Blue Coat Systems, Inc.

ProxySG 900 Series

Models: SG900-10B, SG900-20, SG900-30, SG900-45, SG900-55

Hardware Versions: 090-02988, 090-02989, 090-02902, 090-02903, 090-02904, 090-02905, 090-02908, 090-02909, 090-02979, 090-02980

Firmware Version: 6.5.1.103

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2

Document Version: 0.7

Prepared for:

BLUE COAT

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

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

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

.

Table of Contents

List of Figures

List of Tables

.

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the ProxySG 900 Series (Models: SG900-10B, SG900-20, SG900-30, SG900-45, SG900-55; Firmware Version: 6.5.1.103) from Blue Coat Systems, Inc.. This Security Policy describes how the ProxySG 900 Series appliances meet 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 (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the appliance 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 900 Series (SG900-10B, SG900-20, SG900-30, SG900-45, SG900-55) is referred to in this document as the SG900, 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 900 Series

2.1 Overview

The foundation of Blue Coat's application delivery infrastructure, the Blue Coat ProxySG 900 Series appliances establish points of control that accelerate and secure business applications for users across the distributed organization. The ProxySG 900 Series 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 SG900 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 the ProxySG 900 Series appliances.

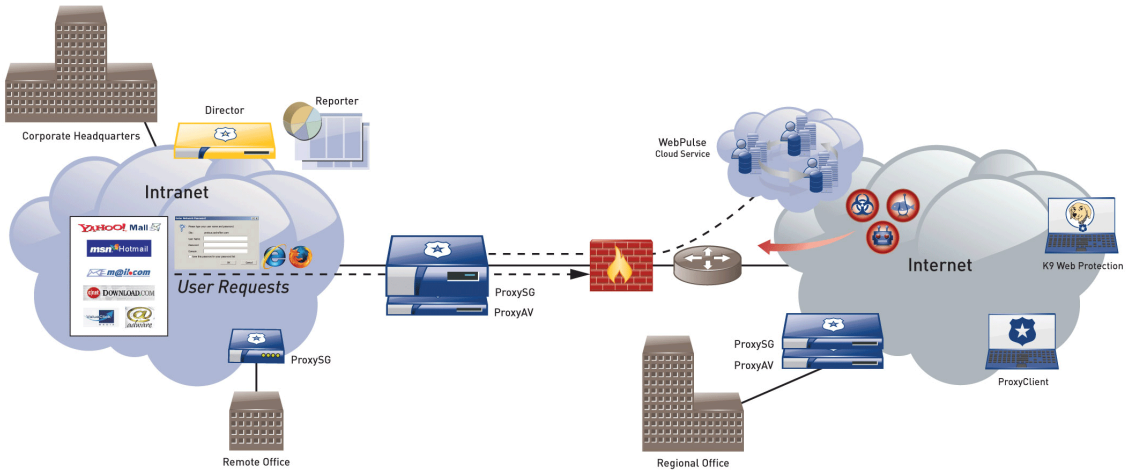

Figure 1 Typical Deployment of a ProxySG 900 Series Appliance

The security provided by the SG900can be used to control, protect, and monitor the Internal Network's use of controlled protocols on the External Network. The SG900 appliances offer a choice of two "editions" via licensing: MACH5 and Proxy. The MACH5 edition appliances have some proxy features disabled (as indicated below). The controlled protocols implemented in the evaluated configuration are:

.

Table 1 MACH5 vs Proxy Edition Capability Differences

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

[1] IMAP – Internet Message Access Protocol
2 TCP – Transmission Control Protocol
[3] POP3 – Post Office Protocol version 3
[4] SMTP – Simple Mail Transfer Protocol

.

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

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 SG900 provides optimization of data transfer between SG900 nodes on a WAN. Optimization is achieved by enforcing a configurable policy (WAN Optimization SFP) on traffic traversing the WAN. Additionally, the SG900 offers network traffic acceleration by using hardware implementations of cryptographic services provided by on-board hardware accelerator cards (HAC) produced by Cavium Networks.

The SG900 is validated at the following FIPS 140-2 Section levels in Table 2.

Table 2 Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	Electromagnetic Interference/Electromagnetic Compatibility	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

[6] AOL – America Online
[6] AOL – America Online
[7] MSN – The Microsoft Network
[8] SOCKS – SOCKet Secure

2.2 Module Specification

For the FIPS 140-2 validation, the crypto module was tested on the following SG900 appliance configurations:

Table 3 SG900 Appliance Configurations

	Hardware Version	
Model	**Proxy Edition**	**MACH5 Edition**
SG900-10B	090-02988	090-02989
SG900-20	090-02903	090-02902
SG900-30	090-02905	090-02904
SG900-45	090-02909	090-02908
SG900-55	090-02979	090-02980

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 and Proxy editions vary in only data processing capabilities; the Crypto Officer and User services of the module are identical for both licensing editions. Table 1 above provides a mapping between the capabilities and the licensing edition.

The SG900 offers an affordable rack-mountable appliance solution for small enterprises and branch offices that have direct access to the Internet. The front panel, as shown in Figure 2 below, has 1 Liquid Crystal Display (LCD) interface, 2 Light Emitting Diodes (LEDs), and six control buttons (NOTE: the front panel control buttons are disabled in FIPS-Approved mode). Connection ports are at the rear, as shown in Figure 3.

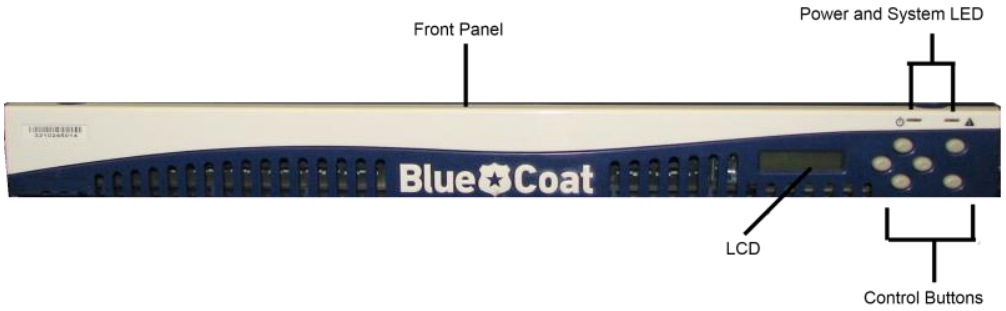

Figure 2 SG900 (Front View)

For the FIPS 140-2 validation, the module was tested on the following SG900 appliance configurations:

- SG900 (SG900-10B, SG900-20, SG900-30, SG900-45, SG900-55) with a Cavium CN1610 PCI-e[9] SSL HAC

The SG900 is a hardware module with a multi-chip standalone embodiment. The overall security level of the module is 2. The cryptographic boundary of the SG900 is defined by the appliance chassis, which surrounds all the hardware and firmware. The module firmware, version 6.5.1.103, contains the SGOS 6.5 Cryptographic Library version 3.1.1.

[9] PCI-e – Peripheral Component Interconnect Express

.

2.3 Module Interfaces

The front panel of the SG900 (as shown in Figure 2) has 1 LCD interface, 2 LEDs, and six control buttons. The control buttons on the front panel are disabled once the module is configured for its Approved mode of operation.

The type and quantity of all ports present in the front panel of the SG900 are given in Table 4.

Table 4 FIPS 140-2 Logical Interface Mappings for the front of the SG900

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 SG900 is described in Table 5.

Table 5 Front Panel LED Status Indications for the SG900

LED	Color	Definition
Power LED	OFF	The SG900 is powered off.
	AMBER	The OS has loaded but has not been loaded.
	FLASHING GREEN TO AMBER	The OS has been loaded but has not been configured.
	GREEN	The OS has loaded and is properly configured.
System LED	OFF	The appliance has not determined the system status.
	GREEN	Healthy.
	AMBER	Warning.
	FLASHING AMBER	Critical Warning.
	BLUE	Diagnostic mode.

The rear of the SG900 is shown in Figure 3.

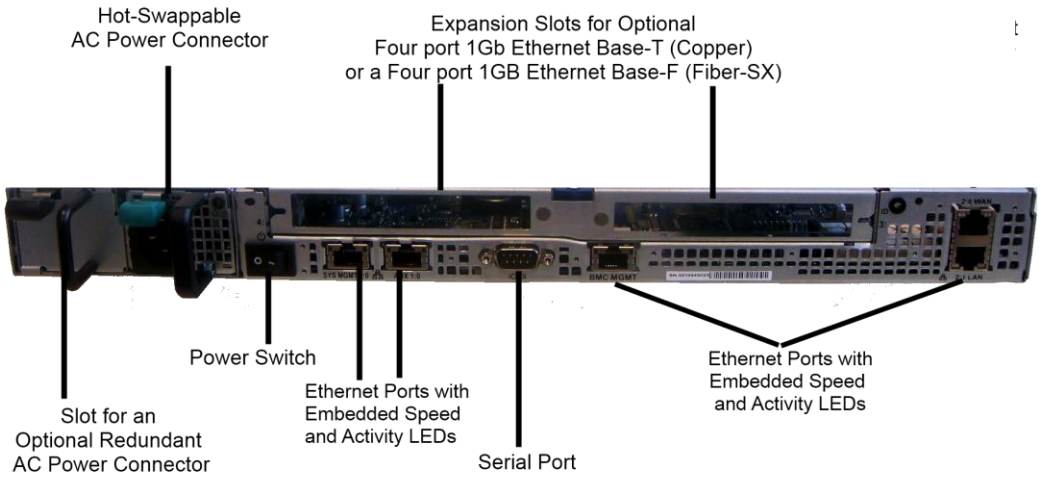

Figure 3 Connection Ports at the Rear of the SG900

The rear side of the SG900 (as shown in Figure 3) contains all the connecting ports. Those ports are:

- An AC power connector.
- A serial port to connect to a Personal Computer (PC) for management.
- Five full-duplex, auto-sensing Ethernet adapter ports supporting 10/100/1000 Base-T connections.
- Two expansion slots for:
  - Four port 1000 Base-F (quad GigE Fiber SX) NIC
  - An optional Four port 1000 Base-T (quad GigE with bypass) NIC
- 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 SG900 are given in Table 6.

Table 6 FIPS 140-2 Logical Interface Mappings for the rear of the SG900

Physical Port/Interface	Quantity	FIPS 140-2 Interface
Ethernet ports	5	• Data Input • Data Output • Control Input • Status Output
Serial ports	1	• Control Input • Status Output
Ethernet Interface – Speed LEDs	5	• Status Output
Ethernet Interface – Activity LEDs	5	• Status Output
AC power connection LED(s)	1 or 2	• Status Output
AC power connection	1 or 2	• Power Input
Power Switch	1	• Control Input

The status indications provided by the LEDs on the SG900 are described in Table 7.

.

Table 7 Rear Panel LED Status Indications for the SG900

LED	Color	Definition
AC power connection LED	OFF	The SG900 is not receiving power.
	GREEN	The SG900 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.

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 11. The modules offer two management interfaces:

- Command Line Interface (CLI) – accessible locally via the serial port (provides access to the Setup Console portion of the CLI which requires the additional "Setup" password to gain access) or remotely using SSH. This interface is used for management of the modules. This interface must be accessed locally via the serial port to perform the initial module configurations (IP address, DNS server, gateway, and subnet mask) and placing the modules into the Approved mode. Management of the module may take place via SSH or locally via the serial port. Authentication is required before any functionality will be available through the CLI.
- Management Console – a graphical user interface accessible remotely with a web browser that supports TLS[10]. This interface is used for management of the modules. Authentication is required before any functionality will be available through the Management Console.

When managing the module over the CLI, COs and Users both log into the modules with administrator accounts entering the "standard", or "unprivileged" mode on the SG900. Unlike Users, COs have the ability to enter the "enabled", or "privileged" mode after initial authentication to the CLI by supplying the "enabled" mode password. Additionally, COs can only enter the "configuration" mode from the "enabled" mode via the CLI, which grants privileges to make configuration level changes. Going from the "enabled" mode to the "configuration" mode does not require additional credentials. The details of these modes of operation are found below in Table 8.

[10] TLS – Transport Layer Security

.

Table 8 FIPS and SG900 Roles

FIPS Roles	SG900 Roles and Privileges
CO	The CO is an administrator of the module that has been granted "enabled" mode access while using the CLI and "read/write" access while using the Management Console. When the CO is using the CLI, and while in the "enabled" mode of operation, COs may put the module in its Approved mode, reset to the factory state (local serial port only) and query if the module is in Approved mode. In addition, COs may do all the services available to Users while not in "enabled" mode. Once the CO has entered the "enabled" mode, the CO may then enter the "configuration" mode via the CLI. The "configuration" mode provides the CO management capabilities to perform tasks such as account management and key management. When the CO is administering the module over the Management Console, they can perform all the same services available in CLI (equivalent to being in the "configuration" mode in the CLI) except the CO is unable to put the module into Approved mode. The CO may monitor the health and status of the modules using SNMPv3. SNMPv3 privacy and authentication keys are assigned to a CO and are not tied to the CO's CLI and Management Console credentials.
User	The User is an administrator of the module that operates only in the "standard" or "unprivileged" mode and has not been granted access to the "enabled" mode in the CLI and has been given "read-only" privileges when using the Management Console. The User will access the CLI and Management Console interfaces for management of the module. When the User is administering the module over the Management Console, they perform all the same services available in CLI ("standard" mode only services). The User may monitor the health and status of the modules using SNMPv3. SNMPv3 privacy and authentication keys are assigned to a User and are not tied to the User's CLI and Management Console credentials.

Descriptions of the services available to a Crypto Officer and User are described below in Table 9 and Table 10 respectively. For each service listed below, COs and Users are assumed to already have authenticated prior to attempting to execute the service. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

- R – Read: The plaintext CSP is read by the service.
- W – Write: The CSP is established, generated, modified, or zeroized by the service.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

2.4.1 Crypto-Officer Role

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

.

Table 9 Crypto Officer Role Services and CSP Access

Service	Description	CSP and Access Required
Set up the module	Set up the first-time network configuration, CO username and password, and enable the module in the FIPS-approved mode of operation. For more information, see section 3.1 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 – RX
* Enter the "configuration" mode	Manage the module in the "configuration" mode of operation, allowing permanent system modifications to be made	None
* Disable FIPS mode	Takes the module out of the FIPS-approved mode of operation, accessible only via the serial port	MAK – W SSH Session Key – W SSH Authentication Key – W TLS Session Key – W TLS Authentication Key – W All CTR_DRBG CSPs – RW
** Firmware Load	Loads new external firmware and performs an integrity test using an RSA digital signature.	Integrity Test public key – WRX
Create remote management session (CLI)	Manage the module through the CLI (SSH) remotely via Ethernet port.	RSA public key – RX RSA private key – RX SSH Session Key – WRX SSH Authentication Key – WRX All CTR_DRBG CSPs – RW
Create remote management session (Management Console)	Manage the module through the Management Console (TLS) remotely via Ethernet port, with optional CAC authentication enabled.	RSA public key – RX RSA private key – RX TLS Session Key – WRX TLS Authentication Key – WRX All CTR_DRBG CSPs – RW
** Create, edit, and delete operator groups	Create, edit and delete operator groups; define common sets of operator permissions.	None
** Create, edit, and delete operators	Create, edit and delete operators (these may be COs or Users); define operator's accounts, change password, and assign permissions.	Crypto-Officer Password – W User Password – W SNMP Privacy Key – W SNMP Authentication Key – W
** Create filter rules (CLI)	Create filters that are applied to user data streams.	None
Create filter rules (Management Console)	Create filters that are applied to user data streams.	None

.

Service	Description	CSP and Access Required
Show FIPS-mode status (CLI)	The CO logs in to the module using the CLI. Entering the command "show version" will display if the module is configured in Approved mode.	None
Show FIPS-mode status (Management Console)	The CO logs in to the module using the Management Console and navigates to the "Configuration" tab that will display if the module is configured in Approved mode.	None
** Manage module configuration	Backup or restore the module configuration	RSA public key – WRX RSA private key – WRX SNMP Privacy Key – WRX SNMP Authentication Key – WRX CO Password – WRX User Password – WRX "Enabled" mode password – WRX
* Zeroize keys	Zeroize keys by taking the module out of FIPS-mode. This will zeroize all CSPs. The zeroization occurs while the module is still in FIPS-mode.	MAK – W SSH Session Key – W SSH Authentication Key – W TLS Session Key – W TLS Authentication Key – W All CTR_DRBG CSPs – W
** Change password	Change Crypto-Officer password	Crypto-Officer Password – W
* Perform self-test	Perform self-test on demand by rebooting the machine	SSH Session Key – W SSH Authentication Key – W TLS Session Key – W TLS Authentication Key – W All CTR_DRBG CSPs – W
* Reboot the module	Reboot the module.	SSH Session Key – W SSH Authentication Key – W TLS Session Key – W TLS Authentication Key – W All CTR_DRBG CSPs – W
Create SNMPv3 session	Monitor the module using SNMPv3	SNMP Privacy Key – RX SNMP Authentication Key – RX

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

2.4.2 User Role

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

.

Table 10 User Services and CSP Access

Service	Description	CSP and Access Required
Create remote management session (CLI)	Manage the module through the CLI (SSH) remotely via Ethernet port.	RSA public key – RX RSA private key – RX SSH Session Key –WRX SSH Authentication Key – WRX All CTR_DRBG CSPs – RW
Create remote management session (Management Console)	Manage the module through the Management Console (TLS) remotely via Ethernet port, with optional CAC authentication enabled.	RSA public key – RX RSA private key – RX TLS Session Key – WRX TLS Authentication Key – WRX All CTR_DRBG CSPs – RW
Create SNMPv3 session	Monitor the health of the module using SNMPv3	SNMP Privacy Key – RX SNMP Authentication Key – RX
Show FIPS-mode status (Management Console)	The User logs in to the module using the Management Console and navigates to the "Configuration" which will display if the module is configured in Approved mode.	None
Show FIPS-mode status (CLI)	The User logs in to the module using the CLI. Entering the command "show version" will display if the module is configured in Approved mode.	None

2.4.3 Additional Services

The module also offers proxying and termination services for the protocols listed in section 2.1. For more information on the non security relevant services of the module, please refer to the *Blue Coat® Systems SGOS Administration Guide*.

2.4.4 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 session. 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 until the operator logs out. Each CO and User Management Console session remains active until the operator logs out or inactivity for a configurable amount of time has elapsed.

Modules used by the United States Department of Defense (DoD) must meet Homeland Security Presidential Directive (HSPD)-12 requirements regarding the use of FIPS 201 validated Common Access Card (CAC) authentication for COs and Users connecting to management functionality of the module. Additionally, other agencies may require FIPS 201 validated PIV[11] II card authentication.

[11] PIV – Personal Identity Verification II

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

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

1. On the management workstation the CO or User opens a browser and establishes a clear-text HTTP connection with the module.
2. Using CPL similar to the VPM `NotifyUser` action, the CO or User is presented with a DoD warning banner which they must positively acknowledge and accept.
3. `NotifyUser` redirects the browser to an HTTPS connection with the module that requires mutual authentication. This is made possible by CPL that puts the module in reverse-proxy mode at this point.
4. The TLS handshakes begin. The reverse-proxy service on the module requires a certificate to complete the handshake (i.e. the `verify-peer` setting has been enabled in the reverse-proxy service).
5. The browser presents the CO or User with a dialog box prompting which certificate to select.
6. The CO or User selects the X.509 certificate on the CAC.
7. The middleware on the management workstation prompts the CO or User for the PIN to unlock the certificate. The CO or User enters the PIN and the certificate is transmitted to the module.
8. The module authenticates the certificate against the CA list that has been configured on the reverse proxy service using local CRLs and OCSP to check for certificate revocation.
9. The CO or User reviews and accepts the certificate issued to the web browser by the module. A mutually authenticated TLS session is now in use.
10. The module extracts the subject name (of the CO or User) from the `subjectAltNames` extension of the X.509 certificate according to configuration of the certificate realms, Within the `subjectAltNames` extension is the CO or User's `userPrincipleName` (UPN) (When PIV cards are used in place of CACs, the CommonName (CN) field is extracted from the certificate instead). The UPN/CN is what ties the CAC identity to the Principle Name (PN) field of a CO or User record in Active Directory (AD), the LDAP server.
11. The certificate realm is configured to use an LDAP realm for authorization. The LDAP user is determined by LDAP search using the following filter: `(userPrincipleName=$(user.name))`.

The CO or User is granted access to the Management Console if the UPN/CN is found in the LDAP directory. The exchanges with the LDAP server are secured using TLS. Conditions like *`group=`* and *`ldap.attribute <name>`* may also be used to authorize the CO or User and to specify if the CO or User should have read-only or read-write access.

The authentication mechanisms used in the module are listed below in Table 11.

.

Table 11 Authentication Mechanisms Used by the Module

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

.

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 (95) with repetition equates to a 1: (95^8), or 1: 6,634,204,312,890,625 chance of false acceptance. The User may connect remotely after establishing a TLS or SSH session.
	Public keys	The module supports using RSA keys for authentication of Users during TLS (when CAC authentication is configured with a local Certificate Realm) or SSH. Using conservative estimates and equating a 2048-bit RSA key to a 112-bit symmetric key, the probability for a random attempt to succeed is $1:2^{112}$ or 1: 5.19×10^{33}.

2.5 Physical Security

The SG900 is a multi-chip standalone cryptographic module and is enclosed in a hard, opaque metal case that completely encloses all of its internal components. There are only a limited set of vent holes provided in the case, and these holes obscure the view of the internal components of the module. Tamper-evident labels are applied to the case to provide physical evidence of attempts to remove the case of the module. The Crypto-Officer is responsible for the placement of tamper-evident labels and baffles and guidance can be found in section 3.1.1.2. The labels and baffles are part of the FIPS Security Kit (Part Number: 085-02742).

All of the module's components are production grade. The SG900 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 SG900. The module does not provide a general purpose operating system nor does it allow operators the ability to load untrusted firmware. The operating system run by the cryptographic module is referred to as Secure Gateway Operating System (SGOS). SGOS is a proprietary real-time embedded operating system.

2.7 Cryptographic Key Management

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

.

Table 12 FIPS-Approved Algorithm Implementations

Algorithm	Firmware Implementation Certificate Number	CN1610 SSL HAC Implementation Certificate Number
Symmetric Key Algorithms		
AES: ECB[12], CBC[13], OFB[14], CFB[15]-128 bit mode for 128-, 192-, and 256-bit key sizes	#2560	#1265
3DES[16]: ECB, CBC, CFB-64, OFB mode for keying option 1 (3 different keys)	#1549	#898
Asymmetric Key Algorithms		
RSA (ANSI X9.31) Key Generation – 2048, 3072, 4096-bit	#1312	#607, #742
RSA PKCS[17]#1 signature generation 2048, 3072, and 4096-bit RSA PKCS#1 signature verification – 1024, 1536, 2048, 3072, and 4096-bit	#1312	#607, #742
Hashing Functions		
SHA[18]-1	#2159	N/A
SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512)	#2159	N/A
Message Authentication Code (MAC) Functions		
HMAC[19] with SHA-1[20]	#1580	N/A
HMAC with SHA-224, SHA-256, SHA-384, SHA-512	#1580	#736 (HMAC SHA-512 only)
Deterministic Random Bit Generator (DRBG)		
SP[21] 800-90 CTR_DRBG (AES-256)	#386	N/A

***NOTE**: As of December 31, 2010, the following algorithms listed in the table above is considered for "legacy-use" only. .*

- *Digital signature verification using RSA key sizes of 1024 and 1536-bits are approved for legacy use only. RSA Signature Verfication using 1536-bits is present only in the firmware implementation.*

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

- RSA PKCS#1 wrap/unwrap (key-wrapping) – 2048, 3072, and 4096–bit sizes providing 112, 130, and 150-bits of security.
- Diffie-Hellman for key agreement during TLS and SSH: 2048-bit keys (provides 112 bits of security).
- Non-Deterministic RNG (NDRNG) for seeding the FIPS-Approved RNG (SP 800-90 CTR_DRBG)

Caveat: The module implements MD5[22] for use with SSL3.1/TLS1.0, which is allowed in the FIPS-Approved mode of operation. Any other use of this function is prohibited.

[12] ECB – Electronic Codebook
[13] CBC – Cipher Block Chaining
[14] OFB – Output Feedback
[15] CFB – Cipher Feedback
[16] 3DES – Triple Data Encryption Standard
[17] PKCS – Public Key Cryptography Standard
[18] SHA – Secure Hash Algorithm
[19] HMAC – Hash-Based Message Authentication Code
[20] HMAC-SHA-1 uses keys of at least 112-bits of security strength.
[21] SP – Special Publication
[22] MD5 – Message Digest v5

.

The module supports the CSPs listed below in Table 13.

Table 13 List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Master Appliance Key (MAK)	AES CBC 256-bit key	Internally generated via FIPS-Approved DRBG.	Never exits the module	Stored in plaintext on non-volatile memory	By disabling the FIPS-Approved mode of operation	Encrypting Crypto-Officer password, SNMP localized key, RSA private key
Integrity Test Public Key	RSA public key 2048 bits	Externally generated, Imported in encrypted form via a secure TLS or SSH session.	Never exits the module	Stored in plaintext on non-volatile memory	Overwritten after upgrade by the key in the newly signed image.	Verifying the integrity of the system image during upgrade or downgrade.
RSA Public Key	2048[23], 3072, and 4096-bits	Modules' public key is internally generated via FIPS-Approved DRBG. Modules' public key can be imported from a back-up configuration.	Output during TLS/SSH negotiation in plaintext. Output during TLS negotiation for CAC authentication Exits in encrypted format when performing a module configuration backup.	Modules' public key is stored on non-volatile memory.	Modules' public key is deleted by command.	Negotiating TLS or SSH sessions

[23] There are separate RSA keypairs used for negotiating SSH and TLS sessions. TLS session negotiations can use 2048, 3072, and 4096-bit RSA keypairs; SSH session negotiations can only use 2048-bit RSA keypairs.

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
	1024, 1536, 2048, 3072, and 4096-bits	Other entities' public keys are sent to the module in plaintext. Can be sent to the module as part of an X.509 certificate during CAC authentication.	Never output	Other entities' public keys reside on volatile memory.	Other entities' public keys are cleared by power cycle.	
RSA Private Key	2048, 3072, and 4096-bits	Internally generated via FIPS-Approved DRBG. Imported in encrypted form via a secure TLS or SSH session. Imported in plaintext via a directly attached cable to the serial port.	Exits in encrypted format when performing a module configuration backup.	Stored in encrypted form on non-volatile memory	Inaccessible by zeroizing encrypting MAK	Negotiating TLS or SSH sessions
DH public key	2048-bits	The module's Public key is internally generated via FIPS-Approved DRBG; while public key of a peer enters the module in plaintext.	The module's Public key exits the module in plaintext.	Stored in plaintext on volatile memory	Rebooting the modules; Remove Power	Negotiating TLS or SSH sessions
DH private key	224-bits	Internally generated via FIPS-Approved DRBG.	Never exits the module	Stored in plaintext on volatile memory	Rebooting the modules; Remove Power	Negotiating TLS or SSH sessions

.

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

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
"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.

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SP 800-90A CTR_DRBG Seed	384-bit random number	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules; Remove Power	Seeding material for the SP800-90A CTR_DRBG
SP 800-90A CTR_DRBG Entropy[24]	256-bit random number with derivation function 384-bit random number without derivation function	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules; Remove Power	Entropy material for the SP800-90A CTR_DRBG
SP 800-90A CTR_DRBG key value	Internal state value	Internally generated	Never	Plaintext in volatile memory	Rebooting the modules; Remove Power	Used for the SP 800-90A CTR_DRBG
SP 800-90A CTR_DRBG V value	Internal state value	Internally generated	Never exits the module	Plaintext in volatile memory	Rebooting the modules; Remove Power	Used for the SP 800-90A CTR_DRBG

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

Keys and passwords that exit the module during a configuration backup are encrypted using a FIPS-Approved encryption algorithm. During the backup process, the CO must select the encryption algorithm to use: AES-128 CBC mode, or AES-256 CBC mode.

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

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 firmware. If any of the firmware self-tests fail, an error is printed to the CLI (when being accessed via the serial port). When this error occurs, the modules halt operation and provide no functionality. The only way to clear the error and resume normal operation is for the Crypto-Officer to reboot the modules. The status output provided below is shown only over the CLI (when being accessed via the serial port).

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

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

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

2.8.1 Power-Up Self-Tests

The SG900 performs the following self-tests using the OpenSSL firmware implementation at power-up:

- Firmware integrity check using an EDC (32-bit CRC)
- Known Answer Tests (KATs)
    - AES encrypt and decrypt KAT
    - 3DES encrypt and decrypt KAT
    - RSA digital signature generation KAT
    - RSA digital signature verification KAT
    - RSA wrap/unwrap KAT
    - SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 KATs
    - HMAC KAT with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 KATs
    - DRBG KAT

Upon successful completion of the firmware implementation self-tests, the SG900 performs the following self-tests on the hardware accelerator card:

- AES-CBC KAT
- 3DES-CBC KAT
- RSA digital signature generation KAT
- RSA digital signature verification KAT
- HMAC SHA-512 KAT

If the hardware accelerator card self-tests pass, further execution of these algorithms will take place in the hardware implementation. If the hardware accelerator card self-tests fail, all algorithm execution will occur exclusively in the firmware 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 SG900 performs the conditional self-tests in Table 14 (only on its firmware implementation of OpenSSL).

Table 14 SG900 Conditional Self-Tests

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

2.8.3 Critical Function Tests

The SG900 performs the SP800-90A DRBG Critical Function tests in Table 15 (only on its firmware implementation of OpenSSL).

.

Table 15 List of Critical Function Tests

Conditional Test	Occurrence
SP 800-90A DRBG Instantiate Test	Done before the instantiation of a new DRBG. The DRBG instantiation algorithm is sent fixed values of entropy, nonce, and personalization string. The output is compared with the value that was expected. If the values match, the test passes. Otherwise, it fails. Error testing is done by forcing an error upon the algorithm. If the algorithm handles the error as expected, the test passes. Otherwise, it fails
SP 800-90A DRBG Generate Test	Done before the first use of the DRBG. The DRBG Generate function tests both the Instantiate and Reseed algorithms. KATs are performed for each security strength supported and for each prediction resistance (if supported). The number of bits requested, additional input (if supported), working internal state, are supplied to the Generate function. If the values used during the test produce the expected results and the errors are handled as expected, the test passes. Otherwise, it fails.
SP 800-90A DRBG Reseed Test	Done before reseeding the DRBG instantiation function (w/o prediction resistance) or before the generation of a new random number (w/ prediction resistance). The DRBG reseed algorithm is sent fixed values of entropy and the internal state value, V. The output is compared with the value that was expected. If the values match, the test passes. Otherwise, it fails. Error testing is done by forcing an error upon the algorithm. If the algorithm handles the error as expected, the test passes. Otherwise, it fails
SP 800-90A DRBG Uninstantiate Test	This test is performed whenever the Instantiate, Generate, or Reseed tests are executed. It demonstrates that error handling is performed correctly and zeroizes the internal state

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 SG900 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: 085-02742) consists of the following items as shown below in Figure 4.

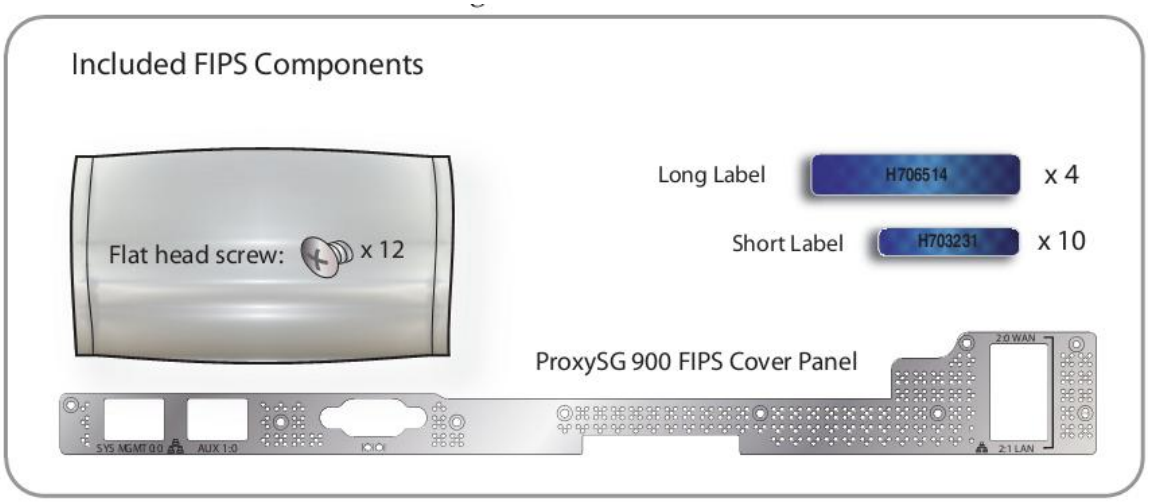

Figure 4 FIPS Security Kit Contents

Note: Two (2) long labels and five (5) short labels are required to secure the appliance. Additional labels are included for reapplication purposes.

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 900 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 to ensure full FIPS 140-2 compliance. Once the seals have been applied, the Crypto Officer must develop an inspection schedule to verify that the external enclosure of the module and the tamper seals have not been damaged or tampered with in any way. If the Crypto-Officer detects evidence of tampering or damage to the labels, the Crypto-Officer must return to the module to the uninitialized factory state, remove and reapply all labels per section 3.1.1.2, and must complete the first-time configuration in order to operate in its FIPS-Approved mode as detailed in section 3.2.1. 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 when applying the tamper-evident labels:

- The minimum temperature of the environment must be 35-degrees Fahrenheit. After application, the labels' acceptable temperature in the operational environment is -5-degrees to 158-degrees Fahrenheit.
- Do not touch the adhesive side of the label. This disrupts the integrity of the adhesive. If a label is removed from a surface, the 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.
- After applying the labels, allow at least 24 hours for the label adhesive to cure.

3.1.1.1 Baffle Installation

The baffles for the rear of the appliance are designed to prevent unauthorized access to key system components by shielding the rear ventilation outlets. Figure 5 below shows the security panel installed in a SG900 appliance equipped with two power supply units.

Figure 5 Rear Security Panel Installed

1. Align the security panel mounting points against the screw locations shown below in Figure 6 and secure with nine (9) flat-head screws. Be aware the FIPS kit includes (3) additional screws, in case some are misplaced or lost during installation.

.

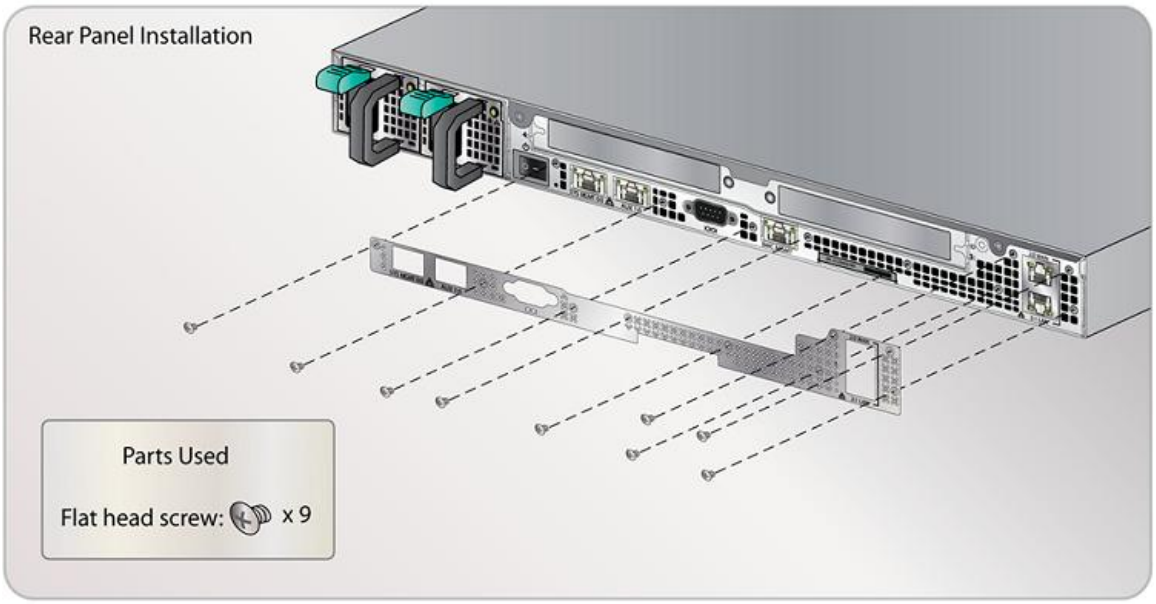

Figure 6 Rear Security Panel Installation

3.1.1.2 Label Installation

The tamper-evident labels are applied over key areas of the chassis to provide tamper-evident security. If the labels are removed after being affixed to a surface, the image self-destructs and leaves a text pattern on the label. Figure 7 below illustrates the tamper-evident features of the label.

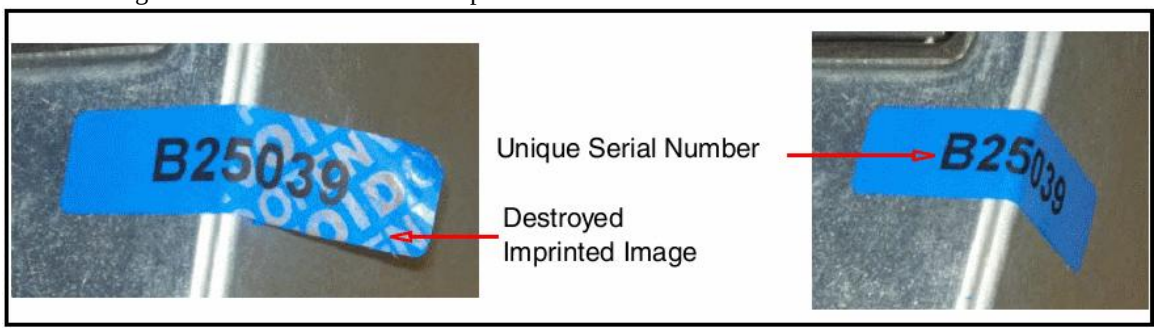

Figure 7 Label Showing Tamper Evidence

1. Use 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.
2. Set the appliance on a flat, slip-proof work space and make sure you have access to all sides of the appliance.
3. Apply two (2) labels over the rear security panel. These labels extend over the bottom edge of the appliance when properly applied because the extraneous material must not cover the vents or ports.
    A. Apply one (1) short label vertically in the non-vented surface between the serial port and appliance serial number shown by Step 3A in Figure 8 below. Make sure the remaining label material crosses over the bottom edge of the appliance.
    B. Apply one (1) short label vertically over the lower-right (when viewed from the rear) corner of the security panel shown by Step 3B in Figure 8 below. Make sure the security label covers the entire screw head, the bottom two rows, across two columns of vents; the remaining label material crosses over the bottom edge of the appliance.

.

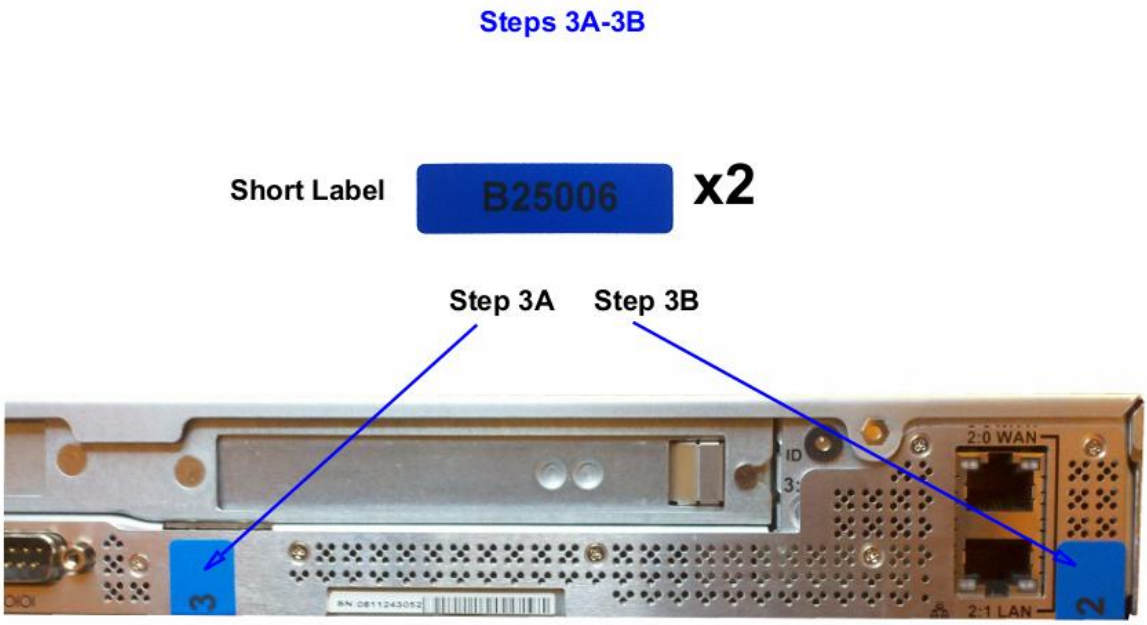

Figure 8 Right-Rear Tamper-Evident Label Application

4. Apply one (1) long label over each power supply unit, as illustrated below in Figure 9. When applying the labels, make sure there is enough material on both ends to properly secure the power supply.

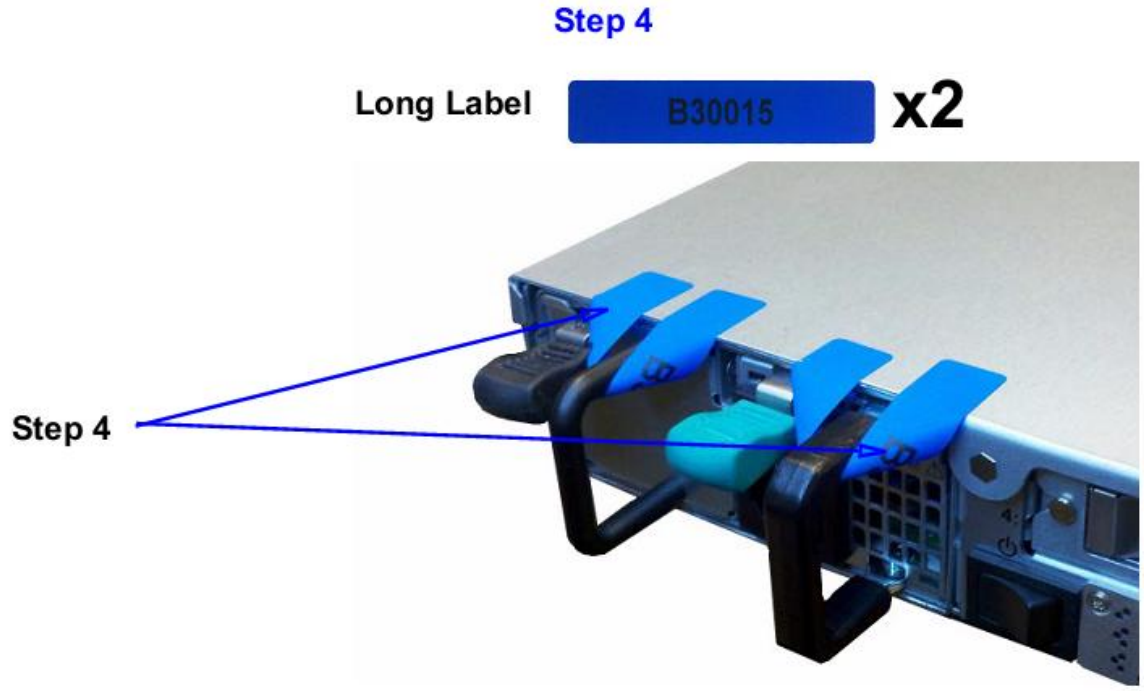

Figure 9 Tamper-Evident Label Application – Power Supplies

5. Apply two (2) short labels over the center cover to prevent unauthorized access to the system components. Each label should be placed on the opposite ends of the appliance, as shown below in Figure 10.

.

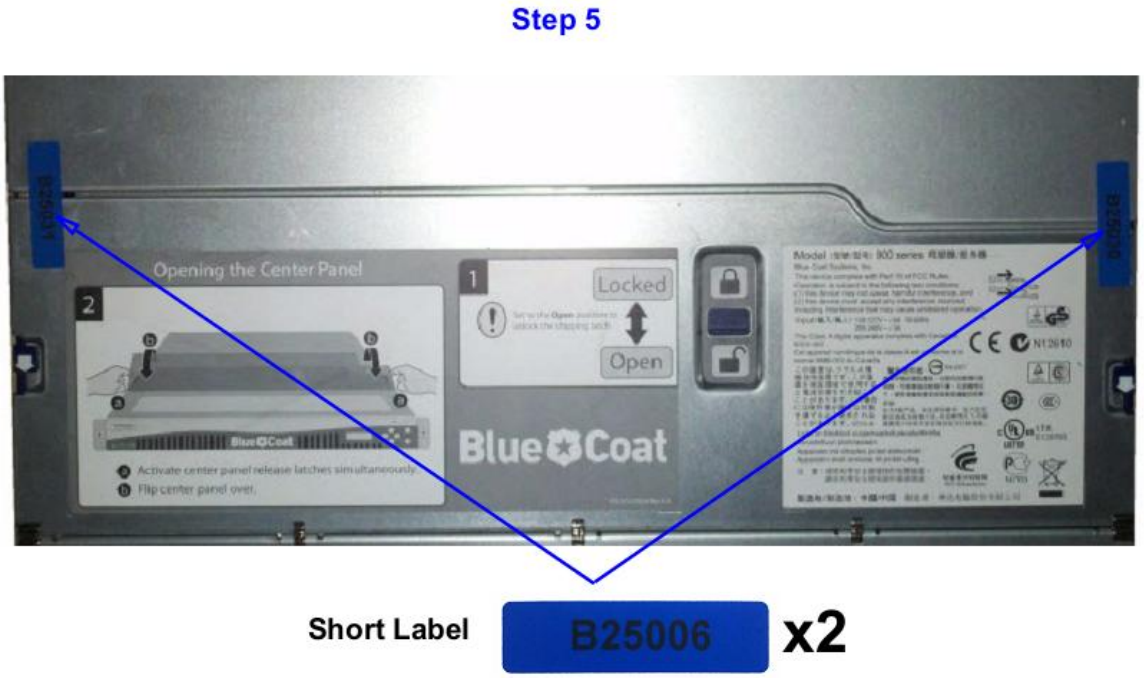

Figure 10 Tamper-Evident Label Application – Top of Appliance

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

6. Facing the front of the appliance, apply one (1) short label over the space between the bezel and top lid, making sure that label is on the center point as shown below in Figure 11.

Figure 11 Tamper-Evident Label Application – Front Bezel

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

3.2 Secure Management

3.2.1 Initialization

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

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

1. Connect a serial cable to a serial port on a PC and to the module's serial port. Open a terminal emulator (such as HyperTerminal) on the PC, and connect to the serial port to which you attached the cable. Create and name a new connection (either a COM or TCP/IP), using the port parameters provided in Table 16.

Table 16 RS-232 Parameters

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

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

3. Press <Enter> three times. When the "Welcome to the SG Appliance Setup Console" prompt appears, the system is ready for the first-time network configuration.

4. Set up the first time configuration by entering the interface number, IP address, IP subnet mask, IP gateway, DNS server parameters, username, and password.

5. Press <Enter> to confirm the configuration when the "Successful Configuration Setup" prompt appears.

6. Repeat step 3.

7. Selection option #1 for the Command Line Interface. This option takes you immediately to the Admin prompt.

8. The Crypto-Officer shall enter the "enabled" mode on the CLI by typing the 'enable' command followed by the 'enable' password.

9. The prompt will change from '>' to '#' signifying the Crypto-Officer is in the 'enabled' mode. Type the command 'fips-mode enable.' When prompted for confirmation, elect 'y' to confirm. Once the reinitialization is complete, the module will display the prompt "The system is in FIPS mode."

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

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

10. Wait for the system to finish rebooting. Repeat step 3.

11. Repeat step 4.

12. The module will prompt for the 'enabled' mode password:

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

13. 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:
```

14. The module will prompt to restrict workstation access. Choose "Yes" or "No."

15. Finally, select the licensing mode. The module will prompt with the following options:

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

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

3.2.2 Management

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

The Crypto-Officer should monitor the module's status regularly. If any irregular activity is noticed or the module is consistently reporting errors, customers should consult Blue Coat Systems Blue Touch Online (BTO) and the administrative guidance documents to resolve the issues. If the problems cannot be resolved through these resources, Blue Coat Systems customer support should be contacted.

The CO must ensure that localized keys used for SNMPv3 authentication and privacy match the key type requirements specified in Table 13. Key sizes less than what is specified shall not be used. The CO password and "enabled" mode password must be at least 8 characters in length. The "Setup" password must be at least 4 characters in length.

When creating or importing key pairs, such as during the restoration of an archived SG900 configuration, the CO must ensure that the "Do not show key pair" option is selected in the Management Console as shown in Figure 12, or the "no-show" argument is passed over the CLI as shown in Figure 13. Please see Section E: Preparing Archives for Restoration on New Devices in the *Blue Coat Systems SGOS Administration Guide, Version 6.5* for further reference.

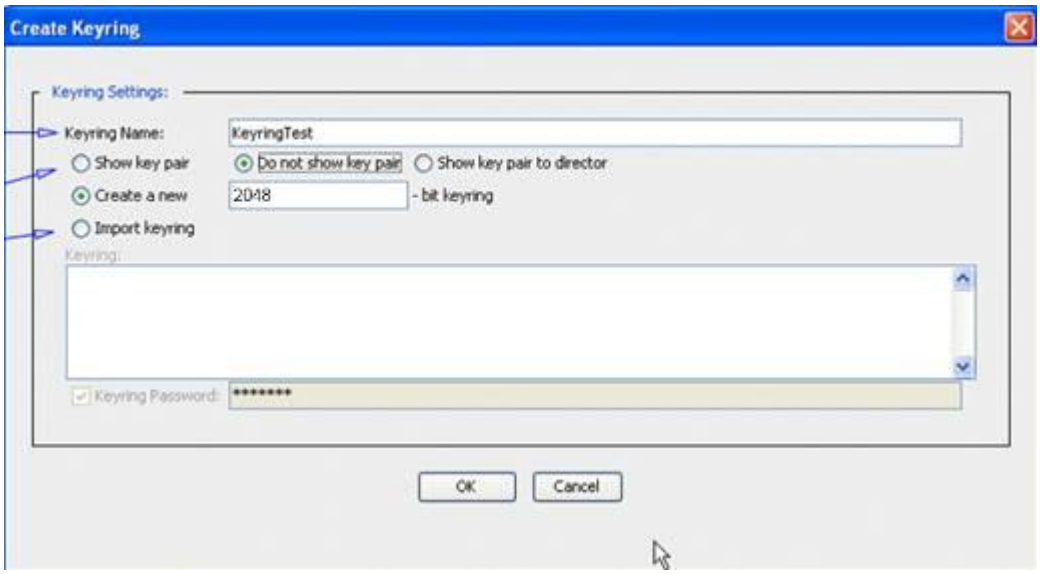

Figure 12 Keyring Creation Management Console Dialogue Box

Related CLI Syntax to Import a Keyring

```
SGOS#(config ssl) inline {keyring show | show-director | no-show}
keyring_id eof
Paste keypair here
eof
```

Figure 13 Keyring Creation CLI Commands

3.2.3 Zeroization

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

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

3.3 User Guidance

The User is only able to access the module remotely via SSH (CLI) or HTTPS (Management Console). The User must change his or her password at the initial login. The User must be diligent to also pick strong

passwords (alphanumeric with minimum 8 characters) that will not be easily guessed, and must not reveal their password to anyone. Additionally, the User should be careful to protect any secret/private keys in their possession, such as TLS or SSH session keys. The User should report to the Crypto Officer if any irregular activity is noticed.

3.4 Non-Approved Mode

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

.

4 Acronyms

This section describes the acronyms used throughout this document.

Table 17 Acronyms

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
BTO	BlueTouch Online
CA	Certificate Authority
CAC	Common Access Card
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CIFS	Common Internet File System
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CN	Common Name
CO	Crypto-Officer
CRNGT	Continuous Random Number Generator Test
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CX4	Four pairs of twin-axial copper wiring
DES	Data Encryption Standard
DNS	Domain Name System
DoD	Department of Defense
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HAC	Hardware Accelerator Card
HDS	HTTP Dynamic Streaming

.

Acronym	Definition
HLS	HTTP Live Streaming
HMAC	Hash-Based Message Authentication Code
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IP	Internet Protocol
KAT	Known Answer Test
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAC	Message Authentication Code
MD5	Message Digest v5
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OS	Operating System
P2P	Peer-to-Peer
PC	Personal Computer
PCI-e	Peripheral Component Interconnect Express
PIN	Personal Identification Number
PIV	Personal Identity Verification
PN	Principle Name
POP3	Post Office Protocol version 3
RS-232	Recommended Standard 232
RSA	Rivest Shamir Adleman
RTMP	Real-Time Messaging Protocol
RTSP	Real-Time Streaming Protocol
SFTP	Secure File Transfer Protocol
SGOS	Secure Gateway Operating System
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOCKS	SOCKet Secure

.

Acronym	Definition
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UPN	User Principle Name
USB	Universal Serial Bus
VoIP	Voice Over Internet Protocol
WAN	Wide Area Network

Prepared by:
Corsec Security, Inc.

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

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