Dell Networking Switches
Security Target

Version 1.0

January 22, 2015

Revision History

Date	Version	Author	Description
06/16/2014	0.1	Cygnacom Solutions	First Draft
08/01/2014	0.2	Cygnacom Solutions	Vendor review & OS v9.6 updates
08/31/2014	0.3	Cygnacom Solutions	Addressing check-in comments
09/12/2014	0.4	Cygnacom Solutions	Vendor review & CAVP certificates
10/16/2014	0.5	Dell	Additional information required from Evaluator
01/19/2015	0.6	Cygnacom Solutions	Update post-testing
01/22/2015	1.0	Cygnacom Solutions	Final Version

Table of Contents

Figures and Tables

1 Security Target Introduction

1.1 Security Target Reference

ST Title: Dell Networking Switches Security Target

ST Version: v1.0

ST Author: CygnaCom Solutions Inc.

ST Date: 01/22/2015

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 v9.6

Table 1: TOE Platforms and Devices

Series	Platforms	Build
Dell Networking S-Series Top-of-rack Switches	S4810	9.6.0.0 P6
	S4820T	9.6.0.0 P6
	S5000	9.6.0.0 P6
	S6000	9.6.0.0 P6
Dell Networking Z-Series End-of-row Switches	Z9000	9.6.0.0 P6
	Z9500	9.6.0.0 P6

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

1.3 TOE Overview

1.3.1 *TOE Product Type*

The Target of Evaluation [TOE] is a Network Device as defined by the *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 [NDPP]: "*A network device is a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise".*

1.3.2 *TOE Usage*

The TOE is the Dell Networking Platforms running Dell Networking OS v9.6 that in the evaluated configuration consists of S4810, S4820T, S5000, S6000 top-of-rack data center switches, and Z9000, Z9500 end-of-row data center 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
    - Generate audit logs for security-relevant events
    - Supports secure communications to remote syslog servers
- Cryptographic Support
    - Validated cryptographic algorithms
    - Data zeroization
- User Data Protection
    - Residual information clearing
- Identification and Authentication
    - Password and user access policies
- Security Management
    - Local and remote administration
- Protection of the TOE Security Function (TSF)
    - Self-test on power-up
    - Trusted update
- TOE Access
    - Role-based access control
    - Session timeout and lockout
- Trusted Path/Channels
    - Trusted path for remote administrators

1.4 TOE Description

The TOE is the Dell Networking Platforms running Dell Networking OS v9.6 that consist of S-Series and Z-Series switches and includes the following appliances:

- Dell Networking S-Series S4810
- Dell Networking S-Series S4820T
- Dell Networking S-Series S5000
- Dell Networking S-Series S6000
- Dell Networking Z-Series Z9000
- Dell Networking Z-Series Z9500

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 S4810
The Dell Networking S-Series S4810 is an ultra-low-latency 10/40GbE top-of-rack switch purpose-built for applications in high-performance data center and computing environments. The S4810 compact 1U design provides 48 dual-speed 1/10GbE Small Form-factor Pluggable (SFP+) ports as well as 4 40GbE Quad SFP+ (QSFP+) uplinks. The S4810 features 1.28 TBps (full-duplex) non-blocking, cut-through switching fabric and delivers line-rate switching with Quality of Service (QoS), Priority-based Flow Control (PFC), Data Center Bridge Exchange (DCBx) and Enhance Transmission Selection (ETS).

Dell Networking S4820T
The Dell Networking S-Series S4820T is a top-of-rack switch purpose-built for applications in data center environments. The S4820T 1U design provides 48 1/10G BASE-T ports that support 100Mb/1Gb/10Gb and 4 40GbE QSFP+ uplinks. The S4820T features 1.28Tbps (full-duplex) non-blocking, cut-through switching fabric and delivers line-rate switching with QoS, PFC, DCBx and ETS.

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) non-blocking, cut-through switching fabric delivering line-rate performance and supports DCBx, Internet Small Computer System Interface (iSCSI), RDMA over converged Ethernet (RoCE) protocols.

Dell Networking S6000
The Dell Networking S-Series S6000 is a top-of-rack switch purpose-built for applications in high-performance data center and computing environments. The S6000 1U design provides

32 40GbE QSFP+ uplinks. The S6000 features 2.5Tbps (full-duplex) non-blocking, cut-through switching fabric and delivers line-rate switching with QoS, PFC, DCBx and ETS.

Dell Networking Z9000
The Dell Networking Z-Series Z9000 is a core or end-of-row switch product designed to meet the requirements for high-density 10/40 GbE aggregation in a data center network. The Z9000 2U design provides 32 40GbE QSFP+ ports or 128 ports of 10 GbE SFP+ realized through breakout cables. The Z9000 features 2.5Tbps (full-duplex) non-blocking, cut-through switching fabric and delivers line-rate switching with QoS, PFC, Link Aggregation Control Protocol (LACP), and ETS.

Dell Networking Z9500
The Dell Networking Z-Series Z9500 is a switch product designed to meet the requirements for high-density 10/40 GbE aggregation in a data center core network. The Z9500 3U design provides up to 132 ports of 40GbE QSFP+ ports with power-efficient operation that allows operating with 36, 84 or 132 ports enabled. The Z9500 features 10.4Tbps (full-duplex) non-blocking, cut-through switching fabric and delivers line-rate sub-2us latency switching with QoS, PFC, LACP, and ETS.

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 Networking OS v9.6) is shared across all platforms.

Dell Networking OS v9.6 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 provides functionality that implements secure channel and protects critical security parameters. 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:

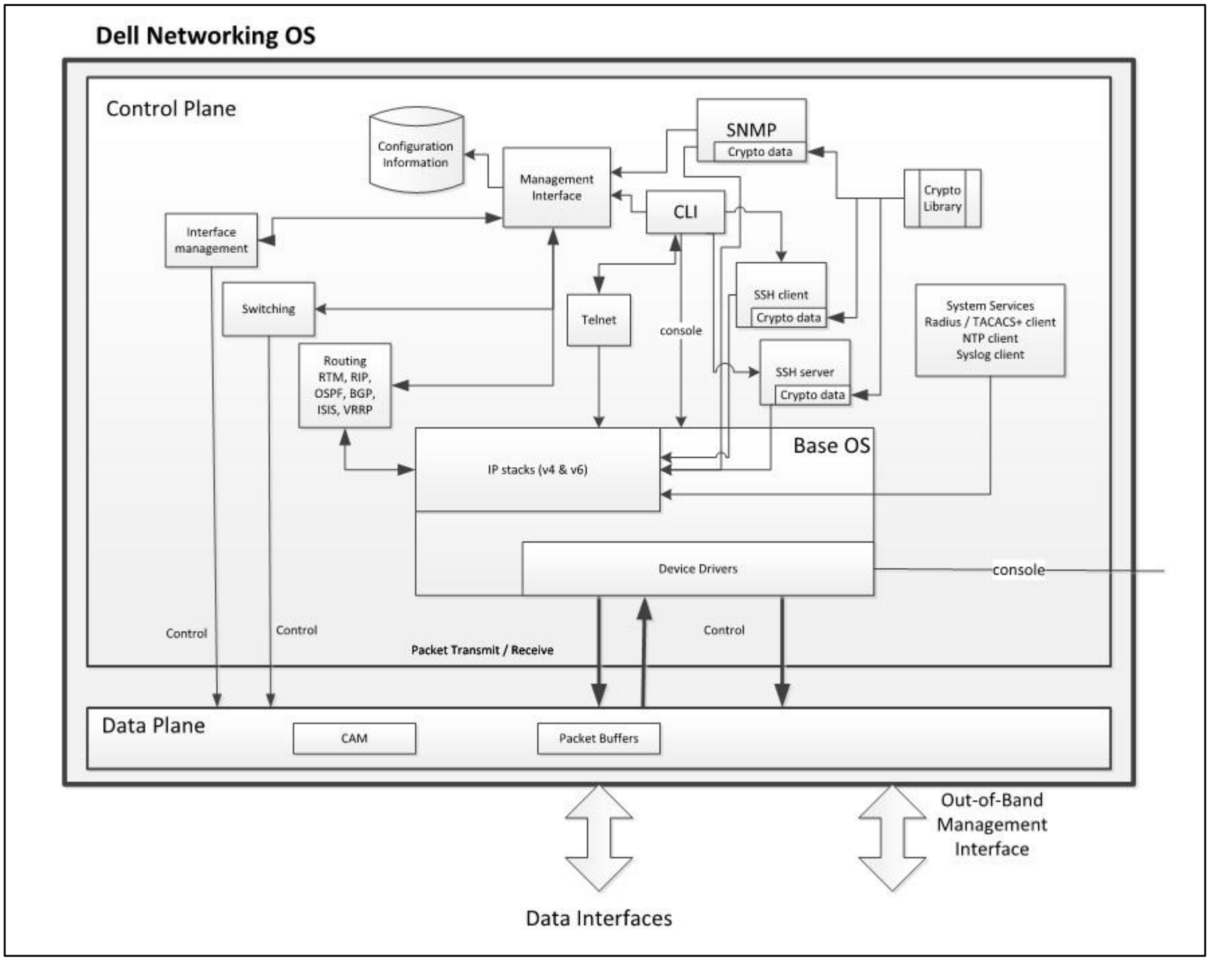

Figure 1: TOE Architecture

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	S4810	Power Architecture e500 Series	1U Top-of-rack	48x 10G SFP+ 4x 40GbE QSFP+
	S4820T	Power Architecture e500 Series	1U Top-of-rack	48 x 1/10G BASE-T 4 x 40GbE QSFP+
	S5000	2 x Power Architecture e500 Series	1U Top-of-rack	4x40GbE QSFP+ 4 module bays with: 0-4 12x 10G SFP+

				or 0-1 12 2/4/8Gbps FC modules
	S6000	Atom Centerton Series	1U Top-of-rack	32x 40GbE QSFP+
Dell Networking Z-Series Switches	Z9000	Xeon C5500 Series	2U End-of-row	32x 40GbE QSFP+
	Z9500	5 x Atom Centerton Series	3U End-of-row	132x 40GbE QSFP+

1.4.2.2 Software

The TOE runs pre-installed Dell Networking OS v9.6. 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 Networking OS v9.6, consists of Dell Operating System and Dell Application Software. Dell Operating System is based on NetBSD OS. 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 Networking OS v9.6 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 is the Dell Networking Platforms running Dell Networking OS v9.6**,** which includes:

- The appliance hardware
  - RJ-45/RS-232 management ports
  - USB management port (except S4810 model)
  - 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:
  - Syslog for external storage of audit logs
  - NTP for synchronizing system time (optional)

The TOE Boundary is outlined in the following figure:

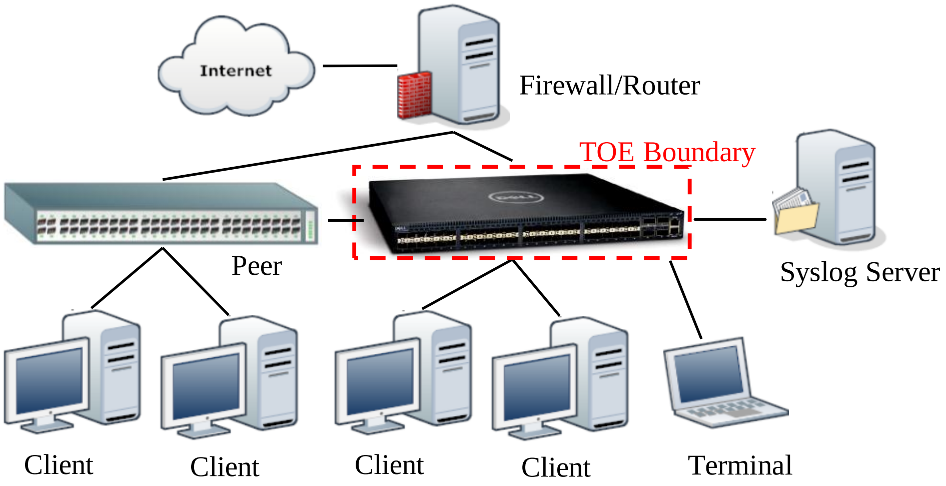

Figure *2*: TOE Boundary

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 logs can be stored locally to be viewed by an administrator or securely sent to a designated syslog server for archiving. The logs can be viewed by administrators using the appropriate CLI commands. The TOE also implements timestamps to ensure reliable audit information is available.

1.4.4.2 Cryptographic Support

The TOE performs the following cryptographic operations:

- Secure channel with following parameters:
    - AES-CBC-128, AES-CBC-256 for data encryption
    - SSH_RSA for host key algorithm
    - HMAC-SHA1, HMAC-SHA1-96, HMAC-SHA2-256 for data integrity
    - diffie-hellman-group14-sha1 for key exchange
- Random Bit Generation using CTR-DRBG (AES-256)
- Critical Security Parameters (CSPs) zeroization

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

1.4.4.3 User Data Protection

The TOE implements multiple measures to ensure residual information is not transmitted. Ingress packets are stored in the managed buffer that allocates dedicated memory space of the exact size required. Once the packet has been either transmitted or discarded, the memory used for that packet is returned back to the pool for reuse.

1.4.4.4 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.

1.4.4.5 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 authorized administrators of the TOE. Authorized 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 “authorized administrator” is used to refer to any administrative user with the appropriate role to perform the relevant functions.

1.4.4.6 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.

1.4.4.7 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.

1.4.4.8 Trusted Path/Channels

The TOE protects remote sessions by establishing a trusted path between itself and the administrator. The TOE prevents disclosure or modification of logs by establishing a trusted channel between itself and the Syslog server. To implement trusted path/secure channel the TOE uses an SSHv2 protocol with password-based or public key-based authentication.

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.
- Remote management using web interface (Secure HTTP or HTTPS) is excluded. The TOE does not satisfy all NDPP requirements for this administrative interface and it is 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), due to RFC-compliant implementations, are unable to satisfy NDPP cryptographic requirements.
- Use of the FTP server is excluded and it is disabled by default.
- Use of the SNMP functionality is excluded and it is disabled by default. The use of SNMPv3 is not restricted; however, it is an excluded function in NDPP evaluations.

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 Command Line Reference Guide for the S4810 System, September 23 2014 *Dell Configuration Guide for the S4810 System, September 23 2014* *Dell Release Notes for the S4810 System, Dell Networking OS v9.6, September 2014* *Dell Command Line Reference Guide for the S4820T System, September 23 2014* *Dell Configuration Guide for the S4820T System, September 23 2014* *Dell Release Notes for the S4820T System, Dell Networking OS v9.6, September 2014* *Dell Command Line Reference Guide for the S5000 System, September 23 2014* *Dell Configuration Guide for the S5000 System, September 23 2014* *Dell Release Notes for the S5000 System, Dell Networking OS v9.6, September 2014* *Dell Command Line Reference Guide for the S6000 System, September 23 2014* *Dell Configuration Guide for the S6000 System, September 23 2014* *Dell Release Notes for the S6000 System, Dell Networking OS v9.6, September 2014* *Dell Command Line Reference Guide for the Z9000 System, September 23 2014* *Dell Configuration Guide for the Z9000 System, September 23 2014* *Dell Release Notes for the Z9000 System, Dell Networking OS v9.6, September 2014* *Dell Command Line Reference Guide for the Z9500 System, September 23 2014* *Dell Configuration Guide for the Z9500 System, June September 23 2014* *Dell Release Notes for the Z9500 System, Dell Networking OS v9.6, September 2014*	[ADMIN]
Dell Common Criteria Addendum Guide, Dell Networking OS v9.6, January 2015	[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, CCMB-2012-09-002*, Version 3.1, Revision 4*	[CC]
Security Requirements for Network Devices Errata #3, 3 November 2014	[ERRATA]
U.S. Government Standard Protection Profile for Network Devices, Version 1.1, 08 June 2012	[NDPP]

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 (PP).

2.2 Protection Profile Claim

The TOE claims *exact* Compliance to *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 [NDPP] as changed/clarified by *Security Requirements for Network Devices Errata #3*, 3 November 2014 [ERRATA].

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 NDPP.

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 *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 [NDPP] as changed/clarified by *Security Requirements for Network Devices Errata #3*, 3 November 2014 [ERRATA] as specified in the PP, verbatim.

Table 5: TOE Threats

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

3.2 Organizational Security Policies (OSPs)

This section identifies the organizational security policies applicable to the *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 [NDPP] as changed/clarified by *Security Requirements for Network Devices Errata #3*, 3 November 2014 [ERRATA] as specified in the PP, verbatim.

Table 6: 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.

3.3 Assumptions

This section identifies assumptions applicable to the *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 [NDPP] as changed/clarified by *Security Requirements for Network Devices Errata #3*, 3 November 2014 [ERRATA] as specified in the PP, verbatim.

Table 7: TOE Assumptions

Assumption Name	Assumption Definition
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4 Security Objectives

This section defines the security objectives of the TOE and its supporting environment.

4.1 Security Objectives for the TOE

This section identifies Security Objectives for the TOE applicable to the *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 [NDPP] as changed/clarified by *Security Requirements for Network Devices Errata #3*, 3 November 2014 [ERRATA] as specified in the PP, verbatim.

Table 8: TOE Security Objectives

Objective Name	TOE Security Objective Definition
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

4.2 Security Objectives for the Operational Environment

This section identifies the Security Objectives for the Operational Environment applicable to the *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 [NDPP] as changed/clarified by *Security Requirements for Network Devices Errata #3*, 3 November 2014 [ERRATA] as specified in the PP, verbatim.

Table 9: Security Objectives for the Operational Environment

Objective Name	Environmental Security Objective Definition
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5 Extended Components Definition

The components listed in the following table have been defined in *U.S. Government Standard Protection Profile for Network Devices, 08 June 2012, Version 1.1* [NDPP] as changed/clarified by *Security Requirements for Network Devices Errata #3*, 3 November 2014 [ERRATA].

The extended components are denoted by adding "_EXT" in the component name.

5.1 Extended Security Functional Components

Table 10: Extended Components

Item	SFR ID	SFR Title
1	FAU_STG_EXT.1	Extended: External Audit Trail Storage
2	FCS_CKM_EXT.4	Extended: Cryptographic Key Zeroization
3	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
4	FCS_SSH_EXT.1	Extended: SSH
5	FIA_PMG_EXT.1	Extended: Password Management
6	FIA_UAU_EXT.2	Extended: Password-based Authentication Mechanism
7	FIA_UIA_EXT.1	Extended: User Identification and Authentication
8	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
9	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)
10	FPT_TST_EXT.1	Extended: TSF Testing
12	FPT_TUD_EXT.1	Extended: Trusted Update
13	FTA_SSL_EXT.1	Extended: TSF-initiated Session Locking

5.2 Extended Security Functional Components Rationale

All extended security functional components are sourced directly from the PP and applied verbatim.

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 letter in parenthesis placed at the end of the component. For example FDP_ACC.1 (a) and FDP_ACC.1 (b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, "a" and "b".
  - **Assignment**: allows the specification of an identified parameter. Assignments are indicated using bold 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 ***italicized bold and underlined text***.

Note 1: Operations already performed in the [NDPP] 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.)

- **Case** - [NDPP] uses an additional convention which defines parts of an SFR that apply only when corresponding selections are made or some other identified conditions exist. Only the applicable cases are identified in this ST.

The TOE security functional requirements are listed in Table 11. All SFRs are based on requirements defined in Part 2 of the Common Criteria or defined in the *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 [NDPP] and changed/clarified by *Security Requirements for Network Devices Errata #3*, 3 November 2014 [ERRATA]

Table 11: TOE Security Functional Components

Functional Component		
1	FAU_GEN.1	Audit Data Generation
2	FAU_GEN.2	User Identity Association
3	FAU_STG_EXT.1	Extended: External Audit Trail Storage
4	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
5	FCS_CKM_EXT.4	Extended: Cryptographic Key Zeroization
6	FCS_COP.1 (1)	Cryptographic Operation (for data encryption/decryption)
7	FCS_COP.1 (2)	Cryptographic Operation (for cryptographic signature)
8	FCS_COP.1 (3)	Cryptographic Operation (for cryptographic hashing)
9	FCS_COP.1 (4)	Cryptographic Operation (for keyed-hash message authentication)
10	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
11	FCS_SSH_EXT.1	Extended: SSH
12	FDP_RIP.2	Full Residual Information Protection
13	FIA_PMG_EXT.1	Extended: Password Management
14	FIA_UAU.7	Protected Authentication Feedback
15	FIA_UAU_EXT.2	Extended: Password-based Authentication Mechanism
16	FIA_UIA_EXT.1	Extended: User Identification and Authentication
17	FMT_MTD.1	Management of TSF Data (for general TSF data)
18	FMT_SMF.1	Specification of Management Functions
19	FMT_SMR.2	Restrictions on Security Roles
20	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
21	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)
22	FPT_STM.1	Reliable Time Stamps
23	FPT_TST_EXT.1	Extended: TSF Testing
24	FPT_TUD_EXT.1	Extended: Trusted Update
25	FTA_SSL.3	TSF-initiated Termination
26	FTA_SSL.4	User-initiated Termination
27	FTA_SSL_EXT.1	Extended: TSF-initiated Session Locking
28	FTA_TAB.1	Default TOE Access Banners
29	FTP_ITC.1	Inter-TSF Trusted Channel
30	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;
d) Specifically defined auditable events listed in Table 12.

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 12.

Table 12: Auditable Events (Table 1 of the NDPP)

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	Start-up and shutdown of the audit functions; All auditable events for the not specified level of audit; and All administrative actions;	No additional information.
FAU_GEN.2	None.	No additional information.
FAU_STG_EXT.1	None.	No additional information.
FCS_CKM.1	None.	No additional information.
FCS_CKM_EXT.4	None.	No additional information.
FCS_COP.1 (1)	None.	No additional information.
FCS_COP.1 (2)	None.	No additional information.
FCS_COP.1 (3)	None.	No additional information.
FCS_COP.1 (4)	None.	No additional information.
FCS_RBG_EXT.1	None.	No additional information.
FCS_SSH_EXT.1	Failure to establish an SSH session	Reason for failure
	Establishment/Termination of an SSH session	Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_RIP.2	None.	No additional information.
FIA_PMG_EXT.1	None.	No additional information.
FIA_UAU.7	None.	No additional information.
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FMT_MTD.1	None.	No additional information.
FMT_SMF.1	None.	No additional information.
FMT_SMR.2	None.	No additional information.
FPT_APW_EXT.1	None.	No additional information.
FPT_SKP_EXT.1	None.	No additional information.
FPT_STM.1	Changes to the time.	The old and new values for the time.
		Origin of the attempt (e.g., IP address).
FPT_TST_EXT.1	None.	No additional information.
FPT_TUD_EXT.1	Initiation of update.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.
FTA_SSL.4	The termination of an interactive session.	No additional information.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_TAB.1	None.	No additional information.
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 Extended: External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to ***[transmit the generated audit data to an external IT entity]*** using a trusted channel implementing the ***[SSH]*** protocol.

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 used for key establishment in accordance with

[

- ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***

]

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

6.1.2.2 FCS_CKM_EXT.4 Extended: Cryptographic Key Zeroization

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

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

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

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

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

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

[RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater]
that meets the following:

Case: RSA Digital Signature Algorithm

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

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

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

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

FCS_COP.1.1 (4) The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC***-[SHA-1, SHA-256],*** key size ***[160, 256 bit],*** and message digest sizes ***[160,***

256] bits that meet the following: FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code", and FIPS PUB 180-3, "Secure Hash Standard".

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

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

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

6.1.2.8 FCS_SSH_EXT.1 Extended: SSH

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

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

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, ***[no other algorithms].***

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

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is ***[hmac-sha1, hmac-sha1-96, hmac-sha2-256].***

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

6.1.3 *User Data Protection (FDP)*

6.1.3.1 FDP_RIP.2 Full Residual Information Protection

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

6.1.4 *Identification and Authentication (FIA)*

6.1.4.1 FIA_PMG_EXT.1 Extended: Password Management

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

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

2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

6.1.4.2 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.

6.1.4.3 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, ***[[remote public-key (SSH) authentication mechanism]]*** to perform administrative user authentication.

6.1.4.4 FIA_UIA_EXT.1 Extended: 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.

6.1.5 *Security Management (FMT)*

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

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

6.1.5.2 FMT_SMF.1 Specification of Management Functions

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

- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using ***[published hash]*** capability prior to installing those updates;
- ***[***
    - ***Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;***
    - ***Ability to configure the cryptographic functionality.***

  ]

6.1.5.3 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- Authorized Administrator.

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

FMT_SMR.2.3 The TSF shall ensure that the conditions:

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

are satisfied.

6.1.6 *Protection of the TSF (FPT)*

6.1.6.1 FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

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

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

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

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

6.1.6.3 FPT_STM.1 Reliable Time Stamps

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

6.1.6.4 FPT_TST_EXT.1: Extended: TSF Testing

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

6.1.6.5 FPT_TUD_EXT.1 Extended: Trusted Update

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

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

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

6.1.7 *TOE Access (FTA)*

6.1.7.1 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.

6.1.7.2 FTA_SSL.4 User-initiated Termination

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

6.1.7.3 FTA_SSL_EXT.1 Extended: 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.

6.1.7.4 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.

6.1.8 *Trusted Path/Channels (FTP)*

6.1.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall use ***[SSH]*** 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].***

6.1.8.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall use ***[SSH]*** provide a trusted communication path between itself and remote administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and detection of modification of the communicated data.

FTP_TRP.1.2 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 4 and Appendix C of the *U.S. Government Standard Protection Profile for Network Devices*, [NDPP] as changed/clarified by [ERRATA]. The TOE Security Assurance Requirements, summarized in the table below, identify the management and evaluative activities required to address the threats identified in [NDPP].

Table 13: [NDPP] 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 14: 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 15: 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 16: 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 17: 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 18: 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 19: 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 20: 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 [NDPP], 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.

6.2.3 *Extended Assurance Activities*

The following subsections define the explicit assurance activities presented in the [NDPP] and [ERRATA] for applicable SAR families. These assurance activities serve to refine the standard SARs previously stated with specific activities to be performed by the evaluators during the course of their evaluation.

6.2.3.1 Class ADV Assurance Activities

Introduction

The functional specification describes the Target Security Functions Interfaces (TSFIs). It is not necessary to have a formal or complete specification of these interfaces. Additionally, because TOEs conforming to this PP will necessarily have interfaces to the Operational Environment that are not directly invokable by TOE users, there is little point specifying that such interfaces be described in and of themselves since only indirect testing of such interfaces may be possible. For this PP, the activities for this family should focus on understanding the interfaces presented in the TSS in response to the functional requirements and the interfaces presented in the AGD documentation. No additional “functional specification” documentation is necessary to satisfy the assurance activities specified.

The interfaces that need to be evaluated are characterized through the information needed to perform the assurance activities listed, rather than as an independent, abstract list.

ADV_FSP.1 Activities

There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described in [NDPP] Section 4.2, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided.

6.2.3.2 Class AGD Assurance Activities

Introduction

The guidance documents will be provided with the developer’s security target. Guidance must include a description of how the authorized user verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by an authorized user.

Guidance must be provided for every operational environment that the product supports as claimed in the ST. This guidance includes

- instructions to successfully install the TOE in that environment; and
- instructions to manage the security of the TOE as a product and as a component of the larger operational environment.

Guidance pertaining to particular security functionality is also provided; specific requirements on such guidance are contained in the assurance activities specified in [NDPP] Section 4.2.

AGD_OPE.1 Activities

Some of the contents of the operational guidance will be verified by the assurance activities in [NDPP] Section 4.2 and evaluation of the TOE according to the CEM. The following additional information is also required.

The operational guidance shall at a minimum list the processes running (or that could run) on the TOE in its evaluated configuration during its operation that are capable of processing data received on the network interfaces (there are likely more than one of these, and this is not limited to the process that "listens" on the network interface). It is acceptable to list all processes running (or that could run) on the TOE in its evaluated configuration instead of attempting to determine just those that process the network data. For each process listed, the administrative guidance will contain a short (e.g., one- or two-line) description of the process' function, and the privilege with which the service runs. "Privilege" includes the hardware privilege level (e.g., ring 0, ring 1), any software privileges specifically associated with the process, and the privileges associated with the user role the process runs as or under.

The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

The documentation must describe the process for verifying updates to the TOE, either by checking the hash or by verifying a digital signature. The evaluator shall verify that this process includes the following steps:

1. For hashes, a description of where the hash for a given update can be obtained. For digital signatures, instructions for obtaining the certificate that will be used by the FCS_COP.1 (2) mechanism to ensure that a signed update has been received from the certificate owner. This may be supplied with the product initially, or may be obtained by some other means.

2. Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).

3. Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the hash/digital signature.

The TOE will likely contain security functionality that does not fall in the scope of evaluation under this PP. The operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities.

AGD_PRE.1 Activities

As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.

6.2.3.3 Class ALC Assurance Activities

Introduction
At the assurance level provided for TOEs conformant to this PP, life-cycle support is limited to end-user-visible aspects of the life-cycle, rather than an examination of the TOE vendor's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it is a reflection on the information to be made available for evaluation at this assurance level.

ALC_CMC.1 Activities
The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. The evaluator shall ensure that this identifier is sufficient for an acquisition entity to use in procuring the TOE (including the appropriate administrative guidance) as specified in the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

ALC_CMS.1 Activities
The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

6.2.3.4 Class ATE Assurance Activities

Introduction
Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through the ATE_IND family, while the latter is through the AVA_VAN family. At the assurance level specified in this PP, testing is based on advertised functionality and interfaces with dependency on the availability of design information. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

ATE_IND.1 Activities
The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluator must document in the test plan that each applicable testing requirement in the ST is covered.

The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated.

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a “fail” and “pass” result (and the supporting details), and not just the “pass” result.

6.2.3.5 Class AVA Assurance Activities

Introduction

The evaluation lab is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products. In most cases, these vulnerabilities will require sophistication beyond that of a basic attacker. Until penetration tools are created and uniformly distributed to the evaluation labs, the evaluator will not be expected to test for these vulnerabilities in the TOE. The labs will be expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used in the development of penetration testing tools and for the development of future protection profiles.

AVA_VAN.1 Activities

As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in network infrastructure devices and the implemented communication protocols in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on boot-up, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.

6.2.4 *Extended Assurance Activities*

The extended assurance activities define the explicit activities specified in the [NDPP] and [ERRATA] for applicable SFR and SAR elements. These activities are detailed in the Assurance Activity Report [AAR].

6.3 Rationale

This ST claims Exact Compliance to *U.S. Government Standard Protection Profile for Network Devices*, 08 June 2012, Version 1.1 [NDPP] as changed/clarified by *Security Requirements for Network Devices Errata #3*, 3 November 2014 [ERRATA]. 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 NDPP. For extended components that were derived from SFRs from CC Part 2 dependencies were based on unmodified SFRs. For extended components without baseline equivalent, no dependency was specified.

Table 21: 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	FAU_GEN.1
FCS_CKM.1	FCS_COP.1 FCS_CKM.4	FCS_COP.1 (2) FCS_CKM._EXT.4
FCS_CKM_EXT.4	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM_EXT.4
FCS_COP.1 (1)	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM_EXT.4
FCS_COP.1 (2)	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM_EXT.4
FCS_COP.1 (3)	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM_EXT.4
FCS_COP.1 (4)	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 FCS_CKM_EXT.4

FCS_RBG_EXT.1	n/a	
FCS_SSH_EXT.1	n/a	
FDP_RIP.2	none	
FIA_PMG_EXT.1	n/a	
FIA_UAU.7	FIA_UAU.1	FIA_UIA_EXT.1
FIA_UAU_EXT.2	FIA_UID.1	FIA_UIA_EXT.1
FIA_UIA_EXT.1	n/a	
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_APW_EXT.1	n/a	
FPT_STM.1	none	
FPT_SKP_EXT.1	n/a	
FPT_TST_EXT.1	none	
FPT_TUD_EXT.1	n/a	
FTA_SSL.3	none	
FTA_SSL.4	none	
FTA_SSL_EXT.1	FIA_UAU.1	FIA_UIA_EXT.1
FTA_TAB.1	none	
FTP_ITC.1	none	
FTP_TRP.1	none	

7 TOE Summary Specification

This chapter describes the security functions:

Table 22: 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_EXT.4
	FCS_COP.1 (1-4)
	FCS_RBG_EXT.1
	FCS_SSH_EXT.1
7.3 User Data protection	FDP_RIP.2
7.4 Identification and Authentication	FIA_UIA_EXT.1
	FIA_UAU_EXT.2
	FIA_PMG_EXT.1
	FIA_UAU.7
7.5 Security Management	FMT_MTD.1
	FMT_SMF.1
	FMT_SMR.2
7.6 Protection of the security functionality	FPT_APW_EXT.1
	FPT_STM.1
	FPT_SKP_EXT.1
	FPT_TST_EXT.1
	FPT_TUD_EXT.1
7.7 TOE access	FTA_SSL.3
	FTA_SSL.4
	FTA_SSL_EXT.1
	FTA_TAB.1
7.8 Trusted path/channels	FTP_ITC.1
	FTP_TRP.1

7.1 Security Audit

FAU_GEN.1, FAU_GEN2, FAU_STG_EXT.1, FPT_STM.1

The TOE generates syslog-conformant audit records for security related events such as administrative action and secure channel establishment in accordance to Table 12 Auditable Events. The audit records reflect a wide range of circumstances, including warnings about the state of device and a variety of security relevant events. TOE supports eight levels of events: emergencies, alerts, critical, errors, warnings, notifications, informational, and debugging. The authorized 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 log 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.

Up to 500 audit records can be stored locally on the appliance depending on administrator defined logging buffer size. When the logging buffer size is set to 524288 then at least 500 audit records (a record is1024 bytes) are saved. On-device audit records exist in a circular buffer; when the buffer gets full, the oldest message is overwritten first. The viewing of the local audit events is restricted to authorized administrators using the appropriate CLI commands. In this way, the audit records are protected against unauthorized access.

The TOE is designed to securely forward audit records to a designated Syslog server over a persistent trusted channel. This trusted channel is implemented with a reverse SSH tunnel that uploads audit records as they generated. If the connection to the external Syslog server is lost, the TOE continues to save local audit logs so there is no loss of audit. However, when the connection to the syslog server is restored the TOE only forwards the newly generated audit records to the syslog. There is no automated log reconciliation process (syncing) between the locally stored records with the syslog server upon the re-establishment of the connection.

The TOE implements a hardware clock that is used to provide a reliable time stamps, the logs can be shown with the actual date and time of the system.

7.2 Cryptography

FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1 (1-4), FCS_RBG_EXT.1, FCS_SSH_EXT.1

The Dell Networking OS v9.6 exclusively relies on the Dell OpenSSL Cryptographic Library Version 2.1 to implement all cryptographic security functionality. The Dell OpenSSL Cryptographic Library Version 2.1 is covered by the following Cryptographic Algorithm Validation Program (CAVP) certificates:

Table 23: Dell Networking Platforms Cryptography

Requirement Class	Requirement Component	Dell Networking Platforms Implementation	Certificate #

FCS: Cryptographic Support	FCS_CKM.1 Cryptographic Key Generation	Implemented by the cryptographic module operating in the FIPS mode. TOE generates all host keys used for key establishment in accordance with NIST SP 800-56B.	RSA #1560
	FCS_CKM_EXT.4 Cryptographic Key Zeroization	Zeroization of all CSP is performed by the cryptographic module.	n/a
	FCS_COP.1(1) Cryptographic Operation (encryption/decryption)	AES-CBC-128 and AES-CBC-256 for data encryption/decryption implemented to meet FIPS PUB 197, “Advanced Encryption Standard (AES)” in compliance with NIST SP 800-38A. Encryption/decryption performed by the cryptographic module operating in the FIPS mode.	AES #2971
	FCS_COP.1(2) Cryptographic Operation (cryptographic signature)	RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater in compliance with FIPS PUB 186-3, “Digital Signature Standard”. Cryptographic signature functionality is performed by the cryptographic module.	RSA #1560
	FCS_COP.1(3) Cryptographic Operation (cryptographic hashing)	SHA-1 and SHA-256 cryptographic hashing implemented to meet FIPS PUB 180-3, “Secure Hash Standard” is performed by the cryptographic module operating in the FIPS mode.	SHA #2497
	FCS_COP.1(4) Cryptographic Operation (keyed-hash message authentication)	HMAC-SHA1 and HMAC-SHA2-256 keyed-hash message authentication implemented to meet FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code”, and FIPS PUB 180-3, “Secure Hash Standard” is performed by the cryptographic module operating in the FIPS mode.	HMAC #1883
	FCS_RBG_EXT.1 Cryptographic Operation (random bit generation)	CTR_DRBG (AES-256) random bit generation implemented to meet NIST SP 800-90 is performed by the cryptographic module running in the FIPS mode.	DRBG #565
	FCS_SSH_EXT.1 SSH	TOE implements SSHv2 protocol and supports public key-based or 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

The TOE uses a software-based random bit generator that complies with NIST Special Publication 800-90 when operating in the FIPS mode. The entropy source is a 256-bit value provided by the Linux Kernel Random Number Generator (LKRNG) extracted from multiple noise sources. The noise sources for the TOE include persistent storage input/output and inter-process communications events, both are software sources. The entropy is not preserved across system reboots and accumulated each time the TOE is started.

The TOE generally fulfills all of the NIST SP 800-56B 'Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography' requirements without extensions, with the following table documenting specific conformance to the publication:

Table 24: NIST SP 800-56B implementation

NIST SP500-56B Section Reference	"should", "should not", or "shall not"	Implemented accordingly?	Rationale for deviation
5.6	Should	Yes	
5.8	Shall Not	No	RSA-OAEP is not supported. RSA PKCS#1 v1.5 padding is used
5.9	Shall Not (1st instance)	Yes	
5.9	Shall Not (2nd instance)	Yes	
6.1	Should Not	Yes	
6.1	Should (1st instance)	Yes	
6.1	Should (2nd instance)	Yes	
6.1	Should (3rd instance)	Yes	
6.1	Should (4th instance)	Yes	
6.1	Shall Not (1st instance)	Yes	
6.1	Shall Not (2nd instance)	Yes	
6.2.3	Should	Yes	
6.5.1	Should	Yes	
6.5.2	Should	Yes	
6.5.2.1	Should	Yes	
6.6	Shall Not	Yes	
7.1.2	Should	Yes	
7.2.1.3	Should	Yes	
7.2.1.3	Should Not	Yes	
7.2.2.3	Shall Not	No	RSA-OAEP is not supported. RSA PKCS#1 v1.5 padding is used

NIST SP500-56B Section Reference	"should", "should not", or "shall not"	Implemented accordingly?	Rationale for deviation
7.2.2.3	Should (1st instance)	No	RSA-OAEP is not supported. RSA PKCS#1 v1.5 padding is used
7.2.2.3	Should (2nd instance)	No	RSA-OAEP is not supported. RSA PKCS#1 v1.5 padding is used
7.2.2.3	Should (3rd instance)	No	RSA-OAEP is not supported. RSA PKCS#1 v1.5 padding is used
7.2.2.3	Should (4th instance)	No	RSA-OAEP is not supported. RSA PKCS#1 v1.5 padding is used
7.2.2.3	Should Not	No	RSA-OAEP is not supported. RSA PKCS#1 v1.5 padding is used
7.2.3.3	Should (1st instance)	No	RSA-KEM-KWS (Key Wrapping Scheme) is not supported
7.2.3.3	Should (2nd instance)	No	RSA-KEM-KWS (Key Wrapping Scheme) is not supported
7.2.3.3	Should (3rd instance)	No	RSA-KEM-KWS (Key Wrapping Scheme) is not supported
7.2.3.3	Should (4th instance)	No	RSA-KEM-KWS (Key Wrapping Scheme) is not supported
7.2.3.3	Should (5th instance)	No	RSA-KEM-KWS (Key Wrapping Scheme) is not supported
7.2.3.3	Should Not	No	RSA-KEM-KWS (Key Wrapping Scheme) is not supported
8	Should	Yes	
8.3.2	Should Not	Yes	

The TOE is designed to zeroize CSPs to mitigate the possibility of disclosure or modification. 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 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 zeroize CSPs (e.g. private RSA keys) that can be invoked by an authorized administrator with a sufficient privilege level. The following table identifies applicable CSPs and summarizes zeroization procedure:

Table 25: Dell Networking Platforms CSPs

Identifier	Name	Generation / Algorithm	Purpose	Storage Location	Zeroization Summary
CSP1	SSH Host key	ANSI X9.31 / RSA	RSA key	NVRAM, RAM (plain text)	•Read the SSH host key: On start of the SSH daemon, NVRAM is read to get the SSH key that was saved from the last key generation. •Generate/Write the SSH host key: Generate a key upon CLI command. The key is stored in RAM. It is also stored (by overwriting it) in NVRAM (in the same function). Next time TOE starts the SSH daemon, the key is read from NVRAM. •Clear the SSH host key through zeriozation command: The RAM and NVRAM are cleared (zeroized) in the same function and manner. Very similar behavior between RAM and NVRAM – they are written at the same time. Reading is slightly different only because NVRAM is read during startup. When key is re-generated, NVRAM and RAM are re-written. Key is read from RAM once SSH is started.
CSP2	SSH Session Keys	ANSI X9.31 / AES-CBC-128 AES-CBC-256	SSH keys – server to client, client to server	RAM (plain text)	Session keys are removed and new keys assigned upon rekeying. Overwritten with 0x00.
CSP3	Diffie-Hellman Key Pair	ANSI x9.31 / DH	Key agreement for SSH sessions	RAM (plain text)	Cleared when device is powered down or as part of session termination. Overwritten by loss of capacitor charge in the memory cell

Identifier	Name	Generation / Algorithm	Purpose	Storage Location	Zeroization Summary
CSP4	Username / Passwords	MD5	Critical security parameters 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 file in protected 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 with 0x00.
CSP5	PRNG Seed key	Entropy	Seed key for PRNG	RAM (plain text)	Cleared when device is powered down or during reboot by the new seed. Overwritten by loss of capacitor charge in the memory cell.

TOE implements the SSHv2 secure communication protocol that complies with RFCs 4251, 4252, 4253, 4254, 6668. The SSHv2 implemented with AES-CBC-128 or AES-CBC-256 ciphers 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. The TOE supports SSHv2 with password-based authentication and allows users to upload and add RSA keys to user’s list of authorized keys for public-key authentication.

TOE cryptographic module is capable of supporting other encryption algorithms, key-hash methods, and key exchange algorithms but they are not used with the SSH protocol and are not part of the evaluated configuration. Packets that exceed 256K in length size are dropped at the application layer per RFC 4253.

7.3 User Data protection

FDP_RIP.2

The TOE implements multiple measures to protect data integrity and to ensure residual information is not transmitted. All network packets are stored in the buffer pool that only exists in the volatile memory. To protect from inadvertent reuse, all network packets travelling through the TOE are stored in this managed buffer. When a packet is received, the exact size of the packet is known and just-large-enough memory block is allocated from available memory space. Metadata is written to the buffer along with the actual packet. Both large and standard network packets are handled the same way, with large packets requiring larger memory blocks. Packets that exceed 256K in length size are dropped at the application layer per RFC 4253. Once the packet has been either transmitted or discarded, the memory used for that packet is returned back to the pool for reuse. The metadata in the buffer is completely overwritten with new metadata for the new received packet. Metadata is never transmitted. Any possible remainder in the packet buffer(s) from the previously held packet is not transmitted or used in processing.

The TOE can be configured to use cut-through switching method, where the process of forwarding a frame starts as soon as the destination is processed but before whole frame has been received. Packets that are received and transmitted through the fast path are not copied up to the control plane. This switch processor has its embedded software and hardware mechanisms to ensure that data from the received packets is not accessible once they have been processed and transmitted or discarded. The switch processor has its own memory space that it uses for packet memory and it manages the use of this memory pool for ingress and egress processing.

7.4 Identification and Authentication

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

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 other management action, except to view the warning banner. The warning banner is displayed before login prompt on any of the management access points (local console or remote SSH sessions). In the evaluated configuration, the TOE does not allow unauthenticated management configuration of the TOE's network routing/switching services.

A requesting user will be prompted to enter a user name and password or present an authorized certificate upon successful connection. The TOE will then compare entered user name/password or certificate 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 session.

For a local administrative session, password character entries are not echoed to the screen. For a remote administrative session, credentials are protected by encrypted 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 that command, then command authorization is granted. Many users can have 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.

The TOE can be configured to authenticate by SSH public key mechanism (RSA) or password-based as defined in RFC 4252. When RSA authentication is used, TOE authenticates administrators against authorized keys database. Upon successful authentication, the TOE assigns administratively defined role to that user for the duration of the session.

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.

7.5 Security Management

FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

The TOE allows remote administration using an SSH 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 done over command-line interface (CLI) that provides access to all management functions used to administer the TOE.

Remote management using web interface (Secure HTTP or HTTPS) is excluded. The TOE does not satisfy all NDPP requirements for this administrative interface and it is disabled in the evaluated configuration.

By default, TOE supports three main modes:

- EXEC mode: This mode allows the administrator to view settings and enter EXEC Privilege mode, which is used to configure the device.
- EXEC Privilege mode: This mode allows the administrator to access all the commands accessible in EXEC mode plus commands to view configurations, manage configuration files, and enter the CONFIGURATION mode to configure interfaces, routes and protocols on the switch.
- CONFIGURATION mode: This mode allows the administrator to configure security features, time settings, and set logging. 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 authorized administrators of the TOE. Authorized 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 Section 6.1.5.2 FMT_SMF.1 'Specification of Management Functions'.

The term "authorized administrator" is used to refer to any administrative user with the appropriate role with sufficient privilege to perform all relevant functions. It is understood that not all administrators will have sufficient permissions assigned to them to perform each administrative function discussed in this document.

7.6 Protection of the security functionality

FPT_APW_EXT.1, FPT_SKP_EXT.1, FPT_STM.1, FPT_TST.1, FPT_TUD.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. encryption) to protect remote administration.

The TOE protects critical security parameters (CSP) such as stored passwords and cryptographic keys so they are not directly accessible in plaintext. Locally stored password information is obscured by use of hashing (MD5). 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 both log accountability (i.e audit generation), synchronization functions, and session idle time out functionality.

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 syslog 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-test. 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.

Upgrading Dell Networking OS is a multi-step process performed by an authorized administrator. An authorized user must authenticate to the 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. The image file, now located on the appliance, is then verified using the “verify” CLI which produces a SHA-256 hash value. The administrator must then visually compare the results to the published hash value on the Dell website. Upon successful comparison, the administrator can then initiate the upgrade.

7.7 TOE access

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

The TOE allows remote and local administrative access using command-line. 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.`

7.8 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 through a dedicated RJ-45 LAN management port. The TOE prevents disclosure or modification of logs by establishing a trusted channel (using SSH) between itself and the syslog server. To implement trusted path/secure channel, the TOE uses SSHv2 protocol with password-based or public key-based authentication. For password-based authentication, a user authenticated against user and role database. For public key-based authentication, SSH keys (RSA) are compared to the authorized keys database.

The TOE implements an encrypted communication channel between itself, audit servers, and remote administrators. This channel is implemented using SSHv2 protocol compliant with all applicable standards. 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, diffiehellman-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.

8 Acronyms and Terminology

8.1.1 *Acronyms*

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

Table 26: 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 27: 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.