Extreme Networks, Inc.VDX Product Series operating with NOS version 7.3.0aa (NDcPP20E) Security Target

Version 0.5
1/4/2019

Prepared for:

Extreme Networks, Inc.

6480 Via Del Oro, San Jose, CA 95119

Prepared By:

Gossamer Laboratories

www.gossamersec.com

LIST OF TABLES

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 VDX Product Series operating with NOS version 7.3.0aa provided by Extreme Networks, Inc. The TOE is being evaluated as a network 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 parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
  - 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 …").
- 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 – Extreme Networks, Inc. VDX Product Series operating with NOS version 7.3.0aa (NDcPP20E) Security Target

ST Version – Version 0.5

ST Date – 1/4/2019

1.2 TOE Reference

TOE Identification – Extreme Networks, Inc. VDX Product Series operating with NOS version 7.3.0aa including the following series and models:

- VDX 6740
- VDX 6740-T
- VDX 6740T-1G
- VDX 6940-36Q
- VDX 6940-144S
- VDX 8770-4 w/ 8770-MM-1 management module
- VDX 8770-8 w/ 8770-MM-1 management module

TOE Developer – Extreme Networks, Inc.

Evaluation Sponsor – Extreme Networks, Inc.

1.3 TOE Overview

The Target of Evaluation (TOE) is VDX Product Series operating with NOS version 7.3.0aa. VDX switches, featuring embedded automation capabilities of Extreme data center fabrics, deliver high performance, capacity, and reliability in data center spine and leaf deployments.

1.4 TOE Description

The Target of Evaluation (TOE) is the VDX Product Series operating with NOS version 7.3.0aa. The VDX Product Series operating with NOS version 7.3.0aa are hardware appliance with embedded software installed on a management processor. Optionally, a number of co-located appliances can be connected in order to work as a unit with a common security policy. The embedded software is a version of Extreme Network's proprietary Multiservice Network Operating System (NOS). The NOS controls the switching and routing of network frames and packets among the connections available on the hardware appliances. These switch/routers include virtual cluster switch (VCS), which allows users to create flatter, virtualized and converged data center networks. These VCS fabrics are scalable, permitting users to expand at their own pace, and simplified, allowing users to manage the fabric as a single entity. VCS-based Ethernet fabrics are convergence-capable.

All TOE appliances are configured at the factory with default parameters and an admin and user account with default passwords. Users must login to access the system's basic features through its Command Line Interface (CLI). However, the product should be configured in accordance with the evaluated configuration prior to being placed into operation. The CLI is a text based interface which is accessible from a directly connected terminal or via a remote terminal using SSH. Administrator can also use REST APIs (over HTTPS) or NetConf (over SSH) for configuring the TOE. The TOE uses SCP to download/compare software images. All of the remote management interfaces are protected using encryption as explained later in this ST.

Model	CPU
VDX- 6740, 6740-T, 6740T-1G, VDX-6940-36Q	Freescale P3041 four e500mc core processors at 1.5 Ghz
VDX6940-144S, VDX8770-4 and VDX8770-8 (including 8770-MM-1)	Freescale P4080 four e500mc core processors at 1.5 Ghz

The VDX 6740 switch is a fixed port switch with 48 10-Gigabit Ethernet (GbE) SFP+ interfaces and four 40 GbE independent 10 GbE SFP+ ports, providing an additional 16 10 GbE SFP+ ports. The Extreme Networks VDX 6740T offers 48 10 GbE 10BASE-T ports and four 40 GbE QSFP+ ports. Each can be broken out into four independent 10 GbE SFP+ ports, providing an additional 16 10 GbE SFP+ ports. The Extreme Networks VDX

6740T-1G offers 48 1000BASE-T ports and two 40 GbE QSFP+ ports. Each 40 GbE port can be broken out into four independent 10 GbE SFP+ ports, providing an additional eight 10 GbE SFP+ ports for uplink.

The VDX 6940-36Q base system has thirty-six 40 Gigabit Ethernet (GbE) QSFP+ ports enabled, or 36 ports can be configured as 144 10Gbe QSFP+ ports in breakout mode.

The VDX 6940-144S base system has Ninety six (96) 10 Gbe SFP+ ports and eight (8) 40Gbe QSFP + Ports enabled and Four (4) 100Gbe/40Gbe QSFP ports enabled

- One-hundred forty-four(144) 10 Gigabit Ethernet (GbE) QSFP+ ports using breakout cables, or
- Ninety-six fixed 10 Gigabit Ethernet (Gbe) QSFP+ ports and additional forty-eight 10 Gbe QSFP+ ports with breakout cables on twelve (12) 40 Gbe ports or
- Ninety-six fixed 10 Gigabit Ethernet (Gbe) QSFP+ ports and additional Thirty-Two(32) 10 Gbe QSFP+ ports with breakout cables on eight (8) 40Gbe ports and Four (4) fixed 100 Gbe QSFP+

The VDX 8770-4 switch provides up to 192 10-Gigabit Ethernet or 1 Gigabit Ethernet external ports or 48 40-Gigabit Ethernet external ports, while the VDX 8770-8 switch provides up to 384 10-Gigabit Ethernet or 1 Gigabit external ports or 96 40-Gigabit Ethernet external ports. The 8770 hardware platforms that support the TOE have a number of common hardware characteristics:

- Dual, redundant management modules (8770-MM-1)
- Serial (console), Ethernet, and USB connections for management modules (though only Brocade branded USB devices are supported)
- Support for short-range and long-range 1 Gbps SFP transceivers
- Support for short-range and long range 10 Gbps SFP+ transceivers
- Support for 40 Gbps QSFP transceivers

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the frames or packets being forwarded out of the device over another interface, or dropped in accordance with a configured policy.

1.4.1 TOE Architecture

The basic architecture of each TOE appliance begins with a hardware appliance with physical network connections. Within the hardware appliance the Extreme Networks NOS is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing and switching functions). NOS enforces applicable security policies on network information flowing through the hardware appliance.

1.4.1.1 Physical Boundaries

Each TOE appliance runs a version of the Extreme Networks NOS and has physical network connections to its environment to facilitate routing and switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

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 a syslog server in the environment. This is generally advisable given the limited audit log storage space on the evaluated appliances.

The TOE sets its internal clock using administrative commands issued at the CLI interface.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by VDX Product Series:

- Security audit
- Cryptographic support
- 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 for numerous activities including policy enforcement, system management and authentication. A syslog server in the environment is relied on to store audit records generated by the TOE. The TOE generates a complete audit record including the IP address of the TOE, the event details, and the time the event occurred. The time stamp is provided by the TOE appliance hardware.

1.4.1.2.2 Cryptographic support

The TOE contains CAVP-tested cryptographic implementations that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including SSH and TLS.

1.4.1.2.3 Identification and authentication

The TOE authenticates administrative users. In order for an administrative user to access the TOE, a user account including a user name and password must be created for the user, and an administrative role must be assigned. The TOE performs the validation of the login credentials.

1.4.1.2.4 Security management

The TOE provides Command Line Interface (CLI) commands to access the wide range of security management functions to manage its security policies. The TOE also provides REST APIs (protected by TLS) and NetConf (protected by SSH) to configure the TOE. Security management commands are limited to authorized users (i.e., administrators) and available only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Authorized Administrator role can actually manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management.

1.4.1.2.5 Protection of the TSF

The TOE implements a number of features design to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

Note that the TOE is a single appliance or a closely grouped (e.g., in the same rack) collection of appliances acting as a unit. As such, no intra-TOE communication is subject to any risks that may require special protection (e.g., cryptographic mechanisms).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

1.4.1.2.6 TOE access

The TOE can be configured to display a message of the day banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

1.4.1.2.7 Trusted path/channels

The TOE protects interactive communication with administrators using SSHv2 for CLI and NetConf access, ensuring both integrity and disclosure protection. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, an attempted connection will not be established. The TOE also provides a REST API interface for security management that is protected with TLS.

The TOE protects communication with network peers, such as a log server, using TLS connections to prevent unintended disclosure or modification of logs. SSHv2 is used to support SCP which the TOE uses for download of TOE updates.

1.4.2 TOE Documentation

Extreme Networks offers a series of documents that describe the installation process for the TOE 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:

- Configuration Guide, Network OS Common Criteria, Supporting Network OS v7.3.0aa, January 2019.

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
- Package Claims:
  - collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, Version 2.0, 14 March 2018 (NDcPP20E)
- NIAP Technical Decisions
  - TD0228, TD0257, TD0259, TD0281, TD0289, TD0290, TD0291, TD0321, TD0324, TD0333, TD0335, TD0336, TD0337, TD0338, TD0339, TD0340, TD0341, TD0342

2.1 Conformance Rationale

The ST conforms to the NDcPP20E. 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 NDcPP20E and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDcPP20E offers additional information about the identified security objectives, but that has not been reproduced here and the NDcPP20E should be consulted if there is interest in that material.

In general, the NDcPP20E has defined Security Objectives appropriate for network devices and as such are applicable to the VDX Product Series operating with NOS version 7.3.0aa TOE.

3.1 Security Objectives for the Operational Environment

OE.ADMIN_CREDENTIALS_SECURE The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

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.NO_THRU_TRAFFIC_PROTECTION The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

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

OE.RESIDUAL_INFORMATION The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

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

OE.UPDATES The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDcPP20E. The NDcPP20E defines the following extended requirements and since they are not redefined in this ST the NDcPP20E should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- FAU_STG_EXT.1: Protected Audit Event Storage
- FCS_HTTPS_EXT.1: HTTPS Protocol
- FCS_RBG_EXT.1: Random Bit Generation
- FCS_SSHS_EXT.1: SSH Server Protocol
- FCS_TLSC_EXT.1: TLS Client Protocol
- FCS_TLSS_EXT.1: TLS Server Protocol
- FIA_PMG_EXT.1: Password Management
- FIA_UAU_EXT.2: Password-based Authentication Mechanism
- FIA_UIA_EXT.1: User Identification and Authentication
- FIA_X509_EXT.1(2): X.509 Certificate Validation (Rev)
- FPT_APW_EXT.1: Protection of Administrator Passwords
- FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
- FPT_STM_EXT.1: Reliable Time Stamps
- FPT_TST_EXT.1: TSF testing
- FPT_TUD_EXT.1: 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 NDcPP20E. The refinements and operations already performed in the NDcPP20E are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDcPP20E and any residual operations have been completed herein. Of particular note, the NDcPP20E 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 NDcPP20E which includes all the SARs for EAL 1. However, the SARs are effectively refined since requirement-specific 'Assurance Activities' are defined in the NDcPP20E that serve to ensure corresponding evaluations will yield more practical and consistent assurance than the EAL 1 assurance requirements alone. The NDcPP20E should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by VDX Product Series operating with NOS version 7.3.0aa TOE.

Requirement Class	Requirement Component
FAU: Security audit	NDcPP20E:FAU_GEN.1: Audit Data Generation
	NDcPP20E:FAU_GEN.2: User identity association
	NDcPP20E:FAU_STG_EXT.1: Protected Audit Event Storage
FCS: Cryptographic support	NDcPP20E:FCS_CKM.1: Cryptographic Key Generation
	NDcPP20E:FCS_CKM.2: Cryptographic Key Establishment
	NDcPP20E:FCS_CKM.4: Cryptographic Key Destruction
	NDcPP20E:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	NDcPP20E:FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)
	NDcPP20E:FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	NDcPP20E:FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)
	NDcPP20E:FCS_HTTPS_EXT.1: HTTPS Protocol
	NDcPP20E:FCS_RBG_EXT.1: Random Bit Generation
	NDcPP20E:FCS_SSHS_EXT.1: SSH Server Protocol
	NDcPP20E:FCS_TLSC_EXT.1: TLS Client Protocol
	NDcPP20E:FCS_TLSS_EXT.1: TLS Server Protocol
FIA: Identification and authentication	NDcPP20E:FIA_AFL.1: Authentication Failure Management
	NDcPP20E:FIA_PMG_EXT.1: Password Management
	NDcPP20E:FIA_UAU.7: Protected Authentication Feedback
	NDcPP20E:FIA_UAU_EXT.2: Password-based Authentication Mechanism
	NDcPP20E:FIA_UIA_EXT.1: User Identification and Authentication
	NDcPP20E:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
	NDcPP20E:FIA_X509_EXT.2: X.509 Certificate Authentication
	NDcPP20E:FIA_X509_EXT.3: X.509 Certificate Requests

FMT: Security management	NDcPP20E:FMT_MOF.1/ManualUpdate: Management of security functions behaviour
	NDcPP20E:FMT_MTD.1/CoreData: Management of TSF Data
	NDcPP20E:FMT_SMF.1: Specification of Management Functions
	NDcPP20E:FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	NDcPP20E:FPT_APW_EXT.1: Protection of Administrator Passwords
	NDcPP20E:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	NDcPP20E:FPT_STM_EXT.1: Reliable Time Stamps
	NDcPP20E:FPT_TST_EXT.1: TSF testing
	NDcPP20E:FPT_TUD_EXT.1: Trusted update
FTA: TOE access	NDcPP20E:FTA_SSL.3: TSF-initiated Termination
	NDcPP20E:FTA_SSL.4: User-initiated Termination
	NDcPP20E:FTA_SSL_EXT.1: TSF-initiated Session Locking
	NDcPP20E:FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	NDcPP20E:FTP_ITC.1: Inter-TSF trusted channel
	NDcPP20E:FTP_TRP.1/Admin: Trusted Path

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (NDcPP20E:FAU_GEN)

NDcPP20E:FAU_GEN.1.1

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

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

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

c) All administrative actions comprising:

- Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- Resetting passwords (name of related user account shall be logged).
- [***no other actions***];

d) Specifically defined auditable events listed in Table 2.

Requirement	Auditable Events	Additional Content
NDcPP20E:FAU_GEN.1		
NDcPP20E:FAU_GEN.2		
NDcPP20E:FAU_STG_EXT.1		
NDcPP20E:FCS_CKM.1		
NDcPP20E:FCS_CKM.2		
NDcPP20E:FCS_CKM.4		
NDcPP20E:FCS_COP.1/DataEncryption		
NDcPP20E:FCS_COP.1/Hash		
NDcPP20E:FCS_COP.1/KeyedHash		

NDcPP20E:FCS_COP.1/SigGen		
NDcPP20E:FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
NDcPP20E:FCS_RBG_EXT.1		
NDcPP20E:FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
NDcPP20E:FCS_TLSC_EXT.1	Failure to establish a TLS Session.	Reason for failure.
NDcPP20E:FCS_TLSS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
NDcPP20E:FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address).
NDcPP20E:FIA_PMG_EXT.1		
NDcPP20E:FIA_UAU.7		
NDcPP20E:FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP20E:FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP20E:FIA_X509_EXT.1(2)	None	None
NDcPP20E:FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	
NDcPP20E:FMT_MTD.1/CoreData	All management activities of TSF data.	
NDcPP20E:FMT_SMF.1		
NDcPP20E:FMT_SMR.2		
NDcPP20E:FPT_APW_EXT.1		
NDcPP20E:FPT_SKP_EXT.1		
NDcPP20E:FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
NDcPP20E:FPT_TST_EXT.1		
NDcPP20E:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	
NDcPP20E:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	
NDcPP20E:FTA_SSL.4	The termination of an interactive session.	
NDcPP20E:FTA_SSL_EXT.1	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The termination of a local session by the session locking mechanism.	
NDcPP20E:FTA_TAB.1		
NDcPP20E:FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted	Identification of the initiator and target of failed trusted channels establishment attempt.

	channel functions.	
NDcPP20E:FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	

NDcPP20E:FAU_GEN.1.2

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, information specified in column three of Table 2.

5.1.1.2 User identity association (NDcPP20E:FAU_GEN.2)

NDcPP20E: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 Protected Audit Event Storage (NDcPP20E:FAU_STG_EXT.1)

NDcPP20E:FAU_STG_EXT.1.1

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

NDcPP20E:FAU_STG_EXT.1.2

The TSF shall be able to store generated audit data on the TOE itself.

NDcPP20E:FAU_STG_EXT.1.3

The TSF shall [***overwrite previous audit records according to the following rule: [audit records are maintained in a circular buffer and oldest records are overwritten first]***] when the local storage space for audit data is full.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (NDcPP20E:FCS_CKM.1)

NDcPP20E:FCS_CKM.1.1

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.3,

- FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3 (per TD0291].

5.1.2.2 Cryptographic Key Establishment (NDcPP20E:FCS_CKM.2)

NDcPP20E:FCS_CKM.2.1

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- RSA-based key establishment schemes that meet the following: NIST Special Publication 800-56B Revision 1, 'Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography',

- Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3].

5.1.2.3 Cryptographic Key Destruction (NDcPP20E:FCS_CKM.4)

NDcPP20E:FCS_CKM.4.1

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

[- ***For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes]];,***

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

that meets the following: No Standard.

5.1.2.4 Cryptographic Operation (AES Data Encryption/Decryption) (NDcPP20E:FCS_COP.1/DataEncryption)

NDcPP20E:FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***CBC, CTR***] mode and cryptographic key sizes [***128 bits, 256 bits***] that meet the following: AES as specified in ISO 18033-3, [***CBC as specified in ISO 10116, CTR as specified in ISO 10116***]**.**

5.1.2.5 Cryptographic Operation (Hash Algorithm) (NDcPP20E:FCS_COP.1/Hash)

NDcPP20E:FCS_COP.1.1/Hash

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

5.1.2.6 Cryptographic Operation (Keyed Hash Algorithm) (NDcPP20E:FCS_COP.1/KeyedHash)

NDcPP20E:FCS_COP.1.1/KeyedHash

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

5.1.2.7 Cryptographic Operation (Signature Generation and Verification) (NDcPP20E:FCS_COP.1/SigGen)

NDcPP20E:FCS_COP.1.1/SigGen

The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits]]

that meet the following:

[- ***For RSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3***].

5.1.2.8 HTTPS Protocol (NDcPP20E:FCS_HTTPS_EXT.1)

NDcPP20E:FCS_HTTPS_EXT.1.1

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

NDcPP20E:FCS_HTTPS_EXT.1.2

The TSF shall implement HTTPS using TLS.

NDcPP20E:FCS_HTTPS_EXT.1.3

If a peer certificate is presented, the TSF shall [***not require client authentication***].

5.1.2.9 Random Bit Generation (NDcPP20E:FCS_RBG_EXT.1)

NDcPP20E:FCS_RBG_EXT.1.1

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

NDcPP20E:FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***one software-based noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011, of the keys and CSPs that it will generate.

5.1.2.10 SSH Server Protocol (FCS_SSHS_EXT.1)

NDcPP20E:FCS_SSHS_EXT.1.1

The TSF shall implement the SSH protocol that complies with RFC(s) [***4251, 4252, 4253, 4254***].

NDcPP20E:FCS_SSHS_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*]**. (TD0339 applied)

NDcPP20E:FCS_SSHS_EXT.1.3

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

NDcPP20E:FCS_SSHS_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [***aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr***]. (TD0337 applied)

NDcPP20E:FCS_SSHS_EXT.1.5

The TSF shall ensure that the SSH public-key based authentication implementation uses [***ssh-rsa***] as its public key algorithm(s) and rejects all other public key algorithms. (TD0259 applied)

NDcPP20E:FCS_SSHS_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [***hmac-sha1, hmac-sha2-256, hmac-sha2-512***] and [***no other MAC algorithms***] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s). (TD0337 applied)

NDcPP20E:FCS_SSHS_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.

NDcPP20E:FCS_SSHS_EXT.1.8

The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

5.1.2.11 TLS Client Protocol (NDcPP20E:FCS_TLSC_EXT.1)

NDcPP20E:FCS_TLSC_EXT.1.1

The TSF shall implement [***TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:
[TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246].

NDcPP20E:FCS_TLSC_EXT.1.2

The TSF shall verify that the presented identifier matches the reference identifier according to RFC 6125.

NDcPP20E:FCS_TLSC_EXT.1.3

The TSF shall only establish a trusted channel if the server certificate is valid. If the server certificate is deemed invalid, then the TSF shall [***not establish the connection***].

NDcPP20E:FCS_TLSC_EXT.1.4

The TSF shall [***not present the Supported Elliptic Curves Extension***] in the Client Hello.

5.1.2.12 TLS Server Protocol (NDcPP20E:FCS_TLSS_EXT.1)

NDcPP20E:FCS_TLSS_EXT.1.1

The TSF shall implement [***TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:
[***TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,***
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246].

NDcPP20E:FCS_TLSS_EXT.1.2

The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [***none***].

NDcPP20E:FCS_TLSS_EXT.1.3

The TSF shall [***perform RSA key establishment with key size [2048 bits]***].

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication Failure Management (NDcPP20E:FIA_AFL.1)

NDcPP20E:FIA_AFL.1.1

The TSF shall detect when an Administrator configurable positive integer within [**1-6**] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely.

NDcPP20E:FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***prevent the offending remote Administrator from successfully authenticating until a configured amount of time elapses].***

5.1.3.2 Password Management (NDcPP20E:FIA_PMG_EXT.1)

NDcPP20E:FIA_PMG_EXT.1.1

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [***'!', '@', '#', '$', '%', '^', '&', '*', ')'***];

b) Minimum password length shall be configurable to [***6***] and [***32***].

5.1.3.3 Protected Authentication Feedback (NDcPP20E:FIA_UAU.7)

NDcPP20E: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.

5.1.3.4 Password-based Authentication Mechanism (NDcPP20E:FIA_UAU_EXT.2)

NDcPP20E:FIA_UAU_EXT.2.1

The TSF shall provide a local password-based authentication mechanism, and [***no other authentication***] to perform local administrative user authentication.

5.1.3.5 User Identification and Authentication (NDcPP20E:FIA_UIA_EXT.1)

NDcPP20E: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;
- [***[network routing and SAN services]***].

NDcPP20E: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.

5.1.3.6 X.509 Certificate Validation (Rev) (NDcPP20E:FIA_X509_EXT.1/Rev)

NDcPP20E:FIA_X509_EXT.1.1/Rev

The TSF shall validate certificates in accordance with the following rules:
- RFC 5280 certificate validation and certificate path validation supporting a minimum path length of three certificates.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE. (TD0340 applied).
- The TSF shall validate the revocation status of the certificate using [***the Online Certificate Status Protocol (OCSP) as specified in RFC 6960***]
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - o Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

NDcPP20E:FIA_X509_EXT.1(2).2

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

5.1.3.7 X.509 Certificate Authentication (NDcPP20E:FIA_X509_EXT.2)

NDcPP20E:FIA_X509_EXT.2.1

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

NDcPP20E:FIA_X509_EXT.2.2

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

5.1.3.8 X.509 Certificate Requests (NDcPP20E:FIA_X509_EXT.3)

NDcPP20E:FIA_X509_EXT.3.1

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

NDcPP20E:FIA_X509_EXT.3.2

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

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behaviour (NDcPP20E:FMT_MOF.1/ManualUpdate)

NDcPP20E:FMT_MOF.1.1/ManualUpdate

The TSF shall restrict the ability to enable the functions to perform manual update to Security Administrators.

5.1.4.2 Management of TSF Data (NDcPP20E:FMT_MTD.1/CoreData)

NDcPP20E:FMT_MTD.1.1/CoreData

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

5.1.4.3 Specification of Management Functions (NDcPP20E:FMT_SMF.1)

NDcPP20E:FMT_SMF.1.1

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

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [***digital signature***] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [***o Ability to configure audit behavior,***

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

5.1.4.4 Restrictions on Security Roles (NDcPP20E:FMT_SMR.2)

NDcPP20E:FMT_SMR.2.1

The TSF shall maintain the roles: - Security Administrator.

NDcPP20E:FMT_SMR.2.2

The TSF shall be able to associate users with roles.

NDcPP20E:FMT_SMR.2.3

The TSF shall ensure that the conditions

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

are satisfied.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Protection of Administrator Passwords (NDcPP20E:FPT_APW_EXT.1)

NDcPP20E:FPT_APW_EXT.1.1

The TSF shall store passwords in non-plaintext form.

NDcPP20E:FPT_APW_EXT.1.2

The TSF shall prevent the reading of plaintext passwords.

5.1.5.2 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) (NDcPP20E:FPT_SKP_EXT.1)

NDcPP20E:FPT_SKP_EXT.1.1

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

5.1.5.3 Reliable Time Stamps (NDcPP20E:FPT_STM_EXT.1)

NDcPP20E:FPT_STM_EXT.1.1

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

NDcPP20E:FPT_STM_EXT.1.2

The TSF shall [***allow the Security Administrator to set the time***].

5.1.5.4 TSF testing (NDcPP20E:FPT_TST_EXT.1)

NDcPP20E:FPT_TST_EXT.1.1

The TSF shall run a suite of the following self-tests [***during initial start-up (on power on)]***] to demonstrate the correct operation of the TSF:

[**- Cryptographic Known Answer Test (KAT)**
- Continuous Tests for entropy and RNG,
- Firmware load test].

5.1.5.5 Trusted update (NDcPP20E:FPT_TUD_EXT.1)

NDcPP20E:FPT_TUD_EXT.1.1

The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [***no other TOE firmware/software version***].

NDcPP20E:FPT_TUD_EXT.1.2

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

NDcPP20E:FPT_TUD_EXT.1.3

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

5.1.6 TOE access (FTA)

5.1.6.1 TSF-initiated Termination (NDcPP20E:FTA_SSL.3)

NDcPP20E:FTA_SSL.3.1

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

5.1.6.2 User-initiated Termination (NDcPP20E:FTA_SSL.4)

NDcPP20E:FTA_SSL.4.1

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

5.1.6.3 TSF-initiated Session Locking (NDcPP20E:FTA_SSL_EXT.1)

NDcPP20E:FTA_SSL_EXT.1.1

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

5.1.6.4 Default TOE Access Banners (NDcPP20E:FTA_TAB.1)

NDcPP20E:FTA_TAB.1.1

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

5.1.7 Trusted path/channels (FTP)

5.1.7.1 Inter-TSF trusted channel (NDcPP20E:FTP_ITC.1)

NDcPP20E:FTP_ITC.1.1

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

NDcPP20E:FTP_ITC.1.2

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

NDcPP20E:FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [***exporting audit events***].

5.1.7.2 Trusted Path (NDcPP20E:FTP_TRP.1/Admin)

NDcPP20E:FTP_TRP.1.1/Admin

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

NDcPP20E:FTP_TRP.1.2/Admin

The TSF shall permit remote Administrators to initiate communication via the trusted path.

NDcPP20E:FTP_TRP.1.3/Admin

The TSF shall require the use of the trusted path for initial Administrator authentication and all remote administration actions.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the 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 â€“ Conformance

AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Survey

Table 2 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 useraccessible 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 fulfill 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 â€“ 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
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

The TOE is designed to produce syslog conformant messages in a number of circumstances including warnings about the device itself (such as temperature, power failures, etc.) as well as security relevant events (the success and failure login of the user, regardless of the authentication mechanism; changing a user's password; adding and deleting user accounts; modification, addition and deletion of ACLs; and violations of the ACL rules). In each case the audit record includes the time and date, identification of the responsible subject (e.g., by network address or user ID), the type of event, the outcome of the event, and other information depending on the event type.

The audit records are stored in a log (internal to the TOE appliance) that is protected so that only an authorized TOE User can read (for which tools accessible via the CLI are provided) or otherwise access them. The protection results from the fact that the logs can be accessed only after a user logs in (see section 6.4 below).

The log stores up to 1024 entries after which the audit entries will be overwritten, oldest first. The administrator (with Authorized Administrator privilege) can (and should) choose to configure one or more external syslog servers where the TOE will send a copy of the audit records if so desired. The TOE can be configured to use TLS to protect audit logs exported to an external server. Audit records are recorded locally and sent to the remote server simultaneously.

The TOE includes a hardware clock that is used to provide reliable time information for the audit records it generates.

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

- NDcPP20E:FAU_GEN.1: The TOE can generate audit records for events include starting and stopping the audit function, administrator commands, and all other events identified in section 5.1.1. Furthermore, each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in section 5.1.1. For cryptographic keys, the act of importing and deleting a key is audited and the associated administrator account that performed the action is recorded.
- NDcPP20E: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.
- NDcPP20E:FAU_STG_EXT.1: The TOE can be configured to export audit records to an external SYSLOG server. This communication is protected with the use of TLS.

6.2 Cryptographic support

The TOE supports a range of cryptographic services provided by the Extreme FIPS Cryptographic Library Version 2.1 (Firmware) running on Freescale E500mc processors in the evaluated TOE models identified in section 1.4. The following functions have been CAVP tested.

Functions	Requirement	Cert #
Encryption/Decryption		
AES CBC (128 and 256 bits) AES CTR (128 and 256 bits)	FCS_COP.1/DataEncryption	AES:5666
Cryptographic signature services		
• RSA Digital Signature Algorithm (rDSA) (modulus 2048)	FCS_COP.1/SigGen	RSA: 3048
Cryptographic hashing		
SHA-1, SHA-256, SHA-512 (digest sizes 160, 256, 512)	FCS_COP.1/Hash	SHS:4540
Keyed-hash message authentication		
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512 (digest sizes 160, 256, 512)	FCS_COP.1/KeyedHash	HMAC:3771
Random bit generation		
CTR_DRBG with sw based noise sources with a minimum of 256 bits of non-determinism	FCS_RBC_EXT.1	DRBG:2288
Key Generation		
• RSA Key Generation	FCS_CKM.1 FCS_CKM.1	RSA: 3048

Table 3 Cryptographic Functions

The TOE uses a software-based random bit generator that complies with Special Publication 800-90 using CTR_DRBG when operating in the FIPS mode. AES-256 is used in conjunction with a minimum of 256 bits of entropy.

The TOE supports the SSHv2 (compliant with RFCs 4251, 4252, 4253, and 4254) and TLS v1.1 (RFC4346), and TLS v1.2 (RFC 5246) secure communication protocols.

The TOE supports TLSv1.1, and v1.2 with the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_ SHA256

The TOE supports SSHv2 with AES (CBC and CTR) 128 or 256 bit ciphers, in conjunction with HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA-512 for message integrity. The TOE supports the following public key methods – ssh-rsa. The TOE offers the following key exchange methods - diffie-hellman-group14-sha1.

The TOE allows users to perform SSHv2 authentication using password based authentication and allows users to upload a public key for SSHv2 public key client authentication. The TOE's SSHv2 implementation limits SSH packets to a size of 256K bytes. Whenever the timeout period or authentication retry limit is reached, the TOE closes the applicable TCP connection and releases the SSH session resources. As SSH packets are being received, the TOE uses a buffer to build all packet information. Once complete, the packet is checked to ensure it can be appropriately decrypted. However, if it is not complete when the buffer becomes full (256K bytes) the packet will be dropped and the connection terminated. There is a TOE initiated rekey before 1 hour or before 1GB whichever comes first. These are the default rekey values but they can be modified by the administrator.

The TOE supports the following secret keys, private keys and CSPs:

Key or CSP:	Zeroized upon:	Stored in:	Zeroized by:
SSH host private key	Command	Flash	Overwriting once with zeros
SSH host public key	Command	Flash	Overwriting once with zeros
SSH client public key	Command	Flash	Overwriting once with zeros
SSH session key	End of session	RAM	Overwriting once with zeros
TLS host private key	Command	Flash	Overwriting once with zeros
TLS host digital certificate	Command	Flash	Overwriting once with zeros
TLS pre-master secret	Handshake done	RAM	Overwriting once with zeros
TLS session key	Close of session	RAM	Overwriting once with zeros
User Password	Command	Flash	Overwriting once with zeros
DRBG Seed	Every 100ms	RAM	Overwritten with new value

Table 4 Cryptographic Keys and CSPs

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

- NDcPP20E:FCS_CKM.1: The TOE supports asymmetric key generation using RSA key establishment as part of TLS and SSH as described in the section above. The TOE acts as both a client and a server for TLS (RSA) and a server for SSH (RSA, DH-14 key generation). The TOE supports DH group 14 key establishment scheme that meets standard RFC 3526, section 3 for interoperability.

- NDcPP20E:FCS_CKM.2: See FCS_CKM.1.

- NDcPP20E:FCS_CKM.4: All data is cleared as identified above.

- NDcPP20E:FCS_COP.1/DataEncryption: The TOE performs encryption and decryption using AES in CBC or CTR mode with key sizes of either 128 or 256. The corresponding CAVP certificate is identified in the table above.

- NDcPP20E:FCS_COP.1/Hash: The TOE supports cryptographic hashing services using SHA-1, SHA-256, and SHA-512 with digest sizes 160, 256, and 512. The corresponding CAVP certificate is identified in the table above,

- NDcPP20E:FCS_COP.1/KeyedHash: The TOE supports keyed-hash message authentication using HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512 using SHA-1/256/512 with 160/256/512-bit keys to produce a 160/256/384 output MAC. The SHA-1/256 and 512 algorithms have block sizes of 512 and 1024-bits respectively. The corresponding CAVP certificate is identified in the table above

- NDcPP20E:FCS_COP.1/SigGen: The TOE supports the use of RSA with 2048 bit key sizes for cryptographic signatures. Digital signatures are used in TLS and SSH communications and on product updates. The corresponding CAVP certificate is identified in the table above.

- NDcPP20E:FCS_HTTPS_EXT.1: The TOE provides a REST API interface for remote administration and fully supports RFC 2818. The TOE acts as an HTTPS server and waits for client connections on TCP port 443. The TOE's HTTPS server supports TLS version 1.1/1.2 only and will deny connection requests from TLS clients with lower versions.

- NDcPP20E:FCS_RBG_EXT.1: The product uses an SP 800-90A AES-256 CTR_DRBG with software based noise sources with a minimum of 256 bits of non-determinism.

- NDcPP20E:FCS_SSHS_EXT.1: The TOE supports SSHv2 as described above for CLI management.

- NDcPP20E:FCS_TLSC_EXT.1: The TOE supports TLS v1.1 and v1.2 with the ciphersuites listed above for its syslog connections. The TOE does not support certificate pinning.

- NDcPP20E:FCS_TLSS_EXT.1: The TOE supports TLS v1.1 and v1.2 with the ciphersuites listed above for the REST API interface. The TOE will reject all SSL and older TLS versions (1.0) for connection attempts. The key agreement parameters of the server key exchange message are specified in the RFC 5246 (section 7.4.3) for TLSv1.2 and RFC 4346 (section 7.4.3) for TLSv1.1. The TOE conforms to both RFCs supporting RSA key establishment.

6.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, except to display warning banners and to permit network traffic to flow through the TOE without identification or authentication so long as it conforms to the information flow policy rules. The TOE authenticates TOE Users against their user name and password or through public-key based authentication.

The Authorized Administrator is able to define local user (or TOE User) accounts and to assign passwords and privilege levels to the accounts. Each user account has a user name, password, and a privilege level associated with it. There is a default privilege level account associated with each privilege level and each has its own password. It is up to the Authorized Administrator to decide whether or how to use these legacy accounts. Note however, that each has an identity, password, and privilege level.

While the Authorized Administrator can create or otherwise modify accounts freely, other users cannot change their own (or any other) security attributes. Note that the TOE supports a password enforcement configuration where the minimum password length can be set by an administrator up to 32 characters. Passwords can be created using any alphabetic, numeric, and a wide range of special characters (identified in FIA_PMG_EXT.1).

Alternative authentication mechanisms can also be configured by an Authorized Administrator using an Authentication Method List. This allows some flexibility in setting up authentication mechanisms when desired. The available mechanisms include Local User Accounts configured on the device. Local authentication methods include both password-based and public-key-based authentication. When authentication is successful, the TOE provides the associated user with applicable (role-based) privileges.

The Authentication Method List is ordered so that it will be processed from first to last. In each case, the user authentication will succeed, fail, or result in an error. If a given authentication method succeeds, the user will be logged in and will be able to perform functions according to their privilege level. If a given authentication mechanism fails, the user will be denied a login session. If the point is reached where every authentication method on the list fails, only an authorized administrator whose password is not rejected will succeed in logging in to the system.

The Authorized Administrator can set a lockout failure count for remote login attempts (the default is 3 attempts). If the count is exceeded, the targeted account is locked until a configured amount of time passes. The local administrator account never gets locked out.

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

- NDcPP20E:FIA_AFL.1: The administrator can set a maximum remote login failure number. If that is exceeded, the account is locked until a configured amount of time passes.
- NDcPP20E:FIA_PMG_EXT.1: The TOE implements a rich set of password composition constraints as described above.
- NDcPP20E:FIA_UAU.7: The TOE does not echo passwords as they are entered; rather '*' characters are echoed when entering passwords.
- NDcPP20E:FIA_UAU_EXT.2: The TOE uses local password-based authentication to login authorized administrative users remotely and locally.
- NDcPP20E:FIA_UIA_EXT.1: The TOE does not offer any services or access to its functions, except for the networking and SAN services and displaying a message of the day banner, without requiring a user to be identified and authenticated.
- NDcPP20E:FIA_X509_EXT.1/Rev: OCSP is supported for X509v3 certificate validation. Certificates are validated as part of the authentication process when they are presented to the TOE and when they are

loaded into the TOE. The following fields are verified as appropriate: SAN checks, CN checks, key usages, chain validation, and lastly expiration status. The common name (or SAN values if present) needs to be an IP address. Wildcards are not allowed in certificates.

- NDcPP20E:FIA_X509_EXT.2: Certificates are checked and if found not valid are not accepted or if the OCSP server cannot be contacted for validity checks, then the certificate is not accepted.
- NDcPP20E:FIA_X509_EXT.3: The TOE generates certificate requests and validates the CA used to sign the certificates.

6.4 Security management

The TOE associates each defined user account with a privilege level. The most privileged level is Authorized Administrator (with regards to the requirements in this Security Target users with lesser privilege levels are referred to collectively simply as TOE users). The TOE implements an internal access control mechanism that bases decisions about the use of functions and access to TOE data on those privilege levels. In this manner, the TOE is able to ensure that only the Authorized Administrator can access audit configuration data, information flow policy ACLs, user and administrator security attributes (including passwords and privilege levels), the logon failure threshold, the remote access user list; and cryptographic support settings.

Other than the Authorized Administrator role, the TOE implements a Read Only level where only basic commands can be issued and no changes can be made and a Port Configuration level where non-security device parameters can be managed. Collectively, this ST refers to all users of the TOE as “TOE Users” where the “Authorized Administrator” is a subset of that broader role.

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 or via a remote terminal using SSH. 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 administrator can use the REST API and NetConf interface to perform the same functions as the CLI.

Once authenticated (none of these functions is available to any user before being identified and authenticated), authorized administrators have access to the following security 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 a login banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Ability to configure audit behavior;
- Ability to set the time which is used for time-stamps.

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

- NDcPP20E:FMT_MOF.1/ManualUpdate: Only the authorized administrator can update the TOE.
- NDcPP20E:FMT_MTD.1/CoreData: Security management is restricted to administrators.
- NDcPP20E:FMT_SMF.1: The TOE provides administrative interfaces to perform the functions identified above.
- NDcPP20E:FMT_SMR.2: The TOE maintains administrative user roles.

6.5 Protection of the TSF

The TOE is an appliance and as such is designed to work independent of other components. While the administrative interface is function rich, the TOE is designed specifically to not provide access to locally stored passwords and also, while cryptographic keys can be entered, the TOE does not disclose any cryptographic keys stored in the TOE. All cryptographic keys are stored in an area of the filesystem not accessible to users and no user interface is provided to access the cryptographic keys. Dynamically generated cryptographic keys, such as for SSH sessions, are stored in RAM only. Cryptographic keys that are stored in the filesystem are protected from access by administrators.

The TOE is a hardware appliance that includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes administrator clock-related functions. The clock is used to provide timestamp for audit records, measuring session inactivity, and supporting timing elements of cryptographic functions. The TOE also implements the timing elements through timeout functionality due to inactivity for terminating both local and remote sessions.

The TOE performs cryptographic algorithm tests, firmware integrity and load tests, and critical function tests. Furthermore, the TOE is designed to query each pluggable module which in turn includes its own diagnostics that will serve to help identify any failing modules. When operating in FIPS mode, the power-on self-tests comply with the FIPS 140-2 requirements for self-testing.

The TOE supports loading a new software image manually by the administrator using CLI commands. From the CLI, an administrator can use either TFTP or SCP in order to download a software image. In either case, prior to actually installing and using the new software image, its digital signature is verified by the TOE. An unverified image cannot be installed.

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

- NDcPP20E:FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- NDcPP20E:FPT_APW_EXT.1: The TOE does not offer any functions that will disclose to any user a plain text password. Furthermore, locally defined passwords are not stored in plaintext form.
- NDcPP20E:FPT_STM.1: The TOE includes its own hardware clock.
- NDcPP20E:FPT_TST_EXT.1: The TOE includes a number of power-on diagnostics and cryptographic self-tests that will serve to ensure the TOE is functioning properly. The tests include cryptographic known answer tests, firmware integrity tests, ensure memory and flash can be accessed as expected, to ensure that software checksums are correct, and also to test the presence and function of plugged devices.

  The firmware signature is validated before it is loaded and executed.

  The random number generator is tested before all the algorithm testing is started.

  The known answer tests include AES-128-CBC, RSA-2048-SHA256, SHA256, SHA384, SHA512, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512.

  Upon failing any of its FIPS mode power-on self-tests, the TOE will continuously reboot.
- NDcPP20E:FPT_TUD_EXT.1: The TOE provides function to query the version and upgrade the software embedded in the TOE appliance. When installing updated software, digital signatures are used to authenticate the update to ensure it is the update intended and originated by Extreme Networks.

6.6 TOE access

The TOE can be configured to display a login banner. The login banner can be configured to display welcome information in conjunction with login prompts. It will be displayed when accessing the TOE via the console and SSH.

The TOE can be configured by an administrator to set a session timeout value (any value up to 240 minutes, with 0 disabling the timeout) – the default timeout is disabled. A session (local or remote) that is inactive (i.e., no commands issuing from the local or remote client) for the defined timeout value will be terminated.

The user will be required to login in after any session has been terminated due to inactivity or after voluntary termination. Of course, administrators can logout of local or remote sessions at any time.

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

- NDcPP20E:FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- NDcPP20E:FTA_SSL.4: The TOE provides the function to logout (or terminate) the both local and remote user sessions as directed by the user.
- NDcPP20E:FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.
- NDcPP20E:FTA_TAB.1: The TOE can be configured to display administrator-defined advisory banners when administrators successfully establish interactive sessions with the TOE, allowing administrators to terminate their session prior to performing any functions.

6.7 Trusted path/channels

The TOE provides a trusted path for its remote administrative users accessing the TOE via the Ethernet ports provided on the TOE using the CLI over SSH, NetConf over SSH, or REST APIs over TLS. Note that local administrator access via the serial port is also allowed for command line access. However this access is protected by physical protection of the serial interface along with the TOE itself.

When an administrator attempts to connect to the TOE remotely, the TOE attempts to negotiate a session. If the session cannot be negotiated, the connection is dropped.

Remote connections to third-party servers are supported for exporting audit records to an external audit server. Communication with an external servers is protected using TLS (as specified earlier).

In all cases, the endpoints are assured by virtue of the certificates installed, trusted, and reviewable when connecting and by virtue of user authentication.

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

- NDcPP20E:FTP_ITC.1: In the evaluated configuration, the TOE must be configured to use TLS to ensure that exported audit records are sent only to the configured server so they are not subject to inappropriate disclosure or modification as the TOE validates the audit server and against the TOE configuration using the certificates presented during TLS negotiation.
- NDcPP20E:FTP_TRP.1: The TOE provides SSH, NetConf, and REST APIs (HTTPS) to ensure secure remote administration. In each case, the administrator can initiate the remote session, the remote session is secured (disclosure and modification) using CAVP tested cryptographic operations, and all remote security management functions require the use of one of these secure channels.