Symantec, A Division of Broadcom

Edge SWG

Version 7.4

FIPS 140-3 Non-Proprietary Security Policy

FIPS 140-3 Security Level: 1
Document Version 1.2
Date: November 2024

Prepared by:

intertek acumen security
www.acumensecurity.net

Introduction

Federal Information Processing Standards Publication 140-3 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) run the Cryptographic Module Validation Program (CMVP). The NVLAP accredits independent testing labs to perform FIPS 140-3 testing; the CMVP validates modules meeting FIPS 140-3 validation. Validated is the term given to a module that is documented and tested against the FIPS 140-3 criteria.

More information is available on the CMVP website at:
https://csrc.nist.gov/projects/cryptographic-module-validation-program.

About this Document

This non-proprietary Cryptographic Module Security Policy for the Edge Secure Web Gateway (SWG); running the Secure Gateway Operating System (SGOS) version 7.4, provides an overview of the product and a high-level description of how it meets the overall Security Level 1 security requirements Federal Information Processing Standards (FIPS) Publication 140-3.

The Edge SWG may also be referred to as the "module" in this document.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Broadcom shall have no liability for any error or damages of any kind resulting from the use of this document.

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.

Notices

Contact Information

Symantec, A Division of Broadcom
1320 Ridder Park Dr,
San Jose, CA 95131
www.broadcom.com

Table of Contents

List of Tables

List of Figures

1. General

1.1 Scope

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.

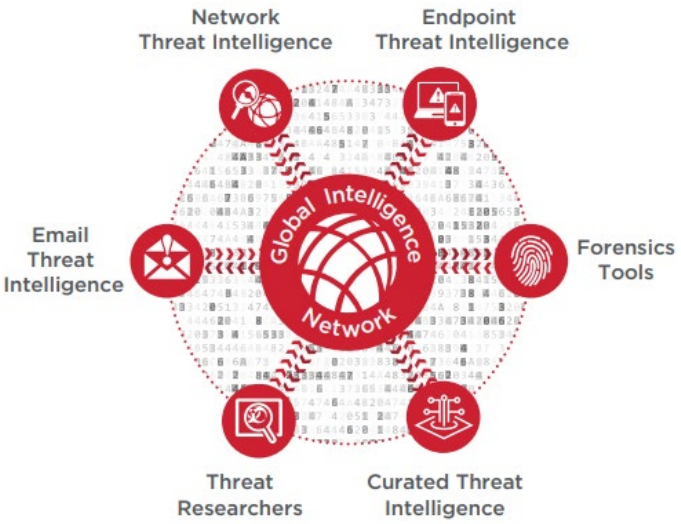
1.2 Overview

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:
    - 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
- 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.



See Figure 1 below for a typical deployment scenario for the Edge SWGs.

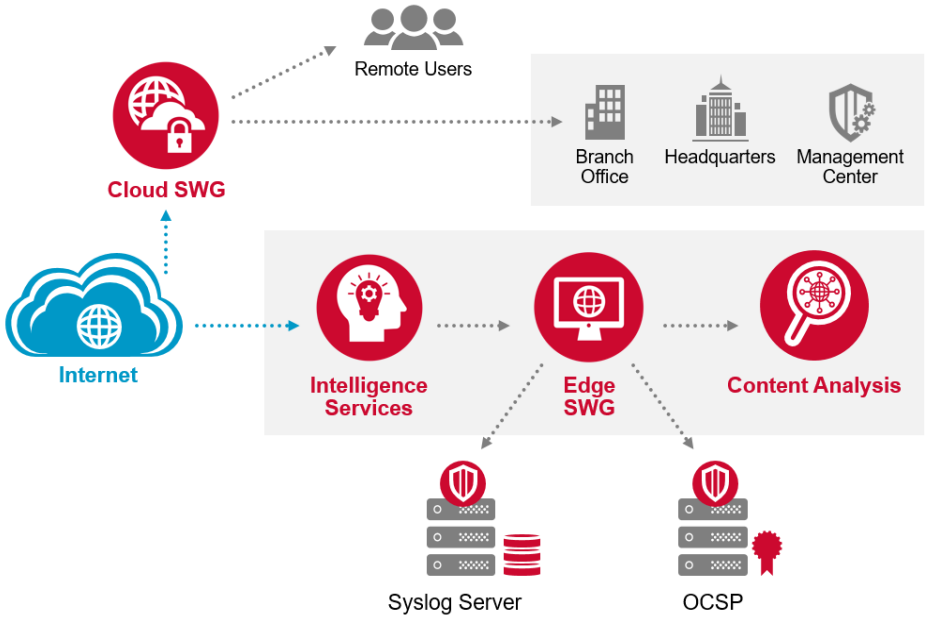


Figure 1 - Typical Deployment of a Secure Web Gateway Virtual Appliance

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))

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

- 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
- TCP[2] tunneling protocols (Secure Shell (SSH))
- Secure Shell
- Telnet Proxy
- ICAP Services
- Netegrity SiteMinder
- Oblix COREid
- Peer-To-Peer
- User Authentication
- Onbox Content Filtering (3rd Party or BCWF[2])
- Offbox Content Filtering (via ICAP)
- SOCKS

Access control is achieved by enforcing configurable policies on controlled protocol traffic to and from the Internal Network users. The policy may include authentication, authorization, content filtering, and auditing.

The module is validated at the overall security level 1 and the following FIPS 140-3 Section levels in Table 1.

ISO/IEC 24759 Section 6.	FIPS 140-3 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

Table 1 - Security Levels

[2] Transmission Control Protocol

2. Cryptographic Module Specification

For the FIPS 140-3 validation, the module was tested on the following operational environments listed in Table 2.

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	SGOS v7.4 (with KVM v2.3 hypervisor)	Symantec SSP-S410	Intel Xeon Silver 4210	With PAA
2	SGOS v7.4 (with VMware ESXi v6.5 hypervisor)	Dell PowerEdge R440	Intel Xeon Silver 4216	With PAA

Table 2 - Tested Operational Environments

Additionally, the vendor affirms that the cryptographic module is also fully supported on the following platforms and operational environments:

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

Table 3 - Vendor Affirmed Operational Environments

No claim can be made as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment, which is not listed on the validation certificate.

2.1 Module Description

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

2.1.1 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 2. 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.

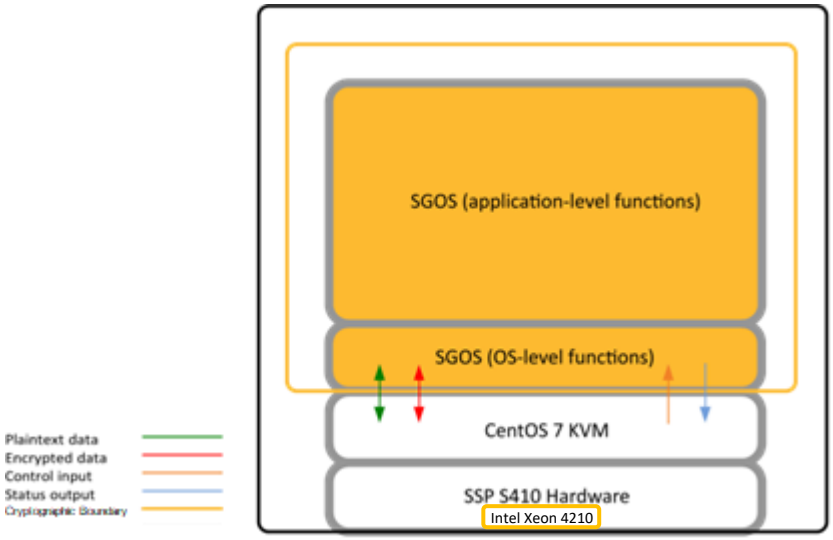


Figure 2 - Cryptographic Boundary Block Diagram for SSP S410

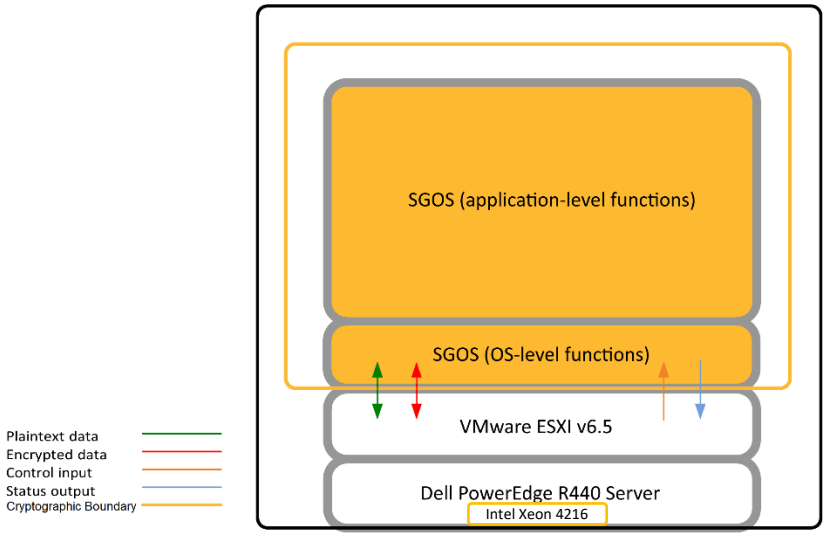


Figure 3 - Cryptographic Boundary Block Diagram for Dell PowerEdge R440

Figure 4 - Intel Xeon Silver 4210

Figure 5 - Intel Xeon Silver 4216

2.2 Modes of Operation

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

2.3 Cryptographic Algorithms

The module implements the Approved algorithms[3] listed in the table below:

[3] 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.

CAVP Cert	Algorithm and Standard	Mode/ Method	Description / Key Size(s) / Key Strength(s)	Use/Function
SGOS Cryptographic Library v5.1.1				
A2936	AES FIPS 197 SP800-38A	CBC, CTR	128, 192, 256	Data Encryption / Decryption
A2936	AES FIPS 197 SP800-38D	GCM	128, 192, 256	Authenticated Encryption, Authenticated Decryption
Vendor Affirmed	CKG SP800-133rev2 Sections 4, 5 and 6.1	N/A	N/A	Symmetric and Asymmetric Key Generation
CVL A2936	CVL SP800-135rev1	KDF SNMP	SNMP (Password Length: 64, 128)	Key Derivation
CVL A2936	CVL SP800-135rev1	KDF SSH	SSH (Cipher: AES-128, AES-192, AES-256)	Key Derivation
CVL A2936	CVL SP800-135rev1	KDF TLS v1.2	TLS v1.2 (SHA2-256, SHA2-384, SHA2-512)	Key Derivation
A2936	DRBG SP800-90Arev1[4]	CTR_DRBG	AES 128, 192, 256	Random Bit Generation
A2936	HMAC FIPS 198-1	HMAC	HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	Message Authentication
A2936	KAS-FFC-SSC SP800-56Arev3	KAS-FFC-SSC dhEphem	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	Shared Secret Computation per SP800-56Arev3
A2936	KAS SP800-56Arev3 SP800-135rev1	KAS-FFC-SSC, KDF SSH, KDF TLS v1.2, TLS v1.3 KDF	KAS-FFC-SSC: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	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.
A2936	PBKDF SP800-132	PBKDF	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	Key Derivation

[4] If CTR_DRBG is used, then the caller shall ensure that the derivation function is enabled.

CAVP Cert	Algorithm and Standard	Mode/ Method	Description / Key Size(s) / Key Strength(s)	Use/Function
A2936	RSA (FIPS 186-4)	KeyGen SigGen SigVer	1024[5], 2048, 3072, 4096 modulo SHA-1[6], SHA2-224, SHA2-256, SHA2-384, SHA2-512; PKCS1 v1.5, PKCSPSS, ANSI X9.31	Key Pair Generation Digital Signature Generation, Digital Signature Verification Per IG C.F, supported RSA modulus sizes specified by ACVP have been CAVP tested. For SigGen, the supported modulus are 2048, 3072 and 4096. For SigVer, the supported key sizes are 1024, 2048, 3072 and 4096.
A2936	SafePrimes SP800-56Arev3	KeyGen KeyVer	ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192	Key Generation, Key Verification
A2936	SHS (FIPS 180-4)	SHA-1[7], SHA2-224, SHA2-256, SHA2-384, SHA2-512	N/A	Message Digest
CVL A2936	CVL RFC8446	TLS v1.3 KDF	SHA2-256, SHA2-384	Key Derivation
N/A	ENT (P) (SP800-90B)	N/A	Seeding for the Approved DRBG (SP 800-90Arev1 CTR_DRBG)	Random Number Generation
VA Blue Coat Boot Loader v5.31				
A3192	SHS (FIPS 180-4)	SHA-1, SHA2-256	N/A	Message Digest as part of Integrity Check
A3192	RSA (FIPS 186-4)	SigVer	2048 modulo SHA2-256; PKCS1 v1.5	Digital Signature Verification as part of Integrity Check
A3192	HMAC (FIPS 198-1)	HMAC-SHA-1	Key Length: 256-1024	Integrity Check

Table 4 - Approved Algorithms

Algorithm	Caveat	Use / Function
AES CBC mode (non-conformant)	All backups are transmitted via SSH (encrypted by the session key), so any non-conformant	Configuration backup encryption

[5] Only for RSA Signature Verification.
[6] Not applicable to RSA Signature Generation.
[7] Only for Non-digital signature and legacy use, all other SHAs acceptable for hash functions applications.

	encryption is redundant/not required for security (No security claimed)	

Table 5 - Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	Use / Function
TLS v1.0/1.1 with MD5	TLS 1.0/1.1 sessions
EC Diffie-Hellman (non-compliant)	Remote management session via SSH and syslog

Table 6 - Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

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

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

2.4 Security Rules

2.4.1 Crypto-Officer Guidance

The Crypto-Officer can monitor and configure the module via the CLI (serial port or SSH).

The Crypto-Officer should monitor the module's status regularly. If any irregular activity is noticed or the module is consistently reporting errors, customers should consult Symantec's Documentation portal and the administrative guidance documents to resolve the issues. If the problems cannot be resolved through these resources, Symantec customer support should be contacted.

Key sizes less than what is specified shall not be used. The Crypto Officer password, "enabled" mode password, "Setup" password and "User" password must be at least 8 characters in length.

2.4.2 User Guidance

The User is only able to access the module remotely via SSH (CLI). The User must change his or her password at the initial login. The User must be diligent to pick strong passwords (alphanumeric with minimum 8 characters) that will not be easily guessed and must not reveal their password to anyone. Additionally, the User should be careful to protect any secret/private keys in their possession, such as TLS or SSH session keys. The User should report to the Crypto-Officer if any irregular activity is noticed. Please refer to Section 11.1.1 for initialization procedures.

2.4.3 Module Correlation

The Crypto-Officer may issue the "show-version" command to view the module identifier and version (SGOS 7.4.0.0 SWG Edition). The module identifier "SWG" denotes the module name "Edge SWG". The version of Edge SWG listed in this Security Policy, 7.4, can be verified by the version of SGOS printed out as part of the "show version" command.

2.4.4 Additional Security Rules

AES GCM IV Generation

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

Scenario 1a TLS 1.2

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 re-distributed.

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 re-distributed.

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.

Key Agreement

ECDH (Elliptic Curve Diffie-Helman) cipher suites or ECDH keypair generated by the module cannot be used in any configuration in the Approved mode of operation. Only DH (Diffie-Hellman) can be used in Approved mode.

3. Cryptographic Module Interfaces

The module's physical ports can be categorized into the following logical interfaces defined by FIPS 140- 3:

- Data input
- Data output
- Control input
- Status output

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. The mapping of the module's logical interfaces in the software to FIPS 140-3 logical interfaces is described in Table 7 below.

Physical port	Logical interface	Data that passes over port/interface
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 7 - Ports and Interfaces

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 Assumption of 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 Table 9. 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.

Role	Service	Input	Output
Crypto-Officer (CO)	Module initialization	See section **11.1.1 Initialization** for input commands	N/A
Crypto-Officer (CO)	Enable mode	”enable”	Command response
Crypto-Officer (CO)	Configuration mode	”conf”	Command response
Crypto-Officer (CO)	Disable Approved mode	”fips-mode disable”	Command response
Crypto-Officer (CO)	Software load	”load upgrade”	Command response
Crypto-Officer (CO) and User	Create remote management session (SSH CLI)	N/A	Command response
Crypto-Officer (CO)	Create, edit, and delete operators	“user create/delete/edit <string>”	Command response
Crypto-Officer (CO)	Create, edit, and delete operator groups	“group create/delete/clear <name>”	Command response
Crypto-Officer (CO) and User	Create SNMPv3 session	“snmp create/delete/edit <community string | user string>”	Command response
Crypto-Officer (CO)	Create filter rules (CLI)	”content filter”	Command response
Crypto-Officer (CO) and User	Show Approved status (CLI)	”show version”	Command response
Crypto-Officer (CO)	Syslog	“syslog add tls**”**	Command response
Crypto-Officer (CO)	Manage module configuration	”configure”	Command response
Crypto-Officer (CO)	Import, replace, and delete SNMP keys	N/A	Command response
Crypto-Officer (CO)	Zeroize keys (serial port only)	”fips-mode disable”	Command response
Crypto-Officer (CO)	Change password hash local user password	”security password”	Command response
Crypto-Officer (CO)	Reboot the module (and perform self-tests)	”restart regular”	Command response
Crypto-Officer (CO) and User	Utility	Command	Command response

Table 8 - Roles, Service Commands, Input and Output

4.2 Authentication Methods

The module supports role-based authentication. COs and Users must authenticate using a user ID and password, or a Client RSA Public Key (SSH only). Secure sessions that authenticate Users have no interface available to access other services (such as Crypto Officer services). Each CO or User SSH session remains active (logged in) and secured until the operator logs out. The authenticated user never leaves the Approved mode, the only services they may call are “Approved” or “Allowed

in the Approved mode" (Tables 4 and 5). Services in Table 6 would require the module to not be in Approved mode and would require a re-initialization of the module.

There is no default password, and passwords are configured while creating the operators (CO/User) during initialization (Section 11.1.1).

The authentication mechanisms used in the module are listed in Table 9.

Role	Authentication Method	Authentication Strength
Crypto-Officer	Password	The module supports password authentication internally. 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 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. 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 =) 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.
	Password ("Enabled" Mode)	The module supports password authentication internally. For password authentication done by the module, passwords are required to be at least 8 characters in length and maximum of 64 bytes (number

Role	Authentication Method	Authentication Strength
		of 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. This password is entered by the Crypto-Officer to enter the "enabled" mode; this is entered locally through the serial port or remotely after establishing an SSH session. 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: 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.
	Password ("Setup")	The module supports password authentication internally. For password authentication done by the module, passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of 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. This password is entered by the Crypto-Officer and is required when using the serial port

Role	Authentication Method	Authentication Strength
		to access the Setup Console portion of the CLI. 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: 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 keys	The module supports using RSA keys for authentication of Crypto-Officers 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: 5.19×10^{33}. 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.
User	Password	The module supports password authentication internally. For password authentication done by the module, passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). An 8-

Role	Authentication Method	Authentication Strength
		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 chances of false acceptance. The User may connect 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 =) 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 Keys	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}. 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 9 - Roles and Authentication

4.3 Services

Descriptions of the services available to a Crypto Officer (CO) and Users are described below in Table 10. For each service listed below, COs and Users are assumed to already have authenticated prior to attempting to execute the service. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

- **G = Generate:** The module generates or derives the SSP
- **R = Read**: The SSP is read from the module (e.g. the SSP is output)
- **W = Write**: The SSP is updated, imported, or written to the module
- **E = Execute:** The module uses the SSP in performing a cryptographic operation
- **Z = Zeroise:** The module zeroizes the SSP.

4.3.1 Crypto Officer Services

Descriptions of the FIPS 140-3 relevant services available to the Crypto-Officer role are provided in Table 10 below. Additional services that do not access SSPs can be found in the following documents:

- ProxySG Content Policy Language Reference, Version 7.4
- ProxySG Command Line Interface Reference, Version 7.4

The link for all documentation can be found here:
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/7-4.html

4.3.2 User Role Services

Descriptions of the FIPS 140-3 relevant services available to the User role are provided in Table 10 below. Additional services that do not access SSPs can be found in the following documents:

- ProxySG Command Line Interface Reference, Version 7.4

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Module initialization	Set up the first-time network configuration, CO username and password, and enable the module in the Approved mode	N/A	Crypto Officer Password “Enabled” mode password “Setup” Password	CO	Crypto Officer Password: W “Enabled” mode password: W “Setup” Password: W	“FIPS mode enabled” will be visible on the serial console upon the successful completion of the cryptographic algorithm self-tests
Enable mode	Manage the module in the “enabled” mode of operation, granting access to higher privileged commands	N/A	“Enabled” mode password	CO	W	Successful completion of the service and enable mode prompt
Configuration mode	Manage the module in the “configuration” mode of operation, allowing permanent system modification to be made	N/A	N/A	CO	N/A	Successful completion of the service and configure mode prompt
Disable Approved mode	Take the module out of the Approved mode of operation and restore it to factory state	N/A	“Enabled” mode password MEK SSH Session Key SSH Session Authentication Key SP800-90Arev1 CTR_DRBG Seed	CO	“Enabled” mode Password: W MEK: Z SSH Session Key: Z SSH Session Authentication Key: Z SP800-90Arev1 CTR_DRBG Seed	N/A

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
			SP800-90Arev1 CTR_DRBG Key Value SP800-90Arev1 CTR_DRBG V Value		: Z SP800-90Arev1 CTR_DRBG Key Value: Z SP800-90Arev1 CTR_DRBG V Value: Z	
Software load	Loads new external software and performs an integrity test using an RSA digital signature	RSA Signature Verification, SHA2-256 Cert. #A3192	Integrity Test Public Key **(not an SSP)**	CO	WE	Image loaded successfully (for verified image). Image loading fails (when image verification fails)
Create remote management session (SSH CLI)	Manage the module through the CLI (SSH) remotely	RSA Signature verification, KAS-FFC-SSC, AES CTR, GCM, CBC, CTR_DRBG, HMAC, SSH KDF, SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SafePrimes, RSA KeyGen, RSA SigGen, ENT (P), CKG	RSA Public Key RSA Private Key Client RSA Public Key DH public key DH private key SSH Session Key SSH Session Authentication Key SP800-90Arev1 CTR_DRBG Seed SP800-90Arev1 CTR_DRBG Key Value	CO, User	RSA Public Key: RE RSA Private Key: RE Client RSA Public Key: RE DH public key: GWRE DH private key: GWRE SSH Session Key: GWRE SSH Session Authentication Key: GWRE SP800-90Arev1 CTR_DRBG Seed: GE	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 after

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
		Cert. #A2936	SP800-90Arev1 CTR_DRBG V Value MEK		SP800-90Arev1 CTR_DRBG Key Value: GE SP800-90Arev1 CTR_DRBG V Value: GE MEK: RE	executing “kex-algs view” command
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	Crypto Officer Password User Password	CO	Crypto Officer Password: WREZ User Password: WREZ	N/A
Create, edit, and delete operator groups	Create, edit, and delete operator groups; define common sets of operator permissions	N/A	N/A	CO	N/A	N/A
Create filter rules (CLI)	Create filters that are applied to user data streams	N/A	N/A	CO	N/A	N/A
Show Approved status (CLI)	The command “show version” will display if the module is configured in Approved mode	N/A	N/A	CO, User	N/A	Successful completion of the service and “System is in FIPS mode” is displayed after executing “show version” command

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Syslog	Setup syslog for logging	RSA Signature verification, KAS-FFC-SSC, AES CTR, GCM, CBC, CTR_DRBG, HMAC, TLS v1.2 KDF, TLS v1.3 KDF, SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SafePrimes, RSA KeyGen, RSA SigGen, ENT (P), CKG Cert. #A2936	RSA Public Key RSA Private Key Client RSA Public Key DH public key DH private key TLS Session Key TLS Session Authentication Key SP800-90Arev1 CTR_DRBG Seed SP800-90Arev1 CTR_DRBG Key Value SP800-90Arev1 CTR_DRBG V Value MEK	CO	RSA Public Key: RE RSA Private Key: RE Client RSA Public Key: RE DH public key: GWRE DH private key: GWRE TLS Session Key: GWRE TLS Session Authentication Key: GWRE SP800-90Arev1 CTR_DRBG Seed : GE SP800-90Arev1 CTR_DRBG Key Value: GE SP800-90Arev1 CTR_DRBG V Value: GE MEK: RE	Connection established to syslog server successfully and “tls 1.2, tls 1.3” versions and “dhe” cipher suites displayed after executing “view ssl-device-profile ” command
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	SNMPv3 Privacy Key SNMPv3 Session Authentication Key SNMPv3 Password MEK	CO	SNMPv3 Privacy Key: W SNMPv3 Session Authentication Key: W SNMPv3 Password: W MEK: RE	N/A
Create SNMPv3 session	Monitor the module using SNMPv3	SNMPv3 KDF Cert. #A2936	SNMPv3 Privacy Key SNMPv3 Session Authentication Key SNMPv3 Password	CO, User	SNMPv3 Privacy Key: RE	Successful completion of the service and “System is in

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
			MEK		SNMPv3 Session Authentication Key: RE SNMPv3 Password: RE MEK: RE	FIPS mode" is displayed after executing "show version" command
Manage module configuration	Backup or restore the module configuration	SSH KDF AES-CBC (non-conformant) Cert. #A2936	RSA Public Key RSA Private Key SSH Session Key SSH Session Authentication Key Crypto Officer Password User Password "Enabled" mode password MEK	CO	RSA Public Key: WRE RSA Private Key: WRE SSH Session Key: GWRE SSH Session Authentication Key: GWRE Crypto Officer Password: WRE User Password: WRE "Enabled" mode password: WRE MEK: RE	Successful completion of the service and "System is in FIPS mode" is displayed after executing "show version" command and "Diffie-hellman" groups displayed after executing "kex-algs view" command
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. The zeroization occurs while the module is still in Approved-mode	N/A	MEK SSH Session Key SSH Session Authentication Key TLS Session Key TLS Session Authentication Key DH private key	CO	MEK: Z SSH Session Key: Z SSH Session Authentication Key: Z TLS Session Key: Z TLS Session Authentication Key: Z DH private key: Z	Successful reboot after executing "fips-mode disable"

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Change password hash local user password	Change Crypto Officer password	PBKDFv2 Cert. #A2936	Crypto Officer Password MEK	CO	Crypto Officer Password: GW MEK: RE	Successful completion of the service and "System is in FIPS mode" is displayed after executing "show version" command
Reboot the module (and perform self-tests)	Perform periodic self-test on demand by power cycling the host platform	N/A	DH public key DH private key SSH Session Key SSH Session Authentication Key TLS Session Key TLS Session Authentication Key SP800-90Arev1 CTR_DRBG Seed SP800-90Arev1 CTR_DRBG Key Value SP800-90Arev1 CTR_DRBG V Value MEK	CO	DH public key: Z DH private key: Z SSH Session Key: Z SSH Session Authentication Key: Z TLS Session Key: Z TLS Session Authentication Key: Z SP800-90Arev1 CTR_DRBG Seed: Z SP800-90Arev1 CTR_DRBG Key Value: Z SP800-90Arev1 CTR_DRBG V Value: Z MEK: RE	"FIPS mode enabled" will be visible on the serial console upon the successful completion of the cryptographic algorithm self-tests
Utility	Services that do not use any SSPs	N/A	N/A	CO, User	N/A	N/A

Table 10 - Approved Services

Service	Description	Algorithms Accessed	Role	Indicator
Proxy Traffic	Proxy Traffic involves the use of TLS v1.0/1.1 sessions, which leverage MD5	MD5, TLS v1.0/1.1 KDF	CO, User	Successful completion of the service and “tls 1, tls 1.1” versions displayed after executing “view ssl-device-profile ” command
Create remote management session (CLI)	Manage the module through the CLI (SSH) remotely	KAS-ECC-SSC	CO, User	Successful completion of the service and “ecdhe” cipher suites displayed after executing “kex-algs view” command

Table 11 - Non-Approved Services

The CO and User roles may monitor the health and status of the modules using SNMPv3. SNMPv3 privacy and authentication keys must be generated by an external application as the module is not capable of generating the keys internally. The keys are not tied to the CO’s CLI credentials

4.4 Self-initiated Cryptographic Output Capability

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

The module performs pre-operational integrity test using HMAC-SHA-1 and RSA 2048 Signature Verification with SHA2-256. The integrity test can be executed on demand by power-cycling the host platform.

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.

6. Operational Environment

Per FIPS 140-3 specifications the module operates in a modifiable operational environment. The module runs on general purpose computers listed in Table 2. 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.

Please refer to Table 2 of this document regarding the Cryptographic Module Tested Configurations.

Except guidelines and installation instructions specified in Sections 2 and 11 of this Security Policy, no other security rules or restrictions to the configuration of the operational environment are required.

Note: The platforms listed in Table 3 are vendor-affirmed per FIPS 140-3. Broadcom, Inc. has verified the module's functionality in the operational environments specified in Table 3 and confirmed that it operates in the same manner as the operational environments listed in Table 2.

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 Parameter Management

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & Related keys
MEK[8] (CSP)	256 bits	AES CBC CKG A2936	Internally generated via Approved DRBG	Never imported Never exits the module	N/A	Stored in plaintext on non-volatile memory	By disabling the Approved mode of operation	Encrypting Crypto Officer Password, User Password, RSA Private Key
Integrity Test Public Key **(not an SSP)**	112 bits	RSA HMAC-SHA-1 SHA2-256 A3192	Externally generated	Imported in encrypted form via a secure SSH session (new key is imported only with a new image) Never exits the module	N/A	Stored in plaintext on non-volatile memory	Overwritten after upgrade by the key in the newly signed image	Verifying the integrity of the system image during upgrade or downgrade
RSA Public Key (PSP)	112, 128, and 152 bits	RSA KDF TLS 1.2, 1.3 KDF SSH SHA-1 SHA2 CKG A2936	Modules' public key is internally generated via Approved DRBG	Modules' public key can be imported from a back-up configuration Output during TLS/SSH[9] negotiation in plaintext	N/A	Stored in encrypted form on non- volatile memory	Module's public key is deleted by command	Negotiating TLS or SSH sessions

[8] Master Encryption Key

[9] SSH session negotiation only uses RSA key pairs of 2048-bits. RSA key pairs of 3072-bits and 4096-bits are only used for TLS session negotiation.

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & Related keys
				Output during TLS negotiation for CAC authentication Exits in encrypted format when performing a module configuration backup				
Client RSA Public Key (PSP)	80, 112, 128, and 152 bits	RSA KDF TLS KDF SSH SHA-1 SHA2 A2936	N/A	Imported in plaintext Never output	N/A	Other entities' public keys reside on volatile memory	Other entities' public keys are cleared by power cycle	Negotiating TLS or SSH sessions
RSA Private Key (CSP)	112, 128, and 152 bits	RSA KDF TLS 1.2, 1.3 KDF SSH SHA-1 SHA2 CKG A2936	Internally generated via Approved DRBG	Imported in encrypted form via a secure SSH session Imported in plaintext via a directly attached cable to the serial port Exported encrypted format	N/A	Stored in encrypted form on non- volatile memory	Inaccessible by zeroizing encrypting MEK	Negotiating TLS or SSH sessions

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & Related keys
				when performing a module configuration backup				
DH public key (PSP)	112 bits	KAS-FFC-SSC SP800-56Arev3 SafePrimes CKG A2936	Module's public key is internally generated via Approved DRBG	Imported in plaintext Exported in plaintext	N/A	Stored in plaintext on volatile memory	Rebooting the module/ Removing power	Negotiating TLS or SSH sessions
DH private key (CSP)	112 bits	KAS-FFC-SSC SP800-56Arev3 SafePrimes CKG A2936	Internally generated via Approved DRBG	Never exits the module	N/A	Stored in plaintext on volatile memory	Rebooting the module/ Removing power	Negotiating TLS or SSH sessions
TLS Session key (CSP)	128, 192, and 256 bits	AES CBC, CTR, or GCM CKG A2936	Internally generated via Approved DRBG	Output in encrypted form during TLS protocol handshake	The keys are established in accordance with SP800-56Arev3	Stored in plaintext on volatile memory	Rebooting the module/ Removing power	Encrypting TLS data
SSH Session key (CSP)	128, 192, and 256 bits	AES CBC, CTR, or GCM CKG A2936	Internally generated via Approved DRBG	Output in encrypted form during SSH protocol handshake	The keys are established in accordance with SP800-56Arev3	Stored in plaintext on volatile memory	Rebooting the module/ Removing power	Encrypting SSH data

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & Related keys
TLS Session Authentication key (CSP)	128, 256, 384 and 512 bits	HMAC SHA2 A2936	Internally generated	Never exits the module	The keys are established in accordance with SP800-56Arev3	Resides in volatile memory in plaintext	Rebooting the module/ Removing power	Data authentication for TLS sessions
SSH Session Authentication key (CSP)	128, 256, 384 and 512 bits	HMAC SHA2 A2936	Internally generated	Never exits the module	The keys are established in accordance with SP800-56Arev3	Resides in volatile memory in plaintext	Rebooting the module/ Removing power	Data authentication for SSH sessions
Crypto Officer Password (CSP)	Minimum of eight (8) and maximum of 64 bytes long printable character string	PBKDFv2 A2936	Externally generated	Enters the module in encrypted form via a secure SSH session Enters the module in plaintext via a directly attached	N/A	Stored in encrypted form on non- volatile memory	Inaccessible by zeroizing the encrypting MEK	Locally authenticating a CO for CLI

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & Related keys
User Password (CSP)				cable to the serial port Exits in encrypted form via a secure TLS session for external authentication Exits in encrypted format when performing a module configuration backup				Locally authenticating a User for CLI
"Enabled" mode password (CSP)	Minimum of eight (8) and maximum of 64 bytes long printable character string	N/A	Externally generated	Enters the module in encrypted form via a secure SSH session Enters the module in plaintext via a directly attached cable to the serial port	N/A	Stored in encrypted form on non- volatile memory	Inaccessible by zeroizing the encrypting MEK	Used by the CO to enter the "privileged" or "enabled" mode when using the CLI

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & Related keys
				Exits in encrypted form via a secure TLS session for external authentication Exits in encrypted format when performing a module configuration backup				
"Setup" Password (CSP)	Minimum of eight (8) and maximum of 64 bytes long printable character string	N/A	Externally generated	Enters the module in plaintext via a directly attached cable to the serial port Never exits the module	N/A	Stored in encrypted form on non- volatile memory	Inaccessible by zeroizing the encrypting MEK	Used by the CO to secure access to the CLI when accessed over the serial port
SP800-90Arev1 CTR_DRBG Seed (CSP)[10]	384 bits	DRBG A2936	Internally generated	Never exits the module	N/A	Plaintext in volatile memory	Rebooting the module/ Removing power	Seeding material for the SP800-90Arev1 CTR_DRBG

[10] (Added per IG D.L)

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & Related keys
SP800-90Arev1 CTR_DRBG Entropy[11] (CSP)[10]	256 bits	ENT (P)	Internally generated within the module's TOEPP	Never exits the module	N/A	Plaintext in volatile memory	Rebooting the module/ Removing power	Entropy material for the SP800-90Arev1 CTR_DRBG
SP800-90Arev1 CTR_DRBG Key Value (CSP)[10]	128, 192 and 256 bits	DRBG A2936	Internally generated	Never exits the module	N/A	Plaintext in volatile memory	Rebooting the module/ Removing power	Used for the SP 800-90Arev1 CTR_DRBG
SP800-90Arev1 CTR_DRBG V Value (CSP)[10]	128, 192 and 256 bits	DRBG A2936	Internally generated	Never exits the module	N/A	Plaintext in volatile memory	Rebooting the module/ Removing power	Used for the SP 800-90Arev1 CTR_DRBG
SNMPv3 Privacy Key (CSP)	128 bits	SNMP KDF A2936	Internally generated	Never exits the module	N/A	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting MEK	Used for SNMPv3 session

[11] The Entropy required by the Approved SP800-90Arev1 CTR_DRBG (with AES-256) is supplied by the ENT (P)

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & Related keys
SNMPv3 Session Authenticati on Key (CSP)	80 bits (SHA1)	SNMP KDF A2936	Internally generated	Never exits the module	N/A	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting MEK	Used for SNMPv3 session
SNMPv3 Password (CSP)	8 bytes password	SNMP KDF A2936	Externally generated	Enters the module in plaintext via a directly attached cable to the serial port	N/A	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting MEK	Used for SNMPv3 session

Table 12 - SSPs

Keys and passwords that exit the module during a configuration backup are encrypted using an Approved encryption algorithm via the TLS or SSH session key. During the backup process, the CO can additionally use either AES-128 CBC or AES-256 CBC mode to encrypt the archive file; however, there is no security claimed on this use of encryption because the key used for encryption is generated using a non-conformant key derivation function.

Zeroisation:
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.

Entropy sources	Minimum number of bits of entropy	Details
NIST SP800-90B compliant ENT (P)	256-bit The estimated amount of entropy per the source's output bit is 0.6.	The Entropy required by the Approved SP800-90Arev1 CTR_DRBG (with AES-256) is supplied by the ENT (P).

Table 13 - Non-Deterministic Random Number Generation Specification

10. Self-Tests

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 other 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 self-
test 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).
The sections below describe the self-tests performed by the module. All the self-tests specified in Section 10.1 are implemented in VA Blue Coat Boot Loader v5.31. All the self-tests specified in Section 10.2 are implemented in SGOS Cryptographic Library v5.1.1.

10.1 Pre-operational Self-Tests

- Software integrity check using RSA SigVer (2048-bit with SHA2-256) and HMAC-SHA-1[12,13] (A3192)

10.2 Conditional Self-Tests

Conditional cryptographic algorithm self-tests (CASTs):

[12] The preoperational self-tests are performed by VA Blue Coat Boot Loader v5.31 library which covers entire image file "7.4.0.0_build_279954_system_gdb.bcsi".
[13] The module executes the RSA SigVer 2048-bit and HMAC-SHA-1 KATs prior to running the pre-operational self-test. Both the integrity tests are sequentially performed on the entire image file "7.4.0.0_build_279954_system_gdb.bcsi".

CAVP Cert. A2936:

- AES-ECB Encrypt KAT (128-bit) (covers AES-CBC)
- AES-ECB Decrypt KAT (128-bit) (covers AES-CBC)
- AES-GCM Encrypt KAT (256-bit)
- AES-GCM Decrypt KAT (256-bit)
- SHA-1 KAT
- SHA2-256 KAT (covered by HMAC-SHA2-256 KAT)
- SHA2-512 KAT
- SHA3-256 KAT (additional KAT, not required by any service/algorithm)
- HMAC-SHA2-256 KAT
- SP800-90Arev1 CTR-DRBG KAT using AES-128
- SP800-56Arev3 DH “Primitive Z” KAT (2048)
- PBKDF KAT
- TLS 1.2 KDF KAT
- TLS 1.3 KDF KAT
- SSH KDF KAT
- SNMP KDF KAT
- SP 800-90B Start-up health tests
- Section 11 CTR_DRBG CAST (Instantiate, Reseed, Generate, Uninstantiate)
- RSA Signature KAT (2048-bit with SHA2-256 and PKCS v1.5)
- RSA Verification KAT (2048-bit with SHA2-256 and PKCS v1.5)
- SP 800-90B Continuous health tests
- Software Load Test using RSA Signature Verification (2048-bit)

CAVP Cert. A3192:

- RSA Verification KAT (2048-bit with SHA2-256)
- HMAC-SHA1 KAT

Conditional pair-wise consistency tests (PCTs):

- RSA Pairwise consistency check upon generation of a keypair
- DH Pairwise consistency check upon generation of a keypair

No data output occurs via the data output interface until all pre-operational self-tests have been completed.

The module also performs a validity check on the installed license. If the license is not valid, the module will not operate.

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

Note the module includes additional self-tests for algorithms that are not callable or used by any service.

11. Life-Cycle Assurance

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*

11.1 Secure Operation/Management

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/proxysg/7-4/Overview_ISG_SGW_VA.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 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, ecdh-sha2-nistp384, ecdh-sha2-nistp256) and syslog (ECDHE-RSA-AES256-GCM-SHA284, ECDHE-RSA-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 6.

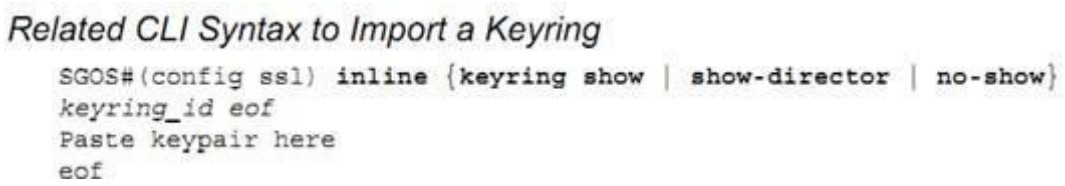


Figure 6 - no-show command

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.

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.