Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100 Security Target

Version 0.7
December 16, 2022

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 Extreme Networks VSP Series Switches 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 Virtual Services Platform (VSP) Series Switches v8.3.100 Security Target

ST Version – Version 0.7

ST Date – December 16, 2022

1.2 TOE Reference

TOE Identification – Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100

TOE Developer – Extreme Networks, Inc.

Evaluation Sponsor – Extreme Networks, Inc.

1.3 TOE Overview

The TOE is the Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100. The TOE is a standalone network device that facilitates Data Link Layer data transfer between network nodes connected to its physical ports. TOE consists of a hardware appliance with embedded firmware. In the evaluated configuration this consists of an instance of either of the VSP4900, VSP7400, VSP8400, or ExtremeAcess Platform (XA) models.

All TOE appliances are shipped ready for immediate access through a Command Line Interface [CLI], with some basic features enabled by default. However, to ensure secure use, the product must be configured prior to being put into a production environment as specified in the user guidance. The CLI is a text based interface which is accessible from a directly connected terminal or via a remote terminal using SSH. All of the remote management interfaces are protected using encryption as explained later in this ST.

1.4 TOE Description

The TOE consists of the hardware models shown in Table 1-1. The TOE links the Mocana 32-bit libraries for cryptographic operations using non-PAA operations only with the Mocana GCM 64k feature enabled.

Platform	Model	Processor
VSP4900	VSP4900-48P	C3338 Intel Atom Denverton
	VSP4900-24S	C3338 Intel Atom Denverton
	VSP4900-24XE	C3538 Intel Atom Denverton
	VSP4900-12MXU-12XE	C3538 Intel Atom Denverton
VSP7400	VSP7400 -32C	C3758 Intel Atom Denverton
	VSP7400-48Y-8C	C3758 Intel Atom Denverton
VSP8400	VSP8404C	Freescale P2020 e500v2
ExtremeAccess Platform XA-1400	XA 1440	C3558 Intel Atom Denverton
	XA 1480	C3758 Intel Atom Denverton

Table 1-1 Extreme networking appliances – hardware

Each model includes an out of band management port that is Intel-based and a set of in band network interfaces that are all Broadcom-based. Therefore, all models have equivalent network interfaces.

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 TOE is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing and switching functions).

There are normally two management interfaces – a browser-based management UI accessed via TLS/HTTPS and a CLI accessed locally or via SSH. However, to meet the requirements listed in this Security Target, the browser-based management UI must be disabled as described by guidance. Thus, in the evaluated configuration only the CLI can be used for management.

The TOE Boundary is outlined in the following figure:

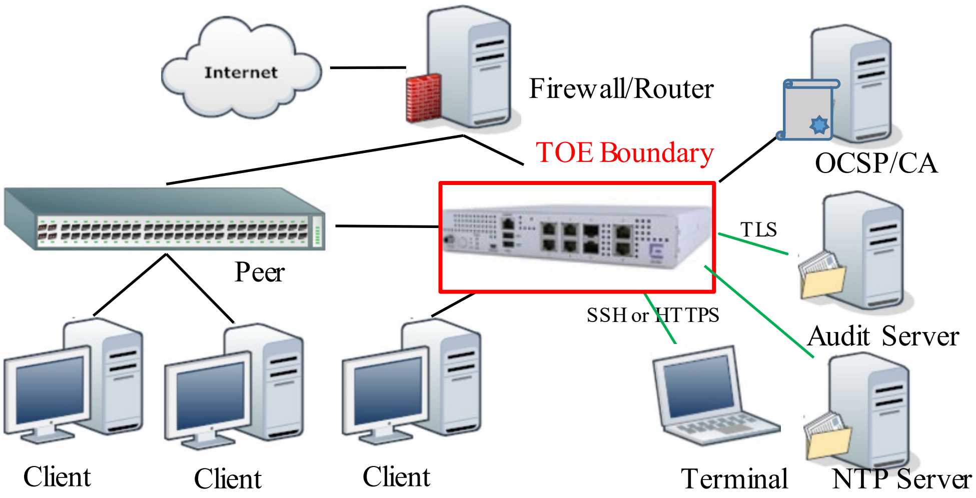

Figure 1: TOE Boundary

1.4.1.1 Physical Boundaries

The physical boundary of the TOE is the Extreme Networks Virtual Services Platform (VSP) Switches running VSP Operating System Software (VOSS) 8.3.100, which includes:

- The appliance hardware
- RJ-45/RS-232 management ports
- USB port
- Embedded software/firmware installed on the appliance
- CLI management interface

Each TOE appliance runs a version of the Extreme proprietary OS 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 management workstation 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 audit server (i.e., a syslog server) that is provided by 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 or can use an NTP server.

The evaluation assumes the Operational Environment of the TOE includes the following:

- The SSH client that is used to access the management interface
- The management workstation that hosts the SSH client
- Syslog server for external storage of audit records
- NTP server for synchronizing system time
- Certificate Authority and OCSP servers to support X.509
- DNS server (optional not depicted in Figure 1)

The scope of the evaluation is limited to the requirements levied upon the TOE in the ST – all other functionality is outside the scope of the evaluation.

The TOE supports a number of features that are not part of the core functionality. These features are not included in the scope of the evaluation:

- Browser-based management UI accessed via TLS/HTTPS is disabled and is not evaluated.
- The use of SNMPv3 is excluded.

- Fabric Extend with IPsec is not evaluated.
- Use of the FTP server is excluded and it is disabled by default.
- Integration with AAA server is not evaluated.
- Virtualized VOSS versions are not included in the scope and are not evaluated.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by Extreme Networks Virtual Services Platform (VSP) Switches running VOSS 8.3.100:

- 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 Network Appliances provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include: failure on invoking cryptographic functionality such as establishment, termination and failure of a TLS session; establishment, termination and failure of an SSH session; all use of the user identification mechanisms; any use of the authentication mechanism; any change in the configuration of the TOE, changes to time, initiation of TOE update, indication of completion of TSF self-test, termination of a remote session; and initiation and termination of a trusted channel.

The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using TLS. The logs for all appliances can be viewed the CLI. The records include the date/time the event occurred, the event/type of event, the user ID associated with the event, and additional information of the event and its success and/or failure.

1.4.1.2.2 Cryptographic support

The TOE utilizes CAVP-tested cryptographic implementations to provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols. This cryptography is used to support the following features:

- TLS client in support of secure channel with remote syslog server,
- SSH server in support of secure CLI remote management interface,
- X.509 certificate validation and
- NTP support.

1.4.1.2.3 Identification and authentication

The TOE provides authentication services for administrative users to connect to the TOEs administrator interfaces (local CLI, and remote CLI). The TOE requires Administrators to authenticate prior to being granted access to any of the management functionality. In the Common Criteria evaluated configuration, the TOE requires a minimum password length be configured between 8 and 32 characters, as well as a minimum RSA key length of 2048 bits. The TOE provides administrator authentication against a local user database.

1.4.1.2.4 Security management

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

- Local console command line administration;
- Remote command line administration via SSHv2;

The TOE provides multiple interfaces to perform administration. While in the CLI command mode, the administrator has access to six distinct modes, or privileges, that provide access to a specific set of commands. Depending on RBAC configuration, not every administrative account would have access to all modes. The CLI modes are as follows:

- User EXEC Mode: Initial mode of access.
- Privileged EXEC Mode: User mode and password combination determines access level.
- Global Configuration Mode: Use this mode to make changes to the running configuration.
- Interface Configuration Mode: Use this mode to modify or configure logical interface, VLAN or a physical interface.
- Router Configuration Mode: Use this mode to modify protocol settings.
- Application Configuration Mode: Use this mode to access the applications.

The system allows administrators to view audit records in EXEC mode.

All administrative functionality is accessed via the CLI. The TOE audits all administrative access. The TOE displays login banners and inactivity timeouts to terminate idle administrative sessions after a set period of inactivity.

1.4.1.2.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls restrictions to management and configuration functionality to Administrators. The TOE prevents reading of private keys and plaintext passwords by any user. The TOE internally maintains the date and time. This date and time are used as a timestamp that is part of each audit record generated by the TOE. Administrators can update the TOE's clock manually or can configure the TOE to synchronize with an external time source. The TOE performs testing to verify correct operation of the security appliances themselves. The TOE verifies all software updates via digital signature (2048-bit RSA/SHA-256) and requires administrative intervention prior to the software updates being installed on the TOE to avoid the installation of unauthorized firmware.

1.4.1.2.6 TOE access

The TOE can terminate inactive sessions after a configurable period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE can also display specified banner on the local and remote CLI interfaces prior to allowing any administrative access to the TOE. The TOE allows users to manually terminate an established management session with the TOE.

1.4.1.2.7 Trusted path/channels

The TOE supports several types of secure communications:

- Trusted paths with remote administrators over SSH,
- Trusted channels with remote IT environment syslog servers over TLS.

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:

- Extreme VOSS Common Criteria Configuration Guide 8.3.100, December 2022

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 5, April 2017.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
    - Part 3 Conformant
- Package Claims:
    - collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)
    - Technical Decisions

Technical Decision	Applied	Notes
TD0670- NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	Yes	
TD0639 - NIT Technical Decision for Clarification for NTP MAC Keys	Yes	
TD0638 – NIT Technical Decision for Key Pair Generation for Authentication	Yes	
TD0636 - NIT Technical Decision for Clarification of Public Key User Authentication for SSH	No	SFR not claimed
TD0635 - NIT Technical Decision for TLS Server and Key Agreement Parameters	No	SFR not claimed (FCS_TLSS_EXT.1)
TD0634 - NIT Technical Decision for Clarification required for testing IPv6	Yes	
TD0633 - NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	No	SFR not claimed
TD0632 - NIT Technical Decision for Consistency with Time Data for vNDs	Yes	
TD0631 - NIT Technical Decision for Clarification of public key authentication for SSH Server	Yes	
TD0592 - NIT Technical Decision for Local Storage of Audit Records	Yes	
TD0591 - NIT Technical Decision for Virtual TOEs and hypervisors	Yes	
TD0581 - NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	Yes	
TD0580 - NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Yes	
TD0572 - NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	Yes	
TD0571 - NiT Technical Decision for Guidance on how to handle FIA_AFL.1	Yes	
TD0570 - NiT Technical Decision for Clarification about FIA_AFL.1	Yes	
TD0569 - NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	No	SFR not claimed
TD0564 - NiT Technical Decision for Vulnerability Analysis Search Criteria	Yes	
TD0563 - NiT Technical Decision for Clarification of audit date information	Yes	
TD0556 - NIT Technical Decision for RFC 5077 question	No	SFR not claimed (FCS_TLSS_EXT.1)
TD0555 - NIT Technical Decision for RFC Reference incorrect in TLSS Test	No	SFR not claimed (FCS_TLSS_EXT.1)
TD0547 - NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Yes	
TD0546 - NIT Technical Decision for DTLS- clarification of Application Note 63	No	SFR not claimed
TD0538 - NIT Technical Decision for Outdated link to allowed-with list	Yes	
TD0537 - NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	Yes	
TD0536 - NIT Technical Decision for Update Verification Inconsistency	Yes	
TD0528 - NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	Yes	
TD0527 - Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	Yes	

Table 2-1 Technical Decisions

2.1 Conformance Rationale

The ST conforms to the NDcPP22e. 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 NDcPP22e and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDcPP22e offers additional information about the identified security objectives, but that has not been reproduced here and the NDcPP22e should be consulted if there is interest in that material.

In general, the NDcPP22e has defined Security Objectives appropriate for network devices and as such are applicable to the Extreme Networks VSP Series Switches 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.COMPONENTS_RUNNING (applies to distributed TOEs only)
For distributed TOEs, the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.

OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.

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

OE.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. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

OE.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality.
For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

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

OE.VM_CONFIGURATION (applies to vNDs only)
For vNDs, the Security Administrator ensures that the VS and VMs are configured to

- reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and
- correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting).

The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration.

If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDcPP22e. The NDcPP22e defines the following extended requirements and since they are not redefined in this ST the NDcPP22e should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
- NDcPP22e:FCS_NTP_EXT.1: NTP Protocol
- NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
- NDcPP22e:FCS_SSHS_EXT.1: SSH Server Protocol
- NDcPP22e:FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication
- NDcPP22e:FIA_PMG_EXT.1: Password Management
- NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
- NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
- NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
- NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication
- NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
- NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
- NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
- NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps
- NDcPP22e:FPT_TST_EXT.1: TSF testing
- NDcPP22e:FPT_TUD_EXT.1: Trusted update
- NDcPP22e: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 NDcPP22e. The refinements and operations already performed in the NDcPP22e are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDcPP22e and any residual operations have been completed herein. Of particular note, the NDcPP22e 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 NDcPP22e. The NDcPP22e should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Extreme Networks VSP Series Switches TOE.

Requirement Class	Requirement Component
FAU: Security audit	NDcPP22e:FAU_GEN.1: Audit Data Generation
	NDcPP22e:FAU_GEN.2: User identity association
	NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
FCS: Cryptographic support	NDcPP22e:FCS_CKM.1: Cryptographic Key Generation
	NDcPP22e:FCS_CKM.2: Cryptographic Key Establishment
	NDcPP22e:FCS_CKM.4: Cryptographic Key Destruction
	NDcPP22e:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	NDcPP22e:FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)
	NDcPP22e:FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	NDcPP22e:FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)
	NDcPP22e:FCS_NTP_EXT.1: NTP Protocol
	NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
	NDcPP22e:FCS_SSHS_EXT.1: SSH Server Protocol
	NDcPP22e:FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication
FIA: Identification and authentication	NDcPP22e:FIA_AFL.1: Authentication Failure Management
	NDcPP22e:FIA_PMG_EXT.1: Password Management
	NDcPP22e:FIA_UAU.7: Protected Authentication Feedback
	NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
	NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
	NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
	NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication
	NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
FMT: Security management	NDcPP22e:FMT_MOF.1/ManualUpdate: Management of security functions behaviour
	NDcPP22e:FMT_MTD.1/CoreData: Management of TSF Data
	NDcPP22e:FMT_MTD.1/CryptoKeys: Management of TSF Data
	NDcPP22e:FMT_SMF.1: Specification of Management Functions
	NDcPP22e:FMT_SMR.2: Restrictions on Security Roles

FPT: Protection of the TSF	NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
	NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps
	NDcPP22e:FPT_TST_EXT.1: TSF testing
	NDcPP22e:FPT_TUD_EXT.1: Trusted update
FTA: TOE access	NDcPP22e:FTA_SSL.3: TSF-initiated Termination
	NDcPP22e:FTA_SSL.4: User-initiated Termination
	NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking
	NDcPP22e:FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	NDcPP22e:FTP_ITC.1: Inter-TSF trusted channel
	NDcPP22e:FTP_TRP.1/Admin: Trusted Path

Table 5-1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (NDcPP22e:FAU_GEN.1)

NDcPP22e: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** 5-2.

Requirement	Auditable Events	Additional Content
NDcPP22e:FAU_GEN.1	None	None
NDcPP22e:FAU_GEN.2	None	None
NDcPP22e:FAU_STG_EXT.1	None	None
NDcPP22e:FCS_CKM.1	None	None
NDcPP22e:FCS_CKM.2	None	None
NDcPP22e:FCS_CKM.4	None	None
NDcPP22e:FCS_COP.1/DataEncryption	None	None
NDcPP22e:FCS_COP.1/Hash	None	None
NDcPP22e:FCS_COP.1/KeyedHash	None	None
NDcPP22e:FCS_COP.1/SigGen	None	None
NDcPP22e:FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server
NDcPP22e:FCS_RBG_EXT.1	None	None
NDcPP22e:FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
NDcPP22e:FCS_TLSC_EXT.1	Failure to establish a TLS Session.	Reason for failure.

NDcPP22e:FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_PMG_EXT.1	None	None
NDcPP22e:FIA_UAU.7	None	None
NDcPP22e:FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
NDcPP22e:FIA_X509_EXT.2	None	None
NDcPP22e:FIA_X509_EXT.3	None	None
NDcPP22e:FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None
NDcPP22e:FMT_MTD.1/CoreData	None	None
NDcPP22e:FMT_MTD.1/CryptoKeys	None	None
NDcPP22e:FMT_SMF.1	All management activities of TSF data.	None
NDcPP22e:FMT_SMR.2	None	None
NDcPP22e:FPT_APW_EXT.1	None	None
NDcPP22e:FPT_SKP_EXT.1	None	None
NDcPP22e: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).
NDcPP22e:FPT_TST_EXT.1	None	None
NDcPP22e:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None
NDcPP22e:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None
NDcPP22e:FTA_SSL.4	The termination of an interactive session.	None
NDcPP22e: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.	None
NDcPP22e:FTA_TAB.1	None	None
NDcPP22e: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.
NDcPP22e:FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path.	None

	Failure of the trusted path functions.	

Table 5-2 Audit events

NDcPP22e: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 5-2.

5.1.1.2 User identity association (NDcPP22e:FAU_GEN.2)

NDcPP22e: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 (NDcPP22e:FAU_STG_EXT.1)

NDcPP22e: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.

NDcPP22e:FAU_STG_EXT.1.2

The TSF shall be able to store generated audit data on the TOE itself. In addition, [***The TOE shall consist of a single standalone component that stores audit data locally***]

NDcPP22e:FAU_STG_EXT.1.3

The TSF shall [***drop new audit data***] when the local storage space for audit data is full.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (NDcPP22e:FCS_CKM.1)

NDcPP22e: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,

- ECC schemes using 'NIST curves' [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4,

-FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.1

- FFC Schemes using 'safe-prime' groups that meet the following: NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography and [RFC 3526]].

5.1.2.2 Cryptographic Key Establishment (NDcPP22e:FCS_CKM.2)

NDcPP22e: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: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1,

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' (TD0581 applied),
- Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography'
- FFC Schemes using "safe-prime" groups that meet the following: NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography and [groups listed in RFC 3526] (TD0580 applied)].

5.1.2.3 Cryptographic Key Destruction (NDcPP22e:FCS_CKM.4)

NDcPP22e: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 [[2]-pass] overwrite consisting of [[one pass of a pseudo-random pattern using the TSF's RBG followed by one pass of zeroes]]***]

that meets the following: No Standard.

5.1.2.4 Cryptographic Operation (AES Data Encryption/Decryption) (NDcPP22e:FCS_COP.1/DataEncryption)

NDcPP22e:FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***CBC, CTR, GCM***] mode and cryptographic key sizes [***128 bits, 256 bits***] that meet the following: AES as specified in ISO 18033-3, [***CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772***].

5.1.2.5 Cryptographic Operation (Hash Algorithm) (NDcPP22e:FCS_COP.1/Hash)

NDcPP22e:FCS_COP.1.1/Hash

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

5.1.2.6 Cryptographic Operation (Keyed Hash Algorithm) (NDcPP22e:FCS_COP.1/KeyedHash)

NDcPP22e: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***] and cryptographic key sizes [**160 bits, 256 bits**] and message digest sizes [***160, 256***] 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) (NDcPP22e:FCS_COP.1/SigGen)

NDcPP22e: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 NTP Protocol (NDcPP22e:FCS_NTP_EXT.1)

NDcPP22e:FCS_NTP_EXT.1.1
The TSF shall use only the following NTP version(s) [***NTP v4 (RFC 5905)***].

NDcPP22e:FCS_NTP_EXT.1.2
The TSF shall update its system time using [***Authentication using [SHA1] as the message digest algorithm(s);***].

NDcPP22e:FCS_NTP_EXT.1.3
The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

NDcPP22e:FCS_NTP_EXT.1.4
The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

5.1.2.9 Random Bit Generation (NDcPP22e:FCS_RBG_EXT.1)

NDcPP22e: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)***].

NDcPP22e:FCS_RBG_EXT.1.2
The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***[one] software-based noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 'Security Strength Table for Hash Functions', of the keys and hashes that it will generate.

5.1.2.10 SSH Server Protocol (NDcPP22e:FCS_SSHS_EXT.1)

NDcPP22e:FCS_SSHS_EXT.1.1
The TSF shall implement the SSH protocol that complies with: RFC(s) 4251, 4252, 4253, 4254, [***4256***].

NDcPP22e:FCS_SSHS_EXT.1.2
The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [***password-based***]. (TD0631 applied)

NDcPP22e:FCS_SSHS_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than [**32768**] bytes in an SSH transport connection are dropped.

NDcPP22e:FCS_SSHS_EXT.1.4
The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [***aes128-ctr, aes256-ctr, aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, aes256-gcm@openssh.com]***.

NDcPP22e:FCS_SSHS_EXT.1.5
The TSF shall ensure that the SSH public-key based authentication implementation uses [***ssh-rsa, x509v3-ssh-rsa, x509v3-rsa2048-sha256***] as its public key algorithm(s) and rejects all other public key algorithms.

NDcPP22e:FCS_SSHS_EXT.1.6
The TSF shall ensure that the SSH transport implementation uses [***hmac-sha1, hmac-sha2-256, implicit***] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

NDcPP22e: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.

NDcPP22e:FCS_SSHS_EXT.1.8

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

5.1.2.11 TLS Client Protocol Without Mutual Authentication (NDcPP22e:FCS_TLSC_EXT.1)

NDcPP22e:FCS_TLSC_EXT.1.1

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

TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289]

and no other ciphersuites.

NDcPP22e:FCS_TLSC_EXT.1.2

The TSF shall verify that the presented identifier matches [***the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN***].

NDcPP22e:FCS_TLSC_EXT.1.3

When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [***Not implement any administrator override mechanism***].

NDcPP22e:FCS_TLSC_EXT.1.4

The TSF shall [***present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1]***] in the Client Hello.

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication Failure Management (NDcPP22e:FIA_AFL.1)

NDcPP22e:FIA_AFL.1.1

The TSF shall detect when an Administrator configurable positive integer within [**1 to 255**] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

NDcPP22e:FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until [the account unlock action] is taken by an Administrator;***].

5.1.3.2 Password Management (NDcPP22e:FIA_PMG_EXT.1)

NDcPP22e: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 between [**8**] and [**32**] characters.

5.1.3.3 Protected Authentication Feedback (NDcPP22e:FIA_UAU.7)

NDcPP22e: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 (NDcPP22e:FIA_UAU_EXT.2)

NDcPP22e:FIA_UAU_EXT.2.1

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

5.1.3.5 User Identification and Authentication (NDcPP22e:FIA_UIA_EXT.1)

NDcPP22e: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***].

NDcPP22e: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 (NDcPP22e:FIA_X509_EXT.1/Rev)

NDcPP22e:FIA_X509_EXT.1.1/Rev

The TSF shall validate certificates in accordance with the following rules:

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

NDcPP22e:FIA_X509_EXT.1.2/Rev

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

5.1.3.7 X.509 Certificate Authentication (NDcPP22e:FIA_X509_EXT.2)

NDcPP22e:FIA_X509_EXT.2.1

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

NDcPP22e:FIA_X509_EXT.2.2

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

5.1.3.8 X.509 Certificate Requests (NDcPP22e:FIA_X509_EXT.3)

NDcPP22e:FIA_X509_EXT.3.1

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

NDcPP22e: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 (NDcPP22e:FMT_MOF.1/ManualUpdate)

NDcPP22e:FMT_MOF.1.1/ManualUpdate

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

5.1.4.2 Management of TSF Data (NDcPP22e:FMT_MTD.1/CoreData)

NDcPP22e:FMT_MTD.1.1/CoreData

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

5.1.4.3 Management of TSF Data (NDcPP22e:FMT_MTD.1/CryptoKeys)

NDcPP22e:FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.1.4.4 Specification of Management Functions (NDcPP22e:FMT_SMF.1)

NDcPP22e:FMT_SMF.1.1

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

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [***digital signature***] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [***Ability to modify the behavior of the transmission of audit data to an external IT entity,***
- ***Ability to manage the cryptographic keys,***
- ***Ability to configure the cryptographic functionality,***
- ***Ability to re-enable an Administrator account,***
- ***Ability to configure thresholds for SSH rekeying,***
- ***Ability to set the time which is used for time-stamps,***
- ***Ability to configure NTP,***
- ***Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors,***
- ***Ability to import X509v3 certificates to the TOE's trust store***
- ***Ability to manage the trusted public keys database***]. (TD0631 applied)

5.1.4.5 Restrictions on Security Roles (NDcPP22e:FMT_SMR.2)

NDcPP22e:FMT_SMR.2.1

The TSF shall maintain the roles: - Security Administrator.

NDcPP22e:FMT_SMR.2.2

The TSF shall be able to associate users with roles.

NDcPP22e: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 (NDcPP22e:FPT_APW_EXT.1)

NDcPP22e:FPT_APW_EXT.1.1

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

NDcPP22e:FPT_APW_EXT.1.2

The TSF shall prevent the reading of plaintext administrative passwords.

5.1.5.2 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) (NDcPP22e:FPT_SKP_EXT.1)

NDcPP22e: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 (NDcPP22e:FPT_STM_EXT.1)

NDcPP22e:FPT_STM_EXT.1.1

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

NDcPP22e:FPT_STM_EXT.1.2

The TSF shall [***allow the Security Administrator to set the time, synchronise time with an NTP server***]. (TD0632 applied)

5.1.5.4 TSF testing (NDcPP22e:FPT_TST_EXT.1)

NDcPP22e:FPT_TST_EXT.1.1

The TSF shall run a suite of the following self-tests [***during initial start-up (on power on), at the conditions [as specified by FIPS PUB 140-2 Section 4.9.2]***] to demonstrate the correct operation of the TSF: [

Power-on self-tests:

Integrity check of the cryptographic module

Known Answer Tests (KAT) of cryptographic primitives

Conditional self-tests:

Key generation pairwise consistency tests

Continuous random number generator testing].

5.1.5.5 Trusted update (NDcPP22e:FPT_TUD_EXT.1)

NDcPP22e:FPT_TUD_EXT.1.1

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

NDcPP22e: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***].

NDcPP22e:FPT_TUD_EXT.1.3

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

5.1.6 TOE access (FTA)

5.1.6.1 TSF-initiated Termination (NDcPP22e:FTA_SSL.3)

NDcPP22e: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 (NDcPP22e:FTA_SSL.4)

NDcPP22e: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 (NDcPP22e:FTA_SSL_EXT.1)

NDcPP22e: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 (NDcPP22e:FTA_TAB.1)

NDcPP22e: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 (NDcPP22e:FTP_ITC.1)

NDcPP22e: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.

NDcPP22e:FTP_ITC.1.2

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

NDcPP22e:FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [**transmitting audit records to an audit server**].

5.1.7.2 Trusted Path (NDcPP22e:FTP_TRP.1/Admin)

NDcPP22e:FTP_TRP.1.1/Admin

The TSF shall be capable of using [***SSH***] 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.

NDcPP22e:FTP_TRP.1.2/Admin

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

NDcPP22e: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 - Conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Survey

Table 5-3 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 TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

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 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 - 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 a single standalone switch that provides extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. The types of events that cause audit records to be generated include identification and authentication related events, and administrative events. Each of the events is specified in the audit record is in sufficient detail to identify the user for which the event is associated (e.g., user identity, IP address), when the event occurred, the outcome of the event, and the type of event that occurred.

The audit functionality of the TOE cannot be separately shutdown and started, only severity level of logging for dispatching logs can be adjusted. Startup and shutdown of auditing coincides with starting and stopping of the TOE.

All audit events recorded locally on the appliance and can also be duplicated over secure channel to an external audit server (i.e., a syslog server). The logs can be viewed via the CLI (local or remote).

Based on the severity code of each audit record, the TOE can be configured to dispatch it to one or more of the following destinations:

- Local log file
- Remote syslog server
- Terminal display

The TOE supports remote audit logging using the syslog format (RFC 5424) with an external server. Audit messages are entered into the log and when a connection exists to an external syslog server the audits are also sent to the syslog server. Audit records associated with administrator activity include the identity of the administrator responsible for the activity.

In the evaluated configuration, the TOE is configured to export syslog records to a specified, external syslog server. The TOE protects communications with this external syslog server using an encrypted via TLS over TCP (RFC 5425) session. The TOE acts as a TLS client in the communication channel with an external syslog server. The TOE automatically ensures that the connection with the syslog server remains active. Once a syslog server has accepted the TLS connection from the TOE, the TOE pushes new audit logs to the syslog server over the TLS protected channel in real time. The audit records are transferred as they are generated.

If the connection with the syslog server is broken and the TLS session times out, the TOE will reconnect automatically after a short waiting period. The TOE will not attempt to retransmit the audit records generated while the connection was broken after normal connectivity is resumed. However, the TOE continues to save its internal audit trail in non-volatile memory regardless of the state of the external syslog server in local internal audit log files.

The TOE is a standalone device that saves its local internal audit log files in non-volatile memory within log files, where it does not overwrite older records. The TOE stops generating new audit records when non-volatile memory becomes 75% full. Only Authorized Administrators are able to clear the local logs using CLI commands. When an

Authorized Administrator clears local log files to make space available, the TOE automatically resumes auditing. When the TOE is not writing to local internal audit log files it will still attempt to send audit records generated to a connected syslog server.

The TOE generates the following types of audit logs during operation:

- Start-up of the TOE from both cold boot and reboot,
- Shutdown of the TOE (when shut down from the CLI),
- All administrative actions (both security relevant and non-security relevant) from the local CLI, Remote CLI, and GUI,
- TLS session establishment and termination with the syslog server,
- Errors during TLS session establishment (e.g., algorithm mismatch),
- Remote administrative SSH connection establishment,
- Remote administrative SSH connection closure,
- Errors during Remote administrative SSH connection establishment,
- Generation of certificate signing requests and associated keys,
- Import of certificates,
- Deletion of certificates,
- Successful authentication attempts (from the local CLI, and Remote CLI),
- Unsuccessful authentication attempts (from the local CLI, and Remote CLI),
- Administration session timeout (from the local CLI, and Remote CLI).
- Unsuccessful certificate validation,
- Unsuccessful certificate revocation status check,
- All attempts to update the TOE software,
- Discontinuous changes to time.

The TOE ensures that each auditable event is associated with the user that triggered the event. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IPv4 address, MAC address, host name, or other configured identification is included in the audit record.

The log records follow a standard format. All system messages include the following information:

- CPU slot number – the CP slot
- Timestamp – the format is MM/DD/YY hh:mm:ss.uuu, where uuu is milliseconds.
- Hostname – the hostname from which the message is generated
- Event code – identifies the event reported
- Module name – identifies the software module from which the log is generated
- Severity level – identifies the severity of the event
- Sequence number – identifies specific CLI command
- Context – specifies the type of the session used to connect to the switch. If the session is a remote session, the remote IP address is identified.
- Username – where applicable, identifies user logged into the switch.
- CLI command – specifies the command typed during the CLI session. All CLI commands are logged.

The Security audit function satisfies the following security functional requirements:

- NDcPP22e:FAU_GEN.1: The TOE can generate all the required auditable events as specified in Table 5-2. 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** 5-2. For cryptographic keys, the act of importing, exporting or deleting a key is audited, the key is identified by name and the associated administrator account is identified.

- NDcPP22e: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.
- NDcPP22e: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. Authorized administrators in EXEC mode are allowed access to view audit records on the TOE. Since EXEC mode is available to all authorized administrators all administrators can view audit records.

6.2 Cryptographic support

The Target of Evaluation (TOE) is the Extreme Networks Virtual Services Platform (VSP) Switches running VOSS 8.3.100. The TOE is software that run within the models shown in **Table 1-1 Extreme networking appliances - hardware**. The TOE includes the Mocana Cryptographic Library v6.5.2f (Software) on the processors shown in Table 1-1. The TOE exclusively relies on Mocana Cryptographic Library v6.5.2f as a provider of all cryptographic functionality. This cryptographic library performs all cryptographic operations in a 32-bit mode and does not utilize Processor Algorithm Accelerators (PAA). The Mocana Cryptographic Library has the Mocana GCM 64K feature enabled (this is tested by CAVP Cert A663).

Functions	Requirement		Cert #
Encryption/Decryption			
AES CBC (128 and 256 bits)	NDcPP22e:FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116	A661
AES CTR (128 and 256 bits)	NDcPP22e:FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116	A661
AES GCM (128 and 256 bits)	NDcPP22e:FCS_COP.1/DataEncryption	NIST SP 800-38A ISO 19772	A663
Cryptographic hashing			
SHA-1, SHA-256, SHA-384, SHA-512 (digest sizes 160, 256, 384,512)	NDcPP22e:FCS_COP.1/Hash	FIPS Pub 180-4 ISO/IEC 10118-3:2004	A661
Keyed-hash message authentication			
HMAC-SHA-1, HMAC-SHA-256 (digest sizes 160, and 256)	NDcPP22e:FCS_COP.1/KeyedHash	FIPS Pub 198-1 FIPS Pub 180-4 ISO/IEC 9797-2:2011	A661
Cryptographic signature services			
RSA Digital Signature Algorithm (rDSA) (modulus 2048)	NDcPP22e:FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 9796-2	A661
Random bit generation			
CTR_DRBG with SW based noise sources with a minimum of 256 bits of non-determinism	NDcPP22e:FCS_RBG_EXT.1	FIPS SP 800-90A ISO/IEC 18031:2011	A661
Key Generation			
RSA Key Generation (2048 bit)	NDcPP22e:FCS_CKM.1	FIPS Pub 186-4	A661
ECDSA Key Generation with Curves P-256, P-384 and P-521		FIPS Pub 186-4	A661
FFC Scheme DSA (2048-bit)		FIPS Pub 186-4	A661

FFC Scheme using Diffie-Hellman Group 14		Per Policy 5: No NIST CAVP, CCTL must perform all assurance/evaluation activities	
Key Establishment			
RSA Key Establishment (2048-bit)	NDcPP22e:FCS_CKM.2	RSAES-PKCS1-v1_5	Vendor Affirmed
ECC Key Establishment with Curves P-256, P-384 and P-521		NIST SP 800-56A Rev 3	A2791
FFC Key Establishment (2048-bit)		NIST SP 800-56A Rev 3	A2791
FFC Schemes using safe-prime groups Diffie-Hellman Group 14		NIST SP 800-56A Rev 3	Verification by known good impl.

Table 6-1 VOSS 8.3.100 Platforms Cryptography

The TSF supports RSA key generation scheme using cryptographic key size of 2048-bit that meet the FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3; standard. The RSA algorithm implementation is provided by the included Mocana cryptographic library. The TSF also supports ECDSA (appendix B.4) and FFC key generation (appendix B.1). RSA key pairs can be generated during the creation of a Certificate Signing Request (CSR). The TOE follows NIST SP 800-56A Rev 3 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' key agreement scheme. The TOE acts as a sender of secret keying material for RSA key establishment.

The following table outlines key establishment schemes used in the TOE:

Scheme	SFRs	Service
ECC key establishment	FCS_TLSC_EXT.1	Remote syslog Server Remote Administration
RSA key establishment	FCS_SSHS_EXT.1	Remote Administration
FFC key establishment	FCS_TLSC_EXT.1	Remote syslog Server
FFC Safe-primes key establishment	FCS_SSHS_EXT.1 (DH 14)	Remote Administration

Table 6-2 VOSS Key Establishment Schemes

TOE actively performs a destruction of keys and Critical Security Parameters (CSPs) when no longer required for use. The switches store several types of keys in volatile memory (RAM) in plaintext. The switches do not store any keys in plaintext form within user-accessible, non-volatile storage. The TOE supports short and long term storage of the following secret keys, private keys and CSPs:

Key or CSP	Cleared upon	Stored in	Cleared by
SSH host private key	Command	Flash	Overwriting with random data followed by zeros
SSH host public key	Command	Flash	Overwriting with random data followed by zeros
SSH session Encryption key	End of session	RAM	Overwriting once with zeros
SSH Session Integrity Key	End of session	RAM	Overwriting once with zeros
TLS host private key	Command	Flash	Overwriting with random data followed by zeros
TLS host digital certificate	Command	Flash	Overwriting with random data followed by zeros
TLS pre-master secret	Handshake done	RAM	Overwriting once with zeros
TLS session Encryption key	Close of session	RAM	Overwriting once with zeros
TLS session Integrity key	Close of session	RAM	Overwriting once with zeros
Account Passwords	Command	Flash	Overwriting with random data followed by zeros

Table 6-3 Cryptographic Keys and CSPs

Each plaintext key stored in volatile memory is associated with a protocol session. In each instance, after the session closes, the key is overwritten with the value “00” After the overwrite operation is complete, the TOE performs a specific "read-verify" operation to confirm that the storage space no longer contains the key.

When a key is deleted from FLASH, the previous value is overwritten with random data from the TSF RBG followed by a one pass of zeros.

The TOE uses SSH for to facilitate secure remote administrative sessions (CLI). The TOE's SSH implementation supports the following:

- Use of 2048-bit RSA keys in support of ssh-rsa, x509v3-ssh-rsa or x509v3-rsa2048-sha256 for public key-based authentication;
    - For x509v3-ssh-rsa or x509v3-rsa2048-sha256 for public key-based authentication the identity of the user must be specified in the certificate’s SubjectAltName: PrincipalName field;
    - For ssh-rsa public key authentication, the user must pre-load their public key into the TOE, before attempting to use their private key during an SSH authentication;
- Dropping SSH packets greater than 32768 bytes. This is accomplished by buffering all data for a particular SSH packet transmission until the buffer limit is reached and then dropping the packet;
- Strict compliance with RFCs 4251, 4252, 4253, 4254, and 4256
- No options included in the RFCs have been implemented;
- Encryption algorithms aes128-ctr, aes256-ctr, aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, and aes256-gcm@openssh.com to ensure confidentiality of the session;
- Password based authentication;
- Hashing algorithm hmac-sha1 and hmac-sha2-256 to ensure the integrity of the session (integrity is also provided implicitly by GCM when using aes128-gcm@openssh.com and aes256-gcm@openssh.com);
- Host public key algorithms use a 2048-bit RSA host key for ssh-rsa, or 2048-bit RSA certificates for x509v3-ssh-rsa and x509v3-rsa2048-sha256 authentication;
- TOE initiates a rekey before 1 hour or before 1GB whichever comes first.
- Enforcement of diffie-hellman-group14-sha1 as the only allowed key exchange method.

The TOE exclusively supports TLS v1.2 secure communication protocol that complies with RFC 5246 when acting as a TLS client. The TOE is a TLS client during communication with Remote syslog Servers.

The following ciphersuites are supported for communications with syslog servers:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ ECDHE_RSA_WITH_AES_256_CBC_SHA384

The TOE supports X509v3 certificates following format defined by RFC 5280 during TLS negotiations. The reference identifier configured on the TOE must be either a hostname/FQDN or an IPv4 address. As part of negotiating a TLS connection, the TOE will verify that peer certificate Subject Alternative Name (SAN) or Common Name (CN) contains expected identifier. The CN field in a certificate is checked only if a SAN Extension is absent from the certificate. The TOE only establishes connection if the peer certificate is valid, is trusted, has a matching reference identifier and has passed the revocation check.

The following identifiers are supported in CN: IPv4 address or a hostname. The following identifiers are supported in SAN: FQDN, IPv4 address. Wildcards are supported in the CN with a hostname or in the SAN with a FQDN identifier.

The specific identifier is configured as part of the external syslog configuration using the "syslog host" command. The "server -cert-name <identifier>" is used to configure the reference identifier. The connection is only accepted when the server from the configured IP address authenticates with a valid certificate containing matching identifier. The TOE does not support certificate pinning.

When the presented identifier in the CN is an IPv4 address, the TOE converts the string to a binary representation of an IPv4 address in network byte order. If there is not an exact binary match, then the verification fails. The TOE expects IPv4 identifier to follow RFC 3986 format, if any unexpected special characters or extra numbers are encountered, the verification fails.

The Cryptographic support function satisfies the following security functional requirements:

- NDcPP22e:FCS_CKM.1: The TOE supports asymmetric key generation using RSA, ECDSA and FFC key establishment as part of TLS and SSH as described in the section above. The TOE acts as a client for TLS (ECDSA, FFC) and a server for SSH (RSA, FFC (DH-14 key generation)). The TOE supports DH group 14 key establishment scheme that meets standard RFC 3526, section 3 for interoperability.
- NDcPP22e:FCS_CKM.2: FCS_CKM.2: See FCS_CKM.1.
- NDcPP22e:FCS_CKM.4: All data is cleared as identified above.
- NDcPP22e:FCS_COP.1/DataEncryption: The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (128 and 256 bit key sizes), AES in CTR mode (128 and 256 bit key sizes) as well as using AES in GCM mode (128 and 256 bit key sizes). AES is implemented in support of TLS and SSH protocols.
- NDcPP22e:FCS_COP.1/Hash: The TOE supports hashing using SHA-1, SHA-256, SHA384 and SHA-512 conforming to FIPS 180-4, Secure Hash Standard (SHS). SHS hashing is used within several services including, NTP hashing and SSH. SHA-256 is used in conjunction with RSA signatures for verification of software image integrity. The TOE also uses SHA-1, SHA-256, SHA-384 and SHA-512 hashing as part of RSA signature generation and verification services.
- NDcPP22e:FCS_COP.1/KeyedHash: The TOE supports keyed hash HMAC-SHA1 and HMAC-SHA256, conforming to ISO/IEC 9797-2:2011. Supported cryptographic key sizes: 160, 256 bits and message digest sizes: 160, 256 bits.
- NDcPP22e:FCS_COP.1/SigGen: The TOE supports generation and verification of RSA Digital Signature Algorithm with modulus of 2048 for cryptographic signature services.
- NDcPP22e:FCS_NTP_EXT.1: The TOE implements NTPv4 protocol to synchronize with an external time servers. The TOE authenticates updates using an administrator-configured SHA1 -based message authentication. The TOE does not synchronize based on broadcast and multicast time updates. The TOE supports configuration of multiple simultaneous time servers and follows RFC 5905 algorithm to prioritize them.
- NDcPP22e:FCS_RBG_EXT.1: The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), in accordance with ISO/IEC 18031:2011. The TOE implements a random bit generator in support of various cryptographic operations, including, RSA key establishment schemes, Diff-Hellman key establishment schemes, TLS session establishment, SSH session establishment. The entropy source used to seed the Deterministic Random Bit Generator is a random set of bits or bytes that are regularly supplied to the DRBG by polling software sources in threads. All random number generation functionality is continuously health tested as per the tests defined in section 11.3 of SP 900-90A. Any initialization or system errors during bring-up or processing of this system causes a reboot resulting in the DRBG being reseeded.
- NDcPP22e:FCS_SSHS_EXT.1: The TOE supports SSHv2 as described above for CLI management.

- NDcPP22e:FCS_TLSC_EXT.1: The TOE supports TLS v1.2 with the ciphersuites listed above for its syslog connections. The TOE offers secp256r1, secp384r1, secp521r1 as supported groups for ECDHE cipher suites when acting as a TLS client.

6.3 Identification and authentication

The administrator can configure the maximum number of failed attempts using the CLI interface. The configurable range is between 1 and 255 attempts. When a user account has exceeded maximum number of unsuccessful authentication attempts it will be locked. The host that the user was connecting from, is also locked out, but that host is automatically unlocked base on a timer. The user account remains locked out till the admin unlocks the user's account using a CLI command. The account lockout feature is not enforced on logins occurring at the local console for the "Privilege" account. This account is allowed to login only at the console, and can unlock other accounts, thus ensuring that a system cannot get into a situation where no administrator access is available.

The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Administrative access to the TOE is facilitated through one of several interfaces,

- Directly connecting to the TOE
- Remotely connecting via SSHv2

Regardless of the interface at which the administrator interacts, the TOE will enforce username and authentication credentials to be presented. Authentication credentials may be a password or public-key at either the local console or via an SSHv2 protected session. The TOE also accepts an X.509v3 certificate as a valid authentication credential over an SSHv2 protected session. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated.

The TOE provides a local password-based authentication mechanism. The process for authentication is the same for administrative access whether administration is occurring via direct connection or remotely. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.

The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: '!', '@', '#', '$', '%', '^', '&', '*', '(', and ')'. The minimum password length is configurable by the Authorized Administrator. When the TOE is in the evaluated configuration, the minimum password length configured by an administrator to a value between 8 and 32 characters (default is 15).

Administrators configure a certificate for each service (i.e., syslog, ssh x509v3 authentication) and those certificates are used by the TOE service for authentication. The administrator is expected to configure the operating environment such that devices in the operating environment and the TOE use accurate time (to support validity check and OCSP response validity periods). The administrator must also ensure that the certificates loaded into the TOE as trusted roots are those that are also accepted by network peers.

The TOE performs X.509v3 certificate validation according to RFC 5280 for the following purposes:

- As a TLS client the TOE validates the certificate presented during the TLS negotiation with the syslog server.
- As an SSH server, the TOE validates the certificate presented by an administrative user during the establishment of an SSH protected session offering the admin CLI.
- When certificates are loaded into the TOE, the imported certificates are validated.

In all of the above scenarios, X.509 certificates validation process includes:

- Certificate expiry date check
- Certificate path (continuity of the certificate chain) validation up to the trusted CA

- Certificate revocation check
- Public key, key algorithm, and parameters check
- Check of certificate issuer
- Process certificate extensions

The TOE requires the certificate presented by the syslog server to include the ServerAuth EKU, and CA certificates to include the BasicConstraints flag as true. Certificates presented by an administrator to the TOE SSH server must include the user identity (i.e., username@domain.com) as a PrincipalName in the SubjectAltName extension.

In a TLS exchange, revocation checking is completed before any encrypted application data is transferred. In an SSH authentication, revocation checking is completed before the SSH session is fully established and before the CLI is offered. The only exception being when the revocation server cannot be contacted, the revocation check is skipped and the validity of the certificate is based on all other checks.

The TOE generates keys and creates Certificate Signing Requests (CSR) with the following fields:

- Common Name
- Organization
- Organizational Unit
- Country

The TOE does not support "device specific information" within the Certificate Request Message.

The Identification and authentication function satisfies the following security functional requirements:

- NDcPP22e:FIA_AFL.1: The administrator can set a maximum remote login failure number. If that is exceeded, the account is locked until the account is manually unlocked by an administrator using a CLI command.
- NDcPP22e:FIA_PMG_EXT.1: The TOE implements a rich set of password composition constraints as described above.
- NDcPP22e:FIA_UAU.7: For a local administrative session, password character entries are not echoed to the screen. For a remote administrative session, credentials are protected by a secure channel.
- NDcPP22e:FIA_UAU_EXT.2: The TOE uses local password-based authentication, SSH public key, and SSH X.509 certificates to login authorized administrative users remotely and locally.
- NDcPP22e:FIA_UIA_EXT.1: The TOE does not offer any services or access to its functions, except for the displaying a message of the day banner, without requiring a user to be identified and authenticated.
- NDcPP22e:FIA_X509_EXT.1/Rev: OCSP is supported for X509v3 certificate validation for TLS and SSH. Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE.
- NDcPP22e:FIA_X509_EXT.2: Certificates are checked and if found not valid are not accepted. When the TOE determines a certificate to be valid and the necessary OCSP server cannot be contacted for a revocation check, then that certificate is not accepted as part of an SSH session negotiation, but the certificates are accepted as part of a TLS session negotiation. This is true for TLS connections to a syslog server and administrator logins using x509v3 certificates via SSH.
- NDcPP22e:FIA_X509_EXT.3: The TOE generates certificate requests and validates the CA used to sign the certificates. In order to verify the revocation status of the presented certificates Online Certificate Status Protocol (OCSP) is used. If the connection to determine the certificate validity cannot be established, the TOE accepts the certificate. Upon import the TOE verifies that the certificate being imported chains to a Trusted root CA.

6.4 Security management

The TOE is securely managed via the CLI which is available through a local console or over an SSHv2 protected session. The CLI offers command line functions which allow administrators to configure the TOE. These command line functions can be used to effectively manage every security policy (supporting all requirements), as well as the non-security relevant aspects of the TOE.

The specific management capabilities defined in this ST include:

- 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 prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [Ability to modify the behavior of the transmission of audit data to an external IT entity,
- Ability to manage the cryptographic keys,
- Ability to configure the cryptographic functionality,
- Ability to re-enable an Administrator account,
- Ability to configure thresholds for SSH rekeying
- Ability to set the time which is used for time-stamps,
- Ability to configure NTP,
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors,
- Ability to import X509v3 certificates to the TOE's trust store, and
- Ability to manage the trusted public keys database.

Management functions are exclusively restricted to Security Administrators with corresponding privileges. The term “Security Administrator” used in the ST refers to any user that has a role that has been assigned any of the privileges allowing to perform any of the management functions. Not every administrator would necessarily have sufficient privileges to access each administrative function.

The TOE supports multiple administrative roles when accessing the administrative interface through the local or remote CLI. These roles define the access that is allowed per role. The following list identifies the configuration capabilities assigned to each role.

- User EXEC Mode: Initial mode of access.
- Privileged EXEC Mode: User mode and password combination determines access level.
- Global Configuration Mode: Use this mode to make changes to the running configuration.
- Interface Configuration Mode: Use this mode to modify or configure logical interface, VLAN or a physical interface.
- Router Configuration Mode: Use this mode to modify a protocol.
- Application Configuration Mode: Use this mode to access the applications.

The following table lists the keys the Security Administrator is able to manage and includes the operations that are available to the Security Administrator that can be performed on those keys. These operations are available to the Security Administrator through commands on the CLI.

Key	Administrator CLI Operations
SSH host private key	Generate, Delete
SSH host public key	Generate, Delete
CA certificate	Import, Delete
TOE private key	Generate, Delete
TOE digital certificate	Generate, Delete

Table 6-4 Administrator Manageable Security Keys

The Security management function satisfies the following security functional requirements:

- NDcPP22e:FMT_MOF.1/ManualUpdate: The TOE does not provide automatic updates to the software version running on the TOE. The Security Administrators can query the software version running on the TOE and can manually initiate updates. The software update consists of installing the new image into primary partition and rebooting the device.
- NDcPP22e:FMT_MTD.1/CoreData: Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. Security management is restricted to administrators. The trust store is accessed when administrators import/remove certificates as described in the Admin Guide. The trust store is protected by default and is restricted such that only administrators have access.
- NDcPP22e:FMT_MTD.1/CryptoKeys: Only administrators can perform management operations including the command to generate and delete cryptographic keys. Administrators can also import and delete CA certificates and their keys into the trust store. All of these administrative actions on keys are described by the Admin Guide.
- NDcPP22e:FMT_SMF.1: The TOE provides administrative interfaces to perform the functions identified above.
- NDcPP22e:FMT_SMR.2: The TOE supports multiple administrative roles when accessing the administrative interface through the local or remote CLI. These roles define the access that is allowed per role. All roles are considered authorized administrators.

6.5 Protection of the TSF

The TOE is designed with a set of self-protection mechanisms. All passwords, and keys stored on the TOE are protected from unauthorized modification and disclosure. The TOE stores symmetric keys only in volatile memory never on persistent media. The TOE admin interface does not provide any mechanism to view or directly modify passwords, symmetric keys, or private keys. Only authorized administrators with sufficient privileges can perform operations on such sensitive data using CLI commands.

The TOE encrypts and stores all private keys in a secure directory that is not readily accessible to administrators; therefore, there is no administrative interface access provided to directly manipulate the keys.

The TOE runs a suite of self-tests during initial start-up to verify its correct operation. If any of the tests fail one of the following will happen: the TOE will enter into an error state until an Administrator intervenes or the TOE will automatically reboot and re-run all the tests. During initialization and self-test execution, the module inhibits all access to the cryptographic algorithms. Additionally, the power-on self-tests are performed after the cryptographic systems are initialized but prior to the underlying OS initialization of external interfaces; this prevents the security appliances from passing any data before completing self-tests. In the event of a power-on self-test failure, the cryptographic module will force the platform to reload and reinitialize the operating system and cryptographic components. This operation ensures no cryptographic algorithms can be accessed unless all power on self-tests are successful. By ensuring that cryptographic operations are accurate and that the TOE software image is unmodified, these self-tests are sufficient to demonstrate the TSF operates as correctly.

These tests include:

- AES Known Answer Test - For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly.
- HMAC Known Answer Test - For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly.
- PRNG/DRBG Known Answer Test - For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly.
- SHA Known Answer Test – For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match and the hash operations are operating correctly.
- RSA Signature Known Answer Test (both signature/verification) - This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly.
- Software Integrity Test - This test is run automatically whenever the system images is loaded and confirms through use of digital signature verification that the image file that's about to be loaded was properly signed and maintained its integrity since being signed. The system image is digitally signed prior to being made available for download from Extreme.

The Authorized Administrator can query the software version running on the TOE, and can initiate updates to software images. When software updates are made available, an administrator can obtain, verify the integrity of via digital signature, and install those updates. The updates can be downloaded from https://support.extremenetworks.com. The TOE image files are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded. The public keys used by the update verification mechanism are contained on the TOE. The TOE compares the update files' signature using a certificate that comes pre-loaded on the device and is stored in the trust store. As part of the build process, the update image is signed with the Extreme private key. This is done using an RSA 2048/SHA-256 digital signature. Only if the signature/hash is correct, will the image be installed. If an update is unsuccessful, a warning is displayed to the administrator. Since the update process attempts to update a different partition than what is currently being run, the current active image remains the same until the reboot. The reboot prompt is offered as part of the update process.

The clock function is reliant on the system clock provided by the underlying hardware. The TOE can be configured to synchronize its internal clock with an NTP server. The date and time are used as the time stamp that is applied to TOE generated audit records, used to track inactivity of administrative sessions, and perform certificate expiration checks.

The Protection of the TSF function satisfies the following security functional requirements:

- NDcPP22e:FPT_APW_EXT.1: Passwords are the only authentication data that is subject to this SFR. No passwords are ever stored as clear text. The TOE does not offer any functions that will disclose to any user a plain text password. Passwords are stored on the TOE in a secured partition in non-plaintext. Prior to writing on disks each password is hashed (SHA-256) with a salt. During subsequent authentication attempts passwords are similarly processed and compared in cyphertext (i.e., hash comparison).

- NDcPP22e:FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- NDcPP22e:FPT_STM_EXT.1: The TOE includes its own hardware clock and can synchronize with a NTP server.
- NDcPP22e: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 are described above.
- NDcPP22e: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 provides the administrative user with an ability to configure inactivity time out periods for administrative sessions. The inactivity period for CLI (local and remote) administrative access is configured separately through the TOE administrative interfaces. When the administrative interface has been idle for more than the configured period of time the session is terminated. After termination, administrative authentication is required to access any of the administrative functionality of the TOE. This is applicable from both local and remote administrative sessions.

The local console CLI and remote SSH CLI can be configured to display a custom login banner. This banner will be displayed prior to allowing Administrator access through either interface.

The TOE access function satisfies the following security functional requirements:

- NDcPP22e:FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- NDcPP22e:FTA_SSL.4: The TOE provides the function to logout (or terminate) both local and remote user sessions as directed by the user.
- NDcPP22e:FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.
- NDcPP22e: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 protects trusted channels with audit servers (syslog servers) using the TLS v1.2 protocol. The TOE is a TLS client in the communications with the audit servers. The TOE provides assured identification of the non-TSF endpoint by validating X.509 certificates. The TOE implements a trust store containing trust anchors which it uses to verify identities of those non-TSF certificates. The TOE utilizes TLS as described in Section 6.2 above.

All remote administrative CLI sessions are protected with an SSHv2 tunnel that provides a secure encrypted session. The SSHv2 session is encrypted using AES encryption. The remote administrators is able to initiate the SSHv2 secure channel to the TOE. Note that local administrator access via the serial port is also allowed for CLI access.

The Trusted path/channels function satisfies the following security functional requirements:

- NDcPP22e: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 syslog server and against the TOE configuration using the certificates presented during TLS negotiation.
- NDcPP22e:FTP_TRP.1/Admin: The TOE provides SSH to ensure secure remote administration. The administrator can initiate the remote SSH session, the remote SSH session is secured from disclosure and modification using CAVP tested cryptographic operations.