Symantec & CA Technologies, a division of Broadcom
Blue Coat Reverse Proxy Virtual Appliance

Software Versions: 6.7.2, 6.7.5

FIPS 140-2 Non-Proprietary Security Policy

FIPS 140-2 Security Level: 1
Document Version: 1.0

COPYRIGHT NOTICE

CONTACT INFORMATION

Symantec & CA Technologies, a division of Broadcom
1320 Ridder Park Dr,
San Jose, CA 95131
www.broadcom.com

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Purpose

This is a *Non-Proprietary Cryptographic Module Security Policy* for the Blue Coat Reverse Proxy Virtual Appliance (RP-VA), software versions 6.7.2 and 6.7.5 from Symantec & CA Technologies, a division of Broadcom. This *Non-Proprietary Security Policy* describes how the Blue Coat Reverse Proxy Virtual Appliance meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the appliance in the Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The Blue Coat Reverse Proxy Virtual Appliance is referred to in this document as the Reverse Proxy Virtual Appliance, Reverse Proxy, RP-VA, crypto module, or module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Symantec website (www.broadcom.com) contains information on the full line of products from Symantec.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The *Non-Proprietary Security Policy* document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- *Vendor Evidence* document
- *Finite State Model* document
- *Submission Summary* document
- Other supporting documentation as additional references

With the exception of this *Non-Proprietary Security Policy*, the FIPS 140-2 Submission Package is proprietary to Symantec and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Symantec.

2. Blue Coat Reverse Proxy Virtual Appliance

2.1 Overview

The Blue Coat Reverse Proxy Virtual Appliance combines robust security, high performance content delivery, and operational simplicity, allowing organizations to secure and accelerate their web applications and public websites.

- **Protects Web Servers**: Reverse Proxy securely isolates general-purpose servers from direct Internet access, acting as an intermediary between web applications and the external clients who attempt to access them. Reverse Proxy provides robust authentication and policy support and can either challenge users or transparently check authentication credentials using an organization's existing security framework. For high performance, low-latency virus scanning of all uploaded content to web servers, Reverse Proxy integrates with CAS and offers a choice of leading anti-virus engines. To ensure confidentiality, Reverse Proxy can be configured to encrypt communications between users and web applications using Secure Sockets Layer (SSL).
- **Accelerates Web Content**: At the heart of the Reverse Proxy solution is SGOS, a secure, object-based operating system specifically designed to handle web content. SGOS combines patented proxy caching technology with an optimized TCP stack for efficient web content acceleration. SGOS's intelligent use of its integrated cache allows 60-90% of an application's web objects to be cached and served directly to users, further enhancing site performance and scalability. In addition, optional SSL services provide hardware-accelerated key negotiation, encryption, and decryption support.
- **Simplifies Operations**: An integrated, optimized virtual appliance that is easy to install, configure, and maintain. The Reverse Proxy's Visual Policy Manager (VPM) provides an intuitive, graphical interface to define and manage a wide range of policy rules. Comprehensive logging and reporting provide detailed accounting information, giving administrators the visibility necessary to assess web usage patterns and track security issues

See Figure 1 for a typical deployment scenario for Reverse Proxy Virtual Appliance.

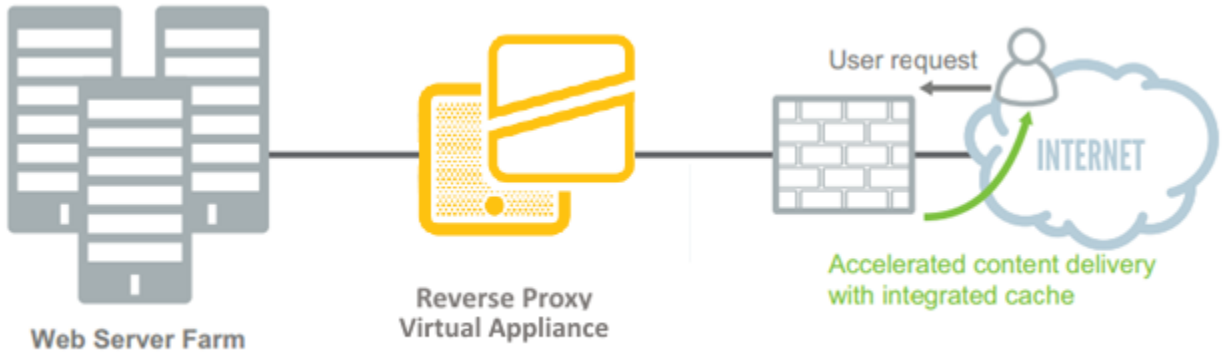

Figure 1 Typical Deployment of a Reverse Proxy Virtual Appliance

The Reverse Proxy Virtual Appliance can be licensed as a Standard Reverse Proxy (SRP) or Advanced Reverse Proxy (ARP). The RP-VA enables organizations to:

- Accelerate delivery of web applications and content through a proxy architecture with integrated caching
- Protect web infrastructure by isolating origin servers from direct Internet access

- Secure external user access to web applications, such as web e-mail, extranets, and public websites, by acting as an SSL termination / origination point
- Save time and money by reducing the number of web servers required
- Implement granular access policies based on users, groups, time of day, location, network address, user agent, and other attributes to meet unique business requirements
- Authenticate clients using existing security framework, including local password files, NTLM, LDAP, RADIUS, one-time passwords, and certificate
- Safeguard their web infrastructure from viruses, worms, and Trojans with real-time AV scanning of all uploaded content
- Deliver high-performance streaming media to thousands of simultaneous users with streaming proxies

The Reverse Proxy Virtual Appliance is validated at the following FIPS 140-2 Section levels in Table 1.

Table 1 Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	Electromagnetic Interference/Electromagnetic Compatibility	1
9	Self-tests	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

For the FIPS 140-2 validation, the crypto module was tested on the following Symantec virtual appliance configurations listed in Table 2.

Table 2 Reverse Proxy Virtual Appliance Configurations

Virtual Appliance Type	Virtual Appliance Part Number	SKU / Short Description
Standard Reverse Proxy (SRP)	076-35373	SRP-VA-C1L-1Y
	076-35376	SRP-VA-C2L-1Y
	076-35379	SRP-VA-C4L-1Y
	076-35382	SRP-VA-C8L-1Y
	076-35385	SRP-VA-C16L-1Y
Advaned Reverse Proxy (ARP)	076-35525	ARP-VA-C1L-1Y
	076-35528	ARP-VA-C2L-1Y
	076-35531	ARP-VA-C4L-1Y
	076-35534	ARP-VA-C8L-1Y
	076-35537	ARP-VA-C16L-1Y

The different part numbers/SKUs in Table 2 represent changes in the number of cores, memory (RAM), and storage space (HDD) available. Reverse Proxy Virtual Appliance can be licensed as an SRP or ARP. All appliance configurations are exactly the same from a cryptographic functionality and boundary perspective. The Crypto Officer and User services of the module are identical for all appliance types running either the SRP or ARP license. The Crypto Officer and User services of the module are identical for both licenses.

The Reverse Proxy Virtual Appliance is a multi-chip standalone software module that meets overall Level 1 FIPS 140-2 requirements. The module was tested and found compliant on a Dell PowerEdge R830 Server using VMware ESXi v6.0 hypervisor to provide the virtualization layer.

The RP-VA software consists of Symantec's proprietary operating system, SGOS v6.7.2 or SGOS v6.7.5. Acting as the guest OS in a VMware ESXi virtual machine, 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, versions 6.7.2 and 6.7.5 contain the following cryptographic libraries:

- SG VA Cryptographic Library version 4.1.1
- SG VA UEFI OS Loader version 4.14
- SG VA TLS Library version 4.1.1
- SG VA SSH Library version 7.2_2
- SG VA SNMP Library version 5.7.2_1

2.2.1 Physical Cryptographic Boundary

As a software module, the virtual appliance has no physical characteristics; however, the physical boundary of the cryptographic module is defined by the hard enclosure around the Dell PowerEdge R830 Server on which it runs. Figure 2 shows the block diagram of the Dell PowerEdge R830 Server (the dashed line surrounding the hardware components represents the module's physical cryptographic boundary, which is the outer case of the hardware platform), and identifies the hardware with which the Dell PowerEdge R830 Server's processor interfaces.

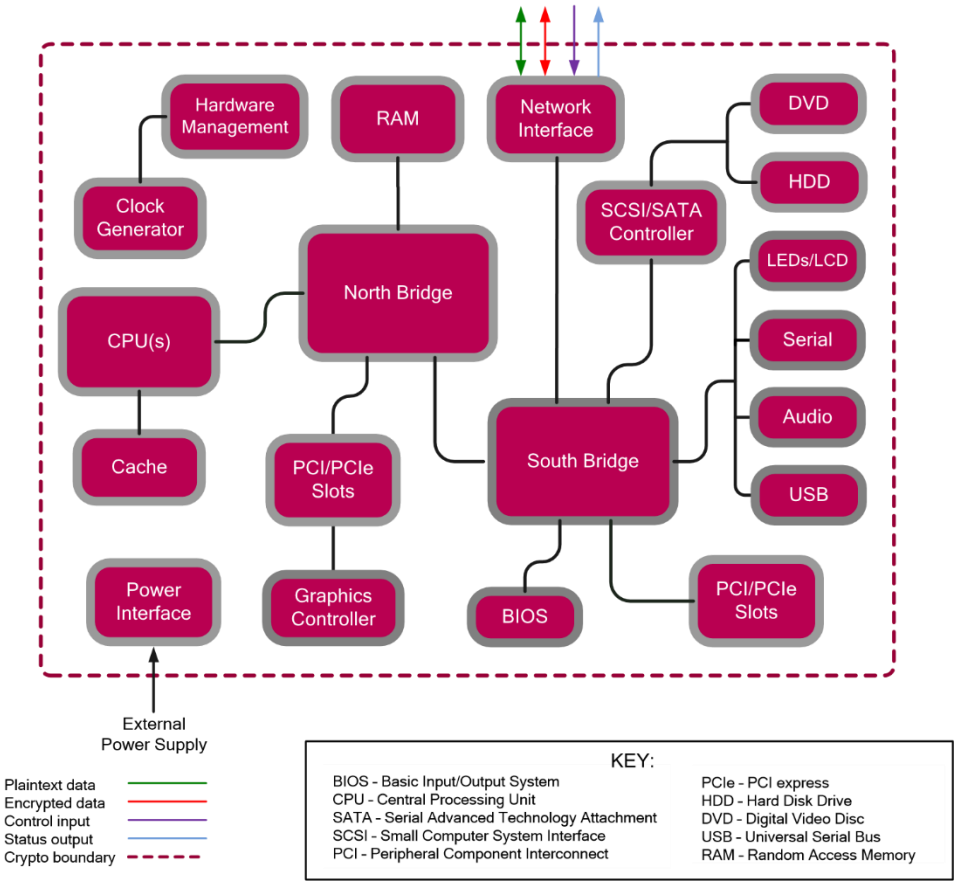

Figure 2 Block Diagram of the Dell PowerEdge R830 Server hardware

The module's physical cryptographic boundary is further illustrated by the black dotted line in Figure 3 below.

The module makes use of the physical interfaces of the tested platform hosting the virtual environment upon which the module is installed. The hypervisor controls and directs all interactions between the RP-VA and the operator, and is responsible for mapping the module's virtual interfaces to the GPC's physical interfaces. These interfaces include the integrated circuits of the system board, processor, network adapters, RAM[1], hard disk, device case, power supply, and fans. Figure 2 shows the block diagram of the Dell PowerEdge R830 Server (the dashed line surrounding the hardware components represents the module's physical cryptographic boundary, which is the outer case of the hardware platform), and identifies the hardware with which the Dell PowerEdge R830 Server's processor interfaces.

2.2.2 Logical Cryptographic Boundary

The logical cryptographic boundary of the module (shown by the red dotted line in Figure 3) consists of the Symantec SGOS v6.7.2 or SGOS v6.7.5, which contains the Symantec SG VA Bootloader v4.14, Symantec SG VA Crypto Library v4.1.1, Symantec SG VA SSH Library v7.2_2, the Symantec SNMP Library v5.7.2_1, and the Symantec SG VA TLS Library v4.1.1.

[1] RAM – Random Access Memory

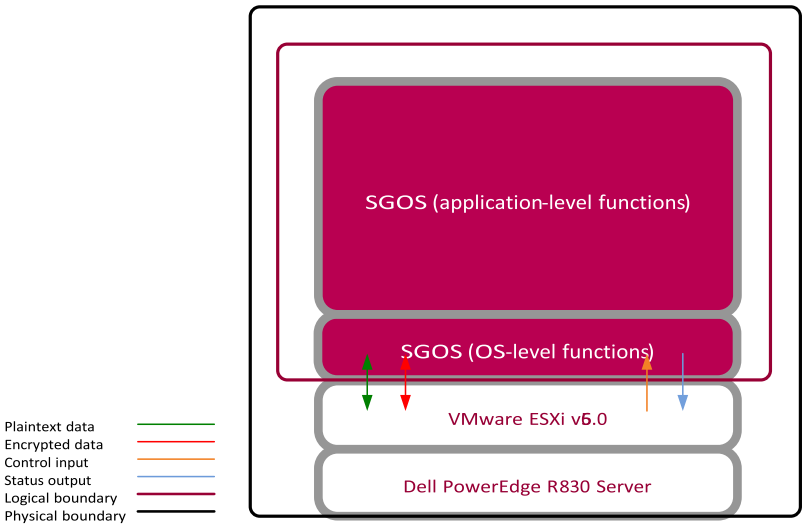

Figure 3 RP-VA Cryptographic Boundary

2.3 Module Interfaces

The module's physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

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

As a software 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 R830 Server). The VMware 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 RP-VA using vSphere Client. The mapping of the module's logical interfaces in the software to FIPS 140-2 logical interfaces is described in Table 3 below.

Table 3 FIPS 140-2 Logical Interface Mappings for the front of the RP-VA

Physical Port / Interface	Logical Port/Interface	FIPS 140-2 Interface
Host System Ethernet (10/100/1000) Ports	Virtual Ethernet Ports Virtual Serial Ports	Data Input Data Output Control Input Status Output
Host System Serial Port	Virtual Serial Port	Control Input Status Output

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 the Virtual Ethernet and Virtual Serial Port interfaces (GUI, SSH CLI, and Serial CLI). Status output consists of the status provided or displayed via the user interfaces (such as GUI, SSH CLI, and Serial CLI) or available log information.

Status output exits the module via the user interfaces (such as GUI , SSH CLI, and Serial CLI) over the Virtual Ethernet or Virtual Serial Ports.

2.4 Roles and Services

Before accessing the modules for any administrative services, COs and Users must authenticate to the module according to the methods specified in Table 8. The modules offer two management interfaces:

- 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.
- Management Console (MC): A graphical user interface accessible remotely with a web browser that supports TLS. This interface is used for management of the modules. Authentication is required before any functionality will be available through the Management Console

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 RP-VA. Unlike Users, COs have the ability to 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 in Table 4.

Table 4 FIPS and RP-VA Roles

FIPS Roles	RP-VA Roles and Privileges
CO	• The CO is an administrator of the module that has been granted "enabled" mode access while using the CLI and "read/write" access while using the Management Console. • 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. • When the CO is administering the module over the Management Console, they can perform all the same services available in CLI (equivalent to being in the "configuration" mode in the CLI) except the CO is unable to put the module into Approved mode.

FIPS Roles	RP-VA Roles and Privileges
User	• 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, and has been given “read-only” privileges when using the Management Console. • The User may access the CLI and Management Console for management of the module. When the User is administering the module over the Management Console, they perform all the same services available in CLI (“standard” mode only services).

Descriptions of the services available to a Crypto Officer (CO) and Users are described below in Table 5 and Table 6 respectively. 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:

- **R**: The CSP is read
- **W**: The CSP is established, generated, modified, or zeroized
- **X:** Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

2.4.1 Crypto-Officer Role

Descriptions of the FIPS 140-2 relevant services available to the Crypto-Officer role are provided in Table 5 below. Additional services are that do not access CSPs can be found in the following documents:

- Symantec SGOS Proxy Administration Guide, Version 6.7.x
- Symantec SGOS Proxy Visual Policy Manager Reference, Version 6.7.x
- Symantec SGOS Proxy Content Policy Language Reference, Version 6.7.x
- Symantec SGOS Command Line Interface Reference, Version 6.7.x

The link for all documentation can be found here: https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/proxysg/6-7.html

Table 5 Crypto Officer Role Services and CSP Access

Service	Description	CSP and Access Required
Set up the module (serial port only)	Set up the first-time network configuration, CO username and password, and enable the module in the Approved mode of operation. For more information, see section 3.1.1 in this *Security Policy*.	CO Password : W “Enabled” mode password: W “Setup” Password: W
Enter the “enabled” mode (CLI)	Manage the module in the “enabled” mode of operation, granting access to higher privileged commands	“Enabled” mode password: RX
* Enter the “configuration” mode (CLI)	Manage the module in the “configuration” mode of operation, allowing permanent system modifications to be made	None

Service	Description	CSP and Access Required
* Disable FIPS mode (serial port only)	Take the module out of the approved mode of operation and restore it to a factory state	"Setup" Password: RX MEK: W SSH Session Key: W SSH Authentication Key: W TLS Session Key: W TLS Authentication Key: W DRBG CSPs: W
** Software Load[2]	Loads new external software and performs an integrity test using an RSA digital signature.	Integrity Test public key: WRX
Create remote management session (CLI)	Manage the module through the CLI (SSH) remotely via Ethernet port.	RSA public key: RX RSA private key: RX Client RSA public key: RX DH public key: WRX DH private key: WRX ECDH public key: WRX ECDH private key: WRX SSH Session Key: WRX SSH Authentication Key: WRX DRBG CSPs: WRX MEK: RX
Create remote management session (MC)	Manage the module through the Management Console (TLS) remotely via Ethernet port, with optional CAC authentication enabled.	RSA public key: RX RSA private key: RX Client RSA public key: RX DH public key: WRX DH private key: WRX ECDH public key: WRX ECDH private key: WRX TLS Session Key: WRX TLS Authentication Key: WRX DRBG CSPs: WRX MEK: RX
** Create, edit, and delete operator groups	Create, edit and delete operator groups; define common sets of operator permissions.	None
** 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.	Crypto-Officer Password: W User Password: W MEK: RX
** Create filter rules (CLI)	Create filters that are applied to user data streams.	None
Create filter rules (MC)	Create filters that are applied to user data streams.	None
Show FIPS-mode status (CLI)	The CO logs in to the module using the CLI. Entering the command "show version" will display if the module is configured in Approved mode.	None
Show FIPS-mode status (MC)	The CO logs in to the module using the Management Console and navigates to the "Configuration" tab that will display if the module is configured in Approved mode.	None

[2] Any other software loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

Service	Description	CSP and Access Required
** Manage module configuration	Backup or restore the module configuration	RSA public key: WRX RSA private key: WRX CO Password: WRX User Password: WRX “Enabled” mode password: WRX MEK: RX
* 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.	MEK: W SSH Session Key: W SSH Authentication Key: W TLS Session Key: W TLS Authentication Key: W DH private key: W ECDH private key: W
** Change password	Change Crypto-Officer password	Crypto-Officer Password: W MEK: RX
* Perform self-test	Perform self-test on demand by rebooting the machine	DH public key: W DH private key: W ECDH public key: W ECDH private key: W SSH Session Key: W SSH Authentication Key: W TLS Session Key: W TLS Authentication Key: W DRBG CSPs: W MEK: RX
* Reboot the module	Reboot the module.	DH public key: W DH private key: W ECDH public key: W ECDH private key: W SSH Session Key: W SSH Authentication Key: W TLS Session Key: W TLS Authentication Key: W DRBG CSPs: W MEK: RX

* - Indicates services that are only available once the CO has entered the “enabled” mode of operation.
** - Indicates services that are only available once the CO has entered the “enabled” mode followed by the “configuration” mode of operation.

2.4.2 User Role

Descriptions of the FIPS 140-2 relevant services available to the User role are provided in Table 6 below. Additional services are that do not access CSPs can be found in the following documents:

- Symantec SGOS Proxy Administration Guide, Version 6.7.x
- Symantec SGOS Proxy Visual Policy Manager Reference, Version 6.7.x
- Symantec SGOS Proxy Content Policy Language Reference, Version 6.7.x
- Symantec SGOS Command Line Interface Reference, Version 6.7.x

Table 6 User Services and CSP Access

Service	Description	CSP And Access Required
Create remote management session (CLI)	Manage the module through the CLI (SSH) remotely via Ethernet port.	RSA public key: RX RSA private key: RX Client RSA public key: RX DH public key: RX DH private key: RX ECDH public key: RX ECDH private key: RX SSH Session Key: WRX SSH Authentication Key: WRX DRBG CSPs: WRX MEK: RX
Create remote management session (MC)	Manage the module through the Management Console (TLS) remotely via Ethernet port, with optional CAC authentication enabled.	RSA public key: RX RSA private key: RX Client RSA public key: RX DH public key: RX DH private key: RX ECDH public key: RX ECDH private key: RX TLS Session Key: WRX TLS Authentication Key: WRX DRBG CSPs: WRX MEK: RX
Show FIPS-mode status (MC)	The User logs in to the module using the Management Console and navigates to the “Configuration” which will display if the module is configured in Approved mode.	None
Show FIPS-mode status (CLI)	The User logs in to the module using the CLI. Entering the command “show version” will display if the module is configured in Approved mode.	None

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 and Management Console credentials. The following non-Approved services in Table 7 are available in a non-Approved mode of operation.

Table 7 Non-Approved Services and Description

Service	Description
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.
Create SNMPv3 session	CO/User monitor the module using SNMPv3
Encrypt configuration backups	Encrypt backup configuration files.

2.4.3 Authentication Mechanism

The module supports role-based authentication. COs and Users must authenticate using a user ID and password, SSH client key (SSH only), or certificates associated with the correct protocol in order to set up the secure session. 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. Each CO and User Management Console session remains active until the operator logs out or inactivity for a configurable amount of time has elapsed.

Modules used by the United States Department of Defense (DoD) must meet Homeland Security Presidential Directive (HSPD)-12 requirements regarding the use of FIPS 201 validated Common Access Card (CAC) authentication for COs and Users connecting to management functionality of the module. Additionally, other agencies may require FIPS 201 validated PIV[3] II card authentication.

When the module is configured to use CAC authentication, it will implement specially configured CPL during administrator authentication in order to facilitate TLS mutual authentication. This is accomplished by modifying the HTTPS-Console service so that it can be configured to validate a client certificate against a chosen certificate authority (CA) list. CAC authentication will take place against a Certificate realm, and CO and User authorization takes place against an LDAP realm.

The authentication procedure leverages 3rd party middleware on the management workstation in order to facilitate two factor authentication of the user to their CAC using a Personal Identification Number (PIN). This process enables the module to retrieve the X.509 certificate from the microprocessor smart card. The process is as follows:

1. On the management workstation the CO or User opens a browser and establishes a clear-text HTTP connection with the module.
2. Using CPL similar to the VPM `NotifyUser` action, the CO or User is presented with a DoD warning banner which they must positively acknowledge and accept.
3. `NotifyUser` redirects the browser to an HTTPS connection with the module that requires mutual authentication. This is made possible by CPL that puts the module in reverse-proxy mode at this point.
4. The TLS handshakes begin. The reverse-proxy service on the module requires a certificate to complete the handshake (i.e. the `verify-peer` setting has been enabled in the reverse-proxy service).
5. The browser presents the CO or User with a dialog box prompting which certificate to select.
6. The CO or User selects the X.509 certificate on the CAC.
7. The middleware on the management workstation prompts the CO or User for the PIN to unlock the certificate. The CO or User enters the PIN and the certificate is transmitted to the module.
8. The module authenticates the certificate against the CA list that has been configured on the reverse proxy service using local CRLs and OCSP to check for certificate revocation.
9. The CO or User reviews and accepts the certificate issued to the web browser by the module. A mutually authenticated TLS session is now in use.
10. The module extracts the subject name (of the CO or User) from the `subjectAltNames` extension of the X.509 certificate according to configuration of the certificate realms, Within the `subjectAltNames` extension is the CO or User's `userPrincipleName` (UPN) (when PIV cards are used in place of CACs, the CommonName (CN) field is extracted from the certificate instead). The UPN/CN is what ties the CAC identity to the Principle Name (PN) field of a CO or User record in Active Directory (AD), the LDAP server.
11. The certificate realm is configured to use an LDAP realm for authorization. The LDAP user is determined by LDAP search using the following filter: `(userPrincipleName=$(user.name))`.

The CO or User is granted access to the Management Console if the UPN/CN is found in the LDAP directory. The exchanges with the LDAP server are secured using TLS. Conditions like *`group=`* and

[3] PIV – Personal Identity Verification II

ldap.attribute <name> may also be used to authorize the CO or User and to specify if the CO or User should have read-only or read-write access.

The authentication mechanisms used in the module are listed in Table 8.

Table 8 Authentication Mechanisms Used by the Module

Role	Type of Authentication	Authentication Strength
Crypto-Officer	Password	The modules support password authentication internally. For password authentication done by the modules, 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 TLS or SSH session.
	Password (“Enabled” Mode)	The modules support password authentication internally. For password authentication done by the modules, 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 to enter the “enabled” mode; this is entered locally through the serial port or remotely after establishing an SSH session.
	Password (“Setup”)	The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at least 4 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). A 4-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1:(95^4), or 1:81,450,625 chance of false acceptance. This password is entered by the Crypto-Officer and is required when using the serial port to access the Setup Console portion of the CLI.
	Public keys	The module supports using RSA keys for authentication of Crypto-Officers during TLS (when CAC authentication is configured with a local Certificate Realm) or 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}.

Role	Type of Authentication	Authentication Strength
User	Password	The modules support password authentication internally. For password authentication done by the modules, 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. The User may connect remotely after establishing a TLS or SSH session.
	Public keys	The module supports using RSA keys for authentication of Users during TLS (when CAC authentication is configured with a local Certificate Realm) or 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}.

2.5 Physical Security

The Reverse Proxy Virtual Appliance is a software module, which FIPS defines as a multi-chip standalone cryptographic module. As such, it does not include physical security mechanisms. Thus, the FIPS 140-2 requirements for physical security are not applicable.

2.6 Operational Environment

The module was tested and found to be compliant with FIPS 140-2 requirements on the following operational environment and hardware:

- Dell PowerEdge R830 Server appliance
- Intel Xeon E5 processor
- VMware ESXi v6.0 with Symantec's SGOS v6.7.2 and SGOS v6.7.5 as the guest OS

All cryptographic keys and CSPs are under the control of the guest operating system, which protects the CSPs against unauthorized disclosure, modification, and substitution.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in the tables below.

Table 9 FIPS-Approved Algorithm Implementations for Crypto Library version 4.1.1

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
4596	AES	SP 800-38A, SP 800-38D	CBC, CTR, GCM[4]	128, 192, 256	Data Encryption / Decryption
4596	KTS	SP 800-38F	AES	128, 192, 256	Key Transport
2446	Triple-DES	SP 800-67	TCBC, ECB	192	Data Encryption / Decryption
2446	KTS	SP 800-38F	Triple-DES	112	Key Transport
3772	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest
3046	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-1-96, HMAC-SHA-256, HMAC-SHA-384 HMAC-SHA-512	128, 192, 256, 256, 512	Message Authentication
2506	RSA	FIPS 186-4	SHA-1[5], SHA-224, SHA-256, SHA-384, SHA-512; PKCS1 v1.5	2048, 3072, 4096	KeyPair Generation Digital Signature Generation, Digital Signature Verification
1541	DRBG	SP 800-90A	CTR-based		Deterministic Random Bit Generation

[4] AES-GCM was only CAVP tested for 256-bits.

[5] Not applicable to RSA Signature Generation.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
N/A[6]	KAS-SSC	SP 800-56A rev3	FFC	Safe Prime groups per SP 800-56Arev3 Appendix D: ffdhe2048 (for TLS) and MODP2048 (for SSH)	Key Agreement Scheme – Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135rev1 (TLS KDF CVL. Cert. #1265 and SSH KDF CVL Cert. #1267).
N/A[7]	KAS-SSC	SP 800-56Arev3	ECC	P-256, P-384, P-521	Key Agreement Scheme – Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135rev1 (TLS KDF CVL. Cert. #1265 and SSH KDF CVL Cert. #1267).
Vendor Affirmed	CKG	SP 800-133			Key Generation

Table 10 FIPS-Approved Algorithm Implementations for UEFI OS Loader version 4.14

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
3773	SHS	FIPS 180-4	SHA-1, SHA-256		Message Digest as part of Integrity Check
2507	RSA	FIPS 186-4	SHA-256; PKCS1 v1.5	2048	Digital Signature Verification as part of Integrity Check
3047	HMAC	FIPS 198-1	HMAC-SHA-1	128	Integrity Check

[6] Vendor Affirmed per IG D.8 Scenario X1 and IG D.1-rev3.

[7] Vendor Affirmed per IG D.8 Scenario X1 and IG D.1-rev3.

Table 11 FIPS-Approved Algorithm Implementations for TLS Library version 4.1.1

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
1265	CVL TLS 1.0, TLS 1.1, TLS 1.2	SP 800-135rev1	TLS 1.2 SHA Sizes = SHA-256, SHA384		Key Derivation

Table 12 FIPS-Approved Algorithm Implementations for SSH Library version 7.2_2

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
1267	CVL SSH	SP 800-135rev1	AES-128 CBC, AES-256 CBC	SHA-1, SHA-256, SHA-384, SHA-512	Key Derivation

Table 13 FIPS-Approved Algorithm Implementations for SNMP Library version 5.7.2_1

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
1268[8]	CVL SNMP	SP 800-135rev1			Key Derivation

[8] SNMP KDF was tested; however, it is not used by an approved service

Table 14 FIPS-Allowed Algorithms

Algorithm	Caveat	Use
RSA Key Wrapping (PKCS#1)	Provides between 112 and 150 bits of encryption strength	Key Wrapping
RSA Signature Verification	1536 bits	Signature Verification
MD5		TLS 1.1 sessions;
Non-Deterministic Random Number generator (NDRNG)[9]		Seeding for the FIPS-Approved DRBG (SP 800-90A CTR_DRBG)

Table 15 Non-Approved Algorithms

Algorithm	Use
AES CFB mode (non-conformant)	SNMP Privacy Key
AES CBC mode (non-conformant)	Configuration backup encryption

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

The vendor affirms generated seeds for private keys are generated per SP 800-133 (unmodified output from a DRBG)

Per SP800-67 rev1, the user is responsible for ensuring the module's limit to 2^32 encryptions with the same Triple-DES key while being used in SSH and/or TLS protocols.

[9] NDRNG is listed on the certificate

The module supports the CSPs listed below in Table 16.

Table 16 List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Master Encryption Key (MEK)	AES CBC 256-bit key	Internally generated via FIPS-Approved DRBG	Never exits the module	Stored in plaintext on non-volatile memory	By disabling the FIPS-Approved mode of operation	Encrypting Crypto-Officer password, RSA private key
Integrity Test Public Key	RSA public key 2048 bits	Externally generated, Imported in encrypted form via a secure TLS or SSH session	Never exits the module	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 Keys	2048-, 3072-, and 4096-bits	Modules' public key is internally generated via FIPS-Approved DRBG Modules' public key can be imported from a back-up configuration	Output during TLS/SSH[10] negotiation in plaintext. Output during TLS negotiation for CAC authentication Exits in encrypted format when performing a module configuration backup	Stored in encrypted form on non-volatile memory	Module's public key is deleted by command	Negotiating TLS or SSH sessions

[10] 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	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Client RSA Public Key	1024, 1536, 2048, 3072, and 4096-bits	Other entities' public keys are sent to the module in plaintext Can be sent to the module as part of an X.509 certificate during CAC authentication	Never output	Other entities' public keys reside on volatile memory	Other entities' public keys are cleared by power cycle	Negotiating TLS or SSH sessions
RSA Private Keys	2048-, 3072-, and 4096-bits	Internally generated via FIPS-Approved DRBG Imported in encrypted form via a secure TLS or SSH session Imported in plaintext via a directly attached cable to the serial port	Exits in encrypted format when performing a module configuration backup	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing encrypting MEK	Negotiating TLS or SSH sessions
DH public key	2048-bits	Module's public key is internally generated via FIPS-Approved DRBG Public key of a peer enters the module in plaintext	The module's Public key exits the module in plaintext	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions
DH private key	224-bits	Internally generated via FIPS-Approved DRBG	Never exits the module	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
ECDH private key	P-256 key	Internally generated via FIPS-Approved DRBG	Never exits the module	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions
ECDH public key	P-256 key	Module's public key is internally generated via FIPS-Approved DRBG Public key of a peer enters the module in plaintext	The module's Public key exits the module in plaintext	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions
TLS or SSH Session key	AES CBC, CTR, or GCM[11] 128-, 192, or 256-bit key Triple-DES CBC keying option 1 (3 different keys)	Internally generated via FIPS-Approved DRBG	Output in encrypted form during TLS or SSH protocol handshake	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Encrypting TLS or SSH data
TLS or SSH Session Authentication key	HMAC SHA-1-, 256-, 384- or 512-bit key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Rebooting the modules Removing power	Data authentication for TLS or SSH sessions

[11] AES GCM is only used as part of TLS 1.2 cipher suites conformant to IG A.5, RFC 5288 and SP 800-52 which are listed in Table 16 of this document.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Crypto Officer Password User Password	Minimum of eight (8) and maximum of 64 bytes long printable character string	Externally generated. Enters the module in encrypted form via a secure TLS or SSH session. Enters the module in plaintext via a directly attached 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	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypted MEK	Locally authenticating a CO or User for Management Console or CLI
“Enabled” mode password	Minimum of eight (8) and maximum of 64 bytes long printable character string	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	Exits in encrypted form via a secure TLS session for external authentication Exits in encrypted format when performing a module configuration backup	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
“Setup” Password	Minimum of four (4) and maximum of 64 bytes long printable character string	Enters the module in plaintext via a directly attached cable to the serial port	Never exits the module	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
SP 800-90A CTR_DRBG Seed	384-bit random number	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules Removing power	Seeding material for the SP800-90A CTR_DRBG

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SP 800-90A CTR_DRBG Entropy[12]	256-bit random number with derivation function 384-bit random number without derivation function	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules Removing power	Entropy material for the SP800-90A CTR_DRBG
SP 800-90A CTR_DRBG key value	Internal state value	Internally generated	Never	Plaintext in volatile memory	Rebooting the modules Removing power	Used for the SP 800-90A CTR_DRBG
SP 800-90A CTR_DRBG V value	Internal state value	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules Removing power	Used for the SP 800-90A CTR_DRBG

NOTE: The Approved DRBG is seeded with a minimum of 384-bits from an entropy-generating NDRNG inside the module's cryptographic boundary.

Keys and passwords that exit the module during a configuration backup are encrypted using a FIPS-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.

[12] The Entropy required by the FIPS-Approved SP 800-90A CTR_DRBG (with AES-256) is supplied by the NDRNG

2.8 Self-Tests

If the module fails the POST Integrity 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):

```
********************* SYSTEM ERROR **********************
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 modules halt operation and provide no functionality. The only way to clear the error and resume normal operation is for the Crypto-Officer to reboot the modules. 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.

2.8.1 Power-Up Self-Tests

The module performs the following self-tests using the UEFI OS Loader:

- Software integrity check

The module performs the following self-tests using the SGOS Cryptographic Library software implementation at power-up:

- Known Answer Tests
  - AES KAT for encryption and decryption
  - AES-GCM KAT for decryption and decryption
  - TDES KAT for encryption and decryption
  - SHA KAT using each of SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
  - HMAC KAT using each of SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
  - RSA Sign/Verify KAT with SHA-256
  - RSA wrap/unwrap KAT
  - SP800-90A DRBG KAT
  - DH “Primitive Z” KAT
  - ECDH “Primitive Z” KAT

No data output occurs via the data output interface until all power-up self tests have completed.

2.8.2 Conditional Self-Tests

The module performs the conditional self-tests in only on its SGOS Cryptographic Library.

- Software Load Test using RSA Signature Verification
- RSA pairwise consistency check upon generation of an RSA keypair
- Continuous RNG test (CRNGT) for the SP800-90A DRBG
- Continuous RNG test (CRNGT) for the Non-Deterministic Random Number Generator (NDRNG)

2.8.3 Critical Function Tests

The Reverse Proxy Virtual Appliance performs the following critical function tests:

- DRBG Instantiate Critical Function Test
- DRBG Reseed Critical Function Test
- DRBG Generate Critical Function Test
- DRBG Uninstantiate Critical Function Test

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

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3. Secure Operation

The Blue Coat Reverse Proxy Virtual Appliance meets FIPS-140-2 Level 1 requirements. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

Caveat: This guide assumes that a virtual environment is already setup and ready for accepting a new virtual appliance installation

3.1 Secure Management

The Crypto-Officer is responsible for initialization and security-relevant configuration and management of the module. Please see the *Symantec SGOS Administration Guide, Version SGOS 6.7.x* for more information on configuring and maintaining the module.

Caveat: While the RP-VA may hold and boot from multiple software images, only the software image documented in this Security Policy (Software Versions: 6.7.2 and 6.7.5) may be used for booting in order to remain compliant. Booting from any other software image will result in a non-compliant module

3.1.1 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 sections found in chapters 2 through 4 of the *Symantec Secure Web Gateway Virtual Appliance Initial Configuration Guide*, For SGOS 6.7.x and later, Platform: VMware vSphere Hypervisor:

- Chapter 2
  - Verify System Requirements
  - Retrieve Appliance Serial Numbers
  - Create a Virtual Switch
- Chapter 3
  - Download the Virtual Appliance Package
  - Import a SWG VA
  - Reserve Resources for the SWG VA
- Power on the SWG VA
  - Chapter 4
  - Perform Initial Configuration
  - Complete Initial Configuration

Once the module has been configured based on the sections found in Chapters 2 through 4, 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 FIPS 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. Access the Web interface at the IP address configured in step 12b above (https://<IP Address>:8082).
17. Login with the credentials created in step 13.
18. Navigate to the Configuration tab. Then expand the Authentication->SSH Inbound Connections menu in the left hand column.
19. Select the Ciphers tab. Deselect the aes256-gcm@openssh.com and the aes128-gcm@openssh.com ciphers. Select the aes256-ctr, aes192-ctr, aes128-ctr, aes256-, and aes128-cbc ciphers.
20. Press Apply and the changes will be saved to the appliance.

Upon completion of these initialization steps, the module is considered to be operating in its Approved mode of operation.

3.1.2 Management

The Crypto-Officer is able to monitor and configure the module via the Management Console (HTTPS over TLS) and 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 CO password and "enabled" mode password must be at least 8 characters in length. The "Setup" password must be at least 4 characters in length.

When creating or importing key pairs, such as during the restoration of an archived backup configuration, the CO must ensure that the "Do not show key pair" option is selected in the Management Console as shown in Figure 3, or the "no-show" argument is passed over the CLI as shown in Figure 4 Please see Section E: Preparing Archives for Restoration on New Devices in the *Symantec SGOS Administration Guide, Version 6.7.x* for further reference.

Figure 3 Keyring Creation Management Console Dialogue Box

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 4 Keyring Creation CLI Commands

3.1.3 Zeroization

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 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 NDRNG entropy values) to be zeroized. The Crypto-Officer must wait until the module has successfully rebooted in order to verify that zeroization has completed.

3.2 User Guidance

The User is only able to access the module remotely via SSH (CLI) or HTTPS (Management Console). 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.

4. Acronyms

This section describes the acronyms used throughout this document.

Table 17 Acronyms

Acronym	Definition
AC	Alternating Current
AES	Advanced Encryption Standard
BMC	Baseboard Management Controller
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CRNGT	Continuous Random Number Generator Test
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DH	Diffie Hellman
DHE	Diffie Hellman Ephemeral
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
ECDH	Elliptic Curve Diffie Hellman
ECDHE	Elliptic Curve Diffie Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GCM	Galois/Counter-Mode
HMAC	Hash-Based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IP	Internet Protocol
KAT	Known Answer Test
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAC	Message Authentication Code
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Managemnt Protocol
SSH	Secure Shell
TLS	Transport Layer Security
USB	Universal Serial Bus