FIPS 140-2 Non-Proprietary Security Policy

Acme Packet 3820 and Acme Packet 4500

FIPS 140-2 Level 2 Validation

Firmware Version ECx 6.4.1 and ECx 6.4.1 M1

Hardware Version A1

August 28, 2015

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140-2

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic products to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment Canada (CSEC) jointly run the Cryptographic Module Validation Program (CMVP). The NIST National Voluntary Laboratory Accreditation Program (NVLAP) accredits independent testing labs to perform FIPS 140-2 testing; the CMVP validates test reports for all cryptographic modules pursuing FIPS 140-2 validation. *Validation* is the term given to a cryptographic module that is documented and tested against the FIPS 140-2 criteria.

More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the Acme Packet 3820 and Acme Packet 4500 from Oracle Communications provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document also contains details on the cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140 mode of operation.

The Oracle Communications Acme Packet 3820 and Acme Packet 4500 may also be referred to as the "modules" in this document.

1.3 External Resources

The Oracle Communications website (http://www.oracle.com/us/products/enterprise-communications/enterprise-session-border-controller/index.html) contains information on the full line of products from Oracle Communications, including a detailed overview of the Acme Packet 3820 and Acme Packet 4500 solution. The Cryptographic Module Validation Program website contains links to the FIPS 140-2 certificate and Oracle Communications contact information.

1.4 Notices

This document may be freely reproduced and distributed in its entirety without modification.

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
ACLI	Acme Command Line Interface
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSEC	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DTR	Derived Testing Requirements
EMS	External Management Server
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
IP	Internet Protocol
KAT	Known Answer Test
NDRNG	Non Deterministic Random Number Generation
NIST	National Institute of Standards and Technology
OS	Operating System
PBX	Private Branch Exchange
RSA	Rivest Shamir Adelman
SBC	Session Border Controller
SHA	Secure Hashing Algorithm
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNMP	Secure Network Management Protocol
SRTP	Secure Real Time Protocol
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
UC	Unified Communications

Table 1 – Acronyms and Terms

2 Oracle Communications Acme Packet 3820 and Acme Packet 4500

2.1 Product Overview

Oracle Communications session border controllers (SBC) provide critical control functions to deliver trusted, first-class interactive communications—voice, video and multimedia sessions—across IP network borders. They support multiple applications in government, service provider, enterprise and contact center networks—from VoIP trunking to hosted enterprise and residential services to fixed-mobile convergence.

The Acme Packet 3820 platform supports up to 4,000 simultaneous signaled sessions for government agencies, smaller service providers, small enterprises and smaller sites within larger organizations.

The Acme Packet 4500 is a carrier-class platform supporting up to 32,000 simultaneous signaled sessions, delivering unmatched capabilities and performance. It offers extremely rich functionality, architectural flexibility, signaling protocol breadth, and satisfies all of the performance, capacity, availability and manageability requirements of defense and security–focused government organizations, service providers, enterprises and contact centers.

The modules feature Acme Packet's custom hardware design tightly integrated with Acme Packet OS to satisfy the most critical infrastructure security requirements.

In government, enterprise, and contact center environments, the Acme Packet 3820 and Acme Packet 4500 secure SIP/H.323 trunking borders to service providers and other 3rd party IP networks and the internet border to remote offices, teleworkers, and mobile employees. In extremely security-conscious organizations, they secure the border to the private VPN connecting other sites. SIP and H.323 interworking capabilities ensure interoperability with and between legacy IP PBX equipment and next-generation unified communications platforms. They control session admission, IP PBX or UC server loads and overloads, IP network transport, and SIP/H.323 session routing to assure SLAs and minimize costs. Regulatory compliance requirements are also satisfied with encryption ensuring session privacy and call/session replication for recording.

2.2 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interference / Electromagnetic Compatibility	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 2 – Validation Level by DTR Section

2.3 Algorithm Implementations

2.3.1 FIPS-Approved Algorithms

The module contains the following algorithm implementations:

- Hifn 8450: bump-in-the-wire processing (HMAC-SHA-1, AES, TRIPLE-DES)
- Broadcom 5862 (BCM5862): DH, SHA-1, HMAC-SHA1, AES and Triple-DES for SSH and TLS
- Firmware running on Intel Core Duo T2500, Intel Core Duo T9400 and Intel Celeron M 440: random number generation, SHA-1, SHA-256, RSA, HMAC-SHA-1, HMAC-SHA-256, and Hash_DRBG

These cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Keyed Hash	HMAC-SHA-1, HMAC-SHA-256	FIPS 198-1	519	Message verification
Hashing	SHA-1, SHA-256	FIPS 180-4	912	Message digest
Symmetric Key	Three key Triple-DES (CBC mode)	NIST SP 800-67	745	Data encryption / decryption
	AES 128 and 256 (CBC, ECB, CTR modes)	FIPS 197	928	Data encryption / decryption

Table 3 – Algorithm Certificates for FIPS-Approved Algorithms in the Hifn 8450

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Hashing	SHA-1	FIPS 180-4	1378	Message digest
Keyed Hash	HMAC-SHA1	FIPS 198-1	907	Message verification
Symmetric Key	Three key Triple-DES (CBC mode)	NIST SP 800-67	1019	Data encryption / decryption
	AES 128 and 256 (CBC, ECB, CTR modes)	FIPS 197	1555	Data encryption / decryption

Table 4 – Algorithm Certificates for FIPS-Approved Algorithms for the BCM5862

Algorithm Type	Algorithm	Standard	F/W 6.4.1 Cert. #	F/W 6.4.1 M1 Cert. #	Use
Hashing	SHA-1 SHA-256	FIPS 180-4	2748	2788	Message digest
Keyed Hash	HMAC-SHA1 HMAC-SHA-256	FIPS 198-1	2107	2143	Message verification (via HMAC-SHA-256) and module integrity (via HMAC-SHA-1
Asymmetric Key	RSA 2048	FIPS 186-2	1697	1724	Verify operations
Random Number Generation	Hash DRBG	SP800-90A	762	791	Random number generation
Key Derivation Function	TLS 1.0/1.1, SSH, SRTP, SNMP[1]	SP 800-135	480	498	Key derivation

Table 5 – Algorithm Certificates for FIPS-Approved Algorithms in Firmware

2.3.2 Non-Approved Algorithms and Protocols

The module implements the following non-approved algorithms and protocols:

- DES
- ARC4
- HMAC-MD5
- IPSEC
    - The FIPS 140-2 module validation does not cover the full protocol implementation for the IKE in IPSec and it is therefore considered a non-Approved service.
- SNMP V3 is considered non-FIPS mode in F/W version ECx 6.4.1.

Unless otherwise noted, Non-Approved algorithms and protocols are not allowed for use in FIPS mode.

2.3.3 Non-Approved but Allowed Algorithms and Protocols

The module implements the following non-approved but allowed algorithms and protocols in FIPS Approved Mode:

[1] SNMP V3 is only FIPS Approved while running F/W version 6.4.1 M1 only.

- RSA (key transport/key establishment)
  - Used in FIPS mode for TLS sessions and SSH key establishment in and provides 112-bits of encryption strength, non-compliant less than 112 bits.
- Diffie-Hellman (key transport/key establishment)
  - Used in FIPS mode for SSH sessions key agreement/key establishment in and provides 112-bits of encryption strength in FIPS Approved Mode, non-compliant less than 112 bits of encryption strength.
- Hardware-based random number generator (entropy generation for seeding DRBG)
  - This RNG is used in FIPS mode only to generate entropy_input to the firmware-based FIPS-approved Hash_DRBG.

2.4 Cryptographic Module Specification

The module is the Oracle Communications Acme Packet 3820 and Acme Packet 4500 running firmware versions ECx 6.4.1 and ECx 6.4.1 M1 on hardware version A1. The module is classified as a multi-chip standalone cryptographic module. The physical cryptographic boundary is defined as the module case and all components within the case. No components are excluded from the requirements of FIPS PUB 140-2.

The specific models included in the validation are as follows:

- Acme Packet 3820
  - Running network processor AMCC NP3750 @400 Mhz and host processor Intel Celeron M 440
  - Running Hifn 8450 and Broadcom 5862 for dedicated, hardware-based cryptographic processing.

- Acme Packet 4500
  - Running network processor AMCC NP3750 @700 Mhz and host processor Intel Core Duo T2500
  - Running network processor AMCC NP3750 @700 Mhz and host processor Intel Core Duo T9400
  - Running Hifn 8450 and Broadcom 5862 for dedicated, hardware-based cryptographic processing.

The physical boundary for the modules are the entire module appliance and are pictured in the images below:

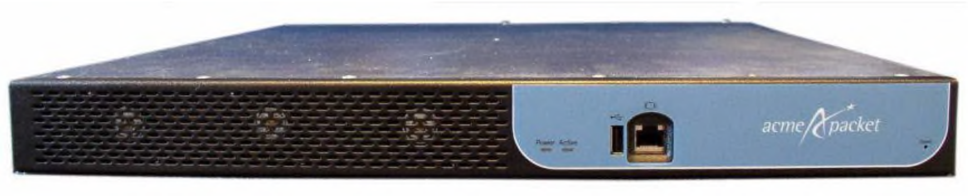

Figure 1 – Acme Packet 3820 Physical Boundary

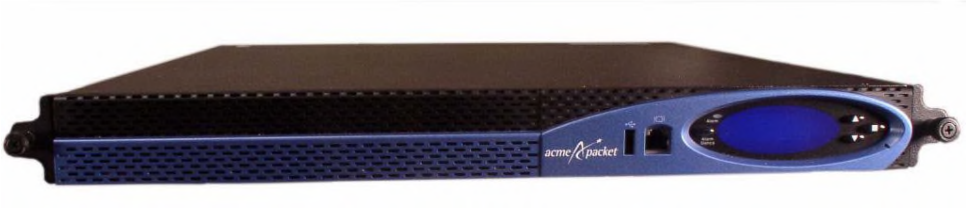

Figure 2 – Acme Packet 4500 Physical Boundary

The logical boundary for the modules is the entire firmware image.

2.5 Module Interfaces

The table below describes the main interfaces on the Acme Packet 3820:

Physical Interface	Description / Use
LEDs[2]	Indicates if any alarms are active on the module. The LED can be three different colors to indicate the severity of the alarms. • Unlit—system is fully functional without any faults • Amber—major alarm has been generated • Red—critical alarm has been generated.
Console Ports	Provides console access to the module. The module supports only one active serial console connection at a time. The rear console port is useful for customers who want permanent console access; the front console port provides easy access to the module for a temporary connection. Console port communication is used for administration and maintenance purposes from a central office (CO) location. Tasks conducted over a console port include: • Creating the initial connection to the module • Accessing and using all functionality available via the ACLI • Performing in-lab system maintenance (services described below)
Alarm Port[3]	Closes a circuit when a specific alarm level becomes active. The module features an alarm control signal interface that can be used in a CO location to indicate when internal alarms are generated. The appliances use alarm levels that correspond to three levels of service-disrupting incidents.
USB Ports	USB ports are disabled.
Network Management Ports	Used for EMS control, CDR accounting, CLI management, and other management functions
Signaling and Media Interfaces	Provide network connectivity for signaling and media traffic.

Table 6 – Acme Packet 3820 Interface Descriptions

The table below describes the main interfaces on the Acme Packet 4500:

[2] LED's do not provide FIPS Status indicators. FIPS status indicators are only in the form of logical indicators

[3] Alarm port does not provide FIPS status indicators.

Physical Interface	Description / Use
LCD	Reports real-time status, alarms, and general system information
LEDs[4]	Indicates if any alarms are active on the module. The LED can be three different colors to indicate the severity of the alarms. • Unlit—system is fully functional without any faults • Amber—major alarm has been generated • Red—critical alarm has been generated.
Console Ports	Provides console access to the module. The module supports only one active serial console connection at a time. The rear console port is useful for customers who want permanent console access; the front console port provides easy access to the module for a temporary connection. Console port communication is used for administration and maintenance purposes from a central office (CO) location. Tasks conducted over a console port include: • Creating the initial connection to the module • Accessing and using all functionality available via the ACLI • Performing in-lab system maintenance (services described below)
Alarm Port[5]	Closes a circuit when a specific alarm level becomes active. The module features an alarm control signal interface that can be used in a CO location to indicate when internal alarms are generated. The appliances use alarm levels that correspond to three levels of service-disrupting incidents.
USB Ports	USB ports are disabled.
Network Management Ports	Used for EMS control, CDR accounting, CLI management, and other management functions
Signaling and Media Interfaces	Provide network connectivity for signaling and media traffic.

Table 7 – Acme Packet 4500 Interface Descriptions

The modules provide a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following table:

FIPS 140-2 Logical Interface	Module Physical Interface	Information Input/Output
Data Input	Ethernet Ports (RJ-45), Console Ports (RJ-45),	Ciphertext (SSH, and TLS packets)
Data Output	Ethernet Ports (RJ-45), Console Ports (RJ-45),	Ciphertext (SSH, and TLS packets)

[4] LED’s do not provide FIPS Status indicators. FIPS status indicators are only in the form of logical indicators

[5] Alarm port does not provide FIPS status indicators.

FIPS 140-2 Logical Interface	Module Physical Interface	Information Input/Output
Control Input	Console Ports (RJ-45), Network Management Ports (RJ-45), On/Off Switch	Plaintext control input via console port (configuration commands, operator passwords), ciphertext control input via network management (EMS control, CDR accounting, CLI management.
Status Output	Network Management Ports (RJ-45), Console Ports (RJ-45), LCD Screen (4500), LEDs	Plaintext status output.
Power	Power Plug, On/Off Switch	N/A

Table 8 – Logical Interface / Physical Interface Mapping

2.6 Roles, Services, and Authentication

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 table below provides a mapping of default roles in the module to the roles defined by FIPS 140-2:

Operator Role	Summary of Services
User	• View configuration versions and a large amount if statistical data for the system's performance • Handle certificate information for TLS and SSH 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	• Show Status • Initiate self-tests

Table 9 – Role Mapping

2.6.1 Operator Services and Descriptions

The services available to the User and Crypto Officer roles in the module are as follows:

Service and Description	Service Input	Service Output	Key/CSP Access	Roles
Configure Initializes the module for FIPS mode of operation	FIPS License, Image integrity (HMAC) value	None	HMAC-SHA-256 key	Crypto Officer
Firmware Update Updates the firmware	Signed firmware image	None	Public Key 1	Crypto Officer
Decrypt Decrypts a block of data Using AES or TRIPLE-DES in FIPS Mode Decrypts a block of data using DES or ARC4 in Non-FIPS mode	Key Encrypted byte stream	Byte stream	TLS Session Keys (TRIPLE-DES) TLS Session Keys (AES128) TLS Session Keys (AES256) TLS Session Keys (DES,ARC4 in Non-FIPS Mode) SSH Session Key (TRIPLE-DES) SSH Session Key (AES128) SSH Session Key (AES256) SSH Session Keys (DES, ARC4 in Non-FIPS Mode) SRTP Session Key (AES-128) SNMP Privacy Key (AES-128) Private Key 2	User

Service and Description	Service Input	Service Output	Key/CSP Access	Roles
Encrypt Encrypts a block of data Using AES or TRIPLE-DES in FIPS Mode Encrypts a block of data using DES or ARC4 in Non-FIPS mode	Key Byte stream	Encrypted byte stream	TLS Session Keys (TRIPLE-DES) TLS Session Keys (AES128) TLS Session Keys (AES256) TLS Session Keys (DES, ARC4 in Non-FIPS Mode) SSH Session Key (TRIPLE-DES) SSH Session Key (AES128) SSH Session Key (AES256) SSH Session Keys (DES, ARC4 in Non-FIPS mode) SRTP Session Key (AES-128) SNMP Privacy Key (AES-128) Public Key 2	User

Service and Description	Service Input	Service Output	Key/CSP Access	Roles
Generate Keys Generates AES or TRIPLE-DES keys for encrypt/decrypt operations in FIPS mode Generates Diffie-Hellman and RSA keys for key transport/key establishment.	Key Size	AES-Keys or TRIPLE-DES Keys in FIPS mode DES keys and ARC4 Keys in Non-FIPS mode	TLS Certificates (RSA, Diffie-Hellman) TLS Session Keys (TRIPLE-DES) TLS Session Keys (AES128) TLS Session Keys (AES256) TLS Session Keys (DES, ARC4 in non-FIPS mode) SSH Certificates (Diffie-Hellman) SSH Session Key (TRIPLE-DES) SSH Session Key (AES128) SSH Session Key (AES256) SSH Session Keys (DES, ARC4 in Non-FIPS mode) SRTP Master Key (AES-128) Public Key 2	User
Verify Verifies the signature of a RSA-signed block Used as part of the TLS protocol negotiation	RSA Signed firmware Nonce transported as part of TLS or SSH	Verification success/failure Verification success/failure	Public Key 1 Public Key 2	User
Hash_Drbg seed Generate a entropy_input for Hash_Drbg	NDRNG generated random bits.	entropy_input	entropy_input Public Key 2	User
Hash_Drbg Generate random number.	Working state C and V	Random number	Hash_DRBG V Hash_DRBG Public Key 2	User

Service and Description	Service Input	Service Output	Key/CSP Access	Roles
HMAC Hash-SHA hash based Message Authentication Code in FIPS mode HMAC-MD5 Hash based Message Authentication Code in Non-FIPS mode	Key, data block	HMAC value	HMAC 160-bit key 1 HMAC 160-bit key 2 (TLS/SSH/SRTP) HMAC 256-bit key Public Key 2 HMAC-MD5 Key (non-FIPS mode)	User
Zeroize CSPs[6] Clears CSPs from memory	Key, Key pair, entropy_input, password	Invalidated CSP	All CSPs	Crypto Officer

Table 10 – Operator Services and Descriptions

The module provides for the following unauthenticated services, which do not require authentication as they are not security relevant functions. These services do not affect the security of the module; these services do not create, disclose, or substitute cryptographic keys or CSPs, nor do they utilize any Approved security functions.

Service and Description	Service Input	Service Output	Key/CSP Access	Roles
Show Status Shows status of the module	None	Module status enabled/disabled	None	Unauthenticated
Initiate self-tests Restarting the module provides a way to run the self-tests on-demand	None	Console display of success/failure. Log entry of success/failure.	None	Unauthenticated

Table 11 – Unauthenticated Operator Services and Descriptions

[6] During zeroization the Crypto-Officer must remain in possession of the module until it has rebooted in order to verify that successfully zeroization has completed.

2.6.2 Operator Authentication

2.6.2.1 Crypto-Officer: Password-Based Authentication

In FIPS-approved mode of operation, the module is accessed via Command Line Interface over the Console ports or via SSH or SNMP over the Network Management Ports. Other than status functions available by viewing the LCD panel, the services described in Table 10 – Operator Services and Descriptions are available only to authenticated operators.

Passwords must be a minimum of 8 characters (see Guidance and Secure Operation section of this document). 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.

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.

The module will permit an operator to change roles provided the operator knows both the User password and the Crypto Officer password.

2.6.2.2 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 keys. A 2048-bit RSA 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 support 60 authentication attempts in one minute, the probability of a success with multiple consecutive attempts in a one-minute period is $3/2^{112}$, which is less than 1/100,000.

2.7 Physical Security

The module is a multiple-chip standalone module and conforms to Level 2 requirements for physical security. For details on tamper evidence, please see Section 3.1.2 – Placement of Tamper Evidence Labels.

2.8 Operational Environment

The module operates in a limited operational model and does not implement a General Purpose Operating System.

The module meets Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B.

2.9 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
TLS Session Keys (TRIPLE-DES, AES-128, AES-256)	TRIPLE-DES CBC 168-bit, AES-128 bit CBC, AES-256 bit CBC For encryption / decryption of TLS session traffic Source: Broadcom	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: RSA key transport **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D
SSH Session Keys (TRIPLE-DES, AES-128, AES-256)	TRIPLE-DES CBC 168-bit, AES-128 bit CBC, AES-256 bit CBC For encryption / decryption of SSH session traffic Source: Broadcom	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: Diffie-Hellman **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
SRTP Master Key (AES-128)	For derivation of the SRTP Session Key	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: Diffie-Hellman **Entry**: NA **Output**: encrypted	Resetting / rebooting the module or power cycling	Crypto Officer R W D
SRTP Session Key (AES-128)	For encryption / decryption of SRTP session traffic	NIST SP 800-135 KDF	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NIST SP 800-135 KDF **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
SNMP Privacy Key (AES-128)	For encryption / encryption of SNMP session traffic	NIST SP 800-135 KDF	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NIST SP 800-135 KDF **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D
Diffie-Hellman Public Key	y=g^x mod p component; Generator g is 2 and p is 2048 (group-14) Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
Diffie-Hellman Private Key	x component of DH; x is 2048 (group-14) Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Resetting / rebooting the module or power cycling	Crypto Officer R W D
HMAC 160-bit key 1	160-bit HMAC-SHA-1 for message verification Source: Broadcom	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Flash RAM in plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Re-formatting flash memory	Crypto Officer R W D
HMAC 160-bit key 2	160-bit HMAC-SHA-1 for message authentication and verification in SSH/TLS, SNMP and SRTP Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Flash RAM in plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory for the respective session.	**Agreement**: NA **Entry**: NA **Output**: None	Re-formatting flash memory	Crypto Officer R W D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
Operator passwords	Alphanumeric passwords externally generated by a human user for authentication to the module. Source: Host Processor	Not generated by the module; defined by the human user of the module	**Storage**: Non Volatile RAM in plaintext **Type**: Static **Association**: controlled by the operating environment	**Agreement**: NA **Entry**: Manual entry via console or SSH management session **Output**: Not Output	Issue command secure_pwd_reset()	Crypto Officer R W D User R W D
Premaster Secret (48 Bytes)	RSA-Encrypted Premaster Secret Message Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: Input during TLS negotiation **Output**: Output to peer encrypted by Public Key	Resetting / rebooting the module or power cycling	Crypto Officer None User None
Master Secret (48 Bytes)	Used for computing the Session Key Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Volatile RAM in plaintext **Type**: Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Resetting / rebooting the module or power cycling	Crypto Officer None User None

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
Hash_DRBG V	440 bits long value V used for generating Hash_DRBG Source: Host Processor	Generated as per section 10.1.1.2 of SP 800-90	**Storage**: Volatile RAM in plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Resetting / rebooting the module or power cycling	Crypto Officer None User None
Hash_DRBG C	440 bits long constant C used for generating Hash_DRBG Source: Host Processor	Generated as per section 10.1.1.2 of SP 800-90	**Storage**: Volatile RAM in plaintext **Type:** Ephemeral **Association**: The operating environment is the one and only owner. Relationship is maintained by the operating environment via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Resetting / rebooting the module or power cycling	Crypto Officer None User None

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
Hash_DRBG Entropy Input String	Input string for DRBG Source: Host Processor	Generated as per section 10.1.1.2 of SP 800-90	**Storage**: Volatile RAM in plaintext **Type:** Ephemeral **Association**: The operating environment is the one and only owner. Relationship is maintained by the operating environment via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Resetting / rebooting the module or power cycling	Crypto Officer None User None
Hash_DRBG Seed Value	Seed value for DRBG Source: Host Processor	Generated as per section 10.1.1.2 of SP 800-90	**Storage**: Volatile RAM in plaintext **Type:** Ephemeral **Association**: The operating environment is the one and only owner. Relationship is maintained by the operating environment via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Resetting / rebooting the module or power cycling	Crypto Officer None User None
Public Key 1	RSA Public 2048-bit for firmware load verification operations. Source: Host Processor	Entered encrypted	**Storage**: Flash in plaintext **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating environment.	**Agreement**: NA **Entry**: NA **Output**: NA	Not destroyed as it is a public key	Crypto Officer R W D User R

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Destruction	Privileges
Public Key 2	RSA Public 2048-bit for key establishment for TLS/SSH sessions. Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Flash in plaintext **Type:** Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via certificates.	**Agreement**: NA **Entry**: NA **Output**: NA	Not destroyed as it is a public key	Crypto Officer R W D User R
Private Key 2	RSA Private 2048-bit for key establishment[7] for TLS/SSH sessions Source: Host Processor	Internal generation by FIPS-approved Hash_DRBG in firmware	**Storage**: Flash in plaintext **Type**: Static **Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Agreement**: NA **Entry**: NA **Output**: NA	Re-formatting flash memory	Crypto Officer R W D User R

R = Read W = Write D = Delete

Table 12 – Key/CSP Management Details

Public keys are protected from unauthorized modification and substitution. The module ensures only authenticated operators have access to keys and functions that can generate keys. Unauthenticated operators do not have write access to modify, change, or delete a public key. For the session certificate, the module generates a PKCS10 certificate request (PKCS 10), and a standard Certificate Authority (CA) generates the certificate.

[7] Key establishment methodology provides 112-bits of encryption strength

2.10 Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the module will output an error dialog and will shut down. When the module is in an error state, no keys or CSPs will be output and the module will not perform cryptographic functions.

The module does not support a bypass function.

The following sections discuss the module's self-tests in more detail.

2.10.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of the module and if any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the users. The module implements the following power-on self-tests:

Implementation	Self Tests Run
Hifn 8450	• TRIPLE-DES encrypt known answer test • TRIPLE-DES decrypt known answer test • AES encrypt known answer test • AES decrypt known answer test • HMAC-SHA-1 known answer test[8]
BCM5862	• TRIPLE-DES encrypt known answer test • TRIPLE-DES decrypt known answer test • AES encrypt known answer test • AES decrypt known answer test • SHA-1 known answer test • HMAC-SHA-1 known answer test
Firmware	• SHA-1 and SHA-256 known answer test • HMAC-SHA-1 and HMAC-SHA-256 known answer test • Hash_DRBG known answer test • Firmware integrity check using HMAC-SHA-256 • RSA (verify) known answer test • KDF KAT

Table 13 - Power-On Self-Tests

The module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module in FIPS approved Mode of Operation.

[8] Note: According to the CMVP FAQ p.57 "If a KAT is implemented for the HMAC-SHA-1, a KAT is not needed for the underlying SHA-1."

2.10.1.1 Status Output

An operator can discern that all power-on self-tests have passed via normal operation of the module and the following log message.

```
FIPS: KAT self test completed successfully.
FIPS: System is currently operating in FIPS 140-2
compatible mode.
```

In the event a POST fails, the module will output the following log message:

```
FIPS: ERROR - System is not in FIPS 140-2 compatible mode
FIPS: ERROR - <Test Name> failed.
```

For example:

```
FIPS: ERROR - RSA pair wise consistency test failed.
```

Note that data output will be inhibited while the module is in an error state (i.e., when a POST fails). No keys or CSPs will be output when the module is in an error state.

2.10.2 Conditional Self-Tests

Conditional self-tests are test that run continuously during operation of the module. If any of these tests fail, the module will enter an error state. The module can be re-initialized to clear the error and resume FIPS mode of operation. No services can be accessed by the operators. The module performs the following conditional self-tests:

Implementation	Self Tests Run
BCM5862	• Continuous NDRNG test
Firmware	• DRBG Health Test as specified in SP 800-90 Section 11.3 • Continuous test on output of seed mechanism • RSA pairwise consistency test for encrypt/decrypt • Firmware load test using RSA 2048

Table 14 – Conditional Self-Tests

2.10.2.1 Status Output

In the event a conditional self-test fails, the module will output the following log message:

```
FIPS: ERROR - System is not in FIPS 140-2 compatible mode
FIPS: ERROR - <Conditional Test Name> failed.
```

For example:

```
FIPS: ERROR - Continuous RNG test failed.
```

Note that data output will be inhibited while the module is in this error state. The module will self-correct this use case as follows:

Test	Remediation
Pairwise consistency test for RSA implementations	Generate a new RSA key pair and rerun test
Continuous test run on output of FIPS-approved Hash_DRBG in firmware	Generate a new value and rerun test
Continuous test on output of FIPS-approved Hash_DRBG in firmware seed mechanism	Generate a new value and rerun test

Table 15 – Conditional Self Tests and Module Remediation

No keys or CSPs will be output when the module is in an error state.

2.10.3 Critical Functions Test

The following are considered critical functions tests:

- Adding additional entropy to NDRNG;
- SP 800-90A DRBG critical function tests;
- KDF KAT performed at power-up.

2.11 Mitigation of Other Attacks

The module does not mitigate attacks.

3 Guidance and Secure Operation

This section describes how to configure the module for FIPS-approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

3.1 Crypto Officer Guidance

3.1.1 Enabling FIPS Mode and General Guidance

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

Additionally, the Crypto Officer must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation[9]:

- Verify that the firmware version of the module is Version ECx 6.4.1 or ECx 6.4.1 M1.
- Ensure all media traffic is encapsulated in a TLS, SSH, or SRTP tunnel as appropriate.
- Ensure that SNMP V3 is configured with AES-128 (Version ECx 6.4.1 M1 only).
- Ensure all management traffic is encapsulated within a trusted session (i.e., Telnet or FTP should not be used in FIPS mode of operation).
- Ensure that the tamper evidence labels are applied by Oracle as specified in Section 3.1.2 – Placement of Tamper Evidence Labels. 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 v1.0:

```
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
```

[9] The licensing may ensure most of these are met. The Crypto Officer should verify all details prior to operation in FIPS mode.

```
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
```

- Ensure use of FIPS-approved cipher suite algorithms for SSH V2.
- Ensure RSA keys are at least 2048-bit keys. No 512-bit or 1024-bit keys can be used in FIPS mode of operation.
- Do not disclose passwords and store passwords in a safe location and according to his/her organization’s systems security policies for password storage.

3.1.2 Placement of Tamper Evidence Labels

To meet Physical Security Requirements for Level 2, the module enclosure must be protected with tamper evidence labels. The tamper evident labels shall be installed for the module to operate in a FIPS Approved mode of operation. Oracle Communications applies the labels at time of manufacture; the Crypto Officer is responsible for ensuring the labels are applied as shown below. Once applied, the Crypto Officer shall not remove or replace the labels unless the module has shown signs of tampering. In the event of tampering or wear and tear on the labels, the Crypto Officer shall return the module to Oracle Communications, where it will be reimaged and returned with a new set of labels.

The Crypto Officer is responsible for

- Verifying the five labels are attached to the appliance as shown in the diagrams below,
- Maintaining the direct control and observation of any changes to the module such as reconfigurations where the tamper evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

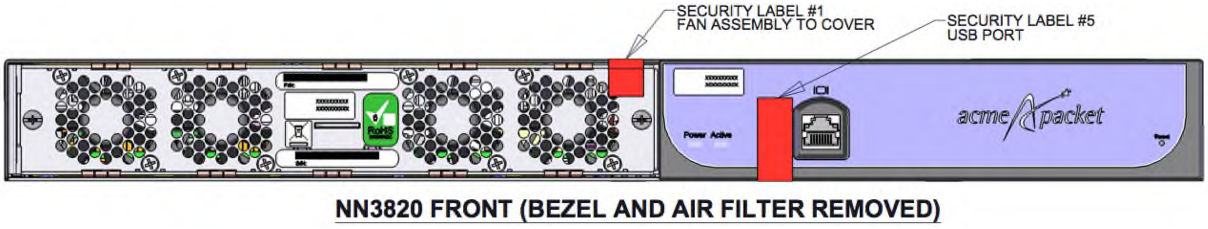

Figure 3 – Acme Packet 3820 Tamper Evidence Label Placement / Front

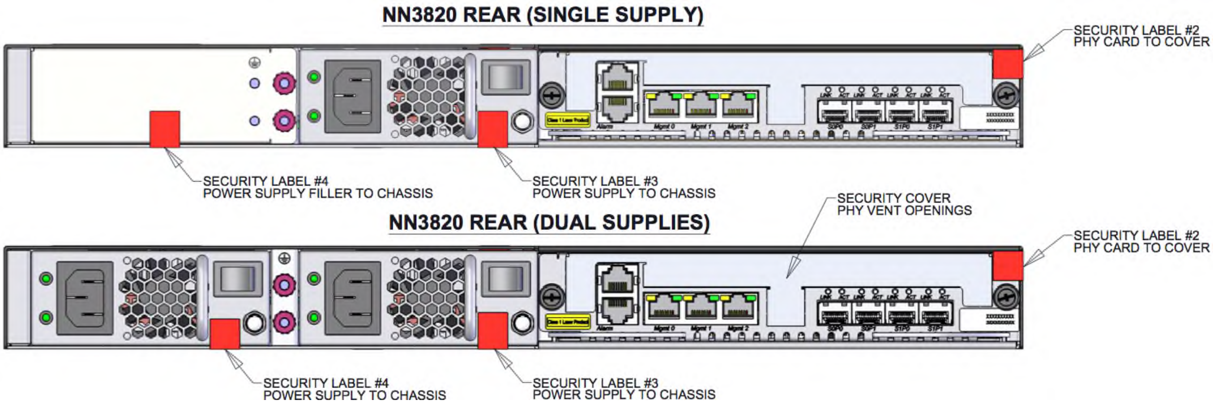

Figure 4 – Acme Packet 3820 Tamper Evidence Label Placement / Rear

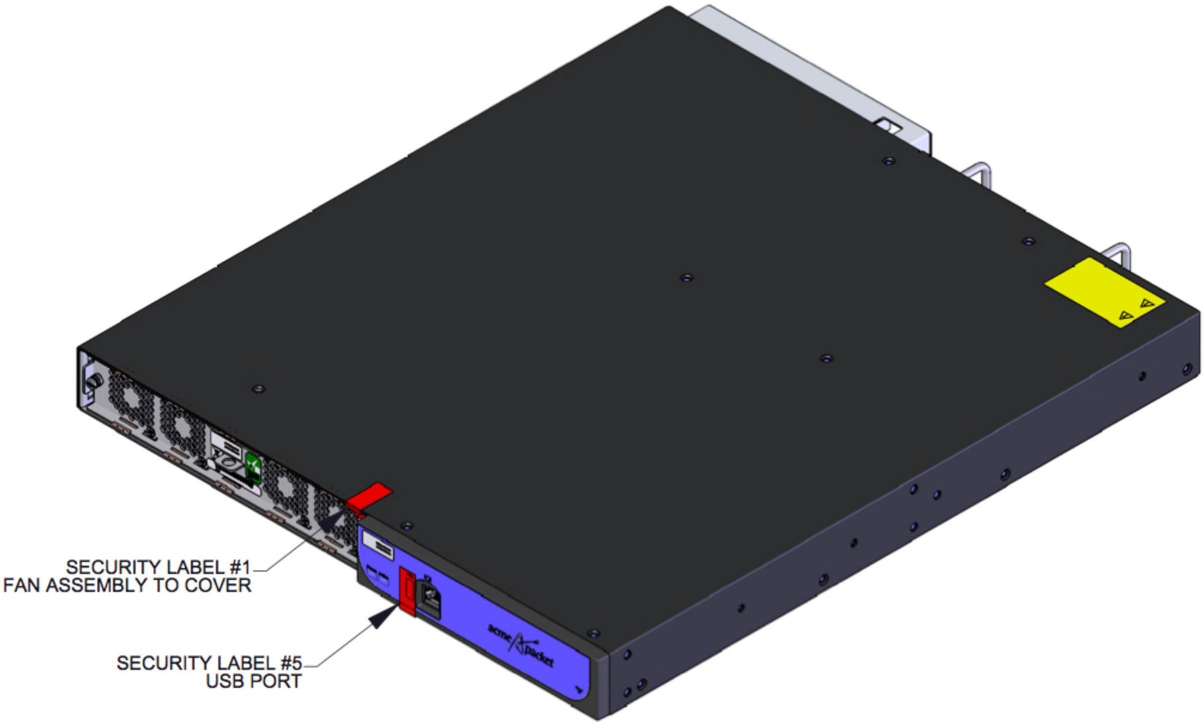

Figure 5 – Acme Packet 3820 Tamper Evidence Label Placement Top/Front

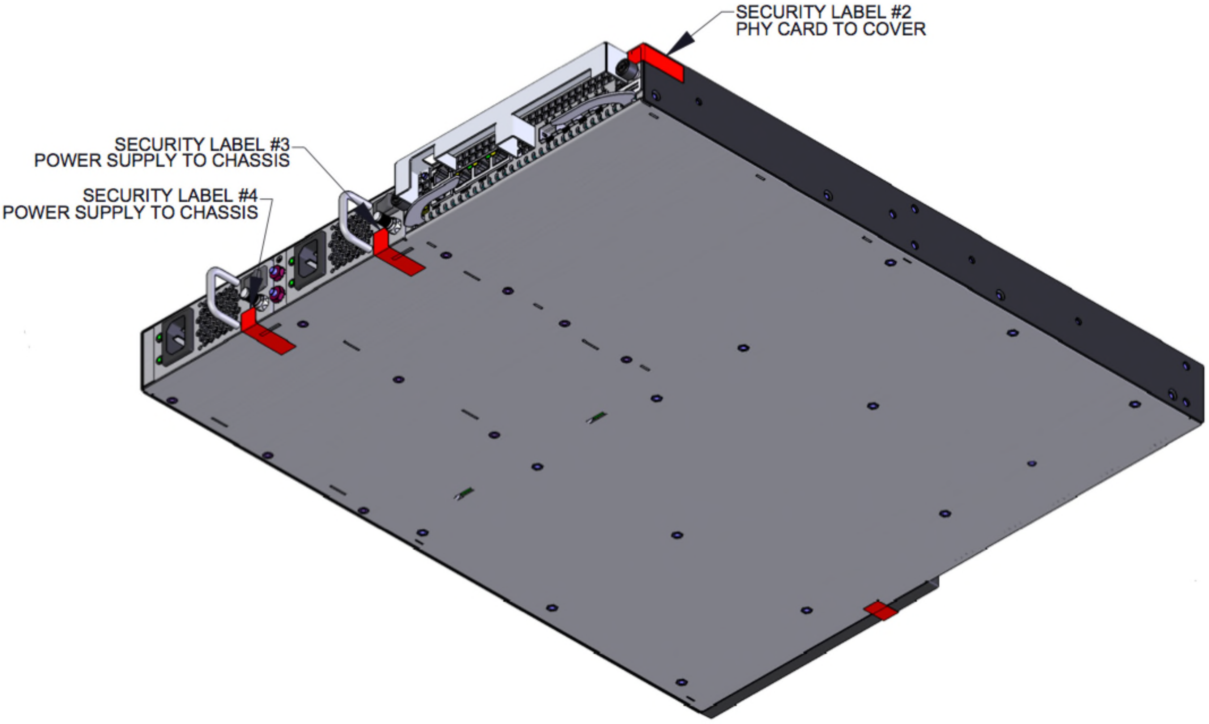

Figure 6 – Acme Packet 3820 Tamper Evidence Label Placement Bottom/Rear

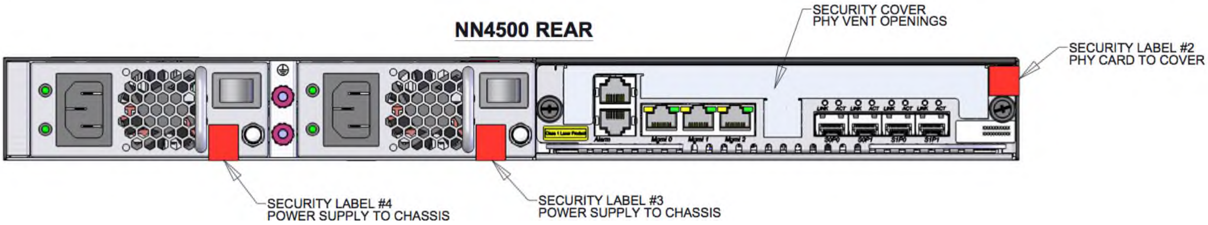

Figure 7 – Acme Packet 4500 Tamper Evidence Label Placement Rear

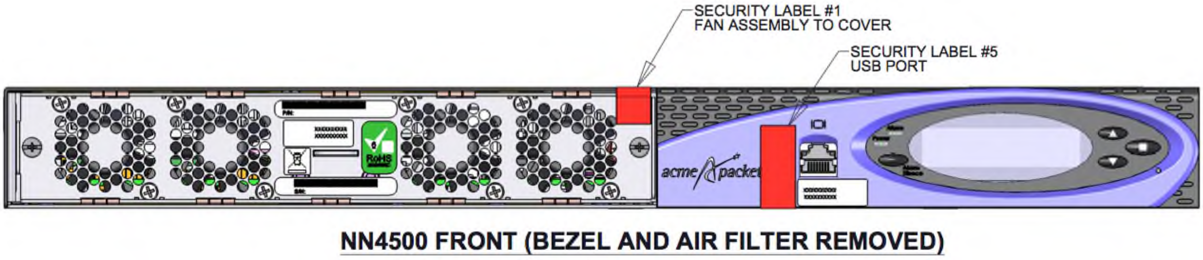

Figure 8 – Acme Packet 4500 Tamper Evidence Label Placement Front

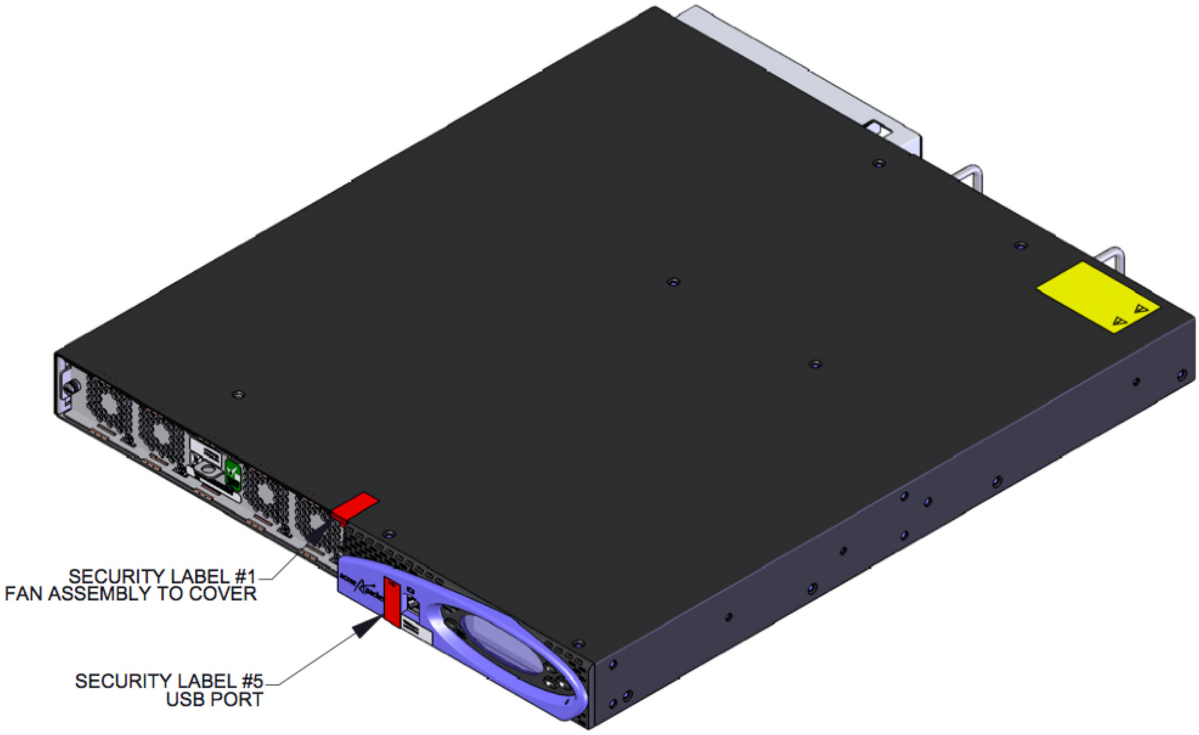

Figure 9 – Acme Packet 4500 Tamper Evidence Label Placement Top/Front

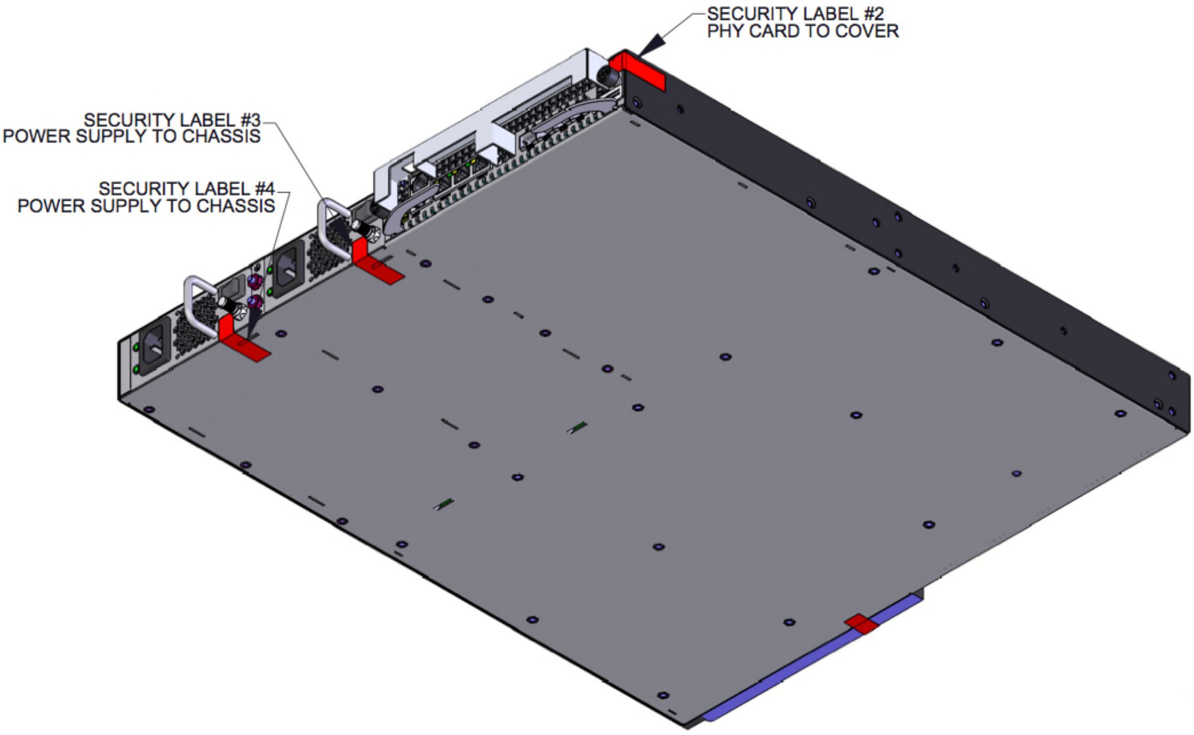

Figure 10 – Acme Packet 4500 Tamper Evidence Label Placement Rear Bottom

Note that Oracle Communications does offer the purchase of additional labels. If labels need to be replaced, please contact Oracle Communications to return the module for reimaging, and Oracle Communications will reimage the module and provide additional label (internal part number LBL-0140-60).

3.2 User Guidance

3.2.1 General Guidance

The User must not disclose passwords and must store passwords in a safe location and according to his/her organization's systems security policies for password storage.

End of Document