Symantec, A Division of Broadcom Symantec Content Analysis Virtual Appliance

Software Version: 3.1.3.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS 140-2 Security Level: 1
Document Version: 0.9

CONTACT INFORMATION

Symantec, 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 Symantec Content Analysis Virtual Appliance (Version 3.1.3.0) from Symantec, A Division of Broadcom. This Non-Proprietary Security Policy describes how CAS 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 Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

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 validation of the module. Content Analysis Virtual Appliance is referred to in this document as CAS, the crypto module, or the 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/projects/cryptographic-module-validation-program/validated-modules/search/) 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
- *Entropy Assessment Report* 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 Symantec Content Analysis

2.1 Overview

The Symantec Content Analysis (CAS) is a critical component of effective protection against advanced targeted attacks achieved via multi-layer file inspection and sandboxing. Together with ProxySG or Symantec Messaging Gateway (SMG), it offers the most complete advanced threat protection in the marketplace for blocking known threats and analyzing zero-day and other advanced threats.

See Figure 1 below for a typical deployment scenario for CAS appliances.
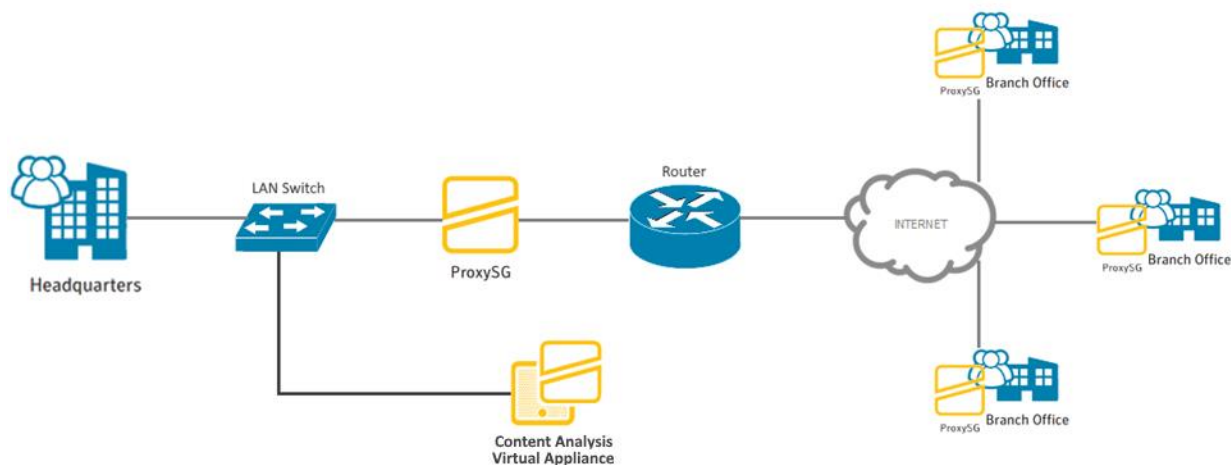
Figure 1 Typical Deployment of CAS

The Content Analysis solution blocks all known threats through inspection of sources and signatures and can centrally analyze unknown content locally and worldwide, leveraging Symantec's Global Intelligence Network. This community-watch effect constantly fortifies your security.

Zero-day threats are escalated automatically within Content Analysis to powerful, dual-detection sandboxing technology. This offers a unique hybrid analysis protocol, including the customizable IntelliVM virtualized sandbox to replicate production environments, and a bare-metal sandbox emulator for accurate analysis and detection of VM-evasive malware. File filtering by Content Analysis mitigates false positive identification of malware and it significantly improves sandbox efficiency by reducing the number of files unnecessarily sent for analysis.

Unlike other sandboxing solutions, information derived from the analysis of malware files is automatically shared with the ProxySG appliances and Content Analysis, so future instances of the malware will be blocked at the gateway.

The solution is powered by the Symantec Global Intelligence Network, informed threat data from more than 70 percent of the Fortune Global 500. The discovery of new malware, threats, or malicious files is shared both locally within your infrastructure, and out through this global community for faster protection against advanced malware and attacks targeting your web, email or mobile environment.

Symantec brings together the full range of products, services, and technologies to deliver advanced threat protection at the web gateway. The table below summarizes its business advantages.

Table 1 Benefits and Advantages

Benefit	Advantage
Scalable, effective defense against advanced targeted attacks, advanced persistent threats, and zero-day malware	Up-to-the-minute threat intelligence is collected from our millions of users to identify unknown threats and shift protection to the gateway.
Defense in depth against advanced threats	At the web and mail gateways, combine real-time blocking and malware scanning, with URI and file whitelisting/blacklisting, static code analysis, and dynamic malware detonation.
More complete detection of zero-day threats	A customizable IntelliVM virtualized sandbox and a bare metal sandbox emulator deliver more accurate analysis and detection of VM evasive malware.

CAS is validated at the following FIPS 140-2 Section levels in Table 2.

Table 2 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 appliance configurations listed in Table 3.

Table 3 CAS Virtual Appliance Configuration

Virtual Appliance Model	Number of Devices
CASVA-100	100
CASVA-C4S	1000

Symantec CAS is a module with a Multi-chip Standalone embodiment. The overall security level of the module is 1. The cryptographic boundary is defined by the virtual appliance, which surrounds all software. The module software, version 3.1.3.0, contains the following cryptographic libraries:

- CAS Cryptographic Library v1.0
- VA Blue Coat Boot Loader Library v5.28
- CAS LRNG Library v1.0

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 Symantec Security Platform (SSP) S410-10 on which it runs. Figure 2 shows the block diagram of the SSP-S410 (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 SSP-S410-10 processor interfaces.
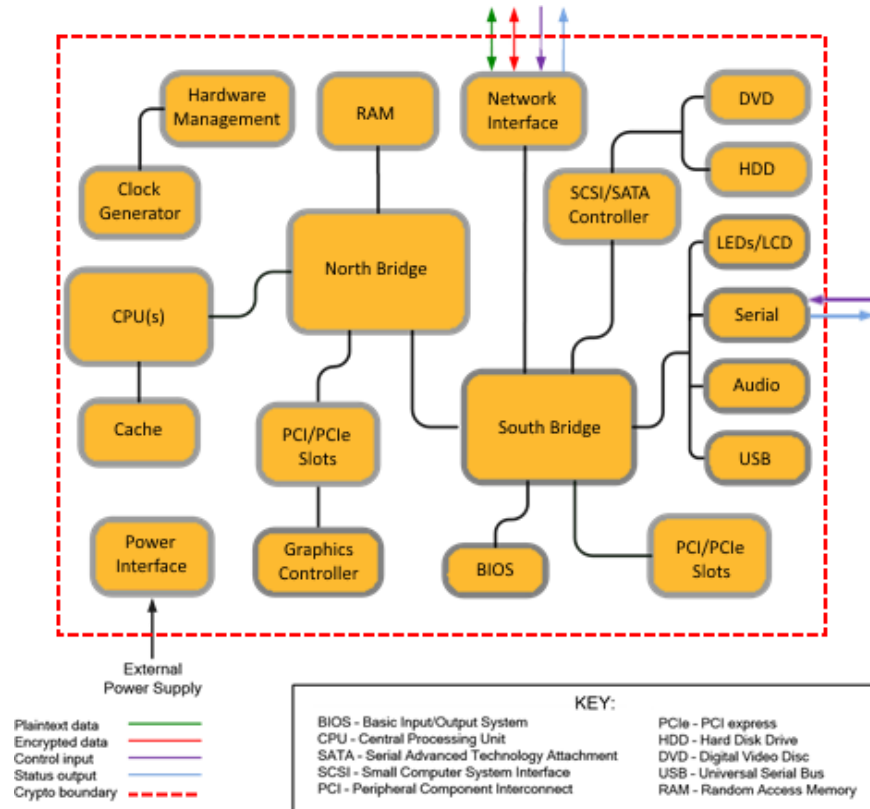
Figure 2 Block Diagram of the SSP-S410-10 hardware

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 CAS 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 SSP-S410-10 (the solid black 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 SSP-S410-10's processor interfaces.

2.2.2   Logical Cryptographic Boundary

The logical cryptographic boundary of the module (shown by the solid yellow line in Figure 3) consists of the OS (CentOS 7), which contains the VA Blue Coat Boot Loader Library v5.28, the CAS OS Cryptographic Library v1.0, and the CAS LRNG Library v1.0.

---

[1] RAM – Random Access Memory
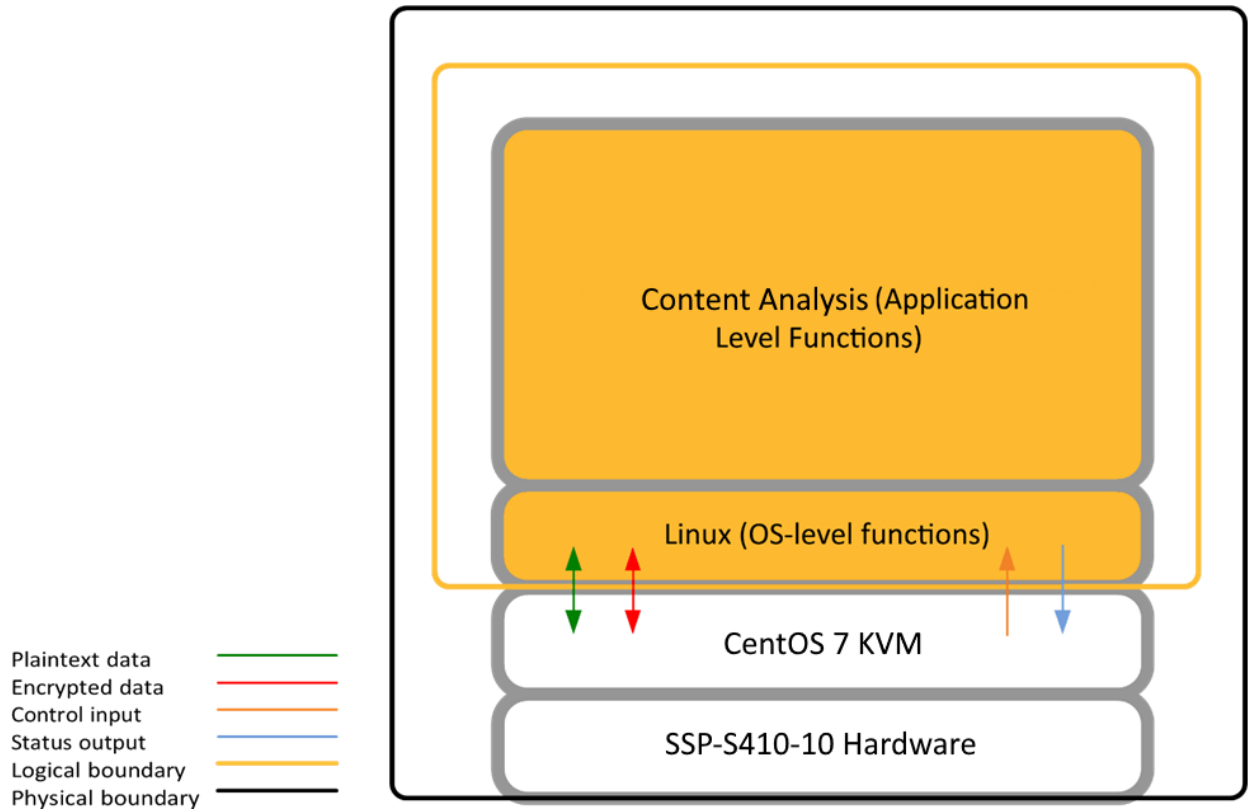
Figure 3 CAS VA Cryptographic Boundary

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 (SSP-S410-10). The Linux KVM 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 (CO) must first map the physical serial port to the CASVA using vSphere Client. The mapping of the module's logical interfaces in the software to FIPS 140-2 logical interfaces is described in Table 4 below.

Table 4 FIPS 140-2 Logical Interface Mappings for the CAS 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 via the Virtual Ethernet and Virtual Serial Port interfaces (Web Interface, SSH CLI, and Serial CLI). Status output consists of the status provided or displayed via the user interfaces (such as Web Interface, SSH CLI, and Serial CLI) or available log information. Status output exits the module via the user interfaces (such as Web Interface, 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 5. The modules offer the following management interface:

- CLI[2] – 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[3]. 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.
- Web Interface – This interface is used for management of the module. It is accessible remotely with a web browser that supports TLS[4]. Authentication is required before any functionality will be available through the Web Interface

When managing the module over the CLI, COs and Users both log into the module with accounts entering the "standard", or "unprivileged" mode on the CLI. 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 5.

---

[2] CLI – Command Line Interface
[3] SSH – Secure Shell protocol
[4] TLS – Transport Layer Security

Table 5 FIPS and CAS Roles

FIPS Roles	Module Roles and Privileges
CO	The CO is an administrator of the module that has been granted "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, and query if the module is in the Approved mode. In addition, COs may do all the services available to Users while not in the "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 Web Interface, they can perform all the same services available in CLI (equivalent to being in the "configuration" mode in the CLI) except the module may not be into the Approved mode via the Web Interface
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. The User may access the CLI and Web Interface for management of the module. When the User is administering the module over the Web Interface, they perform all the same services available in CLI ("standard" mode only services).

Descriptions of the services available to a Crypto Officer (CO) and User are described below in Table 6 respectively. For each service listed below, COs and Users are assumed to already have authenticated prior to attempting to execute the service. There are no additional services that are unauthenticated. 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 6 below. Additional services that do not access CSPs can be found in the *Symantec Content Analysis Command Line Overview, v3.2* located here:

https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/content-analysis/3-1/cli-index.html

Table 6 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 in this *Security Policy*.	CO Password: W "Enabled" mode password: W
Enter the "enabled" mode	Manage the module in the "enabled" mode of operation,	"Enabled" mode password: RX

Service	Description	CSP and Access Required
	granting access to higher privileged commands	
* Enter the "configure" mode	Manage the module in the "configuration" mode of operation, allowing permanent system modifications to be made	None
* Disable FIPS mode	Take the module out of the approved mode of operation and restore it to a factory state	SSH Session Key: W SSH Integrity Key: W TLS Session Key: W TLS Integrity Key: W TLS Pre-Master Secret: W TLS Master Secret: W KAS-FFC private key: W KAS-ECC private key: W DRBG CSPs: W DPK: W DPK: private key: W MDEK: W
Syslog over TLS	Configure the module to use syslog via TLS	RSA public key: RX RSA private key: RX KAS-FFC public key: WRX KAS-FFC private key: WRX KAS-ECC public key: WRX KAS-ECC private key: WRX TLS Session Key: W TLS Integrity Key: W TLS Pre-Master Secret: W TLS Master Secret: W DRBG CSPs: WRX
** Firmware Load[5]	Loads new external firmware and performs an integrity test using an RSA digital signature using the "installed-systems load" command.	Integrity Test public key: WRX
Create remote management session	Manage the module through the CLI (SSH) or Web Interface (TLS) remotely via Ethernet port.	RSA public key: RX RSA private key: RX KAS-FFC public key: WRX KAS-FFC private key: WRX KAS-ECC public key: WRX KAS-ECC private key: WRX SSH Session Key: WRX SSH Integrity Key: WRX DRBG CSPs: WRX DPK: RX CO Password: R

[5] Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation

Service	Description	CSP and Access Required
** Create, edit, and delete User 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 DPK: RX
Show FIPS-mode status	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
* Zeroize keys	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.	SSH Session Key: W SSH Integrity Key: W TLS Session Key: W TLS Integrity Key: W TLS Pre-Master Secret: W TLS Master Secret: W KAS-FFC private key: W KAS-ECC private key: W DPK: W
Modify Scan Service Settings	• Antivirus (AV) Patterns • Scan Behavior • AV File Types • File Reputation • Predictive Analysis Detection sensitive level • Sandboxing • Whitelist/Blacklist settings	None
View Threat Analysis Statistics	• View Cache hits • View Sandboxing reports • View Static Analysis Report • View File Reputation Report • View Whitelist/Blacklist Reports • View system Logs	None
Configure and query password policy	Configure and view the current password policy employed by the module.	None
** Change password	Change Crypto-Officer password	Crypto-Officer Password: RW DPK: RX
* Perform self-test	Perform self-test on demand by rebooting the machine	KAS-FFC public key: W KAS-FFC private key: W KAS-ECC public key: W KAS-ECC private key: W SSH Session Key: W SSH Integrity Key: W TLS Session Key: W

Service	Description	CSP and Access Required
		TLS Integrity Key: W TLS Pre-Master Secret: W TLS Master Secret: W DRBG CSPs: W

* - 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 7 below. Additional services are that do not access CSPs can be found in the *Symantec Content Analysis Command Line Overview, Version 3.1.3.0:*
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/content-analysis/3-1/cli-index.html

Table 7 User Service and CSP Access

Service	Description	CSP and Access Required
Create remote management session	Manage the CAS Module using the CLI (SSH) or Web Interface (TLS) remotely via Ethernet port.	RSA public key: RX RSA private key: RX Client RSA public key: RX KAS-FFC public key: RX KAS-FFC private key: RX KAS-ECC public key: RX KAS-ECC private key: RX SSH Session Key: WRX SSH Integrity Key: WRX DRBG CSPs: WRX DPK: RX
Show FIPS-mode status	Entering the command "show version" will display if the module is configured in Approved Mode.	None
View Threat Analysis Statistics	• View Cache hits • View Sandboxing reports • View Static Analysis Report • View File Reputation Report • View Whitelist/Blacklist Reports View system Logs	None
Show password policy	View the current password policy employed by the module using the "show password-policy-configuration" command.	None

2.4.3   Authentication Mechanism

The module supports role-based authentication. COs and Users must authenticate using a private key (user ID and password), or can alternatively use public key authentication for SSH 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 or TLS session remains active (logged in) and secured until the operator logs out or inactivity for a configurable amount of time has elapsed.

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

Table 8 Authentication Mechanisms Used by Module

Role	Authentication Type	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. 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 approximately 1 in 7.0 million; this is less than 1:100,000 as required by FIPS 140-2.
	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. 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 approximately 1 in 7.0 million; this is less than 1:100,000 as required by FIPS 140-2.

Role	Authentication Type	Authentication Strength
	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. 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 approximately 1 in 7.0 million; this is less than 1:100,000 as required by FIPS 140-2.
	SSH RSA Client keys	The module supports using SSH RSA client keys for authentication of COs 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 140-2.
	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. 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 approximately 1 in 7.0 million; this is less than 1:100,000 as required by FIPS 140-2.
	SSH RSA Client keys	The module supports using SSH RSA client 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

Role	Authentication Type	Authentication Strength
		$1:2^{112}$ or $1: 5.19 \times 10^{33}$. The fastest network connection supported by the module is 1000 Mbps. Hence at most (1000 $\times 10^6 \times 60$ = 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 140-2.

2.5 Physical Security

The CAS VA 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:

- Symantec Security Platform (SSP) S410-10 appliance

- Intel Xeon Silver 4210 (Cascade Lake)

- KVM on CentOS 7

All cryptographic keys and CSPs are under the control of the guest operating system, which protects the CSPs against unauthorized disclosure, modification, and substitution. The module does not provide a general-purpose operating system. The operating system is not modifiable by the operator, and only the modules' signed image can be executed. All software upgrades are digitally-signed, and a conditional self-test (RSA signature verification) is performed during each upgrade.

NOTE: Only FIPS-validated firmware may be loaded to maintain the module's validation.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed below in Table 9.

Table 9 FIPS-Approved Algorithm Implementations for the CAS Cryptographic Library v1.0

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
A1764	AES	SP 800-38A, FIPS 197	CBC, CTR, GCM[6]	AES 128, 256 CBC AES 128, 192, 256 CTR AES 128, 192, 256 GCM	Data Encryption / Decryption
N/A	KTS[7]	SP 800-38F	AES (CBC, CTR, GCM) and HMAC	AES 128, 256 CBC AES 128, 192, 256 CTR AES 128, 192[8], 256 GCM	Key Transport
A1764	AES	SP 800-38E	XTS[9]	128, 256	Data Encryption / Decryption At Rest
A1764	SHS	FIPS 180-4	SHA-1[10], SHA-256, SHA-384, SHA-512		Message Digest

---

[6] AES GCM IV generation method complies with technique #2 in section A.5 of the Implementation Guidance for FIPS PUB 140-2. The AES GCM IV is used in the TLS protocol and in the SSH protocol. In all cases, the AES GCM IV is internally generated via RBG-based construction in compliance with Section 8.2.1 of NIST SP 800-38D using the Approved DRBG within the module's physical boundary and is at least 96 bits in length

[7] KTS - Key establishment methodology provides between 128 and 256 bits of encryption strength

[8] 192 GCM – While this key size was algorithm tested, it is not callable by the module.

[9] XTS mode is only approved for storage device applications

[10] SHA-1 is only used for hashing as part of the SSH and TLS KDFs.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
A1764	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	128, 256, 384, 512	Message Authentication
A1764	RSA	FIPS 186-4	SHA-256, SHA-384 PKCS1 v1.5	2048, 3072, 4096	Digital Signature Generation, Digital Signature Verification
A1764	RSA	FIPS 186-4	PKCS1 v1.5	2048, 3072, 4096	Keypair Generation
A1764	KTS-RSA	SP 800-56B rev 2	KTS-IFC (RSA-OAEP Basic)	2048	Key Transport
A1764	CTR-DRBG	SP 800-90A	CTR-based	AES-256	Deterministic Random Bit Generation
Vendor Affirmed	CKG[11]	SP 800-133			Key Generation
A1764	KAS-SSC	SP 800-56A rev 3	FFC	(2048, 256)	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. A1764 and SSH KDF CVL Cert. A1764).

[11] CKG – Symmetric cryptographic key generation uses the direct output of an approved DRBG with no post-processing per section 4 of NIST SP 800-133rev2. Symmetric keys are generated for CBC, CTR, GCM, and XTS modes.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
A1764	KAS-SSC	SP 800-56A rev 3	ECC	P-256, P-384, P-521[12]	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. A1764 and SSH KDF CVL Cert. A1764).
A1764	CVL TLS 1.0/1.1, TLS 1.2	SP 800-135rev1	TLS 1.2 SHA Sizes = SHA-256, SHA384		Key Derivation
A1764	CVL SSH	SP 800-135rev1	AES-128 CBC, AES-256 CBC	SHA-1, SHA-256, SHA-512	Key Derivation

FIPS-Approved Algorithm Implementations for the three libraries are in Table 10 and Table 11 below.

Table 10 FIPS-Approved Algorithm Implementations for VA Blue Coat Boot Loader Library v5.28

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
A1762	SHS	FIPS 180-4	SHA-1[13], SHA-256		Message Digest as part of Integrity Check
A1762	RSA	FIPS 186-4	SHA-256; PKCS1 v1.5	2048	Digital Signature Verification as part of Integrity Check

---

[12] While the P-256, P-384, and P-521 curves were tested, only P-256 can be called by the module in the Approved mode.

[13] $\mathrm{SHA\text{-}1}$ is as part of HMAC-SHA-1 and is only used for verification purposes as part of the module integrity check.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
A1762	HMAC	FIPS 198-1	HMAC-SHA-1	128	Integrity Check

Table 11 FIPS-Approved Algorithm Implementations for CAS LRNG Library v1.0

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
A1763	SHS	FIPS 180-4	SHA-512		Vetted conditioning component
A1763	CTR-DRBG	SP 800-90A	CTR-based	AES-256	Vetted conditioning component
A1763	AES	SP 800 38A	ECB	256	Vetted Conditioning component
-	ENT (NP[14])[15]	SP 800-90B			Entropy Generation - Seeding for the FIPS-Approved DRBG (SP 800-90 CTR_DRBG)

Table 12 FIPS-Allowed Algorithms

Algorithm	Caveat	Use
RSA Signature Verification	1536, 2048	Signature Verification
MD5	No security is provided by this algorithm.	In TLS 1.0/1.1 Protocol

NOTE: No parts of the TLS or SSH protocols, other than the KDF, have been reviewed or tested by the CAVP and CMVP. FIPS-Allowed algorithms are listed above in Table 12.

---

[14] NP - Non-Physical

[15] ENT (NP) - For seeding the DRBG, the module uses an ENT (NP). The ENT (NP) is implemented by the cryptographic module compliant with SP800-90B and marked as ENT on the certificate. The ENT (NP) provides a 2,048-bit seed with at least 1,139 bits of entropy to the DRBG. The DRBG is thus capable of supporting a minimum of 256 bits of encryption strength in its output

The module supports the CSPs listed below in Table 13 below.

Table 13 List of Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Data Protection Key (DPK)	AES XTS 256-bit key	Internally generated via FIPS-Approved DRBG (per IG A.9)	Never exits the module	Stored in plaintext on non-volatile memory	By disabling the FIPS-Approved mode of operation	Encrypting Crypto-Officer password, User password, "Enabled" mode password, and RSA private key
Firmware Load Test Public Key	RSA public key 2048 bits	Externally generated, Imported in encrypted form via a secure 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	Output during TLS/SSH[17] negotiation in plaintext.	Stored in encrypted form on non-volatile memory	Module's public key is deleted by command	Negotiating TLS or SSH sessions
SSH RSA Client key	2048, 3072, and 4096-bits	Other entities' public keys are sent to the module in plaintext	Never exits the module	Other entities' public keys reside on	Other entities' public keys are cleared by power cycle	Authentication for SSH sessions.

---

[17] SSH session negotiation can only use RSA key pairs of 2048-bits. TLS session negotiation can use RSA key pairs of 2048-bits, 3072-bits and 4096-bits.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
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	Never exits the module	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing encrypting DPK	Negotiating TLS or SSH sessions
KAS-FFC 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
KAS-FFC 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
KAS-ECC private key	P-256 key[18]	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

---

[18] While the P-256, P-384, and P-521 curves were tested, only P-256 can be called by the module in the Approved mode.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
KAS-ECC public key	P-256 key[19]	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 Pre-Master Secret	384-bit key	Input in encrypted form from TLS client	Never	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Establishing the TLS Master Secret
TLS Master Secret	384-bit key	Generated internally during session negotiation	Never exits the module	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Establishing the TLS Session Key
TLS Session key	AES CBC128-,or 256-bit key, AES GCM 128 or 256-bit key	Internally generated via FIPS-Approved DRBG	Output in encrypted form during TLS protocol handshake	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Encrypting TLS data
SSH Session Key	AES CBC 128 or 256-bit key, AES CTR 128, 192, or 256-bit key, AES GCM 128 or 256-bit key	Internally generated via FIPS-Approved DRBG	Output in encrypted form during SSH protocol handshake	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Encrypting SSH data
TLS Integrity key	HMAC SHA-1-, 256-bit, 384-bit key	Internally generated	Never exits the module	Resides in volatile	Rebooting the modules	Data authentication for TLS sessions

[19] While the P-256, P-384, and P-521 curves were tested, only P-256 can be called by the module in the Approved mode.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
				memory in plaintext	Removing power	
SSH Integrity key	HMAC SHA-1-, 256-, 512-bit key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Rebooting the modules Removing power	Data authentication for SSH sessions
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	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypted DPK	Locally authenticating a CO or User for Web Interface 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	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting DPK	Used by the CO to enter the "privileged" or "enabled" mode when using the CLI
SP 800-90A CTR_DRBG Seed[20]	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

---

[20] The CTR DRBG Seed requires a 384-bit number and uses 256 bits of entropy with the derivation function to create the 384-bit value. The 256-bits of CTR DRBG Entropy is obtained from an entropy-generating ENT (NP) inside the module's cryptographic boundary

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SP 800-90A CTR_DRBG Entropy[21]	256-bit random number with 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 ENT (NP) inside the module's cryptographic boundary.

---

[21] The CTR DRBG Entropy required by the FIPS-Approved SP 800-90A CTR_DRBG (with AES-256) is supplied by the ENT (NP). The ENT (NP) provides a full 256 bits of entropy per IG 7.14 Scenario 1A.

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):

```
Boot system failed signature verification
```

If a self-test fails in the CAS Cryptographic Library, the following error is printed to the CLI (when being accessed via the serial port):

```
Open ssl FIPS POST Test failed. Rebooting…
```

When these errors occur, 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 below 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 VA Blue Coat Boot Loader Library:

- Known Answer Tests
    - HMAC KAT using SHA-1; and
    - RSA Sign/Verify KAT with SHA-256
- Firmware integrity check using HMAC-SHA-1

The module performs the following self-tests using the CAS LRNG Library:

- Known Answer Tests
    - SHA-512
    - AES ECB KAT for encryption and decryption
    - SP800-90A DRBG KAT

The module then performs the following self-tests using the CAS Cryptographic Library at power-up:

- Known Answer Tests
    - AES KAT for encryption and decryption
    - AES GCM KAT for encryption and decryption
    - AES XTS KAT for encryption and decryption
    - HMAC KAT using SHA-1, SHA-256, SHA-384, SHA-512
    - RSA Sign/Verify KAT with SHA-256
    - SP800-90A DRBG KAT
    - KAS-FFC-SSC KAT
    - KAS-ECC-SSC 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 for its CAS Cryptographic Library.

- RSA pairwise consistency check upon generation of an RSA keypair
- Continuous RNG test (CRNGT) for the SP800-90A DRBG
- CRNGT for the ENT (NP)
- Firmware Load Test using RSA Signature Verification

The module performs the conditional self-tests for its LRNG Cryptographic Library.

- Entropy Health Tests:
    - Repetition Count Test (RCT[22]) specified in SP800-90 section 4.4.1
    - Adaptive Proportion Test (APT) as specified in SP800-90B section 4.4.2

2.8.3   Critical Function Tests

The module performs the following critical function tests in the VA Blue Coat Boot Loader:

- RSA Signature Verification

The modules performs the following critical function tests on both the CAS OS and CAS LRNG:

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

CAS runs a health check on the CTR DRBGs every 2^24 requests, which is less than the CTR DRBG reseed interval of 2^48 per NIST SP800-90A.

Additionally, per the IG A.9 requirements**,** the CAS Cryptographic Library performs the following critical functions test for AES XTS to ensure that the two keys used in this operation are not identical (Key_1 ≠ Key_2):

- AES XTS Duplicate Key Test

2.9 Mitigation of Other Attacks

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

---

[22] The implemented APT and RCT entropy health tests run on the first 1024 entropy samples at startup.

---

3   Secure Operation

The module can be configured into an explicit FIPS mode of operation as per the instructions provided below in Section 3.1. However, the module supports a non-compliant state, the initialization of which requires an explicit separate configuration. When the module is operating in non-compliant state, the services have access to non-Approved and non-Allowed algorithms. The logical boundary of the module is defined such that all functionality available in non-compliant state is scoped out from the module boundary. Thus, when the module is operating in FIPS Approved mode of operation, it can access only FIPS Approved or Allowed algorithms as access to non-Approved and non-Allowed algorithms are explicitly inhibited by design of the module.

The module meets FIPS-140-2 Level 1requirements. 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 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.

Once the VM has been deployed, the CO must place the module in the Approved mode using the Console Tab which provides access to the virtual serial connection.

1. Download the Virtual Appliance Package (VAP), which consists of the deployment .ISO file.

2. Verify that you have downloaded the .iso file to a directory for which you have privileges.

3. Enter the following command to verify that the kernel module is loaded:

    a.   #lsmod |grep kvm

4. Enter the following command to create and launch the KVM instance

    a.   # virt-install --name kvm_instance_name \

5. Enter the following command to open the console on the Management Center KVM instance.

    a.   # virsh console mc_vm_name

6. Enter the serial number provided (You may need to press "Enter" a few times to display the CLI prompt).
7. Press **Enter** three times.

```
Welcome to the Symantec Content Analysis Virtual Appliance Serial
Console
Version: Content Analysis 3.1.3.0. Release id: 263357 64-bit


------------------------ MENU -----------------------------
1) Command Line Interface
2) Setup Console
------------------------------------------------------------------
Enter option:
```

8. Enter **1** to access the Command Line Interface.

9. Type **enable** and press **Enter**.

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

    When prompted for confirmation, select **Y** to confirm.

    - **NOTE 1**: The fips-mode enable command causes the device to power cycle, zeroing the appliance and returning the configuration values set in steps 1 and 2 to their factory state.

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

12. Enter the properties for the following:

    a. IP address

    b. IP subnet mask

    c. IP gateway

    d. DNS server parameters

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

    ```
    DIRECTIONS:

    The console username, password and enable password are special administrative
    credentials which can be used to log into the command line interface or web
    management interface.


    Enter console password:
    Verify console password:


    Enter enable password:
    Verify enable password:
    ```

Upon completion of these initialization steps, the module is considered to be operating in its Approved mode of operation. There are no additional non-Approved services while operating in the Approved mode.

3.1.1   Management

The Crypto-Officer is able to monitor and configure the module via the Web Interface (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 Product 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.

The CO password and "enabled" mode password must be at least 8 characters in length.

3.1.2   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 DPK. 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 DPK. Once the DPK is zeroized, decryption involving the DPK 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 (NP) 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 (Web Interface). 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. See Table 14 below.

Table 14 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CRNGT	Continuous Random Number Generator Test
CCCS	Canadian Centre for Cyber Security
CSP	Critical Security Parameter
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
HMAC	Hash-Based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
KAS	Key Agreement Scheme
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
TLS	Transport Layer Security