Aruba 2920 Switch Series
Security Target

Version 1.7

August 25th, 2016

Prepared For:

HPE Networking
153 Taylor Street
Littleton, MA 01460

Prepared By

1000 Innovation Drive ♦Kanata, ON K2K 3E7♦703 848-0883♦Fax 703 848-0985

Note: On December 1, 2015, Hewlett Packard Enterprise became two separate companies: Hewlett Packard Enterprise and HP Inc. The network products are part of the new Hewlett Packard Enterprise. In addition, in December 2015, the acquisition of Aruba Networks by Hewlett Packard Enterprise became finalized.

The former HP ProCurve / ProVision network switches are undergoing product rebranding. The rebranding is not complete in the documentation and on the websites. The TOE maybe referred to with the suffix “HP” or “HPE” or the TOE maybe referred to as “ProCurve” or “Aruba”. The NOS maybe referred to as “ProVision” or “ArubaOS”.
For the purpose of this evaluation, these name variations are used interchangeably and refer to the same product.

Table of Contents

Figures and Tables

1 Security Target Introduction

1.1 Security Target Reference

ST Title: Aruba 2920 Switch Series Security Target

ST Version: v1.7

ST Author: CygnaCom Solutions Inc.

ST Date: 08/25/2016

1.2 TOE Reference

TOE Developer: HPE

Evaluation Sponsor: HPE

TOE Identification: Aruba 2920 Switch Series, Version 5.011, WB_15_18_0011I

Platforms	Specific Devices
Aruba 2920 Switch Series	Aruba 2920-24G (J9726A)
	Aruba 2920-24G-PoE+ (J9727A)
	Aruba 2920-48G (J9728A)
	Aruba 2920-48G-PoE+ (J9729A)
	Aruba 2920-48G-PoE+ 740W (J9836A)

Table 1: TOE Platforms and Devices

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 protection profile: "*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 a modular Ethernet switch, based on HPE Networking ASIC, that in the evaluated configuration consists of the Aruba 2920 Switch Series. The TOE offers comprehensive Layer 2 and Layer 3 feature set including RIP, BGP, PoE+, and IPv4 and IPv6 functionalities.

The Aruba 2920 Switch Series provides security, scalability, and ease of use for enterprise edge deployments.

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 Aruba 2920 Switch Series running ArubaOS version 5.011, that includes the following appliances:

- Aruba 2920-24G
- Aruba 2920-24G-PoE+
- Aruba 2920-48G
- Aruba 2920-48G-PoE+
- Aruba 2920-48G-PoE+ 740W

While the physical form factor of each appliance in the HPE Networking family may vary, the underlying hardware and software share a similar architecture. The software utilizes a common code base of a modular nature, with only the modules applicable for the specific hardware loaded.

Aruba 2920-24G
This model contains 24 10/100/1000Mbps ports including four that are combination / dual purpose shared with SFP ports for fiber connectivity. Each unit also has two available port module slots, 1 slot for optional stacking module, and a modular power supply.

The following are the specifications for this switch:

- Supports throughput of up to 95.2 Mpps.
- Switching capacity of 128 Gbps.
- Stacking up to 4 switches.
- The management features: CLI, out of band management (RJ-45, RS-232 or micro USB).

Aruba 2920-24G-PoE+
This model contains 24 10/100/1000Mbps ports including four that are combination / dual purpose shared with SFP ports for fiber connectivity. This model supports Power over Ethernet (PoE) and PoE+ with a 370 Watt power supply. Each nit also has two available port module slots, a stacking module slot, and an available redundant power supply slot.

The following are the specifications for this switch:

- Supports throughput up to 95.2 Mpps.
- Switching capacity is 128 Gbps.
- PoE+ capability of up to 370W PoE+.
- Stacking up to 4 switches.
- The management features: CLI, out of band management (RJ-45, RS-232 or micro USB).

Aruba 2920-48G

This model contains 48 10/100/1000Mbps ports including four that are combination / dual purpose shared with SFP ports for fiber connectivity. Each unit also has two available port module slots, 1 slot for optional stacking module, and a modular power supply.

The following are the specifications for this switch:

- Support throughput up to 130.9 Mpps.
- Switching capacity is 176 Gbps.
- Stacking up to 4 switches.
- The management features: CLI, out of band management (RJ-45, RS-232 or micro USB).

Aruba 2920-48G-PoE+
This model contains 48 10/100/1000Mbps ports including four that are combination / dual purpose shared with SFP ports for fiber connectivity. The model supports Power over Ethernet (PoE) and PoE+ with a 370 Watt power supply. Each unit also has two available port module slots, 1 slot for optional stacking module and a modular power supply.

The following are the specifications for this switch:

- Supports throughput up to 130.9 Mpps.
- Switching capacity is 176 Gbps.
- PoE+ capability of up to 370W PoE+.
- Stacking up to 4 switches.
- The management features: CLI, out of band management (RJ-45, RS-232 or micro USB).

Aruba 2920-48G-PoE+ 740W
This model contains 48 10/100/1000Mbps ports including four that are combination / dual purpose shared with SFP ports for fiber connectivity. The model supports Power over Ethernet (PoE) and PoE+ with a 740 Watt power supply. Each unit also has two available port module slots, 1 slot for optional stacking module and a modular power supply 740W of PoE+ Power.

The following are the specifications for this switch:

- Supports throughput up to 130.9 Mpps.
- Switching capacity is 176 Gbps.
- PoE+ capability of up to 740W PoE+.
- Stacking up to 4 switches.
- The management features: CLI, out of band management (RJ-45, RS-232 or micro USB).

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, ArubaOS is shared across all platforms. The TOE's firmware version is WB_15_18_0011l.

ArubaOS is composed of Greenhills Integrity OS with additional components / 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. A dedicated cryptographic library provides functionality that implements secure channel and protects critical security parameters. The control plane subsystem includes an IP host stack, which can be further subdivided into protocol and control layers, implements switching and routing functions. The system management subsystem, that includes an AAA module, implements administrative interface and maintains configuration information for the TOE.

1.4.2 *TOE Components*

1.4.2.1 Hardware

The TOE consists of the following hardware:

Platforms	Models	Processor
Aruba 2920 Switch Series	Aruba 2920-24G	ARM1176
	Aruba 2920-24G-PoE+	ARM1176
	Aruba 2920-48G	ARM1176
	Aruba 2920-48G-PoE+	ARM1176
	Aruba 2920-48G-PoE+ 740W	ARM1176

Table 2: Networking appliances

1.4.2.2 Software

The TOE runs ArubaOS. 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.

1.4.2.3 Management Interface(s)

The TOE supports remote and local management via a Command Line Interface (CLI). The CLI is accessible via a directly connected RJ-45 cable or a remote connection secured by SSHv2.

1.4.3 *Physical Boundary of the TOE*

The physical boundary of the TOE is the hardware appliance itself running ArubaOS version 5.011.

1.4.4 *Operational Environment*

The Operational Environment of the TOE includes:

- The client software that used to access management interface
- The workstation that hosts the client software
- External IT servers:
  - Syslog for external storage of audit logs
  - SNTP for synchronizing system time
  - DNS server

- The TOE Boundary depicted in the following figure:

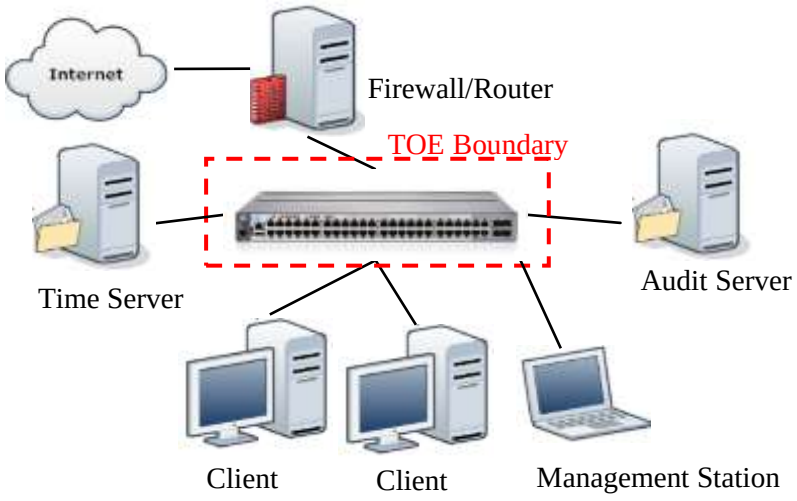

Figure 1: TOE Boundary

1.4.5 *Logical Boundary of the TOE*

The logical boundary of the TOE is defined by implemented security functions as summarized in the Section 1.3.3 of this document. These security functions are further described in the following subsections.

1.4.5.1 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 for viewing by Managers and Operators, and

can be sent securely to a designated syslog server for archiving. The logs can be viewed by Operators and Managers using the appropriate CLI commands. The TOE also implements timestamps to ensure reliable audit information is available using the appropriate CLI commands.

1.4.5.2 Cryptographic Support

The TOE implements the following cryptographic protocols:

- SSHv2 and TLS

The TOE implements the SSHv2 protocol and supports public key-based or password-based authentication with following parameters:

- AES-CBC-128, AES-CBC-256, for data encryption
- SSH_RSA for public-key authentication
- hmac-sha1 for data integrity
- diffie-hellman-group14-sha1 for key exchange

The TOE implements TLS v1.0 protocols and supports the following ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

The TOE implements the following cryptographic functionality:

- Random bit generation using CTR_DRBG(AES) seeded with 256 bits of entropy
- Zeroization of Critical Security Parameters

The TOE uses the cryptographic library to manage Critical Security Parameters (CSPs), by implementing zeroization procedures to mitigate the possibility of disclosure or modification of CSPs. Additionally, the TOE implements commands for on-demand zeroization of CSPs (e.g. private RSA keys) that can be invoked by an authorized administrator with sufficient permissions based on their role.

1.4.5.3 User Data Protection

The TSF ensures that network packets sent from the TOE do not include data “left over” from processing the previous network information.

1.4.5.4 Identification and Authentication

The TOE enforces password-based authentication (RBAC) before allowing access to the command line and menu interfaces. 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 TOE enhances user login security by masking passwords during entry on user login.

1.4.5.5 Security Management

The TOE supports role-based access to the administrative interfaces and management functions. The TOE provides the following management interfaces: a Command Line Interface (CLI), a Menu Interface, and a physical console available on the front panel of the switch appliance. The TOE supports the following roles: Manager, Operator. Both remote and local administration are accomplished over the CLI. that provides access to all management functions used to administer the TOE only for the manager role.

1.4.5.6 Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features. The TOE protects CSPs such as stored passwords and cryptographic keys so they are not directly accessible 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 operation environment. The TOE performs self-tests to detect failure and protect itself from malicious updates.

1.4.5.7 TOE Access

The TOE displays a banner regarding unauthorized use of the TOE before establishing a user session. Banners are customer configurable. The TOE will also terminate a user's session after an administrator-configured period of inactivity. Once a session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

1.4.5.8 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 using the TLS protocol. To implement a trusted path/secure channel the TOE uses SSHv2 protocol.

1.4.6 *Excluded Functionality*

The TOE supports a number of features that are not part of the core functionality. Those features are excluded from 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.
- Routing protocols that integrate authentication or encryption such as Routing Information Protocol (RIPv2), Open Shortest Path First (OSPFv2), and Border Gateway Protocol (BGP). RFC-compliant implementations are unable to satisfy NDPP cryptographic requirements.

- Use of telnet is excluded and it is disabled by default.
- Use of the SFTP server is excluded.
- Use of the SNMPv1 and SNMPv2 functionality is excluded and it is disabled by default. The use of SNMPv3 with read-only community strings is not restricted in the evaluated configuration; however, it is not evaluated.

1.4.7 *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
HPE Switch Software Management and Configuration Guide	[ADMIN]
Aruba 2920 Switch Series CC Configuration Guide	[CC Addendum]
HPE Switch Software Basic Operation Guide	[BOP]

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	[ERRATA3]
U.S. Government Standard Protection Profile for Network Devices, Version 1.1, 08 June 2012	[NDPP]
HPE 2920 Switch Series Datasheet	[PS]
HPE Switch Software Basic Operation Guide	[BOP]
HPE Switch Software Management and Configuration Guide	[ADMIN]

2 Conformance Claims

2.1 Common Criteria Conformance Claim

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

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

2.2 Protection Profile Claim

The TOE claims *exact* Compliance to *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 [ERRATA3]

2.3 Package Claim

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

2.4 Conformance Rationale

This ST claims strict conformance to only one Protection Profile [PP] – the NDPP.

The security problem definition of this ST is consistent with the statement of the security problem definition 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.

2.5 Relevant Technical Decisions

- TD0004: FCS_TLS_EXT Man-in-the-Middle Tests
- TD0011: Clarification on FCS_SSH_EXT.1.4
- TD0012: FCS_SSH_EXT.1 Conflict Resolution
- TD0017: NDPP Audit Shutdown
- TD0019: Testing Data Channel Modification for FTP_ITC.1 and FTP_TRP.1
- TD0026: Update to FPT_TUD_EXT.1

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 specified in the Protection Profile, 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 specified in the Protection Profile, 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 specified in the Protection Profile, 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 specified in the Protection Profile, 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 specified in the Protection Profile, 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] and clarified by *Security Requirements for Network Devices Errata #3*, 3 November 2014 [ERRATA3].

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)
5	FCS_SSH_EXT.1	Explicit: SSH
6	FCS_TLS_EXT.1	Explicit: TLS
7	FIA_PMG_EXT.1	Extended: Password Management
8	FIA_UAU_EXT.2	Extended: Password-based Authentication Mechanism
9	FIA_UIA_EXT.1	Extended: User Identification and Authentication
10	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
11	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)
12	FPT_TST_EXT.1	Extended: TSF Testing
13	FPT_TUD_EXT.1	Extended: Trusted Update
14	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 text 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: Operations already performed in the [NDPP] are not identified in this Security Target

- **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 [ERRATA3]

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)
12	FCS_SSH_EXT.1	Explicit: SSH
13	FCS_TLS_EXT.1	Explicit: TLS
14	FDP_RIP.2	Full Residual Information Protection
15	FIA_PMG_EXT.1	Extended: Password Management
16	FIA_UAU.7	Protected Authentication Feedback
17	FIA_UAU_EXT.2	Extended: Password-based Authentication Mechanism
18	FIA_UIA_EXT.1	Extended: User Identification and Authentication
19	FMT_MTD.1	Management of TSF Data (for general TSF data)
20	FMT_SMF.1	Specification of Management Functions
21	FMT_SMR.2	Restrictions on Security Roles
22	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
23	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)
24	FPT_STM.1	Reliable Time Stamps
25	FPT_TST_EXT.1	Extended: TSF Testing
26	FPT_TUD_EXT.1	Extended: Trusted Update
27	FTA_SSL.3	TSF-initiated Termination
28	FTA_SSL.4	User-initiated Termination
29	FTA_SSL_EXT.1	Extended: TSF-initiated Session Locking
30	FTA_TAB.1	Default TOE Access Banners
31	FTP_ITC.1	Inter-TSF Trusted Channel
32	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.
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**] receive and store audit data from an external IT entity using a trusted channel implementing the [**TLS**] protocol.

6.1.2 *Cryptographic Support (FCS)*

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

FCS_CKM.1.1 **Refinement**: The TSF shall generate asymmetric cryptographic keys used for key establishment in accordance with

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

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

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

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

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

FCS_COP.1.1 (2) **Refinement**: 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) **Refinement:** The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [**SHA-1, SHA-256, SHA-512**] and message digest sizes [**160, 256, 512**] 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) **Refinement:** The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[**SHA-1, SHA-256, SHA-512**], key size [***160, 256, 512 bits***], and message digest sizes [**160, 256, 512**] 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 Explicit: SSH

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, 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 ***[35000 bits]*** 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]**.

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.

6.1.2.9 FCS_TLS_EXT.1 Explicit: TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [**TLS 1.0 (RFC 2246)**] supporting the following ciphersuites:

Mandatory Ciphersuites:
TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:
[
TLS_RSA_WITH_AES_256_CBC_SHA
].

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_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.

6.1.4.3 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

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

6.1.4.4 FIA_UAU.7 Protected Authentication Feedback

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

6.1.5 *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 [**digital signature**] capability prior to installing those updates;
    - **Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;**
    - **Ability to configure the cryptographic functionality**.

]

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_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.

6.1.6.2 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.

6.1.6.3 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_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 [**digital signature mechanism**] prior to installing those updates.

6.1.6.5 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.

6.1.7 *TOE Access (FTA)*

6.1.7.1 FTA_SSL_EXT: 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.

6.1.7.1 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_TAB.1 Default TOE Access Banners

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

6.1.8 *Trusted Path/Channels (FTP)*

6.1.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 **Refinement:** The TSF shall use [**TLS**] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, ***[no other 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 Refinement: The TSF shall permit remote administrators to initiate communication via the trusted path.

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

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] and as modified by [ERRATA3]. 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 analysis

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 [ERRATA3] 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 invocable 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 ST. 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 protocol being evaluated (SSH).

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 [ERRATA3] for applicable SFR and SAR elements. These activities are detailed in the Assurance Activity Report [AAR].

7 TOE Summary Specification

This chapter describes the security functions:

- Security Audit (FAU)
- Cryptography (FCS)
- User Data Protection (FDP)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Protection of the security functionality (FPT)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

7.1 Security Audit

FAU_GEN.1
The TOE is able to generate audit records of security relevant events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function, any use of an administrator command via the CLI interface, as well as all of the events identified in Table 12. The different types of audit records that are provided by the TOE are: info, debug, warning and fatal. Audit logs are stored as strings and have a format which includes the severity, date and time of the event, the nature or type of the triggering event, an indication of whether the event succeeded, failed or had some other outcome, and the identity of the agent responsible for the event. The audit records are protected against unauthorized access by only allowing authorized users to have access to our local audit logs. The logged audit records also include event-specific content that includes at least all of the content required in Table 12.

FAU_GEN.2
All actions performed by the TOE are associated with a username, this information is maintained in the audit record, allowing the events stored there to be traced directly to the user or system for which they were performed.

FAU_STG_EXT.1, FCS_TLS_EXT.1
There is a method of specifying the minimum severity level of the audit logs that shall be sent to a syslog server. Locally stored audit logs are kept regardless of severity level. The severity level of audit is configured through the syslog server configuration. The TOE supports up to 6400 log entries locally. The local audit log is a circular buffer and when the maximum number of entries are reached, the oldest log entries shall be overwritten. Users that fail authentication do not have access to our local audit logs. By default, all event logs are sent to the set of configured syslog servers as well as the local store. The TOE uses the TLS protocol to send generated audit records to an external syslog server.

7.2 Cryptographic Support

FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1 (1-4), FCS_RBG_EXT.1, FCS_SSH_EXT.1.1-FCS_SSH_EXT_1.7, FCS_TLS_EXT.1

The TOE performs all cryptographic operations using a dedicated cryptographic library that implements all cryptographic security functionalities listed in Table 21. The TOE uses a third-party Mocana cryptographic library. All implemented algorithms have been validated to correctly function on the exact hardware and software contained in the TOE, in accordance with the NIST Cryptographic Algorithm Validation Program (CAVP). CAVP certificate numbers are listed in Table 21. The evaluated configuration requires that the TOE must use enhanced secure mode.

The cryptographic library handles random number generation for all cryptographic functionality by utilizing a deterministic random bit generator (DRBG based on AES-CTR) that is implemented according to the specifications outlined in NIST SP 800-90A and seeded from multiple software-based entropy source

Table 21: Aruba 2920 Switch Series Cryptography

Requirement Class	Requirement Component	Aruba 2920 Switch Series Implementation	Certificate
FCS: Cryptographic Support	FCS_CKM.1 Cryptographic Key Generation	Implemented by the cryptographic library operating in the enhanced secure mode. TOE generates all host keys used for key establishment in accordance with NIST SP 800-56B.	RSA:#2043
	FCS_CKM_EXT.4 Cryptographic Key Zeroization	Zeroization of all CSP is performed by the cryptographic library.	N/A
	FCS_COP.1(1) Cryptographic Operation (encryption/decryption)	AES operating in CBC, for data encryption/decryption implemented to meet FIPS PUB 197, “Advanced Encryption Standard (AES)” in compliance with NIST SP 800-38A and NIST SP800-38D. Encryption/decryption performed by the cryptographic library operating in the enhanced secure mode.	AES:#3982
	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 library.	RSA:#2043
	FCS_COP.1(3) Cryptographic Operation (cryptographic hashing)	SHA-1, SHA-256, and SHA-512 cryptographic hashing implemented to meet FIPS PUB 180-3, “Secure Hash Standard” is performed by the cryptographic library operating in the enhanced secure mode.	SHS:#3287
	FCS_COP.1(4)	HMAC-SHA-1, HMAC -SHA-256, and HMAC -SHA-	HMAC:#2598

Requirement Class	Requirement Component	Aruba 2920 Switch Series Implementation	Certificate
	Cryptographic Operation (keyed-hash message authentication)	512 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 library operating in the enhanced secure mode.	
	FCS_RBG_EXT.1 Cryptographic Operation (random bit generation)	CTR_DRBG (AES-256) random bit generation implemented to meet NIST SP 800-90A is performed by the cryptographic library running in the enhanced secure mode.	DRBG:#1175
	Component Validation Test	TLSv1.0	CVL#811
	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-sha1for data integrity • diffie-hellman-group14-sha1 for key exchange	N/A
	FCS_TLS_EXT.1	TOE implements TLS v .1.0, TLS v1.1 and TLS v1.2 using following ciphers: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA	N/A

The TOE implements the FCS_RBG_EXT (Random Bit Generation) security functional component with the following parameters: according to NIST SP 800-90A using CTR-DRBG (AES-256) seeded by an entropy source that accumulated entropy from a software-based noise.

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 22: NIST SP800-56B implementation

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented accordingly?
5.6	Should	Yes
5.8	Shall Not	Yes
5.9	Shall Not (1st instance)	Yes
5.9	Shall Not (2nd instance)	Yes

NIST SP800-56B Section Reference	"should", "should not", or "shall not"	Implemented accordingly?
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	Not Applicable
7.2.1.3	Should Not	Not Applicable
7.2.2.3	Shall Not	Yes
7.2.2.3	Should (1st instance)	Yes
7.2.2.3	Should (2nd instance)	Yes
7.2.2.3	Should (3rd instance)	Yes
7.2.2.3	Should (4th instance)	Yes
7.2.2.3	Should Not	Not Applicable
7.2.3.3	Should (1st instance)	Not Applicable
7.2.3.3	Should (2nd instance)	Not Applicable
7.2.3.3	Should (3rd instance)	Not Applicable
7.2.3.3	Should (4th instance)	Not Applicable
7.2.3.3	Should (5th instance)	Not Applicable
7.2.3.3	Should Not	Not Applicable
8	Should	Not Applicable
8.3.2	Should Not	Not Applicable

The TOE is designed to zeroize CSPs to mitigate the possibility of disclosure or modification. CSPs are stored in FLASH and cleared when no longer used.
The following table identifies applicable CSPs and the zeroization procedure for each:

Table 23: Aruba 2920 Switch Series Keys and CSP's Zeroization

Key/CSP Name	Description	Algorithm	Storage	Zeroization

Key/CSP Name	Description	Algorithm	Storage	Zeroization
User Passwords	Login credentials for authorized administrators.	Direct User Input	Flash- SHA1 RAM - plaintext	Ciphertext in nonvolatile memory is not zerorized. Plaintext in volatile memory is cleared when the device is powered down. Destroyed by loss of capacitor charge in the memory cell.
RSA private key	Identity certificates, also used in protocol negotiations.	RSA, generated using DRBG	Flash – plaintext RAM - plaintext	Private keys are over written with zeros for both volatile and non-volatile memory when no longer in use. Additionally, there is an administrative command to on-demand clear this CSP.
Public keys	Peer public keys used in authentication.	RSA, imported	FLASH -plaintext	Public keys do not need to be protected. Overwritten by a new key when updated.
Diffie-Hellman Key Pair	Key agreement for SSH	DH, generated using DRBG	RAM - plaintext	When the session is terminated, the volatile memory is over written with zeros to clear this CSP.
SSH Session Key	SSHv2 symmetric keys	AES keys, generated using KDF	RAM - plaintext	When no longer in use, the volatile memory is over written with zeros to clear this CSP.
TLS Pre-maser Secret	Key agreement for TLS	RSA or DH, generated using DRBG	RAM - plaintext	When the session is terminated, the volatile memory is over written with zeros to clear this CSP.
TLS Session Keys	TLS symmetric keys	AES keys, generated using KDF	RAM - plaintext	When no longer in use, the volatile memory is over written with zeros to clear this CSP.
DRBG Seed	Seed for PRNG	Entropy	RAM – plaintext	Cleared when the device is powered down or overwritten during reboot by the new seed. Destroyed by loss of capacitor charge in the memory cell.
Firmware Verification Certificate	Certificate used to verify the device firmware.	RSA, part of firmware	FLASH - plaintext	Public keys do not need to be protected. Overwritten by a new key as part of firmware update.

FCS_SSH_EXT.1 Extended: SSH

The TOE implements the SSHv2 protocol, compliant to the following RFCs: 4251, 4252, 4253, and 4254. The TOE supports public key-based and password-based authentication. SSH_RSA public key algorithm is used for authentication. AES-CBC-128, AES-CBC-256 algorithms are used for data encryption. hmac-sha1 are used for data integrity. Diffie-hellman-group14-sha1 is used for key exchange. There is a 32,768 bytes packet buffer and packets that exceed that size would be dropped. All implementations MUST be able to process packets with an uncompressed payload length of 32,768 bytes or less and a total packet size of 35000 bytes or less (including 'packet_length','padding_length', 'payload', 'random padding', and 'mac'). The maximum of 35000 bytes is an arbitrarily chosen value that is larger than the uncompressed length noted above. Implementations SHOULD support longer packets, where they might be needed. For example, if an implementation wants to send a very large number of certificates, the larger packets MAY be sent if the identification string indicates that the other party is able to process them. However, implementations SHOULD check that the packet length is reasonable in order for the implementation to avoid denial of service and/or buffer overflow attacks.

Each SSHv2 session is encrypted using AES encryption supporting the following cryptographic primitives: AES-CBC-128, and AES-CBC-256.

7.3 User Data protection

FDP_RIP.2

When a network packet is sent, the buffer used by the packet is recalled and managed by the buffer pool. After that, if a new packet acquires a buffer from the buffer pool, the new packet data will be used to overwrite any previous data in the buffer. If an allocated buffer exceeds the size of the packet, the additional space will be overwritten (padded) with zeroes.

7.4 Identification and Authentication

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

The TOE is designed to require users to be identified and authenticated before they can access any of the TOE functions. In the evaluated configuration, users can connect to the TOE via a local console or remotely using SSHv2. The user is required to log in prior to successfully establishing a session through which TOE functions can be exercised. Note that the only capabilities allowed prior to users authenticating are the display of the warning banner before authentication, and network switching services. When logging in the TOE will not echo passwords so that passwords are not inadvertently displayed to the user and any other users that might be able to view the login display. Note also that should a console user have their session terminated (e.g., due to inactivity), they are required to successfully authenticate, by re-entering their identity and authentication data, in order to regain access to a new session.

7.5 Security Management

FMT_MTD.1, FMT_SMF.1, FMT_SMR.2

The CLI interface provide capabilities for the authorized administrator to manage cryptographic, audit, and authentication functions and data. The TOE provides two roles: Manager (Security Administrator) and Operator. The manager user is simply the admin and has full control over the device whereas the Operator user may view status information only. Upon successful authentication to the TOE, the Manager role can manage the TSF data to carry out services such as the input of keys, creation and management of user accounts, viewing of system status, key zeroization, performing self-tests, loading new firmware, data encryption and decryption, and configuring the device into factory default settings. Note that the only capabilities allowed prior to users authenticating are the display of the warning banner before authentication.

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. 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 synchronizes the local time with an external SNTP server and Timep Server.

The time stamp is used in the following areas:

- System event logs
- Timer expiry check to kick in periodic Entropy collection
- Password change enforcement after configured timer is expired
- Timer expiry check to download new certificates
- Certificate validity checks – expiry, valid before
- Session inactivity timer checks
- Timer expiry to de authenticate/re-authenticate network clients
- Timer expiry check to clear entries from DHCP snooping database
- All administrator actions – documented in the ST
- Session creation and closing time for TLS, SSH, Telnet

- Time stamp used in crypto logs – KAT, conditional tests, password changes

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 library performs self-tests during startup; the messages are displayed on the console and syslog records generated for both successful and failed tests.

The TOE's Firmware Version is WB_15_18_0011I. Upgrading the ArubaOS firmware is a manual process performed by an authorized administrator. The firmware is digitally signed with RSA. The TOE uses the public key to verify the digital signature. The firmware is readily available on the HPE website. Uploading the firmware to the devices does require successful authentication to the devices. The downloaded image maybe uploaded to the appliances using a secure method such as secure copy. The firmware validation during the download process and will reject the firmware if validation fails. The firmware images are signed by HPE, and the HPE public certificate is stored in the running firmware.

7.7 TOE access

FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4

The TOE can be configured by an administrator to set an interactive session timeout value (any integer value in minutes and optionally in seconds). The inactivity timeout is disabled by default. This session timeout value is applicable to both local and remote sessions. A remote session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated. A local session that is similarly inactive for the defined timeout period will be terminated. The user will be required to re-enter their user id and their password so they can establish a new session once a session is terminated. If the user id and password match those of the user that was locked, the session is reconnected with the console and normal input/output can again occur for that user.

FTA_TAB.1
The TOE can be configured to display administrator-configured advisory banners. A login banner can be configured to display warning information along with login prompts. The banners will be displayed when accessing the TOE via the console, and SSH interfaces.

7.8 Trusted path/channels

FTP_ITC.1, FTP_TRP.1

The TOE can be configured to export audit records to an external syslog server. In order to protect exported audit records from disclosure or modification, the TOE utilizes TLS protocol for this purpose.

To support secure remote administration, the TOE includes an implementation of SSHv2. A remote host (presumably acting on behalf of an administrator) can initiate a secure remote connection for the purpose of security management. Note that only the local console is available by default and each of these remote administration services can be independently enabled by an administrator. In the case of SSHv2, the TOE offers a secure command line interface (CLI) interactive administrator session. An administrator with an appropriate SSHv2-capable client can establish secure remote connections with the TOE using AES-CBC-128 or AES-CBC-256, HMAC-SHA1 and diffie-hellman-group14-sha1. To successfully establish an interactive administrative session, the administrator must be able to provide acceptable user credentials (e.g., user id and password or RSA credentials), after which they will be able to issue commands within their assigned authorizations.

The TOE supports TLS version 1.0 with all claimed ciphers and no optional extensions for the use with the external audit server. The following ciphers are used:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

All of the secure protocols are supported by the cryptographic operations provided by the NIST-validated cryptographic algorithms included in the TOE implementation.

8 Acronyms and Terminology

8.1.1 *Acronyms*

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

Table 24: Acronyms

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

8.1.2 *Product Acronyms and Terminology*

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

Table 25: Terminology

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

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