FIPS 140-2 Non-Proprietary Security Policy

Acme Packet 6300

FIPS 140-2 Level 1 Validation

Hardware Version: 6300

Firmware Version: E-CZ8.0.0

Date: July 17th, 2018

Title: Acme Packet 6300 Security Policy
Date: July 17th, 2018
Author: Acumen Security, LLC.
Contributing Authors:
Oracle Communications Engineering
Oracle Security Evaluations – Global Product Security

Oracle Communications is a Global Business Unit (GBU) of Oracle Corporation

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.
Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com


Oracle is committed to developing practices and products that help protect the environment

ORACLE

TABLE OF CONTENTS

Section	Title	Page
1.	**Introduction**	**1**
1.1	Overview	1
1.2	Document Organization	1
2.	**Acme Packet 6300**	**2**
2.1	Functional Overview	2
3.	**Cryptographic Module Specification**	**3**
3.1	Definition of the Cryptographic Module	3
3.2	FIPS 140-2 Validation Scope	3
3.3	Approved or Allowed Security Functions	4
3.4	Non-Approved But Allowed Security Functions	5
3.5	Non-Approved Security Functions	6
4.	**Module Ports and Interfaces**	**7**
5.	**Physical Security**	**9**
6.	**Roles and Services**	**10**
6.1	Operator Services and Descriptions	10
6.2	Unauthenticated Services and Descriptions	13
6.3	Operator Authentication	13
6.3.1	Crypto-Officer: Password-Based Authentication	13
6.3.2	User: Certificate-Based Authentication	14
6.4	Key and CSP Management	14
7.	**Self-Tests**	**20**
7.1	Power-Up Self-Tests	20
7.1.1	Firmware Integrity Test	20
7.1.2	Mocana Self-Tests	20
7.1.3	Firmware Self-tests	20
7.1.4	Nitrox Self-tests	20
7.1.5	Octeon Self-tests	20
7.2	Critical Functions Self-Tests	21
7.3	Conditional Self-Tests	21
8.	**Crypto-Officer and User Guidance**	**22**
8.1	Secure Setup and Initialization	22
8.2	AES-GCM IV Construction/Usage	23
9.	**Mitigation of other attacks**	**24**
10.	**Appendices**	**25**
10.1	Acronyms, Terms and Abbreviations	25
10.2	References	26

ORACLE

List of Tables

Table 1: FIPS 140-2 Security Requirements....3
Table 2: FIPS Approved or Allowed Security Functions....5
Table 3: Non-Approved but Allowed Security Functions....6
Table 4: Non-Approved Disallowed Functions....6
Table 5 – Mapping of FIPS 140 Logical Interfaces to Physical Ports....7
Table 6 – Physical Ports....8
Table 7 – Service Summary....10
Table 8 – Operator Services and Descriptions....12
Table 9 – Operator Services and Descriptions....13
Table 10 – Crypto-Officer Authentication....14
Table 11 – Crypto-Officer Authentication....14
Table 12 – CSP Table....19
Table 13 – Acronyms....25
Table 14 – References....26

List of Figures

Figure 1: Acme Packet 6300....3
Figure 2: Acme Packet 6300 – Front View....8
Figure 3: Acme Packet 6300 – Rear View....8

1. Introduction

1.1 Overview

This document is the Security Policy for the Acme Packet 6300 appliance manufactured by Oracle Communications. Acme Packet 6300 is also referred to as "the module or module". This Security Policy specifies the security rules under which the module shall operate to meet the requirements of FIPS 140-2 Level 2. It also describes how the Acme Packet 6300 appliance function in order to meet the FIPS requirements, and the actions that operators must take to maintain the security of the modules.

This Security Policy describes the features and design of the Acme Packet 6300 module using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST/CSEC Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

1.2 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Oracle Non-Proprietary Security Policy
- Oracle Vendor Evidence document
- Finite State Machine
- Entropy Assessment Document
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Oracle and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Oracle.

2. Acme Packet 6300

2.1 Functional Overview

The Acme Packet 6300 appliance are specifically designed to meet the unique price performance and manageability requirements of the small to medium sized enterprise and remote office/ branch office. Ideal for small site border control and Session Initiation Protocol (SIP) trunking service termination applications, the Acme Packet 6300 appliance deliver Oracle's industry leading ESBC capabilities in a small form factor appliance. With support for high availability (HA) configurations, hardware assisted transcoding and Quality of Service (QoS) measurement, the Acme Packet 6300 appliance are a natural choice when uncompromising reliability and performance are needed in an entry-level appliance. With models designed for the smallest branch office to the largest data center, the Acme Packet ESBC product family supports distributed, centralized, or hybrid SIP trunking topologies.

Acme Packet 6300 appliance address the unique connectivity, security, and control challenges enterprises often encounter when extending real-time voice, video, and UC sessions to smaller sites. The appliances also helps enterprises contain voice transport costs and overcome the unique regulatory compliance challenges associated with IP telephony. TDM fallback capabilities ensure continuous dial out service at remote sites in the event of WAN or SIP trunk failures. Stateful high availability configurations protect against link and hardware failures. An embedded browser based graphical user interface (GUI) simplifies setup and administration

3. Cryptographic Module Specification

3.1 Definition of the Cryptographic Module

The module consists of the Acme Packet 6300 appliance running firmware version E-CZ8.0.0 on hardware platform 6300. The module is classified as a multi-chip standalone cryptographic module. The physical cryptographic boundary for the Acme Packet 6300 is all components with exception of the removable power supplies.

A representation of the cryptographic boundary is defined below:

Figure 1: **Acme Packet 6300**

3.2 FIPS 140-2 Validation Scope

The Acme Packet 6300 appliance are being validated to overall FIPS 140-2 Level 1 requirements. See Table 1 below.

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles and Services and Authentication	2
Finite State Machine Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 1: FIPS 140-2 Security Requirements

3.3 Approved or Allowed Security Functions

The Acme Packet 6300 appliance contain the following FIPS Approved Algorithms listed in Table 2:

Approved or Allowed Security Functions		Certificate
Symmetric Algorithms		
AES	Firmware: (CBC, ECB, CTR, GCM); Encrypt/Decrypt; Key Size = 128, 256	5247
	Mocana: (CBC); Encrypt/Decrypt; Key Size = 128, 256	5248
	Cavium Nitrox : (CBC); Encrypt/Decrypt; Key Size = 128, 256	5257
	Cavium Octeon: (ECB, CTR); Encrypt/Decrypt; Key Size = 128	5256
Triple DES[1]	Firmware: (CBC); Encrypt/Decrypt; Key Size = 192	2655
	Mocana: (CBC); Encrypt/Decrypt; Key Size = 192	2656
	Cavium Nitrox: (CBC); Encrypt/Decrypt; Key Size = 192	2659
Key Transport		
KTS	Mocana: AES and HMAC. Key establishment methodology provides 128 or 256 bits of encryption strength	5248 3475
KTS	Firmware: AES and HMAC. Key establishment methodology provides 128 or 256 bits of encryption strength	5247 3474
Secure Hash Standard (SHS)		
SHS	Firmware: SHA-1, SHA-256, SHA-384	4225
	Mocana: SHA-1, SHA-256[2]	4226
	Cavium Octeon: SHA-1, SHA-256, SHA-384, SHA-512	2023
Data Authentication Code		
HMAC	Firmware: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384[3]	3474
	Mocana: HMAC-SHA-1, HMAC-SHA-256	3475
	Cavium Octeon: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512[4]	1455
Asymmetric Algorithms		
RSA	Firmware: RSA: FIPS186-4: Public Key Exponent: Fixed (10001) Probable Random Primes: Mod lengths: 2048 (bits) Signature Generation 9.31: Mod 2048 SHA: SHA-1, SHA-256, SHA-384	2806

1 Per IG A.13 the same Triple-DES key shall not be used to encrypt more than 2^20 64-bit blocks of data.

2 SHA-256 in SHS Cert. #4226 was CAVP tested; however it is not utilized by any service

3 HMAC-SHA-256, HMAC-SHA-384 in HMAC Cert. #3474 were CAVP tested; however it is not utilized by any service

4 HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 in HMAC Cert. #1455 were CAVP tested; however it is not utilized by any service

Approved or Allowed Security Functions		Certificate
	Signature Verification 9.31: Mod 2048 SHA: SHA-1, SHA-256, SHA-384 RSA: FIPS186-2 Signature Generation 9.31: Modulus lengths: 4096 SHAs: SHA-256, SHA-384 Signature Verification 9.31: Modulus lengths: 2048, 4096 SHAs: SHA-1, SHA-256, SHA-384	
	Mocana: RSA: 186-4: Public Key Exponent: Fixed (10001) Probable Random Primes: Mod lengths: 2048 (bits) Primality Tests: C.2 Signature Verification PKCS1.5: Mod 1024 SHA: SHA-1 Mod 2048 SHA: SHA-1	2807
ECDSA	Firmware: FIPS186-4: PKG: CURVES (P-256 P-384 Testing Candidates) SigGen: CURVES (P-256: (SHA-256, 384) P-384: (SHA-256, 384) SigVer: CURVES (P-256: (SHA-256, 384) P-384: (SHA-256, 384))	1366
Random Number Generation		
DRBG	Firmware: CTR_DRBG: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256)] Hash_Based DRBG: [Prediction Resistance Tested: Not Enabled (SHA-1)	2007
Key Establishment		
Key Derivation CVL	Firmware: SNMP KDF, SRTP KDF, TLS KDF	1720
	Mocana: IKEv1[5] KDF, SSH KDF	1721
	Cavium Octeon: SRTP KDF	1727
CVL	Cavium Nitrox: NIST SP 800-56A Section 7.1.2 RSADP, Mod Size 2048	1728
Key Generation		
Cryptographic Key Generation (CKG)	Firmware: [SP 800-133] CKG	Vendor affirmed

Table 2: FIPS Approved or Allowed Security Functions

3.4 Non-Approved But Allowed Security Functions

The following are considered non-Approved but allowed security functions:

[5] IKEv1 KDF was CAVP tested; however it is not utilized by any service. IKE and IPSec shall not be used in the Approved mode of operation as stated in Section 8.1

Algorithm	Usage
EC-Diffie-Hellman	CVL Certs. #1720, #1721 and #1727, key agreement; key establishment methodology provides 128 or 192 bits of encryption strength
Diffie-Hellman	CVL Certs. #1720, #1721 and #1727, key agreement; key establishment methodology provides 112 bits of encryption strength
MD5	TLS 1.0, 1.1 KDF
RSA Key Wrapping	CVL Certs. #1720 and #1721, key wrapping, key establishment methodology provides 112-bits of encryption strength
NDRNG	Used for seeding the NIST SP 800-90A Hash_DRBG and CTR_DRBG. Per FIPS 140-2 IG 7.14 scenario 1 (a). The module provides a minimum of 440 bits of entropy input for the Hash_DRBG. The input length for the CTR DRBG depends on the size of the AES key used. If the AES key length is 128 bits, the seed size is 256 bits. If the AES key length is 256 bits, then the seed size is 384 bits.

Table 3: Non-Approved but Allowed Security Functions

3.5 Non-Approved Security Functions

The following services are considered non-Approved and may not be used in a FIPS-approved mode of operation:

Service	Non-Approved Security Functions
SSH	Asymmetric: DSA, Symmetric: Rijndael
SNMP	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES
IKEv1	IKEv1 Key Derivation Function
Diffie-Hellman	Key agreement, less than 112 bits of encryption strength.
RSA Key Wrapping	Key wrapping, less than 112 bits of encryption strength.

Table 4: Non-Approved Disallowed Functions

Services listed in the previous table make use non-compliant cryptographic algorithms. Use of these algorithms are prohibited in a FIPS-approved mode of operation. These services are allowed in FIPS mode when using allowed algorithms (as specified in section 8.1).

ORACLE

4. Module Ports and Interfaces

The table below provides the mapping of ports as per FIPS 140-2 Standard.

Logical Interface	Physical Port 6300	Information Input/Output
Data Input	Ethernet Ports (Slot 0 P0,1 and Slot 1 P0,1) Ethernet MGT Ports (Mgmt0, Mgmt1, Mgmt2)	Cipher text Plain text
Data Output	Ethernet Ports (Slot 0 P0,1 and Slot 1 P0,1) Ethernet MGT Ports (Mgmt0, Mgmt1, Mgmt2)	Cipher text Plain text
Control Input	Console Port Reset Button Power Switch Ethernet Ports (Slot 0 P0,1 and Slot 1 P0,1) Ethernet MGT Ports (Mgmt0, Mgmt1, Mgmt2)	Plaintext control input via console port (configuration commands, operator passwords) Ciphertext control input via network management (EMS control, CDR accounting, CLI management)
Status Output	Console Port Alarm Port Ethernet MGT Ports (Mgmt0, Mgmt1, Mgmt2) LEDs LCD	Plaintext status output via console port. Ciphertext status output via network management
Power	Power Plug	N/A

Table 5 – Mapping of FIPS 140 Logical Interfaces to Physical Ports

The table below describes the interfaces on the Acme 6300 appliance.

Physical Interface	Number of Ports 6300	Description / Use
Console Port	1	Provides console access to the module. The module supports only one active serial console connection at a time. Console port communication is used for administration and maintenance purposes from a central office (CO) location. Tasks conducted over a console port include: • Configuring the boot process and management network • Creating the initial connection to the module • Accessing and using functionality available via the ACLI • Performing in-lab system maintenance (services described below) • Performing factory-reset to zeroize nvram and keys

Alarm Port	1	Provides status output
USB Ports	1	This port is used for recovery. e.g. system re-installation after zeroization.
Management Ethernet ports	3 Mgmt0, Mgmt1, Mgmt2	Used for EMS control, CDR accounting, CLI management, and other management functions
Signaling and Media Ethernet ports	4 Slot 0 P0,1 and Slot 1 P0,1	Provide network connectivity for signaling and media traffic. These ports are also used for incoming and outgoing data (voice) connections.

Table 6 – Physical Ports

Figure 2: Acme Packet 6300 – Front View

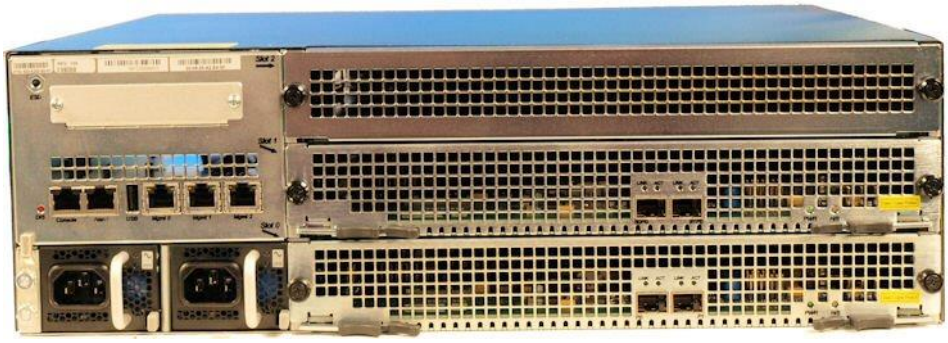

Figure 3: Acme Packet 6300 – Rear View

5. Physical Security

The cryptographic module includes the following physical security mechanisms:

- Production-grade components

6. Roles and Services

As required by FIPS 140-2 Level 2, there are three roles (a Crypto Officer Role, User Role, and Unauthenticated Role) in the module that operators may assume. The module supports role-based authentication, and the respective services for each role are described in the following sections. The below table gives a high level description of all services provided by the module and lists the roles allowed to invoke each service.

Operator Role	Summary of Services
User	• View configuration versions and system performance data • Handle certificate information for TLS functions • Test pattern rules, local policies, and session translations • Display system alarms. • Set the display dimensions for the terminal • Connect to module for data transmission
Crypto-Officer	Allowed access to all system commands and configuration privileges
Unauthenticated	• Request Authentication • Show Status • Initiate self-tests

Table 7 – Service Summary

6.1 Operator Services and Descriptions

The below table provides a full description of all services provided by the module and lists the roles allowed to invoke each service.

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
	X	Configure	Initializes the module for FIPS mode of operation	Bypass Key (HMAC-SHA-256)	R, W, X
	X	Zeroize CSP's	Clears keys/CSPs from memory and disk	All CSP's	Z
	X	Firmware Update	Updates firmware	Firmware Integrity Key (RSA)	R, X
	X	Bypass	Configure bypass using TCP or UDP and viewing bypass service status	Bypass Key (HMAC-SHA-256)	R, W, X
X	X	Decrypt	Decrypts a block of data Using AES or Triple-DES in FIPS Mode in support of a SNMP, SRTP, SSH and/or TLS session	TLS Session Keys (Triple-DES) TLS Session Keys (AES128) TLS Session Keys (AES256)	X X X

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
				SSH Session Key (Triple-DES) SSH Session Key (AES128) SSH Session Key (AES256) SRTP Session Key (AES-128) SNMP Privacy Key (AES-128)	X X X X X
X	X	Encrypt	Encrypts a block of data Using AES or Triple-DES in FIPS Mode in support of a SNMP, SRTP, SSH and/or TLS session	TLS Session Keys (Triple-DES) TLS Session Keys (AES128) TLS Session Keys (AES256) SSH Session Key (Triple-DES) SSH Session Key (AES128) SSH Session Key (AES256) SRTP Session Key (AES-128) SNMP Privacy Key (AES-128	X X X X X X X X
X	X	Generate Keys	Generates AES or Triple-DES keys for encrypt/decrypt operations. Generates Diffie-Hellman, EC Diffe-Hellman, ECDSA and RSA keys for key transport/key establishment in support of a SNMP, SRTP, SSH and/or TLS session	TLS Session Keys (Triple-DES) TLS Session Keys (AES128) TLS Session Keys (AES256) SSH Session Key (Triple-DES) SSH Session Key (AES128) SSH Session Key (AES256) SRTP Session Key (AES-128) SNMP Privacy Key (AES-128) Diffie-Hellman Public Key (DH) Diffie-Hellman Private Key (DH) ECDH Public Key (EC DH) ECDH Private Key (EC DH) SNMP Authentication Key (HMAC-SHA1) SRTP Authentication Key (HMAC-SHA1) SSH authentication private Key (RSA) SSH authentication public key (RSA) TLS authentication private Key (ECDSA/RSA) TLS authentication public key (ECDSA/RSA) TLS premaster secret (shared secret) TLS Master secret (shared secret)	R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W R, W

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
				SRTP Master key (AES-128) SSH Integrity Key (HMAC-SHA1) TLS Integrity Key (HMAC-SHA1)	R, W R, W R, W
X	X	Verify	Used as part of the TLS, SSH protocol negotiation	SSH authentication private Key (RSA) SSH authentication public key (RSA) TLS authentication private Key (ECDSA/RSA) TLS authentication public key (ECDSA/RSA) Diffie-Hellman Public Key (DH) Diffie-Hellman Private Key (DH) ECDH Public Key (EC DH) ECDH Private Key (EC DH)	X X X X X X X X X
X	X	Generate Seed	Generate an entropy_input for DRBGs when required for random number generation	DRBG Seed DRBG Entropy Input String	R, W, X
X	X	Generate Random Number	Generate random number.	DRBG C DRBG V DRBG Key	R, W, X R, W, X
X	X	HMAC	Generate HMAC in support of a SNMP, SRTP, SSH and/or TLS session	SNMP Authentication Key (HMAC-SHA1) SRTP Authentication Key (HMAC-SHA1) SSH Integrity Key (HMAC-SHA1) TLS Integrity Key (HMAC-SHA1)	X X X X
X	X	Generate Certificate	Generate certificate for use with the HTTPS web interface	Web Certificate	R, W, X
X	X	Authenticate	Request authentication to an authorized role	Operator Password	R, W, X

R – Read, W – Write, X – Execute, Z - Zeroize

Table 8 – Operator Services and Descriptions

For all other services, see https://docs.oracle.com/cd/E89499_01/index.htm

6.2 Unauthenticated Services and Descriptions

The below table provides a full description of the unauthenticated services provided by the module:

Service Name	Service Description
On-Demand Self-Test Initialization	This service initiates the FIPS self-test when requested.
Show Status	This service shows the operational status of the module
Factory Reset Service	This service restores the module to factory defaults.

Table 9 – Operator Services and Descriptions

6.3 Operator Authentication

6.3.1 Crypto-Officer: Password-Based Authentication

In FIPS-approved mode of operation, the module is accessed via Command Line Interface over the Web UI, Console ports or via SSH or SNMPv3 over the Network Management Ports. Other than status functions available by viewing the Status LEDs, the services described are available only to authenticated operators.

Method	Probability of a Single Successful Random Attempt	Probability of a Successful Attempt within a Minute
Password-Based (CO and User Authentication)	Passwords must be a minimum of 8 characters. The password can consist of alphanumeric values, {a-z, A-Z, 0-9, and special characters], yielding 94 choices per character. The probability of a successful random attempt is 1/94^8, which is less than 1/1,000,000.	Passwords must be a minimum of 8 characters. The password can consist of alphanumeric values, {a-z, A-Z, 0-9, and special characters], yielding 94 choices per character Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one-minute period is 600/94^8, which is less than 1/100,000.
SNMPv3 Passwords	Passwords must be a minimum of 8 characters. The password can consist of alphanumeric values, {a-z, A-Z, 0-9, and special characters], yielding 94 choices per character. The probability of a successful random attempt is 1/94^8, which is less than 1/1,000,000.	Passwords must be a minimum of 8 characters. The password can consist of alphanumeric values, {a-z, A-Z, 0-9, and special characters], yielding 94 choices per character. Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one-minute period is 600/94^8, which is less than 1/100,000.
Password-Based (Challenge Response)	Passwords must be a minimum of 12 numeric characters. 0-9, yielding 10 choices per character. The probability of a successful random attempt is 1/10^12, which is less than 1/1,000,000.	Passwords must be a minimum of 12 numeric characters. 0-9, yielding 10 choices per character. Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one-minute period is 600/10^12, which is less than 1/100,000.

Table 10 – Crypto-Officer Authentication

6.3.2 User: Certificate-Based Authentication

The module also supports authentication via digital certificates for the User Role as implemented by the TLS and SSH protocols. The module supports a public key based authentication with 2048-bit RSA and 2048-bit ECDSA keys.

Method	Probability of a Single Successful Random Attempt	Probability of a Successful Attempt within a Minute
Certificate-Based	A 2048-bit RSA/ECDSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is 1 /2^112, which is less than 1/1,000,000.	Assuming the module can only perform one (1) digital signature verification per second, the probability of a success with multiple consecutive attempts in a one-minute period is 60/2^112, which is less than 1/100,000.

Table 11 – Crypto-Officer Authentication

6.4 Key and CSP Management

The following keys, cryptographic key components and other critical security parameters are contained in the module. No parts of the SSH, SRTP, TLS, or SNMP protocol, other than the KDF, have been tested by the CAVP and CMVP per FIPS 140-2 D.11.

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
Operator Passwords	Generated by the crypto officer as per the module policy	**Agreement:** NA **Entry:** Entry via console or SSH management session **Output:** Output as part of HA direct physical connection	Non Volatile RAM	Authentication of the crypto officer and user
Firmware Integrity Key (RSA (2048 bits))	Generated externally	**Entry:** entered as part of Firmware image **Output:** Output as part of HA direct physical connection	Flash	Public key used to verify the integrity of firmware and updates
DRBG Entropy Input String	Generated internally from hardware sources	**Agreement:** NA **Entry:** NA	Volatile RAM	Used in the random bit generation process

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
		Output: None		
DRBG Seed	Generated internally from hardware sources	**Agreement:** NA **Entry:** NA **Output:** None	Volatile RAM	Entropy used in the random bit generation process
DRBG Key	Internal value used as part of SP 800-90A CTR_DRBG	**Agreement:** NA **Entry:** NA **Output:** None	Volatile RAM	Used in the random bit generation process
DRBG V	Internal value used as part of SP 800-90A DRBG	**Agreement:** NA **Entry:** NA **Output:** None	Volatile RAM	Used in the random bit generation process
DRBG C	Internal value used as part of SP 800-90A Hash_DRBG	**Agreement:** NA **Entry:** NA **Output:** None	Volatile RAM	Used in the random bit generation process
Diffie-Hellman (DH) Public Key	Internal generation by FIPS-approved CTR_DRBG in firmware	**Agreement:** Diffie-Hellman (2048 bits) **Entry:** NA **Output:** None	Volatile RAM	Used to derive the secret session key during DH key agreement protocol
Diffie-Hellman (DH) Private Key	Internal generation by FIPS-approved CTR_DRBG	**Agreement:** Diffie-Hellman (224 bits) **Entry:** NA	Volatile RAM	Used to derive the secret session key during DH key agreement protocol

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
		Output: None		
Elliptic Diffie-Hellman (ECDH) Public Key	Internal generation by FIPS-approved CTR_DRBG in firmware	**Agreement:** EC Diffie-Hellman (P-256 and P-384) **Entry:** NA **Output:** None	Volatile RAM	Used to derive the secret session key during ECDH key agreement protocol
Elliptic Diffie-Hellman (ECDH) Private Key	Internal generation by FIPS-approved CTR_DRBG	**Agreement**: EC Diffie-Hellman (P-256 and P-384) **Entry**: NA **Output**: None	Volatile RAM	Used to derive the secret session key during ECDH key agreement protocol
SNMP Privacy Key (AES-128)	Derived via NIST SP 800-135 KDF	**Agreement**: NIST SP 800-135 KDF **Entry**: NA **Output**: Output as part of HA direct physical connection	Volatile RAM	For encryption / decryption of SNMP session traffic
SNMP Authentication Key (HMAC-SHA1)	Internal generation by FIPS-approved CTR_DRBG in firmware	**Agreement**: NA **Output**: Output as part of HA direct physical connection	Volatile RAM	160-bit HMAC-SHA-1 for message authentication and verification in SNMP
SRTP Master Key (AES-128)	Internal generation by FIPS-approved Hash_DRBG in firmware	**Agreement**: Diffie-Hellman **Entry**: NA **Output**: encrypted or output as part of HA direct physical connection	Volatile RAM	Generation of SRTP session keys

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
SRTP Session Key (AES-128)	Derived via NIST SP 800-135 KDF	**Agreement**: NIST SP 800-135 KDF **Entry**: NA **Output**: Output as part of HA direct physical connection	Volatile RAM	For encryption / decryption of SRTP session traffic
SRTP Authentication Key (HMAC-SHA1)	Derived from the master key	**Agreement**: NA **Output:** Output as part of HA direct physical connection	Volatile RAM	160-bit HMAC-SHA-1 for message authentication and verification in SRTP
SSH Authentication Private Key (RSA)	Internal generation by FIPS-approved CTR_DRBG per FIPS 186-4	**Agreement**: RSA (2048 bits) **Output:** Output as part of HA direct physical connection	Flash Memory	RSA private key for SSH authentication
SSH Authentication Public Key (RSA)	Internal generation by FIPS-approved CTR_DRBG per FIPS 186-4	**Agreement:** RSA (2048 bits) **Output:** Output as part of HA direct physical connection	Flash Memory	RSA public key for SSH authentication.
SSH Session Keys (Triple-DES, AES-128, AES-256)	Derived via NIST SP 800-135 KDF Note: These keys are generated via SSH (IETF RFC 4251). This protocol enforces limits on the number of total possible encryption/decryption operations.	**Agreement**: Diffie-Hellman	Volatile RAM	Encryption and decryption of SSH session
SSH Integrity Keys (HMAC-SHA1 and HMAC-SHA-256)	Derived via NIST SP 800-135 KDF	**Agreement**: NA **Output:** Output as part of HA direct physical connection	Volatile RAM	160-bit HMAC-SHA-1 for message authentication and verification in SSH
TLS Authentication Private Key (ECDSA/RSA)	Internal generation by FIPS-approved CTR_DRBG per FIPS 186-4	**Agreement**: RSA (2048bits); ECDSA (P- 256/P-384) **Output:** Output as part of HA direct physical connection	Flash Memory	ECDSA/RSA private key for TLS authentication

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
TLS Authentication Public Key (ECDSA/RSA)	Internal generation by FIPS-approved CTR_DRBG per FIPS 186-4	**Agreement**: RSA (2048 bits); ECDSA (P- 256/P-384) **Output:** Output as part of HA direct physical connection	Volatile RAM	ECDSA/RSA public key for TLS authentication.
TLS Premaster Secret (48 Bytes)	Internal generation by FIPS-approved CTR_DRBG in firmware	**Agreement**: NA **Entry**: Input during TLS negotiation **Output**: Output to peer encrypted by Public Key	Volatile RAM	Establishes TLS master secret
TLS Master Secret (48 Bytes)	Derived from the TLS Pre-Master Secret	**Agreement**: NA	Volatile RAM	Used for computing the Session Key
TLS Session Keys (Triple-DES, AES-128, AES-256)	Derived from the TLS Master Secret Note: These keys are generated via TLS (IETF RFC 5246). This protocol enforces limits on the the number of total possible encryption/decryption operations.	**Agreement**: RSA key transport	Volatile RAM	Used for encryption & decryption of TLS session
TLS Integrity Keys (HMAC-SHA1, HMAC-SHA-256 and HMAC-SHA-384)	Internal generation by FIPS-approved CTR_DRBG in firmware	**Agreement**: NA **Output:** Output as part of HA direct physical connection	Volatile RAM	160-bit HMAC-SHA-1 for message authentication and verification in TLS
Web UI Certificate (RSA and ECDSA)	Internal generation by CTR_DRBG in firmware per FIPS 186-4	**Agreement:** NA **Output:** NA	Flash Memory	Authentication for the Web UI using certificates
Bypass Key (HMAC-SHA-256)	Internal generation by FIPS-approved CTR_DRBG in firmware	**Agreement**: NA **Output:** NA	Flash Memory	256-bit HMAC-SHA-256 used to protect bypass table

Table 12 – CSP Table

Note: In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per Section 5 of SP 800-133 (vendor affirmed). The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP 800-90A DRBG.

7. Self-Tests

The modules include an array of self-tests that are run during startup and conditionally during operations to prevent any secure data from being released and to ensure all components are functioning correctly. Self-tests may be run on-demand by power cycling the module.

7.1 Power-Up Self-Tests

Acme Packet 6300 appliance perform the following power-up self-tests when power is applied to the module. These self-tests require no inputs or actions from the operator:

7.1.1 Firmware Integrity Test

- Firmware Integrity Test (RSA 2048/SHA-256)

7.1.2 Mocana Self-Tests

- AES (Encrypt/Decrypt) Known Answer Test;
- Triple-DES (Encrypt/Decrypt) Known Answer Test;
- SHA-1 Known Answer Test;
- HMAC-SHA-1 Known Answer Test;
- HMAC-SHA-256 Known Answer Test; and
- RSA verify Known Answer Test;

7.1.3 Firmware Self-tests

- SHA-1 Known Answer Test;
- SHA-256 Known Answer Test;
- HMAC-SHA-1 Known Answer Test;
- HMAC-SHA-256 Known Answer Test;
- HMAC-SHA-384 Known Answer Test;
- AES (Encrypt/Decrypt) Known Answer Test;
- AES GCM (Encrypt/Decrypt) Known Answer Test;
- Triple-DES (Encrypt/Decrypt) Known Answer Test;
- SP 800-90A DRBG Known Answer Test;
- RSA sign/verify Known Answer Test; and
- ECDSA sign/verify Known Answer Test.

7.1.4 Nitrox Self-tests

- AES (Encrypt/Decrypt) Known Answer Test;
- Triple-DES (Encrypt/Decrypt) Known Answer Test;
- RSA Pair-wise Consistency Test;

7.1.5 Octeon Self-tests

- AES (Encrypt/Decrypt) Known Answer Test;
- HMAC-SHA-1 Known Answer Test.

When the module is in a power-up self-test state or error state, the data output interface is inhibited and remains inhibited until the module can transition into an operational state. While the CO may attempt to restart the module in an effort to clear an error, the module will require re-installation in the event of a hard error such as a failed self-test.

7.2 Critical Functions Self-Tests

Acme Packet 6300 appliance perform the following critical self-tests. These critical function tests are performed for each SP 800-90A DRBG implemented within the module.

- SP 800-90A Instantiation Test
- SP 800-90A Generate Test
- SP 800-90A Reseed Test
- SP 800-90A Uninstantiate Test

7.3 Conditional Self-Tests

The module performs the following conditional self-tests when called by the module:

- Pair Wise consistency tests to verify that the asymmetric keys generated for RSA, and ECDSA work correctly by performing a sign and verify operation;
- Continuous Random Number Generator test to verify that the output of approved-DRBGs is not the same as the previously generated value;
- Continuous Random Number Generator test to verify that the output of entropy is not the same as the previously generated value;
- Bypass conditional test using HMAC-SHA-256 to ensure the mechanism governing media traffic is functioning correctly, and;
- Firmware Load test using a 2048-bit/SHA-256 RSA-Based integrity test to verify firmware to be loaded into the module.

8. Crypto-Officer and User Guidance

FIPS Mode is enabled by a license installed by Oracle, which will open/lock down features where appropriate.

This section describes the configuration, maintenance, and administration of the cryptographic module.

8.1 Secure Setup and Initialization

The operator shall set up the device as defined in the Session Border Controller ACLI Configuration Guide. The Crypto-Officer shall also:

- Verify that the firmware version of the module is Version E-CZ8.0.0.
- Ensure all traffic is encapsulated in a TLS, SSH, or SRTP tunnel as appropriate.
- Enable HTTPS and configure the web server certificate prior to connecting to the WebUI over TLS.
- Ensure that SNMP V3 is configured with AES-128 and HMAC-SHA-1.
- IKE/IPSec shall not be utilized in the Approved mode of operation.
- For SSH, ensure that group 14 or stronger is selected for Diffie-Hellman.
- Ensure all management traffic is encapsulated within a trusted session (i.e., Telnet should not be used in FIPS mode of operation).
- RADIUS and TACACS shall be disabled and not used the Approved mode of operation.
- All operator passwords must be a minimum of 8 characters in length.
- Ensure use of FIPS-approved algorithms for TLS:
    - TLS_RSA_WITH_Triple-DES_EDE_CBC_SHA
    - TLS_DHE_RSA_WITH_Triple-DES_EDE_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_AES_256_CBC_SHA
    - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
    - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
    - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA-256
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA-384
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA-384
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA-256
    - TLS_DHE_RSA_WITH_AES_256_GCM_SHA-384
    - TLS_DHE_RSA_WITH_AES_128_GCM_SHA-256
- Ensure that SSH is configured to use RSA for authentication.
- Ensure RSA keys are at least 2048-bit keys. No 512-bit or 1024-bit keys can be used in FIPS mode of operation.
- Ensure that the same Triple-DES key shall not be used to encrypt more than 2^20 64-bit blocks of data
- Be aware that when configuring High Availability (HA), only a local HA configuration to a directly connected box via a physical cable over the management port is allowed in FIPS Approved Mode. Remote HA is not allowed in FIPS Approved mode.
- Be aware that HA configuration data that contains keys and CSP's must never be transported over an untrusted network.
- Ensure that the HA ports used for the transport of HA data (including keys and CSP's) are bound to a private IP address range during setup.
- Be aware that only the HA state transactions between the two devices over the direct physical connection are permitted over those dedicated ports.

8.2 AES-GCM IV Construction/Usage

In case the module's power is lost and then restored, the key used for the AES GCM encryption or decryption shall be redistributed. The AES GCM IV generation is in compliance with the [RFC5288] and shall only be used for the TLS protocol version 1.2 to be compliant with [FIPS140-2_IG] IG A.5, provision 1 ("TLS protocol IV generation")

9. Mitigation of other attacks

The module does not mitigate attacks beyond those identified in FIPS 140-2

10. Appendices

10.1 Acronyms, Terms and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
BBRAM	Battery Backed RAM
CMVP	Cryptographic Module Validation Program
CDR	Call Data Record
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DHE	Diffie-Hellman Ephemeral
DRBG	Deterministic Random Bit Generator
ESBC	Enterprise Session Border Controller
ECDSA	Elliptic Curve Digital Signature Algorithm
ESBC	Enterprise Session Border Controller
EDC	Error Detection Code
EMS	Enterprise Management Server
HA	High Availability
HMAC	(Keyed) Hash Message Authentication Code
IKE	Internet Key Exchange
KAT	Known Answer Test
KDF	Key Derivation Function
LED	Light Emitting Diode
MGT	Management
NIST	National Institute of Standards and Technology
POST	Power On Self Test
PUB	Publication
RAM	Random Access Memory
ROM	Read Only Memory
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SRTP	Secure Real Time Protocol
TDM	Time Division Multiplexing
TLS	Transport Layer Security

Table 13 – Acronyms

10.2 References

The FIPS 140-2 standard, and information on the CMVP, can be found at http://csrc.nist.gov/groups/STM/cmvp/index.html.

More information describing the module can be found on the Oracle web site at https://www.oracle.com/industries/communications/enterprise/products/session-border-controller/index.html . This Security Policy contains non-proprietary information. All other documentation submitted for FIPS 140-2 conformance testing and validation is "Oracle - Proprietary" and is releasable only under appropriate non-disclosure agreements.

Document	Author	Title
FIPS PUB 140-2	NIST	FIPS PUB 140-2: Security Requirements for Cryptographic Modules
FIPS IG	NIST	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
FIPS PUB 140-2 Annex A	NIST	FIPS 140-2 Annex A: Approved Security Functions
FIPS PUB 140-2 Annex B	NIST	FIPS 140-2 Annex B: Approved Protection Profiles
FIPS PUB 140-2 Annex C	NIST	FIPS 140-2 Annex C: Approved Random Number Generators
FIPS PUB 140-2 Annex D	NIST	FIPS 140-2 Annex D: Approved Key Establishment Techniques
DTR for FIPS PUB 140-2	NIST	Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules
NIST SP 800-67	NIST	Recommendation for the Triple Data Encryption Algorithm TDEA Block Cypher
FIPS PUB 197	NIST	Advanced Encryption Standard
FIPS PUB 198-1	NIST	The Keyed Hash Message Authentication Code (HMAC)
FIPS PUB 186-4	NIST	Digital Signature Standard (DSS)
FIPS PUB 180-4	NIST	Secure Hash Standard (SHS)
NIST SP 800-131A	NIST	Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes
PKCS#1	RSA Laboratories	PKCS#1 v2.1: RSA Cryptographic Standard

Table 14 – References