Dell Networking Platforms
Security Target

Version 1.3

June 8, 2017

Table of Contents

Figures and Tables

1 Security Target Introduction

1.1 Security Target Reference

ST Title: Dell Networking Platforms Security Target

ST Version: v1.3

ST Author: CygnaCom Solutions Inc.

ST Date: 6/8/2017

1.2 TOE Reference

TOE Developer: Dell USA L.P.

Evaluation Sponsor: Dell USA L.P.

TOE Identification: Dell Networking Platforms running Dell Networking OS v9.11

Table 1: TOE Platforms and Devices

Series	Platforms	Build
Dell Networking S-Series Top-of-rack switches	S3124*	9.11.0.P9
	S3148*	
	S3048-ON	
	S4048-ON*	
	S5000	
	S6010-ON	
	S6100-ON	
Dell Networking C-Series Network director and modular switch	C9010	
Dell Networking Z-Series Top-of-rack switch	Z9100-ON	

** These platforms include multiple appliances*

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

PP Identification: collaborative Protection Profile for Network Devices, Version 1.0, February 2015.

1.3 TOE Overview

1.3.1 *TOE Product Type*

The Target of Evaluation [TOE] is a Network Device as defined by the *collaborative Protection Profile for Network Devices v1.0* [NDcPP]: "*A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network".*

1.3.2 *TOE Usage*

The TOE is the Dell Networking Platforms running Dell Networking OS v9.11 that in the evaluated configuration consists of S-Series, C-Series, and Z-Series switches. The TOE provides layer 2 and 3 network management and interconnectivity functionality by offering non-blocking, line-rate Ethernet switching with Quality of Service (QoS) and a full complement of IPv4 and IPv6 features. TOE consists of a hardware appliance with embedded software components.

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 production environment as specified in the user guidance.

1.3.3 *TOE Security Functionality*

- Security Audit
  - Audit record generation for security-relevant events
  - Interoperability with a remote audit server
- Cryptographic Support
  - Validated cryptographic algorithms
  - Destruction of cryptographic keys
- Identification and Authentication
  - User access policies
  - Password and certificate based authentication
- Security Management
  - Local and remote administration
- Protection of the TOE Security Function (TSF)
  - Self-testing on power-up
  - Trusted update
- TOE Access
  - Role-based access control
  - Session timeout and lockout
- Trusted Path/Channels
  - Secure channel for remote administrators
  - Secure channel for authorized IT entities

1.4 TOE Description

The TOE is the Dell Networking Platforms running Dell Networking OS v9.11 that consist of S-Series, C-Series, and Z-Series switches and includes the following appliances:

- Dell Networking S-Series S3124
- Dell Networking S-Series S3124P
- Dell Networking S-Series S3124F
- Dell Networking S-Series S3148
- Dell Networking S-Series S3148P
- Dell Networking S-Series S3048-ON
- Dell Networking S-Series S4048-ON
- Dell Networking S-Series S4048T-ON
- Dell Networking S-Series S5000
- Dell Networking S-Series S6010-ON
- Dell Networking S-Series S6100-ON
- Dell Networking C-Series C9010 and C1048P port extender
- Dell Networking Z-Series Z9100-ON

The TOE consists of both hardware and software components. Each software version is identifiable by the unique build number. Each hardware profile provides a defined set of performance characteristics - switching bandwidth, latency, and port density while offering the same level of security features.

Dell Networking S3100 series
The Dell Networking S3100 series is a power-efficient 1/10GbE top-of-rack switches purpose-built for office and campus networks. S3124, S3124P, S3124F switches feature a data rate up to 212Gbps (full duplex) and a forwarding rate up to 158Mpps; S3148 and S3148P support data rate up to 260Gbps and a forwarding rate up to 193Mpps. These switches deliver line-rate switching with Priority-based Flow Control (PFC), Enhance Transmission Selection (ETS), and network virtualization features such as VRF-lite. The port and power configuration for individual models listed below:

- S3124 offers 24x RJ45 10/100/1000Mb auto-sensing ports, 2x SFP+ ports, 2x GbE combo media ports, and 200W PSU
- S3124F offers 24x 1000-SX (up to 500m distance) or 1000-LX (up to 10km distance) SFP GbE ports, 2x SFP+ ports, 2x GbE combo media ports, and 200W PSU
- S3124P offers 24x RJ45 10/100/1000Mb PoE+ (up to 30.8W) auto- sensing ports, 2x SFP+ ports, 2x GbE combo media ports, and 715W PSU
- S3148 offers 48x RJ45 10/100/1000Mb auto-sensing ports, 2x SFP+ ports, 2x GbE combo media ports, and 200W PSU
- S3148P: 48x RJ45 10/100/1000Mb PoE+ (up to 30.8W) auto- sensing ports, 2x SFP+ ports, 2x GbE combo media ports, and 1100W PSU

Dell Networking S3048-ON

The Dell Networking S3048-ON is a top-of-rack switch built for high-performance, software-defined data centers. The S3048-ON 1U design provides 48 line-rate 1000BASE-T ports that support 10MB/100MB/1GB and four line-rate 10GbE SFP+ ports. The S3048-ON features non-blocking switching architecture that supports up to 260GBps (full-duplex) data rate and up to 131Mpps forwarding rate and enables VRT-lite sharing of networking infrastructure and provides L3 traffic isolation across tenants, including support for multicast and IPv6 routing.

Dell Networking S4000 Series

The Dell Networking S4000 series is an ultra-low-latency 10/40GbE top-of-rack switches built for data center applications. S4000 switches offer data rate up to 1.44Tbps and a forwarding rate up to1080Mpps. The S4048-ON 1U design provides 8 x 10GbE SFP+ ports or 72 10GbE ports with breakout cables and 6 x 40GbE QSFP+ ports. The S4048T-ON provides 48 x 10GBaseT ports plus 24 10GbE ports with breakout cables and 6 x 40GbE QSFP+ ports. The S4000 series supports network virtualization by implementing both network centric virtualization method (VRF-lite) and hypervisor centric virtualization method (VXLAN).

Dell Networking S5000

The Dell Networking S-Series S5000 is a top-of-rack switch purpose-built for LAN and SAN convergence applications in data center environments. The S5000 1U form factor offers modular design with 4 fixed 40GbE QSFP+ uplink ports and 4 modular bays. The S5000 can supports up to 4 12-port 10GbE SFP+ modules, but no more than one 12-port 2/4/8Gbps Fibre Channel (FC) module. The S5000 features 1.28Tbps (full-duplex) and a forwarding rate up to 960Mpps non-blocking switching fabric delivering line-rate performance and supports DCBx, Internet Small Computer System Interface (iSCSI), RDMA over converged Ethernet (RoCE) protocols.

Dell Networking S6010-ON

The Dell Networking S-Series S6010-ON is a top-of-rack switch purpose-built for applications in high-performance data center and computing environments. The S6010-ON 1U design provides 32 40GbE QSFP+ uplinks. The S6000 features 2.56Tbps (full-duplex) non-blocking, cut-through switching fabric and delivers line-rate switching with QoS, VLT, DCBX and iSCSI TLV support.

Dell Networking S6100-ON

The Dell Networking S-Series S6100-ON is a top-of-rack modular switch purpose-built for applications in high-performance data center and computing environments. The S6100-ON 2U design provides up to 32 100G QSFP+ uplinks and two fixed 10GbE SFP+ ports. The S6100-ON features 2.56Tbps (full-duplex) non-blocking, cut-through switching fabric and delivers line-rate switching with PFC, DCBX, and ETS support.

Dell Networking Z9100-ON

The Dell Networking Z-Series Z9100-ON is a 1U top-of-rack core switch purpose-built for applications in high-performance data centers. The Z9100-ON offers high-density 32 ports of 100GbE and two SFP+. The Z9100-ON features 6.4Tbps (full-duplex) non-blocking, cut-through switching fabric and implements priority-based flow control (PFC), data center bridge exchange (DCBX), and enhanced transmission selection (ETS).

Dell Networking C9010

The Dell Networking C-Series C9010 network director and optional C1048P rapid access node is a network device designed to simplify deployment and management of core switches by collapsing separate network tiers into a single logical switching tier and eliminating complexity of protocols running between access and core/aggregation tiers. The C9010 8U platform supports modular slots for up to 10 line card modules, two route processor modules, three fan modules, and four power supply modules supporting up to 60 line-rate 40GbE QSFP+ ports. Each C1048P node supports up to 48-port 1GbE PoE+ ports.

1.4.1 *TOE Architecture*

The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, and processor and software that implements routing and switching functions, configuration information and drivers. While hardware varies between different appliance models, the software (Dell EMC Networking OS v9.11) is shared across all platforms.

Dell EMC Networking OS v9.11 is composed of subsystems designed to implement operational, security, management, and networking functions. Hardware-specific device drivers that reside in the kernel provide abstraction of the hardware components. Dedicated cryptographic module is integrated with protocol libraries that implement secure channel functionality. Control plane subsystem that includes Internet Protocol (IP) host stack, which can be further subdivided into protocol and control layers, implements switching and routing functions. System management subsystem, that includes an Authentication, Authorization and Accounting (AAA) module, implements administrative interface and maintains configuration information.

The figure below outlines the TOE Architecture and subsystem interactions:

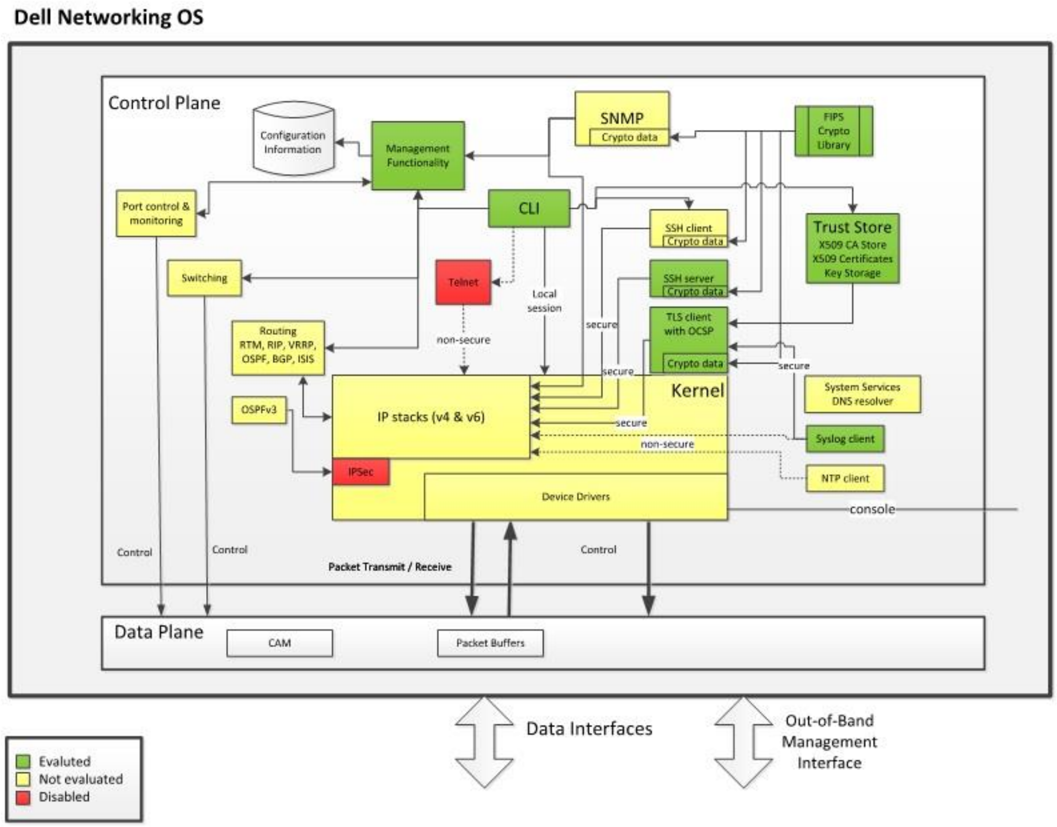

Figure 1: TOE Architecture

1.4.2 *TOE Components*

1.4.2.1 Hardware

The TOE consists of the following hardware:

Table 2: Dell networking appliances

Platform	Model	Processor	Form	Specs
Dell Networking S-Series Switches	S3124	ARM Cortex A9	1U	24 x 1000BASE-T
	S3124P	ARM Cortex A9	1U	24 x 1000BASE-T PoE+
	S3124F	ARM Cortex A9	1U	24 x 1GbE SFP
	S3148	ARM Cortex A9	1U	48 x 1000BASE-T
	S3148P	ARM Cortex A9	1U	48 x 1000BASE-T PoE+
	S3048-ON	Intel Atom	1U	48 x 100BASE-T 4 x 1-GbE SFP+
	S4048-ON	Intel Atom	1U	48 x 10GbE SFP+ 6 x 40GbE QSFP+
	S4048T-ON	Intel Atom	1U	48 x 10GBASE-T 6 x 40GbE QSFP+
	S5000	FreeScale PowerPC e500	1U	4x40GbE QSFP+ 4 module bays with: 12 x 1/10G SFP+ or 12 x 2/4/8Gbps FC modules
	S6010-ON	Intel Atom	1U	32x 40GbE QSFP+
	S6100-ON	Intel Atom	2U	2 x 10GbE SFP+ 4 module bays with: 16 x QSFP+ 40GbE Or 8 x QSFP28 100GbE
Dell Networking C-Series Switches	C9010	Intel Atom	8U	10 module bays with: 24-port 10GbE 10GBASE-T Line Card or 24-port 10GbE SFP+ Line Card or 6-port 40GbE QSFP+ Line Card Or
Dell Networking Z-Series Switches	Z9100-ON	Intel Atom	1U	32 x 100GbE QSFP28

1.4.2.2 Software

The TOE runs pre-installed Dell EMC Networking OS v9.11. This software utilizes a common code base of a modular nature with only the modules applicable to the specific hardware profile initialized on any given hardware appliance.

The software, Dell EMC Networking OS v9.11, consists of Dell Operating System and Dell Application Software. Dell Application Software implements a common code base of a modular nature with only the modules applicable to the specific hardware loaded. Dell Operating System and Dell Application Software are assigned a combined uniquely identifiable build number and are not available separately. Each software build is produced from the same code base and compiled into binary for the specific hardware architecture.

1.4.2.3 Management Interface(s)

The Dell EMC Networking OS v9.11 is configured and managed via a text-based Command Line Interface (CLI). The CLI is accessible from a directly- connected terminal or remotely using SSH. The CLI is structured into different operating modes for security and management purposes. Different sets of commands are available in each mode, and it is possible to limit access to specific commands using permissions.

1.4.3 *Physical Boundary of the TOE*

The physical boundary of the TOE includes:

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

The Operational Environment of the TOE includes:

- The SSH client that is used to remotely access the management interface
- The management workstation that hosts the SSH client
- External IT servers:
  - Audit server for external storage of audit records
  - NTP server for synchronizing system time (optional)
  - Certificate Authority and OCSP servers to support X.509 (optional)

The TOE Boundary is outlined in the following figure:

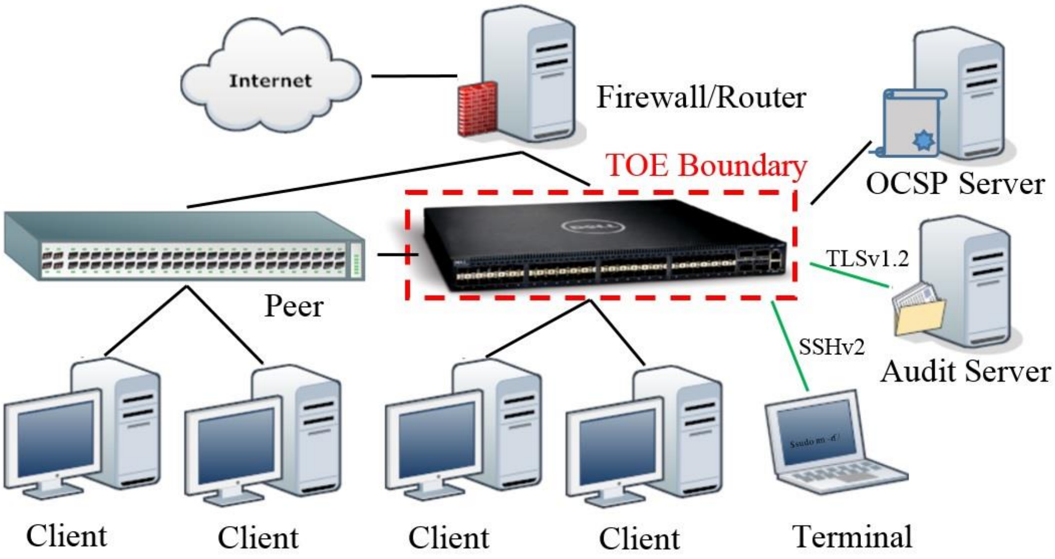

Figure 2**: TOE Boundary**

1.4.4 *Logical Boundary of the TOE*

The logical boundary of the TOE is defined by implemented security functionality as summarized in the Section 1.3.3 of this document.

1.4.4.1 Security Audit

The TOE generates audit records for all security-relevant events. For each event, the TOE records the date and time, the type of event, the subject identity, and the outcome of the event logged. The resulting records can be stored locally or securely sent to a designated audit server for archiving. Security Administrators using the appropriate CLI commands can also view audit records locally. The TOE also implements timestamps to ensure reliable audit information produced.

1.4.4.2 Cryptographic Support

The TOE performs the following cryptographic functionality:

- Encryption, decryption, hashing, keyed-hash message authentication, random number generation, signature generation and verification utilizing dedicated cryptographic library
- Cryptographic functionality is utilized to implement secure channels
  - SSLv2
  - TLSv1.2
- Entropy is collected and used to support seeding with full entropy

- Critical Security Parameters (CSPs) internally stored and cleared when no longer in use
- X509 Certificate authentication integrated with TLS protocol

The TOE uses a dedicated cryptographic module to manage CSPs and implements deletion procedures to mitigate the possibility of disclosure or modification of CSPs. Additionally, the TOE provides commands to on-demand clear CSPs (e.g. host RSA keys), that can be invoked by a Security Administrator with appropriate permissions.

1.4.4.3 Identification and Authentication

The TOE supports Role-Based Access Control (RBAC) managed by an AAA module that stores and manages permissions of all users and their roles. Before any other action, each user is identified with a login name and authenticated with a password. Each authorized user is associated with assigned role and specific permissions that determine access to TOE features. The AAA module stores the assigned role of each user along with all other information required that user to access the TOE.

1.4.4.4 Security Management

The TOE allows remote administration using an SSHv2 session over an out of band LAN management RJ-45 port and local administration using a console via a separate RJ-45 running RS-232 signaling/USB port. Both remote and local administration conducted over command-line interface (CLI) terminal that facilitates access to all management functions used to administer the TOE.

All of the management functions are restricted to the Security Administrators of the TOE. Security Administrators can perform the following actions: manage user accounts and roles, reboot and apply software updates, administer system configuration, and review the audit records.

The term “Security Administrator” is used to refer to any administrative user with the appropriate role to perform the relevant functions.

1.4.4.5 Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features.

The TOE protects CSPs, including stored passwords and cryptographic keys, so they are not directly viewable in plaintext. The TOE also ensures that reliable time information is available for both log accountability and synchronization with the operating environment.

The TOE employs both dedicated communication channels as well as cryptographic means to protect communication between itself and other components in the operational environment.

The TOE performs self-tests to detect internal failures and protect itself from malicious updates.

1.4.4.6 TOE Access

The TOE will display a customizable banner when an administrator initiates an interactive local or remote session. The TOE also enforces an administrator-defined inactivity timeout after which the inactive session is automatically terminated. Once a session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

1.4.4.7 Trusted Path/Channels

The TOE protects remote sessions by establishing a trusted path secured using SSH between itself and the administrator. The TOE prevents disclosure or modification of audit records by establishing a trusted channel using TLS between itself and the audit server.

1.4.5 *Excluded Functionality*

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:

- Any integration and/or communication with authentication servers such as Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control Systems (TACACS) is excluded from the evaluated configuration.
- Any use of HTTP and HTTPS (web interface) or OpenManage Network Manager (ONM) is excluded and are disabled in the evaluated configuration.
- Routing protocols that integrate authentication or encryption such as Routing Information Protocol (RIPv1, RIPv2), Open Shortest Path First (OSPFv2), Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), and Virtual Router Redundancy Protocol (VRRP) are not evaluated. RFC-compliant implementations are unable to satisfy cryptographic requirements outlined in the PP.
- Use of the FTP server is excluded and it is disabled by default.
- Use of the SNMP management functionality is excluded and it is disabled by default. The use of SNMPv3 for monitoring is not restricted; however, it is not evaluated.
- Synchronization with an external NTP server is not restricted; however, this functionality is not evaluated.
- Reverse SSH tunnel with syslog is excluded from the evaluated configuration.

1.4.6 *TOE Guidance and Reference Documents*

The following user guidance documents are provided to customers and are considered part of the TOE:

Table 3: TOE Reference Documents

Reference Title	ID
Dell Networking OS Configuration Guide for the Z9100-ON System 9.11(0.0) Dell Networking OS Configuration Guide for the C9000 System 9.11(0.0) Dell Networking OS Configuration Guide for the S3048-ON System 9.11(0.0 Dell Configuration Guide for the S4048-ON System 9.11(0.0) Dell Configuration Guide for the S3100-ON System 9.11(0.0) Dell 9.11(0.0) Configuration Guide for the S5000 Switch Dell Configuration Guide for the S6000 System 9.11(0.0)	[ADMIN]

Reference Title	ID
Dell Configuration Guide for the S6010-ON System 9.11(0.0) Dell Configuration Guide for the S6100-ON System 9.11(0.0)	
Dell Networking Command Line Reference Guide for the Z9100-ON System 9.11(0.0) Dell Networking Command Line Reference Guide for the C9000 System 9.11(0.0) Dell Networking Command Line Reference Guide for the S3048-ON System 9.11(0.0) Dell Command Line Reference Guide for the S4048-ON System 9.11(0.0) Dell Command Line Reference Guide for the S3100-ON System 9.11(0.0) Dell 9.11(0.0) Command Line Reference Guide for the S5000 Switch Dell Command Line Reference Guide for the S6000 System 9.11(0.0) Dell Command Line Reference Guide for the S6010-ON System 9.11(0.0) Dell Command Line Reference Guide for the S6100-ON System 9.11(0.0)	[REF]
Configuration for Common Criteria NDcPP v1.0 Evaluated Dell Networking OS 9.11(0.0P9)	[CC Addendum]

The documents in the following table were used as reference materials to develop this ST.

Table 4: ST Reference Documents

Reference Title	ID
Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002	[CC]
collaborative Protection Profile for Network Devices, Version 1.0, February 2015	[NDcPP]

2 Conformance Claims

2.1 Common Criteria Conformance Claim

This Security Target [ST] and the Target of Evaluation [TOE] are conformant to the following Common Criteria [CC] specifications:

- *Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components,* Version 3.1, Revision 4, September 2012, CCMB-2012-09-002
  - Part 2 Conformant with additional extended functional components as specified by the protection profile.
- *Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components,* Version 3.1, Revision 4, September 2012, CCMB-2012-09-003
  - Part 3 Conformant with additional assurance activities as specified by the protection profile.

2.2 Protection Profile Claim

The TOE claims *exact* compliance to *collaborative Protection Profile for Network Devices, Version 1.0, February 2015* [NDcPP].

2.2.1 *Technical Decisions*

The following CCEVS technical decisions applied to this evaluation:

- TD0167: NIT Technical Decision for Testing SSH 2^28 packets
- TD0165: NIT Technical Decision for Sending the ServerKeyExchange message when using RSA
- TD0164: NIT Technical Decision for Negative testing for additional ciphers for SSH
- TD0152: NIT Technical Decision for Reference identifiers for TLS in the NDcPP v1.0 and FW cPP v1.0
- TD0150: NIT Technical Decision for Removal of SSH re-key audit events in the NDcPP v1.0 and FW cPP v1.0
- TD0143 - NIT Technical Decision for Failure testing for TLS session establishment in NDcPP and FWcPP
- TD0130- NIT Technical Decision for Requirements for Destruction of Cryptographic Keys
- TD0126 - NIT Technical Decision for TLS Mutual Authentication
  - Note: FCS_TLSC_EXT.2 is still claimed in this ST as the TOE supports mutual authentication over TLS.
- TD0117 - NIT Technical Decision for FIA_X509_EXT.1.1 Requirement in NDcPP
- TD0116 - NIT Technical Decision for a Typo in reference to RSASSA-PKCS1v1_5 in NDcPP and FWcPP

- TD0112 - NIT Technical Decision for TLS testing in the NDcPP v1.0 and FW cPP v1.0.
- TD0094 - NIT Technical Decision for validating a published hash in NDcPP
- TD0093 - NIT Technical Decision for FIA_X509_EXT.1.1 Requirement in NDcPP
- TD0090 - NIT Technical Decision for FMT_SMF.1.1 Requirement in NDcPP

2.3 Package Claim

The TOE does not claim to be conformant with any pre-defined packages.

2.4 Conformance Rationale

This Security Target claims strict conformance to only one PP – the NDcPP and no extended packages.

The Security Problem Definition (SPD) of this ST is consistent with the statement of the SPD in the PP, as the ST claims *exact* conformance to the PP and no other threats, organizational security policies, or assumptions are added.

The security objectives of this ST are consistent with the statement of the security objectives in the PP as the ST claims *exact* conformance to the PP and no other security objectives are added.

The security requirements of this ST are consistent with the statement of the security requirements in the PP as the ST claims *exact* conformance to the PP.

3 Security Problem Definition

3.1 Threats

This section identifies the threats applicable to the TOE as specified in the PP.

Table 5: TOE Threats

Threat Name	Threat Definition
Communications with the Network Device	
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

Threat Name	Threat Definition
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
Valid Updates	
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
Audited Activity	
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
Administrator and Device Credentials and Data	
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.

Threat Name	Threat Definition
Device Failure	
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

3.2 Assumptions

This section identifies assumptions applicable to the TOE as specified in the PP.

Table 6: TOE Assumptions

Assumption Name	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall).

Assumption Name	Assumption Definition
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator’s credentials (private key) used to access the network device are protected by the platform on which they reside.

3.3 Organizational Security Policies

This section identifies the organizational security policies applicable to the TOE as specified in the PP.

Table 7: Organizational Security Policies

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

4 Security Objectives

This section defines the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its supporting environment in meeting the security needs.

4.1 Security Objectives for the TOE

The collaborative Protection Profile for Network Devices v1.0 does not define any security objectives for the TOE.

4.2 Security Objectives for the Operational Environment

This section identifies the security objectives as applicable to the operational environment as specified in the PP. These objectives

Table 8: Security Objectives for the Operational Environment

Objective Name	Environmental Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIAL_SECURE	The administrator’s credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

5 Extended Components Definition

The extended components listed in the Table 9 have been sourced from *collaborative Protection Profile for Network Devices, Version 1.0, February 2015* [NDcPP].

The extended components, as defined in Section 8.3 of *Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 4*, are identified by "_EXT" in the component name. NDcPP Appendix C contains the definitions for all extended components.

5.1 Extended Security Functional Components

Table 9: Extended Components

Functional Component		
1	FAU_STG_EXT.1	Protected Audit Event Storage
2	FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
3	FCS_SSHS_EXT.1	SSH Server Protocol
4	FCS_TLSC_EXT.2	TLS Client Protocol with authentication
5	FIA_PMG_EXT.1	Password Management
6	FIA_UIA_EXT.1	User Identification and Authentication
7	FIA_UAU_EXT.2	Password-based Authentication Mechanism
8	FIA_X509_EXT.1	X.509 Certificate Validation
9	FIA_X509_EXT.2	X.509 Certificate Authentication
10	FIA_X509_EXT.3	X.509 Certificate Requests
11	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
12	FPT_APW_EXT.1	Protection of Administrator Passwords
13	FPT_TST_EXT.1	TSF Testing
14	FPT_TUD_EXT.1	Trusted Update
15	FTA_SSL_EXT.1	TSF-initiated Session Locking

5.2 Extended Security Functional Components Rationale

All extended security functional components are sourced directly from the NDcPP and applied verbatim. Exact compliance required by the NDcPP also mandates inclusion of all applicable extended components defined in the PP.

6 Security Requirements

6.1 Security Functional Requirements

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 number in parenthesis placed at the end of the component. (e.g., SFR_ABC.1**(2)**)
    - **Assignment**: allows the specification of an identified parameter. Assignments are indicated using bold italics and are surrounded by brackets (e.g., ***[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**: are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in <u>***italicized bold and underlined text***</u>.

Note 1: Operations already performed in the NDcPP are not identified in this Security Target.

Note 2: Refinements made by the PP authors will not be identified as refinements in this ST. The "Refinement" identifier is reserved for identifying any refinements made by the ST author.

- **Explicitly stated Security Functional Requirements** (i.e., those not found in Part 2 of the CC) are identified "_EXT" in the component name.)

The TOE security functional requirements are listed in Table 10. All SFRs are based on requirements defined in Part 2 of the Common Criteria or defined in the *collaborative Protection Profile for Network Devices, Version 1.0, February 2015* [NDcPP].

Table 10: TOE Security Functional Components

Functional Components		
1	FAU_GEN.1	Audit Data Generation
2	FAU_GEN.2	User Identity Association
3	FAU_STG_EXT.1	Protected Audit Event Storage
4	FCS_CKM.1	Cryptographic Key Generation
5	FCS_CKM.2	Cryptographic Key Establishment
6	FCS_CKM.4	Cryptographic Key Destruction
7	FCS_COP.1 (1)	Cryptographic Operation (AES Data Encryption/Decryption)
8	FCS_COP.1 (2)	Cryptographic Operation (Signature Generation and Verification)
9	FCS_COP.1 (3)	Cryptographic Operation (Hash Algorithm)
10	FCS_COP.1 (4)	Cryptographic Operation (Keyed Hash Algorithm)
11	FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
12	FCS_SSHS_EXT.1	SSH Server Protocol
13	FCS_TLSC_EXT.2	TLS Client Protocol with authentication
14	FIA_PMG_EXT.1	Password Management
15	FIA_UIA_EXT.1	User Identification and Authentication
16	FIA_UAU_EXT.2	Password-based Authentication Mechanism
17	FIA_UAU.7	Protected Authentication Feedback
18	FIA_X509_EXT.1	X.509 Certificate Validation
19	FIA_X509_EXT.2	X.509 Certificate Authentication
20	FIA_X509_EXT.3	X.509 Certificate Requests
21	FMT_MOF.1	Trusted Update
22	FMT_MTD.1	Management of TSF Data
23	FMT_SMF.1	Specification of Management Functions
24	FMT_SMR.2	Restrictions on Security Roles
25	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
26	FPT_APW_EXT.1	Protection of Administrator Passwords
27	FPT_TST_EXT.1	TSF Testing
28	FPT_TUD_EXT.1	Trusted Update
29	FPT_STM.1	Reliable Time Stamps
30	FTA_SSL_EXT.1	TSF-initiated Session Locking
31	FTA_SSL.3	TSF-initiated Termination
32	FTA_SSL.4	User-initiated Termination
33	FTA_TAB.1	Default TOE Access Banners
34	FTP_ITC.1	Inter-TSF Trusted Channel
35	FTP_TRP.1	Trusted Path

6.1.1 *Security Audit (FAU)*

6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions comprising:
  - Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
  - Security related 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).
  - Starting and stopping services (if applicable)
  - ***[no other actions]***

d) Specifically defined auditable events listed in ***Table 11.***

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information specified in column three of ***Table 11***.

Table 11: Auditable Events (Table 1 of the NDcPP)

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None
FAU_GEN.2	None.	None
FAU_STG_EXT.1	None.	None
FCS_CKM.1	None.	None
FCS_CKM.2	None	None
FCS_CKM.4	None	None
FCS_CKM_EXT.4	None.	None
FCS_COP.1 (1)	None.	None
FCS_COP.1 (2)	None.	None
FCS_COP.1 (3)	None.	None
FCS_COP.1 (4)	None.	None
FCS_RBG_EXT.1	None.	None
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure

Requirement	Auditable Events	Additional Audit Record Contents
	Successful SSH rekey	Non-TOE endpoint of connection (IP address)
FCS_TLSC_EXT.2	Failure to establish a TLS Session	Reason for failure
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1	Any attempt to initiate a manual update	None.
FMT_MTD.1	All management activities of TSF data.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None.
FPT_STM.1	Changes to the time.	The old and new values for the time.
		Origin of the attempt (e.g., IP address).
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel.	Identification of the initiator and target of failed trusted channels establishment attempt.
	Termination of the trusted channel.	
	Failure of the trusted channel functions.	
FTP_TRP.1	Initiation of the trusted channel.	Identification of the claimed user identity.
	Termination of the trusted channel.	
	Failures of the trusted path functions.	

6.1.1.2 FAU_GEN.2 User Identity Association

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

6.1.1.3 FAU_STG_EXT.1 Protected Audit Event Storage

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

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

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

6.1.2 *Cryptographic Support (FCS)*

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

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;]

~~and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]~~.

6.1.2.2 FCS_CKM.2 Cryptographic Key Establishment

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

[RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography";]

~~that meets the following: [assignment: list of standards]~~.

6.1.2.3 FCS_CKM.4 Cryptographic Key Destruction

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

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

- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that

  [logically addresses the storage location of the key and performs a [single], overwrite consisting of [zeroes]];

  that meets the following*: No Standard*.

6.1.2.4 FCS_COP.1 (1) Cryptographic Operation (AES Data Encryption/ Decryption)

FCS_COP.1.1 (1) The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in ***[CBC]*** mode and cryptographic key sizes ***[128 bits, 192 bits, 256 bits]*** that meet the following: AES as specified in ISO 18033-3, ***[CBC as specified in ISO 10116]***.

6.1.2.5 FCS_COP.1 (2) Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1 (2) The TSF shall perform *cryptographic signature services* (generation and verification) in accordance with a specified cryptographic algorithm

[RSA Digital Signature Algorithm (rDSA) with a key size (modulus) [2048 bits, 3072 bits]]

that meets 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].

6.1.2.6 FCS_COP.1 (3) Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1 (3) The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm ***[SHA-1, SHA-256]*** ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~ that meet the following: *ISO/IEC 10118-3:2004.*

6.1.2.7 FCS_COP.1 (4) Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1 (4) 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-bit, 256-bit]*** and message digest sizes ***[160, 256]*** bits that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

6.1.2.8 FCS_RBG_EXT.1 Random Bit Generation

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

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from ***[[two] software-based noise sources]*** 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.

6.1.2.9 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and ***[6668 and no other RFCS].***

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

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

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: aes128-cbc, aes256-cbc, ***[no other algorithms].***

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses ***[ssh-rsa]*** and ***[no other public key algorithms]*** as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses ***[hmac-sha1, hmac-sha1-96, hmac-sha2-256]*** *and* ***[no other MAC algorithms]*** as its MAC algorithm(s) and rejects all other MAC algorithm(s).

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.

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

6.1.2.10 FCS_TLSC_EXT.2 TLS Client Protocol with authentication

FCS_TLSC_EXT.2.1 The TSF shall implement ***[TLS 1.2 (RFC 5246)]*** supporting the following ciphersuites:

- Mandatory Ciphersuites:

  TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268

- ***[Optional Ciphersuites:***

  TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246

  TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246

TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246

TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246

TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246

]

FCS_TLSC_EXT.2.2 The TSF shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.2.3 The TSF shall only establish a trusted channel if the peer certificate is valid.

FCS_TLSC_EXT.2.4 The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: ***[none]*** and no other curves.

FCS_TLSC_EXT.2.5 The TSF shall support mutual authentication using X.509v3 certificates.

6.1.3 *Identification and Authentication (FIA)*

6.1.3.1 FIA_PMG_EXT.1 Password Management

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

a) *Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters:* ***[“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(”, “)”, [“'”, “+”, “,”, “-”, “.”, “/”, “:”, “;”, “<”, “=”, “>”, “[”, “\”, “]”, “_”, “`”, “{”, and “}”]];***

b) *Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater.*

6.1.3.2 FIA_UIA_EXT.1 User Identification and Authentication

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

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

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

6.1.3.3 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, ***[none]*** to perform administrative user authentication.

6.1.3.4 FIA_UAU.7 Protected Authentication Feedback

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

6.1.3.5 FIA_X509_EXT.1 X.509 Certificate Validation

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

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using ***[the Online Certificate Status Protocol (OCSP) as specified in RFC 2560].***
- 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.*

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

6.1.3.6 FIA_X509_EXT.2 X.509 Certificate Authentication

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

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

6.1.3.7 FIA_X509_EXT.3 X.509 Certificate Requests

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

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

6.1.4 *Security Management (FMT)*

6.1.4.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to enable the functions to perform *manual update* to *Security Administrators*.

6.1.4.2 FMT_MTD.1 Management of TSF Data

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

6.1.4.3 FMT_SMF.1 Specification of Management Functions

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

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using* **[hash comparison]** *capability prior to installing those updates;*
- ***[Ability to configure the cryptographic functionality.]***

6.1.4.4 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator.*

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

FMT_SMR.2.3 The TSF shall ensure that the conditions:

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

are satisfied.

6.1.5 *Protection of the TSF (FPT)*

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

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

6.1.5.2 FPT_APW_EXT.1 Protection of Administrator Passwords

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

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

6.1.5.3 FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests ***[during initial start-up (on power on), at the conditions [as specified by FIPS PUB 140-2 Section 4.9.2]]*** to demonstrate the correct operation of the TSF: ***[***

Power-up 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

].

6.1.5.4 FPT_TUD_EXT.1 Trusted Update

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

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

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a ***[published hash]*** prior to installing those updates.

6.1.5.5 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.6 *TOE Access (FTA)*

6.1.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions,

- ***[terminate the session]***

after a Security Administrator-specified time period of inactivity.

6.1.6.2 FTA_SSL.3 TSF-initiated Termination

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

6.1.6.3 FTA_SSL.4 User-initiated Termination

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

6.1.6.4 FTA_TAB.1 Default TOE Access Banners

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

6.1.7 *Trusted Path/Channels (FTP)*

6.1.7.1 FTP_ITC.1 Inter-TSF Trusted Channel

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

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for ***[transmitting audit records to an audit server].***

6.1.7.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 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.

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

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

6.2 Security Assurance Requirements

6.2.1 *Security Assurance Requirements for the TOE*

This section defines the assurance requirements for the TOE. The assurance activities to be performed by the evaluator are defined in Sections 6 of the *collaborative Protection Profile for Network Devices v1.0* [NDcPP] and are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Table 12: Assurance Components

Assurance Class	Assurance Components	
Development	ADV_FSP.1	Basic Functional Specification
Guidance documents	AGD_OPE.1	Operational User guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability Survey

The following tables state the developer action elements, content and presentation elements and evaluator action elements for each of the assurance components.

Table 13: ADV_FSP.1 Basic Functional Specification

Developer action elements	
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.
Content and presentation elements	
ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
Evaluator action elements	
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.

Table 14: AGD_OPE.1 Operational User Guidance

Developer action elements	
AGD_OPE.1.1D	The developer shall provide operational user guidance.
Content and presentation elements	

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.
Evaluator action elements	
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 15: AGD_PRE.1 Preparative Procedures

Developer action elements	
AGD_PRE.1.1D	The developer shall provide the TOE, including its preparative procedures.
Content and presentation elements	
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.
Evaluator action elements	
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.

Table 16: ALC_CMC.1 Labeling of the TOE

Developer action elements	
ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
Content and presentation elements	
ALC_CMC.1.1C	The TOE shall be labeled with its unique reference.
Evaluator action elements	
ALC_CMC.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 17: ALC_CMS.1 TOE CM Coverage

Developer action elements	
ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
Content and presentation elements	
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.
Evaluator action elements	
ALC_CMS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 18: ATE_IND.1 Independent Testing – Conformance

Developer action elements	
ATE_IND.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
ATE_IND.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
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.

Table 19: AVA_VAN.1 Vulnerability Survey

Developer action elements	
AVA_VAN.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
AVA_VAN.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
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.

6.2.2 *Security Assurance Requirements Rationale*

This ST conforms to the [NDcPP], which draws from the CC Security Assurance Requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

6.3 Rationale

This ST claims Exact Compliance to the *collaborative Protection Profile for Network Devices v1.0* [NDcPP]. Therefore:

- All secure usage assumptions, organizational security policies, and threats are completely covered by security objectives.
- Each objective counters or addresses at least one assumption, organizational security policy, or threat.
- The set of components (requirements) in the ST are internally consistent and complete.

6.3.1 *TOE SFR Dependencies*

The following table provides SFR dependency mapping. All SFRs were drawn from the [NDcPP]. For extended components that were derived from SFRs from CC Part 2 dependencies were based on unmodified SFRs, for all other extended components dependencies were determined based on Appendix C Extended Component Definitions.

Table 20: SFR Dependencies

SFR	Dependency	Satisfied by
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FAU_UID.1	FAU_GEN.1 FIA_UIA_EXT.1
FAU_STG_EXT.1	FAU_GEN.1 FTP_ITC.1	FAU_GEN.1 FTP_ITC.1
FCS_CKM.1	FCS_COP.1 FCS_CKM.4	FCS_COP.1 (2) FCS_CKM.4
FCS_CKM.2	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM.4
FCS_CKM.4	FCS_CKM.1	FCS_CKM.1
FCS_COP.1(1)	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM.4
FCS_COP.1(2)	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM.4
FCS_COP.1(3)	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM.4
FCS_COP.1(4)	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM.4
FCS_RBG_EXT.1	none	

FCS_SSHS_EXT.1	FCS_COP.1(1)
	FCS_COP.1(2)
	FCS_COP.1(3)
		FCS_COP.1(1)
		FCS_COP.1(2)
		FCS_COP.1(3)

FCS_TLSC_EXT.2	FCS_COP.1(1)
	FCS_COP.1(2)
	FCS_COP.1(3)
	FCS_RBG_EXT.1
		FCS_COP.1(1)
		FCS_COP.1(2)
		FCS_COP.1(3)
		FCS_RBG_EXT.1

FIA_PMG_EXT.1	none	
FIA_UIA_EXT.1	FTA_TAB.1	FTA_TAB.1
FIA_UAU_EXT.2	none	
FIA_UAU.7	FIA_UAU.1	FIA_UIA_EXT.1
FIA_X509_EXT.1	none	
FIA_X509_EXT.2	none	
FIA_X509_EXT.3	none	
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	none	
FMT_SMR.2	FIA_UID.1	FIA_UIA_EXT.1
FPT_SKP_EXT.1	none	
FPT_APW_EXT.1	none	
FPT_TST_EXT.1	none	

FPT_TUD_EXT.1	FCS_COP.1(1)
	FCS_COP.1(3)
		FCS_COP.1(1)
		FCS_COP.1(3)

FPT_STM.1	none	
FTA_SSL_EXT.1	FIA_UAU.1	FIA_UIA_EXT.1
FTA_SSL.3	none	
FTA_SSL.4	none	
FTA_TAB.1	none	
FTP_ITC.1	none	
FTP_TRP.1	none	

7 TOE Summary Specification

This chapter describes the security functions:

Table 21: TOE Security Functions

Security Objectives	SFR
7.1 Security Audit	FAU_GEN.1
	FAU_GEN.2
	FAU_STG_EXT.1
7.2 Cryptography	FCS_CKM.1
	FCS_CKM.2
	FCS_CKM.4
	FCS_COP.1 (1-4)
	FCS_RBG_EXT.1
	FCS_SSHS_EXT.1
	FCS_TLSC_EXT.2
7.3 Identification and Authentication	FIA_PMG_EXT.1
	FIA_UIA_EXT.1
	FIA_UAU_EXT.2
	FIA_UAU.7
	FIA_X509_EXT.1
	FIA_X509_EXT.2
	FIA_X509_EXT.3
7.4 Security Management	FMT_MOF.1
	FMT_MTD.1
	FMT_SMF.1
	FMT_SMR.2
7.5 Protection of the security functionality	FPT_SKP_EXT.1
	FPT_APW_EXT.1
	FPT_TST_EXT.1
	FPT_TUD_EXT.1
	FPT_STM.1
7.6 TOE access	FTA_SSL_EXT.1
	FTA_SSL.3
	FTA_SSL.4
	FTA_TAB.1
7.7 Trusted path/channels	FTP_ITC.1
	FTP_TRP.1

7.1 Security Audit

FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1, FPT_STM.1

The TOE generates syslog-conformant audit record whenever a security-relevant event occurs. The audit records reflect a wide range of circumstances, including warnings about the state of device and a variety of security relevant events. The TOE supports eight levels of events: emergencies, alerts, critical, errors, warnings, notifications, informational, and debugging. Emergencies are level 0 and debugging is level 7. The Security Administrator must set/ensure the level of the audit logging is set to 7 to be compliant with the CC evaluated configuration.

For each audited event, the date and time, the type of event, the subject identity (e.g. IP address or UserID), and the outcome are logged. The audit records may also contain event-specific content. The security-relevant events that are logged include starting and stopping of the audit functions, TOE configuration changes, as well as all the events specified by the 'Audit Data Generation' functional requirement.

The TOE generates audit records for the following administrative tasks related to cryptographic keys:

- Generation and destruction of a public and associated private key
- Installation and removal of a trusted root or intermediate authority certificate
- Generation of CSR and import of a signed certificate
- Association of a public RSA key with an administrative identity

The audit trail consists of individual audit records, with a unique audit record generated for each event that occurred. Up to 512 audit records can be stored locally on the appliance, or all logs can be sent to an external audit server. On-device audit records exist in a circular buffer; when the buffer gets full, the oldest message is overwritten first. The viewing and clearing of the local audit trail is restricted to authorized administrators with access to `show logging` and `clear logging auditlog` commands. Clearing local audit trail wipes all audit records. In this way, the audit records are protected against unauthorized access and deletion.

The TOE is designed to securely forward audit records to a designated audit server over a persistent trusted channel. This trusted channel is implemented with a mutually authenticated TLS tunnel. When configured, the TOE uploads audit records in syslog (RFC 5424) format as they are generated without any delay. If the connection to the external audit server is lost, the TOE continues to save local audit logs so there is no loss of audit. However, when the connection to the audit server is restored the TOE only forwards the newly generated audit records. There is no automated log reconciliation process (syncing) between the locally stored records with the external audit server upon the re-establishment of the connection. However, the TOE supports multiple simultaneous audit servers enabling high-availability setup.

The TOE implements a hardware clock that could be synchronized with an external timeserver. This system clock is used to generate time stamps that are part of the audit records, the audit trail can be shown with the actual date and time of the system.

7.2 Cryptography

FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1 (1-4), FCS_RBG_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.2

The TOE's Dell EMC Networking OS v9.11 exclusively relies on the Dell OpenSSL Cryptographic Library Version 2.4 operating in FIPS mode to implement all cryptographic security functionality. Dell OpenSSL Cryptographic Library Version 2.4 validated according to FIPS 140-2 as a level 1 software cryptographic module, CMVP certificate #2496 covering RSA, AES, SHA, HMAC and DRBG functionality. This module does not include key establishment functionality, NIST SP800-56B conformance is vendor affirmed." The following Cryptographic Algorithm Validation Program (CAVP) certificates also applicable to the TOE:

Table 22: Dell Networking Platforms Cryptography

Requirement Class	Requirement Component	Dell Networking Platforms Implementation	Certificate #
FCS: Cryptographic Support	FCS_CKM.1 Cryptographic Key Generation	Generating 2048-bit and 3072-bit RSA keypairs validated conforming to FIPS186-4.	RSA #2334
	FCS_CKM.2 Cryptographic Key Establishment	Key establishment according to SP 800-56B: SSH KDF conformant to SP 800-135 TLS KDF conformant to SP 800-135	CVL# 1047
	FCS_CKM.4 Cryptographic Key Destruction	Destruction of all keys is performed by single direct overwrite followed by a read-verify action.	n/a
	FCS_COP.1(1) Cryptographic Operation (AES Data Encryption/Decryption)	AES encryption and decryption used in CBC mode with 128-bit, 192-bit, and 256-bit key sizes validated conforming to FIPS PUB 197.	AES #4320
	FCS_COP.1(2) Cryptographic Operation (Signature Generation and Verification)	RSA signature generation and verification according to RSASSA-PKCS1v1_5 with 2048-bit and 3072-bit key sizes utilizing SHA-1 (protocol only), SHA-256. RSA signature generation and verification according to RSASSA-PSS with 2048-bit and 3072-bit key sizes SHA-1 (protocol only), SHA-256 and salt.	RSA #2334
	FCS_COP.1(3) Cryptographic Operation (Hash Algorithm)	Hashing using SHA-1, SHA-256 validated conforming to FIPS 180-3, Secure Hash Standard (SHS).	SHS #3556

	FCS_COP.1(4) Cryptographic Operation (Keyed Hash Algorithm)	Keyed hash HMAC-SHA1, HMAC-SHA256, validated conforming to FIPS 198, Keyed-Hash Message Authentication Code (HMAC). Supported cryptographic key sizes: 160, 256 bits and message digest sizes: 160, 256 bits. Keyed hash use matches validated hash algorithms implemented by the module.	HMAC #2853
	FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)	CTR_DRBG (AES-256) random bit generation validated conforming to NIST SP PUB 800-90.	DRBG #1376
	FCS_SSHS_EXT.1 SSH Server Protocol	TOE implements SSHv2 protocol and supports password-based authentication with following ciphers: • AES-CBC-128, AES-CBC-256 for data encryption • SSH_RSA for public-key authentication • HMAC-SHA1, HMAC-SHA1-96, HMAC-SHA2-256 for data integrity • diffie-hellman-group14-sha1 for key exchange	n/a
	FCS_TLSC_EXT.2 TLS Client Protocol	TOE implements TLS 1.2 and supports certificate-based authentication with the following ciphers: TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_ SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	n/a

TOE cryptographic library is capable of supporting other encryption algorithms, key-hash methods, and key exchange algorithms but they are disabled in the evaluated configuration.

The TOE uses a software-based random bit generator (DRBG) that complies with NIST SP 800-90 for all cryptographic operations. Each DRBG instance is seeded with full entropy sourced from Linux Kernel Random Number Generator (LKRNG) operating in a blocking mode (/dev/random). All entropy is extracted, processed, and accumulated by LKRNG from multiple software-based noise sources. The following noise sources are used: timing of inter-process communications events, CPU jitter. Accumulated entropy is not preserved across system reboots.

The TOE follows recommendations outlined in the NIST SP 800-56B ‘Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography’ requirements as part of RSA-based key establishment. However, to support RFC-compliant secure channel protocols the TOE implements NIST SP 800-135 TLS and SSH key derivation functions (KDF). TOE acts as a sender of secret keying material for RSA key establishment.

The TOE is designed to destroy Critical Security Parameters (CSPs) when no longer required for use to mitigate the possibility of disclosure. At various times during TOE operation (e.g. an active SSH session) CSPs are present in RAM in plain text, then de-allocated and cleared from memory followed by read-verify when no longer needed (e.g. on SSH session termination). CSPs are also stored in FLASH and cleared when no longer used. Additionally, the TOE implements commands to on-demand clear specific CSPs (e.g. private RSA keys) that can be invoked by a Security Administrator with a sufficient privilege level. The following table identifies applicable CSPs and summarizes zeroization procedure:

Table 23: Dell Networking Platforms CSPs

Identifier	Name	Generation / Algorithm	Purpose	Storage Location	Zeroization Summary
CSP1	Private Key	PKCS1v1_5 / RSA	RSA private key used for public-key based authentication	NVRAM, RAM (plain text)	Single direct overwrite consisting of zeros followed by a read-verify action.
CSP2	Private Key	PKCS1v1_5 / RSA	X509 private key used for certificate-based authentication	NVRAM, RAM (plain text)	Single direct overwrite consisting of zeros followed by a read-verify action.
CSP3	SSH Session Keys	Generated using SSH KDF	SSH keys – server to client, client to server	RAM (plain text)	Single direct overwrite consisting of zeros followed by a read-verify action.
CSP4	Diffie-Hellman Key Pair	DH	Key agreement for SSH sessions	RAM (plain text)	Cleared when device is powered down or as part of session termination. Overwritten by new value or loss of capacitor charge in the memory cell.
CSP5	TLS Pre-master Secret	RSA or DH, generated using DRBG	Key agreement for TLS	RAM (plain text)	Cleared when device is powered down or as part of session termination. Overwritten by new value or loss of capacitor charge in the memory cell.
CSP6	TLS Session Keys	Generated using TLS KDF	Symmetric keys for TLS	RAM (plain text)	Cleared when device is powered down or as part of session termination. Overwritten by new value or loss of capacitor charge in the memory cell.

Identifier	Name	Generation / Algorithm	Purpose	Storage Location	Zeroization Summary
CSP7	Administrative Passwords	SHA256	Credentials used to authenticate the administrator login.	FLASH (cipher text)	Hashed passwords exist locally in a startup configuration file and replaced when that file is edited and saved. The passwords are stored in the hashed form only. Overwritten with new data.
				RAM (cipher and plain text)	Passwords in RAM are zeroized when creating / resetting the password. Both clear text and encrypted forms are stored in RAM. Overwritten by new value or loss of capacitor charge in the memory cell.
CSP8	PRNG Seed key	/dev/random	Seed key for PRNG	RAM (plain text)	Cleared when device is powered down or during reboot by the new seed. Overwritten by new value or loss of capacitor charge in the memory cell.

The TOE implements the SSHv2 secure communication protocol that complies with RFCs 4251, 4252, 4253, 4254, 6668. The SSHv2 implemented with AES128-CBC or AES256-CBC encryption algorithms in combination with HMAC-SHA1, HMAC-SHA1-96, or HMAC-SHA2-256 data integrity algorithms, and diffie-hellman-group14-sha1 for key exchange method and ssh-rsa transport. The TOE utilizes SSHv2 for secure remote administration over CLI interface with password-based authentication and optionally with a RSA public key. SSH packets that exceed 256K in length size are dropped at the application layer per RFC 4253. The SSH connection is automatically rekeyed by default after 60 minutes or 1 GB of data, both of these thresholds are administrator-configurable.

The TOE exclusively supports TLS v1.2 secure communication protocol that complies with RFC 5246. The TOE supports mutual X509v3 certificate-based authentication and the following ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

The TOE implements reference identifier matching according to RFC 6125. The reference identifier specified during configuration of TLS connection. Supported reference identifiers are DNS names or IP addresses. As part of negotiating TLS connection, the TOE will verify that peer certificate Subject Alternative Name (SAN) or Common Name (CN) contains expected identifier. The CN only supports domain names and not ip addresses. CN is checked only if SAN is absent. The TOE is also capable parsing identifiers that include wildcards, but their use is discouraged. The TOE only establishes connection if the peer certificate is valid, trusted, and has a matching reference identifier. The TOE does not implement certificate pinning and does not support Elliptic Curves in the evaluated configuration.

7.3 Identification and Authentication

FIA_PMG_EXT.1, FIA_UIA_EXT.1, FIA_UAU_EXT.2, FIA_UAU.7, FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

The TOE functionality can be logically divided into following categories: Data Plane and Control Plane. The Control Plane is associated with the management port and facilitates TOE's administrative functionality; the Data Plane is primarily associated with various data ports and facilitates TOE switching functionality. The TOE allows unauthenticated network traffic and routing services to utilize Data Plane functionality as part of its core functionality. This unauthenticated traffic does not include any management or configuration traffic and does not directly interface with the Control Plane.

The TOE requires any user to be identified and authenticated before any management action. The warning banner is displayed before login prompt on any of the management access points (local console or remote CLI sessions). In the evaluated configuration, the TOE does not allow unauthenticated configuration of the TOE's network routing/switching services and does not allow any unauthenticated management action.

A requesting user will be prompted to enter a user name and password upon establishing successful connection. The TOE will then compare entered credentials against the known user database. If the combinations match, the TOE will then attribute (bind) the administratively assigned role (predetermined group of privileges that dictate access to TOE functions) to that user for the duration of the management session.

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.

Administrative (management) roles are created with specific job functions in mind. Through these roles, users acquire the permissions to perform their associated job function. If a user's role matches one of the allowed roles for a specific command, then command authorization is granted. Multiple users can be assigned the same role, but each user can be assigned only a single role. Default command permissions are based on CLI mode, any specific command settings, and the permissions allowed by the role commands.

By default, TOE provides four system-defined administrator roles:

- Network Operator (netoperator) - This user role has no privilege to modify any configuration on the switch, but can access Exec mode (monitoring) to view the current configuration and status information.

- Network Administrator (netadmin): This user role can configure, display, and debug the network operations on the switch. Netadmin can access all of the commands that are available from the network operator role. This role does not have access to the commands that are available to the system security administrator for cryptography operations, AAA, or the commands reserved solely for the system administrator.

- Security Administrator (secadmin): This user role can control the security policy across the systems that are within a domain or network topology. The security administrator commands include FIPS mode enablement, password policies, inactivity timeouts, banner establishment, and cryptographic key operations for secure access paths.

- System Administrator (sysadmin). This role has full access to all the commands in the system, exclusive access to commands that manipulate the file system formatting, and access to the system shell. This role can also create user IDs and define other user roles.

For remote administration, implemented as a CLI over SSH, the TOE can be configured to authenticate using public key mechanism (RSA), or password-based, or both. For local administration, only password-based authentication is supported. When RSA authentication is used, the TOE checks presented public key against authorized keys database and verifies possession of a private key by negotiating secure channel using this public key. When both password and certificate are presented, the TOE use public key during handshake negotiation followed by a password verification

Upon successful authentication, the TOE assigns administratively defined role to that user for the duration of the session. The TOE facilitates all administrative actions through the CLI. Successful login is indicated by TOE offering a CLI command prompt.

The TOE supports having a minimum of 15 character password length and supports the using of upper and lower case, numeric, and special character combinations for password construction.

The TOE supports the use of X.509v3 certificates as defined by RFC 5280 to authenticate connections with authorized IT entities. When certificate based authentication is used, the TOE validates presented certificate, checks chain of trust against internal trusted store, and performs certificate revocation check. Certificate validation includes path validation (including checking CA certificates) certificate processing (including validating extendedKeyUsage field), and extension processing (including checking BasicConstraints extension). Verifying chain of trust includes validating each certificate in the chain, verifying that certificate path consist of trusted CA certificates, and performing revocation checks on all certificates in the path. Revocation checking is implemented using OCSP. If any part of authentication fails, connection is terminated at the handshake stage. Specifically, the TOE implements mutually authenticated secure channel using TLSv1.2 to a trusted audit server.

The TOE supports the following methods to obtain a certificate from a trusted CA:

- Manually import certificates in PEM format from an external server over SFTP
- Manually import certificates using removable media

Once the CA certificate is downloaded and prior to adding it to an existing list of trusted certificates the TOE verifies the following:

- Digital signature check
- Basic constrains extension with the CA flag set to true
- Key usage extension with the "keyCertSign" bit is set
- Certificate is not expired

All certificates are stored in a private, persistent location on the TOE. There is no direct access to stored certificates using regular interfaces.

The TOE is capable of generating Certificate Signing Requests (CSR) and authenticating with both CA-signed and self-signed certificates. The CSR is created using the cryptographic library operating in FIPS mode and uses RSA 2048-bit or greater modulus and SHA-256 digest algorithm.

When X509 certificate is presented during TLS handshake, the TOE validates presented certificate and the entire trust chain by performing revocation checks. The revocation check is performed by sending an OCSP request to a trusted OCSP responder and verifying signed response. If connection to OCSP server cannot be established, the administrator can configure default behavior and determine whether to accept the certificate in such cases.

The list of OCSP responders may be manually configured or specified in a CA certificate in the authorityInfoAccess extension.

7.4 Security Management

FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FMT_MOF.1

The TOE allows remote administration via SSHv2 session over an out of band LAN management RJ-45 port and local administration via a directly connected console cable. Both remote and local administration utilizes command-line interface (CLI). The CLI provides access to all management functions used to administer the TOE. The TOE requires each user to be successfully authenticated before allowing any other action on behalf of that user. All other remote management interfaces (e.g. Secure HTTP) are not evaluated and disabled in the evaluated configuration.

By default, CLI implements three main modes:

- EXEC mode: This mode allows the user to view settings and enter EXEC Privilege mode, which is used to configure the device.
- EXEC Privilege mode: This mode allows the user to access all the commands accessible in EXEC mode plus commands to view configurations, clear counters, manage configuration files, run diagnostics, and enable or disable debug operations. In addition, the user can enter the CONFIGURATION mode to configure interfaces, routes and protocols on the switch.
- CONFIGURATION mode: This mode allows the user to configure security features, time settings, set logging and SNMP functions, configure static ARP and MAC addresses, and set line cards on the system. Configuration of specific features or interfaces are subsets of the CONFIGURATION mode.

All TOE commands assigned permissions that can be customized and associated with specific user roles. Permissions for user roles are non-hierarchical, and this allows finer granularity in managing access to the system.

The TOE supports RBAC. Using RBAC, access and authorization is controlled based on a user’s role. All of the management functions are restricted to the Security Administrators of the TOE. Security Administrators with sufficient privilege can perform the following actions: manage administrative accounts, start and shut down TOE, administer system configuration, and review the audit records. The full list of security-relevant management functions is specified in the 6.1.4.3 FMT_SMF.1 ‘Specification of Management Functions’.

The term “Security Administrator” is used to refer to any administrative user with the appropriate role with sufficient privilege to perform all relevant functions. The privilege level determines the functions the user can perform. It is understood that not all administrators will have sufficient permissions assigned to them to perform each administrative function discussed in this document. Specifically, the TOE restricts the ability to perform manual update to System Administrator.

7.5 Protection of the security functionality

FPT_SKP_EXT.1, FPT_APW_EXT.1, FPT_TST_EXT.1, FPT_STM.1, FPT_TUD_EXT.1

The TOE is a standalone appliance designed to function independently, as a result, both security functionality and measures to protect security functionality are focused on self-protection.

The TOE employs both a dedicated communication channels (i.e. separate physical RJ-45 LAN connection for management) as well as cryptographic means (i.e. encrypted secure channels) to protect remote administration.

The TOE protects critical security parameters (CSP) such as stored passwords and cryptographic keys so they are not directly accessible via normal administrative interfaces. Locally stored password information is obscured by use of hashing (SHA256). Additionally, when login-related configuration information is accessed through regular TOE interfaces it is obfuscated by substituting hashed passwords with a series of asterisks.

The TOE is a hardware appliance that implements hardware-based real-time clock managed by embedded OS, which also controls the exposure of administrative functions. This clock is used to produce reliable timestamps that are available for audit trail generation, synchronization with the operational environment, session inactivity checks, and certificate expiration validation.

The TOE performs diagnostic self-tests during start-up and generates audit records to document failure. Some low-level critical failure modes can prevent TOE start-up and as a result will not generate audit records. In such cases, TOE appliance will enter failure mode displaying error codes, typically displayed on the console. The TOE can be configured to reboot or to stop with errors displayed when non-critical errors are encountered. The cryptographic module performs self-tests during startup; the messages are displayed on the console and audit records generated for both successful and failed tests. Self-tests comply with the FIPS 140-2 requirements for self-testing. The module performs known-answer algorithm testing, integrity testing, and conditional self-testing. Failure of any of the FIPS mode tests during boot process will stop start-up process and prompt the user to reload. For all start-up tests, successful completion is indicated by reaching operational status. The diagnostic self-tests monitor the TOE against a set of anticipated faults, therefore outside of failure mode induced by failing self-tests, the TSF is assumed to operate correctly.

Upgrading the TOE is a multi-step process performed by a Security Administrator. An authorized user must authenticate to the secure Dell Support website where the software downloads are available. The downloaded image must be transferred to the appliance using a secure method such as Secure Copy or SFTP. The image file, now located on the appliance, is then verified using the "`verify`" CLI command that produces a SHA-256 hash value. The administrator must then visually compare the results to the published hash value on the Dell website with the produced value. Upon successful comparison, the administrator can then initiate the upgrade. The TOE also implements "`show version`" CLI command that displays information about firmware version running on the TOE.

7.6 TOE access

FTA_SSL.3, FTA_SSL.4, FTA_SSL_EXT.1, FTA_TAB.1

The TOE implements remote and local administrative access via command line interface (CLI). The TOE will display a customizable banner when a user initiates an interactive session either locally or remotely. The TOE's minimum lockout value must be configured to a non 0 value to enforce an administrator-defined inactivity timeout after which the inactive session is automatically terminated. Once a session (local or remote) has been terminated, the TOE requires the user to re-authenticate. The administrator can force termination of current session by issuing the logout function: `exit`.

7.7 Trusted path/channels

FTP_ITC.1, FTP_TRP.1

The TOE protects remote management sessions by establishing a trusted path (using SSH) between itself and the administrator connected to a dedicated RJ-45 LAN management port. When a client attempts to connect using SSHv2, the TOE and the client will negotiate the most secure algorithms available at both ends to protect the session. If the session cannot be negotiated, or the protocols cannot be agreed on, the connection is dropped. After initial connection, protocol negotiation, and key exchange, diffie-hellman-group14-sha1 key exchange algorithm produces a shared secret that is used to derive the AES and the HMAC keys. After that point, all traffic between the TOE and the external entity is encrypted using AES-CBC-128 or AES-CBC-256 symmetric encryption algorithm. Authentication is encapsulated in this encrypted channel. For public key-based authentication, RSA host key pair generated by the TOE or generated elsewhere and imported into the TOE. Client RSA public keys have to be generated elsewhere, imported into the TOE, and added to the authorized keys database.

The TOE protects communications with the audit server by establishing a trusted channel between itself and the audit server. To implement trusted channel, the TOE uses TLS v1.2 protocol with certificate-based authentication. For certificate-based authentication, presented certificate (x.509v3) is first validated and then compared to the authorized certificates database.

8 Acronyms and Terminology

8.1.1 *Acronyms*

The following table defines CC and Product specific acronyms used within this Security Target.

Table 24: Acronyms

Acronym	Definition
CC	Common Criteria
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RFC	Request for Comment
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

8.1.2 *Product Acronyms and Terminology*

The following table defines the CC and Product-specific terminology used within this Security Target.

Table 25: Terminology

Terminology	Definition
AAA	Authentication, Authorization, and Accounting (AAA). A security architecture for distributing systems for controlling remote access to services.
RADIUS	Remote Authentication Dial-In User Service (RADIUS) protocol that includes authentication and authorization.

Terminology	Definition
RSA	Ron **R**ivest, Adi **S**hamir, Leonard **A**dleman. Public-key cryptosystem algorithm.
Routing Protocol	A routing protocol is a means whereby network devices exchange information about the state of the network and used to make decision about the best path for packets to the destination.
TACACS+	Terminal Access Controller Access-Control System Plus, an access control network protocol.