Symantec, A Division of Broadcom

Edge SWG

FIPS 140-3 Non-Proprietary Security Policy

Prepared by:

acumen security

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document describes the security policy for the Edge SWG (SW version: SGOS 7.4) cryptographic module. It contains specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the

FIPS 140-3 standard. The module type is software-hybrid and has a multi-chip standalone embodiment.

1.2 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	2
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

1.3 Additional Information

The Edge SWG appliances from Symantec provide companies with 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 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

• When paired with other Symantec technologies, it can provide:
    o Malware detection using multiple anti-malware engines and detection methods

    o Multi-layered deep content inspection and analysis to detect spam and application-level threats in the payloads of network traffic

    o Data Loss Prevention (DLP) to identify confidential information and block it from leaving the corporate network

    o 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

    o 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

• Integration the world's largest civilian threat intelligence dataset with the Symantec Global Intelligence Network (GIN)

The Symantec Global Intelligence Network (GIN), which monitors more than 175 million endpoints and Edge SWGs protects 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.

The security provided by the Edge SWG can be used to control, protect, and monitor the Internal Network's use of controlled protocols on the External Network. The controlled protocols[1] implemented are:

• Windows Media Optimization (Microsoft Media Streaming (MMS))
• Microsoft Smooth Streaming Optimization
• Real Media Optimization
• Real-Time Streaming Protocol (RTSP) Optimization
• Real-Time Messaging Protocol (RTMP) Optimization
• QuickTime Optimization (Apple HTTP Live Streaming)
• Adobe Flash Optimization (Adobe HTTP Dynamic Streaming)
• Bandwidth Management
• DNS proxy
• Advanced DNS Access Policy
• Hypertext Transfer Protocol (HTTP)/Secure Hypertext Transfer Protocol (HTTPS) Acceleration
• File Transfer Protocol (FTP) Optimization
• Secure Sockets Layer (SSL) Termination/Protocol Optimization
• TCP2 tunneling protocols (Secure Shell (SSH))
• Secure Shell
• Telnet Proxy
• ICAP Services
• Netegrity SiteMinder
• Oblix COREid

[1] These protocols are not executed by the cryptographic module.

• Peer-To-Peer
• User Authentication
• Onbox Content Filtering (3rd Party or BCWF2)
• Offbox Content Filtering (via ICAP)
• SOCKS

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module is a software-hybrid module and has a Multi-Chip Standalone embodiment, that meets overall Level 1 FIPS 140-3 requirements. The module was tested and found complaint on a Dell PowerEdge R440 Server using VMware ESXi v6.5 hypervisor and Symantec SSP-S410 using KVM v2.3.

The module software consists of Symantec's proprietary operating system, SGOS v7.4. Acting as the guest OS in the respective hypervisors, this full-featured operating system includes both OS-level functions as well as the application-level functionality that provides the appliance's optimization and proxying services.

The module software version 7.4 contains the following cryptographic libraries:
• SGOS Cryptographic Library v5.1.1
• VA Blue Coat Boot Loader v5.31

Module Type: Software-hybrid

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The cryptographic boundary of the module (shown by the yellow line in Figures 2 & 3) consists of the SGOS v7.4 (which contains the VA Blue Coat Boot Loader v5.31, and the SGOS Cryptographic Library v5.1.1) and the processors for cryptographic acceleration as listed in Table "Tested Module Identification – Hybrid Disjoint Hardware".

Tested Operational Environment's Physical Perimeter (TOEPP):

The Tested Operational Environment's Physical Perimeter (TOEPP) of the module is the SSP S410 and Dell PowerEdge R440 platforms, in which the module executes.

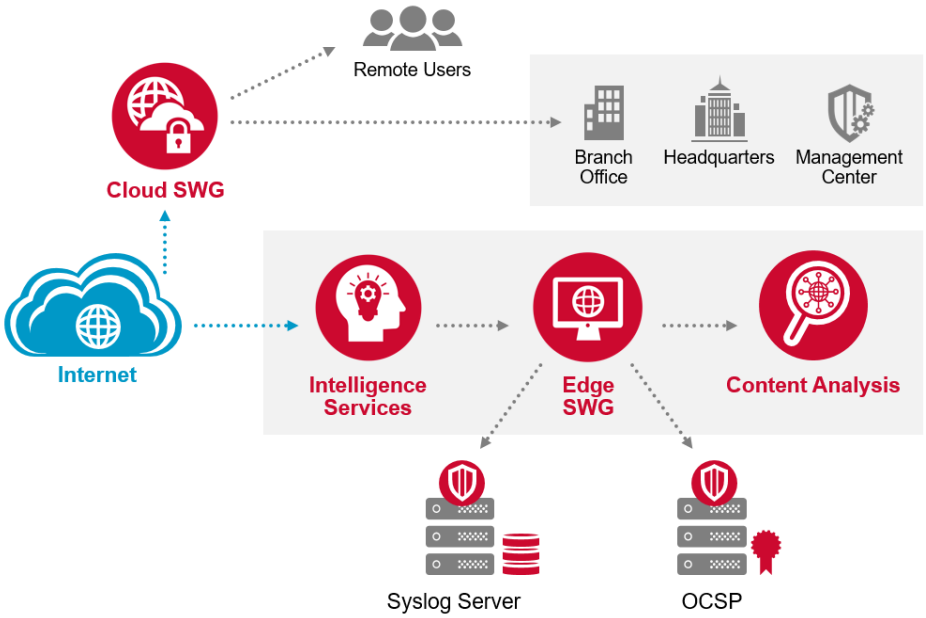

Figure 1 - Typical Deployment of a Secure Web Gateway Virtual Appliance

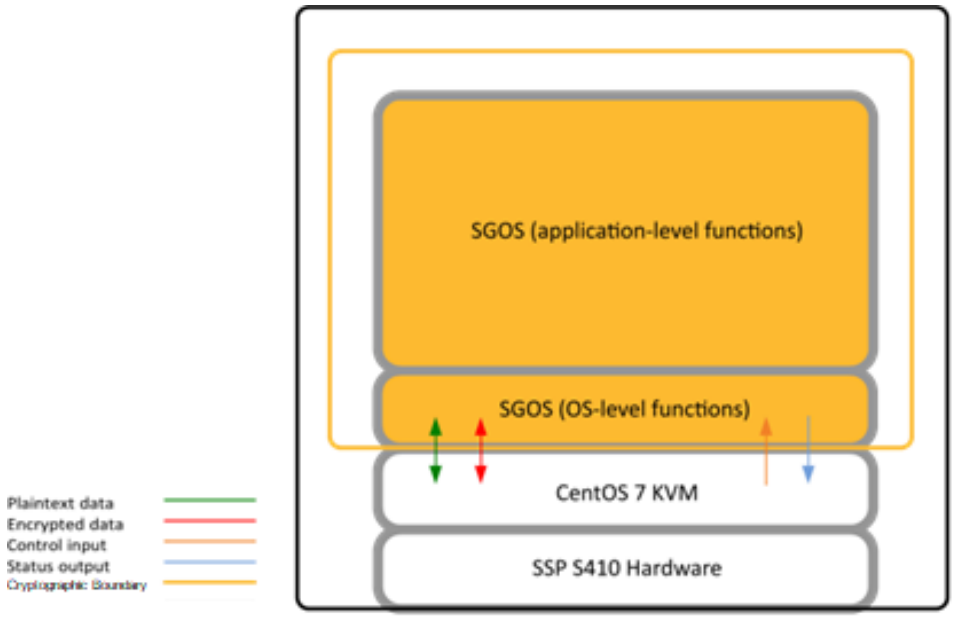

Figure 2: Cryptographic Boundary Block Diagram for SSP S410

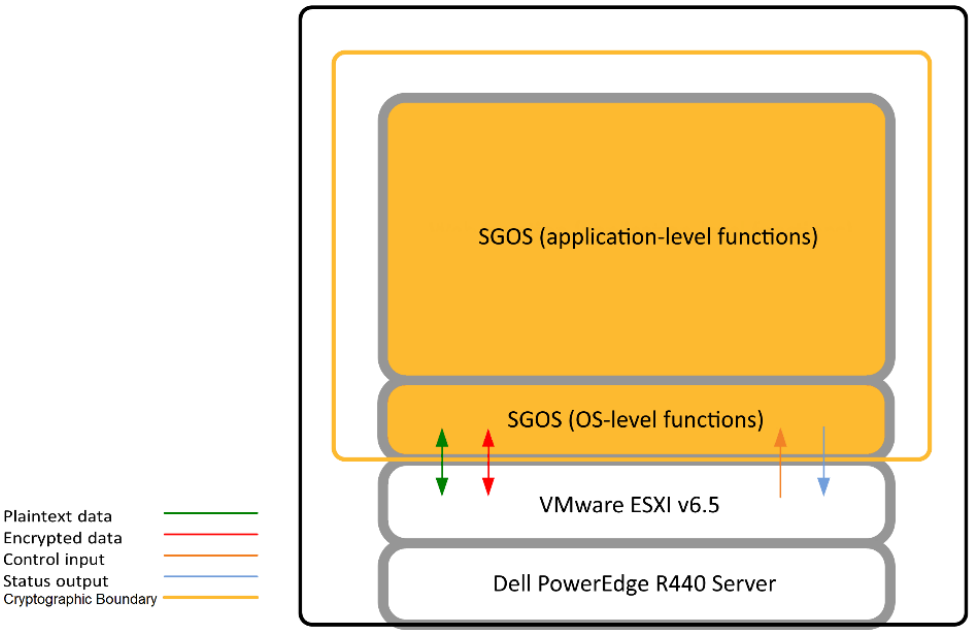

Figure 3 - Cryptographic Boundary Block Diagram for Dell PowerEdge R440

Figure 4 - Intel Xeon Silver 4210

Figure 5 - Intel Xeon Silver 4216

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

Package or File Name	Software/ Firmware Version	Features	Integrity Test
7.4.0.0_build_279954_system_gdb.bcsi	7.4		RSA Signature Verification and HMAC-SHA1

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Intel Xeon Silver 4210	Intel Xeon Silver 4210		Intel Xeon Silver 4210	
Intel Xeon Silver 4216	Intel Xeon Silver 4216		Intel Xeon Silver 4216	

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
SGOS v7.4	Symantec SSP-S410	Intel Xeon Silver 4210	Yes	KVM v2.3	7.4
SGOS v7.4	Dell PowerEdge R440	Intel Xeon Silver 4216	Yes	VMware ESXi v6.5	7.4

Table 4: Tested Operational Environments - Software, Firmware, Hybrid

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform
SGOS v7.4	Microsoft Azure Hypervisor running on Intel Xeon Platinum 8272CL processor
SGOS v7.4	AWS Xen Hypervisor running on Intel Xeon E5-2686 v4 processor
SGOS v7.4	Google Cloud Platform running on Intel Xeon® E5-2689 processor
SGOS v7.4	Microsoft Hyper-V hypervisor running on Intel Xeon Platinum 8260L processor running on Dell PowerEdge R840 server

Table 5: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 Excluded Components

There are no components excluded from the module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	The module supports approved mode of operation, once the initialization steps mentioned in Section 11.1 in the SP are completed.	Approved	Indicators specified for all approved services
Non-Approved Mode	The module supports non-approved mode of operation, where non-approved service are invoked.	Non-Approved	Indicators specified for all non-approved services

Table 6: Modes List and Description

The module supports two modes of operation: Approved and Non-Approved.

Mode Change Instructions and Status:

The module will be in Approved mode once the initialization steps mentioned in Section 11.1.1 are completed. See Tables 4 and 5 for a list of Approved or Allowed algorithms. To transition from Approved mode to Non-Approved mode, the operator should execute “fips-mode-disable” which will trigger zeroization via module reboot. To transition from Non-Approved mode of operation to Approved mode, the operator must run the command “fips-mode enable” along with the initialization instructions as specified in Section 11.1.1. If the initialization steps are not followed as specified in Section 11.1.1, then the module may be operational, in a non-compliant state.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A2936	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A2936	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 8-128 Increment 8	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
		Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	
AES-GCM	A2936	Direction - Decrypt, Encrypt IV Generation - External, Internal Key Length - 128, 192, 256 Tag Length - 104, 112, 120, 128, 32, 64, 96 IV Length - IV Length: 96-1024 Increment 8 Payload Length - Payload Length: 8-65536 Increment 8 AAD Length - AAD Length: 0-65536 Increment 8 IV Generation Mode - 8.2.1	SP 800-38D
Counter DRBG	A2936	Prediction Resistance - Yes Supports Reseed - Yes Mode - AES-128, AES-192, AES-256 Derivation Function Enabled - No, Yes Additional Input - Additional Input: 0-256 Increment 256, Additional Input: 256, Additional Input: 320, Additional Input: 384 Entropy Input - Entropy Input: 128-256 Increment 128, Entropy Input: 256, Entropy Input: 256-512 Increment 128, Entropy Input: 320, Entropy Input: 384 Nonce - Nonce: 0, Nonce: 128 Personalization String Length - Personalization String Length: 0-256 Increment 256, Personalization String Length: 256, Personalization String Length: 320, Personalization String Length: 384 Returned Bits - 256	SP 800-90A Rev. 1
HMAC-SHA-1	A2936	MAC - MAC: 32-160 Increment 8 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA-1	A3192	MAC - MAC: 32-160 Increment 8 Key Length - Key Length: 256-1024 Increment 128	FIPS 198-1
HMAC-SHA2-224	A2936	MAC - MAC: 32-224 Increment 8 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A2936	MAC - MAC: 32-256 Increment 8 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A2936	MAC - MAC: 32-384 Increment 8 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A2936	MAC - MAC: 32-512 Increment 8 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
KAS-FFC-SSC Sp800-56Ar3	A2936	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF SNMP (CVL)	A2936	Password Length - Password Length: 64, 128 Engine ID - 000002b87766554433221100, 80000D5904313030353537353531	SP 800-135 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
KDF SSH (CVL)	A2936	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
KDF TLS (CVL)	A2936	TLS Version - v1.2 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
PBKDF	A2936	Iteration Count - Iteration Count: 1-10000 Increment 1 HMAC Algorithm - SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 Password Length - Password Length: 8-128 Increment 8 Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 112-4096 Increment 8	SP 800-132
RSA KeyGen (FIPS186-4)	A2936	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Info Generated By Server - Yes Public Exponent Mode - Random Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4)	A2936	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA2-224	FIPS 186-4
RSA SigVer (FIPS186-4)	A2936	Signature Type - ANSI X9.31, PKCS 1.5, PKCSPSS Modulo - 1024, 2048, 3072, 4096 Hash Pair - Hash Algorithm - SHA-1 Public Exponent Mode - Random	FIPS 186-4
RSA SigVer (FIPS186-4)	A3192	Signature Type - PKCS 1.5 Modulo - 2048 Hash Pair - Hash Algorithm - SHA2-256 Public Exponent Mode - Random	FIPS 186-4
Safe Primes Key Generation	A2936	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	SP 800-56A Rev. 3
Safe Primes Key Verification	A2936	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	SP 800-56A Rev. 3
SHA-1	A2936	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA-1	A3192	Message Length - Message Length: 8-51200 Increment 8	FIPS 180-4
SHA2-224	A2936	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A2936	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	A3192	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4
SHA2-384	A2936	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A2936	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
TLS v1.3 KDF (CVL)	A2936	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK, PSK-DHE	SP 800-135 Rev. 1

Table 7: Approved Algorithms

The module implements the Approved algorithms[2] listed in the table above.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	Sections 4, 5.1, 5.2 and 6.1

Table 8: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
AES CBC	All backups are transmitted via SSH (encrypted by the session key), so any non-conformant encryption is redundant/not required for security (No security claimed)	Configuration backup encryption

Table 9: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
TLS v1.0/1.1 KDF with MD5	TLS 1.0/1.1 sessions
EC Diffie-Hellman	Remote management session via SSH and syslog

Table 10: Non-Approved, Not Allowed Algorithms

[2] There are algorithms, modes, and key/moduli sizes that have been CAVP-tested but are not used by any Approved service of the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by an Approved service of the module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Encryption	BC-UnAuth	Used to encrypt data		AES-CBC: (A2936) Direction: Encrypt AES-CTR: (A2936) Direction: Encrypt
Decryption	BC-UnAuth	Used to decrypt data		AES-CBC: (A2936) Direction: Decrypt AES-CTR: (A2936) Direction: Decrypt
Authenticated Encryption	BC-Auth	Used to encrypt data		AES-GCM: (A2936) Direction: Encrypt
Authenticated Decryption	BC-Auth	Used to decrypt data		AES-GCM: (A2936) Direction: Decrypt
Key Derivation 1	KAS-135KDF	Key derivation of protocols		KDF SNMP: (A2936) KDF SSH: (A2936) KDF TLS: (A2936) TLS v1.3 KDF: (A2936)
DRBG	DRBG	Random Bit Generator		Counter DRBG: (A2936)
Entropy Source	ENT-P	NIST SP800-90B compliant ENT (P)		
Message Authentication	MAC	Generate and verify message		HMAC-SHA-1: (A2936, A3192) HMAC-SHA2-224: (A2936) HMAC-SHA2-256: (A2936) HMAC-SHA2-384: (A2936) HMAC-SHA2-512: (A2936)

Name	Type	Description	Properties	Algorithms
Shared Secret Computation	KAS-SSC	Shared Secret Computation		KAS-FFC-SSC Sp800-56Ar3: (A2936)
KAS	CKG KAS-Full	Key Agreement Scheme	IG: IG D.F Scenario 2, path (2), split Caveat:Key establishment methodology provides between 112 and 200 bits of security strength Key confirmation:no Key derivation:IG 2.4.B SP 800-135rev1 CVL	KDF SSH: (A2936) KDF TLS: (A2936) TLS v1.3 KDF: (A2936) KAS-FFC-SSC Sp800-56Ar3: (A2936) Safe Primes Key Generation: (A2936) Safe Primes Key Verification: (A2936) CKG: () Key Type: Symmetric and Asymmetric
Key Derivation 2	PBKDF	Password based KDF		PBKDF: (A2936)
Asymmetric Key Generation	AsymKeyPair-KeyGen CKG	Asymmetric Key Generation, used for sign/verify operations		RSA KeyGen (FIPS186-4): (A2936) CKG: () Key Type: Symmetric and Asymmetric
Signature Generation	DigSig-SigGen	Digital Signature Generation using RSA		RSA SigGen (FIPS186-4): (A2936)
Signature Verification	DigSig-SigVer	Digital Signature Verification using RSA		RSA SigVer (FIPS186-4): (A2936, A3192)
Hashing	SHA	Used for message digest		SHA-1: (A2936, A3192) SHA2-224: (A2936) SHA2-256: (A2936, A3192) SHA2-384: (A2936) SHA2-512: (A2936)

Table 11: Security Function Implementations

2.7 Algorithm Specific Information

AES GCM IV Generation:

The module's AES-GCM implementation conforms to IG C.H scenarios 1a, 1d, 2 and 5.

The module is compliant with TLS 1.2 protocol per SP800-52rev2. The AES-GCM IV generation is compliant with RFC5288. The module supports acceptable AES-GCM ciphersuites from Section 3.3.1 of SP800-52rev2.

The module explicitly checks that the nonce_explicit part of the IV (i.e., counter) has not reached the maximum number of potential values (2^{64}-1) for a given session key. Upon detecting exhaustion of the counter, the module returns an error indication, prompting either connection abortion or initiation of a handshake to establish a new encryption key.

If the module experiences power loss and subsequently the power is restored, the calling application must ensure that any AES-GCM keys used for encryption or decryption are redistributed.

Scenario 1d SSHv2

The IV generation is in compliance with SSHv2 and used for AES-GCM encryption. The module is compliant with RFC4252, 4253 and 5647.

Scenario 2 Random internal IV generation

The module also supports an internal IV generation using the module's Approved DRBG, which is complaint with IG C.H and SP800-38D Section 8.2.2. The AES-GCM IV is generated randomly internal to the module using module's Approved DRBG. The DRBG seeds itself from the entropy source. The GCM IV is 96 bits in length. Per Section 9, this 96-bit IV contains 96 bits of entropy.

Scenario 5 TLS 1.3

The module supports a compliant TLS 1.3 as defined in RFC8446. The module uses the ciphersuites found in Appendix B.4 of RFC8446 and the acceptable AES-GCM ciphersuites from Section 3.3.1 of SP800-52rev2. The ciphersuites explicitly select AES-GCM as the encryption/decryption ciphers. The module implements, within its boundary, an IV generation unit for TLS 1.3 that keeps control of the 64-bit counter value within the AES-GCM IV.

If the module experiences power loss and subsequently the power is restored, the calling application must ensure that any AES-GCM keys used for encryption or decryption are redistributed. Upon detecting exhaustion of the counter, the module returns an error indication, prompting either connection abortion or initiation of a handshake to establish a new encryption key.

PBKDF:

Per IG D.N, keys generated using PBKDF shall only be used in data storage applications. The minimum password length allowed is 8 characters and the maximum password length is 64. The worst-case probability of guessing the value is 62^8 assuming all characters are digits, upper-case letters and/or lower-case letters. The operator shall choose the password length and the iteration count in such a way that the combination will make the key derivation computationally intensive. PBKDF is implemented to support option 1a specified in section 5.4 of SP800-132. The keys derived from SP800-132 map to section 3.1 of SP800-133rev2 as indirect generation from DRBG. The minimum iteration count enforced is 10000 and the value is chosen considering both the security that it provides and the performance of the process. The derived keys may only be used in storage applications.

RSA:
Per IG C.F, the RSA modulus lengths supported by the module for RSA signature generation are 2048, 3072, or 4096 bits.

2.8 RBG and Entropy

The Entropy required by the Approved SP800-90Arev1 CTR_DRBG (with AES-256) is supplied by the ENT (P). Per IG D.J, the minimum number of bits of entropy is 256-bits and the estimated amount of entropy per the source's output bit is 0.6.

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
NIST SP800-90B ENT (P)	Physical	Intel Xeon Silver 4210, 4216	1 bit	0.81	AES-CBC-MAC SP800-90B Cert. #A2138

Table 12: Entropy Sources

2.9 Key Generation

Per IG D.H, the vendor affirms symmetric keys and seeds for asymmetric keys are generated per SP800-133rev2 (unmodified output from a DRBG).

2.10 Key Establishment

The module supports "Key Agreement Scheme" per SP800-56Arev3; Scenario 2 path 2 of FIPS 140-3 IG D.F key establishment methodology providing between 112 and 200 bits of encryption strength.

2.11 Industry Protocols

No parts of the TLS, SSH, and SNMP protocols, other than the KDF, have been reviewed or tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Input Registers	Data Input	Input packets
Output Registers	Data Output	Output packets
Control Registers	Control Input	Input packets (Configuration or Administrative data)
Status Registers	Status Output	Status

Table 13: Ports and Interfaces

As a software-hybrid module, the virtual appliance has no physical characteristics. The module's physical and electrical characteristics, manual controls, and physical indicators are those of the host system (Dell PowerEdge R440 and S410 Server) and out of scope of this validation. The hypervisor provides virtualized ports and interfaces for the module. Interaction with the virtual ports created by the hypervisor occurs through the host system's Ethernet port. Management, data, and status traffic must all flow through the Ethernet port. Direct interaction with the module via the host system is possible over the serial port; however, the Crypto Officer must first map the physical serial port to the module using vSphere Client.

Data input and output are the packets utilizing the services provided by the modules. These packets enter and exit the module through the Virtual Ethernet ports. Control input consists of Configuration or Administrative data entered into the modules. Control input enters the module via the Virtual Ethernet and Virtual Serial Port interfaces (SSH CLI, and Serial CLI). Status output consists of the status provided or displayed via the user interfaces (such as SSH CLI, and Serial CLI) or available log information. Status output exits the module via the user interfaces (such as SSH CLI, and Serial CLI) over the Virtual Ethernet or Virtual Serial Ports. The module does not implement a control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password	Password based authentication	Password	For password authentication done by the module, passwords are required to be at minimum 8 characters in length, and at maximum 64 bytes (number of	The Crypto-Officer may connect locally using the serial port or remotely after establishing a SSH session. The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 ×10^6 × 60 = 6 × 10^10) =

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
			characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1: (95^8), or 1:6,634,204,312,890,625 chance of false acceptance which is less than 1:1,000,000	60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: 1 : [95^8 possible passwords / ((6 ×10^10 bits per minute) / 64 bits per password)] = 1: (95^8 possible passwords / 937,500,000 passwords per minute). This equals 1: 7,076,484 or 1 in 7.0 million; this is less than 1:100,000 as required by FIPS 140-3
Public Key Authentication	Public Key based authentication	RSA SigVer (FIPS186-4) (A2936)	The module supports using RSA keys for authentication of Users during SSH. Using conservative estimates and equating a 2048-bit RSA key to a 112-bit symmetric key, the probability for a random attempt to succeed is 1:2^112 or 1: 5.19 x 10^33 which is less than 1:1,000,000	The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 ×10^6 × 60 = 6 × 10^10) = 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is less than 1: (2^112 / 6×10^10), or 1: 86,538,280,975,580,460,475,508, which is less than 1:100,000 as required by FIPS 140-3

Table 14: Authentication Methods

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto-Officer (CO)	Role	Crypto Officer	Password Public Key Authentication
User	Role	User	Password Public Key Authentication

Table 15: Roles

The module supports both Crypto-Officer (CO) and User role. Before accessing the modules for any administrative services, COs and Users must authenticate to the module according to the methods specified in “Authentication Methods” Table. The module offers Command Line Interface:

- Command Line Interface (CLI): Accessible locally via the serial port (provides access to the Setup Console portion of the CLI which requires the additional “Setup” password to gain access) or remotely using SSH. This interface is used for management of the modules. This interface must be accessed locally via the serial port to perform the initial module configurations (IP address, DNS server, gateway, and subnet mask) and placing the modules into the Approved mode. When the module has been properly configured, this interface can be accessed via SSH. Management of the module may take place via SSH or locally via the serial port. Authentication is required before any functionality will be available through the CLI.

When managing the module over the CLI, COs and Users both log into the modules with administrator accounts entering the “standard”, or “unprivileged” mode on the module. Unlike Users, COs can enter the “enabled” or “privileged” mode after initial authentication to the CLI by supplying the “enabled” mode password. Additionally, COs can only enter the “configuration” mode from the “enabled” mode via the CLI, which grants privileges to make configuration level changes. Going from the “enabled” mode to the “configuration” mode does not require additional credentials. The details of these modes of operation are found below:

Crypto-Officer role and privileges:

- The CO is an administrator of the module that has “enabled” mode access while using the CLI.

- When the CO is using the CLI, and while in the “enabled” mode of operation, COs may put the module in its Approved mode, reset to the factory state (local serial port only) and query if the module is in Approved mode. In addition, COs may do all the services available to Users while not in “enabled” mode.

- Once the CO has entered the “enabled” mode, the CO may then enter the “configuration” mode via the CLI. The “configuration” mode provides the CO management capabilities to perform tasks such as account management and key management.

User role and privileges:

- The User is an administrator of the module that operates only in the “standard” or “unprivileged” mode and has not been granted access to the “enabled” mode in the CLI.

- The User may access the CLI for management of the module.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Module Initialization	Set up the first-time network configuration, CO username and password, and enable the module in the Approved mode	"FIPS mode enabled" will be visible on the serial console upon the successful completion of the cryptographic algorithm self-tests	N/A	N/A	None	Crypto-Officer (CO) - Crypto Officer Password: W,E - "Enabled mode" Password: W,E - "Setup" Password: W,E
Enable mode	Manage the module in the "enabled" mode of operation, granting access to higher privileged commands	Successful completion of the service and "enable mode" prompt (i.e., the command line prompt where it specifies "enable" keyword)	N/A	N/A	None	Crypto-Officer (CO) - "Enabled mode" Password: W,E
Configuration mode	Manage the module in the "configuration" mode of operation, allowing permanent system modification to be made	Successful completion of the service and "configure mode" prompt (i.e., the command line prompt where it specifies "configure" keyword)	N/A	N/A	None	Crypto-Officer (CO)
Disable Approved mode	Take the module out of the Approved mode of operation	N/A	"fipsmode disable" command	N/A	None	Crypto-Officer (CO) - "Enabled mode" Password:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	and restore it to factory state					W,E - Master Encryption Key (MEK): Z - SSH Session Key: Z - SSH Session Authentication Key: Z - DRBG Seed: Z - DRBG Key Value: Z - DRBG V Value: Z
Software load	Loads new external software and performs an integrity test using an RSA digital signature	Image loaded successfully (for verified image). Image loading fails (when image verification fails)	N/A	Verification status	Signature Verification	Crypto-Officer (CO)
Create remote management session (SSH CLI)	Manage the module through the CLI (SSH) remotely	Successful connection to the module via SSH and "System is in FIPS mode" is displayed after executing "show version" command and "Diffie-hellman" groups displayed	Client RSA public key	N/A	Encryption Decryption Authenticated Encryption Authenticated Decryption Key Derivation 1 DRBG Entropy Source Message Authentication Shared	Crypto-Officer (CO) - RSA Public Key: R,E - RSA Private Key: R,E - Client RSA Public Key: R,E - DH Public Key: G,R,W,E - DH Private Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		after executing "kexalgs view" command			Secret Computation KAS Asymmetric Key Generation Signature Generation Signature Verification Hashing	G,R,W,E - SSH Session Key: G,R,W,E - SSH Session Authentication Key: G,R,W,E - DRBG Seed: G,E - DRBG Key Value: G,E - DRBG V Value: G,E - Master Encryption Key (MEK): R,E - Entropy Input: G,E - Shared Secret: G,E - SP 800-56Arev3 Domain Parameters: R,E User - RSA Public Key: R,E - RSA Private Key: R,E - Client RSA Public Key: R,E - DH Public Key: G,R,W,E - DH Private Key: G,R,W,E - SSH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Session Key: G,R,W,E - SSH Session Authentication Key: G,R,W,E - DRBG Seed: G,E - DRBG Key Value: G,E - DRBG V Value: G,E - Master Encryption Key (MEK): R,E - Entropy Input: G,E - Shared Secret: G,E - SP 800-56Arev3 Domain Parameters: R,E
Create, edit, and delete operators	Create, edit, and delete operators (these may be Cos or Users); define operator's accounts, change password, and assign permissions	N/A	N/A	N/A	None	Crypto-Officer (CO) - Crypto Officer Password: R,W,E,Z - User Password: R,W,E,Z
Create, edit, and delete operator groups	Create, edit, and delete operator groups; define	N/A	N/A	N/A	None	Crypto-Officer (CO)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	common sets of operator permissions					
Create filter rules	Create filters that are applied to user data streams	N/A	N/A	N/A	None	Crypto-Officer (CO)
Show Approved status (Show Version)	The command "show version" will display if the module is configured in Approved mode	Successful completion of the service and "System is in FIPS mode" is displayed after executing "show version" command	N/A	Successful completion of the service and "System is in FIPS mode" is displayed after executing "show version" command	None	Crypto-Officer (CO) User
Syslog	Setup syslog for logging	Connection established to syslog server successfully and "tls 1.2, tls 1.3" versions and "dhe" cipher suites displayed after executing "view ssldevice-profile " command	Syslog commands	N/A	Encryption Decryption Authenticated Encryption Authenticated Decryption DRBG Entropy Source Message Authentication KAS Asymmetric Key Generation Signature Generation Signature	Crypto-Officer (CO) - RSA Public Key: R,E - RSA Private Key: R,E - Client RSA Public Key: R,E - DH Public Key: G,R,W,E - DH Private Key: G,R,W,E - TLS Session Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Verification Hashing	G,R,W,E - TLS Session Authentication Key: G,R,W,E - DRBG Seed: G,E - DRBG Key Value: G,E - DRBG V Value: G,E - Master Encryption Key (MEK): R,E - Shared Secret: G,E
Import, replace, and delete SNMP keys	Create, edit, and delete operators (these may be COs or Users); define operator's accounts, change password, and assign permissions	N/A	N/A	N/A	None	Crypto-Officer (CO)
Create SNMPv3 session	Monitor the module using SNMPv3	Successful completion of the service and "System is in FIPS mode" is displayed after executing "show version" command	SNMP parameters (username, security level, target IP/port, authentication key, password)	N/A	Key Derivation 1	Crypto-Officer (CO) - SNMPv3 Privacy Key: R,E - SNMPv3 Session Authentication Key: R,E - SNMPv3 Password: R,E - Master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Key (MEK): R,E
Manage module configuration	Backup or restore the module configuration	Successful completion of the service and "System is in FIPS mode" is displayed after executing "show version" command and "Diffiehellman" groups displayed after executing "kexalgs view" command	Commands for the respective configurations	N/A	Key Derivation 1	Crypto-Officer (CO) - RSA Public Key: R,W,E - RSA Private Key: R,W,E - SSH Session Key: G,R,W,E - SSH Session Authentication Key: G,R,W,E - Crypto Officer Password: R,W,E - User Password: R,W,E - "Enabled mode" Password: R,W,E - Master Encryption Key (MEK): R,E
Zeroize keys (serial port only)	Zeroize keys by taking the module out of the Approved mode and restoring it to a factory state. This will zeroize all CSPs.	Successful reboot after executing "fipsmode disable"	N/A	N/A	None	Crypto-Officer (CO) - Master Encryption Key (MEK): Z - SSH Session Key: Z - SSH Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	The zeroization occurs while the module is still in Approved-mode					Authentication Key: Z - TLS Session Key: Z - TLS Session Authentication Key: Z - DH Private Key: Z
Change password hash local user password	Change Crypto Officer password	Successful completion of the service and "System is in FIPS mode" is displayed after executing "show version" command	N/A	N/A	Key Derivation 2	Crypto-Officer (CO) - Crypto Officer Password: G,W - Master Encryption Key (MEK): R,E
Reboot the module (and perform selftests)	Perform periodic self-test on demand by power cycling the host platform	"FIPS mode enabled" will be visible on the serial console upon the successful completion of the cryptographic algorithm self-tests	N/A	N/A	None	Crypto-Officer (CO) - DH Public Key: Z - DH Private Key: Z - SSH Session Key: Z - SSH Session Authentication Key: Z - TLS Session Key: Z - DRBG Seed: Z - DRBG Key Value: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG V Value: Z - Master Encryption Key (MEK): R,E
Utility	Services that do not use any SSP	N/A	Input parameters for the utility function	N/A	None	Crypto-Officer (CO) User

Table 16: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Proxy Traffic	Proxy Traffic involves the use of TLS v1.0/1.1 sessions, which leverage MD5	TLS v1.0/1.1 KDF with MD5	Crypto-Officer (CO), User
Create remote management session (CLI)	Manage the module through the CLI (SSH) remotely	EC Diffie-Hellman	Crypto-Officer (CO), User

Table 17: Non-Approved Services

4.5 External Software/Firmware Loaded

The form of the module is a single image file "7.4.0.0_build_279954_system_gdb.bcsi". The module performs software loading and software load test but does not support complete image replacement.

4.6 Bypass Actions and Status

Not applicable to this module

4.7 Cryptographic Output Actions and Status

The module supports self-initiated cryptographic capability to establish secure connections to external services for licensing and subscription downloads. To prevent inadvertent output due to a single error, this capability is turned on only after obtaining confirmation from the CO:

To properly function, this appliance will need to initiate cryptographically secure connections to external services such as licensing and subscription downloads.

Do you wish to proceed? (y/n)[n]: y
Please enter‘ ’y' again to confirm? (y/n)[n]:

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs pre-operational integrity test using HMAC-SHA-1 and RSA 2048 Signature Verification with SHA2-256.

5.2 Initiate on Demand

The integrity test can be executed on demand by power-cycling the host platform.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied:

Per FIPS 140-3 specifications the module operates in a modifiable operational environment. The module runs on general purpose computers listed in Table “Tested Operational Environments - Software, Firmware, Hybrid”. Additionally, the module only allows the loading of software through the software load test, which ensures the image is appropriately signed by Broadcom, Inc. As such, the applicable modifiable operational environment requirements do apply.

7 Physical Security

The module type is software-hybrid and has a multi-chip standalone embodiment running on a production grade chassis.

8 Non-Invasive Security

This section is not applicable. The module does not implement non-invasive security measures.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
NVRAM	Non-volatile memory	Static
RAM	Volatile memory	Dynamic

Table 18: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input_1	External to the module boundary	RAM	Plaintext	Manual	Electronic	
Input_2	External to the module boundary	NVRAM	Encrypted	Manual	Electronic	Encryption
Output_1	RAM	External to the module boundary	Plaintext	Manual	Electronic	
Output_2	NVRAM	External to the module boundary	Encrypted	Manual	Electronic	Encryption

Table 19: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power Cycle	All SSPs stored in the RAM are zeroized after power cycle	All SSPs stored in the RAM are zeroized after power cycle, thus preventing reuse	On demand, via power cycle
Command based	SSPs can be zeroized by command	SSPs zeroized by command are rewritten with zeros thus preventing reuse	On demand, by issuing command

Table 20: SSP Zeroization Methods

The CO can return the module to its factory state by entering the “enabled” mode on the CLI, followed by the “fips-mode disable” command. This command will automatically reboot the module and zeroize the MEK. The RSA Private Key, Crypto Officer password, User password, “Enabled” mode password, “Setup” password, SNMP Privacy key, and the SNMP Session Authentication key are stored encrypted by the MEK. Once the MEK is zeroized, decryption involving the MEK becomes impossible, making these CSPs unobtainable by an attacker.

In addition, rebooting the module causes all temporary keys stored in volatile memory (SSH Session key, TLS session key, DRBG entropy values, and ENT (P) entropy values) to be zeroized. The Crypto-Officer must wait until the module has successfully rebooted to verify that zeroization has completed.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Master Encryption Key (MEK)	Used for encrypting Crypto Officer Password, User Password, RSA Private Key	256 bit - 256 bit	Symmetric - CSP	DRBG		
RSA Public Key	Used in negotiating TLS or SSH sessions	2048, 3072 and 4096 bit - 112, 128 and 152 bit	Asymmetric Public - PSP	DRBG Asymmetric Key Generation		Signature Generation Signature Verification
Client RSA Public Key	Used in negotiating TLS or SSH sessions	2048, 3072 and 4096 bit - 112, 128 and 152 bit	Asymmetric Public - PSP			
RSA Private Key	Used in negotiating TLS or SSH sessions	2048, 3072 and 4096 bit - 112, 128 and 152 bit	Asymmetric Private - CSP	DRBG Asymmetric Key Generation		Signature Generation Signature Verification
DH Public Key	Used in negotiating TLS or SSH sessions	2048 bit - 112 bit	Asymmetric Public - PSP	DRBG Asymmetric Key Generation		Shared Secret Computation KAS
DH Private Key	Used in negotiating TLS or SSH sessions	2048 bit - 112 bit	Asymmetric Private - CSP	DRBG Asymmetric Key Generation		Shared Secret Computation KAS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS Session Key	Encrypting TLS data	128, 192, 256 bit - 128, 192, 256 bit	Symmetric - CSP		KAS	Encryption
SSH Session Key	Encrypting SSH data	128, 192, 256 bit - 128, 192, 256 bit	Symmetric - CSP		KAS	Encryption
TLS Session Authentication Key	Data authentication for TLS sessions	128, 256, 384, 512 bit - 128-256 bit	Authentication - CSP		KAS	Message Authentication
SSH Session Authentication Key	Data authentication for SSH sessions	128, 256, 384, 512 bit - 128-256 bit	Authentication - CSP		KAS	Message Authentication
Crypto Officer Password	Locally authenticating a CO for CLI	Minimum of eight (8) and maximum of 64 bytes long printable character string - N/A	Password - CSP			
User Password	Locally authenticating an user for CLI	Minimum of eight (8) and maximum of 64 bytes long printable	Password - CSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		character string - N/A				
"Enabled mode" Password	Used by the CO to enter the "privileged" or "enabled" mode when using the CLI	Minimum of eight (8) and maximum of 64 bytes long printable character string - N/A	Password - CSP			
"Setup" Password	Used by the CO to secure access to the CLI when accessed over the serial port	Minimum of eight (8) and maximum of 64 bytes long printable character string - N/A	Password - CSP			
DRBG Seed	Seeding material for the SP800-90Arev1 CTR_DRBG	384 bit - 384 bit	IG D.L DRBG CSP (Seed) - CSP	DRBG		
Entropy Input	Entropy material for the SP800-90Arev1 CTR_DRBG	256 bit - 256 bit	IG D.L DRBG CSP (Entropy Input) - CSP	Entropy Source		
DRBG Key Value	Used for the SP 800-90Arev1 CTR_DRBG	128, 192, 256 bit - 128, 192, 256 bit	IG D.L DRBG CSP (DRBG Key Value) - CSP	DRBG		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG V Value	Used for the SP 800-90Arev1 CTR_DRBG	128, 192, 256 bit - 128, 192, 256 bit	G D.L DRBG CSP (DRBG V Value) - CSP	DRBG		
SNMPv3 Privacy Key	Used for SNMPv3 session	128 bit - 128 bit	Symmetric - CSP	Key Derivation 1		
SNMPv3 Session Authentication Key	Used for SNMPv3 session	160 bit - 128 bit	Symmetric - CSP	DRBG		Key Derivation 1
SNMPv3 Password	Used for SNMPv3 session	64 bit - N/A	Password - CSP			Key Derivation 1
Shared Secret	Used to derive keys	112 - 200 bits - 112 - 200 bits	Shared Secret - CSP	KAS		KAS
SP 800-56Arev3 Domain Parameters	Used to derive shared secret	2048 to 8192 bits - 112 - 200 bits	Domain Parameters - PSP			KAS

Table 21: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Master Encryption Key (MEK)		NVRAM:Plaintext		Command based	RSA Private Key:Encrypts Crypto Officer Password:Encrypts User Password:Encrypts
RSA Public Key	Input_2 Output_2	NVRAM:Encrypted		Command based	RSA Private Key:Paired With
Client RSA Public Key	Input_1	RAM:Plaintext	Cleared by power cycle	Power Cycle	
RSA Private Key	Input_1 Input_2	NVRAM:Encrypted		Command based	RSA Public Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Output_2				
DH Public Key	Input_1 Output_1	RAM:Plaintext	Cleared by power cycle	Power Cycle	DH Private Key:Paired With
DH Private Key		RAM:Plaintext	Cleared by power cycle	Power Cycle	DH Public Key:Paired With
TLS Session Key	Output_2	RAM:Plaintext	Cleared by power cycle	Power Cycle	Shared Secret:Derived From
SSH Session Key	Output_2	RAM:Encrypted	Cleared by power cycle	Power Cycle	Shared Secret:Derived From
TLS Session Authentication Key		RAM:Plaintext	Cleared by power cycle	Power Cycle	
SSH Session Authentication Key		RAM:Plaintext	Cleared by power cycle	Power Cycle	
Crypto Officer Password	Input_1 Input_2 Output_2	NVRAM:Encrypted		Command based	
User Password	Input_1 Input_2 Output_2	NVRAM:Encrypted		Command based	
"Enabled mode" Password	Input_1 Input_2 Output_2	NVRAM:Encrypted		Command based	
"Setup" Password	Input_1 Input_2 Output_2	NVRAM:Encrypted		Command based	
DRBG Seed		RAM:Plaintext	Cleared by power cycle	Power Cycle	
Entropy Input		RAM:Plaintext	Cleared by power cycle	Power Cycle	
DRBG Key Value		RAM:Plaintext	Cleared by power cycle	Power Cycle	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG V Value		RAM:Plaintext	Cleared by power cycle	Power Cycle	
SNMPv3 Privacy Key		NVRAM:Encrypted		Command based	
SNMPv3 Session Authentication Key		NVRAM:Encrypted		Command based	
SNMPv3 Password	Input_1	NVRAM:Encrypted		Command based	
Shared Secret		RAM:Plaintext	Cleared by power cycle	Power Cycle	
SP 800-56Arev3 Domain Parameters		NVRAM:Plaintext		Command based	

Table 22: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer (FIPS186-4) (A3192)	2048-bit with SHA2-256	KAT	SW/FW Integrity	Successful completion	Verify
HMAC-SHA-1 (A3192)	HMAC-SHA1	KAT	SW/FW Integrity	Successful completion	Verify

Table 23: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt (A2936)	128 bit	KAT	CAST	Successful completion	Encrypt	Reboot
AES-GCM Encrypt (A2936)	256 bit	KAT	CAST	Successful completion	Encrypt	Reboot

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA-1 (A2936)	SHA-1	KAT	CAST	Successful completion	Hash	Reboot
SHA2-512 (A2936)	SHA2-512	KAT	CAST	Successful completion	Hash	Reboot
HMAC-SHA2-256 (A2936)	SHA2-256	KAT	CAST	Successful completion	MAC	Reboot
Counter DRBG (A2936)	AES-128	KAT	Critical Function	Successful completion	SP800-90Arev1 Health Test	Reboot
KAS-FFC-SSC Sp800-56Ar3 (A2936)	2048 bit	KAT	CAST	Successful completion	Primitive Z KAT	Reboot
PBKDF (A2936)		KAT	CAST	Successful completion	KDF	Reboot
KDF TLS (A2936)		KAT	CAST	Successful completion	KDF	Reboot
TLS v1.3 KDF (A2936)		KAT	CAST	Successful completion	KDF	Reboot
KDF SSH (A2936)		KAT	CAST	Successful completion	KDF	Reboot
KDF SNMP (A2936)		KAT	CAST	Successful completion	KDF	Reboot
RSA SigGen (FIPS186-4) (A2936)	2048 bit with SHA2-256 and PKCS v1.5	KAT	CAST	Successful completion	Generate	Reboot
RSA SigVer (FIPS186-4) (A2936)	2048 bit with SHA2-256 and PKCS v1.5	KAT	CAST	Successful completion	Verify	Reboot
RSA SigVer (FIPS186-4) SW/FW Load Test (A3192)	2048 bit with SHA2-256 and PKCS v1.5	KAT	SW/FW Load	Successful completion	Verify	Reboot
RSA KeyGen (FIPS186-4) (A2936)		PCT	PCT	Successful completion	KeyGen	New keypair generation
Safe Primes Key Generation (A2936)		PCT	PCT	Successful completion	KeyGen	New keypair generation
HMAC-SHA-1 (A3192)	SHA-1	KAT	CAST	Successful completion	MAC	Reboot
AES-CBC Decrypt (A2936)	128 bit	KAT	CAST	Successful completion	Decrypt	Reboot

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM Decrypt (A2936)	128 bit	KAT	CAST	Successful completion	Decrypt	Reboot
RSA SigVer (FIPS186-4) (A3192)	2048 bit with SHA2-256	KAT	CAST	Successful completion	Verify	Reboot

Table 24: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A3192)	KAT	SW/FW Integrity	On Demand	Reboot
HMAC-SHA-1 (A3192)	KAT	SW/FW Integrity	On Demand	Reboot

Table 25: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt (A2936)	KAT	CAST	On Demand	Reboot
AES-GCM Encrypt (A2936)	KAT	CAST	On Demand	Reboot
SHA-1 (A2936)	KAT	CAST	On Demand	Reboot
SHA2-512 (A2936)	KAT	CAST	On Demand	Reboot
HMAC-SHA2-256 (A2936)	KAT	CAST	On Demand	Reboot
Counter DRBG (A2936)	KAT	Critical Function	On Demand	Reboot
KAS-FFC-SSC Sp800-56Ar3 (A2936)	KAT	CAST	On Demand	Reboot
PBKDF (A2936)	KAT	CAST	On Demand	Reboot
KDF TLS (A2936)	KAT	CAST	On Demand	Reboot
TLS v1.3 KDF (A2936)	KAT	CAST	On Demand	Reboot
KDF SSH (A2936)	KAT	CAST	On Demand	Reboot
KDF SNMP (A2936)	KAT	CAST	On Demand	Reboot

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen (FIPS186-4) (A2936)	KAT	CAST	On Demand	Reboot
RSA SigVer (FIPS186-4) (A2936)	KAT	CAST	On Demand	Reboot
RSA SigVer (FIPS186-4) SW/FW Load Test (A3192)	KAT	SW/FW Load	On Demand	Reboot
RSA KeyGen (FIPS186-4) (A2936)	PCT	PCT	Automatic	Programmatically
Safe Primes Key Generation (A2936)	PCT	PCT	Automatic	Programmatically
HMAC-SHA-1 (A3192)	KAT	CAST	On Demand	Reboot
AES-CBC Decrypt (A2936)	KAT	CAST	On Demand	Reboot
AES-GCM Decrypt (A2936)	KAT	CAST	On Demand	Reboot
RSA SigVer (FIPS186-4) (A3192)	KAT	CAST	On Demand	Reboot

Table 26: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Hard Error	When the pre-operational test or conditional self-test fails, the module enters hard error state, inhibits all data output and halts all operation	Pre-operational self-test failure Conditional self-test failure	Reboot the module	Pre-operational self-test failure: "PKCS7 Signature verification failed, signature does not match". Conditional self-test failure: "The SG Appliance has failed the FIPS Self-test"

Table 27: Error States

If the module fails the Integrity Test (Pre-operational Self-Test), the following error is printed to the CLI (when being accessed via the serial port):

```
PKCS7 Signature verification failed, signature does not match.
```

If any conditional self-tests fail, the following error is printed to the CLI (when being accessed via the serial port):

```
**********SYSTEMERROR**********
The SG Appliance has failed the FIPS Self test.
System startup cannot continue.

**********SYSTEM STARTUP HALTED**********

E)xit FIPS mode and reinitialize system
R)estart and retry FIPS selftest Selection:
```

When either of these errors occurs, the module enters hard error state and halts operation and provides no functionality. The only way to clear the error and resume normal operation is for the Crypto-Officer to reboot the module. The status output provided above is shown only over the CLI (when being accessed via the serial port).

10.5 Operator Initiation of Self-Tests

Self-tests can be executed on demand by rebooting the module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module meets FIPS-140-3 Level 1 requirements. The section below describes how to place and keep the module in Approved mode of operation. Caveat: This guide assumes that a virtual environment is already set up and ready for accepting a new virtual appliance installation.

The Crypto-Officer is responsible for initialization and security-relevant configuration and management of the module. Please see the ProxySG Command Line Interface Reference, November 16 2022 for more information on configuring and maintaining the module.

Caveat: While the Proxy SG may hold and boot from multiple software images, only the software image documented in this Security Policy (SGOS Software Version: 7.4) may be used for booting to remain compliant. Booting from any other software image will void the validation.

11.1.1 Initialization

Physical access to the module's host hardware shall be limited to the Crypto-Officer, and the CO shall be responsible for putting the module into the Approved mode.

Please read the following guide for installation direction for the ESXi operational environment: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/edge-swg/7-4/deploy-edge-swg-va/Gen2_Overview/Gen2_create_the_swg_va/Gen2_download_the_virtual_appliance_package.html.

Once the module has been configured based on the above guide, the CO must place the module in the Approved mode using the Console Tab which provides access to the virtual serial connection.

1. Press Enter three times.

When the system displays Welcome to the SG Appliance Setup Console, it is ready for the first-time network configuration.

2. Enter the properties for the following:
    a. Interface number
    b. IP address
    c. IP subnet mask
    d. IP gateway
    e. DNS server parameters

3. The module will prompt for the console account authentication information:

```
You must configure the console user account now.
Enter console username:
Enter console password:
Enter enable password:
```

4. The module will prompt to secure serial port, select ‘n’

5. When the system displays Successful Configuration Setup, press Enter to confirm the configuration.

6. Press Enter three times.

7. Select option #1 for the Command Line Interface.

8. Type enable and press Enter.

9. Enter the enable mode password.

10. Enter the following command: **fips-mode enable**.

When prompted for confirmation, select Y to confirm. Once the reinitialization is complete, the module displays the prompt “The system is in FIPS mode”.

- NOTE 1: The “fips-mode enable” command causes the device to power cycle, zeroing the Master Encryption Key and returning the configuration values set in steps 1 and 2 to their factory state.
- NOTE 2: This command is only accepted via the CLI when accessed over the serial port.
-

11. After the system has finished rebooting, press Enter three times.

12. Enter the properties for the following:
    a. Interface number
    b. IP address
    c. IP subnet mask
    d. IP gateway
    e. DNS server parameters

13. The module will prompt for the console account credentials:

```
You must configure the console user account now.
Enter console username:
Enter console password:
Enter enable password:
```

14. Configure the setup password to secure the serial port which must be configured while in Approved mode. The system displays the following:

The serial port must be secured, and a setup password must be configured. Enter setup password:

15. Choose Yes or No to restrict workstation access.

16. The operator should not configure the below ciphers to be in approved mode of operation:
    - TLS v1.0/1.1 for syslog
    - ECDH cipher-suites for SSH (curve25519-sha256@libssh.org, ecdh-sha2-nistp521, ecdhsha2-nistp384, ecdh-sha2-nistp256) and syslog (ECDHE-RSA-AES256-GCM-SHA284, ECDHERSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-SHA384, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA, ECDHE-RSA-AES128-SHA)

17. When creating or importing key pairs, such as during the restoration of an archived backup configuration, the CO must ensure the “no-show” argument is passed over the CLI as shown in Figure below:

Related CLI Syntax to Import a Keyring

```
SGOS#(config ssl) inline {keyring show | show-director | no-show}
keyring_id eof
Paste keypair here
eof
```

Figure 6 - no-show command

Upon completion of these initialization steps, the module is considered to be operating in Approved mode of operation. If the steps are not followed exactly as listed here, the module could still be operational but in a non-compliant state.

11.2 Administrator Guidance

The module can be delivered pre-installed on the SSP-S410 appliance, or via the Broadcom Secure download portal: https://support.broadcom.com/security/download-center

11.3 Non-Administrator Guidance

There are no other non-administrator guidance, other than what's specified in this Security Policy.

12 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-3 Level 1 requirements for this validation.