Hewlett-Packard Company
5400/8200 zl Switch Series

Module Name: HP Networking 5400 zl [1,2] and 8200 zl [3,4] Switch Series

Hardware Versions: 5406 zl [1] 5412 zl [2], 8206 zl [3], 8212 zl [4] [A] [B]; Switches: (J8697A [1], J8698A [2], J9447A [3] and J9091A [4] [A] [B]); Management Modules: (J8726A [1,2] and two J9092A [3,4] [A] [B]); Power Supply: (J9306A: one [1,3] or two [2,4]); Support Module: (J9095A [3,4] [A] [B]); Fabric Module: (two J9093A [3,4] [A] [B]); Blank Plate: (5069-8563: five [1,3] or eleven [2,4]); PSU Blank Plate (5003-0753: one [1,3] or two [2,4]); Opacity Shield Kits: (J9710A [1], J9711A [2], J9712A [3] and J9713A [4]); High Performance Fan Trays: (J9721A [1], J9722A [2], J9723A [3] and J9724A [4]); with ([HP Gig-T/SFP+ V2 zl Mod: J9536A] and [Tamper Evident Seal Kit: J9709A]) [1,2,3,4]

Firmware Versions: K.15.07.0003 [A] and K.15.07.0012 [B]

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 1.2.1

Prepared for:

Hewlett-Packard Company
8000 Foothills Blvd
Roseviillle, CA 95747
United States

Phone: +1 (800) 334-5144
http://www.hp.com

Prepared by:

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

Phone: +1 (703) 267-6050
http://www.corsec.com

Disclaimer

The information contained in this document is subject to change without notice.

HEWLLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.
The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be constructed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the 5400/8200 zl Switch Series from Hewlett-Packard Company This Security Policy describes how the 5400/8200 zl Switch Series meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The 5400/8200 zl Switch Series is referred to in this document as 5400/8200 zl switches, the switches, the cryptographic modules, or the modules.

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 HP website (www.hp.com) contains information on the full line of products from HP.
- 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
- Other supporting documentation as additional references

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

1.4 Document Terminology

This document uses FIPS 140-2 terminology that slightly differs from terminology used in the HP Networking product documentation. Please use Table 1 as a reference to avoid confusion.

.

Table 1 – FIPS 140-2 Terminology Comparison

FIPS 140-2 Terminology	HP Networking Equivalent
Cryptographic Module / Module	Refers to the cryptographic physical boundary, such as a 5406, 5412, 8206, 8212 zl Switch (for example, a '5406 cryptographic module' or '5406 module')
Cryptographic Officer (CO)	Refers to the system (cryptographic module) Manager
User	Refers to a user with "Operator" privileges
operator	Refers to an undefined user of the switch
Card	Used in place of a 'zl module' that is installed in a zl switch, such as the zl Management Module, System Support zl Module, and v2 zl Modules. For example, "zl Management card" or "v2 zl card".
Interface	Refers to 1 of 5 FIPS 140-2 logical interfaces (Data in/out, Status out, Control in, Power)

.

2 5400/8200 zl Switch Series

2.1 Overview

The performance, features, and reliability of the 5400/8200 zl switches make them suitable for many applications throughout a network topology – from mission-critical enterprise-class access layer deployments to moderately sized core use models. The 5400/8200 zl Switch Series offer flexibility, in-chassis redundancy, and scalability in modular form factors. The 5400 zl Switch Series is available as a 4U or 7U rack mountable, modular chassis. The 5400 zl Switch Series provides Intelligent Edge features with baseline high availability in a modular form factor. The 8200 zl Switch Series is available as a 6U or 9U rack mountable, modular chassis. The 8200 zl Switch Series combines high performance with comprehensive networking and security features in a highly scalable, modular chassis solution. Together, the 5400/8200 zl switches offer a wide range of networking applications and services.

Key features of the 5400/8200 zl Switch Series include:

- Performance – High-capacity switching fabric
- Security – Virus throttling, detection of malicious attacks, and user access control
- Operational Flexibility – High port density, versatile intelligent ports, and optional service modules
- Resiliency – Redundant power supplies, switch meshing, Virtual Router Redundancy Protocol (VRRP), and redundant management and Fabric Cards (8200 zl series)

Figure 1 shows a sample deployment scenario for the 5400/8200 zl Switch Series.

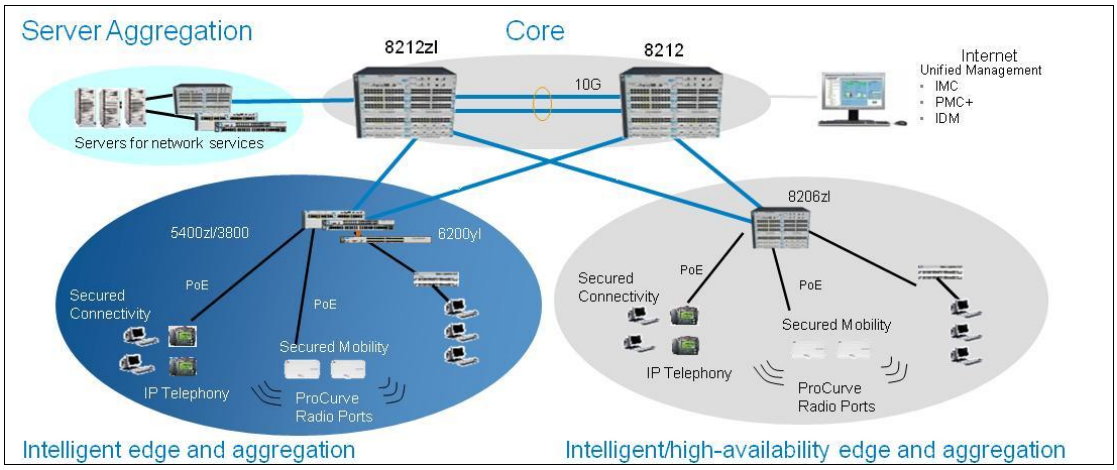

Figure 1 – Sample Deployment for 5400/8200 zl Switch Series

.

2.1.1 HP 5400 zl Switch Series Cryptographic Modules

The HP 5400 zl switches (Figure 2 and Figure 3) are the most advanced intelligent edge switches in the HP Networking product line. The 5400 zl Switch Series is available as a 4U (5406 zl) or 7U (5412 zl) rack mountable, modular chassis. The 5406 zl switch provides 6 interface card slots and the 5412 zl switch provides 12 interface card slots. With a wide variety of GbE and 10GbE interfaces as well as a choice of form factors, the 5400/8200 zl switches offer excellent flexibility and scalability as well as ease of deployment, operation, and maintenance.

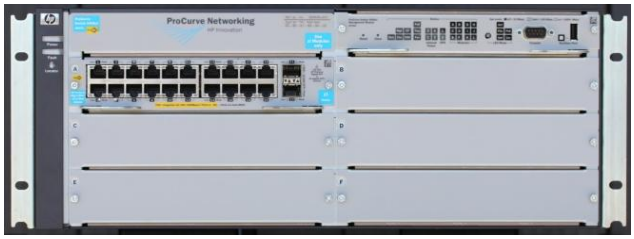

Figure 2 – 5406 zl Switch

Figure 3 – 5412 zl Switch

The 5400 zl switches are targeted as enterprise and midmarket wiring closet switches – designed for low cost with a choice of medium to high port density. The 5400 zl switches offer extensive prioritization features that bring full convergence down to the desktop.

2.1.2 HP 8200 zl Switch Series Cryptographic Modules

The 8200zl switches (Figure 4 and Figure 5) are some of the most advanced Layer 3/Layer 4 switches in the HP Networking product line. The 8200 zl switches incorporate a fully passive backplane and provide modular, redundant switch management and fabric. The 8200 zl Switch Series is available as a 6U (8206 zl) or 9U (8212 zl) rack mountable, modular chassis. The 8206 zl switch provides 6 interface card slots and the 8212 zl switch provides 12 interface card slots. With a wide variety of GbE interfaces, choice of PoE+ and non-PoE ports, and 10 GbE capabilities, the 8200 zl Switch Series offers excellent flexibility and scalability as well as ease of deployment, operation, and maintenance.

.

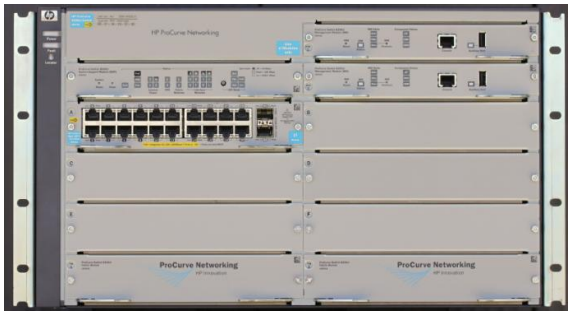

Figure 4 – 8206 zl Switch

Figure 5 – 8212 zl Switch

The 8200 zl switches are deployed as enterprise-class, high-availability, medium-scale core switches with access layer solutions for mission-critical deployments. The switches are ideal for highly converged network access layer solutions where continuity of operations is paramount.

2.1.3 5400/8200 zl Switch Series FIPS Security Levels

The cryptographic modules being evaluated for FIPS 140-2 security requirements are the 5400/8200 zl switches. Table 2 lists the FIPS 140-2 Section levels at which the 5400/8200 zl switches are validated.

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	EMI/EMC[1]	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

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

2.2 Module Specification

The cryptographic modules (5400/8200 zl switches) are hardware modules with multi-chip standalone embodiment. The overall security level of the switches is 2. The physical cryptographic boundary of the 5400/8200 zl switches is defined by the components that make up the exterior of each appliance.

The FIPS validated configuration of the 5406 zl cryptographic module is shown in Figure 2 and consists of the following components:

- Hard metal exterior making up the physical embodiment of each appliance
- (1) HP 5400 zl Management Card
- (1) HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl Card
- (1) HP 1500 W PoE+ zl Power Supply
- (1) HP 5406 zl High Performance Fan Tray
- (5) Metal blank plates for vacant slots
- (1) Metal PSU[2] blank plate for vacant slot

The FIPS validated configuration of the 5412 zl cryptographic module is shown in Figure 3 and consists of the following components:

- Hard metal exterior making up the physical embodiment of each appliance
- (1) HP 5400 zl Management Card
- (1) HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl Card
- (2) HP 1500 W PoE+ zl Power Supply
- (1) HP 5412 zl High Performance Fan Tray
- (11) Metal blank plates for vacant slots
- (2) Metal PSU blank plates for vacant slots

The physical cryptographic boundary of the 5400 zl switches is defined by the red dotted line in Figure 6.

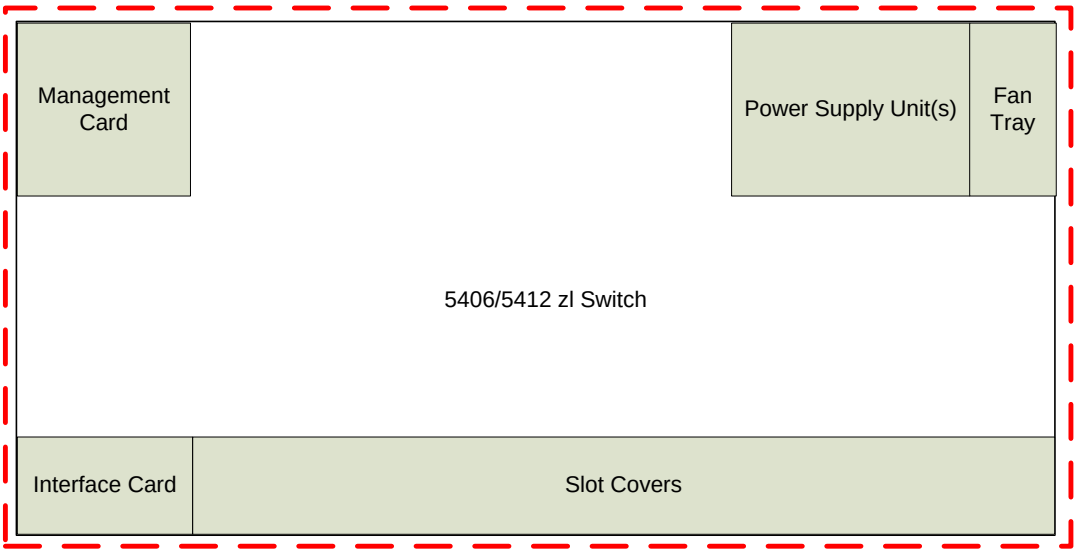

Figure 6 – 5406 zl and 5412 zl Cryptographic Boundary

[2] PSU – Power Supply Unit

.

The FIPS validated configuration of the 8206 zl cryptographic module is shown in Figure 4 and consists of the following components:

- Hard metal exterior making up the physical embodiment of each appliance
- (2) HP 8200 zl Management Cards
- (2) HP 8200 zl Fabric Cards
- (1) HP 8200 zl System Support Card
- (1) HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl Card
- (1) HP 1500 W PoE+ zl Power Supply
- (1) HP 8206 zl High Performance Fan Tray
- (5) Metal blank plates for vacant slots
- (1) Metal PSU blank plate for vacant slot

The FIPS validated configuration of the 8212 zl cryptographic module is shown in Figure 5 and consists of the following components:

- Hard metal exterior making up the physical embodiment of each appliance
- (2) HP 8200 zl Management Cards
- (2) HP 8200 zl Fabric Cards
- (1) HP 8200 zl System Support Card
- (1) HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl Card
- (2) HP 1500 W PoE+ zl Power Supplies
- (1) HP 8212 zl High Performance Fan Tray
- (11) Metal blank plates for vacant slots
- (2) Metal PSU blank plates for vacant slots

The physical cryptographic boundary of the 8200 zl switches is defined by the red dotted line in Figure 7.

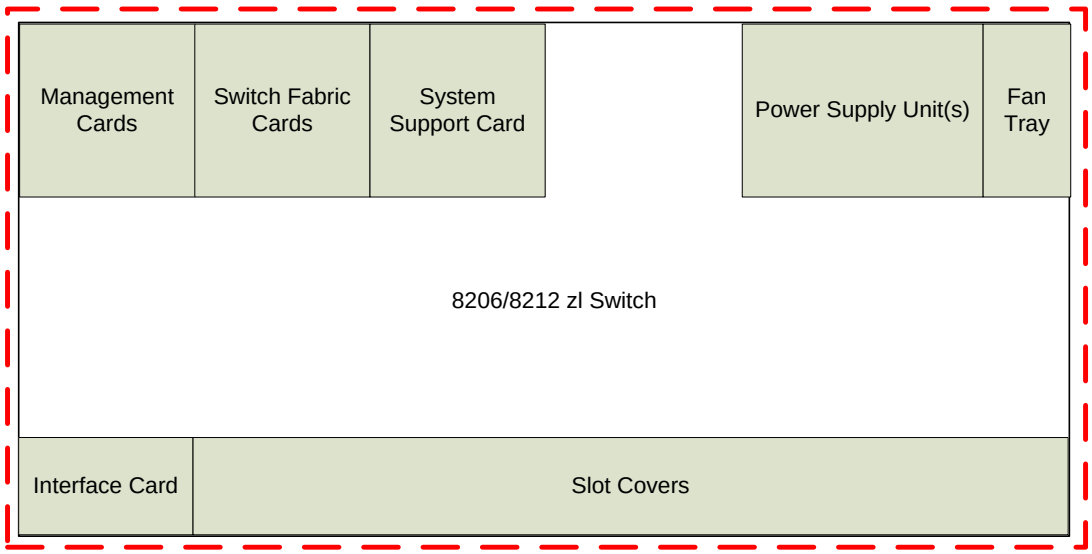

Figure 7 – 8206 zl and 8212 zl Cryptographic Boundary

2.3 Module Interfaces

The 5406 zl, 5412 zl, 8206 zl, and 8212 zl cryptographic modules' physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface
- Power Interface

2.3.1 5400 zl Switch Series Ports and Interfaces

The 5406 zl and 5412 zl include the following logical interface items:

- Management Card
- HP 20-port Gig-T PoE+[3] / 2-port 10-GbE[4] SFP+[5] v2 zl interface card
- Power supplies
- High Performance Fan Tray

The power supplies and fan tray are located at the rear of the appliances. The Management Card consists of a CPU[6], flash memory to hold the firmware image, processor memory for the code execution, status LEDs[7], the cryptographic library, and other support circuitry to interface and control each interface card. The Management Card is the main driver of the 5400 zl switches, which oversees the operation of all zl interface cards. Figure 2 shows the front panel ports and interfaces of the 5406 zl switch.

The mapping of logical and physical interfaces to the FIPS validated configuration of the 5406 zl switch is detailed in Table 3.

Table 3 – Mapping of FIPS 140-2 Logical Interfaces to the 5406 zl Switch

Physical Interfacing Component	FIPS 140-2 Logical Interfaces	5406 zl Switch Port/Interface
(1) Management Card	Data Input	(1) RS-232[8] serial port (DB9)
	Data Output	(1) RS-232 serial port (DB9)
	Control Input	(1) RS-232 serial port (DB9), (1) Push Button
	Status Output	(1) RS-232 serial port (DB9), (32) LEDs
(1) HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl interface card	Data Input	(20) RJ[9]-45 Gig-T PoE+ ports, (2) SFP+ ports
	Data Output	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports
	Control Input	(20) RJ-45 Gig-T PoE+ ports
	Status Output	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports, (44) LED's
	Power Output	(20) RJ-45 Gig-T PoE+ ports

[3] PoE – Power over Ethernet
[4] GbE – Gigabit Ethernet
[5] SFP – Small Form-factor Pluggable
[6] CPU – Central Processing Unit
[7] LED – Light Emitting Diode
[8] RS – Recommended Standard
[9] RJ – Registered Jack

.

Physical Interfacing Component	FIPS 140-2 Logical Interfaces	5406 zl Switch Port/Interface
(1) 1500 W PoE+ (110V/220V) Internal Power Supplies	Power Input	(1) AC[10] Power Interface
	Status Output	(2) LED Indicators
(1) Status Panel	Status Output	(3) LED Indicators
(2) External Power Interfaces	Power Input	(2) PoE Power Connector Interfaces
(1) High performance fan tray	Status Output	(3) LED Indicators

Figure 3 shows the front panel ports and interfaces of the 5412 zl switch.

The mapping of logical and physical interfaces to the FIPS validated configuration of the 5412 zl switch is detailed in Table 4.

Table 4 – Mapping of FIPS 140-2 Logical Interfaces to the 5412 zl Switch

Physical Interfacing Component	FIPS 140-2 Logical Interfaces	5412 zl Switch Port/Interface
(1) Management Card	Data Input	(1) RS-232 serial port (DB9)
	Data Output	(1) RS-232 serial port (DB9)
	Control Input	(1) RS-232 serial port (DB9), (1) Push Button
	Status Output	(1) RS-232 serial port (DB9), (32) LEDs
(1) HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl interface card	Data Input	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports
	Data Output	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports
	Control Input	(20) RJ-45 Gig-T PoE+ ports
	Status Output	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports, (44) LED's
	Power Output	(20) RJ-45 Gig-T PoE+ ports
(2) 1500 W PoE+ (110V/220V) Internal Power Supplies	Power Input	(2) AC Power Interfaces
	Status Output	(4) LED Indicators
(1) Status Panel	Status Output	(3) LED Indicators
(2) External Power Interfaces	Power Input	(2) PoE Power Connector Interfaces
(1) High performance fan tray	Status Output	(3) LED Indicators

[10] AC – Alternating Current

.

2.3.2 8200 zl Switch Series Ports and Interfaces

The 8206 zl and 8212 zl modules include the following logical interface items:

- Management Cards
- HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl interface card
- Fabric Cards
- System Support Card
- Power supplies
- High Performance Fan Tray

The Management Cards of the 8200 zl Switch Series are deployed as redundant cards for enhanced system availability. The cards will automatically synchronize configuration information and firmware images. The switching fabric of the 8200 zl modules is provided by the two Fabric Cards. The System Support Card provides a common area for system status LEDs. The System Support Card also provides a system clock, a multiplexor, and system status LEDs. Figure 4 shows the front panel ports and interfaces for the 8206 zl switch.

The mapping of logical and physical interfaces to the FIPS validated configuration of the 8206 zl switch is detailed in Table 5.

Table 5 – Mapping of FIPS 140-2 Logical Interfaces to the 8206 zl Switch

Physical Interfacing Component	FIPS 140-2 Logical Interfaces	8206 zl Switch Port/Interface
(2) Management Card	Data Input	(2) RS-232 serial port (RJ-45)
	Data Output	(2) RS-232 serial port (RJ-45)
	Control Input	(2) RS-232 serial port (RJ-45)
	Status Output	(2) RS-232 serial port (RJ-45) , (16) LEDs
(1) System Support Card	Control Input	(1) Push button
	Status Out	(29) LEDs
(1) HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl interface card	Data Input	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports
	Data Output	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports
	Control Input	(20) RJ-45 Gig-T PoE+ ports
	Status Output	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports, (44) LED's
	Power Output	(20) RJ-45 Gig-T PoE+ ports
(1) 1500 W PoE+ (110V/220V) Internal Power Supplies	Power Input	(1) AC Power Interfaces
	Status Output	(2) LEDs
(1) Status Panel	Status Output	(3) LED Indicators
(2) External Power Interfaces	Power Input	(2) PoE Power Connector Interfaces
(1) High performance fan tray	Status Output	(3) LEDs

.

Figure 5 shows the front panel view of the base configuration for the 8206 zl switch.

The mapping of logical and physical interfaces to the FIPS validated configuration of the 8212 zl switch is detailed in Table 6.

Table 6 – Mapping of FIPS 140-2 Logical Interfaces to the 8212 zl Switch

Physical Interfacing Component	FIPS 140-2 Logical Interfaces	8212 zl Switch Port/Interface
(2) Management Card	Data Input	(2) RS-232 serial port (RJ-45)
	Data Output	(2) RS-232 serial port (RJ-45)
	Control Input	(2) RS-232 serial port (RJ-45)
	Status Output	(2) RS-232 serial port (RJ-45) , (16) LEDs
(1) System Support Card	Control Input	(1) Push button
	Status Out	(29) LEDs
(1) HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl interface card	Data Input	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports
	Data Output	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports
	Control Input	(20) RJ-45 Gig-T PoE+ ports
	Status Output	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports, (44) LED's
	Power Output	(20) RJ-45 Gig-T PoE+ ports
(2) 1500 W PoE+ (110V/220V) Internal Power Supplies	Power Input	(2) AC Power Interfaces
	Status Output	(4) LED Indicators
(1) Status Panel	Status Output	(3) LED Indicators
(2) External Power Interfaces	Power Input	(2) PoE Power Connector Interfaces
(1) High performance fan tray	Status Output	(3) LED Indicators

2.3.3 zl Interface Cards

The 5400/8200 zl Switch Series modules support a number of different zl-series Interface Cards. The 5406 zl and 8206 zl switches can each support up to 6 zl Interface Cards, while the 5412 zl and 8212 zl switches can each support up to 12 zl Interface Cards. The type and number of interfaces vary on each type of Interface Card. Cryptographic operations are conducted only on the Management Card(s) of the modules. 5400/8200 zl-series Interface Cards do not perform cryptographic functions or use CSP's in their operation.

HP affirms that the 5400/8200 zl Switch Series cryptographic modules will continue to operate at the same level of cryptographic security as the validated configurations when additional Interface Cards listed in Table 7 are introduced. The Cryptographic Officer shall follow the guidance in Section 3.1.3 for Tamper-Evidence Label placement onto the additional Interface Cards in order to maintain the physical security requirements of the modules.

.

Table 7 lists the compatible zl interface cards for the 5400/8200 zl switches along with their associated ports and interfaces.

Table 7 – Mapping of FIPS 140-2 Logical Interfaces to Compatible zl interface cards

Card Name	Supported FIPS 140-2 Logical Interfaces	Interface Card Ports/Interfaces
HP 20-port Gig-T PoE+ / 2-port 10GbE SFP+ v2 zl Card	Data In	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports
	Data Out	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports
	Control In	(20) RJ-45 Gig-T PoE+ ports
	Status Out	(20) RJ-45 Gig-T PoE+ ports, (2) SFP+ ports, (44) LEDs
	Power Out	(20) RJ-45 Gig-T PoE+ ports
HP 24-port Gig-T PoE+ v2 zl Card	Data In	(24) RJ-45 Gig-T PoE+ ports
	Data Out	(24) RJ-45 Gig-T PoE+ ports
	Control In	(24) RJ-45 Gig-T PoE+ ports
	Status Out	(24) RJ-45 Gig-T PoE+ ports, (48) LEDs
	Power Out	(24) RJ-45 Gig-T PoE+ ports
HP 20-port Gig-T PoE+ / 4-port SFP v2 zl Card	Data In	(20) RJ-45 Gig-T PoE+ ports, (4) SFP ports
	Data Out	(20) RJ-45 Gig-T PoE+ ports, (4) SFP ports
	Control In	(20) RJ-45 Gig-T PoE+ ports
	Status Out	(20) RJ-45 Gig-T PoE+ ports, (4) SFP ports, (48) LEDs
	Power Out	(20) RJ-45 Gig-T PoE+ ports
HP 8-port 10GbE SFP+ v2 zl Card	Data In	(8) SFP+ ports
	Data Out	(8) SFP+ ports
	Status Out	(8) SFP+ ports, (16) LEDs
HP 20-port Gig-T / 2-port 10GbE SFP+ v2 zl Card	Data In	(20) RJ-45 Gig-T ports, (2) SFP+ ports
	Data Out	(20) RJ-45 Gig-T ports, (2) SFP+ ports
	Control In	(20) RJ-45 Gig-T ports
	Status Out	(20) RJ-45 Gig-T ports, (2) SFP+ ports, (44) LEDs
HP 24-port SFP v2 zl Card	Data In	(24) SFP ports
	Data Out	(24) SFP ports
	Control In	(24) SFP ports
	Status Out	(24) SFP ports, (48) LEDs

.

HP 8-port 10Gbase-T v2 zl Card	Data In	(8) 10GBase-T ports
	Data Out	(8) 10GBase-T ports
	Control In	(8) 10GBase-T ports
	Status Out	(8) 10GBase-T ports, (16) LEDs
HP 24-port 10/100 PoE+ v2 zl Card	Data In	(24) RJ-45 10/100BaseT PoE+ ports
	Data Out	(24) RJ-45 10/100BaseT PoE+ ports
	Control In	(24) RJ-45 10/100BaseT PoE+ ports
	Status Out	(24) RJ-45 10/100BaseT PoE+ ports, (48) LEDs
	Power Out	(24) RJ-45 10/100BaseT PoE+ ports
HP 24-port Gig-T v2 zl Card	Data In	(24) RJ-45 Gig-T ports
	Data Out	(24) RJ-45 Gig-T ports
	Control In	(24) RJ-45 Gig-T ports
	Status Out	(24) RJ-45 Gig-T ports, (48) LEDs
HP 20-port Gig-T / 4-port SFP v2 zl Card	Data In	(20) RJ-45 Gig-T ports, (4) SFP ports
	Data Out	(20) RJ-45 Gig-T ports, (4) SFP ports
	Control In	(20) RJ-45 Gig-T ports
	Status Out	(20) RJ-45 Gig-T ports, (4) SFP ports, (48) LEDs
HP 12-port Gig-T PoE+ / 12-port SFP v2 zl Card	Data In	(12) RJ-45 Gig-T PoE+ ports, (12) SFP ports
	Data Out	(12) RJ-45 Gig-T PoE+ ports
	Control In	(12) RJ-45 Gig-T PoE+ ports, (12) SFP ports
	Status Out	(12) RJ-45 Gig-T PoE+ ports, (12) SFP ports, (48) LEDs
	Power Out	(12) RJ-45 Gig-T PoE+ ports

2.4 Roles and Services

Each cryptographic module supports two roles (as required by FIPS 140-2) that an operator can assume: a Crypto Officer (Manager) role and a User (Operator) role. Each role is accessed through proper role-based authentication to the switch. Services associated with each role are listed in the following sections.

Please note that the keys and CSPs[11] listed in Table 8 and Table 9 indicate the type of access required using the following notation:

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

[11] CSP – Critical Security Parameter

.

2.4.1 Crypto Officer Role

The Crypto Officer (CO) is responsible for the set up and initialization of the 5400/8200 zl switches as documented in Section 3 (Secure Operation) of this document. The CO has complete control of the switches and is in charge of configuring all of the settings for each switch. The CO can create RSA[12] key pairs for SSH v2[13]. Private keys and CSPs can be viewed by the CO. The CO is also in charge of maintaining access control and checking error and intrusion logs.

Descriptions of the services available to the Crypto Officer role are provided in Table 8 below.

Table 8 – Crypto Officer Services

Service	Description	CSP and Type of Access
Configure Switch	Configuration of CSPs for normal switch operation	Port Access Password – W SNMPv3[14] Authentication/Privacy Passwords – W Global RADIUS[15] Server Shared Secret – W RADIUS Server Host Shared Secret – W TACACS[16] Server Shared Secret – W TACACS Server Host Shared Secret – W 'Key-chain' Key Strings– W SNTP [17] Shared Secret – W VLAN[18] OSPF Shared Secret – W VLAN RIP[19] Shared Secret – W SSH v2 Private/Public Keys – W Encrypt Credentials Encryption Key – W CO Password – W User Password – W ROM[20] Console Password – W
Manage Passwords	Manage CO, User, and BootROM passwords	CO Password – W User Password – W ROM Console Password – W
Initiate Enhanced Secure-Mode (FIPS capable mode)	Reboot the system into a FIPS-Approved mode of operation	All Keys – W
Initiate Standard Secure-Mode (non-FIPS capable mode)	Reboot the system into a non-FIPS Approved mode of operation	All Keys – W
Zeroization	Zeroize all keys and CSPs	All Keys – W
Verify Image Signature	On demand firmware image integrity check	Image Signature – R Image Verification Public Key – X

[12] RSA – Rivest, Shamir, Adleman
[13] SSH – Secure Shell
[14] SNMP – Secure Network Management Protocol
[15] RADIUS – Remote Access Dial-in User Service
[16] TACACS – Terminal Access Controller Access-Control System
[17] SNTP – Simple Network Transfer Protocol
[18] VLAN – Virtual Local Area Network
[19] RIP – Routing Information Protocol
[20] ROM – Read Only Memory

.

Service	Description	CSP and Type of Access
Show CSPs	Display keys and CSPs	Global RADIUS Server Shared Secret – R RADIUS Server Host Shared Secret – R TACACS Server Encryption Key – R TACACS Server Host Shared Secret – R Key-chain Key String – R Router OSPF Shared Secret – R VLAN OSPF Shared Secret – R VLAN RIP Shared Secret – R Port Access Password – R
Establish SSH v2 Connection	Establish a remote SSH v2 session with the switch	CO Password – X SSH v2 Public/Private Key – X SSH v2 Session Key – WRX Diffie-Hellman Public/Private Key – WRX
Reboot/On Demand Self-Tests	Reboot the switch; perform self-tests on demand	None
Show Secure-Mode	Display the current secure mode of the switch	None
Control Chassis LED	Control the "Chassis Locate" LED	None
View Logs	View syslog for system status, warnings, and errors	None

2.4.2 User Role

The User role can verify the firmware image signature on-demand, show the current secure-mode of the switch, view the syslog, and connect to the switch remotely via SSH v2. Descriptions of the services available to the User role are provided in Table 9.

Table 9 – User Services

Service	Description	CSP and Type of Access
Verify Image Signature	On demand firmware image integrity check	Image Signature – R Image Verification Public Key – X
Establish SSH v2 Connection	Establish a remote SSH v2 session with the module	User Password – X SSH v2 Public/Private Key – RX SSH v2 Session Key – WRX Diffie-Hellman Public/Private Key – WRX
Show secure-mode	Display the current secure mode of the module	None
Control Chassis LED	Control the "Chassis Locate" LED	None
View Logs	View syslog for system status, warnings, and errors	None

.

2.4.3 Authentication

The 5400/8200 zl switches support role-based authentication to control access to all services provided by the switches. To perform services on the switches, an operator must log in to the switch by authenticating with the respective role's username and secure password. The CO or User password is only known by those that are associated with that role. The CO and User passwords are initialized by the CO as part of switch initialization, as described in Section 3 (Secure Operation) of this document. Once the operator is authenticated, they will assume their respective role and will be able to carry out the available services listed in Table 8 and Table 9.

2.4.3.1 Authentication Data Protection

The 5400/8200 zl switches do not allow the disclosure, modification, or substitution of authentication data to unauthorized operators. Authentication data can only be modified by the operator who has assumed the CO role.

2.4.3.2 Authentication Mechanism Strength

The 5400/8200 zl switches require a minimum of 8 characters and a maximum of 64 characters for a password. The password may contain any combination of letters, numbers, and special characters (not including 'space') allowing for a total of 94 possible characters. Therefore, there is, at a minimum 94^8 = 6,095,689,385,410,816 possible character combinations. This means there is a 1 in 6,095,689,385,410,816 chance that random access will succeed, surpassing the 1 in 1,000,000 requirements.

The module requires an 8 character password with 94 possible characters per password character; therefore requiring $94^8/100{,}000 = 6.1\text{x}10^{10}$ password attempts in 60 seconds to surpass the 1:100,000 ratio. The processor speed is 666MHz, translating to $1.5\text{x}10^{-9}$ seconds per cycle. Assuming worst case scenario and no overhead, to process ($6.1\text{x}10^{10}$ passwords * 8 bits =) $4.88\text{x}10^{11}$ bits of data, it would take the processor (($4.88\text{x}10^{11}$ bits x $1.5\text{x}10^{-9}$ seconds per cycle)/8 bits per cycle=) 91 seconds to process all $6.1\text{x}10^{10}$ password attempts. Therefore the password strengths meet FIPS 140-2 requirements.

2.5 Physical Security

The 5400/8200 zl Switch Series are multi-chip standalone cryptographic modules. The modules consist of production-grade components that include standard passivation techniques. The chassis, interface card covers, blank plates, power supplies, and fan tray of the 5400/8200 zl switches are made of a hard metal, opaque within the visible spectrum. All ventilation holes present on the modules have either been covered by Tamper-Evidence Labels or an opacity shield, rendering them incapable of disclosing any security-relevant components when inspected. The modules contain removable covers, zl interface cards, power supplies, and fan tray; all of which are protected by Tamper-Evidence Labels.

Correct placement of Tamper-Evidence Labels onto each of the modules is covered in the Section 3 (Secure Operation) of this document.

2.6 Operational Environment

The operational environment running within the 5400/8200 zl switches consists of the Greenhills Integrity Operating System running the latest management firmware (HP K.15.07.0003, K.15.07.0012). The operational environment of the switches is non-modifiable, thus the operational environment requirements do not apply to the 5400/8200 zl switches.

.

2.7 Cryptographic Key Management

The 5400/8200 zl switches implement the FIPS-Approved algorithms listed in Table 10 below.

Table 10 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES[21] ECB[22], CBC[23], CTR[24], CFB[25] Modes: 128-, 192-, and 256-bit keys	1718
Triple-DES[26] CBC: KO[27] 1, 2	1105
HMAC[28]-SHA[29]-1	993
SHA-1, SHA -256 (Firmware Implementation)	1501
SHA-1, SHA-256 (BootROM Implementation)	1600
RSA ANSI[30] X9.31 Key Pair Generation: 1024- to 4096-bit keys	866
RSA PKCS[31] #1 v1.5 Signature Generation and Verification: 1024- to 4096-bit keys (Firmware Implementation)	866
RSA PKCS #1 v1.5 Signature Verification: 1024- to 4096-bit keys (BootROM Implementation)	915
DSA[32] Key Pair Generation: 1024-bit keys	530
DSA Signature Generation/Verification: 1024-bit Keys	530
FIPS 186-2 RNG[33] (Regular) w/ X change notice, K change notice	911
FIPS 186-2 RNG (General Purpose) w/ X change notice	911

Caveat:
Additional information concerning 2-key Triple-DES, 1024- to 1536-bit RSA, 1024-bit DSA and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A.

The 5400/8200 zl switches utilize the following non-Approved algorithms, which are allowed for use in a FIPS-Approved mode of operation:

[21] AES – Advanced Encryption Standard
[22] ECB – Electronic Code Book
[23] CBC – Cipher Block Chaining
[24] CTR – Counter
[25] CFB – Cipher Feedback
[26] DES – Data Encryption Standard
[27] KO – Keying Option
[28] HMAC – (keyed-) Hashed Message Authentication Code
[29] SHA – Secure Hash Algorithm
[30] ANSI – American National Standards Institute
[31] PKCS – Public Key Cryptography Standards
[32] DSA – Digital Signature Algorithm
[33] RNG – Random Number Generator

.

- Diffie-Hellman key agreement (1024- and 2048-bit keys)
  - Key establishment methodology provides 80 or 112 bits of encryption strength
- Message Digest 5 (MD5)
  - Message authentication for use with OSPF, BGP, RADIUS, TACACS, and RIP

.

The 5400/8200 zl switches support the critical security parameters (CSPs) listed below in Table 11.

Table 11 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Port Access Password	Alpha-numeric string	Entered by CO through CLI	Exits in plaintext using CLI command	Non Volatile Flash Memory in plaintext	Password Update; Erase Configuration File*; Zeroize Command; Transition to Standard Secure Mode	Authenticate client device that wishes to access the LAN[34]
SNMPv3 Authentication Password	Alpha-numeric string	Entered by CO through CLI	Never exits the switch	Non Volatile Flash Memory in plaintext	Zeroize Command; Erase Configuration File; Transition to Standard Secure Mode	To ensure message integrity and protection against message replay
SNMPv3 Privacy Password	Alpha-numeric string	Entered by CO through CLI	Never exits the switch	Non Volatile Flash Memory in plaintext	Zeroize Command; Erase Configuration File; Transition to Standard Secure Mode	To ensure packet contents are not disclosed on a network
Global RADIUS Server Shared Secret	Alpha-numeric string	Entered by CO through CLI	Exits in plaintext using CLI command	Non Volatile Flash Memory in plaintext	Zeroize Command; Erase Configuration File; Transition to Standard Secure Mode	A shared secret between switches and RADIUS servers to sign all packets

[34] LAN – Local Area Network

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
RADIUS Server Host Shared Secret	Alpha-numeric string	Entered by CO through CLI	Exits in plaintext using CLI command	Non Volatile Flash Memory in plaintext	Zeroize Command; Erase Configuration File; Transition to Standard Secure Mode	A shared secret between switches and a specific RADIUS server to sign all packets
TACACS Server Encryption Key	Alpha-numeric string	Entered by CO through CLI	Exits in plaintext using CLI command	Non Volatile Flash Memory in plaintext	Zeroize Command; Erase Configuration File; Transition to Standard Secure Mode	A shared secret to remote TACACS server
TACACS Server Host Shared Secret	Alpha-numeric string	Entered by CO through CLI	Exits in plaintext using CLI command	Non Volatile Flash Memory in plaintext	Zeroize Command; Erase Configuration File; Transition to Standard Secure Mode	A shared secret to local TACACS server
Key-chain Key Strings	String of assorted keys	Entered by CO through CLI	Exits in plaintext using CLI command	Non Volatile Flash Memory in plaintext	Zeroize Command; Erase Configuration File; Transition to Standard Secure Mode	Set of keys with a timing mechanism for activating and deactivating individual keys
SNTP Shared Secret	Alpha-numeric string	Entered by CO through CLI	Never exits the switch	Non Volatile Flash Memory in plaintext	Zeroize Command; Erase Configuration File; Transition to Standard Secure Mode	Authentication key for accessing remote SNTP server

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Router OSPF Shared Secret	Alpha-numeric string	Entered by CO through CLI	Exits in plaintext using CLI command	Non Volatile Flash Memory in plaintext	Zeroize Command; Erase Configuration File; Transition to Standard Secure Mode	Exchange routing update information securely
VLAN OSPF Shared Secret	Alpha-numeric string	Entered by CO through CLI	Exits in plaintext using CLI command	Non Volatile Flash Memory in plaintext	Zeroize Command; Erase Configuration File; Transition to Standard Secure Mode	Exchange routing update information securely
VLAN RIP Shared Secret	Alpha-numeric string	Entered by CO through CLI	Exits in plaintext using CLI command	Non Volatile Flash Memory in plaintext	Zeroize Command; Erase Configuration File; Transition to Standard Secure Mode	Exchange routing update information securely
Encrypt Credentials Encryption Key	FIPS 140-2 non-approved encryption key	Entered by CO through CLI	Exits in plaintext using CLI command	Non Volatile Flash Memory in plaintext	Zeroize Command; Transition to Standard Secure Mode	Key used to obfuscate keys stored in the 'config' file
CO Password	Alpha-numeric string	Entered by CO through CLI	Never exits the switch	Non Volatile Flash Memory in plaintext; Non Volatile Flash Memory as SHA-1 hash*	Password update; Zeroize Command; Erase Configuration File*; Transition to Standard Secure Mode	Used for authenticating CO to access appliance locally or over SSH v2

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
User Password	Alpha-numeric string	Entered by CO through CLI	Never exits the switch	Non Volatile Flash Memory in plaintext Non Volatile Flash Memory as SHA-1 hash*	Password update; Zeroize Command; Erase Configuration File*; Transition to Standard Secure Mode	Used for authenticating User to access appliance over SSH v2
ROM Console Password	Alpha-numeric string	Entered by CO through CLI	Never exits the switch	Non Volatile Flash Memory in encrypted form	Password update; Zeroize Command; Transition to Standard Secure Mode	Used for authenticating CO or User to access appliance locally
Image Signature	RSA 2048 signature	Generated external from switch	Exits the switch in encrypted form	Non Volatile Flash Memory	Never	To verify the integrity of the firmware image
BootROM Signature	RSA 2048 signature	Generated external from switch;	Never exits the switch	Non Volatile Flash Memory	Never	To verify the integrity of the BootROM image
Image Verification Public Key	RSA 2048-bit public key	Generated external from switch; Hard coded into code	Never exits the switch	Non Volatile Flash Memory	Never	To verify the integrity of the BootROM and firmware image
FIPS 186-2 Seed	hexidecimal string	Generated internally	Never exits the switch	Volatile Memory, in plaintext	Zeroize Command; Transition to Standard Secure Mode; Switch Shutdown	To calculate SHA-1 string in FIPS 186-2 RNG

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
FIPS 186-2 Seed Key	SHA-1 Digest	Generated Internally	Never exits the switch	Volatile Memory, in plaintext	Zeroize Command; Transition to Standard Secure Mode; Switch Shutdown	To calculate SHA-1 string in FIPS 186-2 RNG
SSH v2 Public Key	RSA 3072-bit Public key	Generated Internally	Exits the switch in plaintext	Non Volatile Flash Memory	Zeroize Command; Transition to Standard Secure Mode	SSH v2 server authentication
SSH v2 Private Key	RSA 3072-bit Private key	Generated internally	Never exits the switch	Non Volatile Flash Memory	Zeroize Command; Transition to Standard Secure Mode	SSH v2 server authentication
SSH v2 Session Key	Shared symmetric key	Generated internally	Never exits the switch	Volatile Memory, in plaintext	Zeroize Command; Terminate session; Switch Shutdown	encrypting/decrypting the data traffic during the SSH v2 session
Diffie-Hellman Key Agreement Private Key	Diffie-Hellman Private Key	Generated internally	Never exits the switch	Volatile Memory, in plaintext	Zeroize Command; Terminate session; Switch Shutdown	Securely exchange information over SSH v2
Diffie-Hellman Key Agreement Public Key	Diffie-Hellman Public Key	Generated internally	Exits the switch in plaintext	Volatile Memory, in plaintext	Zeroize Command; Terminate session; Switch Shutdown	Securely exchange information over SSH v2
BGP Neighbor password	Alpha-numeric key string	Entered by CO through CLI	Exits in plaintext using CLI command	Non Volatile Flash Memory in plaintext	Zeroize Command; Erase Configuration File; Transition to Standard Secure Mode	Exchange routing update information securely

* = The CO has executed the `include-credentials store-in-config` command

2.8 Self-Tests

The 5400/8200 zl Switch Series modules perform cryptographic self-tests during power-up and as needed while performing a Crypto Officer service. The purpose of these self-tests is to verify functionality and correctness of the cryptographic algorithms listed in Table 10. Should any of the power-up self-tests or conditional self-tests fail, the modules will cease operation, inhibiting all data output from the modules. The modules will automatically reboot and perform power-up self-tests. Successful completion of the power-up self-tests will return the module to normal operation.

2.8.1 Power-Up Self-Tests

Power-up self-tests are performed when the 5400/8200 zl switches first power up. There are two instances of power-up self-tests that are performed. The first instance is performed by the BootROM image. The BootROM, used for the selection of a cryptographic firmware image, performs the following self-tests:

- Known Answer Tests (KATs)
  - SHA-1 KAT
  - SHA-256 KAT
  - RSA Pariwise Consistency Test
- BootROM integrity check
- Firmware integrity check (after image has been selected)

The BootROM performs the integrity check on itself to ensure that its image is valid. To perform an integrity check on itself, as well as on images that can be downloaded within, the BootROM needs to first perform RSA signature verification, and then check the SHA-256 hash of the image. If the BootROM integrity check fails, the switch shall be returned to HP. If the firmware integrity check fails, the switch will transition to the BootROM console where a new image with a valid signature can be downloaded.

The second instance of power-up self-tests the 5400/8200 zl switches perform are done once a FIPS Approved image has been loaded by the BootROM and are performed by that image:

- Known Answer Tests (KATs)
  - AES KAT
  - Triple-DES KAT
  - RSA Pairwise Consistency Test
  - DSA Pairwise Consistency Test
  - SHA-1 KAT
  - SHA-256 KAT
  - HMAC SHA-1 KAT
  - FIPS 186-2 Random Number Generator KAT

2.8.2 Conditional Self-Tests

The 5400/8200 zl switches perform the following conditional self-tests:

- Continuous RNG test
- RSA Pairwise Consistency Test
- DSA Pairwise Consistency Test
- Firmware load test

2.9 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

3 Secure Operation

The 5400/8200 zl switches meet Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the modules in FIPS-approved mode of operation. To keep the switches in a FIPS-Approved mode of operation, physical access and control of the modules shall be limited to the Cryptographic Officer. This includes local connections, BootROM access, and power connections. The provided Tamper-Evidence Labels and Opacity Shields shall be installed for the module to operate in a FIPS-Approved mode of operation.

3.1 Initial Appliance Setup

Upon receiving the 5400/8200 zl Switch Series module(s), High Performance Fan Tray, Power Supplies, and associated FIPS security items, the CO shall check that the appliance is not damaged and that all required parts and instructions are included.

The base configuration for the 5406 zl Switch is as follows:

- (1) HP 5406 zl Switch (J8697A) (Included in J9642A)
- (1) HP 5400 zl Management Card (J8726A) (Included in J9642A)
- (1) Rack Mounting Kit (Included in J9642A)
- (5) Blank Plates for vacant slots (5069-8563)
- (1) Metal PSU Blank Plate for vacant slot (5003-0753)
- (1) HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl Card (J9536A)
- (1) HP 1500 W PoE+ zl Power Supply (J9306A)
- (1) Power Cord (Included in J9306A)
- (1) HP 5406 zl High Performance Fan Tray (J9721A)
- (1) HP 5406 zl FIPS Opacity Shield Kit (J9710A)
- (1) HP 16mm x 32mm Tamper-Evidence (120) Labels (J9709A)

The base configuration for the 5412 zl Switch is as follows:

- (1) HP 5412 zl Switch (J8698A) (Included in J9643A)
- (1) HP 5400 zl Management Card (J8726A) (Included in J9643A)
- (1) Rack Mounting Kit (Included in J9643A)
- (11) Blank Plates for vacant slots (5069-8563)
- (2) Metal PSU Blank Plates for vacant slots (5003-0753)
- (1) HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl Card (J9536A)
- (2) HP 1500 W PoE+ zl Power Supply (J9306A)
- (2) Power Cords (Included in J9306A)
- (1) HP 5412 zl High Performance Fan Tray (J9722A)
- (1) HP 5412 zl FIPS Opacity Shield Kit (J9711A)
- (1) HP 16mm x 32mm Tamper-Evidence (120) Labels (J9709A)

The base configuration for the 8206 zl Switch is as follows:

- (1) HP 8206 zl Switch (J9477A) (Included in J9640A)
- (2) HP 8200 zl Management Cards (J9092A) (One Included in J9640A)
- (2) HP 8200 zl Fabric Cards (J9093A) (Included in J9640A)
- (1) HP 8200 zl System Support Card (J9095A) (Included in J9640A)
- (1) Rack Mounting Kit (Included in J9640A)
- (5) Blank Plates for vacant slots (5069-8563)
- (1) Metal PSU Blank Plate for vacant slot (5003-0753)
- (1) HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl Card (J9536A)
- (1) HP 1500 W PoE+ zl Power Supply (J9306A)

.

- (1) Power Cord (Included in J9306A)
- (1) HP 8206 zl High Performance Fan Tray (J9723A)
- (1) HP 8206 zl FIPS Opacity Shield Kit (J9712A)
- (1) HP 16mm x 32mm Tamper-Evidence (120) Labels (J9709A)

The base configuration for the 8212 zl Switch is as follows:

- (1) HP 8212 zl Switch (J9091A) (Included in J9641A)
- (2) HP 8200 zl Management Cards (J9092A) (Included in J9641A)
- (2) HP 8200 zl Fabric Cards (J9093A) (Included in J9641A)
- (1) HP 8200 zl System Support Card (J9095A) (Included in J9641A)
- (1) Rack Mounting Kit (Included in J9641A)
- (11) Blank Plates for vacant slots (5069-8563)
- (2) Metal PSU Blank Plates for vacant slots (5003-0753)
- (1) HP 20-port Gig-T PoE+ / 2-port 10-GbE SFP+ v2 zl Card (J9536A)
- (2) HP 1500 W PoE+ zl Power Supplies (J9306A)
- (2) Power Cords (Included in J9306A)
- (1) HP 8212 zl High Performance Fan Tray (J9724A)
- (1) HP 8212 zl FIPS Opacity Shield Kit (J9713A)
- (1) HP 16mm x 32mm Tamper-Evidence (120) Labels (J9709A)

3.1.1 Installation of High Performance Fan Tray

Use of the FIPS Opacity Shields reduces the thermal performance of the zl Chassis, therefore higher performing fans must be used.

1. With the chassis powered down, remove the standard fan tray that shipped with the chassis and discard.
2. Install the High Performance Fan Tray.

3.1.2 Installation of FIPS Opacity Shields

Each of the 5400/8200 zl switches will require two opacity shields. Installation of opacity shields onto the sides of the 5400/8200 zl switches is required for meeting the physical security requirements set by FIPS PUB 140-2. The steps are outlined as follows:

1. Peel the release liner from the adhesive on Shield Clip A and adhere to the Rack Mount Bracket as shown in Figure 8. Make sure the holes in the Shield Clip are aligned with the holes in the Rack Mount Bracket.

.

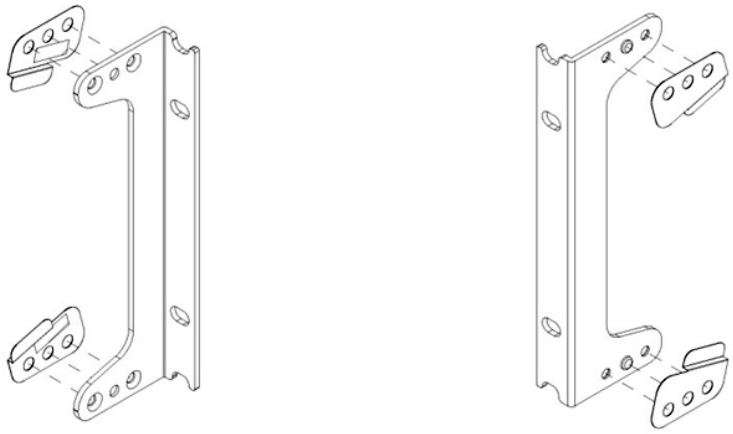

Figure 8 – Shield Clip Placement

2. Repeat for Shield Clip B.

3. Install the Rack Mount Bracket to the chassis in the front position as shown in Figure 9 and secure with four (4) of the included flat head screws.

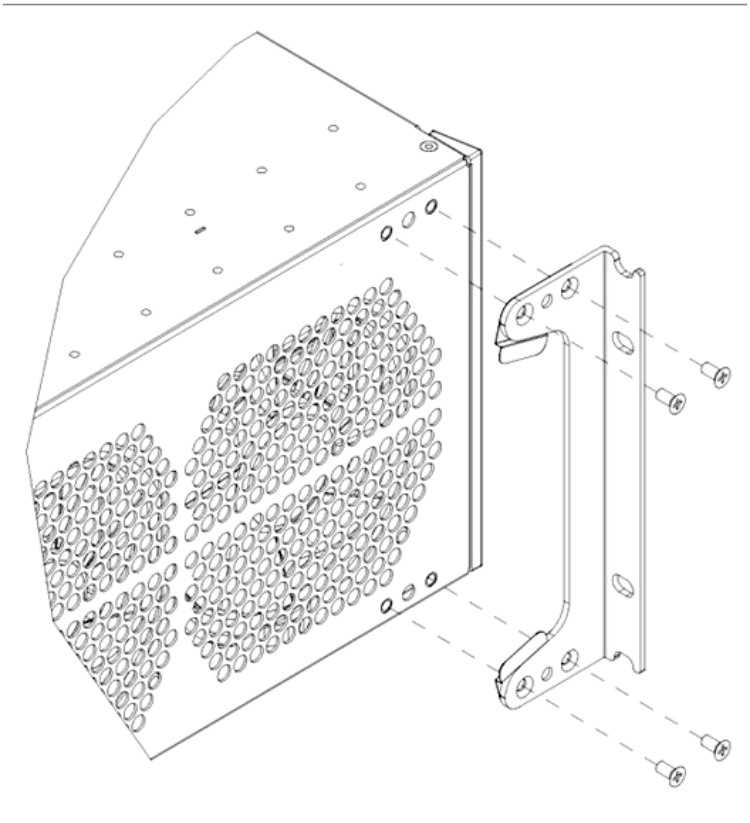

Figure 9 – Rack Mount Bracket Installation

4. Slide the opacity shields completely into the shield clips and secure at the rear with two (2) of the included flat head screws.
5. Repeat for the other side of the chassis.

ATTENTION!: Installation of the Opacity Shields reduces the maximum operating temperature of 5400/8200 zl Chassis to 35°C (95°F).

ATTENTION!: The system must be configured with the 'opacity-shields' configuration command to set proper fan and over temperature behavior.

3.1.3 Tamper-Evidence Label Placement

Placement of Tamper-Evidence Labels is required for meeting the physical security requirements set by FIPS PUB 140-2. HP FIPS Tamper-Evidence Labels are supplied with each module. Please refer to the following list to reference how many total Tamper-Evidence Labels will be used with each module.

- HP 5406 zl Switch: 86 Tamper-Evidence Labels
- HP 5412 zl Switch: 102 Tamper-Evidence Labels
- HP 8206 zl Switch: 92 Tamper-Evidence Labels
- HP 8212 zl Switch: 108 Tamper-Evidence Labels

The HP 5400/8200 zl switches use Tamper-Evidence Labels to protect against unauthorized access through the removable zl interface cards, covers, power supplies, and fan tray. If one of the labels shows evidence of tampering, it is possible the switch has been compromised. It is up to the CO to ensure proper placement of the Tamper-Evidence Labels using the following steps:

- The surface must be dry and free of dirt, oil, and grease, including finger oils. Alcohol pads can be used.
- Slowly peel backing material from label, taking care not to touch the adhesive. Do not use fingers to directly peel label.
- Place the label and apply very firm pressure over the entire label surface to ensure complete adhesion.
- Allow 30 minutes for adhesive to cure. Tamper evidence may not be apparent before this time.

The secure storage and control of unused Tamper-Evidence Labels will be controlled by the CO. The CO is responsible for routinely checking the state of Tamper-Evidence Labels. The CO shall replace any worn Tamper-Evidence Labels following the instructions listed above.

3.1.3.1 5400/8200 zl Management Card Label Placement

Tamper-Evidence Labels need to be placed onto the Management Card(s) of the 5400/8200 zl Switch Series to ensure that they are not removed. For the 5400 zl switches, one Tamper-Evidence Label will be placed between the top of the Management Card and the chassis. A second Tamper-Evidence Label will shall be placed over the USB port on the right-hand side of the Management Card. Lastly, a third Tamper-Evidence label will be placed over the "CLEAR" button on the left-hand side of the Management Card. Correct placement of the Tamper-Evidence Labels onto the 5400 zl Management Card is shown in Figure 10.

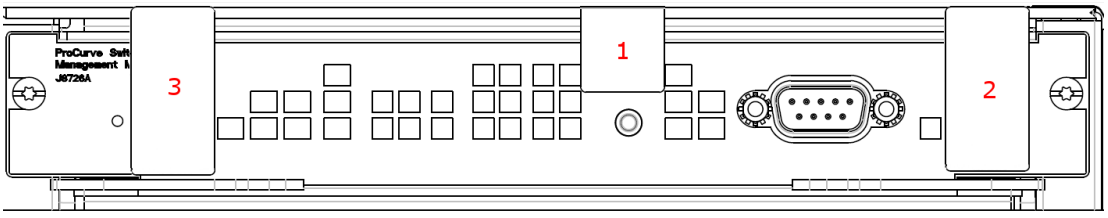

Figure 10 – Tamper-Evidence Label Placement for 5400 zl Management Card

For the 8200 zl switches, one Tamper-Evidence Label will be placed between the top Management Card and the chassis (Label 1). Another label is placed between the bottom Management Card and the top Management Card (Label 2). An additional two Tamper-Evidence Labels will be used to place over the USB ports on both Management Cards (Labels 3 and 4). Correct placement of the Tamper-Evidence Labels onto the 8200 zl Management Cards is shown in Figure 11.

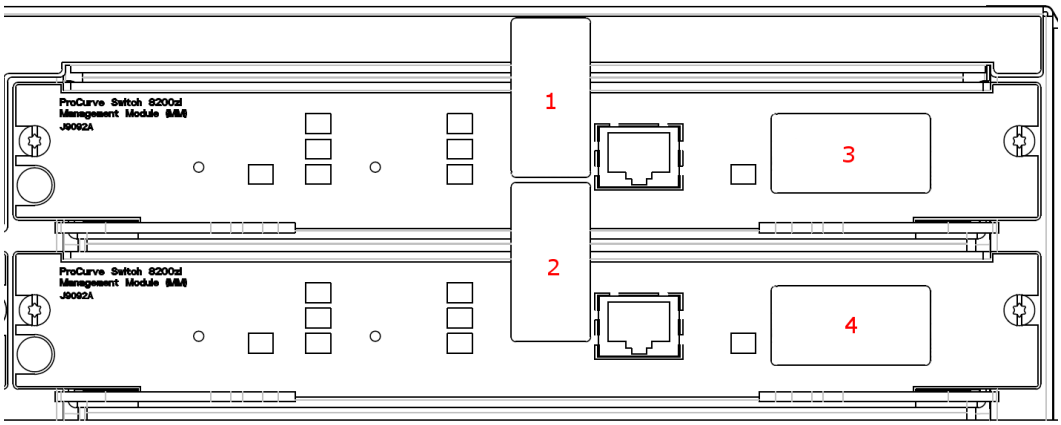

Figure 11 – Tamper-Evidence Label Placement for 8200 zl Management Cards

3.1.3.2 5400/8200 zl Interface Cards and Blank Plates Label Placement

Tamper-Evidence Labels need to be placed between the zl interface module and the adjacent blank plate. For the zl interface card, the Tamper-Evidence Label will be placed between the upper left corner of the card and the chassis. A second label will be placed on the upper right corner between the zl interface card and the adjacent blank plate. One last label will be placed between the upper right corner of the blank plate and the chassis. Ensure that no screw heads are covered by the Tamper-Evidence Labels. Correct placement of the three Tamper-Evidence Labels onto the zl interface cards is shown in Figure 12.

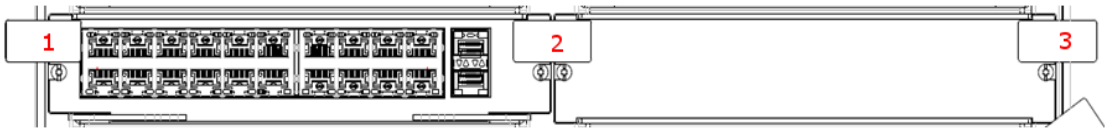

Figure 12 – Tamper-Evidence Label Placement for v2 zl Cards

Tamper-Evidence Labels need to be placed on each of the blank plates to ensure that they are not removed. For each of the blank plates, the Tamper-Evidence Labels will be placed between the blank plate and the chassis as well as between one blank plate and the adjacent blank plate or interface card. Ensure that no screw heads are covered by the Tamper-Evidence Labels. On the 5406 zl and 8206 zl switches, this step will be done twice, for a total of six labels. This step will be done five times on the 5412 zl and 8212 zl switches, requiring a total of 15 labels. The first iteration for all 5400/8200 zl switches and correct placement of the Tamper-Evidence Labels is shown in Figure 13.

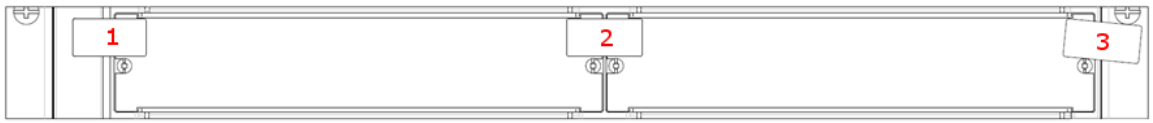

Figure 13 – Tamper-Evidence Label Placement for Blank Plates

.

3.1.3.3 8200 zl System Support Card and Fabric Cards Label Placement

A Tamper-Evidence Label needs to be placed onto the System Support Card of the 8200 zl switches to ensure that it is not removed. One Tamper-Evidence Label will be placed between the System Support Card and the chassis. Correct placement of the Tamper-Evidence Label onto the System Support Card is shown in Figure 14.

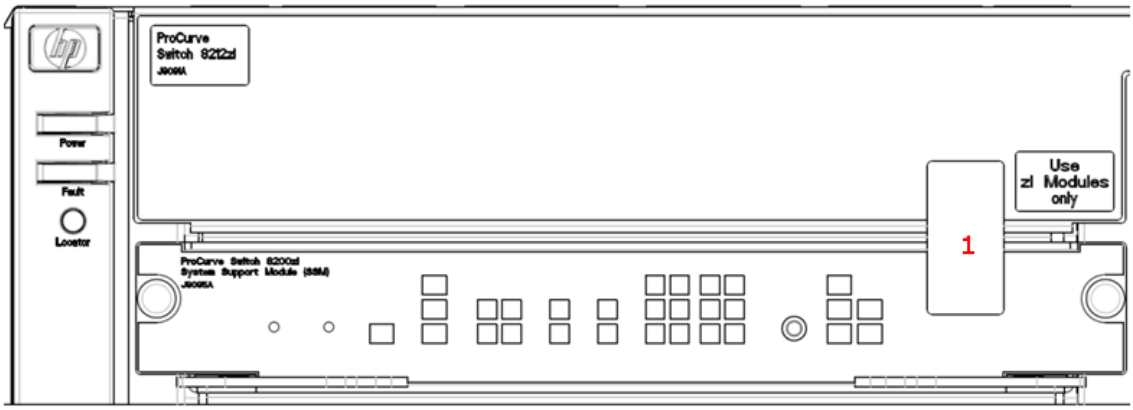

Figure 14 – Tamper-Evidence Label Placement for 8200 zl System Support Card

Two Tamper-Evidence Labels will be needed to ensure that the Fabric Cards are not removed from the 8200 zl switches. For the Fabric Card located on the left-hand side of the chassis, one Tamper-Evidence Label will be placed between the upper left corner of the card and the chassis. For the Fabric Card located on the right-hand side of the chassis, one label will be placed between the upper right corner of the card chassis. Ensure that no screw heads are covered by the Tamper-Evidence Labels. Correct placement of the Tamper-Evidence Labels onto the Fabric Cards is shown in Figure 15.

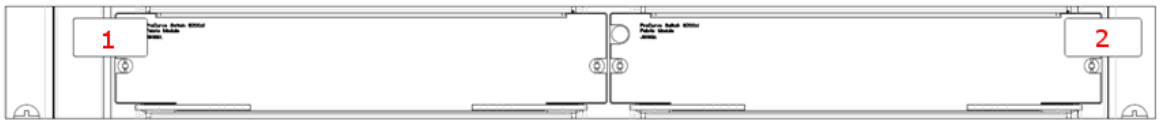

Figure 15 – Tamper-Evidence Label Placement for 8200 zl Fabric Cards

3.1.3.4 5400/8200 zl Top and Bottom Label Placement

There are ventilation holes located on the top and bottom of the 5400/8200 zl switches. These ventilation holes need to be covered with Tamper-Evidence Labels to ensure that nothing within the chassis can be viewed. There are 36 ventilation holes on the top of the chassis and 12 ventilation holes on the bottom of the chassis that need to be covered. Correct placement of the Tamper-Evidence Labels for the top and bottom of the 5400/8200 zl chassis are shown in Figure 16 and Figure 17 respectively. The placement of the unmarked Tamper-Evidence Labels seen on the edges of the chassis is covered in Section 3.1.3.5.

.

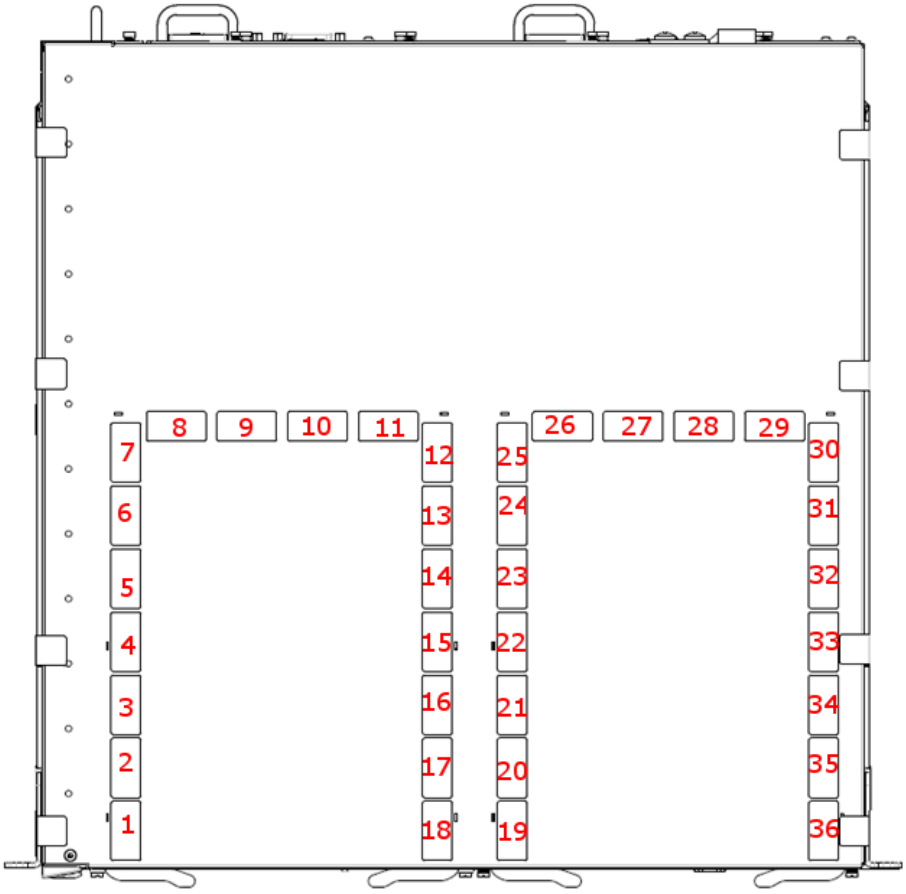

Figure 16 – 5400/8200 zl Top Tamper-Evidence Label Placement

.

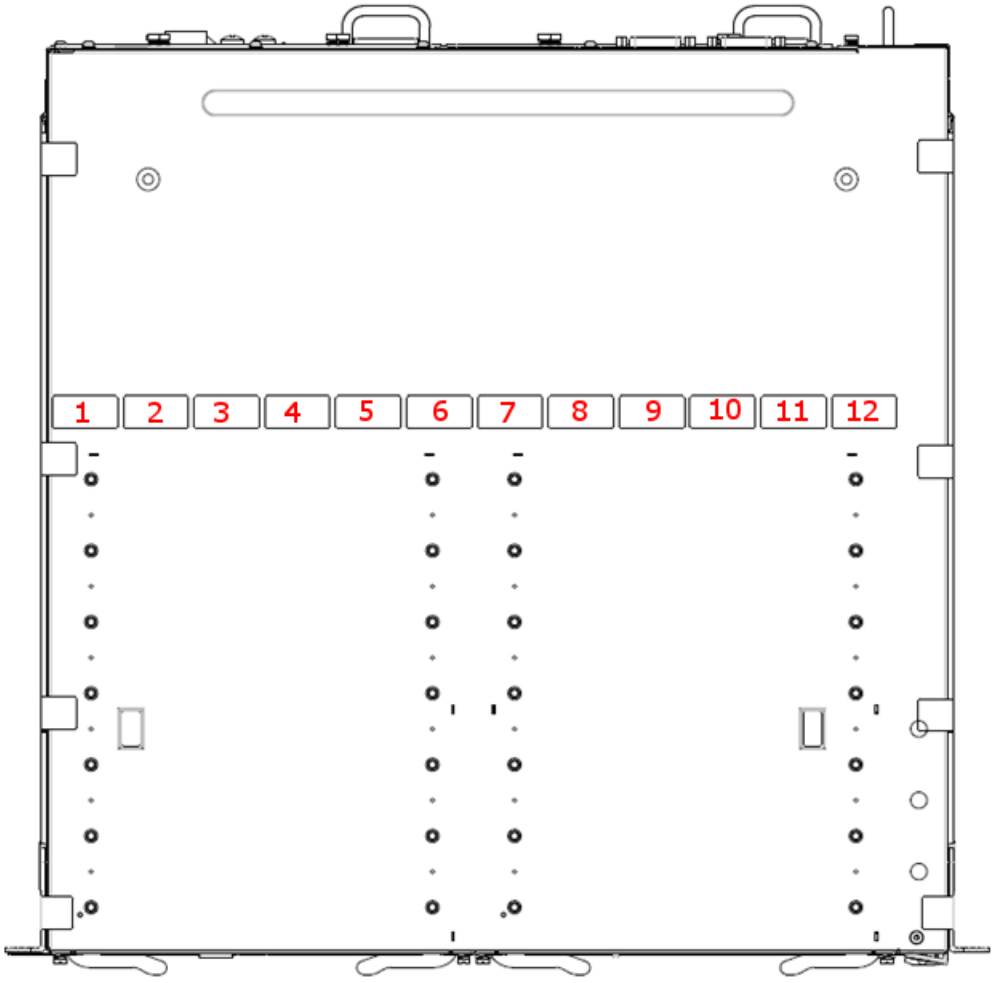

Figure 17 – 5400/8200 zl Bottom Tamper-Evidence Label Placement

3.1.3.5 5400/8200 zl Sides Label Placement

Once the opacity shields have been securely installed onto the 5400/8200 zl Switch Series chassis, Tamper-Evidence Labels must be placed between the shields and the chassis to ensure that they cannot be removed. For the 5406 zl and 8206 zl chassis, two labels will be placed between the opacity shield and the rack mounting bracket. For the 5412 zl and 8212 zl chassis, three labels will be placed in the same location. Two more labels will be placed between the rack mounting bracket and the chassis to ensure the bracket cannot be removed. For all switches, labels will then be placed 3 along the top and 3 along the bottom, wrapping around and fastening to the top or bottom. Finally, labels will be placed along the rear of the opacity shield, securing it against the chassis. In this location, one label will be used for the 5406 zl switch, two labels for the 5412 zl and 8206 zl switch, and three labels for the 8212 zl switch. Repeat these steps for both sides of the module.

The total number of Tamper-Evidence Labels needed for each side of the 5400/8200 zl Switch Series modules is as follows:

- HP 5406 zl Switch: 11 Tamper-Evidence Labels
- HP 5412 zl Switch: 13 Tamper-Evidence Labels
- HP 8206 zl Switch: 12 Tamper-Evidence Labels
- HP 8212 zl Switch: 14 Tamper-Evidence Labels

.

Correct placement of the Tamper-Evidence Labels on one side of the 5406 and 8206 switches is shown in Figure 18 and Figure 19 respectively. The unmarked label located at the rear of the chassis is wrapped around the fan tray. This placement is covered in Section 3.1.3.6.

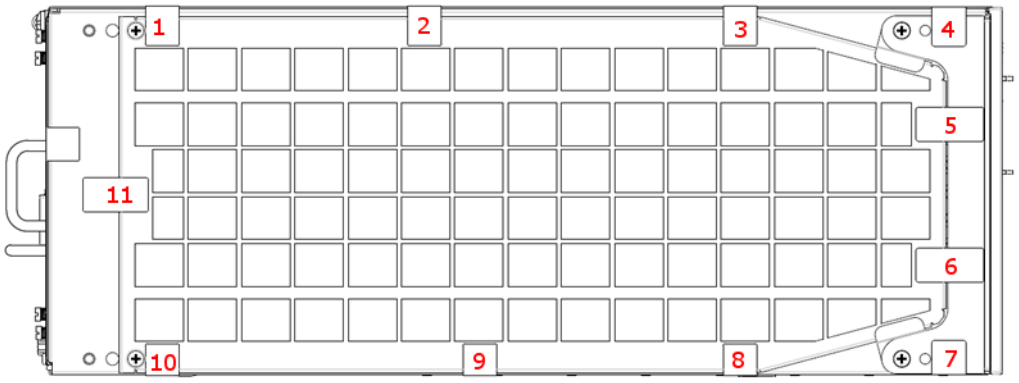

Figure 18 – 5406 Side Tamper-Evidence Label Placement

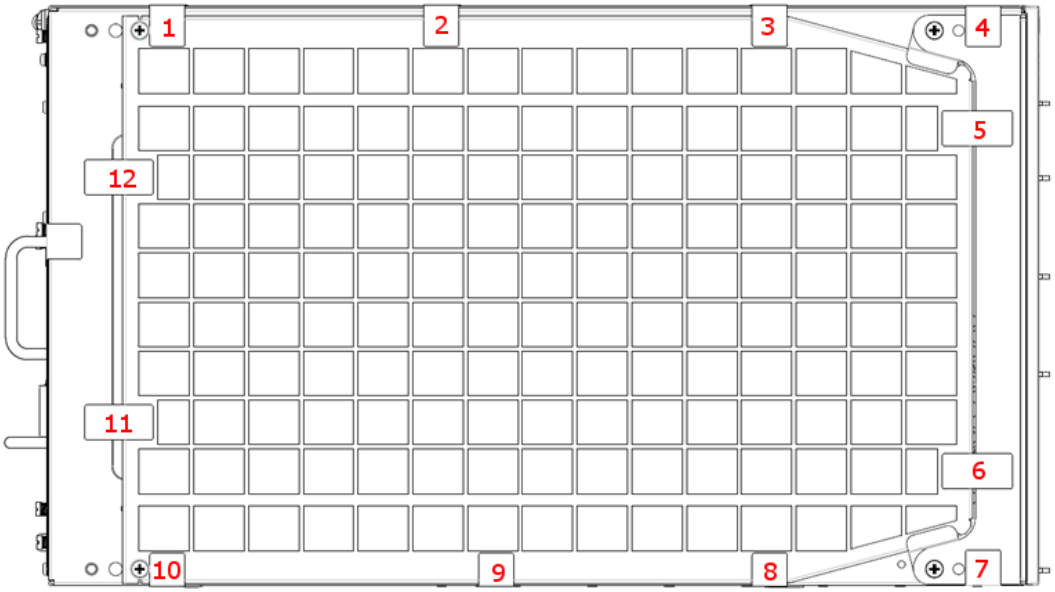

Figure 19 – 8206 Side Tamper-Evidence Label Placement

Correct placement of the Tamper-Evidence Labels on one side of the 5412 and 8212 switches is shown in Figure 20 and Figure 21 respectively. The unmarked label located at the rear of the chassis is wrapped around the fan tray. This placement is covered in Section 3.1.3.6.

.

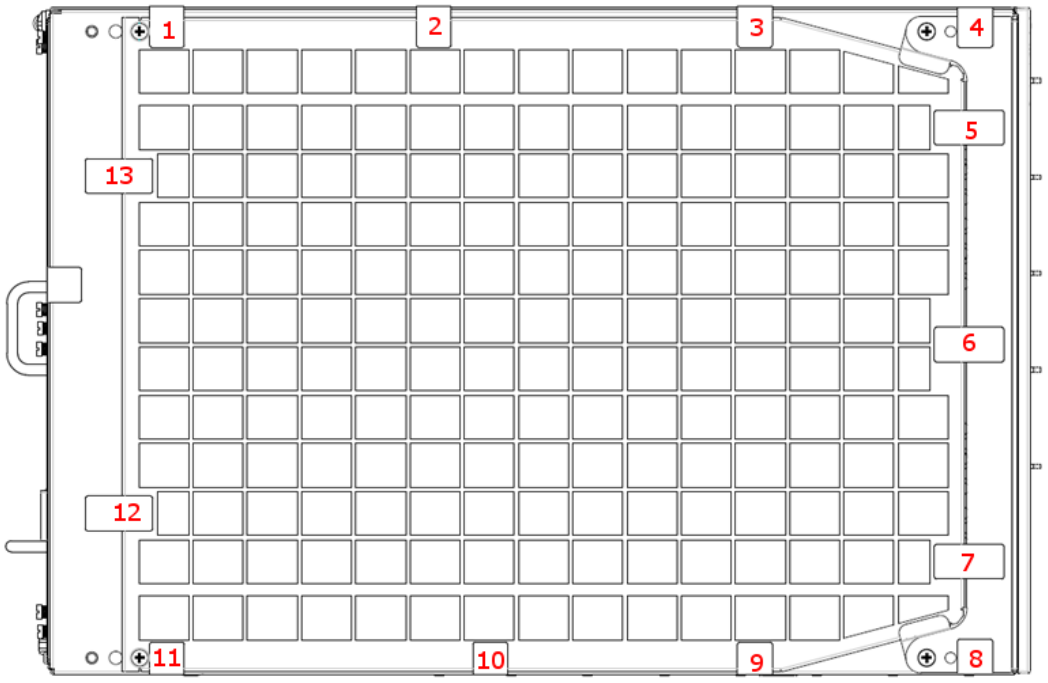

Figure 20 – 5412 Side Tamper-Evidence Label Placement

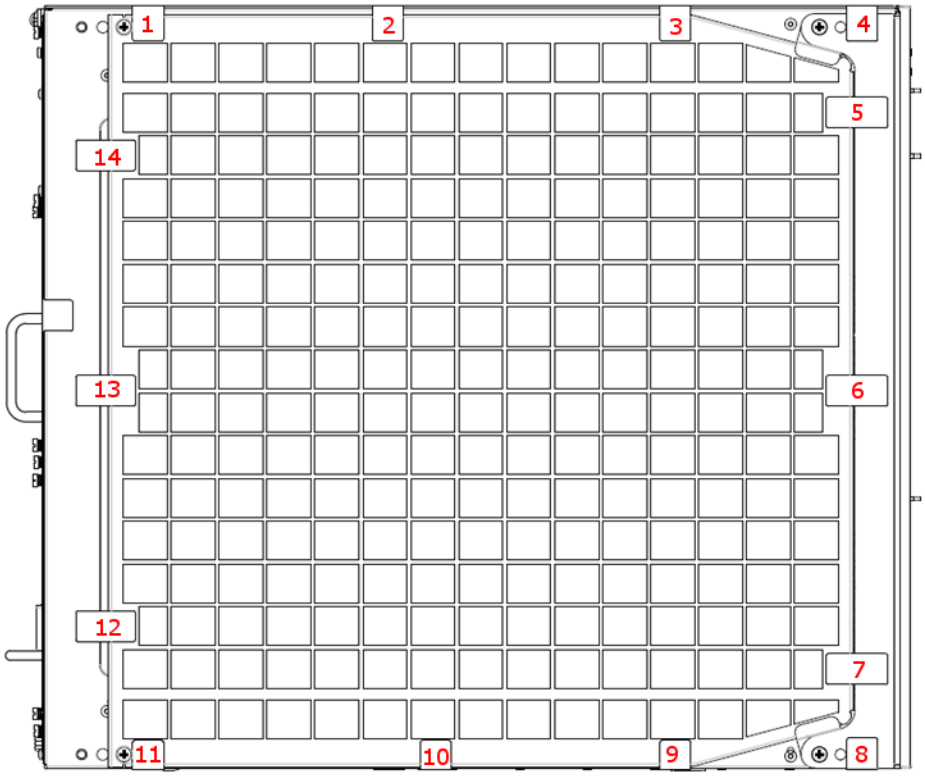

Figure 21 – 8212 Side Tamper-Evidence Label Placement

3.1.3.6 5400/8200 zl Rear Label Placement

Tamper-Evidence Labels are placed on the rear of the 5400/8200 zl Switch Series chassis to secure the removable power supplies and removable fan tray. For the 5406 and 8206 zl appliances, one label will be placed between each power supply and the chassis. A second Tamper-Evidence Label will be placed between the removable fan tray and the chassis; which must be wrapped around the side of the chassis. A third label will be placed between the top of the PSU blank plate and the chassis and a fourth will be placed between the bottom of the PSU blank plate and the chassis. Correct placement of the Tamper-Evidence Labels onto the power supplies or PSU blank plate of the 5406 zl or 8206 zl switch is shown in Figure 22 and Figure 23 respectively.

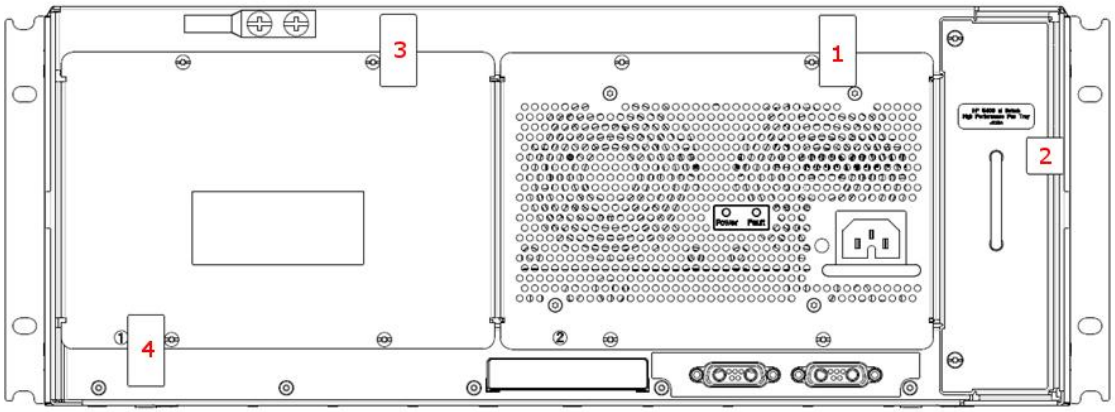

Figure 22 – 5406zl Rear Tamper-Evidence Label Placement

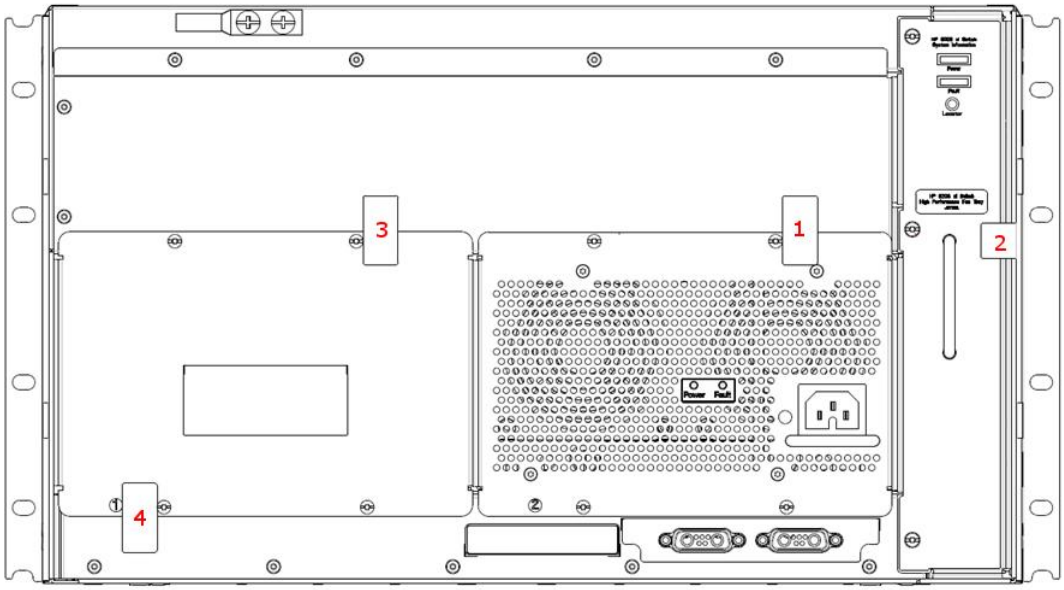

Figure 23 – 8206 zl Rear Tamper-Evidence Label Placement

The rear of the 5412 zl and 8212 zl switches require seven total Tamper-Evidence Labels. Two Tamper-Evidence Labels will be placed between each power supply and the chassis. For the power supply located on the bottom right of the chassis, one Tamper-Evidence Label will be placed between the top right corner of the power supply and the chassis. For the power supply located on the bottom left of the chassis, one

.

Tamper-Evidence Label will be placed between the bottom left corner of the power supply and the chassis. The PSU blank plates require two labels each; one Tamper-Evidence Label placed between the top of the cover and the chassis and one between the bottom of the cover and the chassis. One Tamper-Evidence Label will be placed between the removable fan tray and the chassis, wrapped around the side of the chassis. Correct placement of the Tamper-Evidence Labels onto the power supplies or PSU blank plates of the 5412 zl or 8212 zl switch is shown in Figure 24 and Figure 25 respectively.

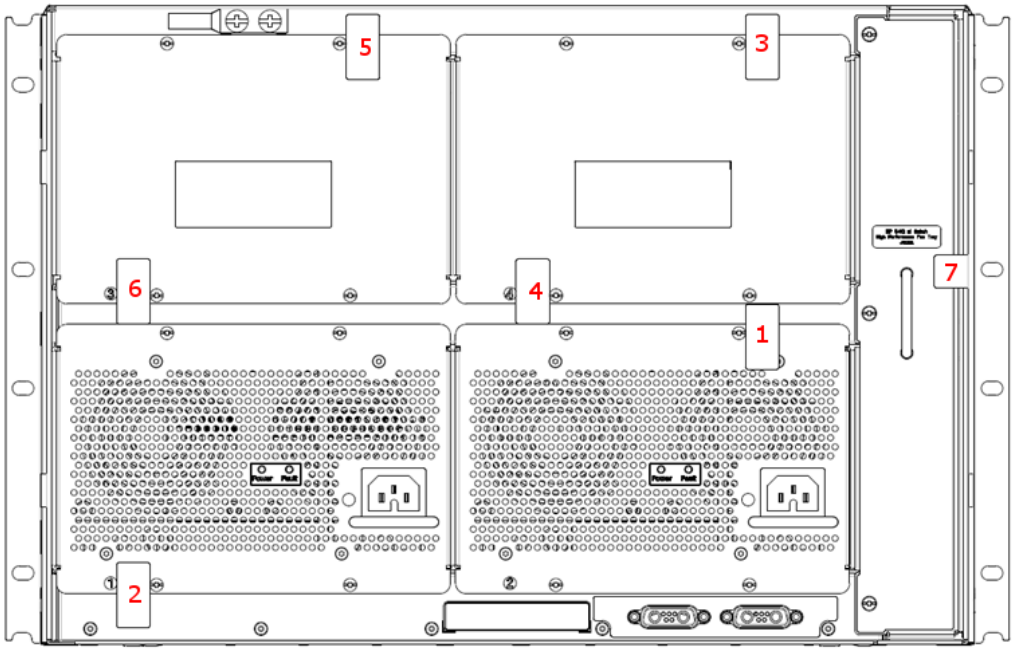

Figure 24 – 5412 zl Rear Tamper-Evidence Label Placement

.

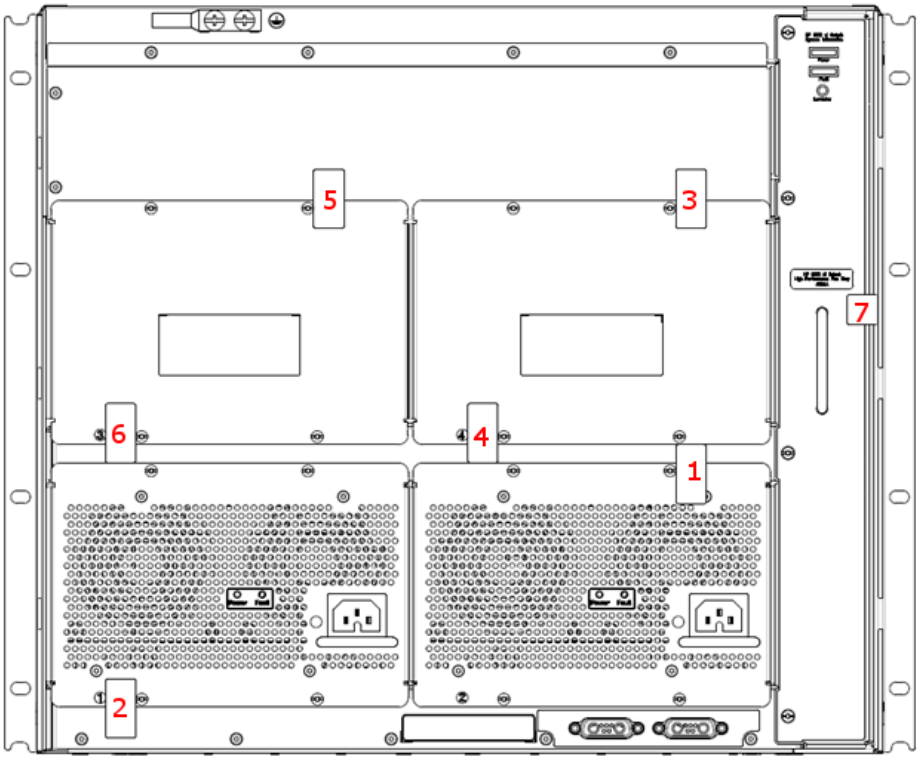

Figure 25 – 8212 zl Rear Tamper-Evidence Label Placement

3.2 Initialization of FIPS Mode

The 5400/8200 zl switches are capable of two different modes of operation. Standard Secure-Mode is the non-FIPS Approved mode of operation for the switches. The FIPS-Approved mode of operation for the switches is referred to as Enhanced Secure-Mode. In this mode of operation, services such as Telnet, TFTP[35], HTTP[36], and SNMPv2 have to be disabled. Auxiliary ports and buttons capable of manual reset and password clearing need to be disabled on the front panel of the modules. Other services in the modules need to be enabled, such as SSH v2, SFTP and SNMPv3. The following initialization steps in this policy must be followed to ensure that the 5400/8200 zl switches are running in a FIPS-Approved mode of operation.

For more information on switch software commands related to Secure Mode, see the chapter titled "Secure Mode (5400zl and 8200zl Switches)" in version K.15.07 or later in the Access Security Guide for your switch.

Note: The FIPS set-up instructions here-in are to be executed from the local serial port of the switch.

Note: The examples show a "`HP-E8212zl#`" prompt. Prompts will differ based on the specific switch model number.

[35] TFTP – Trivial File Transfer Protocol
[36] HTTP – Hypertext Transfer Protocol

3.2.1 Pre-Initialization

Prior to enabling the switch for a FIPS-Approved mode of operation, the CO must download the latest FIPS-Approved firmware image from HP and load it onto the switch. In the following example, the FIPS firmware image is downloaded as the primary flash image using this command structure: `Copy tftp flash <tftp server> <FIPS image>`

```
HP-E8212zl# copy tftp flash 192.168.1.1 K_15_07_0002.swi
```

Once the image has been downloaded, the CO must reboot the switch (still in Standard Secure-Mode) with the newly loaded FIPS-Approved firmware image.

```
HP-E8212zl# boot system flash primary
```

The switch will reboot to the primary flash image. Once presented with the CLI, the CO must download the FIPS-Approved image a second time. This is a mandatory measure to ensure that a FIPS-Approved image is being downloaded appropriately. Again, the FIPS firmware image will be downloaded as the primary flash image:

```
HP-E8212zl# copy tftp flash 192.168.1.1 K_15_07_0002.swi
```

After completing the download, the CO will set the configuration file of the switch to its default settings. This will erase custom keys and other custom configuration settings.

```
HP-E8212zl# erase startup-config
```

After the startup configuration file has been set to its default settings, the CO will enter the 'configuration' context and reboot the switch into a FIPS-ready mode of operation. This means that only FIPS-Approved algorithms and operations are used. Authentication, CSPs, and other services still need to be set up to bring the switch to a FIPS-Approved mode of operation.

```
HP-E8212zl# configure
HP-E8212zl(config)# secure-mode enhanced
```

Before transitioning to Enhanced Secure-Mode, the CO will be asked to confirm whether or not they would like to zeroize the switch, erasing all Management Card files except for the firmware image. Zeroization is required when bringing the switch out of or into a FIPS-Approved mode of operation. This is required so that private keys and CSPs established in one mode of operation cannot be used in another. Zeroization can take up to an hour to complete.

```
The system will be rebooted and all Management Module files except
software images will be erased and zeroized.  This will take up to
60 minutes and the switch will not be usable during that time.
Continue (y/n)?
```

After the CO confirms the above message, the switch will reboot directly into the last loaded firmware image (the FIPS firmware image), run cryptographic self-tests, and do complete zeroization of the switch. Once completed, the switch is ready to be configured to run in a FIPS-Approved mode of operation.

```
ATTENTION: Zeroization has started and will take up to 60 minutes.
           Interrupting this process may cause the switch
           to become unusable.

Backing up firmware images and other system files...
Zeroizing the file system...  100%
Verifying cleanness of the file system...  100%
```

```
Restoring firmware images and other system files...
Zeroization of the file system completed.
Continue initializing..initialization done.
```

3.2.2 Initialization and Configuration

The steps outlined in this section will require the Cryptographic Officer to enter the 'configuration' context in order to execute the commands necessary for initializing the 5400/8200 zl Switch Series modules.

```
HP-E8212zl# configure
```

E8200 zl Switches Only The CO must set the redundancy mode of the two Management Cards to "Nonstop-Switching". This will set the inactive Management Card to "Standby Mode" and will start synchronizing the stored images and all subsequent configuration steps with the currently operating Management Card (Active Management Card). If the Active Management Card fails, the Standby Management Card will be able to take over operation of the switch, eliminating the need to reboot the switch. The 5400 zl switches contain only one Management Card, therefore this operation is unavailable to them.

```
HP-E8212zl(config)# redundancy management-switch nonstop-switching
```

The CO must create passwords for himself or herself, the User, and for the BootROM console in order to meet the security requirements laid out by FIPS PUB 140-2. All other commands for password management not used in this document are prohibited in the FIPS-Approved mode of operation. Password set-up must follow the authentication strength requirements set forth in section 2.4.3.2 (Authentication Mechanism Strength) of this document. A password for the BootROM console is necessary to ensure that only an authorized operator is able to access the BootROM console services. The CO shall be the only one with knowledge of the BootROM password.

```
HP-E8212zl(config)# password operator
New password for operator: ******
Please retype new password for operator: ******

HP-E8212zl(config)# password manager
New password for manager: *******
Please retype new password for manager: *******

HP-E8212zl(config)# password rom-console
Enter password:  *******
Re-enter password:  *******
```

Following password initialization, the CO will disable Telnet services.

```
HP-E8212zl(config)# no telnet-server
```

SSH v2 services will be turned on to allow the User and CO to access the switch's CLI services remotely. To do this, the CO must first generate a new RSA key pair to be used for secure key and message transportation though the SSH v2 connection.

```
HP-E8212zl(config)# crypto key generate ssh rsa bits 3072
Installing new key pair.  If the key/entropy cache is
depleted, this could take up to a minute.
```

The follow command enables the SSH v2 server:

```
HP-E8212zl(config)# ip ssh
```

SFTP/SCP services must be enabled in order to download new firmware images and security updates from HP Networking. It may also be necessary to access an SFTP server to save a copy of the configuration file or device log to an external storage device securely. Enabling SFTP will disable the TFTP service.

```
HP-E8212zl(config)# ip ssh filetransfer
Tftp and auto-tftp have been disabled.
```

As an added security measure, the CO will type the following commands to ensure the switch does not have access to the TFTP client and server services:

```
HP-E8212zl(config)# no tftp client
HP-E8212zl(config)# no tftp server
```

In order to disable SNMPv1 and SNMPv2, the CO must first initialize SNMPv3. Set-up of SNMPv3 requires that an initial user be created with an associated MD5 authentication hash. After creating the 'initial' user, the CO will type in an authentication password and associated privacy password for the 'initial' user:

```
HP-E8212zl(config)# snmpv3 enable
SNMPv3 Initialization process.
Creating user 'initial'
Authentication Protocol: MD5
Enter authentication password: *******
Privacy protocol is DES
Enter privacy password: *******
```

Following the creation of the 'initial' user, the CO will be asked if they would like to create a second user that uses SHA-1 for authentication. The CO will type 'y' then press the "Enter" or "Return" key in order to create the second user.

```
User 'initial' has been created
Would you like to create a user that uses SHA? [y/n] y

Enter user name: crypto_officer
Authentication Protocol: SHA
Enter authentication password: **************
Privacy protocol is DES
Enter privacy password: **************
```

Once the FIPS-Approved user has been created with their associated authentication and privacy passwords, the CO will limit access to SNMPv1 and SNMPv2c messages to 'read only'. This does not disable SNMPv1 and SNMPv2.

```
User creation is done.  SNMPv3 is now functional.
Would you like to restrict SNMPv1 and SNMPv2c messages to have
read only access (you can set this later by the command 'snmp
restrict-access')? [y/n] y
```

The privacy protocol for the SNMPv3 "crypto_officer" user must be changed from DES to AES-128. Use the following command to manually change the privacy protocol for the "crypto_officer" user. Substitute the "*" with a secure password.

```
HP-E8212zl(config)#  snmpv3  user  crypto_officer  auth  sha  ******
                     priv aes ******
```

The following commands will be typed by the CO in order to delete the unapproved SNMPv3 user ('initial') and to disable use of SNMPv1 and SNMPv2.

```
HP-E8212zl(config)# no snmpv3 user initial

HP-E8212zl(config)# no snmp-server enable

HP-E8212zl(config)# snmpv3 only
```

Plaintext connections to the switch are not allowed in a FIPS-Approved mode of operation and must be disabled with the following command:

```
HP-E8212zl(config)# no web-management plaintext
```

HTTPS[37] access to the module must be disabled. The CO can use the following command to disable SSL[38] v3.1/TLS[39] 1.0 web management services.

```
HP-E8212zl(config)# no web-management ssl
```

To prevent unintentional factory reset of the switch, the "Reset" button located on the Management Card of the 5400 zl switches and on the System Support Module of the 8200 zl switches must be disabled. The CO must confirm the prompt with a 'y' to complete the command.

```
HP-E8212zl(config)# no front-panel-security factory-reset
                        **** CAUTION ****
Disabling the factory reset option prevents switch configuation
and passwords from being easily reset or recovered.  Ensure that
you are familiar with the front panel security options before
proceeding.

Continue with disabling the factory reset option[y/n]? y
```

To prevent unintentional password reset of the switch, the "Clear" button located on the Management Card of the 5400 zl switches and on the System Support Module of the 8200 zl switches must be disabled. The CO must confirm the prompt with a 'y' to complete the command.

```
HP-E8212zl(config)# no front-panel-security password-clear
                        **** CAUTION ****
Disabling the clear button prevents switch passwords from being
easily reset or recovered.  Ensure that you are familiar with the
front panel security options before proceeding.

Continue with disabling the clear button [y/n]? y
```

The auxiliary port located on the Management Card must be disabled avoid any unauthorized modifications to the module and its operational environment. Please note: The autorun feature will not function when the USB port is disabled.

```
HP-E8212zl(config)# no usb-port
```

The switch must be configured to set proper fan and over-temperature behavior while FIPS Opacity Shields are installed onto the chassis. The following command will adjust the fan speed and "over temperature" behavior:

[37] HTTPS – Secure Hypertext Transfer Protocol
[38] SSL – Secure Socket Layer
[39] TLS – Transport Layer Security

```
HP-E8212zl(config)# opacity-shields
```

The start-up configuration file needs to be written with the new settings that have been applied in this section. The following command will write the new start-up configuration file:

```
HP-E8212zl(config)# write memory
```

The last steps to ensure that the switch is running in a FIPS-Approved mode of operation is to set the default boot image to the primary image and then reboot the switch into the newly configured FIPS-Approved firmware image.

```
HP-E8212zl(config)# boot set default primary

HP-E8212zl(config)# boot system flash primary
```

3.2.3 Zeroization

Zeroization is required when bringing the switch out of or into a FIPS-Approved mode of operation. This is required so that private keys and CSPs established in one mode of operation cannot be used in another. The 5400/8200 zl switches will execute full system zeroization when the switch is changing secure-mode states. For example, this can be done by calling `secure-mode enhanced` while the switch is in a "secure-mode standard" state. The module will not execute zeroization if calling `secure-mode enhanced` while the switch is currently in the "secure-mode enhanced" state.

Zeroization can also be done by executing the `erase all zeroize` command. This command has the same effect as the above commands; however the switch will not transition to the opposite mode from which the command was called in. These commands shall only be called when accessing the switch directly through a serial connection. Otherwise status information about the zeroization process will not be displayed nor will the operator be able to access the module remotely until remote access has been set up. The only things that will remain on the switch after zeroization has completed are the BootROM image and the firmware images.

3.3 Secure Management

Once the 5400/8200 zl switches have been configured for a FIPS-Approved mode of operation, the Crypto Officer will be responsible for keeping track of and regenerating RSA key pairs for SSH v2 authentication to the switches. Remote management is available via SSH v2. The CO is the only operator that can change configuration settings of the switch, which includes access control, password management, and port security. Physical access to and local control of the 5400/8200 zl switches shall be limited to the Cryptographic Officer.

3.4 User Guidance

The user is only able to access the 5400/8200 zl switches remotely via SSH v2. When accessing the switches remotely via SSH v2, the User will be presented with the same CLI interface as if connected locally. In an SSH v2 session, the user is able to see most of the health information and configuration settings of the switches, but is unable to change them.

3.5 BootROM Guidance

The primary purpose of the BootROM console is to download a new firmware image should there be a problem booting the current FIPS-Approved image. The BootROM may be accessed when rebooting the 5400/8200 zl switches locally through the serial port. When entering into the BootROM, the BootROM

selection menu will present the CO with three options. Option *0* allows the CO to access BootROM console services. Option *1* and Option *2* allow the CO to boot the system into either the primary or secondary firmware image, respectively. Only a FIPS approved firmware image may be selected from the menu. If nothing is pressed within 3 seconds of being presented with the selection menu, the switch will boot into the last booted image.

When accessing the BootROM console from the BootROM selection menu, the CO will be prompted for the BootROM password which was previously configured by the CO during switch initialization. This password shall be different than the CO password. A limited set of commands is available to the Crypto Officer within the BootROM console that allows the CO to download a new image, reboot the switch, zeroize the switch, or display BootROM image versioning information. The BootROM console may be exited at any time, to access the image selection menu, via the `quit` command.

3.6 Product Documentation

For more information on switch software commands related to Secure Mode, see the chapter titled "Secure Mode (5400zl and 8200zl Switches)" in version K.15.07 or later in the Access Security Guide for your switch.

.

4 Acronyms

Table 12 describes the acronyms used throughout this document.

Table 12 – Acronyms

Acronym	Definition
AC	Alternating Current
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CFB	Cipher Feedback Chaining
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CTR	Counter
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GbE	Gigabit Ethernet
HMAC	(keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
KAT	Known Answer Test
KO	Keying Option
LAN	Local Area Network
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OSPF	Open Shortest Path First
PKCS	Public Key Cryptography Standard

.

Acronym	Definition
PoE	Power over Ethernet
PSU	Power Supply Unit
RADIUS	Remote Access Dial-In User Service
RIP	Routing Information Protocol
RJ	Registered Jack
RNG	Random Number Generator
ROM	Read Only Memory
RS	Recommended Standard
RSA	Rivest Shamir and Adleman
SFP	Small Form-factor Pluggable
SHA	Secure Hash Algorithm
SNMP	Secure Network Management Protocol
SNTP	Simple Network Transfer Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TACACS	Terminal Access Controller Access-Control System
TLS	Transport Layer Security
TFTP	Trivial File Transfer Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol

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