
Blue Coat® Systems SSL Visibility Appliance

Model: SV2800

Hardware Versions: 090-03063, 080-03562

Firmware Version: 3.5.2 build 961

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2

Document Revision: 6/18/2014

BLUE COAT

COPYRIGHT NOTICE

©2014 Blue Coat Systems, Inc. All rights reserved. BLUE COAT, PROXYSG, PACKETSHAPER, CACHEFLOW, INTELLIGENCECENTER, CACHEOS, CACHEPULSE, CROSSBEAM, K9, DRTR, MACH5, PACKETWISE, POLICYCENTER, PROXYAV, PROXYCLIENT, SGOS, WEBPULSE, SOLERA NETWORKS, DEEPSEE, DS APPLIANCE, SEE EVERYTHING. KNOW EVERYTHING., SECURITY EMPOWERS BUSINESS, BLUETOUCH, the Blue Coat shield, K9, and Solera Networks logos and other Blue Coat logos are registered trademarks or trademarks of Blue Coat Systems, Inc. or its affiliates in the U.S. and certain other countries. This list may not be complete, and the absence of a trademark from this list does not mean it is not a trademark of Blue Coat or that Blue Coat has stopped using the trademark. All other trademarks mentioned in this document owned by third parties are the property of their respective owners. This document is for informational purposes only.

BLUE COAT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. BLUE COAT PRODUCTS, TECHNICAL SERVICES, AND ANY OTHER TECHNICAL DATA REFERENCED IN THIS DOCUMENT ARE SUBJECT TO U.S. EXPORT CONTROL AND SANCTIONS LAWS, REGULATIONS AND REQUIREMENTS, AND MAY BE SUBJECT TO EXPORT OR IMPORT REGULATIONS IN OTHER COUNTRIES. YOU AGREE TO COMPLY STRICTLY WITH THESE LAWS, REGULATIONS AND REQUIREMENTS, AND ACKNOWLEDGE THAT YOU HAVE THE RESPONSIBILITY TO OBTAIN ANY LICENSES, PERMITS OR OTHER APPROVALS THAT MAY BE REQUIRED IN ORDER TO EXPORT, RE-EXPORT, TRANSFER IN COUNTRY OR IMPORT AFTER DELIVERY TO YOU.

Americas:

Rest of the World:

Blue Coat Systems, Inc.
420 N. Mary Ave.
Sunnyvale, CA 94085

Blue Coat Systems International SARL
3a Route des Arsenaux
1700 Fribourg, Switzerland

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

Document Revision: 6/18/2014

1. Introduction 1

1.1 Purpose 1

1.2 References 1

1.3 Document Organization 1

1.4 Definitions and Acronyms 3

2. SV2800 5

2.1 Overview 5

2.2 Module Specification 9

2.3 Module Interfaces 13

2.4 Roles and Services 17

2.5 Services and CSP Access 20

2.6 Physical Security 26

2.7 Non-Modifiable Operational Environment 27

2.8 Cryptographic Key Management 27

2.9 Self Tests 34

2.10 Design Assurance 36

2.11 Mitigation of Other Attacks 36

3. Secure Operation 37

3.1 Cryptographic Officer Guidance 37

3.2 Tamper Evident Label Management and Application Instructions 37

3.3 Module Initialization 46

3.4 Module Management 49

3.5 Module Zeroization 49

1. Introduction

1.1 Purpose

This document is a non-proprietary Cryptographic Module Security Policy for the Blue Coat SSL Visibility Appliance model SV2800. The SV2800 model should be operated with the v3.5.2 build 961 firmware version. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module, and may freely be reproduced and distributed in its entirety (without modification).

Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules, specifies the U.S. and Canadian Governments' requirements for cryptographic modules. The following pages describe how the Blue Coat SSL Visibility Appliance meets these requirements and how to operate the device in a mode compliant with FIPS 140-2.

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>.

In this document, the Blue Coat SSL Visibility Appliance model SV2800 is referred to as the SV2800, the hardware module, the cryptographic module, or the module.

1.2 References

This document only deals with the operation and capabilities of the SV2800 within the technical terms of a FIPS 140-2 cryptographic module security policy. More information on the SV2800 is available from the following sources:

- The Blue Coat website, www.bluecoat.com, contains information on the full line of products from Blue Coat.
- The Blue Coat customer website, <https://bto.bluecoat.com>, contains product documentation, software downloads, and other 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

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

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

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

1.4 Definitions and Acronyms

Table 1–1 Definition of Terms and Acronyms

Term / Acronym	Definition
10Gig	10 Gigabit Ethernet interface
Active-Inline	Inline SV2800 with an inline security appliance attached
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BTO	Blue Touch Online
CA	Certificate Authority
CBC	Cipher Block Chaining
CLI	Command line interface
CMVP	Cryptographic Module Validation Program
Crypto Officer	Crypto Officer as defined in FIPS 140-2
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DLP	Data Loss Prevention
DPI	Deep Packet Inspection
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FTW	Fail To Wire – hardware network cut through
GigE	Gigabit Ethernet interface.
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over TLS
IDS	Intrusion Detection System
iPass	High density copper cable/connector for 10Gbps Ethernet link
IPS	Intrusion Prevention System
KAT	Known Answer Test
LCD	Liquid Crystal Display

Table 1–1 Definition of Terms and Acronyms

Term / Acronym	Definition
LED	Light Emitting Diodes
MAC	Message Authentication Code
MD5	Message Digest #5
NDRNG	Non-deterministic Random Number Generator
Netmod	Network I/O Module – plug-able – defines network interface used
NFE	Netronome Flow Engine
NFP	Netronome Flow Processor
NIST	National Institute of Standards and Technology
NMI	Non Maskable Interrupt
NPU	Network Processing Unit
NSM	Netronome SSL Module
OS	Operating System
Passive-Inline	Inline SV2800 acting as a tap for a passive security appliance
Passive-Tap	SV2800 connected to a network tap acting as a tap for a passive security appliance
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
POST	Power On Self Test
PRNG	Pseudo Random Number Generator
PSU	Power Supply Unit
RC4	Rivest Cipher 4
SHA	Secure Hash Algorithm
SPAN port	A switch port providing a copy of traffic flowing through the network
SSH	Secure Shell
SSL	Secure Socket Layer
TAP	Device providing a copy of traffic flowing through the network
TLS	Transport Layer Security protocol
TRNG	True Random Number Generator

2. SV2800

2.1 Overview

Blue Coat's SSL Visibility Appliance products provide two main functions when deployed within a network:

- They enable other security appliances to see a non encrypted version of SSL/TLS traffic that is crossing the network. This is called SSL Inspection.
- They can act as a policy control point enabling explicit control over what SSL/TLS traffic is and is not allowed across the network.

The SSL Visibility Appliance is designed to work alongside existing security devices such as Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Data Loss Prevention systems (DLP), Network Forensic appliance and others. It provides a non-encrypted version of SSL/TLS traffic to the associated appliances while maintaining an end-to-end SSL/TLS connection between the client and server involved in the session.

There are three basic connectivity modes that define how the SV2800 and the associated security appliance are connected to each other and to the network. These modes are identified as:

- Active-Inline
- Passive-Inline
- Passive-Tap

The Active/Passive designation refers to the associated security appliance and how it behaves while the Inline/Tap designation refers to how the SV2800 is connected to the network. An "Active" associated appliance processes traffic from the SV2800 and then returns the traffic to the SV2800, while a "Passive" appliance simply consumes traffic from the SV2800.

The SV2800 can be either "Inline," or a TAP, which is connected to a network span or tap port. The following figures show these three modes of operation.

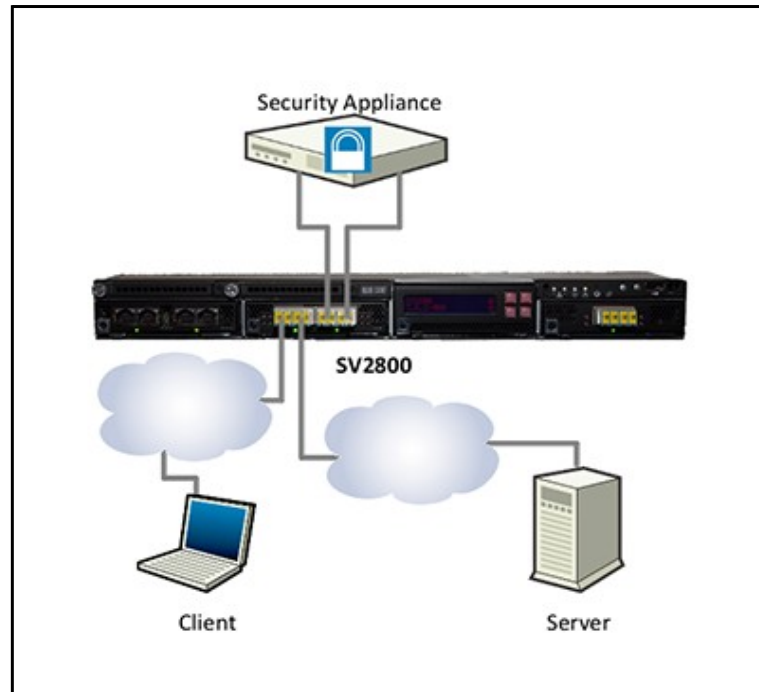


Figure 2-1 Active-Inline Configuration

In Active-Inline mode (Figure 2-1) network traffic flows through both the SV2800 and the attached security appliance. A typical example of this type of deployment would be an IPS attached to the SV2800. This mode of operation supports both SSL Inspection and SSL policy control.

In Passive-Inline mode (Figure 2-2), network traffic flows through the SV2800 only, a copy of the network traffic (some of which may be decrypted) is sent to the attached security appliance. A typical example of this type of deployment would be an IDS or Forensic appliance attached to the SV2800. This mode of operation supports both SSL Inspection and SSL policy control.

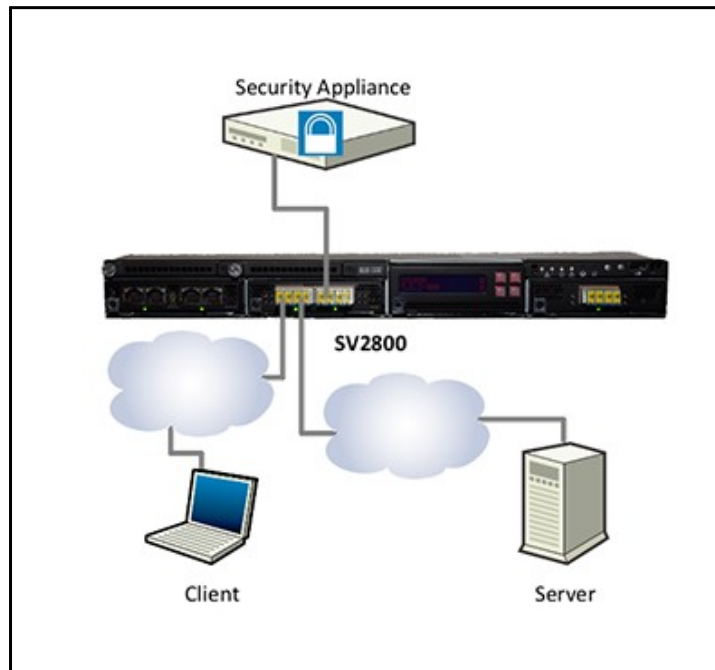


Figure 2-2 Passive-Inline Configuration

In Passive-Tap mode (Figure 2-3), network traffic does not flow through the SV2800 or the attached security appliance. The SV2800 receives a copy of traffic in the network from a TAP device and this traffic (possibly decrypted) is sent to the attached security appliance. A typical example of this type of deployment would be an IDS or Forensic appliance attached to the SV2800, which is in turn attached to a TAP or SPAN port. This mode of operation supports SSL Inspection only and cannot act as an SSL policy control point.

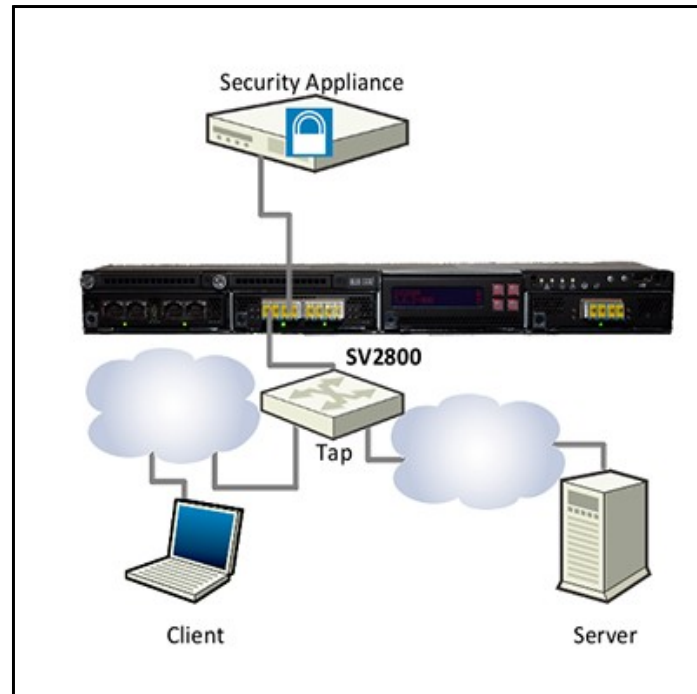


Figure 2–3 Passive-Tap Configuration

By allowing the attached security appliance to view a decrypted version of SSL/TLS traffic, the SSL Visibility Appliance enables the security appliance to detect/block threats that are hidden within encrypted SSL/TLS flows. As the percentage of SSL/TLS traffic in networks is growing significantly with increasing use of Web 2.1 applications and Cloud based applications, it is increasingly important that network security appliances can do their job even when the traffic is sent over SSL/TLS connections.

Detecting, intercepting, decrypting and re-encrypting SSL/TLS traffic is a complex and computationally intense activity. Providing SSL/TLS inspection capabilities in a device that can be placed in-line in either a Gigabit Ethernet or 10 Gigabit Ethernet network link and which will not cause a performance bottleneck requires hardware acceleration. In the case of the SV2800 this acceleration is provided by a Netronome Network Flow Engine (NFE) card that contains one of Netronome's NFP-3240 flow processor chips. The NFP-3240 contains 40 cores optimized for processing network traffic and provides significant acceleration and offload for the standard CPUs used on the SV2800 motherboard.

The SV2800 software provides the ability to inspect both incoming and outgoing SSL/TLS traffic and detects SSL/TLS traffic by deep packet inspection (DPI) so no matter what port the SSL/TLS traffic is using it will be detected. Once an SSL/TLS flow has been detected the SV2800 policy engine determines what to do with the flow:

- it can be inspected providing a decrypted version to the attached appliance(s)
- it can be cut through, allowing the attached appliance(s) to see the original encrypted flow

- it can be blocked such that the flow is terminated and cannot continue.

The policy engine allows policy to be based on a wide range of parameters such as:

- the source/destination IP address of the flow
- the Distinguished Name (DN) of the subject or issuer contained in the SSL/TLS server certificate sent by the server
- the cipher suite being used for the flow

This allows for fine grained control over which SSL/TLS traffic is inspected, and, when the SV2800 is deployed in-line, enables fine grained policy control over what SSL/TLS traffic is allowed in the network.

All SSL/TLS traffic seen by the SV2800, whether it is using approved or non-approved algorithms, will be processed to a degree. At a minimum the SSL/TLS handshake will be observed in order to collect information that the policy engine will use to determine how the flow should be handled. Using the policy rules it is possible to cause the following actions to be applied to a flow:

- block the SSL/TLS flow
- allow the SSL/TLS flow without any inspection
- allow the SSL/TLS flow with the flow being inspected

The policy engine is aware of the cipher suite that the SSL/TLS flow is using, and can base its decision on that. So, it is possible to configure policy settings that will prevent any SSL/TLS flows using non-approved algorithms from being established through the SV2800 if that is desired. If SSL/TLS flows using non-approved algorithms are allowed by the policy engine then they should be considered as being “clear text” due to the use of non-approved algorithms.

2.2 Module Specification

The hardware version numbers in Table 1-2 provides a mapping between the hardware versions and the appliance types available. All appliance types have the exact same hardware and firmware, and are exactly the same from a cryptographic functionality and boundary perspective.

Table 1–2 SV2800 Appliance Configurations

Appliance Type	Hardware Version
Hardware Appliance	090-03063
Try-and-Buy Appliance	080-03562

The Crypto Officer and User services of the module are identical for both appliance types. A Try-And-Buy appliance varies from the Hardware Appliance only in that the firmware that is provided with the appliance is valid for 30 days, after which the full license must be purchased or the hardware appliance must be returned to Blue Coat.

The Blue Coat SV2800 is a high performance transparent SSL/TLS proxy that can be deployed in both Gigabit Ethernet and 10G Ethernet networks. The SV2800 is a 1U high rack mountable device.

The SV2800 has three front facing modular I/O bays that allow for flexibility in the number of network interfaces and in the type of media supported. Network I/O Modules (Netmods) are installed in the three bays to configure the desired combination of interfaces.

All of the Netmod interfaces and the switching module that plug into the front of the SV2800 connect to the network segments on which traffic is being monitored/inspected. These ports are only used to access the network data that is being processed by the SV2800; they are not associated with any cryptographic processes, keys, critical security parameters (CSP) or any FIPS relevant data. These ports do not allow access to the management services of the SV2800 and cannot be used to input or output cryptographic keys, CSPs or any FIPS relevant data. The Netmods and associated switch are therefore deemed to be outside the logical cryptographic boundary.

Figure 2-4 shows an SV2800 device with three Netmods installed. In this example, the Netmods each support 4 x 1Gig copper interfaces. Available Netmod options are listed below, other Netmod types may become available in the future:

- 4 x GigE copper (4 ports of 10/100/1000Base-T with FTW)
- 4 x GigE fiber (4 ports of 1000Base-SX with FTW)
- 2 x 10Gig fiber (2 ports of 10GBase-SR with FTW)
- 2 x 10Gig fiber (2 ports of 10GBase-LR with FTW)

Fail to wire (FTW) hardware allows pairs of network ports to be physically connected to each other in the event that the system is powered off or that a failure is detected. Depending on how the network is connected to the SV2800, this allows network traffic to continue flowing even when the system is powered off or in a failure state. When FTW is active, traffic is passed between ports on a Netmod and never enters the module.

Note: Netmods are NOT hot swappable. The system must be powered off before removal or installation of Netmods.



Figure 2-4 SV2800, Front View with Netmods Installed

Figure 2-5 shows the SV2800 with all Netmods removed.



Figure 2-5 SV2800 Front view with Netmods Removed

From left to right, the front panel includes an LCD display, keypad, status LEDs, NMI button, reset button, ID button, power button and a USB connector.

Figure 2-6 shows the front panel display area in detail. Note that this unit has a 4 x GigE fiber Netmod installed in the right hand bay.



Figure 2-6 SV2800 Front Panel Controls and Display

The combination of Netmods installed in an SV2800 is not important for FIPS 140-2 validation as the Netmods are all outside of the logical cryptographic boundary (see "[2.3 Module Interfaces](#)" on page 13).

The back of the SV2800 is shown in Figure 2-7 and has the following elements going from left to right:

- Serial port (RJ45 connector)
- VGA display connector
- 2 sets of 2 x USB 2.0 ports
- 2 x GigE ports each with two built in LEDs – port 1 is used for management, port 2 is unused
- 2 x hot swappable power supply bays



Figure 2-7 SV2800 Back Panel

Two covers on the upper surface of the SV2800 can be removed to gain access to the interior of the unit. These covers should not be removed by end users, and may require removal by trained field engineers when maintaining a system. The

two covers can be seen fitted in Figure 2-8, and are shown removed in Figure 2-9. These panels need to be sealed with tamper evident labels when operating in FIPS 140-2 mode.

Section "[3.2 Tamper Evident Label Management and Application Instructions](#)" provides guidance on how and where tamper evident labels need to be applied to the SV2800.



Figure 2–8 SV2800 Front/Top, covered, and with and without Netmods Installed



Figure 2–9 SV2800 Front, Top Cover Removed

For FIPS 140-2 Level 2 validation the SV2800 was tested with the following configuration:

- SV2800 chassis with 1 x NFE acceleration card installed
- Internal SATA DIMM for storage, this is an SSD device installed in a DIMM slot on the system board
- 2 x Intel 5620 quad core CPUs and 24GB of memory

This configuration is Blue Coat part number SV2800.

The SV2800 is a multi-chip standalone module that meets overall FIPS 140-2 Level 2 requirements. The module is validated to the following FIPS 140-2 section levels:

Table 2–3 Security Levels Per FIPS 140-2 Section

FIPS 140-2 Section	Section Title	Validated 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	Not applicable
7	Cryptographic Key Management	2
8	Electromagnetic Interference / Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	Not applicable

2.3 Module Interfaces

The logical cryptographic boundary of the module is shown in the following pictures and diagrams. All of the Netmod interfaces and the switching module that plug into the front of the SV2800 connect to the network segments on which traffic is being monitored/inspected. These ports are only used to access the network data that is being processed by the SV2800; they do not allow access to the management services of the SV2800. The Netmods and associated switch are therefore outside the logical cryptographic boundary. Data input/output to the module from the Netmods and associated switch is via two internal 10Gbps Ethernet connections carried over iPass connectors/cables.

The two plugable power supply units and the bays that they plug into are not associated with any cryptographic processes, keys, critical security parameters (CSP), or any FIPS relevant data, and are therefore deemed to be outside of the cryptographic boundary.

Note: Netmods are NOT hot-swappable. Power off the system before you remove or install Netmod.

Figure 2-10 shows the physical cryptographic boundary as a yellow line with the module being everything contained within the yellow boundary line. The physical boundary is defined by the exterior surfaces of the appliance.

Figure 2-11 provides more clarity, making it clear that the mid-plane and anything that plugs into it such as the Netmods is outside the logical cryptographic boundary.



Figure 2-10 SV2800 Cryptographic Boundary Definition

The front panel display and input devices do not connect to the mid-plane and are connected directly to elements within the logical cryptographic boundary. Therefore the LCD display and keypad, status LEDs, power button and USB connector located on the front panel are considered to be within the logical cryptographic boundary.

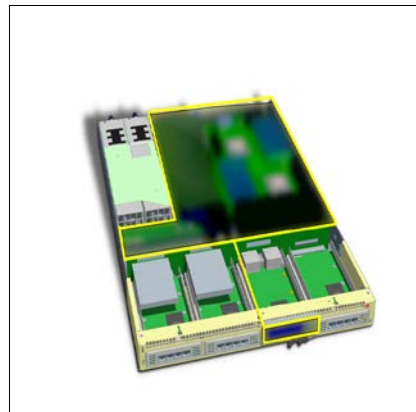


Figure 2-11 SV2800 Internal Layout and Cryptographic Boundary

As noted in Section ["2.2 Module Specification"](#), the SV2800 has a number of connectors located on the front and back panels. These physical interfaces are listed below with details of the FIPS 140-2 logical interfaces they correspond to.

Table 2-4 SV2800 FIPS 140-2 FIPS Logical Interfaces

FIPS 140-2 logical interface	SV2800 port/interface	Panel	Used in FIPS mode?
Data input	2 iPass connectors each carrying a 10Gbps Ethernet link	Internal	Y
Data output	2 iPass connectors each carrying a 10Gbps Ethernet link	Internal	Y
Data output	USB port	Front	Y
Data output	USB ports	Back	Y
Control input/Status output	Keypad	Front	Y
Control input	NMI button	Front	Y
Control input	Reset button	Front	Y
Control input/Status output	ID button	Front	Y
Control input/Status output	Power button	Front	Y
Control input/Status output	USB port	Front	Y
Control input/Status output	Serial port	Back	Y
Control input/Status output	VGA display connector	Back	Y
Control input/Status output	USB port	Back	Y
Status output	Status LED for management Ethernet 1	Front	Y
Status output	LCD display	Front	Y
Status output	Status LED for management Ethernet 2 ^a	Front	Y
Status output	Status LED for hard disk activity	Front	Y
Status output	Status LED for system error	Front	Y
Control input/Status output	Management Ethernet ports 1 and 2 ^b	Back	Y
Status output	Ethernet 1 LEDs	Back	Y
Status output	Ethernet 2 LEDs ^c	Back	Y

Table 2-4 SV2800 FIPS 140-2 FIPS Logical Interfaces

FIPS 140-2 logical interface	SV2800 port/interface	Panel	Used in FIPS mode?
Power input	Power connections from removable PSUs	Back	Y

- a. Ethernet 2 is disabled, so this LED will never light up.
- b. Ethernet 2 is disabled, so it cannot be used for Management.
- c. Ethernet 2 is disabled, so these LEDs will never light up.

The front panel status LEDs for Ethernet 1 and 2 are green when the link is up and flash amber/yellow to indicate traffic flowing over the link. The two LEDs that are part of the Ethernet ports on the rear panel indicate the operating speed of the link and if data is flowing over the link. The left LED viewed from the back of the unit is green if the link is up and flashes to indicate traffic flow. The right LED can be: off indicating a 10 Mbps connection, green indicating a 100 Mbps connection or amber indicating a GigE connection.

The disk activity LED is green and flashes when there is any disk activity on a SATA port in the system.

The system status LED is green/amber and the various display options indicate different system states. Table 2-4 shows the various system states that can be indicated by the system status LED on the front panel of the unit.

Table 2-5 SV2800 System Status Indicator Meaning

Color	State	System status	Meaning
Green	Solid	OK	System ready – no errors detected
Green	Blink	Degraded	Memory, fan, power supply or PCIe failures
Amber	Solid	Fatal	Alarm – system has failed and shut down
Amber	Blink	Non-Fatal	Alarm – system likely to fail – voltage/temp warnings
Green+ Amber	Solid	OK	First 30 seconds after AC power connected
None	Off	Power off	AC or DC power is off

The NMI and Reset buttons are recessed, requiring the use of a straight thin object to press them. Pressing the Reset button will cause the system to be reset. Pressing the NMI button will cause an entry to be saved in the system log file stating that an NMI event was triggered but otherwise has no effect on the system. No information is captured when the NMI button is pressed other than the fact it was pressed.

Pressing the ID button causes a blue LED on the rear panel to the left of the serial port to illuminate. This LED is located behind the back panel, so it is visible through the ventilation holes. The purpose of this LED is to make it easier to locate a system when it is racked in a stack with other systems.

2.4 Roles and Services

The module supports identity based authentication with role based authorization, as required by FIPS 140-2. A single user may have more than one role, and authentication of that user will enable the roles that they are associated with.

The various roles and how they map to FIPS 140-2 defined roles are shown below. For a more detailed listing of the services available to each user, see [Table 2-8](#).

Table 2-6 Description of User Roles

SV2800 Role	Description	FIPS 140-2 role	Authentication type
Auditor	Access to management interface with view only access to logs, appliance settings, and user details. No access to crypto data.	User	Username/ Password
Manage Appliance	Access to management interface and physical appliance with ability to manage appliance, manage alerts and manage users. No access to crypto data or system policies. Cannot set Manage PKI role for a user. Cannot install or reboot appliance without a Crypto Officer present to input the PIN.	Manage Appliance	Username/ Password
Manage Policy	Access to management interface with ability to manage/view policy, manage/view SSL logs and view PKI information.	Manage Policy	Username/ Password
Manage PKI	Access to management interface and physical appliance, with ability to manage/view PKI information, manage PKI role for a user, view appliance settings, and view user details.	Crypto Officer	Username/ Password

It is possible for a single operator to have multiple roles. For example, an administrator might have Manage Appliance and Manage Policy roles, or a Crypto Officer may have both Manage PKI and Manage Policy roles.

For the purposes of FIPS 140-2, any user with the Manage PKI role should be viewed as a Crypto Officer, and any user with the Auditor role should be viewed as a User.

When the system is initialized it enters a bootstrap process and remains in this state until there is at least one user with the Manage Appliance role, and one user with the Manage PKI role. One user could have both roles.

2.4.1 Management Interfaces

Before accessing the module for administrative services, administrators must authenticate using the methods specified in Section ["2.4.2 Authentication Mechanisms"](#). The module offers the following management interfaces:

- WebUI: A graphical user interface accessible remotely with a web browser that supports TLS. Authentication is required before any functionality is available.
- Serial console: A limited command line interface is accessible locally via the serial port. Authentication is required before any functionality is available.

The Web user interface is accessed over a separate management-only Ethernet connection. Connection to this interface does not provide access to data being processed by the module.

A limited set of management interfaces are provided through the LCD, keypad, and LEDs on the front panel of the module. No authentication is required; however, physical access is needed. See [Table 2-8](#) for a full listing of these services.

2.4.2 Authentication Mechanisms

Authentication to the management interfaces enumerated in Section ["2.4.1 Management Interfaces"](#) requires a username and password. Details of the authentication mechanisms are given shown in [Table 2-7](#).

The valid character set that can be used in passwords is:

- lowercase alpha (26 characters)
- uppercase alpha (26 characters)
- numeric (10 characters)
- symbols (32 characters)
- space (one character)

The total valid character set is 95 characters. The password is further limited in that it must contain at least one non-alphabetic character, one uppercase letter, one lowercase letter, and one digit. Further, it cannot be in the dictionary of common passwords. Login attempts are rate limited to 10 per second.

Table A.1 in *NIST Special Publication 800-63-1* shows that with 94 characters there are 30 bits of entropy. 2^{30} is much greater than 1 million, as is $2^{30} / 10$. As the total valid character set of 95 characters is larger than 94 characters, there are at least 30 bits of entropy present.

The PIN configured during initial setup and entered at each subsequent boot must be at least one character, and at most 16 characters. The characters permitted are all uppercase characters, all lowercase characters, and space. Blue Coat recommends using a PIN of at least eight characters.

Table 2–7 SV2800 Authentication Mechanisms

Role	Authentication Type	Single Attempt Strength	Multiple Attempt Strength
Crypto Officer	Username/ password	Passwords must be a minimum of 8 characters with at least one non alphabetic character. The probability of a false positive for a random password guess is less than 1 in 1,000,000. Actual value 2^{30} .	Passwords must be a minimum of 8 characters with at least one non alphabetic character. The probability of a false positive for a maximum of 600 attempts per minute is less than 1 in 1,000,000 over a one minute period. Actual value $2^{30}/10$.
User	Username/ password	Passwords must be a minimum of 8 characters with at least one non alphabetic character. The probability of a false positive for a random password guess is less than 1 in 1,000,000. Actual value 2^{30} .	Passwords must be a minimum of 8 characters with at least one non alphabetic character. The probability of a false positive for a maximum of 600 attempts per minute is less than 1 in 1,000,000 over a one minute period. Actual value $2^{30}/10$.
Manage Appliance	Username/ password	Passwords must be a minimum of 8 characters with at least one non alphabetic character. The probability of a false positive for a random password guess is less than 1 in 1,000,000. Actual value 2^{30} .	Passwords must be a minimum of 8 characters with at least one non alphabetic character. The probability of a false positive for a maximum of 600 attempts per minute is less than 1 in 1,000,000 over a one minute period. Actual value $2^{30}/10$.
Manage Policy	Username/ password	Passwords must be a minimum of 8 characters with at least one non alphabetic character. The probability of a false positive for a random password guess is less than 1 in 1,000,000. Actual value 2^{30} .	Passwords must be a minimum of 8 characters with at least one non alphabetic character. The probability of a false positive for a maximum of 600 attempts per minute is less than 1 in 1,000,000 over a one minute period. Actual value $2^{30}/10$.

2.5 Services and CSP Access

Table 2-7 shows which services can be accessed by users with different roles.

Table 2–8 Services Authorized for Roles

Auditor (User)	Manage Appliance	Manage Policy	Manage PKI (Crypto Officer)	Authorized Service
			Y	Unlock secure store
Y	Y	Y	Y	View dashboards
Y	Y			View system log data
		Y	Y	View/export SSL session log, SSL errors
		Y	Y	View SSL statistics
		Y	Y	View/export intercepted certificates
			Y	Export diagnostic information: PKI state
		Y		Export diagnostic information: policy state
Y	Y	Y	Y	Export diagnostic information: platform state
		Y	Y	Export diagnostic information: SSL statistics
	Y	Y		Export diagnostic information: host statistics, NFP statistics
Y	Y	Y	Y	Export diagnostic information: platform interfaces and platform status statistics
		Y	Y	View debug information: SSL statistics
Y	Y	Y	Y	View debug information: NFE network statistics
	Y	Y		View debug information: NSM host statistics, NSM NFP statistics
		Y		Create/edit/delete rulesets, rules, segments, and user defined lists
		Y	Y	View rulesets, rules, segments, and user defined lists
		Y		Activate/deactivate segments.
			Y	Create/delete/export/import internal CA keys and certificates used for re-signing
			Y	Delete/import external CA certificates
			Y	Delete/import CRLs
			Y	Import/delete trusted certificates

Table 2–8 Services Authorized for Roles

Auditor (User)	Manage Appliance	Manage Policy	Manage PKI (Crypto Officer)	Authorized Service
			Y	Import/delete known keys and certificates
		Y	Y	View PKI information
Y	Y	Y	Y	View software, hardware details
	Y			Configure appliance settings: management network, system time, alerts
Y	Y	Y	Y	View appliance settings
	Y			Configure appliance settings: remote logging configuration
	Y			Create/edit/delete user accounts
			Y	Assign/remove Manage PKI (Crypto Officer) role
Y	Y		Y	View user accounts
Y	Y			View appliance settings: alerts
		Y		Backup policy
		Y		Restore policy
			Y	Backup PKI information
			Y	Restore PKI information
	Y			Backup user accounts
	Y			Restore user accounts
	Y			Backup/restore platform and alert settings
	Y			Halt/reboot appliance from WebUI
			Y	Import user interface certificate and key
Y	Y	Y	Y	Edit grid size in WebUI

If SSL 3.0/TLS 1.0/TLS 1.1 flows using non-approved algorithms are allowed by the policy engine, the flows should be considered as "clear text" due to the use of non-approved algorithms.

Services available to a Crypto Officer and a User are described in [Table 2–9](#). For each service listed, Crypto Officers and Users are assumed to have authenticated prior to attempting to execute the service.

The role of Auditor is equivalent to User, and the role of Manage PKI is equivalent to Crypto Officer.

The type of access to the CSPs uses the following notation:

- Read (R): The plaintext CSP is read by the service
- Write (W): The CSP is established, generated, modified, or zeroized by the service
- Execute (X): The CSP is used within an approved or allowed security function or authentication mechanism

Table 2–9 CSPs Accessed by Authorized Services

User	Crypto Officer	Authorized Service	CSPs
	Y	Unlock secure store	PIN – RX KEK0 - W, X KEK1 - RX Master keys – RX KEK2s - RX Object encryption keys - RX
Y	Y	View dashboards	none
Y		View system log data	none
	Y	View/export SSL session log, SSL errors	none
	Y	View SSL statistics	none
	Y	View/export intercepted certificates	Object encryption keys - X Other entity public keys - R
	Y	Export diagnostic information: PKI state	Object encryption keys - X
Y	Y	Export diagnostic information: platform state	none
	Y	Export diagnostic information: SSL statistics	none
Y	Y	Export diagnostic information: platform interfaces and platform status statistics	none
	Y	View debug information: SSL statistics	none
Y	Y	View debug information: NFE network statistics	none
	Y	View rulesets, rules, segments, and user defined lists	Object encryption keys - X

Table 2-9 CSPs Accessed by Authorized Services

User	Crypto Officer	Authorized Service	CSPs
	Y	Create/delete/export/import internal CA keys and certificates used for re-signing	Object encryption keys - X Resigning CA public keys - RW Resigning CA private keys - RW
	Y	Delete/import external CA certificates	Object encryption keys - WX Trusted certificate public keys - RW
	Y	Delete/import CRLs	Object encryption keys - WX
	Y	Import/delete trusted certificates	Object encryption keys - WX Trusted certificate public keys - W
	Y	Import/delete known keys and certificate	Object encryption keys - WX Known public keys - W Known private keys - W
	Y	View PKI information	Object encryption keys - X Other entity public keys - R Resigning CA public keys - R Trusted certificate public keys - R Known public keys - R Known private keys - R
Y	Y	View software, hardware details	none
Y	Y	View appliance settings	none
	Y	Assign/remove Manage PKI (Crypto Officer) role	Object encryption keys - X
Y	Y	View user accounts	Object encryption keys - X
Y		View appliance settings: alerts	Object encryption keys - X
	Y	Backup PKI information	Backup password - R Backup object key - WX Object encryption keys - X Key exchange public keys - R Key exchange private keys - R Resigning CA public keys - R Resigning CA private keys - R Trusted certificate public keys - R Known public keys - R Known private keys - R

Table 2–9 CSPs Accessed by Authorized Services

User	Crypto Officer	Authorized Service	CSPs
	Y	Restore PKI information	Backup password - R Backup object key - WX Object encryption key - RWX Key exchange public keys - W Key exchange private keys - W Resigning CA public keys - W Resigning CA private keys - W Trusted certificate public keys - W Known public keys - W Known private keys - W
	Y	Import user interface certificate and key	WebUI public key - W WebUI private key - W
Y	Y	Edit grid size in WebUI	none

A limited set of services can be initiated from the front panel keypad, and/or can display output on the front panel display. No authentication is required to access these services; however, physical access to the module is required. Physical access should be limited to the Crypto Officer and the Manage Appliance roles. The available services are described in Table 2-9.

Table 2–10 Services that Do Not Require Authentication

Authorized Service	Description	CSPs
Netmod hardware test ^a	Netmod testing is performed when invoked by a front panel keypad sequence. Status output is displayed on LCD and saved on USB drive.	none
Hardware integrity test	Tests are run automatically at power on/restart. Error and status notifications are displayed on LEDs (see Table 2–5).	none
Firmware integrity test	Tests are run automatically at power on/restart. Error and status notifications are displayed on LCD.	Integrity test public key - RX

Table 2–10 Services that Do Not Require Authentication

Authorized Service	Description	CSPs
Force factory default reset and zeroize keys	<p>Available from the front panel keypad and from the serial console.</p> <p>Factory default reset is forced using the front panel keypad or from the serial console interface. All CSPs and all data on the disk are zeroized. The zeroization occurs while the module is still in Approved mode. See Section "3.5 Module Zeroization" on page 49.</p>	KEK1 - W Master keys – W KEK2s - W Object encryption keys - W WebUI public key - W WebUI private key - W Other entity public keys - W Key Exchange public keys - W Key Exchange private keys - W Resigning CA public keys - W Resigning CA private keys - W Trusted certificate public keys - W Known public keys - W Known private keys - W TLS session keys - W Integrity test public key - W Operator password(s) - W
Enable FIPS mode	Selected during initial configuration from the front panel keypad. Cannot be disabled without a factory default reset.	none
View status	Keypad can be used to scroll through status information on the LCD. Status shown includes network configuration; segment status; statistics such as temperatures, fan speeds, memory utilization, CPU utilization, load; chassis serial number; version of NFE firmware matches expected version.	none
Configure network settings	Keypad can be used to configure network settings. Output is displayed on LCD.	none
Power on/reset appliance	Front panel buttons can be used to power on or reset the appliance. Restarting the appliance includes validating the firmware. It does not include unlocking the secure store with the PIN.	Integrity test public key - RX
Power off appliance	Front panel button can be used to power of the appliance.	none

Table 2-10 Services that Do Not Require Authentication

Authorized Service	Description	CSPs
Setup the module in FIPS mode	Setup the initial configuration for Approved mode of operation and initialize the secure store. See Section "3.3 Module Initialization" .	PIN – RX KEK0 - WX KEK1 - WX Master keys – WX KEK2s - WX Object encryption keys - WX WebUI public key - W WebUI private key - W Key exchange public keys - W Key exchange private keys - W Resigning CA public keys - W Resigning CA private keys - W Trusted certificate public keys - W Operator password(s) - W

- a. Service should only be used when Netmods are installed.

2.6 Physical Security

The SV2800 is a multichip standalone cryptographic module enclosed in a hard, opaque metal case that completely encloses the module's internal components. Ventilation holes provided in the case either do not provide visibility to areas within the cryptographic boundary, or have mechanisms in place to obscure the view of the module's internal components.

Tamper evident labels are fitted to provide physical evidence of attempts to remove the case in order to gain access to the module. Section ["3.2 Tamper Evident Label Management and Application Instructions"](#) shows the placement of the tamper evident labels.

Tamper evident labels are not required on Netmods or power supplies as these are outside the cryptographic boundary of the module.

All module components are production grade. The SV2800 has been tested and meets the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A.

The physical security of the module should be checked on a regular basis, as detailed in Table 2-10.

Table 2–11 Recommended Frequency of Physical Security Checks

Physical Security Mechanism	Recommended Test Frequency	Guidance
Tamper evident labels	Monthly	Examine the module for any sign of removal, replacement or tampering with the tamper evident labels. See Section "3.2.4 Label Inspection" for more details.
Integrity of module enclosure	Monthly	Examine the module for any evidence of new openings or modifications that allow visibility or access to the internal components.

2.7 Non-Modifiable Operational Environment

The operational environment requirements in FIPS 140-2 do not apply to the SV2800, as the module does not provide a general purpose operating system, nor does it allow operators to load software that is not cryptographically signed as being trusted. The SV2800 uses a proprietary non-modifiable operation environment.

2.8 Cryptographic Key Management

The SV2800 implements the FIPS-Approved algorithms listed in Table 2–12. Non-FIPS-Approved algorithms are listed in Table 2–13.

Table 2–12 FIPS Approved Algorithms

Algorithm	Blue Coat SSL Visibility Appliance Crypto Library v0.9.8w Certificate Number	NFP 3240-A2 Certificate Number
Symmetric Key Algorithms		
AES: CBC mode for 128 and 256 bit key sizes	2642	NA
Triple-DES: CBC mode keying options 1 and 2	1585	NA
Asymmetric Key Algorithms		
RSA (ANSI X9.31) key generation - 2048, 3072, 4096 bit	1352	NA
RSA PKCS#1 v1.5 signature generation and verification 1024 (verification only), 2048, 3072 and 4096 bit	1352	NA
RSA PKCS#1 v1.5 signature generation 2048 bit	NA	1238

Table 2–12 FIPS Approved Algorithms

Algorithm	Blue Coat SSL Visibility Appliance Crypto Library v0.9.8w Certificate Number	NFP 3240-A2 Certificate Number
Hashing Functions		
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	2215	NA
Message Authentication Code (MAC) Functions		
HMAC with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	1634	NA
Random Number Generator		
ANSI X9.31 RNG: AES-256 key	1246	NA
Key Derivation		
SP 800-132 v2 section 5.4 PBKDF option 2a	Vendor affirmed	NA
CVL	123	NA

Note: See NIST *SP 800-131A* for more information, as some algorithms may be classified as deprecated, restricted, or legacy-use in the upcoming algorithm transition.

Table 2–13 SV2800 Non-FIPS 140-2 Approved/Allowed Security Functions

Algorithm	Details
RSA	Used for negotiating TLS sessions for management, negotiating SSL/TLS sessions during SSL/TLS interception, resigning server certificates during SSL/TLS interception, making policy decisions for SSL/TLS interception, SSL/TLS decryption and inspection. Key size range: 512 - 15360 bits Key wrapping; key establishment methodologies provide between 112 and 256 bits of encryption strength; non-compliance less than 112 bits of encryption strength.
EC Diffie-Hellman	Used for SSL/TLS sessions during SSL inspection. Key size range: 163 - 571 bits All NIST defined B, K, and P curves Key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength; non-compliant less than 112 bits of encryption strength.
True RNG (TRNG)	Implemented in hardware. Used to provide additional entropy to NDRNG.
Non-deterministic RNG (NDRNG)	Used to seed ANSI X9.31 RNG.
MD5	Used for SSL/TLS sessions during SSL inspection.

Table 2–13 SV2800 Non-FIPS 140-2 Approved/Allowed Security Functions

Algorithm	Details
RC4	Used for SSL/TLS sessions during SSL inspection.
Camelia	Used for SSL/TLS sessions during SSL inspection. Key sizes: 128, 256 bit keys Mode: CBC
DES	Used for SSL/TLS sessions during SSL inspection. Mode: CBC
RSA PKCS #1 wrap/unwrap	Used for SSL/TLS sessions. The key wrapping methodology provides between 112 and 256 bits of encryption strength; non-compliant under 112 bits of encryption strength.
Diffie-Hellman	Used for SSL/TLS sessions during SSL inspection. Diffie-Hellman public key size range: 512 - 15360 bits Diffie-Hellman private key size range: 96 - 512 bits Key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength; non-compliant less than 112 bits of encryption strength.
MD5 based HMAC	Used for SSL/TLS sessions during SSL inspection.

When the module generates ephemeral Diffie-Hellman keys for key exchange, RSA Key wrapping keys for key exchange, or Elliptic Curve Diffie-Hellman keys for key exchange, it uses the same key length as the key seen in the SSL/TLS handshake. The module does not control the size of the keys used by the SSL/TLS endpoints for key exchange.

If SSL 3.0/TLS 1.0/TLS 1.1 flows using non-approved algorithms are allowed by the policy engine, the flows should be considered "clear text" due to the use of non-approved algorithms.

The module supports the following Critical Security Parameters:

Table 2–14 SV2800 Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation/ Input	Output	Storage	Use
Key-encrypting -key 0 (KEK0)	AES CBC 256 bit key	Derived from PIN, using PBKDFv2	Never exits the module	Never stored	KEK0 encrypts KEK1 if KEK1 is saved to USB

Table 2–14 SV2800 Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation/ Input	Output	Storage	Use
Key-encrypting-key 1 (KEK1)	AES CBC 256 bit key	Derived from PIN, using PBKDFv2, or generated using PRNG	Encrypted with KEK0 and output to USB if USB is used, otherwise never exits the module	USB stick or stored in volatile memory	KEK1 encrypts the master keys
Master key	AES CBC 256 bit key	Internally generated using PRNG	Never exits the module	Encrypted using KEK1 and stored on main disk	Used to encrypt KEK2s
Key-encrypting-key 2 (KEK2)	AES CBC 256 bit key	Internally generated using PRNG	Never exits the module	Encrypted using associated master key and stored on main disk	Used to encrypt object encryption keys
Object encryption key	AES CBC 256 bit key	Internally generated using PRNG	Never exits the module	Encrypted using associated KEK2 and stored on main disk	Encrypt data and other CSPs for storage
WebUI public key ^a	RSA 2048 bits only for internally generated RSA 2048, 3072, 4096 bits can be imported	Internally generated using PRNG or can be imported in plaintext	During TLS negotiation in plaintext	Stored in plaintext on internal disk	Negotiating TLS sessions for management
WebUI ^b private key	RSA 2048 bits only for internally generated RSA 2048, 3072, 4096 bits can be imported	Internally generated using PRNG or can be imported in plaintext	Never exits the module	Stored in plaintext on internal disk	Negotiating TLS sessions for management

Table 2–14 SV2800 Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation/ Input	Output	Storage	Use
Other entity public key	RSA 2048, 3072, 4096, 8192 bits DH 2048-15360 bits; all NIST defined B, K, and P curves 224 bits and higher	Sent to the module in plaintext	If not intercepted, output as part of SSL/TLS handshake Viewable in plain text from WebUI	Other entities' public keys reside in volatile memory and may be cached encrypted with associated object encryption key and stored on internal disk	Negotiating SSL/TLS sessions during SSL/TLS interception
Key exchange public key	RSA 2048, 4096 bit DH 2048-15360 bits; all NIST defined B, K, and P curves	Internally generated using PRNG Imported from an encrypted backup	Output during SSL/TLS session negotiation in plaintext. Exported in encrypted backup	Encrypted with associated object encryption key and stored on internal disk	Negotiating SSL/TLS sessions during SSL/TLS interception
Key exchange private key	RSA 2048, 4096 bits DH 160 - 512 bits; all NIST defined B, K, and P curves 224 bits and higher	Internally generated using PRNG Imported from an encrypted backup	Exported in encrypted backup	Encrypted with associated object encryption key and stored on internal disk	Negotiating SSL/TLS sessions during SSL/TLS interception
Resigning CA public key	RSA 2048 bits only for internally generated RSA 2048, 3072, 4096, 8192 bits can be imported	Internally generated using PRNG. Can be imported in encrypted format (PEM or PKCS12 or PKCS8) or plaintext, or from encrypted backup	During TLS negotiation in plaintext. Exported in plaintext in a certificate, or in an encrypted backup	Encrypted with associated object encryption key and stored on internal disk	Resigning server certificates during SSL/TLS interception

Table 2–14 SV2800 Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation/ Input	Output	Storage	Use
Resigning CA private key	RSA 2048 bits only for internally generated RSA 2048, 3072, 4096, 8192 bits can be imported	Internally generated using PRNG Can be imported in encrypted (PEM or PKCS12 or PKCS8) or plaintext, or from encrypted backup	Exported in encrypted backup	Encrypted with associated object encryption key and stored on internal disk	Resigning server certificates during SSL/TLS interception
Trusted certificate public key	RSA 2048, 4096 bits	Imported in plaintext or encrypted form (PEM or PKCS12 or PKCS8), or from encrypted backup	Exported in encrypted backup	Encrypted with associated object encryption key and stored on internal disk	Making policy decisions for SSL/TLS interception
Known public key	RSA 2048, 4096, 8192 bits	Imported in plaintext or encrypted form (PEM or PKCS12 or PKCS8), or from an encrypted backup	Exported in encrypted backup	Encrypted with associated object encryption key and stored on internal disk	SSL/TLS decryption and inspection
Known private key	RSA 2048, 4096, 8192 bits	Imported in plaintext or encrypted form (PEM or PKCS12 or PKCS8), or from an encrypted backup	Exported in encrypted backup	Encrypted with associated object encryption key and stored on internal disk	SSL/TLS decryption and inspection
SSL/TLS session key	AES CBC 128, 256 bit key Triple-DES CBC keyring option 1 and 2	Internally generated using PRNG	Never exits the module	Stored in volatile memory	Encrypting SSL/TLS session data
SSL/TLS session authentication key	HMAC SHA-1	Internally generated	Never exits the module	Stored in volatile memory	Data authentication for SSL/TLS sessions

Table 2–14 SV2800 Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation/ Input	Output	Storage	Use
Backup password	Minimum of 8 characters	Entered over a secure remote session	Never exits the module	Stored in volatile memory	Derive backup object key
Backup object key	AES CBC 256 bit key	Derived from backup password using PBKDFv2	Never exits the module	Stored in volatile memory	Encrypting backup data
PIN; or “master key password”	1-16 characters	Keypad entry by Crypto Officer	Never exits the module	Stored in volatile memory	Used to derive KEK0 if USB is used. Used to derive KEK1 if USB is not used.
Integrity Test Public key	RSA 1024 bit key	Externally generated	Never exits the module	Plaintext on internal disk	Verifying the integrity of the system image during startup
Operator password	Minimum of 8 characters	Enters over a secure remote session	Never exits the module	Encrypted with associated object encryption key and stored on internal disk	Authenticating administrative access
ANSI X9.31 PRNG seed	32 bytes	Internally generated using entropy from NDRNG	Never exits the module	Plaintext in volatile memory	Seeding the FIPS approved PRNG
ANSI X9.31 PRNG key	32 bytes	Internally generated using entropy from NDRNG	Never exits the module	Plaintext in volatile memory	Seeding the FIPS approved PRNG

- a. The Crypto Officer shall only import RSA 2048bit or larger keys.
- b. The Crypto Officer shall only import RSA 2048 bit or larger keys.

During the bootstrap process, you may select to have an AES-256 bit key (KEK1) stored on a removable USB drive. If the option is chosen, KEK1 is encrypted using an AES-256 bit key (KEK0) derived from the PIN prior to being stored on the USB drive. Whenever the device is power cycled or restarted, it will require this drive to be plugged in and the PIN to be input from the front panel keypad. Only with

both the USB drive and the correct PIN can the master keys be unlocked to gain access the secure store. If the option is not chosen, KEK1 is derived from the PIN directly and no KEK0 is created.

KEK0 and KEK1 are derived from the PIN using the FIPS approved Password Based Key Derivation Function (PBKDF) defined in PKCS#5 v2.0; details are provided in *NIST Special Publication 800-132*.

The PIN contains between 8 and 16 characters (when set using the guidance provided) that can be upper or lower case alphabetic characters or the “space” character. Keys derived from the PIN are only used for storage applications. According to *NIST Special Publication 800-63* the strength of the human-generated PIN is between 18 bits and 30 bits. Thus, the probability of a random guess is between 1 in 26^{2e3} (for 8 characters) and 1 in $1e^9$ (for 16 characters)).

During the bootstrap process, a set of AES 256 bit master keys are created using the internal PRNG. Master keys are encrypted with KEK1 and stored internally. The master keys are used to encrypt AES 256 bit object keys. Object keys are created using the internal PRNG and are used to encrypt data and keys for storage. Object keys are created during the bootstrap process and as needed during normal operations. Object keys are stored internally.

2.9 Self Tests

The SV2800 performs the following Power On Self Tests (POST). These are run even if FIPS mode is not enabled:

- Firmware (software) integrity test checks critical O/S components and appliance software binaries using RSA signature verification (1024 bit)
- AES encrypt/decrypt known answer tests (KAT) on software bulk ciphers (128 bit, CBC mode)
- Triple-DES encrypt/decrypt known answer tests (KAT) on software bulk ciphers (keying options 1 and 2)
- RSA known answer tests (KAT) on software signature operations (sign and verify) using the following digests (1024 bit)
 - SHA-1
 - SHA-224
 - SHA-256
 - SHA-384
 - SHA-512
- RSA known answer tests (KAT) on NFP hardware signature operations (sign and verify) using the following digests (1024 bit)
 - SHA-1
 - SHA-224
 - SHA-256
 - SHA-384

-
- SHA-512
 - RSA known answer tests (KAT) on hardware based encryption (encrypt and decrypt)
 - RSA known answer tests (KAT) on software based encryption (encrypt and decrypt)
 - HMAC known answer tests (KAT) on software using the following digests
 - SHA-1
 - SHA-224
 - SHA-256
 - SHA-384
 - SHA-512
 - SHA known answer tests (KAT) on software hash for the following
 - SHA-1
 - SHA-224
 - SHA-256
 - SHA-384
 - SHA-512
 - X9.31 RNG known answer test (KAT)
 - TRNG duplicate and zero output tests

All POSTs are run automatically at start-up. If an error is encountered, the system enters an error state and powers off. The firmware integrity test outputs an error message to the VGA console, serial console, and front panel LCD. Error messages for all other POSTs are output to the system log file and to the front panel LCD.

Once the POSTs have passed, the Crypto Officer can enter the PIN to begin the process of unlocking the secure store and allowing the system to begin operation.

The SV2800 carries out the following conditional self tests:

- Continuous Random Number Generator test for FIPS approved X9.31 deterministic RNG (PRNG)
- NDRNG test when seeding X9.31 RNG (PRNG) at boot
- Continuous TRNG duplicate and zero output tests
- RSA pairwise consistency test when generating RSA keys in software

If an error is encountered in the self tests, the appliance will enter the error state. Error messages are output to the system log file and to the front panel LCD.

The module implements the following critical function tests:

- Adding additional entropy to non-deterministic RNG (NDRNG)

If the critical function test fails, the appliance will enter the error state, and an error message is output to the system log file and to the front panel LCD.

In the event that the system enters an error state, Crypto Officer attention is required to clear the error state.

2.10 Design Assurance

Blue Coat uses the Mercurial Source Code Management (SCM) system for software and document version control, code sharing and build management.

The product is developed primarily in the high level programming languages C++, C, and Python. Assembly code is used for select performance enhancements.

The module is securely delivered from Blue Coat to customers via the mechanism specified by the customer. FedEx, UPS, or any other freight forwarder of their choice can be utilized.

2.11 Mitigation of Other Attacks

The module does not claim to mitigate any attacks beyond those defined in the FIPS 140-2 Level 2 requirements.

3. Secure Operation

The SV2800 conforms to FIPS 140-2 level 2 requirements. This section contains details on how to place the SV2800 into a FIPS approved mode of operation and how to maintain FIPS approved operation.

3.1 Cryptographic Officer Guidance

The Crypto Officer is responsible for initialization and management of the security relevant configuration parameters within the SV2800. The Crypto Officer can access the SV2800 remotely using TLS. When accessed using TLS, the system provides an HTTPS graphical user interface (WebUI).

The Crypto Officer can import an RSA private key and certificate to be used by the WebUI for establishing a TLS session. The Crypto Officer shall only import RSA 2048 bit or larger keys. RSA keys less than 2048 bits are no longer approved for use as of January 1, 2014. See NIST *SP 800-131A* for details.

The Crypto Officer must be allowed physical access to the SV2800. Physical access to the module shall be limited to the Crypto Officer and the Manage Appliance administrators.

Full details on how to configure and manage the SV2800 are contained in the *Blue Coat Systems SV2800 Administration and Deployment Guide for software version 3.5*. This guide can be downloaded from the Blue Coat customer support site (<https://bto.bluecoat.com>).

3.2 Tamper Evident Label Management and Application Instructions

Before enabling FIPS mode the Crypto Officer shall verify that all tamper evident labels are in place and undamaged. If a label is damaged or has been removed (in order to conduct system maintenance for example), then the Crypto Officer must ensure that the damaged or missing label is replaced, and a factory default reset must be performed on the SV2800 before proceeding to enable FIPS mode.

A total of three tamper evident labels must be fitted to the module. In the event that the tamper evident labels require replacement, a pack of new labels can be purchased (P/N: FIPS-LABELS-SV).

The Crypto Officer shall be responsible for the secure storage of any label kits. The Crypto Officer shall be present whenever tamper evident labels are removed or installed to ensure security is maintained and that the module is returned to a FIPS approved state.

Figure 3-12 shows a tamper evident label that has been tampered with. If the "VOID" image is visible or there is other physical damage to the label, the device should not be placed into FIPS mode.

The tamper evident seals shall be installed for the module to operate in a FIPS Approved mode of operation.

The details below show the location of all tamper evident labels and also detail how to remove and replace a label if this is required.



Figure 3-12 Evidence of Tampering

3.2.1 General Label Information

If tamper evident labels require fitting or replacing then this must only be done by the Crypto Officer. The following guidelines must be followed.

- Apply labels to a clean, dry surface. Oily, wet or dusty surfaces will prevent proper label adhesion. Clean each of the designated label areas with isopropyl alcohol, and make sure it is thoroughly dry. Apply a small amount of alcohol to a clean, lint-free cloth. Rub the area to be cleaned for several seconds. Dry the area with a dry portion of the cloth, or allow it to air dry. Do not blow on it, as this may cause saliva to be applied to the surface. Do not touch the surface after it has been cleaned.
- Apply labels to the metal starting at the bend line and with smooth outward strokes toward either end of the label. This will reduce bubbles.
- Once a label is applied, it should not be touched for 2-4 hours to allow the adhesive to cure.
- Apply labels at a temperature of 65F (18C) or above.

3.2.2 Supplied Labels

If tamper evident labels require fitting or replacing then this must only be done by the Crypto Officer using a label kit obtained from Blue Coat Systems.

Labels are supplied in a kit that includes four labels in a bag and one label on the bag. The two smaller labels are 1.5 x 0.6 inches, and are identical. The two larger labels are 2.875 x 1.0 inches, and are identical. The serial number on all labels and on the bag must all be the same.

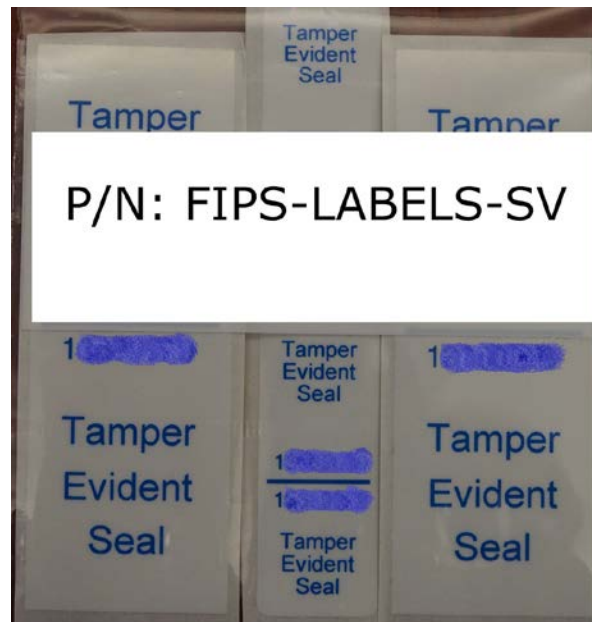


Figure 3–13 FIPS Label Kit

Labels that are applied to the box have the number printed on them twice, once for each plane the label will be in. Each label goes around an edge and secures two planes.

The supplied label kit should be inspected as follows:

- If the labels do not have matching number, or if the bag has been opened, reject the labels.
- If the style of letters does not appear to be the same on all labels, reject the labels. The size of the lettering is smaller on the smaller label.
- If the labels indicate tampering, reject the labels.

The two larger labels in the bag are identical. These are applied to the edge between the top of the chassis and the sides. These labels are white with blue ink.

The two smaller labels in the bag are identical. One of these labels is applied to the top, rear cover of the chassis. The remaining label is a spare label that must be securely stored or destroyed. These labels are also white with blue ink.

The entire label packet must be rejected if the large or small labels are not identical, or if the colors are not white with blue ink.

It is not possible to purchase individual replacement labels. They are only provided as a kit. Three of the labels in the kit should be applied to the system, and the spare label stored securely or destroyed. [Figure 3–13](#) shows a FIPS label kit; the label numbers have been obscured for security.

3.2.3 Label Application

The labels must be applied to the unit without the slide rail kit attached. This can be done before installation or by removing the unit from the rack.

Note: **Warning.** Removal of the unit may require two people and should only be done by qualified personnel.

Note: **Warning!** Failure to follow correct procedure can cause the unit to fall and may cause damage to the unit, other equipment or injury to personnel.

If the unit is mounted in a rack, the unit must be removed. If the unit uses the standard slide kit, follow these steps:

1. Power off the unit.
2. Disconnect all cabling.
3. Provide a clean work surface for applying the labels.
4. Remove the two screws that (optionally) hold the front of the unit to the rack rails. These may not be installed.
5. Pull the unit out from the rack until it stops.
6. Slide the black arrows on the inner slide pieces forward.
7. While holding the arrows, carefully slide the chassis out of the out slide pieces.
8. Remove each inner slide piece by pressing the square button and sliding the inner slide piece toward the back of the unit. This will disengage it from all supports.

To reinstall the unit, follow the installation guide procedure.

Left Side Label Application

The left side label (one of the larger labels which is white, with blue ink) is applied between the middle and rear top covers, this is denoted label 1. It indicates tampering if either of these pieces is removed. Installation involves the following steps:

1. Peel the label from its backing.
2. Place the alignment line along the top left edge of the chassis such that the label is centered on the seam. The markings should be oriented so that the text is "up."
3. Visually verify that continuing the application of the label will cause the screw on the left side of the rear cover panel to be fully covered.
4. Starting at the edge, press on the label and work toward the center of the top of the chassis. Ensure that no bubbles are present.
5. Again starting at the edge, press on the label and work down the left side toward the bottom of the chassis. Ensure that no bubbles are present.
6. Press firmly to all parts of the label to make sure it is fully applied.
7. Confirm that the screw on the left side is fully covered.

Right Side Label Application

The right side label (the second larger one which is white, with blue ink) is applied between the middle and rear top covers, this is denoted label 2. It indicates tampering if either of these pieces is removed. Installation involves the following steps:

1. Peel the label from its backing.
2. Place the alignment line along the top right edge of the chassis such that the label is centered on the seam. The markings should be oriented so that the text "up."
3. Visually verify that continuing the application of the label will cause the screw on the right side of the rear cover panel to be fully covered. Also, the top rivet and rear indentation should be fully covered by the label.
4. Starting at the edge, press on the label and work toward the center of the top of the chassis. Ensure that no bubbles are present.
5. Again starting at the edge, press on the label and work down the right side toward the bottom of the chassis. Ensure that no bubbles are present.
6. Press firmly to all parts of the label to make sure it is fully applied.
7. Confirm that the screw on the right side is fully covered.
8. Confirm that the top rivet on the right side is fully covered.
9. Confirm that the rear indentation is fully covered.

Rear Label Application

The rear label (one of the smaller labels which is white with blue ink) is applied to the center tab on the rear top cover, this is denoted label 3.

This label has a shorter section and a longer section. The shorter section goes on the tab and the longer section goes on the top of the cover. This label indicates tampering if the screw that it covers is removed. Installation involves the following steps:

1. Orient the label so that the text is “up.”
2. Remove the label from the backing.
3. Place the alignment line along the top rear edge of the chassis. Take care to make sure that the label will be completely on the tab when it is applied. The label cannot hang over the edge of the tab.
4. Starting at the edge, press on the label and work down toward the bottom. Make sure that there are no bubbles. Make sure the screw is fully covered. Verify that the label does not hang over the edge of the tab.
5. Starting at the edge, press on the label and work toward the center of the chassis. Make sure that there are no bubbles.
6. Press firmly to all parts of the label to make sure it is fully applied.
7. Confirm that the screw on the rear tab is fully covered.

Follow the installation guide to reinstall the chassis into the rack.

3.2.4 Label Inspection

Before enabling FIPS mode the Crypto Officer must verify that all tamper evident labels are in place and undamaged. The following should be checked before enabling FIPS mode and at regular intervals while the device is operating in FIPS mode:

- Matching numbers.
- Correct colors of label and ink.
- Correct numbers if this information is recorded.
- Indications of tampering (“VOID” markings on the labels).
- Missing labels.
- Labels that do not stick properly.
- Labels that have the edges damaged.
- Discolored or distorted labels.

Following the above guidelines, tamper evident labels at three locations on the SV2800 should be checked in order to ensure that the unit cannot be opened in a manner that allows access to components within the cryptographic boundary.

Figure 3-14 shows the location of the tamper evident label that should be fitted to the rear of the SV2800. The label is applied over the top of the screw that secures the top panel to the rest of the unit, and in such a way that it is impossible to remove the screw or to remove the top panel of the unit without the label being voided.



Figure 3–14 Rear Panel Label Placement

Figure 3-15 shows the rear panel without the label fitted. The label is affixed to the solid panel around the screw, and folds over to adhere to the top panel of the SV2800.



Figure 3–15 Rear Panel without Label Fitted

The remaining two labels are applied to the left and right sides of the SV2800 and prevent the top panels from being removed.

Note: If the cooling fans need to be replaced, the top panel will need to be opened. This will void the labels. A new label kit must be installed after the top panel is opened. The module must also be factory default reset and reinstalled in FIPS approved mode.

Figure 3-16 shows the location of the side and rear labels on the SV2800.



Figure 3–16 Overview of Side and Back Label Positions

Figure 3-17 shows the SV2800 with no Netmods, and with labels.



Figure 3–17 Top Front View with Labels, No Netmods

In the examples, references to left side and right side of the unit mean when viewed from the front.

Figure 3-18 shows the location of the tamper evident label that should be fitted to the right side of the SV2800. The label is applied over the top of the screw that secures the top panel to the rest of the unit and in such a way that it is impossible to remove the screw or to remove the top panel of the unit without the label being voided. Figure 3-19 shows the right side of the SV2800 without the label fitted. The label is affixed to the solid panel around the screw, and folds over to adhere to the top panel of the SV2800.

The corresponding labels should be applied in exactly the same manner to the left side of the SV2800.



Figure 3–18 Right Side Label Location



Figure 3–19 Right Side without Label Fitted

3.3 Module Initialization

The SV2800 can only be placed into or removed from FIPS mode during the bootstrap process when the system is being powered up. The SV2800 will enter the bootstrap process whenever it is powered on or reset. The option to turn FIPS mode on or off is only available during the bootstrap process if the device does not already have a configuration for FIPS mode.

In order to erase the existing FIPS mode configuration and allow FIPS mode to be configured during the bootstrap process, a factory default reset needs to be carried out. Using the front panel keypad, the administrator can trigger a factory default reset by typing a key sequence on the front panel.

The front panel keypad, shown in Figure 3-20, has the keys arranged in the following layout

0	1
2	3

Figure 3–20 Keypad Layout

If the following key sequence is entered during the first 5 seconds after the unit is powered on a factory-default-reset will take place:

- 031203

Note: The factory default sequence only works after the LCD turns on and says "Loading..." on the second line. You have five seconds to enter the sequence at this point.

A factory default reset can also be triggered from the boot loader if a monitor and keyboard are attached to the appliance during boot.

After the factory-default-reset, the SV2800 will be in the same state as when it was originally received and will enter the bootstrap mode when powered on. Full details of the bootstrap process are provided in the *Blue Coat Systems SV2800 Administration and Deployment Guide for software version 3.5*.

During bootstrap mode the WebUI needs to be accessed. By default, the SV2800 will be using DHCP to acquire an IP address. The front panel keypad and LCD can be used to enter IP configuration mode which allows the management network to be configured to use a static IP address. The IP address settings will then be used during the bootstrap phase, and then saved.

Once the SV2800 is in bootstrap mode the WebUI will appear as in Figure 3-21. The only choice for FIPS mode is to enable it or not. Select FIPS Mode Enabled.

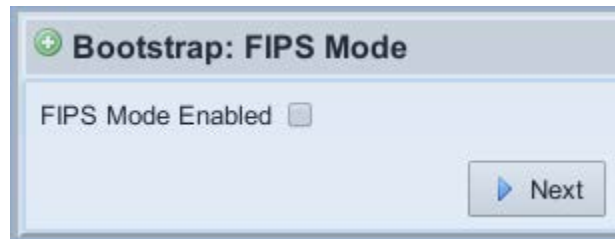


Figure 3–21 FIPS Enable Screen

Once FIPS mode has been selected and the setting has been saved to the secure store, it can only be changed by forcing the system to do a factory default reset. When FIPS mode is selected, a PIN must be created. The PIN must be input by the Crypto Officer and a written copy stored in a secure location accessible only to the Crypto Officer. Whenever the device is power cycled or restarted it will require that the PIN be input from the front panel keypad in order to unlock the master keys, and so access the secure store.

The key sequence “01230123” must be input to enable the PIN entry mode. See the *Blue Coat Systems SV2800 Administration and Deployment Guide for software version 3.5* for more information.

Note: If a USB memory stick is being used for additional security, always insert it before inputting the PIN.

Note: During subsequent restarts of the module, if the PIN is entered incorrectly, you will not see an error. Reinput the PIN.

Once in FIPS mode, the web GUI will appear as in Figure 3-22.

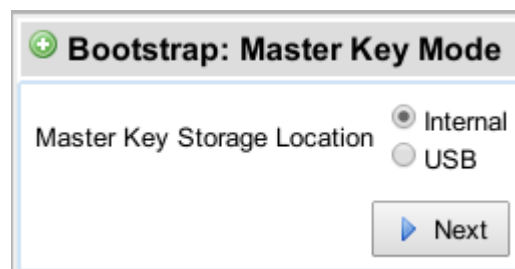


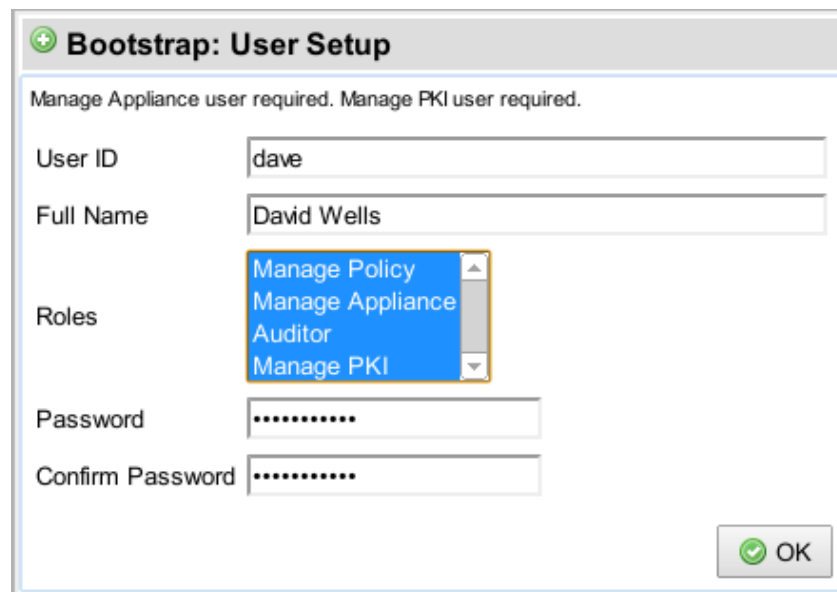
Figure 3–22 FIPS Mode Initial Bootstrap Input Screen

For best security, select the master key storage location to be USB. If the option is chosen, KEK1 is encrypted using an AES-256 bit key (KEK0) derived from the PIN prior to being stored on the USB drive.

Whenever the module is power cycled or restarted, it requires this drive to be plugged in, and the PIN to be input from the front panel keypad. Only with both the USB drive and the correct PIN can the master keys be unlocked to gain access the secure store. The Crypto Officer should maintain control of the USB drive.

If the option is not chosen, only the PIN needs to be entered when the module is power cycled or restarted.

The final stage of the bootstrap process is user setup. At least one user with the Manage Appliance role, and one user with the Manage PKI role must be created. The same user can be given one or more roles. The screen allowing configuration of user(s) with these roles is shown in Figure 3-23.



Bootstrap: User Setup

Manage Appliance user required. Manage PKI user required.

User ID: dave

Full Name: David Wells

Roles: Manage Policy, Manage Appliance, Auditor, Manage PKI

Password:

Confirm Password:

OK

Figure 3–23 Bootstrap User Setup Screen

After creating the necessary user(s) the normal system login screen will appear allowing the user to login, at which point they will have access to the full WebUI to manage the SV2800. At this point a user with the Manage Appliance role can create additional users but cannot give these users the Manage PKI role. Only a user with the Manage PKI role can give this role to a user.

3.4 Module Management

The Crypto Officer can manage the SV2800 via the WebUI (HTTPS over TLS), and the serial console. The Crypto Officer also has physical access to the module and can perform limited management functions, as detailed in [Table 2-10](#). Detailed instructions on how to monitor and troubleshoot the SV2800 are contained in the *Blue Coat Systems SV2800 Administration and Deployment Guide for software version 3.5*.

The Crypto Officer should monitor the SV2800 status regularly. Any irregular activity or reported errors should be investigated by the Crypto Officer and corrected. In the event that correction is not possible, the customer should contact Blue Coat Support for advice.

To take the system out of FIPS mode a factory default reset is required, which will cause all data in the secure store to be zeroed. After the factory default reset, the system will be in the same state as when it originally shipped from the factory. When powered on the system will enter bootstrap mode, during which the FIPS mode for the device can be configured.

3.5 Module Zeroization

Whenever the SV2800 is being taken out of service, returned to Blue Coat for service, or disposed of at the end of its life, the Crypto Officer must ensure that all FIPS mode CSP data is zeroed. This is achieved by forcing the box to undergo a factory default reset. The Crypto Officer must wait until the factory default reset has completed and the system has returned to the bootstrap state to ensure that all data has been zeroed.

The following techniques are used during zeroization:

- Overwrite of entire disk with zeros.
- Factory default reset can only be triggered during a reboot of the appliance.
- All keys and CSPs are zeroized.
- No keys or CSPs are retained after zeroization.
- During the boot process, no remote access to the appliance is possible. After the factory default reset has been triggered during the boot process, no additional commands can be given until the reset has been completed. This prevents an attacker from influencing the zeroization procedure.

