FIPS 140-2 Non-Proprietary Security Policy

Acme Packet 1100 [1] and Acme Packet 3900 [2]

FIPS 140-2 Level 2 Validation

Hardware Version: 1100 [1] and 3900 [2]

Firmware Version: E-CZ 8.0.0

Date: July 20, 2018

Title: Acme Packet 1100 and Acme Packet 3900 Security Policy
Date: July 20, 2018
Author: Acumen Security, LLC.
Contributing Authors:
Oracle Communications Engineering
Oracle Security Evaluations – Global Product Security

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 1100 & 3900**	**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**	**10**
6.	**Roles and Services**	**14**
6.1	Operator Services and Descriptions	14
6.2	Unauthenticated Services and Descriptions	16
6.3	Operator Authentication	17
6.3.1	Crypto-Officer and User: Password-Based Authentication	17
6.4	Key and CSP Management	18
7.	**Self-Tests**	**24**
7.1	Power-Up Self-Tests	24
7.1.1	Firmware Integrity Test	24
7.1.2	Mocana Self-Tests	24
7.1.3	OpenSSL Self-tests	24
7.2	Critical Functions Self-Tests	24
7.3	Conditional Self-Tests	25
8.	**Crypto-Officer and User Guidance**	**26**
8.1	Secure Setup and Initialization	26
8.2	AES-GCM IV Construction/Usage	27
9.	**Mitigation of Other Attacks**	**27**
10.	**Appendices**	**28**
10.1	Acronyms, Terms and Abbreviations	28
10.1	References	29

ORACLE

List of Tables

Table 1: FIPS 140-2 Security Requirements 4
Table 2: FIPS Approved or Allowed Security Functions 5
Table 3: Non-Approved but Allowed Security Functions 5
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 - Security Mechanism Inspection and Test 10
Table 8 – Service Summary 14
Table 9 – Operator Services and Descriptions 16
Table 10 – Operator Services and Descriptions 17
Table 11 – Crypto-Officer and User Authentication 17
Table 12 – CSP Table 22
Table 13 – Acronyms 28
Table 14 – References 29

List of Figures

Figure 1: Acme Packet 1100 3
Figure 2: Acme Packet 3900 3
Figure 3: Acme Packet 1100 – Front View 8
Figure 4: Acme Packet 1100 – Rear View 8
Figure 5: Acme Packet 3900 – Front View 8
Figure 6: Acme Packet 3900 – Rear View 9

1. Introduction

1.1 Overview

This document is the Security Policy for the Acme Packet 1100 and 3900 appliances manufactured by Oracle Communications. Acme Packet 1100 and 3900 are 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 1100 and 3900 appliances 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 1100 and 3900 modules 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 1100 & 3900

2.1 Functional Overview

The Acme Packet 1100 and 3900 appliances 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 1100 and 3900 appliances deliver Oracle's industry leading ESBC capabilities in a small form factor appliance. With support for high availability (HA) configurations, TDM fallback, hardware assisted transcoding and Quality of Service (QoS) measurement, the Acme Packet 1100 and 3900 appliances 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 1100 and 3900 appliances 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 1100 and Acme Packet 3900 appliances running firmware version E-CZ 8.0.0 on hardware platform 1100 and 3900. The module is classified as a multi-chip standalone cryptographic module. The physical cryptographic boundary for the Acme Packet 1100 is defined as the module case and all components within the case. The physical cryptographic boundary for the Acme Packet 3900 is all components with exception of the removable power supplies.

A representation of the cryptographic boundary is defined below:

Figure 1: **Acme Packet 1100**

Figure 2: **Acme Packet 3900**

3.2 FIPS 140-2 Validation Scope

The Acme Packet 1100 and 3900 appliances are being validated to overall FIPS 140-2 Level 2 requirements. See Table 1 below.

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles and Services and Authentication	2
Finite State Machine Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
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 1100 and 3900 appliances contain the following FIPS Approved Algorithms listed in Table 2:

Approved or Allowed Security Functions		Certificate
Symmetric Algorithms		
AES	OpenSSL: (CBC, ECB, CTR, GCM); Encrypt/Decrypt; Key Size = 128, 256	5235
	Mocana: (CBC); Encrypt/Decrypt; Key Size = 128, 256	5269
Triple DES[1]	OpenSSL: (CBC); Encrypt/Decrypt; Key Size = 192	2647
	Mocana: (CBC); Encrypt/Decrypt; Key Size = 192	2667
Secure Hash Standard (SHS)		
SHS	OpenSSL: SHA-1, SHA-256, SHA-384	4215
	Mocana: SHA-1, SHA-256	4239
Data Authentication Code		
HMAC	OpenSSL: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	3467
	Mocana: HMAC-SHA-1, HMAC-SHA-256	3488
Asymmetric Algorithms		
RSA	OpenSSL: RSA: FIPS186-4: 186-4KEY(gen): FIPS186-4_Random_e ALG[ANSIX9.31] SIG(gen) (2048 SHA(256 , 384)) SIG(Ver) (2048 SHA(1, 256, 384)) RSA: FIPS186-2 Signature Generation 9.31: Modulus lengths: 4096 SHAs: SHA-256, SHA-384	2797
	Mocana:	2819

[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.

Approved or Allowed Security Functions		Certificate
	RSA: 186-4: 186-4KEY(gen): FIPS186-4_Random_e PKCS1.5: SIG(Ver) (1024 SHA(1); (2048 SHA (1))	
ECDSA	OpenSSL: 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))	1360
Random Number Generation		
DRBG	OpenSSL: **CTR_DRBG**: [Prediction Resistance Tested: Not Enabled; BlockCipher_Use_df: (AES-256)] **Hash_Based DRBG**: [Prediction Resistance Tested: Not Enabled (SHA-1)	2001
CVL		
CVL	OpenSSL: SNMP KDF, SRTP KDF, TLS KDF	1707
	Mocana: SSH KDF	1743
Key Transport		
KTS	OpenSSL: KTS (AES Cert. #5235 and HMAC Cert. #3467; key establishment methodology provides 128 or 256 bits of encryption strength); KTS (Triple-DES Cert. #2647 and HMAC Cert. #3467; key establishment methodology provides 112 bits of encryption strength)	
	Mocana: KTS (AES Cert. #5269 and HMAC Cert. #3488; key establishment methodology provides 128 or 256 bits of encryption strength); KTS (Triple-DES Cert. #2667 and HMAC Cert. #3488; key establishment methodology provides 112 bits of encryption strength)	

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:

Algorithm	Usage
EC-Diffie-Hellman	CVL Certs. #1707 and 1743, key agreement, key establishment methodology provides 128 or 192-bits of encryption strength.
Diffie-Hellman	CVL Certs. #1707 and 1743, key agreement, key establishment methodology provides 112-bits of encryption strength.
RSA Key Wrapping	CVL Certs. #1707 and 1743, key wrapping, key establishment methodology provides 112-bits of encryption strength.
NDRNG	Used for seeding NIST SP 800-90A DRBG.
MD5	MACing: HMAC MD5, Hashing: MD5

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	MACing: HMAC
TLS	Symmetric: DES, RC4
SNMP	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES
Diffie-Hellman	Key agreement, less than 112 bits of encryption strength.
RSA Key Wrapping	Key wrapping, less than 112 bits of encryption strength.
IKEv1	IKEv1 KDF

Table 4: Non-Approved Disallowed Functions

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

4. Module Ports and Interfaces

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

Logical Interface	Physical Port 1100	Physical Port 3900	Information Input/Output
Data Input	Ethernet INT/EXT Ports TDM Ports	Ethernet SFP Ports P0,1,2,3	Cipher text Plain text
Data Output	Ethernet INT/EXT Ports TDM Ports	Ethernet SFP Ports P0,1,2,3	Cipher text Plain text
Control Input	Console Port Reset Pinhole T1/E1 TDM port Ethernet MGT Port	Console Port Reset Button Power Switch T1/E1 TDM ports Ethernet MGT Ports	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 Ethernet MGT Ports LEDs	Console Port Ethernet MGT Ports LEDs	Plaintext status output via console port. Ciphertext status output via network management
Power	Power Plug	Power Plug	N/A

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

The table below describes the interfaces on the Acme 1100 and 3900 appliances.

Physical Interface	Number of Ports 1100	Number of Ports 3900	Description / Use
Console Port	1	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
USB Ports	2	2	This port is used for recovery only by Oracle. e.g. system re-installation after zeroization. On the AP 1100, the USB ports are blocked. On the AP 3900, a tamper seal is applied over the USB ports.
Management	1	3	Used for EMS control, CDR accounting, CLI management, and other

Physical Interface	Number of Ports 1100	Number of Ports 3900	Description / Use
Ethernet ports			management functions
Signaling and Media Ethernet ports	2 INT/EXT	4 SFP P0,1,2,3	Provide network connectivity for signaling and media traffic. These ports are also used for incoming and outgoing data (voice) connections.
Reset Pinhole – Reset Button	1	1	Provides reset functionality
TDM Ports	4	4	Used to convert analog signals to digital signals

Table 6 – Physical Ports

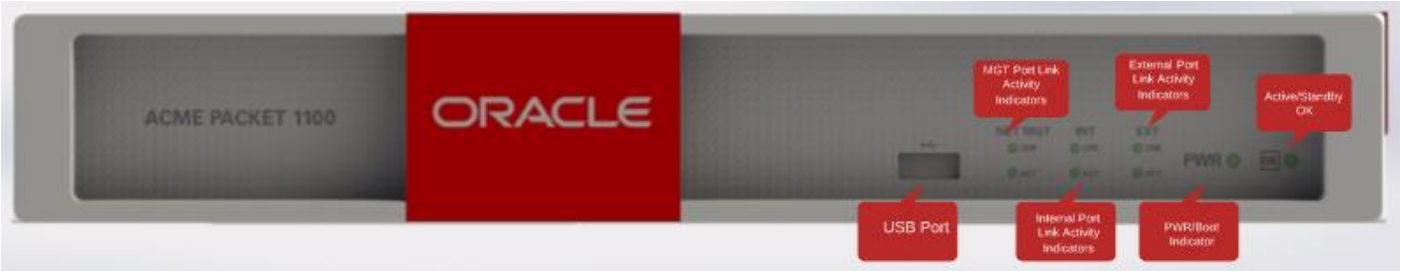

Figure 3: Acme Packet 1100 – Front View

Figure 4: Acme Packet 1100 – Rear View

Figure 5: Acme Packet 3900 – Front View

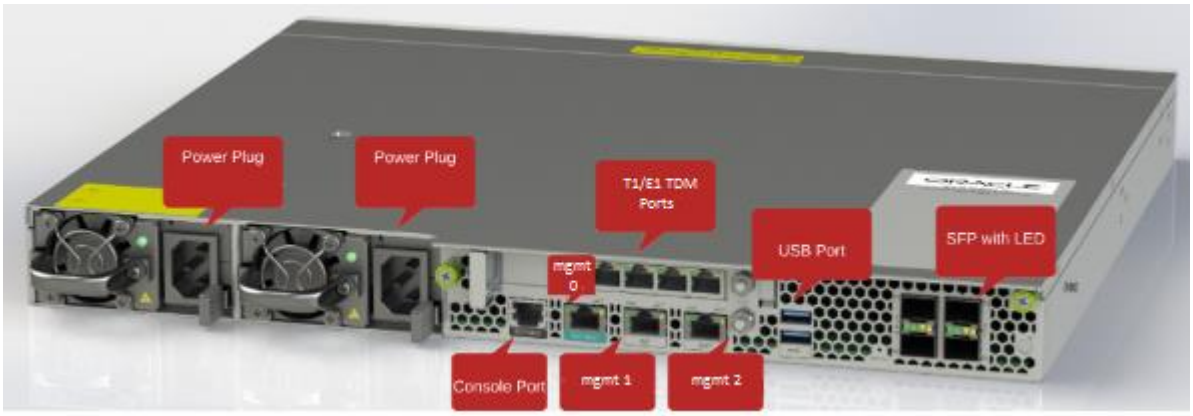

Figure 6: Acme Packet 3900 – Rear View

5. Physical Security

The cryptographic module includes the following physical security mechanisms:

- Production-grade components
- Production-grade opaque enclosure with factory installed tamper evident seals.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Label	In accordance with organization's Security Policy.	Inspect the enclosure and tamper evident tape for physical signs of tampering or attempted access to the cryptographic module. If the module displays signs of tampering or unauthorized access, the Cryptographic Officer should contact Oracle immediately.
Opaque Enclosure	In accordance with organization's Security Policy	Visually inspect the module and ensure for broken casing, open screws and other questionable enclosure inconsistencies.

Table 7 - Security Mechanism Inspection and Test

The module is ships with the tamper seals applied:

- Acme Packet 1100: 2 seals

Figure 7: Rear of Acme Packet 1100

Figure 8: Top side of Acme Packet 1100

- Acme Packet 3900: 3 seals

Figure 9: Front of Acme Packet 3900

Figure 10: Right side of Acme Packet 3900

Figure 11: Top side of Acme Packet 3900

Figure 12: Rear of Acme Packet 3900

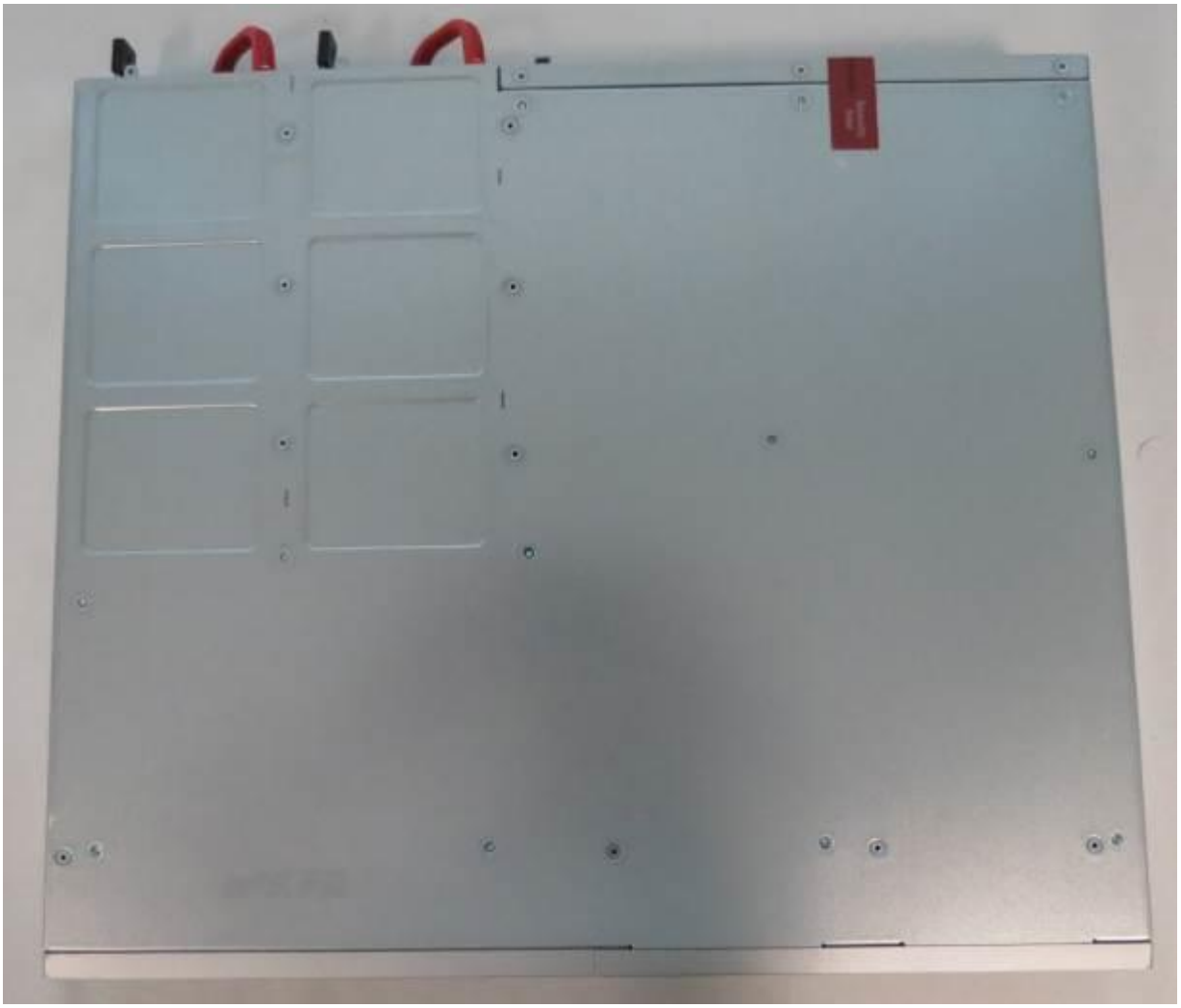

Figure 13: Bottom side of Acme Packet 3900

The Crypto officer is responsible for the following maintenance activities associated with the module physical security,

- Periodically (as defined by the organization's Security Policy) inspect the module tamper tape to ensure that no tampering has occurred
- Review and record the serial numbers of the applied tamper labels in a security log

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 • Test pattern rules, local policies, and session translations • Display system alarms.
Crypto-Officer	Allowed access to all system commands and configuration privileges
Unauthenticated	• Show Status • Initiate self-tests

Table 8 – 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	HMAC-SHA-256 key	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	HMAC-SHA-256 Bypass Key	R, W, X
X	X	Decrypt	Decrypts a block of data Using AES or Triple-DES in FIPS Mode	TLS Session Keys (Triple-DES) TLS Session Keys (AES128) TLS Session Keys (AES256) SSH Session Key (Triple-DES)	X X X X

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
				SSH Session Key (AES128) SSH Session Key (AES256) SRTP Session Key (AES-128) SNMP Privacy Key (AES-128)	X X X X
X	X	Encrypt	Encrypts a block of data Using AES or Triple-DES in FIPS Mode	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 Diffie-Hellman, and RSA keys for key transport/key establishment.	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) EC Diffie-Hellman Public Key (ECDH) EC Diffie-Hellman Private Key (ECDH) 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, TLS Master secret, SRTP Master key	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
X	X	Verify	Used as part of the TLS, SSH protocol negotiation	SSH authentication private Key (RSA)	X

U	CO	Service Name	Service Description	Keys and CSP(s)	Access Type(s)
				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) EC Diffie-Hellman Public Key (ECDH) EC Diffie-Hellman Private Key (ECDH)	X X X X X X X
X	X	Generate Seed	Generate an entropy_input for Hash_Drbg, CTR DRBG	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 R, W, X
X	X	HMAC	Generate HMAC	SNMP Authentication Key SRTP Authentication Key SSH Integrity Keys TLS Integrity Keys	X X X X
X	X	Generate Certificate	Generate certificate	Web UI Certificate	R, W, X
X	X	Authenticate	Authenticate Users	Operator Password	R, W, X

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

For all other services, see https://docs.oracle.com/cd/E92503_01/index.htm.

Table 9 – Operator Services and Descriptions

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 10 – Operator Services and Descriptions

6.3 Operator Authentication

6.3.1 Crypto-Officer and User: 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. 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.	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 module will lock an account after 3 failed authentication attempts; thus, the maximum number of attempts in one minute is 3. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is $3/94^8$ 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. 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.	Passwords must be a minimum of 12 numeric characters. 0-9, yielding 10 choices per character. The module will lock an account after 3 failed authentication attempts; thus, the maximum number of attempts in one minute is 3. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is $3/10^{12}$ which is less than 1/100,000.

Table 11 – Crypto-Officer and User 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, TLS, SNMP or SRTP protocols, other than the KDF, have been tested by the CAVP and CMVP.

The minimum number of bits of entropy requested is 440 bits for the HASH DRBG and 384 bits for the CTR DRBG, therefore providing sufficient entropy strength to seed the DRBG with 256 bits of entropy strength post conditioning.

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
Operator Passwords	Generated by the crypto officer as per the module policy	**Agreement**: NA **Entry**: Manual entry via console or SSH management session **Output**: Output as part of HA direct physical connection to another box	Non-Volatile RAM	Authentication of the crypto officer and user
Firmware Integrity Key (RSA)	Generated externally	**Entry**: RSA (2048 bits) entered as part of Firmware image **Output:** Output as part of HA direct physical connection to another box	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 **Output**: None	Volatile RAM	Used in the random bit generation process
DRBG Seed	Generated internally from hardware sources	**Agreement**: NA **Entry**: NA	Volatile RAM	Entropy used in the random bit generation process

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
		Output: None		
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
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 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
Diffie-Hellman Public Key (DH) 2048-bit	Internal generation by FIPS-approved CTR_DRBG in firmware	**Agreement**: Diffie-Hellman **Entry**: NA **Output**: None	Volatile RAM	Used to derive the secret session key during DH key agreement protocol
Diffie-Hellman Private Key (DH) 224-bit	Internal generation by FIPS-approved CTR_DRBG	**Agreement**: NA **Entry**: NA **Output**: None	Volatile RAM	Used to derive the secret session key during DH key agreement protocol
ECDH Public Key (P-256 and P-384)	Internal generation by FIPS-approved CTR_DRBG in firmware	**Agreement:** EC Diffie-Hellman. **Entry: NA** **Output: None**	Volatile RAM	Used to derive the secret session key during ECDH key agreement protocol
ECDH Private Key (P-	Internal generation by FIPS-	**Agreement**: NA	Volatile RAM	Used to derive the secret session key

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
256 and P-384)	approved CTR_DRBG	**Entry**: NA **Output**: None		during ECDH key agreement protocol
SNMP Privacy Key (AES-128)	NIST SP 800-135 KDF	**Agreement**: NIST SP 800-135 KDF **Entry**: NA **Output**: Output as part of HA direct physical connection to another box	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 to another box	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 to another box	Volatile RAM	Generation of SRTP session keys
SRTP Session Key (AES-128)	NIST SP 800-135 KDF	**Agreement**: NIST SP 800-135 KDF **Entry**: NA **Output**: Output as part of HA direct physical connection to another box	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	Volatile RAM	160-bit HMAC-SHA-1 for message authentication and verification in SRTP

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
		direct physical connection to another box		
SSH Authentication Private Key (RSA)	Internal generation by FIPS-approved Hash_DRBG	**Agreement**: RSA (2048/3072 bits) **Output:** Output as part of HA direct physical connection to another box	Flash	RSA private key for SSH authentication
SSH Authentication Public Key (RSA)	Internal generation by FIPS-approved Hash_DRBG	**Agreement**: RSA (2048/3072 bits) **Output:** Output as part of HA direct physical connection to another box	Flash	RSA public key for SSH authentication.
SSH Session Keys (Triple-DES, AES-128, AES-256)	Derived via SSH KDF. Note: These keys are generated via SSH (IETF RFC 4251). This protocol enforces limits on the the number of total possible encryption/decryption operations.	**Agreement**: Diffie-Hellman	Volatile RAM	Encryption and decryption of SSH session
SSH Integrity Keys (HMAC-SHA1)	Derived via SSH KDF.	**Agreement**: NA **Output:** Output as part of HA direct physical connection to another box	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	**Agreement**: RSA (2048bits); ECDSA (P- 256/P-384) **Output:** Output as part of HA direct physical connection to another box	Flash	ECDSA/RSA private key for TLS authentication
TLS Authentication Public Key (ECDSA/RSA)	Internal generation by FIPS-approved CTR_DRBG	**Agreement**: RSA (2048bits); ECDSA (P- 256/P-384) **Output:** Output as part of HA direct physical connection to another box	Volatile RAM	ECDSA/RSA public key for TLS authentication.

CSP Name	Generation/Input	Establishment/ Export	Storage	Use
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)	Internal generation by FIPS-approved CTR_DRBG in firmware	**Agreement**: NA **Output:** Output as part of HA direct physical connection to another box	Volatile RAM	160-bit HMAC-SHA-1 for message authentication and verification in TLS
Web UI Certificate	Internal generation by FIPS DRBG in Firmware	**Agreement:** NA **Output:** TLS session with operator	Flash	Web server certificate
Bypass Key	HMAC-SHA-256 Bypass	**Agreement:** NA **Output:** NA	Flash	Bypass service

Table 12 – CSP Table

Note: When the module generates symmetric keys or seeds used for generating asymmetric keys, unmodified DRBG output is used as the symmetric key or as the seed for generating the asymmetric keys.

Note: All keys generated by the module use the direct output of a FIPS approved DRBG. This meets the requirements of SP 800-133.

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 1100 and 3900 appliances perform the following power-up self-tests when power is applied to the module. These self-test 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 OpenSSL 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 HASH DRBG Known Answer Test;
- SP 800-90A CTR DRBG Known Answer Test;
- RSA sign/verify Known Answer Test; and
- ECDSA sign/verify 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 1100 and 3900 appliances 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-DRBG is not the same as the previously generated value for both DRBGs;
- 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-CZ 8.0.0.
- Ensure all traffic is encapsulated in a TLS, SSH, or SRTP tunnel as appropriate.
- Ensure that SNMP V3 is configured with AES-128/HMAC only.
- Ensure all management traffic is encapsulated within a trusted session (i.e., Telnet should not be used in FIPS mode of operation).
- Ensure that the tamper evidence labels are applied by Oracle. The tamper evident labels shall be installed for the module to operate in a FIPS Approved mode of operation.
- Inspect the tamper evident labels periodically to verify they are intact and the serial numbers on the applied tamper evident labels match the records in the security log.
- 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 RSA keys are at least 2048-bit keys. No 512-bit or 1024-bit keys can be used in FIPS mode of operation.
- 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.
- IKE and IPSec shall not be used in FIPS approved mode.
- Radius and TACACS+ shall not be used in FIPS approved mode.
- Enable HTTPS and configure the web server certificate prior to connecting to the WebUI over TLS.
- SSH shall only use strengths of group 14 in FIPS approved mode.
- Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

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"); thus, the module is compliant with [SP800-52].

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
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
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
NVRAM	Non-Volatile RAM
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

10.1 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