McAfee Inc. McAfee Advanced Threat Defense (NDPP11e3) Security Target

Version 0.5
2015/05/22

Prepared for:

McAfee Inc.

2821 Mission College Blvd.
Santa Clara, CA 95054

Prepared By:

Gossamer
Laboratories

www.gossamersec.com

1. SECURITY TARGET INTRODUCTION 3

1.1 SECURITY TARGET REFERENCE 3
1.2 TOE REFERENCE 4
1.3 TOE OVERVIEW 4
1.4 TOE DESCRIPTION 4
1.4.1 TOE Architecture 4
1.4.2 TOE Documentation 6

2. CONFORMANCE CLAIMS 7

2.1 CONFORMANCE RATIONALE 7

3. SECURITY OBJECTIVES 8

3.1 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 8

4. EXTENDED COMPONENTS DEFINITION 9

5. SECURITY REQUIREMENTS 10

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 10
5.1.1 Security audit (FAU) 11
5.1.2 Cryptographic support (FCS) 11
5.1.3 User data protection (FDP) 13
5.1.4 Identification and authentication (FIA) 13
5.1.5 Security management (FMT) 14
5.1.6 Protection of the TSF (FPT) 14
5.1.7 TOE access (FTA) 15
5.1.8 Trusted path/channels (FTP) 15
5.2 TOE SECURITY ASSURANCE REQUIREMENTS 16
5.2.1 Development (ADV) 16
5.2.2 Guidance documents (AGD) 17
5.2.3 Life-cycle support (ALC) 18
5.2.4 Tests (ATE) 18
5.2.5 Vulnerability assessment (AVA) 18

6. TOE SUMMARY SPECIFICATION 20

6.1 SECURITY AUDIT 20
6.2 CRYPTOGRAPHIC SUPPORT 21
6.3 USER DATA PROTECTION 23
6.4 IDENTIFICATION AND AUTHENTICATION 24
6.5 SECURITY MANAGEMENT 24
6.6 PROTECTION OF THE TSF 24
6.7 TOE ACCESS 25
6.8 TRUSTED PATH/CHANNELS 25

LIST OF TABLES

Table 1 TOE Security Functional Components 11
Table 2 EAL 1 Assurance Components 16
Table 3 Auditable Events 21
Table 4 Cryptographic Functions 22
Table 5 NIST SP800-56B Conformance 23

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is McAfee Advanced Threat Defense provided by McAfee Inc.. The TOE is being evaluated as a network infrastructure device.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- The NDPP uses an additional convention – the 'case' – which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST and they are identified using **bold** text.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – McAfee Inc. McAfee Advanced Threat Defense (NDPP11e3) Security Target

ST Version – Version 0.5

ST Date – 2015/05/22

1.2 TOE Reference

TOE Identification – McAfee Inc. McAfee Advanced Threat Defense models 3000 and 6000 running software version 3.4.6

TOE Developer – McAfee Inc.

Evaluation Sponsor – McAfee Inc.

1.3 TOE Overview

The Target of Evaluation (TOE) is McAfee Advanced Threat Defense (MATD). MATD detects today's stealthy, zero-day malware with layered approach. It combines low-touch antivirus signatures, reputation, and real-time emulation defenses with in-depth static code and dynamic analysis (sandboxing) to analyze actual behavior.

1.4 TOE Description

The MATD hardware appliance implements dynamic and statistical analysis on data transmitted through a network to provide malware detection, assessment and classification.

The MATD processes the files through the down selectors for statistical analysis and provides a sandbox test environment which includes virtual machines running customer environments, anti-virus, anti-malware, local blacklist and whitelists. Files are executed within virtual machine environments that are monitored by the log file. The log file is then used to generate a security report of the potential malware.

For the purpose of evaluation, MATD will be treated as a network device offering FIPS certified cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to transmit audit records).

1.4.1 TOE Architecture

MATD is provided as a hardware network appliance. The product provides a web interface over TLS and a console connection.

There are two versions of the MATD product (6000 and 3000). While there are different models in the TOE, they differ primarily in physical form factor, number and types of connections and slots, and relative performance. There are some functional differences among the models, but they each provide the same security characteristics as claimed in this security target.

1.4.1.1 Physical Boundaries

The ATD evaluated configuration includes software version 3.4.6 running on one of the following modules:

- ATD-6000: McAfee Advanced Threat Defense 6000, 2U 4x Xeon E5-4640 (2.5GHz), 256GB DDR3, 16TB of HDD storage and 1600MB of SSD storage.
- ATD-3000: McAfee Advanced Treat Defense 3000, 1U 2x Xeon E5-2658 (2.1GHz), 192GB DDR3, 8TB of HDD storage and 800MB of SSD storage.

Since each platform uses the same software and the TOE implements all provided security functions in software, the TOE security behavior remains equivalent on each platform for each of the SFRs defined by the NDPP11e3. These SFRs are instantiated by the same version of the TOE software and in the same way on both platforms. Both platforms have Intel Xeon 64-bit CPUs. Both platforms utilize Linux 3.10.45 and OpenSSL FIPS Object Module 2.0.5, hence the identical software (version 3.4.6) operates on both platforms. The differences simply relate to performance – number of CPUs and amount of memory and HD/SSD storage

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external syslog server in the network environment. This is generally advisable given the limited audit log storage space on the evaluated appliances.

The TOE can be configured to synchronize its internal clock using an external NTP server in the operational environment.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by MATD:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

1.4.1.2.1 Security audit

The TOE generates audit events associated with identification and authentication, management, updates, and user sessions. The TOE can store the events in a local log or export them to a syslog server using a TLS protected channel.

1.4.1.2.2 Cryptographic support

The TOE provides CAVP certified cryptography in support of its TLS implementation. Cryptographic services include key management, random bit generation, encryption/decryption, digital signature and secure hashing.

1.4.1.2.3 User data protection

The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets.

1.4.1.2.4 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of reading the login banner. It provides the ability to both assign attributes (user names, passwords and roles) and to authenticate users against these attributes.

1.4.1.2.5 Security management

The TOE provides a command line (CLI) management interface as well as a graphical user interface (GUI) accessed via the web. The web interface is protected with TLS. The management interface is limited to the authorized administrator (as defined by a role).

1.4.1.2.6 Protection of the TSF

The TOE provides a variety of means of protecting itself. The TOE performs self-tests that cover the correct operation of the TOE. It provides functions necessary to securely update the TOE. It provides a hardware clock to ensure reliable timestamps. It protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an authorized administrator.

1.4.1.2.7 TOE access

The TOE can be configured to display a logon banner before a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions.

1.4.1.2.8 Trusted path/channels

The TOE provides a local console which is subject to physical protection. For remote access, the web GUI is protected by TLS thus ensuring protection against modification and disclosure.

The TOE also protects its audit records from modification and disclosure by using TLS to communicate with the syslog server.

1.4.2 TOE Documentation

McAfee offers a series of documents that describe the installation of the MATD as well as guidance for subsequent use and administration of the applicable security features. The following list of documents was examined as part of the evaluation:

- NDPP Admin Guide, v 0.3, 4/27/15
- ATD 3.4.6 Product Guide, Revision A

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
    - Part 3 Conformant
- Protection Profile for Network Devices, Version 1.1 (with Errata #3), 8 June 2012 (NDPP11e3)
- Package Claims:
    - Assurance Level: EAL 1 conformant

2.1 Conformance Rationale

The ST conforms to the NDPP11e3. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the NDPP11e3 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDPP11e3 offers additional information about the identified security objectives, but that has not been reproduced here and the NDPP11e3 should be consulted if there is interest in that material.

In general, the NDPP11e3 has defined Security Objectives appropriate for network infrastructure device and as such are applicable to the McAfee Advanced Threat Defense TOE.

3.1 Security Objectives for the Operational 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.

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

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

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDPP11e3. The NDPP11e3 defines the following extended requirements and since they are not redefined in this ST the NDPP11e3 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- FAU_STG_EXT.1: External Audit Trail Storage
- FCS_CKM_EXT.4: Cryptographic Key Zeroization
- FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
- FCS_TLS_EXT.1: Explicit: TLS
- FIA_PMG_EXT.1: Password Management
- FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
- FIA_UIA_EXT.1: User Identification and Authentication
- FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
- FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
- FPT_TST_EXT.1: TSF Testing
- FPT_TUD_EXT.1: Extended: Trusted Update
- FTA_SSL_EXT.1: TSF-initiated Session Locking

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the NDPP11e3. The refinements and operations already performed in the NDPP11e3 are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDPP11e3 and any residual operations have been completed herein. Of particular note, the NDPP11e3 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the NDPP11e3 which includes all the SARs for EAL 1. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the NDPP11e3 that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the EAL 1 assurance requirements alone. The NDPP11e3 should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by McAfee Advanced Threat Defense TOE.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User Identity Association
	FAU_STG_EXT.1: External Audit Trail Storage
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication)
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
	FCS_TLS_EXT.1: Explicit: TLS
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UAU_EXT.2: Extended: Password-based Authentication Mechanism
	FIA_UIA_EXT.1: User Identification and Authentication
FMT: Security management	FMT_MTD.1: Management of TSF Data (for general TSF data)
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords
	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_STM.1: Reliable Time Stamps
	FPT_TST_EXT.1: TSF Testing

	FPT_TUD_EXT.1: Extended: Trusted Update
FTA: TOE access	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 Banners
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF trusted channel
	FTP_TRP.1: Trusted Path

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (FAU_GEN.1)

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;
d) Specifically defined auditable events listed in Table 1 (in the NDPP).

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 (in the NDPP).

5.1.1.2 User Identity Association (FAU_GEN.2)

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.

5.1.1.3 External Audit Trail Storage (FAU_STG_EXT.1)

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.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1)

FCS_CKM.1.1

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

- ***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.

.

5.1.2.2 Cryptographic Key Zeroization (FCS_CKM_EXT.4)

FCS_CKM_EXT.4.1

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

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

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 800-38A, NIST SP 800-38D***]

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

FCS_COP.1(2).1

Refinement: The TSF shall perform cryptographic signature services in accordance with a ***(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater***] that meets the following:
[***RSA Digital Signature Algorithm - FIPS PUB 186-2, 'Digital Signature Standard'***].

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

FCS_COP.1(3).1

Refinement: 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: FIPS Pub 180-3, 'Secure Hash Standard.'

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

FCS_COP.1(4).1

Refinement: The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[***SHA-1***], key size [**equal to the input block size**], and message digest sizes [***160***] bits that meet the following: FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code', and FIPS Pub 180-3, 'Secure Hash Standard.'

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

FCS_RBG_EXT.1.1

The TSF shall perform all random bit generation (RBG) services in accordance with [***NIST Special Publication 800-90 using [CTR_DRBG (AES-256)]***] seeded by an entropy source that accumulated entropy from [***a software-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 hashes that it will generate.

5.1.2.8 Explicit: TLS (FCS_TLS_EXT.1)

FCS_TLS_EXT.1.1

The TSF shall implement one or more of the following protocols [***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_RSA_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_RSA_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_RSA_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_RSA_256_GCM_SHA384].

5.1.3 User data protection (FDP)

5.1.3.1 Full Residual Information Protection (FDP_RIP.2)

FDP_RIP.2.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] all objects.

5.1.4 Identification and authentication (FIA)

5.1.4.1 Password Management (FIA_PMG_EXT.1)

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 special characters: [***!, @, #, $, %, ^, &, *, (,)***];
2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater.

5.1.4.2 Protected Authentication Feedback (FIA_UAU.7)

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.

5.1.4.3 Extended: Password-based Authentication Mechanism (FIA_UAU_EXT.2)

FIA_UAU_EXT.2.1

The TSF shall provide a local password-based authentication mechanism, [***none***] to perform administrative user authentication.

5.1.4.4 User Identification and Authentication (FIA_UIA_EXT.1)

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.

5.1.5 Security management (FMT)

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

FMT_MTD.1.1

The TSF shall restrict the ability to manage the TSF data to the Security Administrators.

5.1.5.2 Specification of Management Functions (FMT_SMF.1)

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;
- [***- Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1,***
- Ability to configure the cryptographic functionality].

5.1.5.3 Restrictions on Security Roles (FMT_SMR.2)

FMT_SMR.2.1

The TSF shall maintain the roles: Authorized 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
- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;
are satisfied

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Extended: Protection of Administrator Passwords (FPT_APW_EXT.1)

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.

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

FPT_SKP_EXT.1.1

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

5.1.6.3 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1

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

5.1.6.4 TSF Testing (FPT_TST_EXT.1)

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.

5.1.6.5 Extended: Trusted Update (FPT_TUD_EXT.1)

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.

5.1.7 TOE access (FTA)

5.1.7.1 TSF-initiated Termination (FTA_SSL.3)

FTA_SSL.3.1

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

5.1.7.2 User-initiated Termination (FTA_SSL.4)

FTA_SSL.4.1

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

5.1.7.3 TSF-initiated Session Locking (FTA_SSL_EXT.1)

FTA_SSL_EXT.1.1

The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.1.7.4 Default TOE Access Banners (FTA_TAB.1)

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.

5.1.8 Trusted path/channels (FTP)

5.1.8.1 Inter-TSF trusted channel (FTP_ITC.1)

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, [***no other servers]***] 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 [**transmitting audit records to an audit server**].

5.1.8.2 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1

Refinement: The TSF shall use [***TLS***] 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.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the EAL 1 components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM coverage
ATE: Tests	ATE_IND.1: Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability survey

Table 2 EAL 1 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic functional specification (ADV_FSP.1)

ADV_FSP.1.1d

The developer shall provide a functional specification.

ADV_FSP.1.2d

The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4c

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d

The developer shall provide operational user guidance.

AGD_OPE.1.1c

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6c

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d

The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1c

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d

The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c

The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM coverage (ALC_CMS.1)

ALC_CMS.1.1d

The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c

The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent testing - conformance (ATE_IND.1)

ATE_IND.1.1d

The developer shall provide the TOE for testing.

ATE_IND.1.1c

The TOE shall be suitable for testing.

ATE_IND.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability survey (AVA_VAN.1)

AVA_VAN.1.1d

The developer shall provide the TOE for testing.

AVA_VAN.1.1c

The TOE shall be suitable for testing.

AVA_VAN.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

The TOE generates audit events (see Table 3 Auditable Events) and has the capability to store them internally or export them to an audit log server. The TOE stores its internal audit events in a log that is protected so that only the authorized administrator can read the audit events.

The internal audit log can store at least 400k audit records before it begins overwriting audit events. The authorized administrator is instructed to export audit events to a syslog server. The TOE can be configured to use TLS to protect audit logs exported to the external server.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	Start-up of the audit functions. All use of management functions	
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_RBG_EXT.1	None.	
FCS_TLS_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS session. [1]	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_RIP.2	None.	
FIA_PMG_EXT.1	None.	
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (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.	

Requirement	Auditable Events	Additional Audit Record Contents
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.	
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 3 Auditable Events

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE can generate all the required auditable events as specified in Table 3 Auditable Events. Within each audit event is date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in Table 3 Auditable Events**.**
- FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or network entity (identified by IP address) that caused the event.
- FAU_STG_EXT.1: The TOE can be configured to export audit records to an external syslog server. This communication is protected using TLS.

6.2 Cryptographic support

The TOE includes a FIPS 140 certified crypto module (OpenSSL FIPS Object Module 2.0.5 running on Linux 3.10.45 on Intel x86_64 HW) providing supporting cryptographic functions. The following functions have been FIPS certified in accordance with the identified standards.

Functions	Standards	Certificates
Encryption/Decryption		
• AES ECB and CBC (128 or 256 bits)	FIPS PUB 197 NIST SP 800-38A	3364
Cryptographic signature services		
• Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS PUB 186-4	667
• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FIPS PUB 186-4	1728
Cryptographic hashing		
• SHA-1, SHA-256, SHA-384, and SHA-512 (digest sizes 160, 256, 384, and 512 bits)	FIPS Pub 180-4	2789
Keyed-exchange		

• ECCDH	NIST SP 800-56A	499
Keyed-hash message authentication		
• HMAC-SHA-1(digest size 160)	FIPS Pub 198-1 FIPS Pub 180-4	2144
Random bit generation		
• AES-256 CTR_DRBG with software based noise sources with a minimum of 256 bits of non-determinism	NIST SP 800-90A	792

Table 4 Cryptographic Functions

The TOE generally fulfills all of the NIST SP 800-56B requirements without extensions, the following table specifically identifies the “should”, “should not”, and “shall not” conditions from the publication along with an indication of how the TOE conforms to those conditions.

NIST SP800-56B Section Reference	“should”, “should not”, or “shall not”	Implemented?	Rationale for deviation
5.6	Should	Yes	Not applicable
5.8	shall not	No	Not applicable
5.9	shall not (first occurrence)	No	Not applicable
5.9	shall not (second occurrence)	No	Not applicable
6.1	should not	No	Not applicable
6.1	should (first occurrence)	Yes	Not applicable
6.1	should (second occurrence)	Yes	Not applicable
6.1	should (third occurrence)	Yes	Not applicable
6.1	should (fourth occurrence)	Yes	Not applicable
6.1	shall not (first occurrence)	No	Not applicable
6.1	shall not (second occurrence)	No	Not applicable
6.2.3	Should	Yes	Not applicable
6.5.1	Should	Yes	Not applicable
6.5.2	Should	Yes	Not applicable
6.5.2.1	Should	Yes	Not applicable
6.6	shall not	No	Not applicable
7.1.2	Should	Yes	Not applicable
7.2.1.3	Should	Yes	Not applicable
7.2.1.3	should not	No	Not applicable
7.2.2.3	should (first occurrence)	Yes	Not applicable
7.2.2.3	should (second occurrence)	Yes	Not applicable
7.2.2.3	should (third occurrence)	Yes	Not applicable
7.2.2.3	should (fourth occurrence)	Yes	Not applicable
7.2.2.3	should not	No	Not applicable
7.2.2.3	shall not	No	Not applicable
7.2.3.3	should (first occurrence)	Yes	Not applicable
7.2.3.3	should (second occurrence)	Yes	Not applicable
7.2.3.3	should (third occurrence)	Yes	Not applicable
7.2.3.3	should (fourth occurrence)	Yes	Not applicable
7.2.3.3	should (fifth occurrence)	Yes	Not applicable

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented?	Rationale for deviation
7.2.3.3	should not	No	Not applicable
8	Should	Yes	Not applicable
8.3.2	should not	No	Not applicable

Table 5 NIST SP800-56B Conformance

The product uses an SP 800-90A AES-256 CTR_DRBG.

The TOE provides TLS v1.1, and 1.2 for use by the web GUI and for protecting communications between the TOE and audit server. The TOE supports the ciphers enumerated in section 5.1.2.8

The following table presents the crypto security parameters (CSPs), secret keys, and private keys provided by the TOE. The table also identifies when each CSP or key is cleared.

CSP or Key:	Stored in	Zeroized upon:	Zeroized by:
TLS host RSA private key	On Disk	Command	Overwriting with zeros
TLS host RSA digital certificate	On Disk	Command	Overwriting with zeros
TLS pre-master secret	In Memory	Handshake done	Overwriting with pseudo random data
TLS session key	In Memory	Close of session	Overwriting with pseudo random data
Password hash	On Disk	Command	Overwriting once with zeros

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1: See the 800-56B conformance table.
- FCS_CKM_EXT.4: See the table explaining how keys are zeroized.
- FCS_COP.1(1): See **Table 4 Cryptographic Functions** above
- FCS_COP.1(2): See **Table 4 Cryptographic Functions** above
- FCS_COP.1(3): See **Table 4 Cryptographic Functions** above
- FCS_COP.1(4): See **Table 4 Cryptographic Functions** above
- FCS_RBG_EXT.1: The product uses an SP 800-90A AES-256 CTR_DRBG.
- FCS_TLS_EXT.1: The TOE supports TLS v1.1,and v1.2 with the ciphersuites listed above for the web management interface. For the syslog connection, the TOE supports the following ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA.

6.3 User data protection

The TOE has been designed to ensure that no residual information exists in network packets. When the TOE allocates a new buffer for either an incoming or outgoing a network packet, the new packet data will be used to overwrite any previous data in the buffer. If an allocated buffer exceeds the size of the packet, and additional space will be overwritten (padded) with zeros before the packet is forwarded (to the external network or delivered to the appropriate, internal application).

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_RIP.2: The TOE ensures that previous information contents of resources used for new objects are not discernible in any new object, such as network packets, as described above.

6.4 Identification and authentication

The TOE provides a password mechanism for authenticating users. Users are associated with a username, password, and one or more roles. Users may authenticate locally or via the web interface. Passwords can be composed of any alphabetic, numeric, and a wide range of special characters (identified in FIA_PMG_EXT.1). Passwords are not echoed back when users logon to the TOE.

The TOE requires identification and authentication before allowing access. Only the banner may be presented before authentication is complete.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_PMG_EXT.1: The TOE offers a wide range of characters for passwords as described above.
- FIA_UAU.7: The TOE does not echo passwords as they are entered.
- FIA_UAU_EXT.2: The TOE provides a password mechanism.
- FIA_UIA_EXT.1: The only service offered by the TOE before authentication is complete si the displaying of the logon banner.

6.5 Security management

The TOE provides an administrator role. User accounts that are associated with the administrator role are considered authorized administrators. Authorized Administrator can access audit configuration data, user and administrator security attributes (including [re]setting passwords, but not viewing an existing password), warning banner configuration, and cryptographic support settings.

The TOE offers two administrative interfaces – command line and GIU. The TOE offers command line functions which are accessible via the CLI. The CLI is a text based interface which can be accessed from a directly connected terminal. These command line functions can be used to effectively manage every security policy, as well as the non-security relevant aspects of the TOE.

The TOE also offers a web interface for management. The web interface offers access to the same functions as the CLI. The web interface is available using TLS v1.2.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MTD.1: The TOE restricts the access to manage TSF data that can affect the security functions of the TOE to Authorized Administrator.
- FMT_SMF.1: The TOE includes the functions necessary to manage the cryptomodule and associated functions, configure the warning banner, manage user accounts, and to manage and verify updates of the TOE software and firmware.
- FMT_SMR.2: The TOE includes an administrator account that corresponds to the required ‘Authorized Administrator’ also referred to as ‘Security Administrator’ in some requirements

6.6 Protection of the TSF

The TOE is an appliance and is designed to not offer general purpose operating system interfaces to users. The TOE is designed to not provide access to locally stored passwords (which are protected using SHA512 hashing) and also, while cryptographic keys can be entered, the TOE does not disclose any cryptographic keys stored in the TOE.

The TOE is a hardware appliance that includes a real-time clock. The TOE can be configured to synchronize its clock with a time server. The TOE uses the clock to support several security functions including timestamps for audit records, timing elements of cryptographic functions, and inactivity timeouts.

The TOE contains the OpenSSL FIPS validated module. The FIPS module performs Cryptographic algorithm known answer tests, firmware integrity tests using RSA signature verification and conditional self-tests for CTR-DRBG, Pair-wise consistency tests on generation of RSA keys, and a Firmware load test (RSA signature verification). Upon failing any of its FIPS mode power-on self-tests, the TOE's service dependent upon the failure cryptographic library will abort.

The TOE supports loading updates by the administrator using CLI commands. The administrator obtains the update, and the TOE automatically verifies its digital signature. An unverified update cannot be installed.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_APW_EXT.1: The TOE does not offer any interfaces that will disclose a plaintext password to any user. Additionally, passwords are not stored in plaintext on the TOE.
- FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose a stored cryptographic key to any users.
- FPT_STM.1: The TOE provides a hardware clock and can synchronize with an NTP Server.
- FPT_TST_EXT.1: The TOE performs a suite of self-tests to verify its integrity.
- FPT_TUD_EXT.1: The TOE provides a means for obtaining an installing digitally signed updates.

6.7 TOE access

The TOE provides an inactivity timeout for console and web sessions. The authorized administrator can set the inactivity timeout. When an inactivity period is exceeded, the session is terminated. The user will be required to login in after any session has been terminated due to inactivity or after voluntary termination.

The TOE also provides the ability to set a login banner. The banner is displayed before a user session is established. The banner will be displayed when accessing the TOE via the console or TLS interfaces.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- FTA_SSL.4: The TOE allows a user to logout (or terminate) both local and remote sessions.
- FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.
- FTA_TAB.1: The TOE can be configured to display a login banner when administrators successfully establish interactive sessions with the TOE, allowing users to terminate their session prior to performing any functions.

6.8 Trusted path/channels

The TOE uses TLS to protect communications between itself and the audit server. TLS is also used to protect the communication path for remote administrators. In both cases, TLS ensures traffic is not modified or disclosed.

The Trusted path/channels function is designed to satisfy the following security functional requirements:

- FTP_ITC.1: In the evaluated configuration, the TOE must be configured to use TLS to ensure that any authentication operations and exported audit records are sent only to the configured server so they are not subject to inappropriate disclosure or modification.
- FTP_TRP.1: The TOE provides TLS based on its cryptomodule to ensure secure remote administration. The administrator can initiate the remote session, the remote session is secured (disclosure and modification) using FIPS certified cryptographic operations, and all remote security management functions require the use of one of these secure channels.