

Symantec, A Division of Broadcom Blue Coat ProxySG S400 and S500

Models: ProxySG S400-20, S400-30, S400-40, S500-10, S500-20 and S500-30

ProxySG S400 Hardware Versions: 090-03075, 090-03079, 090-03083, 090-03076, 090-03080, 090-03084

ProxySG S500 Hardware Versions: 090-02998, 090-03000, 090-03579, 090-02999, 090-03001, 090-03580

FIPS Security Kit Version: HW-KIT-FIPS-400, HW-KIT-FIPS-500

Firmware Versions: 6.7.2, 6.7.5

FIPS 140-2 Non-Proprietary Security Policy

FIPS 140-2 Security Level: 2

Document Version: 1.4

COPYRIGHT NOTICE

© 2021 Symantec, A Division of Broadcom. All rights reserved. BLUE COAT, PROXYSG, PACKETSHAPER, CACHEFLOW, INTELLIGENCECENTER, CACHEOS, CACHEPULSE, CROSSBEAM, K9, DRTR, MACH5, PACKETWISE, POLICYCENTER, PROXYAV, PROXYCLIENT, SGOS, WEBPULSE, SOLERA NETWORKS, DEEPSEE, DS APPLIANCE, SEE EVERYTHING. KNOW EVERYTHING., SECURITY EMPOWERS BUSINESS, BLUETOUCH, the Blue Coat shield, K9, and Solera Networks logos and other Blue Coat logos are registered trademarks or trademarks of Symantec Corporation, or its affiliates in the U.S. and certain other countries. This list may not be complete, and the absence of a trademark from this list does not mean it is not a trademark of Symantec or that Symantec has stopped using the trademark. All other trademarks mentioned in this document owned by third parties are the property of their respective owners. This document is for informational purposes only.

SYMANTEC MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. SYMANTEC 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.

CONTACT INFORMATION

Americas:

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

This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table of Contents

1. INTRODUCTION	6
1.1 PURPOSE	6
1.2 REFERENCES	6
1.3 DOCUMENT ORGANIZATION	6
2. BLUE COAT PROXYSG S400 AND S500.....	7
2.1 OVERVIEW.....	7
2.2 MODULE SPECIFICATION.....	11
2.3 MODULE INTERFACES.....	13
2.3.1 ProxySG S400 Appliance	13
2.3.2 ProxySG S500 Appliance	15
2.4 ROLES AND SERVICES.....	19
2.4.1 Crypto-Officer Role.....	20
2.4.2 User Role	23
2.4.3 Authentication Mechanism	24
2.5 PHYSICAL SECURITY	26
2.6 NON-MODIFIABLE OPERATIONAL ENVIRONMENT.....	26
2.7 CRYPTOGRAPHIC KEY MANAGEMENT	27
2.8 SELF-TESTS	37
2.8.1 Power-Up Self-Tests	37
2.8.2 Conditional Self-Tests	38
2.8.3 Critical Function Tests.....	38
2.9 MITIGATION OF OTHER ATTACKS.....	38
3. SECURE OPERATION.....	39
3.1 INITIAL SETUP FOR PROXYSG S400 APPLIANCE	39
3.1.1 ProxySG S400 Label and Baffle Installation.....	39
3.1.1.1 ProxySG S400 Shutter Installation	41
3.1.1.2 ProxySG S400 Label Application.....	43
3.2 INITIAL SETUP FOR PROXYSG S500 APPLIANCE	47
3.2.1 ProxySG S500 Label and Baffle Installation.....	48
3.2.1.1 ProxySG S500 Shutter Installation	49
3.2.1.2 ProxySG S500 Label Application.....	51
3.3 SECURE MANAGEMENT	55
3.3.1 Initialization.....	55
3.3.2 Management	57
3.3.3 Zeroization.....	58
3.4 USER GUIDANCE.....	58
4. ACRONYMS.....	59

List of Figures

FIGURE 1 TYPICAL DEPLOYMENT OF A PROXYSG APPLIANCE.....	7
FIGURE 2 PROXYSG S400 (FRONT VIEW)	12
FIGURE 3 PROXYSG S500 (FRONT VIEW)	12
FIGURE 4 CONNECTION PORTS AT THE FRONT OF THE PROXYSG S400.....	13
FIGURE 5 CONNECTION PORTS AT THE REAR OF THE PROXYSG S400	14
FIGURE 6 CONNECTION PORTS AT THE FRONT OF THE PROXYSG S500.....	16
FIGURE 7 CONNECTION PORTS AT THE REAR OF THE PROXYSG S500	17
FIGURE 8 PROXYSG S400 FIPS SECURITY KIT CONTENTS	39
FIGURE 9 PROXYSG S400 SHUTTER DISASSEMBLY	41
FIGURE 10 PROXYSG S400 LOWER SHUTTER INSTALLATION.....	41
FIGURE 11 PROXYSG S400 UPPER SHUTTER INSTALLATION	42
FIGURE 12 PROXYSG S400 LABELS SHOWING TAMPER EVIDENCE	43
FIGURE 13 PROXYSG S400 REAR EDGE LABEL INSTALLATION	44
FIGURE 14 PROXYSG S400 POWER SUPPLY LABEL INSTALLATION	45
FIGURE 15 PROXYSG S400 TOP BEZEL AND COVER LABEL INSTALLATION	46
FIGURE 16 PROXYSG S500 FIPS SECURITY KIT CONTENTS	47
FIGURE 17 PROXYSG S500 SHUTTER DISASSEMBLY	49
FIGURE 18 PROXYSG S500 LOWER SHUTTER INSTALLATION.....	49
FIGURE 19 PROXYSG S500 UPPER SHUTTER INSTALLATION	50
FIGURE 20 PROXYSG S500 LABELS SHOWING TAMPER EVIDENCE	51
FIGURE 21 PROXYSG S500 REAR EDGE LABEL INSTALLATION	52
FIGURE 22 PROXYSG S500 POWER SUPPLY LABEL INSTALLATION	53
FIGURE 23 PROXYSG S500 TOP BEZEL AND COVER LABEL INSTALLATION	54
FIGURE 24 KEYRING CREATION MANAGEMENT CONSOLE DIALOGUE BOX	58
FIGURE 25 KEYRING CREATION CLI COMMANDS	58

List of Tables

TABLE 1 MACH5 VS. PROXY EDITION CAPABILITY DIFFERENCES	8
TABLE 2 SECURITY LEVEL PER FIPS 140-2 SECTION.....	10
TABLE 3 PROXYSG APPLIANCE CONFIGURATIONS.....	11
TABLE 4 FIPS 140-2 LOGICAL INTERFACE MAPPINGS FOR THE FRONT OF THE PROXYSG S400	13
TABLE 5 FRONT PANEL LED STATUS INDICATIONS FOR THE PROXYSG S400	14
TABLE 6 FIPS 140-2 LOGICAL INTERFACE MAPPINGS FOR THE REAR OF THE PROXYSG S400	15
TABLE 7 REAR PANEL LED STATUS INDICATIONS FOR THE PROXYSG S400	15
TABLE 8 FIPS 140-2 LOGICAL INTERFACE MAPPINGS FOR THE FRONT OF THE PROXYSG S500	16
TABLE 9 FRONT PANEL LED STATUS INDICATIONS FOR THE PROXYSG S500	16
TABLE 10 FIPS 140-2 LOGICAL INTERFACE MAPPINGS FOR THE REAR OF THE PROXYSG S500	17
TABLE 11 REAR PANEL LED STATUS INDICATIONS FOR THE PROXYSG S500	18
TABLE 12 FIPS AND PROXYSG ROLES.....	19
TABLE 13 CRYPTO OFFICER ROLE SERVICES AND CSP ACCESS.....	20
TABLE 14 USER SERVICES AND CSP ACCESS.....	23
TABLE 15 NON-APPROVED SERVICES AND DESCRIPTION	24
TABLE 16 AUTHENTICATION MECHANISMS USED BY THE MODULE.....	25
TABLE 17 FIPS-APPROVED ALGORITHM IMPLEMENTATIONS FOR CRYPTO LIBRARY VERSION 4.1.1	27
TABLE 18 FIPS-APPROVED ALGORITHM IMPLEMENTATIONS FOR UEFI OS LOADER VERSION 4.14	28
TABLE 19 FIPS-APPROVED ALGORITHM IMPLEMENTATIONS FOR TLS LIBRARY VERSION 4.1.1	28
TABLE 20 FIPS-APPROVED ALGORITHM IMPLEMENTATIONS FOR SSH LIBRARY VERSION 7.2_2	28

TABLE 21 FIPS-APPROVED ALGORITHM IMPLEMENTATIONS FOR SNMP LIBRARY VERSION 5.7.2_1	29
TABLE 22 FIPS-ALLOWED ALGORITHMS	29
TABLE 23 NON-APPROVED ALGORITHMS	29
TABLE 24 LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS.....	31
TABLE 25 RS-232 PARAMETERS.....	55
TABLE 26 ACRONYMS.....	59

1. Introduction

1.1 Purpose

This is a *Non-Proprietary Cryptographic Module Security Policy* for the Blue Coat ProxySG S400 and S500 appliances (Firmware Versions 6.7.2 or 6.7.5; Models: ProxySG S400-20, ProxySG S400-30, ProxySG S400-40, ProxySG S500-10, ProxySG S500-20 and ProxySG S500-30) from Symantec Corporation. Either firmware version 6.7.2 or 6.7.5 running on the listed hardware platforms is considered to be validated. This *Non-Proprietary Security Policy* describes how the Blue Coat ProxySG S400 and Blue Coat ProxySG S500 meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at <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 validation of the module. The Blue Coat ProxySG S400 and Blue Coat ProxySG S500 is referred to in this document as ProxySG, S400 and S500, crypto module, or module.

1.2 References

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

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

1.3 Document Organization

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

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

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

2. Blue Coat ProxySG S400 and S500

2.1 Overview

The foundation of Symantec's application delivery infrastructure, Blue Coat ProxySG appliances establish points of control that accelerate and secure business applications for users across the distributed organization. Symantec 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:

- **Security:** Symantec'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.
- **Performance:** Symantec'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.
- **Control:** Symantec'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 for a typical deployment scenario for ProxySG appliances.

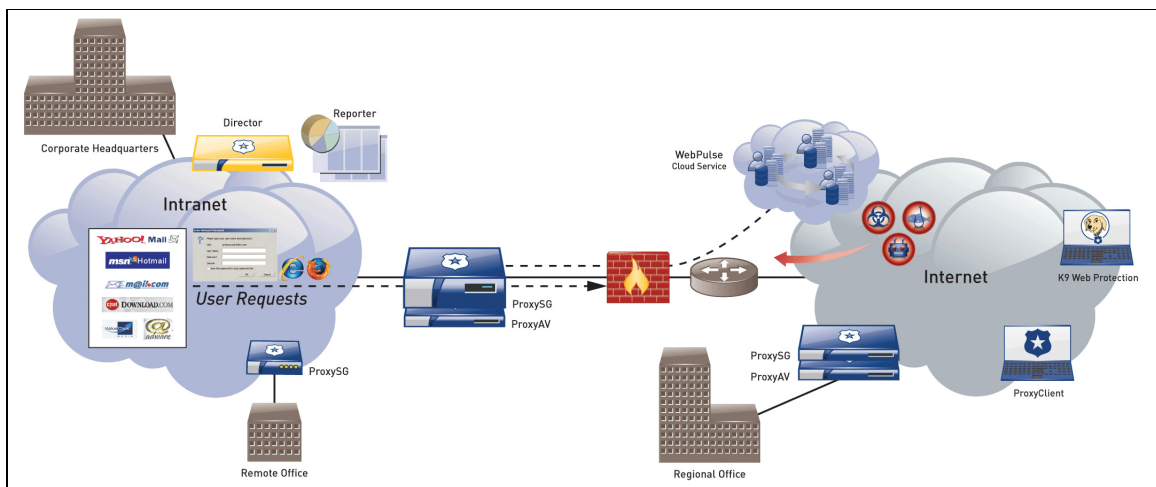


Figure 1 Typical Deployment of a ProxySG Appliance

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 listed in Table 1 below.

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
ICAP Services	No	Yes
Netegrity SiteMinder	No	Yes
Obliv COREid	No	Yes
Peer-To-Peer	No	Yes
User Authentication ⁵	Yes	Yes
Onbox Content Filtering (3 rd Party or BCWF ⁶)	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 feature¹⁰ of the Intel processor.

The Blue Coat ProxySG S400 and S500 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
9	Self-tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

¹ IMAP – Internet Message Access Protocol

² TCP – Transmission Control Protocol

³ POP3 – Post Office Protocol version 3

⁴ SMTP – Simple Mail Transfer Protocol

⁵ User authentication on MACH5 to identify a proxy user is supported when forwarding to the Symantec 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.

2.2 Module Specification

For the FIPS 140-2 validation, the crypto module was tested on the following Symantec appliance configurations listed in Table 3.

Table 3 Blue Coat ProxySG Appliance Configurations

Appliance Type	Hardware Version	Model	SKU / Short Description
Hardware Appliance MACH5 Edition	090-03075	SG-S400-20	SG-S400-20-M5
	090-03079	SG-S400-30	SG-S400-30-M5
	090-03083	SG-S400-40	SG-S400-40-M5
	090-02998	SG-S500-10	SG-S500-10-M5
	090-03000	SG-S500-20	SG-S500-20-M5
	090-03579	SG-S500-30	SG-S500-30-M5
Hardware Appliance Proxy Edition	090-03076	SG-S400-20	SG-S400-20-PR
	090-03080	SG-S400-30	SG-S400-30-PR
	090-03084	SG-S400-40	SG-S400-40-PR
	090-02999	SG-S500-10	SG-S500-10-PR
	090-03001	SG-S500-20	SG-S500-20-PR
	090-03580	SG-S500-30	SG-S500-30-PR

The hardware version numbers in Table 3 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 MACH5 vs. Proxy Edition Capability Differences provides a mapping between the capabilities and the licensing edition.

Each appliance type in Table 3 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, SG-S400-40, SG-S500-10, SG-S500-20, or SG-S500-30 that comes pre-configured with either the Proxy edition or MACH5 edition of SGOS. 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 of the S400 appliance 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 5 below.

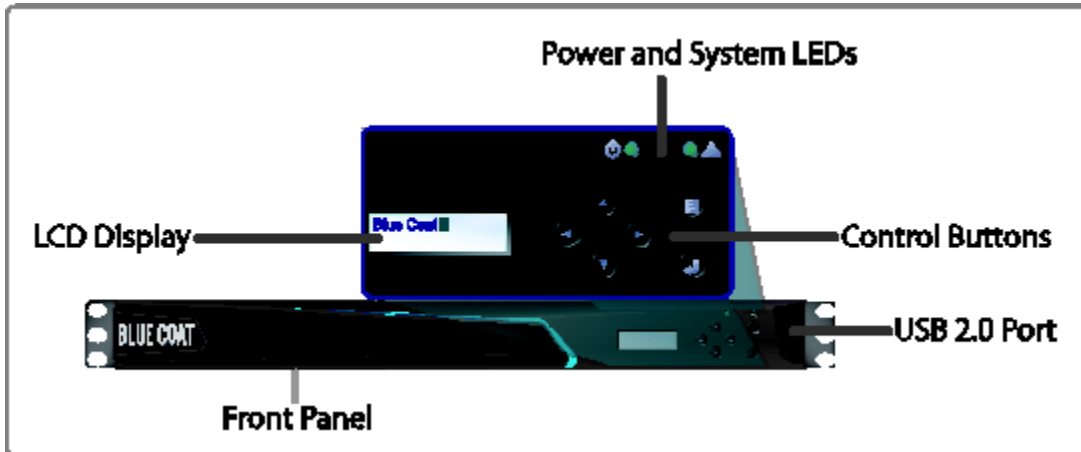


Figure 2 ProxySG S400 (Front View)

The ProxySG S500 offers an affordable rack-mountable appliance solution for small enterprises and branch offices that have direct access to the Internet.

The front panel of the S500 appliance 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 7 below.

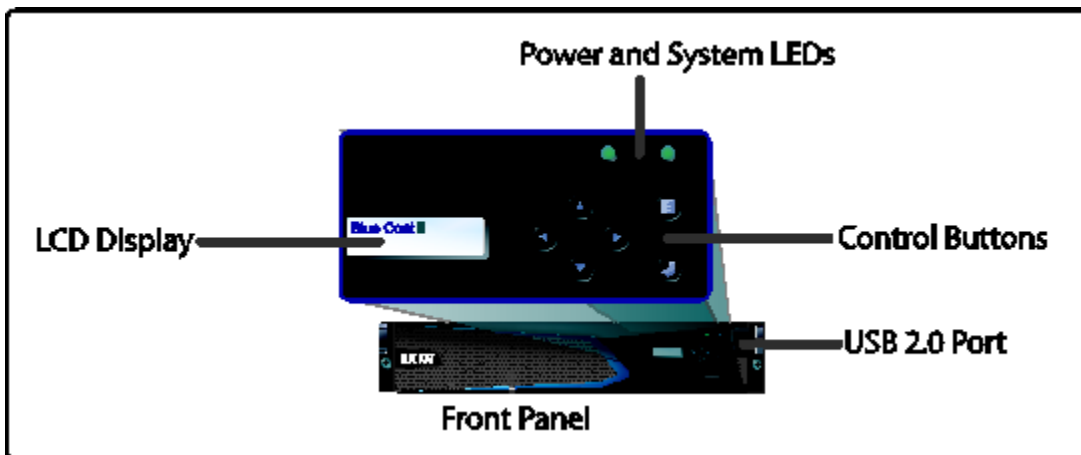


Figure 3 ProxySG S500 (Front View)

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

- ProxySG S400-20
- ProxySG S400-30
- ProxySG S400-40
- ProxySG S500-10
- ProxySG S500-20

ProxySG S500-30

The Blue Coat ProxySG is a module with a Multi-chip Standalone embodiment. The overall security level of the module is 2. The cryptographic boundary of the Blue Coat ProxySG is defined by the appliance chassis, which surrounds all the hardware and firmware. The module firmware, versions 6.7.2 and 6.7.5, contains the following cryptographic libraries:

- SGOS Cryptographic Library version 4.1.1
- SGOS UEFI OS Loader version 4.14
- SGOS TLS Library version 4.1.1
- SGOS SSH Library version 7.2_2
- SGOS SNMP Library version 5.7.2_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

2.3.1 ProxySG S400 Appliance

The front panel of the ProxySG S400 (as shown below in Figure 4) has a Liquid Crystal Display (LCD), two Light Emitting Diodes (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.



Figure 4 Connection Ports at the Front of the ProxySG S400

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
Control Buttons	6	N/A (buttons are disabled)
USB 2.0 Port	1	N/A (port is disabled)

The status indications provided by the LEDs on the front of 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 appliance 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 5.

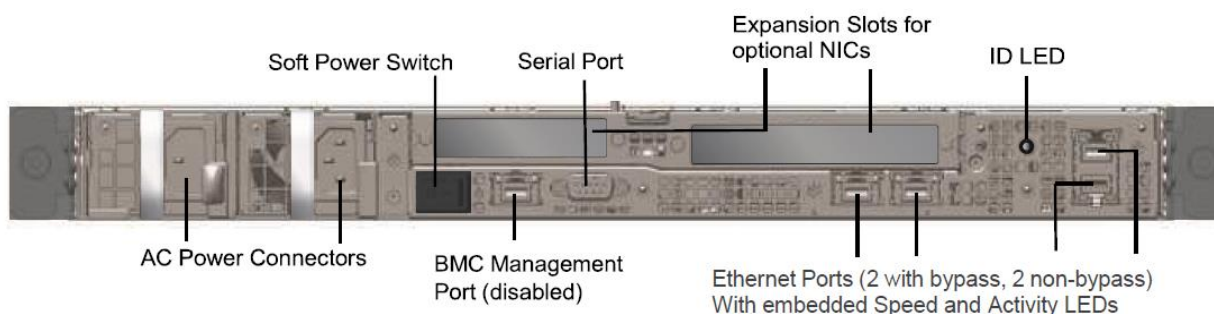


Figure 5 Connection Ports at the Rear of the ProxySG S400

The rear side of the ProxySG S400 (shown in Figure 5) 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 management¹¹
- 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 slots¹²

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.

The type and quantity of all ports present in rear panel of the ProxySG S400 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 ¹⁴ Management Port	1	N/A (port is disabled)
Serial ports	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 S400 are described in Table 7.

Table 7 Rear Panel LED Status Indications for the ProxySG S400

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

2.3.2 ProxySG S500 Appliance

The front panel of the ProxySG S500 (as shown below in Figure 6) has a Liquid Crystal Display (LCD), two Light Emitting Diodes (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.

¹³ The port can be used to access all functionality provided by the module. However, it is the preferred port for management.

¹⁴ BMC – Base Management Controller



Figure 6 Connection Ports at the Front of the ProxySG S500

The type and quantity of all ports present in the front panel of the ProxySG S500 are given in Table 8.

Table 8 FIPS 140-2 Logical Interface Mappings for the front of the ProxySG S500

Physical Port / Interface	Quantity	FIPS 140-2 Interface
LEDs	2	Status Output
LCD	1	Status Output
Control Buttons	6	N/A (buttons are disabled)
USB 2.0 Port	1	N/A (port is disabled)

The status indications provided by the LEDs on the ProxySG S500 are described in Table 9.

Table 9 Front Panel LED Status Indications for the ProxySG S500

LED	Color	Definition
Power LED	OFF	The appliance 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 S500 is shown in Figure 7.

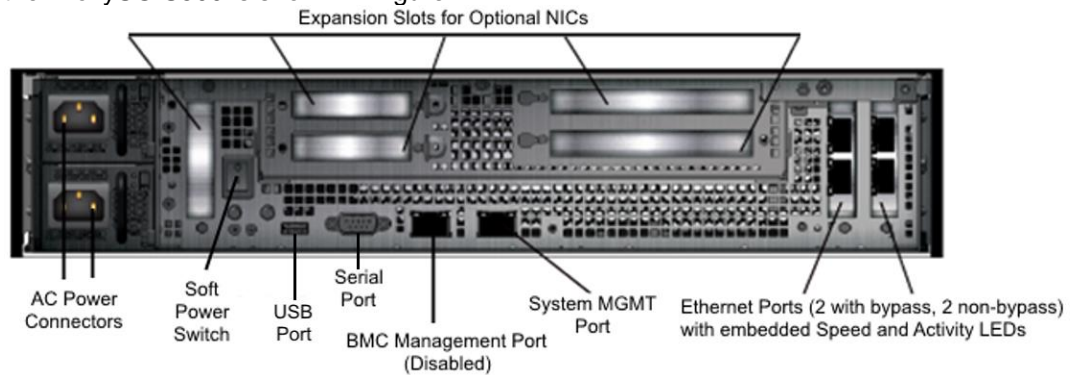


Figure 7 Connection Ports at the Rear of the ProxySG S500

The rear side of the ProxySG S500 (shown in Figure 7) 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 10G Base T Ethernet NICs
- One onboard, non-bypass 10/100/1000 Base T Ethernet adapter port for system management¹⁵
- One onboard 10/100/1000 Base T BMC management port (disabled/for internal use only)
- Five expansion slots¹⁶
- USB 2.0 port (disabled)

The type and quantity of all ports present in rear panel of the ProxySG S500 are given in Table 10.

Table 10 FIPS 140-2 Logical Interface Mappings for the rear of the ProxySG S500

Physical Port / Interface	Quantity	FIPS 140-2 Interface
Ethernet Ports	4	Data Input Data Output Control Input Status Output
System Management port ¹⁷	1	Data Input Data Output Control Input Status Output
BMC ¹⁸ Management Port	1	N/A (port is disabled)
Serial ports	1	Control Input Status Output
Ethernet Interface – Speed LEDs	5	Status Output
Ethernet Interface – Activity LEDs	5	Status Output
AC Power	2	Power Input
Soft Power Switch	1	Control Input
USB 2.0 Port	1	N/A (port is disabled)

¹⁵ The port can be used to access all functionality provided by the module. However, it is the preferred port for management.

¹⁶ Optional NICs are not included in the validation.

¹⁷ The port can be used to access all functionality provided by the module. However, it is the preferred port for management.

¹⁸ BMC – Base Management Controller

The status indications provided by the LEDs on the rear of the ProxySG S500 are described in Table 11.

Table 11 Rear Panel LED Status Indications for the ProxySG S500

LED	Color	Definition
AC power connection LED	OFF	The module is not receiving power.
	GREEN	The module is receiving power.
Ethernet Interface – Activity LEDs	OFF	No link is present.
	GREEN	Link is present
	FLASHING GREEN	Link activity.
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 16. The modules offer two management interfaces:

- **Command Line Interface (CLI):** Accessible locally via the serial port (provides access to the Setup Console portion of the CLI which requires the additional “Setup” password to gain access) or remotely using SSH. This interface is used for management of the modules. This interface must be accessed locally via the serial port to perform the initial module configurations (IP address, DNS server, gateway, and subnet mask) and placing the modules into the Approved mode. When the module has been properly configured, this interface can be accessed via SSH. Management of the module may take place via SSH or locally via the serial port. Authentication is required before any functionality will be available through the CLI.
- **Management Console (MC):** A graphical user interface accessible remotely with a web browser that supports TLS. This interface is used for management of the modules. Authentication is required before any functionality will be available through the Management Console

When managing the module over the CLI, COs and Users both log into the modules with administrator accounts entering the “standard”, or “unprivileged” mode on the 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 12.

Table 12 FIPS and ProxySG Roles

FIPS Roles	ProxySG Roles and Privileges
CO	<ul style="list-style-type: none"> • The CO is an administrator of the module that has been granted “enabled” mode access while using the CLI and “read/write” access while using the Management Console. • When the CO is using the CLI, and while in the “enabled” mode of operation, COs may put the module in its Approved mode, reset to the factory state (local serial port only) and query if the module is in Approved mode. In addition, COs may do all the services available to Users while not in “enabled” mode. • Once the CO has entered the “enabled” mode, the CO may then enter the “configuration” mode via the CLI. The “configuration” mode provides the CO management capabilities to perform tasks such as account management and key management. • When the CO is administering the module over the Management Console, they can perform all the same services available in CLI (equivalent to being in the “configuration” mode in the CLI) except the CO is unable to put the module into Approved mode.

FIPS Roles	ProxySG Roles and Privileges
User	<ul style="list-style-type: none"> The User is an administrator of the module that operates only in the “standard” or “unprivileged” mode and has not been granted access to the “enabled” mode in the CLI, and has been given “read-only” privileges when using the Management Console. The User may access the CLI and Management Console for management of the module. When the User is administering the module over the Management Console, they perform all the same services available in CLI (“standard” mode only services).

Descriptions of the services available to a Crypto Officer (CO) and Users are described below in Table 13 and Table 14 respectively. For each service listed below, COs and Users are assumed to already have authenticated prior to attempting to execute the service. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

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

2.4.1 Crypto-Officer Role

Descriptions of the FIPS 140-2 relevant services available to the Crypto-Officer role are provided in Table 13 below. Additional services that do not access CSPs can be found in the following documents:

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

Table 13 Crypto Officer Role Services and CSP Access

SERVICE	DESCRIPTION	CSP AND ACCESS REQUIRED
Set up the module (serial port only)	Set up the first-time network configuration, CO username and password, and enable the module in the Approved mode of operation. For more information, see section 3.3.1 in this <i>Security Policy</i> .	CO Password : W “Enabled” mode password: W “Setup” Password: W
Enter the “enabled” mode (CLI)	Manage the module in the “enabled” mode of operation, granting access to higher privileged commands	“Enabled” mode password: RX
* Enter the “configuration” mode (CLI)	Manage the module in the “configuration” mode of operation, allowing permanent system modifications to be made	None
* Disable FIPS mode (serial port only)	Take the module out of the approved mode of operation and restore it to a factory state	MEK: W SSH Session Key: W SSH Authentication Key: W TLS Session Key: W TLS Authentication Key: W DRBG CSPs: W
** Firmware Load	Loads new external firmware and performs an integrity test using an RSA digital signature.	Integrity Test public key: WRX

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 DH public key: WRX DH private key: WRX ECDH public key: WRX ECDH private key: WRX SSH Session Key: WRX SSH Authentication Key: WRX DRBG CSPs: WRX MEK: RX
Create remote management session (MC)	Manage the module through the Management Console (TLS) remotely via Ethernet port, with optional CAC authentication enabled.	RSA public key: RX RSA private key: RX DH public key: WRX DH private key: WRX ECDH public key: WRX ECDH private key: WRX TLS Session Key: WRX TLS Authentication Key: WRX DRBG CSPs: WRX MEK: RX
** Create, edit, and delete operator groups	Create, edit and delete operator groups; define common sets of operator permissions.	None
** Create, edit, and delete operators	Create, edit and delete operators (these may be COs or Users); define operator's accounts, change password, and assign permissions.	Crypto-Officer Password: W User Password: W MEK: RX
** Create filter rules (CLI)	Create filters that are applied to user data streams.	None
Create filter rules (MC)	Create filters that are applied to user data streams.	None
Show FIPS-mode status (CLI)	The CO logs in to the module using the CLI. Entering the command "show version" will display if the module is configured in Approved mode.	None
Show FIPS-mode status (MC)	The CO logs in to the module using the Management Console and navigates to the "Configuration" tab that will display if the module is configured in Approved mode.	None
** Manage module configuration	Backup or restore the module configuration	RSA public key: WRX RSA private key: WRX CO Password: WRX User Password: WRX "Enabled" mode password: WRX MEK: RX

SERVICE	DESCRIPTION	CSP AND ACCESS REQUIRED
* Zeroize keys (serial port only)	Zeroize keys by taking the module out of the Approved mode and restoring it to a factory state. This will zeroize all CSPs. The zeroization occurs while the module is still in Approved-mode.	MEK: W SSH Session Key: W SSH Authentication Key: W TLS Session Key: W TLS Authentication Key: W RSA private key: W DH private key: W ECDH private key: W CO and User Passwords: W Setup Password: W Enabled Mode Password: W
** Change password	Change Crypto-Officer password	Crypto-Officer Password: W MEK: RX
* Perform self-test	Perform self-test on demand by rebooting the machine	SSH Session Key: W SSH Authentication Key: W TLS Session Key: W TLS Authentication Key: W MEK: RX
* Reboot the module	Reboot the module.	DH public key: W DH private key: W ECDH public key: W ECDH private key: W SSH Session Key: W SSH Authentication Key: W TLS Session Key: W TLS Authentication Key: W DRBG CSPs: W MEK: RX

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

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

2.4.2 User Role

Descriptions of the FIPS 140-2 relevant services available to the User role are provided in Table 14 below. Additional services are that do not access CSPs can be found in the following documents:

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

Table 14 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 DH public key: RX DH private key: RX ECDH public key: RX ECDH private key: RX SSH Session Key: WRX SSH Authentication Key: WRX DRBG CSPs: WRX MEK: RX
Create remote management session (MC)	Manage the module through the Management Console (TLS) remotely via Ethernet port, with optional CAC authentication enabled.	RSA public key: RX RSA private key: RX DH public key: RX DH private key: RX ECDH public key: RX ECDH private key: RX TLS Session Key: WRX TLS Authentication Key: WRX DRBG CSPs: WRX MEK: RX
Show FIPS-mode status (MC)	The User logs in to the module using the Management Console and navigates to the "Configuration" which will display if the module is configured in Approved mode.	None
Show FIPS-mode status (CLI)	The User logs in to the module using the CLI. Entering the command "show version" will display if the module is configured in Approved mode.	None

The CO and User roles may monitor the health and status of the modules using SNMPv3. SNMPv3 privacy and authentication keys must be generated by an external application as the module is not capable of generating the keys internally. The keys are not tied to the CO's CLI and Management Console credentials. No security is claimed from the use of the SNMPv3 protocol in the module. Keys and CSPs encrypted using a SNMP are considered in plaintext form.

Table 15 Non-Approved Services and Description

SERVICE	DESCRIPTION
Import, replace, and delete SNMP keys	Create, edit and delete operators (these may be COs or Users); define operator's accounts, change password, and assign permissions.
Create SNMPv3 session	CO/User monitor the module using SNMPv3

2.4.3 Authentication Mechanism

The module supports role-based authentication. COs and Users must authenticate using a user ID and password, SSH client key (SSH only), or certificates associated with the correct protocol in order to set up the secure session. Secure sessions that authenticate Users have no interface available to access other services (such as Crypto Officer services). Each CO or User SSH session remains active (logged in) and secured until the operator logs out or inactivity for a configurable amount of time has elapsed. 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 PIV¹⁹ II card authentication.

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

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

1. On the management workstation the CO or User opens a browser and establishes a clear-text HTTP connection with the module.
2. Using CPL similar to the VPM `NotifyUser` action, the CO or User is presented with a DoD warning banner which they must positively acknowledge and accept.
3. `NotifyUser` redirects the browser to an HTTPS connection with the module that requires mutual authentication. This is made possible by CPL that puts the module in reverse-proxy mode at this point.
4. The TLS handshakes begin. The reverse-proxy service on the module requires a certificate to complete the handshake (i.e. the `verify-peer` setting has been enabled in the reverse-proxy service).
5. The browser presents the CO or User with a dialog box prompting which certificate to select.
6. The CO or User selects the X.509 certificate on the CAC.
7. The middleware on the management workstation prompts the CO or User for the PIN to unlock the certificate. The CO or User enters the PIN and the certificate is transmitted to the module.
8. The module authenticates the certificate against the CA list that has been configured on the reverse proxy service using local CRLs and OCSP to check for certificate revocation.
9. The CO or User reviews and accepts the certificate issued to the web browser by the module. A mutually authenticated TLS session is now in use.

¹⁹ PIV – Personal Identity Verification II

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 in Table 16.

Table 16 Authentication Mechanisms Used by the Module

Role	Type of Authentication	Authentication Strength
Crypto-Officer	Password	The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at minimum 8 characters in length, and at maximum 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1:(95 ⁸), or 1:6,634,204,312,890,625 chance of false acceptance. The Crypto-Officer may connect locally using the serial port or remotely after establishing a TLS or SSH session.
	Password ("Enabled" Mode)	The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1: (95 ⁸), or 1:6,634,204,312,890,625 chance of false acceptance. This password is entered by the Crypto-Officer to enter the "enabled" mode; this is entered locally through the serial port or remotely after establishing an SSH session.
	Password ("Setup")	The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at least 4 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). A 4-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1:(95 ⁴), or 1:81,450,625 chance of false acceptance. This password is entered by the Crypto-Officer and is required when using the serial port to access the Setup Console portion of the CLI.

Role	Type of Authentication	Authentication Strength
	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 $1: 6,634,204,312,890,625$ 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 $1: 5.19 \times 10^{33}$.

2.5 Physical Security

The Blue Coat ProxySG is a Multi-chip Standalone cryptographic module. It 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 and instructions can be found in section 3.1.1.2 for the S400 models and section 3.2.1.2 for the S500 models. The labels and baffles are part of the FIPS Security Kit for the S400 models (Part Number: 085-02891; HW-KIT-FIPS-400) and S500 models (Part Number 085-02870; HW-KIT-FIPS-500).

All of the module's components are production grade. The Blue Coat 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 Blue Coat ProxySG. 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 the tables below.

Table 17 FIPS-Approved Algorithm Implementations for Crypto Library version 4.1.1

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
4552	AES	SP 800-38A, SP 800-38D	CBC, CTR, GCM	128, 192, 256	Data Encryption / Decryption
4552	KTS	SP 800-38F	AES	128, 192, 256	Key Transport
2423	Triple-DES	SP 800-67	TCBC, ECB	192	Data Encryption / Decryption
2423	KTS	SP 800-38F	Triple-DES	112	Key Transport
3730	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest
3006	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA1-96, HMAC-SHA-224 ²⁰ , HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	128, 192, 256, 256, 512	Message Authentication
2479	RSA	FIPS 186-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512; PKCS1 v1.5	2048, 3072, 4096 for Signature Generation; and 1024, 2048, 3072, 4096 for Signature Verification	KeyPair Generation Digital Signature Generation, Digital Signature Verification
1502	DRBG	SP 800-90A	CTR-based	256	Deterministic Random Bit Generation
1231	CVL FFC	SP 800-56A	FFC	(2048, 224)	Key Agreement
1231 ²¹	CVL ECDH	SP 800-56A	ECC	P-256, P-384, P-521	Key Agreement

²⁰ HMAC-SHA-224 has been tested; however it is not used by any service.

²¹ P-256 and P-521 has been tested for CVL ECDH; however it is not used by any service

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
Vendor Affirmed	CKG	SP 800-133			Key Generation

Table 18 FIPS-Approved Algorithm Implementations for UEFI OS Loader version 4.14

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
3729	SHS	FIPS 180-4	SHA-1, SHA-256		Message Digest as part of Integrity Check
2478	RSA	FIPS 186-4	SHA-256; PKCS1 v1.5	2048	Digital Signature Verification as part of Integrity Check
3005	HMAC	FIPS 198-1	HMAC-SHA-1	128	Integrity Check

Table 19 FIPS-Approved Algorithm Implementations for TLS Library version 4.1.1

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
1237	CVL TLS 1.0, TLS 1.1, TLS 1.2	SP 800-135rev1	TLS 1.2 SHA Sizes = SHA-256, SHA384		Key Derivation

Table 20 FIPS-Approved Algorithm Implementations for SSH Library version 7.2_2

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
1233	CVL SSH	SP 800-135rev1	AES-128 CBC, AES-256 CBC	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Key Derivation

Table 21 FIPS-Approved Algorithm Implementations for SNMP Library version 5.7.2_1

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
1235 ²²	CVL SNMP	SP 800-135rev1			Key Derivation

Table 22 FIPS-Allowed Algorithms

Algorithm	Caveat	Use
RSA Key Wrapping (PKCS#1)	Provides between 112 and 150 bits of encryption strength	Key Wrapping
RSA Signature Verification	1536 bits	Signature Verification
Diffie-Hellman	Provides 112 bits of encryption strength	Key Agreement
Elliptic Curve Diffie-Hellman	Provides 192 bits of encryption strength	Key Agreement
MD5		TLS 1.1 sessions
Non-Deterministic Random Number generator (NDRNG) ²³		Seeding for the FIPS-Approved DRBG (SP 800-90 CTR_DRBG)

Table 23 Non-Approved Algorithms

Algorithm	Use
AES CFB mode (non-conformant)	SNMP Privacy Key

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

²² SNMP KDF was tested; however, it is not used by any service

²³ NDRNG is listed on the certificate

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

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

The module supports the CSPs listed below in Table 24.

Table 24 List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Master Encryption Key (MEK)	AES CBC 256-bit key	Internally generated via FIPS-Approved DRBG	Never exits the module	Stored in plaintext on non-volatile memory	By disabling the FIPS-Approved mode of operation	Encrypting Crypto-Officer password, RSA private key
Integrity Test Public Key	RSA public key 2048 bits	Externally generated, Imported in encrypted form via a secure TLS or SSH session	Never exits the module	Stored in plaintext on non-volatile memory	Overwritten after upgrade by the key in the newly signed image	Verifying the integrity of the system image during upgrade or downgrade
RSA Public Keys	2048-, 3072-, and 4096-bits	Modules' public key is internally generated via FIPS-Approved DRBG Modules' public key can be imported from a back-up configuration	Output during TLS/SSH ²⁴ negotiation in plaintext. Output during TLS negotiation for CAC authentication Exits in encrypted format when performing a module configuration backup	Stored in encrypted form on non-volatile memory	Module's public key is deleted by command	Negotiating TLS or SSH sessions

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
RSA Public Key	1024, 1536, 2048, 3072, and 4096-bits	Other entities' public keys are sent to the module in plaintext Can be sent to the module as part of an X.509 certificate during CAC authentication	Never output	Other entities' public keys reside on volatile memory	Other entities' public keys are cleared by power cycle	Negotiating TLS or SSH sessions
RSA Private Keys	2048-, 3072-, and 4096-bits	Internally generated via FIPS-Approved DRBG Imported in encrypted form via a secure TLS or SSH session Imported in plaintext via a directly attached cable to the serial port	Exits in encrypted format when performing a module configuration backup	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing encrypting MEK	Negotiating TLS or SSH sessions
DH public key	2048-bits	Module's public key is internally generated via FIPS-Approved DRBG Public key of a peer enters the module in plaintext	The module's Public key exits the module in plaintext	Stored in plaintext on volatile memory	Inaccessible by disabling FIPS-mode 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	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power	Negotiating TLS or SSH sessions
ECDH private key	P-256 key	Internally generated via FIPS-Approved DRBG	Never exits the module	Stored in plaintext on volatile memory	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power	Negotiating TLS or SSH sessions
ECDH public key	P-256 key	Module's public key is internally generated via FIPS-Approved DRBG Public key of a peer enters the module in plaintext	The module's Public key exits the module in plaintext	Stored in plaintext on volatile memory	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power	Negotiating TLS or SSH sessions

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
TLS or SSH Session key	AES CBC, CTR, or GCM ²⁵ 128-, 192, or 256-bit key Triple-DES CBC keying option 1 (3 different keys)	Internally generated via FIPS-Approved DRBG	Output in encrypted form during TLS or SSH protocol handshake	Stored in plaintext on volatile memory	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power	Encrypting TLS or SSH data
TLS or SSH Session Authentication key	HMAC SHA-1-, 256-, 384- or 512-bit key	Internally generated	Never exits the module	Resides in volatile memory in plaintext	Inaccessible by disabling FIPS-mode 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 encrypted MEK	Locally authenticating a CO or User for Management Console or CLI

²⁵ AES GCM is only used as part of TLS 1.2 cipher suites conformant to IG A.5, RFC 5288 and SP 800-52 which are listed in Table 24 of this document

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 MEK	Used by the CO to enter the “privileged” or “enabled” mode when using the CLI
“Setup” Password	Minimum of four (4) and maximum of 64 bytes long printable character string	Enters the module in plaintext via a directly attached cable to the serial port	Never exits the module	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting MEK	Used by the CO to secure access to the CLI when accessed over the serial port
SP 800-90A CTR_DRBG Seed	384-bit random number	Internally generated	Never exits the module	Plaintext in volatile memory	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power	Seeding material for the SP800-90A CTR_DRBG
SP 800-90A CTR_DRBG Entropy ²⁶	256-bit random number with derivation function 384-bit random number without derivation function	Internally generated	Never exits the module	Plaintext in volatile memory	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power	Entropy material for the SP800-90A CTR_DRBG

²⁶ The Entropy required by the FIPS-Approved SP 800-90 CTR_DRBG (with AES-256) is supplied by the NDRNG

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	Inaccessible by disabling FIPS-mode 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	Inaccessible by disabling FIPS-mode Rebooting the modules Removing power	Used for the SP 800-90A CTR_DRBG

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

Keys and passwords that exit the module during a configuration backup are encrypted using a FIPS-Approved encryption algorithm. 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 the module fails the POST Integrity Test, the following error is printed to the CLI (when being accessed via the serial port):

```
PKCS7 Signature verification failed, signature does not match.
```

If any other firmware self-tests fail, the following error is printed to the CLI (when being accessed via the serial port):

```
***** SYSTEM ERROR *****
The SG Appliance has failed the FIPS Self test.
System startup cannot continue.

***** SYSTEM STARTUP HALTED *****
E)xit FIPS mode and reinitialize system
R)estart and retry FIPS self-test
Selection:
```

When either of these errors occurs, the modules halt operation and provide no functionality. The only way to clear the error and resume normal operation is for the Crypto-Officer to reboot the modules. The status output provided below is shown only over the CLI (when being accessed via the serial port).

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

2.8.1 Power-Up Self-Tests

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

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

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

- Known Answer Tests

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

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

2.8.2 Conditional Self-Tests

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

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

2.8.3 Critical Function Tests

The Blue Coat ProxySG performs the following critical function tests:

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

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

2.9 Mitigation of Other Attacks

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

3. Secure Operation

The Blue Coat ProxySG meets FIPS-140-2 Level 2 requirements. The sections below describe how to place and keep the module in FIPS-Approved mode of operation. The tamper seals and FIPS kit shall be installed for the module to operate in a FIPS Approved mode of operation

3.1 Initial Setup for ProxySG S400 Appliance

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-KIT-FIPS-400) for the modules consists of the following items as shown below in Figure 8.

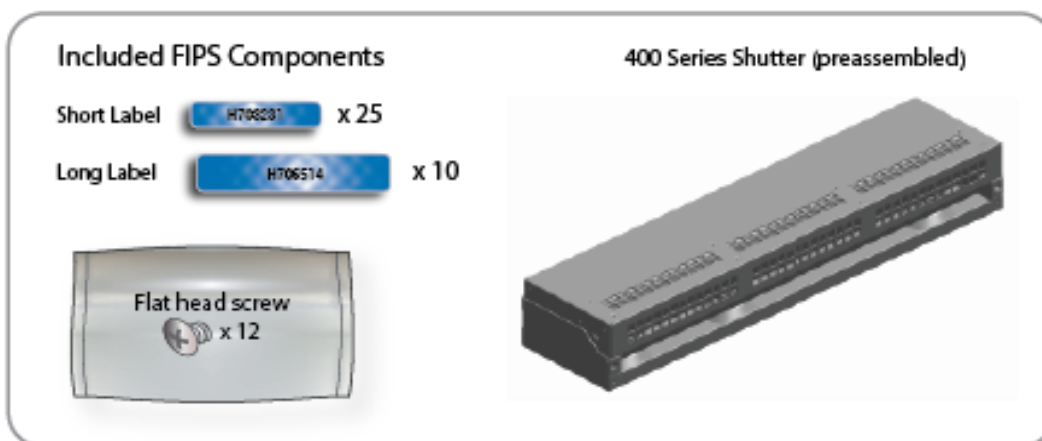


Figure 8 ProxySG S400 FIPS Security Kit Contents

The FIPS security kit may include either red or blue labels.

Note: Included in the S400 FIPS Kit, there are (25) 'Short Labels' and (10) 'Long labels'; however, only (5) short labels and (2) long labels are required for FIPS compliance. Additional labels are provided for reapplication purposes.

3.1.1 ProxySG S400 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 (red or blue):

- 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 accidentally touch the adhesive side, discard that label and apply another one.

Label application tips (for red or blue labels):

- 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 ProxySG S400 Shutter Installation

The two piece rear shutter (S400 Series Shutter as shown in Figure 8) 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.

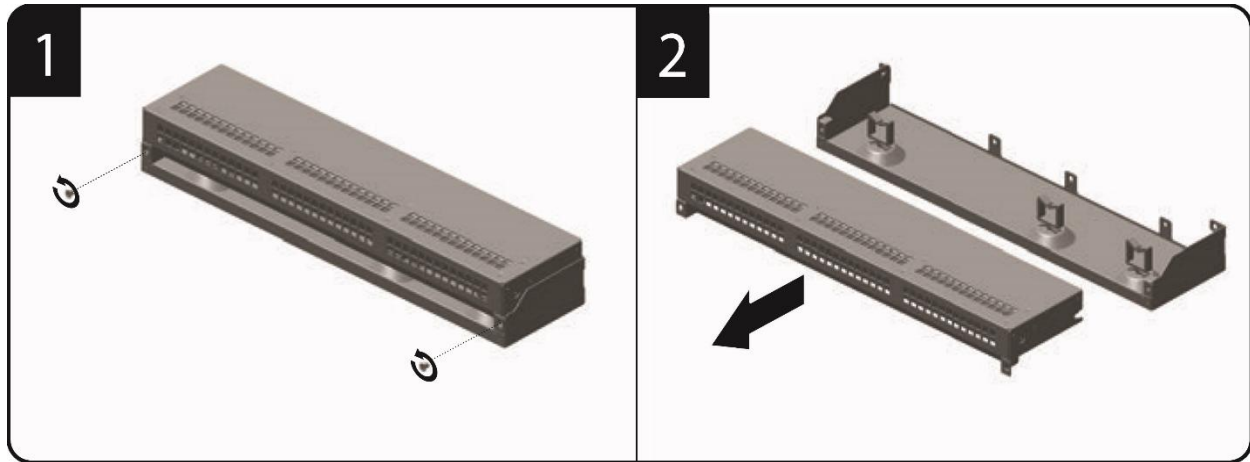


Figure 9 ProxySG S400 Shutter Disassembly

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.

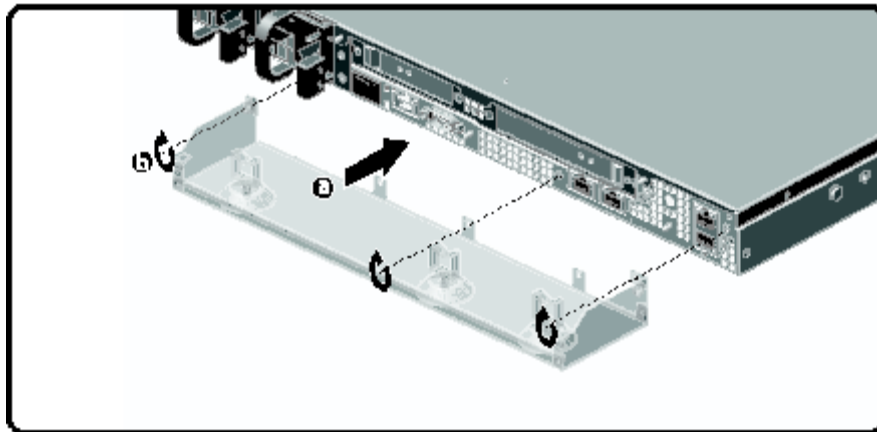


Figure 10 ProxySG S400 Lower Shutter Installation

3. Rack mount the appliance. Refer to the S400 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.

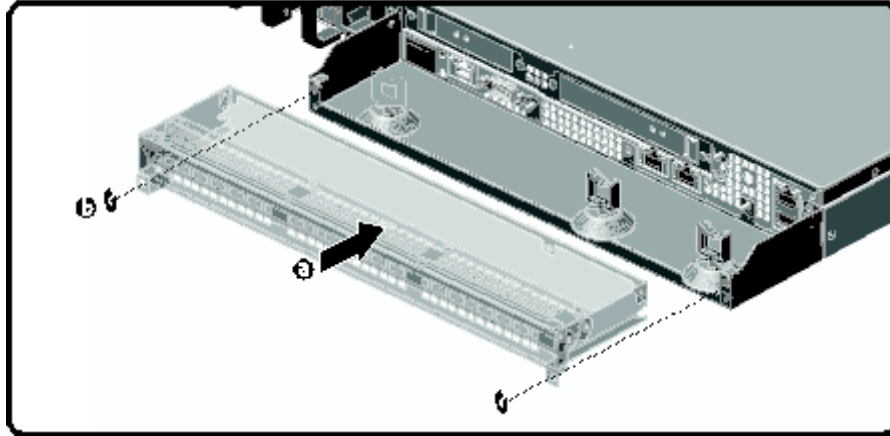


Figure 11 ProxySG S400 Upper Shutter Installation

3.1.1.2 ProxySG S400 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 12 below illustrates the tamper-evident features of the label.



Figure 12 ProxySG S400 Labels 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.

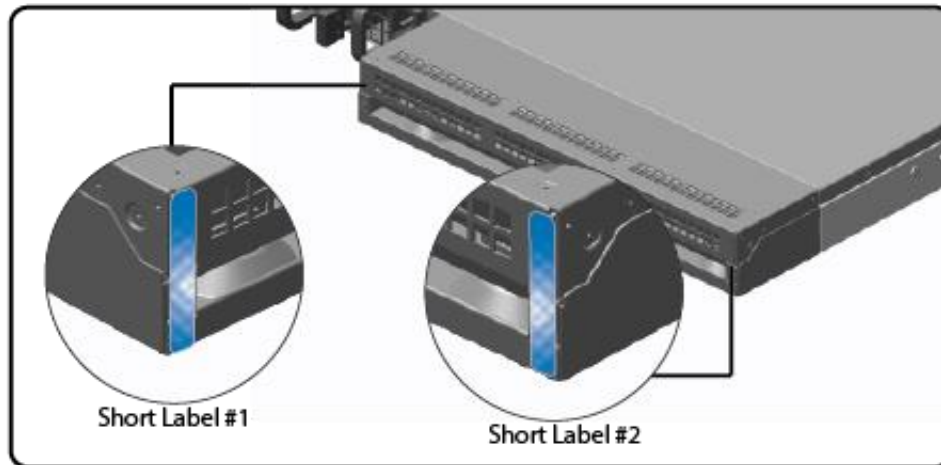


Figure 13 ProxySG S400 Rear Edge Label Installation

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, 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 not cover any of the vent holes.

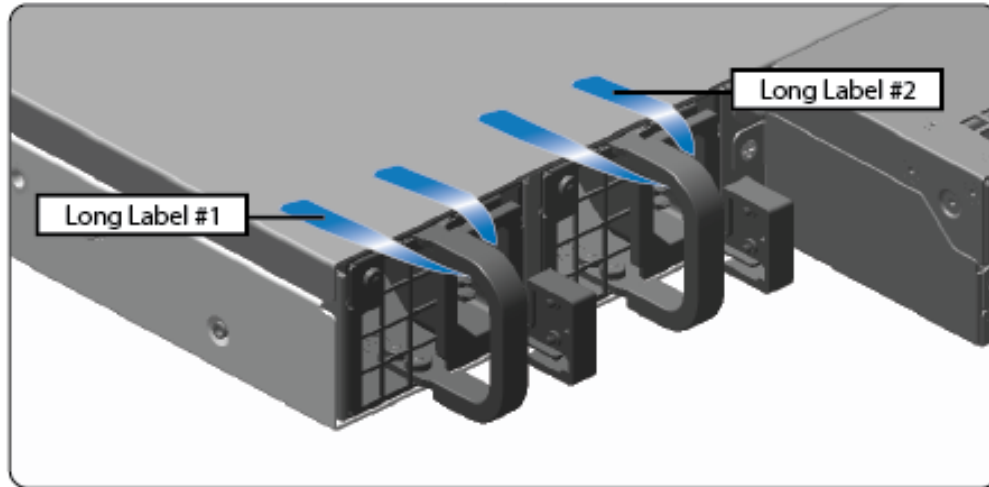


Figure 14 ProxySG S400 Power Supply Label Installation

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.

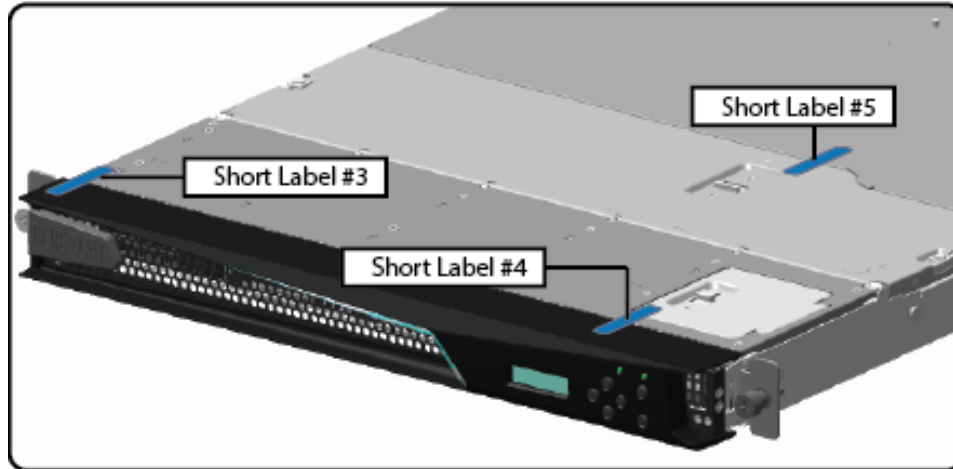


Figure 15 ProxySG S400 Top Bezel and Cover Label Installation

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 Initial Setup for ProxySG S500 Appliance

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 (085-02870; HW-KIT-FIPS-500) for the modules consists of the following items as shown below in Figure 16.

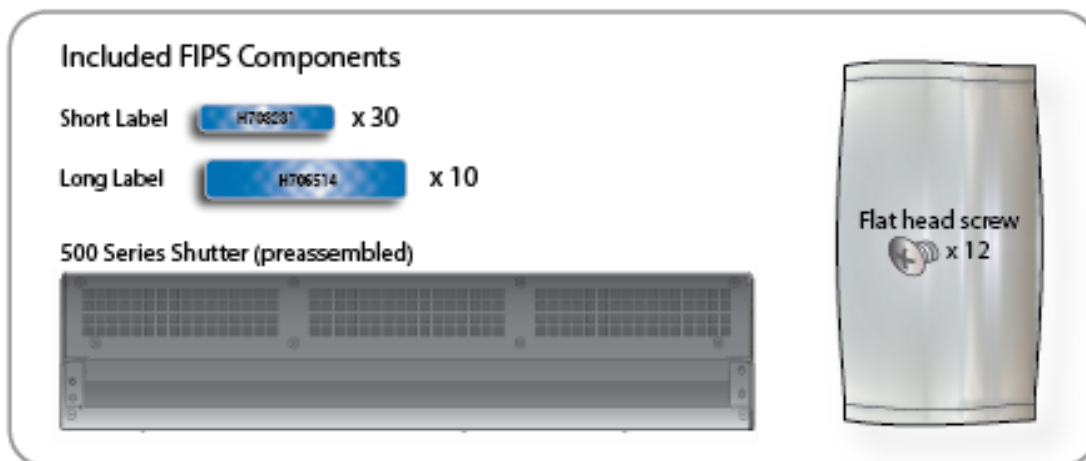


Figure 16 ProxySG S500 FIPS Security Kit Contents

Note: Included in the S500 FIPS Kit, there are (30) 'Short Labels' and (10) 'Long labels'; however, only (8) short labels and (2) long labels are required for FIPS compliance. Additional labels are provided for reapplication purposes.

3.2.1 ProxySG S500 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 (red or blue):

- 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 accidentally touch the adhesive side, discard that label and apply another one.

Label application tips (for red or blue labels):

- 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.

3.2.1.1 ProxySG S500 Shutter Installation

The two piece rear shutter (S500 Series Shutter as shown in Figure 16) 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.

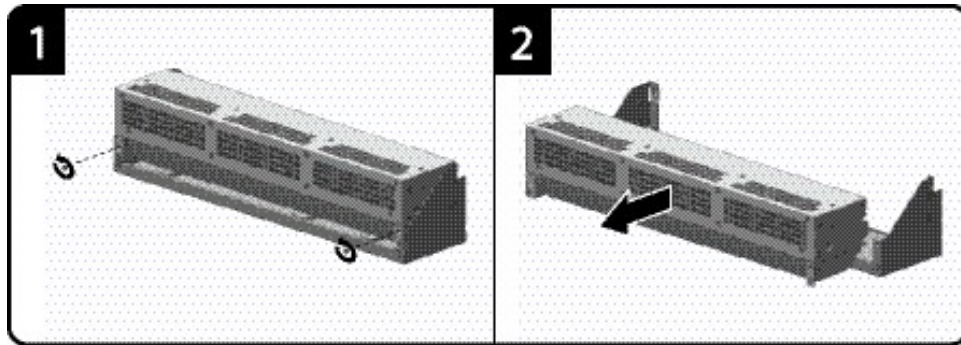


Figure 17 ProxySG S500 Shutter Disassembly

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.

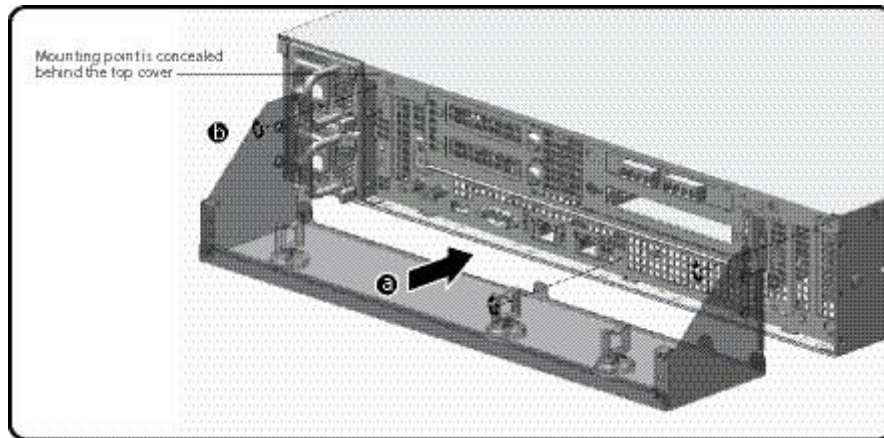


Figure 18 ProxySG S500 Lower Shutter Installation

3. Rack mount the appliance. Refer to the S500 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.

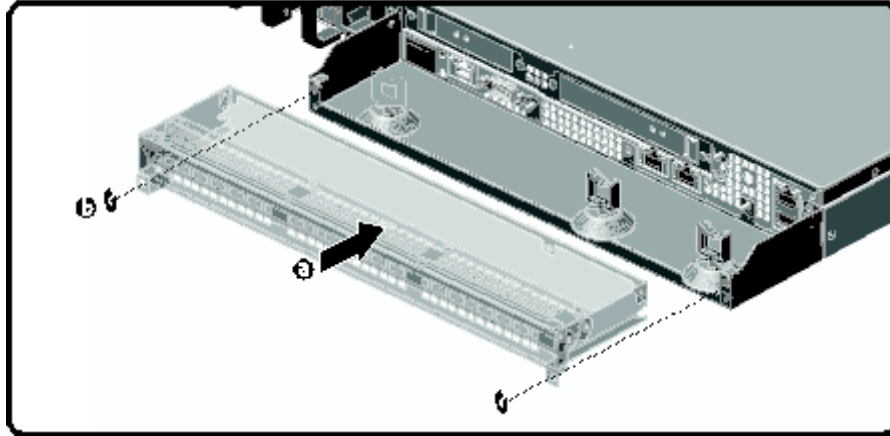


Figure 19 ProxySG S500 Upper Shutter Installation

3.2.1.2 ProxySG S500 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 12 below illustrates the tamper-evident features of the label.



Figure 20 ProxySG S500 Labels 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.

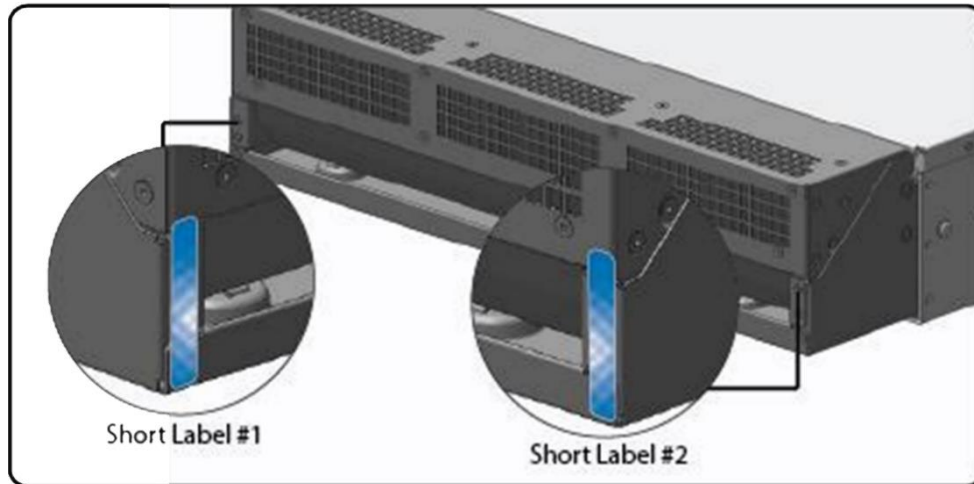


Figure 21 ProxySG S500 Rear Edge Label Installation

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, 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 not cover any of the vent holes.

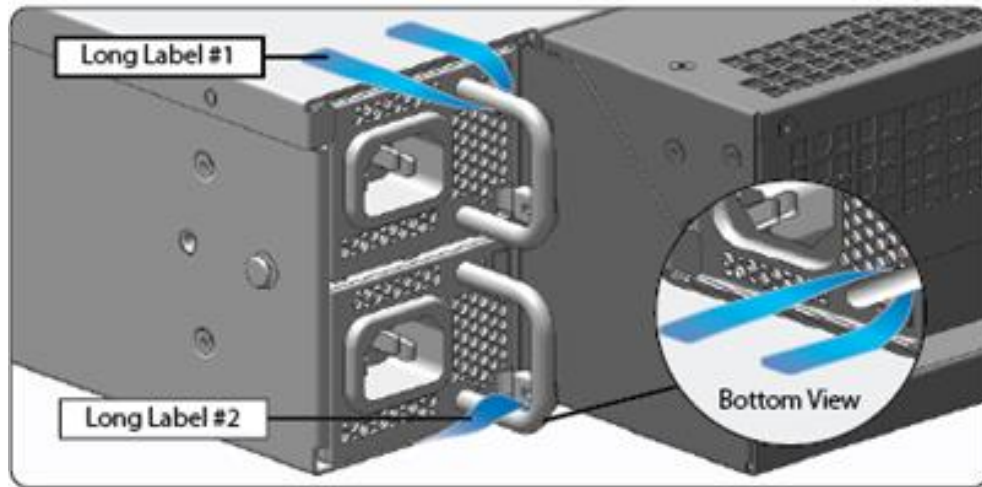


Figure 22 ProxySG S500 Power Supply Label Installation

4. Apply six (6) short red or blue labels (short labels 3, 4, 5, 6, 7, and 8) over the opposite ends of the bezel, center cover, and the rear cover panel to prevent unauthorized access to the system components. Each label should be placed on the opposite ends of the appliance, as shown below.

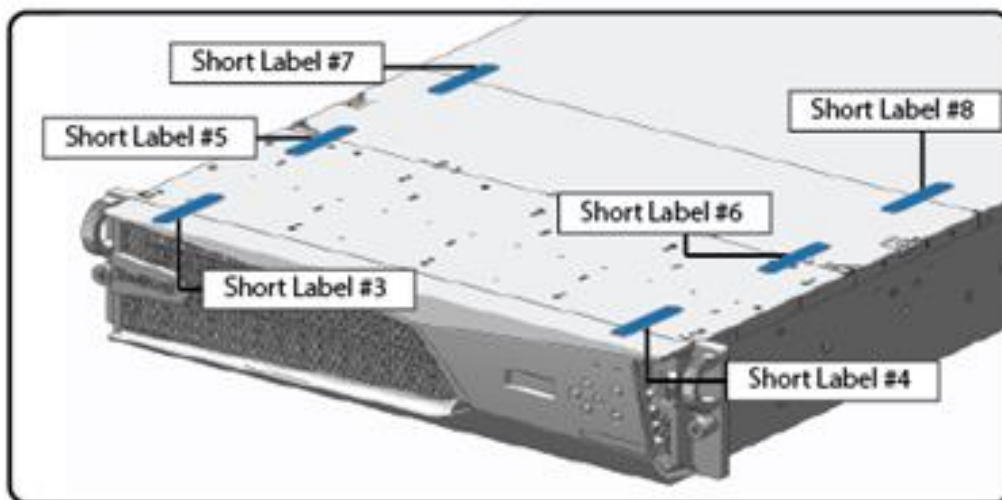


Figure 23 ProxySG S500 Top Bezel and Cover Label Installation

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.

3.3 Secure Management

3.3.1 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. Note, these same steps in this section shall be followed after the zeroization command is entered.

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 25.

Table 25 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

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

```
You must configure the console user account now.
```

```
Enter console username:
```

```
Enter console password:
```

```
Enter enable password:
```

6. The module will prompt to secure serial port, select 'n'
7. When the system displays `Successful Configuration Setup`, press **Enter** to confirm the configuration.
8. Press **Enter** three times.

9. Select option #1 for the Command Line Interface.

10. Type **enable** and press **Enter**.

11. Enter the enable mode password.

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

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

- **NOTE 1:** The `fips-mode enable` command causes the device to power cycle, zeroing the Master Encryption Key and returning the configuration values set in steps 1 and 2 to their factory state.
- **NOTE 2:** This command is only accepted via the CLI when accessed over the serial port.

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

14. Enter the properties for the following:

- a. Interface number
- b. IP address
- c. IP subnet mask
- d. IP gateway
- e. DNS server parameters

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

```
You must configure the console user account now.
```

```
Enter console username:
```

```
Enter console password:
```

```
Enter enable password:
```

16. 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:
```

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

18. Select the licensing mode:

```
M)ACH5 Edition
```

```
P)roxy Edition
```

```
R)everse Proxy
```

19. Access the Web interface at the IP address configured in step 14b above (<https://<IP Address>:8082>).

20. Login with the credentials created in step 15.

21. Navigate to the Configuration tab. Then expand the Authentication->SSH Inbound Connections menu in the left hand column.

22. Select the Ciphers tab. Deselect the [aes256-gcm@openssh.com](#) and the [aes128-gcm@openssh.com](#) ciphers. Select the aes256-ctr, aes192-ctr, aes128-ctr, aes256-, and aes128-cbc ciphers.

23. Press Apply and the changes will be saved to the appliance.

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

3.3.2 Management

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

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

The CO password and "enabled" mode password must be at least 8 characters in length. 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 backup configuration, the CO must ensure that the "Do not show key pair" option is selected in the Management Console as shown in Figure 24, or the "no-show" argument is passed over the CLI as shown in Figure 25. Please see Section E: Preparing Archives for Restoration on New Devices in the *Symantec Systems SGOS Administration Guide, Version 6.7.x* for further reference.

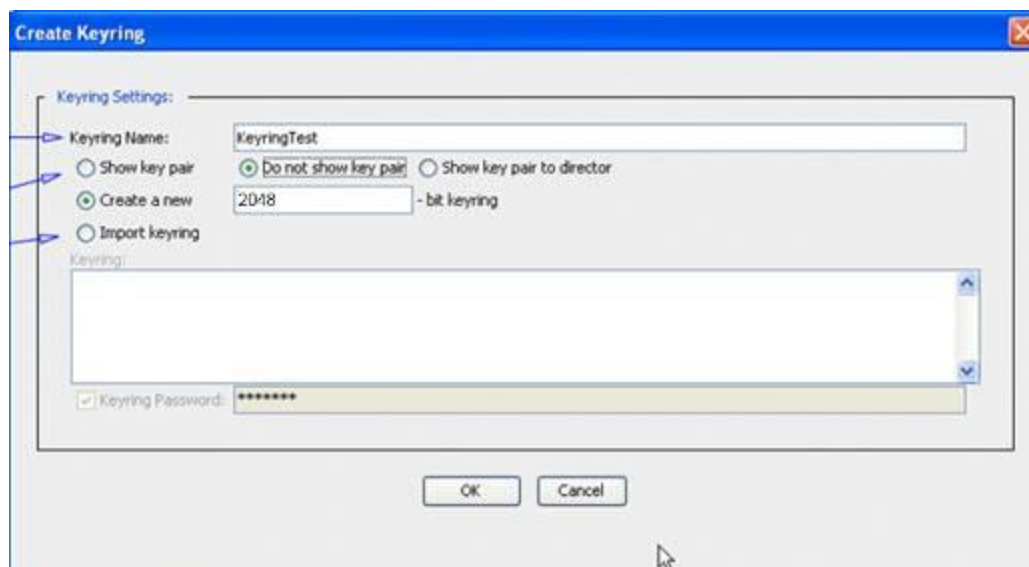


Figure 24 Keyring Creation Management Console Dialogue Box

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 25 Keyring Creation CLI Commands

3.3.3 Zeroization

The CO can return the module to its factory state by entering the “enabled” mode on the CLI, followed by the “fips-mode disable” command. This command will automatically reboot the module and zeroize the MEK. The RSA private key, Crypto-Officer password, User password, “Enabled” mode password, “Setup” password, SNMP Privacy key, and the SNMP Authentication key are stored encrypted by the MEK. Once the MEK is zeroized, decryption involving the MEK becomes impossible, making these CSPs unobtainable by an attacker.

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

3.4 User Guidance

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

4. Acronyms

This section describes the acronyms used throughout this document.

Table 26 Acronyms

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