Blue Coat Systems, Inc.

ProxySG 600 Appliance

Models: ProxySG 600-10, 600-20, 600-35
Hardware Version: 090-02911, 090-02912, 090-02913, 090-02914, 090-02915, 090-02916
Firmware Version: 6.1

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 1.3

Prepared for:

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

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

Prepared by:

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

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

Table of Contents

List of Figures

List of Tables

.

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the ProxySG 600 Appliance (Models : ProxySG 600-10, 600-20, 600-35; Firmware Version: 6.1) from Blue Coat Systems, Inc.. This Security Policy describes how the ProxySG 600 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 appliances in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The ProxySG 600 Appliance is referred to in this document collectively as *ProxySG 600*, *crypto module*, or *module*.

1.2 References

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

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

1.3 Document Organization

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

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

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

2 ProxySG 600

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 below for a typical deployment scenario for ProxySG appliances.

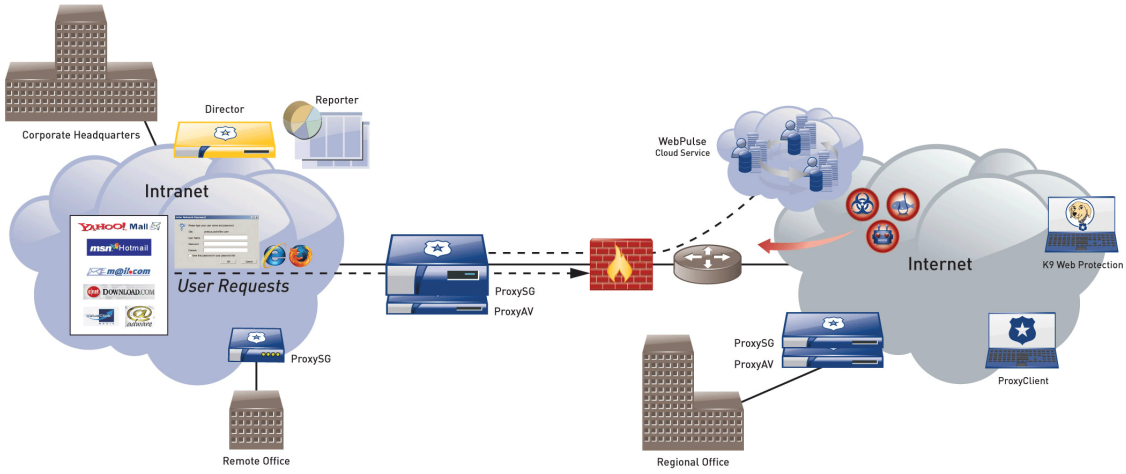

Figure 1 Typical Deployment of a ProxySG Appliance

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 evaluated configurations are:

- Secure Hypertext Transfer Protocol (HTTPS)

- Transmission Control Protocol (TCP) tunneling protocols such as Secure Shell (SSH) v2.0
- Common Internet File System (CIFS)
- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Sock-Et-S (SOCKS)
- SSL (The modules' software cryptographic algorithm implementations are based on the OpenSSL open-source library)
- Telnet
- IM & Streaming

Control is achieved by enforcing a configurable policy 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. Optimization is achieved by enforcing a configurable policy (WAN Optimization SFP) on traffic traversing the WAN.

The ProxySG 600 is validated at the following FIPS 140-2 Section levels in Table 1:

Table 1 Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	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	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

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

Table 2 ProxySG 600 Appliance Configurations

Model	Hardware Version	
	Proxy Edition	MACH5 Edition
ProxySG 600-10	090-02912	090-02911
ProxySG 600-20	090-02914	090-02913
ProxySG 600-35	090-02916	090-02915

The Proxy edition and MACH5 edition hardware version numbers represent licensing options available. The MACH5 and Proxy editions run on the exact same hardware and firmware and are exactly the same from a cryptographic functionality and boundary perspective. The MACH5 edition provides acceleration, optimization, and caching features that optimize and secure the flow of information to any user. The Proxy edition provides all the functionality of the MACH5 but also acts as a secure web gateway. Capabilities found only in the Proxy Edition consist of protecting the network from malware, spyware, preventing data leakage, and ensuring user compliance with corporate network guidelines.

The ProxySG 600 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), 2 Light Emitting Diodes (LEDs), and 6 control buttons (NOTE: the front panel control buttons are disabled in FIPS-Approved mode).

Connection ports are at the rear, as shown in Figure 3.

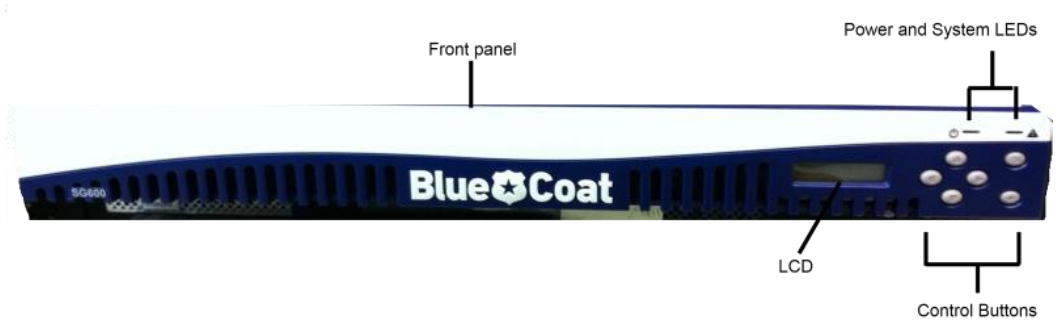

Figure 2 ProxySG 600 (Front View)

The ProxySG 600 is a hardware module with a multi-chip standalone embodiment. The overall security level of the module is 2. The cryptographic boundary of the ProxySG 600 is defined by the appliance chassis, which surrounds all the hardware and software. The module Firmware, version 6.1, contains the SGOS 6.1 Cryptographic Library version 2.1.1.

2.3 Module Interfaces

The front panel of the ProxySG 600 (as shown in Figure 2) has an LCD interface, 2 LEDs, and six control buttons. The control buttons on the front panel are disabled in FIPS-approved mode of operation. Outside

of FIPS-approved mode, the control buttons allow the operator to configure the IP address, Subnet mask, Gateway address, DNS address, console password and enable password.

These control buttons work in conjunction with the LCD display to provide a menu command interface:

- Top right corner: Menu button
- Bottom right corner: Enter button
- Remaining four buttons: Up, Down, Left, Right

The type and quantity of all ports present in the front panel of the ProxySG 600 are given in Table 3.

Table 3 FIPS 140-2 Logical Interface Mappings for the front of the ProxySG 600

Physical Port/Interface	Quantity	FIPS 140-2 Interface
LEDs	2	• Status Output
LCD	1	• Status Output

The status indications provided by the LEDs on the ProxySG 600 is described in Table 4.

Table 4 Front Panel LED Status Indications for the ProxySG 600

LED	Color	Definition
Power LED	OFF	The ProxySG is powered off.
	AMBER	The OS has loaded but has not been loaded.
	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	The appliance is functioning properly.
	AMBER	The appliance has encountered a warning.
	FLASHING AMBER	The appliance has encountered a critical problem.

The rear of the ProxySG 600 is shown in Figure 3.

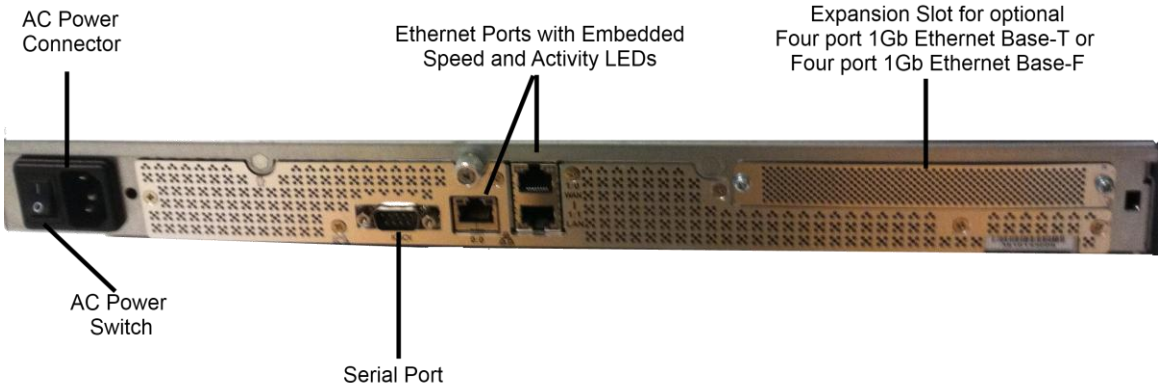

Figure 3 Connection Ports at the Rear of the ProxySG 600-10, 20, 35

The rear side of the 600 (shown in Figure 3) contains all the connecting ports. Those ports are:

- An AC power connector.
- A serial port to connect to a Personal Computer (PC) for management.
- Two 10/100/1000 Base T Ethernet adapter ports.
- One 10/100/1000 Base T Ethernet adapter port for management.
- An expansion slot for:
  - An optional Four port 1000 Base-F (quad GigE Fiber SX) NIC
  - An optional Four port 1000 Base-T (quad GigE with bypass) NIC

The type and quantity of all ports present in rear panel of the ProxySG 600 are given in Table 5.

Table 5 FIPS 140-2 Logical Interface Mappings for the rear of the ProxySG 600

Physical Port/Interface	Quantity	FIPS 140-2 Interface
Ethernet ports	3	• Data Input • Data Output • Control Input • Status Output
Serial ports	1	• Control Input • Status Output
Ethernet Interface – Speed LEDs	3	• Status Output
Ethernet Interface – Activity LEDs	3	• Status Output
AC power	1	• Power Input
Power Switch	1	• Control Input

The status indications provided by the LEDs on the rear of the ProxySG 600 are described in Table 6.

Table 6 Rear Panel LED Status Indications for the ProxySG 600

LED	Color	Definition
Ethernet Interface – Activity LEDs	OFF	No link is present.
	GREEN	Link is present.

.

	FLASHING GREEN	Link activity.
Ethernet Interface – Activity LEDs	OFF	10 Mbps speed connection is present.
	GREEN	100 Mbps speed connection is present.
	AMBER	1000 Mbps speed connection is present.

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 10. The modules offer two management interfaces:

- CLI – accessible locally via the serial port (requires the "Setup" password to gain access) or remotely using SSH. This interface is used for management of the modules. This interface is used for the initial module configurations (IP address, DNS server, gateway, and subnet mask), putting the modules into FIPS mode (serial port only), and management of the modules. Authentication is required before any functionality will be available through the CLI.
- Web GUI – 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 Web GUI.

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 7.

Table 7 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 Web GUI. When the CO is using the CLI, and while in the "enabled" mode of operation, COs may put the module in and out of FIPS mode (local serial port only) and query if the modules are in FIPS 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 Web GUI, 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 FIPS mode. The CO may monitor the health and status of the modules using SNMPv3. SNMPv3 privacy and authentication keys are assigned to a CO and are not tied to the CO's CLI and Web GUI 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 Web GUI. The User will access the CLI and Web GUI interfaces for management of the module. When the User is administering the module over the Web GUI, they perform all the same services available in CLI ("standard" mode only services) and additionally, can query the FIPS mode status of the module in the Web GUI

.

	only. The User may monitor the health and status of the modules using SNMPv3. SNMPv3 privacy and authentication keys are assigned to a User and are not tied to the User's CLI and Web GUI credentials.

Descriptions of the services available to a Crypto Officer and User are described below in Table 8 and Table 9 respectively. For each service listed below, COs and Users are assumed to already have authenticated prior to attempting to execute the service. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

- R: The CSP is read
- W: The CSP is established, generated, modified, or zeroized

2.4.1 Crypto-Officer Role

Descriptions of the services available to the Crypto-Officer role are provided in the table below.

Table 8 Crypto Officer Role Services and CSP Access

Service	Description	CSP and Access Required
Set up the module	Set up the first-time network configuration, CO username and password, and enable the module in the FIPS-approved mode of operation. For more information, see section 3.2.1 in the Security Policy.	CO Password – W "Enabled" mode password – W "Setup" Password – W
Enter the "enabled" mode	Manage the module in the "enabled" mode of operation, granting access to higher privileged commands	Enabled" mode password – R
* Enter the "configuration" mode	Manage the module in the "configuration" mode of operation, allowing permanent system modifications to be made	None
* Disable FIPS mode	Takes the module out of the FIPS-approved mode of operation, accessible only via the serial port	MAK – W SSH Session Key – W TLS Session Key – W
** Firmware Upgrade/Downgrade	Loads new external firmware and performs an integrity test using an RSA digital signature.	Integrity Test public key – R, W
Create remote management session (CLI)	Manage the module through the CLI (SSH) remotely via Ethernet port.	RSA public key – R RSA private key – R SSH Session Key – R, W
Create remote management session (Web GUI)	Manage the module through the GUI (TLS) remotely via Ethernet port.	RSA public key – R RSA private key – R TLS Session Key – R, W

.

Service	Description	CSP and Access Required
** 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 (Web GUI)	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 FIPS mode.	None
Show FIPS-mode status (Web GUI)	The CO logs in to the module using the Web GUI and navigates to the "Configuration" tab that will display if the module is configured in FIPS mode.	None
** Manage module configuration	Backup or restore the module configuration	RSA public key – R, W RSA private key – R, W SNMP Privacy Key – R, W SNMP Authentication Key – R, W CO Password – R, W User Password – R, W "Enabled" mode password – R, W
* Zeroize keys	Zeroize the MAK by taking the module out of FIPS-mode. This action initiates a reboot which zeroizes temporary session keys. The zeroization occurs while the module is still in FIPS-mode.	MAK – W SSH Session Key – W TLS Session 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 TLS Session Key – W

.

Service	Description	CSP and Access Required
* Reboot the module	Reboot the module.	SSH Session Key – W TLS Session Key – W
Create SNMPv3 session	Monitor the module using SNMPv3	SNMP Privacy Key – R SNMP Authentication Key – R

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

2.4.2 User Role

Descriptions of the services available to the User role are provided in the table below.

Table 9 User Services and CSP Access

Service	Description	CSP and Access Required
Create remote management session (CLI)	Manage the module through the CLI (SSH) remotely via Ethernet port.	RSA public key – R RSA private key – R SSH Session Key – R, W
Create remote management session (Web GUI)	Manage the module through the GUI (TLS) remotely via Ethernet port.	RSA public key – R RSA private key – R TLS Session Key – R, W
Create SNMPv3 session	Monitor the health of the module using SNMPv3	SNMP Privacy Key – R SNMP Authentication Key – R
Show FIPS-mode status (Web GUI)	The User logs in to the module using the Web GUI and navigates to the "Configuration" which will display if the module is configured in FIPS 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 FIPS mode.	None

2.4.3 Authentication Mechanism

COs and Users must authenticate using a user ID and password, SSH client key (SSH only), or certificates associated with the correct protocol in order to set up the secure tunnel. Secure sessions that authenticate for User services have no interface available to access other services (i.e. Crypto Officer services). Each CO or User SSH session remains active (logged in) and secured using the tunneling protocol until the

operator logs out. CO and User Web GUI sessions remain active until the operator logs out or inactivity for a configurable amount of time has elapsed.

Modules used by the United States Department of Defense (DoD) must meet Homeland Security Presidential Directive (HSPD)-12 requirements regarding the use of FIPS 201 validated Common Access Card (CAC) authentication for COs and Users connecting to management functionality of the module. Additionally, other agencies may require FIPS 201 validated PIV[1] II card authentication.

COs and Users connecting to the module through the Web GUI must first establish a TLS session. In order to facilitate TLS mutual authentication, the module requires a certificate to complete the handshake. The CO or User must select the X509 certificate on the CAC through the browser. The module authenticates the certificate against the Certificate Authority list that has been configured for the module to use. The module then issues the browser a certificate which is reviewed and accepted by the CO or User.

The module extracts the username field from the X509 certificate and the CO or User must provide the Personal Identification Number (PIN) associated with this username. The username field is grayed out ensuring that only the owner the CAC will be authenticating to the module. The CO and User PIN are sent to an external LDAP server where authorization occurs.

The authentication mechanisms used in the module are listed below in Table 10.

[1] PIV – Personal Identity Verification II

.

Table 10 Authentication Mechanisms Used by the Module

Role	Type of Authentication	Authentication Strength
Crypto-Officer	Password	The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (92) with repetition equates to a 1: (92^8), or 1: 5,132,188,731,375,616 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 (92) with repetition equates to a 1: (92^8), or 1: 5,132,188,731,375,616 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 (92) with repetition equates to a 1: (92^4), or 1: 71,639,296 chance of false acceptance. This password is entered by the Crypto-Officer and is required when using the serial port to access the CLI.
	Public keys	The module supports using RSA keys for authentication of Crypto-Officers during TLS or SSH. Using conservative estimates and equating a 1024 bit RSA key to an 80 bit symmetric key, the probability for a random attempt to succeed is 1:2^{80} or 1: 1,208,925,819,614,629,174,706,176.

.

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 (92) with repetition equates to a 1: (92^8), or 1: 5,132,188,731,375,616 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 or SSH. Using conservative estimates and equating a 1024 bit RSA key to an 80 bit symmetric key, the probability for a random attempt to succeed is 1:2^{80} or 1: 1,208,925,819,614,629,174,706,176.

2.5 Physical Security

The ProxySG 600 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 Section3.1.1.2. The labels and baffles are part of the FIPS Security Kit (Part Number: 085-02762).

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 Operational Environment

The operational environment requirements do not apply to the ProxySG 600 Appliance. The module does not provide a general purpose operating system nor does it allow operators the ability to load untrusted software. 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 11 below.

.

Table 11 FIPS-Approved Algorithm Implementations

Algorithm	Firmware Implementation Certificate Number	Hardware Accelerator Card		
		Appliance	Card	Certificate Number
Symmetric Key Algorithms				
AES: ECB[2], CBC[3], OFB[4], CFB[5]-128 bit mode for 128-, 192-, and 256-bit key sizes	1875	600	CN501	105
Triple-DES[6]: ECB, CBC, CFB-64, OFB mode for keying option 1 (3 different keys)	1218	600	CN501	217
Asymmetric Key Algorithms				
RSA PKCS[7]#1 sign/verify – 1024-, 1536-, 2048-bit	956	N/A	N/A	
Hashing Functions				
SHA[8]-1	1648	N/A	N/A	
SHA-224, SHA-256, SHA-384, SHA-512	1648	N/A	N/A	
Message Authentication Code (MAC) Functions				
HMAC[9] with SHA-1	1120	N/A	N/A	
HMAC with SHA-2	1120	N/A	N/A	
Deterministic Random Bit Generator (DRBG)				
SP[10] 800-90 Hash-Based DRBG (SHA-256)	153	N/A	N/A	

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

- RSA PKCS#1 wrap/unwrap (key-wrapping) – 1024, 1536, and 2048–bit sizes providing 80, 92, and 112-bits of security.
- Non Deterministic RNG (NDRNG) for seeding the FIPS-Approved RNG (SP 800-90 Hash-Based DRBG)

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

.

The module supports the CSPs listed below in Table 12.

Table 12 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 Approved FIPS RNG.	Never exits the module	Stored in plaintext	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 Imported in plaintext via a directly attached cable to the serial port	Never exits the module	Stored in plaintext	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	1024, 1536, and 2048-bits	Modules' public key is internally generated via Approved FIPS RNG. Other entities' public keys are sent to the module in plaintext. Modules' public key can be imported from a back-up configuration.	Output during TLS/SSH negotiation in plaintext. Exits in encrypted format when performing a module configuration backup.	Modules' public key is stored on non-volatile memory. Other entities' public keys reside on volatile memory.	Modules' public key is deleted by command. Other entities' public keys are cleared by power cycle.	Negotiating TLS or SSH sessions

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
RSA Private Key	1024, 1536, and 2048-bits	Internally generated via Approved FIPS RNG. 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
TLS or SSH Session Key	AES CBC 128-, 192-, or 256-bit key TDES CBC keying option 1 (3 different keys)	Internally generated via Approved FIPS RNG.	Output in encrypted form during TLS or SSH protocol handshake	Stored in plaintext on volatile memory	Rebooting the modules	Encrypting TLS or SSH data
Crypto-Officer Password User Password	Minimum of eight (8) and maximum of 64 bytes long printable character string	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 in encrypted form via a secure TLS or SSH 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 GUI 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	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 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.	Imported in plaintext via a directly attached cable to the serial port.	Never exits the module.	Stored in encrypted form on non-volatile memory.	Inaccessible by zeroizing 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	Encrypting SNMPv3 packets.
SNMP Authentication Key	HMAC-SHA-1-96 – bit key	Externally generated, Imported in encrypted form via a secure TLS or SSH session 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	Authenticating SNMPv3 packets.
SP 800-90 Hash-Based DRBG Entropy[12]	160-bit random number	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules	Seeding the FIPS-approved DRBG

[12] The Entropy used by the FIPS-Approved SP 800-90 Hash-Based DRBG is acquired using a non-Approved NDRNG.

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SP 800-90 Hash-Based DRBG V value	Internal hash DRBG state value	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules	Used for the SP 800-90 Hash-Based DRBG
SP 800-90 Hash-Based DRBG C value	Internal hash DRBG state value	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules	Used for the SP 800-90 Hash-Based DRBG

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: Triple-DES CBC mode, AES-128 CBC mode, or AES-256 CBC mode.

2.8 Self-Tests

If any of the hardware accelerator cards self-tests fail, then the module forces the corresponding card to enter an error state, logs the error to a file, and shuts down the card. The modules will only use the cryptographic implementations found in the software. If any of the software 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:
```

NOTE: The menu options presented here are not functional and a reboot must be executed by entering the "^X^C" command (accomplished by typing *Control* + *X* followed by *Control* + *C*).

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

2.8.1 Power-Up Self-Tests

The ProxySG 600 Appliance performs the following self-tests using the OpenSSL software implementation at power-up:

- Firmware integrity check using SHA-512
- Known Answer Tests (KATs)
  - AES KAT
  - Triple-DES KAT
  - RSA digital signature generation KAT
  - RSA digital signature verification KAT
  - SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 KATs
  - HMAC KAT with SHA-1
  - HMAC KAT with SHA-2
  - DRBG KAT
- Pairwise Consistency Test for RSA key wrapping (wrap/unwrap)

Upon successful completion of the software implementation self-tests, the ProxySG 600 performs the following self-tests on the hardware acceleration card:

- AES-CBC KAT
- Triple-DES KAT

If the hardware acceleration card self-tests pass, further execution of these algorithms will take place in the hardware implementation.

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

.

2.8.2 Conditional Self-Tests

The ProxySG 600 performs the following conditional self-tests, only on its firmware implementation of OpenSSL:

Table 13 ProxySG 600 Conditional Self-Tests

Conditional Self-Test	Occurrence
Firmware upgrade/downgrade (RSA sign/verify)	This test is run when the firmware is upgraded or downgraded. An RSA digital signature verification is performed over the firmware. If the verification succeeds, the test succeeds; otherwise it fails.
RSA pairwise consistency test	This test is run upon generation of an RSA key pair for key transport. The public key is used to wrap a block of data, and the resultant ciphertext is compared with the original data. If they are the same, the test fails. If they differ, then the private key is used to unwrap the ciphertext, and the resultant plaintext is compared to the original data. If they are the same, the test passes. Otherwise, it is failed.
Continuous RNG Test (CRNGT) for the FIPS-Approved DRBG	This test is run upon generation of random data by the DRBG to detect failure to a constant value.
CRNGT for the non-Approved NDRNG	This test is run when the DRBG is requesting entropy. When entropy has been gathered, this test compares the collected entropy with the previously collected entropy. If they are equal, the test fails. If they differ, the newly collected entropy is returned to be used by the DRBG.

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 600 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: 085-02762) consists of the following items as shown below in Figure 4.

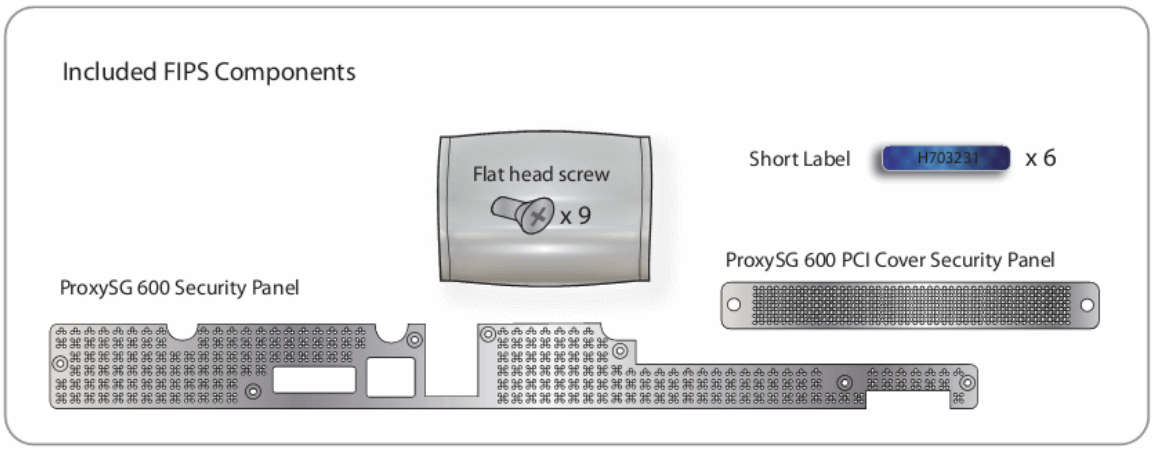

Figure 4 FIPS Security Kit Contents

Note: There are six (6) 'Short Labels' included; however, only three (3) are required for FIPS compliance. There are three additional labels provided.

A hard copy of the guidance found below in section 3.1.1.2 is also included in the kit in a documents titled *"ProxySG 600 Series, FIPS Compliance Guide: Tamper Evident Panel and Label Installation, Rev B.0".*

3.1.1 Label and Baffle Installation Instructions

The Crypto-Officer is responsible for applying the tamper-evident labels at the client's deployment site. 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 leaves 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 finger tip 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 Baffle Installation

1. The rear baffle and PCI cover (ProxySG 600 Security Panel and ProxySG 600 PCI Cover Security Panel respecvtively as shown in Figure 4) are designed to prevent unauthorized access to key system components by shielding the rear ventilation outlets. Note: The PCI cover is only used in appliances without an option card.
2. To install the rear baffle, align the security panel mounting points against the screw locations shown below in Figure 5 with seven (7) flat-head screws.

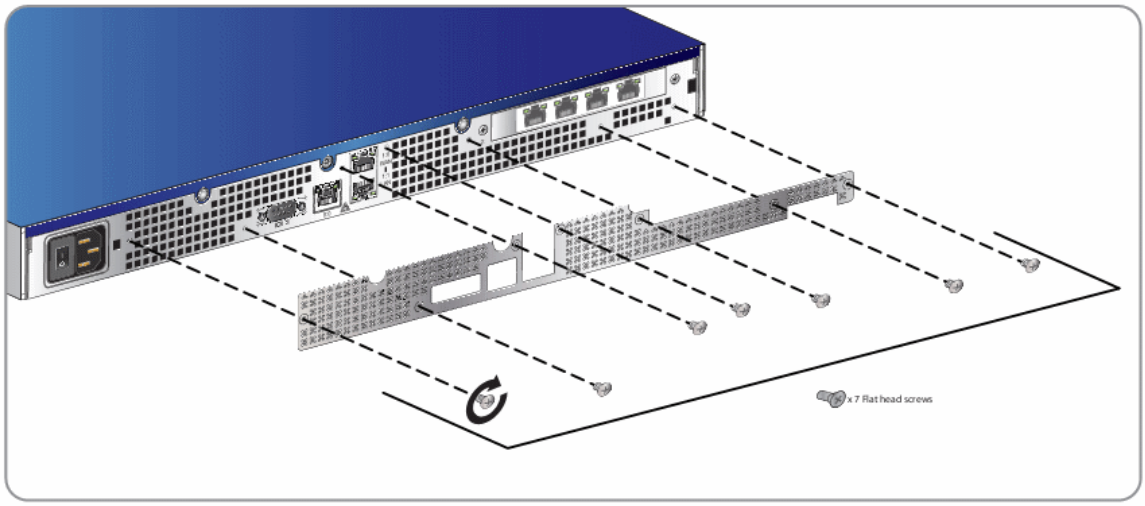

Figure 5 Rear Baffle Installation

3. Install the PCI cover as shown in Figure 6 if you do not have an option card installed in your appliance. To install the PCI cover, you must:

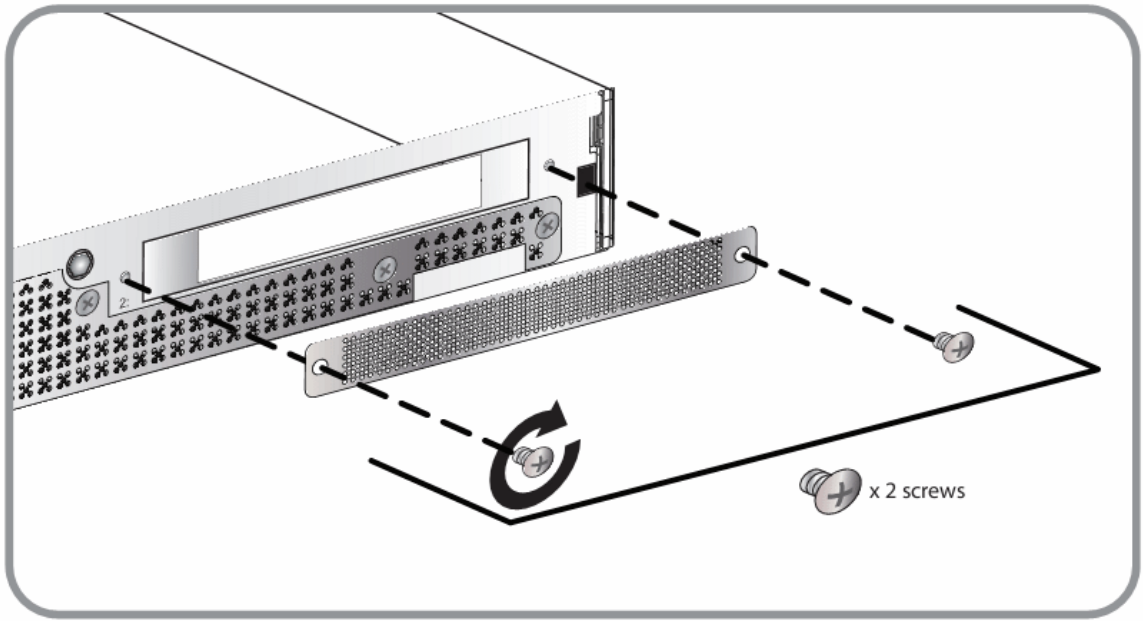

Figure 6 PCI Cover Installation

a. Remove the chassis cover from the appliance

b. Remove the PCI slot plate by supporting it using one hand and removing both screws.

c. Align the PCI slot plate against the chassis interior and install the PCI cover using two screws.

d. Reinstall the appliance cover.

3.1.1.2 Label Installation

The tamper-evident 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 text pattern on the label. Figure 7 below illustrates the tamper-evident features of the label.

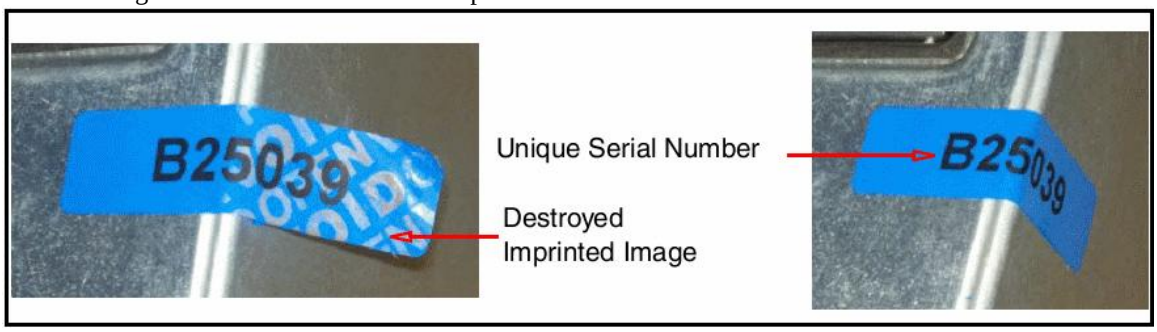

Figure 7 Label Showing Tamper Evidence

1. Use alchohol swabs to clean the label location surface using Isopropyl Alchohol (99%); this ensures complete adhesion. Verify that all the surfaces are dry before applying the labels.
2. Set the appliance on a flat, slip-proof work space and make sure you have access to all sides of the appliance.
3. Apply one (1) label vertically over a section of the rear baffle, across the center of the PCI cover, and over the top edge of the appliance as shown below in Figure 8.

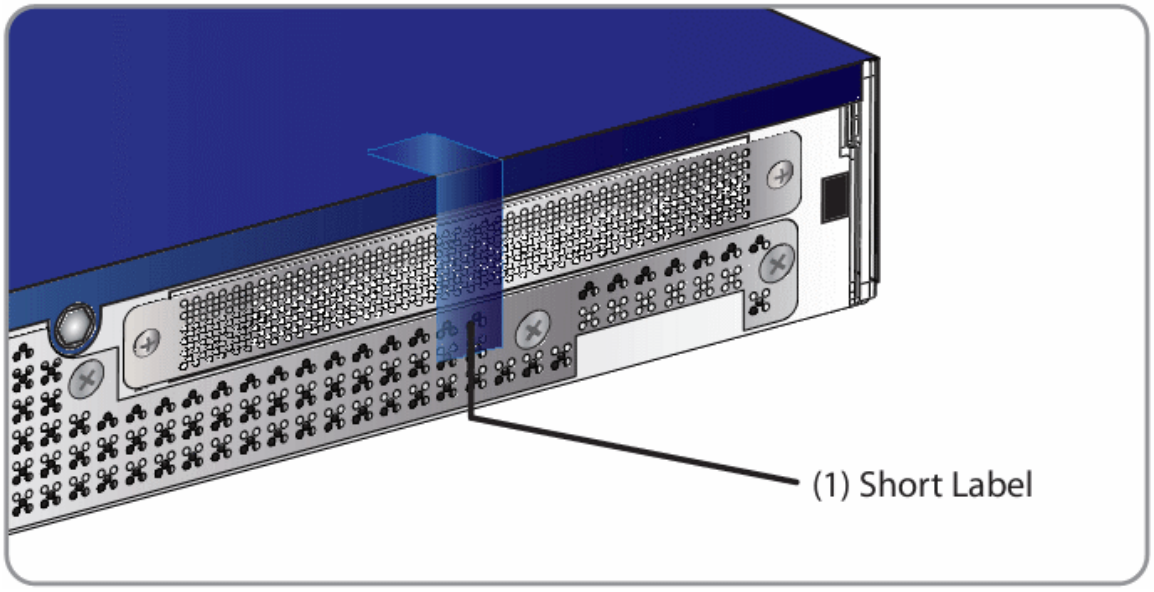

Figure 8 Tamper Evident Label Placement over the PCI Cover

4. Apply two (2) labels to the rear baffle on the left side of the appliance as shown below in Figure 9.

- Apply one (1) label vertically over the upper-left (when looking from the rear of the appliance) flush mount hexagonal insert and the rear baffle. Make sure the label does not interfere with any of the vents; the remaining label material crosses over the top edge of the appliance.

- Apply one (1) label vertically over the lower-left corner of the rear baffle. The label should cover the bottom 2 rows, across two columns of venitalation holes. The remaining label material crosses over the bottom edge of the appliance

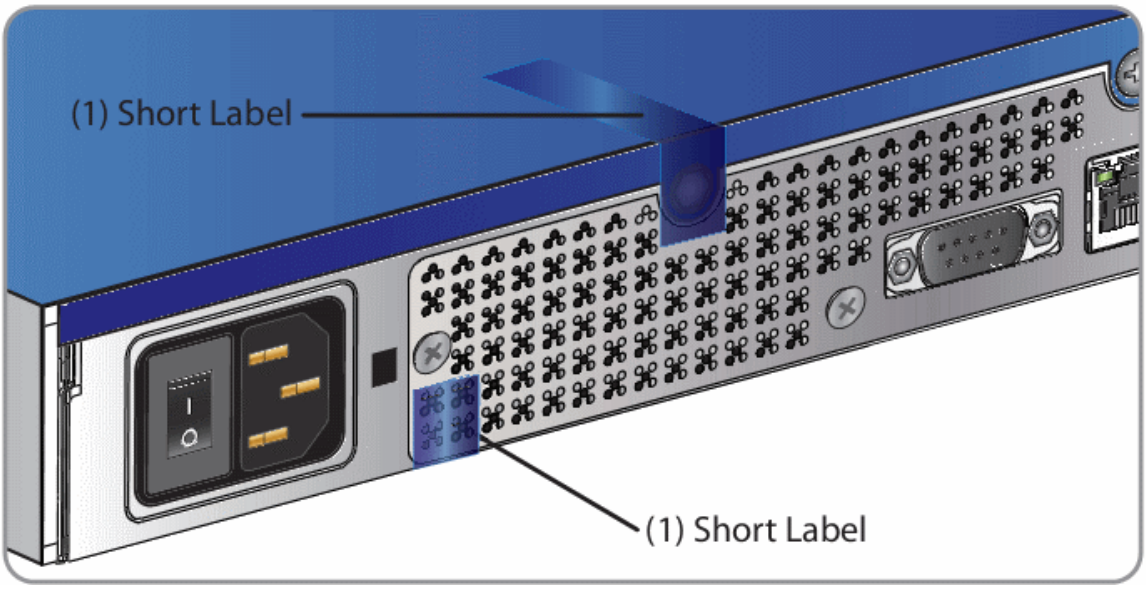

Figure 9 Tamper Evident Label Placement on Left Rear of Appliance

5. Rack mount the appliance being cautious not to damage the labels during the mounting process.
6. Reinstall the power cables.
7. Reinstall the network cables
8. Power-on the appliance.

3.2 Secure Management

3.2.1 Initialization

The module needs to have a minimal first-time configuration in order to be accessed by a web browser. The process of establishing the initial configuration via a secure serial port is described below. Physical access to the module shall be limited to the Cryptographic Officer. Therefore, the CO is the only operator that can put the module into the FIPS-approved mode as it requires physical access to the module.

- PC: Connect a serial cable to a serial port on 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 described in Table 14.

.

Table 14 RS232 Parameters

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

Power on the module and wait for the system to finish booting.

- Press <Enter> three times.
- When the "Welcome to the ProxySG Appliance Setup Console" prompt appears, the system is ready for the first-time network configuration.
- Set up the first time configuration by entering the interface number, IP address, IP subnet mask, IP gateway, DNS server parameters, username, and password.
- In addition to configuring the Internet Protocol service, the modules FIPS-Approved mode of operation must also be enabled (default is disabled). Setting the FIPS-Approved mode to "enabled" ensures that all security functions used are FIPS-Approved. The module will transition to the FIPS-Approved mode when the Cryptographic Officer enters the "enabled" mode on the CLI followed by the "fips-mode enable" command. The entry of this command causes the device to power cycle and Zeroize the Master Appliance Key. **NOTE:** This command is only accepted via the CLI when accessed over the serial port.
- Once the module has completed the power cycle to operate in FIPS mode, the administrator user name, administrator password and the "enabled mode" password all must be configured.
    - "You must configure the console user account now.
      Enter console username:
      Enter console password:
      Enter enable password:
- The administrator must configure the setup password to secure the serial port which must be configured while in FIPS mode. The module will prompt the following:
    - "The serial port must be secured and a setup password must be configured.
      Enter setup password: "
- Finally, the licensing mode must be selected when the module prompts the following options:
    - M)ACH5 Edition
    - P)roxy Edition

3.2.2 Management

The Crypto-Officer is able to monitor and configure the module via the Web GUI (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, then 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 12. Key sizes less than what is specified shall not be used while in the FIPS-Approved mode of operation. The CO password and "enabled" mode password must be at least 8 characters in length. The "Setup" password must be at least 4 characters in length.

When creating or importing key pairs, such as during the restoration of an archived ProxySG configuration, the CO must ensure that the "Do not show key pair" option is selected in the Web GUI as shown in Figure 10, or the "no-show" argument is passed over the CLI as shown in Figure 11. Please see Section E: Preparing Archives for Restoration on New Devices in the Blue Coat Systems SGOS Administration Guide, Version 6.1 for further reference.

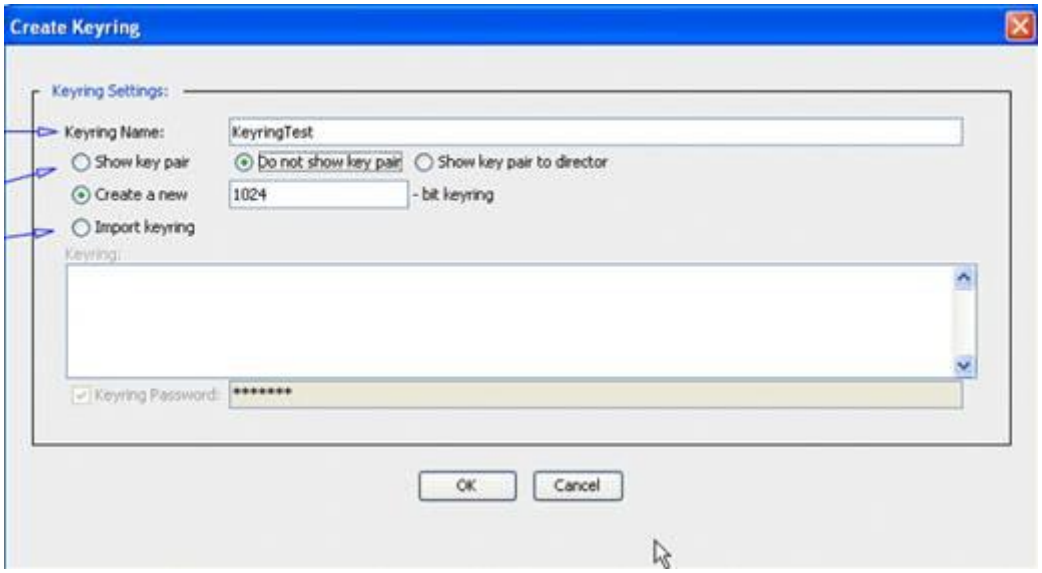

Figure 10 Keyring Creation Web GUI Dialogue Box

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 11 Keyring Creation CLI Commands

The module can only be taken out of FIPS-Approved mode when accessing the CLI over the serial port. The CO must enter the "enabled" mode on the CLI before the FIPS-approved mode can be enabled or disabled. A CLI command ("fips-mode enable/disable") will allow FIPS-approved mode to be enabled or disabled. To ensure that CSPs are not shared across FIPS-Approved mode and Non-Approved mode, any change to the FIPS-Approved mode parameter will trigger a zeroization of the Master Appliance Key and

force the module to power cycle. The FIPS-Approved mode parameter will not be modified until after the Master Appliance Key and power-cycle has completed.

3.2.3 Zeroization

At the end of its life cycle or when taking the module out of FIPS-Approved mode, the module must be fully zeroized to protect CSPs. When switching between FIPS-Approved mode and non- FIPS-Approved mode, the module automatically reboots and zeroizes 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 modules causes all temporary keys (SSH Session key, TLS session key, and the hash-based DRBG entropy) 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 modules remotely via SSH (CLI) or HTTPS (Web GUI). 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 15 Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standard Institute
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
CO	Crypto-Officer
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CX4	Four pairs of twin-axial copper wiring
DES	Data Encryption Standard
DNS	Domain Name System
DoD	Department of Defense
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	Hash-Based Message Authentication Code
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IM	Instant Messaging

.

Acronym	Definition
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
PIV	Personal Identity Verification
RC2	Rivest Cipher 2
RC4	Rivest Cipher 4
RS-232	Recommended Standard 232
RSA	Rivest Shamir Adleman
RTSP	Real-Time Streaming Protocol
SFTP	Secure File Transfer Protocol
SGOS	Secure Gateway Operating System
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SOCKS	Sock-Et-S
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
VoIP	Voice Over Internet Protocol
WAN	Wide Area Network

Prepared by:
Corsec Security, Inc.

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

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