

Blue Coat Systems, Inc.

ProxySG 9000 Appliance

Models: ProxySG 9000-10, 9000-20, 9000-20B

Hardware Versions: 090-02844, 090-02843, 090-02840, 090-02839, 090-02984, 090-02985

Firmware Versions: 5.5, 5.5.7.2

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2

Document Version: 1.2



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

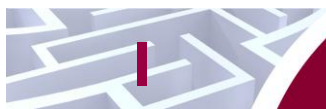
1	INTRODUCTION	4
1.1	PURPOSE	4
1.2	REFERENCES.....	4
1.3	DOCUMENT ORGANIZATION.....	4
2	PROXYSG 9000 APPLIANCE	5
2.1	OVERVIEW.....	5
2.2	MODULE SPECIFICATION	7
2.3	MODULE INTERFACES.....	8
2.4	ROLES AND SERVICES.....	11
2.4.1	<i>Crypto-Officer Role.....</i>	<i>12</i>
2.4.2	<i>User Role.....</i>	<i>14</i>
2.4.3	<i>Authentication Mechanism.....</i>	<i>14</i>
2.5	PHYSICAL SECURITY	17
2.6	OPERATIONAL ENVIRONMENT.....	17
2.7	CRYPTOGRAPHIC KEY MANAGEMENT	17
2.8	SELF-TESTS.....	23
2.8.1	<i>Power-Up Self-Tests.....</i>	<i>23</i>
2.8.2	<i>Conditional Self-Tests.....</i>	<i>24</i>
2.9	MITIGATION OF OTHER ATTACKS.....	24
3	SECURE OPERATION	25
3.1	INITIAL SETUP	25
3.1.1	<i>Label and Baffle Installation Instructions.....</i>	<i>26</i>
3.2	SECURE MANAGEMENT	31
3.2.1	<i>Initialization.....</i>	<i>31</i>
3.2.2	<i>Management.....</i>	<i>33</i>
3.2.3	<i>Zeroization.....</i>	<i>34</i>
3.3	USER GUIDANCE.....	34
4	ACRONYMS	35

Table of Figures

FIGURE 1	TYPICAL DEPLOYMENT OF A PROXYSG APPLIANCE.....	5
FIGURE 2	PROXYSG 9000 (FRONT VIEW).....	7
FIGURE 3	PROXYSG 9000 (FRONT PANEL OPEN).....	8
FIGURE 4	CONNECTION PORTS AT THE REAR OF THE PROXYSG 9000	9
FIGURE 5	FIPS SECURITY KIT CONTENTS.....	25
FIGURE 6	INSTALLED LOUVERED SHUTTERS AND TAMPER EVIDENT LABELS.....	26
FIGURE 7	LARGE LOUVER ALIGNMENT	27
FIGURE 8	SMALL LOUVER ALIGNMENT.....	27
FIGURE 9	LABEL SHOWING TAMPER EVIDENCE.....	28
FIGURE 10	TAMPER EVIDENT LABELS FOR POWER SUPPLIES	28
FIGURE 11	TAMPER EVIDENT LABEL APPLICATION – RIGHT SIDE OF LARGE LOUVERED SHUTTER.....	29
FIGURE 12	TAMPER EVIDENT LABEL APPLICATION – SMALL LOUVERED SHUTTER.....	29
FIGURE 13	TAMPER EVIDENT LABEL APPLICATION – TOP SIDE OF LARGE LOUVERED SHUTTER	30
FIGURE 14	TAMPER EVIDENT LABEL APPLICATION – TOP AND SIDE OF APPLIANCE	30
FIGURE 15	FRONT BEZEL LABEL APPLICATION POINTS.....	31
FIGURE 16	KEYRING CREATION WEB GUI DIALOGUE BOX	33
FIGURE 17	KEYRING CREATION CLI COMMANDS.....	33

List of Tables

TABLE 1 SECURITY LEVEL PER FIPS 140-2 SECTION	6
TABLE 2 PROXYSG 9000 APPLIANCE CONFIGURATIONS	7
TABLE 3 FIPS 140-2 LOGICAL INTERFACE MAPPINGS FOR THE FRONT OF THE PROXYSG 9000-10/20	8
TABLE 4 FRONT PANEL LED STATUS INDICATIONS FOR THE PROXYSG 9000	8
TABLE 5 FIPS 140-2 LOGICAL INTERFACE MAPPINGS FOR THE REAR OF THE PROXYSG 9000.....	10
TABLE 6 REAR PANEL LED STATUS INDICATIONS FOR THE PROXYSG 9000	10
TABLE 7 FIPS AND PROXYSG ROLES.....	11
TABLE 8 CRYPTO OFFICER ROLE SERVICES AND CSP ACCESS.....	12
TABLE 9 USER SERVICES AND CSP ACCESS	14
TABLE 10 AUTHENTICATION MECHANISMS USED BY THE MODULE.....	16
TABLE 11 FIPS-APPROVED ALGORITHM IMPLEMENTATIONS	17
TABLE 12 LIST OF CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPs	19
TABLE 13 PROXYSG 9000 CONDITIONAL SELF-TESTS	24
TABLE 14 RS232 PARAMETERS.....	32
TABLE 15 ACRONYMS.....	35



Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the ProxySG 9000 Appliance (Models: ProxySG 9000-10, 9000-20, 9000-20B; Firmware Versions: 5.5, 5.5.7.2) from Blue Coat Systems, Inc.. This Security Policy describes how the ProxySG 9000 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 module 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 9000 Appliance is referred to in this document as *ProxySG 9000*, *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 9000 Appliance

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.

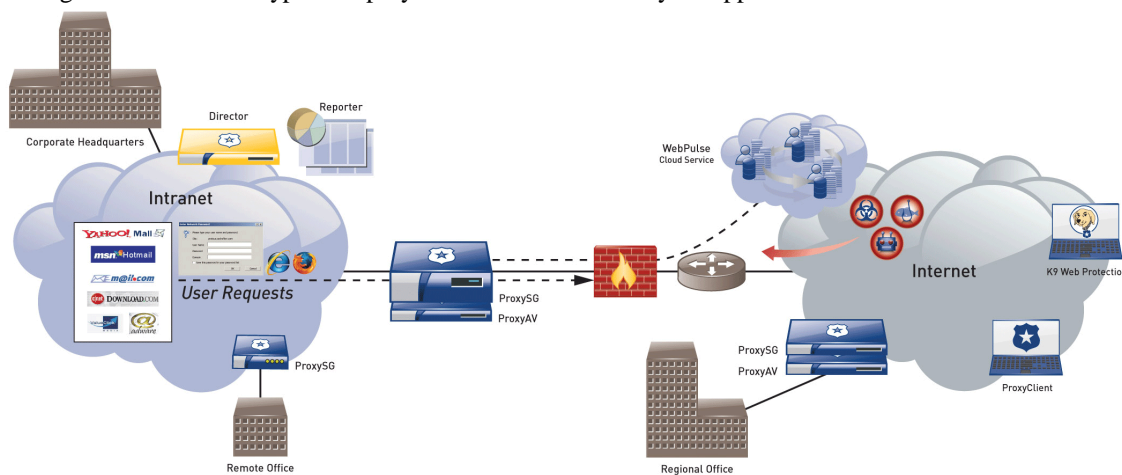


Figure 1 Typical Deployment of a ProxySG Appliance

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 configuration 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)
- Messaging Application Programming Interface (MAPI)
- 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 9000 Appliance is validated at the following FIPS 140-2 Section levels:

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 9000 Appliance Configurations

Model	Hardware Version	
	Proxy Edition	MACH5 Edition
ProxySG 9000-10	090-02844	090-02843
ProxySG 9000-20	090-02840	090-02839
ProxySG 9000-20B	090-02984	090-02985

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 Blue Coat ProxySG 9000 Appliance is the high-end proxy appliance platform, providing even the largest enterprises with accelerated web communications. Located at the Internet gateway, the ProxySG 9000 Appliance platform enables effective control of the enterprise's Internet traffic. The ProxySG 9000 Appliance has 1 Liquid Crystal Display (LCD) and 2 Light Emitting Diodes (LEDs) at the front of the module as shown in Figure 2.



Figure 2 ProxySG 9000 (Front View)

The front panel of the module can be opened as shown in Figure 3. When open, the LCD and 2 LEDs remain visible. Additionally, the open front panel exposes a power button, control buttons, and disk drive bays (NOTE: the front panel cannot be opened due to tamper evident labels placed on the front panel eliminating access to the control buttons and disk drive bays when operating in FIPS mode). The module can accept up to ten hard disk drives, which are used to store logs, configuration data, and System Files. Section 3 of this document provides guidance on how to apply tamper-evident labels on this module.



Figure 3 ProxySG 9000 (Front Panel Open)

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

- ProxySG 9000-10/20 with a Cavium CN1620 Security Macro Processor

The ProxySG 9000 Appliance 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 9000 Appliance is defined by the appliance chassis, which surrounds all the hardware and software. The module Firmware, versions 5.5 and 5.5.7.2, contains the SGOS 5.5 Cryptographic Library version 1.12.1.

2.3 Module Interfaces

The front panel of the ProxySG 9000 is shown in Figure 2. When the module is running, there are 2 LEDs that provide status output that are visible through the front bezel.

The type and quantity of all ports present in the front panel of the ProxySG 9000 is given in Table 3.

Table 3 FIPS 140-2 Logical Interface Mappings for the front of the ProxySG 9000-10/20

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 front of the ProxySG 9000 are described in Table 4.

Table 4 Front Panel LED Status Indications for the ProxySG 9000

LED	Color	Definition
Power LED (The left LED when facing module)	OFF	Powered off.
	AMBER	Loading the OS.
	FLASHING AMBER TO GREEN	Unconfigured.
	GREEN	Powered on and configured.

System LED (The right LED when facing module)	OFF	10 Mbps speed connection is present.
	GREEN	Healthy.
	AMBER	Warning.
	RED	Critical Warning.
	BLUE	Diagnostic Mode.

The rear of the ProxySG 9000 is shown in Figure 4 below.

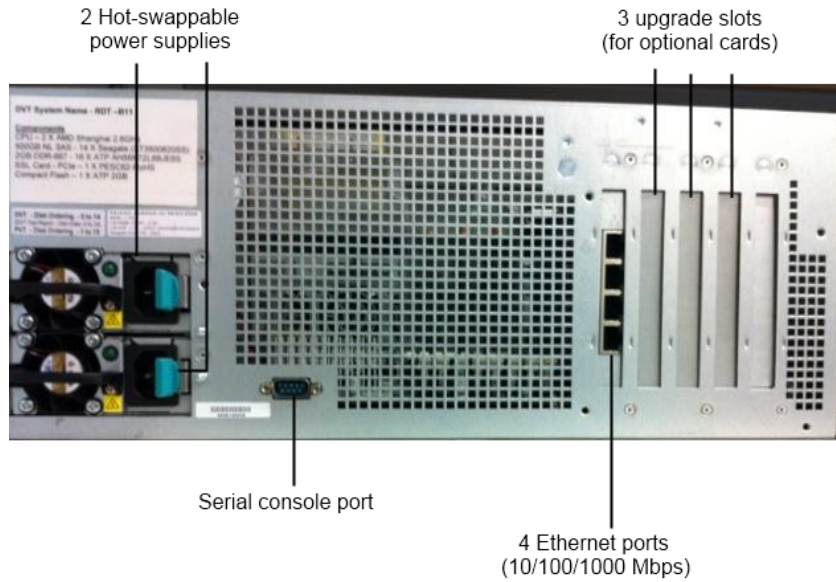


Figure 4 Connection Ports at the Rear of the ProxySG 9000

The ProxySG 9000 connection ports are located at the rear of the unit. Those connections are:

- Four Ethernet Interfaces: Four integrated 10/100/1000 Mbps onboard through a network riser card for high-speed connections. The module is shipped by default from the factory with this card installed on the custom slot labeled 0.
- Serial port: The serial port connects to a Personal Computer (PC).
- Three upgrade slots (labeled 1-3) for additional network cards. Slots can be used for a four port 1Gb copper card, a four port 1Gb fiber card, or a two port 10Gb copper card (CX4¹ interface). The other slots are for the pre-installed network riser card (slot 0) and pre-installed SSL accelerator card (slot 4).
- Two hot-swappable AC power supplies with power connectors. When configured in the FIPS-approved mode of operation, there is tamper evident labels over the two power supplies restricting them from being removed.

The type and quantity of all ports present in rear panel of the ProxySG 9000 are given in Table 5.

Table 5 FIPS 140-2 Logical Interface Mappings for the rear of the ProxySG 9000

Physical Port/Interface	Quantity	FIPS 140-2 Interface
Network ports	4	<ul style="list-style-type: none"> • Data Input • Data Output • Control Input • Status Output
Serial port	1	<ul style="list-style-type: none"> • Control Input • Status Output
Ethernet Interface – Speed LEDs	4	<ul style="list-style-type: none"> • Status Output
Ethernet Interface – Activity LEDs	4	<ul style="list-style-type: none"> • Status Output
AC power connection LED	2	<ul style="list-style-type: none"> • Status Output
AC power connection	2	<ul style="list-style-type: none"> • Power Input

The status indications provided by the LEDs on the rear of the ProxySG 9000 are described in Table 6.

Table 6 Rear Panel LED Status Indications for the ProxySG 9000

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

¹ Four pairs of twin-axial copper wiring

2.4 Roles and Services

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

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

- CLI – accessible 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
** Create, edit, and delete operator groups	Create, edit and delete operator groups; define common sets of operator permissions.	None

Service	Description	CSP and Access Required
** 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 into or 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
* Reboot the module	Reboot the module.	SSH Session Key – W TLS Session Key – W

Service	Description	CSP and Access Required
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 PIV² 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 is sent to an external LDAP server where authorization occurs.

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

² 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.

Role	Type of Authentication	Authentication Strength
User	Password	The modules support password authentication internally. For password authentication done by the modules, passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (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 9000 Appliance is multi-chip standalone cryptographic module and is enclosed in a hard, opaque metal case that completely encloses all of the internal components. There are only a limited set of vent holes provided in the case, and these holes obscure the view of the internal components of the module. Tamper-evident labels are applied to the case to provide physical evidence of attempts to remove the case of the module. The Crypto-Officer is responsible for the placement of tamper-evident labels and baffles and guidance can be found in section 3.1.1.2. The labels and baffles are part of the FIPS Security Kit (Part Number: 085-02718).

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 9000 Appliance. The module does not provide a general purpose operating system (OS) nor does it allow operators to load un-trusted software. The OS run by the cryptographic module is referred to as Secure Gateway Operating System (SGOS). SGOS is a proprietary real-time embedded OS.

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

Algorithm	Firmware Implementation Certificate Number	Hardware Accelerator Card		
		Appliance	Card	Certificate Number
Symmetric Key Algorithms				
AES: ECB ³ , CBC ⁴ , OFB ⁵ , CFB ⁶ -128 bit mode for 128-, 192-, and 256-bit key sizes	#1885	9000	CNI620	1265
Triple-DES ⁷ : ECB, CBC, CFB-64, OFB mode for keying option 1 (3 different keys)	#1224	9000	CNI620	898
Asymmetric Key Algorithms				
RSA PKCS ⁸ #1 sign/verify – 1024-, 1536-, 2048-, 3072-, 4096- bit	#962	N/A		N/A
Hashing Functions				
SHA ⁹ -1	#1656	N/A		N/A
Message Authentication Code (MAC) Functions				
HMAC ¹⁰ with SHA-1	#1127	N/A		N/A
Pseudo Random Number Generator (PRNG)				
ANSI ¹¹ x9.31 Appendix A.4.2 PRNG	#987	N/A		N/A

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

- RSA PKCS#1 wrapping/unwrapping (key-wrapping) – 1024, 1536, 2048, 3072, and 4096-bit sizes providing 80, 92, 112, 128, and 150-bits of security.
- Non Deterministic RNG (NDRNG) for seeding the FIPS-Approved RNG (ANSI X9.31 Appendix A.4.2 PRNG)
- MD5 (integrity checking)

³ ECB – Electronic Codebook

⁴ CBC – Cipher Block Chaining

⁵ OFB – Output Feedback

⁶ CFB – Cipher Feedback

⁷ DES – Data Encryption Standard

⁸ PKCS – Public Key Cryptography Standard

⁹ SHA – Secure Hash Algorithm

¹⁰ HMAC – Hash-Based Message Authentication Code

¹¹ ANSI – American National Standards Institute

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, 2048, 3072 and 4096-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, 2048, 3072 and 4096-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 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	Enters the module 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.	Enters the module in plaintext via a directly attached cable to the serial port.	Never exits the module.	Stored in encrypted form on non-volatile memory.	Inaccessible by zeroizing the encrypting MAK.	Used by the CO to secure access to the CLI when accessed over the serial port.
SNMP Privacy Key	AES CFB 128 -bit key	Externally generated, Imported in encrypted form via a secure TLS or SSH session Imported in plaintext via a directly attached cable to the serial port.	Exits the module encrypted over TLS or encrypted during a configuration backup.	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing the encrypting MAK	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.
ANSI X9.31 Appendix A.4.2 PRNG seed ¹²	160-bit random number	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules	Seeding the FIPS-approved PRNG

¹² The seed used by the FIPS-Approved ANSI X9.31 Appendix 4.2 PRNG is acquired using a non-Approved NDRNG.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
ANSI X9.31 Appendix A.4.2 PRNG key	112-bit random number	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules	Used to create the Master Appliance Key and SSH and TLS session keys

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 9000 performs the following self-tests using the OpenSSL software implementation at power-up:

- Firmware integrity check using MD5 Error Detection Code (EDC)
- Known Answer Tests (KATs)
 - AES KAT
 - Triple-DES KAT
 - RSA digital signature generation KAT
 - RSA digital signature verification KAT
 - SHA-1 KAT
 - HMAC KAT with SHA-1
 - PRNG KAT
- Pairwise Consistency Test for RSA key wrapping (wrap/unwrap)

Upon successful completion of the software implementation self-tests, the ProxySG 9000 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 9000 performs the following conditional self-tests, only on its firmware implementation of OpenSSL:

Table 13 ProxySG 9000 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 PRNG	This test is run upon generation of random data by the PRNG to detect failure to a constant value.
CRNGT for the non-Approved NDRNG	This test is run when the PRNG 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 PRNG.

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 9000 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: 085-02718) consists of the following items as shown below in Figure 5.






Name	Part
(4) Long Labels	 <p>Note: Two (2) long labels are required to secure the appliance. Additional labels are included for reapplication purposes.</p>
(14) Short Labels	 <p>Note: Seven(7) short labels are required to secure the appliance. Additional labels are included for reapplication purposes.</p>
(1) Large Louvered Shutter	
(1) Small Louvered Shutter	
(6) Flat-Head Screws	

Figure 5 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 document titled “ProxySG 9000 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 installing the baffle (security panel) and 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 seals. The Crypto-Officer is responsible for the direct control and observation of any changes to the module such as reconfigurations where the tamper evident seals 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 requirements when applying the tamper-evident labels:

- The minimum temperature of the environment must be 35-degrees Fahrenheit for the application of the tamper evident labels. After application, the labels’ temperature tolerance range in the operational environment is between -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 accidentally 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

The louvered shutters contained in the FIPS kit are designed to prevent unauthorized access to key system components by shielding the rear ventilation outlets. The kit includes one large shutter, which covers the primary ventilation outlet and a smaller shutter, which covers the secondary outlet. Both shutters are installed using the included flat-head screws. Figure 6 below shows the louvered shutters and security labels installed on a ProxySG 9000.

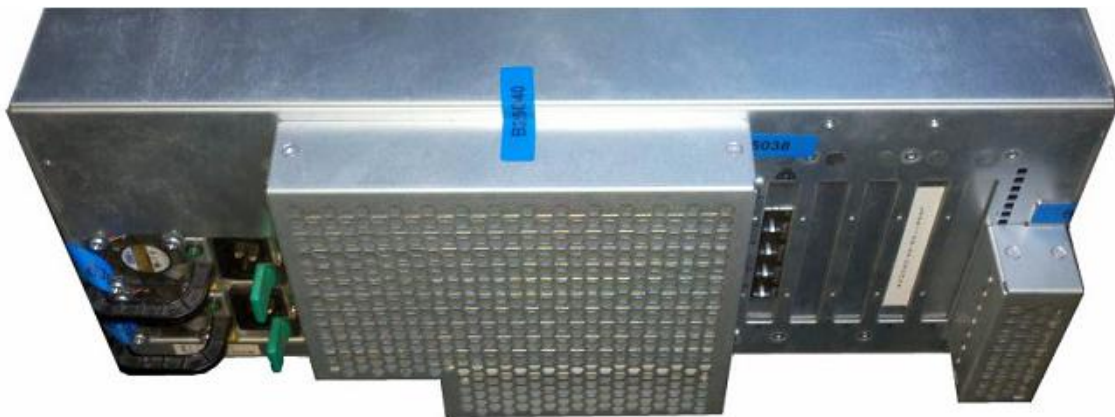
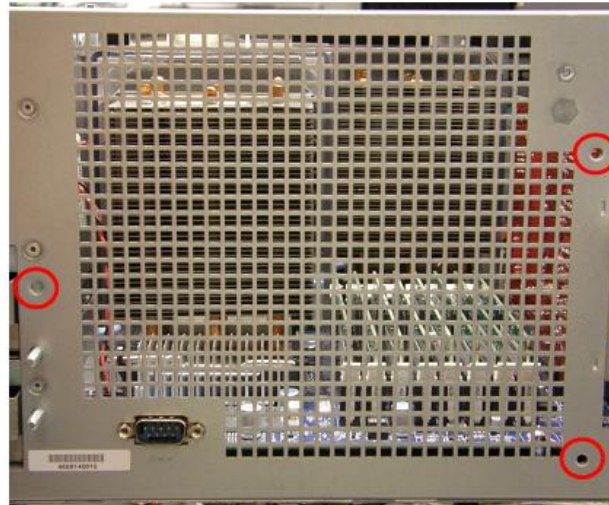


Figure 6 Installed Louvered Shutters and Tamper Evident Labels

1. Align the large louvered shutter mounting points against the screw locations and secure with three flat-head screws as shown below in Figure 7.

Step 1

Flat-Head Screw

**Figure 7 Large Louver Alignment**

- Align the small louvered shutter against the mounting points and secure with two flat-head screws.

Step 2

Flat-Head Screw

**Figure 8 Small Louver Alignment****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 9 below illustrates the tamper-evident features of the label.

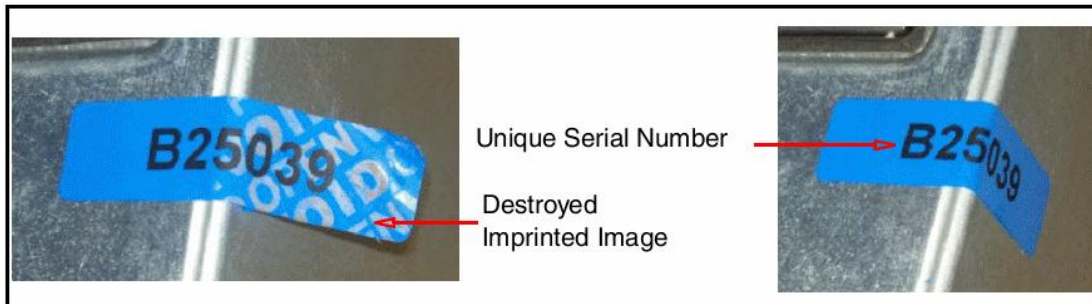


Figure 9 Label Showing Tamper Evidence

1. 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. Set the appliance on a flat, slip-proof work space and make sure you have access to all sides of the appliance.
2. Apply one long label over each power supply unit as shown below in Figure 10. When applying the labels, make sure there is enough material on both ends to properly secure the power supply!

Step 2

Long Label



x2



Figure 10 Tamper Evident Labels for Power Supplies

3. Apply one short label across the right side of the large louvered shutter and over the chassis. Be sure that the label covers both parts in equal amounts as shown below in Figure 11.

Step 3

Short Label **B25006**

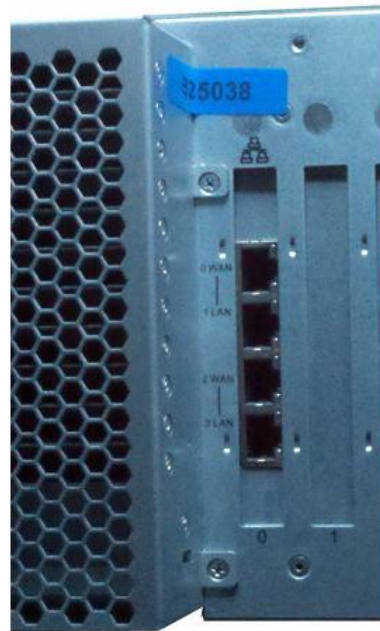


Figure 11 Tamper Evident Label Application – Right Side of Large Louvered Shutter

4. Apply one short label across and over the small louvered shutter mounting tab. Make sure it covers the entire mounting tab including the screw and extends over the right edge of the appliance as shown by Step 4 in Figure 12 below.

Step 4-5

Short Label **B25006** x2

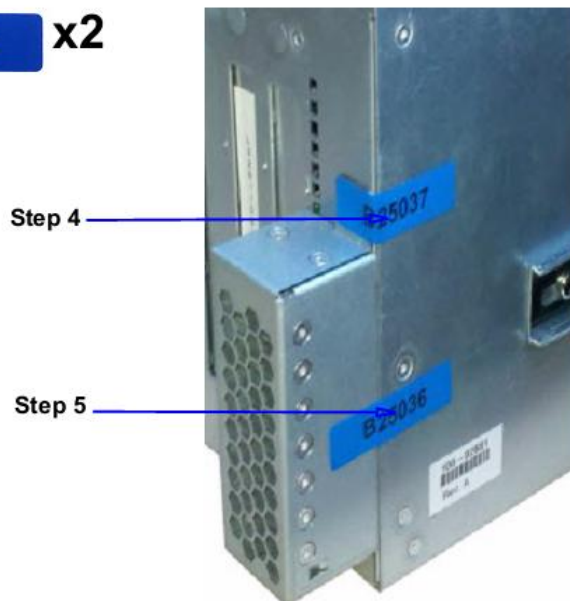


Figure 12 Tamper Evident Label Application – Small Louvered Shutter

5. Apply one short label across the center of the small louvered shutter. Make sure it covers both the small louvered shutter and extends over the right edge of the appliance as shown by Step 5 in Figure 12 above.
6. Apply one short label vertically over the large louvered shutter and over the top edge of the appliance as shown below in Figure 13. Make sure the label contacts all edges of the surfaces without any gaps.

Step 6

Short Label  x1

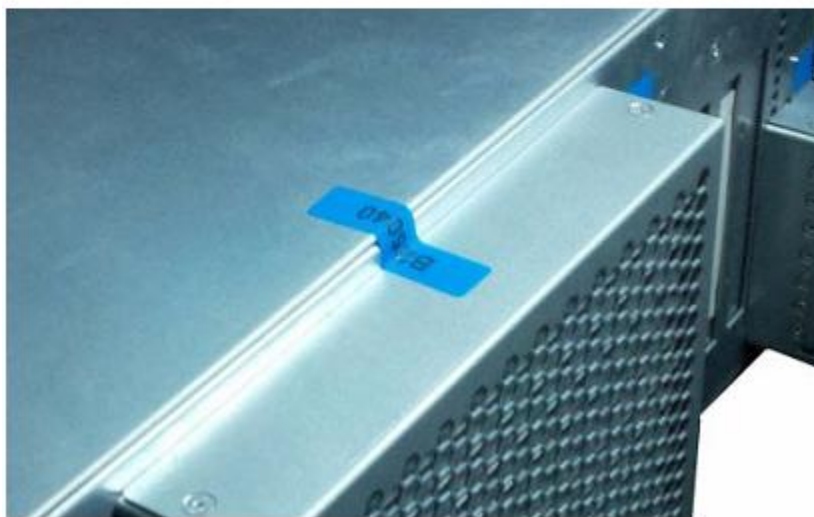


Figure 13 Tamper Evident Label Application – Top Side of Large Louvered Shutter

7. Apply one short label across the edge of the middle panel on the top of the appliance to secure the panel to the chassis. The label should be placed approximately 3/4" (three-quarters of an inch) beyond the release tab as shown below in Figure 14.

Step 7

Short Label  x1



Figure 14 Tamper Evident Label Application – Top and Side of Appliance

8. Rack mount the appliance being cautious not to damage the labels during the mounting process.
9. Reinstall the power cables.
10. Reinstall the network cables
11. Power-on the appliance.
12. Close the bezel.
13. Apply two (2) short labels across the chassis and bezel to prevent unauthorized access to the front panel and hard disk carriers. Each label should be placed on the opposite ends of the appliance, as shown below in Figure 15.

Step 13



Figure 15 Front Bezel Label Application Points

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

3.2 Secure Management

3.2.1 Initialization

The module needs to have a basic first-time configuration in order to be accessed by a web browser. The process of initial configuration via the 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 the 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), and verify that the port is set using the parameters described in the table below.

Table 14 RS232 Parameters

RS-232 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.
- The first-time network configuration sets up the Internet Protocol (IP) service configuration, including 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 module’s 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 16, or the "no-show" argument is passed over the CLI as shown in Figure 17. Please see Section E: Preparing Archives for Restoration on New Devices in the Blue Coat Systems SGOS Administration Guide, Version 5.5 for further reference.

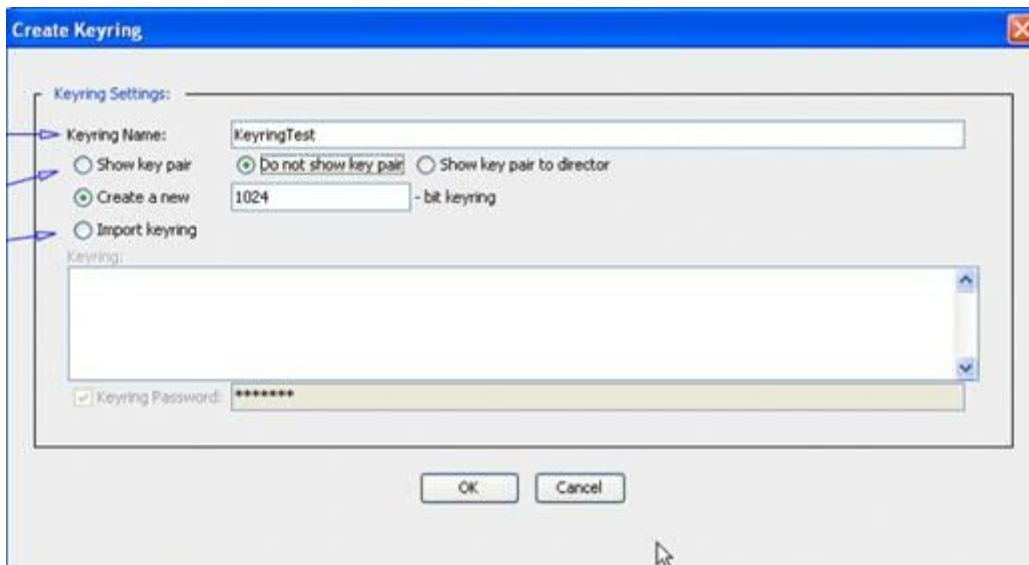


Figure 16 Keyring Creation Web GUI Dialogue Box

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 17 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 between FIPS-Approved mode and Non-Approved mode, any change between modes will trigger a zeroization of the Master Appliance Key and force the module to power cycle. The FIPS mode parameter will not be modified until after the Master Appliance Key has been regenerated and a power-cycle has completed.

3.2.3 Zeroization

At the end of its life cycle or when taking the module out of the FIPS-approved mode, the module must be fully zeroized to protect CSPs. When switching between the 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, ANSI x9.31 seed, and ANSI x9.31 key) 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
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
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
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IM	Instant Messaging
IP	Internet Protocol
KAT	Known Answer Test
LCD	Liquid Crystal Display
LED	Light Emitting Diode

Acronym	Definition
MAC	Message Authentication Code
MD5	Message Digest Algorithm 5
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OS	Operating System
P2P	Peer-to-Peer
PC	Personal Computer
PRNG	Pseudo Random Number Generator
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.

The logo for Corsec, featuring the word "Corsec" in a bold, red, serif font, centered within a white, horizontally-oriented oval that has a subtle 3D effect with a shadow on the bottom.

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>