Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4

Security Target

Document Version: 1.0

September 22, 2023

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Revision History

Version	Date	Changes
Version 0.1	March 28, 2022	Initial Release
Version 0.2	June 17, 2022	Updated after inputs from Symantec
Version 0.3	June 27, 2022	Updated after inputs from Symantec
Version 0.5	October 7, 2022	TD list updated and references to GUI removed.
Version 0.6	November 4, 2022	Updated after inputs from validators and CAVP cert details were added.
Version 0.7	December 6, 2022	Updated as per Observation Report
Version 0.8	February 7, 2023	Updated as per Observation Report
Version 0.9	March 28, 2023	Updated as per Observation Report
Version 1.0	August 11, 2023	Updated as per Observation Report

Table of Contents

1 INTRODUCTION 6
1.1 Security Target and TOE Reference 6
1.2 TOE Overview 6
1.3 TOE Description 8
1.3.1 Physical Boundaries 9
1.3.2 Security Functions Provided by the TOE 11
1.3.3 TOE Documentation 13
1.3.4 References 13
1.4 TOE Environment 14
1.5 TOE Minimum Deployment Requirements 14
1.6 TOE Delivery 14
1.7 Product Functionality not Included in the Scope of the Evaluation 15
2 CONFORMANCE CLAIMS 16
2.1 CC Conformance Claims 16
2.2 Protection Profile Conformance 16
2.3 Conformance Rationale 16
2.3.1 Technical Decisions 16
3 SECURITY PROBLEM DEFINITION 19
3.1 Threats 19
3.2 Assumptions 20
3.3 Organizational Security Policies 23
4 SECURITY OBJECTIVES 24
4.1 Security Objectives for the TOE 24
4.2 Security Objectives for the Operational Environment 24
5 EXTENDED COMPONENTS DEFINITION 26
6 SECURITY FUNCTIONAL REQUIREMENTS 27
6.1 Conventions 28
6.2 Security Functional Requirements 28
6.2.1 Security Audit (FAU) 28
6.2.2 Cryptographic Support (FCS) 32
6.2.3 Identification and Authentication (FIA) 35
6.2.4 Security Management (FMT) 37
6.2.5 Protection of the TSF (FPT) 38
6.2.6 TOE Access (FTA) 39
6.2.7 Trusted Path/Channels (FTP) 40
6.3 TOE SFR Dependencies Rationale for SFRs 41
6.4 Security Assurance Requirements 41
6.5 Assurance Measures 41
7 TOE SUMMARY SPECIFICATION 43
7.1 CAVP Algorithm Certificate Details 55
7.2 Cryptographic Key Destruction 56
8 ACRONYM TABLE 58

List of Tables

Table 1 - TOE/ST Identification 6
Table 2 - TOE Cryptography Implementation 11
Table 3 - TOE Documentation 13
Table 4 – IT Environment Components 14
Table 5 – Relevant Technical Decisions 16
Table 6 – Threats 19
Table 7 – Assumptions 21
Table 8 – OSPs 23
Table 9 – Security Objectives for the Operational Environment 24
Table 11 - Security Functional Requirements and Auditable Events 29
Table 12 - Security Assurance Requirements 41
Table 13 - TOE Security Assurance Measures 41
Table 14 - TOE Summary Specification SFR Description 43
Table 15 – CAVP Algorithm Certificate References 55
Table 16 - Key Storage and Zeroization 56
Table 17 - Acronyms 58

List of Figures

Figure 1 - Representative TOE Deployment 8
Figure 2 - TOE Boundaries 10

1 Introduction

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

1.1 Security Target and TOE Reference

This section provides the information needed to identify and control the TOE and the ST.

Table 1 - TOE/ST Identification

Category	Identifier
ST Title	Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4 Security Target
ST Version	1.0
ST Date	August 11, 2023
ST Author	Symantec Corporation, A Division of Broadcom
TOE Identifier	Symantec Edge Secure Web Gateway (SWG)
TOE Version	7.4.1.1
TOE Developer	Symantec Corporation, A Division of Broadcom
Key Words	Network Device, Secure Gateway, Web Proxy

1.2 TOE Overview

The TOE is the Symantec Edge SWG running SGOS software version 7.4. The Symantec Edge SWG is not tied to any specific hardware. The TOE type is a network device. The purpose of the TOE is to provide a layer of security between an Internal and External Network (typically an office network and the Internet). The TOE allows administrators to create and manage configurable policies on controlled protocol traffic to and from the Internal Network users. A policy may include authentication, authorization, content filtering, and auditing.

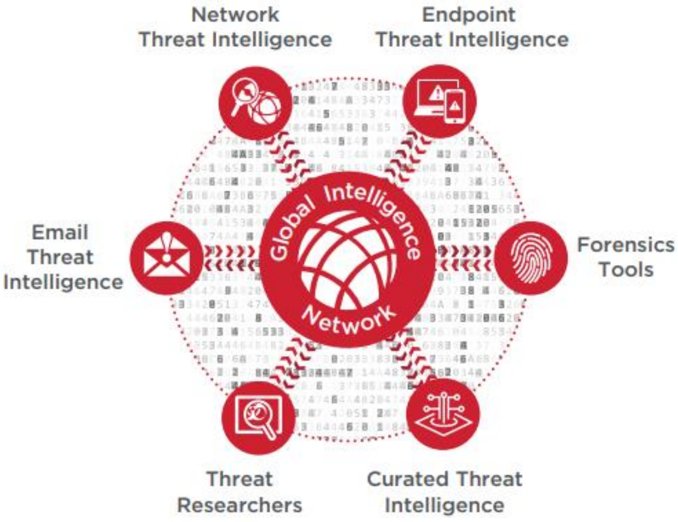
The Edge SWG appliances from Symantec provide companies the ability to deploy a scalable proxy-based security solution to protect their organization against advanced threats. The Edge SWG acts as gateway between web users and the Internet: a single point where all web traffic can be monitored and corporate policies for web use can be enforced. This strategic position makes the Edge SWG a natural place to build in additional network security technologies that defend against a very wide range of cybercrimes, malware, and phishing.

The Edge SWG offers the following features.

- High-speed decryption and re-encryption of SSL/TLS traffic, so attackers cannot use encryption to conceal malware or command and control traffic into and out of the corporate network,
- Universal Policy Enforcement (UPE) from Symantec allows organizations to enforce acceptable web use policies for employees who connect through the Edge SWG. Symantec allows you to centralize your policy creation, maintenance, and installation for simplified unified administration.

- Out of the box protection - Recommended, strong, and maximum policies crafted by security experts.
- Immediate protection with the broadest advanced threat integrations
- Direct cloud application visibility and real-time controls
- Unmatched performance and reliability
- Logs and reports on how users connect to websites.
- Strong user authentication can be incorporated into the policies, supporting a wide variety of identity sources, including NTLM, LDAP, RADIUS, one-time passwords, and certificates.
- Integration of the world’s largest civilian threat intelligence dataset with the Symantec Global Intelligence Network (GIN)
- When paired with other Symantec technologies, it can provide:
  - Malware detection using multiple anti-malware engines and detection methods.
  - Multi-layered deep content inspection and analysis to detect spam and application-level threats in the payloads of network traffic.
  - Data Loss Prevention (DLP) to identify confidential information and block it from leaving the corporate network.
  - Cloud Access Security Broker (CASB) features to monitor and control what applications users can access and how documents and files are sent to the cloud.
  - Web (browser) isolation to create a safe browsing experience, prevent malware from moving from browsers onto employees’ systems, and block sharing of credentials on suspicious websites.

The Symantec Global Intelligence Network (GIN), which monitors more than 175 million endpoints and Edge SWGs protecting 80 million users. It uses artificial intelligence to analyze over 3.7 billion lines of telemetry to identify and categorize emerging threats and suspicious and malicious URLs and websites. Key data is continually forwarded to hardware and virtual Edge SWGs in data centers and in cloud deployments and to hosted SaaS platforms.


Network Threat Intelligence
Endpoint Threat Intelligence
Email Threat Intelligence
Global Intelligence Network
Forensics Tools
Threat Researchers
Curated Threat Intelligence

1.3 TOE Description

This section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references.

For the Symantec Edge SWG with SGOS v7.4, TOE evaluated configuration is comprised of one instance of the SGOS executing on SSP[1]-S410-20 hardware running ISG and a virtual appliance Dell Power Edge R440 hardware platform with ESXi 6.5.

Note: The Integrated Secure Gateway (ISG) is the software on the Symantec Security Platform (SSP) appliance used to deploy applications. The ISG appliance hosts the network security applications e.g., Edge SWG.

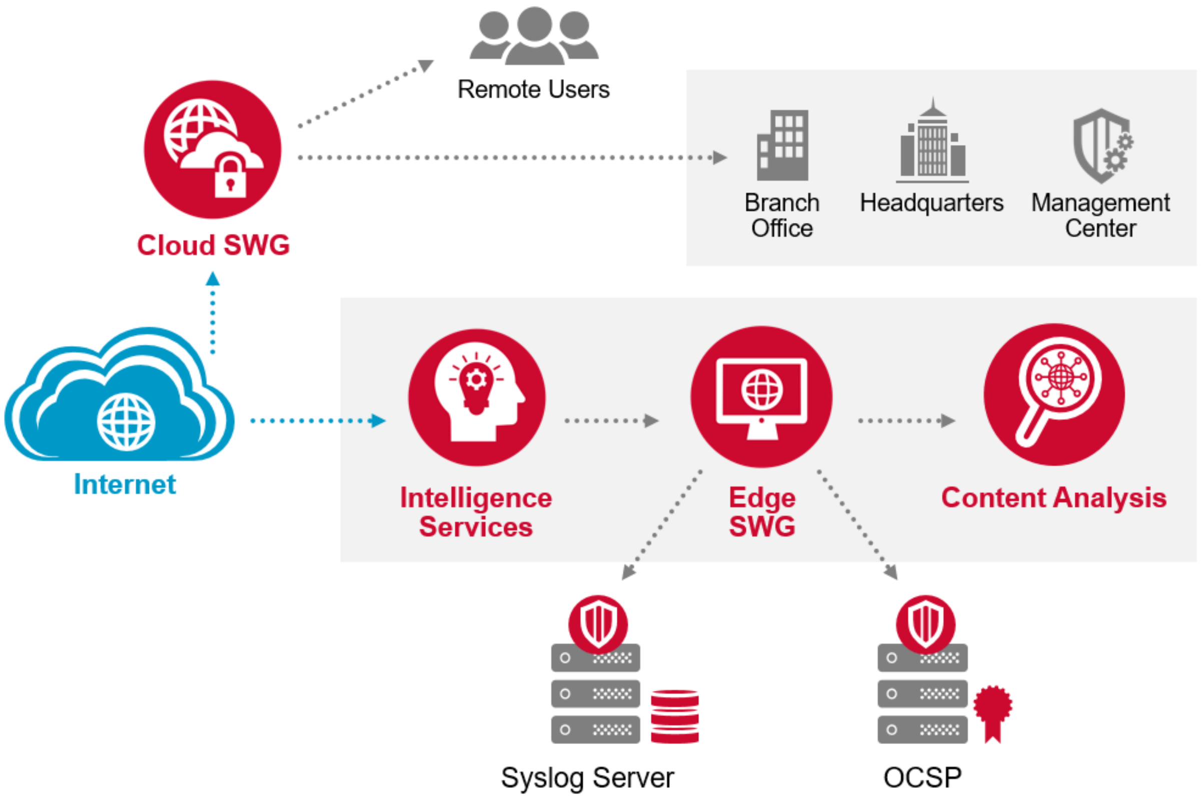


Figure 1 - Representative TOE Deployment

A brief overview of each component in the above figure is as follows:

- **Cloud SWG** - Edge SWG running as a SaaS on Google Cloud Platform (cloud version of Edge SWG), same functionality as the TOE, just in the cloud.
- **Intelligence Services** -This is where all the data that ProxySG can use to help filter and protect based on URL reputation/categorization (is this a safe URL?)
- **Edge SWG** - the TOE

[1] SSP – Symantec Security Platform

- **Content Analysis** - Can analyze the content being accessed (files, web pages) and look at them for potential viruses/malware. Edge SWG applies filters on traffic and can use the result/verdict received from Content Analysis to allow or deny traffic through the proxy.
- **Syslog server** - A syslog server is a destination for transmitting audit logs.
- **OCSP** - Online Certificate Status Protocol (OCSP) is a method used to check the revocation status of digital certificates, ensuring that they are still valid and trustworthy. This process is conducted online, providing real-time validation of certificate status.
- **Remote Users** - Users navigating for web traffic (these users generally are not aware of the Edge SWG explicitly).
- **Branch Office** - A Branch Office is a remote location that serves as a representation of the company to its customers, appearing as though they have a physical office presence.
- **Headquarters** – It is a facility similar to the Branch Office but older/bigger.
- **Management Center -** Symantec product that can be used to manage Edge SWGs. Meant to centralize management tasks.

1.3.1 Physical Boundaries

The TOE is a software solution that is comprised of the network device and its configurations described in Section 1.3. The boundaries are illustrated in Figure 2. The red rectangle represents the physical boundary of the TOE.

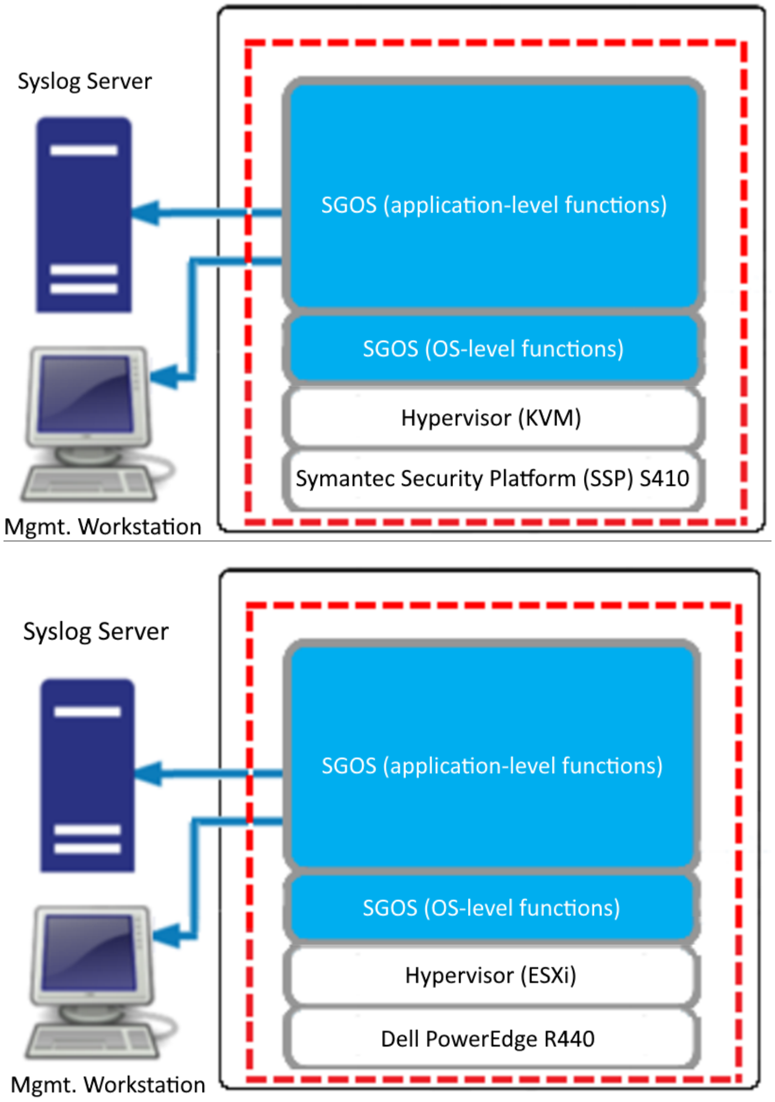

Syslog Server
SGOS (application-level functions)
SGOS (OS-level functions)
Hypervisor (KVM)
Symantec Security Platform (SSP) S410
Mgmt. Workstation
Syslog Server
SGOS (application-level functions)
SGOS (OS-level functions)
Hypervisor (ESXi)
Dell PowerEdge R440
Mgmt. Workstation

Figure 2 - TOE Boundaries

The TOE boundary includes the ‘SGOS’ software version 7.4. Licenses activate different features in the executable.

The TOE physical boundary also includes the following:

- VMware ESXi 6.5 Hypervisor hosted on Dell Power Edge R440, with Intel Xeon Silver 4216 Processor (Cascade Lake)
- SSP-S410-20 with ISG using Intel Xeon Silver 4210 Processor (Cascade Lake)

1.3.2 Security Functions Provided by the TOE

The TOE provides the security functions required by the collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v2.2e or NDcPP.

1.3.2.1 Security Audit

The Network Appliances provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include:

- Start-up of the TOE from both cold boot and reboot,
- Shutdown of the TOE (when shut down from the local CLI and Remote CLI),
- All administrative actions (both security relevant and non-security relevant) from the local CLI and remote CLI,
- Remote administrative SSH connection establishment,
- Remote administrative SSH connection closure,
- Errors during Remote administrative SSH connection establishment,
- Generation of self-signed certificates,
- Import of certificates,
- Deletion of certificates,
- Successful authentication attempts (from the local CLI and Remote CLI),
- Unsuccessful authentication attempts (from the local CLI and Remote CLI),
- All attempts to update the TOE software,
- Changes to time,
- Start of a local administrative session,
- End of a local administrative session,
- Administration session timeout (from the local CLI and Remote CLI).

The TOE is configured to transmit its audit messages to an external audit server. Communication with the audit server is protected using TLS.

The logs for all the appliances can be viewed via the CLI. The records include the date/time the event occurred, the event/type of event, the user ID associated with the event, and additional information of the event and its success and/or failure.

1.3.2.2 Cryptographic Support

The TOE provides cryptographic support for the following features,

- TLSv1.2 connectivity with the following entities:
  - Audit Server.
- SSH connectivity with the following entities:
  - Management SSH Client.
- Secure software update

Table 2 - TOE Cryptography Implementation

Cryptographic Method	Use within the TOE
AES	• TLS Traffic Encryption/Decryption • SSH Traffic Encryption/Decryption
RSA	• TLS Session Establishment

Cryptographic Method	Use within the TOE
	• SSH Session Establishment
SP800-90A	• TLS Session Establishment • SSH Session Establishment
SHS	• Used to provide TLS traffic integrity verification • Used to provide SSH traffic integrity verification
HMAC-SHS	• Used to provide TLS traffic integrity verification • Used to provide SSH traffic integrity verification
SP800-56A	• TLS Session Establishment • SSH Session Establishment
SP800-135rev1	• TLS Session Key Derivation • SSH Session Key Derivation

The TOE provides cryptographic support for the services as described in sections 6.2.2.1 through 6.2.2.10 under FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, FCS_COP.1/KeyedHash, FCS_RBG_EXT.1, FCS_SSHS_EXT.1 and FCS_TLSC_EXT.1, security functional requirements. Additional details are included in section 6.

The CAVP certificate numbers for the cryptographic algorithms are given in Table 15. The TOE uses SGOS 7.4 with OpenSSL v3.0 to implement protocol logic as well as all the cryptographic primitives used by the protocols.

1.3.2.3 Identification and Authentication

The TOE provides authentication services for administrative users to connect to the TOE's administrator interfaces (local CLI and remote CLI). The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on any TOE administrative interface.

1.3.2.4 Security Management

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

- Local console command line administration;
- Remote CLI administration via SSH;

All administration functions can be accessed via remote CLI or via a direct connection to the TOE. The TOE provides the ability to securely manage the below listed functions;

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE;
- Update to the TOE.

1.3.2.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Administrators. The TOE prevents reading cryptographic keys and passwords. Additionally, the TOE software (7.4) is custom-built for the appliance.

The TOE maintains the date and time using an authenticated NTP server. This date and time are used as the timestamp that is applied to audit records generated by the TOE. Administrators can configure an authenticated NTP server. Finally, the TOE performs testing to verify correct operation of the security appliances themselves. The TOE verifies all software updates via digital signature (2048-bit RSA/SHA-256) and requires administrative intervention prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

1.3.2.6 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE displays an Authorized Administrator specified banner on both the local and remote CLI management interfaces prior to allowing any administrative access to the TOE.

1.3.2.7 Trusted Path/Channels

The TOE supports several types of secure communications, including,

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

1.3.3 TOE Documentation

The following documents are essential to understanding and controlling the TOE in the evaluated configuration:

Table 3 - TOE Documentation

Reference	Title	Version	Date
[CC]	Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4 Common Criteria Administrative Guidance	0.8	August 11, 2023
[ST]	Symantec Edge SWG with SGOS v7.4 Security Target	1.0	August 11, 2023
[CM]	Symantec Edge SWG with SGOS 7.4 Configuration Management	0.4	August 11, 2023
[FSP]	Symantec Edge SWG with SGOS 7.4 Functional Specification Document	0.4	August 11, 2023
[CLI]	Edge SWG 7.4.x Command Line Interface Reference	0.1	July 26, 2023
[ISG]	ISG 2.1 Administration and Deployment Guide	0.1	June 16, 2022

1.3.4 References

In additional to TOE documentation, the following reference may also be valuable when understanding and controlling the TOE:

- collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e]

1.4 TOE Environment

The following environmental components are required to operate the TOE in the evaluated configuration:

Table 4 – IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Remote Management Workstation (GUI).	No	This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS and TLS protected channels.
Remote Management Workstation (CLI).	Yes	This includes any IT Environment Management workstation with an SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels.
Local Management Workstation (CLI).	Yes	This includes any IT Environment Management workstation with a local CLI support that is used by the TOE administrator to support TOE administration through a direct connection.
NTP Server	Yes	NTP server supporting SHA-1 integrity verification.
Audit Server	Yes	The audit server is used for remote storage of audit records that have been generated by and pulled from the TOE.
CA/OCSP Server	Yes	A server with a certification authority and certificate revocation list used by the TOE for validating the X.509 certificates used for TLS connection establishment.

1.5 TOE Minimum Deployment Requirements

The TOE minimum requirements for the ESXi environment are as follows:

- Minimum Virtual CPU – 1 GHz (minimum), 2.6 GHz (recommended)
- Minimum Virtual Disk requirements space – 1x8 GB Boot disk, 2 (or more) 100 GB Data disk.
- Minimum Virtual Memory – 4 GB
- Processor – Intel Xeon Silver 4216 Processor (Cascade Lake)
- Hypervisor – VMware ESXi 6.5

The SSP-S410-20 is a preconfigured appliance that includes the following specifications:

- CPU – 2 x 10 core 2.2 GHz
- Processor – Intel Xeon Silver 4210 Processor (Cascade Lake)
- Memory – 96 GB
- Disk – 2 x 960 GB of Data Disk and 2 x 64 GB Boot Disk

1.6 TOE Delivery

Customers with an active account may download the TOE securely from: https://support.broadcom.com/group/ecx/.

The TOE build maintains integrity throughout the delivery process by limiting access to current customers, supporting downloads over TLS, and providing an MD5 and SHA-256 hash for TOE verification post download.

1.7 Product Functionality not Included in the Scope of the Evaluation

The following product functionality is not included in the CC evaluation:

- Java Management Console

2 Conformance Claims

This section identifies the TOE conformance claims, conformance rationale, and relevant Technical Decisions (TDs).

2.1 CC Conformance Claims

The TOE is conformant to the following:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017 (Extended)
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision 5, April 2017 **(**Conformant**)**

2.2 Protection Profile Conformance

This ST claims exact conformance to the following:

- collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [PP-ND]

2.3 Conformance Rationale

This ST provides exact conformance to the items listed in the previous section. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile (PP), performing only the operations defined there.

2.3.1 Technical Decisions

All NIAP TDs issued to date and applicable to NDcPP v2.2e have been considered. Table 5 identifies all applicable TDs.

Table 5 – Relevant Technical Decisions

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0527: Updated to Certificate Revocation Testing (FIA_X509_EXT.1)	Y	
TD0528: NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	Y	
TD0536: NIT Technical Decision for Update Verification Inconsistency	Y	
TD0537: NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	Y	
TD0538: NIT Technical Decision for Outdated link to allowed-with list	Y	
TD0546: NIT Technical Decision for DTLS – clarification of Application Note 63	N	The TOE does not support DTLS.
TD0547: NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Y	

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0555: NIT Technical Decision for RFC Reference incorrect in TLSS Test	N	The TOE does not support TLSS functionality.
TD0556: NIT Technical Decisions for RFC 5077 question	N	The TOE does not support TLSS functionality.
TD0563: NIT Technical Decision for Clarification of audit date information	Y	
TD0564: NIT Technical Decision for Vulnerability Analysis Search Criteria	Y	
TD0569: NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	N	The TOE does not support DTLSS functionality.
TD0570: NIT Technical Decision for Clarification about FIA_AFL.1	Y	
TD0571: NIT Technical Decision for Guidance on how to handle FIA_AFL.1	Y	
TD0572: NIT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	Y	
TD0580: NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Y	
TD0581: NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	Y	
TD0591: NIT Technical Decision for Virtual TOEs and hypervisors	Y	
TD0592: NIT Technical Decision for Local Storage of Audit Records	Y	
TD0631: NIT Technical Decision for Clarification of public key authentication for SSH Server	Y	
TD0632: NIT Technical Decision for Consistency with Time Data for vNDs	Y	
TD0633: NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	N	The TOE does not claim IPSec functionality.

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0634: NIT Technical Decision for Clarification required for testing IPv6	Y	
TD0635: NIT Technical Decision for TLS Server and Key Agreement Parameters	N	The TOE does not claim TLS Server functionality.
TD0636: NIT Technical Decision for Clarification of Public Key User Authentication for SSH	N	The TOE does not support SSH Client functionality.
TD0638: NIT Technical Decision for Key Pair Generation for Authentication	Y	
TD0639: NIT Technical Decision for Clarification for NTP MAC Keys	Y	
TD0670: NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	N	The TOE does not claim TLSC with Mutual Authentication.
TD0738: NIT Technical Decision for Link to Allowed-With List	Y	

3 Security Problem Definition

The security problem definition has been taken directly from the claimed PP and any relevant EPs/Modules/Packages specified in Section 2.2 and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any Organizational Security Policies (OSPs) that the TOE is expected to enforce.

3.1 Threats

The threats included in Table 6 are drawn directly from the PP and any EPs/Modules/Packages specified in Section 2.2.

Table 6 – Threats

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of

ID	Threat
	confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.2 Assumptions

The assumptions included in Table 7 are drawn directly from PP and any relevant EPs/Modules/Packages.

Table 7 – Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

ID	Assumption
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_ADMINISTRATOR	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATION	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

3.3 Organizational Security Policies

The OSPs included in Table 8 are drawn directly from the CPP_ND_V2.2e.

Table 8 – OSPs

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

4 Security Objectives

The security objectives have been taken directly from the claimed PP and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the TOE

CPP_ND_V2.2e does not define any security objectives that apply to the TOE.

4.2 Security Objectives for the Operational Environment

Security objectives for the operational environment assist the TOE in correctly providing its security functionality. These objectives, which are found in the table below, track with the assumptions about the TOE operational environment.

Table 9 – Security Objectives for the Operational Environment

ID	Objectives for the Operational Environment
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

ID	Objectives for the Operational Environment
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
OE.VM_CONFIGURATION	For vNDs, the Security Administrator ensures that the VS and VMs are configured to • Reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • Correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting).

5 Extended Components Definition

The extended components i.e. those not defined in CC Part 2 or CC Part 3 are listed in Table 10 below. These are from the NDcPP.

Table 10 Extended Components

PP	SFR	Description
NDcPP	FAU_STG_EXT.1	Protected Audit Event Storage
NDcPP	FCS_NTP_EXT.1	NTP Protocol
NDcPP	FCS_RBG_EXT.1	Random Bit Generation
NDcPP	FCS_SSHS_EXT.1	SSH Server Protocol
NDcPP	FCS_TLSC_EXT.1	TLS Client Protocol
NDcPP	FIA_PMG_EXT.1	Password Management
NDcPP	FIA_UAU_EXT.2	Password-based Authentication Mechanism
NDcPP	FIA_UIA_EXT.1	User Identification and Authentication
NDcPP	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
NDcPP	FIA_X509_EXT.2	X.509 Certificate Authentication
NDcPP	FIA_X509_EXT.3	X.509 Certificate Requests
NDcPP	FPT_APW_EXT.1	Protection of Administrator Passwords
NDcPP	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric, and private keys)
NDcPP	FPT_STM_EXT.1	Reliable Time Stamps
NDcPP	FPT_TST_EXT.1	TSF testing
NDcPP	FPT_TUD_EXT.1	Trusted update
NDcPP	FTA_SSL_EXT.1	TSF-initiated Session Locking

6 Security Functional Requirements

This section identifies the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revisions 5, April 2017, and all international interpretations.

Table 11 – SFRs

Requirement	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG_EXT.1	Protected Audit Event Storage
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FCS_NTP_EXT.1	NTP Protocol
FCS_RBG_EXT.1	Random Bit Generation
FCS_SSHS_EXT.1	SSH Server Protocol
FCS_TLSC_EXT.1	TLS Client Protocol without Mutual Authentication
FIA_AFL.1	Authentication Failure Management
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU_EXT.2	Password-based Authentication Mechanism
FIA_UAU.7	Protected Authentication Feedback
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FIA_X509_EXT.3	X.509 Certificate Requests
FMT_MOF.1/Functions	Management of Security Functions Behaviour
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
FMT_MTD.1/CoreData	Management of TSF Data
FMT_MTD.1/CryptoKeys	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on security roles
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_TST_EXT.1	TSF Testing

Requirement	Description
FPT_STM_EXT.1	Reliable Time Stamps
FPT_TUD_EXT.1	Trusted Update
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_SSL_EXT.1	TSF-initiated Session Locking
FTA_TAB.1	Default TOE Access Banner
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1/Admin	Trusted Path

6.1 Conventions

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.
- Where operations were completed in the PP and relevant EPs/Modules/Packages, the formatting used in the PP has been retained.
- Extended SFRs are identified by the addition of "EXT" after the requirement name.

6.2 Security Functional Requirements

This section includes the security functional requirements for this ST.

6.2.1 Security Audit (FAU)

6.2.1.1 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) Auditable events for the not specified level of audit; and

c) *All administrative actions comprising:*

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

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

FAU_GEN.1.2

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, *information specified in column three of Table 10.*

Table 10 - Security Functional Requirements and Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	• Start-up and shut-down of the audit functions • Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators) • Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed) • Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged) • Resetting passwords (name of related user account shall be logged)	None
FAU_GEN.2	None	None
FAU_STG_EXT.1	None	None
FCS_CKM.1	None	None
FCS_CKM.2	None	None
FCS_CKM.4	None	None
FCS_COP.1/DataEncryption	None	None
FCS_COP.1/SigGen	None	None
FCS_COP.1/Hash	None	None
FCS_COP.1/KeyedHash	None	None
FCS_NTP_EXT.1	• Configuration of a new time server • Removal of configured time server	Identity if new/removed time server
FCS_RBG_EXT.1	None	None

Requirement	Auditable Events	Additional Audit Record Contents
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address)
FIA_PMG_EXT.1	None	None
FIA_UIA_EXT.1	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)
FIA_UAU_EXT.2	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)
FIA_UAU.7	None	None
FIA_X509_EXT.1/Rev	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store	• Reason for failure of certificate validation • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None	None
FMT_MOF.1/Functions	None	None
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None
FMT_MTD.1/CoreData	All management activities of TSF data	None
FMT_MTD.1/CryptoKeys	None	None
FMT_SMF.1	None	None
FMT_SMR.2	None	None
FPT_SKP_EXT.1	None	None
FPT_APW_EXT.1	None	None
FPT_TST_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None

Requirement	Auditable Events	Additional Audit Record Contents
FTA_SSL.3	The termination of a remote session by the session locking mechanism	None
FTA_SSL.4	The termination of an interactive session	None
FTA_SSL_EXT.1 (if "lock the session" is selected)	Any attempts at unlocking of an interactive session	None
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism	None
FTA_TAB.1	None	None
FTP_ITC.1	• Initiation of the trusted channel • Termination of the trusted channel • Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1/Admin	• Initiation of the trusted path • Termination of the trusted path. • Failure of the trusted path functions.	None

6.2.1.2 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.

6.2.1.3 FAU_STG_EXT.1 Protected Audit Event Storage

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

FAU_STG_EXT.1.2
The TSF Shall be able to store generated audit data on the TOE itself. In addition [

- *The TOE shall consist of a single standalone component that stores audit data locally*

].

FAU_STG_EXT.1.3
The TSF shall [*overwrite previous audit records according to the following rule: [when the log storage has reached its configured capacity]*] when the local storage space for audit data is full.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1
The TSF shall generate **asymmetric** cryptographic key in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;
- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1
- FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526].

].

6.2.2.2 FCS_CKM.2 Cryptographic Key Establishment

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

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [selection: groups listed in RFC 3526, groups listed in RFC 7919].

].

Application Note: This SFR has been updated as per TD0580 and TD0581

6.2.2.3 FCS_CKM.4 Cryptographic Key Destruction

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

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

that meets the following: *No Standard.*

6.2.2.4 FCS_COP.1/DataEncryption Cryptographic Operations (AES Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption

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

6.2.2.5 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen

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

- *RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits, 3072 bits]*

]

that meet the following: [

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

].

6.2.2.6 FCS_COP.1/Hash Cryptographic Operations (Hash Algorithm)

FCS_COP.1.1/Hash

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

6.2.2.7 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash

The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [*HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512*] and cryptographic key sizes *[160, 256, 384, 512 bits]* **and message digest sizes [*160, 256, 384, 512*] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

6.2.2.8 FCS_NTP_EXT.1 NTP Protocol

FCS_NTP_EXT.1.1

The TSF shall use only the following NTP version(s) [*NTP v3 (RFC 1305)*].

FCS_NTP_EXT.1.2

The TSF shall update its system time using [selection:

- Authentication using [*SHA1*] as the message digest algorithm(s);

  ].

FCS_NTP_EXT.1.3

The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

FCS_NTP_EXT.1.4

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

6.2.2.9 FCS_RBG_EXT.1 Random Bit Generation

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

FCS_RBG_EXT.1.2
The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [*[2] software-based noise source*] with a minimum of [*256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

6.2.2.10 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1
The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [*4256, 5647, 5656, 6668, 8268*].

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

Application Note: This SFR has been updated as per TD0631.

FCS_SSHS_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than *[1522]* bytes in an SSH transport connection are dropped.

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

FCS_SSHS_EXT.1.5
The TSF shall ensure that the SSH public-key based authentication implementation uses [*ssh-rsa, rsa-sha2-256, rsa-sha2-512*] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6
The TSF shall ensure that the SSH transport implementation uses [*hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512*] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7
The TSF shall ensure that [*diffie-hellman-group14-sha1, ecdh-sha2-nistp256*] and [*ecdh-sha2-nistp384, ecdh-sha2-nistp521*] are the only allowed key exchange methods used for the SSH protocol.

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

6.2.2.11 FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

FCS_TLSC_EXT.1.1
The TSF shall implement [*TLS 1.2 (RFC 5246)* and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

- *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

] and no other ciphersuites.

FCS_TLSC_EXT.1.2
The TSF shall verify that the presented identifier matches [*the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN, IPv6 address in the CN or SAN, IPv4 address in SAN, IPv6 address in the SAN, and no other attribute types*].

FCS_TLSC_EXT.1.3
When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- *Not implement any administrator override mechanism*

].

FCS_TLSC_EXT.1.4
The TSF shall [*present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups:* [*secp256r1, secp384r1, secp521r1*] *and no other curves/groups*] in the Client Hello.

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1
The TSF shall detect when an Administrator configurable positive integer within *[1 to 60]* unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been met, the TSF shall [*prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until [unlocking the locked user account] is taken by an Administrator.*

6.2.3.2 FIA_PMG_EXT.1 Password Management

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

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

b) Minimum password length shall be configurable to between *[8]* and *[64]* characters.

6.2.3.3 FIA_UIA_EXT.1 User Identification and Authentication

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

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

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

6.2.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1
The TSF shall provide a local [*password-based*] authentication mechanism to perform local administrative user authentication.

6.2.3.5 FIA_UAU.7.1 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**.

6.2.3.6 FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates**.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [*the Online Certificate Status Protocol (OCSP) as specified in RFC 6960*].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
  - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

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

6.2.3.7 FIA_X509_EXT.2 X.509 Certificate Authentication

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

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

Application Note: This SFR has been updated as per TD0537.

6.2.3.8 FIA_X509_EXT.3 X.509 Certificate Requests

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

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

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MOF.1/Functions Management of Security Functions Behaviour.

FMT_MOF.1.1/Functions
The TSF shall restrict the ability to [selection: *modify the behaviour of*] the functions [selection: *transmission of audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full*] to *Security Administrators*.

6.2.4.2 FMT_MOF.1/ManualUpdate Management of Security Functions Behavior

FMT_MOF.1.1/ManualUpdate
The TSF shall restrict the ability to enable the function *to perform manual updates to Security Administrators*.

6.2.4.3 FMT_MTD.1/CoreData Management of TSF Data

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

6.2.4.4 FMT_MTD.1/CryptoKeys Management of TSF Data

FMT_MTD.1.1/CryptoKeys
The TSF shall restrict the ability to *manage* the *cryptographic keys* to *Security Administrators*.

6.2.4.5 FMT_SMF.1 Specification of Management Functions

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

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

- [
    - *Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);*
    - *Ability to modify the behaviour of the transmission of audit data to an external IT entity;*
    - *Ability to manage the cryptographic keys;*
    - *Ability to configure the cryptographic functionality;*
    - *Ability to re-enable an Administrator account;*
    - *Ability to configure NTP;*
    - *Ability to configure the reference identifier for the peer;*
    - *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;*
    - *Ability to import X.509v3 certificates to the TOE's trust store;*
    - *Ability to manage the trusted public keys database;*
    - *No other capabilities*].

Application Note: This SFR has been updated as per TD0631.

6.2.4.6 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1
The TSF shall maintain the roles:

- *Security Administrator*

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

FMT_SMR.2.3
The TSF shall ensure that the conditions

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

are satisfied.

6.2.5 Protection of the TSF (FPT)

6.2.5.1 FPT_APW_EXT.1 Protection of Administrator Passwords

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

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

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

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

6.2.5.3 FPT_STM_EXT.1 Reliable Time Stamps

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

FPT_STM_EXT.1.2
The TSF shall [*synchronise time with an NTP server*].

Application Note: This SFR has been updated as per TD0632.

6.2.5.4 FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1
The TSF shall run a suite of the following self-tests [*during initial start-up (on power on), periodically during normal operation, at the request of the authorised user, at the conditions [manual reboot]*] to demonstrate the correct operation of the TSF: *[AES Known Answer Test, HMAC Known Answer Test, RNG*[2]*/DRBG* [3]*Known Answer Test, SHA Known Answer Test, RSA Signature Known Answer Test (both signature/verification), DH*[4] *Known Answer Test, ECDH*[5] *Known Answer Test].*

6.2.5.5 FPT_TUD_EXT.1 Trusted Update

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

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

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

6.2.6 TOE Access (FTA)

6.2.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1
The TSF Shall, for local interactive sessions, [

- *terminate the session*]

after a Security Administrator-specified time period of inactivity

[2] RNG – Random Number Generator
[3] DRBG – Deterministic Random Bit Generator
[4] DH – Diffie Hellman
[5] ECDH – Elliptic Curve Diffie Hellman

6.2.6.2 FTA_SSL.3 TSF-initiated Termination

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

6.2.6.3 FTA_SSL.4 User-initiated Termination

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

6.2.6.4 FTA_TAB.1 Default TOE Access Banners

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

6.2.7 Trusted Path/Channels (FTP)

6.2.7.1 FTP_ITC.1 Inter-TSF Trusted Channel

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

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

FTP_ITC.1.3
The TSF shall initiate communication via the trusted channel for *[communication with the audit server over TLS]*.

6.2.7.2 FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin
The TSF shall **be capable of using [*SSH*] to** provide a communication path between itself and **authorized** remote **Administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and provides detection of modification of the channel data**.

FTP_TRP.1.2/Admin
The TSF shall permit remote **Administrators** to initiate communication via the trusted path.

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

6.3 TOE SFR Dependencies Rationale for SFRs

The PP contains all the requirements claimed in this ST. As such, the dependencies are not applicable since the PP has been approved.

6.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the PP, which is derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table 11.

Table 11 - Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic functionality specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

6.5 Assurance Measures

The TOE satisfied the identified assurance requirements. This section identifies the Assurance Measures applied by Broadcom Inc. to satisfy the assurance requirements. The following table lists the details.

Table 12 - TOE Security Assurance Measures

SAR Component	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).

SAR Component	How the SAR will be met
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ALC_CMS.1	
ATE_IND.1	Vendor will provide the TOE for testing.
AVA_VAN.1	Vendor will provide the TOE for testing. Vendor will provide a document identifying the list of software and hardware components.

7 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 13 - TOE Summary Specification SFR Description

Requirement	TSS Description
FAU_GEN.1	The TOE provides extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. The types of events that cause audit records to be generated include identification and authentication related events, and administrative events. Each of the events is specified in the audit record is in enough detail to identify the user for which the event is associated (e.g. user identity, MAC address, IP address), when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. The logs for all of the appliances can be viewed via the CLI (local or remote). Additionally, the TOE supports remote audit logging with an external audit server. Audit messages are entered into the log and the subset of the log contents are sent to the audit server. When an administrative command is executed, the TOE sets up the session data structure which includes the “user identity”. When an audit log is generated, the session data is passed along with the audit information and the TOE extracts the “user identity” from the session data structure. The TOE generates the following types of audit logs during operation: • Start-up of the TOE from both cold boot and reboot, • Shutdown of the TOE (when shut down from the local CLI and Remote CLI), • All administrative actions (both security relevant and non-security relevant) from the local CLI and Remote CLI, • Remote administrative SSH connection establishment, • Remote administrative SSH connection closure, • Failures during Remote administrative SSH connection establishment, • Generation of self-signed certificates, • Import of certificates, • Deletion of certificates, • Successful authentication attempts (from the local CLI and Remote CLI), • Unsuccessful authentication attempts (from the local CLI and Remote CLI), • All attempts to update the TOE software, • Changes to time, • Start of a local administrative session, • End of a local administrative session,

Requirement	TSS Description
	Administration session timeout (from the local CLI and Remote CLI).
FAU_GEN.2	The TOE ensures that each auditable event is associated with the user that triggered the event. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IPv4 address, MAC address, host name, or other configured identification is included in the audit record. The audit record is generated with the required information and stored plaintext on the device.
FAU_STG_EXT.1	The TOE provides the ability to securely transmit audit logs to an external audit server using syslog over TLS in real-time. The TOE is a standalone and stores logs locally. The maximum size of audit records stored by the TOE can be configured by an administrator. The upper limit on local audit storage is based on the amount of available hard drive space, but an administrator can set a lower limit if desired. For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. Only Authorized Administrators can clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents. However, the Authorized Administrator may do a onetime configuration that will not allow the administrator to erase logs. This command is irreversible and does not reset even if the machine is returned to factory defaults.
FCS_CKM.1	The TOE can create an RSA public-private key pair with an RSA key size of 2048 and 3072 bits. The RSA algorithm implementation is provided by the included OpenSSL cryptographic library. The RSA key pair can be used to generate a Certificate Signing Request (CSR). The TOE generates Elliptic-curve keys using NIST curves P-256, P-384, and P-521 with key sizes of 256, 384, and 521 bits respectively that meets the standard FIPS 186-4, Appendix B4. Used as a part of TLS session establishment. Key generation via Diffie-Hellman group 14 per RFC 3526, Section 3 is also included since key establishment using Diffie-Hellman group 14 is included in FCS_CKM.2. The relevant NIST CAVP certificate numbers are listed in Table 14.
FCS_CKM.2	In support of secure cryptographic protocols, the TOE supports key establishment schemes, including, • FFC Diffie-Hellman as specified in NIST SP 800-56A Revision 2: Used as part of SSH and TLS session establishment, • Elliptic Curve Diffie-Hellman as specified in NIST SP 800-56A Revision 2: used as part of SSH and TLS session establishment, • Diffie-Hellman group 14 per RFC 3526, Section 3: Used as part of SSH session establishment.

Requirement	TSS Description
	The TOE is fully compliant to both SP 800-56A and SP 800-56B. The TOE implements each "shall" statement in each standard and do not implement any "shall not" statements in either of the standards. When using Diffie-Hellman group 14 key establishment, the TOE always acts as the receiver. That is the TOE only acts as a server in the exchange. The TOE uses the FFC Diffie-Hellman key establishment methodology of NIST SP 800-56A Revision 2 with the exception that the prime specified in RFC 3526 Section 3 is used. The relevant NIST CAVP certificate numbers are listed in Table 14.
FCS_CKM.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) when no longer required for use. The TOE stores several types of keys in volatile memory in plaintext, including, • Diffie-Hellman Private/Public Key Pair, • Elliptic Curve Diffie-Hellman Private/Public Key Pair, • SSH Session Encryption Key, • SSH Session Integrity Key, • TLS Session Encryption Key, • TLS Session Integrity Key. Each plaintext key stored in volatile memory is associated with a cryptographic session. In each instance, after the session closes, the key is overwritten with the value "00" After the overwrite operation is complete, the TOE performs a specific "read-verify" operation to confirm that the storage space no longer contains the key. The TOE stores RSA key pairs used for TLS and SSH in non-volatile storage and a Master Encryption Key (MEK) is used to encrypt all the other keys stored in non-volatile storage. These are overwritten three times using a random pattern provided by the SP 800-90A DRBG. All keys within the TSF are securely destroyed as per the descriptions given in Table 15.
FCS_COP.1/DataEncryption	The TOE provides symmetric encryption and decryption capabilities using AES in CTR and GCM[6] mode (128 and 256 bits for CTR and GCM) as described AES as specified in ISO 18033-3. AES is implemented in support of the following protocols: TLS, and SSH. The relevant NIST CAVP certificate numbers are listed in Table 14.
FCS_COP.1/SigGen	The TOE provides cryptographic signature services using following algorithms and key sizes:

[6] GCM – Galois Counter Mode

Requirement	TSS Description
	- RSA Digital Signature Algorithm with key sizes of 2048 and 3072 as specified in section 5.5 of the FIPS PUB 186-4, "Digital Signature Standard." The relevant NIST CAVP certificate numbers are listed in Table 14.
FCS_COP.1/Hash	The TOE provides cryptographic hashing services using SHS as specified in FIPS Pub 180-3 "Secure Hash Standard." SHS hashing is used within several services including, hashing, TLS (SHA1, SHA256, SHA384), SSH (SHA1, SHA256, SHA384, SHA-512) and NTP (SHA1). The message digest sizes supported are: 160, 256, 384, and 512 bits. The relevant NIST CAVP certificate numbers are listed in Table 14.
FCS_COP.1/KeyedHash	The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512. The product supports the following cryptographic parameters for MACing, as specified in ISO/IEC 9797-2:2011: - Key length: 160, 256, 384, 512-bits - Hash function used: SHA-1, SHA-256, SHA-384, and SHA-512 - Block size: 512, 1024-bits - Output MAC: 160, 256, 384, 512-bits The relevant NIST CAVP certificate numbers are listed in Table 14.
FCS_NTP_EXT.1	The TSF supports time updates using NTPv3. The TSF authenticates updates using an administrator configured symmetric key and SHA-1. The TOE rejects broadcast and multicast time updates. The TOE enforces a maximum limit of 32 NTP time sources that can be configured.
FCS_RBG_EXT.1	The TOE produces all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using CTR_DRBG (AES). The TOE implements a random bit generator in support of various cryptographic operations, including, RSA key establishment schemes, Diff-Hellman key establishment schemes, TLS session establishment and SSH session establishment. The entropy source used to seed the Deterministic Random Bit Generator is a random set of bits or bytes that are regularly supplied to the DRBG by polling four different set of software sources in threads. All entropy is continuously health tested by the DRBG as per the tests defined in section 11.3 of SP 900-90A before being used as a seed (instantiate, generate, reseed, and uninstantiate). Additionally, each call to the entropy source is subject to a continuous random number generator test to ensure that there are no stuck conditions. Any initialization or system errors during bring-up or processing of this system causes a reboot resulting in the DRBG being reseeded. The relevant NIST CAVP certificate numbers are listed in Table 14.
FCS_SSHS_EXT.1	The TOE uses SSH for to facilitate secure remote administrative sessions (CLI). The TOE's SSH implementation supports the following,

Requirement	TSS Description
	• Strict compliance with RFCs 4251, 4252, 4253, 4254, 4256, 5647, 5656, 6668, 8268 • Only password-based authentication and public key-based authentication; • The TOE uses the username presented by the client as the user's identity. • The TOE then authorizes the connection if the presented public key matches an authorized public key for the claimed identity. • For public key-based authentication, use of 2048-bit RSA keys in support of SSH_RSA. • Dropping SSH packets greater than 1522 bytes. This is accomplished by buffering all data for a particular SSH packet transmission until the buffer limit is reached and then dropping the packet; • Encryption algorithms aes128-ctr, aes256-ctr, aes-128-gcm@openssh.com, aes-256-gcm@openssh.com to ensure confidentiality of the session and reject all other encryption algorithms; • Hashing algorithm hmac-sha1, hmac-sha-1-96, hmac-sha2-256, hmac-sha2-512 ensure the integrity of the session, and reject all other MAC algorithms; • The TOE enforces diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521 as the only allowed key exchange methods. • The TOE forces a rekey before reaching 1 hour or 2^28 bytes (which is less than aggregate of one gigabyte of data), whichever occurs first.
FCS_TLSC_EXT.1	The TOE operates as a TLS client for the trusted channel with the remote syslog server. TOE supports TLS 1.2. Connections using another version of TLS or SSL, such as, TLS 1.0 or SSL 3.0 are actively denied by the TOE. The following ciphersuites are supported for communications with the remote audit server: • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 All other proposed Ciphersuites are denied. The Ciphersuites are user configurable.

Requirement	TSS Description
	The reference identifier for the remote audit server is configured by the administrator using the CLI. When the TLS client receives an X.509 certificate from the server, the client will compare the reference identifier with the established Subject Alternative Names (SANs) in the certificate. If a SAN is available and does not match the reference identifier, then the verification fails, and the channel is terminated. If there are no SANs of the correct type (IP address or DNS name) in the certificate, then the TOE will compare the reference identifier to the CN (IP address or DNS name) in the certificate Subject. If there is no CN, then the verification fails, and the channel is terminated. If the CN exists and does not match, then the verification fails, and the channel is terminated. Otherwise, the reference identifier verification passes, and additional verification actions can proceed. The TOE supports wildcards for DNS names in the CN and SAN. For both DNS Name and CN matching, the hostname must be an exact match or wildcard match. In the case of a wildcard match, the wildcard must be the left-most component, wildcard matches a single component, and there are at least two non-wildcard components. When the reference identifier is an IP address, the TOE converts the IP address to a binary representation in network byte order. IPv4 addresses are converted directly from decimal to binary, IPv6 addresses are converted as specified in RFC 5952. The TOE compares the binary IP address against all the IP Address entries in the Subject Alternative Name extension. If there is not an exact binary match, then the verification fails. The TLS client does not support certificate pinning or administrator override of certificate validation failures. The TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: P-256, P-384, and P-521. The non-TOE server can choose to negotiate the elliptic curve from this set for any of the mutually negotiable elliptic curve Ciphersuites. The TOE does not support presentation of an X.509v3 client certificate for authentication as required by the non-TOE Server.
FIA_AFL.1	The TOE permits administrators to set a positive integer for failed remote authentication attempts. When this limit is met, a trusted administrator must manually unlock the locked-out user before a successful authentication happens. The local console account is not subject to the lockout mechanism. This account should not be used for day-to-day administrator.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “’”, “+”, “-“, “=”, “.”, “/”, “\”, “:”, “;”, “<”, “>”, “[“, “]”, “_”, “{“, “}”, “|”, “~” “`” . The minimum password length is settable by the Authorized Administrator.

Requirement	TSS Description
	When the TOE is configured for "Common Criteria Compliance" the minimum password length is set to 8 characters and the maximum password length is 64 characters.
FIA_UIA_EXT.1 FIA_UAU_EXT.2 FIA_UAU.7	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Administrative access to the TOE is facilitated through one of several interfaces, • Directly connecting to the TOE • Remotely connecting via SSHv2 Regardless of the interface at which the administrator interacts, the TOE will enforce username and password authentication. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. The TOE provides a local password-based mechanism. The process for authentication is the same for administrative access whether administration is occurring via direct connection or remotely. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure. The password is obscured by 'providing with asterisks'.
FIA_X509_EXT.1/Rev	The TOE performs X.509 certificate validation at the following points: • TLS client validation of server certificates; • When certificates are loaded into the TOE, such as when importing CAs, certificate responses and other device-level certificates. In all scenarios, certificates are checked for several validation characteristics: a) If the certificate 'notAfter' date is in the past, then this is an expired certificate which is considered invalid; b) The certificate chain must terminate with a trusted CA certificate; c) Server certificates consumed by the TOE TLS client must have a 'serverAuthentication' extendedKeyUsage purpose; d) OCSP certificates presented for OCSP responses must have the 'ocspSigning' extendedKeyUsage purpose. Certificate revocation checking for the above scenarios is performed by querying with an OCSP Responder. As X.509 certificates are not used for trusted updates, firmware integrity self-tests or client authentication, the code-signing and

Requirement	TSS Description
	clientAuthentication purpose is NOT checked in the extendedKeyUsage for related certificates. A trusted CA certificate is defined as any certificate loaded into the TOE trust store that has, at a minimum, a basicConstraints extension with the CA flag set to TRUE.
FIA_X509_EXT.2	The TOE has a trust store where root CA and intermediate CA certificates can be stored. The trust store is not cached: if a certificate is deleted, it is immediately untrusted. If a certificate is added to the trust store, it is immediately trusted for its given scope. Revocation checking is performed on both leaf and intermediate CA certificates when a leaf certificate is presented to the TOE as part of the certificate chain during authentication. The X.509 certificates for each of the given scenarios are validated using the certificate path validation algorithm defined in RFC 5280, which can be summarized as follows: a) The public key algorithm and parameters are checked. b) The current date/time is checked against the validity period revocation status is checked c) Issuer name of X matches the subject name of X+1 d) Name constraints are checked e) Policy OIDs are checked f) Policy constraints are checked; issuers are ensured to have CA signing bits g) Path length is checked h) Critical extensions are processed If, during the entire trust chain verification activity, any certificate under review fails a verification check, then the entire trust chain is deemed untrusted. As part of the verification process, OCSP is used to determine whether the certificate is revoked or not. If the OCSP response is unknown or cannot be obtained, then the TOE will use the last cached information available about certificate to accept or reject the certificate (or the TOE will treat the certificate as revoked/ as valid). The TOE contacts the OCSP responder hourly during an hourly check of certificates in the trust store. Instructions for configuring the trusted IT entities to supply appropriate X.509 certificates are captured in the guidance documents.
FIA_X509_EXT.3	For the Certificate Signing Request, a CN is required and may be an IP address or a DNS name. SAN is optional and may be an IPv4 address, IPv6 address or a DNS name.
FMT_MOF.1/Functions	The TOE restricts the ability to modify (enable/disable) transmission of audit records to an external audit server to Security Administrators.
FMT_MOF.1/ManualUpdate	The TOE does not provide automatic updates to the software version running on the TOE.

Requirement	TSS Description
	The Security Administrators (i.e. Authorized Administrators) can query the software version running on the TOE, and can initiate updates to (replacements of) software images. When software updates are made available, the Authorized Administrators can obtain, verify the integrity of, and install those updates. This verification uses manual checking of published hashes.
FMT_MTD.1/CoreData	Users are required to login before being provided with access to any administrative functions. The TOE provides the ability for Security Administrators (i.e., Authorized Administrators) to access TOE data, such as audit data, configuration data, security attributes, session thresholds, administration of X.509 certificates and updates. Access to this data is governed by the privileges assigned to the administrative users. None of this functionality is accessible prior to the administrator logging into the TOE. The term "Authorized Administrator" is used in this ST to refer to any of the predefined user privilege levels.
FMT_MTD.1/CryptoKeys	The TOE restricts the ability to manage SSH (session keys), TLS (session keys), and any configured X.509 certificates (public and private key pairs) to security administrators via command line.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The Security Administrators (a.k.a Authorized Administrators) user can connect to the TOE using the CLI to perform these functions via remote CLI over SSHv2 or at the local console. The specific management capabilities available from the TOE include: • Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI, as described above, • Ability to configure the access banner, • Ability to configure the session inactivity time before session termination or locking, • Ability to update the TOE, and to verify the updates using hash comparison capability prior to installing those updates, • Ability to configure the authentication failure parameters; • Ability to configure audit behavior, in particularly, changes to the size of the audit space, ; • Ability to configure the cryptographic functionality. The ability to manage the cryptographic functionality which allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating RSA keys; • Ability to re-enable an Administrator account; • Ability to configure NTP; • Ability to configure the reference identifier for the peer (SAN-IP address and SAN-DNS hostname); • Import and delete X.509v3 certificates;

Requirement	TSS Description
	• Generate and delete cryptographic keys. In particular, a security administrator can generate and delete the cryptographic keys associated with CSRs.
FMT_SMR.2	The TOE supports multiple administrative roles when accessing the administrative interface through the local or remote CLI. These roles define the access that is allowed per role. Read-only users: - View system status and logs. - View policy configuration and reports. - View user information and statistics. - View proxy server and cache settings. - View network topology and connectivity information. Read/Write users: - Create, edit, and delete policies. - Configure and modify proxy settings. - Manage user accounts and groups. - Configure and manage authentication and authorization settings. - View and modify system logs and alerts. - Configure and manage network and SSL settings. Any user with either read-only or read/write user-role can use the local/remote interface securely using appropriate authentication to perform their tasks without compromising the security of the TOE.
FPT_APW_EXT.1	No passwords are ever stored as clear text. Passwords are stored on the TOE in a secured partition in non-plaintext. Prior to writing on disks each password is hashed (SHA-256) using the PBKDFv2 algorithm. During subsequent authentication attempts passwords entered are converted using the same PBKDFv2 algorithm. This is compared to the digest value for that user stored in the secured partition. Access is only granted if the values match.
FPT_SKP_EXT.1	All keys stored on the TOE are protected from unauthorized modification and substitution. The TOE stores symmetric keys only in volatile memory never on persistent media. The TOE admin interface does not provide any mechanism to view sensitive data (passwords or keys) once stored. Unauthenticated operators do not have write access to modify, change, or delete keys. The TOE stores all asymmetric keys in a secure directory that is not readily accessible to administrators; therefore, there is no administrative interface access provided to directly manipulate the keys.
FPT_STM_EXT.1	The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the NTP configuration. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The time can be updated by a Security Administrator automatically by configurating NTP synchronization.

Requirement	TSS Description
FPT_TST_EXT.1	The TOE runs a suite of self-tests during initial start-up to verify its correct operation. During the system bootup process (power on or reboot), the TOE performs various power-on self-test (POSTs) for the cryptographic components of the TOE. During initialization and but prior to the underlying OS initialization of external interfaces; this prevents the security appliances from passing any data before self-test execution, the module inhibits all access to the cryptographic algorithms. Additionally, the power-on self-tests are performed after the cryptographic systems are initialized completing self-tests. In the event of a power-on self-test failure, the cryptographic module will force the platform to reload and reinitialize the operating system and cryptographic components. This operation ensures no cryptographic algorithms can be accessed unless all power on self-tests is successful. These tests include: • AES Known Answer Test - For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly. • HMAC Known Answer Test - For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly. • RNG/DRBG Known Answer Test - For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly. • SHA Known Answer Test – For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match, and the hash operations are operating correctly. • RSA Signature Known Answer Test (both signature/verification) - This test takes a known plaintext value and Private/Public key pair and uses the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly. • DH Known Answer Test – This test takes known input to the “z” calculation for Diffie-Hellman and compares the result to a known “z” value.

Requirement	TSS Description
	• ECDH Known Answer Test – This test takes known input to the "z" calculation for Elliptic Curve Diffie-Hellman and compares the result to a known "z" value.
FPT_TUD_EXT.1	Authorized Administrator can query the software version running on the TOE by using the 'show version' command and can initiate updates to software images. When software updates are made available, an administrator can obtain, verify the integrity of the software by manually verifying the hash of the downloaded software with the hash published on the website, and install those updates. The updates can be downloaded from https://support.broadcom.com/group/ecx/downloads?. During the execution of the image, an integrity check will be performed. Only if the hash is correct, will the image be installed. If an update is unsuccessful, a message is delivered to the user. Since the update process attempts to update a different copy than what is currently being run, the current active image remains the same and the user continues to run the same code that was being run before the upgrade attempt was made. There is no delayed activation of the software version. FOR EXSi TOE: · When the restart upgrade command is initiated, the TOE is rebooted with the freshly loaded image. FOR SSP TOE: · When an application is created for a particular software version, and that application is started, that software image is activated.
FTA_SSL_EXT.1 FTA_SSL.3 FTA_SSL.4	The TOE provides the administrative user to define inactivity time out periods for administrative sessions. The inactivity period is the same for CLI (local and remote) and are configured through the TOE administrative interfaces. If an administrative session remains inactive for the configured length of time, the administrative session is terminated. After termination, administrative authentication is required to access any of the administrative functionality of the TOE. This is applicable from both local and remote administrative sessions. An Authorized Administrator is able to exit out of both local and remote administrative sessions. When accessing the TOE via the CLI (both local and remote), the exit command is used.
FTA_TAB.1	For TOE administration, the CLI (SSH) and local console CLI are available. Prior to an administrative user authenticating, that user is presented with an access display banner which displays an advisory notice and consent warning message regarding unauthorized use of the TOE. This banner will be displayed prior to allowing Administrator access through those interfaces.

Requirement	TSS Description
FTP_ITC.1	The TOE protects communications with authorized audit server via TLS. This protects the data from disclosure by encryption and by checksums that verify that data has not been modified.
FTP_TRP.1/Admin	All remote administrative communications take place over a secure encrypted session. Remote CLI connections take place over an SSHv2 tunnel. The SSHv2 session is encrypted using AES encryption. The remote administrators are able to initiate SSHv2 communications with the TOE. The TOE rejects all insecure remote authentication attempts (e.g., telnet).

7.1 CAVP Algorithm Certificate Details

Each of these cryptographic algorithms have been validated as identified in Table 14 below.

Table 14 – CAVP Algorithm Certificate References

Algorithm	Description	Standard	CAVP Certificate	SFR
AES	Encryption/Decryption	AES specified in ISO 18033-3 CTR as specified in ISO 10116 GCM specified in ISO 19772	A2936	FCS_COP.1/DataEncryption
RSA	Key Generation Signature Generation/Verification	FIPS 186-4	A2936	FCS_CKM.1 FCS_COP.1/SigGen
HMAC	Keyed-Hashing	ISO/IEC 9797-2:2011	A2936	FCS_COP.1/KeyedHash
SHS	Hashing	ISO/IEC 10118-3:2004	A2936	FCS_COP.1/Hash
KAS-ECC Component	Key Establishment	SP 800-56A	A2936	FCS_CKM.2
DRBG	Random Bit Generation	SP800-90A	A2936	FCS_RBG_EXT.1

7.2 Cryptographic Key Destruction

The table below describes the key zeroization provided by the TOE and as referenced in FCS_CKM.4.

Table 15 - Key Storage and Zeroization

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
Master Encryption Key (MEK)	Encrypting Crypto-Officer password, RSA private key	Stored in plaintext on non-volatile memory	By disabling the FIPS-Approved mode of operation
Integrity Test Public Key	Verifying the integrity of the system image during upgrade or downgrade	Stored in plaintext on non-volatile memory	Overwritten after upgrade by the key in the newly signed image
RSA Public Keys	Negotiating TLS or SSH sessions	Stored in encrypted form on non-volatile memory	Module's public key is deleted by command
RSA Public Key	Negotiating TLS or SSH sessions	Other entities' public keys reside on volatile memory	Other entities' public keys are cleared by power cycle
RSA Private Keys	Negotiating TLS or SSH sessions	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing encrypting MEK
DH public key	Negotiating TLS or SSH sessions	Stored in plaintext on volatile memory	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power
DH private key	Negotiating TLS or SSH sessions	Stored in plaintext on volatile memory	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power
ECDH private key	Negotiating TLS or SSH sessions	Stored in plaintext on volatile memory	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power
ECDH public key	Negotiating TLS or SSH sessions	Stored in plaintext on volatile memory	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
TLS or SSH Session key	Encrypting TLS or SSH data	Stored in plaintext on volatile memory	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power
TLS or SSH Session Authentication key	Data authentication for TLS or SSH sessions	Resides in volatile memory in plaintext	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power
Crypto Officer Password User Password	Locally authenticating a CO or User for Management Console or CLI	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypted MEK
“Enabled” mode password	Used by the CO to enter the “privileged” or “enabled” mode when using the CLI	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting MEK
“Setup” Password	Used by the CO to secure access to the CLI when accessed over the serial port	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting MEK
SP 800-90A CTR_DRBG Seed	Seeding material for the SP800-90A CTR_DRBG	Plaintext in volatile memory	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power
SP 800-90A CTR_DRBG Entropy	Entropy material for the SP800-90A CTR_DRBG	Plaintext in volatile memory	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power

8 Acronym Table

Acronyms should be included as an Appendix in each document.

Table 16 - Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
DH	Diffie Hellman
DRBG	Deterministic Random Bit Generator
ECDH	Elliptic Curve Diffie Hellman
GCM	Galois Counter Mode
IP	Internet Protocol
NDcPP	Network Device collaborative Protection Profile
NIAP	Nation Information Assurance Partnership
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest, Shamir & Adleman
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
ST	Security Target
SWG	Secure Web Gateway
TOE	Target of Evaluation
TLS	Transport Layer Security
TSS	TOE Summary Specification
CDP	CRL Distribution Point