Recently acquired by Aruba,
a Hewlett Packard Enterprise company

Silver Peak Systems, Inc.

Silver Peak EdgeConnect

running Firmware versions

ECOS 8.1.9 and ECOS 9.1.0

FIPS 140-2 Level 1 Non-Proprietary Security Policy

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 1 of 46

Non-Proprietary

Contents

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 2 of 46

Non-Proprietary

Figures

Tables

Document Revision History

Version	Date	Author	Description
1.0	February 2022	Silver Peak Systems, Inc.	Initial Release
1.1	December 2022	Silver Peak Systems, Inc.	Updates for NIST CMVP review comments
1.2	February 2023	Silver Peak Systems, Inc.	Updates for NIST CMVP review comments
1.3	June 2023	Silver Peak Systems, Inc.	Updates for NIST CMVP review comments

Aruba, a Hewlett Packard Enterprise company, acquired Silver Peak Systems, Inc. in 2020.
For more details see HPE Completes Acquisition of SD-WAN Leader Silver Peak.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 3 of 46

Non-Proprietary

1 Purpose of this Document

This security policy provides information regarding the FIPS 140-2 Level 1 validation of Silver Peak EdgeConnect (also referred to as EdgeConnect in the remainder of this document) running firmware versions ECOS 8.1.8 and ECOS 9.1.0. The module type is firmware only. This document is non-proprietary and describes how EdgeConnect hardware and virtual appliances running ECOS firmware releases ECOS 8.1.9 and ECOS 9.1.0 meet the security requirements of FIPS 140-2 Level 1, and how to place and maintain the appliances with ECOS Firmware in the secure FIPS 140-2 mode.

This policy was prepared as part of the FIPS 140-2 Level 1 validation of the product.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) website at: https://csrc.nist.gov/projects/cryptographic-module-validation-program

2 Overview

Silver Peak's EdgeConnect Platform includes a set of hardware and virtual appliances that are optimized for a range of enterprise branch-office, headquarters, and data center applications. They deliver predictable application performance over any combination of transport services, providing a virtual network overlay that aligns enterprise application performance requirements with underlying network resources. EdgeConnect SD-WAN includes features such as Business Intent Overlays, network segmentation, security services, analytics, and reporting. Orchestrated, application-driven security policies direct enterprise traffic to internal subnets over the optimized SD-WAN fabric, internet breakout for trusted SaaS service, and 3rd party network services such as cloud-hosted security services or public clouds offering Infrastructure as a Service (IaaS).
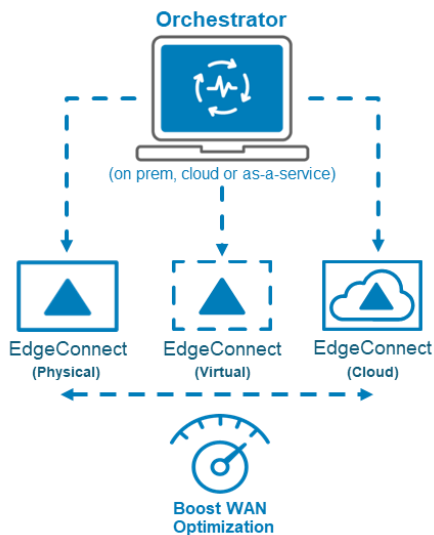
Boost™ is an optional performance pack that combines Silver Peak WAN optimization technology to create a high-performance SD-WAN solution, allowing companies to accelerate performance of latency-sensitive applications and minimize transmission of repetitive data across the WAN in a single, fully integrated SD-WAN solution. Boost™ is an optional feature that does not impact the module's FIPS validation.

EdgeConnect OS (ECOS) Firmware can be either deployed on an x86-based hardware appliance or on a hypervisor as a virtual appliance.

Note that Orchestrator and Cloud Portal are out of scope of this validation.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 4 of 46

Non-Proprietary

2.1 Validated EdgeConnect OS (ECOS) Firmware with EdgeConnect Hardware and Virtual Appliances

The module type is firmware only. The validated EdgeConnect OS (ECOS) Firmware versions:

EdgeConnect OS (ECOS) Versions
8.1.9, 9.1.0

The tested platforms consisted of the EdgeConnect hardware and virtual appliances:

EdgeConnect Hardware and Virtual Appliances	ECOS Versions	Operating Systems	CPU Information
EC-XS	• 8.1.9 • 9.1.0	• Fedora Core 6 (2.6.38 Kernel) • Yocto 2.7.3 Warrior (4.19.87 Kernel)	• Intel Atom C3558 CPU (Denverton) with AES-NI enabled • Intel Atom C3558 CPU (Denverton) with AES-NI disabled

2.1.1   EdgeConnect Platforms

Silver Peak's development processes are such that future releases under ECOS 8.1.9 and ECOS 9.1.0 should be FIPS validateable and meet the claims made in this document. Only the versions that explicitly appear on the certificate, however, are formally validated.

The following EdgeConnect hardware appliance configurations are vendor affirmed.

EdgeConnect HW Appliance	Operating System	Processor
EC-US	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Atom™ CPU E3825@ 1.33 GHz
EC-XS	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Atom™ C2358 (Rangely), 1.7 GHz
EC-XS (2020)	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Atom™ C3558 (Denverton), 2.20 GHz
EC-S	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon® CPU E3-1268L v3, 2.30GHz
EC-S-P	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon® D-2123IT
EC-M	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon® CPU E3-1270 v5, 3.60GHz
EC-M-P	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon® CPU E-2176G 3.7GHz
EC-M-P	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon® CPU E3-1270 v5, 3.60GHz
EC-M-H	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon® D-2163IT,12C/24T (Skylake D), 2.10GHz
EC-L, EC-L-NM	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon® CPU E5-2650 v3, 2.30GHz

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 5 of 46

Non-Proprietary

EC-L-P, EC-L-P-NM	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon® Gold 5118, 2.30 GHz
EC-L-H	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon-Gold 5218, 2.3GHz
EC-XL, EC-XL-NM	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon® CPU E5-2680 v3, 2.50GHz
EC-XL-P, EC-XL-P-NM (10G)	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon® Gold 6126, 2.60 GHz
EC-XL-P, EC-XL-P-NM (25G)	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon® Gold 6126, 2.60 GHz
EC-XL-H	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Intel® Xeon-Gold 5218, 2.3GHz

The following EdgeConnect virtual appliance configurations are vendor affirmed.

EdgeConnect Virtual Appliance	Operating System	Hypervisor
EC-V	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	VMware ESXi/ESX 6.7
EC-V	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	VMware ESXi/ESX 7.0
EC-V	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Red Hat KVM 8.x
EC-V	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	KVM, QEMU 4.x
EC-V	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Microsoft Hyper V 10.0
EC-V	Fedora Core 6 (2.6.38 Kernel) and Yocto 2.7.3 Warrior (4.19.87 Kernel)	Citrix Xen Server 8.1.0

The CMVP allows porting of this cryptographic module from the operational environment specified on the validation certificate to an operational environment which was not included as part of the validation testing as long as the porting rules of FIPS 140-2 Implementation Guidance G.5 are followed. As per FIPS 140-2 Implementation Guidance G.5, no claim can be made as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed above. The cryptographic module is also supported on the vendor affirmed operational environments for which FIPS operational testing and algorithm testing was not performed.

The CMVP makes no claim as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed on the validation certificate.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 6 of 46

Non-Proprietary

2.2 Cryptographic Module Boundaries of Physical Hardware Appliances

For FIPS 140-2 Level 1 validation, the EdgeConnect hardware appliances have been validated as multi-chip standalone cryptographic modules. The opaque metal chassis physically encloses the complete set of hardware and firmware components and represents the physical cryptographic boundary of the module. The physical cryptographic boundary is defined as encompassing the top, front, left, right, rear, and bottom surfaces of the chassis.

The following sections include, for each validated EdgeConnect hardware appliance, labelled views, status indicator LEDs identification, dimensions, weight, and environmental ranges.

2.2.1   EC-XS

The following sections provide images of the EC-XS appliance and document it's LED status indicators.

2.2.1.1   EC-XS Views

Figure 1 EC-XS Front View

Figure 2 EC-XS Rear View

Figure 3 EC-XS Left Side View

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 7 of 46

Non-Proprietary

Figure 4 EC-XS Right Side View

The EC-XS side views above show the factory-installed louver which ensures FIPS enclosure opacity.

Figure 5 EC-XS Top View

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 8 of 46

Non-Proprietary
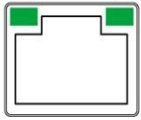
Figure 6 EC-XS Bottom View

2.2.1.2 EC-XS LED Status Indicators

Table 1 EC-XS LED Status Indicators

View	LED	Definition
Front LEDs	Power	• **Illuminated** = System is powered on • **Not illuminated** = System is powered off
	SSD	• **Blinking** = Data access activities
Rear LEDs	Speed	• **Amber** = Connection speed is 1000 Mbps • **Green** = Connection speed is 100 Mbps • **Not illuminated** = Connection speed is 10 Mbps
	Link/ACT	• **Amber** **solid** = Port is active • **Amber** **blinking** = There is traffic

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 9 of 46

Non-Proprietary

2.2.2   EC-XS Power, Dimensions, and Weight

Spec	EC-XS
Power Requirements	100–240VAC 50–60Hz,34 W / 116 BTU
Power Supplies	Single (Power Adapter)
Height	1.73 in. (44 mm)
Width	9.09 in. (231 mm)
Depth	7.87 in. (200 mm)
Weight	3.5 lbs. (1.6 kg)

2.2.3   Environmental Ranges

Model	Spec	Range
All Models	Temperature (Operating)	0°C to 40°C (32°F to 104°F)
	Temperature (Storage)	-40°C to 65°C (-40°F to 149°F)
	Altitude (Operating)	Up to 10,000 ft. (3,048 m)
	Altitude (Storage)	Up to 40,000 ft. (12,192 m)
EC-XS	Humidity (Operating)	8% to 90% relative humidity, non-condensing
	Humidity (Storage)	8% to 95% relative humidity, non-condensing

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 10 of 46

Non-Proprietary

2.3 Cryptographic Module Boundaries of Virtual Appliances

For FIPS 140-2 Level 1 validation, the module has been tested as a multi-chip standalone firmware module. The logical cryptographic boundary of the EdgeConnect virtual appliance is defined as the entirety of the OVA file installed on the hypervisor which contains the firmware image (EdgeConnect OS (ECOS) Firmware shown below). The physical boundary is the surface of the computer chassis. For the hardware EdgeConnect appliance, the below diagram is applicable but do note that the Virtual Host is not applicable to hardware models.
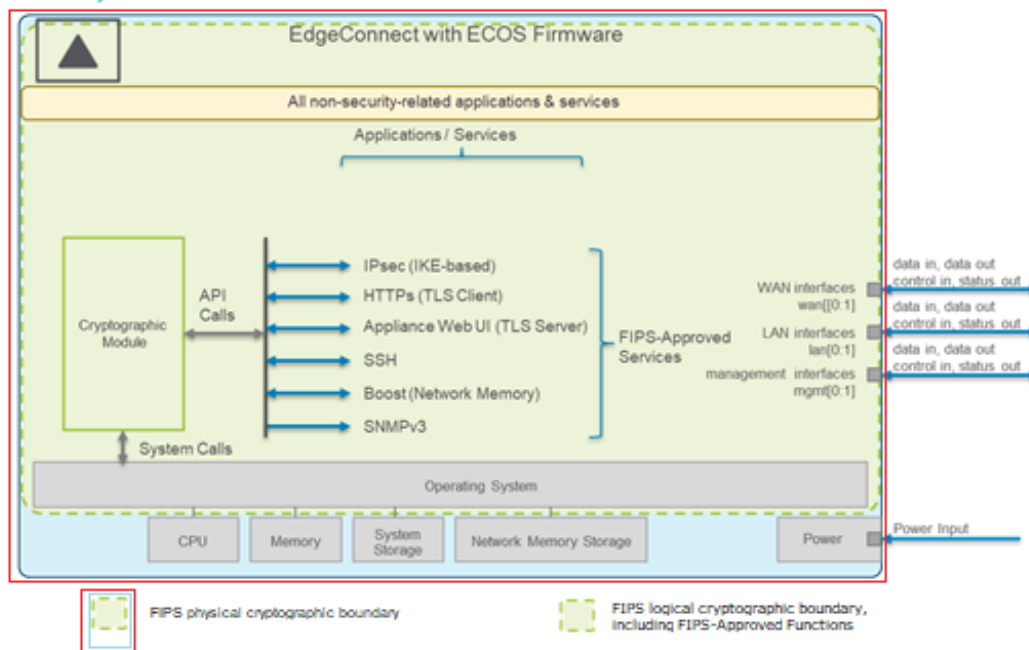
Figure 7 Functional Block Diagram of ECOS System Components

2.4 Logical Interfaces

The following tables list the EC-XS physical interfaces and their respective logical interfaces as defined by FIPS 140-2.

Table 2 EC-XS Physical and FIPS 140-2 Logical Interfaces

Module Physical Interfaces	Count	FIPS 140-2 Logical Interface(s)
Management Ports: mgmt0, mgmt1 10/100/1000 Ethernet Ports	2	Data Input, Data Output, Control Input, Status Output
Network Ports: wan0, wan1, lan0, lan1 10/100/1000 Ethernet Ports	4	Data Input, Data Output, Control Input, Status Output
LEDs	14	Status Output: 1 Power, 1 Disk, 12 RJ-45
Power Button	1	Control Input
Power Jack	1	Power Input
Reset Button	1	Not Used
RJ-45 Console Port	1	Not Used
USB Ports	2	Not Used

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 11 of 46

Non-Proprietary

Please note for EdgeConnect virtual appliances, the product can support up to 64 virtual network ports.

2.5 Intended Level of Security

The cryptographic module meets FIPS 140-2 Level 1 requirements. The module is a multi-chip standalone device. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Table 3 Intended Level of Security

Section	FIPS 140-2 Section Title	Security Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services and Authentication	2
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
Overall	Overall Cryptographic Module Validation Level	1

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 12 of 46

Non-Proprietary

3 Physical Security

The Silver Peak EdgeConnect FIPS Hardware appliances are a scalable, multi-processor, standalone network devices and are enclosed in a robust opaque steel housing. The enclosure of the module has been designed to satisfy FIPS 140-2 Security Level 1 physical security requirements. Refer to the Recommended Frequency of Inspection table below.

Table 4 Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection / Test	Inspection / Test Guidance Details
Physical metal chassis	Once per month	If physical damaged is observed, and ECOS is still running, execute the Zeroize for Factory Return command from the CLI: `fips secure erase` and return the module to the factory.

The Silver Peak EdgeConnect FIPS Virtual appliance must be run on a production grade platform (such as a standard commercially made PC, laptop, server, etc.) to meet requirements from FIPS 140-2 Security Level 1. The platforms used for the virtual appliances, as tested in this validation, meet the requirements for Security Level 1 physical security requirements. Refer to the Recommended Frequency of Inspection table above for the virtual host.

4 Operational Environment

The operational environment of the Hardware appliance is non-modifiable. The Operating System (OS) is Linux, a real-time, multi-threaded operating system that supports memory protection between processes. Access to the underlying Linux implementation is disabled in the FIPS mode of operation. Only Silver Peak provided interfaces are used, and the Command Line Interface (CLI) is a restricted command set. The module only allows the loading of trusted and verified firmware that is provided by Silver Peak. Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation. The hardware appliances used during testing met Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B, Class B, which vacuously meets requirements for Class A in FIPS 140-2 Area 8 (Security Level 1).

The operational environment of the Virtual appliance is limited. The tested operating systems segregate user processes into separate process spaces. Each process space is logically separated from all other processes by the operating system software and hardware. The module functions entirely within the process space of the calling application, and implicitly satisfies the FIPS 140-2 requirement for a single user mode of operation. The platforms meet Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B, Class B, which vacuously meets requirements for Class A in FIPS 140-2 Area 8 (Security Level 1).

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 13 of 46

Non-Proprietary

5 Roles, Services, and Authentication

5.1 Roles

The module supports role-based authentication with a Crypto Officer role and a User role. The Crypto Officer installs and administers the module. The Users use the cryptographic services provided by the module. The module supports up to 10 concurrent WebUI or API operators with ECOS 9.1.0 (there is no limit to the number of users in ECOS 8.1.9). The module's access control rules, system timing, and internal controls maintain separation of the multiple concurrent operators. There are no additional roles (e.g., Maintenance) supported nor a bypass capability.

5.2 Services with Crypto Officer and User Roles

Table 5 Roles and Services, below lists all Services and maps the associated Roles as well as the Type of Access to Cryptographic Keys and Critical Security Parameters (CSPs).

The Types of Access to Cryptographic Keys and CSPs include:

- R – Read
- E – Execute
- W – Write or Create
- Z – Zeroize
- N/A – Not Applicable

Table 5 Roles and Services

Service	CO	User	Description	Input	Output	CSP / Algorithm - Type of Access [Item # in Table 9 Cryptographic Keys and CSPs]
Run Self-test	√	√	Perform self-tests on demand	N/A	Status output	N/A - N/A [N/A]
Reboot	√	√	Trigger a module reboot	Command	Progress information	N/A - N/A [N/A]
Zeroize for Factory Return	√	√	Zeroizes all CSPs and Keys and securely erases all system disks and network memory disks. ECOS is no longer running, and the module must be returned to the factory.	Command	Progress information	All CSPs - All: Z [N/A]

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 14 of 46

Non-Proprietary

Firmware image download	√	√	Download the firmware image file onto the inactive system partition.	Command	Progress information	TLS as Client - TLS Keys: R, W, E [12 – 21]
Firmware update[1]	√	√	Update firmware on the module.	Command	Progress information	Firmware Upgrade – F/W update key: R, E [32]
Show Status	√	√	Show Status services including show network configuration, show routing and flows, show alarms, show appliance information, show licensing, and show syslog. Status command is available from: CLI, Web User Interface, API.	Command	Output	Passwords – N/A [22]. IP address of Syslog receiver – N/A [N/A]
ECOS Configuration	√	√	Provide services for ECOS configuration, administration, maintenance, and support via the ECOS Web User Interface, the ECOS API, and CLI over SSH	Command	Status output	Passwords - Password: R, W [22]. TLS as Server - TLS Keys: R, W, E [1 – 11]. SSH - SSH Keys: R, W, E [36 – 44]. DRBG seed: R, W [46]

---

[1] Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 15 of 46

Non-Proprietary

Orchestrator	√	√	Configuration, administration, maintenance, support, and monitoring. Orchestrator is out of scope of this validation but ECOS interacts with it.	Configuration	Status	TLS as Client - TLS Keys: R, W, E [12 – 21]. Password: R, W [22]. SSH Keys: R, W, E [36 – 44]. DRBG seed: R, W [46]
SNMPv3	√	√	Provide ability to query management information.	SNMPv3 requests	SNMPv3 responses	SNMP - SNMP Keys: R, W, E [33 – 35]. SNMP Password: R, W [33]
IKEv1/IKEv2 IPSec	√	√	Access the module's IPSec services to secure network traffic.	IKEv1/IKEv2 inputs and data; IPSec inputs, commands, and data	IKEv1/IKEv2 outputs, status, and data; IPSec outputs, status, and data	IPsec - IPsec Keys: R, W, E [24 – 31]. DRBG seed: R, W [46]
HTTPS over TLS	√	√	Secure browser connection over Transport Layer Security (TLS)	TLS inputs, commands, and data	TLS outputs, status, and data	TLS as Server - TLS Keys: R, W, E [1 – 11]. DRBG seed: R, W [46]

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 16 of 46

Non-Proprietary

SSHv2	√	√	Provide authenticated and encrypted remote management sessions while using the CLI.	SSHv2 key agreement parameters, SSH inputs, and data	SSHv2 outputs and data	SSH Keys: R, W, E [36 – 44].
Boost	√	√	WAN optimization with Data Deduplication using network memory (with disk encryption) and TCP acceleration (TCP acceleration does not use cryptographic services). Boost is an optional licensed ECOS feature.	Configuration	Status	Disk Encryption [23]. IPsec Keys: R, W, E [24 – 31]. DRBG seed: R, W [46]
Network Configuration	√	√	Provide CO and User the ability to configure network interfaces, access control lists, query network statuses, and SDWAN capabilities.	Configuration	Status	N/A - N/A [N/A]

5.3 Unauthenticated Services

The appliance can perform Layer 2/3/4 generic services including 802.1 VLAN, IP forwarding, ICMP, and Ping functionality without authentication. These services do not involve any cryptographic processing.

Additional unauthenticated services include performance of the power-on self-tests and system show status indication via LEDs.

5.4 Services Available in Non-FIPS Mode

The following services are available in Non-FIPS mode:

- All the services that are available in FIPS mode are also available in non-FIPS mode.
- If not operating in the Approved mode as per the procedures in section 6, FIPS-Approved Mode of Operation, then non-Approved algorithms and/or sizes are available.
- Debugging via the console port (non-Approved).

For additional non-security-relevant services offered by the module, please refer to the Silver Peak Reference documentation listed in section 11.1, Silver Peak and Aruba, a Hewlett Packard Enterprise company, Documentation.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 17 of 46

Non-Proprietary

5.5 Non-Approved Services Non-Approved in FIPS Mode

The following are non-Approved services non-Approved in FIPS Mode which if enabled will disable FIPS mode:

- Diffie-Hellman using Groups 1, 2, and 5.

5.6 Authentication Mechanisms

The module supports role-based authentication. Role-based authentication is performed before the Crypto Officer enters privileged mode using admin (CO or user) password via Web Interface or SSHv2. Role-based authentication is also performed for User authentication. This includes password and RSA/ECDSA-based authentication mechanisms.

The strength of each authentication mechanism is described below.

Table 6 Estimated Strength of Authentication Mechanisms

Authentication Type	Role	Strength
Password-based authentication **(CLI over SSH, API, and TLS-enabled Web browser using HTTPS)**	Crypto Officer and User	Passwords are required to be a minimum of eight ASCII characters and a maximum of 64 with a minimum of one letter and one number. Given these restrictions, the probability of randomly guessing the correct sequence is one (1) in 3,608,347,333,959,680 (this calculation assumes that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^8 (Total number of 8-digit passwords) – 84^8 (Total number of 8-digit passwords without numbers) – 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it is double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is 60,000/3,608,347,333,959,680, which is less than 1 in 100,000 required by FIPS 140-2. Additionally, invalid attempts are further restricted since for the first minute, the module permits unlimited attempts, but if there are more than four failed attempts in the previous 60 seconds, then login attempts are blocked for one minute.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 18 of 46

Non-Proprietary

RSA-based authentication (TLS/IKEv2)	User	The module supports 2048-bit RSA key authentication during TLS and IKEv2. RSA 2048-bit keys correspond to 112 bits of security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in 2^{112}, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is $60{,}000/2^{112}$, which is less than 1 in 100,000 required by FIPS 140-2.
Password-based authentication (SNMPv3)	Crypto Officer and User	Passwords are required to be a minimum of 20 ASCII characters and a maximum of 128 with a minimum of one letter and one number. Given these restrictions, the probability of randomly guessing the correct sequence is one (1) in 2,595,157,722,610,600,000,000,000,000,000,000,000 (this calculation assumes that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^{20} (Total number of 20-digit passwords) – 84^{20} (Total number of 20-digit passwords without numbers) – 42^{20} (Total number of 20-digit passwords without letters) + 32^{20} (Total number of 20-digit passwords without letters or numbers, added since it is double-counted in the previous two subtractions) = 2,595,157,722,610,600,000,000,000,000,000,000,000). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is 60,000/ 2,595,157,722,610,600,000,000,000,000,000,000,000, which is considerably less than 1 in 100,000 required by FIPS 140-2. Additionally, invalid attempts are further restricted since for the first minute, the module permits unlimited attempts, but if there are more than four failed attempts in the previous 60 seconds, then login attempts are blocked for one minute.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 19 of 46

Non-Proprietary

RSA-based authentication **(SSH/HTTPS over TLS)**	Crypto Officer and User	The module supports 2048-bit RSA key authentication during SSH and TLS. RSA 2048-bit keys correspond to 112 bits of security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in 2^112, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is 60,000/2^112, which is less than 1 in 100,000 required by FIPS 140-2. These keys can be used for admin authentication. The same lockout mechanism as with password-based authentication exists so the same added restrictions for invalid attempts exist.
ECDSA-based authentication **(HTTPS over TLS)**	Crypto Officer and User	ECDSA signing and verification is used to authenticate to the module during HTTPS over TLS. Only ECDSA approved encryption algorithms are supported in the FIPS mode of operation. For ECDSA P-256 provides 128 bits of equivalent security, and P-384 provides 192 bits of equivalent security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in 2^128, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is 60,000/2^128, which is less than 1 in 100,000 required by FIPS 140-2. These keys can be used for admin authentication.
Pre-shared key-based authentication **(IKEv1)**	Crypto Officer and User	The password requirements are the same as the CO role above, except that the maximum ASCII characters can be 64. Additionally, exactly 64 HEX characters can be entered. Assuming the weakest option of 8 ASCII characters, the authentication mechanism strength is the same as the Password-based 8 ASCII characters authentication above.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 20 of 46

Non-Proprietary

6 FIPS-Approved Mode of Operation

The module is intended to always operate in the FIPS-Approved mode. To enter FIPS mode, the Crypto Officer must perform the following initial steps:

- Initially invoke the user interface using the default password, at which time the Crypto Officer must change the default password.

- After changing the CO or User password, the CO must issue the CLI command:

```
(config) # fips enable
This operation will cause a system reboot.
Do you want to proceed? [y/n] y
```

- Upon successful reboot and power-up self-test execution, the module is in FIPS-Approved Mode of Operation.

- Confirm that FIPS mode has been enabled.

```
(config) # fips show
FIPS mode: Enabled
```

The Crypto Officer must ensure that the appliance is always operating in a FIPS-Approved mode of operation. This can be achieved by ensuring the following:

- FIPS-Approved Mode must be enabled on the appliance before Users are permitted to use the appliance.

- Passwords must be at least eight (8) characters long.

- Access to the appliance Web Interface is permitted only using HTTPS over a TLS tunnel. Basic HTTP and HTTP over SSL are not permitted.

- Only SNMPv3 read-only may be enabled. SNMPv1 and SNMPv2 are not allowed.

- Only FIPS-Approved algorithms can be used for cryptographic services. Please refer to Section 6.1, FIPS Approved Cryptographic Functions, for the list of Approved algorithms.

- The appliance logs must be monitored. If a strange activity is found, the Crypto Officer should take the appliance offline and investigate.

- The hardware appliance or virtual host must be regularly examined for signs of tampering. Refer to Section 3, Physical Security for the recommended frequency.

- All configuration performed through the Orchestrator must ensure that only the Approved algorithms and services are enabled on the FIPS-enabled appliance.

- The user is responsible for zeroizing all CSPs when switching modes.

- Refer to Section 7, Non-Approved FIPS Mode Configurations for non-Approved configurations in FIPS-Approved mode.

In the event that a Crypto Officer needs to remove EdgeConnect from FIPS mode, the following steps should be performed:

- The CO must Issue the CLI command:

```
(config) # fips disable
This operation will cause a system reboot.
Do you want to proceed? [y/n] y
```

- If the device is being sent back for RMA or being decommissioned, the CO should also perform the CLI command 'fips secure erase'.
    - o Please note this command will zeroize the drive and require assistance from vendor support.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 21 of 46

Non-Proprietary

6.1 FIPS Approved Cryptographic Functions

The following approved cryptographic algorithms are used in the FIPS-Approved mode of operation. The cryptographic library where the cryptographic algorithms are implemented is the **Silver Peak ECOS Cryptographic library**.

Only the algorithms, modes and key sizes listed in the following table are implemented by the module in the FIPS Approved Mode. Other options listed in the referenced CAVP certificates are latent and not used.

All Algorithm Modes listed in the table below have been tested with the Automated Cryptographic Validation Testing (ACVT) program, but not all tested modes are used.

Table 7 Approved Cryptographic Functions

CAVP Certs	Algorithm	Standards	Mode / Method	Key Lengths, Curves or Moduli	Use
#A1957 #A1958 #C2122 #C2163 #C2209 #C2214	AES	SP 800-38A, FIPS 197, SP 800-38D, SP 800-38F	CBC, CFB128, CTR, ECB, GCM [Note 1]	128, 192, 256 bits	Data Encryption/ Decryption KTS (AES Certs. #A1957, #A1958, #C2122 and #C2209, and HMAC Certs. #C2126 and #C2211; key establishment methodology provides 128 or 256 bits of encryption strength)
#C2123 #C2210	CVL	SP 800-56A	KAS-ECC CDH Component	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Module implements the ECC CDH primitive from SP 800-56A, identical to the primitive described in SP 800-56Ar3. This is compliant as per FIPS 140-2 IG G.20 resolution #2.
Vendor Affirmed	CKG	SP 800-133 Rev2			Key Generation [Note 6]

CAVP Certs	Algorithm	Standards	Mode / Method	Key Lengths, Curves or Moduli	Use
#C2135 #C2213	CVL TLS 1.2 IKEv1 SSHv2 SNMPv3	SP 800-135 KDF	IKEv1: PSK TLS v1.2	IKEv1: DH 2048-bit; SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 SSH: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 TLS: SHA2-256, SHA2-384, SHA2-512 SNMP Password Length: 64-128 bits	Key Derivation [Note 4]
#A1957	CVL TLS 1.2 IKEv1 IKEv2 SSHv2 SNMPv3	SP 800-135 KDF	IKEv1: PSK TLS v1.2	IKEv1: DH 2048-bit; SHA-1, SHA2-256, SHA2-384, SHA2-512 IKEv2: DH 2048-bit; SHA-1, SHA2-256, SHA2-384, SHA2-512 SSH: SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 TLS: SHA2-256, SHA2-384, SHA2-512 SNMP Password Length: 64-128 bits	Key Derivation [Note 4]
#A1957 #C2136 #C2212	DRBG	SP 800-90A	Counter based	256 bits	Deterministic Random Bit Generation [Note 2]
ENT (P)	TRNG	SP 800-90B			Random Number Generation

CAVP Certs	Algorithm	Standards	Mode / Method	Key Lengths, Curves or Moduli	Use
#A1957	ECDSA	FIPS 186-4	Key Pair Generation	P-224, P-256, P-384, P-521 K-233, K-283, K-409, K-571 B-233, B-283, B-409, B-571	Key Pair Generation
#A1957 #C2126 #C2211	HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	160, 256, 224, 384, 512	Message Authentication
#A1957	KAS-SSC ECC/FFC	SP 800-56A Rev3	ECC: Ephemeral Unified FFC: DhEphem	ECC: P-256, P-384 FFC: MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 KAS Roles – Initiator, Responder	Key Agreement Scheme – Shared Secret Computation
KAS-SSC: #A1957 CVL: #C2135 #C2213	KAS	SP 800-56A Rev3 SP 800-135 KDF	KAS-SSC: ECC: Ephemeral Unified FFC: DhEphem CVL: TLS v1.2	EC Diffie-Hellman P-256, P-384 Diffie-Hellman MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192 with TLS 1.2 KDF	Key Agreement Scheme – IG D.8, scenario X1 (2) Key Agreement Scheme per SP 800-56Arev3 with Key Derivation per SP 800-135 KDF [Note 5]

CAVP Certs	Algorithm	Standards	Mode / Method	Key Lengths, Curves or Moduli	Use
#A1957 #C2161 #C2215	RSA	FIPS 186-4 FIPS 186-2	PKCS1 v1.5 ANSI X9.31 SHA-1 _Note 3_ SHA-224 SHA-256 SHA-384 SHA-512	RSA KeyGen (186-4) 2048, 3072 RSA SigGen (186-4) 2048, 3072 RSA SigGen (186-2) 4096 RSA SigVer (186-2) 1024 _Note 3_, 1536 _Note 3_, 2048, 3072, 4096	Digital Signature Generation and Verification Key Generation
#A1957	Safe Primes	SP 800-56A Rev3	KeyGen	MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	Safe Primes Key Generation
#A1957 #C2121 #C2208	SHS	FIPS 180-4	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	160, 256, 224, 384, 512	Message Digest

Note 1: *The module's AES-GCM implementation complies with IG A.5 scenario 1 method ii) and RFC 5288. AES-GCM is only used in TLS version 1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev2, Section 3.3.1: for a complete list of the module's supported AES-GCM ciphers for TLS 1.2, refer to section 11.4 below. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. If the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.*

Note 2: *The minimum number of bits of entropy generated by the module is 256 bits.*

Note 3: *SHA-1 and modulus sizes 1024 and 1536 are only used in RSA Signature Verification for legacy use only (186-2).*

Note 4: *No parts of these protocols, other than the Key Derivation Function (KDF), have been tested by the CAVP and CMVP. KDF algorithms previously were listed under Component Validation List (CVL); this is kept for backwards compatibility.*

Note 5: *The module provides Diffie-Hellman and EC Diffie-Hellman key agreement schemes compliant with SP800-56Arev3 and used as part of the protocol key exchange in accordance with scenario X1 (2) of IG D.8; that is, the shared secret computation (KAS-FFC-SSC and KAS-ECC-SSC) followed by the derivation of the keying material using SP800-135 KDF.*

Note 6: *The module directly uses the unmodified output of the DRBG for key generation.*

6.2 Non-FIPS Approved but Allowed Cryptographic Algorithms

The Algorithm listed in Table 8 below is Non-FIPS Approved but Allowed cryptographic functions because it is covered in Implementation Guidance (IG) as follows:

Table 8 Approved Cryptographic Functions Non-FIPS Approved but Allowed Cryptographic Functions

Algorithm	Caveat	Use / Compliance
RSA Key Wrapping using 2048 / 3072 bit keys	Provides 112 or 128 bits of encryption strength.	Used for key establishment such as in TLS handshake. Complies with IG D.9 Allowed Methods since only PKCS#1-v1.5 padding scheme based on section 8.1 of RFC 2313 with RSA modulus 2048 bits and 3072 bits is used.

7 Non-Approved FIPS Mode Configurations

When FIPS mode is enabled, the following configuration options are non-Approved and are Not Permitted for use in the FIPS-Approved mode of operation:

- Configuring the device in legacy router mode, in-line bridge mode, or server mode is not FIPS approved.
- Orchestrator IPSec UDP tunnels that are not IKE-based IPSec
- Any combination of DES, MD5, and PPTP
- Firmware images signed with SHA-1
- Null Encryption
- TLS with Diffie-Hellman Group 2
- SNMPv1 or SNMPv2
- Certificates with less than 112 bits security strength as used with IKEv1, IPSec, TLS, SSH, and/or user authentication
- bSec
- HTTP
- UDP and GRE tunnels
- Diffie Hellman Groups 1, 2, or 5
- Disabled DH
- SSL decryption

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 26 of 46

Non-Proprietary

8 Cryptographic Key Management and Critical Security Parameters (CSPs)

The table below describes cryptographic keys and Critical Security Parameters (CSPs) used by the module.

Table 9 Cryptographic Keys and CSPs

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
TLS as Server (ECOS Web UI)						
1	**TLS Pre-Master Secret**. - Used to derive TLS Master Secret.	Secret (48 bytes)	Generation: N/A Establishment: Elliptical Curve Diffie-Hellman (EC DH), RSA Key Wrapping	Input: Input via RSA Key Wrapping Output: N/A	Plaintext in RAM.	Zeroize upon completion of processing ClientKeyExchange message.
2	**TLS Master Secret**. - Used to derive TLS encryption key and TLS HMAC Key.	Secret (48 bytes)	Generation: N/A Establishment: Master Secret is derived via the key derivation function defined in SP800-135 KDF (TLS 1.2) using the TLS Pre-Master Secret.	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon termination of TLS session or module restart.
3	**TLS AES Key**. - Used during encryption and decryption of data within the TLS protocol.	AES-CBC (128, 256 bits) AES-GCM (128, 256 bits) (Note: 192 bits not supported)	Generation: N/A Establishment: AES Key is derived via the key derivation function defined in SP800-135 KDF (TLS 1.2).	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon termination of TLS session or module restart.

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
4	**TLS HMAC Key**. - Used to protect integrity of data within the TLS protocol.	HMAC using SHA-1, SHA-256, SHA-384 (160/256/384 bits)	Generation: N/A Establishment: HMAC Key is derived using TLS 1.2 KDF.	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon termination of TLS session or module restart.
5	**TLS Server RSA Public Key**. - Used during the TLS handshake.	RSA (2048 bits or larger)	Generation: If the default, self-signed certificate is used, ECOS generates the appliance Public Key using FIPS Approved SP800-90A DRBG in compliance with FIPS 186-4 RSA key pair generation method. Establishment: N/A	Input: If a certificate is installed by the Crypto Officer, a private key file is also installed which includes the Public Key. Output: Output in plaintext	Plaintext in RAM. Plaintext on Disk.	Zeroize in RAM upon termination of TLS session or module restart. Zeroize in hard drive upon invocation of FIPS secure erase operation.
6	**TLS Server RSA Private Key**. - Used during the TLS handshake.	RSA (2048 bits or larger)	Generation: If the default, self-signed certificate is used, ECOS generates the appliance Private Key using FIPS Approved SP800-90A DRBG in compliance with FIPS 186-4 RSA key pair generation method. Establishment: N/A	Input: If a certificate is installed by the Crypto Officer, a private key file is also installed. Output: N/A	Plaintext in RAM. Plaintext on Disk.	Zeroize in RAM upon termination of TLS session or module restart. Zeroize in hard drive upon invocation of FIPS secure erase operation.
7	**TLS Client RSA Public Key**. - TLS client sends the Public Key.	RSA (2048 bits, 3072 bits)	Generation: N/A Establishment: N/A	Input: Input in plaintext Output: N/A	Plaintext in RAM.	Zeroize in RAM upon termination of TLS session or module restart.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 28 of 46

Non-Proprietary

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
8	**TLS Server EC Diffie-Hellman Public Key**. - Used during the TLS handshake to establish the ECDH Shared Secret.	EC Diffie-Hellman (Curves: P-224, P-256, P-384, P-521 B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571)	Generation: Public Key is generated using FIPS Approved SP800-90A DRBG. Establishment: N/A	Input: N/A Output: Output in plaintext	Plaintext in RAM.	Zeroize upon termination of TLS session or module restart.
9	**TLS Server EC Diffie-Hellman Private Key**. - Used during the TLS handshake to establish the ECDH Shared Secret.	EC Diffie-Hellman (Curves: P-224, P-256, P-384, P-521 B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571)	Generation: Private Key is generated using FIPS Approved SP800-90A DRBG. Establishment: N/A	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon termination of TLS session or module restart.
10	**TLS Client EC Diffie-Hellman Public Key**. - Used during the TLS handshake to establish the ECDH Shared Secret.	EC Diffie-Hellman (Curves: P-224, P-256, P-384, P-521 B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571)	Generation: N/A Establishment: N/A	Input: Input in plaintext Output: N/A	Plaintext in RAM.	Zeroize upon termination of TLS session or module restart.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 29 of 46

Non-Proprietary

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
11	**TLS KDF Internal States**. - Used to derive Master Secret from Pre-Master Secret and to derive key materials from Master Secret.	SP800-135 KDF (TLS)	Generation: N/A Establishment: N/A	Input: N/A Output: N/A	N/A	Zeroize upon termination of TLS session or module restart.
TLS as Client (ECOS Client of Orchestrator, Cloud Portal, and Image Server)						
12	**TLS Pre-Master Secret**. - Used to derive TLS Master Secret.	Secret (48 bytes)	Generation: N/A Establishment: Elliptical Curve Diffie-Hellman (ECDH), RSA Key Wrapping	Input: N/A Output: Output in plaintext	Plaintext in RAM.	Zeroize inside ssl3_send_client_key_exchange or module restart.
13	**TLS Master Secret**. - Used to derive TLS encryption key and TLS HMAC Key.	Secret (48 bytes)	Generation: N/A Establishment: Master Secret is derived via the key derivation function defined in SP800-135 KDF (TLS 1.2) using the TLS Pre-Master Secret.	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon termination of TLS session or module restart.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy　　　　Page 30 of 46

Non-Proprietary

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
14	**TLS AES Key**. - Used during encryption and decryption of data within the TLS protocol.	AES-CBC (128, 256 bits) AES-GCM (128, 256 bits) (Note: 192 bits not supported)	Generation: N/A Establishment: AES Key is derived via the key derivation function defined in SP800-135 KDF (TLS 1.2).	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon termination of TLS session or module restart.
15	**TLS HMAC Key**. - Used to protect integrity of data within the TLS protocol.	HMAC using SHA-1, SHA-256, SHA-384 (160/256/384 bits)	Generation: N/A Establishment: HMAC Key is derived using TLS 1.2 KDF.	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon termination of TLS session or module restart.
16	**TLS Server RSA Public Key**. - Used during the TLS handshake.	RSA (2048 bits or larger)	Generation: N/A Establishment: N/A	Input: Input in plaintext Output: N/A	Plaintext in RAM.	Zeroize in RAM upon termination of TLS session or module restart. Zeroize in hard drive upon invocation of FIPS secure erase operation.
17	**TLS Client EC Diffie-Hellman Public Key**. - Used during the TLS handshake to establish the ECDH Shared Secret.	EC Diffie-Hellman (Curves: P-224, P-256, P-384, P-521 B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571)	Generation: Public Key is generated using FIPS Approved SP800-90A DRBG. Establishment: N/A	Input: N/A Output: Output in plaintext	Plaintext in RAM.	Zeroize upon termination of TLS session or module restart.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 31 of 46

Non-Proprietary

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
18	**TLS Client EC Diffie-Hellman Private Key**. - Used during the TLS handshake to establish the ECDH Shared Secret.	EC Diffie-Hellman (Curves: P-224, P-256, P-384, P-521 B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571)	Generation: Private Key is generated using FIPS Approved SP800-90A DRBG. Establishment: N/A	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon termination of TLS session or module restart.
19	**TLS Server EC Diffie-Hellman Public Key**. - Used during the TLS handshake to establish the ECDH Shared Secret.	EC Diffie-Hellman (Curves: P-224, P-256, P-384, P-521 B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571)	Generation: N/A Establishment: N/A	Input: Input in plaintext Output: N/A	Plaintext in RAM.	Zeroize upon termination of TLS session or module restart.
20	**TLS KDF Internal States**. - Used to derive Master Secret from Pre-Master Secret and to derive key materials from Master Secret.	SP800-135 KDF (TLS)	Generation: N/A Establishment: N/A	Input: N/A Output: N/A	N/A	Zeroize upon termination of TLS session or module restart.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 32 of 46

Non-Proprietary

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
21	**Trusted Root CA Public Keys**. - Used to authenticate the TLS server.	RSA (2048 bits, 4096 bits), EC Diffie-Hellman (Curves: P-256, P-384), ECDSA using SHA-1, SHA-256, SHA-384, SHA-512 (160/256/384 /512 bits)	Generation: N/A Establishment: N/A	Input: Factory installed Output: N/A	Plaintext in RAM. Plaintext in Hard drive.	Zeroize upon invocation of FIPS secure erase operation.
Passwords						
22	**CO and User Login Passwords**. - Used for operator authentication to the CLI, WebUI.	Password (8-64 characters)	Generation: N/A Establishment: N/A	Input: User inputs plaintext Password 8-64 printable characters [0-9, a-z, A-Z, 33 special characters (DEL excluded)] Output: N/A	Plaintext in RAM.	Zeroize upon user account deletion or FIPS secure erase operation.
Disk Encryption						

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 33 of 46

Non-Proprietary

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
23	**Encryption Private Key.** - Used to encrypt Boost data pages on disk.	AES-CBC-128 (128 bits)	Generation: Private Key is generated using FIPS Approved SP800-90A DRBG. Establishment: N/A	Input: N/A Output: N/A	Plaintext in RAM. Plaintext on Disk.	Zeroize upon invocation of CLI "reboot clean" command or invocation of FIPS secure erase operation.
IPSec						
24	**IPSec Pre-Shared Key (PSK).** - Used for tunnel peer authentication.	Shared Secret (8 - 64 ASCII characters)	Generation: N/A Establishment: N/A	Input: User inputs plaintext Password 8-64 printable characters [0-9, a-z, A-Z, 33 special characters (DEL excluded)] Output: N/A	Plaintext in RAM. Plaintext on Disk.	Zeroize upon IPSec tunnel deletion or FIPS secure erase operation.
25	**IPSec Diffie-Hellman Private Key.** - Used during the IPSec handshake to establish the DH Shared Secret.	Diffie-Hellman Group 14-18 (default is DH group 14) (2048 bits)	Generation: Public and Private Keys are generated internally using FIPS Approved SP800-90A DRBG. Establishment: N/A	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon deletion of IPSec tunnel or module restart.
26	**IPSec Diffie-Hellman Public Key.** - Used during the IPSec handshake to establish the DH Shared Secret.	Diffie-Hellman Group 14-18 (default is DH group 14) (2048 bits)	Generation: Public and Private Keys are generated internally using FIPS Approved SP800-90A DRBG. Establishment: N/A	Input: N/A Output: Output in plaintext	Plaintext in RAM.	Zeroize upon deletion of IPSec tunnel or module restart.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy　　　　Page 34 of 46

Non-Proprietary

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
27	**IPSec Diffie-Hellman Peer Public Key**. - Used during the IPSec handshake to establish the DH Shared Secret.	Diffie-Hellman Group 14-18 (default is DH group 14) (2048 bits)	Generation: N/A Establishment: N/A	Input: Received in a message during key exchange from the peer Output: N/A	Plaintext in RAM.	Zeroize upon deletion of IPSec tunnel or module restart.
28	**IPSec Diffie-Hellman Shared Secret**. - Used to derive encryption and HMAC Keys.	Diffie-Hellman Group 14-18 (default is DH group 14) (2048 bits)	Generation: N/A Establishment: Derived using DH Public and Private Keys	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon deletion of IPSec tunnel or module restart.
29	**IPSec AES Keys**. - Used during encryption and decryption of data within the IPSec protocol.	AES-CBC (128, 256 bits)	Generation: N/A Establishment: AES Key is derived via a key derivation function defined in SP800-135 KDF (IKEv1 and IKEv2).	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon deletion of IPSec tunnel or module restart.
30	**IPSec HMAC Keys**. - Used to protect integrity of data within the IPSec protocol.	HMAC using SHA-1, SHA-256, SHA-384, SHA-512 (160/256/384/512 bits)	Generation: N/A Establishment: HMAC Key is derived using IKEv1 and IKEv2 KDFs defined in SP800-135 KDF.	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon deletion of IPSec tunnel or module restart.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 35 of 46

Non-Proprietary

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
31	**IPSec IKEv1 and IKEv2 KDF Internal State**. - Used to derive encryption and HMAC Key from Shared Secret.	SP800-135 KDF (IKEv1 and IKEv2)	Generation: N/A Establishment: N/A	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon deletion of IPSec tunnel or module restart.
Firmware Upgrade						
32	**Firmware Update RSA Key**. - Used to protect integrity during firmware update.	RSA (4096 bits)	Generation: N/A Establishment: N/A	Input: Input in plaintext Output: N/A	Plaintext in RAM. Plaintext on Disk.	Zeroize upon FIPS secure erase operation.
SNMPv3						
33	**SNMPv3 Authentication and Privacy Password**. - Used to establish SNMPv3 sessions.	Password (20-32 characters)	Generation: N/A Establishment: N/A	Input: User inputs Authentication and Privacy Password. Minimum 20-character length including [a-z][A-Z][0-9]. Output: N/A	Plaintext in RAM. Stored on Disk with hash.	Zeroize upon FIPS secure erase operation.

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
34	**SNMPv3 Authentication and Privacy Secret**. - Used to establish SNMPv3 sessions.	SHA-1, AES-CBC-128 (128 bits)	Generation: N/A Establishment: Derived via a key derivation function defined in SP800-135 KDF (SNMPv3).	Input: N/A Output: N/A	Plaintext in RAM. Plaintext on Disk.	Zeroize upon termination of session or module restart.
35	**SNMPv3 KDF Internal States**. - Used to derive encryption and HMAC Key from Shared Secret.	SP800-135 KDF (SNMPv3)	Generation: N/A Establishment: N/A	Input: N/A Output: N/A	N/A	Zeroize upon termination of session or module restart.
SSHv2						
36	**SSH Server RSA Public Key**. - Used to authenticate the SSH handshake.	RSA (2048 bits)	Generation: Default Public Key generated on first boot using FIPS Approved SP800-90A DRBG in compliance with FIPS 186-4 RSA key pair generation method if it does not exist in manufacturing database. User can request re-generation. Establishment: N/A	Input: Factory installed into the manufacturing database. Output: Output in plaintext.	Plaintext in RAM. Plaintext on Disk.	Zeroize upon FIPS secure erase operation.

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
37	**SSH Server RSA Private Key**. - Used to authenticate the SSH handshake.	RSA (2048 bits)	Generation: Default Private Key generated on first boot using FIPS Approved SP800-90A DRBG in compliance with FIPS 186-4 RSA key pair generation method if it does not exist in manufacturing database. User can request re-generation. Establishment: N/A	Input: Factory installed into the manufacturing database. Output: N/A	Plaintext in RAM. Plaintext on Disk.	Zeroize upon FIPS secure erase operation.
38	**SSH Client RSA Public Key**. - Used during the SSH handshake to establish the Shared Secret.	RSA (2048 bits)	Generation: N/A Establishment: N/A	Input: Input in plaintext. Output: N/A	Plaintext in RAM.	Zeroize upon termination of SSH session or module restart.
39	**SSH Server Diffie-Hellman Public Key**. - Used during the SSH handshake to establish the Shared Secret.	DH group 14 (2048 bits)	Generation: Public Key is generated using FIPS Approved SP800-90A DRBG. Establishment: N/A	Input: N/A Output: Output in plaintext	Plaintext in RAM.	Zeroize upon termination of SSH session or module restart.
40	**SSH Server Diffie-Hellman Private Key**. - Used during the SSH handshake to establish the Shared Secret.	DH group 14 (2048 bits)	Generation: Private Key is generated using FIPS Approved SP800-90A DRBG. Establishment: N/A	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon termination of SSH session or module restart.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 38 of 46

Non-Proprietary

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
41	**SSH Client Diffie-Hellman Public Key**. - Used during the SSH handshake to establish the Shared Secret.	DH group 14 (2048 bits)	Generation: N/A Establishment: N/A	Input: Input in plaintext Output: N/A	Plaintext in RAM.	Zeroize upon termination of SSH session or module restart.
42	**SSH AES Key**. - Used during encryption and decryption of data within the SSH protocol.	AES-CTR (128, 192, 256 bits)	Generation: N/A Establishment: AES Key is derived via a key derivation function defined in SP800-135 KDF (SSHv2).	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon termination of SSH session or module restart.
43	**SSH HMAC Key**. - Used to protect integrity of data within the SSH protocol.	HMAC using SHA-1 (160 bits)	Generation: N/A Establishment: HMAC Key is derived via a key derivation function defined in SP800-135 KDF (SSHv2).	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon termination of SSH session or module restart.
44	**SSH KDF Internal States**. - Used to derive encryption and HMAC Key from Shared Secret.	SP800-135 KDF (SSHv2)	Generation: N/A Establishment: N/A	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize upon termination of SSH session or module restart.
DRBG						

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 39 of 46

Non-Proprietary

Item	Description/Usage	Type	Generation/ Establishment	Input/Output	Storage	Zeroization
45	**Entropy Input into CTR_DRBG with Derivation Function**. - Used during generation of random numbers.	Intel RDRAND Entropy Input length is equal to the AES Key length - AES-256 (256 bits)	Generation: Generated using Intel RDRAND instruction. Establishment: N/A	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize by rebooting the module.
46	**CTR_DRBG Seed**. - Used during generation of random numbers.	SP 800-90A CTR_DRBG (AES-256) with Derivation Function (384 bits) Seed length = key length + 128 bits	Generation: Derived from entropy, nonce and personalization string. Establishment: N/A	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize by rebooting the module.
47	**CTR_DRBG Internal States: V and Key**. - Used during generation of random numbers.	SP 800-90A CTR_DRBG (AES-256) with Derivation Function Values of V (128-bits) and Key (256 bits)	Generation: Derived from seed. Establishment: N/A	Input: N/A Output: N/A	Plaintext in RAM.	Zeroize by calling fips/rand/fips_drbg_lib.c:FIPS_ drbg_free() or by rebooting the module.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 40 of 46

Non-Proprietary

9 Self-Tests

The module performs the following Power on Self-Tests (POSTs) and Conditional tests. Self-tests are performed during power-on or on demand. Upon failure of either a power-on or conditional self-test, the module returns an error status and halts its cryptographic operation and output of Critical Security Parameters (CSP).

9.1 Power-On Self-Tests (POSTs)

Table 10 Power-On Self Tests

Algorithm	Test
AES	KATs using ECB mode (encryption/decryption)
	KATs using CBC mode (encryption/decryption)
AES-GCM	KAT using 256-bit key length (encryption/decryption)
ECC CDH	Primitive "Z" Computation KAT, P-224
FFC CDH	Primitive "Z" Computation KAT, MODP-2048
SP800-90A DRBG	KAT for CTR_DRBG
Developer-defined Health Tests per SP 800-90B	Continuous Health Tests (CHTs) [Note 1] for ENT (P)
ECDSA	KAT using P224, SHA-512 (sign / verify)
HMAC-SHA-1	Firmware Integrity Test (OpenSSL Library)
HMAC	KAT using SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512
KDF	KAT for TLS 1.2
	KAT for IKEv1
	KAT for IKEv2
	KAT for SSH
	KAT for SNMP
RSA	KAT using 2048 bit key, SHA-256 (sign / verify)
	KAT using 2048 bit key (encryption / decryption)
SHA-1	ECOS Firmware Integrity Self-test
SHS	KAT using SHA-1 [Note 2]

Note 1: *Developer- defined Continuous Health Tests (CHTs) include coverage of SP 800-90B RCT and APT health tests, and the startup tests are run over at least 1024 consecutive samples.*

Note 2: *SHA-1 has a Known Answer Test (KAT). SHA-224, SHA-256, SHA-384, and SHA-512 are tested as part of HMAC.*

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 41 of 46

Non-Proprietary

9.2 Conditional Self Tests

Table 11 Conditional Self Tests

Algorithm	Test
DRBG	Continuous Random Number Generator Test [Note 1]
ENT (P)	SP800-90B Continuous Health Tests
ENT (P)	Continuous Random Number Generator Test
ECDSA	Pairwise Consistency Test (sign / verify)
KAS ECC/FFC	As per SP 800-56A Rev3: For ECC, the module performs full public-key validation For FFC, the module performs partial public-key validation
RSA	Pairwise Consistency Test (sign / verify) Pairwise Consistency Test (encryption / decryption)
RSA Sig Ver	Firmware Update Self-Test (RSA 4096-bit verification)

Note 1: *The module performs DRBG health tests as defined in Section 11.3 of SP800-90A, and continuous random number generator test (CRNGT) to ensure that consecutive random numbers do not repeat.*

Upon successful completion of the power-on self-tests, the module displays the results to the console.

```
FIPS AES-NI Power On Self Test Succeeded
FIPS OpenSSL Power On Self Test Succeeded
FIPS system files integrity check: OK
```

- Confirm self-tests completed by checking the messages and associated times on the console.

In the event of a KATs failure, the appliance logs different messages on the console, depending on the error.

```
FIPS AES-NI POST FAILED
FIPS OpenSSL Power-on Self-tests FAILED
FIPS system files integrity check: FAILED
```

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 42 of 46

Non-Proprietary

10 Mitigation of Other Attacks

As per IG 11.1, since the module has not been purposely designed, built and publicly documented to mitigate one or more specific attacks, the Mitigation of Other Attacks requirements are not applicable.

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

11 Reference Documents

11.1 Silver Peak and Aruba, a Hewlett Packard Enterprise company, Documentation

Aruba, a Hewlett Packard Enterprise company, acquired Silver Peak in 2020. For more details see HPE Completes Acquisition of SD-WAN Leader Silver Peak.

The Silver Peak and Aruba Networks web sites contain information on the full line of products from Silver Peak and Aruba Networks:

https://www.silver-peak.com/

https://www.arubanetworks.com/

Full Silver Peak EdgeConnect documentation (including Command Line Interface (CLI) Reference Guides, User Guides, and Hardware Reference Guides) can be found at the links provided below:

https://www.silver-peak.com/support/user-documentation/all-documents?field_userdoc_suite_tid=74&field_userdoc_release_tid=All&field_userdoc_type_tid=All

https://www.arubanetworks.com/support-services/silver-peak-documentation/

The NIST Validated Modules web site contains contact information for answers to technical questions for the validated product:

https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search

Enter **Silver Peak** in the Vendor field then select Search to see a list of FIPS certified Silver Peak products.

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 43 of 46

Non-Proprietary

11.2   Glossary and Definitions

The following table includes terms and abbreviations used in cryptographic security reference documentation.

Abbreviation	Meaning
AES	Advanced Encryption Standard, as specified in [FIPS 197]
AES-GCM	AES with Galois/Counter Mode
ANSI	American National Standards Institute
APT	Adaptive Proportion Test (NIST SP 800-90B)
AS	Assertion
CAVP	Cryptographic Algorithm Validation Program
CAVS	Cryptographic Algorithm Validation System
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CESG	Communications-Electronics Security Group
CFB	Cipher Feedback
CHT	Continuous Health Test (NIST SP 800-90B)
CKG	Cryptographic Key Generation
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
EC DH	Elliptic Curve Diffie-Hellman (Algorithm)
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman (NIST SP 800-56A)
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode (GCM) and GMAC Algorithm
HMAC	Keyed-Hash Message Authentication Code, as specified in [FIPS 198]
KAS	Key Agreement Schemes and Key Confirmation (NIST SP 800-56A)
MAC	Message Authentication Code
MD5	Message Digest 5
MMT	Multi-block Message Test
NRBG	Non-deterministic Random Bit Generator
OS	Operating System
PKCS	Public Key Cryptography Standard
RBG	Random Bit Generator
RCT	Repetition Count Test (NIST SP 800-90B)
RNG	Random Number Generator
RSA	Rivest Shamir Adleman Cryptographic System (FIPS 186-4)
RSA	Reversible Digital Signature Algorithm (FIPS186-2 and FIPS186-3 RSA)
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSH	Secure Shell
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 44 of 46

Non-Proprietary

11.3 NIST Cryptographic Security Reference Documentation

NIST cryptographic security reference documentation can be found at https://csrc.nist.gov/publications/fips and https://csrc.nist.gov/publications/sp800.

Reference	Specification
[ANS X9.31]	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
[FIPS 140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS 180-4]	Secure Hash Standard (SHS)
[FIPS 186-2/4]	Digital Signature Standard
[FIPS 197]	Advanced Encryption Standard
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)
[FIPS 202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
[PKCS#1 v2.1]	RSA Cryptography Standard
[PKCS#5]	Password-Based Cryptography Standard
[PKCS#12]	Personal Information Exchange Syntax Standard
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[SP 800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
[SP 800-52]	Guidelines for the Selection, Configuration, and Use of TLS Implementations
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP 800-56C]	Recommendation for Key Derivation through Extraction-then-Expansion
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[SP 800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions
[SP 800-132]	Recommendation for Password-Based Key Derivation
[SP 800-135]	Recommendation for Existing Application –Specific Key Derivation Functions

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 45 of 46

Non-Proprietary

11.4   ECOS Supported Cipher Suites for TLS 1.2 from NIST SP 800-52 Section 3.3.1

The following lists the cipher suites for TLS 1.2 from NIST SP 800-52 revision 2, section 3.3.1, that are supported by the module for all releases of ECOS:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

The following lists the additional cipher suites for TLS 1.2 from NIST SP 800-52 revision 1, section 3.3.1, that are supported by the module for only ECOS release 8.1.9:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_GCM_SHA384

Silver Peak EdgeConnect running Firmware versions ECOS 8.1.9 and ECOS 9.1.0 FIPS 140-2 Level 1 Security Policy   Page 46 of 46

Non-Proprietary