSH. The relevant FIPS certificate numbers are listed in Table 10, Section 1.5.2.2.
FCS_COP.1(2)	The TOE provides cryptographic signature services using • RSA Signature Algorithm with key size of 2048 and greater, • ECDSA Signature Algorithm with curve 384. The relevant FIPS certificate numbers include, RSA #1759, #1758 ECDSA #696.
FCS_COP.1(3)	The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 as specified in FIPS Pub 180-3 “Secure Hash Standard.” SHS is implemented in the following protocols: TLS and SSH. The relevant FIPS certificate numbers are listed in Table 10, Section 1.5.2.2.
FCS_COP.1(4)	The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 as specified in FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code,” and FIPS 180-3, “Secure Hash Standard.” HMAC is implemented in the following protocols: TLS and SSH. The relevant FIPS certificate numbers are listed in Section 1.5.2.2.
FCS_SSH_EXT.1	The TOE uses SSH for multiple purposes, including, communications between remote TOE components and remote administrative communications. The TOE's SSH implementation supports the following, • Compliance with RFCs 4251, 4252, 4253, and 4254; • Dropping SSH packets greater than 65,535 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; • Encryption algorithms AES-CBC-128, AES-CBC-256, AEAD_AES_128_GCM, and AEAD_AES_256_GCM to ensure confidentiality of the session; • Use of the SSH_RSA public key algorithms for authentication; • Password based authentication; • Hashing algorithm hmac-sha1, hmac-sha2-256, hmac-sha2-512 to ensure the integrity of the session; • Enforcement of DH Group 14 as the only allowed key exchange method.
FCS_TLS_EXT.1	In support of secure communication with external entities, the TOE supports the TLS protocol. TLS is used to facilitate communication with the following entities, • Remote administrators • Remote audit servers • Remote LDAP servers The TOE supports the following ciphersuites for communications with remote administrators: • TLS_RSA_WITH_AES_128_CBC_SHA

TOE SFR	Rationale
	• TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_ SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 The TOE supports the following ciphersuites for communications with remote audit and LDAP servers: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_ SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
FCS_HTTPS_EXT.1	The TOE provides management functionality over an HTTPS connection using the TLS implementation described above. The TOE's HTTPS protocol complies with RFC 2818.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90. The entropy source used to seed the Deterministic Random Bit Generator is a random set of bits or bytes that are regularly supplied to the DRBG by from a combined hardware/software source. All RNG entropy source samplings are continuously health tested by the NIST DRBG as per SP 900-90A before using them as a seed. The tests are part of the FIPS validation procedures for the DBRG and are part of the NIST validations for FIPS 140-2 for the products.
FDP_RIP.2	The TOE ensures that packets transmitted from the TOE do not contain residual information from previous packets. Packets that are not the required length are padded

<table>
<tr><th>TOE SFR</th><th>Rationale</th></tr>
<tr><td></td><td>with zeros. Residual data is never transmitted from the TOE. Once packet handling is complete, its content is overwritten before memory buffer which previously contained the packet is reused.</td></tr>
<tr><td>FIA_PMG_EXT.1</td><td>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. When the TOE is configured for "Common Criteria Compliance" the minimum password length is set to 15 characters.</td></tr>
<tr><td>FIA_UIA_EXT.1</td><td rowspan="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 the CMS appliance GUI via HTTPS/TLS
Regardless of the interface at which the administrator interacts, the TOE prompts the user for a user name and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated.

The TOE provides a local password based authentication mechanism as well as LDAP authentication, if configured.

The process for authentication is the same for administrative access whether administration is occurring via direct connection or 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 password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.</td></tr>
<tr><td>FIA_UAU_EXT.2</td></tr>
<tr><td>FIA_UAU.7</td><td>For all authentication, regardless of the interface, the TOE displays only "*" characters when the administrative password is entered so that the password is obscured.</td></tr>
<tr><td>FMT_MTD.1</td><td>The TOE provides the ability for the administrative user to manage the TOE including accessing TOE data, such as audit data, configuration data, security attributes, session thresholds and updates. The TOE supports several types of administrative user roles. Collectively this sub-roles comprise the Authorized 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</td></tr>
</table>

TOE SFR	Rationale
	trace how events occurred. Together these roles are collectively known as the “Authorized Administrator” Each of the predefined administrative sub-roles have a set of permissions that will grant them access to the TOE data, though with some sub-roles, the access is limited. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the privileged and semi-privileged levels. The term “Authorized Administrator” is used in this ST to refer to any user which has been assigned a sub-role that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The administrative user can connect to the TOE either via CLI or through the TOE GUI to perform these functions. However, the specific configurable parameters available through the TOE CLI is limited. All general administration is expected to take place through the TOE GUI. • The specific management capabilities available from the TOE include: • Local and remote administration of the TOE services and security characteristics; • The ability to update the TOE software (image integrity verification is provided using RSA 2048-bit SHA-256 digital signature); • Ability to configure the TLS and SSH functionality; • Ability to enable, disable, determine and modify the behavior of all the security functions of the TOE via the GUI.
FMT_SMR.2	The TOE maintains Authorized Administrators that are comprised of the sub-roles described above in the FMT_MTD.1 row of this table. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to each of the sub-roles supported by the TOE. The term “Authorized Administrator” is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. The assigned sub-role determines the functions the user can perform; hence the Authorized Administrator with the appropriate privileges. The TOE authenticates all access to the administrative interfaces using a username and password. The TOE supports both local administration and remote authentication.
FPT SKP EXT.1 FPT APW EXT.1	The TOE stores all private keys in a secure directory that is not readily accessible to administrators; hence no interface access. 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_STM.1	The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the system clock provided by the underlying hardware. The TOE can optionally be set to receive clock updates from an NTP server. 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.
FPT TUD EXT.1	Authorized Administrator can query the software version running on the TOE, and can initiate updates to software images. When software updates are made available by FireEye an administrator can obtain, verify the integrity of, and install those updates. Software updates are downloaded to the TOE via an image fetch command. However, the software

TOE SFR	Rationale
	image will never be installed without explicit administrative intervention. The TOE image files are digitally signed so their integrity can be verified during the upgrade process, and an image that fails an integrity check will not be loaded.
FPT TST EXT.1	As a FIPS 140-2 validated product, 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 Power on Startup Test (POST) components for all the cryptographic modules perform the POST. Refer to the FIPS Security Policy for available options and management of the cryptographic self-test. The Software Integrity Test is run automatically whenever the system images are loaded and confirms through use of a hash verification that the image file to be loaded hash not been corrupted and has maintained its integrity.
FPT_ITT.1	The TOE supports the inter-TOE communications, as follows. The CMS appliances act as the main configuration point for the TOE. All TOE configuration takes place through the CMS GUI, CLI/SSHv2, or WebUI/TLS. The CMS communicates with each of the other TOE appliances via SSHv2. In response all TOE appliances send audit data to be reviewed to the CMS. The audit records are stored and reviewable from the CMS GUI. This is also over an SSHv2 channel. There are no other inter-TOE communications.
FTA_SSL_EXT.1 FTA_SSL.3	An Authorized Administrator can configure maximum inactivity times administrative sessions through the TOE GUI interface. The configuration of inactivity periods are applied on a per interface basis. A configured inactivity period will be applied to both local and remote sessions in the same manner. The session will be terminated and will require authentication to establish a new session.
FTA_SSL.4	An Authorized Administrator is able to exit out of both local and remote administrative sessions.
FTA_TAB.1	Authorized administrators can define a custom login banner that will be displayed at the following interfaces, • Local CLI • Remote CLI • Remote GUI This banner will be displayed prior to allowing Authorized Administrator access through those interfaces.
FTP_ITC.1	The TOE supports communications with several types of authorized IT entities, including, • Audit Servers • LDAP Servers Each of these connections are protected via a TLS connection. This protects the data from disclosure by encryption and by MACs that verify that data has not been modified.
FTP_TRP.1	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. Remote GUI connections take place over a TLS connection. The TLS session is encrypted using AES encryption. The remote administrators are able to initiate both SSHv2 and TLS communications with the TOE.

Table 14 TOE Summary Specification SFR Description

5.1 Key Zeroization

The following table describes the key zeroization referenced by FCS_CKM_EXT.4 provided by the TOE.

Keys	Type	Zeroization Description
Diffie Hellman private key	DH Key	Keys are overwritten with zeros at power cycle.
Diffie Hellman public key	DH Key	Keys are overwritten with zeros at power cycle.
SSH Private Key	RSA Private Key	Key is overwritten by zeros when the compliance declassify zeroize command is issued.
SSH Public Key	RSA Public Key	Key is overwritten by zeros when the compliance declassify zeroize command is issued.
SSH Session Key	AES Key	Keys are overwritten with zeros at power cycle.
TLS Private Key	RSA Private Key	Key is overwritten by zeros when the compliance declassify zeroize command is issued.
TLS Public Key	RSA Public Key	Key is overwritten by zeros when the compliance declassify zeroize command is issued.
TLS Session Encryption Key	AES Key	Keys are overwritten with zeros at power cycle.
TLS Session Integrity Key	HMAC Key	Keys are overwritten with zeros at power cycle.

Table 15 Key Zeroization

Annex A: References

The following documentation was used to prepare this ST:

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004
[NDPP]	Protection Profile for Network Devices, version 1.1, June 8, 2012
[ERRATA#3]	Security Requirements for Network Devices Errata #2, 3 November 2014
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 186-2]	FIPS PUB 186-2 Federal Information Processing Standards Publication 2000 January 27
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008

Table 16: References