# Blue Coat Systems, Inc.
# ProxySG8100

(Hardware Versions: 100-02644, 106-02835, and 106-02883 with Firmware Version: 5.3.1.9)

# FIPS 140-2
# Non-Proprietary Security Policy

**Level 2 Validation**

**Document Version 1.2**

Prepared for:

Prepared by:

**Blue Coat Systems, Inc.**

420 N. Mary Avenue
Sunnyvale, CA  94085
Phone: (866) 30.BCOAT (22628)
(408) 220-2200
Fax: (408) 220-2250
http://www.bluecoat.com

**Corsec Security, Inc.**

10340 Democracy Lane, Suite 201
Fairfax, VA  22030

Phone: (703) 267-6050

Fax: (703) 267-6810
http://www.corsec.com

## Revision History

| Version | Modification Date | Modified By | Description of Changes |
|---------|-------------------|-------------|------------------------|
| 0.1 | 2008-11-03 | Rumman Mahmud | Initial draft. |
| 0.2 | 2009-01-29 | Rumman Mahmud | Updated version. |
| 1.0 | 2009-01-30 | Rumman Mahmud | Updated version. |
| 1.1 | 2009-09-15 | J.McCally | Clarified statements in response to CMVP comments |
| 1.2 | 2009-10-26 | Darryl Johnson | Updated to address CMVP comments. |

# Table of Contents

# Table of Figures

# List of Tables

# 1   Introduction

## 1.1   Purpose

This is a non-proprietary Cryptographic Module Security Policy for the ProxySG8100 from Blue Coat Systems, Inc.. This Security Policy describes how the ProxySG8100 meet the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – Security Requirements for Cryptographic Module) details the U.S. and Canadian Government requirements for cryptographic module. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at: http://csrc.nist.gov/groups/STM/cmvp/index.html.

The ProxySG8100 is referred to in this document as the ProxySG, the hardware module, the cryptographic module, or the 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 (http://www.bluecoat.com) contains information on the full line of products from Blue Coat.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to 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 Machine
- Other supporting documentation as additional references

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

# 2  ProxySG8100

## 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.  The ProxySG is one of several appliance lines manufactured by Blue Coat Systems.  The ProxySG comes in several models, such as the 210, 510, 810, and 8100.  Differences between product models allow for different performance and scalability options, as shown in Figure 1 below.



**Figure 1 – ProxySG Appliance Performance vs. Scalability**

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 2 below for a typical deployment scenario for ProxySG appliances.

**Figure 2 – 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. Proxy edition of the ProxySG has been tested for FIPS 140-2. The MACH5 edition appliances have some proxy features disabled (as indicated below). The controlled protocols implemented in the evaluated configuration are:

- Secure Hypertext Transfer Protocol (HTTPS)
- Secure File Transfer Protocol (SFTP)
- Transmission Control Protocol (TCP) tunneling protocols such as Secure Shell version 2.0 (SSHV2)

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.

## 2.2 Module Specification

The Blue Coat ProxySG8100 is the high-end proxy appliance platform, providing even the largest enterprises with accelerated web communications. Located at the Internet gateway, the ProxySG8100 platform enables effective control of the enterprise's Internet traffic. The ProxySG8100 has an Liquid Crystal Display (LCD) and Light Emitting Diodes (LEDs) at the front of the module as shown in Figure 3.



**Figure 3 – Front View of the ProxySG8100**

The front panel of the module can be opened as shown in Figure 4. When open, the LCD and LEDs remain visible. Additionally, the open front panel exposes a power button, control buttons, and eight (8) disk drive bays (NOTE: the front panel control buttons are disabled in FIPS mode).. The module can accept up to eight (8) hard disk drives which are used to stores logs, configuration data, and System Files. Populated disk drive bays must be sealed with

tamper-evident labels while operating in FIPS mode.  Section 3 of this document provides guidance on how to apply tamper-evident labels on this module.
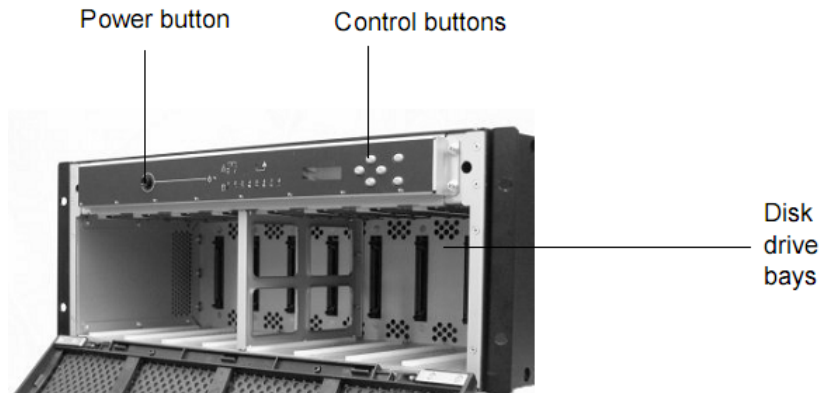


**Figure 4 – ProxySG8100 with the Front Panel Open**

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

- ProxySG8100 with no hardware acceleration card (Assembly #100-02644)
- ProxySG8100 with a Cavium CN1010 SSL card (Assembly #106-02883)
- ProxySG8100 with a Broadcom 5825 SSL card (Assembly #106-02835)

The ProxySG8100 is a multi-chip standalone module that meets overall Level 2 FIPS 140-2 requirements.  It is validated at the FIPS 140-2 Section levels as described 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 | EMI/EMC[1] | 2 |
| 9 | Self-tests | 2 |
| 10 | Design Assurance | 2 |
| 11 | Mitigation of Other Attacks | N/A |
| 14 | Cryptographic module Security Policy | 2 |

---

[1] EMI/EMC – Electromagnetic Interference/Electromagnetic Compatibility

## 2.3 Module Interfaces

The cryptographic boundary of the module is defined by the metal chassis, which surrounds all the hardware and software components as shown in Figure 3 of this document.  As mentioned in Section 2.2 above, the rear side of the module contains all the connecting ports, which are:

- Two network interfaces: two integrated 10/100/1000 Mbps[2] on-board ports for high-speed connections.  The module is shipped with a Dual GigE Copper card installed in the expansion slot labeled 2.  This card has two 10/100/1000 Mbps ports for high-speed connections.
- Serial console port: The serial console port connects to a Personal Computer (PC).
- Four upgrade slots for additional network and add-in cards.  Slots 2 and 3 accept Dual or Quad GigE Copper or Fiber LX cards and slots 4 and 5 accept SSL Accelerator cards.
- Two Universal Serial Bus (USB) ports (disabled in FIPS mode of operation).
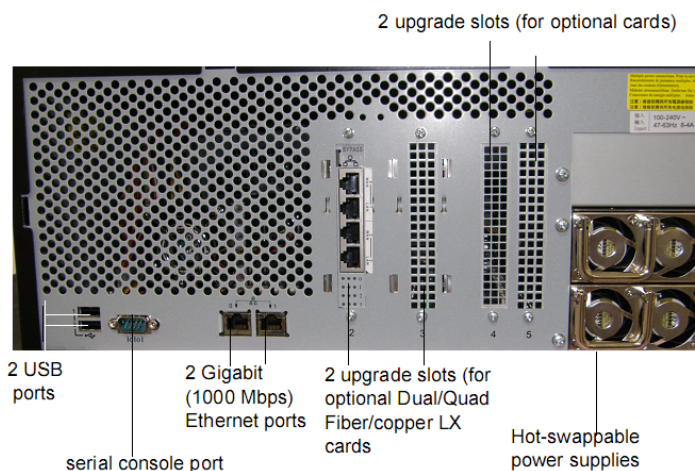- Removable AC power supplies with power connectors.



**Figure 5 – Connection Ports at the Back of the ProxySG8100**

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following Table 2.

**Table 2 – FIPS 140-2 Logical Interfaces**

| FIPS 140-2 Logical Interface | ProxySG8100 Port/Interface |
|---|---|
| Data Input | Network ports |
| Data Output | Network ports |
| Control Input | Power button, serial port, network ports |
| Status Output | LEDs, LCD, serial port, network ports |
| Power | AC power connections |

---

[2] Mbps – megabits per second

## 2.4 Roles and Services

The module supports role-based authentication. There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto-Officer role and a User role.

### 2.4.1 Crypto-Officer Role

The Crypto-Officer (CO) has administrator responsibilities that include installing and uninstalling the module. This role has permissions to view (monitor) and manage (configure) ProxySG configuration and user settings. The CO may monitor and configure the module locally over a secure serial port, or remotely over a TLS[3] v1.0, SSH[4] v2.0, or SNMP[5] v3 connection. Note that keys used for communications via SNMP are generated externally and input into the module.

Crypto-Officers can manually execute the power-up self-tests by rebooting the hardware module. Descriptions of the services available to the Crypto-Officer role are provided in the table below.

**Table 3 –Crypto Officer Role Services and CSP Access**

| Service | Description | CSPs Access |
|---|---|---|
| Install/uninstall the module | Install the module according to Security Policy guidelines; uninstall the module. | Master Appliance Key (MAK) – write |
| Firmware Upgrade | Allows new external firmware to be loaded and verified using an RSA digital signature. | RSA public key – read, write |
| Configuring the ProxySG | Define network interfaces and settings; set the protocols the ProxySG will support; load authentication information. | RSA public key – read, write<br>RSA private key – read, write<br>Session key – read, write<br>Master Appliance Key – read, write<br>Password – read, write<br>SNMP encryption key – read, write |
| Create, edit, and delete user groups | Create, edit and delete user groups; define common sets of user permissions. | RSA public key – read, write<br>RSA private key – read, write<br>Session key – read, write<br>Password – read, write |
| Create, edit, and delete users | Create, edit and delete users; define user accounts, change password, and assign permissions. | RSA public key – read, write<br>RSA private key – read, write<br>Session key – read, write<br>Password – read, write |
| Create filter rules | Create filters that are applied to user data streams. | RSA public key – read, write<br>RSA private key – read, write<br>Session key – read, write |
| Show status | View the ProxySG configuration, active sessions and logs. | RSA public key – read, write<br>RSA private key – read, write<br>Session key – read, write<br>SNMP encryption key – read, write |
| Reset the module | Shut down or reset the module | None |

---

[3] TLS – Transport Layer Security

[4] SSH – Secure Shell

[5] SNMP – Simple Network Management Protocol

| Service | Description | CSPs Access |
|---|---|---|
| Manage module configuration | Backup or restore the module configuration | RSA public key – read, write<br>RSA private key – read, write<br>Session key – read, write<br>Master Appliance Key – read, write<br>Password – read, write<br>SNMP encryption key – read, write |
| Zeroize keys | Zeroize keys | Zeroize |
| Change password | Change Crypto-Officer password | RSA public key – read, write<br>RSA private key – read, write<br>Session key – read, write<br>Password – read, write |
| Perform Self-test | Perform self-test on demand by rebooting the machine | None |

### 2.4.2   User Role

The User can utilize the module's Internet Content Application Protocol (ICAP) and Access Log services.  The ICAP service scans User web transmissions for malicious content.  Access logging allows you to track Web usage for the entire network or specific information on user or department usage patterns.  The User services in the module (over the TLS protocol) are based on the permissions set by the administrator.  A User does not have administrator rights to manage the module or manage Users.  A User cannot view or manage ProxySG configuration or User settings.  Descriptions of the services available to the User role are provided in the table below.

#### Table 4 – User Role Services and CSP Access

| Service | Description | CSP Access |
|---|---|---|
| ICAP server access | Access the object scanning service of web content. | RSA public key – read, write<br>RSA private key – read, write<br>Session key – read, write<br>Password – read, write |
| View status log | Track web usage for the entire network or specific information on user or department usage patterns | RSA public key – read, write<br>RSA private key – read, write<br>Session key – read, write<br>Password – read, write |

### 2.4.3   Authentication Mechanism

The Crypto-Officer can access the module locally over the serial port and remotely over a TLS, SSH, or SNMPv3 session.  The Crypto-Officer and User authenticate using a user ID and password.  The authentication mechanisms used in the module are listed below in Table 5.

#### Table 5 – Authentication Mechanisms Used by the Module

| Role | Authentication Type | Strength |
|---|---|---|
| Crypto-Officer | Password | 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 ASCII characters (92) with repetition equates to a 1 in $92^4$ chance of false acceptance.<br><br>For multiple attacks within a one minute period the probability of a random attempt succeeding or false acceptance is in $60/92^4$. |

| Role | Authentication Type | Strength |
|------|---------------------|----------|
| User | Password | 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 ASCII characters (92) with repetition equates to a 1 in $92^4$ chance of false acceptance.<br><br>For multiple attacks within a one minute period the probability of a random attempt succeeding or false acceptance is in $60/92^4$. |

## 2.5  Physical Security

The ProxySG8100 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-evidence labels are applied to the case to provide physical evidence of attempts to remove the case of the module.  The placement of tamper-evidence labels can be found in Section 3.

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 ProxySG8100.  The module does not provide a general purpose operating system nor does it allow operators 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 following cryptographic algorithms listed in Table 6.

**Table 6 - Cryptographic Algorithms Implemented in the Module**

| FIPS Approved or Allowed Security Functions | Certificate Numbers |
|---------------------------------------------|---------------------|
| **Symmetric Key Algorithms** | |
| Advanced Encryption Standard (AES): ECB, CBC, OFB, CFB-128 bit mode for 128, 192, and 256 bit key sizes | 859 |
| Triple-DES: ECB, CBC, CFB-64, OFB mode for 1 and 2 keying option | 706 |
| **Asymmetric Key Algorithms** | |
| DSA PQG generation, key pair generation, sign/verify – 1024-bit | 310 |
| RSA PKCS#1 sign/verify – 1024-, 1536-, 2048-, 3072-, 4096-bit | 413 |
| RSA (key wrapping; key establishment methodology provides 80 and 112 bits of encryption strength.) | Not applicable |
| Diffie-Hellman (key agreement; key establishment methodology provides 80 and 112 bits of encryption strength) | Not applicable |
| **Hashing Function** | |
| SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | 854 |
| **Message Authentication Code (MAC) function** | |

| FIPS Approved or Allowed Security Functions | Certificate Numbers |
|---|---|
| HMAC with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 | 476 |
| **Pseudo Random Number Generator (PRNG)** | |
| ANSI x9.31 Appendix A.4.2 PRNG | 491 |
| **Non FIPS Approved Functions** | |
| RNG that seeds the FIPS-approved random number generator | |
| MD-5 | |
| RC2, RC4 | |
| Blowfish | |

The module supports the following critical security parameters:

**Table 7 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs**

| Key | Key Type | Generation / Input | Output | Storage | Use |
|---|---|---|---|---|---|
| Master Appliance Key (MAK) | AES 256 CBC key | Internally generated | Never exits the module | Stored in plaintext | Encrypting password, SNMP encryption key, and RSA private key |
| Integrity Test Public Key | RSA 1024 public key | Externally generated, entered in plaintext | Never exits the module | Stored in plaintext | Verifying the integrity of the system image during upgrade |
| RSA  public key | 1024 bits,  2048 bits | Module's public key is internally generated. Other entities' public keys are sent to the module in plaintext. | During TLS/SSH negotiation in plaintext | Module's public key is stored on non-volatile memory. Other entities' public keys reside on volatile memory. | Negotiating TLS or SSH sessions |
| RSA private key | 1024 bits,  2048 bits | Internally generated | Never exits the module | Encrypted on non-volatile memory | Negotiating TLS or SSH sessions |

| Key | Key Type | Generation / Input | Output | Storage | Use |
|-----|----------|--------------------|--------|---------|-----|
| Session Key | AES CBC 128, 192, or 256 bit key<br><br>Triple-DES CBC 2 or 3 keying option | Internally generated | In encrypted form during TLS or SSH protocol handshake | Plaintext on volatile memory | Encrypting TLS or SSH data |
| Crypto-Officer Password | Minimum of four (4) printable characters with upper or lower case letters, numbers, and symbols | Enters the module over a secure remote session or via serial port | Never exits the module | Encrypted on non-volatile memory | Authenticating a CO for GUI[6] or CLI |
| SNMP encryption key | AES CFB 128, 192, or 256 key | Externally generated, enters the module in plaintext via the serial port or encrypted over the network port | Never exits the module | Encrypted on non-volatile memory | Encrypting SNMPv3 traffic |
| ANSI X9.31 Appendix A.4.2 PRNG seed | 64-bit random number | Internally generated | Never exits the module | Plaintext in volatile memory | Seeding the FIPS-approved PRNG |
| ANSI X9.31 Appendix A.4.2 PRNG key | Triple-DES 112-bit key | Internally generated | Never exits the module | Plaintext in volatile memory | Generating the FIPS-approved PRNG |

## 2.8  Self-Tests

The ProxySG8100 performs the following self-tests at power-up:

- Firmware integrity check using MD-5 Error Detection Code (EDC)
- Known Answer Tests (KATs)
    - o   AES KAT
    - o   Triple-DES KAT
    - o   RSA KAT for sign/verify and encrypt/decrypt
    - o   SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 KATs
    - o   HMAC KATs with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512
    - o   PRNG KAT
- DSA pairwise consistency check

The ProxySG8100 performs the following conditional self-tests:

- Continuous RNG Test (CRNGT) for both FIPS-approved and non-approved PRNGs
- RSA pairwise consistency check
- DSA pairwise consistency check
- Firmware update test using RSA signature verification

---

[6] GUI – Graphical User Interface

The cryptographic module performs the following critical tests at power-up:

- Verify validity of license

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. If any of the software self-tests fail, the module enters an error state, logging the error in the event log. The ProxySG requires Crypto-Officer's attention to clear the error state.

## 2.9  Design Assurance

Blue Coat uses the Perforce Configuration Management (CM) system. The Perforce software is used in software and document version control, code sharing, and build management. Perforce also keeps track of what versions of files were used for each release and what combinations were used in builds.

Additionally, Microsoft Visual SourceSafe (VSS) version 6.0 is used to provide configuration management for the ProxySG8100's FIPS documentation. This software provides access control, versioning, and logging.

## 2.10 Mitigation of Other Attacks

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

# 3  Secure Operation

The ProxySG8100 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  Crypto-Officer Guidance

The Crypto-Officer is responsible for the initialization of the security-relevant configuration and management activities for the module through the web management interface, serial port, or front LCD management panel. Please see the Blue Coat® Systems SG8100 Series Installation Guide (Blue Coat® Document Number 321-02878) for more information on setting up, configuring and maintaining the module.

Please note the aforementioned document is provided by the vendors in a CD along with the module.  The guide is also available in an online library only accessible to Blue Coat customers.

Before enabling FIPS mode, the tamper-evidence labels and faceplates must be applied as shown in the Section 3.1.1.  The vendor provides the following materials to meet the required physical security requirements.

**Table 8 – Tamper-Evident Labels and Faceplates**

| Name | Part |
|------|------|
| Square label |  |
| Rectangular label |  |
| Port faceplate |  |
| NIC[7] faceplate |   2-port NIC faceplate—ethernet card    2-port NIC faceplate—fiber card |

---

[7] NIC – Network Interface Card

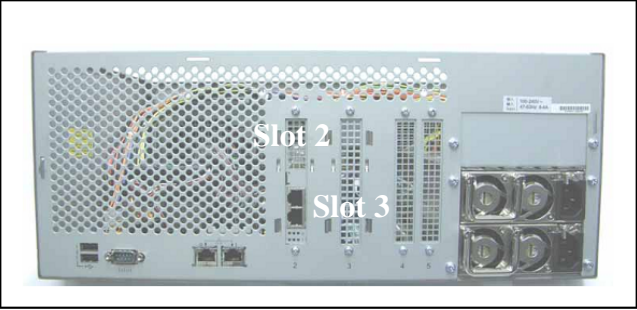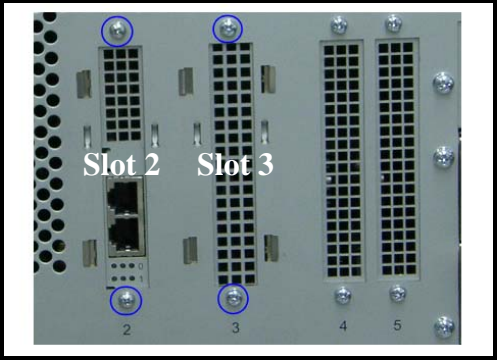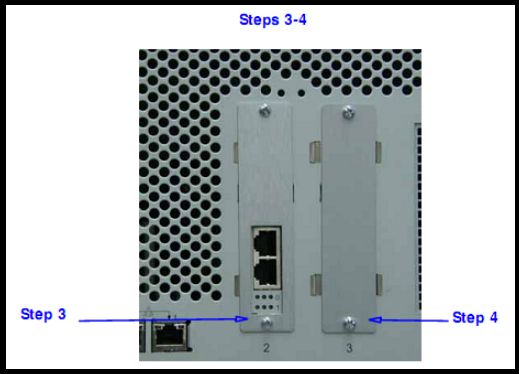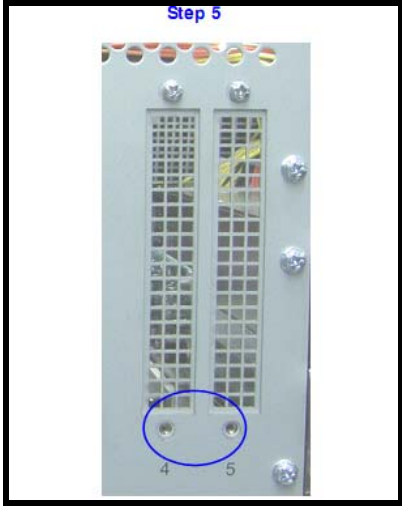| Name | Part |
|---|---|
| | 4-port NIC faceplate<br><br>No option card faceplate |
| Port faceplate |  |
| Port faceplate screws and nuts |  |
| 2-port NIC faceplate |  |
| Option card faceplate |  |

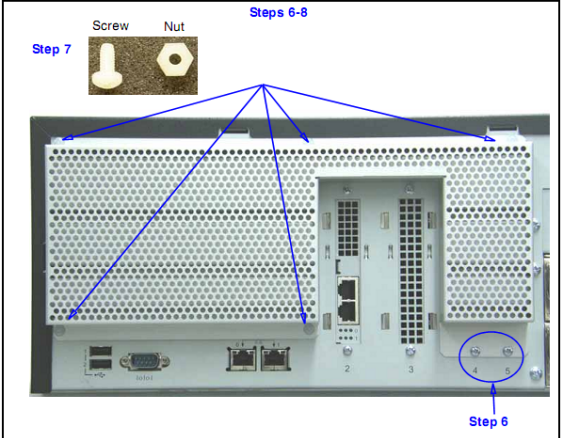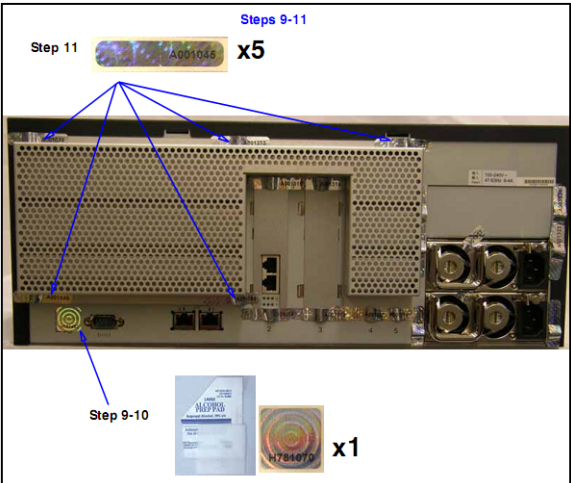### 3.1.1   Label Precautions and Application Instructions

Crypto-Officers must adhere to the following when applying the tamper-evident labels:
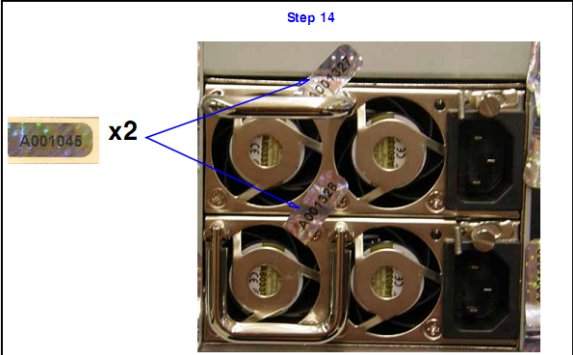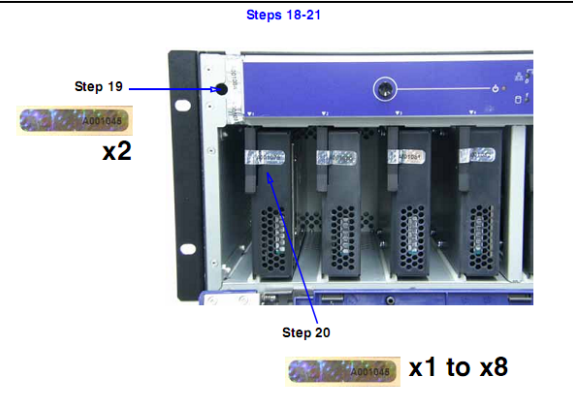
- The minimum temperature of the environment must be 35-degrees Fahrenheit. After application, the labels' acceptable temperature in the operational environment is -50-degrees to 200-degrees Fahrenheit.

- 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 hologram image is destroyed and the label leaves a patterned silicone adhesive 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.

Label and faceplate application instruction for ProxySG8100 is provided in the Table 9 below.

**Table 9 - Label and Faceplate Application Instructions**

| Step | Procedure | Figure |
|------|-----------|--------|
| 1 | Remove all cover screws (sides and top); remove the cover and position yourself behind the appliance. |  |
| 2 | Remove the two screws that secure the 2-port NIC card (Slot 2).  Slot 3 either contains an option card or a place-holder bracket.  Remove the two screws.  If the slot contains a place-holder bracket, hold the bracket in place while removing the screws (bottom first) to avoid it slipping and potentially damaging sensitive hardware components in the appliance. |  |
| 3 | Align the 2-port NIC card faceplate (Slot 2) and secure with the screws.  Note: If Slot 3 contains a 4-port NIC card, Step 4 is not required.  Proceed to Step 5. |  |
| 4 | Align the option card faceplate (Slot 3) and secure with the screws.  If you are reattaching the slot bracket instead (if no option card exists), hold the bracket in place while reinserting the screws. | |

| Step | Procedure | Figure |
|------|-----------|--------|
| 5 | Remove the bottom screws of the SSL card upgrade Slots 4 and 5. Do not remove the top screws. |  |
| 6 | Align the port faceplate as shown; secure with the two screws that were removed from Slots 4 and 5 in Step 5. |  |
| 7 | Insert the screw and nut:<br><br>a) Place the nut over the screw hole on the appliance.<br><br>b) Align the hole in the port faceplate over the nut.<br><br>c) Insert the screw into the hole in the faceplate and use a screwdriver to tighten the screw to the faceplate and nut. | |
| 8 | Reattach the top cover; secure with top and side screws. | |
| 9 | Use alcohol swab to clean USB port area to ensure proper adhesion. |  |
| 10 | Apply one square label over the USB port, as illustrated. | |
| 11 | Apply rectangular labels over each of the screw heads installed in Step 7, as illustrated. | |
| 12 | Apply rectangular labels over each screw head, as illustrated. Labels can overlap, but keep the serial numbers visible. |  |

| Step | Procedure | Figure |
|------|-----------|--------|
| 13 | Take two rectangular labels and cut them at the perforation.  Discard the halves of the labels that do not contain the serial numbers. | |
| 14 | Apply the cut labels to the tops of the power sources, keeping the serial numbers visible, as illustrated.<br><br>Note: When applying the labels, do not block the air flow of the power Source. |  |
| 15 | Use alcohol swab to clean all screw hole areas to ensure proper adhesion. |  |
| 16 | Apply square labels over each screw hole on one side of the SG8100. | |
| 17 | Repeat on the other side. | |
| 18 | Open the front panel. |  |
| 19 | Apply two rectangular labels over the screws securing the blue console panel (left and right sides). | |
| 20 | Apply rectangular labels over each present drive release lever (up to eight drives). | |
| 21 | Close the front panel. | |

| Step | Procedure | Figure |
|------|-----------|--------|
| 22 | Clean the two screw hole areas on top of the appliance.  Apply two square labels over the screw holes. |  |
| 23 | Rack-mount the appliance. | |

### 3.1.2    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.

- PC: Connect a serial cable to a serial port on the PC and to the module's serial console 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 10 – RS232 Parameters**

| RS-232C Parameters | 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.  The following configuration alert displays:

```
****************** CONFIGURATION ALERT ******************
System startup cannot continue for one of these reasons:
    (a) Need at least one adapter (or bridge) configured with an
    address and
        subnet.
    (b) Need the console password and enable password.
********* SYSTEM STARTUP TEMPORARILY SUSPENDED  *********
Press "enter" three times to activate the serial console
```

**Figure 6 – Initial Setup: Configuration Alert**

- 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 configuration sets up 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 Mode of operation must also be enabled (default is disabled). Setting FIPS mode to "enabled" ensures that all security functions used are FIPS Approved. The module will transition to to the FIPS mode when the Cryptographic Officer enters "fips-mode enable" command via serial port. The entry of this command causes the device to power cycle and Zeroize the Master Appliance Key. **NOTE:** This command is only accepted via serial port.

### 3.1.3   Management

The Crypto-Officer is able to monitor and configure the module via the web interface (HTTPS over TLS), serial port, or secure telnet (telnet over TLS).  Detailed instructions to monitor and troubleshoot the systems are provided in Blue Coat® Systems Installation Guides mentioned in the Blue Coat® Systems SG8100 Series Installation Guide.

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 module can be taken out of FIPS mode using the secure serial setup console only.  A CLI command ("fips-mode") will allow FIPS mode to be enabled or disabled.  To ensure that CPSs are not shared across FIPS Approved mode and Non-Approved mode, any change to FIPS mode parameter 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 and power-cycle has completed.

### 3.1.4   Zeroization

At the end of its life cycle or when taking the module out of FIPS mode, the module must be fully zeroized to protect CSPs.  When switching between FIPS mode and non-FIPS mode, the module automatically reboot, zeroizing all the CSPs.  The Crypto-Officer must wait until the module has successfully rebooted in order to verify that zeroization has completed.

## 3.2  User Guidance

The User does not have the ability to configure sensitive information on the module, with the exception of their authentication data.  Although the User does not have any ability to modify the configuration of the module, they should report any irregular activity they notice to the Crypto-Officer.

# 4   Acronyms

**Table 11 – Acronyms**

| Acronym | Definition |
| --- | --- |
| ANSI | American National Standards Institute |
| CIFS | Common Internet File System |
| CLI | Command Line Interface |
| CM | Configuration Management |
| CMVP | Cryptographic Module Validation Program |
| CO | Crypto-Officer |
| CRNGT | Continuous Random Number Generator Test |
| CSP | Critical Security Parameter |
| DSA | Digital Signature Algorithm |
| EDC | Error Detection Code |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| FIPS | Federal Information Processing Standard |
| FTP | File Transfer Protocol |
| GUI | Graphical User Interface |
| HMAC | (Keyed-) Hash Message Authentication Code |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Secure Hypertext Transfer Protocol |
| ICAP | Internet Content Application Protocol |
| IM | Instant Messaging |
| IP | Internet Protocol |
| KAT | Known Answer Test |
| LCD | Liquid Crystal Display |
| LED | Light Emitting Diode |
| MAC | Message Authentication Code |
| MAPI | Messaging Application Programming Interface |
| MMS | Microsoft Media Streaming |
| NIC | Network Interface Card |
| NIST | National Institute of Standards and Technology |
| NVLAP | National Voluntary Laboratory Accreditation Program |
| OS | Operating System |
| P2P | Peer-to-Peer |
| PC | Personal Computer |

| Acronym | Definition |
|---------|------------|
| PRNG | Pseudo Random Number Generator |
| RAM | Random Access Memory |
| RNG | Random Number Generator |
| RSA | Rivest Shamir and Adleman |
| RTSP | Real-Time Streaming Protocol |
| SGOS | Secure Gateway Operating System |
| SHA | Secure Hash Algorithm |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| SSL | Secure Socket Layer |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| VoIP | Voice-over-IP |
| VSS | Visual SourceSafe |
| WAN | Wide Area Network |