cPacket Networks, Inc.

cVu 16100 Network Packet Broker

Hardware Model: cVu 16100 NG TAA

Firmware Version: 21.3.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2

Document Version: 0.8

Prepared for:

cPacket Networks, Inc.
480 N. McCarthy Blvd, Suite 100
Milpitas, CA 95035
United States of America

Phone: +1 650 969-9500
www.cpacket.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the cVu 16100 Network Packet Broker (Hardware Model: cVu 16100 NG TAA, Firmware Version: 21.3.0) from cPacket Networks, Inc. (cPacket). This Security Policy describes how the cVu 16100 Network Packet Broker meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.[1] and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS).

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The cVu 16100 Network Packet Broker is referred to in this document as cVu 16100 Network Packet Broker, cVu 16100, or the module.

1.2 References

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

- The cPacket website (https://www.cpacket.com) contains information on the full line of products from cPacket.
- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

1.3 Document Organization

The Security Policy document is organized into two primary sections. Section 2 provides an overview of the validated module. This includes a general description of the capabilities and the use of cryptography, as well as a presentation of the validation level achieved in each applicable functional area of the FIPS standard. It also provides high-level descriptions of how the module meets FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions, management methods, and applicable usages policies.

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

[1] U.S. – United States

2. cVu 16100 Network Packet Broker

2.1 Overview

cPacket delivers visibility vendors can trust through network monitoring and packet brokering solutions to solve today's biggest network challenges. Their cutting-edge technology enables network and security teams to proactively identify issues in real-time before negatively impacting end-users. Only cPacket inspects all the packets delivering the right data to the right tools at the right time and provides detailed network analytics dashboards. The cPacket solutions provide greater network visibility for security tools or performance monitoring tools and are designed to overcome scalability issues and reduce troubleshooting time, resulting in increased security, reduced complexity, lower costs, and a faster return on investment. Leading enterprises, service providers, healthcare organizations, and governments rely on cPacket solutions for improved agility, higher performance, and greater efficiency.

The cPacket cVu series of network packet brokers are built on a distributed, scalable architecture to completely eliminate the risk of randomly dropped packets. They have pre-ingress and post-egress smart ports with dedicated resources to inspect, process, and report network traffic. These smart ports perform filtering, slicing, decapsulation, deduplication, nanosecond time-stamping, burst calculation, and load balancing. Each data port is configurable as either an input or output port. The data ports also feature complete packet inspection filters and support load balancing and aggregation and distribution/duplication of packets in a one-to-many, many-to-one, and any-to-any configuration.

The cVu 16100 Network Packet Broker (shown in Figure 1) is a hardware appliance from the cPacket cVu series of network packet brokers. It has a 2U[2] form factor and both RJ-45[3] Ethernet and serial interfaces for management. It supports flexible port speed assignments and can be configured to support 64 data ports of 10 GbE[4] QSFP+[5] or 16 data ports of either 100 GbE QSFP28[6] or 40 GbE QSFP+, or a combination thereof. Each appliance runs the Ubuntu 18.04 operating system.

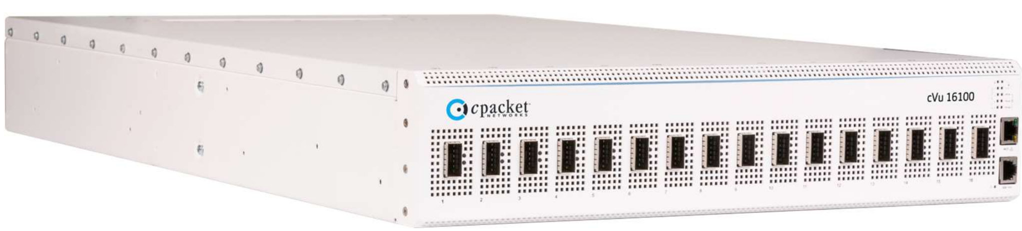

Figure 1 – cVu 16100 Network Packet Broker

[2] U – Rack Unit
[3] RJ-45 – Registered Jack-45
[4] GbE – Gigabit Ethernet
[5] QSFP+ – Quad Small Form-Factor Pluggable Plus
[6] QSFP28 – Quad Small Form-Factor Pluggable 28

Management of the cVu 16100 is accomplished via the following methods:

- Web-based graphical user interface (GUI) called the Web UI[7], accessible remotely via HTTPS[8] over the Ethernet management port
- REST[9] API[10], accessible remotely via HTTPS over the Ethernet management port
- Command Line Interface (CLI), accessible remotely via SSH[11] over the Ethernet management port
- Serial Console, accessible locally via direct attachment to the serial console port from a computer using a null modem cable

cVu uses the SNMP[12] v3 protocol for discovery applications as well as the generation of traps in the event of system error or abnormal traffic conditions. The SNMP interface is accessed over the Ethernet management port.

The cVu 16100 is validated at the FIPS 140-2 section levels shown in Table 1.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A[13]
7	Cryptographic Key Management	2
8	EMI/EMC[14]	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The cVu 16100 is a hardware cryptographic module with a multiple-chip standalone embodiment. The overall security level of the module is 2.

[7] UI – User Interface
[8] HTTPS – Hypertext Transfer Protocol Secure
[9] REST – Representational State Transfer
[10] API – Application Programming Interface
[11] SSH – Secure Shell
[12] SNMP – Simple Network Management Protocol
[13] N/A – Not Applicable
[14] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

The module is comprised of the cVu 16100 appliance running the version Firmware Version: 21.3.0 firmware. The firmware executes using the general-purpose CPU[15] and RAM[16] contained within the cVu 16100 appliance.

The cryptographic boundary surrounds the physical enclosure of the appliance and includes the cVu 16100 firmware and all internal hardware. The main hardware components consist of processors, memories, SATA[17] HDD[18], Ethernet switches, controllers, fans, and the enclosure containing all of these components. Note that the four field-replaceable power supplies are considered outside the module boundary.

2.2.1 Modes of Operation

The module will be in its Approved mode of operation when all power-up self-tests have completed successfully, Further, when initialized and configured according to the guidance in this Security Policy, the module does not support a non-Approved mode of operation.

2.2.2 Algorithm Implementations

Cryptographic functions are provided by the cPacket Cryptographic, SSH KDF[19], TLS[20] KDF, SNMP KDF, and SHA-3 libraries (see Table 2 below).

Table 2 – Cryptographic Algorithm Providers

Certificate Number	Implementation Name	Version	Use
A2251	cPacket Cryptographic Library	1.0	Firmware-based cryptographic primitives
A2253	cPacket SSH KDF Library	1.0	SSH v2 KDF implementation
A2254	cPacket TLS KDF Library	1.0	TLS v1.2 KDF implementation
A2252	cPacket SNMP KDF Library	1.0	SNMP v3 KDF implementation
A2250	cPacket SHA-3 Implementation	1.0	Provides the SHA-3 that is used as a conditioning function for the CPU Jitter entropy source.

The module implements the FIPS-Approved algorithms listed in Table 3 below.

[15] CPU – Central Processing Unit
[16] RAM – Random Access Memory
[17] SATA – Serial Advanced Technology Attachment
[18] HDD – Hard Disk Drive
[19] KDF – Key Derivation Function
[20] TLS – Transport Layer Security

Table 3 – FIPS Approved Algorithm Implementations

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
A2251	AES[21]	*FIPS PUB[22] 197* *NIST SP[23] 800-38A*	CFB128[24], CTR[25], ECB[26]	128, 192, 256	Encryption/decryption *ECB mode is used only for self-testing.*
		NIST SP 800-38B	CMAC[27]	128, 192, 256	MAC Generation/verification *This implementation is not used by the module.*
		NIST SP 800-38D	GCM[28]	128, 256	Encryption/decryption
Vendor Affirmed	CKG[29]	*NIST SP 800-133rev2*	-	-	Cryptographic key generation
A2252	CVL[30]	*NIST SP 800-135rev1*	SNMP v3 KDF	-	Key derivation
A2253	CVL	*NIST SP 800-135rev1*	SSH v2 KDF	-	Key derivation
A2254	CVL	*RFC[31] 7627*	TLS v1.2 KDF	-	Key derivation
A2251	DRBG[32]	*NIST SP 800-90Arev1*	Counter-based (derivation function – yes; prediction resistance – no)	256-bit AES-CTR	Deterministic random bit generation
A2251	DSA	*FIPS PUB 186-4*	-	2048/224, 2048/256, 3072/256	Key pair generation
			SHA2[33]-224, SHA2-256, SHA2-384, SHA2,512	2048/224, 2048/256, 3072/256	Domain parameter generation
			SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2,512	1024/160, 2048/224, 2048/256, 3072/256	Domain parameter verification
			SHA2-224, SHA2-256, SHA2-384, SHA2,512	2048/224, 2048/256, 3072/256	Digital signature generation *This implementation is not used by the module.*

[21] AES – Advanced Encryption Standard
[22] PUB – Publication
[23] SP – Special Publication
[24] CFB – Cipher Feedback
[25] CTR – Counter
[26] ECB – Electronic Code Book
[27] CMAC – Cipher-Based Message Authentication Code
[28] GCM – Galois Counter Mode
[29] CKG – Cryptographic Key Generation
[30] CVL – Component Validation List
[31] RFC – Request for Comment
[32] DRBG – Deterministic Random Bit Generator
[33] SHA – Secure Hash Algorithm

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
			SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2,512	1024/160, 2048/224, 2048/256, 3072/256	Digital signature verification *This implementation is not used by the module.*
A2251	ECDSA[34]	*FIPS PUB 186-4*	-	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Key pair generation
			-	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Public key validation
			SHA2-224, SHA2-256, SHA2-384, SHA2-512	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Digital signature generation
			SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Digital signature verification
N/A	ENT (NP)[35]	*NIST SP 800-90B*	-	-	Non-deterministic random bit generation[36]
A2251	HMAC[37]	*FIPS PUB 198-1*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	112 (minimum)	Message authentication
A2251 A2253 A2254	KAS[38]	*NIST SP 800-56Arev3* *NIST SP 800-135rev1*	KAS-ECC-SSC[39] with SSH KDF	ephemeralUnified	Key agreement *Key establishment methodology provides between 112 and 256 bits of encryption strength.*
			KAS-FFC-SSC[40] with SSH KDF	dhEphem	Key agreement *Key establishment methodology provides 112 bits of encryption strength.*
		NIST SP 800-56Arev3 *RFC 7627*	KAS-ECC-SSC with TLS KDF	ephemeralUnified	Key agreement *Key establishment methodology provides between 112 and 256 bits of encryption strength.*

[34] ECDSA – Elliptic Curve Digital Signature Algorithm
[35] ENT (NP) – Entropy (Non-Physical)
[36] Per *FIPS Implementation Guidance* G.13, non-deterministic random bit generators tested for compliance to *NIST SP 800-90B* are considered Approved.
[37] HMAC – Keyed-Hash Message Authentication Code
[38] KAS – Key Agreement Scheme
[39] KAS-ECC-SSC – Key Agreement Scheme - Elliptic Curve Cryptography - Shared Secret Computation
[40] KAS-FFC-SSC – Key Agreement Scheme - Finite Field Cryptography - Shared Secret Computation

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
			KAS-FFC-SSC with TLS KDF	dhEphem	Key agreement *Key establishment methodology provides 112 bits of encryption strength.*
A2251	KAS-ECC-SSC	*NIST SP 800-56Arev3*	ephemeralUnified	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Shared secret computation
A2251	KAS-FFC-SSC	*NIST SP 800-56Arev3*	dhEphem	2048/224, 2048/256	
A2251	KTS[41]	*NIST SP 800-38F*	AES-GCM[42]	128, 256	Key transport (authenticated encryption) *Key establishment methodology provides 128 or 256 bits of encryption strength.*
A2251	RSA[43]	*FIPS PUB 186-4, Appendix B.3.3*	-	2048, 3072	Key pair generation
A2251	RSA	*FIPS PUB 186-4*	X9.31	2048, 3072, 4096 (SHA2-256, SHA2-384, SHA2-512)	Digital signature generation
				1024, 2048, 3072, 4096 (SHA-1, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
			PKCS#1[44] 1.5	2048, 3072, 4096 (SHA2-256, SHA2-384, SHA2-512)	Digital signature generation
				1024, 2048, 3072, 4096 (SHA-1, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
			PSS[45]	2048, 3072, 4096 (SHA2-256, SHA2-384, SHA2-512)	Digital signature generation
				1024, 2048, 3072, 4096 (SHA-1, SHA2-256, SHA2-384, SHA2-512)	Digital signature verification
A2250	SHA-3	*FIPS PUB 202*	SHA3-256	-	Message digest
A2251	SHS[46]	*FIPS PUB 180-4*	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	-	Message digest

**No parts of the SNMP, SSH, and TLS protocols, other than the KDFs, have been tested by the CAVP and CMVP.*

The vendor affirms the following cryptographic security methods:

[41] KTS – Key Transport Scheme
[42] Per *FIPS 140-2 Implementation Guidance* D.9, AES-GCM is an Approved key transport technique.
[43] RSA – Rivest Shamir Adleman
[44] PKCS – Public Key Cryptography Standard
[45] PSS – Probabilistic Signature Scheme
[46] SHS – Secure Hash Standard

- Cryptographic key generation – As per section 6.1 of *NIST SP 800-133*, the module uses its FIPS-Approved CTR-based DRBG specified in *NIST SP 800-90Arev1* to generate cryptographic keys and seeds for asymmetric key generation. The resulting symmetric keys and seeds are the unmodified output from the DRBG. The DRBG is seeded via a *NIST SP* 800-*90B* compliant CPU jitter-based entropy source internal to the module, which was assessed per the guidance in *FIPS 140-2 IG* 7.15. The module requests 384 bits of entropy from the calling application per request.

2.3 Module Ports and Interfaces

The module's design separates the physical ports and interfaces into four logically distinct and isolated categories. They are:

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

The cVu 16100 contains the physical ports and interfaces shown in Figure 2 and Figure 3.

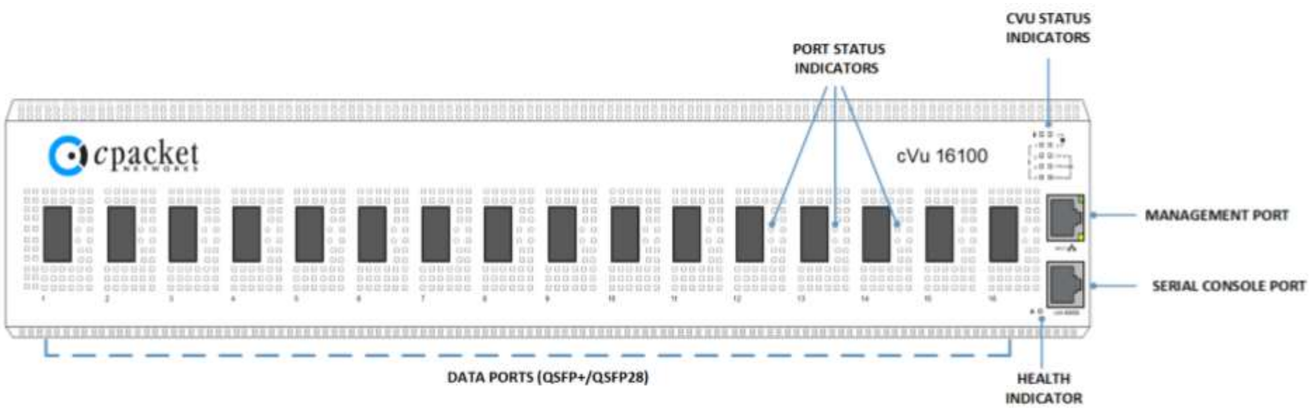

Figure 2 – cVu 16100 Ports and Interfaces (Front)

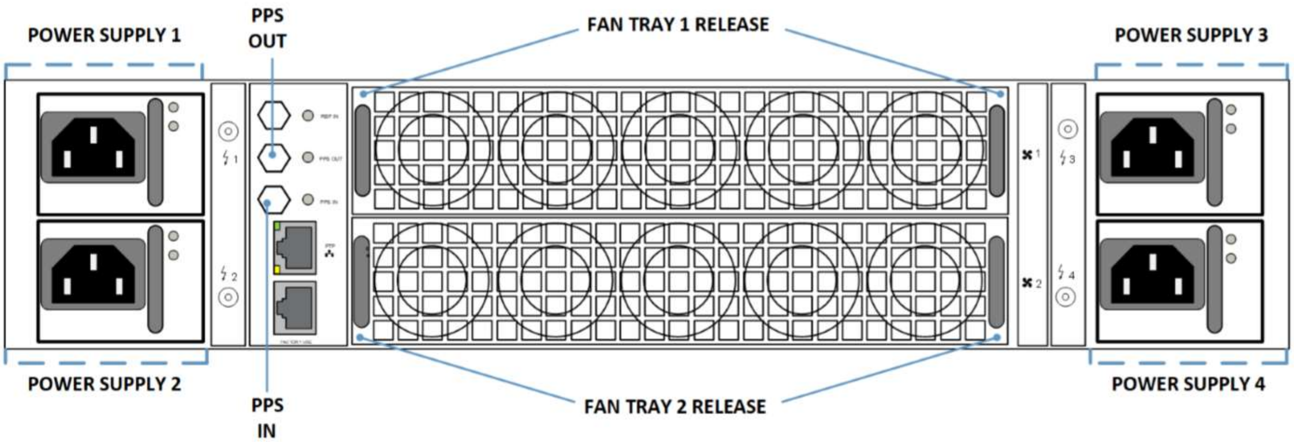

Figure 3 – cVu 16100 Ports and Interfaces (Rear)

Table 4 provides the mapping from the physical interfaces to logical interfaces as defined by FIPS 140-2 for the CVU 16100.

Table 4 – FIPS 140-2 Logical Interface Mappings for the CVU 16100

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
Front Panel			
Data ports	16	Data ports comprised of QSFP28 and/or QSFP+ ports	• Data Input • Data Output
Port status indicators	16 (1 per data port)	Solid yellow – insert Solid green – link Flashing green – activity Flashing yellow – error	• Status Output
cVu status indicator (Temperature)	1	Solid green – all is well Solid red – danger zone Flashing red – failsafe	• Status Output
cVu status indicator (Power Supply)	4 (1 per PSU[47])	Solid green – power supply active Solid red – power supply inactive Flashing red – power supply removed from chassis	• Status Output
cVu status indicator (Fan Tray)	2 (1 per fan tray module)	Solid green – fan tray is operating properly Solid red – fan tray requires replacement Flashing red – fan tray is removed from chassis	• Status Output

[47] PSU – Power Supply Unit

Physical Port/Interface	Quantity	Description	FIPS 140-2 Logical Interface
cVu status indicator (PTP[48] In)	1	PTP not currently supported	N/A
cVu status indicator (PPS[49] In)	1	Solid green – valid signal Off – no PPS signal present	• Status Output
cVu status indicator (PPS Out)	1	Solid green – valid signal	• Status Output
Health indicator	1	Indicates health of system: Flashing green – all is well. If not flashing green, refer to other cVu status indicators.	• Status Output
Management port	1	Used to access the Web UI and CLI (via SSH)	• Data Input • Data Output • Control Input • Status Output
Serial console port	1	Used to access the serial console	• Data Input • Data Output • Control Input • Status Output
Rear Panel			
REF In indicator	1	N/A – unused.	• N/A
PPS In indicator	1	Solid green – valid signal Off – no PPS signal present	• Status Output
PPS Out indicator	1	Solid green – valid signal	• Status Output
PPS input	1	PPS input via SMA connector	• Control Input
PPS output	1	PPS output	• Status Output
PTP input	1	Used to configure PTP based time synchronization	• Control Input
Fan trays	2	Fan trays, each containing five fan modules	• N/A
Factory use port	1	Disabled via tamper-evident seal	• N/A
Power connectors	4	Power connectors	• Power Input

2.4 Roles and Services and Authentication

The sections below describe the module's roles and services and define any authentication methods employed.

[48] PTP – Precision Time Protocol
[49] PPS – Pulse-Per-Second

2.4.1 Authorized Roles

The module supports multiple concurrent operators. The module supports two authorized roles that operators may assume:

- Crypto Officer (CO) role – responsible for initial setup and configuration of the module into FIPS mode. The CO role maps to the "admin" product role and has read/write access to all system configuration parameters, backup/restore, and user add/remove. This role can access the module over the serial console, CLI, Web UI, or REST API. This role can also perform services via SNMP v3 (i.e., issue SNMP v3 discovery commands). The full list of CO services can be found in Tables 5–7 below.

- User role – has read-only access to overview, reports, system counter/alerts, and version information. The User role maps to the "L1" product role. This role can access the Web UI and REST API. This role does not have access to the serial console. The full list of User services can be found Table 6 below. Note that the product supports other predefined roles with permissions between L1 and admin (L2, L3 Restricted, and L3). Custom roles may also be defined by the CO using access control lists.

2.4.2 Operator Services

The CO has access to the services listed in Table 5 using the serial console and CLI. Services available to the CO and User over the Web UI and REST API are listed in Table 6.

Please note that the keys and Critical Security Parameters (CSPs) listed in Tables 5–6 indicate the type of access required using the following notation:

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

Table 5 – CO Services via the Serial Console and CLI

Service	Description	Input	Output	CSP and Type of Access
Establish SSH session	Establish SSH session over CLI	Command and parameters	Command response; status output	ECDH Public Component – R/X ECDH Private Component – X SSH Private Key – W/X SSH Public Key – W/X SSH Shared Secret – W/X SSH Session Key – R/W/X SSH Authentication Key – W/X

Service	Description	Input	Output	CSP and Type of Access
Network configuration	Configure basic networking parameters like IP[50] address, CLI port, hostname, NTP[51], and DNS[52] settings	Command and parameters	Command response; status output	None
Restart device	Restart the cVu device	Command	Command response; status output	All ephemeral keys and CSPs – W
Add/remove/list Admin level users	Add, remove, or list the Admin level users	Command and parameters	Command response; status output	CO Password – W
Display SNMP v3 settings[53]	Display SNMP v3 settings	Command	Command response; status output	None
Version Info	Show device information, like hardware model number and firmware version	Command	Command response; status output	None
Configure Syslog	Configure port and IP address for Syslog server(s)	Command and parameters	Command response; status output	None

[50] IP – Internet Protocol
[51] NTP – Network Time Protocol
[52] DNS – Domain Name System
[53] While SNMP v2 settings can be configured via the serial console, SNMP v2 is prohibited from use in FIPS mode. Only SNMP v3 shall be configured. SNMP v3 settings may be displayed via the serial console, but are configured only through the Web UI.

Table 6 – CO and User Services via Web UI and REST API

Service	Role		Description	Input	Output	CSP and Type of Access
	CO	User				
Establish TLS session	✓	✓	Establish Web UI or REST API session using TLS protocol	Command and parameters	Command response; Status output	Diffie-Hellman Public Key – R/X Diffie-Hellman Private Key – X ECDH Public Component – R/X ECDH Private Component – X TLS Private Key – R/X TLS Peer Public Key – R/X TLS Pre-Master Secret – R/W/X TLS Master Secret – W/X TLS Session Key – R/W/X TLS Authentication Key – R/W/X AES GCM IV – R/W/X
Network configuration	✓		Web UI: configure IP address, gateway, netmask, NTP, Syslog, DNS, and web port	Command and parameters	Command response; status output	None
Version Info	✓	✓	Show device information, like hardware model number and firmware version	Command	Command response; status output	None
Manage Certificates	✓		Paste in certificate or key file Web UI only	Command and parameters; certificates and keys	Command response; status output	RSA Private Key – R/W/X RSA Public Key – R/W/X ECDSA Private Key – R/W/X ECDSA Public Key – R/W/X
Restart device	✓		Restart the cVu device Web UI only	Command	Command response; status output	All ephemeral keys and CSPs – W
Factory restore	✓		Return the system to factory state and zeroize all keys and CSPs	Command	Command response; status output	All persistent keys/CSPs – W
Firmware update	✓		Update firmware Web UI only	Command and parameters	Command response; status output	Firmware Load Authentication Key – R/X
Add/remove/list users	✓		Add, remove, or list users	Command and parameters	Command response; status output	CO password – W User password – W
Configure password policy	✓		Define the password policy	Command and parameters	Command response; status output	None
Change own password	✓	✓	Change own password	Command; password	Command response; status output	CO password – W User password – W

Service	Role		Description	Input	Output	CSP and Type of Access
	CO	User				
Configure SNMP v3 settings	✓		Configure SNMP v3 settings	Command and parameters	Command response; status output	SNMP Authentication Password – R/W SNMP Encryption Password – R/W
Encrypt/Decrypt SNMP data	✓		Encrypt/decrypt SNMP data Web UI only	Establish SNMP protocol session	SNMP session established	SNMP Encryption Key – R/X SNMP Encryption Password – R/X
Authenticate SNMP data	✓		Authenticate SNMP data Web UI only	Establish SNMP protocol session	SNMP session established	SNMP Authentication Key – R/X SNMP Authentication Password – R/X
System Backup and Restore	✓		Perform system backups and restores	Command and parameters	Command response; status output	None

2.4.3 Additional Services

The module provides a limited number of services for which the operator is not required to assume an authorized role. Table 7 lists the services for which the operator is not required to assume an authorized role. None of these services disclose or substitute cryptographic keys and CSPs or otherwise affect the security of the module.

Table 7 – Additional Services

Service	Description	Input	Output	CSP and Type of Access
Zeroize	Zeroize ephemeral keys and CSPs	Power cycle using power connectors	Status output	All ephemeral keys/CSPs – W
Perform on-demand self-tests	Perform power-up self-tests on demand	Power cycle using power connectors	Status output	All ephemeral keys/CSPs – W
Authenticate to module	Authenticate to module	Command and parameters	Status output	CO Password – X User Password – X

2.4.4 Authentication Methods

The module supports identity-based authentication. Operators authenticate with password-based authentication. Each operator has their own account with a username and password used to authenticate to the module. Account credentials are stored locally.

2.4.5 Strength of Authentication Mechanisms

The strength of the authentication mechanism is such that for each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur.

The module enforces password requirements that are configured by the CO. Refer to section 3.1.4 for guidance on configuring a password policy to ensure each password meets the following requirements:

- Minimum of ten (10) characters
- At least one of 26 uppercase letter: A-Z
- At least one of 26 lowercase letter: a-z
- At least one of 10 digits: 0-9
- At least one of 35 special characters: !"#$%&\'()*+,-./:;<=>?@[\ ]^_`{|}~

Assuming a ten (10) character password with one uppercase letter, one lowercase letter, one number, one special character, and the remaining characters randomly chosen from the 97-character allowed set, the total number of valid password permutations possible is:

$$26 * 26 * 10 * 35 * 97^6 = 197{,}081{,}176{,}366{,}201{,}400 = 1.97 \times 10^{17}$$

Thus, the probability that a random attempt will succeed is 1.97×10^{17}, which is less than 1:1,000,000 as required by FIPS 140-2.

Probability of a successful random attempt during a one-minute period

For the serial console, the operator is limited to how many characters they can enter via the serial console, which operates at 115,200 bps. Translating to 14,400 bytes/sec, and a minimum password length of 10 characters, this would yield a conservative maximum of 1440 attempts per second, or 86,400 per minute. Therefore, using the probability that a random attempt will succeed or a false acceptance will occur in one minute is:

1: (1.97×10^{17} possible passwords / 86,400 password attempts per minute)
1: 2.28×10^{12}

This is less than 1:100,000 within one minute as required by FIPS 140-2.

For the CLI, Web UI, and REST API, the operator is limited to how many characters they can enter via the 1 Gbps management port. Translating to 125,000 bytes/sec, and a minimum password length of 10 characters, this would yield a conservative maximum of 12,500 attempts per second, or 750,000 per minute. Therefore, the probability that a random attempt will succeed, or a false acceptance will occur, in one minute is:

1: (1.97×10^{17} possible passwords / 750,000 password attempts per minute)
1: 2.63×10^{11}

This is less than 1:100,000 within one minute as required by FIPS 140-2.

2.5 Physical Security

The cVu 16100 is a multiple-chip standalone cryptographic module. The contents of the module, including all hardware components, firmware, and data are protected by the module enclosure. The module enclosure consists of a hard, opaque metal case as shown in Figure 4.

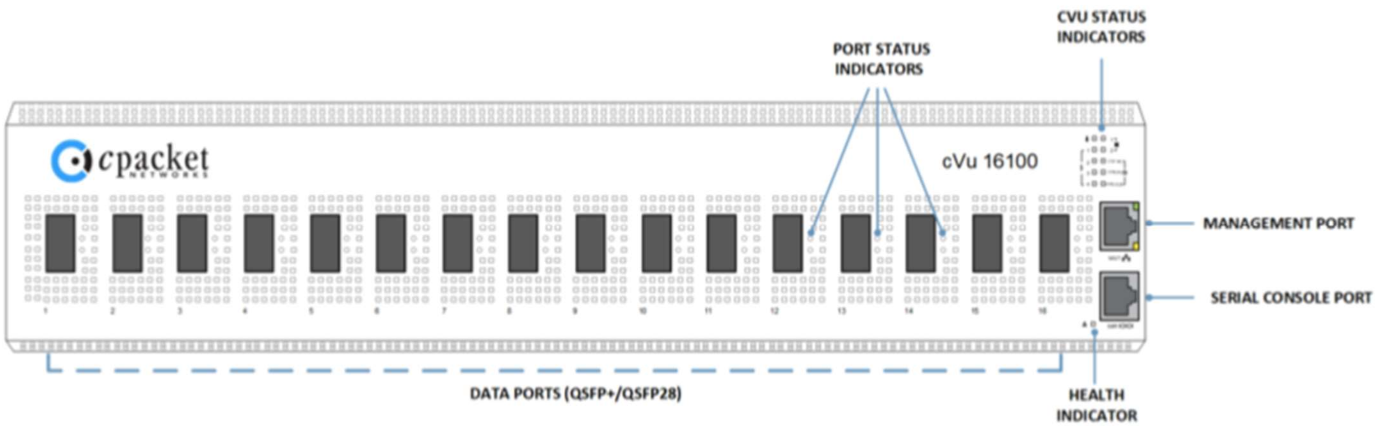

Figure 4 – cVu 16100 Module Enclosure

Factory applied, serial numbered, tamper-evident seals are used to protect the module's removable top cover, fan tray assemblies, and factory use port. Figure 5 shows an example of the tamper-evident seal used for the appliance.

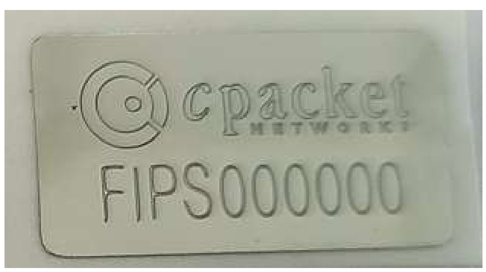

Figure 5 – cVu 16100 Tamper-Evident Seal

Once the module has been configured for operation in the Approved mode, the module cannot be accessed without signs of tampering. Four tamper-evident seals are applied to the module. Two tamper-evident seals are applied to screws on the top cover of the appliance, one in the front and one in the rear, to protect the top cover. One tamper-evident seal is applied to the two fan tray assemblies and device chassis at the rear of the appliance. One tamper-evident seal is applied to the factory use port.

Figure 6 shows the location of the tamper-evident seal applied to cover one of the eleven screws on the top front of the appliance that secure the top cover of the appliance (far right screw). Figure 7 shows the location of the tamper-evident seal applied to cover one of the two screws on the top rear of the appliance that secure the top cover of the appliance (far right screw). The combination of these two tamper-evident seals prevents the top cover from being rotated or lifted without showing tamper evidence.

Figure 8 shows the location of the tamper-evident seal applied to the fan tray assemblies and the device chassis. It is applied at a location on the right where the two fan tray assemblies meet and spans both fan tray assemblies and the device chassis.

Figure 9 shows the location of the tamper-evident seal applied to the factory use port.

Figure 6 – Tamper-Evident Seal on Screw on Top Cover of cVu 16100 Enclosure (Front)

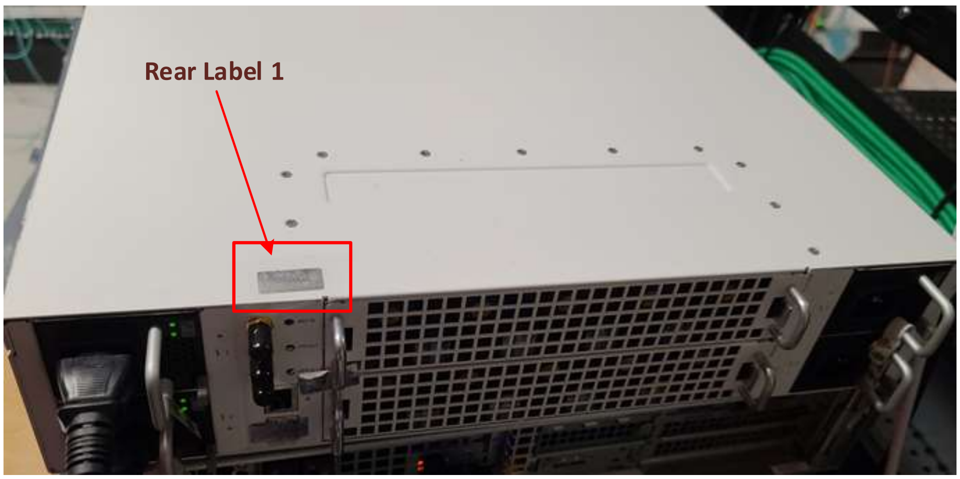

Figure 7 – Tamper-Evident Seal on Screw on Top Cover of cVu 16100 Enclosure (Rear)

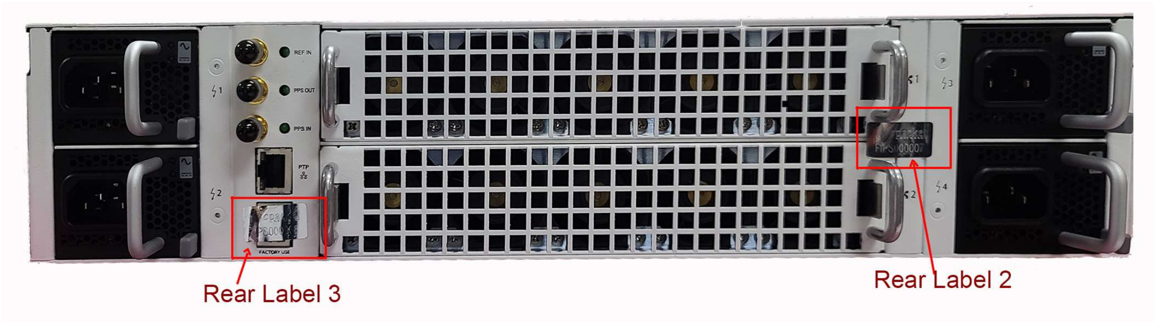

Figure 8 – Tamper-Evident Seal on cVu 16100 Fan Tray Assemblies and Chassis (Rear Label 2)

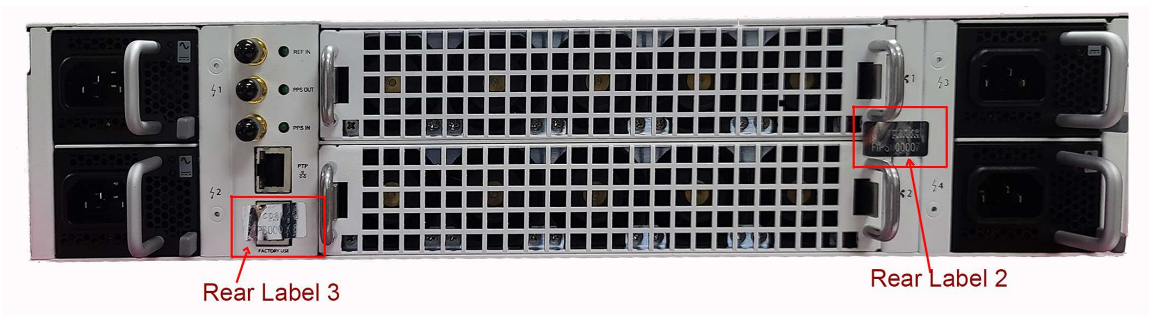

Figure 9 – Tamper-Evident Seal on cVu 16100 Factory Use Port (Rear Label 3)

2.6 Operational Environment

The module employs a non-modifiable operating environment. The cPacket cVu firmware is executed by the module's Intel Xeon D-1541 processor.

The operational environment of the module does not provide a general-purpose OS[54] to the operator. The operational environment is not modifiable by the operator, and only the module's signed image can be executed. All firmware upgrades are digitally signed, and a conditional self-test (2048-bit RSA signature verification) is performed during each upgrade. If the signature test fails, the upgrade process is aborted, and the current firmware remains loaded.

NOTE: Only FIPS-validated firmware may be loaded to maintain the module's validation.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 8.

[54] OS – Operating System

Table 8 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
AES GCM IV	96-bit value	Constructed (external to the AES-GCM implementation but internal to the module boundary) per TLS and SSH protocol specifications	Never exits the module	Plaintext in volatile memory	Reboot, power cycle	IV value for AES GCM encryption in TLS and SSH protocols
Diffie-Hellman Private Key	224/256-bit DH private key	Generated internally via Approved DRBG (per FIPS PUB 186-4)	Never exits the module	Plaintext in volatile memory	Upon session termination Reboot, power cycle	Key agreement within TLS protocol
Diffie-Hellman Public Key	2048-bit DH public key	[for the module] Generated internally via Approved DRBG (per FIPS PUB 186-4) [for a peer[55]] Generated externally and entered in plaintext	[for the module] Exits the module in plaintext form [for a peer] Never exits the module	Plaintext in volatile memory	Upon session termination Reboot, power cycle	Key agreement within TLS protocol
ECDH Private Component	Private component of ECDH: B-233, B-283, B-409, B-571 K-233, K-283, K-409, K-571 P-224, P-256, P-384, P-521	Generated internally via Approved DRBG (per FIPS PUB 186-4)	Never exits the module	Plaintext in volatile memory	Upon session termination Reboot, power cycle	Generation of SSH and TLS shared secrets
ECDH Public Component	Public component of ECDH: B-233, B-283, B-409, B-571 K-233, K-283, K-409, K-571 P-224, P-256, P-384, P-521	Generated via Approved DRBG (per FIPS PUB 186-4) [for a peer] Generated externally and entered in plaintext	Exits in plaintext form [for a peer] Never exits the module	Plaintext in volatile memory	Upon session termination Reboot, power cycle	Generation of SSH and TLS shared secrets
SSH Private Key	2048/3072/4096-bit RSA private key	Generated via Approved DRBG (per FIPS PUB 186-4)	Never exits the module	Plaintext in volatile memory	Factory restore	Authentication during SSH session negotiation
SSH Public Key	2048/3072/4096-bit RSA public key	Generated internally via Approved DRBG (per FIPS PUB 186-4)	Exits the module in plaintext form	Plaintext in volatile memory	Factory restore	Authentication during SSH session negotiation

[55] "Peer" refers to the management workstation.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SSH Shared Secret	256-bit shared secret	Established internally via ECDH shared secret computation	Never exits the module	Plaintext in volatile memory	Upon session termination Reboot, power cycle	Derivation of the SSH Session Key and SSH Authentication Key
SSH Session Key	128/192/256-bit AES CTR key 128/256-bit AES GCM key	Derived internally via SSH KDF	Never exits the module	Plaintext in volatile memory	Upon session termination Reboot, power cycle	Encryption and decryption of SSH session packets
SSH Authentication Key	256/512-bit HMAC key or AES-GCM (for GCM-based cipher suites only) key	Derived internally via SSH KDF	Never exits the module	Plaintext in volatile memory	Upon session termination Reboot, power cycle	Authentication of SSH session packets
TLS Private Key	2048/3072/4096-bit RSA private key ECDSA private key: B-233, B-283, B-409, B-571 K-233, K-283, K-409, K-571 P-224, P-256, P-384, P-521	Generated externally and imported in PEM file format via Web UI (RSA/ECDSA)	Never exits the module	Plaintext in volatile memory	Factory restore	TLS authentication
TLS Public Key	2048/3072/4096-bit RSA public key ECDSA public key: B-233, B-283, B-409, B-571 K-233, K-283, K-409, K-571 P-224, P-256, P-384, P-521	Generated externally and imported in PEM file format via Web UI (RSA/ECDSA)	Exits the module in plaintext form	Plaintext in volatile memory	Factory restore	TLS authentication
TLS Master Secret	256/384-bit shared secret DH/ECDH shared secret	Established internally via DH/ECDH shared secret computation	Never exits the module	Plaintext in volatile memory	Upon session termination Reboot, power cycle	Derivation of the TLS Session Key and TLS Authentication Key
TLS Session Key	128/256-bit AES GCM key	Derived internally using the TLS Master Secret via TLS KDF	Never exits the module	Plaintext in volatile memory	Upon session termination Reboot, power cycle	Encryption and decryption of TLS session packets
TLS Authentication Key	256/384-bit HMAC key	Derived internally using the TLS Master Secret via TLS KDF	Never exits the module	Plaintext in volatile memory	Upon session termination Reboot, power cycle	Authentication of TLS session packets

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
DRBG Seed	384-bit value	Generated internally using entropy input string	Never exits the module	Plaintext in volatile memory	Reboot, power cycle	Seeding material for DRBG
Entropy Input String	256-bit string	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot, power cycle	Entropy material for SP 800-90A DRBG
DRBG Key Value	Internal DRBG state value	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot, power cycle	Random number generation
DRBG 'V' Value	Internal DRBG state value	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot, power cycle	Random number generation
Operator Password	Alphanumeric string Minimum of ten (10) characters	Input electronically in ciphertext via Web UI or REST API over TLS session OR Input electronically in ciphertext via CLI over SSH (CO only) OR Input electronically in plaintext via serial console port (CO only)	Never exits the module	Hashed in non-volatile memory	Factory restore	Authentication to the module
Firmware Load Authentication Key	2048-bit RSA public key	Hard coded key preloaded at the factory	Never exits the module	Plaintext in non-volatile memory	Not zeroized	Verifying the RSA signature of the digest of a new software load package
SNMP Authentication Password	Eight characters minimum	Input electronically in ciphertext via Web UI over TLS session	Never output from module	Obfuscated with SHA2-256 hash in non-volatile memory	Factory restore	Deriving the SNMP Authentication Key
SNMP Encryption Password	Eight characters minimum	Input electronically in ciphertext via Web UI over TLS session	Never output from module	Obfuscated with SHA2-256 hash in non-volatile memory	Factory restore	Deriving the SNMP Encryption Key

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SNMP Encryption Key	AES 128/192/256-bit CFB128 key	Derived internally using SNMP KDF	Never output from module	Plaintext in volatile memory	End SNMP session, power cycle	Encryption/Decryption for SNMP
SNMP Authentication Key	HMAC SHA-1/SHA2-224/SHA2-256/SHA2-384-SHA2-512 key	Derived internally using SNMP KDF	Never output from module	Plaintext in volatile memory	End SNMP session, power cycle	Message authentication for SNMP

The AES-GCM IV is constructed for use with industry-standard protocols as follows:

- TLS 1.2 – When used with TLS, the AES-GCM IV is generated in compliance with *RFC 5288 - AES Galois Counter Mode (GCM) Cipher Suites for TLS* and section 8.2.1 *of NIST SP 800-38D*. When the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, the module will trigger a handshake to establish a new encryption key. The module supports the GCM cipher suites specified in section 3.3.1 of *NIST SP 800-52rev2*. When an AES GCM IV constructed in compliance with the TLS 1.2 protocol, that IV is only used in the context of the AES GCM mode encryption within TLS 1.2 protocol (as described in *RFC 5116*, *RFC 5246*, *RFC 5288*, and *RFC 5289*).

- SSHv2 – When used with SSH, the AES-GCM IV is generated in compliance with *RFC 5647 - AES Galois Counter Mode for the Secure Shell Transport Layer Protocol* and section 8.2.1 *of NIST SP 800-38D*. When an AES GCM IV constructed in compliance with the SSHv2 protocol, that IV is only used in the context of the AES GCM mode encryption within the SSHv2 protocol (as described in *RFC 4252*, *RFC 4253*, and *RFC 5647*).

2.8 EMI / EMC

The module was tested and found to be conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2.9 Self-Tests

Self-tests are performed by the module when the module is first powered up and initialized, as well as during module operation when certain conditions exist. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

2.9.1 Power-Up Self-Tests

The module performs the following self-tests at power-up to verify the integrity of the firmware image and the correct operation of the FIPS-Approved algorithm implementations:

- Firmware Integrity Tests:
    - cPacket application software – using a 256-bit Error Detection Code (based on SHA2-256)
    - OpenSSL libraries – using an HMAC SHA2-256 digest

- Cryptographic algorithm tests:
    - AES ECB encrypt and decrypt KATs[56] (128 bits)
    - AES GCM encrypt and decrypt KATs (256 bits)
    - SHA KATs (SHA-1, SHA2-512)
    - SHA3-256 KAT
    - CTR DRBG KAT
    - RSA sign/verify KAT (2048 bits, PKCS#1 v1.5 scheme and SHA2-256)
    - ECDSA sign/verify PCT (P-256/K-233 curves and SHA2-256)
    - FFC DH Primitive "Z" Computation KAT (2048 bits)

[56] KAT – Known Answer Test

  - ECC CDH Primitive “Z” Computation KAT (P-256 curve)
  - SSH v2 KDF KAT
  - TLS v1.2 KDF KAT

Per FIPS 140-2 IG 9.2, since the module performs an HMAC SHA2-256 KAT, an explicit KAT for SHA2-256 is not required.

Per FIPS 140-2 IG 9.4, since the testing of AES-GCM and AES-ECB covers both authenticated encryption functions as well as forward and inverse cipher functions, explicit KATs for the other supported modes of AES are not required.

Per FIPS 140-2 IG 9.4, since the implementations for SHA-1, SHA2-256, and SHA2-512 are tested by existing power-up KATs, explicit KATs for SHA2-224 and SHA2-384 are not required.

2.9.2 Conditional Self-Tests

The module performs the following conditional self-tests:

- Firmware Load Test using 2048-bit RSA signature verification with SHA2-256
- RSA sign/verify PCT (2048-bits, SHA2-256)
- Stuck Test on entropy source
- Repetition Count Test on entropy source
- Adaptive Proportion Test on entropy source
- Lag Predictor Test on entropy source

2.9.3 Critical Functions Self-Tests

The module performs health checks for the DRBG’s Generate, Instantiate, and Reseed functions as specified in section 11.3 of *NIST SP 800-90Arev1*. These tests are performed as power-up tests. Entropy start-up tests as described in section 4.2 of *NIST SP 800-90B* are also performed at module power-up.

2.9.4 Self-Test Failure Handling

On failure of a conditional firmware load self-test, the module transitions to a soft error state. The upgrade process is automatically aborted, and no changes are made to the module firmware. An error is written to the Web UI and audit log, the error state is cleared, and the module then resumes normal operation with the currently loaded firmware.

If the module fails any other self-test, the module enters a “Critical” error state and logs the error. All access to the cryptographic functionality and CSPs is disabled. All data outputs via data output interfaces are inhibited and cryptographic operations are halted. The only action available from this state is to power-cycle the module to trigger the re-execution of the power-up self-tests.

To exit the critical error state, the CO shall power cycle the appliance. The error condition is considered to have been cleared if the module successfully passes all of the subsequent power-up self-tests. If the module continues to fail subsequent power-up self-tests, the module is considered to be malfunctioning or compromised, and the module should be sent to cPacket for repair or replacement.

2.9.5 Other Assurances

The module performs assurances for its key agreement schemes as specified in the following sections of *NIST SP 800-56Arev3:*

- Section 5.5.2 (for assurances of domain parameter validity)
- Section 5.6.2.1 (for assurances required by the key pair owner)
- Section 5.6.2.2 (for assurances required by the key pair recipient)

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to provide additional mitigation mechanisms beyond those required for the FIPS 140-2 Level 2 validation.

3. Secure Operation

The sections below describe how to place and keep the module in the FIPS-approved mode of operation. **Any operation of the module without following the guidance provided below will result in non-compliant use and is outside the scope of this Security Policy.**

3.1 Installation and Configuration

The CO shall be responsible for receiving, installing, initializing, and maintaining the cVu 16100 appliance. To operate the module in the Approved mode, the CO shall configure the module via the Web UI or serial console as directed by this Security Policy. The following sections provide the CO with important instructions and guidance for the secure installation and configuration of the cVu 16100 appliance.

3.1.1 Physical Inspection

For the module to be considered running in its FIPS-Approved mode of operation, the factory-installed tamper-evident seals must be in place as specified in section 2.5. Upon receipt, the CO shall inspect the module to ensure the tamper-evident seals have been properly installed.

3.1.2 Initial Setup

Upon receiving the cVu 16100 hardware, the CO shall check that the system is not damaged and that all required parts and instructions are included. The CO shall check to ensure that none of the tamper-evident seals (as described in section 2.5) have been altered. If any of the seals are altered, do not use the appliance, and contact cPacket Customer Support immediately for guidance.

The CO shall refer to section 2 "Installation" of the *cPacket Networks cVu 16100, cVu 8100, and cVu 4100 User Guide* for general installation instructions.

3.1.3 Network Configuration and Settings

The next step is to confirm general network connectivity and configuration through a web browser, as instructed in section 5 "Startup" of the *cPacket Networks cVu 16100, cVu 8100, and cVu 4100 User Guide*. The CO shall login to the Web UI with the default credentials supplied by cPacket.

3.1.4 Serial Console Authentication

The CO must configure the serial console to enforce authentication as follows:

1. Login to the Web UI.
2. Select **Config/Status**.
3. Select **Advanced → Serial console**.

4. Set **Enable Authentication Support** to "Yes" and click "Save".

After this step, serial console restarts and asks for username.

3.1.5 Certificates

The CO must replace the default appliance server certificate with a new ECDSA or RSA certificate as follows:

1. Login to the Web UI.
2. Select **Config → User Mgmt → Certificates**.
3. Paste in an ECDSA or RSA certificate and corresponding private key.
4. Click "Save".

3.1.6 Password Policy

The module allows for the configuration of the password policy that dictates the content and quality of the passwords used to access the module. The default password policy is set as follows:

- Minimum Unique Uppercase Letters: 1
- Minimum Unique Lowercase Letters: 1
- Minimum Unique Digits: 1
- Minimum Unique "Non Alpha Numerics" (special characters): 1
- Minimum Length: 10

The CO must ensure that the password policy is configured with the settings above by navigating to **Config → User Mgmt → Policies** on the Web UI. If any changes are made, the CO must click the "Save" button when done.

More stringent policy settings can be configured at the CO's discretion.

3.1.7 Default Operator Passwords

The module provides default passwords for initial module access. The CO shall ensure that all default passwords are changed immediately after their initial use. This is performed via the Web UI by navigating to **Config → User Mgmt → Users**, modifying the password, and clicking on the "Save" button.

Administrator-level users can also be added and deleted from the cVu's serial console with the *users_add* and *users_delete* commands.

Note that modifying GUI password changes serial console passwords as well.

3.1.8 FIPS-Approved Mode Configuration

When configured by following the installation and configuration procedures above, the module only operates in a FIPS-Approved mode. Thus, the current status of the module when operational is always in the FIPS-Approved mode.

3.2 Crypto Officer Guidance

The CO is responsible for initialization and security-relevant configuration and management of the module.

3.2.1 Management

Once installed and configured, the CO is responsible for maintaining and monitoring the status of the module to ensure that it is running in its FIPS-Approved mode. Please refer to Section 3.1.8 for guidance that the Crypto Officer must follow for the module to be considered running in a FIPS-Approved mode of operation.

3.2.2 Zeroization

Please refer to Table 8 for the key zeroization techniques and the applicable keys. All ephemeral keys and CSPs can be zeroized by power-cycling the module. In addition, protocol session (i.e., TLS, SSH, SNMP) keys will automatically be zeroized at the end of the protocol session.

Persistently-stored keys and CSPs can be zeroized by restoring the module to factory defaults using the **Factory Restore** menu item from the Web UI.

3.2.3 Restore to Factory State

The module is restored to factory defaults by logging into the Web UI as a CO and navigating to this link:

```
https:\\<Device hostname or IP address>\factory_restore
```

3.2.4 Firmware Updates

Firmware updates are performed by logging into the Web UI as a CO and navigating to **Config/Status → Advanced → Update**.

3.2.5 Tamper-Evident Seal Application and Periodic Inspection

If a CO needs to replace a tamper-evident seal over the life-cycle of the module, the new tamper-evident seal must be applied as follows:

- Log the position and serial number of any seal to be replaced as well as the serial number of the replacement seal.
- Clean the appliance surface with isopropyl alcohol in the area where the seal will be placed and let dry.
- Apply the seal firmly to the target surface as shown in Figures 6-9.
- After applying the seal, allow at least 24 hours for the label adhesive to cure.

The CO is also responsible for the following:

- Securing and having control at all times of any unused seals

- Direct control and observation of any changes to the appliance where the seals are removed or installed to ensure that the security of the appliance is maintained during such changes and that the appliance is returned to its Approved state

The CO is also required to periodically inspect the module for evidence of tampering at intervals specified per end-user policy. The CO must visually inspect the tamper-evident seals for tears, rips, dissolved adhesive, and other signs of tampering. If evidence of tampering is found during periodic inspection, the CO must take the device out of operation and contact cPacket Customer Support.

Six spare seals are shipped with the module. If a customer requires additional seals, they may contact cPacket customer support to place an order using part number LBL0040.

3.3 User Guidance

The User does not have the ability to configure sensitive information on the module, except for their password. The User must be diligent to pick strong passwords and must not reveal their password to anyone.

3.4 Additional Guidance and Usage Policies

This section notes additional policies below that must be followed by module operators:

- The CO shall power-cycle the module if the module has encountered a critical error and becomes non-operational. If power cycling the module does not correct the error condition, the module is considered to be compromised or malfunctioned and should be sent back to cPacket for repair or replacement.

- For FIPS mode operation, SNMP v2 shall not be used. When configuring SNMP v3 settings, the CO shall select SHA (and not MD5) for the Auth Protocol and AES (and not DES or DES3) for the Privacy Protocol.

- For FIPS mode operation, only local authentication shall be used. TACACS and RADIUS shall not be used.

- Only RSA certificates with key lengths greater than or equal to 2048-bits shall be loaded into the Web UI.

- The module allows for the loading of new firmware and employs an Approved message authentication technique to test its integrity. However, to maintain an Approved mode of operation, the CO must ensure that only FIPS-validated firmware is loaded. Any firmware/software 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.

4. Acronyms and Abbreviations

Table 9 provides definitions for the acronyms and abbreviations used in this document.

Table 9 – Acronyms and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CLI	Command Line Interface
CMAC	Cipher-Based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
CSR	Certificate Signing Request
CTR	Counter
CVL	Component Validation List
DH	Diffie-Hellman
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
ENT (NP)	Entropy (Non-Physical)
FFC DH	Finite Field Cryptography Diffie-Hellman
FIPS	Federal Information Processing Standard

Term	Definition
GbE	Gigabit Ethernet
GCM	Galois/Counter Mode
GHz	Gigahertz
GUI	Graphical User Interface
HDD	Hard Disk Drive
HMAC	(keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IV	Initialization Vector
KAS	Key Agreement Scheme
KAS-ECC-SSC	Key Agreement Scheme - Elliptic Curve Cryptography - Shared Secret Computation
KAS-FFC-SSC	Key Agreement Scheme - Finite Field Cryptography - Shared Secret Computation
KAT	Known Answer Test
KDF	Key Derivation Function
KPG	Key Pair Generation
KTS	Key Transport Scheme
N/A	Not Applicable
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PCT	Pairwise Consistency Test
PKCS	Public Key Cryptography Standard
PKG	Public Key (Q) Generation
PKV	Public Key (Q) Validation
PPS	Pulse-Per-Second
PSS	Probabilistic Signature Scheme
PTP	Precision Time Protocol
PUB	Publication
PSU	Power Supply Unit
QSFP28	Quad Small Form-Factor Pluggable 28
QSFP+	Quad Small Form-Factor Pluggable Plus
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
REST	Representational State Transfer

Term	Definition
RFC	Request for Comment
RJ-45	Registered Jack-45
RSA	Rivest Shamir Adleman
SATA	Serial Advanced Technology Attachment
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
SP	Special Publication
SSH	Secure Shell
SSL	Secure Socket Layer
TACACS+	Terminal Access Controller Access-Control System Plus
TLS	Transport Layer Security
U	Rack Unit
UI	User Interface
U.S.	United States

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com