



HP MSR30/50 Routers with Encryption Accelerator Modules

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation

Version 1.01

March 2012

Table of Contents

| | |
|---------------------------------------------------------------------------|-----------|
| 1 Introduction | 6 |
| 2 Overview | 6 |
| 2.1 HP MSR30 Router Series..... | 6 |
| 2.2 HP MSR50 Router Series..... | 8 |
| 3 Security Appliance Validation Level | 9 |
| 4 Physical Characteristics and Security Appliance Interfaces | 10 |
| 4.1 HP MSR30 Router Series Interfaces | 10 |
| 4.2 HP MSR50 Router Series Interfaces | 13 |
| 4.3 Physical Interfaces Mapping..... | 14 |
| 5 Roles, Services, and Authentication | 15 |
| 5.1 Roles | 15 |
| 5.2 Services | 15 |
| 5.3 Authentication Mechanisms..... | 18 |
| 6 Approved Cryptographic Algorithms | 20 |
| 7 Non-approved Cryptographic Algorithms | 20 |
| 8 Cryptographic Key Management | 20 |
| 8.1 Access Control Policy..... | 23 |
| 9 Self-Tests | 25 |
| 9.1 Power-On Self-Tests | 25 |
| 9.2 Conditional Self-Tests | 26 |
| 10 Delivery and Operation | 26 |
| 10.1 Secure Delivery | 26 |
| 10.2 Secure Operation | 27 |
| 11 Physical Security Mechanism | 28 |
| 12 Mitigation of Other Attacks | 29 |
| 13 Documentation References | 29 |
| 13.1 Obtaining documentation..... | 29 |
| 13.2 Technical support | 29 |

FIPS 140-2 Non-Proprietary Security Policy for the HP MSR30/50 Routers

Keywords: Security Policy, CSP, Roles, Service, Cryptographic Module

List of abbreviations:

| Abbreviation | Full spelling |
|--------------|-----------------------------------------------|
| AAA | Authentication, Authorization, and Accounting |
| AES | Advanced Encryption Standard |
| BRI | Basic Rate Interface |
| CE1 | Channelized E1 |
| CE3 | Channelized E3 |
| CF | Compact Flash |
| CLI | Command Line Interface |
| CMVP | Cryptographic Module Validation Program |
| CPOS | Channelized Packet Over SONET/SDH |
| CSP | Critical Security Parameter |
| CT1 | Channelized T1 |
| DES | Data Encryption Standard |
| DOA | Dead on arrival |
| FCoE | Fibre Channel over Ethernet |
| FE1 | Fractional E1 |
| FIC | Flexible Interface Card |
| FIP | Flexible Interface Platform |
| FIPS | Federal Information Processing Standard |
| FT1 | Fractional T1 |
| G.SHDSL | SHDSL |
| HIM | High-speed Interface Module |
| HMAC | Hash-based Message Authentication Code |
| HTTP | Hyper Text Transfer Protocol |
| IKE | Internet Key Exchange |
| IPsec | Internet Protocol Security |
| IRF | Intelligent Resilient Framework |
| ISDN | Integrated Services Digital Network |

| Abbreviation | Full spelling |
|--------------|------------------------------------------------------------|
| KAT | Known Answer Test |
| LED | Light Emitting Diode |
| LPU | Line Processing Unit |
| MAC | Message Authentication Code |
| MAN | Metropolitan Area Network |
| Mbps | Megabits per second |
| MIM | Multifunctional Interface Module |
| MPLS | Multiprotocol Label Switching |
| MPU | Main Processing Unit |
| NAT | Network Address Translation |
| NIST | National Institute of Standards and Technology |
| NP | Network Processor |
| OAA | Open Application Architecture |
| OAP | Open Application Platform |
| OC | Optical Carrier |
| OSPF | Open Shortest Path First |
| PRI | Primary Rate Interface |
| PSU | Power Supply Unit |
| QoS | Quality of Service |
| RADIUS | Remote Authentication Dial In User Service |
| RAM | Random Access Memory |
| RSA | Rivest Shamir and Adleman method for asymmetric encryption |
| SDH | Synchronous Digital Hierarchy |
| SHDSL | Single-pair high-speed digital subscriber line |
| SIC | Smart Interface Card |
| SFP | Small Form-Factor Pluggable |
| SFP+ | Enhanced Small Form-Factor Pluggable |
| SHA | Secure Hash Algorithm |
| SIC | Smart interface card |
| SMB | SubMinature version B |
| SONET | Synchronous Optical Networking |
| SRPU | Switching and routing processor unit |
| SSL | Secure Sockets Layer |
| STM | Synchronous Transport Module |

| Abbreviation | Full spelling |
|--------------|----------------------------------------|
| TLS | Transport Layer Security |
| VCPM | Voice Co-Processing Module |
| VPLS | Virtual Private LAN Service |
| VPM | Voice Processing Module |
| XFP | 10 Gigabit Small Form-Factor Pluggable |

1 Introduction

This document is a non-proprietary Cryptographic Module Security Policy for HP MSR30/50 Ethernet routers (MSR30 and MSR50 series). The policy describes how the HP MSR30/50 routers meet the requirements of FIPS 140-2. This document also describes how to configure HP MSR30/50 routers in FIPS 140-2 mode. This document was prepared as part of the Level 2 FIPS 140-2 validation.

FIPS 140-2 standard details the U.S. Government requirements for cryptographic security appliances. More information about the standard and validation program is available on the NIST website at <http://csrc.nist.gov/groups/STM/cmvp/>

0037553004

This document includes the following sections:

- Overview
- Security Appliance Validation Level
- Physical Characteristics and Security Appliance Interfaces
- Roles, Services and Authentication
- FIPS Approved Algorithms
- Non-FIPS Approved Algorithms
- Cryptographic Key Management
- Self-Tests
- Delivery and Operation
- Physical Security Mechanism
- Mitigation of Other Attacks
- Obtaining Documentation and Technical Assistance

2 Overview

The HP MSR30/50 provides devices are suitable for a range of uses: core routers on small and medium enterprise networks, access routers for network branches on some large-sized enterprise networks, regional offices, and mid-sized businesses.

2.1 HP MSR30 Router Series

Designed for connecting enterprise branches, regional offices as well as customer presence equipment (CPE) by service providers, the HP MSR30 Series delivers unmatched performance and flexibility. A high-performance processor with modular design, this platform delivers embedded applications for business productivity, enhanced security and performance acceleration. HP MSR30 series routers feature a comprehensive portfolio of interface and modules for reliable, scalable LAN and WAN communications, along with unparalleled security and converged services with integrated encryption and voice processing.

Testing included nine models in the MSR30 series:

- HP MSR30-10 Router
- HP MSR30-10 DC Router
- HP MSR30-20 DC Router
- HP MSR30-40 Router
- HP MSR30-40 DC Router
- HP MSR30-60 Router
- HP MSR30-60 DC Router
- HP MSR30-20 PoE Router
- HP MSR30-60 PoE Router

Figure 1 shows a representative of the series. This series requires 3 Tamper-evident labels and 2 opacity shields.

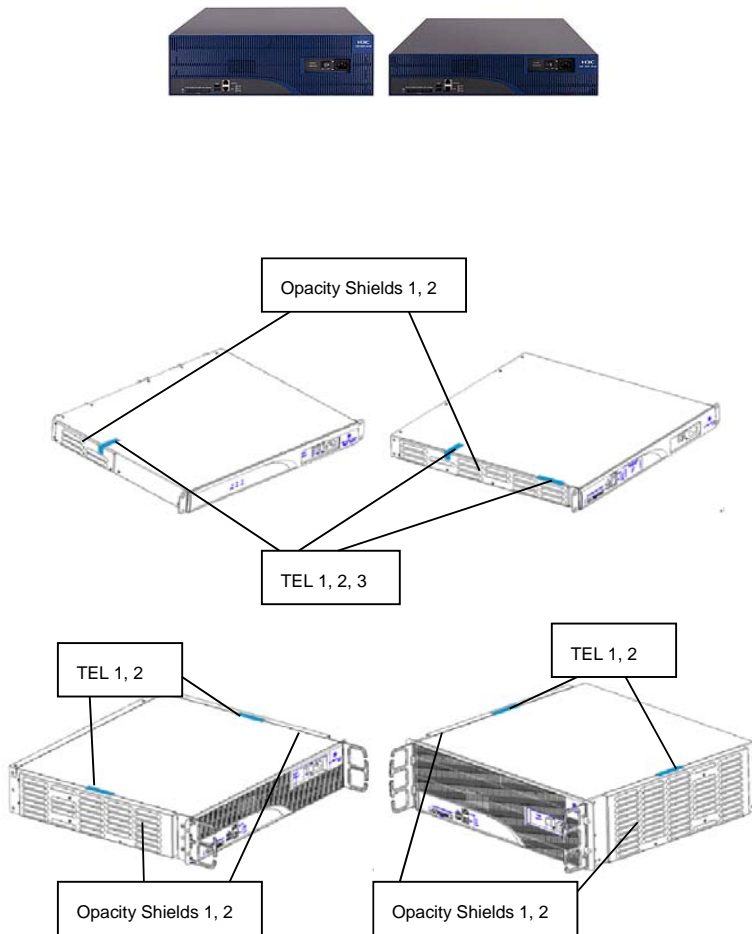


Figure 1 HP MSR30 Router Series Representative View

2.2 HP MSR50 Router Series

The HP MSR50 Series Multi-Service Routers are designed for large branches and regional offices to connect to corporate network over WAN. These routers deliver high-performance, security and integrated services on a single platform. They feature optional embedded hardware-based encryption and voice processing. The routers are based on a 1.7 GHz CPU and deliver superior performance forwarding up to 1280 Kpps. These routers are highly flexible with a wide choice of connectivity and routing choices. With a full-featured, resilient routing platform, including IPv6 and MPLS support, as well as comprehensive integrated security services, these routers enhance network functionality and simplify management and reduce complexity. High-performance rack-mount platforms, the 3U-high MSR50-40 and 4U-high MSR50-60 router chassis offer flexible, feature-rich open application architecture (OAA)-ready resilient WAN routing to connect branches to the corporate network

Testing included two models in the HP MSR50 series:

- HP MSR50-40 Router
- HP MSR50-60 Router

Figure 2 shows a representative of the series. This series requires 29 Tamper-evident labels and 2 opacity shields, 38 Tamper-evident labels and 2 opacity shields when configured as shown.

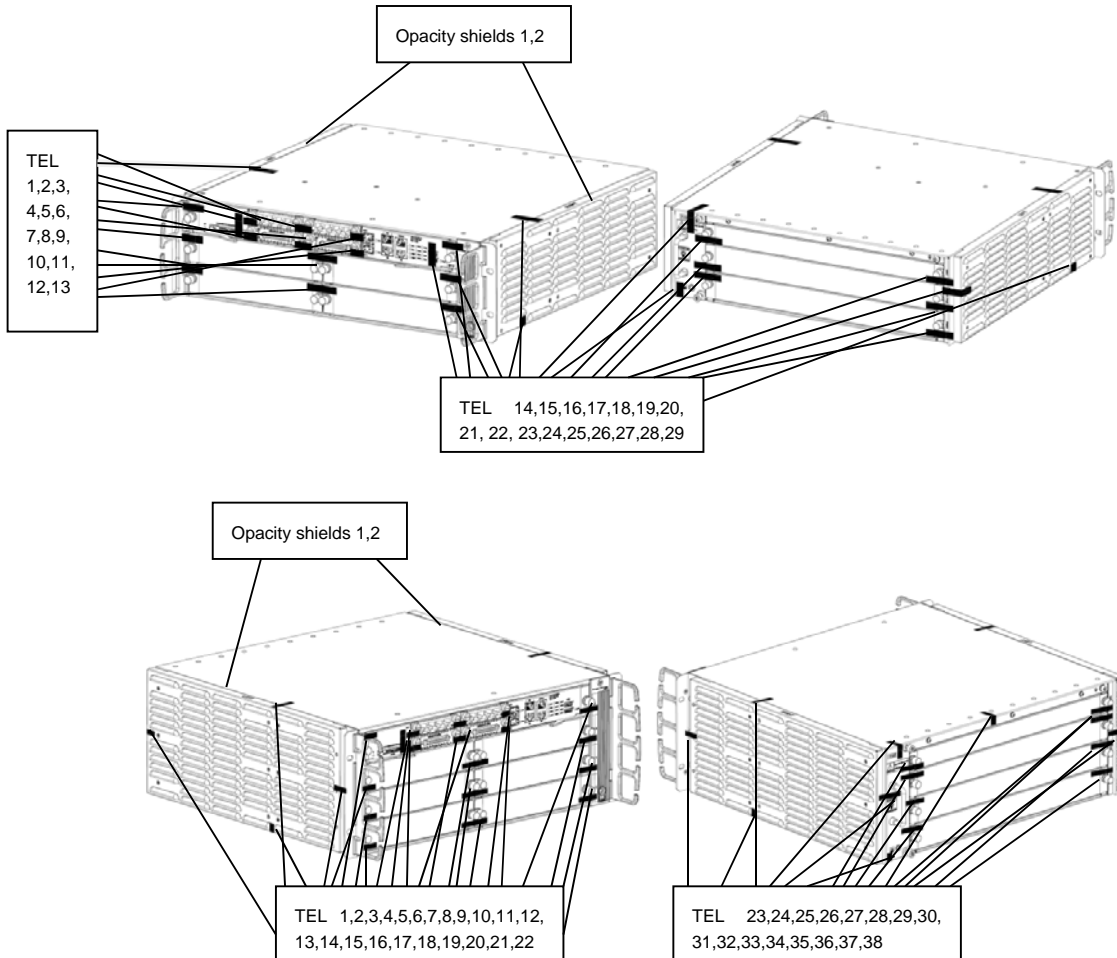


Figure 2 HP MSR50 Router Series Representative View

3 Security Appliance Validation Level

Table 1 lists the level of validation for each area in the FIPS PUB 140-2.

Table 1 Validation Level by Section

| No. | Area | Level |
|-----|---------------------------------------------------------|-------|
| 1 | Cryptographic Module Specification | 2 |
| 2 | Cryptographic Module Ports and Interfaces | 2 |
| 3 | Roles, Services, and Authentication | 2 |
| 4 | Finite State Model | 2 |
| 5 | Physical Security | 2 |
| 6 | Operational Environment | N/A |
| 7 | Cryptographic Key management | 2 |
| 8 | Electromagnetic Interface/Electromagnetic Compatibility | 2 |
| 9 | Self-Tests | 2 |
| 10 | Design Assurance | 2 |
| 11 | Mitigation of Other Attacks | N/A |

4 Physical Characteristics and Security Appliance Interfaces

Each HP MSR30/50 router is a multi-chip standalone security appliance. The cryptographic boundary is defined as encompassing the “top,” “front,” “left,” “right,” “rear”, and “bottom” surfaces of the integrated chassis. The general components of each router include firmware and hardware which are placed in the three-dimensional space within the chassis.

The HP MSR30/50 series routers use a modular design. Each HP MSR30 router supports smart interface cards (SICs) and multifunction interface modules (MIMs). Each HP MSR50 router supports SICs and flexible interface cards (FICs). The MSR50 routers require a main processing unit (MPU). An MPU process protocols, provides low-speed forwarding, controls interfaces, detects faults, runs the router system application, and stores configuration.

HP MSR routers include fixed-port.

4.1 HP MSR30 Router Series Interfaces

HP MSR30 routers support two types of interface modules: SICs and MIMs. SICs are small and cost-effective modules. SIC include DSIC, which are double wide modules. MIMs are more high-density and affordable modules. Routers MSR30-20, MSR30-20 DC, MSR30-40, MSR30-40 DC, MSR30-60 and MSR30-60 DC support four SIC modules and two, four, and six MIMs respectively. HP offers HIMs providing a variety of ports:

- 10/100 Mbps Ethernet (1 port)

- SFP 100 Mbps (1 port)
- 10/100 Mbps Ethernet L2 switching module (4 and 9 ports)
- 10/100 Mbps Ethernet L2 switching module with PoE (4 and 9 ports)
- Gigabit Ethernet / SFP Gigabit combination (1 port)
- Enhanced synchronous/asynchronous serial (1 port)
- Fractional E1 (1 and 2 ports (DB-15 connector))
- E1/CE1/PRI (1 port)
- Fractional T1 (1 port)
- T1/CT1/PRI (1 port)
- ADSL over POTS
- ADSL over ISDN (1 port)
- Analog modem (1 and 2 ports)
- Asynchronous serial (8 and 16 ports (DB-60 and four DB-28 connectors, respectively))
- ISDN BRI S/T (1 and 2 ports)
- ISDN BRI U (1 and 2 ports)
- E1 voice (1 channel (DB-15 connector))
- T1 voice (1 channel)
- Voice module subscriber circuit (1 and 2 ports)
- Voice module FXO (1 and 2 ports)
- ISDN BRI S/T voice (1 and 2 ports)
- 2-port voice subscriber circuit & 1-port voice AT0 analog trunk
- 4-port voice subscriber circuit & 1-port voice AT0 analog trunk
- Input and output audio and DOOR RELAY control signal output
- 8 Wire G.SHDSL (1 port)

MIMs provide:

- 10M100M Ethernet (1, 2, and 4 ports)
- Gigabit Ethernet (1 and 2 ports)
- SFP Gigabit (1 and 2 ports)
- 10M/100M Ethernet L2 switching module (16 ports)
- 10M/100M Ethernet L2 switching module PoE (16 ports)
- 10M/100M Ethernet with combination Gigabit Ethernet / SFP Gigabit layer 2 switching (24 ports with 2 combination ports)
- 10M/100M Ethernet PoE with combination Gigabit Ethernet / SFP Gigabit layer 2 switching (24 ports with 2 combination ports)
- 10M/100M Ethernet layer 2 switching (48 ports)
- Enhanced synchronous/asynchronous serial (2, 4, and 8 channel)
- Enhanced asynchronous serial (8, and 16 ports)
- MIM-1E1 MIM-2E1 MIM-4E1 *****
- MIM-8E1 (120) MIM-8E1 (75)
- MIM-1E1-F MIM-2E1-F MIM-8E1-F
- MIM-8E1 (120)-F MIM-8E1 (75)-F
- MIM-1T1 MIM-2T1 MIM-4T1
- MIM-8T1
- MIM-1T1-F MIM-2T1-F MIM-4T1-F MIM-8T1-F

- MIM-1G.SHDSL
- MIM-4BSE
- MIM-1CT3 MIM-1CE3 MIM-1CT3-V2 MIM-1CE3-V2
- M-1ATM-OC3
- MIM-1AE3
- MIM-1AT3
- MIM-1POS
- MIM-1POS-V2
- MIM-1CPOS (E)
- MIM-1CPOS (T))
- MIM1-AMM MIM-1ASL M-1ASM
- MIM-IMA-8E1(75/120) MIM-IMA-4E1(75/120)
- MIM-IMA-8T1 MIM-IMA-4T1
- MIM-1SHL-4W
- MIM-6AM MIM-12AM
- MIM-6FCM
- MIM -1VE1 MIM -2VE1
- MIM -1VT1 MIM -2VT1
- MIM-2FXS MIM-4FXS MIM-16FXS
- MIM-2FXO MIM-4FX
- MIM-8FXS-8FXO
- MIM-2EM MIM-4EM
- MIM-2BSV
- MIM-4BSV
- E1/CE1/FE1 (8 ports (DB-68 connector with BNC splitter cable))
- CT1/FT1 (8 ports (DB-68 connector with RJ-45 splitter cable))
- E3/CE3 (1 port (2 SMB interfaces for Tx/Rx))
- T3/CT3 (1 port (2 SMB interfaces for Tx/Rx))
- OC-3/STM-1 ATM (1 port)
- Serial (2, 4, and 8 ports (DB-28 interfaces supporting V.24, V.35, RS-449, X.21, and RS-530))

Each HIM and each MIM has LEDs for port status.

The HP MSR Router has two slots for interface modules (either HIMs or MIMs). It has four fixed ports, which are combination ports (Gigabit Ethernet / SFP Gigabit). It provides multiple management interfaces: a serial console port, an auxiliary serial port, two USB ports (type A and B), a CF card slot, power switch, and reset switch. There are status LEDs for CF card, RPS, interface module slots, system, AC power supply, and fixed ports.

The HP MSR Routers have a distributed architecture. HIMs and MIMs are mounted in flexible interface platform (FIP) modules, which are in turn mounted in a router to support different network services. The routers support FIP-110 and FIP-210 modules. A FIP-110 has four slots for MIMs. A FIP-210 has two slots for either HIMs or MIMs. Each FIP also has two combination ports (Gigabit Ethernet / SPF Gigabit) with status LEDs. The routers have, respectively, two, four, and eight service module slots that can each accommodate a FIP module. One service module slot may be used for an MPU in place of a FIP module.

Routers MSR30-20, MSR30-20 DC, MSR30-40, MSR30-40 DC, MSR30-60 and MSR30-60 DC support four SICs and two, four, and six MIMs, respectively. MSR30-10 and MSR30-10 DC routers support two SIC and one MIM.

The HP MSR30 routers support service aggregation platform (SAP) modules. A SAP module provides network ports for receiving packets from the network and sending packets to the network. HP MSR30 routers support two types of SAP modules, one type with 48 Gigabit Ethernet ports and the other type with 24 SFP Gigabit port. Both models can be routed or switched. Each SAP module has status LEDs for each port as well as for the SAP module itself. An HP MSR30 Router service module slot can accommodate a SAP module.

The HP MSR30 routers with distributed architecture each require at least one MPU. There are two types of MPU: RPE-X1 and RSE-X1. The MPUs have similar interfaces: reset button, Gigabit Ethernet management port, serial console port, auxiliary serial port, two USB ports (type A and B), and a CF card slot with CF card button. They have LEDs for run, system alarm, active/standby, management port, USB, and CF card status. RSE-X1 has an additional power status LED. The MPU differ in form factor. RPE-X1 is a half-slot wide while RSE-X1 is a full slot wide. Each model supports up to two MPU. Each router has a slot dedicated for an MPU, which can accommodate two RPE-X1 MPU. One service slot may be used for an MPU to accommodate two RSE-X1 MPUs.

4.2 HP MSR50 Router Series Interfaces

HP MSR50 Routers have slots for up to 12 LPUs. HP MSR50 routers support two types of LPUs. One type has a fixed set of ports and the other type hosts interface daughter cards. Fixed-port LPUs provide:

- Gigabit Ethernet (48 ports),
- SFP Gigabit (48 ports),
- XFP 10-Gigabit (2 and 4 ports),
- Gigabit Ethernet and SPF Gigabit (24 ports (16 Gigabit Ethernet ports and 8 combination))

HP offers four LPU that support interface daughter cards. SPE-1010-II and SPE-1010-E-II each support one interface daughter card. SPE-1020-II and SPE-1020-E-II each support two interface daughter cards. Interface daughter cards provide:

- Gigabit Ethernet (20 ports),
- SFP Gigabit (10 and 20 ports),
- XFP 10-Gigabit (1 port),
- OC-48c/STM-16c RPR SFP (2 ports),
- OC-192c/STM-64c RPR XFP (1 port),
- OC-3c/OC-12c POS SFP (8 ports),
- OC-48c/STM-16c POS SFP (4 ports),
- OC-192c/STM-64c POS XFP (1 port),
- OC-3c ATM SFP (4 ports),
- OC-12c ATM SFP (1 port),
- OC-3c/STM-1c POS SFP (2 ports) and SFP Gigabit (6 ports),
- OC-12c/STM-4c POS SFP (2 ports) and SFP Gigabit (6 ports),
- OC-48c/STM-16c POS SFP (2 ports) and SFP Gigabit (4 ports),

- OC-3/STM-1 CPOS E1/T1 SFP (1 and 2 ports) and SFP Gigabit (8 ports),
- CE1/CT1 (8 ports) and SFP Gigabit (8 ports),
- OC-3 E3/T3 (4 ports) and SFP Gigabit (4 ports),
- OC-12 E3/T3 (1 port) and SFP Gigabit (4 ports),
- CE1/TE1 (32 ports (2 DB-28 connectors) and SFP Gigabit (2 ports),

HP MSR50 Routers each have two slots for MPUs. The routers support SR02SRP1F3 and SR02SRP2F3 MPU. The MPUs present the same interfaces: SMB coaxial clock interfaces, reset button, USB (type A and B), console serial port, auxiliary serial port, RS-232/485¹, Gigabit Ethernet management port, and CF card slot. They have LEDs for LPU, MPU, USB, and CF card status.

Each HP MSR50 router can accommodate two power supply units. HP has power supply units for AC power. Each power supply unit has a power switch and status LEDs. All LPU and MPUs allow for additional connectivity, but do not process any security relevant data or information.

4.3 Physical Interfaces Mapping

The physical interfaces provided by the HP MSR30/50 routers map to four FIPS 140-2 defined logical interface: data input, data output, control input and status output. Table 2 presents the mapping.

Table 2 Correspondence between Physical and Logical Interfaces

| Physical Interface | FIPS 140-2 Logical Interface |
|---------------------------------------|------------------------------|
| Networking ports | Data Input Interface |
| Console port | |
| Management Ethernet port | |
| CF card slot | |
| Networking ports | Data Output Interface |
| Console port | |
| Management Ethernet port | |
| CF card slot | |
| Networking ports | Control Input Interface |
| Console port | |
| Management Ethernet port | |
| Power switches | |
| Reset Switch | |
| Port status LED mode switching button | Status Output Interface |
| Networking ports | |
| Console port | |
| Management Ethernet port | |
| LEDs | Power Interface |
| Power Slot | |
| Backplane | |
| USB ports | |
| AUX port | Unused Interface |
| SMB coaxial clock interfaces | |
| RS-232/485 interfaces | |
| | |

¹ The RS-232/485 interfaces is reserved and not supported at present.

5 Roles, Services, and Authentication

5.1 Roles

The HP MSR30/50 routers provide management and VPN roles. There are four management roles: Visit, Monitor, Config, and Manage. Roles Visit, Monitor, and Config correspond to the FIPS 140-2 User Role. The Manage role corresponds to the FIPS 140-2 Crypto Officer role. The devices allow multiple management users to operate the appliance simultaneously.

The HP MSR30/50 routers do not employ a maintenance interface and do not have a maintenance role.

5.2 Services

The HP MSR30/50 routers provide Internet Protocol Security (IPsec) service with Internet Key Exchange (IKE). An HP MSR30/50 router can apply the IPsec service to protect network data and to protect communication between itself and Authentication, Authorization, and Accounting (AAA) servers. The service is applied at the protocol level, and consequently, IPsec is not associated with a role. IPsec with IKE supports:

- Multiprotocol Label Switching (MPLS) Layer 3 VPN,
- MPLS Layer 2 VPN,
- Virtual Private LAN Service (VPLS),
- Multicast Domain multicast VPN,
- Open Shortest Path First (OSPF) Multi-VPN Instance Customer Edge,
- Dynamic Virtual Private Network, and
- Embedded VPN firewall.

The IPsec service is limited to the following protocol / algorithm combinations in FIPS mode of operation:

- ah (SHA-1)
- esp (AES, Triple-DES)

HP MSR30/50 routers provide six classes of management services:

- View device status,
- Network functions,
- Security management,
- Review the audit trail,
- View running status, and
- Configure the security appliance.

You can access these management services by using any of the following methods:

- Console Port
- SSH
- Web user interface via HTTPS

The console port and SSH present a command line interface while the web user interface is a graphical user interface. The following table lists services available to each role within each class of service. The role in the brackets is the corresponding role specified in FIPS 140-2. HP MSR30/50 routers do not support bypass (that is, services provided without cryptographic processing).

Table 3 Services by Role

| Role | Privilege level | Services |
|---------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Visit [User role] | 0 | 1) View device status: Currently running image version; Installed hardware components status and version. 2) Network functions: Network diagnostic service such as “ping”; Network connection service such as “SSH” client. 3) Security management: Change the privilege level. |
| Monitor [User role] | 1 | 1) View device status: Currently running image version; Installed hardware components status and version 2) Network functions: Network diagnostic service such as “ping”; Network connection service such as “SSH” client. 3) Security management: Change the privilege level. 4) Review the audit trail; |
| Config [User role] | 2 | 1) View device status: Currently running image version; Installed hardware components status and version 2) Network functions: Network diagnostic service such as “ping”; Network connection service such as “SSH” client. 3) Security management: Change the privilege level; Reset and change the password of same/lower privilege user; Maintenance of the super password; Maintenance (create, destroy, import, export) of public key/private key/shared key. 4) Review the audit trail 5) View running status: Memory status, |

| Role | Privilege level | Services |
|------------------------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | <p>Packet statistics, Interface status, Current running Image version, Current configuration, Routing table, Active sessions, Temperature, SNMP MIB statistics.</p> <p>6) Configure the security appliance: Save configuration; Management of information center (start-up and shut down audit functions; setting logbuffer, setting logfile; setting log output destination); Managing (create, modify, delete apply) the filtering rules; Management of firewall; Define network interfaces and settings; Set the protocols the security appliance will support; enable interfaces and network services.</p> |
| Manage [Crypto Officer role] | 3 | <p>1) View device status: Currently running image version; Installed hardware components status and version</p> <p>2) Network functions: Network diagnostic service such as “ping”; Network connection service such as “SSH” client.</p> <p>3) Security management: Change the privilege level; Reset and change the password of same/lower privilege user; Maintenance of the super password; Maintenance (create, destroy, import, export) of public key/private key/shared key; Shut down or Reboot the security appliance; Management (create, delete, modify) of the user group; Management (create, delete, modify) of the user account;</p> |

| Role | Privilege level | Services |
|------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | <p>Management of the time;</p> <p>Maintenance (delete, modify) system start-up parameters;</p> <p>File operation (e.g. dir, copy, del);</p> <p>Management of the command privilege;</p> <p>Install or remove HP MSR30/50 Security Appliance.</p> <p>4) Review the audit trail;</p> <p>5) View running status: Memory status, Packet statistics, Interface status, Current running image version, Current configuration, Routing table, Active sessions, Temperature, SNMP MIB statistics.</p> <p>6) Configure the security appliance: Save configuration;</p> <p>Management of information center (start-up and shut down audit functions; setting logbuffer, setting logfile; setting log output destination delete of the audit trail.);</p> <p>Managing (create, modify, delete apply) the filtering rules;</p> <p>Management of firewall;</p> <p>Define network interfaces and settings;</p> <p>Set the protocols the security appliance will support (e.g. SFTP server, SSH server);</p> <p>enable interfaces and network services;</p> <p>Management of access control scheme (e.g. domain and RADIUS scheme).</p> |

The “Fundamentals Configuration Guide” chapter of each product’s configuration document provides details of the commands that provide the services listed in Table 3. This documentation is located at <http://h17007.www1.hp.com/us/en/products/routers/index.aspx>

5.3 Authentication Mechanisms

HP MSR 30/50 Routers support both role-based and identity-based authentication.

- Identity-based authentication

Each user is authenticated upon initial access to the device. The authentication is identity-based. All users can be authenticated locally, and optionally supports authentication via a RADIUS and TACACS server.

To logon to the appliances, an operator must connect to it through one of the management interfaces (console port, SSH, HTTPS) and provide a password.

- Role-based authentication

Each User can switch to a different user privilege level without logging out and terminating the current connection. To switch to a different privilege level, a user must provide the privilege level switching authentication information. The authentication is role-based. All users can be authenticated locally, and optionally supports authentication via a RADIUS and TACACS+ server.

After the privilege level switching, users can continue to manage the device without relogging in, but the commands they can execute have changed. For example, with the user privilege level 3, a user can configure system parameters as crypto officer role. After switching to user privilege level 0, the user can execute only basic commands like ping and tracert and use a few display commands as user role.

Operators must be authenticated using user names and passwords. The passwords must:

- 1) Be a minimum of six characters long, and the maximum password size is 63.
- 2) Be a combination of alphabetic and numeric characters.
- 3) Contain punctuation characters.
- 4) Contain lower and upper case characters.

The probability of a false positive for a random password guess is less than 1 in 1,000,000. This is also valid for RADIUS or TACACS+ shared secret keys

The users who try to log in or switch to a different user privilege level can be authenticated by RADIUS and TACACS+ Server. The device (RADIUS client) and the RADIUS server use a shared key to authenticate RADIUS packets and encrypt user passwords exchanged between them. For more details, see RFC 2865: 3 Packet Format Authenticator field and 5.2 User-password

6 Approved Cryptographic Algorithms

Table 4 lists the FIPS-Approved algorithms HP MSR30/50 routers provide.

Table 4 FIPS-Approved Cryptography Algorithms

| Algorithm | Application | Certificate |
|---------------|--------------------------------------------|-------------|
| AES | Encryption/decryption | 1927 |
| Triple-DES | Encryption/decryption | 1254 |
| SHA | SHA hashing | 1692 |
| HMAC SHA | HMAC SHA for hashed message authentication | 1161 |
| RSA | Signing and verifying | 993 |
| DSA | Signing and verifying | 611 |
| X9.31 for RNG | Random number generation | 1014 |

7 Non-approved Cryptographic Algorithms

HP MSR30/50 routers provide additional cryptographic algorithms that are not FIPS Approved:

- DES
- RC4
- MD5
- MD5 HMAC
- RSA (key wrapping; key establishment methodology provides 80 or 112 bits of encryption strength)
- Diffie-Hellman (key agreement; key establishment methodology provides 80 or 112 bits of encryption strength)

8 Cryptographic Key Management

The security appliances use a variety of Critical Security Parameters (CSP) during operation. Table 5 lists the CSP including cryptographic keys used by the HP MSR30/50 security routers. It summarizes generation, storage, and zeroization methods for the CSP.

Table 5 Cryptographic Security Parameters

| # | Key/ CSP Name | Generation/ Algorithm | Description | Storage | Zeroization |
|---|------------------|--------------------------|-------------|---------|-------------|
|---|------------------|--------------------------|-------------|---------|-------------|

| # | Key/ CSP Name | Generation/ Algorithm | Description | Storage | Zeroization |
|------|---------------------------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| CSP1 | RSA public/private keys | ANSI X9.31/RSA | Identity certificates for the security appliance itself and also used in IPSec, TLS, and SSH negotiations. The security appliance supports 1024 ~ 2048 bit key sizes. | Private Key-FLASH (cipher text/Triple-DES) and RAM (plain text) Public Key-FLASH(cipher text/Triple-DES)and RAM (plain text) | Private Key-Using CLI command to zeroize, then reboot. Public Key - Using CLI command to zeroize, then reboot. |
| CSP2 | DSA public/private keys | ANSI X9.31/DSA | Identity certificates for the security appliance itself and also used in SSH negotiations. | Private Key-FLASH (cipher text/ Triple-DES) and RAM (plain text) Public Key-FLASH(cipher text/ Triple-DES and RAM (plain text) | Private Key-Using CLI command to zeroize, then reboot. Public Key - Using CLI command to zeroize, then reboot. |
| CSP3 | Diffie-Hellman Key Pairs | ANSI X9.31 / DH | Key agreement for IKE, TLS, and SSH sessions. | RAM (plain text) | Resetting or rebooting the security appliance. |
| CSP4 | Public keys | DSA / RSA | Public keys of peers | FLASH(plain text)/RAM (plain text) | Delete public keys of peers from configuration, write to startup config, then reboot |
| CSP5 | TLS Traffic Keys | Generated using the TLS protocol (X9.31PRNG + HMAC-SHA1 + either DH or RSA) Algorithm: Also Triple-DES & AES | Used in HTTPS connections | RAM (plain text) | Resetting or rebooting the security appliance. |
| CSP6 | SSH Session Keys | ANSI X9.31 / Triple-DES-AES | SSH keys | RAM (plain text) | Resetting or rebooting the security appliance |
| CSP7 | IPSec authentication keys | ANSI X9.31 / Triple-DES-AES / DH | Exchanged using the IKE protocol and the public/private key pairs. These are Triple-DES or AES keys. | RAM (plain text) | Resetting or rebooting the security appliance |
| CSP8 | IPSec traffic keys | ANSI X9.31 / Triple-DES-AES / DH | Exchanged using the IKE protocol and the public/private key pairs. These are Triple-DES or AES keys. | RAM (plain text) | Resetting or rebooting the security appliance |

| # | Key/ CSP Name | Generation/ Algorithm | Description | Storage | Zeroization |
|-------|-----------------------------------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSP9 | IPSec authentication keys | Triple-DES-AES | Triple-DES or AES Keys are manually configured for IPv6 routing protocol such as OSPFv3, RIPng, IPv6 BGP. | FLASH(plain text)/RAM (plain text) | Delete IPsec keys from configuration, write to startup config, then reboot |
| CSP10 | IPSec traffic keys | Triple-DES-AES | Triple-DES or AES Keys are manually configured for IPv6 routing protocol such as OSPFv3, RIPng, IPv6 BGP. | FLASH(plain text)/RAM (plain text) | Delete IPsec keys from configuration, write to startup config, then reboot |
| CSP11 | IKE pre-shared keys | Shared Secret | Entered by the Crypto-Officer in plain text form and used for authentication during IKE | FLASH(plain text) and RAM (plain text) | Deleting keys from the configuration via erase flash: command (or replacing), write to startup config, then reboot. |
| CSP12 | IKE Authentication key | Generated using IKE (X9.31+HMAC-SHA1+DH). Algorithms: Triple-DES, AES, SHA-1 | Used to encrypt and authenticate IKE negotiations | RAM (plain text) | Resetting or rebooting the security appliance |
| CSP13 | IKE Encryption Key | Generated using IKE (X9.31+HMAC-SHA1+DH). Algorithms: Triple-DES, AES, SHA-1 | Used to encrypt IKE negotiations | RAM (plain text) | Resetting or rebooting the security appliance |
| CSP14 | RADIUS shared secret keys | Shared Secret | Used for authenticating the RADIUS server to the security appliance and vice versa. Entered by the Crypto-Officer in plain text form and stored in plain text form. | FLASH (plain text) and RAM (plain text) | Deleting keys from the configuration via erase flash: command (or replacing), write to startup config, then reboot. |
| CSP15 | Username/ Passwords/ super password | Secret | Critical security parameters used to authenticate the administrator login or privilege promoting. | FLASH (plain text) and RAM (plain text) | Overwriting the passwords with new ones, write to startup config, then reboot. |
| CSP16 | Certificates of Certificate Authorities (CAs) | ANSI X9.31 | Necessary to verify certificates issued by the CA. Install the CA's certificate prior to installing subordinate certificates. | FLASH (plain text) and RAM (plain text) | 1. Delete PKI domain from configuration via erase flash: command, write to startup config, then reboot. 2. Use "pki delete-certificate" CLI command to delete certificates, then reboot |

| # | Key/ CSP Name | Generation/ Algorithm | Description | Storage | Zeroization |
|-------|------------------|--------------------------|-------------------------|------------------|-----------------------------------------|
| CSP17 | PRNG Seed Key | Entropy | Seed key for X9.31 PRNG | RAM (plain text) | Zeroized with generation of new seed |

8.1 Access Control Policy

Table 6, Table 7, and Table 8 list by role services accessing CSPs. Each table identifies the services that access each CSP along with the type of access allowed for the role(s). The types of access are: read (r), write (w), and delete (d).

Table 6 CSP Access by Service for Visit and Monitor Roles

| Service Access /CSP | View device status | Network functions | Security management |
|---------------------------|--------------------------|----------------------|------------------------|
| CSP1 | r | r | r |
| CSP2 | r | r | r |
| CSP3 | r | r | r |
| CSP4 | r | r | r |
| CSP5 | r | r | r |
| CSP6 | r | r | r |
| CSP7 | r | r | r |
| CSP8 | r | r | r |
| CSP9 | r | r | r |
| CSP10 | r | r | r |
| CSP11 | r | r | r |
| CSP12 | r | r | r |
| CSP13 | r | r | r |
| CSP14 | r | r | r |
| CSP14 | r | r | r |
| CSP16 | r | r | r |
| CSP17 | r | r | r |

r = read, w = write, d = delete

Table 7 Access by Service for Config Role

| Service Access /CSP | View device status | Network functions | Security management | Review the audit trail | View running status | Configure the security appliance |
|---------------------|--------------------|-------------------|---------------------|------------------------|---------------------|----------------------------------|
| CSP1 | r | r | rwd | r | r | r |
| CSP2 | r | r | rwd | r | r | r |
| CSP3 | r | r | rwd | r | r | r |
| CSP4 | r | r | rwd | r | r | r |
| CSP5 | r | r | rwd | r | r | r |
| CSP6 | r | r | rwd | r | r | r |
| CSP7 | r | r | rwd | r | r | r |
| CSP8 | r | r | rwd | r | r | r |
| CSP9 | r | r | rwd | r | r | r |
| CSP10 | r | r | rwd | r | r | r |
| CSP11 | r | r | rwd | r | r | r |
| CSP12 | r | r | rwd | r | r | r |
| CSP13 | r | r | rwd | r | r | r |
| CSP14 | r | r | r | r | r | r |
| CSP15 | r | r | rwd | r | r | r |
| CSP16 | r | r | rwd | r | r | r |
| CSP17 | r | r | rwd | r | r | r |

Table 8 Access by Service for Manage Role

| Service Access /CSP | View device status | Network functions | Security management | Review the audit trail | View running status | Configure the security appliance |
|---------------------|--------------------|-------------------|---------------------|------------------------|---------------------|----------------------------------|
| CSP1 | r | r | rwd | r | r | r |
| CSP2 | r | r | rwd | r | r | r |
| CSP3 | r | r | rwd | r | r | r |
| CSP4 | r | r | rwd | r | r | r |
| CSP5 | r | r | rwd | r | r | r |

| Service Access /CSP | View device status | Network functions | Security management | Review the audit trail | View running status | Configure the security appliance |
|---------------------|--------------------|-------------------|---------------------|------------------------|---------------------|----------------------------------|
| CSP6 | r | r | rwd | r | r | r |
| CSP7 | r | r | rwd | r | r | r |
| CSP8 | r | r | rwd | r | r | r |
| CSP9 | r | r | rwd | r | r | r |
| CSP10 | r | r | rwd | r | r | r |
| CSP11 | r | r | rwd | r | r | r |
| CSP12 | r | r | rwd | r | r | r |
| CSP13 | r | r | rwd | r | r | r |
| CSP14 | r | r | rwd | r | r | r |
| CSP15 | r | r | rwd | r | r | r |
| CSP16 | r | r | rwd | r | r | r |
| CSP17 | r | r | rwd | r | r | r |

9 Self-Tests

HP MSR30/50 routers include an array of self-tests that are run during startup and during operations to prevent any secure data from being released and to insure all components are functioning correctly.

9.1 Power-On Self-Tests

The routers perform all power-on self-tests automatically at boot when FIPS mode is enabled. All power-on self-tests must be passed before any role can perform services. The power-on self-tests are performed prior to the initialization of the forwarding function, which prevents the security appliance from passing any data during a power-on self-test failure.

Table 9 HP MSR30/50 Switch Power-On Self-Tests

| Implementation | Tests Performed |
|-----------------------------|----------------------------------|
| Security Appliance Software | Software/firmware Test |
| | DSA KAT (signature/verification) |
| | RSA KAT (signature/verification) |
| | RSA KAT (encrypt/decrypt) |
| | AES KAT |
| | Triple-DES KAT |
| | SHA-1 KAT |

| Implementation | Tests Performed |
|----------------------------------|----------------------------------|
| Security Appliance crypto engine | HMAC SHA-1 KAT |
| | PRNG KAT |
| | DSA KAT (signature/verification) |
| | RSA KAT (signature/verification) |
| | RSA KAT (encrypt/decrypt) |
| | AES KAT |
| | Triple-DES KAT |
| | SHA-1 KAT |
| | HMAC SHA-1 KAT |
| PRNG KAT | |

9.2 Conditional Self-Tests

Table 10 lists the conditional self-tests implemented by the routers. Conditional self tests run when a router generates a DSA or RSA key pair and when it generates a random number.

Table 10 HP MSR30/50 Switch Conditional Self-Tests

| Implementation | Tests Performed |
|-----------------------------|---------------------------------------------------------------------------|
| Security Appliance Software | Pairwise consistency test for RSA |
| | Pairwise consistency test for DSA |
| | Continuous Random Number Generator Test for the FIPS-approved RNG (X9.31) |

10 Delivery and Operation

10.1 Secure Delivery

To ensure no one has tampered with the goods during delivery, inspect the MSR30/50 router physical package and check as follows:

- Outer Package Inspection
 - 1) Check that the outer carton is in good condition.
 - 2) Check the package for a HP Quality Seal or IPQC Seal, and ensure that it is intact.
 - 3) Check that the IPQC seal on the plastic bag inside the carton is intact.
 - 4) If any check failed, the goods shall be treated as dead-on-arrival (DOA) goods.
- Packing List Verification

Check against the packing list for discrepancy in material type and quantity. If any discrepancy found, the goods shall be treated as DOA goods.
- External Visual Inspection

Inspect the cabinet or chassis for any defects, loose connections, damages, and illegible marks. If any surface defect or material shortage found, the goods shall be treated as DOA goods.
- Confirm Software/firmware
 - 1) Version verification

To verify the software version, start the appliance, view the self test result during startup, and use the display version command to check that the software version is Comware software, Version 5.2, Release 1002(CC). 'FIPS1402&CC' indicate it is a FIPS 140-2 and CC certification version. If software loading failed or the version information is incorrect, please contact HP for support.

2) SHA-256 verification

To verify that software/firmware has not been tampered, run SHA Hash command on the appliance. If the hash value is different from release notes of this software, contact HP for support. To get release notes, please access HP website.

- DOA (Dead on Arrival)

If the package is damaged, any label/seal is incorrect or tampered, stop unpacking the goods, retain the package, and report to HP for further investigation. The damaged goods will be replaced if necessary.

10.2 Secure Operation

The rules for securely operating an HP MSR30/50 router in FIPS mode are:

- 1) Install and connect the device according to the installation and configuration guides.
- 2) Start the device, and enter the configuration interface.
- 3) Check and configure the clock.
- 4) By default, the device does not run in FIPS mode. Enable the device to work in FIPS mode using the **fips mode enable** command in system view. This will allow the router to internally enforce FIPS-compliance behavior, such as run power-up self-test and conditional self-test.
- 5) Delete all MD5-based digital certificates.
- 6) Delete the DSA key pairs that have a modulus length of less than 1024 bits and all RSA key pairs.
- 7) Set up username/password for crypto officer role and user role. Each password must comprise no less than 6 characters and must contain uppercase and lowercase letters, digits, and special characters.
- 8) Save the configurations and re-start the device.
The device works in FIPS mode after restarting:
- 9) Configure the security appliance to use SSHv2.
- 10) Configure the security appliance to use HTTPS for performing system management.

An operator can determine whether a router is in FIPS mode with the command **display fips status**. When in FIPS mode:

- The FTP/TFTP server is disabled.
- The Telnet server is disabled.
- The HTTP server is disabled.
- SNMP v1 and SNMP v2c are disabled. Only SNMP v3 is available.
- The SSL server only supports TLS1.0.
- The SSH server does not support SSHv1 clients
- Generated RSA/DSA key pairs have a modulus length from 1024 to 2048 bits.

- SSH, SNMPv3, IPsec and SSL do not support DES, RC4, or MD5.

11 Physical Security Mechanism

FIPS 140-2 Security Level 2 Physical Security requirements mandate that a cryptographic module have an opaque enclosure with tamper-evident seals for doors or removable covers. All MSR-series routers need both opacity shields and tamper-evident seals to meet the Physical Security requirements.

The Crypto Officer is responsible for properly placing all tamper evident labels on a router. The security labels recommended for FIPS 140-2 compliance are provided in the FIPS Kits:

All units use the same label kits:

| Label Kit – Description | Label Kit - Part Number |
|---------------------------------------------|-------------------------|
| HP 12mm x 60mm Tamper-Evidence (30) Labels | JG585A |
| HP 12mm x 60mm Tamper-Evidence (100) Labels | JG586A |

The customer can order either kit to provide the required number of labels for their installation needs.

The opacity kit for each product model is below.

MSR30 series:

| Unit | Opacity Kit – Description | Opacity kit – Part Number |
|---------------------------------------------|--------------------------------|---------------------------|
| HP MSR30-10 Router HP MSR30-10 DC Router | HP MSR30-10 Opacity Shield Kit | JG582A |
| HP MSR30-20 Router HP MSR30-20 DC Router | HP MSR30-20 Opacity Shield Kit | JG579A |
| HP MSR30-40 Router HP MSR30-40 DC Router | HP MSR30-40 Opacity Shield Kit | JG580A |
| HP MSR30-60 Router HP MSR30-60 DC Router | HP MSR30-60 Opacity Shield Kit | JG581A |
| HP MSR30-20 PoE Router | HP MSR30-20 Opacity Shield Kit | JG579A |
| HP MSR30-40 PoE Router | HP MSR30-40 Opacity Shield Kit | JG580A |
| HP MSR30-60 PoE Router | HP MSR30-60 Opacity Shield Kit | JG581A |

MSR50 series:

| Unit | Opacity Kit – Description | Opacity kit – Part Number |
|-----------------------|--------------------------------|---------------------------|
| HP MSR50-40 Router | HP MSR50-40 Opacity Shield Kit | JG583A |
| HP MSR50-60 Router | HP MSR50-60 Opacity Shield Kit | JG584A |
| HP MSR50-40 DC Router | HP MSR50-40 Opacity Shield Kit | JG583A |

These security labels are very fragile and cannot be removed without clear signs of damage to the labels.

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

The Crypto Officer is responsible for properly placing all tamper evident labels on a router and is responsible for the securing and control of any unused seals and opacity shields. The Crypto Officer shall clean the module of any grease, dirt, or oil before applying the tamper-evident labels or opacity shields. The Crypto Officer is also responsible for the direct control and observation of any changes to the modules such as reconfigurations where the tamper-evident labels or opacity shields are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS approved state.

Each modular router is entirely encased by a thick steel chassis. Modular routers have MPU slots, LPU slots, fan trays, power supplies, and covers. Use the procedure described in the install guide to apply tamper evident labels and opacity shields to the router.

Any chassis slot that is not populated with a module must have a slot cover installed in order to operate in a FIPS compliant mode. The slot covers are included with each chassis, and additional slot covers may be ordered from HP.

The Crypto Officer should inspect the tamper evident labels periodically to verify they are intact and the serial numbers on the applied tamper evident labels match the records in the security log.

12 Mitigation of Other Attacks

The Security appliances do not claim to mitigate any attacks in a FIPS approved mode of operation.

13 Documentation References

13.1 Obtaining documentation

You can access the HP Networking products page: <http://h17007.www1.hp.com/us/en/> , where you can obtain the up-to-date documents of HP Routers and Switches, such as datasheet, installation manual, configuration guide, command reference, and so on.

13.2 Technical support

For technical or sales related question please refer to the contacts list on the HP website: <http://www.HP.com>.

The actual support website is:

<http://www8.hp.com/us/en/support-drivers.html>