FastIron ICX™ 7450 Series Switch/Router

FIPS 140-2 Non-Proprietary Security Policy Level 1

Document Version 2.5

November 9, 2020

Table of Contents:

Table of Tables:

Table of Figures:

1 Introduction

The FastIron® ICX® 7450 Switch delivers the performance, flexibility, and scalability required for enterprise Gigabit Ethernet (GbE) access deployment. It offers market-leading stacking density with up to 12 switches (576x 1 GbE and 48x 10 GbE ports) per stack and combines chassis-level performance and reliability with the flexibility, cost-effectiveness, and "pay as you grow" scalability of a stackable solution. This stackable switch is one of the first in its class to offer 40 GbE uplinks, enabling enterprises to dramatically increase their network capacity while using their existing optical wire infrastructure. In addition, the ICX 7450 is the industry's first stackable switching solution to combine the performance and flexibility of network switching with the advantages of site-to-site IPsec VPN security to ensure end-to-end data integrity without the need for dedicated encryption appliances. The Ruckus ICX 7450 IPSec Service Module provides hardware-based acceleration for IPsec VPNs using Advanced Encryption Standards (AES). It leverages programmable hardware technology to future-proof data protection, enabling more capabilities to be added as business needs evolve.

2 Overview

The FIPS 140-2 validation includes hardware devices running the firmware version presented in Table 1. The module meets an overall FIPS 140-2 compliance of Security Level 1.

Table 2 list the devices included in this validation.

Table 3 lists the three (3) ICX 7450 series devices, referred collectively for the remainder of this document as ICX 7450 device (cryptographic module, or simply the module). Each ICX 7450 device is a fixed-port switch which provides three (3) modular slots. In addition, four (4) different optional port modules are offered for the ICX 7450. These modules are interchangeable and can be installed in any of the three modular slots within the ICX 7450. This environment is a multi-chip standalone cryptographic module. ICX 7450 offers a selection of PoE/non-PoE and AC/DC power supply options with front-to-back or back-to-front airflow cooling options. The DC power supply can be installed in either PoE or non-PoE switches. The power supplies and fan tray assemblies are part of the cryptographic boundary. Unpopulated power supplies and fan trays are covered by opaque bezels, which are part of the cryptographic boundary when the secondary redundant power supplies and/or fans trays are not used. The cryptographic boundary for each ICX 7450 device is represented by the opaque enclosure (including the power supply, fan tray and bezels) with removable cover.

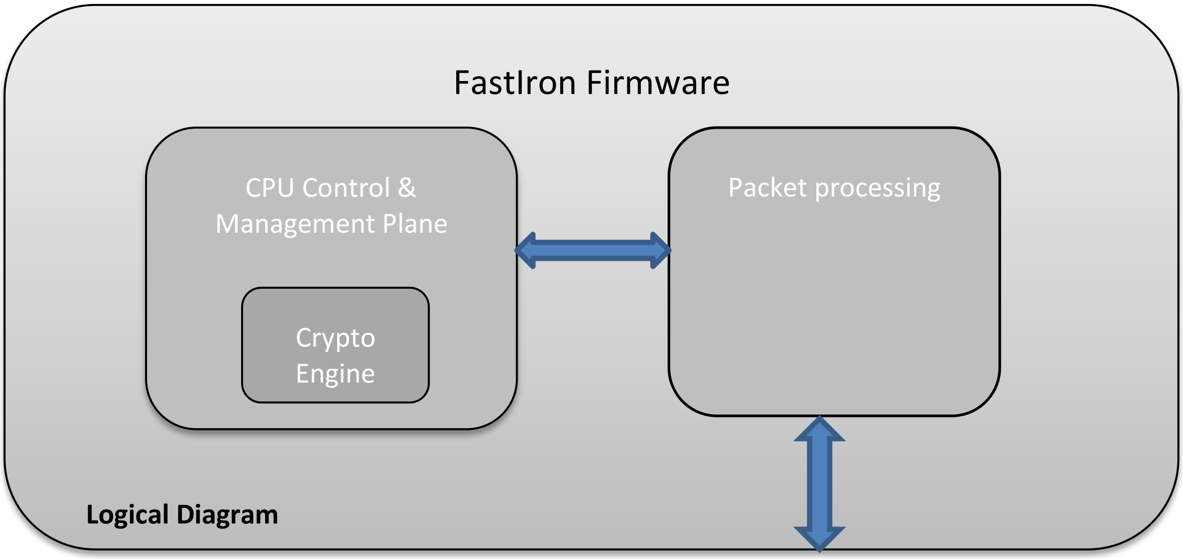

Figure 1 - Block diagram

3 FastIron Firmware

Each of the ICX series runs a different firmware image which is built from the same source code. This firmware image includes the cryptographic functionality described under Section 6. The firmware can be built as an "S" (switch) or an "R" (router) version. The "R" image has Router functionality in addition to the functionality in the "S" image. The source code for cryptographic module on both images is identical and is compiled identically. The "-I" and "-E" designations in Table 3 define the airflow direction as either intake or exhaust. The "-24" and "-48" designations in Table 2 define the port count, and the designator "P" following the port count indicate PoE+ ports; the designator "F" indicate Small Form-Factor Pluggable (SFP) ports. Otherwise, devices with similar SKUs are identical.

Firmware Versions
IronWare R08.0.90a
IronWare R08.0.95a

Table 1 - Firmware Versions

4 ICX 7450 Series

SKU	Brief Description
ICX7450-24P-E2	24-port 1 GbE PoE+ switch
ICX7450-48P-E2	48-port 1 GbE PoE+ switch
ICX7450-48F-E2	48x 1GbE SFP ports switch
ICX7400-SERVICE-MOD	Ruckus ICX IPSec module

Table 2 - ICX 7450 Switch Family Part Numbers of Validated Cryptographic Modules

ICX 7450 Hardware Versions		
Switch Models	**Components**	**Field Replaceable Units (Max Count)**
ICX7450-24P (See notes 1, 2, 3 below)	Modules:	Three (3) slots could be occupied with a combination of any of these modules (see Table Notes below). ICX7400-4X1GF (1), ICX7400-4X10GF (3), ICX7400-4X10GC (3), ICX7400-1X40GQ (3) ICX7400-SERVICE-MOD (1)
	Power Supply:	RPS16-E (2), or RPS16DC-E (2), or RPS16-I (2), or RPS16DC-I (2)
	Fan Tray:	ICX-FAN10-I (2), or ICX-FAN10-E (2)
	Filler Panel:	Filler Panel (5)
ICX7450-48P (See notes 1, 2, 3, 4 below)	Modules:	Three (3) slots could be occupied with a combination of any of these modules (see Table Notes below). ICX7400-4X1GF (1), ICX7400-4X10GF (3), ICX7400-4X10GC (3), ICX7400-1X40GQ (2) ICX-7400-SERVICE-MOD (1)
	Power Supply:	RPS16-E (2), or RPS16DC-E (2), or RPS16-I (2), or RPS16DC-I (2)
	Fan Tray:	ICX-FAN10-I (2), or ICX-FAN10-E (2)
	Filler Panel:	Filler Panel (5)
ICX7450-48F (See notes 1, 2, 3, 4 below)	Modules:	Three (3) slots could be occupied with a combination of any of these modules (see Table Notes below). ICX7400-4X1GF (1), ICX7400-4X10GF (3), ICX7400-4X10GC (3), ICX7400-1X40GQ (2) ICX7400-SERVICE-MOD (1)
	Power Supply:	RPS15-E (2), or RPS16DC-E (2), or RPS15-I (2), or RPS16DC-I (2)
	Fan Tray:	ICX-FAN10-I (2), or ICX-FAN10-E (2)
	Filler Panel:	Filler Panel (5)

Table 3 - ICX 7450 Support Matrix

Table Notes:

1. Each Switch model shall be fully populated with a minimum of one Power Supply and one Fan unit, with every remaining slot populated with a Field Replaceable Unit[1] (FRU) as per the table above.

2. Direction of the airflow for the Power Supply shall match the direction of the airflow of the Fan unit (e.g., ICX-FAN10-E shall be used in conjunction with RPS15-E, RPS16-E and RPS16DC-E).

3. The ICX7400-4X1GF (P/N: 80-1008334-01) FRU shall only be inserted in the front panel slot.

4. The ICX7400-1X40GQ (P/N: 80-1008331-01) FRU shall not be inserted in the front panel slot.

See Table 2, ICX 7450 Switch Family Part Numbers of Validated Cryptographic Modules.

Figure 2 and Figure 3 illustrate the ICX7450-48P with ICX-7400-SERVICE -MODULE inserted.

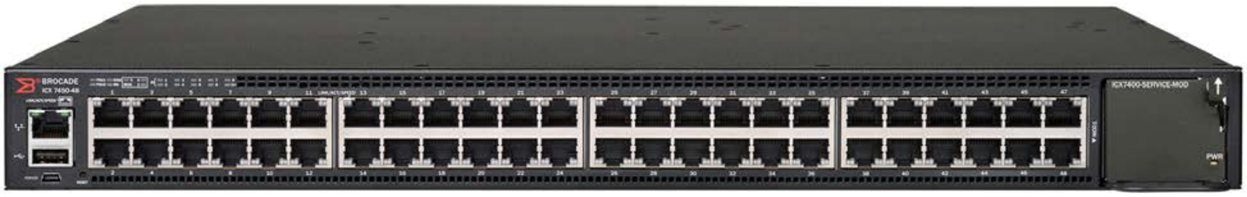

Figure 2 - Front/top side if IX7450-48P with IPSec module inserted

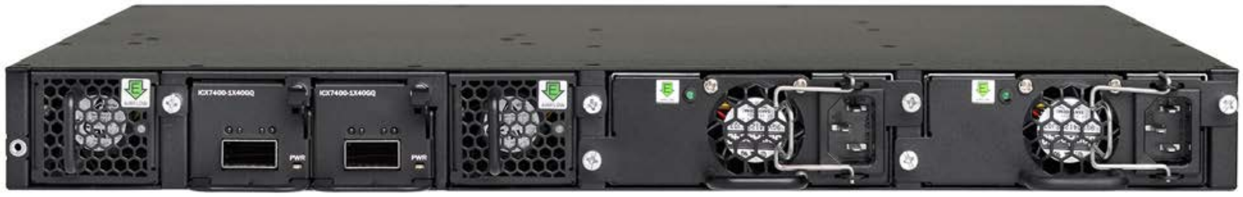

Figure 3 - Back side of ICX7450-48P with IPSec module inserted

Figure 4 and Figure 5 shows ICX7450-24P with optional Ruckus ICX7400-1X40GQ with QSFP+ uplink module.

[1] While conventional, the term “Field Replaceable Unit” is a misnomer here. To preserve the module boundary, FRUs must not be replaced in the field once the module has been commissioned.

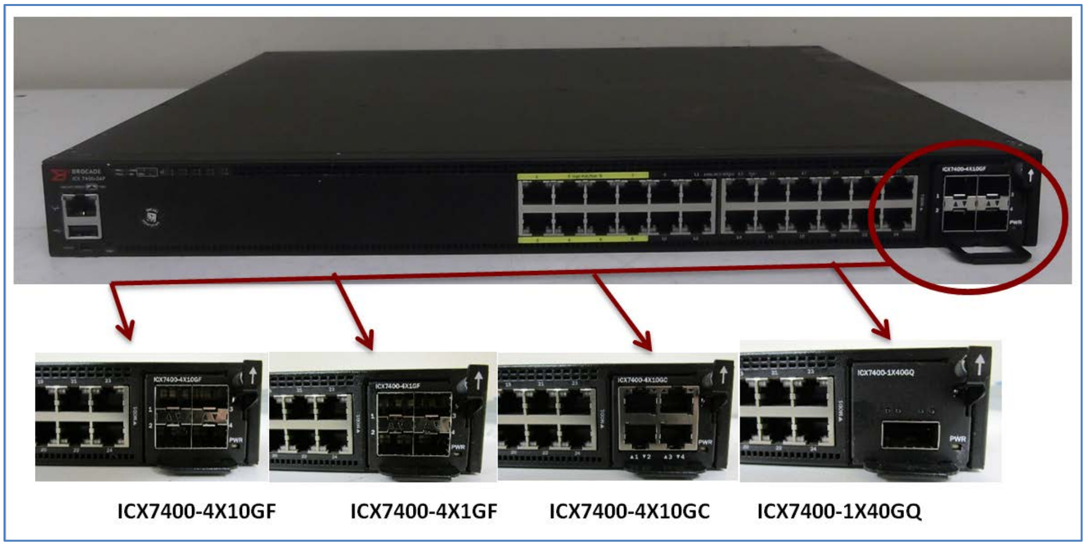

Figure 4 - Front/top side of the module ICX7450-24P with ICX7400-4X10GF, ICX7400-4X1GF, ICX7400-4X10GC and ICX7400-1X40GQ

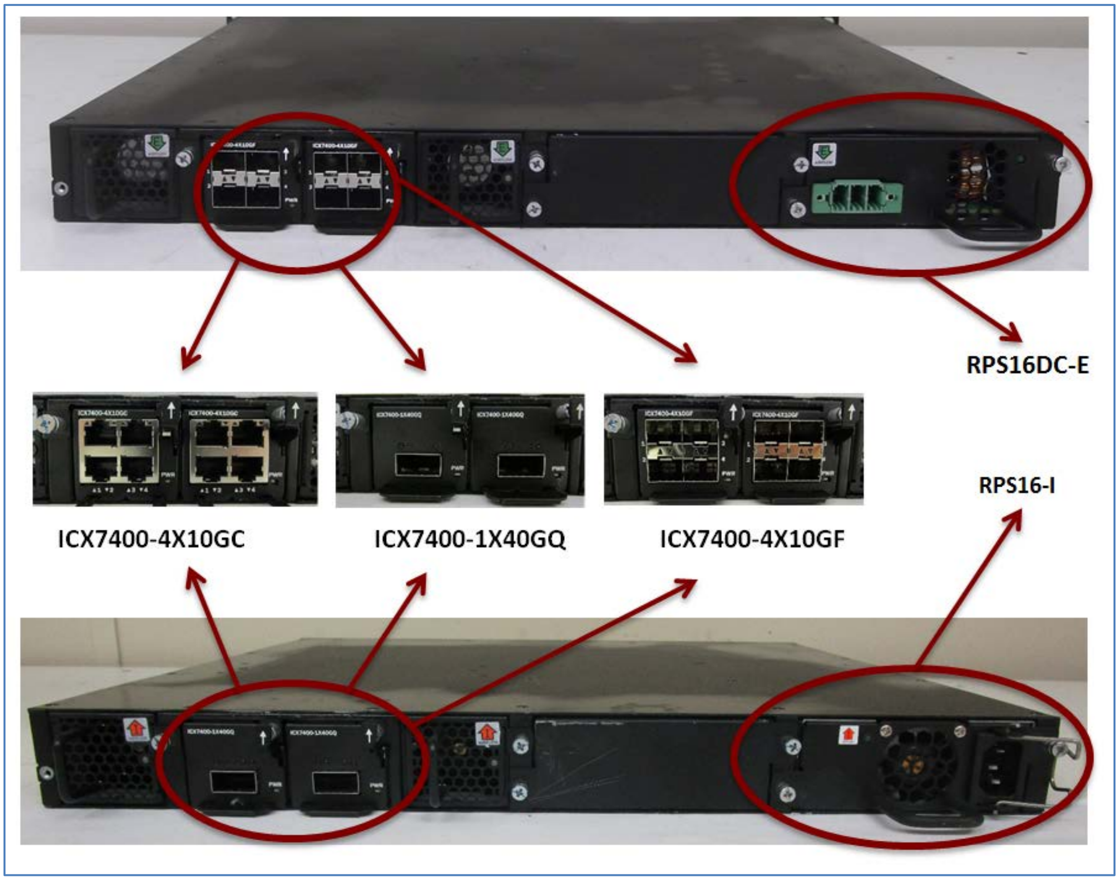

Figure 5 - Back side of the module ICX7450-24P with ICX7400-4X10GC, ICX7400-1X40GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom]

Figure 6 and Figure 7 show ICX7450-48P with optional Ruckus ICX7400-4X10GF with SFP+ uplink module.

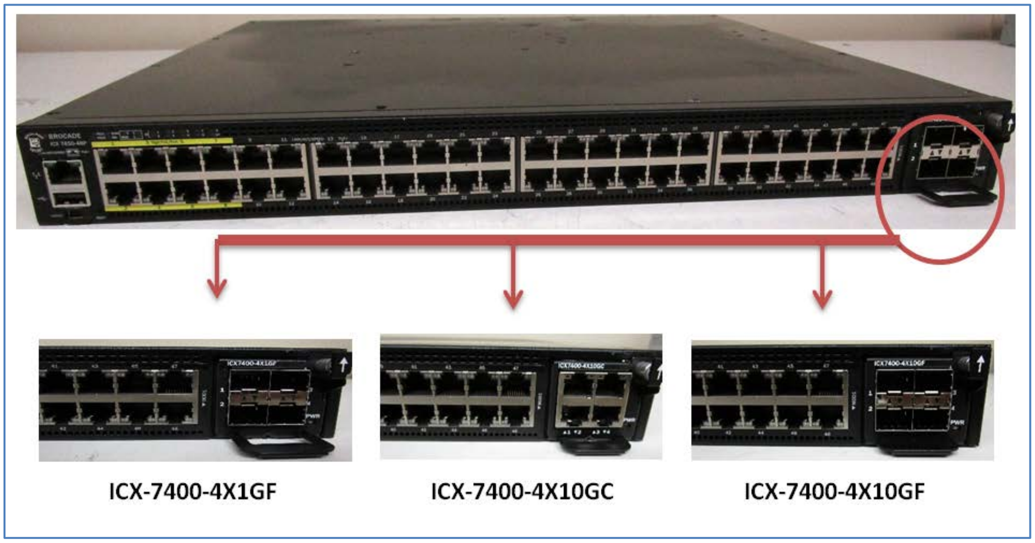

Figure 6 - Front/top side of the module ICX7450-48P with ICX74004X1GF, ICX7400-4X10GC and ICX7400-4X10GF

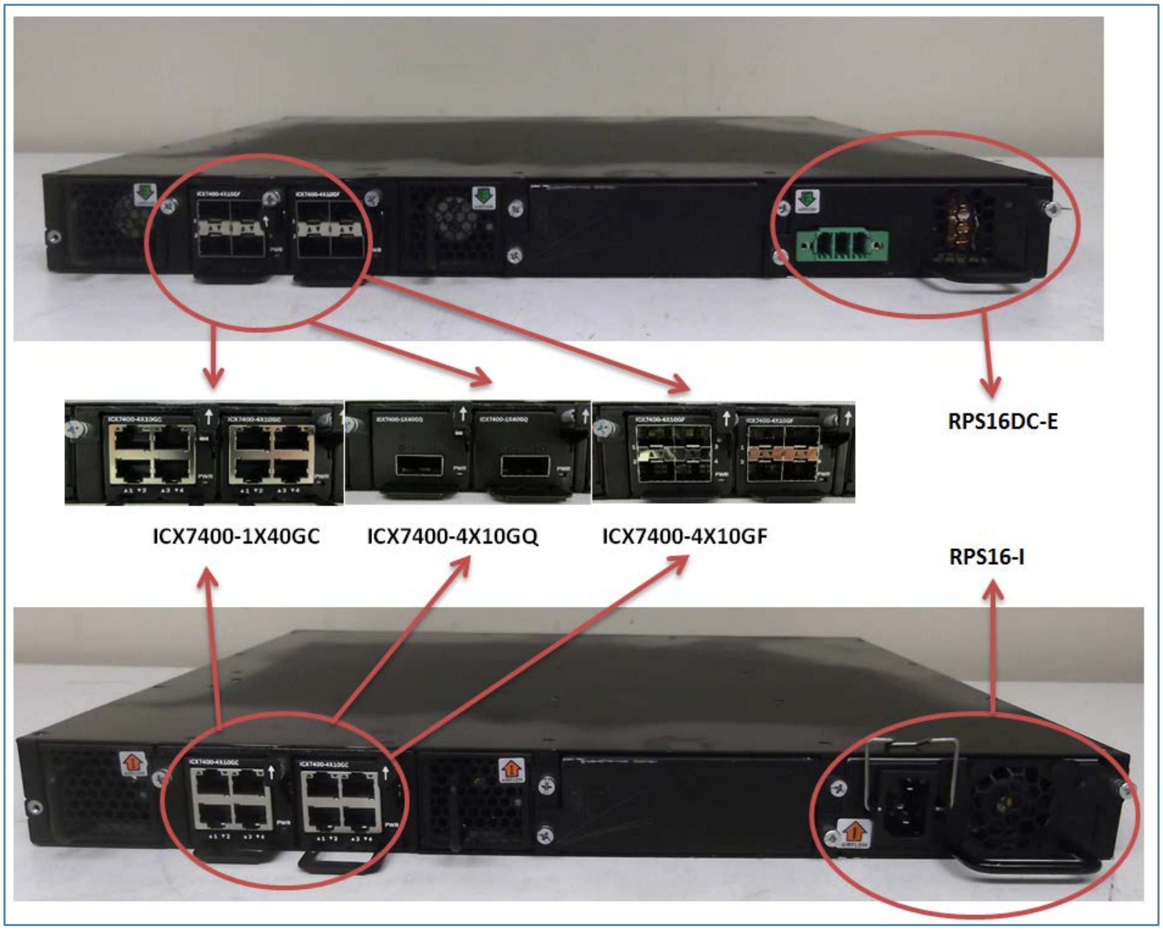

Figure 7 - Back side of the module ICX7450-48P with ICX7400-1X40GC, ICX7400-4X10GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom]

Figure 8 and Figure 9 show ICX7450-48F with optional Ruckus ICX 7400-4X10GF with SFP+ uplink module.

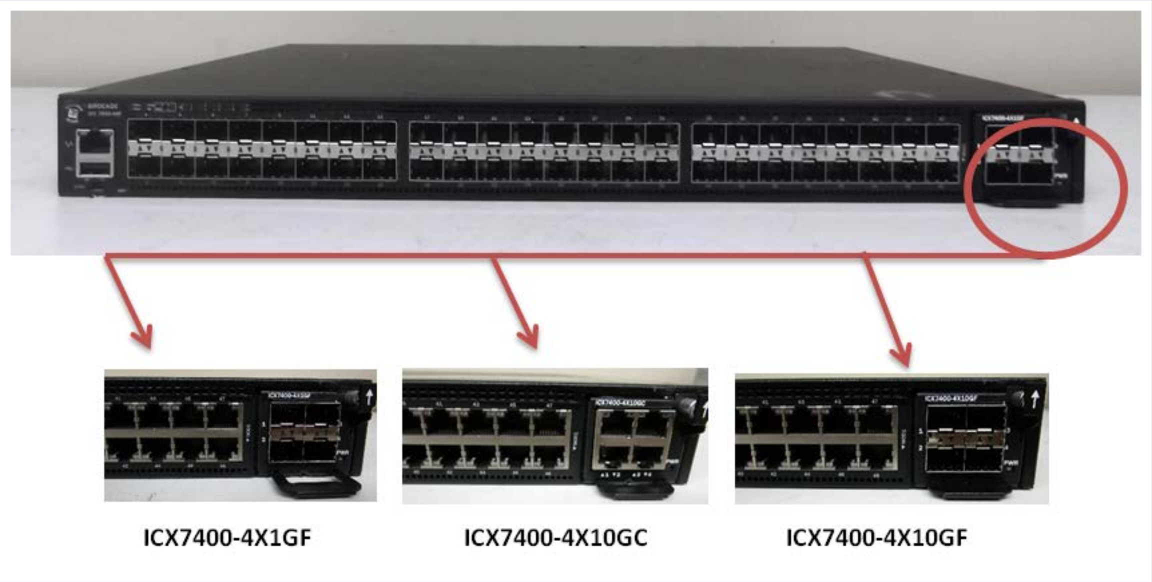

Figure 8 - Front/top side of the module ICX7450-48F with ICX7400-4X1GF, ICX7400-4X10GC and ICX7400-4X10GF

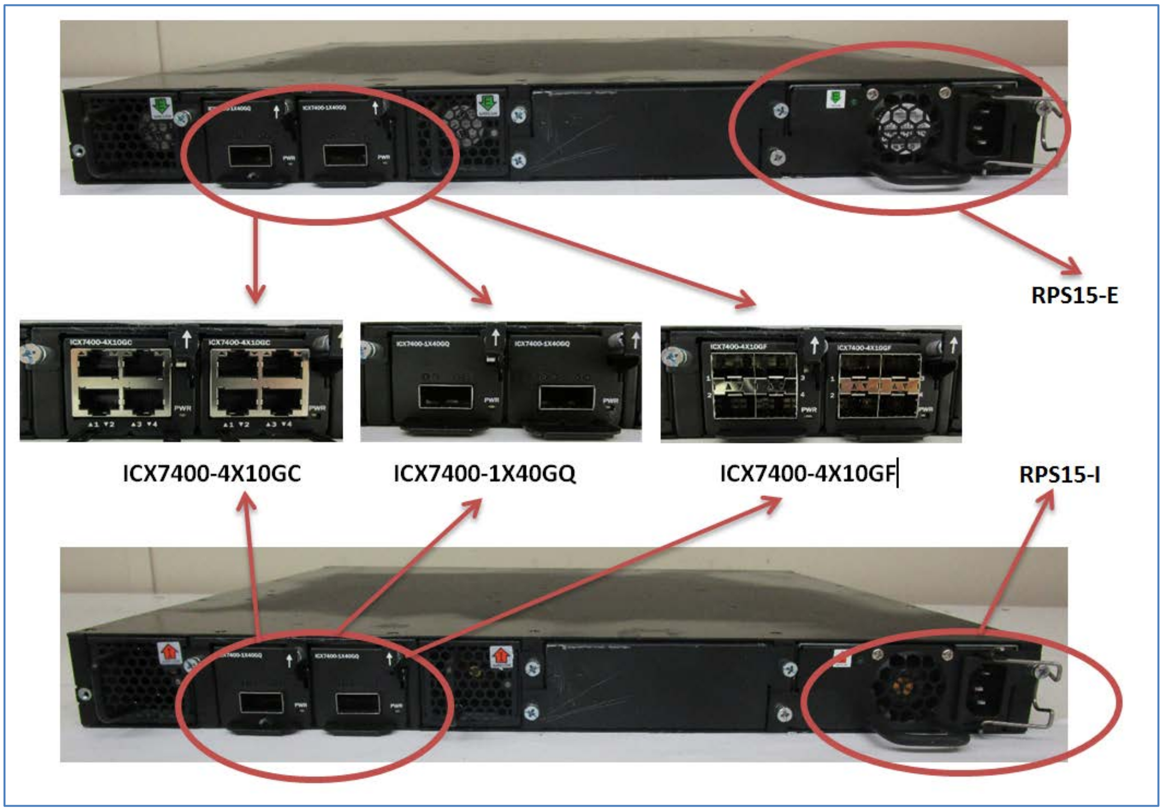

Figure 9 - Back side of the module ICX7450-48F with ICX7400-1X40GC, ICX7400-4X10GQ and ICX7400-4X10GF [DC power supply top; AC power supply bottom]

5 Ports and Interfaces

5.1 ICX 7450 Series

An ICX 7450 device provides network ports, management connectors, and a status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

The ICX 7450 devices provide a range of physical network ports. The series supports both copper and fiber connectors. The ICX 7450 device has one RJ-45 network management port, one mini USB serial management port, and one USB storage port on the front panel.

Table 4 shows the correspondence between the physical interfaces of an ICX 7450 device and the logical interfaces defined in FIPS 140-2.

Physical Port	Logical Interface
SFP ports	Data input, Data output, Control input, Status output
QSFP ports	Data input, Data output, Control input, Status output
10/100/1000 Mbps RJ-45 ports	Data input, Data output, Control input, Status output
AC socket	Power
DC socket	Power
Console Port	Data input, Control input, Status output
Out of band management port	Data input, Status output
Reset	Control input
LED	Status output
USB type-A port	This port is permanently disabled

Table 4 - ICX 7450 Port mapping to logical interface

Table 5 through Table 12 summarizes the physical port LED status provided by ICX 7450 devices.

LED state	Status of hardware
Off (no light)	Not cabled
Steady amber	Port link is up in 10/100 Mbps mode. No traffic is being transmitted
Blinking amber	There is 10/100 Mbps traffic and packets are being transmitted or received
Steady green	Port link is up in 1 Gbps mode. No traffic is being transmitted
Blinking green	There is 1 Gbps traffic and packets are being transmitted or received

Table 5 - Management port (10/100/1000 Mbps) status LED

LED state	Status of hardware
Off (no light)	Not cabled
Steady amber	Link is up in 100 Mbps mode.
Blinking amber	There is 100 Mbps traffic and packets are being transmitted or received

Steady green	Link is up in 1 Gbps mode
Blinking green	There is 1 Gbps traffic and packets are being transmitted or received

Table 6 - 100/1000 Mbps RJ-45 port LEDs

LED state	Status of hardware
Steady green	Port is providing POE power to a connected device.
Off	Port is not providing PoE power

Table 7 - 100/1000 Mbps RJ-45 PoE LEDs

LED state	Status of hardware
Off (no light)	Not cabled
Steady amber	Link is up in 100 Mbps mode.
Blinking amber	There is 100 Mbps traffic and packets are being transmitted or received
Steady green	Link is up in 1 Gbps mode
Blinking green	There is 1 Gbps traffic and packets are being transmitted or received

Table 8 - 100/1000 Mbps SFP port LEDs

LED state	Status of hardware
Off (no light)	Not cabled
Steady amber	Link is up in 1 Gbps mode.
Blinking amber	There is 1 Gbps traffic and packets are being transmitted or received
Steady green	Link is up in 10 Gbps mode
Blinking green	There is 10 Gbps traffic and packets are being transmitted or received

Table 9 - 1/10 Gbps RJ-45 port LEDs

LED state	Status of hardware
Off (no light)	Not cabled
Steady amber	Link is up in 1 GbE mode.
Blinking amber	There is 1 GbE traffic and packets are being transmitted or received
Steady green	Link is up in 10 GbE mode
Blinking green	There is 10 GbE traffic and packets are being transmitted or received

Table 10 - 1/10 GbE SFP+ module port LEDs

LED state	Status of hardware
Off (no light)	Not cabled
Steady green	Link is up in 40 GbE mode (MOD2 data uplink mode or MOD3/MOD4 stacking mode)
Blinking green	There is 40 GbE traffic and packets are being transmitted or received

Table 11 - 40 GbE mode QSFP+ module port LEDs (left-side LED)

LED state	Status of hardware
Off (no light)	Not cabled
Steady amber	Port lane link is up in 10 GbE mode (MOD2 data uplink mode)
Blinking amber	There is 10 GbE traffic and packets are being transmitted or received

Table 12 - 4x10 GbE mode QSFP+ module port LEDs

Table 13 through Table 18 summarizes the system LED status provided by ICX 7450 devices.

LED state	Status of hardware
Off (no light)	System is off or there is no power
Steady green	PSU is on and functioning properly
Steady amber	PSU is missing power or in a faulty state (such as PSU fan failure)

Table 13 ICX 7450 - PSU1 and PSU2 LEDs

LED state	Status of hardware
Off (no light)	Diagnostic is off
Blinking green	System self-diagnostic test is in progress
Steady green	System self-diagnostic test has successfully completed
Steady amber	System self-diagnostic test has detected a fault

Table 14 - ICX 7450 - DIAG LED

LED state	Status of hardware
Off (no light)	Stacking mode is enabled and the switch is a stack member operating in slave mode, or the switch is operating in standalone mode.
Blinking green	Device is initializing
Steady green	Stacking mode is enabled and the switch is the stack master
Steady amber	Stacking mode is initializing and the switch is the standby controller
Blinking amber	Stacking mode is initializing and the switch is in stacking master arbitration/selection state.

Table 15 - ICX 7450 - MS LED

LED state	Status of hardware

Off (no light)	Module is used for stacking or no module is installed. For stacking modules, this means that stacking mode is enabled, and the switch is a stack member, or the switch is operating in stand-alone mode
Steady green	Module is operating normally. For stacking modules, this means that stacking mode is enabled, and the switch is a stack master

Table 16 - ICX 7450 - MOD LED

LED state	Status of hardware
Steady green	Indicates stack unit identifier. (Unit numbers 11 and 12 are shown by using the 10+ LED in combination with the 1 or 2 LED.)

Table 17 - ICX 7450 - Stack ID LEDs

LED state	Status of hardware
Off (no light)	Module is not receiving power
Steady green	Module is on and functioning properly
Steady amber	Module is on and booting up

Table 18 - ICX 7450 - Module Power LED (all media/stacking modules)

6 Modes of Operation

ICX 7450 devices have two modes of operation: FIPS Approved mode and non-Approved mode. Section 6.3 describes services and cryptographic algorithms available in FIPS-Approved mode. In FIPS non-Approved mode, the module runs without these FIPS policy rules applied. Section 8.3 FIPS Approved Mode describes how to invoke FIPS Approved mode. Before the module has been invoked into the FIPS Approved mode for the first time, the module is in an initial non-compliant state. Power on Self-Tests (POSTs), other than the Firmware Integrity Test, do not run in this initial state. Once the FIPS Approved mode is invoked, self-tests will continue to run in both the FIPS Approved mode and FIPS non-Approved mode.

6.1 Module Validation Level

The module meets an overall FIPS 140-2 compliance of Security Level 1

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Table 19 - Security Requirements and Levels

6.2 Roles

In FIPS Approved mode, the cryptographic modules support five (5) roles: Crypto Officer, Port Configuration Administrator, User Role, MACsec Peer and IKEv2/IPsec Peer:

1. Crypto Officer Role (Super User): The Crypto Officer Role on the device in FIPS Approved mode is equivalent to the administrator role super-user in non-FIPS mode. The Crypto Officer Role has complete access to the system. The Crypto Officer is the only role that can perform firmware loading.

2. Port Configuration Administrator Role (Port Configuration): The Port Configuration Administrator Role on the device in FIPS Approved mode is equivalent to the port-config, a port

configuration user in non- FIPS Approved mode. Hence, the Port Configuration Administrator Role has read-and-write access for specific ports but not for global (system-wide) parameters.

3. User Role (Read Only): The User Role on the device in FIPS Approved mode has read-only privileges and no configuration mode access (user).

4. MACsec Peer - A peer device which establishes a MACsec connection with the cryptographic module using AES GCM 128-bit pre-shared key.

5. IKEv2/IPsec Peer role - A peer device which establishes an IPsec tunnel which includes IKEv2 negotiation for key establishment, and subsequent IPsec tunnel for data transport between the IPsec peer.

The User role has read-only access to the cryptographic module while the Crypto Officer Role has access to all device commands. The cryptographic modules do not have a maintenance interface or maintenance role.

Section 7.2 describes the authentication policy for user roles.

6.3 Services

The services available to an operator depend on the operator's role. Unauthenticated operators may view externally visible status LED. LED signals indicate status that allows operators to determine if the network connections are functioning properly. Unauthenticated operators can also perform self-tests via a power-cycle. They can also view the module status by entering CLI "*`fips show`*" command.

For all other services, an operator must authenticate to the device as described in section 7.2 Authentication. The cryptographic modules provide services for remote communication (SSHv2, SNMPv3 and Console) for management and configuration of cryptographic functions. The following subsections describe services available to operators based on role. Each description includes lists of cryptographic functions and critical security parameters (CSP) associated with the service. Table 20 summarizes the available FIPS Approved cryptographic functions.

Table 21 lists cryptographic functions that while not FIPS Approved are allowed in FIPS Approved mode of operation.

Label	**Cryptographic Algorithms**	**Cert.**
AES	[FIPS 197] Advanced Encryption Algorithm Encryption, Decryption, MAC Generate & Verify Modes: ECB(128,192,256 bits)*, CBC(128,192,256 bits), CMAC(128 bits), CFB (128 bits), CTR (128,192,256 bits) and KW(128 bits) *Tested only as a prerequisite for other algorithms.	#5022
AES implemented in IPSec Service Module	[FIPS 197] Advanced Encryption Algorithm Encryption, Decryption, MAC Generate & Verify Modes: ECB(128,256 bits)*, GCM(128,256 bits)	#5074

	*Tested only as a prerequisite for other algorithms.	
AES implemented for MacSec in BCM82756	[FIPS 197] Advanced Encryption Algorithm Encryption, Decryption, MAC Generate & Verify Modes: ECB(128,256 bits)*, GCM(128,256 bits) *Tested only as a prerequisite for other algorithms. Please note that other operations have been tested for AES #4550 but are not used.	#4550
CVL	[SP 800-135] Application Specific Key Derivation Functions IKEv2 KDF, SNMPv3 KDF, SSHv2 KDF Please note that the CAVP and CMVP do not examine this module's implementations of the above protocols.	#1567
CVL	[SP 800-56A] Key Agreement Scheme Function: KAS "All Except KDF" Variants: DH-2048: dhEphem with FC ECDH P-256 and P-384: Ephemeral Unified with EC, ED	#1566
DRBG	[SP 800-90A] Deterministic Random Bit Generators Variants: CTR DRBG with AES-256 (with PR and DF) Please note that HASH DRBG was also tested but was not used.	#1837
DSA	[FIPS 186-4] Digital Signature Algorithm Key Generation* Size: DSA-2048 *DSA-2048 Key Generation was tested only as a prerequisite to Diffie Hellman key exchange (see "DH KA" in the table below). Please note that other operations have been tested but are not used. (Please refer to DSA Cert. #1318 for details.)	#1318
ECDSA	[FIPS 186-4] Elliptic Curve Digital Signature Algorithm Key Generation, Signature Generation, Signature Verification, SigGen Component Test, PKV Curves: P-256, P-384 Hashes: SHA-256 (for P-256), SHA-384 (for P-384)	#1282
HMAC	[FIPS 198-1] Keyed-Hash Message Authentication code MAC Generate & Verify	#3336

	Variants: HMAC-SHA-1 (96, 160-bit tag) HMAC-SHA-256 (128, 192, 256-bit tags) HMAC-SHA-384 (192-bit tag)	
KBKDF	[SP800-108] Key-Based KDF Variant: KDF in Counter Mode, using AES-128-CMAC as PRF	#166
KTS	[SP800-38F §3.1] Functions: Key Wrap, Key Unwrap Variants: AES-128-KW AES-128-CTR and HMAC-SHA-1 AES-256-CTR and HMAC-SHA-1 AES-128-CBC and HMAC-SHA-1 AES-128-CBC and HMAC-SHA-256 AES-256-CBC and HMAC-SHA-1 AES-256-CBC and HMAC-SHA-256	AES #5022, HMAC #3336
RSA	[FIPS 186-4] Rivest Shamir Adleman Signature Algorithm Key Generation, Signature Generation, Signature Verification Sizes: RSA-1024*, RSA-2048 Hashes: SHA-1*, SHA-224, SHA-256, SHA-384, SHA-512 Padding Schemes: X9.31, PKCS 1.5, PSS *RSA-1024 is used for legacy signature verification only. SHA-1 is used for protocol-specific signature generation and legacy signature verification only. Please refer to RSA Cert. #2707 for the exact keysize/hash/padding combinations supported.	#2707
SHA	[FIPS 180-4] Secure Hash Algorithm (SHA-1*, SHA-224, SHA-256, SHA-384, SHA-512) Used for signature operations, as a component of other algorithms (e.g. HMAC, DRBG), password obfuscation, and other purposes *SHA-1 is only used for legacy signature verification, and for protocol-specific signature generation.	#4081

Table 20 – FIPS Approved Cryptographic Algorithms allowed in FIPS Approved mode

Table 21 below lists all FIPS non-Approved Cryptographic Algorithms available in FIPS Approved Mode.

Label	Cryptographic Algorithms
DH KA	Diffie-Hellman with safe primes [L=2048, N=2048] (key agreement; key establishment methodology provides 112 bits of encryption strength) using diffie-hellman-group-exchange-sha256
ECDH	Elliptic Curve Diffie Hellman with P-256 and P-384 (key agreement; key establishment methodology provides between 128 and 192 bits of encryption strength)
KW	RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
MD5	MD5 is used in the Approved mode for three purposes: • RADIUS obfuscated password output during operator authentication (this function is not exposed to the operator) • RADIUS server authenticity check (this function is not exposed to the operator)
NDRNG	Generation of seeds for DRBG with an estimated entropy rate of 6.7 bits per byte and 140 bytes per function call

Table 21 - FIPS non-Approved Cryptographic Algorithms available in FIPS Approved Mode

Table 22 below, lists Roles, FIPS non-Approved Cryptographic Functions, Protocols, and Services only available in non-FIPS Approved Mode

Role	Service / Function	Description
This is not a user accessible service	HTTPS Cipher Suites	Hyper Text Transport Protocol in secure connection mode
Crypto Officer Role, User Role	HTTP	Hyper Text Transport Protocol (plaintext; no cryptography)
Crypto Officer Role, User Role	SSHv2	2-key Triple-DES (non-compliant), 3-key Triple-DES (non-compliant)

Role	Service / Function	Description
Crypto Officer Role, User Role	SNMP { Simple Network Management Protocol v1, v2 and v3 with MD5 / DES, AES (non-compliant) / SHA-1 (non-compliant) }	MD5 and DES, AES (non-compliant) / SHA-1 (non-compliant), SNMPv1, SNMPv2c and SNMPv3 (non-compliant) in noAuthNoPriv, authNoPriv modes Modes: DES in authPriv mode for SNMPV3 (non-compliant) Key sizes: DES 56 bits, AES-128 (non-compliant)
Crypto Officer Role	TFTP (Trivial File Transfer Protocol)	Trivial File Transfer Protocol (TFTP) is a file transfer protocol notable for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment. Compared to FTP, TFTP is extremely limited, providing no authentication, and is rarely used interactively by a user. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
This is not a user accessible service	"Two-way encryption"	Base64
This is not a user accessible service	MD5	Message Digest 5 algorithm is used as cryptographic hash function to check for verification of data integrity and wide variety of cryptographic applications Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	Syslog	Syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	VSRP	Virtual Switch Redundancy Protocol Modes: Layer 2 mode Key sizes: Not Applicable (plaintext; no cryptography)

Role	Service / Function	Description
Crypto Officer Role, User Role	VRRP/VRRP-E	Virtual Router Redundancy Protocol (VRRP) and Virtual Router Redundancy Protocol (VRRP-E) Enhancement Modes: Layer 3 mode Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	MSTP	Multiple Spanning Tree Protocol Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	NTP (Authentication using MD5)	Network Time Protocol Modes: MD5 and SHA-1 (non-compliant) for authentication Key sizes: 20 bytes
Crypto Officer Role, User Role	BGP	Border Gateway Protocol (BGP) is a standardized exterior gateway protocol. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
This is not a user accessible service	AES-192 (non-compliant)	AES-192 (non-compliant) encryption/decryption is only available in non-FIPS mode
This is not a user accessible service	DSA (non-compliant)	DSA (non-compliant) digital signature generation/verification only available in non- FIPS mode

Table 22 - Roles, FIPS non-Approved Cryptographic Functions and Protocols only available in non-FIPS Approved Mode

Note: In addition to Table 22, all algorithms in Tables 20 and 21 are available in the non-Approved mode but are not compliant with the usual applicable standards.

6.4 User Role Services

6.4.1 SSHv2

This service provides a secure session between the cryptographic module and an SSHv2 client using SSHv2 protocol. The cryptographic module authenticates an SSHv2 client and provides an encrypted communication channel. An operator may use an SSHv2 session for managing the device via the command line interface.

The cryptographic modules support three kinds of SSHv2 client authentication: password, client public key and keyboard interactive. For password authentication, an operator attempting to establish an SSHv2 session provides a password through the SSHv2 client. The cryptographic module authenticates operator with passwords stored on the device, on a RADIUS server. Section 7.2 Authentication provides authentication details.

The keyboard interactive (KI) authentication goes one step ahead. It allows multiple challenges to be issued by the cryptographic module, using the backend RADIUS server, to the SSHv2 client. Only after the SSHv2 client responds correctly to the challenges, will the SSHv2 client get authenticated and proper access is given to the cryptographic module.

SSHv2 supports Diffie-Hellman (DH) to configure the modulus size on the SSHv2 server for the purpose of key- exchange.

Maximum number of concurrent SSHv2 user sessions supported is five (5).

The following encryption algorithms are available for negotiation during the key exchange with an SSHv2 client:

- AES-CTR with a 128-bit key (aes128-ctr),
- AES-CTR with a 256-bit key (aes256-ctr),

All secure hashing is done with HMAC-SHA-1.

The following MAC algorithms are available for negotiation during the key exchange with an SSHv2 client: (hmac-sha1) HMAC-SHA1 (digest length = key length = 20 bytes)

In User role access, the client is given access to three (3) commands: *enable*, *exit* and *terminal*. The enable command allows user to re-authenticate using a different role. If the role is the same, based on the credentials given during the *enable* command, the user has access to a small subset of commands that can perform *ping traceroute* in addition to *show* commands.

6.4.2 SNMP

SNMPv1 and SNMPv2 services are disabled in FIPS mode and the SNMPv3 service with authentication as HMAC-MD5 and privacy as DES are also disabled (only HMAC-SHA-1 and AES-CFB are used). The SNMPv3 service within User role allows read-only access to the SNMP MIB within the FastIron device. The device does not provide SNMP MIB access to CSPs when operating in FIPS Approved mode. All other MIB objects are made available for use in approved FIPS mode. These other MIB objects provide capability to monitor the various functional entities in the module which are non-security relevant.

6.4.3 Console

Console connection occurs via a directly connected RS-232 serial cable. Once authenticated as the User, the module provides console commands to display information about a Ruckus cryptographic module and perform basic tasks (such as pings). The User role has read-only privileges and no configuration mode access. The list of commands available is the same as the list mentioned in the SSHv2 service.

6.4.4 NTP

The NTP [same as NTPv4] Network Time Protocol configuration and time statistics details can be viewed but not configured.

6.4.5 IKEv2/IPsec

The User role can read the configuration for this service. This service is described in Section 6.6.6 below.

6.5 Port Configuration Administrator Role Services

6.5.1 SSHv2

This service is described in Section 6.4.1 above.

The Port Configuration Administrator will have seven commands, which allows this user to run show commands, run ping or trace route. The `enable` command allows the user to re-authenticate as described in Section 6.4.1. Within the configuration mode, this role provides access to all the port configuration commands, e.g., all sub-commands within “interface eth 1/1” command. This operator can transfer and store firmware images and configuration files between the network and the system and review the configuration.

6.5.2 SNMP

The SNMP service is not available for a Port Configuration Administrator Role Service.

6.5.3 Console

This service is described in Section 6.4.3 above. Console access as the Port Configuration Administrator provides an operator with the same capabilities as User Console commands plus configuration commands associated with a network port on the device. EXEC commands. The list of commands available is the same as those mentioned in the SSHv2 service.

6.5.4 NTP

The NTP [same as NTPv4] Network Time Protocol configuration and time statistics details can be viewed but not configured.

6.5.5 IKEv2/IPsec

The Port Configuration Administrator role can read the configuration for this service. This service is described in Section 6.6.6 below.

6.6 Crypto Officer Role Services

6.6.1 SSHv2

In addition to the two methods of authentication, password and keyboard interactive, described in Section 6.4.1, SSHv2 service in this role supports RSA public key authentication, in which the device stores a collection of client public keys. Only clients with a private key that corresponds to one of the stored public keys can gain access to the device using SSHv2. After a client presents a public key which matches one of the stored CO SSHv2 public keys, and provides a corresponding signature, the device will give Crypto Officer access to the entire module.

The Crypto Officer can perform configuration changes to the module (including enabling and disabling MACsec on a per-port basis, which configures alternating bypass). This role has full read and write access to the cryptographic module.

When firmware download is desired, the Crypto Officer shall download firmware download in the primary image and secondary image.

The Crypto Officer can perform zeroization by invoking the firmware command "`fips zeroize all`" or session termination.

6.6.2 SCP

This is a secure copy service. The service supports both outbound and inbound copies of configuration, binary images, or files. Binary Images can be copied and installed similar to TFTP operation (that is, upload from device to host and download from host to device, respectively). SCP automatically uses the authentication methods, encryption algorithm, and MAC algorithm configured for SSHv2. For example, if password authentication is enabled for SSHv2, the user is prompted for a user name and password before SCP allows a file to be transferred. One use of SCP on the cryptographic modules is to copy user digital certificates and host public-private key pairs to the device in support of HTTPS. Other use could be to copy configuration to/from the cryptographic module.

6.6.3 SNMP

This service is described in Section 6.4.2 above. The SNMP service within Crypto Officer Role allows read- write access to only Non-Security Relevant elements of the SNMP MIB within the FastIron device.

6.6.4 Console

Logging in through the CLI service is described in Section 6.4.3 above. Console commands provide an authenticated Crypto Officer complete access to all the commands within the cryptographic module. This operator can enable, disable and perform status checks. This operator can also enable any service by configuring the corresponding command. For example, to turn on SSHv2 service, the operator creates a pair of RSA host keys, to configure the authentication scheme for SSHv2 access; afterwards the operator may securely import additional pairs of RSA host keys as needed over a secured SSHv2 connection. To enable the Web Management service, the operator would securely import a pair of RSA host keys and a digital certificate using corresponding commands (over a secured SSHv2 connection) and enable the HTTPS server.

NOTE: The cryptographic module "does not" support DSA key generation in FIPS mode, except as part of Diffie Hellman.

6.6.5 NTP

The NTP [same as NTPv4] Network Time Protocol can be configured to provide cryptographic authentication of messages with the clients/peers, and with its upstream time server. Symmetric key scheme is supported for authentication.

NTPv4 specification (RFC-5905), allows any one of possibly 65,534 message digest keys (excluding zero), each distinguished by a 32-bit key ID, to authenticate an association. The servers and clients involved must agree on the key ID, key type and key to authenticate NTP packets.

NTP service with MD5 key authentication is disabled in FIPS mode.

NTPv4 service with SHA1 key authentication is available upon configuration in FIPS mode. This is not a cryptographic service

6.6.6 IKEv2/IPsec

The Crypto-officer can configure the IKEv2/IPsec service.

The Crypto-officer role on the IPsec supported interface line card, allows IKEv2 and IPsec sessions to be established with a remote peer based on the IKEv2 and IPsec configuration on the device.

1) IKEv2 profile:
    a) Auth profile
        i) Keypair:
            (1) ECDSA P-256, and P-384

    OR

        ii) Pre-shared keys:
            (1) IKEv2 and IPsec PSK
    b) IKE security parameters
        i) The following cipher sequence is supported for IKEv2:
            (1) aes-256-cbc
            (2) aes-128-cbc
    c) IKE proposal
        i) The following key-exchange (KEX) is supported for IKEv2:
            (1) diffie-hellman-group-14
            (2) EC diffie-hellman-group-19
            (3) EC diffie-hellman-group-20
        ii) The following Message Authentication Code (MAC) is used for integrity check:
            (1) HMAC-SHA-256 [128-bit tag]
            (2) HMAC-SHA-384 [192-bit tag]
        iii) The following PRF is supported for IKEv2:
            (1) PRF-HMAC-SHA2-256
            (2) PRF-HMAC-SHA2-384
2) IPsec profile:

a) The following cipher sequence is supported for IPsec:

    i) aes-256-gcm

    ii) aes-128-gcm

6.7 MACsec Peer Role Services

6.7.1 MACsec

Establishes and maintains MACsec sessions with the cryptographic module using AES 128-bit pre-shared keys.

6.8 Services accessible by IKEv2/IPsec Peer role

This section only lists supported services accessible by IKEv2/IPsec Peer role.

6.8.1.1 IKEv2/IPsec

This implicit role is available on the IPsec supported interface line card and allows IKEv2 and IPsec sessions to be established with a remote peer based on the IKEv2 and IPsec configuration on the device.

NOTE: Following protocols relies on the security strength provided by this service:

- L2 Over IPsec

This service is described in Section 6.6.6 above.

7 Policies

7.1 Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the FIPS 140-2 Level 1 security requirements. After configuring a FastIron device to operate in FIPS Approved mode, the Crypto Officer can execute the "fips self-tests" command to perform algorithm self-tests. If an error is detected during the self-test, the module is reloaded once and comes back in the initial non-compliant state. The Crypto Officer has an opportunity to fix the error conditions. Once "fips self-tests" command runs successfully without any error, the Crypto Officer can save the configuration and reload the module. Once the module enters FIPS Approved mode, these self-tests are always executed during POST, even if the module later runs in non-Approved mode.

1) The cryptographic module provides role-based authentication.

2) Until the module is placed in a valid role, the operator does not have access to any Critical Security Parameters (CSPs).

3) The module does not perform MACsec encryption by default. MACsec has to be enabled via configuration. The MACsec configuration can be used to enable Alternating Bypass or full encryption.

4) The AES GCM session key used in the IKEv2/IPSec service is established via the IKEv2 KDF (internally). For Ipsec, the module performs an IKEv2 exchange to derive the Ipsec keys, compliant with RFC 4106, RFC 5282, and RFC 7296. For MACsec, the module is an Authenticator. The link between the Peer and the Authenticator should be secured to prevent the possibility of an attacker to introduce foreign equipment into the local area network.

5) The GCM key and IV are session specific; if the module loses power the implementation is required to renegotiate a new IKE session and thus a new GCM key and IV will be created.

6) The cryptographic module performs the following tests:

    a) Power up Self-Tests:

        i) Cryptographic Known Answer Tests (KAT):

            (1) AES-128,192,256-bit key sizes KAT (encrypt) in CBC, ECB, CTR and CFB modes*

            (2) AES-128,192,256-bit key sizes KAT (decrypt) in CBC, ECB, CTR and CFB modes*

            (3) AES-CMAC KAT*

            (4) AES-KW KAT*

            (5) SHA-1,256,384,512 KAT (Hashing)

            (6) HMAC-SHA-1,256 KAT (Hashing)

            (7) RSA 2048-bit key size KAT (encrypt)

            (8) RSA 2048-bit key size KAT (decrypt)

            (9) RSA 2048-bit key size, SHA-256,384,512 Hash KAT (signature generation)

            (10) RSA 2048-bit key size, SHA-256,384,512 Hash KAT (signature verification)

            (11) DRBG KAT (CTR_DRBG) and Health Tests

            (12) SP800-135 TLS v1.0 KDF KAT (CVL #1567)

            (13) SP800-135 SSHv2 KDF KAT (CVL #1567)

            (14) SP800-135 TLS v1.2 KDF KAT (CVL #1567)

(15) SP800-135 SNMPv3 KDF KAT (CVL #1567)

(16) SP800-108 KBKDF KAT

(17) AES-GCM KATs for IPsec (#5074) and MACsec (#4550)

(18) ECDSA KATs (sign and verify)

(19) Diffie-Hellman KAT (Primitive “Z” computation)

*All AES self-tests are for AES #5022, unless otherwise specified.

ii) Firmware Integrity Test (CRC 32) [run in FIPS mode and non-FIPS mode]

iii) If the module does not detect an error during the Power on Self-Test (POST), at the conclusion of the test, the console displays the message shown below.

```
Crypto module initialization and Known Answer Test (KAT) Passed
```

iv) If the module detects an error during the POST, at the conclusion of the test, the console displays the message shown below. After displaying the failure message, the module reboots.

```
Crypto Module Failed < Reason String >
```

b) Conditional Self-Tests:

i) Continuous Random Number Generator (RNG) test – performed on NDRNG

ii) Continuous Random Number Generator test – performed on DRBG

iii) RSA 2048 SHA-256 Pairwise Consistency Test (Sign/Verify)

iv) RSA 2048 SHA-256 Pairwise Consistency Test (Encrypt/Decrypt)

v) Firmware Load Test: RSA 2048 bit, SHA-256 Signature Verification

vi) Alternating Bypass Test

vii) Manual Key Entry Test: N/A

viii) ECDSA Pairwise Consistency Test (Sign/Verify)

7) At any time, the cryptographic module is in an idle state, the operator can command the module to perform the power-up self-test by executing the “`fips self-tests`” command.

8) Data output to services defined in Section 6.3 Services is inhibited during key generation, self-tests, zeroization, and error states.

9) Status information does not contain CSPs or sensitive data that if used could compromise the module.

10) As per FIPS 140-2 Implementation Guidance D.11, Ruckus hereby states that the following protocols have not been reviewed or tested by the CAVP or CMVP:
    a) TLS v1.0/1.1
    b) SSHv2
    c) TLS v1.2
    d) SNMPv3
    e) IKEv2

11) The module acts as authenticator within the MACsec protocol. The module should only be used together with other CMVP-validated modules to provide a peer to authenticator connection. The link between peer and authenticator should be secured to prevent the possibility for an attacker to introduce foreign equipment into the LAN. The module creates IV’s for MACsec in compliance with IEEE 802.1AE and its applicable amendments.

7.1.1 FIPS Fatal Cryptographic Module Failure

When POST is successful, the following messages will be displayed on the console:

```
FIPS Power On Self Tests and KAT tests successful.
Running continuous DRBG check.
Running continuous DRBG check successful.
Pairwise consistency check successful.
fips crypto drbg health check tests ran successful.

Crypto module initialization and Known Answer Test (KAT) Passed.
```

In order to operate a cryptographic module securely, an operator should be aware of the following rules for FIPS Approved mode of operation:

External communication channels / ports are not available before initialization of the cryptographic module.

The cryptographic module uses a FIPS Approved random number generator, CTR_DRBG.

The cryptographic modules shall use FIPS Approved key generation methods:

1) RSA public and private keys in accordance with [ANSI X9.31]

The cryptographic module tests prime numbers generated for RSA keys using Miller-Rabin test. See [ANSI X9.31]

The cryptographic modules shall use Approved (or allowed) key establishment techniques:

1) Diffie-Hellman

2) RSA Key Wrapping

3) AES Key Wrapping

The cryptographic modules shall restrict key entry and key generation to authenticated roles.

The cryptographic modules shall not display plaintext secret or private keys. The device shall display "…" in place of plaintext keys.

The cryptographic module uses automated methods to establish session keys for SSHv2 and IKEv2. The cryptographic module only performs "get" operations using SNMP.

7.2 Authentication

The cryptographic modules support role-based authentication. A device can perform authentication and authorization (that is, role selection) using RADIUS and local configuration database. Moreover, the cryptographic modules support multiple authentication methods for each service.

New ICX switches that are initially deployed must be accessed using the default local username and password. The default username and password apply to all forms of access. The administrator will be prompted to create a new password after logging in. ICX devices that are already deployed with a previous release and upgraded to FW version 08.0.90a will not be affected by this change. To implement one or more authentication methods for securing access to the device, an operator in the Crypto Officer Role configures authentication-method lists that set the order in which a device consults authentication methods. In an authentication-method list, an operator specifies an access method (Console, SSHv2, Web and SNMP) and the order in which the device tries one or more of the following authentication methods:

1) Line Password Authentication,
2) Enable Password Authentication,
3) Local User Authentication,
4) RADIUS Authentication with exec authorization and command authorization, and
5) Pre-shared keys

When a list is configured, the device attempts the first method listed to provide authentication. If that method is not available, (for example, the device cannot reach a RADIUS server) the device tries the next method until a method in the list is available or all methods have been tried.

The cryptographic modules allow multiple concurrent operators through SSHv2 and the console, only limited by the system resources.

7.2.1 Line Password Authentication Method

The Line Password Authentication method uses the Telnet password to authenticate an operator.

To use Line Password Authentication, a Crypto Officer must set the Telnet password. Please note that when operating in FIPS mode, Telnet is disabled, and Line Password Authentication is not available.

7.2.2 Enable Password Authentication Method

The Enable Password Authentication Method uses a password corresponding to each role to authenticate an operator. An operator must enter the read-only password to select the User role. An operator enters the port-config password to select the Port Configuration Administrator role. An operator enters the super-user password to select the Crypto Officer Role.

To use Enable Password Authentication, a Crypto Officer must set the password for each privilege level.

7.2.3 Local Password Authentication Method

The Local Password Authentication Method uses a password associated with a user name to authenticate an operator. An operator enters a user name and corresponding password. The cryptographic modules assign the role associated with the user name to the operator when authentication is successful.

To use Local Password Authentication, a Crypto Officer must define user accounts. The definition includes a user name, password, and privilege level (which determines role).

7.2.4 RADIUS Authentication Method

The RADIUS Authentication method uses one or more RADIUS servers to verify user names and passwords. The cryptographic modules prompt an operator for user name and password. The device sends the user name and password to the RADIUS server. Upon successful authentication, the RADIUS server returns the operator's privilege level, which determines the operator's role. If a RADIUS server does not respond, the cryptographic module will send the user name and password information to the next configured RADIUS server.

However, while the actual password verification occurs on the RADIUS server, this is still treated as password-based authentication to the module.

The cryptographic modules support additional command authorization with RADIUS Authentication. The following events occur when RADIUS command authorization takes place.

1) A user previously authenticated by a RADIUS server enters a command on the cryptographic module.
2) The cryptographic module looks at its configuration to see if the command is at a privilege level that requires RADIUS command authorization.
3) If the command belongs to a privilege level that requires authorization, the Ruckus cryptographic modules looks at the list of commands returned to it when RADIUS server authenticated the user.

NOTE: After RADIUS authentication takes place, the command list resides on the cryptographic module. The device does not consult the RADIUS server again once the operator has been authenticated. This means that any changes made to the operator's command list on the RADIUS server are not reflected until the next time the RADIUS server authenticates the operator, and the server sends a new command list to the cryptographic module.

To use RADIUS authentication, a Crypto Officer must configure RADIUS server settings along with authentication and authorization settings.

7.2.5 Strength of Authentication

This section describes the strength of each authentication method.

7.2.5.1 IKEv2/IPsec Peer Role

Knowledge of strength of IKEv2 ECDSA Private Key:

> When configuring the smallest curve P-256, the probability that a random attempt will succeed, or a false acceptance will occur is 1/2^128, which is less than 1/1,000,000.
>
> 256 attempts are allowed in a one-minute period. Therefore, the probability of a random success in a one-minute period is 256/2^128, which is less than 1/100,000.

Knowledge of strength of IKEv2 Pre-Shared Key (PSK):

> The IKEv2 Pre-Shared Key is a 112-bit HMAC Key, the probability that a random attempt will succeed, or a false acceptance will occur is 1/2^112, which is less than 1/1,000,000.
>
> 256 attempts are allowed in a one-minute period. Therefore, the probability of a random success in a one-minute period is 256/2^112, which is less than 1/100,000.

7.2.5.2 MACsec Peer Role (only)

The MACsec Peer Role is assumed implicitly as follows:

Specifically, in reference to MACsec Peer Role only, the probability of a successful random guess of the AES 128-bit pre-shared key is 1/ 2^128 for a random attempt, which is less than 1/1,000,000. The module only supports a maximum of 60 attempts during a one-minute period due to the timing of the protocol. This means that the probability of false authorization with multiple consecutive random attempts during a one-minute period is 60 / 2^128, which is less than 1/100,000.

7.2.5.3 All other roles (except MACsec & IPSec/IKEv2 Peer Role)

All other users except for the MACsec Peer Role can utilize all other available authentication techniques for the purpose of authentication.

The cryptographic modules minimize the likelihood that a random authentication attempt will succeed. The module supports minimum eight (8) character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore, the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000. The minimum length also applies to the RADIUS secret.

The module enforces a one second delay for each attempted password verification, therefore maximum of 60 attempts per minute, thus the probability of multiple consecutive attempts within a one-minute period is 60/80^8 which is less than 1/100,000.

The probability of a successful random guess of a RADIUS password during a one-minute period is less than three (3) in 1,000,000 which is less than 1/100,000 as the authentication message needs to go to the server from the switch and then the response needs to come back to the switch.

For the SNMPv3 secret used for authentication, the module supports minimum eight (8) character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore, the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000.

The module can process one (1) authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one-minute period is 6000/80^8 which is less than 1/100,000.

For the SNMPv3 secret used for privacy, the module supports minimum 12-character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore, the probability of a random attempt is 1/ 80^12 which is less than 1/1,000,000.

The module can process one (1) authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one-minute period is 6000/80^12 which is less than 1/100,000.

For the NTP secret, the module supports minimum eight (8) character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore, the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000.

The module can process one (1) authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one-minute period is 6000/80^8 which is less than 1/100,000.

7.2.6 Pre-shared keys Method

The MACsec Peer role establishes and maintains MACsec sessions using AES 128-bit pre-shared keys that are configured by the Crypto Officer.

Access Control Policy and CSP & Public Key access Table 23 and Table 24 summarize the access operators in each role have to critical security parameters. The table entries have the following meanings:

1) r – Operator can read the value of the item,
2) w - Operator can write a new value for the item,
3) x - Operator can use the value of the item without direct access (for example encrypt with an encryption key)
4) d - Operator can delete the value of the item (zeroize).

Roles & Services / CSPs & Public Keys	User Role					Port Configuration Administrator					Crypto Officer Role					
	SSHv2	SNMP	Console	NTP	IKEv2/IPsec	SSHv2	SNMP	Console	NTP	IKEv2/IPSec	SSHv2	SCP	SNMP	Console	NTP	IKEv2/IPSec
SSHv2 Host RSA Private Key (2048 bit)	x					x					xwd	x		wd		
SSHv2 DH Private Key (2048 bit)	x					x					xwd	x		wd		
SSHv2 DH Shared Secret Key (2048 bit)	x					x					wxd	x		wxd		
SSHv2/SCP Session Keys (128 and 256 bit AES-CTR)	x					x					wxd	x		wxd		
SSHv2/SCP Authentication Key (160-bits HMAC-SHA-1)	x					x					wxd	x		wxd		
SSHv2 KDF Internal State	x					x					wxd	x		wxd		
DRBG Entropy Input	x				x	x				x	wxd	x		wxd		x
CTR_DRBG Internal State	x	x	x		x	x	x	x		x	wxd	x	x	X		x
User Password	x	x	x								xrwd	xrwd		xrwd		
Port Administrator Password						x	x	x			xrwd	xrwd		xrwd		

Roles & Services CSPs & Public Keys	User Role					Port Configuration Administrator					Crypto Officer Role					
	SSHv2	SNMP	Console	NTP	IKEv2/IPsec	SSHv2	SNMP	Console	NTP	IKEv2/IPSec	SSHv2	SCP	SNMP	Console	NTP	IKEv2/IPSec
Crypto Officer Password											xrwd	xrwd	x	xrwd		
RADIUS Secret	x		x		x	x		x		x	xrwd	xrwd		xrwd		x
IKEv2 ECDSA Private Key (P-256)											rwd			wd		wd
IKEv2 ECDSA Private Key (P-384)											rwd			wd		wd
IKEv2 Pre-Shared Key (PSK)											rwd			rwd		wd
IKEv2 RSA Private Key											rwd			wd		wd
PKI SCEP Enrollment RSA 2048-bit Private Key											d			d		
(All other IKE & IPsec keys, see Appendix A)											d			d		
SNMPv3 secret	r	rx	r			r	r	r			rwd	rwd	r	rwd		rwd
NTP secret	r			r	r	r		r	rx		rwd	rwd	r	rw	rwd	
CAK											rwd	rwd		rwd		
CKN											rwd	rwd		rwd		
ICK											d			d		
KEK											d			d		
SAK											dx			dx		
SP800-108 KDF Internal State											rwd			rwd		
Firmware Integrity / Firmware Load RSA Public Key											x					
SSHv2 Host RSA Public key	rx				x	rx					xrwd	xrw		rwd		
SSHv2 Client RSA Public Key	rx				x	rx					xrwd	xrwd		xrwd		

Roles & Services	User Role					Port Configuration Administrator					Crypto Officer Role					
CSPs & Public Keys	SSHv2	SNMP	Console	NTP	IKEv2/IPsec	SSHv2	SNMP	Console	NTP	IKEv2/IPSec	SSHv2	SCP	SNMP	Console	NTP	IKEv2/IPSec
SSHv2 DH Public Key	rx				x	rx			xd	x	xrwd					
SSHv2 DH Peer Public Key	wx				x	wx			xd	x	xrwd					
IKEv2 DH Public Key											d					rwd
IKEv2 ECDH Public Key (P-256)											d					rwd
IKEv2 ECDH Public Key (P-384)											d					rwd
IKEv2 ECDSA Public Key (P-256)											d			rwd		rwd
IKEv2 ECDSA Public Key (P-384)											d			rwd		rwd
IKEv2 RSA Public Key											d			rwd		rwd
PKI SCEP Enrollment RSA Public Key											d			rwd		rwd

Table 23 - Access Control Policy and CSP & Public Key access

Service / CSPs	MACsec Service
CAK	xd

CKN	xd
ICK	xd
KEK	xd
SAK	rwxd
SP800-108 KDF Internal State	xd

Table 24 - Access Control Policy and CSP access for MACsec Peer role

7.2.6.1 Access Control and Critical Security Parameters (CSPs) for IKEv2/IPsec Peer role

Access control and CSPs for IKEv2/IPsec Peer role is shown in table below:

Service CSPs & Public Keys	IKEv2/IPsec
DRBG Entropy Input	xd
CTR_DRBG Internal State	xd
IKEv2/IPsec Authentication Key	xwd
IKEv2 KDF State	xwd
IKEv2 DH Group-14 Private Key 2048-bit MODP	xwd
IKEv2 ECDH Group-19 Private Key (P-256)	xwd
IKEv2 ECDH Group-20 Private Key (P-384)	xwd
IKEv2 ECDSA Private Key (P-256)	xd
IKEv2 ECDSA Private Key (P-384)	xd
PKI SCEP Enrollment RSA 2048-bit Private Key	xwd
IKEv2 Encrypt/Decrypt Key	xwd
IPsec ESP Encrypt/Decrypt Key	xwd
IKEv2 DH Group-14 Shared Secret 2048-bit MODP	xwd
IKEv2 ECDH Group-19 Shared Secret (P-256)	xwd
IKEv2 ECDH Group-20 Shared Secret (P-384)	xwd
IKEv2 Pre-Shared Key (PSK)	xd
IKEv2 RSA Private Key	xwd
IKEv2 DH Group-14 Public Key 2048-bit MODP	xwd
IKEv2 ECDH Group-19 Public Key (P-256)	xwd
IKEv2 ECDH Group-20 Public Key (P-384)	xwd

Service CSPs & Public Keys	IKEv2/IPsec
IKEv2 ECDSA Public Key (P-256)	xd
IKEv2 ECDSA Public Key (P-384)	xd
IKEv2 RSA Public Key	xwd
PKI SCEP Enrollment RSA 2048-bit Public Key	xwd

Table 25 - Access Control and CSPs for the IKEv2/IPsec Peer role

7.2.7 CSP Zeroization

All CSPs can be zeroized by executing the “`fips zeroize all`” command. This command can be executed via the Console and SSHv2 service.

8 Description of FIPS Approved Mode

This section describes:

A. FIPS Approved mode, Section 8.1, describes:
   - This section describes required actions before you can use the module in FIPS Approved mode of operation
   - The nature of operational conditions in the module while operating in FIPS Approved mode.

B. Displaying mode status, Section 8.2, provides details on how to examine the status for the module's mode of operation.

C. Invoking FIPS Approved mode, Section 8.3, describes the required steps in order to invoke the FIPS Approved mode on the module.

8.1 FIPS Approved Mode

This section describes FIPS Approved mode of operation and the sequence of actions that places a Ruckus cryptographic module in FIPS Approved mode.

FIPS Approved mode disables the following:

1) Telnet access including the telnet server command
2) Command `ip ssh scp disable`
3) TFTP access
4) SNMP access to CSP MIB objects
5) Access to all commands within the monitor mode
6) Port 280

Entering FIPS Approved mode also clears:

1) Protocol shared secret and host passwords
2) SSHv2 RSA host keys

FIPS Approved mode enables:

1) SCP

8.2 Displaying Mode Status

The cryptographic modules provide the `fips show` command to display status information about the device's FIPS mode. This command displays information about the policy settings. This information includes the status of administrative commands for security policy, the status of security policy enforcement and security policy settings.

The `fips enable` command changes the status of administrative commands; see also Section 8.1, FIPS Approved Mode.

The following example shows the output of the `fips show` command before an operator enters the `fips enable` command. Displayed status information indicates that administrative commands for security policy are unavailable (Administrative Status is OFF) and the device is not enforcing a security policy (Operational Status is OFF).

```
FIPS mode: Administrative Status: OFF, Operational Status: OFF
```

The following example shows the output of the `fips show` command after an operator enters the `fips enable` command. Displayed status information indicates that administrative commands for security policy are available (Administrative Status is ON) but the device is not enforcing a security policy yet (Operational Status is OFF).

```
FIPS mode: Administrative Status: ON, Operational Status: OFF
Some shared secrets inherited from non-Approved mode may not be fips
compliant and has to be zeroized. The system needs to be reloaded to operate
in FIPS mode.
System Specific:
OS monitor mode access: Disabled
Management Protocol Specific:
Telnet server: Disabled
TFTP Client: Disabled
HTTPS SSL 3.0: Disabled
SNMP Access to security objects: Disabled
Critical Security Parameter Updates across FIPS Boundary:
Protocol shared secret and host passwords: Clear
SSHv2 RSA Host Keys: Clear
```

The following example shows the output of the `fips show` command after the device reloads successfully in the default strict FIPS mode. Displayed status information indicates that administrative commands for security policy are available (Administrative Status is ON) and the device is enforcing a security policy (Operational Status is ON).

```
FIPS mode: Administrative Status: ON, Operational Status: ON
System Specific:
OS monitor mode access: Disabled
Management Protocol Specific:
Telnet server: Disabled
TFTP Client: Disabled
HTTPS SSL 3.0: Disabled
SNMP Access to security objects: Disabled
Critical Security Parameter Updates across FIPS Boundary:
Protocol shared secret and host passwords:    Clear
SSHv2 RSA Host Keys: Clear
```

8.3 Invoking FIPS Approved Mode

Crypto Officer may use “FastIron FIPS and Common Criteria Configuration Guide” documentation on ruckuswireless.com for configuration of these devices.

To invoke the FIPS Approved mode of operation, perform the following steps:

1) Assume Crypto Officer role.

2) Enter command: `fips enable`

   The device enables FIPS administrative commands. The device is not in FIPS Approved Mode of operation yet. Do not change the default strict FIPS security policy, which is required for FIPS Approved mode.

3) Enter command: `fips zeroize all`
   The device zeros out the shared secrets used by various networking protocols including host access passwords, SSHv2 host keys, and HTTPS host keys with the digital signature. This will delete all the users.

4) Enter command: `no web-management hp-top-tools`

   The device will turn off access by HP ProCurve Manager via port 280.

5) Generate the SSHv2 Host RSA Private Key (2048 bit) and SSHv2 Host RSA Public Key.

   a) Use CLI command: `crypto key generate`

6) Copy signature files of all the affected images to the flash memory.

   a) Use CLI command: `copy scp <syntax>`

7) Create a new user

   a) Use user command: `user <username> password <password>`

8) Enter command: `write memory`.

   The device saves the running configuration as the startup configuration.

9) Enter command: `reload`

   The device resets and begins operation in FIPS Approved mode.
   (**NOTE**: Do not press B as the module is reloading).

10) Enter command: `fips show` (This command displays the FIPS-related status, which should confirm the security policy is the default security policy.)

9 Glossary

Term/Acronym	Description
AES	Advanced Encryption Standard
CBC	Cipher-Block Chaining
CLI	Command Line Interface
CSP	Critical Security Parameter
DES	Data Encryption Standard
DF	Derivation Function (for SP800-90A DRBG)
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook mode
FI	FastIron
GbE	Gigabit Ethernet
GCM	Galois/Counter Mode symmetric key cryptographic
GMAC	Galois Message Authentication Code (GMAC): an authentication-only variant of the GCM
HMAC	Keyed-Hash Message Authentication Code
KDF	Key Derivation Function
LED	Light-Emitting Diode
MACsec	MAC Security standard
Mbps	Megabits per second
NDRNG	Non-Deterministic Random Number Generator
POE	Power over Ethernet
POE+	High Power over Ethernet
PR	Prediction Resistance (for SP800-90A DRBG)
RADIUS	Remote Authentication Dial in User Service
RSA	Rivest Shamir Adleman
SCP	Secure Copy
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSHv2	Secure Shell
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security

Table 26 - Glossary

10 References

[FIPS 186-2+] Federal Information Processing Standards Publication 186-2 (+Change Notice), Digital Signature Standard (DSS), 27 January 2000

[FIPS 186-4] Digital Signature Standard (DSS), July 2013

[RSA PKCS #1] PKCS #1: RSA Cryptography Specifications Version 2.1

[SP800-90A Rev.1] National Institute of Standards and Technology Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), June 2015

11 Appendix A: Critical Security Parameters

The module supports the following CSPs and public keys:

11.1 SSHv2 & SCP

1. SSHv2 Host RSA Private Key (2048 bit)
   - Description: Used to authenticate SSHv2 server to client
   - Type: RSA-2048 Private Key
   - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
   - Establishment: N/A
   - Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Output: N/A
   - Storage: Plaintext in RAM and BER encoded (plaintext) in Compact Flash
   - Key-to-Entity: Process
   - Zeroization: "fips zeroize all" command

2. SSHv2 DH Private Key (2048 bit)
   - Description: Used in SCP and SSHv2 to establish a shared secret
   - Type: DH-2048 Private Key
   - Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Establishment: N/A
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: Process
   - Zeroization: Session termination and "fips zeroize all" command

3. SSHv2 DH Shared Secret Key (2048 bit)
   - Description: Output from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.
   - Type: DH Shared Secret
   - Generation: N/A
   - Establishment: SSHv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User
   - Zeroization: Session termination and "fips zeroize all" command

4. SSHv2/SCP Session Keys (128 and 256 bit AES-CTR)
   - Description: AES encryption key used to secure SSHv2/SCP
   - Type: AES-128-CTR or AES-256-CTR Key

- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

5. SSHv2/SCP Authentication Key (160 bits HMAC-SHA-1)
   - Description: Session authentication key used to authenticate and provide integrity of SSHv2 session
   - Type: HMAC-SHA-1
   - Generation: N/A
   - Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User
   - Zeroization: Session termination and "fips zeroize all" command

6. SSHv2 KDF Internal State
   - Description: Used to generate Host encryption and authentication key
   - Type: KDF
   - Generation: N/A
   - Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User
   - Zeroization: Session termination and "fips zeroize all" command

11.2 Random Number Generation

7. DRBG Entropy Input
   - Description: Entropy Input for the SP800-90A CTR_DRBG
   - Type: DRBG Seed material
   - Generation: internally generated; raw random data from NDRNG
   - Establishment: N/A
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: Process
   - Zeroization: Power cycle and "fips zeroize all" command

8. DRBG Internal States

- Description: Internal State of SP800-90A CTR_DRBG (V and Key)
- Type: SP800-90A DRBG State
- Generation: SP800-90A DRBG State modification (instantiate, generate, etc.)
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: Power cycle and "fips zeroize all" command

11.3 Passwords & Related Secrets

9. User Password
    - Description: Password used to authenticate User (8 to 48 characters)
    - Type: Authentication data
    - Generation: N/A
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session
    - Storage: MD5 digest in plaintext in Compact Flash
    - Key-to-Entity: User
    - Zeroization: "fips zeroize all" command

10. Port Administrator Password
    - Description: Password used to authenticate Port Configuration Administrator (8 to 48 characters)
    - Type: Authentication data
    - Generation: N/A
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session
    - Storage: MD5 digest in plaintext in Compact Flash
    - Key-to-Entity: User
    - Zeroization: "fips zeroize all" command

11. Crypto Officer Password
    - Description: Password used to authenticate Crypto Officer (8 to 48 characters)
    - Type: Authentication data
    - Generation: N/A
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session
    - Storage: MD5 digest in plaintext in Compact Flash
    - Key-to-Entity: User
    - Zeroization: "fips zeroize all" command

12. RADIUS Secret
    - Description: Used to authenticate the RADIUS server (8 to 64 characters)
    - Type: Authentication data
    - Generation: N/A
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session
    - Storage: Plaintext in RAM, Ruckus proprietary two-way encrypted using base-64 (plaintext) in RAM and Compact Flash
    - Key-to-Entity: Process
    - Zeroization: "fips zeroize all" command

11.4 IKEv2 and IPsec

13. IKEv2/IPSec Authentication Key
    - Description: Authentication
    - Type: 256 bits or 384 bits HMAC
    - Establishment: IKEv2 KDF as per SP800-135 Section 4.1.1; allowed method as per FIPS 140-2 IG D.8 Scenario 4
    - Entry: N/A
    - Output: N/A
    - Storage: Encrypted in RAM
    - Key-to-Entity: IKEv2 SPI
    - Zeroization: Session termination and "fips zeroize all" command

14. IKEv2 KDF State
    - Description: IKEv2 KDF State
    - Type: HMAC-SHA-256 and HMAC-SHA-384
    - Generation: N/A
    - Establishment: IKEv2 KDF as per SP800-135 Section 4.1.1; allowed method as per FIPS 140-2 IG D.8 Scenario 4
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: IKEv2 SPI
    - Zeroization: Handshake completion and "fips zeroize all" command

15. IKEv2 ECDH Group-19 Private Key (P-256)
    - Description: ECDH private key
    - Type: ECDH
    - Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG; this is Approved as per SP800-56A
    - Establishment: N/A
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: IKEv2 SPI

- Zeroization: "fips zeroize all" command

16. IKEv2 ECDH Group-20 Private Key (P-384)
    - Description: ECDH private key
    - Type: ECDH
    - Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG; this is Approved as per SP800-56A
    - Establishment: N/A
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: IKEv2 SPI
    - Zeroization: "fips zeroize all" command

17. IKEv2 ECDSA Private Key (P-256)
    - Description: Private Key
    - Type: ECDSA
    - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
    - Establishment: N/A
    - Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Storage: Local persistent on MM
    - Key-to-Entity: IKEv2/IPsec Peer role
    - Zeroization: "fips zeroize all" command

18. IKEv2 ECDSA Private Key (P-384)
    - Description: Private Key
    - Type: ECDSA
    - Generation: - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
    - Establishment: N/A
    - Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Storage: Local persistent on MM
    - Key-to-Entity: IKEv2/IPsec Peer role
    - Zeroization: "fips zeroize all" command

19. PKI SCEP Enrollment RSA 2048-bit Private Key
    - Description: One-time key: SCEP protocol signing. Generated during certificate enrollment
    - Type: RSA key pair
    - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method

- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Temporarily stored in memory not Flash
- Key-to-Entity: IKEv2/IPsec Peer role
- Zeroization: Key is destroyed/zeroized as soon as the SCEP enrollment is complete.

20. IKEv2 Encrypt/Decrypt Key
    - Description: Encryption/Decryption only used for IKEv2 control packets
    - Type: AES-128-CBC and AES-256-CBC
    - Generation: N/A
    - Establishment: IKEv2 KDF as per SP800-135 Section 4.1.1; allowed method as per FIPS 140-2 IG D.8 Scenario 4
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: IKEv2 SPI
    - Zeroization: "fips zeroize all" command

21. IPsec ESP Encrypt/Decrypt Key
    - Description: Encryption and Decryption used for IPsec encapsulated data packets
    - Type: AES-128-GCM and AES-256-GCM
    - Generation: N/A
    - Establishment: IKEv2 KDF as per SP800-135 Section 4.1.1; allowed method as per FIPS 140-2 IG D.8 Scenario 4
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: IPsec SPI
    - Zeroization: "fips zeroize all" command

22. IKEv2 DH Group-14 Shared Secret 2048-bits MODP
    - Description: DH shared secret
    - Type: DH
    - Generation: N/A
    - Establishment: IKEv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: IKEv2 SPI
    - Zeroization: "fips zeroize all" command or when the session is deleted.

23. IKEv2 ECDH Group-19 Shared Secret (P-256)
    - Description: ECDH shared secret
    - Type: ECDH
    - Generation: N/A

- Establishment: IKEv2 ECDH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: IKEv2 SPI
- Zeroization: "fips zeroize all" command or when the session is deleted.

24. IKEv2 ECDH Group-20 Shared Secret (P-384)
    - Description: ECDH shared secret
    - Type: ECDH
    - Generation: N/A
    - Establishment: IKEv2 ECDH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: IKEv2 SPI
    - Zeroization: "fips zeroize all" command or when the session is deleted.

25. IKEv2 Pre-Shared Key (PSK)
    - Description: Pre-Shared Key;
    - Type: KDF
    - Generation: N/A
    - Establishment: N/A
    - Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Storage: Plaintext in RAM
    - Key-to-Entity: IKEv2 SPI
    - Zeroization: "fips zeroize all" command

26. IKEv2 RSA Private Key
    - Description: Private Key
    - Type: RSA key pair
    - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
    - Establishment: N/A
    - Entry: Key transport: AES Encrypted & HMAC-SHA-2 authenticated over IKEv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Output: Key transport: AES Encrypted & HMAC-SHA-2 authenticated over IKEv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Storage: Local persistent on MM
    - Key-to-Entity: IKEv2/IPsec Peer role
    - Zeroization: Key is destroyed/zeroized as soon as the SCEP enrollment is complete.

27. IKEv2 DH Group-14 Private Key 2048-bit MODP

- Description: DH private key
- Type: DH
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is Approved as per SP800-56A
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in memory
- Key-to-Entity: IKEv2 SPI
- Zeroization: "fips zeroize all" command

11.5 Miscellaneous

28. SNMPv3 secret
    - Description: Used for authentication (SHA1, Password is 8 to 16 characters long) and for privacy (AES-CFB 128-bit, Password 12 to 20 characters)
    - Type: Authentication data and privacy
    - Generation: N/A - generated outside of the module
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: SHA1 hashed in configuration, output encrypted / authenticated over SSHv2 session
    - Storage: SHA1 digest and AES are stored in Compact Flash
    - Key-to-Entity: Process: User
    - Zeroization: Session termination and "fips zeroize all" command

29. NTP secret
    - Description: Authentication (SHA1, Password is 8 to 16 characters long)
    - Type: Authentication data
    - Generation: N/A - generated outside of the module
    - Establishment: N/A
    - Entry: Configured by the operator, entered authenticated over SSHv2 session
    - Output: SHA1 hashed in configuration, output authenticated over SSHv2 session
    - Storage: SHA1 digest is stored in Compact Flash
    - Key-to-Entity: Process: User
    - Zeroization: Session termination and "fips zeroize all" command

30. CAK
    - Description: Connectivity association key - main master key; Pre-shared key; 128 bits in length
    - Type: KDF Input
    - Generation: N/A - generated outside of the module
    - Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1

- Storage: Plaintext in configuration file (Flash); Save configuration
- Key-to-Entity: Process: MKA
- Zeroization: Session termination and "fips zeroize all" command

31. CKN
    - Description: Connectivity key name; pre-shared key; 128-bits in length)
    - Type: KDF input
    - Generation: N/A - generated outside of the module
    - Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Storage: Plaintext in configuration file (Flash); Save configuration
    - Key-to-Entity: Process: MKA
    - Zeroization: Session termination and "fips zeroize all" command

32. ICK
    - Description: Integrity checksum key; 128-bits. This is the ICV key used to verify the integrity of MKPDUs
    - Type: AES CMAC 128
    - Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF
    - Establishment: N/A
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: Process: MKA
    - Zeroization: Session termination and "fips zeroize all" command

33. KEK
    - Description: Key encryption key; 128-bits
    - Type: AES Key Wrap
    - Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF
    - Establishment: N/A
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: Process: MKA
    - Zeroization: Session termination and "fips zeroize all" command

34. SAK
    - Description: Secure association key; 128-bits
    - Type: GCM Key
    - Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF
    - Establishment: Key transport: AES Encrypted with the KEK (KTS)
    - Entry: Input AES encrypted by the KEK

- Output: Output AES encrypted by the KEK
- Storage: Plaintext in RAM and Plaintext in Marvell chip
- Key-to-Entity: Process: MACsec
- Zeroization: Session termination and "fips zeroize all" command

35. SP800-108 KDF Internal State
    - Description: SP800-108 KDF
    - Type: SP800-108 (AES 128 CMAC in Counter Mode)
    - Generation: SP800-108 KDF
    - Establishment: N/A
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: Process: MKA
    - Zeroization: Session termination and "fips zeroize all" command

12 Public Keys

12.1 Firmware

1. Firmware Integrity / Firmware Load RSA Public Key
   - Description: RSA 2048-bit public key used to verify signature of firmware of the module
   - Type: RSA Public Key
   - Generation: N/A, Generated outside the module
   - Establishment: N/A
   - Entry: Through firmware update
   - Output: N/A
   - Storage: Plaintext in RAM, Plaintext in Compact Flash
   - Key-to-Entity: Process

12.2 SSHv2

2. SSHv2 Host RSA Public Key
   - Description: (2048-bit); Used to establish shared secrets
   - Type: RSA Public Key
   - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
   - Establishment: N/A
   - Entry: Configured by the operator; Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Output: Plaintext
   - Storage: Plaintext in RAM, Plaintext in Compact Flash
   - Key-to-Entity: Process

3. SSHv2 Client RSA Public Key
   - Description: (2048-bit); Used to establish shared secrets
   - Type: RSA Public Key
   - Generation: N/A, generated outside the module
   - Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Entry: Configured by the operator; Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Output: N/A
   - Storage: Plaintext in RAM, Plaintext in Compact Flash
   - Key-to-Entity: Process

4. SSHv2 DH Public Key
   - Description: (2048-bit modulus); Used to establish shared secrets (SSHv2 and DHCHAP)
   - Type: DH Public Key
   - Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Establishment: N/A
   - Entry: N/A

- Output: Plaintext
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

5. SSHv2 DH Peer Public Key
   - Description: (2048-bit modulus); Used to establish shared secrets (SSHv2 and DHCHAP)
   - Type: DH Peer Public Key
   - Generation: N/A
   - Establishment: N/A
   - Entry: Plaintext
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: Process

12.3 IKEv2 and IPsec

6. IKEv2 DH Group-14 Public Key 2048-bit MODP
   - Description: DH public key
   - Type: DH
   - Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is Approved as per SP800-56A
   - Establishment: N/A
   - Entry: N/A
   - Output: Plaintext
   - Storage: Plaintext in RAM
   - Key-to-Entity: IKEv2 SPI

7. IKEv2 ECDH Group-19 Public Key (P-256)
   - Description: ECDH public key
   - Type: ECDH
   - Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG; this is Approved as per SP800-56A
   - Establishment: N/A
   - Entry: N/A
   - Output: Plaintext
   - Storage: Plaintext in RAM
   - Key-to-Entity: IKEv2 SPI

8. IKEv2 ECDH Group-20 Public Key (P-384)
   - Description: ECDH public key
   - Type: ECDH
   - Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the SP800-90A DRBG; this is Approved as per SP800-56A
   - Establishment: N/A
   - Entry: N/A

- Output: Plaintext
- Storage: Plaintext in RAM
- Key-to-Entity: IKEv2 SPI

9. IKEv2 ECDSA Public Key (P-256)
    - Description: Public Key
    - Type: ECDSA
    - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
    - Establishment: N/A
    - Entry: Key transport: AES Encrypted & HMAC-SHA-2 authenticated over IKEv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Output: Key transport: AES Encrypted & HMAC-SHA-2 authenticated over IKEv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Storage: Plaintext in RAM, Plaintext in Compact Flash
    - Key-to-Entity: IKEv2/IPsec Peer role

10. IKEv2 ECDSA Public Key (P-384)
    - Description: Public Key
    - Type: ECDSA
    - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
    - Establishment: N/A
    - Entry: Key transport: AES Encrypted & HMAC-SHA-2 authenticated over IKEv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Output: Key transport: AES Encrypted & HMAC-SHA-2 authenticated over IKEv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Storage: Plaintext in RAM, Plaintext in Compact Flash
    - Key-to-Entity: IKEv2/IPsec Peer role

11. IKEv2 RSA Public Key
    - Description: (2048 bit); Used to establish shared secrets
    - Type: RSA Public Key
    - Generation: -As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
    - Establishment: N/A
    - Entry: Key transport: AES Encrypted & HMAC-SHA-2 authenticated over IKEv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Output: Key transport: AES Encrypted & HMAC-SHA-2 authenticated over IKEv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
    - Storage: Plaintext in RAM, Plaintext in Compact Flash
    - Key-to-Entity: IKEv2/IPsec Peer role
    - Zeroization: "fips zeroize all" command

12. PKI SCEP Enrollment RSA 2048-bit Public Key
    - Description: One-time key: SCEP protocol signing. Generated during certificate enrollment
    - Type: RSA key pair

- Generation: -As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Temporarily stored in memory not Flash
- Key-to-Entity: IKEv2/IPsec Peer role