Blue Coat Systems, Inc.

Secure Web Gateway Virtual Appliance-V100

Software Version: 6.5.2.8

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.5

Prepared for:

BLUE COAT

Blue Coat Systems, Inc.
420 N. Mary Avenue
Sunnyvale, CA 94085
United States of America

Phone: +1 866 30 BCOAT (22628)
Email: usinfo@bluecoat.com
http://www.bluecoat.com

Prepared by:

Corsec

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

List of Figures

List of Tables

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Secure Web Gateway Virtual Appliance-V100 (SWG VA-V100) (Software Version: 6.5.2.8) from Blue Coat Systems, Inc. This Security Policy describes how the Secure Web Gateway Virtual Appliance-V100 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 Canada (CSEC) 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 Secure Web Gateway Virtual Appliance-V100 is referred to in this document as SWG VA-V100, 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 Blue Coat website (www.bluecoat.com) contains information on the full line of products from Blue Coat.
- 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 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
- Validation Submission Summary
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Blue Coat. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Blue Coat and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Blue Coat.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2 SWG VA-V100

2.1 Overview

The Blue Coat Secure Web Gateway Virtual Appliance (SWG VA-V100) combines the market-leading security capabilities of Blue Coat ProxySG with the flexibility of virtualization to provide a cost-effective enterprise branch office solution. With the new Blue Coat Secure Web Gateway Virtual Appliance, businesses can support Web security and other critical remote office infrastructure on a common platform, reducing costs and IT resource requirements.

The Blue Coat SWG VA-V100 is a powerful yet flexible tool for providing security and control, threat prevention, and accelerated disaster recovery in an easy-to-deploy virtual appliance:

- Web 2.0 Security and Control – The Blue Coat Unified Security Solution is uniquely designed to offer a comprehensive, enterprise-wide web security solution that can help close network security gaps and protect users wherever they work. SWG VA-V100 extends the same rich policy controls in ProxySG to the branch environment. With unified reporting that provides a single pane of glass visibility across all users, and centralized management through the Blue Coat Director, the SWG VA-V100 solution allows enterprises to seamlessly extend full protection and control to their branch offices
- Threat Prevention – Integrating with Blue Coat WebPulse, the SWG VA-V100 is able to protect against zero-day attacks through 'negative day' defense. Blue Coat WebPulse is constantly monitoring over 500 malware delivery networks to identify and proactively block attacks at the origin.
- Disaster Recovery – With SWG VA-V100, enterprises can quickly bring up an SWG deployment in case of disaster recovery, and even leverage a backup image of the solution.
- Simplified Deployment – The Blue Coat SWG VA-V100 greatly simplifies the deployment by enabling hardware consolidation and alleviating much of the IT administrative overhead. Running on VMWare ESX and ESXi, SWG VA-V100 shares the same server hardware with other virtual appliances, which significantly streamlines and accelerates the SWG deployment process. As a result, deployment that once took days can now be completed in just hours

See Figure 1 below for a typical deployment scenario for SWG VA-V100s.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

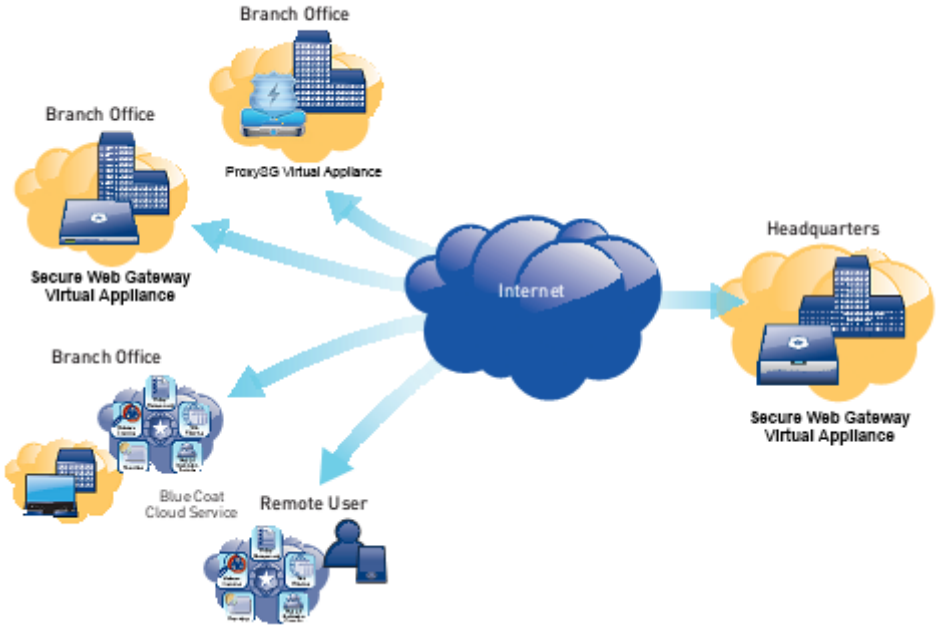

Figure 1 Typical Deployment of a SWG VA-V100

The security provided by the SWG VA-V100 can be used to control, protect, and monitor the Internal Network's use of controlled protocols on the External Network. The controlled protocols implemented in the evaluated configurations are:

- Windows Media Optimization (Microsoft Media Streaming (MMS))
- Microsoft Smooth Streaming Optimization
- Real Media Optimization
- Real-Time Streaming Protocol (RTSP) Optimization
- Real-Time Messaging Protocol (RTMP) Optimization
- QuickTime Optimization (Apple HTTP Live Streaming)
- Adobe Flash Optimization (Adobe HTTP Dynamic Streaming)
- Bandwidth Management
- DNS proxy
- Advanced DNS Access Policy
- Hypertext Transfer Protocol (HTTP)/Secure Hypertext Transfer Protocol (HTTPS) Acceleration
- File Transfer Protocol (FTP) Optimization
- Secure Sockets Layer (SSL) Termination/Protocol Optimization
- TCP[1] tunneling protocols (Secure Shell (SSH))
- Secure Shell
- Telnet Proxy
- ICAP Services
- Netegrity SiteMinder
- Oblix COREid
- Peer-To-Peer
- User Authentication
- Onbox Content Filtering (3rd Party or BCWF[2])

1 TCP – Transmission Control Protocol

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- Offbox Content Filtering (via ICAP)
- SOCKS[3]

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

The SWG VA-V100 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	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Secure Web Gateway Virtual Appliance-V100 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 R720 Server using VMware ESXi v5.1 hypervisor to provide the virtualization layer.

The SWG VA-V100 software consists of Blue Coat's proprietary operating system, SGOS v6.5.2.50. 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. Cryptographic services are provided by the Blue Coat SG VA Starter v4.5, Blue Coat SG VA Crypto Library v3.1.2, Blue Coat SG VA SSH Library v1.0, and Blue Coat SG VA TLS Library v1.0 (which are all part of SGOS).

The module implements the FIPS-Approved algorithms listed in below in Table 2, Table 3, Table 4, and Table 5.

[2] BCWF – Blue Coat Web Filter
[3] SOCKS – SOCKet Secure

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Table 2 FIPS-Approved Algorithm Implementations – SG VA Starter

Algorithm	Certificate Number
Hashing Functions	
SHA[4]-1	#2306
MAC Functions	
HMAC[5] with SHA-1	#1715

Table 3 FIPS-Approved Algorithm Implementations – SG VA Crypto Library

Algorithm	Certificate Number
Symmetric Key Algorithms	
AES: ECB[6], CBC[7], OFB[8], CFB[9]-128 bit mode for 128-, 192-, and 256-bit key sizes	#2737
3DES[10]: ECB, CBC, CFB-64, OFB mode for keying option 1 (3 different keys)	#1648
Asymmetric Key Algorithms	
RSA (ANSI X9.31) Key Generation – 2048, 3072, 4096-bit RSA PKCS[11]#1 signature generation – 2048, 3072, and 4096-bit RSA PKCS#1 signature verification – 1024, 1536, 2048, 3072, and 4096-bit	#1427
Hashing Functions	
SHA-1	#2307
SHA-224, SHA-256, SHA-384, SHA-512	
Message Authentication Code (MAC) Functions	
HMAC with SHA-1	#1716
HMAC with SHA-224, SHA-256, SHA-384, SHA-512	
Deterministic Random Bit Generator (DRBG)	
SP[12] 800-90 CTR_DRBG (AES-256)	#458

***NOTE**: As of December 31, 2010, the following algorithm listed in the table above is considered "legacy-use" only.*

- *Digital signature verification using RSA key sizes of 1024 and 1536-bits are approved for legacy use only.*

[4] SHA – Secure Hash Algorithm
[5] HMAC – Hash-Based Message Authentication Code
[6] ECB – Electronic Codebook
[7] CBC – Cipher Block Chaining
[8] OFB – Output Feedback
[9] CFB – Cipher Feedback
[10] 3DES – Triple Data Encryption Standard
[11] PKCS – Public Key Cryptography Standard
[12] SP – Special Publication

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Table 4 FIPS-Approved Algorithm Implementations – SG VA SSH Library

Algorithm	Certificate Number
Key Derivation Function (KDF)	
SSH KDF	#182

***NOTE**: While the SSH KDF has been validated by the CAVP, this protocol has not been reviewed or tested by the CAVP and CMVP.*

Table 5 FIPS-Approved Algorithm Implementations – SG VA TLS Library

Algorithm	Certificate Number
KDF	
TLS KDF	#328

***NOTE**: While the TLS KDF has been validated by the CAVP, this protocol has not been reviewed or tested by the CAVP and CMVP.*

The module utilizes the following non-FIPS-Approved algorithms:

- RSA PKCS#1 wrap/unwrap (key-wrapping) – 2048, 3072, and 4096–bit sizes providing 112, 130, and 150-bits of security.
- Diffie-Hellman for key agreement during TLS and SSH: 2048-bit keys (provides 112 bits of security).
- Non-Deterministic RNG (NDRNG) for seeding the non-Approved Entropy PRNG
- Non-Approved Entropy PRNG for seeding the FIPS-Approved DRBG (SP800-90A CTR_DRBG (using AES-256))

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 R720 Server on which it runs. Figure 2 shows the block diagram of the Dell PowerEdge R720 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 R720 Server's processor interfaces.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

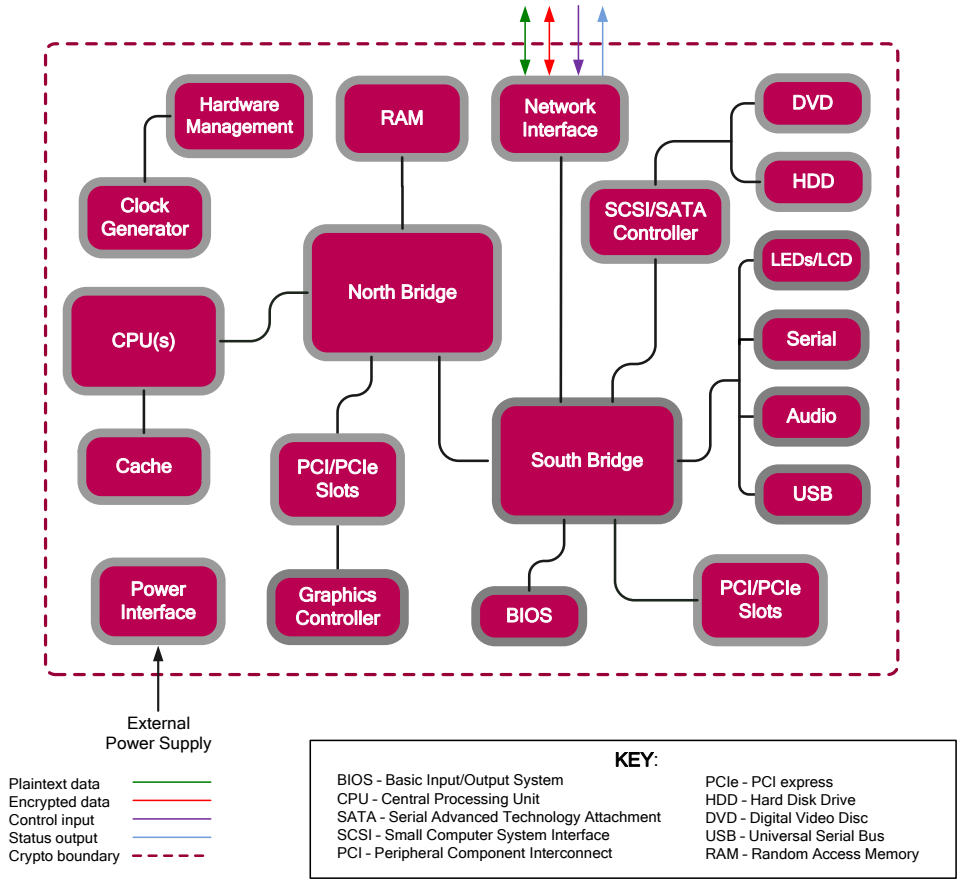

Figure 2 Block Diagram of the Dell PowerEdge R720 Server hardware

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 SWG VA-V100 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[13], hard disk, device case, power supply, and fans. Figure 2 shows the block diagram of the Dell PowerEdge R720 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 R720 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 Blue Coat SGOS v6.5.2.50, which contains the Blue Coat SG VA Starter v4.5, Blue Coat SG VA Crypto Library v3.1.2, Blue Coat SG VA SSH Library v1.0, and Blue Coat SG VA TLS Library v1.0.

[13] RAM – Random Access Memory

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

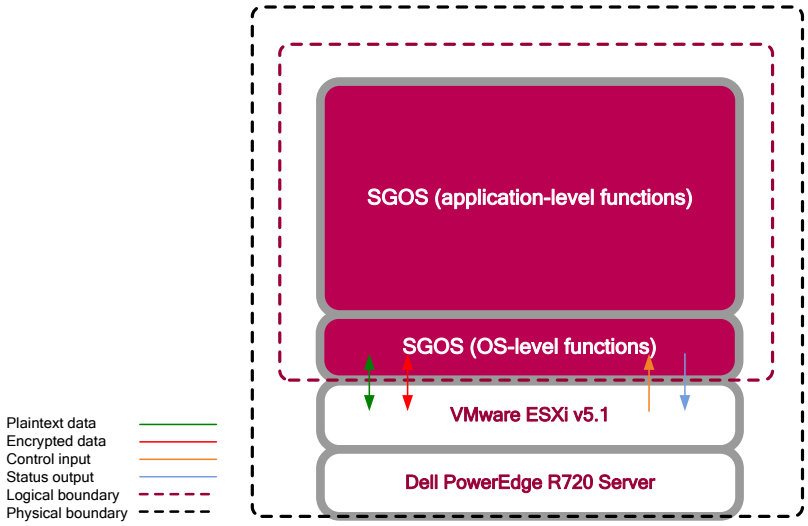

Figure 3 SWG VA-V100 Cryptographic Boundaries

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 R720 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 SWG VA-V100 using vSphere Client. The mapping of the module's logical interfaces in the software to FIPS 140-2 logical interfaces is described in Table 6 below.

Table 6 Virtual Appliance FIPS 140-2 Logical Interface Mappings

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

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Physical Port/Interface	Logical Port/Interface	FIPS 140-2 Interface
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

The module supports role-based authentication. There are two authorized roles in the module that an operator may assume: a Crypto-Officer (CO) role and a User role.

Before accessing the modules for any administrative services, COs and Users must authenticate to the module according to the methods specified in Table 10. The modules offer two management interfaces:

- CLI – accessible only remotely via the Console Tab (within VMware vCenter Server, provides access to the Setup Console portion of the CLI which requires the additional "Setup" password to gain access) or using SSH. This interface is used for management of the modules. This interface must be accessed via the Console Tab 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 via the Console Tab. Authentication is required before any functionality will be available through the CLI.

- Management Console – 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 SWG VA-V100. 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 7.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Table 7 FIPS and SWG VA-V100 Roles

FIPS Roles	SWG VA-V100 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 (Console Tab 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. The CO may monitor the health and status of the modules using SNMPv3. SNMPv3 privacy and authentication keys are assigned to a CO and are not tied to the CO's CLI and Management Console credentials.
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 will access the CLI and Management Console interfaces 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). The User may monitor the health and status of the modules using SNMPv3. SNMPv3 privacy and authentication keys are assigned to a User and are not tied to the User's CLI and Management Console credentials.

Descriptions of the services available to a Crypto-Officer and User are described below in Table 8 and Table 9 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 services available to the Crypto-Officer role are provided in the table below.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Table 8 Crypto-Officer Role Services and CSP Access

Service	Description	CSP and Access Required
Set up the module	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 the Security Policy.	CO Password – W "Enabled" mode password – W "Setup" Password – W
Enter the "enabled" mode	Manage the module in the "enabled" mode of operation, granting access to higher privileged commands	Enabled" mode password – RX
* Enter the "configuration" mode	Manage the module in the "configuration" mode of operation, allowing permanent system modifications to be made	None
* Disable FIPS mode	Re-initializes the module to a factory state (accessible only via the CLI via the Console Tab)	MAK – W SSH Session Key – W SSH Authentication Key – W TLS Session Key – W TLS Authentication Key – W
** Software Load	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 SSH Session Key – WRX SSH Authentication Key –WRX
Create remote management session (Management Console)	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 TLS Session Key – WRX TLS Authentication Key – WRX
** 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 SNMP Privacy Key – W SNMP Authentication Key – W
** Create filter rules (CLI)	Create filters that are applied to user data streams.	None
Create filter rules (Management Console)	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 (Management Console)	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

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Service	Description	CSP and Access Required
** Manage module configuration	Backup or restore the module configuration	RSA public key – WRX RSA private key – WRX SNMP Privacy Key – WRX SNMP Authentication Key – WRX CO Password – WRX User Password – WRX "Enabled" mode password – WRX
* Zeroize keys	Zeroize keys by re-initializing the module to a factory state (accessible only via the Console Tab). This will zeroize all CSPs. The zeroization occurs while the module is still in Approved-mode.	MAK – W SSH Session Key – W SSH Authentication Key – W TLS Session Key – W TLS Authentication Key – W
** Change password	Change Crypto-Officer password	Crypto-Officer Password – W
* Perform self-test	Perform self-test on demand by rebooting the machine	SSH Session Key – W SSH Authentication Key – W TLS Session Key – W TLS Authentication Key – W
* Reboot the module	Reboot the module	SSH Session Key – W SSH Authentication Key – W TLS Session Key – W TLS Authentication Key – W
Create SNMPv3 session	Monitor the module using SNMPv3	SNMP Privacy Key – RX SNMP Authentication Key – 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 services available to the User role are provided in the table below.

Table 9 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 SSH Session Key –WRX SSH Authentication Key –WRX
Create remote management session (Management Console)	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 TLS Session Key – WRX TLS Authentication Key – WRX
Create SNMPv3 session	Monitor the health of the module using SNMPv3	SNMP Privacy Key – RX SNMP Authentication Key – RX

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Service	Description	CSP and Access Required
Show FIPS-mode status (Management Console)	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

2.4.3 Additional Services

The module also offers proxying and termination services for the protocols listed in section 2.1. To provide these services, the module utilizes the following cryptographic functions:

- Approved
  - AES
  - Triple-DES
  - DSA
  - RSA
  - SHA
  - HMAC
  - SP800-90A CTR_DRBG
  - Diffie Hellman
- Non-compliant
  - ANSI X9.31 PRNG
- non-Approved
  - CAST-128
  - DES
  - RC2
  - RC4
  - Camellia
  - MD2
  - MD5
  - HMAC-MD5
  - RIPE-MD-160

The use of the non-Approved algorithms listed above is not relevant to the secure operation of the module and the output of their use is equivalent to plaintext. For more information on the non security relevant services of the module, please refer to the *Blue Coat® Systems SGOS Administration Guide.*

2.4.4 Authentication Mechanism

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 for User services have no interface available to access other services (i.e. 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 sessions remain 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

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Card (CAC) authentication for COs and Users connecting to management functionality of the module. Additionally, other agencies may require FIPS 201 validated PIV[14] II card authentication.

When the module is configured to use CAC authentication, the module 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 third-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 *`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 below in Table 10.

[14] PIV – Personal Identity Verification II

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Table 10 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 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 Crypto-Officer may connect locally using the host system's serial port or remotely after establishing a TLS or SSH session (Management Console, SSH CLI, Console Tab).
	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 through the Console Tab or 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 Console Tab 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}.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

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: 5.19×10^{33}.

2.5 Physical Security

The Secure Web Gateway Virtual Appliance-V100 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 R720 Server appliance
  - Two Six-Core Intel Xeon 5300 processors (2.5 Ghz clock speed)
  - VMware ESXi v5.1 with Blue Coat's SGOS v6.5.2.50 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.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 11.

Table 11 List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Master Appliance Key (MAK)	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 and returning to factory state.	Encrypting Crypto-Officer password, SNMP localized key, 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 Key	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[15] negotiation in plaintext. Output during TLS negotiation for CAC authentication Exits in encrypted format when performing a module configuration backup.	Modules' public key is stored on non-volatile memory.	Modules' public key is deleted by command.	Negotiating TLS or SSH sessions

[15] 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.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
	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.	
RSA Private Key	2048, 3072, and 4096-bits	Internally generated via FIPS-Approved DRBG. Imported in encrypted form via a secure TLS or SSH session Enters the module in plaintext via a virtual serial connection.	Exits in encrypted format when performing a module configuration backup.	Stored in encrypted form on non-volatile memory	Made inaccessible by zeroizing the encrypting MAK upon leaving FIPS mode (returning to factory state).	Negotiating TLS or SSH sessions
DH public key	2048-bits	The module's Public key is internally generated via FIPS-Approved DRBG; while 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; remove 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; remove power	Negotiating TLS or SSH sessions

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
TLS or SSH Session Key	AES CBC 128-, or 256-bit key 3DES 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; remove power	Encrypting TLS or SSH data
TLS or SSH Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Rebooting the modules; remove power	Data authentication for TLS or 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 virtual serial connection.	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.	Made inaccessible by zeroizing the encrypting MAK upon leaving FIPS mode (returning to factory state).	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 virtual serial connection.	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.	Made inaccessible by zeroizing the encrypting MAK upon leaving FIPS mode (returning to factory state).	Used by the CO to enter the "privileged" or "enabled" mode when using the CLI.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
"Setup" Password	Minimum of four (4) and maximum of 64 bytes long printable character string.	Enters the module in plaintext via a virtual serial connection.	Never exits the module.	Stored in encrypted form on non-volatile memory.	Made inaccessible by zeroizing the encrypting MAK upon leaving FIPS mode (returning to factory state).	Used by the CO to secure access to the CLI when accessed over the virtual serial connection.
SNMP Privacy Key	AES CFB 128 -bit key	Externally generated, Imported in encrypted form via a secure TLS or SSH session Enters the module in plaintext via a virtual serial connection.	Exits the module encrypted over TLS or encrypted during a configuration backup.	Stored in encrypted form on non-volatile memory	Made inaccessible by zeroizing the encrypting MAK upon leaving FIPS mode (returning to factory state).	Encrypting SNMPv3 packets.
SNMP Authentication Key	HMAC-SHA-1-96 – bit key	Externally generated, Imported in encrypted form via a secure TLS or SSH session Enters the module in plaintext via a virtual serial connection.	Exits the module encrypted over TLS or encrypted during a configuration backup.	Stored in encrypted form on non-volatile memory	Made inaccessible by zeroizing the encrypting MAK upon leaving FIPS mode (returning to factory state).	Authenticating SNMPv3 packets.
SP 800-90A CTR_DRBG Seed	384-bit random number	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules; remove power	Seeding material for the SP800-90A CTR_DRBG
SP 800-90A CTR_DRBG Entropy[16]	256-bit random number with derivation function	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules; remove power	Entropy material for the SP800-90A CTR_DRBG

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

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SP 800-90A CTR_DRBG key value	Internal state value	Internally generated	Never	Plaintext in volatile memory	Rebooting the modules; remove 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; remove power	Used for the SP 800-90A CTR_DRBG

NOTE: *that some algorithms may be classified as deprecated, restricted, or legacy-use. Please consult NIST SP 800-131A for details.*

Keys and passwords that exit the module during a configuration backup are encrypted using a FIPS-Approved encryption algorithm. During the backup process, the CO must select the encryption algorithm to use: AES-128 CBC mode, or AES-256 CBC mode. The encryption algorithm selected by the CO should only be used to encrypt keys of less than or equal strength.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2.8 Self-Tests

If any of the self-tests fail, an error is printed to the CLI (when being accessed via the Console Tab). When this error 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 below is shown only over the CLI (when being accessed via the virtual 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:
```

The sections below describe the self-tests performed by the module.

2.8.1 Power-Up Self-Tests

The Secure Web Gateway Virtual Appliance-V100 performs the following self-tests at power-up:

- Software integrity check using HMAC SHA-1 (performed by SG VA Starter v4.5)
- Known Answer Tests (KATs) (performed by SG VA Crypto Library 3.1.2)
    - AES Encrypt KAT
    - AES Decrypt KAT
    - 3DES Encrypt KAT
    - 3DES Decrypt KAT
    - RSA digital signature generation KAT
    - RSA digital signature verification KAT
    - RSA wrap/unwrap KAT
    - SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 KATs
    - HMAC KAT with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 KATs
    - DRBG 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 SWG VA-V100 performs the following conditional self-tests.

- Continuous RNG Test (CRNGT) for FIPS-Approved DRBG
- CRNGT for NDRNG
- CRNGT for Entropy PRNG
- RSA pairwise consistency test upon generation of an RSA keypair
- Software Load Test using RSA signature verification

2.8.3 Critical Function Tests

The Secure Web Gateway Virtual Appliance implements the SP 800-90A CTR_DRBG as its random number generator. The following critical function tests are implemented by the module:

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

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- DRBG Uninstantiate Critical Function Test

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.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3 Secure Operation

The Secure Web Gateway Virtual Appliance-V100 meets Level 1 requirements for FIPS 140-2. 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 *Blue Coat Systems SGOS Administration Guide, Version SGOS 6.5.x* for more information on configuring and maintaining the module.

Caveat: While the SWG VA-V100 may hold and boot from multiple software images, only the software image documented in this Security Policy (Software Version: 6.5.2.8) 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 *Blue Coat® Systems Secure Web Gateway Virtual Appliance-V100 Initial Configuration Guide, For SGOS 6.4.1 or 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. The CO must enter the 'enabled' mode (which requires the enable password) and enter the 'fips-mode enable' command. Entering this command will reset the configuration performed in Chapter 4 and cause an immediate reboot. Once the module has finished rebooting, the CO must perform the initial configuration as described in Chapter 4, the section titled 'Perform Initial Configuration.' The CO will also have to specify a password to secure the 'Setup Console' access, available through 'Console Tab.'

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 (Console Tab or SSH).

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 Blue Coat Systems Blue Touch Online (BTO) and the administrative guidance documents to resolve the issues. If the problems cannot be resolved through these resources, Blue Coat Systems customer support should be contacted.

The CO must ensure that localized keys used for SNMPv3 authentication and privacy match the key type requirements specified in Table 11. 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 8 characters in length.

When creating or importing key pairs, such as during the restoration of an archived SWG VA configuration, the CO must ensure that the "Do not show key pair" option is selected in the Management Console as shown in Figure 4, or the "no-show" argument is passed over the CLI as shown in Figure 5. Please see Section E: Preparing Archives for Restoration on New Devices in the *Blue Coat Systems SGOS Administration Guide, Version 6.5* for further reference.

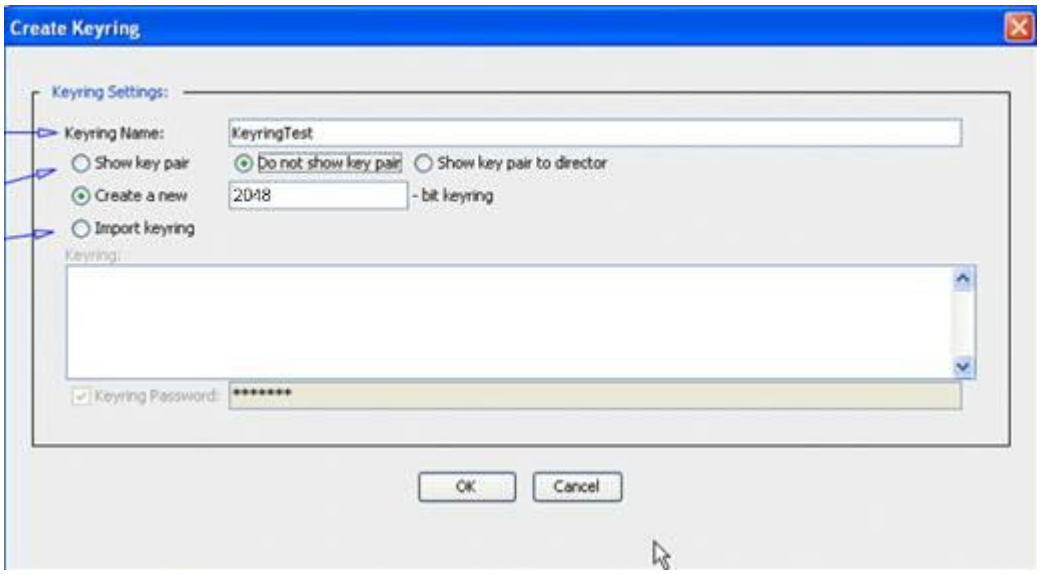

Figure 4 Keyring Creation Management Console Dialogue Box

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 5 Keyring Creation CLI Commands

3.1.3 Zeroization

The CO can return the module to an uninitialized 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 MAK, which renders all of the following CSPs inaccessible: RSA private key, Crypto-Officer password, User password, "Enabled" mode password, "Setup" password, SNMP Privacy key, and the

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

SNMP Authentication key. Once the MAK is zeroized, decryption involving the MAK becomes impossible, making these CPSs 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, Entropy PRNG 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.

3.3 Non-Approved Mode

When initialized and configured according to the Crypto-Officer guidance in this Security Policy, the module does not support a non-Approved mode of operation.

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

4 Acronyms

This section describes the acronyms used throughout this document.

Table 12 Acronyms

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
BTO	BlueTouch Online
CA	Certificate Authority
CAC	Common Access Card
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CIFS	Common Internet File System
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CN	Common Name
CO	Crypto-Officer
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CX4	Four pairs of twin-axial copper wiring
DES	Data Encryption Standard
DNS	Domain Name System
DoD	Department of Defense
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HDS	HTTP Dynamic Streaming
HLS	HTTP Live Streaming
HMAC	Hash-Based Message Authentication Code

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Acronym	Definition
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IM	Instant Messaging
IMAP	Internet Message Access 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
OFB	Output Feedback
OS	Operating System
P2P	Peer-to-Peer
PC	Personal Computer
PCI-e	Peripheral Component Interconnect Express
PIN	Personal Identification Number
PIV	Personal Identity Verification
PN	Principle Name
POP3	Post Office Protocol version 3
RC2	Rivest Cipher 2
RC4	Rivest Cipher 4
RS-232	Recommended Standard 232
RSA	Rivest Shamir Adleman
RTMP	Real-Time Messaging Protocol
RTSP	Real-Time Streaming Protocol
SFTP	Secure File Transfer Protocol
SGOS	Secure Gateway Operating System
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOCKS	SOCKet Secure
SSH	Secure Shell

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

.

Acronym	Definition
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UPN	User Principle Name
VoIP	Voice Over Internet Protocol
WAN	Wide Area Network

© 2014 Blue Coat Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com