Blue Coat® Systems

ProxySG S400 Series

Models: ProxySG S400-20, S400-30, S400-40

Hardware Versions: 080-03568, 080-03572, 080-03576, 080-03570, 080-03574, 080-03578, 090-03075, 090-03079, 090-03083, 080-03571, 080-03575, 080-03579, 090-03076, 090-03080, 090-03084

FIPS Security Kit Version: 085-02891

Firmware Versions: 6.5.2.9 build 144008

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2

Document Version: 08/15/2014

BLUE COAT

COPYRIGHT NOTICE

BLUE COAT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. BLUE COAT PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Americas: Rest of the World:
Blue Coat Systems, Inc. Blue Coat Systems International SARL
420 N. Mary Ave. 3a Route des Arsenaux
Sunnyvale, CA 94085 1700 Fribourg, Switzerland

Table of Contents

1. INTRODUCTION 5
1.1 PURPOSE 5
1.2 REFERENCES 5
1.3 DOCUMENT ORGANIZATION 5
2. PROXYSG S400 6
2.1 OVERVIEW 6
2.2 MODULE SPECIFICATION 9
2.3 MODULE INTERFACES 10
2.4 ROLES AND SERVICES 13
2.4.1 Crypto-Officer Role *15*
2.4.2 User Role *17*
2.4.3 Authentication Mechanism *18*
2.5 PHYSICAL SECURITY 21
2.6 NON-MODIFIABLE OPERATIONAL ENVIRONMENT 21
2.7 CRYPTOGRAPHIC KEY MANAGEMENT 21
2.8 SELF-TESTS 29
2.8.1 Power-Up Self-Tests *29*
2.8.2 Conditional Self-Tests *29*
2.8.3 Critical Function Tests *30*
2.9 MITIGATION OF OTHER ATTACKS 30
3. SECURE OPERATION 31
3.1 INITIAL SETUP 31
3.1.1 Label and Baffle Installation Instructions *31*
3.2 SECURE MANAGEMENT 35
3.2.1 Initialization *35*
3.2.2 Management *39*
3.2.3 Zeroization *39*
3.3 USER GUIDANCE 40
3.4 NON-APPROVED MODE 40
4. ACRONYMS 41

List of Figures

FIGURE 1 TYPICAL DEPLOYMENT OF A PROXYSG APPLIANCE 6
FIGURE 2 PROXYSG S400 (FRONT VIEW) 10
FIGURE 3 CONNECTION PORTS AT THE REAR OF THE PROXYSG S400 11
FIGURE 4 FIPS SECURITY KIT CONTENTS 31
FIGURE 5 SHUTTER DISASSEMBLY 32
FIGURE 6 LOWER SHUTTER INSTALLATION 32
FIGURE 7 UPPER SHUTTER INSTALLATION 33
FIGURE 8 LABEL SHOWING TAMPER EVIDENCE 33
FIGURE 9 KEYRING CREATION MANAGEMENT CONSOLE DIALOGUE BOX 39
FIGURE 10 KEYRING CREATION CLI COMMANDS 39

List of Tables

TABLE 1 MACH5 VS. PROXY EDITION CAPABILITY DIFFERENCES.....7
TABLE 2 SECURITY LEVEL PER FIPS 140-2 SECTION.....8
TABLE 3 PROXYSG S400 APPLIANCE CONFIGURATIONS.....9
TABLE 4 FIPS 140-2 LOGICAL INTERFACE MAPPINGS FOR THE FRONT OF THE PROXYSG S400.....11
TABLE 5 FRONT PANEL LED STATUS INDICATIONS FOR THE PROXYSG S400.....11
TABLE 6 FIPS 140-2 LOGICAL INTERFACE MAPPINGS FOR THE REAR OF THE PROXYSG S400.....12
TABLE 7 REAR PANEL LED STATUS INDICATIONS FOR THE PROXYSG S400.....12
TABLE 8 FIPS AND PROXYSG ROLES.....13
TABLE 9 CRYPTO OFFICER ROLE SERVICES AND CSP ACCESS.....16
TABLE 10 USER SERVICES AND CSP ACCESS.....17
TABLE 11 AUTHENTICATION MECHANISMS USED BY THE MODULE.....19
TABLE 12 FIPS-APPROVED ALGORITHM IMPLEMENTATIONS.....21
TABLE 13 LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS.....23
TABLE 14 RS-232 PARAMETERS.....35
TABLE 15 ACRONYMS.....41

1. Introduction

1.1 Purpose

This is a *Non-Proprietary Cryptographic Module Security Policy* for the ProxySG S400 Appliance (Models: ProxySG S400-20, ProxySG S400-30, ProxySG S400-40; Firmware Version: 6.5.2.9 build 144008)) from Blue Coat Systems, Inc. This *Non-Proprietary Security Policy* describes how the ProxySG S400 Appliance meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment 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 2 FIPS 140-2 validation of the module. The ProxySG S400 Appliance is referred to in this document as: ProxySG S400-20, ProxySG S400-30, ProxySG S400-40, ProxySG S400, 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
- *Submission Summary* document
- Other supporting documentation as additional references

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

2. ProxySG S400

2.1 Overview

The foundation of Blue Coat's application delivery infrastructure, Blue Coat ProxySG appliances establish points of control that accelerate and secure business applications for users across the distributed organization. Blue Coat appliances serve as an Internet proxy and wide area network (WAN) optimizer. The purpose of the appliances is to provide a layer of security between an Internal and External Network (typically an office network and the Internet), and to provide acceleration and compression of transmitted data.

As the world's leading proxy appliance, the Blue Coat ProxySG is a powerful yet flexible tool for improving both application performance and security, removing the need for compromise:

- **Performance**: Blue Coat's patented "MACH5" acceleration technology combines five different capabilities onto one box. Together, they optimize application performance and help ensure delivery of critical applications. User and application fluent, MACH5 improves the user experience no matter where the application is located, internally or externally on the Internet.
- **Security**: Blue Coat's industry leading security architecture addresses a wide range of requirements, including filtering Web content, preventing spyware and other malicious mobile code, scanning for viruses, inspecting encrypted Secure Sockets Layer (SSL) traffic, and controlling instant messaging (IM), Voice-over-IP (VoIP), peer-to-peer (P2P), and streaming traffic.
- **Control**: Blue Coat's patented Policy Processing Engine empowers administrators to make intelligent decisions. Using a wide range of attributes such as user, application, content and others, organizations can effectively align security and performance policies with corporate priorities.

See Figure 1, Typical Deployment of a ProxySG Appliance, next, for a typical deployment scenario for ProxySG appliances.

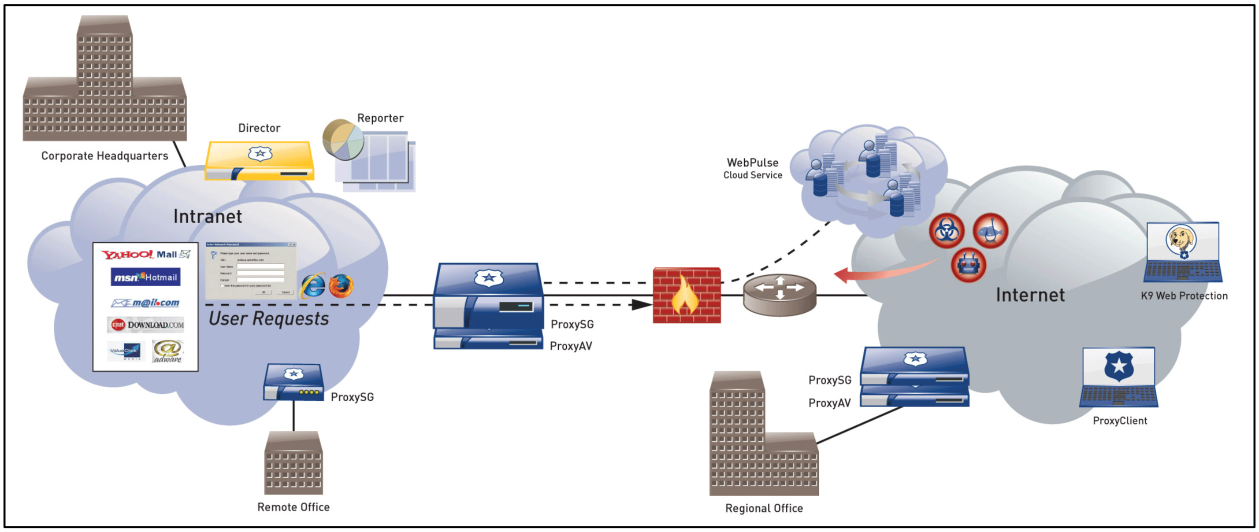


Figure 1 Typical Deployment of a ProxySG Appliance

The security provided by the ProxySG can be used to control, protect, and monitor the Internal Network's use of controlled protocols on the External Network. The ProxySG appliances offer a choice of two editions" via licensing: MACH5 and Proxy. The controlled protocols implemented in the tested configurations are:

Table 1 MACH5 vs. Proxy Edition Capability Differences

Capability	Licensing Edition	
	MACH5	Proxy
Common Internet File System (CIFS) Acceleration	Yes	Yes
Windows Media Optimization (Microsoft Media Streaming (MMS)	Yes	Yes
Microsoft Smooth Streaming Optimization	Yes	Yes
Real Media Optimization	Yes	Yes
Real-Time Streaming Protocol (RTSP) Optimization	Yes	Yes
Real-Time Messaging Protocol (RTMP) Optimization	Yes	Yes
QuickTime Optimization (Apple HTTP Live Streaming)	Yes	Yes
Adobe Flash Optimization (Adobe HTTP Dynamic Streaming)	Optional	Optional
Bandwidth Management	Yes	Yes
DNS proxy	Yes	Yes
Advanced DNS Access Policy	No	Yes
Hypertext Transfer Protocol (HTTP)/ Secure Hypertext Transfer Protocol (HTTPS) Acceleration	Yes	Yes
File Transfer Protocol (FTP) Acceleration	Yes	Yes
Secure Sockets Layer (SSL) Acceleration	Yes	Yes
IMAP[1] Acceleration	Yes	Yes
TCP[2] tunneling protocols (Secure Shell (SSH))	Yes	Yes
POP[3] Acceleration	Yes	Yes
SMTP[4] Acceleration	Yes	Yes
Messaging Application Programming Interface (MAPI) Acceleration	Yes	Yes
Secure Shell	Yes	Yes
Telnet Proxy	Yes	Yes

[1] IMAP – Internet Message Access Protocol

[2] TCP – Transmission Control Protocol

[3] POP3 – Post Office Protocol version 3

[4] SMTP – Simple Mail Transfer Protocol

Capability	Licensing Edition	
	MACH5	Proxy
ICAP Services	No	Yes
Netegrity SiteMinder	No	Yes
Oblix COREid	No	Yes
Peer-To-Peer	No	Yes
User Authentication[5]	Yes	Yes
Onbox Content Filtering (3rd Party or BCWF[6])	No	Yes
Offbox Content Filtering (e.g. Websense)	No	Yes
Instant Messaging (AOL[7], Yahoo, MSN[8])	No	Yes
SOCKS[9]	No	Yes
SSL Termination/Proxy	Yes	Yes

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. In addition, the ProxySG provides optimization of data transfer between ProxySG nodes on a WAN using its Application Delivery Network (ADN) technology. Optimization is achieved by enforcing a configurable policy on traffic traversing the WAN. Additionally, the ProxySG offers network traffic acceleration by using the AES-NI feature[10] of the Intel processor.

The ProxySG S400 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	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	Electromagnetic Interference/Electromagnetic Compatibility	2

[5] User authentication on MACH5 to identify a proxy user is supported when forwarding to the Blue Coat Cloud Service for policy enforcement.
[6] BCWF – Blue Coat Web Filter
[7] AOL – America Online
[8] MSN – The Microsoft Network
[9] SOCKS – SOCKet Secure
[10] The AES-NI feature is always enabled.

Section	Section Title	Level
9	Self-tests	2
10	Design Assurance	2
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 Blue Coat appliance configurations:

Table 3 ProxySG S400 Appliance Configurations

Appliance Type	Hardware Version	SKU / Short Description
Cold Standby Appliance	080-03568	SG-S400-20-CS
	080-03572	SG-S400-30-CS
	080-03576	SG-S400-40-CS
Try-And-Buy Appliance MACH5 Edition	080-03570	TAB-SG-S400-20-M5
	080-03574	TAB-SG-S400-30-M5
	080-03578	TAB-SG-S400-40-M5
Hardware Appliance MACH5 Edition	090-03075	SG-S400-20-M5
	090-03079	SG-S400-30-M5
	090-03083	SG-S400-40-M5
Try-And-Buy Appliance Proxy Edition	080-03571	TAB-SG-S400-20-PR
	080-03575	TAB-SG-S400-30-PR
	080-03579	TAB-SG-S400-40-PR
Hardware Appliance Proxy Edition	090-03076	SG-S400-20-PR
	090-03080	SG-S400-30-PR
	090-03084	SG-S400-40-PR

The hardware version numbers in Table 3 above represent licensing options available. All appliance types and editions run on the exact same hardware and firmware, and are exactly the same from a cryptographic functionality and boundary perspective. Table 1 provides a mapping between the capabilities and the licensing edition.

Each appliance type in Table 3 above has the exact same hardware, and can be licensed to run either the MACH5 or Proxy edition of SGOS. A hardware appliance is an SG-S400-20, SG-S400-30, or SG-S400-40 that comes pre-configured with either the Proxy edition or MACH5 edition of SGOS. A Try-And-Buy appliance varies only in that the license for either the MACH5 or Proxy edition that is provided with the appliance is valid for 30 days, after which the full license must be purchased or the hardware appliance must be returned to Blue Coat. A Cold Standby appliance varies only in that neither edition is pre-installed; the customer may choose to install either a Proxy or MACH5 edition license. The hardware for all three types of appliances is the same. The Crypto Officer and User services of the module are identical for all appliance types running either the MACH5 or Proxy edition.

Each edition of SGOS runs on the exact same hardware and firmware and is exactly the same from a cryptographic functionality and boundary perspective. The MACH5 and Proxy editions vary in only data processing capabilities. The Crypto Officer and User services of the module are identical for both licensing editions.

The ProxySG S400 offers an affordable rack-mountable appliance solution for small enterprises and branch offices that have direct access to the Internet.

The front panel, as shown in Figure 2 below, has 1 Liquid Crystal Display (LCD), two Light Emitting Diodes (LEDs), and 6 control buttons (NOTE: the front panel control buttons are disabled when configured for Approved mode of operation). Connection ports are at the rear, as shown in Figure 3.

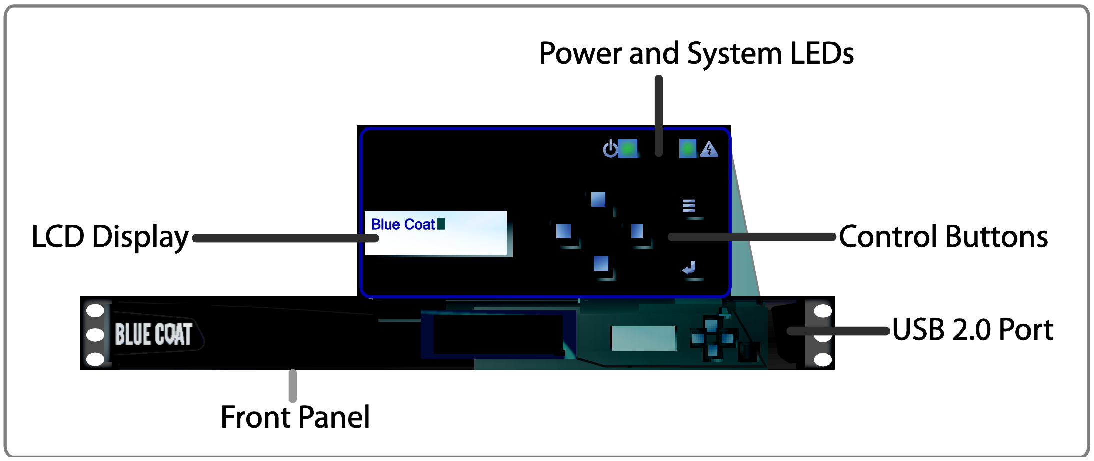


Figure 2 ProxySG S400 (Front View)

For the FIPS 140-2 validation, the module was tested on the following Blue Coat appliance configurations:

- ProxySG S400-20
- ProxySG S400-30
- ProxySG S400-40

The ProxySG S400 is a module with a multi-chip standalone embodiment. The overall security level of the module is 2. The cryptographic boundary of the ProxySG S400 is defined by the appliance chassis, which surrounds all the hardware and firmware. The module firmware, version 6.5.2.9 build 144008, contains the following cryptographic libraries:

- SGOS Cryptographic Library version 3.1.4.
- SGOS UEFI OS Loader version 3.15
- SGOS TLS Library version 3.1.5
- SGOS SSH Library version 6.3_1

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

The front panel of the ProxySG SG400 (as shown in Figure 2) has an LCD interface, two LEDs, and six control buttons. The control buttons on the front panel are disabled once the module is configured for its Approved mode of operation.

The type and quantity of all ports present in the front panel of the ProxySG S400 are given in Table 4.

Table 4 FIPS 140-2 Logical Interface Mappings for the front of the ProxySG S400

Physical Port/Interface	Quantity	FIPS 140-2 Interface
LEDs	2	Status Output
LCD	1	Status Output
USB 2.0 port	1	N/A (port is disabled)

The status indications provided by the LEDs on the ProxySG S400 is described in Table 5.

Table 5 Front Panel LED Status Indications for the ProxySG S400

LED	Color	Definition
Power LED	OFF	The ProxySG is powered off.
	AMBER	The appliance is booting and the OS load is not yet complete.
	FLASHING GREEN TO AMBER	The OS has been loaded but has not been configured.
	GREEN	The OS has loaded and is properly configured.
System LED	OFF	The appliance has not determined the system status.
	GREEN	Healthy.
	AMBER	Warning.
	FLASHING AMBER	Critical Warning.

The rear of the ProxySG S400 is shown in Figure 3.

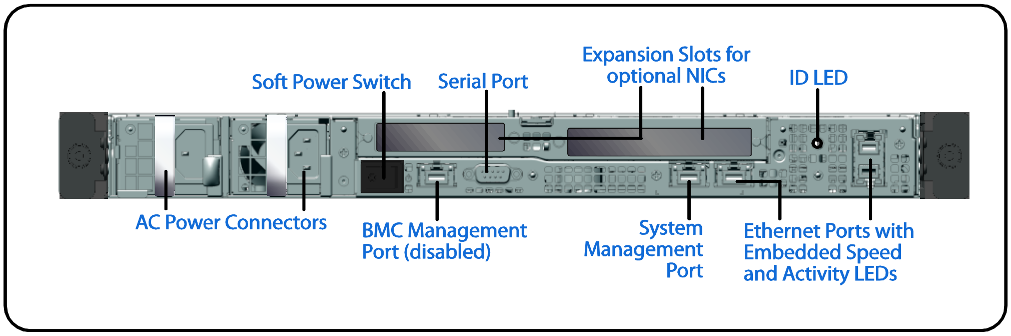

Soft Power Switch
Serial Port
Expansion Slots for optional NICs
ID LED
AC Power Connectors
BMC Management Port (disabled)
System Management Port
Ethernet Ports with Embedded Speed and Activity LEDs

Figure 3 Connection Ports at the Rear of the ProxySG S400

The rear side of the ProxySG S400 (shown in Figure 3) contains all the connecting ports. Those ports are:

- Two AC power connectors

- A serial port to connect to a Personal Computer (PC) for management
- (2) Dual port, bypass-capable 10/100/1000 Base T Ethernet adapter ports
- One onboard, non-bypass 10/100/1000 Base T Ethernet adapter port for system management[11]
- One onboard, non-bypass 10/100/1000 Base T Ethernet adapter port
- One onboard 10/100 Base T BMC management port (disabled/for internal use only)
- Two expansion slots[12]

The type and quantity of all ports present in rear panel of the ProxySG SG400 are given in Table 6.

Table 6 FIPS 140-2 Logical Interface Mappings for the Rear of the ProxySG S400

Physical Port/Interface	Quantity	FIPS 140-2 Interface
Ethernet ports	3	Data Input Data Output Control Input Status Output
System management port[13]	1	Data Input Data Output Control Input Status Output
BMC management port	1	N/A (port is disabled)
Serial port	1	Control Input Status Output
Ethernet Interface – Speed LEDs	4	Status Output
Ethernet Interface – Activity LEDs	4	Status Output
AC power	2	Power Input
Soft power Switch	1	Control Input

The status indications provided by the LEDs on the rear of the ProxySG S400are described in Table 7.

Table 7 Rear Panel LED Status Indications for the ProxySG S400

LED	Color	Definition
AC power connection LED	OFF	The ProxySG is not receiving power.
	GREEN	The ProxySG is receiving power.
Ethernet Interface – Activity LEDs	OFF	No link is present.
	GREEN	Link is present.
	FLASHING GREEN	Link activity.

[11] The port can be used to access all functionality provided by the module. However, it is the preferred port for management.
[12] Optional NICs are not included in the validation.
[13] The port can be used to access all functionality provided by the module. However, it is the preferred port for management.

LED	Color	Definition
Ethernet Interface – Speed LEDs	OFF	10 Mbps speed connection is present.
	GREEN	100 Mbps speed connection is present.
	AMBER	1000 Mbps speed connection is present.
ID LED	OFF	Not supported in SGOS.

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 11. The modules offer two management interfaces:

- **CLI**: Accessible locally via the serial port (provides access to the Setup Console portion of the CLI which requires the additional "Setup" password to gain access) or remotely using SSH. This interface is used for management of the modules. This interface must be accessed locally via the serial port to perform the initial module configurations (IP address, DNS server, gateway, and subnet mask) and placing the modules into the Approved mode. When the module has been properly configured, this interface can be accessed via SSH. Management of the module may take place via SSH or locally via the serial port. Authentication is required before any functionality will be available through the CLI.
- **Management Console**: 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 ProxySG. 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 8.

Table 8 FIPS and ProxySG Roles

FIPS Roles	ProxySG Roles and Privileges
CO	• The CO is an administrator of the module that has been granted "enabled" mode access while using the CLI and "read/write" access while using the Management Console. • When the CO is using the CLI, and while in the "enabled" mode of operation, COs may put the module in its Approved mode, reset to the factory state (local serial port only) and query if the module is in Approved mode. In addition, COs may do all the services available to Users while not in "enabled" mode.

FIPS Roles	ProxySG Roles and Privileges
	• 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 must be generated by an external application as the module is not capable of generating the keys internally. The 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 must be generated by an external application as the module is not capable of generating the keys internally. The 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 9 and Descriptions of the FIPS 140-2 relevant services available to the User role are provided in the table below. Additional services that do not access CSPs can be found in the *Blue Coat Systems SGOS Administration Guide, Version 6.5.2.x,* and in the *Blue Coat Systems ProxySG Appliance Command Line Interface Reference, Version SGOS 6.5, Release SGOS 6.5.2.*

Table 10 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**: CSP is read
- **W**: 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 the table below. Additional services that do not access CSPs can be found in the *Blue Coat Systems SGOS Administration Guide, Version 6.5.2.x*, and in the *Blue Coat Systems ProxySG Appliance Command Line Interface Reference, Version SGOS 6.5, Release SGOS 6.5.2*.

Table 9 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 3.2.1 in this *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 serial port)	MAK: W SSH Session Key: W SSH Authentication Key: W TLS Session Key: W TLS Authentication Key: W
** Firmware Load	Loads new external firmware 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

Service	Description	CSP and Access Required
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
** 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 serial port). 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 FIPS 140-2 relevant services available to the User role are provided in the table below. Additional services that do not access CSPs can be found in the *Blue Coat Systems SGOS Administration Guide, Version 6.5.2.x*, and in the *Blue Coat Systems ProxySG Appliance Command Line Interface Reference, Version SGOS 6.5, Release SGOS 6.5.2*.

Table 10 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

Service	Description	CSP and Access Required
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
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 Authentication Mechanism

The module supports role-based authentication. COs and Users must authenticate using a user ID and password, SSH client key (SSH only), or certificates associated with the correct protocol in order to set up the secure session. Secure sessions that authenticate Users have no interface available to access other services (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 session remains active until the operator logs out or inactivity for a configurable amount of time has elapsed.

Modules used by the United States Department of Defense (DoD) must meet Homeland Security Presidential Directive (HSPD)-12 requirements regarding the use of FIPS 201 validated Common Access Card (CAC) authentication for COs and Users connecting to management functionality of the module. Additionally, other agencies may require FIPS 201 validated PIV[14] II card authentication.

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

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

1. On the management workstation the CO or User opens a browser and establishes a clear-text HTTP connection with the module.
2. Using CPL similar to the VPM `NotifyUser` action, the CO or User is presented with a DoD warning banner which they must positively acknowledge and accept.

[14] PIV – Personal Identity Verification II

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 11.

Table 11 Authentication Mechanisms Used by the Module

Role	Type of Authentication	Authentication Strength
Crypto-Officer	Password	The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at minimum 8 characters in length, and at maximum 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1: (95^8), or 1: 6,634,204,312,890,625 chance of false acceptance. The Crypto-Officer may connect locally using the serial port or remotely after establishing a TLS or SSH session.

Role	Type of Authentication	Authentication Strength
	Password (“Enabled” Mode)	The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1: (95^8), or 1: 6,634,204,312,890,625 chance of false acceptance. This password is entered by the Crypto-Officer to enter the “enabled” mode; this is entered locally through the serial port or remotely after establishing an SSH session.
	Password (“Setup”)	The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at least 4 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). A 4-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1: (95^4), or 1: 81,450,625 chance of false acceptance. This password is entered by the Crypto-Officer and is required when using the serial port to access the Setup Console portion of the CLI.
	Public keys	The module supports using RSA keys for authentication of Crypto-Officers during TLS (when CAC authentication is configured with a local Certificate Realm) or SSH. Using conservative estimates and equating a 2048-bit RSA key to a 112-bit symmetric key, the probability for a random attempt to succeed is $1:2^{112}$ or $1: 5.19 \times 10^{33}$.
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 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 $1: 5.19 \times 10^{33}$.

2.5 Physical Security

The ProxySG S400 Appliance is a multi-chip standalone cryptographic module and is enclosed in a hard, opaque metal case that completely encloses all of its internal components. There are only a limited set of vent holes provided in the case, and these holes obscure the view of the internal components of the module. Tamper-evident labels are applied to the case to provide physical evidence of attempts to remove the case of the module. The Crypto-Officer is responsible for the placement of tamper-evident labels and baffles and guidance can be found in Section 3.1.1.2. The labels and baffles are part of the FIPS Security Kit (Part Number: 085-02891; HW-KIT-FIPS-400).

All of the module's components are production grade. The ProxySG was tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2.6 Non-Modifiable Operational Environment

The operational environment requirements do not apply to the ProxySG S400 Appliance. The module does not provide a general purpose operating system nor does it allow operators the ability to load untrusted firmware. The operating system run by the cryptographic module is referred to as Secure Gateway Operating System (SGOS). SGOS is a proprietary real-time embedded operating system.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 12 below.

Table 12 FIPS-Approved Algorithm Implementations

Algorithm	Crypto Library version 3.1.4 Implementation Certificate Number	UEFI OS Loader version 3.15 Implementation Certificate Number	TLS Library version 3.1.5 Implementation Certificate Number	SSH Library Version 6.3_1 Implementation Certificiate Number
Symmetric Key Algorithms				
AES: ECB[15], CBC[16], OFB[17], CFB-128[18] bit mode for 128-, 192-, and 256-bit key sizes	2931	N/A	N/A	N/A
Triple-DES[19]: ECB, CBC, CFB-64, OFB mode for keying option 1 (3 different keys)	1744	N/A	N/A	N/A
Asymmetric Key Algorithms				
RSA (ANSI X9.31) Key Generation – 2048, 3072, 4096-bit	1536	N/A	N/A	N/A

[15] ECB – Electronic Codebook
[16] CBC – Cipher Block Chaining
[17] OFB – Output Feedback
[18] CFB – Cipher Feedback
[19] Triple-DES – Triple Data Encryption Standard

Algorithm	Crypto Library version 3.1.4 Implementation Certificate Number	UEFI OS Loader version 3.15 Implementation Certificate Number	TLS Library version 3.1.5 Implementation Certificate Number	SSH Library Version 6.3_1 Implementation Certificate Number
RSA PKCS #1[20] signature generation – 2048, 3072, and 4096-bit RSA PKCS#1 signature verification – 1024, 1536, 2048, 3072, and 4096-bit	1536	N/A	N/A	N/A
Hashing Functions				
SHA-1[21]	2467	2291	N/A	N/A
SHA-224, SHA-256, SHA-384, SHA-512	2467	N/A	N/A	N/A
Message Authentication Code (MAC) Functions				
HMAC[22] with SHA-1	1857	1700	N/A	N/A
HMAC with SHA-224, SHA-256, SHA-384, SHA-512	1857	N/A	N/A	N/A
Deterministic Random Bit Generator (DRBG)				
SP 800-90[23] CTR_DRBG (AES-256)	541	N/A	N/A	N/A
Key Derivation Function (KDF)				
TLS KDF	N/A	N/A	332	N/A
SSH KDF	N/A	N/A	N/A	181

***NOTE**: As of December 31, 2013, 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. RSA Signature Verfication using 1536-bits is present only in the firmware implementation*

The TLS, SSH, and SNMP protocols have 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.
- MD5 used during TLS sessions
- Diffie-Hellman for key agreement during TLS and SSH: 2048-bit keys (provides 112 bits of security).
- Non-Deterministic RNG (NDRNG) for seeding the pseudo RNG (PRNG)
- PRNG for seeding the FIPS-Approved DRBG (SP 800-90 CTR_DRBG)

[20] PKCS – Public Key Cryptography Standard
[21] SHA – Secure Hash Algorithm
[22] HMAC – Hash-Based Message Authentication Code
[23] SP – Special Publication

The module supports the CSPs listed below in Table 13.

Table 13 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	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[24] 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

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

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
	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 Imported in plaintext via a directly attached cable to the serial port	Exits in encrypted format when performing a module configuration backup	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing encrypting MAK	Negotiating TLS or SSH sessions
DH public key	2048-bits	Module's public key is internally generated via FIPS-Approved DRBG Public key of a peer enters the module in plaintext	The module's Public key exits the module in plaintext	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
DH private key	224-bits	Internally generated via FIPS-Approved DRBG	Never exits the module	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Negotiating TLS or SSH sessions
TLS or SSH Session Key	AES CBC 128-, or 256-bit key Triple-DES CBC keying option 1 (3 different keys)	Internally generated via FIPS-Approved DRBG	Output in encrypted form during TLS or SSH protocol handshake	Stored in plaintext on volatile memory	Rebooting the modules Removing power	Encrypting TLS or SSH data
TLS or SSH Session Authentication Key	HMAC SHA-1 key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Rebooting the modules Removing power	Data authentication for TLS or SSH sessions
Crypto-Officer Password User Password	Minimum of eight (8) and maximum of 64 bytes long printable character string	Externally generated. Enters the module in encrypted form via a secure TLS or SSH session Enters the module in plaintext via a directly attached cable to the serial port	Exits in encrypted form via a secure TLS session for external authentication Exits in encrypted format when performing a module configuration backup	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting MAK	Locally authenticating a CO or User for Management Console or CLI

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
"Enabled" mode password	Minimum of eight (8) and maximum of 64 bytes long printable character string	Enters the module in encrypted form via a secure SSH session Enters the module in plaintext via a directly attached cable to the serial port	Exits in encrypted form via a secure TLS session for external authentication Exits in encrypted format when performing a module configuration backup	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting MAK	Used by the CO to enter the "privileged" or "enabled" mode when using the CLI
"Setup" Password	Minimum of four (4) and maximum of 64 bytes long printable character string	Enters the module in plaintext via a directly attached cable to the serial port	Never exits the module	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting MAK	Used by the CO to secure access to the CLI when accessed over the serial port
SNMP Privacy Key	AES CFB 128 -bit key	Externally generated, Imported in encrypted form via a secure TLS or SSH session Imported in plaintext via a directly attached cable to the serial port	Exits the module encrypted over TLS or encrypted during a configuration backup	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting MAK Can be deleted by command	Encrypting SNMPv3 packets

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SNMP Authentication Key	HMAC-SHA-1-96 –bit key	Externally generated, Imported in encrypted form via a secure TLS or SSH session Imported in plaintext via a directly attached cable to the serial port	Exits the module encrypted over TLS or encrypted during a configuration backup	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting MAK Can be deleted by command	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 Removing power	Seeding material for the SP800-90A CTR_DRBG
SP 800-90A CTR_DRBG Entropy[25]	256-bit random number with derivation function 384-bit random number without derivation function	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules Removing power	Entropy material for the SP800-90A CTR_DRBG
SP 800-90A CTR_DRBG key value	Internal state value	Internally generated	Never	Plaintext in volatile memory	Rebooting the modules Removing power	Used for the SP 800-90A CTR_DRBG
SP 800-90A CTR_DRBG V value	Internal state value	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules Removing power	Used for the SP 800-90A CTR_DRBG

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

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

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 CO must choose a key strength that is greater than or equal to the strength of the key being encrypted.

2.8 Self-Tests

If any of the firmware self-tests fail, an error is printed to the CLI (when being accessed via the serial port). 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 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 ProxySG S400 Appliance performs the following self-tests using the UEFI OS Loader:

- Firmware integrity check using an HMAC-SHA1 (32-bit CRC)

The ProxySG SG-S400 Appliance performs the following self-tests using the OpenSSL Cryptographic Library firmware implementation at power-up:

- Known Answer Tests (KATs)
  - AES encrypt KAT
  - AES decrypt KAT
  - Triple-DES encrypt KAT
  - Triple-DES 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 ProxySG S400 performs the conditional self-tests in only on its firmware implementation of OpenSSL Cryptographic Library.

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

2.8.3 Critical Function Tests

The ProxySG S400 implements the SP800-90A 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
- 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 2 requirements for this validation.

3. Secure Operation

The ProxySG SG-S400 Appliance meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

3.1 Initial Setup

Before powering-up the module, the CO must ensure that the required tamper-evident labels (included in the FIPS security kit) are correctly applied to the enclosure. The FIPS security kit (Part Number: 085-02891; HW-FIPS-KIT-400) consists of the following items as shown below in Figure 4 FIPS Security Kit Contents .

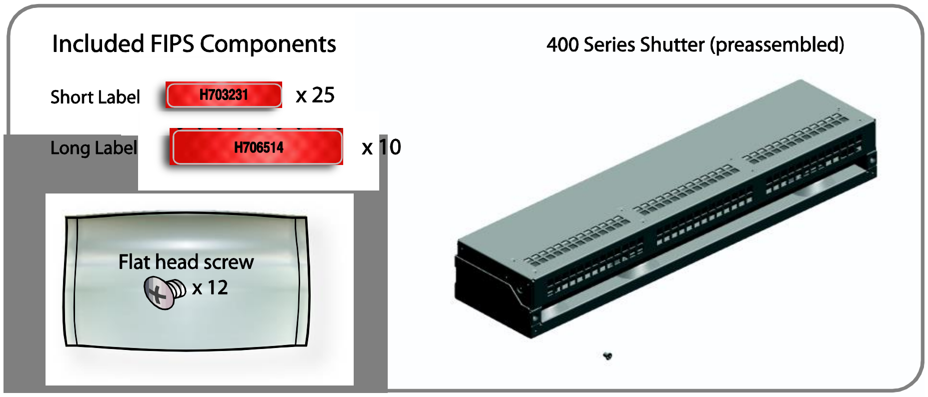


Figure 4 FIPS Security Kit Contents

FIPS Security Kits may include either red or blue labels.

Note: There are (25) 'Short Labels' and (10) 'Long labels' included with the FIPS kit; however, only (5) short labels and (2) long labels are required for FIPS compliance. Additional labels are provided for reapplication purposes.

3.1.1 Label and Baffle Installation Instructions

The Crypto-Officer is responsible for installing the baffle (security panel) and applying the tamper-evident labels at the client's deployment site to ensure full FIPS 140-2 compliance. Once the seals have been applied, the Crypto Officer must develop an inspection schedule to verify that the external enclosure of the module and the tamper seals have not been damaged or tampered with in any way. The Crypto-Officer is responsible for securing and having control at all times of any unused labels. The Crypto-Officer is responsible for the direct control and observation of any changes to the module such as reconfigurations where the tamper-evident labels or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

Crypto-Officers must adhere to the following when applying the tamper-evident labels:

- The minimum temperature of the environment must be 35-degrees Fahrenheit. After application, the labels' acceptable temperature in the operational environment is -5-degrees to 158-degrees Fahrenheit.

- Do not touch the adhesive side of the label. This disrupts the integrity of the adhesive. If a label is removed from a surface, the image is destroyed and the label shows tamper-evident text as evidence. If you accidently touch the adhesive side, discard that label and apply another one.

Label application tips:

- Apply skin moisturizer on your fingers before handling.
- Use a rubber fingertip to partially remove the label from its backing.
- After applying the labels, allow at least 24 hours for the label adhesive to cure.

3.1.1.1 Shutter Installation

The two piece rear shutter (400 Series Shutter as shown in Figure 4 FIPS Security Kit Contents) is designed to prevent unauthorized access to key system components by shielding the rear ventilation outlets, option cards, interfaces, and the soft power switch.

1. Remove the top shutter from the bottom shutter by removing two (2) screws and pulling directly rearward. Set the top shutter aside in a safe location.

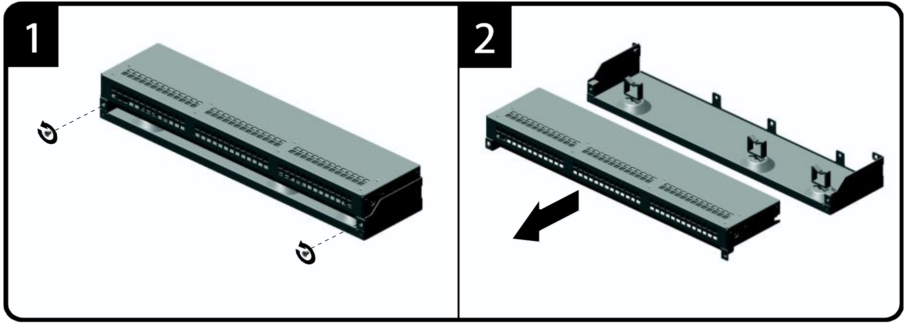


Figure 5 Shutter Disassembly

2. Align the bottom shutter mounting points against the screw locations and the alignment pins on the chassis and secure with three (3) flat-head screws. Be aware the FIPS kit includes (7) additional screws, in case some are misplaced or lost during installation.

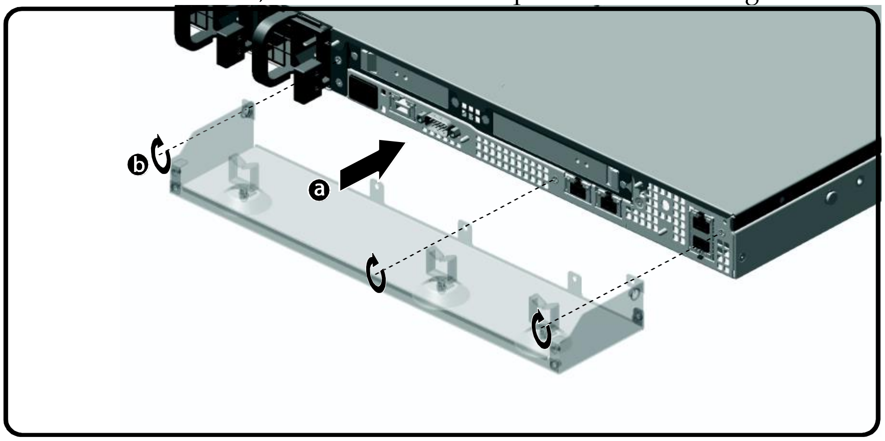


Figure 6 Lower Shutter Installation

3. Rack mount the appliance. Refer to the 400 Series Maintenance and Upgrade Guide for instructions and safety information on rack-mounting the appliance.

4. Reinstall the appliance network and other interconnect cables to their respective locations.

   Note: All network and interconnect cables must be installed at this time to prevent reopening of the shutters and subsequent reapplication of the security labels.

5. Route the network cables through the cable management anchors to prevent cables from obstructing airflow.

6. Install the top shutter by aligning the notches with the raised pins on the appliance and secure with two (2) flat-head screws. Be aware the FIPS kit includes (7) additional screws, in case some are misplaced or lost during installation.

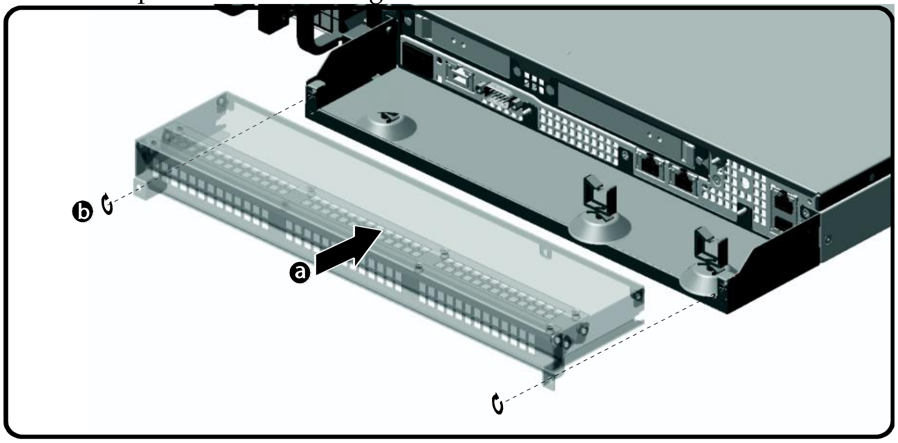


Figure 7 Upper Shutter Installation

3.1.1.2 Label Application

The FIPS compliant labels are applied over key areas of the chassis to provide tamper-evident security. If the labels are removed after being affixed to a surface, the image self-destructs and leaves a pattern of VOID markings on the label. The image below illustrates the tamper-evident features of the label. Figure 8 below illustrates the tamper-evident features of the label.

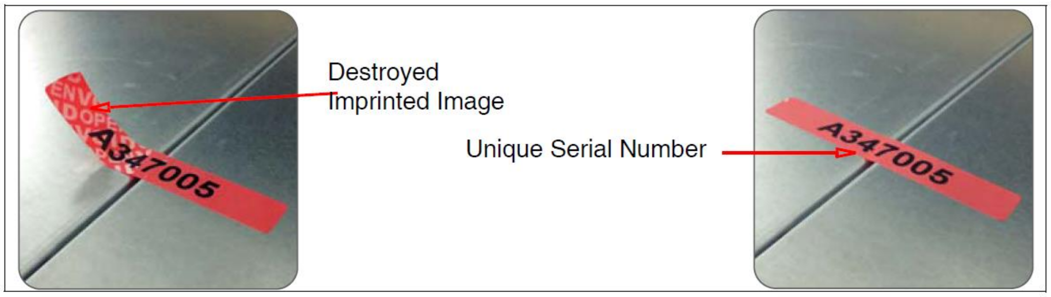
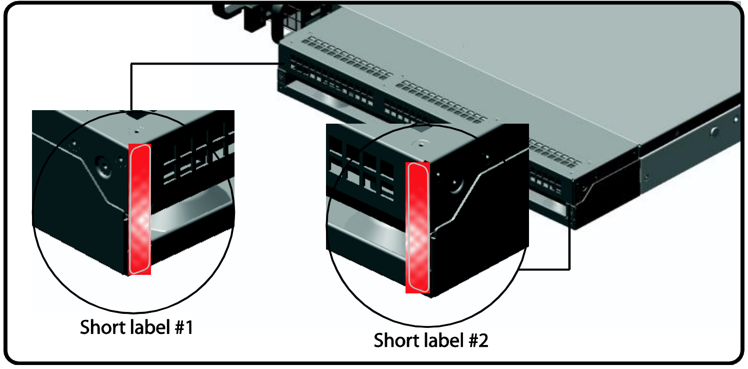


Figure 8 Label Showing Tamper Evidence

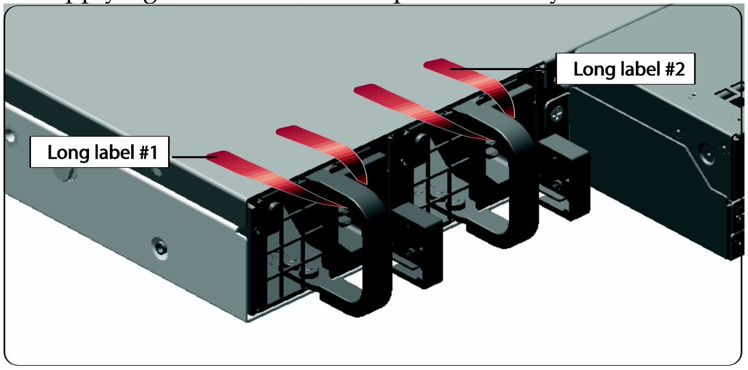
Use alcohol swabs to clean the label location surface using Isopropyl Alcohol (99%); this ensures complete adhesion. Verify that all the surfaces are dry before applying the labels.

1. Set the appliance on a flat, slip-proof work space and make sure you have access to all sides of the appliance.

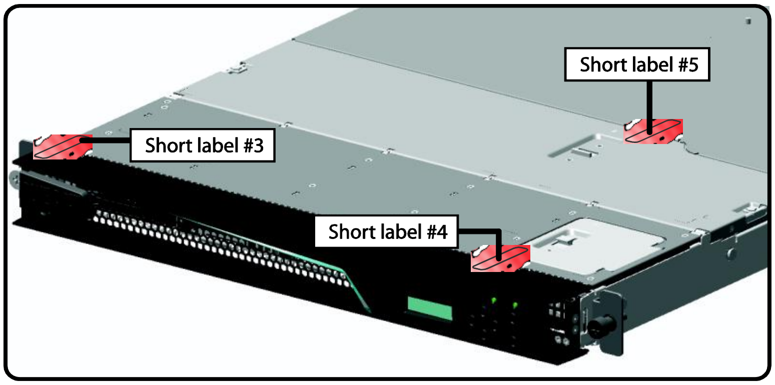
2. Apply two (2) short labels (short labels 1 and 2) over the exposed shutter screw heads. These labels extend slightly over the left and right edges of the shutter when properly applied.



3. Apply one (1) long label through each power supply unit (long labels 1 and 2) and/or dummy cover in a U-shape, making sure to route the label through the handle and to apply the ends of the label on the chassis top and bottom, as illustrated below. When applying the labels in, make sure there is enough material on both ends to properly secure the power supply. When you are applying these labels, it is imperative that you do no cover any of the vent holes.



4. Apply two (2) short labels (short labels 3 and 4) over the opposite ends of the bezel and one (1) short label (short label 5) over the center cover panel curvature to prevent unauthorized access to the system components. Each label should be placed on the opposite ends of the appliance, as shown below



Note: The chassis-center cover labels are destroyed each time the center cover is opened. Be sure to re-secure the appliance after servicing!

5. Power-on the appliance by plugging in the power cords.

3.2 Secure Management

3.2.1 Initialization

The module is delivered in an uninitialized factory state, and requires minimal first-time configuration to operate in FIPS-Approved mode and be accessed by a web browser. Physical access to the module shall be limited to the Crypto-Officer (CO), and the CO shall be responsible for putting the module into the Approved mode.

The process of establishing the initial configuration via a secure serial port is described below.

1. Connect a serial cable to a PC and to the module's serial port. Open a terminal emulator (such as HyperTerminal) on the PC, and connect to the serial port to which you attached the cable. Create and name a new connection (either a COM or TCP/IP), using the port parameters provided in Table 14.

Table 14 RS-232 Parameters

RS-232C Parameter	Parameter Setting
Baud rate	9600 bps
Data bits	8
Parity	None
Stop bits	1
Flow control	None

2. Power up the module and wait for the system to finish booting.
3. Press **Enter** three times.

   When the system displays `Welcome to the SG Appliance Setup Console`, it is ready for the first-time network configuration.
4. Enter the properties for the following:
   a. Interface number
   b. IP address
   c. IP subnet mask
   d. IP gateway
   e. DNS server parameters
   f. Username and password.
5. When the system displays `Successful Configuration Setup,` press **Enter** to confirm the configuration.
6. Press **Enter** three times.
7. Select option #1 for the Command Line Interface.

8. Type **enable** and press **Enter**.
9. Enter the enable mode password.
10. Type the command **# show installed-systems** to check the attributes of the current image. You will see output similar to the following:

```
10.168.100.32 - Blue Coat SG-S400 Series#show installed-systems
ProxySG Appliance Systems
1. Version: SGOS 6.5.2.1, Release ID: 144008
   Friday June 13 2014 02:54:25 UTC,
   Attributes: Locked, FIPS capable
   Boot Status: Last boot succeeded, Last Successful Boot: Tuesday June 3
2014 15:05:41 UTC
   Disk Layout: Compatible
2. Version: N/A, Release ID: N/A ( EMPTY )
   No Timestamp,
   Attributes: None
   Boot Status: Unknown, Last Successful Boot: Unknown
   Disk Layout: Unknown
3. Version: N/A, Release ID: N/A ( EMPTY )
   No Timestamp,
   Attributes: None
   Boot Status: Unknown, Last Successful Boot: Unknown
   Disk Layout: Unknown
4. Version: N/A, Release ID: N/A ( EMPTY )
   No Timestamp,
   Attributes: None
   Boot Status: Unknown, Last Successful Boot: Unknown
   Disk Layout: Unknown
5. Version: N/A, Release ID: N/A ( EMPTY )
   No Timestamp,
   Attributes: None
   Boot Status: Unknown, Last Successful Boot: Unknown
   Disk Layout: Unknown
Default system to run on next hardware restart: 1
Default replacement being used. (oldest unlocked system)
Current running system: 1
Enforce signed: Disabled.
```

11. If the `Attribute` is not set to `Signed`, as seen in the example above, you must download the signed image from BTO, then install and upgrade to the image. These steps are described in steps 12 through 28. If the `Attribute` is set to `Signed`, go directly to step 29.
12. Login to your BTO account from a PC. Click the **Downloads** tab.
13. In the **Download Central Home** page, select the product **ProxySG**.
14. Select the appropriate product model of the ProxySG, SG-S400, in the **My Entitled Products** pane.
15. In the **My Product Models** page, select the HW configuration that matches the ProxySG model being initialized: SG-S400-20, SG-S400-30, or SG-S400-40.
16. Select version 6.5.2.9.
17. Accept the software terms and conditions.
18. In the **Product Download** page, select the signed image ProxySG_6.5.2.9_144008_x64.bcsi.
19. Save the image file to the PC desktop.
20. Copy the image file to a trusted webserver accessible by the ProxySG. The webserver must be configured to use the TLS protocol.
21. Using the serial console, access the appliance CLI.
22. Enter the following command:

    # config terminal
23. Specify the network path of the signed image on the web server by entering the following command:

    # upgrade-path <*url*>
24. Enter the following command to download the signed image to the ProxySG:

    # load upgrade
25. After the download has completed, enter the following command to reboot using the new image:

    # restart upgrade
26. Monitor the serial console and wait for the system to finish booting.
27. Press **Enter** three times.

    When the system displays the `Welcome to the SG Appliance Setup Console` prompt, the system is ready for the first-time FIPS initialization.
28. Select option #1 for the Command Line Interface. This option takes you immediately to the Admin prompt.
29. Type **enable** and press **Enter**.
30. Enter the enable mode password.
31. Repeat step 10 to confirm that the signed image is installed. You will get output similar to the following showing that the `Attribute` is set to `Signed`:

```
10.168.100.32 - Blue Coat SG-S400 Series#show installed-systems

ProxySG Appliance Systems

1. Version: SGOS 6.5.2.9, Release ID: 144008

   Friday June 13 2014 02:54:25 UTC,
   Attributes: Signed, FIPS capable
   Boot Status: Last boot succeeded, Last Successful Boot: Tuesday June 3
2014 16:26:12 UTC
   Disk Layout: Compatible
......
```

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

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

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

    - **NOTE 2**: This command is only accepted via the CLI when accessed over the serial port.

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

34. Enter the properties for the following:

    a. Interface number

    b. IP address

    c. IP subnet mask

    d. IP gateway

    e. DNS server parameters

    f. Username and password.

35. The module will prompt for the enabled mode password:

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

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

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

37. Choose **Yes** or **No** to restrict workstation access.

38. Select the licensing mode:

    ```
    M)ACH5 Edition
    P)roxy Edition
    ```

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

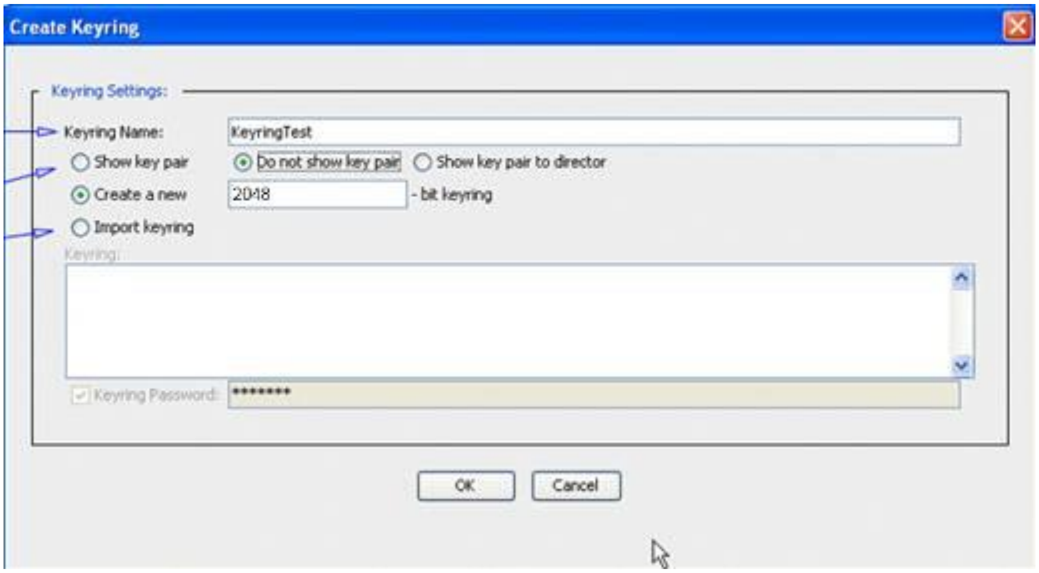
3.2.2 Management

The Crypto-Officer is able to monitor and configure the module via the Management Console (HTTPS over TLS) and the CLI (serial port or SSH).

The Crypto-Officer should monitor the module's status regularly. If any irregular activity is noticed or the module is consistently reporting errors, customers should consult 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 13. 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 ProxySG configuration, the CO must ensure that the "Do not show key pair" option is selected in the Management Console as shown in Figure 9 Keyring Creation Management Console Dialogue Box, or the "no-show" argument is passed over the CLI as shown in Figure 10 . Please see Section E: Preparing Archives for Restoration on New Devices in the *Blue Coat Systems SGOS Administration Guide, Version 6.5.2.x* for further reference.



Keyring Name: KeyringTest

○ Show key pair ● Do not show key pair ○ Show key pair to director

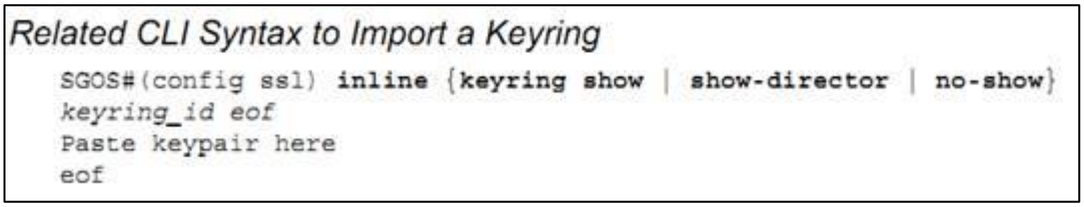
● Create a new 2048 -bit keyring

○ Import keyring

Keyring:

☑ Keyring Password: ********

Figure 9 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 10 Keyring Creation CLI Commands

3.2.3 Zeroization

The CO can return the module to its factory state by entering the "enabled" mode on the CLI, followed by the "fips-mode disable" command. This command will automatically reboot the module and zeroize the

MAK. The RSA private key, Crypto-Officer password, User password, “Enabled” mode password, “Setup” password, SNMP Privacy key, and the SNMP Authentication key are all stored encrypted by the MAK. Once the MAK is zeroized, decryption involving the MAK becomes impossible, making these CSPs unobtainable by an attacker.

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

3.3 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.

3.4 Non-Approved Mode

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

4. Acronyms

This section describes the acronyms used throughout this document.

Table 15 Acronyms

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
AES-NI	AES New Instructions
BMC	Baseband Management Controller
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
DH	Diffie Hellman
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
HAC	Hardware Accelerator Card

Acronym	Definition
HDS	HTTP Dynamic Streaming
HLS	HTTP Live Streaming
HMAC	Hash-Based Message Authentication Code
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

Acronym	Definition
SNMP	Simple Network Management Protocol
SOCKS	SOCKet Secure
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UPN	User Principle Name
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VoIP	Voice Over Internet Protocol
WAN	Wide Area Network